インドネシア共和国
情報セキュリティ能力向上
プロジェクト
詳細計画策定調査報告書

平成26年９月
（2014年）

独立行政法人国際協力機構
社会基盤・平和構築部

基盤
ＪＲ
14-194

インドネシア共和国
情報セキュリティ能力向上
プロジェクト
詳細計画策定調査報告書

平成26年９月
（2014 年）

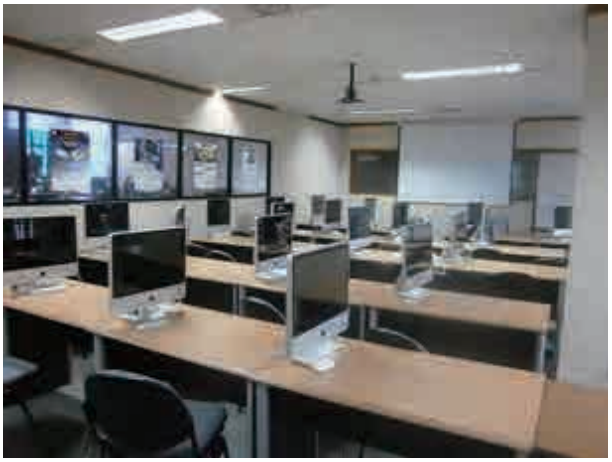
独立行政法人国際協力機構
社会基盤・平和構築部

目　　次

調査時写真

Minutes of Meeting 署名

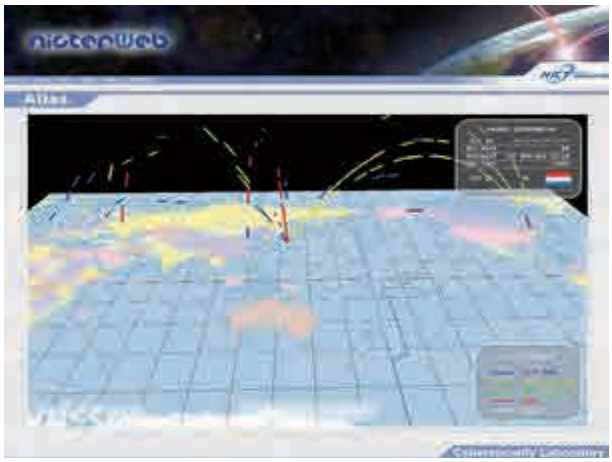
インドネシア国インターネット基本セキュリティ
インシデント対応チーム（ID-SIRTII/CC）との協議



ID-SIRTII の研修用教室

KOICA 支援で設立された国立 ICT 人材育成センター
（NICT-HRD）

KOICA 支援で設立された NICT-HRD 内には
宿泊施設も完備されている。



【参考】nicter の画面（NICT の Web から：
http://www.nicter.jp/nw_public/scripts/atlas.php）

略　語　表

略　語	英　語	意味・説明
ACAD-CSIRT	Indonesia Academic Computer Security Incident Response Team	インドネシア学術 CSIRT
APCERT	Asia Pacific Computer Emergency Response Team	アジア太平洋地域コンピュータ緊急対応チーム
APJII	Asosiasi Penyelenggara Jasa Internet Indonesia	インドネシアの ISP 業界団体
ASEAN	Association of Southeast Asian Nations	東南アジア諸国連合
BCP	Business Continuity Planning	事業継続計画
CA	Certification Authority	認証局
CCNA	Cisco Certified Network Associate	世界最大手のネットワーク機器メーカー Cisco Systems 社による技術者認定資格のひとつ
CERT	Computer Emergency Response Team	コンピュータ緊急対応チーム（セキュリティに関する情報の収集・提供や、インターネット上で不正アクセスを受けた場合の報告受け付けなどを行う非営利団体の一般的な名称）
CIO	Chief Information Officer	最高情報責任者
CISO	Chief Information Security Officer	最高情報セキュリティ責任者
CISSP	Certified Information Systems Security Professional	国際的に認められた情報セキュリティ・プロフェッショナル認証資格
CLM	Cambodia, Lao PDR, and Myanmar	カンボジア、ラオス、ミャンマー
C/P	Counterpart	カウンターパート
CSIRT	Computer Security Incident Response Team	コンピュータセキュリティインシデント対応チーム（インターネット上で何らかの問題（主にセキュリティ上の問題）が起きていないかを監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査を行ったりする組織の総称）
DoS	Denial of Services	サービス停止（Denial of Service attack とは、サーバなどのネットワークを構成する機器に対して攻撃を行い、サービスの提供を不能な状態にすること）
e-KTP	Kartu Tanda Penduduk Elektronik（Indonesia Electronic ID Card）	電子式身分証明書

FIRST	Forum of Incident Response and Security Team	CSIRT の国際的なフォーラム
ICT	Information Communication Technology	情報通信技術
ID-CERT	Indonesia Computer Emergency Response Team	インドネシア国コンピュータ緊急対応チーム
ID-SIRTII/CC	Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center	インドネシア国インターネット基盤セキュリティインシデント対応チーム
IEC	International Electrotechnical Commission	国際電気標準会議
IPA	Information-technology Promotion Agency, Japan	独立行政法人情報処理推進機構
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
ISP	Internet Service Provider	インターネット・サービス・プロバイダー
IT	Information Technology	情報技術
JP-CERT	Japan Computer Emergency Response Team	日本国コンピュータ緊急対応チーム（通常、日本語でも JP-CERT と呼ばれている）
KOICA	Korea International Cooperation Agency	韓国国際協力団
MCIT	Ministry of Communication and Information Technology	情報通信省
MM	Man Month	人月
MOU	Memorandum of Understanding	覚書
NAP	National Access Point	ナショナル・アクセス・ポイント（国に設けられたインターネット接続のための接続地点）
NGO	Non-Governmental Organization	非政府組織
nicter	Network Incident analysis Center for Tactical Emergency Response	独立行政法人情報通信研究機構（NICT）が研究開発を進めているインシデント分析システム
NICT-HRD	National Information and Communication Technology-Human Resourced Development	国立 ICT 人材育成センター

OIC-CERT	Organisation of Islamic Conference - Computer Emergency Response Team	イスラム諸国会議機構 CERT
PANDI	Pengelola Nama Domain Internet Indonesia	「.id」のレジストラ
PDSI	Pusat Data dan Sarana Informatika	情報基盤データセンター
PRACTICE	Proactive Response Against Cyber-attacks Through International Collaborative Exchange	国際連携によるサイバー攻撃予知・即応プロジェクト
SMS	Short Message Service	ショートメッセージサービス
SNS	Social Networking Service	ソーシャル・ネットワーキング・サービス

第１章　調査の概要

１－１　プロジェクトの背景

インターネットの急激な普及に伴い、情報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にして Web サイトや端末に不正に接続し、サイトの改ざん、機密情報の外部流出をねらう行為であるサイバー攻撃の被害が国際的に増加している。2013 年 3 月には、韓国にて放送局、銀行等が大規模なサーバー攻撃を受け、わが国もこれら組織的攻撃を受ける可能性は十分にあり、対応が急務となっている。

コンピュータウイルスや DoS 攻撃といったサイバー攻撃の脅威はインターネットを介して攻撃対象に到達するため、情報セリュリティ対策が不十分な国の情報システムは、サイバー攻撃に対して脆弱なだけでなく、サイバー攻撃の発信元や経由地点（踏み台）として利用されるリスクが高くなり、その国のビジネス環境の信頼性低下を招くことになる。逆に、情報セリュリティレベルの高い国においては、ビジネス環境の信頼性が高まり、高付加価値及び知識集約型産業への直接投資が促進されることが期待される。

このような背景から、インドネシア共和国（以下、「インドネシア」と記す）政府は 2007 年に情報通信省（Ministry of Communication and Information Technology：MCIT）傘下に National CERT（コンピュータ緊急対応チーム ; Computer Emergency Response Team）であるインドネシア国インターネット基盤セキュリティインシデント対応チーム（Indonesia Security Incident Response Team on Internet Infrastructure / Coordination Center : ID-SIRTII/CC）を設け、さらに 2012 年には同省内の情報セキュリティ担当部門下に Government CERT を設けるなど、自国における情報セリュリティレベルの向上を図っている。しかしながら、インドネシアを“踏み台”とした ASEAN 諸国へのサイバー攻撃や ASEAN 諸国からインドネシアへのサイバー攻撃は多く、十分な対策ができているとはいえない。このため、インドネシアは同分野における経験や技術レベルの優れているわが国からの支援を要請した。

しかしながら、サイバー攻撃は主にインターネットを介して行われることから、一国だけでの情報セキュリティ対策は限定的であり、より効果的な対策を行うためには、各国・地域のサイバー攻撃情報を収集・分析し、国際的なサイバー攻撃を予知・即応するための取り組みが必要である。このため、同要請を受け JICA は 2013 年 4 月に調査団を派遣し、インドネシア政府機関における情報セリュリティ関連組織体制及び各組織の能力の確認を行うとともに、ASEAN 諸国との連携可能性についても、MCIT と協議を行った。その結果、本プロジェクトにおいては、MCIT 内の情報セキュリティ担当部局を中心に、インドネシアの情報セキュリティ対応能力向上を主目的としつつ、インドネシアに対する支援のみではなく、他 ASEAN 諸国への広域的連携可能性も視野に入れつつプロジェクトを実施する方針となった。

ASEAN 全体の情報セリュリティレベルを向上させることは、各国の経済活動の促進に寄与するとともに、ひいてはわが国に対するサイバー攻撃の予知も可能となり、情報セキュリティの安全性向上に貢献するものであるともいえる。

１－２　調査の目的

今回実施の調査は、インドネシア政府からの協力要請の背景、内容を確認し、先方政府及び関係機関との協議、また必要な情報の収集・分析を経て、協力計画を策定することを目的とした。

１－３　調査団の構成

担　当	氏　名	所　属
団長／情報セキュリティ	井出　博之	JICA 国際協力専門員
協力企画	竹内　知成	JICA 経済基盤開発部計画・調整課 兼 運輸交通・情報通信第二課 主任調査役

１－４　調査日程

2013 年 7 月 14 日から 2013 年 7 月 24 日

１－５　主要面談者

氏　名	所　属
Ashwin Sasongko	MCIT Director General for Informatics Applications
Bambang Heru Tjahjono	MCIT Director of Information Security
Yudhistira	MCIT Head of Risk Management Section, Directorate of Information Security
Yan Rianto	MCIT Head of Data Center（PDSI）
Rudi Lumanto	Senior Advisor to Minister on Information Systems 兼 Chairman of ID-SIRTII/CC
M. Nur Gunawan	Vice Head of NICT-HRD Management Unit
Imam M.Shofi	Vice Head of NICT-HRD Management Unit
Aries Susanto HT.	Ministry of Regional Affairs Syarif Hidayatullah Sate Islamic University, Faculty of Science and Technology, Assistant Professor
Muhammad Salahuddien	ID-SIRTII/CC Vice Chairman of Operation & Network Security
Muhammad Salman	ID-SIRTII/CC Vice Chairman of External Collaboration
Bisyron Wahyudi	ID-SIRTII/CC Vice Chairman of Data Center, Application & Database
Adri Gautama	PT. Cisco Systems Indonesia Area Academy Manager
Sihmirmo Adi	PT. Telkom Indonesia Information System Center, Deputy Senior Manager

第２章　インドネシアの情報セキュリティ環境の現状

本調査では、現地情報セキュリティ環境の調査に十分な時間を割くことができなかったため、この章は JICA が別途実施した調査の報告書「ASEAN 諸国における情報セキュリティ情報収集・確認調査報告書（2012 年 12 月）」を参照し、新たに判明した部分のみ加筆・修正している。

２－１　一般情報

首都	ジャカルタ
政体	大統領制、共和制
言語	インドネシア語
宗教	イスラム教 88.1%、キリスト教 9.3%（プロテスタント 6.1%、カトリック 3.2%）、ヒンズー教 1.8%、仏教 0.6%、儒教 0.1%、その他 0.1%（2010 年、宗教省統計）
面積	約 189 万平方キロメートル（日本の約 5 倍）
人口	約 2.38 億人（2010 年、政府推計）
人口密度	127.53 人/km²
通貨単位	インドネシア・ルピア
GDP(名目)	8,466 億ドル
経済成長率	6.5%
貿易額	輸出：2,035.0 億ドル、輸入：1,774.4 億ドル

[出典：外務省　http://www.mofa.go.jp/mofaj/area/indonesia/data.html]

２－２　インターネット関連データ

インターネット利用者数	2,183 万人（2010 年）
インターネット加入者数	21 万 8,200 人（2010 年）
ブロードバンド利用者数	170 万人（2010 年）
利用者層	インターネットの世帯普及率は 2009 年時点で 0.8%だが、多くは携帯電話から利用
接続形態	DSL、CATV
利用場所	携帯電話を用いたインターネットアクセスが中心 Warnet と呼ばれる公衆インターネット接続センターが、インターネット接続普及の中心的な役割を担っている）
利用目的	Facebook などの SNS を携帯端末を用いて利用する方法が一般的
料金	－

[出典：総務省　世界情報通信便覧　http://g-ict.soumu.go.jp/]

２－３　情報セキュリティ関連の事例・統計情報

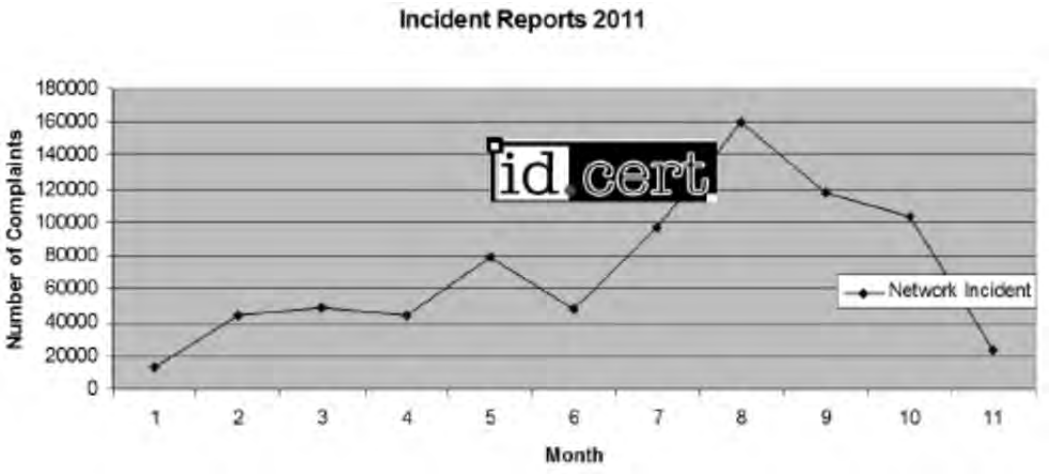
インドネシアのサイバー攻撃に関するインシデントの統計情報は、インドネシア国コンピュータ緊急対応チーム（Indonesia Computer Emergency Response Team：ID-CERT）、ID-SIRTII/CC によって収集が行われている。ID-CERT は攻撃を受けた側の報告に基づく統計を整備し、ID-SIRTII/CC

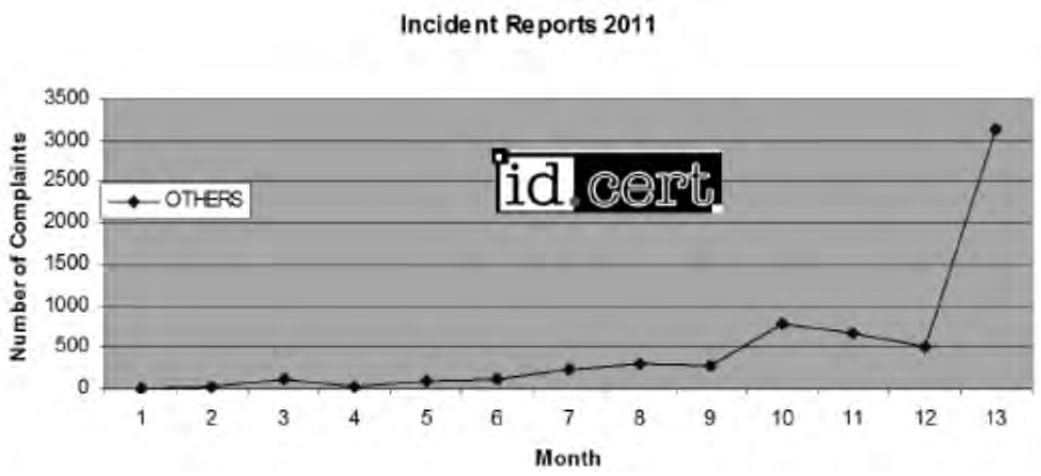
は同様の手法に加えて国内の主要なインターネット・サービス・プロバイダー（Internet Service Provider：ISP）などに置かれたセンサでインターネット上の脅威の観測を行っている。MCIT は、政府組織に関する統計を持っているが、非開示としている。

