Republic of the Union of Myanmar

Ministry of Communications and Information Technology

Data Collection Survey
for
Cyber Security
in
Republic of the Union of Myanmar

Final Report

November 2015

Japan International Cooperation Agency (JICA)

Mitsubishi Research Institute Inc.

Yachiyo Engineering Co., Ltd.

EI
CR (5)
15 - 177

Table of Contents

Table of Contents
List of Figures and Tables
Pictures of Survey
Abbreviations

Chapter 1 Background to the Project 1-1

Chapter 2 Overview of the Project 2-1
2.1 Objectives of the Project 2-1
2.2 Relevant Organization 2-1
2.3 Work Plan 2-2
2.4 Main Activities in the On-site Survey 2-3

Chapter 3 Survey of the Basic Information on the Information and Communication Sector 3-1
3.1 General Information 3-1
3.2 Situation of Internet Usage 3-5
3.3 Situation on the Internet Usage by the Government and Commerce 3-7
3.4 Main ICT Systems and Facilities 3-9

Chapter 4 Survey of Current Situation of Cyber Security 4-1
4.1 Incidents and Statistics relating to Cyber Security 4-1
4.2 Organizations relating to Cyber Security 4-2
4.3 Cyber Security Strategies, Policies, Legal Systems and Guidelines 4-10
4.4 Development of Human Resources in the Science & Technology, IT and Cyber Security Fields 4-15
4.5 Activities of Government Organizations in Charge of Security Measures 4-19
4.6 Assistance in the Cyber Security Field Provided by Other Governments and Donors 4-27
4.7 Comparison with Other ASEAN Countries 4-31

Chapter 5 Status of Security Countermeasures in Government and Related Organizations 5-1
5.1 Security Assessment for Government ICT Environment 5-1
5.2 Vulnerability Assessment on e-Government System 5-7
5.3 Vulnerability Assessment for Website of Government Organization 5-11
5.4 Evaluation of Governmental Data Center 5-14
5.5 Other Security Enhancement Facility in Government 5-19
5.6 Security Measures Taken by Telecommunications Carriers 5-19
5.7 Security Measures of Central Bank System 5-21

5.8 Trend and Needs of Private Sector 5-22

Chapter 6 Consideration of Cyber Security Issues and Countermeasures 6-1
6.1 Cyber Security Countermeasure Issues of Government Cyber Security Countermeasure Related Organization, Government Organization and Related Organization 6-2
6.2 Cyber Security Countermeasures for Each Issue 6-3
6.3 Order of Countermeasures 6-7

Chapter 7 Study on the Contents and Priorities in Japanese Assistance 7-1
7.1 Policy on the Study on Assistance Measures 7-1
7.2 Study on the Assistance Plan 7-2
7.3 Analysis of the Technical Cooperation Project with the Five Criteria for Evaluating ODA Project and Conclusion 7-9
7.4 Study on the Relevance of the Request for Grant Aid Assistance 7-14

Chapter 8 Conclusion and Future Issues 8-1

List of Figures and Tables

Chapter 2

Figure 2.3-1 Work Plan 2-2
Table 2.2-1 Major relevant organization 2-1
Table 2.4-1 Member of the survey and Assignment 2-3
Table 2.4-2 Survey Schedule 2-4

Chapter 3

Figure 3.1-1 Map of Myanmar 3-3
Figure 3.2-1 Number of Internet Users with Wired Connection 3-6
Figure 3.2-2 Internet Connection Speed (Gbps) and Number of Mobile Phone Users 3-6
Figure 3.2-3 Number of Internet Users 3-6
Table 3.1-1 Populations of the administrative divisions 3-3
Table 3.1-2 Major economic indices of Myanmar 3-5
Table 3.2-1 Internet Fees 3-7
Table 3.3-1 e-commerce-related activity 3-8
Table 3.4-1 Government-run data centers 3-11

Chapter 4

Figure 4.1-1 Cyber security incidents reported by mmCERT 4-2
Figure 4.1-2 Source region of cyber-attacks reported by mmCERT 4-2
Figure 4.2-1 Organizational interrelation 4-3
Figure 4.2-2 Organizational chart of MCIT 4-6
Figure 4.2-3 Organizational chart of the Ministry of Science and Technology 4-8
Figure 4.2-4 Organizational chart of the Ministry of Education 4-9
Table 4.1-1 Incidents relating Cyber Security in Myanmar 4-1
Table 4.3-1 Expected cyber security strategy, policy, legal system or guideline in Myanmar 4-11
Table 4.5-1 List of cyber security measures taken by ministries and agencies 4-27
Table 4.6-1 Assistance provided by other donor countries and international organizations 4-29
Table 4.6-2 Records of Japan's assistance 4-30
Table 4.7-1 e-Government Development Index of ASEAN countries 4-31
Table 4.7-2 Global Cyber Security Index of ASEAN countries 4-32
Table 4.7-3 Categorization of ASEAN countries to review possible international collaboration 4-33

Chapter 5

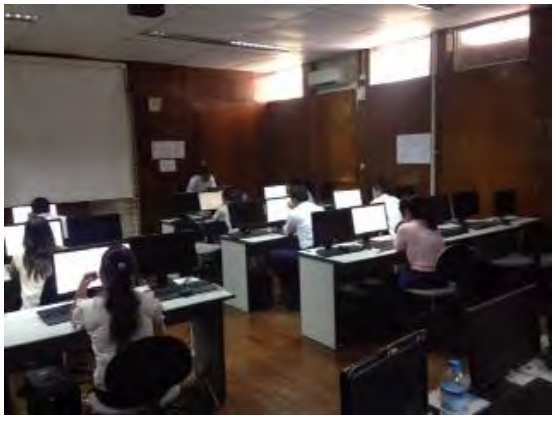
Figure 5.1-1 Current ICT environment of Myanmar government 5-5
Figure 5.1-2 Japanese Government ICT environment 5-6

Figure 5.1-3 Expected ICT environment for Myanmar government 5-6
Figure 5.2-1 System structure of e-Document Management System 5-9
Figure 5.2-2 Result of vulnerability test on Internet side port 5-10
Figure 5.2-3 Result of vulnerability test on Internet side port 5-11
Figure 5.3-1 Website of MCIT 5-12
Figure 5.3-2 Vulnerability Scan Result of the webserver 5-13
Figure 5.4-1 Gate 5-15
Figure 5.4-2 Security guard post 5-15
Figure 5.4-3 Outdoor surveillance camera 5-16
Figure 5.4-4 Building entrance 5-16
Figure 5.4-5 Entrance in Building 5-16
Figure 5.4-6 Server room entrance (fingerprint authentication) 5-17
Figure 5.4-7 Office entrance 5-17
Figure 5.4-8 UPS power supply cable 5-17
Figure 5.4-9 Distribution line (2 system) 5-18
Figure 5.4-10 Emergency power generator 5-18
Table 5.2-1 e-Government systems in S-12 data center 5-8
Table 5.4-1 Data Center Survey Items 5-14
Table 5.4-2 Data Center Survey Area and Place 5-14

Chapter 6
Table 6.2-1 Cyber Security Countermeasures 6-3
Table 6.3-1 Roadmap of Development of Laws, Standards and Guidelines and Reinforcement of Organizational Structure 6-8
Table 6.3-2 Roadmap of Functional Reinforcement 6-9
Table 6.3-3 Roadmap of Reinforcement of Cooperation and Awareness Raising 6-9

Chapter 7
Figure 7.4-1 Data centers and the locations of the installation of the equipment requested for procurement in the grant aid assistance 7-15
Table 7.2-1 Results of the evaluation of cyber security measures assumed for the implementation in Myanmar with the policy on the study on the assistance measures for the Japanese assistance 7-3
Table 7.2-2 Main activities assumed in the draft technical cooperation project 7-7

Pictures of Survey

<table>
<tr><td>  </td><td>  </td></tr>
<tr><td>mmCERT has established in 2010 to collect information, support, and make adjustments to cyber security measures.</td><td>Discussion between Ministry of Communications and Information Technology (MCIT) and JICA Survey Team.</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>The survey team paid a courtesy call on the Deputy Minister of MCIT and reported the state of survey halfway.</td><td>Explanation of the result of on-site survey. About 60 members from 33 organizations participated.</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>ICTTI provides various IT-related training courses that continue for from several weeks to several months are implemented for students who have graduated from the university.</td><td>The data center in Dekkhina provides space, power supply, networking service and so on for the government and private companies as the hosting service.</td></tr>
</table>

Abbreviations

ADB	Asian Development Bank
ADS	Anti DDoS System
APCERT	Asia Pacific Computer Emergency Response Team
CB Bank	Co-operative Bank
CBM	Central Bank of Myanmar
CDMA	Code Division Multiple Access
CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response
CERT	Computer Emergency Response Team
CICC	Center of the International Cooperation for Computerization
CIO	Chief Information Officer
CS	Cyber Security
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer
DAC	Development Assistance Committee
DDoS	Distributed Denial of Service attack
DLP	Data Loss Prevention / Data Leak Protection
DoS	Denial of Service attack
DPI	Deep Packet Inspection
DSL	Digital Subscriber Line
E/N	Exchange of Notes
EDI	Electronic Data Interchange
EDMS	Electronic Document Management System
EGDI	e-Government Development Index
e-NTF	e-National Task Force
ERP	Enterprise Resource Planning
EU	European Union
FW	Firewall
GCI	Global Cyber Security Index
GDP	Gross Domestic Product
GNI	Gross National Income
GSM	Global System for Mobile Communications
GSOC	Government Security Operation Coordination team
ICT	Information and Communications Technology
ICTTI	Information and Communication Technology Training Institute
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IMCEITS	India-Myanmar Centre for Enhancement of IT Skills

IPA	Information-technology Promotion Agency
IPS	Intrusion Prevention System
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT&CS	Information Technology and Cyber Security Department
ITU	International Telecommunication Union
JICA	Japan International Cooperation Agency
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center
KOICA	Korea International Cooperation Agency
LAN	Local Area Network
LG-WAN	Local Government Wide Area Network
MCF	Myanmar Computer Federation
MCIT	Ministry of Communications and Information Technology
MCPA	Myanmar Computer Professional Association
MJJI	Myanmar-Japan Joint Initiative
mmCERT	Myanmar Computer Emergency Response Team
MOCO	Ministry of Commerce
MOE	Ministry of Education
MOH	Ministry of Health
MOST	Ministry of Science and Technology
MPT	Myanmar Posts and Telecommunications
MPU	Myanmar Payment Union
MTU	Mandalay Technological University
NCC	National Consumer Council
NCDP	National Comprehensive Development Plan
NCSC	National Cyber Security Center
NCSSC	National Cyber Security Steering Committee
NDC	Nai Pyi Taw Development Committee
NISC	National Center of Incident Readiness and Strategy for Cyber Security
ODA	Official Development Assistance
PCIDSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure
POC	Point of Contact
PPP	Public Private Partnerships
PTD	Posts and Telecommunications Department
PTU	Pyay Technological University
SLA	Service Level Agreement

SNS	Social Networking Service
UCSM	University of Computer Studies, Mandalay
UCSY	University of Computer Studies, Yangon
UPS	Uninterruptible Power Supply
USAID	United States Agency for International Development
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
WB	World Bank
W-CDMA	Wideband Code Division Multiple Access
WiMax	Worldwide Interoperability for Microwave Access

Chapter 1 **Background to the Project**

The necessity of measures to ensure cyber security has increasingly been felt as the Internet has rapidly spread. Especially, cases of damage from cyberattacks on government bodies and private business, such as illegal falsification of websites, leakage of confidential information, forcibly shutting down critical systems, have been increasing all over the world. In Japan, it was found in 2011 that industries related to defense and infrastructure, including heavy industry companies, both the Houses of Representatives and Councilors, and central government ministries and agencies, came under cyberattack one after another, and the Japanese government started measures to reinforce cyber security by enhancing information cooperation between the public and private sectors.

Japan is making efforts to create safe and secure environments for using information communication technology (ICT) in the ASEAN region, including Japan and Myanmar, within the framework of the ASEAN economic ministers' meeting "Asia Knowledge Economy Initiative" in 2008 and the Japan-ASEAN Information Security Policy meeting, which has been going on since 2009. In Myanmar, information communication is superintended by the Ministry of Communication and Information Technology (MCIT). MCIT has been promoting the formulation of a Myanmar government master plan, receiving cooperation from the Asian Development Bank since 2014, and the importance of cyber security measures has increasingly been recognized in the country.

In this situation, the Myanmar government established the Myanmar Computer Emergency Response Team (hereafter referred to as "mmCERT") in 2010 as an organization to collect information, support, and make adjustments to cyber security measures. In 2013, a national cyber security operation committee was set up as an organization to promote cyber security, which has been tackling the reinforcement of cyber security in Myanmar. In April 2015, an IT cyber security agency, under the command of the MCIT which would take charge of cyber security in the Myanmar government, was established.

In the field of cyber security, balanced reinforcement of laws and regulations, organizations, and human development, and cooperation between public and private sectors are necessary. However, the Myanmar government's comprehensive strategy, role sharing among government organizations and between public and private sectors, progress in the present measures, and policy for reinforcement are not clear.

It is necessary to put in order the items to be reinforced and their priorities and make clear the fields where Japan can extend its support as Myanmar will try to improve its cyber security.

Chapter 2 **Overview of the Project**

2.1 **Objectives of the Project**

The objectives of this project is to collect and confirm information on the strategy and policy related to the cyber security in Myanmar, the present situation of cyber security measures of the related government agencies and private enterprises, and challenges in the respective fields. To understand and analyze the needs of Japanese cooperation in the field of cyber security and confirm the direction of support from Japan's ODA are also investigated in the project.

2.2 **Relevant Organization**

The major relevant organizations of Japan and Myanmar in this survey are shown in Table2.2-1

Table2.2-1 Major relevant organization

Organization	Abbreviation
Japan	
National Center of Incident Readiness and Strategy for Cyber security	NISC
Japan Computer Emergency Response Team / Coordination Center	JPCERT/CC
NEC Corporation	NEC
FUJITSU LIMITED	FUJITSU
NTT Communications	NTT Com
Myanmar	
Ministry of Communications and Information Technology	MCIT
Posts and Telecommunications Department	PTD
Myanmar Posts and Telecommunications	MPT
Information Technology and Cyber Security Department	IT&CS
Myanmar Computer Emergency Response Team	mmCERT
Ministry of Science and Technology	MOST
Ministry of Education	MOE
National Cyber Security Steering Committee	NCSSC
Ministry of Health	MOH
Ministry of Commerce	MOCo
Nai Pyi Taw Development Committee	NDC
Ministry of National Planning and Economic Development	MNPED
Information and Communication Technology Training Institute	ICTTI
Yangon Technological University	YTU
Central Bank	CB
Myanmar – Japan Center	MJC
Myanmar Computer Federation	MCF
KDDI Summit Global Myanmar Company Limited	KSGM
Yatanarpon Teleport	Yatanarpon
RedLink	RedLink
Vision to Motion	V2M
Alpha	Alpha
Korea International Cooperation Agency	KOICA
Asian Development Bank	ADB
World Bank	WB

2.3 **Work Plan**

The work plan is shown in Figure2.3-1

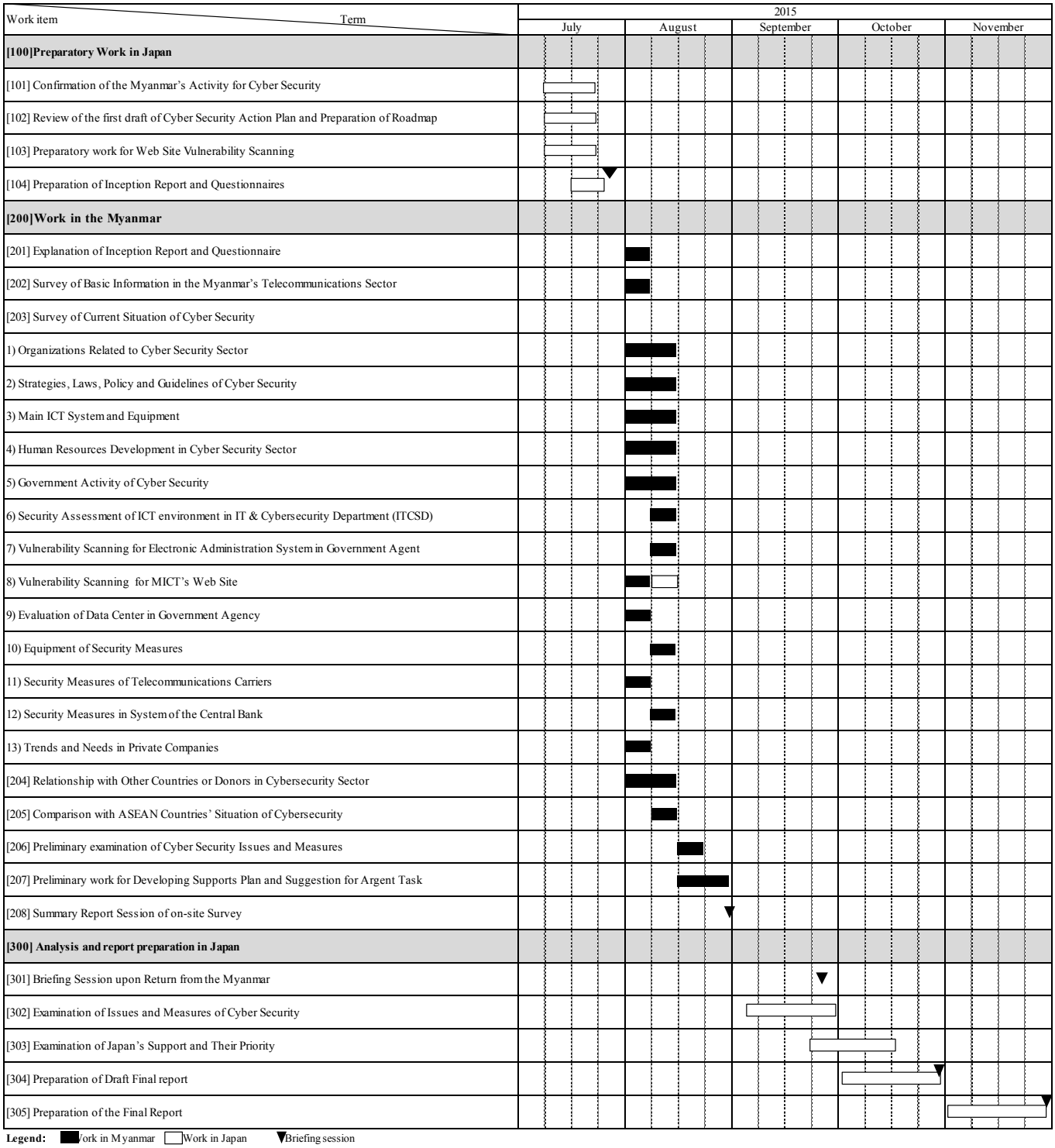


Figure2.3-1 Work plan

2.4 Main Activities in the On-site Survey

The survey team members and their main activities are shown in Table2.4-1. The survey schedule is shown in Table2.4-2

Table2.4-1 Member of the survey and Assignment

Name	Organization	Assignment	Main Activities	Stay Schedule
Mr. Akio SATO	MRI	Chief Consultant/ Cyber Strategy	Management of the project Investigation of the strategy in the field of the cyber security	2015/8/2 – 8/29
Mr. Masayasu MURANO	MRI	Security Measure Plannng1/ Vulnerability Assessment	Consideration of measures of regulation, legislative system and guideline Evaluation of the WEB site vulnerability	2015/8/2 – 8/7, 2015/8/23 – 8/28
Mr. Takashi NAKAMURA	MRI	Security Measure Planning 2/ Security Assessment	Security assessment and evaluation of the e-Government system	2015/8/11 – 8/29
Mr. Kengo MIYAMOTO	YEC	Data Center Evaluation	Evaluation of the Data Center of the related government agencies	2015/8/2 – 8/29
Mr. Yoshitaka IKEDA	YEC	ICT System	Consideration of maintenance plan of ICT and equipment for cyber security	2015/8/2 – 8/29
Mr. Naoaki NAMBU	YEC	Human Resource Development/ Assistance Plan	Consideration of support based on the development of human resources	2015/8/2 – 8/30

Table2.4-2 Survey Schedule

No.	Date		JICA	Survey Team						Stay
			Leader	Chief Consultant / Cyber strategy	Human Resource Development /Assistance Plan	ICT system	Data Center Evaluation	Security Measures Planning1/Vulnerability Assessment	Security Measures Planning2/ Security Assessment	
1	2015/8/2	Sun	Moving [Tokyo→Yangon]	Moving [Tokyo→Yangon]						Yangon
2	2015/8/3	Mon	AM: 09:00, Courtesy call on Embassy of Japan in Myanmar and explanation of the survey schedule and Inception Report 10:30, Explanation of Inception Report (mmCERT) PM: Visit of a Japanese Company in Myanmar							Yangon
3	2015/8/4	Tue	Moving [ND101 Yangon(7:00) → Nay Pyi Taw(7:55)] AM: Explanation of Inception Report and Minutes of Meeting (IT Cyber Security Department) PM: Team meeting				Moving [ND101 Yangon(7:00) → Nay Pyi Taw(7:55)] AM: Joint explanation of Inception Report and Minutes of Meeting (IT Cyber Security Department) PM: Data Center evaluation	Moving [ND101 Yangon(7:00) → Nay Pyi Taw(7:55)] AM: Joint explanation of Inception Report and Minutes of Meeting (IT Cyber Security Department) PM: Team meeting		Nay Pyi Taw
4	2015/8/5	Wed	AM: Team meeting PM: Explanation of Inception Report and Minutes of Meeting (MOST, MOE)				Data Center Evaluation	WEB site vulnerability assessment		Nay Pyi Taw
5	2015/8/6	Thurs	AM: Team meeting PM: Signing Minutes of Meeting Moving [Nay Pyi Taw → Yangon] Report to Embassy of Japan in Myanmar and JICA Myanmar office	AM: Team meeting PM: Signing Minutes of Meeting Moving [ND9110 Nay Pyi Taw(18:20) → Yangon(19:20)]	AM: Team meeting PM: Signing Minutes of Meeting		AM: Team meeting PM: Signing Minutes of Meeting Moving [ND9110 Nay Pyi Taw(18:20) → Yangon(19:20)]	AM: Team meeting PM: Signing Minutes of Meeting Moving [ND9110 Nay Pyi Taw(18:20) → Yangon(19:20)]		Yangon Nay Pyi Taw
6	2015/8/7	Fri	Moving [In-flight → Japan (6:50)]	AM: Explanation of Inception Report (Myanmar Computer Federation) PM: Explanation of Inception Report (Central Bank) Data Center Evaluation(Hanthawady)	AM: Hearing and gathering information (MOC) PM: Hearing and gathering information (MOI)		AM: Explanation of Inception Report (Myanmar Computer Federation) PM: Explanation of Inception Report (Central Bank) Data Center Evaluation(Hanthawady)	Moving [In-flight → Japan (6:50)]		Yangon Nay Pyi Taw In-flight
7	2015/8/8	Sat		Moving [ND107 Yangon(11:25) → Nay Pyi Taw(12:20)] Team meeting/gathering of the collected materials	Team meeting/gathering of the collected materials		Moving [ND107 Yangon(11:25) → Nay Pyi Taw(12:20)] Team meeting/gathering of the collected materials			Naypyidaw
8	2015/8/9	Sun		Gathering of the collected materials						Nay Pyi Taw
9	2015/8/10	Mon		AM: Hearing and gathering information (MOCO) PM: Hearing and gathering information (MOH)						Nay Pyi Taw
10	2015/8/11	Tue		AM: Hearing and gathering information (NDH) PM: Data Center Evaluation(Dekhina)					Moving [Tokyo(11:00) → Yangon(15:40)] Moving [ND111 Yangon(18:25) → Nay Pyi Taw(19:20)]	Nay Pyi Taw
11	2015/8/12	Wed		AM: Courtesy call on Deputy Minister of MCIT PM: Data analysis			AM: Courtesy call on Deputy Minister of MCIT PM: Data Center evaluation(Dekhina)	WEB site vulnerability assessment from Japan	EDMS vulnerability assessment	Nay Pyi Taw
12	2015/8/13	Thurs		AM: Team meeting PM: Hearing of ADB	AM: Team meeting PM: Hearing of ADB Hearing of MONPED		AM: Team meeting PM: Hearing of ADB		AM: Team meeting PM: Hearing of ADB	Nay Pyi Taw
13	2015/8/14	Fri		AM: Team meeting PM: Hearing of MPT					AM: Team meeting PM: Hearing of MPT	Nay Pyi Taw
14	2015/8/15	Sat		Team meeting					Team meeting	Nay Pyi Taw
15	2015/8/16	Sun		Team meeting					Team meeting	Nay Pyi Taw
16	2015/8/17	Mon		Supplemental survey					Supplemental survey	Nay Pyi Taw
17	2015/8/18	Tue		Data Center evaluation(S12)	Data analysis	Data analysis	Data Center evaluation(S12)		Data Center evaluation(S12)	Nay Pyi Taw
18	2015/8/19	Wed		Supplemental survey Moving [ND122 Nay Pyi Taw(18:30) → Yangon(19:25)]	Data analysis	Supplemental survey Moving [ND122 Nay Pyi Taw(18:30) → Yangon(19:25)]	Supplemental survey Moving [ND122 Nay Pyi Taw(18:30) → Yangon(19:25)]		Supplemental survey Moving [ND122 Nay Pyi Taw(18:30) → Yangon(19:25)]	Nay Pyi Taw
19	2015/8/20	Thurs		AM: Hearing of ITIP PM: Hearing of YTU Hearing of KOICA	Data analysis	AM: Hearing of ITIP PM: Hearing of YTU Hearing of KOICA	AM: Hearing of JICA PM: Hearing of YTSY Hearing of RONETZ		AM: Hearing of JICA PM: Hearing of YTSY Hearing of RONETZ	Nay Pyi Taw
20	2015/8/21	Fri		AM: Hearing of MJCHRD PM: Hearing of WB	Data analysis	AM: Hearing of MJCHRD PM: Hearing of WB	AM: Hearing of RedLink PM: Hearing of Vison to Motion MyanmarCo., LTD		AM: Hearing of RedLink PM: Hearing of Yatanapon	Nay Pyi Taw
21	2015/8/22	Sat		AM: Hearing of Fujitsu Moving [SD102 Yangon(18:00) → Nay Pyi Taw(18:50)]	Data analysis	AM: Hearing of Fujitsu Moving [SD102 Yangon(18:00) → Nay Pyi Taw(18:50)]	AM: Hearing of Fujitsu Moving [SD102 Yangon(18:00) → Nay Pyi Taw(18:50)]		AM: Hearing of Fujitsu Moving [SD102 Yangon(18:00) → Nay Pyi Taw(18:50)]	Nay Pyi Taw
22	2015/8/23	Sun		Team meeting				Moving [Tokyo(11:00) → Yangon(15:40)] Moving [SO102 Yangon(18:00) → Nai Pyi taw(18:50)]	Team meeting	Nay Pyi Taw
23	2015/8/24	Mon		AM: Team meeting PM: Hearing of MCIT		AM: Team meeting PM: Preparation for Survey report session of on-site survey	AM: Team meeting PM: WEB vulnerability assessment			Nay Pyi Taw
24	2015/8/25	Tue		Preparation for Survey report session of on-site survey						Nay Pyi Taw
25	2015/8/26	Wed		Preparation for Survey report session of on-site survey						Nay Pyi Taw
26	2015/8/27	Thurs		AM: Summary report session of on-site survey Moving [UB104 Nay Pyi Taw(18:10) → Yangon(19:00)]				AM: Summary report session of on-site survey Moving [UB104 Nay Pyi Taw(18:10) → Yangon(19:00)] Moving [Yangon (21:45) → In-flight]	AM: Summary report session of on-site survey Moving [UB104 Nay Pyi Taw(18:10) → Yangon(19:00)]	Yangon In-flight
27	2015/8/28	Fri		Survey results report to Embassy of Japan in Myanmar and JICA Myanmar office, and greetings of return Moving[Yangon (21:45) → In-flight]				Moving [In-flight →Japan (6:50)]	Survey results report to Embassy of Japan in Myanmar and JICA Myanmar office, and greetings of return Moving [Yangon (21:45) → In-flight]	In-flight
28	2015/8/29	Sat		Moving [In-flight →Japan (6:50)]	Moving [In-flight(7:30) →In-flight]	Moving [In-flight →Japan (6:50)]	Moving [In-flight →Japan (6:50)]		Moving [In-flight → Japan (6:50)]	In-flight
29	2015/8/30	Sun			Moving [In-flight → Botswana]					

Chapter 3 Survey of the Basic Information on the Information and Communication Sector

3.1 General Information

3.1.1 Geographical Features

Myanmar is located in the western part of the Indochina Peninsula in the southeast area. It is characterized by the territory which is long in the north-south direction stretching from 10°N to 28°N. It is bordered by China, Thailand and Laos in the east and India and Bangladesh in the west. The total length of the international border with these countries is approx. 4,600 km. It is fringed by the Gulf of Martaban and the Bay of Bengal, both of which are parts of the Indian Ocean, to the south. The total length of the shoreline in Myanmar is approx. 2,000 km. It has a total area of 676,578 km^2, 19.2 % of which is used as farmland.

The Ayeyarwady River, which flows between two mountain ranges, runs through the country from the north to the south and divides the country in the eastern and western parts. It has formed a huge delta near its mouth, which is the largest rice producing area in Myanmar thanks to the fertile soil and abundant water resource. The Salween River flows in the eastern part of the country, having its origin in Tibet. It flows through Yunnan Province of China and the Shan Hills in northeastern Myanmar and flows into the Gulf of Martaban. Because of the presence of many rapids, navigation of ships on the river is limited. Therefore, the river is not expected to contribute to the economic development of the river basin.

The Ayeyarwady River divides the mountainous land of Myanmar with many large and small rivers into the eastern and western parts. Because of this topographic condition, infrastructure in the country has been developed in the north-south direction along the Ayeyarwady River. The trunk lines of roads, railways, etc. have been constructed between Yangon and Mandalay and branch lines run from the trunk lines in the east-west direction. While the trunk roads and rail lines in the north-south direction have been the major routes of physical distribution for a long time, the infrastructure development in the east-west direction has been hampered by the presence of mountains and numerous rivers.

