ミャンマー国
通信・情報技術省

ミャンマー国
サイバーセキュリティにかかる
情報収集・確認調査報告書

平成 27 年 11 月
(2015 年)

独立行政法人
国際協力機構（JICA）

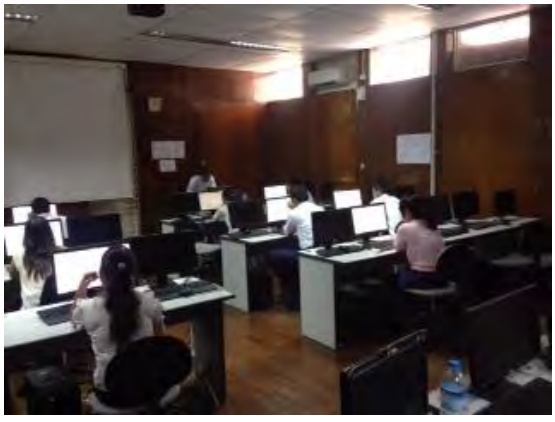
株式会社三菱総合研究所
八千代エンジニヤリング株式会社

基盤
CR(5)
15-176

目　　次

図表リスト

巻頭写真

<table>
<tr><td>  </td><td>  </td></tr>
<tr><td>mmCERT のオフィスの様子。職員は管理職が 15 名、その他職員が 10 名で構成される。</td><td>ミニッツ協議の様子。調査の方針について通信･情報技術省の局次長である Soe Thein 氏と協議した。</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>通信・情報技術省の副大臣を表敬訪問し、調査の途中経過について報告した。</td><td>現地調査終了時報告会の様子。33 組織から約 60 名が参加した。</td></tr>
<tr><td>  </td><td>  </td></tr>
<tr><td>ICTTI（情報通信技術訓練センター）では、大学を卒業した生徒を対象に数週間～数か月の様々な IT 関連トレーニングを行っている。</td><td>データセンター内観（デッキーナ）
政府や民間企業に対しホスティングサービスとして場所、電源、ネットワーク等の提供を行っている。</td></tr>
</table>

略 語 集

ADB	Asian Development Bank（アジア開発銀行）
ADS	Anti DDoS System (アンチ DDoS システム)
APCERT	Asia Pacific Computer Emergency Response Team（アジア太平洋コンピュータ緊急対応チーム）
CB Bank	Co-operative Bank（共同組合銀行）
CBM	Central Bank of Myanmar（ミャンマー中央銀行）
CDMA	Code Division Multiple Access（符号分割多元接続）
CEPTOAR	Capability for Engineering of Protection, Technical Operation, Analysis and Response（情報共有・分析機能）
CERT	Computer Emergency Response Team（コンピュータ緊急対応チーム）
CICC	Center of the International Cooperation for Computerization（国際情報化協力センター）
CIO	Chief Information Officer（最高情報責任者）
CS	Cyber Security（サイバーセキュリティ）
CSIRT	Computer Security Incident Response Team（シーサート）
CSO	Chief Security Officer（最高セキュリティ責任者）
DAC	Development Assistance Committee（開発援助委員会）
DDoS	Distributed Denial of Service attack（ディードス攻撃）
DLP	Data Loss Prevention / Data Leak Protection（情報漏えい防止）
DoS	Denial of Service attack（ドス攻撃）
DPI	Deep Packet Inspection（ディープ・パケット・インスペクション）
DSL	Digital Subscriber Line（デジタル加入者線）
E/N	Exchange of Notes（交換公文）
EDI	Electronic Data Interchange（電子データ交換）
EDMS	Electronic Document Management System（電子文書管理システム）
EGDI	E-Government Development Index（電子政府の開発状況の指標の一つ）
e-NTF	e-National Task Force（電子国家対策委員会）
ERP	Enterprise Resource Planning（統合基幹業務システム）
EU	European Union（欧州連合）
FW	Firewall（ファイアウォール）
GCI	Global Cybersecurity Index（グローバルサイバーセキュリティインデックス）
GDP	Gross Domestic Product（国内総生産）
GNI	Gross National Income（国民総所得）
GSM	Global System for Mobile Communications（第 2 世代移動通信システム規格）
GSOC	Government Security Operation Coordination team（政府機関情報セキュリティ横断監視・即応調整チーム）
ICT	Information and Communications Technology（情報通信技術）

ICTTI	Information and Communication Technology Training Institute（情報通信技術訓練センター）
IDS	Intrusion Detection System（侵入検知システム）
IEC	International Electrotechnical Commission（国際電気標準会議）
IMCEITS	India-Myanmar Centre for Enhancement of IT Skills
IPA	Information-technology Promotion Agency（情報処理推進機構）
IPS	Intrusion Prevention System（侵入防御システム）
IS	Information Security（情報セキュリティ）
ISMS	Information Security Management System（情報セキュリティマネジメントシステム）
ISO	International Organization for Standardization（国際標準化機構）
IT&CS	Information Technology and Cyber Security Department（IT サイバーセキュリティ局）
ITU	International Telecommunication Union（国際電気通信連合）
JICA	Japan International Cooperation Agency（国際協力機構）
JPCERT/CC	Japan Computer Emergency Response Team / Coordination Center（日本コンピュータ緊急対応チーム/コーディネーションセンター）
KOICA	Korea International Cooperation Agency（韓国国際協力団）
LAN	Local Area Network（ローカルエリアネットワーク）
LG-WAN	Local Government Wide Area Network（総合行政ネットワーク）
MCF	Myanmar Computer Federation（ミャンマーコンピュータ連盟）
MCIT	Ministry of Communications and Information Technology（通信・情報技術省）
MCPA	Myanmar Computer Professional Association（ミャンマーコンピュータ専門家協会）
MJJI	Myanmar-Japan Joint Initiative（日ミャンマー共同イニシアティブ）
mmCERT	Myanmar Computer Emergency Response Team（ミャンマーコンピュータ緊急対応チーム）
MOCO	Ministry of Commerce（商務省）
MOE	Ministry of Education（教育省）
MOH	Ministry of Health（保健省）
MOST	Ministry of Science and Technology（科学技術省）
MPT	Myanmar Posts and Telecommunications（ミャンマー郵電公社）
MPU	Myanmar Payment Union（銀行連合）
MTU	Mandalay Technological University（マンダレー技術大学）
NCC	National Consumer Council（全英消費者協議会）
NCDP	National Comprehensive Development Plan（国家開発計画）
NCSC	National Cyber Security Center（国家サイバーセキュリティセンター）
NCSSC	National Cyber Security Steering Committee（国家サイバーセキュリティ運営委員会）
NDC	Nai Pyi Taw Development Committee（ネピドー開発委員会）
NISC	National Center of Incident Readiness and Strategy for Cybersecurity（内閣サイバーセキュリティセンター）

ODA	Official Development Assistance（政府開発援助）
PCIDSS	Payment Card Industry Data Security Standard（PCI データセキュリティスタンダード）
PKI	Public Key Infrastructure（公開鍵基盤）
POC	Point of Contact（接点、連絡先）
PPP	Public Private Partnerships（公民連携）
PTD	Posts and Telecommunications Department（郵便電気通信局）
PTU	Pyay Technological University（ピィ技術大学）
SLA	Service Level Agreement（サービス品質保証）
SNS	Social Networking Service（ソーシャルネットワークサービス）
UCSM	University of Computer Studies, Mandalay（マンダレー・コンピュータ大学）
UCSY	University of Computer Studies, Yangon（ヤンゴン・コンピュータ大学）
UPS	Uninterruptible Power Supply（無停電電源装置）
USAID	United States Agency for International Development（アメリカ合衆国国際開発庁）
VPN	Virtual Private Network（仮想プライベートネットワーク）
WAF	Web Application Firewall（ウェブアプリケーションファイアウォール）
WAN	Wide Area Network（ワイドエリアネットワーク）
WB	World Bank（世界銀行）
W-CDMA	Wideband Code Division Multiple Access（第 3 世代携帯電話の無線アクセス方式の一つ）
WiMax	Worldwide Interoperability for Microwave Access（無線通信技術の規格のひとつ）

第1章　業務の背景

インターネットの急激な普及に伴い、サイバーセキュリティに関する対策の必要性は日増しに高まっている。特に、政府機関や民間企業などを標的とした、不正なウェブサイト改ざん、機密情報の外部流出、重要システム強制停止等を行うサイバー攻撃による被害事例が国際的に増加している。我が国においても 2011 年に重工業企業など防衛・インフラ関連産業や衆参両院、中央省庁が相次いでサイバー攻撃を受けていたことが発覚し、政府として官民情報連携強化などによるサイバーセキュリティ対策の強化に乗り出している。

我が国は、2008 年日・ASEAN 経済大臣会合「アジア知識経済化イニシアティブ」及び 2009 年より継続実施中の「日 ASEAN 情報セキュリティ政策会議」の枠組みにおいて、我が国およびミャンマー（以下、「ミ」国という。）を含む ASEAN における安心安全な情報通信技術（以下、「ICT」という。）利用環境の構築に向けた取り組みを実施している。「ミ」国においては、情報通信については主に、通信・情報技術省（以下、「MCIT」という。）が主管しており、MCIT は 2014 年よりアジア開発銀行の協力をうけ、ミャンマー電子政府マスタープランの作成を進めており、電子政府の利用環境としても「ミ」国内におけるサイバーセキュリティ対策についての重要性認識が向上してきている。

係る状況において、「ミ」国政府は 2010 年にサイバーセキュリティ対策の情報収集、対策支援、各種調整機関としてミャンマーComputer Emergency Response Team（以下、「mmCERT」という。）を設立した。2013 年にはサイバーセキュリティの推進機構として国家サイバーセキュリティ運営委員会を設立し、同国のサイバーセキュリティ対策の強化に取り組んできた。さらに、2015 年 4 月に新たに「ミ」国政府内のサイバーセキュリティ対策を一手に担うべく IT サイバーセキュリティ局（以下 IT&CS）が MCIT 配下に設立された。

一方で、サイバーセキュリティ分野については、法令、組織、人材育成等のバランスのとれた強化、および、官民双方の協力が不可欠であるが、「ミ」国政府のサイバーセキュリティに係る包括的な戦略、政府組織間や官民の役割分担、現状の対策整備状況、および強化方針が明確となっていない。

今後、「ミ」国がサイバーセキュリティ向上に取り組むに際し、対応を強化すべき事項や優先度を整理し、我が国による支援可能な分野を明らかにする必要がある。

第2章　業務の概要

2.1　調査の目的

「ミ」国のサイバーセキュリティについて、サイバーセキュリティに係る戦略、政策、関連官庁および民間企業等のサイバーセキュリティ対策の現状、当該分野の課題等について情報を収集・確認するとともに、サイバーセキュリティに係る協力ニーズを把握・分析した上で、我が国ODAによる支援内容の方向性を確認することを目的とする。

2.2　調査の対象

調査の対象は以下の通りである。また、調査における本邦及び「ミ」国の主要関係機関を表2.2-1にまとめる。

表2.2-1　主要関係機関

日本語表記		英語表記	略称
日本側			
政府	内閣サイバーセキュリティセンター	National Center of Incident Readiness and Strategy for Cybersecurity	NISC
	一般社団法人 JPCERT コーディネーションセンター	Japan Computer Emergency Response Team / Coordination Center	JPCERT/CC
民間	日本電気株式会社	NEC Corporation	NEC
	富士通株式会社	FUJITSU LIMITED	FUJITSU
	NTT コミュニケーションズ	NTT Communications	NTT Com
「ミ」国側			
政府	通信・情報技術省	Ministry of Communications and Information Technology	MCIT
	郵便電気通信局	Posts and Telecommunications Department	PTD
	ミャンマー郵電公社	Myanmar Posts and Telecommunications	MPT
	IT サイバーセキュリティ局	Information Technology and Cyber Security Department	IT&CS
	mmCERT	Myanmar Computer Emergency Response Team	mmCERT
	科学技術省	Ministry of Science and Technology	MOST
	教育省	Ministry of Education	MOE
	国家サイバーセキュリティ運営委員会	National Cyber Security Steering Committee	NCSSC
	保健省	Ministry of Health	MOH
	商務省	Ministry of Commerce	MOCo
	ネピドー開発委員会	Nai Pyi Taw Development Committee	NDC
	国家計画・経済発展省	Ministry of National Planning and Economic Development	MNPED
	情報・通信技術訓練研究所	Information and Communication Technology Training Institute	ICTTI
	ヤンゴン工科大学	Yangon Technological University	YTU
	中央銀行	Central Bank	CB
	ミャンマー日本人材開発センター	Myanmar – Japan Center	日本人材開発センター

民間	ミャンマーコンピュータ連盟	Myanmar Computer Federation	MCF
	KSGM	KDDI Summit Global Myanmar Company Limited	KSGM
	ヤタナポンテレポート	Yatanarpon Teleport	Yatanarpon
	レッドリンク	RedLink	RedLink
	V2M	Vision to Motion	V2M
	Alpha	Alpha	Alpha
その他			
ドナー	韓国国際協力機構	Korea International Cooperation Agency	KOICA
	アジア開発銀行	Asian Development Bank	ADB
	世界銀行	World Bank	WB

2.3 業務の実施スケジュール

業務の実施スケジュールを図 2.3-1 に示す。

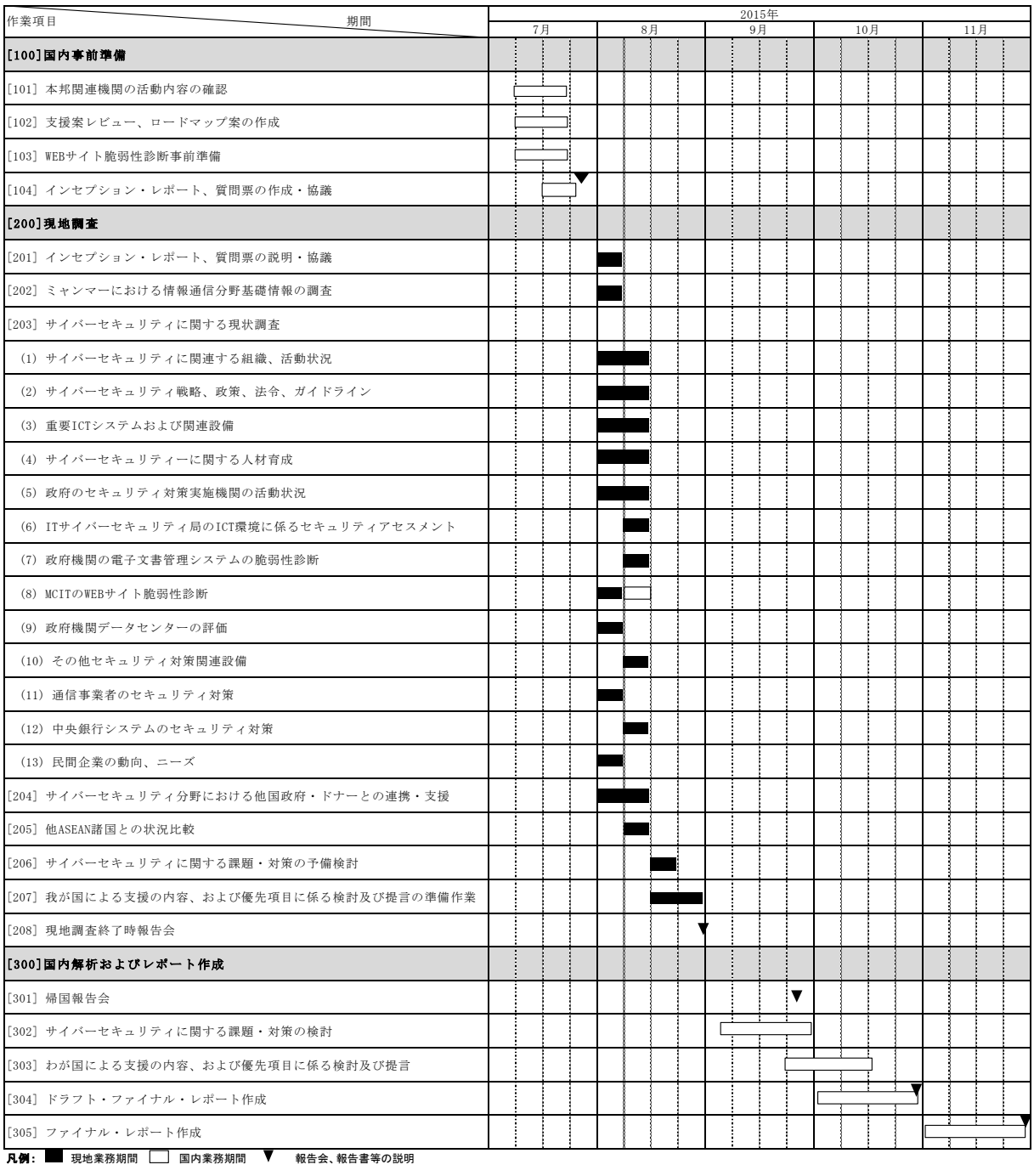


図 2.3-1　業務実施スケジュール

2.4　現地派遣期間における主な活動

下表 2.4-1 に現地調査の調査団員と担当業務を示す。また、表 2.4-2 に現地での主な活動を示す。

表 2.4-1　調査団員と担当業務

氏名	所属	担当業務	主な役割	現地調査期間
佐藤　明男	MRI	業務主任／ サイバー戦略	プロジェクト全体の管理、サイバーセキュリティに係る戦略等の調査	2015/8/2 – 8/29
村野　正泰	MRI	セキュリティ対策計画 1／ 脆弱性診断	規制・法制度、ガイドライン等の対策検討、 WEB 脆弱性診断の実施	2015/8/2 – 8/7, 2015/8/23 – 8/28
中村　尚	MRI	セキュリティ対策計画 2／ セキュリティアセスメント	セキュリティアセスメント及び電子政府システムの脆弱性診断の実施	2015/8/11 – 8/29
宮本　健吾	YEC	データセンター評価	政府機関データセンターの評価	2015/8/2 – 8/29
池田　好孝	YEC	ICT システム	ICT 及びセキュリティ関連設備の整備計画の検討	2015/8/2 – 8/29
南部　尚昭	YEC	人材育成計画／ 協力支援内容検討	人材育成等を踏まえた協力支援内容の検討	2015/8/2 – 8/30

表 2.4-2　現地での主な活動

No.	月日	曜日	官団員	調査団員						宿泊地
			総括	業務主任/サイバー戦略	人材育成計画/協力支援内容検討	ICTシステム	データセンター評価	セキュリティ対策計画1/ 脆弱性診断	セキュリティ対策計画2/ セキュリティアセスメント	
1	2015/8/2	日	移動 [東京→ヤンゴン]	移動 [東京 (11:00) → ヤンゴン (15:40)]						ヤンゴン
2	2015/8/3	月	AM: 09:00, 在ミャンマー日本国大使館表敬訪問、調査日程・ｲﾝｾﾌﾟｼｮﾝ・ﾚﾎﾟｰﾄ等の説明 10:30, インセプション・レポート等の協議 (mmCERT) PM: 13:30, KSGM訪問 16:00, NEC訪問							ヤンゴン
3	2015/8/4	火	移動 [ND101 ヤンゴン(7:00) → ネピドー(7:55)] AM: ｲﾝｾﾌﾟｼｮﾝ・ﾚﾎﾟｰﾄ及びMM等の協議(ITサイバーセキュリティ局) PM: 団内打合				移動 [ND101 ヤンゴン(7:00) → ネピドー(7:55)] AM: ｲﾝｾﾌﾟｼｮﾝ・ﾚﾎﾟｰﾄ及びMM等の協議(ITサイバーセキュリティ局) PM: データセンター評価実施	移動 [ND101 ヤンゴン(7:00) → ネピドー(7:55)] AM: ｲﾝｾﾌﾟｼｮﾝ・ﾚﾎﾟｰﾄ及びMM等の協議(ITサイバーセキュリティ局) PM: 団内打合		ネピドー
4	2015/8/5	水	AM: 団内打合 PM:ｲﾝｾﾌﾟｼｮﾝ・ﾚﾎﾟｰﾄ等の合同協議（科学技術省、教育省）				データセンター評価実施	Webサイト 脆弱性診断		ネピドー
5	2015/8/6	木	AM: 団内打合 PM: MM協議及び署名 移動 [ネピドー → ヤンゴン] 在ミャンマー日本国大使館報告 JICA事務所報告	AM: 団内打合 PM: MM協議及び署名 移動 [ND9110 ネピドー(18:20) → ヤンゴン(19:20)]	AM: 団内打合 PM: MM協議及び署名		AM: 団内打合 PM: MM協議及び署名 移動 [ND9110 ネピドー(18:20) → ヤンゴン(19:20)]	AM: 団内打合 PM: MM協議及び署名 移動 [ND9110 ネピドー(18:20) → ヤンゴン(19:20)] 移動 [ヤンゴン (21:45) → 機内]		ヤンゴン ネピドー
6	2015/8/7	金	移動 [機内 → 日本 (6:50)]	AM: ｲﾝｾﾌﾟｼｮﾝ・ﾚﾎﾟｰﾄ等の協議 (ミャンマーコンピュータ連盟) PM: ｲﾝｾﾌﾟｼｮﾝ・ﾚﾎﾟｰﾄ等の協議（中央銀行) データセンター評価 (Hanthawady)	AM: 情報収集(MOC) PM: 情報収集(MOI)		AM: ｲﾝｾﾌﾟｼｮﾝ・ﾚﾎﾟｰﾄ等の協議 (ミャンマーコンピュータ連盟) PM: ｲﾝｾﾌﾟｼｮﾝ・ﾚﾎﾟｰﾄ等の協議（中央銀行) データセンター評価 (Hanthawady)	移動 [機内 → 日本 (6:50)]		ヤンゴン ネピドー 機内泊
7	2015/8/8	土		移動 [ND107 ヤンゴン(11:25) → ネピドー(12:20)] 団内打合/収集資料整理	団内打合/ 収集資料整理		移動 [ND107 ヤンゴン(11:25) → ネピドー(12:20)] 団内打合/収集資料整理			ネピドー
8	2015/8/9	日		収集資料整理			収集資料整理			ネピドー
9	2015/8/10	月		AM: 情報収集(MOCO) PM: 情報収集(MOH)						ネピドー
10	2015/8/11	火		AM: 情報収集(NDH) PM: データセンター訪問（Dekhina）					移動 [東京(11:00) → ヤンゴン (15:40)] 移動 [ND123 ヤンゴン(19:30) → ネピドー(20:25)]	ネピドー
11	2015/8/12	水		AM: MCIT副大臣表敬訪問 PM: 収集資料整理			AM: MCIT副大臣表敬訪問 PM: データセンター評価	Webサイト 脆弱性診断	電子文書管理システム 脆弱性診断	ネピドー
12	2015/8/13	木		AM: 団内打合 PM: ADBヒアリング	AM: 団内打合 PM: ADBヒアリング MONPED		AM: 団内打合 PM: ADBヒアリング		AM: 団内打合 PM: ADBヒアリング 電子文書管理システム脆弱性診断	ネピドー
13	2015/8/14	金		AM: 団内打合 PM: 情報収集(MPT)					AM: 団内打合 PM: 情報収集(MPT)	ネピドー
14	2015/8/15	土		団内打合					団内打合	ネピドー
15	2015/8/16	日		団内打合					団内打合	ネピドー
16	2015/8/17	月		補足調査					補足調査	ネピドー
17	2015/8/18	火		データセンター調査(S12ビル)	予備検討	予備検討	データセンター調査(S12ビル)		データセンター調査(S12ビル)	ネピドー
18	2015/8/19	水		補足調査 移動 [ND122 ネピドー(18:30) → ヤンゴン(19:25)]	予備検討	補足調査 移動 [ND122 ネピドー(18:30) → ヤンゴン(19:25)]	補足調査 移動 [ND122 ネピドー(18:30) → ヤンゴン(19:25)]		補足調査 移動 [ND122 ネピドー(18:30) → ヤンゴン(19:25)]	ネピドー ヤンゴン
19	2015/8/20	木		AM: 情報収集(ITIP) PM: 情報収集(ヤンゴン工科大学) 情報収集(KOICA)	予備検討	AM: 情報収集(ITIP) PM: 情報収集(ヤンゴン工科大学) 情報収集(KOICA)	AM: 情報収集(JICA) PM: 情報収集(ヤンゴンコンピュータ大学) 情報収集(RONETZ)		AM: 情報収集(JICA) PM: 情報収集(ヤンゴンコンピュータ大学) 情報収集(RONETZ)	ネピドー ヤンゴン
20	2015/8/21	金		AM: 日本人材開発センター PM: Workshop参加(World Bank) 情報収集(World Bank)	予備検討	AM: 日本人材開発センター PM: Workshop参加(World Bank) 情報収集(World Bank)	AM: 情報収集(RedLink) PM: 情報収集(Vision to Motion Myanmar Co., Ltd.)		AM: 情報収集(RedLink) PM: 情報収集(yatanarpon)	ネピドー ヤンゴン
21	2015/8/22	土		AM: 情報収集(Fujitsu) PM: 移動 [SO102 ヤンゴン(18:00) → ネピドー(18:50)]	予備検討	AM: 情報収集(Fujitsu) PM: 移動 [SO102 ヤンゴン(18:00) → ネピドー(18:50)]	AM: 情報収集(Fujitsu) PM: 移動 [SO102 ヤンゴン(18:00) → ネピドー(18:50)]		AM: 情報収集(Fujitsu) PM: 移動 [SO102 ヤンゴン(18:00) → ネピドー(18:50)]	ネピドー
22	2015/8/23	日		団内打合				移動 [東京(11:00) → ヤンゴン (15:40)] 移動 [SO102 ヤンゴン(18:00) → ネピドー(18:50)]	団内打合	ネピドー
23	2015/8/24	月		AM: 団内打合 PM: 情報収集(MCIT)		AM: 団内打合 PM: 現地終了時報告会用資料作成	AM: 団内打合 PM: Webサイト脆弱性診断			ネピドー
24	2015/8/25	火		現地調査終了時報告会用資料作成						ネピドー
25	2015/8/26	水		現地調査終了時報告会用資料作成						ネピドー
26	2015/8/27	木		AM: 現地調査終了時報告会 移動 [UB104 ネピドー(18:10) → ヤンゴン(19:00)]				現地調査終了時報告会 移動 [UB104 ネピドー(18:10) → ヤンゴン(19:00)] 移動 [ヤンゴン (21:45) → 機内]	現地調査終了時報告会 移動 [UB104 ネピドー(18:10) → ヤンゴン(19:00)]	ヤンゴン 機内泊
27	2015/8/28	金		PM: 調査結果報告及び帰国挨拶（JICAミャンマー事務所） 調査結果報告及び帰国挨拶（在ミャンマー日本大使館） 移動 [ヤンゴン (21:45) → 機内]				移動 [機内 → 日本 (6:50)]	PM: 調査結果報告及び帰国挨拶 （JICAミャンマー事務所） 調査結果報告及び帰国挨拶 （在ミャンマー日本大使館） 移動 [ヤンゴン (21:45) → 機内]	機内泊
28	2015/8/29	土		移動 [機内 → 日本 (6:50)]	移動 [機内(7:30) → 機内]	移動 [機内 → 日本 (6:50)]	移動 [機内 → 日本 (6:50)]		移動 [機内 → 日本 (6:50)]	機内泊
29	2015/8/30	日			移動 [機内 → ボツワナ]					

第3章　情報通信分野基礎情報調査

3.1　一般情報

3.1.1　地勢

「ミ」国は東南アジアのインドシナ半島西部に位置し、北緯 10 度から 28 度にまたがる南北に長い国土が特徴の国である。国土の東側は中国、タイ、ラオス、西側はインド、バングラディッシュとそれぞれ接し、国境の総延長距離は約 4,600km に達している。国土の南側はインド洋に属するマルタバン湾とベンガル湾とに面しており、海岸線の全長は約 2,000km である。総面積は 676,578km^2 であり、そのうち 19.2%が耕地として利用されている。

国土の東と西を分かつように、二つの山並みとそれらに挟まれたエーヤワディ川が北から南に縦断している。エーヤワディ川の河口付近には広大なデルタ地帯が形成されている。このデルタ地帯は肥沃な土壌と豊富な水資源により最大の米の産地となっている。また、東側にはサルウィン川が流れている。サルウィン川はチベットを源流とし、中国雲南省を通過し「ミ」国北東部のシャン台地に流れマルタバン湾に到達する。急流が多く船の航行が制限されているため、流域では経済的な効果は期待されていない。

「ミ」国は山岳地帯及び大小無数の河川によりエーヤワディ川を境に東西に分断されている。この地形的条件により、国内のインフラはエーヤワディ川に沿って南北に発達してきた。道路や鉄道等の主要幹線はヤンゴンからマンダレー間に整備され、主要幹線から東西方向に支線が延びている。南北方向を結ぶ主要幹線は古くから流通の中心となっている一方で、東西方向は山岳地帯及び無数の河川により分断され、インフラの発達が阻害されている。

3.1.2　気候

国土の大半が熱帯又は亜熱帯に属し、大きく 3 つの季節が移り変わっている。4 月と 5 月は酷暑期、6 月から 10 月中旬までは雨期、10 月下旬から 3 月までは乾期である。6 月から 9 月は湿った温かな風が吹き込む南西モンスーンの影響を強く受け、曇りや雨の日が多く高温多湿の夏となる。12 月から 4 月は乾いた空気を運ぶ北東モンスーンの影響を受け、晴れの日が多く雨が少ない。ただし、「ミ」国は南北に長く高低差も大きいため気温や降水量は地域差がある。特に北部には標高 3,000 メートルを超える地域があり、この辺りはツンドラ気候となっている。

「ミ」国では、雨期になると多量の降雨により数多くの災害が引き起こされている。チンドウィン川、エーヤワディ川、サルウィン川流域では、毎年のように洪水災害が発生している。近年では、2015 年 7 月中旬から続く豪雨が大規模な洪水災害に発展した。これにより、テイン・セイン大統領はチン州、ラカイン州、サガイン管区、マグウェ管区の 4 つの地方行政区に対し非常事態宣言を発している。この洪水災害による被害は、死者 100 名以上、被災者 160 万人、避難者数 38 万世帯にのぼっている（Myanmar: Floods Emergency Situation Report No. 5 as of 21 August 2015）。

また、プレモンスーン（4 月～5 月頃）、ポストモンスーン（9 月～10 月頃）と呼ばれる時期はベンガル湾上にサイクロンが発生しやすい。通常は、バングラディッシュやインド側へ移動していくが、2008 年 4 月に発生したサイクロン・ナルギスのように、稀に「ミ」国に上陸することがある。サイクロン・ナルギスは死者・行方不明者 10 万人を超す甚大な被害をもたらした。

3.1.3　社会・人口

1948 年、イギリスから独立しビルマ連邦が誕生した。当時の首都はヤンゴンだが、2006 年に地理的な優位性を考慮し、首都をネピドーへ遷都した。数回の国名変更を経て、2010 年から正式国名がミャンマー連邦共和国となる。

国内には 100 以上の民族が暮らしており、人口の 68%をビルマ族、残り 32%を少数民族が占めている（シャン族 9%、カレン族 7%、ラカイン族 4%、華人 3%、印橋 2%、モン族 2%、その他 5%）。民族間の差別問題や争いは少ないが、一部の民族は国籍が与えられていないといった問題を抱えている。ラカイン州に多く住むロヒンギャ族の場合は「ミ」国内ではバングラディッシュ移民とみなされており、「ミ」国の国籍をもてない状況である。ロヒンギャ族は「ミ」国では少数派であるイスラム教徒であり、近年、仏教徒との間で衝突が起き迫害を受けている。なお、宗教については、国民の 90%近くが仏教徒であり、その後にキリスト教徒 4%、イスラム教徒 4%、その他 1%と続く。

出所：d-maps.com

図 3.1-1　「ミ」国地図

「ミ」国は 7 つの管区域と 7 つの州、そして連邦直轄区域である首都ネピドーに分かれている。官区域と州は同等の地位を有しているが、ビルマ族が多く住む地域を官区域、少数民族が多く住む地域を州として区分している。州の名は、その地域に住む主たる民族から名付けられている。官区域、州別の人口は表 3.1-1 に示すとおりであり、「ミ」国の総人口は、50,279,900 人となる。また、人口密度は 74.3 人/km^2 である。

表 3.1-1　行政区分別の人口

No.	管区/州/連邦地区	人口（人）
1	エーヤワディ管区	6,184,829
2	ザガイン管区	5,325,347
3	タニンダーリ管区	1,408,401
4	バゴー管区	4,867,373
5	マグウェ管区	3,917,055
6	マンダレー管区	6,165,723
7	ヤンゴン管区	7,360,703
8	カチン州	1,642,841
9	カヤー州	286,627
10	カレン州	1,504,326
11	シャン州	5,824,432
12	チン州	478,801
13	モン州	2,054,393
14	ラカイン州	2,098,807
15	ネピドー連邦地区	1,160,242
合計		**50,279,900**

出所：Ministry of Immigration and Population ″The 2014 Myanmar Population and Housing Census The Union Report Census Report Volume2″

3.1.4 経済動向

1988 年に国軍のクーデターにより軍事政権が成立し、外国投資法の制定等経済開放政策を推進した。この政策による非現実的な為替レートや硬直的な経済構造等が経済発展を妨げ，外貨不足が顕著化した。2003 年には民間銀行や一般企業が深刻な資金不足に見舞われた。さらに、アウン・サン・スー・チー氏の拘束に対して米国が対ミャンマー経済制裁法を制定、これが国内産業への打撃となった。2004 年には「ミ」国の民主化状況に進展が見られないことを理由に、EU が「ミ」国の国営企業への借款の禁止等を含む制裁措置の強化を決定した。2007 年には政府によるエネルギーの公定価格引き上げが大規模なデモを誘発し、このデモ参加者に対する「ミ」国政府の実力行使に対して，米国・EU は経済制裁措置の強化、豪州は金融制裁措置を取った。軍事政権時代の経済政策の失敗並びに各国からの経済制裁により、「ミ」国経済は長らく低迷を続けていた。

しかし、2010 年にアウン・サン・スー・チー氏の自宅軟禁を解除、2011 年には現テイン・セイン政権が発足し民政移管が実現すると、欧米諸国は「ミ」国が進めている政治・経済改革を評価し，米国は 2012 年に宝石一部品目を除く「ミ」国製品の禁輸措置を解除，EU も 2013 年に武器禁輸措置を除く対「ミ」国経済制裁を解除している。テイン・セイン政権は民主化に向けて、為替レート統一化に向けた管理変動相場制の導入、外国投資受入の円滑化にむけた外国投資法の改正等に取り組んでいる。

「ミ」国の実質 GDP 成長率は 6～8%程度で成長を続けており、GDP の内訳をみると、国民の 70%が従事する農業セクターの割合が高い。近年、徐々にその割合を下げてはいるが、毎年 30%以上を占める「ミ」国の主要産業となっている。これに次いで製造業と商業がそれぞれ 20%程度の割合を占めている。GNI については、以前は後発開発途上国を認定するための基準の一つである「一人当たり GNI（2008-2010 年平均）：992 米ドル以下」を満たしていたが、2011 年以降 1,100 ドルを超え、その後も成長を続けている。

表 3.1-2　「ミ」国の主要経済指標

項目	2010/11	2011/12	2012/13	2013/14※1	2014/15※2
実質 GDP（kyats）	39,847	43,368	47,851	54,756	63,323
実質 GDP（10 億ドル）	49.6	56.2	55.8	56.8	65.3
実質 GDP 成長率（%）	5.9	7.3	8.3	7.7	8.3
国民一人当たり GNI（ドル）	799	1,107	1,164	1,183	1,270
GDP 内訳（%）※3					
農業	36.9	32.5	30.5		
鉱業	0.9	5.8	6.1		
製造業	19.9	19.7	19.9		
電気・ガス・水	1.1	1.0	1.2		
建設	4.6	4.7	4.9		
商業	20.0	19.3	19.4	―	
運輸・通信	12.4	12.8	13.3		
金融	0.1	0.1	0.2		
行政	2.3	2.1	2.6		
その他	1.9	1.9	2.1		

※1　見積り値　※2　予測値 ※3　GDP内訳（%）はAsian Development Bank “Key Indicators for Asia and the Pacific 2014　より試算

出所：International Monetary Fund “IMF Country Report No. 14/307 October 2014

3.2　インターネット関連データ

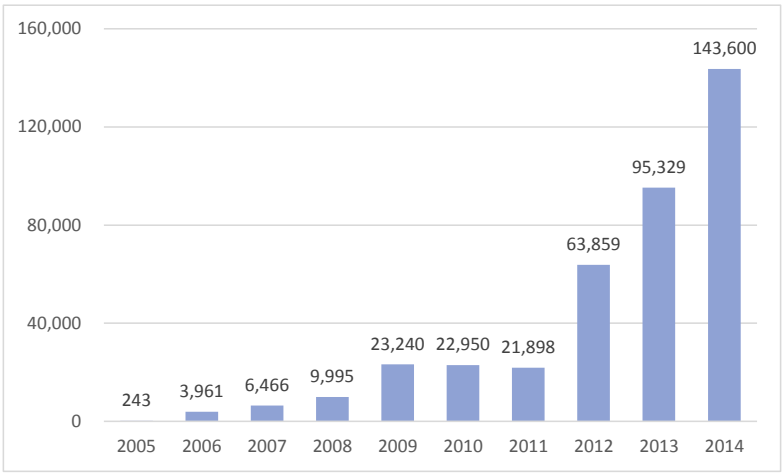
2014 年時点での固定回線インターネット利用者数の統計情報では接続可能範囲や利用料金が高額である等の課題から人口の 1%未満と少数であるが、実際には急増する携帯電話のデータ通信などにより上昇している。また、ネットカフェや無料の Wi-Fi スポットの普及により統計上現れない利用者も拡大している。

利用料金について、ビジネス用途を想定した定額で高額なプランも提供されているが、携帯電話のデータ通信の利用料金は従量制で少額から利用できるよう設定されており、近年の利用者増加を促進している。

これらの利用者拡大の傾向はサイバー攻撃の対象を広げるのみならず攻撃元の多様化とそれに伴う被害の拡大にも繋がっており、インターネットに関わるキュリティ対策の重要性も増すものと考えられる。

3.2.1　インターネット利用者数の推移

「ミ」国におけるインターネット利用者数は 2005 年時点では 243 件で、2011 年の 21,898 件まで一定の成長を続けていたが、2012 年に 63,859 件と前年比 3 倍近くに急増し、2014 年には 143,600 件まで成長している。しかし、約 6300 万人の人口比で見た場合は 1%未満で成長途中であるもののまだ普及している状態には至っていない。

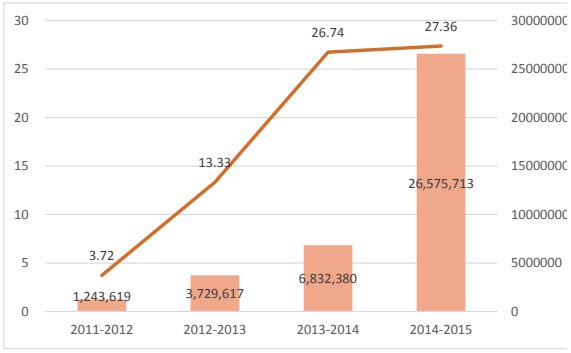


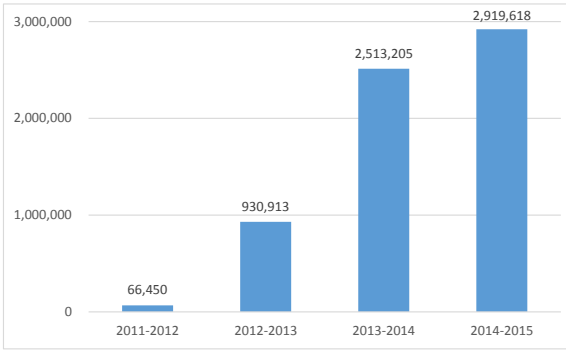
出展：ITU [ICT Statistics]

図 3.2-1　固定回線インターネット利用者数の推移

これらインターネット接続はインターネットカフェやレストランなどの無料の公衆 Wi-Fi サービスとして提供されており、日常的にインターネットをできる利用者数は統計上の数値よりも相当数多いと考えられる。

MCIT 公表値より、2013 年から 2014 年にかけてインターネットの回線速度が改善されたことを受けて携帯電話加入者のデータ通信利用者が急激に増加したことによって国内のインターネット利用者数が約 292 万人規模まで増加したと分析している。





出展：MCIT [Ministry of Communications and Information Technology of the Republic]と ITU [ICT Statistics]より作成

図 3.2-2　インターネット回線速度(Gbps)と携帯電話利用者数の推移

図 3.2-3　インターネット利用者数の推移

3.2.2 インターネット利用料金

固定回線のインターネット利用料金について、MPT と RedLink の提供しているサービスを以下に整理する。インターネット接続には初期費用と月額使用量が発生し、月内の通信量に制限はない。光回線については 100Mbps と高速回線まで提供されているが、提供可能なエリアが限られており、同等の速度ではないが DSL や WiMax などの接続形態も提供されている。

表 3.2-1　インターネット利用料金

事業社	接続形態	回線容量	初期費用[MMK]	月額[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

現在「ミ」国では 2G と呼ばれる GSM、CDMA 方式と 3G と呼ばれる W-CDMA 方式によりサービスを行っている。携帯電話によるインターネットの使用については、まず携帯電話に加入の上データ通信サービスを利用する必要がある。SIM カードを購入することで携帯電話の加入となるが、その金額は、MPT、ooredoo、Telenor の 3 社ともに 1,500 チャットで販売しており、通信料は MPT の場合 7.5 チャット/1MB で提供している。その他、通信料 400MB で 2800 チャット、1GB で 6500 チャットといったパッケージなども準備されており、各社より提供されている。

3.3 インターネットの利用状況

3.3.1 電子行政手続き

「ミ」国の行政機関では、内部事務はもとより、市民向けの行政サービスは対面、紙文書でのやり取りが中心である。2000 年代初頭から電子政府化への取り組みが行われており、電子ビザ、電子パスポート、スマート・スクール、電子調達、貿易 EDI などの様々なパイロット・プロジェクトが官民協力で行われ、莫大な費用が投じられてきたが、省庁内の行政手続きや省庁間のフレームワークが明文化されてないことなどが電子化の障壁となっており、本格導入に至ったものはわずかである。現在でも「ミ」国政府は、電子政府化を積極的に推進しており、ADB の支援により「Myanmar e-Governance ICT Master Plan 2015」を作成中(4.3 節 サイバーセキュリティ戦略、政策、法令、ガイドライン参照)であるが、電子政府に対する法令やガイドラインが存在しないため、省庁間の連携が取れておらず、各省庁において調達が非効率的、予算の検討が進まないなどの問題が起こっている。

現在行われている代表的な電子行政手続きの例として、出入国管理・人口省が提供している電子ビザサービス、商務省が提供しているオンライン会社登記サービスなどが挙げられる。これらは登録から支払いまですべてオンラインで行うことが可能である。また、他省庁においても電子行政を進める取り組みは進められており、教育省では、教育ポータルサイトの立ち上げを計画しており、また商務省では輸出入ライセンスのオンライン発行の計画を進めているなど、今後各省庁から様々なサービスが提供されると考えられるが、それに伴いサイバー攻撃が増加することは容易に想像できる。現在はサイバー攻撃に対して各省庁が個別で検知や対応を行っており、情報や経験が共有される仕組みもない。そのため、今後電子政府を進めていく上で、政府機関を横断し監視する GSOC の設立が望まれる。