ID-CERT では通信事業者や ISP と連携し、レポートを収集した結果を統計情報として発表している。レポートはネットワークインシデント、スパム、知財権の侵害、マルウェア、フィッシング、詐欺に分かれている。このうち、アジア太平洋地域コンピュータ緊急対応チーム（Asia Pacific Computer Emergency Response Team : APCERT）Annual Report 2011 で公開された情報は図２－１のように、ネットワークインシデントとその他のインシデントに分類されている。2011 年は 3 つの政府機関、「.id」のレジストラの PANDI、ニュースポータルサイトの DETIK.NET、5 つの通信事業者、及び、6 つのナショナル・アクセス・ポイント（National Access Point：NAP）、25 の ISP などから情報提供を受けて調査を行っており、報告者からの統計情報や不正利用に関わるレポートの収集など約 100 万件のインシデントに関するレポートを収集したと発表している。また、調査は MCIT、インドネシアの ISP の団体である Asosiasi Penyelenggara Jasa Internet Indonesia（APJII）及び PANDI からの資金提供を受けている。

図２－１に記載されているネットワークインシデントには、DoS 攻撃、オープンリレー、オープンプロキシ、ポートスキャン、ポートプローブ（HTTP/HTTPS、FTP、TELNET、TCP、SSH、CGI、RPC、Netbios、VNC Portscan）及び SQL インジェクションが含まれる。その他、スパム、知財権の侵害、マルウェア、フィッシング、詐欺といった項目別に 2011 年のインシデント発生状況が示されている。

2011 年よりわが国総務省の国際サイバープロジェクト（現在の PRACTICE プロジェクト）の一環として、インシデント等の観測センサの設置に関する協力を進めている。





出典：Indonesia CERT

図２－１　ID-CERT によるインシデントの統計

他方、ID-SIRTII/CC では主要なアクセスポイントに設置しているセンサの計測情報に基づき、統計情報を ID-SIRTII/CC のウェブサイト上で公開している。ID-SIRTII/CC では APJII などと連携し、攻撃手法に関する統計、攻撃の目標の統計等のインシデントの統計を公開している（表２－１、表２－２、表２－３、表２－４）。ID-SIRTII/CC の公表資料ではセンサは計測可能なトラフィックの 70%程度を収集しているとされている。2011 年に観測された悪意のある攻撃の疑いは約 5,000 万件であり、最も多い攻撃は Remote File Inclusion (RFI)13 である。

表２－１　2011 年上半期のセンサによるインシデント報告件数

Event	Jan	Feb	Mar	Apr	May
SQL heap-based overflow attempt (1:4990)	3.816.558	1.896.932	620.217	298.380	334.451
SQL Worm propagation attempt OUTBOUND (1:2004)	3.815.875	1.896.424	619.854	297.696	334.015
SQL Worm propagation attempt (1:2003)	3.815.730	1.896.319	619.843	297.567	333.984
DNS large number of NXDOMAIN replies - possible DNS cache poisoning (1:13948)	1.305.044	600.877	495.552	559.266	737.578
SMTP_HEADER_NAME_OVERFLOW (124:7)	333.228	347.196	419	0	0
SMTP_COMMAND_OVERFLOW (124:1)	295.859	347.196	276.255	0	0
HI_CLIENT_NON_RFC_CHAR (119:14)	295.276	69.646	76.226	5.588	4.550
WEB-CLIENT Safari-Internet Explorer SearchPath blended threat attempt (3:15468)	130.918	123.781	181.008	82.316	20.361
NETBIOS DCERPC NCACN-IP-TCP path canonicalization stack (3:14782)	124.846	70.506	88.574	43.903	9.383
NETBIOS DCERPC NCACN-IP-TCP overflow attempt (1:7209)	124.836	70.125	88.494	43.323	9.189
TOTAL	14.058.170	7.319.002	3.066.442	1.628.039	1.783.511

* 10 Most Active Events

出典：ID-SIRTII/CC ウェブサイト

表２－２　2011 年下半期のセンサによるインシデント報告件数

Event	Jun	Jul	Aug	Sep	Oct	Nov	Des
SQL probe response overflow attempt (1:2329)	21.868	1.112.492	856.809	713.389	661.043	648.750	759.139
SQL version overflow attempt (1:2050)	0	1.069.338	2.277.601	1.322.518	557.023	232.206	333.921
SQL heap-based overflow attempt (1:4989)	0	389.364	177.739	4.114.729	322.462	562.248	1.054.678
BOTNET-CNC Virut DNS request attempt (1:16304)	242.036	210.447	205.684	140.579	215.716	283.957	197.088
BOTNET-CNC Virut DNS request for C&C attempt (1:16302)	206.458	163.642	140.337	167.246	270.843	306.829	263.910
BOTNET-CNC Palevo bot DNS request for C&C attempt (1:16297)	66.421	47.187	27.227	16.932	23.470	23.525	24.139
BOTNET-CNC Palevo bot DNS request attempt (1:16298)	65.553	45.902	26.932	17.053	23.491	23.586	23.615
WEB-CLIENT Windows help file download request (1:17407)	25.408	16.750	16.545	16.105	13.973	11.047	2.797
SPYWARE-PUT Torpig bot sinkhole server DNS lookup attempt (1:16693)	20.409	14.093	9.876	6.931	3.352	642	638
WEB-MISC Microsoft ASP.NET information disclosure attempt (3:17429)	18.150	13.796	6.689	1.575	2.403	5.819	7.499
Other	297.853	131.177	182.631	154.014	135.746	117.283	314.042
TOTAL	942.288	3.214.188	3.928.070	6.671.071	2.229.522	2.215.892	2.981.466

* 10 Most Active Events

出典：ID-SIRTII/CC ウェブサイト

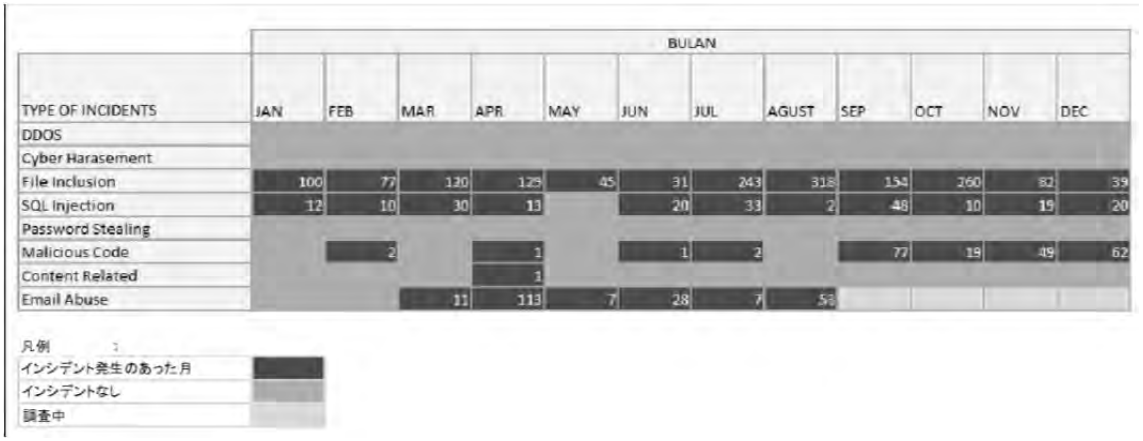
表２－３　2011 年のインシデント分類

Classification	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Misc Attack	9.265.750	4.412.183	1.751.258	1.161.333	1.407.615	154.060	406	2.081	1.539	6.984	10.808	4.770
Attempted Administrator Privilege Gain	4.653.292	2.549.203	1.161.362	416.932	402.630	40.867	1.463.948	2.461.394	5.127.160	884.703	800.065	1.402.242
Attempted User Privilege Gain	287.568	215.619	257.479	96.806	31.501	68.107	1.135.140	892.301	732.629	683.432	667.075	769.397
Attempted Denial of Service	118.416	154.191	106.304	42.294	140	29.588	19.351	24.342	26.192	38.960	16.079	20.893
Misc Activity	68.331	50.031	62.414	32.951	39.218	105.934	91.734	56.537	37.710	40.912	44.256	120.638
A Network Trojan was Detected	47.333	32.968	35.562	24.906	40.089	559.356	464.261	434.749	352.842	540.480	624.202	507.928
Generic Protocol Command Decode	11.631	8.263	5.625	716	557	281	0	58	11	1.480	1.673	305
Web Application Attack	3.839	64	409	397	814	258	3.633	2.774	1.845	2.449	1.911	6.633
Potentially Bad Traffic	3.530	73.150	97.307	9.285	6.896	37	2.289	1.380	1.514	1.314	131	1.004
Detection of a Denial of Service Attack	642	546	303	0	0	0	0	0	1	0	81	0
TOTAL	14.460.341	7.496.218	3.478.023	1.785.620	1.929.460	958.488	3.180.762	3.875.616	6.281.443	2.200.714	2.166.281	2.833.810

* 10 Active Events Classification

出典：ID-SIRTII/CC ウェブサイト

表２－４　2011 年のインシデント発生件数



出典：ID-SIRTII/CC ウェブサイト

２－４　情報セキュリティ戦略、政策、施策

インドネシアでは、情報セキュリティに関する戦略や政策、施策としてサイバー演習やネットワークトラフィックの監視が行われている。サイバー演習は過去に 3 回実施しており、政府機関、通信事業者が参加し実施している。ネットワーク上のトラフィック監視においては ID-SIRTII/CC が通信事業者と連携し、センサを設置して IP アドレス、ポート番号、タイムスタンプ等の情報を収集している。

表２－４　主な情報セキュリティ政策

政　策	発表年	担　当	概　要
National Cyber Exercise	2009 年	MCIT ID-SIRTII/CC	2009 年より政府組織と通信分野の事業者が参加し、サイバー演習を実施している。2012 年 2 月時点でガス、水道、電力などの重要インフラ事業者は参加していない。
トラフィック監視	2006 年	ID-SIRTII/CC	ID-SIRTII/CC のマルウェアラボでは APJII や ISP などと連携し、ネットワーク上にセンサを設置し情報を収集している。収集の目的はインターネット上の不正行為によって発生する攻撃トラフィックを監視し、早期警戒情報を出すことで重要インフラ（銀行、金融、交通機関、電

			力、行政）を接続する国内のインターネットを守ることにある。具体的には、この取り組みではパケットに含まれる IP アドレス（発信元、宛先）、ポート番号、タイムスタンプの収集を行っている。

出典：ASEAN 諸国における情報 セキュリティ情報収集・確認調査報告書

・National Information Security Index for Government Institutions（政府機関の情報セキュリティ指数）

MCIT は、インドネシアの中央省庁及び地方政府のセキュリティ対応レベルを、ISO/IEC 27001 シリーズ（情報セキュリティ規格群）に基づき指数化している（National Information Security Index for Government Institutions（政府機関の情報セキュリティ指数で、インドネシア語では、「Index KAMI」と称される）。2011 年度は、中央政府 21 機関について実施し、2012 年度は、地方政府にも適用し 62 機関に実施された。今後、国営企業や民間企業にも適用する意向である。評価項目は、リスク管理、技術、フレームワークなどの観点で、主なセキュリティ事項に関する準備状況、成熟度を 4 レベルで評価している。

ISO/IEC 27001 シリーズの導入に関しては、Ministry Recommendation として、官民の全組織に対し、Index KAMI もしくは ISMS のような Management System を導入するよう推奨している。

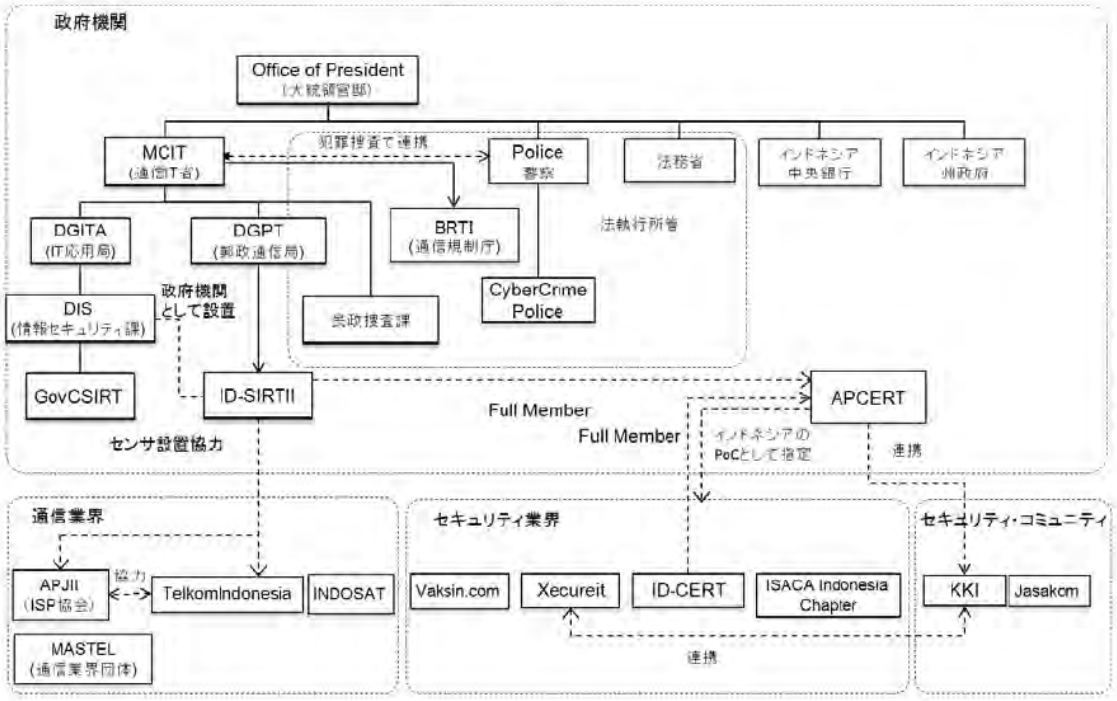
・電子式身分証明書（e-KTP）

現在の身分証明書を IC チップ化し、国民の身分証明書を全国共通化する取り組みである。自動車免許、選挙、徴税など、一元的に管理するものである。2010 年度から推進を開始しているが、まだ、あまり普及していない。国民全体に普及するにはまだしばらく期間を要する見通しである。

２－５　情報セキュリティ担当省庁、企業、組織

２－５－１　全体像

インドネシアにおける情報セキュリティ担当省庁、企業、組織の俯瞰図は以下のとおりである。インドネシアは大統領制の下で中央政府及び地方政府（州政府等）による行政構造をもち、大統領が任命する閣僚のうち MCIT（図２－２中では「通信 IT 省」）を中心として、法務省、警察等が情報セキュリティに関わる取り組みを進めている。中央政府各省庁の情報セキュリティ対策レベルは、MCIT・情報セキュリティ局が ISMS のサブセットとして開発した Index KAMI を用いて計測されており、地方政府への適用の検討も進められている。



出典：ASEAN 諸国における情報セキュリティ情報収集・確認調査報告書

図２－２　インドネシアの主な情報セキュリティ関連組織の関係

主な組織の概要は以下のとおりである。

分類	組織名称	主な活動（役割、人員、予算規模）
政府組織	Kementerian Komunikasi dan Informatika〔情報通信省（MCIT）〕	インドネシアの情報通信分野の政策策定と実施を行う政府機関。郵便・電気通信・放送の垣根を越えて、周波数等の希少資源の配分と技術規格の策定等を行う郵電資源・機器総局（Direktrat Jenderal Sumber Daya dan Perangkat Pos dan Informatika）、事業者の規制監督等を行う郵電管理総局（Direktorat Jenderal Penyelenggaraan Pos dan Informatika）、電子政府、アプリケーション等を所掌する情報通信アプリケーション総局（Direktorat Jenderal Aplikasi Informatika、英語名は Directorate General of Information Applications）、メディア等を所掌する公共情報通信総局（Direktorat Jenderal Informasi dan Komunikasi Publik）等から同省は構成されている。情報セキュリティを管轄するのは情報通信アプリケーション総局であり、その下に位置する情報セキュリティ局（Direktorat Keaman Informasi、英語名は Directorate of Information Security）が実施部局である。2005 年に ICT に関する所管省庁が MCIT に一元化されている。

