シスコ
年次サイバーセキュリティ レポート（2017 年）

cisco

目次

概要

攻撃の対象範囲が増えるにつれ、防御側には、最も重要な目標に注力する必要性が生じてきます。それは、攻撃者の活動範囲を制限することです。

攻撃側は、意のままに使用できるツールをこれまでよりも多く所有しています。また、各ツールをいつ使用すれば最大限の効果を得られるのかということについても熟知しています。モバイル エンドポイントとオンライン トラフィックの急増は、攻撃側に有利に働き、活動範囲や攻撃対象、アプローチの選択肢も増えています。

拡大する脅威に対応するために防御側が取ることができる手段は沢山あります。たとえば、情報提供や保護のために、別々に機能するベストオブブリード方式のソリューションを購入することができます。また、有能な人材が不足している雇用市場において、限られた予算で他社と人材を奪い合うことができます。

すべての攻撃を阻止することは不可能かもしれません。しかし、攻撃者の活動領域を制限して資産侵害の能力を抑えることによって、脅威のリスクとその影響を最小限に抑えることは可能です。実行できる手段の 1 つは、さまざまなセキュリティ ツールを、相互に接続された統合型のセキュリティ アーキテクチャにまとめることです。

自動化されたアーキテクチャのもとに連動する統合セキュリティ ツールを使用すると、脅威の検出と軽減プロセスを効率化することができます。そのため、より複雑で永続的な問題に取り組む時間が生まれます。多くの組織が、6 つ以上のベンダーのソリューションを使用しています（53 ページ）。多くの場合、セキュリティ チームは特定の日に受信したセキュリティ アラートの半分しか調査できません。

シスコ年次サイバーセキュリティ レポート（2017 年）では、シスコのセキュリティ リサーチからもたらされた調査、洞察、および今後の展望についてご紹介します。そこで、より多くの活動時間を得ようとしている攻撃側と、攻撃側にチャンスを与えないように努める防御側との間にある絶え間ないプッシュ/プルの力学を明らかにします。また、シスコの脅威研究者とその他のエキスパートが集計したデータを考察します。シスコの調査および洞察は、今日の急速に進化する巧妙な脅威に組織が効果的に対応できるようにするためのものです。

このレポートは次のセクションに分かれています。

攻撃者の行動

このセクションでは、攻撃者が脆弱なネットワークを調査してマルウェアを配布する方法について考察します。電子メール、サードパーティ製クラウド アプリケーション、アドウェアなどのツールを兵器化する方法について説明します。また、サイバー犯罪者が攻撃の導入段階で使用する方法を説明します。このセクションでは「進化時間」（TTE）調査についても紹介し、どのように攻撃者が戦略の鮮度を保ち、検出を回避するのかを示します。また、検出時間（TTD）の平均中央値を短縮するためのシスコの取り組みについて、最新情報をご紹介します。さらに、さまざまな業界および地域のマルウェア リスクに関するシスコの最新の調査についても説明します。

防御側の行動

このセクションでは、脆弱性に関する最新情報を提供します。焦点の 1 つはミドルウェア ライブラリの新たな弱点です。この弱点によって、攻撃者は多くのアプリケーションで同じツールを使用できるようになるため、時間とコストを削減できます。また、パッチ適用のトレンドに関するシスコの調査結果も共有します。ユーザに定期的に更新を提供して、一般的な Web ブラウザおよび生産性ソリューションのより安全なバージョンを導入するよう促す利点について説明します。

2017 年シスコ セキュリティ機能ベンチマーク調査

このセクションでは、シスコの 3 回目のセキュリティ機能ベンチマーク調査の結果を示します。この調査は、組織のセキュリティ状況に関するセキュリティ プロフェッショナルの認識に焦点を当てています。本年、セキュリティ プロフェッショナルは手にしているツールに自信を持っているようですが、こうしたツールが攻撃者の活動範囲を削減できるかどうかについては、確信を持てていません。また、この調査は、一般的なセキュリティ侵害がビジネス チャンス、収益、および顧客に重大な影響を及ぼすことも示しています。同時に、違反によって組織の技術およびプロセスの改善が促進されています。組織のセキュリティ状況に関する分析については、49 ページを参照してください。

業界

このセクションでは、バリュー チェーンのセキュリティを確保することの重要性について説明します。ベンダー製品のゼロデイ エクスプロイトおよび脆弱性に関する情報を蓄積している政府の潜在リスクを考察します。また、高速環境でデータを保護するソリューションとしての高速暗号化の使用について説明します。最後に、世界のインターネット トラフィックと潜在的な攻撃対象が増加した場合の、組織のセキュリティ上の課題の概要を示します。

まとめ

シスコは結論として、攻撃チェーンに応じて日常的なセキュリティ課題に対応し、攻撃者の活動範囲を狭めることができるように、セキュリティ プラクティスを導入することを推奨します。また、このセクションでは、経営陣のリーダーシップ、ポリシー、プロトコル、およびツールを関連付けて脅威の回避、検出、および軽減を実現する、統合されたシンプルなセキュリティ アプローチを確立するためのガイダンスも提供します。

主な調査結果

- 3 つの主要なエクスプロイト キット（Angler、Nuclear、および Neutrino）は、それよりもマイナーなキットや新規参入キットが活躍する余地を残して 2016 年の脅威状況から突然姿を消しました。
- 2017 年シスコ セキュリティ機能ベンチマーク調査によると、大半の企業は自社環境で 6 社以上のセキュリティ ベンダーと 6 つ以上のセキュリティ製品を使用しています。55 % のセキュリティ プロフェショナルは 6 社以上のベンダーを使用しており、45 % は 1 ～ 5 社のベンダーを使用しています。また、65 % は 6 つまたはそれ以上の製品を使用しています。
- ベンチマーク調査によると、高度なセキュリティ製品およびソリューションの導入に対する障壁の上位は、予算（回答者の 35 %）、製品の互換性（28 %）、認証（25 %）、および人材（25 %）です。
- 2017 年シスコ セキュリティ機能ベンチマーク調査では、さまざまな制約によって、組織が 1 日に受信したセキュリティ アラートの 56 % しか調査できていないことがわかりました。調査されたアラートの半数（28 %）は適切なものと見なされ、修正されているのはさらにその半分以下（46 %）です。また、セキュリティ運用マネージャの 44 % が 1 日あたり 5000 件以上のセキュリティ アラートを受信しています。
- 2016 年に従業員が企業環境に導入した、接続中のサードパーティ製クラウド アプリケーションの 27 %に高いセキュリティ リスクがありました。オープン認証（OAuth）接続では企業のインフラストラクチャに接続し、ユーザがアクセス権を付与すると企業クラウドおよび software-as-a-service（SaaS）プラットフォームと自由に通信できます。
- さまざまな業種の 130 の組織を対象としたシスコの調査では、これらの企業の 75 % がアドウェア感染の影響を受けていることがわかりました。攻撃者は、潜在的にこれらの感染を使用して他のマルウェア攻撃を促進することができます。
- マルバタイジング キャンペーンの背後に潜む攻撃者は、ブローカー（「ゲート」とも呼ばれる中間サイトを）を使用することが増えてきています。ブローカーを使用すると、攻撃者はより速いスピードで移動したり、操作可能領域を維持したり、検出を回避したりすることができます。これらの中間リンクによって、攻撃者は最初のリダイレクションを変更せずに別の悪意あるサーバにすばやく切り替えることができます。
- スパムは電子メール総数のおよそ 3 分の 2（65 %）に達し、シスコの調査によると世界のスパム量は大規模かつ活発なスパム送信ボットネットによって増加しています。シスコの脅威研究者によると、2016 年に確認された世界のスパムの約 8 ～ 10 % は悪意のあるものと分類されました。さらに、悪意のある添付ファイル付きのスパムも割合が増加しており、攻撃者はキャンペーンを成功させるためにさまざまなファイル タイプを試していると推測されます。
- セキュリティ機能ベンチマーク調査によると、まだセキュリティ侵害の被害を受けていない組織は自分たちのネットワークが安全であると信じている可能性があります。調査対象のセキュリティ プロフェッショナルの 49 % が、所属組織がセキュリティ侵害後に風評被害への対策を迫られたと述べたことを考えると、この自信はおそらく間違っています。

- 2017 年シスコ セキュリティ機能ベンチマーク調査では、攻撃を受けた組織の約 4 分の 1 がビジネス チャンスを失ったこともわかっています。また、その 40 % が相当な損失を被ったと述べています。20 % の組織は攻撃によって顧客を失い、およそ 30 % は収益を失いました。
- ベンチマーク調査の回答によると、侵害が発生したときに影響を受ける可能性が最も高い機能は業務と財務（それぞれ 36 % および 30 %）で、その次にブランドへの評価と顧客維持（両方とも 26 %）が続きます。
- セキュリティ侵害に起因するネットワーク停止の影響は、時として長期にわたります。ベンチマーク調査によると、停止の 45 % が 1 ～ 8 時間続き、15 % が 9 ～ 16 時間、11 % が 17 ～ 24 時間続きました。これらの停止の 41 %（55 ページを参照）は、システムの 11 ～ 30 % に影響を及ぼしました。
- ミドルウェア（プラットフォームまたはアプリケーション間にブリッジまたはコネクタを提供するソフトウェア）の脆弱性はより顕著になっており、ミドルウェアが一般的な脅威ベクトルになりつつあることに懸念が広がっています。多くの企業はミドルウェアに頼っているため、この脅威はあらゆる業界に影響する可能性があります。シスコのプロジェクト中、調査された新しい脆弱性の大部分がミドルウェアの使用に起因するものであることが、シスコの脅威の研究者達によって発見しました。
- パッチおよびアップグレードのインストールに関して言えば、ソフトウェア アップデートの間隔がユーザの行動に影響する可能性があります。シスコの研究者によると、定期的で予測可能な更新スケジュールによってユーザはより早くソフトウェアを更新するようになるため、攻撃者が脆弱性を利用できる時間が短縮されます。
- 2017 年のセキュリティ機能ベンチマーク調査では、大半の組織がそのセキュリティの 20 % 以上をサードパーティ ベンダーに頼っており、サードパーティ ベンダーに最も依存している組織は将来的に依存度が拡大する可能性が最も高いことがわかりました。

はじめに

はじめに

攻撃者は、組織のリソースにアクセスしたり無制限の活動時間を獲得したりするための、広範かつ多様なテクノロジー ポートフォリオを有しています。それらの手法は、基本的な機能をすべてカバーしており、さらに次の内容を含んでいます。

- パッチ適用/更新漏れの利用
- ソーシャル エンジニアリング トラップへの誘い込み
- 広告などの本物と思われているオンライン コンテンツにマルウェアを挿入

攻撃者はミドルウェアの脆弱性の悪用から悪意のあるスパムのドロップまで、他にも多くの操作を実行できます。また、彼らは目的を達成すると、迅速かつ静かにその活動を終了します。

攻撃者は絶えず、脅威を進化させ、高速で移動し、活動領域を拡大する方法を見つけようとしています。モバイル スピードの高速化とオンライン デバイスの急増は、インターネット トラフィックを爆発的に増加させましたが、それによって攻撃対象も拡大し、攻撃者にとっては都合の良い状況となっています。そのため、企業のリスクも高まっています。2017 年シスコ セキュリティ機能ベンチマーク調査で、攻撃を受けたことがある組織の 3 分の 1 以上が収益の 20 % またはそれ以上を失ったことがわかりました。回答者の 49 % が、セキュリティ侵害に関する風評被害への対策を迫られたと述べています。

収益に損害を受けて堅実なビジネスを維持できる企業がどれだけ存在するでしょうか。防御側は、攻撃者の活動領域の削減にリソースを集中させる必要があります。そうすれば攻撃者は、有益な企業リソースにアクセスしたり、検出されずに活動したりすることが非常に困難であると判断します。

自動化はこの目標の達成に不可欠です。自動化によってネットワーク環境の通常のアクティビティを理解できるようになるため、少ないリソースを実際の脅威の調査や解決に集中させることができます。セキュリティ運用を簡素化することも、攻撃者による無制限な活動を排除するために効果的です。ただし、ベンチマーク調査では、大半の組織が 6 社以上のベンダーの 6 つ以上のソリューションを使用していることが示されています（53 ページ）。

このように複雑に絡み合った技術と圧倒的な数のセキュリティアラートが、十分な保護を妨げる要因です。セキュリティ人材の追加はもちろん役立ちます。理論的には、関与するエキスパートが多いほど組織の技術管理能力が向上し、より良い成果がもたらされます。しかしながら、有能なセキュリティ人材は不足しており、さらに予算も限られているとあっては、大量雇用はできそうにありません。大半の組織は今いる人材でなんとか間に合わせる必要があります。そうした場合、外部の人材でセキュリティ チームを補強しつつ、予算を節約しようと試みます。

このレポートで後ほど説明しますが、これらの課題に対する実際の解答は、人材、プロセス、および技術を統一された方法で運用可能にすることです。セキュリティを実効あるものにすることは、企業が保護すべき対象と、最重要資産を保護するための手法を本当に理解するということです。

2017 年シスコ年次サイバーセキュリティ レポートは、組織やユーザが攻撃を防御できるように設計された、当社の最先端のセキュリティ技術を紹介します。また、攻撃者がこれらの防御を突破するために使用する技術や戦略についても説明します。このレポートでは、2017 年シスコ セキュリティ機能ベンチマーク調査の主な考察結果についても紹介しています。ここでは、企業のセキュリティ ポスチャと、攻撃に対する準備の度合いについて調査しています。

攻撃範囲の拡大

攻撃範囲の拡大

*モバイル デバイス、パブリック クラウド、クラウド インフラ、ユーザの行動。*シスコの第 3 回の年次セキュリティ機能ベンチマーク調査に参加したセキュリティ プロフェッショナルは、サイバー攻撃への組織の露出リスクを考えた場合にこれらのすべての要素を上位の懸念事項に挙げています（図 1）。これは当然とも言えます。モバイル デバイスの急増によって、保護すべきエンドポイントが増えているからです。クラウドはセキュリティの境界を拡張しています。また、ユーザは常にセキュリティ チェーンにおける弱点となります。

ビジネスのデジタル化が進むにつれて、また Internet of Everything（IoE）[1] が実現し始めると、防御側の不安はさらに大きくなります。攻撃対象が拡大すれば、攻撃者にはより多くの活動範囲が与えられます。

10 年以上にわたって、Cisco® Visual Networking Index（VNI）は世界の IP トラフィック予測を提供し、ネットワークの成長を促進する動的な要因を分析してきました。最新レポート『*The Zettabyte Era—Trends and Analysis*』[2] からこれらの統計について考察します。

- 年間の世界の IP トラフィックは、2016 年の終わりまでにゼタバイト（ZB）のしきい値を上回り、2020 年までに 1 年あたり 2.3 ZB に達します（ゼタバイトは 1000 エクサバイト、または 10 億テラバイトです）。これは、次の 5 年で世界の IP トラフィックが 3 倍に増加することを表しています。
- ワイヤレス デバイスやモバイル デバイスからのトラフィックは、2020 年までに IP トラフィック全体の 3 分の 2（66 %）を占めるようになります。有線デバイスの割合はわずか 34 % です。
- 2015 年から 2020 年で、ブロードバンドの平均速度は約 2 倍になります。
- 2020 年までに、すべてのコンシューマの世界的なインターネット トラフィックは、2015 年の 70 % から上昇してその 82 % が IP ビデオ トラフィックになります。

図 1　サイバー攻撃に関するセキュリティ プロフェッショナルの最大の懸念

モバイル デバイス	パブリック クラウド内のデータ	クラウド インフラストラクチャ	ユーザの行動（電子メールや Web サイト内の悪意のあるリンクをクリックするなど）
58 %	57 %	57 %	57 %

「非常に困難」または「極めて困難」のカテゴリを検出したセキュリティ プロフェッショナルの割合

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

2017 年版の図表はこちらからダウンロードしてください：**www.cisco.com/go/acr2017graphics**

[1] Internet of Everything についてのよくある質問 [英語]、シスコ：http://ioeassessment.cisco.com/learn/ioe-faq。
[2] *ゼタバイトの時代 — トレンドと分析 [英語]*、Cisco VNI、2016 年：
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html。

さらに、『*Cisco VNI™ Forecast and Methodology, 2015–2020*』ホワイト ペーパー[3] では、2020 年の世界のインターネット トラフィック量は 2005 年の 95 倍になると予測されています。

この機に便乗したいサイバー犯罪者も当然このような傾向に注目しています。シスコは、地下経済に潜む攻撃者がこの変わりゆく環境でより俊敏に動けるよう準備していることをすでに確認しています。こうした攻撃者は、拡大する攻撃範囲において目的を遂げられるように設計された、ターゲットを絞った多様な攻撃手法を開発しています。一方で、セキュリティ チームは常に緊急対応の体制で圧倒的な数のアラートに対処しています。こうした部門は、ネットワーク環境で多数のセキュリティ製品に頼らなければならず、これによってさらに複雑さが増すため、脅威に対して一層脆弱になる可能性があります。

組織に必要なのは次のような対応です。

- セキュリティ テクノロジーの統合
- セキュリティ運用の簡素化
- 自動化の推進

このアプローチによって、運用コストの削減、セキュリティ担当者の負担軽減、および優れたセキュリティ成果を実現できます。最も重要なことは、攻撃者が無制限に活動している領域を排除することに、より多くの時間をかけることができるようになることです。

[3] *2015 年から 2020 年にかけての Cisco VNI の予測と方法論 [英語]*、Cisco VNI、2016 年：http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html。

攻撃者の行動

攻撃者の行動

偵察 | 武器化 | 配信 | インストール

攻撃者は、ターゲットを調査し、特定し、選択します。

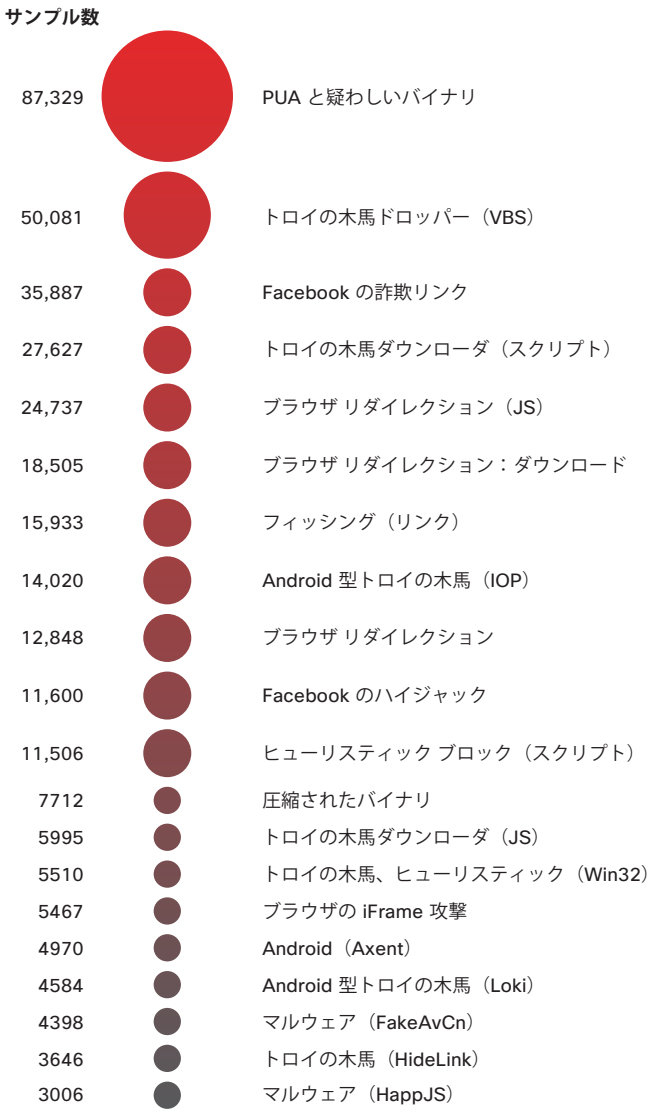
Web 攻撃の手法：攻撃者は「ショート テール型」脅威でキャンペーンの土台を構築

調査は、サイバー攻撃を開始するための最初のステップです。この段階で、攻撃者は、ユーザのコンピュータにアクセスして最終的には組織への侵入を可能にする、脆弱なインターネット インフラやネットワークの弱点を探します。

2016 年の Web 攻撃手段リストでは、疑わしい Windows バイナリと望ましくないアプリケーション（Potentially Unwanted Applications：PUA）が大差で上位を占めています（図 2を参照）。疑わしい Windows バイナリは、スパイウェアやアドウェアなどの脅威を配布します。悪意のあるブラウザ拡張機能は PUA の一例です。

アンケート詐欺とともに偽のオファーおよびメディア コンテンツを含む Facebook 詐欺は、リストの 3 位にランクされました。最もよく確認されたマルウェアに関する年次および中期のリストで Facebook 詐欺が継続して突出していることは、多くのサイバー攻撃でソーシャル エンジニアリングが基本的な役割を果たしていることを浮き彫りにしています。Facebook には世界中で毎月約 18 億人のアクティブ ユーザが存在します。[4] これが、サイバー犯罪者やユーザをだまそうとしているその他の攻撃者の論理上のテリトリとなります。前向きな動きの 1 つとして、Facebook は、偽のニュースやデマ ウイルスを排除する対策を講じることを最近発表しました。アナリスト達は、そのようなコンテンツが 2016 年のアメリカ大統領選挙で有権者に影響する可能性があると示唆しています。[5]

図 2 最も多く観察されたマルウェア



出典：シスコ セキュリティ リサーチ

[4] Facebook の統計 [英語]、2016 年 9 月：http://newsroom.fb.com/company-info/。

[5] ザッカーバーグ、Facebook の「偽ニュース」排除を誓う [英語]、Jessica Guynn、Kevin McCoy 著、*USA Today*、2016 年 11 月 14日：http://www.usatoday.com/story/tech/2016/11/13/zuckerberg-vows-weed-out-facebook-fake-news/93770512/。

ブラウザのリダイレクション マルウェアは、2016 年に最もよく確認されたマルウェア タイプの上位 5 つに入りました。『*Cisco 2016 Midyear Cybersecurity Report*』[6] で説明されているように、ブラウザ感染が起こると、ランサムウェアや他のマルウェア キャンペーンを仕掛るために使用される、悪意のある広告（マルバタイジング）に晒される可能性があります。シスコの脅威研究者は、広告インジェクタ、ブラウザ設定のハイジャッカー、ユーティリティ、およびダウンローダを含む悪意のあるアドウェアがますます大きな問題になっていると警告しています。実際、シスコはアドウェア問題の研究の一環として最近調査した企業の 75 % でアドウェア感染を特定しました（このトピックの詳細については、23 ページの「調査によって 75 % の組織がアドウェア感染の影響を受けたことが判明」を参照してください）。

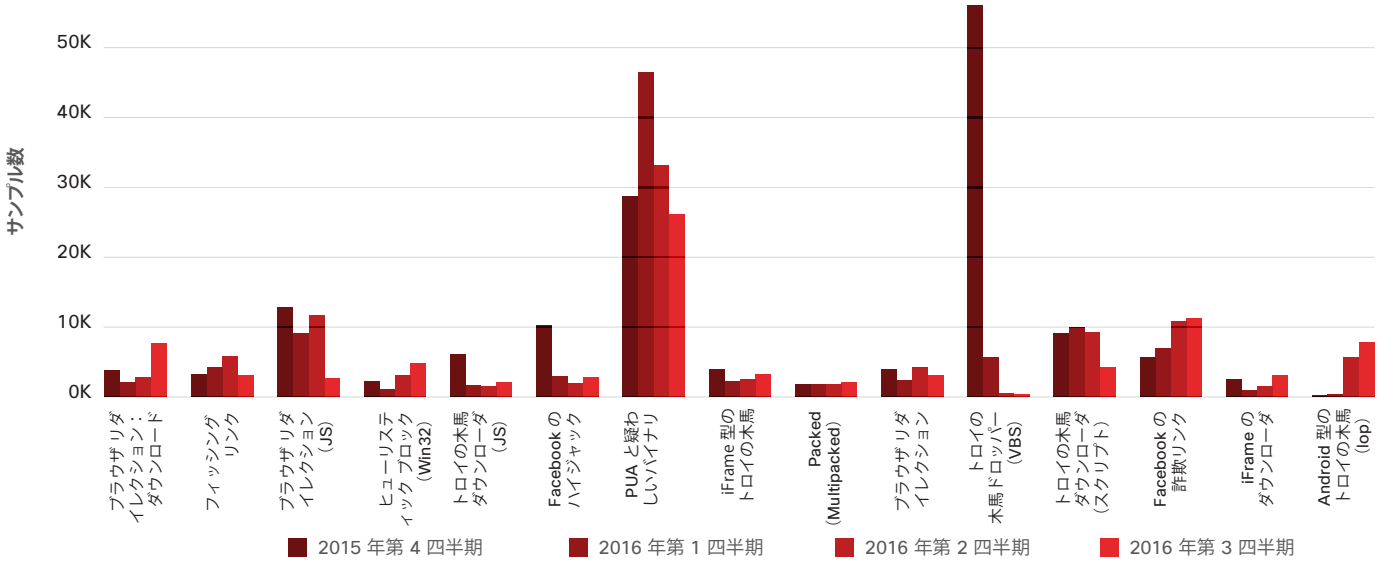
ブラウザの JavaScript 不正使用マルウェアやブラウザの iFrame 不正使用マルウェアなど図 3 にリストされている他のマルウェア タイプもブラウザ感染を助長するように設計されています。トロイの木馬（ドロッパーおよびダウンローダ）もよく確認されたマルウェア タイプの上位 5 つに入っています。これは、トロイの木馬がユーザのコンピュータや組織のネットワークに最初にアクセスするためのツールとして依然として普及していることを示しています。

もう一つの注目すべき傾向は、Android オペレーティング プラットフォームのユーザを狙ったマルウェアの使用が一貫して高いことです。Android 型トロイの木馬は、過去 2 年にわたってショート テール型脅威のリストで着実に上昇しています。また、2016 年の最もよく確認されたマルウェア タイプのトップ 10 にランクされました。図 2（前のページを参照）に示されたショート テール型脅威の最後に現れる Loki マルウェアは、他のファイルやプログラムを複製したり感染させたりする可能性があるため特に問題です。

図 3 は、シスコの脅威研究者が 2015 年の終わりから観察しているマルウェアの傾向を示しています。また、この図から攻撃者が Web ベース攻撃の調査段階で明らかに変化していることがわかります。現在、より多くの脅威が脆弱なブラウザとプラグインを特に探し求めています。この変化は、従来の Web 攻撃ベクトルで数多くのユーザを悪用することがより困難になっているため、攻撃者のマルバタイジングへの依存が高まっていることと一致しています（15 ページの次のセクション「Web 攻撃のベクトル：Flash は衰退しつつあるが引き続き警戒が必要」を参照してください）。

個人ユーザ、セキュリティ プロフェッショナル、および企業へのメッセージは明確です。つまり、ブラウザが安全であることを確認し、不要なブラウザ プラグインを無効化または削除することは、マルウェア感染の防止に非常に効果的だということです。これらの感染は、ランサムウェア キャンペーンなどの重大かつ破壊的で損害の大きい攻撃につながる可能性があります。こうした簡単な手順で、一般的な Web ベースの脅威への露出を大幅に減らし、攻撃者が攻撃チェーンの次の段階（兵器化）を実行する活動領域を見つけられないようにすることができます。

図 3　2015 年第 4 四半期から 2016 年第 3 四半期にかけて最も多く観察されたマルウェア



出典：シスコ セキュリティ リサーチ

[6] *2016 年シスコ中期サイバーセキュリティ レポート [英語]*：http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html。

偵察 | 武器化 | 配信 | インストール

攻撃者はリモート アクセス マルウェアに成果物ペイロードのエクスプロイトを組み合わせる。

Web 攻撃のベクトル：Flash は衰退しつつあるが引き続き警戒が必要

Adobe Flash は長い間、システムを悪用したり脅かしたりしようとする攻撃者にとって、魅力的な Web 攻撃ベクトルでした。ただし、Web 上の Adobe Flash コンテンツの量は継続的に減少しており、また、Flash の脆弱性に関する意識が高まっているため、サイバー犯罪者がこれまでに行っていた規模でユーザを悪用することは難しくなっています。

Adobe 自体はソフトウェア プラットフォームの全面的な開発およびサポートから撤退しており、HTML5 などの新しい標準を導入するよう開発者に促しています。[7] 一般的な Web ブラウザのプロバイダーも Flash に対しての見解を明確にしています。たとえば、Google は 2016 年に Chrome ブラウザでの Adobe Flash の全面的なサポートを中止すると発表しました。[8] Firefox は従来の Flash コンテンツは引き続きサポートしていますが、「ユーザ エクスペリエンスに必要のない特定の Flash コンテンツ」はブロックしています。[9]

Flash は衰退していく可能性がありますが、エクスプロイト キットの開発者は攻撃ベクトルとしてこれが持続するよう支援しています。しかし、こうした傾向が変わるかもしれない兆候も見られます。3 つのメジャーなエクスプロイト キット（Angler、Nuclear、および Neutrino）が 2016 年の脅威の展望から突然姿を消した後、シスコの脅威研究者は Flash 関連のインターネット トラフィックが大幅に減少したことを確認しました（20 ページ の「メジャーなエクスプロイト キットが消失し、より少数の主要キットと新規参入キットにチャンスが到来」を参照してください）。Angler エクスプロイト キットの背後に潜む攻撃者は、ユーザを悪用するために Flash の脆弱性を狙っていました。Nuclear エクスプロイト キットも Flash に重点を置いていました。また、Neutrino は Flash ファイルに依存してエクスプロイトを配布していました。

ユーザは、ビジネス上の理由から Flash を必要としない場合も、引き続き注意して Flash をアンインストールする必要があります。Flash を使用する必要がある場合は、更新で最新状態を維持する必要があります。自動のパッチ適用機能を備えた Web ブラウザを使用すると役に立ちます。13 ページの「Web 攻撃の手法：攻撃者は「ショート テール型」脅威でキャンペーンの土台を構築」で説明したように、安全なブラウザを使用し、不要なブラウザ プラグインを無効化または削除することで、Web ベースの脅威への露出を大幅に削減できます。

Java、PDF、および Silverlight

Java と PDF の両方のインターネット トラフィックは、2016 年に著しく減少しました。Silverlight のトラフィックは、脅威研究者が定期的に追跡する必要がないほどのレベルにまで達しています。

Java は、かつては主要な Web 攻撃ベクトルでしたが、ここ数年でセキュリティ ポスチャが大幅に向上しています。Java ブラウザ プラグインを排除するという 2016 年初めの Oracle 社の決定は、Java をあまり魅力的でない Web 攻撃ベクトルとするのに効果的でした。PDF 攻撃もめったに見られなくなっています。この攻撃は簡単に検出できるようになったため、多くの攻撃者は現在この方法をあまり使用しません。

ただし、Flash 同様、サイバー犯罪者はユーザの隙を突くために Java、PDF、および Silverlight を依然として使用しています。個人ユーザ、企業、およびセキュリティ プロフェッショナルは、これらの潜在的なセキュリティ侵害の方法を認識する必要があります。これらの脅威にさらされるリスクを軽減するには、次のような対策を行う必要があります。

- パッチのダウンロード
- 最新の Web テクノロジーの使用
- リスクがある Web コンテンツの回避

[7] Flash、HTML5 およびオープン Web 標準 [英語]、Adobe ニュース、2015 年 11 月：https://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html。
[8] Flash と Chrome [英語]、Anthony LaForge 著、The Keyword ブログ、Google、2016 年 8 月 9 日：https://blog.google/products/chrome/flash-and-chrome/。
[9] Firefox における Adobe Flash の使用量の減少 [英語]、Benjamin Smedberg 著、Future Release ブログ、Mozilla、2016 年 7 月 20 日：https://blog.mozilla.org/futurereleases/2016/07/20/reducing-adobe-flash-usage-in-firefox/。

アプリケーション セキュリティ：アプリケーション展開中の OAuth 接続リスクの管理

企業がクラウドに移行すると、セキュリティ境界は仮想レルムに拡張されます。ただし、そのセキュリティ境界は、従業員が環境に導入する、相互に接続されたサードパーティ製クラウド アプリケーションによってすぐに消失します。

従業員は、生産性を向上させ、仕事中にも接続したままであることを希望しています。しかし、これらのシャドー IT アプリケーションよって企業に対するリスクが発生します。これらは企業のインフラストラクチャに接続しており、ユーザがオープン認証（OAuth）でアクセス権を付与するとすぐに企業クラウドや software-as-a-service（SaaS）プラットフォームと自由に通信できます。これらのアプリケーションのアクセス可能範囲は広範（時には過剰）になる場合があります。また、これらは企業データを表示、削除、外部化、および保存することが可能で、ユーザの代理をすることさえできるため、慎重に管理する必要があります。

現在シスコの一部門であるクラウド セキュリティ プロバイダーの CloudLock は、さまざまな業界を代表する 900 の組織のサンプル グループで、接続中のサードパーティ製クラウド アプリケーションの増加を追跡しています。図 4 に示すように、2016 年の初めには、約 129,000 個のユニークなアプリケーションが確認されました。10 月末までに、その数は 222,000 個に増加しました。

アプリケーションの数は、2014 年から約 11 倍に増加しています（図 5 を参照）。

最もリスクの高いアプリケーションの分類

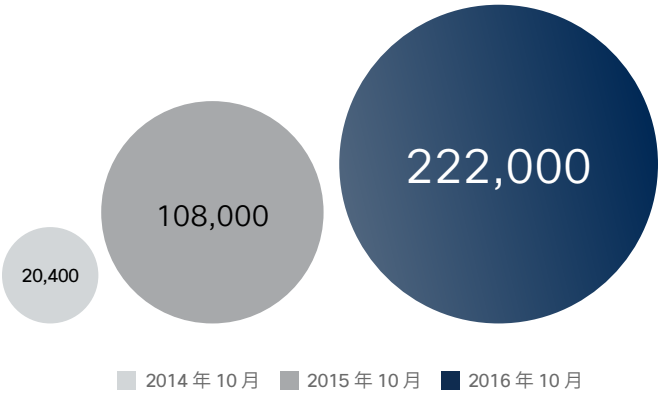
自社環境で接続中のサードパーティ製クラウド アプリケーションの中でネットワーク セキュリティに対するリスクが最も高いものをセキュリティ チームが理解できるように、CloudLock はクラウド アプリケーション リスク インデックス（CARI）を開発しました。このプロセスには次のようにさまざまな評価が含まれています。

- **データ アクセス要件：**組織は他の質問と共に次の質問に回答しています。「アプリケーションの許可に必要な権限は何ですか?」、「データ アクセス件の付与は、OAuth 接続を通して企業の SaaS プラットフォームにプログラム的に（API）アクセスできることを意味しますか?」、「このアプリケーション（および、拡大解釈してベンダー）はユーザの代理となり、表示や削除などの企業データの処理を実行できますか?」。
- **コミュニティの信頼性評価：**このアセスメントにはピア別およびクラウドソーシングによる評価が使用されます。
- **アプリケーションの脅威インテリジェンス：**サイバーセキュリティのエキスパートによるこの包括的なバックグラウンド チェックは、セキュリティ認定、侵害歴、アナリスト レビューなどのアプリケーションのさまざまなセキュリティ属性に基づいています。

図 4 2016 年のサードパーティのコネクテッド クラウド アプリケーションの急激な拡大

出典：Cisco CloudLock

図 5 サードパーティのクラウド アプリケーションの増加量（対前年比）



出典：Cisco CloudLock

2017 年版の図表はこちらからダウンロードしてください：
www.cisco.com/go/acr2017graphics

リスク スコアと例

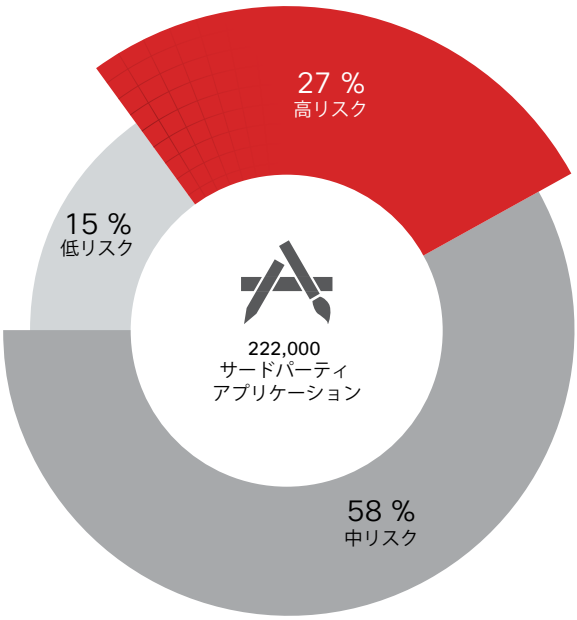
CloudLock は、CARI を使用してサードパーティのクラウド アプリケーションを分類した後、各アプリに 1（最低リスク）から 5（最大リスク）までのリスク スコアを割り当てます。

スコア 1 のアプリケーションは、たとえば、最小限のアクセス範囲（電子メールのみなど）、コミュニティの信頼性評価が 100%、侵害履歴がない場合です。

スコア 5 のアプリケーションは、フル アカウント アクセス（電子メール、ドキュメント、ナビゲーション履歴、カレンダーなどを確認できる）のアプリ、信頼性評価が 8%（管理者の 8% にしか信頼されていないことを意味する）、セキュリティ証明書が存在しない場合が考えられます。

CloudLock は、CARI を使用してサンプルの 900 の組織で特定された 222,000 個のアプリケーションを分類しました。これらすべてのアプリケーションの 27 % が高リスクと見なされ、大半が中リスク カテゴリになりました（図 6 を参照）。これらの組織の半数が、2016 年の夏にリリースされた人気のゲーム アプリケーションに関連する OAuth 接続を使用していました。

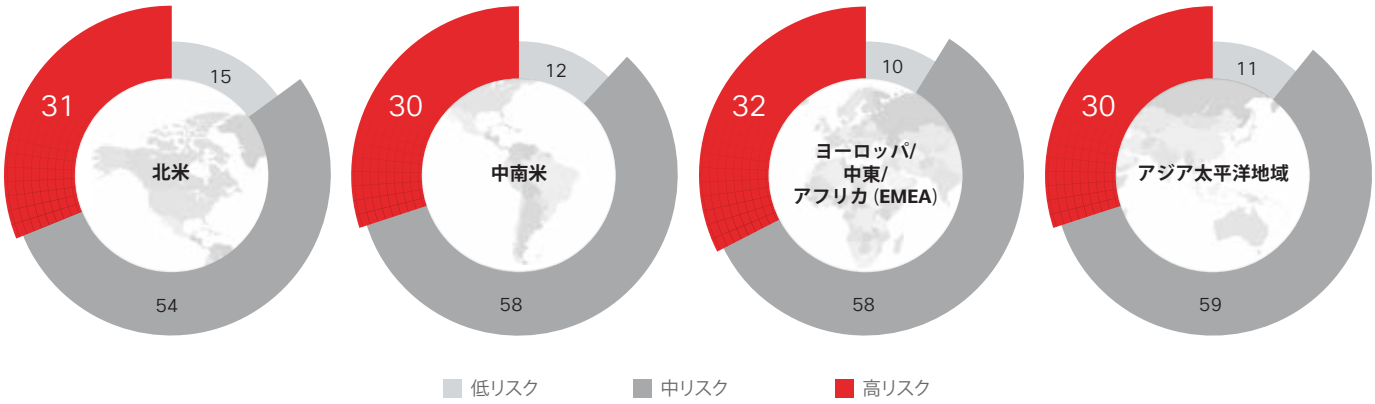
図 6 高リスクに分類されるサードパーティ アプリケーション



出典：Cisco CloudLock

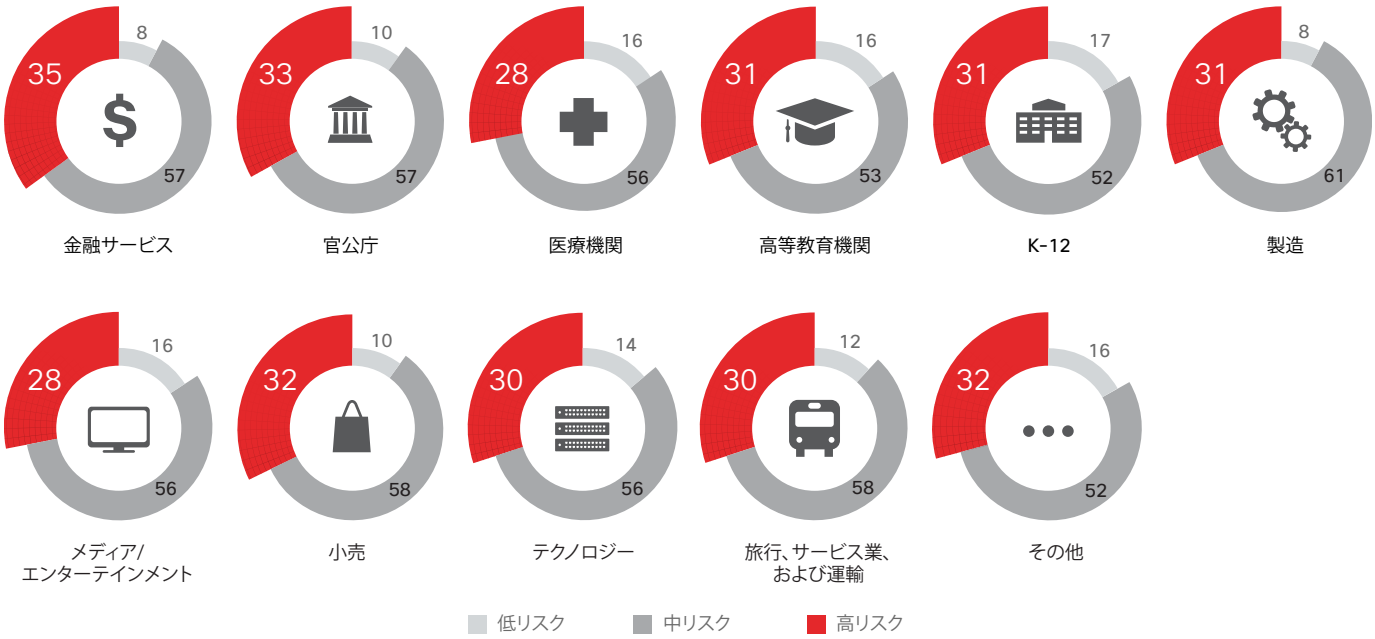
シスコの分析によって、規模、業界、または地域に関係なくすべての組織で低リスク、中リスク、および高リスクのアプリケーションが比較的均等に分散していることがわかりました（図 7 および図 8 を参照）。

