平成 20 年度内閣官房情報セキュリティセンター委託調査

平成 **20** 年度

「各国における情報セキュリティに対する取り組みに関する調査」

～ 情報セキュリティ分野における国際協調・貢献 ～

概要

2009 年 **3** 月

株式会社三菱総合研究所

(1) 情報セキュリティ分野における国際協調・貢献に関する研究会について

2008 年 6 月 19 日に発表された「セキュアジャパン 2008」において、政府・自治体、重要インフラ、企業、個人の各主体横断的な情報セキュリティ基盤の形成のための活動として、情報セキュリティ技術戦略の推進、情報セキュリティ人材の育成、犯罪の取締り及び権利利益の保護・救済に加え、情報セキュリティ分野における国際連携・協調が挙げられている。特に、2008 年度においては、2007 年度に策定した国際協調・貢献に取り組むための基本方針の具体化を行うことが明記されている。

2009 年 2 月 24 日、25 日の両日、「第 1 回 日・ASEAN 情報セキュリティ政策会議」が、インドネシア、カンボジア、タイ、フィリピン、ブルネイ、ベトナム、マレーシア、ミャンマー、ラオスの各国の参加により開催され、「情報セキュリティ分野における日・ASEAN の連携枠組み」を活用して情報セキュリティ分野における連携を行うこと、および、日本が、2009 年から 2012 年にかけて、「情報セキュリティ分野における日・ASEAN の連携」を実行するために必要な支援を行うことが合意された。

こうした背景の下、「セキュアジャパン 2008」に明記された「国際協調・貢献に取り組むための基本方針の具体化を行う」という課題への取り組みを推進するために、情報セキュリティ分野における国際協調・貢献に関する研究会が設置された。本研究会の目標とする成果は、情報セキュリティ分野における国際協調・貢献の方向性を明確化し、個別施策の実施戦略を具体化することである。

計 5 回開催された研究会では、事務局が実施した文献調査および ASEAN 諸国・日本国内におけるヒアリング調査により得られた情報を材料として、委員である情報セキュリティ分野の有識者から意見をいただくとともに、情報セキュリティの分野だけにとどまらない広範囲にわたる検討が行われた。

(2) 情報セキュリティ分野における国際協調・貢献に向けた取り組みの方向性

「セキュアジャパン 2008」をもとに[1]、東南アジアの情報セキュリティ分野における国際協調・貢献に向けた取り組みの方向性を以下のように設定する。

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

[1] 「セキュアジャパン 2008」には、国際連携・協調の施策として、「国際的な安全・安心の基盤づくり・環境の整備への貢献」、「情報セキュリティ領域での我が国発の国際貢献」が述べられており、具体的施策として上記１）－５）に関連する事項が記述されている。

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

(3) 東南アジア諸国における各種のリスクに関する状況

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として、治安、自然災害、感染症、社会インフラ、法制度、人材、情報セキュリティを想定すると、東南アジア各国の各種リスクに関する概要は以下のようになる。

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

(4) 各国の情報セキュリティに関する動向

シンガポールとマレーシア以外の東南アジア諸国においては、全般的に日本より情報セキュリティに対する意識・関心が低く、特に、企業活動の根本となる情報管理と機密情報漏洩に関する意識が低いという問題点があることが判明した。また、7 カ国全てにおいて、特に中小企業の経営者が、情報セキュリティ対策の必要性を認識しておらず、中小企業における情報セキュリティ対策が進んでいないことが明らかとなった。

具体的には、以下の傾向があることが明らかとなった。

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、電子メールシステムを含む様々なシステムの可用性が低下している

日本とは異なる社会的・文化的背景として特に留意すべき項目として、たとえば、マレーシアにおいて実施されている政策で、企業や官公庁において、民族ごとに一定の人数を雇用することを義務付ける政策がある。同様の原理が情報セキュリティ対策においても適用されるため、海外資本の企業が現地の人間を従業員として採用している場合、その従業員が離職する際に、情報セキュリティに関するルール(転職時の情報の持ち出し禁止等)を遵守させることができないという状況がある。

(5) 現地の日本企業における情報セキュリティの状況

東南アジア諸国に進出している日本企業のうち、ヒアリング調査を実施したいくつかの企業では、以下に記すような情報セキュリティ対策上の問題を抱えていることが明らかに

なった。

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施状況を、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

現地進出日本企業における情報セキュリティ上の問題は、現地事業所のトップが情報セキュリティ対策の重要性を理解しておらず、また、現地の情報セキュリティや各種のリスクに関する実情を把握していないことと、日本の本社が情報セキュリティ対策の重要性を認識していないことに起因して発生しているケースが多い。