政府組織	Dewan Teknologi Informasi dan Komunikasi Nasional（The Indonesian National ICT Council）	大統領令 No.20/2006 により設立された委員会であり、ICT の全般的な政策、戦略を策定する。ICT 推進における政府機関、産業、専門コミュニティ等関係部門の国内調整を行う委員会。大統領が議長を務め、情報通信大臣と他の大臣 9 人から構成される。
政府に準じる組織	ID-SIRTII/CC	2006 年に設立されたインドネシアの国際連携 CSIRT（Computer Security Incident Response Team ; コンピュータセキュリティインシデント対応チーム）で、情報通信省郵電管理総局通信局（Directorate of Telecommunication）の所管下にある独立した民間団体である。APCERT、CSIRT の国際的なフォーラム（FIRST）、イスラム諸国会議機構（OIC-CERT）に加盟している。次のような活動を行っている。 ・セキュリティマネジメントに関わる当事者への教育 ・トラフィックの監視、インシデントの検出、ISP 等の関連組織への早期警戒情報の配信 ・法執行機関に対するサポートを目的としたログファイルの収集、整理、保存及び管理 ・インターネットセキュリティに関する相談受付及びインシデント対応 ・シミュレーションラボ及びトレーニングセンターの設立 ・技術的アドバイスやコンサルティング ・国際連携活動の実施 設立にあたっては MCIT 郵電管理総局、インドネシア警察、法務省、インドネシア中央銀行、APJII（インドネシアの ISP 団体）、Asosiasi Warung Internet Indonesia（インターネットカフェに関する団体）、インドネシア・クレジットカード協会、MASTEL（通信関連の企業団体）が協力した。インドネシア国内のネットワークに監視用センサを設置し、トラフィック監視を行うとともに、JP-CERT の行っているインターネット定点観測プロジェクト TSUBAME に参加している。
研究機関	ID-CERT	1998 年に設立されたインドネシアのインシデント・ハンドリングを行っている機関である。代表者は Budi Rahardjo 博士と Andika Triwidada 氏であり、アジア太平洋地域の CSIRT による国際フォーラム APCERT の設立メンバーのひとつである。ID-SIRTII/CC が国の機関であるのに対して、ID-CERT はインドネシア国内の個人のボランティアによって成立している組織である。主な活動としては、インシデント・ハンドリングに加え、インシデントの統計情報の提供、フィッシングサイトやスパムメール等のインターネットの不正利用に関する調査、他の CSIRT とのコーディネーションなどを行っている。2011 年に寄せられたインシデント件数は約 100 万件であり、

		これらの情報を整理している。2010 年以降、ID-CERT の Ahmad Alkazimy 氏が情報通信省、PANDI（インドネシアの「.id」ドメイン管理を行う団体）と協力し、インターネットの不正利用に関する調査を行っている。2010 年はインドネシア国内の 3 つの通信事業者、2 つの NAP、6 つの ISP の協力の下に調査を行い、2011 年は 3 つの政府機関、PANDI、ニュースポータルサイト DETIK.NET、5 つの通信事業者、6 つの NAP、25 の ISP 等から情報提供を受けて調査を行っている。 その他の活動として、マルウェアに関する統計を作成しておりハニーポットなどを用いた実験を行っている。
研究機関	Indonesia Academic Computer Security Incident Response Team（ACAD-CSIRT）	インドネシア学術 CSIRT（ACAD-CSIRT）は、2011 年 4 月に設立された国公立大学、私立大学などの 40 校から構成される CSIRT である。代表者は IGN Mantra （ABFII-CSIRT）であり、ID-SIRTII/CC が設立に関与している。
民間団体	APJII	1996 年に設立された ISP の団体であり、インドネシアにおける ISP の接続料金を定めている。同国内の ID-SIRTII/CC が行っているセンサ設置などの協力を行っている。
民間団体	Information Security Professional Network（ISPN）	インドネシアのセキュリティ企業 XecureIT の人材研修部門が中心となってつくられた、インドネシアの最高情報責任者（CIO）、最高情報セキュリティ責任者（CISO）、IT 部門責任者、情報セキュリティコンサルタント、セキュリティ管理者、セキュリティ関係技術者、セキュリティ監査人向けの情報セキュリティコミュニティであり、年に数回の情報交換を行っている。コミュニティへの参加にはメンバーの承認が必要であり、閉じたコミュニティの中で情報交換が行われている。2012 年 12 月時点で LinkedIn コミュニティには 757 名が参加。
民間団体	ICT-Watch	ICT、情報セキュリティ分野の研修教育なども行っている非政府組織（NGO）である。研修は、MCIT、ID-SIRTII/CC が支援している。

２－５－２　情報通信省情報セキュリティ局

情報通信省情報通信アプリケーション総局情報セキュリティ局（Directorate of Information Security）は以下のとおり 5 つの課から構成される。（所属スタッフ数は 2013 年 7 月時点）

課	役　割
Information Security Governance	セキュリティマネジメントなどを扱っており、ISO/IEC 27001 シリーズ等の国際標準に整合したポリシー（Index KAMI）など情報セキュリティに係る方針やガイドの作成と普及を担当。所属スタッフ 6 名。

Information Security Technology	政府認証局（CA）の構築を行っている。ハニーポットなどに係る政策も検討している。所属スタッフ 5 名。
Monitoring Evaluation and Incident Response	Gov-CSIRT は、この部署を指す通称である。インシデント監視に係る政策を担当し、かつ、政府組織のインシデント監視と対応を行っている。（他方、ID-SIRTII/CC はインフラに専念している。）技術指導書の作成のほか、アプリケーションも担当している。所属スタッフ 5 名。
Forensics and Low Enforcement	デジタル鑑識を担当。サイバー上のインシデント解決に関し、警察と同等の権限をもつ。所属スタッフ 12 名。
Information Security and Culture	情報セキュリティに関する啓発活動を担当。所属スタッフ 5 名。

Gov-CSIRT と ID-SIRTII/CC との違いは、ID-SIRTII/CC が、インフラに焦点を当てていることや、TSUBAME やマタガルーダといった IP トラフィックの観測センサをもっている点である。方向性としては、ID-SIRTII/CC が National CERT として国全体をカバーし、Gov-CSIRT が政府機関（中央と地方を含め約 560 部局）のインシデント・ハンドリングの一次受けとなることを志向しているが、Gov-CSIRT の活動は活発ではない。

２－５－３　ID-SIRTII/CC

ID-SIRTII/CC の会長、副会長等のボードメンバーは、MCIT 大臣が設置する委員会によって選定される。委員会の構成員は、MCIT、警察、インドネシアのインターネットコミュニティ関係者、専門家、大学等の学術機関等から構成される。選定のプロセスは以下のとおりである。

（1）ボードメンバー職の募集アナウンス（4 カ月前）
（2）候補者の受け付けと行政機関による評価
（3）筆記審査、健康診査、面接審査
（4）委員会審査結果を推薦として情報通信大臣に通知
（5）MCIT 大臣による任命

組織としては、以下の部署から構成される 40 名の職員により運営されている。事務局とトップ 2 以外はすべて任期が決定しており契約ベースである。副会長以上は 3 年任期、それ以下（スタッフレベル）は単年度契約である。法律で 2 年以上契約スタッフを雇用すると正規職員として雇用する義務があるが、法で定められた組織規程上、正規職員を増やすことは不可能なためこのような運営になっているが、上位ポジションの採用募集に応募するなど別契約として継続して雇用されるスタッフが多く、スタッフの平均勤続期間は 5 年程度と推測される。

・研究開発部
・データセンター&アプリケーション部
・運用管理部
・国際連携部
・社会化・広報部

多くの職員は、研究開発部に所属している。 インドネシアにおける主な CSIRT のインシデント情報源については、大きくネットワーク観測センサと被害レポートに分けられる。ID-SIRTII/CC は観測センサやハニーポットによる情報収集を行っている。特に、MCIT 大臣令 No.26 により、通信キャリアはトラフィック情報を ID-SIRTII/CC に提供するよう義務づけられている。一方、被害レポートについては、ID-SIRTII/CC、ID-CERT、Gov-CSIRT、Academic-CERT などが受け付けを行っており、インシデントの情報源としている。MCIT と ID-SIRTII/CC は、すべてのセクター及び各地方政府に CSIRT 設置の推進を行っている。ID-SIRTII/CC は、それらの CERT コーディネーションセンター（CC）の役割を果たすことが期待されている。

また、ID-SIRTII/CC は官民組織の CSIRT 設立支援のための技術研修を行っており、次のようなトレーニングモジュールをもっている。

A. Security
   - Cyber – 6 Introduction
   - Hacker Techniques and Exploits
   - Incident Handling and Intrusion
   - Network Pen Testing
   - Web App Pen Testing
   - Wireless Pen Testing
   - Securing Windows and Linux

B. Forensic
   - Windows Forensic
   - Network Forensic
   - Mobile Device Forensic
   - Linux Forensic

C. Honeypot and Malware Analysis
   - Malware
   - Honeypot

D. Application
   - Secure Coding in PHP
   - Secure Database in MySQL
   - Secure Coding in Java

E. Management
   - Creating & Managing CSIRT
   - Introducing of Security Professional Certification
   - IT Security Project Management

２－６　情報セキュリティ教育

初等、中等課程における教育カリキュラムには IT 系の科目は含まれておらず、高等教育以前での IT 教育はなされていない。遠隔教育システムの中学校や高等学校への導入が進められているが、IT 教育に特化した使い方はされていない。

高等教育での ICT 教育は高等専門学校、大学において中心的に教育が行われている。これらの

機関では資格取得のためのカリキュラムが大学の授業に組み込まれている。インドネシアの主要な大学（インドネシア大学、グナダルマ大学、ビナ・ヌサンタラ大学、バンドン工科大学等）には外国政府の援助による IT 人材育成プロジェクトや、企業による IT センターの設置などの提携が進んでいる。日本の協力としては、無償資金協力で設立されたスラバヤ電子工学ポリテクニックに対して、JICA の技術協力「スラバヤ電子工学ポリテクニック」（1987～1994 年）、「電気系ポリテクニック教員養成計画プロジェクト」（1999～2006 年）が実施された。

その他、国民全体の ICT 教育として PC 操作などの指導を行う労働・移民省管轄の職業訓練校や民間の研修機関が存在する。これらの民間研修機関ではマイクロソフト、シスコシステムズ、オラクル等の企業認定資格の取得を目的としている。

情報セキュリティに関しては、The SANS Institute などに依頼して国際証明書研究プログラム（International Certificate Training Program）においてデジタル鑑識などに関するセミナーを 2013 年にバリ島などで行っている。ただし、SANS のセミナー費用が高いことが課題となっている。インドネシアでも、CISSP（Certified Information Systems Security Professional）資格認定はある程度認知されている。MCIT の情報セキュリティ局がインドネシア語で研修を行った。参加者は、政府、大学から 20 人程度。インドネシアで資格を取得しているのは 70 人程度と考えられる。まだ、有資格者は少ないため、MCIT では、地方でも研修が行えるようなシステムを構築したいと考えている。また、MCIT ではシステム可用性の高度化、ショートメッセージサービス（SMS）に関する教材（インドネシア語）などを作成し、研修に用いている。

インドネシア政府は、情報セキュリティ分野の人材資格証明制度（Certification for Human Resource in the field of Information Security）を行っている。ID-SIRTII/CC と MCIT は、ICT-watch を含む多くの NGO を支援し教育を行っている。2012 年 6 月には MCIT、ID-SIRTII/CC 共催で、バンドンにおいて CSIRT 立ち上げ支援ワークショップを開催した。また、2012 年度に、CA の電子署名、ベストプラクティス、サイバー公証人（Cyber Notary）などに関するワークショップを実施し、大学、地方政府などから 40 人が参加した。

韓国国際協力団（KOICA）の支援で設立された MCIT 管轄下の国立 ICT 人材育成センター（National Information and Communication Technology-Human Resourced Development：NICT-HRD）では、5,000 人/年程度の訓練を行っており、その 9 割が政府職員、残りは一般民間人（周辺の市民や小学校から大学までの学生）となっている。費用はすべて政府負担で無料である。トレーニング内容は基礎的なものから、CISSP のような高度なものまで各種取り揃えているが、センターの教員では扱えない高度な研修は、外部民間企業に委託して実施している。

２－７　電子商取引の普及状況

航空券、ホテル等のチケッティング利用は一般的になっている。また、Amazon など欧米系の利用は多い。日本からは楽天が進出し、楽天に出店するインドネシア企業も多いがまだ知名度は高くない。 インターネット・バンキングの利用はまだ少ないとみられる。

２－８　民間の動向、ニーズ

インドネシアでは金融機関を対象としたインシデントが多く、オンラインバンキング・サイトで利用される ID とパスワードを盗み取る目的の攻撃が多いとの声がヒアリング先民間企業から聞かれた。具体的にはブラジル、米国の銀行のサイトのフィッシングサイトがインドネシア内に

つくられているとの報告が通信事業者からなされている。この事例では、インドネシア国外の事業者から ID-CERT に通報が行われ、ID-CERT から関係する ISP にウェブサイトの閉鎖要請が行われた。また、ID-SIRTII/CC によれば 2011 年における金融機関に対する攻撃は 11,000 件以上にのぼっている。これを受けて金融機関は積極的に情報セキュリティ対策を行っており、情報セキュリティに関する監査も行われている。情報セキュリティ監査に関する団体 ISACA Indonesia Chapter では年に数回、会員向けのセミナーを開催しており、参加者は金融機関関係者が多数を占めている。

政府（中央銀行）の規制により、金融機関は、メインサイトから 30km 以上離れた場所にデータセンターやオフィスなどの BCP（事業継続計画）サイトを構築することが義務化された。また、前述のとおり、情報通信省は Ministry Recommendation として、官民の全組織に対し、Index KAMI もしくは ISMS のような Management System を導入するよう働きかけている。

２－９　情報セキュリティ分野における他国・ドナーとの連携・支援

MCIT は韓国電子通信研究所と 2011 年度に覚書（MOU）を締結し、2012 年度にセキュリティ促進デーや国際セミナーなどの、ステークホルダーに対する啓発イベントを実施した。また、KOICA の支援で MCIT の IT トレーニングセンター（BPPTIK Ciputat）が設立されている。他国政府からの情報セキュリティに関する資金的な支援は受けていない。情報セキュリティに関する政府間の機材提供の支援は、日本の nicter の観測センサが MCIT のデータセンターに設置されている程度で、他国からの提供は受けていない。シンガポールとは情報セキュリティに関する MOU を結んでいる。ID-SIRTII/CC は、イスラム圏の CSIRT 連携組織 OIC-CERT のメンバーであり、連携を行っている。また、日本、中国、マレーシア、韓国と研修支援などに関する MOU を締結している。ID-SIRTII/CC は JP-CERT/CC が実施している TSUBAME プロジェクトメンバーであり、日本をはじめとする他国との情報共有を行っている。また、2011 年より総務省の国際サイバープロジェクト（現在の PRACTICE プロジェクト）の一環として、インシデント等の観測センサの設置に関する協力（サイバー攻撃観測データ共有プロジェクト）を進めている。

２－10　情報セキュリティに関する課題・対策

２－10－１　法制度・規制

インドネシアにおけるサイバーセキュリティに関する法制度は、通信法と情報電子取引法が重要であり、政省令等の策定も進められている。電子署名、個人情報保護は、情報電子取引法の一部として規定されている。 インドネシアにおける情報セキュリティに関する法制度や規制は以下のとおり。

分　類	法制度・規制	年	概　要
通信	Act No.36/1999 regarding National Telecommunication Industry （国家通信産業法）	1999	1999 年 9 月に成立し、2000 年 9 月より施行されたインドネシアにおける電気通信の基本法である。同法により、電気通信事業が電気通信網事業（設備を設置運用してサービスを提供する）、電気通信サービス事業（設備を借用して

			サービスを提供する)、特別電気通信事業（公共業務や国防・治安維持のために、放送等を含む電気通信サービスを提供）の 3 つに区分された（第 7 条)。
通信	Ministry of Communication and Information Technology Regulation No.27/PER/M. KOMINFO/9/2006	2006	インドネシア国内の IP ベースネットワークのセキュリティに関する情報通信省の省令である。この中で、ID-SIRTII/CC が行うネットワーク観測に関して、センサで取得する情報（ソース・デスティネーション IP アドレス、ポート番号、タイムスタンプ）も規定されている。
電子商取引	Draft Government Regulation, Electronic System Provider and Electronic Transaction.	2012 年現在草案	CA の信頼性確保、電子署名、電子代理人、電子証明書、取引サービス・プロバイダー、電子政府、リスク管理、スパム・ドメイン・ネームなどに関する規定が検討されている。
通信	Ministerial Regulation No.26/PER/M. KOMINFO/2007 regarding Indonesian Security Incident Response Team on Internet Infrastructure	2007	ID-SIRTII/CC 設置に関して規定している MCIT の省令。ID-SIRTII/CC の所管する業務や権限、組織構成、トラフィックモニタリングに関して定められている。
電子署名、個人情報保護	Information and Electronic Transaction Law No.11 of 2008 No. 11/2008 Article 31 （情報電子取引法）	2008	電子商取引・契約、認証、電子署名、ドメイン名管理から個人情報保護やサイバー犯罪規制までを包含する法である。情報電子取引法は、立法から 4 年経過しており、具体的な政策推進の必要性から政令案 Regulation, Electronic System Provider and Electronic Transaction.を策定している。

２－10－２　政府

全世界的なサイバー攻撃の増加に伴い、情報セキュリティを所管する省庁や企業で、情報セキュリティに対する意識が高まりつつある。しかしながら、情報セキュリティ対策は利益を生むものではないため、対策を実施するための予算は獲得しづらい状況にある。

また、情報セキュリティに関する法律は 2005 年から国会において議論が開始され、2008 年に成立し、2010 年に施行された情報電子取引法である。インドネシアにおけるサイバー法であり、サイバー犯罪、電子認証や契約、個人情報保護について規定されている。本法律は、秘密情報や保護すべき情報の定義不足などから改正を検討中である。

