



Cisco 2016 年次セキュリティレポート



概要

セキュリティ プロフェッショナルは保護戦略を見直さなくてはなりません。

攻撃する側も守る側も開発を続けるため、テクノロジーと戦術をますます高度化しています。その中で、攻撃側は強力なバックエンド インフラストラクチャを構築し、それにより活動を開始し展開しています。オンライン犯罪者は、被害者から金銭を巻き上げ、データや知的財産を盗みながらも検出をかくぐる手口を高度化させています。

2016 年シスコ年次セキュリティレポートでは、シスコ セキュリティ リサーチによる調査、洞察、および見解を示し、豊富なツールを次々と利用する攻撃者を検出および阻止する上で、防御側が直面している課題を取り上げます。レポートはまた、Level 3 Threat Research Labs などの外部の専門家の調査を紹介し、現在の脅威の傾向を明らかにしようと試みています。

シスコの研究者が集めたデータを詳細に検討することで、時間を追った変化を明らかにし、データの意味するものを洞察し、セキュリティ プロフェッショナルがどのように脅威に対応すべきか説明します。

このレポートでは、次の内容について説明します。

脅威インテリジェンス

シスコの研究者が突きとめたサイバーセキュリティの主な傾向と、Web 攻撃ベクトル、Web 攻撃方法、および脆弱性の変化について考えます。また、ランサムウェアなどの増大する脅威についての詳細も含んでいます。シスコ セキュリティ リサーチは、2015 年に確認された傾向を分析するために、グローバルなテレメトリ データを活用しました。

業界の洞察

増加する暗号化の利用や、それによる潜在的なセキュリティ リスクなど、企業に影響を及ぼすセキュリティ傾向について考えます。中小規模企業 (SMB) のネットワーク保護の仕方に存在する弱点を取り上げています。また、旧式でサポートがないかサポート期限の切れたソフトウェアにより IT インフラストラクチャを維持している企業についても調査しています。

セキュリティ機能のベンチマーク調査

シスコの 2 回目のセキュリティ機能ベンチマーク調査の結果を取り上げます。ここでは、セキュリティ プロフェッショナルが認識している自社のセキュリティの状態に注目しています。2015 年と 2014 年の調査結果を比較すると、セキュリティ最高責任者 (CSO) とセキュリティ運用 (セキュリティ担当部署) マネージャは、セキュリティ インフラストラクチャが最新状態かどうか、または攻撃を阻止できるかどうかについて、自信を失っていると感じました。しかし調査では、ネットワークを強化するために、企業がトレーニングやセキュリティ プロセスを強化していることもわかっています。この調査結果は、2016 年シスコ年次セキュリティレポートのみのものです。

将来の展望

セキュリティに影響する地政学的な状況を考察します。サイバーセキュリティに関する幹部の懸念を分析したり、セキュリティ リスクや信頼性に関する IT の意思決定者の見解を取り上げたりするなど、シスコの調査で得られた発見について検証します。また、シスコのさらなる検出時間 (TTD) 短縮について最新情報を提供し、脅威への対策として統合型脅威防御アーキテクチャに移行することの意義を説明します。

目次

エグゼクティブ サマリー	2	業界の洞察	29
主な傾向と特徴	4	暗号化: 成長著しいトレンド、防御側にとっての課題	30
獲物を逃さない: 今日のサイバー犯罪者は金儲けが最優先	7	オンライン犯罪者による WordPress サーバ アクティビティが増加	33
脅威インテリジェンス	9	老朽化するインフラストラクチャ: 10年越しの問題	35
注目のストーリー	10	「中小企業が各国のビジネスにおけるセキュリティ上の弱みに」	37
高利益を上げる大規模なエクスプロイト キットやランサムウェアの攻撃を、業界の連携によってシスコが排除	10	シスコによるセキュリティ機能のベンチマーク調査	41
業界の協調した取り組みが、インターネット最大の DDoS ボットネットの停止を支援	14	準備の兆候が見られるなかでの信頼度の低下	42
セキュリティ専門家との連携	16	将来の展望	55
ボットネットの指令: 世界の状況	17	地政学的な展望: インターネット ガバナンスの状況の不確実性	56
DNS の盲点: 指示管理に DNS を使う攻撃	19	幹部に重くのしかかるサイバーセキュリティ問題	57
脅威インテリジェンス分析	20	信頼性の調査: 企業のリスクと課題に注目	58
Web 攻撃ベクトル	20	検出時間: 時間枠を縮小し続けるための競争	60
Web 攻撃の方法	21	統合型脅威防御の 6 カ条	62
最新の脅威	23	数の力: 業界が協力することの価値	63
業界別のマルウェア出現リスク	25	シスコについて	64
Web ブロック アクティビティ: 地域別の概要	27	シスコ年次セキュリティ レポート (2016 年) の貢献者	65
		シスコ パートナーの貢献者	67
		付録	68

主な傾向と特徴

主な傾向と特徴

サイバー犯罪者は、効率と収益性の高い方法で攻撃するために、バックエンド インフラストラクチャを改良してきました。

- シスコでは、Level 3 Threat Research Labs の支援やホスティング プロバイダーである Limestone Networks の協力を得て、1 日当たり 90,000 人が被害を受け、攻撃者に年間数千万ドルの利益をもたらした、米国で最大の Angler エクスプロイト キットの動作を突きとめ、停止させました。
- シスコの研究者がこれまでに確認した、主な分散型サービス妨害 (DDoS) の 1 つである SSHPsychos (Group 93) のボットネットは、シスコと Level 3 Threat Research Labs の力を合わせた取り組みによって、著しく弱体化しました。前述の Angler の例のように、この成功は、業界が連携して攻撃に立ち向かうことの重要性を示しています。
- 悪意のあるブラウザ拡張機能は、ビジネス上のデータ漏えいの主な原因であり、広範囲に渡る問題です。調査対象の組織の 85 % 以上が、悪意のあるブラウザ拡張機能の影響を受けていると推測されます。
- 2015 年 7 月にシスコが分析した一群の組織に影響を及ぼしているボットネットの指示管理行動の大半では、Bedep、Gamarue、Miuref などの有名なボットネットが主流でした。
- 「既知の脅威」と判断されたマルウェアをシスコが分析したところ、そのマルウェアの大部分 (91.3 %) が、Domain Name Service (DNS) を使って攻撃を実行していました。DNSクエリーのレトロスペクティブ調査から、シスコは、顧客のネットワークで使用されている「不正」な DNS リゾルバを特定しました。顧客は、従業員がインフラストラクチャの一部としてそのリゾルバを使用していることに気づいていませんでした。
- Adobe Flash の脆弱性は、依然としてサイバー犯罪者に利用されがちです。しかし、ソフトウェア ベンダーは、Flash テクノロジーを通じてユーザがマルウェアにさらされる危険性を抑えようとしています。
- 2015 年の傾向を見た結果、シスコの研究者は、暗号化された HTTPS トラフィックが転換点となり、まもなくインターネットトラフィックの主流となるだろうと考えています。暗号化は消費者の保護に役立ちますが、セキュリティ製品の効果を損なうことにもなり、セキュリティ コミュニティが脅威を追跡するのが難しくなります。こうした課題に加え、一部のマルウェアは、さまざまなポートに渡って暗号化通信を開始できます。
- 攻撃者は、一般的な Web 開発プラットフォームである WordPress で作成された感染 Web サイトを犯行に利用しています。彼らはそこにサーバリソースを集め、検出を回避しています。

- 老朽化したインフラストラクチャが増えるにつれ、組織は感染に対してますます脆弱なまま取り残されます。インターネット上の 115,000 台のシスコ デバイスを分析した結果、サンプルの 92 % のデバイスが既知の脆弱性を持つソフトウェアを実行していることがわかりました。さらに、分析に含まれた現場のシスコ デバイスの 31 % が販売終了となっており、8 % が寿命を迎えていました。
- シスコの 2015 年のセキュリティ機能ベンチマーク調査では、セキュリティ責任者のセキュリティ ツールやプロセスへの安心感が、2015 年には 2014 年に比べて低くなっていることがわかりました。たとえば、2015 年には 59 % の組織がセキュリティ インフラストラクチャは「最新状態」と答えましたが、2014 年には 64 % でした。しかし、セキュリティへの懸念が高まったことで、防御力改善への動きが始まっています。
- ベンチマーク調査では、中小規模企業 (SMB) の防御策が大企業に比べて少ないことがわかっています。たとえば、2015 年には 48 % の SMB が Web セキュリティを使用していると答えましたが、2014 年には 59 % でした。また、2015 年には 29 % がパッチや構成ツールを使用していると答えましたが、2014 年には 39 % でした。こうした弱さにより、攻撃者が SMB のネットワークを侵害しやすくなり、SMB の顧客にリスクが生じる可能性があります。
- シスコは 2015 年 5 月から、ネットワーク内の既知の脅威の平均検出時間 (TTD) を、約 17 時間に短縮し、1 日かからないようにしました。これは業界の現在の概算 TTD (100 ~ 200日) をはるかに上回ります。

獲物を逃さない：
今日のサイバー犯罪者は金儲
けが最優先

獲物を逃さない： 今日のサイバー犯罪者は金儲 けが最優先

過去には、多くのオンライン犯罪者がインターネットの影に潜んでいました。また、企業のネットワークに短時間だけ侵入してエクスプロイトを実行することで、検出を逃れようとしていました。現在、大胆になったサイバー犯罪者は正規のオンラインリソースを活用しています。サーバ容量をかすめ取り、データを盗み、オンライン被害者に対して情報をたてに金銭を要求します。

こうした作戦は、防御側と攻撃側の戦いにおいて急増しています。攻撃側がオンラインで操作できそうな場所をたくさん見つけると、その影響が急激に拡大します。

このレポートで、シスコのセキュリティ研究者は、攻撃者が強固なインフラストラクチャを構築して、作戦をより強力かつ効果的にするために使う戦術を取り上げています。攻撃者は利益を上げるために、より効率的な方法を次々と採用しますが、多くの場合、サーバリソースの利用に注目しています。

ランサムウェアの急増(10 ページ参照)がよい例です。ランサムウェアは犯罪者にとって、ユーザから直接金銭を引き出せる簡単な方法です。攻撃者が 1 日当たり何万人ものユーザをほぼ中断なく攻撃する作戦を採れば、その見返りは巨額になります。作戦で利益を上げる優れた方法を考えるのに加え、攻撃者は正規のリソースを侵害の拠点としています。

一部のランサムウェア亜種の作成者やエクスプロイトの開発者は、ハッキングされた WordPress Web サイトへとトラフィックを移して、検出を回避しサーバスペースを使用しています(33 ページ参照)。SSHPsychos はシスコの研究者がこれまでに確認した中でも最大のボットネットの 1 つですが、これを利用する犯罪者は、標準ネットワーク上でほとんど何の障害もなく操作を行っていました。その行為は、シスコと Level 3 Threat Research Labs が共同で駆除しようとする対応に応じて、サービスプロバイダーがボットネット作成者のトラフィックをブロックするまで続きました。

脅威インテリジェンス

脅威インテリジェンス

シスコは、このレポートのために、テレメトリ データを世界規模で収集して分析しました。マルウェア トラフィックなど、検出された脅威に対するシスコの継続的な調査と分析は、今後起こりうる犯罪に対する洞察と脅威の検出に活用できます。

注目のストーリー

高利益を上げる大規模な 익스プロイト キットやランサムウェアの攻撃を、業界の連携によってシスコが排除

Angler 익스プロイト キットは、市場で最大かつ最も効率的な 익스プロイト キットの 1 つです。悪意のある目立つ広告や、ランサムウェアの攻撃とリンクしており、シスコの脅威研究者が過去数年に渡り詳細に監視してきた、ランサムウェアの活動の全体的な増大においても大きな要因です。犯罪者はランサムウェアを使ってユーザのファイルを暗号化し、ユーザが「身代金」(通常 300 ~ 500 ドル)を支払った後で復号キーを渡します。

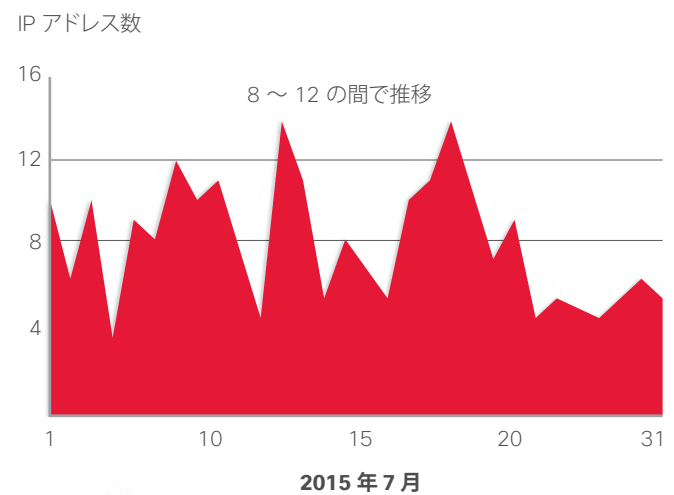
2015 年度のシスコ中間セキュリティ レポートによれば、ビットコインなどの暗号通貨や Tor などの匿名化ネットワークにより、犯罪者がマルウェア市場に参入し、素早く収益を得ることが容易になっています。ランサムウェアの人気上昇は、2つのメリットと関係があります。犯罪者にとってはメンテナンス作業が少ないことと、ユーザが暗号通貨で直接犯罪者に支払うため、迅速に収益化できることです。

シスコは Angler および関連するランサムウェアの傾向を調査する中で、この 익스プロイト キットの一部のオペレータが、極めて高い割合で、Limestone Networks が運用するサーバ上にあるワールドワイド プロキシ サーバを Angler に使用していることを突きとめました。このサーバの使い方は、シスコの研究者が最近の闇経済に発見した別の傾向、すなわち犯罪者が正規のリソースと悪意のあるリソースを取り混ぜて作戦を実行するという傾向の典型的な例です。

今回の場合、Angler をサポートする IP インフラストラクチャは大規模ではありませんでした。アクティブなシステムの 1 日当たりの数は、主に 8 ~ 12 の間で変化しました。ほとんどは 1 日アクティブになったただけでした。図 1 は、2015 年 7 月中にシスコが確認した一意の IP アドレスの数です。

シスコは、Angler のオペレータが基本的に直線的なやり方で IP アドレスを利用していき、脅威を隠して金儲けの邪魔が入らないようにしていることを発見しました。

図 1. 日付順の Angler IP アドレス (2015 年 7 月)



出典:シスコ セキュリティリサーチ

共有    

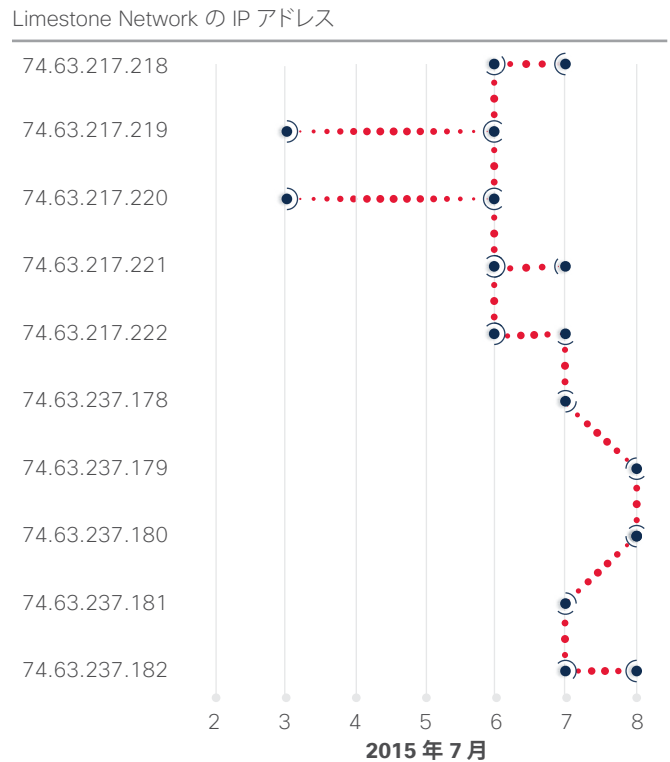
図 2 に示すように、Angler はある IP アドレス(ここでは 74.63.217.218)から始めています。システムがユーザを攻撃して、防御側で検出できる「ノイズ」を発生させると、攻撃者は次の IP アドレス(74.63.217.219)に移ります。この動作は、1 つのホスティング プロバイダーのほぼ連続する IP スペースのブロックすべてに続けられます。

シスコは IP 情報を検証して、それらの IP アドレスに関連付けられた自律システム番号 (ASN) とプロバイダーを特定しました。その結果、Angler 関連のトラフィックのほとんどが 2 つの正規ホスティング プロバイダー、つまり Limestone Networks および Hetzner が運用するサーバから来ているとわかりました(図 3)。7 月のトラフィック量全体のほぼ 75 % に上ったのです。

シスコはまず、Angler のグローバルな活動を最もホスティングしていると思われた Limestone Networks に連絡し、Limestone は協力の機会を受け入れました。Limestone では毎月非常にたくさんのクレジットカードの支払い拒否を処理していたのですが、これは攻撃者が偽名で不正なクレジットカードを使い、何千ドルにも相当するたくさんのサーバをランダムに購入していたからです。

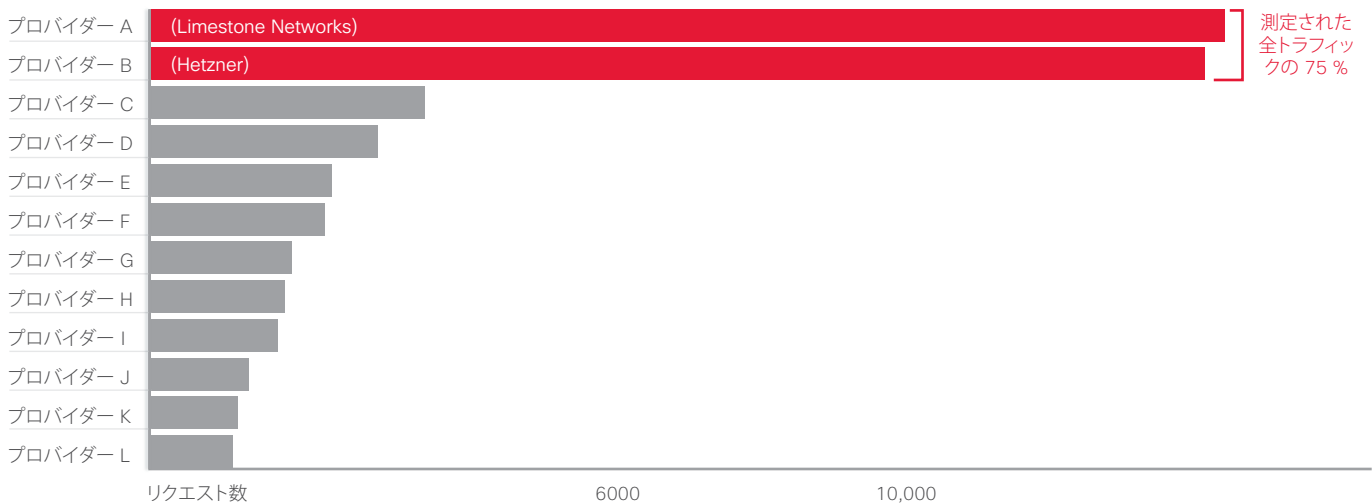
共有    

図 2. Angler のサポート率が低い IP インフラストラクチャ



出典:シスコセキュリティリサーチ

図 3. プロバイダー別の Angler HTTP リクエスト(2015 年 7 月)



出典:シスコセキュリティリサーチ

サーバを購入する攻撃者のやり方は、不正行為を 1 人の人物と関連付けるのを難しくしていました。たとえば、犯罪者は 1 日に 3 ~ 4 台のサーバを購入し、次の日には別の名前とクレジットカードを使って 3 ~ 4 台のサーバを購入します。彼らはこのように、感染したサーバが特定されて防御側にオフラインにされると、基本的に 1 つの IP アドレスから次の IP アドレスへと移っていきました。

この行動を調査するため、シスコは Level 3 Threat Research Labs と OpenDNS (シスコのグループ会社) に協力を求めました。Level 3 Threat Research Labs が脅威に関してグローバルで優れた洞察を提供したため、シスコは、脅威の範囲とそのピーク時にはどの程度大規模になるかを、さらに掘り下げて考えることができました。一方 OpenDNS は、脅威に関連したドメインの行動について独自の見解を示しました。これにより、シスコはドメイン シャドーイングなどの方法がどのように攻撃者に取り入れられているかについての理解を深めることができました。

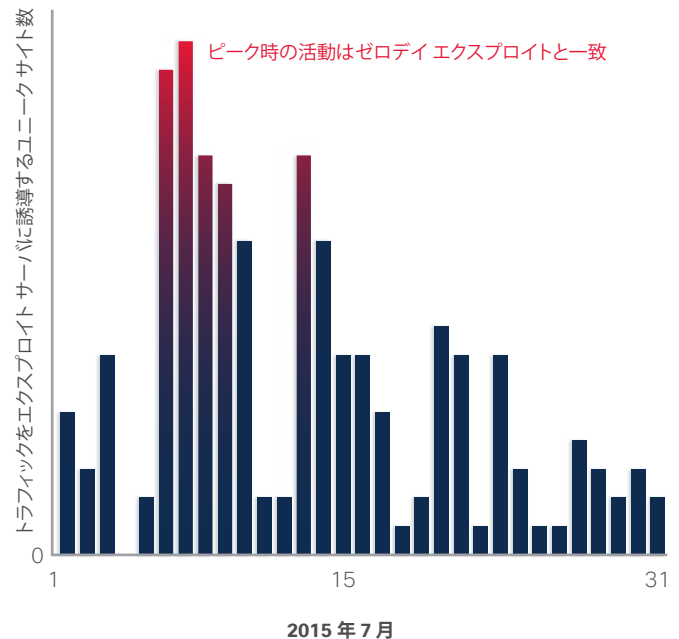
シスコの脅威研究者は次に、特にユーザがどのように Angler に遭遇し、悪意のあるペイロードを送りつけられるのかに目を向けました。研究者は、人気 Web サイトが悪意のある広告を通じて Angler エクスプロイト キットにユーザをリダイレクトしていることを確認しました。偽の広告は、ニュース、不動産、大衆文化など、何百もの主なサイトに置かれていました。こうしたサイトは一般的に、セキュリティコミュニティ内で「既知の善良な」サイトとみなされています。

さらにシスコの脅威研究者は、アメリカの小規模な地方紙に載った個人の死亡記事など、一見するとランダムで小規模な無数の Web サイトが同様のリダイレクトを行っているのを見つけました。後に挙げた戦略は高齢者を対象としたものでしょう。一般的にこの世代は Microsoft Internet Explorer などのデフォルトの Web ブラウザを使う傾向があり、多くの場合 Adobe Flash の脆弱性を定期的に補正する必要性に気づいていません。

Angler の動作でもう 1 つ注目すべき点は、ユニーク リファラーの数とそれが使用された頻度の低さにあります。(図 4) シスコは Angler エクスプロイト キットに人々を誘導するユニークサイトを 15,000 以上見つけましたが、その 99.8 % が 10 回未満しか使われていませんでした。つまり、リファラーは短期間だけ

有効で、数名のユーザが攻撃対象となった後で削除されたこととなります。私たちは 2015 年 7 月の分析で、活動のピークは様々なハッキングチームのゼロデイ エクスプロイトと一致していることに気づきました (CVE-2015-5119、CVE-2015-5122)。¹

図 4. 日付順のユニーク リファラー (2015 年 7 月)

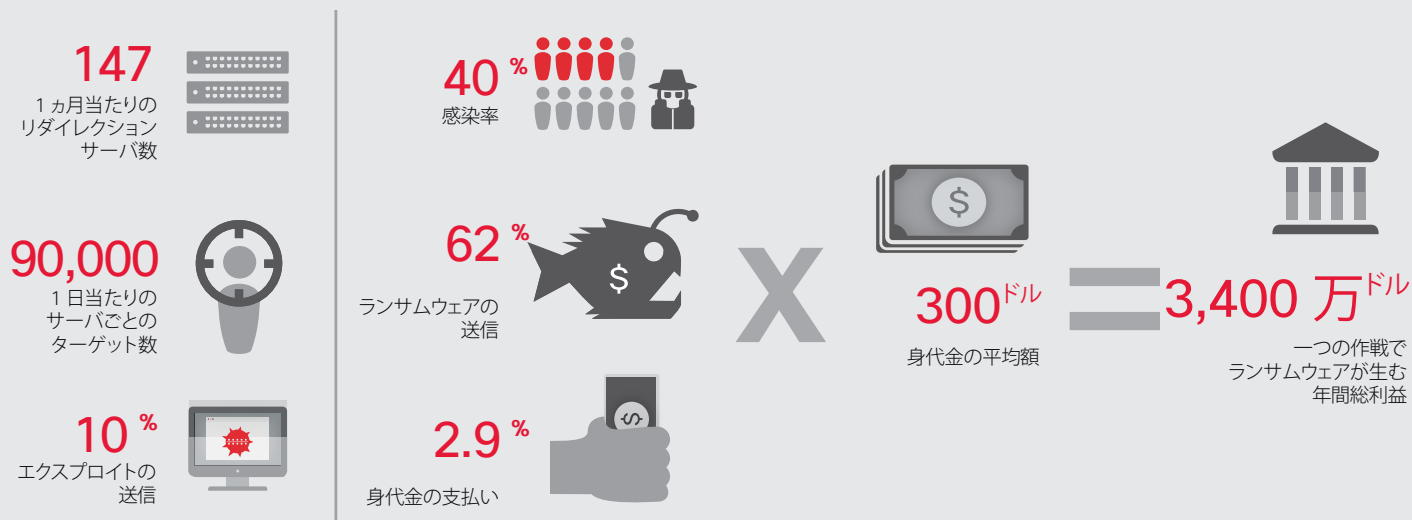


出典:シスコ セキュリティリサーチ

この特有の操作で送信された Angler ペイロードの約 60 % が、何らかのランサムウェア亜種を送信していたとシスコは判断しました。多くは Cryptowall 3.0 ですが、別のタイプのペイロードは、クリック詐欺攻撃のマルウェアをインストールするためによく使われる Bedep というマルウェア ダウンローダを含んでいました。「ブラウザの感染:感染が広がり、データ漏えいの主な原因に」[16 ページ](#)を参照)。マルウェアは両タイプとも、感染したユーザから労せずばやく多額の金銭を巻き上げられる仕組みになっています。

¹ 『Adobe がハッキングチームの Flash Player ゼロデイを修正』 [英語] Eduard Kovacs, SecurityWeek, 2015 年 7 月 8 日、<http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day>

! Angler の収益



1 か月当たり 9,515 人のユーザが身代金を支払っています

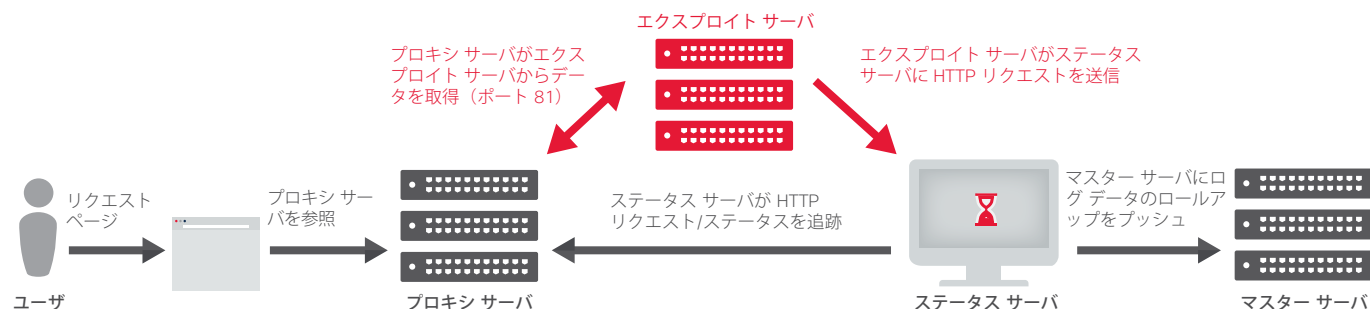
出典:シスコ セキュリティリサーチ

シスコの調査によると、この特定の作戦における Angler エクスプロイト キットの半分を主導した主犯は、1 日に最大で 90,000 人の被害者を狙いました。シスコの予測では、その作戦で攻撃者は年間 3,000 万ドル以上を稼いでいました。

Hetzner のネットワークでも同様の成功率だったと考えられます。つまり、シスコの分析時、Limestone Networks や Hetzner のサーバに関連する操作の背後にいる攻撃者が、世界中のすべての Angler の活動の半分を主導していたこととなります。シスコの研究者は、この操作により年間 6,000 万ドルの総利益を生み出せると見積もっています。

共有    

図 5. Angler のバックエンド インフラストラクチャ



出典:シスコ セキュリティリサーチ

シスコは、ユーザが接続していたサーバが、悪意のある Angler の活動を実際にはホストしていなかったことも発見しました。それらはコンジットとして働いていたのです。ユーザはリダイレクトの連鎖に陥り、ランディング ページの GET リクエストを送信しますが、それによりプロキシ サーバにたどり着きます。プロキシ サーバは、別の国の別のプロバイダーのエクスプロイト サーバにトラフィックをルーティングします。この調査では、単一のエクスプロイト サーバが複数のプロキシ サーバに関連付けられていることがわかりました。(図 5 を参照)。

シスコはヘルス モニタリングなどのタスクを扱っているステータス サーバを特定しました。ステータス サーバが監視している単一プロキシ サーバはすべて、一対のユニーク URL を持っていました。パスがクエリされると、ステータス サーバが HTTP ステータスコード「204」メッセージを返します。攻撃者は各プロキシ サーバを一意的に識別し、動作しているだけでなく、防御側が手を加えていないかも確認します。もう一方の URL を使って、攻撃者はプロキシ サーバからログを収集して、ネットワークがどの程度効率的に動作しているか判断します。

シスコが Angler エクスプロイト キットの活動を調査することができた重要な要素に、業界の連携があります。最終的に、それが米国のサービス プロバイダーにおける Angler プロキシ サーバへのリダイレクトを止め、日々多数のユーザに影響を与えている高度なサイバー犯罪についての認識を促すことにつながりました。

共有

シスコは Limestone Networks と緊密に連携して、新しいサーバがオンラインになったら特定し、注意深く監視してそれらが削除されるか確認しました。しばらくして攻撃者は Limestone Networks から手を引き、それに続いて世界的な Angler の活動も減少しました。



Angler エクスプロイト キットが生み出す国際的な収益源をシスコがどのように打破したかについては、シスコのセキュリティ ブログ『[注目の脅威: Cisco Talos がランサムウェアだけで年間 6,000 万ドルを稼ぎ出す大規模な国際的エクスプロイト キットへのアクセスを阻止](#)』[英語] をご覧ください。

業界の協調した取り組みが、インターネット最大の DDoS ボットネットの停止を支援

統合型脅威防御テクノロジーは、主な攻撃が企業ネットワークに影響する前に阻止します。しかし多くの場合、潜在的に大規模な攻撃を阻止するには、技術上の防御だけでなく、サービス プロバイダー、セキュリティ ベンダー、および業界グループの間の協調が必要です。

犯罪者が活動で利益を得ようと懸命になればなるほど、テクノロジー業界は協力してよりよい対応をし、犯罪戦略を打ち破る必要があります。シスコのセキュリティ研究者がこれまでに確認した、主な DDoS ボットネットの 1 つである SSHPsychos (または Group 93) は、シスコと Level 3 Threat Research Labs の協働の後、著しく弱体化しました。

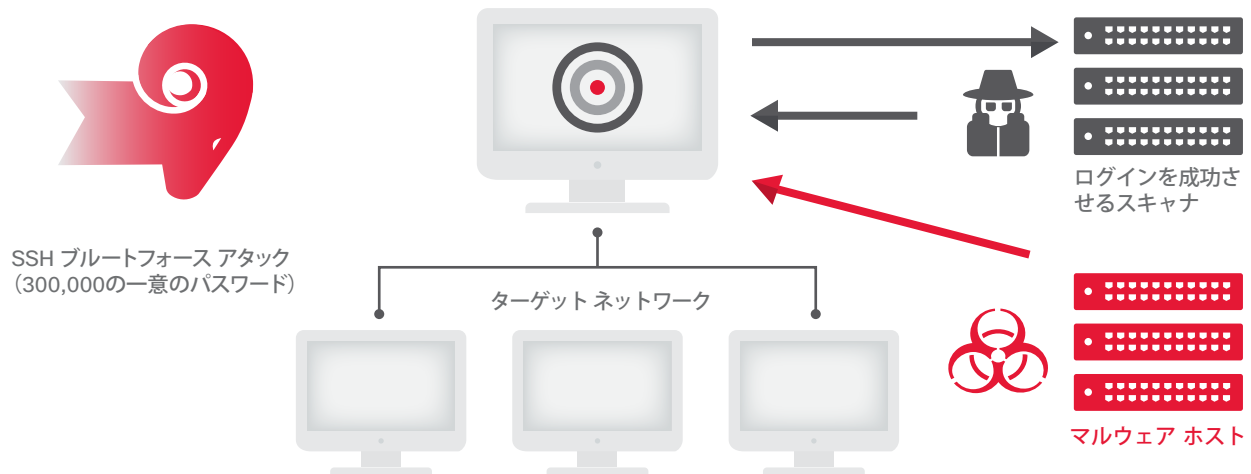
独特の脅威

SSHPsychos DDoS ネットワークはいくつかの理由で独特の脅威と言えます。インターネット全体に分散する何万ものマシンの協力を得られるため、デバイス ベースで対応できない分散型サービス妨害 (DDoS) 攻撃を開始できます。今回の場合、ボットネットはセキュア シェル (SSH) を含むブルートフォース アタックを使って作成されていました (図 6)。SSH プロトコルはセキュアなコミュニケーションを可能にし、一般的にシステムのリモート管理にも使用されます。シスコと Level 3 の分析によると、時には SSHPsychos がすべてのグローバル インターネット SSH トラフィックの 35 % 以上を占めていました (図 7)。