3.1.2 Climate

Most of Myanmar is in the tropical and subtropical climate zones. There are three distinct seasons in the year, *i.e.* the hot season in April and May, the rainy season from June to mid-October and the dry season from late October to March. Myanmar has a hot and humid summer with many cloudy and rainy days between June and September because it is strongly affected by the southwestern monsoon, which brings humid and warm air to the area in this period. The country has many fine days and little rainfall between December and April because it is strongly affected by the northeastern monsoon, which brings dry air to the area at this time. There are also significant regional differences in temperature and precipitation within Myanmar because it is long in the north-south direction and there is significant elevation difference within the country. Even the tundra climate is found in the northern part of the country where the elevation is above 3,000 m.

Heavy rainfall in the rainy season has caused many disasters in Myanmar. Flood disasters occur almost every year in the basins of the Chindwin, Ayeyarwady and Salween Rivers. Recently, the heavy rainfall which began in mid-July 2015 caused a large-scale flood disaster. The President, Thein Sein declared a state of emergency in four local administrative divisions, Chin State, Rakhine State, Sagaing Region and Magway Region. More than 100 people were killed and 1.6 million people were affected by this flood and the people in 380,000 households were evacuated. (Myanmar: Floods Emergency Situation Report No. 5 as of 21 August 2015)

Cyclones are likely to form in the Bay of Bengal in the periods called the pre-monsoon season (in April and May) and the post-monsoon season (in September and October). These cyclones usually move toward Bangladesh and India. In rare occasions, cyclones have struck Myanmar, as Cyclone Nargis, which formed in April 2008, did. This cyclone caused great damage to the country including more than 100,000 people dead or missing.

3.1.3 **Society and Population**

The Union of Burma gained independence from the United Kingdom in 1948. Yangon had been its capital since the independence until the capital was relocated to Naypyidaw in 2006 for its geographic advantage. After several changes of names, the country officially became the Republic of the Union of Myanmar in 2010.

There are more than 100 ethnic groups living in Myanmar. The Burmese account for 68 % of the population and smaller ethnic groups account for the remaining 32 % (Shan: 9%, Karen: 7%, Rakhine: 4%, Chinese: 3%, Indians: 2 %, Mon: 2% and the others: 5%). Although there is little discrimination and few conflicts between those ethnic groups, there is a problem that the government does not give the nationality of Myanmar to certain ethnic groups. As the government recognizes the Rohingya people living in a large number in Rakhine State as immigrants from Bangladesh in Myanmar, they are unable to obtain Myanmar nationality. The Rohingya people are Muslims who are minority in Myanmar and they have been involved in conflict with Buddhists and have been persecuted recently. Nearly 90 % of the people in Myanmar are Buddhists, followed by Christians (4 %), Muslims (4 %) and others (1 %).

Figure 3.1-1 Map of Myanmar

Source: d-maps.com

Myanmar consists of seven regions, seven states and the Naypyidaw Union Territory. While a region and a state have an equivalent status, the former is used for the areas where the Burmese live in a large number and the latter is used for the areas where the minority groups live in a large number. Each state is named after the major ethnic group in the area. Table 3.1-1 shows the population of each region and state. The total population and the population density of Myanmar are 50,279,900 people and 74.3 people/km^2, respectively.

Table 3.1-1 Populations of the administrative divisions

No.	Region/state/union territory	Population (people)
1	Ayeyarwady Region	6,184,829
2	Sagaing Region	5,325,347
3	Tanintharyi Region	1,408,401
4	Bago Region	4,867,373
5	Magway Region	3,917,055
6	Mandalay Region	6,165,723
7	Yangon Region	7,360,703
8	Kachin State	1,642,841
9	Kayah State	286,627
10	Kayin State	1,504,326
11	Shan State	5,824,432
12	Chin State	478,801
13	Mon State	2,054,393
14	Rakhine State	2,098,807
15	Naypyidaw Union Territory	1,160,242
Total		**50,279,900**

Source: Ministry of Immigration and Population "The 2014 Myanmar Population and Housing Census The Union Report Census Report Volume 2"

3.1.4 Economic Performance

The military government established after the coup d'état of the national armed forces in 1988 promoted an open economic policy including enactment of the Foreign Investment Act. The unrealistic foreign exchange rates and the rigid economic structure based on this policy hindered the economic development and created critical shortage of foreign exchange. In 2003, private banks and ordinary companies faced serious shortage of funds. In addition, the enactment of the Burmese Freedom and

Democracy Act of 2003 in the United States (US) against the detention of Ms. Aung San Suu Kyi was a serious blow to the industries in Myanmar. In 2004, the European Union (EU) decided to reinforce the sanctions against Myanmar with the addition of the prohibition on loans to state companies of Myanmar for the lack of the progress in the democratization. The rise of the official prices of energy by the Government of Myanmar led to large-scale demonstrations. The use of force on the demonstrators by the government led to the reinforcement of the economic sanctions by the US and the EU and enforcement of financial sanctions by Australia. Because of the failure of the economic policy of the military government and the economic sanctions imposed by various countries, the economy of the Myanmar had been in a slump for a long period.

However, after the release of Ms. Aung San Suu Kyi from house arrest in 2010 and the transfer to a civilian government with the establishment of the current Thein Sein Administration, the Western countries appreciated Myanmar's efforts for the political and economic reform. The US lifted the sanctions on the import of products of Myanmar except for some gemstones in 2012 and the EU lifted the economic sanctions against Myanmar except the embargo on export of weapons in 2013. The Thein Sein Administration has been taking measures for the democratization including the introduction of a managed floating rate system for the standardization of foreign exchange rates and amendment of the Foreign Investment Act for the facilitation of foreign investment.

The real GDP of Myanmar has been increasing at the rate of 6% - 8 % per year. The agriculture sector in which 70 % of the people are engaged has contributed most to its GDP. Although the share of the agriculture sector in GDP has been on the decline recently, it still accounts for more than 30 % of GDP of the country, followed by the manufacturing and commerce sectors, both of which account for approx. 20 % of GDP. Although GNI per capita of Myanmar once satisfied one of the criteria for the recognition as a "least developed country", "GNI per capita (average between 2008 and 2010) of less than US $ 992," it has been on the increase since it surpassed US $ 1,100 in 2011.

Table 3.1-2 Major economic indices of Myanmar

Item	2010/11	2011/12	2012/13	2013/14※1	2014/15※2
Real GDP (kyats)	39,847	43,368	47,851	54,756	63,323
Real GDP (billion US $)	49.6	56.2	55.8	56.8	65.3
Real GDP growth rate (%)	5.9	7.3	8.3	7.7	8.3
GNI per capita (US $)	799	1,107	1,164	1,183	1,270
Breakdown of GDP (%)					
Agriculture	36.9	32.5	30.5		
Mining	0.9	5.8	6.1		
Manufacturing	19.9	19.7	19.9		
Utilities	1.1	1.0	1.2		
Construction	4.6	4.7	4.9		
Commerce	20.0	19.3	19.4	―	
Transport and communications	12.4	12.8	13.3		
Financial	0.1	0.1	0.2		
Administration	2.3	2.1	2.6		
Miscellaneous	1.9	1.9	2.1		

Sources: "IMF Country Report No. 14/307 October 2014," International Monetary Fund;
Breakdown of GDP (%): Estimates from "Key Indicators for Asia and the Pacific 2014," Asian Development Bank

※1: Estimates, ※2: Projections

3.2 Situation of Internet Usage

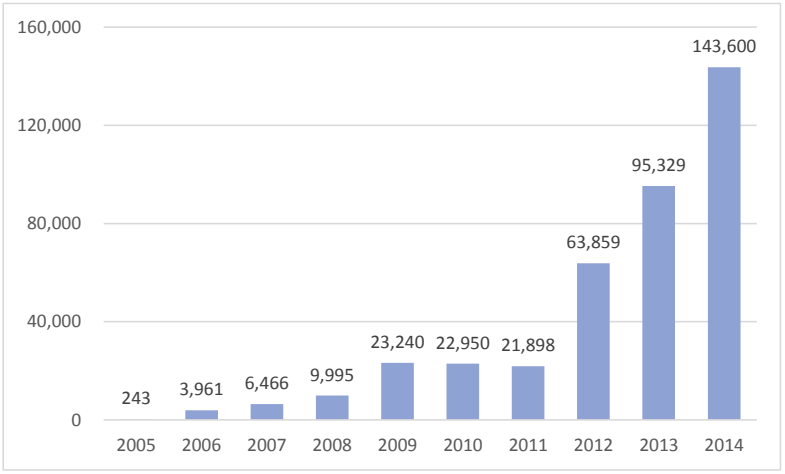
The statistics of Internet users with the wired connection as of 2014 reveal that it is as small as less than one percent of the population due to such problems as the scope of connectable area and high service fees. However, it is increasing in reality because of the rapidly growing mobile phone data communication services. Users that do not appear on statistical data are also increasing via Internet café and free Wi-Fi spots.

The recent increase is also promoted by the pay-as-you-go plans of mobile phone data communication services that are offered to make them available at a small fee, while high fixed-fee services are also provided mainly for business use.

The user increase not only expands the target of cyberattacks but leads to the diversification of attacking sources and expansion of damage involved and thus the importance of Internet security measures will grow.

3.2.1 Trend of Number of Internet Users

The number of Internet users was 243 in 2005 and it continued to increase steadily to 21,898 in 2011. It then nearly tripled to 63,859 in 2012 from the previous year and grew to 143,600 in 2014. However, it is still less than one percent of the population which is approx. 63 million.



Source: ITU [ICT Statistics]

Figure 3.2-1 Number of Internet Users with Wired Connection

The Internet connection is available at Internet café and as free Wi-Fi service at restaurants and other public space and thus the number of people to whom Internet is available on a regular basis is much bigger than the statistical data.

It is analyzed based on figures released by the MCIT that the number of Internet users increased to approx. 2.92 million as a result of a rapid increase in the number of mobile phone data communication users thanks to the improvement of Internet connection speed from 2013 to 2014.

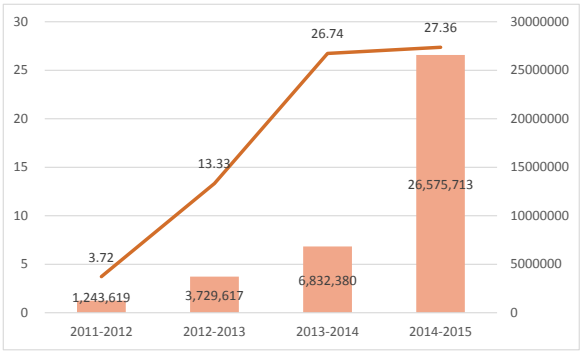


Figure 3.2-2 Internet Connection Speed (Gbps) and Number of Mobile Phone Users

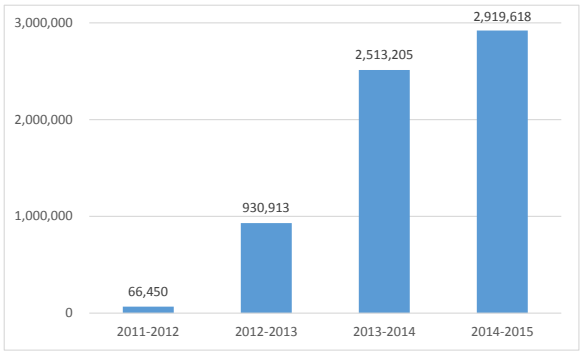


Figure 3.2-3 Number of Internet Users

Source: Produced based on MCIT [Ministry of Communications and Information Technology of the Republic] and ITU [ICT Statistics]

3.2.2 Internet Usage Fees

As for wired Internet connection fees, the service fees provided by MPT and RedLink are shown below. The Internet connection requires initial fees and monthly service fees and the monthly communication volume is unlimited. Although the fiber-optic connection is available at high speed up to 100 Mbps, it is only available within in a limited area. Other kinds of connection such as DSL and WiMax are also available although the speed is slower.

Table 3.2-1 Internet Fees

Service Provider	Connection Mode	Bandwidth	Initial Fee [MMK]	Monthly Fee [MMK]
MPT	DSL	512kbps	50,000	17,000
MPT	DSL	2.5Mbps	50,000	80,000
MPT	FTTx	1Mbps	200,000	100,000
MPT	FTTx	10Mbps	500,000	800,000
MPT	FTTx	100Mbps	1,000,000	7,000,000
RedLink	WiMax	512kbps	USD800	USD130
RedLink	FTTx	1Mbps	500,000	75,000
RedLink	FTTx	2Mbps	500,000	125,000

In Myanmar, Internet services are provided in GSM and CDMA types that are called 2G and W-CDMA type that is called 3G. The mobile phone Internet service requires data connection service use in addition to mobile phone subscription. Mobile phone subscription is to purchase a SIM card, which is sold at 1,500 kyats by all of the three mobile providers, MPT, ooredoo and Telenor. MPT charges the communication fee of 7.5 kyats per MB. All companies also provide various packaged services that include 2,800 kyats for every 400MB and 6,500 kyats per GB.

3.3 Situation on the Internet Usage by the Government and Commerce

3.3.1 e-Government Services

Face-to-face exchange of paper documents is mainly used in not only internal office work, but also administrative services to the citizens in administrative organizations in Myanmar. Various pilot projects including those for the introduction of electronic visa and passport systems, the establishment of smart schools and the introduction of electronic procurement and trade EDI systems have been implemented in the public-private partnership since the early 2000's as measures to develop an e-government. Although a huge amount of money has been invested on those projects, only a few of them have developed into full-scale projects partly because the absence of rules stipulating administrative procedures in government ministries and agencies and frameworks for inter-ministerial and inter-agency procedures has been an obstacle to the digitization. Myanmar government continues to promote the development of e-government. While the government is preparing "Myanmar e-Governance ICT Master Plan 2015" with the assistance from ADB (see Section 4.3 "Cyber Security Strategies, Policies, Laws and Guidelines" for reference), there is no coordination between government ministries and agencies on this matter because of the absence of the laws and guidelines on e-government and the absence of the coordination has resulted in such problems as inefficient procurement and slow progress in budgetary consideration in individual government ministries and agencies.

The currently-available major e-government services include the electronic visa service provided by the Ministry of Immigration and Population and the online company registration service provided by the Ministry of Commerce (MOC). It is possible to complete the entire process from application to fee payment on-line in these services. Other government ministries and agencies are also making efforts to develop e-government. The Ministry of Education (MOE) is planning to establish an educational portal site and MOC is planning to develop a system for the online issuance of import and export licenses. As exemplified above, government ministries and agencies are expected to begin to provide various online services. It is easy to expect that the increase in the number of online services will lead to the increase in cyberattacks on them. At present, government ministries and agencies are detecting and responding to cyberattacks independently and there is no system to share the information and experience on the attacks among them. Therefore, the establishment of GSOC as an organization to monitor networks and Websites of all the governmental organizations is recommended for the development of e-government.

3.3.2 **Electronic Commerce (e-Commerce)**

Because of the improvement in the Internet connection and the rapid increase of mobile phone users, the number of online stores selling clothing items and electric appliances has been on the increase for the last few years in Myanmar and particularly in Yangon. Not only large companies targeting the markets in the ASEAN countries, but also a large number of owners of actual stores and individuals have established online store sites. As a result, there are several hundreds of large and small online stores in Myanmar. However, cash payment is still the major payment methods despite the rapid development of an environment for online payment since around 2014 including the launch of mobile and Internet banking services by Co-operative Bank (CB Bank) and KBZ Bank and the launch of online services by an Internet mail order company which accept online payment. The online payment is not recognized by many people and it is still being developed.

The table below shows the recent e-commerce-related activities.

Table 3.3-1 E-commerce-related activity

Year	Month	E-commerce-related activity
2014	Feb.	The development of a basic accounting system of the Central Bank of Myanmar (CBM) began (a Grant-aid cooperation project of JICA).
	Jul.	Ayeyarwady Bank launched the first Internet banking service in Myanmar.
	Aug.	Co-operative Bank (CB Bank) and KBZ Bank launched mobile and Internet banking services.
2015	Feb.	Some airline companies and hotels began to accept online payment with Myanmar Payment Union (MPU) card.
	Apr.	MPT announced its plan to provide goods delivery and online payment services at 1,380 post offices in the country.

Year	Month	E-commerce-related activity
	May	CBM approved credit card services by the MPU-member banks.
	May	Zan IT Solution launched an e-book service through an Internet mail order site which accepts credit card payment.
	Jun.	MCIT established the IT and Cyber Security Department. The amendment of the Electronic Transaction Law and the preparation of the Cyber Security Bill began.
	Dec.	The Yangon Stock Exchange is expected to be opened.

Source: Information made public by CICC (the Center for the International Cooperation for Computerization)

The State Peace and Development Council enacted the Electronic Transaction Law as legislation governing e-commerce in 2004. The purposes of this law are as follows:

- To provide technical assistance in e-commerce for the construction of a modernized and developed nation,
- To create opportunities for further development of all the sectors including human resources, economy, society and education with the e-commerce technologies,
- To authenticate electronic records and electronic data correspondences and to provide legal protection to matters related to domestic and international transactions based on the electronic data through computer networks,
- To enable simultaneous transmission, reception and storage of domestic and foreign data with the use of the e-commerce technologies and
- To enable effective and rapid communication and cooperation between international and regional organizations, governmental departments and organizations of Myanmar and foreign countries, private organizations and individuals through computer networks

3.4 Main ICT Systems and Facilities

The Survey Team conducted an interview survey on the existing and planned ICT systems, data centers and critical infrastructure, which Myanmar government considered important. The findings of the survey are described in the following.

3.4.1 ICT Systems

The ICT systems currently in operation include the electronic document management system, online visa issuance system and company registration system. Various government ministries and agencies are planning to introduce ICT systems and are steadily introducing new ICT systems. For example, MOE is developing an educational portal service and the Customs Department of the Ministry of Finance is introducing an electronic customs clearance system with the assistance from JICA.

However, Myanmar government has failed to recognize the difference in the level of importance of those existing and planned ICT systems. The reasons for this lack of recognition are as follows:

- No organization or individual has full understanding of the current state of ICT systems in government organizations including ministries and agencies and the ICT systems in Myanmar have not been systematically organized.

- The government fails to recognize the need to determine the level of importance of each ICT system because the development of ICT systems is still in progress and, thus, the number of the systems like those mentioned above, websites and mail systems operated by individual government ministries and agencies is not so large in Myanmar.

It is not difficult to deduce from the rapid development in the IT sector currently observed in Myanmar that a variety of ICT systems will be developed in series in government ministries and agencies and the use of extremely important ICT systems including those which are considered as mission critical systems will begin in the near future. Myanmar government shall have to first create an inventory of ICT resources in government ministries and agencies including ICT systems, hardware and software and understand and analyze their current state. Then, Myanmar government shall have to discuss what kind of information and systems shall have to be protected for the national security and designate critical ICT systems.

3.4.2 **Data Centers**

There are four data centers operated by government organizations in Myanmar. MPT operates data centers in Hanthawaddy in Yangon and Dekkhina in Naypyidaw and provides hosting services to the public and private sectors. Government organizations used to have their servers in the Hanthawaddy Data Center. However, many government ministries and agencies have relocated their servers to Dekkhina Data Center since the relocation of the capital to Naypyidaw mainly for the ease of maintenance and access.
MCIT operates two data centers in S-12 Building (one of the office buildings of MCIT) and Thayetkhon. An electronic document management system and the government personnel management system are in operation in the data center in S-12 Building. The data center in Thayetkhon is used by the armed forces. Detailed information of this data center has not been obtained.

Table 3.4-1 shows the outline of the government-run data centers. Meanwhile, Hitachi, Ltd. and MICTDC (Myanmar ICT Development Corporation Co., LTD.) are developing the first large-scale data center to be owned and operated by private companies in Myanmar for its opening at the end of 2016.

Table 3.4-1 Government-run data centers

Operator	Location	User	Description
MPT	Hanthawaddy (Yangon)	Government and private sector	This data center provides a hosting service. Mainly web servers of government organizations are installed in it. FWs are installed in the center as a security measure. Many government ministries and agencies have relocated their servers to Dekkhina Data Center since the relocation of the capital to Naypyidaw.
	Dekkhina (Naypyidaw)	Government and private sector	This data center provides a hosting service. Mainly mail servers and web servers of government organizations are installed in it. FW, mail filter, anti-virus software and IDS/IPS are installed in the center for cyber security.
MCIT	S-12 Building (Naypyidaw)	Government	Mail servers of government organizations are installed in the data center. An electronic document management system and the government personnel management system are located in this center. FW, WFA, mail filter and anti-virus software are installed in the center for cyber security.
	Thayetkhon (Naypyidaw)	Unknown	This is a military data center. Details of this center are unknown because access to it was denied.

3.4.3 Critical Infrastructure

Critical infrastructure is the basis of the lives and social activities of the people. The infrastructure in a total of 13 sectors, information and communication, financial, air transport, railway, electric power, gas, government and administrative service, health, water, physical distribution, science, credit and petroleum sectors, is designated as critical infrastructure in Japan. Different countries have different definitions of critical infrastructure and select it from different sectors. Regardless of these differences, it is extremely important to protect critical infrastructure because troubles on such infrastructure systems caused by cyberattacks will have great impact on the society. However, critical infrastructure has not been designated in Myanmar. Therefore, Myanmar government will have to first analyze the extent of the reliance on ICT systems of infrastructure in each sector and the area affected by IT failure in each sector and designate critical infrastructure.

Chapter 4 Survey of Current Situation of Cyber Security

4.1 Incidents and Statistics relating to Cyber Security

A survey on cyber security-related incidents and statistics in Myanmar was carried out.

4.1.1 Incidents relating to Cyber Security

As for cyber security-related incidents in Myanmar, the report of mmCERT, news media (mainly, WEB news media) and the interview records of ministries are used to collect the information. There was no systematic information about the cyber security incidents in Myanmar, because ICT infrastructure is under developing in Myanmar. There were large-scale attacks against government agencies and unauthorized access against the database of the national examination test results in June 2015. Those kind of incidents such as information leakage have been reported as well

Table 4.1-1 Incidents relating Cyber Security in Myanmar

Year	Target / Event	Description
2008	Government	18 ministries were attacked from Bangladesh.
2010	Presidential Election	・≒30,000 DDoS attacks ・Internet uncontestable during office hours over 10 days
2012-2013	Government, etc.	Attacks detected by mmCERT during 2012-2013: ✧ Targeted DDoS / DoS attack ✧ Targeted E-mail attack ✧ Web defacement ✧ SPAM E-mail ✧ Phishing ✧ Violation of privacy in SNS/Scanning
2015	National Exam.	The result of national examination was overwritten by unauthorized access.
2015	Diet members, etc.	Myanmar Hacker group, ”New Generation Wave”, stole diet member’s E-mail records by unauthorized access.

Source: ：mmCERT, ”About mmCERT (Our Issue, Challenges & Initiatives)”,

Myanmar Hacker Attacks News Feed (http://hackerattacks.einnews.com/country/myanmar), etc.

4.1.2 Statistics relating to Cyber Security

The information reported by mmCERT is only as something public about statistics information on the cyber security relation in Myanmar.

Majority of cyber security incidents reported by mmCERT is malware (67%). It has the majority (91%) in malware incident and exploiting known vulnerability (24%).

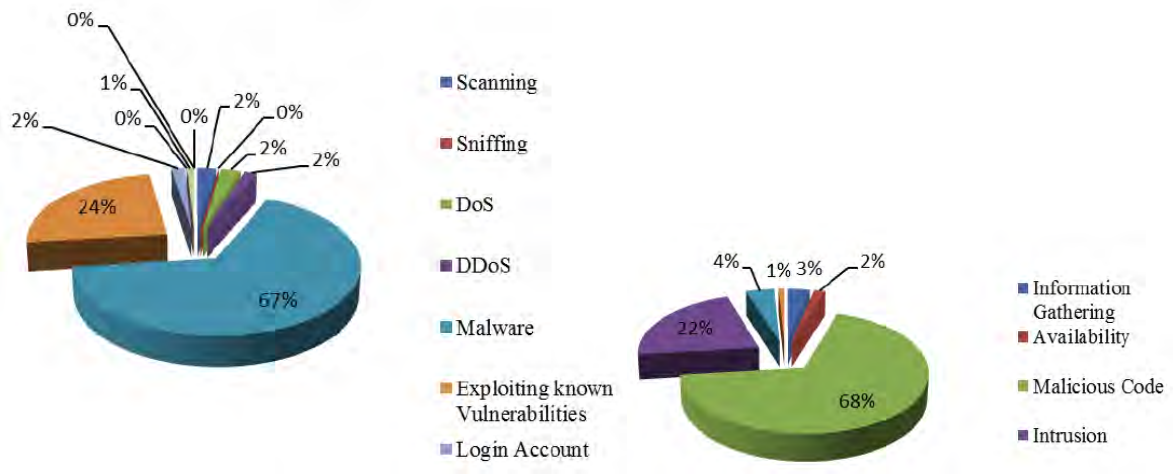


Figure 4.1-1 Cyber security incidents reported by mmCERT

Left: Type of incidents, Right: Category of incidents

Source: : APCERT Annual Report 2014（http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2014.pdf）

By using a sensor that is installed by TSUBAME project of JPCERT/CC, the source of cyber-attacks that mmCERT has reported, China accounted for 60%, and then attack from the United States was second place accounted for 15%. In case of Japan reported by JPCERT/CC, China ranked first, the United States has become a second place, so there was no difference between Myanmar and Japan in the big trend.

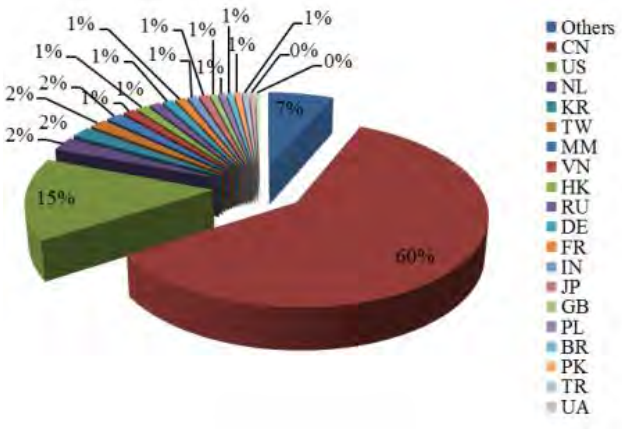


Figure 4.1-2 Source region of cyber-attacks reported by mmCERT

Source: : APCERT Annual Report 2014（http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2014.pdf）

4.2 Organizations relating to Cyber Security

4.2.1 Organizations relating to Cyber Security and their Interrelations

There are a number of organizations related to cyber security in Myanmar and they, independently or in collaboration, are making efforts to enhance cyber security measures. Figure 4.2-1 shows such organizations and their interrelations.

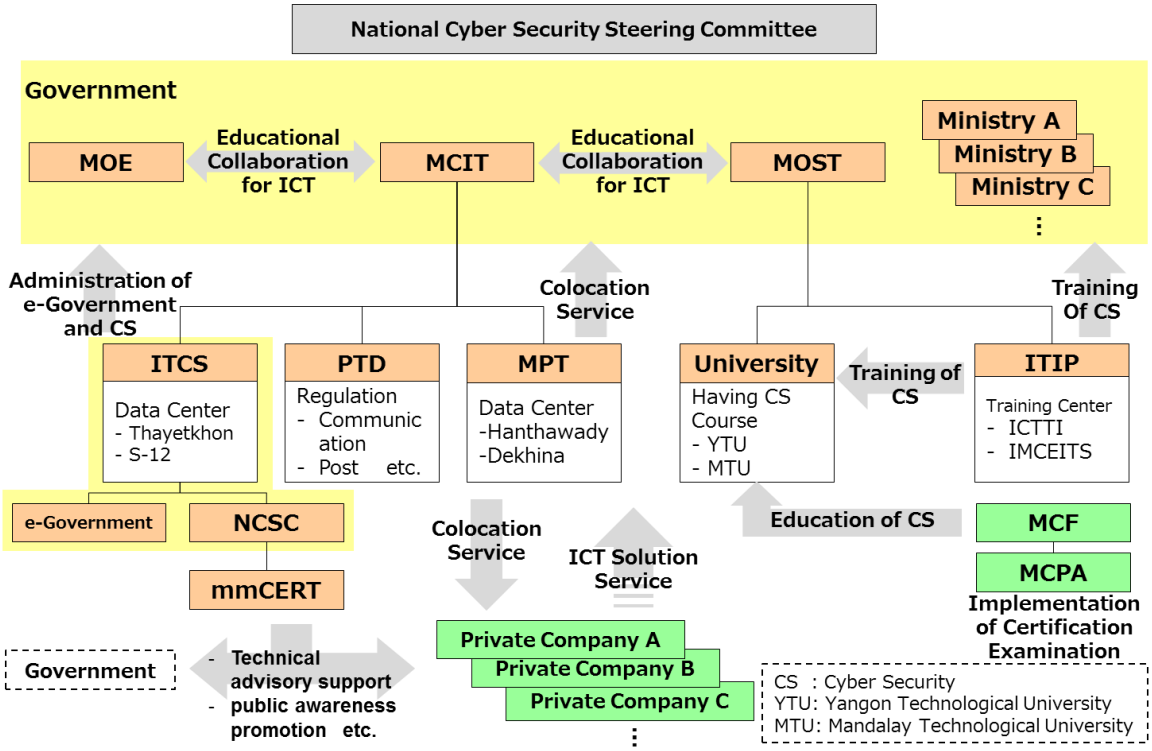


Figure 4.2-1 Organizational interrelation

The National Cyber Security Steering Committee (NCSSC), a cross-ministerial organization established in 2013 is a higher-level committee on cyber security. The committee makes decisions related to cyber security and cybercrimes and coordinates interests among concerned parties.

The Myanmar Posts and Telecommunications (MPT) is an entity under the supervision of MCIT which is in charge of telecommunications in the country. MPT provides hosting services to the government and private companies. Another entity similarly under the supervision of MCIT, IT&CS, has the National Cyber Security Center and the e-Government Department under it and each of these two organizations manages and operates cyber security measures at government organizations and manages the e-Government system. In addition, mmCERT which is under the supervision of the National Cyber Security Center offers education on cyber security and technical advice related to cyberattacks to government organizations and private companies.

The Ministry of Science and Technology (MOST) and the Ministry of Education (MOE) both in charge of education in Myanmar have universities and colleges and training centers under them and develop human resources through them. Colleges and universities regulated by MOE provide education in human studies, while colleges and universities regulated by MOST provide technological education. As the result, IT-related technical knowledge is to be studied at these colleges and universities regulated by MOST.

