



情報セキュリティ分野における 日本とASEANとの連携について

2011年2月26日

内閣官房情報セキュリティセンター

内閣参事官 高田 充人

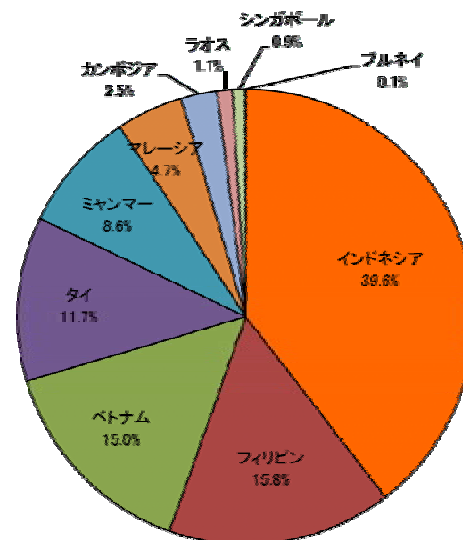
ASEAN各国の人口と1人あたりGDPの現状

	人口(万人)	1人あたりGDP(米ドル)
ブルネイ	40	35,394
カンボジア	1,481	677
インドネシア	22,996	2,349
ラオス	632	940
マレーシア	2,747	6,975
ミャンマー	5,002	499
フィリピン	9,198	1,745
シンガポール	499	36,537
タイ	6,776	3,894
ベトナム	8,728	1,052
ASEAN	58,099	2,557
日本	12,756	39,727
世界計	677,524	8,594