SSHPsychosは、中国と米国の2カ国で稼働しています。ブルートフォース ログインの攻撃は、300,000 の一意のパスワードを使って、中国を拠点とするホスティング プロバイダーから発生しました。攻撃者が正しいルート パスワードを推測してログインできた時点で、ブルートフォース アタックが止まりました。24時間後、攻撃者は米国の IP アドレスからログインし、感染したマシンに DDoS ルートキットをインストールしました。明らかに、ネットワーク管理者の疑いを抑える戦術でした。ボットネットの対象はさまざまですが、大手のインターネット サービス プロバイダー (ISP) であることが多いように思われます。

共有    

図 6. SSHPsychos はブルートフォース アタックを使用



出典:シスコ セキュリティリサーチ

図 7. SSHPsychos はピーク時には世界のインターネット トラフィックの約 35 % を占める



出典:シスコ セキュリティリサーチ

セキュリティ専門家との連携

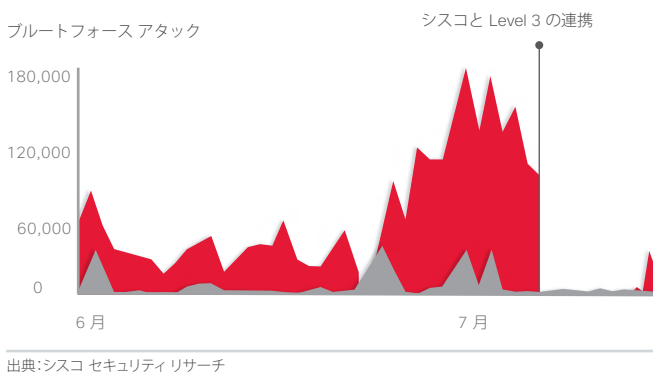
DDoS ネットワークが大規模なため、シスコの研究者は、損害を食い止めるのは難しいと認識していました。ブルートフォース グループをインターネットから効果的に追い出せる組織と手を組んで作業することが不可欠でした。しかしバックボーン プロバイダーは、顧客のコンテンツをフィルタリングするのをためらいます。

シスコは Level 3 Threat Research Labs に協力を求めました。Level 3 がネットブロックのトラフィック、または多くの IP アドレスを分析した結果、SSHPsychos が存在すると考えられました (103.41.124.0/23)。正規のトラフィックがそのアドレスから発生したり、そのアドレスを宛先としていたりしていないことを確認しました。ネットワークトラフィックをそのネットワーク内で null ルーティングし、関連ドメインのサービス プロバイダーに連絡して、ネットワークのトラフィックを削除するよう依頼しました。

この取り組みの成果は即座に表れました (図 8)。元のネットワークでは新しい活動が見られませんでした。ネットブロック 43.255.190.0/23 の新しいネットワークでは、大量の SSH ブルートフォース アタック トラフィックが見られました。SSHPsychos についても同様の振る舞いがありました。SSHPsychos 関連のトラフィックが急激に再発したのを受けて、シスコと Level 3 は 103.41.124.0/23 および新しいネットブロックの 43.255.190.0/23 に対して対策を採ることに決めました。

SSHPsychos が利用しているネットブロックを閉鎖しても、DDoS ネットワークが永久に無効になるわけではありません。しかし、作成者が操作を実行する速度を確実に抑え、少なくとも一時的には SSHPsychos が新しいマシンに広がることを防ぎました。

図 8. SSHPsychos のトラフィックが介入後に激減



サイバー犯罪者は大規模な攻撃ネットワークを構築するため、セキュリティ業界は、SSHPsychos のような脅威に直面したときに連携するという道を探らなければなりません。大手のドメイン プロバイダー、ISP、ホスティング プロバイダー、DNS リゾルバ、およびセキュリティ ベンダーは、正規のトラフィックだけを扱うためのネットワークでオンライン犯罪者がエクスプロイトを開始するのを、もはや傍観することはできません。つまり、犯罪者が悪意のあるトラフィックをある程度わかりやすい形で発信したら、業界は、こうした正規ネットワークへの犯罪経路を削除しなくては行けないのです。



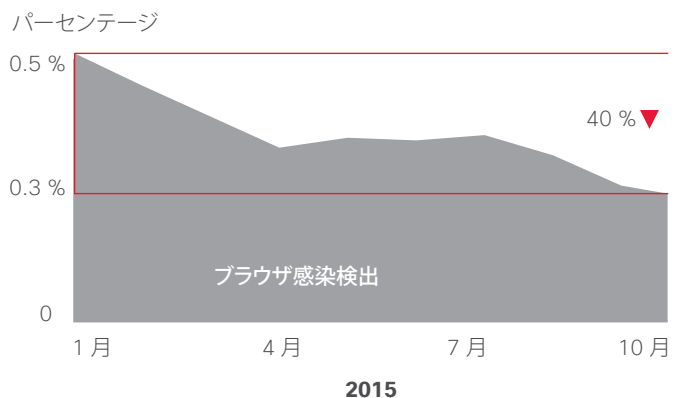
SSHPsychos の脅威へのシスコと Level 3 Threat Research Labs の対応については、シスコのセキュリティ ブログ『[注目の脅威: SSHPsychos](#)』[英語]をご覧ください。

ブラウザの感染:感染が広がり、データ漏えいの主な原因に

セキュリティ チームは、ブラウザのアドオンは脅威の程度が低いと考えがちですが、監視の優先度を上げ、こうしたタイプの感染を迅速に特定し修正できるようにする必要があります。

対策を急ぐ理由:シスコの調査によると、ブラウザの感染は組織が把握しているよりも広く蔓延しています。2015 年 1 月から 10 月まで、26 ファミリの悪意のあるブラウザ アドオンを調査しました (図 9)。この期間のブラウザ感染のパターンを見ると、感染数はゆるやかに減少しているように見えます。

図 9. ブラウザの感染 (2015 年 1 月～10 月)



しかし、だまされてはいけません。この期間のHTTPSトラフィック量が増加し、URL情報が暗号化により目視で判読できなくなっていたため、主に私たちが追跡していた26ファミリーに関連する感染の指標を特定することが難しくなったのです。(暗号化とそれがもたらす防御側への課題については、「暗号化:採用の広がり」と防御側の課題」30ページを参照してください)。

悪意のあるブラウザ拡張機能は情報を盗むため、データ漏えいの主な原因にもなり得ます。ユーザが感染したブラウザで新しいWebページを開くたびに、悪意のあるブラウザ拡張機能がデータを収集します。ユーザが訪れる内部または外部のWebページすべてについて、基本的情報以上の詳細を引き出しています。また、URLに組み込まれた機密性の高い情報も収集しています。この情報には、ユーザ認証情報、顧客データ、および組織の内部APIおよびインフラストラクチャに関する詳細が含まれます。

悪意のある多目的ブラウザ拡張機能は、ソフトウェアバンドルまたはアドウェアにより提供されます。それらは、さまざまな方法でユーザを利用して利益を引き出せるよう設計されています。感染したブラウザでは、広告表示やポップアップなどの悪意のある広告をユーザがクリックするよう誘導します。また、感染したリンクをクリックしたり、悪意のある広告で見つけた感染ファイルをダウンロードしたりするようユーザを誘導することによって、マルウェアを配布できます。また、ユーザのブラウザリクエストをハイジャックし、検索エンジンの検索結果ページに悪意のあるWebページを挿入できます。

シスコの調査対象の45の企業全体では、毎月組織の85%以上が悪意のあるブラウザ拡張機能に侵されていることがわかりました。この結果は、こうした攻撃の規模の大きさを浮き彫りにしています。感染したブラウザは比較的軽度の脅威と見なされ、数日またはさらに長く検出されず解決されないことがあるため、攻撃者に作戦を実行する時間やチャンスを与えてしまいます(「検出時間:攻撃のチャンス減らすための競争」60ページ参照)。

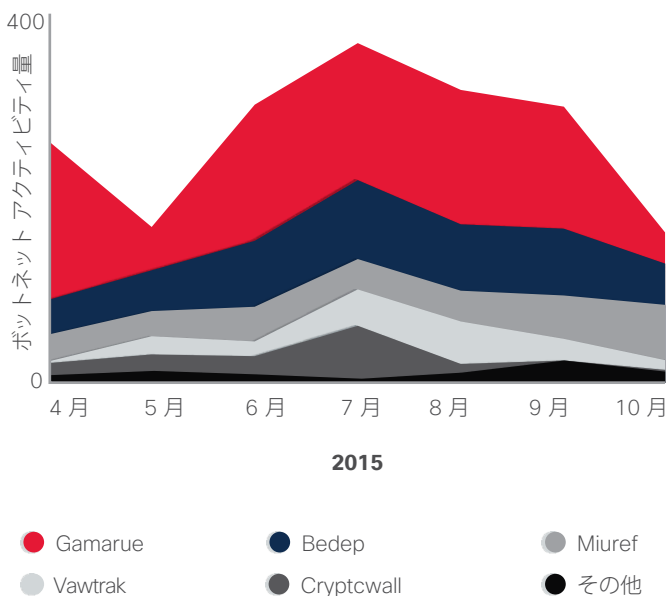
そのため、セキュリティチームはこのリスクの監視にもっとリソースを割り当て、脅威の優先順位付けをさらに自動化していく必要があると私たちは提言します。

ボットネットの指令:世界の状況

ボットネットはマルウェア感染したコンピュータのネットワークです。攻撃者はそれらをグループとして制御し、スパムの送信やDDoS攻撃の開始など、特定のタスクを実行するよう命令します。その規模も数も年を追うごとに大きくなっています。現在の脅威の状況を世界規模で理解するために、2015年4月から10月にかけて121社のネットワークを分析し、よく見られる8つのボットネットの1つ以上の形跡があるか調べました。データはボットネットの活動の一般的概要を提供するために標準化されました(図10)。

この期間、最もよく見られた指示管理の脅威はGamarueでした。これは情報を盗むモジュール式の多目的マルウェアで、長年出回っています。

図10. 個々の脅威の拡大(感染ユーザの割合)



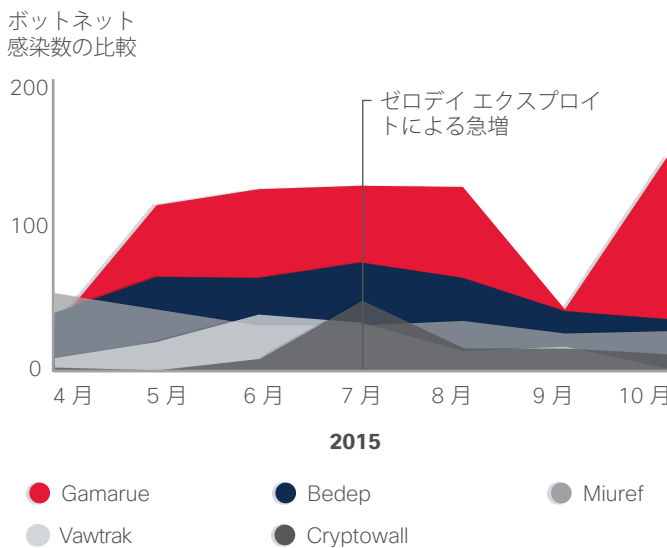
出典:シスコセキュリティリサーチ

ランサムウェア Cryptowall 3.0 に関連する感染数が大幅に増加したのは 7 月でした。この動きは、Cryptowall ペイロードをドロップすることで知られる Angler エクスプロイト キットに主に起因します。2015 年度のシスコ中間セキュリティレポートによれば、Angler などエクスプロイト キットの作成者は、Adobe Flash の「パッチ適用もれ」、つまり Adobe のアップデートリリースからユーザが実際にアップグレードするまでの期間をすばやく利用していました²。シスコの脅威研究者は、2015 年 7 月の急増を、ハッキングチームのリークで明らかになった Flash ゼロデイ エクスプロイト CVE-2015-5119 に起因するものと考えています³。

Angler エクスプロイト キットはまた、クリック詐欺戦略の実行に使用される Bedep Trojan を発信します。この脅威の普及もやや広がったことが 7 月に報告されています (図 11)。

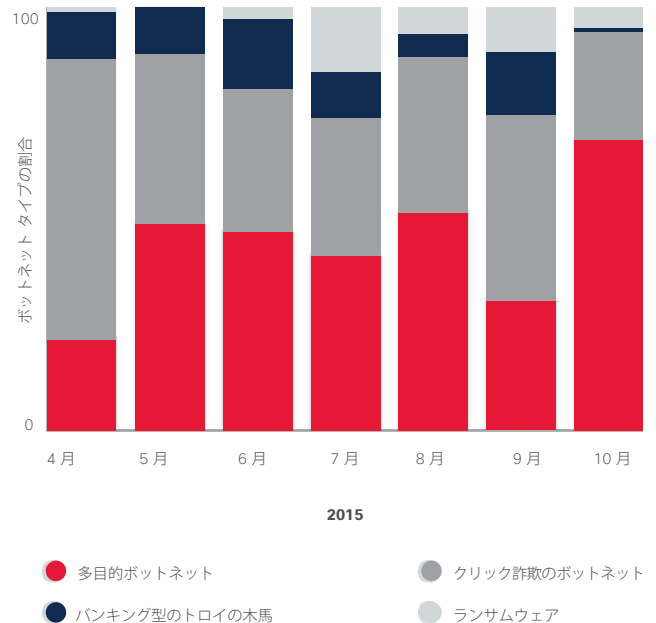
Bedep、Gamarue、および Miuref (別のトロイの木馬で、クリック詐欺を行うブラウザ ハイジャッカー) を合わせると、私たちが分析した対象ユーザにおけるボットネットの指示管理活動の 65 % 以上を占めていました。

図 11. 月ごとの脅威調査: 感染ユーザ数ベース



出典:シスコ セキュリティリサーチ

図 12. 月ごとの脅威調査: 脅威カテゴリベース



出典:シスコセキュリティリサーチ

分析期間中、Bedep 感染の割合は比較的安定していましたが、Miuref 感染には低下が見られました。シスコはこれを、HTTPS トラフィックが増加し、Miuref の感染指標が表に出なかったためと考えています。

図 12 は、監視期間中のほとんどの感染の原因となったボットネットの種類を示しています。Gamarue や Sality などの多目的ボットネットが群を抜いており、次にクリック詐欺のボットネットが続きます。バンキング型のトロイの木馬が第 3 位で、この脅威が古いながらも依然として蔓延していることを示しています。

共有

² シスコ 2015 年中期セキュリティレポート: <http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html>

³ 『Adobe がハッキングチームの Flash Player ゼロデイを修正』 [英語] Eduard Kovacs、SecurityWeek、2015 年 7 月 8 日、<http://www.securityweek.com/adobe-patches-hacking-teams-flash-player-zero-day>

DNS の盲点: 指示管理に DNS を使う攻撃

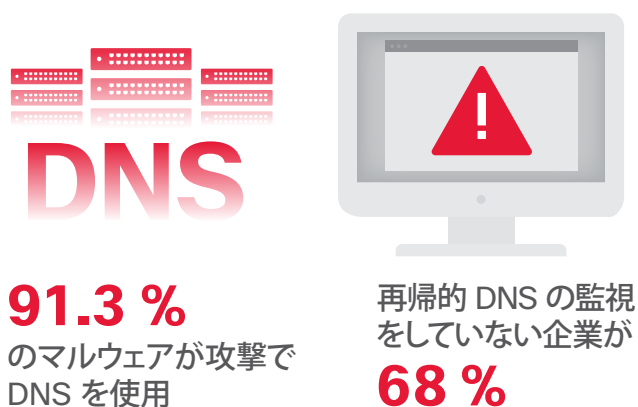
「既知の脅威」と判断されたマルウェアをシスコが分析したところ、そのマルウェアの大部分 (91.3 %) が、3 つの方法のいずれかで Domain Name Service (DNS) を使っていました。

- 指示管理の獲得
- データの搾取
- トラフィックのリダイレクト

この割合に達するため、所有するさまざまなサンドボックスからサンプルとなる振る舞いをマイニングしました。DNS をまったく使わないよう決められているか、DNS をインターネットの「ヘルスチェック」実行に使うだけのマルウェアは、分析の対象から外しました。残りのマルウェアは、不正と評価されるか不正が疑われるサイトへの接続に DNS を使っていました。

マルウェアの作戦を進めるのに攻撃者が DNS を頼っているにも関わらず、セキュリティ目的で DNS を監視している会社はほとんどありませんでした (または DNS をまったく監視していませんでした)。監視がないため、DNS は攻撃者にとって理想的な抜け道となっています。シスコが行った最近の調査 (図 13 参照) によると、68 % のセキュリティ プロフェッショナルが、組織が再帰的 DNS からの脅威を監視していないと報告しています。(再帰的 DNS ネームサーバは、要求ホストに目的のドメイン名の IP アドレスを提供します)。

図 13. 再帰的 DNS からの脅威を監視



出典: シスコ セキュリティリサーチ

DNS はなぜ多くの組織にとってセキュリティ上の盲点なのでしょう。主な理由は、セキュリティ チームと DNS 専門家が一般的に社内の異なる IT グループで働いており、頻繁な交流が行われていないことです。

しかし交流すべきなのです。前述の 3 つの行動のいずれかにすでに DNS を使っているマルウェア感染を特定し封じ込めるには、DNS の監視が不可欠です。また、この DNS の監視が、攻撃を支えるインフラストラクチャのタイプの特特定からその源の発見まで、攻撃をさらに調査するためのさまざまなコンポーネントを計画する上で重要な一歩となります。

しかし、DNS の監視に必要なのはセキュリティ チームと DNS チームの協力だけではありません。相関分析のための適切なテクノロジーと専門知識をとりそろえる必要があります。(さらなる洞察については、「高利益を上げる大規模なエクスプロイト キットやランサムウェアの攻撃を、業界の連携によってシスコが排除」(10 ページ)を参照し、Angler エクスプロイト キットが使っている IP について、OpenDNS の支援でシスコがどのようにドメインの可視性を向上したかをご覧ください)。

レトロスペクティブ DNS 分析

DNS クエリおよびそれに続く TCP トラフィックや UDP トラフィックに関するシスコのレトロスペクティブ調査では、多数のマルウェア ソースを特定しています。これには指示管理サーバ、Web サイト、分散ポイントが含まれます。またレトロスペクティブ調査では、脅威リスト、コミュニティの脅威レポート、サイバー攻撃に見られる傾向、および顧客の業界特有の脆弱性に関する知識などのインテリジェンスを活用して、脅威の程度が高いコンテンツを検出します。

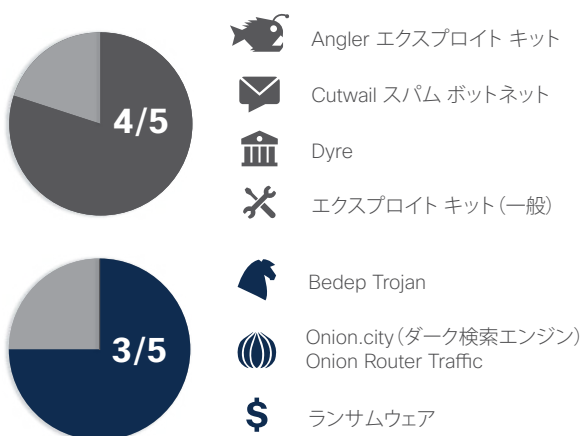
シスコのレトロスペクティブ レポートは、Advanced Persistent Threat (APT) の行動に一般的に関連する「緩慢な」データ搾取を見つけることができます。これは、従来の脅威検出テクノロジーでは多くの場合とらえることができません。分析の目的は、発信される膨大な量の通信トラフィックの中に異常を見つけることです。この「裏返し」のアプローチで、見逃してしまいそうな潜在的な不正データや有害なネットワーク動作を発見することができます。

こうして、顧客のネットワークで使用されている「不正」な DNS リゾルバを特定することができました。顧客は、従業員がインフラストラクチャの一部としてそのリゾルバを使用していることに気づいていませんでした。DNS リゾルバの使用を積極的に管理および監視しないと、DNS キャッシュ ポイズニングや DNS リダイレクションなど悪意のある行動につながるおそれがあります。

不正な DNS リゾルバの発見と特定に加え、レトロスペクティブ調査では、顧客のネットワークに次のような問題を発見しました。

- 顧客のアドレス空間が第三者のスパム・マルウェア ブロックリストにある
- 顧客のアドレス空間が既知の Zeus および Palevo の指示管理サーバに誘導している
- CTB-Locker、Angler、DarkHotel など、アクティブなマルウェア活動がある
- Tor、電子メールの自動転送、およびオンライン文書変換の使用など、疑わしい行動がある
- 中国拠点のドメインへの広範な DNS トンネリング
- DNS の「タイポスクワッティング」⁴
- 内部クライアントが顧客の信頼が高い DNS インフラストラクチャを迂回する

複数の業界に渡るシスコ カスタム スレット インテリジェンスのお客様からサンプルを選んで調査することで、次のタイプのマルウェアを、それぞれ対象の全顧客に換算した割合で発見しました。



⁴ タイポスクワッティングとは、実際のドメイン名に似たドメイン名を登録することです。目的のドメイン名をうっかり入力しまちがえたユーザを狙って攻撃者が使う戦略です。

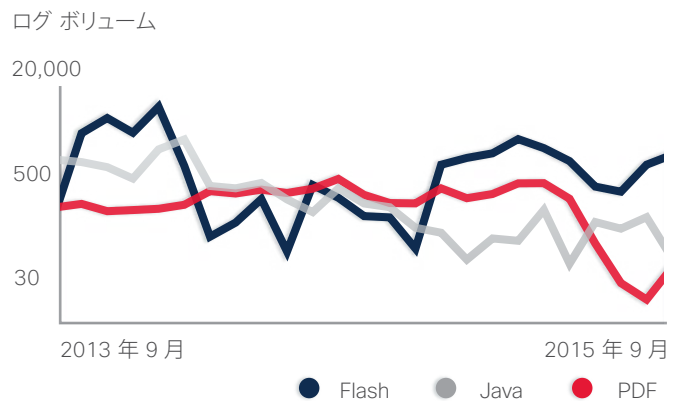
脅威インテリジェンス分析

Web 攻撃ベクトル

ADOBE FLASH: ついに下火に

Flash の全体的件数は昨年減少したとはいえ(次項「**Adobe Flash および PDF コンテンツの傾向**」参照)、依然としてエクスプロイトキット開発者に好んで使われています。実際、Flash マルウェアは 2015 年の傾向として特に増加も減少もしませんでした(図 14)。Flash 関連のマルウェアは、しばらくの間エクスプロイトの主要ベクトルであり続けられると思われます。注目すべき点は、Angler エクスプロイトキットの作成者たちが Flash の脆弱性を狙うことが非常に多いということです。

図 14. 攻撃ベクトルの共有 (2年間の比較)



出典:シスコ セキュリティリサーチ

ブラウジングから Adobe Flash をなくそうという業界の圧力により、Web 上の Flash コンテンツ量は減少しつつあります(次項「**Adobe Flash および PDF コンテンツの傾向**」参照)。これは近年 Java コンテンツに見られた現象と似ており、結果として Java マルウェアの着実な減少傾向につながりました(実際 Angler の作成者は、もはや Java エクスプロイトを含むような手間はかけません)。一方、PDF マルウェアの量は、非常に安定しています。

Microsoft Silverlight も攻撃ベクトルとしては衰退しました。多くのベンダーで、Silverlight がブラウザへの統合に使う API のサポートを止めたからです。多くの企業は HTML5 ベースのテクノロジーを採用し、Silverlight から離れました。Microsoft は差し当たり Silverlight の新バージョンの予定はないと言っており、現在はセキュリティ関連のアップデートを発行しているだけです。

ADOBE FLASH および PDF コンテンツの傾向

シスコの研究者は、Web 上の Adobe Flash コンテンツの緩やかな減少に着目しています (図 15)。Amazon や Google などインターネット大手の最近の動向が、Flash コンテンツの減少の要因となっています。これらの企業では、Flash を使う広告を受け付けないかブロックしています。

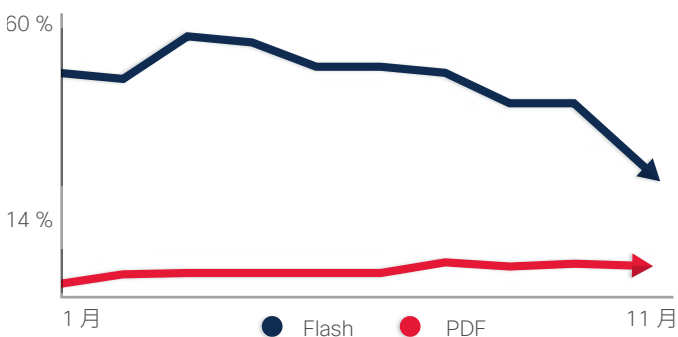
一方で PDF コンテンツは昨年非常に安定しており、そのままの状態が続くと思われます。しかし、しばらく主要な Web 攻撃ベクトルとはなっていません。

Flash コンテンツの減少はしばらく続くと思われ、それが加速する可能性もあります。Adobe はついに Flash を段階的に廃止することを発表しました⁵。しかし、Flash が完全に消えるまでには時間がかかりそうです。Flash は Google Chrome、Microsoft Internet Explorer、Microsoft Edge などのブラウザに組み込まれており、ゲームやビデオなどの Web コンテンツで依然として幅広く使われています。

しかし、今後数年で新しいテクノロジー (HTML5 やモバイルプラットフォームなど) が採用されると、Java、Flash、Silverlight などの Web 攻撃ベクトルの長期的傾向がますます明らかになります。時間がたつにつれ、勢力は弱まるでしょう。そのため、金儲けを企む攻撃者にとっては魅力がなくなると考えられます。彼らは、簡単に多くのユーザを攻撃し、短期間で利益を生むことができるベクトルを重視するからです。

図 15. Flash および PDF の全体的なトラフィックの割合

インターネットトラフィック全体における割合



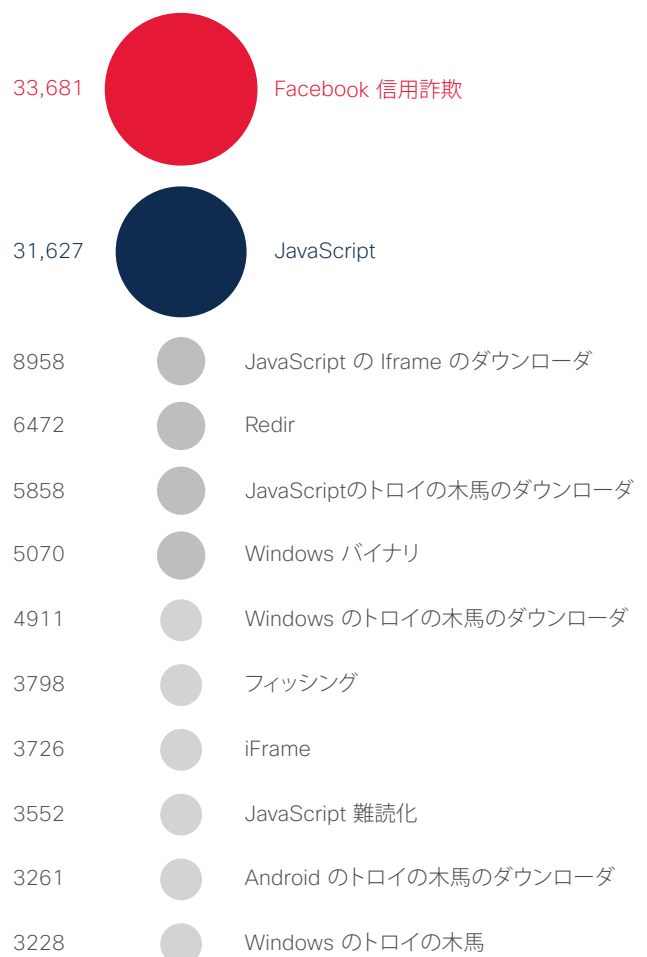
出典:シスコ セキュリティリサーチ

Web 攻撃の方法

図 16 と図 17 は、攻撃者が組織のネットワークにアクセスするために使用するさまざまなマルウェアを示しています。図 16 は、アドウェア、スパイウェア、悪意のあるリダイレクト、iFrame エクスプロイト、フィッシングなど、最も一般的なマルウェアを示しています。

図 16. 最も広く確認されたマルウェア

総計 (sample_count) X 1000



出典:シスコ セキュリティリサーチ

⁵『Adobeニュース:Flash、HTML5、およびオープン Web 標準』[英語] Adobe, 2015 年 11 月 30 日:
<http://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html>

図 16 は、犯罪者が初回のアクセスを獲得するために使うさまざまなマルウェアとして見ることができます。これらは、多数のユーザを比較的簡単に攻撃できる確実でコスト効率の高い方法です。シスコの調査では、JavaScript エクスプロイトや Facebook 信用詐欺（ソーシャル エンジニアリング）が最もよく使われる攻撃方法です。

図 17 は比較的数量が少ないマルウェアを示しています。「数が少ない」ということが「効果的でない」ということを意味するのではないことに注意してください。シスコ セキュリティ リサーチによれば、数が少ないマルウェアは、新たに登場した脅威か、対象を絞り込んだ戦術である場合があります。

こうした高度な手法の多くは、感染したユーザからできるだけ多くの価値を引き出すよう設計されています。価値の高いデータを盗んだり、ユーザのデジタル資産を押さえて身代金を要求したりします。

したがって、Web マルウェアをモニタする場合、最も頻繁に見られる脅威の種類に注力するだけでは不十分です。あらゆる種類の攻撃を考慮する必要があります。

図 17. 比較的数量が少ないマルウェアの例

総計 (sample_count) < 40



出典:シスコ セキュリティ リサーチ

最新の脅威

ADOBE FLASH が脆弱性の第 1 位

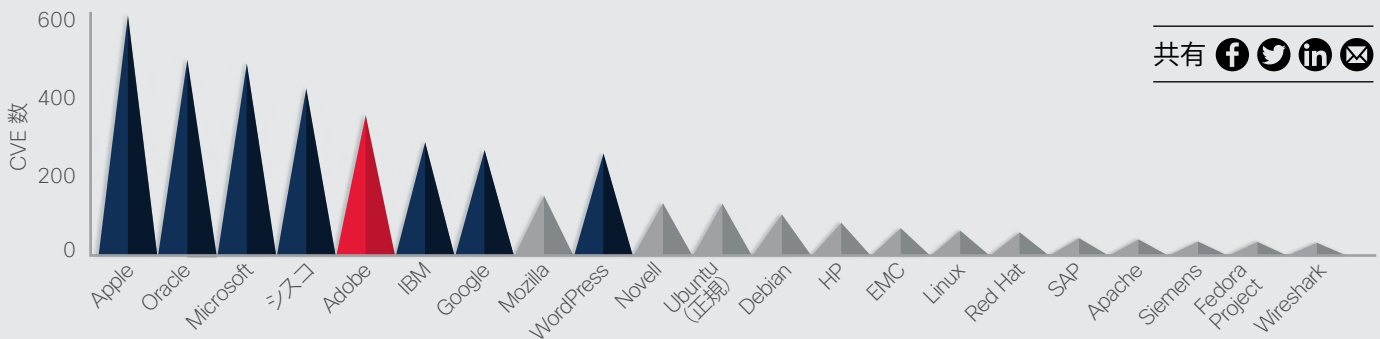
Adobe Flash プラットフォームは、この数年間犯罪者がよく使用する脅威ベクトルです。Flash の脆弱性は依然として、緊急度の高いアラートに挙げられます。幸い、2015年に、エクスプロイトがよく発生する Web ブラウザなどの製品のベンダーがこの弱点に気づき、攻撃者のチャンスを減らす対策を取り始めています。

2016年には、犯罪者は Adobe Flash ユーザのエクスプロイトや攻撃に集中すると思われます。こうした Flash の脆弱性により、エクスプロイトがオンラインで公開されていたり、エクスプロイトキットの一部として販売されていたりします。(21 ページにあるとおり、Flash 関連のコンテンツは減少しましたが、Flash は依然としてエクスプロイトの主要ベクトルであり続けています)。

一般的な別の脅威ベクトルである Java の影響を抑えるために取られた戦略に習い、多くの Web ブラウザが Flash をブロックするかサンドボックスを用いてユーザを保護しています。これは望ましい展開ですが、攻撃者が今後しばらくは依然としてエクスプロイトの開始に成功するだろうと心に留めておくことが重要です。ユーザは必要に応じてブラウザをアップデートすることを怠るかもしれず、犯罪者は旧バージョンのブラウザソフトウェアを狙ったエクスプロイトを開始し続けるでしょう。

しかしシスコの研究者は、よく使われる Web ブラウザやオペレーティングシステムに組み込まれた保護機能により、Flash への犯罪者の依存が減るだろうと考えています。オンライン攻撃者はできるだけ効率的に最良の結果(利益など)を得ようとするため、高い投資回収率が見込めない攻撃に取り組むことはありません。

❗ 図 18. ベンダー別の CVE の総数



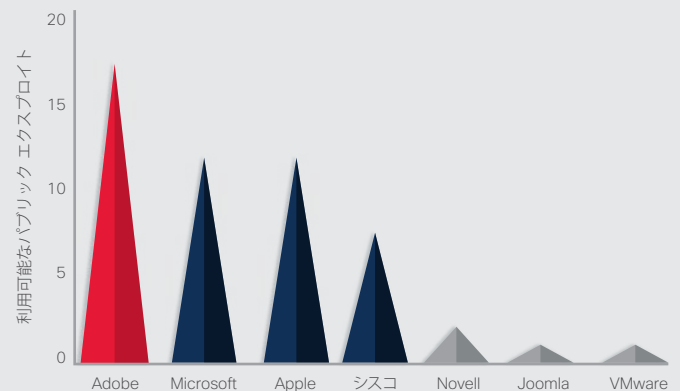
出典:シスコ セキュリティリサーチ, National Vulnerability Database