An entity under the supervision of MOST, the Institute for Technological Innovation Promotion (ITIP), provides students and government officials with cyber security education and training in order to raise the technological level of cyber security in Myanmar. Furthermore, in some cases, MOST and MOE provide education and training in collaboration with MCIT. Effective and efficient processes are

realized, as there has been mutual cooperation between MCIT and such ministries in charge of education as MOST and MOE.

The Myanmar Computer Federation which is a private association having a total of 30,000 private company members also provides students and government officials with cyber security education and training. By managing qualifying examinations and providing training to give certificates, the federation contributes to improve the status of human resources who are supposed to support future cyber security.

4.2.2 National Cyber Security Steering Committee

In Myanmar, the telecommunications market was opened up following the revision of the Telecommunications Law in 2013 and as the result the number of those who use the Internet, broadband communications networks and mobile phones increased. Meanwhile, the numbers of cybercrimes and cyberattacks have been on the rise, too, and the importance of cyber security measures has been increasing. Under such circumstances, in 2013, Myanmar established the National Cyber Security Steering Committee as an entity to make decisions related to cyber security measures and cybercrimes and coordinate interests among concerned parties. The committee is led by the Minister of MCIT who acts as its chair, and has a total of 16 members including government officials and individuals from the private sector. The committee is positioned as a higher-level committee for cyber security in Myanmar.

The committee's major activities include the committee meeting on cyber security to be held around once every two months and meetings of subcommittees. Whether the committee meeting has actually been held or not, however, could not be confirmed.

The National Cyber Security Steering Committee has working-level subcommittees composed of officials from concerned ministries, where discussions have been made on six topics including cyber security and cybercrimes.

The National Cyber Security Steering Committee is composed of members who are officials and employees of government ministries and private companies. As it is able to make cross-ministerial decisions, some say it is desirable that the committee should identify the key infrastructure, while others say the actual activities performed by the committee are not clearly visible. The influence of the committee is not known for certain.

4.2.3 Telecommunications Sector

MCIT to supervise telecommunications in Myanmar develops telecommunications policies, manages and regulates telecommunications services, issues licenses and standardizes telecommunications systems. Since 2015 when its structure was reorganized, MCIT has been composed of the following four entities and has a structure shown in Figure 4.2-2 below.

- Myanmar Posts and Telecommunications (MPT) which acts as a carrier of mobile, fixed-line

and international communications

- IT & Cyber Security Department (IT&CS) in charge of development of cyber security
- Post and Telecommunications Department (PTD) in charge of regulating postal, telecommunications and broadcasting services
- Myanmar Posts in charge of postal service

IT&CS has six different organizations under it. Additionally under the National Cyber Security Center, there is mmCERT as a lower-level organization. When any incident is reported, mmCERT is to analyze it and examine countermeasures. Currently mmCERT is the only entity for this process and it also has a function to make coordination among private companies.

- National Cyber Security Center responsible for cyber security of the government (having mmCERT under its supervision)
- Electronic Government Department responsible for the operation and management of electronic government in Myanmar
- Training Center Department in charge of the operation and management of training centers for officials of all ministries and agencies of the Myanmar Government
- Legal and International Cooperation Department responsible for legal affairs and international cooperation
- General and Financial Affairs Department responsible for the management and operation and financial matters of the entire organization
- Satellite Communication Department in charge of satellite communication

Among departments and other entities listed above, MPT, IT&CS and those under the supervision of IT&CS including the National Cyber Security Center, the Electronic Government Department and mmCERT are organizations that are highly relevant to cyber security.
Following the structural reorganization, the office of director general at MCIT has been vacant and Mr. Soe Thein, the Deputy Director General, has two offices concurrently.

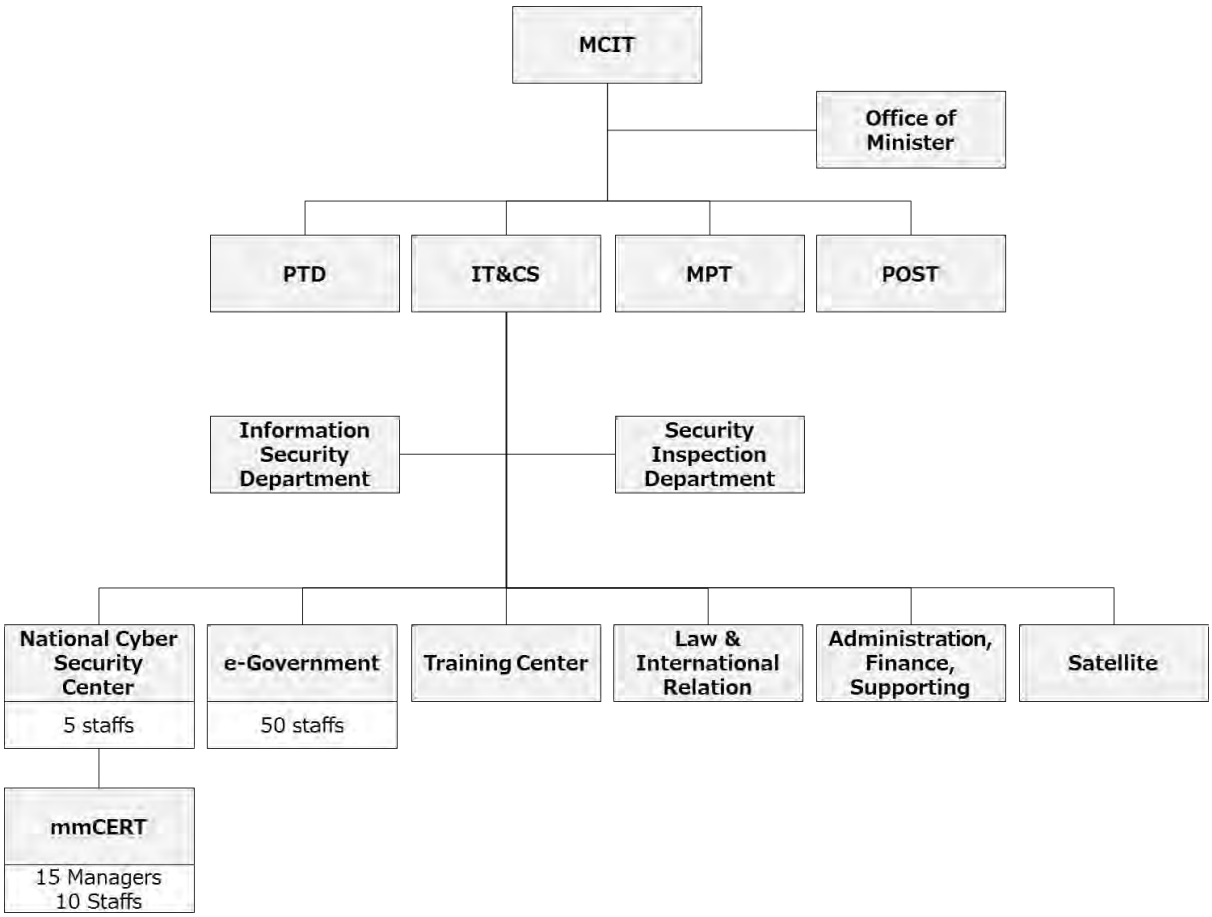


Figure 4.2-2 Organizational chart of MCIT

MPT has a data center each in Hanthawaddy, Yangon and in Dekkhina in Naypyidaw and these two data centers provide the hosting service to provide sites, the power source, networks, etc. to the government and private companies in a joint operation with KDDI SUMMIT GLOBAL SINGAPORE PTE. LTD. (KSGM; a joint venture established by KDDI Corp. and Sumitomo Corp.). The centers have fundamental security measures by installing a firewall, while users are required to have their own measures beyond that. Currently, however, users cannot afford to have appropriate security measures for the reason of a shortage of budgets, human resources and security policies.

At present, it is planned that MPT will be privatized in FY2016.

IT&CS has the National Cyber Security Center and the Electronic Government Department under it and manages and operates cyber security measures for each of government entities as well as manages and operates the electronic government. In addition, IT&CS has a data center in Thayetkhon in the suburb of Naypyidaw and S-12 building in Naypyidaw, respectively, and in the latter, IT&CS has been enhancing the operation of the electronic document management system and the government employee management system. Although there was originally an organization to manage and operate the Internet and an electronic government in the IT Bureau, a lower-level entity of MPT, when the attack on DDoS occurred at the time the election was held in 2010, the organization of IT Bureau was reviewed and enhanced, which led to the establishment of IT&CS under MPT. Later in April 2015, when the reorganization was implemented, MPT became independent from MCIT and IT&CS

remained to be under the supervision of MCIT not moving along with MPT.
The IT Bureau under the supervision of the present MPT is an entity to implement activities mainly related to Enterprise Resource Planning (ERP) of MPT.
At the time IT&CS became independent, several tens of employees of MPT moved to IT&CS and it now operates with a total of 60 officials. Of these, about 50 officials belong to the Electronic Government Department, with 5 remaining officials belonging to the National Cyber Security Center. Presently, with an unbalanced distribution of personnel, the Electronic Government Department has a larger number of employees, while the National Cyber Security Center is lacking staff and being unable to perform its task sufficiently. For the future, therefore, it is planned to rearrange the distribution of personnel within IT&CS as well as to increase the number of personnel to around 300 by transferring some of MPT personnel to IT&CS.
In the meantime, mmCERT located in Yangon is an entity to receive and analyze incident reports and examine countermeasures and provide technical advice to prevent recurrence. While mmCERT monitors the operation of the data center in Yangon but not of the data center located in Naypyidaw, which means its major role is essentially the provision of advice to private companies. mmCERT was once under the supervision of MOST but, following the reorganization process, it is now supervised by the National Cyber Security Center. Currently, mmCERT has 15 managers and 10 general employees. MCIT is the provider of operating funds of mmCERT. However, in reality, mmCERT is unable to fully perform its task due to a shortage of human resources and funds.

4.2.4 **Organizations Developing Human Resources in the Telecommunications Field**

MOST and MOE that are ministries in charge of education in the Myanmar government develop human resources in the telecommunications field through colleges and universities and training centers they regulate.
MOST has five departments under it, including Department of Technical and Vocational Education, Technological Research Department, Department of Atomic Energy, Department of Technology Promotion and Coordination and Biotechnology Research Department. MOST also has colleges and universities and laboratories specialized in technology-related studies such as computer science, engineering and science. The colleges and universities regulated by MOST include, among others, University of Computer Studies, Yangon, University of Computer Studies, Mandalay, Yangon Technological University, Mandalay Technological University and Pyay Technological University. Pyay Technological University is under the supervision of the Department of Technical and Vocational Education, while other universities regulated by MOST are supervised by the Department of Technology Promotion and Coordination. Although currently there is no university or college that has courses specialized in cyber security in Myanmar, students can study telecommunications through two courses, computer science and computer technology, at undergraduate and master courses of the University of Computer Studies, Yangon and the University of Computer Studies, Mandalay. In addition to this, students can study data security at the doctoral course for computer technology. In Myanmar, however, computer science-related studies are not popular among students, because they

cannot find good job opportunities matching their specialty as well as the compensation they can get as a specialist in this field is lower than that of other kinds of jobs in the country. Another problem is a large gap between special knowledge that can be acquired at university or college and such knowledge companies want their employees to have.

The Institute of Technological Innovation Promotion supervised by MOST has two training centers, which are Information and Communication Technology Training Institute and India-Myanmar Centre for Enhancement of IT Skills, and these centers are operated with assistance of JICA and India, respectively. These two training centers offer training courses that continue for from several weeks to several months with an aim at developing human resources specialized in networks and software. Trainees are required to be graduates of college or university if they want to participate in these training courses and a six-month course costs about 200,000 kyats. Trainees, however, can get a scholarship offered by private companies such as NTT Data Corp. The training courses are available not only for college and university graduates but also for government employees and the latter can attend the training course free of charge. Currently, the Institute of Technological Innovation Promotion is constructing a new research and development building that, when completed, can function as a training center and at the same time a new base for research and development (R&D). There is also a plan to set up a department that focuses on cyber security as a specialized R&D subject. It is planned that, starting April 2016, colleges and universities now regulated by MOST will be operated under the supervision of MOE.

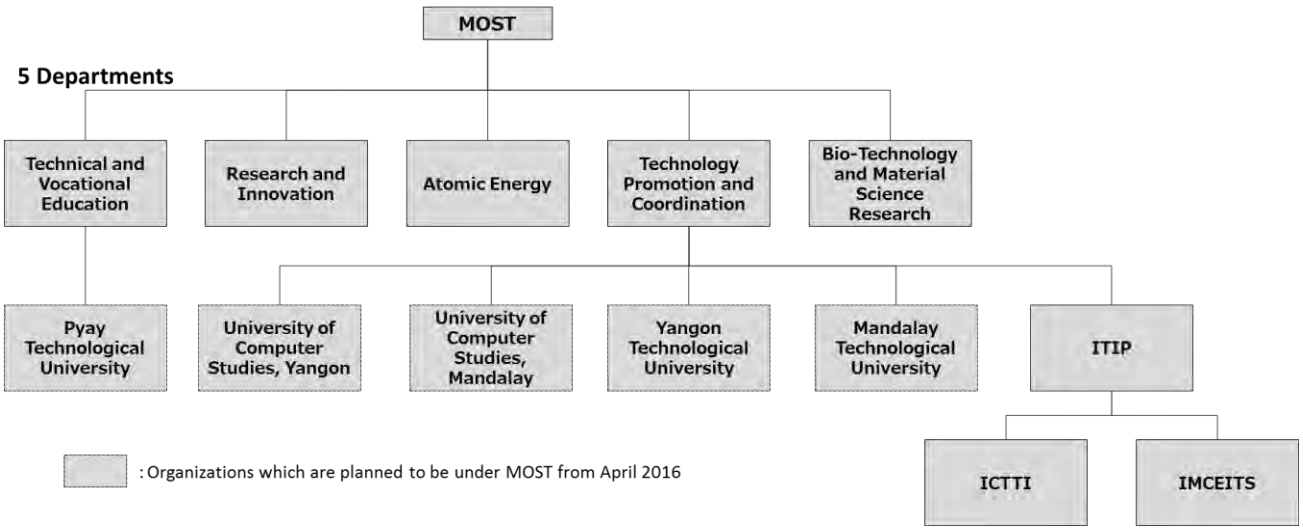


Figure 4.2-3 Organizational chart of the Ministry of Science and Technology

MOE has seven departments including Department of Higher Education, Department of Teacher Training, Department of Human Resources and Educational Planning, Department of Basic Education, Myanmar Language Commission, Department of Myanmar Examinations and Department of Myanmar Education Research Bureau. Under it, MOE has colleges and universities specialized in human studies, where, although there is no course specialized in cyber security, e-Government systems courses are in place as one of study subjects in the telecommunications field.

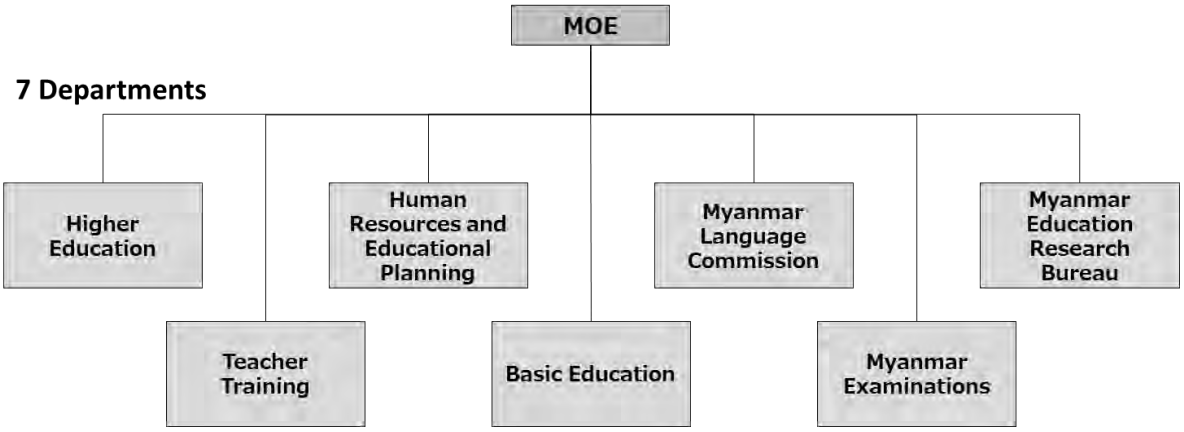


Figure 4.2-4 Organizational chart of the Ministry of Education

4.2.5 **Private Companies**

The Myanmar Computer Federation which has the membership of 30,000 private companies and its affiliated organization, the Myanmar Computer Professional Association mainly based in Yangon, are private organizations that work to improve the level of IT capability in Myanmar. The functions and competence of the Myanmar Computer Federation are defined in the Computer Science Development Law, Article 24, as follows:

A) Development of necessary committees and organizations along with their functions and the national computer science base that can keep pace with the times
B) Implementation of research into computer science and provision of advice to those who implement computer science research
C) Promotion of expansion of the use of computer science in various business areas
D) Speculation of the content of courses and subjects to be studied at the computer training schools
E) Examination to make judgment on whether the level of instruction at computer training schools meet the predetermined standard or not
F) Provision of courses and lectures on computer science and implementation of contests and study tours
G) Implementation of computer science examinations and presentation of certificates and medals
H) Provision of advice to the Myanmar Computer Science Development Council in a timely manner in order to promote development of computer science
I) Support to manufacturers in order to improve the quality of computer hardware and software
J) Support to production and domestic and overseas sale of computer hardware and software
K) Development of plans related to information technology based on the direction of the Myanmar Computer Science Development Council
L) Contact with international computer-related organizations
M) Coordination related to hosting of relevant domestic and international councils, conferences, task forces, lecture meetings and study publication meetings and dispatching delegations to

such events

N) Realization of system designs that allow the use of Myanmarese on computers
O) Advice to government ministries and agencies and other organizations that require computer-related advice
P) Editing, publishing and distribution of computer-related books, papers, journals and magazines
Q) Establishment of libraries that collect domestic and overseas books on computers
R) Contribution to the acquisition of basic computer knowledge by younger generations, particularly students and to the development of excellent computer scientists
S) Offering of prize money to excellent computer scientists and inventors
T) Recommendation of candidates of excellent computer scientists and inventors to be awarded with an honorary title to the council
U) Advice to the council to protect interests of computer scientists and inventors
V) Determination of organizational structure of necessary committees and other organizations and their functions and tasks
W) Execution of computer science-related tasks commissioned by the council

The Myanmar Computer Federation operates in accordance with the rules listed above. It is particularly committed to the development of human resources and it hosts annual cyber security seminars in various regions, gives instructions to teachers and students with an aim at improving the level of IT education and provides training that continues for several months in response to the government request. It has diverse training courses with different content from basic knowledge to more advanced techniques, and in some training courses, certificates are given to those who completed the course. In addition, qualifying examinations that are mutually certified with a Japanese entity, the Information-Technology Promotion Agency (IPA), are given.

4.3 Cyber Security Strategies, Policies, Legal Systems and Guidelines

As MCIT is responsible for all kind of policies related to ICT including security in Myanmar government, strategy, policy and roadmap of cyber security shall be considered by MCIT. Therefore, MCIT have carried out organization reformation as motioned above and IT&CS is in charge of drafting these issues.

Nevertheless, a strategy, policy, legal system or guideline that shall become the cornerstone of government's cyber security is still undeveloped in current situation.

For basic framework for government cyber security, the strategy, policy, legal system or guideline as following table shall be expected.

Table 4.3-1 Expected cyber security strategy, policy, legal system or guideline in Myanmar

Category	Implementation	Situation
Basic policy, strategy related to cyber security	No	IT&CS is in charge of drafting. IT&CS is stating it is under construction, but completion schedule is unknown.
Legal system for cyber criminal	Partial	No specific act is established for cybercriminal, but basic penal regulations are defined in "The Electronic Transactions Law" and "The Computer Science Development Law".
Legal system for privacy and data protection	No	Basic penal regulations for such as confidential information or defamation are defined in "The Electronic Transactions Law", but no exact law is established.
Legal system for electronic contents	Yes	"The Electronic Transactions Law" defines some handling rules of information such as a limitation on creation, edition and distribution of information that damage other's libel or property. On the other hand, "The Computer Science Development Law" defines penal regulations on trade of pirated contents/information.
Legal system for electronic commerce	Yes	Basic rules for electronic commerce are defined in "The Electronic Transactions Law".
Legal system for protection of consumers and young ages	Partial	Basic rules for protection of young ages are descripted on article 292 and 293 of "The Penal Code". For consumer protection, Ministry of Commerce established "Consumer Protection Law" in 2014. Meanwhile, both acts are not considering a peculiarity on cyber space.

Among ICT related basic legal systems in Myanmar, the acts that especially including regulations on cyber security are "The Computer Science Development Law", "The Electronic Transactions Law" and "The Telecommunications Law (of 2013)".

"The Telecommunications Law" which established in 2013 is the act that defined business rules for private telecom operators who are approved by government aim to progress liberalization of communication market in Myanmar, so the act regulates condition for license, duty for operators and penal regulation majorly. From the viewpoint of cyber security, there are some descriptions for protection of individual users, though most of them are about basic items such as an obligation of present a tariff.

“The Computer Science Development Law” which established in 1994 regulates Myanmar Computer Science Development Council as an observation organization and Myanmar Computer Federation as a promotion organization. The act also defines limitation and penal regulation for utilization of computer technology such as an authority to regulate tradable computer products or authority to approve network connection.

“The Electronic Transactions Law” which established in 2004 regulates that the contracts, records, signature and communication transaction on electronic environment shall be available as same as real one regardless of the media. In addition, it defines Electronic Transactions Control Board as management organization, also descript about the administrative disposition for a violator and penal regulation for basic cases such as detrimental action for nation, electronic destruction/obstruction, interruption of information or libel.

As national level development plan related to ICT, “Myanmar Telecommunications Master Plan” is drafted with a cooperation of World Bank and it is under review as of Aug. 2015, and also “Myanmar e-Governance ICT Master Plan 2015” which more focused to the promotion of e-Government is drafted with a cooperation of ADB and already handed to Myanmar government (not yet issued by Myanmar government as of Aug. 2015). The previous period ICT Master Plan (2010-2015) was established with a cooperation of KOICA.

As challenges for security and privacy in “Myanmar Telecommunications Master Plan”, the necessity of counter measures for; a) Creation of network redundancy plan, b) Creation of national cyber security policy, c) Standard definition for legal interrupt of telecom network, d) Containment of “grey traffic” are indicated.

On the other hand, “Myanmar e-Governance ICT Master Plan 2015” indicates that development of legal systems and IT policy as necessary activities for cyber security to promote e-Government. As a development of legal systems (in “4.2 Recommendations on amendments to ICT Law”); a) Creation of new institutions to implement the e-Governance initiatives that can coordinate government departments and have direct authority on budget, b) Usage of cryptography based electronic signatures, c) Legal systems on protection of Intellectual Property Rights, critical infrastructure protection, cybercrime, social media usage, e-commerce including electronic payments, privacy and data protection and dispute resolution modes in a virtual world are indicated as necessary point. In contrast, as a development of ICT Policy (“4.7 Recommendations on IT Policies”); a) technology related policies (such as policy for inter-operability and adoption of open standards, use of government integration framework, information security policy, shared IT infrastructure, digital security and PKI) b) Electronic service delivery related policies (such as multi-channel access, electronic payments), c) Capacity building policies (such as digital literacy and skill up-gradation, multi-lateral, international and academic collaborative skill), d) E-Governance management policies (such as e-Procurement, budgetary allocations, PPP, quality assurance) are also indicated.

4.3.1 Basic Policy, Strategy relating to Cyber Security

Drafting process of Cyber Security strategy in Myanmar is under progress with cooperation of expert

dispatched by JICA. Draft action plan was created as of 2015 and it is still under consultation in MCIT.

Although Drafting of ICT Security Policy in Myanmar government shall be done by IT&CS which newly established in MCIT, not only current state of progress or drafting schedule but also the scope and other detail of ICT Security Policy haven't unveiled yet. The expected reason for no information on current status and content is less-progress of consideration due to a lack of human resources in security group of IT&CS the section which just established and still in startup phase. In addition, IT&CS also doesn't have original budget because currently operated by former budget allocation that have allocated before organization reforming.

However IT&CS make a drafting schedule clear by organization enforcement that they are currently planning, experts with certain knowledge and experience are still necessary for development of ICT Security policy. Therefore, the acquisition of such human resource is important factor.

In current situation, the scope of ICT security policy as the policy is targeted for all Myanmar government or only MCIT is still unknown. Even if the policy is targeted only MCIT, as well as it is required by all Myanmar government and no other available ICT security policy have been established, other ministries or agencies shall refer MCIT's ICT security policy.

According to such situation, ICT Security Policy that currently under construction in MCIT shall be a critical step for upgrade of cyber security in Myanmar government.

4.3.2 **Legal System for Cyber Criminal**

Related regulations (controls) in "The Electronic Transactions Law" and "The Computer Science Development Law" are as follows;

- Detrimental action to national solidarity, economy or culture such as national confidence or legal order
- Action that causing loss and damage by sending, hacking, modifying, altering, destroying, stealing of information
- Interception, abuse or impersonation such as using security number, password or electronic signature
- Creation, modification, distribution of information to be detrimental to the interest of or to lower the dignity of any organization or any person
- Violations to the prohibitions contained in the order issued by the Control Board

These conditions are basic concepts and detailed specific standards shall be handled by Control Board. As private telecom operator mentioned that they aren't clear for counter measure (such as where/how to complain) if they detect address of illegal users, the role-sharing and standard shall be concreted to validate the control.

4.3.3 Legal System for Privacy and Data Protection

Specific Privacy protection law is not yet established in Myanmar. According to not only promote service with utilization of safe network but also promote awareness raising of individual security as descripted in action plan of Cyber Security strategy. Therefore, the Privacy protection law is expected to be established.

On the other hand, for data protection, "The official secret law" exists for protection of confidential information. But in fact, regular account of Gmail is still used in government organization. Therefore, adjusted legal systems which to consider about the case that confidential or critical information used on network or new cloud technology, shall be necessary.

4.3.4 Legal System for Electronic Contents

In "The Electronic Transactions Law", there are penal regulation that limits creation, edition and distribution of contents that damage other's libel or property. In "The Computer Science Development Law", there are penal regulations on trade of pirated contents/information. On the other hand, for a substance of contents, there is also a relation with "The official secret law" and future privacy and data protection related law which isn't exist now.

Since the quality and substance of electronic contents shall be defined in guideline, major necessary conditions and penalties are already covered by existing legal system.

4.3.5 Legal System for Electronic Commerce

As mentioned above, "The Electronic Transactions Law" is established in 2004. Above-mentioned major conditions are descripted in 2004; e-commerce was improving not in Myanmar but in foreign countries at that time so it was quite early law establishment for Myanmar.

As well as electronic transaction law is already established in all ASEAN Member States including Cambodia which will be established very soon, e-commerce environment that based on electronic transaction law will be critical even from connectivity of ASEAN.

4.3.6 Legal System for Protection of Consumers and Young Ages

As basic rules for protection of young ages that descripted in "The Penal Code", addition to regular conditions such as limitation trade, distribution and import/export of obscene products, special description (additional penalties) shall be added on if target is less than 20 years old.

For "Consumer Protection Law", Ministry of Commerce drafted in 2012 and established in 2014. The law is aiming not only at protection of consumer but also at platform construction of business environment in neighbor ASEAN area (similar consumer protection law is installed in 5 ASEAN countries).

Meanwhile, since those laws are not considering cases that happened in cyber space, coverage of laws including "Electronic Transaction Law" shall be assessed.

4.4 Development of Human Resources in the Science & Technology, IT and Cyber Security Fields

Human resources specialized in cyber security are not developed in Myanmar and, therefore, organizations or individuals interested in cyber security have been working separately on human resources development and on acquisition of knowledge in the cyber security field, as the country develops human resources for science & technology (S&T) and IT in general including computer science. Considering such a circumstance, discussions are made in the following section concerning how human resources are currently developed both in the fields of S&T and IT in general and in the specialized field of cyber security.

Discussions are also made on how the government ministries and agencies and private companies are working on the development of such human resources.

4.4.1 Development of Human Resources in the Basic (theoretical) Science & Technology and IT Fields

For domestic human resources development in the S&T field in Myanmar including IT and cyber security, the Ministry of Science and Technology (MOST) is in charge, from development of policies and strategies to even general education for a broader base of population. The roles of MOST include the development of specialist workers, engineers, scientists & technologists and other technicians in the most advanced S&T fields, so that the national economy can grow and the government can exercise its tasks responsibly to reach solutions for R&D issues. Specifically, the following six matters are the responsibility of MOST.

- To implement R&D plans for the growth of national economy
- To improve the level of people's lives, by enhancing the economy through the use of national resources
- To strengthen the productivity of agricultural and industrial sectors, by transferring technology and sharing knowledge that can be acquired through advancement of R&D
- To make and implement human resources development plans to nurture specialists in the S&T field
- To implement experiments and analysis, quality management and standardization of industrial raw materials and end products
- To implement research on the use of nuclear energy with safety measures in place

In Myanmar, in 1996, the government enforced the Computer Science Development Law, 1996, for the purposes of defining matters to be considered in the development and diffusion of computer science and of managing import and export of computer software and related information. Following the enforcement of the law, in September 2000 and later, MOST established a total of 24 computer colleges one after another, including University of Computer Studies, Yangon (UCSY) and University of Computer Studies, Mandalay (UCSM). In addition to these, MOST regulates other colleges and

universities like Yangon Technological University (YTU), Mandalay Technological University (MTU) and Pyay Technological University (PTU), while the above-mentioned 24 colleges such as UCSY and UCSM are those specialized in IT and computer science.

UCSY is a college leading the IT and computer science fields in Myanmar. Accordingly therefore, middle and higher-ranked government officials and senior engineers of private companies working on IT are often graduates of UCSY. UCSY has undergraduate, master and doctoral courses, with two subjects of computer science and computer technology in place in each of undergraduate and master's courses. There is no curriculum specialized in cyber security and its doctoral course only has data security (data security measures) study in its computer technology course. According to MOST, UCSY will have a practical course specialized in cyber security in the future. In Myanmar, colleges and universities are all nationally established and there are 36 universities and 112 colleges in total in the country. Colleges and universities specialized in technology are regulated by MOST, those specialized in human studies are regulated by MOE, those specialized in agriculture are regulated by the Ministry of Agriculture and those specialized in medicine are regulated by the Ministry of Health. In the future, however, all colleges and universities are planned to be regulated centrally by MOE.

