グローバル企業のサイバーセキュリティ対策

～サイバーレジリエンス向上のための“シフトレフト”

藤原　佑介

2003年入社
金融サービス本部
シニア・マネジャー

堀口　敦史

2010年入社
金融サービス本部
シニア・マネジャー

数年前まで、グローバル企業のサイバーセキュリティ対策は「いかにサイバー攻撃から自社を守るか」が議論の中心であった。

しかしながら、サイバー攻撃が多様化・高度化して行くにつれ、グローバル企業は「いかにサイバー攻撃によるセキュリティ侵害を早く検出し、被害を最小限に留め、対策を講じるか」、すなわち“サイバーレジリエンス”に議論の焦点を移している。

本寄稿では、グローバル企業がサイバーレジリエンスを向上させるため、セキュリティ侵害の早期検知、すなわち検知段階の“シフトレフト”にいかに取り組んで来たか、3つのステップに分けてご紹介したい。

サイバーレジリエンスの向上

近年、グローバル企業はセキュリティ領域へのシステム投資を増やしており、そのサイバーレジリエンスを着実に向上させている。

アクセンチュアが2018年に世界15か国の企業幹部、約4,600人を対象に実施したサイバーレジリエンス調査によると、WannaCryを含むランサムウェア等の標的型攻撃が前年比約2倍に増えたのに対して、セキュリティ侵害に至った割合は30%から13%に低下したとの回答を得られた。

また、セキュリティ侵害の検知スピードは、2017年では「1ヵ月内に検知」が約30%であったのに対し、2018年は89%にまで増加しており、迅速化していることが確認された。

さらに、サイバーレジリエンスのケーパビリティ自己診断では、「高いパフォーマンスを発揮している」と評価した項目が2017年は33項目中11項目であったのに対し、2018年は19項目にまで増えており、まだまだ盤石とはいえないものの、自信を深めている様子がうかがえる。

セキュリティ領域へのシステム投資

では、グローバル企業はどの程度セキュリティ領域へシステム投資を行っているか。

多くの企業において、サイバーレジリエンスのガバナンスやレポート体系が大きく変化しており、システム予算の承認は27%が取締役会（前年比11%増）、32%がCEOや経営会議（前年比22%増）にて承認されている。

上位組織での意思決定が増えたことによってビジネス側のサイバーレジリエンスの意識は高まり、結果としてセキュリティ領域へのシステム投資額やシステム予算全体に占める割合が大幅に増加している。

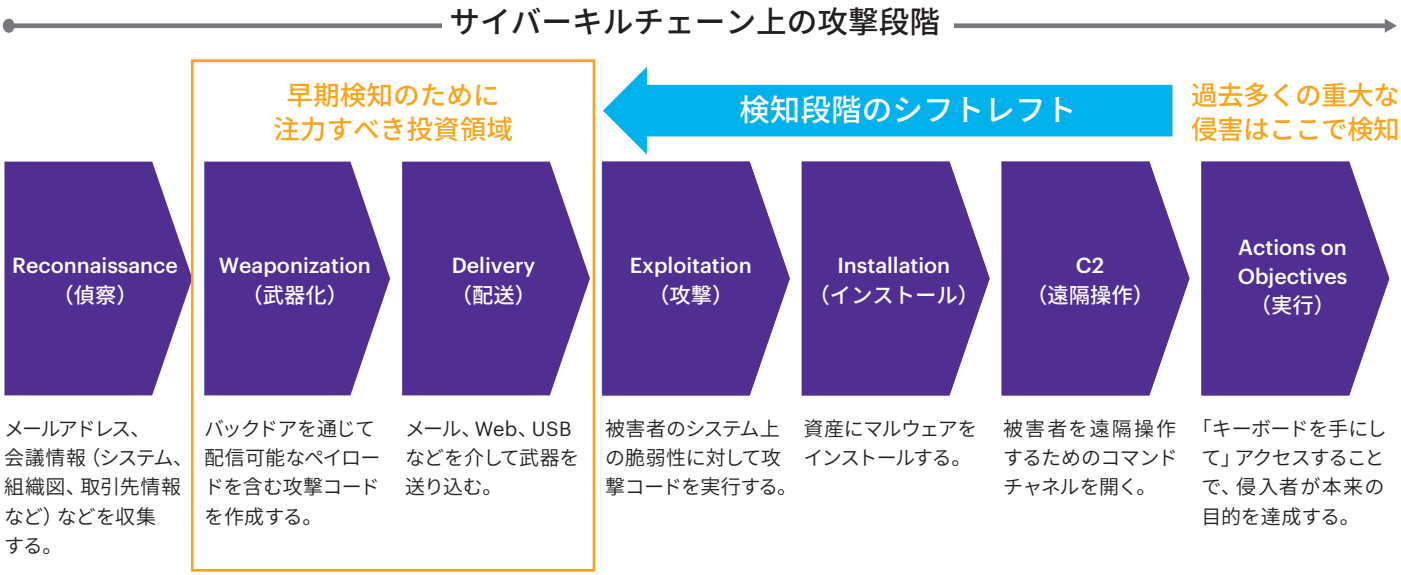
実際、システム予算の10%以上をセキュリティ領域に投資している企業は前年比で3倍以上（22%から74%）に増えており、直近3ヵ年の投資額は増えたと回答する企業も64%から90%に増えている。