上記のグラフは、2015年にベンダーが公開した CVE の総数を示しています。このグラフが示すように、Adobe が突出しているわけではないことに注目してください。一方、エクスプロイトが可能な脆弱性を表す右のグラフでは、Adobe が上位になっています。

また、2015年の WordPress の製品の脆弱性は 12 件だけです。他の 240 件の脆弱性はサードパーティ コントリビュータが作成したプラグインやスクリプトからのものです。

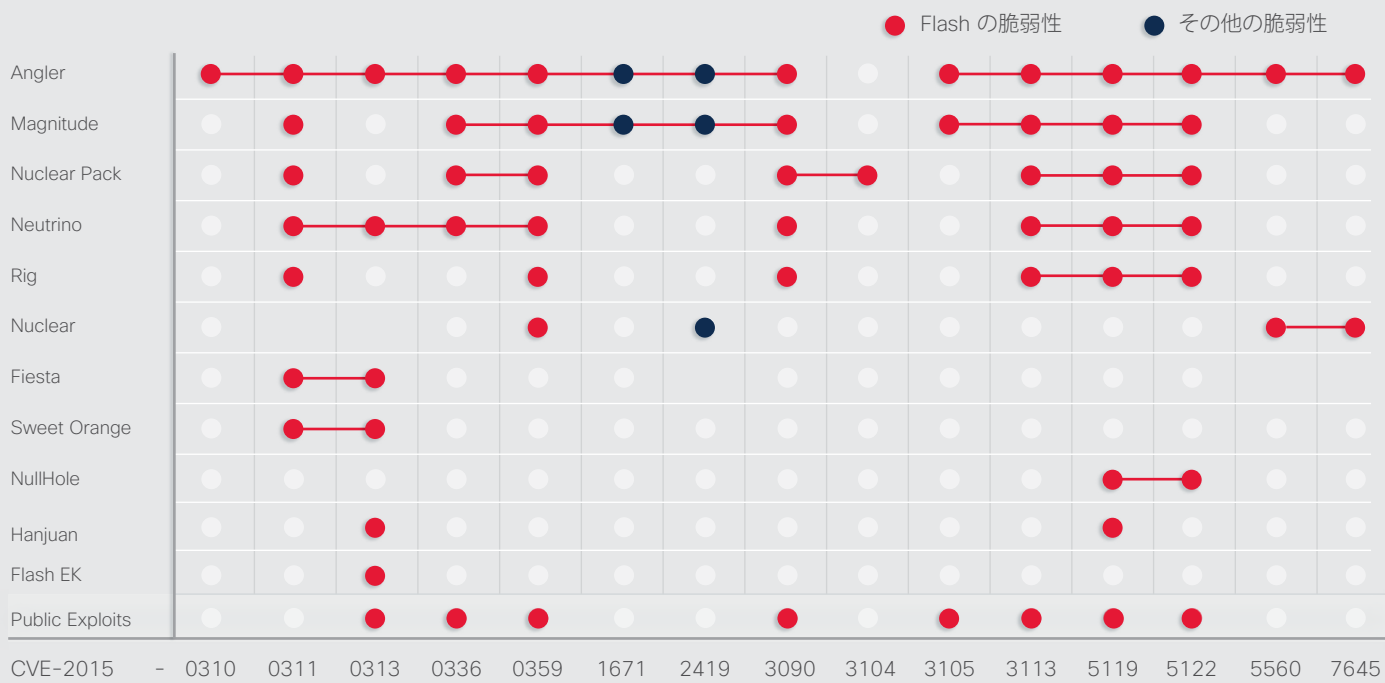
図 20 に示すように、脆弱性および関連するエクスプロイトのリストは、セキュリティ プロフェッショナルの手引きとなり得ます。それを使うことにより、ハイリスクで最もよく見られる脆弱性を管理し優先順位付けして、ローリスクの脆弱性より先に修正することができます。ベンダー別の CVE の詳細については、CVE Details の Web サイト (<https://www.cvedetails.com/top-50-products.php>) [英語] をご覧ください。

図 19. ベンダーの脆弱性別のパブリック エクスプロイト数



出典:シスコ セキュリティリサーチ, Metasploit, Exploit DB

図 20. 一般的な脆弱性



出典:シスコ セキュリティリサーチ

図 20 はハイリスクの脆弱性を表し、その脆弱性がエクスプロイトキットに有料で含まれているかどうか(「Flash EK」の行を参照)、または公開されているエクスプロイトがあるかどうか(「パブリックエクスプロイト」の行を参照)を示しています。機能的なエクスプロイトが可能な脆弱性は、修正の優先順位が高くなります。

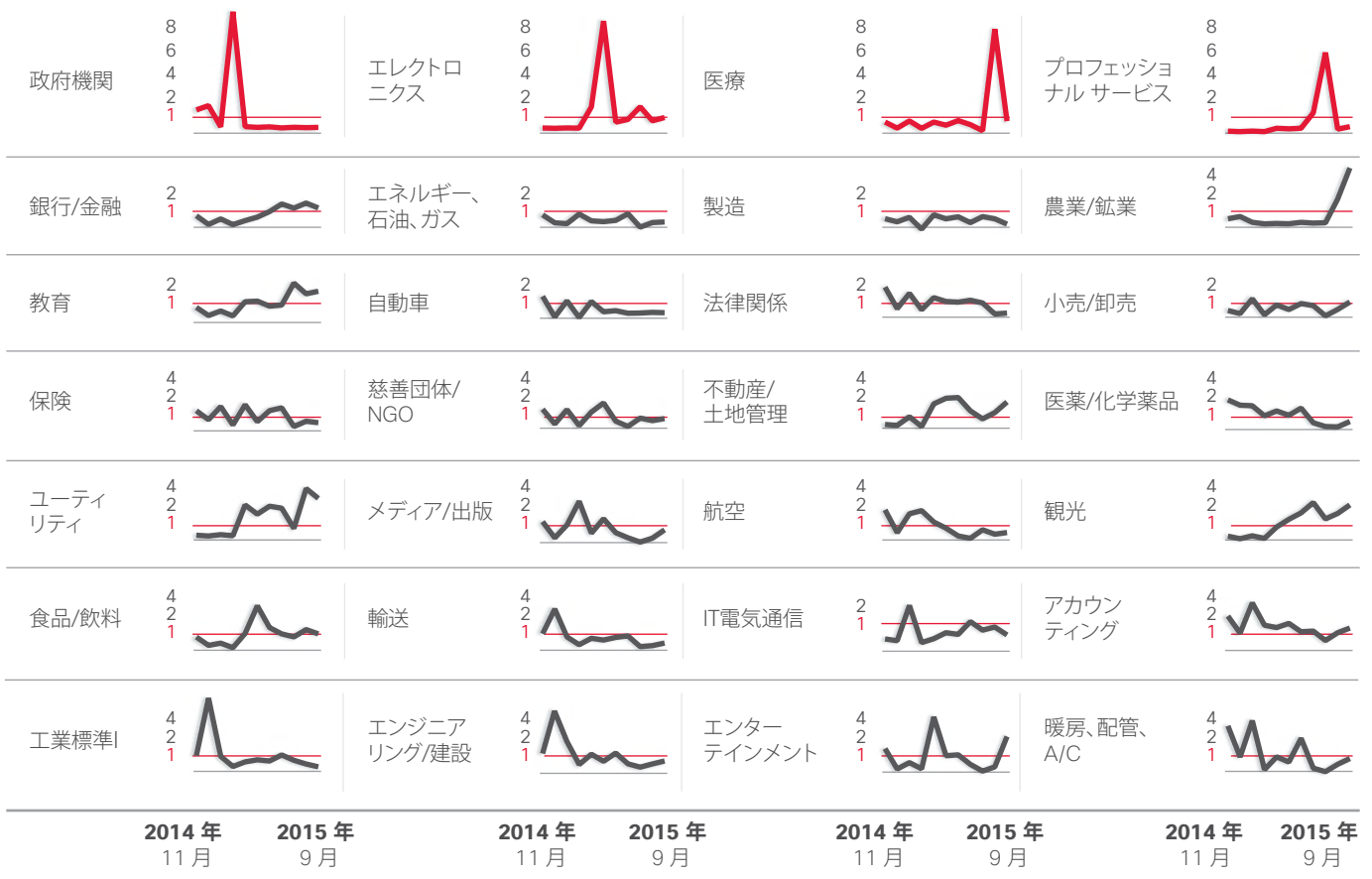
このリストは、セキュリティプロフェッショナルが修正や改善を優先順位付けする際に役に立ちます。任意の製品のエクスプロイトの有無(公開されているかエクスプロイトキットに含まれている)は、必ずしも攻撃が行われていることを意味しません。

業界別のマルウェア出現リスク

ハイリスクな業界の Web マルウェア出現を追跡するために、攻撃トラフィックの相対的な量(「ブロック率」と、「正常」または予想されるトラフィックの相対的な量を調査しました。

図 21 は、通常のネットワークトラフィックに対する比率として、28 の業界とその関連するブロック アクティビティを示します。比率 1.0 は、観察されたトラフィックの量にブロック数が比例していることを示します。1.0 よりも大きい値は、予想よりも高いブロック率を表し、1.0 よりも小さい値は、予想よりも低いブロック率を示しています。

図 21. 月ごとの業界のブロック率 (2014 年 11 月～2015 年 9 月)

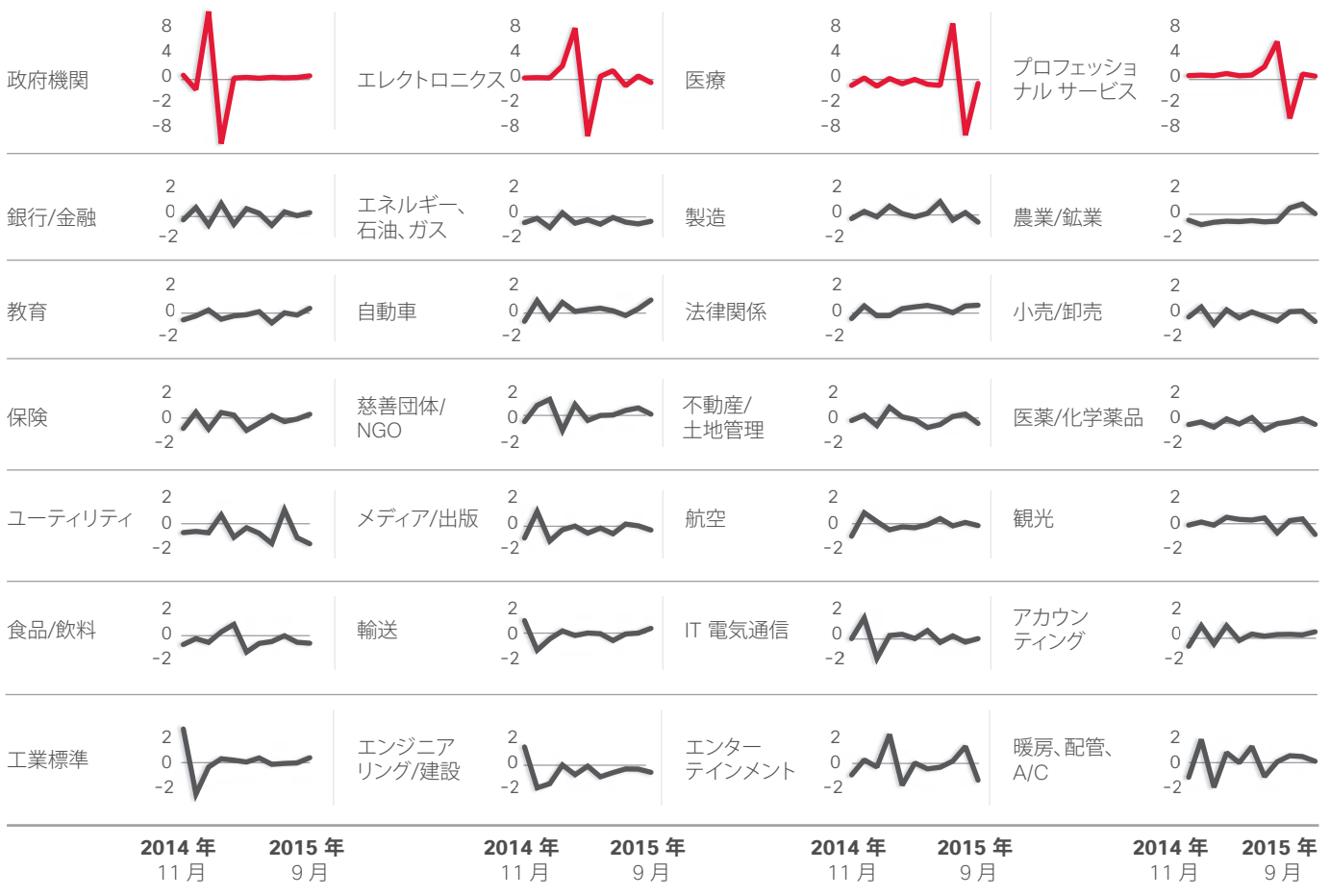


出典:シスコ セキュリティリサーチ

図 22 は、特定の業界への攻撃者の狙いがどのように変わっているかを示しています。(ゼロは実質的な変化がないことを示します)。2015 年 1 月から 3 月は、最もブロック率の高い業界は政府機関でした。3 月から 5 月は電子工業で、夏にはプロフェッショナル サービスのブロック率が最大でした。2015 年の秋になると、医療機関のブロック率がすべての業界を押さえていました。

シスコの調査によると、2015 年にブロック アクティビティが多かった 4 つの業種は、すべてトロイの木馬関連の攻撃を受けていました。政府機関はまた、非常に多くの PHP インジェクション攻撃を受け、プロフェッショナル サービスでは iFrame 攻撃を数多く受けました。

図 22. 業種ごとのブロック率 (月ごとの比較)



出典:シスコ セキュリティリサーチ

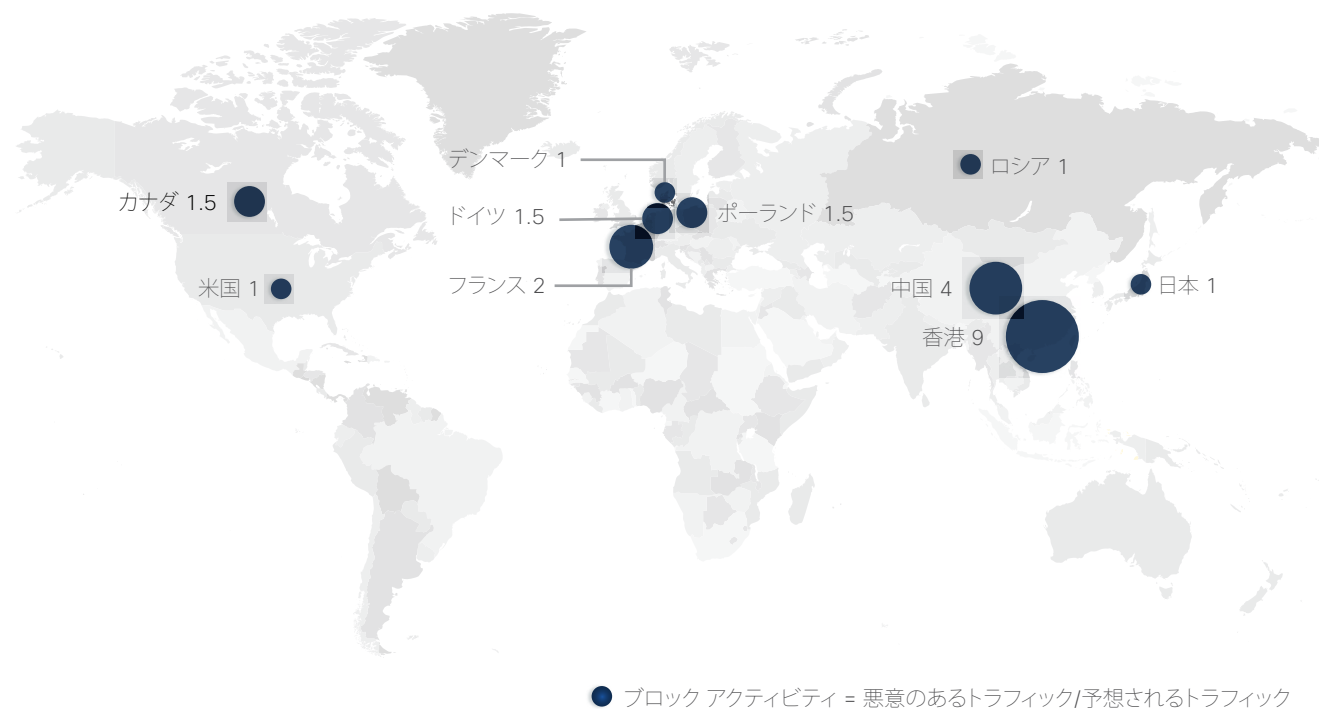
共有    

Web ブロック アクティビティ:地域別の概要

シスコはまた、マルウェアベースのブロック アクティビティの元となっている国と地域を調べました(図 23)。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。悪意のある攻撃者は国境を意識することなく、最も効果的なマルウェアをホストします。

図 23. 国または地域別 Web ブロック



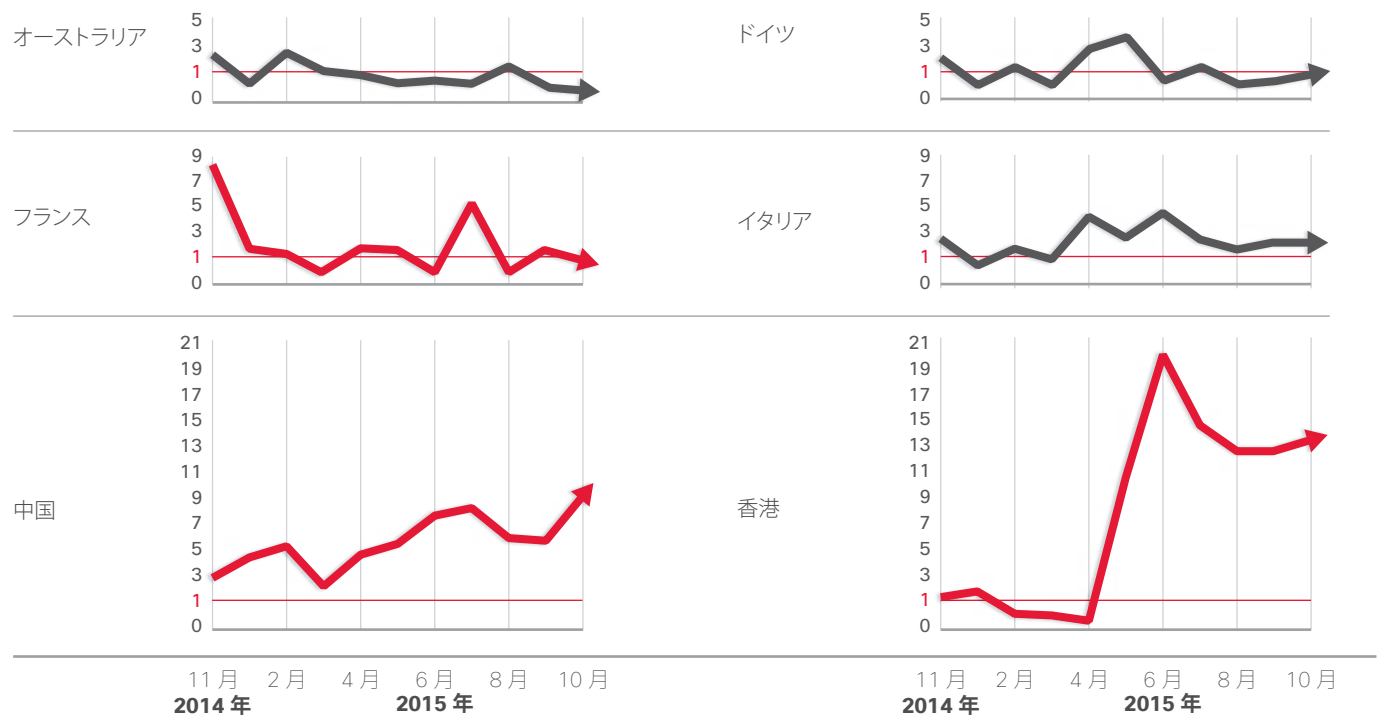
出典:シスコ セキュリティリサーチ

また、商業的に発展している大規模ネットワークが存在し、大量のインターネットトラフィックが処理されていることが、高いブロックアクティビティのもう 1 つの要因として考えられ、香港が 1 位になったのはそうした理由もあります。

2015 年の春先から、フランスに代わって香港の Web ブロックアクティビティが通常より多くなったことに注目してください。両国とも以降は Web ブロックアクティビティが著しく減りますが、当初のアクティビティ率が基準をはるかに上回っていたため、最近になって減少しても、年度末には年度初めより香港の順位が非常に上がっています。フランスのアクティビティの急増は、夏中盤までに通常のレベルに戻りました。

図 24 は、2014 年 11 月から 2015 年 10 月までの国別または地域別の月ごとの比較を示しており、こうした順位の背景を説明しています。

図 24. 国または地域別 Web ブロック数(月ごとの比較、2014 年 11 月～ 2015 年 10 月)



出典:シスコ セキュリティリサーチ

業界の洞察

業界の洞察

シスコでは、セキュリティのトレンドと実践に関する調査と分析を実施しています。逆説的ですが、セキュリティ機能によって防御側が脅威を追跡することが困難になり、組織や個人ユーザが侵入や攻撃にさらされるリスクが増大する場合があります。

暗号化: 成長著しいトレンド、防御側にとっての課題

暗号化には十分な意義があります。企業は自社の知的財産などの機密データを保護する必要があり、広告主は広告コンテンツとバックエンド分析の完全性を維持する必要があります。また、顧客のプライバシー保護に重点を置く企業が増えています。

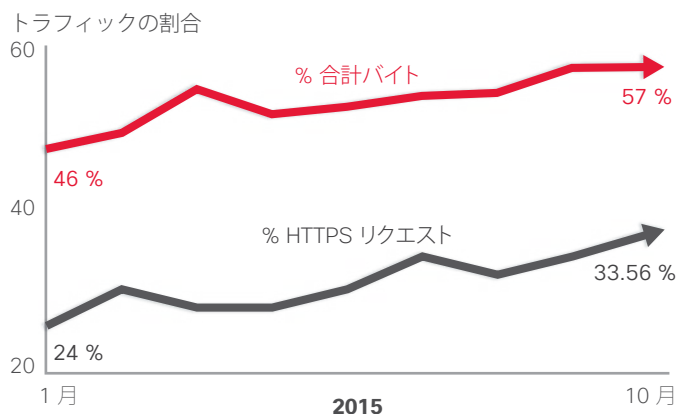
ただし、暗号化により、組織が誤った安心感を得るなどのセキュリティ問題が生じることも事実です。組織は、データがエンティティ間で送信される場合の暗号化に関してはうまく実行できるようになりましたが、多くの場合、保管中のデータの安全性は確保されていません。ここ数年の最も重要な侵害の多くは、データセンターなどの社内システムに保存された非暗号化データを利用するものでした。攻撃者にとって、これはまるで鍵のかかっていない倉庫まで物資を運ぶ安全なトラックを追跡するようなものです。

また、エンドツーエンドの暗号化が一部のセキュリティ製品の効果を抑える場合があることを理解することも重要です。暗号化は、悪意のあるアクティビティの特定や追跡に使用する侵害の指標を隠してしまいます。

ただし、機密データを暗号化しないというのは論外です。セキュリティツールとそのオペレータは、データストリームのヘッダなどの非暗号化情報を他のコンテキスト情報のソースとともに収集して暗号化トラフィックを分析することで、この新しい状況に適応する必要があります。フルパケットキャプチャなどのペイロードの可視性に依存するツールの効果は減少しています。今必要とされているのは、Cisco NetFlow などのメタデータベースの分析です。

当社の調査担当者は、2015 年のトレンドの観察によって、暗号化トラフィック、特に HTTPS が転換点に到達したことを示唆しています。これはまだトランザクションの主流ではありませんが、すぐにインターネット上のトラフィックの主要な形式となるでしょう。実際、当社の調査によると、暗号化トラフィックは転送されるバイトの 50 % 以上を安定して独占しています (図 25)。これは、HTTPS のオーバーヘッドや、ファイルストレージサイトへの転送など、HTTPS を介して送られる大容量のコンテンツなどによります。

図 25. SSL の割合



出典:シスコ セキュリティリサーチ

どの Web トランザクションでも、大量のデータが送信 (アウトバウンド) され、受信 (インバウンド) されています。HTTPS トランザクションには、HTTP のアウトバウンド要求より約 2000 バイト多いアウトバウンド要求があります。HTTPS のインバウンド要求にもオーバーヘッドはありますが、応答が大きいため重要性は高くありません。

共有    

Web トランザクションごとの入出力バイトを組み合わせることで、Web トランザクションごとに関与する全バイトのうち、HTTPS を使用して暗号化されている割合を決定できます。HTTPS トラフィックと追加オーバーヘッドの増加により、2015 年 1 月には 46 % だった HTTPS バイトがすべての Web トラフィックに占める割合は、10 月には 57 % まで上昇しました (図 25)。

また、HTTPS 要求が徐々に増え続けており、2015 年 1 月時点と比較するとその増加が著しいことも Web トラフィック分析によりわかります。図 25 で示すように、1 月の要求の 24 % は HTTPS プロトコルを使用し、残りは HTTP を使用していました。

10 月までに確認された要求の 33.56 % が HTTPS を使用していました。さらに、インバウンドの HTTPS バイトの割合が増加していることもわかりました。これは年間を通じてあてはまりました。HTTPS を使用するトラフィック量が増加すると、より多くの帯域幅が必要になります。トランザクションごとに 5 kbps がさらに必要です。

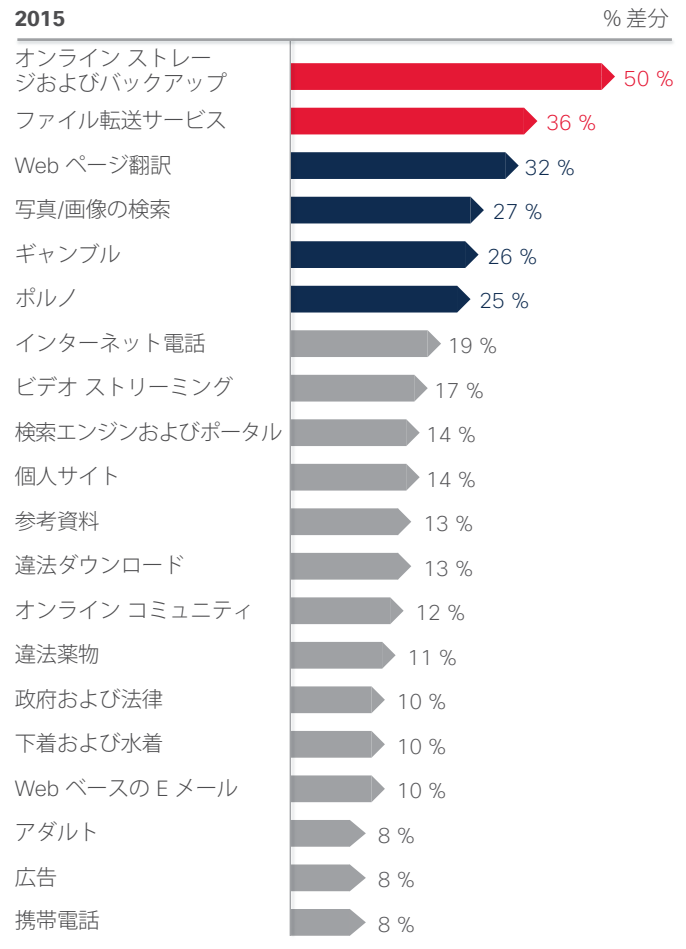
暗号化された Web トラフィックの全体的な増加の原因として、主に以下の要因が考えられます。

- モバイル アプリケーション トラフィックの増加 (本質的に暗号化されている)
- 暗号化されたビデオのダウンロード要求の増加
- 攻撃対象となる「機密データを安全に」保持するストレージとバックアップ サーバへの要求の増加

事実、図 26 に示すように、オンライン ストレージおよびバックアップ リソースへの HTTPS の要求は、2015 年初めから 50 % 増加しています。ファイル転送サービスも同じ期間中に 36 % と大幅に増加しました。

つまり、暗号化されたトランザクション数と、各トランザクション内の暗号化されたバイト数の両方で、暗号化アクティビティの発生数が増加していると言えます。それぞれ独自の利点と潜在的リスクがあるため、可視性を高めるのに役立つ、統合された脅威に対する防御が必要になります。

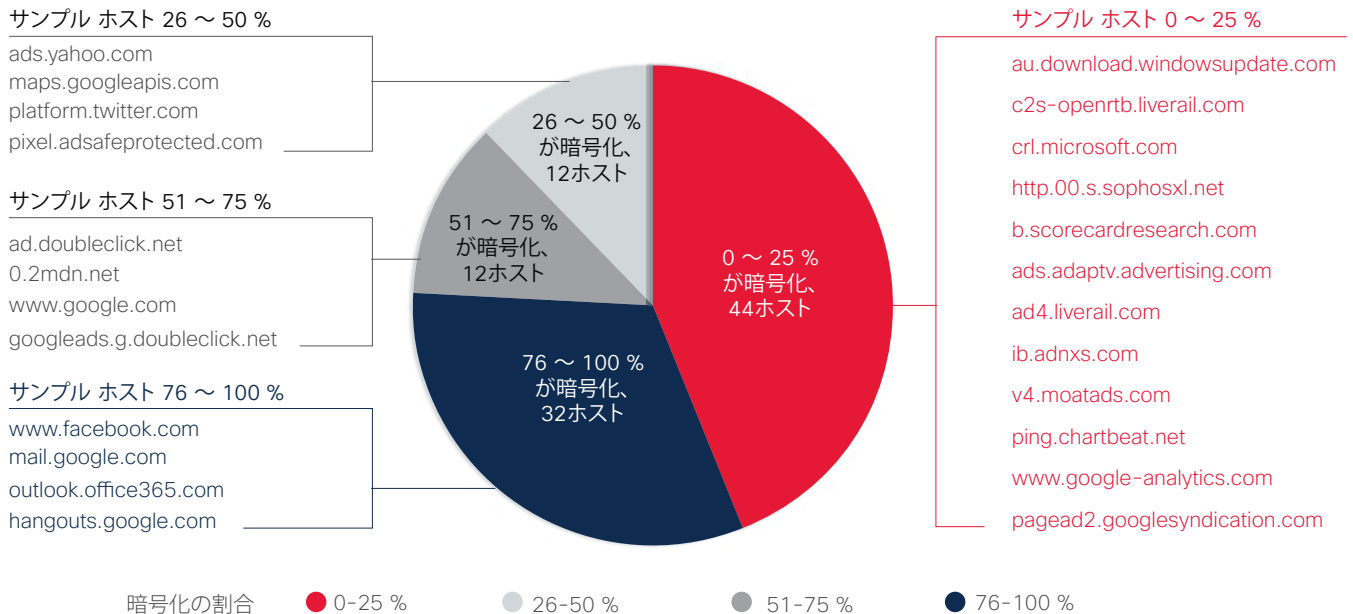
図 26. HTTPS 要求: 2015 年 1 月から 9 月にかけて最大の変化



出典:シスコ セキュリティリサーチ

共有    

図 27. HTTPS トラフィックを暗号化する上位ホスト



出典:シスコ セキュリティリサーチ

要求の多い上位ドメイン(図 27)を見ると、Google と Facebook のメイン コンテンツ ページの多くが暗号化されていることがわかります。通常、暗号化されている広告トラフィックはわずか 10 % です。

データ暗号化は、課題はあるものの、脅威が取り巻く現在の環境において必須となっています。攻撃者はきわめて巧みにユーザのアクセス制御を回避し、ストレージや転送のあらゆる段階で重要な情報が保護されないようにします。

このため、セキュリティ チームは Web トラフィックのパターンを監視し、HTTPS 要求が疑わしい場所に関係するものでないかを確認する必要があります。定義済みポート上の暗号化トラフィックだけに注目しないでください。当社の調査では、次のセクションで説明するように、さまざまなポートでマルウェアが暗号化通信を開始する可能性が高いことがわかっています。

エントロピー ファクタ

高いエントロピーは、暗号化または圧縮されたファイル転送または通信を示す優れた指標となります。⁶基本的な暗号プロトコルの知識を必要としないため、エントロピーの監視は比較的容易である点もセキュリティ チームにとって有利です。

2015 年 6 月 1 日から始まった 3 ヶ月の調査期間中に、シスコのセキュリティ調査担当者は、提出された 598,138 個の「脅威スコア:100」のマルウェア サンプルから、7,480,178 のフローを確認しました。この期間中、958,851 個、つまり 12.82 % の高エントロピー フローがありました。

また、Transport Layer Security (TLS) プロトコル上で 917,052 個 (12.26 %) のフローを確認しました。保護された HTTP のデフォルト ポートである 443 以外のポートでは、8419 個の TLS フローがありました。確認されたマルウェアが通信に使用したポートの一部は、21、53、80、500 でした。

暗号化されたインターネットトラフィックのレベルが上昇するにつれ、統合型の脅威に対する防御アーキテクチャを導入することがますます重要になります(「統合された脅威に対する防御の 6 つの原則」、62 ページを参照)。ポイント ソリューションは暗号化トラフィックの潜在的な脅威の特定には効果がありません。統合型セキュリティ プラットフォームでは、セキュリティ チームはデバイスやネットワークで何が起きているかをより深く理解できるようになり、疑わしい活動パターンを容易に特定することができます。

