# 新興国における情報セキュリティ
# ～海外進出、オフショア開発等の視点から～

2011年2月26日

株式会社三菱総合研究所
村瀬一郎

# 各国の情報セキュリティの動向

# マルウェアの駆除数（国別）

| | 国/地域 | 駆除されたコンピュータ（1Q10） | 駆除されたコンピュータ（2Q10）） | 変化 |
|---|---|---|---|---|
| 1 | 米国 | 11,025,811 | 9,609,215 | -12.8% ▼ |
| 2 | ブラジル | 2,026,578 | 2,354,709 | 16.2% ▲ |
| 3 | 中国 | 2,168,810 | 1,943,154 | -10.4% ▼ |
| 4 | フランス | 1,943,841 | 1,510,857 | -22.3% ▼ |
| 5 | スペイン | 1,358,584 | 1,348,683 | -0.7% ▼ |
| 6 | 英国 | 1,490,594 | 1,285,570 | -13.8% ▼ |
| 7 | 韓国 | 962,624 | 1,015,173 | 5.5% ▲ |
| 8 | ドイツ | 949,625 | 925,332 | -2.6% ▼ |
| 9 | イタリア | 836,593 | 794,099 | -5.1% ▼ |
| 10 | ロシア | 700,685 | 783,210 | 11.8% ▲ |
| 11 | メキシコ | 768,646 | 764,060 | -0.6% ▼ |

・インターネット上の脅威を考える上で、新興国は無視できない

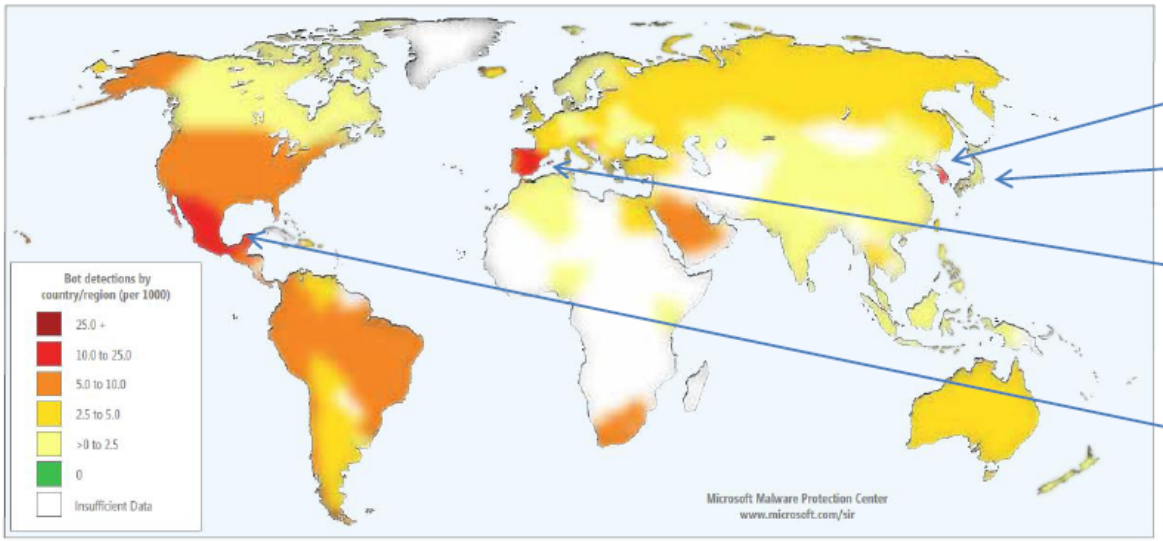
・日本のマルウェア駆除数は他国と比べると少ない

Microsoft_Security Intelligence Report Volume9
January through June 2010
http://www.microsoft.com/downloads/details.aspx?FamilyID=b5f9eddc-70dc-4b11-996b-1bc6987c44b9&displayLang=ja

