3－4．当社がご支援できること

当社は、これまで70社を超える多方面の業態の企業様に対して、セキュリティ対策の企画立案から対策導入を実施してまいりました。またニッセイグループにおいて長年に渡り、実務としてセキュリティ運用にも携わっており、セキュリティ事件・事故の早期対処に必要なノウハウを有しております。

これらノウハウを基に、セキュリティ対策実施状況の可視化・具体的な対策導入だけではなく、インシデント検知・分析・対応等のセキュリティ運用までご支援いたします。

4.最後に

日々報道される標的型攻撃による被害は、対策の困難さや原因の根深さを浮き彫りにする一方で、CSIRTを始めとする組織的なセキュリティ運営の重要性・有効性も露にしています。

組織の規模に関わらず、外部や内部から情報を窃取されるリスクは存在し、攻撃された場合の完全な防御は困難です。そのためにも、行政機関やセキュリティベンダー等が発信する情報から課題や教訓を知り、組織内でこれらを共有することは、セキュリティ強化に向けた有効な指針となります。

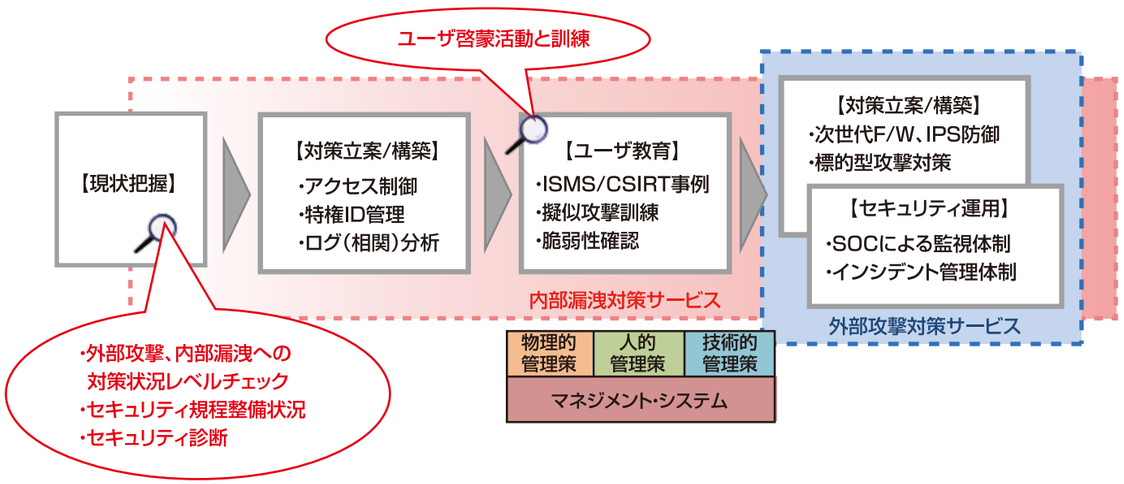
まずは組織の現状を把握し、問題の所在を可視化することから始めてみてはいかがでしょうか？

（参考文献）
・IPA　標的型攻撃対策　2014年2月
・IPA　情報セキュリティ10大脅威2015　2015年3月
・内閣サイバーセキュリティセンター
　日本年金機構における個人情報流出事案に関する原因究明調査結果　2015年8月

（ITソリューション営業本部　川西　康文）

この記事に関するお問い合わせは、以下へお願いいたします。
インフライノベーション事業部　ビジネスイノベーション室
生駒　勝治／津田　和典
TEL:03-5714-5715　FAX:03-3735-1667
e-mail:security_info@nissay-it.co.jp

［図2　当社のサービス範囲］



ニッセイ情報テクノロジー株式会社
〒144-8721 東京都大田区蒲田5丁目37番1号 ニッセイアロマスクエア　TEL:(03)5714-4624　FAX:(03)5713-0178
http://www.nissay-it.co.jp

NISSAY IT Report

ニッセイ情報テクノロジー株式会社

セキュリティトータルサービスのご紹介

情報システムへの不正アクセスや攻撃を通じた機密情報の漏えい或いは業務停止を防ぐため、行政や企業等の組織においては、従来からネットワークの通信制御やデータの暗号化、ソフトウェア脆弱性修正プログラムの適用、ウィルス対策ソフト導入等の対策を実施してきました。しかしながら昨今の標的型攻撃に代表されるように、情報窃取の手口は巧妙化・複合化が進んでいます。このため、セキュリティ事故・事件を発生させない対策だけではなく、発生しても早期に対処できる対策が必要となります。