In collaboration with Keio University of Japan, from 2014 to 2016, UCSY plans to mutually dispatch and receive two students with each other. This collaboration is a part of the "Re-inventing Japan Project" which was inaugurated in 2011 by Japan's Ministry of Education, Culture, Sports, Science and Technology (commissioned to the Japan Society for the Promotion of Science). At colleges and universities of Myanmar having only limited curriculum and a limited number of teaching staff, it is considered to be effective to collaborate with overseas universities. At UCSY, English is used when teaching and students are adaptive to studies taught in English. Therefore, it is expected that international cooperation between colleges and universities in Myanmar and overseas countries can have a great effect on acquisition of appropriate basic knowledge necessary for computer science and cyber security.

On the other hand, according to MOE, although they have an intention to expand ICT-related curriculum to improve the base ICT skill of Myanmar in general, they are currently unable to offer ICT courses across the nation since there are quite a few rural regions that are not yet electrified.

In Myanmar, there are not many opportunities to have a job in the computer science field, too, and hence, the field, as a major study subject, is not popular among students. Of all science courses, medicine and engineering-related courses are more popular. In the future, it is required to have appropriate measures to motivate students to major in IT-related courses, for example, by providing some incentives.

4.4.2 Need for Developing Human Resources in the More Practical S&T and IT Fields

In the e-ASEAN framework agreed in November 2000, the Myanmar government committed itself to other ASEAN countries to the promotion of information infrastructure construction and electronic commerce, the liberalization of ICT devices and services, an improvement in ICT literacy and creation of an electronic society and the establishment of e-Government. Following this commitment, the

government set up the e-National Task Force (e-NTF) and in 2004 to 2005, developed the ICT Master Plan (2010 to 2015) obtaining assistance from South Korea. Within e-NTF, a total of seven committees were set up for the areas of ICT application, ICT education, ICT infrastructure, ICT legal system, ICT liberalization, ICT statistics and ICT standardization in order to promote detailed measures to realize the e-Government. The ICT Master Plan developed obtaining assistance of the Korean International Cooperation Agency (KOICA) was a plan targeted at a time period up to 2015 and therefore, Myanmar is now working on the development of detailed measures for promoting ICT and realizing e-Government with assistance of the World Bank and the Asian Development Bank (ADB) which started to be given in 2014.

To this end, it is urgently necessary to develop human resources not only with an aim at constructing theories and allowing to acquire basic knowledge, which is underway at colleges and universities regulated by MOST, but also developing human resources focusing on the more practical fields of IT and cyber security.

4.4.3 Efforts for Human Resources Development and the Level of Technological Capability of Myanmar Government Ministries and Agencies

Human resources development at ministries and agencies of the Myanmar government are principally carried out not based on comprehensive guidelines and each ministry or agency independently makes efforts depending on available budgets and manpower. Under such circumstances, MOST and the Ministry of Communication and Information Technology (MCIT) jointly provide a 10-week IT training course to government officials who are in charge of IT. The training course is provided at the English Language Professional School (ELPS) owned by MOST in Naypyidaw and officials from 12 to 13 ministries and agencies have been attending the training. The training is provided with a budget of MOST and it is composed of two courses listed below. It, however, does not offer training on cyber security and only how to handle firewalls are taught as part of Course B.

(A) Web development: How to create websites and how to manage databases
(B) Network technology: Basic network structure, web servers, mail servers, file servers

Meanwhile, mmCERT provides its own employees with practical training for the following eight areas.

- System management
- Network management
- Malware analysis
- Web development
- Web application penetration test
- Vulnerabilities diagnosis
- Programming
- Incident response

mmCERT has 15 managers and 10 general employees and, of those managers and employees, only seven experts have knowledge on programs and networks. Although practical training has been provided at mmCERT, it has only limited effect as there are just a small number of employees to be trained. It is an urgent matter for mmCERT to enhance its personnel base in addition to promoting human resource development.

The Ministry of Construction and the Ministry of Commerce also actively develop human resources in the IT field independently."

In order to manage and operate databases to be managed by the Ministry of Construction (refer to Activities of the Government Organizations in Charge of Security Measures in the section below), in April 2015, a planning and telecommunications office was established within a total of four departments of the ministry. These offices' main task is the development of plans and there are not so many IT-related tasks and, of a total of 110 employees of the five departments including the Office of Minister of Construction, IT specialists are only four or five for each department. About 500 employees are able to operate computers at the ministry and training has been provided to these employees at two venues. Training centers owned by private companies are also utilized for this purpose.

Training on computer design and architecture design is also provided to those selected from among 4,000 engineers in around Myanmar. However, as they do not have enough knowledge to provide IT training, the Ministry of Construction does not consider that training has been provided sufficiently.

On the other hand, the Ministry of Commerce has around 13 employees in its ICT section, who are in charge mainly of publication of journals. Although it is required by an official notice of MCIT that the ministry should appoint a Chief Information Officer (CIO) and a Chief Security Officer (CSO), respectively, a CSO has not been appointed for the reason of a shortage of engineers with enough technical skills and the CIO is now responsible for tasks of both CIO and CSO.

In 2005, the Ministry of Commerce set up a training room within the ministry building, where the ministry provides small-scale training on software using 20 computers. For this training, lecturers are invited from outside software companies and in the past lecturers had been invited even from Malaysia. The training session is held around 10 times annually and there are several different courses depending on the level of trainees. In addition, the ministry let its officials attend a training course offered in collaboration between MCIT and MOST mentioned above.

Even though officials in charge of IT at the ministry can have opportunities to receive training on IT and cyber security, some of such officials in charge of IT are concerned about their inability to accumulate knowledge and experience obtained through training, since they are supposed to be relocated to other sections within the Myanmar government. Furthermore, they point out they have difficulty to retain knowledge and techniques because they cannot have follow-up after completing the seminar or training. Meanwhile, the Deputy Minister of MCIT considers human resource development and capacity building as important for government employees to acquire sustainable cyber security skills. He points out that capacity building should be promoted not separately for each individual but for the organization as a whole in a comprehensive manner.

4.4.4 Efforts of Human Resources Development in the Private Sector

The Myanmar Computer Federation (MCF) has a membership of 30,000 private companies and is an organization to promote the level of IT capability in cooperation with its member companies. MCF holds a seminar on security in various areas of Myanmar annually. In addition, as part of education on IT, MCF offers training to high school teachers in charge of information-related subjects and even gives lessons directly to high school students when the school so requests. In response to the Myanmar government's request, in 2014, MCF offered a three-month seminar along with a more advanced training course.

Meanwhile, considering that it would help the country to secure experts with a certain level of knowledge if an IT qualification system is established to provide an incentive to IT experts, the Myanmar Computer Professional Association (MCPA) set up Myanmar's own qualification examination program. In 2002, the examination program was developed and since March 2002, the examination has been given annually. In addition to this program, people in Myanmar can take an examination under a program of the National Consumer Council (NCC) of the UK and under a mutual qualification examination jointly offered with the Japan Telecommunications Engineering and Consulting Service, which started in January 2003. There are also ICT vendor qualification examination programs offered by Microsoft, Oracle, Cisco and IBM, respectively.

In addition, there are private computer schools, which total over 100 only in Yangon City. Computer schools operated by the leading Myanmar companies, KMD and MCC group, are highly popular and these schools have their branch schools around the country. Among scientific subjects, however, computer science is less popular and it is desirable that a mechanism will be developed for human resources development, while taking measures to improve the status of IT experts.

4.5 Activities of Government Organizations in Charge of Security Measures

4.5.1 Activities of the Ministry of Communications and Information Technology

The Ministry of Communications and Information Technology (MCIT) is an organization to develop security policies for the country as a whole and is currently drafting the First Cyber Security Action Plan (draft Action Plan) with assistance of JICA's experts and implementing the reorganization of the ministry.

As of August 2015, the draft Action Plan has not been approved within MCIT and the process to translate the draft into Myanmarese to be used when explaining the plan to the Minister is underway. By the end of September, explanation to the Minister is planned to be finished.

Meanwhile, as described in Section 4.2, "Organizations Related to Cyber Security," the above-mentioned reorganization was carried out so that the former structure composed of one office and two bureaus including the Office of Minister, MPT and the Posts and Telecommunications Department (PTD) would be changed and the IT-related business except for postal and telecommunication services would fall under the supervision of IT&CS, as former responsivities of MPT were split up among IT&CS, MPT and the Myanmar Posts. In addition, PTD continues to play

the role of a regulatory organization for postal and information and communication services, and the former 2 bureau system was reorganized into a 4 bureau system.

At IT&CS, there are 6 departments, including General and Financial Affairs Department, Training Center Department, Electronic Government Department, Legal and International Cooperation Department, Satellite Communication Department and National Cyber Security Center (NCSC). NCSC is expected to comprehensively be in charge of cyber Security. It is intended to aggregate all functions related to cyber security and centrally manage human resources development and responses to incidents. Although MPT originally had an IT bureau, which in turn had an organization to manage and operate the e-Government and the Internet, following the DDoS attack which occurred in 2010, the IT bureau's organization was reviewed and enhanced, while the separation and privatization of MPT as a communication carrier led to the establishment of IT&CS to supervise cyber security of the country. For the time being, the most important activities for NCSC are to develop the draft Action Plan as well as annual business plans and budgets.

As IT&CS has just been established, cyber security measures for the Myanmar government organizations are currently the responsibility of each ministry or agency, including installation of devices, introduction of applications, detection of attacks, procedures and guidelines for sharing information, human resources development and budgeting. However, current measures are limited to the installation of firewalls for databases accessible through online services and anti-virus software for individual devices, and these measures are taken independently by each ministry or agency. Also, no rules and guidelines have been clearly established concerning how to respond to suspicious e-mails or how to use free e-mail addresses.

In the following sections, from 4.5-2 to 4.5.11, discussions are made on how other ministries are implementing responses, which we learned from the hearing survey.

4.5.2 Myanmar Posts and Telecommunications (MPT)

Cyber attacks on MPT recognized so far is the DDoS attack which occurred when the election was held in 2010, as mentioned above. It was also reported that private companies using the hosting service of MPT were attacked. Following these attacks, however, no particular security measures have been taken.

There are two data centers managed and operated by MPT, following the reorganization, including those in Hanthawaddy in Yangon and in Dekkhina in Naypyidaw. These two data centers play the role of a gateway for international telecommunications and they created a redundant configuration.

In addition, these two data centers offer the hosting service via web server to be used by each ministry or agency for their online service and a mail server. The hosting service provided by MPT is the provision of venues to install devices and other facilities such as power sources. Therefore, MPT does not have security measures other than firewalls. The document management system commonly used by the government ministries and agencies and important data are controlled at other data centers situated in Naypyidaw (S12 Building and Tatkonn). A device provided through Japan's grant aid (The Project for Urgent Improvement of Communication Networks, 2012) is installed in Dekkhina and no

attack on the device has been reported so far.

4.5.3 mmCERT

In order to fulfill the following four roles, mmCERT works to promote responses to incidents, sharing of the latest information on cyber threats and cyber security, support concerning technical consultation and to improve Myanmarese people's awareness. Situated in Yangon, mmCERT supervises data centers owned and operated by MPT, while the government's data not stored in the data centers in Yangon are not in the scope of supervision of mmCERT.

- Development of national IT vision through international cooperation with CERTs of other countries on cyber security and cybercrimes
- Sending out security-related information and recommendations
- Provision of technical assistance
- Cooperation of law enforcement agencies in charge of cybercrimes

For the above purposes, mmCERT provides cyber security courses to students of UCSY and private companies. In addition, as an activity to improve Myanmarese people's awareness, mmCERT also provides training courses, delivers leaflets and develops guidelines on password setting.

4.5.4 Ministry of Science and Technology

The Ministry of Science and Technology (MOST), on its website, shares only basic information and does not provide any online service through the website. Accordingly therefore, the website of MOST has never experienced a cyber attack.

At MOST, each employee at the level of section manager or higher has a computer on loan to connect to the ministry's network, while other devices including smartphones can also connect to the network. In total, about 500 devices are connected to the MOST networks. The web server is situated in the server room of MOST and is protected from web-based or zero day attacks by a security product called FireEye.

The network is managed by employees of IT department at MOST, who confirm and analyze alerts on a daily basis and work to solve problems if any. In addition, if any serious and major alert is confirmed, a private company having the license of the FireEye service is to provide support to the IT department.

Although a personnel database system to incorporate human affairs information of MOST is under construction (in which common terminology is to be used and which will only be accessible by MOST employees) following the advancement of the e-Government project, no cyber security budgets have been requested as of now. MOST, however, considers budgets can be allocated for the trainings to be implemented by colleges and universities it regulates.

4.5.5 Ministry of Education

At the Ministry of Education (MOE), the first cyberattacks were identified about 10 years ago. The

website of the ministry had cyber attacks and its server went down for several days. More recently in June 2015, the database of university entrance examination results suffered an unlawful access and it was found that data were falsified in this incident. Meanwhile, because of these kinds of incidents including another in which the MOE mail server was hacked, MOE is aware of cyber attack risks it has. Following the cyber attack incidents which occurred about 10 years ago, guidelines on how to respond to cyber attacks were developed, while no procedures or rules were established to control possible intensification of such attacks and reporting to and information sharing with other ministries have not been done as well. Furthermore, even if MOE develops action plans and such plans are implemented, no verification is made later, which leads to an inability to confirm whether planned measures are effective or not. Therefore, according to MOE, important data are at present stored in an independent computer that is isolated from the Internet.

In response to the government notice based on request from MCIT and to take cyber security measures, MOE created the offices of CIO and CSO and appointed two CSOs. In addition, the ministry has its employees attend cyber security training provided by MCIT and MOST, while, considering that they have not acquired sufficient computer literacy, it also having its employees attend a training course on electronic documents management.

For taking cyber security measures, MOE believes that it should improve devices to monitor cyber attacks and develop basic ICT skills among employees in the future.

4.5.6 **Ministry of Industry**

Formerly the Ministry of Industry had data centers only in Yangon but, after the capital of Myanmar was moved to Naypyidaw in 2007, the ministry in 2010 set up data centers in the new capital, too. As security measures, only firewalls have been installed and tasks to install software and manage servers are contracted to private vendors. In terms of cyber security, the ministry has prioritized introduction of applications over human resources development, and management of application installation is also contracted to private companies. As the result, the Ministry of Industry cannot acquire enough knowhow to provide training to its employees and is forced to have them attend training courses provided by MCIT or private companies.

As part of its online service, the Ministry of Industry handles information on biddings, licenses, and individuals who want to attend the training centers. For example, the ministry allows users to obtain or renew the manufacturer's licenses via the online service. Holders of the manufacturer's licenses are required to renew them every two years. The ministry has already started offering the online service for license acquisition and renewal, since holders living in distant areas have inconvenience to come all the way to Naypyidaw for such processes. Currently, the online service centers are located in each township and from where private companies can make registration.

Within the ministry, LAN is in place through cable and Wi-Fi and around 200 computers as well as smartphones and tablets can get connected to the network. As a security measure, within LAN, websites are separated into those accessible by any employee without need to enter the password and others accessible only when the correct password is entered. Anti-virus software has been installed on

all computers and is updated regularly at the ministry. Costs necessary for this are operation costs including license fees for anti-virus software and purchase of the server and application and it totals about US$25,000 annually, for which annual budgets are appropriated. Concerning the purchase of devices, however, the amount of budget allocated is not always the same amount as budget requested.
Meantime, there are no rules on how to operate email exchanges and many employees of the ministry use their own free email address. The ministry has more than 50 email addresses that are based on its domain name and these domain name addresses are assigned to higher-level managers, while a large number of employees use free email addresses as well. For example, if an employee of the ministry sends an email from the ministry's domain name address to a free mail address, the email will be treated as a spam mail, while not a few employees open emails without hesitation when they deem those emails are from their acquaintance. At the Ministry of Industry, the mail server has a sufficiently large capacity and it is urgently necessary to develop unified rules for email operation including assignment of email addresses to all employees and appropriate use of emails.

4.5.7 Ministry of Construction

The Ministry of Construction has an Intranet which uses infrastructure owned by MPT and connects with 14 local cities in order to manage the country's infrastructure such as roads and bridges as well as to share information. IT-related budgets of the Ministry of Construction represent about 1% of its total budget and the IT budgets are not always fully secured every year. Most of the IT budgets are spent on the purchase of computers and software (about US$15,000) and budgets that can be allocated to cyber security are even more limited. In addition, there is a shortage of IT knowledge within the ministry, which makes it difficult to secure budgets for the purpose. It is planned to build systems for video conference, reporting and electronic document management within three years and it is expected that US$250,000 will be required for the above system construction, excluding annual license fees, maintenance costs and operational costs for upgrading.
The Ministry of Construction manages data in the following five ways:

- To assign authorities to access important files
- To set a password for each computer terminal
- To set a password to each Microsoft application
- To install anti-virus software to key computers that are connected to the network
- To allow only particular important documents to be duplicated

There are some concerns, however, for example, some of operating systems were installed without any license arrangement and not all computers have anti-virus software.
In 2009, in Myanmar, when 18 ministries had a cyber attack from Bangladesh simultaneously, at some ministries, data stored in their database were deleted, while the Ministry of Construction was able to avoid such damage because data were backed up as the ministry was constructing its new website at that time.

The Ministry of Construction is now planning to purchase its own e-mail server system as part of the shift to e-Government. Currently, there are not many email addresses based on the ministry domain name as well as the mail server has a limited capacity, which resulted in a situation where many of its employees are using free email addresses. In order to allow employees use the ministry domain name email addresses, the number of such email addresses should be increased gradually from 500 to 1,500 so that all employees at the ministry and its regional offices can have a domain name based email address.

Thanks to the experience in the process of e-Government development and the lesson learned through the cyber attack which occurred in the past, the ministry is now aware of the importance of cyber security. While, in the past, the ministry only had four to five personnel in charge of telecommunications (responsibility shared among more than one employee) at each department, in April 2015 it set up a new Planning and IT Office in response to the direction of the Minister of Construction. It is urgently needed to develop human resources that can take responsibility of telecommunications in the ministry.

4.5.8 Ministry of Commerce

The Ministry of Commerce (MOCO) issues export and import licenses and accepts corporate registrations. At MOCO, there are a total of 13 systems including management systems and application systems under operation. MOCO has 20 regional offices and an Intranet is in place between the headquarters and those regional offices. For security purposes, the ministry installed firewalls at its headquarters and the communications between the headquarters and regional offices are made via Virtual Private Network (VPN). However, a security device is installed only at the headquarters in Naypyidaw and regional offices do not have such device. For approving logon of VPN user accounts, a domain controller is used. In addition, MOCO has its server in the data center of MPT situated in Hanthawaddy in Yangon and the server is maintained by a vendor in Yangon under a service agreement. The reason why the task is contracted to the vendor in Yangon is that the ministry needs to respond within one hour when a cyber attack occurs. Based on the past cyber attack experience, the ministry finds it difficult to respond promptly to an emergency from Naypyidaw.

For sharing data among employees, external memories such as USB memory sticks are used and data is not shared between computers connected within the network. There are no guidelines on cyber security and proper awareness has not been established about correct emergency responses such as isolation of attacked computers from LAN. In addition, as smartphones become widespread, currently employees can access the ministry's Wi-Fi service from their phones. Therefore, MOCO considers they need to develop guidelines.

MOCO allows its employees to use free email accounts for email exchanges. There are several reasons for this: the number of email accounts with the government domain name is limited; not enough capacity is available for attaching large files; those government domain email addresses are prone to virus attacks; and the application used for government domain email addresses has no filtering function to reject spam mails. For the future, MOCO says it will introduce a document exchange

system and a web application mail system to promote the use of government domain mail addresses.
In the past, MOCO had its IT personnel attend opinion exchange meetings of CIOs and CSOs of other ministries and agencies, which are held by MCIT. This meeting was held seven or eight times in a year but more recently instead of holding the meeting, information is shared via emails. MOCO considers that, in the future, rather than holding the meeting to be attended only by government ministries, the government should get private companies excelling the government organizations in technical skills in cyber security involved in the discussions on cyber security.
Since IT budgets are allocated year by year, it is not certain whether cyber security budgets sufficient to take necessary measures can be secured or not. The Myanmar government has been advancing its e-Government project but purchases are made independently by each ministry or agency. For example, the purchase of training room described in 4.4.3 above cost about US$100,000.

4.5.9 Ministry of Health

Also at the Ministry of Health, the development of e-Government has been underway as it is going on at other ministries. The Ministry of Health has been using an electronic document management system. At the data center of MPT in Yangon, the ministry has two servers for a health information system and a health management system using the hosting service. As the result, various ministries and agencies have access to raw data owned by the Ministry of Health stored there. In relation to this, the ministry considers that maintenance of security is extremely important. Because of the current skill of the ministry's personnel, however, the Ministry of Health is forced to contract some security tasks to local private companies. Due to a shortage of budgets, this year, no maintenance agreement has been made with private service vendors.
At the ministry, anti-virus software is installed on all computers, while no device that can detect viruses has been introduced. Therefore, notices of virus detection made by the software are the only way to identify virus attacks at the moment. Additionally, a number of employees have access to data stored in the ministry through their smartphone or mobile phone, too.
At the Ministry of Health, a CIO is appointed to supervise the electronic document management system and the website but no CSO is appointed. The ministry understands the importance of security measures, while there are almost no personnel who have necessary knowledge and skill and employees are not certain how to promote security measures under the present situation where no guidelines are established. In addition, appropriate knowhow does not stay at the ministry as employees who were sent to and completed IT training often leave the ministry. The Ministry of Health has six departments and it considers every department should have personnel with security knowledge. In reality, however, enough manpower cannot be secured at the ministry.

4.5.10 Central Bank of Myanmar

Unlike Japan, Myanmar has not established special security standards for the financial industry. The current system is not connected to the Internet and, therefore, the Central Bank has no concern for security and considers that it should prioritize education and awareness activity. When the system

becomes operative online in the future, however, cyber security measures would be an indispensable condition.

The Central Bank has no definition concerning important assets. Under the military regime to date, information on important assets has been made confidential but as the country is more incorporated into the global market economy, it is necessary to review what kind of information should remain confidential and what should be disclosed.

Currently, the Central Bank is about to develop security guidelines in accordance with the Information Security Management System (ISMS). It is planned to start operation of an accounting system in December 2015 and a CV net in January 2016. When Myanmar is to have its financial industry grow, cyber security should be positioned as an important element. It is essential to develop and strengthen the environment in which its people can have money deposited in banks without concern.

4.5.11 **Naypyidaw Development Committee: NDC**

The Naypyidaw Development Committee (NDC) is a local administrative body in charge of development of Naypyidaw. Under the leadership of the mayor and the deputy mayor of Naypyidaw, the committee has seven members and there are eight townships and a total of 800 employees under the control of NDC. Of these employees, a total of 76 employees use computers, with 2 employees using computers at each township and at each of 20 departments of the NDC headquarters, respectively, and 20 using computers at the ICT section. Other employees use their own mobile phones or tablets. The number of computers that are connected to the Internet, however, is 20 units which are situated at the ICT section, where data are backed up regularly. For the time being, NDC does not provide any online service and what it manages is mainly emails sent or received by its employees. NDC has its own domain name email addresses but only a part of the accounts are assigned to employees.

At NDC, the CIO also acts as CSO concurrently. Because of a shortage of knowledge, how the CSO should act is not understood clearly. As task loads of CIO and CSO are increasing and as there are not many applicants, too, it is difficult to select suitable candidates. The present CIO has knowledge of programming and develops applications. Construction and management of website which NDC cannot carry out by itself are contracted to independent vendors. IPS/IDS have not been introduced because NDC lacks necessary knowledge.

NDC has suffered cyber attacks on its website. Whenever it was attacked, the website was recovered with backup data. Without taking any appropriate measures later, however, NDC has been attacked again and again. Having no guidelines or training courses on cyber security and lacking cyber security knowledge, NDC is unable to take any measures. It is planned to provide online service and expand its ICT system in the future and in line with the plan, possible security measures are now being studied.

Its ICT Department was established only one year ago and the bureau requests budgets based on operational costs of necessary activities and gets approval. The actual amount of budget spent during the past year was US$80,000 in total. The budget was spent on the server, network configuration, firewalls and maintenance contracts for website.

4.5.12 Comparison of Responses made by Ministries and Agencies

Table 4.5-1 shows responses made by the ministries and other agencies discussed in sections from 4.5.1 to 4.5.11 above.

Following the DDoS attacks in 2010 and as awareness of the importance of security measures increased, most of the Myanmar government's ministries have installed a firewall. Meanwhile, there are many ministries allowing their employees to connect to Wi-Fi from mobile devices. The fact indicates there is a tendency to prioritize convenience over security. There are a number of issues to be solved in the future. For example, although MCIT recommends to assign a CIO and CSO as personnel in charge of IT respectively and to divide their responsibilities, only two ministries have already appointed a CSO, and a response manual has not been developed, too.

Table 4.5-1 List of cyber security measures taken by ministries and agencies

	CS attack	CS device	Connection from mobile device	Contracting to private sector	CIO	CSO	Response manual, etc.	Training	Budgets
MCIT	○	○ FW/ TSUBAME	○	-	○	×	○ mmCERT only	○	○
MOST	×	○	×	○	○	×	×	○	○
MOE	○	×	-	-	○	○	Guidelines	○	○
Ministry of Industry	-	△ FW only	○	○	○	×	-	△ Not having own courses	○
Ministry of Construction	○	×	-	-	○	×	-	○	○
MOCO	○	△ FW only	-	○	○	○	-	○	○
Ministry of Health	-	△ FW only	○	○	○	×	-	○	○
NDC	○	△ FW only	○	○	○	×	×	×	○

Legend: ○in place, ×not in place, △with some conditions

CS: Cyber Security; CIO: Chief Information Officer; CSO: Chief Security Officer; NDC: Naypyidaw Development Committee; FW: Firewall

*MPT is an independent telecommunications carrier and the information for MCIT in the above table does not include that on MPT but includes that on mmCERT.

4.6 Assistance in the Cyber Security Field Provided by Other Governments and Donors

No other governments or donors offer collaboration or assistance exclusively in the cyber security field. In this section, discussion is made on other governments and donors' assistance in the telecommunications field.

Since 2004, among other governments and donors, South Korea, China and India are the major providers of assistance in the telecommunications field to Myanmar. After the start of the Thein Sein administration in March 2011, not only Japan but also international organizations like the World Bank and the Asian Development Bank (ADB) started offering assistance.

The World Bank offers assistance to solve issues concerning public service and infrastructure in rural areas, climate changes, the gender issue and the hygiene and sanitation system in the fields of irrigation and sewage, hygiene and sanitation, ports, waterways and ships, central government management, forests and education. As it is necessary to make efforts jointly with the telecommunication sector in education or the provision of public services to rural areas, the World Bank has implemented a project to revolutionize the telecommunications sector (refer to Table 4.6-1).

ADB set targets of mid-term outcome in the development of a sustainable and free economy and job creation for poverty reduction and has the following assistance priorities in its strategic efforts that are centered tentatively at individual and organizational capability development, improvement in structural economic environment and the development of convenience of life and infrastructure in rural areas.

- A sustainable environment should be built with environmental considerations and by integrating development strategies and plans in important sectors.
- Favorable governance should be carried out by achieving transparency in public finance and accountability.
- The private sector should be developed through policies for investment and trade and in an enhanced legal and regulatory environment.
- Regional cooperation and integration should be achieved in trade and investment.
- Equality between men and women should be realized based on women's capability development and analysis of gender gap in job creation and entrepreneur opportunities.

In the telecommunications sector, South Korea and China have provided assistance to the development of an e-Governance master plan through jointly financed technical cooperation between the two countries (refer to Table 4.6-1) but it was not made a prioritized area. The two countries plan to promote the use of ICT in vocational training for women in rural areas.

The US Agency for International Development (USAID) has the following four prioritized policies: (1) Promotion of control through democracy, human rights and laws; (2) Enhancement of transparent governance systems; (3) Implementation of peace and reconciliation and; (4) Improvement in hygiene and sanitation, food security, economic opportunities and living standard. USAID provides assistance to broadcasting and journalism, for example, for fostering of fair and neutral media but does not provide direct assistance in the telecommunications field.

Since 2004, KOICA has been providing assistance actively for the ICT master plan and the shift to e-Government but the e-Government project has not advanced as initially planned due to a shortage of funds at the side of the Myanmar government.

Meanwhile, Japan's assistance to Myanmar in the telecommunications field has been carried out

through various schemes such as technical, grant aid and loan assistance, as presented in Table 4.6-2.