# マルウェアの感染率

## 世界のマルウェア感染状況から見えてきた課題

Bot infection rates by country/region in 2Q10




**Bot Cleanings Per 1000 MSRT Executions (Bot CCM)**

韓国
14.6台

日本 25か国中トップ
0.6台

スペイン
12.4台

メキシコ
11.4台

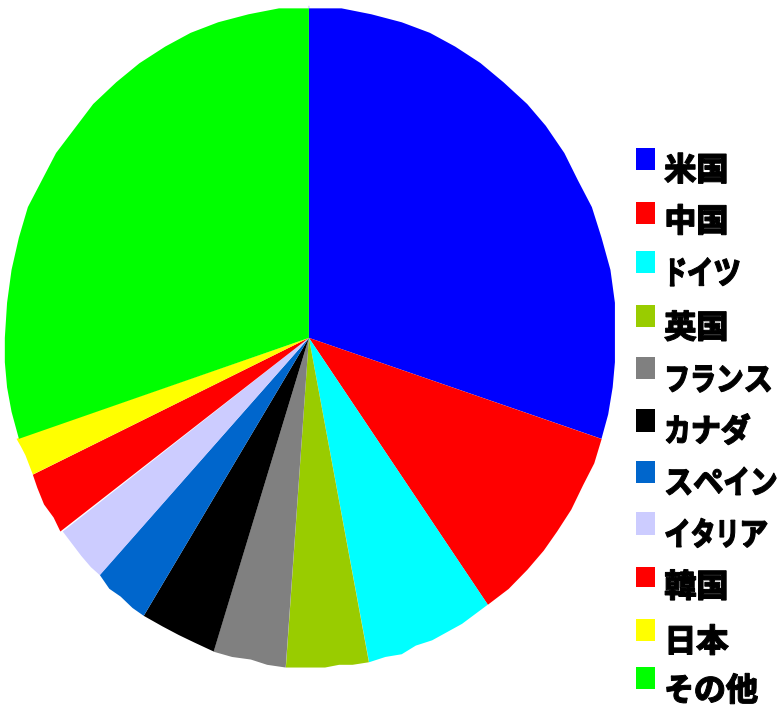
マイクロソフトによる調査（Microsoft Security Intelligence Report Volume9）を基に作成

日本の周辺諸国はマルウェア感染率が高い？
⇒日本だけクリーンになっても常にサイバー攻撃に晒される可能性

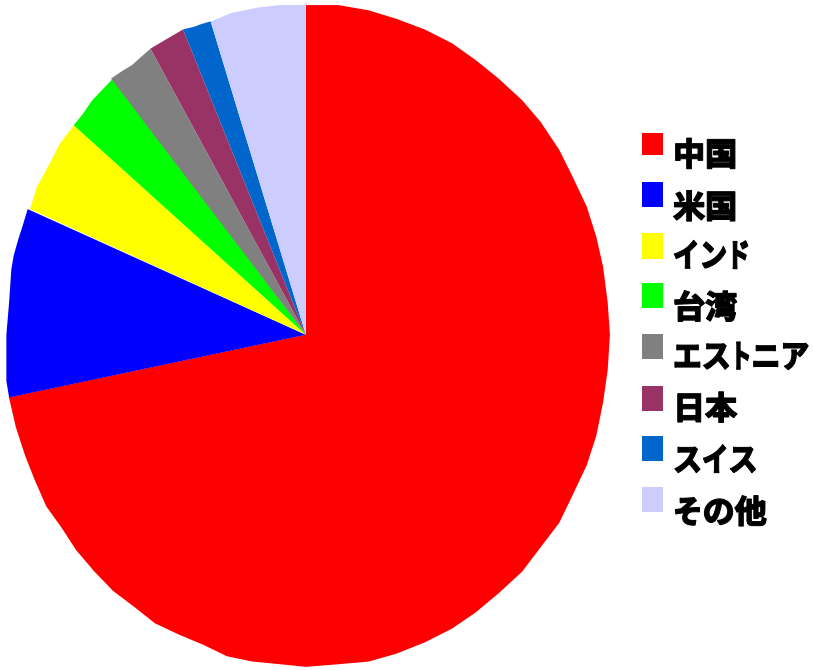
そもそも世界のマルウェア感染状況を同じ指標で正確に把握できているか？

「ボット対策における国際連携は可能か？」 より抜粋 http://yoshioka-lab.sakura.ne.jp/tscf/css2010/5-noritake.pdf