本レポートでは、情報漏えいの典型例と課題点、ならびに当社ソリューションについてご紹介します。

1.脆弱性とは

脆弱性とはセキュリティ対策上の欠陥を指し、その原因は業務アプリケーションやソフトウェアの仕様・設定不備等に加え、組織が遵守すべきセキュリティ関連規定の欠落、従業員の知識不足・モラル欠如も含まれます。また、情報システムを取り巻く環境は絶えず変化するため、脆弱性対策も継続的な見直しが求められます。

情報システムにおいては、外部と接続するネットワークの分離、閲覧可能なウェブサイトを制限する、外部からの不審な通信を遮断する等、多層的な防御が有効です。組織運営においては、セキュリティ事故・事件に備えた体制構築、行動要領の周知、模擬訓練により、従業員それぞれが攻撃に対応する能力を養わなければなりません。

2.情報漏えいの典型例

2−1.標的型攻撃

標的型攻撃は、「計画立案(調査)」「初期潜入」「攻撃基盤構築」「侵入・内部調査」「目的遂行」の順に実行されます。攻撃者は、対象とする組織の業務内容や保有する機密情報、公開メールアドレス等を調査し、ウィルスを添付或いは攻撃者のウェブサイトへ誘導する偽装メールを送付します。結果、ウィルスに感染したパソコンや情報システムを通じて、目的とする情報の窃取や破壊が遂行されます。

＜主な対策＞

・セキュリティ事件、事故発生時に迅速に対応できる体制の構築
・従業員に対するセキュリティ教育の実施
・情報システムを利用できる従業員の厳格化
・ネットワークの監視強化

2−2.内部不正

組織関係者による情報窃取は、情報システムの利用権限や監視機能の不備、帳票の放置、責任者による点検運営の欠落等の不適切な環境を衝いて犯行が行われます。内部事情に精通しているため重要情報の所在や入手経路・手段を理解しており、また、組織へ不利益を与えることや情報の売買により金銭を得るといった動機を有していることから、一度に膨大な情報が漏えいするリスクを有しています。

＜主な対策＞

・セキュリティ対策を推進する組織体制の整備
・従業員に対するセキュリティ教育の実施
・情報資産の利用権限の厳格化と管理の徹底
・システム操作の記録と監視
・入退室の監視や持ち込み物等の確認
・なりすましの防止(察知されにくいパスワードや生体認証の導入等)

3.課題点

セキュリティ脆弱性や対策に関する認知度・理解度は高まっていますが、経営層や各部門は現実的には様々な課題や悩みを抱えておられます。情報セキュリティ対策は組織全体で取り組みを推進する必要がある一方、それぞれが認知できていることも限定的になりがちなため、組織横断的に課題を共有・棚卸しすることが、対策強化に向けたスタートラインとなります。

3−1.経営層から見た課題

顧客・従業員の個人情報や機密情報の漏えいは組織の評判を著しく毀損し、また、事象発覚後の調査・報告・是正措置或いは補填にかかる金銭的・時間的損失は甚大です。

従来から各種社内規定の整備や監督官庁の方針に準拠した体制や運営構築を行いつつも、次のような課題をお持ちです。

・事故や事件が発生した際の規定や体制は準備できているか
・それらの規定や運営の効果性は評価できているか
・十分な対策を行うにはどの程度のコストが必要か

3−2.情報システム部門から見た課題

システム企画・開発・保守運用・委託ベンダー管理等の一連の業務のなかで、情報システム部門はセキュリティ事故・事件の防止や対応における中心的な役割を担います。しかしながら、情報システムやデータの規模と種類は増大し、求められる運用要件も複雑化しており、次のような課題をお持ちです。

・事故や事件の具体的な事象を洗い出せているか
・具体的な事象が発生した際、的確かつ有効的に行動できるか
・どのような製品やソリューションを組み合わせれば、事象発生に気づくことができるか
・既に情報漏えいが発生していないか

3−3.ユーザー部門から見た課題

業務において取り扱う顧客の個人情報やその他機密情報は、情報システムや紙媒体のほか、USBメモリやテープ等の外部記憶媒体で取り扱われます。また、スマートデバイスの普及により情報システムの利用方法やデータの保管手段も多様化するなか、次のような課題をお持ちです。

・重要な情報資産や、情報漏えいした際の影響がそもそも把握できているのか
・対策は情報システム部門のみに委ねて大丈夫か、ユーザー部門で実施すべきことは無いか
・事故や事件が発生した際、何を行うべきなのか

[図1　これまでのセキュリティ対策と課題点]