図 7 低リスク、中リスク、および高リスクアプリケーションの地域別分布



出典：Cisco CloudLock

図 8 低リスク、中リスク、および高リスクアプリケーションの業界別分布



出典：Cisco CloudLock

2017 年版の図表はこちらからダウンロードしてください：**www.cisco.com/go/acr2017graphics**

雑音の排除

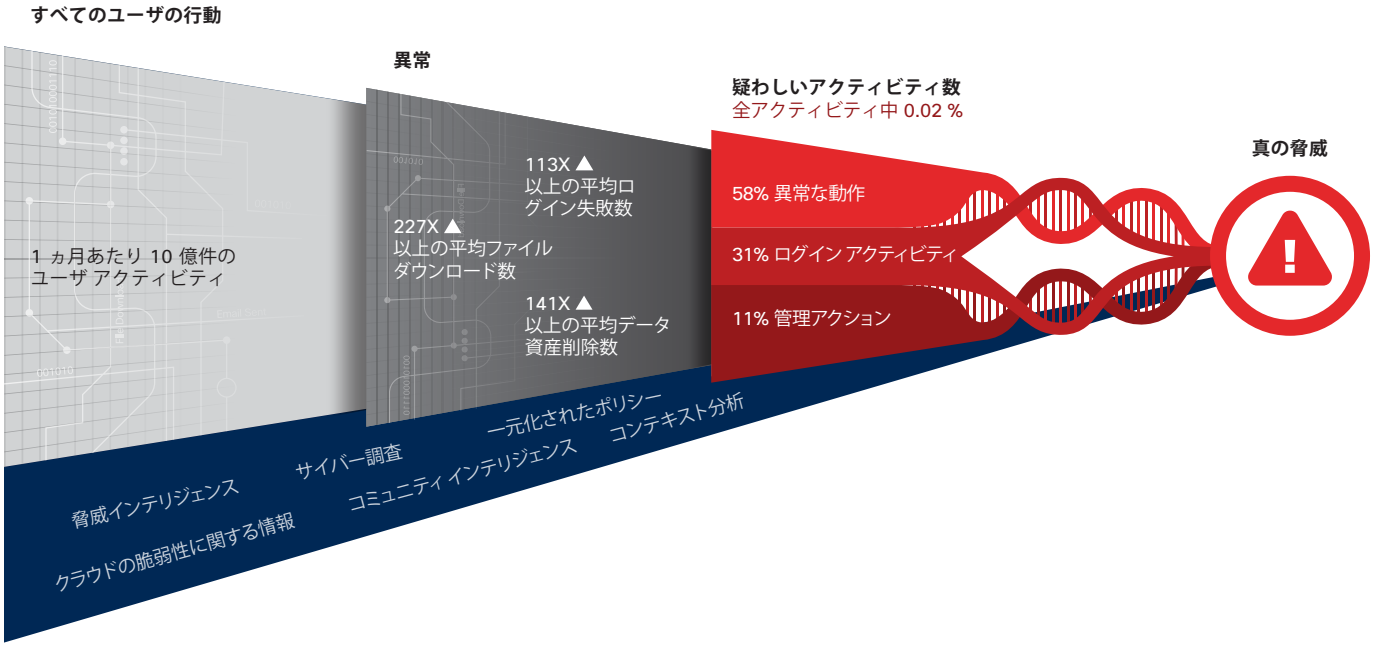
サードパーティ製クラウド アプリケーションを含む企業の SaaS プラットフォームでユーザおよびエンティティの不審な行動を特定するために、セキュリティ チームは、数十億ものユーザ アクティビティをふるいにかけて、その組織環境での通常のユーザ行動パターンを定義する必要があります。また、予測したパターンから外れた異常を探す必要があります。その後、疑わしいアクティビティの相互関係を明らかにして、調査が必要な本当の脅威を特定する必要があります。

不審なアクティビティの一例は、短期間での複数の国からの過度なログイン アクティビティです。特定の組織における通常のユーザ行動では、従業員が 1 週間にせいぜい 1 ヵ国または 2 ヵ国から特定のアプリケーションにログインします。1 人のユーザが 1 週間のうちに 68 ヵ国からアプリケーションにログインを開始している場合、セキュリティ チームはそのアクティビティを調査して正当であることを確認する必要があります。

シスコの分析によると、接続中のサードパーティ製クラウド アプリケーションに関連付けられた 5000 個のユーザ アクティビティのうち疑わしいものはわずか 1 つ（0.02 %）です。セキュリティ チームの課題は、当然のことながらその 1 つのインスタンスを正確に特定することです。

自動化によってのみ、セキュリティ チームはセキュリティ アラートの「雑音」を排除して、リソースを本当の脅威の調査に集中させることができます。前述の（および図 9 に示す）通常のユーザ アクティビティと潜在的に疑わしいユーザ アクティビティを特定する段階的なプロセスは、自動化の使用とすべての段階で適用されるアルゴリズムに左右されます。

図 9 自動化（プロセス）によるユーザの行動パターンの特定



出典：Cisco CloudLock

シェアする

偵察 | 武器化 | **配信** | インストール

攻撃者は、電子メール、添付ファイル、Web サイトの悪意ある使用やその他のツールを通じて、対象にサイバー攻撃をしかけます。

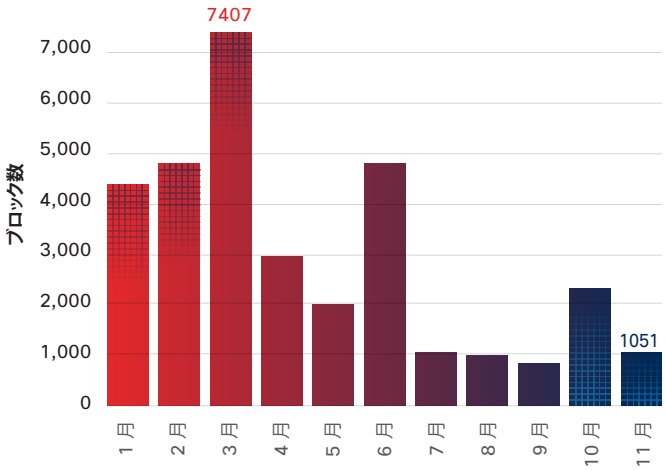
メジャーなエクスプロイト キットが消失し、小型のキットと新規参入キットにチャンスが到来

2016 年に、エクスプロイト キット環境に劇的な変化が見られました。年始には、Angler、Nuclear、Neutrino、および RIG が明らかにエクスプロイト キットの中心でした。11 月までに、そのグループで依然として使われているものは RIG のみになりました。図 10 に示すように、エクスプロイト キットのアクティビティは 6 月頃に大幅に減少しました。

Nuclear が最初に消え、5 月に突然活動を休止しました。開発者が Nuclear を止めた理由は不明です。Neutrino エクスプロイト キットも 2016 年に消失しましたが、これは Flash ファイルに依存して脆弱性を提供していました（2016 年の既知のエクスプロイト キットにおける上位の脆弱性のリストについては、次のページの図 11 を参照してください）。

Flash は攻撃者にとって依然として魅力的な Web 攻撃ベクトルのままですが、時間が経つにつれてその魅力は低下していくものと思われます。Flash を完全にサポートするサイトやブラウザは少なくなるか、またはほとんどなくなり、一般的に Flash の脆弱性に関する認識は高くなっています（このトピックの詳細については、15 ページの「Web 攻撃のベクトル：Flash は衰退しつつあるが引き続き警戒が必要」を参照してください）。

図 10 エクスプロイト キットのランディング ページのブロック数、2016 年 1 月～11 月



出典：シスコ セキュリティ リサーチ

2017 年版の図表はこちらからダウンロードしてください：
www.cisco.com/go/acr2017graphics

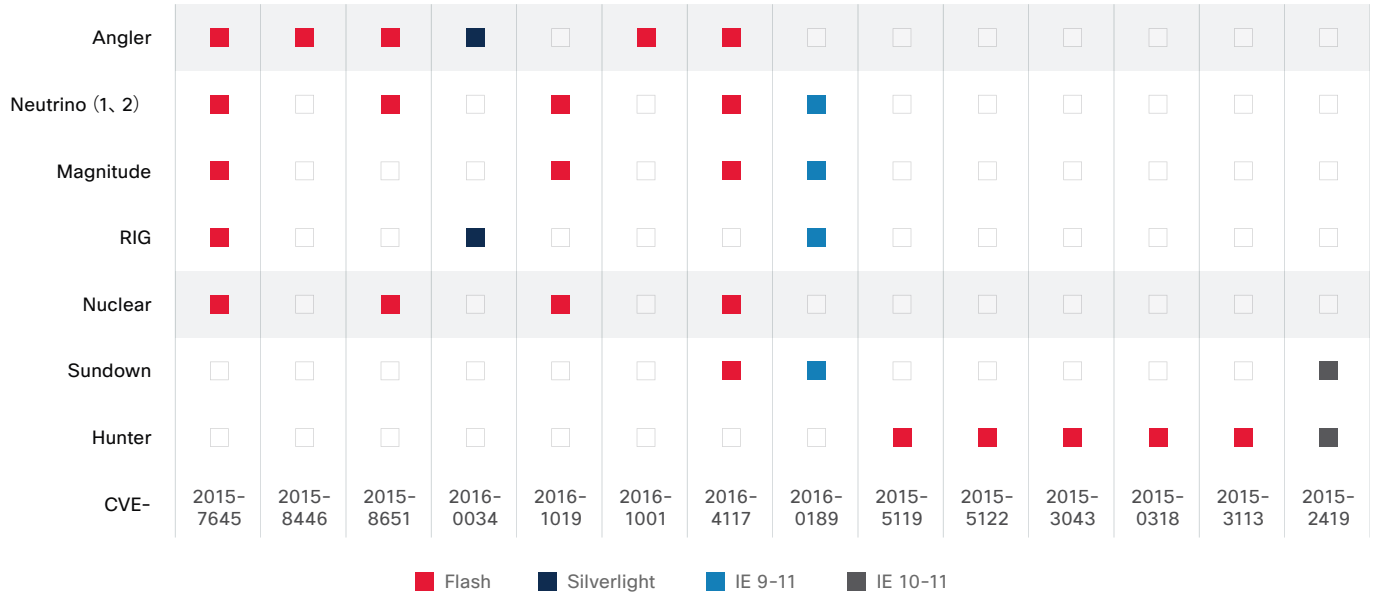
主要キットの沈黙

既知のエクスプロイト キットの中で最も高度で最大の Angler も Flash の脆弱性をターゲットにしており、さまざまな知名度の高いマルバタイジングやランサムウェア キャンペーンに関係していました。しかし、Nuclear および Neutrino の消失とは異なり、2016 年の Angler の離脱の理由は明らかです。

春の終わりに、約 50 人のハッカーおよびサイバー犯罪者がロシアで逮捕されました。このグループは、特にロシアの銀行を狙うバンキング型トロイの木馬である Lurk マルウェアに関係していました。[10] シスコの脅威研究者は、Lurk が Angler を通してロシア国内の被害者に大規模に配布されていたという事実を含め、Lurk と Angler の間の明確な関係を特定しました。逮捕後、Angler はエクスプロイト キットの市場から姿を消しました。[11]

現在、メジャーなエクスプロイト キットの 3 つが後進に道を譲ったため、よりマイナーなキットと新規参入キットが市場シェアを拡大する可能性があります。これらはより巧妙で俊敏になっています。2016 年の終わりに増加を示したエクスプロイト キットは Sundown、Sweet Orange、および Magnitude です。これらのキットは RIG と同様に、Flash、Silverlight、および Microsoft Internet Explorer の脆弱性を狙うことが知られています（図 11 を参照）。Flash をアンインストールし、不要なブラウザ プラグインを無効化または削除することで、ユーザはこれらの脅威に脅かされるリスクを軽減できます。

図 11 エクスプロイト キットで狙われやすい脆弱性



出典：シスコ セキュリティ リサーチ

[10] ロシアのハッカー、2,500 万ドル超の盗難で逮捕 [英語]、BBC News、2016 年 6 月 2 日：http://www.bbc.com/news/technology-36434104。
[11] このトピックについての詳細は、2016 年 7 月のシスコ Talos ブログ投稿、点と点を結ぶとクライムウェアの変化が明らかに [英語] を参照してください。

マルバタイジング：攻撃者はブローカを使用してスピードと俊敏性を高める

ユーザをエクスプロイト キットに誘導する方法として、侵害された Web サイトとマルバタイジングという 2 つがあります。攻撃者は、悪意のある広告や侵害された Web サイトにつながるエクスプロイト キットのランディング ページへのリンクを設置するか、ブローカとして知られる中間リンクを使用します（これらのリンクは感染した Web サイトとエクスプロイト キットのサーバ間に設置され、「ゲート」とも呼ばれます）。ブローカは、ユーザにマルウェアのペイロードを配信する実際のエクスプロイト キットと最初のリダイレクトの間の仲介役になります。

活動スペースを維持し、検出を避けるには、迅速に動く必要があることが攻撃者によって認識されるにつれ、後者の手法がより一般的になっています。ブローカを使えば、攻撃者は最初のリダイレクトを変更せずに、悪意のあるサーバから別のサーバにすばやく切り替えることができます。感染チェーンを開始するために Web サイトや悪意のある広告を常に変更し続ける必要がないため、エクスプロイト キットはより長期間のキャンペーンを実行できます。

ShadowGate：コスト効率の高いキャンペーン

従来の Web 攻撃ベクトルだけでは多数のユーザを侵害することが困難になったため（15 ページを参照）、攻撃者はユーザをエクスプロイト キットに導くためにマルバタイジングに依存することが多くなっています。シスコの脅威リサーチャーは、最近のグローバルなマルバタイジング キャンペーンを「ShadowGate」と名付けました。このキャンペーンは、地域全体のユーザを標的とする、悪意のある大規模広告が、攻撃者にいかに高い柔軟性と機会を提供するかを示しています。

ShadowGate には、ポップカルチャーから小売、ポルノからニュースに至るさまざまな Web サイトが含まれました。北米、欧州、アジア太平洋、中東の何百万人ものユーザが潜在的に影響を受けました。このキャンペーンのグローバルなリーチと多数の言語の使用は特筆すべきポイントです。

ドメイン シャドウイングを使用した ShadowGate が初めて見つかったのは 2015 年初頭でした。その後、活動を休止したり、再開したりを繰り返しながら、エクスプロイト キットのランディング ページにトラフィックを導きました。当初、ShadowGate は Angler エクスプロイト キットだけにユーザを誘導するために使用されていました。しかし、Angler が 2016 年夏に消滅してから、ユーザは Neutrino エクスプロイト キットに誘導され、数ケ月後に同じく消滅するまで続きました（この事例の詳細については、20 ページの「小規模企業や新規参入者にとって、重大なエクスプロイト キットの消滅は機会となる」を参照してください）。

ShadowGate が大量の Web トラフィックを使用したとはいえ、ユーザがエクスプロイト キットに誘導されたのはほんの一部でした。悪意のある広告の大半はページに表示されるインプレッション広告で、ユーザの操作を必要としませんでした。このオンライン広告モデルにより、ShadowGate に関与した攻撃者は、キャンペーンを高いコスト効率で運用することができました。

ShadowGate に対するシスコの調査は、Web ホスティングの大企業との連携につながりました。この協力により、攻撃者がアクティビティをホストするために使用していた登録アカウントを再要求することで、脅威を軽減しました。その後、該当するすべてのサブドメインを削除しました。

ShadowGate キャンペーンの詳細については、2016 年 9 月のシスコ Talos ブログ投稿、Talos、ShadowGate を削除：グローバル マルバタイジング キャンペーンを阻止 [英語] を参照してください。

調査によって 75 % の組織がアドウェア感染の影響を受けたことが判明

正当な目的に使用される場合、アドウェアはリダイレクション、ポップアップ、および広告インジェクションによって広告をダウンロードまたは表示し、作成者に収益をもたらすソフトウェアです。ただし、サイバー犯罪者も収益源を増やすためにアドウェアをツールとして使用します。犯罪者は悪意のあるアドウェアを広告インジェクションで収益を上げるために使用するだけでなく、DNSChanger マルウェアなどの他のマルウェア キャンペーンを促進するための最初のステップとしても使用します。悪意のあるアドウェアはソフトウェア バンドルを通して配布されます。パブリッシャは、多数の悪意のあるアドウェア アプリケーションとともに正当なアプリケーションを含めて 1 つのインストーラを作成します。

攻撃者はアドウェアを使用して次のことを行います。

- 広告を挿入します。更なる感染やエクスプロイト キットへの露出を引き起こす可能性があります。
- ブラウザおよびオペレーティング システム設定を変更して、セキュリティを弱体化させます。
- ウイルス対策製品またはその他のセキュリティ製品を破壊します。
- 他の悪意のあるソフトウェアをインストールできるように、ホストを完全に制御します。
- 場所、ID、使用中のサービス、およびよくアクセスするサイトを手掛かりにしてユーザを追跡します。
- 個人データ、クレデンシャル、インフラストラクチャ情報（例：企業の内部売上のページ）などの情報を密かに盗み出します。

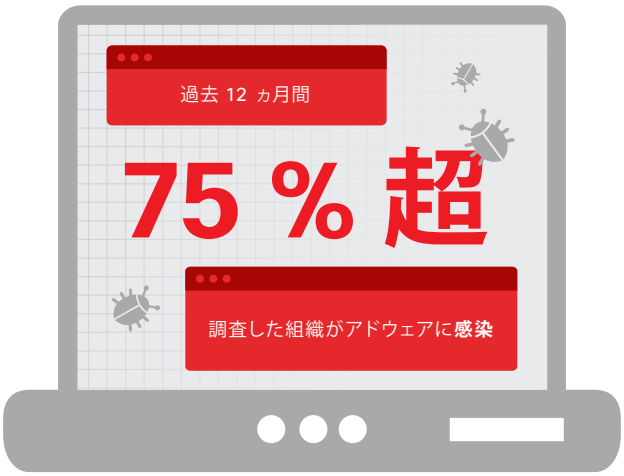
企業のアドウェア問題の範囲を評価するために、シスコの脅威研究者は 80 の異なるアドウェアのバリエーションを調査しました。さまざまな業界の約 130 の組織を調査対象として、調査は 2015 年 11 月から 2016 年 11 月まで実施されました。

シスコは、各コンポーネントの主な行動に基づいて、アドウェアを 4 つのグループに分類しました。

- **広告インジェクタ：**このアドウェアは通常ブラウザに常駐し、すべてのオペレーティング システムに影響を及ぼすことができます。
- ブラウザ設定ハイジャッカー：このアドウェア コンポーネントはコンピュータの設定を変更して、ブラウザのセキュリティを低下させることができます。
- **ユーティリティ：**アドウェアの大きい部分を占める、拡大中のカテゴリです。ユーティリティは、ユーザに PC 最適化などの便利なサービスを提供する Web アプリケーションです。これらのアプリケーションは広告を挿入できますが、主な目的はユーザを説得してサービス料金を支払わせることです。ただし、多くの場合、ユーティリティは詐欺でしかなく、ユーザに利益をもたらしません。
- **ダウンローダ：**このアドウェアは、ツールバーなどの他のソフトウェアを提供できます。

調査の結果、調査対象の組織の 75 % がアドウェア感染の影響を受けていました。

図 12 アドウェアに感染した組織の割合



出典：シスコ セキュリティ リサーチ

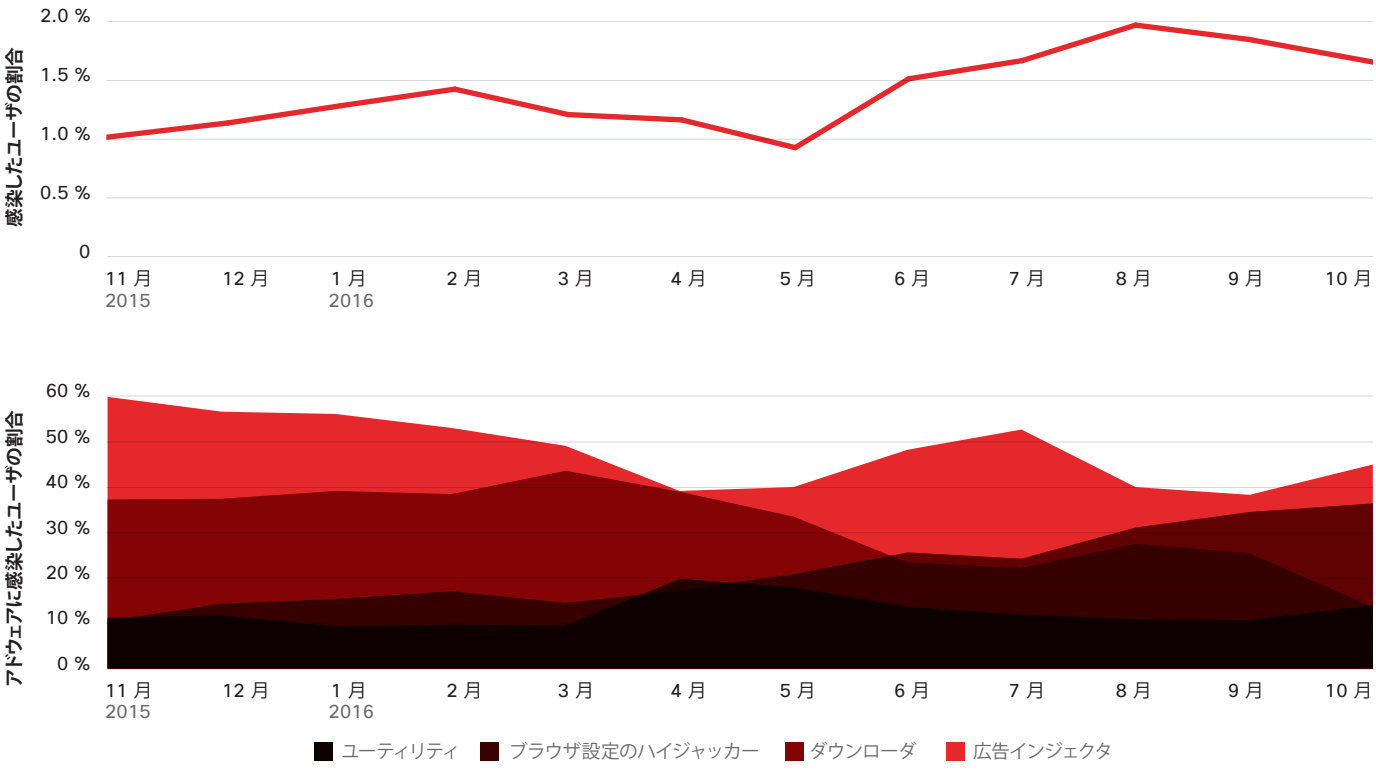
シェアする

図 13 は、調査対象の組織で確認されたインシデントのタイプを示しています。最大の感染源は広告インジェクタでした。この事実は、これらの望ましくないアプリケーションの大半が Web ブラウザをターゲットとしていることを意味します。また、この数年間でブラウザ ベースの感染が拡大していることも判明しました。これは、攻撃者が、この戦略によってユーザの侵害に成功していることを示します。

調査で特定されたすべてのアドウェア コンポーネントは、ユーザと組織に悪意のあるアクティビティのリスクを及ぼす可能性があります。セキュリティ チームは、アドウェア感染がもたらす脅威を認識し、組織のユーザにもリスクを十分に認識させる必要があります。

このトピックの詳細については、シスコ セキュリティ ブログの 2016 年 2 月の投稿「DNSChanger Outbreak Linked to Adware Install Base」を参照してください。

図 13 合計インシデント数に対するアドウェア コンポーネントの内訳



出典：シスコ セキュリティ リサーチ

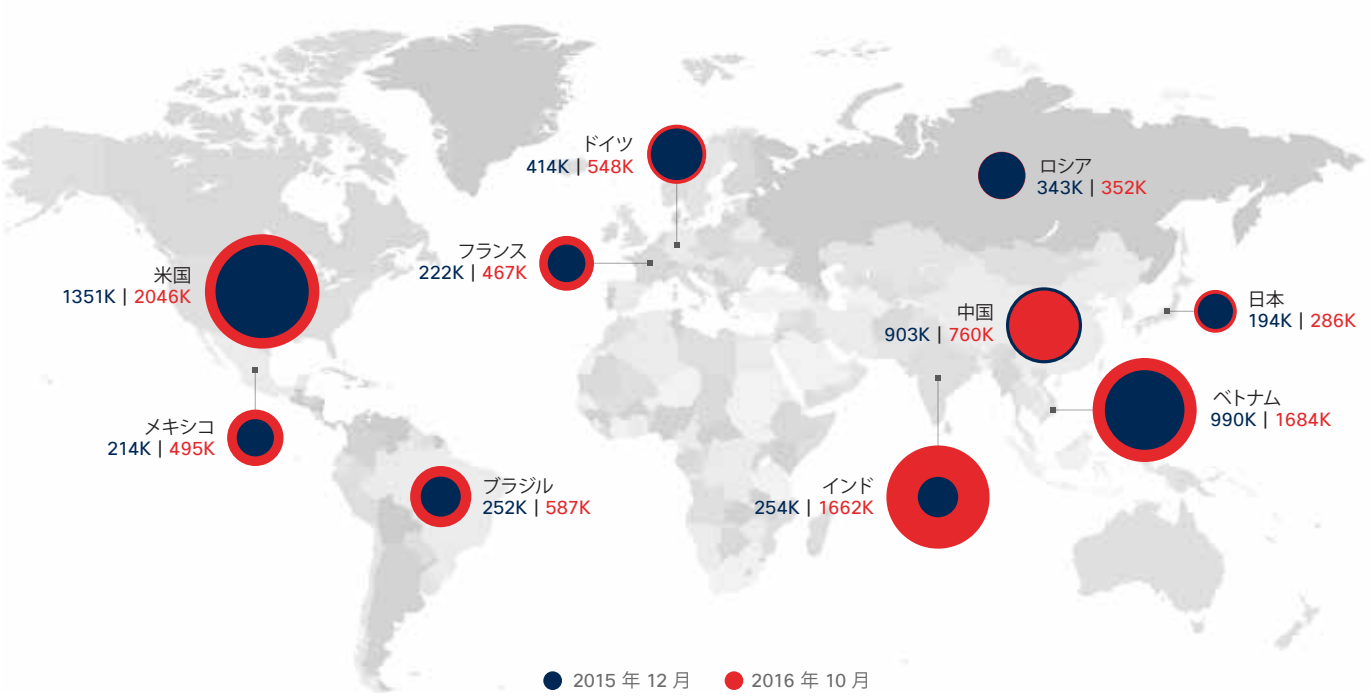
2017 年版の図表はこちらからダウンロードしてください：**www.cisco.com/go/acr2017graphics**

グローバル スパムが増加しており、それとともに悪意のある添付ファイルの割合も増加している

シスコの脅威研究者は、電子メールの総量に占めるスパムの割合を推定するために、2016 年にオプトイン カスタマー テレメトリを使用して 2 回の調査を実施しました。その結果、スパムが電子メールの総量の約 3 分の 2（65 %）を占めることが判明しました。また、この調査では、主に大規模に拡大しているスパム送信ボットネット（Necurs など）により、グローバル スパム量が増加していることが示唆されています。さらに、シスコの分析により、2016 年に観測されたグローバル スパムの約 8 ～ 10 % が悪意のあるものと分類できることが分かりました。

2016 年の 8 月から 10 月 にかけて、IP 接続ブロック数が大幅に増加しました（図 14）。[12] この動向は、スパム量の全体的な増加と、スパム送信者に関する情報に適応するレピュテーション システムによるものである可能性があります。

図 14 国別 IP ブロック数、2015 年 12 月～ 2016 年 11 月



出典：シスコ セキュリティ リサーチ

シェアする

[12] IP 接続ブロック数とは、スパム送信者のレピュテーション スコアが低いためにスパム検出テクノロジーによって直ちにブロックされたスパム メッセージの数です。たとえば、既知のスパム送信ボットネットや、スパム攻撃への関与が周知の侵害されたネットワークから送られたメッセージなどがあります。

コンポジット ブロック リスト（CBL）から作成された 5 年間のグラフ（疑わしいスパム送信コンピュータ感染の DNS ベースの「ブラックホール リスト」[13]）も、2016 年にスパムの総量が急増していることを示しています（図 15）。

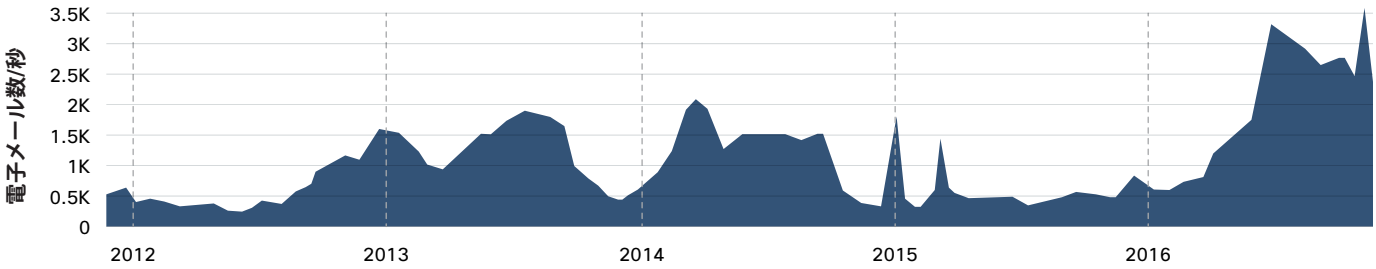
CBL からの 10 年間のデータ（図はありません）を調べると、2016 年のスパム量は、過去最大だった 2010 年に近いことが分かります。新しいスパム対策技術と、スパム関連ボットネットの大型摘発により、近年はスパムのレベルが低い状態が続いていました。シスコの脅威研究者は、最近のグローバル スパムの増加が Necurs ボットネットによるものと考えています。Necurs は Locky ランサムウェアの主要な媒体です。また、銀行系のトロイの木馬である Dridex などの脅威も拡散させています。

図 16 は、2016 年に観測されたスパム量の変化を示す、シスコの SpamCop サービスによって生成された社内用グラフです。

このグラフは、2015 年 11 月から 2016 年 11 月にかけての SpamCop ブロック リスト（SCBL）の全体的なサイズを示しています。SCBL の各行は、異なる IP アドレスを表します。

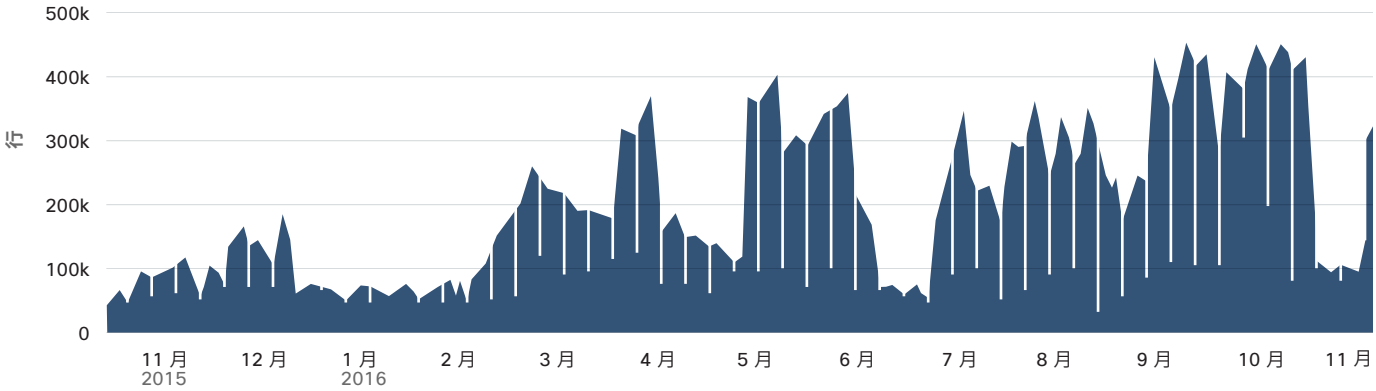
2015 年 11 月から 2016 年 2 月の間は、SCBL のサイズが 200,000 IP アドレス未満で推移しています。SCBL のサイズは、9 月と 10 月 に 400,000 IP アドレスを超え、その 10 月中に減少しています。シスコの脅威研究者は、これを、Necurs のオペレータが単に休暇を取ったためと考えています。また、6 月に大幅に減少している点に注目してください。5 月末に、銀行系のトロイの木馬である Lurk に関連する逮捕劇がありました（21 ページを参照）。その後、Necurs を含む複数の知名度の高い脅威が鳴りを潜めました。ただし、その 3 週間後には、Necurs は、活動を再開し、2 時間未満で 200,000 を超える IP アドレスが SCBL に追加されました。

図 15 スパムの合計数



出典：CBL

図 16 SCBL 全体の規模



出典：SpamCop

[13] CBL の詳細については、http://www.abuseat.org/ を参照してください。

Necurs スパムを送信するホスト IP の多くは、2 年以上にわたって感染しています。ボットネットの全容が解明されないように、Necurs は感染したホストの一部からのみスパムを送信します。感染したホストは、たとえば 2 ～ 3 日間使用され、その後 2 ～ 3 週間は再使用されないこともあります。このような使用方法が、スパム攻撃に対応するセキュリティ担当者の仕事を複雑にしています。セキュリティ担当者が感染したホストを発見し、完全に排除したと信じていても、Necurs の背後にいる攻撃者は、別の攻撃を開始する時間を稼いでいるにすぎません。

2016 年 10 月に観測されたスパムの総量の 75 % に悪意のある添付ファイルが含まれていました。そのスパムのほとんどが、Necurs ボットネットによって送信されていました（図 17 を参照）。Necurs は、JavaScript、.hta、.wsf、VBScript ダウンローダなどの組み込み実行ファイルが含まれた悪意のある .zip 添付ファイルを送信します。スパムの総量に占める悪意のある添付ファイルを含むスパムの割合を計算する際は、「コンテナ」ファイル（.zip）とその中の「子」ファイル（JavaScript ファイルなど）の両方を単一の悪意のある添付ファイルとしてカウントしています。

攻撃者は悪意のあるスパムの活動を常に新しいものにするためにさまざまなタイプの添付ファイルで実験している

シスコの脅威研究者は、悪意のあるスパムの検出を妨げるために攻撃者が異なるタイプの添付ファイルをどのように使用しているのかを調べました。その結果、さまざまなファイル タイプで実験し、成功しないときは戦術をすばやく切り替えることによって、攻撃者が戦略を進化させ続けていることが分かりました。

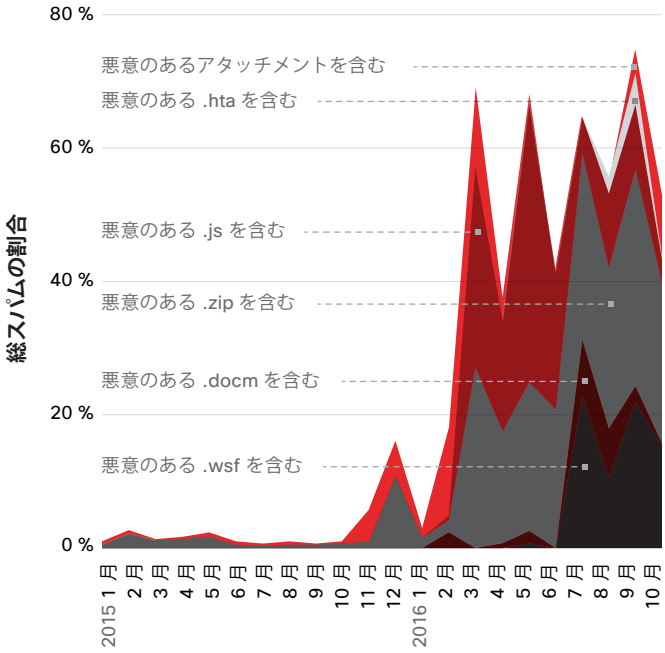
図 17 は、観測期間に悪意のあるスパムのオペレータが .docm、JavaScript、.wsf、および .hta ファイルを使用してどのように実験したかが示されています。前述のように、これらのファイル タイプの多くが、Necurs ボットネットによって送信されるスパムに関連付けられています（シスコが行った他のファイル タイプに関する調査については 78 ページの付録を参照）。

ある月の異なるファイル タイプの割合は、その月に観測された、スパムの総量に占める悪意のある添付ファイルを含むスパムの割合を使用して取得されます。したがって、たとえば 2016 年 7 月の .docm ファイルは、観測された悪意のある添付ファイルの 8 % に相当していました。

2016 年の .wsf ファイルのパターン（図 17 を参照）は、攻撃者が時間とともに悪意のあるスパムの戦術を進化させる様子を示しています。このファイル タイプは、2016 年 2 月までは悪意のある添付ファイルとしてほとんど使用されていませんでした。その後、Necurs ボットネットの活動が活発になるにつれて、このファイル タイプの使用が増えはじめました。7 月には、.wsf ファイルはすべての悪意のあるスパムの添付ファイルの 22 % を占めるようになりました。これは、Necurs ボットネットを主たる原因としてグローバル スパムの活動が急増した時期とも重なります（前のセクションを参照）。

8 月、9 月、10 月と、.wsf ファイルの割合に変動が見られました。これは、このファイル タイプが頻繁に検出されるようになって攻撃者が手控えていることを示しています。

図 17 悪意のある添付ファイルを含むスパムの割合



出典：シスコ セキュリティ リサーチ

Hailstorm とスノーシュー

防御者にとって特に厄介な 2 種類の悪意のあるスパム攻撃があります。それは、Hailstorm 攻撃とスノーシュー攻撃です。どちらも高スピードとターゲットを絞った攻撃を特徴としており、非常に効果的な攻撃です。

Hailstorm 攻撃はスパム対策システムをターゲットとしています。これらの攻撃の背後にいるオペレータは、スパムが活動を開始する瞬間と、スパム対策システムがそれを検出して対象の範囲をスパム対策スキャナに渡すまでのごくわずかな時間を利用します。攻撃者には、通常、活動が検出されてからブロックされるまでに動くことのできる時間が数秒または数分しかありません。

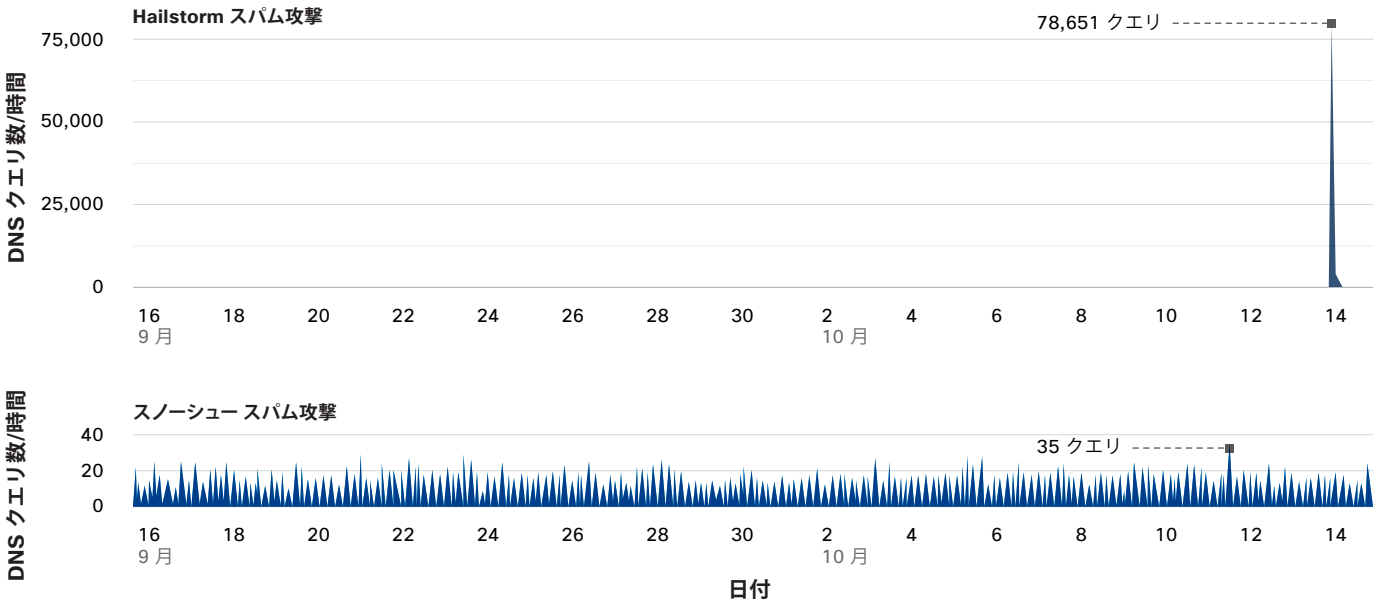
図 18 で急増しているのは、Hailstorm 攻撃です。この活動は、シスコの調査結果に示されています。攻撃の直前には、当該の IP アドレスを解決しているコンピュータはありませんでした。その後、突然、DNS でドメインを解決するコンピュータの数が 78,000 以上に急増し、ゼロに戻りました。

また、図 18 では、Hailstorm 攻撃をスノーシュー スパムの活動と比較しています。攻撃者はスノーシューにおいて、ボリュームベースの検出ソリューションによるレーダーを回避することを試みています。一定数の DNS ルックアップが存在していますが、その数は 1 時間あたり約 25 クエリにすぎません。これらの低ボリューム攻撃は、攻撃者が広範囲の IP アドレスから静かにスパムをばら撒くことを可能にします。

これらのスパム攻撃は動作が異なっていますが、共通する点があります。どちらのアプローチでも、攻撃者は以下のことが可能です。

- クリーンな IP およびドメインから送信することにより、低信頼性の評価を回避する。
- 専門のコンテンツを持ちサブスクリプションが管理されたマーケティング メールを偽装する。
- 質の低いスクリプトやスパム ボットではなく高度に設定された電子メール システムを使用する。
- 転送確認逆引き DNS（FCrDNS）および送信ドメイン認証である Sender Policy Framework（SFP）レコードを正しくセットアップする。

図 18 Hailstorm 攻撃とスノーシュー スパム攻撃の比較



出典：Cisco Investigate

攻撃者は、テキストを変化させ、ファイル タイプを循環させることによって、コンテンツ検出で発見されにくくすることもできます。（サイバー犯罪者が脅威を進化させて防御者から逃れる方法の詳細については、34 ページの「進化時間」のセクションを参照）。悪意のあるファイルをスパムに添付した、攻撃者による実験的な手法については、前のセクションを参照してください。