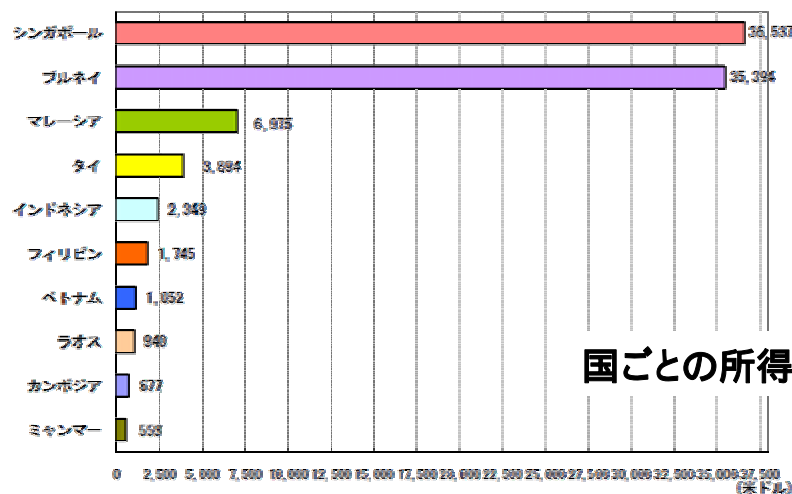
ASEANの人口は日本の約4.6倍

ASEANの1人あたりGDPは

- ・世界平均の29.7%
- ・日本の6.4%



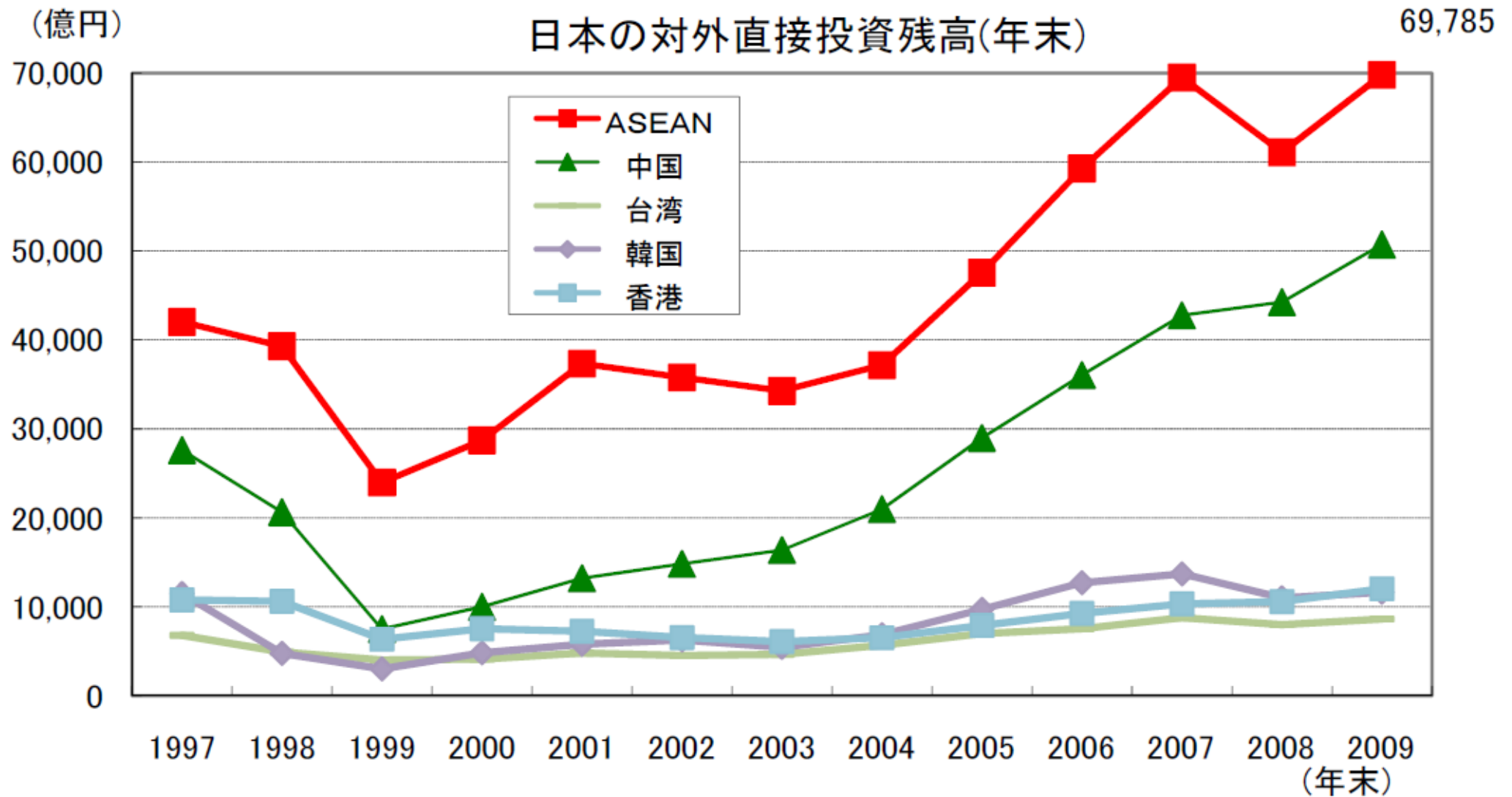
国ごとの人口規模は大きく異なる



国ごとの所得水準も大きく異なる

出典: 目で見えるASEAN –ASEAN経済統計基礎資料- (平成22年)

我が国の対ASEAN直接投資残高の推移



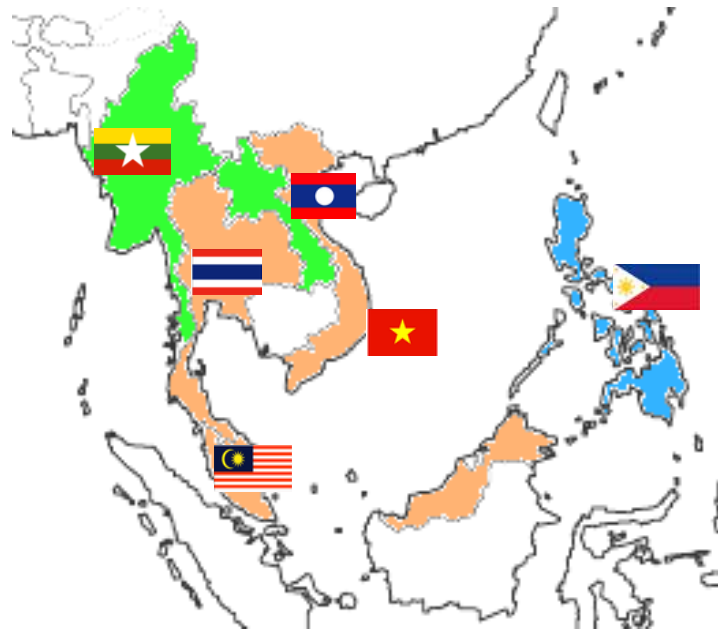
出典: 目で見るASEAN -ASEAN経済統計基礎資料- (平成22年)

