2015
グローバル脅威
インテリジェンス・レポート

（日　本　語　訳）

NTT Group

Table of Contents

セクション A

セクション A.1 エグゼクティブ・サマリ

2015 グローバル脅威インテリジェンス・レポートについて

過去数年間、セキュリティ業界は APT(Advanced Persistent Threat)や高度な脅威の対処に注力してきました。高度な脅威は組織の最重要データを狙い、先進的なセキュリティベンダでさえ進行中の高度な攻撃を見つけるのに苦戦しています。また、組織に「実践の基礎」が備わってなければ、攻撃は高度でなくても成功してしまいます。そのような基礎として、例えば、成熟したパッチ管理プロセス、インシデント対応手順、端末保護の制御、フィッシング攻撃や PC 上のマルウェアを見つけるための適切な従業員トレーニング等があります。基礎がしっかりしてないと、まず、攻撃者は既知の脆弱性をついたり、**ソーシャルエンジニアリング**攻撃を用いる等して、人間の隙をついて侵入します。さらに、高度な手法を用いて、発見されることなく攻撃を継続し、深く潜入していきます。

本レポートでは、APT だけが組織が考慮すべき攻撃ではないということを示します。NTT グループが 2014 年に収集したデータによると、多くの組織が依然、あまり高度とはいえない脅威でさえ効果的に防げていません。

そこで、本レポートは、比較的高度でない攻撃手法、そして、そのような攻撃に効果的に対処する方法に焦点をあてています。また、エンドユーザのリスクに関しても解説します。今やエンドユーザは企業の防御線(perimeter)となり、適切な防御が必要となってきています。

セキュリティ業界では、誰もが被害にあうことを想定しておく必要があるとよく言われていますが、多くの組織はそのアドバイスに従っていません。２０１４年における NTT グループの調査では、大多数の組織が、自分の環境に起こる重大なインシデント対処の準備ができていませんでした。

最近、脅威インテリジェンスがホットなトピックになっています。しかし、市場には、「脅威インテリジェンスとは何か」について、大きな混乱があります。この混乱をなくすために、「 脅威インテリジェンスとは何か」、そして「いかにそれを実現するか」について NTT グループによる簡明な定義を提示します。脅威インテリジェンスを適切に活用すれば、 組織のセキュリティのコントロールを強化できます。

DDoS 攻撃(Distributed Denial of Service: 分散型 DoS 攻撃)は、攻撃対象のサービスがお客様に提供できなくなるように複数のサイトから攻撃をしかけるという手法です。ここでは、2014 年に NTT グループが検出した DDoS 攻撃の概要について、特に、DDoS 攻撃のタイプ別の増減及びタイプの分布率を中心に、解説します。

本レポートの各セクションでは、読者の皆様が脅威を回避するために取りうる手法を比較し選択肢として提案しています。

セクション A.2 – 主な調査結果

地域別およびビジネスセクタ別の攻撃動向

本レポートでは、NTT グループはいくつかの異なる脅威について考察 しています。それらの脅威は NTT のお客様に向けられたものですが、地理的な位置関係や特定のビジネスセクタとの関係において違いがあります。

- **金融セクタは引き続き最も標的にされているセクタで、観測された攻撃全体の 18%に相当。**
  金融セクタに対する標的型攻撃は、引き続き長期トレンドを踏襲しています。2014 年に金融セクタを支援したインシデント対応のほとんどは、電子送金に関する不正、フィッシング、および標的型フィッシングと直接関係しています。
- **専門サービス業（経営コンサルタントや法律事務所、公認会計士など）に対する攻撃は 9%から 15%に推移。**
  専門サービス業に対する攻撃の増加は、これらサービス企業と攻撃対象企業間の情報連結が必要という本質的な特徴に起因するリスクの結果です。この分野では、一般的にセキュリティ対策が手薄になりがちですが、攻撃者にとっては価値の高い攻撃対象です。
- **教育セクタにおけるマルウエアに起因するセキュリティイベントは 42%から 35%に下落。**
  2013 年のレポートと比較した場合 7%の減少が見られましたが、教育セクタは全セクタの全マルウエアによるイベントのうち、依然として 3 分の 1 以上を占めます。
- **NTT のグローバル顧客に対する攻撃のうち 56%は、米国内の IP アドレスが起点。**
  2013 年のデータでは 49%でしたが、今年は 7%上昇しています。攻撃者は標的の近くにあるシステムを利用し、地理的フィルタリングによる防御方法を回避することがしばしばあります。米国は高度にネットワーク化された国でもあり、攻撃者が利用するリソースには事欠きません。

脆弱性、攻撃そして流出

エクスプロイトキットとは、複数のエクスプロイト（ソフトウェアやハードウェアの脆弱性を狙った攻撃のために書かれたプログラム）をひとまとめにすることで、標的となったエンドユーザのシステムに対して、より簡単で、継続した攻撃を可能にした攻撃用のツールキットのことです。今年の脆弱性データおよびエクスプロイトキットに対する分析により、昨年の調査結果は確固たるものとなり、さらにエクスプロイトキットの組織に対するインパクトも見えてきました。

- **2014 年においてエクスプロイトキットが対象とする脆弱性の 80%以上は 2013 年及び 2014 年に公表。**
  2012 年、エクスプロイトキットが狙う脆弱性の公表されてからの平均経過年数は 2 年弱でした。2013 年および 2014 年には、同平均経過年数は 1 年強になっていました。エクスプロイトキットの開発者たちは狙ったシステムへ確実に侵入にするため、ツールの使い勝手と効率性向上に集中しています。エクスプロイトキットの機能を最新化しておくことが、サイバー犯罪をビジネス化することの重要な要因となっています。

- **2012 年から 2014 年において、Adobe Flash の脆弱性を悪用したエクスプロイトキットが増加。**
  2014 年に検出された Flash の脆弱性の数は過去最大でした。このことがエクスプロイトキットにおける、Flash 関連エクスプロイトの増加の一因になっています。アングラー・エクスプロイトキットは Adobe Flash のゼロデイ・エクスプロイトを含んでおり、他とは一線を画したものとなっています。

- **NTP（Network Time Protocol）の DDoS アンプ攻撃は 2014 年に NTT グループが観測した DDoS 攻撃全体の 32%に相当。**
  2014 年の第一四半期の間に、NTP アンプ攻撃は同年の DDoS 活動の最も大きな部分を占めました。このタイプの攻撃は、実行が簡単なことと、攻撃をサポートする DDoS ツールが手に入りやすいことが、この傾向の一因となっています。

- **UDP(User Diagram Protocol)の DDoS アンプ攻撃は NTT グループが観測した DDoS 攻撃全体の 63%に相当。**
  UDP ベースの攻撃（NTP、SSDP 及び DNS）は全体の約 3 分の 2 を占めました。

- **2014 年を通じて、全ての企業内システムにおいて特定された脆弱性の 76%は発見・公表から二年以上経過、同 9%は十年以上経過。**
  共通脆弱性評価システム（CVSS:Common Vulnerability Scoring System)においてスコア 4.0 以上の脆弱性についてのデータによると、効果的なパッチ管理に関して重大な懸念があります。CVSS では、スコア 4.0 以上というのは中から高度の脆弱性を含んでおり、多くのコンプライアンス・アセスメントを満足しない可能性が高いものです。これらの脆弱性の多くはエクスプロイトキットで攻撃可能なものです。

- **2014 年に検知した Web アプリケーションへの攻撃の 26%はインジェクションによるもので、前年比で 9%上昇。**
  Web アプリケーションへのインジェクション攻撃とは、システムには正当なクエリ（問合せ）と見えるが、実は悪意のあるコードやデータを送り込むというものです。このような攻撃は、しばしばデータ流出や遠隔コマンド操作を可能にします。このタイプの脆弱性は、独自開発のプログラムにおいてセキュアなプログラミングや品質保証テストを怠ることにより発生します。また、第三者の脆弱性のあるプログラム・ライブラリやフレームワークが起因となることもあります。

インシデント対応と事例研究

組織の攻撃検知能力と組織の攻撃対処能力は必ずしも一致しません。このレポートでは、今日の組織が直面している問題を具体的に説明するため、対策とケーススタディを交えながら、新たに得た知見を紹介します。

- **NTT グループではマルウェア、DDoS、侵入調査の三つのコア分野に焦点を当てたインシデント対応への取り組みを継続的に監視。**
  自組織内でインシデント対応能力を持つことの重要性を認識している組織もありますが、それでも外部サポートに頼ろうとする傾向があります。それ以外の組織では、日々の業務での対応には適応できていますが、より複雑なセキュリティイベントとなると、外部の専門家に未だに頼っているのが現状です。

- **NTT グループの DDoS 攻撃対応は 2013 年の 31%から 2014 年の 18%まで急激に減少。**
  技術が広く利用可能、入手可能になり、DDoS 攻撃の緩和に関する教育が広く浸透したため、NTT グループでは、DDoS 攻撃に対して外部のサポートを必要とすることが減りまし

た。2014 年では、特に NTP(NetworkTime Protocol)と SSDP (Simple Service Discovery Protocol)を狙った大規模な DDoS 攻撃がありましたが、効果的な緩和方式を用いることで、結果的にこの分野でのインシデント対応サポートの減少につながりました。

- **マルウェアの脅威に関するインシデント対応は 2013 年に比べ 9%増加し、43%から 52%へ。**
  エクスプロイトキットの機能拡大に伴い、NTT グループにおけるマルウェアの脅威に対するインシデント対応サポートは確実に増加しました。その大部分は、広く配布されているマルウェアへの対応でした。

- **基本的な対応・対策はあらゆるケースに対して準備不足。75%の組織では公式なインシデント対応計画が欠如。**
  NTT グループが 2014 年に観測したインシデントのうち、かなり多くの事例において、適切なネットワークのセグメント化やマルウェア感染の予防、パッチ管理、モニタリング、インシデント対応の計画化を実施できていれば、被害の予防や影響範囲を少なくできたことが分かりました。これらの基本的な対応・対策を まったく導入できていない場合が、大組織のなかでさえ、数多くあります。

- **ケーススタディ：標的型フィッシング攻撃 - 効果的な緩和方式で、被害試算額の 80%を削減。**
  このケーススタディでは、本来、127,000 米ドル以上のコストがかかる可能性があった、ある標的型フィッシング攻撃の法的措置や調査に対して、どのようにコストを 25,000 米ドルに抑えたかを詳細に記述します。

- **ケーススタディ：Web アプリケーションへの DDoS 攻撃。**
  能動的な DDoS 攻撃対策における早い段階での検知・対策により、結果として、風評被害や金銭的な損失を回避できた組織を紹介します。

セクション B: グローバルデータ分析と分析結果

セクション B.1: はじめに

本節では、2014 年に NTT グループ内のセキュリティ会社が収集したグローバルレベルでの攻撃情報を分析した結果について述べます。ログ、イベント、攻撃、顧客から収集したインシデントおよび脆弱性情報、ハニーポットやサンドボックス、DDoS 対策サービス等に関する NTT の研究結果に基づき分析を実施しています。

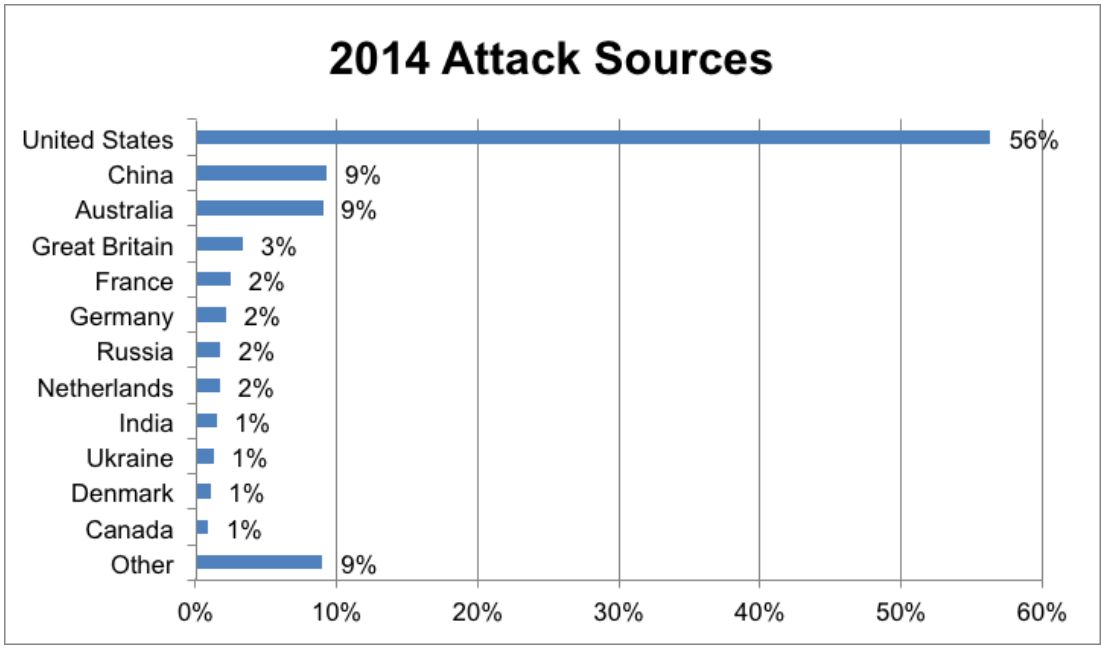
通常の運用を通して、NTT グループはセキュリティに関するログ、アラート、イベントおよび攻撃情報を収集し、相関関係・前後関係を見出したうえで分析を実施しています。NTT グループは毎年数兆ものログと数十億もの攻撃について処理しています。NTT グループの顧客数の大きさと多様性により、処理されたデータは多くの組織が直面する脅威を表しているといえます。

本節で表現されているデータは、攻撃イベントの特定に関係するログイベントから生成しています。生ログデータやネットワークトラフィックではなく、検証によって攻撃イベントと特定されたデータを分析することで、実際の攻撃状況をより正確に提示することが可能です。攻撃イベントを適切に分類しないことや偵察目的の膨大なネットワークトラフィック、偽陽性のイベント、SOC によって観測されている大量の DDoS 攻撃はかえって、実際の攻撃によるインシデントを見過ごす結果を招きます。

セクション B.2:2014 年攻撃解析

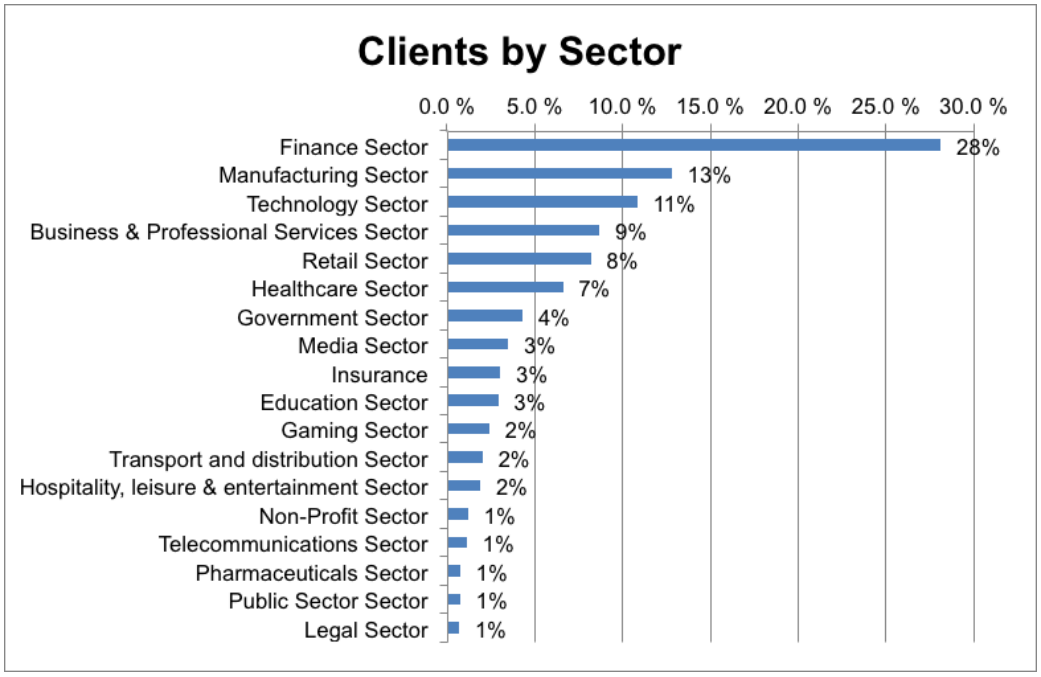
以下で示す図の通り、NTT の顧客に対する攻撃の 56%は米国内の IP アドレスが攻撃元になっています。この事実は 2014 年版の NTT GTIR 内で述べられている解析結果を裏付けています。2014 年版では、2013 年における攻撃の 49%は米国内の IP アドレスが攻撃元であることを示していました。

NTT グループはその背景にまで解析をすすめます。生データは、米国が攻撃元の大部分を占めている一方で、米国以外の国が何もしていないことを意味しているようにみえますが、実際の状況は違います。GoDaddy®、Amazon Web Services®、Google®、Microsoft®のようなクラウドホスティングサービスの品質と利便性向上により、攻撃者はこれらのサービスを利用して攻撃元の実際のアドレスを隠蔽します。IP アドレスをみると攻撃元は米国内を示していますが、実際には、攻撃者は世界中至る所に存在しうるのです。



Caption: 2014 年の攻撃元国別グラフ

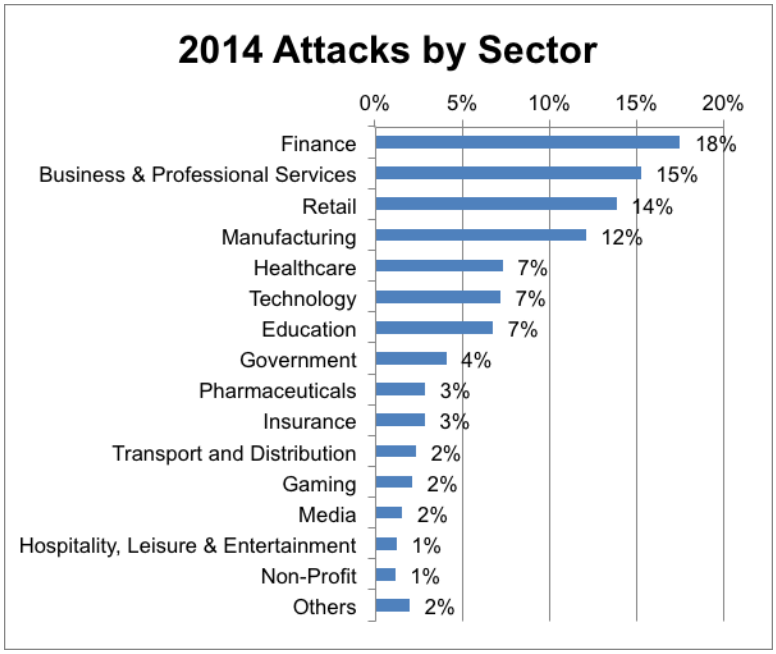
次の図は、NTT の顧客の業種別の分布を表しています。今年のレポートでは、業種別の特色をより正確に表せるように、顧客の業種を 14 から 18 に再整理しました。本レポートでは、解析したデータにもとづき、この再整理後の業種に基づいて、分野の再配置が、示した分析結果に対していつ重大な影響を及ぼしたのか示します。



Caption: 2014 年の顧客の業種別グラフ

以下の図は、攻撃全体における標的にされた業種ごとの分布を示しています。検知した攻撃のうち 18%は金融業に対するもので、継続的に 1 位の状況です。これは 2013 年から基本的に変化しておらず、2013 年は攻撃の 20%が金融業に向けられたものでした。新規顧客の追加とより多様な地理的要素に加え、業種の再整理のため、単純なデータ比較は難しいですが、分野ごとの攻撃の多くは 2013 年以来進化しています。

業種の再整理と検知した攻撃の詳細を考慮すると、製造業に対する攻撃は昨年に匹敵するレベルでした。一方、専門サービス業（経営コンサルタントや法律事務所、公認会計士など）および小売業に対する攻撃は増加しました。NTT グループは専門サービス業をとりわけ標的としている動向をいくつか把握しています。この業種は他業種ほどの情報セキュリティのリソースを有しておらず、最終的なターゲットとしての位置づけだけでなく、他の最終目標への踏み台として、攻撃者に狙われていると推測します。小売業は引き続き、攻撃者の標的となっています。

