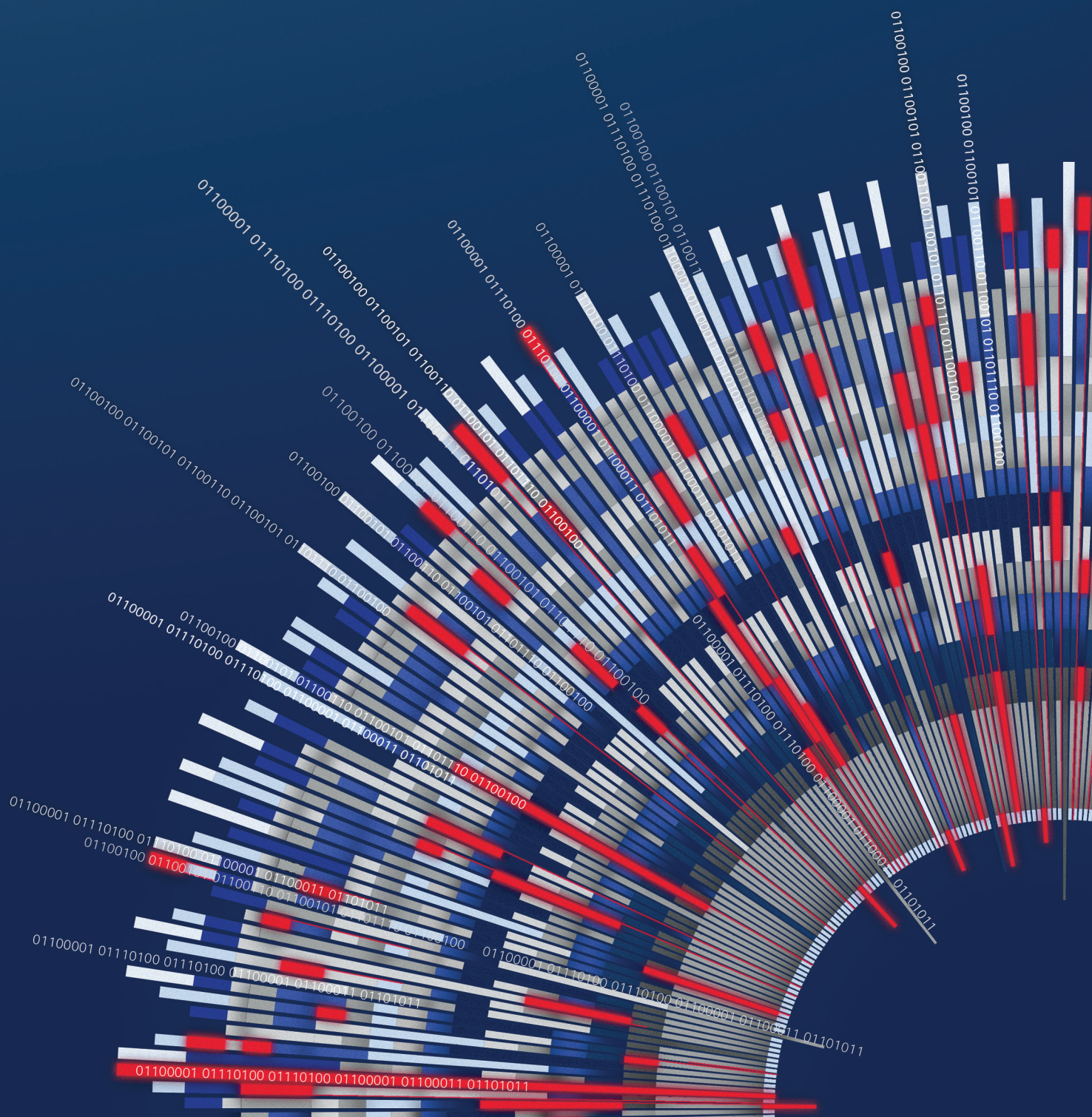
# シスコ 2015 年
# 中期セキュリティ レポート



# エグゼクティブ サマリー

攻撃側の技術が高度化し、ネットワークの防御を破り、検出を回避するマルウェアが開発・投入される中、セキュリティ業界全体も同じペースで新たな技術を取り入れようとしています。

こうした傾向は、セキュリティ製品やサービスを購入する組織にとって大きな課題を突き付けます。セキュリティ ギャップを埋めるために個別的なソリューションを選択することによって、結果的に脆弱な場所ができてしまうからです。

シスコ 2015 年中期セキュリティ レポートでは、こうした相関する課題について検討するとともに、最も強力な脅威に関する最新情報を提供します。このレポートでは、シスコのエキスパートによる調査に基づいて、2015 年前半に見られた主な脅威の概要について説明します。また、今後の傾向を予測し、セキュリティ ソリューションとサービスを求めている中小および大規模組織向けの提言も行います。

## このレポートは、次の 2 つの部分に分かれています。

### 脅威インテリジェンス

このセクションでは、シスコによる最新の脅威研究の概要を示します。次の内容について説明します。

- Angler などのエクスプロイト キットの最新情報
- 犯罪者による Microsoft Office 関連のマクロ使用の増加
- 検出回避のためにマルウェア作成者が取る新たな手法
- 特定の業種でのマルウェア遭遇リスク
- 脅威検出時間
- スパム、脅威アラート、Java エクスプロイト、マルバタイジングに関する最新情報

### 分析と所見

このセクションでは、セキュリティ業界の統合や、統合脅威防御という新たなコンセプトについて扱います。その他のトピックとしては、信頼性とセキュリティを製品に組み込むことの重要性と、人材が不足するセキュリティ市場においてセキュリティ サービス組織を関与させることの意義が含まれます。最後に、組織全体で取り組むサイバーガバナンス フレームワークが、グローバルな持続的ビジネス イノベーションと経済成長に向けた第一歩であることを説明します。

# 主な傾向と特徴

*攻撃者は、検出されずにネットワークに忍び込み、セキュリティ対策を回避するために常に新しい技術を取り入れています。*

- Adobe Flash の脆弱性を利用したエクスプロイトが増えています。これらのエクスプロイトは、Angler や Nuclear など、広く使用されているエクスプロイト キットに定期的に組み込まれています。
- Angler は、全体的な巧妙さと有効性の点で、エクスプロイト キット市場を引き続きリードしています。
- ランサムウェア（身代金要求ウィルス）などのクライムウェアの運営元は、専門の開発チームを雇って資金提供し、収益を上げ続けています。
- 攻撃者は、検出を回避しつつ、指揮および統制の通信を中継するため、匿名 Web ネットワークである Tor と Invisible Internet Project（I2P）を利用し始めています。
- 攻撃者は、マルウェアの配布に Microsoft Office マクロの使用を再開しています。これは一度は廃れた手法ですが、悪意のある者がセキュリティ保護を阻止する新しい方法を探している中で、再度取り上げられています。
- 一部のエクスプロイト キット作成者は、エクスプロイト キットをホストする Web ランディング ページに、ジェーン・オースティンの古典小説『*分別と多感*』のテキストを取り込んでいます。ウイルス対策などのセキュリティ ソリューションは、そのようなテキストを「解読」した後、多くの場合これらのページを正当なものとして分類します。
- マルウェア作成者は、ネットワーク上での存在を隠すために、サンドボックス検出などの手法を利用するようになっています。
- 2015 年の最初の 5 ヵ月間、スパムの量は、米国、中国、ロシア連邦で増加していますが、他の地域では比較的一定しています。
- セキュリティ業界は、オープン ソース ソリューションにおける脆弱性の軽減に注力しています。
- 2015 年シスコ年次セキュリティ レポートで説明した傾向が続き、Java 関連のエクスプロイトは、2015 年の前半は減少しています。

# 目次


**エグゼクティブ サマリー ..... 2**

**主な傾向と特徴 ..... 3**

**概要 ..... 5**

**脅威インテリジェンス ..... 7**

2015 年前半は Flash のエクスプロイトが増加 ..... 8

Flash への注目により、Angler が優位性を確保 ..... 10

Angler：見えないところで動作 ..... 11

ペイロードの暗号化により Angler 検出までの時間が長期化 ..... 12

エクスプロイト キットの作成者はランディング ページを隠すために教養人を気取る ..... 13

ランサムウェアの進化：革新の事例とハードルの低下 ..... 13

ネットワーク通信を隠すため、サイバー犯罪者は Tor を採用 ..... 15

Microsoft Office マクロがエクスプロイトの起動手段として復活 ..... 15

Rombertik：データを盗むだけでなく破壊もできるマルウェア ..... 18

スパム量は一定 ..... 20

脅威と脆弱性：エクスプロイトがよくあるコーディング エラーを悪用 ..... 21

サードパーティの脆弱性 ..... 21

Java を使用したエクスプロイトは減少 ..... 24

マルウェア作成者が採用する検出と回避の手法 ..... 25

マルウェアに遭遇する業界別リスク：攻撃を受けない業界はない ..... 26

ブロック アクティビティ：地域別の概要 ..... 27

Web ベースの攻撃の種類 ..... 28

マルバタイジングの最新情報：検出を回避し攻撃の効率を高めるための Web ベースの脅威が拡散 ..... 29

検出時間：定義 ..... 30

**分析と所見 ..... 31**

サイバーセキュリティに関して実施すべきアクション：セキュリティ ベンダーによる迅速なイノベーション ..... 32

業界の統合と統合型脅威防御 ..... 33

信頼できる製品 ..... 33

専門技術の価値 ..... 34

将来のイノベーションを支えるためのグローバル サイバーガバナンス フレームワーク ..... 35

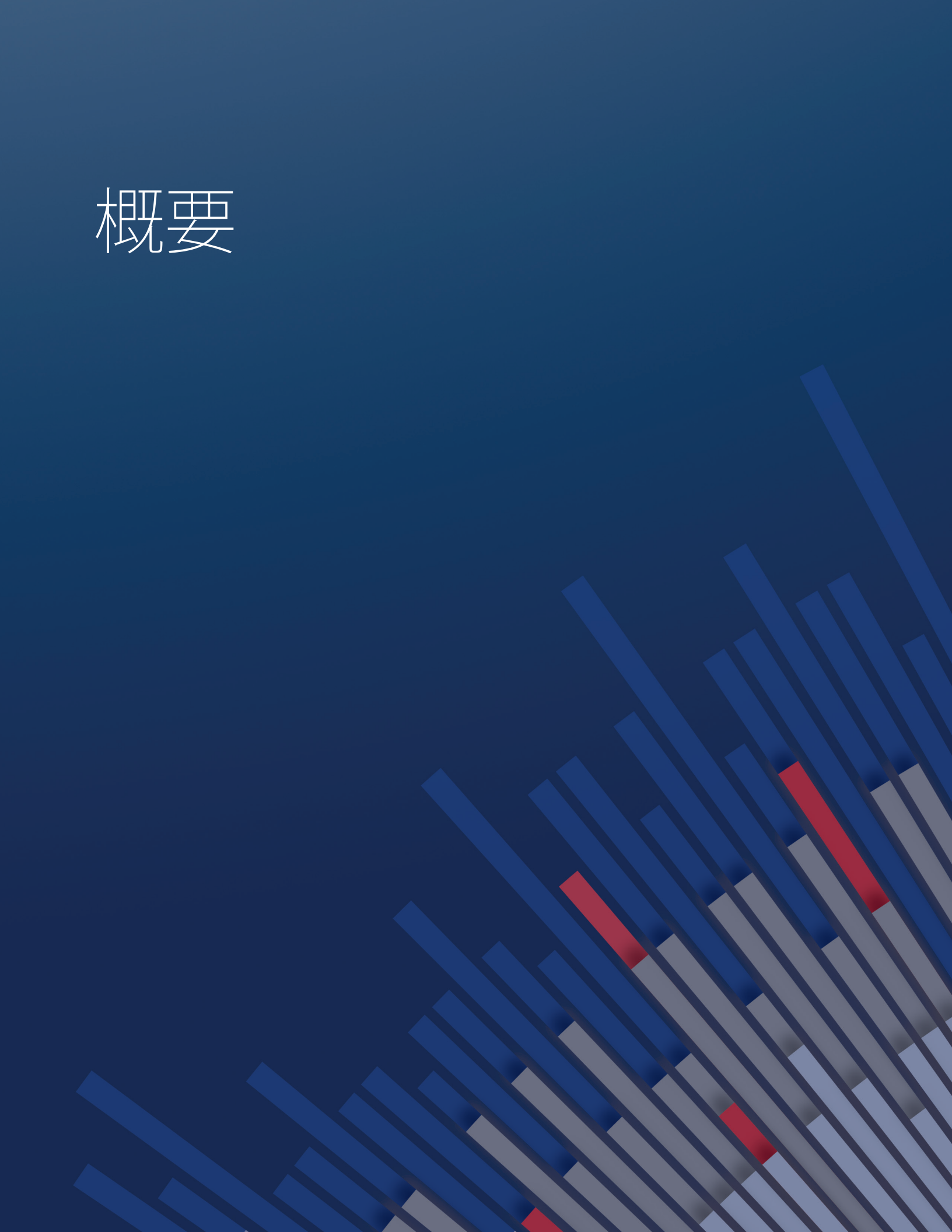
協調的なルール造り：将来の方向性 ..... 35

**まとめ ..... 37**

**シスコについて ..... 39**

シスコ 2015 年中間セキュリティ レポートの執筆者 ..... 40

# 概要



# 概要

*マルウェアの作成者とオンラインの犯罪者が開発した手法は、この数年間でますます高度化しています。ここ最近のシスコ セキュリティ レポートでは、地下経済におけるそのような技術革新と、攻撃者の先回りを目論むセキュリティ プロフェッショナルについて紹介してきました。*

最近の傾向としては、脅威アクターが、新しい技術を迅速に取り入れ、システムを侵害して検出を回避するための能力を高めつつあることが挙げられます。2015 年前半のオンライン攻撃者の特徴は、新しいツールと戦略を進化させ、古いツールと戦略を再利用して、セキュリティ防衛をかいくぐろうとしていることです。不明化などの手法を通じて、ネットワーク防御をこっそり通過するだけでなく、検出されることがあったとしても、それよりも遙か前にエクスプロイトを実行するようになっています。

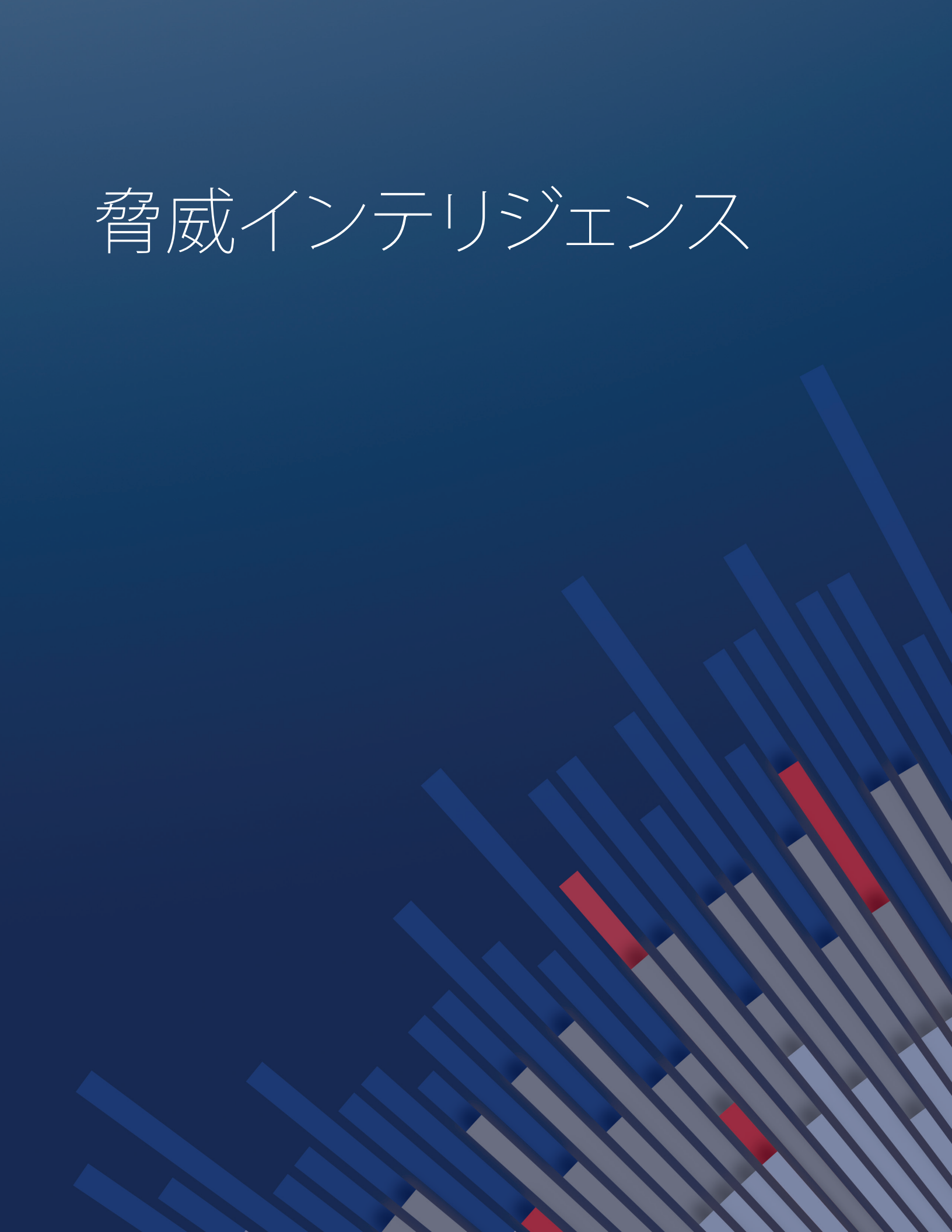
セキュリティ ベンダーは、独自のイノベーションで対処しています。たとえば、.cab や .chm などの形式を使用する新しい攻撃が検出されたことから、研究者はこれらの新しいファイル形式の分析もサポートするようになっています。また、ベンダーは新しい検出エンジンを開発しており、常に新しいヒューリスティック手法を評価および進化させ続けています。