図 19 は、生成回数の多い脅威発生アラートを示しています。これは、2016 年中、攻撃者が電子メールのセキュリティ チェックやルールを回避するためにスパムやフィッシング メッセージを頻繁に更新したことを示しています。これらの悪意あるメッセージから被害を受けることを避けるために、どのようなタイプの電子メール脅威が普及しているかを把握することが重要です。

図 19 上位の脅威アウトブレイク アラート

バージョン	パブリケーション ID	パブリケーション名と URL	メッセージの概要	添付ファイルのファイルタイプ	言語	最終パブリケーション日
96	35656	RuleID4626	請求書、支払い	.zip	ドイツ語、英語	2016/04/25
87	34577	RuleID10277	発注書	.zip	ドイツ語、英語	2016/06/02
82	36916	RuleID4400KVR	発注書	.zip	英語	2016/02/01
74	38971	RuleID15448	発注書、支払い、領収書	.zip, .gz	英語	2016/08/08
72	41513	RuleID18688	注文、支払い、セミナー	.zip	英語	2016/09/01
70	40056	RuleID6396	発注書、支払い、領収書	.rar	英語	2016/06/07
66	34796	RuleID5118	製品の注文、支払い	.zip	ドイツ語、英語	2016/09/29
64	39317	RuleID4626 (cont)	請求書、支払い、出荷	.zip	英語、ドイツ語、スペイン語	2016/01/28
64	36917	RuleID4961KVR	確認、支払い/転送、注文、出荷	.zip	英語	2016/07/08
63	37179	RuleID13288	到達通知書、出廷、チケットの請求	.zip	英語、スペイン語	2016/07/21
61	38095	RuleID858KVR	出荷、見積書、支払い	.zip	英語	2016/08/01
58	39150	RuleID4961KVR	見積り依頼、製品の注文	.zip	英語、ドイツ語、複数の言語	2016/01/25
47	41886	RuleID4961	転送、出荷、請求書	.zip	英語、ドイツ語、スペイン語	2016/02/22

出典：シスコ セキュリティ リサーチ

2017 年版の図表はこちらからダウンロードしてください：**www.cisco.com/go/acr2017graphics**

偵察 | 武器化 | 配信 | インストール

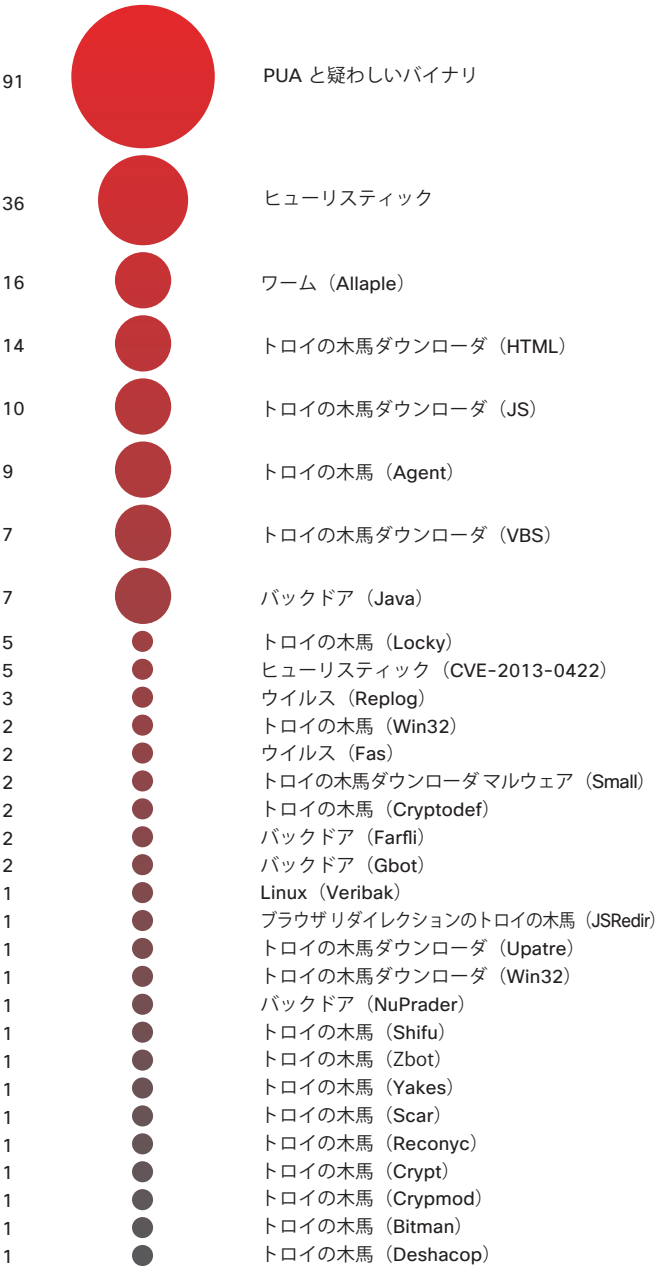
脅威が有効になると、対象のシステムにバック ドアをインストールして、攻撃者に永続的なアクセスを提供します。

Web 攻撃の手法：「ロング テール」攻撃された際の脅威を明らかにすることで、ユーザにとって容易に回避することができる

Web 攻撃手法の分布のいわゆるロング テール（図 20）には、一連の攻撃活動の後半（インストール）で使用される小容量のマルウェア タイプのコレクションが含まれています。このフェーズでは、配信された脅威（銀行系のトロイの木馬、ウイルス、ダウンローダ、またはその他のエクスプロイト）によってバック ドアがターゲット システムにインストールされ、永続的なアクセスと、データを抜き取り、ランサムウェア攻撃を開始し、その他の損害を与える機会が攻撃者に提供されます。

図 20 に示されている脅威は、最も一般的に観測された上位 50 のマルウェア タイプ以外に発見されたマルウェア シグネチャのサンプルです。Web 攻撃のロングテールは、実質的にはその瞬間に発生するものであり、攻撃が成功した後に、そのマシン上で密かに実行されます。これらの感染の多くは、最初に、悪意のあるアドウェアに遭遇するか、巧妙に準備されたフィッシング詐欺に直面することによって発生します。これらは、多くの場合、ユーザが簡単に回避し、素早く対処することができる状況です。

図 20 比較的観察数が少ないマルウェアのサンプル



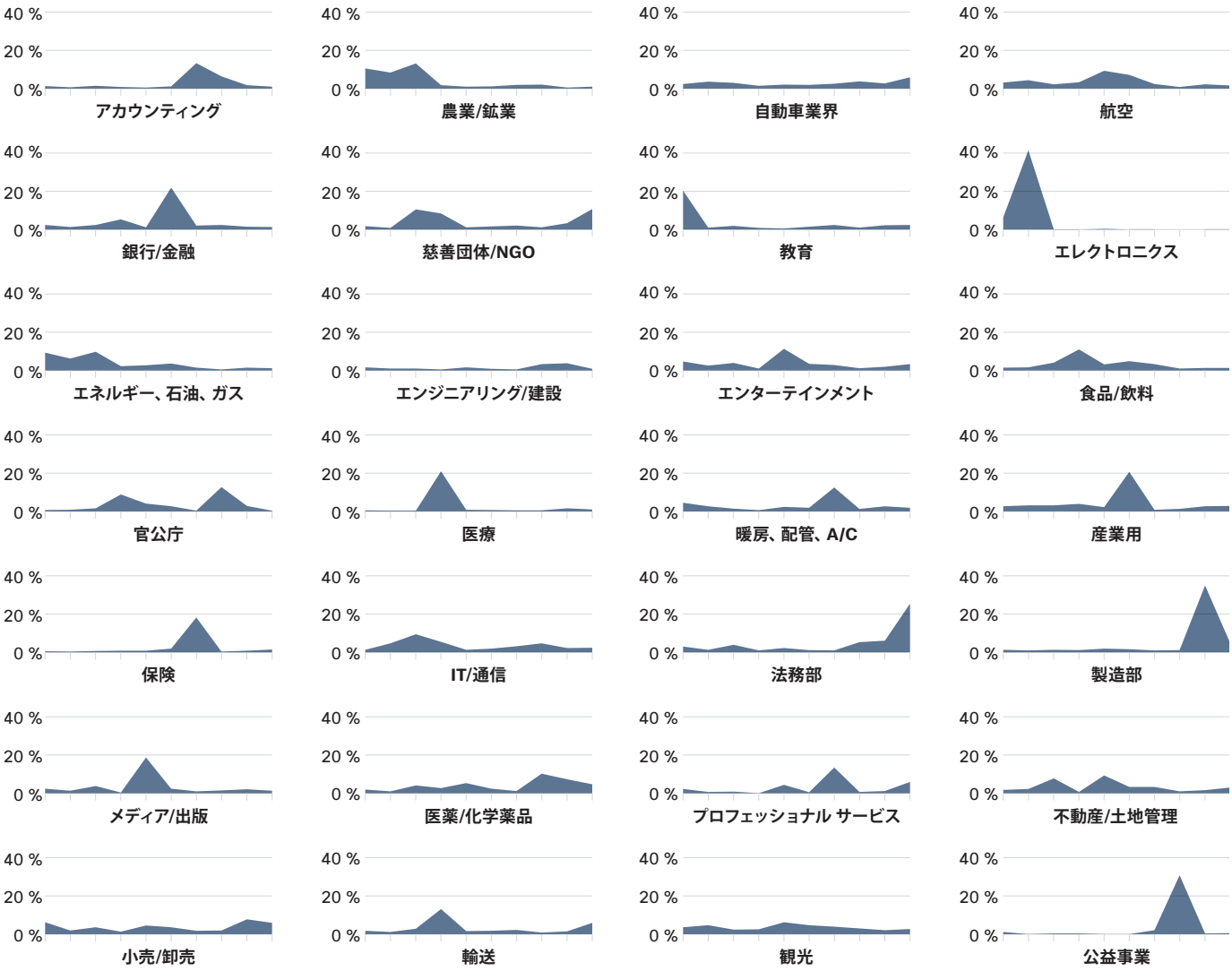
出典：シスコ セキュリティ リサーチ

マルウェア遭遇の業種別リスク：攻撃者はすべての対象に価値を見出す

『*Cisco 2016 Midyear Cybersecurity Report*』に示されているマルウェアのリスクに関する重要なメッセージは、「安全な業種はない」というものでした。シスコの研究者が実施した、業種別の攻撃トラフィック（「ブロック率」）と「正常な」または予期されるトラフィックに関する定期的な調査から判断すると、このメッセージは、その年の後半には現実のものになりました。

特定業種とその経時的なブロック率を見ると（図 21）、どの業種も、数ヵ月のうちにはどこかで攻撃トラフィックが発生しており、そのレベルもさまざまです。攻撃に波があることから、業種によって攻撃の影響を受ける回数が異なっていることは明らかですが、どれも見過ごすことのできないものです。

図 21 月ごとの業界ブロック率（パーセンテージ）



出典：シスコ セキュリティ リサーチ

シェアする

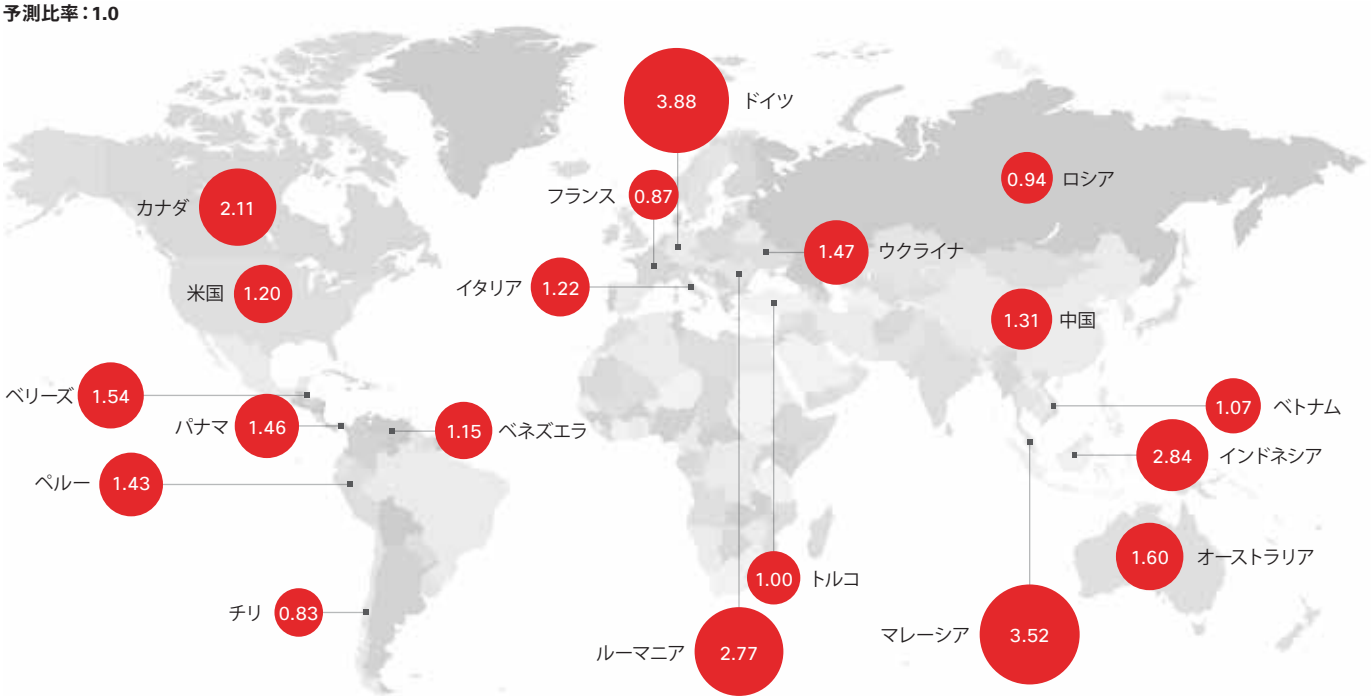
Web ブロック アクティビティの地域別の概要

攻撃者は、攻撃活動を開始できる脆弱なインフラを探しながら、拠点を頻繁に移します。全体的なインターネット トラフィック量とブロック アクティビティを調べることにより、シスコの脅威研究者は、マルウェアの発生源に関する洞察を提供できます。

図 22 のように、米国からのトラフィックのブロック率は、『*Cisco 2016 Midyear Cybersecurity Report*』で報告されたものから多少増加しています。米国のブロックのシェアは非常に大きなものですが、これはこの国が持つオンライン トラフィックのシェアが非常に大きいためであると考えられます。加えて、米国は、世界最大のマルウェア攻撃ターゲットの 1 つです。

セキュリティ プロフェッショナルが考慮すべき点として、業種別の Web ブロック アクティビティと同様に、地域別の Web ブロック アクティビティは、マルウェア トラフィックがグローバルな問題であることを示しています。

図 22 国別 Web ブロック数



出典：シスコ セキュリティ リサーチ

シェアする

検出時間：防御者の進展を評価するために不可欠な尺度

シスコでは、検出時間（TTD）の中央値に関する可能な限り正確な予測を追跡し報告するために、TTD を測定するアプローチを継続的に改善しています。このアプローチに関する最近の調整により、最初に検出されたときには「不明」と分類されたファイルに対する可視化が強化され、継続的な分析とグローバルな観測の後に「既知の脅威」として識別されるようになりました。データのより大きな全体像により、脅威が最初に発生した時点と、セキュリティ チームがそれを脅威と判断するまでにかかった正確な時間を特定するシスコの能力が向上しました。

この新しい洞察により、シスコの TTD 中央値は 2015 年 11 月の時点で 39 時間だったと判断されました（図 23 を参照）。2016 年 1 月までにシスコの TTD 中央値は 6.9 時間に短縮されました。2016 年 10 月に実施されたデータの収集と分析の結果、シスコの脅威研究者は、2015 年 11 月から 2016 年 10 月の期間にシスコ製品が 14 時間という TTD 中央値を達成したことを確認しました（注：2016 年の TTD 中央値の図は観測期間の中央値の平均です）。

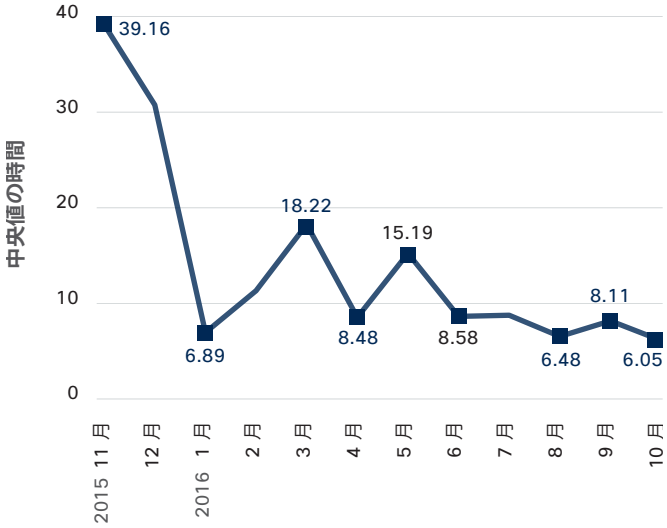
TTD 中央値は 2016 年の間に変動していますが、全体として減少する傾向にあります。TTD 中央値の増加は、攻撃者が新しい脅威の波を起こした時点を示しています。その後の減少は、防御者が優勢で、既知の脅威を迅速に特定できた期間を反映しています。

図 23 は、TTD の中央値が 2016 年 4 月末に約 15 時間だったことも示しています。これは、『*Cisco 2016 Midyear Cybersecurity Report*』で報告された 13 時間よりも大きくなっています。[14] 15 時間という数値は、2015 年 11 月から 2016 年 4 月に収集されたデータに基づいています。このデータの取得には、ファイルに関するより詳細なレトロスペクティブ（遡及的）情報の分析に対するシスコの変更されたアプローチが使用されていません。2016 年の 5 月から 10 月 にかけて TTD が約 9 時間に短縮されたことを報告できます。

遡及的データの確認は、シスコの TTD 中央値をより正確に測定するためだけでなく、脅威が時間とともにどのように進化するのかを調査するためにも重要です。活動中の多数の脅威が特有の方法で逃げ回るため、セキュリティ コミュニティに既知のものであっても、その識別に時間がかかる場合があります。

攻撃者は、検出を回避し、活動時間を延ばすために、特定のマルウェア ファミリを進化させます。この戦術が、防御者の追跡、保守、およびさまざまなタイプの既知の脅威の迅速な検出の進展を妨げています（このトピックの詳細については、34 ページの「進化時間：一部の脅威は常に変化している」を参照）。ただし、サイバー犯罪者が脅威を頻繁かつ迅速に進化させているという事実は、脅威の活動と収益性を維持する方法を見出す上で強力な圧力を常に受けていることを示しています。

図 23 月別 TTD 中央値



出典：シスコ セキュリティ リサーチ

シスコでは、検出時間（TDD）を侵害から脅威が検出されるまでの時間として定義しています。この時間は、世界中で導入されているシスコのセキュリティ製品から収集されたオプトイン セキュリティ テレメトリから決定されます。シスコは、グローバルな可視性と継続的な分析モデルを使用することで、出現時に分類でされていないどのような悪意のあるコードであっても、エンドポイントで悪意のあるコードが実行された瞬間から、それが脅威であると判断される時間までを測定することができます。

[14] *2016 年シスコ中期サイバーセキュリティ レポート [英語]*: **http://www.cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html**.

進化時間：一部の脅威は常に変化している

サイバー犯罪者は、マルウェアの力と収益性を維持するために、さまざまな難読化手法を使用しています。そのために使用される 2 つの一般的な手法は、ペイロード配信タイプを進化させることと、新しいファイルを迅速に生成する（ハッシュのみの検出方式を無効化する）ことです。シスコの研究者は、攻撃者が 6 つのよく知られたマルウェア ファミリ（Locky、Cerber、Nemucod、Adwind RAT、Kryptik、および Dridex）で検出を回避させ、ユーザとシステムを継続して侵害させるために、これらの 2 つの手法をどのように使用したかを綿密に調べました。

この分析を通じて、「進化時間」（TTE）、つまり攻撃者が特定のマルウェアの配信方法を変更するためにかかった各時間や各戦術における変更時間の測定に取り組みました。そして、シスコのさまざまなソース（具体的には Web プロキシ データ、クラウド、およびエンドポイントの高度なマルウェア対策製品とコンポジット マルウェア対策エンジン）から得られた Web 攻撃データを分析しました。

シスコの研究者は、マルウェアを配信するファイルの拡張子とユーザのシステムによって定義されたファイル コンテンツ（または MIME）タイプの変化を調べました。その結果、各マルウェア ファミリには固有の進化のパターンがあることが分かりました。そこで、ファミリごとに、Web と電子メールの両方について配信手法のパターンを調べました。また、攻撃者が新しいファイル（したがって、新しいハッシュ）を作成する頻度を確認するために、各マルウェア ファミリに関連する固有のハッシュの寿命を追跡しました。

調査の結果、以下のことが判明しました。

- ランサムウェア ファミリのローテーションは、新しいバイナリのローテーションに似ていると思われます。ただし、Locky は、より多くのファイル拡張子と MIME の組み合わせを使用してペイロードを配信しています。
- 一部のマルウェア ファミリでは、わずかなファイル配信手法のみが使用されています。その他では、10 以上の手法が使用されています。攻撃者は、有効なバイナリを長期間にわたって使用する傾向があります。それ以外は、ファイルが出現するとすぐに消滅しています。これは、マルウェアの作成者が戦術を切り替える必要に迫られていることを示します。
- Adwind RAT および Kryptik マルウェア ファミリについては、TTD 中央値が比較的大きくなっています（TTD の詳細については、33 ページを参照）。また、これらファミリについては、ファイルの寿命が比較的長いグループも確認されています。このことは、検出が困難であることが分かったバイナリを攻撃者が再利用していることを示唆します。
- Dridex マルウェア ファミリのファイル寿命を調べると、地下経済では、この一時流行した銀行系のトロイの木馬の使用が断念されている可能性があると考えられます。2016 年の後半には、このマルウェアを配信する新しいバイナリが開発されたため、Dridex の検出数が減少しました。この傾向は、マルウェアの作成者がこの脅威を進化させることに価値を見出せなくなったか、検出をより困難にするマルウェアのパッケージ化の新しい方法を発見したことを示唆しています。

TTE と TTD

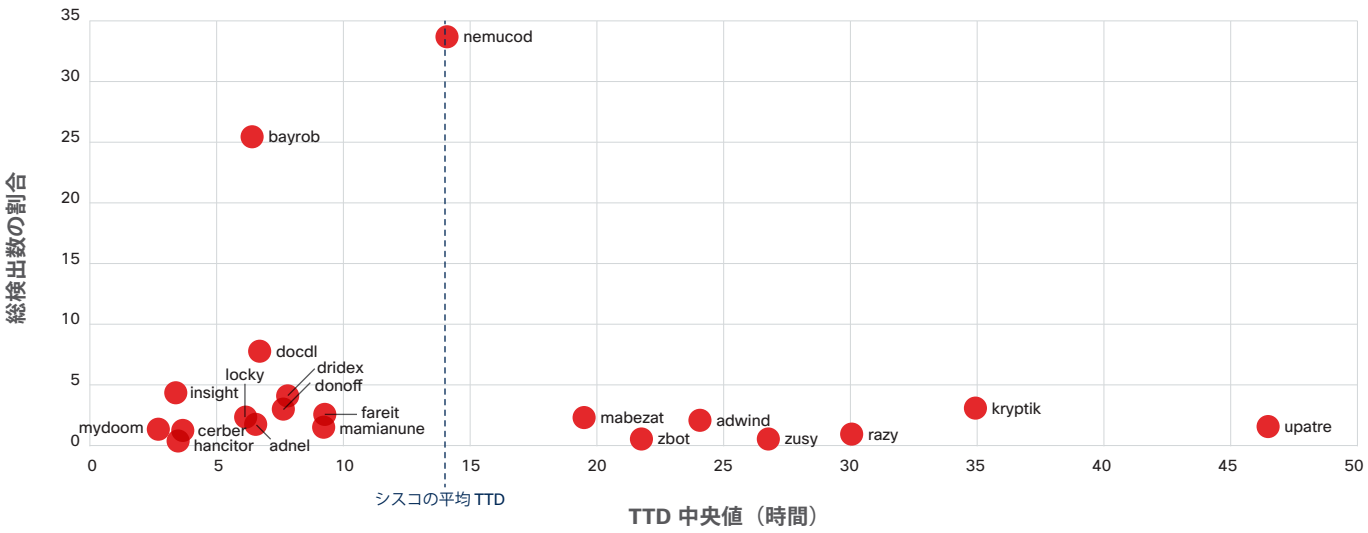
図 24 には、TTE に関する調査で分析した 6 つのマルウェア ファミリが示されています。この図は、シスコの研究者が 2015 年 11 月から 2016 年 11 月にかけて観測したマルウェア ファミリの検出数上位 20 の TTD 中央値を示しています。この期間の平均 TTD 中央値は約 14 時間でした（TTD の計算方法の詳細については、33 ページを参照）。

シスコ製品が TTD 中央値未満で検出しているマルウェア ファミリの多くは、素早く拡散し、そのためにより普及している、産業化された脅威です。Cerber と Locky（どちらもランサムウェアのタイプ）は、その一例です。

攻撃者があまり、または、まったく進化させる気のない、普及した古い脅威も、通常、TTD 中央値未満で検出されます。これらの例には、Bayrob（ボットネット マルウェア）、Mydoom（Microsoft Windows に影響を与えるワーム）、Dridex（銀行系のトロイの木馬）などのマルウェア ファミリが含まれます。

以下のセクションでは、Locky、Nemucod、Adwind RAT、および Kryptik マルウェア ファミリの TTE と TTD に関する調査の概要を示します。Cerber と Dridex の詳細な調査結果については、78 ページの付録を参照してください。

図 24 上位マルウェア ファミリの TTD の中央値（検出数上位 20 ファミリ）



出典：シスコ セキュリティ リサーチ

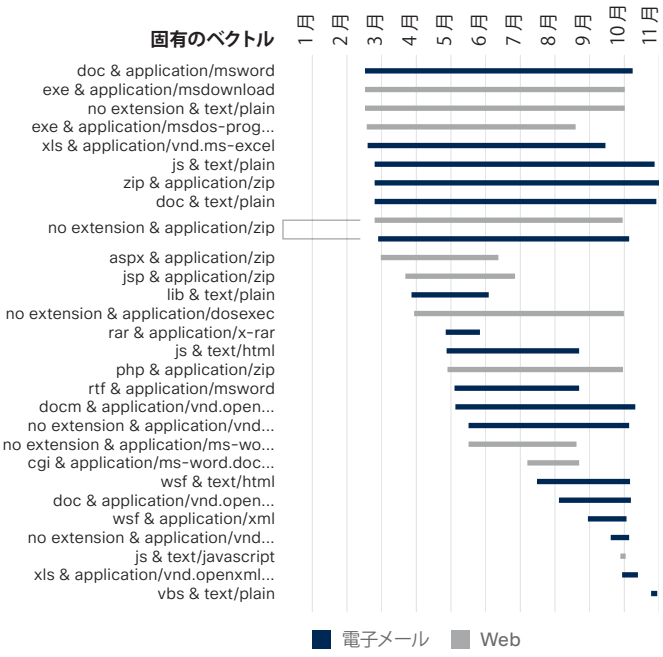
TTE 分析：Locky

シスコの TTE 調査により、Locky と Cerber は、Web や電子メールを通じてマルウェアを配信するために、限られた数のファイル拡張子と MIME の組み合わせを利用していることが分かりました（図 25 を参照）。Microsoft Word に関連するファイル コンテンツタイプ（msdownload、MS Word）を含むいくつかの組み合わせが観測されました。ただし、関連するファイル拡張子（.exe と .cgi）は、Word ファイルを指し示していませんでした。悪意のある .zip ファイルを指し示しているコンテンツ タイプも識別されました。

また、Locky と Cerber はどちらも、ファイル ベースの検出を回避する試みとして、頻繁に新しいバイナリを使用しているようです。図 26 には、Locky マルウェア ファミリのファイル寿命が示されています。図の上段は、ある月の間に観測されたファイルの寿命を示しています。図の下段は、Locky 関連ハッシュ（新しいファイルと以前に観測されたファイルの両方）の量が月ごとにどのように変化しているかを示しています。

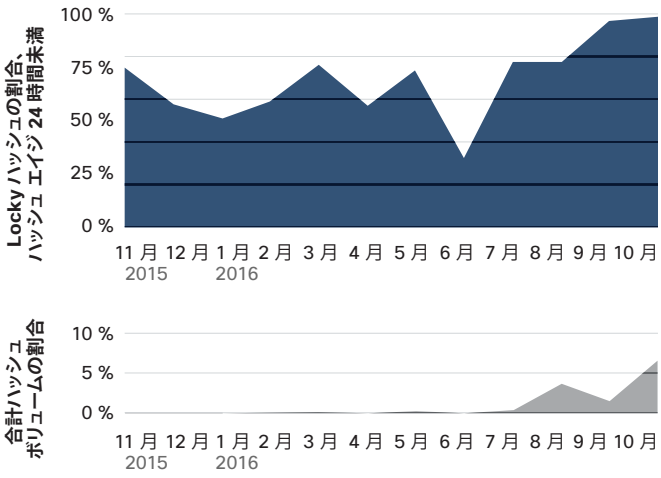
図 26 では、6 月の量の減少とファイル寿命の分布にも注目してください。Locky を配信することが知られている Necurs ボットネットは 6 月に停止しました。これにより、その月にマルウェア作成者によるマルウェア更新の作業が滞ったと思われます。しかし、すぐに回復したことは明らかです。7 月までに、このマルウェアは、最初に検出されてから 1 日未満という大半のマルウェア（74 %）によって構成されるより標準的な寿命のグループに戻っています。

図 25　脅威ファミリのファイル拡張子と MIME の組み合わせ、および Locky ペイロードにつながり、Locky ペイロードを含む指標（Web および電子メール ベクトル）



出典：シスコ セキュリティ リサーチ

図 26　Locky マルウェア ファミリのハッシュ年齢と 1 ヵ月あたりに確認された全ハッシュ ボリュームの割合



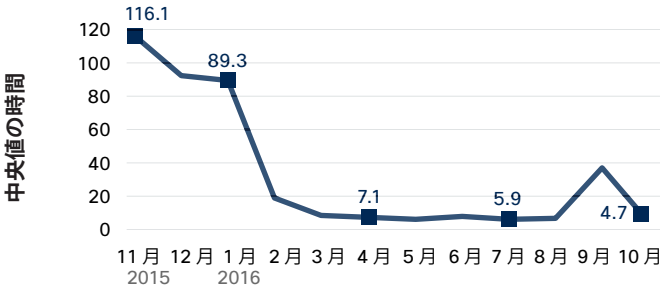
出典：シスコ セキュリティ リサーチ

シェアする

このランサムウェアのバイナリの迅速な循環は、驚くには当たりません。Locky と Cerber のインスタンスは、多くの場合、取り込まれた日かその 1 ～ 2 日後には検出されます。そのため、攻撃者は、これらの脅威がアクティブかつ効果的な状態を保つために、継続的に進化させる必要があります（前述のように、図 24 は、シスコ製品が Locky と Cerber の両方のランサムウェアを 2016 年に TTD 中央値未満で検出したことを示しています）。

図 27 は、2015 年 11 月の約 116 時間から 2016 年 10 月の 5 時間未満に急減した Locky ランサムウェアの TTD 中央値を示しています。

図 27 Locky マルウェア ファミリの TTD



出典：シスコ セキュリティ リサーチ

TTE 分析：Nemucod

2016 年では、Nemucod は、図 24 に示されている上位 20 ファミリの中でも最も頻繁に検出されたマルウェアでした。攻撃者は、このダウンローダ マルウェアを使用して、ランサムウェアやその他の脅威（クリック詐欺を促進するバックドアのトロイの木馬など）を配信しました。Nemucod の一部の亜種は、Nemucod マルウェア ペイロードを配信するエンジンとしても使用されました。

図 28 Nemucod のファイル拡張子と MIME の組み合わせ（Web および電子メール ベクトル）

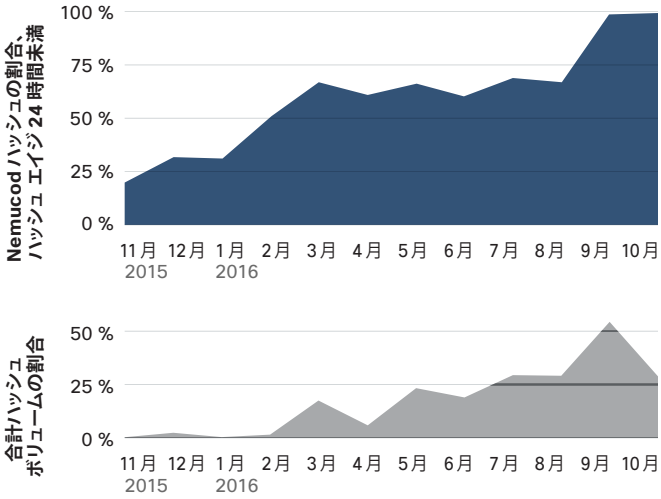
出典：シスコ セキュリティ リサーチ

Nemucod マルウェアが 2016 年にこれほど普及した理由の 1 つは、作成者がこの脅威を頻繁に進化させたことにある、とシスコの脅威研究者は考えています。シスコでは、Web 通じてマルウェアを配信するために使用された Nemucod ファミリに関連する、15 を超えるファイル拡張子と MIME の組み合わせを特定しました。さらに多くの組み合わせが、電子メールを通じて脅威をユーザにもたらすために使用されました（図 28）。

悪意のある zip ファイルまたはアーカイブにユーザの目を向けるために、いくつかのファイル拡張子と MIME の組み合わせ（Web および電子メール）が設計されました。また、攻撃者は、シスコが観測した数ヵ月の間に多数の組み合わせを再利用しています。

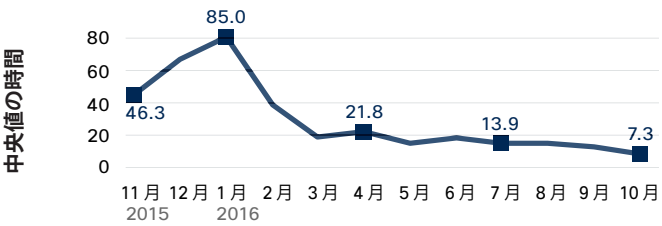
図 29 に示されているように、多数の Nemucod ハッシュの寿命は、検出から 2 日未満です。2016 年の 9 月と 10 月には、ブロックされた Nemucod ファミリに関連するほとんどすべてのバイナリの寿命が 1 日未満になっています。

図 29 Nemucod マルウェア ファミリのハッシュ年齢と 1 ヵ月あたりに確認された全ハッシュ ボリュームの割合



出典：シスコ セキュリティ リサーチ

図 30 Nemucod マルウェア ファミリの TTD



出典：シスコ セキュリティ リサーチ

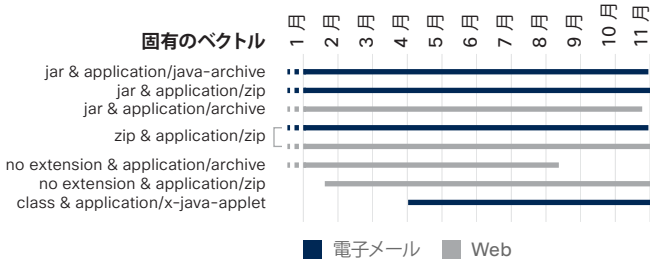
TTE 分析：Adwind RAT

シスコの脅威研究者は、Adwind RAT（リモート アクセスのトロイの木馬）マルウェアが .zip または .jar ファイルを含むファイル拡張子と MIME の組み合わせを使用して配信されたことを確認しました。これは、マルウェアが電子メールまたは Web 攻撃ベクトルのどちらを通じて配信されている場合にも当てはまります（図 31 を参照）。

Adwind RAT では、ほとんどのファイルの寿命が 1 ～ 2 日になったと思われる 9 月と 10 月を除き、2016 年の観測期間のほとんど全体でさまざまな寿命のハッシュを使用していました（図 32）。

また、Adwind RAT の TTD 中央値が、分析した他のマルウェアファミリの TTD 中央値よりも安定して高いことを確認しました（図 33）。マルウェアの作成者は、Adwind RATの成功を維持させる検出されにくい配信メカニズムを開発していたようです。このため、他のマルウェア ファミリを使用する攻撃者のように頻繁または迅速に新しいハッシュを循環させる必要がありません。Adwind のトロイの木馬は、JSocket や AlienSpy といった別名でも知られています。

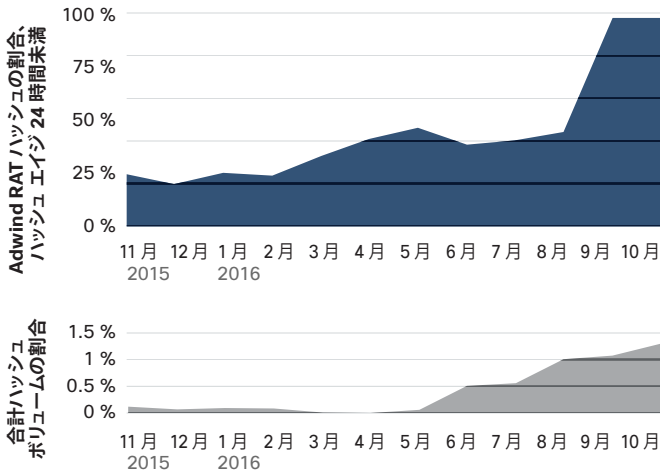
図 31 Adwind RAT のファイル拡張子と MIME の組み合わせ（Web および電子メール ベクトル）



出典：シスコ セキュリティ リサーチ

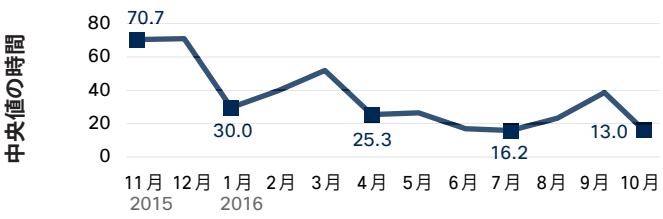
2017 年版の図表はこちらからダウンロードしてください：
www.cisco.com/go/acr2017graphics

図 32 Adwind RAT マルウェア ファミリのハッシュ年齢と 1 ヵ月あたりに確認された全ハッシュ ボリュームの割合



出典：シスコ セキュリティ リサーチ

図 33 Adwind RAT マルウェア ファミリの TTD



出典：シスコ セキュリティ リサーチ

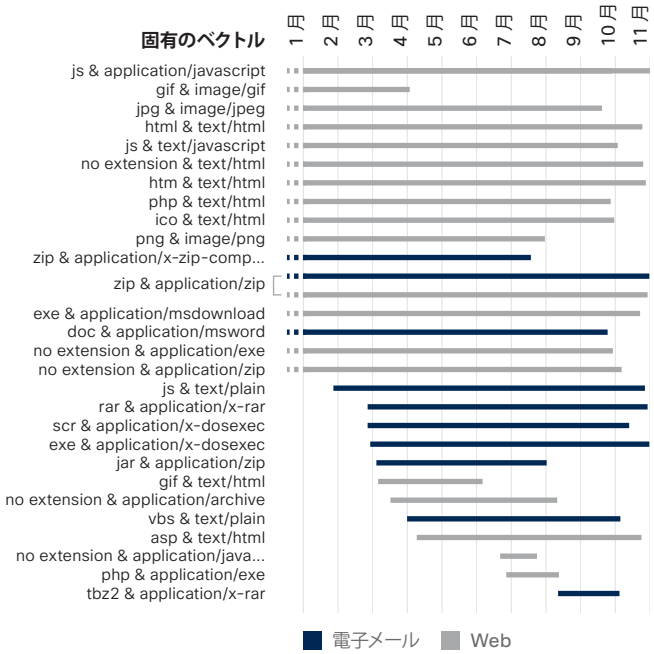
TTE 分析：Kryptik

Kryptik も、Adwind RAT マルウェアと同様に、2015 年 11 月から 2016 年 10 月までの TTE 調査においてシスコが分析した他のマルウェア ファミリよりも安定して高い TTD 中央値（約 20 時間）を保持していました（図 36）。ただし、10 月には、シスコ製品によって Kryptik マルウェアの TTD 中央値が 9 時間未満に低下しました（図 36）。

Kryptik マルウェア ファミリでも、特に 2016 年の前半において、シスコが分析した他のマルウェア ファミリよりも広範囲の寿命のハッシュが使用されていました。非常に長期にわたって比較的古いハッシュに依存している Kryptik の作成者の能力は、防御者がこのマルウェア タイプの検出に苦慮していることを示します。

シスコが観測した期間中に、Kryptik の作成者は、Web 攻撃ベクトルによる広範囲のペイロード配信手法を使用しました。この作成者は、Web と電子メールの両方に関してファイル拡張子と MIME の組み合わせにおいて JavaScript ファイルとアーカイブ ファイル（.zip ファイルなど）を使用しました（図 34 を参照）。この組み合わせの一部は 2011 年に遡ります。

図 34 Kryptik のファイル拡張子と MIME の組み合わせ（Web および電子メール ベクトル）

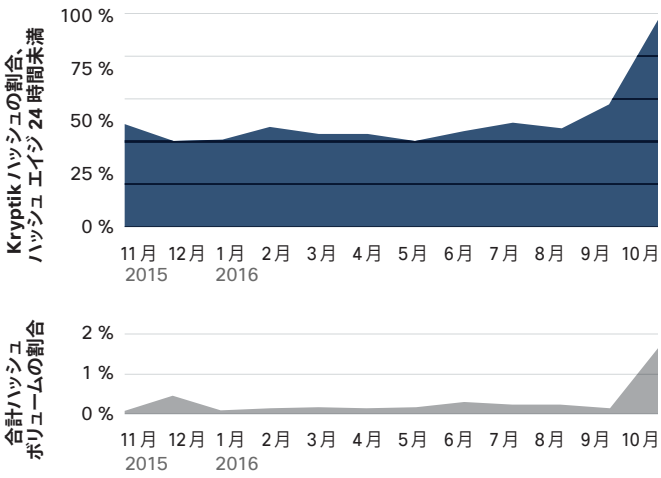


出典：シスコ セキュリティ リサーチ

6 つのマルウェア ファミリを分析することで、脅威が首尾よく活動できるわずかな時間を利用するために、攻撃者が戦術を頻繁に変更する必要があることが分かりました。これらの調整は、脅威を進化させた後にも防御者が既知のマルウェアを迅速に検出するようになってきていることを示します。攻撃者は、検出を回避し、活動を維持するための新しい方法を見出す必要に迫られています。

