2018 年 1 月 15 日

ServiceNow、2018 年のセキュリティオペレーションのトレンド予測を発表

GDPR、レスポンスの自動化、*CISO* の経営参加、*IoT* に関するセキュリティ情勢を予見

ServiceNow Japan 株式会社（本社：東京都港区、社長：村瀬 将思　以下、ServiceNow）は本日、2018 年のセキュリティオペレーションに関する 4 つの予測を発表しました。

2017 年は、WannaCry などのランサムウェアによる高度で広範囲にわたるデータ侵害が毎日のように増加し、世界中の 1 億人以上の人々に影響を及ぼしました。2018 年も、サイバー攻撃のスピードと複雑化が増すことが予想され、防御や対応のアプローチが企業のデータを守る上で大きなカギとなります。ServiceNow Inc.のセキュリティ CTO であるブレンダン・オコナー(Brendan O'Connor)が、2018 年に注視すべき企業のセキュリティオペレーションの主な傾向を次のように予測しました。

予測 1：EU による GDPR 違反の企業へのペナルティーが課せられる

2018 年 5 月 25 日より一般データ保護規則（GDPR）が執行されることに伴い、EU は罰金を科す最初の企業の 1 社を見せしめにして、すべての企業が GDPR を真剣に考慮すべきである、というメッセージを発する可能性があります。

GDPR は、欧州連合（EU）内で個人に対するデータ保護を強化して統合するための法的枠組みを提供するだけではなく、EU で顧客や従業員を抱える世界中のすべての企業活動に影響を与えます。企業は個人データを処理、保存、および保護する方法に関する責任を問われる可能性があり、違反した場合には制裁金は最高 2,000 万ユーロ、または全世界の年間売上高の 4%のいずれか高い方が課せられます。このような企業による違反は世界的な注目を集めるため、他の企業は GDPR を遵守するための計画に前向きに取り組まざるをえなくなります。

予測 2：セキュリティレスポンスの自動化が「持つ者」と「持たざる者」への分かれ道となる

2018 年はセキュリティレスポンスを自動化するか否かが、セキュリティに関して「持つ者」と「持たざる者」へ分かれるカギになります。これまで、データ保護と脅威検知といったセキュリティ技術が発展してきた中で、見過ごされてきた分野がレスポンスです。自動化のためのツールとそ

れを積極的に受け入れる文化を持ち、ビジネスの成長に向けて活用する企業は、そうでない企業よりも優れた業績を上げることになります。

自動化を取り入れる企業にとっての利点は、セキュリティ担当者が日常のマニュアル作業から解放されることです。セキュリティ担当者は、組織を強化する戦略的なプロジェクトに集中することに、より多くの時間をかけられるようになります。現在、多くの組織が使用している多数のセキュリティツールは大量のアラートをセキュリティ担当者に通知します。担当者は、スプレッドシートや電子メールを使用してこのアラートへの対応を管理しており、莫大な量のアラートが原因でインシデントの調査に相当な時間を費やしています。 一方で、セキュリティレスポンスに自動化を取り入れた企業の IT 部門は、莫大な量のアラートへの対応ではなく、セキュリティオペレーションのレポート作成が業務の重要な部分になります。彼らはスケーラブルなプロセスを整え、進捗状況を測る立場になります。また自動化により、システムに対するパッチの適用時期の判断が容易になるほか、フィッシング攻撃に対して、日単位ではなく分単位で対応できるようにもなります。

予測 3：CISO(Chief Information Security Officer)の企業経営への参加が重要になる

CISO がより積極的に企業経営に関わるようになり、経営幹部や取締役がセキュリティ対策の費用対効果に関する理解を深めることで、ビジネスのあらゆる側面に価値を生み出すようになります。セキュリティ対策は、短期的には規制や法令遵守、顧客との関係構築、株主からの信頼の向上、知的財産やおよびブランドの保護などに寄与します。

経営陣はセキュリティ対策に対して理解を深める一歩を踏み出す必要がありますが、セキュリティチームは経営陣に対して更にもう一歩踏み出す必要があります。セキュリティチームはリスクと影響を経営陣が多用するビジネス用語を用いて投資に対する価値をさらに明確に説明する必要があります。CISO と経営陣の間の知識のギャップを埋めることが、セキュリティを確保するための効果的な枠組みの構築につながります。

予測 4：サイバー空間でのセキュリティ侵害が、物理的に影響を及ぼす

2018 年には、セキュリティ侵害の影響が人々の実生活の物理的なレベルまで及びます。医療機器やウェアラブル機器のハッキングの他、また、産業用 IoT デバイスや自動運転車が影響を受けることも考えられます。

今日、企業を悩ませているセキュリティ侵害は、主に情報セキュリティにおける侵害です。クレジットカード情報、マイナンバー、または個人的なデジタル情報の盗難は重大な侵害ですが、被害者

が物理的な危害を被ることはありません。しかし、家においてもガレージの扉から冷蔵庫に至るまでデバイスの高性能化・ネットワーク化が進み、政府、企業、そして個人は、現在のインフラストラクチャのセキュリティをより詳しく見直し、対策を立てることに迫られます。

###

ServiceNow について

ServiceNow Inc.は、世界で最も急成長を遂げている企業向けクラウドサービス企業の 1 社です。同社が扱う SaaS 型サービスマネジメントツール「ServiceNow」は、ITSM(IT サービスマネジメント)を中心に世界で 5,300 社の導入実績があります。要件に合わせて容易に利用可能なポータル、データベース、ワークフロー、開発環境、機械学習機能を擁する単一プラットフォーム上で、ITSM、カスタマーサービス、セキュリティオペレーション、人事管理サービスを提供しているので、企業内の広範囲なビジネスプロセスを、部門組織を横断する形でワークフロー化することができます。独自の業務アプリケーションを簡易に開発することも可能なので、企業のデジタル化、業務最適化を推進し、従業員、ユーザー、お客さまに高いエクスペリエンスを提供する企業変革の基盤となります。
http://www.servicenow.co.jp

###

本件に関する報道関係者からのお問い合わせ
ServiceNow Japan 株式会社　マーケティング本部
今村 康弘　（yasuhiro.imamura@servicenow.com）
TEL: 03-4572-9246

ServiceNow 広報担当　PR 代理店　ウェーバー・シャンドウィック　大城／下出
Tel： 03-5427-7384（大城）/ 7360（下出）
E-mail：servicenow-jppr@webershandwick.com