セキュリティ ベンダーは、俊敏であり続けることの必要性を理解しています。セキュリティ ベンダーやそのネットワークがわずかでも気を抜くと、攻撃者が優勢になります。しかし、業界のイノベーションのペースは、十分に迅速であるとは言えません。

多くのベンダーが、セキュリティの問題に対し、断片的なソリューションや個別的なソリューションを提供しています。また、セキュリティ ツールを購入する組織は、包括的で戦略的なソリューションではなく、その場しのぎの製品を求めています。しかし、セキュリティ全体に渡ってテクノロジーやプロセスを統合していないため、セキュリティ ツールの管理は複雑で扱いにくいものになります。

セキュリティ業界の統合と、先進テクノロジーの密接な統合により、将来的には、製品別のアプローチを採用しなくて済むようになる可能性があります (ページ 33 を参照)。それまでの間、中小規模および大規模組織とそのセキュリティ チームは、このレポートで述べている高度な脅威に対応するために、テクノロジーを構成要素とする、プロアクティブで包括的な防御戦略を利用できるものと考えられます。

# 脅威インテリジェンス



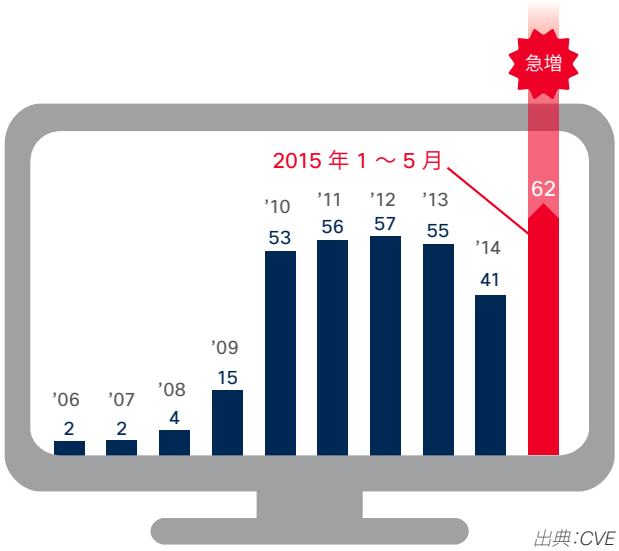
# 脅威インテリジェンス

*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。*

## 2015 年前半は Flash のエクスプロイトが増加

2015 年の最初の 5 ヵ月間、Common Vulnerabilities and Exposures（CVE）プロジェクトは、ユーザのマシン上でのコード実行に結びつく Adobe Flash Player の 62 件の脆弱性を公開しました。図 1 に示すように、2014 年には、この種の脆弱性は 41 件しか見つかっていません。2 番目に件数が多かった2012 年には、このような Flash の脆弱性が 57 件確認されました。現在の行動パターンが年度の後半も続けば、2015 年にはこれらのエクスプロイトの数が 100 を超え、史上最高を記録します。

図 1. ユーザのマシン上でのコード実行に結びつく Flash の脆弱性の数：2006 年 1 月～ 2015 年 6 月




*出典：CVE*

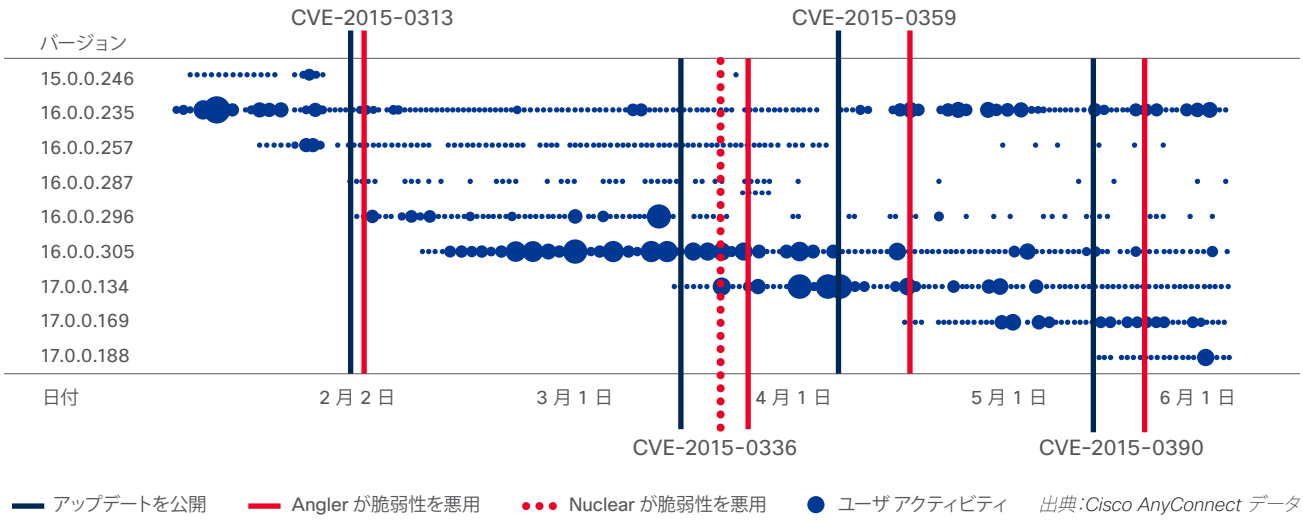
シスコでは、Flash の脆弱性のエクスプロイトが最近増えている理由として、主に次の 2 つの要因があると考えています。

- Flash のエクスプロイトは、Angler など、広く使用されているエクスプロイト キットの最新バージョンに定期的に統合されています（ページ 9 を参照）。
- Adobe は Flash Player を頻繁に更新していますが、多くのユーザは、修正対象の脆弱性をターゲットとするエクスプロイトから自身を保護するための更新を、迅速には行っていません。

多くのユーザは、Adobe Flash を常に更新しておくことを困難に感じているようですが、アップグレードに気づいていない可能性もあります。図 2 は、Angler の作成者がこの「パッチ適用ギャップ」（Adobe が更新プログラムをリリースしてからユーザが実際にアップグレードするまでの時間）を利用していることを示しています（シスコのテクノロジーを使用すれば、研究者が任意の時点でユーザのソフトウェア バージョンをモニタすることができます）。

レポートの共有

図 2. Flash のバージョン別のリクエスト（日単位）




たとえば、図 2 の 2015 年 2 月の期間に、多くのユーザが最新バージョンの Flash（16.0.0.305）に移行していることがわかります。その更新プログラムは、2015 年 2 月 2 日にリリースされ、CVE-2015-0313 の脆弱性に対処しています。しかし、ユーザが新しいバージョンの Flash に移行している間、Angler は以前のバージョンの既知の脆弱性を積極的に悪用しました。

また、図 2 は、Angler エクスプロイト キットの作成者が、CVE-2015-0313 の脆弱性をターゲットにした有効なエクスプロイトを素早く開発してリリースできることも示しています。シスコは、2015 年の前半に、他の Flash エクスプロイトについても同様の素早いイノベーションが行われていることに気付きました。たとえば、もう 1 つの高度で常にアクティブなエクスプロイト キットである Nuclear は、CVE-2015-0336 の脆弱性を素早くターゲットにしました。Angler は、その後すぐに同じ脆弱性を悪用し始めました。

パッチ適用ギャップは、Java ユーザが攻撃者に付け入られ続けている理由の 1 つです（図 3 を参照）。

Flash などの新しい脆弱性をターゲットとするように設計されている攻撃が、Angler や Nuclear などのエクスプロイト キットに素早く統合されることから、セキュリティ チームがこれに追いつくことはますます難しくなっています。これらの脅威を識別するにはレトロスペクティブ分析が必要な場合も多いため、検出に要する時間も長くなります。

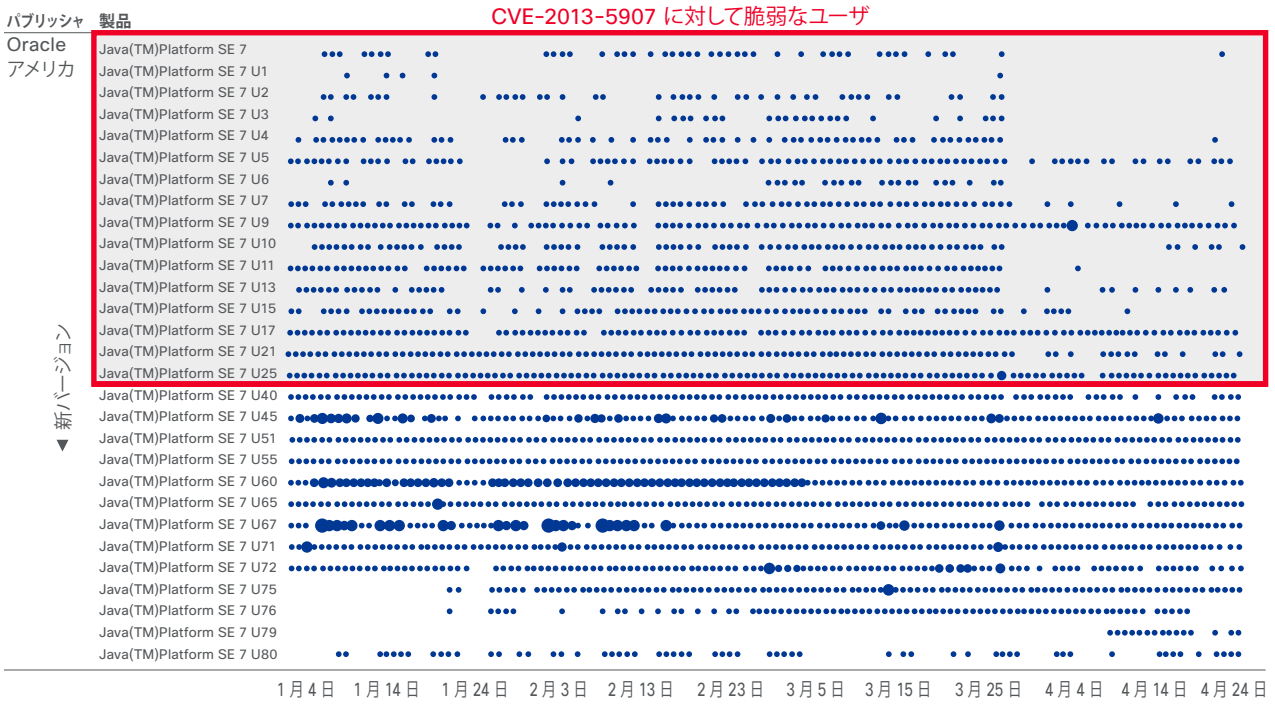
単一の検出エンジンのみに依存している個人ユーザや組織は、侵害のリスクが大きくなります。また、レトロスペクティブ分析機能のない環境では、ゼロデイ攻撃や回避手段を通じて送信された脅威が長時間検出されないままになりかねず、まったく検出されないこともあり得ます。

しかし、1 つの基本的な対策として、迅速かつ定期的にソフトウェアのパッチを適用すれば、Flash や Java の既知の脆弱性を悪用するように設計された脅威のリスクが大幅に軽減されます。

レポートの共有

図 3. Java のバージョン別のリクエストの数（日単位）






*出典：Cisco Cloud Web Security データ*

## Flash への注目により、Angler が優位性を確保



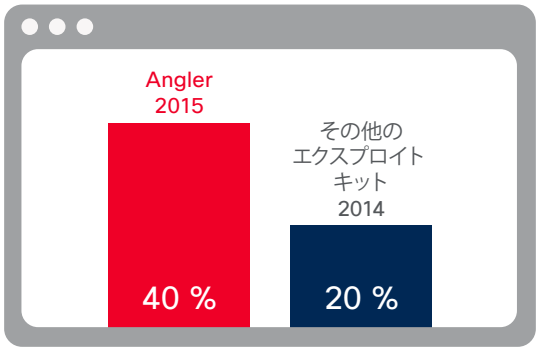
今年の初め[1]、シスコは Angler エクスプロイト キットを、流通している既知のエクスプロイト キットの中で注目すべきものとして選びました。その理由は、Flash、Java、Microsoft Internet Explorer、Silverlight の脆弱性の利用方法が革新的であるためです。2015 年に入って以来、Angler は、エクスプロイト キットの高度さと有効性の点でトップに位置しています。

エクスプロイト キットの作成者は、Adobe Flash の脆弱性に集中的かつ迅速に対応していることは注目に値します。

シスコでは、Angler エクスプロイト キットの Web 上のランディング ページにたどり着いたユーザの 40 % が侵害されていると報告しています（図 4 を参照）。これは、Angler が Flash などの悪用可能な既知の脆弱姓を認識できることを意味しています。その後 Angler は、ユーザのマシンにペイロードをダウンロードします。

これに比べて、2014 年には、さまざまなエクスプロイトを組み合わせることを特徴とする、他の広く使用されているキットの平均成功率は、シスコの調査によれば 20 % に過ぎませんでした。

図 4. 悪用された訪問者の割合
2014 年 12 月～ 2015 年 5 月




*出典：シスコ セキュリティ リサーチ*

1 『2015 年シスコ年次セキュリティ レポート』（2015 年 1 月）：http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html。

## Angler：見えないところで動作

Angler がオンラインでユーザを侵害することに成功した理由のひとつは、シンプルですが実は綿密に構成された Web ランディング ページにあります。シスコの研究者は、通常の Web ページのふりをしてユーザを欺くために使用される、コンピュータによって生成されたランディング ページは、エクスプロイト キットの作成者がデータ サイエンスに基づいて作成している可能性があると指摘しています。マルバタイジング（悪意のあるオンライン広告）が、これらのページに Web トラフィックを一貫して導く主な促進要因となっている可能性があります（マルバタイジングの詳細については、ページ 29 を参照してください）。

Angler は、検出を避けることにも秀でています。「ドメイン シャドウイング」は、作成者が最近採用した手法の 1 つです。エクスプロイト キットの作成者は、ドメイン名登録者のアカウントを侵害し、侵害されたユーザの正規のドメインの下にサブドメインを登録します。ユーザは、アカウント情報を確認しない限り、これらのサブドメインがあることを知りません。サブドメインは悪意のあるサーバを指しています。サブドメインは大量にあり、存続期間が短くランダムなため、ブロックするのは困難です。

ドメイン シャドウイングは新しいものではありませんが、その使用は 2014 年 12 月以降増加を続けています。シスコの調査によると、その時以降、エクスプロイト キットの作成者による既知のサブドメイン アクティビティの 75 % 以上が Angler に起因している可能性があります。エクスプロイト キットはファイル エクスプロイトを通じて、ランサムウェアであるトロイの木馬の Cryptowall など、さまざまな悪意のあるペイロードを提供します。

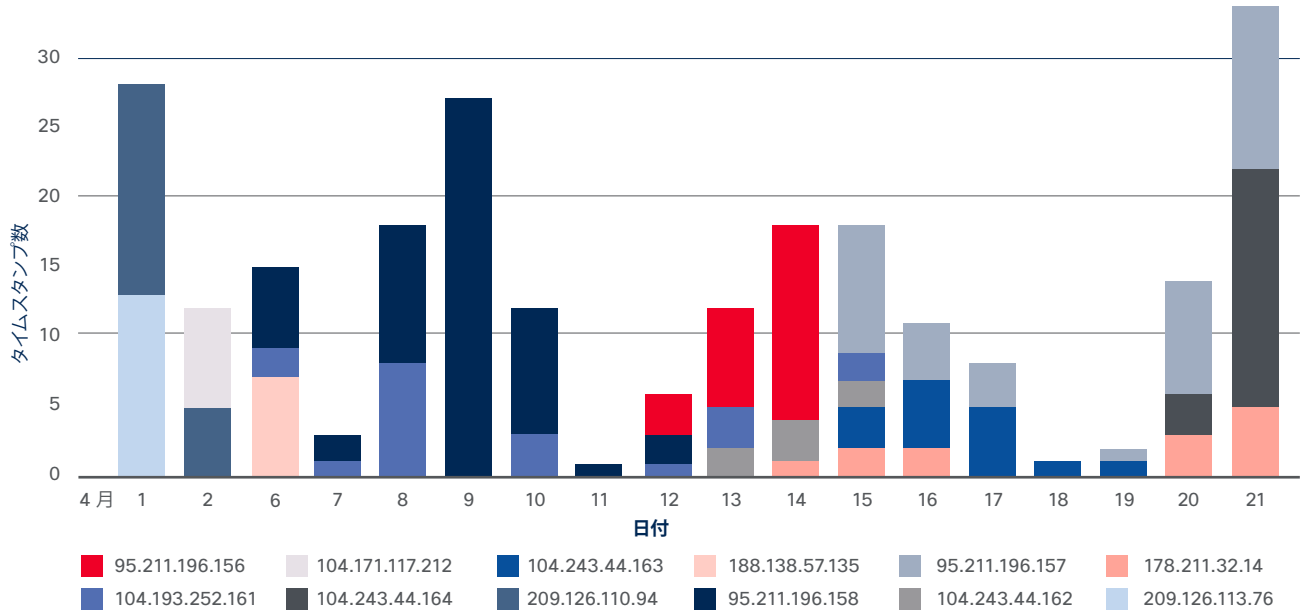
Angler エクスプロイト キットは、ドメイン シャドウイングに加えて、検出をさらに困難にするために複数の IP アドレスを使用します。図 5 の例は、Angler が特定の日にどれだけ頻繁に IP を切り替えることができるかを示しています。パターンはランダムに現れます。

