www.pwc.com/jp

サイバーセキュリティの疑問に答える

継続的な取り組みの必要性

pwc

経営幹部がサイバーセキュリティに継続的に取り組むことは、ビジネスの保護だけではなく、収益拡大にもつながる。

サイバーセキュリティの問題が質量ともに増大する中、継続的な取り組みがますます必要になっている

米国の小売業には構造的なセキュリティ問題が根強く残っている。小売業および消費財を扱う企業へのサイバー攻撃の増加は、近年の主なデータ侵害事例から明らかである。2013年12月中に発生したインシデントからも、脅威が増し攻撃の手口がより巧妙になっていることがわかる。

サイバー犯罪者は顧客のペイメントカードデータを盗むことで、膨大な利益を手にすることができる。そのため、ハッカーはまず小売業者を狙い、顧客の機密情報を引き出そうとする。小売業者においてセキュリティ侵害が起こり顧客情報の盗難または紛失が発生した場合、悪評が立ち客足が遠のく他、多額の費用がかかる訴訟を提起されたり、PCI SSC（Payment Card Industry Security Standards Council）から高額な罰金を科されたりする恐れがある。

PwCが経験に基づいて把握している構造的なセキュリティ問題

サイバー犯罪者が顧客のペイメントカードの「トラックデータ（クレジットカードの裏の磁気ストライプに記録されている電子データ）」にアクセスするには、小売御者のPOS端末にスキミング用のソフトウエアをインストールする方法が最も一般的である。このスキミングソフトウエアにより、顧客が購入時に機械に通したカードから磁気ストライプのデータを読み取る。サイバー犯罪者はこの「トラックデータ」を取得し新しいカードの磁気ストライプにそのデータを移すことでカードを偽造することができるのだ。

この種の攻撃については、フォレンジックの観点から主に三つの疑問が生じる。まず、犯罪者はPOS端末にどのようにしてアクセスしスキミングソフトウエアを大規模にインストールするのだろうか。そして、スキミングで入手したデータをどのように抜き取るのだろうか。さらに、セキュリティ監視による検知をどのようにすり抜けているのだろうか。この窃盗に内部者が協力している場合、その協力者がPOSシステムへのアクセス権と知識を悪用してスキミングソフトウエアをインストールし、データを収集するための手順を策定しソフトウエアの設定をした後、セキュリティ監視が実行されている中であってもそれを無効化したり、あるいは迂回することによって犯罪の露見を防ぐ。このような内部の協力者は、信頼はできないが監視対象ではなく、小売業者のPOSインフラストラクチャーに正当にアクセスできる者であり、従業員、契約業者、ベンダーなどが挙げられる。一方、正当なアクセス権を持たない外部者がデータを盗もうとする場合は、外部の人間が協調して次の行動を順番に取る可能性がある（これは当社が関わったデータ侵害事例に基づいている）。

1. 初期侵入：インターネットに接続されているシステムやデバイスの脆弱性を見つけ出し悪用するか、人為的ミスによって生じたシステム設定の不備を突いて、インフラストラクチャーにアクセスする。
2. 偵察：実装されているセキュリティ対策を把握し、標的とするアプリケーションやビジネスプロセスを特定するために、インフラストラクチャーへのアクセス権を使用してシステム環境の検証を実行する。
3. 攻撃：POS端末に狙いを定め、適切なプロセスの中にツールを潜ませ、クレジットカードおよびデビットカードのトランザクションのうち、暗号化されていないものを見つけ出し記録する。
4. データの抜き出し：取得した情報をひそかに抜き取る。
5. 隠蔽：攻撃者はこれらの活動全てを、システム環境に実装されたセキュリティ対策によって検知されないように隠す必要がある。

このような活動にどれくらいの期間がかかるかは、手口の巧妙さの度合いによって大きく異なるが、場合によっては数カ月、数年かけて仕掛けられることもある。最初の偵察と侵入から実際の攻撃まで数カ月前の間が空いている場合、収集される機密データの量はその間に増えることにる。

データ侵害またはインシデントにおいて、攻撃の初期段階にみられる兆候を捉えることによって、POS端末（またはPOS情報が一元管理されているデータベース）からの情報漏洩を最小限に抑制または回避できる。最新のセキュリティ監視や検知機能を実装していても、巧妙な攻撃者ほど、ひそかに少しずつ監視や検知のメカニズムを迂回し、何日、何カ月、ときには何年もかけて入念にアクセスできる範囲を拡大させ、重要なシステムに入り込む。経営幹部は常に、攻撃者による準備がすでに始まっている可能性があること、また攻撃者が重要資産であるデータを引き出そうと虎視眈々と機をうかがっていることに、十分留意する必要がある。