ASEANに進出した日系企業のニーズ

「在ASEAN日系企業からの要望書」(平成21年6月29日)
進出先で直面する事業環境の問題点の改善に関する要望をとりまとめ、スリンASEAN事務総長に提出したもの。

要望書の3つのポイント



1. 期限通りの AEC (ASEAN 経済共同体) の実現とそれを確保するための十分なモニタリング
2. ASEAN 域内のインフラや産業基盤の更なる充実・整備
3. 日本を含む対話国との貿易投資の促進と保護主義的な動きの牽制







具体的要望事項

B4. 社会基盤の開発

情報インフラ

通信環境(インターネット、固定・携帯電話)の早期改善
(ミャンマー 、ラオス )

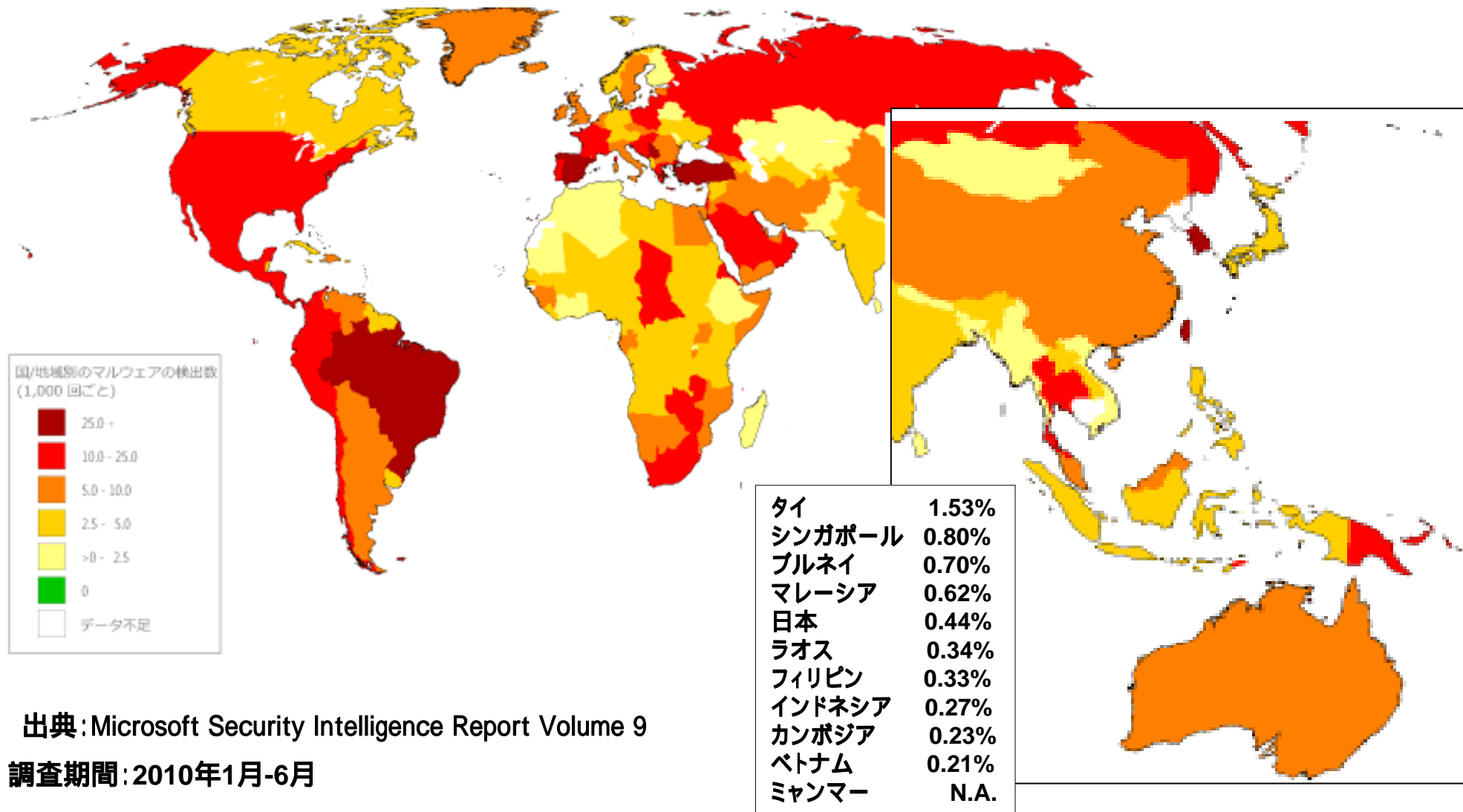
通信回線容量が小さく、速度が遅い通信インフラの
容量拡大
(フィリピン )