Cisco 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）のブログ投稿『**Threat Spotlight: Angler Lurking in the Domain Shadows（脅威のスポットライト：ドメイン シャドウに潜む Angler）**』[英語] では、Angler が悪意のあるコンテンツを提供できるサブドメインをどのように作成し、この種の攻撃を検出するために、セキュリティに対する多層防御アプローチが不可欠な理由について説明しています。

また、Talos グループのブログ投稿『**Domain Shadowing Goes Nuclear: A Story in Failed Sophistication（ドメイン シャドウイングを利用する Nuclear：高度化の失敗）**』[英語] では、ドメイン シャドウイングを含む Nuclear キャンペーンについて調べています。この未完成のキットは、完成すればエクスプロイト キット プラットフォームとして成功する可能性があります。

図 5. 成功する Flash エクスプロイト、2015 年 4 月

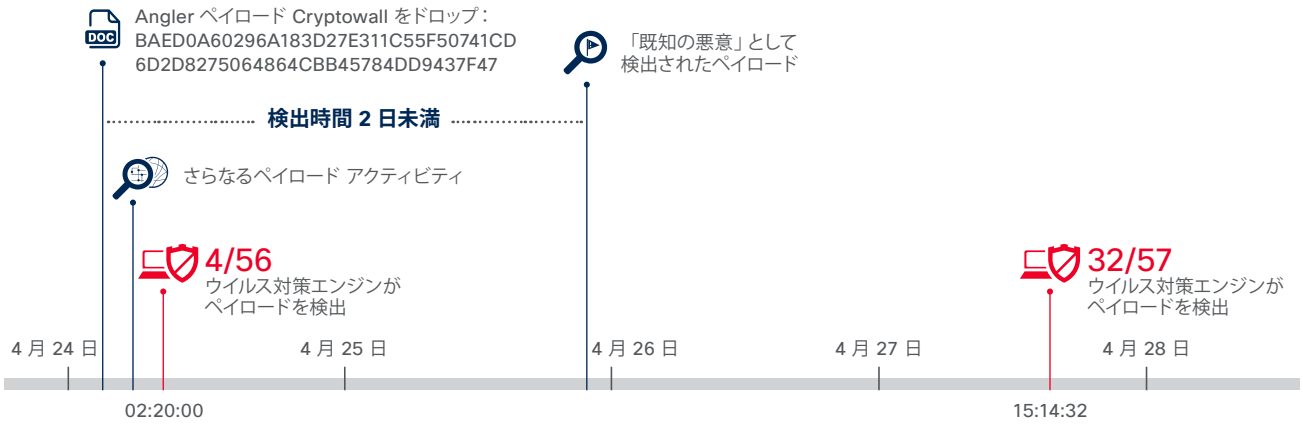
レポートの共有




* 色は IP の範囲を表します。

*出典：シスコ セキュリティ リサーチ*

図 6. Angler ペイロードの検出時間は、2015 年 4 年 24 日に低下




*出典：シスコ セキュリティ リサーチ*

## ペイロードの暗号化により Angler 検出までの時間が長期化

Angler は、通常は暗号化されたペイロードを送信します。これは、多くの場合トロイの木馬である Cryptowall です。このペイロードは、最初にブロックされていない場合、レトロスペクティブを使用しないと識別できず、脅威の検出に数日かかる場合があります。

いったんペイロードが検出されると、革新性の評判を求めて行動するエクスプロイト キットの作成者は、Cryptowall などの脅威を提供し、ウイルス対策ソリューションを回避するための手法を速やかに開発します。

図 6 は、2015 年 4 月 24 日に最初にドロップされた、Angler ペイロード Cryptowall（BAED0A60296A183D27E311C55F50741CD6D-2D8275064864CBB45784DD9437F47）の検出に要した時間を示しています。

最初の日には、VirusTotal によって導入された 56 種類のウイルス対策エンジンのうち、マルウェアの新しいインスタンスを正しく識別できたものは 4 種類しかありませんでした。しかし、4 月 27 日までに、57 種類のウイルス対策エンジンのうち 32 種類が脅威を検出しました。

- 2015-04-24 02:20:00 **4/56**（導入された 56 種類のウイルス対策エンジンのうち、4 種類がペイロードを検出）
- 2015-04-27 15:14:32 **32/57**（導入された 57 種類のウイルス対策エンジンのうち、32 種類がペイロードを検出）

シスコは、4 月 24 日にこの脅威を「不明」として識別し、2 日以内に脅威を分析して、レトロスペクティブによって脅威を宣言（「既知の悪意」と分類）しました。

検出時間の定義と計算方法についての詳細は、ページ 30 の「検出時間：定義」を参照してください。

レポートの共有

### エクスプロイト キットの作成者はランディング ページを隠すために教養人を気取る

一部のエクスプロイト キットの作成者は、19 世紀の文学作品を使用して 21 世紀の脅威を隠そうとしています。具体的には、一部の攻撃者は、エクスプロイト キットをホストする Web ランディング ページに、ジェーン・オースティンの『*分別と多感*』のテキストを組み込んでいます。

エクスプロイト キットのランディング ページに古典テキストの一節を加えることは、従来のランダムなテキストを使用するアプローチよりも不明化の手法として効果的です。雑誌やブログなどのより現代的な作品のテキストを使用することも効果的です。ウイルス対策などのセキュリティ ソリューションは、そのようなテキストを「解読」した後、多くの場合この Web ページを正当なものとして分類します。

ユーザにとって、エリノア・ダッシュウッドやジェニング夫人などの愛すべきオースティンの登場人物が Web ページで予期せず参照されていると、当惑する可能性がありますが、すぐに心配になるものではありません。不快感がないことで、エクスプロイトを開始するための多くの機会を攻撃者に与えます。

ランダムなテキストではなく有名な作品を使用することは、脅威アクターが検出を避けるために自身の方式をいかに変えているかを示す 1 つの例に過ぎません。

図 7. エクスプロイト キットのランディング ページで使用されている『*分別と多感*』のテキストの例

```
https://rt1.mtd.cisco-services.com/Ticket/
Display.html?
id=137668&results=ad470ba70bfbd94464c2a0e9deff943b

Sense and sensibility - jane austin
    <small>
      Mr. Ferrars comfortable as a continual flow of
tears would permit her. In the society of both. Why
they should both attend through
    </small>
     She looked down as a difference of the three, by
their presence; and it will be so easily settled. it
    <i>
     the cruel situation in which she had by that
which only could convince her, a better match for
your mother--will you allow him to give rise to
conjectures, which might make it rare; for his
sisters by the hand, and speaking in an audible
voice, and walking the
    </i>
```

*出典：シスコ セキュリティ リサーチ*

## ランサムウェアの進化：革新の事例とハードルの低下

レポートの共有

今日繁栄しているマルウェア経済では、ビットコインなどの暗号通貨、Tor などの匿名化ネットワーク（ページ 15 を参照）などにより、良心を持たない人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。検出を避け続けながらさらに収益を上げることができるようにするため、ランサムウェアなどのクライムウェアの運営元は、独自の専門開発チームを雇って資金提供し、新しい亜種と手法を開発しています。

ランサムウェアは、ユーザのファイルを暗号化します。財務ファイルから家族の写真まで、あらゆるものがターゲットとなり、ユーザが「身代金」を支払った後にのみキーを提供します。ランサムウェアは、大企業、学校、個人ユーザまで、あらゆる人をターゲットにしています。

一般にマルウェアは、電子メールやエクスプロイト キットなど多数のベクトルで送信されます。たとえば、エクスプロイト キットである Angler（ページ 11 を参照）は、Cryptowall ペイロードをドロップすることで知られています。Cryptowall は、元の亜種である Cryptolocker の後に現れ、2014 年の中頃に警察による取締りを受けました。

図 8 は、ユーザがランサムウェア TeslaCrypt に遭遇したときに表示される可能性があるメッセージの例を示しています。TeslaCrypt は、Cryptolocker から派生したものであるかのように装います。

図 8. ランサムウェア TeslaCrypt による画面上のメッセージの例

*出典：シスコ セキュリティ リサーチ*

要求される身代金は法外なものではありません。通常は 300 ～ 500 ドルです。なぜそのように控えめな金額になっているのでしょうか。ランサムウェアを導入する攻撃者は、最適な料金を決定するために市場調査を行ってきました。考え方としては、ユーザが支払わなかったり、警察に相談する気にさせるほど身代金を高く設定しないということです。身代金というよりも、迷惑をかけられないための料金に近いものです。そして、ユーザは全額を払い込みます。

シスコは、ほぼすべてのランサムウェア関連のトランザクションが、匿名 Web ネットワークである Tor を通じて行われていることを報告しています（ページ 15 を参照）。攻撃者は、Tor や Invisible Internet Project（I2P）などのチャネルを使用することで、検出されるリスクを低くし、収益性を高めています。I2P は、アプリケーションが偽名でセキュアにメッセージを相互送信できるようにするためのコンピュータ ネットワーク レイヤです。多くのランサムウェアの運営元にも、ウイルス対策プロバイダーからの更新ファイルを監視する開発チームがおり、亜種が検出され、手法を変えるべきタイミングを作成者が知ることができるようになっています。

攻撃者は、暗号通貨であるビットコインを使用して支払いを受けているため、トランザクションを警察が追跡するのはより困難になっています。また、市場で良い評判を維持する、つまり支払いが処理された後にユーザが暗号化されたファイルにアクセスできるようにするという約束を果たすことを知らしめるため、多くのランサムウェアの運営元は、入念なカスタマー サポート体制を確立してきました。

シスコは最近、オンライン ゲームの利用者など、特定のユーザ グループを侵害するように設計された、多数のカスタマイズされた一連の攻撃を確認しました。一部のランサムウェアの作成者は、アイスランド語などのあまり一般的でない言語でも亜種を作成し、これらの言語が主に話されている地域のユーザがランサムウェアのメッセージを無視しないようにしています。

ユーザは、最も価値のあるファイルをバックアップし、隔離（ネットワークから「エア ギャップ」）することで、自身を保護することができます。身代金を支払ってファイルを復号化した後も、システムが危険にさらされている可能性があることを認識する必要があります。ほぼすべてのランサムウェアは複数ベクトルです。マルウェアは別のマルウェアによってドロップされた可能性があります。つまり、システムをクリーンであると見なす前に、初期感染ベクトルを解決する必要があります。

ランサムウェアの傾向の詳細については、Talos グループのブログ投稿『**Cryptowall 3.0: Back to Basics（Cryptowall 3.0：基本に還る）**』[英語] と『**Threat Spotlight: TeslaCrypt—Decrypt It Yourself（脅威のスポットライト：TeslaCrypt - 自分自身で復号化）**』[英語] を参照してください。

### ネットワーク通信を隠すため、サイバー犯罪者は Tor を採用

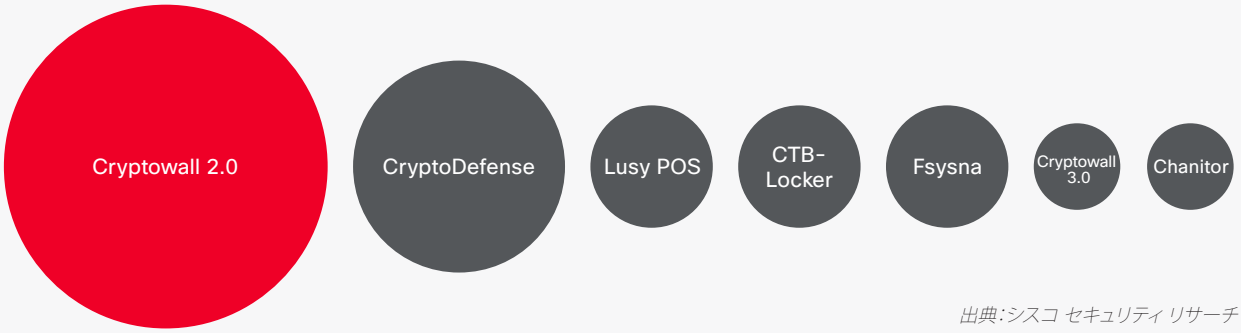
マルウェアの作成者は、検出を回避し、サーバの場所を知られないままにしようとします。これを行うには、多くの攻撃者は匿名 Web ネットワーク Tor を使用して指揮および統制の通信を中継します。

シスコの研究者は、マルウェア ファミリ、特にランサムウェアの変種が Tor トラフィックを生成していた複数のケースを検出しました。Tor は、企業内で正規の目的で使用されることもありますが（たとえばセキュリティ プロフェッショナルによる使用）、その存在は、ネットワーク上にマルウェア トラフィックがあることを示している可能性があります。正規のユーザを引き付ける Tor の特性のいくつかは犯罪者にとっても魅力的です。

ネットワーク内に Tor アクティビティを検出したセキュリティ プロフェッショナルは、この発見を悪意のあるアクティビティの他の兆候（不明な実行可能ファイルのダウンロードやエクスプロイト キット サーバへの接続）と関連付けて、Tor トラフィックが正規のものかどうかを判断する必要があります。

図 9 に示すように、ランサムウェアである Cryptowall 2.0 やいくつかのマルウェア ファミリを導入する攻撃者は Tor のユーザです （「ランサムウェアの進化：革新の事例とハードルの低下」、ページ 13を参照してください）。このデータは、シスコによるカスタマー ネットワークのモニタリングから得られたものであり、2014 年 10 月から 2015 年 5 月の間にマルウェア ファミリ内で Tor が使用された事例を示しています。

図 9. Tor を使用して通信するマルウェア ファミリ




*出典：シスコ セキュリティ リサーチ*

## Microsoft Office マクロがエクスプロイトの起動手段として復活

レポートの共有

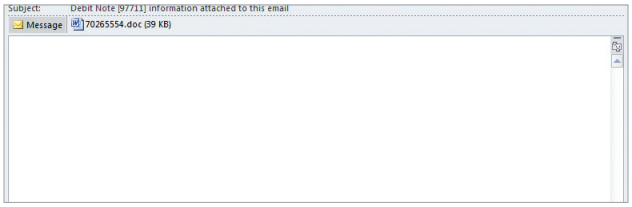
バンキング用のトロイの木馬を送り込むために Microsoft Office マクロを使用するケースが急増していることは、オンライン犯罪が 2 つの傾向に収束していることを示しています。その傾向とは、古いツールまたは脅威ベクトルの再利用のための復活と、脅威を迅速かつ頻繁に変更して、何度も繰り返し行い、検出を回避することです。

これらのトロイの木馬が使用する古いツールは、Microsoft Word などの Microsoft Office 製品のマクロです。これらのマクロは、何年も前に攻撃者がよく利用しましたが、デフォルト設定でオフになったために、人気がなくなりました。しかし、不正な攻撃者は、ソーシャル エンジニアリング技術を使用してユーザがマクロを有効にするように説得することで、新たな手口を追加します。

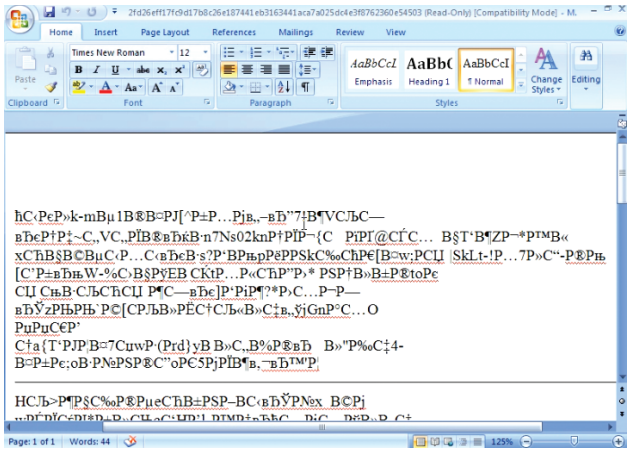
シスコは、トロイの木馬の Dridex が電子メールの添付ファイルとして送信された、最近の 2 つのキャンペーンを調査しました。各電子メールは特定の受信者に送信され、請求書などの重要なドキュメントが含まれていると記されていました。2015 年の途中の時点で、新しい Dridex 関連のキャンペーンが毎日検出されています。

