CompTIA

INFORMATION SECURITY TRENDS

SECTION 1: MARKET OVERVIEW

RESEARCH

TENTH ANNUAL • NOVEMBER 2012

情報セキュリティ投資

以下のデータからもわかるように、セキュリティに対する継続的な注視はセキュリティ関連の製品やサービスのセールスを確固なものとしています。

- PricewaterhouseCoopers の報告書によると、2011 年の世界のサイバーセキュリティ投資は 600 億ドルに達し、今後 5 年間は、毎年その投資額の 10%の増加が予測されています。報告書によると、米国ではプライベートセクターと政府の均等に投資が行われている一方で、他国ではほぼプライベートセクターが推進力となっていることがわかりました。
- ガートナーによると、2011 年の世界のセキュリティソフトウェアの売り上げは 177 億ドルでした。これは 2010 年と比較し 7.5%の増加です。こうした売り上げの上位 5 企業は、シマンテック、マカフィー、トレンドマイクロ、IBM、EMC で、市場の 44%を占めています。
- IDC では、中小企業（SMB）のセキュリティテクノロジーの投資が、大幅な成長をみせるとし、2015 年には 56 億ドルになると予測しています。SMB の IT 投資は、毎年 5～6%増加していくであろうと予測していて、セキュリティ製品やソリューションへの投資は、その倍の速さで増加するであろうとみています。
- Infonetics からのデータでは、ネットワークセキュリティ市場の収益が 2016 年までに 67 億ドルになることを示しています。このカテゴリにおける 2011 年の売り上げ上位 3 社は、シスコ、Cehckpoint、Juniper でした。
- IDC は、ワールドワイドのマネージドセキュリティサービス（MSS）市場が 2011 年に 149 億ドルに達すると予測していて、2016 年には 261 億ドルになるとしています。ネットワークセキュリティサービス市場は、2011 年から 2016 年にかけ、CAGR（年複利成長率）19.7%と、非常に大きな成長をするというデータが出ています。2011 年から 2012 年にかけてマネージドセキュリティサービ

新興分野にみる情報セキュリティ投資

セキュリティ投資の一部には、データロス、モバイルセキュリティ、クラウドセキュリティといった新興分野への投資増加も含まれます。

- 2012 年現在、漏えい被害件数は 900 万以上であることから（Identity Resource Center データより）、Data Loss Prevention（DLP: データロス防止）市場の成長はいうまでもありません。2010 年発表の IDC のデータでは、2009 年の DLP 市場は、$262.3 ミリオン（2.6 億ドル）と推定。今後 5 年間で 20.2%の割合で成長を続け、2014 年には$658 ミリオン（6.6 億ドル）以上となると予測しています。2011/2012 年においては$387 ミリオンから$472 ミリオンになると予測されています。
- Vision Gain および Juniper Research のデータでは、モバイルセキュリティの成長も指摘されています。Vision Gain は、グローバルでのモビリティセキュリティ市場は 2012 年$1.6 ビリオン（16 億ドル）に達すると予測。Juniper Research は、2016 年までにモビリティセキュリティソフトウェアプロバイダーは$3.6 ビリオン（36 億ドル）にもなるビジネス機会があると想定しています。
- Forrester の調査では、クラウドセキュリティは 2015 年までに$1.5 ビリオン（15 億ドル）市場になると予測。Tech Navio のデータでは、2010 年、クラウドセキュリティ市場はグローバルのセキュリティ市場の 2%を占めていたことを言及。2014 年にはこの割合は 4%まで上昇すると発表しています。
- 企業がセキュリティ脅威の対応に追われるように、IDC では、セキュリティ市場は 2009 年の$198 ビリオン（1980 億ドル）から 2014 年には$905 ビリオン（9050 億ドル）まで成長するであろうと予測しています。

スの世界でみた成長率は 12.6%でした。

・ チャネルの観点からみると、セキュリティに関連するチャネル企業の 66%が、来年の収益の成長を見込んでいます。またそのうち 16%が、大幅な増加（10%以上）を予測しています。

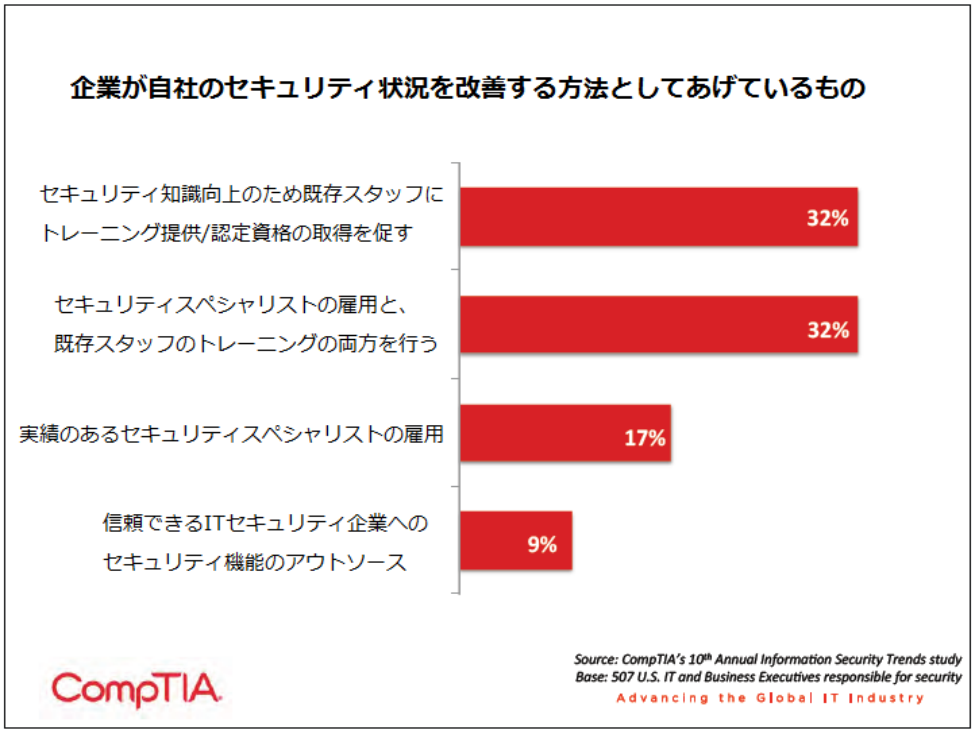
InformationWeek Analytics が実施した戦略的セキュリティ調査では、昨年度と同様に、約 4 企業のうち 1 企業の割合で、彼らの IT 予算の 10%以上をセキュリティに投資していると回答していました。ROI の観点からみると、情報セキュリティへの投資は妥当であることがわかります。2012 年ノートンのサイバー犯罪報告書では、消費者サイバー犯罪の直接的コストは、世界で 1 千億ドルになると推定されています。これは一人当たりの平均損失額が 197 ドルとなり、ソーシャルやモバイルといったプラットフォームでの犯罪数が増えていることがわかっています。Ponemon Institute 発表の、2011 年のデータ漏えいに関するコスト調査では、組織における被害額そして、盗難/紛失から生じた被害額の報告は昨年比で減少傾向にあるものの、それぞれ前者は 550 万ドル、後者は 194 ドル（1 件あたり）となっています。