⁶ エントロピー: コンピューティングでは、エントロピー (無秩序さや予測の困難度) とは、オペレーティング システムやアプリケーションが、ランダムなデータを必要とする暗号化などの用途に使用するために集めた乱数を指します。

❗ 暗号化への流れ: ケース データ

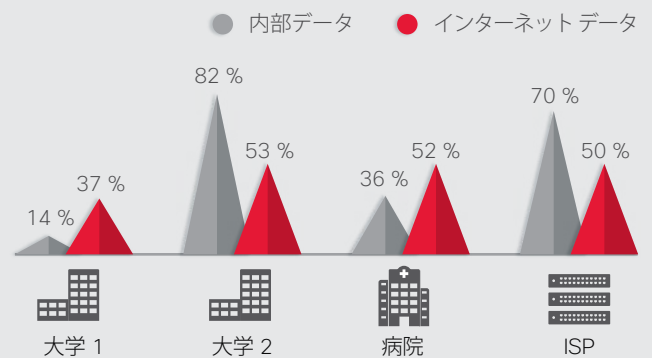
シスコ傘下の Lancope は、3つの業種(大学 2 校、病院、ISP プロバイダ、すべて米国に拠点を置く)で内部およびインターネットのトラフィックの暗号化率を調査しました。

大学のうち、1 校はほぼすべての内部トラフィックが暗号化されていることがわかりました(82%)。また、同大学のインターネットトラフィックの 53% は暗号化されていました。これらの結果は、Lancope が他の業種で観察した傾向と同じ水準でした。

病院の内部データのうち、暗号化されていたのはわずか 36% でしたが、しかし、インターネットトラフィックの半分以上(52%)が暗号化されていました。

大手 ISP プロバイダでは、内部トラフィックの 70% が暗号化され、インターネットトラフィックの 50% が暗号化されていました。

Lancope が行ったこの調査から、さまざまな業界でデータの暗号化が幅広く普及している様子が伺えます。シスコは、組織への侵害の影響を抑えるために、保管中のデータの暗号化にも同様に注力すべきだと推奨しています。



出典: Lancope Threat Research Labs

オンライン犯罪者による WordPress サーバ アクティビティが増加

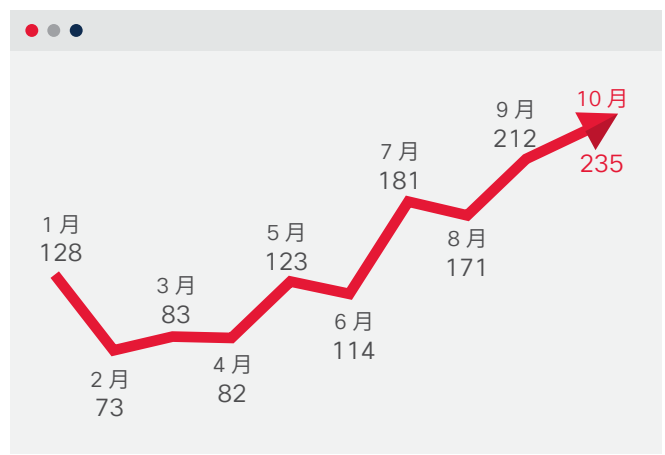
このレポートの概要で説明したとおり、オンライン犯罪者は摘発を避ける新たな方法だけでなく、その活動の効率とコストを削減するための方法も追求し続けています。その格好の標的として、Web サイトやブログの著名な開発プラットフォームである WordPress を使用して作成した Web サイトを狙うサイバー犯罪者が増えています。WordPress のサイトでは、攻撃者がサーバに侵入し、その安定したストリームを制御して、ランサムウェア、銀行詐欺、フィッシング攻撃をサポートするインフラストラクチャを作成することができます。インターネットには、セキュリティの観点から見て管理が放棄された状態の WordPress で作成されたサイトがあふれています。新しいセキュリティ問題が表面化する場合、これらのサイトが侵入を受け、攻撃に組み込まれていることが数多くあります。

シスコのセキュリティ調査担当者は、ランサムウェアなどのマルウェアのサポートに使用されるシステムを分析して、多くのオンライン犯罪者のオンライン アクティビティが、侵害された WordPress サーバにシフトしていることを突き止めました。犯罪者によって使用された WordPress ドメインの数は、2015 年 2 月から 10 月までの間で 221% 増加しました(図 28 を参照)。

シスコの調査担当者は、この犯罪拠点の移行にはいくつかの理由があると見ています。ランサムウェアが他のツールを使用して

暗号キーまたは他の指揮および統制情報を伝達する場合、これらの通信を検出またはブロックすることができるので、暗号化プロセスは完了できません。しかし、感染した WordPress サーバを介して暗号キーをリレーする通信は一見正常なため、ファイルの暗号化が完了する可能性が高まります。つまり、WordPress サイトがリレー エージェントとして機能するのです。

図 28. マルウェア作成者が利用する WordPress ドメインの数



出典: シスコ セキュリティリサーチ

他のテクノロジーの欠点を回避するため、犯罪者は WordPress を使用してマルウェアのペイロードと指揮および統制サーバをホストすることにしました。WordPress のサイトにはいくつかの利点があります。たとえば、放棄されたサイトの多くはセキュリティ保護が脆弱で、犯罪者がサイトに侵入するすきを与えます。

感染したシステムを使用してマルウェアの操作を実行する場合のリスクは、侵害が検出されると、そのハッキングされたサーバを停止されるというものです。これが攻撃の最中に発生すると、マルウェア ダウンローダはそのペイロードを取得できないか、マルウェアが指揮および統制サーバと通信できなくなる可能性があります。シスコのセキュリティ調査担当者は、マルウェアが複数の WordPress サーバを使用することでこの課題を解決していることに気づきました。さらに、感染した WordPress サーバのリストが Pastebin などのデータ共有サイトに保存されていることを発見しました。

マルウェアはこのリストを使用して、感染したサーバが停止されてもマルウェアが機能できる、有効な指揮および統制サーバを探したのです。調査担当者は、ペイロードを保存する WordPress サイトのリストを含むマルウェア ダウンローダも特定しました。1 つのダウンロード サイトが機能しないと、マルウェアは次のサイトに移動し、有効な WordPress サーバから悪意あるペイロードをダウンロードします。

感染した WordPress サイトの多くは最新バージョンの WordPress を実行しておらず、管理者パスワードが脆弱で、セキュリティ パッチのないプラグインを使用していました。

これらの脆弱性が原因となり、攻撃者が WordPress サーバに狙いをつけ、マルウェアのインフラストラクチャとして使用したのです (図 29 を参照)。

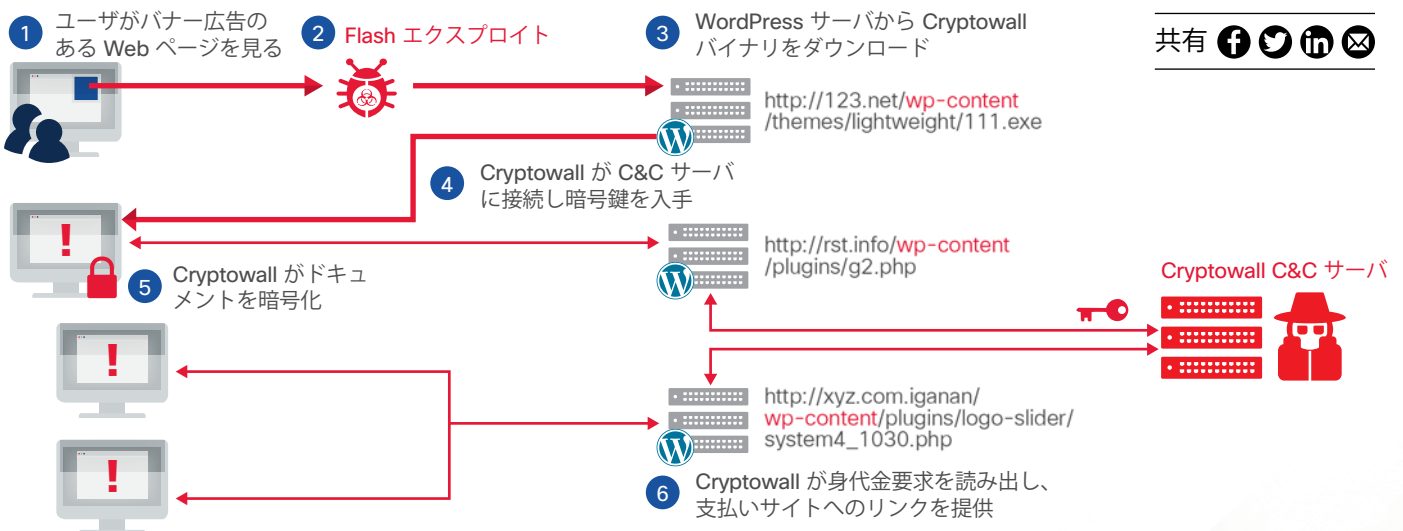
シスコの調査担当者は、感染した WordPress サイトでホストされることの多いソフトウェアとファイル タイプの一部を確認しました。

- エクスプロイト キットによる攻撃用ペイロードである実行可能ファイル
- Dridex や Dyre などのマルウェアのコンフィギュレーション ファイル
- 指揮および統制インフラストラクチャを隠す指揮および統制通信を中継するプロキシ コード
- ユーザ名とパスワードを収集するフィッシング Web ページ
- エクスプロイト キット サーバにトラフィックをリダイレクトする HTML スクリプト

さらに、シスコの調査担当者はインフラストラクチャに WordPress の感染サイトを使用する多くのマルウェア ファミリーを特定しました。

- Dridex 情報窃盗
- Pony パスワード窃盗
- TeslaCrypt ランサムウェア
- Cryptowall 3.0 ランサムウェア
- TorrentLocker ランサムウェア
- Andromeda スпам ボットネット
- Bartallex トロイの木馬ドロッパー

図 29. WordPress サイトが侵害されるしくみ



出典:シスコ セキュリティリサーチ

- Necurs 情報窃盗
- 偽のログイン ページ

犯罪者が WordPress をホスティングすることでもたらされる脅威が懸念される場合、セキュリティ プロフェッショナルは、WordPress で作成されたサイトからのコンテンツのフローを調べる Web セキュリティ テクノロジーを探さなければなりません。ネットワークが単なる Web ページやイメージではなく、WordPress サイトからプログラムをダウンロードしている場合、このようなトラフィックは異常であると見なすことができます (ただし、WordPress サイトが正当なプログラムをホストする可能性はあります)。

老朽化するインフラストラクチャ:10年越しの問題

現在、インターネット接続、デジタル化、事業の成功は IT と OT (運用テクノロジー) のインフラストラクチャに依存していることから、すべての企業はある意味 IT 企業であると言えます。これは、企業は IT セキュリティを優先する必要があることを意味します。しかし、多くの組織は、古い旧式のコンポーネントと脆弱なオペレーティング システムで構築された、サイバー攻撃に弱いネットワーク インフラストラクチャに依存しています。

当社は最近、老朽化したインフラストラクチャ (および脆弱性へのパッチの適用の軽視) がもたらすセキュリティ リスクに注目してもらうため、インターネット上および顧客環境にある 115,000 台のシスコ デバイスを分析しました。

115,000 台のデバイスは、インターネットをスキャンして得られた 1 日分のサンプルと、その後デバイスを「裏側から」確認することで特定しました (インターネットからの観点とエンタープライズへの観点から)。当社のスキャンと分析により、115,000 台のデバイスのうち 106,000 台で実行されているソフトウェアに既知の脆弱性があることがわかりました。これは、当社のサンプルのうち、インターネット上にあるシスコ デバイスの 92 % が既知の脆弱性の影響を受ける可能性があることを意味します。

! このトピックの詳細については、シスコ セキュリティ ブログの投稿をお読みください。

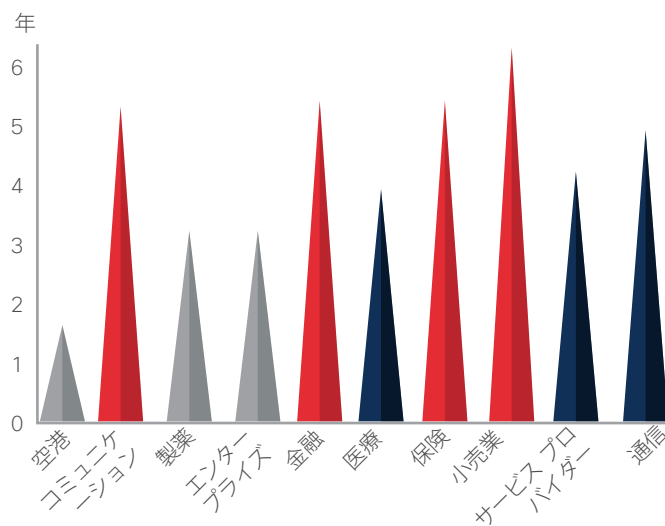
「IT セキュリティ:成熟度が過大評価されるとき」[英語]

「進化する Cisco IOS デバイスへの攻撃」[英語]

「SYNful Knock: Cisco IOS ソフトウェアへの攻撃の検出と緩和」[英語]

また、これらのデバイスで実行されているソフトウェア バージョンに平均で 26 の脆弱性があることがわかりました。さらに、多くの組織がネットワーク インフラストラクチャで古いソフトウェアを実行していることがわかりました (図 30)。金融、医療、小売業の顧客は、6 年以上前のバージョンのシスコ ソフトウェアを使用していました。

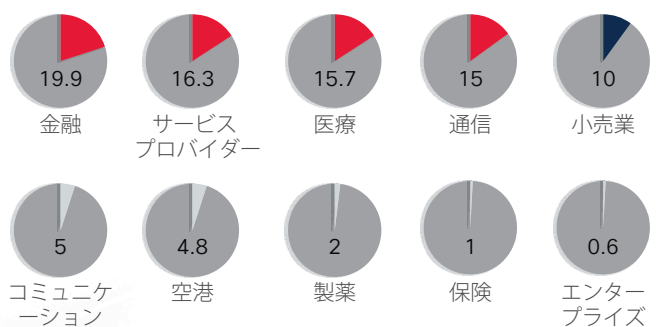
図 30. ソフトウェアの平均使用年数



出典:シスコ セキュリティリサーチ

また、分析したインフラストラクチャ デバイスの多くがサポート終了日 (LDoS) を経過しており、これらのデバイスの更新や安全性の向上ができないことがわかりました (図 31)。これらのデバイスは既知の脆弱性に対するパッチも受信していないので、新しい脅威に関する情報を受け取ることができません。当社は顧客にこの問題を通知しました。

図 31. インフラストラクチャ デバイス向け LDoS の割合



出典:シスコ セキュリティリサーチ

また、分析したサンプルの 115,000 台のデバイスのうち、8 % がサポート終了段階に達しており、別の 31 % は 1 ~ 4 年以内にサポートが終了します。

老朽化した旧式の IT インフラストラクチャは、組織の脆弱性となります。Internet of Things (IoT) や Internet of Everything (IoE) が普及するにつれて、安全なネットワーク インフラストラクチャに依存し、ネットワークを経由するデータと通信の整合性を確保することの重要性がますます高まっています。これは IoE の成功に不可欠です。

シスコのお客様の多くは、10 年前にネットワーク インフラストラクチャを構築しています。その当時、多くの企業はインフラストラクチャに 100 % 依存するようになるとは考えていませんでした。また、インフラストラクチャが攻撃の主な対象となるとも予測していませんでした。

インフラストラクチャの更新は高価でネットワークのダウンタイムを必要とするため、避けられがちです。簡単な更新では不十分なこともあるでしょう。一部の製品はアップグレードするには古すぎて、ビジネスを保護するために必要な最新のセキュリティソリューションを組み込むことができません。

上記の事実だけでも、インフラストラクチャを維持する重要性がわかります。組織は、定期的なアップグレードを計画し、敵に先を越される前に、重要なインフラストラクチャを積極的に管理することの価値を認識する必要があります。

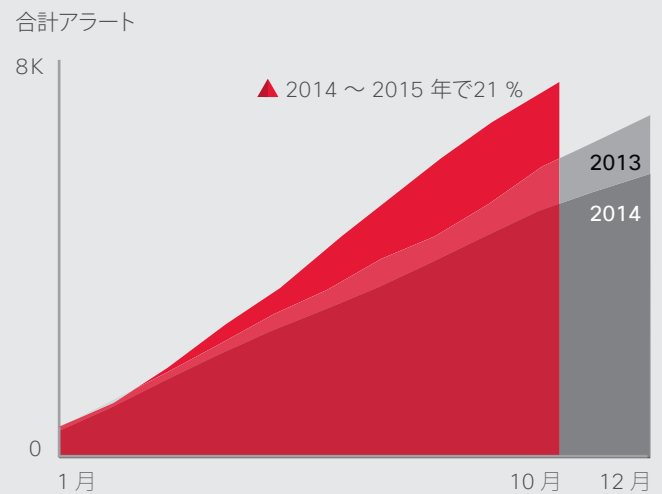
⚠ アラートの累計数が脆弱性管理へのコミットメントの増大を示す

老朽化したインフラストラクチャへの依存は、攻撃者にうってつけの突破口となります。しかし、オープンソースおよび独自ソリューションの製品脆弱性を含めて、アラートの累計数が増加していることは、テクノロジー業界が攻撃者に機会を与えないように慎重になっていることを示唆しています。

アラートの累積数は、2014 年から 2015 年にかけて 21 % 増加しました。特に 2015 年 7 月から 9 月までに著しい拡大が見られました。この増加の大部分は Microsoft、Apple などのベンダーからの主要ソフトウェアアップデートに起因すると考えられます。これは、製品のアップデートがソフトウェアの脆弱性についてのレポートの増加につながるためです。

現在、主要なソフトウェアベンダーがパッチとアップグレードを大量にリリースし、この活動についてベンダーはより透明性を高めています。このアラート数の増加が、システムボリュームとソフトウェアインベントリ、脆弱性と脅威に関する情報の管理に役立つセキュリティインテリジェンスと管理プラットフォームを使用して、脆弱性管理を自動化している組織を後押ししています。これらのシステムとアプリケーションプログラミングインターフェイス (API) を使用することで、より効率的でタイムリーな、効果的なセキュリティ管理を企業規模の大小を問わず実現できます。

図 32. 年間累積アラート総数



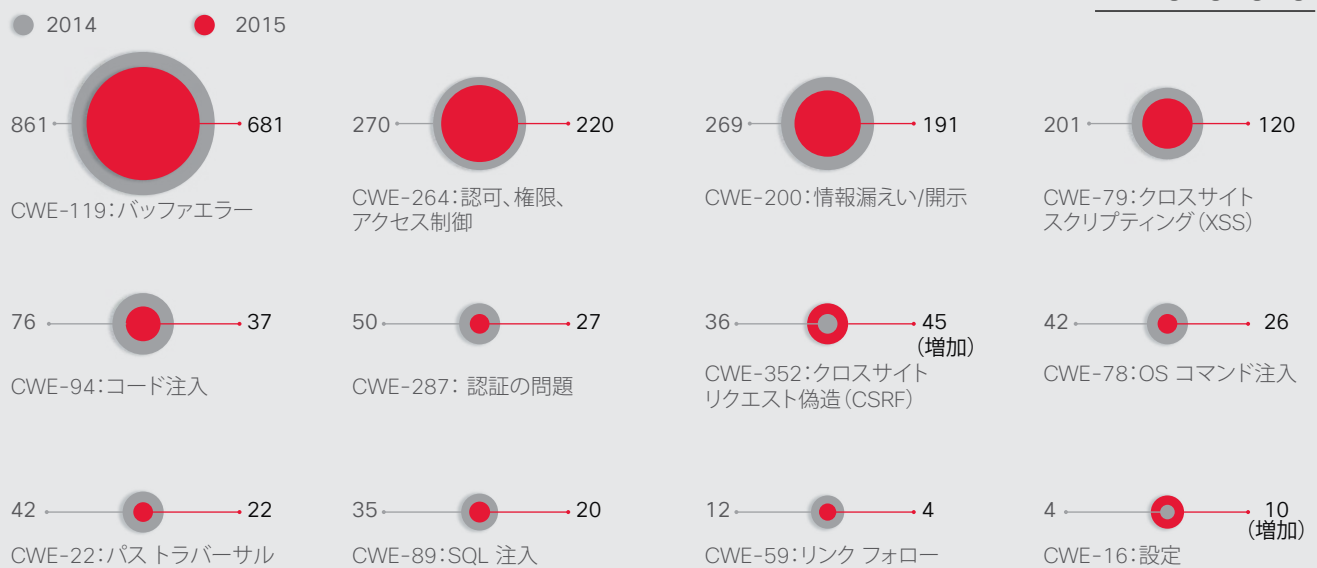
出典:シスコ セキュリティリサーチ

⚠ 脅威のカテゴリ: バッファ エラー、情報漏洩と情報開示の減少

一般的な脆弱性のカテゴリの調査では、クロスサイト スクリプティング (XSS) の脆弱性は 2014 年から 2015 年にかけて 47 % 減少しました (図 33)。この低下は、脆弱性テストに注目が集まった結果であると考えられます。ベンダーは、製品の販売前にこれらの脆弱性を特定し、修正する技能を高めています。

2015 年には情報漏洩や情報開示の脆弱性が 15 % 低下しました。これらの脆弱性は、明示的なアクセスをもたないサードパーティへの偶然の開示も含まれます。ベンダーがデータへのアクセスを許可または禁止する制御機能に注目するようになったため、このような一般的な脆弱性の発生頻度は低下しました。

図 33. 共通のカテゴリの脆弱性の数



出典: シスコ セキュリティリサーチ

共有    

「中小企業が各国のビジネスにおけるセキュリティ上の弱点に」

SMB は国の経済において重要な役割を果たします。顧客によってデータを委任される SMB には、オンライン攻撃者からこの情報を保護する責任もあります。ただし、2015 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で説明されているように (41 ページを参照)、SMB の攻撃に対する防御力は、この課題で必要とされる能力に到達していない兆候が見られます。これらの弱点は、SMB の顧客をリスクにさらすことにつながります。SMB のネットワークを侵害できる攻撃者は、企業ネットワークへのパスも見つけ出すことができます。

2014 年のシスコによるセキュリティ機能のベンチマーク調査結果から判断すると、SMB が使用する侵害分析を行うプロセスや脅威防御ツールの数は前年よりも減少しています。たとえば、2014 年では SMB の 59 % が Web セキュリティを活用したと回答していますが、2015 年では 48 % でした。パッチ適用ツールやコンフィギュレーション ツールを使用したと回答した割合は 2014 年は 39 % でしたが、2015 年ではわずか 29 % でした。

さらに、セキュリティ担当エグゼクティブを配置していない SMB の回答者のうち、約 4 分の 1 は自社がオンライン犯罪の格好の標的になるとは考えていませんでした。これは、最先端のオンライン攻撃を妨ぐことができるという過度の自信、もっと言えば、自社が攻撃を受けることなどありえないという考えを示唆するものです。

SMB がインシデント対応チームを使用する可能性は低い

多くの場合、SMB がインシデント対応チームおよび脅威インテリジェンス チームを配置する可能性は大企業よりも低くなります。予算的な制約がその一因として考えられます。回答者は、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際の最大の障壁の1つとして、予算を挙げています。どちらのチームも配置しているのは、大企業(従業員数 1,000 名以上)の 72 % に対して、従業員数 500 名未満の企業では 67 % でした。

SMB では、侵害を分析し、インシデントの原因を排除し、システムをインシデント発生前のレベルに復元するために使用するプロセスも少ないです(図 35)。たとえば、ネットワーク フロー分析を使用してシステムの侵害を分析しているのは、従業員数 10,000 名以上の企業では 53 % であるのに対し、従業員

数 500 名未満の企業では 43 % です。脆弱性が疑われるアプリケーションにパッチを適用し、更新を行っているのは従業員数 10,000 名以上の企業では 60 % であるのに対し、従業員数 500 名未満の企業では 51 % です。

SMB が脅威に対する防御を活用する割合は下降気味です。たとえば、2014 年には SMB の 52 % がモバイル セキュリティを使用していましたが、2015 年ではわずか 42 % です。また、2014 年に脆弱性スキャンを使用していた SMB は 48 % でしたが、2015 年には 40 % になっていました(図 36 を参照)。

図 36. 2015 年は SMB の防御が減少

セキュリティに対する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(あれば)はどれですか。	2014	2015
モバイル セキュリティ	52 %	42 %
安全なワイヤレス	51 %	41 %
脆弱性スキャン	48 %	40 %
VPN	46 %	36 %
セキュリティ情報およびイベント管理(SIEM)	42 %	35 %
ペネトレーション テスト	38 %	32 %
ネットワーク調査	41 %	29 %
パッチの適用および構成	39 %	29 %
エンドポイント調査	31 %	23 %

出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 34. SMB の最大の障害

次のうち、高度なセキュリティ プロセスやテクノロジーを採用するに当たって最大の障害と考えられるのはどれですか。

企業規模	250-499	500-999	1000-9999	10,000+
予算の制約	40 %	39 %	39 %	41 %
レガシー システムとの互換性の問題	32 %	30 %	32 %	34 %
競合する優先事項	25 %	25 %	24 %	24 %

出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 35. SMB は大企業よりも使用するセキュリティ プロセスが少ない

感染システムを分析するために、お客様の組織が使っているプロセス(あれば)はどれですか。

企業規模	250-499	500-999	1000-9999	10,000+
メモリ調査	30 %	34 %	34 %	37 %
ネットワーク フロー分析	43 %	47 %	52 %	53 %
相互に関連するイベント/ログの分析	34 %	34 %	40 %	42 %
外部(またはサードパーティ)のインシデント対応/分析チーム	30 %	32 %	34 %	39 %
システム ログ分析	47 %	51 %	55 %	59 %
レジストリ分析	43 %	43 %	49 %	52 %
IOC 検出	31 %	34 %	37 %	36 %

感染したシステムをインシデント前の業務可能なレベルに復元するために、お客様の組織はどのようなプロセスを使っていますか。

脆弱性を持つと見なされたアプリケーションにパッチを適用し、更新している	51 %	53 %	57 %	60 %
検出機能や制御機能を追加または新規導入している	49 %	55 %	57 %	61 %

出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

SMB では大企業と比べて防御ツールの使用が少ない傾向にあることが、なぜ重要になるのでしょうか。セキュリティ環境では、攻撃者がネットワークに入り込み、検出されないようにするより高度な戦術を練っています。よって、組織がネットワークを保護せずに放置したり、将来の再発を回避するために侵害がどのように発生したか把握するプロセスを延期できる状況ではありません。

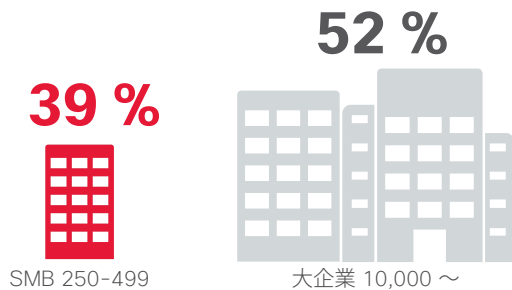
また、SMB は自社の脆弱性が大企業の顧客やそのネットワークに対するリスクへ変わることを認識していない場合があります。現在、犯罪者は、1 つのネットワークに入り込んで別のより有益なネットワークへのエントリポイントを探ることが多く、SMB は、そのような攻撃の開始ポイントとなるおそれがあります。

公共のデータ漏洩への対応経験が少ない

SMB は、大企業と比べて公共のセキュリティ違反に対応した経験が少ない場合があります。これは、ネットワーク側からみて、SMB のフットプリントが小さいことが原因であると考えられます。従業員数 10,000 名以上の企業の 52 % が公共のセキュリティ違反への対応経験がありますが、従業員数 500 名未満の企業ではわずか 39 % でした。

図 37. SMB が公共のセキュリティ違反を報告することは少ない

公共のセキュリティ違反に対処しなくてはならなかった



出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

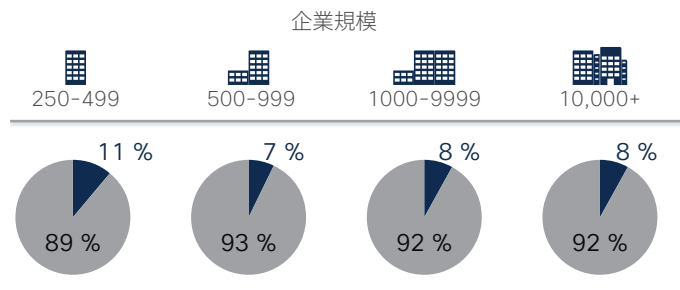
共有    

公共のセキュリティ違反は、言うまでもなくビジネスを中断させ、損害を与えるものですが、1 つだけ利点があります。これがきっかけとなり、企業が自社のセキュリティ保護について詳しく調べ、それらの強化を検討するようになることです。シスコの調査データ (74 ページを参照) によると、大企業が公共のデータ漏洩の影響を受けると、セキュリティ技術を大幅にアップグレードし、より強力なプロセスを実装するようになります。

図 38. SMB は自社を価値あるターゲットとして認識していない

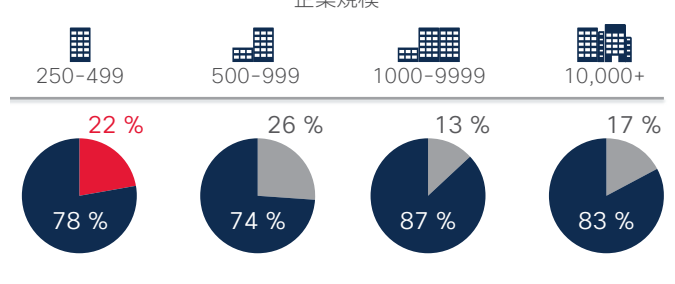
セキュリティの直接責任者であり、説明責任を負う幹部を組織内に置いていますか。

● はい ● いいえ



組織は攻撃側にとって価値の高いターゲットではない (セキュリティの直接責任者であり、説明責任を負う幹部を組織内に置いていない理由)

● はい ● いいえ



出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

自らがサイバー犯罪のターゲットとなるということに関する SMB の認識が、脅威の状況認識に関するギャップで見取れます。上記の図 38 で示すように、従業員数 500 名未満の企業の 22 % は、自社を価値の高いターゲットとして見ていないため、セキュリティに直接責任を持つエグゼクティブを配置していません。

2015 年はセキュリティ機能を外部に委託する SMB が増加見込み





この調査結果では、全体的にセキュリティ機能を外部に委託する SMB が増えていることを示していますが、一般にアドバイスやコンサルティングなどのサービスを外部に委託する SMB の割合は大企業よりも低くなります。たとえば、大企業の 55 % はアドバイスやコンサルティング サービスを外部に委託していますが、従業員数 500 名未満の企業では 46 % です。大企業の 56 % がセキュリティ監査タスクを外部に委託していますが、従業員数 500 名未満の企業では 42 % でした(図 39 を参照)。

ただし、2015 年では少なくとも一部のセキュリティ サービスを外部に委託する SMB が増えています。2014 年には従業員数 500 名未満の企業の 24 % が外部委託サービスを使用していないと回答していました。2015 年では、同じ回答をした SMB はわずか 18 % でした。

セキュリティを管理する手段として外部委託を採用する SMB が増加しているという事実はよい知らせです。SMB が少ないスタッフや予算に負担を強わずにネットワークを保護するための柔軟なツールを求めていることがわかります。ただし、SMB はセキュリティ プロセスの外部委託がネットワーク侵害の可能性を大幅に低減すると誤って考えてしまう場合があります。サードパーティにセキュリティの責任を押し付けるかもしれません。しかし、このような視点は希望的観測に終わるでしょう。なぜなら、エンタープライズ レベルのセキュリティ保護を提供できるのは、攻撃を調べて影響を軽減するだけでなく、それを防ぐ完全に統合された脅威に対する防御システムのみだからです。

図 39. 2015 年はより多くの SMB がセキュリティ サービスを外部に委託する

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(あれば)はどれですか。

企業規模	 250-499	 500-999	 1000-9999	 10,000+
アドバイスとコンサルティング	46 %	51 %	54 %	55 %
モニタリング	45 %	46 %	42 %	44 %
監査	42 %	46 %	46 %	56 %
インシデント対応	39 %	44 %	44 %	40 %
脅威インテリジェンス	35 %	37 %	42 %	41 %
修復	33 %	38 %	36 %	36 %
なし	18 %	12 %	11 %	10 %

お客様の組織 (250 ~ 499名の SMB) がそのサービスの委託を決めた理由はなんですか。



出典: シスコによる 2015 年セキュリティ機能のベンチマーク調査



シスコによるセキュリティ機能の ベンチマーク調査

シスコによるセキュリティ機能のベンチマーク調査

組織のセキュリティの状態に関するセキュリティ担当者の認識を把握するために、シスコでは、さまざまな規模の数カ国の組織の最高セキュリティ責任者 (CSO) とセキュリティ担当部署 (SecOps) マネージャにセキュリティリソースや手順についての考えを質問しました。2015 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では、現在使用中のセキュリティ機能とセキュリティ対策に関する成熟度を考察し、それらの結果を 2014 年に初めて開催した調査時の結果と比較します。