財務諸表の統合監査および財務報告にかかわる内部統制の範囲

統合監査

サイバー攻撃が統合監査の範囲に含まれることはほとんどない。全て、独立監査人は、1934年証券取引所法第13a-15条および第15d-15条に従った企業の開示および手順の設計および運用性の有効性を定期的に評価する必要がある。財務諸表の統合監査および財務報告にかかわる内部統制（統合監査）には、全ての重要な事項について、あらかじめ定義された時点において、財務報告に対する内部統制の有効性評価を実施するという側面がある。この評価は、トレッドウェイ委員会組織委員会（COSO）が定義している統合フレームワークに基づいて行われる。

サードパーティ／第三者型の決済代行事業者

多くのサードパーティでは、サービス監査人が米国公認会計士協会による保証業務基準書（SSAE）第16号に従い、管理策がユーザー組織の財務報告にかかわる内部統制に関連する可能性がある場合に、ユーザー組織にサービスを提供する組織の管理策を報告している。ただし、これらの管理策は財務報告に関するものであるため、典型的なサイバー攻撃を検知するようには作られていない。

その他の懸念事項

Payment Card Industry Data Security Standards（PCI DSS）

ペイメントカード業界の加盟店および決済代行事業者のセキュリティには、ペイメントカード業界のデータセキュリティ基準（PCI DSS）の情報セキュリティに関するベストプラクティスが適用されている。この基準には、ペイメントカード保有者のデータの格納、処理、伝送を実行する事業者が満たすべき12の要件が定められている。これらの要件により、決済を安全に行える環境を構築できるようになるのだ。PCIコンプライアンスを達成するための要素は、評価、改善、報告[1]という3段階に分けられる。

注目すべきは、基準を満たしたPCIシステムで多くの侵害が発生していることである。さまざまな原因が考えられるが、私たちの経験上、狙われるのは主に磁気ストライプカードである。磁気ストライプカードには、欧州、カナダ、南米で使用されている集積回路とチップを搭載したEMV[2]カード基準に比べ、複製が容易で管理が困難であるという難点がある。EMVカードの場合、カード番号などのデータだけでは直接金銭に結び付けることが難しいため、スキミングを手口とする窃盗では敬遠される。磁気ストライプカードが主流な国々ではデータが狙われやすく、結果としてPCI SSCから科される罰金は高額に上る可能性がある。

1 https://www.pcisecuritystandards.org/security_standards/getting_started.php
2 Europay, MasterCard and Visa（集積回路を搭載したカードの相互運用のためのグローバル基準）

2011年10月13日SECのサイバーセキュリティ上の情報開示に関するガイダンスおよびその他の情報開示

2011年10月13日、証券取引委員会（SEC）はサイバーセキュリティ上の情報開示に関するガイダンスを発行した。このガイダンスでは、重大なサイバーインシデントによる損失その他の結果を開示するため、Form 6-K（外国会社臨時報告書）または Form 8-K（重要事項発生時の臨時報告書）の提出の他、「財政状態および経営成績に関する経営者による説明と分析」においてサイバーセキュリティインシデントに関する情報開示を求めている）[3]。

経営陣、リスク管理、内部監査 - 三つの防衛線の構築

企業のデータを標的とする攻撃の増加に伴い、三つの防衛線を構築し、継続的に補強していくことを推奨する。

1. **経営陣：**一般的に情報セキュリティリスクの管理に長けている企業では、組織のトップレベルがセキュリティ管理体制に関する責任を負っている。経営陣は、リスクの評価、コントロールの実装、リスクの低減に関するオーナーシップを発揮し、実行責任と説明責任を果たす。
2. **リスク管理およびコンプライアンス部門：**リスク管理部門は、経営陣に効果的なリスク管理プラクティスの実装を促し、監視する。また、リスクの当事者がリスクに関して十分な情報を提供できるように支援する。
3. **内部監査部門：**内部監査部門は、第一・第二の防衛線がどのように機能するかも含め、組織によるリスク評価およびコントロールがどの程度有効かを経営陣に示すため、（コンサルティング活動に基づく）客観的な情報を提供する。重大なリスク領域では、この第三の防衛線が少なくとも第一・第二の防衛線と同程度に強固である必要がある。的確かつ客観的な情報を提供する機能が備わっていないと、情報プライバシーに関する慣行が不十分または時代遅れになるという現実的なリスクを抱えることになる。この機能を提供する役割を担うのが内部監査部門だが、そのためには相応の権限とリソースが必要である。

この三つの防衛線は、データプライバシーおよびセキュリティに限られるものではない。企業が抱えているあらゆる重大なリスクに対応するため、これらの防衛線を構築し、健全に運用する必要がある。多くの企業にとって、情報セキュリティおよびプライバシーの問題は、財務や評判に悪影響を及ぼし、低減が困難な重大なリスクの一つである。

3 http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm, 脚注2.