MCIT では、情報セキュリティの人材育成を最大の課題として挙げている。政府内の若手、地方政府職員を育成していくかが問題である。

MCIT としては、Index KAMI を地方政府にも普及させること及び省庁に審査結果を通知することで、意識啓発を促したいと考えている。

２－10－３　組織（政府系機関、民間企業など）

MCIT では、電気通信業界、エネルギー業界、運輸制御業界など重要インフラ事業者のセキュリティ対策に焦点を当てている。MCIT は、Index KAMI を、政府組織から重要インフラ事業者にも拡大して適用する方針である。また、その他の民間事業者に対しても、省令により、ISO/IEC27001 シリーズの取得を推奨している。インドネシアでは情報セキュリティをはじめとする IT スキル人材が不足しており、技術対策を行ったとしても運用人材の面で十分に対応できていない。インドネシアでは海外向けの光ファイバーの容量に余裕がなく、トラフィックを監視した際のデータ共有を行うための方法が課題となる。また、国内インフラについても、十分に整備されているとはいえず、インターネットはモバイル通信網を中心とした普及が進んでいる。企業からは、電子マネーの推進も重要ととらえられているが、ルールなどの整備が進んでいない点などが課題として挙げられている。

２－10－４　国民（一般ユーザ）

インドネシアでは SNS を騙ったフィッシングサイトによる被害が出ている。有名人のアダルト動画を掲載しているとした Facebook アプリケーションを紹介し、Facebook の Web サイト上のアプリケーションに偽装したフィッシングサイトに誘導することで、ID/パスワードを抜き取る手法が DETIK.NET によって報じられている。抜き取られた ID/パスワードは、攻撃者がこれらを用いてログインした後に知人に「財布を落としたのでお金を貸してほしい」といった内容のメッセージを送信するなどして、金銭を騙し取るために利用される。インドネシアでは違法コピーのソフトウェアが多く利用されており、セキュリティパッチを適用できない場合がある（ID-SIRTII/CC によれば、海賊版 OS に、セキュリティパッチを当てる違法サーバーも存在するとのこと）。また、通信環境の悪さなどによりアップデートが適切に行われていないことから、マルウェアに感染しやすい環境にある。市中のマーケットには通信環境が悪いことからオープンソース・ソフトウェアを CD で販売する店舗が存在し、違法コピー製品もこれらの製品と同様に販売されている。

国民の違法コピーの撲滅については、オープンソースの推進も有効と MCIT は考えている。オープンソースの普及は敷居が高いが、一定の普及が進めば、不正ソフトの問題解決の一助となる。

２－11　情報セキュリティに関するニーズ及び課題

政府、民間組織、国民等からのニーズの優先度の高いものを整理すると以下のようになる。

- 中央政府の若手官僚、地方政府のセキュリティ人材の育成 今後セキュリティ政策を担う若手官僚、地方政府の人材を育成することにより、セキュリティ政策推進の原動力とする。特に、州政府に対して Index KAMI の普及促進を行う場合、一定数の専門家を必要とするため、そのような専門家人材の育成が課題である。
- Index KAMI を、中央政府から、地方政府、重要インフラ事業者に拡大し、現状の把握と当事者の意識啓発を促す。

第３章　支援事業（プロジェクト）の基本方針

３－１　プロジェクトの目標

「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の向上」を目標とする。

クラッキングやウィルス等のインターネット上の脅威が日々増大するなか、インドネシア情報通信省（MCIT）情報通信アプリケーション総局情報セキュリティ局は、中央及び地方政府の各部局における安全な IT 利用を推進する責務を負っている。しかしながら、多くの政府部局は、いまだ適切な情報セキュリティ対策を実施できていない。情報セキュリティ局の能力向上が、各政府機関のセキュリティ対策強化に直結すると考えられることから、本プロジェクトでは上述の目標を掲げ、さらに、

・情報セキュリティ局の機能強化
・政府の各部局における安全な IT 利用をサポートする仕組みの確立
・情報セキュリティ啓発活動の改善

を成果の柱として、目標の達成をめざす。

加えて、本プロジェクトでは、可能な範囲で他の ASEAN 諸国との連携を図ることとする。これは、

・国境をまたいで発生するインシデントに対抗するには、多国間の協力体制構築が必須であること
・各国で必要とされる情報セキュリティ対策技術や管理体制には共通点が多いこと
・日・ASEAN 友好協力 40 周年記念事業として、サイバーセキュリティ分野での協力推進を閣僚級で合意する予定であること（2013 年 9 月）

といった点を考慮のうえ、プロジェクトに取り入れられた活動である。

３－２　プロジェクトの対象範囲、対象者

情報セキュリティ局（Directorate of Information Security）所属のスタッフを主要なカウンターパート（C/P）とする。プロジェクト実施体制は図３－１のとおり。

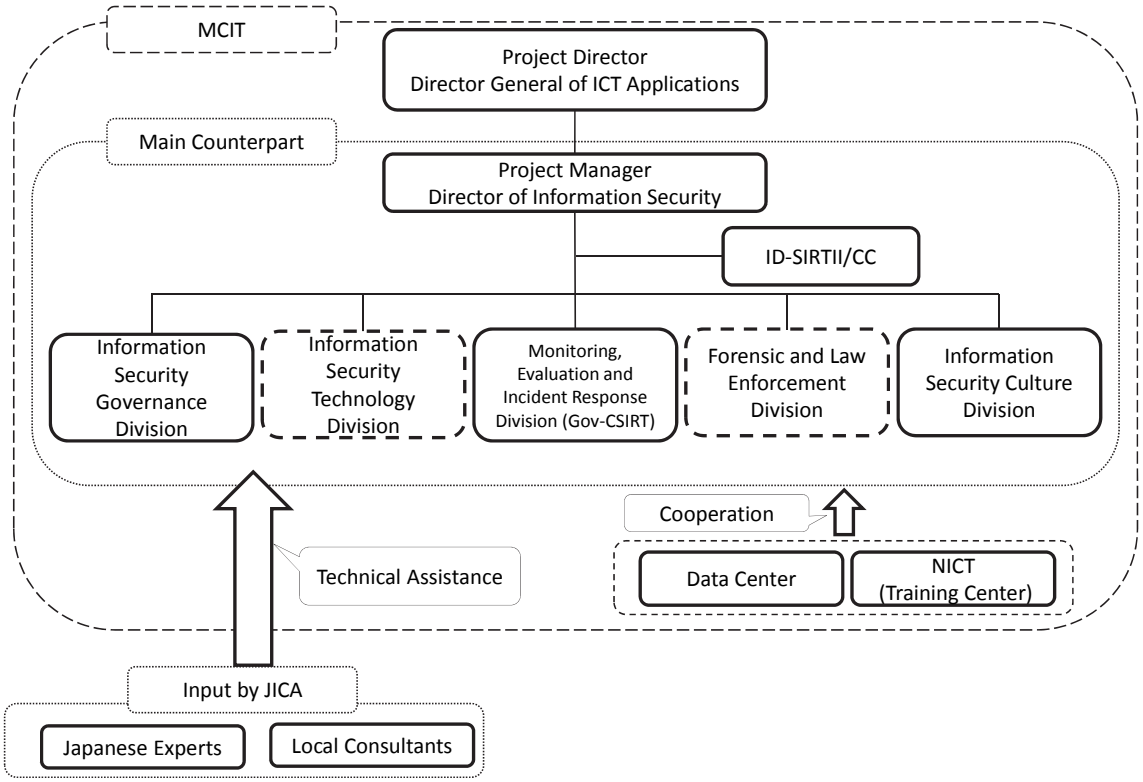


図３－１　プロジェクト実施体制

ID-SIRTII/CC は、インドネシア政府の予算的措置のうえでは MCIT 郵電管理総局通信局に所属しているが、実際は情報セキュリティ局と密に連携しながら業務を遂行していることから、本プロジェクトでは、直接の C/P として扱う。National CERT の役割を果たしている ID-SIRTII/CC のスタッフの IT スキルが比較的高いので、中・上級レベルの技術移転（例：データマイニング、マルウェア解析）は、ここのスタッフの要望を基に計画する。

一方、以下に挙げる 3 つの課については、政府機関の安全な IT 利用を促進する役目を担っているが、スタッフの IT スキルはそれほど高くないため、初級・中級レベルの技術移転〔例：Cisco CCNA、CCNA Security、ISMS（情報セキュリティマネジメントシステム)〕は、これらの課に所属するスタッフの要望を基に計画する。

・Information Security Governance Division
・Monitoring, Evaluation and Incident Response Division
・Information Security, Culture Division

また、以下に挙げる 2 つの課については、インフラ整備や特殊な分野であるため、これらの課を直接のターゲットとした技術移転は行わない。ただし、上述の技術移転のなかで、これら 2 つの課に所属するスタッフの能力向上に資するものがあれば、積極的に参加するよう働きかけるものとする。

・Information Security Technology Division
・Forensic and Law Enforcement Division

３－３　活動項目

３－３－１　情報セキュリティ局の機能強化

情報セキュリティ局は歴史が浅いため、C/P は組織構成の見直しや、要員スキルの改善の必要性を感じている。このため、プロジェクトでは以下の活動を行う。

①　情報セキュリティ局の組織構成と要員スキルの再設計

情報セキュリティ局の理想的な組織構成案と、各組織の要員に必要となるスキルを定義する。具体的な活動としては、日本及び先進 ASEAN 諸国の同等組織の構成や要員スキルを知る視察・研修を実施したうえ、C/P とともに理想的な組織構成案をつくり上げていく。

②　要員の技術スキル向上

「３－２　プロジェクトの対象範囲、対象者」で述べたような技術移転や研修を企画・実施する。インドネシアでは、民間ベースで要素技術（例：ネットワーク基礎、プログラミング基礎）を教えられる機関が複数存在するため、技術移転や研修の企画にあたっては、原則として現地リソースを最大限活用し、現地人材では実施が難しい高度な技術移転（例：データマイニング、マルウェア解析）についてのみ、本邦及び第三国のリソースを活用する方針とする。

なお、他の ASEAN 諸国、特に National CERT 設立間もないカンボジア、ラオス、ミャンマー（CLM）の CERT スタッフにも有益な技術移転や研修がインドネシアで実施可能な場合には、これらの国々を対象としたものも企画・実施することとする。また、多国間で行うインシデント・ハンドリング演習も、同様の考え方で実施を検討する。

③　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づくり

情報処理分野の技術革新のスピードは早く、加えて新たな種類のサイバー上の脅威も次々と出現するため、情報セキュリティ対策のトレンドに追いつくことは容易ではない。日本を含めた先進各国でも、試行錯誤しながら対応している分野も多い。そこで、C/P が興味をもっているトピックに対し、本邦や先進 ASEAN 諸国への視察等を企画し、他国の事例を参照できる環境を整える。調査時点では、具体的なトピックとして次のようなものが挙がっているが、プロジェクト実施中に C/P の希望や情報セキュリティ分野のトレンドを考慮してトピックを選択することとする。

・重要インフラ向け情報セキュリティ対策
・重大インシデント発生時の官民関連機関の連携方法
・政府組織のデータセンター設置基準

なお、この活動に関しては、他の ASEAN 諸国の関心が高く、かつ日本で実施することが適当と思われるトピックに関しては、プロジェクトではなく、課題別研修で扱うことも視野に入れる。同様の視点で、沖縄で ASEAN を対象とした情報セキュリティ関連の国際会議をプロジェクト後半に開催することも検討する。

３－３－２　政府機関の安全な IT 利用を促進する仕組みの確立

情報セキュリティ局は、各政府組織の情報セキュリティ対策能力向上のために、ISMS の普及、及び、各組織での CSIRT 設置を促進するという方針をもっている。このため、プロジェクトでは以下の活動を行う。

① Index KAMI 導入支援体制の構築

ISO/IEK 27001 シリーズで定義されている ISMS は網羅的ではあるが、完全な実施にはコストがかかるため、情報セキュリティ局では Index KAMI と呼ばれる独自の簡易版 ISMS を開発・運用している。しかしながら、この Index KAMI は、継続的なセキュリティ改善活動が省かれているなど、C/P 自身が問題視している部分が残っている。そこで、まず Index KAMI の評価と改善に着手する。Index KAMI は ISO 27001 をベースにするという方針で開発されたため、同方針は堅持しつつ、インドネシア政府機関で実施可能で、継続的改善をモニターできる指標などを追加していく。同時に、新 Index KAMI を各政府機関で運用する Index KAMI Internal/External Assessor の教育コースの開発を行う。この Assessor は、自分の所属組織に対しては Index KAMI 導入支援コンサルタント（Internal Assessor）としての役割を果たし、かつ、それ以外の組織に対しては評価者（External Assessor）としての役割を果たすものである。さらに、これら Index KAMI や教育コースの有用性を確認するため、パイロットサイトとなる政府機関を定め、その機関への Index KAMI 導入を行う。

② CSIRT 導入支援体制の構築

CSIRT はその所属組織内のセキュリティ対策を行う部署である。現在、国家レベルの CSIRT である ID-SIRTII/CC が各種トレーニングコースを開発し、官民の隔てなく各組織への CSIRT 構築支援をしているが、政府機関への CSIRT 普及は進んでいない。一方、ID-SIRTII/CC の業務量が多いため、政府機関への CSIRT 構築支援は情報セキュリティ局にある Gov-CSIRT も担っていく必要があると考えられる。そこで、プロジェクトでは、各政府機関で CSIRT マネジャーになる人材の育成コースを開発し、前述のパイロットサイトとなる政府機関に対し、人材育成及び CSIRT 構築支援を実施する。人材育成コースは、ID-SIRTII/CC がもつ既存の教育モジュールをベースに、取捨選択を行い、より低い技術レベルのトレーニングが必要と認められる場合は、その部分の開発も行う。

３－３－３　情報セキュリティ啓発活動の改善

Index KAMI の導入や CSIRT の設置は、各政府機関の情報セキュリティ対策機能の強化といえるが、組織内の情報セキュリティを守るには、これだけでは不十分で、組織内のスタッフおのおのの情報セキュリティに対する意識を高めることも同時に必要となる。そこでプロジェクトでは以下の活動を行う。

① 啓発対象者への普及方法の確立

日本や他の ASEAN 諸国が実施している普及方法を学び、それを基に、インドネシアに適した普及方法を構築する。主たる啓発対象者は政府機関スタッフ。さらに、構築した方法と、次に挙げる啓発用教材を用い、普及活動を試行する。対象は３－３－２項で述べたパイロットサイト、及び、可能な範囲でセミナー等を開催し、他の組織への普及活動も試みる。

② 啓発用教材の開発

日本の啓発用教材を精査し、インドネシアに適したものを選択のうえ、そのローカライズ及び翻訳を行う。

なお、この活動についても他の ASEAN 諸国の関心が高く、かつ日本で実施することが適当と思われるトピックに関しては、プロジェクトではなく課題別研修で扱うことを視野に入れる。

３－４　プロジェクト期間と要員構成

３－４－１　期　間

プロジェクト期間は最低限 2 年を想定している。概略スケジュールについては付属資料１. Minutes of Meeting の Annex II「Plan of Operation」を参照のこと。ただし、

- C/P である情報セキュリティ局は、JICA の技術協力プロジェクトの経験がないため、JICA とのプロジェクト実施方法を理解するまで、ある程度の時間が必要と考えられること
- 地方のパイロットサイトでの活動は、今の時点では対象者のスキルが不明なため、実施に想定外の時間がかかる可能性があること
- インドネシア政府側の規則で、派遣専門家が決まってから実際の派遣まで 4 カ月間を要すること
- 情報セキュリティ局スタッフの IT スキルレベルが現時点では正確に測れていないため、技術移転に予想以上の時間がかかる可能性があること
- C/P はすべて現職スタッフであり、技術移転は彼らの業務スケジュールと調整しつつ計画しなければならないこと

などの諸点を考慮し、安全をみて 2 年半のプロジェクトにすることが望ましい。

３－４－２　インドネシア側の要員構成

- プロジェクト・ディレクター：　情報通信アプリケーション総局長
- プロジェクト・マネジャー：　情報セキュリティ局長

その他の C/P は３－２節で述べたとおりである。

３－４－３　日本側の要員構成

以下のような要員が必要と予想される。また、必要に応じて、現地の IT コンサルタントを雇上し、技術移転や IT 知識が必要な業務（例 : 現地研修のアレンジやモニタリング）を実施する。

長期専門家	・チーフアドバイザー ・情報セキュリティ技術 ・業務調整員（IT 研修企画）
短期専門家 （公示または公募）	・ISMS ローカライズ（6MM） ・組織強化（4MM）
短期専門家 （省庁推薦）	・CERT 能力強化（経産省推薦。JP-CERT スタッフを想定。1 週間×4 回程度） ・情報セキュリティ啓蒙（経産省推薦。IPA スタッフを想定。1 週間×2 回程度） ・IP トラッフィクモニタリング/nicter 活用（総務省からの推薦　1 週間×2 回程度） ・情報セキュリティ対策のための政府組織構成（内閣府、もしくは経産省、総務省推薦。1 週間×1 回程度）

３－５　プロジェクト実施上の留意点

（１）パイロットサイトの選択

パイロットサイトへの情報セキュリティ対策導入は、プロジェクト目標の指標にもなり得るので、慎重な選択が求められる。特に、政府部内でも IT 利活用が進んでいる部署にするか、それとも平均的な部署を選ぶかは大きな問題である。どちらを選ぶかはプロジェクト専門家と C/P との間で決めることになるが、プロジェクト目標の指標とする場合は、パイロット開始前に、到達目標を明確に決めておくことが求められる。