サイバーセキュリティと IT 要員

情報セキュリティは、需要（デマンド）が供給（サプライ）を上回るという特異な分野の一つでもあります。Indeed.com の求人集積では、情報セキュリティの職数は 2006 年以降上昇を示しています。

米国労働統計局では、2011 年に情報セキュリティ分析者というカテゴリを設け、2010 年から 2020 年の 10 年間における増加率を 22%と予測しています。全職業の成長率平均は 14%といわれています。2012 年(ISC)2 の Career Impact Study 調査では、必要スキルを持つ IT セキュリティプロフェッショナルの確保は困難であること、また回答者の 96%が雇用されていると回答しました。また、セキュリティの予算と雇用は増加傾向にあり、人員における優先ニーズはセキュリティであることがわかりました。CompTIA の「10th Annual Information Security Trends（第 10 回情報セキュリティ動向）」では、回答者 49%がセキュリティスペシャリストの雇用を検討していると同時に、既存スタッフのトレーニングを検討してい

ると回答していました。



CompTIA の調査では、5 社のうち 1 社の割合において、IT セキュリティスペシャリストの雇用は難航したと報告しています。この数字は、昨年は 40%であったことから、大幅に低減していることがわかります。外部データではセキュリティプロフェッショナルの需要の大きさを示していることから、昨年の雇用が停滞していたということにもなり得ます。

CompTIA®

INFORMATION SECURITY TRENDS

SECTION 2: SECURITY IN A NEW TECHNOLOGY LANDSCAPE

RESEARCH

TENTH ANNUAL • NOVEMBER 2012

変化に対する反応

セキュリティ領域は、テクノロジー環境の構成や変化と密接に関係しています。ツールやプラクティスは既存の使用環境をもとに構築され、またテクノロジー変化があると、攻撃者はそうした変化を攻撃のチャンスと捉えます。セキュリティは本来多くの企業にとってより敏感に対応するべき項目なのです。つまり、テクノロジーを特定の方法で使うということがわかっているのであれば、そのテクノロジーのセキュア状態を保つための手順を踏まなければならないのです。将来利用されるかもしれないテクノロジーに必要となるセキュリティツールに投資する企業はほとんどいません。

セキュリティ実践者の観点からみると、市場の変化にすばやく反応する必要性および、新しいテクノロジーを積極的に検討する必要性があるといいます。テクノロジーは、広範囲的に導入されることがわかっていることから「転換期」にあり、セキュリティベンダーやサービスプロバイダーは、長期的な見方、過去の事例や現在の知識を今後の可能性に活かすよう取り組みをするべきです。ネットワーク化されたオフィスやインターネット上のビジネスへの移行は新しいセキュリティ手法をもたらし、進行中のエンタープライズテクノロジーは今後重要な展開を見せるでしょう。

CompTIA の第 10 回情報セキュリティ動向調査では、現在起きている変化を以下のように特徴付けいます。またエンドユーザーは、それらをセキュリティプラクティスに影響を与える要因として認識しています。

- 57%: インターネットベースアプリケーションへのさらなる依存

エンタープライズテクノロジーの主要な出来事

様々な種類の産業/機械テクノロジーがビジネスに大きな影響を与えましたが、90 年代半ばからテクノロジーを支配していたのは情報テクノロジー（IT）です。IBM は、この期間を 5 つの類型に分けています。必ずしもすべてを包括するものではありませんが、テクノロジーおよびセキュリティでの変化を捉える上でのひとつの基準を提供しています。

- **メインフレーム**（大型汎用コンピュータ）：最初にビジネス用に使用されたコンピュータは専門知識が必要とされた高価マシンでしたが、導入した企業は大きな競争優位性を実感することができました。
- **デパートメンタルコンピューティング**（部門コンピュータ）：コンピューティングがエンドユーザーにより近くなった第 1 ステージです。IT 部門は、完全監視を必要としないコンピューティングの使用を検討することとなります。
- **PC**: PC の導入を境に、エンドユーザーはテクノロジーに精通し、多くの操作が可能になります。物理メディアに保存することで仕事を自宅に持ち帰ることが可能に。企業データの切り離しに関するガイドラインの実施が進められます。
- **インターネット**：より速い接続性により、新しいビジネスモデルやセキュリティ要件が誕生します。世界中に情報を発信することで、世界も企業システムにアクセスが可能と成り得るという双方向のパスが生まれます。
- **ソーシャルビジネス**：さらなるコマンド＆コントロールの体制がエンドユーザーにゆだねられます。

- 55%：デバイス、システム、ユーザーのより大きなインターコネクティビティ（相互接続性）
- 51%：ソーシャルネットワーキングの上昇

クラウドコンピューティング、モビリティ、ソーシャルビジネスは、エンタープライズでのテクノロジーの在り方に変化をもたらす 3 大要因としてあげられます。これら要因については以前の調査内容でも言及されましたが、ソーシャルネットワーキングが上位に入っているという点で異なります。攻撃者はこうしたトレンドの導入を悪用し、無防備となった脆弱性の発見を常に行っています。IT 部門やソリューションプロバイダーは潜在する脅威に十分認識し、新たな防御策で迅速に対応しなければなりません。

モバイルデバイスの管理

モビリティは、クラウドコンピューティング以上に、企業の IT フローやセキュリティポリシーに混乱をもたらすかもしれません。多くの IT 部門がメインの作業デバイスをラップトップとしていることから、セキュアな領域に留まることは困難であるように思えます。しかし消費者市場でのスマートホンやタブレットの導入および使用は、企業レベルまで影響を与え始めていることから、企業は対応を再検証する必要性に追われています。