最初のキャンペーン（キャンペーン 1）の電子メールの件名は、添付ファイルが非常に重要なビジネス ドキュメントであると受信者に思わせようとしていましたが、電子メール自体は空白のケースがありました。

### Dridex：キャンペーン 1



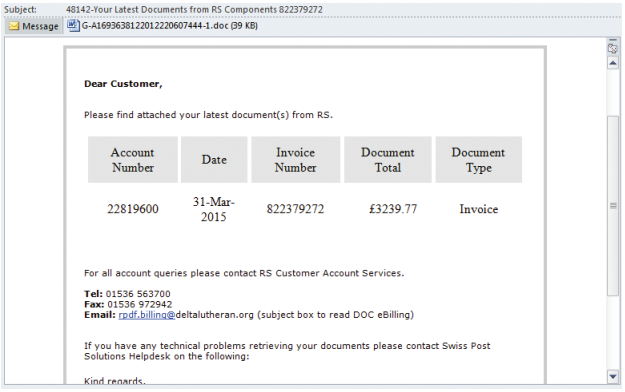

受信者が添付ファイルを開くと、無意味なテキストだらけの Word ドキュメントが表示されました。



分析した第 2 の電子メール キャンペーン（キャンペーン 2）には、正当なものに見えるメッセージが含まれており、特定のアカウントと請求番号が記載され、添付されたドキュメントが請求書であると書かれていました。しかし、受信者が Word の添付ファイルを開くと、キャンペーン 1 のユーザが遭遇した内容と同様に、無意味なテキストが表示されました。

レポートの共有

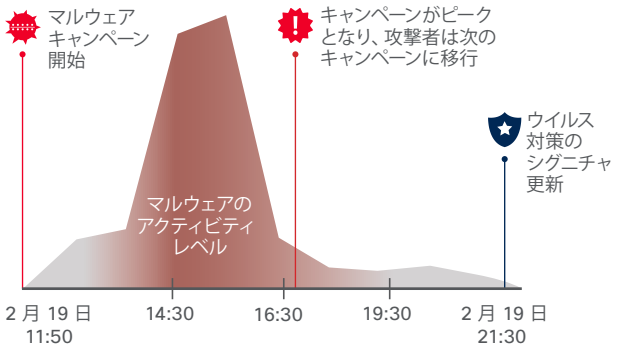
### Dridex：キャンペーン 2




どちらのキャンペーンでも、電子メールの受信者が添付された Word ドキュメントを開くとすぐに、悪意のあるアクティビティが発生しました。裏では、cmd.exe と PowerShell を使用して、ハードコードされた IP アドレスから悪意のある実行可能ファイルがダウンロードされました。確認した一部のキャンペーンでは、マクロを有効にする方法をユーザに知らせる手順が含まれていました。いったんマクロを有効にすると、Dridex は、被害者の銀行口座のログインとパスワードを盗もうとします。

シスコの研究者は、Dridex ペイロードを運ぶスパム キャンペーンは非常に短期間（おそらく数時間）である傾向があり、防御を回避するために頻繁に変異していることに気づきました。ウイルス対策ソリューションは有用なセキュリティ機能を実行しますが、これらの短期間のスパム キャンペーンの検出には適していません。キャンペーンが検出されるまでに、攻撃者は電子メールの内容、ユーザ エージェント、添付ファイル、参照先をすでに変えていました。その後キャンペーンが再度開始されます。これにより、ウイルス対策システムはもう一度新しく検出することを余儀なくされます。図 10 は DyrezaC のマルウェア キャンペーンを示しており、ウイルス対策の更新はキャンペーンが終了した後で行われます。

図 10. DyrezaC はウイルス対策システムよりも速く動作可能




*出典：シスコ セキュリティ リサーチ*

スパム、Microsoft Office マクロ、Dridex を組み合わせるというこのアプローチは、2015 年の前半にサイバー犯罪者の間で流行したものと推測されます。シスコは、このトロイの木馬を送信する、850 件の電子メールと添付された Microsoft Office ファイルのユニーク サンプルを調べました。これは、1 つのスパム キャンペーンのユニーク サンプルとしては比較的多い数です。これらの素早く変異するキャンペーンの作成者は、セキュリティの回避について高度な理解を持っていると思われます。また、これらの脅威への対処がウイルス対策による検出に頼っていることを認識し、確実に検出を避けるようにしています。

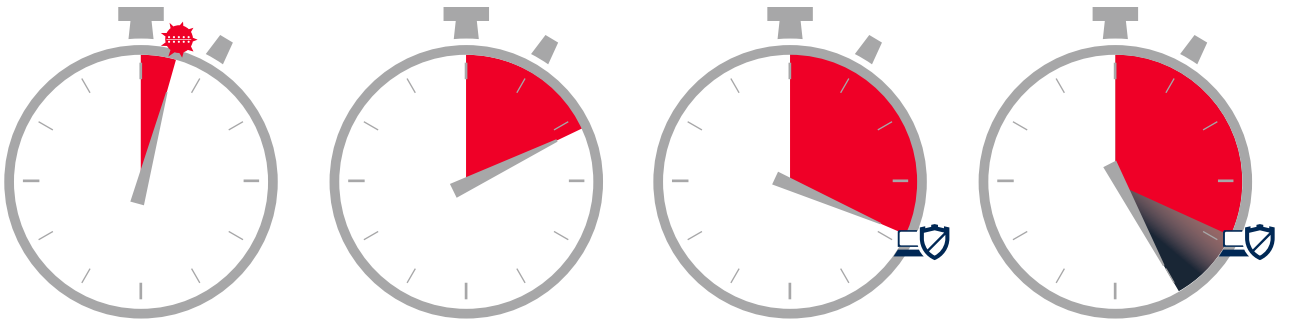
図 11 の例に示す図は、ウイルス対策エンジンが Dridex の脅威を検出し始める前に数時間が経過したことを示しています。キャンペーンは約 5 時間継続したため、ウイルス対策ソリューションは、キャンペーンの最後の部分でしか保護を提供できませんでした。

ウイルス対策ソリューションは、マクロ エクスプロイトを過去のものと見なしている可能性があるため、セキュリティ プロフェッショナルは、これらの脅威からネットワークを保護するための準備ができていない可能性があります。そのような脅威に対する最善の防御は、複数のセキュリティ ソリューションがウイルス対策と連携して動作する多層防御戦略です。たとえば、ウイルス発生フィルタは、疑いのあるメッセージを最大で 12 時間検疫し、ウイルス対策ツールが新しい脅威に追いつくことができるようにします。

トロイの木馬 Dridex と Microsoft Office マクロの詳細については、Talos グループのブログ投稿 **『Threat Spotlight: Spam Served With a Side of Dridex（脅威のスポットライト：Dridex とともに機能するスパム）』** [英語] を参照してください。

図 11. Dridex の検出グラフ、2015 年 3 月、4 月






*出典：シスコ セキュリティ リサーチ*

## Rombertik：データを盗むだけでなく破壊もできるマルウェア

高度なマルウェアの作成者は、セキュリティ システムによって調べられたときにブロックされたり破壊されたりするのを避けるために、動作を停止するようにマルウェアを設計します。これに対応してセキュリティ研究者は、攻撃者が検出を逃れ続けることが難しくなるような、新たな静的、動的、自動化された分析ツールを常に探し求めています。

この目標に向けて、シスコは最近 Rombertik をリバースエンジニアリングしました。Rombertik は複雑なマルウェアであり、リバース エンジニアリングの際に行われるような、バイナリを改変しようとする試みを検出するものと考えられます。Rombertik は、そのホスト コンピュータのマスター ブート レコード（MBR）を破壊しようとします。それが不可能な場合は、ユーザのホーム ディレクトリにあるファイルの破壊を試みます。その活動から注意をそらそうとするマルウェアとは異なり、Rombertik は、他のものよりも目立つように設計されているようです。リバースエンジニアリングは、シスコなどの脅威研究者が、回避機能を含むマルウェアの動作を理解するために使用する、きわめて重要な手法です。

Rombertik の目的は、ユーザの Web ブラウザに接続して機密性の高いユーザ情報を取得し、攻撃者によって制御されているサーバに送信することです。この点では、Rombertik は Dyre と呼ばれるマルウェアに似ています。[2]ただし、Dyre は銀行のログイン情報を盗むために存在しているのに対し、Rombertik はあらゆる種類のユーザ データを無差別に集めているように見えます。

図 12. Rombertik 独自の分析対策と悪意のある動作の組み合わせ

レポートの共有

出典：シスコ セキュリティ リサーチ

Rombertik は、ソーシャル エンジニアリングを使用し、受信者にマルウェアが組み込まれた添付ファイルをダウンロードして解凍するように促すスパムやフィッシング メッセージを通じて、ユーザのシステムに足がかりを得ます。ユーザが解凍したファイルは PDF のように見えますが、実際には、システムの侵害を開始するスクリーンセーバーの実行可能ファイルです。図 12 に示すように、自身が変更されていることを検出した Rombertik は、システムの MBR を破壊してコンピュータを再起動しようとします。これによりコンピュータは動作不能になります。

### 今日のマルウェアにおける高度な分析対策ツール

Rombertik は、マルウェアの世界に起きようとしていることの先駆者かもしれません。というのは、マルウェアの作成者は、仲間が成功した戦略を素早く取り入れるからです。シスコの研究者が発見したように、Rombertik には、不明化と破壊を狙ったいくつもの機能が巧妙に組み込まれています。たとえば、Rombertik には必要以上の「ゴミ」のコードが含まれているため、セキュリティ分析者はマルウェアの確認と分析により多くの時間を費やすことを強いられ、すべての機能を調べるための時間が無くなります。

検出を回避し、サンドボックスを強制的にタイムアウトさせてから悪意のあるペイロードを実行するために、Rombertik は独特のアプローチを採用しています。通常、マルウェアは、タイムアウトを強制するため、サンドボックス内では「スリープ」状態になります。しかし、セキュリティ分析ツールが、「スリープ」状態にあるプロセスをより効果的に検出できるようになると、マルウェアの作成者は新しい戦略を必要としました。

Rombertik の場合、このマルウェアは、メモリにランダムなデータのバイトを 96 億回書き込みます。これはアプリケーション トレース ツールとサンドボックスの両方に影響を与えます。サンドボックスは、アプリケーションが実際にスリープしていないことから、それが意図的に停止していることを判定できない場合があります。また、96 億回の書き込み命令をすべて記録するには非常に時間がかかり、どちらのタイプのツールでも分析が複雑になります。

Rombertik には、分析またはリバースエンジニアリングされた場合に、不明化のためのそのような手法が多数使用されていますが、その最終的な変更対策手法は、重大な損害を引き起こすことが可能であるということです。分析用に変更されていることを検出したマルウェアは、マシンの MBR を上書きしようとします。MBR を上書きするアクセス許可が得られない場合は、ユーザのホーム フォルダ内のファイルをすべて破棄します。再起動したマシンは動作不能になります。

Rombertik がすべての変更対策チェックに合格すると、最終的にその主な作業を開始します。それは、ユーザがブラウザに入力したすべてのデータを盗み、その情報をサーバに転送することです。

### Rombertik：セキュリティ防御ベンダーのハードルを引き上げる

Rombertik の驚くような特徴は、その分析を回避するための高度な手法と、それが動作しているマシンのオペレーティング システム ソフトウェアに損害を与える能力です。このアプローチは、このようなマルウェアと将来確実に衝突するであろうセキュリティ防御ベンダーにとって、ハードルを引き上げます。他のマルウェア作成者が、Rombertik の戦術を自分のものとして使うだけでなく、より有害なものにすることは確実です。

優れたセキュリティ対策は、ユーザの保護に役立ちますが、不明な送信元からの添付ファイルをクリックしないようにユーザを教育することも有効です。しかし、Rombertik のように巧妙に作られた危険なマルウェアの脅威に対し、攻撃前、攻撃中、攻撃後の連続する攻撃全体を対象とした多層防御アプローチも必要になります。

Rombertik マルウェアの詳細な分析については、Talos グループのブログ投稿**『Threat Spotlight: Rombertik – Gazing Past the Smoke, Mirrors, and Trapdoors（脅威のスポットライト：Rombertik - スモーク、ミラー、トラップドアを超えて見る）』**[英語] を参照してください。

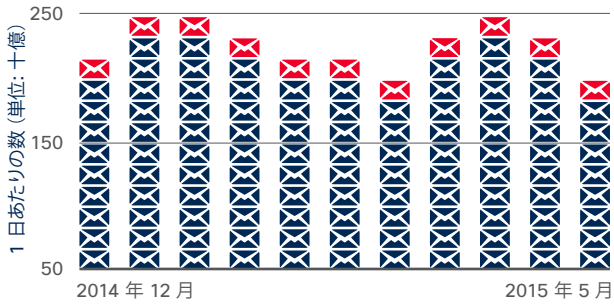
2 『Threat Spotlight: Dyre/Dyreza: An Analysis to Discover the DGA（脅威のスポットライト：Dyre/Dyreza：DGA 検出のための分析）』、シスコ セキュリティ ブログ、2015 年 3 月 30 日、http://blogs.cisco.com/security/talos/threat-spotlight-dyre。

## スパム量は一定

攻撃者がネットワーク防御を破るためのより高度な方法を開発する中で、スパムとフィッシングの電子メールは、これらの攻撃において引き続き大きな役割を果たしています。ただし、図 13 に示すように、世界中のスパムの量は比較的一定しています。

図 14 に示すように、国ごとの分析によれば、スパムの量は、米国、中国、ロシア連邦で増加していますが、他の地域では比較的一定です。シスコでは、これらの変化を、根本にあるスパマー ネットワークの相対的な活動の変動が原因であると考えています。

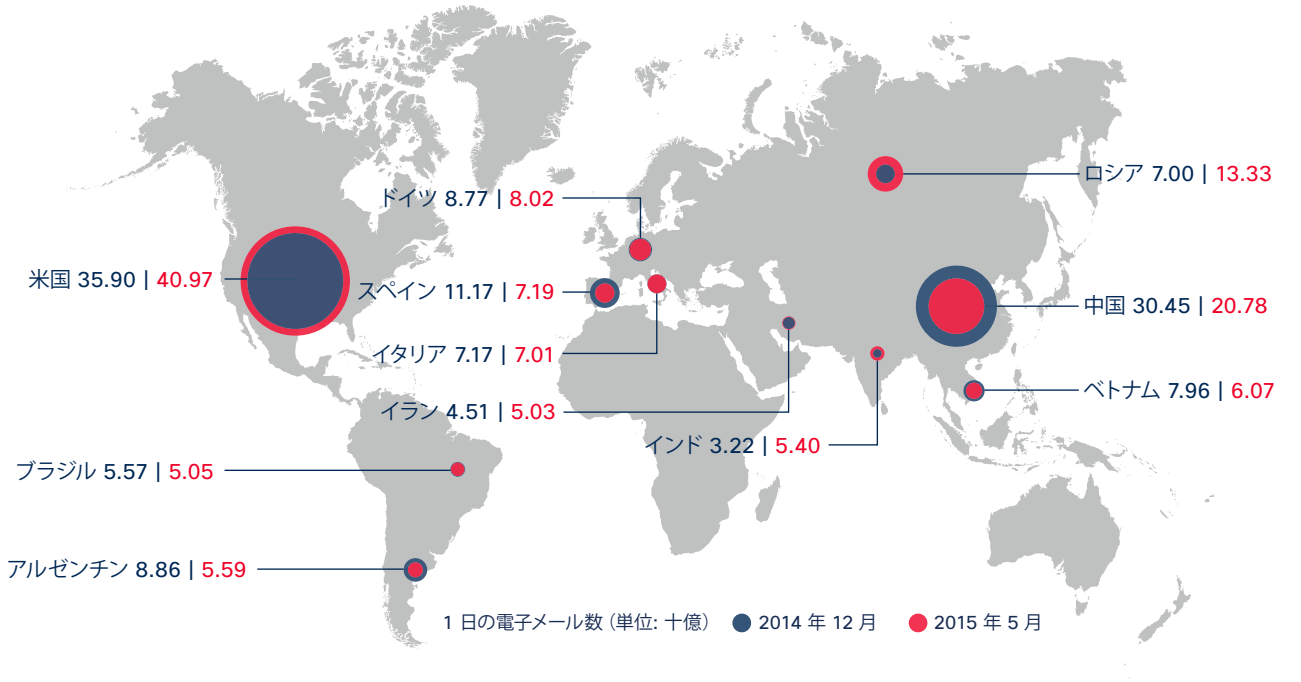
図 13. スパム量は一定




*出典:シスコ セキュリティ リサーチ*

図 14. 国別のスパム件数

レポートの共有




*出典:シスコ セキュリティ リサーチ*

## 脅威と脆弱性：エクスプロイトがよくあるコーディング エラーを悪用

2015 年前半の最も一般的な脆弱性を調べると、同じ種類のエラーが毎年現れていることがわかります。たとえば、図 15 に示すように、バッファ エラーは、National Vulnerability Database（全国脆弱性データベース）（https://nvd.nist.gov/cwe.cfm）で定義されている Common Weakness Enumeration（CWE）の脅威カテゴリ リストの先頭に復帰しています。