Table 4.6-1 Assistance provided by other donor countries and international organizations (Telecommunications, in 2004 and later)

No.	Project	Year	Amount (US$ Million)	Donor
1.	Assistance to the preparation of Myanmar ICT development master plan Summary: Preparation of an ICT master plan (2010-2015) targeting at the e-National Task Force (e-NTF)	August 2004 to August 2005	0.95 (Grant aid)	Korea
2.	Myanmar e-Government Basic System	November 2005 to October 2006	12.00 (Loan assistance)	Korea
3.	Construction of Yatanarpon Cybercity Summary: India assists in the software area and China in the hardware area. The teleport center (started operation in Dec. 2007) and the incubation center (in Dec. 2008).	Since 2007	N/A	India, China
4.	Telecom development project (MPT)	In around 2007 (Details N/A)	3.02 (Loan assistance)	China
5.	GSM system expansion project (MPT)	In around 2007 (Details N/A)	1.25 (Loan assistance)	China
6.	National telecom network construction project	Planned in 2007 (Details N/A)	150.00	China
7.	corDECT system construction and cross-border connection project (MPT)	N/A	7.00 (Loan assistance)	India
8.	India and Myanmar e-learning & research center (e-NTF)	Planned in 2007 (Planned to be a five-year project) (Details N/A)	N/A	India
9.	Software technology training center (USCY) Summary: Dispatch of lecturers and acceptance of trainees	Since October 2008	N/A (Technical assistance)	India
10.	Broadband satellite network project (MPT)	In around 2007 (Details N/A)	15.00	Thailand
11.	Telecommunications Sector Reform Project Components: ・Construction of a structural connection environment ・Expansion of connection to rural areas ・e-Government infrastructure construction ・Assistance for project implementation management	May 2014 to Dec. 2019 (Planned)	31.50	World Bank
12.	Preparation of e-Governance master plan and review of academic organizations' capability in the telecommunications	March 2014 to June 2015	1.50 (0.50 each)	ADB, Korea

No.	Project	Year	Amount (US$ Million)	Donor
	sector		(Technical assistance)	and China
	Joint funding of South Korea's e-Asia and knowledge sharing fund and China's regional cooperation and poverty reduction fund			
13.	Overall evaluation of Myanmar's ICT sector	July 2014 to June 2015	N/A (Technical assistance)	ADB

Source:
World Bank
(http://www.worldbank.org/projects/search?lang=en&searchTerm=&countrycode_exact=MM)
ADB (http://www.adb.org/projects/documents/search/country/mya?keywords=)
USAID (http://portfolio.usaid.gov/#)
Materials of FY2012 First JTEC Conference (Jan. 18, 2012)
http://www.jtec.or.jp/2012.1.18kouenkai_kouno2.pdf

Table 4.6-2 Records of Japan's assistance (Telecommunications, in 2006 and later)

No.	Project	Year	Amount (¥100 million)	Scheme
1.	Project on ICT Human Resource Development at ICT Training Institute in the Union of Myanmar	December 2006 to November 2011	3.10	Technical project
2.	The Project for Urgent Improvement of Communication Networks	2012 (E/N concluded)	17.10	Grant aid
3.	The Project for Development of ICT System for Central Banking	2013 (E/N concluded)	51.00	Grant aid
4.	Advisor for Improvement of Telecommunication Infrastructure	November 2013 to June 2015	-	Loan assistance Dispatch of experts
5.	Communication Network Improvement Project	March 2015 to August 2019 (Planned)	105.00	Loan assistance
6.	Policy Advisor for Communication and Information Technology	October 2015 to September 2016 (Planned)	-	Loan assistance Dispatch of experts

Source:
ODA Data by country, Ministry of Foreign Affairs of Japan (Myanmar)
(http://www.mofa.go.jp/mofaj/gaiko/oda/index.html)
JICA Knowledge Site (http://gwweb.jica.go.jp/KM/KM_Frame.nsf/NaviIndex?OpenNavigator)

4.7 Comparison with Other ASEAN Countries

Some comparisons were made between Myanmar and other ASEAN countries, in terms of e-Government and cyber security. The following discussion includes major results of such comparisons.

4.7.1 e-Government

In order to compare Myanmar with other ASEAN countries with respect to the development of e-Government, the e-Government Development Index (EGDI)[1] developed by the United Nations is used. EGDI is created by analyzing the government's online service, telecommunication infrastructure and human capital to understand how far each government has developed e-Government. Among ASEAN countries, Myanmar ranks the worst, particularly the country gets low marks in online service and communications infrastructure. The top ASEAN country in this ranking is Singapore. Among all countries, South Korea ranks top and Japan is at the 6th from the top.

Table 4.7-1 e-Government Development Index of ASEAN countries

Rank	Country	EGDI[2]	Online Service Component	Telecomm. Infrastructure Component	Human Capital Component
3	Singapore	**0.9076**	0.9921	0.8793	0.8515
(6)	*(Japan)*	***0.8874***	*0.9449*	*0.8553*	*0.8621*
52	Malaysia	**0.6115**	0.6772	0.4455	0.7119
86	Brunei Darussalam	**0.5042**	0.3622	0.3690	0.7815
95	Philippines	**0.4768**	0.4803	0.2451	0.7051
99	Viet Nam	**0.4705**	0.4173	0.3792	0.6148
102	Thailand	**0.4631**	0.4409	0.2843	0.6640
106	Indonesia	**0.4487**	0.3622	0.3054	0.6786
139	Cambodia	**0.2999**	0.1732	0.2075	0.5189
152	Lao	**0.2659**	0.1417	0.1618	0.4941
175	**Myanmar**	**0.1869**	0.0236	0.0084	0.5288

4.7.2 Cyber Security

In order to compare Myanmar with other ASEAN countries with respect to cyber security measures, the Global Cyber Security Index (GCI)[3] prepared by ITU and the "Data Collection Survey for

[1] UN, E-Government Survey 2014

[2] EGDI : E-Government Development Index

[3] ITU, Global Cybersecurity Index & Cyberwellness Profiles

Information Security in ASEAN Countries" (2012) prepared by JICA are used.

ITU's GCI is prepared by analyzing each country's cyber security measures in terms of development of legal systems, technical measures, organizational measures, capability development and cooperation. Among ASEAN countries, Myanmar ranks the 6th, while it gets low marks in the development of legal systems and organizational measures. The top ASEAN country in this ranking is Malaysia. Among all countries, the US ranks the top and Japan is positioned in the 5th rank.

In this GCI, a number of countries often belong to the same rank and all countries are positioned in somewhere in a total of 29 ranks. For example, Japan is positioned in the 5th rank, while sharing the ranking of 8th with other countries. In the 5th rank, there are seven more countries than Japan.

Table 4.7-2 Global Cyber Security Index of ASEAN countries

Rank	**Country**	**GCI**	**Legal**	**Technical**	**Organi-zational**	**Capacity Building**	**Coope-ration**
3/29	Malaysia	**0.7647**	0.7500	0.8333	1.0000	0.6250	0.6250
(5/29)	*(Japan)*	***0.7059***	*1.0000*	*0.6667*	*0.7500*	*0.6250*	*0.6250*
6/29	Singapore	**0.6765**	0.7500	0.6667	0.7500	0.7500	0.5000
13/29	Indonesia	**0.4706**	1.0000	0.3333	0.2500	0.5000	0.5000
15/29	Thailand	**0.4118**	0.5000	0.3333	0.5000	0.2500	0.5000
16/29	Brunei Darussalam	**0.3824**	0.7500	0.3333	0.1250	0.3750	0.5000
16/29	**Myanmar**	**0.3824**	0.2500	0.5000	0.2500	0.5000	0.3750
17/29	Philippines	**0.3529**	1.0000	0.3333	0.3750	0.3750	0.0000
18/29	Viet Nam	**0.3235**	0.5000	0.3333	0.1250	0.5000	0.2500
25/29	Cambodia	**0.1176**	0.2500	0.3333	0.1250	0.0000	0.0000
27/29	Lao	**0.0588**	0.0000	0.3333	0.0000	0.0000	0.0000

In the "Data Collection Survey for Information Security in ASEAN Countries," based on the latest data of ASEAN countries such as ICT trend, economic situations, the level of security measures and international relations, analysis is made, while categorizing those countries into the following groups: "Information Security (IS) advanced country;" "Country with issues on IS policy promotion;" and "Country with issues on IS leader development." Into the category of country with issues on IS leader development, Myanmar was grouped along with Laos and Cambodia. In these three countries, the development of an ICT environment cannot be considered sufficient nor are securities measures properly taken and their economic standard is deemed low, too. They are expecting to obtain assistance from other countries, both at the government level and at the large company level.

Table 4.7-3 Categorization of ASEAN countries to review possible international collaboration

Category	**Country**
IS advanced country	Singapore, Brunei Darussalam, Malaysia
Country with issues on IS policy promotion	Thailand, Philippines, Indonesia, Viet Nam
Country with issues on IS leader development	Lao, Cambodia, **Myanmar**

Chapter 5 Status of Security Countermeasures in Government and Related Organizations

5.1 Security Assessment for Government ICT Environment

5.1.1 Target of Security Assessment

As a result of organization reforming in MCIT, MPT took charge of each ministry and agency and start operate them as a part of MPT's co-location service.
On the other hand, systems shared by ministry and agency moved to operation under the new established IT&CS, e-Government group that took charge of operation was established a part form security group.
According to above assignment, IT&CS took charge of 2 of 4 data centers owned by MCIT, one is in Naypyidaw city (called "S-12"), another is in north of Naypyidaw (called "Thayetkhon"). E-Government system is installed in S-12.
IT&CS is considering S-12 data center as an important ICT environment which deploy and operate e-Government systems continuously. Therefore, this data center shall be an ICT environment that empowered with sufficient security counter measures.
Owning to this background, with observation for operation process and situation of S-12 data center (especially e-Government system), security assessment on following points were conducted in this survey.

- Security policy, Operation rules
- State of implementation of security patch
- Management of operational log properly
- Procedures for Incident Report (including escalation rules)
- Staff organization
- Awareness for information securities
- State of implementation of technical measures

5.1.2 Result of Security Assessment

The current situation that government staffs using regular Gmail service instead of e-mail address provided by government, to share or handle information with it, containing critical risk on security. On the contrary, there is no government use WAN or LAN (such as "Kasumigaseki WAN" or "LG-WAN" in Japan) developed in Myanmar government. Moreover, also MCIT the regulatory of ICT have not developed their LAN yet, currently they are connecting to commercial internet service by each unit (per section, per room, etc.) and all transaction are going through public internet.
Therefore, MCIT is structurally impossible to protect ICT Security by their network. Though it is needless to say that counter measures such as facility investment are necessary, time and budget shall be required for the counter measures. Due to this situation and priority considering, ensure security level with awareness rising and operation is critical.

For above viewpoint, with observation on operation situation, result of security assessment becomes as follows.

I. Security policy, Operation rules

[Current Situation]

However the Security policy supposed to be drafted by security group of IT&CS, currently drafting have not progressed due to the group is lacking human and financial resources for example only one staff in group or doesn't have their original budget because of organization reformation.

By contrast, e-Government group who is in charge of operation of e-Government systems is continuously operating under the situation of no rules/guidelines such as security policy. In addition, due to limited operation staff, operation rules are not documented so it depend to arbitrary decision of operation staff and also no review system for appropriateness of operation flow.

Moreover, system maintenance is limited to recovery of system function (temporally contract with local company); there is no changing on system (no change management process applied) such as revision or upgrade, as well as no PDCA cycle enforced.

[Counter Measure]

To develop security policy, at least preparation of several human resources with knowledge and experiment or budget reservation for hiring consultant with skill to support development shall be necessary. Nevertheless the security policy is not only helpful for all security management but also contribute all government in Myanmar by referring even if the policy developed by IT&CS is only targeted for MCIT. For that point of view, the referable security policy is highly expected by every ministries and agencies; it must be developed as soon as possible.

In addition, the operation rules such as change management shall be defined in security policy.

II. State of implementation of security patch

[Current Situation]

Patch application on e-Government system is conducted by operation staff with their arbitrary decision. From the result of vulnerability assessment descripted below, security patches provided by vendors are applied but it is not defined as rules, furthermore an influence test, approval process flow and application record are not controlled.

[Counter Measure]

In security policy or operation policy, it is necessary to clarify patch application rules such as application process to enable situation share between operation team, periodic check of application necessity, technical verification method (flow) for application or confirmation of role-sharing and responsibility for application.

III. Management of operational log properly

[Current Situation]

Monitoring of system log is conducted at all time as required, but frequency or level of monitoring is not defined clearly and it depends on each administrator. Though the volume of daily operation work is unclear, daily operation log such as creation and share of daily report is not conducted systematically.

[Counter Measure]

For monitoring of system log and access log, its frequency and method shall be ruled clearly, its result shall be shared with many staff and recommended to conduct with plenty of manpower. For daily operation log, it is recommended to establish situation share method by creating formatted daily report at least.

IV. Procedures for Incident Report (including escalation rules)

[Current Situation]

When incident or problem occurred, there is a process that administrator documents (reports) its detail and counter measure to manager. Though daily managed problems are not documented, the management system for long term problem resolution, priority of the problem doesn't have a management system.

[Counter Measure]

It is required to define rules for documented management method such as a problem management format or an incident management format, stipulate the method and operation process.

V. Staff organization

[Current Situation]

E-government group have approximately 50 staffs, nevertheless only two in total, one each administrator assigned for e-Government system and mail system. It is impossible to conduct daily operation if administrator is absent.

In addition, since it is hard to find satisfied volume of human resource in data center site (S-12), technical staff is very few.

[Counter Measure]

For administrator, each system shall be assigned more than 2 staffs with satisfied operation skills (concurrent permissible). Beside, operation staffs shall be enforced as soon as possible. Since IT&CS is currently in growing process, more technical staff expected to be complemented form MPT. If it is difficult to find such staff, it is possible to train by government.

In addition, human resources planning for IT&CS also required as soon as possible.

VI. Awareness for information securities

[Current Situation]

From the result of interview survey on academic (university) relatives in Myanmar, since security education in Myanmar is almost nothing, awareness on security is basically low. Especially for expert in security is hard to hire.

[Counter Measure]

To raise security awareness, security education or enlightenment shall be important; moreover prior to these, standard of conduct shall be developed and presented based on security policy.
From the point of view, establishment of security policy is required as soon as possible.

VII. State of implementation of technical measures

[Current Situation]

Accordingly there is no LAN or WAN implemented, all users of e-Document management system will access from public Internet. Thereby, the system has to be connected to internet and a security counter measure will be necessary.
For the security measures conducted in data center, basic minimum protection such as anti-virus for each servers or firewall and VPN that protect network environment. On the other hand, advanced packet level monitoring function such as IDS/IPS, DDOS attack or application/contents level security measure such as WAF, DLP are not installed.

[Counter Measure]

However the firewall hardware which is upgradable to IDS/IPS has been installed in data center, it is not activated at this time. For the purpose of operate country's e-government system, advanced security shall be important, but operation is conducted by staffs themselves and the staffs who can technically catch up is still limited; as result operate various security counter measure is difficult in current situation.
Therefore, important security measures are as follows.

- With activation of IDS/IPS function, monitoring of more detailed security situation is necessary (additionally, able to protect e-government system users)
- In addition to various log collection, preservation and analysis, installation of functions that support operation such as error detection, it covers human resource shortage.
- Though installed e-Government system is limited, important document shall be handled in e-Document Management System. Therefore, Application/Content level security management is necessary.

5.1.3 Required counter measures for future Myanmar government ICT environment

Each of above-mentioned assessment result shall be taken counter measure as soon as possible. On the other hand, because ICT environment in Myanmar government is still in beginning phase of development, in addition to above-mentioned counter measures necessary environment development shall be progress upon future ICT environment development blueprint.

Current network environment of MCIT is as below figure. Internet connection is installed to each small group such as section or physical area such as a room; every PC is connected to each network via small LAN or wireless access point. Thereby, user environment in MCIT is quite similar to ordinary home user's environment and there is no organization-overall security measure is installed.

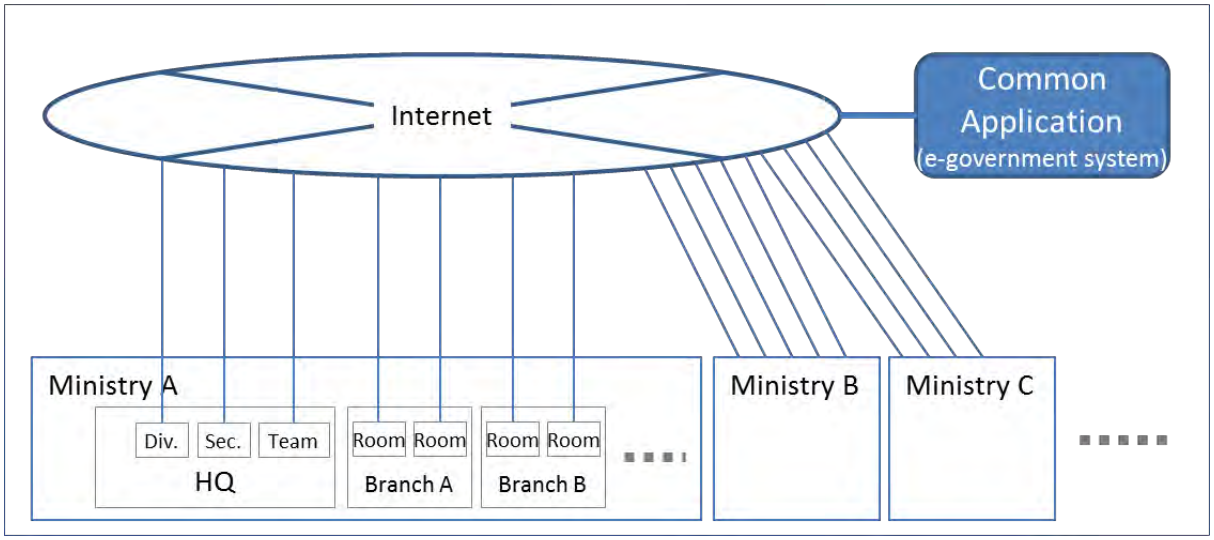


Figure 5.1-1 Current ICT environment of Myanmar government

In this case, most of information management in ministries/agencies such as internal user machine, transferred information, whereabouts of information asset and control situation is difficult to manage. Thereby, it is also difficult to manage total counter measure against expected security threats.

Moreover, for the common application to share with all government that MCIT expected to provide must control with exclusive terminal or user side management (ID/Password) because of difficulty on detection and management of user machine.

In case of using exclusive terminal, all application use shall be accessed from limited exclusive terminal; it shall reduce user's usability, therefor USB memory or user's local network will be connected and it will cause some security risk.

In case of using user side management, since control limited to user access, cyber-attack such as spoofing is not able to protect and manage including trace & track.

On the other hand, Japanese government already implemented LAN or WAN for each ministry and "Kasumigaseki WAN" as an interconnect network between ministries. With this network environment, critical information is able to handle in this exclusive network, furthermore each ministry's network and "Kasumigaseki WAN" are protected by security measure. This model enables total security

management of government and it has been applied not only in Japanese government but also in many organizations including advanced country's governments or large enterprises.

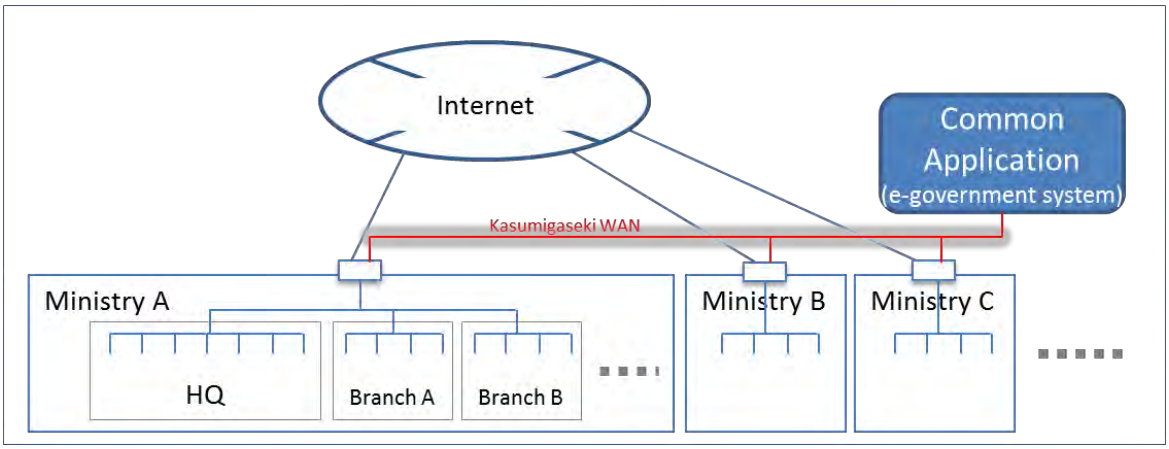


Figure 5.1-2 Japanese Government ICT environment

However even in Myanmar government re-build ICT environment as above figure in the future, it is difficult to complete rapidly due to its cost (annual operation cost of "Kasumigaseki WAN" rise up to 300 million yen) and human resource stock of operation/management staff. As Japanese case took 4 to 5 years including coordination among government organizations, it shall be a project to tackle with mid-term scope.

Especially in Myanmar, as government network is under development as mentioned above, from viewpoint of control of information assets and total security, it is recommended to give priority to network integration as below figure.

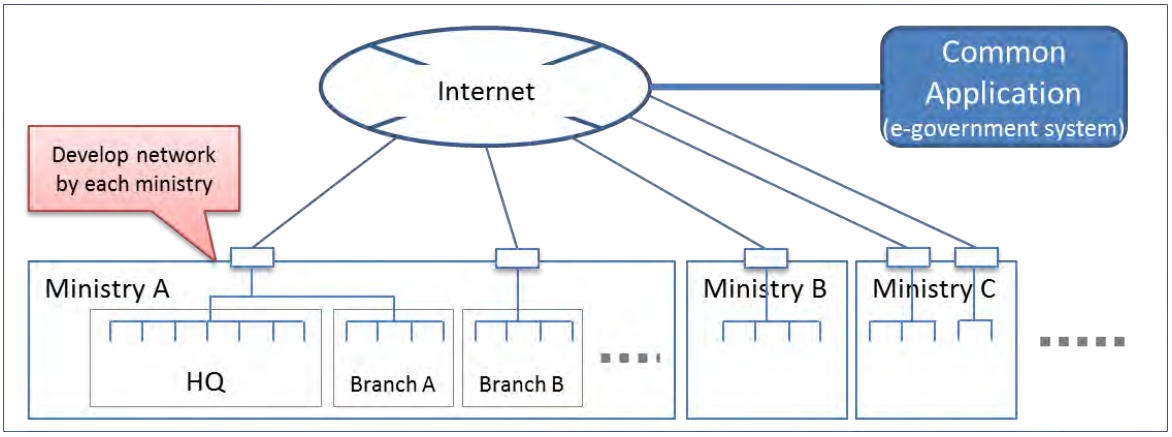


Figure 5.1-3 Expected ICT environment for Myanmar government

For network integration, the priority is not unification into one network but reorganization of scattered internet connection small LAN or WAN into manageable numbers and comprehend connection point

to external network (public internet). Consequently to this integration, designing and development of WAN for each government organization and inter government organization, security counter measure in shared application become available.
For network development of each government organization, each organization needs establishment of coordination team, survey on current situation and design plan and cost for development.
Among these processes, survey on current situation and design plan requires expertise for security and large scale network. Since human development of each ministry requires long time so that integration will be delayed, cooperation shall be efficient such as provision of basic plan as template or dispatch of expert for basic research or planning which is also effective for capacity building of government staff.
By contrast, for financial cooperation, since running cost will be a big potion compare to initial cost, a careful consideration shall be required such as budget volume.
On the other hand, for data center which common application installed expected to be taken more high level security counter measure because all governments may share the safety benefit for their use of application. For this reason, intensive technical assistance (include installation of security hardware) shall contributes to enhancement of ICT environment for Myanmar government.

5.2 Vulnerability Assessment on e-Government System

5.2.1 Target e-Government System for Vulnerability Assessment

As part of survey on current situation of security counter measure for e-Government system in Myanmar, the survey team conducted vulnerability assessment as below on selected server of the system.

- Collection of latent vulnerability information using specified scan tool (“Nessus”)
- Vulnerability assessment based on interview to person in charge of security policy development and vulnerability information collected in above
- Risk assessment such as what concern occurs which probability

As of end of August 2015, e-government systems installed (or to be installed) in S-12 data center are following four systems (as table below).
Except systems under development, two of e-government systems are currently activated and operated - Email system and e-Document Management System. Among these two, typical application based system is only e-Document Management System.
According to above reasons, the survey team selected e-Document Management System as vulnerability assessment target.

Table 5.2-1 e-Government systems in S-12 data center

System	Description	Status
Email System	Email server for government staffs but its account is only provided to a part of staffs such as high class officers (not for every staffs)	Under operation
Human Resource Management System	Personnel related information management system for all government and it is under development. One development server is currently connected.	Under development
e-Document Management System	The system to stock and manage e-document handled in government. It is currently under operation and every ministry and agency is using.	Under operation
Government portal system	Portal service to provide one-stop usability for web site and government service site (or its links). It is planned to develop soon.	Before development (Only hardware is installed)

5.2.2 Outline of e-Document Management System and Point of Vulnerability Assessment

E-Document Management System is the system which to register and store electronic government documents and it provides evenly 100GB storage for one ministry/agency, it also provide WEB base interface to register, search, manage and view documents. MCIT provide common application and lower layer environment and each ministry/agency manage access to system (user management) and actual utilization.

The system structure of e-document system server (EDMS Server) and peripherals is as figure below, 2 virtual servers for each totally 60 virtual servers defined on 30 physical servers (machine). Each physical server has totally 4 network ports installed, 2 ports for each virtual server and those are gathered to switches on internet side (EDMS Switch), other 2 ports connected to 2 route of internal management network switch (VM Switch and Hardware Management Switch). For public internet, the system is connected through firewall, use VPN to access from internet.

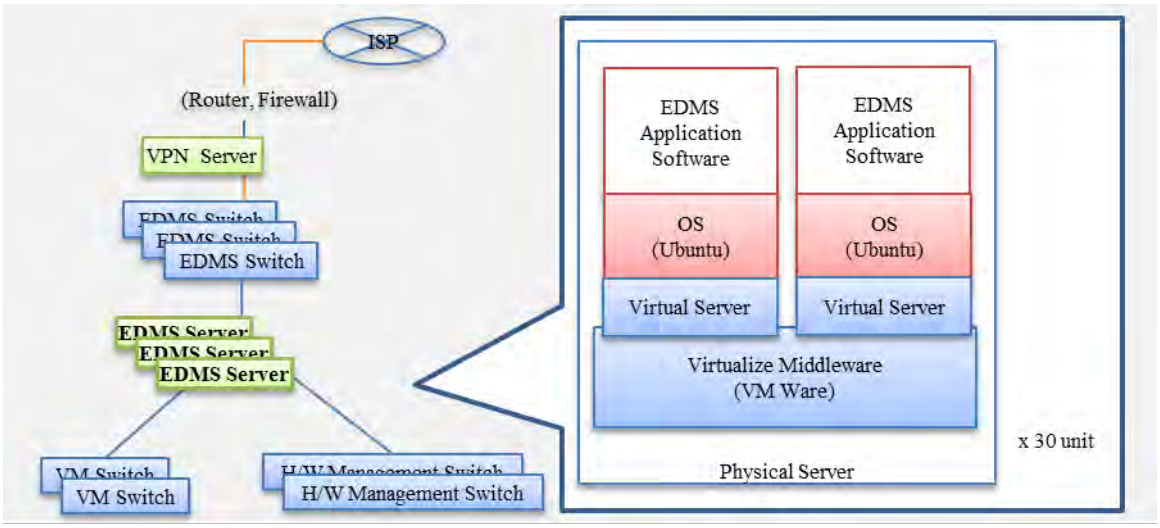


Figure 5.2-1 System Structure of e-Document Management System

Considering its system structure, EDMS Server has two way network connection points - internet side and internal side. Therefore, possible attacking risk exist from internet side port by users and outsider and from internal side port by whom invaded data center such as evil insider.

Owing to this, the survey team run vulnerability scan using scanning tool on 2 network connection points of EDMS server, one is internet side port that faced by virtual server interface and another one is internal side port that faced by interface under virtualization middleware.

5.2.3 Result of Vulnerability Assessment on e-Government System

I. Vulnerability assessment on internet side connection

Internet side port is assigned to each virtual server, so what is able to scan from internet side network access is the vulnerability situation above virtual server. From internet side port, there is a possibility to receive attack from users connecting via VPN with connection permission or attacker from public internet who break through VPN with some reason. The attack is expected to have more possibility and frequency compare to internal attack, therefore it is important to taken sufficient security counter measure.

As of Aug. 2015, scanning result with specified tool (Nessus) for security vulnerability on internet side (connect test machine to EDMS switch and scan from connected environment) was such as Figure 5.2-2.

Detected security hole categorized to four by severity level as “Critical” “High” “Medium” and “Low”. “Medium” or “Low” means take counter measure if it is timely or continuously pay attention to the risk.

For the internet side, 3 points of “Low” level security vulnerability were found, but there was no “Critical” or “High” level security vulnerability was not found. As a result, target server was taken sufficient security counter measure at survey date.

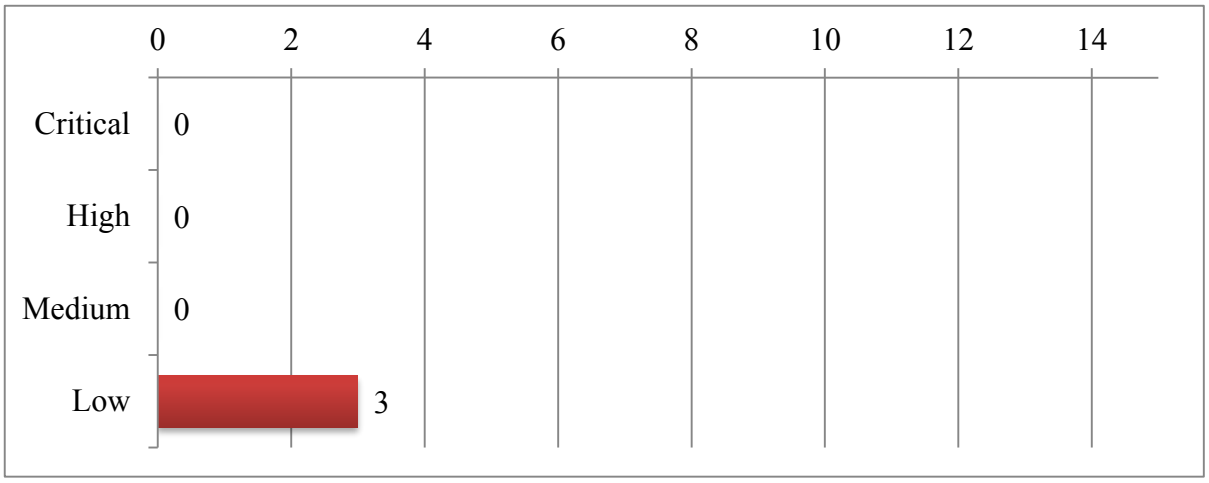


Figure 5.2-2 Result of vulnerability test on Internet side port

For 3 vulnerability risk detected by Nessus, one was risk on Cleartext Credential of web server, other 2 was vulnerability related to SSH. Both are risk that must keep attention, but area of influence is limited, it is not necessary to correspond rapidly and counter measure is still not difficult.
In addition, the purpose of system server is limited, operated on Linux OS, application on server is still simple. Therefore, the most of security setting is fulfilled with initial setting, furthermore security management in operation phase is already simplified, and it is another reason reducing vulnerability.
Thereby, security risk on internet port side of EDMS server shall be alright with adequate operation and maintenance including necessary patch application.