準備の兆候が見られるなかでの信頼度の低下

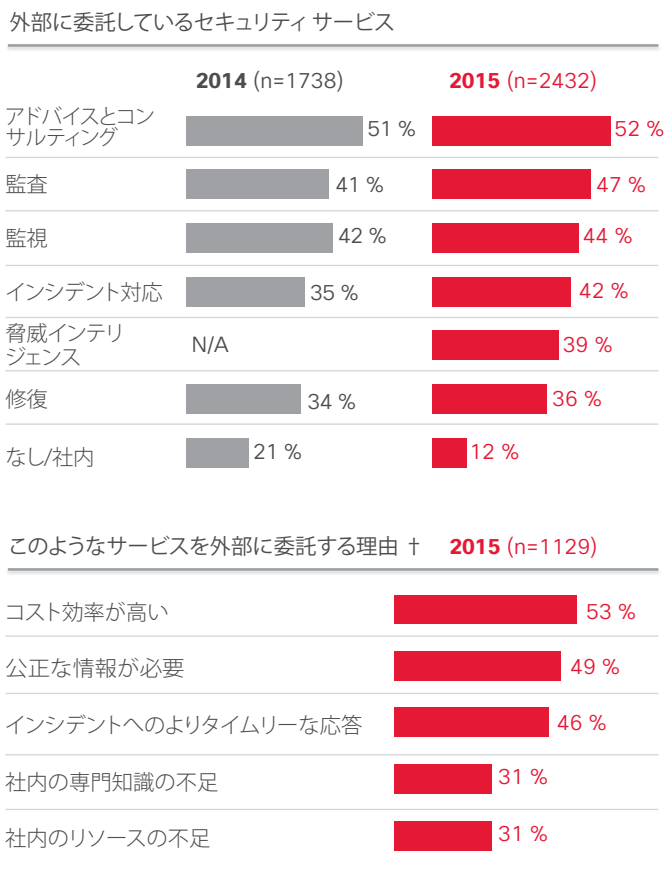
シスコの調査結果は、昨今の巧妙な脅威を受け、セキュリティプロフェッショナルの信頼度が揺らいでいることを示唆しています。一方、セキュリティについての懸念が深まるにつれ、これらのプロフェッショナルがネットワークを保護する方法が変化しています。たとえば、セキュリティトレーニングの増加、正式な文書化されたポリシーの増加、そしてセキュリティ監査、コンサルティング、およびインシデント対応などのタスクの外部委託の増加などが見られます。つまり、セキュリティプロフェッショナルはネットワークを襲う脅威に立ち向かおうとしているのです。

トレーニングと外部委託への流れは望ましい展開ですが、それだけでは十分ではありません。脅威を検出し、封じ込め、修復を向上させるツールとプロセスの使用を増やし続ける必要があります。予算的な制約とソリューションの互換性という障壁の中で、企業は統合型の脅威に対する防御を提供する有効なソリューションを検討する必要があります。セキュリティ業界は、公共のセキュリティ違反が発生したときに他の組織と連携して動く必要があります (SSHPsychos のボットネットとの連携など。[14 ページ](#)を参照)。知識を共有すれば、将来の攻撃を防ぐことができるからです。

リソース:外部委託を採用する組織が増加

セキュリティプロフェッショナルは、脅威を認識すると、コンサルタントまたはベンダーの方がより効率的に管理できるセキュリティタスクを外部に委託するなど、防御を強化する方法を模索します。2015年では、調査対象企業の47%がセキュリティ監査を外部に委託しており、2014年の41%から増加しました。また、2015年にインシデント対応プロセスを外部に委託したのは42%で、対して2014年では35%でした(図40)。

図40. 外部に委託されるサービスの概要



† セキュリティサービスを外部に委託しているセキュリティ担当者 (2015年, n=2129)

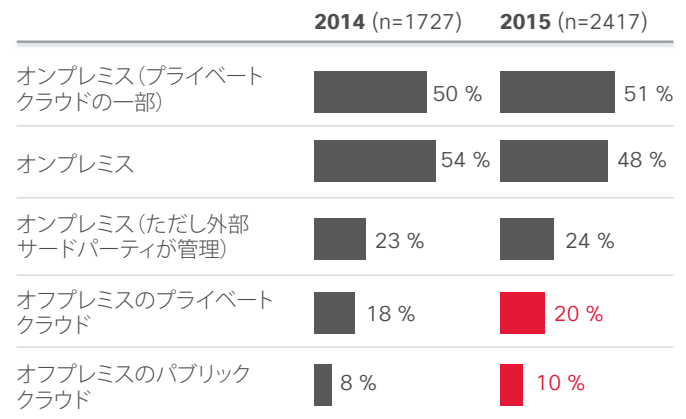
出典:2015年のシスコによるセキュリティ機能のベンチマーク調査

少なくとも一部のセキュリティ機能を外部に委託しているセキュリティプロフェッショナルが増えています。2014年には、調査回答者の21%がセキュリティサービスを外部に委託していませんでした。2015年にはこの数が12%に大幅減少しました。53%が外部委託をコスト効率の高さから実施していると回答し、49%が公正な洞察を得るためにサービスを外部に委託していると回答しました。

ネットワークやデータをさらに保護するため、セキュリティプロフェッショナルはオフプレミスでネットワークをホストするという概念を受け入れつつあります。まだオンプレミスでのホスティングが支持されていますが、オフプレミスのソリューションを使用するプロフェッショナルの数は増加しています。2015年には、20%がオフプレミスのプライベートクラウドソリューションを使用しているのに対して、2014年では18%でした(図41)。


図41. オフプレミスホスティングの増加

組織のネットワークのオンプレミスでのホスティングは引き続き最も多く見られますが、オフプレミスホスティングが昨年から増加



出典:2015年のシスコによるセキュリティ機能のベンチマーク調査

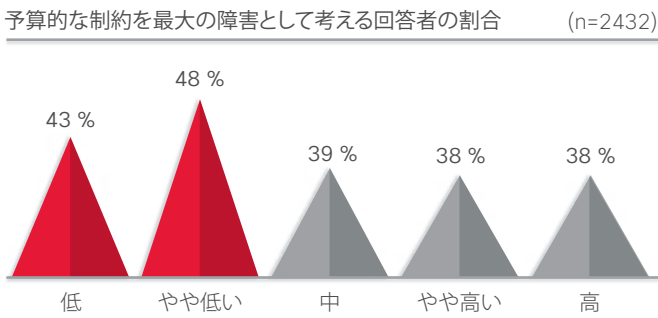
図 42. 予算的な制約はセキュリティのアップグレードの大きな障害となる

高度なセキュリティを導入する上での最大の障壁		2015 (n=2432)	
予算的な制約 	 39 %	知識の不足	 23 %
互換性の問題	 32 %	組織の文化/姿勢	 23 %
認定要件	 25 %	熟練スタッフの不足	 22 %
競合する優先事項	 24 %	効果が実証されるまでの購入への抵抗感	 22 %
現在の作業負荷が重すぎる	 24 %	経営陣の賛同	 20 %

出典: 2015 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

シスコが調査したセキュリティ チームは、ネットワークをより効果的に保護することに熱心ですが、計画の実行能力が限定されている場合があります。セキュリティ プロフェッショナルによると、予算的な制約 (39 %) がセキュリティ サービスやツールを選択または拒否する際の最大の理由であり、それにテクノロジーの互換性の問題 (32 %) が続きました (図 42 を参照)。予算的な制約は、下位から中程度の成熟度の企業にとってより大きな問題となっています (図 43 を参照)。全セキュリティ プロフェッショナルからの回答を見ると、高度なセキュリティ プロセスの導入の障害として予算的な制約を挙げたのは 39 % でした。この数値は成熟度が下位の範囲の企業では 43 %、中間の範囲の企業では 48 % にはね上がります。

図 43. 予算的な制約は、成熟度の低い会社にとって大きな障害となる



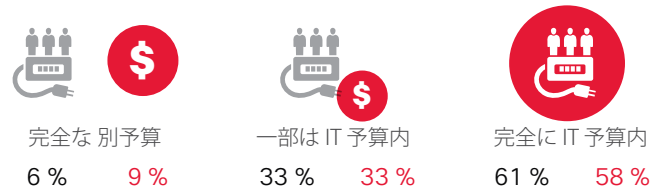
出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

組織がセキュリティ リソースについて深く検討していることを示す 1 つのサインは、セキュリティ予算の設定方法にあります。調査結果によると、IT 予算全体からセキュリティ予算を区別している組織の数はわずかに増加しています。2014 年では、プロフェッショナルの 6 % がセキュリティと IT 予算を完全に区別していましたが、2015 年にはその割合が 9 % に上昇しました (図 44 を参照)。

図 44. セキュリティ予算を別に組む組織がわずかに増加

セキュリティの予算は IT 予算の一部ですか。

2014 (n=1720) 2015 (n=2417)



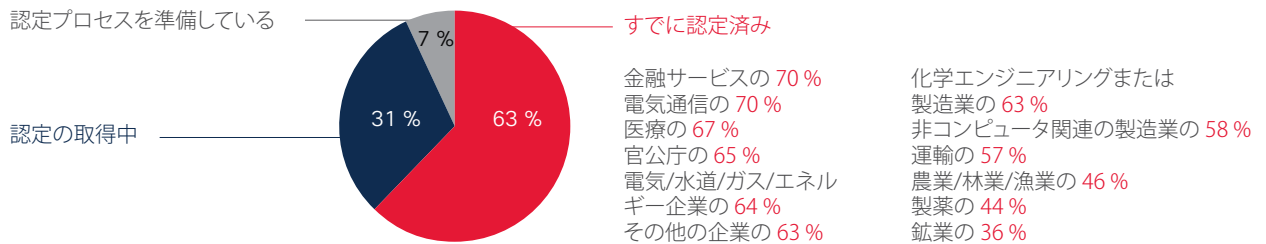
出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

組織がセキュリティ ポリシーを標準化したり、認定を受けようとすることは、セキュリティ向上への取り組みを示します。セキュリティ プロフェッショナルの約 3 分の 2 が、自社組織は標準化されたセキュリティ ポリシーやセキュリティ プラクティスの認定を

受けているか、認定途中であると述べています (図 45)。これは、企業がセキュリティ知識の向上と、脅威への対応に価値を見出しているというもう 1 つの良い兆候です。

図 45. ほとんどの組織は認定済みか、認定が必要だと感じている

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組織 (2015 年、n=1265)



出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

セキュリティ対策の活用方法を調査したところ、企業で最もよく使用されるセキュリティ ツールはファイアウォールであり (65%)、その後にデータ損失防止 (56%) と認証ツール (53%) が続きます (図 46 を参照)。2015 年に、企業のクラウドベースのツールへの依存はやや低くなりました。セキュリティ

プロフェッショナルはセキュリティ サービスの外部委託に意欲を示しますが (43 ページを参照)、ツールの社内導入がトレンドになりそうです。(完全なリストについては、71 ページを参照してください。)

図 46. ファイアウォールとデータ損失の防止が最もよく使用されるセキュリティ ツールである

クラウドベースのサービスを通じて管理している防御の内容 (セキュリティの脅威に対する防御を使用していると回答したセキュリティ担当者)

組織が利用するセキュリティ脅威防御	2014 (n=1738)	2015 (n=2432)	2014 (n=1646)	2015 (n=2268)
ファイアウォール *	N/A	65%		31%
データ損失の防止	55%	56%		
認証	52%	53%		
暗号化/プライバシー/データ保護	53%	53%		
電子メール/メッセージング セキュリティ	56%	52%	37%	34%
Web セキュリティ	59%	51%	37%	31%
ネットワーク、セキュリティ、ファイアウォール、侵入防止 *	60%	N/A	35%	

* ファイアウォールと侵入防御は、2014 年では 1 つのコードでした。「ネットワーク セキュリティ、ファイアウォール、および侵入防御」

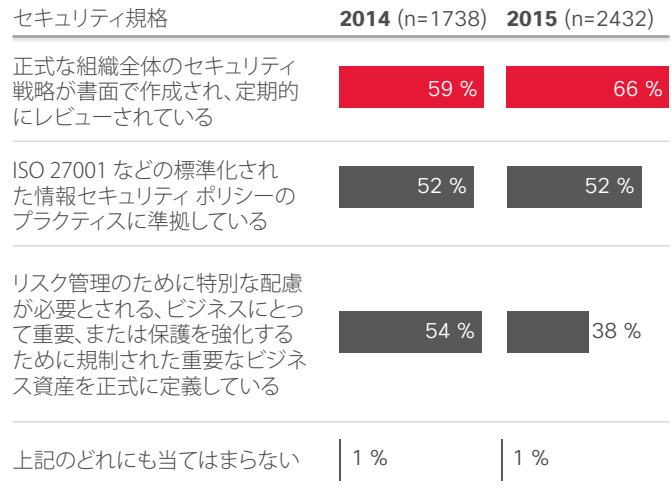
出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

機能：確信度の低下

セキュリティ インフラストラクチャが最新であると確信しているセキュリティ プロフェッショナルの数は、2014 年より 2015 年の方が減少しています。この確信度の低下は、幾度となく繰り返された大企業への強烈な攻撃と、それによるプライベート データの盗難、そしてネットワークへの侵入を許した会社による公的な謝罪によってもたらされたことは疑いの余地がありません。

しかし、この確信度の低下は、より強力なポリシー開発への関心の高まりを伴います。図 47 に示すように、2015 年には 2014 年 (59 %) よりも多くの企業 (66 %) が正式なセキュリティ戦略書を作成しています

図 47. 正式なセキュリティ ポリシーを作成する組織が増加している



出典：2015 年のシスコによるセキュリティ機能のベンチマーク調査



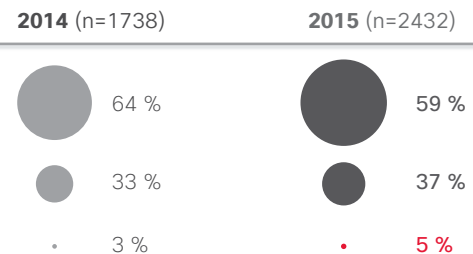
図 48. 2015 年は確信度が低下

御社のセキュリティ インフラストラクチャをどのように評価しますか。

当社のセキュリティ インフラストラクチャは最新であり、最良のテクノロジーが利用可能になると常に更新している

定期的にセキュリティ テクノロジーを交換もしくは更新しているものの、最新かつ最高のツールを備えてはいない

セキュリティ テクノロジーが古くなったり、機能しなくなった場合にのみ、またはまったく新しいニーズを発見した場合に、セキュリティ テクノロジーを交換もしくは更新している



出典：2015 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

確信度の低下は、セキュリティ プロフェッショナルのテクノロジーへの信頼度のわずかな低下に現れています。2014 年には、64 % がセキュリティ インフラストラクチャが最新であり、常にアップグレードされていると回答していました。2015 年には、その数が 59 % に減少しました (図 48)。また、2014 年に組織が最新のセキュリティ ツールを装備していないと回答したのは 33 % でしたが、この数は 2015 年に 37 % に上昇しました。

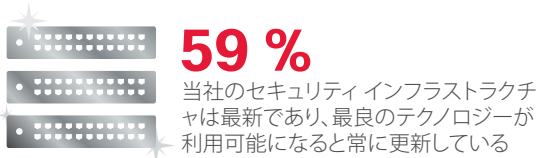
CSO はセキュリティ担当部署マネージャよりも楽観的であり、セキュリティ インフラストラクチャが最新であると考え、セキュリティ担当部署マネージャが 54 % であるのに対し、CSO は 65 % と、かなり高い信頼を示していました。セキュリティ担当部署マネージャの確信は、日常的なセキュリティ インシデントへの対応により、セキュリティの準備状況に不安を覚えたことが原因で低下したと思われる。

図 49. 侵害検出機能に対する確信度は不安定

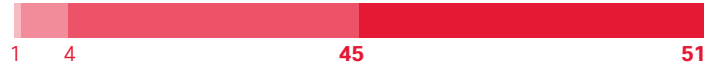
御社のセキュリティ インフラストラクチャをどのように評価しますか。

(2015 年, n=2432)

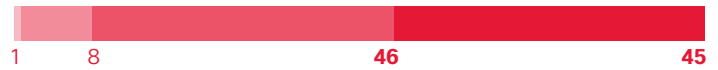
まったくそう思わない | そう思わない | そう思う | 非常にそう思う



セキュリティの弱点が本格的なインシデントになる前に検出できる組織の割合



侵害の範囲を判断し、それを修復できる自信がある組織の割合



出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

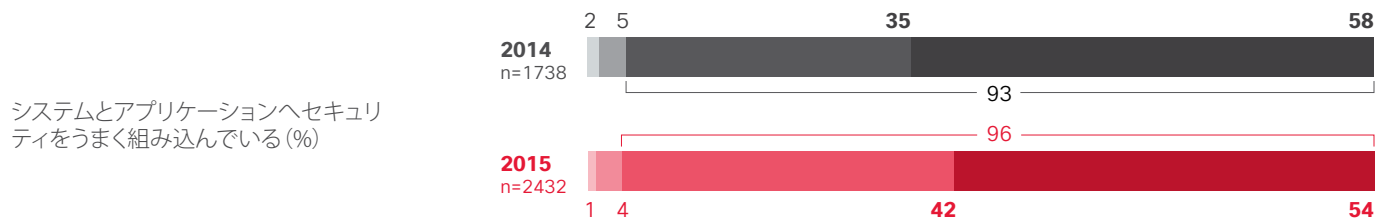
セキュリティ プロフェッショナルは、攻撃を阻止する能力についても複雑な確信度を示しています。51 % が本格的なインシデントになる前にセキュリティの弱点を検出できると強く確信していますが、ネットワーク侵害の範囲を決定して損害を修復する能力について自信があるのはわずか 45 % でした (図 49 を参照)。

セキュリティ プロフェッショナルは、攻撃からネットワークを保護する能力への確信度も弱いことを示しています。たとえば、2015 年には、システムの取得、開発、維持という手順へセキュリティをうまく組み込んでいると強く確信しているプロフェッショナルの割合は減少しています (2014 年の 58 % に対して 2015 年は 54 %。図 50 を参照)。(完全なリストについては、76 ページを参照してください。)

図 50. システムへのセキュリティ組み込み機能に対する確信度が低下

セキュリティ ポリシー

まったくそう思わない | そう思わない | そう思う | 非常にそう思う



出典: 2015 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

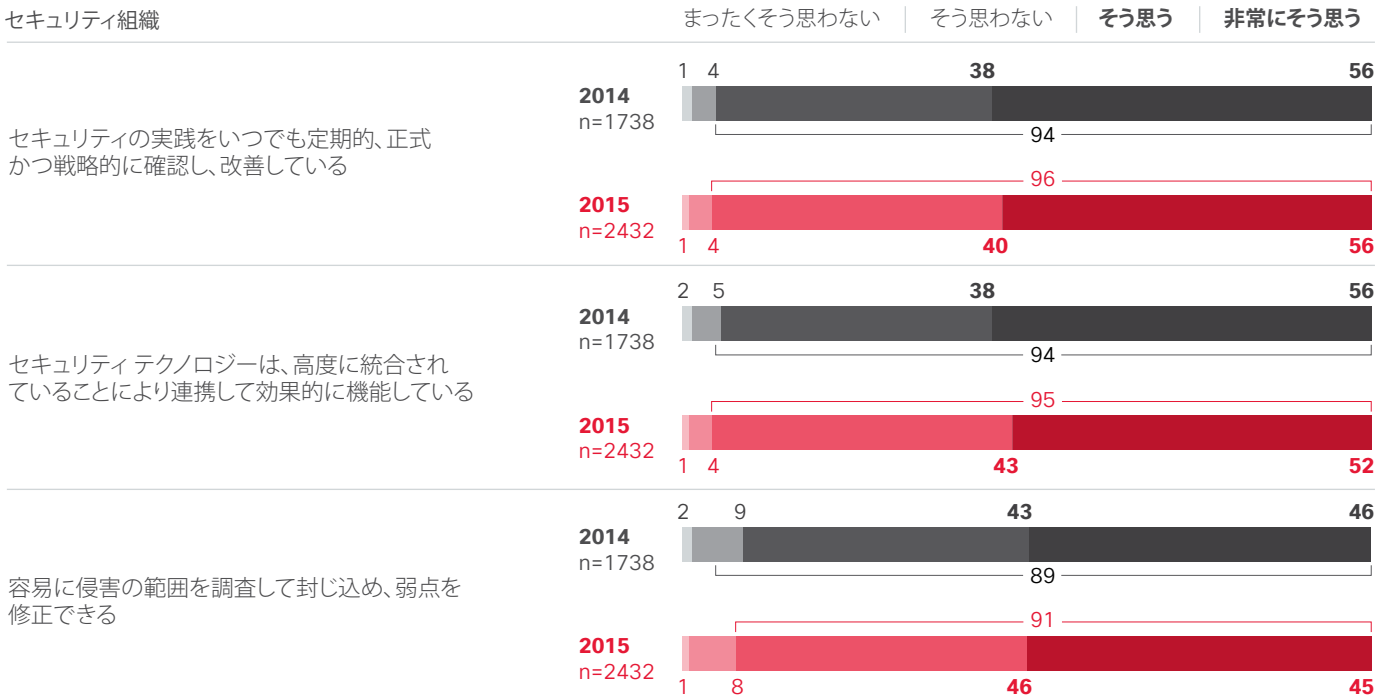
共有

セキュリティ機能の確信度があまり高くない分野もあります。たとえば、2015 年には、セキュリティ インシデントの実際の発生を確認するのに適したシステムを備えていると考えているのは回答者の 54 % に過ぎませんでした (図 51 を参照)。(完全なリストについては、77 ページを参照してください。)

また、回答者はシステムがそのような侵害の範囲を見極め、封じ込めることができると完全には信じていません。セキュリティプラクティスの見直しと改善を定期的に、正式かつ戦略的に実施していると回答したのは 56 % で、セキュリティテクノロジーがうまく統合され、連携が効果的に機能していると考えているのは 52 % でした (図 52 を参照)。(完全なリストについては、79 ページを参照してください。)

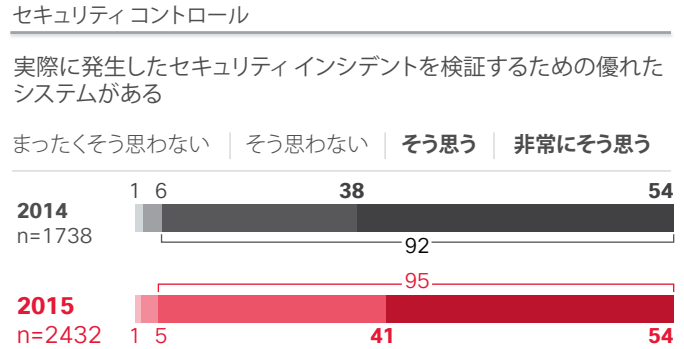
共有    

図 52. 侵害の封じ込め機能に対する企業の確信度は不安定



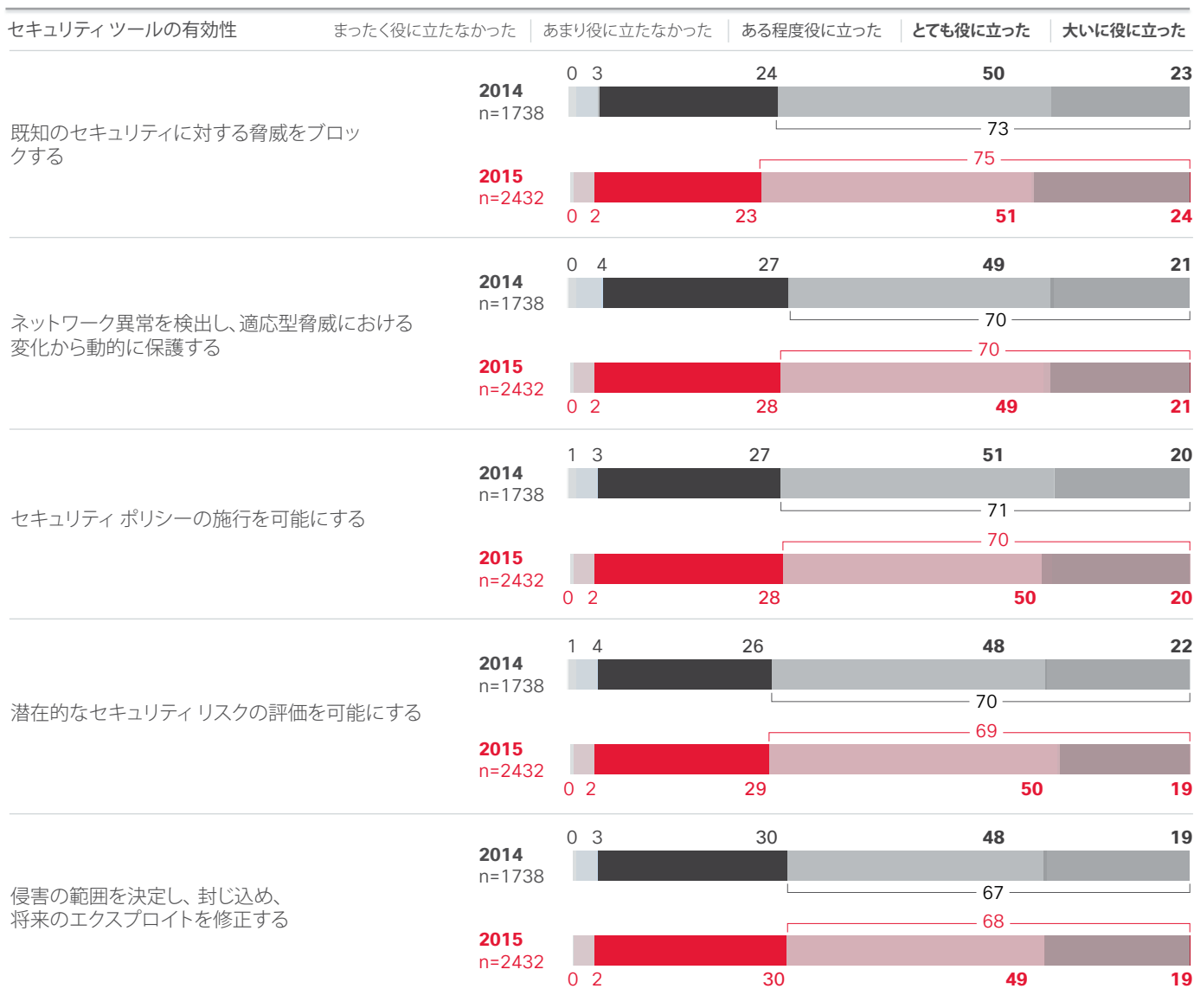
出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

図 51. 企業はセキュリティ制御が十分であると確信している



出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

図 53. 企業の 4 分の 1 はセキュリティ ツールはある程度しか有効でないと考えている



出典:2015 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

2014 年の回答者と同じく、2015 年もセキュリティ プロフェッショナルの 4 分の 1 以上が自社のセキュリティ ツールの効果が部分的であるとする認識を示しています (図 53)。

公共のセキュリティ違反は、組織にとって決定的な瞬間となる傾向があります。違反が起きると、組織は将来の違反を防ぐ必要性をより強く認識するのです。ただし、2015 年には、組織が公共のセキュリティ違反に対応しなければならないと回答したセキュリティ プロフェッショナルの数は減少しました。具体的には、2014 年には 53 % でしたが、2015 年には 48 % になりました (図 54)。

セキュリティ プロフェッショナルは、セキュリティ プロセスを強化する重要性を再認識できたという点で、違反にも価値があると認めています。公共のセキュリティ違反による影響を受けたセキュリティ プロフェッショナルの 47 % が、結果としてポリシーと手順の改善につながったと回答しています。たとえば、回答者の 43 % が、公共のセキュリティ違反後にセキュリティ トレーニングの数が増えたと述べており、42 % がセキュリティ 防御テクノロジーへの投資が拡大したと回答しています。

公共のセキュリティ違反に悩まされた組織はセキュリティ プロセスを強化する可能性が高くなります。2015 年では、セキュリティ プロフェッショナルの 97 % が、少なくとも年に 1 回はトレーニングを実施しており、2014 年の 82 % から順調に増加しています (82 ページの図 90 を参照)。

共有    

図 54. 公共のセキュリティ違反がセキュリティの向上につながる場合がある

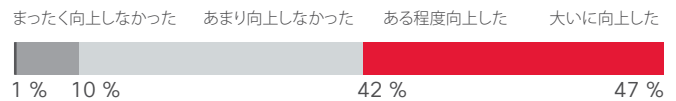
組織は、セキュリティ侵害に対する世間の詮索に対処しなければならなかったことがありますか。(n=1701) (n=1347)

2014
53 %
必要

対

2015
48 %
はい

侵害がきっかけとなり、セキュリティに対する脅威の防衛ポリシーはどの程度向上しましたか。手順または技術に関してお答えください。(n=1134)



出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

図 55. 多くの組織がセキュリティ トレーニングを実施している

2015 年に、回答者の 43 % が、公共のセキュリティ違反後にセキュリティ トレーニングの数が増えたと述べています。

43 % 

出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

成熟度: 予算的な制約がどのレベルでも上位を占める

組織がより高度なセキュリティ プラクティスとポリシーを展開するにつれ、セキュリティの準備状況に関する評価が変化すると考えられます。2015 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では、各社のセキュリティ プロセスに関する回答に基づいて、調査の回答者とその組織を 5 つの成熟度カテゴリに分類しました (図 56)。この調査では、機能、業界、国などのさまざまな特性が成熟度にどのように影響するかについて調べました。

興味深いことに、成熟度が異なる組織同士でも、より高度なセキュリティ プロセスとツールを実装する上での障害は部分的に共通しています。正確な割合は多少異なりますが、予算的な制約はどの成熟度でも課題の最上位に位置しています (図 57)。

図 56. セキュリティ プロセスに基づいて組織を格付けした成熟度モデル

研究したうえで、セキュリティ プロセスを目的とする一連の質問に基づいた 5 つのセグメントのソリューションを選択しました。5 つのセグメントのソリューションは、能力成熟度モデル統合 (CMMI) に沿ってマッピングされます。

	レベル	5 セグメント ベースのソリューション	
モバイル	1	プロセスの改善に重点を置く	● 高
定量的に管理された状態	2	プロセスを定量的に測定および管理	● やや高い
定義	3	プロセスを組織に合わせて特徴付け、多くの場合プロアクティブ	● 中
反復可能	4	プロセスをプロジェクトに合わせて特徴付け、多くの場合リアクティブ	● やや低い
当初	5	アドホックなプロセス、予測不可能	● 低

出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

図 57. 成熟度の影響を受けない、より高度なセキュリティを導入する上での障害

次のうち、高度なセキュリティ プロセスやテクノロジーを採用するに当たって最大の障害と考えられるのはどれですか。

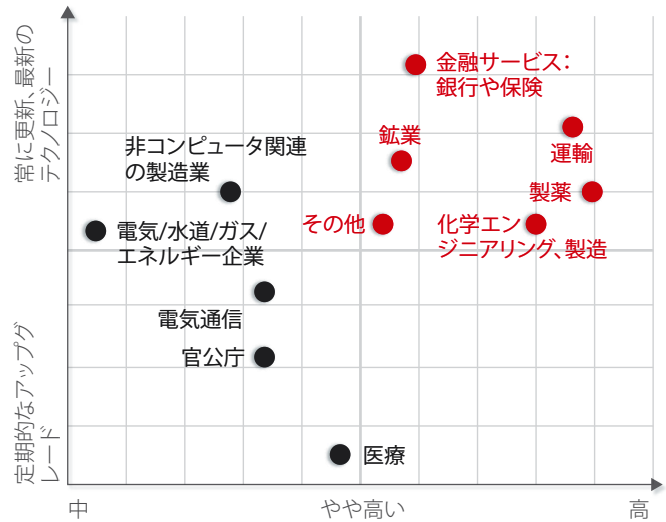
技術的洗練度	● 低	● やや低い	● 中	● やや高い	● 高
予算的な制約	43 %	48 %	39 %	38 %	38 %
経営陣の賛同	14 %	20 %	20 %	22 %	19 %
競合する優先事項	19 %	27 %	26 %	26 %	22 %
熟練スタッフの不足	21 %	27 %	22 %	19 %	23 %
高度なセキュリティ プロセスとテクノロジーに関する知識の不足	31 %	20 %	25 %	23 %	22 %
レガシー システムとの互換性の問題	21 %	28 %	29 %	34 %	33 %
認定要件	14 %	17 %	26 %	27 %	25 %
セキュリティに関する組織文化や意識	31 %	23 %	23 %	22 %	21 %
市場で有効性が実証されるまでの購入への抵抗感	12 %	25 %	24 %	25 %	19 %
新しい責任を引き受けるには現在の作業負担が重すぎる	36 %	23 %	25 %	25 %	22 %

出典: 2015 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

右の図は、さまざまな業界のセキュリティ インフラストラクチャの質と成熟度をマッピングしたものです。この図は、調査回答者のセキュリティ プロセスに関する認識に基づいています。4 分割された領域の右上に近づくほど、成熟度とインフラストラクチャの質が高いことを示しています。

下の図は、業種ごとに成熟度の配置を示したものです。2015 年には、調査を実施した運輸業や製菓業のほぼ半分が高成熟度セグメントでした。電気通信と電気/水道/ガスは、2014 年と比べて 2015 年では高成熟度セグメントの割合が減少しています。この結果は、調査回答者のセキュリティ プロセスに関する認識に基づいています。