経営陣はセキュリティ上の事象にどのように対応すべきか？

経営陣は独立監査プロセスにより、自社の情報セキュリティプログラムの十分な品質と機能を確保する以上の利点を得ることができる。外部監査、第三者監査および経営陣によるガバナンス、リスク、コンプライアンス検証に何が含まれ、何が含まれないのかを把握できるよう、経営陣がプロセスに関与することが望まれる。より深いリスク評価を実施し、セキュリティやプライバシーに限らず、ITリスク全体を幅広く対象とするとよいだろう。

また、経営陣が緊密に協力し、サイバーセキュリティに関するリスクおよび機会を把握し、管理するための方策について理解を深めることも必要である。サイバーセキュリティに関するリスクの割合を低減させる策として、サイバー保険の利用を検討するのもよいだろう。さらに、企業として侵害への対応を統一して定めることも不可欠である。これはすぐに実行に移すことができ、反復可能なビジネスプロセスである必要がある。データ侵害による影響がブランド、評判、取引関係に及ぶことから、このプロセスは全社共通となる。内部における対応のみならず、外部（メディア、クライアント、従業員、取引先、その他の利害関係者）に対するメッセージも重要である。

規制当局にとっては日常的なセキュリティ事象 - 経営陣はどのような知識を獲得し、どのように準備すべきか？

米国では、多くの規制当局が情報漏洩に目を光らせ、被害を受けた組織を調査している。全て、サイバー攻撃が発生すると、州検事総長、連邦取引委員会（FTC）、市民権局が乗り出す。最近では、状況を注視していたFTCが、消費者の対応および自衛に関する助言を含む条項を発表した。

FTCは「一般消費者に対する反競争的、欺瞞的または不公正な商慣行を防止」[4]することを使命とし、「市場における不正、欺瞞、不公正な商慣行を防止」[5]することを戦略的目標の一つとして掲げていることから、情報漏洩が発生した企業の調査を頻繁に実施する。場合によっては、同意判決に基づき、包括的な情報セキュリティおよびプライバシープログラムの設計、実装、維持や、独立した第三者からプログラムの有効性評価を長期的に（多くの場合は20年間）受けるよう要求することもある。多くの場合、情報漏洩が発生した組織はFTCなどの規制当局から罰金を科されることになる。このような調査に適切に備え、規制当局に対して誠実な取り組みを示すために、侵害が発生する前に包括的な情報セキュリティおよびプライバシープログラムを設計しておくとよいだろう。

4　http://www.ftc.gov/about-ftc
5　同上

これまでに取り上げたリスクは、運用やコンプライアンスに関するもであった。その他のエンタープライズリスクについても真剣に検討する必要がある。巧妙化した国家レベルの攻撃者（攻撃者のタイプの概要については図1を参照）は、機密性の高い知的財産や、通信、その他の戦略的資産および情報を狙う。保証およびコンプライアンスに関する基準は、内部不正に関するリスクにはほとんど対応していない。エンタープライズリスクは独立した統合監査の範囲には含まれず、情報漏洩が発生した場合、一般投資家への情報開示は特に要件とはなっていない。しかし、情報漏洩が起これば、事業部門や製品、サービスに重大な影響を及ぼしかねない。

サイバー犯罪のタイプ - 大統領命令と検討すべき疑問

2013年2月、オバマ大統領は銀行や金融を含む重要なインフラストラクチャーに重点を置いたサイバーセキュリティの自主基準を求める大統領命令に署名した。2014年2月、国土安全保障省（DHS）はこの包括的な一連の基準を「サイバセキュリティフレームワーク」として発表する。ただし、作成に関わった関係者ですら、国家レベルまたは組織犯罪などの手強い脅威から完全に保護することはできない恐れがあると指摘している。ここに、コンプライアンス（法令遵守）とセキュリティ（安全性）の差がある。この差を埋めるには、経営陣の行動が不可欠である。