バッファ エラー、入力検証、リソース管理エラーは、図 15 の最も頻繁な 3 つの CWE ですが、長年にわたり犯罪者によって悪用されている 5 つの最も一般的なコーディング エラーに含まれています。ベンダーが CWE リストを認識していると仮定すると、これらのエラーはなぜそのように定期的に発生し続けるのでしょうか。

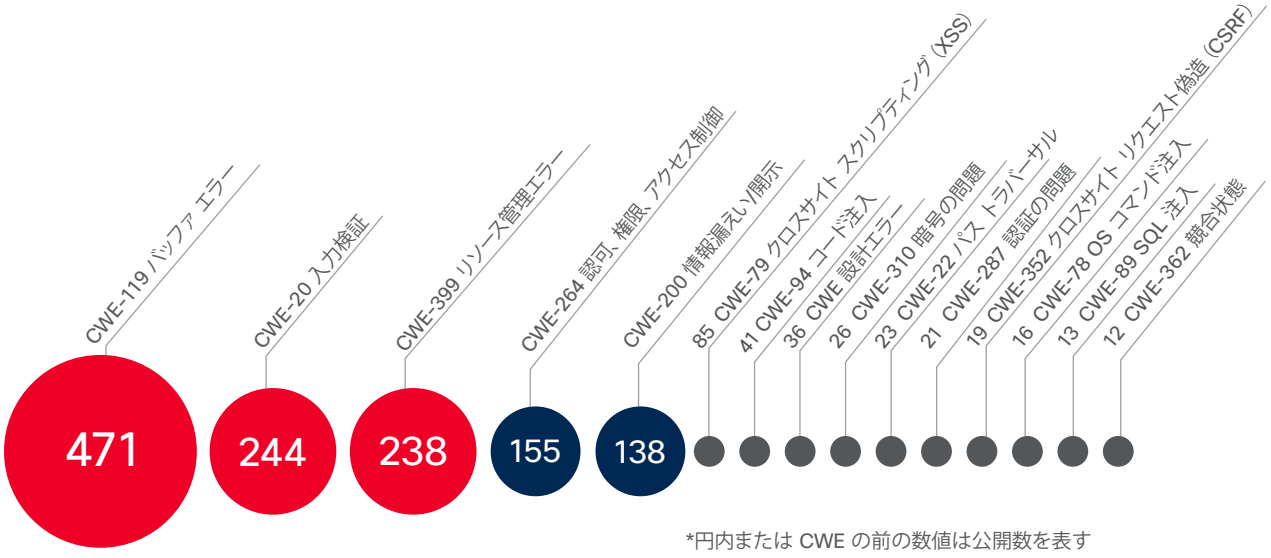
問題は、セキュアな開発ライフサイクルに対する注意が十分に払われていないことにあります。セキュリティ対策と脆弱性テストは、製品を開発する際に組み込まれている必要があります。しかし、ベンダーは、製品が市場に出回るのを待ってからその脆弱性に対処しています。

ベンダーは、開発ライフサイクルにおけるセキュリティに重点を置かない限り、脆弱性を検出、修正、報告するための後追い作業に時間と資金を費やし続けることになります。さらに、セキュリティ ベンダーは、自身のソリューションを信頼でき安全なものにするためにあらゆる努力を行っていることを顧客に納得してもらう必要があります。この場合は、脆弱性テストを製品開発の不可欠な構成要素にすることです。

### サードパーティの脆弱性

Transport Layer Security（TLS）の扱いにおけるセキュリティの欠陥である Heartbleed が 2014 年 4 月に公開されてから、サードパーティ ソフトウェアの脆弱性が、攻撃者を排除しようとする企業にとってやっかいな問題となりました。Heartbleed は、特にオープン ソース ソリューションが普及する中で、サードパーティ ソフトウェア（TPS）の脆弱性を入念に調査するきっかけとなりました。

図 15. 最も一般的な CWE の脆弱性



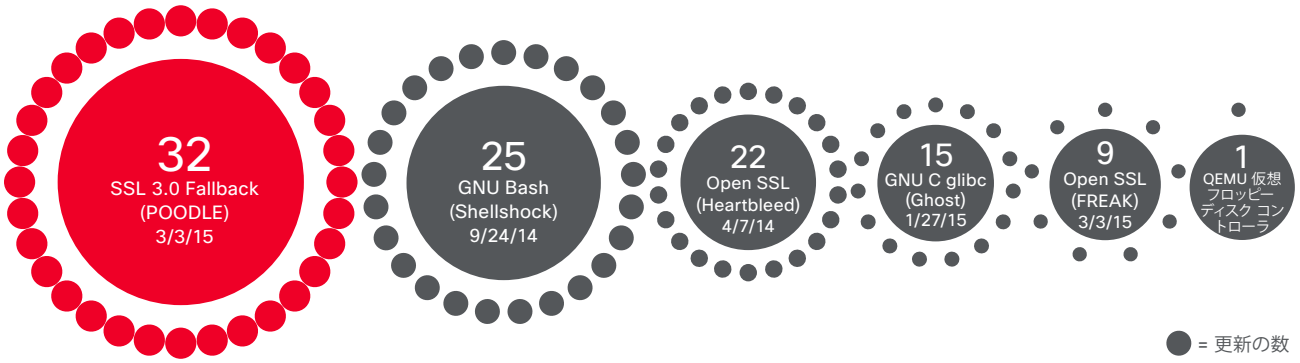

*円内または CWE の前の数値は公開数を表す

*出典：シスコ セキュリティ リサーチ*

レポートの共有

図 16. オープン ソースの脆弱性






*出典:シスコ セキュリティ リサーチ*

図 16 は、シスコが 2015 年前半に追跡した、最も一般的なオープン ソースの脆弱性のうちの 6 つを示しています（ベンダーによる対応の詳しいタイムラインについては、上記の脆弱性をクリックし、アラート履歴まで下にスクロールしてください）。

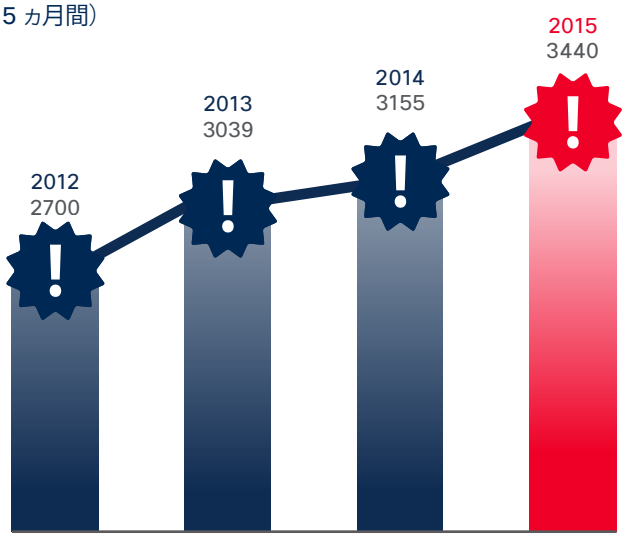
オープン ソースの脆弱性は、固有の課題を投げかけています。それは、脆弱性をなくすには、多くのベンダーの連係が必要だということです。オープン ソース ソリューションを保守している開発者コミュニティは、修正またはパッチを迅速に提供できるかもしれませんが、修正は製品のすべてのバージョンに組み込まれる必要があります。

良いニュースは、オープン ソースの脆弱性に対する認識が高まることで、セキュリティ コミュニティがより迅速に脆弱性に対処していることです。たとえば、仮想化システムのためのオープン ソース コードに影響を与える脆弱性である VENOM（Virtualized Environment Neglected Operations Manipulation）が最初に明らかになったとき、各ベンダーは、脆弱性が公表される前にパッチをリリースしました。

シスコを含む複数の大手テクノロジー企業による OpenSSL への最近の投資は、OpenSSL インフラストラクチャの改善に役立っています。投資は、The Linux Foundation への寄付の形をとっています。こうした投資は、セキュリティ研究者がコード レビューを実施するのに役立っています。これは、オープン ソース ソリューションの修正とパッチの特定に役立ちます。[3]

多くの企業がオープン ソース ソフトウェアを使用している中で、セキュリティ プロフェッショナルは、オープン ソースが自組織のどこでどのように使用され、オープン ソース パッケージやライブラリが最新であるかどうかについても詳しく理解する必要があります。これは、先に進む際に、ソフトウェア サプライ チェーン管理がますます重要になることを意味します。

図 17. 年間累積アラート総数（2012 ～ 2015 年の最初の 5 ヵ月間）




*出典:シスコ セキュリティ リサーチ*

レポートの共有

3 『Cisco, Linux Foundation, and OpenSSL（シスコ、Linux の基盤と OpenSSL）』[英語]、シスコ セキュリティ ブログ、2014 年 4 月 25 日: http://blogs.cisco.com/security/cisco-linux-foundation-and-openssl。

2015 年の最初の 5 ヵ月間についての年間累積 IntelliShield アラートの合計は、2014 年の同じ期間と比べて若干増加しています（表 1）。シスコが以前言及したように、合計アラート数が増加し続けていることは、ベンダーがセキュリティ テストと自身の脆弱性の特定および修正に注力していることによる当然の結果です。

表 1. アラート アクティビティ レベル

| | 更新 | 新規 | 合計 |
|---|---|---|---|
| 1 月 | 211 | 359 | 570 |
| 2 月 | 255 | 379 | 634 |
| 3 月 | 285 | 471 | 756 |
| 4 月 | 321 | 450 | 771 |
| 5 月 | 237 | 472 | 709 |
| | **1309** | **2131** | **3440** |
| **2014 年 1 ～ 5 月の** | | **合計アラート数：3155** | |

*出典：シスコ セキュリティ リサーチ*

表 1 は、報告されたアラートと更新済みアラートのアクティビティを示しています。2015 年 5 月には、アラートの総数は 2014 年 5 月と比べて 9 % 増加しています。セキュリティ ベンダーと研究者は、より多くの新しいアラートを確認していますが、更新済みアラートの数は減っています。そのため、各組織は、パッチ管理への取り組みを強化する必要があります。

表 2 は、共通脆弱性評価システム（CVSS）による、最も広く悪用されている脆弱性の一部を示しています。米国国立標準技術研究所（NIST）の全国脆弱性データベース（NVD）は、IT の脆弱性の特徴と影響を開示して、CVSS に対応するためのフレームワークを提供します。

CVSS の表の「Urgency（深刻度）」スコアは、これらの脆弱性が活発に悪用されているかどうかを示しています。エクスプロイト対象の製品リストを見ると、これらの製品のうちのどれを使用しており、モニタとパッチ適用が必要なのはどれかも判断できます。

レポートの共有

表 2. 最も悪用された脆弱性

| アラート ID | 見出し | 緊急度 | 信頼性 | 重大度 | CVSS ベース | CVSS 一時 |
|---|---|---|---|---|---|---|
| 35845 | GNU Bash の環境変数文字列値の処理 | ●●●●○ | ●●●●● | ●●●●○ | 10.0 | 9.0 |
| 35816 | GNU Bash の環境変数コマンド インジェクションの脆弱性 | ●●●●○ | ●●●●● | ●●●●○ | 10.0 | 8.6 |
| 37181 | GNU glibc の gethost 関数呼び出しのバッファ オーバーフローの脆弱性 | ●●○○○ | ●●●●● | ●●●●○ | 10.0 | 7.8 |
| 37318 | Adobe Flash Player リモート コード実行に関する脆弱性 | ●●○○○ | ●●●●● | ●●●●○ | 9.3 | 7.7 |
| 37848 | Elasticsearch Groovy スクリプト エンジンのサンドボックス バイパス | ●●○○○ | ●●●●● | ●●●●○ | 9.3 | 7.7 |
| 37123 | Adobe Flash Player の解放済みメモリ使用で任意のコードを実行 | ●●○○○ | ●●●●● | ●●●●○ | 9.3 | 7.7 |
| 36849 | Network Time Protocol デーモンのスタック バッファ オーバーフローの脆弱性 | ●●○○○ | ●●●●● | ●●●○○ | 7.5 | 5.5 |
| 37181 | GNU glibc の gethost 関数呼び出しのバッファ オーバーフローの脆弱性 | ●●○○○ | ●●●●● | ●●●●○ | 10.0 | 7.8 |
| 36956 | OpenSSL RSA 一時キーの暗号化ダウングレードの脆弱性（FREAK） | ●●○○○ | ●●●●● | ●●○○○ | 5.0 | 4.1 |

*出典：シスコ セキュリティ リサーチ*

## Java を使用したエクスプロイトは減少

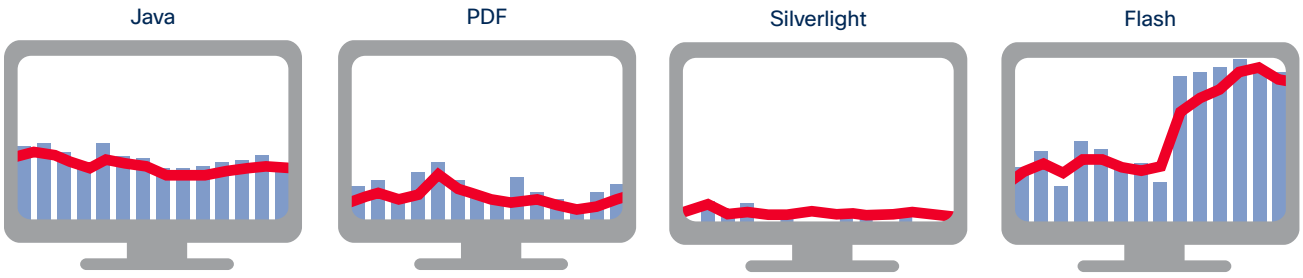
2015 年シスコ年次セキュリティ レポート[4]で取り上げ、解説した傾向が続き、Java 関連のエクスプロイトは、2015 年の前半は減少しました。Java は、オンライン犯罪者が好む攻撃ベクトルでしたが、セキュリティの向上とパッチ適用の強化により、攻撃者を遠ざけてきました。2013 年以降、Java のゼロデイ エクスプロイトは公開されていません。

Oracle は、署名されていないアプレットの段階的な廃止など、Java のセキュリティを高めるためにいくつかの方策を講じてきました。最新バージョンである Java 8 には、以前のリリースよりも厳格な制御が含まれています。Java を有効にするよう求めるダイアログボックスなど、ユーザからの入力が必要なため、悪用はより困難です。

Oracle は、2015 年 4 月に、Java 7 のサポートを終了することを発表しました。[5]残念ながら、ベンダーが製品の特定のバージョンのサポートを終了しても、企業が新しいバージョンをすぐに全面導入することはありません。この時間的な遅れにより、犯罪者がサポートされなくなったバージョンの脆弱性を悪用する機会が生まれます。今後企業が Java 7 から Java 8 に移行する中で、Java エクスプロイトの数が増加する可能性があります。

図 18. 最も一般的なマルウェア ベクトル

レポートの共有




*出典：シスコ セキュリティ リサーチ*

図 18 は、2015 年前半の Java、PDF、Flash のエクスプロイトのログ量を示しています。PDF のエクスプロイトは月ごとに異なりますが、通常、Flash のエクスプロイトほど一般的ではありません。Flash はエクスプロイト キットの開発者が好むツールであるため、上のログ量グラフでの存在は、Angler などのエクスプロイト キットが関係する犯罪活動の拡散に直接結びつけることができます（ページ 10 を参照）。さらに、Flash、PDF、Java に基づくエクスプロイトと比べて、Silverlight のエクスプロイトの量はごくわずかです。

4 『2015 年シスコ年次セキュリティ レポート』（2015 年 1 月）：http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html。

5 『Oracle to End Publicly Available Security Fixes for Java 7 This Month』、Paul Krill、*InfoWorld*、2015 年 4 月 15 日：http://www.infoworld.com/article/2909685/application-development/oracle-cutting-publicly-available-security-fixes-for-java-7-this-month [英語]。

### マルウェア作成者が採用する検出と回避の手法

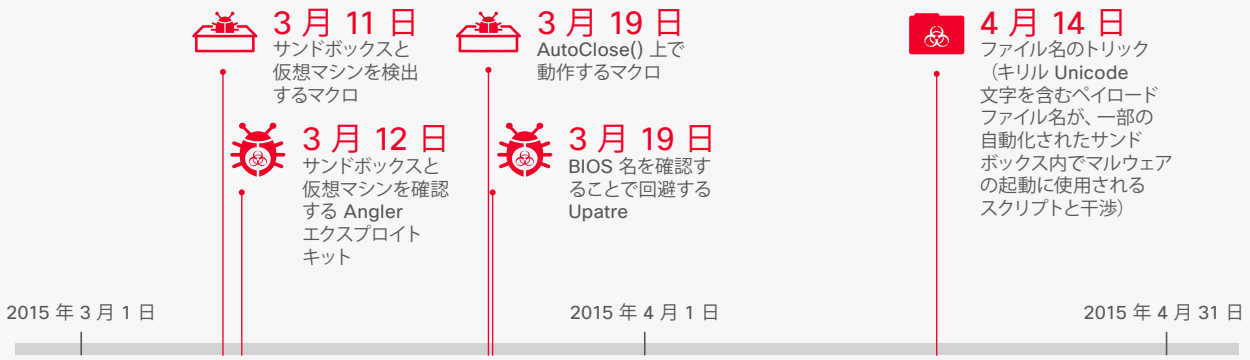
オンライン犯罪者は、セキュリティ研究者やテクノロジー ソリューションから自身の活動を巧妙に隠すようになりました。たとえば、研究者がマルウェアを起動してその活動を記録するために使用するサンドボックスなど、従来の制御を回避しようとするマルウェアを作成します。