II. Vulnerability assessment on internal side connection

For internal side, one port for control and manage VM ware and another one port for management of hardware were reserved on each physical server, and it is possible to manipulate and manage including modification of server settings.
Though this server connect 2 port for management purpose and both ports are integrated to each switches, there is no other type of servers or machines will connect to these switches and connecting operation terminal temporally in case of operation. For this reason, attack from internal side is limited to the case such as jacking physical port of these internal switches, so by combination with access control to data center room, security is more reliable.
As of Aug. 2015, scanning result with specified tool (Nessus) for security vulnerability on internal side (connect test machine to VM switch and scan from connected environment) was such as Figure 5.2-3.
For the internal side ports, 1 points of “High” level and 12 points of “medium” level security vulnerability were found. Since number of security vulnerability is raised compare to internet side, the basic security is guaranteed with combination of access control for data center room, the result doesn’t mean there is a critical issue on security vulnerability.

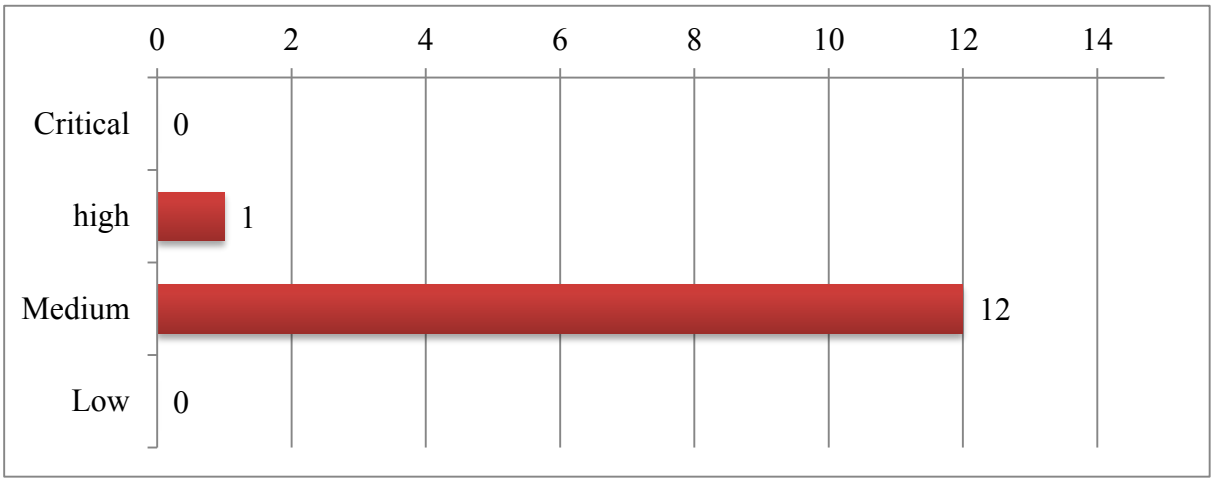


Figure 5.2-3 Result of vulnerability test on Internet side port

Detected "High" level vulnerability and eight of twelve "Medium" level vulnerabilities are able to correspond by applying patches, but as mentioned above, periodical patch application is not conducted in daily operation. For other detected vulnerabilities such as three points related to SSL and one point related to transport layer issue, aren't serious issues if considering the internal ports are not open to public.

Thereby, security risk on internal port side of EDMS server doesn't have critical vulnerability if data center is managed adequately. On the other hand, including detected "High" level vulnerability, more sufficient security level shall be realized if patches applied adequately. Including periodic patch application, operation upon security policy is strongly recommended.

5.3 Vulnerability Assessment for Website of Government Organization.

5.3.1 Target Website of Vulnerability Assessment

Vulnerability assessment for website of Myanmar government organization was conducted to grasp cybersecurity management capability of the organization. The assessment method is follows:

- Vulnerability scanning using Nessus
- Vulnerability assessment from interview with manager and operator of the website
- Risk assessment of the website

At the end of August 2015, Myanmar government websites are operated by MPT and installed in the Hanthawady DC in Yangon. MCIT website (http://www.mcit.gov.mm/) was selected as an assessment target.

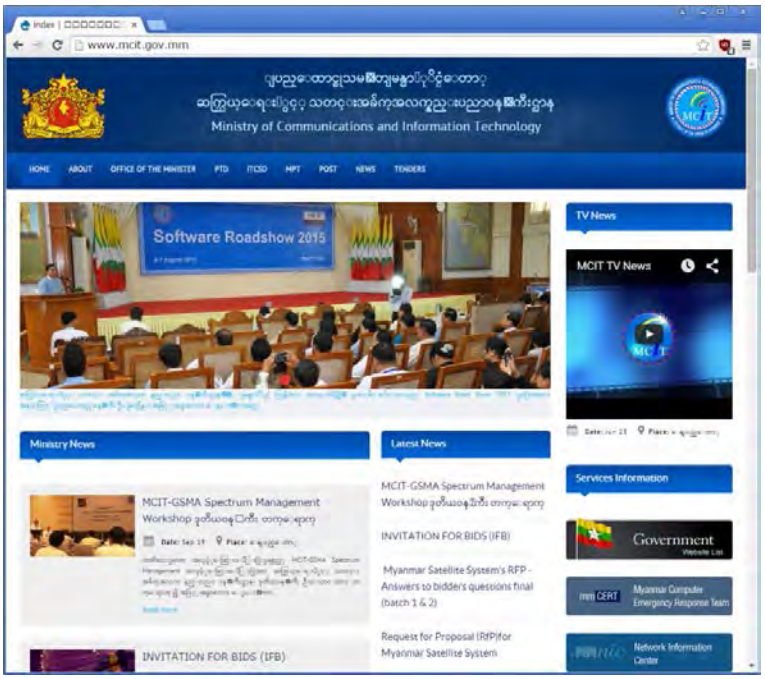


Figure 5.3-1 Website of MCIT

5.3.2 About the Website and the Overview of Vulnerability Assessment

The website of MCIT is implemented by a general WEB server that stored static content. As mentioned already, the WEB server is installed in Hanthawady data center of MPT. The webserver is operated by MPT in Yangon, Contents are managed by MCIT in Naypyidaw. The contents owner is in each department.

The objective of the vulnerability assessment is to verify technology management capability of Myanmar government and to reveal the existence of vulnerability. For this objective, we did a diagnosis which simulates the cyber-attack from the internet.

5.3.3 Vulnerability Assessment Result of the Website

I. Vulnerability Assessment using Scan Tool

Since the internet ports on the webserver are exposed to various cyber-attack through firewall, it is important that sufficient security measures should have been taken.

The result of vulnerability scanning using Nessus (August 2015) is described below.

The security holes detected are categorized into “Critical”, “High”, “Medium” and “Low”. “Medium” and “Low” security holes are substantially negligible ones.

We found 9 “Medium” security holes and one “Low” security hole. We could not find “High” or “Critical” security hole. No critical or major vulnerability found on the website. We could summarize that MCIT website ware relatively well managed.

Note: There are no test site for website of MCIT, so we assessed the webserver under operation. Therefor vulnerability scanning tool was used as “safe-mode” to prevent the damage to the web

service operation. Therefore we could not to test all the known vulnerability on the server.

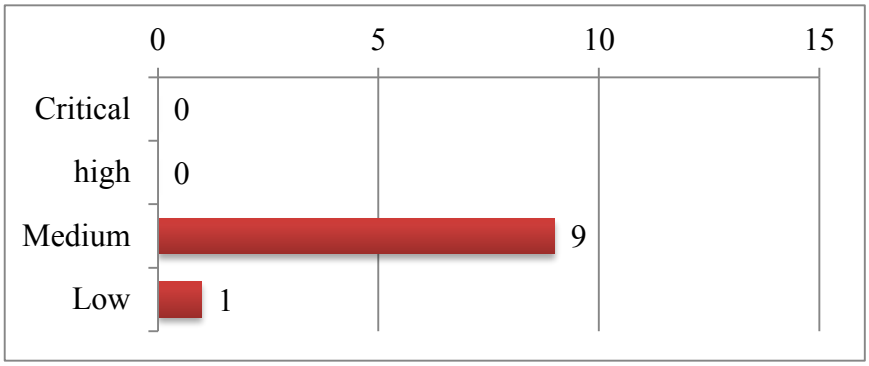


Figure 5.3-2 Vulnerability Scan Result of the webserver

The 7 out of 9 “Medium” vulnerabilities and one “Low” vulnerability are related to SSL version or SSL Certificate. This is not desirable but we don't say that there is high risk at this time. One of the rest of “Medium” vulnerabilities is related to PHP version disclosure, and the other is related to clickjacking vulnerability. Both of vulnerability is easy to correspond by setting webserver correctly.
The webserver hosts no confidential information and no complex services. That management of security measures at the operational phase is relatively easy, it can be considered a factor of vulnerability is relatively suppressed.
It is important to manage appropriate operation and maintenance such as patch management for the webserver.

II. Vulnerability Assessment using Interview

The result of vulnerability assessment using interview with manager of MCIT about organizational management system is described below.

- ITCS has no rules, no guidelines and no manuals to operate the website.
- Manager of website is assigned.
- There is no contract document with MPT.
- MCIT do not manage server operational log.
- MCIT backed up the contents of the server.

Many organizational vulnerabilities are found through the assessment. The current major operational problems are:

- Lack of rules, no guidelines and no manuals to operate the website.
- A line of demarcation between ITCS and MPT is not clear.

5.4 Evaluation of Governmental Data Center

5.4.1 Survey Method

Japan Data Center Council has formulated the Data Center Security Guidebook for data center operators to design and operate data center with appropriate security. The survey team checked standards items for evaluating data center security in Myanmar based on it with the council and studied below items related to quality, reliability and availability of data center.

Table 5.4-1 Data Center Survey Items

	Item	Contents
1	Security gate	Function as means of access control and permission
2	Rack	Heat flow composition, quake resistance, access control
3	Access control	Control items and recoding function
4	Identity authentication	Authentication method of individual to be authenticated
5	Image surveillance	Surveillance system composition
6	Fire detection	Fire detection system and prediction systems
7	Intrusion detection	Intrusion detection sensor
8	Integrated management	Introduced or not, system configuration
9	Network security	Introduction and configuration of various device to take measures
10	Locational condition	Conditions against natural disaster, electricity and other infrastructure development
11	Business continuation	Budget allocation, workforce and staff skills

Source: Produced based on Data Center Security Guidebook

Items in the above table were arranged into physical areas below to sort out items to be allocated in each area.

Table 5.4-2 Data Center Survey Area and Place

	Area	Place
(1)	Premises area	Gate
		Fence
(2)	Entrance area	Front entrance for visitors
		Entrance for carried-in and out equipment
		Entrance for employees
		Building windows and exterior wall
(3)	Inspection area	Baggage screening room
(4)	Shared area	Office
		Server room

(5)	Critical area	Rack
		Critical equipment room
(6)	External area	Location

Items were evaluated based on field survey and interview with the managers.

5.4.2 Survey Outline

Survey Target: MCIT S-12 building Fl.1
Survey Place: S12 Exchange Building, Naypyidaw, Myanmar
Survey Date: August 4 and 5, 2015
On-site handling: Tint Khine (MCIT IT Department, Second Assistant Engineer)

5.4.3 Survey Results

I. Premises area

The gate was lockable and sufficiently robust and tall to prevent unauthorized entry and security guards are assigned around the clock in three shifts for access control. However, no crime prevention system or intrusion detection system is installed for the fence and thus the anti-intrusion measures in the area is not sufficient.

Figure 5.4-1 Gate

Figure 5.4-2 Security guard post

II. Entrance area

Security camera surveillance measures against entries on the premises area are taken. However, no measure against entries in buildings, which include setting up visitor reception desk, is taken and thus both data center visitors and visitors to other offices in the building can have access. This enables accompanied entry, intrusion of unwanted people and destruction for intrusion.

Figure 5.4-3 Outdoor surveillance camera

Figure 5.4-4 Building entrance

III. Inspection area

There is no baggage screening room and it enables unauthorized intrusion, accompanied entry and carry-in of unwanted items as in the case of the entrance area.

Figure5.4-5 Entrance in Building

IV. Shared area

Although the office area is set up, a UPS is installed and network camera is monitored in the server room, there is no access control system for the area and this enables unauthorized entry. The power supply cable from the UPS to server room is exposed and its destruction may cause suspension of power supply in case of power outage.

The server room is equipped with an image surveillance system, a fingerprint authentication entry control system, and a fire detection system and a fire prediction system is planned to be installed. The fingerprint authentication prevents outsiders from entering the facility alone as the registration is limited to relevant members. However, there are possibilities of accompanied entry and unauthorized use of information with no entry rules or entry count system.

Figure 5.4-6 Server room entrance (fingerprint authentication)

Figure 5.4-7 Office entrance

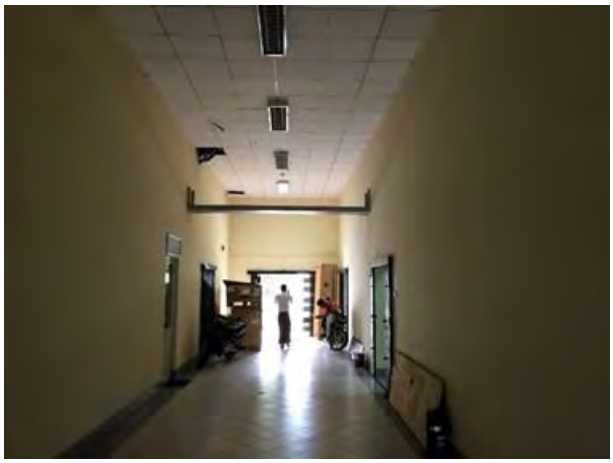


Figure 5.4-8 UPS power supply cable

V. Critical area

Although the unauthorized operation of the rack is monitored by the image surveillance in the server room, the rack door lock is not controlled and it enables unauthorized operation of device installed on the rack. Other critical device and equipment with the capacity to satisfy the demand of air conditioning and measures against power outage are installed.

As no ADS or IDS/IPS is installed for the network security and no measure for inside the OS is properly taken, there is a risk of attack via the network.

*No photographs as photography is prohibited in the room.

VI. External area

A 380V special cable is installed separately from the general power cable next to the power substation for power source duplexing to secure power supply. In case of power outage, the special line will be used and two power generators are installed on the premises to be prepared for further risks. As for the

location, there is a risk of intrusion from outside because it is situated in front of a relatively wide two-way two-lane street and it is easily accessible from outside. However, no damage by flood, earthquake or fire has been caused since the building became in use in 2005, which suggests that it is located in an area with a low risk of natural disasters.

Figure 5.4-9 Distribution line (2 system)

Figure 5.4-10 Emergency power generator

5.4.4 **Evaluation**

As for the data center quality, access control measures for the entrance and inspection areas are necessary as the measures against intrusion on the premise are not sufficient although they are sufficient against intrusion from outside. Although power supply measures are taken with careful consideration, there is concern over the disconnection of UPS power supply by unauthorized intruders. It is necessary to introduce access rules and rack locking control against accompanied entry and unauthorized operation of information device.

As for the data center reliability, unauthorized operation via the network is the biggest concern because of insufficient network security measures. Although network camera monitoring is carried out against unauthorized operation of information device by unauthorized intruders, there is insufficient awareness of security in the office area and thus more institutional efforts also need to be taken.

As for the data center availability, it is not sufficient enough to be reliable as measures against unauthorized intrusion and destruction are insufficient although no damage has been caused by disasters, etc.

The target data center is deemed to be operated stably as no serious accident has been recognized. However, there are concerns as pointed out above and safe operation will be guaranteed when they are eliminated.

5.5 Other Security Enhancement Facility in Government

In Myanmar, KOICA was leading assistance on e-government masterplan development in 2000 – 2010, was pushing development of e-government in Myanmar. As part of it, for cybersecurity related facility, development of PKI have been conducted in 2006.

However as of now, the use of PKI seems very limited because Myanmar ICT environment began to develop only a few years ago and people still in poor network environment or almost no e-government application provided to public. To accelerate PKI in future, it is important to consider the use case without personal terminal such as IC card.

5.6 Security Measures Taken by Telecommunications Carriers

The Survey Team conducted an interview survey on security measures taken by telecommunications carriers in Myanmar at local communications carriers, RedLink and Yatanarpon Teleport.

5.6.1 Security Measures

1) RedLink Communications

RedLink provides Internet access to its clients. It does not provide a hosting service or server space to the clients. Therefore, its practical security measures are mainly for the protection of its network and basic measures such as the installation of firewalls and the management of access permissions list and users are used for this purpose. Clients who wish to have additional security measures are to take such measures as the installation of an additional firewall by themselves. Password and encrypting systems (at the level of those provided by Microsoft) are used for the handling of important documents and files as a security measure in the business operation.

The network of RedLink was affected by a large-scale DDoS attack approximately three years ago. It was not possible to identify whether the source of the attack had been in a foreign country or in Myanmar. While minor attacks have been made on the network, a serious attack which could have shut down servers has not been made on it. While attacks have been made on its website, they have not caused any serious problems.

RedLink is aware of the importance of cyber security. However, as it has to focus on the network operation at present, it has not been able to establish a team specialized in IT security. Although the company has appointed persons in charge of security, their duties are limited to the configuration of the firewalls, detection of attacks and protection of servers and it is hard to find a person specialized in cyber security in Myanmar.

RedLink has an IT security policy, which is not compliant with ISO 27002. Since the government has not presented a framework concerning IT security, the company formulated the policy independently. RedLink cooperates with mmCERT in the provision and exchange of various information.

2) Yatanarpon Teleport

Yatanarpon Teleport provides not only Internet access but also services including a hosting service at its data center. Although it has established a department responsible for security measures as a new department, it is aware of the lack of technical specialization of the department and the need to accumulate experience in taking security measures. The company is very well aware of the importance of security. However, in reality, it does not have either the human resources or the time to take sufficient security measures because both its human resources and work time are used for daily business operation and customer relations. Nor does the company have extra funds to invest on very expensive security and anti-DDoS equipment.

A large-scale DDoS attack was made on the system of Yatanarpon Teleport in 2010. While its system has a function to detect certain attacks at the router, it does not have a mitigation system against cyber attacks. The only protection available is that by firewalls. While this protection system is protecting the server group, it is not able to protect the networks of its clients.

While the government operates websites using the hosting service of Yatanarpon Teleport, the government has not made a special request on the security of the sites. As the government has not enacted a law or published guidelines on cyber security, Yatanarpon Teleport has developed its own cyber security policy. The company is providing its services in accordance with the policy. Also it does not have SLAs with its clients.

Yatanarpon Teleport has formulated a simple security policy on the installation of servers and firewalls and the use of the hosting service. The policy includes such practical measures as closing of unnecessary ports and control on access to external systems. The company installed an access-logging server in its system and the above-mentioned new department for security measures is monitoring the accesses with this server. If an abnormality is detected, the clients will be notified. The company also owns a DPI (deep packet inspection) device. When this device detects an abnormality in a network of a client, the client will be notified of it.

5.6.2 Problems Faced by the Telecommunications Carriers

The expansion of the mobile communication services began in Myanmar approximately two years ago after the government had opened up the communication market and the number of Internet users began to increase with the expansion of the service. As the government has been promoting the development of e-Government taking advantage of this situation, the importance of cyber security has been increasing. However, Myanmar does not have a legal system or framework including guidelines on cyber security. There is no rule at all concerning where a carrier shall report an IP address of an attacker who made a cyber attack on its system even if the carrier has managed to identify the address. Cooperation among communications carriers plays an important role in reinforcing cyber security. However, the existing cooperation between the carriers is not sufficient. While mmCERT is functioning as a place for the communications carriers to offer and share information on security, those carriers have to have certain basic standards (including a common policy) to reinforce cyber security. Against this background, the government is required to develop a legal framework on information

security, protection of personal information, data protection and cybercrimes urgently.
Myanmar has a problem in the human resource development in cyber security. As there has been little cooperation between the academia (universities) and the private sector at present, there is a large gap between what the private sector needs and what is taught in universities. This gap is particularly large in cyber security. As even graduates of colleges specialized in computer science have little knowledge of cyber security, communications carriers have to train their employees on it. The human resources in cyber security will have to be developed in a public-private-academia partnership.

5.7 Security Measures of Central Bank System

Modernization of the financial sector is in progress in Myanmar. However, many business procedures including fund settlement between the head and branch offices of the Central Bank and between it and commercial banks have yet to be computerized and security measures with the modernization in view are insufficient although limited measures are implemented. While the independence and enhanced function of the Central Bank and introduction of electronic payment and other business systems there are of urgent need to participate in international economic activities, its work business efficiency improvement is in progress also for smooth and steady implementation monetary policies.
Against the backdrop, JICA is implementing the *Project* for Development of *ICT System* for *Central Banking to improve the work system of the bank*. It is implemented as system security measures based on the recognition and concept listed below.

- No security standards are formulated in the financial sector in Myanmar and its necessity is recognized.
- All information has been considered confidential because of its institutional background and important assets need to be defined first in thinking security measures of asset management.
- Security guidelines are formulated in the Project in accordance with the ISMS and based on ordinary business operation.
- Internet connection is not an assumption of the system and thus there is little concern over Internet security. However it is also important to raise its awareness.
- The Ministry of Finance also needs a system of coordination and reflection in policies as supervisory guidelines as the supervisory agency.
- The Administration and IT Department (AITD Central Bank) with approx. 40 workforce is in charge of the system in the Central Bank. Although it has an internal audit section for system defense, it has no system surveillance function.

With the recognition of the need for the definition of important assets and formulation of guidelines based on their operation as well as the improvement of sections in charge as the preposition of security measures, there is a plan to carry it out in cooperation with the partner country.

5.8 Trend and Needs of Private Sector

Although some private foreign companies provide cyber security services for telecommunication operators, no Myanmar-based company provides such services as its main services. Although Myanmar private companies recognize the threat against cyber security, they are just feeling the potential of the countermeasures working as profitable business. Private foreign companies see the current cyber security situation as a business opportunity and Microsoft Corp. and many other companies call for the need for such measures.

Meanwhile, domestic IT companies, particularly telecommunications operators, continue to grow rapidly supported by the recent institutional reform and deregulation. However, the growth of system integrators, software companies and other peripheral business operators is lagging behind and the scale of the sector is smaller than other countries. Security measures of such business operators themselves are also insufficient and they cannot guarantee the security of services they provide.

The conditions for emergence of business operators that ensure cyber security have yet to be developed. Against the backdrop, the survey team conducted interview with Myanmar-based IT companies about the industry in the country and sorted out what the private companies expect the government as summarized below.

- Employment of students who majored in IT is difficult. Although a substantial number of students with expertise knowledge graduate, excellent human resources find employment in Singapore and other foreign countries and the remaining are employed by non-IT companies. As a result few students are employed by Myanmar-based IT companies. The government is expected to develop a policy to promote such human resources to be employed by domestic IT companies.
- The government is expected to increase investment in IT to promote its vitalization.
- It is important to promote more competition among private companies when the public sector procures IT assets. The competition of technical standards and specifications will also vitalize the IT sector.
- Registration fees incurred for company establishment are also barriers against starting an IT business. It does not require a substantial amount of initial investment and involves little risk and entrepreneurs pay it all with their own fund. A scheme of getting a bank loan to contribute to IT companies will promote starting a business.
- Many small IT companies were started within the last one year as a result of economic growth and improvement of communications infrastructure. The government is expected to further improve such an environment and conditions.
- Development of legislation is behind the technological development and it acts as a barrier against project implementation. It is important for the government to review laws again for computerization of government procedures.
- Some ministries and agencies have no IT use or cyber security policies in the introduction of e-Government. There is also a problem of the lack of integrated framework among them. The

government is expected to formulate and integrate them.

The survey team also listened to requests for promotion of IT sector and specific demand related to IT projects. The priority issue is to develop a system to utilize private companies in view of the formulation of policies among ministries and agencies within the government to promote cyber security measures and vitalization of IT sector.

Chapter 6 Consideration of Cyber Security Issues and Countermeasures

In this chapter, cyber security issues extracted from chapter 4 and 5 are sorted out and countermeasures corresponding to the issues will be described. Problems and issues in the sector of government, critical infrastructure, private company and citizens are described in the following figure. Issues in each sector need countermeasures categorized as development of laws, standards and guidelines, enforcement of organization itself, functional enforcement of each related organization, collaboration enforcement and awareness raising for the whole level of cyber security countermeasures. The following figure shows the relationship between the issues and countermeasures as well.

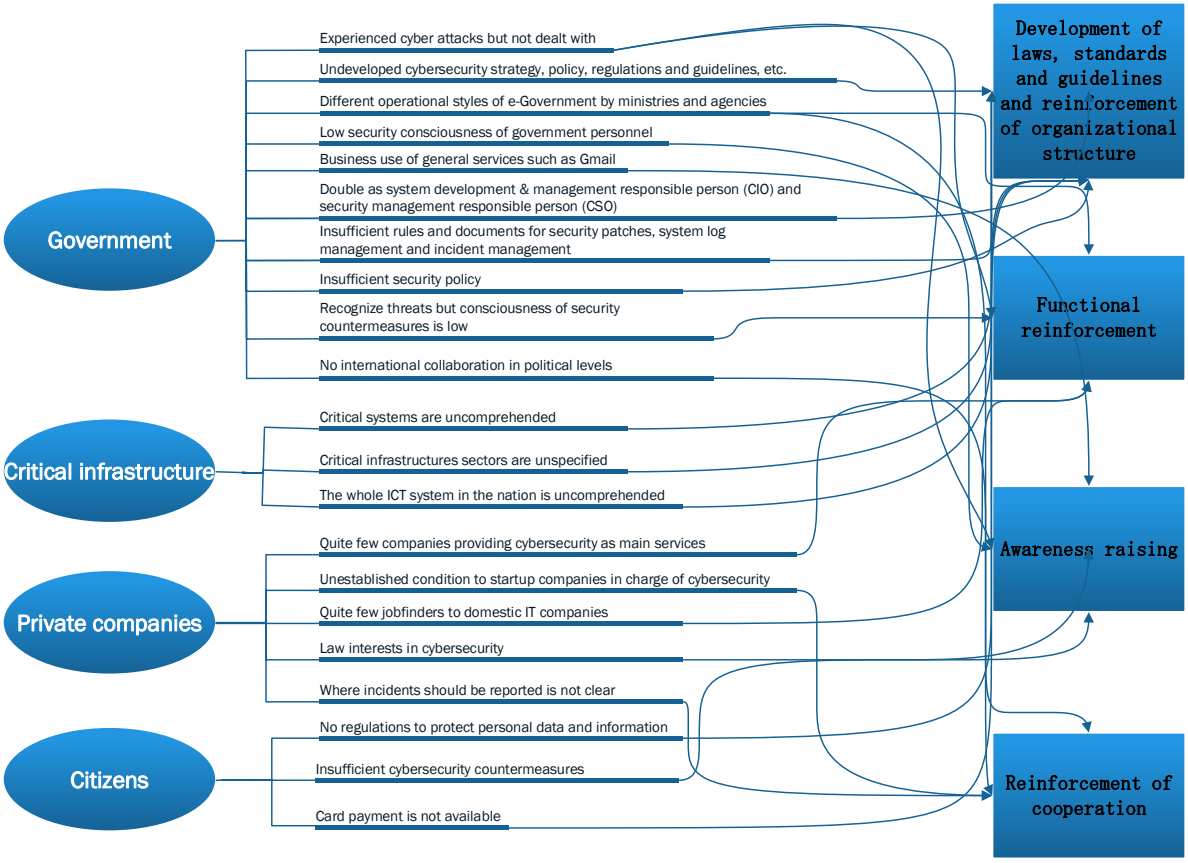


Figure 6-1 Relationship between the Issues and Countermeasures

Although the categories are different from the draft Action Plan drafted in 2015, the categories target government, critical infrastructure, private companies and citizens and the subjects are same as the draft Action Plan. Since the countermeasures should be executed cross-sectional subjects or depend on the former countermeasures executed and cannot be executed plural, they are assorted in the categories above.

6.1 Cyber Security Countermeasure Issues of Government Cyber Security Countermeasure Related Organization, Government Organization and Related Organization

6.1.1 Development of Laws, Standards and Guidelines and Reinforcement of Organizational Structure

According to "4.5 Activities of Government Organizations in Charge of Security Measures," efforts of the Electronic Government have been started since the beginning of 2000. However there are no guidelines and guidance to introduce the Electronic Government provided, there are still large anxieties to introduce and utilize the Electronic Government in the ministries considering to introduce the Electronic Government. There are many ministries which are using colocation services provided by MPT, however standards related security and detail procedures have not been provided.

Since cyber security attacks against critical infrastructures affects the life of citizens and critical infrastructures assume to be targeted from other countries, definition and subjective sectors are not yet specified in Myanmar.

The usage of internet and portable terminals is high rocketing, although guidelines objected literacy education targeted civil usage and personal data protection legislations are not established.

As for the issues in the governmental organization, inventory making, arrangements and management of information assets and risk assessments are not practiced. Security incidents and best practice of cyber security countermeasures are not shared among ministries. There are no organization and environment to monitor the Electronic Government and Web application established. NCSC staff within IT&CS are not sufficiently prepared. CSO is not assigned in each ministry or even the ministry it is assigned, CIO holds its position concurrently and separation of responsibilities is not clarified between CIO who promotes to develop information system and CSO who check and audit information system from the view of cyber security. As for the information communication related organizations, roles of MCIT and MPT are not clearly separated at this point.

6.1.2 Functional Reinforcement

It's free to enter information system room in each ministry and monitor function is not properly operated and physical countermeasure is not implemented. There are different levels of technical countermeasures implementing and operating FW, IPS/IDS, anti-virus software and filtering software among ministries. As for the electronic commerce, corresponding to international standards has not been started yet.

There are few human resources who have incident detection and analysis skills in government organization in charge of cyber security measures. No programs for cyber security human resource development are provided and no facilities for periodical training are established. So CSO capacity building in each ministry and human resource developing for cyber security team lead by CSO are necessary. Ensuring similar skillful human resource in critical infrastructures and private companies will be an issue in near future.

6.1.3 Collaboration Reinforcement

Since critical infrastructure sectors are not specified yet in Myanmar, information sharing and reporting systems are not established. Since private companies don't develop in-house CSIRT, when some incidents happen within the companies, contact and report systems with mmCERT are not established.

There are few political level of international collaboration. As for the international issue, information are mainly provided from APCERT or JPCERT/CC but still quite few inputs are provided from mmCERT.

