トピックス

グローバル企業のセキュリティ管理戦略

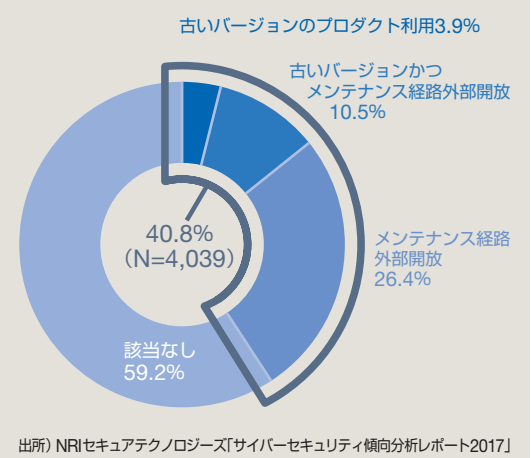
グローバル企業のセキュリティ統括部門は、事業領域・事業規模・企業文化が異なる各グループ企業に共通の、グローバルWebセキュリティ管理プログラムの構築が求められている。本稿では、グローバル企業がセキュリティ管理プログラムを構築・運用する際に直面する問題点、対応するセキュリティ統括部門が持つべき役割、運営のポイントについて解説する。

NRIセキュアテクノロジーズ サイバーセキュリティサービス事業本部
サイバーセキュリティサービス一部 副主任コンサルタント
石川 朝久（いしかわ ともひさ）
専門はセキュリティ監査、グローバルセキュリティ管理支援など

グローバル企業の課題

グローバル企業はさまざまなビジネス領域で活躍しているが、そのグループ企業のセキュリティ成熟度は多種多様である。事業領域、事業規模、企業文化などが異なることもその一因だが、悪意のある攻撃者が存在する以上、セキュリティについての意識を高める必要はなくならない。NRIセキュアテクノロジーズ（NRIセキュア）では、サイバーセキュリティの傾向分析レポートを毎年発表している。2017年の調査によると、企業が保有するWebサイトのうち、およそ4割は容易に攻撃可能という結果であった（図1参照）。さらに2016年の調査では、企業が把握できていた自社・自組織のWebサイトは、存在するWebサイトのおよそ5割にとどまっており、国内よりも海外にその傾向が見られた。グループ企業のブランディングとビジネスを守る観点から、システム管理者や各社に依存した「個の管理」ではなく、グループ全体で一元的に管理する「群の管理」へパラダイムシフトを行う必要がある。そのためにはグループ企業に対して、共通のグローバルWebセキュリティ管理プログラム（以下、管理プログラム）の展開が求められる。しかしその推進には、以下の2つの課題が存在する。

図1　問題が検出されたサイトの割合



出所）NRIセキュアテクノロジーズ「サイバーセキュリティ傾向分析レポート2017」

①セキュリティリソースの不足

グループ共通の管理プログラムを実施するには、各グループ会社にセキュリティに対する十分なリソース（予算・人材）があることが不可欠である。しかし十分なリソースがなく、プログラムが進まない事例が散見される。特に小規模なグループ企業ではそうしたケースが多い。

②管理プログラムへの現場の理解と負担

現場において管理プログラムへの理解が得られない、あるいは現場が管理計画の実施に負担を感じている場合、多くの障壁が発生する。「(管理プログラムの趣旨が理解されず)依頼通りに必要な情報が共有されない」、「グループ内の担当者が繁忙で推進できない」など、さまざまな理由で遅延する傾向がある。

セキュリティ統括部門の役割

グループ全体のセキュリティ統括部門(以下、統括部門)は、上記の課題を踏まえたうえでグローバルの管理プログラムを推進する必要がある。統括部門が担うべき役割は、リスクの把握と対策の推進である。実施すべき活動は、大きく分けて以下の4つと考えられる。