（２）ASEAN 諸国からの研修員受入れ

本プロジェクトでは、ASEAN 諸国の研修員を受け入れ、インドネシアで研修を行う可能性が高いが、もともと二国間協力のプロジェクトである本件でこれを実現するには、JICA 内部の手続き方法を事前に明らかにしておくことが必須である。また、その過程で、旅費・日当、宿泊費の精算や招待状送付、宿泊施設アレンジといった多くの作業をプロジェクトでこなす必要があると判明した場合、プロジェクトから現地の旅行業者に業務を委託できるようにするなど、柔軟な対応ができるよう配慮する必要がある。

（３）東京センター課題別研修、及び沖縄センターとの国際会議合同開催

どちらも、本プロジェクトと連携しながら内容を詰める必要があるが、このような連携はあまり例がないため、どのような方法で三者の連携をとるのか、プロジェクト開始前に JICA 内で方針を確立する必要がある。

第４章　団長所感

本調査で面談できたのは非常に限られた人々であったが、インドネシアの IT 業界や IT エンジニアのスキル水準は、カンボジア、ラオスといった国々に比べると明らかに高いと感じた。このようなレベルに達しているインドネシアにおいて、情報セキュリティを扱う技プロを実施することは時宜に適っているという印象を受けた。

本件は、日本側、インドネシア側ともに関係者が多く、各組織からの要望が多岐にわたっているが、まずは実行可能なプロジェクト内容にまとめることができたと感じている。

しかしながら、本調査は、通常の技プロ詳細設計調査に比して期間が短く、情報セキリュティ関係諸機関、特に民間や地方政府の現状把握に十分な時間を割くことはできなかった。また、同じく時間的制約から、プロジェクト・マネジャーとなる情報セキュリティ局長との議論に時間をかけ、主にその結果を基にプロジェクト設計を行っている。実際の技術移転対象となる同局スタッフや ID-SIRTII/CC スタッフともプロジェクト内容について議論できれば理想的であったが、実際は彼らへのヒアリングのみで、議論をする機会をもつまでには至らなかった。このため、プロジェクト開始後、予期していなかった活動が必要となる可能性もあるため、実施にあたっては、通常の技プロ以上に、先方と活動内容についての認識合わせをする場を設けることが必須であると考える。

付　属　資　料

１．Minutes of Meeting

２．協議面談録

MINUTES OF MEETING
BETWEEN
THE REPUBLIC OF INDONESIA
AND
JAPAN INTERNATIONAL COOPERATION AGENCY
ON
JAPANESE TECHNICAL COOPERATION
FOR
PROJECT FOR STRENGTHENING INFORMATION SECURITY MEASURES

In response to the request submitted by the Government of the Republic of Indonesia (hereinafter referred to as "Indonesia"), Japan International Cooperation Agency (hereinafter referred to as "JICA") has dispatched the Detail Planning Survey Team (hereinafter referred to as "the Team") headed by Mr. Hiroyuki IDE (Senior Advisor, JICA HQ) from the 14th July to 23rd July, 2013 for the purpose of discussion on the technical cooperation project on "Project for Strengthening Information Security Measures" (hereinafter referred to as "the Project").

During its stay in Indonesia, the Team exchanged views and had a series of discussions for the purpose of working out the framework and contents of the Project with the authorities concerned of the Government of Indonesia.

As a result of the discussions, both sides agreed on the matters referred to in the documents attached hereto.

Jakarta, 23 July, 2013

Mr. Hiroyuki IDE
Team Leader
Senior Advisor,
Japan International Cooperation Agency (JICA)

Mr. Bambang Heru Tjahjono
Director of Information Security
Directorate General of ICT Applications
Ministry of Communication and Information Technology, Republic of Indonesia

THE ATTACHED DOCUMENT

I Outline of the Project

1. Framework of the Project

Both sides agreed, in principle, on the framework and implementation plan of the Project that is given as Draft Record of Discussions (R/D) (Annex I).

After going through the JICA's internal approval, the R/D will be formally signed by the Chief Representative of JICA Indonesia Office and the Representative of the Ministry of Communication and Information Technology, Government of Indonesia as the official document that defines the framework and implementation plan of the Project.

The PO (Plan of Operations) and the PDM (Project Design Matrix) will be used as management tools of the Project, which will be periodically reviewed and revised as necessity arises. The first Joint Coordination Committee (hereinafter referred to as "JCC") shall be convened within 6(six) months after the commencement of the Project to approve the first version of PDM and PO.

2. Project Title

Reflecting the design of the Project, it is suggested to change the title of the Project from "Project for Strengthening Information Security Measures" at the time of the request into "Project on Capacity Building for Information Security".

3. Term of the Cooperation

The duration of the Project was supposed to be two year at the time of the request. However, reflecting the design of the Project, Indonesia side requested to extend the Project duration to be two and half year. JICA will inform the decision regarding the Project duration thought tentatively the Project duration on the draft version of R/D (Annex I) is two years from the date of first dispatch of JICA expert to Indonesia. (From December 2013 to December 2015)

4. Responsible & Implementing Agency of the Project

Responsible Ministry: Ministry of Communication and Information Technology (hereinafter referred to as "MCIT")

Implementing Agencies: MCIT

MCIT shall be responsible for 1) the Project implementation activities, 2) coordination among related organizations, and 3) support for human resource development of staffs.

II Principles of the Project implementation

It was discussed and confirmed that the main objective of this project will be to improve the capacity on information security incidents and prevention and mitigation from cybercrimes in Indonesia. Nowadays, cyber security is no longer a matter of one country because there is no

boundary on the Internet. Therefore, the information security level should be secured through establishing the regional network for information sharing on cyber threats. In consideration of this aspect, the Project will involve the other ASEAN countries to establish such a regional foundation. For example, the Project activity is planning to include;

- ✓ involving the related authorities and personnel from ASEAN countries to several trainings,
- ✓ visiting ASEAN countries for the purpose of information sharing and study, and
- ✓ conducting conferences and seminars inviting related stakeholders from ASEAN countries.

Furthermore, the Project will collaborate with several projects which have been already commenced and implemented by MCIT and ID-SIRTII/CC in Indonesia together with the Ministry of Internal Affairs and Communications, the Ministry of Economy, Trade and Industry, and National Information Security Center, in Japan.

III Provisional Schedule

The following schedule is suggested for the preparation of the Project thought the commencement of the Project will be decided according to the request from MCIT.

(1) Signing of R/D: by the middle of August, 2013
(2) Commencement of the Project: December, 2013 or January, 2014

IV Other Issues Discussed

(1) Status of ID-SIRTII/CC in the Project
ID-SIRTII/CC will be treated as a subdivision under Information Security Department of MCIT in the Project though ID-SIRTII/CC is not under the Information Security Department according to the official structure of MCIT. It is because that ID-SIRTII/CC is one of the main functions for information security management in Indonesia.

(2) Cost sharing for the Project activities
Both sides agreed that the budget for the Project activities in Indonesia, such as per diem and travel allowance for domestic training for Counterpart, will be shared by MCIT and JICA.

(3) Cost for cooperation to ASEAN countries
Both sides agreed that the budget for involving related stakeholders from ASEAN countries will be covered by JICA. Indonesian side will cooperate with JICA to support the other ASEAN countries. JICA will bear the cost for such support. For example, when trainings/seminars/conferences for ASEAN countries are conducted in Indonesia, JICA will cover followings;

- per diem and travel allowance for participants from ASEAN countries
- rewards for lecturers even if the counterparts become lectures
- facilities and equipment even if the counterparts provide facilities and equipment
- other necessary cost

(4) Office space for Japanese experts

JICA explained to MCIT that MCIT is responsible for providing necessary office space for Japanese experts. MCIT understood it.

Annex I	Draft Record of Discussions (R/D)
Annex II	Draft Outline of the Project

Annex I

(Draft)

RECORD OF DISCUSSIONS

ON

PROJECT ON CAPACITY BUILDING FOR INFORMATION SECURITY

AGREED UPON BETWEEN

MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY,

AND

JAPAN INTERNATIONAL COOPERATION AGENCY

Jakarta, XX of August, 2013

Mr. Atsushi SASAKI Chief Representative Indonesia Office, Japan International Cooperation Agency	Dr. Ashwin Sasongko Director General of ICT Applications Ministry of Communication and Information Technology, Republic of Indonesia

With regard to the Project on Capacity Building for Information Security (hereinafter referred to as "the Project"), the Japan International Cooperation Agency (hereinafter referred to as "JICA") held a series of discussions with the Ministry of Communication and Information Technology, Republic of Indonesia (hereinafter referred to as "MCIT") and relevant organizations to develop a detailed plan of the Project.

JICA and MCIT (hereinafter referred to as "both parties") agreed the details of the Project and the main points discussed as described in the Appendix I and the Appendix II respectively.

Both parties also agreed that MCIT, the counterpart to JICA, will be responsible for the implementation of the Project in cooperation with JICA, coordinate with other relevant organizations and ensure that the self-reliant operation of the Project is sustained during and after the implementation period in order to contribute toward social, economic and technological development of the Republic of Indonesia.

The Project will be implemented within the framework of the Colombo Plan on Technical Cooperation Scheme and the Note Verbales to be exchanged between the Government of Japan (hereinafter referred to as "GOJ") and the Government of Indonesia (hereinafter referred to as "GOI").

Appendix I: Project Description
Appendix II: Main Points Discussed

PROJECT DESCRIPTION

I. BACKGROUND

Network security is a global issue. Recently, some threats such as DDoS attacks through bot virus and spam mails are serious problems to be taken care urgently.

In Indonesia as well, those information security threats become bigger with development of ICT. Indonesia ranked tenth in Symantec's global list as the country accounted for 2.4% of the world's cybercrimes in 2011. Data from Indonesia Security Incident Response Team / Coordinating Center (ID-SIRTII/CC) shows that there were about 39 million attacks in 2012, and of those, 35% originated from outside the country while 65% came from within. According to the report from DAKA advisory on the meeting of the cyber security challenge in Indonesia in 2012, approximately 86% of Internet users in Indonesia are victims of cybercrimes and it is also reported that Indonesia is more prone to cybercrimes than most other countries.

If effective measures are not introduced, malicious Internet users who try to spread the threats would gather in Indonesia. It will result in deterioration of trust in both economic and social activities. The threats might cause not only an obstruction factor of economic growth of Indonesia, but also give damage to all over the world through networks.

Therefore, it is essential to implement information security measures as the network infrastructure develops and utilization of ICT is prevailed.

II. OUTLINE OF THE PROJECT

Details of the Project are described in the Logical Framework (Project Design Matrix: PDM) (Annex I) and the tentative Plan of Operations (Annex II)

1. Implementation Structure

The Project Implementation Structure is given in the Annex III. The roles and assignments of relevant organizations are as follows:

(1) MCIT

(a) Project Director:

Director General of ICT Applications will be responsible for overall administration and implementation of the Project.

(b) Project Manager:

Director of Information Security will be responsible for regular-basis management of the Project.

(2) ID-SIRTII/CC

ID-SIRTII/CC will be treated as a subdivision under Information

Security Directorate of MCIT in the Project implementation structure though ID-SIRTII/CC is not under the Information Security Directorate according to the official structure of MCIT. It is because that ID-SIRTII/CC is one of the main functions for information security management in Indonesia.

(3) JICA Experts

The JICA experts will give necessary technical guidance, advice and recommendations to MCIT on any matters pertaining to the implementation of the Project.

(4) Joint Coordination Committee

Joint Coordination Committee (hereinafter referred to as "JCC") chaired by the Project Director will be established in order to monitor the Project at high level and facilitate inter-organizational coordination. JCC will be held at least once in six months and whenever deems it necessary. JCC will approve an annual work plan, review overall progress, conduct monitoring and evaluation of the Project, and exchange opinions on major issues that arise during the implementation of the Project. If necessary, working level committees/groups/Implementation Committee under "JCC" shall be organized to facilitate better coordination and communication among stakeholders.

2. Target Areas and Beneficiaries

Expected direct beneficiaries are to be MCIT and government officers related to information security measures. Expected potential beneficiaries are all Internet users in Indonesia.

3. Duration

Two years from December 2013 to December 2015

4. Reports

MCIT and JICA experts will jointly prepare the following reports in English.

(1) Progress Report on semiannual basis until the project completion

(2) Project Completion Report at the end of the project

III. RESPONSIBILITIES OF MCIT

1. MCIT will take necessary measures to:

(1) ensure that the technologies and knowledge acquired by the nationals of Indonesia as a result of Japanese technical cooperation contributes to the economic and social development of Indonesia, and that the knowledge and experience acquired by the personnel of Indonesia from technical training as well as the equipment provided by JICA will be utilized effectively in the implementation of the Project; and

(2) grant privileges, exemptions and benefits to the JICA experts referred to in II-1 (3) above and their families, which are no less favorable than those granted to experts and members of the missions and their families of third countries or international organizations performing similar missions in Indonesia under the Colombo Plan Technical Cooperation Scheme.

2. MCIT will take necessary measures to:
   (1) provide security-related information as well as measures to ensure the safety of the JICA experts; and
   (2) permit the JICA experts to enter, leave and sojourn in Indonesia for the duration of their assignments therein and exempt them from foreign registration requirements and consular fees.

3. MCIT will bear claims, if any arises, against the JICA experts resulting from, occurring in the course of, or otherwise connected with, the discharge of their duties in the implementation of the Project, except when such claims arise from gross negligence or willful misconduct on the part of the JICA experts.

IV. EVALUATION

1. MCIT and JICA will jointly conduct the following evaluations and reviews.

   (1) Mid-term review at the middle of the cooperation term
   (2) Terminal evaluation during the last six (6) months of the cooperation term

2. JICA will conduct the following evaluations and surveys to mainly verify sustainability and impact of the Project and draw lessons. MCIT is required to provide necessary support for them.

   (1) Ex-post evaluation three (3) years after the project completion, in principle
   (2) Follow-up surveys on necessity basis

V. PROMOTION OF PUBLIC SUPPORT

For the purpose of promoting support for the Project, MCIT will take appropriate measures to make the Project widely known to the people of Indonesia.

VI. MUTUAL CONSULTATION

MCIT and JICA will consult each other whenever any major issues arise in the course of Project implementation.

VII. AMENDMENTS

The record of discussions may be amended by the minutes of meetings among MCIT and JICA.

The minutes of meetings will be signed by authorized persons of each side who may be different from the signers of the record of discussions.

Annex I	Logical Framework (Project Design Matrix: PDM) (draft)
Annex II	Plan of Operations (draft)
Annex III	Project Organization Chart (draft)
Annex IV	Joint Coordination Committee (draft)

Project Design Matrix (Draft: as of 23rd July, 2013) (Version 0.9)
Project Title : Project on Capacity building for Information Security
Cooperation timeline : December 2013～December 2015
Implementing Organization in Japan : JICA
Implementing Agency in Indonesia : Ministry of Communication and Information Technology in Indonesia (MCIT)
Target area : All Indonesia
Target people : **Direct beneficiaries** : MCIT and ID-SIRTII//CC staffs, People working on information security in the other ASEAN countries
Indirect beneficiaries : All internet users and all organizations using the internet in Indonesia and the other ASEAN countries

Narrative Summary	Objectively Verifiable Indicators	Means of Verification	Important Assumptions
Overall Goal			
Information security measures in Indonesia are improved	-The number of government offices which introduced Index KAMI in Indonesia is increased. -The number of government offices which established CSIRT in Indonesia is increased.	-Report from Index KAMI internal/external assessors -Report from CSIRT managers	
Project Purpose			
Operational capacity for information security measures in MCIT is improved.	-Index KAMI is introduced in government offices in pilot projects sites. -CSIRT is established in government offices in pilot projects sites - The Index KAMI internal/external assessors and CSIRT managers are satisfied with support of MCIT.	-Report from Index KAMI internal/external assessors -Report from CSIRT managers	-Indonesia's government policy on information security is strengthened -Majority of the trained staffs of MCIT and ID-SIRTII/CC/CC will keep working with the same organization after the completion of the project -Budget for project operation is secured by MCIT
Outputs			
1. Function of Information Security Department is Strengthen 2. Mechanism to support governmental offices is established 3. Awareness raising is improved	1-1. Draft of ideal structure and function of Information Security Department is developed. 1-2. Job performance skill is increased. 1-3. Network for information sharing with ASEAN (including Japan) is established. 2-1. Index KAMI is Improved. Training for new Index KAMI is conducted. Trainees are satisfied with the training. 2-2. Training for CSIRT manager is conducted. Trainees are satisfied with the training. 3-1. The number of facilitators and participants for awareness raising activities is increased. 3-2. Coverage of created materials for awareness raising is expanded.	1-1. Documented Draft of ideal structure and function of Information Security Department 1-2. Performance evaluation reports, and, interview to counterparts 1-3. Report of studied conducted 2-1. Document of improved Index KAMI, training curriculum, and raining implementation reports 2-2. Training curriculum, and training implementation reports 3-1. Reports on awareness activities 3-2. Reports on awareness activities and created materials	-Budget for project operation is secured by MCIT