注力すべき投資領域

ロッキード・マーチン社がサイバー攻撃における一連の行為をフローとしてモデル化した「サイバーキルチェーン」がグローバルレベルで標準的に使用されている。サイバーキルチェーンを理解することにより、攻撃の段階ごとに必要な対策を講じる、あるいは攻撃を検知した場合に次の行動を予測して早期の対策を講じることができる。

グローバル企業はこれまで「Actions on Objectives（実行）」の段階で多くの重大

図表1 サイバーキルチェーン上の注力ステップ



な侵害を検知していたが、「Weaponization（武器化）」「Delivery（配送）」の領域にシステム投資を注力することで、侵害の早期検知、すなわち検知段階の“シフトレフト”を試みてきた（図表1）。

“シフトレフト”へのアプローチ

悪意を持った攻撃者は「Exploitation（攻撃）」を実行する前の段階で、実際にどのような攻撃を企てているのか。その企てを把握し、先読み型の対策立案・実行が可能な運営態勢を構築するため、3つのステップが必要と我々は考えている（図表2）。

1st ステップ：脅威・脆弱性情報のリアルタイム収集

先読み型の対策立案・実行に向け、どのような脅威・脆弱性があるかを幅広くリアルタイムに把握することが“シフトレフト”への1stステップである。

Threat Intelligence Feedsの活用

マルウェアは1秒間に約15個の新種が発生していると推計されており、グローバルレベルの脅威・脆弱性情報を手動でリアルタイムに収集することは現実的に不可能である。この問題の解決策として、「Threat Intelligence Feeds」の導入を推奨する。Threat Intelligence Feedsは、国内外から様々なソースを収集し、経験豊富なアナリストによる分析情報をAPIにて提供している。自社IT環境とAPI連携を行うことで、脅威・脆弱性情報をリアルタイムに収集することができる。

政府官公庁の情報活用

また、政府官公庁が提供している情報も活用したい。代表的な情報源として、JPCERT/CC及びIPA/ISECが運営する「JVN（Japan Vulnerability Notes）」が挙げられる。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報をAPIにて提供している。