3.3.2 電子商取引

「ミ」国では近年のインターネット接続の向上と携帯電話の急速な普及率の増加に伴い、過去数年間にわたり、特にヤンゴン市を中心に、衣料品や電化製品などをインターネットで販売するオンラインストアが増加している。ASEAN 諸国をターゲットとした大手企業だけでなく、実店舗を構えているショップ経営者や、個人でのオンラインストアサイトの立ち上げも盛んであり、大小含め数百のオンラインストアが存在している。支払いに関しては、共同組合銀行（CB 銀行）と KBZ 銀行によるモバイル&インターネットバンキングの開始や、クレジットカード決済可能なインターネット通販会社がサービス開始するなど、2014 年頃からオンライン決済が可能となる環境が急速に整備されつつあるが、依然として現金取引が主流であり、オンライン決済は認知度が低く、発展途上である。

以下に、最近の電子商取引関連の動向を示す。

表 3.3-1　電子商取引に関する動向

年	月	電子商取引に関する動向
2014	2	中央銀行（CBM）における勘定系基幹システムの開発がスタート（JICA 無償資金協力）
	7	エーヤワディ銀行がミャンマー初となるネットバンキングサービスを開始
	8	共同組合銀行（CB 銀行）と KBZ 銀行がモバイル&ネットバンキングを開始
2015	2	銀行連合（MPU）カードによるオンライン決済を一部の航空会社、ホテルで開始
	4	MPT は全国 1,380 ヶ所の郵便局を活用し、商品発送とオンライン決済サービスへの参入を計画
	5	CBM は MPU 加盟の銀行に対して、クレジットカードサービスの提供を許可
	5	クレジットカード決済可能なインターネット通販サイトとして、Zan IT Solution が電子書籍サービスを開始

年	月	電子商取引に関する動向
	6	MCIT に IT&サイバーセキュリティ局が開設される 電子商取引法の改定とサイバーセキュリティ法の法案を作成開始
	12	ヤンゴン商取引所が開設予定

出所：CICC（国際情報化協力センター）公開資料

電子商取引に関する法律として、2004 年に電子取引法 (electronic transaction law) が国家平和発展評議会により制定されている。本法の目的は以下の通りである。

① 近代的及び発展した国家建設のための電子取引技術支援

② 電子取引技術により人的資源、経済、社会及び教育分野を含む全ての分野での更なる発展の機会を得る。

③ 電子記録及び電子データ書信の真実性及び確実性を認識し、及びそれらのコンピュータ網を使用した内外の取引の事項に関して法的保護を与える

④ 電子取引技術を使用した国内及び外国情報の同時の伝達、受信及び貯蔵を可能にする

⑤ コンピュータ網を使用した国際組織、地域組織、外国、国内外の政府部局及び組織、民間組織及び個人との効果的及び迅速な通信及び協力を可能にする。

3.4 重要 ICT システムおよび関連設備

「ミ」国政府が重要だと考える構築済み、および構築が予定されている ICT システム、データセンター、重要インフラについてヒアリングを行った。結果を以下に示す。

3.4.1 ICT システム

現在稼働している ICT システムとして、電子文書管理システム、オンラインビザ発行システム、会社登記システムなどがある。また将来的にも様々な省庁で ICT システムが計画されており、例えば、教育省が現在構築を進めている教育ポータルサービス、JICA の支援で現在導入が行われている財務省関税局への電子通関システムなど、着々と新たな ICT システム導入が進んでいる。しかし、「ミ」国政府は現在構築済み、および構築が予定されている ICT システムに対して、重要度認識はない。主な理由は以下の通りである。

◆ 各省庁を含む政府機関の ICT システムの現状を把握している組織や人物が存在しておらず、「ミ」国内で ICT システムが整理されていない。

◆ 「ミ」国における ICT システムは発展途上であり、上述したシステムや、各省庁のウェブサイトやメールシステムなどあまり多くないため、重要度を決定する必要性がないと感じてい

る。

現在の「ミ」国の急速な IT セクターの急速な発展を勘案すると、近い将来、各省庁で様々な ICT システムが次々と開発され、ミッションクリティカルシステムなど重要度がきわめて高い ICT システムが利用されることは容易に考えられる。まずは、「ミ」国政府は各省庁の ICT システムやハード・ソフト含むリソースのインベントリを作成し、現在の状況を把握・整理する必要がある。その後、「ミ」国として守るべき情報やシステムは何かという議論を行い、重要 ICT システムを決定していく必要がある。

3.4.2 データセンター

「ミ」国には政府系データセンターが現在 4 つ存在する。MPT が管理しているデータセンターがヤンゴンの Hanthawady とネピドーの Dakekina にあり、政府、民間を対象にホスティングサービスを提供している。政府機関のサーバはもともと Hanthawady データセンターを使用していたが、首都がネピドーに移転したことにより、主に保守管理などのアクセスの面から Dakekina データセンターに移動させた省庁も多い。

MCIT が管理しているデータセンターとして、S-12 ビル（MCIT の局舎の一つ）と Thayetkhon にある。S-12 ビルのデータセンターでは、電子文書管理システムと政府人事管理システムが稼働しており、Thayetkhon は軍用設備の中に入っているデータセンターであり、詳細は不明である。

局舎政府系のデータセンターの概要を表 3.4-1 に示す。また、「ミ」国初となる純民間企業による大型データセンター設立に向けて、日立製作所と MCITDC（Myanmar ICT Development Corporation CO., LTD.）が 2016 年末稼働を目指して開発中である。

表 3.4-1　政府系データセンター概要

責任組織	設置拠点	利用者	概要
MPT	Hanthawady（ヤンゴン）	政府 民間	ホスティングサービスを提供しており、主に政府機関の Web サーバが設置されている。セキュリティ対策としては FW が設置されている。ネピドーへの首都移転に伴い、Dakekina データセンターにサーバを移転した省庁も多い。
	Dakekina（ネピドー）	政府 民間	ホスティングサービスを提供しており、主に政府機関メールサーバ、Web サーバが設置されている。セキュリティ対策として、FW、メールフィルタ、アンチウィルス、IDS/IPS が導入されている。
MCIT	S-12 ビル（ネピドー）	政府	政府機関のメールサーバが設置されている。また、電子文書管理システム、政府人事管理システムが存在する。セキュリティ対策として FW、WAF、メールフィルタ、アンチウィルスが導入されている。
	Thayetkhon（ネピドー）	不明	軍が関連しているデータセンターであり、本調査中の立ち入りは許可されず、詳細は不明である。

3.4.3 重要インフラ

重要インフラとは国民の生活、および社会活動の基盤であり、日本では情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、科学、クレジット、石油の合計 13 分野が指定されている。なお、重要インフラの定義、分野については、国によって違いがあるがこれらのシステムが攻撃を受け、障害が発生した際に社会に与えるインパクトは大きく、重要インフラの防護は極めて重要である。しかし、現在「ミ」国では重要インフラの特定は行われていない。よって、まずは、ICT システムへの依存度や IT 障害発生時の影響範囲等を踏まえ、「ミ」国での重要インフラの指定を「ミ」国政府自身で迅速に行う必要がある。

第4章　サイバーセキュリティに関する現状調査

4.1　サイバーセキュリティ関連の事例・統計情報

「ミ」国におけるサイバーセキュリティ関連の事例・統計情報について調査を行った。

4.1.1 サイバーセキュリティ関連の事例

「ミ」国におけるサイバーセキュリティ関連の事例について、mmCERT が公開している情報、報道（主に WEB）及び省庁等へのインタビューにより調査を行った。いずれの情報も体系的なものではなく、また「ミ」国の ICT 普及が遅れていることもあり、得られた事例はそれほど多くなかったが、政府機関に対する大規模な攻撃や、最近では 2015 年 6 月には、大学入試試験結果のデータベースに不正アクセスがあり、データの改ざんなどが判明した事件などが報告されている。

表 4.1-1　「ミ」国におけるサイバーセキュリティ関連の事例

発生年	攻撃対象	概要
2008	政府機関	18 省庁がバングラディッシュの IP アドレスから攻撃を受けた
2010	政府機関等	大統領選挙時に選挙妨害を目的としたサイバー攻撃を受けた ・約 30,000 の DDoS 攻撃 ・オフィスアワーのインターネット接続が 10 日間にわたり妨害
2012-2013	政府機関等	mmCERT によると期間中に政府機関に対する様々な攻撃が観測されている ・標的型 DDOS/DoS 攻撃 ・標的型 E-mail 攻撃 ・Web 改ざん ・SPAM E-mail ・フィッシング ・SNS 等によるよるプライバシー侵害
2015	教育省	教育省の大学入試試験結果のデータベースに不正アクセスがあり、データの改ざんなどが判明
2015	議会メンバー	ミャンマーのハッカーグループ”New Generation Wave”の不正アクセスによるミャンマー議会の議員の電子メールレコードの窃盗

出所：mmCERT, ”About mmCERT (Our Issue, Challenges & Initiatives)”、
Myanmar Hacker Attacks News Feed（http://hackerattacks.einnews.com/country/myanmar）、他

4.1.2　サイバーセキュリティ関連の統計情報

「ミ」国におけるサイバーセキュリティ関連の統計情報については mmCERT が調査した情報が公的なものとしては唯一である。

「ミ」国において mmCERT が対応したサイバーセキュリティ関連のインシデントは、過半（67%）がマルウェアで、既知の脆弱性の探査（24%）とあわせると大半（91%）を占めている。

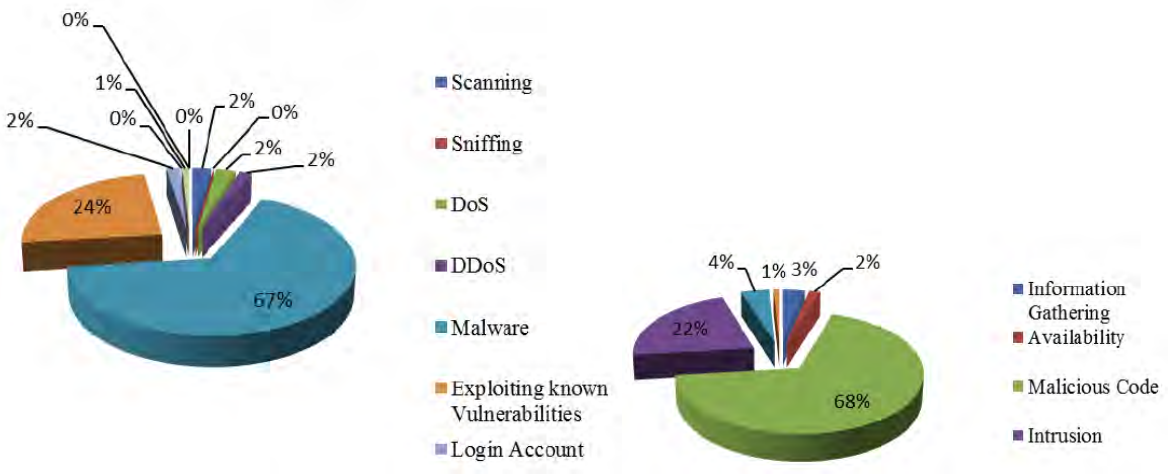


図 4.1-1　mmCERT が対応したサイバーセキュリティインシデント
左：インシデントのタイプ　右：インシデントのカテゴリ

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

また JPCERT/CC の TSUBAME プロジェクトによって設置されたセンサーを用いて、mmCERT が観測したサイバー攻撃の発信元は、中国が 60%と過半を占め、次いで米国からの攻撃が 15%を占め 2 位であった。JPCERT/CC が日本に設置した TSUBAME センサーで観測した結果でも、中国が 1 位、米国が 2 位となっており、大きな傾向に差は無い。

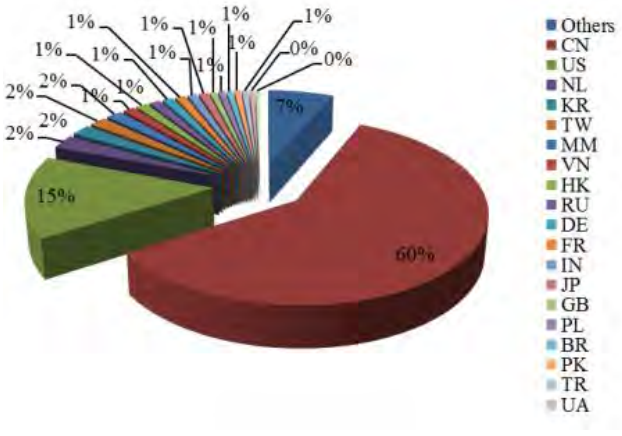


図 4.1-2　mmCERT が観測したサイバー攻撃の発信元

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

4.2　サイバーセキュリティに関連する組織

4.2.1　サイバーセキュリティに関連する組織及び相関

「ミ」国にはサイバーセキュリティに係る組織が多数存在し、それぞれが単独あるいは連携してサイバーセキュリティ対策の強化に努めている。サイバーセキュリティに関連する組織及び各組織の相関関係を図 4.2-1 に示す。

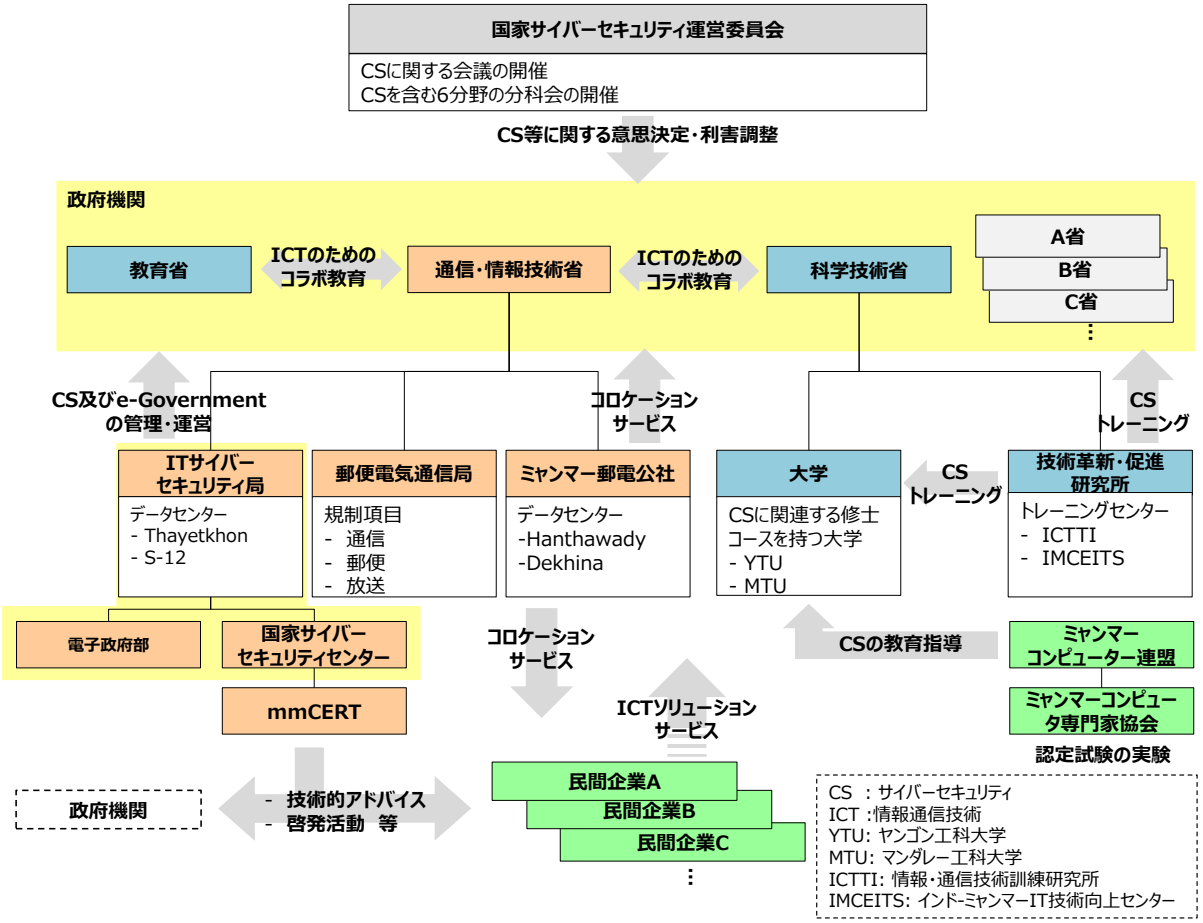


図 4.2-1　組織相関図

2013 年に省庁横断的に設立された国家サイバーセキュリティ運営委員会は、サイバーセキュリティに関する上級委員会である。同委員会では、サイバーセキュリティやサイバー犯罪に関する意思決定や利害調整を行っている。

「ミ」国の情報通信を主管する MCIT の一部局であるミャンマー郵電公社（Myanmar Posts and Telecommunications 、以下、MPT）は、政府や民間企業を対象にホスティングサービスを展開している。同じく MCIT の一部局である IT&CS は下部組織に国家サイバーセキュリティセンターと e-Government 部をもち、それぞれ政府機関におけるサイバーセキュリティ対策と e-Government の管理・運営を行っている。そして国家サイバーセキュリティセンター傘下である mmCERT は、政府機関や民間企業に対して啓発活動やサイバー攻撃に関する技術的なアドバイス等を行っている。

「ミ」国の教育を主管する科学技術省及び教育省は、傘下に複数の大学やトレーニングセンターをもち、これらを通じて人材育成を実施している。教育省傘下の大学では、人文・科学系、科学技術省傘下では技術系と専門が分かれている。そのため、IT 技術に関係する専門知識は、科学技術省が主管する大学で修学することなる。

科学技術省傘下の技術革新・促進研究所は学生や政府職員を対象にサイバーセキュリティに関する教育・トレーニングを行い、「ミ」国の技術レベルの底上げに努めている。また、科学技術省並びに教育省は、MCIT と共同で教育・トレーニングを実施している事例もある。情報通信を主管する MCIT と教育を主管する科学技術省及び教育省が相互に協力し合うことで、効果的・効率的な活動となっている。

民間企業 30,000 社の登録を有する民間団体のミャンマーコンピュータ連盟も同様に、学生や政府職員を対象にサイバーセキュリティに関する教育・トレーニングを行っている。同連盟はさらに資格試験の実施や証書発行付きのトレーニングを行い、サイバーセキュリティを担う人材の地位向上に貢献している。

4.2.2 国家サイバーセキュリティ運営委員会

「ミ」国では 2013 年の通信法改正に伴い通信市場が開放され、インターネット利用者数、ブロードバンド利用者数、携帯電話利用者数が増加した。一方で、サイバー犯罪・攻撃も増加傾向にあるため、サイバーセキュリティ対策の重要性が高まっている。このような状況において「ミ」国は同年、サイバーセキュリティ対策やサイバー犯罪に関する意思決定及び利害調整を行う組織として、国家サイバーセキュリティ運営委員会を設立した。同委員会は MCIT の大臣が議長を務め、政府関係者、民間関係者含めた 16 名が所属しており、「ミ」国のサイバーセキュリティにおける上級委員会として位置付けられている。

主な活動は 2 ヶ月に 1 回程度のサイバーセキュリティに係る会議の開催、また、会議から派生した分科会の開催である。ただし、当該委員会の開催実績は確認できていない。

一方、国家サイバーセキュリティ運営員会は各省庁等の実務者レベルで分科会を設置しており、サイバーセキュリティやサイバー犯罪を含めた計 6 種類のテーマを議論している。

複数の省庁関係者や民間企業から構成される国家サイバーセキュリティ運営委員会は、省庁横断的な決定が可能となるため、同委員会により重要インフラの特定を行うことが望ましいと言った意見もある反面、活動している実態が見え難いという批判もあり、具体的な影響力は不明である。

4.2.3 情報通信セクター

「ミ」国の情報通信を主管する組織である MCIT は、情報通信に関する政策立案、通信サービスの管理監督、各種免許の付与、通信システムに関する標準化等を行っている。2015 年の組織改編により、現在は図 4.2-2 に示す組織構成となっており、MCIT は以下の 4 つの局から構成される。

- 移動体通信、固定通信、海外通信等と行う通信事業体である MPT
- サイバーセキュリティに関する開発を行う IT&CS
- 郵便、通信、放送分野の規制を行う郵便電気通信局
- 郵便事業体であるミャンマー郵便

IT&CS は以下の 6 つの部から構成される。そして国家サイバーセキュリティセンターの下部組織には mmCERT が存在する。mmCERT はインシデントの報告を受けその解析、対策検討等を行う組織で、「ミ」国には現在 mmCERT だけであり、民間企業に対する調整機能も有しているものである。

- 政府のサイバーセキュリティを所掌する国家サイバーセキュリティセンター（配下に mmCERT）
- 電子政府の運営・管理を担う電子政府部

- 全省庁職員を対象としたトレーニングセンターを管理・運営するトレーニングセンター部
- 法務や国際協調を担う法務・国際連携部
- 組織の管理運営や財務を担う総務・財務部
- 衛星通信を所掌する衛星通信部

上記のうち、MPT、IT&CS またその下部組織である国家サイバーセキュリティセンター並びに電子政府部そして mmCERT は、サイバーセキュリティと関連が強い組織である。

なお組織改編以降、MCIT の局長が不在のため、現在は局次長である Chit Wai 氏（2015 年 8 月時点）がその役職を兼任している。

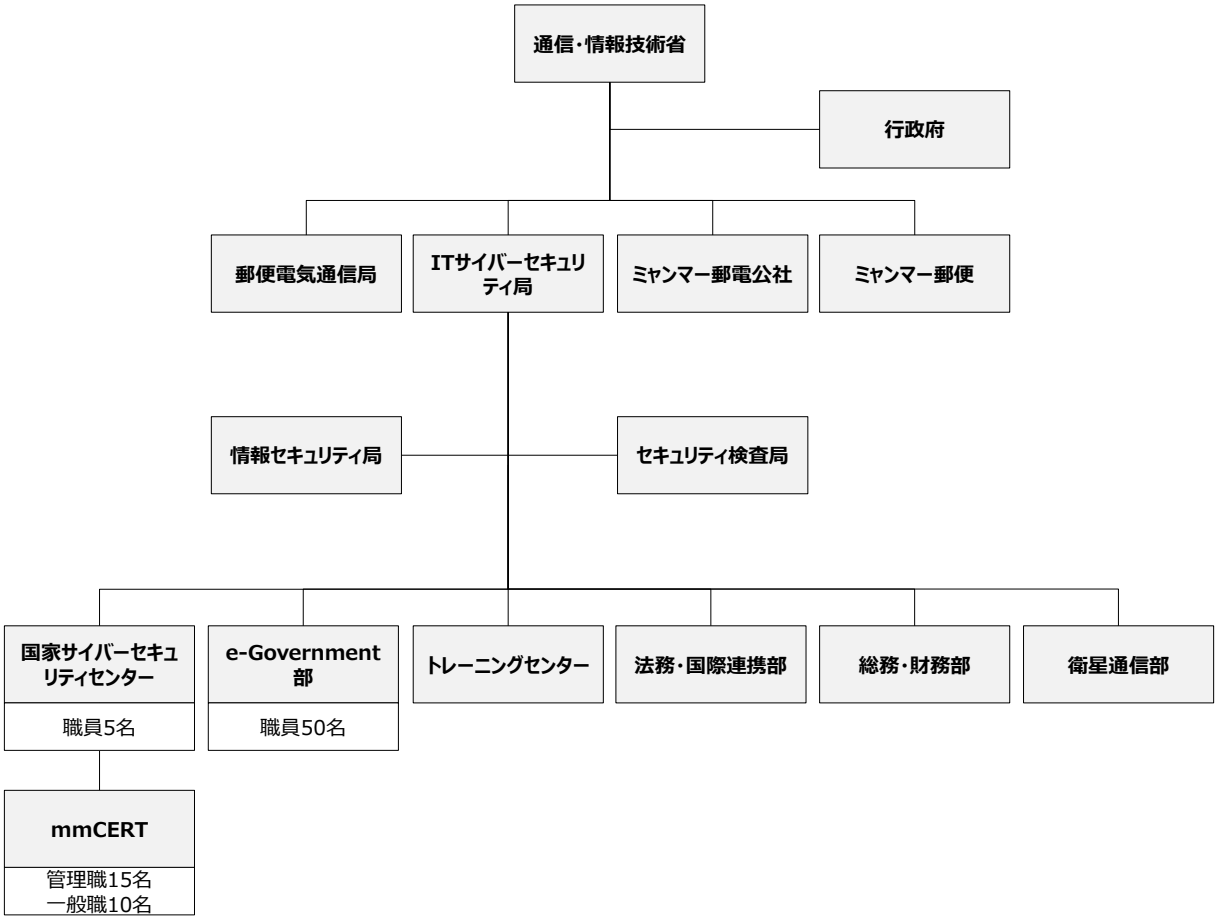


図 4.2-2　MCIT 組織図

MPT はヤンゴンにあるハンタウディとネピドーのデッキーナにデータセンターを所有しており、KSGM（KDDI 株式会社と住友商事株式会社の合弁会社である KDDI SUMMIT GLOBAL SINGAPORE PTE. LTD.が「ミ」国に設立した子会社）とのジョイント・オペレーションにより政府や民間企業に対しホスティングサービスとして場所、電源、ネットワーク等の提供を行っている。セキュリティ対策としてファイアウォールによる基本的な対策を講じているが、それ以上の対策は利用者それぞれが講じることとしている。一方で、利用者は予算、人材、セキュリティポリシーがない等の理由から適切なセキュリティ対策を講じられていないのが現状である。

なお、MPT は 2016 年度に民営化を予定している。

IT&CS は下部組織に国家サイバーセキュリティセンターと電子政府部をもち、それぞれ政府機関のサイバーセキュリティ対策や電子政府の管理・運営を行っている。さらに、ネピドー郊外のテッコンとネピドーの S-12 ビルにデータセンターを所有し、S-12 ビル内のデータセンターでは電子文書管理システムや政府職員管理システムの運用を進めている。もともと、MPT の下部組織である IT 局内にインターネットや電子政府の管理運営を行う組織が存在していたが、2010 年の選挙時に発生した DDoS 攻撃が契機となり、当該 IT 局の組織的な見直しと強化が行われ、MPT のもとに IT&CS が設立された。その後、2015 年 4 月の組織改編時に MPT は MCIT から独立した組織となり、IT&CS は、MPT 配下ではなく、MCIT の中に残された。

なお、現在の MPT 配下の IT 局は、主に MPT の ERP（Enterprise Resource Planning）に関する業務を行う組織となっている。

IT&CS には独立時に MPT の職員数十名が異動しており、現在は職員 60 名の組織となっている。このうち約 50 名は電子政府部に所属し、残る職員のうち 5 名は国家サイバーセキュリティセンターに所属している。現状では電子政府部に人員が偏っており、国家サイバーセキュリティセンターは人材不足により十分に活動できていない状況である。そのため今後、IT&CS 内で人員の配置替えを行い、さらに MPT からの異動により将来的に IT&CS の職員を 300 人程度まで増員予定である。

他方、ヤンゴンにある mmCERT は、インシデントに関する報告を受け付け、それを解析し再発防止の対策検討・技術的な助言を行う組織であるが、ヤンゴンにあるデータセンターの監視を行っており、ネピドーにあるデータセンターの監視は行っていいないため、実質、民間企業に対する助言等の役割が主なものである。以前は科学技術省の傘下だったが、組織改編以降、国家サイバーセキュリティセンターの傘下となっている。現在の mmCERT は管理職 15 名、一般職員 10 名で構成されている。また、活動に必要な資金は MCIT から割り当てられている。しかし現状は人材・資金不足のため十分に活動できていない。

4.2.4 情報通信分野における人材育成機関

「ミ」国の教育を主管する科学技術省及び教育省は、傘下の大学及びトレーニングセンターを通じて情報通信分野における人材育成を実施している。

科学技術省は、技術・職業教育局、研究・技術革新局、原子力局、技術推進・調整局、バイオテクノロジー材料科学研究局の 5 部局で構成されている。傘下にコンピュータサイエンス、工学、科学等の技術系の学問を専門とする大学や研究所をもち、ヤンゴン・コンピュータ大学、マンダレー・コンピュータ大学、ヤンゴン工科大学、マンダレー工科大学そしてピイ工科大学等が含まれる。なお、ピイ工科大学は技術・職業教育局の傘下であるが、その他の大学は技術推進・調整局の傘下である。現在サイバーセキュリティに特化した学科を有する大学は存在しないが、ヤンゴン・コンピュータ大学及びマンダレー・コンピュータ大学では情報通信分野に関連して、学士・修士課程でコンピュータサイエンスとコンピュータ技術の 2 コースを学ぶことができる。さらに、コンピュータ技術の博士課程ではデータ・セキュリティについて学ぶことができる。しかし、「ミ」国ではこれらの専門性を活かせる就職先の受け皿が小さいこと、他の業種と比較して賃金が低いことが影響しコースの人気は高くない。また、大学で習得できる専門知識と企業が求める人材の

専門知識のレベルに大きなギャップがあることも課題である。

科学技術省の下部組織である技術革新・促進研究所は、情報通信技術訓練センターとインド-ミャンマーIT 能力向上センターの 2 つのトレーニングセンターを有しており、それぞれ JICA の支援とインドの支援を受けて運営している。両トレーニングセンターは、数週間から数か月にわたるネットワークやソフトウェア等に関する人材育成トレーニングコースを提供している。トレーニングコースへの入学条件は大学の卒業資格を有していることであり、半年のコースで約 200,000 チャットの授業料が必要となる。ただし、授業料については NTT データ等の企業の奨学金制度を活用することができる。入学は学生だけでなく政府職員も可能であり、政府職員については授業料が無料となっている。現在、技術革新・促進研究所はトレーニングセンターとしての機能に加えて新たに研究開発の拠点となる研究棟を建設中である。将来的に研究開発テーマの一つとしてサイバーセキュリティ部門を設置する予定がある。

なお、科学技術省傘下の大学は 2016 年 4 月から教育省傘下となる予定である。

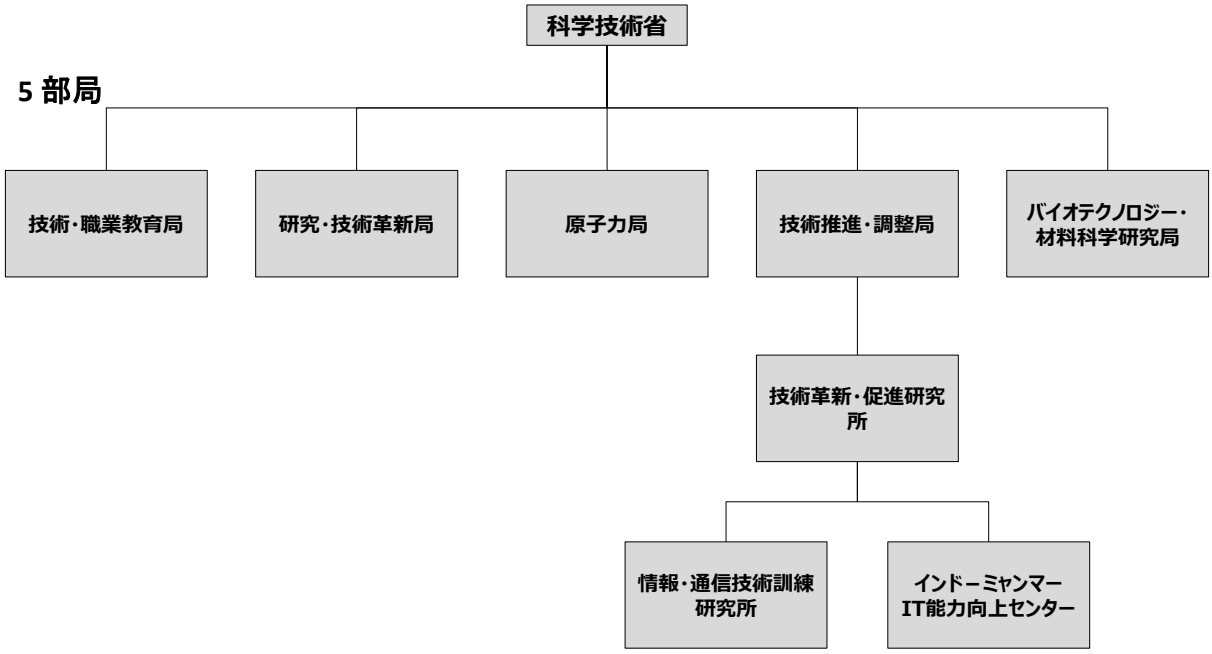


図 4.2-3　科学技術省組織図

教育省は、高等教育局、教育養成局、人材・教育計画局、基礎教育局、ミャンマー言語委員会、ミャンマー試験局、ミャンマー教育研究局の 7 部局で構成されている。傘下に人文・科学系の大学をもち、これらの大学にはサイバーセキュリティに特化したコースは存在しないが、情報通信分野に関連して電子政府システム等のコースが開設されている。

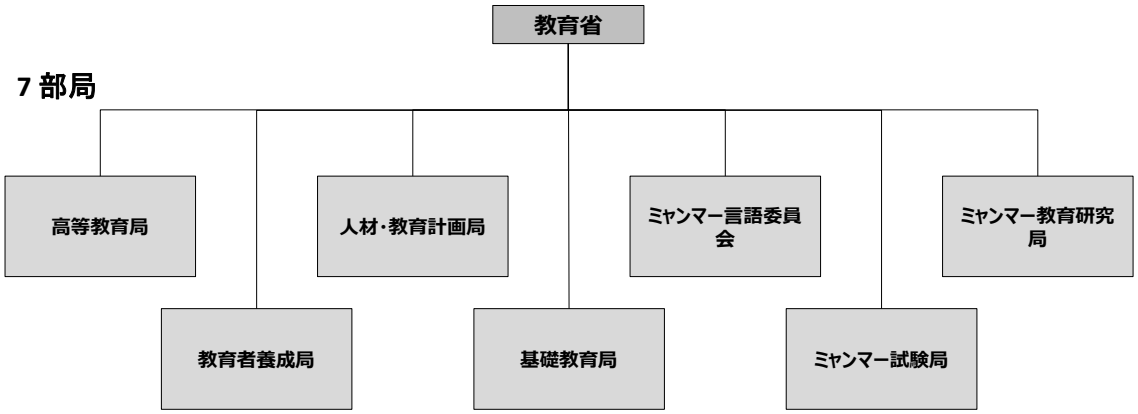


図 4.2-4　教育省組織図

4.2.5　民間企業

民間企業 30,000 社の登録を有するミャンマーコンピュータ連盟及びその下部組織の一つであり主にヤンゴンを拠点に活動するミャンマーコンピュータ専門家協会は、IT 水準の向上を目指す民間団体である。ミャンマーコンピュータ連盟の職務及び権限はコンピュータ科学開発法 24 条において以下のとおり示されている。

- 必要な委員会及び機関の組織及び当該昨日及時勢に遅れない国家のコンピュータ科学の開発の遂行
- コンピュータ科学の研究の実施、コンピュータ科学の研究実施者へ助言の提供
- 各事業分野におけるコンピュータ科学の利用の範囲拡大の促進
- コンピュータ訓練学校の講義要領及び履修過程の規定
- コンピュータ訓練学校での指導が基準を上回るか否かの判断を行うための検査
- コンピュータ科学コース、講義、競技会及び研修旅行の実行
- コンピュータ科学試験の開催及び証明書並びにメダルの授与
- コンピュータ科学の発展のために、時宜に応じた評議会への助言の提供
- コンピュータ・ハードウェア及びコンピュータ・ソフトウェアの質向上のための生産者への支援
- コンピュータ・ハードウェア及びコンピュータ・ソフトウェアの生産並びに国内外での販売支援

- 評議会の指導に従った情報技術に関する計画の策定
- 国際的コンピュータ組織との連絡
- 必要な国内外の協議会、会議、作業部会、講演会、論文発表会の開催及び代表団派遣の調整
- ミャンマー語をコンピュータで使用できるようにするためのシステムの公安の実現
- コンピュータに関する助言を求める政府部門及び政府機関に対する助言
- コンピュータに関する書籍、論文、定期刊行物及び雑誌の編集、発行及び配布
- 国内外からコンピュータに関する書籍を収集した図書館の設置
- 若者、特に学生のコンピュータの基礎知識の習得及び傑出したコンピュータ科学者の輩出を行うための貢献
- 傑出したコンピュータ科学者及び発明者への賞金の授与
- 国家による傑出したコンピュータ科学者及び発明者への名誉称号授与に関する評議会への推薦
- コンピュータ科学者及び発明者の利益保護のための評議会への助言
- 必要な委員会及び機関の組織及び当該機能及び職務の決定
- 評議会から任じられたコンピュータ科学に関する業務の遂行

同連盟は上記の規則に則って活動している。特に人材育成に注力しており、年 1 回各地域でサイバーセキュリティに関するセミナーの開催、IT の教育水準向上を目的とした教師や学生に対する指導、政府の要請を受けて数カ月にわたるトレーニングの開催等を行っている。トレーニングの内容は基礎的なものから発展的なものまで多岐にわたり、内容により証書を発行する場合もある。さらに、日本の組織である情報処理推進機構（IPA）と相互認証された資格試験も実施している。

4.3 サイバーセキュリティ戦略、政策、法令、ガイドライン

「ミ」国政府におけるセキュリティも含めた情報通信に係る政策については MCIT に任せられており、サイバーセキュリティ戦略、ポリシー及びロードマップ等については MCIT において検討作成されることとなる。これを踏まえて MCIT では、前項のとおり組織整備を行っており、IT&CS においてこれらの策定を進めることとしている。

しかしながら現状では、政府のサイバーセキュリティの土台とすべきサイバーセキュリティに係る戦略、政策、法令、ガイドライン等について、その多くが未整備の状態にある。

政府のサイバーセキュリティの基礎となる法制度の枠組みとしては、下表のような制度群が考えられる。

表 4.3-1 「ミ」国におけるサイバーセキュリティに係る法制度の枠組み

区分	整備有無	現状
サイバーセキュリティに係る基本方針・基本戦略	×	IT&CS にて策定を担当し、現在策定中としているが、策定予定時期は現時点では不明である。
サイバー犯罪に係る法制度	△	サイバー犯罪に特化した法令は規定されていないが、電子取引法及びコンピュータ科学開発法においておおまかな罰則等について規定している。
個人情報及びデータの保護に係る法制度	×	電子取引法に機密情報や名誉棄損等への罰則は規定されているが、個別の法令は規定されていない。
電子コンテンツに係る法令	○	電子取引法において、他者の利益や名誉を毀損する情報の作成・変更・配布の規制等、取り扱い情報に係る罰則が規定されている。 またコンピュータ科学開発法では海賊版コンテンツや情報の輸出入に対する罰則が規定されている。
電子取引に係る法令	○	電子取引法において電子商取引の基礎となるルールが規定されている。
青少年保護、消費者保護等に係る法令	△	青少年保護については刑法（The Penal Code）292 及び 293 条にて基本的な規定がされている。 また、消費者保護については商務省（Ministry of Commerce）から 2014 年に消費者保護法（Consumer Protection Law）が策定されている。 但し、いずれもサイバー上の特異性に配慮した規定とはなっていない

なお、「ミ」国における ICT 関連の基本的な法令のうち、特にサイバーセキュリティに関連した規定が定められている法令としては、「コンピュータ科学開発法（The Computer Science Development Law）」、「電子取引法（The Electronic Transactions Law）」及び「電気通信法（The Telecommunications Law (of 2013)）」が挙げられる。

2013 年に制定された電気通信法は、「ミ」国における通信自由化に向けて、民間の電気通信事業を認可するにあたっての事業ルール等を定めたものであり、主に免許に関する規定、通信事業者の義務と罰則などが示されているが、具体的な規定については MCIT に委ねられている。サイバーセキュリティの観点では、個人の保護に係る規定があるものの、概ね利用料金の提示等の基本的事項が中心である。

1994 年に制定されたコンピュータ科学開発法では、主にその監督機関としてのミャンマーコンピュータ科学開発評議会及び推進機関としてのミャンマーコンピュータ連盟が規定されているほか、輸出入可能なコンピュータ製品等の規定権限、ネットワークへの接続許可権限等、コンピュータの利活用に係る規制及び罰則が規定されている。

2004 年に策定された電子取引法では、電子的な契約行為がメディアに関係なく有効性を持つことを始め、電子的記録、署名及びコミュニケーションが現実界と同等の有効性を保持することを規定している。また、管理組織として電子取引管理理事会の設置を規定しているほか、法令違反者への行政処分や国家への損失、電子的な破壊・妨害行為、情報の盗用・漏えい及び名誉の既存といった一般的事項に対する罰則等が規定されている。

また国家レベルの ICT に係る開発計画（マスタープラン）として「Myanmar Telecommunications Master Plan」が World Bank の協力によりドラフトが作成され 2015 年 8 月現在においてレビューが行われており、また特に電子政府推進にフォーカスした「Myanmar e-Governance ICT Master Plan 2015」が ADB の協力により原案が作成され、既にミャンマー政府に提供されている（政府からの交付は 2015 年 8 月末現在行われていない）。ちなみに前季（2010-2015 年）の電子統治マスタープランについては KOICA の協力により策定されている。

前者においては、具体的なセキュリティとプライバシー保護に係る項目として、a)ネットワークの冗長性の構築、b)国家サイバーセキュリティポリシーの策定、c)合法的傍受に係る基準の策定、d)グレー・トラフィック[1]への対応等の必要性が指摘されている。

また後者においては、電子政府推進において必要とされるサイバーセキュリティへの取り組みとして法整備と IT ポリシーの整備が指摘されている。法整備に係る指摘（“4.2 Recommendations on amendments to ICT Law”）としては、電子政府を推進するうえで、a)政府機関相互の調整が可能で且つ予算権限に直接影響力のある推進組織の設置、b)暗号化ベースの電子署名の使用、c)知的財産権保護、重要インフラ保護、サイバー犯罪法、ソーシャルメディア利用、電子決済を含む電子商取引、プライバシー及びデータ保護、サイバー上の紛争解決方式等に係る法整備が必要としている。また IT ポリシーの整備に係る指摘（“4.7 Recommendations on IT Policies”）としては、a)技術関するポリシー（オープンな規格への対応、統一的なフレームワーク、情報セキュリティポリシー、共同利用インフラ、セキュリティ技術及び PKI 等）、b)電子サービスの提供に係るポリシー（多方式でのアクセス、電子決済等）、c)人材育成ポリシー（リテラシー及びスキル、多国間及び学術分野との協業等）、d)電子政府管理ポリシー（電子調達、予算配分、PPP、品質保証等）の整備が挙げられている。

4.3.1 サイバーセキュリティに係る基本方針・基本戦略

「ミ」国のサイバーセキュリティ戦略については、JICA より派遣された専門家が MCIT に対して支援を行いつつ立案が進められている。2015 年においてアクションプラン（案）が作成され、現在も MCIT 内部で検討が行われている。

「ミ」国の政府における ICT セキュリティポリシーの策定は、MCIT 内に新設された IT&CS にて行うこととなっているが、現段階での進行状況及び策定予定時期については明言されておらず、また当該 ICT セキュリティポリシーのスコープ等の詳細についても明確にはなっていない。進行状況及び内容が見えない要因としては、IT&CS 内のセキュリティ担当部門の組織が立ち上げ段階であり実質的に要員が不足していること、加えて旧組織に紐づいた予算で運営されているため IT&CS では独自の今年度予算を有していないこと等から具体的な検討に入れていないことが挙げ

[1] 無認可のオペレータによる通信トラフィック

られる。

今後、IT&CS では組織の補強を予定しており、その補強状況によって ICT セキュリティポリシー策定のスケジュールが見えてくるものと考えられるが、ICT セキュリティポリシーの策定においてはある程度の知識・経験を有する人材が必要であり、IT&CS においてそのような人材の確保ができるかが重要なポイントとなる。

また現在想定している ICT セキュリティポリシーがどのようなスコープのものか、具体的には政府全体に適用することを想定したものか、MCIT 内での適用を想定したものかについても現時点で明確にはなっていない。「ミ」国政府全体としては前者が必要とされているが、仮に MCIT にて策定するものが後者のとおり MCIT 内への適用を想定したものであったとしても、現時点で他府省において有効な ICT セキュリティポリシーは特にないことから、MCIT の ICT セキュリティポリシーを展開・適用することは可能である。