Activities		
Output 1 (Function of Information Security Department is Strengthen) 1-1. Create a plan of ideal structure and function of Information Security Department - Study organizational structure and function of similar organization in Japan and ASEAN countries - Develop a draft plan of ideal structure and function based on other countries' organizational structure to MCIT 1-2. Improve technical skill of staffs (Malware analysis, Reverse engineering, data mining, etc.) - Conduct basic level trainings (ISMS, etc.) - Conduct middle level trainings (NICTER monitoring, CCNA, etc.) - Conduct high level trainings (Malware analysis, Data mining, etc.) - Conduct practical exercise for incident handling 1-3. Establish a network with Japan and ASEAN countries for studying future trends - Study an operation procedure for incident handling in Japan and ASEAN countries - Study a guideline for companies dealing with critical infrastructure in Japan and ASEAN countries - Study on a standard for data center (server room) for government organization in Japan and ASEAN countries	Inputs 【Japanese Side】 **Dispatch of Experts** Long term Expert ・Chief Adviser ・Project coordinator/Training Planning Short term Expert ・ISMS ・Organization reinforcement ・CSIRT Management ・Network Security/(ex. NICTER) ・Others **Equipment** ・Training equipment (e.g. hardware, software) ・Training material (including multimedia material) ・Others **Training** ・In Japan / third country **Others** ・Conference ・Operational expense 【Indonesia Side】 **Assignment of Personnel** ・Project Director ・Project Manager ・Counterparts **Facilities** ・Office Space (including office equipment) ・Training venue **Local Cost** ・Utility costs **Others** ・Administrative and operational cost	-Counterparts allocate sufficient time for the Project -Budget for project operation is secured by MCIT
Output 2 (Mechanism to support governmental offices is established) 2-1. Create a method to introduce Index KAMI to government offices - Assess and improve Index KAMI - Create a training course for KAMI local internal/external assessors - Conduct the training for local government staffs from pilot project sites - Support to introduce KAMI to government offices in pilot project sites 2-2. Create a method to establish CSIRT in government offices - Create a training course for government staffs to be a CSIRT manager - Conduct the training for local government staffs from pilot project sites - Conduct the training for CERT staffs from ASEAN countries - Support to establish CSIRT in government offices in pilot project sites - Share the good practice with ASEAN countries		**Prerequisite** -Necessary counterparts are assigned for the Project
Output 3 (Human resource, which has technical and management skills for ensuring information security, is developed in Indonesia and the other ASEAN countries.) 3-1. Create a method (channel) for awareness raising - Study best practices of Japan and ASEAN countries for awareness raising - Make connections to related stakeholders (Government offices) 3-2. Create materials for awareness raising - Study materials for awareness raising in Japan - Adapt and customize (translate) and/or develop the materials to Indonesia - Conduct awareness raising - Involve ASEAN countries to share materials for awareness raising		

Plan of Operations (Draft)
Project Name : Project on Capacity building for Information Security
Target Areas: All Indonesia

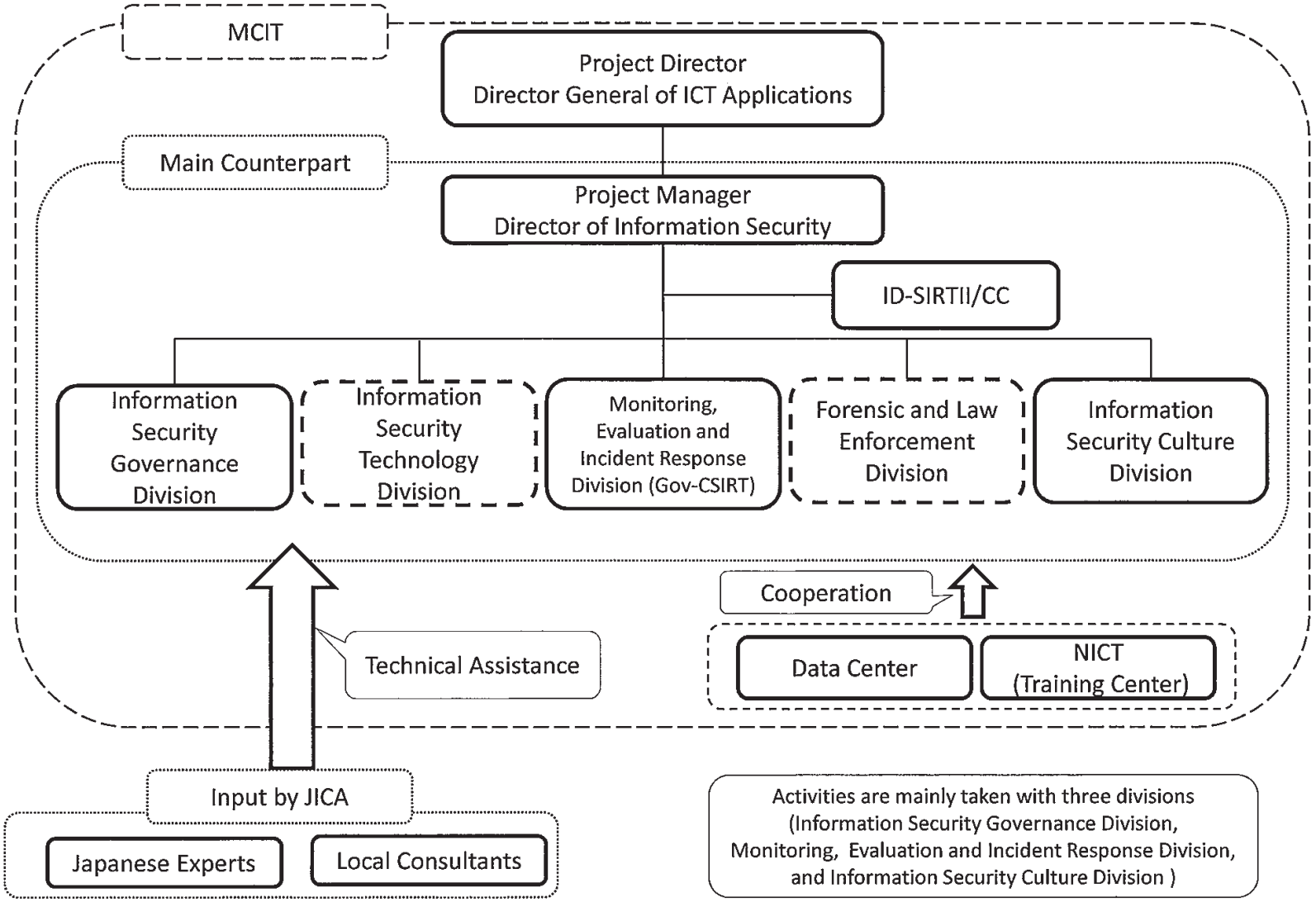
Annex II

Duration : December 2013 – December 2015

Activities	1st year (2013-2014)												2nd year (2014-2015)											
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Outputs 1: Strengthen function of Information Security Department																								
1-1 Create a plan of ideal structure and function of Information Security Department																								
1-2 Improve technical skill of staffs (Malware analysis, Reverse engineering, data mining, etc.)																								
1-3 Establish a network with Japan and ASEAN countries for studying future trends (operational procedure, guideline for critical infrastructure, data center standard)																								
Outputs 2: Establish mechanism to support governmental offices																								
2-1 Create a method to introduce Index KAMI to government offices																								
2-2 Create a method to establish CSIRT in government offices																								
(Introoduce Index KAMI and CSIRT to the Pilot site)																								
Outputs 3: Improve awareness raising																								
3-1 Create a method (channel) for awareness raising																								
3-2 Create materials for awareness raising																								

Annex III

Project Organization Chart (Draft)



Annex IV

Joint Coordination Committee

1. Functions

The Joint Coordination Committee will meet at least once a six months and whenever necessary arises. Its functions are as follows.

(1) To formulate the annual work plan of the Project

(2) To review the progress of the Project

(3) To review and exchange opinions on major issues that may arise during the implementation of the Project, with involvement of private sectors

2. Composition

(1) Chairperson of JCC

- Project Director

(2) Members

<Indonesian members>

- Project Manager
- Representative(s) from ID-SIRTII/CC
- Representative(s) from IT industries
- Representative(s) from critical infrastructure companies

<Japanese members>

- Representative from Embassy of Japan in Indonesia
- Representative from JICA Indonesia Office
- JICA Expert Team

<Others>

- Other personnel/expert appointed by the Chairperson of the JCC

3. Others

If necessary, working level committees/groups under "JCC" shall be organized to facilitate better coordination and communication among stakeholders.

End

Appendix II

MAIN POINTS DISCUSSED

1. Cooperation to ASEAN countries

MCIT and JICA (hereinafter referred to as "both sides") agreed that the Project will involve the other ASEAN countries to establish a network for knowledge sharing on information security. For example, the Project activity is planning to include;

- involving the related authorities and personnel from ASEAN countries to several trainings,
- visiting ASEAN countries for the purpose of information sharing and study, and
- conducting conferences and seminars inviting related stakeholders from ASEAN countries.

2. Cost sharing for the Project activities

Both sides agreed that the budget for the Project activities in Indonesia, such as per diem and travel allowance for domestic training for Counterpart, will be shared by MCIT and JICA.

3. Cost for cooperation to ASEAN countries

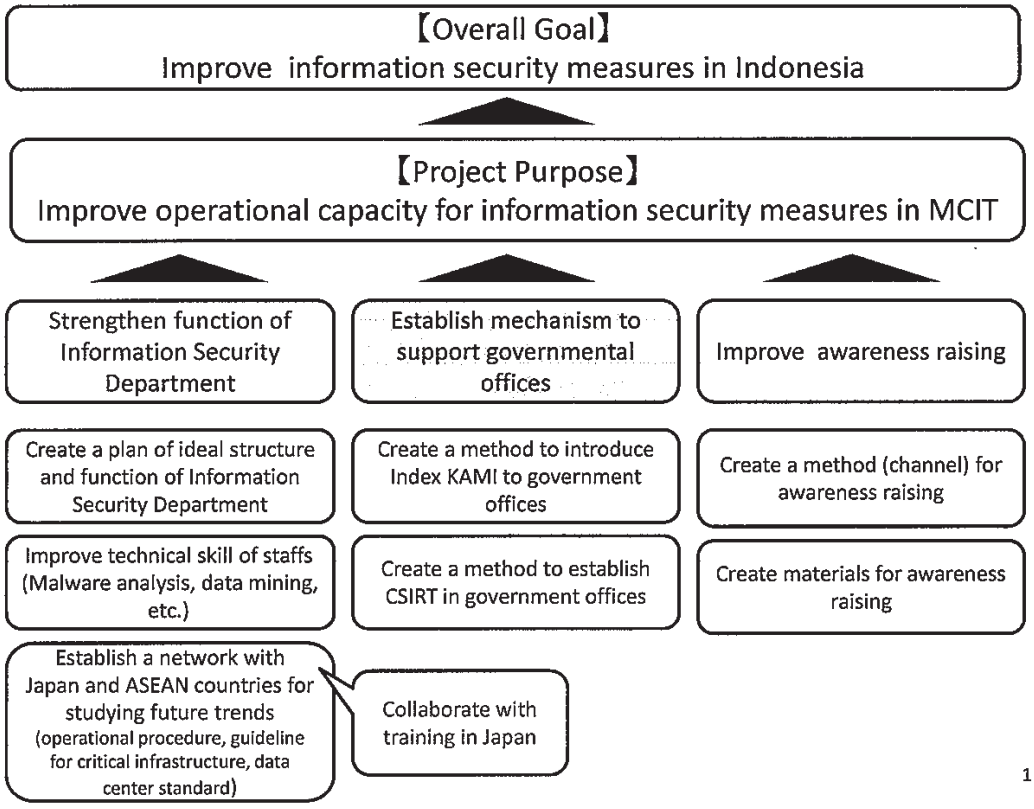
Both sides agreed that the budget for involving related stakeholders from ASEAN countries will be covered by JICA. Indonesian side will cooperate with JICA to support the other ASEAN countries. JICA will bear the cost for such support. For example, when trainings/seminars/conferences for ASEAN countries are conducted in Indonesia, JICA will cover followings;

- per diem and travel allowance for participants from ASEAN countries
- rewards for lecturers even if the counterparts become lectures
- facilities and equipment even if the counterparts provide facilities and equipment
- other necessary cost