図 58. インフラストラクチャと業種別のセキュリティの成熟度の度合い

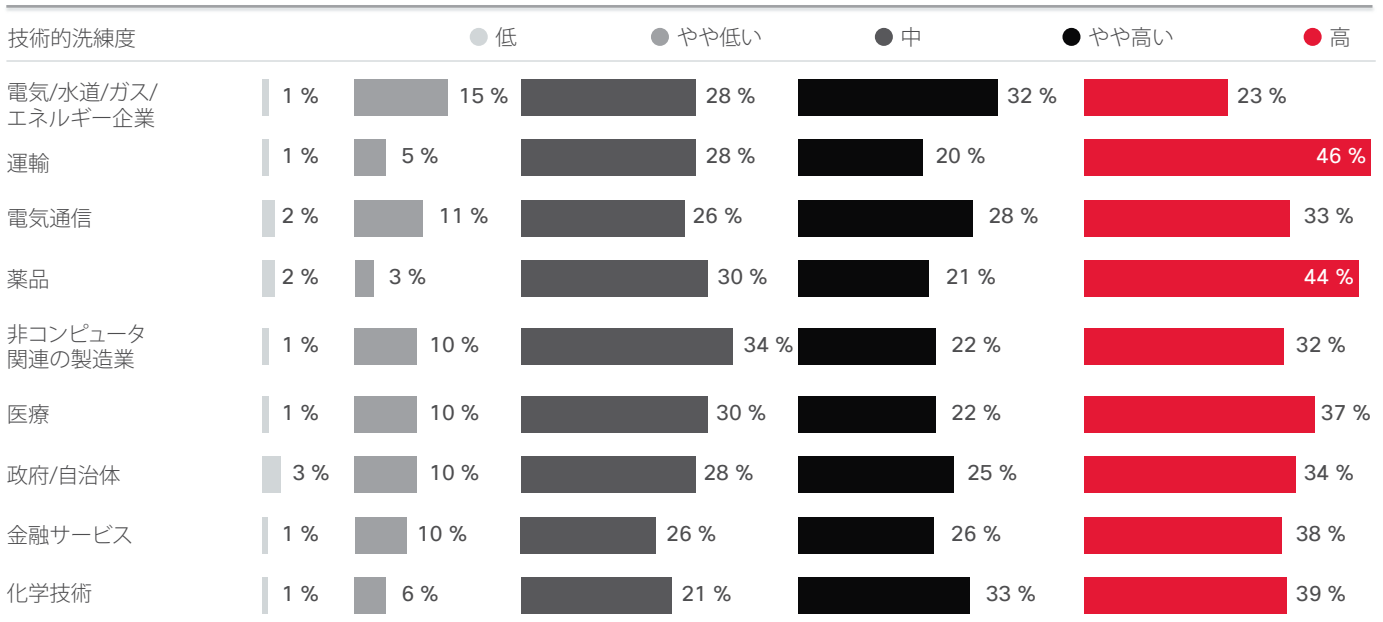


出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

共有

図 59. 業種別成熟度

業種別セグメント分布

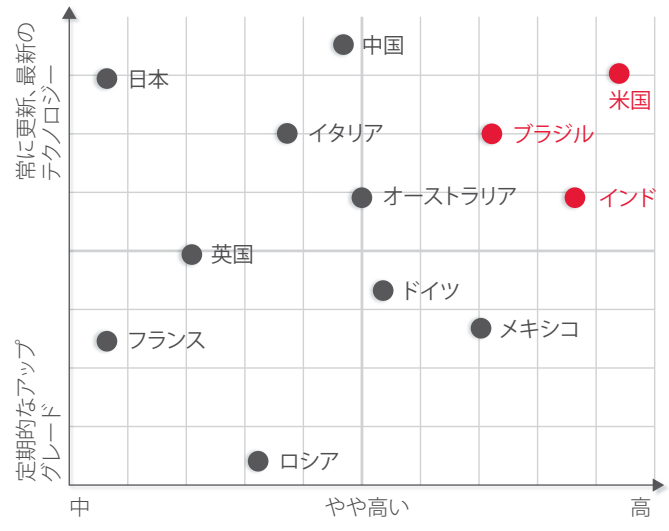


出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

右の図は、さまざまな国のセキュリティ インフラストラクチャの質と成熟度をマッピングしたものです。4 分割された領域の右上に近づくほど、成熟度とインフラストラクチャの質が高いことを示しています。これらの結果は、セキュリティ プロフェッショナルによるセキュリティの準備状況に関する認識値に基づいていることに注意してください。

下の図は、国ごとの成熟度の配置を示したものです。この結果は、調査回答者のセキュリティ プロセスに関する認識に基づいています。

図 60. インフラストラクチャと国別のセキュリティの成熟度の度合い



出典: 2015 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

共有

図 61. 国別成熟度

国別セグメント分布	2014 (n=1637)					2015 (n=2401)				
技術的洗練度	● 2014	● 低	● やや低い	● 中	● やや高い	● 低	● やや低い	● 中	● やや高い	● 高
米国	3% 2%	10% 4%	27% 22%	16% 27%	44% 45%					
ブラジル	2% 1%	5% 9%	24% 24%	35% 26%	34% 40%					
ドイツ	1% 1%	4% 12%	27% 24%	25% 24%	43% 39%					
イタリア	1% 4%	23% 3%	13% 36%	25% 23%	38% 34%					
英国	8% 0%	8% 14%	25% 32%	18% 22%	41% 32%					
オーストラリア	9% 1%	7% 5%	19% 29%	35% 36%	30% 29%					
中国	0% 0%	3% 6%	32% 37%	29% 25%	36% 32%					
インド	7% 1%	3% 4%	20% 21%	16% 34%	54% 40%					
日本	7% 2%	15% 16%	14% 34%	40% 16%	24% 32%					
メキシコ	6%	8%	20%	16%	50%					
ロシア	1%	14%	27%	26%	32%					
フランス	1%	15%	35%	20%	29%					

出典: 2015 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

推奨：現状認識に対応する

シスコによるセキュリティ機能のベンチマーク調査が示すように、セキュリティプロフェッショナルは現実を認識しています。攻撃をブロックする体制が準備できているかについて、セキュリティプロフェッショナルの確信は揺れています。しかし、目立った攻撃によって得られる現状認識は、セキュリティトレーニングや正式なポリシー作成の状況から判断すると、業界にプラスの効果をもたらします。また、監査やインシデント対応サービスの外部委託頻度の増加は、防御側がエキスパートによる支援を求めていることを示します。

企業はセキュリティ準備状況の認識を高め続け、セキュリティプロフェッショナルはテクノロジーとスタッフをサポートするため、予算配分の増加に挑まなければなりません。さらに、セキュリティプロフェッショナルは、脅威を検出できるだけでなく、その影響を封じ込め、将来の攻撃を防ぐための知識を深めるツールを導入することで、確信度を引き上げることができます。

将来の展望

将来の展望

シスコの専門家が、データ転送に関する法律の変更や暗号化の使用についての議論を含め、インターネットガバナンスの状況の変化に対する洞察を示します。また、このセクションでは、シスコによる2つの調査の結果についても説明します。1つは、サイバーセキュリティに関して幹部が懸念している問題の調査です。もう1つは、セキュリティリスクと信頼性についてのIT意思決定者の見解に焦点を当てています。さらに、統合型脅威防御アーキテクチャの価値の概要を示し、検出時間(TTD)の短縮におけるシスコの進歩について最新情報を提供します。

地政学的な展望: インターネットガバナンスの状況の不確実性

エドワード スノーデン以降、インターネットガバナンスの地政学的な状況は大きく変化しています。現在、国境を越えた情報の自由な移動について不確実性が蔓延しています。オーストリアのプライバシー活動家マックス・シュレムスがソーシャル ネットワーキングの巨大企業 Facebook に対して起こした画期的な訴訟はおそらく最も大きなインパクトを与えました。この訴訟により、2015年10月6日、欧州連合司法裁判所(CJEU)は米国のセーフハーバー協定は無効であるとの判決を下しました。⁷

その結果、企業はEUから米国にデータを転送する際に、セーフハーバー以外のメカニズムや法的保護に頼らざるを得なくなっていますが、今度はそれらが調査される可能性があります。データ企業は、それでもなお、このデータ移動が及ぼす副次的影響を評価しようとしています。また、EUと米国の当局は過去2年間、セーフハーバーの代替策を検討してきましたが、考えられる新しいメカニズムには懸念があります。CJEUの懸念に十分に対処しない場合は、2016年1月の期限までに実現されないか、または市場の信頼回復に失敗する可能性が高く、また無効になる恐れがあります。⁸

データ保護の専門家は、セーフハーバー 2.0 は以前の協定に劣らず議論的になると予想しています。法定で異議を申し立てられ、さらに無効を申告されることによって、まったく同じ道をたどる可能性があります。⁹

消費者や組織に対する利点、犯罪やテロリスト活動の捜査における警察の課題を含め、エンドツーエンドの暗号化も今後、政府機関と業界の間での議題となります。2015年11月にパリで発生したテロによって、何人かの政治家は、捜査官が暗号化された通信内容にアクセスできるようにすることを強く求めました。¹⁰これによって、Safe Harbor 2.0 の作成に拍車がかかり、市民の人権に関する問題はセキュリティ問題の後回しにされています。

⁷ 「The Court of Justice declares that the Commission's U.S. Safe Harbour Decision is invalid」、CJEU、2015年10月6日:
<http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> [英語]

⁸ 「Safe Harbor 2.0 framework begins to capsize as January deadline nears」、グリーン・ムーディ著、Ars Technica、2015年11月16日:
<http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/> [英語]

⁹ 「Safe Harbor 2.0 framework begins to capsize as January deadline nears」、グリーン・ムーディ著、Ars Technica、2015年11月16日:
<http://arstechnica.com/tech-policy/2015/11/safe-harbour-2-0-framework-begins-to-capsize-as-january-deadline-nears/> [英語]

¹⁰ 「Paris Attacks Fan Encryption Debate」、ダニー・ヤドロフ、アリスティア・バー、若林大介著、The Wall Street Journal、2015年11月19日:
<http://www.wsj.com/articles/paris-attacks-fan-encryption-debate-1447987407> [英語]

このような不確実な状況の中で、組織は自分達のビジネスがデータ転送に関する法律を遵守していることを確認するためにデータプロバイダーに何を要求するべきでしょうか？短期的には、EU外にデータを転送する際にセーフハーバーだけでなくEUの標準契約条項または拘束的企業準則を使用しているという保証をベンダーに確実に要求する必要があります。

組織が監視すべきもう1つの主要な地政学的問題は、脆弱性とエクスプロイトに関連します。一部の政府は、兵器化されたソフトウェアと呼ばれる未パッチの脆弱性の市場拡大について大きな懸念を示しています。世界でネットワークを保護する方法を探す場合、このようなツールはセキュリティ調査コミュニティに不可欠です。しかし、善良な使用を意図したこのテクノロジーが悪人、特に抑圧的な政権の手に渡ると、金融犯罪、国家秘密や企業秘密の盗用、政治的反対者の抑圧、または重要なインフラストラクチャの破壊に使用される可能性があります。

重要な調査を実行せずに未パッチの脆弱性へのアクセスをどのように制限するのかということは、政府機関が今後数ヶ月から数年で明確に取り組んで行く問題です。政府機関がこの難しい問題に取り組む場合には、政策決定がセキュリティに与える影響を慎重に評価する必要があります。たとえば、未公開の脆弱性に関する情報の伝送を管理する法律が不確実だと、ベンダーがその脆弱性にパッチ適用する機会を得る前に、セキュリティ脅威の調査の進行が鈍り、脆弱性の公開が助長される可能性があります。この不確実性を解消する方法は、全世界共通である必要があります。

幹部に重くのしかかるサイバーセキュリティ問題

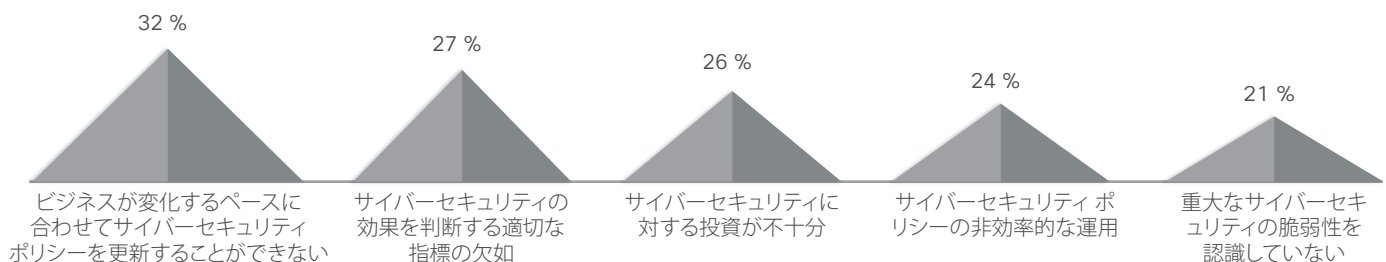
確かに、徹底したセキュリティによって企業は重大なセキュリティ侵害や攻撃を防止することができます。しかし、企業が成功するチャンスも高められるのでしょうか。2015年10月にシスコが実施した、ビジネスおよびデジタル戦略でのサイバーセキュリティの役割に関する財務および基幹業務幹部への調査によると、企業の幹部は脅威からビジネスを保護することがビジネスの成功または失敗に影響する可能性があると理解しています。組織がデジタル化されるにつれ、成長はデジタルプラットフォームを保護する能力に左右されます。

調査結果が示すように、サイバーセキュリティは幹部にとって重要な懸念事項となっており、サイバーセキュリティ侵害について48%が非常に懸念していると述べ、39%がどちらかといえば懸念していると述べています。この懸念は拡大傾向にあり、41%が3年前よりもセキュリティ侵害について非常に懸念していると述べ、42%が以前よりもやや懸念していると述べました。

ビジネスリーダーは、投資家や規制当局が、その他のビジネス機能について質問するのと同様にセキュリティプロセスについてもより厳しい質問を投げかけてくると予想しています。回答者の92%は、将来、規制当局と投資家が企業にサイバーセキュリティリスクの影響度に関するより多くの情報を提供することを期待するようになると考えています。

企業は、直面するサイバーセキュリティ問題にも鋭い感覚を持っているようです。最も多く見られる問題はサイバーセキュリティポリシーがビジネスの変化に対応できないことで、その次はセキュリティの効果を判断する基準がないことでした(図62)。

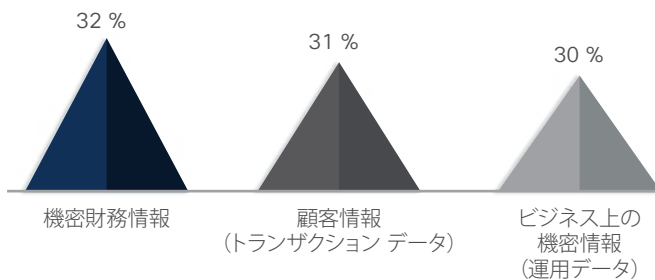
図 62. 困難なサイバーセキュリティ問題に直面する企業



出典:シスコセキュリティリサーチ

約 3 分の 1 の幹部は、重要なデータの保護についても不安を持っています。最も保護することが難しい情報のタイプについて尋ねると、32 % が「機密財務情報」を選択しました。回答者は、次に保護が難しいデータのタイプに「顧客情報」と「機密業務情報」の 2 つを挙げました(図 63 を参照)。

図 63. 重要なデータの保護について懸念する幹部



出典:シスコ セキュリティリサーチ

信頼性の調査:企業のリスクと課題に注目

情報セキュリティ侵害の絶え間ない増加は、企業が自社のシステム、データ、ビジネス パートナー、顧客、および従業員が安全だと信頼できることの必要性を示しています。シスコは、信頼が、IT およびネットワーク インフラストラクチャを選択する際にビジネスが考慮する主要な要素になると考えています。実際に、多くのビジネスでは、現在、インフラストラクチャを構成するソリューションの製品ライフサイクル全体でセキュリティと信頼性を統合することが必要となっています。

2015 年 10 月に、シスコは、セキュリティのリスクと課題についての IT 意思決定者の見解を評価して IT ベンダーの信頼性が IT 投資で果たす役割を確認するために調査を行いました。さまざまな国の組織の情報セキュリティ意思決定者と非情報セキュリティ意思決定者の両方を調査しました(シスコの方法論を含め、セキュリティ リスクと信頼性の調査の詳細は、[付録](#)を参照してください)。

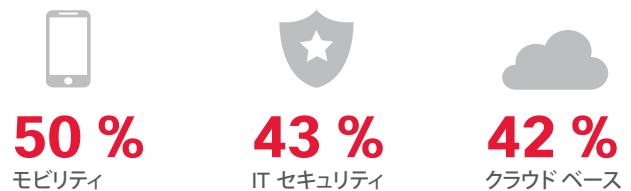
次に調査結果を示します。

回答者の 65 % が、自身の組織は深刻なレベルのセキュリティリスクに直面していると考えていることがわかりました。そのリスクは、モバイルの使用、IT セキュリティ、企業内のクラウドベースソリューションに起因するものです(図 64)。

図 64. セキュリティ リスクの認識



企業は自社インフラストラクチャの次の領域がセキュリティ侵害のリスクが高いと認識しています。



出典:セキュリティ リスクと信頼性調査、シスコ

共有

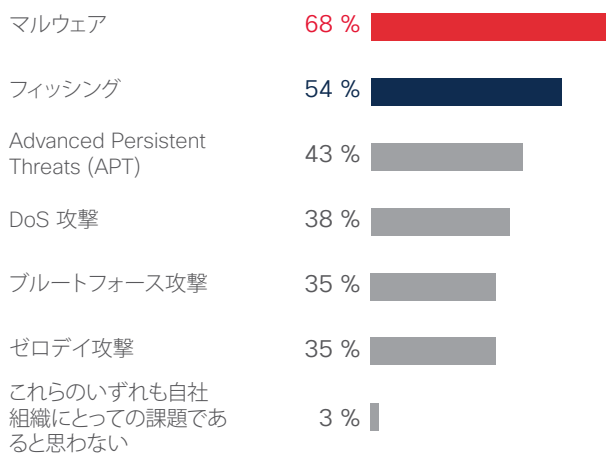
この調査の回答者の 68 % は、組織が直面する外部からのセキュリティ問題のトップにマルウェアを指定しました。上位 3 つの回答はこの他にフィッシング(54 %)、Advanced Persistent Threat (43 %) です(図 65 を参照)。

社内セキュリティ問題(図 66 を参照)については、回答者の半分以上(54 %)が不正なソフトウェア ダウンロードをトップの脅威に挙げ、その次に従業員による社内セキュリティ侵害(47 %)、ハードウェアおよびソフトウェアの脆弱性(46 %)が続きました。

また、ほとんどの企業(92 %)が組織内に専用セキュリティ チームを雇用していることがわかりました。回答者の 88 % は、定期的に更新される組織全体の公式なセキュリティ戦略があると報告しています。ただし、IT ベンダーの信頼性を検証するための標準化されたポリシーおよび手順を持つ組織は 59 % のみでした(図 67 参照)。

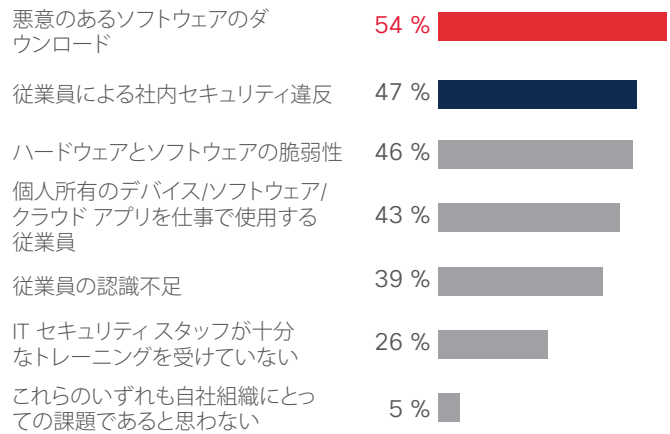
さらに、大企業の約半分(49 %)が最新テクノロジーでセキュリティ インフラストラクチャを最新状態に保ち、その他のほとんどがインフラストラクチャを定期的にアップグレードしています。調査によると、使用しているテクノロジーが時代遅れになるまでアップグレードを待つ組織はごくわずかでした。

図 65. 直面している外部の問題(全回答者)



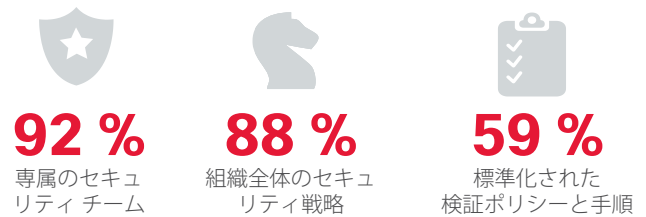
出典:セキュリティリスクと信頼性調査、シスコ

図 66. 直面している社内セキュリティ問題(全回答者)



出典:セキュリティリスクと信頼性調査、シスコ

図 67. 大企業の大半は専用のセキュリティチームを設置



出典:セキュリティリスクと信頼性調査、シスコ



ベンダーはどのように信頼性を示すことができるか

今日の脅威中心の現状では、ベンダーのプロセス、ポリシー、テクノロジー、および従業員に対する信頼、ならびにそれらを検証する能力に対する信頼が、ベンダーと企業の間で長く続く信頼関係を構築するための基本となります。

テクノロジー ベンダーは、次の方法で信頼性を示します。

- 最初からソリューションおよびバリューチェーンにセキュリティを組み込む
- リスクを軽減するポリシーとプロセスを適所に配置して遵守する
- セキュリティ意識の高い文化を作る
- 迅速かつ透徹的に侵害に対応する
- インシデント後に迅速な修復を提供し、絶え間なく警戒する

もちろん、インフラストラクチャをアップグレードすることをお勧めします。あらゆる規模の組織が、ネットワークのすべての側面にセキュリティが設計された安全で信頼性の高いインフラストラクチャの導入を必要としています。ただし、オープンでセキュリティ意識の高い文化を育むことによって攻撃を縮小することもできます。

この文化を構築するには、組織が、企業全体に及ぶ一貫したポリシーを適用し、セキュリティがビジネスのあらゆる側面に確実に組み込まれたプロセスを実施する必要があります。そして、このセキュリティ中心の考え方をパートナーやサプライヤーのエコシステムに拡大するよう尽力し、顧客、パートナー、その他の関係者と協力して透明性と責任を継続的に示していく必要があります。

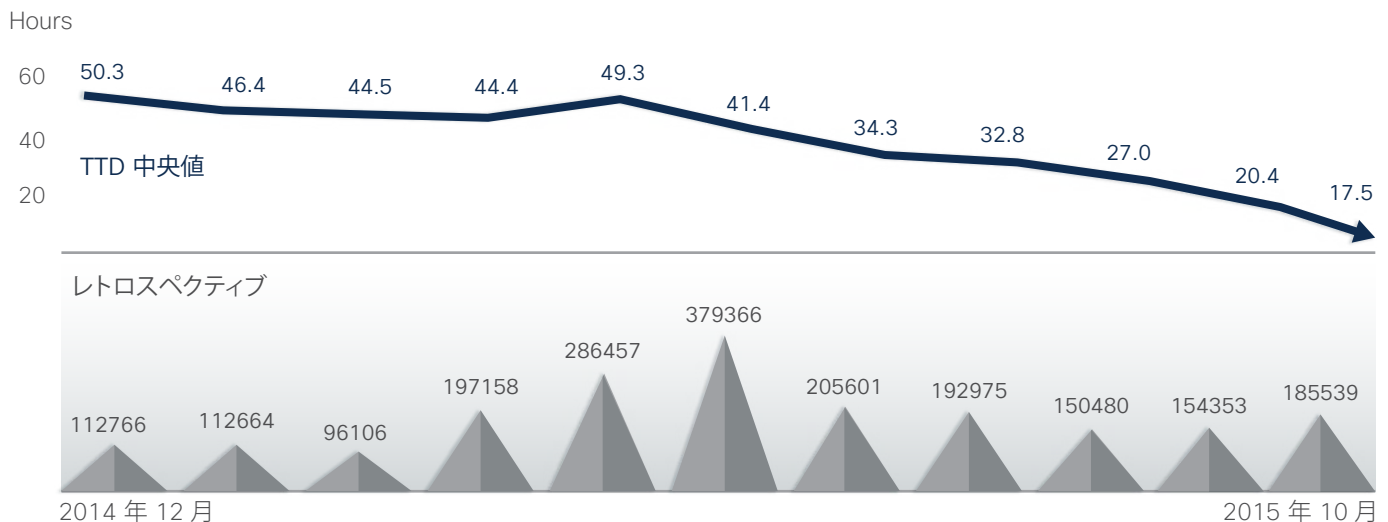
検出時間: 時間枠を縮小し続けるための競争

シスコは、「検出時間」(TTD)を不明なファイルが最初に観察されてから脅威が検出されるまでの時間と定義しています。この時間は、世界中に導入されているシスコセキュリティ製品から収集したオプトインセキュリティテレメトリを使用して決定されています。

図 68 の「レトロスペクティブ」カテゴリは、当初「不明」と分類され、後で「既知の悪意」に変わったファイルの数を示しています。

「シスコ中間セキュリティレポート(2015年)」で報告されているように、TTD中央値は約2日(50時間)でした。

図 68. 検出時間、2014年12月～2015年10月



出典:シスコセキュリティリサーチ

統合型脅威防御の 6 カ条

シスコ中間セキュリティ レポート (2015 年) で、シスコのセキュリティ専門家は、適応性のある統合型ソリューションの必要性により、今後 5 年以内にセキュリティ業界が大幅に変化すると提言しています。その結果、業界の統合が進み、拡張性の高い統合型脅威防御アーキテクチャへの動きが一元化されます。このようなアーキテクチャは、多くのソリューションに可視性、制御、インテリジェンス、およびコンテキストを提供します。

この「検出と対応」のフレームワークによって、既知の脅威と新しい脅威の両方に対して迅速に対応できるようになります。この新しいアーキテクチャの核は、完全な状況認識を実現する可視性プラットフォームで、脅威を評価したり、ローカル インテリジェンスとグローバル インテリジェンスを相互に関係付けたり、防御を最適化するために継続的に更新されます。このプラットフォームの目的は、すべてのベンダーの製品をその上で運用し、貢献させるための基盤を構築することです。可視性によって、より多くの脅威ベクトルに対して優れた保護を提供し、より多くの攻撃を阻止できます。

次に、統合型脅威防御の 6 カ条を示します。これによって、組織とそのセキュリティ ベンダーはこのアーキテクチャの目的と潜在的な利点を詳しく理解することができます。

1. 脅威の増加と高度化に対応するには、豊富なネットワークおよびセキュリティアーキテクチャが必要です。

過去 25 年間、従来のセキュリティ モデルでは「問題が見つかったから製品を購入」していました。ただし、これらのソリューションは、多数の異なるセキュリティ ベンダーのテクノロジーを集めていることが多く、有意義な方法で相互に通信しません。これらのソリューションは、セキュリティ イベントに関する情報とインテリジェンスを生成し、これがイベントプラットフォームに統合され、セキュリティ担当者によって分析されます。

統合型脅威防御アーキテクチャは検出および応答のフレームワークで、豊富な機能を提供し、自動の効率的な方法で導入済みのインフラストラクチャからより多くの情報を収集することで脅威に対する迅速な対応をサポートします。このフレームワークは、セキュリティ環境をよりインテリジェントに観察します。疑わしいイベントやポリシー違反をセキュリティ チームに警告するだけでなく、ネットワークとそこで発生していることを明確に描写し、セキュリティに関してより良い決定を示すことができますようにします。

2. クラス最高レベルのテクノロジーのみでは、現在または将来の脅威の状況に対処できません。これは、ネットワーク環境を複雑にするだけです。

組織は「クラス最高レベル」のセキュリティ テクノロジーに投資しますが、これらのソリューションが実際に機能するかどうかを判断する方法はあるのでしょうか。ここ数年の大きなセキュリティ侵害に関するニュースは、多くのセキュリティテクノロジーが適切に機能していない証拠です。失敗するときは、ひどく失敗します。

クラス最高レベルのソリューションを提供するセキュリティベンダーが急増しても、これらのベンダーが競合とわずかに違うものではなく根本的に異なるソリューションを提供しなければ、セキュリティ環境は向上しません。しかし、今日、セキュリティの中核を担う主要ベンダーの製品の多くに大きな違いはありません。

3. 暗号化されたトラフィックが増加すると、特定ポイントの製品を無効にする暗号化された悪質な行為に集中できる統合型脅威防御が必要になります。

このレポートで説明しているように、暗号化された Web トラフィックが増加しています。暗号化の使用にはもちろん十分な理由がありますが、暗号によってセキュリティ チームが脅威を追跡できにくくなる場合もあります。

暗号化「問題」への回答は、デバイスまたはネットワークで起こっていることへの可視性を向上することです。統合型セキュリティ プラットフォームは、これを実現できます。

4. オープン API は、統合型脅威防御アーキテクチャに不可欠です。

マルチベンダー環境には、優れた可視性、コンテキスト、および制御を提供する共通プラットフォームが必要です。フロントエンド統合プラットフォームを構築すると、自動化がサポートされ、セキュリティ製品自体にさらに意識を向けることができるようになります。

5. 統合型脅威防御アーキテクチャは、調整やソフトウェアのインストールおよび管理の手間を削減します。

セキュリティ ベンダーは、できるだけ機能豊富なプラットフォームを提供して、1 つのプラットフォームに拡張機能を提供していくようにする必要があります。これにより、攻撃者に簡単にアクセスするチャンスや隠れ場所を与えることになるセキュリティ環境の複雑さや断片化を低減することができます。

6. 統合型脅威防御の自動化と連携により、検出、封じ込め、修復の時間を短縮できます。

誤検出が減少することで、セキュリティ チームは最も重要な問題に集中できます。コンテキスト情報によって、進行中のイベントの最前線の分析がサポートされ、これらのイベントに即時の注意が必要かどうかをチームが評価できるようになり、最終的には自動応答とより詳細な分析を行うことができます。

数の力：業界が協力することの価値

業界の協力は、より迅速な脅威への対応を可能にする将来の統合型脅威防御アーキテクチャの開発だけでなく、ますます革新的で大胆かつ執拗になる脅威者の世界的なコミュニティに遅れをとらないようにするためにも重要です。攻撃者は、検出されにくく非常に収益性の高い活動をさらに巧みに展開するようになっています。彼らの多くは、現在、インフラストラクチャ内の合法的な資産を使用してその活動をサポートし、大きな成功を収めています。

この状況を考えると、シスコによるセキュリティ機能のベンチマーク調査(2015年)の調査対象であった防御者が組織のセキュリティを保護する能力に自信を失っても不思議ではありません。シスコは、予防的かつ継続的な業界の協力がサイバー犯罪者の活動の暴露、攻撃者が収益を上げる力の弱体化、将来の攻撃を開始するチャンスの削減に大きな影響を与え、それを防御側が実施していくことを提案します。

このレポートの最初に詳しく説明したように(10ページから始まる「特集記事」を参照)、シスコ パートナーの貢献者の間や Cisco Collective Security Intelligence (CSI) エコシステム内での協力、およびサービス プロバイダーとの協力によって、シスコは Angler エクスプロイト キットが関与する世界的な活動を発見、検証、および阻止したり、シスコの研究者がこれまで観察してきた最大の DDoS ボットネットの 1 つ、SSHPsychos を弱体化させたりすることができました。

シスコについて

シスコについて

シスコは、実世界にインテリジェントなサイバーセキュリティを提供し、広い範囲に及ぶ攻撃ベクトルに対して、業界内で最も包括的で高度な脅威保護ソリューションのポートフォリオを提供しています。シスコによる脅威中心型の運用化されたセキュリティアプローチを採用すると、複雑さが緩和され、分断化が抑えられます。同時に、優れた可視性、一貫した管理、そして攻撃前、攻撃中、攻撃後の高度な脅威保護が提供されます。

Collective Security Intelligence (CSI) エコシステムの研究者は、デバイスとセンサーの膨大なフットプリント、パブリック フィードおよびプライベート フィード、シスコのオープン ソース コミュニティから取得したテレメトリを使って、1 つの傘の下に業界トップの脅威インテリジェンスを集結させています。これにより、何十億もの Web リクエストと何百万もの電子メール、マルウェアのサンプル、およびネットワーク侵入という量が毎日取り込まれています。

当社の高度なインフラストラクチャとシステムでこのテレメトリを処理することで、機械学習システムと研究者は、ネットワーク、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、電子メールの境界を越える脅威、さらにはクラウドからの脅威を追跡して、根本原因と発生範囲を特定することができます。その結果得られたインテリジェンスは、当社の製品とサービス提供に対するリアルタイムの保護に変換され、全世界のシスコのお客様に即時に提供されます。

シスコの、脅威中心型のセキュリティアプローチについては、www.cisco.com/go/security [英語] を参照してください。

シスコ年次セキュリティ レポート (2016 年) の貢献者

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、シスコのお客様、製品、およびサービスに優れた保護を提供するために尽力するセキュリティ専門家のエリート グループです。Talos は、最先端の脅威研究者で構成され、既知の脅威と新たな脅威を検出、分析、防御するシスコ製品向けに脅威インテリジェンスを構築するための高度なシステムでサポートされています。Talos は、Snort.org、ClamAV、SenderBase.org、SpamCop の公式ルール セットを維持し、シスコ CSI エコシステムに脅威情報を提供する主要なチームです。

アドバンスド サービス クラウドおよび IT、最適化チーム

このチームは、世界の最大規模のサービス プロバイダーや企業向けに、推奨事項を提供し、ネットワーク、データセンター、およびクラウド ソリューションを最適化します。クライアントの重要なソリューションの可用性、パフォーマンス、およびセキュリティを最大化することに重点を置いたコンサルティング サービスを提供します。Fortune 500 企業の 75 % 以上に最適化サービスを提供しています。

ACTIVE THREAT ANALYTICS チーム

Cisco Active Threat Analytics (ATA) チームは、高度なビッグデータテクノロジーを活用して、既知の侵入、ゼロデイ攻撃、高度な永続的脅威からの組織の保護を支援しています。この完全なマネージド サービスは、シスコのセキュリティ専門家と、シスコのセキュリティオペレーションセンターのグローバルネットワークによって提供されます。常時警戒とオンデマンド分析を 24 時間 365 日提供します。

CISCO THOUGHT LEADERSHIP ORGANIZATION

Cisco Thought Leadership Organization は、組織、業界、およびエクスペリエンスを変革する世界的なチャンス、市場の移行、および主要なソリューションに光を当てます。この組織は、急激に変化する世界で企業が期待できること、競争に打ち勝つ方法について、鋭く、予言的な見解を示します。ほとんどのチームのソートリーダーシップは、シームレスかつ安全に物理環境と仮想環境の橋渡しをすることで組織がデジタル化し、迅速に革新を進め、希望するビジネス成果を実現できるようにすることに焦点を当てています。