①情報資産の棚卸し支援

各グループ企業がどんなシステムや情報を保有しているか、各社の棚卸し活動を推進する。情報資産の棚卸しができていない場合、セキュリティが破られた際の影響を正確に把握できず、適切なセキュリティ投資の判断ができない可能性がある。

②セキュリティ水準(TO-BE)の定義

ガイドラインを策定し、統括部門が要求する具体的なセキュリティ水準を明文化することが必要である。

③管理プログラムの立案・運用

各システムにおけるセキュリティの現状(AS-IS)を把握するための、管理プログラムを立案する。リソース面の弱い小規模なグループ企業に特に配慮し、現場の負担が少なく実効性のある管理プログラムを企画することが求められる。

④各グループ企業の支援・モニタリング

発見したリスクに関してモニタリングを適切に行う。これによりグループ会社に共通する課題を抽出・把握でき、さらなる支援や新たな施策の企画・構築の提案につながると考えられる。

管理プログラムの取り組みの実例

一例として、筆者が顧客企業の統括部門とともに、管理プログラムを構築・運用した事例を紹介したい。

A社は、国内外に50社以上のグループ企業を持つ企業である。各グループ企業のビジネス領域はさまざまであり、セキュリティ成熟度もまた同様である。A社は特に公開Webサイトのリスクを把握したいと考えていたが、グローバル共通でのセキュリティ企画・実施の経験はなかった。そのため、前節で述べた4つの活動を統括部門が実施できるよう、NRIセキュアは次のような段階的なアプローチにより支援を行った。

(1)グローバルに点在するWebサイトの把握

グローバルに点在するWebサイトを把握するため、まずWebサイトの棚卸しを実施した。これは「情報資産管理」とも呼ばれ、自社が保有しているWebサイトを一覧化し、守るべきシステムを正確に把握する、セキュリティの基本的なアクティビティである。そのため、各社のIT担当者へのヒアリングとNRIセキュアのWebサイト探索棚卸しサービスを組み合わせ、保有しているWebサイトを網羅的に洗い出した。

(2) Webセキュリティガイドラインの策定

次に統括部門の担当者と共同で、Webセキュリティガイドラインを策定した。このガイドラインは2つの点で重要な役割を持つ。

1つ目は、Webサイトの重要度に基づく分類を行うことである。棚卸しをしたWebサイトの情報と各サイトが取り扱う情報に基づき、Webサイトを重要度で分類し、リスクベースで対応の優先度を検討できる枠組みを構築した。

2つ目は、実施すべきセキュリティ対策を具体的かつ網羅的に記載し、項目ごとに実施の優先度を定義することである。統括部門として求めるセキュリティ水準を定義し、取り組むべき対策の優先度を明文化した。

このように、ガイドラインの策定は複数の観点から有益である。まずグループ会社や統括部門の担当者が、問題点や対策を議論する共通言語にできる。そのため、対策指針や定義を明確にした会議が可能となる。さらに、リソース不足になりやすい小規模なグループ企業の支援としても機能する。例えば脆弱(ぜいじゃく)性の修正をベンダーに指示する場合でも、担当者はガイドラインを提示することで、修正指針を明確にベンダーに示すことが可能である。

(3) 現場に寄り添った評価スキーム構築

守るべきシステムの一覧があり、目指すべき水準（TO-BE）が確定したため、現状評価（AS-IS）のためのスキーム設計を行った。特に以下の3点に配慮した。

まず、公開システムのセキュリティを評価する場合、一般的にはセキュリティ診断を行うが、予算が少ないグループ企業に対して低いコストでの提供を実現するため、安価でありながら重大な問題が適切に検出できる手法を検討・構築した。

次にステークホルダーの定義と役割の明確化を行った。各担当者の位置づけと役割を文書化し、実施時に担当者が迷うことがないように手順書やチェックリストを用意した。海外拠点とのやり取りでは通常、英語が使用されるが、英語は拠点の担当者にとっても第二言語であることが多い。そのため、やりとりを文書化することは、コミュニケーションミスの防止や円滑な管理プログラム推進のためにも必要不可欠である。