(6) 東南アジア諸国における製造業の強化のための支援

東南アジア諸国における日本企業の現地製造拠点の強化のためには、日本企業および現地企業が製造・生産ノウハウに関する情報の管理・保護と、製造ラインの自動化や管理を行うための情報システムの安全性と可用性を確保するための施策が重要となる。現地企業を対象としたヒアリング調査の結果、現地の日本企業(特に中小規模の企業)の情報セキュリティ対策が必ずしも十分でないこと、現地企業における情報セキュリティ対策の実施を現地スタッフに任せた結果、適切な対策が実施されていない(本社のガバナンスが効いていない)といった問題点があることが明らかとなった。また、情報セキュリティ対策は、利益を生み出さないコスト要因として認識される傾向にあることから、その実施を東南アジア諸国の企業に包括的に要請していくためには、企業ごとに取り組みの推進を図るといった手法では限界があると考えられる[2]。

情報セキュリティ対策を着実に実施していく上では、当然のことながら対策を実施するスキルを有する人材の育成という観点は欠かせない。したがって、今後、東南アジア諸国の企業における情報セキュリティ対策の向上のためには、現地の日本企業における情報セキュリティ対策の徹底をはじめとして、現地企業の情報セキュリティ対策の実施を促進するためのインセンティブ付与、現地の日本企業の要求を満たすスキルを有する労働人材の

[2] 企業間の力関係によって、たとえば、委託元の企業規模が委託先よりも小さい場合には、委託先に対して情報セキュリティ対策を強制することが難しいといったケースがあると考えられるため

育成、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などの施策が有効であると考えられる。

具体的には、以下の取り組みが考えられる。

- 海外企業による東南アジア諸国への投資[3]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

(7) 東南アジア諸国における高付加価値産業の創出

東南アジア諸国において、各国の市場の開拓・獲得を目的としたマーケティング・研究開発を安全かつ効果的・効率的に行うためには、現地日系企業および現地企業において、研究開発・マーケティングを行う上で核となる重要情報の管理の重要性を理解し、管理を適切に実行することができる研究者や技術者あるいはマーケティング担当者の育成、研究開発の成果である知的財産やマーケティングの成果である営業秘密を保護するための法律の整備および制度や体制の構築、研究開発の成果を品質面で担保するための製品の信頼性・可用性・安全性の保証等を促進する施策の実施、製品が複数の企業によって製造される場合に、その製造過程(サプライチェーン)に関わる全ての企業や組織を対象とした情報セキュリティ対策の実施が重要である。

現地企業を対象としたヒアリング調査の結果、従業員の離職に際して情報漏えいが発生する傾向が高いという問題点が明らかとなった。すなわち、現地日系企業で基礎的な研修を受け、業務に従事していた研究者が他の企業に転職する[4]際に、就業規則や雇用契約書に業務上知りえた重要情報の取扱いを制限する条項が含まれていたとしても、当該国においてそれを担保する法律が整備されていない、あるいは、訴訟を起こしても企業側が勝てるような社会状況ではないといった理由により、人材の流出に伴って、他社に重要情報が漏えいすることを防ぐための有効な手段をとることができないのが現状である。

東南アジア各国の高付加価値産業への移行・育成を図る上では、上記の施策に加え、明らかとなった課題を解決するための施策を実施することが必須である。

それらの施策をまとめると、以下のようになる。

---

[3] 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

[4] 現地における企業間の人材の流動性は、一般的に日本よりも高い

- 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

(8) 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

日本と東南アジア地域全体における社会活動や経済活動の継続性を確保するためには、重要インフラの事業継続性の確保や各種オンラインサービスを提供するためのインフラとしての ICT 環境の信頼性・可用性の向上が求められる。現地企業に対するヒアリング調査の結果、東南アジア諸国に進出している、あるいは東南アジア諸国と取引を行う日本企業から、重要インフラの中でも特に、情報通信インフラの信頼性・可用性の低さや回線の帯域幅の少なさ、さらには、少数の事業者がサービスを寡占的に提供していることによる価格の硬直性といった項目が問題点として指摘された。このことから、東南アジア地域における社会継続性の確保のために、情報セキュリティ対策の実施だけでなく、物理的な面を含めた全てのリスクへの対処、コストパフォーマンスの高い通信ネットワークの構築といった課題に対して、我が国の取り組みに比肩するような高いレベルでの取り組みが期待されていることが明らかとなった。

そのような取り組みを実施するためには、政府間、通信事業者間での連携体制を強化し、それぞれが保有するベストプラクティス等の知見の供与・共有が求められてくる。このような取り組みは、中長期的には、通信インフラに限らず、情報システムへの依存度を高める政府および全ての重要インフラ事業者においても同様に求められるものであるが、東南アジア諸国における情報セキュリティ対策の実施状況は、現時点では国によって大きく異なることから、まずは当該政策を行う政府機関同士の連携を強めることで、各国における情報セキュリティ文化の醸成を図る必要がある。

具体的には、以下の取り組みが考えられる。

- 特に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