# 日本に対する不正アクセスの発信国




Source：シマンテック




Source：不正侵入検知システムにおける
不正なアクセスの検知分析（警察庁）

# 東南アジア各国の情報セキュリティに関する状況（2009年時点）

| | ウイルス感染による被害 | 機密情報漏洩 | ソフトウエアの不正コピー | 政府における情報セキュリティ対策 | ISPが提供する情報セキュリティサービス |
|---|---|---|---|---|---|
| シンガポール | 広くウイルス感染による被害を受けていたが、対策の推進により、沈静化しつつある | 報告なし（実際に起きていない） | 取り締まりが厳しくなっているため、減少傾向にある | 対策予算が計上され、ファイアウォール、ウイルス対策ソフト、IDSが導入されている | ほぼなされている |
| マレーシア | 増加傾向 | 問題として認識されていない | 同上 | 同上 | 同上 |
| タイ | 同上 | 同上 | 問題として認識されている | 対策予算が計上されていないため、ファイアウォール等の情報セキュリティ対策が導入されていない | ほとんどなされていない |
| ベトナム | 同上 | 同上 | 同上 | 同上 | 同上 |
| フィリピン | 同上 | 同上 | 同上 | 同上 | 同上 |
| インドネシア | 同上 | 同上 | 同上 | 同上 | 同上 |
| カンボジア | 同上 | 同上 | 問題として認識されていない | 同上 | 同上 |

各種資料より三菱総合研究所にて作成

# ソフトウェア不正コピーの実態とその解消による経済効果(2009)

PC用ソフトウェア違法コピー率4年間で10パーセントポイント減少による経済効果の分配

| | 2009年違法コピー率 | 経済効果総額（単位:100万ドル） | 現地シェア額（単位:100万ドル） | 現地シェア比率 |
|---|---|---|---|---|
| **アジア太平洋** | | | | |
| オーストラリア | 25% | $2,253 | $1,582 | 70% |
| 中国 | 79% | $15,966 | $13,469 | 84% |
| 香港 | 47% | $378 | $327 | 87% |
| インド | 65% | $4,662 | $3,526 | 76% |
| インドネシア | 86% | $2,433 | $1,343 | 55% |
| 日本 | 21% | $8,907 | $6,903 | 77% |
| マレーシア | 58% | $1,017 | $788 | 77% |
| フィリピン | 69% | $329 | $223 | 68% |
| シンガポール | 35% | $520 | $389 | 75% |
| 韓国 | 41% | $1,497 | $1,075 | 72% |
| 台湾 | 38% | $531 | $388 | 73% |
| タイ | 75% | $1,297 | $599 | 46% |
| ベトナム | 85% | $1,173 | $713 | 61% |
| **小計** | **59%** | **$40,963** | **$31,325** | **76%** |

ソフトウェア違法コピーインパクト調査 http://portal.bsa.org/piracyimpact2010/studies/piracyimpactstudy2010_japanese.pdf

# 各国の情報セキュリティに関する動向（まとめ）

## 1）機密情報管理に係る傾向

・重要な情報と重要ではない情報の峻別を行う意識・習慣がない
・重要情報が記載・記録された紙や記憶媒体の取扱いに慎重さを欠き、紛失につながる
・重要情報が記載・記録された紙や記憶媒体の紛失に気づかないことがある

## 2）ソフトウェアの違法コピーや各種情報セキュリティ対策に係る傾向

・正規ソフトウエアの価格が現地の所得水準と比較して高額であるという理由により、違法コピーソフトウエアの利用が拡大しており、正規ソフトウエアのみが対象となっている修正ソフトウエアを適用することができず、ウイルス感染が拡大する
・ファイアウォール、IDS、ウイルス対策ソフトウエア導入等の基本的対策がなされないことがある
・USBメモリ等の外部記憶媒体をウイルスに感染したPCに接続した後に、セキュリティパッチが当てられていない違法コピーソフトウエアを使用しているPCに接続するということが繰り返される結果、ウイルス感染が拡大する
・サーバにおけるウイルス対策が適切に実施されていないため、サーバがウイルスに感染し、障害が発生することが頻繁にあり、結果的に、電子メールを含む様々なシステムの可用性が低下している