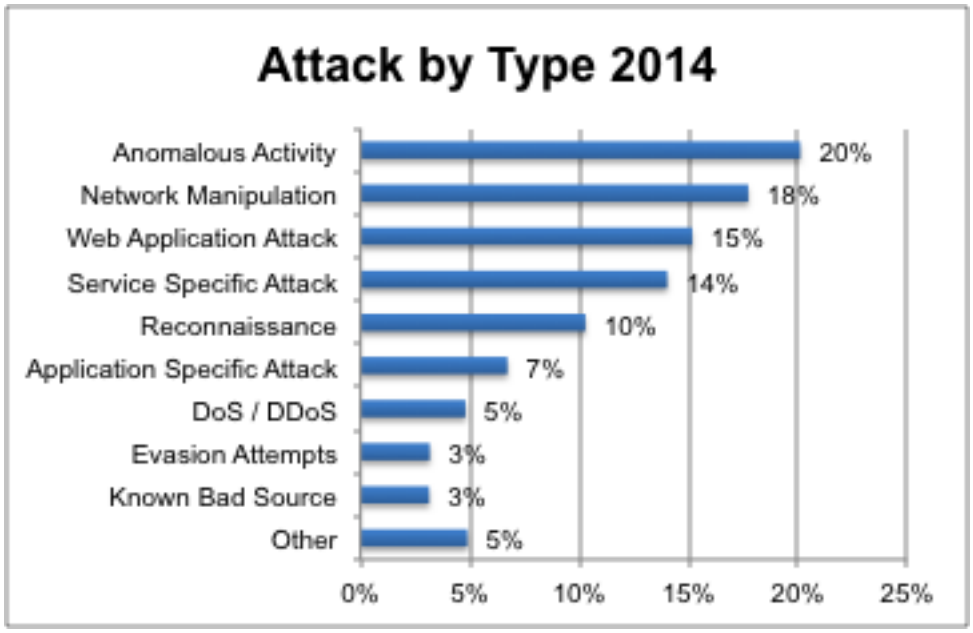


Caption: 2014 年の攻撃の業種別グラフ

全世界の全業種を対象に攻撃タイプを分類したグラフを示します。特権レベルでのアクセス試行やエクスプロイトソフトウェア、その他通常にはない活動を含む異常な振る舞いは、2 位(15%)から 1 位(20%)に変化しました。遠隔操作および Web アプリケーションに対する攻撃、特定のサービスに対する攻撃もすべて著しく増加しました。主にアラートの精度を向上し、敵意の少ない活動として攻撃を再分類したことにより、偵察活動は 2013 年の 4%から 10%に増加しました。

これは、攻撃者が標的型攻撃の対象者や脆弱性がありそうな端末やアプリケーションを探すために、より多くの時間と労力を費やしていることを示しています。またエクスプロイトキットの傑出した有効性も示しています。セキュリティ脅威が広がるメカニズムの一部として頻繁にメンテナンスされているエクスプロイトキットは、パッチが適用されていない OS やアプリケーションの大規模な感染において大きな役割を果たしています。より詳細な情報はセクション C: エクスプロイトキットを参照ください。

DoS/DDoS 攻撃や既知の悪性ソースなどの他のカテゴリは、昨年のレポートと同等のレベルを示しています。



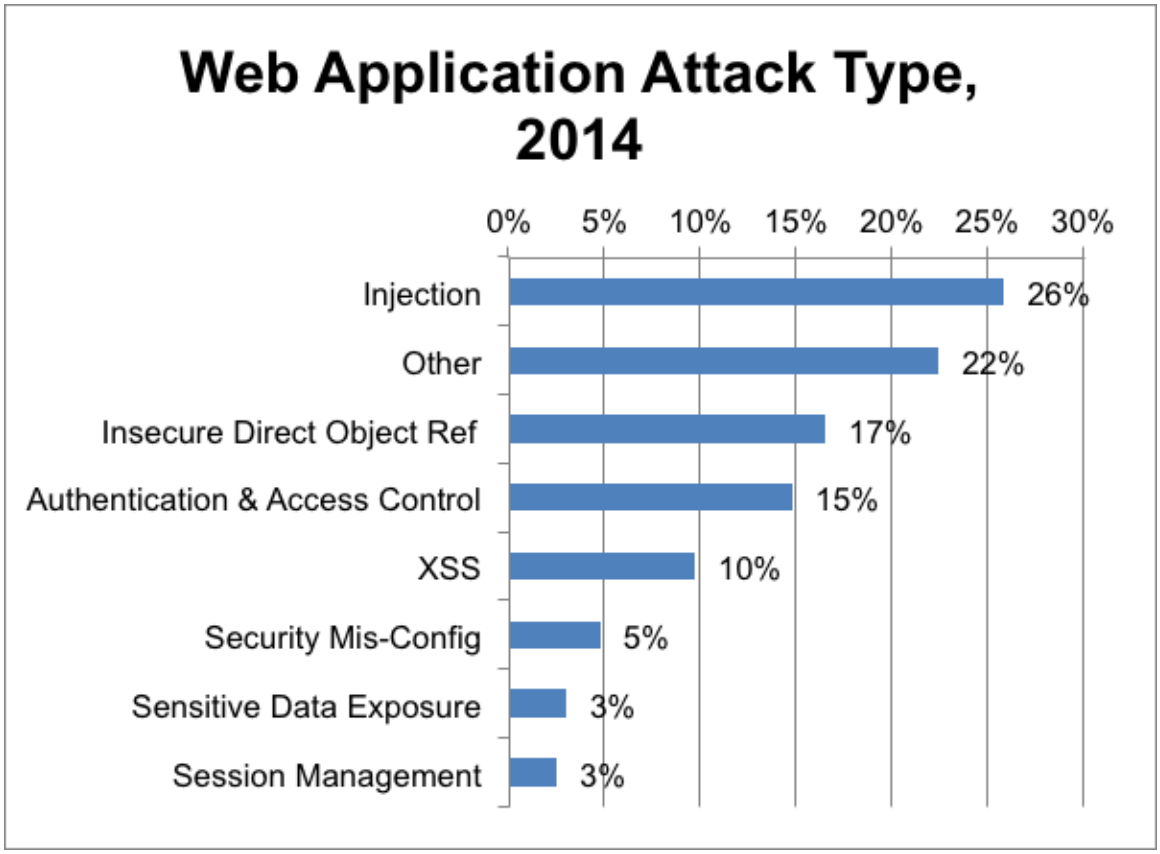
Caption: 2014 年の攻撃タイプ別グラフ

次の図は、2014 年に NTT グループによって３番目に多く観測された攻撃種別である、Web アプリケーションに対する攻撃について示しています。これは一般に、企業がインターネットに公開しているアプリケーションに対する攻撃を反映しているため重要な領域であるといえます。

2014 年に観測された Web アプリケーションに対する攻撃のうち 26%は、SQL インジェクションや LDAP インジェクションを含む、インジェクション形式の攻撃でした。これは、インジェクションを最も多い脆弱性として報告している OWASP トップ 10Web アプリケーション脆弱性リストと関係があります。また、これは 2013 年の 9%から大きく増加しています（2014 年は 26%）。OWASP[0] ランキングでは 4 位と 2 位に位置する「セキュアでないオブジェクトの直接参照」と「認証とアクセス制御」がそれぞれ 3%、4%減少しています。これらのリスクはいずれも本来アクセスできないはずの情報に攻撃者がアクセスできることを許してしまいます。

クロスサイトスクリプティング（XSS）とセキュリティ設定のミスはいずれも 2013 年と同程度でした。実存する XSS 脆弱性の多さにもかかわらず、実際に攻撃された数が比較的少ないことには少なからず違和感を覚えます。

[0] https://www.owasp.org/index.php/Main_Page



Caption: 2014 年 Injection 攻撃が Web アプリケーション攻撃の中ではトップ

2014 年の脆弱性データは、様々な規模・分野にまたがる組織に対する複数のベンダ製品による脆弱性スキャン結果データから生成されています。これらのベンダは例えば Qualys®, や Nessus®, Saint, McAfee®, Rapid7®, Foundstone®, Retina®を含みます。次の図は外部および内部からのスキャンにより発見された脆弱性のトップ 10 を示しています。世界中からより幅広く収集したデータの追加や新規の顧客からのデータの追加により、2013 年と 2014 年の脆弱性データの比較は難しくなっています。

外部脆弱性 トップ 10	全外部脆弱性 に占める割合	内部脆弱維の トップ 10	全内部脆弱性 に占める割合
旧バージョンの PHP	15%	旧バージョンの Java Runtime Environment	11%
旧バージョンの ApacheWeb サーバ	10%	Oracle Java SE 重要パッチアップデート	10%
旧バージョンの Apache Tomcat サーバ	9%	Java Web Start に存在する複数の脆弱性	7%
クロスサイト スクリプティング	5%	MS Windows セキュリティアップデートの適用漏れ	7%
SSL/TLS による 情報漏えい	5%	旧バージョンの Flash Player	6%
旧バージョンの Open SSL	3%	旧バージョンの Adobe Reader と Acrobat	3%
SSL/TLS 再ネゴシエーション　ハンドシェーク	3%	旧バージョンの Internet Explorer	3%
サードパーティの脆弱な Apache プラグイン	2%	Oracle の複数の脆弱性	2%
Web 上の平文の ユーザ名/パスワード	2%	旧バージョンもしくはパッチ適用漏れの Oracle DB	1%
旧バージョンの OpenSSH	2%	旧バージョンの OpenSSH	1%

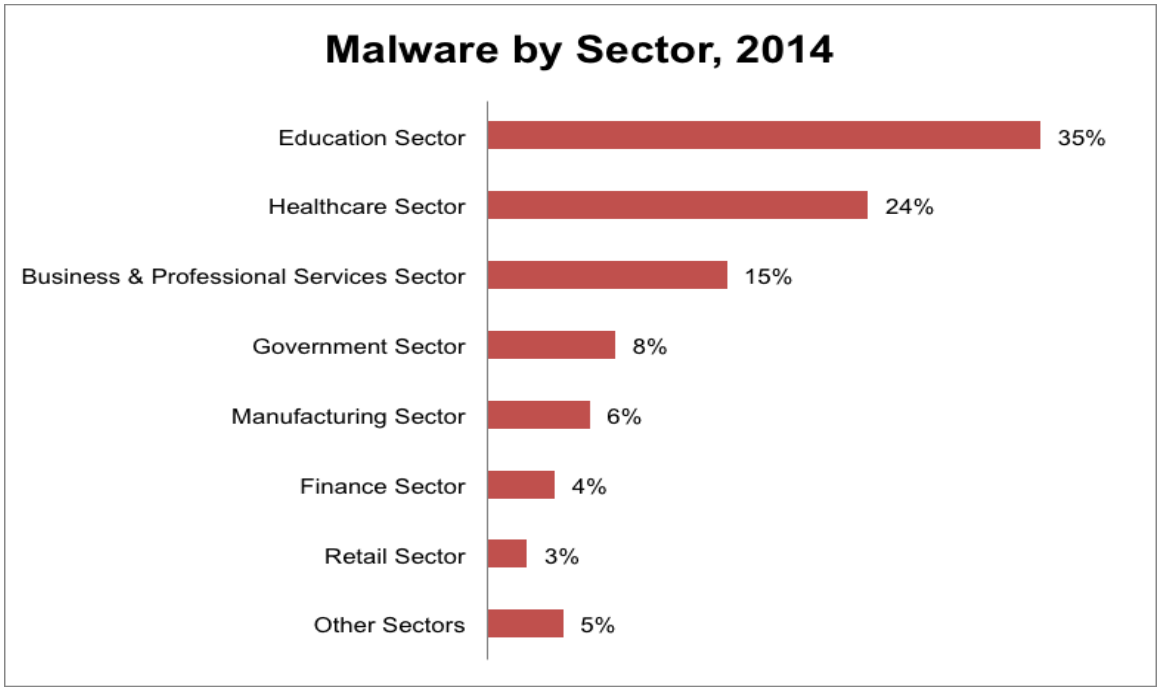
Caption: 2014 年の外部と内部それぞれに存在する脆弱性 Top 10

NTT グループは、幅広い情報源からマルウェア検体を収集し解析しています。これらの情報源は、NTT グループのセキュリティ基盤、インシデントレスポンス調査、マルウェアレポジトリ、マルウェアフィード、クライアント PC とのやりとり、自社保有のハニーポットネットワークなどを含みます。この解析により、検知・防御用シグネチャの独自開発が可能となり、お客様をより安全に守ることができるようになります。次の図は、マルウェアの業種別の分布を示します。

教育分野では、昨年の 42%から減少したものの 2014 年には 35%となり、同年に検知されたマルウェア関連の全イベントの 3 分の 1 以上を依然として占めています。大学やその他の教育機関では、個人の端末を使って公衆ネットワークに接続するようなエンドユーザを多数抱える上に、情報を容易に入手できることを優先する風潮があります。また、オペレーティングシステムやパッチ適用状況にばらつきがある私有端末の利用や様々な教育レベルのエンドユーザ、防御手法が混在している環境が、このような状況を招いているといえます。

専門サービス業は観測されたマルウェアの 15%を占め、2013 年の 23%から 8%の減少となりました。これは本業種における顧客数の割合の減少とほぼ一致しています。医療分野は観測された

マルウェアの 24%を占め、2013 年の 3%から 21%の増加となりました。NTT グループは医療分野の顧客を多く獲得し、また、2013 年の本分野の顧客の一部を別の業種へ再整理したため、前年との直接比較においては実際よりも変化があるようにみえます。また、医療分野を標的とした攻撃全般についての大きな増加は NTT グループでは確認できませんでしたが、攻撃者がより頻繁に個人情報を狙うようになった可能性があります。



Caption: マルウェアの業種別グラフ

セクション C: エクスプロイトキット　―　運用ライフサイクルと最近の傾向

セクション C.1：はじめに：エクスプロイトキット

ソフトウェアのエクスプロイトは、オペレーティングシステム、アプリケーション、サポートライブラリやフレームワークにおいてパッチが適用されていない欠陥や構成ミスをうまく利用します。このようなエクスプロイトによって、攻撃者は悪意のあるソフトウェアを脆弱な機器にインストールすることができます。エクスプロイトキットは、ハッカーフォーラムや IRC（インターネットリレーチャット）チャネルで普通に販売されているソフトウェアパッケージです。これには、**エンドユーザ**側技術（Internet Explorer、Adobe Flash など）の既知の脆弱性をターゲットとしたソフトウェアエクスプロイトなどが含まれます。エクスプロイトキットを利用することで、キットのユーザー（このセクションで「攻撃者」という用語を使用するとき、「エクスプロイトキット」ユーザーを指しています）は独自のエクスプロイトを開発しなくても、脆弱なシステムに対して大規模な攻撃を仕掛けることができるのです。ただし、経験が乏しいハッカーになりたての犯罪者にとっては、エクスプロイトキットを入手したからといって即座に攻撃能力が得られるわけではありません。大規模攻撃を成功させるには相当の知識とスキルが必要です。エクスプロイトキットは、攻撃を成功させるための一要素にすぎないのです。

本章では、エクスプロイト開発プロセスの概略とともに、大規模攻撃でエクスプロイトキットが果たす役割を解説します。この解説を読んでいただくことで、エクスプロイトのライフサイクルや、大規模攻撃の一要素としてキットが果たす役割を理解しやすくなるでしょう。エクスプロイトを適切に使用するにはスキルが必要です。エクスプロイトキットはあくまで攻撃プロセスの一部を自動化し、管理するのに役立つものです。エクスプロイトキットの開発には、これとはまったく異なるスキルが必要とされますが、エクスプロイトキットの成功と長きにわたって使用される鍵となります。エクスプロイトキットの増加は、サイバー犯罪経済のコモディティ化と専門化の結果といえます。

本章は、2014 年に NTT グループが確認したエクスプロイトキットの傾向分析も紹介します。流通しているエクスプロイトキット間の激化する競争によって、開発者らは自らのキットに最新のエクスプロイトを採用しようと駆り立てられています。たとえば、2014 年のエクスプロイトキットの主な展開の一つとして、NTT グループは Adobe Flash エクスプロイトの使用が増加したことを観測しています。

「エクスプロイトキット　―　運用ライフサイクルと最近の傾向」に関する詳細説明は、以下の項目も参照してください。

エクスプロイトキットの開発と運用ライフサイクル

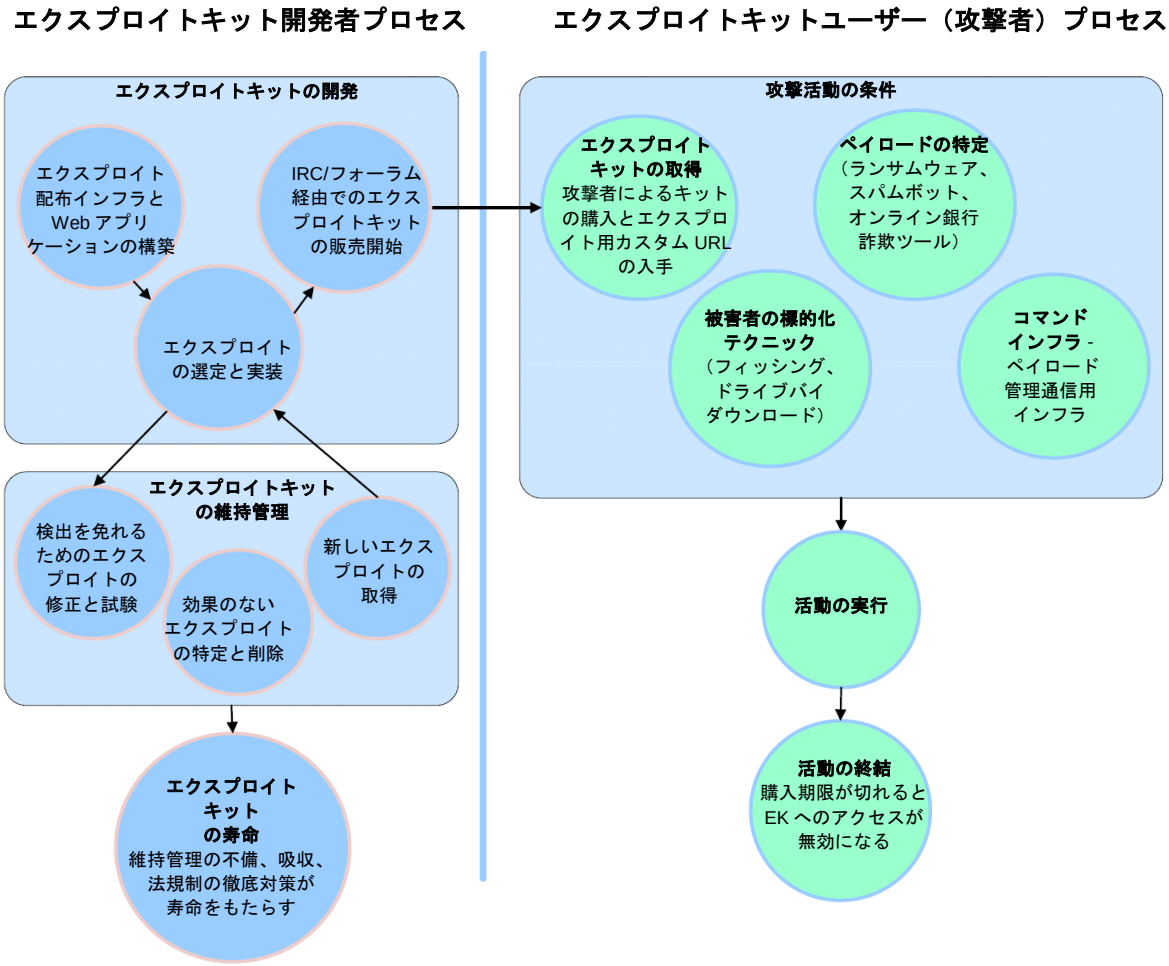
エクスプロイトキットで標的とされる脆弱性

エクスプロイトキットの月別検出数

セクション C.2: エクスプロイトキットの開発と運用ライフサイクル

このセクションは、エクスプロイトキット（EK）のライフサイクルを、開発者と攻撃者の両方の視点からざっと見ていきます。

下の図は、エクスプロイトキットの 2 つのプロセスを示しています。最初の図は、エクスプロイトキットの開発と維持管理のプロセスです。2 つ目の図は、攻撃者がエクスプロイトキットを利用するプロセスです。



タイトル：エクスプロイトキットの開発と運用ライフサイクルの依存関係

エクスプロイトキット開発者プロセス

エクスプロイトキットの開発

エクスプロイト配布インフラと Web アプリケーションの構築

攻撃者にとってエクスプロイトキットは「サービスとしてのソフトウェア（SaaS）」であり、エクスプロイトキットの開発サイクルは普通の組織によるソフトウェア開発ライフサイクルとよく似ています。エクスプロイトキット開発の最初のステップは、エクスプロイト配布インフ

ラストラクチャを管理インターフェースや攻撃者インターフェースとともに構築することです。エクスプロイトキットには、代表的に以下のものが含まれます。

- **攻撃者アクセスコンソール**（エクスプロイトキットパネル） — エクスプロイトキットを利用する攻撃者は、エクスプロイトキットのコントロールパネルへの暗号化されたログイン経由でコンソールにアクセスします。次の Fiesta エクスプロイトキットのスクリーンショットに示すように[1]、典型的にはこのコンソールによって、攻撃者はエクスプロイトの試行状況のモニタリング、不正利用された機器数の特定のほか、さまざまな技術プロファイルへのエクスプロイト成功率の計測を行うことができます。

タイトル：Fiesta エクスプロイトキットのユーザーコンソール

[1] 出典： http://blog.0x3a.com/post/62375513265/fiesta-exploit-kit-analysis-serving-msie-exploit

- **管理者コンソール** –管理者コンソールはエクスプロイトキットパネルの延長である場合もそうでない場合もありますが、エクスプロイトキット開発者が全体的なアプリケーションの使用状況やエクスプロイトの効果についてモニタリングするのに使用します。
- **ランディングページ** –標的とされる被害者は、開発者が用意したカスタム URL を経由してエクスプロイトキットのランディングページに誘導されます。このランディングページは、遠隔地にある被害者のシステムの特徴をつかみ、被害者のシステムプロファイルを標的としたエクスプロイトを実行しようとします。