モバイルセキュリティの懸念事項上位

回答者の%が、懸念事項の「深刻性」を表します

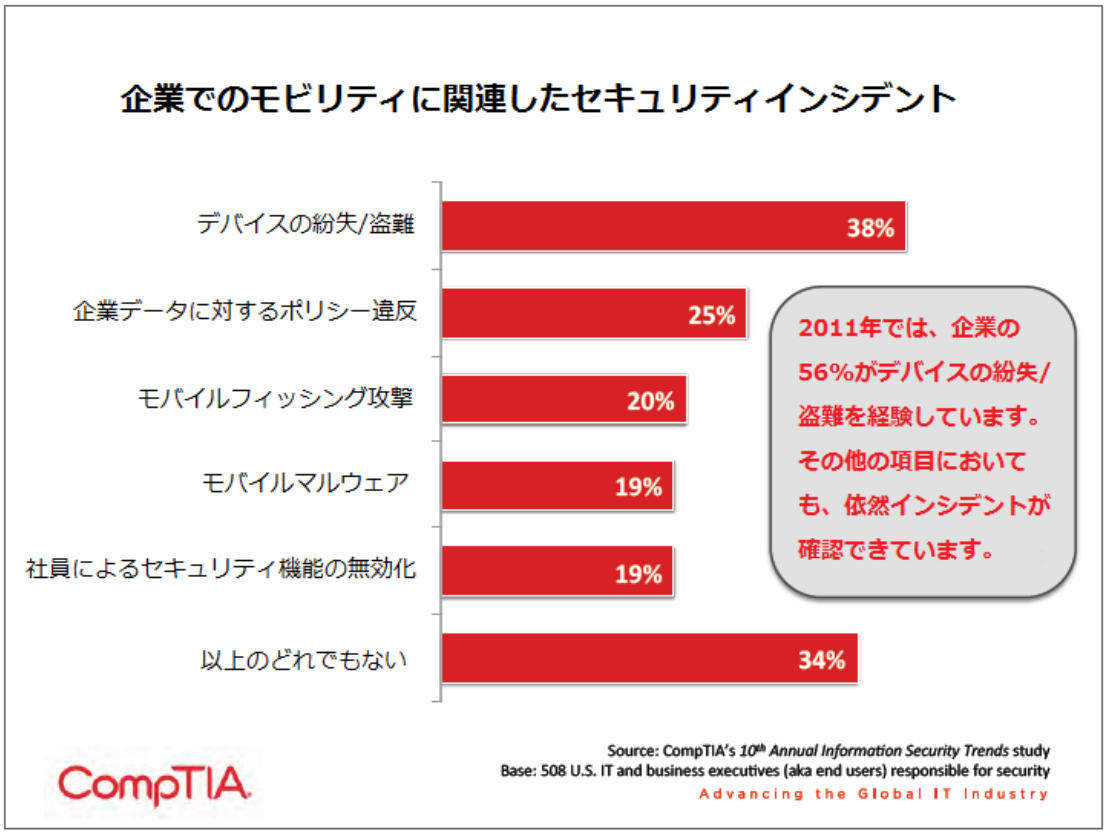
33%	許可のないアプリケーションのダウンロード
30%	企業デバイスの盗難または紛失
29%	オープン Wi-Fi ネットワークに関連するリスク
29%	マルバタイジング 悪意のある広告
28%	ソーシャルメディアに関連するリスク
28%	モバイルデバイスに特定したウイルス/マルウェア

スマートホンやタブレットにはメインの課題が 2 つあります。一つは、エンドユーザーは IT 部門が提供するデバイスの使用を好ましいと思わない点があります。社員は、スマートホンやタブレットに対する私的なつながりを強く感じることから、自身が好むデバイスの使用を望む傾向があります。これは BYOD（Bring Your Own Device）を支える主な推進力となっています。

二つ目の課題には、これらデバイスはラップトップよりさらにクローズドの環境にあるという点です。IT 部門は、スマートホンとタブレットに今まで同様の保護措置を取ることができないことから、制御された形での企業システムやデータのアクセスの管理が難しくなります。また、セキュリティ措置がインストールされたことで、デバイス機能に影響を与える、生産性に影響を与えるといったことも考慮する必要があります。

許可のないアプリケーションのダウンロードは、セキュリティプロフェッショナルの間でも常に上位にあるセキュリティ懸念事項です。これはアンドロイドエコシステムでのマルウェアの増加が原因となっています。comScore の市場インテリジェンスデータでは、アンドロイドが US スマートホン市場の 53%を占

めていることがわかっています。トレンドマイクロでは、アンドロイドマルウェアは予想成長の 2 倍の速さで進み、2012 年の終わりには 250,000 のマルウェアサンプルがみつかるだろうと予測しています。iOS もマルウェアの影響を受けないわけではありません。マルウェアフリーの 5 年間の後、2012 年 7 月に App Store で最初のマルウェア「Find and Call」が発見されました。



現時点においては企業におけるモバイルマルウェアは主要な問題としてはあがっていません。また、「セキュリティ機能の無効化」の回答については、デバイスにセキュリティ機能をインストールしている企業の数に依存しています。（モバイルデバイスの解錠にパスコードを必要とする企業は 67%でした）

調査結果では、デバイスの紛失や盗難が最も一般的なセキュリティインシデントとしてあがりました。これは Mobile Device Management（MDM: モバイルデバイス管理）の概念を牽引しています。企業が実施するモバイルセキュリティインシデントの対策方法には、追跡ソフトウェアのインストール（47%）、デバイス紛失時の手順書の作成（44%）、モバイルデバイスの暗号化の実施（43%）といったデバイスの追跡やセキュア化が中心となります。一年前のインシデント数から大幅な減少が見られていることから、これらの戦略はデバイスの紛失や盗難に効果を発揮しているようです。

モバイルセキュリティインシデントを経験したわずか 37%の企業は、正式なモビリティポリシーの作成に着手していることがわかりました。CompTIA の「Trends in Enterprise Mobility（エンタープライズモビ

リティの動向)」調査では、調査参加の企業のわずか 22%が、組織内に正式なモビリティポリシーが存在すると回答していました。また、そのようなポリシーを策定中であるとした企業は 20%でした。モバイルデバイス使用は、多くの社員にとって日常となっていることから、アクティビティの許容範囲について適切に明記しなければなりません。モビリティのガイドラインはすでに存在するポリシーに付加的に作成されるのではなく、モバイルデバイスを使用する人員の割合や、業務フローへの影響を考慮し、モバイルデバイスだけの個別ポリシーを策定し、企業規定を明確にするのが望ましいといえるでしょう。