6.1.4 Awareness Raising

Although the cyber security mind of director level personnel in each ministry is quite high, most of the personnel who don't use or are limited to use PCs have very low cyber security literacy and don't consider about cyber security.

Since executives of private companies and information system personnel have law cyber security mind, seminars and trainings are not frequently practiced even when security personnel are interested in.

6.2 Cyber Security Countermeasures for Each Issue

Cyber security countermeasures for each issue in 6.1 will be described in the following table.

Table 6.2-1 Cyber Security Countermeasures

Large Category	Small Category	Measures	Contents
Development of laws, standards and guidelines and reinforcement of organizational structure	Laws, standards and guidelines, etc.	Formulation of baseline standards on cyber security for the use of e-Government	MCIT provides baseline standards on cyber security for the use of e-Government to each ministry.
		Formulation of a practical rule on the use of web applications (including the use of homepages of government ministries and agencies)	MCIT drafts and provides a practical procedure, security standards and some rules on the use of web applications to each ministry and agency.
		Identification (definition) of the critical infrastructure sectors appropriate for Myanmar using that of other countries as reference and formulation of "Safety Standards" which stipulate the level of cyber security measures in each of the critical infrastructure sectors	National Cyber Security steering Committee identify (specify) the critical infrastructure sectors appropriate for Myanmar using that of other countries as reference.
			MCIT drafts guidelines of "Safety Standards" which stipulate the level of cyber security measures in each of the critical infrastructure sectors.

Large Category	Small Category	Measures	Contents
			Guidelines of “Safety Standards” which prescribe the level of cyber security measures in each of the critical infrastructure sectors are prepared.
		Enactment and enforcement of the Personal Data Protection Law for the regulation on the use of smartphones and mobile banking used by an increasing number of people	MCIT enacts and amends Telecommunications law 2013. (Personal Data Protection Law should be discussed in other part.)
		Enactment and enforcement of cyber security related laws	MCIT arranges Cyber Security Basic Law and Illegal Access Prohibition Law.
		Development of cyber security guidelines by an association of communications carriers in accordance with the standards of MCIT	Based on cyber security guidelines of MCIT, industry groups draft cyber security guidelines.
	Development of organizational structures	Development and operation of a framework for information sharing between government ministries and agencies	Each ministry and agency identifies the personnel in charge of cyber security. MCIT establishes periodical information sharing system and conducts the role as a secretariat.
		Development of an organizational structure (including human resource development) in GSOC, an organization to monitor e-Government systems and web applications of all the government ministries and agencies 24 hours a day, and an environment for its work	MCIT ensures human resource development for operating GSOC and establishes environment to monitor e-Government systems and web applications of all the government ministries and agencies 24 hours a day.
		Employment of a sufficient number of security personnel required by MCIT (National Cyber Security Center and mmCERT, in particular)	MCIT rapidly ensures a sufficient number of security personnel required by MCIT (National Cyber Security Center and mmCERT, in particular).
		Appointment of CSOs in government ministries and agencies and demarcation of the duties of CSOs and CIOs	Each ministry appoints CSO and CIO. Government ministries and agencies segregate the duties of CSOs and CIOs (Separation of duties).
	Job sharing	Organizational reform in the communication sector	Roles of MCIT and MPT should be clearly specified.

Large Category	Small Category	Measures	Contents
		Development of an inter-ministerial and inter-agency cooperation system led by MCIT	MCIT establishes an inter-ministerial and inter-agency information report and sharing committee organization.
		Reinforcement of intergovernmental cooperation	MCIT develops collaboration mechanism to collaborate with political level National CERT as POC (Point of Contact).
Functional reinforcement	Improvement of equipment and applications	Reinforcement of the physical measures on information systems in government ministries and agencies	MCIT leads each ministry and agency to implement biometric identification function, entering and leaving management function and surveillance camera system.
		Reinforcement of the technical measures on information systems in government ministries and agencies	MCIT leads each ministry and agency to implement and operate properly Firewall, IPS/IDS, anti-virus software, and Proxy server, mail filtering, authentication system, log management and encryption.
		Implementation of control system security and e-commerce security measures on the assumption that the global standards such as IEC62443 and PCIDSS is to be introduced	Global standards such as IEC62443 and PCIDSS are introduced to promote future energy management system and credit-card payment.
	Human resource development	Reinforcement of the capacity to detect and analyze incidents on the government systems	MCIT periodically conducts trainings for capacity building to detect and analyze incidents on National Cyber Security Center, mmCERT, and CSOs and cyber security teams of ministries and agencies.
		Reinforcement of the capacity to detect and analyze incidents on critical infrastructure	Ministries in charge of critical infrastructures periodically conduct trainings for capacity building to detect and analyze incidents on critical infrastructures based on the standards drafted by MCIT.
		Reinforcement of the capacity to detect and analyze incidents on private companies	Industry group periodically conducts trainings for capacity building to detect and analyze incidents on private companies
		Training of CSOs of government ministries and agencies and human resource development for the cyber security teams led by CSOs	MCIT leads government ministries and agencies to draft cyber security policy, to conduct cyber security assessment and audit cyber security periodically, and to

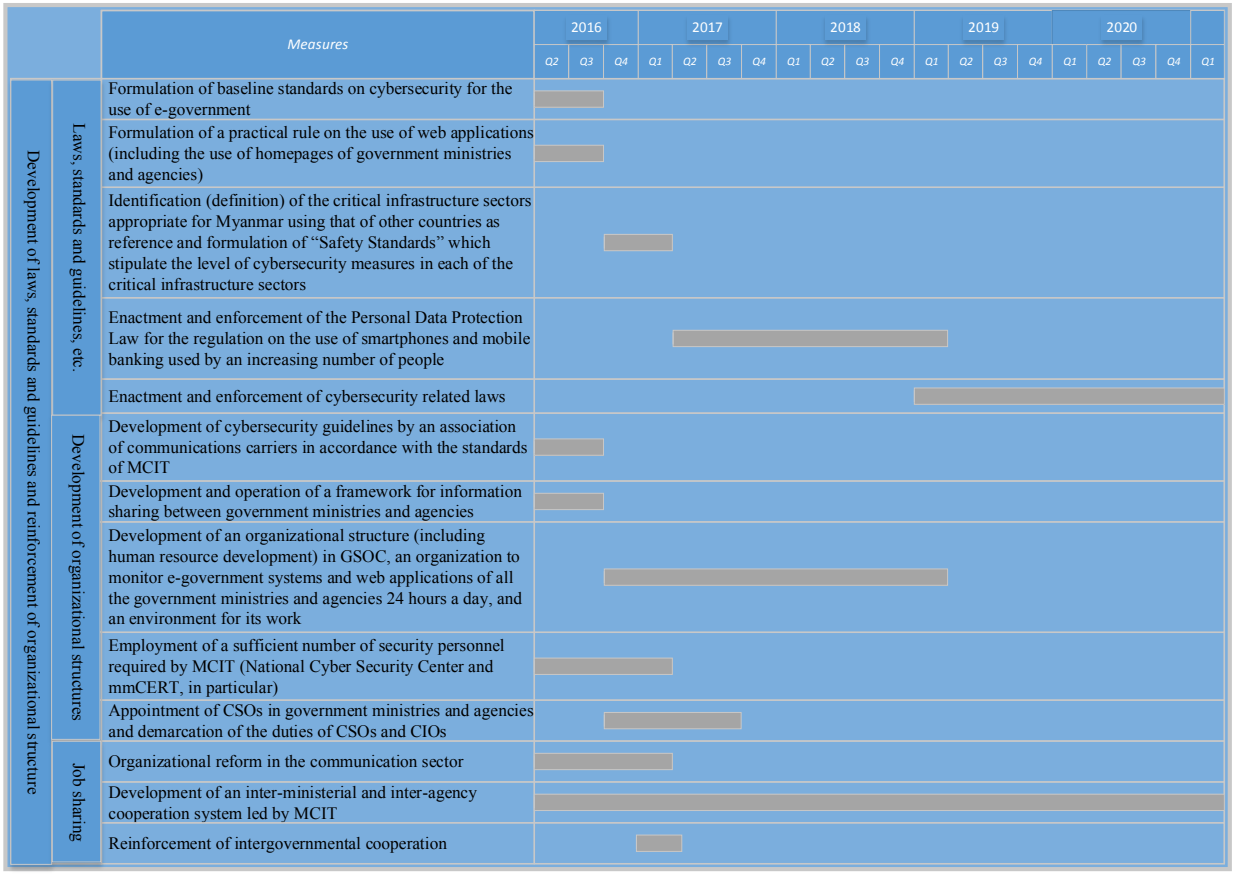
Large Category	Small Category	Measures	Contents
			evaluate and report cyber security.
		Implementation of training and practices on cyber security including those through international cooperation for the human resource development in cyber security	MCIT arranges to conduct training for cyber security resource development and cyber exercises with the collaboration of foreign cyber security related organizations.
		Quantitative and qualitative improvement of the human resources in cyber security through the cooperation with universities, graduate schools, research institutes and computer-related private organizations (including MCF, etc.)	・Establish information sharing and communication committee ・Startup governmental scheme to promote personnel exchange from universities, graduate schools, research institutes and computer-related private organizations (including MCF, etc.) ・Promote to advance computer engineers status
		Development of teaching contents	MICT develops human development program and online teaching contents against all the personnel in the government.
Reinforcement of cooperation	Domestic cooperation	Development and operation of a mechanism for information sharing and communication on the security of critical infrastructure	IT&CS develops and operates a mechanism for information sharing and communication on the security of critical infrastructure as a secretariat.
		Development of a communication mechanism between CSIRTs of individual companies and mmCERT	mmCERT provides CSIRT development guideline and tools to spread internal CSIRT within general companies and reinforces contact & reporting system and emergency response system.
	International cooperation	Sharing and utilization of the information of the best practices in other countries	MCIT collects the information of best practices in other countries and share timely information within government
		Development of the foundation for information security through international cooperation	MCIT guides to establish information security infrastructure to utilize political level of international collaboration with National CERT/CSIRTs in ASEAN countries.

Large Category	Small Category	Measures	Contents
Awareness raising		Awareness raising activities for all government personnel	Awareness raising program to raise the level of the cyber security literacy of all personnel in all governments and agencies.
		Implementation of cyber security related awareness raising activities for executives and person in charge of information systems of private companies	Awareness raising activities based on ISO/IEC27014 (Information Security Governance) should be recommended for government procurement condition and cyber security personnel demands promotion.
		Implementation of awareness raising activities to improve awareness of cyber security and improvement of cyber security literacy	Cyber security awareness raising contents for citizens to use smartphone safely should be developed and promoted for diffusion.
		Reinforcement of the capacity to implement cyber security countermeasures of government ministries and agencies	MCIT periodically conducts awareness raising activities of cyber security countermeasures against all ministries and agencies.

6.3 Order of Countermeasures

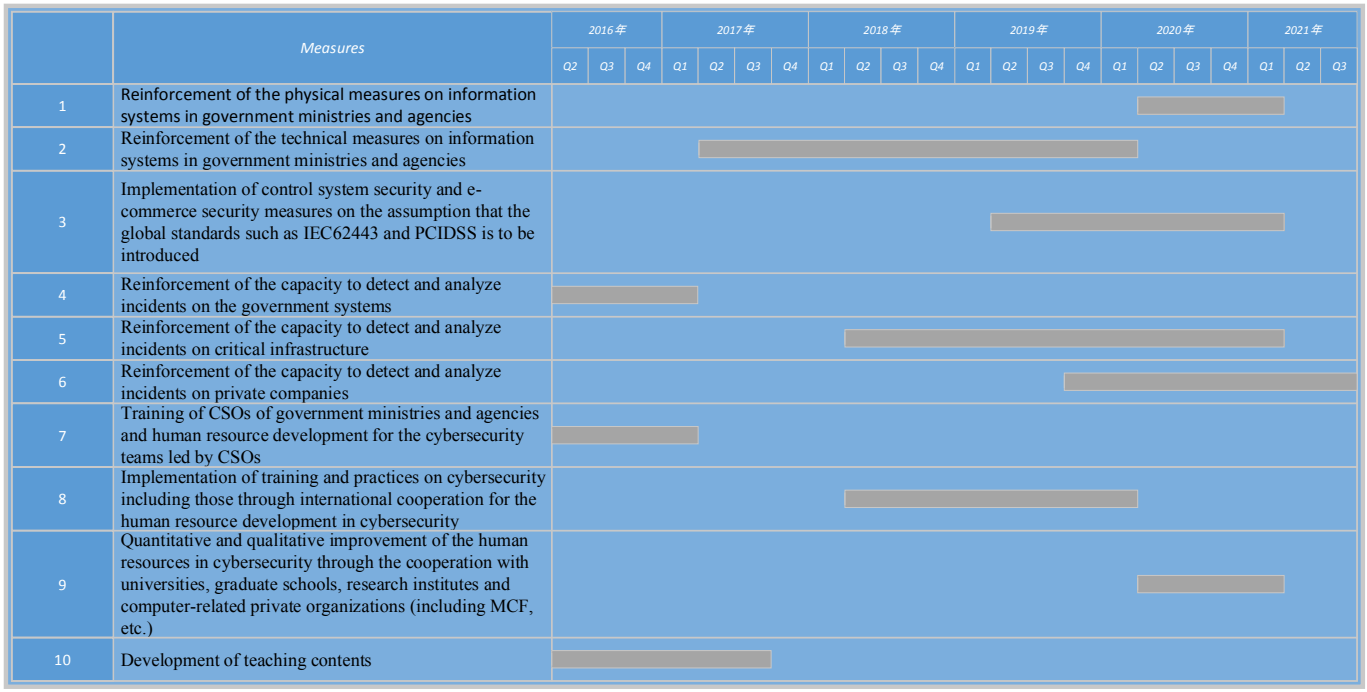
Considering importance and urgency in Myanmar, order of countermeasures is described in the following roadmap arranged by the large category. Drafting elementary guidelines and regulations and developing cross-agency common framework will promote secure utilization of g-Government, clarify the responsibilities within the government and establish the structure to proceed cyber security monitoring and countermeasures.

Table 6.3-1 Roadmap of Development of Laws, Standards and Guidelines and Reinforcement of Organizational Structure



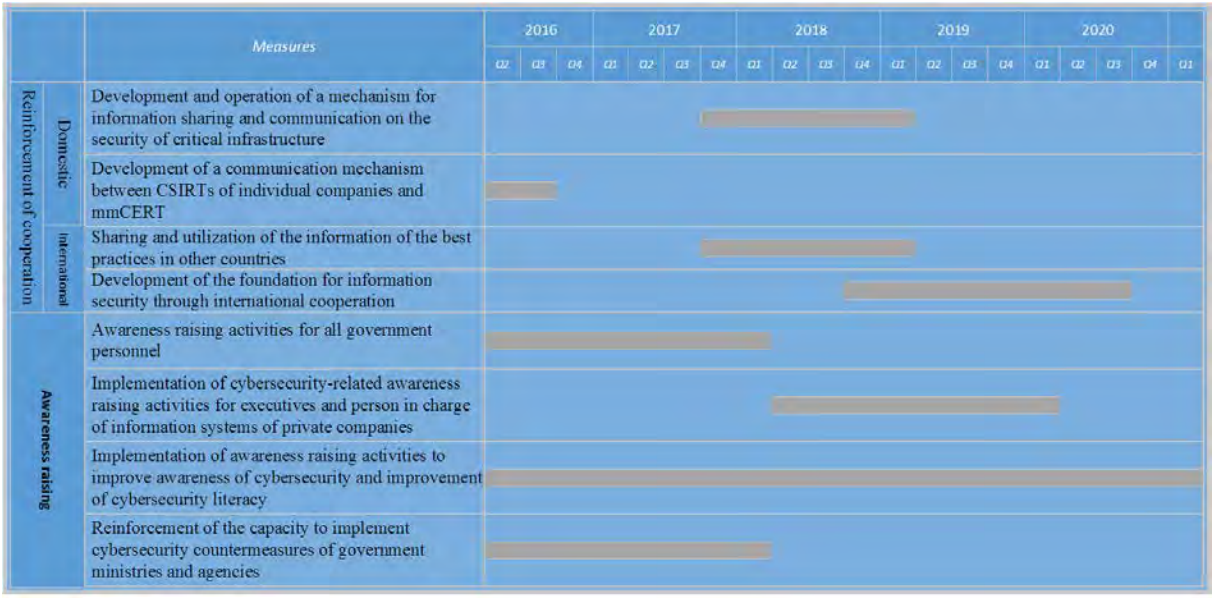
The whole government capability is enforced by proceeding the development of educational material contents in parallel with reinforcing incident detection and analysis skill of government system and human resource development for cyber security team of each ministry and agency. After the preparation of human resource development, physical and technical measures of government information system and devices and application environment compliant to international standardization should be reinforced.

Table 6.3-2 Roadmap of Functional Reinforcement



CSIRT related organization, critical infrastructures, domestic collaboration by government and international collaboration should be reinforced in the middle and long term. Awareness raising against whole personnel of government and whole citizens should be started as soon as possible and continued.

Table 6.3-3 Roadmap of Reinforcement of cooperation and Awareness Raising



Chapter 7 Study on the Contents and Priorities in Japanese Assistance

7.1 Policy on the Study on Assistance Measures

The terms of reference (TOR) of this survey describe the importance and urgency of the measures, the maintenance capacity and development problems of the recipient and the relative advantage of Japan on the measures as the important points in the study on the contents of the Japanese assistance. TOR also stipulates that, if infrastructure development is an assumption for the implementation of the assistance, this assumption is also to be studied.

Therefore, the study on the contents of and priorities in the Japanese assistance was carried out in accordance with the following policies. Each of the cyber security measures recommended for the implementation in Myanmar studied in Chapter 6 was evaluated on the six criteria mentioned below and a study was conducted on which ODA scheme could be used for the implementation of each of those measures. Then, the relevance of implementing each of those measures in an ODA scheme was evaluated. As implementing each measure which complied with the six criteria mentioned below as an independent assistance project was expected to be inefficient use of the assistance, a study was conducted on the possibility of implementing multiple measures in a single project in the study for the formulation of practical assistance projects.

As there was no assistance measure requiring infrastructure development as an assumption for its implementation, this assumption was not included in the criteria of the study. It is also to be noted that the Deputy Minister of Communication and Information Technology made a comment on this Project to the Survey Team while the team was conducting the field survey. In this comment, he expressed his concern that the state of the ICT sector might have been changed drastically from the current state by December, when the final report of this survey is scheduled to be submitted, as the ICT-related markets are growing very rapidly and, based on this concern, requested the project to be commenced in near future and the assistance to be provided for short-term rather than long-term goals.

I. A measure to be assisted should be a cyber security measure of great importance

Cyber security measures which were expected to have positive impact on the society, and the implementation of other measures during the systematic development of cyber security measures were selected as components of the assistance.

II. A measure to be assisted should be a cyber security measure of great urgency

Cyber security measures which should be taken in early stages in the systematic development of cyber security measures were evaluated. The measures which were stipulated to be implemented in early stages in the timeline for the implementation of assistance measures described in Chapter 6 and which, if not implemented, could delay the progress of other measures were selected as components of the assistance.

III. A measure to be assisted should be a measure which cannot be implemented independently by Myanmar because of their lack of experience and knowledge in cyber

security

Cyber security measures which could not be implemented by Myanmar with its current technical capacity were selected as components of the assistance. In this analysis, not only the technical capacity of individual engineers but that of the counterpart organization including whether or not the organization has the human resources required for implementing those measures, were taken into consideration.

IV. The implementation of a measure to be assisted should not interfere with the sustainable implementation of cyber security measures by Myanmar

Cyber security measures that Myanmar had already begun to take, those that Myanmar should take with its own initiatives and those that Myanmar was expected to become able to take independently after the completion of the assistance were studied so that Myanmar would not become overly reliant on assistance from foreign countries and donor organizations in future.

V. A measure to be assisted should be a measure in an area where Japan has an applicable technology

Cyber security measures in the areas mentioned below were selected as components of the assistance: 1) the areas where the similar mechanisms, policies, plans and organizational structures had already been developed and used in Japan and successful cases of their use in Japan could be emulated in Myanmar with the current state of Myanmar and 2) the areas where the competitiveness of equipment manufactured and solutions developed in Japan is extremely high in the global market.

VI. Policy on the Study on the Use of ODA Schemes

An analysis was conducted on the applicability of the ODA schemes of Japan including Technical Cooperation, Grant Aid Assistance and ODA Loan to the implementation of the cyber security measures. Measures which should be implemented by Myanmar and those that Myanmar already had technical capacity to take and was expected to acquire technical capacity to take in future were excluded from the assistance so that not all the measures were to be implemented with the ODA assistance and sustainability of the measures was to be established. A study was also conducted on the possibility of implementing multiple measures in one project, in addition to the applicability of the schemes.

7.2 Study on the Assistance Plan

7.2.1 Evaluation with the Policy on the Study on Assistance Measures

The Survey Team evaluated the assumed cyber security measures mentioned in Chapter 6 on the criteria in the policy on the study on assistance measures described in section 7.1. The result of the evaluation is shown in Table 7.2-1. The necessity for the implementation of each measure evaluated on the basis of the study policy is described in the column of ‘Remarks’ in the table.

Table 7.2-1 Results of the evaluation of cyber security measures assumed for the implementation in Myanmar with the policy on the study on the assistance measures for the Japanese assistance

No.	Purpose	Subject	Measure	Importance[1]	Urgency[2]	Lack of experience and knowledge in Myanmar[3]	Interference with the sustainability[4]	Applicable technologies[5]	ODA scheme[6]	Remarks
1	Development of laws, standards and guidelines and reinforcement of organizational structure	Laws, standards and guidelines, etc.	Formulation of baseline standards on cyber security for the use of e-Government	◎	◎	◎	◎	◎	TC-A	Security standards for e-Government will be the basis of the operation of e-Government. The formulation of the standards is urgently required as the development of e-Government is in progress.
2			Formulation of a practical rule on the use of web applications (including the use of homepages of government ministries and agencies)	◎	◎	◎	◎	◎	TC-A	Government organizations will distribute public information through their websites when the development of e-Government has been completed. The formulation of the rule is urgently required for the safe operation of these sites.
3			Identification (definition) of the critical infrastructure sectors appropriate for Myanmar using that of other countries as reference and formulation of "Safety Standards" which stipulate the level of cyber security measures in each of the critical infrastructure sectors	◎	◎	◎	◎	○	TC-A	It will be impossible to take cyber security measures on critical infrastructure without identification of critical infrastructure.
4				○	○	◎	◎	○	Myanmar	It will be necessary to prepare guidelines for the formulation of safety standards appropriate for Myanmar after the identification of the critical infrastructure mentioned above.
5				△	△	◎	◎	○	Myanmar	It will be necessary to formulate safety standards appropriate for Myanmar after the identification of the critical infrastructure and the preparation of the guidelines mentioned above.
6			Enactment and enforcement of the Personal Information Protection Law for the regulation on the use of smartphones and mobile banking used by an increasing number of people	○	○	△	△	△	Myanmar	Although this law will be required in future, the priority is on the detailed analysis of the social condition on the use of smartphones, etc.
7			Enactment and enforcement of cyber security related laws	○	○	△	△	○	Myanmar	It will be possible to maintain cyber security by creating standards on cyber security measures first, taking practical measures and, then, enacting and enforcing the cyber security related laws.
8			Development of cyber security guidelines by an industry group in accordance with the standards of MCIT	○	○	○	◎	○	N/A	It will be efficient to develop guidelines which are beneficial to the industry group after the government has completed the development of standards and laws.
9		Development of organizational structures	Development and operation of a framework for information sharing between government ministries and agencies	◎	◎	○ Absence of the implementation capacity	◎	◎	TC-A	There is an urgent need for the sharing of the information required for each government ministry and agency to respond to cyber attacks.
10			Development of an organizational structure (including human resource development) in GSOC, an organization to monitor e-Government systems and web applications of all the government ministries and	◎	○ The priority is on the	◎	○	○	GA-A (in part)	While cyber--incidents have not been fully analyzed in Myanmar, GSOC is to perform an essential role in the response to cyber attacks.

No.	Purpose	Subject	Measure	Importance[1]	Urgency[2]	Lack of experience and knowledge in Myanmar[3]	Interference with the sustainability[4]	Applicable technologies[5]	ODA scheme[6]	Remarks
			agencies 24 hours a day, and an environment for its work		detection of incidents					
11			Employment of a sufficient number of security personnel required by MCIT (National Cyber security Center and mmCERT, in particular)	◎	◎	× A plan already exists.	○	○	Myanmar	Employment of a sufficient number of workers is required more urgently than human resource development.
12			Appointment of CSOs in government ministries and agencies and demarcation of the duties of CSOs and CIOs	◎	◎	○ Absence of the implementation capacity	◎	○	TC-A	Different persons should be appointed as CSO and CIO for the appropriate implementation of cyber security measures.
13		Responsibilities	Organizational reform in the communication sector	◎	○	×	×	×	Myanmar	It is necessary to demarcate the roles of MPT, which is to be privatized, and MCIT clearly and conduct a study on the systems and mechanisms including those for the maintenance of data centers required for cyber security.
14			Development of an inter-ministerial and inter-agency cooperation system led by MCIT	◎	◎	○ Absence of the implementation capacity	◎	◎	TC-A	There is an urgent need for the sharing of the information required for each government ministry and agency to respond to cyber attacks.
15			Reinforcement of intergovernmental cooperation	◎	◎	○	◎	○	TC-A	Cooperation with CERTs in other countries is essential for the analysis of incidents.
16	Functional reinforcement	Introduction/improvement of equipment and applications	Reinforcement of the physical measures on information systems in government ministries and agencies	△	△	△	○	○	Myanmar	Physical measures are effective in maintaining cyber security. However, it is necessary to prepare standards and guidelines on those measures and to study the measures to be taken in accordance with the standards and guidelines before taking those measures.
17			Reinforcement of the technical measures on information systems in government ministries and agencies	○	○	△	○	○	Myanmar	Technical measures are effective in maintaining cyber security. However, as mentioned above, it is necessary to prepare standards and guidelines on those measures and to study the measures to be taken in accordance with the standards and guidelines before taking those measures.
18			Implementation of e-commerce security measures on the assumption that the global standard PCIDSS is to be introduced	△	△	○	○	△	Myanmar	The priority is on the development of various legal systems and guidelines on e-commerce.
19		Human resource development	Reinforcement of the capacity to detect and analyze incidents on the government systems	◎	◎	◎	○	◎	TC-A	The capacity to detect and analyze incidents in the cyber security related organizations in Myanmar is insufficient. Their technical capacity in cyber security has to be improved urgently.

No.	Purpose	Subject	Measure	Importance[1]	Urgency[2]	Lack of experience and knowledge in Myanmar[3]	Interference with the sustainability[4]	Applicable technologies[5]	ODA scheme[6]	Remarks
20				○ Great importance expected in future	○	○	○	◎	GA-B (to be implemented with measures in other sectors)	The facility to be established is for the development of required technical capacity using simulated incidents. There are cases of successful capacity development with similar facilities in Japan. It will be possible for Myanmar to use this facility to develop human resources independently in future.
21			Reinforcement of the capacity to detect and analyze incidents on critical infrastructure	○	△	◎	×	○	Myanmar	This measure is to be taken after the identification of critical infrastructure and the preparation of the guidelines have been completed.
22			Reinforcement of the capacity to detect and analyze incidents of private companies	○	△	△	×	○	N/A	This measure is to be taken after an industry group has completed the preparation of cyber security guidelines.
23			Training of CSOs of government ministries and agencies and human resource development for the cyber security teams led by CSOs	◎	◎	△	×	△	Myanmar	It is considered possible for Myanmar to implement sufficient cyber security measures if appropriate people are appointed as CSOs and CIOs.
24			Implementation of training and practices on cyber security including those through international cooperation for the human resource development in cyber security	○	○	○	×	△	Myanmar	This measure is to be taken preferably after the capacity to implement basic cyber security measures in Myanmar has been improved to a certain level.
25			Quantitative and qualitative improvement of the human resources in cyber security through the cooperation with universities, graduate schools, research institutes and computer-related private organizations (including MCF, etc.)	△	△	△	×	×	Myanmar	Sufficient information sharing is required in the discussion on measures to train assistant engineers.
26				○	○	△	×	×	Myanmar	This measure is required for the training of assistant engineers.
27				◎	○	△	×	×	Myanmar	This measure is important as a long-term measure for human resource development.
28			Development of teaching materials	◎	◎	◎	◎	◎	TC-A	As the development of e-Government progresses, the implementation of a training program for government employees is urgently required.
29	Reinforcement of cooperation	Domestic cooperation	Development and operation of a mechanism for information sharing and communication on the security of critical infrastructures	○	○	△	×	△	Myanmar	The priority is on the identification of critical infrastructure and preparation of the standards and guidelines.
30			Development of a communication mechanism between CSIRTs of individual companies and mmCERT	○	○	△	×	○	N/A	The priority is on the preparation of guidelines, etc. to urge private companies to establish CSIRTs.
31		International cooperation	Sharing and utilization of the information on the best practices in other countries	○	○	△	×	○	Myanmar	It will be efficient to analyze the details of the incidents occurred in Myanmar before examining the best practices in other countries for their applicability in Myanmar.

No.	Purpose	Subject	Measure	Importance[1]	Urgency[2]	Lack of experience and knowledge in Myanmar[3]	Interference with the sustainability[4]	Applicable technologies[5]	ODA scheme[6]	Remarks
32			Development of the foundation for information security through international cooperation	○	○	○	○	○	Myanmar	Some government organizations including mmCERT have already been engaged in international cooperation. The establishment of an organization responsible for cyber security in the government is expected to improve the effectiveness of the international cooperation in cyber security.
33	Awareness raising		Awareness raising activities for all government employees	◎	◎	◎	◎	◎	TC-A	The improvement of the cyber security literacy of government employees is urgently required as the development of e-Government progresses.
34			Implementation of cyber security-related awareness raising activities for executives and people in charge of IT systems of private companies	○	○	○	×	○	N/A	This is a measure to be studied while the guidelines for private companies are being prepared.
35			Implementation of awareness raising activities to improve awareness of cyber security and improvement of cyber security literacy	◎	◎	◎	◎	◎	TC-A	The awareness raising activities for the people are urgently required as the demand on smartphones increases.
36			Reinforcement of the capacity to implement cyber security measures of government ministries and agencies	◎	◎	△ Lacking the implementation capacity	◎	○	TC-A	The impact of the activities to raise awareness to cyber security of government employees will increase if they are implemented continuously.