エクスプロイトの選定と実装

エクスプロイトの選び方は開発者によってさまざまです。公開されたエクスプロイトコードを漁る者、個人が作成したエクスプロイトを購入する者、あるいは自分たちでエクスプロイトを開発するリソースを持っている者もいます。一部の例では、Angler エクスプロイトキットに含まれる最近のエクスプロイトに見られるように、ときには自分たちのものも含むゼロデイ脆弱性を利用することもあります。このようなやり方で、エクスプロイトの成功率が飛躍的に上がることがあります（ゼロデイ脆弱性に対するパッチは存在しないため）。成功率が上がれば、開発者はエクスプロイトキットの使用料を大幅に引き上げることができます。

エクスプロイトキットの販売開始

一般的にエクスプロイトキットの販売方法は、エクスプロイトキット開発者が頻繁に訪れる掲示板や IRC チャネルで一定の信頼を獲得している個人向けに限定されます。開発者は不正ソフトへのアクセスを誘っていますが、彼らの収入はそのソフトがどの程度の期間使用しつづけられるかにかかっています。未熟あるいは「信頼の置けない」買い手に製品の利用を許すと、開発者のビジネス（と彼らの自由）にとって多大なリスクが生じる可能性があります。

エクスプロイトキットの支払い方法には、数々の選択肢があります。よく利用されているのは Bitcoin です。また、エクスプロイトキットの開発者が、開発者のマルウェアがユーザーのマルウェアとともに被害者の機器にインストールされている間だけユーザーにキットへのアクセスを許可するケースもあります。開発者はこのような利益分配契約によって、エクスプロイトキットユーザーが獲得した被害者に開発者自身のマルウェアを便乗させることができるのです。こうして開発者は攻撃者の仕事をうまく利用し、直接的にはあまり手を下さなくても被害者へのアクセスを増やすことができます。

エクスプロイトキットの維持管理と寿命

効果的なエクスプロイトキットは、複数のエクスプロイトがバンドルされた単なるパッケージではありません。ダイナミックな市場で出回る他の製品と同様に、最大限の効果と価値を確保するにはエクスプロイトキットの積極的な維持管理が必要です。

試験と修正

エクスプロイトキットがリリースされ使用が開始されたら、開発者はキットのエクスプロイトが成功しているかどうかの統計データを監視します。特定のエクスプロイトの成功率が他より低ければ、修正を加えて効果の改善を図ったり検出を免れるようにしたりする場合があります。これは、エクスプロイトの寿命が尽きるまで行われます。検出を免れる技術としては、クライアント PC 側にインストールされたセキュリティソフトウェアの検出などが考えられます。こうすることで、セキュリティプロファイルに対して効果のあることが分かっているエクスプ

ロイトの種類をエクスプロイトキットが判断できます。そのほか、ペイロードの難読化や暗号化も検出を免れる技術の一つです。

寿命がきたエクスプロイトの削除

エンドポイントの保護システムに検出機構が組み込まれたり脆弱性の対処が行われたりするにつれ、エクスプロイトキットにとってのエクスプロイトの価値は時間とともに薄れていきます。エクスプロイトキットの管理者が寿命になったエクスプロイトを見つけた時点で、それらをエクスプロイトキットから削除します。

新しいエクスプロイトの取得

効果を失ったあるいは寿命がきたエクスプロイトが削除されたら、新しいエクスプロイトを取得して差し替えなければなりません。このプロセスは最初にエクスプロイトを取得したとき（個人所有のエクスプロイトの購入や内部開発による）と同様にすすむか、あるいは公開されたエクスプロイトコードの取得およびカスタマイズによって行われます。

エクスプロイトキット全体の寿命

エクスプロイトキット業界は競争の激しい世界です。最新あるいは効果的なエクスプロイトを維持できない、価格競争力がない、競合キットと同じような特徴や機能を提供できないエクスプロイトキットは、すぐさまユーザーを失います。また、通常エクスプロイトキットが寿命に達するのは、キットの維持管理の不備、競争力の欠如、他のキットへの吸収、法規制の徹底対策がきっかけになります。

エクスプロイトキット攻撃者のライフサイクル

攻撃活動の条件

攻撃者は単にエクスプロイトキットを購入し、ボタンをクリックし、被害者へのエクスプロイトを開始するわけではありません。エクスプロイトは、大規模攻撃の実行に必要な要素の１つにすぎません。攻撃者は通常、自らの攻撃活動を活動足らしめる明確な動機を持っています。大規模攻撃活動を行おうと考えた主な動機は、以下のいずれかの場合が多いです。

- 利益追求
- ボットネットインフラ
- 恐喝
- 野心、功名心
- ハクティビズム

大規模攻撃にはエクスプロイトのほかに、被害者を惹きつけるしくみ、配信する悪意のあるペイロード、不正利用された被害者の機器とデータを送受信する指令管理インフラが必要です。これらのリソースは、エクスプロイトキットによって提供されるわけではありません。

効果的な攻撃活動に必要な要素を下記にまとめました。各要素が実行される決まった順番はありませんが、大規模エクスプロイト方式の攻撃を成功させるには、これらの要素がそろっていなくてはなりません。

- **ペイロードの特定** — 攻撃者は、エクスプロイトキットで配信する、攻撃目標に合った悪意のあるペイロードを特定する必要があります。エクスプロイトキット攻撃者のペイロードでよくあるのは、オンライン銀行詐欺ツール、ランサムウェア、ボットネット

アプリケーションです。エクスプロイトキットがこれらのペイロードを直接提供する場合もしない場合もありますが、攻撃者は自力でペイロードを入手し、アップロードし、まき散らしていきます。

- **被害者の標的化** — エクスプロイトキットを利用した攻撃には、エクスプロイトキットのランディングページにユーザーを誘い込むしくみが必要です。これにはさまざまな方法が考えられます。以下の方法がもっとも一般的です。
    - 被害者を敵意のあるランディングページに誘い込むよう工夫されたフィッシング E メール
    - 疑うことを知らない閲覧者をランディングページに誘導するよう不正に仕組まれた公開 Web ページ
    - 悪意のあるまたは不正利用された広告によって Web サイトの閲覧者をランディングページに誘導する悪質広告

  エクスプロイトキットそのものに標的獲得機能はありません。しかし、攻撃者はスパムボット運営者など他の悪意のあるソフトウェア開発者から標的獲得機能を購入できないことはありません。

- **エクスプロイトとペイロード配信** — これが、エクスプロイトキットが果たす役割です。エクスプロイトキットのランディングページに被害者が誘い込まれると、キットが被害者の特徴をつかみ、効果のありそうなエクスプロイトを特定し、システムをエクスプロイトし、攻撃者のペイロードを送り付けます。
- **ポストエクスプロイト** — 被害者が不正利用されたあと、攻撃者にとって必要となるのは被害者のシステムのデータを管理回収するメカニズムです。指令制御インフラは一般にエクスプロイトキットによって提供されるわけではなく、攻撃者自身が開発したり購入したりする必要があります。

活動の実行と終結 — 一般的に、あるエクスプロイトキットを購入すると、そのエクスプロイトキットコンソールへの一定時間のユーザーアクセスが許可されます。その一定時間が終了すると、ユーザーのアクセス権は撤回され、エクスプロイトキットの利用は停止になり、活動は終了します。

「エクスプロイトキット — 運用ライフサイクルと最近の傾向」に関する詳細説明は、以下の項目も参照してください。

はじめに：エクスプロイトキット

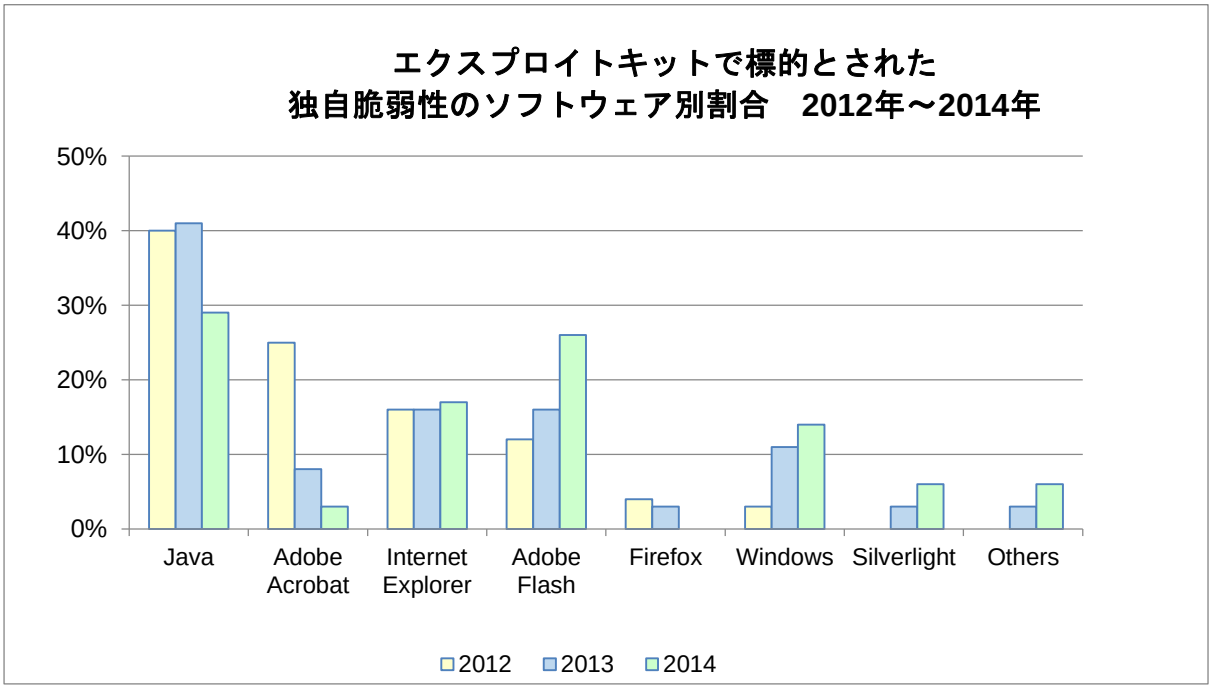
エクスプロイトキットで標的とされる脆弱性

エクスプロイトキットの月別検出数

セクション C.3：エクスプロイトキットで標的とされる脆弱性

2012 年、2013 年、2014 年にリリースされたエクスプロイトキットで標的とされた独自の脆弱性攻撃を、標的技術ごとに示したものが下のグラフです[2]。このデータには明らかな 4 つの傾向があります。

- Adobe Acrobat エクスプロイトの減少
- Java エクスプロイトの減少
- Adobe Flash エクスプロイトの増加
- 一貫して続く Internet Explorer エクスプロイト

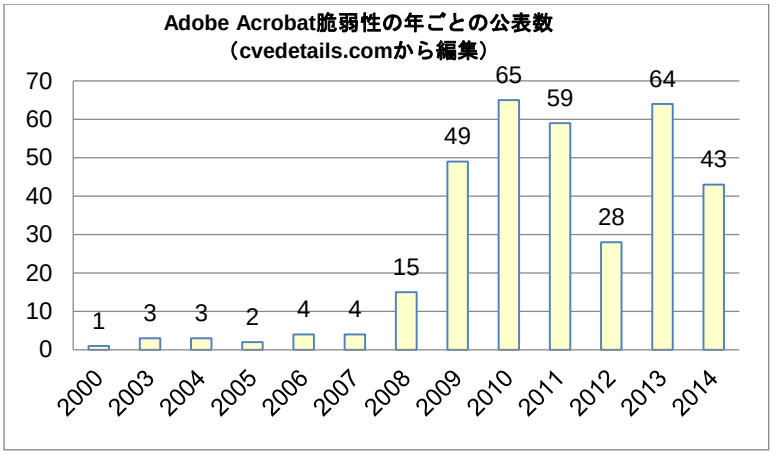


タイトル：エクスプロイトキットで標的とされた脆弱性のソフトウェア別割合（%）

上のグラフに見られる傾向について以下で説明します。

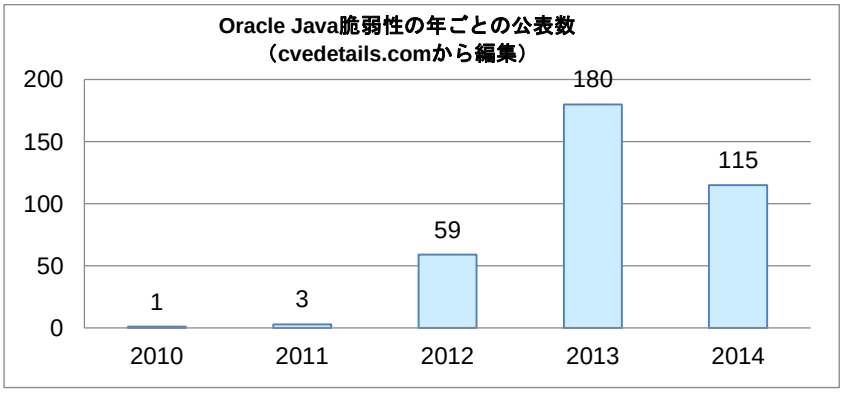
- **Adobe Acrobat 標的化の減少**　—　エクスプロイトキットにおける Adobe Acrobat エクスプロイトの使用は、2012 年から 2014 年にかけて確実に減少しています。この減少に寄与した要因の一つは、Adobe Acrobat エクスプロイトでは他のブラウザーや Flash 方式エクスプロイトに比べて必要とされるユーザーの介在度が高いことです。下のグラフに示すように、2013 年と 2014 年とでは Adobe Acrobat 脆弱性の公表数が 33 パーセント低下しています。

[2] このグラフには、過去および現在のエクスプロイトキットデータの優れたリソースである http://contagiodump.blogspot.com のデータが含まれています。



タイトル：Adobe Acrobat 脆弱性の年ごとの公表数

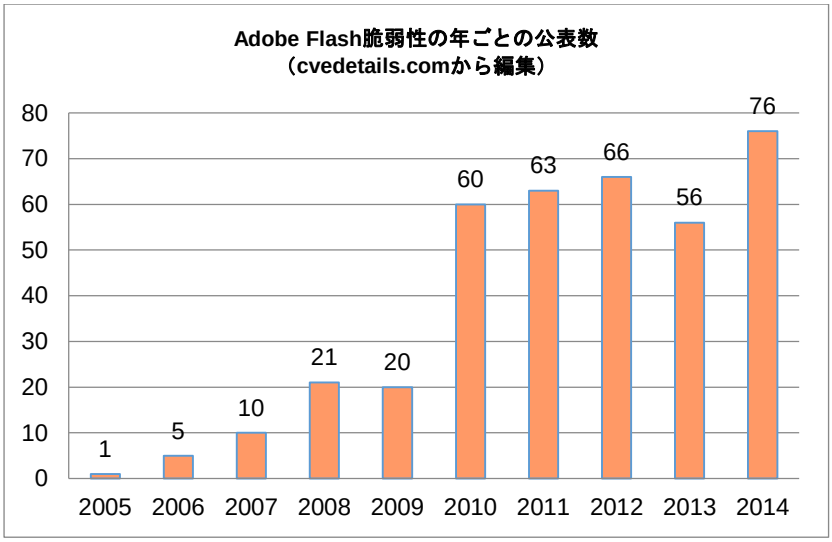
- **Java 標的化の減少** — エクスプロイトキットで標的とされた Java 脆弱性は、2013 年から 2014 年にかけて大幅に減少しています。これは、下のグラフに示すように、2014 年に確認された Java 脆弱性が 36 パーセント減少していることによるものです。



タイトル：Oracle Java 脆弱性の年ごとの公表数

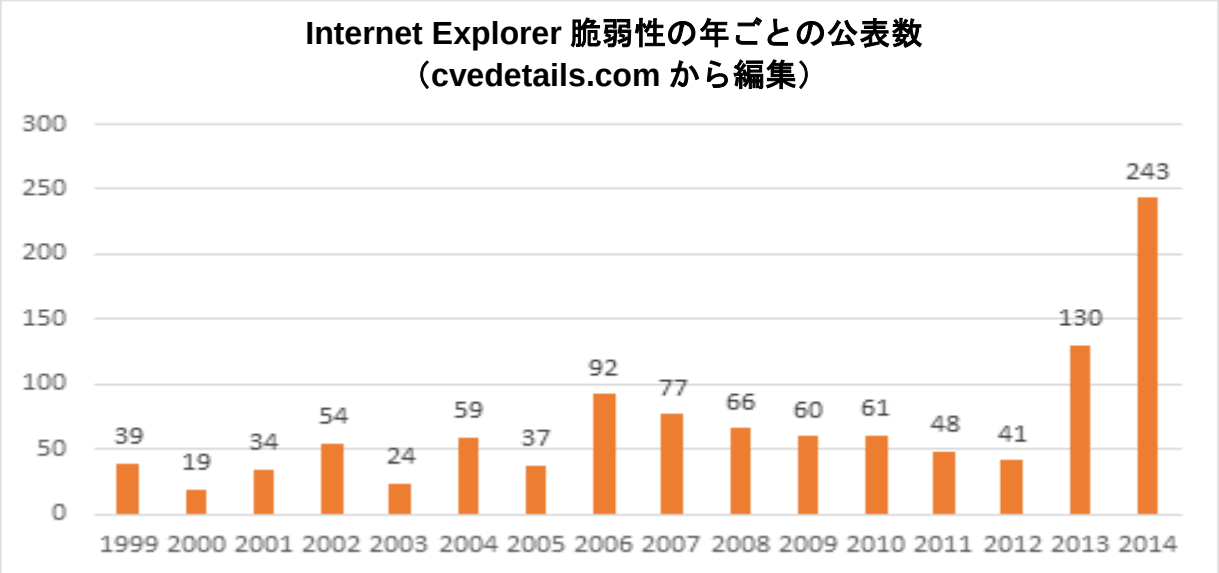
- **Adobe Flash 標的化の増加** — エクスプロイトキットにおける Adobe Flash エクスプロイトの使用は、2012 年から 2014 年にかけて増加しています。2014 年に Java と Internet Explorer のセキュリティに対して大幅な改善がなされた後[3]、エクスプロイト研究者は次第に Flash に注目するようになってきました。2014 年の Flash 脆弱性の確認数は過去最高で、下のグラフに示すように 2013 年から 36 パーセントも増加しています。

[3] FireEye は最近、従来の Adobe Flash の弱点について技術的な考察を発表しました（https://www.fireeye.com/blog/threat-research/2015/03/flash_in_2015.html）。



タイトル：Adobe Flash 脆弱性の年ごとの公表数

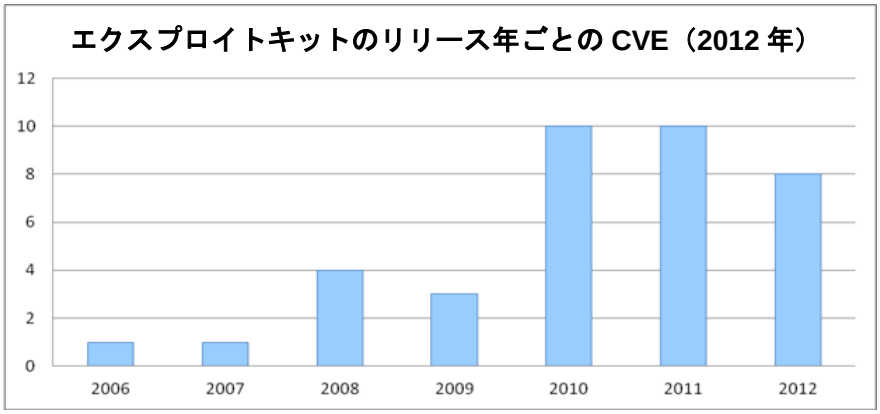
- **一貫して続く Internet Explorer の標的化** — Internet Explorer は依然として Windows オペレーティングシステム上のデフォルトブラウザーとして配布されており、企業環境のエンドユーザシステムで広く使用されています。Internet Explorer が選択のターゲットでありつづけている理由は、一般的なブラウザーであるからだけではなく、ここ数年脆弱性が相次いでいたためです。さらに重要なことに、その脆弱性の多さ（71 パーセント）ゆえに、攻撃者はリモートでのコード実行や制限の回避など猛威を振るうことができるのです。