企業がモビリティ戦略を立てる一方、インテリジェントセンサや machine-to-machine（M2M）システムの高まりがモビリティカテゴリに見られ、そこにはセキュリティリスクも存在しています。センサからストリームされるデータはビジネスに有効となるよう分析がされますが、同時にサイバー犯罪者もデータの搾取方法に着手しているかもしれません。まずはデータの強力な暗号化が良いとされます。後にはセキュリティやプライバシーに関するベストプラクティスが紹介されるでしょう。このトピックについては、CompTIA の An Introduction to M2M Systems 白書で確認することができます。

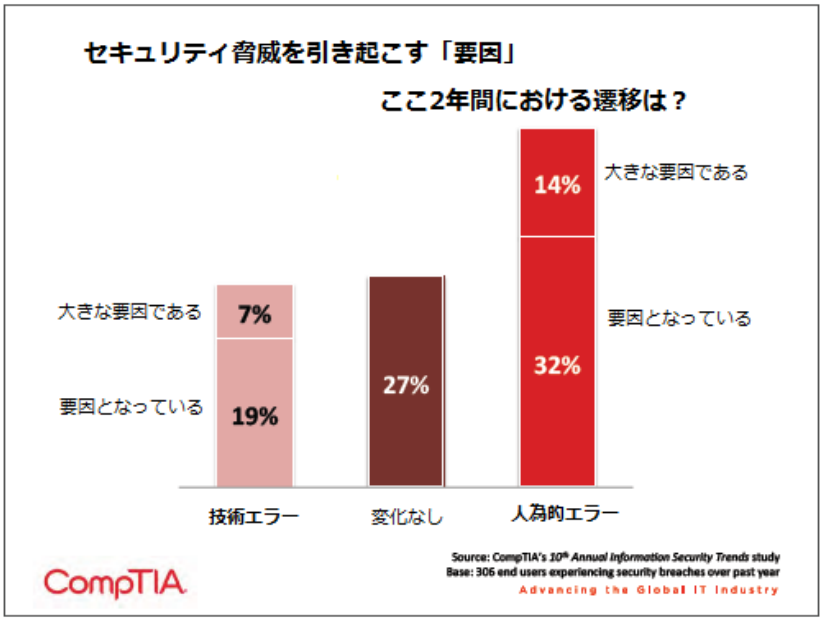
エンドユーザーにとって多くの権限を有することは多くの責任を意味します

IBM はエンタープライズテクノロジー時代の第 5 フェーズを「ソーシャルビジネス」としています。またソーシャルネットワークは、企業のコミュニケーションやコラボレーションの在り方を変える「手段」の代表例でもあります。ソーシャルメディアサイト（例：Facebook、Twitter、LinkedIn）上でのマーケティングや顧客コミュニケーション、またソーシャルビジネスツール（例：Jive、Telligent、IBM コネクション）を使ったインターナルのコミュニケーションやコラボレーションを実施など、ソーシャルテクノロジーはエンタープライズに大きな影響力を与えています。

こうした影響に比例して、セキュリティへの懸念も増加しています。ソーシャルネットワークは私的な情報を共有するというコンセプトのもとにあり、ユーザーはソーシャルサイトを安全なプラットフォームとして閲覧する傾向があります。スパム送信者やサイバー犯罪者は、そうした見解を利用し攻撃を仕掛けます。知人から送られたかのようにみえる短縮 URL、ソーシャルサイトで実行される有害なアプリケーション、マルバタイジングと呼ばれる不正なバナー広告など、マルウェアやウイルスは様々な手法で展開されています。これらの中にはシステムにワームやトロージャンをもたらし、それらが深刻な脅威となって企業を脅かすこともあります。また、like-jacking（like ジャッキング）として知られる、不正操作を行うボットのようなものも存在します。

またソーシャル空間における深刻なセキュリティ脅威も存在します。ソーシャルエンジニアリングのスキームは、巧みな言葉や盗み聞きなどの手段によって、パスワード等の個人情報を入手することを目的としています。攻撃者は、ユーザーによって公開された情報を使い、なりすましをし、アカウントアクセスに必要となる情報のリクエストを行います。標的となるアカウントが企業である場合その被害は莫大なもの

と成り得ます。Wired のシニアライターである Mat Honan は、2012 年 8 月に自身におきたハッキング体験を語っています。適切に保護されていないアカウントがいかに容易にハッキングされてしまうか、アカウントを相互リンクさせること、個人/ビジネスアカウントでの同じパスワードの使いまわしの危険性を発表しています。



このような問題はコンシューマライゼーションとして考えられます。テクサポートに頼ることなく、コンピューティングリソースにアクセスし簡単に利用ができることで、より多くの生産性がうまれます。しかし、そのようなリソースを扱う際、どのような事が違反/侵害行為と成り得るのかなど、ユーザーにセキュリティ知識が必要とされないことで生じるセキュリティリスクの可能性も存在します。

セキュリティインシデントを経験している企業は、コンシューマライゼーションが与える影響を理解しています。過去 2 年間をみても、人為的エラーが違反行為における要因として増加していることがわかっています。こうした人為的エラーは、悪意的な理由よりも、専門的知識の欠如や、規律の怠りが原因と考えられています。

人為的要因に関しては、外的脅威からの保護とは異なるアプローチが必要です。テクノロジーの活用はもちろん、教育、トレーニング、ポリシー実施が重要なカギを握ることとなります。後半のセクションでは、コンシューマライゼーションの問題を検証し、企業のセキュリティへの取り組みに対す洞察を提供しています。

CompTIA

INFORMATION SECURITY TRENDS

SECTION 3: THREATS AND DEFENSES

RESEARCH

TENTH ANNUAL • NOVEMBER 2012

脅威の情勢

IT の世界では、セキュリティ違反/侵害のニュースは日常的となっています。デジタルデータは、コンシューマやビジネスにおいてますます重要な役割を担い、そのデータはクラウドコンピューティングにつながっています。大きなセキュリティインシデントが起こる毎に、企業のセキュリティスキームの定期的アップデートの必要性が浮き彫りとなり、ユーザーは変化する環境に注意をする必要があります。

機密情報に関わる違反/侵害事項は、企業の評判を傷つけ、小さな事項であっても企業の財務に影響を及ぼします。本レポートのセクション 1 ではセキュリティ脅威により発生するコストについて言及しましたが、データ回復、ウイルス除去に費やす時間が生じることから、収益面は直接的かつ間接的な影響を受けます。セキュリティ脅威の一連はその大きさに関わらず、コストの蓄積に直結しているのです。

Symantec は、サイバーセキュリティ脅威の性質や発生数を分析するインテリジェンスレポートを月毎に発行しています。2012 年 9 月の報告には、いくつかの共通項目における見解が含まれています。