図1：攻撃者のプロファイル

悪意ある攻撃	動機	標的	影響
国家レベル	• 経済、政治、軍事的優位性	• 企業秘密 • ビジネスにおける機密情報 • 新技術 • 主要インフラ	• 競争優位性の喪失 • 主要インフラの停止
組織的な犯罪	• 即時性のある金銭的利益 • 将来の金銭的利益を得るための情報収集	• 財務／決済システム • 個人情報 • ペイメントカード情報 • 保護されている健康情報	• 規制当局からの調査および罰金に伴う出費 • 消費者団体訴訟や株主代表訴訟 • 顧客からの信頼の失墜
政治的ハッカー（ハクティビスト）	• 政治的・社会的変革への影響 • 商慣行に対する変更圧力	• 企業秘密 • ビジネスにおける機密情報 • 経営幹部、従業員、顧客、取引先に関する情報	• 事業活動の停止 • ブランドや評判 • 顧客からの信頼の失墜
内部者	• 個人的利益、金銭上の利益 • 職場での復讐 • 愛国心	• 販売、取引、市場に関する戦略 • 企業秘密、知的財産、研究開発 • 事業運営 • 個人に関する情報	• 企業秘密の漏洩 • 運営の停止 • ブランドや評判 • 国家安全保障への影響

経営幹部がサイバーセキュリティに継続的に取り組むことは、ビジネスの保護だけではなく、収益拡大にもつながる。組織としてサイバーセキュリティ態勢を評価するとき、最初に検討すべき領域は少なくとも三つあり、幹部以上のメンバーが以下の質問に答える形で評価する必要がある。

1. **サイバーセキュリティ戦略および能力の強化**：統合サイバーセキュリティ戦略は、組織のビジネスモデルの基幹を成していますか？戦略では、セキュリティの範囲全体（技術、物理、プロセス、人的資源）を考慮していますか？組織として必要なリソースを確保し、投資を行っていますか？重大な脅威、新技術、戦略的イニシアチブについて、内部のビジネスリーダーに情報を提供する機能はありますか？サイバーセキュリティ戦略を利害関係者や投資家、規制当局、ビジネス上のエコシステムのパートナーに説明できますか？
2. **セキュリティリスク環境の変化の把握と適応**：ビジネスを展開するうえでどの情報に価値があるのかを把握していますか？それらの資産を適切に保護するために、セキュリティ対策に優先順位を付けていますか？資産が損なわれた場合のビジネスへの影響を数値化していますか？ビジネスにおける脅威の大きな変化を把握していますか？組織にとっての敵は誰ですか？敵の標的は何ですか？どのような方法が用いられる可能性がありますか？内部者の脅威に関して、どのような管理策が整備されていますか？組織として、内外の情報源を積極的に利用していますか？セキュリティ侵害が発生したことはありますか？その侵害をどのように検知しましたか？セキュリティ上の事象や活動に対する管理策および対策の即応性はどうですか？業界が抱えている脅威について情報を収集し、理解するために、官民協同のコミュニティに積極的に参加していますか？セキュリティ管理策の状態を定期的に評価していますか？セキュリティインシデントに対応するための計画はありますか？その計画に基づく訓練は行っていますか？
3. **共通の構想と文化を通じてのセキュリティ態勢の向上**：従業員は情報資産の保護における各自の役割を理解していますか？また、必要なツールとトレーニングを受けていますか？サプライヤーやサービスプロバイダーに対し、どのような保証を求めていますか？リスクポートフォリオの監視、監査、改善を積極的に行っていますか？エコシステム全体で資産を保護するための基準を整備していますか？

近年のセキュリティ事象や企業を取り巻く脅威の進化から、POSおよび決済システムの見直しは必須である。ただし、経営幹部が前に挙げた疑問に向き合う際には、小売バリューチェーン全体、また基盤となるITシステムについても考える必要がある。POSおよび決済システムインフラストラクチャーでは、業界の運用基準により、強化されたセキュリティ保護策が長年にわたって重視されてきた。一般的に、これらのPOSおよび決済システムは、小売業界で最高の技術的保護が施された環境と見なされている。事実、データ保護の観点から、これほど配慮の行き届いたシステムは他にはほとんどない。多くの企業においては、安全性が非常に高いはずの環境で情報漏洩が発生した場合には、技術エコシステムとして連携していたエリアを超えてどの程度影響を受けるかを検討する必要がある。