End

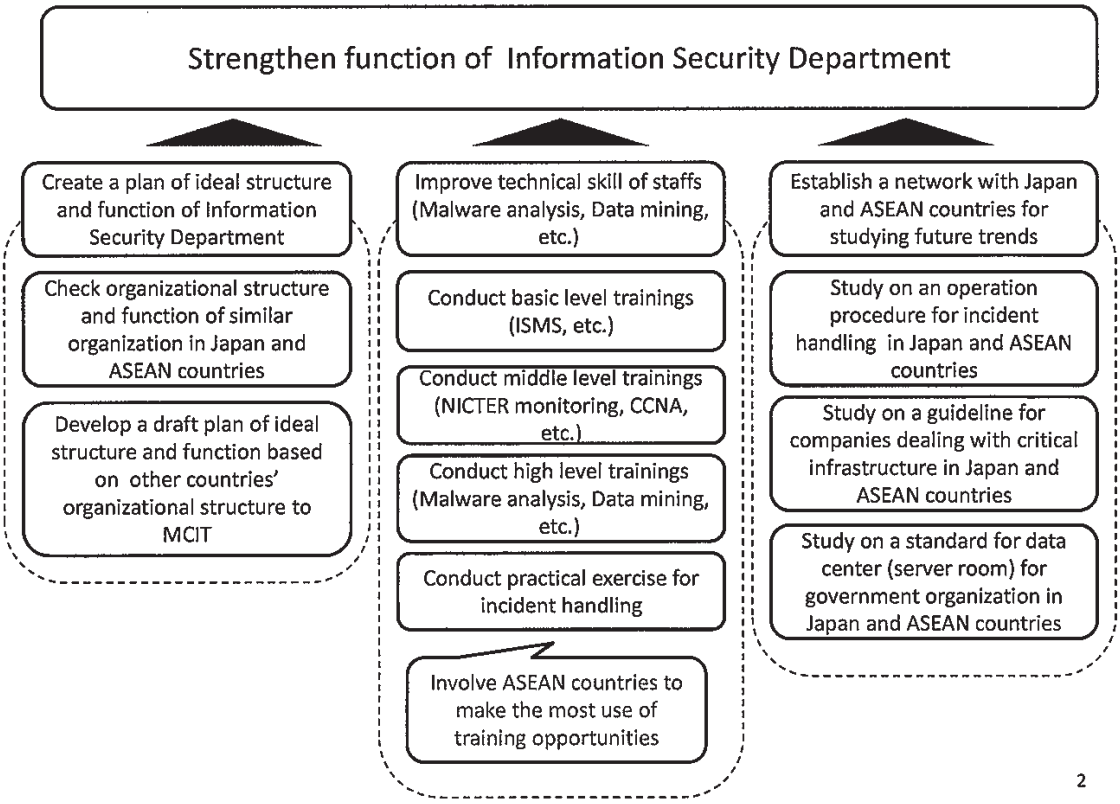
【Draft Outline of the Project】

Annex II



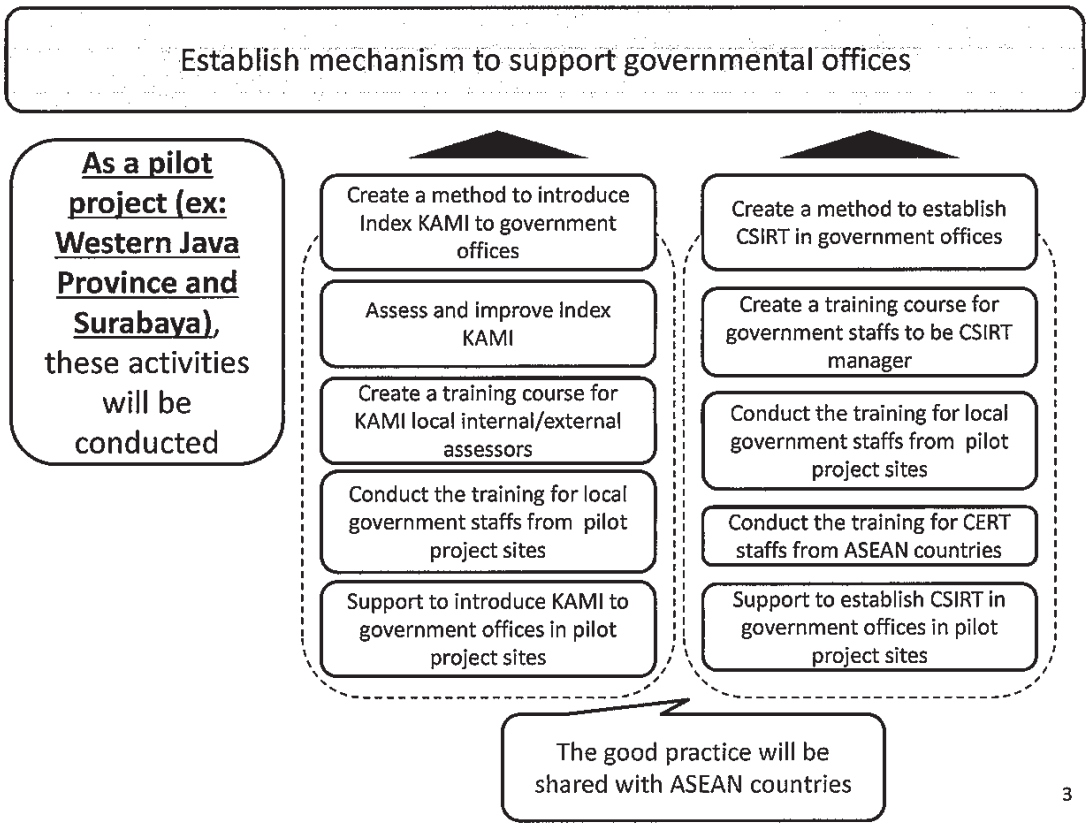
1

【Draft Outline of the Project】



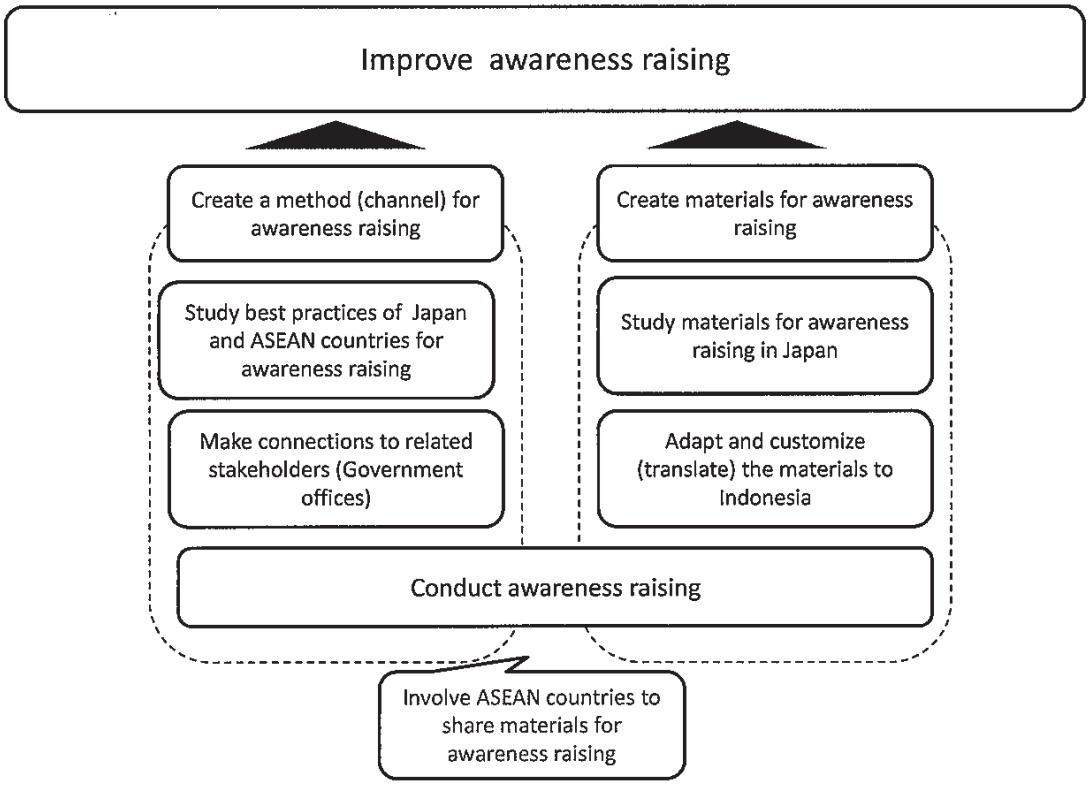
2

【Draft Outline of the Project】



3

【Draft Outline of the Project】



4

２．協議面談録

面談メモ

日時	2013 年 7 月 15 日　11 時 00 分～12 時 10 分
議題	情報セキュリティ能力向上プロジェクトの実施について
出席者	（先方） インドネシア通信情報省（MCIT） Head of Data Center（PDSI）: Dr. Yan Rianto（東海大学に留学経験があり、日本語もある程度話せる） （当方） JICA　井出国際協力専門員 JICA 経済基盤開発部運輸交通・情報通信第二課　竹内職員（記録） JICA インドネシア事務所　リス（Ms. Sulistyo Wardani）現地スタッフ
場所	通信情報省
メモ	情報セキュリティ能力向上プロジェクトの実施について、nicter の運用を所管している MCIT の PDSI と打合せを行った。竹内よりプレゼン資料に沿って今次調査の目的・日程・概要を説明し、その後、Data Center の担当業務やスキル等についてヒアリングした。概要は以下のとおり。 ・Data Center 職員は、28 名（うちエンジニア 10 名）。 ・Data Center の所掌は MCIT のデータ管理のみであり、他の省庁のデータ管理は行っていない。各省庁（中央政府約 40 機関、地方政府約 500 機関）は独自にデータ管理をしており、全政府用のデータセンターは存在しない。 ・関税システム（National Single Window）など、各省庁横断で開発・運用されているシステムもわずかながらある。 ・省庁間のメールはインターネット経由。Gmail や Yahoo メールを使用している者も多い。 ・Data Center の提供する主なサービスは、①アプリケーション開発（勤怠管理システムなど市販のソフトをカスタマイズして開発している）、②インターネットアクセス、③イントラネットアクセス。 ・システムのプラットフォームは OSS（Cent OS、Ubuntu、Debian）が多い。 ・ルータは MikroTik 社製（ラトビアの会社）が多い。以前はシスコ社製を使用していたが高価なため、安価なものでよいところは乗り換えた。スイッチは HP 社製、IBM 社製を使用。 ・サーバー仮想化ソフトは、OSS の KVM（Linux 上の仮想化技術）と、その運用ツールである Ovirt を使用。 ・Data Center のエンジニアには Cisco や MikroTik 等の資格保持者もいる。主に、民間のトレーニングを受講して資格取得やスキルアップをしている（Ovirt については OJT、OSS の OS については民間企業の研修）。 ・Data Center で必要とされるトレーニングは、セキュリティマネジメント分野。例えば、ペネトレーションテストなど、民間トレーニング企業が提供できないレベルのものが必要。 ・技プロ後の人材流出のリスクは高くないと考えている。 ・現在新データセンターを MICT 内のビルに設立する準備中。このデータセンターが完

	成したら来年 ISMS（ISO/IEK27001）を取得しようと考えている（MCIT 全体ではなく、この部局のみでの ISMS 取得）。取得については民間のコンサルに委託する予定。 ・現在、ISMS ほど充実した規定はなく、非常にシンプルな内部規定はある。 ・Disaster Recovery については、民間のデータセンターをバックアップとして利用している。 ・ISMS は政府機関よりも民間企業での認知度が高い。ITIL も同様。 ・インドネシア国内に 3,000 以上の ISP があるが、Government ISP はない。Internet Exchange ポイントは民間ベース。 ・Disaster Recovery は特に配慮していない。バックアップファイルを民間 ISP のデータセンターに預けている程度。 ・本件で供与を希望する機材は特にはない。機材は十分整っている。 ・情報セキュリティ対策の啓蒙活動で MCIT が対象としているのは、中央政府約 40 機関と地方政府約 500 機関である。 ・Data Center の職員を研修に参加させる場合は、2 週間までならそれほど難しくはない。とても重要な研修内容であれば 1～2 カ月の研修も許可は出せる。 ・新人エンジニア向けの大まかな研修方針は、Dr.Yan の頭にはあるが、きちんと文書化やカリキュラム化されたものはない。研修への参加は、各職員から要望を受けて、Dr.Yan が本人の専門性やスキルレベルを考慮したうえで承認している。 ・MCIT で情報セキュリティ対策を全組織的に主管するのは、Information Security 局の Mr. バンバンである。本プロジェクトについても相談はされている。彼からの指示で Data Center 局はどのように本プロジェクトに参加・協力するかが決まる。 ・各部局で勝手にシステム導入をしてしまうので困る。各部局とも、予算が取れれば独自にシステムを構築してよい状況にある。それを統制する権利は Data Center にはなく、必要に応じて IP の割り当てを行うことしかしていない。 ・Data Center が管理しているサーバーに関しては、IDS で外部からの攻撃を監視している。 ・nicter が導入された理由は、大臣と Mr.ルディ及び Mr.バンバンが日本を訪問した際に nicter を見て導入したいといったためと認識している。nicter は通常運用では活用していない。ダークネットしか見ていないので、イントラネット内の感染した PC を発見するといった運用はできない。パケットのデータ解析が独自にできればよいが、そのようなスキルをもった人材は MCIT にはいない。 ・現在、情報セキュリティに係る啓蒙用 Web サイトはないが、あればよいとは思う。 ・Data Center が毎年作成している報告書には、運用しているアプリケーションの数（Usage of Application）や Service Level（MTBF や MTTR など）を記録している。 以上 ※備考：本記録は先方参加者の確認を経たものではない。

面談メモ

日時	2013 年 7 月 16 日　9 時 00 分～11 時 00 分
議題	情報セキュリティ能力向上プロジェクトの実施について
出席者	（先方） インドネシア通信情報省（MCIT） Vice Head of NICT-HRD Management Unit）：Mr. M. Nur Gunawan Vice Head of NICT-HRD Management Unit）：Mr. Imam M.Shofi Ministry of Regional Affairs Syarif Hidayatullah Sate Islamic University, Faculty of Science and Technology Assistant Professor：Ms. Aries Susanto HT. その他 3 名 （当方） JICA　井出国際協力専門員 JICA 経済基盤開発部運輸交通・情報通信第二課　竹内職員（記録） JICA インドネシア事務所　リス（Ms. Sulistyo Wardani）現地スタッフ
場所	通信情報省
メモ	情報セキュリティ能力向上プロジェクトの実施について、MCIT の Human Resourse Development 局傘下の国立 ICT 人材育成センター（NICT-HRD）へのヒアリングを行った。概要は以下のとおり。 【NICT-HRD について】 ・2010 年に韓国の借款（約 20 億円）で設立された。韓国からの専門家派遣や韓国への研修（短期のものから、修士号、博士号留学まで）の支援も同時に実施された。 ・土地は Islamic University が提供しており、2009 年に韓国（KOICA）、MCIT、Islamic University の間で交わされた覚書にて、2019 年までは MCIT が運営管理を行い、2019 年以降は運営管理権を Islamic University へ移譲することとなっている。 ・予算は MCIT より配布されている。 【トレーニング内容について】（詳細はパンフレット参照） ・ICT トレーニングは 9 割が政府機関及び教育機関（小学校から大学まで）が対象。トレーニングはすべて無料（政府予算でカバーされている）。民間へのトレーニングは禁止（費用を受け取って実施することもしていない）。残る 1 割の対象は一般人。公募で受講者を募り無料でトレーニングを実施。 ・年間約 5,000 名にトレーニングを実施。100 人程度用の宿泊施設もあり。 ・内容は、マルチメディア作成（TV 番組含む）、一般的な PC 操作から、システム開発、ネットワーキング、GIS、Oracle 社やマイクロティック社などの資格試験（講師はインドやシンガポールなど外国人が来ることもある）、SSCP、CISSP といった情報セキュリティの国際標準資格試験用のトレーニングを実施。Cisco 資格用トレーニングはなし。 ・講師は内部人材と外部人材。外部講師は民間企業。 ・テキストは国際標準資格やメーカー系資格については英語。NICT 独自のトレーニングコースについては、現地語。 ・修了生には NICT 発行の Certificate を授与。 ・情報セキュリティに特化した研修としては、Linux サーバ Administration やネットワー

	クセキュリティ（スノートなど）。主な受講者層は大学生。 ・SSCP、CISSP といった情報セキュリティの国際標準資格試験用のトレーニングも実施。合格率は SSCP（40 名参加し合格者なし）、CISSP（10 名参加し 2 名合格）。 ・講師は「ユニプロ」という現地企業。講師費用は 100 時間で 950USD。レクチャーは英語。 ・大学機関でも情報セキュリティに特化したラボを保有していない大学は、NICT の研修を活用するケースがある。 【MCIT との連携について】 ・MCIT のプロジェクト実施機関として研究活動を実施。マレーシアの大学機関、韓国、ドイツ、英国といった外国の機関との共同研究などに取り組んでいる。 ・情報セキュリティに関する啓蒙キャンペーンを MCIT と共同で実施。MCIT のバンバン局長が NICT 生徒に対するセミナー講演を実施したり、学校機関（教師、生徒）への啓蒙活動を実施。 （この後、施設見学を実施） 以上 ※備考：本記録は先方参加者の確認を経たものではない。

面談メモ

日時	2013 年 7 月 16 日　13 時 00 分～14 時 30 分
議題	情報セキュリティ能力向上プロジェクトの実施について
出席者	（先方） インドネシア通信情報省（MCIT） Director General for Informatics Applications：Dr. Ashwin Sasongko Director of Information Security：Mr. Bambang Heru Tjahjono （当方） 日本大使館 ASEAN 日本政府代表部　吉田一等書記官 JICA　井出国際協力専門員 経済基盤開発部運輸交通・情報通信第二課　竹内職員（記録） JICA インドネシア事務所　黛所員 松田主席 リス（Ms. Sulistyo Wardani）現地スタッフ
場所	通信情報省
メモ	情報セキュリティ能力向上プロジェクトの実施について、MCIT アシュウィン総局長、バンバン局長と打合せを行った。竹内よりプレゼン資料に沿って今次調査の目的、日程、概要を説明し、その後意見交換をした。意見交換の概要は以下のとおり。 （吉田）つい先日、本プロジェクトは正式に採択された。本プロジェクトは「日 ASEAN サイバーセキュリティ人材育成イニシアティブ」のひとつであり、日本側は総務省、経済産業省、NISC、JICA といった関連機関が連携して支援する。基本的にはインドネシアとのバイの協力であるが、活動では ASEAN 諸国を巻き込む内容と考えている。 （アシュウィン）本プロジェクトと、PRACTICE プロジェクトと TSUBAME プロジェクトとの関係は？ （吉田）PRACTICE と TSUBAME は個別プロジェクトとして実施されているものだが、本プロジェクトでは両プロジェクトとも連携する。 （アシュウィン）2013 年 9 月の日 ASEAN サイバーセキュリティに関する閣僚政策会議の準備会合が 8 月にあるが、そのために日本の協力について、どの国に nicter と TSUBAME が導入されているかを明確に知りたい。 （吉田）了解した。説明資料を準備してお送りする。 （竹内）プロジェクト開始時期は最短で 2013 年 12 月と考えているが、インドネシアの予算年度が 1 月から始まることを考慮すると、2014 年 1 月開始とした方がよいか。 （アシュウィン）1 月だと使える予算がない場合もあるため、プロジェクト開始時期は 2013 年 12 月開始の方がよい場合もある。どちらにするかは内部で検討する。 （井出）ASEAN 諸国から人を招いてインドネシアでの研修を実施する場合、内容によってはインドネシア側に講師となってもらいたい。 （アシュウィン）講師になることは問題ない。ただし、講師謝金を誰が支払うかにもよる。その点はバンバンと協議してほしい。またその場合は誰の名前で招待状を出すのか？

	（竹内）講師謝金は JICA の規定に沿ってある程度はプロジェクト予算から支出することも可能。追ってバンバン氏と協議したい。招待状についてはプロジェクト名で出すのは可能か？ （バンバン）招待状については、プロジェクト名で出すことに問題ない。講師謝金のほかにも、JICA 専門家に同行する地方出張時などの費用負担は、明確に整理したい。 （井出）費用負担に係る懸念は理解する。追って協議したい。 以上 ※備考：本記録は先方参加者の確認を経たものではない。

面談メモ

日時	2013 年 7 月 16 日　14 時 30 分～17 時 30 分
議題	情報セキュリティ能力向上プロジェクトの実施について
出席者	（先方） インドネシア通信情報省（MCIT） Director of Information Security：Mr. Bambang Heru Tjahjono Head of Risk Management Section, Directorate of Information Security:Mr. Yudhistira （当方） 日本大使館 ASEAN 日本政府代表部　吉田一等書記官 JICA　井出国際協力専門員 経済基盤開発部運輸交通・情報通信第二課　竹内職員（記録） JICA インドネシア事務所　黛所員 松田主席 リス（Ms. Sulistyo Wardani）現地スタッフ
場所	通信情報省
メモ	情報セキュリティ能力向上プロジェクトの実施について、本プロジェクトのカウンターパートとなる MCIT の Information Security 局と打合せを行った（プロジェクト Outline の各 Output に先方ニーズを引き出すヒアリングを行った）。内容は下記のとおり。 **OUTPUT　1．Instructional Measure について** 【ISMS について】 ・政府機関のうち重要な機密情報を扱う e-Procurement　Division と Human Resource Unit は ISMS 取得済み。地方では、スラバヤ地方政府の e-Procurement　Division とスラバヤの MCIT 事務所が ISMS を取得済み。 ・ISMS 取得は、ISMS 導入コンサルタントに委託した。 ・今後も ISMS を政府機関に導入することはあまり考えていない。ISMS を簡素化した独自の情報セキュリティ対策診断ツール「Index KAMI」の導入を推進する方針である。 【Index KAMI について】 ・「Index KAMI」をインドネシアの National Standard にしたい。 ・「Index KAMI」の指標は Governance、Risk Management、Framework、Asset Management、Technology & Security の 5 つ。組織の情報セキュリティレベルを５段階（最もすぐれているのがレベル５）で評価する仕組み。 ・「Index　KAMI」での診断は約 150 の政府機関で実施済みだが、ほとんどがレベル２以下という結果。 ・「Index KAMI」の診断レベルを向上させるためのコンサルティングは、やっていない。 ・「Index KAMI」の Assessor（アセスメント実施コンサルタント）は 20 名以上いる。うち約 10 名が MCIT 職員。研修を受講して合格すると Assessor 資格を取得できる。バンバン氏自身も Assessor 資格保有者（これは、正規の ISMS 審査員の研修と思われる）。 ・政府機関が地方も含めると約 560 ある。このため本プロジェクトでのターゲットは質より量。まずは 2014 年末までに 200 の政府機関部局（組織ではなく部局単位）に「Index KAMI」を導入したい。 ・政府ガイドラインで 2017 年 11 月までに情報セキュリティに関する National