- スパム発生率： 75%（ワールドワードで送られるメールの 4 件中 3 件はスパム）
- 245 件中の 1 件は、フィッシングとして特定される
- 211 件中の 1 件は、マルウェアを含む
- 1 日に 780 のマリシャスウェブサイトがブロックされている

これらの数字は変動をしますが、全体に共通した傾向があります。2010 年の半ば以降、スパムの数は徐々に減少し、マリシャスウェブサイトの数は 2010 年および 2011 年後半の急増時と比べ以前のレベルに戻っています。スパムの減少はあるものの、依然この分野はアクティブであることには変わりなく、攻撃者は常に機会をうかがっています。E メール管理サービスを行う Baydin は、平均的な E メールユーザーは一日に推定 147 通を受信するといいます。これは個人および会社メールの両方をカウントしていますが、フィッシング/マルウェアの発生件数レートを見ると、E メールユーザーは毎週これらの脅威を目にしていることとなります。

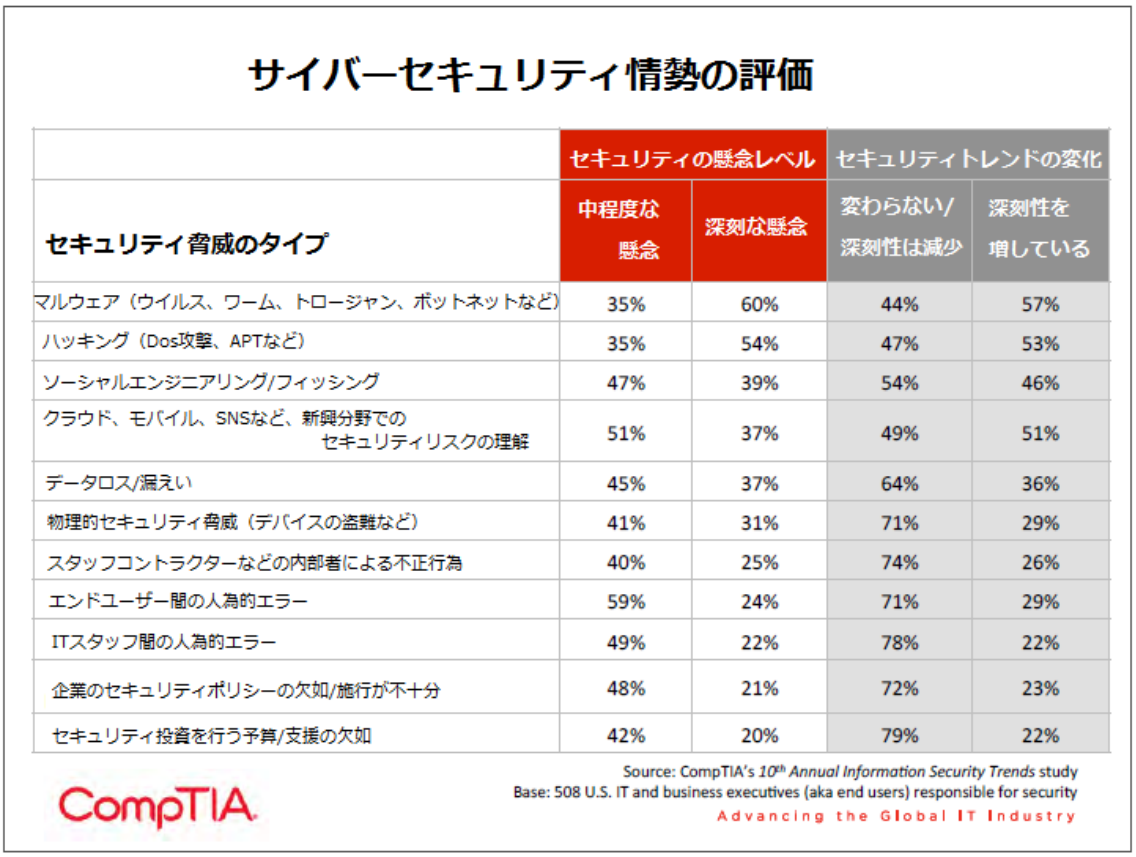
また上記以外にも、テクノロジーの変化をついた新しい形態の攻撃も登場しています。

- 企業の大半が内部ポータルを持つことから、Advanced Persistent Threats（APT: アドバンスドパーシスタントスレット攻撃）や Denial of Service（DoS: ドス攻撃）が、情報搾取やサービス提供の不能化を試みる攻撃者の一般的な手法となっています。
- iPhone や iPad の登場は、ラップトップ市場に波及効果を及ぼし、MacBook 市場は徐徐に下降しました。残念なことにこうした成功は標的にされやすく、2012 年 4 月に 600,000 の Mac が Flashback トロージャンに感染されるというニュースが流れました。これは、Mac を標的としたマルウェアの先駆けとなりました。
- IPv6 プロトコルが広く導入され始めたこともまた標的原因となりました。サイバー犯罪者は、プロトコルの脆弱性、IPv4 からインスタンスを移動する際見つかったいかなる脆弱性につけ込み、悪用する

ことが可能です。

企業のセキュリティ対策は、外部からの攻撃者だけではなく内部漏えい（悪意のあるなしに関わらず）のリスクにも万全でなければなりません。また、複雑化する規制環境も整える必要があります。

CompTIA の「10th Annual Information Security Trends（第 10 回情報セキュリティ動向）」調査の参加企業は、これらのリスクを十分理解をしています。最大の懸念は、マルウェア、ハッキング、ソーシャルエンジニアリングなどの外部的脅威に集中していました。悪意のある内部者による不正行為や、意図的ではない人為的エラーなどの内部的脅威はリストの下位にあがりました。



サイバーセキュリティ情勢の評価

	セキュリティの懸念レベル		セキュリティトレンドの変化	
セキュリティ脅威のタイプ	中程度な懸念	深刻な懸念	変わらない/深刻性は減少	深刻性を増している
マルウェア（ウイルス、ワーム、トロージャン、ボットネットなど）	35%	60%	44%	57%
ハッキング（Dos攻撃、APTなど）	35%	54%	47%	53%
ソーシャルエンジニアリング/フィッシング	47%	39%	54%	46%
クラウド、モバイル、SNSなど、新興分野でのセキュリティリスクの理解	51%	37%	49%	51%
データロス/漏えい	45%	37%	64%	36%
物理的セキュリティ脅威（デバイスの盗難など）	41%	31%	71%	29%
スタッフコントラクターなどの内部者による不正行為	40%	25%	74%	26%
エンドユーザー間の人為的エラー	59%	24%	71%	29%
ITスタッフ間の人為的エラー	49%	22%	78%	22%
企業のセキュリティポリシーの欠如/施行が不十分	48%	21%	72%	23%
セキュリティ投資を行う予算/支援の欠如	42%	20%	79%	22%