シスコが確認したケースでは、そのようなサンドボックス活動を検出したマルウェアは悪意のある活動を実行しませんでした。この戦略は、Angler エクスプロイト キットの亜種、Upatre マルウェアの亜種、悪意のある Microsoft Office ドキュメントで見られました。

このような回避戦略を採るマルウェアから防御するには、多層防御アプローチを採用する必要があります。このアプローチには、マルウェアが最初の防御線をすり抜けた後に、レトロスペクティブによってマルウェアをスキャンし識別するための機能が含まれているのが理想です。

#### 最近のサンドボックス検出

サンドボックス検出は、マルウェア作成者にとって新しい戦略ではありませんが、2015 年の 3 ～ 4 月の間に以下の事例を確認したシスコの研究者によれば、ありふれたものになりつつあります。



## マルウェアに遭遇する業界別リスク：攻撃を受けない業界はない

シスコでは、正確な調査のために、Web マルウェアに遭遇する危険性の高い業種の追跡方法を改善・簡素化してきました。シスコは、Cisco® Cloud Web Security を利用するすべての組織の遭遇率の中央値と、このサービスを利用している特定業界におけるすべての企業の遭遇率の中央値を比較することをやめました。今後は、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比較します。

図 19 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、25 の主要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。

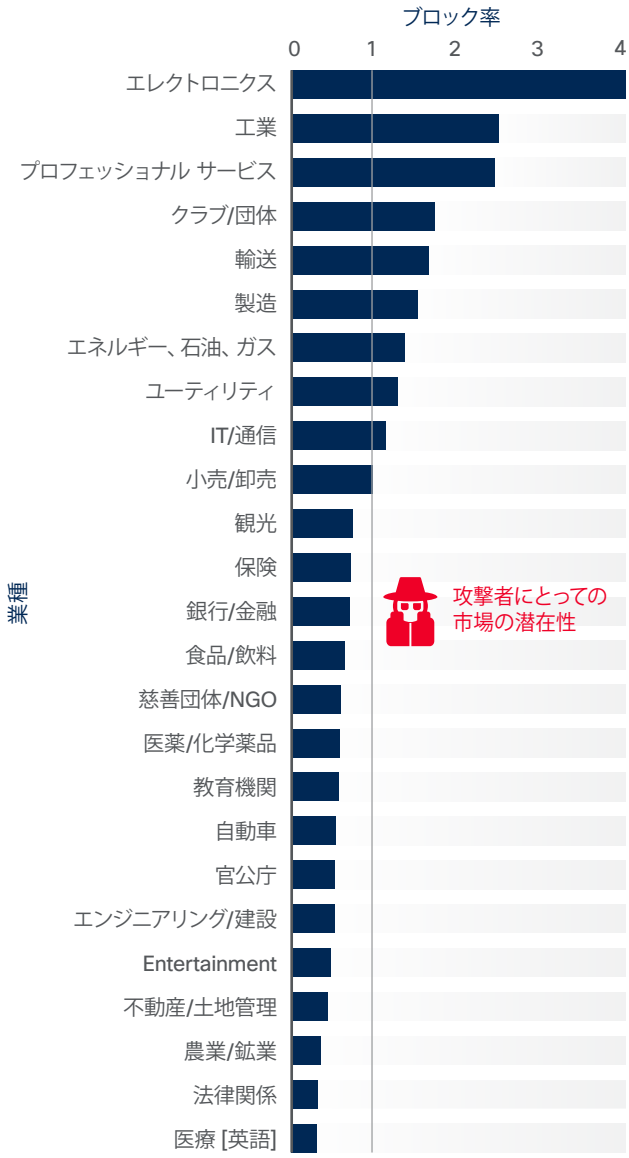
たとえば、小売りおよび卸売業界のブロック率は、その業界で観察されたトラフィック量に比例しています。

シスコのお客様のブロック率を調べたところ、エレクトロニクス業界は、追跡した 25 の業界の中で、ブロックした攻撃が最も多かったことがわかりました。シスコでは、エレクトロニクス業界の高いブロック率が、Android スパイウェアの拡散によるものだと考えています。

図 19 に示すように、ほとんどの業界は、通常のネットワーク トラフィックに対する攻撃の比率が「通常」レベル（1.0 のライン）にあります。しかし、現在 1.0 のラインを超えている業界が、攻撃に対して非常に脆弱であると考えるのは誤解を招く恐れがあります。というのは、特にこの分析では 2015 年の前半のみを対象としているためです。

さらに、ターゲットになるという点において、どの業界も、他の業界より「安全である」と考えるべきではありません。あらゆる業界のあらゆる組織は脆弱であり、攻撃されると仮定すべきであり、多層的な防御戦略を適宜実装する必要があります。

図 19. 確認されたトラフィック量と比べた業種ごとのブロック率




*出典：シスコ セキュリティ リサーチ*

レポートの共有

### ブロック アクティビティ：地域別の概要

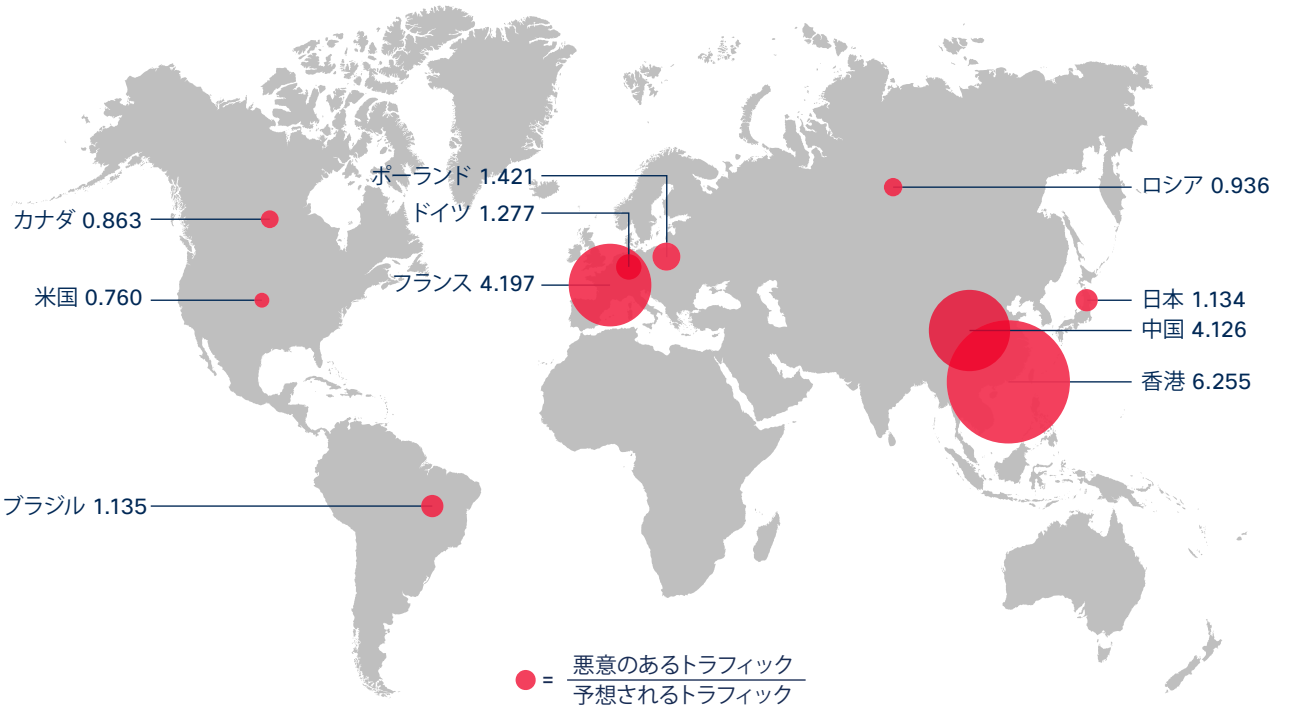
シスコの研究者は、マルウェア ベースのブロックアクティビティの元となっている国と地域も調べました（図 20）。調査対象の国は、インターネット トラフィックの量に基づいて選ばれました。ブロック率 1.0 は、観察されたブロック数がネットワークの規模に比例していることを示します。

マルウェアは、脆弱性のあるデバイスに足がかりを得ます。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。大量のインターネット ボリュームを処理する、大規模で商業的に存続可能なネットワークの存在が、高いブロック アクティビティのもう 1 つの要因です。

図 20 は、サーバがホストされている場所に関係しています。この図は、悪意のある Web アクティビティのパターンがここに示された国や地域に起因するということを示しているわけではありません。リスト上で 1 位となっている香港は、脆弱な Web サーバが高い割合で確認される地域の例です。フランスでホストされている少数のネットワークが、レポート期間の途中まで拡散に参加しており、そのことで統計データが予想よりも高くなっています。

図 20. 国または地域別 Web ブロック

レポートの共有




*出典：シスコ セキュリティ リサーチ*

### Web ベースの攻撃の種類

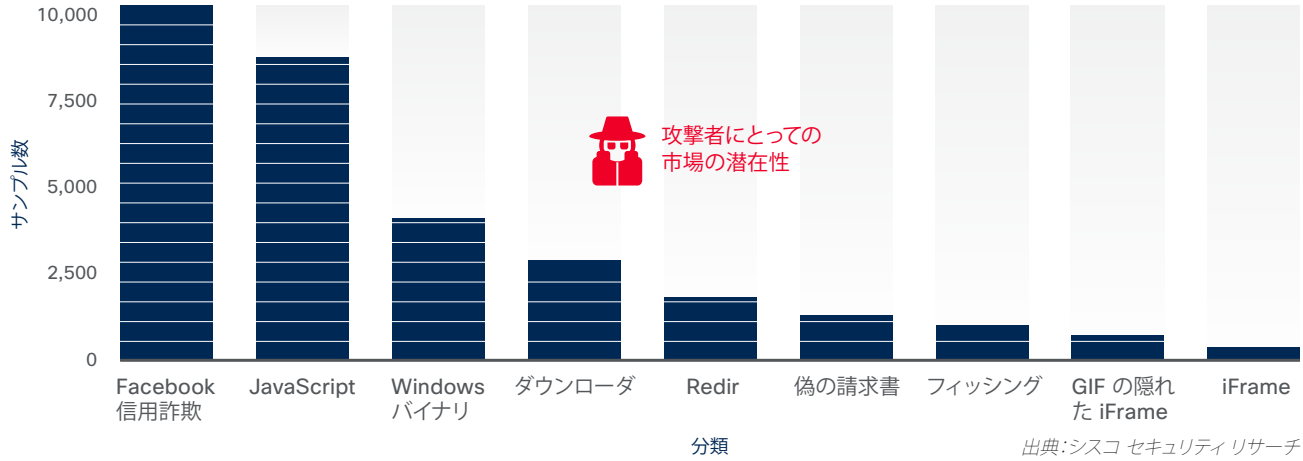
図 21 と図 22 は、攻撃者が組織のネットワークにアクセスするために使用するさまざまな手法を示しています。図 21 は、Facebook 信用詐欺や悪意のあるリダイレクトなど、最も一般的な方法を示しています。

図 22 は、調べたブラインド サンプル中に観察された、数の少ない攻撃方法を示しています。「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。数の少ない攻撃方法と、それに関連するマルウェアは、新たに現れた脅威や、ターゲットを絞り込んだキャンペーンである可能性があります。

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。

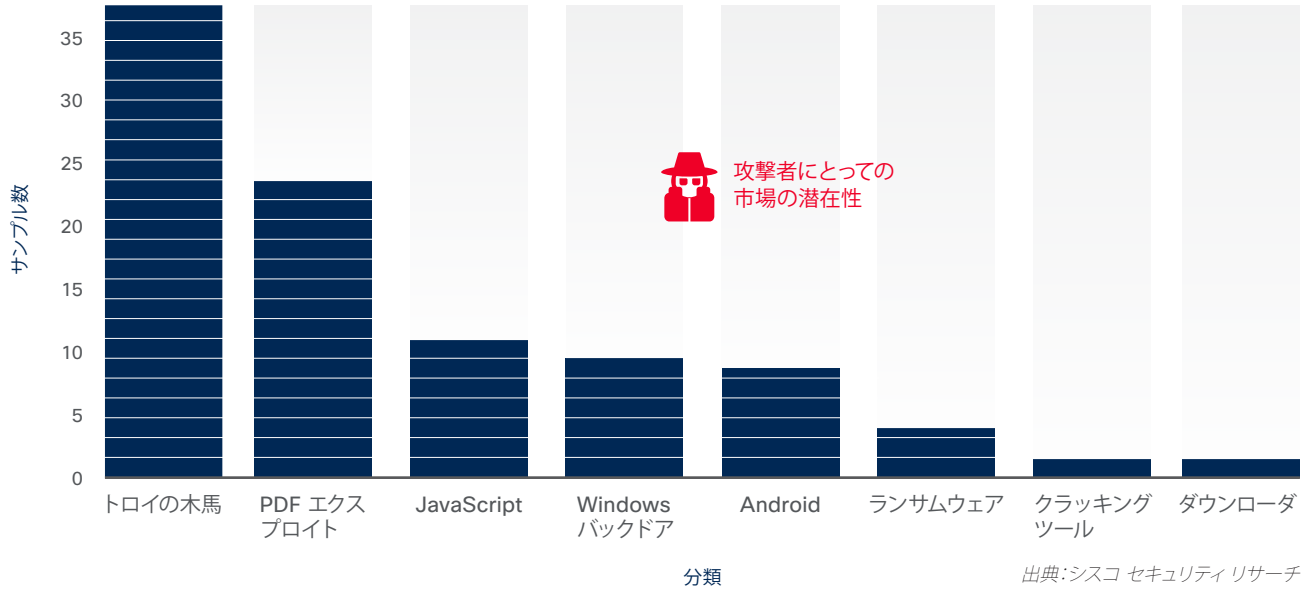
図 21. 最も広く確認された方法

レポートの共有




出典：シスコ セキュリティ リサーチ

図 22. 確認された少量の方法の例




出典：シスコ セキュリティ リサーチ

## マルバタイジングの最新情報：検出を回避し攻撃の効率を高めるための Web ベース脅威の変異が拡散

2015 年シスコ年次セキュリティ レポート[6]で報告したように、シスコは、2014 年にマルウェアや不要なアプリケーションを配布するための手段として、Web ブラウザのアドオンからマルバタイジングを使用する、非常に高度なボットネットに似た Web ベースの脅威の詳細に分析しました。マルウェア ファミリには、Adware MultiPlug という明確なシグニチャがあります。ブラウザ拡張は、PDF ツールやビデオ プレーヤーなど、一見便利に見えて不要なアプリケーションにバンドルされています。

これらの不要なアプリケーションと、それに付属するバンドルソフトウェアをインストールすると感染します。多くの場合、これらは、ユーザが本質的に信頼したり無害であると見なすブラウザ アドオンです。ユーザ情報、特にユーザが参照している内部または外部の Web ページ（ユーザ証明書ではありません）が、インストールされたこれらのブラウザ拡張によって裏で取得されます。

マルウェアの配布は、PPI（Pay-Per-Install）の収益スキームに従っています。この方式では、パブリッシャは元のアプリケーションにバンドルされているソフトウェアがインストールされるたびに支払いを受けます。これにより、対象ホストへの影響を抑え、非常に多くのユーザから長期にわたり収益を得るように意図的に設計されたマルウェアが流行することになります。

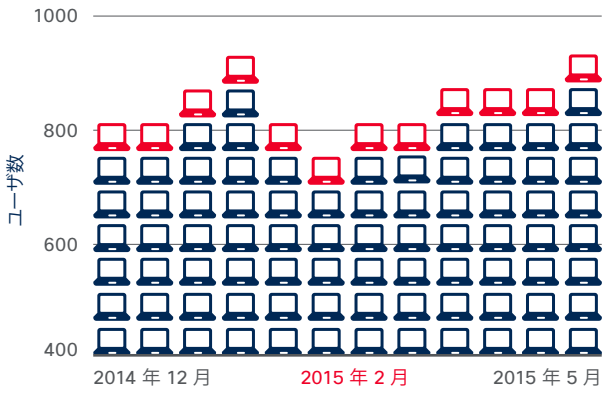
### 一般的な Web トラフィックでの偽装

シスコはこの脅威を 1 年以上にわたってモニタしてきました。この脅威は、検出されないように、常に変化していることが分かります。この脅威があるドメイン名を使用する平均期間は 3 ヵ月であり、アドオン名も絶えず変化します。シスコ 2015 年度セキュリティ レポートで報告したように、シスコはこれまで 4000 を超える異なるアドオン名と、この脅威に関連する 500 を超えるドメインを検出してきました。