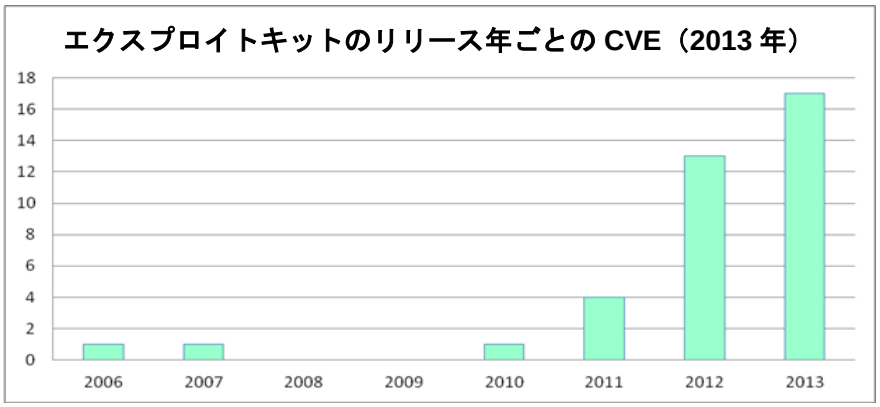
タイトル：Internet Explorer 脆弱性の年ごとの公表数

2014 年エクスプロイトキットで標的にされた脆弱性の年数別分布

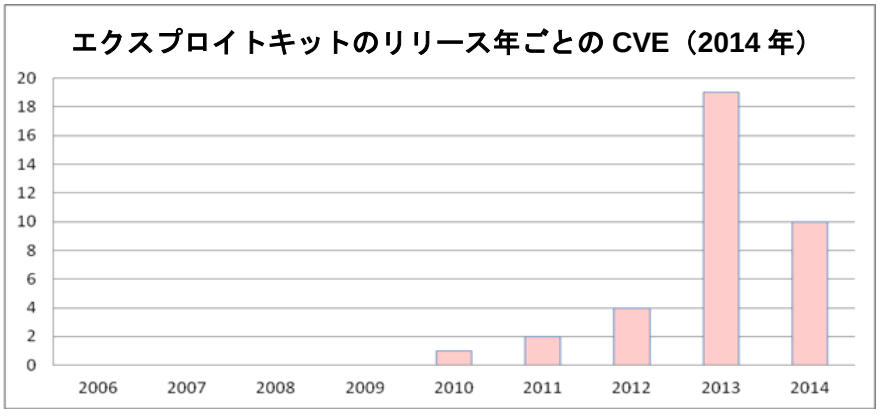
エクスプロイトキットは最新の脆弱性を利用しつづけます。以下のグラフは、2012 年から 2014 年までのエクスプロイトキットに含まれる脆弱性の年ごとの分布を示します。2012 年に NTT グループが調べたところ、エクスプロイトキットに含まれる脆弱性の平均年数は 2 年を少し下回ることが分かりました。一方、2013 年と 2014 年では、脆弱性の平均年数はわずか 1 年余りでした。この傾向から、攻撃者の手管はますます洗練されてきており、企業が対抗する機会を得る前にエクスプロイトキットをさっさと更新する能力を高めてきていることが分かります。



タイトル：エクスプロイトキットのリリース年ごとの CVE（2012 年）



タイトル：エクスプロイトキットのリリース年ごとの CVE（2013 年）



タイトル：エクスプロイトキットのリリース年ごとの CVE（2014 年）

2014 年にリリースされたエクスプロイトキットの脆弱性の 80 パーセント以上は、2013 年と 2014 年に公表されたものです。このデータは 2013 年と類似しており、この傾向は今後も続いていくとみられます。その理由は、開発者はより成功率の高い新しいエクスプロイトを組み込

むことで自らの製品を差異化しようと考えており、こうしたエクスプロイトキットの激しい競争が背景にあるためです。

2014 年のエクスプロイトキットで標的となった最多の脆弱性

2014 年にリリースされたエクスプロイトキットの脆弱性で割合が多かった 10 位までを下の表に示します[4]。

CVE	この脆弱性をエクスプロイトしたキットの割合	被害を受けたソフトウェアなど
CVE-2013-2551	62%	Microsoft Internet Explorer
CVE-2014-0515	52%	Adobe Flash
CVE-2013-0074	38%	Microsoft Silverlight
CVE-2013-2465	38%	Oracle Java SE
CVE-2013-0634	29%	Adobe Flash
CVE-2013-2460	29%	Oracle Java SE
CVE-2014-0322	29%	Microsoft Internet Explorer
CVE-2014-0497	29%	Adobe Flash
CVE-2014-0569	29%	Adobe Flash
CVE-2012-0507	24%	Oracle Java SE
CVE-2012-1723	24%	Oracle Java SE

2013 年には、エクスプロイトキットに含まれる 10 大エクスプロイトに入っていた Adobe Flash エクスプロイトは 1 つだけでした。それが 2014 年には、4 つの Adobe Flash エクスプロイトが 10 大エクスプロイトにランクインしました。2013 年は 10 大エクスプロイトのうち 8 つが Java に関係していました。2014 年は 10 大エクスプロイトのうち 4 つしか Java に関わっていませんでした。

2014 年のエクスプロイトキットで最多のエクスプロイトは、Microsoft Internet Explorer エクスプロイト（CVE-2013-2551）でした。この脆弱性はもともと、Vupen Security が発見したものです。Vupen Security はゼロデイ脆弱性の発見を専門としており、CVE-2013-2551 のエクスプロイトが 2013 年 Pwn2Own ハッキングコンテストで優勝しています。Vupen はその後、脆弱性をどのようにエクスプロイトしたかの詳しい手順を説明したブログを大々的に公開しています[5]。この公開された詳細情報は、エクスプロイトキットでいかに人気を博しているかを物語って

[4] この表は、contagiodump.blogspot.com のデータも使用しています。

[5] http://www.vupen.com/blog/20130522.Advanced_Exploitation_of_IE10_Windows8_Pwn2Own_2013.php

います。このエクスプロイトは Internet Explorer に対して確実な効果があり、それも人気の理由であるかもしれません。

「エクスプロイトキット　—　運用ライフサイクルと最近の傾向」に関する詳細説明は、以下の項目も参照してください。

はじめに：エクスプロイトキット

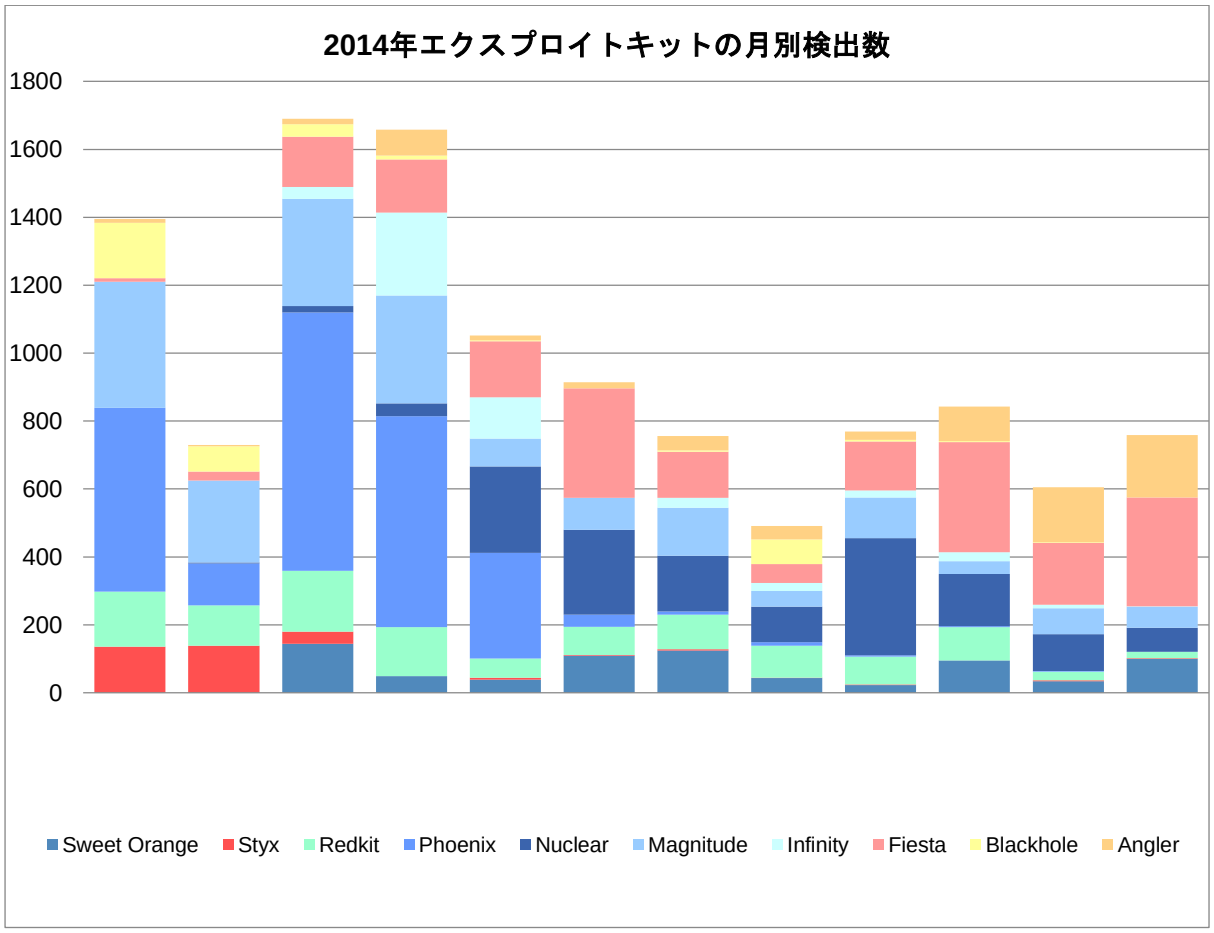
エクスプロイトキットの開発と運用ライフサイクル

エクスプロイトキットで標的とされる脆弱性

エクスプロイトキットの月別検出数

セクション C.4: エクスプロイトキットの月別検出数

014 年に NTT が検出した 10 大エクスプロイトキットの月ごとの傾向を下のグラフに示します。



タイトル：エクスプロイトキットの月別検出数（2014 年）

エクスプロイトキットは確実に検出するのが難しいものです。エクスプロイトキットを検出する最良の方法はランディングページを見つけることですが、それは常に変化します。また、エクスプロイトの人気にも潮の満ち引きのような波があり、それが月によって検出状況が変動する一因にもなっています。エクスプロイトキットはエンタープライズアプリケーションと同じようなサイクルでリリースされます。エクスプロイトキットに含まれるエクスプロイトが鮮度や効果を失くすとそのキットの人気は低下するかもしれませんが、賞味期限の過ぎたエクスプロイトが最新の効果的なエクスプロイトに置き換えられればキットの利用は増えていくでしょう。

このデータから以下のような数々の傾向を確認できます。

- **Blackhole の最終的な消滅** — 2013 年 10 月に Blackhole エクスプロイトキットの作成者「Paunch」が逮捕されてから、Blackhole に対する支持は終わりました。NTT は、かつてもてはやされたキットの使用が 2014 年をかけて縮小していき、その年の第 4 四半期に完全に消滅したことを確認しました。Blackhole は 2 年以上のあいだエクスプロイトキットのトップでありつづけ、その座を守るため積極的な維持が図られました。
- **Phoenix エクスプロイトキットの終焉** — Blackhole と同様に、NTT は 2014 年に Phoenix エクスプロイトキットがついに終焉したことを確認しました。Phoenix の開発者が 2013 年 4 月に逮捕されてから Phoenix エクスプロイトキットの活動が徐々に収縮していくのを NTT は観測しています。現在このキットは、完全に後退したとみなされています。
- **Angler の使用増加** — Angler は、最新のエクスプロイトが組み込まれていること、また古いエクスプロイトの撤退によって、現在もっとも活動的なエクスプロイトキットであるとみられます。Angler はゼロデイ Adobe Flash エクスプロイトを組み込むことで、競合キットとの差異化を図っています。こうした特徴が 2014 年後半の人気上昇につながり、Angler の Adobe Flash ゼロデイ脆弱性（CVE-2015-0311、CVE-2015-0313）のリリースで、この人気は 2015 年に入っても続いています。

エクスプロイトキットから身を守るための推奨事項

エクスプロイトキットに関連したリスクを下げるために、組織は次の手順を検討すべきです。

- **効果的なパッチ管理を確保する** — エクスプロイトキットの典型的な手法は、パッチは存在するものの適用が行われていない脆弱性に対してエクスプロイトを用いるやり方です。エクスプロイトキットの開発者が新たなエクスプロイトを配備するスピードは、最初に脆弱性が明らかになってから組織がパッチを適用するまでの時間差をうまく利用しているのです。**エンドユーザ**の機器に有効なパッチ管理プロセスを確保することが、エクスプロイトキットから身を守るのに極めて重要な最初のステップです。組織は、Java や Adobe Flash のような Web との接続ソフトや技術に特に注意を払うべきです。これらのソフトは、Microsoft プログラムに関わる企業向けのロールアウト機能と同じようなものを備えていないため、パッチの適用を実践して効果を計測するツールが配備されている状態を組織は徹底する必要があります。
- **ソーシャルエンジニアリング（フィッシング）研修** — 機密性の高いデータの維持管理やアクセスを行う組織にとって、標準的なセキュリティ意識向上の研修だけでは不十分です。鍵になる社員に対して実世界でのソーシャルエンジニアリング試験を実施し、実際のフィッシング状況の検出や対応能力を確認しなければなりません。
- **広告ブロックソフトウェア** — 攻撃者は、エクスプロイトキットのランディングページに被害者を誘い込むために、頻繁に悪質広告を利用します。広告ブロックソフト、あるいはコンテンツのフィルタリングを行うウェブプロキシーの使用によって、悪質広告の効果を抑えることができると考えられます。
- **IP レピュテーションサービス** — 悪質と分かっている IP アドレスやドメインへのアクセスを警告したり遮断したりできる IP レピュテーションサービスを利用することによって、組織のユーザーがそのようなアドレスに誤ってアクセスしてしまう事態を防止することができます。ただし、IP レピュテーションサービスは、あくまで補助的な管理ツールとみなすべきです。エクスプロイトキットのアドレスは検出を逃れるため頻繁に変わるため、ランディングページ URL の正確かつ包括的なリアルタイムリストを維持することは困難だと考えられます。
- **脅威インテリジェンス** — 脅威インテリジェンスサービスは、まさに現在積極的に In-the-Wild ウイルスリストに掲載されているウイルスによりエクスプロイトされている脆弱性を組織が特定するのに利用できます。このサービスはパッチ管理プロセスに対する補完的な管理ツールとなり、脆弱性に対するパッチ適用を優先的に実施することができます。
- **エンドポイント保護** — エンドポイント保護の実現によって、組織は多大な損害が発生する前に、エクスプロイトキットによって機器にドロップされたマルウェアの存在を検出しやすくなります。

「エクスプロイトキット — 運用ライフサイクルと最近の傾向」に関する詳細説明は、以下の項目も参照してください。

はじめに：エクスプロイトキット

エクスプロイトキットの開発と運用ライフサイクル

エクスプロイトキットで標的とされる脆弱性

セクション D：ユーザーが防衛ライン

セクション D.1：はじめに：ユーザーが防衛ライン

業界がセキュリティの防衛ラインとみなしているものが変化し続けていることを、セキュリティ専門家は以前から認識していました。IT 管理者やセキュリティ管理者は、明確なネットワーク セキュリティ防衛ラインが組織を外部の攻撃から守ってくれることなど、もはや当てにできません。データはユーザーの間に分散しており、ユーザーは、一貫した制御が難しい、高度にモバイル化された環境の中に存在しています。

歴史的に見て、変化する防衛ラインの概念は、主として検証可能な事実としてではなく、エピソードによって逸話的に形作られてきました。2014 年を通じて NTT グループでは、脆弱性と攻撃に関する膨大な量のデータの収集を行い、崩壊しつつある防衛ラインの概念を裏付けました。具体的に言うと、ユーザーが防衛ラインであるということです。（「ユーザーは攻撃を受けやすい」の項を参照）

ユーザー エンドポイントに対する攻撃および Flash、Java および Adobe によくみられる脆弱性による感染率に関する詳細な分析には、これまでの年に見られていたものよりも予測のつきやすい特徴がありました。組織のセキュリティ コントロールは、1 週間のユーザの就業日パターンに相関する傾向を攻撃の中に見出しました。マルウェアのトラフィックは、従業員がオフィスに戻ってくる週初めに急上昇し、同じように、検出済み感染率と攻撃数においては週末に減少しています（「週末の傾向」の項を参照）。これはなぜでしょうか。

マルウェアはますます複雑なものとなり、ハッカーは、エクスプロイト・キットを加速度的に使用して、攻撃対象の環境で効き目の大きいマルウェアを送り込むようになってきました。しかし、ユーザーを標的とした攻撃は通常、そのユーザーが勤務する組織ネットワークへアクセスするための入口です。たとえば、今年 POS マルウェアが使われた小売業者に対する攻撃の中には、**エンドユーザ**を標的としたフィッシング攻撃から生まれたものがありました。ビジネスマインドを持ちあわせた攻撃者は、セキュリティシステムの中で最も弱いリンクである**エンドユーザ**を特に重視することで効率化をはかっていると思われます。（ケーススタディ「スピアフィッシング活動」参照）。

デジタルビジネスは、利用可能なデータをどれだけ効率的に使用できるかがポイントです。犯罪組織も同様に、データの価値を利用しようと攻撃目標との競争を続けています。**エンドユーザ**による企業データへの恒常的なリアルタイムアクセスが一般化するにつれて、ますます**エンドユーザ**は同じデータソースを欲しがる攻撃者の標的となっていきます。さらに悪いことに、あまりに多くの場合において、こういったユーザーこそ攻撃者が会社に侵入する入口となるのです。

「ユーザーが防衛ライン」に関しては、以下の項目も参照してください。

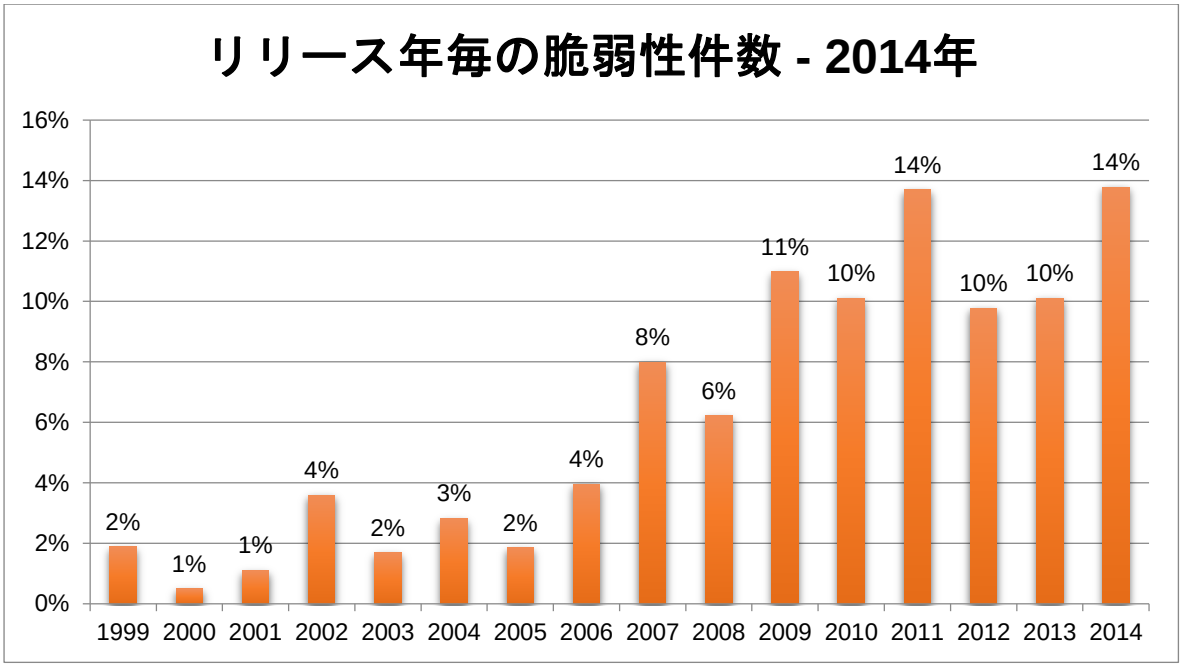
セクション D.2：ユーザーは攻撃を受けやすい

NTT グループでは 2014 年を通じて、クライアントのシステムに非常に多くの脆弱性を目にしてきました。これらの脆弱性の一部からその詳細を調べてみると、上位 10 位の中で 7 種類の脆弱性がサーバーではなく、**エンドユーザ**のシステムに存在していたことなど、興味深い情報がいくつか明らかになってきました。これが実際の攻撃に与えている影響については、「週末の傾向」を参照してください。

上位 10 位の脆弱性
旧バージョンの Java Runtime Environment
Oracle Java SE 重要パッチアップデート
Java Web Start に存在する複数の脆弱性
MS Windows セキュリティアップデートの適用漏れ
旧バージョンの Flash Player
旧バージョンの Adobe Reader と Acrobat
旧バージョンの Internet Explorer
Oracle の複数の脆弱性
旧バージョンもしくはパッチ適用漏れの Oracle DB
旧バージョンの OpenSSH