各国の情報セキュリティ政策における情報連携モデルに関する調査研究　http://www.nisc.go.jp/inquiry/pdf/renkei_model.pdf

# 現地進出日本企業における情報セキュリティの実態

1）現地事業所のトップが情報セキュリティの重要性を理解しておらず、情報システムの管理や情報セキュリティ対策の実施を現地スタッフ任せにすることが多い。そのため、情報システムの管理や情報セキュリティ対策が適切にあるいは全く実施されない

2）機密情報管理とウイルス対策の実態を、現地事業所のトップが把握していないことが多い

3）機密情報管理とウイルス対策の実態を現地事業所のトップが把握していても、それらの問題を経営上の問題と認識していないため、日本の本社からの指示がない限り適切な対応がとられることがない

4）日本の本社においても、情報セキュリティ対策の重要性を認識していない場合が多く、現地事業所に対して情報セキュリティ対策の実施を指示することは少ない

各国の情報セキュリティ政策における情報連携モデルに関する調査研究　http://www.nisc.go.jp/inquiry/pdf/renkei_model.pdf

# 日系企業が東南アジア諸国へ進出する際に考慮すべき項目およびそのリスクの相対的大きさの評価

| | タイ | ベトナム | カンボジア | フィリピン | インドネシア | マレーシア | シンガポール |
|---|---|---|---|---|---|---|---|
| 治安 | 小 | 小 | 中 | 中 | 中 | 小 | 小 |
| 自然災害 | 中 | 大 | 小 | 大 | 大 | 中 | 小 |
| 感染症 | 大 | 大 | 中 | 大 | 大 | 中 | 小 |
| 社会インフラ | 小 | 中（電力に問題） | 大 | 中（電力に問題） | 中（下水道、通信） | 小 | 小 |
| 法制度 | 小 | 中 | 大 | 大 | 大 | 小 | 小 |
| 人材 | 小 | 中 | 大 | 中 | 中 | 中 | 小 |
| 情報セキュリティ | 中 | 中 | 大 | 中 | 中 | 小 | 小 |

各種資料より三菱総合研究所にて作成

1. マレーシア、シンガポール以外の国は情報セキュリティ上のリスクが高い
2. タイ、マレーシア、シンガポールは、治安および社会インフラに関するリスクが小さい
3. カンボジア、フィリピン、インドネシアは、治安に関するリスクが高い
4. ベトナム、フィリピン、インドネシアは、社会インフラの一部に問題を抱えている
5. カンボジア、フィリピン、インドネシアは法制度に関するリスクが高い
6. カンボジアは、治安、社会インフラ、人材、情報セキュリティ上のリスクが高い

各国の情報セキュリティ政策における情報連携モデルに関する調査研究　http://www.nisc.go.jp/inquiry/pdf/renkei_model.pdf