広帯域で信頼性の高い国際通信ネットワークの整備
(ベトナム 、マレーシア 、タイ )

出典: 在 ASEAN 進出日系企業からの要望書 (アセアン日本人商工会議所連合会)

ASEANにおける情報セキュリティの現状

- ・我が国のマルウェア感染率 (0.44%) は世界平均 (0.96%) を大きく下回る
- ・ASEAN地域は国々で地域差あり



出典: Microsoft Security Intelligence Report Volume 9

調査期間: 2010年1月-6月

ASEANにおけるトップレベルドメインの危険度

高リスク  低リスク

国または名前	TLD	2010年 世界リスクランキング	2009年 世界リスクランキング	2010年 追跡ドメインの総数	2010年 リスクの高いドメインの総数
ベトナム	VN	3 ↑	39	24,988	14,492
フィリピン	PH	25 ↓	6	9,625	418
ラオス	LA	35 ↓	26	4,143	122
マレーシア	MY	47 ↑	80	15,200	221
タイ	TH	48 ↓	32	8,912	130
インドネシア	ID	69 ↓	56	6,138	52
シンガポール	SG	81 ↓	10	15,632	105
日本	JP	104 ↓	103	464,408	547

✓ 昨年の評価以降に改善されたトップレベルドメイン(TLD)上位5位のうち、2つがASEAN加盟国 (シンガポール(.SG) 及びフィリピン(.PH))。

これらの2つのTLDは、いずれも昨年は、最もリスクが高いTLDの上位10個にランクインしていた。

✓ ベトナム(.VN)は、昨年の評価では比較的安全なドメインだったが、本年の調査では、悪意のあるアクティビティと関連があり、ボットネット等の一部として悪用されている。

✓ 日本は世界でもリスクの低いトップレベルドメインのひとつであり、アジア太平洋地域でもっとも危険が少ないと評価。

出典: 危険なWebサイトの世界分布 2010, McAfee より抜粋

ASEAN ICT Master Plan 2015 (2011年1月策定)

概要

ICTの普及を通じて、ASEANにおける投資経済環境の改善や発展を目指した戦略計画。6つの戦略的な取り組みを通じて、以下の4つの成果を得るとしている。

1. ASEANにおける成長の原動力としてICTを利用
2. ASEANをICTのハブとする
3. ASEAN市民の生活を改善する
4. ICTによる社会経済環境の深化



情報セキュリティに関する取組み(抜粋)

2.4 信頼の醸成

- ・教育を通じた民間向けのサイバーセキュリティの意識啓発を実施
- ・個人情報保護の確立

4.2 情報セキュリティとデータ保護、CERT連携

- ・ネットワークセキュリティの共通的な最低標準を作成
- ・ビジネスの継続性と災害対応におけるベストプラクティスモデルを全業界に渡って作成
- ・CERT連携や知見の共有等を推進 (ASEAN Network Security Action Council の設置)
- ・データおよび情報インフラを保護する活動のベストプラクティスを共有

5.2 人材育成の更新と認定制度

- ・ICTスキルセットの見直し (サイバーセキュリティ専門家等)