これらの状況を踏まえると、MCIT における ICT セキュリティポリシーの策定は「ミ」国政府におけるサイバーセキュリティ向上において重要なステップとなる。

4.3.2 サイバー犯罪に係る法制度

電子取引法及びコンピュータ科学開発法における主な規定としては以下のようなものがある。

- 国家機密、法秩序等の国家の安全保障、経済及び文化を損なう行為
- 発信、ハッキング、変更、破壊、盗用等の不正行為により損害を与える行為
- 通信の妨害、パスワードや電子署名等の成りすましや悪用行為
- 他者の利益又は名誉を毀損する情報の作成、変更又は配布等の行為
- 電子取引管理理事会の発した禁止命令に対する違反行為

これらの罰則規定は基本的な考え方であり、具体的な基準等は電子取引管理理事会が取り扱うものと考えられる。しかしながら通信キャリアから、不正行為の可能性があるアドレス等が特定できても（どこに訴えればよいのか等）対処方法が不明であるとの指摘があったとおり、実際に取り締まりが機能するための役割連携や適用基準の具体化等が必要とされる。

4.3.3 個人情報及びデータの保護に係る法制度

「ミ」国において個人情報保護に係る具体的な法制度は規定されていない。個人情報保護については、単に安全なネットワークを利用したサービスの普及に資するだけでなく、前述のサイバーセキュリティ戦略アクションプラン（案）にも示されているとおり、個人のセキュリティに対する意識向上の契機及び後ろ盾となるものであり、早期の法制化が望まれる。

一方で、データ保護について、国家の重要情報については国家機密法が制定されている。しかしながら政府機関の電子メールにおいて Gmail の一般アカウントが利用されている現状に鑑み、国家に係る情報又は重要インフラに係る情報がネットワーク上にて扱われる、更にはクラウド等の技術が活用される現在に適応した法制度のあり方について考慮する必要がある。

4.3.4 電子コンテンツに係る法制度

電子取引法において、他者の利益や名誉を毀損する情報の作成・変更・配布の規制等、取り扱い情報に係る罰則規定が記載されている。またコンピュータ科学開発法においても海賊版コンテンツや情報の輸出入に対する罰則が規定されている。更に電子コンテンツの内容に係る法令としては前述の国家機密法等も関係すると考えられ、また現在は規定がないが前述の個人情報及びデータ保護に係る法制度とも関係する。

電子コンテンツの質や内容については、基本的にはガイドライン等によって規定されるものであり、主要な罰則については既存の規定である程度担保されていると考えられる。

4.3.5 電子取引に係る法制度

前述のとおり、2004 年に電子取引法が策定されている。電子取引法の詳細は既に記載のとおりであり、「ミ」国外で電子商取引が進みつつあった 2004 年に策定されているが、同時期における「ミ」国の情報通信環境は未普及の状況にあり、比較的早期の着手であった。

策定間近といわれるカンボジアも含め、ASEAN 各国においても電子取引法の策定は既に行われており、電子取引法をベースとした電子商取引環境における ASEAN 域内での連携の観点からも重視されている。

4.3.6 青少年保護、消費者保護等に係る法制度

青少年保護については刑法において基本的な記載があり、公序良俗に反する物品等の販売、流通、輸出入といった行為の禁止に加え、20 才以下の青少年を対象にした場合の特記（厳罰化）が示されている。

消費者保護法は 2012 年に商務省から法案が提出され 2014 年に策定された。「ミ」国における消費者の保護を主たる目的としつつ、更に周辺の ASEAN 地域（5 ヶ国で同様の法令が規定されている）と連携した商環境の基盤づくりの推進も視野に入れたものとしている。

一方でこれらの法令については必ずしもサイバー空間上での事象を想定したものではないため、電子取引法等のサイバー関連法と合わせて、十分にカバーされているか等、ルールの整理を行う必要がある。

4.4 科学技術、IT 及びサイバーセキュリティに関する人材育成

「ミ」国におけるサイバーセキュリティに特化した人材育成は行われておらず、コンピュータサイエンスなどの科学技術や IT 全般の人材育成を行う中で、サイバーセキュリティに関心がある組織ないしは個人が個別にサイバーセキュリティ分野の人材育成や知見の保有を行っている。そのため本節では、サイバーセキュリティに関する人材育成ではなく、科学技術及び IT 分野における人材育成とサイバーセキュリティに特化した人材育成の現状双方について述べることとする。

さらに、政府省庁と民間におけるそれぞれの人材育成の取り組みについて述べる。

4.4.1 基礎的（理論的）な科学技術分野及び IT 分野の人材育成

「ミ」国においては、IT 及びサイバーセキュリティなど、科学技術に関する国内の人材育成については、科学技術省（Ministry of Science and Technology）が、政策・戦略の立案から、裾野教育

等までを行っている。科学技術省の役割には、国家経済の進歩につながり、研究や開発課題解決に向けた業務の執行をよりよく行うために、最先端の科学技術分野における職能工、技師、科学技術者及びその他技術者の育成がある。具体的には、以下の 6 項目となっている。

- **国家経済の発展のために、研究及び開発計画を実行すること**
- **国家資源の活用により経済の強化を行い、国民の生活レベル向上を行うこと**
- **研究や開発の進展を通じ得られる技術移転ならびに知識の共有により、農業及び工業分野における生産力を高めること**
- **科学技術分野の専門家を養うために人材育成計画及び実行すること**
- **工業原料及び最終生成物に対する実験分析、品質管理、標準化を実施すること**
- **安全対策を施した原子力エネルギーの利用に関する研究を行うこと**

「ミ」国では、コンピュータサイエンスの開発・普及に必要な実施事項を定義しコンピュータ・ソフトウェアやこれに伴う情報の輸出入を管理することを目的に、1996 年にコンピュータサイエンス開発法（Computer Science Development Law, 1996）を施行した。科学技術省では同法の施行により、2000 年 9 月以降 、ヤンゴン・コンピュータ大学（University of Computer Studies, Yangon、以下、UCSY）及びマンダレー・コンピュータ大学（University of Computer Studies, Mandalay、以下、UCSM）をはじめとする 24 のコンピュータカレッジを相次いで設立した。科学技術省が所轄する大学は他にもヤンゴン技術大学（Yangon Technological University、以下、YTU）、マンダレー技術大学（Mandalay Technological University、以下、MTU）、ピィ技術大学（Pyay Technological University、以下、PTU）があるが、UCSY 及び UCSM 等の 24 大学は IT 及びコンピュータサイエンスの単科大学・カレッジとなっている。

そのため、UCSY は「ミ」国の IT 及びコンピュータサイエンス分野をリードする存在であり、IT 分野の中高官政府職員ならびに民間企業の上位技術者の多くは UCSY を卒業している。UCSY は、学士、修士及び博士課程があり、学士・修士はそれぞれコンピュータサイエンスとコンピュータ技術の 2 コースを持つ。サイバーセキュリティに特化したカリキュラムは現在のところなく、博士課程のコンピュータ技術にデータ・セキュリティ（データの機密保護）のカリキュラムが存在するのみである。科学技術省によれば、今後 UCSY でも、サイバーセキュリティに特化した実習講座の開設を行うことになるだろうとのことである。ちなみに「ミ」国の大学がすべて国立で、大学数は、36 総合大学、112 単科大学となっている。大学の所掌は、上記の大学を含む技術系大学は科学技術省、人文・科学系等は教育省、農業系大学は農業省、医学系大学は保健省となっている。ただし、今後は、大学の所掌は教育省に統一する計画となっている。

なお、UCSY は日本の慶應義塾大学との連携により、平成 26 年～28 年で双方 2 名ずつ学生の派遣/受入れを実施・計画している。この連携は我が国文部科学省が平成 23 年から実施（日本学術振興会に委託）している「大学の世界展開力強化事業」で行っているものである。カリキュラムの内容や教員数に限りのある「ミ」国の大学では、海外の大学との連携も効果的な取り組みであると考えられる。UCSY では教授言語に英語を使用しており英語の講義に学生が適応しているこ

とも踏まえ、大学間の国際連携によりコンピュータサイエンス及びサイバーセキュリティに必要な基礎知識の習得に効果をあげられるものと期待される。

一方、教育省によると、「ミ」国全体の ICT 能力の底上げにつなげるために、ICT 関連のカリキュラムを拡充したいとの意識があるが、地方部に未電化地域が多くあることにより、全国的に ICT に関連した授業を行うことができないとしている。

また、「ミ」国内ではコンピュータサイエンス分野に関する就職機会が少なく、同分野の専攻は人気が高くない。理科系では、医療系や工学系の人気が高くなっている。今後は、IT 系を専攻するインセンティブなどを踏まえ、育成が必要な分野へ相応の対策が求められる。

4.4.2 実践的な科学技術分野及び IT 分野の人材育成の必要性

2000 年 11 月に合意した e-ASEAN フレームワークでは、「ミ」国政府は ASEAN 諸国に対し 、情報インフラの構築、電子商取引の促進、ICT 関連機器やサービスの自由化、ICT 能力（ICT Literacy）の向上と電子社会の創造、電子政府の設立について進めていくことをコミットした。これに伴い電子国家対策委員会（eNational タスクフォース、以下 e-NTF）を設立し、2004~2005 年に韓国の支援により ICT マスタープラン（2010-2015 年）を作成した。e-NTF には、ICT アプリケーション、ICT 教育、ICT インフラストラクチャー、ICT 法制度、ICT 自由化、ICT 統計、ICT 標準化の 7 つの委員会が形成されており、電子政府化（e-Government）の実現に向けた具体的施策の推進を開始している。KOICA の支援で作られた ICT マスタープランが 2015 年までを対象としているものであったため、その後、2014 年から始まった世界銀行及びアジア開発銀行（ADB）のそれぞれの支援により、ICT 化の推進や電子政府化の具体的施策が進められている。

このため、科学技術省傘下の大学が行っている理論の構築、基礎知識の習得である人材育成だけではなく、IT ならびにサイバーセキュリティを主眼に置いた実践的な人材育成が急務となっている。

4.4.3 各省庁の人材育成の取り組み状況及び技術レベル

「ミ」国政府機関による人材育成の実施状況は、基本的に統一の指針等はなく、各省庁の予算、要員状況に応じて、個別に対応しているのが実態である。そうした中で、科学技術省と MCIT が共同で IT に関する 10 週間の教育コースを政府 IT 担当職員に提供している。研修場所は科学技術省が所有するネピドーにある English Language Professional School（ELPS）を活用し、現在のところ、12～13 省庁からの参加がある。予算は、科学技術省が予算化しており、教育コースは下記の 2 つのコースになっている。ただし、サイバーセキュリティに関連する内容は含まれておらず、ファイアウォールの取り扱いについてコース B に含まれているのみとなっている。

(1) ウェブ開発：ウェブサイトの作り方、データベースの管理
(2) ネットワーク技術：基礎ネットワーク構造、ウェブサーバ、メールサーバ、ファイルサーバー

一方、mmCERT では内部の職員に対し、下記 8 項目の実践的な研修を行っている。

- システム管理
- ネットワーク管理

- マルウェア分析
- ウェブ開発
- ウェブアプリケーション侵入テスト
- 脆弱性診断
- プログラミング
- インシデント対応

mmCERT の職員は管理者が 15 名、その他職員が 10 名であり、この内、プログラムやネットワークの知識を有している専門職は 7 名のみである。実践的な内容の研修を行っているが、対象となるスタッフが少ないため効果は限定的である。人材の育成とともに人員の増強も急務である。また、建設省（Ministry of Construction）及び商務省（Ministry of Commerce）では、独自の IT 関連の人材育成を積極的に行っている。

建設省が管理するデータベースの管理・運営（次項政府のセキュリティ対策実施機関の活動状況を参照）のため、建設省内にある 4 つの部門に計画情報通信室が 2015 年 4 月に開設された。業務としては計画業務を主に行っており、IT に関する業務は少なく、4 部署に大臣室を合わせた 5 つの部署の合計 110 人の職員のうち、IT 専門担当者は各部門 4~5 人である。また省内でコンピュータを使用できる職員は 500 人程度であり、これらの職員向けに、2 か所の会場に分けトレーニングを実施している。また、民間企業のトレーニングセンターも活用している。

さらに全国のエンジニア 4,000 人の中から選抜し、コンピュータデザインやアーキテクチャデザインの教育も実施している。ただし、IT 教育を行うための知識が不足しているため、建設省では十分な研修が実施されているとは考えていない。

他方、商務省の ICT 部署には 13 人ほど所属しており、ジャーナルなどの出版に係る仕事を主に行っている。MCIT からの通達で各省は最高情報責任者（Chief Information Officer、以下、CIO）と最高セキュリティ責任者（Chief Security Officer、以下、CSO）をそれぞれ配置することになっているが、商務省内には十分な技術力を持つエンジニアが不足しているため CSO を単独で配置できず、CIO が CSO を兼任し、業務にあたっている。

商務省では 2005 年に庁舎内にトレーニングルームを作り、20 台の PC を使用して小規模なソフトウェアのトレーニングを開催している。講師は外部のソフトウェア関連会社から招いており、過去にはマレーシアから講師を招いたこともある。トレーニングは年 10 回程度行っており、受講者のレベルに合わせて複数のコースを用意している。この他、前述の MCIT と科学技術省で行っている教育コースにも職員を参加させている。

IT 担当者の中には、IT 及びサイバーセキュリティに必要な研修を行ったとしても、「ミ」国政府の職員の配置換えのため、研修で得られた知識や経験が蓄積されないことを懸念する担当者もいる。さらに、セミナーや訓練に参加しても、その後のフォローアップがないため知識・技術が定着しにくい状況にあるとも指摘する。一方、MCIT 副大臣は、持続可能なサイバーセキュリティに対する能力を身につけるためには、人材育成、能力強化が重要であるとしている。能力強化は個別のものだけではなく、組織として総合的に能力強化されることが必要としている。

4.4.4 民間の人材育成の取組

ミャンマーコンピュータ連盟（Myanmar Computer Federation、以下、MCF）は、民間企業 3 万社が登録されており、会員企業と連携しながら IT 水準向上を目指す団体である。MCF では、年に一回、各地域でセキュリティに関するセミナーを開催している。また、IT に関する教育として、高校の情報科目を扱う講師に対し教育研修を行っているとともに、学校からの要望に応じて高校生に対しても直接授業を実施している。「ミ」国政府からの要請で、2014 年には 3 ヶ月間のセミナーを実施し、さらに上級訓練も別に実施している。

一方、IT 関連の資格制度を作り、一定水準以上の技術者の確保と IT 技術者のインセンティブが得られることを考慮し、ミャンマーコンピュータ専門家協会（Myanmar Computer Professional Association、以下、MCPA）がミャンマー独自の認定試験を設けている。2002 年に制度が作られ、同年 3 月から年 1 回実施している。また海外では英国の全英消費者協議会 National Consumer Council: NCC）が実施している試験、2003 年 1 月から実施されている日本の一般財団法人海外通信・放送コンサルティング協力との相互認証試験制度もある。その他、ICT ベンダーの認定試験があり、マイクロソフト、オラクル、シスコ、IBM がそれぞれ実施している。

さらに民間のコンピュータスクールも設立されており、ヤンゴン市内だけで、約 100 校あり、「ミ」国 IT 企業大手 KMD と MCC グループが運営するコンピュータスクールの人気が高く、全国展開を行っている。ただし、一般的には理科系の中でもコンピュータサイエンス分野は他の分野より人気が低く、IT 技術者の地位向上策などにも配慮しながら、人材育成が行えるように仕組みを検討していくことが望まれる。

4.5 政府のセキュリティ対策実施機関の活動状況

4.5.1 通信・情報技術省の活動状況

MCIT は、「ミ」国政府全体のセキュリティ方針・政策を立案する機関であり、現在は、JICA 専門家の支援による第一次サイバーセキュリティ行動計画案（以下、行動計画案）の作成と MCIT 内の組織の改編に着手しているところである。

基本行動計画案は、MCIT 内の決裁が 2015 年 8 月時点で済んでおらず、大臣等への説明用に担当者がミャンマー語に翻訳を行っている段階である。9 月には大臣等への説明を終える予定としている。

一方、組織改変は第 4.2 項「サイバーセキュリティに関連する組織」に記載のとおり、大臣室、MPT 及び郵便電気通信局（Post and Telecommunications Department、以下、PTD）の 1 室 2 局体制から、MPT が実施していた部分を IT&CS、MPT 及びミャンマー郵便に分け、郵便事業及び通信事業以外の IT 関連業務は IT&CS の担当とした。また PTD については、郵便・情報通信に関する規制機関の役割だけを PTD に残し、2 局体制を 4 局体制へと改革したところである。

IT&CS の中には、総務・財務、研修、電子政府、法務・国際連携、衛星通信、国家サイバーセキュリティセンター（National Cyber Security Center、以下、NCSC）の 6 部署に分かれており、サイバーセキュリティに関しては、NCSC が統括して行うことになっている。サイバーセキュリティに関連する機能を集約し、人材育成、インシデントの対応等を一元的に行うことを狙いとしている。もともと MPT の中には IT 局があり、その下に電子政府及びインターネットの管理運用を行う組織が存在していたが、2010 年に発生した DDoS 攻撃が契機となり、IT 局の組織的な見直し

と強化が行われ、また MPT が通信事業者として独立し民営化されていくので、国家におけるサイバーセキュリティを所掌する IT&CS の設立につながった。当面の NCSC のもっとも重要な活動は、上記基本計画案を決定し、年次ごとの事業計画と予算化の作業となっている。

IT&CS がようやく出来上がったばかりであるため、「ミ」国政府関係機関のサイバーセキュリティ対策は、機材の設置、アプリケーションの導入、攻撃の検知、情報共有のための手順・ガイドライン、人材育成及び予算化など、各省庁に委ねられている。各省庁で設置しているオンラインサービス用のデータベースなど、ファイアウォールだけを設置しているだけの対応や、個別端末ベースでは、パソコンにアンチウィルスソフトをインストールするだけ、不審メールを受け取った時の対応やフリーメールアドレスの使用に関するルール、ガイドライン等が明確にされていない。

以下、第 4.5.2～4.5.11 項にヒアリングをしたその他の省庁の対応状況を述べる。

4.5.2 ミャンマー郵電公社（MPT）

これまで認識されている MPT が受けたサイバー攻撃は、上述の 2010 年の選挙時に発生した DDoS 攻撃である。また、MPT のホスティングサービスを利用している企業に対する攻撃が報告されている。サイバー攻撃の発生後、セキュリティ対策は特にその後講じていない状況である。組織改編によって MPT が管理運営するデータセンターは、ヤンゴンにあるハンタウディ（Hanthawady）とネピドーのデッキーナ（Dkekina）の 2 ヶ所のデータセンターとなった。この 2 つのデータセンターは国際通信のゲートウェイとなっており、双方により冗長構成をとっている。

またこの 2 つのデータセンターは、各省庁のオンラインサービス用のウェブサーバ、メールサーバなどが設置されており、ホスティングサービスを提供している。MPT のホスティングサービスは、機器の設置場所と電源などの設備提供という形態にしている。そのため、ファイアウォール以上のセキュリティ対策は MPT では行っていない。政府共通の電子文書管理システムや他の重要なデータは、MPT のデータセンターではなくネピドーにある他のデータセンター（S12 ビルとタッコン（Tatkon））で管理されている。ちなみに我が国の無償資金協力（通信網緊急改善計画、2012 年）で供与された機材はデッキーナに設置されているが、これまで攻撃を受けた報告はない。

4.5.3 mmCERT

mmCERT は下記の 4 つの役割を実行するため、インシデントの対処、最新の脅威・セキュリティ情報の共有、技術顧問支援、国民意識向上の促進にあたっている。mmCERT はヤンゴンに設置されており、監視はヤンゴンの MPT が所有・運営するデータセンターを対象としており、ヤンゴンのデータセンターにあるデータ以外の政府系のデータは対象外となっている。

- サイバーセキュリティ及びサイバー犯罪に対する各国 CERT との国際連携による全国的な IT ビジョンの作成
- セキュリティ情報及び勧告の発信
- 技術支援の提供
- サイバー犯罪の法執行機関との協力

そのため mmCERT では、UCSY 等の学生、企業などを対象に、サイバーセキュリティの講習を行っている。また、国民意識の向上活動として、講義、パンフレット配布の実施及びパスワードの設定ガイドライン等を作成している。

4.5.4 科学技術省 (Ministry of Science and Technology)

科学技術省のウェブサイトでは、科学技術省の基本的な情報のみ載せており、ウェブサイトを通じたオンラインサービスなどは行ってはいない。そのため、これまでサイバー攻撃を受けたことはない。

課長以上が PC を貸与され科学技術省のネットワークに接続している他、スマートフォンなどのデバイスもネットワークにつながれており、約 500 程度の端末が開学技術省のネットワークに接続している。科学技術省のウェブサーバは省内のサーバールームに設置され、FireEye というセキュリティ機材によって、web-based 攻撃、ゼロデイ攻撃等対処している。

ネットワーク管理者は毎日アラート確認・分析し、IT 部署の職員が問題解決にあたっている。加えて、深刻で重大なアラートを受けていることが確認された場合は、FireEye の提携企業ラインセンスを持つ民間会社が IT 部署の支援にあたることになっている。

電子政府化の推進に伴い、現在、科学技術省の職員のみ閲覧できるシステムとして、科学技術省職員の人事データベースシステム（要語句の統一）を構築しているが、サイバーセキュリティに関する予算は現段階のところ要求していない。ただし、科学技術省傘下の大学による研修予算については予算割当が可能と科学技術では考えている。

4.5.5 教育省 (Ministry of Education)

教育省において、最初にサイバー攻撃が認識されたのは 10 年ほど前になる。教育省のウェブサイトがサイバー攻撃を受け、数日間サーバがダウンしている。また最近でも 2015 年 6 月には、大学入試試験結果のデータベースに不正アクセスがあり、データの改ざんなどが判明した。教育省のメールサーバへのハッキングなども確認されているため、サイバー攻撃のリスクがあることが認識されている。10 年ほど前のサイバー攻撃を契機に、サイバー攻撃を受けた時のガイドラインが作られたが、現段階では激化抑制の手順や規則は存在しておらず、他の省庁などにも報告し情報を共有していない。また、実施計画を作り、実施しても検証を行っていないので、有効な手段かどうか把握できていない。そのため、重要なデータについてはインターネットから隔離したコンピュータに格納しているとのことである。

教育省としては、サイバーセキュリティ対策として、まず、MCIT からの要請に基づいた政府通達により、CIO と CSO を配置し、2 名の CSO を任命している。また MCIT・科学技術省が開催するサイバーセキュリティ研修にも職員を参加させるとともに、コンピュータ・リテラシーが十分ではないため、電子書類管理の研修コースにも職員を参加させている。

教育省では、今後サイバーセキュリティ対策として、サイバー攻撃の監視装置とともに職員の基礎的な ICT スキルの向上を今後行っていかなければいけないと考えている。

4.5.6 産業省（Ministry of Industry）

2007 年にネピドーに首都を遷都したことで、2010 年には、これまでヤンゴンだけであったデータセンターをネピドーにも設置した。セキュリティ対策としては、ファイアウォールのみで、ソフトウェアのインストールやサーバの監理については、民間のベンダーに委託している。サイバーセキュリティ対策としては、人材育成よりもアプリケーションの導入が優先されており、民間企業に管理を任せている。そのため、独自に研修を行うノウハウがなく、MCIT もしくは民間企業が開催する研修に職員を参加させている。

産業省では、入札情報、ライセンスの情報、トレーニングセンター入学志望者の個人情報をオンラインサービスの一環で扱っている。例えば製造業ライセンスの取得・更新等、にオンラインサービスが利用できるようにしている。更新は 2 年ごとに必要であり、ヤンゴン所在の企業がわざわざネピドーに来ないと登録・更新ができないと不都合なので、オンラインサービスを開始しており、現在はオンラインサービスセンターが各タウンシップにあり、そこから各企業は登録できるようになっている。

また省内では、ケーブルと Wi-Fi により LAN が構築され、200 台程度のコンピュータが接続されている上、スマートフォンやタブレットなども接続されている。セキュリティ対策として、LAN 内では、全員が閲覧できるサイトとパスワードによって許可されるサイトと区別している。アンチウィルスソフトはすべてのパソコンに導入済みで定期的にアップデートしている。必要な運用経費は、アンチウィルスソフトのライセンス料金などを含む維持管理費とサーバやアプリケーション購入費用の USD 25,000/年ほどで、毎年予算が割り当てられる。ただし、機材の調達等については、要求予算がそのまま割り当てられるわけではない。

一方、電子メールの運用ルールはなく、多くの職員がフリーのメールアドレスを使っている。産業省のドメインのメールアドレスは 50 強であり、役職上位のものに割り当てられているが、フリーのメールアドレスを併用している職員も多い。例えば省庁のドメインからフリーメールへメールを送信すると、スパム扱いになるが、知り合いからのメールは躊躇なく開封する職員が多い。産業省では、メールサーバの容量も十分であるとしており、すべての職員へのメールアドレス割当とメールの適切な利用など、今後、全省統一の運用ルール作りが急務である。

4.5.7 建設省

建設省では、MPT のインフラを使って、道路、橋梁等インフラ管理・情報共有のため 14 の地方都市とイントラネットを構築している。建設省の IT 関連の予算は、建設省全体予算の約 1 %で、かつ毎年確実に確保されているわけではない。IT 関連予算の多くは、PC やソフトの購入（およそ USD15,000）に使用されるため、サイバーセキュリティに割り当てられる予算はさらに限られている。また IT 関連の知識が不足しているため、予算が取りにくい現状もある。今後 3 年間でビデオ会議システム、レポートシステム、電子文書管理システムを構築する予定であり、ライセンス料/年、維持管理費用、アップグレードの運用経費を除く予算は USD 25 万を見込んでいる。

現在の建設省のデータ管理方法は、以下の 5 点である。

I. 重要なファイルにアクセスできる権限を付与する
II. コンピュータ端末ごとにパスワードを設定する

III. Microsoft のアプリケーション別にパスワードを設定する
IV. ネットワークにつながっている重要なコンピュータはアンチウィルスソフトを導入する
V. 重要な書類は決められたものだけがコピーをできる

ただし、オペレーティングシステムはライセンス無しでインストールされているものもあり、すべてのコンピュータにアンチウィルスソフトは導入されていない等、問題点もある。
2009 年には 18 省庁がバングラデシュから一斉にサイバー攻撃を受けているが、データベースの情報が削除されている省庁がある中、建設省は新しいウェブサイトを構築する準備をしていたため、データのバックアップを持っており、難を免れた。

建設省では電子政府化の移行とともに独自のメールサーバーシステムを調達することにしている。現在は、建設省ドメインのメールアドレスは少なく、またメールサーバの容量が限られているため、多くの職員がフリーメールアドレスを使用している。建設省ドメインアドレスを職員が使えるようにするため、500、1,500 と段階的に増やし、全職員と地方事務所の職員が建設省ドメインでメールを使うことができるようにする。

電子政府化とサイバー攻撃を受けた経験などから、建設省でもサイバーセキュリティは重要であるという認識が持たれており、これまで各部に情報通信担当（複数担務）4~5 名を置いていただけであったが、大臣の指示で 2015 年 4 月に、計画・情報通信室を新たに設けている。今後、情報通信担当者の人材育成が急務である。

4.5.8 商務省（Ministry of Commerce）

商務省（Ministry of Commerce、以下、MOCO）では輸入・輸出のライセンス許可、会社の登録等を行っている。この他に管理システムやアプリケーションシステム等、合計 13 のシステムが運用されている。MOCO は 20 の地方オフィスを持ち、本省と地方オフィスとの間にはイントラネットが構築されている。セキュリティ対策として、MOCO 本省にはファイアウォールがあり、本省と地方オフィスとの通信は VPN（バーチャル・プライベート・ネットワークの略）で行っている。セキュリティ対策機材があるのは、ネピドーの本省だけであり、地方オフィスにはセキュリティ対策機材は設置されていない。VPN のユーザーアカウントのログオン承認についてはドメインコントローラを使用している。またヤンゴンのハンタワディ（Hanthawady）にある MPT のデータセンターに MOCO のサーバを設置しており、ヤンゴンの業者とのサービス契約によりサーバの保守管理を行っている。業者に委託している理由は、過去のサイバー攻撃を鑑み、緊急時に 1 時間以内での対応が可能とするために、ヤンゴンの業者との保守管理契約を選択した。ネピドーからでは緊急時の迅速な対応が難しいからである。

一方、職員間のデータの共有は USB メモリスティックなどの外部メモリを使用しており、ネットワーク内の PC 間でデータの共有は行われていない。またサイバーセキュリティに関するガイドラインはなく、攻撃を受けた時の LAN から当該 PC の切り離しなどは認識されていない。加えてスマートフォンの普及により、携帯電話を省内 Wi-Fi に接続している現状もあり、ガイドラインの作成が必要であると MOCO では考えている。

また、職員のメール使用については、フリーのメールアカウントの利用を許容している。理由は、政府ドメインのメールはアカウント数が限られていること、メールに添付できるファイルの

容量が少ない、政府ドメインメールの方がフリーメールよりウィルスが送らてくる頻度が高い、政府ドメインメールのアプリケーションはスパムメールのフィルタリング機能がないなどである。今後は、文書交換システムやウェブアプリケーションメールなどを導入し、政府ドメインメールの使用を促進する方向とのことである。

これまで MOCO では、他省庁との連携として、MCIT が主催する各省庁の CIO や CSO による意見交換会に担当者を参加させてきている。この意見交換会は年間 7～8 回開催されてきていたが、近年は会議の開催に代わり、メールなどで情報共有しているだけに留まっている。今後は、各省庁だけの意見交換会の開催ではなく、サイバーセキュリティに関する技術能力が政府機関より秀でている民間企業も巻き込み、サイバーセキュリティについて考えていく必要があると MOCO は考えている。

なお、IT 予算は年ごとに決められるため、サイバーセキュリティ対策相応分として予算が確保できるかどうかは、不透明である。ミャンマー政府では電子政府化を進めているが、それぞれの省庁が各調達を独自に進めている。ちなみに、第 4.4.3 項に記載のトレーニングルームの調達には、USD 10 万ほどかかっている。

4.5.9 保健省（Ministry of Health）

保健省では他の省庁と同様に電子政府化を進めている最中であり、電子文書管理システムを利用している。ヤンゴンの MPT のデータセンターに保健情報システムと保健管理システムの 2 つのサーバをホスティングサービスにより設置し、様々な省庁が、保健省が有する生データにアクセスしている。そのため、セキュリティ保持は極めて重要だと考えている。しかしながら省内のスタッフのスキルや知識を考慮し、保守運用については、地元の民間企業に委託せざるを得ない状況である。ただし、今年は予算不足のため、保守運用契約が結ばれていない。

省内のパソコンにはすべてアンチウィルスソフトがインストールされているが、ウィルスなどを検知できる機材等は、設置されていない。アンチウィルスソフトによるウィルス検知の通知が、ウィルスが侵入してきたことを知らせる唯一の機能である。また多くの職員がスマートフォンなどの携帯電話によって、省内のデータにアクセスしている実態がある。

保健省では CIO を配置し、電子文章管理システムとウェブサイトの監理を行っているが、CSO は配置していない。セキュリティ対策の重要性は理解しているが、知識やスキルを保持しているスタッフは皆無で、ガイドラインなどもない状況で、どのように進めていけばいいかわからない状況である。また IT 研修などに職員を参加させても転職をしてしまい、ノウハウが省内に定着していない。保健省に 6 つの局があり、すべての部署にセキュリティの知識があるスタッフを配置するべきと考えているが、実際には職員が確保できていない。

4.5.10 中央銀行

日本のように金融業界特有のセキュリティ基準は、「ミ」国では定められていない。現在のシステムはインターネットに接続したシステムではないため、セキュリティに対する懸念を持っておらず、普及啓発をまず実施すべきと中央銀行では考えている。ただし、今後システムがオンラインで運用される際には、サイバーセキュリティ対策は必須条件である。

中央銀行では重要資産に対して、定義付けが行われていない。これまでの軍事政権下では全て

を機密情報にしていたが、今後、市場経済に取り込まれていく中で、機密にすべき情報の整理は必要である。

現在中央銀行では、ISMS に準拠したセキュリティガイドラインを作成しようとしているところである。会計システムは 2015 年 12 月、CV ネットは 2016 年 1 月から、それぞれ運用開始予定である。「ミ」国の金融が発展する上で、サイバーセキュリティは重要な位置付けとなる。安心して預金できる環境の整備・強化が肝要である。

4.5.11 ネピドー開発委員会 (Naypyitaw Development Committee: NDC)

ネピドー開発委員会（Naypyitaw Development Committee、以下、NDC）は、ネピドーの開発を実施する地方自治体である。市長、副市長のもと 7 名の委員が選任されており、NDC 管轄の 8 つのタウンシップを含め総勢 800 人に職員がいる。この内、パソコンを使用しているのは、76 人程度、各タウンシップ、20 ある NDC 本部の部署ではそれぞれ 2 名が、また ICT 部では 20 人が使用している。その他の職員は個人の携帯、タブレットを使用している。ただし、パソコンでインターネットに接続しているのは、ICT 部の 20 台であり、データは常にバックアアップをとっている。NDC では現在のところオンラインサービスは提供しておらず、NDC で管理しているデータのほとんどは職員のメールである。NDC ドメインのメールアドレスはあるが、アカウントは一部にしか割り当てられていない。

NDC では、CIO が CSO を兼任している。しかし、現状では知識が不足しているため、CSO としてどのような活動をしていくべきか理解されていない。また、CIO や CSO は仕事量も増加するため、希望者が少なく、人選に難航している。現在の CIO は、プログラミングなどの知識はあり、自身でアプリケーションなどの開発を行っている。ウェブサイトの構築・管理については、NDC で行うことができないため、外部委託している。IPS/IDS については知識がなく、導入されていない。

NDC は NDC のウェブサイトに対し、サイバー攻撃を受けたことがある。攻撃を受けるたびにバックアップを再送して回復しているが、その後に適切な対策が講じられないため、再度攻撃を受けているのが現状である。サイバーセキュリティに関するガイドラインやトレーニングがなく、サイバーセキュリティに関する知識が乏しいことため、対策を講じることができていない。今後、オンラインサービスの提供、ICT システムを拡充する計画があるが、それに合わせて、セキュリティ対策の検討を行っている。ただし、ICT 局は 1 年前に設立されたばかりで、予算については、必要な活動費等ベースで申請し、承認を得ているのが現状である。ちなみに、この 1 年間の予算実行実績は、USD 8 万である。サーバ、ネットワーク構築機材、ファイアウォール、ウェブサイトの管理委託費等に使用されている。

4.5.12 各省庁対応状況の比較

表 4.5-1 に、第 4.5.1～4.5.11 で述べた各省庁の対応状況を一覧にして示す。

2010 年に発生した DDoS 攻撃により、セキュリティ対策の認知が向上した結果、ほとんどの省庁ではファイアウォールを設置している。その一方で携帯端末の省内 Wifi 接続を許可している省庁が多く、セキュリティよりも利便性を優先している傾向が見て取れる。IT 担当者は、MCIT から CIO と CSO の役割分離を推奨されているものの、CSO を任命しているとこは 2 省と少なく、また

対応マニュアルが未整備など、今後の課題が多い。

表 4.5-1　各省庁のサイバーセキュリティ対応状況一覧

	CS 攻撃	CS 機材	携帯端末接続	民間委託	CIO	CSO	対応ﾏﾆｭｱﾙ等	研修	予算
通信・情報技術省	○	○ FW/ TSUBAME	○	-	○	×	○ mmCERT のみ	○	○
科学技術省	×	○	×	○	○	×	×	○	○
教育省	○	×	-	-	○	○	ｶﾞｲﾄﾞﾗｲﾝ	○	○
産業省	-	△ FW のみ	○	○	○	×	-	△ 独自無	○
建設省	○	×	-	-	○	×	-	○	○
商務省	○	△ FW のみ	-	○	○	○	-	○	○
保健省	-	△ FW のみ	○	○	○	×	-	○	○
NDC	○	△ FW のみ	○	○	○	×	×	×	○

凡例：○有、×無、△条件付

CS: サイバーセキュリティ、CIO: 最高情報責任者、CSO: 最高セキュリティ責任者

NDC: ネピドー開発委員会、FW: ファイアウォール

※MPT は通信事業者として既に独立した組織になっているため、通信・情報技術省の情報は、MPT を含まないものである。また mmCERT は含まれている。

4.6　サイバーセキュリティ分野における他国政府・ドナーの支援状況

サイバーセキュリティに限定した他国政府及びドナーの連携・支援は行われていないため、本項では情報通信分野における他国政府・ドナーの支援状況をまとめる。

2004 年以降、「ミ」国の情報通信分野に支援を行っている他国政府及びドナーは、韓国、中国、インドが中心であった。しかし、2011 年 3 月のテイン・セイン政権発足後は、日本のみならず、国際機関である世界銀行、アジア開発銀行による支援が行われるようになった。

世界銀行は、灌漑・下水、保健衛生、港湾・水路・船舶、中央政府管理、森林、教育分野いついて、農村への公共サービス・インフラ、気候変動、ジェンダー、保健衛生システムの課題解決のための支援を行っている。教育や地域への公共サービスの提供では通信セクターと連携が必要であり、電気通信セクター改革プロジェクトを行っている（表 4.6-1 参照）。

ADB は、持続的かつ開放的な経済発展と貧困削減のための雇用創出を中期的な支援成果としており、個人・組織の能力開発、構造的経済環境の向上及び農村における生活の利便性やインフラ開発を暫定的な戦略の柱として、下記の支援重点項目を掲げている。

- 環境配慮と重要分野の開発戦略及び計画の融合を通した持続的な環境
- 財政の透明性及び説明責任による良い統治
- 投資・貿易のための政策、法・規制環境の強化を通した民間セクターの発展
- 交易・投資等における地域内協力と統合
- 女性の能力開発、雇用・起業機会の創出などにおける男女格差の分析よる男女の平等

通信セクターについては、韓国、中国との共同資金の技術協力により電子統治のマスタープラン（表 4.6-1 参照）の作成を支援してものの重点分野としてはおらず、地方の女性に対する職業訓練等で ICT の利用を図るとしている。

USAID は、①民主主義、人権及び法による支配の促進、②透明なガバナンス制度の強化、平和と和解プロセスの実行、④保健衛生、食糧安全保障、経済機会及び生活の向上の 4 項目を重点支援策としており、公正、中立なメディアの育成など放送、ジャーナリズムについては支援をしているが通信分野に直接的な支援は行っていない。

KOICA は、2004 年から ICT 分野のマスタープランや電子政府化の移行について積極的な支援を行っているが、「ミ」国政府の資金不足のため、電子政府化は当初計画通りに進展していないのが実情である。

一方、我が国の情報通信分野における「ミ」国に対する支援は、表 4.6-2 に記載したとおりで、技術協力、無償資金協力及び有償資金協など、様々なスキームによって支援を行っている。

表 4.6-1　他ドナー国・国際機関による援助実績（情報通信分野、2004 年以降）

No.	案件名	実施年度	金額 (百万 USD)	ドナー
1.	ミャンマーICT 開発マスタープラン作成支援 概要 : 国家対策委員会（e-National Task Force : e-NTF)を対象にした ICT マスタープラン（2010-2015 年）の作成	2004 年 8 月～ 2005 年 8 月	0.95 （無償）	韓国
2.	ミャンマー電子政府基本システム	2005 年 11 月～ 2006 年 10 月	12.00 （借款）	韓国
3.	ヤダナボン・サイバーシティ建設 概要:インドがソフトウェア、中国がハードウェアを支援。テレポートセンター（2007 年 12 月稼働）インキュベーションセンター（2008 年 12 月稼働）	2007 年~	不明	インド、中国
4.	テレコム開発プロジェクト（MPT）	2007 年前後（詳細不明）	3.02 （借款）	中国
5.	GSM システム拡張プロジェクト（MPT）	2007 年前後（詳細不明）	1.25 （借款）	中国
6.	全国テレコム・ネットワーク構築プロジェクト	2007 年に計画（詳細不明）	150.00	中国
7.	corDECT システム構築と越境 OFC 接続プロジェクト（MPT）	不明	7.00 （借款）	インド
8.	インド・ミャンマーe ラーニング&リサーチセンター（e-NTF）	2007 年に計画（5 年間の予定）（詳細不明）	不明	インド
9.	ソフトウェア技術訓練センター（UCSY） 概要：講師派遣、研修員受入	2008 年 10 月~	不明 （技術協力）	インド
10.	ブロードバンド衛星ネットワークプロジェクト（MPT）	2007 年前後（詳細不明）	15.00	タイ
11.	電気通信セクター改革プロジェクト コンポーネント： ・構造的な接続環境の構築	2014 年 5 月～ 2019 年 12 月（予定）	31.50	世界銀行

No.	案件名	実施年度	金額 (百万 USD)	ドナー
	・農村部への接続拡大 ・電子政府基盤構築 ・プロジェクト実施管理支援			
12.	電子統治マスタープランの作成及び情報通信技術セクターの学術機関における能力考察 韓国の e-アジア及び知見共有基金ならびに中国の地域 協力及び貧困削減基金との共同資金	2014 年 3 月～2015 年 6 月	1.50（各 0.50）（技術協力）	ADB/ 韓国/中国
13.	「ミ」国 ICT セクター全体評価	2014 年 7 月～2015 年 6 月	不明（技術協力）	ADB

出所：

世銀（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/#）

平成 24 年度第 1 回 JTEC 講演会資料（2012.1.18）http://www.jtec.or.jp/2012.1.18kouenkai_kouno2.pdf

表 4.6-2　我が国による援助実績（情報通信分野、2006 年以降）

No.	案件名	実施年度	金額 (億円)	スキーム
1.	ソフトウェア及びネットワーク技術者育成プロジェクト	2006 年 12 月～2011 年 11 月	3.10	技プロ
2.	通信網緊急改善計画	2012 年（E/N 締結）	17.10	無償
3.	中央銀行業務ＩＣＴシステム整備計画	2013 年（E/N 締結）	51.00	無償
4.	情報通信インフラ改善アドバイザー	2013 年 11 月～2015 年 6 月	-	有償専門家
5.	通信網改善事業	2015 年 3 月～2019 年 8 月（予定）	105.00	有償
6.	通信政策アドバイザー	2015 年 10 月~2016 年 9 月（予定）	-	有償専門家

出所：

外務省 ODA 国別データブック（対ミャンマー）（http://www.mofa.go.jp/mofaj/gaiko/oda/index.html）

JICA ナレッジサイト（http://gwweb.jica.go.jp/KM/KM_Frame.nsf/NaviIndex?OpenNavigator）

4.7　他 ASEAN 諸国との状況比較

電子政府及びサイバーセキュリティの側面から、「ミ」国を他の ASEAN 諸国と比較した結果が幾つか存在する。ここではその代表的なものについて紹介を行う。

4.7.1　電子政府

電子政府の開発状況について「ミ」国を他の ASEAN 諸国と比較したものとして、UN が作成した E-Government Development Index（EGDI）[2]がある。EGDI は、各国の電子政府の開発状況について、政府のオンラインサービス、通信インフラ、人的資本の観点から分析し算出したものであ

[2] UN, E-Government Survey 2014

る。ASEAN 加盟国の中で比較すると、「ミ」国は最下位となっているが、特にオンラインサービスと通信インフラの評価が低くなっている。ASEAN でトップはシンガポールである。ちなみに全体での一位は韓国であり、日本は全体の 6 位となっている。

表 4.7-1　ASEAN 諸国の E-Government Development Index

Rank	**Country**	**EGDI**[3]	**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　サイバーセキュリティ