Source: CompTIA's *10th Annual Information Security Trends* study
Base: 508 U.S. IT and business executives (aka end users) responsible for security
Advancing the Global IT Industry

全般に、前回の調査よりも懸念レベルが減少していることがわかりました。その一例に、データロス/漏えいを「深刻な問題」としている率が、前調査では 54%であったことなどがあります。

この減少は、調査参加企業に起きた違反インシデントに対する認識に基づいているように思われます。第 9 回情報セキュリティ動向の調査では、76%の企業が過去 1 年においてセキュリティインシデントを経験していました。最新の調査ではその数字は 61%まで減少しています。セキュリティの専門家は、一度何らかのインシデント経験をしている企業は、以降セキュリティをとても深刻に捉える傾向があるとしています。

しかし懸念レベルや発生件数の減少は、サイバー犯罪との戦いにおける進歩では決してありません。事実、多くの企業は、発見されることのなかった違反インシデントの存在を認めるでしょう。小さな違反インシデントやデータロスは長い期間気付かれないことがありますが、損害を与えることには変わりありません。

PandaLabs は、日々受信するファイル 206,000 件のうち 73,000 件は、新種マルウェアであることを報告しています。2011 年を「セキュリティ侵害の年」とした IBM の X-Force リサーチチームは、2012 年 9,000 もの新たな脆弱性が見つかるであろうと予測し、この数字は 2010 年の記録をしのぎます。ハッキングとマルウェアはサイバー犯罪者にとって最も有利な手段であり、新しいテクノロジーの導入は、内部者が不正行為を行う機会となってしまうのです。

CompTIA®

INFORMATION SECURITY TRENDS

SECTION 4: CHANGING SECURITY MINDSETS

RESEARCH

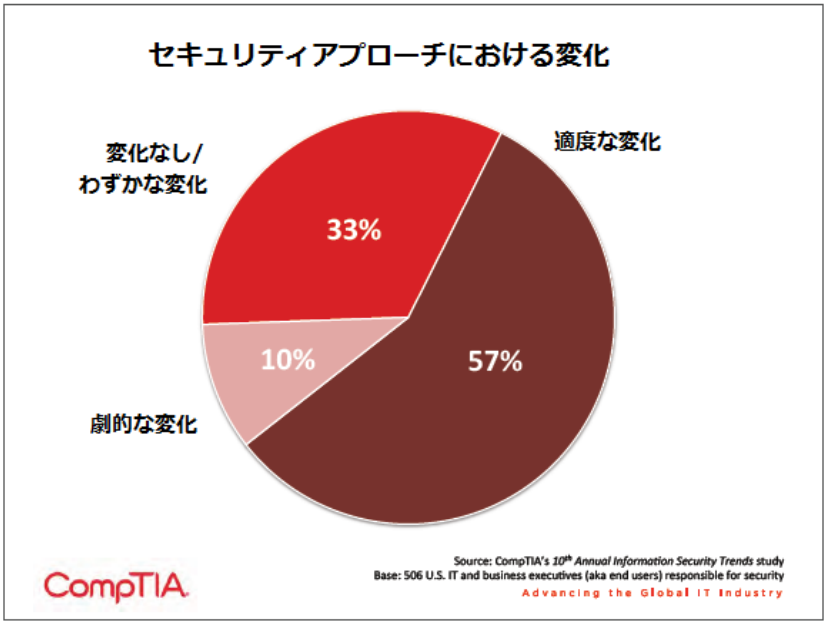
TENTH ANNUAL • NOVEMBER 2012

異なるアプローチ

従来のセキュリティテクノロジーは変化を続け、新たなテクノロジーが新たな問題に着手すべく始動しています。ファイアウォールがその良い一例といえるでしょう。ファイアウォールはパケットインスペクションをもとにネットワークトラフィックを内部でフィルターしますが、アプリケーションやプロトコルを理解するというレベルまで進歩しました。新しいテクノロジーには、Data Loss Prevention（DLP: データロス防止）や、Identity Access Management（IAM: アイデンティティアクセス管理）の分野があり、セキュリティ製品が、クラウドソリューションやモバイルデバイスを活用している企業のニーズに応えようという取り組みを行っています。

しかし、これらテクノロジーは、より大きなセキュリティフレームワークで使用されるべきものなのです。企業資産を保護するセキュア境界を作り上げることは至難であるいう概念が一般的に受け入れられている一方、従来のファイアウォールを超え、テクノロジーは進歩しているという方向に議論は向かっているようです。現状においては、包括的アプローチが経営のトップレベルから全部門に渡って再度見直される必要があるようようです。

CompTIA の調査に参加した企業の 3 分の 2 が、過去 2 年間において、自社のセキュリティに対するアプローチに変化があったと回答しています。劇的な変化があったと回答している企業もわずかながらありましたが、大半は適度な変化があったといいます。回答者は自身が所属する組織においてセキュリティの関与が高いことを踏まえると、彼らの言う「適度な変化」は、事業部門の社員からすると劇的な変化として捉えることもできます。



新たなセキュリティアプローチをもたらした要因には、IT 運用における変化があります。調査では 51%がクラウドソリューションまたはモビリティ戦略の導入により、新しいセキュリティ戦略が組まれたと回答していました。また、他組織で発生したセキュリティ違反事項（44%）、内部で発生したセキュリティ違反行為（31%）が推進力となっていることから、企業のセキュリティインシデントに反応する傾向がうかがえます。その他の推進力には、新しい知識のきっかけとなったトレーニングや認定資格の取り入れ、ビ