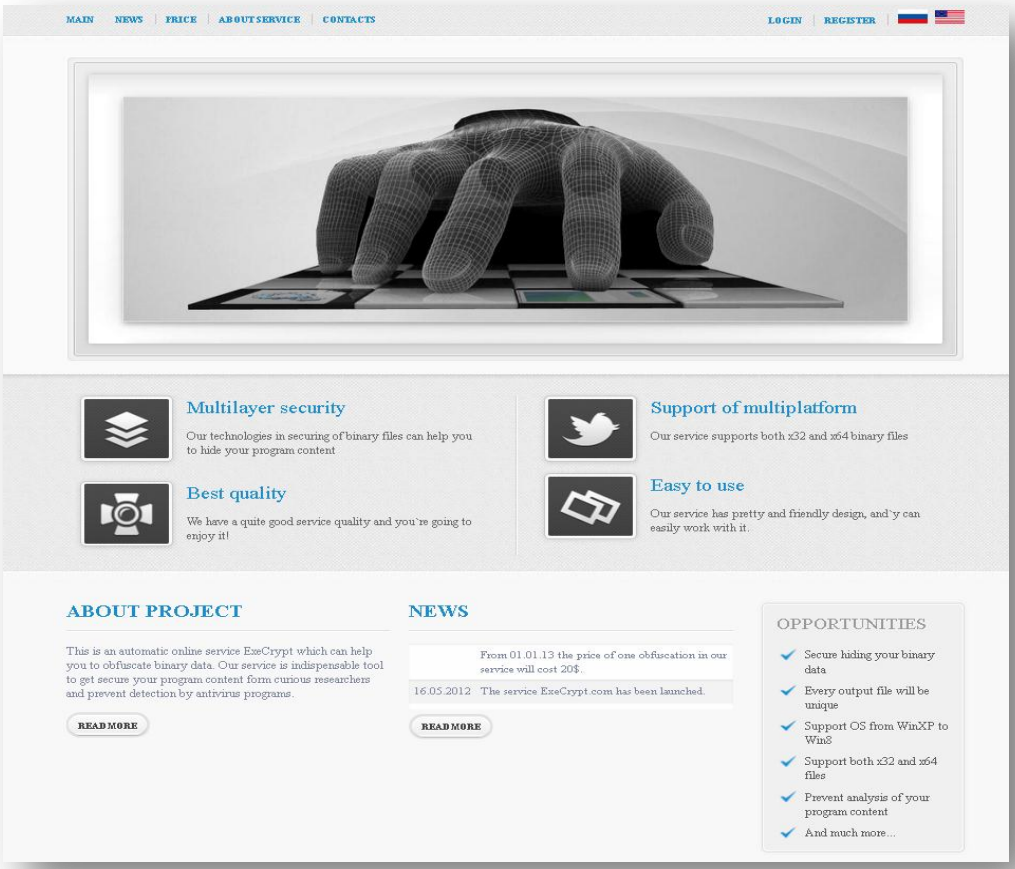
タイトル：2014 年において最も頻度の高い脆弱性上位 10 位

一番大きな影響は、多くの場合、**エンドユーザ**のシステムはパッチが当てられていない脆弱性だらけであることから、**エンドユーザ**が弱点となることです。このレポートが作成された時点では、2014 年の上位 10 位の脆弱性すべてに対して、その影響を緩和するパッチが入手可能でした。システムにパッチを適用して最新の状態としておくのは時間がかかる面倒な作業ですし、特に、高度にモバイル化され、様々な種類のハードウェアとソフトウェアが混在した環境を地理的に分散した状況でかかえる組織では、非常に困難な場合もあります。



タイトル：2014 年に検出された脆弱性のリリース年毎の割合

2014 年の 1 年間に企業の全システムで確認された脆弱性の 76 パーセントが 2012 年もしくはそれ以前のもの、すなわち 2 年以上経過しているものであり、9 パーセント近くが 10 年以上前から存在するものでした。脆弱性の多くが操作が簡単なエクスプロイト キットに速やかに組み込まれているため、攻撃者は、一連の作戦の一部として難なく使用できるようになってきました（詳細は「エクスプロイト」の章を参照）。



タイトル：暗号化ツールを販売しているダークウェブ上の Web サイトの 1 ページ。サポートとセキュリティが含まれている。

幸いなことに、クライアントが原因となる脆弱性による露出を低減するために、各組織が取り得るベストな手段が 1 つだけですが、存在します。各組織は、脆弱性管理プログラムを改善することです。具体的には、あらゆる**エンドユーザ**のクライアントシステムが自組織のパッチ管理プロセスの対象とすることを徹底します。実のところ、これは見かけよりもずっと複雑なものであり、以下のように多様な関連推奨事項が含まれることもあります。

- **エンドユーザ**のマシンのセキュリティ強度を増し、管理するために、設定内容を定義します。そこには、許可されるオペレーティング システム、アプリケーション、ユーティリティに加えて、どのブラウザが組織に関する用途にサポートされているのかまでも定義されている必要があります。組織が自らの「基準となる標準」をよりコンパクトでより一貫性を持ったものとするほど、その標準を用いたシステムの維持は簡単になります。
- ユーザーに対してこの標準の内容を明確に伝えた上で、「許可されない」ソフトウェアは単に許可されないだけではなく、不正であることを明確にします。不正なソフトウェアを使用すると懲戒処分の対象となり得ることを、すべてのユーザーに対して明確にします。

- 不正なものかもしれないソフトウェアを念頭に、新規ソフトウェアのインストールなど、システム構成の変更が可能な管理者アカウントの使用は最低限に抑えます。
- 定期的かつ能動的に**エンドユーザ**システムにパッチ適用を実施し、パッチがインストールされていることを確認します。
- 内外から認証を受けた脆弱性スキャンを定期的に実行してポリシーから外れたシステムを特定し、検出されたシステムにはパッチを適用します。
- 「特別」なソフトウェアや高い権限が与えられたユーザーを追跡する例外プロセス管理を積極的に進めます。

「ユーザーが防衛ライン」に関しては、以下の項目も参照してください。

ユーザーが防衛ライン

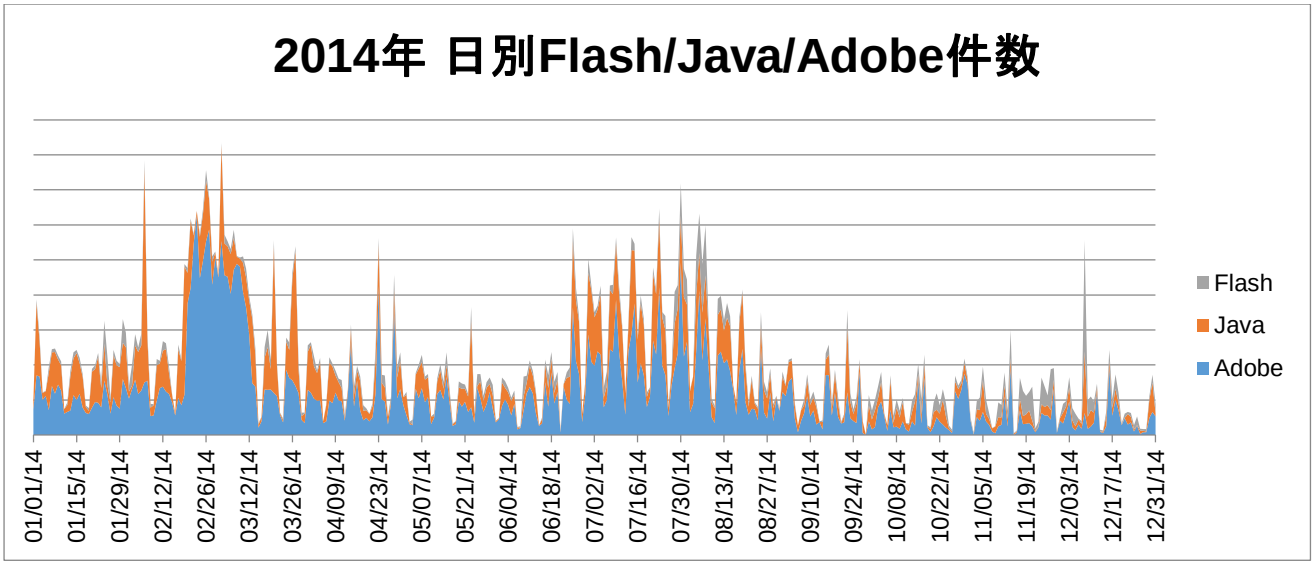
週末の傾向

ケーススタディ「スピア フィッシング活動」

セクション D.3：週末の傾向

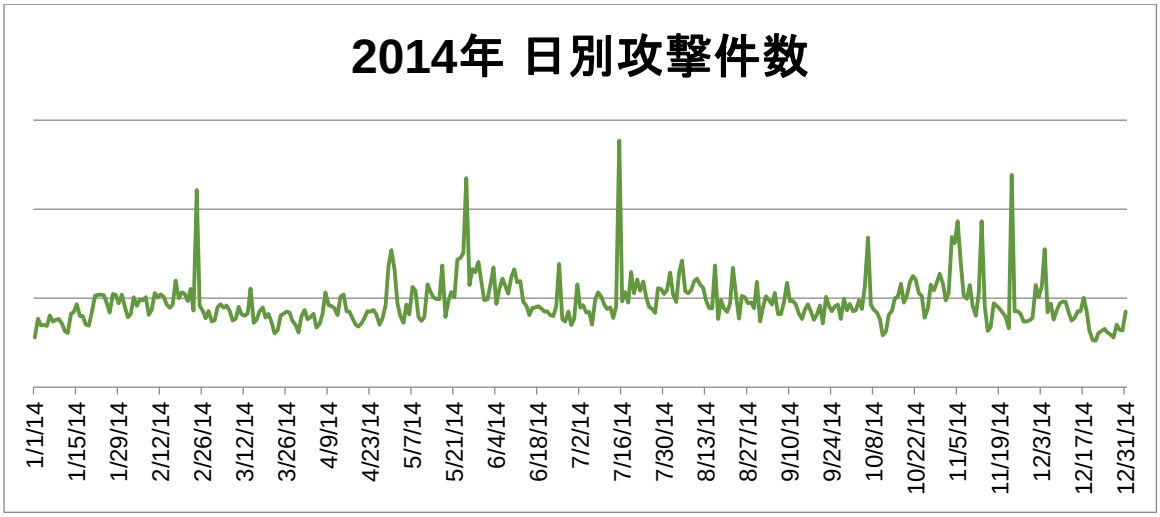
「ユーザーは攻撃を受けやすい」の項では、どれだけの重大な脆弱性がサーバーではなく**エンドユーザ**マシンに関するものであるかについて扱いました。しかし、**エンドユーザ**システムの脆弱性は、どのシステムが攻撃を受けているかという点と関係があるのでしょうか。

次のグラフは、2014 年に NTT グループが検出した Flash/Java/Adobe（Acrobat と Acrobat Reader）に対するエクスプロイトの回数を示しています。このグラフには、年間を通じて定期的に活動が行われており、攻撃検出数が増えるほど期間が短いことが表れています。大幅な急上昇は重なることの多いイベントの組み合わせであり、過去の脆弱性に対する新たなベンダーシグネチャ、偽陽性の警告を発生させる傾向のある未確認のシグネチャ、および本当に新しい脆弱性や活動が警告のトリガとなった際に発生しています。ただし、データを詳しく調べてみると、それ以外にも興味深い傾向があることがわかります。検出された攻撃の定期的な落ち込みは、完全に週末と一致しているのです。



タイトル - グラフの落ち込みは、通常はユーザーが企業ネットワークにアクセスしない週末に発生

この週末の傾向は、Flash/Java/Adobe のエクスプロイトに限ったものではありません。次の図には、2014 年 1 年間のインターネットをベースとするあらゆる攻撃の規模が示されています。Flash/Java/Adobe の攻撃の検出とよく似て、インターネットをベースとする全攻撃の図には、年間を通じてある一定の規則性がみられます。この図にもまた、1 週間にわたって検出件数が一定である中に、ちょうど週末に攻撃数に落ち込みが見られるという、同じような規則的傾向が示されています。この現象は、週末には攻撃が少ないということを意味しているのでしょうか。



タイトル：2014 年のインターネットをベースとする攻撃の年間表示

歴史的にサイバー犯罪の標的となってきた Web サイト、e コマース サイト、アプリケーションおよびシステムに対する攻撃に、曜日が関係するとは思えません。それどころか、人員配置や監視のレベルが下がる週末に増えると予想できそうです。

しかし、2014 年の 1 年間を通じて NTT グループが監視を行った組織のセキュリティ インフラストラクチャでは、検出される攻撃の件数は週末や祝日に決まって、大幅に減少しました。週末や祝日には、従業員はオフィスに出社しておらず、企業の**エンドユーザ** システムは電源が切られているか、使用されていないかのいずれかです。週末の攻撃件数がかなり落ち込むのは、組織の監視システムが**エンドユーザ**に関連するセキュリティ イベントを対象としていることの証明にもなっています。この**エンドユーザ**関連の特性は、検出されるすべての攻撃において重要な構成要素となっています。

各組織では、**エンドユーザ**システムに対する攻撃の効果を軽減する措置を講ずることができます。

- 組織のネットワークやデータにアクセス可能なあらゆる**エンドユーザ** デバイス上で、最新で有効なアンチウイルス／アンチマルウェア ソリューションを維持します。これは単純な対策ですが、適切に管理されたアンチウイルスは、40～50 パーセントのマルウェアを検出します。
- ファイルの完全性監視、エンドポイント暗号化、イベント監視などの拡張されたエンドポイント保護を検討します。
- 管理者アカウントの使用は最小限とします。ユーザーは、自分の作業を行うために最低限必要となるレベルの権限を持つユーザーレベルのパスワードでログオンさせるようにします。管理者アクセス権を用いてブラウジングするとリスクが増加します。
- 稼動中のすべてのコンピューターは、業務中であるか否かに関わらず、組織の VPN を通じてインターネットにアクセスさせるようにします。ブラックリストにある Web サイトを含めて、VPN 接続を通じた安全なブラウジングの習慣をつけることと、組織がセキュリティへの攻撃や不正利用を確実に検出できるように、ポータブルなラップトップには常時能動的なセキュリティ監視を行うことを徹底します。
- **エンドユーザ**システム用の、攻撃に対するトレーニングが含まれたセキュリティリテラシー向上に関するプログラムを提供します。組織のトレーニングプログラムには、ソーシャル エンジニアリングとフィッシングが含まれるようにします。
- **エンドユーザ** データをオフラインでバックアップして、ローカルシステムに対する不正利用、マルウェア、およびランサムウェアによる影響を最小限に抑えます。
- プロキシおよびコンテンツ フィルタリング機能の実装と監視を行います。

「ユーザーが防衛ライン」に関しては、以下の項目も参照してください。

ユーザーが防衛ライン

ユーザーは攻撃を受けやすい

セクション D.4：ケーススタディ「スピア フィッシング活動」

ケーススタディの教訓

攻撃の成功には、技術的先進性は必要ではありません。

概要

2014 年 8 月、Aerobanet（クライアントが特定されないように名前を変えてあります）は NTT グループに連絡を取って、スピア フィッシング攻撃と疑われる事象に対する助力を求めました。

NTT グループでは、Aerobanet が巧妙に仕組まれたソーシャル エンジニアリング／フィッシング活動の対象となっていることを突き止めました。この活動では、Aerobanet 社内の電信送金要求および承認プロセスに関する詳細な知識を用いて、虚偽の電信送金を完了させるように担当者を欺いていました。NTT グループのセキュリティ コンサルタントは、この攻撃に対する迅速な調査と対策を支援しました。

イベントの時系列

以下の表にイベントの時系列を示します。

日付	イベント
1 日目	電信送金の指示が書かれたフィッシングの最初の電子メールを受信
2 日目	Aerobanet は、最初の指示に従って資金を送金
5 日目	電信送金を要求する 2 番目の電子メールを受信
6 日目	電信送金を依頼する 3 番目の電子メールを受信
9 日目	Aerobanet では電信送金の処理中に疑問を抱き、NTT グループに連絡を取って詐欺的なフィッシング電子メールの調査を開始
9～11 日目	NTT グループは詐欺的な電子メールの精査と偽サーバーの調査を行い、追加の内部レビューを開始
15 日目	NTT グループではマルウェアは存在しないものと断定し、この攻撃はソーシャル エンジニアリング／フィッシング攻撃と特定

タイトル：イベントの時系列 - スピア フィッシング

イベントの説明

2014 年 8 月、電信送金が何回か成功した後、Aerobanet は、資金の電信送金を依頼する電子メールに疑念をいだきました。その疑念が浮上したのは、通常より高い頻度で電信送金が短期間に行われていることに担当者が気づいたときでした。Aerobanet は NTT グループに連絡を取って、疑惑の検証と攻撃調査の支援を依頼しました。

初期調査によって、攻撃はフィッシング メールを通じて行われていたことが確認されました。この電子メールは巧妙に作成されており、Aerobanet 社内のプロセスと従業員の役割について詳しい知識を攻撃者が持っていることを示唆する次のような点を含んでいました。

- 攻撃者は、電信送金を開始するには社内のどのユーザーを標的とすべきか知っていました。
- 攻撃者は、電信送金を承認できるユーザーが誰であるかの内部情報を持っていました。
- 電子メールには、電信送金が承認されたように見せかけるための偽のメール スレッド履歴が含まれていました。

- 電子メールには、その電子メールが公的なものと見せかけるように作成された PDF が添付されていました。
- 電子メールには、公的なものと見せかけるために、正規に登録されている有効なドメインが使用されていました。このドメインは、サードパーティーのクラウドベースのプロビジョニング サイトを経由して登録されていました。

この電子メールは、電信送金に不可欠な情報と指示内容が含まれるように作成されていました。偽のメール スレッド履歴には数日分のメールが含まれているように見せかけられており、そこには、正当な従業員が送金の依頼と承認を行ったかのような電子メールが含まれていました。電子メールの作成に用いられた詳細度からは、攻撃者が Aerobanet 社内のプロセスや手順に関する知識を持っていることが示唆されていました。NTT グループのセキュリティ アナリストは、Aerobanet に関する攻撃者の知識がソーシャルエンジニアリングによるものか、それ以外の情報源から得られたものかの特定には至りませんでした。

NTT グループでは、これと類似したスピア フィッシング攻撃の増加を捕捉していました。このことは、オンサイト アナリストが Aerobanet に対する攻撃の性質を明らかにし、フィッシング攻撃であることを検証する際に大いに役立ちました。セキュリティ コンサルタントは、フィッシングメールのドメインが Aerobanet の正しいドメインとは微妙に異なっていることに気づきました。この攻撃者は、無料で試用できるドメイン サービスを利用して、攻撃で用いた有効なドメインの作成と登録を行いました。NTT グループでは、攻撃者がクラウドの提供するドメインを使用することが増えていると認識していますが、その理由は、これらのサイトは安価（または無料）であり、設定が簡単で、速やかに利用可能であるためです。このケースでは、クラウドが提供するドメインが不正な電子メール ドメインとして利用されました。

Aerobanet に対して、攻撃者は実際の攻撃対象によく似た「Aerobannet」というドメイン名を用意しました。フィッシング メールの受信者は、偽のドメイン名の中に余分な「n」があることを認識していませんでした。これによって、攻撃者は、電信送金に関する電子メールのやり取りに自分が含まれるように出来ました。攻撃者は、偽の Aerobannet サイト上に電子メール アカウントを作成しましたが、この名前に電信送金の承認に責任を持つ実在する Aerobanet の役員の名前を用いました（johndoe@aerobanet.com に対して johndoe@aerobannet.com）。従業員は社内ユーザーからの電子メールに対応しているものと信じ込んでいましたが、実際には、攻撃者の偽の社外電子メール アカウントとやり取りをしていたのです。

電子メールには、電信送金に対する郵送先住所と口座番号が示された PDF ファイルも添付されていました。この添付ファイルによって、電信送金の依頼に対する信用度が増しました。PDF の分析を行いましたが、マルウェアは検出されませんでした。PDF に書かれた住所は、住宅地の住所でした。

NTT グループの解析では、攻撃者が Aerobanet のインフラストラクチャに侵入したことを示す証拠はありませんでした。アナリストの分析では、マルウェアと環境への内部アクセスのどちらも検知していません。ソーシャル エンジニアリング技術やスピア フィッシング技術に限定された攻撃は比較的珍しいものですが、この攻撃のように専門家により仕組まれたものである場合には、成功率がとても高くなります。NTT グループでは昨年中にこのような攻撃シナリオをいくつか目にしてきており、この種の攻撃者の成功率は高まっているものと思われます。

NTT グループのセキュリティ コンサルタントは、無料で試用可能なドメインがこの攻撃においてどのような役割を担ったかを説明し、電信送金が偽のものであったことを示す資料を提供しました。Aerobanet はこの資料を銀行に提供し、不正送金された資金のほぼ全額の払い戻しを受けることができました。

その後、Aerobanet では承認プロセスを変更して、あらゆる電信送金は事前に、本人に直接会うか電話による確認を行ってから実行するものとしました。

根本的原因

この攻撃が成功したのは、非常に正確で目標が明確な一連の電子メールによって、Aerobanet の担当者がこの電信送金は真正なものであると信じ込んだことによります。この攻撃で使用された偽ドメインによって一連の電子メールに信頼性が加わり、その結果、スピアフィッシング攻撃が成功したのです。

インシデントのコスト

Aerobanet がこのイベントにおいて実際にかかったコストの情報を提供してくれました。

品目	コスト
上記の調査、改善、および専門家による インシデントサポートの実コスト	$15,400
弁護士および広告宣伝に関するサポートの実コスト	$8,775
電信送金による潜在的損失額	$127,530
電信送金回収額	-$126,630
イベントに直接関連する実コストの総額	$25,075

タイトル：イベントのコスト - スピア フィッシング

ケーススタディのまとめ

通常、スピア フィッシング攻撃はそれ以上に高度な攻撃の第 1 段階であり、それ自身が攻撃として機能することは滅多にありません。このケースでは、高度に標的が絞られたスピア フィッシング メールのスレッドが仕立て上げられており、偽の電信送金依頼を担当者が信じこんでしまいました。この電子メールには妥当な依頼者と適切なやり取りが含まれており、あたかも社内ドメインから発信されたものであるかのように見えたため、社内担当者は、すぐには依頼を疑うことはありませんでした。その結果として、担当者は疑念が持ち上がる前に電信送金を何回か実行してしまいました。