各国のサイバーセキュリティ対策状況について「ミ」国を他の ASEAN 諸国と比較したものとして、ITU が作成した Global Cybersecurity Index（GCI）[4]及び JICA「ASEAN 諸国における情報セキュリティ情報収集・確認調査（2012 年）」がある。

ITU GCI は、各国のサイバーセキュリティ対策状況について、法制度の整備状況、技術的対策、組織的対策、能力開発、協力の観点から分析し算出したものである。ASEAN 加盟国の中で比較すると、「ミ」国は 6 番目となっているが、特に法制度の整備状況と組織的対策の評価が低くなっている。ASEAN でトップはマレーシアである。ちなみに全体での一位は米国であり、日本は全体の第 5 ランクに位置づけられている。

なお、GCI は同一 GCI に多数の国が属しており、全ての国は 29 のランクのどこかに位置づけられることになる。例えば日本は第 5 ランクに位置づけられているが、全体では同率 8 位であり、第 5 ランクには日本の他 7 ヶ国が位置づけられている。

[3] EGDI : E-Government Development Index

[4] ITU, Global Cybersecurity Index & Cyberwellness Profiles

表 4.7-2　ASEAN 諸国の Global Cybersecurity Index

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

JICA「ASEAN 諸国における情報セキュリティ情報収集・確認調査」では、ASEAN 諸国の ICT 動向、経済状況、セキュリティ対策レベル、国際関係など最近の動向をもとに、各国を「IS（Information Security）先発国」「IS 政策推進課題国」「IS 先導者育成課題国」に類型化して整理を行っている。ミャンマーはこの中で、「IS 先導者育成課題国」に分類されている。IS 先導者育成課題国としては、ミャンマーの他、ラオス、カンボジアが分類されている。これらの国では ICT 環境整備、セキュリティ対策等が十分とは言えず、経済水準も低いレベルにあり、政府レベルや大企業レベルにおいても諸外国の支援が期待されている国々である。

表 4.7-3　ASEAN 諸国との国際連携を検討する上での類型化

分類	**Country**
IS 先発国	Singapore, Brunei Darussalam, Malaysia
IS 政策推進課題国	Thailand, Philippines, Indonesia, Viet Nam
IS 先導者育成課題国	Lao, Cambodia, **Myanmar**

第5章　政府機関及び関連組織等におけるセキュリティ対策状況

5.1　政府機関の ICT 環境に係るセキュリティアセスメント

5.1.1　セキュリティアセスメントの対象

前述したMCIT内における組織改編の結果､各府省のWEBサイトについてはMPTが引き継ぎ、通信事業者としてのコロケーションサービスの一環としていされることとなった。

一方で、e-Government 等の政府機関が共同利用するシステムについては、新たに設置されたIT&CS が所管することが決定しており､セキュリティの担当部署とは別に e-Government の担当部署が設置されており、電子行政システムの運用を行っている。

これらの役割の整理に伴い、IT&CS では、4 箇所あった MCIT のデータセンターのうち、ネピドー市内 1 箇所（以下、S-12)、ネピドー北部の 1 箇所（以下、Thayetkhon）の計 2 箇所のデータセンターを引き継いでおり、このうち電子行政システムについては前者の S-12 に設置している。

IT&CS では、S-12 データセンターについて、今後も電子行政システムを整備・運用する重要な ICT 環境として想定している。このため当該データセンターは十分なセキュリティ対策が必要とされる ICT 環境となる。

これらの背景に鑑み、S-12 データセンター（特に電子行政システム）の運用方法及び実態を踏まえて、以下の項目についてセキュリティアセスメントを実施した。

- セキュリティポリシー、運用ルール、変更管理手順
- ベンダー製パッチの実装状況
- 適正な運用ログの管理
- インシデントレポート手順（エスカレーションルール含む）
- 人員体制
- 情報セキュリティに対する意識
- 技術的対策の実施状況

5.1.2　セキュリティアセスメント結果

政府職員が政府のメールアドレスではなく、Gmail 等の一般のサービスを利用して情報伝達や共有を行っている状況自体が既にセキュリティ上の危険性を有しているが、そもそも「ミ」国政府の ICT 環境として、日本の霞ヶ関 WAN や LG-WAN のような行政専用のネットワークが存在していない。更に、情報通信を所管する MCIT においても全省的な省内 LAN を保有しておらず、一定の単位毎（部署毎や部屋毎等）で個々に商用のインターネットサービスを引き込んでおり、全ての電子行政システムの利用や情報のやり取りはインターネット経由で行われている。

このため、もとより自組織の情報セキュリティを自身で技術的に保護することができる構成になっていない。これに対する技術的或いは設備投資的な対策は必要なのはいうまでもないが、整備には一定の時間と予算を要するものであり、喫緊性を考慮すると、まず利用に際しての行動規範や意識の向上、運用方法等によってセキュリティレベルを確保することも重要である。

以上の観点から、政府機関の ICT 環境にとして、IT&CS における ICT 環境の運用状況に係る調査を踏まえ、セキュリティの診断を行った。

(1)　セキュリティポリシー、運用ルール、変更管理手順

【実施状況】

セキュリティポリシーにはついては、セキュリティ部門にて策定することとなっているが、すでに記載のとおり、セキュリティ部門に MCIT のプロパー職員が責任者のみという状況、組織改変直後であり IT&CS の独自予算も割り当てられていない現実もあり、策定は進んでいない。

一方、電子政府システムの運用を任されている e-Government 部門では、セキュリティポリシー等のルールやガイドラインが無いなかで、現場主導で電子政府システムを運営している。また現時点で運用者が人数的にも限られていることもあり、それらの運用ルールはドキュメント化されておらず、実質的に担当者の判断に基づく運用となっており、組織的に運用手順の妥当性についてレビューされる仕組みもない。

また、現場で想定している保守は障害復旧（国内企業にスポット保守を依頼する）のみであり、改良や機能拡張のためのシステム変更は行われておらず（変更管理等もない）、システムの PDCA も運用されていない。

【対策】

セキュリティポリシーについては、最低でも数名の知識・経験を有した人材の確保、または策定を支援できるスキルを有した事業者に対して委託可能な予算の確保が必要とされる。しかし当該セキュリティポリシーは、全てのセキュリティ管理の規範として重要なだけでなく、仮に IT&CS で策定予定のものが MCIT を想定したものであっても、他府省への適用や展開は可能で、「ミ」国政府全体に寄与するものであり、実際に各府省からの期待は高く、可能な限り早期の策定が求められる。

また変更管理などの運用ルールについても、基本的にセキュリティポリシーにおいて規定・明文化されることが求められる。

(2)　ベンダー製パッチの実装状況

【実施状況】

電子行政システムへのパッチの適用は管理者の判断で、管理者自らの操作で行われている。後述の脆弱性診断の結果にもあるとおり、実態としては適宜パッチが適用されていると考えるが、パッチの適用にかかるルールは明文化されておらず、事前の影響度テストや適用時の承認プロセス、適用履歴の記録等も管理されていない。

【対策】

パッチの適用において、組織内で状況共有ができる適用時の手続き、適用の必要性の定期的な確認、適用時の技術的な確認検証方法（手順）、適用に当たっての役割分担と責任範囲等を確定し、セキュリティポリシー又は個別の運用ポリシー等で明文化することが求められる。

(3)　適正な運用ログの管理

【実施状況】

システムのログについては随時確認を行っているが、確認のタイミングや確認深度は管理者の裁量となっており、明示的に定められてはいない。日常の運用のログについては、日常的に実施している運用業務がどれほど存在しているかが不明ではあるが、特に日報等の作成及び共有は行われていない。

【対策】

システムログやアクセスログ等の確認は、タイミングや方法についてルール化するとともに、より多くのスタッフでそれを共有し、十分なマンパワーをかけて実施することが望まれる。また日常の運用ログについては、最低限、定型的な日報を作成する等によって状況の共有手段を確立することが求められる。

(4) インシデントレポート手順（エスカレーションルール含む）

【実施状況】

インシデントや課題が発生した場合、管理者がインシデントの内容や対処などをドキュメント化（レポートを作成）し、上長に報告するプロセスは実施されている。但し、日常的な課題の管理についてはドキュメント化されてはおらず、長期的な課題の解決、課題の優先度の判断等は管理できる仕組みとなっていない。

【対策】

課題管理表やインシデント管理表等でドキュメント化された管理手法についてルール化し、手法及び運用プロセスについて明文化することが求められる。

(5) 人員体制

【実施状況】

e-Government 部門には 50 名程度の要員が確保されているとされているが、電子行政システムを管理している（管理者権限を有している）要員は、メールシステム 1 人、電子文書管理システム 1 人の計 2 人で、管理者が不在の場合は運用作業が行えない状況である。

加えて、データセンターが設置されている庁舎（S-12）全体でも、それだけの要員が確認できないことから、技術スタッフの人員数は極めて少ないことが懸念される。

【対策】

管理権限者については、最低でも各システムに対して、運用能力を有した人材を複数割り当てる必要がある（複数システムの兼任は可能）。また運用作業に当たる要員の増強も早期に求められる状況である。IT&CS の組織は現在も拡充過程であり、今後 MPT からも要員の補充が想定されるところではあるが、技術スタッフの確保ができない場合、内部で養成することも視野に入れる必要がある。

また IT&CS としての要員計画についても早期に明確化が求められる。

(6)　情報セキュリティに対する意識

【実施状況】

「ミ」国内の学術機関（大学）に対するヒアリング調査からも明らかとなっているが、「ミ」国内におけるセキュリティに対する教育は皆無に等しく、一般のセキュリティに対する意識は基本的に低い。特に技術的にセキュリティに熟達している人材は、現状ではほとんど確保困難と考えられる。

【対策】

組織内のセキュリティ意識の向上においては、研修等でのセキュリティ教育や啓発が重要になるが、それに先立ちセキュリティポリシー等の行動規範を策定及び提示する必要がある。
この観点からもセキュリティポリシーの早期策定が求められる。

(7)　技術的対策の実施状況

【実施状況】

LAN あるいは WAN が整備されていないため、電子文書管理システムの利用者は全てインターネット経由でシステムを利用する。このため当該システムはインターネットに接続される必要があり、相応のセキュリティ対策が必要となる。

現在、データセンターに整備されているセキュリティ対策としては、各サーバへのウィルス対策や、当該システムのネットワーク環境を守るファイアウォールと VPN があり、最低限の防御対策は施されてはいる。一方で IDS/IPS、DDOS 攻撃対策等のパケットレベルの高度な監視機能、WAF、DLP 等のアプリケーション／コンテンツレベルのセキュリティ対策については導入されていない。

【対策】

データセンターには IDS/IPS の機能を拡張追加できるファイアウォール機器が導入されているものの、現段階では運用されていない。国の電子政府システムを運用する上で高度なセキュリティ対策は重要であるが、当該システムの運用は職員自らが行なっており、且つ技術的に対応できる人材が少ないため、数多くのセキュリティ対策を運用することは現状では困難と考える。
このため、重視されるセキュリティ対策として以下の導入が有効と考えられる。

- IDS/IPS 機能等の導入により詳細なセキュリティ状況の現状把握が必要（加えて電子政府システム利用府省に対する被害拡大の防止にも有効）
- 各種ログ等の統合的収集・保管と分析に加えて、異常検知等の運用を効率化する機能やサービスの導入についても、人材面での課題をカバーし、実質的にセキュリティ対策を向上させる点で有効
- 現段階ではアプリケーションが限定されているが、電子文書管理システムをはじめ重要文書が取り扱われることから、アプリケーション／コンテンツレベルのセキュリティは必要

5.1.3　政府機関の ICT 環境において今後求められる対策

前述の個別のアセスメント結果に対する対策は早急な対策として重要である。一方で「ミ」国政府機関の ICT 環境そのものが未整備に近い状態であることから、上記のような対処療法的な対策だけではなく、本来構築すべき ICT 環境のあり方を念頭に置いたうえで、必要な環境整備を進めていくことも重要である。

現在 MCIT 内のネットワーク環境は下図のとおりであり、MCIT 内の部局や室等の小規模組織或いは庁内の部屋等の物理的な単位でインターネット回線を引き入れ、小規模な LAN や無線 LAN 等で庁内の PC が接続されている。その利用者環境は、通常の一般ユーザの環境とほぼ変わりなく、組織としてのセキュリティ対策等は行われていない。

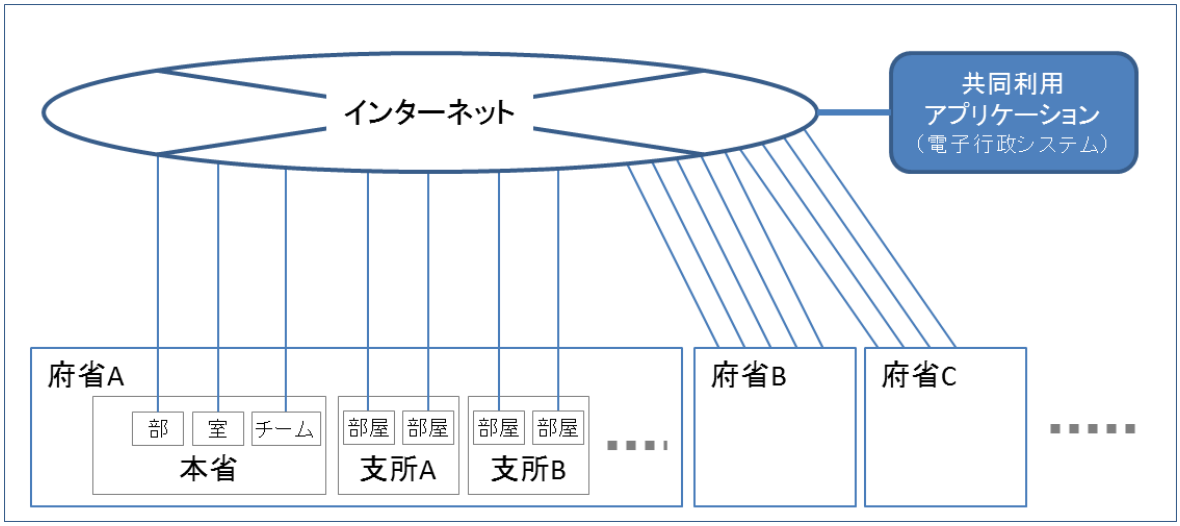


図 5.1-1　「ミ」国政府の ICT 環境

この場合、省内の利用者機器の管理、受発信された情報、省内情報資産の所在や管理状況等、省内の情報管理のほとんどについて実施することが困難であり、想定されるセキュリティの脅威に対して統合的に対策を施し、それを管理することも困難となる。

また MCIT が提供しようとしている府省間で共同利用するアプリケーションについても、利用者機器の管理・把握が困難となるため、利用者側に専用端末を設置するか利用者レベルでの管理（ID/パスワード等）とせざるをえなくなる。

前者の場合であれば限られた専用端末のみからのアプリケーション利用となるため、利用者側の利便性に影響するだけでなく、専用端末へのファイルの移送等において USB 等のメモリが使われるかセキュリティ対策があまり行われていない利用者のネットワークに接続されてしまうかになり、セキュリティへの懸念も依然として残る。

後者の場合は、利用者の管理のみであるため、なりすまし等の行為による攻撃に対しては、事後のトレーサビリティも含めて十分な防御・管理ができない。

一方で我が国の政府機関では、下図のとおり各府省単位で省内 LAN 及び WAN が構築・管理されており、更に各府省間は霞ヶ関 WAN で接続されている。これによって政府内での重要通信が専用の閉じたネットワーク内で行うことができ、加えて各府省及び霞ヶ関 WAN の各レベルにお

いても相応のセキュリティ対策がなされている。これらの構成は我が国政府に限らず、一定の整備が進んでいる国、大規模な企業等でも同様の構成となっており、統括的にセキュリティ対策の実施と管理がなされている。

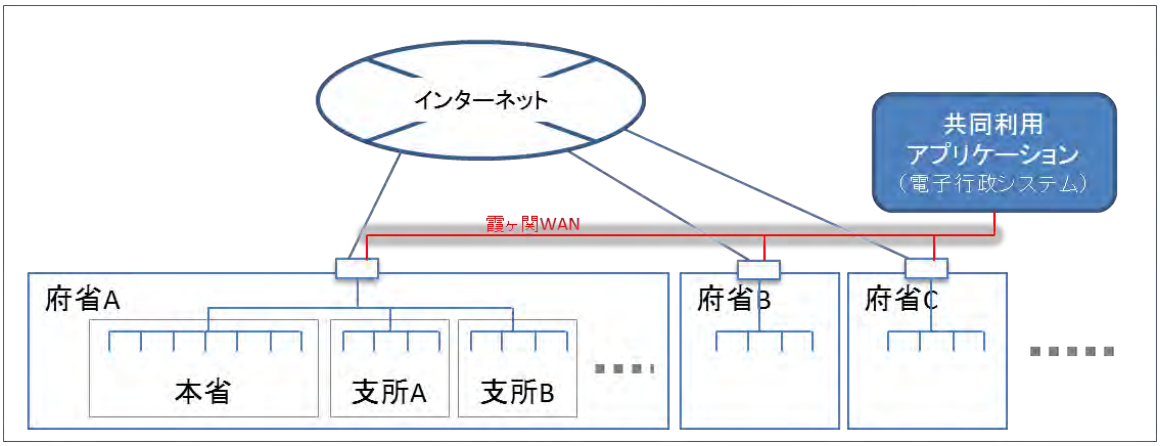


図 5.1-2　我が国政府の ICT 環境

「ミ」国においても、将来的には上図のような ICT 環境を整備することが望ましいが、要する費用（霞が関 WAN の運用経費は年間で 3 億円程度）、運用・管理のための人材の観点から、早期の導入は困難と考えられる。また、我が国の場合でも府省間の調整等を含めて 4～5 年程度を要しており、中期的視野で取り組んでいく必要がある。

特に「ミ」国の場合、前述のとおり各府省のネットワークが構築されておらず、情報資産の把握や統合的なセキュリティ対策の観点からも、下図のように各府省のネットワーク統合が優先的に行われる必要がある。

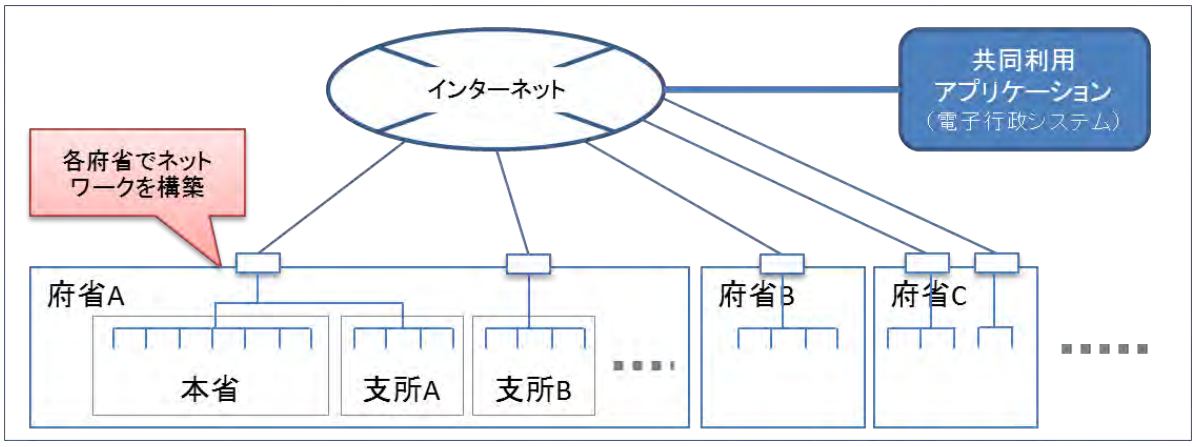


図 5.1-3　「ミ」国政府において当面目指すべき ICT 環境

各府省のネットワークの構築においては、必ずしも単一のネットワークに統一することが優先されるのではなく、各府省である程度限定された単位で LAN や小規模 WAN を再構築し、まず外部ネットワーク（現状ではインターネット）への接続点を把握することが重要である。これによ

り各府省の WAN 或いは府省共通の WAN の設計・検討、共通アプリケーション側でのセキュリティの設計・導入が可能になる。

各府省のネットワークの構築に際しては、府省毎に省内の調整体制の構築、現況の把握調査と再設計作業、再整備の費用等が工程として必要となる。

この内、現況の把握調査と再設計作業については、セキュリティ及び大規模ネットワークに係る一定の専門知識が必要であり、各府省の担当者の育成を待っていては着手が大幅に遅れることから、基本構成のひな形の提供に加え、担当者の育成も兼ねた調査或いは設計に資する専門家の派遣等の支援があれば効果的と考えられる。

しかし再整備の費用等については、構築に係る費用よりも運用経費のウェイトが大きいため、資金援助の等については、「ミ」国側での運用経費の負担力も考慮するなど、慎重な検討が求められる。

一方で、アプリケーションを提供するデータセンター側については、共同利用によって全府省がアプリケーション利用時の安全性も広く享受できることを考慮すると、これらの動向も踏まえつつ、より高度なセキュリティ対策を実現することが望まれる。このため、これに対して技術的支援（実現する適切なセキュリティ機器等も含む）を集中的に行うことは、「ミ」国政府機関の ICT 環境の向上に大きく寄与するものと考えられる。

5.2 政府機関の電子行政システムの脆弱性診断

5.2.1 脆弱性診断の対象とする電子行政システム

「ミ」国における政府機関の電子行政システムのセキュリティ対策の状況把握の一環として、具体的なシステム（サーバ）を選定したうえで、以下の手段により脆弱性診断を実施した。

- 脆弱性スキャンツール（Nessus）により潜在的な脆弱性情報の取得
- 脆弱性情報をもとにセキュリティポリシーの策定担当者または実施担当者に対する個別ヒアリング調査により脆弱性の影響評価
- どのような事態がどの程度で発生し影響を与えるかリスクの評価

2015 年 8 月末現在において、S-12 データセンターに設置されている電子行政システムは下表のとおりであり、4 つのシステムが存在している。

新たに開発中にシステムを除くと、現時点で稼働・運用されている電子行政システムはメールシステムと電子文書管理システムの 2 つのシステムであり、いわゆるアプリケーションサービスを提供しているシステムは電子文書管理システムのみとなる。

以上から脆弱性診断を行う対象として、電子文書管理システムを選定した。

表 5.2-1 S-12 データセンターの電子行政システム

システム	概要	状態
メールシステム	政府職員のメールサーバで、役職上位者等の一部職員のアカウントが提供されている（全職員	運用中

システム	概要	状態
	分ではない)。	
政府人事管理システム	政府全体の人事関連情報及び事務用のシステムで、現在開発中である。現況では開発環境としてサーバ 1 台が接続されている。	開発中
電子文書管理システム	政府機関で取り扱われている電子文書を登録・管理するシステムで、現在運用中で、各府省が利用している。	運用中
政府ポータルシステム	各府省の Web サイトや一般向けに提供しているサービスの窓口一元化（リンク等）を提供するシステムで、これから開発を予定している。	開発前 （機器設置済）

5.2.2 電子文書管理システムの概要と脆弱性診断のポイント

電子文書管理システムは電子化された政府文書を登録し保管するシステムで、各府省に対して一律で 100GB のストレージ容量が割り当てられ、WEB ベースで登録、検索、管理、閲覧等が行えるインターフェースが共通アプリケーションとして提供されている。MCIT では共通アプリケーション以下の環境を整備し提供しており、アクセス権の管理（利用者管理）等の実際の利用については各府省に役割分界されている。

電子文書管理システムのサーバ（EDMS サーバ）及びその周辺部の構成は下図のとおりで、30 台の物理サーバ（機器）に各 2 台、計 60 台分の仮想サーバが定義されている。各物理サーバには 4 つのネットワークポートが装備されており、うち 2 ポートは各仮想サーバ単位でインターネット側に接続されるスイッチ（EDMS スイッチ）に集約されており、残りの 2 ポートは管理用に内部側の 2 系統のスイッチ（VM スイッチ及びハードウェア管理スイッチ）にそれぞれ接続されている。またインターネットにはファイアウォールを介して接続されており、VPN を使用してインターネットからアクセスする方式となっている。

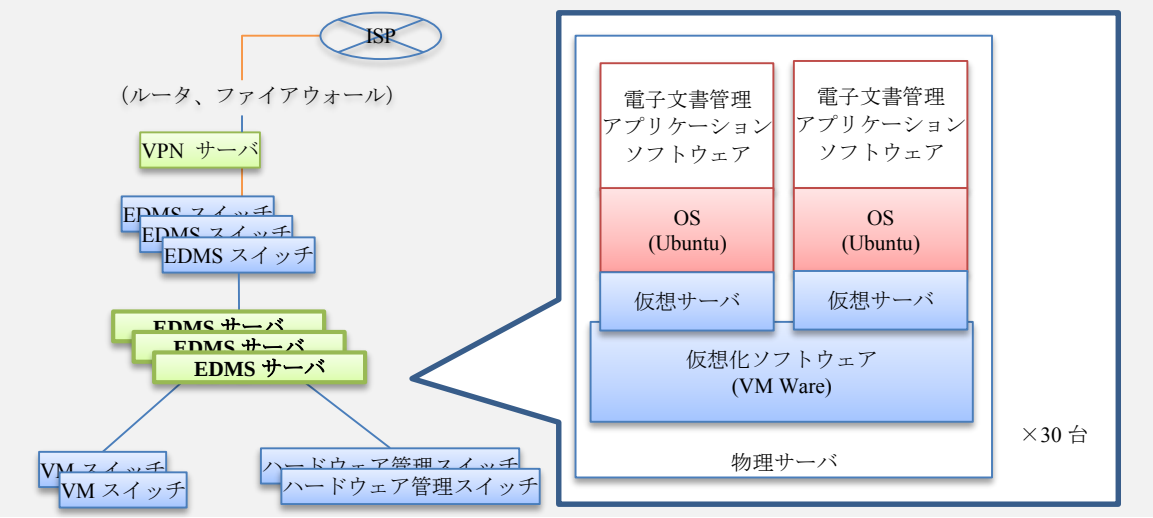


図 5.2-1 電子文書管理システムのサーバ等の構成

以上の構成を踏まえると、EDMS サーバは、仮想サーバ単位で接続されているインターネット側と管理用に接続されている内部側の 2 つの接続点が存在しており、サーバに対する攻撃としては、ユーザや外部者によるインターネット側からの攻撃の可能性と、内部者等がデータセンターに侵入して内部側から行われる攻撃の可能性が存在する。

このためスキャンツールを使用した EDMS サーバの脆弱性調査においては、仮想サーバが面するインターネット側と仮想化ソフトウェア以下のインターフェースとなる内部側の両方について調査することとした。

5.2.3 電子行政システムの脆弱性診断結果

(1) インターネット側からの脆弱性診断結果

インターネット側のポートは仮想サーバ単位に割り振られていることから、インターネット側からアクセスした場合に確認できるのは仮想化サーバ上のシステムの状況である。インターネット側のポートは、VPN での接続権限を有するユーザをはじめとして、何らかの形でファイアウォール及び VPN を潜り抜けたインターネット上からの攻撃を受ける可能性を有しており、攻撃の可能性・頻度としては内部側に比べると高く、十分なセキュリティ対策がなされていることが重要である。

2015 年 8 月時点で脆弱性スキャンツール（Nessus）を用いて実施したインターネット側（EDMS スイッチにスキャン端末を接続して実施）からのセキュリティホール等の診断結果は下図のとおりであった。

検出されたセキュリティホールの重要度は、緊急性の高い方から「Critical」「High」「Medium」「Low」の 4 段階に分類されており、実質的に Medium 及び Low については、時期をみて対応又は念のため危険性について認識をしておくといったレベルのものとなる。

EDMS サーバのインターネット側ポートについては、Low レベルのセキュリティホールが 3 件検出されたものの、早期又は緊急の対応が求められる High 又は Critical レベルのセキュリティホールは検出されず、調査時点で比較的セキュリティ対策が施された状態であることが確認された。

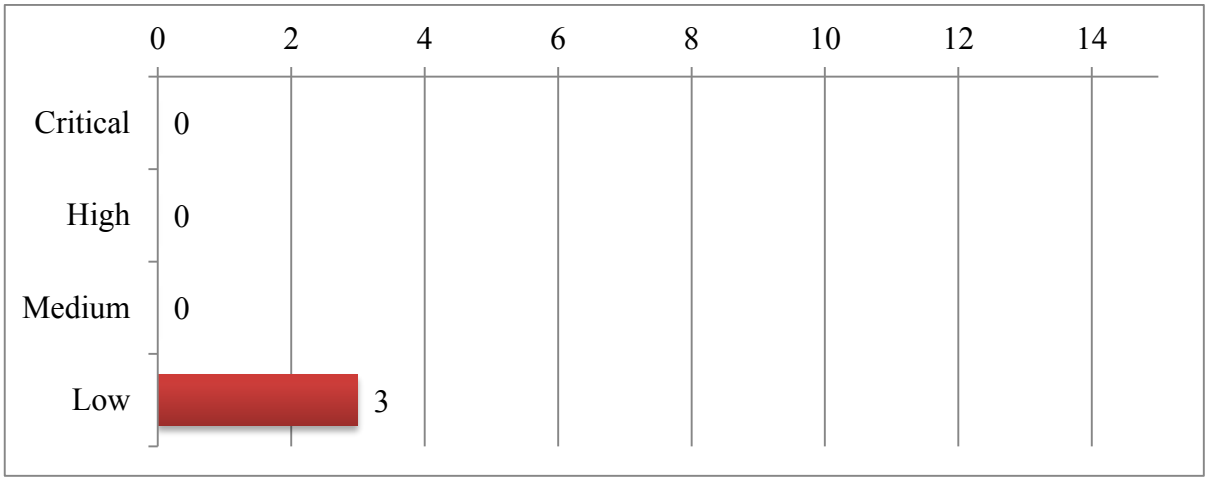


図 5.2-2 インターネット側ポートの脆弱性診断結果

検出された 3 件については、Web サーバにおける Cleartext Credential の危険性の指摘 1 件、SSH に関する危険性の指摘 2 件であり、留意すべき危険性ではあるが、影響範囲は小さく、緊急に対応を要するものではないうえ、対応自体も比較的容易である。

当該サーバは用途が限られており、Linux 系の OS を採用し、稼働しているアプリケーションについてもシンプルなものである。このため導入時の設定で大半のセキュリティ対策が実現されており、運用段階でのセキュリティ対策の管理が比較的容易であることも、脆弱性が抑えられている要因と考えられる。

よって当該サーバにおけるインターネット側のポートについては、今後、必要なパッチの適用など、妥当な運用・保守作業が行われることで問題はないと考えられる。

(2) 内部側からの脆弱性診断結果

内部側のポートは物理サーバ 1 台につき、仮想化ソフトの制御・管理のためのポートが 1 つ、ハードウェアの管理のためのポートが 1 つ設けられており、仮想サーバより下のレイヤを含めてアクセスすることができ、サーバの設定も含めた制御・管理の操作が可能である。

但し当該サーバについては、サーバ群の制御・管理のためにそれぞれ 2 つのポートをスイッチ（VM スイッチ及びハードウェア管理スイッチ）で集約しているが、それらのスイッチにはサーバ以外の機器は接続されておらず、管理の際もそれらのスイッチに一時的に運用端末を接続して操作を行っている。このため内部側からの攻撃は、データセンター室内にあるこれらのスイッチに物理的に接続することが前提となり、データセンター自体の入退室等の管理とあわせてセキュリティが担保されるものとなる。

2015 年 8 月時点で脆弱性スキャンツール（Nessus）を用いて実施した内部側（今回は VM スイッチにスキャン端末を接続して実施）からのセキュリティホール等の診断結果は下図のとおりであった。

EDMS サーバの内部側ポートについては、High レベルのセキュリティホールが 1 件、Medium レベルのセキュリティホールが 12 件検出された。セキュリティホールの件数としては、インターネット側に比べると多くなっているが、前述のとおりそもそもデータセンターへの侵入の段階で

一定のセキュリティの担保がなされていることから、システムの脆弱性に重大な問題があるというものではない。

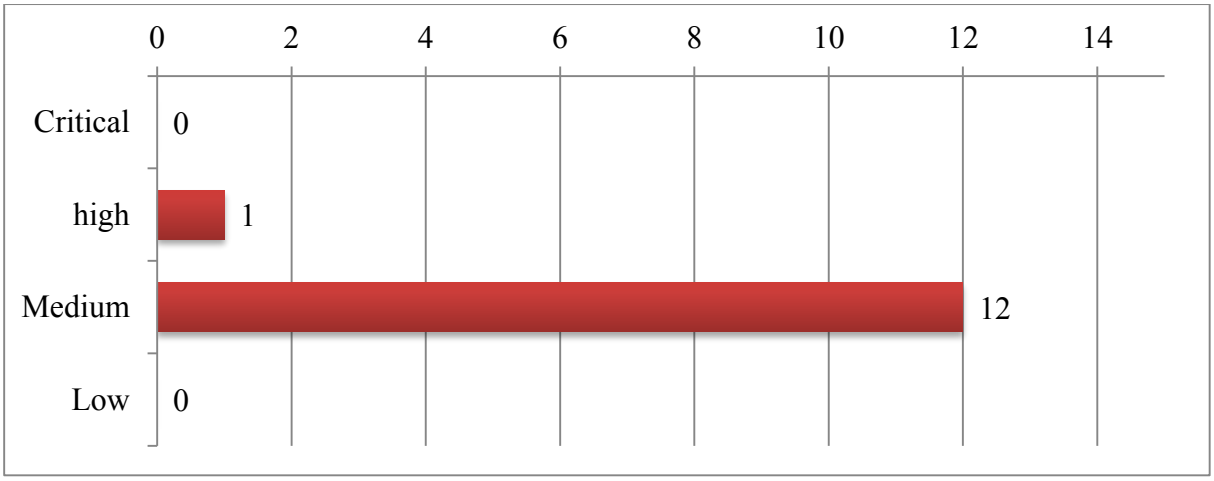


図 5.2-3 内部側ポートの脆弱性診断結果

検出されたセキュリティホールのうち、High レベル 1 件及び Medium レベル 8 件については仮想化ソフトウェアへのパッチ適用により対応可能なものであるが、前述のとおり現状の運用においては定期的なパッチの適用は行われていない。その他の検出されたセキュリティホールとしては、SSL に係る指摘が 3 件、通信のトランスポート層に係る指摘が 1 件であり、これらについては内部側のポートが不特定多数に開かれたものではないことを考慮すると、即座に対応が必要なレベルのセキュリティホールではない。

以上から内部側のポートについても、データセンターの適切な管理等を前提とすると重大な脆弱性はないと判断される。但し、検出された High レベルのセキュリティホールを含め、適切にパッチが適用されていれば更に良好な状態である点もあることから、定期的なパッチの適用を含めて、セキュリティポリシーに則った運用管理を行うことが重要である。

5.3 政府機関の WEB サイトの脆弱性診断

5.3.1 脆弱性診断の対象とする WEB サイト

「ミ」国における政府機関の WEB サイトのセキュリティ対策の状況把握の一環として、具体的なシステム（サーバ）を選定したうえで、以下の手段により脆弱性診断を実施した。

- 脆弱性スキャンツール（Nessus）により潜在的な脆弱性情報の取得
- 脆弱性情報をもとにセキュリティポリシーの策定担当者または実施担当者に対する個別ヒアリング調査により脆弱性の影響評価
- どのような事態がどの程度で発生し影響を与えるかリスクの評価

2015 年 8 月末現在において、政府機関の WEB サイトの多くはヤンゴンの Hanthawady に設置されており、MPT が政府、民間を対象に提供しているホスティングサービスを用いて実装されてい

る。脆弱性診断を行う対象として、ヤンゴンの Hanthawady に設置されている典型的な政府機関の WEB サイトとして、MCIT の WEB サイト（http://www.mcit.gov.mm/）を対象として選定した。

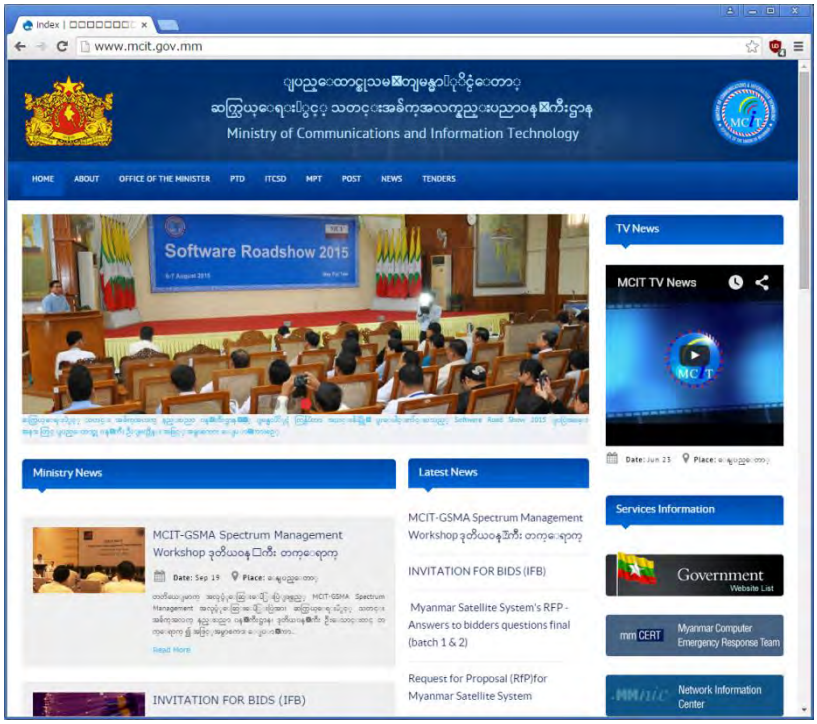


図 5.3-1 MCIT の WEB サイト

5.3.2 WEB サイトの概要と脆弱性診断のポイント

MCIT の WEB サイトは静的コンテンツを格納が格納された一般的な WEB サーバにより実現されている。前述したように、当該 WEB サーバは MPT の Hanthawady データセンターに設置されている。サーバのオペレーションは MPT（ヤンゴン）、コンテンツ管理は MCIT（ネピドー）が担当しており、コンテンツ管理者は部局毎におり、それとは別にモデレータが置かれている。

今回の脆弱性診断は、政府としての管理能力を検証するという側面が強いことから、MPT におけるオペレーションに焦点を当てるのではなく、MCIT のセキュリティ管理水準と、その管理の結果として脆弱性がどの程度存在するのかについて明らかにすることを目標とする。以上の目標から、WEB サーバに対する攻撃としては、ユーザや外部者によるインターネット側からの攻撃の可能性を重視し調査を行った。

5.3.3 WEB サイトの脆弱性診断結果

(1) インターネット側からの脆弱性診断結果

インターネット側のポートは様々な外部からの攻撃にさらされることが想定されることから、何らかの形でファイアウォールを潜り抜けたインターネット上からの攻撃を受ける可能性を有しており、攻撃の可能性・頻度としては内部側に比べると高く、十分なセキュリティ対策がなされていることが重要である。

2015 年 8 月時点で脆弱性スキャンツール（Nessus）を用いて実施したインターネット側からのセキュリティホール等の診断結果は下図のとおりであった。

検出されたセキュリティホールの重要度は、緊急性の高い方から「Critical」「High」「Medium」「Low」の 4 段階に分類されており、実質的に Medium 及び Low については、時期をみて対応又は念のため危険性について認識をしておくといったレベルのものとなる。

WEB サーバのインターネット側ポートについては、Medium レベルのセキュリティホールが 9 件、Low レベルのセキュリティホールが 1 件検出されたものの、早期又は緊急の対応が求められる High 又は Critical レベルのセキュリティホールは検出されず、調査時点で比較的セキュリティ対策が施された状態であることが確認された。なお、MCIT の WEB サイトはテストサイトなどが存在しないため、実稼働中の WEB サイトを対象として脆弱性検査を行った。したがって WEB サイトの稼動に影響があるような脆弱性検査手法を用いることが出来なかったことから、上記の結果は本 WEB サイトの既知の脆弱性を全て調査したものでない事に留意する必要がある。

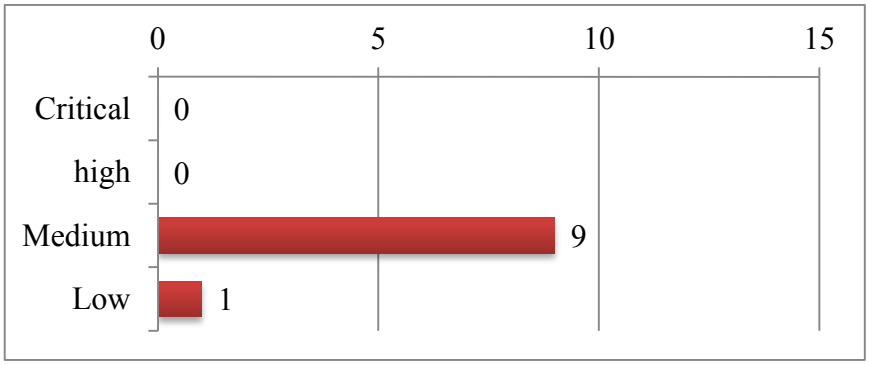


図 5.3-2 インターネット側ポートの脆弱性診断結果

検出された Medium の脆弱性 9 件のうち 7 件、Low の脆弱性 1 件については、SSL のバージョンや SSL 証明書に関するものであり、当該 WEB サイトの性質を考えると望ましくは無いが、直ちに危険性があるというものではない。残りの Medium の脆弱性のうち一件は PHP のバージョン等の情報が開示されている脆弱性、もう一件はクリックジャッキングに関する脆弱性である。
いずれも Web サーバの設定を修正することが望ましいが対応自体は比較的容易である。

当該サーバに掲示されている情報は一般的なものであり、複雑なサービスを提供していないなどシンプルなものである。このため OS や WEB サーバのパッチを定期的に適用するだけで良いなど、運用段階でのセキュリティ対策の管理が比較的容易であることも、脆弱性が抑えられている要因と考えられる。

よって当該サーバにおけるインターネット側のポートについては、今後、必要なパッチの適用など、妥当な運用・保守作業が行われることで問題はないと考えられる。

(2) 管理プロセス面からの脆弱性診断結果

MCIT の管理者に WEB サイトの管理状況についてヒアリングを行うことで、管理面の脆弱性について評価を行った。具体的な管理状況は以下の通りである。

- 脆弱性管理・パッチマネジメント・インシデント管理等に関するルールや文書は存在しない（NCSC がルールを作成中）。
- 管理担当者は決められている。
- MPT に対する委託について、書面による取り決めは行っていない。
- MCIT 側では運用ログは管理していない（MPT 側で管理）。

- コンテンツのバックアップは取得している。

現状の管理面の課題としては、セキュリティや運用に関するルールが一切存在せず、また運用を委託している MPT との間での責任分界が不明確であるなど、多くの組織的脆弱性が存在していることがわかった。

5.4 政府機関データセンターの評価

5.4.1 調査方法

日本データセンター協会ではデータセンター事業者が「適切なセキュリティ」を実現したデータセンターを設計･運用することを目的に「データセンターセキュリティガイドブック」を策定している。これをもとに日本データセンター協会に対して「ミ」国におけるデータセンターのセキュリティを評価する際に基準となる項目を確認し、データセンターの品質、信頼性、可用性に関わる要素として以下の項目について調査を行った。

表 5.4-1　データセンター調査項目

No.	項目	内容
1	セキュリティゲート	入退館の規制・許可の手段としての機能
2	ラック	熱流構成、耐震性能、アクセス制御
3	入退管理	管理項目、記録機能
4	本人認証	被認証者の認証方法
5	画像監視	監視システムの構成
6	火災検知	発生検知システム、予兆検知システム
7	侵入検知	侵入検知センサー
8	統合管理	導入有無、システム構成
9	ネットワークセキュリティ	各種対策装置の導入状況と構成
10	立地条件	自然災害に対する条件､電力等のインフラ整備状況
11	事業の継続運用	予算割当、職員数、職員の技術スキル