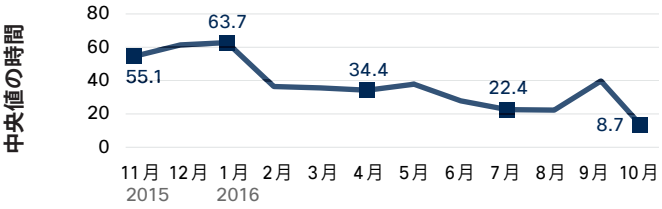
すべてのマルウェア ファミリが異なる振る舞いをする、この急速に進化する複雑な状況においては、人間の専門知識とポイントソリューションだけでは、脅威を迅速に特定して対処するのに十分ではありません。TTD の改善と感染時の迅速な修復には、脅威に関するリアルタイムの洞察を提供する統合セキュリティ アーキテクチャと自動検出および防御機能が不可欠です。

図 35 Kryptik マルウェア ファミリのハッシュ年齢と 1 ヵ月あたりに確認された全ハッシュ ボリュームの割合



出典：シスコ セキュリティ リサーチ

図 36 Kryptik マルウェア ファミリの TTD



出典：シスコ セキュリティ リサーチ

防御側の行動

防御側の行動

2016 年の脆弱性の減少

シスコの調査によると、2016 年の後半には、ベンダーが情報開示した脆弱性の数が 2015 年から大幅に減少しました（図 37）。National Vulnerability Database でも同様の減少が示されています。情報開示された脆弱性アドバイザリの減少の原因は、完全に明確にはなっていません。

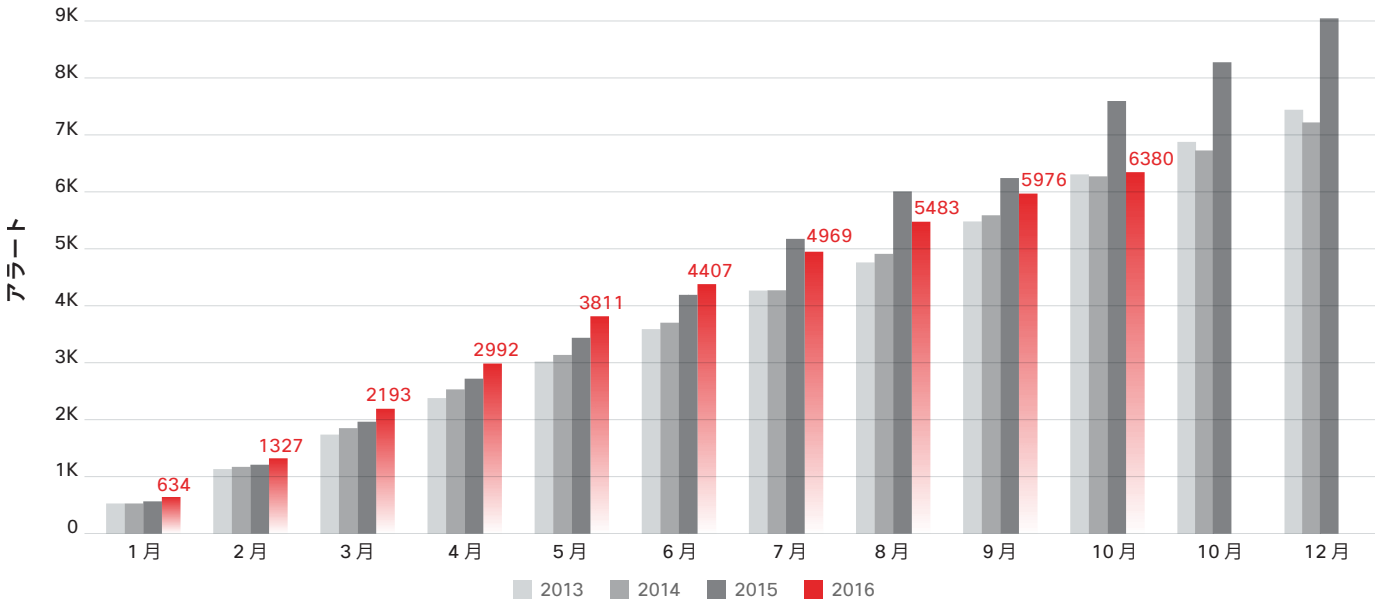
2015 年に脆弱性に関して、いつになく激しい動きがあったために 2016 年の数が脆弱性アドバイザリの通常のペースを反映している可能性には注意する必要があります。2015 年 1 月から 10 月 のアラートの総数は 7602 に達しました。2016 年の同じ期間では、アラートの総数が 6380 に達しています。2014 年のこの期間は、アラートの総数が 6272 でした。

2015 年の多数の脆弱性レポートは、ベンダーが既存の製品およびコードをより綿密に調べ、安全な開発ライフサイクル（SDL）をより慎重に導入し、脆弱性を特定して修正していたことを示す可能性があります。報告された脆弱性の減少は、こうした取り組みの効果が表れていることを示す可能性があります。つまり、ベンダーは、現在、製品を市場に投入する前に脆弱性を特定して修正することに重点を置きつつあるということです。

2016 年の Apple は、脆弱性が最も劇的に減少したことを示すベンダーでした。同社は、2015 年に 705 の脆弱性を報告し、2016 年に 324 の脆弱性を報告しました（54 % の減少）。同様に、シスコは 2015 年に 488 の脆弱性を報告し、2016 年に 310 の脆弱性を報告しました（36 % の減少）。

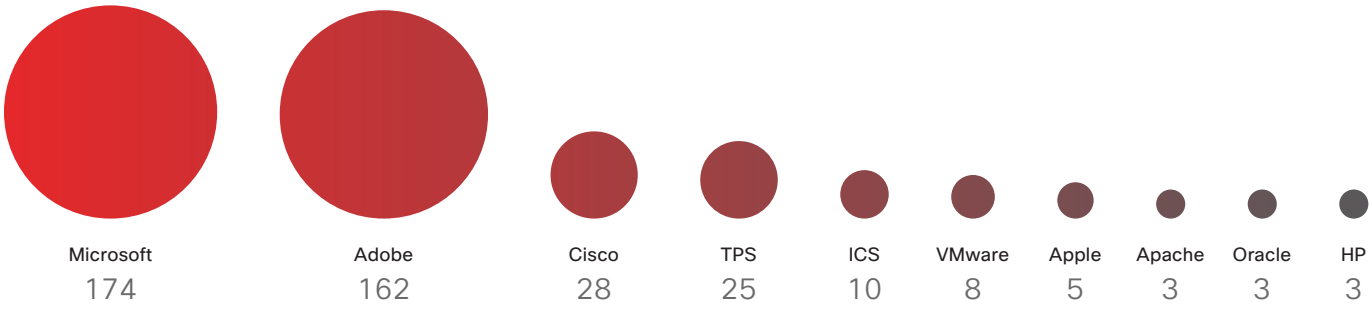
セキュリティ研究者の間での懸念事項は、セキュリティ プロフェッショナルの間に「脆弱性疲れ」が生まれているのではないかということです。この数ヵ月は、ハートブリードのために 2014 年に発生したような、業界全体に衝撃波を浴びせる重大な脆弱性の通知はありませんでした。実際、ハートブリードのような「名前付き」の脆弱性をめぐる過剰な騒動や 2015 年の脆弱性の増加は、多くの場合、疲労度を高め、少なくとも脆弱性の報告への関心を低下させます。

図 37 年間累積アラート総数



出典：シスコ セキュリティ リサーチ

図 38 ベンダーとタイプ別の重大な脆弱性に関する勧告



出典：National Vulnerability Database (NVD)

シスコは現在、「重大」、「高」、「中」、「低」のレベルで評価する重大度/影響評価（SIR）を使用しています。この評価は、共通脆弱性評価システム（CVSS）のスコアの簡素化された優先順位付けを反映しています。また、CVSS v2.0 の後続である CVSS v3.0 を採用しました。この変更により、一部の脆弱性は以前よりも高いスコアになることがあり、セキュリティ プロフェッショナルが「中」「低」ではなく「重大」「高」と評価される脆弱性がわずかに増加したと理解する可能性があります。このスコアの変更に関する詳細については、シスコ セキュリティのブログ投稿、セキュリティ脆弱性評価の進化：Sequel [英語] を参照してください。

「2017年シスコ セキュリティ機能ベンチマーク調査」（49 ページ）で、セキュリティ プロフェッショナルは、セキュリティ組織に関する同意のわずかな減少を示しました。この減少は、アップグレードやパッチを継続的に適用する必要性に関する「疲れ」に結びついている可能性があります。たとえば、セキュリティ対策を定期的に、形式的に、かつ戦略的に評価し、改善することに強い同意を示したセキュリティ プロフェッショナルは 2016 年には 53 % でしたが、2014 年と 2015 年は 56 % でした。

もちろん、脆弱性の減少によって、脅威の状況に関して自信過剰になることは禁物です。知名度の高い脆弱性がないとしても、脅威に対する警戒を解くべきではありません。

過去のレポートに示したように、セキュリティ プロフェッショナルは、パッチの優先順位付けに協力して取り組む必要があります。セキュリティ スタッフやその他のリソースが不足しているために、使用可能なすべてのパッチをすぐにインストールできない場合は、ネットワークの安全にとって最も重要なものを評価し、それらを優先的に適用してください。

2017 年版の図表はこちらからダウンロードしてください：
www.cisco.com/go/acr2017graphics

図 39 重大な脆弱性に指定された勧告の例

アドバイザリ タイトル	発行日
Adobe Acrobat および Acrobat Reader のメモリ破損コード実行の脆弱性	2016 年 7 月 28 日
Adobe Acrobat および Acrobat Reader のメモリ破損リモート コード実行の脆弱性	2016 年 7 月 28 日
Adobe Acrobat および Acrobat Reader のメモリ破損の脆弱性	2016 年 7 月 21 日
Adobe Acrobat および Acrobat Reader の整数オーバーフローの脆弱性	2016 年 5 月 23 日
Adobe Acrobat および Acrobat Reader のメモリ破損リモート コード実行の脆弱性	2016 年 2 月 08 日
Adobe Acrobat および Acrobat Reader のメモリ破損の脆弱性	2016 年 7 月 28 日
Adobe Acrobat および Acrobat Reader のメモリ破損の脆弱性	2016 年 7 月 18 日
Adobe Acrobat および Acrobat Reader のメモリ破損の脆弱性	2016 年 6 月 23 日
Adobe Acrobat および Acrobat Reader のメモリ破損の脆弱性	2016 年 5 月 24 日
Adobe Acrobat および Acrobat Reader のメモリ破損の脆弱性	2016 年 5 月 23 日

出典：シスコ セキュリティ リサーチ

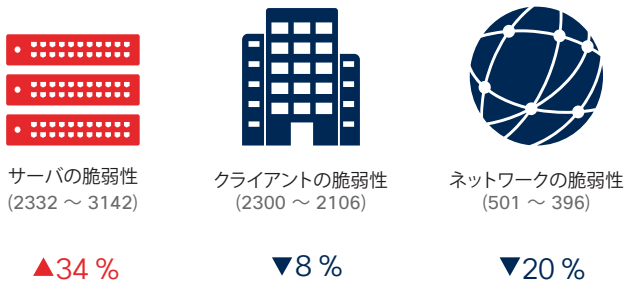
上記の勧告は、2016 年に重大と評価された脆弱性であり、複数のソースからエクスプロイト コードが公開されていることや、現場でアクティブに開発されていることが報告されています。

サーバとクライアントの脆弱性

『*Cisco 2016 Midyear Cybersecurity Report*』に示されているように、攻撃者は、サーバ側のソリューション内で活動するための時間帯と場所を探しています。サーバ ソフトウェア内で攻撃を開始することにより、より多くのネットワーク リソースを制御できたり、他の重要なソリューション間で水平移動できたりする可能性が生まれます。

シスコの研究者は、クライアントとサーバの脆弱性をベンダーごとに追跡しました（図 40）。

図 40 クライアント/サーバの脆弱性の内訳、2015 年～2016 年



出典：National Vulnerability Database

ミドルウェア：攻撃者はパッチ未適用のソフトウェアを狙っている

『*Cisco 2016 Midyear Cybersecurity Report*』では、サーバ側のシステムへの攻撃に関するデータを共有しました。2017 年に、防御側の対応や脅威の認識が遅れる場所を探し求める攻撃者の注意を引くのは、プラットフォームやアプリケーションを接続するミドルウェアと考えられます。

シスコの研究者は、サードパーティ製ソフトウェアの脆弱性を調べているときに、それらのソフトウェアで月平均 14 の新しい脆弱性を発見しました。これらの62にもおよぶ脆弱性は、ミドルウェアの使用によるものと考えられました。62 の脆弱性のうち、20 は PDF を処理するコード内で、12 は画像を処理するコード内、10 は一般的なオフィス生産性ソリューションのコード内、9 つは圧縮用のコード内、11 はその他のライブラリ内でそれぞれ発見されました（図 41）。

ミドルウェアのライブラリは、より顧客に近いソフトウェア、つまりユーザが日常的に直接操作するソフトウエアのように迅速に更新されることはないため、セキュリティに対する固有の脅威をもたらします。ミドルウェア ライブラリはソフトウェア監査の対象外になっている場合があり、そのために脆弱性が残されている可能性があります。

図 41 ミドルウェア ライブラリで見つかった脆弱性

出典：シスコ セキュリティ リサーチ

組織は、ミドルウェアが安全であることは運にまかせて、人目を引くソリューションの更新により大きな関心を置いているようです。攻撃者は人目を引かない経路からネットワークに侵入しようとはしないだろうという想定は、間違いである可能性があります。このようにミドルウェアは、防御者のセキュリティ上の盲点となっており、攻撃者に攻撃の機会を与えています。

多くのミドルウェア ソリューションはオープン ソース開発者から提供されるものであるため、ミドルウェア ライブラリの更新の課題はオープンソース ソフトウェアの問題（『*Cisco 2015 Midyear Security Report*』を参照）に密接に関係しています（ただし、目下の問題は、オープン ソースと独自規格の両方のミドルウェア開発者に影響を与える可能性があります）。このため、ミドルウェア ライブラリは、それらの更新された状態を維持する多くの開発者に依存している場合があります。酷使されている IT またはセキュリティ チームが管理する必要のあるタスクのリストでは、ミドルウェア ライブラリの更新が最優先事項になっていないかもしれませんが、もっと注意を向ける必要があります。

ミドルウェアの脆弱性がもたらす、攻撃者に悪用されかねない潜在的な影響とはどのようなものでしょうか。ミドルウェアとその他の重要なシステム（電子メール、メッセージングなど）が接続されていることを考えると、攻撃者は、これらのシステムを水平移動し、フィッシング メッセージやスパムを送信することができます。あるいは、攻撃者は、認可されたユーザになりすまし、ユーザ間の信頼関係を悪用して、さらなるアクセスを可能にすることができます。

ミドルウェアの脆弱性を通じて開始される攻撃の被害者にならないために、以下のことが必要です。

- 使用するアプリケーションの既知の依存関係とライブラリのリストを積極的に維持する。
- それらのアプリケーションのセキュリティを積極的にモニタし、リスクをできるだけ軽減する。
- ソフトウェア ベンダーとの契約に、パッチを迅速に適用するためのサービス レベル契約を含める。
- ソフトウェアの依存関係とライブラリの使用を定期的に監査し、確認する。
- 製品の保守およびテストの方法の詳細をベンダーに問い合わせる。

パッチ適用のわずかな遅れが、攻撃者の活動の余地を増やし、重要なシステムの制御を奪取するために使用できる時間を増やします。次のセクションでは、Web ブラウザなどの一般的なソリューションへのパッチ適用の影響と動向について説明します。

パッチ適用時間：リカバリ時間枠を短縮する

多くのユーザは、パッチのダウンロードとインストールを迅速に行ってはいません。攻撃者は、ネットワークに侵入するために、これらのパッチ未適用の脆弱性を利用します。シスコの最新の調査により、ユーザにパッチのダウンロードおよびインストールを促す鍵が、ベンダーからのソフトウェア アップデートのパターンにある可能性が浮上しました。

セキュリティ パッチのリリースは、攻撃者に、悪用する価値がある脆弱性の存在を明確に示します。高度な攻撃者は、多くの場合、しばらくすればそれらの脆弱性を発見して利用するでしょうが、それ以外の大多数の攻撃者にとっては、パッチの通知が旧バージョン攻撃の解禁日となります。

ソフトウェア ベンダーが定期的なスケジュールで新しいバージョンをリリースすれば、ユーザもアップデートをダウンロードおよびインストールするように条件付けられます。逆に、ベンダーのアップグレード リリースが不規則だと、ユーザがそれらをインストールする可能性が低下します。そして、悪用可能な脆弱性を持つ古いソリューションを使用し続けます。

アップグレードのサイクルに影響を与えるその他の行動には、以下のものがあります。

- リマインダの通知がどの程度業務に支障をきたすか。
- オプトアウトがどの程度容易であるか。
- ソフトウェアの使用がどの程度の頻度か。

ベンダーによってアップグレードがリリースされたときにユーザがインストールする可能性の高い時間帯は、一定ではありません。シスコの研究者は、顧客が使用するエンドポイントへのソフトウェアのインストールについて調べました。ソフトウェアは次の 3 つのカテゴリに分類されました。

- **最新のバージョン：**エンドポイントで実行されているソフトウェアは、利用可能な最新バージョンだった。
- **最近のバージョン：**エンドポイントで実行されているソフトウェアは、最新ではないが、直近の 3 つのバージョンのいずれかだった。
- **古いバージョン：**エンドポイントで実行されているソフトウェアは、最新バージョンの 4 つ前もしくはそれよりも古いバージョンだった。

たとえば、2017 年 1 月 1 日にソフトウェア ベンダーがバージョン 28 をリリースした場合、バージョン 28 は「最新のバージョン」であり、バージョン 26 は「最近のバージョン」であり、バージョン 23 は「古いバージョン」です（次ページの図には、ソフトウェアの 1 つ以上のバージョンがリリースされる毎週の時間帯のコールアウトが示されています）。

Adobe Flash のユーザの調査（図 42）では、更新リリースの最初の週にユーザの約 80 % がソフトウェアの最新バージョンをインストールしていることが分かりました。つまり、ユーザの大半が最新バージョンに更新するまでに約 1 週間しかかかっていません。この 1 週間の「リカバリ」期間が、ハッカーの攻撃の機会を表します。

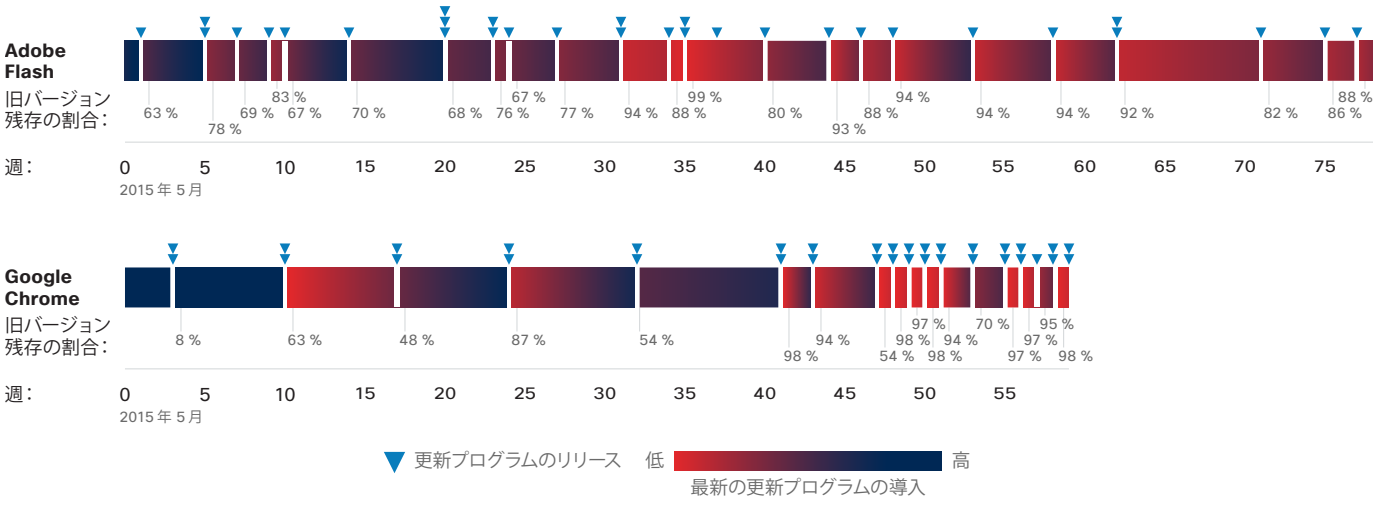
Adobe Flash グラフィックで最近の 2015 年第 4 四半期を参照すると、最新バージョンのユーザ数の急激な減少が見て取れます。調査対象となった期間中、Adobe は、機能の追加、バグ修正、セキュリティ アップデートを同時に含む 5 つのバージョンの Flash を次々にリリースしました。このような相次ぐ更新は、ユーザを混乱させる可能性があります。ユーザは、これほど多くの更新プログラムをダウンロードする必要があるかどうか疑問に感じるかもしれません。多数のアップグレード通知にうんざりしている可能性があります。また、すでに重要な更新はダウンロード済みであると考えて、新しい通知を無視するおそれもあります。更新のインストールに対する関心の欠如は、その理由が何であれ、防御者にとって不利な材料となります。

Google Chrome Web ブラウザの試験アップグレードでは、異なるパターンが認められます。同アップグレードには、定期的なアップグレード パターンと、更新通知を無視しにくくする厳格なオプトアウト ポリシーが適用されます。図 42 に示されているとおり、最新バージョンを実行するエンドポイントは、数週間にもわたって比較的一定に保たれています。

Chrome のデータは、ユーザが比較的迅速に更新を適用していることを示しています。定期更新の場合、リカバリのタイムラインはおよそ 1 週間です。しかしながら、2016 年第 2 四半期から第 3 四半期に及ぶ 9 週間の期間には、7 回の更新がありました。この期間中、ユーザは更新を適用していましたが、更新疲れが見られるようになりました。大多数は更新しているものの、古いバージョンを使用し続けるユーザの割合が着実に増加しました。

Mozilla Firefox ブラウザは、定期的なスケジュールでの更新を提供しますが、更新リリース後のリカバリ期間は 1 ヵ月ほどかかるようです。つまり、Firefox ユーザは、Chrome ユーザほど頻繁に更新をダウンロードしインストールしていません。その理由の 1 つは、一部のユーザが、Firefox ブラウザを日常的に使用していないために、更新通知を目にしてダウンロードする機会がない可能性があることです（次のページの図 43 を参照してください）。

図 42 Adobe Flash および Google Chrome のパッチ適用時間



出典：シスコ セキュリティ リサーチ

Firefox は、ほぼ隔週で更新されており、調査期間中に更新の頻度が増加していることがわかりました。頻度の増加は、母集団内で古いバージョンの Firefox が増加したことを反映しています。リカバリ期間はおよそ 1.5 週間ですが、この期間はオーバーラップしています。最新の状態を維持しようとするユーザの数は、ユーザ ベースのわずか 30 パーセントまで低下しています。いくつかの時点では、ユーザの 3 分の 2 が、最新バージョンよりも 4 バージョン前のブラウザを依然として使用し続けています。そのため、Firefox が問題に迅速に対処して、バグを修正しているにもかかわらず、ユーザ ベースが同じ頻度で更新および再起動することはありません。

ソフトウェアの場合、その使用レベルも、脆弱性の指標の 1 つと思われます。ユーザがソフトウェアに頻繁にアクセスしないために、パッチやアップグレードを適用する必要に気付かない場合、見過ごされたソフトウェアにより、攻撃者が活動する空間的また時間的な隙が生じます。

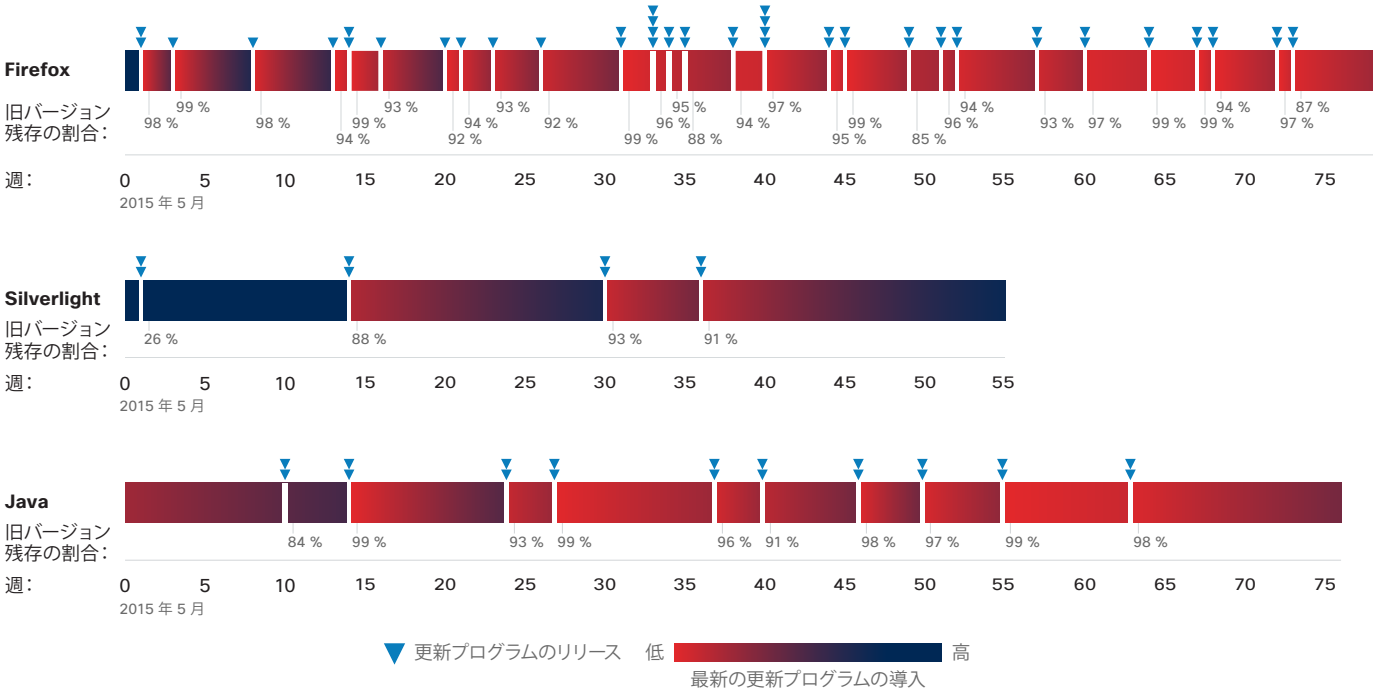
その点が Microsoft Silverlight を対象とする調査で明らかになりました。調査は、リリース後にユーザがアップグレードをインストールするまでのリカバリ期間が 2 ヵ月にも及ぶことを示しています。ある時点で、5 週間の間に 2 回のリリースがあり、3 ヵ月以上にわたってユーザ数に影響を及ぼしました。その影響は、2015 年第 4 四半期から 2016 年第 1 四半期の期間に観察することができます。

Microsoft は、2012 年に Silverlight のサポート終了を通知しましたが、パッチおよびバグ修正のリリースは継続中です。とはいえ、Internet Explorer の場合と同様、古くなったパッチ未適用のソフトウェアは、攻撃者に容易に悪用されるおそれがあるという問題が発生しています。

Java ユーザのリカバリ期間は、大多数が最新のリリースよりも 1 バージョンから 3 バージョン前のソフトウェアを実行していることを示しています。リカバリにかかる時間は約 3 週間です。Java の場合の特異なパターンは、最近のバージョンを使用するユーザが大勢を占めているということです。Java の更新周期は 1 ヵ月から 2 ヵ月です。

パッチ適用までの時間周期から学べる全般的な教訓は、アップグレード リリースのパターンは、ユーザのセキュリティ ポスチャの一要因であり、ネットワークを危険にさらす可能性があるということです。

図 43 Firefox、Silverlight および Java のパッチ適用時間



出典：シスコ セキュリティ リサーチ

2017 年版の図表はこちらからダウンロードしてください：**www.cisco.com/go/acr2017graphics**

2017 年シスコ セキュリティ機能ベンチマーク調査

2017 年シスコ セキュリティ機能ベンチマーク調査

自らの組織におけるセキュリティの状態に関するセキュリティ プロフェッショナルの見解を評価するため、シスコは、幾つかの国で、さまざまな規模の組織のセキュリティ最高責任者（CSO）とセキュリティ運用（SecOps）マネージャに、組織のセキュリティ リソースおよび手順についての見解を尋ねました。『2017 年シスコ セキュリティ機能ベンチマーク調査』は、現在使用中のセキュリティ対策およびセキュリティ慣行の成熟度に対する洞察を提供し、2016 年および 2015 年のレポートにおける結果との比較を行います。この調査は 13 ヵ国で実施され、2900 名から回答が得られました。

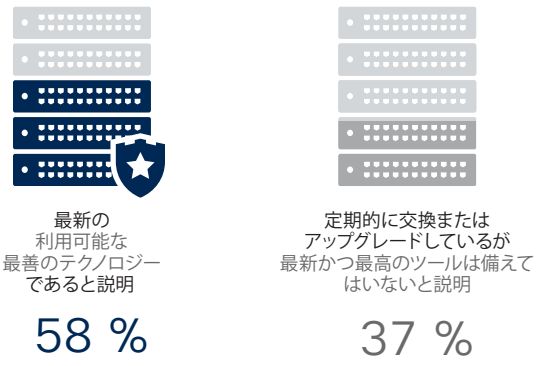
セキュリティ プロフェッショナルは、組織のセキュリティを向上させたいと願っていますが、その方法は、攻撃者の複雑な状況と、活動領域を広げようとする敵の試みに応じたものである必要があります。多くの組織は、多くのベンダーによる多くのソリューションに依存しています。この手法により、速度、接続されるデバイス、トラフィックの面でインターネットが成長を続けるにつれて、ネットワーク保護の複雑さと混乱が増大する結果になっています。組織は、自らを守ることを願うなら、簡潔さと統合を目標とする必要があります。

見解：セキュリティ プロフェッショナルはツールを信頼しているが、それらを効果的に使用しているという確信がない

ほとんどのセキュリティ プロフェッショナルは、適切なソリューションを手にしており、組織のセキュリティ インフラは最新であると考えています。しかしながら、調査によると、この信頼感にはいくらかの不安が伴っています。これらのプロフェッショナルは、手にしているテクノロジーを本当の意味で正しく利用するための予算と知識を常に獲得できるとは限りません。

組織に対する脅威はあらゆる方面で生じます。敵は抜け目がなく独創的であり、防御の裏をかくことができます。このような、身を引き締めねばならない環境においても、セキュリティ プロフェッショナルの大部分は組織のセキュリティ インフラは最新であると自負しています。とはいえ、その自身は数年前に比べると揺らぎつつあるようです。2016 年には、回答者の 58 パーセントが、組織のセキュリティ インフラは最新で、最新のテクノロジーで常にアップグレードされていると語りました。また 37 パーセントは、セキュリティ テクノロジーを定期的に置き換えまたはアップグレードしているものの、最新かつ最高のツールを備えてはいないと述べています（図 44）。

図 44 セキュリティ インフラストラクチャが最新であると考えるセキュリティ プロフェッショナルの割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

さらに、セキュリティ プロフェッショナルの 3 分の 2 超は、組織のセキュリティ ツールが非常に有効または極めて有効と感じています。たとえば、74 パーセントは、既知のセキュリティに対する脅威のブロックに、組織のツールが非常に有効または極めて有効と考えており、71 パーセントは、ネットワーク異常の検出と適応型脅威の変化に対する動的な防御に、組織のツールが有効と考えています（図 45）。

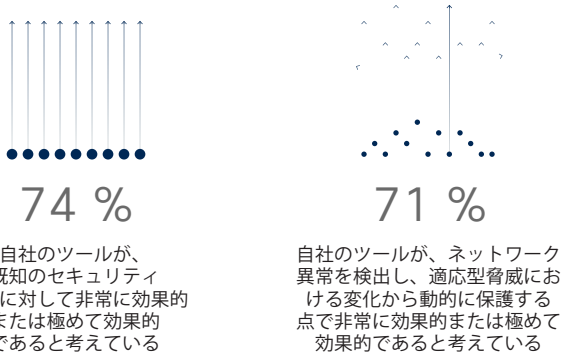
問題となるのは、ツールに対する確信が、有効なセキュリティに必ずしも結び付くとは限らないことです。調査結果が示すように、セキュリティ部門は、多くのベンダーからの複雑なツールや、人材不足に悩まされています。要約すると、この状況は「意図と現実の対立」の問題ということになります。セキュリティ プロフェッショナルは、簡潔で有効なセキュリティ ツールを必要としていますが、このビジョンの実現に必要な統合的アプローチをもっていません。

セキュリティは、依然として多くの組織の首脳陣の最優先課題です。さらにセキュリティ プロフェッショナルは、エグゼクティブ チームがセキュリティを組織の主要な目標のリストの上位に置いていると考えています。当然ながら、課題となるのは、エグゼクティブのサポートを、セキュリティに関する成果に影響を及ぼし得る人材およびテクノロジーに見合ったものとすることです。

エグゼクティブ リーダーがセキュリティを最優先課題としていることを明確に肯定するセキュリティ プロフェッショナルの数は、2016 年には 59 パーセントでしたが、2015 年の 61 パーセント、2014 年の 63 パーセントから若干減少しました（図 46）。2016 年、55 パーセントのセキュリティ プロフェッショナルが、セキュリティ上の権限と責任が組織のエグゼクティブ チーム内で明確にされていることを認めました。2015 年および 2014 年には 58 パーセントが肯定しています。

つまり、セキュリティ プロフェッショナルは、利用可能なツールを信頼しており、セキュリティ問題への対処に当たって、企業のリーダーに話を聞いてもらえているように見えます。しかしながら、その信頼感はいくらか弱まりつつあります。セキュリティ プロフェッショナルは、攻撃者が成功を収めており、拡大を続ける攻撃対象の管理が困難であると感じ始めています。

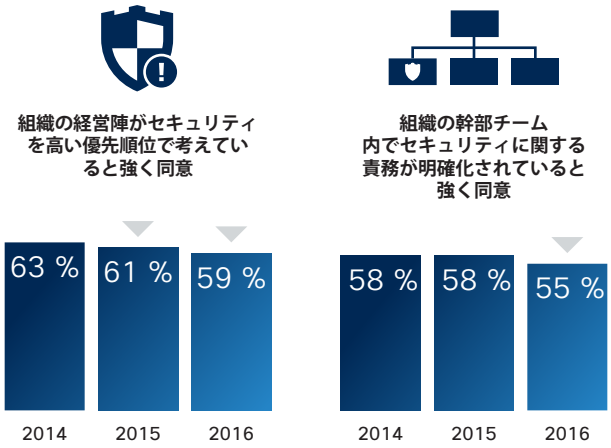
図 45 さまざまなセキュリティ ツールが非常に効果的であると認識しているセキュリティ プロフェッショナルの割合



2016 (n=2912)

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 46 エグゼクティブ レベルでセキュリティの優先順位が高いと考えるセキュリティ プロフェッショナルの割合、2014 年～2016 年



2014 (n=1738)、2015 (n=2432)、2016 (n=2912)

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

シェアする

制約：時間、人材、予算が脅威への対応能力に影響を及ぼす

セキュリティ プロフェッショナルが、脅威を検出し、被害を軽減するのに必要なツールを備えているとある程度確信している場合でも、特定の構造的制約が目標達成の妨げになることも認識しています。予算的な制約は常に頭を悩ます問題です。とはいえ、有効なセキュリティに対する他の制約は、セキュリティの簡素化および自動化の問題と関連しています。

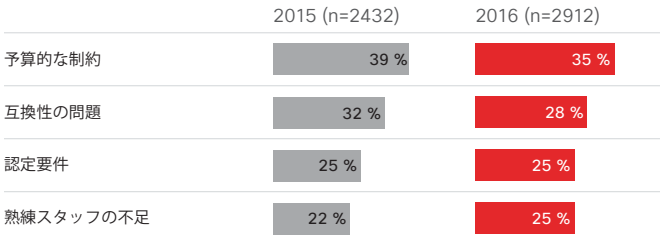
2016 年、図 47 に示すとおり、セキュリティ プロフェッショナルの 35 パーセントが、高度なセキュリティ プロセス採用に対する最大の障害は予算であると述べています（39 パーセントが第 1 の障害は予算であると述べた 2015 年からわずかに減少）。2015 年には、レガシー システムとの互換性の問題が、2 番目に大きな共通の障害でした。2016 年には 28 パーセントが互換性を挙げており、2015 年には 32 パーセントでした。

予算は問題の一部にすぎません。たとえば、互換性の問題は、統合されていない分断されたシステムの問題と関連しています。また、熟練スタッフの不足は、ツールは備えているものの、セキュリティ環境で生じている事柄を本当に理解している人材がいないという問題を表しています。

標的型攻撃と敵の戦略の変化に対抗するために必要な専門知識と決断力を考慮すると、人材の確保は重要な課題です。十分にリソースを与えられた、熟練した IT セキュリティ チームは、適切なツールと相まって、テクノロジーとポリシーを連動させ、より優れたセキュリティ上の成果を上げることを可能にします。

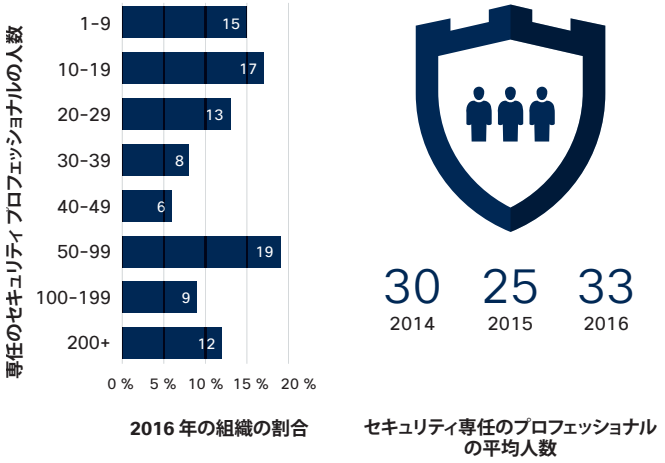
調査対象の組織に属するセキュリティ プロフェッショナル数の中央値は 33 名で、2015 年には 25 名でした。2016 年には、組織の 19 パーセントは 50 名から 99 名の専任セキュリティ プロフェッショナルを擁し、9 パーセントが 100 名から 199 名、また 12 パーセントが 200 名以上のセキュリティ プロフェッショナルを擁しています（図 48）。

図 47 セキュリティの最大の障害



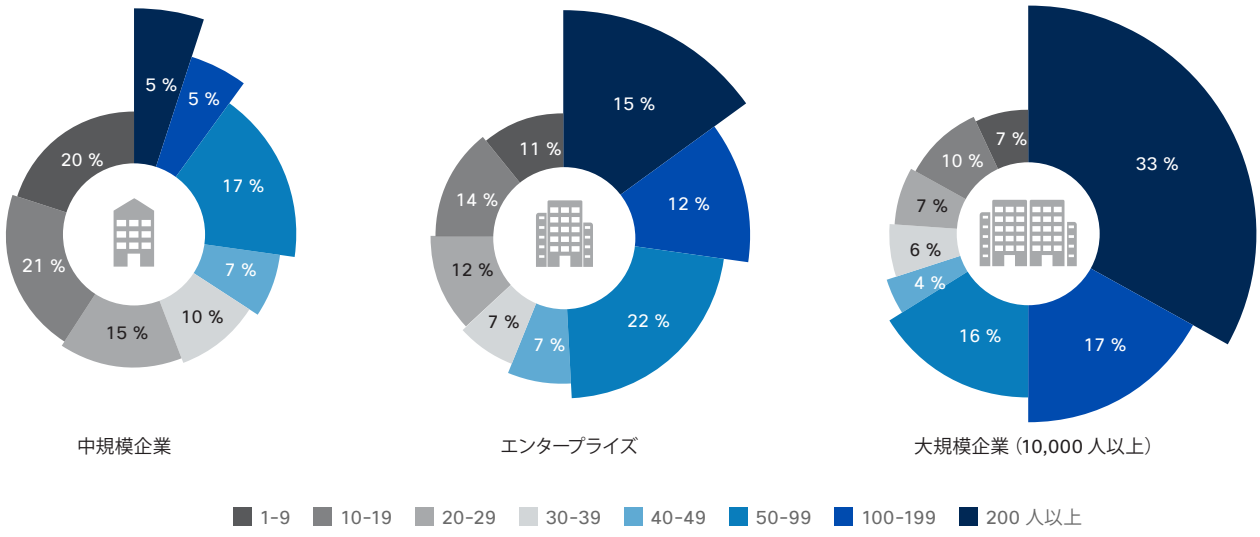
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 48 組織に採用されているセキュリティ プロフェッショナルの人数



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 49 組織の規模別のセキュリティ プロフェッショナルの人数



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

セキュリティ プロフェッショナルの数は、組織の規模によって異なります。図 49 に示されているとおり、従業員数 10,000 名を超える大企業の 33 パーセントは、少なくとも 200 名のセキュリティ担当社員を擁しています。

どのような制約がある場合でも、セキュリティ プロフェッショナルは、今後現れる脅威への対処にとってどのような要素が妨げとなるかについて、検討する必要があります。

たとえば、予算については、どのくらいあれば十分でしょうか。調査の回答者が説明しているとおり、セキュリティ チームは、IT 環境の範囲内であっても、企業のその他多くの優先事項と競合しなければなりません。ツールを増やすための資金を確保できなければ、与えられている予算を一層有効活用する必要があります。たとえば、限られた人員数を埋め合わせるために自動化を活用できます。

ソフトウェアおよびハードウェアの互換性の問題についても、同様の質問を投げかける必要があります。互換性の問題が増える中、その多くが有効に機能していない可能性のあるさまざまなバージョンのソフトウェアとハードウェアをどれほど多く管理しなければならないのでしょう。またセキュリティ チームは、複数の認定要件をどのように維持すればよいでしょうか。

アウトソーシングとクラウドが予算拡大につながる

ベンチマーク調査に参加している多くのセキュリティ プロフェッショナルは、セキュリティ製品の購入時に資金不足を実感していました。彼らは一部のタスクをアウトソーシングしたり、クラウド ソリューションを使用することで予算を拡大しました。自動化も導入しました。