2015 年 1 月には、研究者は脅威が変異したことを確認しました。特に、この脅威は、一般的な Web トラフィックに自身を隠すことができるよう、検出を避けるためにその URL 符号化方式を捨てました。この戦略の移行により、この脅威のユーザを侵害する有効性が高まったように思われます。

シスコは、この新しいパターンに関連するトラフィックを 2014 年 8 月までさかのぼって追跡しましたが、2014 年 12 月から 2015 年 1 月の期間のトラフィック量により人目を引くようになっただけでした。図 23 に示すように、この脅威に関連して影響を受けるユーザ数は、2 月以降増加傾向にあります。

図 23. 影響を受けたユーザの数（月別）、2014 年 12 月～2015 年 5 月




*出典：シスコ セキュリティ リサーチ*

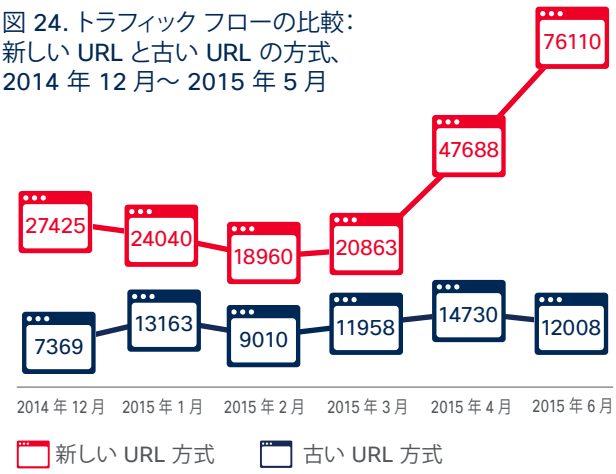
この調査の詳細については、Talos グループのブログ投稿『**Bad Browser Plug-Ins Gone Wild: Malvertising, Data Exfiltration, and Malware, Oh My!（不正なブラウザ、プラグインの狂乱：マルバタイジング、データ流出、マルウェア）**』[英語] を参照してください。

レポートの共有

6 『2015 年シスコ年次セキュリティ レポート』(2015 年 1 月)：http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html。

図 24 は、新しい URL 方式に関連するトラフィック フローの数が、特に 2015 年 3 月以降、古い方式を大幅に上回っていることを示しています。

図 24. トラフィック フローの比較：新しい URL と古い URL の方式、2014 年 12 月～ 2015 年 5 月




*出典：シスコ セキュリティ リサーチ*

## 検出時間：定義

シスコは、「検出時間」（TTD）を、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 25 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。

レトロスペクティブの数は、2014 年 12 月以降増加しています。この傾向は、マルウェア作成者が素早く革新し、常にセキュリティ ベンダーの一歩先にいることのもう 1 つの指標です。しかし、同時に、シスコによる脅威検出の TTD の中央値は低下しています。

2014 年 12 月時点では、分析によって不明なファイルが脅威であることがわかるまでの TTD の中央値は、約 2 日（50 時間）でした。検出時間の現在の業界標準は 100 ～ 200 日であり、今日のマルウェア作成者による素早いイノベーションを考えると、許容できないレベルです。

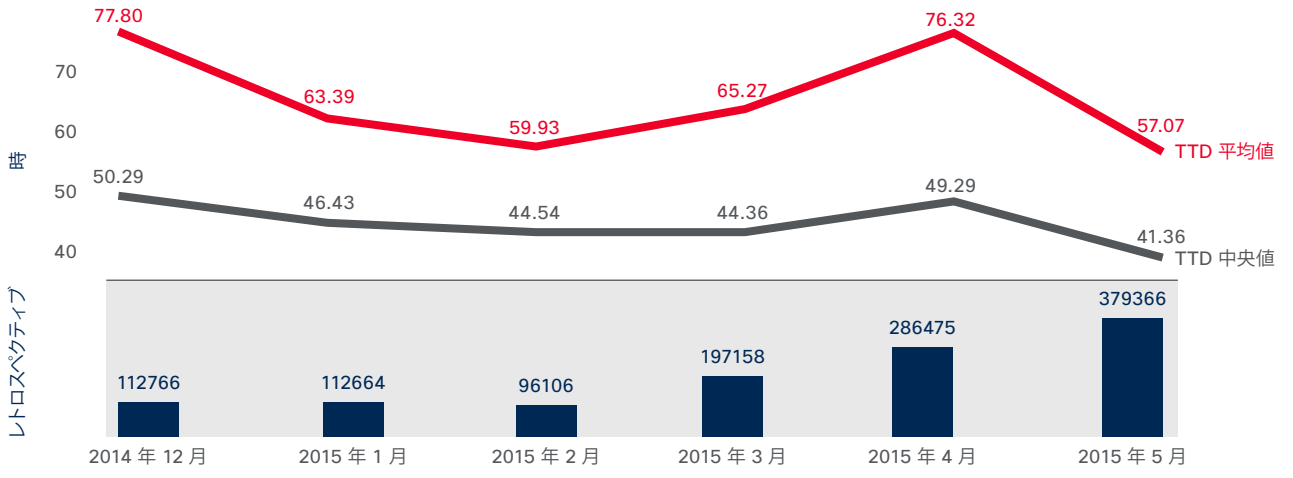
シスコは、レトロスペクティブの最近の増加傾向が、回避行動（「マルウェア作成者が採用する検出と回避の手法」、ページ 25）と、Angler および Nuclear エクスプロイト キットによる新しい Flash エクスプロイトのペイロード送信成功（ページ 9 を参照）に起因すると考えています。

1 月から 3 月まで TTD の中央値はほぼ同じ（44 ～ 46 時間）ですが、若干低下傾向にありました。4 月には、49 時間に微増しました。

しかし、5 月末までに、シスコの TTD は約 41 時間に短縮されました。この改善は、回避的ではあるものの斬新ではない、Cryptowall などの一般的なマルウェアを迅速に識別できることが 1 つの要因になっています。

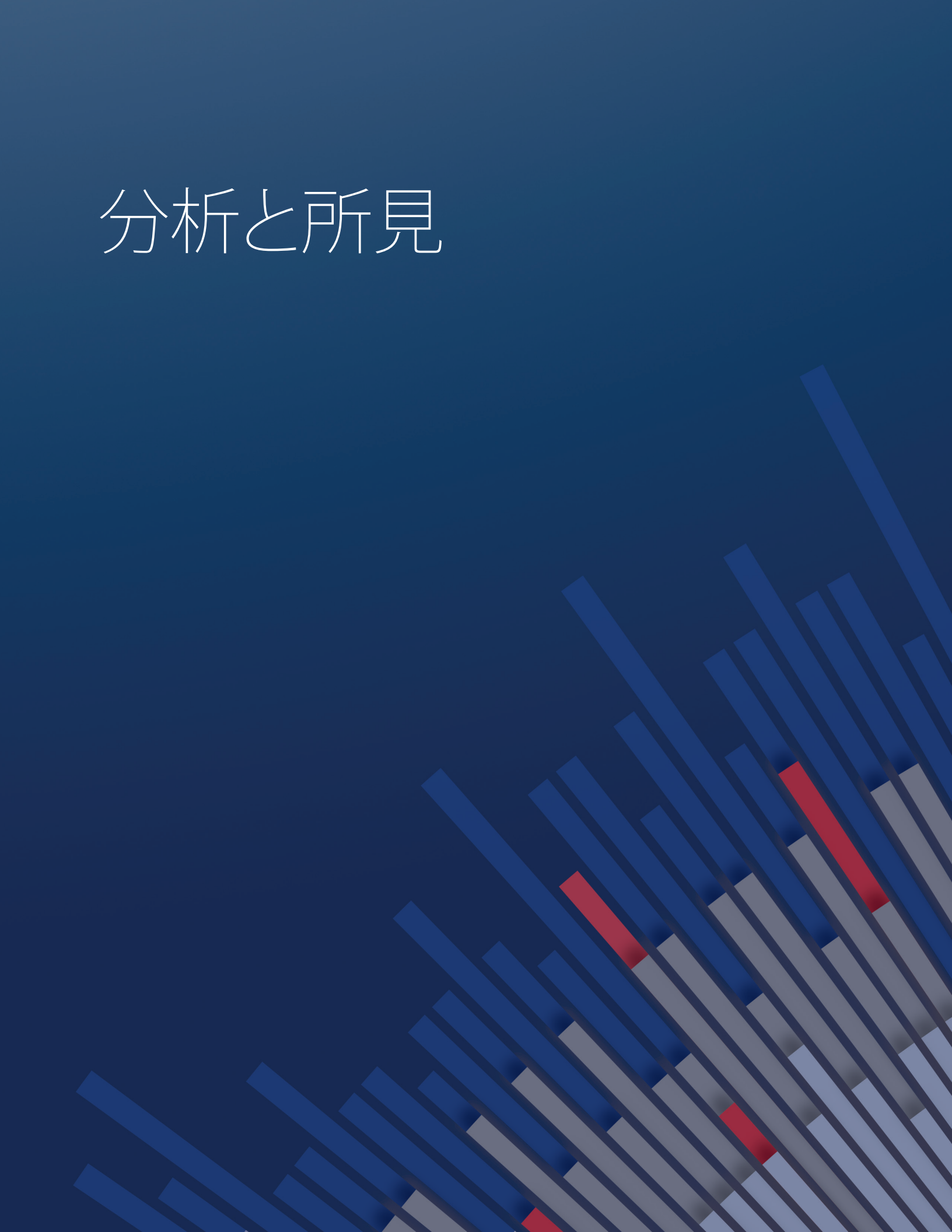
レポートの共有

図 25. レトロスペクティブ、TTD 平均値、TTD 中央値、2014 年 12 月～ 2015 年 5 月




*出典：シスコ セキュリティ リサーチ*

# 分析と所見



# サイバーセキュリティに関して実施すべきアクション：セキュリティ ベンダーによる迅速なイノベーション

*シスコのセキュリティ専門家は、セキュリティ業界は今すぐ変わる必要があると述べています。検出時間を短縮し、攻撃を回避できる、革新的で、適応可能で、信頼性の高いセキュリティ ソリューションを開発するために、集約と統合を促進することが必要です。さらに、シスコの地理的/政治的分野の専門家は、世界のビジネスのイノベーションと経済成長を支えるサイバーガバナンスの重要性について知見を提供しています。*

ユーザやシステムに対する侵害が確実に発生すると想定される世界では、セキュリティ回避型の脅威の検出は、組織とセキュリティ チームにとって明らかに必要な取り組みのひとつです。脅威アクティビティは、国家によるものを含め、増加する一方です。そのため多くの組織は、ビジネスやインフラに対するサイバー攻撃が行われてもクリティカルなサービスを復旧できるように、ビジネスを継続させるための計画立案に真剣に取り組むようになっています。

しかし同時に、ビジネスと個人ユーザの両方が、サイバー攻撃を検出するだけでなく効果的に避けることができる機能の開発をセキュリティ業界に切望していることも明らかです。ユーザは最低でも、より短時間で検出と解決を行うソリューションを求めています。

今のところ、セキュリティの複雑さがこれらの要求を満たすうえでの妨げとなっています。

セキュリティ業界には、1 つまたは複数の優れた製品からセキュリティ スイートを構成している、大手ベンダーが存在します。ただし、こうしたスイートに含まれる一部のソリューションは、主なソリューションほど効果的ではなく、また、それらと連携していない場合もあります。

一方、セキュリティ業界のニッチ ベンダーは、個別的なセキュリティ ギャップの解消に役立つ製品を開発しています。多くの組織は、一歩下がった場所から包括的にセキュリティを見るのではなく、既知のギャップを埋めるために最新のイノベーションにすぐに投資してしまいがちです。

その結果、製品の「つぎはぎ対応」が生まれ、セキュリティ チームによる管理が困難になります。複数ソリューションの機能が重複していたり、業界標準を満たしていなかったり、相互運用できない事態が生じます。そして、平均的なユーザが求める規模で導入できないニッチなテクノロジーは、いくら効果的であっても、通常、寿命が短くなります。

さらに、多くのセキュリティ テクノロジーでは、最新のリスクに適応するために、組織のセキュリティ アーキテクチャを全面的に刷新する必要があります。セキュリティ業界の大手またはニッチのいずれのベンダーのテクノロジーも、変化し続ける脅威に合わせて進化することはできません。これは持続可能なモデルではありません。

## 業界の統合と統合型脅威防御

シスコのセキュリティ専門家は、適応型ソリューションの必要性から、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。業界がひとつになり、多くのソリューションに可視性、制御、インテリジェンス、コンテキストを提供する、統合型の脅威防御アーキテクチャへと移行していくことが予想されます。

この検出と対応のフレームワークは、既知の脅威と新しい脅威の両方に対して迅速な対応を支援します。このアーキテクチャの中心は、状況を完全に可視化するプラットフォームです。これは、脅威を評価し、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関連付け、防御を最適化するために、継続的に更新される必要があります。ローカル インテリジェンスは、インフラストラクチャに関するコンテキストを提供するのに対し、グローバル インテリジェンスは、分析および即時的な保護の共有のために検出されたすべてのイベントと侵害の指標を関連付けます。

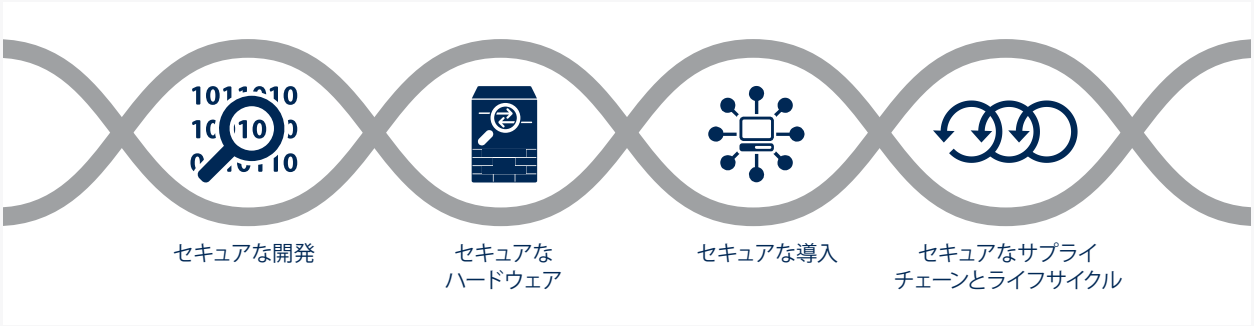
可視化プラットフォームの目的は、すべてのベンダーの製品をその上で運用し、貢献させるための基盤を構築することです。このシステムは、セキュリティ コミュニティから入手できる大量のセキュリティ情報を取り入れ、それに基づいて機能します。それによって提供される可視性により、セキュリティ チームはより細かな制御が可能となるため、より多くの脅威ベクトルに対して優れた保護を提供し、より多くの攻撃を阻止できます。

これは、すべてのエンド ユーザが、今日の脅威アクターの高度な戦略から自らを防御できるようにするために、セキュリティ業界が目指すべき方向性です。ただし、ここで説明したような、統合された脅威防御機能を開発するには、ニッチ ベンダーと、長年続いている大手ベンダーを含め、すべてのセキュリティ ベンダーのいっそうの協力、対話、連携が必要です。

業界は、特にアライアンスを通じて、より積極的かつ適切な方法で情報を共有するために、大きく前進しています。しかし、セキュリティ対策に必要なイノベーションを促進し、展開されたセキュリティ スタック全体で体系的な対応を実現するには、脅威情報をリアルタイムで自動的に交換する必要があります。業界が一致団結し、ネットワーク全体にナレッジとインテリジェンスを素早く配布できるようになれば、攻撃者が匿名性を維持しながら成功し続ける可能性が低くなります。

### 信頼できる製品

レポートの共有




今後 5 年間でセキュリティ業界の集約と統合が進むにつれて、新しいセキュリティ製品とサービスを購入する組織は、それらのソリューションが有効で、持続性があり、信頼できることを確認する必要があります。

各組織は、セキュリティ ベンダーやその他の IT ベンダーが製品にセキュリティを組み込むために何を行っているかを、時間をかけて理解する必要があります。また、各組織は、これらの製品が、それらの製品を組織に提供するサプライ チェーンのあらゆる場所で信頼性を維持していることを確認する必要があります。それに加えて、ベンダーの製品が信頼できることを実証し、その主張を契約によって裏付けるようベンダーに依頼する必要があります。

## 専門技術の価値

セキュリティ ベンダーには、信頼性の高いソリューションに投資し、セキュリティ テクノロジーを最新に保つことの重要性をエンド ユーザに理解してもらううえで、果たすべき重要な役割があります。従来のインフラストラクチャに頼っている組織は、データ、システム、ユーザ、つまりビジネス全体を危険にさらしています。

多くの組織におけるセキュリティ人材の不足は、リスク環境とベンダー状況の両方の進展をモニタできるスキルを持ったリソースが限られていることを意味します。社内のセキュリティの専門知識にアクセスできないことが原因となって、多くの組織でセキュリティ防御を構築する際断片的または「つぎはぎ対応」アプローチが採られてしまいます（ページ 32 を参照）。