出所：「データセンターセキュリティガイドブック」より作成

調査に際して上記項目を以下の物理的区画に落とし込み、各区画において配置されるべき項目を整理した。

表 5.4-2　データセンター調査区画・場所

No.	区画	場所
(1)	敷地区画	門扉
		外周フェンス
(2)	エントランス区画	正面来客口
		機器搬入・搬出口
		従業員出入口
		建屋窓・外壁
(3)	検査区画	手荷物検査室
(4)	共有区画	オフィス

No.	区画	場所
		サーバ室
(5)	重要区画	ラック
		重要設備室
(6)	外部区画	立地

これら項目ついて、現地を訪問し確認および管理者へのヒアリングにより項目ごとに実施した。

5.4.2 調査概要

調査対象：MCIT　S-12 ビルディング 1 階

調査場所：S12 Exchange Building, Nay Pyi Taw, Myanmar

調査日時：2015 年 8 月 4 日・5 日

現地対応：Tint Khine (MCIT IT Department, Second Assistant Engineer)

5.4.3 調査結果

(1) 敷地区画

門扉進入対策として、施錠可能かつ強固・十分な高さを持つ門扉が設置され、24 時間 3 交代制の警備員配置により入退場の管理が行われている。しかし、外周フェンスへの防犯システム・侵入検知システムは設置されておらず区画への侵入対策は十分ではない。

図 5.4-1　門扉

図 5.4-2　警備員駐在所

(2) エントランス区画

敷地区画の入場者に対してカメラによる監視は対策されているが、建物への入場について来館者受付等の対策はなされておらず、データセンター訪問者や建屋の他事務所への訪問者の区別なく入場可能となっており関係者以外のアクセスが可能で共連れ、不審者の侵入、破壊による侵入の恐れがある。

図 5.4-3　屋外監視カメラ

図 5.4-4　建屋入口

(3)　検査区画

手荷物検査室が設置されておらず、エントランス区画と同様に不正侵入、共連れ、不審物持込の恐れがある。

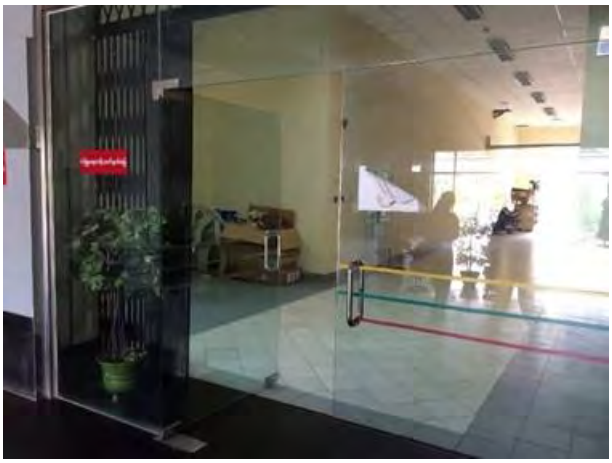


図 5.4-5　建屋内区画入口

(4)　共有区画

オフィス区画を設置し、UPS の設置とサーバ室内のネットワークカメラを監視しているが、オフィス区画への入退室管理システムがなく不正侵入の恐れがある。また、UPS からサーバ室への給電用のケーブルが露出しておりこれらの破壊により停電時の供給停止の恐れがある。

サーバ室は画像監視システム・指紋認証による入室管理システム、火災検知システムが設置されており、火災予兆検知システムの設置予定である。指紋認証については、登録を関係者に限定し部外者の独自侵入を防いでいるが、部外者の入室規定や在室カウントシステムはなく共連れ及び情報の不正持ち出しの恐れがある。

図 5.4-6　サーバ室入口(指紋認証)

図 5.4-7　オフィス入口

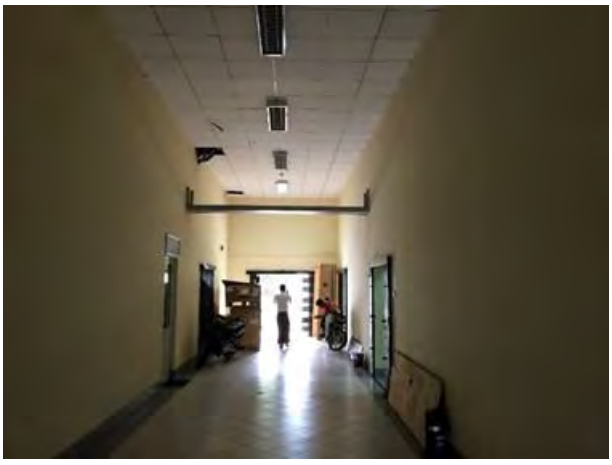


図 5.4-8　UPS 給電ケーブル

(5)　重要区画

サーバ室内において画像監視によりラックの不正操作に対する監視を行われているがラック扉の施錠管理が行われておらず、ラック設置機器への不正操作の恐れがある。その他重要機器である停電対策、冷房について需要量を計算して満足する容量の機器が設置さている。

ネットワークセキュリティについて、ADS、IDS/IPS が設置されておらず、OS 内部の対策も適切に行われていないことから、ネットワーク経由の攻撃に対するリスクもある。

*室内の写真撮影は許可されていないため参考写真なし

(6)　外部区画

電力供給について、配電所に隣接し一般の電力線とは別に 380V の専用線を引いて電源の二重化がなされている。停電時は専用線を利用し、さらなるリスクに備えて敷地内に自家発電機 2 台を設置している。立地環境について、対向 2 車線の比較的大きな通りに面しており、外部からアクセスが容易になっているため外部侵入のリスクがある。しかし、2005 年の建物の供与を開始して以来、洪水・地震・火災による被害は発生しておらず自然災害へのリスクが低い立地環境にあると考えられる。

図 5.4-9　配電線(2 系統)

図 5.4-10　非常用発電機

5.4.4　評価

データセンターの品質について、敷地外からの侵入に対策がなされているものの敷地内の対策において不足があるため、エントランス区画、検査区画への入退室対策が必要である。また、電力供給について十分配慮されているが、不正侵入者による UPS 給電の断線による停電が懸念される。共連れ防止と情報機器への不正操作に対して入退室の規定とラック施錠管理が必要である。

データセンターの信頼性について、ネットワークセキュリティ対策が不十分であることからネットワーク経由の不正操作が最も懸念される。また不正侵入者による情報機器への不正操作に対してネットワークカメラによる監視を行われているが、オフィス区画へのセキュリティ意識が不十分で体制的な整備も併用する必要がある。

データセンターの可用性について、実績から災害等による被害は発生していないものの万が一の不正侵入や破壊工作に対する備えは不十分であるため、安心できる水準ではない。

対象のデータセンターについて、実績から大規模な事故等が認められないことから安定した運用がなされていると判断されるが、上記の指摘項目が懸念としてあり、こられが満足されることでより安全な運用が保証されると考えられる。

5.5　政府機関におけるその他セキュリティ対策関連設備

「ミ」国では、2000～2010 まで、KOICA が中心となって電子政府のマスタープランを支援しており、「ミ」国の電子政府整備の後押しをしてきた。その一環として、サイバーセキュリティ関連プラットフォームとしては 2006 年に PKI の導入が行われている。

しかしながら、「ミ」国内の通信環境整備がこの数年のことであり、一般の利用者が依然として非力な環境であることや、一般向けの電子政府アプリケーションがほとんどないこととから、から、現時点での PKI の利用は極めて限定的であると想定される。今後、PKI を活用するためには、IC カード等、個人端末を必須としない利用方法の導入も検討が必要と考えられる。

5.6　通信事業者のセキュリティ対策

「ミ」国の通信事業者のセキュリティ対策について、現地通信事業者である RedLink 社と Yatanarpon Teleport 社からヒアリングを行った。

5.6.1 セキュリティへの取り組みについて

(1) RedLink 社

同社のサービスはインターネットアクセスの提供であり、ホスティングサービスやサーバスペースの提供などは行っていない。そのため具体的なセキュリティとしては同社のネットワークに対する防御が中心であり、ファイアウォールの設置、アクセス許可リストの整備、ユーザ管理等の基本的な対策が施されている。それ以上のセキュリティを望む顧客においては、顧客側で独自にファイアウォール等を設置することとしている。業務上でのセキュリティ対策としては、重要なドキュメント類には（Microsoft が提供するレベルの）パスワード及び暗号化を用いるようにしている。

これまで同社では、3 年ほど前に、国外からか国内か不明であるが大規模な DDOS 攻撃が問題となった。また、細かな攻撃を受けたりすることもあるが、サーバを停止されるような重大な攻撃は受けていない。ウェブサイトへの攻撃はあるが、重大な事態には至っていない。

同社はセキュリティの重要性については認識しているが、現状ではオペレーションに注力せざるを得ないため、IT セキュリティに特化したチームは構成できていない。セキュリティに関する担当者は配置しているが、主にファイアウォールの設定やアタックの特定等、サーバの防御を担当業務に限られており、サイバーセキュリティに特化した人材は少ない。

IT セキュリティポリシーは作成しているが、ISO27002 には準拠したものではない。また特に政府からも IT セキュリティに係るフレームワークは示されていないため、独自に作成したものである。mmCERT とは連携しており、様々な情報提供・情報交換を行っている。

(2) Yatanapon Teleport 社

Yatanarpon Teleport はインターネットアクセスの提供に加えて、自社のデータセンターからホスティングサービスなどをサービスとして提供している。同社では新たなセキュリティ対策部署を立ち上げたが、技術的専門性についてはまだ不足している状況で、まだまだ経験を積む必要性があると認識している。セキュリティの重要性については強く認識しているが、日々のオペレーションや顧客対応に人と時間がが割かれており、十分にセキュリティについて対応している余裕がないのが現状である。また、セキュリティや対 DDOS の機器等は非常に高価であるため、投資する余力がない。

2010 年に大規模な DDOS 攻撃を経験している。同社はルータである程度探知できる機能は有しているが、アタックに対する防御システム（Mitigation System）は持っておらず、ファイアウォールでの防御のみである。このためサーバ群については防御しているが、顧客のネットワークまでは防御できていない。

同社のホスティングサービスを利用している政府のウェブサイトがあるが、セキュリティに関しては政府からは特に要求はない。サイバーセキュリティに関しては、政府から法律やガイドラインが示されていないため、同社独自のポリシーを定めており、そのポリシーに従ってサービスを提供している。また特に SLA も設定していない。

サーバの導入やファイアウォールの設置、ホスティングサービスの利用等に係る簡易なセキュリティポリシーは策定しおり、具体的には不要ポートの停止や外部へのアクセスの管理等が盛り込まれている。アクセスロギングサーバを設置し、上記の新たなセキュリティ対策部署がアクセ

スを監視しており、異常があれば知らせるようになっている。DPI（Deep Packet Inspection）のデバイスも保持しており、顧客のネットワークに異常があれば顧客に知らせるようにしている。

5.6.2 通信事業者が抱える課題

「ミ」国では２年程前から政府が通信市場を開放し、移動体通信が伸びはじめたことでインターネット利用者が増え始め、これを踏まえて政府は e-Government を推進しており、サイバーセキュリティの重要性も高くなっている。これに対して、現状ではサイバーセキュリティに対する法制度やガイドライン等のフレームワークが何一つない状況である。ネット上でサイバー攻撃を受けて、キャリアがその IP アドレスを特定できたとしても、その情報をどこに報告すればよいのか何も決められていない。また、サイバーセキュリティ強化には、通信事業者同士の連携が重要となるが、現状では連携は十分にとれていない。mmCERT は通信事業者間のセキュリティに関する情報提供、情報共有の場としては機能しているが、通信事業者が最低限のレベル（共通するポリシー等）を有している必要がある。これらの現状を踏まえ、政府は早急に情報セキュリティ、個人情報保護、データ保護、サイバー犯罪等に対する法規制（フレームワーク）を整える必要がある。

人材育成に関しても課題がある。現在「ミ」国では、アカデミア（大学）と民間企業の連携はほとんどなく、民間企業が求めているものと大学が教育している内容には大きなギャップがある。特にサイバーセキュリティに至っては、コンピュータ系の大学を出てきた学生であっても、サイバーセキュリティに関する知識はほとんどなく、企業内での育成が必須となっている。今後は、産官学が連携してサイバーセキュリティ人材を育てていく必要がある。

5.7 中央銀行システムのセキュリティ対策

現在「ミ」国では、金融セクターの近代化を進めているが、中央銀行の本支店間及び市中銀行との間での資金決済等多くの業務が電子化されておらず、従って限定的にセキュリティ対策が実施されているものの近代化を見据えた対策は十分ではない状況にある。また、国際的な経済活動への参画にあたっても中央銀行の独立性及び機能強化、電子決済等の業務システム導入等が急務とされる中、金融政策の円滑かつ着実な実施のためにも中央銀行業務の効率化を進めている状況にある。

これらの現状から JICA では中央銀行における業務システムの整備行うため「中央銀行業務 ICT システム整備計画」プロジェクトを実施している。当該プロジェクトではシステムへのセキュリティ対策として主に以下の認識と考え方に基づいて進められている。

- 「ミ」国の金融業界におけるセキュリティ基準は策定されていない状態にあり、必要性が認識されている。
- 体制的な背景から、これまでほぼ全ての情報が機密情報として位置づけられており、資産管理のためのセキュリティ対策を考える場合重要資産への定義が先に必要である。
- ISMS に準拠し、かつ日常的な業務内容からセキュリティガイドラインをプロジェクト内で作成する。
- 当該システムはインターネットへの接続を前提としていないため、インターネットセキュリティに対する懸念は低いものの、普及啓発の観点から重要と考える。

- 監督機関である金融庁も監督指針として調整・政策反映を行う仕組みが必要である。
- 中央銀行では 40 人規模の Administration and IT Department : AITD がシステム所管部署に該当する。当該部署にはシステム防御の内部監査部門が存在しているが、システム監視機能を有していない状況である。

セキュリティ対策の前提となる重要資産の定義とそれらの運用に基づいたガイドラインの策定、そして担当部局の整備が必要であるとの認識のもと、相手国と協力して実施されていく計画である。

5.8 民間企業の動向、ニーズ

民間企業では通信事業社向けにサイバーセキュリティをサービスとして提供する海外会社があるものの国内企業で主たるサービスとして扱う企業は存在していない。国内民間企業の間ではサイバーセキュリティに対する脅威を認識しているものの、その対策がビジネスとして成立するかについては可能性を感じている程度に留まっている。また、海外の民間企業からは「ミ」国のサイバーセキュリティに関する現状はビジネスチャンスであると捉えられており、マイクロソフト社を始めとして対策の必要性を提唱する企業は多い。

一方、国内の IT 業界では近年の制度改革や規制緩和を受けて通信事業社を筆頭に大きく成長を続けている状態にあるが、システムインテグレータやソフトウェア会社等の周辺事業の成長が追いついておらず他国と比較して業界規模は小規模に留まっている状態である。また、事業社自身のセキュリティ対策も不十分であり、提供するサービスのセキュリティが担保されている状況ではない。

そのため、その中からもサイバーセキュリティを担う事業社が産まれる条件が未整備の状況にあると言える。そこで現在営業している国内 IT 企業に対して「ミ」国に IT 業界に関するヒアリング調査を行い、以下に民間企業から政府に対するニーズを整理した。

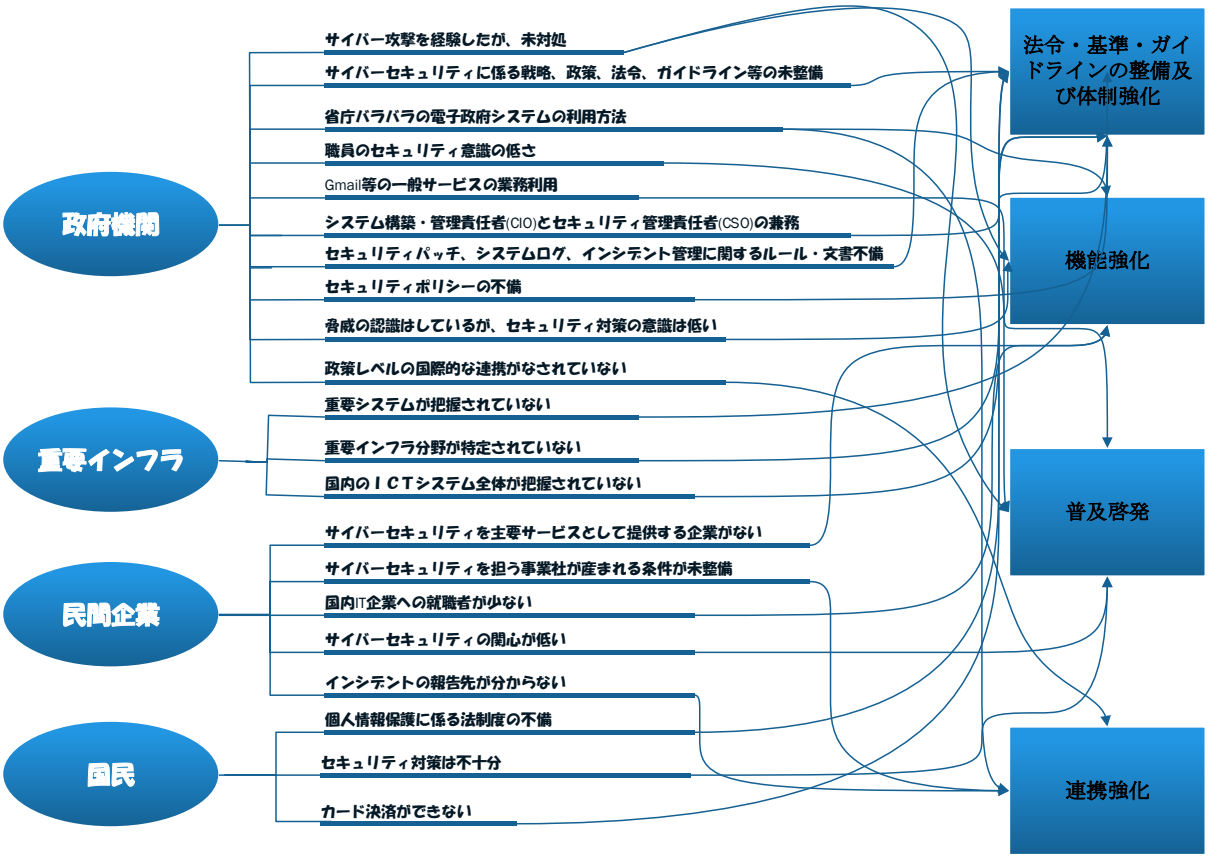
- IT 系を専攻した学生の就職が課題である。相当数の専門知識を備えた学生が卒業しているが、優秀な人材はシンガポール等の海外での就職を目指し、残りの人材も IT とは関係のない企業へ就職しているため国内 IT 企業への就職者が少ない状況である。IT 企業への就職を促進するような政策を期待したい。
- IT 業界の活性化を促進するため、IT に対する Government investment の増加を期待したい。
- 公共セクターの IT 資産等の調達について、より民間の競争促進が重要である。技術水準や仕様まで要求できる競争が同様に IT 業界の活性化につながる。
- 会社の設立に各機関への登録費用が発生することも IT 業界を含む起業に際しての障壁である。IT 起業は初期投資額がさほど高額でなくリスクの低いものであり、起業家は自己資金で全てを支払い設立している状況であるが、銀行からのローンを IT 企業へ拠出できる制度があれば起業は促進される。
- 多くの小規模 IT 企業が 1 年以内に起業している状況で、これは経済成長と通信インフラが改善されたことによる。これらの環境・条件のさらなる整備が望まれる。
- 法整備が技術の成長に追いついておらず、プロジェクト実施の障壁になっている。行政手続きの電子化に際して再度法律の見直しが重要である。
- e-Government の導入に際して、IT 利用およびサイバーセキュリティに関するポリシーが

無い省庁もある。さらにそれら省庁間のフレームワークが統一されていない点も問題である。これらの策定および統一を期待したい。

IT 業界の促進に関する要望や、IT 関係のプロジェクトに関する具体的な要望まで聴取された。これらから、サイバーセキュリティ対策を推進する上でも政府内部で省庁間の連携したポリシー策定や IT 業界の活性化を視野に入れた民間企業を活用する仕組みの構築が優先課題であると考えられる。

第6章　サイバーセキュリティに関する課題・対策の検討

第４章及び第５章から抽出されるサイバーセキュリティに関する課題を整理し、課題の項目ごとに対して検討した対策案について述べる。政府機関、重要インフラ、民間企業、国民の分野ごとに問題点・課題を以下の図にまとめる。それぞれの対象における課題について必要となる対策は、大きく分けて法令・基準・ガイドラインの整備、体制そのものの強化、それぞれの関連組織の機能強化、連携強化、全体としてサイバーセキュリティ対策の底上げをする普及啓発に分類される。以下に、対象分野における課題と対策案の対応を示す。



課題と対策の対応

なお、当該対策案に関しては 2015 年に策定されているサイバーセキュリティ戦略アクションプラン（案）との分類の仕方は異なっているが、アクションプラン（案）と同様に政府、重要インフラ、民間企業及び国民を対策の対象とするものであり、実施すべき対策が複数の対象分野にまたがるものや順序関係に依存し平行して進められない項目もあるため、上記の分類に整理する。

6.1 政府のセキュリティ対策実施機関、政府機関及び関連組織等におけるセキュリティ対策の課題

6.1.1 法令・基準・ガイドラインの整備及び体制強化

4.5 節の政府のセキュリティ対策実施機関の活動状況によると、2000 年初頭から電子政府化の取り組みは進められているが、各省庁が電子政府を利用するためにセキュリティを確保しながら安心して導入できるガイドラインやガイダンスが整備されていないため、電子政府の導入を検討している各省庁にとって電子政府を導入・利用することへの不安は大きい。また、ウェブアプリケーションは MPT が提供しているホスティングサービスを利用している省庁が多いが、セキュリティに関する基準や具体的な規定等は定められていない。

重要インフラにおけるサイバーセキュリティ攻撃は国民の生活に大きな影響を及ぼすので他国からの攻撃の対象となることも想定されるが、「ミ」国では守るべき重要インフラ分野の定義及び対象となる分野も特定されていない状況である。

インターネットの利用及びスマートフォン等の携帯端末の利用が急増しているが、市民の利用を対象としたリテラシー教育を目的としたガイドラインや個人情報保護法等の法律が整備されていない。

また、政府内の体制に関する課題としては、情報資産のインベントリ作成、整理及び管理、リスクアセスメントの実施がなされてない。各省庁間でのセキュリティインシデントやサイバーセキュリティ対策実施のベストプラクティスが情報共有されていない。各省庁の電子政府システム及びウェブアプリケーションを監視する体制及び環境が整備されていない。そもそも、IT&CS 内の NCSC のスタッフが確保されていない。各省庁に CSO が設置されておらず、任命されている場合も CIO と兼務している省庁が多く、情報システムを促進させる CIO とサイバーセキュリティの視点からチェック・監査する CSO との役割分担が明確化されていない。情報通信に関連する組織として MCIT と MPT の役割分担も現時点では、明確化されていない。

6.1.2 機能強化

各省庁における情報システムは出入りが自由であり、監視機能が機能していない等、物理的対策が実施されていない場合が見受けられる。また、FW、IPS/IDS、ウィルス対策ソフトウェア、フィルタリングソフトウエアの導入・運用等の技術的対策に関しても各省庁でレベル間がある。電子商取引に関しては、国際基準への対応もこれからである。

政府のセキュリティ対策実施機関においても、インシデントの検知・解析スキルを保有する人材は少なく、人材育成するプログラムや定期的にトレーニングするための施設も整備されていない。各省庁における CSO の育成、CSO が率いるサイバーセキュリティチームを構成するための人材育成も平行して必要である。政府だけでなく、今後、必要となる重要インフラや民間企業においても同様のスキルを有する人材の確保は近い将来、課題となる。

6.1.3 連携強化

国内においては、重要インフラ分野の特定がされていないため、重要インフラセキュリティの情報共有や連絡体制が整備されていない。また、社内 CSIRT を構築している民間企業はほとんど

ないためインシデントが発生した場合、mmCERT との連絡や報告体制が確立していない。

国際的な課題としても、現状では APCERT や JPCERT/CC からの情報提供が主の状況であり、逆の情報提供数は少ない。

6.1.4 普及啓発

各省庁の局長級レベルのサイバーセキュリティに対する意識はそれなりに高いものの、PC を使用していない、使用が限られている全職員のサイバーセキュリティリテラシーは非常に低く、サイバーセキュリティに対する意識もない状況である。

民間企業における経営層、情報システム責任者のサイバーセキュリティに対するサイバーセキュリティ意識は低いため、セキュリティ担当者がサイバーセキュリティに対するセミナーやトレーニングに対する関心を示したとしても、具体的に実施される頻度は低い状況である。

6.2 各課題に対するサイバーセキュリティ対策案

6.1 節の課題に対するサイバーセキュリティ対策案を以下に示す。

表 6.2-1 セキュリティ対策案

大項目	小項目	対策	内容
法令基準ガイドラインの整備および体制強化	法令・基準・ガイドライン等	電子政府（e-Government)の利用におけるサイバーセキュリティのベースライン基準の策定	MCIT が各省庁の電子政府を利用する際に最低限必要なセキュリティ基準を策定し提供する。
		ウェブアプリケーション（各省庁のホームページ利用を含む）の利用における具体的な規定の策定	MCIT が各省庁の web アプリケーションを利用する際の具体的な手順セキュリティ基準、留意点、等を策定し、提供する。
		各国の重要インフラ分野を参考にしミャンマー国に合致した重要インフラ分野を特定（定義）し、重要インフラ分野ごとにサイバーセキュリティ対策の水準を定めた「安全基準」の策定支援	国家サイバーセキュリティステアリングコミッティーが、各国の重要インフラ分野を参考にし、ミャンマー国に合致した重要インフラ分野を特定（定義）する。
			MCIT が重要インフラ分野ごとにサイバーセキュリティ対策の水準を定めた「安全基準」の策定ガイドラインを作成する。
			重要インフラ分野ごとにサイバーセキュリティ対策の水準を定めた「安全基準」を策定する。
		利用者が急増しているスマートフォン、モバイルバンキング等の利用を対象とした個人情報保護法の整備	MCIT が通信関連法（Telecommunications law 2013 年に制定）の整備、修正する（個人情報保護法の有無は別途確認）。

大項目	小項目	対策	内容
		サイバーセキュリティに対する関連法の整備	MCIT がサイバーセキュリティ基本法、不正アクセス禁止法等を整備する。
		MCIT の基準に基づき業界団体によるサイバーセキュリティガイドライン整備	MCIT の基準に基づき、業界団体がサイバーセキュリティガイドラインを作成する。
	体制整備	各省庁の横断的情報共有フレームワークの構築・運用	各省庁から情報セキュリティに関する責任者を特定し、MCIT が事務局をしながらサイバーセキュリティに関する情報を定期的に共有する体制を構築する。
		各省庁の電子政府システムおよびウェブアプリケーションシステムを省横断的に２４時間監視するＧＳＯＣの体制構築（人材育成含む）および環境整備	MCIT が GSOC をオペレーションできる人材を確保し、育成するとともに 24 時間インシデントを監視できるために、インンシデントの検知・解析する機材の調達、ライセンス購入・維持を含めた環境整備を行う。
		MCIT のセキュリティ関連職員（特に National Cyber Security Center、mmCERT）の人員確保	MCIT が提供する機能を果たすに十分なセキュリティ関連職員（特に National Cyber Security Center、mmCERT）の人員を早急に確保する。
		各省庁における CSO の設置および CIO との役割分担の明確化	各省庁が CSO と CIO を任命し、セキュリティとＩＴシステム構築の役割分担を明確にする（職務分離）。
	役割分担	通信セクターの体制リフォーム	MCIT と MPT のサイバーセキュリティ分野における役割分担を明確にする。
		MCIT を中心とした各省庁との連携体制構築	MCIT が情報共有のための他省庁との情報連絡委員会（仮）組織を設置する。
		政府間の国際連携強化	海外の POC(Point of Contact)である National CERT との政策的に連携する仕組みを構築する。
機能強化	機材･アプリケーションの整備	各省庁における情報システムへの物理的対策の強化	MCIT の主導の下、各省庁が生体認証機能、入退室管理機能、監視カメラによる監視体制を徹底する。
		各省庁における情報システムへの技術的対策の強化	MCIT の主導の下、各省庁が Firewall、IPS/IDS、ウィルス対策ソフト、Proxy サーバ、メールフィルタ、認証システム、ログ管理、暗号化の導入および適正運用を徹底する。

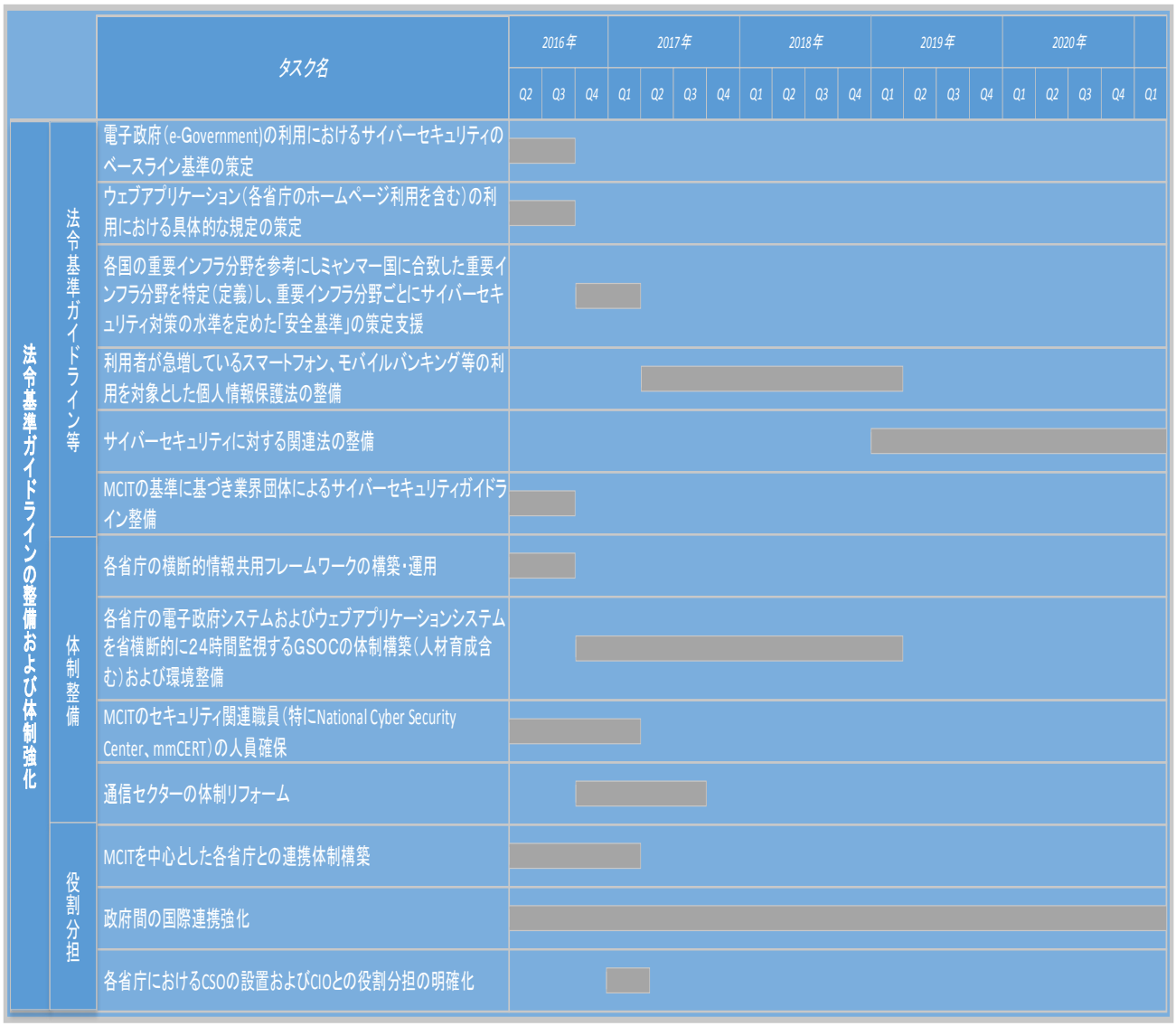
大項目	小項目	対策	内容
		IEC62443、PCIDSS 等の国際標準の導入を前提とした制御システムや電子商取引セキュリティ対策の推進	将来、エネルギーマネジメントシステムやクレジットカード決済などを促進するために、国際基準 PCIDSS を導入する。
	人材育成	政府システムにおけるインシデントの検知・解析能力の強化	National Cyber Security Center, mmCERT, 各省庁の CSO およびサイバーセキュリティチームのインシデント検知・解析能力を強化するためのトレーニングを MCIT が定期的に実施する。
		重要インフラにおけるインシデントの検知・解析能力の強化	MCIT が作る基準を基に、重要インフラを所轄する各省庁がインシデント検知・解析能力を強化するためのトレーニングを定期的に実施する。
		民間企業におけるインシデントの検知・解析能力の強化	業界団体などによるインシデント検知・解析能力を強化するためのトレーニングを定期的に実施する。
		各省庁の CSO の育成およびＣＳＯ率いるサイバーセキュリティチームの人材育成	MCIT の主導の下、各省庁がサイバーセキュリティポリシーの策定、サイバーセキュリティアセスメントの実施、サイバーセキュリティ監査の定期的実施、サイバーセキュリティ評価・報告を実施する。
		諸外国との連携を含めたサイバーセキュリティ人材育成のための研修、サイバー演習の実施	MCIT の調整の下、諸外国におけるサイバーセキュリティ関連機関との連携によりサイバーセキュリティ人材育成のための研修、サイバー演習を実施する。
		大学・大学院、研究機関、コンピュータ関連民間団体(ＭＣＦ等)と連携したサイバーセキュリティ人材の量的拡大と質的拡大	・情報連絡会を設置する。 ・大学・大学院、研究機関、コンピュータ関連民間団体(ＭＣＦ等)が人材交流（講師派遣、インターンシップの推奨）できる政府のスキーム立ち上げを行う。 ・コンピュータ技術者の地位向上施策を行う。
		教材の開発	政府職員に対する人材育成プログラム、オンライン教材の開発を行う。
連携強化	国内	重要インフラセキュリティ情報共有・連絡体制の構築・運用	IT&CS を事務局とした重要インフラセクター、重要インフラ監督省庁などを含めた重要インフラセキュリティ情報共有・連絡体制の構築・運用を行う。

大項目	小項目	対策	内容
		個別社内 CSIRT と mmCERT との連絡体制構築	一般企業において社内 CSIRT が普及するため、mmCERT が CSIRT 構築ガイドラインやツールを提供するとともに連絡体制構築およびサイバー攻撃に対する緊急対応体制を強化する。
	国際	各国のベストプラクティスに関する情報の共有と活用	MCIT 主導の下、各国のサイバーセキュリティに関するベストプラクティスの情報を収集し、適宜政府内に展開する。
		国際連携を利用した情報セキュリティ基盤の整備	MCIT 調整の下、ASEAN 諸国の CERT/CSIRT 間地域連携などの政策的国際連携を利用した情報セキュリティ基盤を整備する。
普及啓発		各省庁の全職員に対する普及啓発	各省庁の全職員に対するサイバーセキュリティリテラシーを向上するプログラムを実施する。
		企業の経営層、情報システム担当者に対するセキュリティ関連普及啓発活動の実施	ISO/IEC27014(セキュリティガバナンス）の基準に基づいた普及啓発活動の奨励(政府調達での ISO の取得義務付け等)し、サイバーセキュリティ人材の需要を促進する。
		サイバーセキュリティ意識向上のための啓発活動の実施、サイバーセキュリティリテラシー向上	国民に対するスマートフォン利用におけるサイバーセキュリティ普及啓発コンテンツを開発し、普及を促進する。。
		各府省庁のサイバーセキュリティ対策の推進力強化	MCIT が各省庁に対しサイバーセキュリティ対策に関する普及啓発活動を定期的に実施する。

6.3　対策の順序

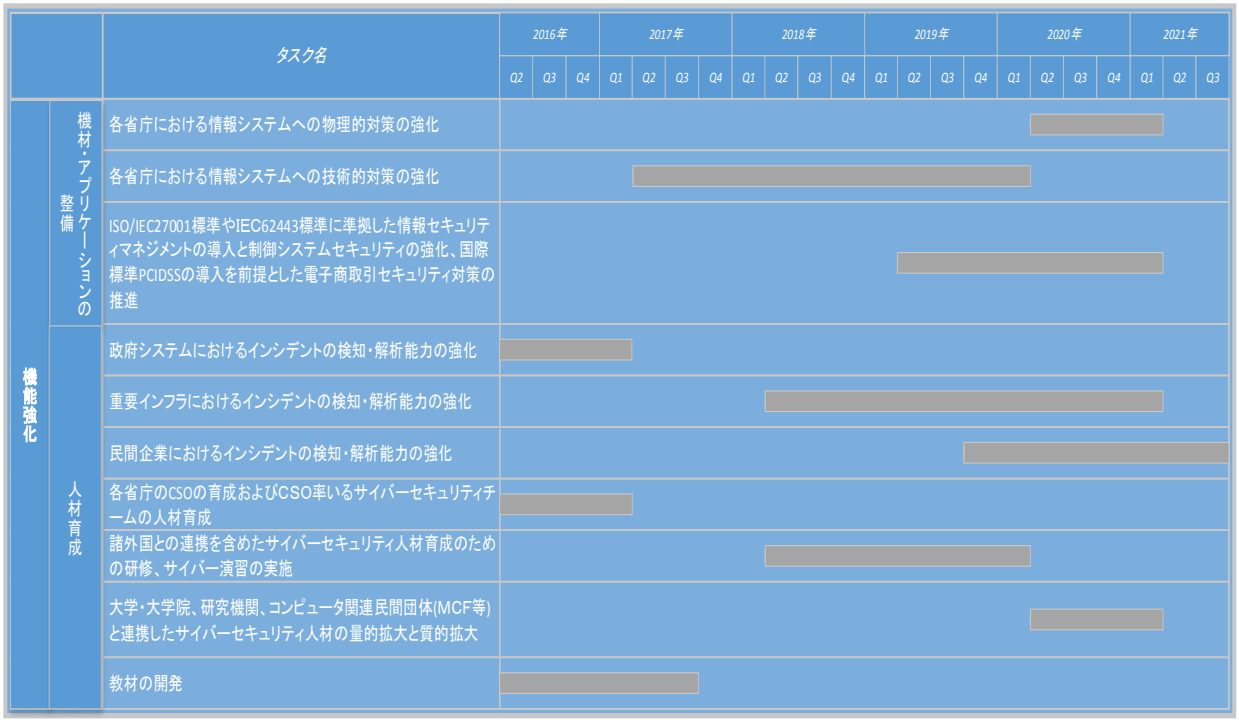
対策の順序としては、「ミ」国における重要度及び緊急性を考慮し、以下に大項目ごとのロードマップを示す。ます、初歩的なガイドラインや規定を策定するとともに各省庁横断的な共有フレームワークを構築することにより、電子政府の安全な利活用を推進し、政府内での役割分担が明確化され、サイバーセキュリティの監視・対策を進める体制が整備されていく。

表 6.3-1　法令基準ガイドラインの整備及び体制強化のロードマップ



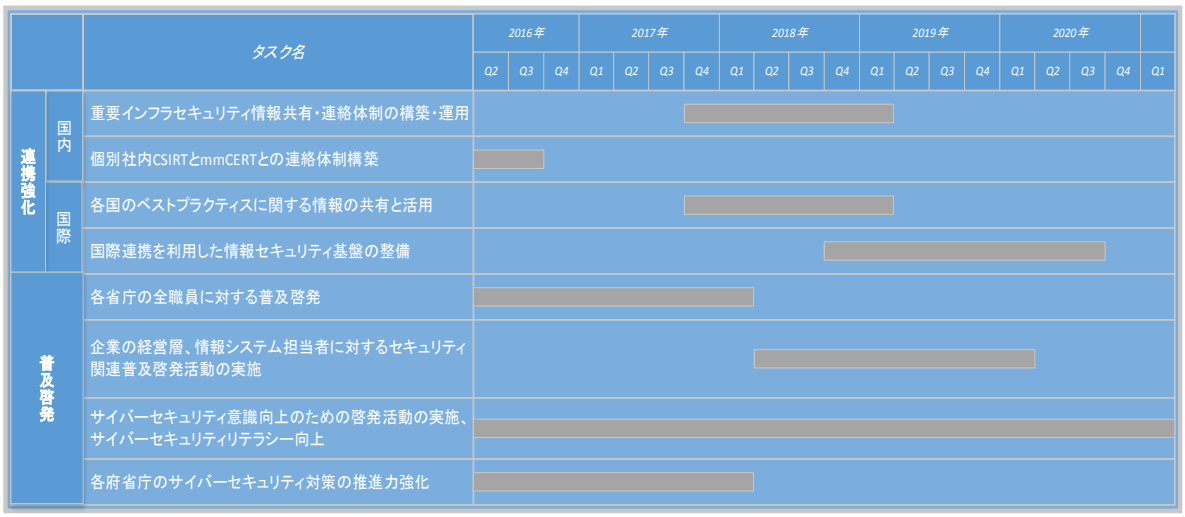
教材コンテンツの開発を進めるとともに政府システムにおけるインシデントの検知・解析能力、各省庁のサイバーセキュリティチームのための人材育成を強化することにより、政府全体の機能を強化する。人材育成の準備が整ってきたところで、政府の情報システムの物理的対策及び技術的対策や国際標準化に準拠した機材・アプリケーション環境の整備を強化する。

表 6.3-2　機能強化のロードマップ



中長期的に CSIRT 関連組織、重要インフラ、政府による国内連携、国際連携を強化していく。また、政府の全職員、国民全体を対象とする普及啓発に関しては活動を早期に開始するとともに、継続的に展開していく。

表 6.3-3　連携強化及び普及啓発のロードマップ



第7章　我が国による支援の内容、および優先項目に係る検討

7.1　支援策検討方針

業務指示書に記載されている我が国による支援内容検討に際しての留意事項は、重要度、緊急性、維持管理能力、開発課題及び我が国独自の優位性の有無となっている。また支援内容検討にあたって前提となるインフラ整備がある場合は、その前提条件の検討も行うこととなっている。

そのため、我が国による支援内容の検討及びその優先項目に係る検討方針は、まず、第 6 章で検討した「ミ」国において実施されることが望ましいと考えられるサイバーセキュリティ対策案ごとに下記の 6 項目について検討を行い、合わせて ODA 案件として利用可能なスキームを検討する。その上で、プロジェクト・案件ごとに、ODA 案件としての妥当性を検討する。ただし、下記 6 項目に合致するものを個別支援案として実施することは、支援の非効率を生むことが想定されるため、具体的なプロジェクト案を検討する中で、同一プロジェクトとして実施できるか考察する。

なお、支援内容検討のためのインフラ整備の前提条件検討に該当するものが無かったため、検討方針項目から削除した。また、現地調査中には、通信・情報技術副大臣から、ICT 関連の市場は急激に成長しており、本調査の最終報告書が提出される予定である 12 月には現在の状況が激変していることに対する懸念があり、プロジェクトの早期開始を望んでいること、長期的な未来ではなく、短期的な未来を考慮して支援を進めてほしいとのコメントがあったことを付記する。

① 重要度の高いサイバーセキュリティ対策に対する支援であること
サイバーセキュリティ対策を体系的に整備していく中で、実施による社会的インパクト等が見込め、かつその他の対策案にもインパクトを及ぼすものかどうか評価検討する。

