ASEAN地域の情報セキュリティの課題
―現地の事情を考慮した実効性のある対策とは―

ASEAN地域では、少ない例外はあるものの、総じて情報セキュリティが日本や欧米のようには根付いていない。その背景には新興国ならではの事情もあり、その点を考慮しないと情報セキュリティ対策の実効性はなかなか高まらない。本稿では、日本や欧米とは異なる現地の特徴を考慮した対策の要点について考察する。

野村総合研究所 システムコンサルティング事業本部
産業ITコンサルティング部 上級システムコンサルタント
村上 俊輔（むらかみ しゅんすけ）
専門はシステム化構想・計画策定、グローバルITガバナンス

ASEAN地域における情報セキュリティの現状

海外に事業拠点を持つ多くの日本企業が、現地拠点の情報セキュリティ対策に苦心している。特にASEAN地域における情報セキュリティについて、日本本社のIT部門責任者、情報セキュリティ担当者の方から悩みを聞くことが多い。

ところで、ひと口にASEAN地域といっても、ITや情報セキュリティの観点からは2つのグループに分けられる。

1つ目のグループにはインドネシア、タイ、マレーシア、フィリピン、ベトナムが含まれる。多くの日本企業がすでに拠点を置いている国々であり、現地メンバーの教育や啓発、ポリシー策定、ツール導入などの対策が講じられているが、情報セキュリティがなかなか根付かないというのが現状のようである。

もう1つのグループにはカンボジア、ラオス、ミャンマー、ブルネイが含まれる。日本企業が進出して間もないか近い将来進出を予定している国々で、情報セキュリティ以前にITリテラシーの教育を優先されなければならない段階である。

本稿で述べるASEAN地域は1つ目のグループの国々を意識しているが、2つ目のグループの国々でも日本企業の進出が進んだ段階で同じ問題が出てくることは言うまでもない。なお、シンガポールは新興国の部類に属さず、個人情報保護法も日本より早く整備されるなど情報セキュリティ対策が進んでいるため、本稿では対象外とする。

まず、ASEAN地域の現地拠点における情報セキュリティの現状を表す事例を2つ紹介しよう。

製造業のA社では、過去数年にわたり日本本社が主導して現地拠点に対して情報セキュリティポリシーの策定と展開、啓発や教育を実施してきた。本社では基本的な対策を終えたと判断し、実際の運用は現地拠点に任せていた。本社としてもある程度安心していたその時、ある拠点で情報セキュリティ事故が発生した。原因を調査すると驚くべき事実が明らかになった。拠点の担当者がポリシーを独自の判断で変更し、マニュアルの内容も併せ

て変更していたのである。

同じく製造業のB社では、ある部門長が現地の他の企業に転職した際、退職前に会社の機密情報を自分の個人メールアドレスに送っていたことが発覚した。その後の調査によると、部門長だけでなく組織ぐるみで行われていた可能性もあるという。

この2つの事例は氷山の一角であり、ほとんどの日本企業は情報セキュリティ対策に苦心している。

情報セキュリティが根付かない原因

ASEAN地域の拠点で情報セキュリティが根付かないのは、以下の3つが主な原因であると思われる。

(1) 経験の少なさ

現在では、情報セキュリティは「性悪説」に基づくべきだという考えが受け入れられているが、上に挙げた2つの事例は、人間を本来的に弱い生き物とする「性弱説」で考える必要もある。ただし、ここで言うところの「性弱説」は限定的なもので、あくまでも情報セキュリティのルールを順守する意識の弱さを表すものとする。

A社の場合、策定したポリシーやルールを勝手に変えてしまった担当者に悪意があったわけではなく、拠点の業務を効率的に進めることを優先して、つい情報セキュリティを後回しにしてしまったのであろう。B社の場合は確信犯であったかもしれないので「性悪説」が浮かんでくるが、それでもルールを守るという意志が相対的に弱かったことは間違いない。

情報セキュリティのルールが守られにくいのは文化や国民性の問題ではなく、ASEAN地域ではまだ情報セキュリティの取り組みが浅いという、時間や経験の問題と考えるべきである。日本においても、一昔前は現在のように情報セキュリティの意識がそれほど高かったわけではない。会社のPCを当たり前のように個人目的で利用し、本番システムに対するアクセス管理も現在と比べると厳密なものではなかったはずである。従って、ASEAN地域の情報セキュリティレベルも時間がたてば上がっていくと考えられる。だからといって、情報システムへの攻撃がかつてと比較にならないほど多くまた高度化している今、それを待っているわけにはいかない。

(2) 組織体制の不備

人材の流動性も影響を及ぼす。担当者の離職は日本でも珍しくはないが、問題は情報セキュリティを担当する社員の離職が及ぼす影響の大きさである。日本や欧米では情報セキュリティ専門の組織・チームを設置していることが多く、1人の担当者が離職しても組織・チームで穴を埋めることができる。しかしASEAN地域の現地拠点では、その規模にもよるが、情報セキュリティ専門の組織がなく、情報システムの担当者が他の業務と兼任で担当し、しかも担当者が1人だけというケースが多い。その担当者が離職してしまうと急いで別の社員を担当者として教育しなければならず、その間の対策に不備が生じる可能性は低くない。