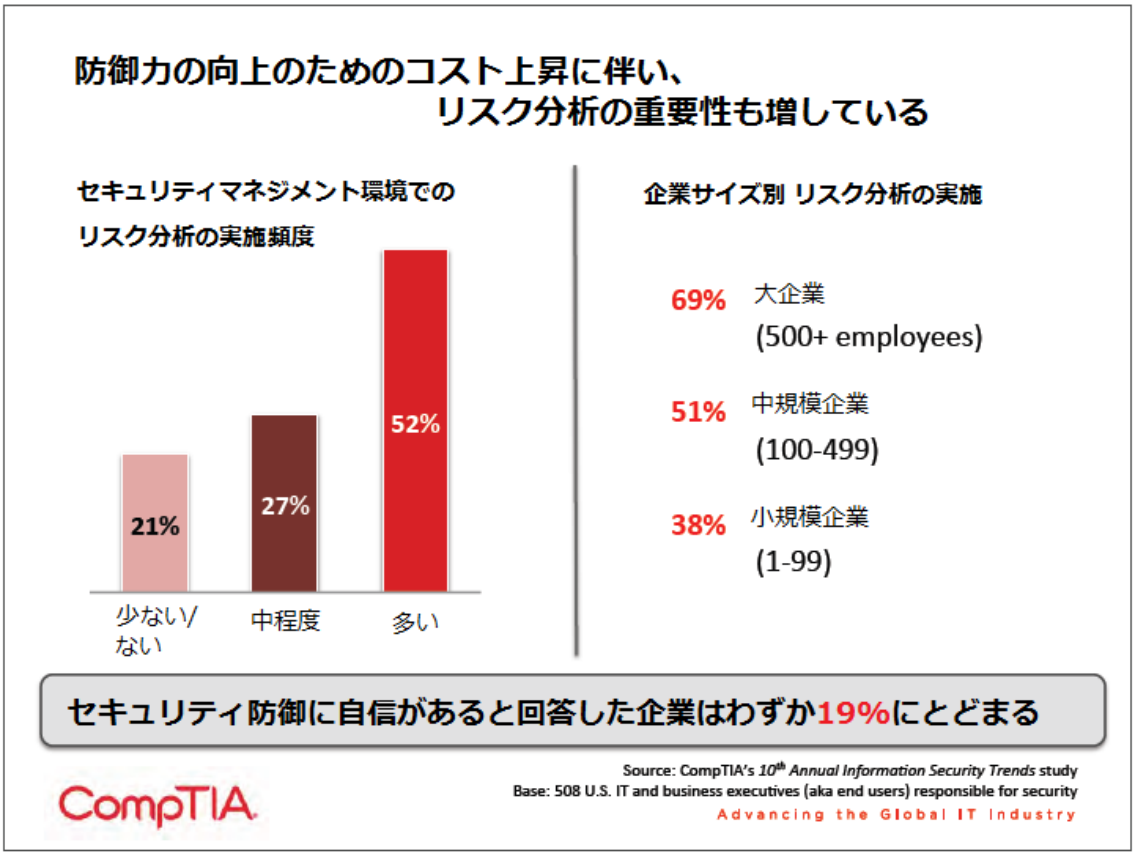
ジネス運用における変化、新しい分野への取り組みがありました。

近年のセキュリティアプローチには、「リスク分析」と「エンドユーザーの意識」という主に 2 つの分野での取り組みがあります。多くの企業はセキュリティリスク分析に精通していて、様々なリスクレベルに応じた適切な取り組みを行う一方、未だ従来の発想で運用をしている企業もあるでしょう。一般に、企業はエンドユーザーがいる成長曲線からさらに後れを取るといわれ、顧客主導の IT 情勢においてユーザーにセキュリティの知識や責任を提供することの重要性を十分理解していないことが問題としてあります。

リスクの分析、軽減、許容度

リスク分析は、プロジェクトマネジメントの思考を持つ企業にとってはなおさら、ビジネスをする上で欠かすことはできません。典型的な分析アクティビティには、リスク発生の確率、潜在する影響の推定、緩和/回避戦略の決定が含まれるでしょう。緩和/回避（ミティゲーション）を作り上げるまでの時間と労力は、（リスク発生の）確率やその影響に直接関連してきます。

企業情報を（物理的またはデジタルであろうと）単に機密箇所に保管していた時代は企業のリスク分析に対するアプローチはよりシンプルであったかもしれません。いかなる機密レベルの情報も、同じ扱いでセキュアな境界に置かれていたでしょう。また、そうした情報へのアクセスは、社内または VPN からであっても企業デバイスに制限することで、より容易な管理とされていました。PC が家庭で使用され始め、ノート PC が仕事のメインデバイスになっても、従業員が企業データを誤って外部に共有してしまう可能性はそれほど高くはありませんでした。



クラウドコンピューティングとモビリティのトレンドが、比較的短期間のうちに上記のような状況を一変させることになります。定義によると、パブリッククラウドコンピューティングでは、データを企業管理の外に置くことをいい、利用できる企業システムがなければモバイルデバイスで生産性を高めることも非常に困難となります。企業は、どちらの条件が打撃となるのか評価するのではなく、より強固な防御が必要となっているのです。

当然すべてのデータやシステムに強力な防御を確保することは費用がかかります。サーバーのアップタイムを例にして考えてください。もし、年間 100 万ドルの収益になるシステムが、99.9%（Amazon Web Services SLA で定義される）アップタイムのハードウェアで稼働をしているとしたら、年間 19 ドルの損失となるダウンタイムは約 10 分間ということになります。99.99%アップタイムを達成することで、ダウンタイムは 1 分に減らせることになりロスは 1.90 ドルになります。しかし、年間 20 ドル未満のために新たなバックアップソリューションを見つけることはないといえるでしょう。

同様のコスト構造はセキュリティ他の面にも言えることができます。セキュリティ防御に「自信あり」と答えている企業は 5 社のうち 1 社の割合にとどまりますが、組織によってはクラウドやモバイル環境においてすべてのデータをセキュア化し「万全」な状態にするために必要な投資をまかなえないという現状もあるようです。

結果として、企業は特定の技術を用いてリスク軽減をする、という違う方向からの戦略を始めています。また特定の種類のデータはクラウドソリューション向きではないと判断される場合もあります。企業の財務データ、クレジットカードデータ、知的財産に関するデータは社内で保管されるのが一般的とされます。またクラウドモデルを活用するためプライベートクラウドを作る企業もあるかもしれません。

リスク分析の注意点の一つに、IT 部門だけにとどまらないということがあります。その他のテクノロジー分野がそうであるように、セキュリティは企業全体の課題であり、リスクマネジメントの要件にかなうものとなります。すべてのエグゼクティブ（または利害関係者）は、何がリスクとなり、企業のビジネスにとってどの分野が最も重要となるのかを統括的に決定しなければなりません。CFP、CMO、事業部のエグゼクティブは、データに関する意見を提供し、CIO はセキュリティに関連するコストや複雑性について提案することができるでしょう。