<Legend>

1 Importance: ◎indicates a measure with great importance.
2 Urgency: ◎indicates a measure with great urgency.
3 Lack of experience and knowledge in Myanmar: ◎indicates a measure for which Myanmar has insufficient experience and knowledge.
4 Interference with the sustainability: × indicates a measure which is likely to interfere with sustainable implementation of cyber security measures by Myanmar.
5 Applicable technologies: ◎indicates a measure in which a technology used in Japan can be also used in Myanmar.
6 ODA schemes: ‘TC’ and ‘GA’ indicate that measures are to be implemented in a technical cooperation project and a grant aid project, respectively. ‘A’ and ‘B’ after ‘TC’ and ‘GA’ indicate different technical cooperation and grant aid projects. ‘Myanmar’ indicates a measure to be implemented not by ODA project but independently by Myanmar. ‘N/A’ indicates a measure which cannot be included in an ODA project because it is a measure that directly assists the private sector.

7.2.2 Technical Cooperation Project

I. Project Outline

In the discussion on the plan for Japanese assistance to Myanmar in cyber security, the Survey Team found that it was possible to improve cyber security in the entire Myanmar in a short period of time by implementing many measures of great importance and urgency in a single technical assistance project. The measures marked with 'TC' in the 'ODA scheme' column in Table 7.2-1 are those to be included in the project.

The implementation of this project will require the submission of a request for technical cooperation project by Myanmar and Myanmar government and JICA will have to agree on the contents of the Project before its implementation. Meanwhile, the contents of the Project as assumed at present are described in the following paragraphs. The implementation of this Project will improve the capacity to implement basic cyber security measures and, at the same time, make it possible to study assistance measures to develop and improve the environment for the establishment of GSOC.

Many of the short-term measures that the Deputy Minister of Communication and Information Technology mentioned in his comment will be implemented in this technical cooperation project.

The outline of this draft technical cooperation project is described in the following. The result of the evaluation of its relevance is described in section 7.3.

- Project title: Project for Capacity Development on cyber security in the Republic of the Union of Myanmar (provisional)
- Project purpose: The capacity to implement basic cyber security measures is improved.
- Overall goal: The capacity to implement cyber security measures is improved.
- Outputs:

  Output 1: Policies, promotion measures, systems and standard guidelines are formulated.
  Output 2: Organizational structures concerning cyber security are developed.
  Output 3: Functions to monitor cyber attacks are developed.
  Output 4: Awareness of government employees on cyber attacks is improved.

- Main activities

Table 7.2-2 below shows the main activities planned for the achievement of the outputs mentioned above. In principle, the planned activities correspond to the security measures mentioned above. However, activities which are expected to create the foundation for the development of human resources to be required in future have been added from the viewpoint of ensuring the sustainability of the project.

Table 7.2-2 Main activities assumed in the draft technical cooperation project

	Main activities (assumed)	The number of the corresponding security measure in Table 7.2-1
Activities for Output 1		
1-1	Baseline standards on cyber security are to be formulated.	1
1-2	A practical rule on the use of web application is to be formulated.	2
1-3	Critical infrastructures are to be defined.	3
Activities for Output 2		
2-1	Inter-ministerial coordination committee on cyber security information is to be established.	9 and 14
2-2	The duties of CSOs and CIOs are to be demarcated and CSOs and	12

	Main activities (assumed)	The number of the corresponding security measure in Table 7.2-1
	CIOs are to be appointed.	
2-3	The Point of Contact (POC) is to be appointed.	15
2-4	Myanmar is to exchange and share incidents information with international organizations through POC.	15
Activities for Output 3		
3-1	Trainings to improve incidents detection and analysis capacity of CSOs of ministries and agencies and mmCERT are to be implemented.	19
3-2	Online teaching materials for government employees are to be developed.	28
3-3	A curriculum for the training on the incidents detection and analysis is to be developed in cooperation with universities and industrial associations.	Recommendation of the Survey Team
Activities for Output 4		
4-1	A program to improve cyber security literacy is to be formulated.	33
4-2	MCIT is to hold cyber security awareness raising workshops for government ministries and agencies.	36
4-3	Contents for the awareness raising activities on cyber security in the use of smartphones are to be developed.	35

◆ Counterpart (C/P) organizations
- Supervising organization: MCIT
- Implementing organizations: IT&CS, mmCERT
- Cooperating organizations: Scientific and technological universities and the Myanmar Computer Federation

◆ Japanese inputs
- Japanese experts (in six areas of expertise, a total of approx. 60 M/M)
- Incident detection system (including applications)
  Reference case (without redundant configuration)

  [For the installation in S12]
  ・DDoS detection unit
  ・IDS/IPS
  ・WAF

  [For the training]
  ・Router
  ・DDoS detection unit
  ・Firewall
  ・Mail server
  ・Mail filter
  ・IDS/IPS
  ・Web server
  ・WAF

◆ Implementation period: 3 years

II. Study Subjects

JICA is implementing a technical cooperation project, "Project on Capacity Building for Information Security," for the scheduled period of between July 2014 and January 2017. The purpose of the project is to improve the capacity of the Ministry of Communications and Information Technology of Indonesia in the implementation of information security measures. The project is expected to produce the following outputs: 1) the improvement of the functions of the Directorate of Information Security, 2) the establishment of a mechanism to support the secure use of IT at government departments and 3) the improvement of the information security awareness raising activities.

"Contents of the awareness raising in activities on cyber security in the use of smartphones are to be developed" is included in the activities in the outline plan of the technical cooperation project mentioned in 7.2.2 (1). The project being implemented in Indonesia also includes the establishment of a mechanism for cyber security awareness raising and development of teaching materials for the awareness raising as its components. In addition, the project includes a plan to study the current state of the cyber security including the guidelines on incident response procedures and critical infrastructure and standard equipment and measures at data centers in Japan and other ASEAN countries for the creation of a network to understand the trends in cybersecurity measures in future.

By implementing this technical cooperation project in cooperation with similar technical cooperation projects being implemented in the ASEAN area, it will become possible to establish a cyber security system conforming to the condition in the area and provide awareness raising activities to the people. In practice, it will be beneficial for the Myanmar counterparts to visit Indonesia in the third-country training program to observe the project activities being implemented and outputs being examined and analyze the activities and outputs to improve their activities. Meanwhile, the Indonesian counterparts will be able to obtain practical information on incidents in Myanmar from the Myanmar counterparts and utilize the information in their training on incident response.

7.3 Analysis of the Technical Cooperation Project with the Five Criteria for Evaluating ODA Project and Conclusion

The result of the preliminary evaluation of the draft technical cooperation project mentioned in section 7.2 with five DAC Criteria is described below. The Survey Team hopes that this evaluation result will facilitate the formulation of the technical cooperation project.

7.3.1 Relevance

The Survey Team has concluded that this Project is highly relevant for the reasons mentioned below.

I. Consistency with the Development Policies of Myanmar

The e-National Task Force established in 2004 prepared "Myanmar ICT Development Master Plan" with the assistance from South Korea. Since then, Myanmar has implemented "Myanmar Basic e-Government System" with a loan from South Korea and improved and expanded the facilities and network of MPT as national efforts to develop the ICT sector.

Meanwhile, Myanmar government led by the Ministry of National Planning and Economic Development prepared a national development plan, "National Comprehensive Development Plan (NCDP)" after the transfer to the civilian administration and set forth the seven strategies mentioned below in it.

- Strengthening Governance & Institution
- Enabling Business Environment
- Expand domestic & global connectivity
- Fostering Competitive Sectors
- Local Economic Potentials
- Human Development
- Environmental Protection

Later, Myanmar government formulated a five-year plan for the period between 2011 and 2015 (which has not been made public) based on NCDP. Meanwhile, the Government of Japan has established the "Myanmar-Japan Joint Initiative" (MJJI) with Myanmar government and has been studying practical measures to execute NCDP and the five-year plan effectively and to facilitate and accelerate the development of an investment environment in Myanmar. Myanmar government and the Government of Japan published the result of the study as the Myanmar Industrial Development Vision in July 2015. The Vision defines the five policies mentioned below as its pillars.

- Industrial development leveraged by the improvement of infrastructure and connectivity
- Development of predictable and efficient business environment and system foundation
- Human resource development to support "human-oriented development"
- Other strategic and cross-sectorial policies
- Realization of the potential of agriculture, forestry and fisheries

MCIT of Myanmar is formulating "Myanmar Telecommunications Master Plan 2015" on the basis of these national development plans with the assistance from the World Bank. The foci of this master plan are on 1) connecting the people in Myanmar in a coordinated way with communication technologies, 2) developing an environment for the high-speed Internet connection to have an advantage in economic activities and 3) promoting the development of e-Government. The formulation of this master plan is in the final stage. In addition, MCIT has formulated the "e-Governance Master Plan" with the assistance from ADB and proposed the milestones and the activities to be taken for the development of e-Government in the master plan. The master plan describes that the development of e-Government and the improvement in the internet connectivity in Myanmar are closely linked with the development strategies and that they are cross-sector tasks and activities of high priority.

On the other hand, as incident inventory information of cyber attacks has not been accumulated, it has not been possible even to evaluate how much risk created by cyber attacks that Myanmar is exposed to. As the communication networks are to be expanded and improved in the Communication Network

Improvement Project assisted by Japan, the risk of Myanmar being used in springboard attacks to other countries including ASEAN countries is expected to increase with the increase in the number of Internet users resulting from the dramatic change in the telecommunication environment including the use of smartphones. Therefore, the vulnerability of cyber security including the vulnerability to cyber attacks is an obstacle to execute the communication policy of Myanmar. This vulnerability may become not only a great obstacle to the expansion of the Internet and the development of e-Government, but also a possible cause of accusation from other countries if Myanmar has failed to react effectively against those springboard attacks. Under the circumstances, this technical cooperation project on cyber security is expected to contribute to the fulfillment of a high-priority development need of Myanmar. Therefore, the Project is consistent with the telecommunication policy of Myanmar.

II. Consistency with the Country Assistance Policy of Japan

After the new administration of Myanmar began the process of democratization in 2011, Myanmar government and the Government of Japan held a summit meeting on April 21st, 2012, and agreed on the importance of strengthening the bilateral relationship. In accordance with this agreement, the Government of Japan changed the economic assistance policy for Myanmar. This new policy describes "Development of human resources and systems to support the economy and society" as one of the three priority areas of assistance to Myanmar. Since the purpose of this technical cooperation project is to improve the capacity to implement basic cyber security measures focusing on the development of human resources, organizations and systems, it is consistent with the country assistance policy for Myanmar.

III. Relevance of the Technical Cooperation Project as a Means of Assistance

The Government of Japan has implemented assistance projects including two grant aid projects, "The Project for Urgent Improvement of Communication Networks" (in 2012) and "The Project for Development of ICT System for Central Banking" (in 2013), and two technical cooperation projects, "Project on ICT Human Resource Development at ICT Training Institute" (from 2006 to 2011) and "Project for Enhancement of Engineering Higher Education" (from 2013 to 2018) in the ICT sector in Myanmar. The development of a training curriculum on the incident detection and analysis with the human resources developed in the project activities in the above-mentioned project and in cooperation with universities and industrial associations is expected to create a synergic effect. Since the cooperation with universities and industrial associations is expected to facilitate development of a system for cyber security which includes them, this cooperation will contribute to the smooth implementation of this Project and may facilitate the creation of close relationships between ICT engineers of Myanmar and Japanese ICT engineers. In addition, KDDI and Sumitomo Corporation entered the ICT market in Myanmar in a joint venture with MPT and established partnership with MPT in the entire area of its business including the development of communication networks throughout the country and the Internet service provision. Therefore, the implementation of this Project is expected to increase the advantage of Japan in the ICT sector in Myanmar.

7.3.2 Effectiveness

The effectiveness of this Project is expected from the reasons mentioned below.

I. Interpretation of the Project Purpose

The project purpose is interpreted as the development of the technical capacity to support the execution of the master plan in the ICT sector of Myanmar at its foundation. If sufficient cyber security measures are not taken, the systems and mechanisms to be developed in accordance with the master plan could be destroyed or wasted. Therefore, the implementation of this Project is effective.

II. Causal Relationships

In this Project, Output 1 is to be achieved with the development of a legal framework, a policy, a plan for awareness creation activities and guidelines on cyber security and Outputs 2 and 3 are to be achieved with the establishment of an inter-ministerial and inter-agency organization, the development and improvement of the human resource to respond to incidents and the establishment of the function to detect cyber attacks required for the establishment of cyber security. As those activities are essential for the achievement of the project purpose, the composition of the project is considered appropriate. The awareness creation activities to be implemented for the achievement of Output 4 will draw people's attention to the necessity of and create the motivation for them to participate in cyber security, prevention of damage caused by cyber attacks and long-term human resource development in cyber security. Such attention and motivation will lead to the achievement of project outputs and overall goal. The discussion mentioned above has revealed the existence of direct relationships between the outputs, project purpose and overall goal of this Project.

7.3.3 Efficiency

Attention shall have to be paid to the maintenance of the efficiency of this Project for the reasons mentioned below.

I. Causal Relationship

A concern has been raised about the feasibility and sustainability of this Project on the basis of the points mentioned below.

The first point is that a basic plan on cyber security has not been formulated and that Myanmar government has not officially approved the "Myanmar Telecommunication Master Plan" or "e-Governance Master Plan." Although significant revision is not expected in the final stage of their formulation, such revision may restrict certain project activities if it is made. The second point is the restructuring of the entire MCIT including MPT conducted as part of the reorganization of government organizations. There is also a plan to transfer the jurisdiction over the engineering and computer science universities to MOE. Such changes concerning the organizations to be involved in this Project may create a risk of increasing the time required for decision-making and coordination for the project implementation. The third point, which is related to the second point, is an undeniable possibility of

significant changes in the budgeting and budgetary allocation resulting from the restructuring. As such changes may cause chaos in the budget implementation, they are matters of concern to the efficiency of the project.

7.3.4 Impact

Positive impact is expected from the implementation of this Project for the reasons mentioned below.

I. Interpretation of the Overall Goal

This Project is an effort to facilitate provision of public services by the government and bring indirect benefit to mobile phone users, whose number is increasing rapidly. This Project is to bring indirect benefit to all those who use ICT effectively and who are engaged in socio-economic activities using ICT safely and appropriately.

II. Indirect Impact

As the assistance of the World Bank and ADB in rural development and gender issues is focused on vocational training through ICT, synergic impact with the activities of other donors can be expected from the implementation of this Project. The activities to be implemented for Output 1 are those essential for private companies in Myanmar to conduct socio-economic activities safely. While it is difficult for small- and medium-sized companies to spend a significant amount of money on cyber security measures, the protection and promotion of the small- and medium-sized companies, which comprise 87 % of the companies in Myanmar, is important for the economic development of Myanmar. The implementation of this Project will contribute indirectly to the human resource development in many small- and medium-sized IT vendors.

7.3.5 Sustainability

This Project is expected to have sustainability as mentioned below.

I. Policy Aspect

ICT-related activities are a key factor for the World Bank and ADB to provide the assistance that they prioritize. The development of e-Government is designated as a measure that all the government ministries and agencies should take. For these reasons, the government as a whole is expected to take the cyber security measures in a sustainable fashion.

II. Organizational Aspect

The organizational structure for implementation of general cyber security measures has been established with the establishment of the National Cyber Security Center (NCSC). The jurisdiction over mmCERT has been transferred from the Ministry of Science and Technology to NCSC. The organizational structure in Myanmar government for cyber security is being developed with these measures. Engineers employed by MPT are to be transferred to the newly established NCSC as part of

the personnel assignment plan for NCSC.

III. Technical Aspect

As mentioned above, the posts of engineers in NCSC are to be filled with the transfer of staff members of MPT. As they have been employed as workers in the communication sector and have the basic technical capacity, it is not necessary to provide them with technical training at the basic level. mmCERT has started collecting and analyzing information in the international cooperation with JPCERT. These frameworks are expected to be maintained in future and the technical capacity in cyber security is expected to be maintained and improved with the international cooperation. Therefore, there is no problem concerning the sustainability in the technical aspect.

IV. Financial Aspect

An appropriate amount of budget seems to have been allocated for the operation of equipment and facilities procured by the government for the provision of online services and the establishment of the data center for the development of e-Government. The system operation does not seem to have been suspended because of the expiry of software license. If an appropriate amount of budget is not allocated to the data center which stores electronic assets of government ministries and agencies and a cyber attack is made on the center, the government will suffer great damage and a huge amount of money will be required for the repair. Therefore, the budget required for cyber security is expected to be secured through smooth coordination between the relevant organizations which is expected from the establishment of an inter-ministerial and inter-agency coordination organization to be established as an activity of this Project.

7.3.6 Conclusion

The Survey Team concludes that the significance of the implementation of this Project is high because it is sufficiently consistent with the development policies and needs of Myanmar and the assistance policy of Japan and the team has confirmed the relevance of the plan for the project.

7.4 Study on the Relevance of the Request for Grant Aid Assistance

This survey was implemented in response to a request for grant aid assistance submitted by Myanmar government. Therefore, Myanmar government expects the grant aid assistance as the modality of the Japanese assistance. However, the Survey Team considers that it is not appropriate to implement all the contents of the request mentioned above in a Japanese grant aid project for the reasons mentioned below and that they should be revised in accordance with the outcome of the technical cooperation project mentioned in section 7.3.

The request concerned corresponds to part of the assistance measure No. 10 in Table 7.2-1.

7.4.1 Changes after the Reception of the Request

I. Restructuring of MCIT

The request stipulates the data center operated by MPT as the location of the installation of the equipment mentioned in it (see 7.4.1.1.2 below for detail). However, MPT has become only responsible for the communication services since the reorganization of MCIT in April 2015. IT&CS, which was established in the reorganization, is performing such duties as sorting of data, development of the e-Government systems and monitoring of cyber attacks. In other words, MPT is no longer responsible for the cyber security measures. Furthermore, MPT is scheduled to be privatized next year. After the privatization, MPT will compete with the private communications carrier in the hosting service at the aforementioned data center and this competition is expected to intensify in future. Therefore, it is appropriate to consider that MPT is not qualified as a direct beneficiary of the requested ODA assistance.

II. Roles of MPT and IT&CS

The equipment of GSOC to be procured in the grant aid project was to be installed in Hanthawaddy and Dekkhina Data Centers in the original plan (Figure 7.4-1). However, they have been the data centers operated by MPT since the reorganization mentioned above.

Government ministries and agencies are using the hosting service of MPT and have their web servers and mail servers installed in these two data centers. Yatanarpon Teleport, the competitor of MPT, has government ministries and agencies as its clients of the similar service.

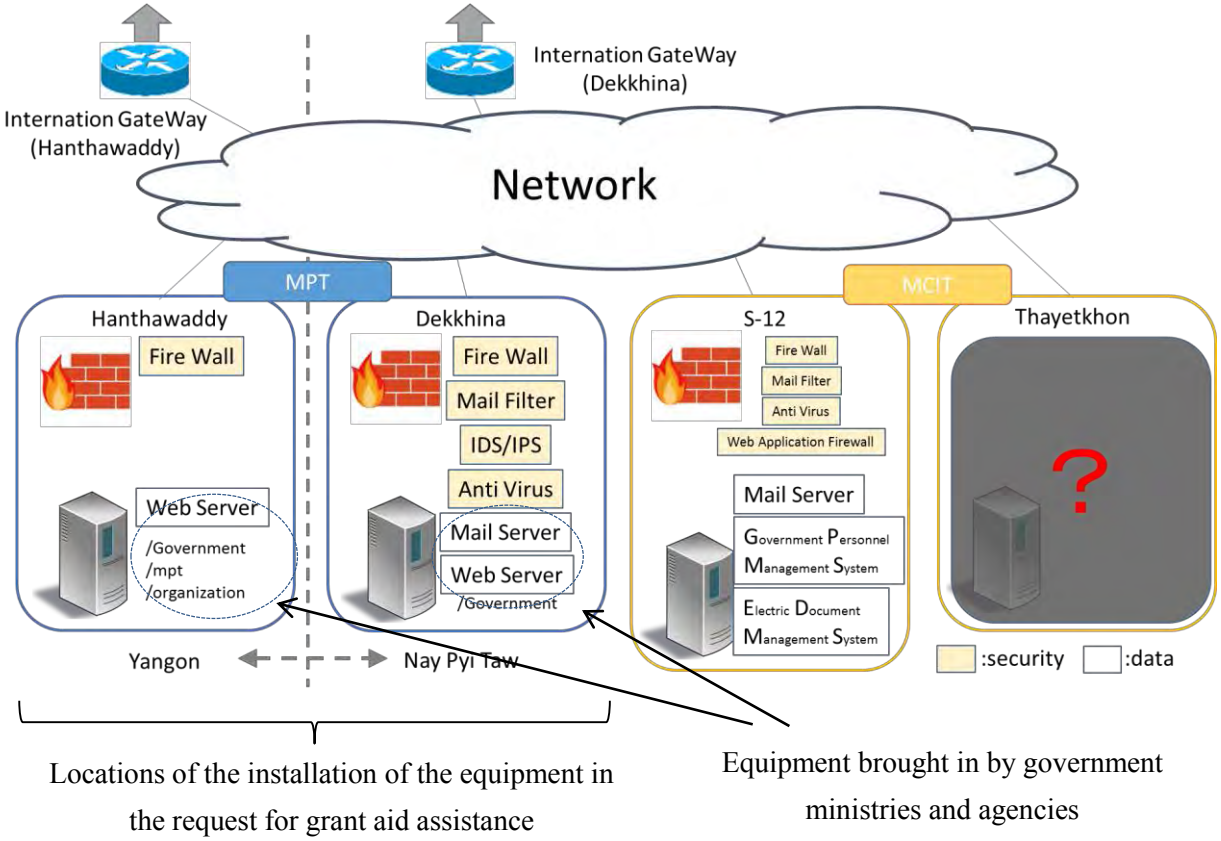


Figure 7.4-1 Data centers and the locations of the installation of the equipment requested for procurement in the grant aid assistance

Meanwhile, the government as a whole is actively promoting the development of e-Government.
In order to mitigate negative impact of the relocation of the capital to Naypyidaw on the quality of administrative services, Myanmar government has been providing the online administrative services (*e.g.* the online company registration system operated by MOC). The ICT Master Plan, which includes measures to develop e-Government prepared by the World Bank, and the e-Governance Master Plan prepared by ADB also urge Myanmar government to promote e-Government.
MCIT has installed the electronic document management system and the government personnel management system in S-12 Building in Naypyidaw as a new measure to develop e-Government. However, as the newly developed IT&CS does not have sufficient staff members to operate these systems, MCIT is planning to transfer approx. 50 staff members of MPT to IT&CS in this fiscal year. The policy of MCIT is to eventually transfer a total of 200 to 300 staff members of MPT to IT&CS.

7.4.2 Problems in the Implementation of Grant Aid Project

I. Evaluation of the Impact of the Project to Provide Equipment to GSOC

The role of GSOC, when it is established, will be not to protect networks from cyber attacks but to detect them. It will be human beings that make decision on the measures to be taken and implement them so that the area affected by an attack and damage caused by it will not exceed certain levels. There are many types of cyber attacks and new types of attacks are created in short cycles. This is the reason for the difficulty in evaluating the project impact quantitatively.
It is generally believed that 25 % to 30 % of attacks of known types can be prevented. As it is almost impossible even to detect known types of attacks in Myanmar at present, the improvement of the prevention ratio of known attacks to 25 % could be used as an indicator of the project impact. However, it is difficult to incorporate serious impact which may be caused by new types of attacks in an indicator of the project impact.
Alternatively, an indicator based on the operational impact may be used in the evaluation of the project impact. For example, the number of detected attacks may be used as such an indicator.
It is possible to conduct a study on a qualitative indicator of the project impact using the level of technical difficulty and efficiency of a countermeasure based on the visualization of cyber attacks. However, it is difficult to conduct such a study where even the types of incidents which are actually occurring are unknown.

II. Reform of MPT and Considerations to Private Communications Carriers

The networks of MPT have been used for the hosting service to government ministries and agencies. Their e-mail systems are connected to the Internet through a network of MPT. Because of the configuration of these networks, MTP could practically become an exclusive provider of a hosting service by manipulating the fee setting for other private communications carriers which intend to provide a hosting service to government ministries and agencies. Meanwhile, a hosting service is generally provided as a business model including security measures. Therefore, a private carrier may provide a hosting service inclusive of security measures in future.

If MPT is allowed to provide a service that it has provided as a public service exclusively using the system that it has been using, a function of the market principle of lowering communication fees may be completely or partially obstructed and, as a result, the communication sector may develop less than expected. It will be beneficial to the people of Myanmar if measures are taken to maintain a sound competition principle between MPT scheduled to be privatized next year and private communications carriers.

Therefore, the grant aid assistance should be designed to bring indirect benefit to carriers other than MPT and, as a result, bring benefit to the people, so that the implementation of the assistance would not give MPT a competitive edge over the other carriers. The purpose and outcome of the use of equipment to be provided should be scrutinized to design such assistance.

III. Implementing Organization of the Grant Aid Project

If it is decided to implement the grant aid project, the National Cyber Security Center (NCSC) of IT&CS is expected to be the department responsible for the project in the implementing organization because of the restructuring in MCIT. It is considered impossible for NCSC to implement and manage the project appropriately because it has only five staff members at present. Therefore, it will be necessary to confirm that NCSC has completed the preparation to implement the grant aid project before its implementation.

7.4.3 Measures to be Taken

There is no doubt concerning the general need to install a detection system against cyber attacks. Therefore, the Survey Team recommends that a minimum input of essential equipment and applications should be made for the time being and that detection equipment and applications corresponding to the technical capacity of (the personnel of) Myanmar should be installed after the capacity has improved in future.

Therefore, it is considered reasonable to include the urgently required essential equipment and applications in the minimum input in the equipment to be procured in the technical cooperation project proposed in section 7.2.2 and to procure and install the rest of required equipment in the grant aid project to be implemented later. It is worth studying the possibility of procuring the equipment as part of the grant aid assistance to the development of e-Government with the indicators of the project impact taken into consideration.

The subjects of the study on the relevance of implementing the grant aid project are as follows.

I. Review of the contents and scope of the assistance

This grant aid project shall be considered as the assistance to facilitate the development of e-Government, instead of assistance to GSOC. e-Government is expected to improve the availability of public services for socio-economic activities in communities and facilitate their development. Thus, the implementation of this Project is consistent with “Support for improvement of people’s lives,” one

of the priority assistance areas of Government of Japan for Myanmar.

II. Duplication with the assistance of the World Bank

The World Bank is assisting the procurement of equipment of the data center for e-Government established in S-12 Building. Some of the pieces of equipment to be procured have an accessary cyber attacks detection function. The details of the assistance of the World Bank shall have to be studied thoroughly in the stage of formulation the grant aid project to avoid duplication of assistance.

III. Coordination with the technical cooperation project and implementation period

The inclusion of the creation of incidents inventory in the technical cooperation project will make it possible to conduct a study on the contents of the assistance to make it effective. As the equipment is to be provided in the technical cooperation project, it will be possible to postpone the implementation of the grant aid project and conduct a study on appropriate contents of the grant aid project. The grant aid project shall have to be designed so that the provision of the equipment can be made at opportune timing while the system, organizational structure and human resource are being developed urgently in the technical cooperation project in order to counteract the threat of cyber attacks.

The decision on the necessity to revise the request depends largely on the discretion of the Minister of Communication and Information Technology. The decision on the contents of government projects is made at the Planning Committee (under the jurisdiction of the Ministry of National Planning and Economic Development). Then the Financial Committee under the jurisdiction of the Ministry of Finance approves the budgetary allocation to the projects. The Planning Committee assesses project contents. Requests for assistance are submitted through the Foreign Aid Management Committee. Revision and re-submission of the request will not be necessary, if the minister is able to explain the change of the scope of the project to those committees. If the minister wishes to obtain the approval of the committees for the revision of the contents of the request, a new request shall have to be submitted. If the grant aid project is to be assessed after the progress of the technical cooperation project is observed, the assessment will be conducted several years after the submission of the original request. Therefore, it is considered necessary to study the handling of the request carefully.

Chapter 8 **Conclusion and Future Issues**

Development of training center for conducting effective and periodical training is described as one of reinforcement measures for incident detection and analytical skills for government systems in measure 20 of table 7.2-1. This simulates to generate incidents and cultivate necessary technical capability. Since there are several kinds of cyber attacks are occurred in short term, it is effective method to correspond continuously by themselves in Myanmar.

Human resource development is one of 7 strategies of NCDP and matches the direction of our country's assistance which likewise puts emphasis on human resource development. Although Myanmar doesn't have enough technical know-how to develop such training center and has difficulty to prepare for the construction fee. On the other hand, our country has similar successful case of establishment such as Control System Security Center (CSSC) and holds possible use of technologies.

After relocating the capital to Naypyidaw, Yangon is still base for private companies' business. Companies related to IT and cybersecurity mainly locate in Yangon and take business trip for maintenance of government servers and network development outsourcing from Yangon. Especially it is difficult to treat emergency response in server maintenance contract and it is expected to found those companies around Naypyidaw. Therefore IT industry will be developed by taking human resource development in a big picture and collaborating with industrial development measures in Myanmar (draft).

Industries in Myanmar are currently overconcentration in Yangon. In order to decentralize industries and make efforts to have economic effects on local cities around, the second ICT park should be developed and attract telecommunication companies and ICT related companies for developing applications and systems. The base for human resource development should be established in the ICT Park. As the part of the facility, it is worth consideration of developing cyber security training center which our country has know-how by grant aid project.

ICT utilization centering on smartphone exceeds the progress of telecommunication network development and improves rapidly. Human resource development for IT sector, however there are still not stabled recruit opportunities in computer science. Since there are no ICT related companies in Naypyidaw, ministries and agencies have to contract with those companies in Yangon for services when it is necessary. It cannot be denied that there is ineffective business management by geographical distance between Yangon and Naypyidaw. In order to improve these factors, not only considering simple cyber security countermeasures draft but also improving the status of engineers and ensuring recruit opportunities is the most important issue and it is necessary to decentralize bases of private companies.

Considering effective economic evolution by cross-sectoral issues solution is expected and our country's grant aid project is hoped to be of some help. When this grant aid project is conducted, synergetic effects will be expected by conducting a technical cooperation project (this project assumes second phase of the technical cooperation project described in section 7.2.2) which aims to teach the advanced usage of the equipment and develop detection and response capacity for cyber security.