セキュリティ

ITマネジメント（内部統制）

知ってますか？キャスビー、EDR、ピーサート

2019年のセキュリティ対策、5つのヒント（前編）

従来の標的型攻撃や不正アクセスだけでなく、IoTデバイスや仮想通貨などにも拡大しているサイバーセキュリティ・リスク。次々と登場する新たな脅威にどう対応すれば良いのでしょうか。セキュリティリサーチャであり、OWASPの活動や総務省CYDER実行委員なども務める岡田良太郎氏が、2019年に企業が計画的に取り組むべきセキュリティ対策について、5つのヒントを紹介します。

5つのヒント

1. ビジネス推進のステークホルダー拡大
2. 働き方改革によるワークプレースの多様化
3. システムのアップデートマネージメント
4. クラウドサービスの一括コントロール
5. セキュリティ推進のリーダーシップとスタイル

2019年を迎え、多くの皆さんが久しぶりの長期休暇を楽しまれたかもしれません。久しぶりに開ける業務用のメールボックスは、仕事だけでなくリスクも盛りだくさん。フィッシングサイトへの誘導メール、マルウェアのダウンロードを誘発するメール、さらには脅迫メールも、わんさと飛び交っているようで、私の周辺でも感染・被害報告をいくつか耳にしています。

サイバーセキュリティ・リスクにおいて昨年来高まっている脅威には、従来の標的型攻撃やウェブアプリケーションへの不正アクセスに加え、仮想通貨からIoTデバイスなど多岐にわたるエリアへの攻撃が関係しており、個人のみならず企業への影響も拡がっています。企業では、セキュリティ対応チームとしてCSIRT（Computer Security Incident Response Team ／シーサート）が続々と設立され、有事の火消し対応の体制確保は喫緊の課題とされています。

しかし、サイバーセキュリティは、いつまでこのような行き当たりばったりの「火消し」に右往左往するのでしょうか。近年、攻撃サイドの利益率が14倍だとの報告もありました。この相手に有利すぎる負け試合に消耗しつづけ、被害者であるにも関わらず、関係者に謝罪し続ける事態をいつまで看過しなければならないのでしょうか。また、企業のCISO（Chief Information Security Officer ／最高情報セキュリティ責任者）は、どうすれば良いのでしょうか。

様々なシステム連携によってビジネスが成立する現在、それらシステムを活用する事業の現状と変化にはどのようなリスクがあり、それをどのようにコントロールするのか。セキュリティ対策を有事の解決だけに委ねるのではなく、事前に計画的に織り込むことが肝心です。ご存知のとおり、たいていプロセスというものは左から右に描きますが、事前の段階は左側＝レフトにあるので、このプラクティスを「シフトレフト」と言います。そこで、このシフトレフトを企業のセキュリティとして計画的に実現していくための検討ポイントを考えてみたいと思います。特に2019年年頭の時点で、多くの企業に影響を及ぼす5つのポイントをとりあげ、セキュリティ対策計画におけるヒントを前編・後編で示したいと思います。前編の本稿では、ビジネス推進のステークホルダー拡大の影響、また働き方改革によるワークプレースの多様化について解説します。

ヒント1

ビジネス推進のステークホルダー拡大

IT調達がカジュアルなものになっています。企業の業務を支えるハードウェアからアプリケーション、またバックエンドのデータベースに至るまで、様々な企業が入り乱れて成り立っています。それにともない、協力企業、関連企業も増えており、1つの事業を完結させるための関係者、その所属組織は少なくありません。一箇所にリスクを完結させることはもはや不可能です。

これは、セキュリティ活動や教育啓発、ひいてはポリシーによるガバナンスの限界を意味しています。攻撃者から見れば、1つの企業のデータを窃取する攻撃面はありとあらゆるところにあるということです。同時に、被害が発生した場合の影響範囲も、自社だけにとどめることが極めて困難となります。この状況が、これから論じるいくつかのキーワードとかけ合わさると、セキュリティには「事業とマッチした戦略が必要」であることが鮮明に見えてきます。