<http://www.aseansec.org/documents/ASEAN%20ICT%20Masterplan%202015.pdf>

ASEANの情報セキュリティに係る政策動向

	国家戦略	CERT	意識啓発
日本	国民を守る情報セキュリティ戦略	JPCERT/CC他多数	
ブルネイ 	E-Government Strategic Plan 2009-2014	BruCERT 	
カンボジア 	なし	CamCERT 	×
インドネシア 	なし	ID-SIRTII 	
ラオス 	National Information and Communication Technology Policy No. 057	LaoCERT (2011年立ち上げ予定)	
マレーシア 	National Cyber Security Policy (NCSP)	MyCERT	
ミャンマー 	ICT development master plan and action plan (2006 2010)	mmCERT	
フィリピン 	National Cyber Security Plan	PH-CERT 	
シンガポール 	Infocomm Security Masterplan 2	IDA	
タイ 	National ICT Security Master Plan 2009-2013	ThaiCERT 	
ベトナム 	National Development Master Plan for Digital Information Security	Vn CERT 	

NationalCERT または GovCERT等

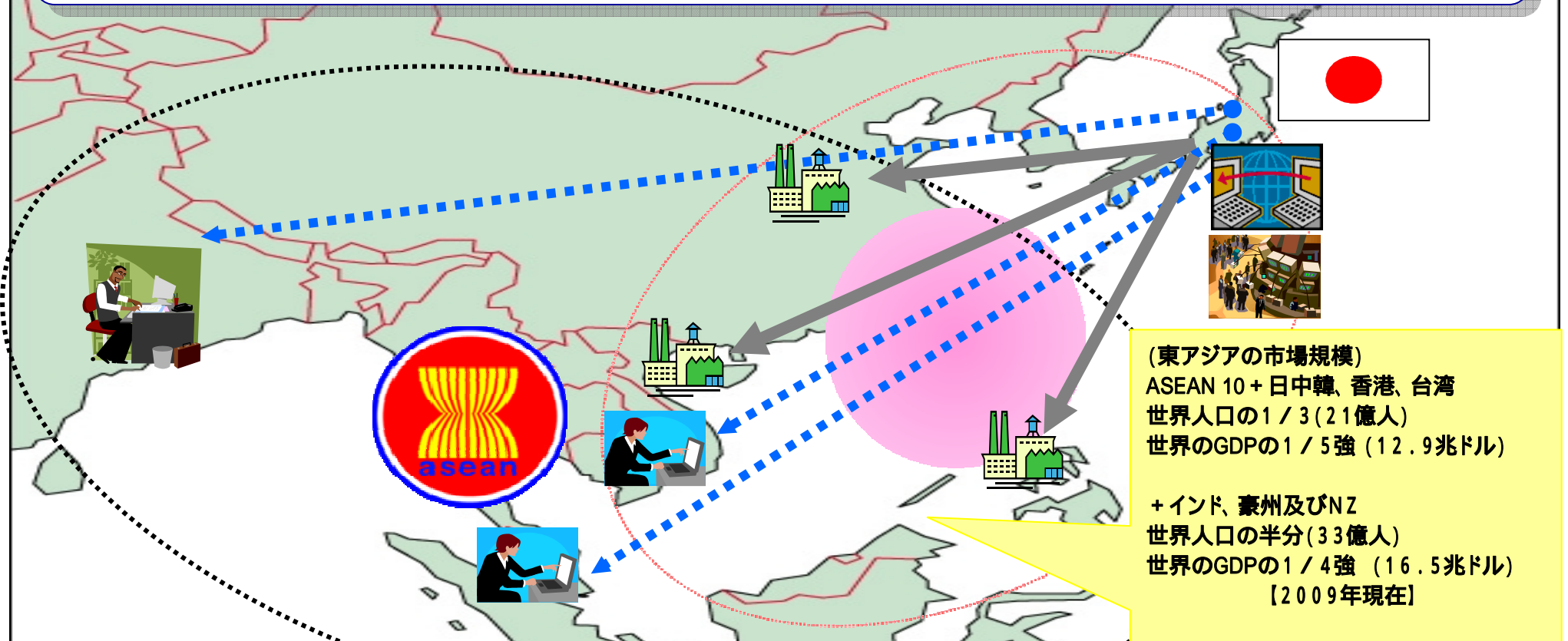
東アジア経済社会における情報セキュリティ面での連携・協力の必要性

東アジアへの日系企業の直接投資の拡大(→), 国際委託の進展(●●●●)