さらにグローバルPMO（Program Management Office）と呼ばれる事務局を設立した。グローバルPMOは調整・進捗(しんちょく)管理・技術的問い合わせなども含め包括的に対応する役割を担う。そのため統括部門の担当者とNRIセキュアのメンバーによる混成チームを立ち上げ、事務局運営、技術的支援、英語業務などを得意とする幅広い人材を投入した。

(4) パイロット運用とプログラム改善

管理プログラムを継続させ、かつ定着させるには、担当者が扱いやすいスキームにする必要がある。そのため、協力的なグループ企業に対して実際に管理プログラムを実施し、フィードバックを受けながら改善を進めていった。また、担当者がセキュリティに不慣れな場合は、本フェーズでサポートしながら管理プログラムを推進した。これにより管理プログラムに慣れてもらい、定着を狙う効果も期待できるのである。

(5) 本格運用と収集データの活用

本格運用における重要な点としては、管理

プログラムの実施を通じて得られたデータを可視化し、対策状況をモニタリングすること、また次の企画にデータを活用するプロセスを構築することが挙げられる。例えば、各システムを地域別・リスク別に分類し、グラフ化することで、地域特性に応じたフォローアップ計画の検討や、重点的なモニタリングを必要とするシステムを可視化できる。

別の事例になるが、プロダクトの脆弱性が公表された場合、管理プログラムの実施過程で収集したプロダクト情報を利用する。そこから該当するシステムを絞り込み、パッチの支援やモニタリングなど、プロアクティブな対応が可能となったケースもある。

成功に導くポイント

最後に、管理プログラムのグローバル展開を成功に導くポイントを3つ提言する。

①経営層を巻き込んだ運用

管理プログラムの推進には、経営層の関与が不可欠である。特に非協力的なグループ企業の存在や、繁忙による進捗の遅延などの場合、経営層への定期報告や、経営層を含めた検討や通達は、円滑な運用において大きな意味を持つ。また海外拠点に対する調整は、言語面・文化面から困難が多い。その際には「駐在員を通じて伝える」、「担当役員にエスカレーションする」など、各種の支援を受けるためにも経営層の関与は重要である。実際にNRIセキュアのお客さまでも、グローバルに管理プログラムを推進する際には、グローバルの経営層会議で概要を説明し、協力を得る事例が多い。

②現場の負荷軽減を意識した設計

管理プログラムの継続・定着には、各グループ企業の担当者にとって使いやすいスキームを構築する必要がある。そのためプログラム設計時には、現場が担うコスト・運用負担に留意して設計を行うとともに、フィードバックに対して柔軟に改善を進めていくべきである。また、担当者がセキュリティ管理に不慣れな場合にも適切に脆弱性の修正指示ができるよう、報告書の書式や手順のガイドラインを詳細に作り込み、統括部門からの指示が出しやすいようにするなどといった、現場担当者を支援する工夫が重要である。

③セキュリティの弱点を作らせないフォロー体制

セキュリティに対する成熟度が高いグループ企業では管理プログラムを適切に運用できるが、成熟度が低い企業の場合は脆弱性の修正に時間がかかるなど、順調に進まないケースも多い。そのためグローバルPMOにおいて質問・相談の窓口を用意し、ベンダーへの説明や修正方針策定の支援など、各グループ企業に寄り添った対応を一貫して実施することが必要である。グローバルPMOが質問を取りまとめることにより、対策のノウハウや各グループ企業がつまずきやすいポイントなども把握できる。これによりグループ共通の課題として情報を共有し、より自立的な対応を促すことも可能となる。

上記の3点に留意して、管理プログラムを立案、スキームを構築し、グループ企業に対して円滑な運用を展開していくことこそが、グローバル企業に点在するセキュリティの脆弱性を取り除くカギになると考える。 ■