② 緊急性の高いサイバーセキュリティ対策に対する支援であること
サイバーセキュリティ対策を体系的に整備していく中で、時系列的に早期の段階で取り組むべきものを評価検討する。第 6 章で記載している対策案実施のタイムラインで早期の実施が求められており、なおかつ、当該対策を実施しないと他の対策が滞る可能性があるかどうかを判断する。

③ サイバーセキュリティに関する経験・知識等が不足しているため、「ミ」国独自で進めることが難しいもの
現状の「ミ」国における技術力では対処が難しいものを評価検討する。技術力は個々の技術者の能力だけではなく、組織として必要な人員を確保しているかなどの点も踏まえる。

④ 将来的な「ミ」国における持続的な取り組みへの期待を阻害しないもの
「ミ」国が将来にわたり、他国・ドナーからの過度な支援に依存しないことに配慮し、既に「ミ」国独自の取り組みが始まっているもの、「ミ」国のイニシアティブによって行うべきもの、支援案件を通じ、「ミ」国が独自に進めていくことができると想定できるものについて、評価検討する。

⑤ 我が国において活用可能な技術を有しているもの
既に我が国において、同様の制度、政策、計画及び体制整備等が実施されており、我が国の成功モデルが「ミ」国の現状を鑑みて参考にできるもの、我が国で製造されている機材、ソリューションが世界市場において、その競争力が極めて高いもの等について評価検討する。

⑥ ODA スキームの検討方針
技術協力プロジェクト、無償資金協力事業、円借款等、我が国の ODA スキームとして活用可能なものを検討する。また「ミ」国独自で実施すべきもの、実施する能力が既に備わっているもしくは今後見込めるものについても合わせて検討し、すべての対策が ODA による支援を基にするものではなく、自立発展性の確保に配慮する。また活用可能なスキームの検討だけではなく、同一プロジェクトとして実施できるかも合わせて検討する。

7.2 支援策案の検討

7.2.1 支援策案検討方針に対する評価

第 7.1 節に述べた支援案検討方針に基づいて、第 6 章で述べたサイバーセキュリティ対策案について、それぞれ、検討方針事項に対してどのように評価できるか整理したものが、表 7.2-1 である。合わせて、備考欄に検討方針を鑑みた必要性等についても記述する。

表 7.2-1　「ミ」国で想定されるサイバーセキュリティ対策案と我が国支援案検討方針の評価一覧

番号	大項目	中項目	小項目	重要度[1]	緊急性[2]	「ミ」国経験・知識不足[3]	持続的取組阻害[4]	活用可能な技術[5]	ODA スキーム[6]	備考
1	法令基準ガイドラインの整備および体制強化	法令・基準・ガイドライン等	電子政府（e-Government）の利用におけるサイバーセキュリティのベースライン基準の策定	◎	◎	◎	◎	◎	技プロ-A	電子政府のセキュリティ基準は、電子政府の運用の根幹となる。電子政府化が進行する中、策定は緊急を要する。
2			ウェブアプリケーション（各省庁のホームページ利用を含む）の利用における具体的な規定の策定	◎	◎	◎	◎	◎	技プロ-A	電子政府化に伴い、政府関連情報がウェブサイトを通じて提供する。安全な運用を行うために、規定の策定が急がれる。
3			各国の重要インフラ分野を参考にし、ミャンマー国に合致した重要インフラ分野を特定（定義）し、重要インフラ分野ごとにサイバーセキュリティ対策の水準を定めた「安全基準」の策定	◎	◎	◎	◎	○	技プロ-A	重要インフラを特定しないと、重要インフラに対するサイバーセキュリティ対策が施せない。
4				○	○	◎	◎	○	「ミ」国	上記の特定後に「ミ」国に適合した安全基準の作成のためのガイドライン作りが必要となる。
5				△	△	◎	◎	○	「ミ」国	上記の特定及びガイドライン作成後に「ミ」国に適合した安全基準の作成が必要となる。
6			利用者が急増しているスマートフォン、モバイルバンキング等の利用を対象とした個人情報保護法の整備	○	○	△	△	△	「ミ」国	将来的には必要となる法令であるが、スマートフォン等の利用に関する社会状況の詳細把握が先決である。
7			サイバーセキュリティに対する関連法の整備	○	○	△	△	○	「ミ」国	サイバーセキュリティ対策に関する基準作成を先行させ、具体的な対策を施した上で関連法令の整備を行うことで対応可能。
8			MCIT の基準に基づき業界団体によるサイバーセキュリティガイドライン整備	○	○	○	◎	○	N/A	国の基準、法令などが整備された上で、業界団体に裨益するガイドラインの作成が有効。
9		体制整備	各省庁の横断的情報共有フレームワークの構築・運用	◎	◎	○ 実行力無	◎	◎	技プロ-A	サイバー攻撃に対する個別対処を行う上で必要な情報共有を行うことは急務である。
10			各省庁の電子政府システムおよびウェブアプリケーションシステムを省横断的に２４時間監視する GSOC の体制構築（人材育成含む）および環境整備	◎	○ インシデントの把握が先決	◎	○	○	無償-A （一部）	インシデントの把握ができていないのが現状であるが、サイバー攻撃に対処するために、GSOC は必要な機能である。
11			MCIT のセキュリティ関連職員（特に National Cyber Security Center、mmCERT）の人員確保	◎	◎	× 既に計画案有	○	○	「ミ」国	人材の育成より、人員の確保が急務である。
12			各省庁における CSO の設置および CIO との役割分担の明確化	◎	◎	○ 実行力無	◎	○	技プロ-A	適切なサイバーセキュリティ対策を行うためには、CSO と CIO は別々に任命される必要がある。
13		役割分担	通信セクターの体制リフォーム	◎	○	×	×	×	「ミ」国	民営化予定の MPT の役割と MCIT の役割を明確にし､データセンターの維持など、必要な制度、仕組み等を検討する必要がある。
14			MCIT を中心とした各省庁との連携体制構築	◎	◎	○ 実行力無	◎	◎	技プロ-A	サイバー攻撃に対する個別対処を行う上で必要な情報共有を行うことは急務である。

番号	大項目	中項目	小項目	重要度[1]	緊急性[2]	「ミ」国経験・知識不足[3]	持続的取組阻害[4]	活用可能な技術[5]	ODA スキーム[6]	備考
15			政府間の国際連携強化	◎	◎	○	◎	○	技プロ-A	インシデントの分析には海外の CERT の連携が必要不可欠である。
16	機能強化	機材・アプリケーションの整備	各省庁における情報システムへの物理的対策の強化	△	△	△	○	○	「ミ」国	物理的なサイバーセキュリティ対策として効果があるが、まずは、基準やガイドラインを作成し、これに基づき、検討する必要がある。
17			各省庁における情報システムへの技術的対策の強化	○	○	△	○	○	「ミ」国	技術的なサイバーセキュリティ対策として効果があるが、上記同様、まずは、基準やガイドラインを作成し、これに基づき、検討する必要がある。
18			国際標準 PCIDSS の導入を前提とした電子商取引セキュリティ対策の推進	△	△	○	○	△	「ミ」国	電子商取引に関する様々な法制度、ガイドライン等の整備が先決である。
19		人材育成	政府システムにおけるインシデントの検知・解析能力の強化	◎	◎	◎	○	◎	技プロ-A	「ミ」国関係機関におけるインシデントの検知・解析能力は十分備わっていない。早急に技術力を向上させる必要がある。
20				○ 将来的な重要度高	○	○	○	◎	無償-B （他分野との連携）	インシデントを疑似的に発生させ、必要な技術力を養うもので、我が国においても同様の設備の成功例がある。将来的に「ミ」国が自立して人材育成を行うことが可能。
21			重要インフラにおけるインシデントの検知・解析能力の強化	○	△	◎	×	○	「ミ」国	重要インフラの特定やガイドラインが作成された後、実施すべき事案である。
22			民間企業におけるインシデントの検知・解析能力の強化	○	△	△	×	○	N/A	業界団体がサイバーセキュリティガイドラインを作成した後に実施すべき事案である。
23			各省庁の CSO の育成及び CSO が率いるサイバーセキュリティチームの人材育成	◎	◎	△	×	△	「ミ」国	CSO と CIO がそれぞれ任命されれば、「ミ」国で十分に実行する能力があると考えられる。
24			諸外国との連携を含めたサイバーセキュリティ人材育成のための研修、サイバー演習の実施	○	○	○	×	△	「ミ」国	まず基礎的なサイバーセキュリティ対処能力を高めた後に、実施していくことが望まれるもの。
25			大学・大学院、研究機関、コンピュータ関連民間団体(MCF等)と連携したサイバーセキュリティ人材の量的拡大と質的拡大	△	△	△	×	×	「ミ」国	裾野技術者育成の施策検討において、十分な情報共有が求められる。
26				○	○	△	×	×	「ミ」国	裾野技術者を育成するために、必要な施策である。
27				◎	○	△	×	×	「ミ」国	人材育成の長期的対策として、重要な施策である。
28			教材の開発	◎	◎	◎	◎	◎	技プロ-A	電子政府化に伴い、早急に政府職員向け人材育成プログラムの実施が求められる。
29	連携強化	国内	重要インフラセキュリティ情報共有・連絡体制の構築・運用	○	○	△	×	△	「ミ」国	重要インフラの特定や基準、ガイドラインの作成が先決である。
30			個別社内 CSIRT と mmCERT との連絡体制構築	○	○	△	×	○	N/A	一般企業に CSIRT の設置を奨励するガイドライン等の作成が先決である。

番号	大項目	中項目	小項目	重要度[1]	緊急性[2]	「ミ」国経験・知識不足[3]	持続的取組阻害[4]	活用可能な技術[5]	ODA スキーム[6]	備考
31		国際	各国のベストプラクティスに関する情報の共有と活用	○	○	Δ	×	○	「ミ」国	「ミ」国内のインシデントの内容把握を行った後に、活用可能な各国のベストプラクティスを検討することが効率的である。
32			国際連携を利用した情報セキュリティ基盤の整備	○	○	○	○	○	「ミ」国	既に mmCERT など国際連携を行っている。今後、政府内のサイバーセキュリティに対する組織が整備されれば、効果的な国際連携が行えるものと考えられる。
33	普及啓発		各省庁の全職員に対する普及啓発	◎	◎	◎	◎	◎	技プロ-A	電子政府化が進展する中で、政府職員のサイバーセキュリティリテラシーの向上は急務である。
34			企業の経営層、情報システム担当者に対するセキュリティ関連普及啓発活動の実施	○	○	○	×	○	N/A	民間企業向けのガイドラインの整備を行う中で、検討していく事案である。
35			サイバーセキュリティ意識向上のための啓発活動の実施、サイバーセキュリティリテラシー向上	◎	◎	◎	◎	◎	技プロ-A	スマートフォン需要が急増する中、国民向けの普及啓発策は急務である。
36			各府省庁のサイバーセキュリティ対策の推進力強化	◎	◎	Δ 実行力に欠ける	◎	○	技プロ-A	政府職員のサイバーセキュリティに対する普及啓発は持続的に行うことで、効果が増大する。

＜凡例＞
1 重要度：◎は重要度が高い
2 緊急性：◎は緊急性が高い
3「ミ」国経験・知識不足：◎は「ミ」国における経験・知識が不足している
4 持続的取組阻害：×は「ミ」国の持続的な取り組みを阻害する可能性が高い
5 活用可能な技術：◎は我が国において活用可能な技術がある
6 ODA スキーム：“技プロ”、“無償”等のスキームの後に記されている A、B の記号は、同一プロジェクトで実施するものかどうかを指している。また“「ミ」国”は、技プロもしくは無償等の ODA の実施ではなく、「ミ」国独自に実施すべきと考えられるもの、“N/A”は直接民間に対する支援となるので、ODA 案件として適応不可

7.2.2 技術協力プロジェクト

(1) プロジェクト概要

サイバーセキュリティにおける「ミ」国に対する我が国支援案の検討を行った結果、多くの重要でかつ緊急性の高い対策は、技術協力プロジェクトとして一つのプロジェクトにより、迅速に「ミ」国全体のサイバーセキュリティ対策につなげていくことが可能と考えられる。表 7.2-1 の ODA スキーム欄に「技プロ」と記載されているものが、該当するものである。

今後、「ミ」国で技術協力プロジェクトの要請を行う必要があると思われ、また技術協力プロジェクトの内容を「ミ」国政府と JICA で合意する必要があるが、現在想定できる内容を以下に記す。これにより、サイバーセキュリティに対する基礎的対応能力が整備され、並行して GSOC の設置環境の整備・強化支援策を検討することが可能となる。

なお、当該技術協力プロジェクトを実施することで、通信・情報技術副大臣のコメントにある短期的な対応の多くが対処されることになる。

以下、技術協力プロジェクト案の概要について述べる。また、第 7.3 節に本技術協力プロジェクト案に対する妥当性を検討した結果を述べる。

○ プロジェクト名:ミャンマー国サイバーセキュリティに関する能力向上プロジェクト(仮題)
○ プロジェクト目標:サイバーセキュリティに対する基礎的対応能力が整備される。
○ 上位目標:サイバーセキュリティに対する対応能力が高まる。
○ 成果:
成果 1:政策、促進策、制度、基準のガイドラインなどが整備される。
成果 2:サイバーセキュリティに関係する組織体制が整備される。
成果 3:サイバー攻撃に対するモニタリング機能が整備される。
成果 4:サイバー攻撃に対する職員の意識が向上する。

○ 主な活動

上記成果を達成するために考えられる主な活動案を下表 7.2-2 に示す。活動案は基本的に対策案と合致しているが、プロジェクトの持続性の観点に配慮し、今後必要な人材を育成するための礎となると期待されるものを加えている。

表 7.2-2 技術協力プロジェクト案の主な活動案

	主な活動(案)	表 7.2-1 に記載の対策番号
成果 1 関連		
1-1.	サイバーセキュリティのベースライン基準を作成する	1
1-2.	ウェブアプリケーションの利用における具体的な規定を作成する	2
1-3.	重要インフラの定義を行う	3
成果 2 関連		
2-1.	省庁横断サイバーセキュリティ情報連絡会を設置する	9 及び 14
2-2.	CSO/CIO の役割分担を行い任命する	12
2-3.	Point of Contact(POC)を任命する	15
2-4.	POC を通じた国際機関とのインシデント情報等を交換・共有する	15
成果 3 関連		
3-1.	各省庁の CSO および mmCERT のインシデント検知・解析能力を向上させるためのトレーニングを実施する	19
3-2.	政府職員向けオンライン教材を開発する	28
3-3.	大学、業界団体と連携したインシデント検知・解析能力研修カリキュラムを開発する	調査団からの提案
成果 4 関連		

	主な活動（案）	表 7.2-1 に記載の対策番号
4-1.	サイバーセキュリティリテラシー向上プログラムを作成する	33
4-2.	MCIT が各省庁向けにサイバー対策普及ワークショップを開催する	36
4-3.	スマートフォン利用におけるサイバーセキュリティ普及啓発コンテンツを開発する	35

○ C/P 機関
- 責任機関：MCIT
- 実施機関：MCIT　IT&サイバーセキュリティ局、mmCERT
- 関係機関：科学技術大学、ミャンマーコンピュータ連盟

○ 日本側投入
- 日本人専門家（6 分野、計 60 M/M 程度）
- インシデント検知機材（アプリケーション含む）
  参考例（冗長構成なし）

【S12 用】
- DDoS 検知
- IDS/IPS
- WAF

【研修用】
- ルータ
- DDoS 検知
- ファイアウォール
- メールサーバ
- メールフィルタ
- IDS/IPS
- ウェブサーバ
- WAF

○ 実施期間：3 年

(2) 検討課題

2014 年 7 月から 2017 年 1 月までの予定で、JICA による技術協力プロジェクト「情報セキュリティ能力向上プロジェクト」が実施されている。インドネシア情報通信省の情報セキュリティ対策実施能力が向上することをプロジェクト目標にし、①情報セキュリティ局の機能強化、②政府の各部局におけるセキュアな IT 利用をサポートする仕組みの確立、③情報セキュリティ啓発活動の改善が成果として期待されている。

上記(1)項で述べた技術協力プロジェクト概要案の活動には、「スマートフォン利用におけるサイバーセキュリティ普及啓発コンテンツを開発する」が含まれており、インドネシアにおけるプロジェクトにもサイバーセキュリティ普及啓発のための仕組みづくりや、これに必要な教材作成が盛り込まれている。さらに情報セキュリティ対策の将来トレンドを知るためのネットワーク作りとして、インシデント対応手順、重要インフラに関連したガイドライン及びデータセンターの標準装備・対応など、日本をはじめ ASEAN 各国の現状を調査することになっている。

先行する ASEAN 内の類似の技術協力プロジェクトと連携することにより、地域状況に合致したサイバーセキュリティの仕組みを作り、国民に対する啓発活動を進めていくことが可能となる。具体的には、第三国研修により、「ミ」国カウンターパートがインドネシアに赴き、プロジェクトの活動状況や進捗、また成果の取りまとめ状況を確認し、自分たちの活動に生かせるように検討することは価値がある。一方、インドネシアのカウンターパートは、「ミ」国からインシデントの状況など具体的な情報を得て、インシデント対応の訓練等に役立てることが可能となる。

7.3 技術協力プロジェクトに対する評価 5 項目による分析と結論

第 7.2 節で述べた技術協力プロジェクト案について、DAC の 5 項目評価に基づいた事前評価を下記に述べる。これにより、技術協力プロジェクトの案件形成が迅速に進むことを期待する。

7.3.1 妥当性

本プロジェクトは、以下の理由から妥当性が高いと判断される。

(1) 「ミ」国側の開発政策との整合性

「ミ」国では、韓国の支援を受け、2004 年に設置された国家対策委員会により、「ミャンマーICT 開発マスタープラン」が作成された。それ以降、電子政府基本システムを韓国の借款で行い、また MPT の設備、ネットワークの拡充を図り、ICT の国家的取り組みを進めてきている。

一方、「ミ」国は民政移行後に国家計画・経済発展省が中心となって国家開発計画である「National Comprehensive Development Plan（以下、NCDP）」を作成し、下記 7 つの戦略を打ち出した。

① Strengthening Governance & Institution
② Enabling Business Environment
③ Expand domestic & global connectivity
④ Fostering Competitive Sectors
⑤ Local Economic Potentials
⑥ Human Development
⑦ Environmental Protection

その後、「ミ」国は、NCDP を基礎として 2011～2015 年を対象とする 5 ヶ年計画を策定した（同 5 ヶ年計画は未公表）。一方、我が国は「ミ」国政府とともに「日ミャンマー共同イニシアティブ（MJJI）」を設置し、NCDP と 5 ヶ年計画を効果的に実行し、かつ「ミ」国における投資環境の整備を促進・迅速化するための具体的な取組を検討している。その結果、2015 年 7 月に「ミ」国産業発展ビジョンを我が国と「ミ」国政府は公表し、同ビジョンの柱となる 5 つの政策を、下記のとおりに定めた。

① インフラと連結性の向上をテコにした産業振興
② 予見可能で効率的なビジネス環境・制度基盤整備
③ 「人間中心の開発」を支える人材の育成
④ その他の戦略的・横断的政策

⑤ 農林水産業の潜 在力の具現化

これらの国家開発計画に基づき、「ミ」国通信・情報技術省は世銀の支援により「ミャンマー電気通信マスタープラン 2015」を作成中である。このマスタープランは、「ミ」国国内の人々を通信技術により有機的に結び付けること、経済活動の優位性を得るための高速インターネットによる接続環境を構築すること、電子政府化を促進することに焦点を絞っている。このマスタープランは最終化段階である。これに加え通信・情報技術省は ADB の支援で電子統治マスタープランを作り電子政府化のためのマイルストーンと実施事項を提言している。電子政府化及び「ミ」国のインターネット網の接続環境の向上は、開発戦略に密接につながり、分野横断的な課題で優先度の高い活動として記載されている。

反面、「ミ」国は、サイバー攻撃のインシデントインベントリ情報が整備されておらず、サイバー攻撃に対するリスクがどの程度顕在しているか測定も出来ない状態となっている。今後、通信網改善事業を通じて我が国の支援で通信網が拡充されていく中で、スマートフォンの利用などにより劇的に通信事情が変化し、ネット利用者が増えることで、「ミ」国が ASEAN 諸国を含む他国への踏み台にされる可能性がより高まっていくと考えられる。そのため、サイバー攻撃などセキュリティの脆弱性は、「ミ」国通信政策を推し進めるための障害であり、インターネットの普及や電子政府化の大きな妨げになるとともに踏み台攻撃に効果的に対処できないことに対して他国から非難を浴びる恐れもある。これらを勘案すると、サイバーセキュリティに対応する本技術協力プロジェクトは「ミ」国の優先度の高い開発ニーズへの貢献となり電気通信政策と合致している。

(2) 日本の援助政策との整合性

2011 年以降の新政権の民主化への取組を受け、2012 年 4 月に 2012 年 4 月 21 日に行われた日本・ミャンマー首脳会談において、二国間関係を強化する重要性が確認され、我が国政府は経済協力方針を変更した。支援の重点分野 3 つの内の一つとして「経済・社会を支える人材の能力向上や制度の整備」が示されており、人材育成や組織・制度の整備を重点に置き、サイバーセキュリティに対する基礎的対応能力を向上させる目的である本技術協力プロジェクトは同方針に合致する。

(3) 手段としての適切性

これまでの協力実績として、無償資金協力は「通信網緊急改善計画（2012 年）」、「中央銀行業務 ICT システム整備計画（2013 年）」、技術協力プロジェクトでは「ソフトウェア及びネットワーク技術者育成プロジェクト（2006 年～2011 年）」及び「工学教育拡充プロジェクト（2013 年～2018 年」等がある。これらのプロジェクト活動を通して生まれた人材を活用し、大学・業界団体と連携したインシデント検知・解析能力の研修カリキュラム作成を行うことは、過去案件との相乗効果が見込める。また、連携を行う大学・団体との体制構築が円滑になると想定され、プロジェクトを着実に実施する助けになるとともに、「ミ」国と我が国の情報通信分野の技術者の密接な関係構築を促進する可能性がある。さらに 2014 年には、KDDI と住友商事が「ミ」国 MPT との共同事業で、「ミ」国通信市場に参入をし、「ミ」国全土の通信網の整備及びインターネットサービスプロバイダーとしての業務など、MPT のあらゆる事業におけるパートナシップを得ている。本プロジェクトの実施により、「ミ」国の情報通信分野における我が国の優位性がより高まることが期待される。

7.3.2 有効性

本プロジェクトは、以下の理由から有効性が見込まれる。

(1) プロジェクト目標の内容

プロジェクト目標が示す内容は、「ミ」国の情報通信分野のマスタープランを根底から支える技術力の形成であり、サイバーセキュリティ対策が脆弱である場合、当該マスタープランで導入するシステムや仕組みが破壊されるまたは無駄になることが考えられるため、本プロジェクトの実施は有効である。

(2) 因果関係

プロジェクトの成果として、成果 1 でサイバーセキュリティに関する法的枠組み、政策、普及計画、ガイドライン等の整備を行うとしており、成果 2 と 3 では、サイバーセキュリティに必要な省庁横断的組織の構築、インシデント発生時の人為的対応力の強化と能力向上、サイバー攻撃の検知を行う機能を備える取組み内容であり、プロジェクト目標の達成に必要不可欠なものが適切に設定されている。また、成果 4 として取り組むサイバーセキュリティに関する普及啓発は、サイバーセキュリティの必要性、サイバー被害の拡大防止、長期的な人材育成への着眼動機づけとなり、プロジェクト成果と上位目標の達成にもつながり、成果、プロジェクト目標、上位目標の関連性が明確である。

7.3.3 効率性

本プロジェクトは、以下の理由から効率性の維持に留意する必要がある。

(1) 因果関係

本プロジェクトは、以下の点からプロジェクトの実現性と維持に懸念がもたれる。

第 1 に、サイバーセキュリティに関する基本計画が未作成であり、かつ「ミャンマー電気通信マスタープラン」及び「電子統治マスタープラン」が正式に「ミ」国政府で承認されていない。それぞれ最終化段階で大幅な内容変更があることは想定されていないが、変更される場合はプロジェクト活動に制約を与える可能性がある。第 2 に、政府機関は組織改変があり、MPT などを含めた MCIT 全体の組織改変が実行された。また工科大学、コンピュータサイエンス大学の所轄が教育省に変わることが計画されているなど、プロジェクトの関係機関を取り巻く状況の変化により、プロジェクトの意思決定や調整に手間取る可能性がある。第 3 に、第 2 と関係するが、組織改変により予算編成と予算割当に大きな変更がある可能性が否めない。予算の執行において、混乱が生じる可能性があることが、プロジェクトの効率性については懸案事項である。

7.3.4 インパクト

本プロジェクトは、以下の理由から正の影響が期待できる。

(1) 上位目標の内容

本プロジェクトは、政府の公共サービスの実施を円滑に進めるための取り組みであり、かつ急激に増えている携帯電話加入者へ間接的にアプローチするものである。ICT を効果的に利用し、

安全にかつ適切に ICT を活用した社会経済活動を営むすべての人々に間接的に裨益するものである。

(2) 波及効果

世銀、ADB などは、地方開発、ジェンダーへの取り組みについて、ICT を利用した職業訓練などを支援の重点に据えているため、他ドナーの活動との相乗効果も期待できる。また成果 1 で実施する活動は、「ミ」国の民間企業が安全に社会経済活動をおくる上で、必須である。サイバーセキュリティ対策に巨額の費用をかけることが困難な中小企業であるが、中小企業が「ミ」国全体の 87 %を占める中で、中小企業の保護・育成は「ミ」国の経済発展のためには重要である。また多くの中小企業の IT ベンダーへの間接的な人材育成にもつながる。

7.3.5 持続性

本プロジェクトは、以下のように持続性が期待できる。

(1) 政策面

ICT に関連した取り組みは、世銀、ADB などが重要項目として挙げている支援を実施する際のキーファクターとなっており、電子政府化はすべての省庁が実施すべき取組みとして位置付けていることから、政府全体での持続的な取り組みが期待できる。

(2) 組織面

国家サイバーセキュリティセンター（NCSC）を組織し、サイバーセキュリティの全般的な取り組みを実施する組織が明確になった。また科学技術省傘下となっていた mmCERT も NCSC の配下になり、政府内の体制が整備されつつある。新組織である NCSC には、これまで MPT の職員であった技術者が転籍する予定であり、人材確保策もある。

(3) 技術面

上述のように NCSC の技術者は MPT の職員の転籍によって確保される。これまで通信事業者として業務に従事していた基本的技術力を保有している技術者であるため、技術的に初歩から人材育成をする必要はない。また mmCERT は JPCERT 等と既に国際連携に基づき、情報を収集分析している。これらの枠組みは今後も継続され、国際連携による技術力の維持・向上が期待できる。そのため技術面での持続性は問題ない。

(4) 財政面

これまで政府がオンラインサービスの提供のために調達した機材、設備及び電子政府化のためのデータセンター構築においては、適切な運用経費が割当られ、ソフトウェアのライセンス失効などでシステムが停止するような状況は見受けられない。また各省庁の電子資産を管理するデータセンターについては、適切な運用経費が確保されない場合、サイバー攻撃を受けた際の政府内ダメージが大きく巨額の修繕費が必要となる。さらにプロジェクト活動によって構築される省庁横断的な調整機関が設置されることから、関係機関間での円滑な調整により予算が確保されることが期待される。

7.3.6 結論

本事業は、「ミ」国の開発政策、開発ニーズ、日本の援助方針と十分に合致しており、また計画の適切性が認められることから、実施の意義は高いと判断される。

7.4 無償要請に対する妥当性の検討

本調査は、「ミ」国政府の無償要請を契機に実施されたものであるため、無償案件は我が国の支援策として「ミ」国政府では期待されている。しかしながら、以下に記載する理由により、当該要請内容のまま我が国の無償案件として進めることは適切ではなく、第 7.3 節で述べた技術協力プロジェクトの進捗を見ながら、要請内容の見直しを行うべきである。

なお、当該要請は、表 7.2-1 に記載の対策案の中で番号 10 の一部が該当する。

7.4.1 要請書受領後の状況変化

(1) MCIT の組織改革

要請書に記載の機材の設置場所は、MPT が管理するデータセンターとなっている（詳細は次項(2)を参照）が、MCIT は省内の組織改革を 2015 年 4 月に実施し、MPT は通信事業だけを担当することになった。また IT&CS が新しくでき、データの整備、電子政府システムの構築、サイバー攻撃のモニタリング等を行っており、サイバーセキュリティ対策は MPT からの管轄外になっている。さらに MPT は来年民営化される予定となっており、ホスティングサービスにより民間通信事業者と当該データセンターにおいて競合関係にあり、また今後その関係が一層強まる可能性が高いため、本要請における ODA 支援には慎重な検討が必要である。

(2) MPT と IT&CS の役割

当初、無償資金協力事業による GSOC 機材の設置場所は、下図 7.4-1 の Hanthawady 及び Dakekina データセンターに設置させる予定であったが、上記組織改革により、当該データセンターは MPT が運営するデータセンターとなっている。

この 2 つのデータセンターには、MPT のホスティングサービスにより、各省庁のオンラインサービス用のウェブサーバ、メールサーバなどが設置されている。ちなみに、同様のサービスで、MPT の競合相手であるヤタナポンも政府省庁を顧客としている。

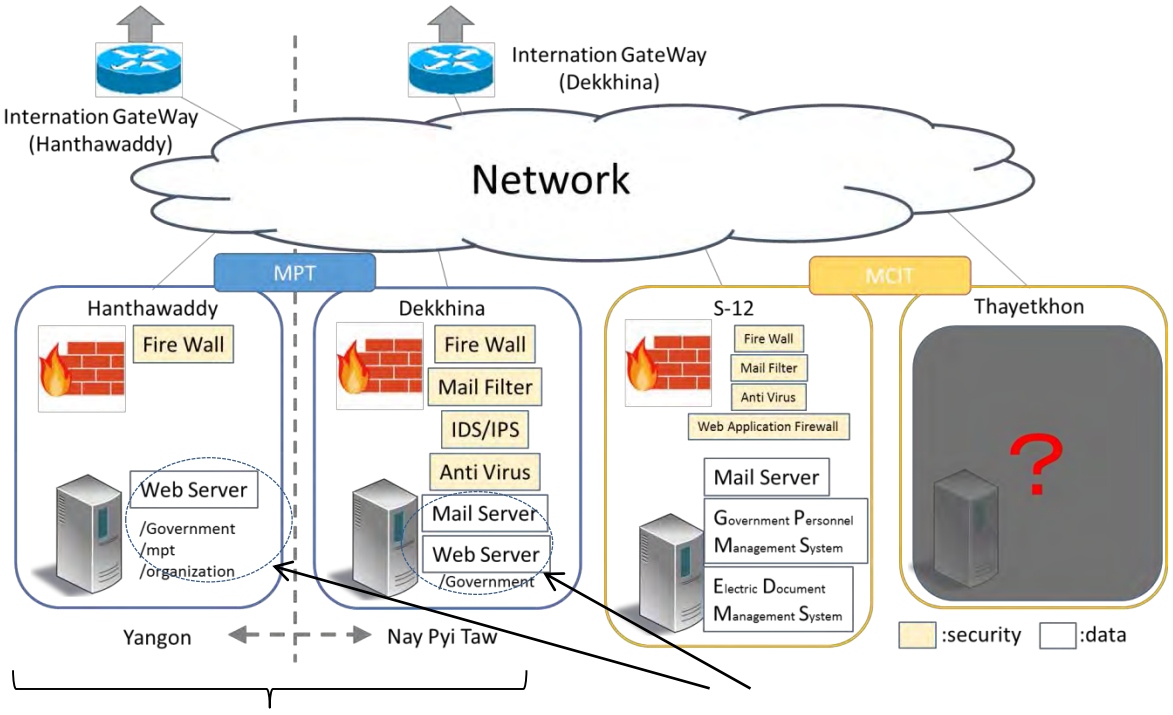


図 7.4-1　各データセンターと無償要請の機材設置場所の関係

一方、政府全体は電子政府を積極的に推し進めている。

理由は、ネピドーに遷都したことによる、行政サービスの低下を防ぐためのオンラインサービスの提供（例、産業省が実施している企業登録のウェブ化）、世銀が作成した ICT マスタープランによる電子政府化への取り組み及び ADB が作成した電子統治マスタープランなどが影響している。

そのため MCIT はネピドーの S-12 ビルに新しく電子政府の取組として、電子文書管理システム、政府職員管理システムなどを設置している。しかしこれらを運用する職員が新しい組織の IT&CS には不足しているので、今年度中に 50 人ほどの職員を MPT から転属させる計画を持っており、最終的には 200～300 人ほどを IT&CS へ転籍させる方針である。

7.4.2　無償資金実施の場合の課題

(1)　GSOC に対する機材案件の事業効果の測定

GSOC を設置した場合、GSOC の役割は、サイバー攻撃を防御するのではなく、サイバー攻撃を検知し、攻撃範囲や被害が、ある一定規模以上広がらないように人為的な判断を介し最終的な対処が行われるものである。また、サイバー攻撃の種類は様々で短期的な周期で進化し新たな攻撃手法を生み出している。そのため、定量的な事業効果の測定が課題である。

一般的に既知の攻撃に対処して、攻撃を防げるのは、25～30 %程度と考えられており、現状、既知の攻撃もほとんど検知できない中から 25 %改善するという見方もできるが、新たな深刻な攻撃を受けることもあり、そうした面を考慮した効果指標の設定は困難である。

一方、運用面の効果をベースに考えることも一考であり、たとえば、攻撃の検知数を事業効果指標にあげることがこれに当てはまる。

定性的な効果指標については、サイバー攻撃の可視化による、対処の容易さ、効率性などを踏まえて検討することが可能であるが、どのようなインシデントが実際に発生しているか把握できていない状況で、これらの検討をすることは困難である。

(2) MPT 改革と民間事業者への配慮

現在、各省庁のホスティングサービスについては、これまで MPT のネットワーク網を使用しており、メールなどは MPT のネットワークを通じてインターネットにつながっている。これらのネットワークの構成が影響し、民間通信事業者がホスティングサービスを省庁に提供する場合は、MPT による他の民間通信事業者向け料金設定によっては、実質的に排他的なサービスの提供になる可能性がある。一方、ホスティングサービスは一般的にセキュリティ対策を含めたサービスの提供もビジネスモデルとして存在しており、将来的にセキュリティを含めたサービスが民間通信事業者から提供される可能性もある。

今後、MPT の事業が政府事業として行っていたことを基礎に、排他的に実行できる場合は、通信料などが市場原理により低下することに歯止めがかかるか、鈍化し、結果、通信分野の発展が想定よりも遅くなる可能性がある。来年から民営化される予定の MPT については、民間通信事業者との健全な競争原理が成り立つことに配慮するのが「ミ」国国民の利益につながる。

そのため、無償資金による協力は、将来的に MPT の、MPT 以外の民間通信事業者に対する競争優位をもたらすことがないよう、供与される機材の使用用途及び効用を厳密に確認し、また他の事業者が間接的に受益者となり、結果、国民の利益につながるものにしていくべきであると考えられる。例えば、国際通信のゲートウェイに対する DDoS 対策に関しては政府への支援強化が望まれる

(3) 無償資金事業の実施機関

MCIT 内の組織改革により、無償事業が実施される場合は、IT&CS の National Cyber Security Center（NCSC）が実施機関の担当部署になるとのことである。NCSC には現在 5 人の職員しかおらず、維持運営管理が適切に行えるとは考え難い。体制が整ったことを確認することが無償案件を実施する上で必須となる。

7.4.3 今後の対応

サイバー攻撃に対処するための検知装置は、基本的に整備する必要があることに疑いの余地はない。最低限必要な機材・アプリケーションを当面投入し、将来的にはミャンマー（職員）の技術スキルに合致した検知機材・アプリケーションを整備することが望まれる。

そのため、第 7.2.2 項に別途提案した技術協力プロジェクトの供与機材として、緊急に必要最小限の基本的な検知機材・アプリケーションを含めておき、無償事業で残りの必要な機材の整備を行うことが合理的であると考えられる。ただし、無償資金協力は事業効果指標を考慮し、電子政府支援の一部の機材として扱うなどの対処も検討に値する。

無償資金協力事業として、妥当性を検討する上で、検討課題は下記のとおりである。

① 協力内容と範囲の見直し

GSOC 案件ではなく、電子政府促進の支援案件と捉える。電子政府は、地域の社会経済活動上の利便性を向上させ、地域開発に結び付くものと考えられる。「国民の生活向上のための支援」は日本政府の支援重点分野と合致する。

② 世銀支援との重複確認

世銀が S-12 ビルの設置の電子政府用データセンターの機材調達を支援している。調達予定機材の中には、サイバー攻撃の検知機能が付加されている機材もあり、無償資金協力事業を具体化する段階では支援の重複を十分に検討する必要がある。

③ 技術協力プロジェクトとの連携と実施時期

インシデントのインベントリ作成などを技術協力プロジェクトの活動の中に入れることで、効果的な協力内容を検討できる。技術協力プロジェクトでの機材供与を行う中で、無償資金協力の実施時期を延ばし、適切な内容の無償資金協力の検討が可能となる。一方、サイバー攻撃の脅威を鑑みれば、技術協力プロジェクトにより制度・体制整備、人材育成などを緊急に進めつつ、無償資金協力による機材供与が時宜を得たものとなるよう留意すべきである。

なお、要請書の見直しの要否については、MCIT 大臣の裁量によるところが大きい。また、政府事業内容は、Planning Committee（国家計画・経済開発省所轄）で決定される。その後、財務省所轄の Financial Committee で予算の確認をする。事業内容の査定は Planning Committee で行われる。援助要請は Foreign Aid Management of Committee を窓口にしている。事業スコープが変わる場合、これらの Committee への説明を大臣ができると考えるならば、要請書の見直し再提出は不要と考えられるが、再度 Committee へ変更内容で承認を得たいと大臣が考えた場合、再提出が必要となる。ただし、技術協力プロジェクトの実施状況を観察した後に検討する場合、要請接頭後から数年経つことになり、要請書の取り扱いについて、慎重に検討する必要があると考えられる。

第8章　提言及び今後の課題

政府システムにおけるインシデントの検知・解析能力の強化策の一つとして、定期的なトレーニングを効果的に実施するためのトレーニングセンターの建設を表 7.2-1 の対策案 20 として記載している。これは、インシデントを疑似的に発生させ、必要な技術力を養うもので、短期的な周期で様々な種類のサイバー攻撃が発生している現状を鑑みた場合、「ミ」国独自に持続的に対応するための有効な手段であると考えられる。

対策案としても NCDP の 7 つの戦略である人材育成と、同じく人材育成に重きを置いている我が国の支援の方向性に合致している。一方、「ミ」国にはトレーニングセンターを建設する技術的ノウハウが不十分で、建設費用の捻出も困難である。また我が国においても同様の設備の成功例があり、活用可能な技術がある。

さらに、ネピドーに遷都後、民間企業は未だヤンゴンをベースに事業を行っている。IT 及びサイバーセキュリティに関する企業の所在はすべてヤンゴンであり、各省庁のサーバ等の保守管理やネットワーク構築等のアウトソーシング業務は、すべてヤンゴンからの出張ベースで民間企業が業務にあたっている。特にサーバの保守契約は緊急対応の取り扱いが出張ベースとだと困難であり、ネピドー周辺での起業などが望まれる。そのため、人材育成を大きな視野でとらえ、下記のような「ミ」国の産業振興策（案）と連携して行うことにより、IT 分野の発展が見込めるのではないかと考えられる。

現在「ミ」国の産業は、ヤンゴンの一極集中である。産業を分散し、周辺地方都市に経済効果が生まれるよう働きかけるため、第 2 の ICT パークをネピドーに建設し、通信事業者、アプリケーションの開発、システム構築等の ICT 関連企業の誘致を行い、パーク内に人材育成の拠点を設ける。その一部として、我が国がノウハウを有するサイバーセキュリティ・トレーニングセンターを無償資金事業で実施することも検討に値する。

スマートフォンを中心とした「ミ」国内の ICT 利用は、通信網の整備の進展を上回る勢いで、急速に高まっている。IT 関連の人材育成は急務であるが、コンピュータサイエンス分野に関する就職機会が少なく、また大学においても同分野の専攻はそれほど人気が高くない。また、上述のように各省庁の局舎があるネピドーには ICT 関連企業が無く、基本的にヤンゴンの企業と各省庁は必要な場合、サービス等の契約を結んでいる。ヤンゴンとネピドーといった地理的な距離により、非効率な業務管理が生まれていることは否めない。これらの要因を改善するためには、単純なサイバーセキュリティ対策案の検討だけではなく、産業振興策などとの連携によって、技術者の地位向上や就職機会の確保が最重要課題であり、かつ民間の拠点の分散化も必要であると考えられる。

分野横断的な課題解決により、効果的な経済発展の検討が行わることを期待するとともに、我が国の無償資金協力事業が、その一助となることを願うものである。

なお、当該無償資金協力が行われる場合、無償資金協力で供与された機材の取り扱いや、高度な検知・対応能力を養う技術移転を目的とした技術協力プロジェクト(第 7.2.2.項で述べた技術協力プロジェクトの第 2 フェーズを想定)を実施することで、無償資金協力事業との相乗効果が期待できる。

添付資料１　　関係者（面談者）リスト

1. 関係者（面会者）リスト

所属及び氏名	職位
在ミャンマー日本国大使館	
松尾秀明	参事官
山本和弘	二等書記官
JICA ミャンマー事務所	
紀古鮎美	所員
通信・情報技術省	
Thaung Tin	Deputy Minister
Sai Saw Lin Tun	Deputy Director General
国家サイバーセキュリティ運営委員会	
Ye Naing Moe	Director
ミャンマー郵電公社	
Mo Swe	Chef Engineer
mmCERT	
Mie Mie Su Thwin	Associate Professor
Kam Khan Sang	Staff
建設省	
Kyi Hlaing Win	Director
Yan Naung	Deputy Director
Ye Sis Min	Assistant Director
Nay Win Aung	Assistant Director
教育省	
Khine Mye	Director General
Zaw Myint	Director General
Li Theim nlainy	Director
Daw Than Than Htay	Deputy Director
Li Khin Mawng Kyaw	Asistant Director
Li Saw Hyunt Khime	Staff Officer
保健省	
Aye Aye Sein	Deputy Director General
産業省	
Aung Moe	Deputy Director
科学技術省	
Me Me Cho hfway	Deputy Director General
Nay Min Tun	Deputy Director
Ei Ei Khin	Deputiy Director

所属及び氏名	職位
Daw Khin Cho Lusin	Assistant Director
Kyaw thet Khaing	Assistant Director
商工省	
Minn Minn	Deputy Director General
Myo Khing Win	Deputy Director
国家計画・経済発展省	
工藤つとむ	JICA 専門官
ヤンゴン工科大学	
白川浩	チーフアドバイザー
濱田　勇	業務調整員
ミャンマー日本人材開発センター	
金丸守正	チーフアドバイザー
ネピドー開発委員会	
Zaw win	Director
ミャンマーコンピュータ連盟	
Than Than Tint	Vice President
Khun Oo	President
ミャンマーコンピュータ専門協会	
Min Oo	President
Ye Yint Win	President
情報・通信技術訓練研究所	
Mayachi Lai Lai Thein	Center Director
Nan Gi Khan	Assistant Professor
Aye Age Nyein	-
KOICA	
Nam, Kwon-Hyoung	Chief Resident Representative
Soe, Yungchae	Young Professional
Yatanarpon Teleport	
Thein Myint Khine	Department Head
Redlink	
Prasert Laosaengpha	Chief Technical Officer
Wai Lin Oo	Deputy Chief Engineer
Vision to Motion	
明石　栄超	-
Alpha	
Ye Myat	-

