グローバルセキュリティ統制の勘所
―絵に描いた餅で終わらせないために―

NRIセキュアテクノロジーズが毎年実施している「企業における情報セキュリティ実態調査」（以下、「実態調査」）で、セキュリティレベルの国内外の格差が明らかになった。本稿では、日本をベースにした完璧なはずのセキュリティ統制計画がグローバル展開に失敗する現状を紹介し、異文化理解を踏まえた施策展開の大切さについて筆者の経験を基に考察する。

セキュリティレベルにグローバル格差

本稿では、グローバルセキュリティ統制を「日本企業が自社・自グループの海外拠点向けに情報セキュリティ対策を計画し、これを展開・浸透させること」と定義する。多くの日本企業がグローバル化を進める一方で、事業の成長スピードにグローバルセキュリティ統制が追い付かず、国内外のセキュリティレベルに差があることが指摘されてきた。

2013年に実施した「実態調査」で、その格差の実態がはっきり確かめられた。海外拠点に対するセキュリティ統制ができていると回答した企業は、支店で46.8%、連結子会社で43.4%と半分以下にとどまり、国内拠点との違いが明らかである（図１参照）。

グローバルセキュリティ統制を阻む要因

ここで、グローバルセキュリティ統制の具体的な課題に着目してみよう（表１参照）。

海外拠点におけるセキュリティ統制上の重要課題は、意識の低さや担当者の兼務など、要員の確保やリテラシーに関するものであり、体制面の強化が必要という結論に落ち着く。しかしながら、これは一筋縄ではいかない問題である。筆者の経験に照らすと、グローバルセキュリティ統制に悩みを持つ企業には次のような共通点がある。

①国内拠点のベストプラクティスをベースに高度な統制計画を策定しがち

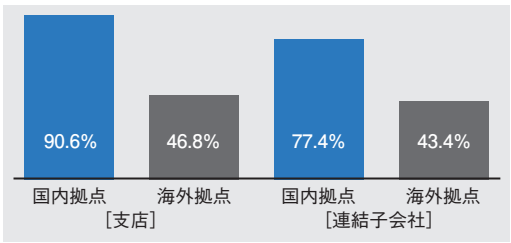
②展開対象となる地域・国の文化的な特性とその差異を考慮することを忘れがち

すなわち、日本人の特性といわれる勤勉さや究める精神によって策定された完璧なはずの統制計画が、海外のさまざまな地域特性に阻まれて現地に浸透せず、役に立たない計画（絵に描いた餅）となってしまうのである。

ASEANに見られる地域特性

地域特性について、早くから日本企業の進出先となったASEAN（東南アジア諸国連合）を例に考えてみよう。ASEAN全体では、次の３つの特性が挙げられる。

図１　セキュリティ統制が取れていると感じる企業



NRIセキュアテクノロジーズ
コンサルティング事業本部
ストラテジーコンサルティング部長
足立道拡（あだちみちひろ）

専門は情報セキュリティ対策に関するコンサルティング全般

①人材流動性の高さ

人材流動性の高さはASEANの顕著な傾向で、さまざまな背景を持つ人が次々とやって来る。新たに入ってきた人へのセキュリティ教育はもちろん大切だが、筆者は、一律のルールで縛るのは逆効果と考えている。どうしてもルールにせざるを得ないものは必要最低限の項目に絞り、禁止事項だけでなく順守事項を明確にすることが大切である。

表1　海外拠点の課題トップ5（複数回答）

順位	課題	割合	国内での順位
1	現地のセキュリティ意識が低い	60.0%	2位
2	拠点担当者が兼務のため、セキュリティ業務がおろそかになりがち	54.7%	1位
3	IT機器・サービスの調達・仕様の全体最適化が困難	50.4%	5位
3	セキュリティルール類の整備が困難	50.4%	6位
5	IT利活用のモニタリング・資産管理が困難	50.1%	4位

②セキュリティリテラシーの不足傾向

現地の人員のリテラシーが必ずしも高くないことを前提に対策を考えたい。欧米では「悪意のある人」が脅威の前提だが、ASEANでは「リテラシー不足の人」を脅威の前提とすべきである。例えば、ASEANの一部ではマルウェアの混入などセキュリティリスクが高いはずの違法コピーが会社への貢献（コスト削減）と認識されることがある。こうした認識を改めるべく、現地の日本人従業員が日本らしい工夫をしている例を目にした。江戸時代の高札（法令を記した立札）を模したイラストで現地従業員に「違法コピーの禁止」を訴えたのである。見た人の記憶に残りやすく、日本の文化に興味や関心を持つ現地従業員に大変に好評だったという。

③国と文化の多様性

国によって経済的な格差があり、シンガポールではPCやソフトウェアなどの調達は問題ないが、それ以外の国では現地では調達が難しい場合がある。セキュリティもカスタマイズが必要である。例えば、中国系の社会では、夕食を自宅で家族と食べ、その後で自宅で仕事をするという文化がある。会社貸与のPCを持ち出すニーズが高いため、それに応じたセキュリティ対策が重要になる。

海外拠点の現状を出発点に

ある大手グローバル企業でセキュリティ統制を担当されている方が「海外拠点の現状を肯定するところから始める姿勢こそが大事」と話されていた。まさに金言であり、この姿勢こそ事業のグローバル展開の大前提に据えられるべきである。最後に、グローバルセキュリティ統制の手順である「計画、展開、浸透」に沿って心構えを整理しよう。

①最低限のベースライン定義（計画）
②現状肯定とスモールスタート（展開）
③システム化と伝え方の工夫（浸透）

本稿がグローバルセキュリティ統制検討の一助となれば幸いである。 ■