(3) 日本本社のガバナンス不足

事例に挙げたA社の場合、情報セキュリ

ティポリシーを変えた社員がいたこと、変えることができたこと（運用ルールの徹底不足）に加えて、変えたことに日本本社が気付かなかったという問題もある。B社の場合も、ルール違反に気付かなかった点では同様である。すなわち、現地社員や組織体制の問題であるだけでなく、日本本社のガバナンスの問題でもあるわけだ。現地に駐在している日本本社からの担当者も2～3年周期で入れ替わることが多く、心のどこかに「自分が駐在している間に問題が起きさえしなければよい」という考えがある可能性も否めない。これもガバナンス力を弱める原因になり得る。

「性弱説」に基づいた実効性のある対策を

ASEAN地域の現地拠点において情報セキュリティがなかなか根付かない理由として大きく3つの問題があると述べた。あらためて整理すると次のようになる。

①人の問題

情報セキュリティのレベルは経験など時間軸の問題でもあり、現時点では「性弱説」を意識すべきである。

②組織体制の問題

日本や欧米と異なり、情報セキュリティを専門とする組織がない。

③日本本社のガバナンス力の不足

日本本社はポリシーの策定までは行うが、実際の運用を現地任せにする傾向がある。

この3つの問題を踏まえて、ASEAN地域の拠点における情報セキュリティ対策の改善について考えてみよう。

(1) 情報セキュリティ対策ツールの活用

新興国において情報セキュリティ対策が根付かない3つの問題を解決する手段の1つとして、情報セキュリティ対策ツールの活用が有効である。

まず組織体制の問題について言うと、新興国各拠点の組織体制を強化することは現実的には非常に難しいと思われる。現在の体制は、各拠点の規模、人的リソース、投入可能なコストに応じたものであり、余裕があればすでに対策を講じているはずだからである。このような状況下での1つの工夫として、日本本社からリモート監視が可能な情報セキュリティ対策ツールを導入することで、各拠点の体制を変えることなくバーチャルな情報セキュリティ組織を築き、各拠点の対策を強化するやり方が挙げられる。

ある企業では、新興国向けの情報セキュリティガバナンスを強化するため、情報セキュリティ規定をポリシー、スタンダード、プロシージャーの3段階に分けて策定している。また、これらの規定は教育や啓発だけでは根付かないと考え、情報セキュリティ対策ツールを組み合わせて現地社員の気付きを促す仕組みとしている。例えば、アクセス権限を持たないファイルサーバーにアクセスしようとすると、「アクセス権がないサーバーへのアクセスはセキュリティ規定違反となります。セキュリティ規定○○を再度確認してください」といったメッセージが表示される。何が問題かを本人に確認させながら、業務の中で教育や啓発の効果を高めているのである。

最後に人の問題についてである。ガバナンス力強化の事例にもあるように、新興国拠点

の現状が表しているのは、いくら対策を強化したとしても、人の問題を解決できない限りその対策を根付かせるのは難しいということではないだろうか。情報セキュリティ規定を整備し、根気強く教育を続けることはもちろん重要だが、それと並行して「性弱説」を意識した対策を実施することが必要となる。

その意味でもやはり、日本や欧米以上に情報セキュリティ対策ツールを活用することが重要なポイントとなる。ツールを使えば、ファイルサーバーのアクセス権限を日本本社以上に細かく規定したり、ハードディスクが抜かれてしまっても困らないように中のデータを暗号化したりすることもできる。ツール導入後の運用では、管理者権限を持ったメンバーを日本本社のみに限定し、現地で設定を変更できないようにすることもできる。このように、情報セキュリティ対策ツールの活用は、人の問題（情報セキュリティの意識の問題）だけでなく、組織体制やガバナンスの問題の解決にも有効である。

(2) コスト問題の解決策

ASEAN地域の現地拠点に情報セキュリティ対策ツールを導入するためには、コストの問題を解決しなければならない。現地拠点の予算が限られているために、導入したくてもできない企業も多いであろう。

この問題を解決するために、以下のような工夫をしている企業がある。

①日本本社の予算で対策する

日本本社の予算で現地拠点を援助している企業がある。現地拠点のコスト的な負担が軽減されるとともに、本社主導の対策がやりやすくなるという利点がある。

②現地拠点の負担を業績評価に加味する

日本本社が予算を持つ場合でも、全ての費用を本社が負担することには、日本や現地の税法上の問題がある。そこで、各拠点側にも部分的に費用を負担させている企業がある。本社では、拠点の業績を評価する際に、負担した費用も売り上げや利益に加味するなどして現地拠点の対策を促している。

ASEAN拠点における情報セキュリティの確立に向けて

情報セキュリティに関する法制度は、当然ながら各国で違いがある。個人情報保護法だけ見ても、当局への届け出義務の有無や、罰則の有無などばらばらである。従って、前述の対策をいざ実施しようとすると、国による法制度の違いを把握して適切に対応する必要が出てくる。

野村総合研究所（NRI）がNRIセキュアテクノロジーズと共に海外進出企業に対して行った支援の経験を踏まえると、情報セキュリティ対策には次のような課題を国ごとに1つ1つ解決していくことが不可欠である。

①最新の法規制への対応
②法規制が与える影響の評価と情報セキュリティ対策への反映
③最適な情報セキュリティ対策ツールの選定
④限られた人的リソースによる導入後の運用

これらを企業が独自に行うことは容易ではないだろう。新興国における情報セキュリティ対策の知見と経験、組織的に支援できる体制を有する外部の専門家と共に取り組むことをぜひお勧めしたい。 ■