COGNITIVE THREAT ANALYTICS

シスコのコグニティブ脅威分析は、ネットワークトラフィックデータの統計的分析を使用して、漏洩、保護されたネットワーク内のマルウェアの動作、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情報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。高度な統計モデリングと機械学習を活用して、新たな脅威を独自の的に特定し、検出内容から学習して、長期的に適応します。

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組織とかかわり、テクノロジー部門をサポートする公的なポリシーや規則の作成を支援したり、政府機関がその目標を達成できるよう支援します。グローバル ガバメント アフェアズ チームは、テクノロジー推進の公的ポリシーおよび規則を作成したり、これに影響を及ぼします。業界関係者や関連パートナーと協力することで、このチームは、世界、国内、および地域レベルでのポリシー決定の支援に目を向け、シスコのビジネスを左右するポリシーや全体的な ICT の採択に影響力を持つために政府機関のリーダーとの関係を構築します。グローバル ガバメント アフェアズ チームは、シスコが世界中でテクノロジーの使用を促進および保護することができるよう支援する、当選経験のある当局者、議院法学者、取締役、米政府高官、および政府業務の専門家によって構成されています。

INTELLISHIELD チーム

IntelliShield チームは、脆弱性と脅威の研究、分析、統合、およびシスコ セキュリティ リサーチ アンド オペレーションズ全体と外部ソースからのデータと情報の関連付けを行い、シスコの複数の製品とサービスを支える IntelliShield セキュリティ インテリジェンス サービスを生み出しています。

LANCOPE

シスコの傘下にある Lancop は、今日の脅威から企業を保護するためのネットワークの可視性とセキュリティ インテリジェンスを提供する主要なプロバイダーです。NetFlow、IPFIX、その他のタイプのネットワーク テレメトリを分析することによって、Lancop の StealthWatch® システムはコンテキスト認識型のセキュリティ分析を実現し、APT や DDoS からゼロデイ マルウェアや内部関係者による脅威に至る幅広い範囲の攻撃をすばやく検出します。企業ネットワーク間での継続的な横方向の監視と、ユーザ、デバイス、およびアプリケーションの識別を組み合わせることで、Lancop はインシデント対応のスピードアップ、フォレンジック調査の向上、および企業リスクの削減を実現します。

OPENDNS

シスコの OpenDNS は、世界最大のクラウド型セキュリティ プラットフォームで、160 カ国以上にわたる 6,500 万人以上のデイリー ユーザに提供されています。OpenDNS ラボは、セキュリティ プラットフォームをサポートする OpenDNS のセキュリティ リサーチ チームです。詳細は、www.opendns.com [英語] または <https://labs.opendns.com> [英語] を参照してください。

SECURITY AND TRUST ORGANIZATION

シスコの Security and Trust Organization は、役員室のメンバーや世界のリーダーの考える最も重要な 2 つの問題に対処するためのシスコの取り組みを明確に示します。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の保護、シスコの製品とサービス ポートフォリオにおける Cisco Secure Development Lifecycle と Trustworthy System の実現、および絶えず進化するサイバー脅威からのシスコの保護、が含まれています。シスコは、人員、ポリシー、プロセス、およびテクノロジーを含む全体的なアプローチでセキュリティと信頼を広めます。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。詳細は、<http://trust.cisco.com> [英語] を参照してください。

SECURITY RESEARCH AND OPERATIONS (SR&O)

Security Research & Operations (SR&O) は、業界トップクラスの Product Security Incident Response Team (PSIRT) を含め、シスコの全製品およびサービスに対する脅威および脆弱性の管理に責任を負います。SR&O は、Cisco Live や Black Hat などのイベントやシスコおよび業界の仲間との協力などで、進化する脅威の状況を理解できるように顧客を支援します。さらに、SR&O はシスコの Custom Threat Intelligence (CTI) などの新しいサービスを提供します。このサービスでは、既存のセキュリティ インフラストラクチャでは検出または軽減されなかった侵害の指標を識別できます。

シスコ パートナーの貢献者

LEVEL 3 の脅威研究ラボ

Level 3 Communications は、コロラド州ブルームフィールドに拠点を置くトップクラスの世界的通信プロバイダーで、企業、政府機関、およびキャリア顧客に通信サービスを提供しています。大規模なファイバ ネットワークで 3 つの大陸に配備され、海底設備によって接続されたシスコのグローバル サービス プラットフォームは、60 カ国以上の 500 を超える市場に及ぶ主要都市圏地下深くの資産が特長です。Level 3 のネットワークによって、世界中の脅威の状況を包括的に捉えることができます。

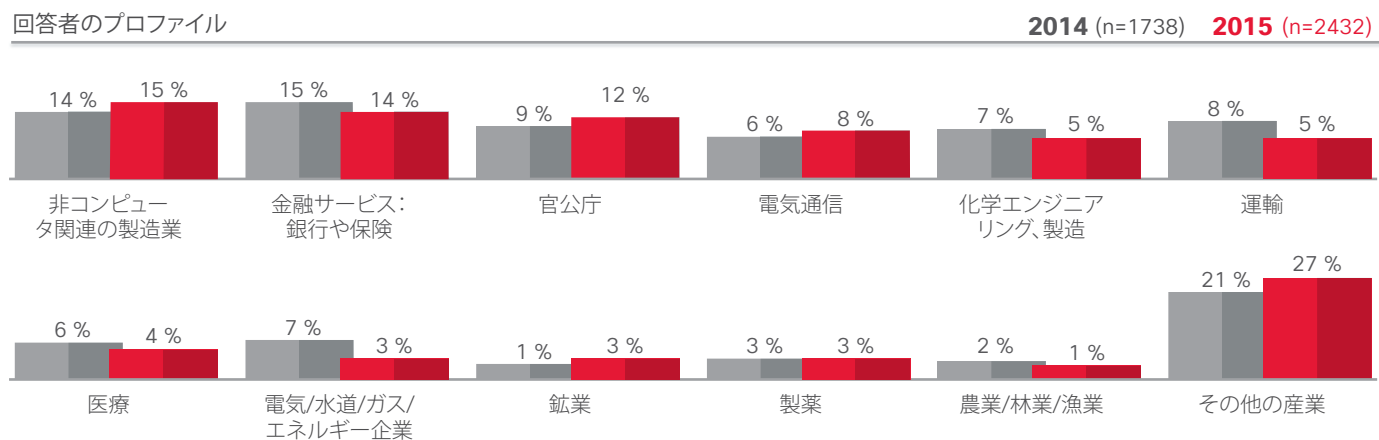
Level 3 の脅威研究ラボは、世界中の脅威の状況を予防的に分析し、Level 3 の顧客、ネットワーク、およびパブリック インターネットを保護できるように組織内外で情報を相互に関連付けるセキュリティ グループです。このグループは、脅威を研究したり軽減したりするために、Cisco Talos などの業界のリーダーと定期的に提携しています。

付録

付録

シスコによるセキュリティ機能のベンチマーク調査(2015年): 回答者のプロフィールおよびリソース

図 71. 回答者のプロフィール



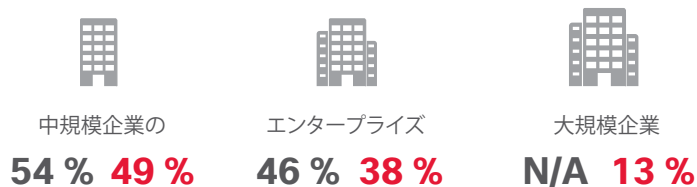
CSO と SecOps

● CSOs ● SecOps



組織の規模

2014 2015



セキュリティが関与する領域

2014

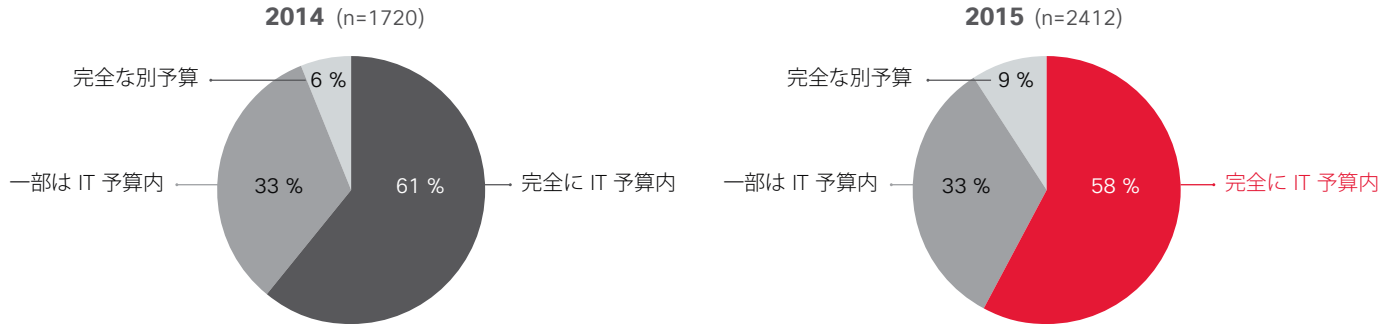
2015



出典: 2015年のシスコによるセキュリティ機能のベンチマーク調査

図 72. IT 予算とは別にセキュリティ予算がある回答者は 9 % しかいないが、2014 年以降大幅に増加している

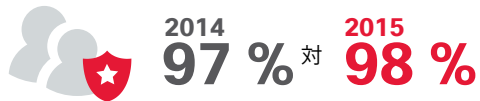
セキュリティの予算は IT 予算の一部ですか。(IT 部門のメンバー)



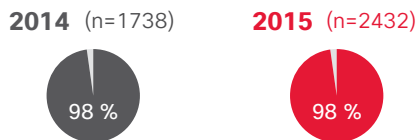
出典: IT 年のシスコによるセキュリティ機能のベンチマーク調査

図 73. 役職: 回答者およびそのマネージャ

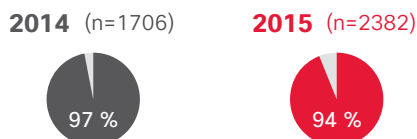
IT 部門のメンバー



セキュリティ専属の部門またはチーム



セキュリティ チームのメンバー



役職








































マネージャの役職

最高セキュリティ責任者	22%	最高経営責任者	34%
最高技術責任者	18%	社長/オーナー	18%
IT 部門のディレクタまたはマネージャ	16%	最高セキュリティ責任者	16%
最高情報責任者	13%	最高情報責任者	6%
セキュリティ オペレーション部門のディレクタ	7%	最高技術責任者	6%
IT セキュリティ部門の VP	5%	IT 部門のディレクタまたはマネージャ	4%
リスクおよびコンプライアンス責任者	4%	IT セキュリティ部門の VP	4%
セキュリティ オペレーションのマネージャ	4%	IT 担当副社長	2%
セキュリティ アーキテクト	4%	経営陣	2%
IT 担当副社長	3%	最高執行責任者	1%
最高執行責任者	3%	最高財務責任者	1%
別の役職	2%	別の役職	0%

出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

図 74. ファイアウォールが最も一般的に使用されているセキュリティ脅威防御ツールで、2015 年にクラウドベース サービスで管理されているセキュリティ脅威防御は 2014 年に比べて少なくなっている

クラウドベースのサービスを通じて管理している防御の内容 (セキュリティの脅威に対する防御を使用していると回答したセキュリティ担当者)

組織が利用するセキュリティ脅威防御	2014 (n=1738)	2015 (n=2432)	2014 (n=1646)	2015 (n=2268)
ファイアウォール *	N/A	 65 %		31 %
データ損失の防止 (DLP)	 55 %	 56 %		
認証	 52 %	 53 %		
暗号化/プライバシー/データ保護	 53 %	 53 %		
電子メール/メッセージング セキュリティ	 56 %	 52 %	37 %	34 %
Web セキュリティ	 59 %	 51 %	37 %	31 %
エンドポイント保護/マルウェア対策	 49 %	 49 %	25 %	25 %
アクセス コントロール/許可	 53 %	 48 %		
ID の管理/ユーザ プロビジョニング	 45 %	 45 %		
侵入防御 *	N/A	 44 %		20 %
モビリティ セキュリティ	 51 %	 44 %	28 %	24 %
安全なワイヤレス	 50 %	 41 %	26 %	19 %
脆弱性スキャン	 48 %	 41 %	25 %	21 %
VPN	 48 %	 40 %	26 %	21 %
セキュリティ情報およびイベント管理	 43 %	 38 %		
DDoS 防御	 36 %	 37 %		
ペネトレーション テスト	 38 %	 34 %	20 %	17 %
パッチの適用および構成	 39 %	 32 %		
ネットワーク調査	 42 %	 31 %		
エンドポイント調査	 31 %	 26 %		
ネットワーク、セキュリティ、ファイアウォール、侵入防止 *	 60 %	N/A	35 %	
上記のどれにも当てはまらない	1 %	1 %	13 %	11 %

* ファイアウォールと侵入防御は、2014 年では 1 つのコードでした。

* ネットワーク セキュリティ、ファイアウォール、侵入防止 *

出典: 2015 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

アウトソーシング

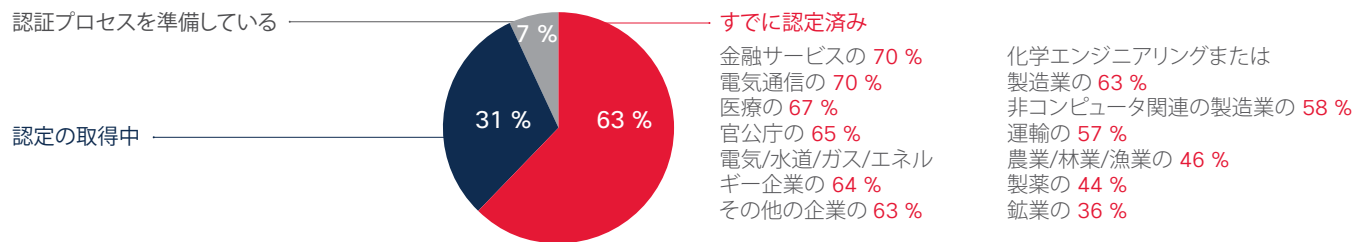
図 75. アウトソーシングされるセキュリティ サービスのトップはアドバイスとコンサルティングである

監査とインシデント対応の外部委託の大幅な増加。アウトソーシングは、よりコスト効率が高いと見なされている。

昨年と同様、半数(52%)は ISO 27001 などの標準化されたセキュリティ ポリシーの実践に準じている。これらの多くはすでに認定されているか、認定の取得中である。

標準化されたセキュリティ ポリシーの実践

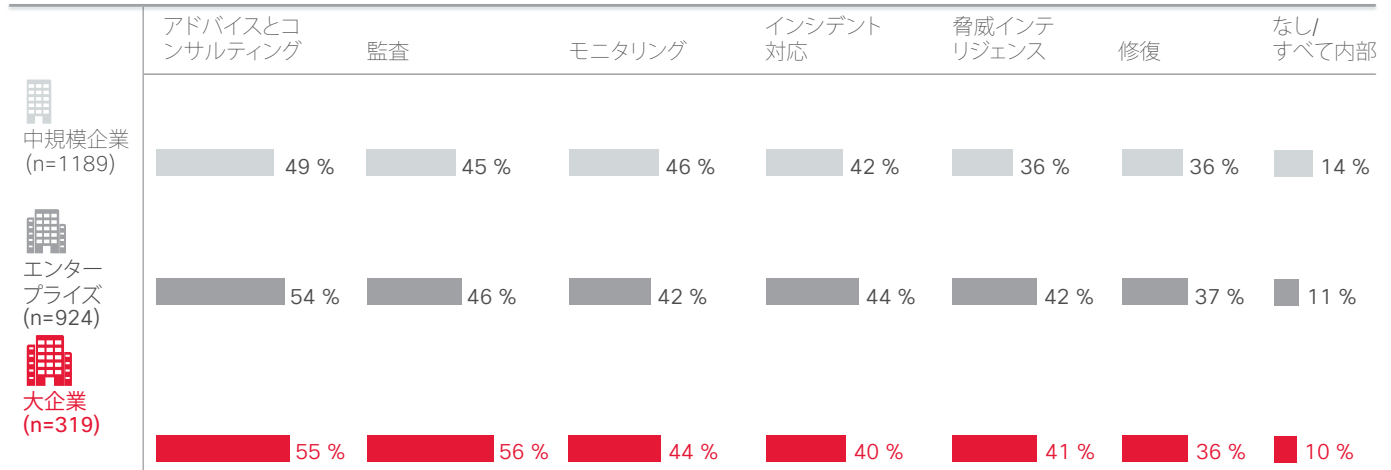
標準化された情報セキュリティ ポリシーの実践に準拠している組織 (2015: n=1265)



出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

図 76. アウトソーシングに対する企業の見解: 大企業は監査、アドバイス、およびコンサルティングをアウトソーシングする可能性が非常に高い

外部に委託しているセキュリティ サービス



出典: 2015 年のシスコによるセキュリティ機能のベンチマーク調査

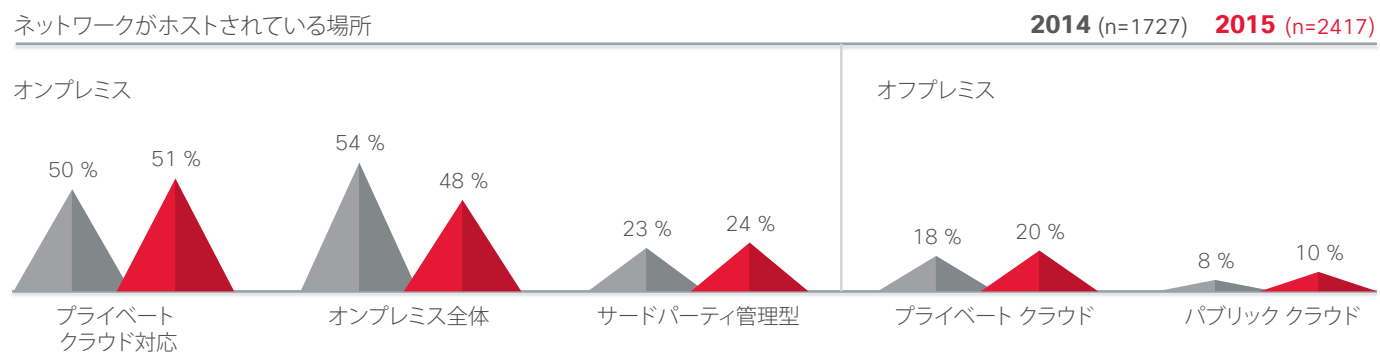
図 77. アウトソーシングに対する企業の見解:日本ではアドバイスとコンサルティングをアウトソーシングする可能性が非常に高い

外部に委託しているセキュリティ サービス

合計	米国	ブラジル	ドイツ	イタリア	英国	オーストラリア	中国	インド	日本	メキシコ	ロシア	フランス
アドバイスとコンサルティング 52 %	52 %	51 %	49 %	51 %	44 %	54 %	52 %	54 %	64 %	58 %	41 %	55 %
監査 47 %	50 %	55 %	38 %	48 %	50 %	36 %	33 %	51 %	41 %	63 %	40 %	59 %
監視 44 %	48 %	49 %	32 %	39 %	41 %	52 %	31 %	51 %	51 %	49 %	37 %	50 %
インシデント対応 42 %	46 %	39 %	32 %	38 %	43 %	53 %	34 %	49 %	53 %	45 %	27 %	54 %
脅威インテリジェンス 39 %	42 %	40 %	37 %	46 %	36 %	16 %	36 %	48 %	47 %	44 %	42 %	39 %
修復 36 %	34 %	32 %	38 %	34 %	31 %	47 %	37 %	41 %	40 %	21 %	41 %	41 %
なし/すべて内部 12 %	18 %	9 %	18 %	13 %	19 %	4 %	19 %	12 %	10 %	3 %	16 %	4 %

出典:2015 年のシスコによるセキュリティ機能のベンチマーク調査

図 78. ネットワークのオンプレミス ホスティングは一般的だが、オフプレミス ホスティングは昨年から増加している



出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

セキュリティ侵害の公表

図 79. 2015 年のレポートでは、セキュリティ侵害に対する世間の詮索に対処しなかった組織は 2014 年に比べて少なくなっている

セキュリティ違反は、セキュリティ強化を推進する大きな要素

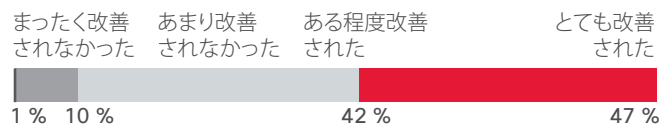
2014 年と比較して、2015 年のレポートではセキュリティ違反に関する世間の詮索に対応しなければならない組織の数は減少しています。



出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 80. セキュリティ侵害の公表によりセキュリティが向上することがある

セキュリティに対する脅威への御社の防御ポリシー、手順、テクノロジーは、こうした違反によってどの程度改善されたでしょうか。(n=1134)



CSOは、SecOpsマネージャと比べて、多くがセキュリティ違反後の改善について言及しています。

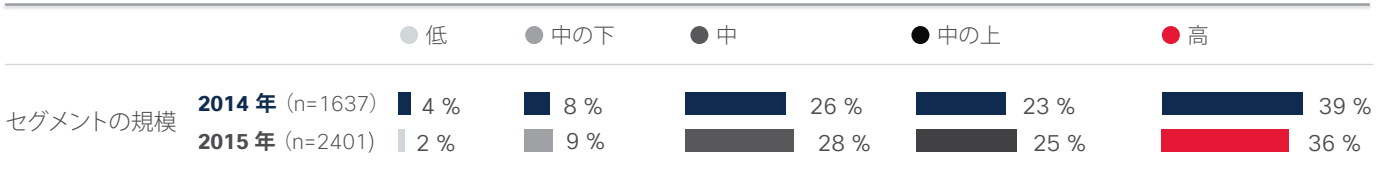
出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

リーダーシップと成熟度

図 81. 5つのセグメントのモデルはセキュリティ能力成熟度モデル(CMM)に沿って追跡される

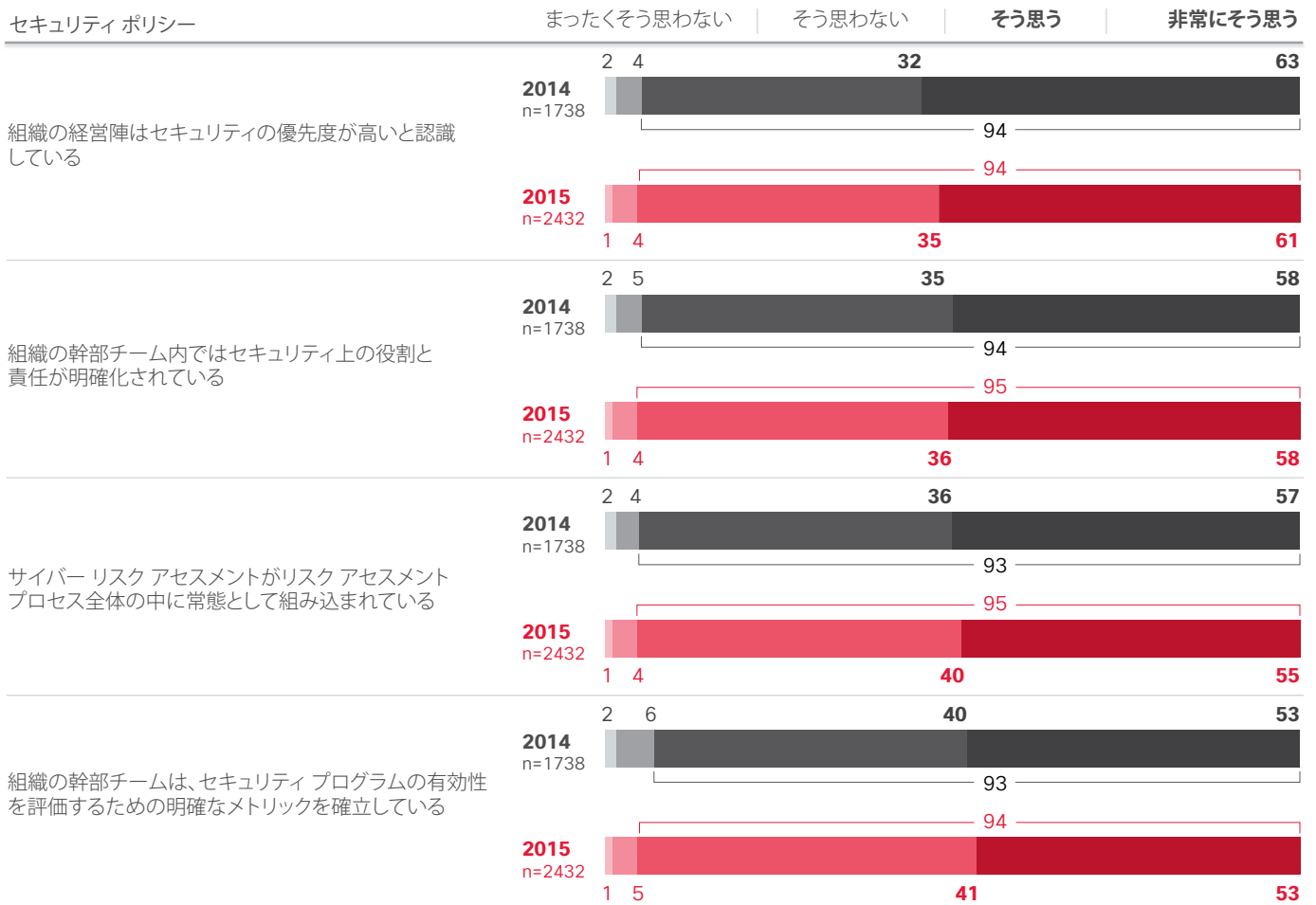
セグメントは、セキュリティの優先順位の成熟度と、それがどのようにプロセスと手順に変換されるかに関して、前年度の調査とよく似たパターンを反映しています。

60% 以上がセキュリティ成熟度プロファイルに合致しています。
この結果は、国および業界の大部分に当てはまります。



出典:シスコによる 2015年セキュリティ機能のベンチマーク調査

図 82. 2014年のように、経営陣はセキュリティを優先事項と認識していることにほとんど同意するか強く同意している



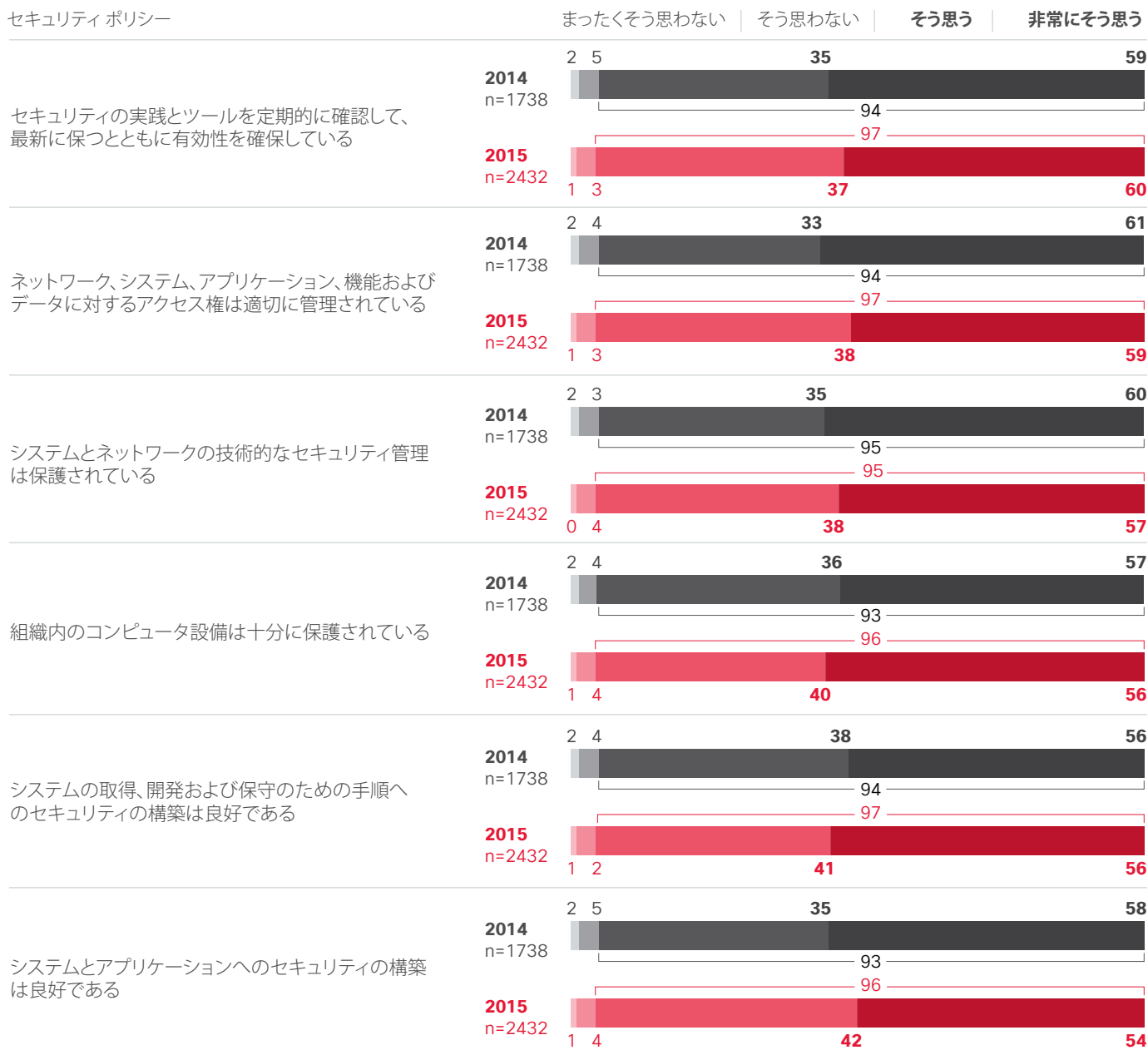
製薬業界の回答者は、その他のすべての産業の専門家に比べて、著しく多数が「組織の幹部チームは、セキュリティ プログラムの有効性を評価するための明確なメトリックを確立している」という項目に強く同意しています。

CSOは、SecOpsと比べて著しく多数が、幹部チームの関与についてのすべての項目に同意しています。

出典:シスコによる 2015年セキュリティ機能のベンチマーク調査

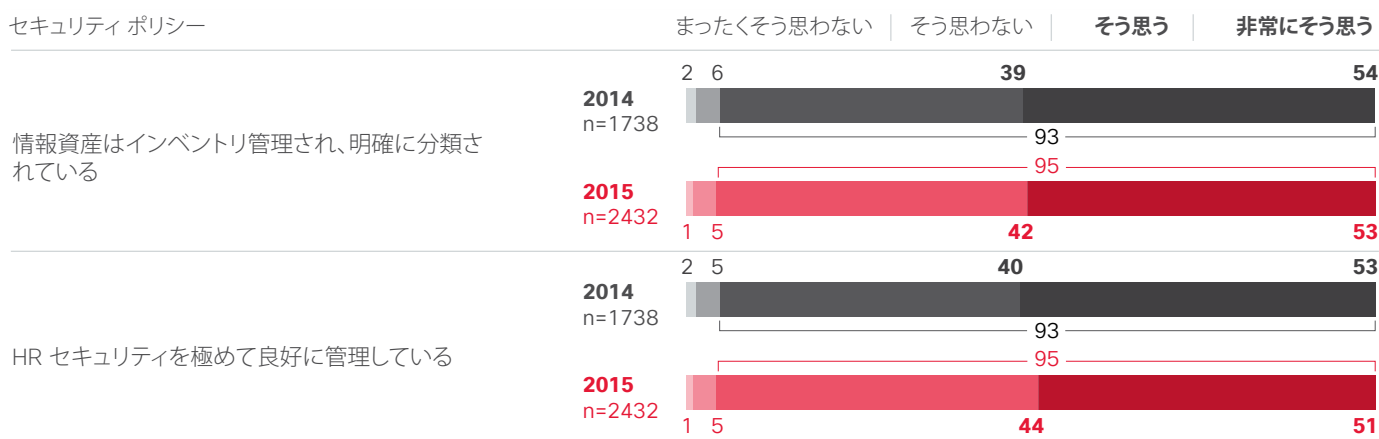
プロセス

図 83. システムにセキュリティを組み込む能力の確信度は不安定



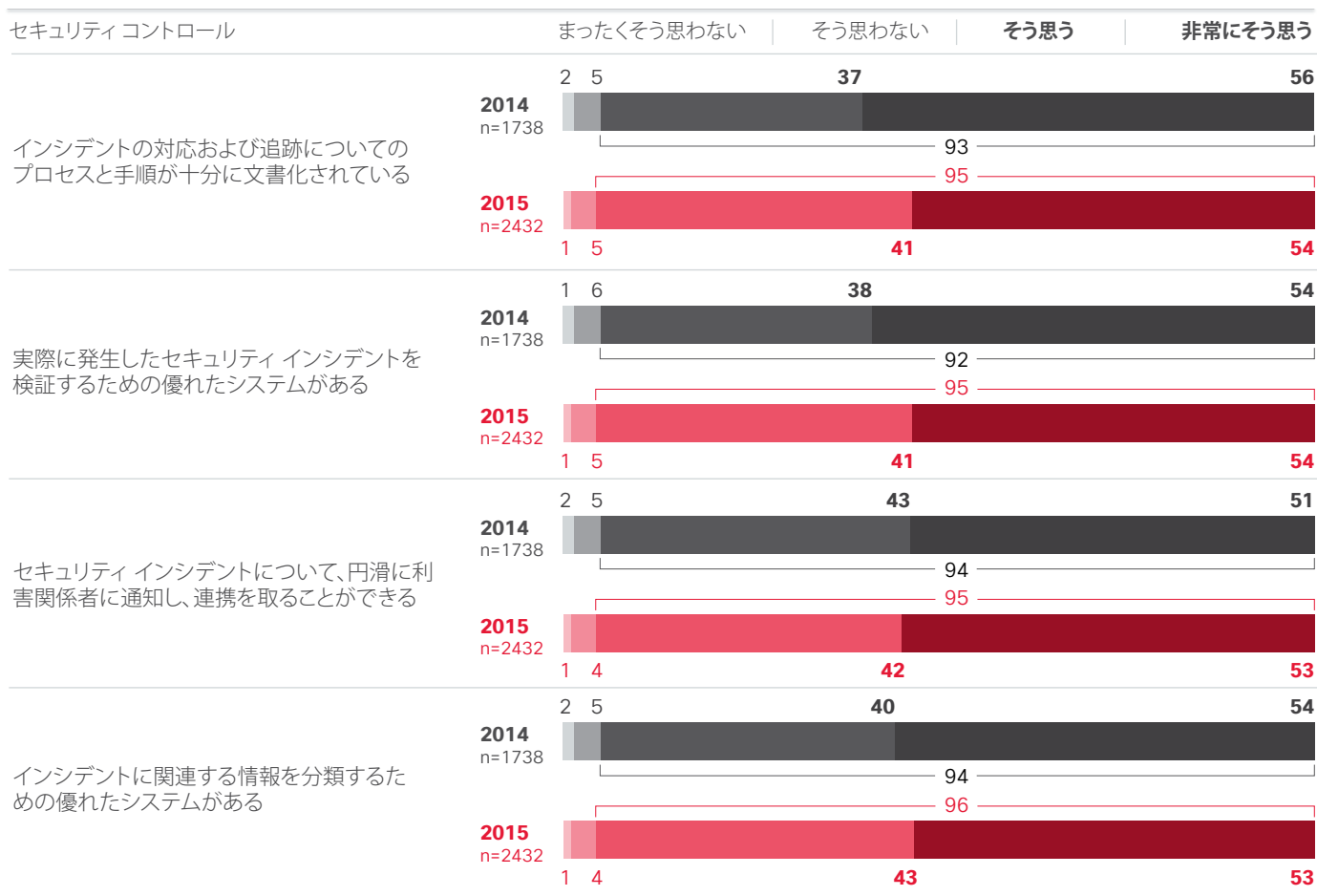
出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 83. システムにセキュリティを組み込む能力の確信度は不安定 (続き)