	Certification を取得することが一般企業にも推奨されているが、ISMS を取得することは費用面・工数的に不可能なので、ISMS の代わりに「Index KAMI」を普及させたい。 ・現在、地方政府には情報セキュリティに詳しい人材が不足している。そこで政府組織内に情報セキュリティ担当のファンクショナルポジション（専門性をもった職員のポジション）を新たに設置するように要請を出している。 ・このファンクショナルポジションとなる人材を育成したい。彼らが「Index KAMI」を組織に導入するためのキーマンとなる。2014～2015 年に必要なファンクショナルポジション人材数は 300 名ほど（「Index KAMI」の新規導入政府部局（約 150）×2 名/部局＝300 名）。 ・民間企業にもこのような人材が必要であるが、MCIT の所掌範囲ではない。MCIT のターゲットは政府機関のみ。 ・このような人材育成のための研修を MCIT は実施できない。研修実施機関ではないため、研修は他の機関に依頼するかたちをとらざるを得ない。MCIT が独自に実施可能なものは3日間以内のセミナーのみ。政府内部人材の育成は Educational Training Agency（MCIT 傘下）が所掌している。 ・本プロジェクトでは、ファンクショナルポジション人材を育成するトレーナーを育てたい。そのためには、育成用カリキュラムも必要。これが Institutional Measure の Output のひとつとなり得る。トレーナー育成は ID-SIRTII や NICT へ実施を依頼するかたちとなるが、どの機関へ依頼するかはこれから検討する。 【データセンターアセスメントについて】 ・各政府機関より必要なデータセンター要件についての問合せを受けることが多いが、政府機関のデータセンターのレベルをアセスメントできる人材がいない。 ・日本の富士通ショールームを訪問した際、データセンター要件の基準的なものがあると聞いたが、インドネシアにもそのような基準が欲しい。要件はデータセンターの運用面ではなく、電源の二重化等ハード的なものを指している。 ・政府向けデータセンター要件基準の作成は Institutional Measure の Output のひとつとなり得る。 【Risk Management Policy について】 ・重要インフラ（電気、水道、空港、鉄道、金融など）については、Risk Management Policy が必要と考えているが、現在はない。 ・マレーシアには、National Critical Infrastructure Protection Policy があると聞いている。 ・BT テレコムもそういったポリシーを作成している。 ・重要インフラ Risk Management Policy 作成は Institutional Measure の Output のひとつとなり得る。 ・日本の NISC が類似のポリシーをもっている可能性あり。また、日本では各業界団体がガイドラインを設けているだろう（吉田）。 【官民の情報共有について】 ・情報セキュリティに関する官民の情報共有のガイドラインがないが、必要と考えている。 ・「サイバーセキュリティデスク」を新たに設置する予定だが、情報共有をどうやっていくかは明確な指針がない。 ・日本の取り組みを紹介してもらいたい。 ・米国のアイザックのような仕組み（CERT はインシデントハンドリングのみだが、ア

	イザックの仕組みはインシデントに限定せずに毎日情報交換を行う）と理解するが、仕組みづくりを 2 年間で実施するのは困難だろう。本プロジェクトでは取り組み事例の紹介程度にとどめることが妥当と考える（吉田）。 **OUTPUT 3. Human Resource Development について** 【研修対象となる関連組織について】 ・ID-SIRTII（Indonesia Security Incident Response Team on Internet Infrastructure）はその名称に「Infrastructure」とあるように IP インフラのみを監視している。 ・ID-CERT はパブリック CERT である。アカデミックな研究を含め、外国からの情報セキュリティ関連レポートを収集し情報を MCIT へ提供している。 ・Gov-CERT（Information Security 局傘下のプロジェクトベースで運営）は政府の情報セキュリティ対策をプロモートするための機関である。 ・ID-SIRTII からのレポート内容には満足している。 ・インシデントレスポンスのガイドライン（関連機関の連絡・連携体制に係るガイドラインのことと思われる）がない。 【啓蒙活動（Awareness Raising）について】 ・ターゲットの優先順位は、「政府機関　＞　重要インフラ企業　＞　一般企業　＞　一般人」というもの。 ・一般人向けの啓蒙活動は、Safe and Health Internet を所掌する別の部局が担当している。一般人向けの啓蒙活動としては Facilitation for Community という活動もある。 ・本プロジェクトで対象とするべきは、政府機関と重要インフラ企業だが、それ以外も含めることも可能。どの範囲までを含めるかは内部で検討する（次回協議までに決めておく）。 以上 ※備考：本記録は先方参加者の確認を経たものではない。

面談メモ

日時	2013 年 7 月 17 日　14 時 00 分～17 時 00 分
議題	情報セキュリティ能力向上プロジェクトの実施について
出席者	（先方） インドネシア通信情報省（MCIT） Senior Advisor to Minister on Information Systems：Dr. Rudi Lumanto （日本の電気通信大学を卒業して、その後、日本のソニーに勤務した経験あり） ID-SIRTII（Indonesia Security Incident Response Team on Internet Infrastructure） Vice Chairman of Operation & Network Security Dept：Mr. Muhammad Salahuddien Vice Chairman of External Collaboration Dept：Mr. Muhammad Salman Vice Chairman of Data Center, Application & Database Dept：Mr. Bisyron Wahyudi （当方） JICA 井出国際協力専門員 JICA 経済基盤開発部運輸交通・情報通信第二課　竹内職員（記録）
場所	通信情報省での協議後、ID-SIRTII に移動しルディ氏以外と協議を継続
メモ	情報セキュリティ能力向上プロジェクトの実施について、MCIT ルディ大臣補佐官及び ID-SIRTII と打合せを行った。竹内よりプレゼン資料に沿って概要を説明後、ヒアリングを行った。概要は以下のとおり。 ・ID-SIRTII は MCIT の Information Security 局の下ではなく、Telecommunication インフラ担当局の下に位置づけられる。（後日、バンバン局長との打合せにて、これは予算上の位置づけであり、実際は Information Security 局との連携の方が強いとのこと。） ・インシデントハンドリングは Information Security 局ではなく、ID-SIRTII が実施している。 ・情報セキュリティ関する対応は ID-SIRTII と Gov-CSIRT だけではハンドリングできないほど多いため、各政府機関に組織独自の CSIRT を設置したい。この目標は ID-SIRTII 独自の目標・計画であり、政府の計画ではない。ただ、Information Security 局も同じ意見と思う。 ・ID-SIRTII の戦略や計画は独自に決定している。 ・政府機関にインシデントについて Gov-CSIRT へレポートする規則はない。（そうすることが理想ではあるが） ・独自に CSIRT を設置している機関もある。その場合、CSIRT の TOR はその機関が内部で決定しているが、CSIRT 設置に係る支援（研修等）は ID-SIRTII が行うこともある。 ・インドネシアでは組織上層部ですら意識改革の必要性を十分理解しておらず、情報セキュリティ対策は技術的対策のみでよいと思っている層が多い。このため、啓蒙活動が重要。 ・Index KAMI は Awareness Raising の役割もある。アセスメントの過程で情報セキュリティ対策の重要性に気付くツールでもある。 ・民間企業に対しての研修は、インシデントハンドリング、Awareness Raising、CSIRT 設立支援など。 ・研修実施について、カリキュラムは独自開発したものある。ただ、人員の問題で大多

	数への研修実施は困難。 ・本プロジェクト内でカンボジア、ラオス、ミャンマー等の CERT スタッフに研修を実施することは可能。2013 年 9 月に APCERT を招いて研修を実施する予定もあり、他国 CERT への支援には抵抗はない。 ・ほとんどの研修テキストは英語であり、講義を英語で実施することも問題ない。 ・インドネシアでは高いスキルを身に付けるためには英語力が重要。 ・ID-SIRTII の機能としては、JP-CERT の機能と同様である。ネットワークのモニタリング、早期警報などを実施している。 ・現時点での課題は、各種監視データの分析能力を向上させるためにデータマイニング技術を高めたい。中国の CERT ではこのような取り組みをしていると聞く。 ・また、マルウェア解析の技術も高めたい。4 カ月前より PRACTICE の下で、マルウェア情報の共有をテレコムアイザックと開始した。当地の大学アカデミック CSIRT（約 40 の大学が参加）と連携してハニーポット設置の計画もある。テレコムアイザック（NTT の則武氏）の協力を得て 2013 年 8 月にハニーポット設置を計画している。 ・nicter のネットワークモニタリングは MCIT が実施中。ID-SIRTII では TSUBAME（JP-CERT が開発し APCERT 連携を実施）及び独自開発中のマタガルーダ（インドネシア語で「鷹の目」の意味）でモニタリングを実施している。 ・TSUBAME とマタガルーダの機能は同じであるが、TSUBAME は APCERT 連携により他国の情報も入手できるメリットがある。 ・（今後 nicter を使いたいかという問いに対して）使えるなら活用したいと考えている。監視システムが 3 種類となるが、多ければ多いほど比較ができるため、メリットはある。 ・ID-SIRTII の研究開発能力を高めたい。例えばリバースエンジニアリング技術などを高めたい。アセンブラ言語を理解するエンジニアも ID-SIRTII にいる。 （ここから、ID-SIRTII へ移動して協議を実施。ルディ氏は退席。） ・マタガルーダはまだプロトタイプである。ソースファイヤーやフォーティネットといった監視用の商用ソフトウェアをこれまで使用しているが、ライセンス料金が高いことと、インドネシア独自のシグニチャには対応困難なことがあり、独自にマタガルーダを OSS で開発することにした。 ・今後、マタガルーダを民間企業等にも提供していきたい。民間企業によっては企業内ネットワークの情報を ID-SIRTII へ提供することもあり得る。そうすれば、より広範囲のネットワークモニタリングが可能となるほか、企業の情報セキュリティ対策レベルを上げることにもつながる。 ・民間企業等へ展開するためにマタガルーダを搭載したハードウェアを開発したいとも考えている。 ・商用ウイルス対策ソフトでは対応できないインドネシアのローカルウイルスも存在する。このため ID-SIRTII にはマルウェア解析技術が必要。 ・海賊版ソフトが普及しているため、そもそも情報セキュリティ対策が困難である。ちなみに、海賊版 Windows でも Windows Update が可能なものもある（中国のサーバへ接続しているが、そこからマルウェア感染することもあり得る）。 ・ID-SIRTII での研修は講師 1 名＋アシスタント 2 名で約 20 名の生徒を教えるのが標準。

	以上 ※備考：本記録は先方参加者の確認を経たものではない。

面談メモ

日時	2013 年 7 月 18 日　9 時 00 分～9 時 45 分
議題	インドネシアでのシスコアカデミー実施状況について
出席者	（先方） PT. Cisco Systems Indonesia　Area Academy Manager：Mr. Adri Gautama （当方） JICA　井出国際協力専門員 経済基盤開発部運輸交通・情報通信第二課　竹内職員（記録）
場所	PT. Cisco Systems Indonesia
メモ	情報セキュリティ能力向上プロジェクトに関連し、本プロジェクトの研修トピックとなる可能性が高い CCNA 等の資格試験やその研修について PT. Cisco Systems Indonesia と打合せを行った。内容は下記のとおり。 ・本来シスコアカデミーは学生対象だが、インドネシアでは政府機関を対象にした研修も実施している。最近、運輸省への研修を実施した。 ・インドネシアで最も優秀な Cisco 認定の研修機関は、ジョグジャカルタ（ジャカルタからは車で 20 時間、飛行機で 1 時間）にあるガジャマダ大学である。機材や施設も整っている。ただし、CCNB 試験の研修はない。 ・インドネシアに 7 名いる CCNA の ITQ 試験合格者のうち、1 名がガジャマダ大学の講師。他には、国立インドネシア大学や私学の BINA NUSANTARA 大学といった大学の講師も合格している。 ・ID-SIRTII へは、Cisco 製品のトレーニングや情報提供などの協力を行っている。 ・研修等の講師として Cisco 社から謝金ベースで人を派遣することは可能。情報セキュリティ分野であれば、シンガポールのジョシュワ氏が詳しい。必要なら紹介することもできる。 ・インドネシア国内で情報セキュリティ分野のリーディングカンパニーがどこかは、社内で聞いてみて、分かれば調査団へ連絡する。 ・インドネシア国内でも、ペネトレーションテストを実施できる業者はある。 ・MikroTik 社（ラトビアの会社）のネットワーク機器は、インドネシアではそれなりのシェアがある。ワイヤレスアクセスに適しているが、高い信頼性があるとは言い難い。オープンソースのため、一社製品に限定しにくい政府機関で使用されているケースが多い。 ・MikroTik 製品の研修の中身の約半分は、Cisco 製品とのコンフィギュレーションにかかるもの。 ・他の ASEAN 諸国ではミクロテック製品はあまり普及していない。 ・中国フォアウェイがインドネシアへ参入した当初は、同社製品が普及したが、カスタマーサービスの悪さから現在では普及していない。 ・MCIT が実施している Index KAMI については、聞いたことはない。 ・Cisco インドネシアでは、ISMS コンサルサービスは提供していない。 以上

	※備考：本記録は先方参加者の確認を経たものではない。

面談メモ

日時	2013 年 7 月 18 日　11 時 00 分～12 時 00 分
議題	インドネシア民間セクターの情報セキュリティ対策について
出席者	（先方） PT. Telkom Indonesia Information System Center, Deputy Senior Manager：Mr. Sihmirmo Adi Internet Data Center and Infrastructure Operation, Operation Senior Manager：Mr. Taufik R&D of Network Management：Mr. Bambang Soekanto Application & Content, CDEV Multimedia Manager：Mr. Fridh Zurriyadi Ridwan IT Strategy & Governance, AVP IT Policy & Standard：Mr. Wartono Purwanto、他 （当方） JICA 井出国際協力専門員 JICA 経済基盤開発部運輸交通・情報通信第二課　竹内職員（記録）
場所	PT. Telkom Indonesia
メモ	情報セキュリティ能力向上プロジェクトに関連し、民間企業の情報セキュリティ対策についてインドネシア最大手通信事業者 PT. Telkom Indonesia と打合せを行った。内容は下記のとおり。 ・Telkom Indonesia は国営通信事業者であり市場シェアは約 60%を占める。 ・情報セキュリティについては、ID-CERT、ID-SIRTII から関連情報を毎月もらっている。 ・自社のセキュリティポリシーあり。 ・インシデントは ID-SIRTII へレポートしている。MCIT にはレポートしていない。 ・ID-CERT と ID-SIRTII の支援を受けつつ自社の CSIRT 設立に取り組んでいる。 ・ID-SIRTII は、通信事業者 11 社を対象に、通信事業者用 CERT「Telkom-CERT」を設立しようと計画している。 ・インドネシア固有のウイルスが検知された場合は、商用ウイルス対策ソフト開発会社（←ノートンやシマンテックなどを意味する）へレポートしている。 ・情報セキュリティについては ID-SIRTII の研修を受けることもある。 ・昨年、ISMS を取得した。その際には JP-CERT の協力も受け、自社内の人材（インターナルオディター）が旗振り役で ISMS を導入した。ただし、安くない費用がかかるので認証は受けていない。 ・ISMS の導入企業同士でアセスメントを実施するのが経済的で良い方法だろう。外国の ISMS コンサルに高い費用を払わなくてすむ。 ・インドネシアで情報通信インフラ関連の仕事をする者の間で ISMS はよく知られている。 ・情報セキュリティについては、民間に対する直接的な政府支援が必要とは思わないが、啓蒙活動（Awareness Raising）は政府の役割として必要である。 ・通信事業者として PC-I-DSS（クレジットカードのデータセキュリティ）や USGAAP（米国会計標準）に見合う情報セキュリティ対策が必要であり、社員研修としては、自社で実施するほか、現地 IT 研修業者へ委託することもある。 ・社員は、CEH（Certified Ethical Hacker: EC-Council）などの情報セキュリティ関連資格保持者もいる。

	・政府に期待することは、技術的なサポートというよりも、情報セキュリティに関する方向性の提示である。 以上 ※備考：本記録は先方参加者の確認を経たものではない。


ジャイカ
JICA