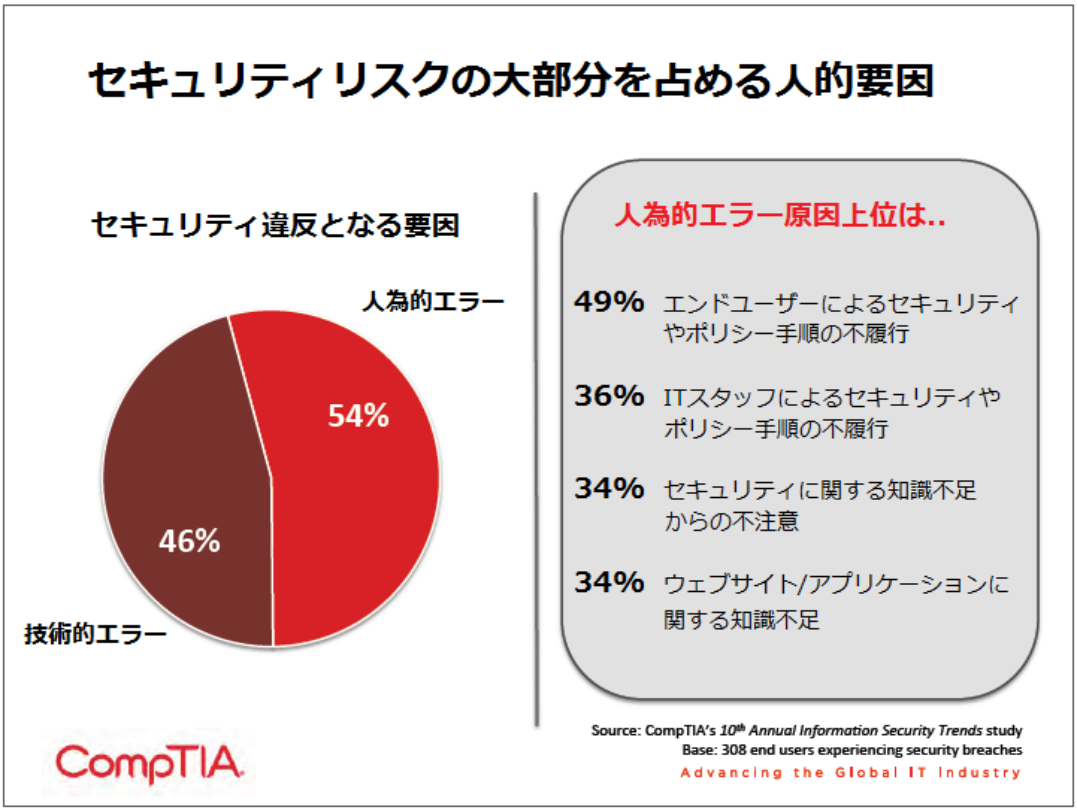
エンドユーザー教育の強化

クラウドコンピューティング、モビリティ、ソーシャルメディアは「IT のコンシューマライゼーション」トレンドの象徴といえます。セクション 2 では、クラウドおよびモビリティで問題となる懸念事項を取り上げましたが、ソーシャルメディアから生じる脅威はプロバイダーレビューやデバイスマネジメントを通して容易に想定できるものではありません。

セキュリティ脅威における人為的要因は増加しています。エンドユーザーは、時に IT チームの管理下でない状況でも、デバイスやビジネスクラスのシステムをコントロールすることが可能となっています。エンドユーザーは、これらシステムを活用することもできますが、セキュリティの予備知識や経験不足から潜在する脅威に気付かないこともしばしばあります。

人為的要素を特に危険なものにしてしまう原因に、リスクの大きさに気付くまでに時間がかかるという点があります。セキュリティ脅威について聞いたところ、回答者は外部から来る脅威（マルウェア、ハッキング、フィッシング）に対して一番強く懸念を示しました。それと比較すると、エンドユーザーや IT スタッフ間の人為的エラーへの懸念は低く評価されていました。ですが過去 2 年間のデータを見ると、70%以上が人為的エラーは減少しておらず、むしろ悪化していると回答しています。

セクション 2 で示した通り、企業は「人為的エラー」が違反事項やデータロスの原因として上昇していると認識しています。第 10 回目の調査では 54%が「人為的要因」をセキュリティ違反の原因としてあげています。これは第 9 回目の調査 52%からの上昇となります。



不満を抱く社員がアクセス権を持つことから、問題を起こしたり機密情報を盗むといった、悪意を伴う人為的要因も一部存在するかもしれませんが、多くのケースにおいてはセキュリティ手順の不履行や知識不足から引き起こる不意の人為的エラーであることがわかります。

テクノロジーはこの問題を完全に解決できるわけではありません。セキュリティ脅威やその環境を理解する専門家はセキュリティツールが最も効果的といいます。今日のビジネスには、従業員一人一人がセキュリティ環境において意識や知識のレベルを上げる必要があるというジレンマがあります。それは、認定資格を持つサブジェクトマターエキスパートといった高いレベルではなく、ベストプラクティスが何であるかを理解することができるレベルをいいます。

また、エンドユーザー教育やトレーニングは、セキュリティ違反をなくすための主な手段といえるでしょう。これは、専門家にセキュリティを委託している企業、必要となるツールに単に支出をしていただけの企業にとって大きな方向転換となります。また IT 部門やソリューションプロバイダーにおいても、ユーザーベースに自身の知識を効率的に啓発する方法を見つけなければなりません。

IT セキュリティの「製品」を強調しすぎるとその他の 3 つ分野「ポリシー」「プロセス」「人」において盲点ができてしまいます。セキュリティに強い企業は 4 つ全ての分野に焦点を置いています：「ポリシー」は企業のガイドラインを定義し、「プロセス」は保全を行い、「製品」はモニタリングを支援し、最後に「人」はトレーニングされることで意識や責任をより高めることができます。テクノロジーはワークフォースの生産性を向上するため活用が可能であり、企業はサイバーセキュリティのリスクにさらされないためにも全体でセキュリティに取り組む必要があるのです。

セキュリティトレーニングで考慮するポイント

- セキュリティ脅威は変化し続けるものであることから、トレーニングは継続的に行われる必要があります。セキュリティトレーニングはワンタイムまたは年に一度の実施といった考えを持つマネジメント層に説明するのは困難であるかもしれません。
- インタラクティブトレーニングは、概念を明確にするだけではなく、従業員にとっても有意義なものとなるでしょう。フィッシングのシミュレーションや、紛失を装い USB メモリを置いておくなどはその一例です。
- ベースラインや追跡方法を決めておくことが重要です。例えば、フィッシングシミュレーションにおいては、不審リンクをクリックしてしまった従業員は初回時 40%であったことを記録します。後のシミュレーションでプログレスを見るためこうした数字は追跡できるようにしておきます。