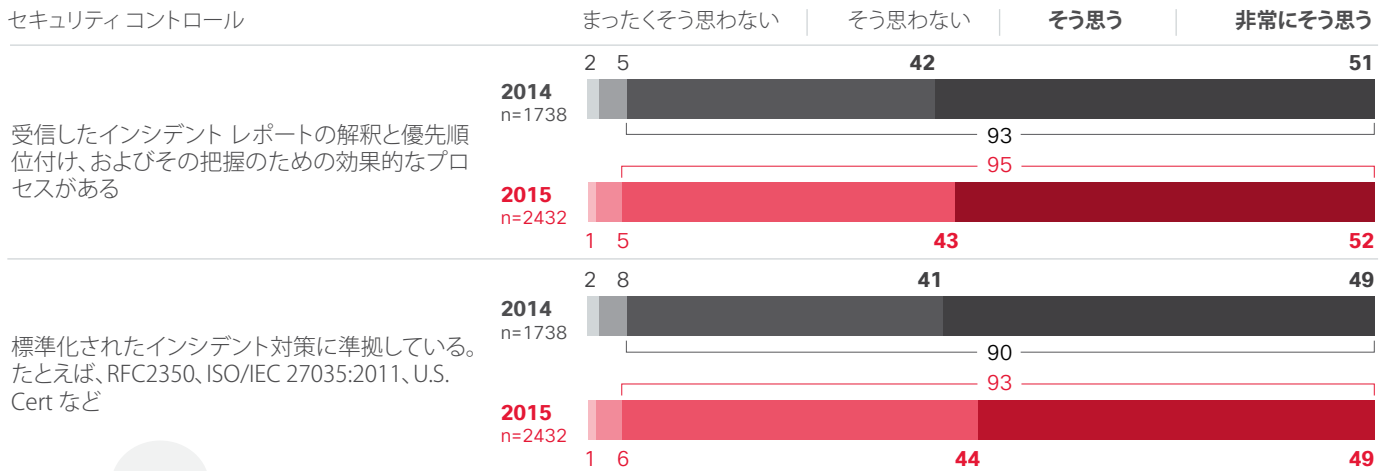
出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 84. 企業はセキュリティ制御が十分であると確信している



出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 84. 企業はセキュリティ制御が十分であると確信している (続き)

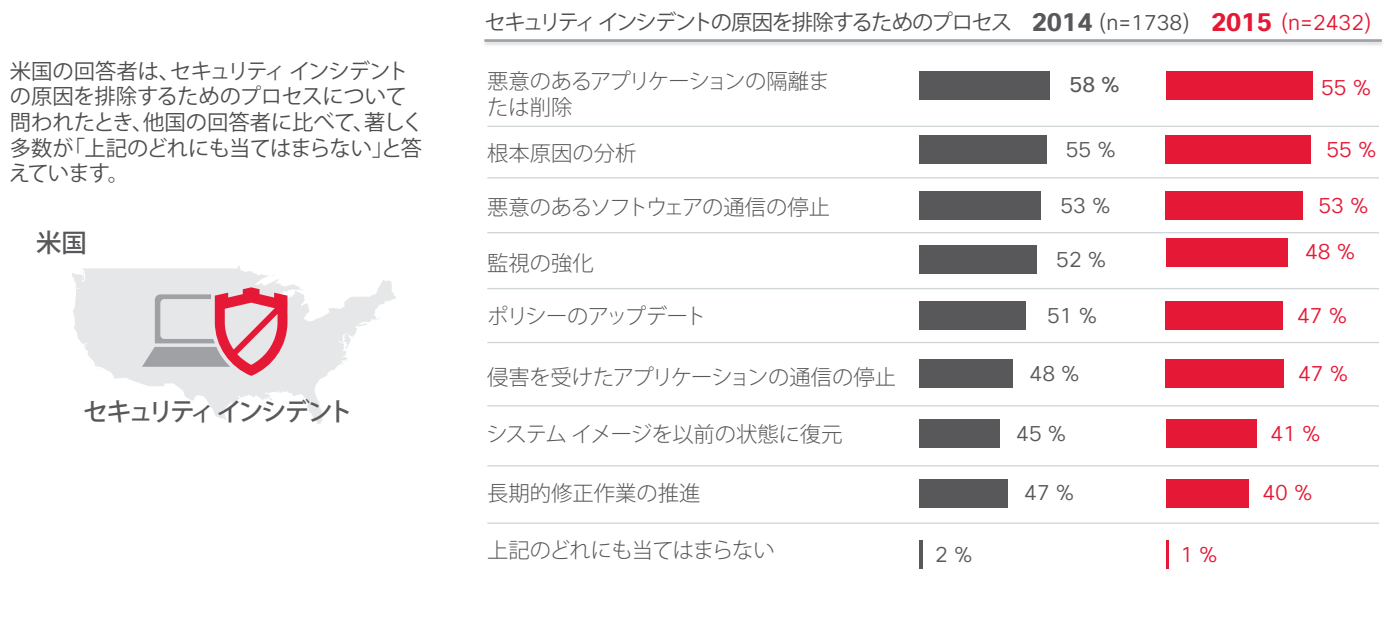


金融サービス業の回答者は、その他のすべての産業の専門家と比べて、多数が「インシデントに関連する情報を分類するための優れたシステムがある」という項目に強く同意しています。

「セキュリティ インシデントについて、円滑に利害関係者に通知し、連携を取ることができる」という項目を除いて、多くのCSOが、SecOpsマネージャに比べて、セキュリティ コントロールに関してより肯定的な見方をしています。

出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 85. 引き続き、悪意のあるアプリケーションの検疫/削除と根本原因の分析がプロセスのトップである



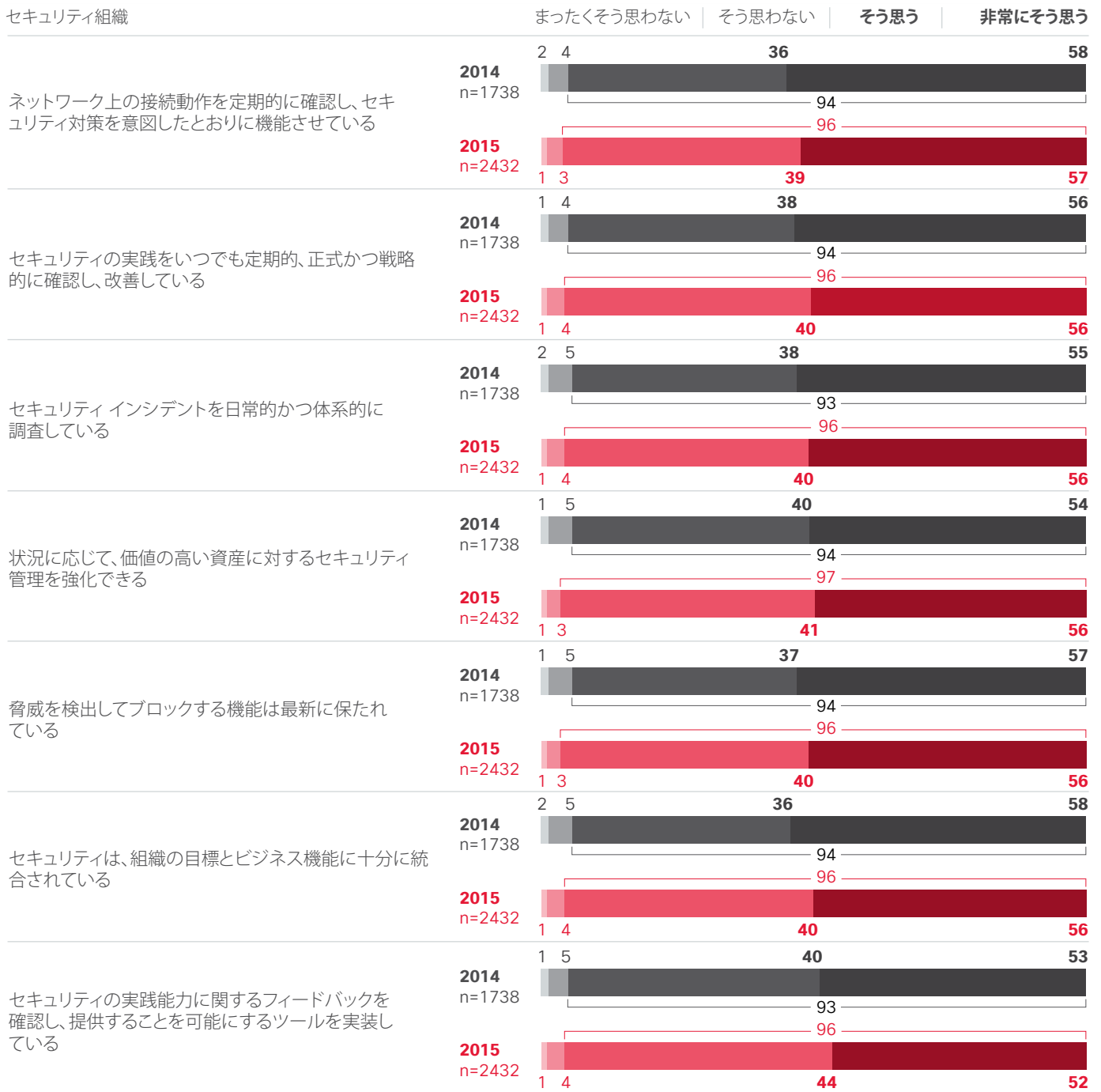
米国の回答者は、セキュリティ インシデントの原因を排除するためのプロセスについて問われたとき、他国の回答者に比べて、著しく多数が「上記のどれにも当てはまらない」と答えています。

米国



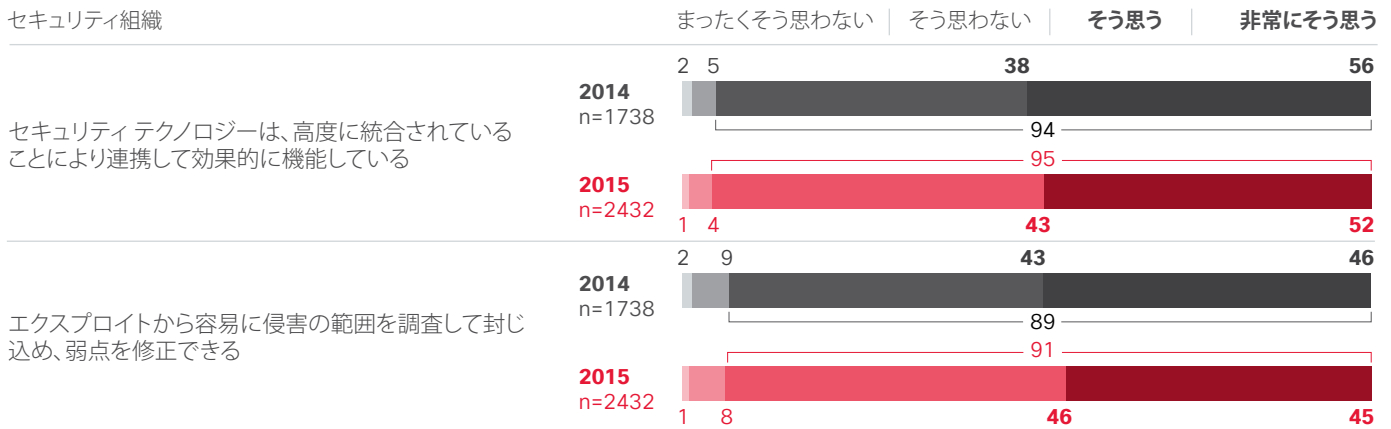
出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 86. 侵害の封じ込め機能に対する企業の確信度は不安定



出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

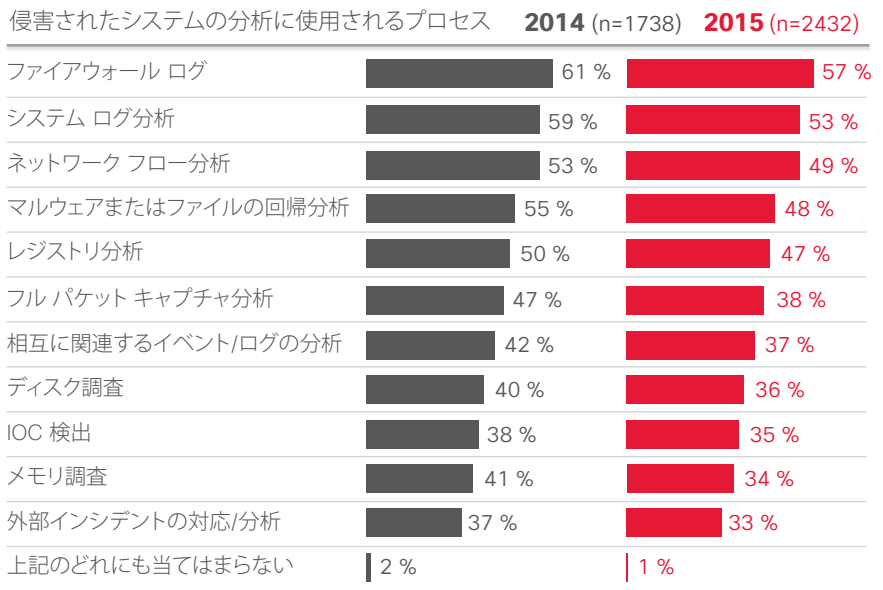
図 86. 侵害の封じ込め機能に対する企業の確信度は不安定 (続き)



出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 87. 引き続き、ファイアウォール ログおよびシステムログ分析は侵害されたシステムの分析に最もよく使用されるプロセスである

エンタープライズおよび大規模企業は、中規模企業よりも、侵害を受けたシステムの分析に多くのプロセスを利用すると回答しています。



出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 88. インシデント前のバックアップからの復元は影響を受けるシステムを復元するために 2015 年に最もよく使用されたプロセスである

中国の回答者は、調査対象である他国の回答者に比べて、脆弱性を持つと見なされたアプリケーションにより頻繁にパッチを適用し、更新していると回答しています。



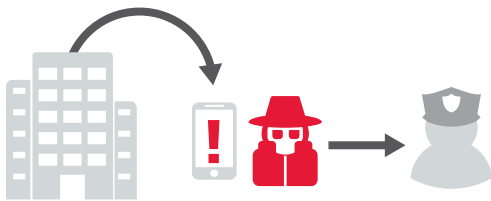
影響を受けたシステムの復旧プロセス	2014 (n=1738)	2015 (n=2432)
インシデント前のバックアップから復旧している	57 %	59 %
インシデント後に特定された弱点に基づいて、追加のまたは新規の検出および管理を実施している	60 %	56 %
脆弱性を持つと見なされたアプリケーションにパッチを適用し、更新している	60 %	55 %
差分復旧 (インシデントによって発生した変更を除去)	56 %	51 %
ゴールド イメージ復旧	35 %	35 %
上記のどれにも当てはまらない	2 %	1 %

出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 89. CEO または 社長にセキュリティ インシデントが報告される可能性が最も高く、その次に業務部門と財務部門が続く

より大規模な企業の回答者は、中規模およびエンタープライズ企業の回答者に比べて、著しく多数がインシデントの発生時に外部機関に通知すると回答しています。

大規模企業



インシデントの際に通知を受けるグループ	2014 (n=1738)	2015 (n=2432)
最高経営責任者	N/A	45 %
業務部門	46 %	40 %
財務部	N/A	40 %
テクノロジー パートナー	45 %	34 %
エンジニアリング	38 %	33 %
人事	36 %	33 %
法務部	36 %	32 %
製造部	33 %	28 %
全従業員	35 %	27 %
広報部	28 %	24 %
ビジネス パートナー	32 %	21 %
外部機関	22 %	18 %
保険会社	N/A	15 %

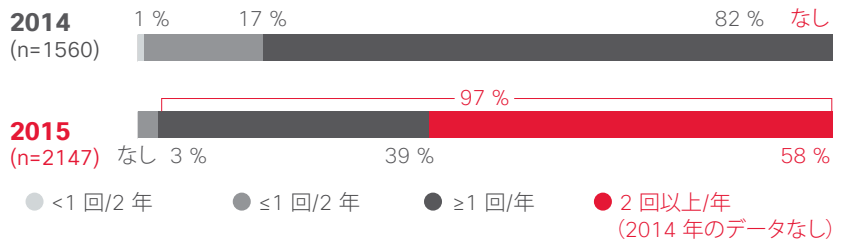
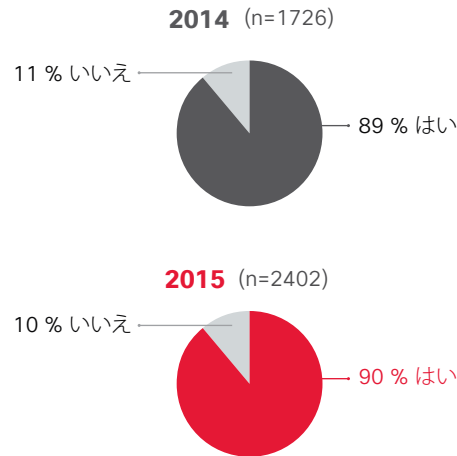
出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

トレーニング

図 90. ほぼすべての企業 (97 %) が少なくとも年に一度はセキュリティトレーニングを提供している

セキュリティに対する認識プログラムやトレーニングプログラムがセキュリティ担当の部署に対して定期的に行われていますか。(セキュリティ専任の回答者)

セキュリティトレーニングを行う頻度はどのくらいですか。(トレーニングを受けているセキュリティチームの回答者)



セキュリティ違反を経験している企業 (96 %) は、経験していない企業 (83 %) と比べて、より多くが定期的にセキュリティに対する認識のトレーニングプログラムを実施しています。

している **96%** 対 していない **83%**

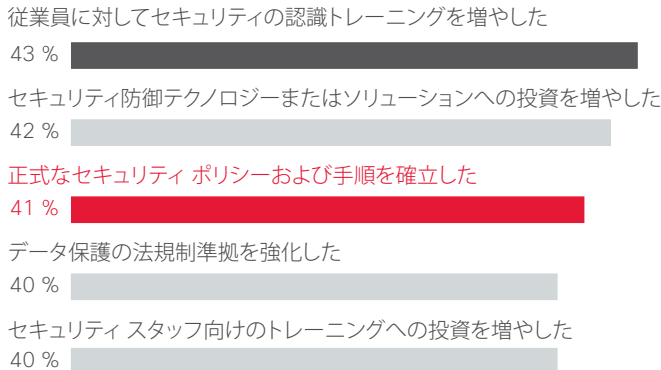
大規模 (93 %) 企業は、中規模 (88 %) およびエンタープライズ (89 %) 企業に比べて、より多くが定期的にセキュリティに対する認識のトレーニングプログラムを実施していると回答しています。

大規模企業 **93%** 中規模企業 **88%** エンタープライズ **89%**

出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 91. セキュリティ認識トレーニングの頻度と公式のセキュリティポリシーの策定率は両方とも 2014 以降増加している — 行動の証拠

(上位 5 件) セキュリティ違反の影響を受けた回答者 (2015 年、n=1109)



従業員に対してセキュリティの認識トレーニングを増やした

2015 年、回答者の 43 パーセントが、漏洩が明らかになった後セキュリティトレーニングを増やしたと回答しています。

43%

2015 年、回答者の 41 パーセントが正式なセキュリティポリシーと手順を策定したと回答しています。

41%

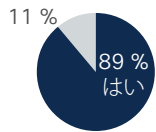
出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

図 92. 2014 年のように、約 9 割がセキュリティスタッフがセキュリティに焦点を当てた会議やトレーニングに参加していると述べている

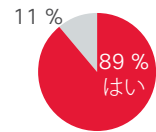
セキュリティスタッフのメンバーはカンファレンスや外部のトレーニングに出席して、そのスキルを向上および維持していますか。(セキュリティ専任の回答者)

従業員はセキュリティ業界の会議または委員会に属していますか。(セキュリティ専任の回答者)

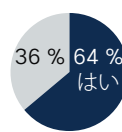
2014 (n=1738)



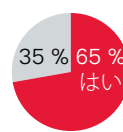
2015 (n=2432)



2014 (n=1738)



2015 (n=2432)



出典:シスコによる 2015 年セキュリティ機能のベンチマーク調査

セキュリティ リスクと信頼性の調査

図 93. 背景と手法

シスコは、企業およびサービス プロバイダーの IT に関する意思決定者が持つ、組織が抱えるセキュリティ上のリスクおよび課題に対する認識、そして、IT ベンダーの信頼性が IT ソリューション購入時に果たす役割についてより深く理解したいと考えています。

具体的な目的は次のとおりです。



外部および内部の脅威と脆弱性によるリスクレベルを測定する。



セキュリティ リスクを軽減するために実装される、戦略、ポリシー、ソリューションを理解する。



IT ソリューションの購入プロセスと、そのプロセスにおいて IT ベンダーの信頼性が果たす役割を明確にする。



IT ベンダーの信頼性を検証する方法についての情報に興味があるか測定する。



業界別/対象者別に、セキュリティ リスクの観点、またはリスクを軽減するアプローチに違いがあるかどうかを判断する。

方法: 量的アプローチと質的アプローチ

この 2 つの方法を活用して、各調査対象の詳細を把握します。

(すべての回答者は IT 購入意思決定に関与)

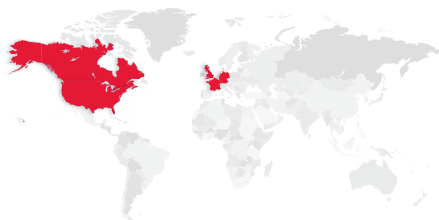


定量的な Web ベースの調査
1050 社の ITDM を対象
(米国 402 社、英国 282 社、ドイツ 197 社、フランス 169 社)



定性的で詳細なインタビュー
20 社のサービス プロバイダーを対象
(米国 7 社、カナダ 3 社、英国 3 社、ドイツ 4 社、フランス 3 社)

調査は米国、英国、フランス、ドイツ、カナダ (IDI のみ) で実施



2015 年 8 月～ 9 月にデータ収集を実施



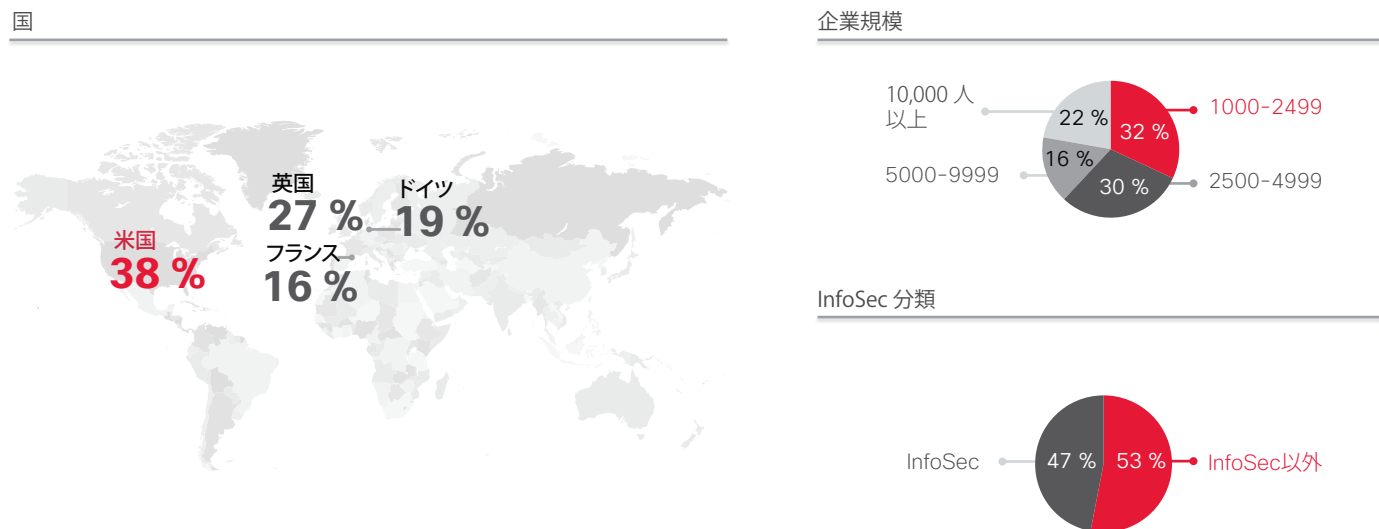
20
具体的な Web ベース アンケート



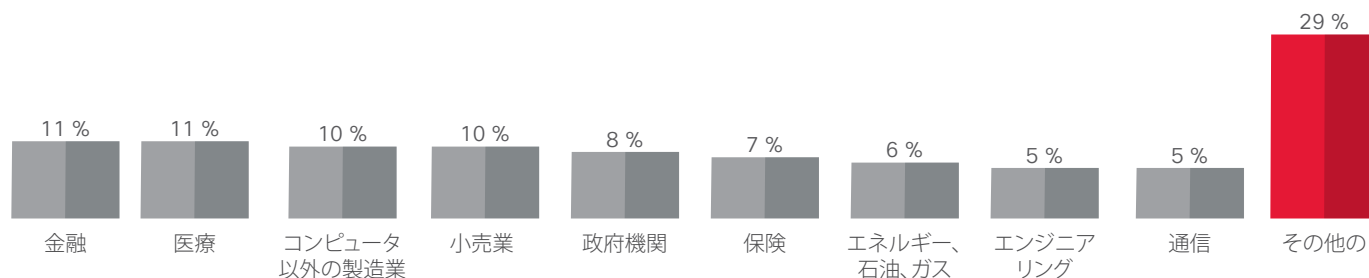
45
具体的で詳細なインタビュー

出典: セキュリティ リスクと信頼性調査、シスコ

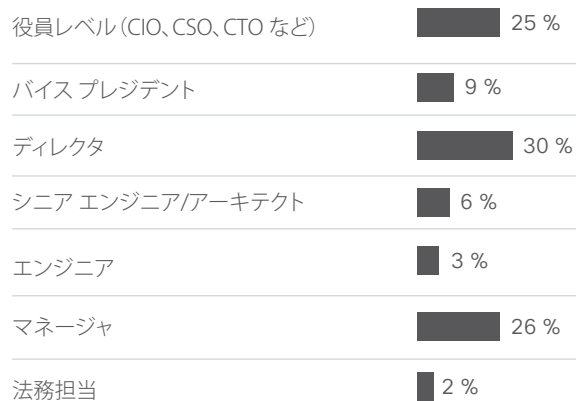
図 94. 企業の回答者のプロフィール(定量的)



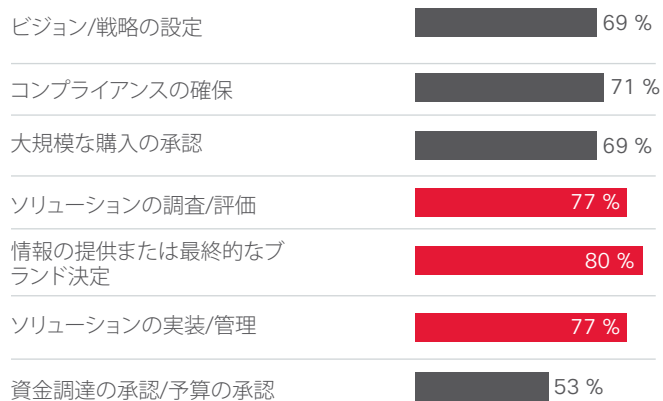
業界 (5 % 超が回答)



役職

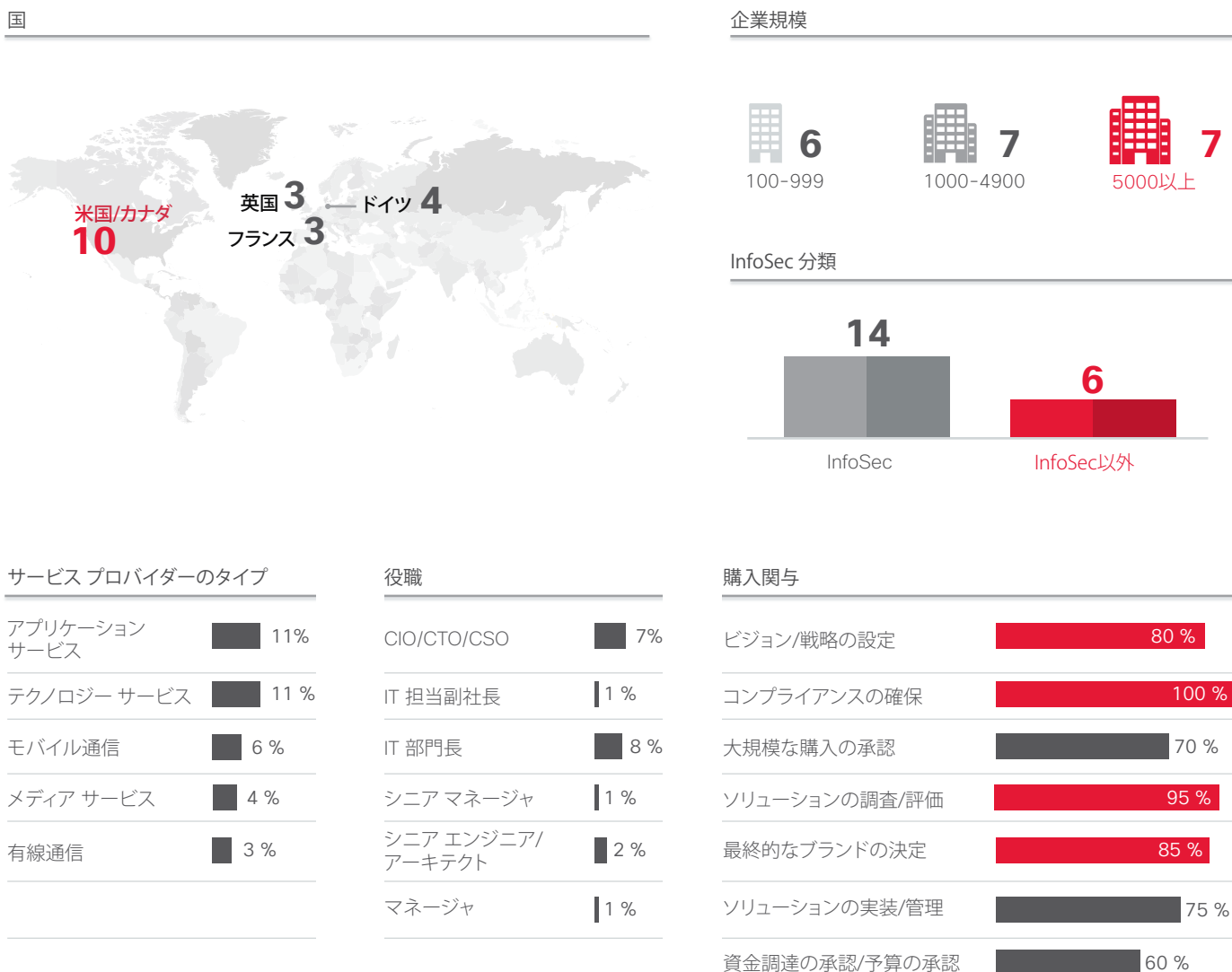


購入関与



出典: セキュリティリスクと信頼性調査、シスコ

図 95. サービス プロバイダーのプロファイル (定数的)



出典: セキュリティリスクと信頼性調査、シスコ

©2016 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(1602R)

この資料の記載内容は2016年2月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



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>

お問い合わせ先