これらの制限を別として、セキュリティ プロフェッショナルは、セキュリティ運用を以前よりも重視しなくなっています。この傾向は、セキュリティ プロフェッショナルが最適ではないセキュリティ インフラストラクチャを構築してしまうという問題を発生させる可能性があります。セキュリティ運用に力点を置かなくなることは、拡大する攻撃対象を防御する備えが組織にないことを示している可能性があります。

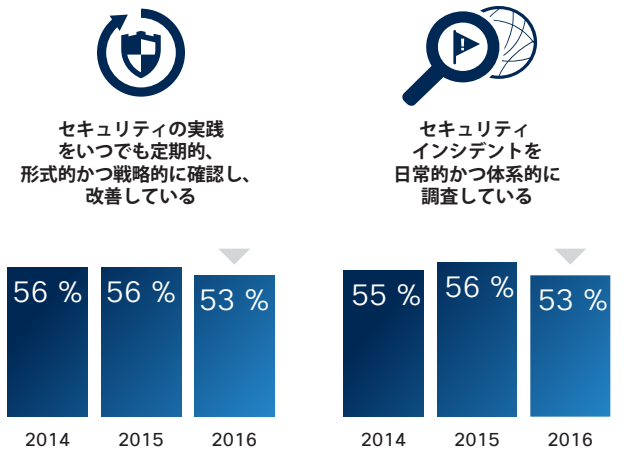
たとえば、2016 年に、回答者の 53 パーセントは、セキュリティ対策を定期的、形式的、戦略的に確認し改善していることを明確に肯定しました。2014 年および 2015 年には、56 パーセントが明確に肯定しています。同様に、2016 年には、53 パーセントが、セキュリティ インシデントを定期的かつ体系的に調査していることを明確に肯定しており、2014 年には 55 パーセントが、2015 年には 56 パーセントが肯定しています（図 50）。

セキュリティ プロフェッショナルが、セキュリティを活用する目標を達成し損なっている場合、保有するツールを有効に展開できないとしても不思議ではなく、新しいツールの追加についてはなおさらです。調査の回答者が語ったとおり、すでに手にしているテクノロジーを活用できていない場合、セキュリティ プロセスを自動化する一層簡潔で合理化されたツールが必要です。さらに、そのようなツールは、ネットワーク環境で生じている事柄の全体的な状況を示すものである必要があります。

セキュリティにおける統合の欠如により、悪意ある人物が攻撃を仕掛ける時間的また空間的な隙が生じる可能性があります。セキュリティ プロフェッショナルが多くのベンダーのソリューションやプラットフォームを同時に処理しようとする傾向は、シームレスな防御の構築を複雑なものにしかねません。図 51 に示されているとおり、大多数の企業は、自社の環境の中で、6 社を超えるセキュリティ ベンダーと、6 つを超えるセキュリティ製品を使用しています。セキュリティ プロフェッショナルの 55 パーセントは少なくとも 6 社のベンダーを使用しており、45 パーセントは 1 社から 5 社のベンダーを使用し、65 パーセントは 6 つ以上の製品を使用しています。

2017 年版の図表はこちらからダウンロードしてください：
www.cisco.com/go/acr2017graphics

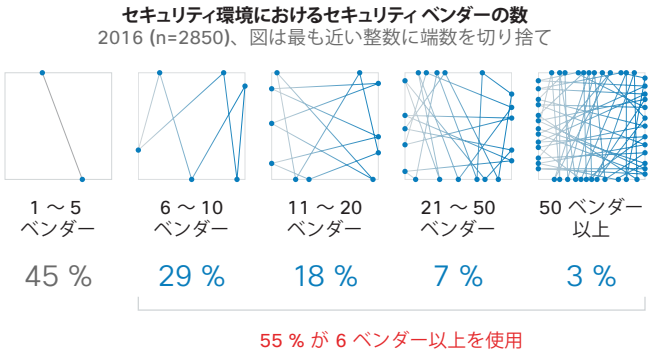
図 50 セキュリティ オペレーション運用の説明に強く同意した回答者の割合

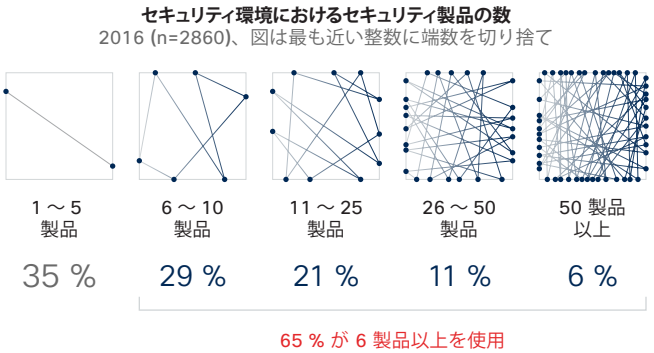


2014 (n=1738)、2015 (n=2432)、2016 (n=2912)

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

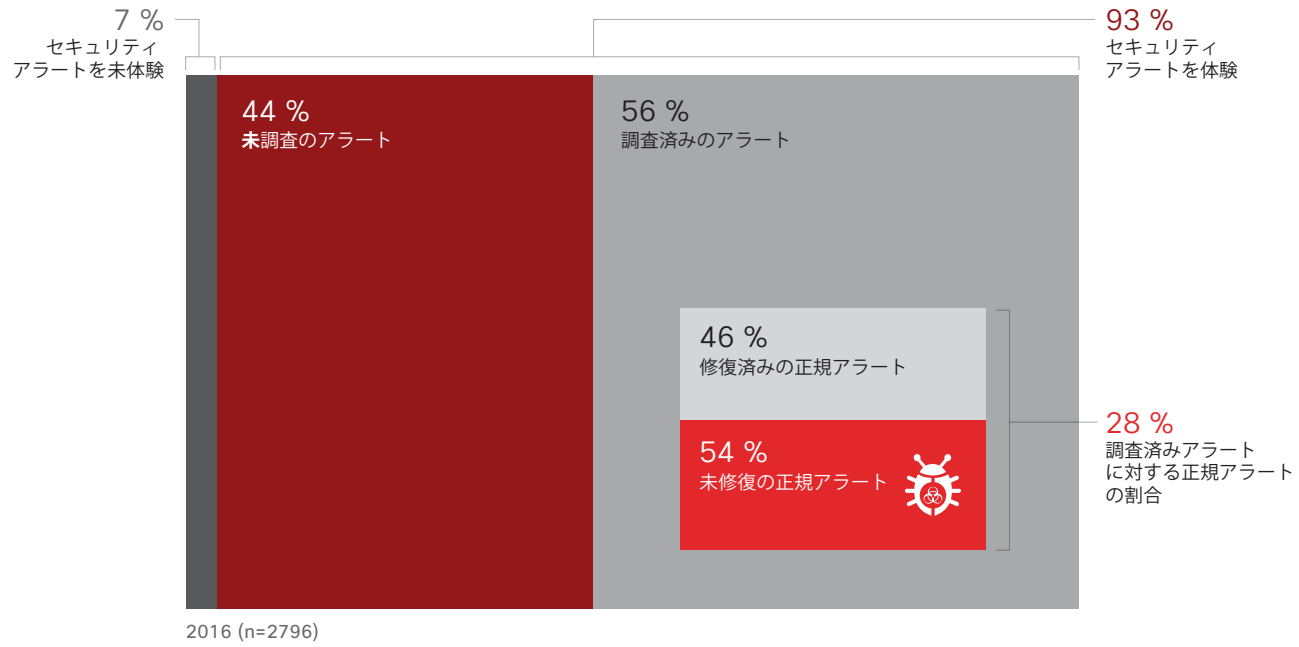
図 51 組織が利用するセキュリティ ベンダーと製品の数





出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 52 調査または修正が実施されないセキュリティ アラートの割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

操作運用に関する目標を達成し損ない、ツールが最大限有効に活用されず、人員数が十分ではない場合、セキュリティは弱体化します。セキュリティ プロフェッショナルは、どのアラートが重大で、なぜ発生しているのかを判断するための人材、ツール、自動化ソリューションがないというだけの理由で、アラートの調査を割愛せざるを得ません。

おそらく、統合型防御システムがない、またはスタッフに時間がないといったいくつかの要因で、組織は、特定の日に受信するセキュリティ アラートの半数をやや超える調査を行えるにすぎません。図 52 に示されているとおり、アラートの 56 パーセントが調査され、44 パーセントは調査されません。調査されたアラートの 28 パーセントは正規のアラートだと考えられます。正規のアラートの 46 パーセントは、その後修復されています。

具体的な例を挙げると、1 つの組織が 1 日につき 5000 のアラートを記録するとします。その場合、

- 2800 のアラート（56 パーセント）が調査され、2200（44パーセント）は調査されないことになります。
- 調査されたアラートのうち、784 のアラート（28 パーセント）は本物で、2016（72 パーセント）は本物ではありません。
- 本物のアラートのうち、360（46 パーセント）は修復され、424（54 パーセント）は修復されません。

アラートの約半分が調査されないという事実は、不安の原因となるに違いありません。修復されない一群のアラートには何が含まれるのでしょうか。迷惑メールを広めるだけの低レベルの脅威でしょうか。あるいは、ランサムウェア攻撃やネットワークの停止を引き起こすのでしょうか。脅威に関する状況をよく広く調査し理解するため、組織は、自動化や、正しく統合されたソリューションを利用する必要があります。自動化は、貴重なリソースを最大限活用し、検出や調査の重荷からセキュリティ チームを解放するのに役立ちます。

あまりに多くのアラートを確認できない場合、アラートが組織の全体的な成功に及ぼす影響についての疑問が生じます。調査されないそのような脅威は、企業の生産性、顧客満足度、信頼性にどのような影響を与えるでしょうか。回答者が語ったとおり、小規模なネットワーク停止やセキュリティ侵害は、損益に長期的な影響を及ぼす可能性があります。損失が比較的小さく、影響を受けたシステムを特定し隔離することが容易な場合でも、セキュリティ リーダーは、組織に与えたストレスのために、侵害を重大なものと見なします。

シェアする

ストレスは、多くの点で組織に影響を及ぼします。セキュリティ チームは、セキュリティ侵害の後に生じるネットワーク停止の管理に時間を割かなければなりません。そのような停止のおよそ半数は、8 時間ほども長く継続しました。停止の 45 パーセントは、1 時間から 8 時間継続しました（図 53）。15 パーセントは 9 時間から 16 時間、11 パーセントは 17 時間から 24 時間継続しています。停止の 41 パーセントは、組織のシステムのうち 11 パーセントから 30 パーセントに影響を及ぼしました。

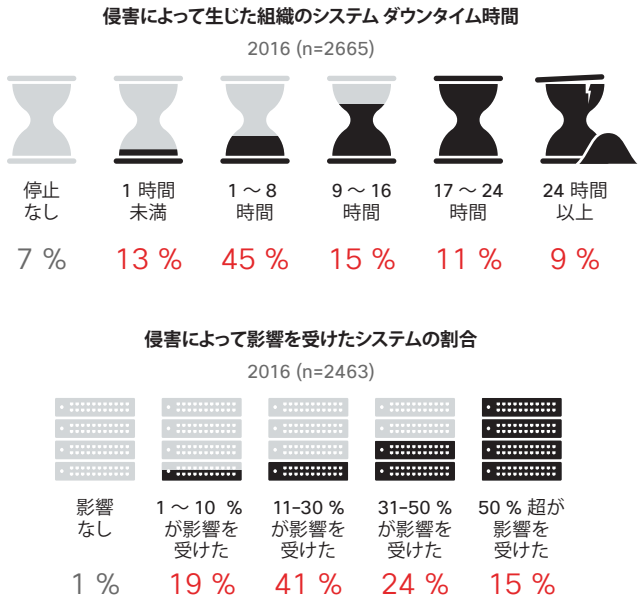
影響：より多くの組織が侵害による損失を経験している

侵害の影響は停止に限定されません。侵害は、経費、時間、レピュテーションの損失をも生じさせます。この打撃を回避できると考えるセキュリティ チームは、データの現実を無視しています。シスコの調査が示すとおり、組織の約半数は、セキュリティ侵害の後、風評被害への対策を迫られました。攻撃者の能力と戦術の範囲を考えると、問題は、セキュリティ侵害が発生するかどうかではなく、いつ発生するかです。

ベンチマーク調査が示すとおり、侵害が発生すると、セキュリティ プロフェッショナルは不愉快な現実に直面することとなります。往々にして、セキュリティ戦略が変更され、防御が強化されます。攻撃者によるネットワーク侵害を受けたことがない組織は、被害を免れたことで安心するかもしれません。しかしながら、その安心感はおそらく誤っています。

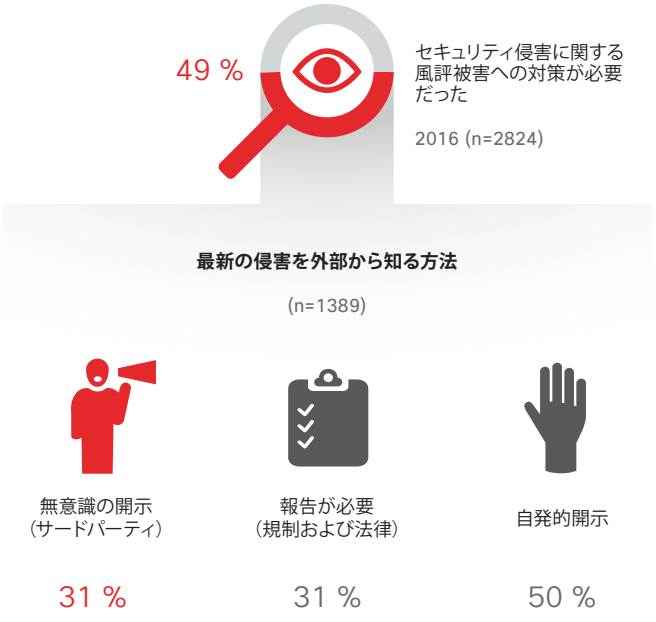
調査対象となったセキュリティ プロフェッショナルの 49 パーセントが、セキュリティ侵害に関する風評被害への対策を迫られたと述べています。これらの組織のうち、49 パーセントは自発的に侵害について情報開示しましたが、31 パーセントは開示情報をサードパーティが作成したと述べました（図 54）。つまり、調査対象となった企業の約 3 分の 1 は、侵害についての自発的ではない情報開示に対応せざるを得なかったことになります。目立たないように侵害に対処できた時代は、とうの昔に過ぎ去ったことは明らかです。膨大な数の規制機関、メディア、ソーシャル メディアのユーザが、ニュースを暴露しようと待ち構えています。

図 53 セキュリティ侵害によるサービス停止の長さと範囲



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 54 公共のセキュリティ侵害を経験した組織の割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 55　公となったセキュリティ侵害によって影響を受ける可能性が最も高い職務

出典：シスコ セキュリティ リサーチ

組織にもたらされる損害は、侵害やサービス停止の回復にかかる時間をはるかに上回ります。その影響は甚大であり、企業が最大限努力して回避すべきものです。

図 55 に示されているとおり、セキュリティ プロフェッショナルの 36 パーセントは、最も影響を受けるのは、業務部門であると述べています。これは、運輸から医療、製造に至る業界に影響を及ぼす生産性のコア システムの機能が低下したり、さらには停止することを意味します。

業務部門に次いで、財務部門は、最も影響を受けやすい職務であり（回答者の 30 パーセントが言及）、ブランドへの評価と顧客維持がそれに続きます（両方が 26 パーセント）。

成長し成功を収めることを目指しながら、重要な部門がセキュリティ侵害の影響を受けることを望む組織はありません。セキュリティ プロフェッショナルは調査結果を確認し、自分の組織も侵害による同種の損失を被っていないか、また、そうした損害を将来的に被る可能性について、自らに問いただす必要があります。

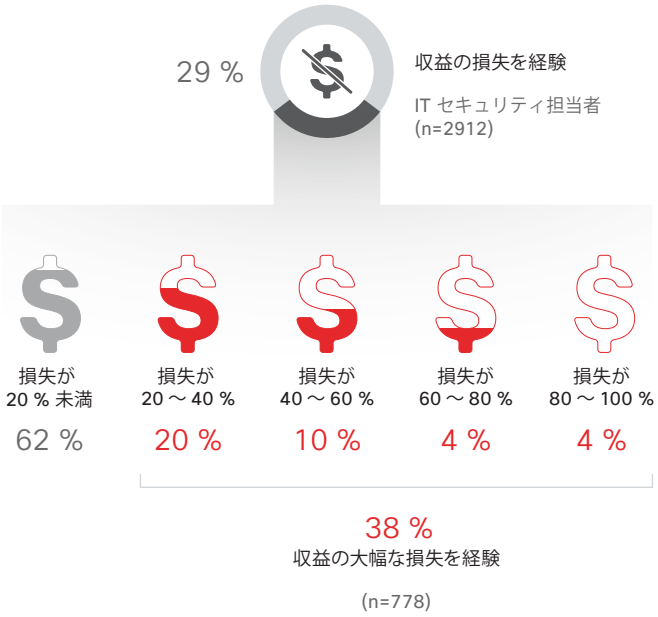
オンライン攻撃を受ける企業の機会損失は重大です。調査対象となったセキュリティ プロフェッショナルの 23 パーセントは、2016 年に、攻撃による機会損失を経験したと語りました（図 56）。そのグループのうち、58 パーセントは機会損失が全体で 20 パーセント未満であると述べ、25 パーセントは機会損失が 20 から 40 パーセント、9 パーセントは機会損失が 40 から 60 パーセントに上ったと述べています。

多くの組織は、公開されたセキュリティ侵害が原因で発生した収益損失を定量化できます。図 57 に示されているとおり、セキュリティ プロフェッショナルの 29 パーセントは、攻撃による減収を経験したと語りました。そのグループのうち、38 パーセントは、減収が 20 パーセント以上だったと述べています。

オンライン攻撃は、顧客の減少にもつながります。図 58 に示されているとおり、組織の 22 パーセントは、攻撃の結果、顧客が失われたと述べています。そのグループのうち、39 パーセントは、顧客の 20 パーセントあるいはそれ以上を失ったと語りました。

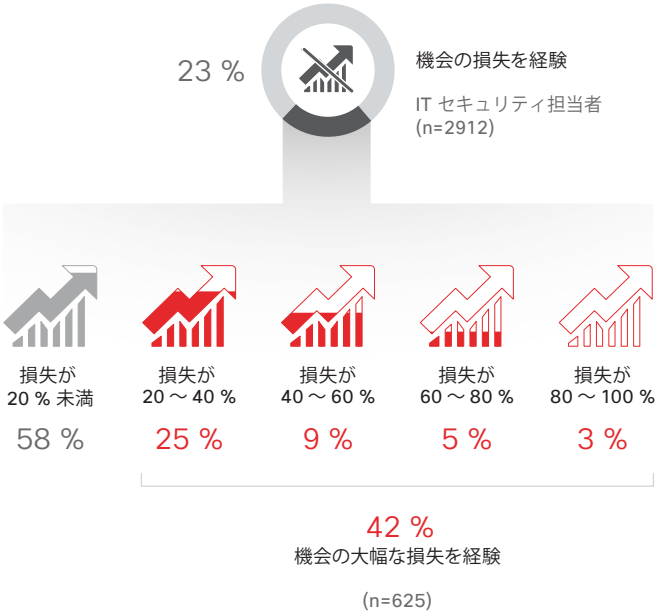
2017 年版の図表はこちらからダウンロードしてください：
www.cisco.com/go/acr2017graphics

図 57　攻撃の結果として組織が被る収益損失の割合



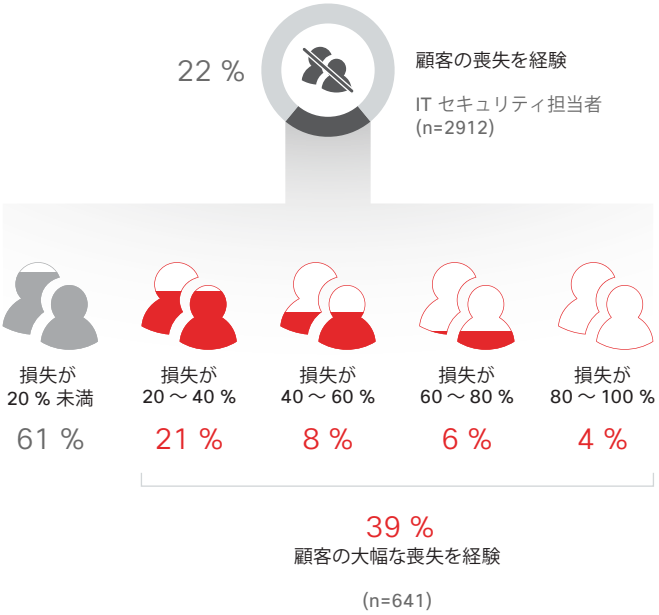
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 56　攻撃の結果として失われるビジネス チャンスの割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 58　攻撃が原因で企業が失う顧客の割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

結果：世間の厳しい監視の目はセキュリティ改善の一助となる

調査結果が示すとおり、侵害の影響は長く続き、広範囲に及びます。組織がある時点で侵害の影響を受けたと仮定すると、問題は次に何が起こるのかということです。侵害を発生しにくくするために、経営陣は自らの注意とリソースをどこに振り向けるべきでしょうか。

侵害の余波は、学習の機会であり、より優れたアプローチへの投資という点で無駄にすべきではない経験となります。

セキュリティ プロフェッショナルの 90 パーセントは、図 59 に示されているとおり、セキュリティ侵害が脅威防御テクノロジーやプロセスの改善を促進すると述べています。侵害の影響を受けた組織のうち、38 パーセントは IT 部門からセキュリティ チームを分離する対応を実施したと語っており、38 パーセントは従業員のセキュリティ啓発トレーニングが増えたと述べ、37 パーセントはサイバーセキュリティ リスク分析とリスク緩和により重きを置くようになったと述べています。

図 59 セキュリティ侵害がセキュリティ強化を推進する

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

組織は、人材、テクノロジーの互換性、予算の制約を超えて行動するため、創造性を発揮する必要があることを認めています。戦略の 1 つは、業務の予算を強化し、社内以外の人材を活用するため、アウトソーシング サービスを採用することです。

2016 年には、セキュリティ プロフェッショナルの 51 パーセントがアドバイスとコンサルティングを外部委託し、45 パーセントがインシデント対応を外部委託しました（図 60）。42 パーセントは、アウトソーシング サービスを利用してコストを削減していると述べ、48 パーセントがそのようにして先入観のない知見を得ていると述べています。

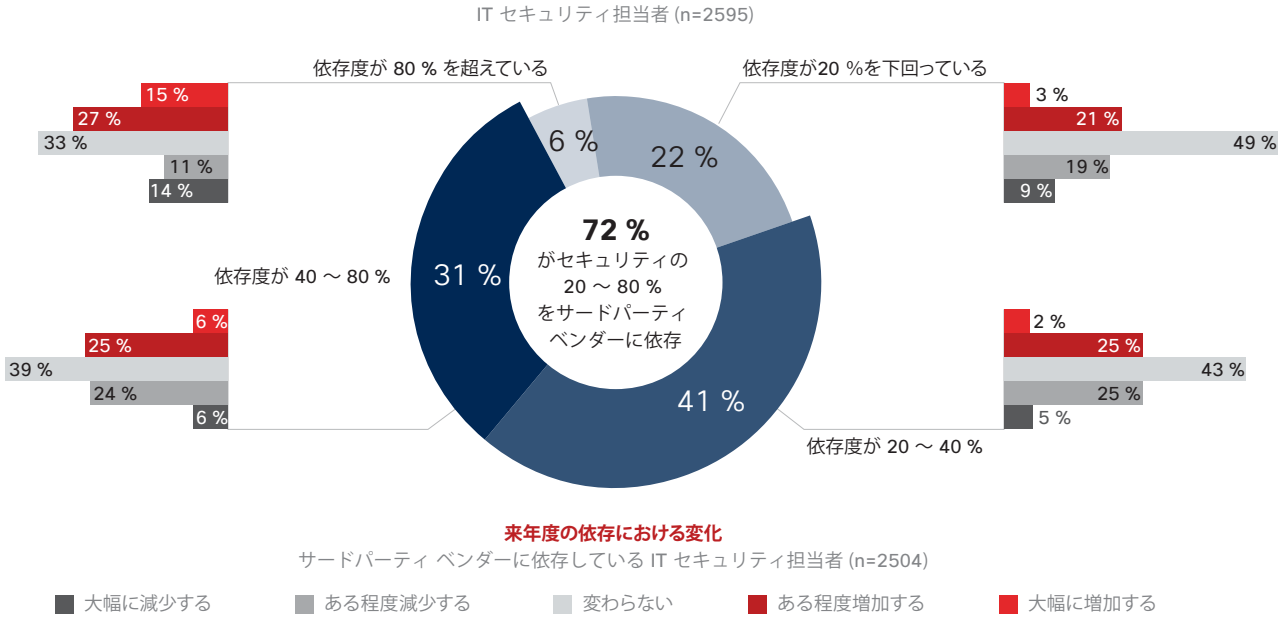
アウトソーシングで対応する際、組織は、サードパーティ ベンダーも利用して防御戦略を強化しています。このセキュリティ エコシステムにより、セキュリティに関する責任の分担が可能になります。

セキュリティ プロフェッショナルの 72 パーセントは、図 61 に示されているとおり、組織のセキュリティの 20 から 80 パーセントをサードパーティ ベンダーに依存していると語りました。セキュリティに関して外部の支援に依存するところが大きい組織は、将来サードパーティ ベンダーの使用を増やすつもりであると述べる傾向がありました。

図 60 アウトソーシングへの組織の依存度

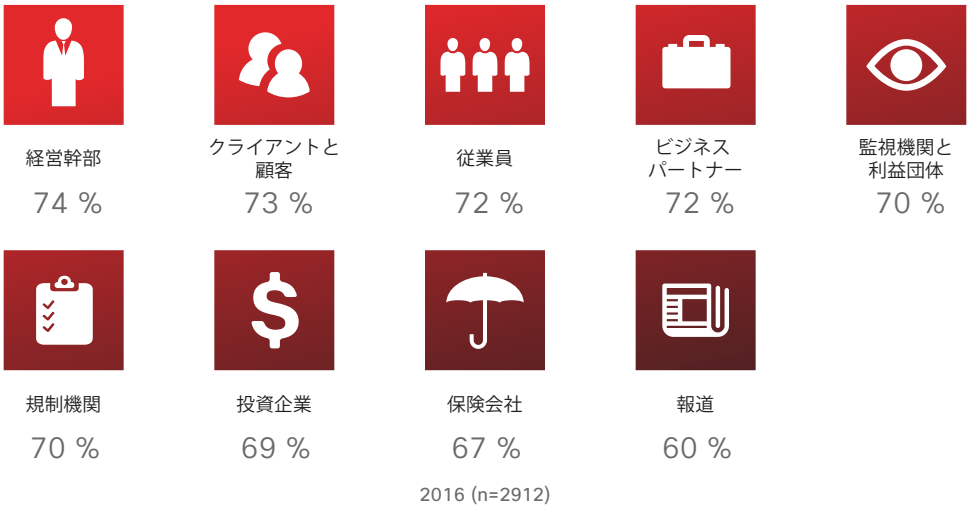
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 61 アウトソーシングに依存する組織の割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 62 精査の増加原因

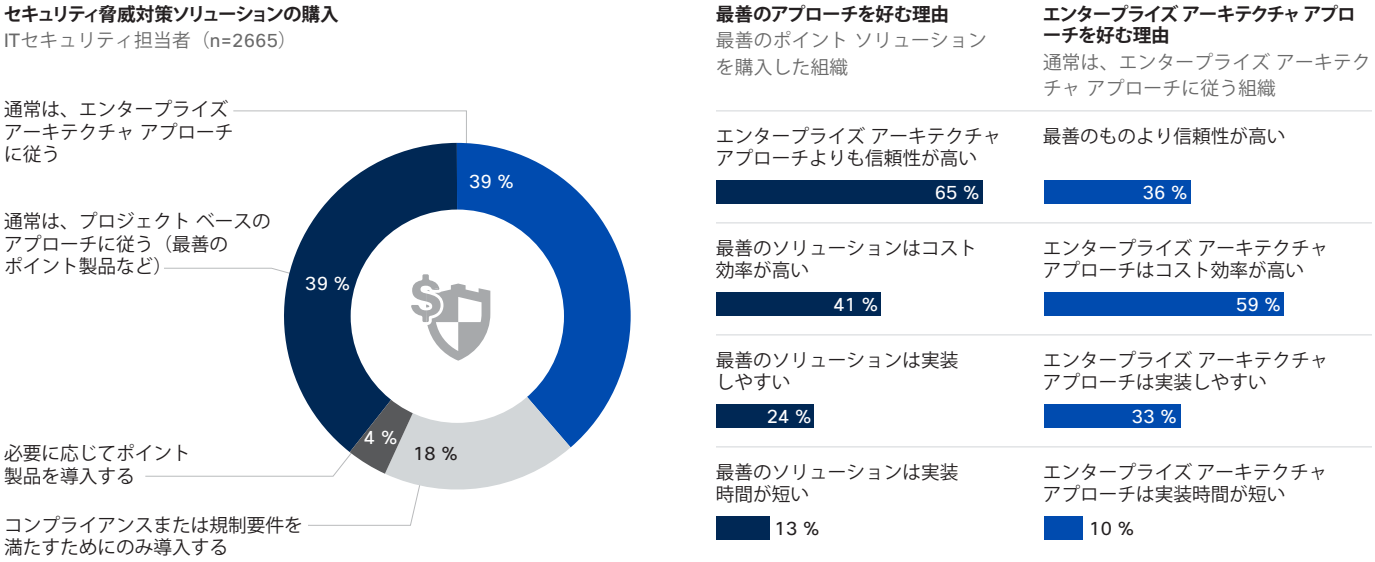


出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

組織がセキュリティ ポスチャを強化するための手順を実行するにつれて、その取り組みに一層の注意が向けられることを期待できます。そのような監視は、影響力をもつ観察者からのものであり、無視できません。これら観察者の不安に対処する方法は、自らを防御する組織の能力に多大な影響を及ぼします。

図 62 に示されているとおり、セキュリティ プロフェッショナルの 74 パーセントは監視がエグゼクティブ リーダーからのものであると述べ、73 パーセントはクライアントと顧客から、72 パーセントは従業員からと述べています。

図 63 信頼性とコスト効率がセキュリティの意思決定を促進する



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

信頼対コスト：セキュリティ ソリューション購入の促進要因

セキュリティ プロフェッショナルは、組織の保護に最も適したソリューションを求めていますが、理想とする安全な環境の構築方法については見解が異なります。さまざまな問題を解決することを信じて、さまざまなベンダーから最良のソリューションをベストオブブリード方式で購入する、という考え方もあれば、最もコスト効率が高いのは統合型アーキテクチャである、という考え方もあります。セキュリティ投資を推進するさまざまな要素があるとはいえ、一層の簡素化は、あらゆる組織に利益をもたらします。

図 63 に示されているとおり、ベストオブブリードのソリューションと統合ソリューションのいずれかを選択する際に、セキュリティ プロフェッショナルの見解は信頼性とコストの点で真っ二つに分かれています。65 パーセントは、エンタープライズ アーキテクチャのアプローチよりも信頼できるので、ベストオブブリードのソリューションを支持すると述べました。一方、59 パーセントは、よりコスト効率が高いと考えて、アーキテクチャ アプローチを支持すると語っています。

これは二者択一のジレンマではありません。組織は、ベストオブブリードのセキュリティ ソリューションと統合型のセキュリティ ソリューションの両方を必要とします。いずれのアプローチも利益をもたらし、自動化された対応ツールを実現しつつ、セキュリティを簡素化します（図 63）。

ベストオブブリードのソリューションと統合型のアプローチを組み合わせることにより、セキュリティ チームは、シンプルながら、より簡潔かつ有効なセキュリティに向けた措置を講じることが可能になります。統合型のアプローチは、セキュリティ プロフェッショナルが防御のあらゆる段階で生じる事柄を理解するのに役立ちます。このようなアプローチは、攻撃者の活動領域を縮小させます。簡潔で、チームがソリューションを広範囲に展開することを可能にします。オープンで、必要に応じてベストオブブリードのソリューションの導入も可能です。また、迅速な検出のために自動化されています。

サマリ：ベンチマーク調査で明らかになった事柄

単にセキュリティ ツールを収集することと、それらのツールを活用してリスクを軽減し、敵の活動領域を封じることとの間には雲泥の差があります。ベンチマーク調査の回答者は、攻撃を阻止するツールを手にしていると考えています。とはいえ、それと同時に、人員の不足や、製品が互換性に乏しいなどの制約が、優れたツールを期待よりも効果の薄いものにしてしまう場合があることも認めています。

侵害の影響についての粛然とさせられる調査結果は、セキュリティ プロフェッショナルにとって、プロセスとプロトコルの改善が必要であることの十分な証拠となります。減収や顧客の喪失といった現実的かつ直接的な影響があるとなれば、セキュリティ保護のギャップがなくなることをただ願うだけでは済まなくなります。なせなら、問題は、侵害が「発生するかどうか」ではなく、「いつ発生するか」だからです。

ベンチマーク調査により明らかになった事柄の 1 つは、機動的かつ有効なセキュリティを制限する制約は常に存在するということです。セキュリティ プロフェッショナルが必要と考える程度にまで予算と人材が満たされることは決してないでしょう。それらの制約を甘受するのであれば、セキュリティの簡素化と、自動化されたソリューションの導入は理にかなっています。

またセキュリティの簡素化には、ベストオブブリードのソリューションと統合型アーキテクチャが活用されます。組織にはどちらのアプローチのもたらす利益も必要です。

業界

業界

バリュー チェーンのセキュリティ：デジタル世界における成功の要はサードパーティ リスクの軽減にある

バリュー チェーンのセキュリティは、相互に繋がりあった経済における成功に不可欠な要素です。バリュー チェーン（ハードウェア、ソフトウェア、サービスのエンドツーエンドのライフサイクル）全体を通して、適切な場所、適切な時間に適切なセキュリティが存在するかどうかを確認することは急務です。

バリュー チェーンの 8 つの段階が図 64 に示されています。

情報技術と運用技術は、デジタル化された世界を 1 つにまとめています。組織にとって、社内ビジネス モデル、商品、インフラストラクチャの保護に集中するだけでは十分ではありません。組織はバリュー チェーン全体に目を向け、ビジネス モデルやサービスに関与する各サードパーティがセキュリティ リスクを生じさせるかどうかを考慮する必要があります。

端的に答えるならば、サードパーティがセキュリティ リスクを生じさせる可能性は高いといえます。SANS Institute による調査は、データ漏洩の 80 パーセントがサードパーティから発生していることを明らかにしました。[15] リスクを軽減するため、信頼が暗黙的なものではなく、セキュリティが各成員の責任であるようなバリュー チェーンを構築する必要があります。この目標の達成に向けての基本段階として、組織は次の事柄を実行する必要があります。

- サードパーティのエコシステムにおけるキー プレーヤーを特定し、それらのサードパーティが何をもたらすかを把握する
- 共有が可能で、エコシステム内のさまざまなサードパーティに展開できる柔軟なセキュリティ アーキテクチャを開発する
- これらのサード パーティが、組織のセキュリティ アーキテクチャで設定された許容度の範囲内で運営されているかどうかを評価する
- デジタル化の進行につれて、エコシステムがもたらす可能性のある新たなセキュリティ リスクに警戒する

組織は、サードパーティ エコシステムの関与が必要な、あるいは関与が必要ではないとしても同エコシステムに影響を及ぼす新しいビジネス モデルや商品を導入する前に、セキュリティについて考慮する必要があります。潜在的な価値と生産性向上を、潜在的リスク、特にデータ セキュリティとプライバシーに関するリスクと比較するべきです。

バリュー チェーンの重要性に対する認識は、世界的に、また特定の産業セクターにおいても高まりつつあります。最近の米国 IT 調達法は、情報技術およびサイバーセキュリティ取得に向けた調達の際、オープン テクノロジー標準に関する、米国防総省による 1 年間の評価を義務付けました。[16] 結束の固いエネルギー セクターでは、North American Electric Reliability Corporation（NERC）が、サイバー バリュー チェーンに対応する新しい要件を作成しています。[17]

図 64 バリュー チェーンの各段階

出典：シスコ

[15] *サプライ チェーンにおけるサイバー リスクへの対抗*、SANS Institute、2015 年：https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252。
[16] 公法 114-92 §
[17] NERC はこの取り組みの実施を米国連邦政府エネルギー規制機関 18 CFR パート 40 [整理番号 RM15-14-002、オーダー番号 829] によって命令された。

組織は、サードパーティとともに、「データはどのように、誰によって作成されるのか」や、「データはデジタル的に抽出されるべきか」などの質問に答える必要があります。事をさらに明確にするには、「自分たちが収集または作成したデジタル資産を誰が所有するのか」や、「その情報を誰と共有するべきか」といった質問に答えなければなりません。答えが必要なもう 1 つの重要な質問は、「侵害が発生した場合、誰がどのような責任や義務を負うのか」です。

このバリュー チェーン中心型アプローチは、ソリューションのライフサイクルの各段階で、セキュリティ上の配慮が確実に払われるようにするのに役立ちます。適切なアーキテクチャは、適切なセキュリティ標準への準拠と相まって、バリュー チェーン全体での広範に及ぶセキュリティの促進と、信頼の構築を後押しします。

地政学的最新情報：暗号化、信頼、そして透明性を求める呼びかけ

以前のサイバーセキュリティ レポートで、シスコの地政学専門家は、インターネット ガバナンスに関する状況の不確実性、個人の権利と国の権限との対立、政府と民間企業がデータ保護に伴うジレンマを乗り越える方法について調査しました。これらの議論に共通のトピックは、暗号化です。シスコは、今後しばらくの間、暗号化が、サイバーセキュリティに関する議論の中に浸透し、議論を支配さえすると考えています。

国や地域のデータ プライバシー保護法の急増は、そのような法に対処しようとするベンダーとユーザを困惑させてきました。この不確実な環境では、データ主権やデータ ローカリゼーションのような問題に注目が集まるようになり、複雑な発展途上のプライバシー規制に準拠するため、ビジネスが創造的なソリューションを求めていることから、クラウド コンピューティングや、ローカライズされたデータ ストレージの成長を促進しています。[18]

同時に、データ漏洩や標的型攻撃（ATP）の増加や、民族国家の支援の下に行われたハッキング（米国大統領選挙のような注目度の高いイベントの間に行われたものも含む）に関する報道より、ユーザは、自分の機微な情報やプライバシーが保護されるという確信が持てなくなっています。

スノーデン後の時代の政府は、必要に応じたデジタル通信とデータへのアクセスの規制をますます声高に求めるようになっています。その一方で、ユーザは、プライバシーを熱烈に願い求めてきました。テロリストが所有していた iPhone に関する Apple と FBI の間の最近の衝突のような出来事によって、プライバシーに関するユーザの不安が和らぐことはありませんでした。むしろこの出来事は、特に米国で、エンドツーエンドの暗号化についてデジタル ユーザ世代が知る機会となりました。今日、多くのユーザは、テクノロジー プロバイダーにエンドツーエンド暗号化を要求しており、暗号化キーを保持することを求めています。

これは、既知のサイバーセキュリティの世界における根本的な変化を明確に示しています。組織は、互いに矛盾する課題に対処できるように、環境を構築する必要があります。

この変化が続く間、一層多くの政府は、往々にして広範にわたり、製造業者、通信プロバイダー、あるいはユーザに知られずに、暗号化や技術的保護対策を回避または突破する法的な権限を自らに付与しようとします。この事態は、当局とテクノロジー企業の間に緊張を生むだけではなく、第三国の機関がアクセスした自国民のデータを見ることに必ずしも熱心ではない政府の間にも緊張を生じさせます。多くの政府は、ベンダー ソフトウェアで検出したゼロデイ攻撃と脆弱性に関する情報を収集します。しかしながら、保持している情報に関して常にベンダーに対し透明性を確保しているわけではなく、それらの情報を迅速にベンダーと共有することもありません。

そのような価値ある情報を抱え込んでしまうと、ベンダーは、自社製品のセキュリティを向上させたり、脅威からのユーザの保護を改善したりすることができなくなります。一部の情報を非公開にとどめておく十分な理由が政府にあるかもしれないとはいえ、グローバル サイバーセキュリティの世界では、一層の透明性と信頼が必要とされています。そのため、政府は、ゼロデイ攻撃についてのデータの蓄積に関する現在の施策を率直に評価する必要があります。政府は、ベンダーとの情報の共有が誰にとってもはるかに安全なデジタル環境につながる可能性があるという基本姿勢に基づいて取り組みを開始するべきです。

[18] このトピックについての詳細は、「規制の不確実性が継続するとデータ ローカリゼーションが減退する」[英語]、Stephen Dockery 著、2016 年 6 月 6 日、*The Wall Street Journal* を参照してください：http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/。

高速暗号化：転送中のデータを保護するスケーラブルなソリューション

65 ページの地政学セクションで説明したように、エンドツーエンドの暗号化は当面、政府と企業の間に議論と困惑を生み続けるでしょう。しかし、この問題に起因する緊張感にもかかわらず、顧客が保持するキーを使用したエンドツーエンドのデータ暗号化への需要は増加しています。

シスコの地政学専門家は、特に広告中心のビジネス モデルで、データのストリームやプールの一部は、少なくとも短期的に、ベンダー マネージド キーによって暗号化される状態が継続すると予想しています。ただし、それ以外の部分については、その逆の流れへの法的義務が存在しないことから、顧客が保持するキーを使用したエンドツーエンドの暗号化の使用が勢いを増す事態を想定しなければなりません。

一方、特にデータがあるデータセンターから別のデータセンターに高速で移動するときに、移動中のデータをより制御しながら保護する方法を模索している組織について考えてみましょう。これは従来、レガシー テクノロジーの限界とネットワーク パフォーマンスに与える影響が原因となり、企業にとっては困難な作業でした。しかし、新しいアプローチによってこのプロセスは容易になっています。

1 つのソリューションは、アプリケーションが暗号化データに変更されるアプリケーション レイヤ セキュリティです。組織が使用するアプリケーションの数によって、このタイプのセキュリティの導入時には大量のリソースが必要であり、実装は複雑で、運用コストがかかる場合があります。