サードパーティの専門知識を確保することにより、組織は、変化する脅威の状況に応じて方向転換する柔軟性を得られます。セキュリティ サービス プロバイダーは、セキュリティ全体に目を向けて、企業が投資し、セキュリティへの投資を最大限に生かすよう支援できる立場にあります。

限られたセキュリティ チームの増強に加えて、サードパーティの専門家は、組織のセキュリティ ポスチャの強度をテストする評価を提供できます。また、脆弱性などのリスクに対処するための効果的な戦略を明確化するよう支援できます。また、組織が自動化を導入し、検出が困難で次々と現れる脅威と戦うために必要な分析とリアルタイムな脅威の関連付けを行うソリューションを管理することも支援できます。

一部の組織は、モバイル、ソーシャル、クラウドなどの新しいビジネス モデルを採用する際に、セキュリティ サービス プロバイダーの指導に頼っています。また、各組織が事業を行っている市場でのデータ プライバシーとデータ支配権の要件に対処する際の支援を求めている組織もあります。中小企業を含むその他の組織は、大企業が使用しているセキュリティ テクノロジーと運用を活用しようとし、ビジネス ニーズを満たす管理型のホストされたモデルを見つけるためにサードパーティのエキスパートを活用しています。

## 将来のイノベーションを支えるためのグローバル サイバーガバナンス フレームワーク

世界中の企業は、競争力を高め顧客に利益をもたらすビジネス モデルを維持するために、インターネットにより大きく依存するようになっています。その一方で、その成功を妨害し得る戦術を展開する攻撃者に直面しています。サイバー リスクを放置したままにすると、すべての企業のイノベーションと経済成長に大きなリスクがもたらされます。

シスコの地理的/政治的分野のエキスパートは、複数の関係者が協力するサイバーガバナンス フレームワークが、グローバル ビジネスの継続的なイノベーションと経済成長に向けた前向きなステップであり、デジタル エコノミーにおける投資を支えるものとしてとらえています。しかし、現在のガバナンス フレームワークでは、企業はサイバー攻撃から保護されません。このようなサイバー攻撃には、情報漏洩と知的財産の盗難につながる攻撃だけでなく、グローバルなサプライチェーンを混乱させたり、重要なインフラストラクチャに損害を与えたり、さらなる悪影響を与える能力を持つ攻撃が含まれています。

多くの企業はサイバー攻撃に対する対応策を推進しません。他国の警察による支援が欠けているためです。ただし、サイバー攻撃が公共の利益に反し、制裁措置が必要であることに多くの政府が理解を示すようになっています。

効果的なグローバル サイバーガバナンスが欠如していると、新たな脅威を検出して防ぐ適応型テクノロジーを開発するためのコラボレーションが阻害される可能性もあります。このほど、デジタル監視ツールなど、特定の軍事・民生両用のテクノロジーの輸出を管理することを目的とした、ボランティアの国際的な申し合わせであるワッセナー・アレンジメント[7] に変更が提案されました。この提案により、こうした管理が抑制され、セキュリティ研究者は、規制の重荷なしに同業者と情報を共有できなくなります。このような傾向が続くと、セキュリティ研究に大きな影響を与え、業界の人材不足をさらに悪化させる可能性があります。

### 協調的なルール造り：将来の方向性

境界の問題、特に、政府がどのようにして国民や企業に関するデータを収集し、その情報を司法権と共有するのか、また共有しないのかという問題は、結束力のあるサイバーガバナンスの実現に必要不可欠な協調を困難にします。Internet of Things が浸透し、世界がますます相互接続される中で、企業、政府、社会は、増大するセキュリティとプライバシーの課題に対処するために、より効果的に協力する必要があります。

現在、国際舞台での組織間の協力と信頼は、どうひいき目に見ても一部の組織に限定され、他の組織間には存在しません。強固な協力関係を持つ組織でさえ、サイバーガバナンスに関しては理念が競合し、各自の国家主権の関心事と自市民に利益をもたらす法律を制定することに当然注力しています。気候変動に関する議論と同様に、ごく一部の組織だけが議論に参加し、小規模な対策でさえも、意見の一致に至ることは困難です。

少なくとも地域レベルでは、国境を超える努力がいくつか行われています。たとえば、欧州連合（EU）では、提案されたネットワーク・情報セキュリティ（NIS）指令を通じて、情報共有の調整を改善する動きがあります。この指令は、「加盟国の間と、公共部門および民間部門の間の協力を改善する」ことなどにより、「EU 内のサイバー セキュリティの共通レベルを高める」ことを狙いとしています。[8]

また、欧州と米国は、司法当局の間で共有されるデータのためのデータ保護標準を設定する、データ保護の「包括合意」への署名に近づいているようです。この合意は、どのような方法でどのような種類のデータにアクセスできるかについてのより大きな質問に答えるものではありません。しかし、管轄区域の対立の間に企業を追いやってきた、2 つの権力の間の緊張した空気を改善するうえでは、ある程度の役に立つ可能性があります。EU と米国で活動する組織の法律、技術、セキュリティ チームは、包括的合意に署名されれば、アクセス要件ついて協力する必要があります。

7 『Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items（ワッセナー・アレンジメント 2013 完全合意の実現：侵入と調査の項目）』[英語]、*Federal Register*. https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items。

8 『Network and Information Security (NIS) Directive（ネットワークと情報セキュリティに関する指令）』[英語]、European Commission: http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive。

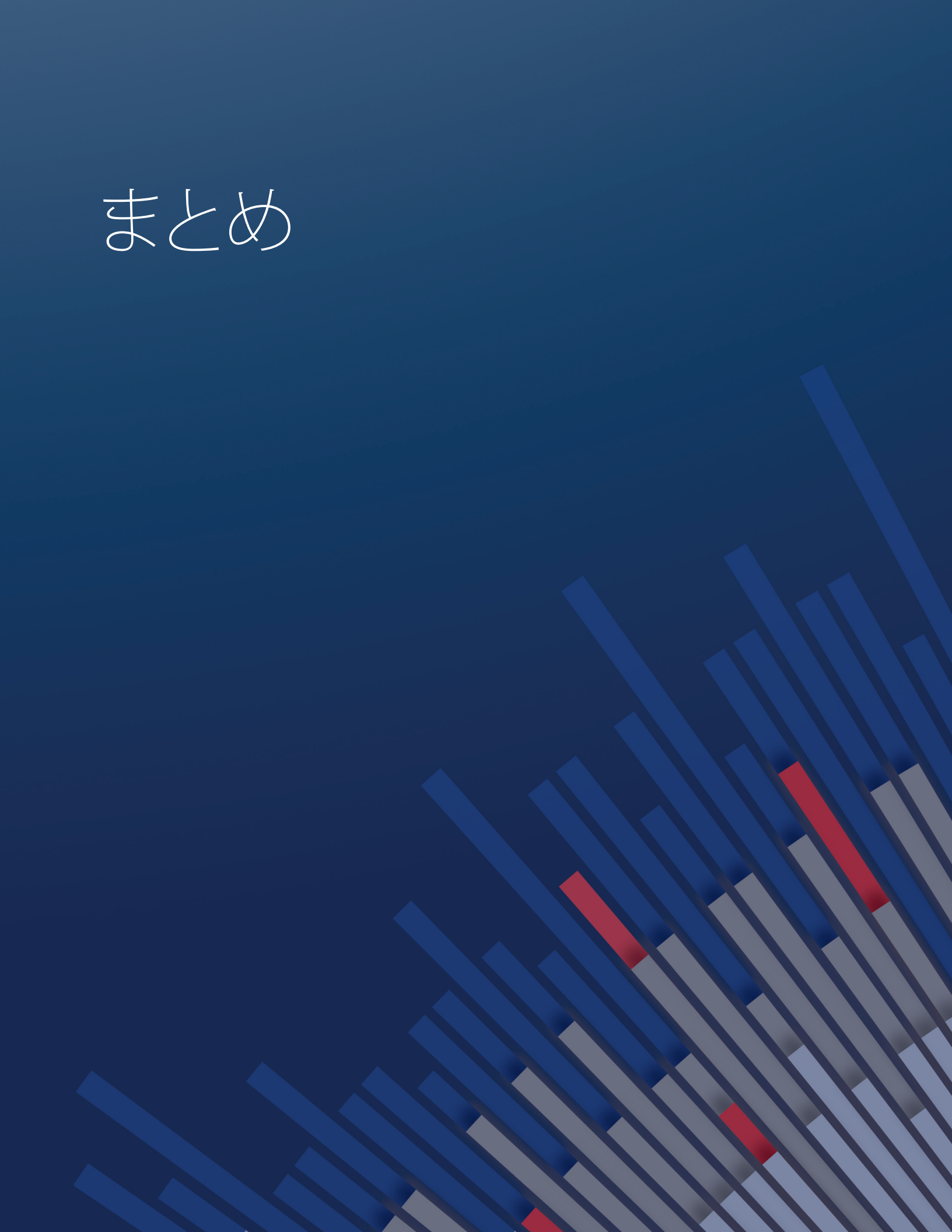
しかし、欧州で進行中のその他の規制は、特にビジネスにとって高い境界を作り出すことになりかねません。EU の機関は、新しい一般データ保護規則（GDPR）を年末までに決定しようとしています。これは、現在の EU データ保護指令を置き換えるものです。

この規則には、個人データの幅広い定義と、それらのデータをどのように管理すべきかについての規範的ルールが含まれており、従わない場合は高い罰金が課されます。それは、EU との間または EU の中でビジネスを行う組織が、顧客データを収集、保管、使用し、情報漏洩を報告する方法について大きな影響を与えます。GDPR は、より大きな責任と透明性を持たせることを意図しており、多くの組織に、少なくともデータ プライバシーとガバナンスに対するアプローチを調べ、ベスト プラクティスを採用するよう強制します。

たとえば、技術チームは、国境を越えたデータの移動についての制限や問題に関し、設計上の配慮を行う必要があります。「個人データ」と見なされるデータと見なされないデータの、機密性の地域による違いにも注意する必要があります。また、セキュリティ チームは、データ転送に影響を与える開発、個人データの定義、ネットワークおよび情報セキュリティ処理の法的根拠、情報漏洩の報告義務にも気を配る必要があります。

ルール作成の整合性を高めることは、データ保護規則に関する政府間のネゴシエーションを促すサイバーガバナンス フレームワークの構築に向けた道筋としての役割を果たすと同時に、業界がその間で板挟みになるのを防ぐことができます。それが起きるまで、セキュリティ担当者は、さまざまな国によって発行されたルールが業務に与える影響について、組織の意思決定者に理解してもらうよう、積極的な役割を果たす必要があります。互換性のないシステム、耐え難いほどの負担となったり矛盾するデータ要件、プライバシー法の違反、データ転送および処理要件などが課題となります。

# まとめ



# まとめ

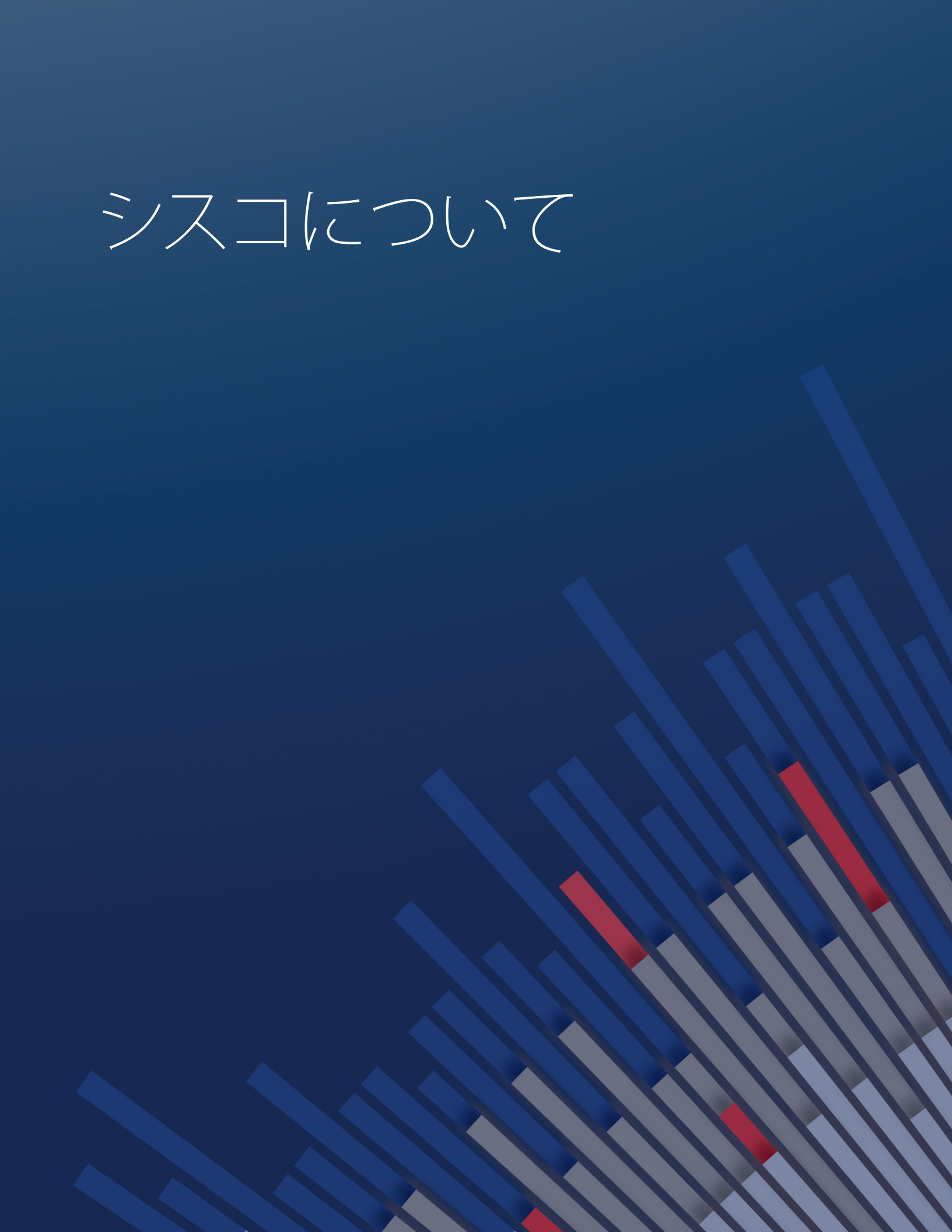
このレポートで説明した脅威は、組織とそのセキュリティ チーム、個々のユーザが直面するサイバーセキュリティ課題の一部に過ぎません。2015 年は、サイバー攻撃のイノベーション、復元力、回避能力がこれまでにないスピードで進化していることがわかっています。攻撃者は、成功のためにあらゆる障壁を乗り越えることに余念がありません。セキュリティ業界が脅威をブロックし検出するためのテクノロジーを開発できるのと同じ速度で、悪意ある攻撃者は、戦術全体を変更することができます。

攻撃者とセキュリティ ベンダー間のイノベーションの競争は加速する一方であり、何もせずに傍観している組織は攻撃に対してより脆弱になる危険があります。ビジネスに影響を与えるサイバーセキュリティのリスクを特定して対処することと、適切な人、プロセス、テクノロジーを組み合わせてそのような課題に対処することについて、積極的になる必要があります。

シスコの上級副社長兼セキュリティ ビジネス グループのジェネラル マネージャのデビッド・ゴッケラーは次のように述べています。「セキュリティは、組織がそのビジネスについて総体的に考える際、その一部となる必要があります。非常に多くのものが危険にさらされています。それは、ブランド、評判、知的財産、顧客のデータなどです。このすべてが危険にさらされているのです。組織には、適切なセキュリティ ポスチャによってそのリスクを最小化するための体系的なアプローチが必要です」

信頼できる製品は、有効なセキュリティ ポスチャの不可欠な要素であると、シスコのチーフ セキュリティおよびトラスト担当者のジョン・N・スチュワートは述べています。「組織は、侵害が避けられないという事実を受け入れたくありません。信頼でき、復元力があり、最も高度な脅威でさえも回避できる製品を提供するようセキュリティ業界に期待しています」

# 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、原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 2015 年中間セキュリティ レポートの執筆者

### 集合型セキュリティ インテリジェンス

Cisco Collective Security Intelligence（CSI）は、複数のセキュリティ ソリューションで共有され、業界最先端のセキュリティ保護と有効性を提供します。CSI は、脅威研究者に加えて、インテリジェンス インフラストラクチャ、製品およびサービス テレメトリ、パブリックおよびプライベート フィード、オープン ソース コミュニティによって推進されています。

### Talos セキュリティ インテリジェンスおよびリサーチ グループ

Talos 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のための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。

### 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。

### 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 エキスパートと、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。これは、常時警戒とオンデマンド分析を 24 時間 365 日提供します。

### コグニティブ脅威分析

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、新たな脅威を独立的に特定し、検出内容から学習して、長期的に適応します。

©2015 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。(1502R)
この資料の記載内容は2015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。

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

15.08