脅威への緩和策 — スピア フィッシング

各組織は、スピア フィッシング攻撃を防御する各種のセキュリティ コントロールについて検討する必要があります。

- **対象を絞ったセキュリティ意識トレーニングの実施**：攻撃者はスピア フィッシング攻撃を実行して成功しました。ソーシャル エンジニアリングおよびフィッシング攻撃を自ら見つけるためのガイダンスが含まれるセキュリティ意識向上トレーニングを、Aerobanet がそれ以前に実施していたならば、この攻撃はもっと早く認識されていたかもしれません。このようなトレーニングでは、受講の対象となる組織の状況を考慮する必要があります。企業のプロセスや手順に合わせてカスタマイズし、従業員が関係する可能性のある攻撃の事例を用いる必要があります。
- **ソーシャル エンジニアリング テストの実施**：重要な業務を管理する社員には、トレーニング以上の試験を行う必要があります。ソーシャル エンジニアリングの専門家とともに試験を行い、進行中の攻撃を特定するスキルを試します。重大な脅威の多くは、ソーシャル エンジニアリング攻撃から始まります。重要な社員が攻撃の検出に対する適切な用意が確実に出来ているようにするのは、技術的なシステムを強化して攻撃に耐えるようにするのと同じぐらい重要です。
- **重要取引に対する二重コントロールの導入**：攻撃者は、電信送金が承認されたかのように見せかけた電子メール スレッドの中に、十分な情報を入れ込んでいました。電子メール通信とは別の経路で 2 次承認を得るための確認プロセスを組み込むことにより、送金実行の企てに対して注意信号を示すことが出来たかもしれません。（電話、FAX、紙コピーによる）能動的な確認があれば、その送金が本当に承認されたものであるかを検証するやり取りが追加で行われていたことでしょう。
- **電子メール DNS 検証の構成**：スピア フィッシング攻撃が成功するためには、複数レイヤのインフラストラクチャを欺く必要があります。電子メール サーバーに Sender ID Framework を構成して、送信者が適切な IP アドレスを使用していることを確認するのが重要な理由はここにあります。この技術を用いると、送信者が受信者に電子メールを送信した際に、受信者の電子メール サーバーは Sender ID Framework に問い合わせを行います。Sender ID Framework は、ソース IP アドレスが電子メールの送信されたドメインと一致するかどうか照合するように、DNS サーバーに依頼します。IP アドレスが一致しない場合には、その電子メールはブロックか廃棄が行われます。一致した場合には、受信者に転送されます。今回のようなフィッシング攻撃の多くで行われているように、電子メール アドレスがメール ヘッダの中で詐称された場合には、この処理は効果があります。ただし、（攻撃者が Aerobanet/Aerobannet に対して行ったように）攻撃者が攻撃対象のドメインに似たドメインを立ち上げて、その類似の「偽造」ドメインに対する DNS レコードを管理した場合には、DNS 照合は効果的ではありません。

- **電子メール フィッシング信頼度レベルの構成**：フィッシング信頼度レベル（PCL）は、Microsoft Exchange 環境を通じて入手可能なツールです。このツールは 1 から 8 までのスケールを持つ値を生成しますが、この値には、ある電子メールがフィッシング攻撃の一部であるかの可能性が反映されています。そのサイトの電子メール管理者は、PCL 値スケールにおける格付けに応じて、それぞれの電子メールをどのように処理するかを選択可能となり、更なる脅威の特定や攻撃全体の阻止に役立つことがあります。
- **異常／詐欺検出の導入**：この攻撃は、電信送金のパターンが変則的であることに担当者の 1 人が気づいたことから特定されました。この担当者は、電信送金依頼の回数が著しく増加していることに気づき、想定される限度額を超えていたことから、直近の依頼を点検しました。大量の取引を処理する可能性のある大きな組織ではとりわけ、このような変則的な行いを識別できる能力は貴重なものです。今回のようなインシデントでは、手作業によるチェックと、可能な範囲で自動化されたチェックを導入して、慎重な取り扱いを要する取引の頻度や規模が予想範囲を超えることを識別することが組織に必要となります。金融機関の中には、組織が取引限度額の設定と確認を行う支援を行うところもあります。

セクション E：インシデント対応

セクション E.1：はじめに

インシデント対応: 企業の能力は徐々に成熟

2014 年は、セキュリティとビジネス両方の統率者に対して、サイバー攻撃が組織にどれだけの影響を与えるのかの評価を促す年でもありました。この年には、著名で広く知られた数多くのブランドが悪意のある行為者の標的となりました。

非常に馴染みのある多くのブランドがニュースの見出しを賑わしましたが、それは同様な脅威や損失による影響を被ったたくさんの組織の一部に過ぎません。

脅威の影響範囲を左右する重要な要因の 1 つには、その脅威の特定、隔離、被害の軽減に対する組織の有効度があります。一般的に、組織が有効な方法で迅速に対応できるほど、脅威の影響を制御できる可能性が大きくなります。

NTT グループでは、さまざまな業界のインシデント対応に関わっており、どの業界も攻撃を免れないことを示してきました。どの業界であっても有効なインシデント対応が必要です。

「インシデント対応」に関しては、以下の項目も参照してください。

インシデント対応の種類

分野別インシデント

インシデント対応の重要性

インシデント調査に基づく 5 つの重要推奨事項

脅威インテリジェンスの定義

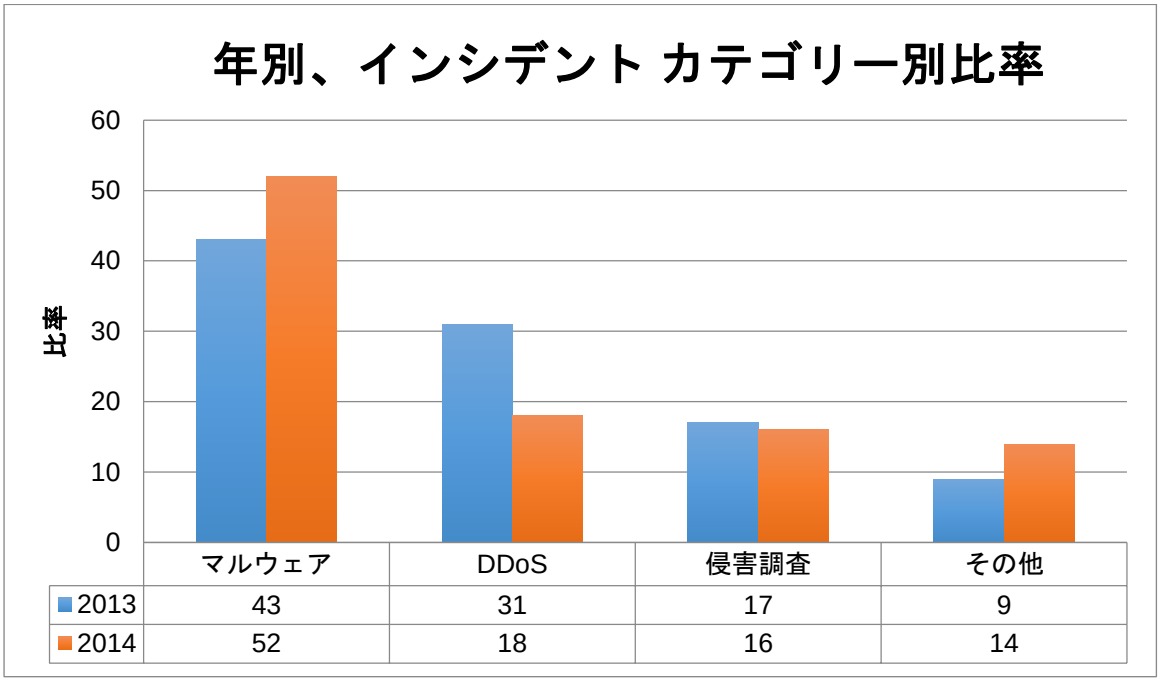
セクション E.2：インシデント対応の種類

2014 年に行った NTT によるインシデント対応は、3 種類のインシデントカテゴリー（マルウェア、DDoS、および脅威に関する調査）以外にはほとんど無かったという結果でした。マルウェアおよび DDoS をベースとする対応のカテゴリーの監視結果にはわずかな変化がありましたが、2014 年の全般的な傾向としては、これまでの監視結果と一致するものでした。

マルウェアの性能は、攻撃者による配布方法と残存性能の進歩に伴い、進化を続けています。2014 年のマルウェア関連脅威の件数には増加が認められますが、マルウェア関連のインシデント対応活動の大部分で、潜在的な感染による影響の確認と改善方法に関するガイダンスが必要でした。今日の組織はマルウェアの脅威に関する知識が豊かとなっており、被害軽減策にも投資を行ってはいるものの、その大半においては、発見したマルウェアの検疫と根絶を行う方法、マルウェア関連のインシデントの取り扱い方法の理解にいまだ問題を抱えていることが、この結果から明かとなっています。

DDoS 攻撃に対する意識と優先度が向上したことにより、2014 年の被害軽減策には進歩が見られました。DDoS 被害軽減ツールが成熟し、そのコストが下がって導入数が拡大したことが、2014 年に確認された DDoS 攻撃の減少に貢献する要素であったと思われます。DDoS 攻撃に関するインシデント対応調査の比率は急減しました（2013 年の 31 パーセントから 2014 年の 18 パーセントへ。次のグラフ参照）。これまでに確認された攻撃やそれらに関する議論、有力ブランドに対する DDoS 攻撃に関する主要メディアの報道は、このような攻撃を管理する能力に対して大きな影響を与えたものと思われます。

次のグラフは、2013 年と 2014 年における NTT グループによるインシデント対応の傾向を示しています。



タイトル：年別のインシデント カテゴリー比率

「インシデント対応」に関しては、以下の項目も参照してください。

はじめに：インシデント対応

分野別インシデント

インシデント対応の重要性

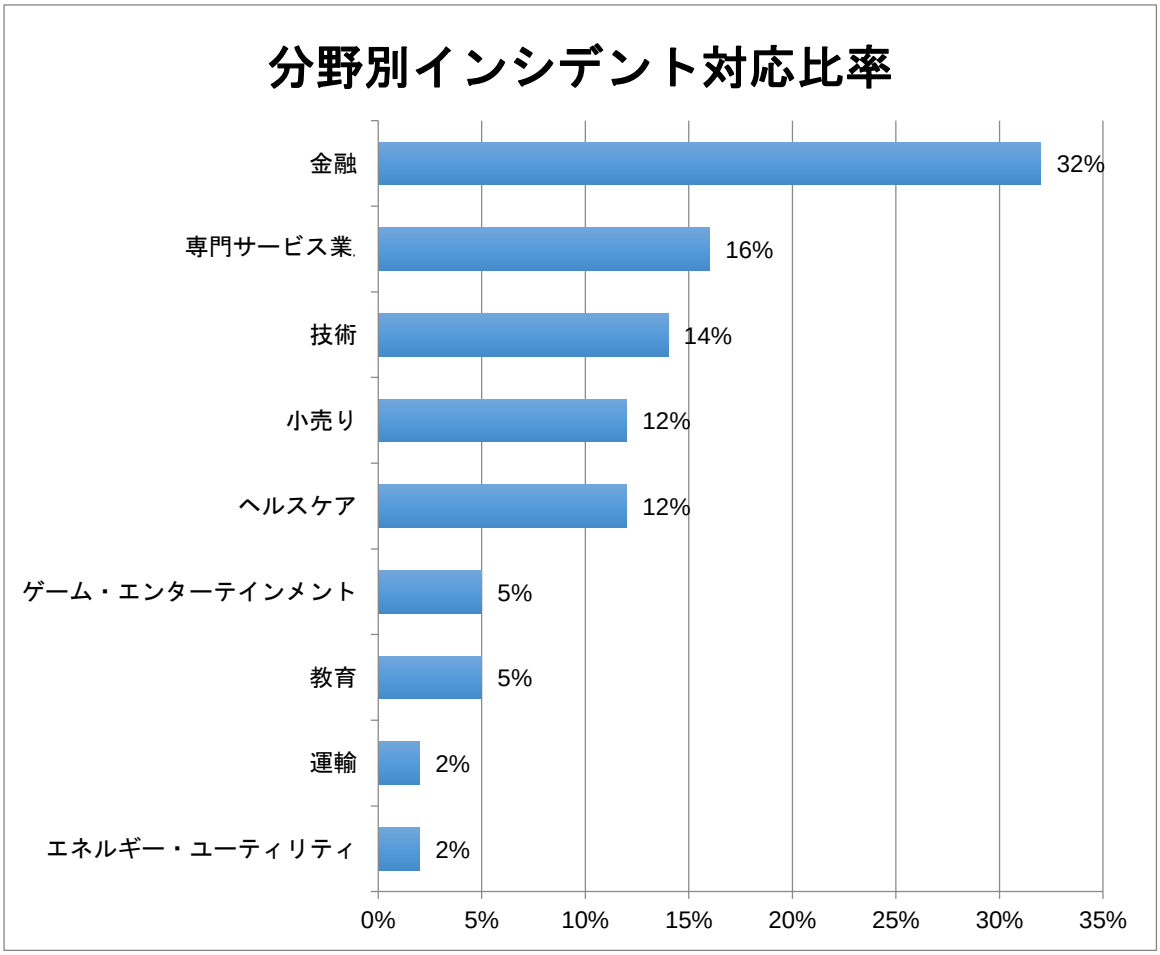
インシデント調査に基づく 5 つの重要推奨事項

脅威インテリジェンスの定義

セクション E.3：分野別インシデント

市場分野別インシデント対応

NTT グループの 2014 年のインシデント対応を次のグラフのように、いくつかの業種に分類してみました。この中には統計的に目立たない業種もあるにせよ、いずれの業種においても、組織におけるセキュリティ管理策には、公式のインシデント対応のプロセスと手順が含まれているべきです。金融分野のインシデント対応サポート活動の比率が高いのは、主として、この業種に攻撃者が常に関心を持っており、この業界が攻撃にセンシティブであるからです。



タイトル 分野別インシデント対応比率

「インシデント対応」に関しては、以下の項目も参照してください。

はじめに：インシデント対応

インシデント対応の種類

インシデント対応の重要性

インシデント調査に基づく 5 つの重要推奨事項

脅威インテリジェンスの定義

セクション E.4：インシデント対応の重要性

NTT グループでは、各組織のインシデント対応体制に一定の成熟が見られることは認識していますが、大半の場合、その対応は受動的（脅威が直接的影響を及ぼしてから組織がリソースを確保すること）なままです。NTT グループの観測結果によれば、先を見越してインシデントへの準備を行っている組織はほとんどありません。昨年版の GTIR にも述べた通り、基本的な体制を予め確立しておくことにより、組織のインシデント検出から調査、対応する能力が向上しますので、被害軽減に要する時間を短縮して、組織の最終的な損失額を圧縮することができます。

インシデント対応計画に対する組織の取り組み方

NTT グループでは、組織のインシデント対応を 4 種類に分類しました。ほとんどのケースにおいて、以下の 4 カテゴリーのどれかに区分されます。

- **対応計画無し（外部サポート無し）—** 残念なことに多くの場合には、各組織では対応計画の開発や検証に十分な時間を費やしていません。さらには、インシデント対応の社外管理やサポートに対して予算を確保している組織もほとんどありません。分析結果によると、2014 年に NTT グループがインシデント対応を伴うサポートを行った組織の 74 パーセントには、重大なインシデントに対処するための方針と計画、手順、サポート契約先のいずれもありませんでした。この傾向は、組織の 77 パーセントには公式な計画が無かった 2013 年から続いています。
- **対応計画無し（外部サポートあり）—** 組織の中にはインシデント対応の価値を認識しているところもあり、先を見越してサードパーティーによるインシデント対応サポートへの投資を行っています。小規模な社内 IT リソースを抱える組織では、対応能力を持たない組織のサポートを専門とするインシデント対応プロバイダーと契約するのが一般的です。これにも大きな価値があるかもしれませんが、契約を行う組織では、万一インシデントが発生した場合に、自分たちが行うべき役割が残っていることを認識する必要があります。インシデントの中でインシデント対応プロバイダーのサポートがどのような役割を担っているかを組織が把握することが極めて重要です。

- **既存計画を現在熟成中（外部サポートあり）**— 昨年中の NTT グループによる調査では、各組織が脅威の影響を緩和する方法に緩やかな改善がみられるという良い傾向もありました。組織の中には、インシデント対応能力向上に対する投資を始めたところもあります。これらの組織では、計画、プロセス、手順、ツール、および教育に重点を置いており、多くの場合、これらの体制の確立と検証を行っている間は、依然としてサードパーティー プロバイダーによる継続的サポートに依存しています。さらには、サードパーティーのインシデント対応プロバイダーは、技術的観点からサポートを提供するだけではなく、計画、方針、および手順の策定に関与する場合もあります。サードパーティーのプロバイダーは、自身の知見やノウハウを共有し、各組織のインシデント対応ニーズに対応することができます。
- **成熟した計画および能力（必要時には外部サポート）**— ほとんどの組織には、効果的なインシデント対応の定義や体制確立、成熟、維持を行う能力も資質も資金もありません。インシデント対応を自社内のチームですすめた場合、高度な対応要件のサポートに特殊な専門技術が必要な状況がでてきます。たとえば、自社のインシデント対応チームの多くは、詳細なフォレンジック分析のトレーニングや、マルウェアのリバースエンジニアリングにより将来的に攻撃に使われるかもしれない技術を発見するようなトレーニングは受けていません。サードパーティーによるインシデント対応サービスに対して、このような役割を依頼することにしている組織もあります。

結論

NTT グループが過去数年間に協力した組織の大部分では、インシデント対応が最優先事項ではないのか、組織にとって効果的な計画の価値を認識するのが単に非常に困難なのかのいずれかです。多くの場合、インシデント対応への準備と投資の緊急性は、ビジネスに対して大きな影響の及ぶイベントを経験した後になって初めて生じるものです。

適切なセキュリティ対策には、よくできた組織設計と管理策を通じて脆弱性を検出し影響を最小限に抑える能力だけではなく、それ以外のすべてがうまくいかなかった場合にも対応可能な能力が備わっているものです。

「インシデント対応」に関しては、以下の項目も参照してください。

はじめに：インシデント対応

インシデント対応の種類

セクション E.5：インシデント調査に基づく 5 つの重要推奨事項

2014 年に、NTT グループではさまざまなインシデントへの対応活動を行いました。これらの対応内容を整理したところ、これらのインシデント全体に共通する事象と推奨事項が明らかとなりました。さらに、NTT グループでは、これらの結果を広く公表されている脅威から得られた情報と比較しました。この分析によって、多くの組織において、検出能力、調査能力、および被害軽減能力が基本レベルでも成熟レベルでも不足していることで損なわれている領域をいくつか特定できました。

その結果として、我々は、各組織が自社環境においてこれら 5 つの管理対象領域の有効性を評価することを推奨します。この推奨事項には、ある組織のネットワークとセキュリティ インフラストラクチャの基本部分として実装されるべき基本的管理策が説明されています。NTT グループの分析によって、多くの組織では、これらの管理対象領域を効率的な方法で実装するのに苦慮していることが明らかとなりました。

管理対象領域 1：ネットワークのセグメント化

調査を行った脅威の多くは、ネットワーク セグメントの 1 つから発生し、攻撃の進行につれて社内ネットワーク全体に拡散していました。戦略的価値のあるシステム、攻撃対象候補、攻撃者が継続的な攻撃のための起点とし続けるのに役立つシステムを見つけようとして、攻撃者は組織全体を側面から不正利用します。

NTT グループが監視している組織ネットワークの中には、フラット（非階層的）なネットワーク インフラストラクチャがあります。これらのネットワークでは、機能領域の定義は適切ではありません。異なるネットワーク領域にはそれぞれ独自のデータ要件やアクセス要件がありますが、この事実は認識も徹底もされていませんでした。社内ネットワークのセグメント化では、セグメント間を流れるデータを精査することが必要です。たとえば、コールセンター環境にいる従業員は開発環境にアクセスする必要はないでしょうから、業務に必要な機能によって環境を分離し、アクセス コントロール リスト（ACL）でアクセスを制限すべきです。

各組織は、ルーターのアクセス コントロール リストと Virtual Local Area Networks（VLAN）を用いてネットワークをセグメント化するだけではなく、侵入検知・防止システム（IDS/IPS）、ファイアウォールによる検知・予防対策を実装する必要があります。これによって組織の能力が向上して、分離コントロールのバイパスなどの潜在的に悪意のあるネットワーク トラフィックの識別を支援する検知・防御能力が提供できるようになります。

ネットワークのセグメント化に加えて、各組織では、システム管理機能は特定のサブネットに分離されたネットワークから実行することを徹底する必要があります。これにより、管理行為は誰が行えるのか、どのネットワークセグメントから実行することが認められているのかという点に関して、より厳密な制御が可能となります。

さらに、このような対策は攻撃の進行を遅らせ、ネットワークへの侵入に時間がかかって人目につくようになり、やり遂げることが難しくなります。攻撃者がある環境の中で到達可能範囲を拡大しようとするたびに、情報収集、攻撃、不正利用のプロセスを繰り返し強いられる場合には、特にそうです。

セキュリティとコンプライアンスへの手始めとしてとしては、ネットワーク、データ、およびプロセスを適切に分離することで容易に大きな成果を得ることができます。ここで重要なのは、アクセス制御、ネットワーク トポロジー、およびデータ伝達経路の文書化を徹底することです。

ネットワークのセグメント化に対する重要な考察と推奨事項には、次の内容が含まれます。

- 重要なデータ、プロセス、およびシステムが含まれる重要セグメントの特定
- データ要件とアクセス要件の保護の必要性に基づき、重要領域を効果的にセグメント化するセキュリティ ゾーンの定義
- 組織のシステムに対する管理機能がサポートされるゾーン毎へのアクセス コントロール リストの適用と分離
- ネットワーク環境の成長や変化に応じて、アクセス制限が定められた目標を満たしていることの継続的確認