もう 1 つ勢いを増しているアプローチが、転送中のデータを保護する暗号化機能をネットワークまたはクラウド サービスに組み込むことです。これは従来の VPN ゲートウェイ モデルを進化させたものであり、ネットワークの動的な性質とデータセンター トラフィックの高速転送レートに対応するソリューションです。企業は新機能によってもたらされる運用効率とコスト効率を活用して、その環境内のアプリケーションから別の場所に高速で移動するデータを保護します。

しかし、ネットワークベースの暗号化はデータを保護するためのツールの 1 つにすぎません。転送中または保存中のデータを確実に保護するため、組織はこの課題に包括的に向き合わなければなりません。手始めに、テクノロジー ベンダーに基本的だけれども重要な、次のような質問をすることです。

- 転送時のデータをどのように保護するか。
- 保存時のデータをどのように保護するか。
- 誰がデータにアクセスできるか。
- データはどこに保存されているか。
- データ削除をいつ、どのような基準で実施するかといったポリシーはどういったものか。

繰り返しますが、これらの質問はデータ保護に関する広範な議論の開始点にすぎず、データの復元力や可用性のような内容の話し合いに展開させる必要があります。

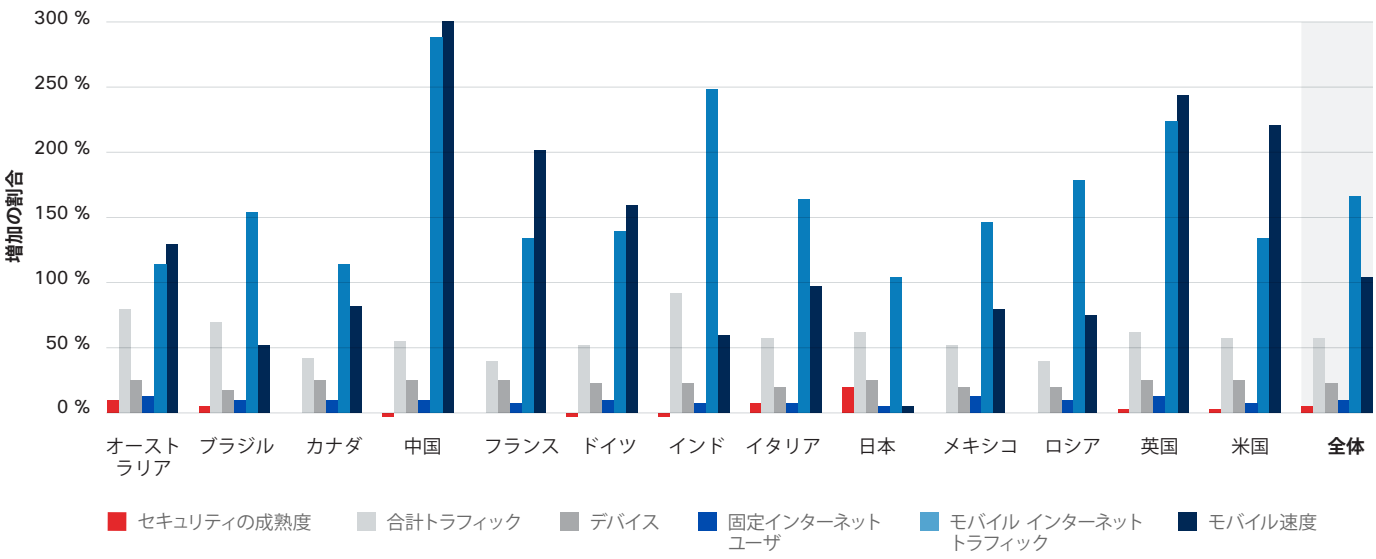
ネットワーク パフォーマンスおよび導入とセキュリティの成熟度の比較：オンライン速度、トラフィック、準備態勢は同じペースで成長しない

防御側は、敵に先を越されまいとします。後れを取るなら、潜在的に危険な状況に置かれることになります。懸念となるのは、攻撃側が活動する領域と時間を広げるのと同じペースでは、防御側がセキュリティ ポスチャを改善できないことです。固定型およびモバイル型のインターネット トラフィックが世界中で増大しているため、防御者は、セキュリティ インフラストラクチャの成熟度の向上を、トラフィックの増大に見合ったものとするよう義務付けられています。

Cisco VNI による予測では、モバイルおよび Wi-Fi トラフィックを含む、世界の IP トラフィックが年に 1 度調査されます。この予測では、IPトラフィック、インターネット ユーザの数、IP ネットワークでサポートされるパーソナル デバイスや Machine-to-Machine（M2M）接続の数に関する 5 年間の予測が示されます（VNI による予測の詳細についてはこちらを参照してください）。たとえば、この予測では、2020 年までに、スマートフォンが IP トラフィック全体の 30 パーセントを占めるようになると予想されています。

シスコは、VNI による予測を、シスコの年次セキュリティ機能ベンチマーク調査から抽出された防御者の成熟度に関するデータと照合しました（49 ページを参照）。2015 年、2016 年、2017 年のベンチマーク レポートにおける成熟度の成長率を調べると、図 65 に示されているとおり、セキュリティの成熟度は、インターネット トラフィックの増加と比べて思わしくありません。事実、中国、ドイツなどの一部の国では、同じ期間中に、成熟度に若干の低下が生じています。特にブロードバンドの速度は、図 65 に示されているとおり、ネットワークに関する他の変数と比べて著しく速いペースで向上し伸長しました。速度の向上と接続デバイスの増加により、一層のトラフィック拡張が促進されますが、組織は、同じペースでセキュリティ対策やインフラストラクチャを強化しようと苦心しています。

図 65　セキュリティの成熟度と成長率



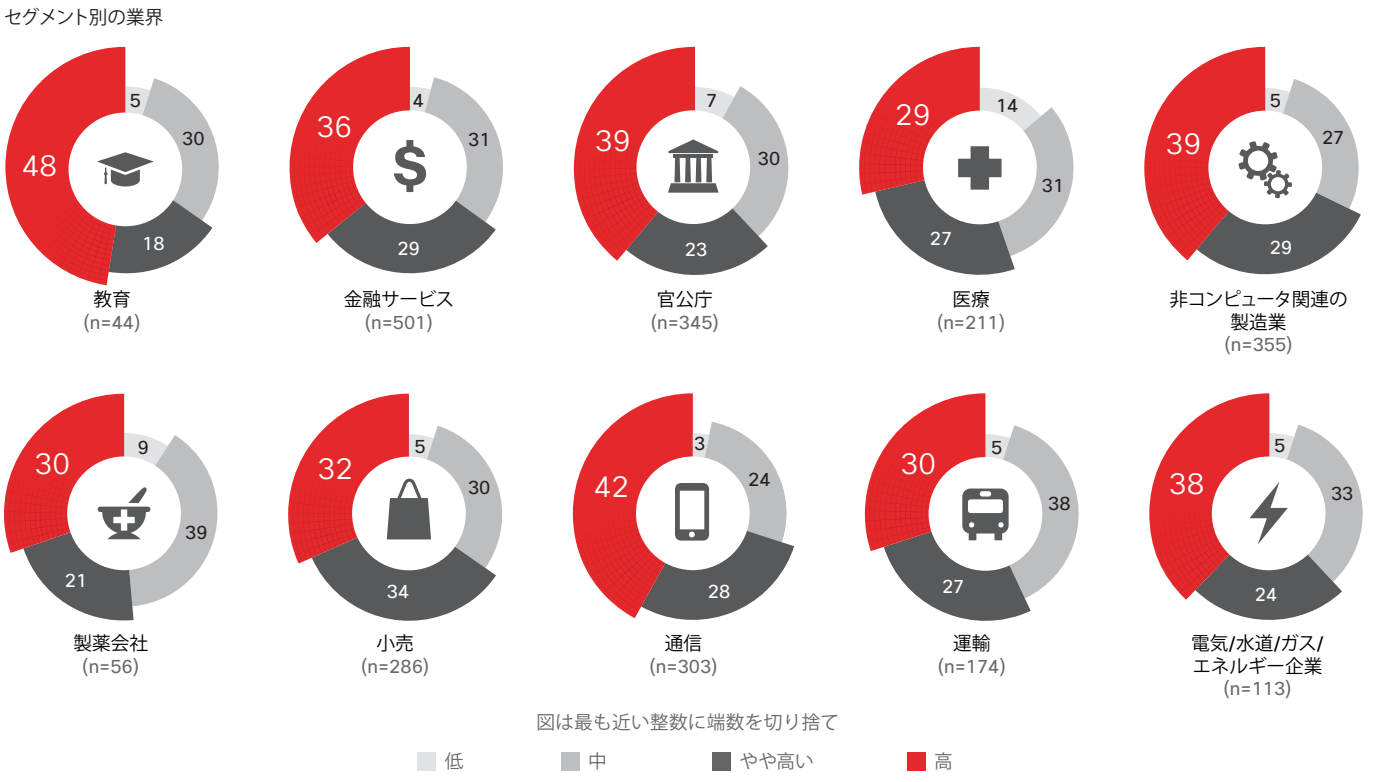
出典：シスコ セキュリティ リサーチ、2017 年のシスコによるセキュリティ機能のベンチマーク調査

一部の業界は、図 66 に示されているとおり、他の業界と比べて、セキュリティの成熟度に関して遅れています。特に、製薬業界、医療業界、運輸業界は、他の業界に後れを取っています。

モバイルの速度の飛躍的な向上は、通信プロバイダーが 4G および LTE ネットワークを導入した結果であることに留意することが重要です。2010 年代の終わりまでに 5G ネットワークの大規模導入が可能になると、モバイルの速度は、固定型ネットワークの速度と同等になると見込まれています。現行の Mobile VNI による予測によると、5G が広範に導入された場合、グローバル モバイル トラフィックが全 IP トラフィックの中で一層大きな部分を占めるようになると思われます。2015 年の全世界のモバイル トラフィックは IP トラフィック全体の 5% でしたが、VNI の予測によると、2020 年には IP トラフィック全体の 16% にまで増加すると予測されています。

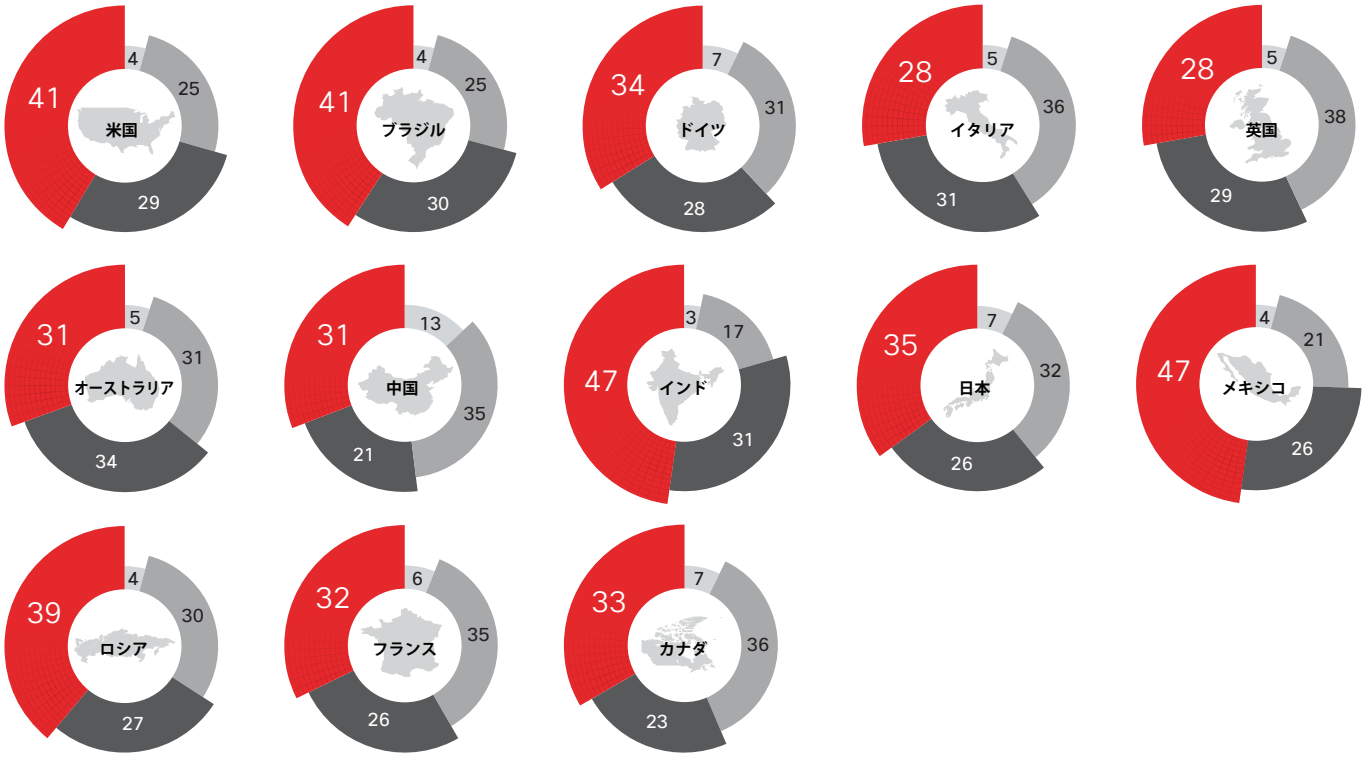
インターネット トラフィックの増加は攻撃対象の増加を示します。この流れに後れを取らないように、セキュリティ組織は成熟に向けた取り組みを段階的かつ迅速に引き上げる必要があることは明らかです。さらに、企業ネットワークに固定/有線接続されている以外のエンドポイントの使用量の増加に対応する必要もあります。また、従業員が個人用デバイスを使用して企業データにアクセスする傾向の拡大にも対応しなければなりません。

図 66 業種別のセキュリティの成熟度



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 67 国別のセキュリティの成熟度



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

高速化はインターネット トラフィックの増加を促進する唯一の要因ではありません。IoT はインターネットに接続するデバイスの数を加速させ、トラフィックの増加に寄与するだけでなく、新たな攻撃の潜在ルートにもなっています。

Cisco VNI の予測に関する詳細については、シスコ Web サイトを参照するか、2015 年から 2020 年にかけての年間 VNI 予測のシスコのブログ記事をお読みください。

まとめ

まとめ

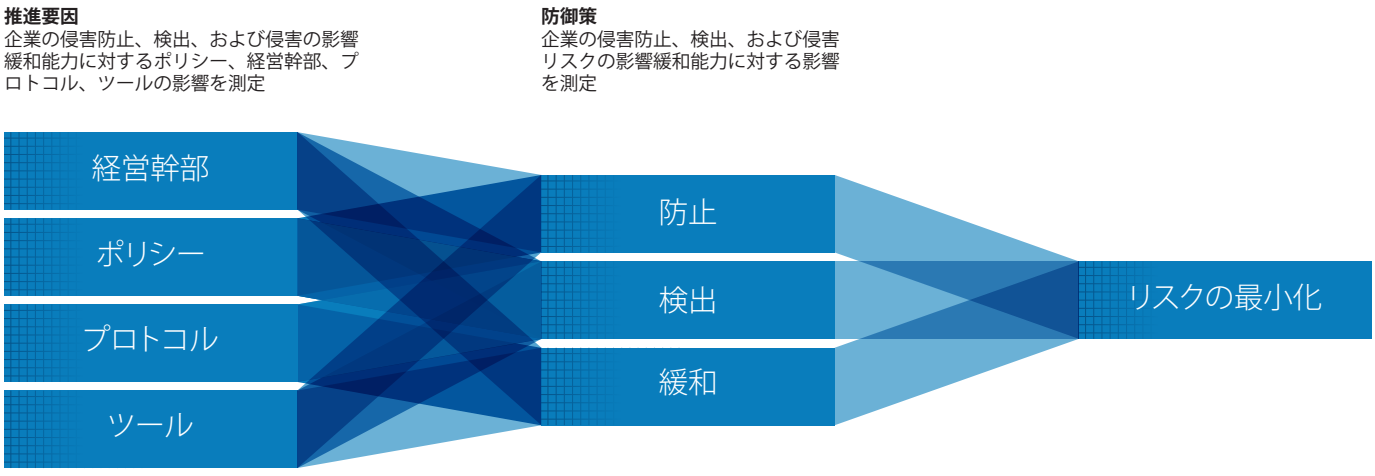
攻撃対象の急激な拡大を受け、セキュリティに対して相互に関連する統合的なアプローチが求められている

シスコのセキュリティ機能ベンチマーク調査（49 ページを参照）のデータを分析すると、組織がリスクを最小化することに役立つパターンや意思決定を考察することができます。そこから、リスクに大きな差が生まれるセキュリティ投資を、どの分野に対して行うべきかを確認できます。リスクの測定には、セキュリティ侵害の期間に加え、システム停止比率も加味されています（セキュリティ侵害の期間と影響を受けるシステムについては、55 ページの図 53 を参照）。

企業がリスクに対して有効な対策をどのように創出するかを理解するには、リスクの防止、検出、緩和に影響する要因を検討する必要があります（図 68 を参照）。これらの要因には、次の要素を含める必要があります。

- **経営陣：**上級役員はセキュリティの優先順位を設定する必要があります。これは攻撃の緩和と防止のために不可欠です。幹部チームは、セキュリティ プログラムの有効性を評価するための、明確で確固としたメトリックが必要です。
- **ポリシー：**ポリシーはリスクの軽減に強く結びついています。ネットワーク、システム、アプリケーション、機能、およびデータへのアクセス権限を制御することは、セキュリティ侵害による障害を軽減する機能に影響します。さらに、セキュリティ対策の定期的なレビューを確実に実施するポリシーが、攻撃の防止に役に立ちます。
- **プロトコル：**適切なプロトコルはセキュリティ侵害の防止と検出に役立ちますが、リスク軽減とも強固な関係があります。特に、ネットワーク上の接続アクティビティを定期的にレビューし、セキュリティ対策が機能していることを確認することは、予防と緩和の両方にとって重要です。セキュリティ対策を定期的、形式的かつ戦略的に、長期にわたり確認し、改善することも有益です。
- **ツール：**ツールの賢明かつ適切な応用は、リスク軽減に最も強固に結びつきます。ツールを使用すると、ユーザは検出と防止、リスク緩和に不可欠なフィードバックを確認し、提供できます。

図 68 リスクを最小化するための要因と対策



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

2017 年版の図表はこちらからダウンロードしてください：**www.cisco.com/go/acr2017graphics**

組織が使用するセキュリティ対策（防止、検出、リスク緩和）は、組織がリスクを最小化する能力の有効性を示す指標と見なすことができます（図 68 を参照）。

これらの対策には次の要素が含まれていなければなりません。

- **予防：**セキュリティ侵害の影響を最小化するため、従業員はセキュリティ障害や問題を報告する必要があります。セキュリティに関するプロセスと手順が明確かつ十分に理解されていることも重要です。
- **検出：**セキュリティ侵害の影響を最小化するために最適な検出方法とは、本格的なインシデントになる前に組織がセキュリティの弱点を特定できるようにする方法です。そのためには、インシデントに関連する情報を分類するための優れたシステムが不可欠です。
- **軽減：**インシデントへの対応および追跡に関する文書化されたプロセスと手順は、セキュリティ侵害を有効に軽減するための鍵となります。組織が自社の危機対応を管理するための強力なプロトコルも必要です。

これらの要因と対策すべてが相互に結びつき、互いに依存しています。セキュリティ プロフェッショナルがいくつかの要因と 1 ～ 2 個のセキュリティ対策を選び出すだけで、セキュリティの問題を解決したことにはなりません。すべての要因、すべてのセキュリティ対策が必要です。セキュリティ チームは、自社の弱点（リーダーからのサポート レベルの低さ、セキュリティ侵害を軽減するツールの欠如など）を分析し、セキュリティのどの部分に投資すべきかを計算する必要があります。

重要な目標：攻撃者の活動領域の削減

攻撃者が活動する余地を減らし（理想的には根絶）、攻撃者の存在を周知のものとすることが、防御側にとっての最優先事項となります。現実にはすべての攻撃を阻止することは誰にもできませんし、保護すべき対象のすべてを守ることも不可能です。しかし、サイバー犯罪者がそのキャンペーンを効果的なものとし、収益を得るために必要な活動領域をなくすことに注力すれば、監視の目をくぐり抜けて重要なデータとシステムに到達することを防ぐことができます。

このレポートでは、ユーザとシステムを侵害して攻撃をしかけるために攻撃者が使用するさまざまなアプローチを分類しました。当社が使用するカテゴリ（偵察、武器化、配信、インストール）は、攻撃が一般的に攻撃チェーンのどこに展開されているかに基づきます。この演習は、攻撃者がデバイスやシステムに拠点を確立し、キャンペーンを開始し、彼らが求めるメリットを享受するために脆弱性などの弱点をいつ、どこでどのようにして利用するか説明するために作成されました。

シスコは、防御側が攻撃者の基本プロセスに対抗するためのセキュリティ アプローチを適応させることを提案します。たとえば、偵察段階で攻撃を阻止するには、セキュリティ チームは次のことを行わなければなりません。

- 最新の脅威と脆弱性についての情報収集
- ネットワークへのアクセス制御の確認
- 拡大している攻撃対象に組織がさらされることを制限
- コンフィギュレーションの管理
- このワークにより知識が得られた一貫性のある対応策と手順の開発

武器化の脅威がもたらされたら、防御側は所持しているすべてのツールを適用して、その脅威の拡大と深刻化を防ぐ必要があります。ここで統合セキュリティ アーキテクチャが重要になります。このアーキテクチャは、脅威に関するリアルタイムのインサイトを提供し、脅威の検出を改善するために必要な自動検出と防御を提供します。

インストール段階では、セキュリティ チームは侵害に対応し、調査している間にも、環境の状態について常に最新の情報を得ておく必要があります。その環境が単純で、オープンであり、自動化されていて、防御側が前述の他の事前対策を取り入れていた場合、次のような重要な質問に対応できるように企業のリソースを集中させることができます。

- 攻撃者は何にアクセスしたか。
- なぜそれが可能だったのか。
- 彼らはどこに向かったか。
- まだ社内のネットワーク内で活動しているか。

これらの質問への回答により、セキュリティ チームはさらなる攻撃を防ぐために適切なアクションを実行できるだけでなく、考えられるエクスポージャーと必要な情報開示に関して経営陣と役員に伝えることができます。企業は次に、セキュリティ侵害の間に特定されたセキュリティ ギャップ（攻撃が成功するために必要な活動スペースをもたらす弱点）に対応するために、包括的な制御と緩和が実施されていることを確認するプロセスを開始します。

シスコについて

シスコが提供する実世界向けのインテリジェントなサイバーセキュリティは、幅広い攻撃ベクトルにわたって、業界最大の包括的な高度な脅威からの保護ソリューションポートフォリオをもたらします。シスコによる脅威中心型の運用化されたセキュリティアプローチを採用すると、複雑さが緩和され、分断化が抑えられます。同時に、優れた可視性、一貫した管理、そして攻撃前、攻撃中、攻撃後の高度な脅威保護が提供されます。

シスコの集合型セキュリティ インテリジェンス（CSI）エコシステムの脅威リサーチャーは、業界をリードする脅威インテリジェンスを単独の傘の下に取りまとめます。これには、さまざまなデバイスとセンサー、パブリック フィードとプライベート フィード、およびオープンソース コミュニティのフットプリントから得られるテレメトリを使用します。これにより、何十億もの Web リクエストと何百万もの電子メール、マルウェアのサンプル、およびネットワーク侵入という量が毎日取り込まれています。

当社の洗練されたインフラストラクチャおよびシステムは、このテレメトリを消費して機械学習システムやリサーチャーがネットワーク全体、データセンター、エンドポイント、モバイル デバイス、仮想システム、Web、電子メール、そしてクラウドからの脅威を追跡し、根本原因とスコープのアウトブレイクを特定できるようにします。その結果得られるインテリジェンスが当社の製品およびサービスのリアルタイム保護に変換され、全世界のシスコのお客様に迅速に提供されます。

シスコの脅威中心型のセキュリティへのアプローチについての詳細は、www.cisco.com/go/security をご覧ください。

2017 年シスコ年次サイバーセキュリティ レポートの執筆者

CloudLock

シスコの子会社である CloudLock は、組織によるクラウドの安全な使用を支援するクラウド アクセス セキュリティ ブローカ（CASB）ソリューションの大手プロバイダーです。CloudLock は、ユーザ、データ、アプリケーション全体の Software-as-a-Service（SaaS）、Platform-as-a-Service（PaaS）、および Infrastructure-as-a-Service（IaaS）環境の可視性と制御を実現します。CloudLock はデータ サイエンティスト主導の CyberLab とクラウド ソーシング セキュリティ分析を通じて、実用的なサイバーセキュリティのインテリジェンスを提供します。詳細については、https://www.cloudlock.com を参照してください。

Security and Trust Organization

シスコの Security and Trust Organization は、企業の重役と世界的リーダーを等しく悩ませる最も重要な 2 つの問題に対応するためのシスコのコミットメントを示します。この組織の基本的な使命には、シスコの公的機関および民間のお客様を保護し、シスコの製品とサービス ポートフォリオ全体で Cisco Secure Development Lifecycle と Trustworthy System の取り組みを実現して確実なものとし、Cisco Enterprise を進化し続ける脅威から保護することなどがあります。シスコは、人、ポリシー、プロセス、テクノロジーを含む広範囲なセキュリティと信頼性に対して全体的なアプローチを取っています。Security and Trust Organization は、InfoSec、信頼できるエンジニアリング、データ保護とプライバシー、クラウド セキュリティ、透明性と検証、および Advanced Security Research and Government を重視しながら、運用効率を向上させます。詳細については、http://trust.cisco.com を参照してください。

グローバル ガバメント アフェアズ

シスコは、さまざまなレベルで政府と連携して、テクノロジー分野をサポートし、政府が掲げる目標の達成を支援する公的ポリシーや規制の作成をお手伝いしています。グローバル ガバメント アフェアズ チームは、テクノロジー重視の公的ポリシーや規制を作成し、影響を及ぼします。このチームは、業界のステークホルダーおよび関連パートナーと協力して取り組みながら、シスコのビジネスと全体的な ICT の導入に影響を与えるポリシーに働きかけるように政府のリーダーとの関係性を構築し、国際レベル、国内レベル、地域レベルでポリシーの意思決定を支援します。ガバメント アフェアズ チームは、世界中でテクノロジーの使用を促進および保護するシスコの活動を支援している、選挙で選ばれた元役員、国会議員、規制当局、米政府高官、公務員で構成されます。

Cognitive Threat Analytics

シスコの Cognitive Threat Analytics は、ネットワーク トラフィック データの統計分析により、保護されたネットワーク内での侵害、マルウェアの活動、およびその他のセキュリティ上の脅威を検出するクラウドベースのサービスです。このソリューションは、動作分析と異常検出を使用してマルウェアへの感染やデータ漏洩の症状を識別することにより、境界ベースの防御におけるギャップを解消します。Cognitive Threat Analytics は、高度な統計モデリングと機械学習を使用して、新しい脅威を独自に特定し、その内容から学習し、経時的に適応します。

IntelliShield チーム

IntelliShield チームは、Cisco セキュリティ リサーチ/オペレーション部門および外部ソースから得たデータや情報の脆弱性と脅威調査、分析、統合、関連付けを行い、複数のシスコ製品とサービスを支える IntelliShield セキュリティ インテリジェンス サービスを生み出します。

Talos セキュリティ インテリジェンスおよびリサーチ グループ

Talos はシスコの脅威インテリジェンス組織であり、シスコのお客様、製品、サービスに優れた保護を提供することを専門とするセキュリティ エキスパートのエリート グループです。Talos は、既知の脅威や新たな脅威の検出、分析、防御を行うシスコ製品向けに脅威インテリジェンスを構築するための高度なシステムによってサポートされる、最先端の脅威研究者で構成されます。Talos は Snort.org、ClamAV、SenderBase.org、SpamCop の公式ルール セットを維持し、Cisco CSI エコシステムに脅威情報を提供する主なチームです。

Security Research and Operations（SR&O）

Security Research and Operations（SR&O）は、業界トップクラスの Product Security Incident Response Team（PSIRT）を含むすべてのシスコ製品とサービスの脅威と脆弱性の管理を担います。SR&O は、お客様が Cisco Live や Black Hat 会議などのイベントで、また、シスコや業界全体でそのピアとのコラボレーションを通じて、進化し続ける脅威の状況を理解することを支援します。さらに、SR&O は既存のセキュリティ インフラストラクチャで検出または軽減されなかった侵害の指標を特定できる、シスコの Custom Threat Intelligence（CTI）のような新しいサービスを提供します。

Cisco Visual Networking Index（VNI）

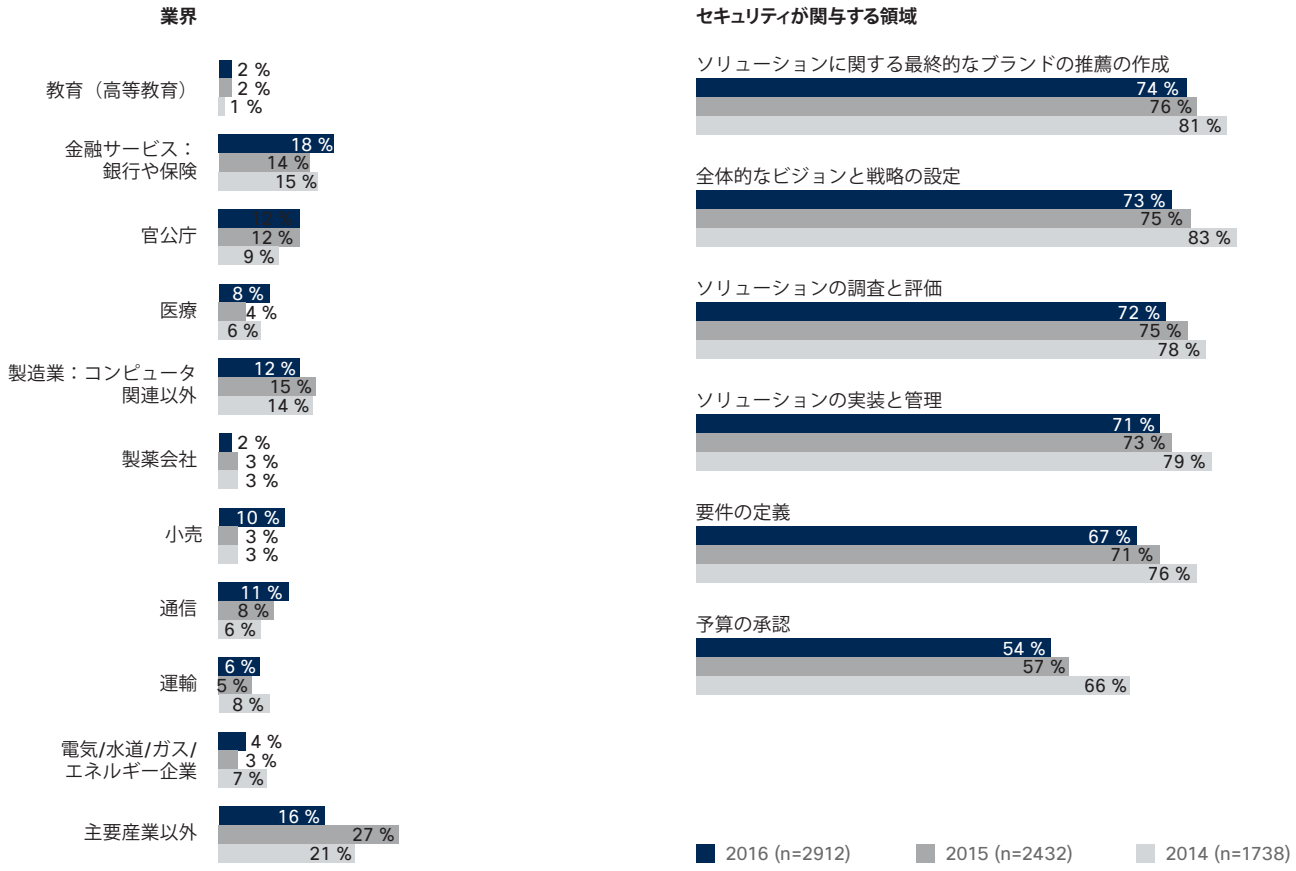
Cisco VNI による 2015 年から 2020 年にかけての世界の IP トラフィック予測は、独立したアナリストの予測と現実のネットワークの使用状況データに依拠しています。この基礎情報の上に、世界の IP トラフィックおよびサービスの導入に関するシスコ独自の見積が重ね合わされています。詳細な手法の説明は、完成版のレポートに記載されています。11 年の歴史の中で、Cisco VNI の研究はインターネットの成長指標として高く評価されるようになりました。連邦政府、ネットワーク レギュレーター、学術研究者、通信会社、テクノロジー専門家、業界誌や経営誌、アナリストは、この年間調査に依拠してデジタルの未来に関する計画を策定しています。

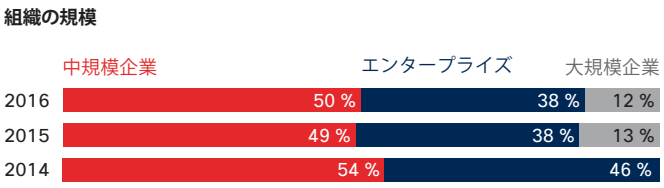
付録

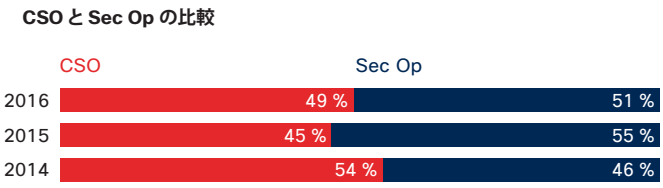
付録

2017 年シスコ セキュリティ機能ベンチマーク調査

図 69 サーベイ機能ベンチマーク調査







出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 70 専任のセキュリティ専門家の人数

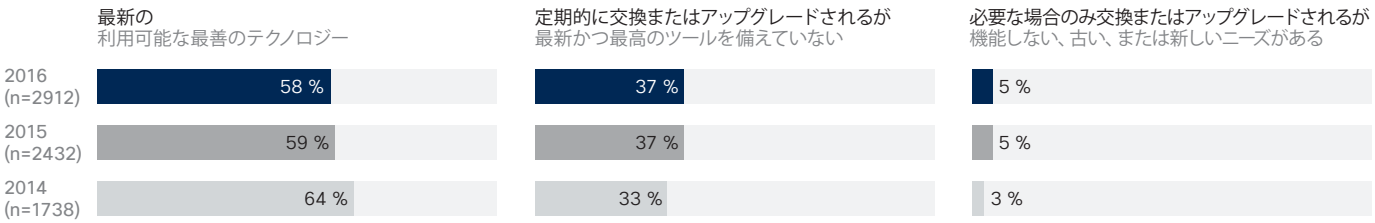
	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
1-9	18 %	17 %	15 %
10-19	16 %	18 %	17 %
20-29	12 %	17 %	13 %
30-39	8 %	9 %	8 %
40-49	4 %	4 %	6 %
50-99	19 %	16 %	19 %
100-199	9 %	9 %	9 %
200 以上	15 %	10 %	12 %
セキュリティ専任のプロフェッショナルの平均人数	**30**	**25**	**33**

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

認識

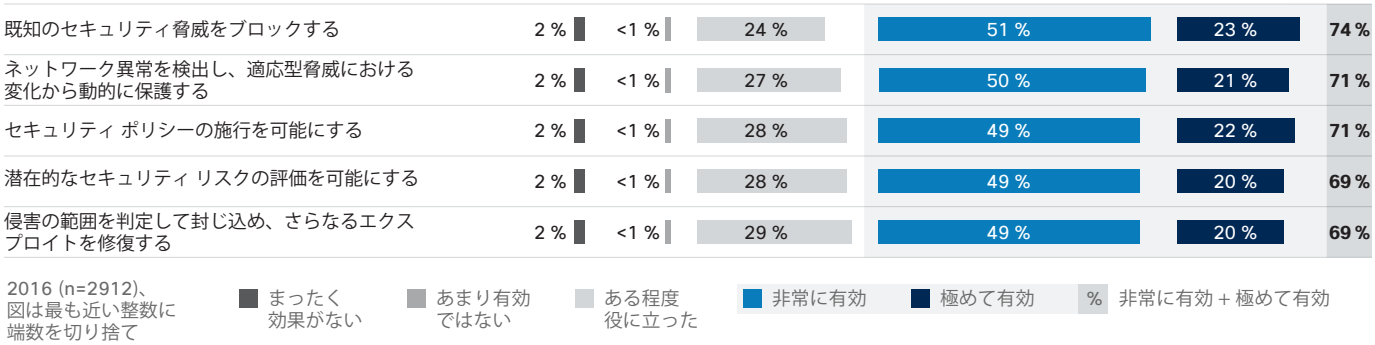
図 71 セキュリティ プロフェッショナルのほとんどはセキュリティ インフラストラクチャが最新であると考えている

御社のセキュリティ インフラストラクチャをどのように評価しますか。



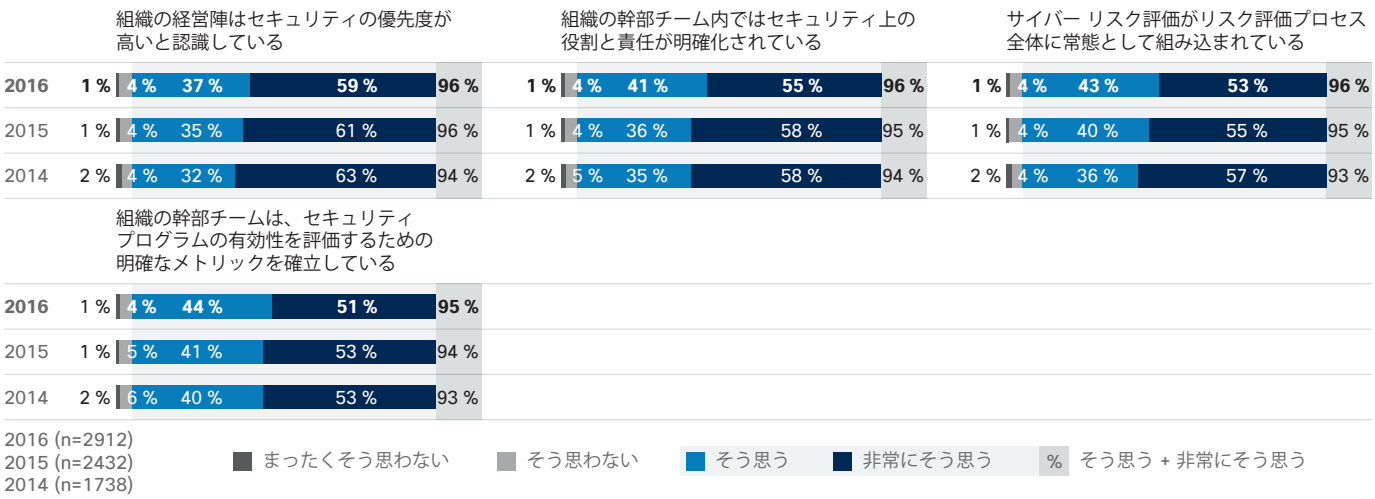
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 72 さまざまなセキュリティ ツールが非常に効果的であると認識しているセキュリティ プロフェッショナルの割合



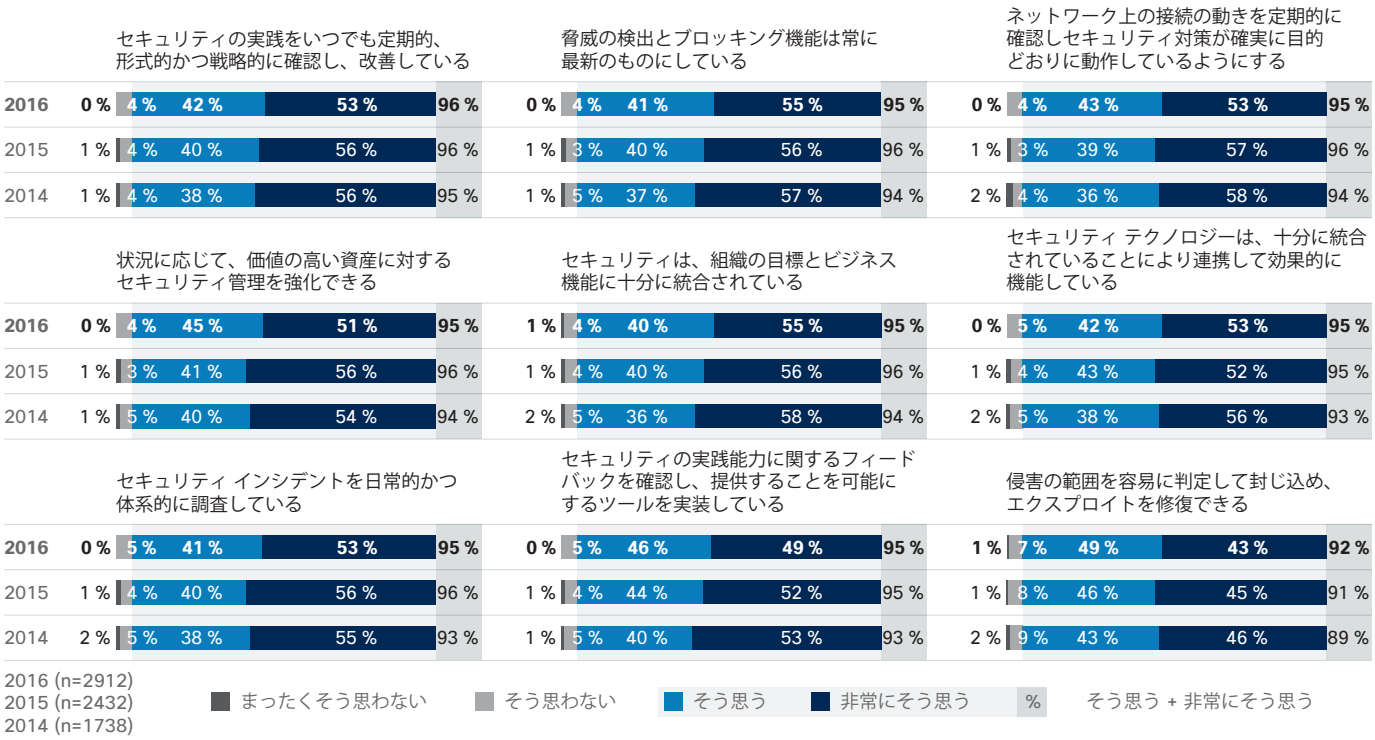
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 73 エグゼクティブ レベルでセキュリティの優先順位が高いと考えるセキュリティ プロフェッショナルの割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 74 セキュリティ オペレーション運用の説明に強く同意した回答者の割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