日本の知見・経験の共有による域内での情報セキュリティ対策水準の向上

地域内でのIT障害に起因する国境を越えた被害が発生(○)

域内各国で官民連携して対応を行う枠組みの構築を通じ、情報インフラの信頼性向上



- ・ビジネス活動の基盤である情報セキュリティの国際展開は、経済関係の深化を担保するもの
- ・ASEANとの協力関係を端緒として取組を開始

情報セキュリティに関する日ASEAN連携枠組み合意文書

於：第一回日ASEAN情報セキュリティ政策会議 (平成21年2月25日)

1

セキュアなビジネス環境の醸成

経験の共有と共通の手段の構築

民間部門における技術的能力の開発

人材育成の支援

2

セキュアなICT利用に向けた環境構築

事業者間における協力体制の確立

CERT/CSIRT間連携の強化

人材開発と研究開発

3

政府が主導する情報セキュリティ政策

http://www.nisc.go.jp/press/pdf/aseanj_conf2009_agreement_press.pdf より抜粋したもの

日ASEANの情報セキュリティに関する協力の枠組み

高級事務

日ASEAN情報セキュリティ政策会議

局長・審議官クラスによる、情報セキュリティ分野におけるASEANとの協力枠組み等を議論、決定することが目的
日本では内閣官房情報セキュリティセンター (NISC)、総務省及び経済産業省が共催
第一回 (東京、2009年2月)、第二回 (タイ・バンコック、2010年3月) で開催
第三回 は2011年3月に東京で 開催予定



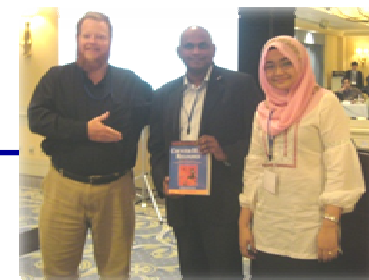
日ASEAN政府ネットワークセキュリティワークショップ

課長クラスを対象とした、政府機関の情報セキュリティ対策についての取組み事項を議論することが目的
NISCが主催
第一回 (東京、2009年10月)、第二回 (ベトナム・ハノイ、2010年12月)
第三回は2011年中に開催予定 (日本)



日ASEAN政府情報セキュリティトレーニング

実務担当者を対象とした、情報セキュリティの政策立案、オペレーションの実務能力向上のためのトレーニング
NISCが主催
第一回 (東京、2010年8月)
第二回は2011年中に開催予定 (日本)



オペレーション担当者
GOVERNMENT等


政策立案担当者

日ASEANにおける情報セキュリティに係る協力の概要

政府情報セキュリティトレーニング (2010年8月、東京)

- NISC主催
- 政策立案コース(4日間)、オペレーションコース(5日間)の2コースを開催
- 政策立案コースは、各国における政策アップデートと、日ASEAN共同の意識啓発に関する議論を実施
- オペレーションコースは、実機操作を含むセキュリティオペレーションに求められる知識を事例を交えて学習し、最終日に効果測定となる演習を実施。


参加者からの声

- 
- ✓ 我が国のインターネット政策において、セキュリティに対する優先度を向上させるに十分な情報が豊富であった。
 - ✓ このコースは非常によく検討されていて、価値のあるコースである。
 - ✓ テキストも判りやすく、演習において提示されるヒントの内容や時期も適切であった。

第二回 政府ネットワークセキュリティワークショップ (2010年12月、ハノイ)

- ベトナム情報通信省(MIC)、NISC共催
- 政府機関における情報セキュリティレベル向上に向けたキャパシティビルディングについての議論
- 日ASEANでの意識啓発共同イベントの内容に関する議論

日ASEAN政策会議に、以下の議題を提言

- 
- ✓ 情報セキュリティに関する「情報セキュリティ成熟モデル」の発展
 - ✓ 情報セキュリティキャパシティビルディングに関するロードマップを発展、決定
 - ✓ 意識啓発に関する共同の取組みを実施