管理対象領域 2：マルウェア検出・予防策

多くの場合、マルウェアはネットワークに侵入するための最初の攻撃能力として用いられ、技術的脆弱性と人的脆弱性の両方を組み合わせて利用されています。

残念なことに、ここ数年間に NTT グループが目にした事例によると、ホストベースのアンチウイルス ソリューションでは、世の中に出回っているウイルスのせいぜい半分しか捕捉出来ません。現に 2014 年版 GTIR のために NTT グループにて行ったマルウェアの調査での検出率は、約 46 パーセントでした。NTT グループがサポートした数多くのインシデント対応においてマルウェアが検出されましたが、これらの感染されたシステムは、アンチウイルス ソフトウェアが旧バージョンのものであったり、アンチウイルス ソフトウェアがインストールされていないものでした。多くの場合、マルウェアはアンチウイルス ソリューションを無効化して、残存性能を上げています。

ホストベースのセキュリティのみに依存するのは、マルウェア脅威に対する戦略としては優れたものとは言えません。各組織は、マルウェアを使った悪意のある行為の兆候を察知できるよう、ネットワークと電子メール通信の精査を行える技術も検討する必要があります。

マルウェア検出・予防策に関する基本的な推奨事項には、以下のようなものがあります。

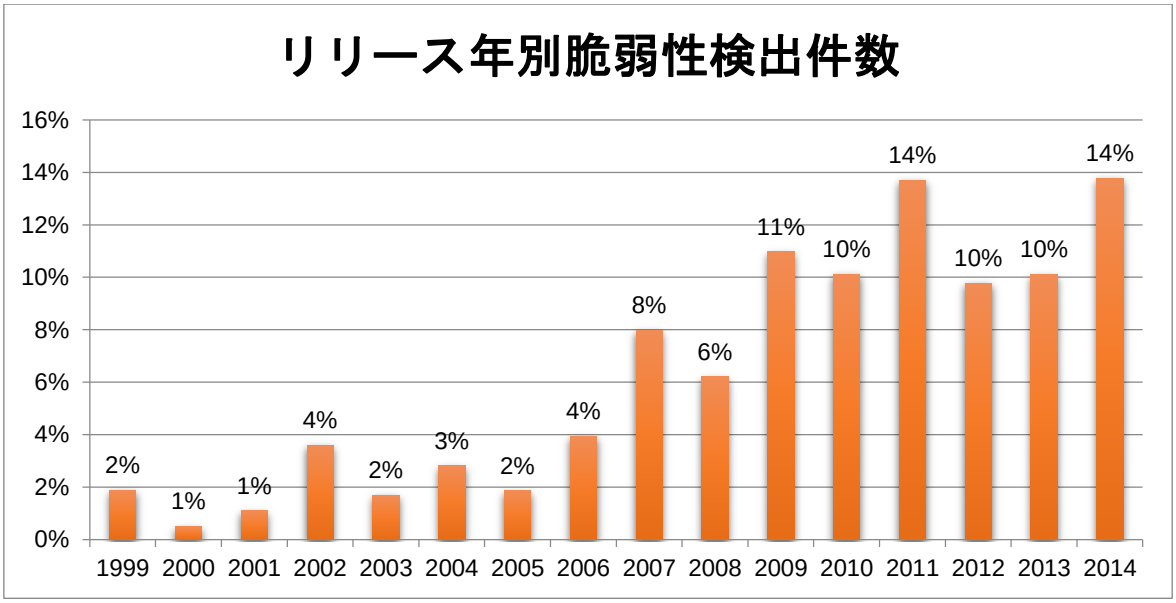
- 自分の組織のマルウェア被害軽減戦略を規定して、実装する対策では、複数のポイントで検知と可視化ができるにします。
- ホストベースだけではなくネットワークベースの検出能力と検疫能力にも投資を行います。
- マルウェア製品コンソールからログを収集して、ログ監視 SIEM/MSSP ソリューションの一部として機能させます。
- マルウェアのインシデントの取り扱いに関する方針と手順を策定します。
- マルウェア対策が規定通りに動作していることを確認し、必要に応じて調整を施します。

50 パーセントの防御からでも最大限の能力を引き出すには、サーバーとエンドポイントにホストベースのアンチウイルス ソリューションがインストールされており、定期的なアップデートとウイルスに対する定常的なスキャンが行われていることが必要であると理解することが重要です。ネットワークベースとホストベースのアンチウイルス ソリューションを常に監視して、最大限の能力を確実に引き出すようにする必要があります。

管理対象領域 3：パッチ適用と構成管理

NTT グループが 2014 年に分析した脅威の大部分には、パッチが適用されていないシステムや不適切に構成されたシステムが含まれていました。多くの場合、その不正利用はサードパーティー アプリケーションの脆弱性が直接関係するものでした。悪意のある攻撃者は、システムやネットワークへの最初の足掛かりを得る手段として、パッチが適用されていない脆弱性を持つシステムを探し出します。エクスプロイト キットの多くは、攻撃者は新たに発見された脆弱性に対するパッチを組織が適用するよりも早く攻撃の自動化が可能であるという認識をもっていることを前提に作成されています。昨年版の GTIR にも記載されているように、NTT グループでは、脆弱性管理プログラムを持っていない組織では、CVSS スコアが‘4.0 以上の脆弱性に対するパッチの適用に平均で 200 日近く要していることを確認しています。

パッチが適用されていない過去の脆弱性は、多くの攻撃者にとって比較的簡単なエクスプロイト経路となります。2014 年に NTT 脆弱性スキャン管理サービスによってクライアント システム内に検出された脆弱性の 76 パーセントが、2012 年またはそれ以前から存在するものであり、丸 2 年以上が経過していたことになります。2014 年に NTT グループが検出した脆弱性の 9 パーセント近くが、10 年以上経過したものでした。



タイトル：2014 年の新規脆弱性は多いが、一部は 1999 年まで遡る

構成管理とパッチ管理は新しい概念ではありませんが、脆弱性スキャンデータを定性的に分析した結果は、大半の組織の取り組みがいまだに不十分であることを物語っています。多くの組織では、重要で社外に向いているサーバーに対するパッチの適用にいまだに注意を集中していますが、今日の攻撃の大半は、**エンドユーザ**とサードパーティー アプリケーションに焦点を絞っています。

構成管理やパッチ管理の問題による潜在的損失を軽減するために、組織は以下の内容を行う必要があります。

- 構成管理および変更管理の方針と手順の文書化
- オペレーティング システム、ネットワーク機器、サードパーティー アプリケーションに対するパッチ管理の方針と手順の文書化
- 構成管理とパッチ管理のプロセスを迅速化するソリューションの導入と、関連作業の文書化
- 環境内のあらゆる技術に対する脆弱性の状況に関し、組織内での可視化と認識の徹底
- パッチの緊急エスカレーションのプロセス構築（特に、世の中に広く拡散しているウイルスにより、盛んにエクスプロイトされている脆弱性が組織の機器上に存在する状況において）
- 試験計画の策定およびどの対策とプロセスが想定通りに動作しているかの確認

構成管理とパッチ管理は時間がかかる難しい作業かもしれません。分散し、さまざまな**エンドユーザ**機器が使われる混在環境を管理する場合には特にそうです。強制力をもつパッチ管理プログラムを実装することで、サーバーと**エンドユーザ** システムのどちらからも一般的な脆弱性を取り除き、より新しいエクスプロイトや一般的なエクスプロイト キットの有効性を最小限に抑えることが可能となります。

管理対象領域 4：監視

NTT グループが 2014 年に分析した脅威の中には、かなりの長時間動作していたマルウェアもありました。各組織では、最初の不正行為が発生してから数か月後にいくつかの脅威を発見しましたが、その時点でデータはすでに消失していました。多くの場合、攻撃者は組織ネットワークに足掛かりを得て、検出を回避しつつ被害者の環境を通じて遠隔操作の対象を拡大しながら、辛抱強い攻撃活動を繰り広げます。これらの脅威の中にはマルウェア システムや IDS からのアラート通知を受けていたものもありましたが、無視されていました。

多くの脅威には、組織の社内ネットワークに広く分散する複数システムにおける不正利用がありました。多くの場合、これら不正利用されたシステムは、不正利用に関連のある通信（マルウェアのダウンロード、データの流出）に長時間関わっていました。ここには、社内サーバー間の不正な通信だけではなく、社内外両方のコマンド コントロール（C&C）サーバーとの通信も含まれていました。

真に効果的な監視には、システムのログやアラートだけではなく、通常時のネットワークの挙動把握も含まれています。挙動監視により、環境内の異常な活動を検知できます。例えば次のようなものがあります。

- 一度も通信を行ったことのないシステムが、唐突に大量の情報の交換を始めた。
- 複数の分散システムが、少数の集約化されたシステムとの通信を唐突に始めた。
- （一層明白ではあるものの、多くの場合には多くの組織ではいまだに検出されていないものとして）これまで静かだった社内システムが、唐突に社外システムとの通信を始めた。

組織が監視に対する投資効果を最大限にするために、NTT グループでは次の内容を推奨します。

- すべてのログが同じ条件で生成されているわけではありません。セキュリティ エンジニアがログや機器、システムを活用し、事象の把握をします。
- 強力な監視が実現できている場合のほとんどは、長年の成熟ならびに継続的計画と改善の結果です。監視に関する戦術的計画を策定して、実行します。
- 監視計画によって、脅威の最中に発生する活動をどれだけ上手に特定可能かが左右しますが、組織がコンプライアンス要件を満たすための活用も可能です。複数のユースケースに適用して、監視を最大限に活用します。
- 他のセキュリティ コントロールと同様に、監視は階層化された状態で最大の効果が得られます。ネットワーク レイヤとアプリケーション レイヤでログを取得します。社外に向いている IDS/IPS、ファイアウォール、WAF のログを取得しますが、それ以外にディレクトリ サービス、アンチウイルス、ファイル監視、データベース、Web アプリケーション、プロキシ、および DLP についても検討します。

- 機器を横断的に活動する悪意のある振る舞いを検知するのではなく、振る舞いの起点となる機器を監視することをを検討します。

管理対象領域 5：能動的インシデント対応

2014 年に NTT グループのインシデント対応サービスを利用した組織のおよそ 74%には、機能しうるインシデント対応計画がありませんでした。インシデント対応計画は、それが実行可能な場合に限って有効なものとなります。

分析を行ったインシデントにおいて、NTT グループは多くの組織が以下のような同じ自問自答を行っていることに気づきました。

- このアラートは本当に脅威を構成するものだったのだろうか。組織は本当に攻撃されていたのだろうか。
- 組織の誰が対応すべきだろうか。組織は脅威の証拠保存、サービスの復旧、データの保護のいずれに第一優先があるのだろうか。それともそれ以外に優先度の高いものはあるのだろうか。
- どのシステムやデータを最優先に対応すべきだろうか。
- 組織の（ISP などの）サードパーティー ベンダーはどの会社で、窓口は誰なのだろうか（窓口の電話番号は何番なのだろうか）。

これらは、インシデント対応計画が策定、調整、見直し、試験を経て練り上げられる間に認識される疑問点そのものです。

攻撃の最中に計画されたどおりの方法でインシデント対応するのは極めて難しく、失敗すれば、期間と攻撃に伴う損失額が拡大します。進行中の脅威の混乱の中でインシデント対応がどのようなものであるべきかを組織が見出そうとした場合には、対応プロセスはより一層複雑化します。

有効なインシデント対応計画とは、攻撃が発生する前に次のような活動を定めるものです。

- 役割や責任など、インシデント対応チームを明確に定義します。
- ISP テクニカル サポートなどの関連するベンダーおよびサードパーティーの連絡先情報を文書化し、それらをどのようにプロセスに当てはめるかを規定します。
- 組織内にはないが必要なスキルを把握し、それらをいかに補完し、活用するかを規定します。
- インシデント中に効率的に連絡を取るプロセスを規定します。
- インシデントが始まった際と終了した際の宣言を行う基準を規定します。

これは実際のインシデント対応計画をかなり簡略したものであり、速やかに実装し、すべての責任者に対して明確に伝達する手順が必要となります。残念なことに、NTT グループによる 2014 年のインシデントの分析によると、この単純な概念は、往々にして最も成熟した組織ですらも見落とされていることがわかりました。

結論

不正利用のすべてが、このセクションで論じた基本的コントロールの欠如の結果なのではありませんが、攻撃を受けたすべての組織において、この領域の真に有効なコントロールが実装されていたならば、それらの組織の回復力はもっと高く、攻撃に対する対応の準備が出来ていたはずです。これらの 5 種類の管理対象領域を効果的に対策実装することにより、どの組織においてもセキュリティに対するプラスの影響が即時に生まれます。

「インシデント対応」に関しては、以下の項目も参照してください。

はじめに：インシデント対応

インシデント対応の種類

分野別インシデント

インシデント対応の重要性

脅威インテリジェンスの定義

セクション E.6：脅威インテリジェンスの定義

脅威インテリジェンスの定義

ここ数年間、セキュリティ業界では「脅威インテリジェンス」という用語にさまざま定義を当てはめてきました。このセクションでは、NTT グループによる定義と、それをどのようにクライアントに適用しているかを紹介し、包括的な脅威インテリジェンス戦略の重要な構成要素とメリットについていくつか論じます。

脅威インテリジェンスの核となる意味は、さまざまな情報源からのデータと情報の丹念な収集、相関関係・前後関係を意識した分析、インテリジェンスの作成、およびインテリジェンス利用者への配信など、広義のインテリジェンス基本方針の特定的な用途のことです。

コア インテリジェンス分野

インテリジェンス コミュニティ（IC）によると、5 つのコア インテリジェンス分野が存在します。

- 人的インテリジェンス（HUMINT）- 人的リソースからの情報収集
- オープン ソース インテリジェンス（OSINT）- データマイニングや高度検索技術を通じた一般に入手可能な公開情報の探査、エクスプロイト、および拡大
- 信号インテリジェンス（SIGINT）- 通信システム、レーダー、兵器システムから送信される信号の収集とエクスプロイト
- 画像インテリジェンス（IMINT）- さまざまな地上、航空機、衛星からの収集者によって収集と処理が行われた地理空間情報
- 計測・痕跡インテリジェンス（MASINT）- レーダー、レーザー、パッシブ式電気光学センサー、地震センサーなどのセンサー類といった技術的測定装置を用いて収集された情報を用いて、そのシグネチャから相手を特定するインテリジェンスの技術部門

サイバーインテリジェンスの定義

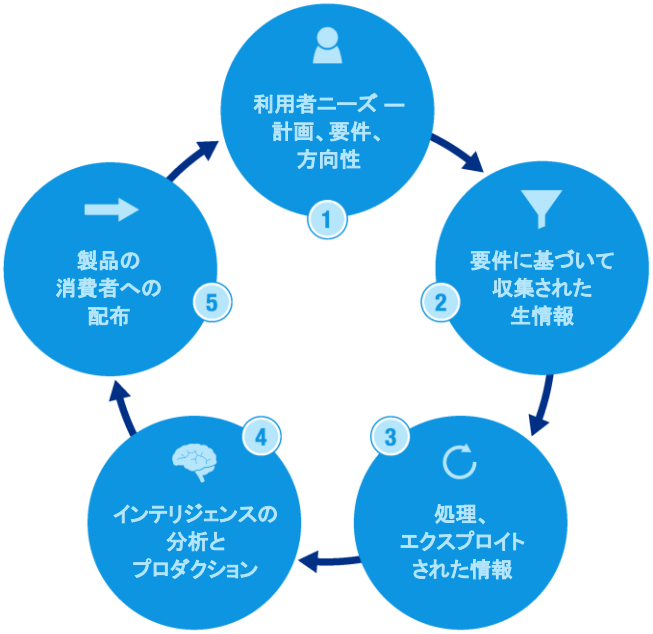
サイバーインテリジェンス（CYINT）はコア インテリジェンス分野の 1 つでこそありませんが、5 つのコア分野のいかなる組み合わせからでも、そのすべてからでも構成されるハイブリッドな領域です。サイバーセキュリティの重要構成要素として用いられることもありますが、CYINT はサイバーセキュリティ任務とは独立に機能しており、政府や産業のあらゆる分野にまたがるさまざまな活動をサポートします。

各組織にとっては、急速に浮上しつつあるこのインテリジェンス領域が幅広い可能性を有しており、サイバー脅威の実行者、脆弱性に関する技術的データ、マルウェア、IP レピュテーション データを特定する以上のことに利用可能であることを認識することが極めて重要です。CYINT はこのような狭い限界の先に進んでおり、そこにはデジタル脅威の予測へとつながる可能性のある、組織の物理的環境と関係のある行動やイベントの分析が網羅されています。

インテリジェンス サイクル

NTT グループでは、世界中の数多くの企業が適切な脅威インテリジェンス プログラムを導入するお手伝いを行っています。我々の全体的アプローチの概要は以下のものです。

1. 計画、要件、方向性 - インテリジェンス収集の計画と方向づけには、優先インテリジェンス要求から最終的なインテリジェンス製品までのインテリジェンス活動全体の管理が含まれます。
2. 収集 - 脅威インテリジェンス サービスでは、適切な情報源から潜在的に有用な生データを収集します。
3. 処理 - 収集されたデータは、詳細分析に適した標準フォーマットに統合されます。
4. 分析とプロダクション - 収集されたデータは、対象事項の専門家によって、顧客環境に対する潜在的脅威を特定し、脅威に対する対策を開発するための分析が行われます。
5. 配布 - インテリジェンス分析はステークホルダーに配布され、適切な処置を導きます。



タイトル：インテリジェンス サイクルの 5 つのステップ

情報とインテリジェンス

多くのセキュリティ脅威インテリジェンス ベンダーが何と言おうとも、データと情報はインテリジェンスではありません。以下の例をご覧ください。

情報：Java のゼロデイ脆弱性に対するあるエクスプロイトが、セキュリティ メーリング リストで公開されます。その後まもなく、その脆弱性を悪用しているマルウェアが割り出されます。セキュリティ ベンダーはこの脅威についてクライアントに通知を行い、被害を軽減するための推奨事項を提供します。これは脅威「情報」であり有用な情報ではありますが、定義から必然的に脅威「インテリジェンス」ではありません。

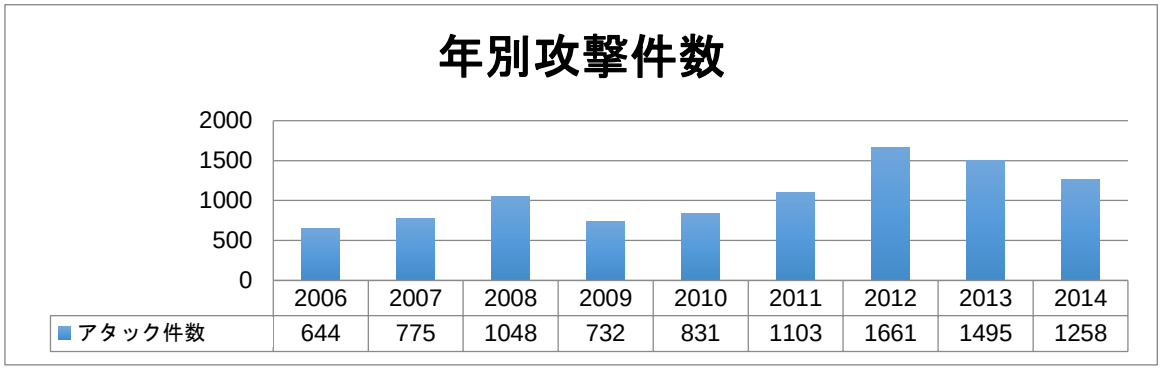
インテリジェンス：Java の脆弱性のエクスプロイトを監視していたセキュリティ ベンダーは、アジアにおける感染率が米国よりもかなり高いことに気づきます。ボットネット コマンド コントロール システムに関連のあるコードを被害者の装置上にインストールする新種のマルウェアが、In-the-Wild ウイルスリストに掲載されています。時を同じくして、ある大手金融機関が中小地方銀行数行の買収を公表します。これにより、不渡り小切手手数料が 20 ドルから 35 ドルに値上がりし、消費者は怒っています。いくつかのハクティビストのグループが、米国の銀行システムに抗議する議論を Twitter などのソーシャル メディア サイト上で始めており、大手機関のオンライン取引を 1 日停止させると公言しています。あるハクティビストの Twitter アカウントから、ボットネット コマンド コントロール ソフトウェアの使用の指令が出されますが、これは、Java マルウェアによってインストールされたボットネット クライアント コードに関係するもののようです。

これらのデータ ポイントを継ぎ合わせることにより、次のようなより鮮明なイメージが得られます。米国の銀行は、Java の脆弱性に基づくボットネットを用いた、ハクティビスト グループによる DDoS（分散型サービス拒否）攻撃の標的となりがちです。感染特性に関して知られている情報に基づき、銀行は、その攻撃がアジアを起源とする IP アドレスを起点とするものであると推測しています。これが脅威インテリジェンスであり、数多くの類似点の無い情報源から収集して、特定の標的に対する特定の脅威を識別するために人間のアナリストによる統合が行われた情報となります。