所属及び氏名	職位

現地調査終了時報告会出席者

裁判員連盟	
Ye Myo Oo	Staff Officer
農業灌漑省	
Nyi Nyi Lwin	Deputy Director
Tin Sein	Director
内務省	
Win Min Aung	Deputy Director
Thin Thin Swe	Staff Officer
商工省	
Tun Naing	Deputy Director
通信・情報技術省	
Ye Naing Moe	Director
Sai Saw Lin Tun	Deputy Director
建設省	
Zayar Lynn	Staff Officer
協同組合省	
Khine Thazin	Assistant Director
Theingi Hnin	Officer
防衛省	
Myat Min Oo	Head of Department
Nyein Chan	Head of Department
教育省	
Khin Maung Kyaw	Assistant Director
Saw Nyunt Khaing	Staff Officer
電力省	
Aye Myat Mon	Staff Officer
Tint Soe Win	-
エネルギー省	
Nay Zaw Htoo	Assistant Director
Yin Nyein Ei	Officer
Soe Mama Thu	Head of Branch
経済省	
Nay Lin Htet	Deputy Director
外務相	
Aung Kyaw Moe	Director/Assistant Secretary

所属及び氏名	職位
保健省	
Htay Aung	Director
Aye Aye Sein	Deputy Director General
内務省	
Tun Nay Win	Director
ホテル・観光省	
Kyaw Moe Naing	Staff Officer
移民・人口省	
Yin Yin Tin	-
Naing Phyo Kyaw	Staff Officer
産業省	
Myint Maung Maung	Assistant Director
Aye Myat Myat Thu	Leader
Aung Moe	Assistant Director
情報省	
Han Lynn Aung	Deputy Director
労働・雇用・社会福祉省	
Win Nyunt Oo	Deputy Director
国家計画・経済発展省	
Zaw Min Htay	Assistant Director
Han Myo Aung	Assistant Secretary (CIO)
鉄道省	
Daw Than Than Myint	Deputy Director
教務省	
Tin Min Hlaing	Assistant Director
San Tun Aung	Deputy Director
科学技術省	
Aye Nwe Thaing	Staff Officer
Kyaw Thet Khaing	Assistant Director
社会福祉省	
Mi Mi Thwe	Deputy Director
Daw Thet Thet Aung	ー
運輸省	
Min Min Htun	Assistant Director
Win Ko Ko	Staff Officer
ミャンマー鉄道	
Myint Thu	Manager

所属及び氏名	職位
ネピドー開発評議会	
Minn Mon Zaw	Staff Officer
Hla Myint	Deputy Director
最高裁判官連盟	
Ko Ko Lwin	Deputy Director
Kyi Win	Assistant Director
弁護士連盟	
Phyo Phyo Khin	Assistant Director
Nay New Thant	Staff Officer
国家公務員委員会	
Aye Aye Thwin	Director
Myint Swe	Director
選挙管理委員会	
Tun Naing Oo	Deputy Director
Myat Htun Oo	Deputy Director

添付資料２　　調査議事録

2. 調査議事録

KDDI Summit Global Myanmar Company Limited(KSGM)打合せ議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 3 日（月）　13:00～14:00
開催場所	KDDI Summit Global Myanmar Company Limited 打合せ室
出席者 （敬称略）	KDDI Summit Global Myanmar Company Limited (KSGM) 松村　祥一郎　ミャンマー通信事業プロジェクト部技術管理チーム長 多田　昌宏　　グローバル事業本部グローバルコンシューマビジネス副本部長 青山　忍　　ジェネラルマネージャー 南雲　光文　　マネージャー 間々田　航太　部長 JICA 舘山　丈太郎　課長補佐 コンサルタント 佐藤　明男　業務主任/サイバー戦略 村野　正泰　セキュリティ対策計画 1/脆弱性診断 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ 現地の日系法人である KSGM に対してヒアリングを行った。ヒアリングの目的は、日本企業が独自に提供できるソリューションや機材の確認および政府に代わり民間企業が事業を実施できる領域を探ることである。 内容： 1.　調査の実施方法について （KSGM）調査はどのように行うのか。 （調査団）MCIT を中心に、関係省庁、関係機関、民間通信事業者などからヒアリングを行い、サイバーセキュリティに関する現状やニーズ、問題点を明らかにしていく。また、文書管理システムや政府機関の WEB サイトに対して脆弱性診断を行う。

2. MPT の組織体制について

（KSGM）MPT とは 2014 年の 9 月からジョイント・オペレーションを開始した。技術分野の職員は約 3,000 人程度であり、チーフエンジニアをトップとして、約 40 程度のランクに分かれている。管理職は 250 人程度である。この中で IT 関係の知識を有しているのはごく一部である。また、オフィサー以上の役職の人間に限り PC が与えられている。

3. MPT の現状認識について

（KSGM）NEC や中国系企業のベンダーに ICT システムを任せているため、ノウハウが蓄積されていない。また、技術者のスキルは低い。モバイルに関する事業は、比較的最近行われてきたことや、短期工事のため、ベンダーから図面などを入手することが可能だが、固定系通信事業など、短期で工事が終わらないものについては、最終的な図面等が残っておらず、それぞれの担当者の手帳の中や頭の中に存在している状態である。担当者の異動や退職などにより、誰も把握できていない状況に陥っている。ジョイント・オペレーション以前に、ミャンマーには光ファイバーが 21 本敷設されていたが､それぞれどのルートを走っているかわからないため利用できずにいる。また、NTT コミュニケーションズが導入した SAMRAI も、扱える人材が異動したため十分に機能していない。

メールサーバには最低限のセキュリティがかけられている。しかし、使い手側である MPT のセキュリティに対する意識が甘いため、有効に機能していない。

（調査団）MPT 職員に対する育成についてどのように考えているか。

（KSGM）MPT 職員に関しては教育プログラムを今後 3 年くらいかけて実施していく予定である。ただし、競争が激しい分野については、MPT 職員の成長を待ってはいられないため、KSGM が独自に事業を実施する。

4. サイバーセキュリティの裨益効果について

（調査団）MPT のセキュリティが保たれると、国全体に裨益効果はあるか。

（KSGM）固定網の管理は MPT が行っているため裨益効果はあると考えられる。ただし、法改正により民間企業もライセンスを取得できるようになったため、競争性の確保に問題がある。

	（調査団）MPT がサイバーセキュリティなどのサービスを実施するようになるか。 （KSGM）将来的には可能性がある。ITCS を設立したのはサイバーセキュリティが重要であるとミャンマー政府が認識しているからだと考えられる。また、公社化も行っている。 5. 技術規制について （調査団）サイバーセキュリティに関する技術的な規制等は存在しているか。 （KSGM）軍により通信傍受が強制されている。もともとは音声データだけだったが、最近はパケット、メールも監視しているようだ。また、最近できた法律により、各オペレータは政府のデータセンターに接続しなければならない。 6. 重要インフラの定義について （調査団）重要インフラの定義については、トップダウンで進めるのか、もしくはボトムアップで進めるのか、どちらがミャンマーに適していると考えるか。 （KSGM）トップダウンがよい。大統領府が音頭を取って進めるのが理想的だ。ただし、関係省庁が多くなると、大統領府にアサインされた大臣がかなり大きなイニシアティブを持って進める必要がある。 7. ITCS について （KSGM）ITCS のネットワークセンターが 2015 年 7 月に誕生した。既存のシステムの監視、制御、セキュリティ構築を行っている。ITCS のような、国の然るべき機関が音頭をとってサイバーセキュリティを進めるべきである。現状では人材が少ないため、キャパシティビルディングを早急に実施していく必要がある。ただし、ITCS 独力では困難であると感じているため、日本国として支援していく必要がある。 8. 今後のサイバーセキュリティについて 現在は紙ベースで機密情報等を管理しているが、電子政府の実施によりデータ化

	することでサイバーセキュリティが必要になる。現状では守るべきものがなく、また重要インフラも指定されていない。電力やガスが最重要だが、省庁間が縦割りで、関連する省庁を増やしていくと収拾がつかなくなる可能性がある。相当な先導力が必要となるため、MCIT が他省庁をまとめることは困難であると考えている。大統領府が音頭をとって進めることが理想である。 9. MPT の資産について （調査団）MPT の人材と資金力は十分あるのか。 （KSGM）政府内に人材が不足している。MPT は 97 年以降、新入社員を採用していない。コンピュータサイエンス大学等の卒業生はミャンマーに進出した企業に就職しているようだが、ミャンマー進出企業間のジョブホッピングが若者達に広まってきており、流動的である。MPT の予算については今年度まではあるが、来年度以降はない。 10. その他 ・MPT とのジョイント・オペレーションは 2014 年から 10 年間の契約である。 ・携帯加入者のデータベース化は今から行われる。現状では、顧客の情報と電話番号が紐付けされていない。
添付書類	なし
収集資料	なし

mmCERT ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 3 日（月）　11:00～12:00
開催場所	mmCERT オフィス
出　席　者 （敬称略）	mmCERT Mie Mie Su Thwin　Associate Professor Kam Khan Sang JICA 舘山　丈太郎　課長補佐 コンサルタント 佐藤　明男　業務主任/サイバー戦略 村野　正泰　セキュリティ対策計画 1/脆弱性診断 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ インセプション・レポートの協議および情報収集を行った。 内容： 1.　mmCERT の活動について mmCERT の活動目標は、サイバーセキュリティに関する技術的な支援と法律の施行である。将来的には、市民啓発活動やインシデントの解析を行う計画がある。現在は、アジア各国から指導者を呼び、サイバーセキュリティに関する講習を行っており、対象は、コンピュータ科学大学の学生、企業など様々である。また、周知・啓発活動として、レクチャー、パンフレットの配布、パスワードの設定ガイドライン等を作成している。 ただし、人材・資金不足しているため十分に活動できていない。 2.　他組織との連携について 他の組織との連携は重要と考えている。IMPACT とは現在も連携しており、カンファレンス等に参加している。また、APCERT にはサイバーセキュリティに係る

	データ等を送付している。このデータはAPCERTのメンバー内でのみシェアされている。 3. サイバー攻撃の統計について サイバー攻撃に関する統計データはMCITが所有しており、mmCERTでは保管していない。ただし、最近オンラインバンキングが急増していることもあり、フィッシング詐欺が増加している。 4. mmCERTの予算について mmCERTの予算はMCITからおりている。給料の支払い、機材購入、トレーニング費用等に使用している。予算額については把握していない。専門職のスタッフは7人のみである。プログラムやネットワークの知識を有している。 5. 組織改革について 組織改革の目的は、サイバーセキュリティに関連する機能を集約することである。例えば、人材育成、インシデントのハンドリング等である。
添付書類	なし
収集資料	なし

NEC インタビュー議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 3 日（月）　16:00～17:00
開催場所	NEC ヤンゴン事務所
出　席　者 （敬称略）	NEC 寺西　康　　ヤンゴン事務所所長 新井　亮太 JICA 本部 舘山　丈太郎　主任調査役 コンサルタント 佐藤　明男　　業務主任/サイバー戦略 村野　正康　　セキュリティ対策計画 1/脆弱性診断 南部　尚昭　　人材育成計画/協力支援内容検討 池田　好孝　　ICT システム 宮本　健吾　　データセンター評価 藤原　慧矢　　業務調整
協議内容	＜概　要＞ NEC のサイバーセキュリティに関するこれまでの取り組みと、本調査に対する今後の協力体制について意見交換を行った。 1.　NEC の取り組み ミャンマー国（以下「ミ」国）IT 環境の普及に伴いサイバー攻撃の脅威にさらされることは不可避であり、その攻撃は高度化する傾向にある中で、現在「ミ」国は無防備の状態である。当社は「ミ」国は早期の対策を必要とする認識で、SOC、国家ポリシー、組織化が重要であると考え MCIT に対して啓蒙活動を行ってきた。その結果として MCIT から日本への要請書提出に至っている。 また、ASEAN セキュリティ会議の後に大臣と面談を行い、ワークショップの要請を受けるなど「ミ」国側からのアプローチもあった。要請を請けて 2014 年 2 月にワークショップを開催し 100 名の政府関係者に参加頂いた。5 月には MCIT の大臣が来日し、総務省からの依頼を受けて当社の SOC を見学いただいた実績を有する。 2.　討議

	調査団:「ミ」国はサイバーセキュリティに関する課題が山積しており優先度が見極められない状況の中にありながらも自発性に欠けるよう見受けられる。そこで、一度これまでの経緯を思考から外して、被害が何であるか、何を守るべきかなど具体的に自発的に考えることが重要ではないかと考えるが意見を頂きたい。 NEC：セキュリティポリシーが必要であろうと考えるが、その前に教育に問題があるため、現段階ではセキュリティポリシーを作成する段階に達していないと思う。 調査団：サイバーセキュリティが「ミ」国の開発課題に対してどのように貢献するのか、技プロで技術水準の標準化を進めることで日本技術の導入環境が整備されると考えるが如何であろうか。 NEC：教育をパッケージとして提供するプログラムがある。GSOC 官民連携という手法をあるだろう。これらは提案手法の話でもあるため当社でも検討させて頂きたい。 3. その他 1) mmCERT の監視対象はヤンゴンの MPT が有するデータセンターを対象としており、政府系のデータは対象外としている。 2) IT&サイバーセキュリティ局に所属している Ye Naing Moe 氏が現状を最も理解している人物である。さらに Deputy Chief Engineer の女性 2 名が詳細を理解している。 3) 選挙の際、DDoS 攻撃が検知されたが、その意図は不明で中国からの攻撃であったことだけが分かっている。また通信無償で NEC が納入した機材に対して攻撃があった報告はない。
添付書類	なし
収集資料	なし

在ミャンマー日本国大使館表敬議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 3 日（月）　9:00～10:00
開催場所	在ミャンマー日本大使館
出　席　者 （敬称略）	在ミャンマー日本国大使館 松尾　秀明　参事官 山本　和弘　二等書記官 JICA 舘山　丈太郎　課長補佐 紀古　鮎美　　ミャンマー事務所　所員 コンサルタント 佐藤　明男　業務主任/サイバー戦略 村野　正泰　セキュリティ対策計画 1/脆弱性診断 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ ミャンマー国入りの報告と今後の調査に対するコメントを受けるため、在ミャンマー日本国大使館を表敬した。 内容： 1.　ミャンマーの現状 （山本　二等書記官）ミャンマーの技術者はレベルが低く、ケーブルの敷設やシステムの構築等、大部分をベンダーに任せているため、自身ではほとんどできない。 （松尾　参事官）各省はドメインを保持しておらず、主に Gmail を利用している。このため、サイバー攻撃を受けた場合においても省自体には影響がほとんどない。しかし、現在行っている書類のデータ化は機密情報の流出可能性がある。紙ベースでの書類処理は多大な時間と労力を要していたが、セキュリティの面では安全ともいえる。一方で、書類のデータ化は機密情報の流出可能性がある。ＰＣは便利である一方で、サイバー攻撃の危険性があることを彼らが十分に認識する必要がある。

	2. 調査の方針に対するコメント （松尾　参事官）他ドナーと重複した支援を行うことは避けたい。また、これまで行われてきた他ドナーの支援を見ると、それぞれが点で支援を行ってきているため、うまくつなぎ合わせて面の支援を考えてほしい。また、ミャンマーでサイバーセキュリティの支援を行う必要性について、本調査でのヒアリングから明らかにしてほしい。 3. 軍関係者の関与について （調査団）軍関係者が本調査に関与する可能性はあるか。 （山本　二等書記官）要請の段階では国防省の関与はない。国防省は独自の通信帯をもっているため、今後もないことが予想される。MPT のトップはもともと軍のトップであった。しかし、去年の 3 月以降空席であり、現在はジェネラルマネージャーが兼任しており、この人物は MPT のたたき上げである。 4. MPT の公社化について （調査団）MPT の公社化はどのような状況か。 （松尾　参事官）MPT の公社化については、世界銀行の支援のもと行われているが、まだ進んでいないという認識である。 5. 予算の執行能力について （調査団）ミャンマーの予算の執行能力はどうか。 （松尾　参事官）財務省に必要性をアピールできれば予算を確保することができる。予算枠に対して厳格に執行している。 以上
添付書類	なし
収集資料	なし

IT サイバーセキュリティ局 (ITCS) ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 4 日（火）　11:00～12:00
開催場所	MPT オフィス (S12 ビル)
出　席　者 （敬称略）	NCSC Ye Naing Moe: Director JICA 舘山　丈太郎　課長補佐 コンサルタント 佐藤　明男　業務主任/サイバー戦略 村野　正泰　セキュリティ対策計画 1/脆弱性診断 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ インセプション・レポートの協議および情報収集を行った。 内容： 1.　組織構成について ・2015 年 4 月の組織改編により、MCIT (Ministry of Communication and Information Technology)は主に MPT (Myanmar Posts and Telecommunications), PTD (Post and Telecommunications Department) 、および ITCS (IT Cyber Security Department, ITCS) 等の部門で構成されている。 ・ITCS は NCSC (National Cyber Security Center)や e-Government 局を含む合計 6 つの組織で構成されている。 ・ITCS には現在の 60 名程度の職員が在籍しているが、そのうち約 50 名が e-Government 局に所属している。NCSC の職員は 5 名であるが、MCIT に所属の職員は Ye Naing Moe 氏ただ 1 人である。e-Government 局に人員が集中しているが、

	今後、何人かの職員は異動される予定である。 ・今後の計画として 300 人程度まで ITCS のスタッフを増員する予定である。また、mmCERT についても今後 35 人まで増員させる計画がある。mmCERT については現在職員はヤンゴンにしかいない。 2. 組織活動について 組織のミッションはサイバーセキュリティの研究開発、注意喚起、事前・事後対応等である。 3. IT 関連のマスタープランについて IT 関連のマスタープランについては、韓国の支援で作成された ICT マスタープラン、ADE の支援の下作成中である e-governance マスタープランがある。また、JICA 専門家が作成を支援したサイバーセキュリティのアクションプランについては承認のプロセスの最中である。 4. ステアリングコミッティについて サイバーセキュリティやサイバー犯罪に関する意思決定や利害調整を行う委員会として MCIT の大臣を議長とするステアリングコミッティがある。2 ヶ月に 1 回程度会議を開いており、政府関係者、民間関係者含め 16 人が所属している。アドミ業務を行う事務局は存在しない。分科会はサイバーセキュリティ、サイバー犯罪を含め合計 6 種類が存在している。重要インフラの特定については、このステアリングコミッティ内で進めることが望ましいと Ye Naing Moe 氏は考えている。
添付書類	なし
収集資料	なし

MOE (Ministry of Education) ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 5 日（水）　15:30～16:30
開催場所	内オフィス
出　席　者 （敬称略）	MOE Khine Mye : director general Zaw Myint : director general Daw Than Than Htay : deputy director Li Thein Naing : director JICA 舘山　丈太郎　課長補佐 コンサルタント 佐藤　明男　業務主任/サイバー戦略 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム
協議内容	＜概　要＞ サイバーセキュリティに関する人材育成や現在の取組み、IT 利用の実情を調査するために、MOE (Ministry of Education) にヒアリングを行った。 内容： 1.　サイバー攻撃について ・14 か月前に MOE の WEB サイトがサイバー攻撃を受け、数日間サーバがダウンしている。また 2015 年 6 月に大学入試試験の結果のデータベースが不正アクセスを受け、データの改ざんなどが判明した。MOE のメールサーバへのハッキングなども確認されている。このようなサイバー攻撃に対して、エスカレーションなどのプロセスや規則は存在せず、他の省庁などにも報告していないのが現状である。 ・現在では、重要なデータについてはインターネットから隔離したコンピュータに格納している。 2.　Chief Information Officer (CIO), CSO (Chief Security Officer) について

	・以前、CIO と CSO をすべての省内に配置するという通達が政府から出され、CIO と CSO を配置した。ただし、全省庁が CIO と CSO を今でも配置しているかどうか不明である。 3. MOE の IT 関連教育への取組について ・サイバーセキュリティに特化したコースは存在しないが、ICT に関連した講義として、電子政府システム、スマート ID の二つのコースがあり、これらは MCIT から提供されたものである。 ・ICT に関する授業やコースの拡充を図りたいが、地方については未だ無電化地域も多く、ICT に関連した授業を行うことができないのが現状である。また、予算の関係もあり、ICT への取り組みは遅れている。 ・コンピュータサイエンス専攻や講義はミャンマー国では人気が低い。理由は、ミヤンマー国内で同分野に関する仕事が少ないからである。現在は、医療系や工学系の人気が高い。
添付書類	なし
収集資料	なし

MOST (Ministry of Science and Technology) ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 5 日（水）　14:00～15:00
開催場所	MOST 内オフィス
出席者 （敬称略）	MOST Me Me Cho Htway : deputy director general Nay Min Tun : deputy director (ICT section) Ei Ei Khin : deputy director (ICT section) 他 2 名 JICA 舘山　丈太郎　課長補佐 コンサルタント 佐藤　明男　業務主任/サイバー戦略 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム
協議内容	＜概　要＞ サイバーセキュリティの実情を調査するため、MOST (Ministry of Science and Technology) にヒアリングを行った。 内容： 1.　MOST における IT 利用について ・省庁の WEB サイトでは MOST の基本的な情報のみ載せており、Web サイトからのオンラインサービスなどを行ってはいない。これまでサイバー攻撃を受けたことはない。 ・現在、MOST 職員の人事データベースシステムを構築している。このシステムは、MOST 自身で構築しており MCIT や MPT から協力は受けていない。MOST の職員のみ閲覧できるシステムである。 ・Director 以上が PC を保持している。スマートフォンなどのデバイスも考慮すると、約 500 程度の端末が MOST のネットワークにつながっている。

	2. MOST と他省庁の連携について ・以前はミャンマーに 24 校あるすべての大学が Ministry of Education (MOE) の傘下であった。現在はコンピュータサイエンス系の大学は MOST の傘下となっている。 ・MOST と MCIT が共同で IT に関する教育コースを提供している。サイバーセキュリティについても同コースに含まれている。省内のエンジニアに対してのトレーニングにも利用されている。 ・プログラミングなど IT の基礎知識を学ぶ 10 週間のコース最近実施しており、12～13 の省庁から職員が参加している。 3. その他 ・IT やサイバーセキュリティの研究者は MCIT ではなく、大学に所属している。
添付書類	なし
収集資料	なし

Minutes of Meeting 協議議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 6 日（木）　13:00～14:00
開催場所	MCIT オフィス (S12 ビル)
出　席　者 （敬称略）	MCIT (Ministry of Communications and Information Technology) IT&CS (Information Technology and Cyber Security) Department Sai Saw Lin Tun　Deputy Director General Ye Naing Moe　Director JICA 舘山　丈太郎　課長補佐 コンサルタント 佐藤　明男　業務主任/サイバー戦略 村野　正泰　セキュリティ対策計画 1/脆弱性診断 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ M/M (Minutes of Meeting) の内容について Sai Saw Lin Tun 氏に確認して頂き、署名を行った。署名後、今後の調査の進め方について意見交換を行った。以下に意見交換の詳細を示す。 1.　面談依頼について ・サイバーセキュリティに関連する省庁の面談については、IT&CS からアポイントメントの依頼を行う。 ・Ooredoo や Telenor など通信事業者に対するアポイントメントは PTD (Post and Telecommunication Department) との面談の際に担当者に依頼する。 2.　その他 ・来年度の IT&CS の予算はまだ確定していない。スタッフにいては、60 人増員を計画しているが、来年度は 30 人程度しか確保できない見通しである。

添 付 書 類	なし
収 集 資 料	なし

ミャンマーコンピュータ連盟インタビュー議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 7 日（金）　11:00～12:00
開催場所	ミャンマーコンピュータ連盟　事務所 (MCIT Park 内)
出　席　者 （敬称略）	MCF (Myanmar Computer Federation): Than Than Tint　Vice President Khun Oo　President MPCA(Myanmar Computer Professionals Association): Min Oo　President Ye Yint Win　President コンサルタント 佐藤　明男　業務主任/サイバー戦略 宮本　健吾　データセンター評価
協議内容	＜概　要＞ MCF の活動、サイバーセキュリティに関する話題提供、本調査に対する今後の協力体制について意見交換を行った。 1. MCF と MCPA の組織体系について MCF は複数の下部組織を有する統括組織であり、MCPA はヤンゴン地域の教育提供を主とする組織である。MCF は民間企業 30,000 社の登録を有し、これら連携しながら IT 水準向上を目指す団体である。 2. MCF の活動について MCF では、年に一回各地域でセキュリティに関するセミナーを開催している。また、IT に関する教育で高校の講師に対して教育を施すとともに、学生に対する直接授業も提供している。政府からの要請で昨年 3 ヶ月間セミナーを実施し、さらに要請を請けて証書発行の付くアドバンストレーニングを行った。 3. 討議 調査団 : 当方より Questionnaire を送付するため、8/14 までに回答頂きたい。また、連盟加入企業の中でサイバー攻撃を受けた経験のある企業へのヒアリングを実施したい。調査団がヤンゴンを再訪する 8/12 に可能な企業と調整をお願いしたい。 MCF : 後ほどメールを確認のうえ返答する。 MCF : ODA の対象として当連盟のような民間団体は対象となるであろうか、また、ODA の実施まではどの程度時間を有するであろうか。 調査団 : ODA の対象として「ミ」国の合意や形態によっては協力の可能性はある。実施開始については協力内容による。本調査はそのための基礎調査である。 調査団 :「ミ」国のサイバーセキュリティに関する情報を収集している機関や団体

	などをご存知ないだろうか。 MCF：スマートフォンの普及に伴い、e コマースなどでのリスクが高まっていると認識しているものの、サイバーセキュリティへの認識が非常に低く、情報収集する機関は存在していない現状にある。 調査団：サイバーセキュリティはプロフェッショナルにより実現されるものではない。現状は各組織の能力に即した設計に基づきセキュリティ対策を行っているが、非経済になる場合が多い。設計段階から適切な水準を確保する上でも認知向上が重要である。 MCF：サイバーセキュリティもやはり経験から学ぶことであろうと考える。民間企業に経験から学んでいる企業もある。
添付書類	なし
収集資料	なし

MOC (Ministry of Construction) ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 7 日（金）　10:00～11:30
開催場所	MOC 内オフィス
出席者 （敬称略）	MOC Kyi Hlaing Win　Director Yan Naung　Deputy Director (CIO) Ye Sis Min　Assistant Director Nay Win Aung　Assistant Director コンサルタント 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 藤原　慧矢　業務調整
協議内容	＜概　要＞ サイバーセキュリティの実情を調査するため、MOC (Ministry of Construction)にヒアリングを行った。 内容： 1.　ICT の利用について 電子政府のアプリケーション、WEB サイトの運用をしている。今後はオンラインサービスの提供を考えており、現在構築中である。また、GSI による道路、建物、橋の工事・開発および土地管理のデータベース化や、インテリジェンス・トランスポーテーション・システムの開発を行っている。土地計画や道路の拡張計画等のデータ化の予定もある。 2.　データの利用、管理状況について ・紙ベースの情報は電子文書管理システムに移行中である。予算、将来計画、機密情報等の重要な情報はオフラインのサーバに保管している。さらに、重要なファイルについては、アクセス権限を持たせる、重要度に応じて複数のパスワードを設定する、コピー機の利用者を制限することで機密文書の流出を防いでいる。ウィルス対策については、アンチウィルスソフトのインストールの実施等を行って管理している。ただし、アンチウィルスソフトはオンラインになっている重要な PC のみインストールされている。これは、予算が限られているためライセンス料の支払いが困難なためである。

3. メールの利用について

・MOC 用の政府のドメインを取得しているが、多くは Gmail 等を利用してメールの送受信をしている。政府のメールはメールボックスの容量が 2MB しかなく、アップロード、ダウンロードが遅く、ユーザーインターフェースが洗練されていない。メールサーバが長期間アップデートされていない。今後、MOC の予算で外国製サーバを購入し､データセンターに設置する予定がある｡予算は 15,000USD である。調達については、海外企業と提携しているミャンマー国内の企業に依頼している。MOC の職員は全国に 13,000 人程度いるため、役職の高いものから順にアカウントを割り当てていく。

4. IT 関連予算について

・IT 関連の予算全体の 1%程度しかなく、毎年確保されるわけではない。IT 関連予算の多くは､PC やソフトの購入に使用されるため､サイバーセキュリティに割り当てられる予算はさらに限られている。

5. イントラネットについて

・MPT のインフラを使って 14 の地方都市でイントラネットを構築している。それらの地域ではイントラネットを使用することが可能である。また、今後 3 年間ビデオ会議システム、レポートシステム、電子文書管理システムを構築する予定であり、予算は 250,000USD を見込んでいる。ただし、この金額に毎年のライセンス料、維持管理費用、アップグレードに要する費用は含んでいない。

・イントラネット構築に必要となる設備は MOC が提供しているが、回線使用料の支払いについては地方事務所が負担し、MPT に使用料を支払っている。

6. IT 担当者について

・省庁内にある 4 つの部門に計画情報通信オフィスが 4 月に開設された。業務としては計画業務をメインに行っており、IT に関する業務は少ない。4 部署に 20 人ずつ、大臣のオフィスに 30 人所属しており合計で 110 人在籍しているが、IT 専門担当者は各部門 4~5 人である。

	7. 人材育成について ・省内のコンピュータを使用できる人材 500 人程度に対し、トレーニングを実施している。研修会場は 2 か所存在する。また、民間企業のトレーニングセンターも活用している。 ・全国のエンジニア 4,000 人の中から選別して、コンピュータデザインやアーキテクチャデザインの教育を実施している。 ・IT エンジニアの教育は必要であるが、教育を行うための知識が不足しているため、日本の支援で補ってほしいと MOC は考えている。 8. サイバー攻撃について ・2009 年にバングラディッシュから攻撃を受けた。MOC だけでなく 18 省庁が被害にあっている。MOC の被害状況は、古い WEB サイトが攻撃を受けたことにより 2 日間サーバが停止した。他省庁では、データベースの消去、情報流出が発生したと聞いている。
添付書類	なし
収集資料	なし

MOI (Ministry of Industry) ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 7 日（金）　13:00～14:30
開催場所	MCIT 内打合せ室
出席者 （敬称略）	MOI U Aung Moe　Deputy Director コンサルタント 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 藤原　慧矢　業務調整
協議内容	＜概　要＞ サイバーセキュリティの実情を調査するため、MOI (Ministry of Industry)に対してヒアリングを行った。 内容： 1.　サイバーセキュリティの現状について ・以前はヤンゴンのデータセンターを使用していた。ソフトウェアのインストールやサーバの監理については民間のベンダーに委託している。セキュリティ対策はファイアウォールのみである。2007 年に省庁がヤンゴンからネピドーに移動したのをきっかけに、2010 年にネピドーにもデータセンターが設置された。このデータセンターのセキュリティ対策もファイアウォールのみである。 ・政府は ICT に対する姿勢は、人材育成よりもアプリケーションの充実化に重きを置いている。サイバーセキュリティに関しては、民間企業に頼らなければいけない現状がある。 ・情報の取り扱いを民間に任せるのは支障があると理解しているが、現状、省庁のセキュリティレベルは民間企業よりも低いレベルにあり、また、機密情報も少ないため民間に委託している。 2.　データセンターで扱っているデータについて ・入札情報、ライセンスの情報、トレーニングセンター入学志望者の個人情報を

	扱っている。なお、ライセンスとは製造許可である。各地のオンラインサービスセンターで登録に必要なデータを入力し、そのデータをもとに、ネピドーで審査を行いライセンス付与する。これにより、ライセンス登録のためにネピドーに来る必要がなくなった。また、登録されたデータは企業間交流の促進に利用している。 3. サイバー攻撃の有無について ・MOI に対するサイバー攻撃はこれまで確認されていない。 4. サイバーセキュリティに関する予算について ・予算については、アンチウィルスソフトなどを含む維持管理費とサーバやアプリケーション購入費用の二種類に分かれている。前者については毎年、約 25,000USD 程度である。後者については、必要性に応じて申請して購入を行っている。 5. IT 担当者について ・IT 担当者については 5 人である。 6. セキュリティ対策について ・省内にあるすべての PC にアンチウィルスソフトがインストールされている。また、定期的なアップデートも実施している。 7. メールの利用について ・省庁のドメインは取得しているが、職員全員に割り当てるだけのアカウント数がないため、職員の多くは Gmail を使っている。省庁のドメインが割り当てられるのは、役職が上位の職員だけである。省庁のドメインから Gmail へメールを送信すると、スパム扱いになる。しかし、知り合いからのメールは躊躇いなく開封する職員が多い。

	8. 人材育成について ・IT 関連教育については、MCIT が主導で行っており、MOI では行っていない。 9. サイバーセキュリティに関連した計画について ・サイバーセキュリティに関連した今後の計画として、データセンターのセキュリティ対策が充実するように働きかけていく。 10. インターネットの利用について ・インターネットへの接続は Wi-Fi と有線、両方使用している。インターネットへ接続する際にはパスワードが必要である。省内のＰＣはすべて、インターネットにつなげる環境にある。ＰＣは全部で 200 台程度あり、これは iPad 等のタブレット端末も含んでいる。
添付書類	なし
収集資料	なし

中央銀行プロジェクトインタビュー議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 7 日（金）　14:00～15:20
開催場所	中央銀行　事務所
出　席　者 （敬称略）	JICA Project for modernizing the Funds Payment and Securities Settlement System in Myanmar Central Bank of Myanmar 石塚　雅典　Chief Advisor コンサルタント 佐藤　明男　　業務主任/サイバー戦略 宮本　健吾　　データセンター評価
協議内容	＜概　要＞ 中央銀行プロジェクトの実施に際して、現在把握しているセキュリティに関する課題などについてヒアリングを行った。 1.　中央銀行について 石塚氏：現在のシステムはインターネットに接続したシステムではないため、セキュリティに対する懸念はないだろうが、普及啓発が先であろうと思われる。日本では金融業界特有のセキュリティ基準を定めているが、「ミ」国は業界に無い様子である。中央銀行に対するヒアリングにおいて重要資産に関する質問を行ったが、明確な返答が得られない状況である。これまでは全てが機密情報であったため機密にすべき情報が整理されていない。例えば、金融機関の名前や財務情報という質問を行ったが自身で把握できていないため答えられない状況であった。 調査団：CSO やＩＴ責任者など中央銀行ではどうなっているか。 石塚氏：AITD (Administration and IT department)が所管になるだろう。システムの防御の内部監査部門があるが、システムを監視する機能はない。ＩＴ関係で全体 40 人規模であろう。IT 知識を有している人材であり、運用担当者を含む人数である。 石塚氏：プロジェクトの構成は決済システムと会計システムに分かれる。決済システムはＮＴＴデータと富士通が担当し、会計システムは大和総研が担当している。本年中はプロジェクトが動いていると思われる。ＩＳＭＳを準拠したセキュリティガイドラインはプロジェクト内で作成しようとしており、大和総研が担当で進めている。ＣＶネットの運用は来年 1 月を予定し、会計システムは今年 12 月からを予定している。 調査団：ＢＣＰはどのように考えているか？

	石塚氏：プロジェクトスコープ外だが必要性は認識している。BCP の要請は外国銀行からくる場合が多い。 石塚氏：省庁間で問題認識があるならば情報共有からはじめるべきであろう。ミャンマーはレガシーコストゼロで最先端のシステムを導入する志向が高い。銀行マスタープランを作成したプロセスにミャンマーが関わった様子がない。 金融機関は信頼が最重要な機能である。信用の獲得は短時日で達成できるものではない。 調査団：現在の課題は何であろうか？ 石塚氏：中央銀行のあり方についてマインドセットの変更が必要であろう。マーケットありきの中央銀行であるが、マーケットが無い状況である。社会主義経済の発想からは市場有意の発想が少ない。また、政府から独立した中央銀が理想である。国債を断れるような銀行が必要である。 Ministry of finance と同格の組織で、職員は公務員。幹部クラスは人事院での一括採用という現状である。 調査団：NCSC に各省庁から出向を質問したことがあるが出向自体が稀であるとの回答であった。 石塚氏：我々も省庁間の配置転換を提言したことがあったが、受け入れられなかった。日本でも現場を動きながら経験から把握している。 調査団：本調査では出口戦略に苦慮している。 石塚氏：地ならしという認識で望むことで拓けるのはないだろうか。アポイントはＣＰから働きかけで動くことが良いであろう。この国の金融が発展するうえでサイバーセキュリティは重要な位置にあたる。安心して預金できる環境が整備され強化されることが大事である。 石塚氏：ASEAN の取り組みはあるか？ 調査団：日-ASEAN の取り組みがある。 石塚氏：将来的には金融も国境を越えて接続する動きがある。ある意味では ASEAN 標準や国債基準が必要だと思う。 ボンドマーケットをつなぐ動きがある。アジアのどこかが通貨建てで日本国債を発行できるようになるだろう。 調査団：CSIRT ,CERT は国際連携が進んでいる。APCERT の取り組みがあり、その中に mmCERT が入っている。
添付書類	なし
収集資料	なし

MOCO (Ministry of Commerce) ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 10 日（月）　10:00～11:30
開催場所	MOCO 内オフィス
出　席　者 （敬称略）	MOCO Minn Minn　　Deputy Director General Myo Khing Win　Deputy Director (Information Technology Division) コンサルタント 佐藤　明男　業務主任/サイバー戦略 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ サイバーセキュリティの実情を調査するため、MOCO (Ministry of Commerce) にヒアリングを行った。 内容： 1.　ICT 利用とセキュリティ対策について ・MOCO では輸入・輸出のライセンス許可、会社の登録等を行っている。この他に管理システムやアプリケーションシステム等、合計 13 のシステムの運用を行っている。 ・MOCO と 20 の地方オフィスにはイントラネットが構築されている。セキュリティ対策として、MOCO はファイアウォールがあり、MOCO と地方オフィスとの通信は VPN で行っている。ユーザーアカウントのログオン承認についてはドメインコントローラを使用している。 2.　サイバー攻撃の有無について これまでに 5 回程度サイバー攻撃を受けている。ヤンゴンの Hanthawady にあるデータセンターにサーバを設定しているため、距離の問題から MOCO での管理が難しく、ヤンゴンの地元業者とのサービス契約によりサーバの保守管理を行って

	いる。 3. オンラインでの支払いについて 会社の登記などのオンラインサービスを提供しているが、以前は Web サイトで登録を行い、その情報をプリントアウトし MOCO で支払うというサービスになっていた。しかし現在は、銀行と提携したため、登録から支払いまですべてオンラインで対応できている。 4. モバイルバンキングや ATM の利用について 現在のところモバイルバンキングや ATM の利用者は少ない。給料は現在、現金で支払われるが、今後は銀行振り込みになることが望ましいと MOCO は考えている。 5. MOCO 内の技術者について MOCO には約 1300 人のスタッフが在籍しており、ネピドーのオフィスには約 300 名程度が配置されている。ICT 部署には 13 人ほど所属しており、ジャーナルなどの出版に係る仕事を主に行っている。MCIT からの通達で CIO，CSO をそれぞれ配置することになっているが、MOCO 内には十分な技術力を持つエンジニアがいないため CSO を配置できていない。彼らが CIO と CSO を兼任している状態である。 6. 省庁間連携について MCIT 主催で各省庁の CIO や CSO が集まり意見交換を行う会議が年間 7～8 回開催されてきた。しかし、近年は集まることはなく、メールなどで情報共有している状態にとどまっている。今後は、各省庁だけでなく、スキルの面で政府より秀でている民間企業も巻き込みサイバーセキュリティについて考えていく必要があると MOCO は考えている。 7. 人材育成について 2005 年に MOCO のオフィスビル内にトレーニングルームを作り、20 台の PC を使用して小規模なソフトウェアのトレーニングを開催している。講師はソフトウ

	ェア関連会社から招いている。過去にはマレーシアから講師を招いたこともある。トレーニングは年 10 回程度行っており、受講者のレベルに合わせて複数のコースを用意している。この他、MCIT が用意するコースに職員を参加させる場合もある。 8. 予算について 予算は状況に応じて変わるが e-Government 関連予算については十分に配分されている。IT 関連の予算としては、約 100,000USD 程度である。 9. セキュリティマネジメントについて 5 年前からオンラインストレージを利用したデータシェアリングを行っており、毎週月曜にはデータを消去している。ネットワーク上に存在する様々な資源やその利用者の情報や権限などを一元管理するために Active Directory を利用している。 10. メールアカウントについて Gmail を使う理由は、以前の政府アカウントは容量が小さく、メールも遅く使いづらかったためである。ウィルスに感染した例もある。さらに、Gmail であればフィルターがかかっているが、政府のアカウントはフィルターがかけられていない。このような理由から、使い勝手の良い Gmail を使っている。
添付書類	なし
収集資料	なし

MOH (Ministry of Health)ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 10 日（月）　10:00～11:30
開催場所	MOH 内オフィス
出　席　者 （敬称略）	MOH Aye Aye Sein: Dy. Director General コンサルタント 佐藤　明男　業務主任/サイバー戦略 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ サイバーセキュリティの実情を調査するため、MOH (Ministry of Health) にヒアリングを行った。 内容： 1.　ICT システムについて 現在、電子オフィス化を進めている最中である。電子文書管理システムを利用しており、ヤンゴンのデータセンターに 2 つのサーバを設置している。様々な省庁が MOH の保持しているローデータにアクセスするため、セキュリティ保持は極めて重要だと感じている。保守運用については、地元の民間企業に委託しており、民間企業に任せることはデータ流出などの点で危険が高いと考えているが、省内のスタッフのスキルや知識を考慮すると、現在は民間企業に頼まざるを得ない状況である。 CIO が電子文章管理システムと Web サイトの監理を行っているが、CSO は配置していない。MPT が提供しているコロケーションサービスを利用して Web サービスを提供している 2.　セキュリティ対策について ウィルス対策ソフトとしてカスペルスキー社の製品を導入している。セキュリティ対策の重要性は理解しているが、知識やスキルを保持しているスタッフは皆無で、ガイドラインなどもない状況で、どのように進めていけばいいかわからない

	状況である。また、MOH は部署が多いため、すべての部署にセキュリティの知識があるスタッフを配置すべきだと MOH は考えている。 3. サイバーセキュリティに関する課題 ミャンマー政府の問題であるが、職員の配置換えが多く、トレーニングを行ってもすぐに移動してしまい知識や経験が蓄積されない。また、セミナーやトレーニングに参加しても、その後のフォローアップがないため定着しない。 また、仕事の割り振りにも問題があり、現状では適切な仕事の役割分担ができていない。自身の仕事に集中できるように環境を整える必要がある。
添付書類	なし
収集資料	なし

NDC(Nai Pyi Taw Development Committee)ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 11 日（火）　10:50～12:20
開催場所	MPT 内オフィス
出席者 （敬称略）	NDC Li Zaw Win　Director (CIO) コンサルタント 佐藤　明男　業務主任/サイバー戦略 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ サイバーセキュリティの実情を調査するため、NDC (Nai Pyi Taw Development Committee) ヒアリングを行った。 内容： 1.　NDC について ・組織構成は、議長を頂点に副議長、7 人の委員で構成されている。各委員の下にはそれぞれセクレタリーが配置されており、セクレタリーのまとめ役としてパーマネントセクレタリーが存在する。NDC の職員は全体で約 800 人おり、ネピドーのオフィス以外に、地方オフィスが 8 ヶ所ある。このうち PC を使用しているのは 76 人である。 ・NDC は準政府組織である。組織の活動としてはネピドーの道路、橋の開発を行っている。開発に係る費用は、中央政府からの予算割当てはないため、税収等により自身で調達している。ただし、大規模なインフラに関しては中央政府が支出する。NDC の WEB サーバはネピドーの Dakekina データセンターに設置されている。 2.　サイバー攻撃の有無について ・WEB サイトに対して、サイバー攻撃を受けたことがある。攻撃を受けるたびにバックアップを再送して回復している。しかし、その後に適切な対策が講じられ