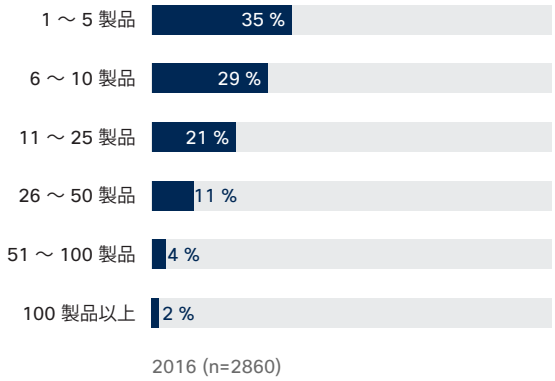
制約

図 75 セキュリティの最大の障害

	2015 (n=2432)	2016 (n=2912)
予算的な制約	39 %	35 %
互換性の問題	32 %	28 %
認定要件	25 %	25 %
熟練スタッフの不足	22 %	25 %
競合する優先事項	24 %	24 %
現在の作業負荷が重すぎる	24 %	23 %
知識の不足	23 %	22 %
効果が実証されるまでの購入への抵抗感	22 %	22 %
組織の文化/姿勢	23 %	22 %
組織は攻撃側にとって価値の高いターゲットではない	N/A	18 %
セキュリティは経営陣レベルの優先事項ではない	N/A	17 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 76 組織が利用するセキュリティ ベンダーと製品の数



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 77 組織の規模別の使用するセキュリティ ベンダーの数

セキュリティ環境で使用しているセキュリティ ベンダーの数（ブランド、製造業者など）。	中規模企業（従業員数 250 ～ 1,000 人）	企業（従業員数 1,000 ～ 10,000 人）	大規模企業（従業員数 10,000 人以上）
1 ～ 5	46.9 %	43.4 %	39.9 %
6 ～ 10	28.4 %	30.9 %	21.3 %
11 ～ 20	17.6 %	15.8 %	23.1 %
21 ～ 50	5.6 %	7.1 %	8.7 %
50 以上	1.4 %	2.8 %	6.9 %
合計組織数	**1435**	**1082**	**333**

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 78 組織の規模別の使用するセキュリティ製品の数

セキュリティ環境で使用しているセキュリティ製品の数。	中規模企業（従業員数 250 ～ 1,000 人）	企業（従業員数 1,000 ～ 10,000 人）	大規模企業（従業員数 10,000 人以上）
1 ～ 5	37.9 %	32.7 %	25.1 %
6 ～ 10	29.0 %	30.1 %	22.5 %
11 ～ 25	19.8 %	20.4 %	23.7 %
26 ～ 50	9.6 %	10.5 %	15.6 %
51 ～ 100	3.0 %	4.3 %	7.8 %
100 以上	0.8 %	1.9 %	5.4 %
合計組織数	**1442**	**1084**	**334**

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 79 IT 予算に組み込まれるセキュリティ予算の前年比減少率

セキュリティの予算は IT 予算の一部ですか。（IT 部門のメンバー）	2014 (n=1673)	2015 (n=2374)	2016 (n=2828)
完全に IT 予算内	61 %	58 %	55 %
一部は IT 予算内	33 %	33 %	36 %
完全な別予算	6 %	9 %	9 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

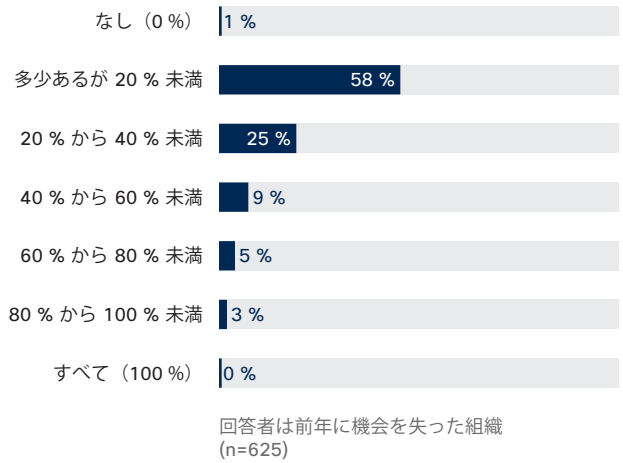
図 80 IT 予算に対するセキュリティ支出の前年比減少率

1 機能としてのセキュリティに対する IT 予算の支出	2014 (n=1673)	2015 (n=2374)	2016 (n=2828)
0 %	7 %	9 %	10 %
1-5 %	4 %	3 %	4 %
6-10 %	12 %	11 %	16 %
11-15 %	23 %	23 %	27 %
16-25 %	29 %	31 %	26 %
26 %-50 %	21 %	19 %	15 %
51 % 以上	5 %	4 %	2 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

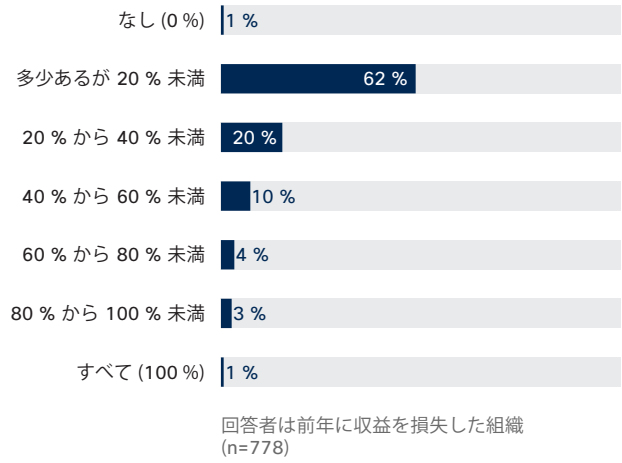
影響

図 81 攻撃によって失われる組織の機会の割合



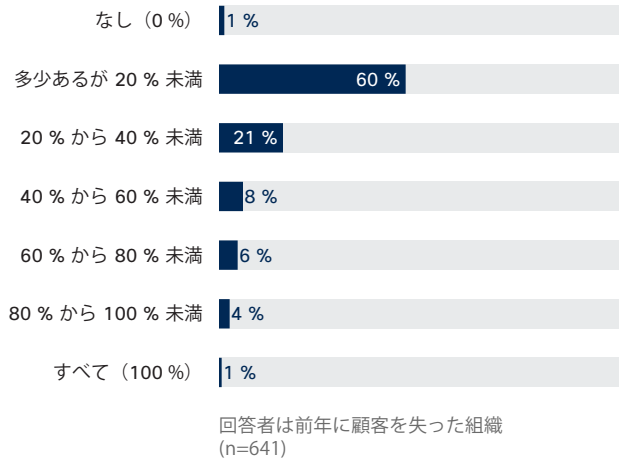
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 82 攻撃によって失われる組織の収益の割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 83 攻撃によって失われる組織の顧客の割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

成果

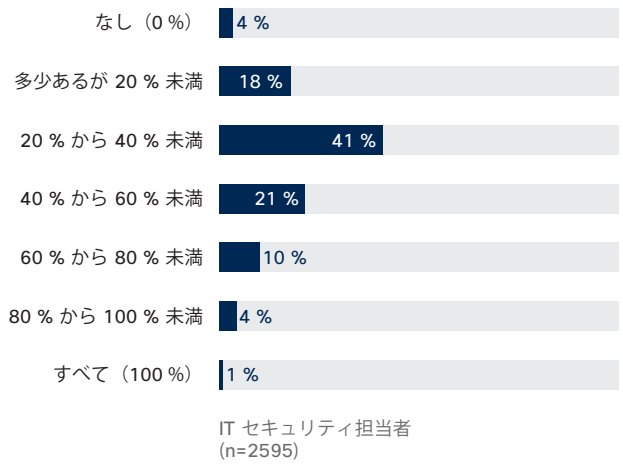
図 84 アウトソーシングに依存する組織の割合

外部に委託しているセキュリティ サービス	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
アドバイスとコンサルティング	51 %	52 %	51 %
監査	41 %	47 %	46 %
インシデント対応	35 %	42 %	45 %
モニタリング	42 %	44 %	45 %
脅威インテリジェンス	N/A	39 %	41 %
修復	34 %	36 %	35 %
なし/すべて内部	21 %	12 %	10 %

このようなサービスを外部に委託する理由	2015 (n=2129)	2016 (n=2631)
コスト効率が高い	53 %	52 %
公正な情報が必要	49 %	48 %
インシデントへのよりタイムリーな応答	46 %	46 %
社内の専門知識の不足	31 %	33 %
社内のリソースの不足	31 %	33 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 85 組織がサード パーティ ベンダーに依存する割合



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 86 組織の規模別のアウトソーシングされるセキュリティ サービスの割合

外部に委託しているセキュリティ サービス	中規模企業（n=1459）	エンタープライズ（n=1102）	大企業（n=351）
アドバイスとコンサルティング	50 %	52 %	51 %
監査	44 %	47 %	50 %
モニタリング	46 %	43 %	44 %
脅威インテリジェンス	41 %	41 %	40 %
インシデント対応	48 %	44 %	39 %
修復	35 %	34 %	37 %
なし/すべて内部	8 %	11 %	11 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 87 精査の増加原因

経営幹部	2 %	4 %	20 %	44 %	30 %	74 %
クライアントと顧客	2 %	4 %	21 %	41 %	32 %	73 %
従業員	2 %	5 %	22 %	44 %	28 %	72 %
ビジネス パートナー	2 %	5 %	22 %	43 %	29 %	72 %
監視機関と利益団体	2 %	5 %	23 %	44 %	26 %	70 %
規制機関	2 %	4 %	24 %	43 %	27 %	70 %
投資企業	3 %	5 %	23 %	41 %	28 %	69 %
保険会社	3 %	5 %	25 %	41 %	26 %	67 %
報道	4 %	8 %	28 %	39 %	21 %	60 %

2016（n=2912）、図は最も近い整数に端数を切り捨て

まったく監視されていない / あまり監視されていない / 多少監視されている / 非常に監視されている / 極めて監視されている / % 非常に監視されている + 極めて監視されている

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

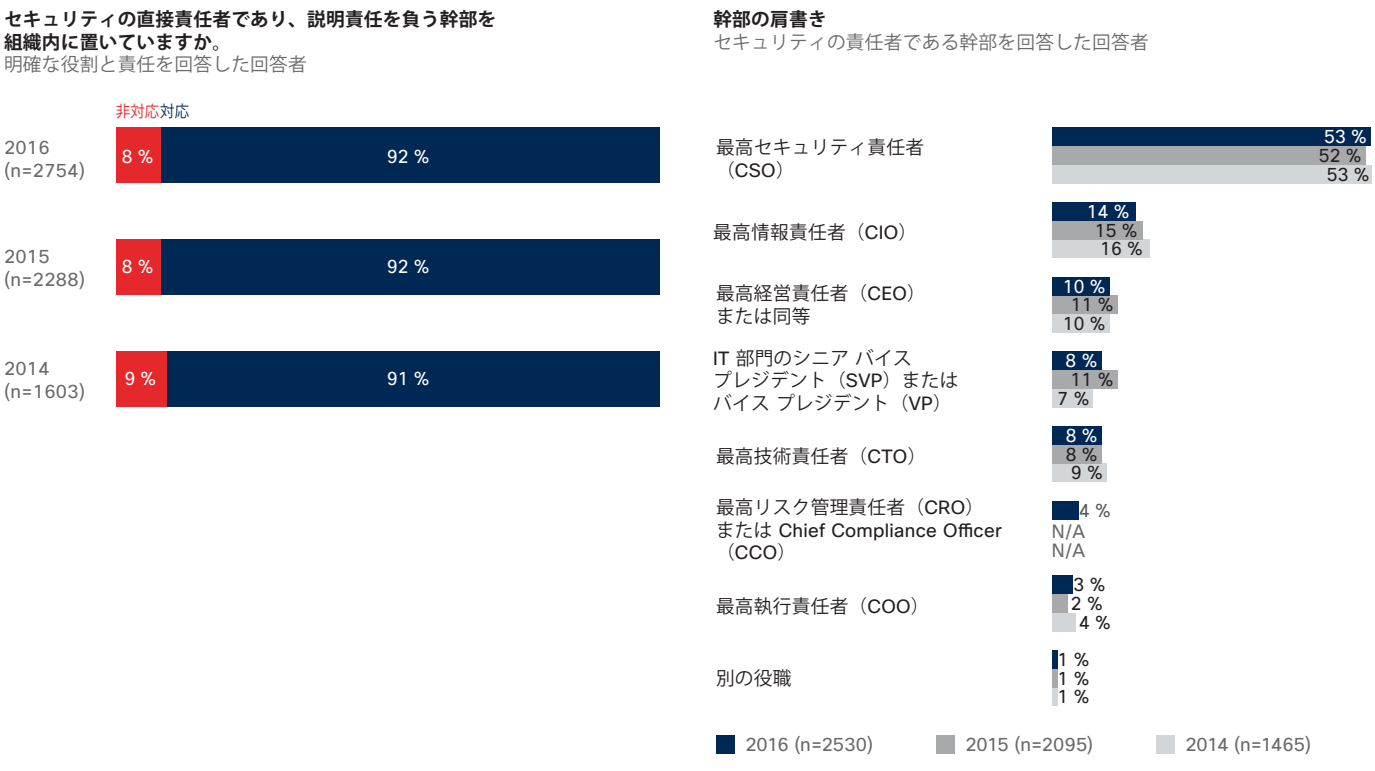
図 88 オフプレミスのプライベート クラウド、サードパーティ マネージド オンプレミス ホスティングの増加

ネットワークがホストされている場所	2014 (n=1727)	2015 (n=2417)	2016 (n=2887)
オンプレミス（プライベート クラウドの一部）	50 %	51 %	50 %
オンプレミス	54 %	48 %	46 %
オンプレミス（ただし外部サードパーティが管理）	23 %	24 %	27 %
オフプレミスのプライベート クラウド	18 %	20 %	25 %
オフプレミスのパブリック クラウド	8 %	10 %	9 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

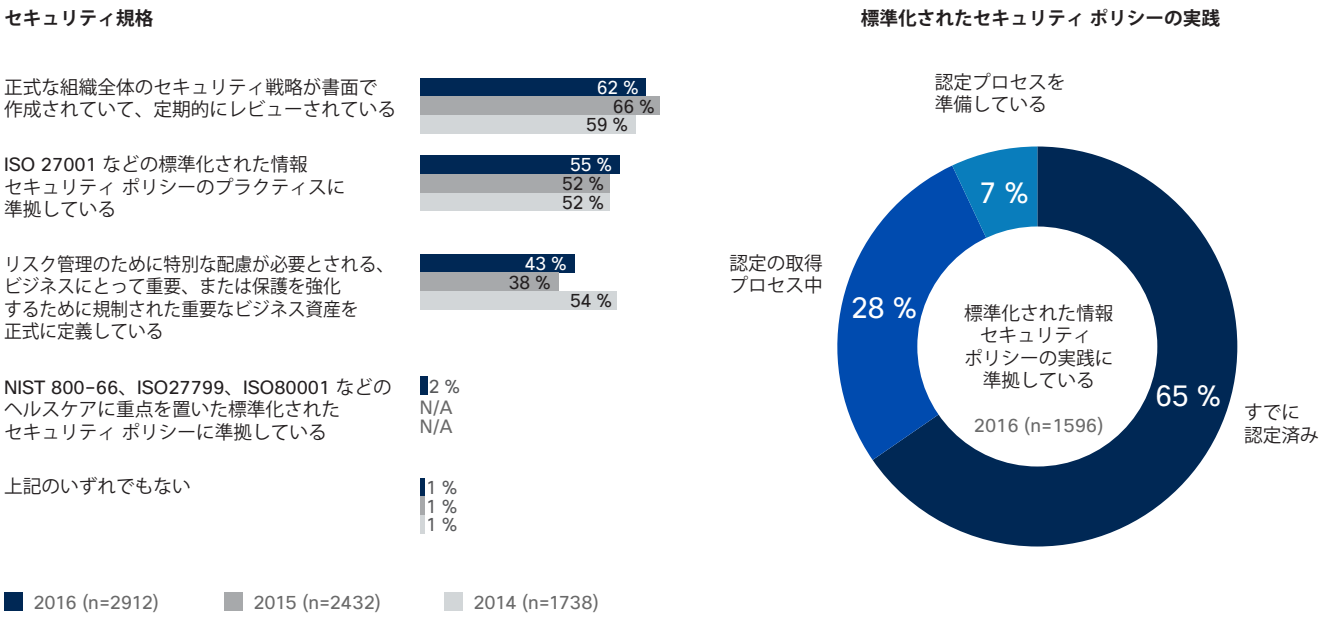
運用、ポリシー、手順、および機能

図 89 セキュリティ エグゼクティブを有する企業の割合



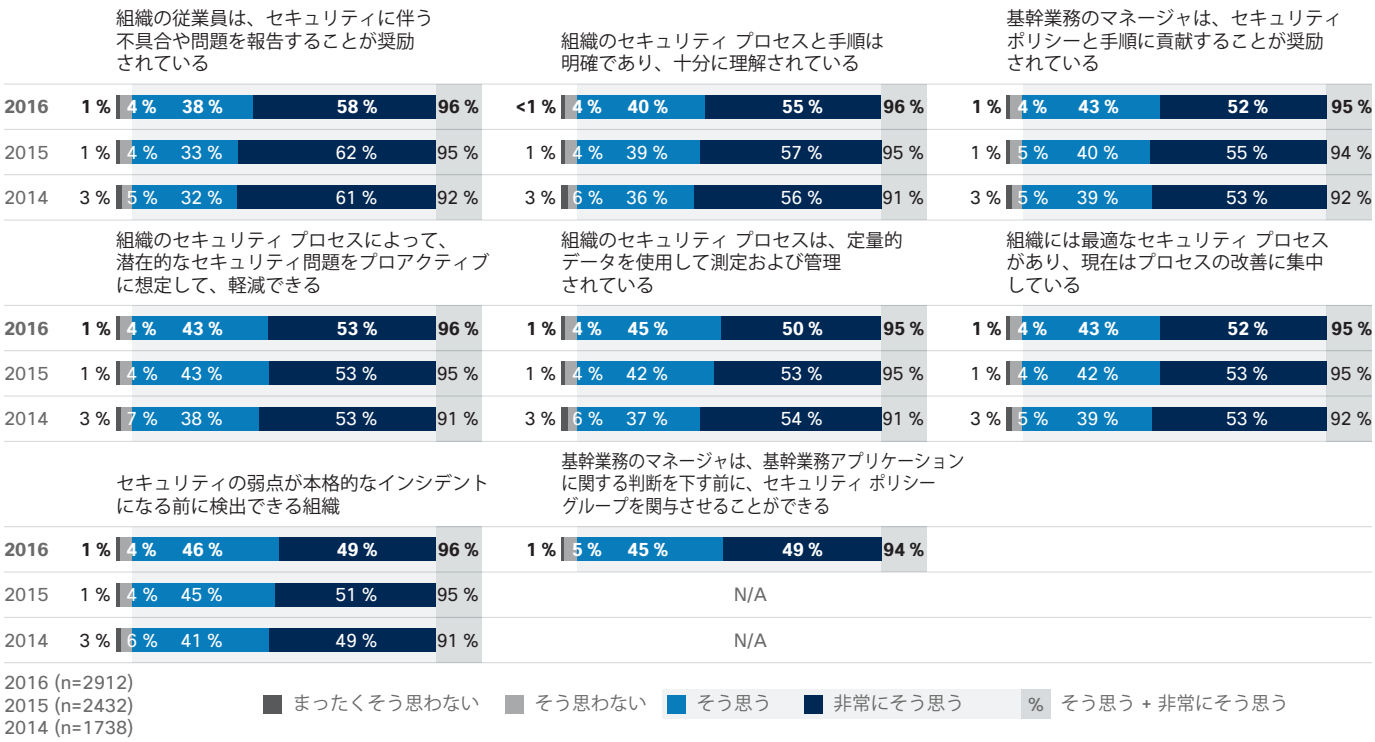
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 90 正式な組織全体のセキュリティ戦略があり、標準化されたセキュリティ ポリシーを実践している企業の割合



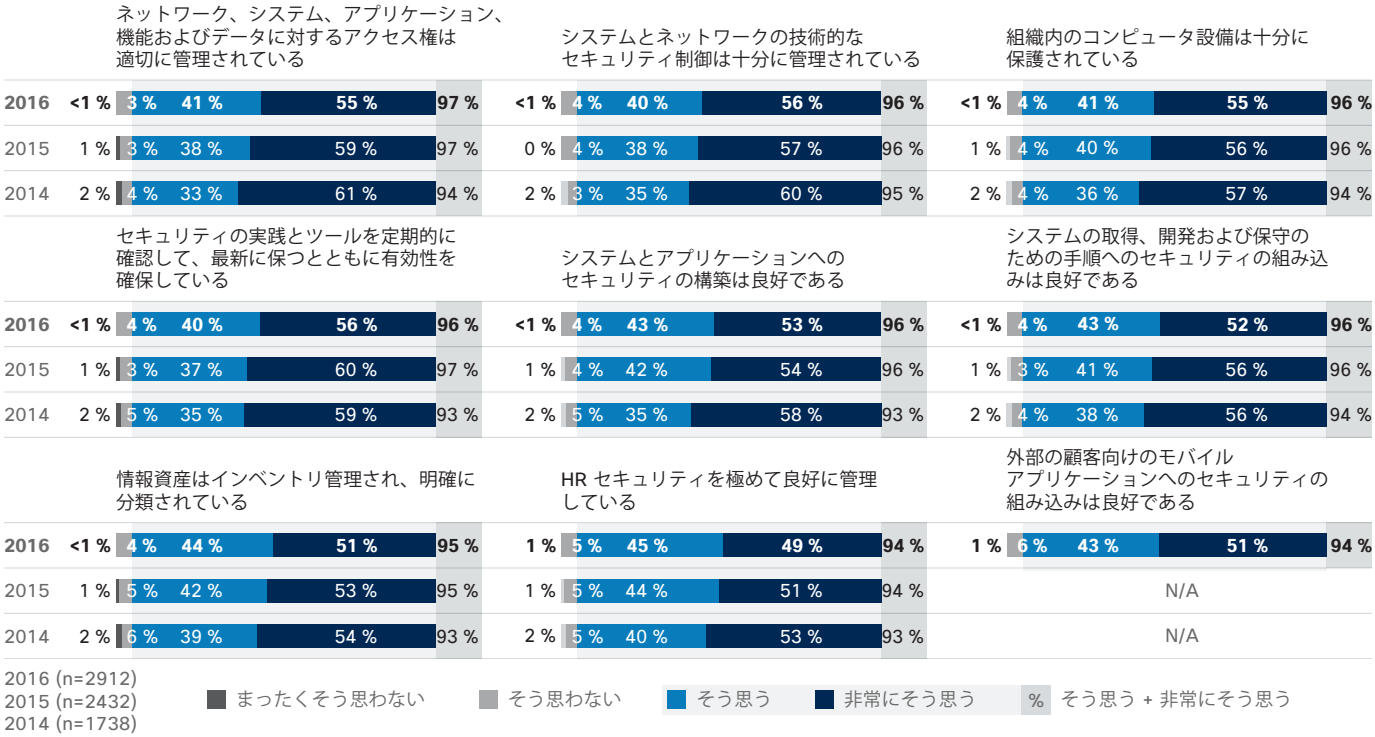
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 91 セキュリティ プロセスの説明に強く同意した回答者の割合



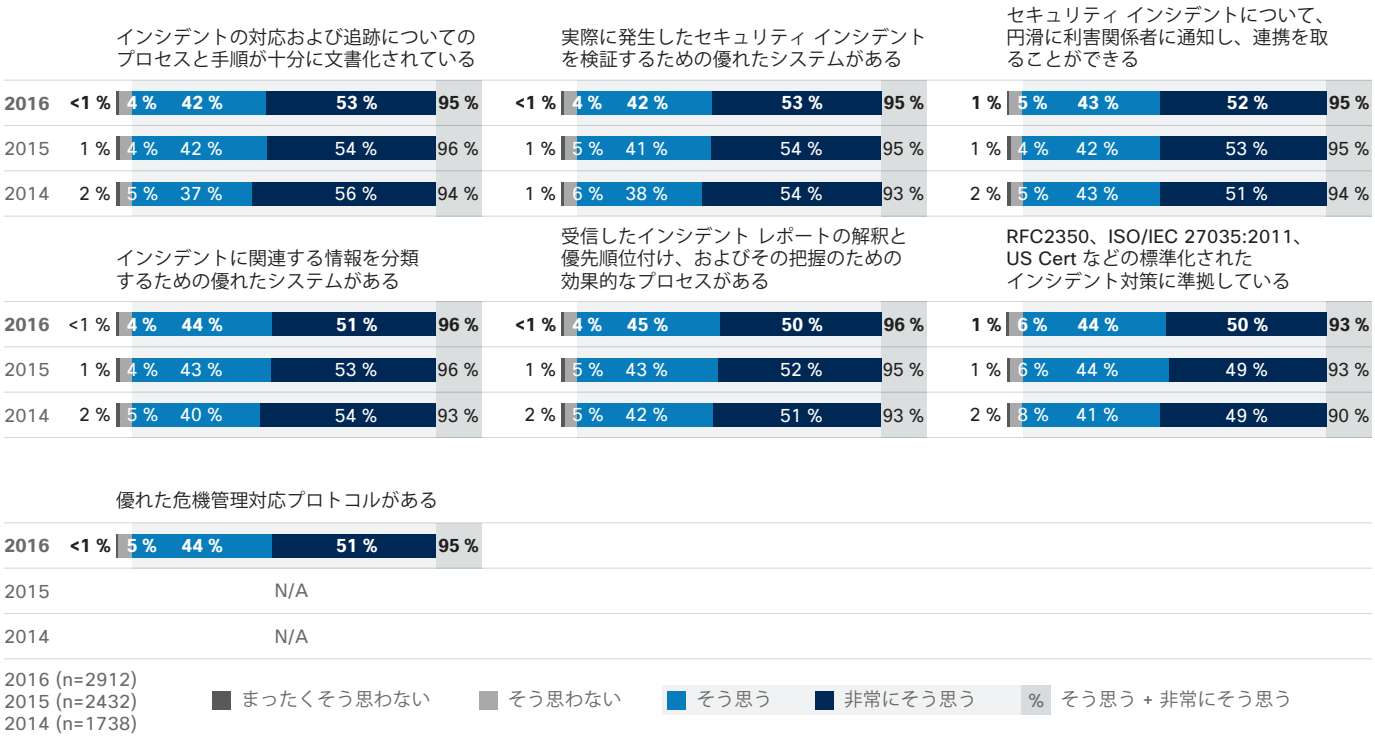
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 92 セキュリティ プロセスの説明に強く同意した回答者の割合



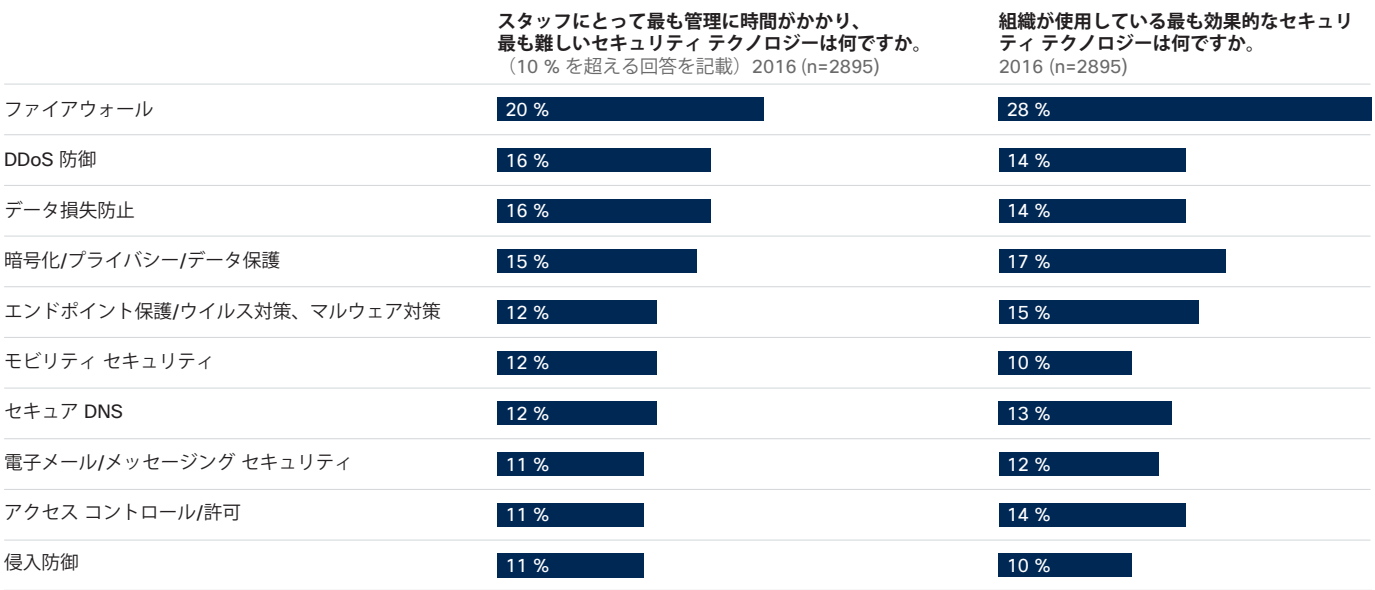
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 93 セキュリティ制御の説明に強く同意した回答者の割合



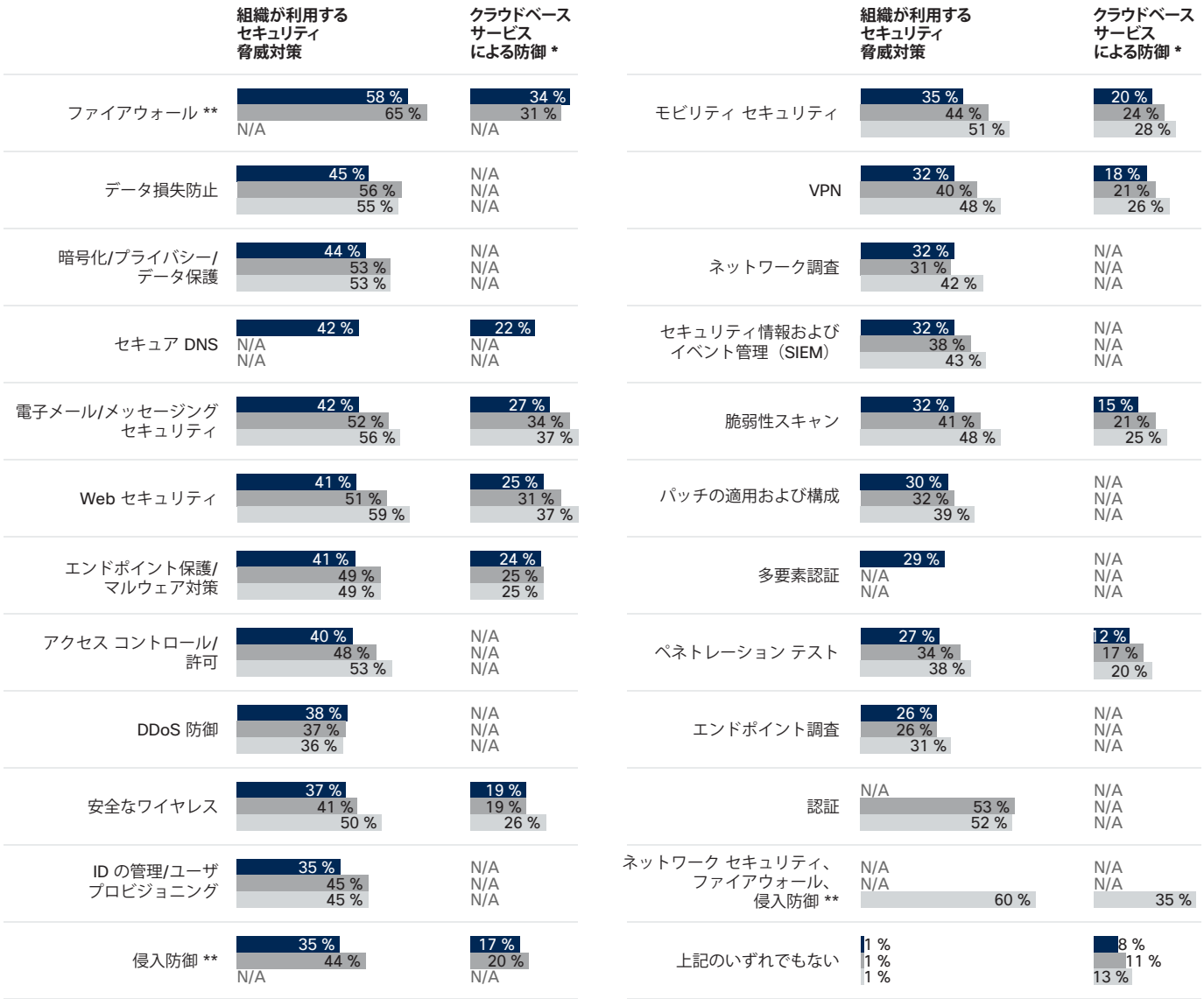
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 94 セキュリティ テクノロジーの管理と有効性



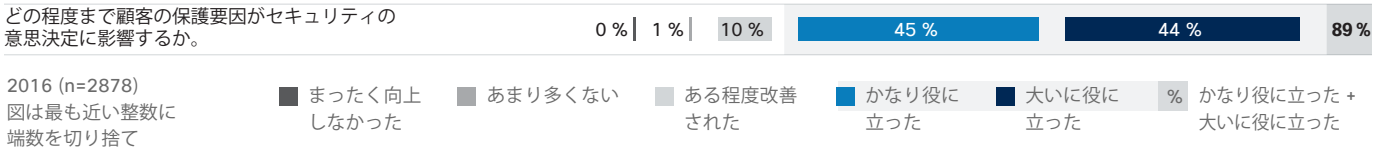
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 95 セキュリティに対する脅威対策の前年比使用率



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

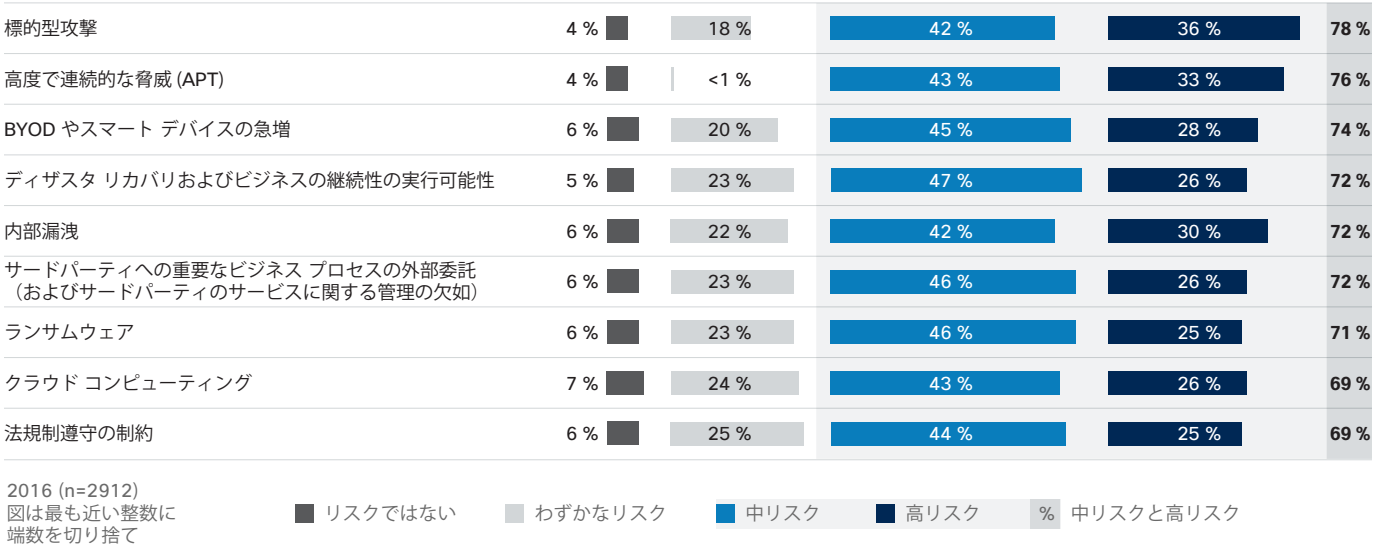
図 96 セキュリティに関する意思決定で顧客の保護を考慮する程度



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

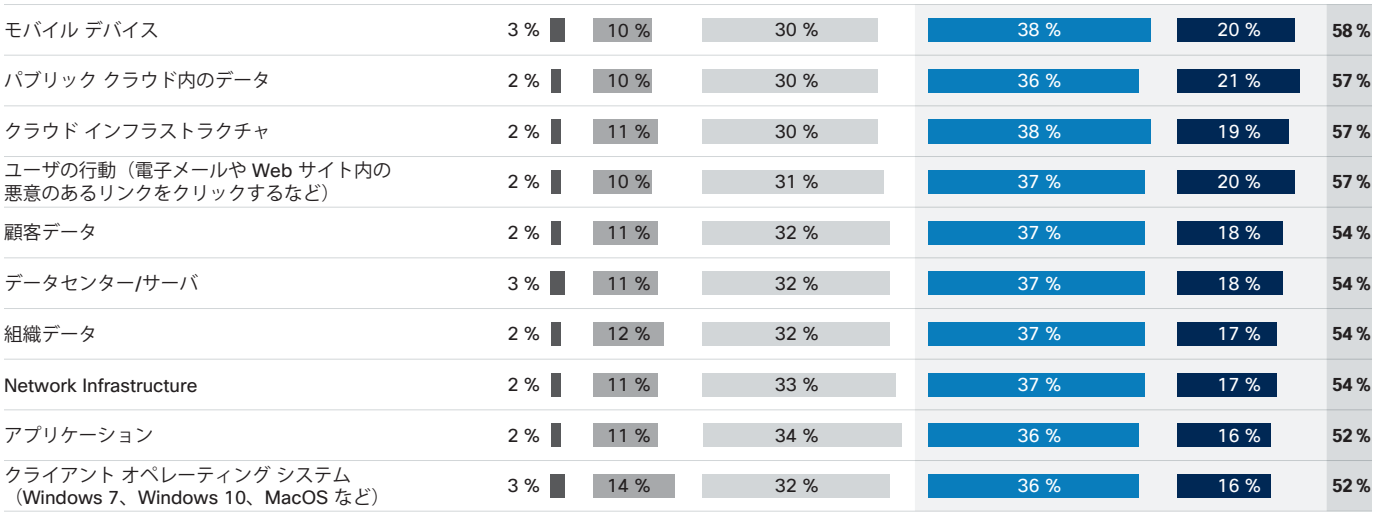
リスクと脆弱性

図 97 サイバー攻撃に関連する IT セキュリティ担当者の最大の懸念材料の原因



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 98 サイバー攻撃に関連するセキュリティ プロフェッショナルの最大の懸念材料の原因



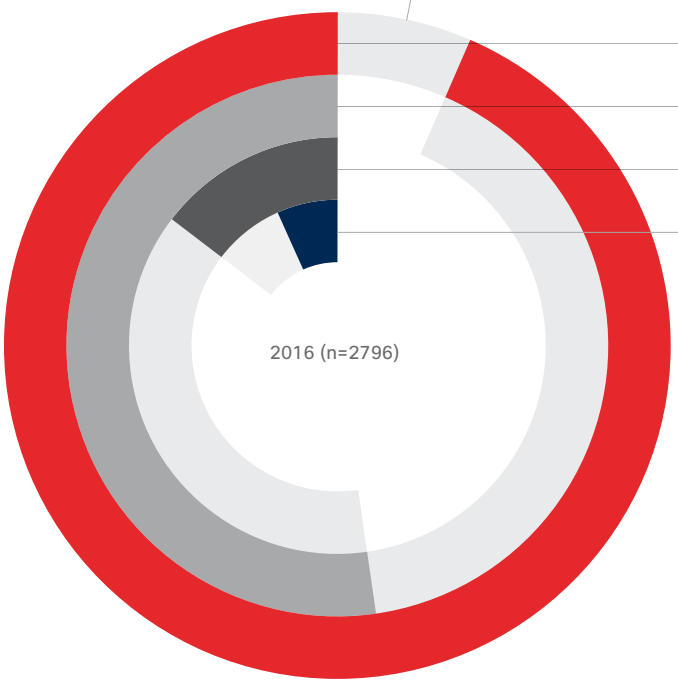
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 99 セキュリティ チームの取り組み内容の分布

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

インシデント対応

図 100 調査または修正が実施されるセキュリティ アラートの割合



7 %	セキュリティ アラートを未経験
93 %	セキュリティ アラートを経験
56 %	調査済みのアラート
28 %	調査済みアラートに対する正規アラートの割合
46 %	修復済みの正規アラート

組織で毎日確認されているアラートの平均数	
5K 未満	50 %
5K ～ 10K	15 %
10K ～ 50K	11 %
50K ～ 100K	8 %
100K ～ 150K	6 %
150K 超	4 %

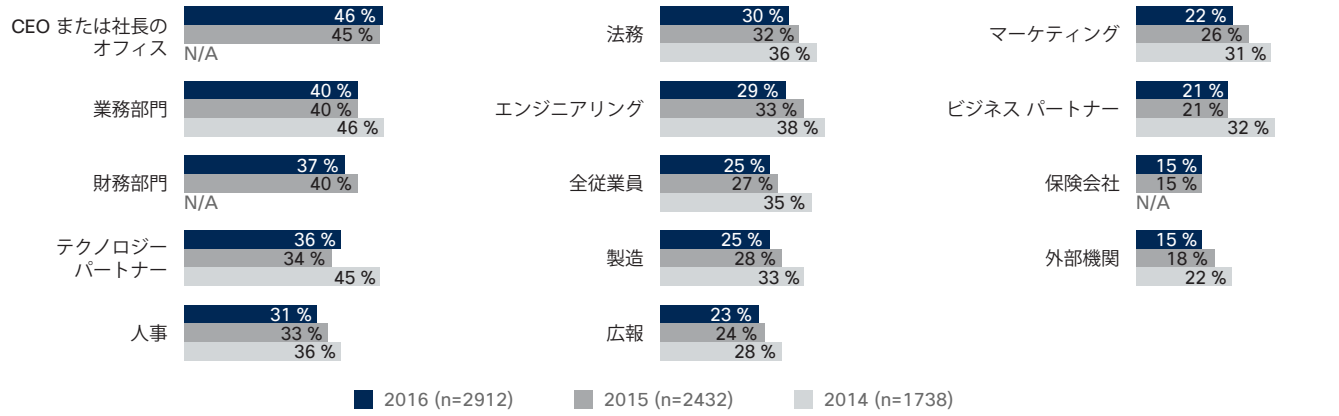
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 101 セキュリティ侵害を検出するまでの平均時間