# 東南アジア諸国の産業政策と産業の実態

| | 産業政策 | 産業の実態 |
|---|---|---|
| シンガポール | 金融を中心としたビジネス分野でのアジアにおけるハブを目指し、高付加価値産業を確立する | 欧米の金融機関の進出が盛んであり、また、欧米の製造業が東南アジア地域のヘッドクオータを設置するなど、高付加価値産業が確立している |
| マレーシア | 海外の製造業の研究開発拠点を誘致し、高付加価値産業を確立する | 日本の製造業の研究開発・設計拠点が進出しており、高付加価値産業が確立されつつある |
| タイ | 海外から自動車産業の研究開発・製造拠点を誘致することにより、高付加価値産業を確立する | 人材の育成・確保がボトルネックとなり、研究開発拠点の誘致は進んでおらず、労働集約型産業が中心となっている |
| ベトナム | 海外からハイテク産業を誘致し、高付加価値産業の確立を目指す | ハイテク産業誘致のために必要なスキルを有する人材の育成が進んでおらず、労働集約型産業、高付加価値産業の確立はできていない |
| フィリピン | 欧米企業からの高度なビジネスプロセスのアウトソーシング受託により、高付加価値産業の確立を目指す | 欧米の企業は、高度な業務(ソフトウエアの設計・開発等)をインドに委託し、比較的単純な業務(コールセンターやコーディング) をフィリピンに委託するケースが多いため、高付加価値産業の確立はできていない |
| インドネシア | 雇用吸収力が大きい製造業の下請けなどの裾野産業を誘致し、労働集約型産業を確立する | 裾野産業の誘致は成功しつつあり、日系企業の製造拠点もあるが、まだ十分な雇用吸収力を有しているとはいえない |
| カンボジア | 一次産業と製靴・縫製業等生活必需品に関連する製造業を重視し、労働集約型産業を確立する | 一次産業、製造業ともに十分には育っていない |

各種資料より三菱総合研究所にて作成

# 最近のトピックス

## 1．新興国における法制度

### 1）中国 CCC

海外で生産された暗号化製品（暗号化ソフト）の中国への持込み及び中国での使用については、国家暗号管理機構への申請、許可が必要になります。また、日本 からの出張者が中国に暗号化製品（暗号化ソフトを搭載したノートパソコンなど）を持ち込み、使用する場合も、事前に申請、許可

### 2）インド ソースコード開示

携帯電話向け通信設備を政府に納入する日米欧などの企業に対して、ソフトウエアの設計図に当たる機密情報「ソースコード」の開示を義務付ける規制

## 2．海外への技術移転

トヨタ<7203.T>が中国に研究開発会社を設立、11年4月から一部稼働

2010年 11月 17日 15:57 JST

記事を印刷する | ブックマーク　[−] 文字サイズ [+]

いいね！　ツイートする　0

［東京　17日　ロイター］ トヨタ自動車(7203.T: 株価, ニュース, レポート)は17日、中国の江蘇省常熟市に研究開発会社「トヨタ自動車研究開発センター（中国）」を設立したと発表した。2011年4月から一部稼働し、13年までに主要設備を整える。中国で車両の使用環境や顧客ニーズを調査し商品企画に反映するほか、中国における環境対応車の調査研究や中国向けエンジンの開発などを行う。

新会社の資本金は2億3400万ドル。従業員数200人で立ち上げ、将来的に1000人規模まで拡大する計画。土地面積は234万平方メートル。そのうち建屋が69万平方メートルで、テストコースが74万平方メートル。トヨタは中国の生産合弁会社内に研究開発センターをもつが、新会社を設置することで調査研究を充実させる。

http://jp.reuters.com/article/domesticEquities2/idJPnTK047113820101117



**パナソニックのグローバル採用枠**

パナソニックの場合、10年度新卒採用1250人のうち海外で外国人を採用する「グ ローバル採用枠」は750人だった。11年度は外国人の割合を増やし、新卒採用1390人のうち、「グローバル採用枠」を1100人にする。残る290人 についても、日本人だけを採るわけではない。

# 日本の情報セキュリティ政策の方向性

# 情報セキュリティ分野における日本の国際貢献

**背景**

- **経済活動のグローバル化、ICTを活用した経済活動の高まり**
- **ネットワークのボーダレス性を利用したサイバー攻撃のグローバル化が急速に進展**

**新たな課題**

- **国境を越えた脅威に対する共同対応を円滑に行うため、共通理解の醸成の必要性**
- **情報セキュリティに関する各国の状況を踏まえた上での均一水準の確保の必要性**