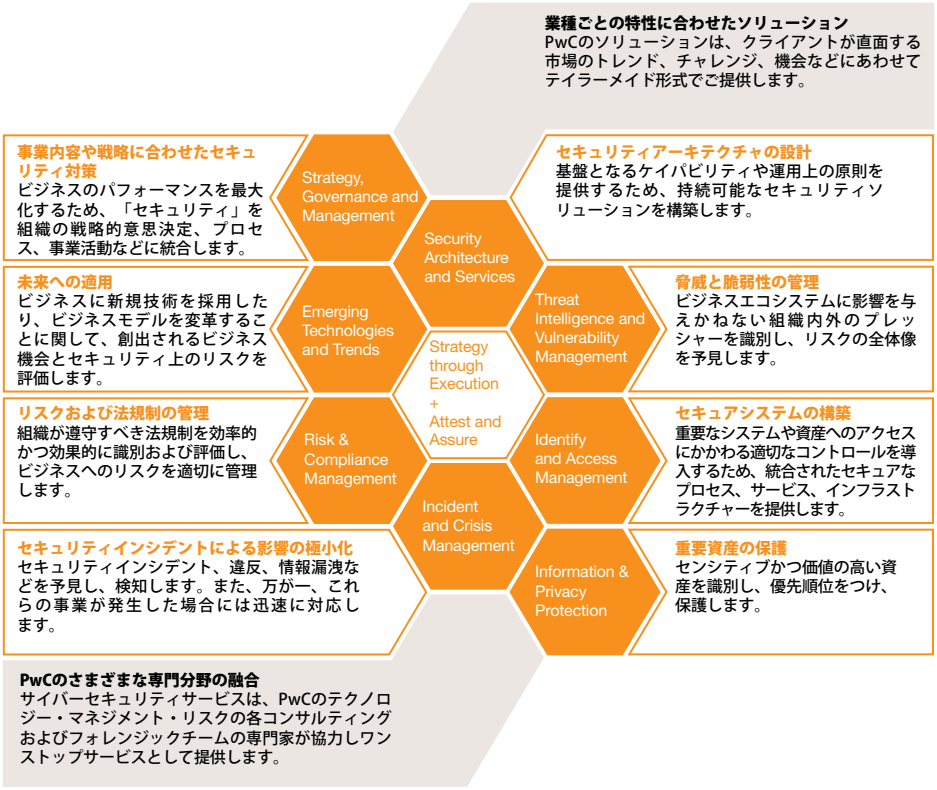
PwCのケイパビリティ

PwCは、攻撃者の一歩先を行く動的なサイバー攻撃および侵害／インシデントの兆候の察知、ビジネスエコシステムに内在するリスクへの適応および対応、ビジネス戦略の基礎を成す最重要資産の優先順位付けと保護を支援します。

PwCのサイバーセキュリティコンサルティングサービスは、市場で定評のあるベストプラクティスに基づいています。将来の脅威に備えた革新的なソリューションをただちに提供することで、グローバルにつながったエコシステムの中で動的に変化するサイバーリスクへの適応および対応を可能にします。

オバマ大統領が掲げるサイバーセキュリティ構想と同様に、企業の経営幹部にとってもセキュリティをどのように評価するかということは重要な問題です。評価および監査にはどのような基準を用いるべきでしょうか？その結果を実際のセキュリティに結び付けるにはどうすればよいでしょうか？また、企業の経営陣、株主に対し、サイバーリスクやその他の企業リスクの透明性と可視性をどのように実現するかという問題も同様に重要です。

図2：PwCが提供するサイバーセキュリティコンサルティングサービスの各種ソリューション*



*PwCが提供できるサービスの範囲は、独立性の問題によってお客様が制限された事業体かどうかによって異なります。いずれの場合も、PwCはお客様にさまざまな機能を提供できます。

お問い合わせ先

プライスウォーターハウスクーパース株式会社
コンサルティング部門　テクノロジー

松崎　真樹
パートナー
03-3546-8480
maki.matsuzaki@jp.pwc.com

山本　直樹
ディレクター
03-3546-8480
naoki.n.yamamoto@jp.pwc.com

林　和洋
マネージャー
03-3546-8480
kazuhiro.hayashi@jp.pwc.com

矢野　薫
マネージャー
03-3546-8480
kaoru.yano@jp.pwc.com

当社Webサイトはこちら
http://www.pwc.com/jp/advisory

www.pwc.com/jp

本報告書は、PwC メンバーファームが2014年1月に発行した『Answering your cybersecurity questions - The need for continued action』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/japan-knowledge/report.jhtml
オリジナル（英語版）はこちらからダウンロードできます。 http://www.pwc.com/us/en/increasing-it-effectiveness/publications/answering-your-cybersecurity-questions.jhtml
日本語版発刊月： 2014年4月 管理番号： M201403-6