	2016 (n=2860)
8 時間未満	43 %
9 ～ 24 時間	25 %
25 ～ 48 時間	15 %
3 日以上 1 週間未満	7 %
1 ～ 2 週間	5 %
3 週間～ 1 ヵ月	3 %
1 ～ 3 ヵ月	1 %
4 ヵ月以上 1 年未満	1 %
1 年以上	0 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 102 インシデントの際に通知を受けるグループ



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 103 組織がセキュリティ パフォーマンスの評価に使用する KPI

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 104 侵害されたシステムを分析するためのプロセスの前年比の使用率

侵害を受けたシステムの分析プロセス	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
ファイアウォール ログ	61 %	57 %	56 %
システム ログ分析	59 %	53 %	50 %
ネットワーク フロー分析	53 %	49 %	49 %
マルウェアまたはファイルの回帰分析	55 %	48 %	47 %
レジストリ分析	50 %	47 %	43 %
フル パケット キャプチャ分析	47 %	38 %	40 %
IOC 検出	38 %	35 %	38 %
ディスク調査	40 %	36 %	36 %
相互に関連するイベント/ログの分析	42 %	37 %	35 %
メモリ調査	41 %	34 %	34 %
外部インシデントの対応/分析チーム	37 %	33 %	34 %
上記のいずれでもない	2 %	1 %	1 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 105 セキュリティ インシデントの原因を排除するためのプロセスの前年比の使用率

セキュリティ インシデントの原因を排除するためのプロセス	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
悪意のあるアプリケーションの検疫または削除	58 %	55 %	52 %
根本原因の分析	55 %	55 %	51 %
悪意のあるソフトウェアの通信の停止	53 %	53 %	48 %
監視の強化	52 %	48 %	48 %
ポリシーのアップデート	51 %	47 %	45 %
侵害を受けたアプリケーションの通信の停止	48 %	47 %	43 %
長期的な修復の開発	47 %	40 %	41 %
前の状態へのシステムの再イメージ化	45 %	41 %	39 %
上記のいずれでもない	2 %	1 %	1 %

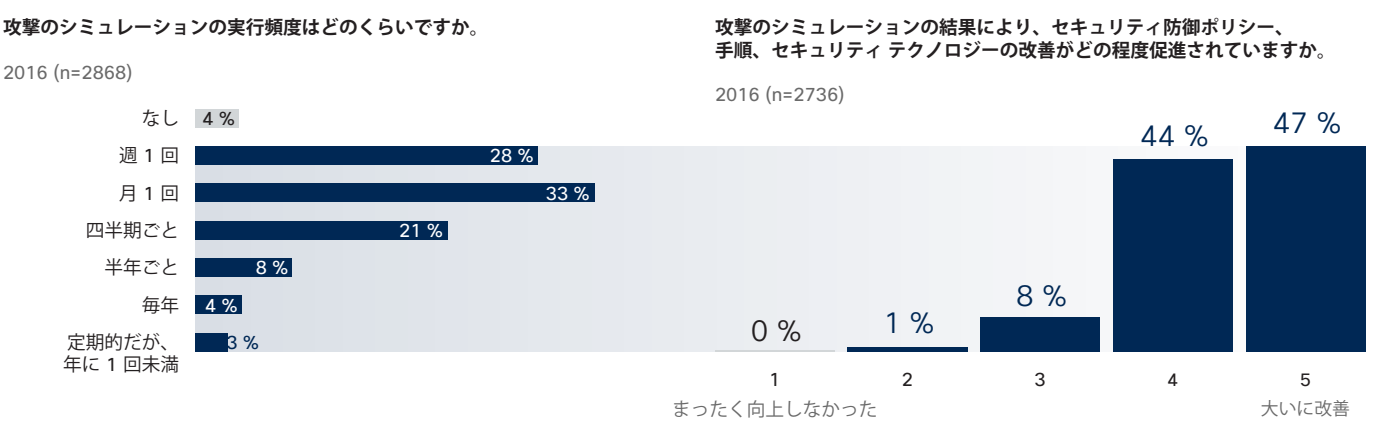
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 106 影響を被ったシステムを復元するためのプロセスの前年比の使用率

影響を受けたシステムの復旧プロセス	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
インシデント後に特定された弱点に基づいて、追加または新規の検出および管理を実施している	60 %	56 %	56 %
インシデント前のバックアップから復旧している	57 %	59 %	55 %
脆弱性を持つと見なされたアプリケーションにパッチを適用し、更新している	60 %	55 %	53 %
差分復旧（インシデントによって発生した変更を除去）	56 %	51 %	50 %
ゴールド イメージ復旧	35 %	35 %	34 %
上記のどれにも当てはまらない	2 %	1 %	1 %

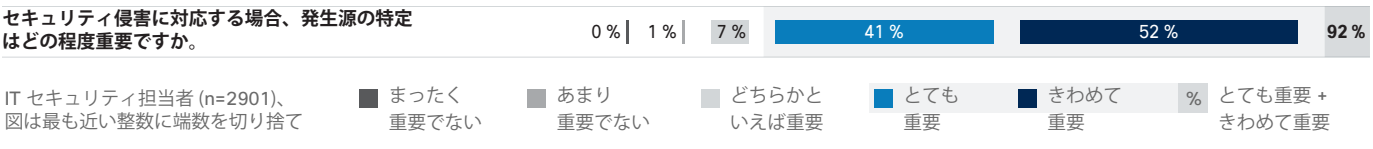
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 107 攻撃シミュレーション：セキュリティ対策の改善を促進する頻度と範囲



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

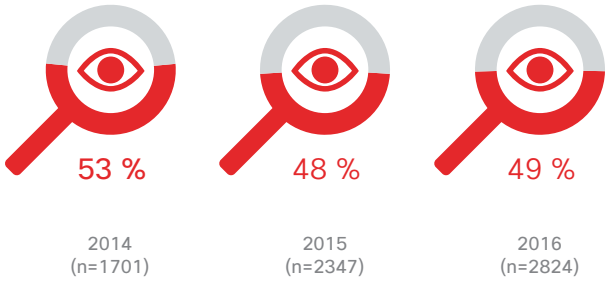
図 108 セキュリティ侵害の発生源を特定することの重要性



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

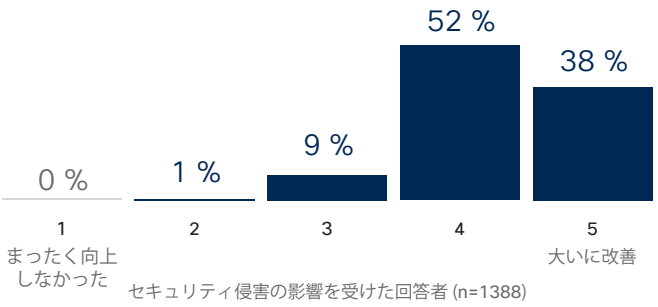
侵害とその影響

図 109 公共のセキュリティ侵害を経験した組織の割合



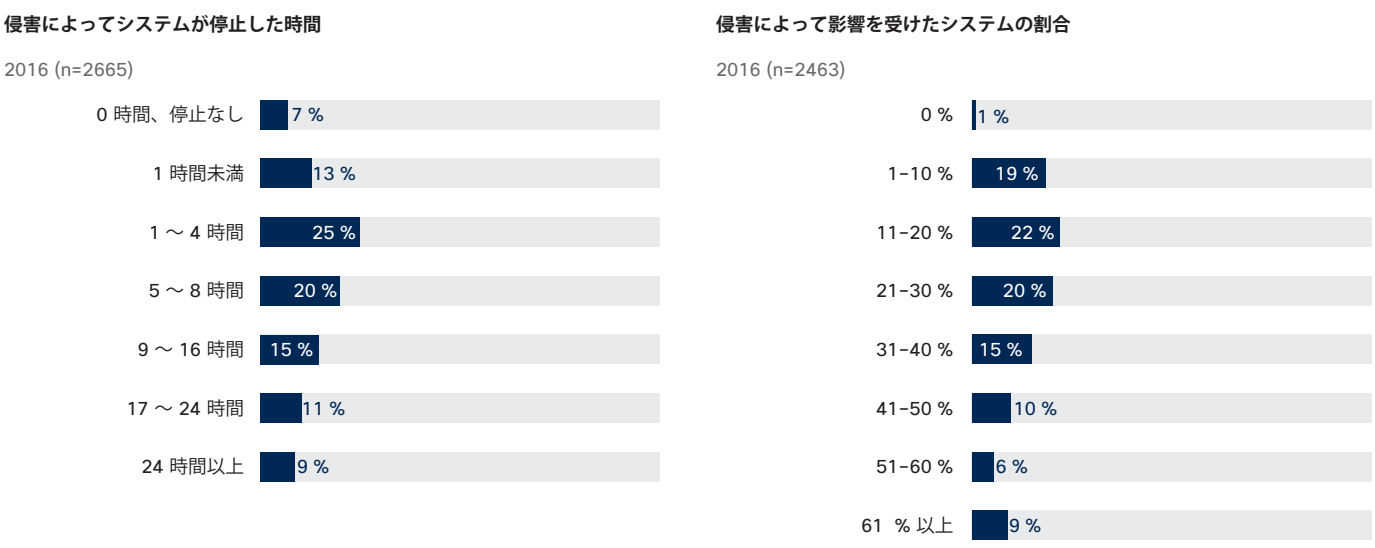
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 110 侵害によって、セキュリティに対する脅威対策のポリシー、手順、テクノロジーの機能はどの程度改善されたか。



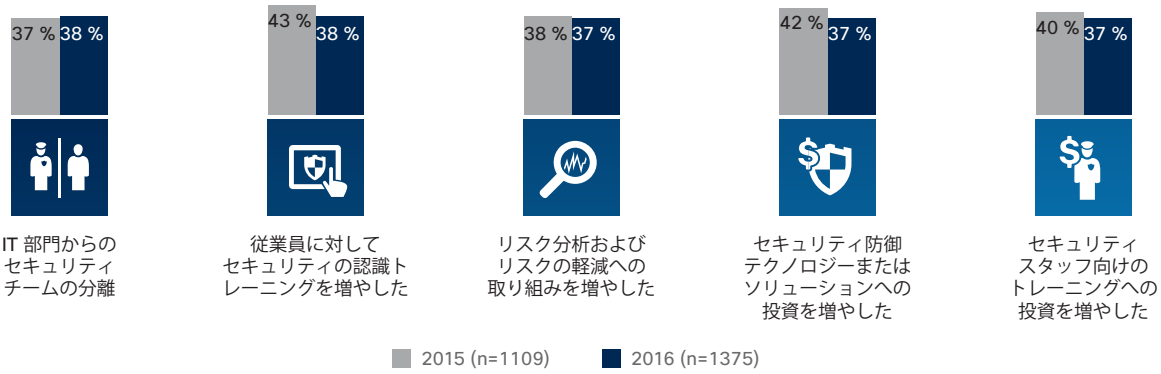
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 111 セキュリティ侵害によるサービス停止の長さと範囲



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 112 セキュリティ侵害から企業を保護するために実施した改善内容



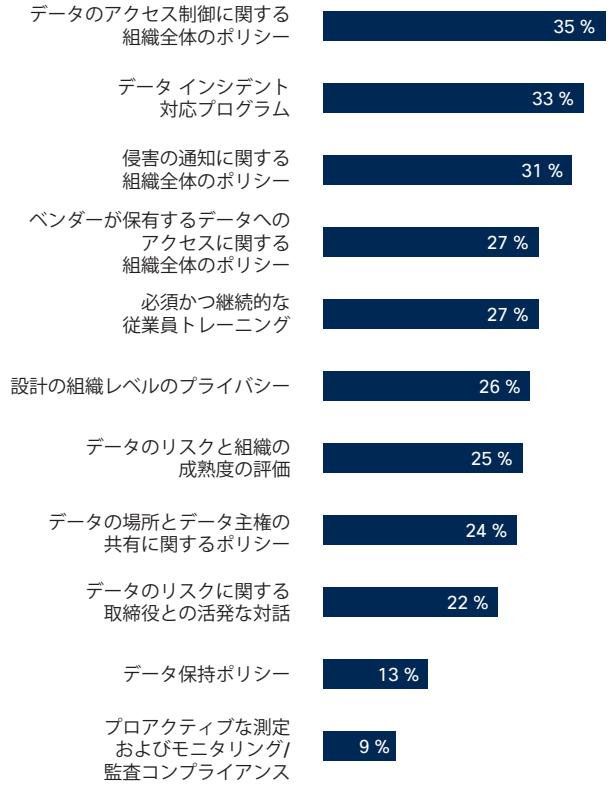
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

ベンダーの選択と期待

図 113 ベンダーにとってのデータ保護とプライバシーの重要性

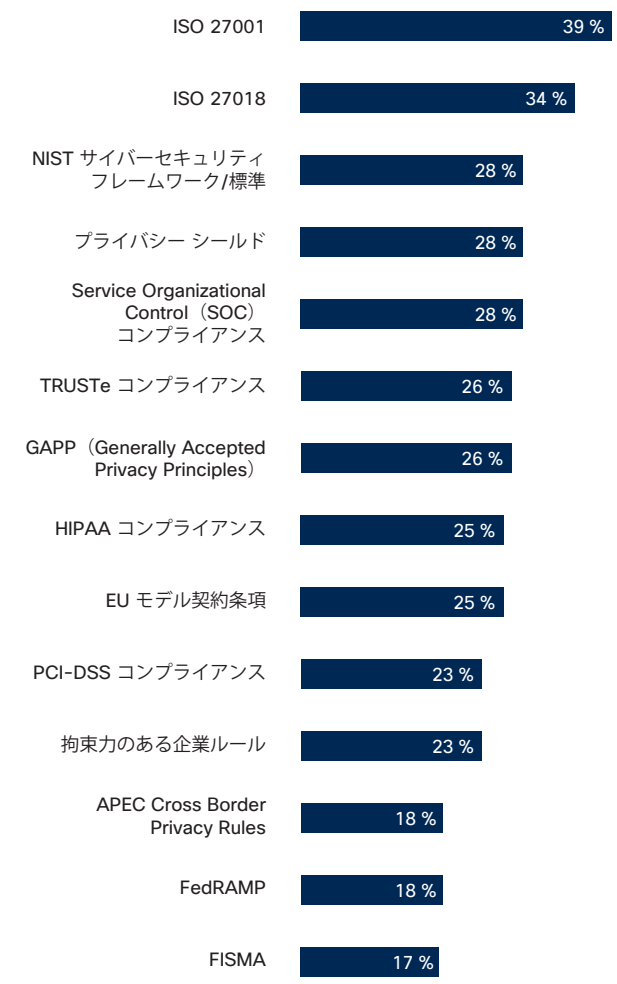
ベンダーが備えるべき最も重要なデータ保護とプライバシーのプロセスおよびポリシーは何ですか。

2016 (n=2912)



御社と協力するためにベンダーに必要とされるデータ保護、プライバシーの標準および認定は何ですか。

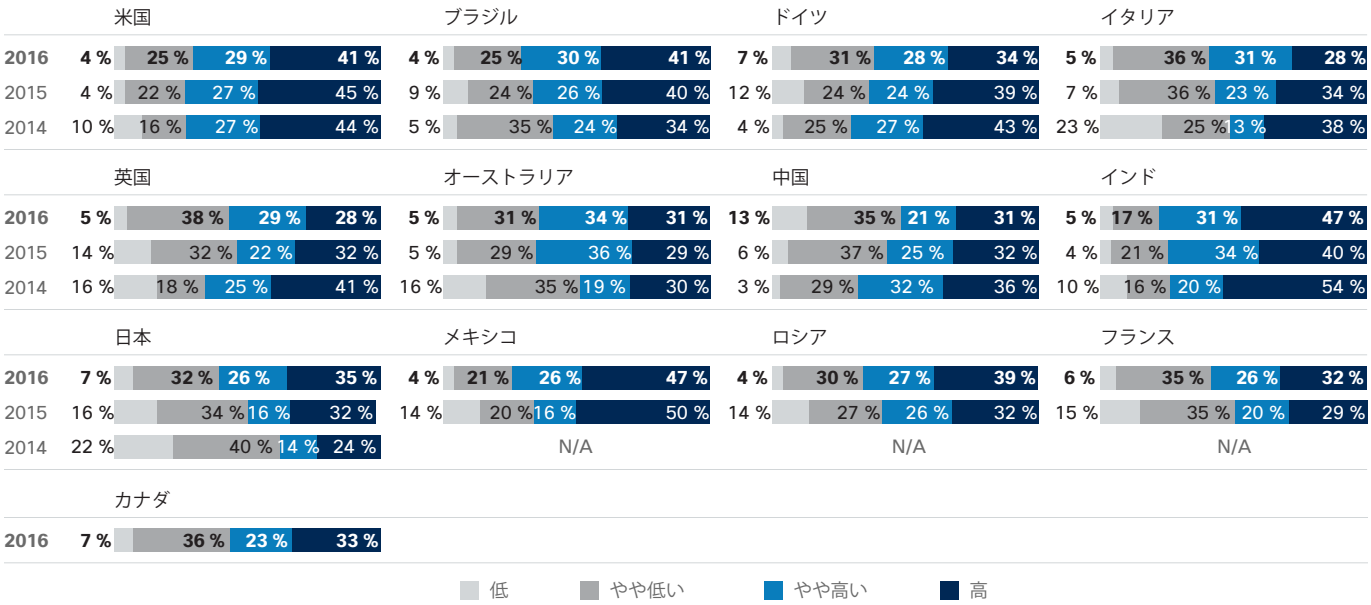
2016 (n=2870)



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

セキュリティ能力成熟度モデル

図 114 国別のセキュリティの成熟度

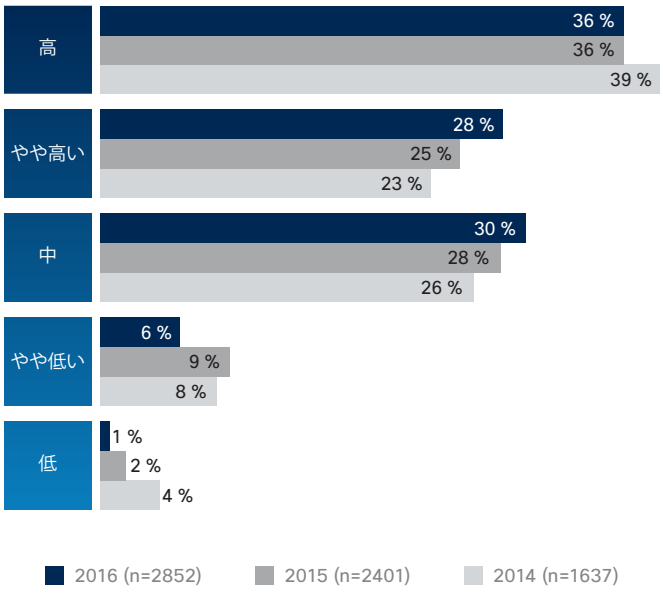


出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 115 成熟度モデルはセキュリティ プロセスに基づいて組織をランク付ける

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 116 成熟度モデルのセグメントのサイジング

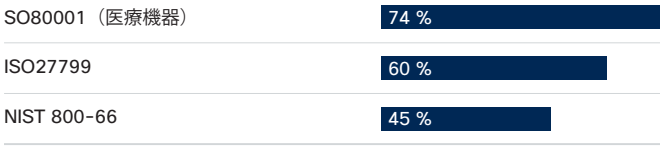


出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

業界固有

図 117 標準化されたセキュリティ ポリシーを実装した医療ビジネスの割合

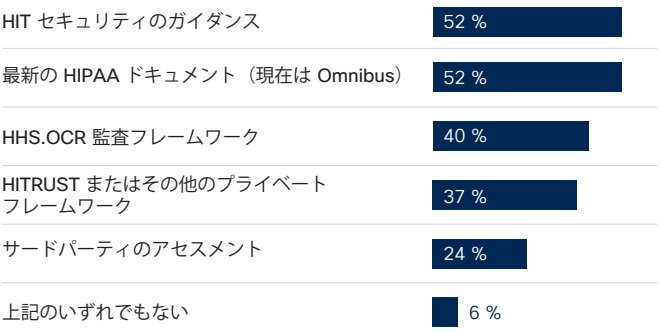
実装済みの標準化されたセキュリティ ポリシー
医療機関固有の情報セキュリティ ポリシーのプラクティスに準拠している医療機関（2016 年、n=65）



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 118 医療機関が HIPAA プライバシー ルールに対する自社の状況を測るために使用するリソース

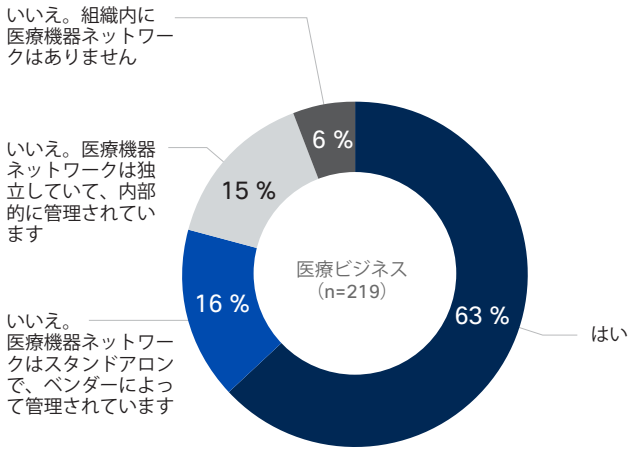
HIPAA のプライバシー ルールとセキュリティに照らして自社を測定するために使用しているリソースはどれですか。
医療ビジネス 2016 (n=219)



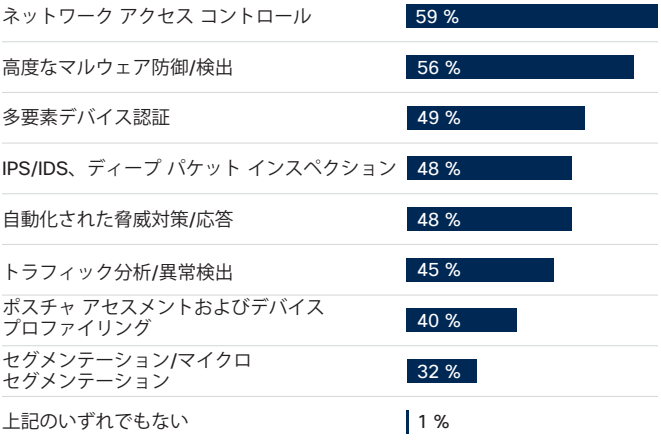
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 119 医療機器のネットワークを備えた医療ビジネスの中で最も一般的なセキュリティ対策

主要な病院ネットワークと統合された医療機器ネットワークがありますか。



医療機器ネットワークを保護するために実装しているセキュリティ対策はどれですか（ある場合）。
組織内に医療機器ネットワークがある企業（n=207）



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 120 通信業界のサンプル プロファイル

御社が主に関係している通信サブセクターはどれですか。
通信ビジネス (n=307)

通信装置	47 %
サービス プロバイダー（従来型）	33 %
ケーブル/サテライト オペレータ	11 %
メディア/ブロードキャスティング	7 %
オーバーザトップ プロバイダー（Netflix、Hulu など）	2 %

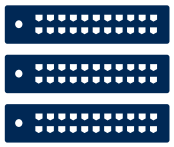
御社が顧客に提供しているサービスはどれですか。
通信ビジネス (n=308)

エンド カスタマーに提供される マネージド セキュリティ サービス	71 %
IP（テレビを含む）、モバイルなどの コア実稼働ネットワーク	60 %
企業環境	59 %
データセンター	57 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 121 通信業界のセキュリティ戦略の要因

セキュリティ戦略とプロトコルの相対的優先順位
通信ビジネス (n=308)



可用性の平均的割合

34 %

可用性：データへの信頼性の高いアクセスを保証

機密性の平均的割合

36 %

機密性：データが適切な当事者によってのみアクセスされることを保証

整合性の平均的割合

31 %

整合性：データが正確かつ正しいことを保証

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 122 通信業界のセキュリティの優先度

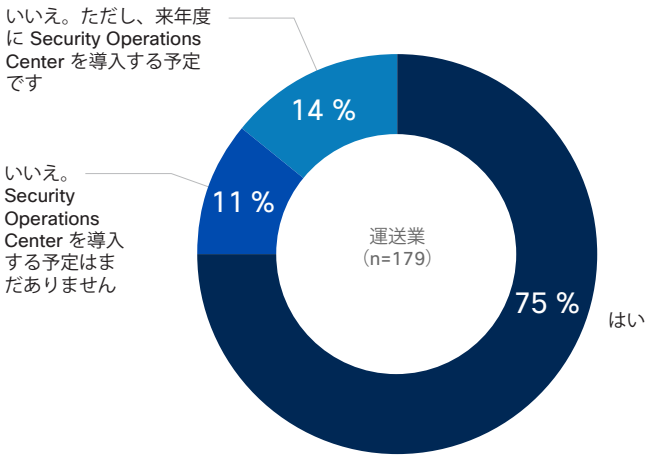
組織のセキュリティの優先順位の観点からのランク
通信ビジネス (n=308)

	1 番にランク付け	2 番にランク付け	3 番にランク付け	4 番にランク付け
データセンターのセキュリティ保護	34 %	21 %	24 %	22 %
高可用性 IP およびモバイル サービスを提供するコア実稼働ネットワーク	26 %	21 %	29 %	24 %
マネージド セキュリティ サービスの提供	21 %	30 %	19 %	30 %
エンタープライズ ネットワークと内部データ	20 %	28 %	29 %	24 %

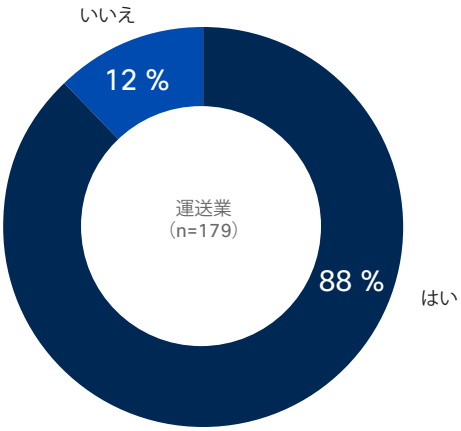
出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 123 輸送業界のサンプル プロファイル

御社は Security Operations Center（SOC）を利用していますか。



御社はセキュリティ標準化団体や業界団体に参加していますか。



御社が主に関係している運輸サブセクターはどれですか。
運送業（n=180）

運輸/物流	54 %
公共交通機関	11 %
鉄道	9 %
道路	9 %
航空	7 %
海上	5 %
車両	5 %

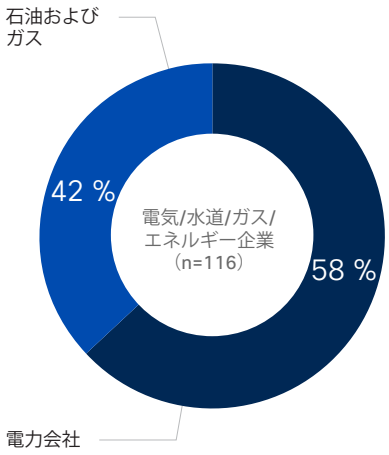
担当しているセキュリティ分野は次のうちどれですか。
運送業（n=180）

業務テクノロジーのセキュリティ	84 %
重要インフラのセキュリティ	71 %
車両のセキュリティ	43 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 124 公益事業/エネルギー業界のサンプル プロファイル

御社が主に関係している電気/水道/ガス/エネルギーのサブセクターはどれですか。



サイバーセキュリティ インシデントに対する会社の対応計画をテストするために、どの程度の頻度で訓練を実施していますか。

6 ヵ月ごとに一度	55 %
年に一度	37 %
2 年ごとに一度	6 %
めったにない	2 %
なし	0 %

電気/水道/ガス/エネルギー企業（n=116）

ドリルや訓練を実施する際に参加する当事者は誰ですか。

セキュリティ パートナー	84 %
内部のセキュリティ担当者以外の人員	69 %
ビジネス パートナー	64 %
ファースト レスポンダ	33 %
地元または州の機関	31 %
連邦政府機関	26 %
その他のユーティリティ プロバイダー	20 %
上記のいずれでもない	1 %

電気/水道/ガス/エネルギー企業（n=116）

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

図 125 金融サービス業界のサンプル プロファイル

御社が主に関係している金融サービス サブセクターはどれですか。

金融市場	52 %
リテール バンキング	25 %
保険	23 %

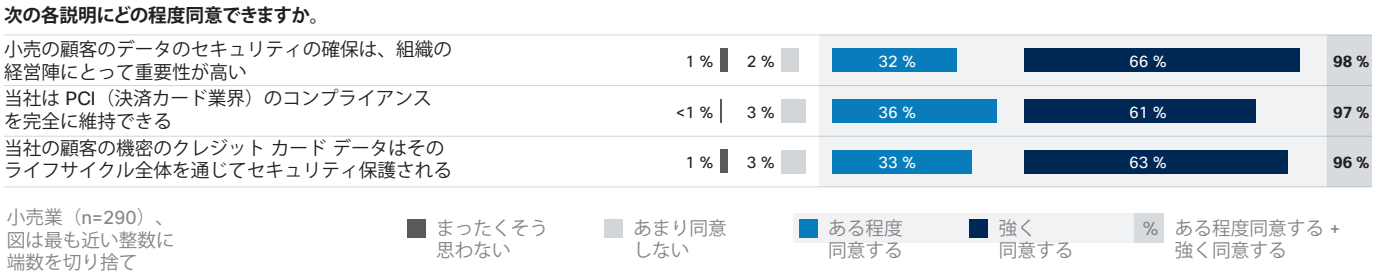
金融サービス ビジネス（n=509）
図は最も近い整数に端数を切り捨て

以下のトレンドによる影響をセキュリティがどの程度受けていると思いますか。

	まったく向上しなかった			大いに改善		%	上位 2つの選択肢
デジタル ビジネス	1 %	1 %	10 %	41 %	47 %		88 %
FinTech	0 %	2 %	10 %	46 %	42 %		88 %
DevOps	0 %	1 %	13 %	47 %	39 %		85 %
BiModal IT	0 %	2 %	15 %	48 %	35 %		82 %

出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

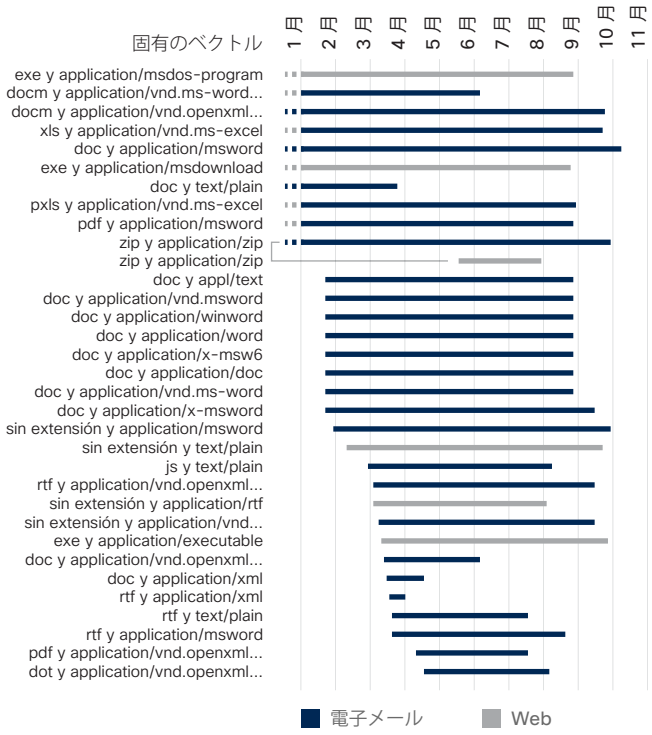
図 126 小売業界のデータ セキュリティ



出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

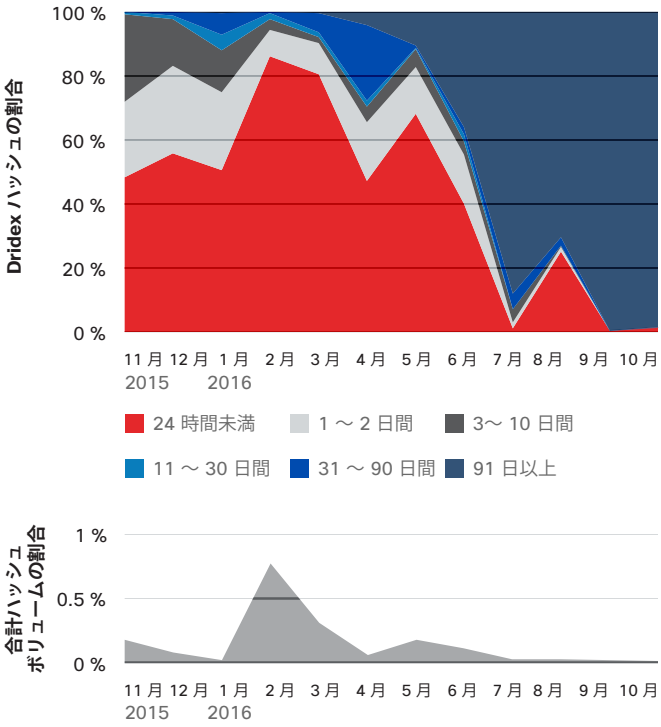
マルウェア ファミリ

図 127 Dridex のファイル拡張子と MIME の組み合わせ（Web および電子メール ベクトル）



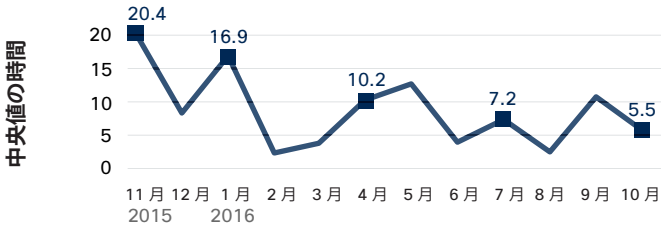
出典：シスコ セキュリティ リサーチ

図 128 Dridex マルウェア ファミリのハッシュ年齢と 1 ヵ月あたりに確認された全ハッシュ ボリュームの割合



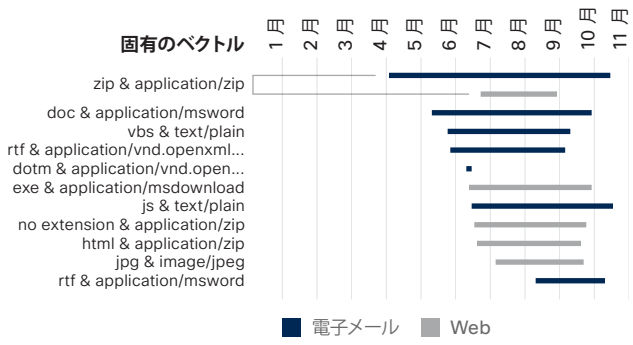
出典：シスコ セキュリティ リサーチ

図 129 Dridex マルウェア ファミリの TTD



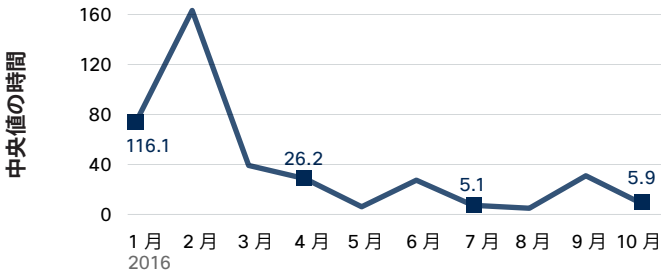
出典：シスコ セキュリティ リサーチ

図 130　脅威ファミリのファイル拡張子と MIME の組み合わせ、および Cerber ペイロードにつながり、Cerber ペイロードを含む指標（Web および電子メール ベクトル）



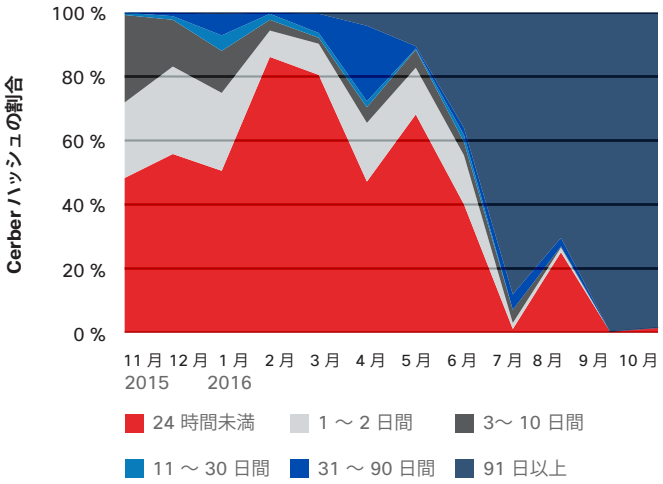
出典：シスコ セキュリティ リサーチ

図 131　Cerber マルウェア ファミリの TTD



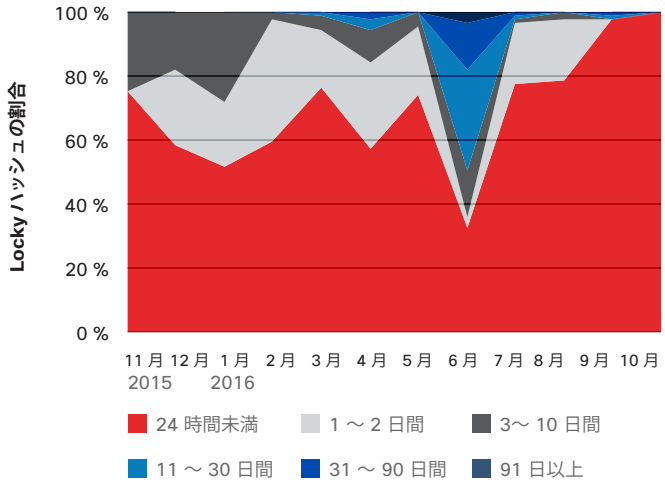
出典：シスコ セキュリティ リサーチ

図 132　Cerber マルウェア ファミリのハッシュ年齢と 1 ヵ月あたりに確認された全ハッシュ ボリュームの割合



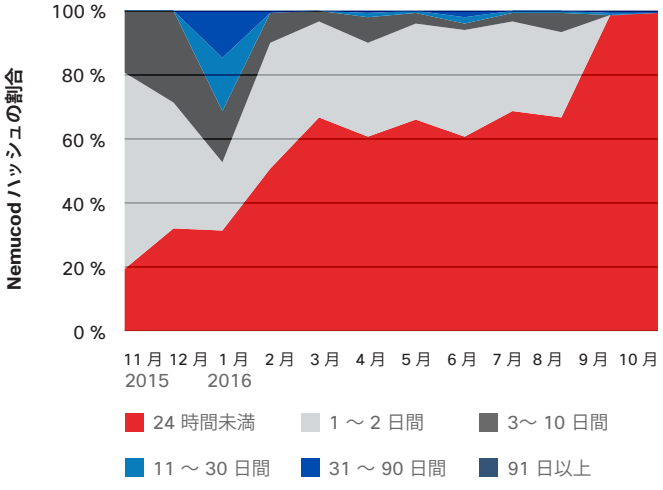
出典：シスコ セキュリティ リサーチ

図 133　1 ヵ月あたりの Locky マルウェア ファミリのハッシュ年齢



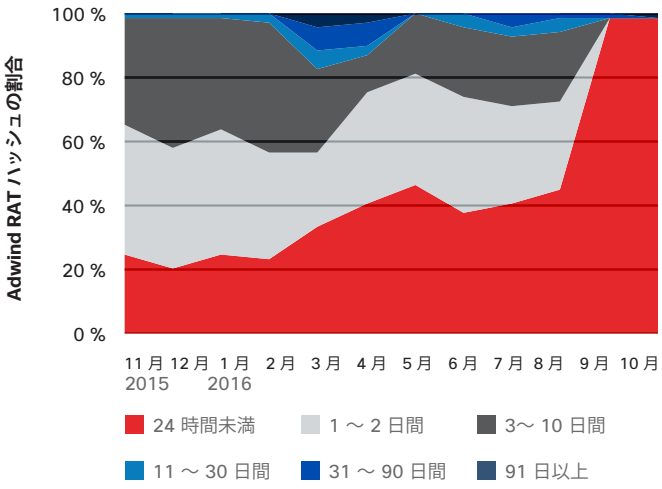
出典：シスコ セキュリティ リサーチ

図 134　1 ヵ月あたりの Nemucod マルウェア ファミリのハッシュ年齢



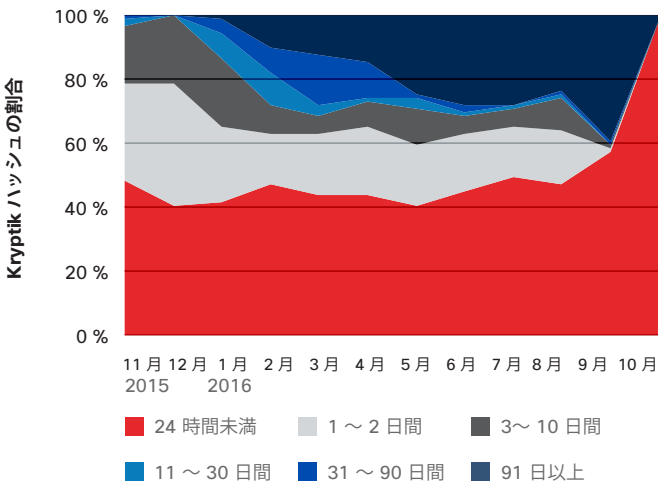
出典：シスコ セキュリティ リサーチ

図 135　1 ヵ月あたりの Adwind RAT マルウェア ファミリのハッシュ年齢



出典：シスコ セキュリティ リサーチ

図 136　1 ヵ月あたりの Kryptik マルウェア ファミリのハッシュ年齢



出典：シスコ セキュリティ リサーチ

グラフィックをダウンロード

このレポートのすべてのグラフィックは、次の場所からダウンロードできます：
www.cisco.com/go/acr2017graphics

更新情報と修正

このレポートの情報の更新情報と修正内容を確認するには、次の場所を参照してください：
www.cisco.com/go/acr2017errata

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

17.03