# 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

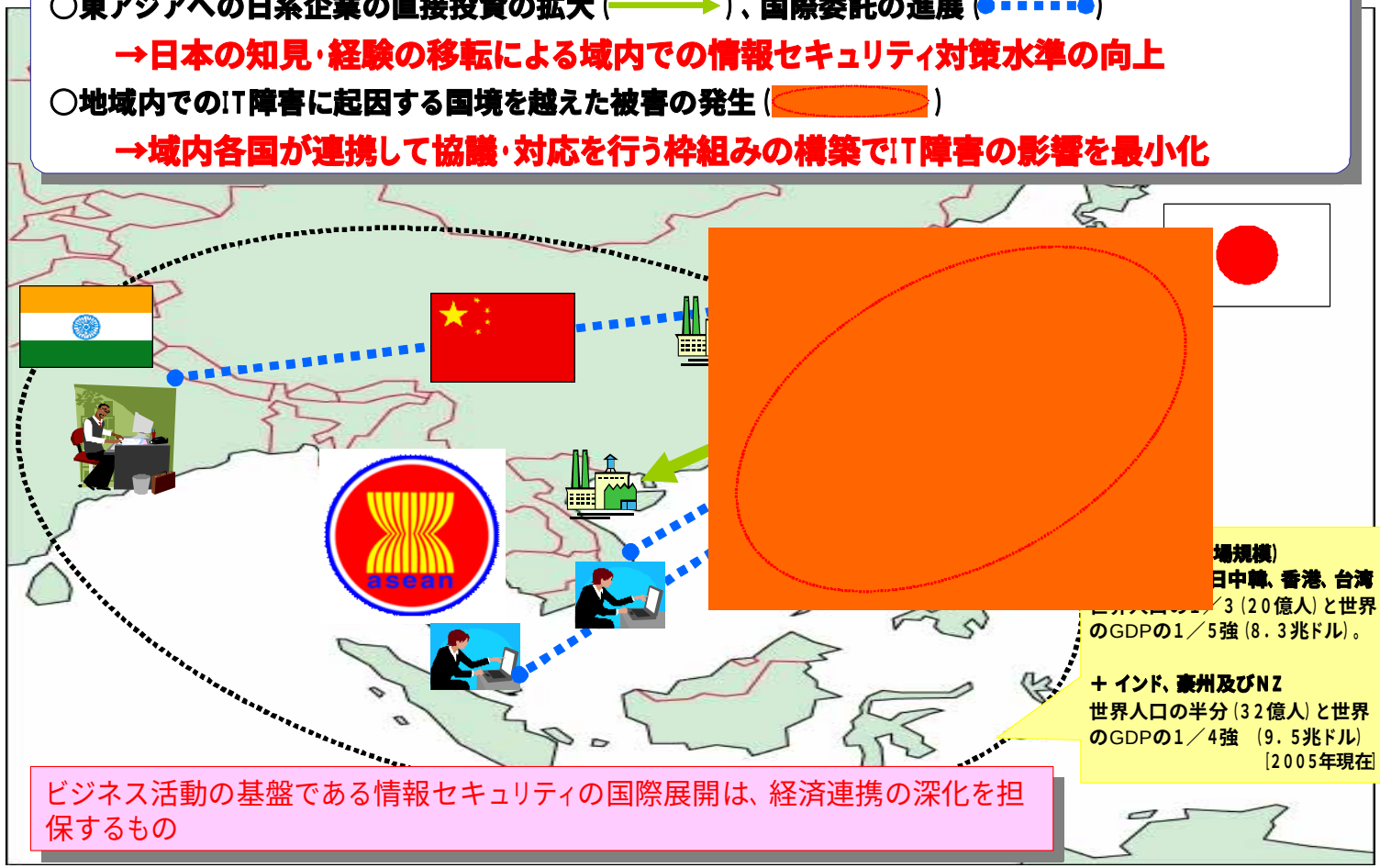
## 東アジア経済社会における情報セキュリティ面での連携・協力の必要性

○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・経験の移転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の発生（　　）

→域内各国が連携して協議・対応を行う枠組みの構築でIT障害の影響を最小化




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、経済連携の深化を担保するもの

# 日本の情報セキュリティ分野における国際貢献・強調の方向性

## 1) 経済関係の深化が進む東南アジア地域のビジネス環境向上に向けた協調・貢献の推進

(セキュア・アジアビジネス環境 (Secure Asian Business Environment) 構想)