	ないため、再度攻撃を受けている。 ・サイバーセキュリティに関するガイドラインやトレーニングがなく、サイバーセキュリティに関する知識が乏しいことため､対策を講じることができていない。また､NDC が設立されてからあまり時間が経過していないため、サイバーセキュリティ以外にも重要な仕事が多く、時間も人も予算を割くのが難しい。今後、オンラインサービスの提供、ICT システムを拡充する計画があるが、それに合わせて、セキュリティ対策を講じるよう検討している。 3. CSO について ・CIO が CSO を兼任している。しかし、現状では知識が不足しているため、CSO としてどのような活動をしていくべきか理解していない。また､CIO や CSO は地位が高く、仕事量も増加するため、希望者が少なく、人選が難しい。 ・現在の CIO である Li Zaw Win 氏は、プログラミングなどの知識はあり、自身でアプリケーションなどの開発を行っている。WEB サイトの構築・管理については、自身で行うことができないため外部委託している。IPS/IDS については知識がなく、必要性が認識できれば購入する。 4. 予算について ・サイバーセキュリティに関して特定財源はない。ICT 局は 1 年前に設立されたばかりで、予算についてはまだ検討していない。現在は、必要な活動費等を議長に要請し、承認を得ることで Central Fund から予算が割り当てられている。 ・サイバーセキュリティに関する予算実績は、80,000 ドルである。サーバ、ネットワーク構築機材、ファイアウォール、WEB サイトの管理委託費等に使用した。 5. NDC で管理するデータについて ・オンラインサービスは提供しておらず､NDC で管理しているデータのほとんどは職員のメールである。

	6. 政府ドメインについて ・NDC ドメインのメールアドレスはあるが、アカウントは一部にしか割り当てられていない。 7. その他 Nai Pyi Taw Development Committee は開発を担当し、組織名が類似する Nay Pyi Taw Development Council は管理を担当している。
添付書類	なし
収集資料	なし

データセンター（Dekkhina）ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 11 日（火）　14:00～15:00
開催場所	データセンター（Dekkhina）
出　席　者 （敬称略）	MPT Yay Kyi Aye Assistant Engineer (Information and technology Department) コンサルタント 佐藤　明男　業務主任/サイバー戦略 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ サイバーセキュリティの実情を調査するため、ヒアリングを行った。 内容： 1.　データセンター（Dekkhina）について 政府や民間に対してコロケーションサービスを提供している。サービスの価格はラックの使用幅を表すUで決定し、６Ｕで 120,000 チャット/月である。また、ラック 1 つをレンタルする場合は 600,000 チャット/月である。 MPT はサービスを提供するのみで、セキュリティ対策に関しては各自で行う必要がある。 2.　支援の可能性について （MPT）ＭＣＩＴ内の組織改編で MPT と ITCS に分かれ、それぞれ 2 か所のデータセンターを管理している。MPT のデータセンターでは、政府および民間のサーバを管理している。一方で ITCS のデータセンターでは政府のサーバのみ管理している。これは e-gov に関するサーバである。 （調査団）政府系のサーバは一か所にまとめた方がよい。トラブルに対処しやすい、設置コストを抑えられる等の理由から、ミャンマーの事情にあう。 日本の ODA に関しては例えば、e-gov の部分を支援し、MPT の管理部分はミャン

	マー自身でセキュリティ対策を講じる方法もある。 （MPT）その場合でも、MPT に対する技術的な支援はほしい。
添付書類	なし
収集資料	なし

MCIT (Ministry of Communication and Information Technology) 副大臣面談議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 12 日（木）　11:00～12:00
開催場所	MCIT 内オフィス
出席者 （敬称略）	MCIT H.E. U Thaung Tin: Deputy Minister Sai Saw Lin Tun: Deputy Director General Ye Naing Moe: Director JICA 稲田　恭輔　JICA ミャンマー事務所次長 コンサルタント 佐藤　明男　業務主任/サイバー戦略 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ MCIT(Ministry of Communication and Information Technology)の副大臣である H.E. U Thaung Tun 氏と面談を行い、本調査の今後の進め方について意見交換を行った。以下、副大臣との質疑応答の内容を示す。 内容： 1.　他のマスタープランと合致した支援 現在ミャンマー国には、e-Government マスタープラン、ICT マスタープラン(8 月末にリリース予定)が存在しているが、サイバーセキュリティの支援に関しては、これら 2 つのマスタープランの内容と合致した方向性で進めてほしいという要望が副大臣からあった。 2.　人材育成に関する要望 副大臣はサイバーセキュリティに関する支援について、サステナビリティを強く望んでおり、重要なポイントは能力育成と考えている。個別の能力強化のみならず、組織として総合的に能力強化される支援を望んでいる。

	3. 市場の急激な変化への対応 ICT 関連の市場は急激に成長しており、本調査の最終報告書が提出される予定である 12 月には現在の状況が激変していることを副大臣は危惧しており、プロジェクトの早期開始を望んでいる。長期的な未来ではなく、短期的な未来を考慮して支援を進めてほしいと副大臣からコメントを頂いた。 以上
添付書類	なし
収集資料	なし

NPED(Ministry of National Planning and Economic Development)ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 13 日（木）　15:50～17:00
開催場所	NPED 内オフィス
出席者 （敬称略）	NPED 工藤　つとむ　JICA 専門官 コンサルタント 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 藤原　慧矢　業務調整
協議内容	＜概　要＞ 国家開発計画におけるサイバーセキュリティの位置づけを調査するため、ヒアリングを行った。 内容： 1.　開発計画におけるサイバーセキュリティの位置づけについて 以前のミャンマーの重点開発分野は 10 分野であった。ICT に関連する項目として携帯電話等に関する項目が記載されていた。 現在では 7 分野に変更された。7 分野とは、電力、水、農業開発、雇用創出、観光、金融セプター、貿易の促進であり、ICT に関連する項目は明示されていない。ただし、7 分野と絡めた ICT の解釈は可能である。 また、ミャンマー産業発展ビジョンにおける重点項目は、インフラ開発、農業開発、電力、交通である。こちらにも通信は明示されていないが、同様に包括的な ICT の解釈は可能である。 第一次 5 か年計画は 2011 年～2015 年の計画として執行されている。しかし、非公開のため内容については不明である。現在、第二次 5 か年計画を作成中であるが、日本国として公開を希望している。 なお、5 か年計画に ICT に関する記載がある場合でも、それに対して予算が付くとは限らない。

2. 支援の方針について

サイバーセキュリティは公共と民間の責任分界点を明確にする必要がある。ミャンマーで明確化に取り組むのはもちろんであるが、ドナー側も明確化を支援していく必要がある。

また、MPT は事業者なのか規制側なのか、位置づけを明らかにする必要がある。

MCIT はあくまで一省庁のため、他省庁に対しても働きかけが有効であるか疑問がある。大統領府にサイバーセキュリティの重要性を理解させ、トップダウンで取り組んでいくことで早急な進展を望める。

e-gov プログラムは韓国の積極的な支援を受けているが、資金不足のため進展していない。

世界銀行、韓国、日本等のドナーによる支援をマッピングしていくことで、点の支援から面の支援への進展が期待できる。

3. 予算について

各省庁は年次計画を計画省へ提出する。計画省の承認が得られればプランニングコミッションを通過し、ファイナンシャルコミッションへ提出される。予算と合致していれば計画は承認されるが、一方で予算超過している場合には差し戻しされ、計画を見直すことになる。

そのため、年次計画をみれば予算の中身がわかる。

予算要求は 11 月までに提出し、確定は 3 月となる。また、補正予算は 9 月までに提出し、確定は 10 月となる。

半年に 1 回、予算の見直し機会がある。

4. 質疑応答

（調査団）サイバーセキュリティに関する雇用を増やす計画があるが、それは可能なのか。

	（工藤専門官）予算内であれば可能である。 5.　その他 ・無償資金協力の要請内容の変更は割と簡単に行うことが可能。 ・今後の選挙が少なからずリスクとなる可能性がある。
添付書類	なし
収集資料	なし

MPT (Myanmar Posts and Telecommunications) ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 14 日（金）　13:50～15:00
開催場所	MCIT 内オフィス
出席者 （敬称略）	MPT Myo Swe; Chef Engineer (Information & Technology Department) コンサルタント 佐藤　明男　業務主任/サイバー戦略 南部　尚昭　人材育成計画/協力支援内容検討 池田　好孝　ICT システム 宮本　健吾　データセンター評価 藤原　慧矢　業務調整
協議内容	＜概　要＞ MPT (Myanmar Posts and Telecommunications)に対してインセプション・レポートの協議および情報収集を行った。 内容： 1.　組織について MPT の中に IT 局があり、その下に e-Government やインターネットの管理運用を行う組織が存在していた。しかし、2010 年に発生した DDoS 攻撃が契機となり、IT 局の組織的な見直しと強化が行われ、現在の ITCS が設立された。設立の中心人物は、Myo Swe 氏と、Ye Naing Moe 氏（現在 National Cyber Security Center に在籍）である。 2015 年の組織改編により、ITCS は MPT から独立した組織となり、現在の MPT の IT 局は、MPT の ERP (Enterprise Resource Planning)に関する仕事を主に行っている。MPT には現在 50 人の職員がいるが、ITCS の職員を 200 人に増員する計画のため、MPT 職員数名を ITCS へ異動する予定がある。 2.　無償事業の担当部署 2015 年 11 月の選挙の際に、再度 DDoS 攻撃の発生を懸念し、JICA へ支援要請が MPT から出された。しかし、MCIT 内の組織改革により、無償事業が実施される場合は、ITCS　の NCSC (National Cyber Security Center) が実施機関の担当部署になるとのことである。

	3. MPT の民営化について MPT の公社化については 2016 年からを予定している。民営化についてはさらに 5~6 年を要する見込みである。この間は政府組織の一部であり、民営化は世界銀行の支援を受けて実施している。 4. サイバー攻撃の有無について MPT が受けたサイバー攻撃は、2010 年の選挙時に発生した DDoS 攻撃である。また、MPT のコロケーションサービスを利用している企業に対する攻撃が報告されている。サイバー攻撃の発生後、セキュリティ対策は特にその後講じていない状況である。 5. 各データセンターについて Hanthawady と Dkekina の 2 か所のデータセンターでは各省庁のオンラインサービス用のウェブサーバ、メールサーバなどが設置されており、コロケーションサービスを提供している。コロケーションサービスについては、MPT は場所と電源などの設備を提供しているという認識のため、ファイアウォール以上のセキュリティ対策は MPT では行わない。電子文書管理システムや政府の重要なデータはネピドーにある S12 ビルデータセンターと Thayetkhon のデータセンターで管理されている。 S12 ビルのデータセンターについて、以前は VPN で接続を行っていたが、様々な省庁から要望があったため現在では地方、外国にいる場合でも確認できるようにインターネット接続されている。
添付書類	なし
収集資料	なし

ICTTI(Information and Communication Technology Training Institute)ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 20 日（木）　10:00～12:00
開催場所	ICTTI 内ミーティングルーム
組織略称	MOST (Ministry of Science and Technology) ITIP (Institute of Technical Innovation and Promotion) ICTTI　(Information and Communication Technology Training Institute) IMCEITS (India- Myanmar Centre for Enhancement of Information Technology Skills)
出席者 （敬称略）	ICTTI Dr. Maychi Lai Lai Thein: Center Director Dr. Nan Gi Khan: Assistant Professor Daw Aye Age Nyein コンサルタント 佐藤　明男　業務主任/サイバー戦略 池田　好孝　ICT システム
協議内容	＜概　要＞ サイバーセキュリティに関する人材やトレーニングを調査するために ICTTI 所長である Maychi Lai Lai Thein 氏を訪問し話を伺った。打合せ後、ICTTI と IMCEITS の教室やサーバールームなど施設見学を行った。 1.　関連組織について ITIP は MOST に属しており、ICTTI と IMCEITS という 2 つのトレーニングセンターで構成されている。ICTTI は JICA の支援を受けており、IMCEITS はインドからの支援を受けている。両トレーニングセンターはネットワークやソフトウェアなど ICT 人材育成のトレーニングコースを提供している。 2.　ICTTI 基礎情報 2005 年に設立されており、現在スタッフは合計 60 名在籍している。大学を卒業した生徒を対象に数週間～数か月の様々な IT 関連のトレーニングを行っている。生徒数は年間で 800 名程度である。これまで日本以外の支援は受けていない。現在組織改編を行っており、まだプレジデントオフィスで審議中だが、これまでのトレーニングセンターの機能だけでなく、新たに研究開発の機能を追加するために研究棟を建設中である。

	3. 生徒について ITIP に入学するためには、大学の卒業資格が必須である。半年のコースで授業料が約 200,000 チャットとなっている。NTT データは優秀な学生に対してスカラシップ制度を設けている。卒業生は、日系企業や政府など様々なところに就職している。学生だけでなく政府の職員も入学可能であり、授業量は無料である。現在も MCIT の職員が数名受講している。 4. JICA の支援について 過去に ICTTI に対して 7 名の専門家の派遣が行われてきた。シニアボランティアの派遣も行われている。ICTTI は設立以降、日本以外の他国からの支援を受けたことはない。また、IMCEITS もインド以外の支援は入っていない。 道路や建物などの点で中国の支援に頼っているが、テクノロジー関連については日本を信頼しており、支援してほしいと考えている。これまで CITTI にコンタクトした中国企業も存在しない。 5. 予算について 年間の予算については決まっておらず、必要に応じて MOST に申請し、MOST から承認が得られれば申請額がもらえる仕組みとなっている。 6. サイバーセキュリティについて ミャンマーでサイバーセキュリティを効率よく進めるためには、機材だけでなく人材育成や能力強化などを同時に、かつスモールスタートで行っていくのがよいと ICTTI は考えている。また、サイバーセキュリティのコース提供を前向きに考えており、特に銀行職員に対して需要があると予想している。組織改編後の組織では、研究開発部の下にサイバーセキュリティの研究開発部門が設置される予定である。 7. ネピドーでのトレーニングセンターの可能性について ネピドーで新たなトレーニングセンターをオープンする可能性は低い。理由は、生徒が政府関係者しか集まらず、採算が合わない、講師の確保が困難（ネピドーに長期滞在してくれる講師確保が困難）なためである。
添付書類	なし
収集資料	なし

KOICA (Korea International Cooperation Agency) ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 20 日（木）　16:00～17:00
開催場所	KOICA 所長室
出席者 （敬称略）	KOICA Nam, Kwon-Hyoung: Chief Resident Representative Soe, Yungchae: Young Professional コンサルタント 佐藤　明男　業務主任/サイバー戦略 池田　好孝　ICT システム
協議内容	＜概　要＞ KOICA (Korea International Cooperation Agency) ミャンマー事務所を訪問し、IT 関連分野における支援について話を伺った。 1. IT 関係プロジェクトについて 現在 KOICA では以下の 2 つの IT 関連のプロジェクトを進めている。 一つ目は統計データシステムのインストレーションである。MNPED (Ministry of National Planning and Economic Development) の下の CSO (Central Statistical Organization)に対して、各省庁や機関などから集まってくる統計データを管理し、全国民が様々な統計データをオンラインで閲覧できるプロジェクトを実施中である。システムやデータベースの開発はすでに終了しており、近々リリースする予定である。 二つ目は法律情報システムの構築である。ミャンマー国には国民が自由に法律を閲覧できるシステムが存在しない。本システムの構築により全国民がオンラインで法律を観覧できるようになる。システムの詳細はまだ決定していない。 2. 日本と韓国の支援のデマケについて KOICA は ICT 分野に興味を持っており、今後も力を入れていく。中でも特に教育や研究分野における支援を行う方針である。現在考えているのは、光ファイバー網の構築、大学と民間企業が交流できる場としてのプラットフォームの構築などがある。ICT 分野はミャンマー国で飛躍的に成長しており、オンラインバンキングなどの普及により、サイバーセキュリティの支援は重要性も緊急度も高い。日本が行うサイバーセキュリティの支援と KOICA が今後行う ICT 関連の支援がオーバーラップしないように連携して支援の方向性を考えていきたい。

	3. その他 ミャンマー国から KOICA に数年前にサイバーセキュリティに関する支援を求める要請があった。
添付書類	なし
収集資料	なし

ヤンゴン工科大学ヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 20 日（木）　13:00～14:00
開催場所	ヤンゴン工科大学
出　席　者 （敬称略）	ヤンゴン工科大学 白川　浩　チーフアドバイザー 濱田　勇　業務調整員 コンサルタント 佐藤　明男　業務主任/サイバー戦略 池田　好孝　ICT システム
協議内容	＜概　要＞ ヤンゴン工科大学（Yangon Technological University、以下 YTU）では「ミャンマー国工学教育拡充プロジェクト」が JICA の支援により進められている。本プロジェクトでの取り組みやサイバーセキュリティ関連事項について日本人専門家である白川浩博士に話を伺った。 1. YTU について YTU はミャンマー国内にある工科系の大学の中でトップの大学であり、日本でいう東京工業大学にあたる。以前は科学技術省の管轄であったが、現在は教育省に属している。 2. 生徒のレベルについて ミャンマー国では高校卒業前に全国統一の試験があり、YTU にはその試験の 1 番～500 番程度の約 200 人が毎年入学している。ただし、暗記に中心の教育を受けてきているため、考える力が低く、また、優秀な人材は海外の大学へ進むため、YTU の生徒の中で優秀な者は一握りである。軍事政権以前は、ミャンマー国の教育レベルは高かったが、軍事政権により教育レベルが大きく低下した。現在は教育を立て直すことが急務である。YTU の卒業生で建設省や科学技術省の局長級、次官級の人間も多い。現在でも YTU 卒業後、政府機関に就職する学生は多い。 3. JICA の支援について 工学系の中核大学である YTU とマンダレー工科大学の製造･インフラ関連の 6 学科（電力、電子、情報技術、メカトロ、機械、土木）における教育・研究能力の強化を目的にこれまで以下の 2 つの JICA プロジェクトが行われている。

	・技術協力プロジェクト「工学教育拡充プロジェクト」　期間：2013-2018 年 ・無償資金協力「工科系大学拡充計画」贈与契約締結：2014 年 8 月 工学教育拡充プロジェクトは 5 年間の計画であるが、これまでの状況や現在の状況を勘案すると、あと 10 年近く必要だと白川氏は考えている。 4. サイバーセキュリティに対する認識について （白川氏）サイバーセキュリティを考えた際に、一般的なセキュリティの知識を持った人間、緊急の対応ができる人間の 2 種類必要だと考えている。政府組織に前者の人間は少なからず存在すると感じているが、後者については皆無である。また民間においても製品の知識は豊富にある人が増えてきているが、後者の人材は育っていないと思われる。そのため、いきなり無償資金協力を進めることに対しては懐疑的であり、技術協力からスタートすることが妥当である。 5. サイバーセキュリティ人材の発掘について （白川氏）ミャンマー国では資格の取得が好きな人間が多く、様々な研修やトレーニングに参加し、多数の資格を保持している。サイバーセキュリティ人材の発掘に関しては、人材発掘の確立を上げるために、多数の人を集めて研修を行い、その中からモチベーションが高い人やスキルの秀でた人を引き抜き、その人たちに対して持続的にトレーニングを行う組織を立ち上げるのがよいかもしれない。 6. サイバーセキュリティ普及・啓発活動について （白川氏）MCIT（Ministry of Communication and Information Technology）は情報教育を行う研修センターを保持しており、その研修センターの中に、日本で半年から 10 ヵ月程度研修を受けた講師が 5 人程度いる。その研修センターを活用すれば、政府関係者に対するサイバーセキュリティの普及・啓発活動は可能だと考える。既存の組織の有効活用し、政府関係者のトレーニングを行い、また大学と連携し、教育大学や工科大学において、教員や新入生に対してサイバーセキュリティも含めた倫理教育を必須にすることも効果的だと考える。 7. その他 ミャンマー国はトップダウンで物事が進む。各省の大臣の上のポジションとして、5 人の上級大臣がいるので、上級大臣に話を持っていくことができれば、物事が大きく進む。
添付書類	なし
収集資料	なし

ミャンマー国日本人材開発センターヒアリング議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 21 日（金）　10:00～11:00
開催場所	UMFCCI ビル 12F　打合せ室
出　席　者 （敬称略）	ミャンマー日本人材開発センター 金丸　守正　チーフアドバイザー コンサルタント 佐藤　明男　業務主任/サイバー戦略 池田　好孝　ICT システム
協議内容	＜概　要＞ ミャンマー人材開発センターの金丸氏に面会し、サイバーセキュリティ人材育成についてヒアリングを行った。 1.　日本人材開発センターについて 日本人材開発センターは JICA と MOC (Ministry of Commerce)、ミャンマー商工会議所連盟の協力体制で行われる「ミャンマー日本人材開発センタープロジェクト」の拠点となるもので、ミャンマーにおけるビジネス人材の育成や、日本―ミャンマー間の人材交流促進を目的として 2013 年に設立された。従来の日本センターに比べ、当初から事業を「ビジネス研修とそれに伴う人材交流」に絞り込み、日本的経営・生産管理手法を生かした講義を通じて、ミャンマーの明日の経済活動を担う人材育成に特化している。また加盟企業 27,000 社というミャンマー経済界を代表する組織である UMFCCI ビルへの入居により、現地産業界のニーズの的確な把握と活動への反映が可能であることが大きな特長である。 2.　サイバーセキュリティコースの開催の実現可否について （金丸）人材開発センターは、現在、中間管理職を対象にビジネスに必要な知識とノウハウを教えることを目的としており、その目的に沿ったコースを提供しなければならない。そのため、サイバーセキュリティに関して、企業や政府の職員にトレーニングする必要性は感じているが、同センターの目的とは異なるため、現在のところコース提供は難しい。 まずは、サイバーセキュリティに関する JICA 専門家を派遣し、制度や体制を整えることがミャンマー国に必要である。
添付書類	なし
収集資料	なし

V2M, Alpha インタビュー議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 21 日（金）　14:00～15:30
開催場所	V2M オフィス
出席者 （敬称略）	Vision to Motion: 明石　栄超 Alpha: Ye Myat コンサルタント 宮本　健吾　　データセンター評価
協議内容	＜概　要＞ 明石氏,Ye 氏に自身の起業や IT 業界に関係する話題をご提供頂いた。 1.　会社概要 V2M ソフトウェアのサービス提供など、IT ソリューションの提供を通して日系企業のミャンマー進出支援を行っている。その他、管理委託や構築、ソフト開発、販売代行もサービス提供している。 また、市場調査や事業社登録、経理等を代行支援し、日本企業の実績や日本の大手調査会社のミャンマー窓口としても実績を有する。社長は 15 年間日本で就労して日本人に帰化し明石姓を持っている。 Alpha 社 1997 年に創業し、コンピュータ販売から開始して ICT ベンダーとしてマンダレー地区でビジネスを行っている。市場に応じてソフトウェア販売、ネットワーク構築等へ拡大してきている。その他、データの電子化やマンダレーの e-Gov プロジェクトにも関与した経験がある。マンダレーコンピュータインダストリー（MCF 配下の MIEE）の理事を 2004-2008 年に勤めた。（MCF は MCPA,MCIE,MCEE,を有する。）MCF と関連しているため ICT の発展に関して情報を有している。モバイルで仏教の教本を学習するプログラムやミャンマー語入力できる「ゾウジ」というアプリを開発した。 2.　マンダレー地域のプロジェクトについて かつてマンダレー地域での e-Gov プロジェクトの調査に参加したことがあるが成

	功しなかった。現在では ADB が再ＦＳを Infosys 社に委託して実施している。e-コマースに関する調査を銀行・IT セクターとともに進めている。 Alpha 社は様々な政府系のプロジェクトに参加してきたが、ほとんど不成功に終わっている。その理由は、手続き・基準・セキュリティポリシー等の必要性が認知されておらず、整備もされていないことによると考える。 3. サイバーセキュリティについて 過去にマイクロソフトのセキュリティに関する調査が行われたが､その結果は“ほとんど無い”との評価であった。mmCERT の対応能力も低く、サーバ 2 台程度しか機器を持っていない。これでは国の団体としては不足している。政府は情報を公開する程度の能力はあるが、秘匿すべき情報等の対処ができていない。 調査団：サイバーセキュリティのレベルは？ 低いとのみ認識している。 調査団：サーバ攻撃に対する種類について認識等はあるか？ ウェブページが対象になるだろうが、それ自体も大変少ないもの。データセンターも MPT が有する数件のみで大変少ない。サーバーダウンが発生しても、さほど問題視されていない状況である。また、それに対する対策はミラーサーバーに転送する程度である。中央銀行はインターネットに接続しておらず、オンラインバンクは 1 件しか知られていない。300 支店の銀行がオンラインではなく、一日一回シンクするのみである。オンラインバンキング利用者は一般サラリーマンくらいでほとんどの人は口座を持っていない｡利用の上限額は一日 10 万チャットと非常に小額である。 調査団：経済成長する上で外資系企業等はサイバーセキュリティを条件として認識するのではないか。重要であるが、そこにビジネスチャンスを見ているか？ 具体的にイメージはできていないが需要はあると思う。最低でもウェブ環境がセキュアで業務処理をＩＴで対応するためにセキュリティが必要であろう。部分的にプライベート環境に対して民間による FW や電子証明ｎ提供があるだろう。プロバイダーの環境は事業社が対応すべきだろう。IT 環境の整備には費用がかかる話である、経営者判断を含めて市場が決まると見ている。 4. IT 人材について 調査団：サイバーセキュリティの人材育成をどう考えられるか サービス業としてのセキュリティに興味がある。メンテナンスなどでビジネスの

	機会はあるだろう。しかし、現状では難しいと思う。ライセンスフィーは経営者に認知されていない。経営者は機器購入の時点で満足しメンテナンスまで考慮しない。現在はソフトウェアの販売はハードウェアとバンドルされてようやく販売できている。 調査団：コンピュータ大学のカリキュラムにもセキュリティに関する教育が行われていないがどう考えられるか。 セキュリティ人材をどのように育成するかが課題と考える。業界も人材不足でありどこも課題である。コンピュータ大学の卒業生ですら IT 企業へ就職していない。全国で年間 6000 人はコンピュータ系のカリキュラムを終えて卒業した人材がいるはずであるが、実際は IT 業界全体で 2000 人程度しか就労していない。これまでの UCSY 卒業生だけでも 60000 人程度はいるはずである。これはコンピュータ業界の規模が小さいことが原因であろう。卒業生もできるだけ高収入を求めて関係ない業種に就職し、コンピュータから遠ざかって行く。当社も 20 人前後と小企業であるため業務の受託できる数も限られてしまう。 ミャンマー経済の問題もあり、チャンスを求めてシンガポールに人材が出て行く。新たに育成された IT 人材がいたとしても、そのうち 40%程度の優秀な人材は海外へ出て行き、残り 60%は国内へ残るが、IT をやめてしまうと聞いている。 調査団：国内における IT 系の人気度はいかがか？ 他の業界は母数が少ないため競争が発生しており人気に見えるかもしれないが、IT 系は一般的には人気度高いであろう。 調査団：ミャンマーで人気のあるＩＴ企業は？ ①MIT：myanmar information technology ソフトウェア会社 ②Ace:大和総研が関係しているソフトウェア会社。 ③global wave：200 人程度で、創業者はシンガポールで働いていた。 の 3 社である。 5. 政府に対する要望は? インターネット回線の状態が良くない状態である。ファイバー回線を接続しているが モバイル回線よりも品質が悪く、二日間故障から回復されないこともある。 政府と民間企業の連絡があまりなく紹介を受けても仕事にならない場合が多い。IT ソリューションを紹介する機会を得たが、e-Goverment の導入を目指しているようである。しかし、その前にどの課題から解決するか、規則を設定するか、ポリシーの内容をどのように決定するか、法律を整備するかをなどはっきりさせな

	ければならないと思う。 その他、電子証明書、通信インフラやデータセンターの整備を期待したい。 政府の中の IT ソリューションについて、民間企業へもっと広く開放して欲しい。海外製品を購入する際にも民間企業を活用願いたい。政府系業務を通じて IT 業界も発展するだろうと考える。 ADB 支援で電子化する案件があり会社登録局の電子化である。しかし、実際に導入しようとしたところ 100 年前の法律が障壁となった。
添付書類	なし
収集資料	なし

RedLink 社インタビュー議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 21 日（金）　14:00～14:50
開催場所	RedLink オフィス
出席者 （敬称略）	RedLink: Prasert Laosaengpha　Chief Technical officer Wai Lin Oo　Deputy Chief Engineer コンサルタント 中村　尚　　セキュリティ対策計画 2/セキュリティアセスメント
協議内容	＜概　要＞ 現地通信事業者である RedLink にてセキュリティを統括している Laosaengpha 氏と Oo 氏に情報通信事業者におけるセキュリティへの取り組み状況などについて情報をご提供頂いた。 1.　セキュリティへの取り組みについて 同社のサービスはインターネットアクセスの提供であり、コロケーションやサーバスペースの提供などは行っていない。そのため具体的なセキュリティとしては同社のネットワークに対する防御が中心であり、ファイアウォールの設置、アクセス許可リストの整備、ユーザ管理等の基本的な対策が施されている。それ以上のセキュリティを望む顧客においては、顧客側で独自にファイアウォール等を設置することとしている。 業務上でのセキュリティ対策としては、重要なドキュメント類には（Microsoft が提供するレベルの）パスワード及び暗号化を用いるようにしている。 なお、ミャンマーには ROOT CA（ルート認証局）があるが、一般の民間事業者によって運営されている状況であり、これは問題がある。 調査団：IT セキュリティポリシーは作成しているか？ それは ISO 27002 に準拠したものか？ IT セキュリティを考慮したガイドラインは作成しているが、ISO27002 には準じていない。また特に政府からも IT セキュリティに係るフレームワークは示されていないため、独自に作成したものである。 調査団：IT セキュリティに特化した組織の構築等は行っているのか？

	セキュリティの重要性については強く思うが、現状ではオペレーションに注力せざるを得ないため、IT セキュリティに特化したチームは構成できていない。サイバーセキュリティに特化した人材も少ない。 セキュリティに関しては担当者はおり、主にファイアウォールの設定やアタックの特定等、サーバの防御を担当する人間はいる。 調査団：IT セキュリティに関する民間の連携や団体等はあるのか？ セキュリティにフォーカスした連携はまだない。mmCERT とは連携しており、様々な情報提供・情報交換もしている。ミャンマーではセキュリティに特化した活動をしている唯一の機関と思われる。 2. 人材の確保について 現在ミャンマーでは、アカデミー（大学）と民間企業の連携はほとんどなく、そのつなぎとなる機関もほとんど存在していない。このため、民間企業が求めているものと大学が教育している内容には大きなギャップがある。 特にサイバーセキュリティに至っては、コンピュータ系の大学を出てきた学生であっても、何がサイバーセキュリティであるかをわかっていない。 調査団：インターンシップ等の教育プログラムはないのか？ 残念ながらない。企業側のニーズにあった教育はあまり望めない。もっと産官学が連携して人材を育てていく必要がある。それはセキュリティだけでなく IT 全体にいえることである。他の国では IoT 等が注目されているが、ミャンマーの IT 産業はそのようなレベルではなく、ようやく産業が始まったところであり、成長の過程にある。つい４カ月ほど前にもライセンスの簡素化等の改正が行われており、暗中模索のところである。 調査団：社内での教育はどのようにしているのか？ エリア及び利用者の拡大のために、現地サービスマン等を中心に研修を行っている。サーバ防御の担当者等は外部のトレーニングクラスに２～３か月程派遣したりしている。いずれにしても現状では入社後に自社で育てるしかない。 調査団：具体的な攻撃は受けているか？セキュリティ上の課題等はあるか？ 特に重要なセキュリティ課題については直面してはないない。３年ほど前に、国外からか国内からかはわからないが大規模な DDOS 攻撃が問題となった。細かな

	攻撃を受けたりすることもあるが、サーバを停止されるような重大な攻撃は受けていない。ウェブサイトへの攻撃はあるが、重大ではない。 3. 政府への要望等 ミャンマーでは２年程前から政府が通信市場を開放し、移動体通信が伸びはじめたことでインターネット利用者が増え始め、これを踏まえて政府は e-Government を検討している。これによってサイバーセキュリティの重要性も高くなってきた。これに対して、現状ではサイバーセキュリティに対するフレームワーク（法制度、ガイドライン等）が何一つない状況である。ネット上でアタックを受けて、キャリアがその IP アドレスを特定できたとしても、それを誰に報告すればよいのか何も決められていない。警察に報告しても警察はどう動く必要があるのかが分かっていない状況である。 調査団：政府への要望や提案があればご教示頂きたい。 政府の職員はいまだ Gmail を使っているような状況であり、早期に多くを期待するのは難しいと思うが、まずは、サイバーセキュリティ、個人情報保護、データ保護、サイバー犯罪等に対する法規制（フレームワーク）を整えてほしい。
添付書類	なし
収集資料	なし

Yatanarpon Teleport インタビュー議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 21 日（金）　15:00～16:00
開催場所	Yatanarpon Teleport HQ オフィス
出　席　者 （敬称略）	Yatanarpon Teleport: Thein Myint Khine　　Department Head コンサルタント 中村　尚　　セキュリティ対策計画 2/セキュリティアセスメント
協議内容	＜概　要＞ 現地通信事業者である Yatanarpon Teleport にてセキュリティを統括している Khine 氏に情報通信事業者におけるセキュリティへの取り組み状況などについて情報をご提供頂いた。 1.　セキュリティへの取り組みについて Yatanarpon Teleport のサービスはインターネットアクセスの提供に加えてコロケーションなども行っている。同社では新たなセキュリティ対策部署を立ち上げたが、技術的専門性についてはまだ不足している状況で、まだまだ経験を積む必要性があると認識している。それまでネットワークセキュリティについては、他の部署が行ってきた。セキュリティの重要性については強く同意するが、現状は日々のオペレーションに力が割かれており、十分にセキュリティについて対応している余裕がない。 サーバの導入やファイアウォールの設置、コロケーションの利用等に係る簡易なセキュリティポリシーは策定している。具体的には不要ポートの停止や外部へのアクセスの管理等が盛り込まれている。 アクセスロギングサーバを設置し、上記の新たなセキュリティ対策部署がアクセスを監視しており、異常があれば知らせるようになっている。DPI（Deep Packet Inspection）のデバイスも持っており、顧客のネットワークに異常があれば顧客に知らせるようにしている。 ５年前に（選挙に向けて）大規模な DDOS 攻撃があった。ルータである程度探知できる機能は有しており、また BTB コミュニティを立ち上げ、何かあればルータで絞る等を行っている。しかしアタックに対する防御システム（Mitigation System）は持っておらず、ファイアウォールでの防御のみである。このためサーバ群については防御しているが、顧客のネットワークまでは防御できていない。 調査団：BTB コミュニティは誰が入っているのか？ 社内での情報共有のためのコミュニティであり、対外的には情報共有としては

mmCERT が中心で、通知などを受けて対応を行っている。しかし外部から通報を受けても、内部ネットワークは NAT を介してローカル IP アドレスが使用されているため、顧客の機器から外部のネットワークに対して攻撃していても、その機器を特定しにくいのが現状である。現状ではアクセスログをひたすら監視するしかなく、弱みといえる。

調査団：政府のウェブサイトをコロケーションしているが、その際に独自のセキュリティの要求等はあるのか？
政府からは特に要求はない。Yatanarpon Teleport ではポリシーを定めており、他のユーザと同様にそのポリシーに従ってサービスを提供している。サイバーセキュリティに関してはあまり政府から法律やガイドラインは示されていないため、独自にポリシーを定めるしかない。また特に SLA も設定していない。

2. 人材の確保について

大学レベルで習得する知識と実際に必要な知識の間には大きなギャップがあり、企業側の要望も考慮したカリキュラムをもっと考えてほしい。大学の卒業生を新規採用した場合、企業内での育成は必須となる。

調査団：セキュリティのスペシャリスト人材をどのように増やしていけばよいか？
セキュリティのスペシャリストを確保するためには、自社で育成するか外部から調達するかであるが、外部からの調達については、自社社員として雇用する以外は外注や委託等でとなるが、当社ではポリシーの関係で外部への委託は難しい。
基本的には自社において、基本的な技術を有した人（既存社員等）にセキュリティの教育を施すのが最も近道と考えられる。その際、日本は既に様々なセキュリティ危機の経験を有していると思われるので、それらの経験を共有してくれれば非常に参考になると思われる。

調査団：社内での教育はどのようにしているか？
新たな機器の導入等の際はベンダーのトレーニングについても受けている。ほとんどは OJT である。経験が重要なので、実際に使用している担当者による経験の共有等の教育プログラムを有している。

調査団：外部の研修への派遣などはおこなっているのか？
新たなプロジェクト等によって、予算とともに教育が必要となる場合は外部の研修を利用することも考えられる。

調査団：具体的な攻撃は受けているか？セキュリティ上の課題等はあるか？
セキュリティについては重要であることは非常に認識しているが、定常のオペレー

	ションや顧客対応に時間を割かれており、またセキュリティや対 DDOS の機器等は非常に高価であり、なかなかこれらに投資をする余力もない。 せめて政府の協力ということでは、DDOS 対策をインターナショナル・ゲートウェイのレベルで整備してくれると少しは改善されると思われる。 現状では提供しているネットワークの内部については、例えばサーバ等に攻撃があった場合、容易に攻撃元をトレースできるが、外部になると攻撃元をトレースすることは非常に難しくなる。 3. 政府への要望等 課題解決には通信事業者同士の連携が重要となるが、現状では各社バラバラであり連携は十分にとれていない。mmCERT は通信事業者間のセキュリティに関する情報提供、情報共有の場としては機能しているが、通信事業者が最低限のレベル（共通するポリシー等）を有している必要があり、政府にはそのあたりのガイドラインや調整役等をお願いしたい。 調査団：その他に（セキュリティだけではなく）政府への要望はあるか？ 現在、インターネットコネクションの拡張は制限を受けており、キャリアで自由に拡張することができない。市場拡大のためにもより自由に拡張できるようにしてほしい。
添付書類	なし
収集資料	なし

Minutes of Meeting 協議議事録

調　査　名	ミャンマー国サイバーセキュリティにかかる情報収集・確認調査
開催日時	平成 27 年 8 月 24 日（月）　15:00～16:30
開催場所	MCIT オフィス (S2 ビル)
出　席　者 （敬称略）	MCIT (Ministry of Communications and Information Technology) IT&CS (Information Technology and Cyber Security) Department Sai Saw Lin Tun　Deputy Director General コンサルタント 佐藤　明男　業務主任/サイバー戦略 南部　尚昭　人材育成計画/協力支援内容検討
協議内容	＜概　要＞ 8 月 27 日予定されている現地調査概要報告の報告内容と招待する省への招待方法、質問表に回答について協議を行った。以下に意見交換の詳細を示す。 1.　支援の方向性について （調査団）現地調査を通して、サイバーセキュリティ分野への支援についての必要性はあると考えている。また人材育成が最も重要であると感じている。サイバーセキュリティは、攻撃を受けた時の対処方法が肝心で、人為的な調整が不可欠である。またサイバーセキュリティに関する政府政策・方針、重要インフラの定義、制度、基準・ガイドライン等が整備されていない状況下では、職員のサイバー攻撃に対するモニタリング、対応能力向上と合わせて行う必要があると思っている。 そのため、4 つの成果を調査団の中で検討しているところである。1 つ目は、政策、促進策、制度、基準のガイドラインなどを整備すること。二つ目はサイバーセキュリティに関係する組織体制の整備、3 つ目はサイバー攻撃に対するモニタリング機能の整備。これには、モニタリング用の基本的な機材の調達も含むのが良いと考えている。4 つ目は、サイバー攻撃に対する職員の意識の向上で、職員の意識向上を通じて、国民にも伝わるようにできないかと思っている。 無償の要請として GSOC の機材整備があるが、MPT が来年度には民営化すること、データセンターの MPT 所有分と政府所有分が要請書の機材配置の想定と異なること、政策・方針、法制度、基準・ガイドラインが準備されてから、どのような仕様の設備にするかを考えたほうが適切な内容のコンポーネントを検討できることを理由として、まず技プロを開始してからその対処を考える方が良いと思っているが、副局長のこれに対するお考えを伺いたい。 （DGD）人材育成は非常に重要だと理解している、と同時に、監視システムやセキ

	ュリティシステムの導入も重要である。mmCERT が ASEAN の枠組みや他国の CERT との連携を行っている。PTD が規制局であるがサイバーセキュリティに関する規制のフレームワークを我々から提案することもできる。一方 GSOC の機材の整備・更新は重要視している。 データセンターを構築しようとしている中、サイバーセキュリティでは、データの保護、アプリケーションの保護を考えなければならない。また 4G も導入されていく中、政府のデータセンターは B2B、G2G 等、様々な状況で使用されていく。つまり政府のデータセンターは、その内容と通信手段について、注目されていくことになる。 政策、基準、規則などを作ってから GSOC を設置した場合、政策などを作っている最中にもデータセンターはサイバー攻撃に身をさらすことになる。基準、規則などを作るのにどの程度時間がかかるかは定かではないが、平行的に進めることが良いと考える。 また、重要インフラの定義付けであるが、給水システム、電力等、誰が見ても重要なインフラと分かるが、省庁間の統一見解を求めるのは難しい。それぞれの省庁は皆、異なったセキュリティレベルにある。統一基準を作るよりはそれぞれが必要なセキュリティレベルで対策を進めていくのが今は必要であると考えるが（何もしないで放置しておくことはできない。）、ワークショップなどで意見を聞くことも可能である。 MCIT はトレーニングセンター政府機関を要し、職人対する研修やセミナーを定期的に実施している。すべての省庁が e-learning を行っている。ITU もサイバーセキュリティトレーニングを提供している。APCERT でのサイバーセキュリティに対する連携もある。データのセキュリティ保護の強化、各省の異なるセキュリティレベルについて検討し、それぞれの状況に応じたサイバー攻撃に対応できる組織を強化してきたい。最低でもサイバー攻撃を検知し、対処し、復旧をどのように行うか判断できる人材を育てていきたい。決して、各省に対して画一的なセキュリティ対策を押し付けたくはない。 （調査団）技プロで調達する機材である程度のモニターもできる。また現在データセンターに設置された機材では、サイバー攻撃に対処するための機能が付いているものがある。しかしながら、その機能をなぜか生かしていない。これを合わせて使えば、まずは基本的な部分の対応ができる。その中で人材を育て、技能が身についた段階で、機材をアップグレードするなどの方がミャンマーの現状に合致していると考える。 主だったドナーにヒアリングをした結果、どのドナーもサイバーセキュリティ分野の支援は検討しておらず、IT や電子政府について、支援の主流ではないが、行っている、または行う可能性があると分かった。調査団はサイバーセキュリティについて、支援の重要性は認識している。ミャンマーにとって最善の方法で出来得る支援を検討したいと思っている。

	（DGD）人材育成が重要で、技プロを検討すること、また GSOC の基本的な進め方は、将来的な拡張ということは理解した。 2. 現地調査概要報告について （DGD）27 日でアレンジする。午前か、午後かは、会場の確保と合わせて別途連絡する。招待者についは、ヒアリングした政府機関からそれぞれ 2~3 名ということで承知した。招待状の発出、開会のあいさつなど、省内で確認して連絡する。ヒアリングした省庁については、別途メールで送付して欲しい。 3. 質問表の回答について （DGD）質問表の内容を把握していないので、質問表を再度メールで送付した欲しい。自分の手元にある回答内容を含んだドキュメントについては、すぐに提供する。手に入るものから順次提供する。 （DGD）予算については、どのレベルのものを出すのかで、手続きが異なる。MCIT 全体のものは、確認しないと手に入るかどう分からない。ITCS 局は今年できた局であるため、本年度の予算はない。MPT のものは手に入るか確認する。また MPT の予算の内訳は MPT 内部の 6 つの部署レベルのものが手に入るか確認する。予算も手に入るものから順次提供する。
添 付 書 類	なし
収 集 資 料	なし