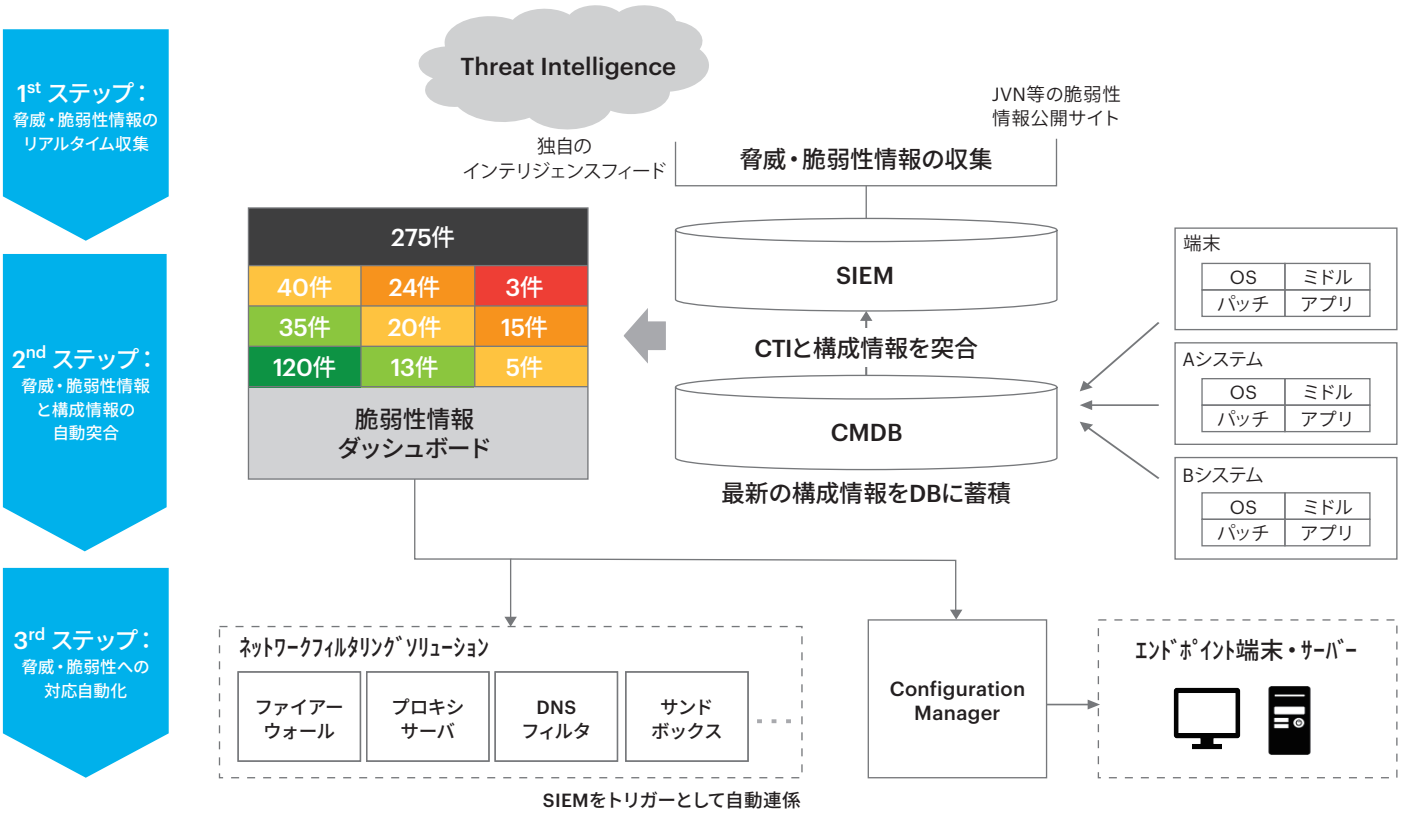
2nd ステップ：脅威・脆弱性情報と構成情報の自動突合

収集した脅威・脆弱性情報が自社IT資産に該当するかをリアルタイムに把握することが“シフトレフト”への2ndステップである。

IT資産情報管理の高度化

自社IT資産（PC端末・利用アプリケーション等を含む）の脅威・脆弱性を把握するためには、自社IT資産を統合的に管理し、バージョンを含めた情報を常に最新化しておく必要がある。一般的に、各社CMDB（Configuration Management Database）を活用してIT資産管理を行っていると思われるが、管理対象として外れがちなBYOD（Bring Your Own Device）や外部委託先のシステムも含めて、情報の最新化を徹底する必要がある。

図表2 シフトレフトのための自動化例



脅威・脆弱性のダッシュボード化

脅威・脆弱性が自社IT資産に潜んでいるかを把握するために、脅威・脆弱性情報とIT資産を突合する必要がある。ただし、数千からなる脅威・脆弱性情報とIT資産情報を手動で突合するのは、正確性・リアルタイム性の観点で限界がある。この問題の解決策として、SIEM（Security Information and Event Management）を用いた突合の自動化を推奨する。SIEMを活用することにより、脅威・脆弱性情報とIT資産を高頻度で突合することができ、どの機器にどのような脅威・脆弱性があるかをダッシュボード上でリアルタイムに確認することができる。

3rd ステップ：脅威・脆弱性への対応自動化

識別した自社IT資産の脅威・脆弱性への対応を自動化することが“シフトレフト”への3rdステップである。

Configuration Managerによる対応

自社の脅威・脆弱性を識別した結果、対応を要する機器が数千と膨らむケースが多々ある。社員への対応依頼やIT担当者による対応を手動で行う場合、リアルタイム性や網羅性が損なわれるリスクが高い。Configuration Managerを活用することで、強制的に該当機器への対応（機器起動・インストール・アンインストール・アップデート・ブラックリスト化等）を自動実行することができる。

SIEMとネットワークフィルタリングソリューションの連動

収集した脅威・脆弱性情報をファイアーウォールやプロキシーサーバー等に設定することで、メール・Webを介した攻撃を検知・防止することができる。攻撃を受ける前のタイムリーな設定が必要となるため、SIEMとネットワークフィルタリングソリューションを連動し、脅威・脆弱性情報の収集からフィルタ設定までの処理自動化を行うことを推奨する。

最後に

弊社調査によると多くの企業幹部は自社のサイバーレジリエンスに自信を持っている。しかしながら、弊社が日本で実施したダークウェブ調査では、企業の社員情報流出等の懸念を検知しており、企業はセキュリティ侵害にすら気付いていないケースもある。

拡大する攻撃対象、高度化する攻撃、爆発的なデータ量の増加等、増大し続ける課題に対応するためにも、サイバーレジリエンスの向上にぜひ継続的に取り組んで頂きたい。