・情報セキュリティ文化の醸成や情報セキュリティ水準の向上等を通じ、企業が安全・安心に事業活動を行うことができる環境の整備

・人材育成や意識啓発、情報セキュリティ対策のベストモデルの普及等の協調・貢献を行うとともに、域内各国による自発的な意識啓発活動を促進

## 2) 情報セキュリティに係る新しい諸権利に係る検討及び議論への貢献

・自由なIT利用との関係や、IT利用に起因するインシデントによって被害を受けた者の救済等の観点から、グローバルな議論に貢献

## 3) サイバー攻撃等、ICTに起因する脅威への対応のための取り組みの推進 (リスクのないICT (ICT Risk - Free) 構想)

・サイバー攻撃等、ICTに起因する脅威に関して、高級事務レベル等で問題意識を共有し、適切に対処すべく、多国間での議論に積極的に参加・貢献

・国境を越えたサイバー犯罪対策について、多国間における議論を引き続き促進

## 4) 情報セキュリティに係るグローバルなルールや標準の策定への貢献

・我が国の情報セキュリティに関する取り組みの優れた点を把握し、ベストプラクティスとして活用できるような取り組みルール等を明確化

・国際的なフォーラム等での議論に積極的に参加し、貢献

## 5) 様々な国際フォーラム等における提案や議論への積極的な参加

・必要な情報を適時適切に入手できるよう、既存のグローバルな取り組みについても、より積極的に参加・関与

・国際協力・貢献の一環として、多国間のフォーラムの開催場所として貢献するなど、多国間のフォーラムを主導すべく努力

各国の情報セキュリティ政策における情報連携モデルに関する調査研究　http://www.nisc.go.jp/inquiry/pdf/renkei_model.pdf

# 東南アジア支援のための具体的施策

## 1) 東南アジア諸国における製造業の強化のための支援

•海外企業による東南アジア諸国への投資に関係するルールの整備に関する現地政府への働きかけ
•現地日系企業の経営陣に対する現地の実情に合致した情報セキュリティ対策の必要性に関する普及啓発
•現地日系企業および現地企業が基本的な情報セキュリティ対策を実施する際に参照するガイドラインやベストプラクティス集の策定
•情報セキュリティ意識を有する現地労働人材育成のための支援
•現地日系企業からの情報セキュリティに関する問い合わせを受けるヘルプデスクの設置
•金融分野におけるいわゆる投資ではなく、企業が現地で事業活動を行うために資金や従業員等のリソースを投入する事を指す

## 2) 東南アジア諸国における高付加価値産業の創出

•情報セキュリティ意識を有する研究開発分野・マーケティング分野における人材の育成支援
•知的財産保護や営業秘密保護を含む企業間の適正な競争環境確立のための支援
•サプライチェーンを対象とした情報セキュリティ対策のための基盤整備
•従業員を対象とした情報セキュリティ教育および情報セキュリティ意識向上のための研修等の実施

## 3)日本と東南アジア地域全体の社会継続性確保に向けた重要インフラおよびICT環境の整備

•通信インフラの整備に重点を置いた、各国の実情を考慮したセキュアな重要インフラ整備の支援
•各国政府のICTインフラ整備の支援
•通信事業者における情報セキュリティ対策の向上を目的とした、通信事業者間の連携の活性化支援
•通信障害や情報セキュリティインシデントが発生した場合の対処・復旧手順等をまとめたBCPの作成支援およびその実効性を高めるための訓練の実施支援
•政府機関および重要インフラ事業者における情報セキュリティ文化の醸成

各国の情報セキュリティ政策における情報連携モデルに関する調査研究　http://www.nisc.go.jp/inquiry/pdf/renkei_model.pdf

# 現地研究開発における3つのモデル

1．最先端技術移転しないモデル
現地向けの研究開発のみ行う

2．お任せモデル（アップルモデル）
部品や製造技術には関与せず、現地に任せる

3．グローバル企業モデル（IBMモデル）
国境は意識せず、グローバル企業内で情報管理を実施する