IT環境の多様化に伴い、ワーカーに必要とされるセキュリティ・リテラシーも変わってきます。個人情報の取扱ひとつとっても、会社では個人情報取扱研修などポリシーによる教育は、形式的で、毎年同じものが行われていないでしょうか。ISMS対応という旗印のもと、もう何年もポリシーの改定をしていないということはないでしょうか。これでは、業務を推進する手段はどんどん進んでいけばいくほど、「セキュリティ」が化石になっていくリスクが高まっていきます。

セキュリティ・リテラシー教育は、もっと実務に寄り添う形になっていかなければ有効性を発揮できないことを意味しています。ご承知のとおり、事業が異なればリスクも異なります。フロントとバックオフィスではリスクが違います。経営陣と現場の部門では、リスクが違います。もっと言えば、ソフトウェア開発部門と、運用部門では、リスクが違います。会社のさまざまな職務が様々なシステムが入り乱れる中で、「情報を扱う」ということは全社全業務をひとまとめにできるほどシンプルではありません。

「業務に特化したセキュリティ」を推進する教育プログラムは、それぞれの事業をサイバーセキュリティのみならず、ミスオペレーションなどによって引き起こされる事業継続を阻む問題に直面するリスクを大きく下げることにつながります。

ヒント2

働き方改革によるワークプレースの多様化

「働き方改革」。昨年これほど、多くの情報システム部門の既存ポリシーを変化させなければならないバズワードはなかったのではないでしょうか。それによって、VPN（仮想プライベート ネットワーク）設置やリモートアクセスがぐんぐん推進されています。その状況で、誰がどこから社内のリソースにアクセスしているのかを管理するのをあきらめてしまうかもしれません。はたまた、実際に働いているのは自社の人間ではなく、もしかしたら別の人かもしれません。

加えてモバイルデバイスが多機能・高性能になり、どこでもインターネットに接続でき、社内へのVPNを確立するのが用意になりました。アプリケーションが便利になり、もはやOSとハードウェアの機能や性能をケアすることも少なくなっています。

例えば、PCやスマホに保存されているエラーログを見るひとは滅多にいないことでしょう。ユーザーにとっては、アプリケーションをどう扱うかだけの話だからです。こうした状況は、情報システム部門から見れば、デバイスの保護や管理にユーザーの手を借りられないということを意味しています。

そこで、それぞれの端末へのアンチウィルスソフト展開というシンプルな防御手段から、端末やサーバーなどのエンドポイントまで監視対象を広げるEDR（Endpoint Detection and Response）統合というアプローチへの変化は急加速しています。何かあったら報告してもらうという人頼みのプロセスをやめ、さまざまな端末で起きるインシデントに対応する手段を全体で統合していくという方向です。これにより、ネットワーク通信でのセキュリティとの自動的な

連携や、専門スタッフがネットワークやデバイスを常時監視するSOC（Security Operation Center ／セキュリティ監視拠点）という外部のセキュリティ運用サービスの活用もできるようになります。

後編では、情報システムのセキュリティに関わるトピックを扱います。今やビジネスに欠かすことのできないクラウドサービス活用との関わりについてもスポットをあてたいと思います。また、企業でセキュリティを推進するための組織的な取り組みについて紹介します。

岡田良太郎（おかだりょうたろう）
株式会社アスタリスク・リサーチ 代表取締役/エグゼクティブ・リサーチャ

セキュリティリサーチャ。国内の企業や団体におけるセキュリティイニシアチブの継続的な支援に従事している。また、セキュリティ堅牢化・プロジェクトWASForum Hardening Project（ワスフォーラム・ハードニングプロジェクト）オーガナイザ、グローバルコミュニティ OWASP（オワスプ）のJapanチャプターリーダーを務め、2014年にThe OWASP Foundationより "Best Chapter Leader"を受賞。BBT大学では教員として「教養としてのサイバーセキュリティ」科目を担当している。また、政府・公共機関に協力し、情報セキュリティ10大脅威選考委員、総務省CYDER実行委員。CISA、MBAを保持。