情報セキュリティにおける脅威インテリジェンスの重要性

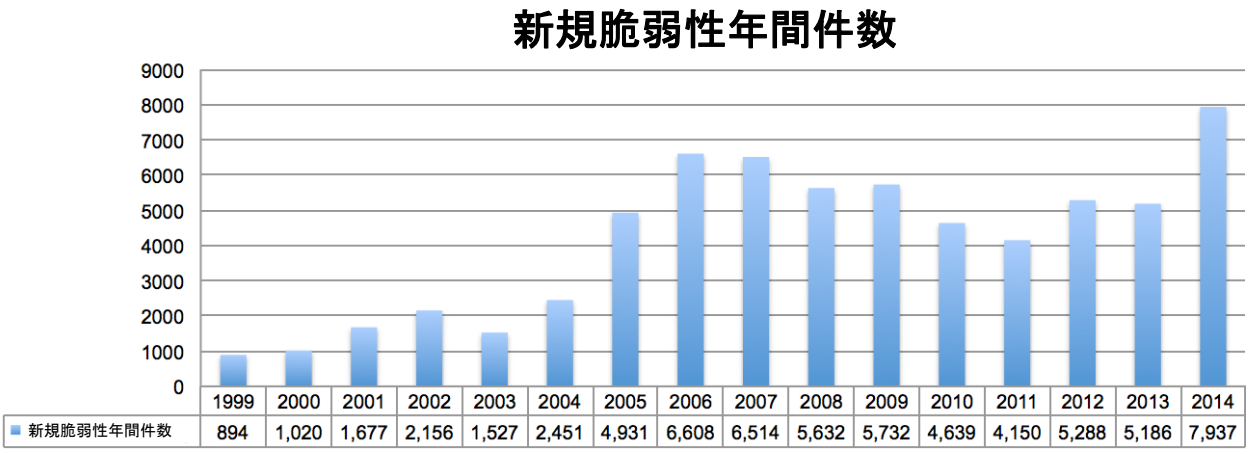
脅威インテリジェンスが決定的な情報セキュリティ要件として認識され始めた主な理由としては、次の 4 点があります。

サイバー脅威の特徴の変化：各組織は、セキュリティの脅威における劇的な変化に対する防御を行い、攻撃の外見には狭義の技術的要因をはるかに超えるものが包含されていることを理解する必要があります。サイバー脅威の実行者は、もはや特異な性格や反体制派の個人やグループなどではありません。今では、国家やそこから資金提供を受けているグループには限らず、大量のリソース、サポート、専門技術が思いのままとなる、国境を越えて組織された犯罪グループなども含まれています。その反対に、多くの場合、組織防衛の任務を背負った人は、適切な防衛の立ち上げに限られたリソースと予算しか持っておらず、脅威とは非対称な状況となっています。文書化されたデータ損失インシデントの件数が増加を続けているのは、最近の攻撃の成功率が向上していることの証明となっています。次のグラフは、http://datalossdb.org/statistics にある文書化された攻撃数の増加を示しています。



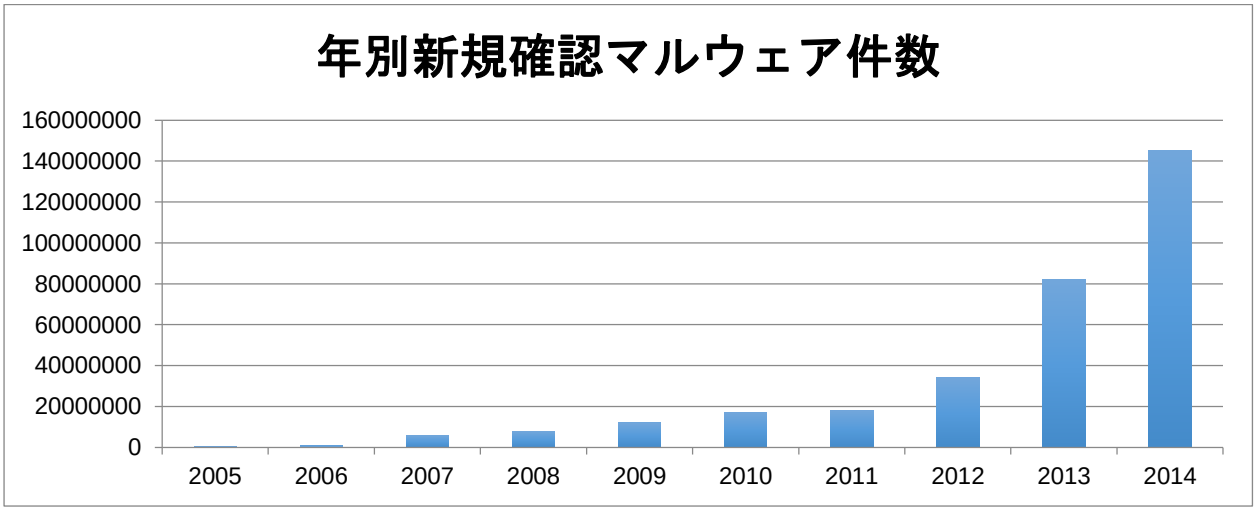
タイトル：攻撃回数はほぼ毎年増加

情報セキュリティ脆弱性の件数：情報セキュリティ担当者が分析しなければならないデータ量は、手に負えないほどの規模となっています。各組織では、脆弱性、ゼロデイ脅威、マルウェア、エクスプロイト キット、ボットネット、持続的標的型攻撃（APT）、および標的型攻撃の日常的な流入に対応する必要があります。ここ 15 年間の各 1 年間に見つかった共通脆弱性識別子（CVE）（http://web.nvd.nist.gov/view/vuln/statistics）の数を以下の図 3 に示します。2005 年以降、毎年 4,000 件以上の新たなセキュリティ脆弱性が発見されています。



タイトル：新たな脆弱性の年間件数はほぼ管理不能

次のグラフにあるように、近年ではマルウェア検出数も増加しています。このグラフを一目見ただけでも、1 年間に見つかった新たなマルウェアの数は、2011 年以降劇的に上昇していることがわかります（http://www.av-test.org/en/statistics/malware/）。



タイトル：新たなマルウェアの数は、単なる増加ではなく急上昇

ある組織の環境を標的とした脅威に関するインテリジェンスは、改善活動の優先度設定の役に立つことから、被害軽減活動とリソースは、最も必要性と防衛価値の高い領域に振り向けられます。

技術の発展と使用方法の変化：大半の組織で使われている技術の数は、わずか数年前よりも劇的に増えています。Bring Your Own Device（BYOD）化への動き、VPN を通じて企業ネットワークに参加する遠隔勤務者、無線ネットワークの広まり、および増加する仮想化とクラウド コンピューティングの利用のいずれもが、典型的な組織環境内で使われている技術の劇的な増加をもたらしました。通常であれば、新たな技術は過去の技術に取って替わるものではありません。ほとんどの場合は追加となり、その結果として組織が攻撃を受ける境界面と内部で見つかる脆弱性が正味で増えることになります。境界線が定められた同種組織ネットワークというものは、もはや存在していません。混在・分散型のユーザーと技術ベースが新たな標準です。この新たな現実では、複雑さと潜在的リスクが以前よりも増加しています。

脅威インテリジェンスの手頃なアウトソーシング：各組織では、増加するリスクと上記リストのすべての要素から受ける攻撃の回数の増加に直面しており、あっという間にリソースが破綻してしまうかもしれません。幸いにも、多くのベンダーから脅威インテリジェンス サービスが提供されており、こういった組織が脅威や攻撃に対する準備、防衛、対応を迅速に行うための支援が行われています。

各組織での脅威インテリジェンスの使用法

組織ごとに、情報セキュリティ特性、保護すべき資産、専門技術のレベル、使用されているセキュリティ技術の種類は異なります。その結果として、組織が異なれば、脅威インテリジェンス サービスに対する理解もニーズも期待内容も異なります。組織的な脅威インテリジェンスのニーズに影響を及ぼす要因としては、組織の規模、政府機関や主な業種との関係性、ファイアウォールの外にあるサプライチェーンと情報が共有される範囲、および社内セキュリティ リソースの洗練度などがあります。

たとえば、人目に触れることも少なく、一般に攻撃者が期待するような類のデータの格納や送信を行っていない組織では、公共の場での露出度が高い組織や、求める価値の高いデータを持っていたり議論を呼んでいたりする話題に関係する組織とは、また違った脅威インテリジェンスに対するニーズがあるものと思われます。また、高度に政治的な産業に関与している国際組織であれば、活動家グループからの攻撃、競合他社に対する攻撃、注目を集める会議やイベント、産業スパイのようなトピックに対する的を絞ったインテリジェンスを必要としているかもしれません。

結論

情報セキュリティのコミュニティにおいて、インテリジェンス、サイバーインテリジェンス、そしてサイバー脅威インテリジェンスという用語は、大々的かつ区別なく使用されてきましたが、往々にしてその使い方は誤っていました。これらの用語は、自動化されたデータ フィード サービスや、脅威の更なる検出と被害の軽減に使用される可能性のあるデータを表現するものとして、全く不正確な形で使用されてきました。しかしながら、これらの用語それぞれの極めて特異な性質は、真のインテリジェンスとは何であるか、それはどうやって得られるのかという点に関する基本的な理解の上に構築されるものです。統一的な理解のためには、セキュリティ業界の用語を伝統的なインテリジェンス コミュニティのものに整合させることが重要です。

伝統的インテリジェンス コミュニティでは、長期にわたって脅威インテリジェンス情報の管理を行っており、完全ではないとしても、プロセスを改善する機会がありました。業界は、彼らが学んだ教訓を適用して、新種のサイバー脅威インテリジェンスの有効性を最大化することが必要です。

ここ数年にわたるサイバーセキュリティを取り巻く状況の変化は、脅威インテリジェンス サービスのニーズに対する一番の駆動力となっています。各組織が脅威インテリジェンスの新たな提供元を求める際には、セキュリティ業界から提供されているさまざまな種類のインテリジェンスを意識する必要があります。

「インシデント対応」に関しては、以下の項目も参照してください。

はじめに：インシデント対応

インシデント対応の種類

分野別インシデント

インシデント対応の重要性

インシデント調査に基づく 5 つの重要推奨事項

セクション F：分散型サービス拒否攻撃

セクション F.1：DDoS 攻撃序論

サービス拒否（Dos）と分散型サービス拒否（DDos）は、これまで長い間悪意のある行為者によって使用されてきたありふれた攻撃技術ですが、各組織では、これらの脅威の被害を適切に軽減するのに今でも苦労しています。このような攻撃は、被害を受けた組織に大きな影響を与える可能性があります。ここ数年間、NTT グループでは、クライアントに対してこのような攻撃への準備の支援を行ってきました。

セキュリティ市場には毎年、DoS および DDoS の脅威による被害を軽減する新たな機能が登場しています。アプリケーション レイヤ アプライアンスからコンテンツ配信ネットワークの機能まで、こうした攻撃の影響の管理には大きな注目が集まっています。

以下のセクションでは、DDoS 攻撃の分析と、標的にされた組織に対して正当なアプリケーション機能を使用した DDoS 攻撃のケーススタディを紹介します。

「分散型サービス拒否攻撃」に関しては、以下の項目も参照してください。

DDoS 攻撃序論

分散型サービス拒否の観測結果

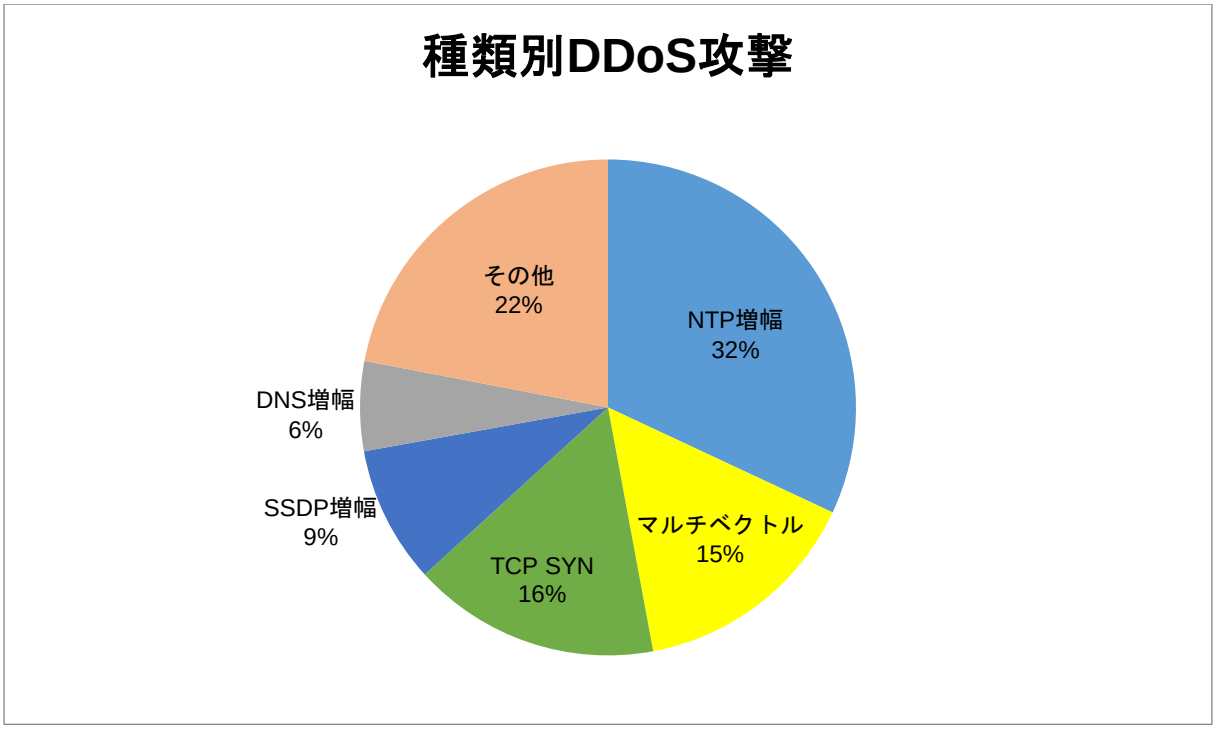
分散型サービス拒否の種別分布のカレンダー形式表示

ケーススタディ：Web アプリケーション DDoS 攻撃

セクション F.2：分散型サービス拒否の観測結果

NTT は世界最大のインターネット プロバイダーの 1 つであり、グローバルに公開されている NTT ネットワークを通過する世界のインターネット トラフィックは大きなシェアを占めています。全世界をカバーし、この大きな帯域を管理するプロバイダーである NTT の重要な業務の 1 つには、大規模な分散型サービス拒否（DDoS）攻撃の被害軽減があります。歴史的に見て、この攻撃は、正当なサービスが利用不能となるほどの分量のデータまたはアクティビティで、被害者のネットワークをオーバーフローさせることに集中してきました。こういった量的攻撃は、（本レポートのセクション F.4 にある Web アプリケーション DDoS 攻撃に関するケーススタディで説明されているように）アプリケーションの処理リソースを食いつぶすアプリケーション向けの DDoS 攻撃とはかなり異なるものです。

2014 年に NTT が観測した DDoS 攻撃の分布（攻撃種類別）を次のグラフに示します。



タイトル：NTP 増幅が攻撃種類別攻撃回数の首位に

観測された DDoS 攻撃全体の 63 パーセントが、UDP ベースのプロトコルとサービス（NTP、SSDP、および DNS）に関連するものでした。2014 年に観測されたさまざまな DDoS 攻撃種別に関する考察を以下に示します。

NTP 増幅攻撃

我々が観測した最もありふれた攻撃種別は、2014 年の DDoS 攻撃全体の 32 パーセントを占めている、ネットワーク タイム プロトコル（NTP）増幅攻撃でした。この攻撃では、攻撃者は、NTP クエリのソース アドレスを標的としている被害者のアドレスに変更した後に、この故意に詐称したクエリを 1 台以上の NTP サーバーに送信します。NTP サーバーは、被害者の IP アドレス（詐称されたソース アドレス）に応答を返します。

この攻撃を増幅する構成要素が、この攻撃を興味深くしている部分です。特定の NTP オプションを使用すると、NTP サーバーに対する非常に小さなクエリから、非常に大きな応答を発生させることができます。

TCP SYN フラッド攻撃

全体の 16 パーセントを占める、最多の DDoS 攻撃種別の中の別の種別であり、最古でかつここ何年も最もばらつきなく観測される攻撃種別の 1 つでもあります。TCP SYN フラッド攻撃は、標的とするネットワークを大量の TCP SYN リクエストでオーバーフローさせることで実行され、その結果として利用可能なリソースが枯渇します。

被害軽減コントロールが導入されていない場合、悪意のある攻撃者は、このやり口を使ってサーバーへの部分的にオープンされたコネクションを大量に生成できます。この操作が利用可能なセッションをすべて使い果たし、通常は正当なサービスにアクセス可能であるはずのポートにユーザーが接続できなくなります。

攻撃者は、リソースを枯渇させる別の技術を使用することにより、SYN フラッドの成功をさらに確実なものとすることが出来ます。その技術としては、ソース IP アドレスの詐称、複数ポートの標的化、複数の分散ソースからの攻撃、そしてボットネットの使用などが考えられます。

SSDP 増幅攻撃

2014 年に観測されたもう 1 つの DDoS トラフィック種別には、シンプル サービス ディスカバリ プロトコル（SSDP）増幅があり、観測された DDoS 攻撃全体の 9 パーセントを占めていました。SSDP は、機器相互のディスカバリと接続を支援するために作成されたものであり、ユニバーサル プラグ アンド プレイ（UPnP）プロトコルの一部となっています。このプロトコルが最初に導入されたのは 1999 年であり、標準で UDP ポート 1900 番を通信に使用します。

DNS 増幅や NTP 増幅などそれ以外の攻撃と同様に、攻撃者は、特別に仕立てられたリクエストを SSDP が有効となっている機器に送信し、その応答を標的とするシステムに誘導します。サービスのデフォルト設定は UDP/1900 ですが、それ以外のポートやサービスに応答を送信するようにも設定可能です。SSDP が有効となっている機器が不足している訳ではないため、攻撃者にとっては、リフレクションや増幅をベースとする攻撃の間に使用するのに適した候補です。攻撃者は、いくつかのツールを用いて SSDP が有効となっている機器を特定し、攻撃を開始することができます。

SSDP DDoS 攻撃を実行可能なボットネットは、不正利用されているホーム コンピューティング、ネットワーク、住宅用アプリケーションを用いて攻撃を実行することもあります。特にネットワーク モデム／ルーターのバンドル ソフトウェア、ワイヤレス アクセス ポイント、数多くの家庭用娯楽機器、およびゲームシステムなどの住宅用アプリケーションにおいては、SSDP が広く利用されているため、SSDP DDoS 攻撃は継続するものと思われます。

残念なことに、SSDP を実装している機器の大半ではデフォルトでこの機能が有効となっており、家庭内ユーザーがこのサービスにパッチを適用したり、無効としたりする見込みはありません。

マルチベクトル攻撃

マルチベクトル攻撃では、1 回のインシデントの中で、さまざまな種別の DDoS 攻撃を組み合わせて使用します。多くの場合、攻撃者は 1 つの方法を使って攻撃を開始しますが、最初の攻撃方法が期待したほどの効果を上げなかった場合には、その攻撃の最中にやり方を変更することがあります。

その一方で攻撃者は、成功を確実なものとするために、同時に複数の攻撃手法を用いることもあります。たとえば、攻撃者は NTP 増幅で攻撃を開始した後に、SYN フラッド、SSDP、アプリケーション固有の手法などを使って攻撃の効果を拡大させることがあります。

成功確率が上がるため、マルチベクトル攻撃は強力なやり口です。この攻撃は、防御と組織の担当者を圧倒するように設計されています。異なる攻撃技術には異なる被害軽減と防御の手法が必要となるため、各組織にとっては、マルチベクトル攻撃への対応は難題かもしれません。

DDoS による被害を軽減するための推奨事項

DDoS 攻撃はしばらく前から存在しています。予防対策が成熟する期間もあり、対策の中には他のものよりも信頼性が高いことが証明されているものもあります。各組織固有の環境で評価を行う必要があるものの、NTT グループでは次の推奨事項を提案しています。

技術的推奨事項

- 各組織は、複数の技術を活用することにより、DDoS による被害を軽減するコントロールに階層的手法の導入を検討する必要があります。
- Web アプリケーション ファイアウォールなどのオンサイトのアプリケーション DoS 被害緩和サービスを導入します。
- 上流の ISP を含む複数の入口において、また、コンテンツ配信ネットワークやスクラビング サービスを介して、トラフィックをフィルタリングします。サードパーティーのトラフィック スクラビング フィルタリング サービスでは、多くの場合、複数種別の DDoS 攻撃に対応する必要性を事前に察知しているため、これらが有用である可能性があります。
- 攻撃が展開するにつれて帯域をスケール可能な動的帯域サービスを導入します。これは長期的ソリューションとしては最適なものではありませんが、初期段階の攻撃の影響をある程度吸収するのに役立つ可能性があります。
- ネットワーク ファイアウォール、ロード バランサー、およびサーバーの多くでは、レート制限またはセッション タイムアウトがサポートされています。組織の担当者が環境とすでに利用可能となっているツールを確実に理解するように徹底します。
- 組織および ISP の TCP SYN フラッド攻撃対応能力を理解します。多くの ISP では、詐称 IP アドレスの検出を導入しており、デフォルトでフィルタリングします。

- 多くの場合、ISP では大量の攻撃のフィルタリングにおいて目覚ましい効果を発揮しますが、小規模な攻撃には気づかずにフィルタリングされない恐れがあることに留意してください。
- 攻撃対象によっては、ホストベースまたはアプリケーションベースのコントロールが、セッションまたはコネクションの枯渇被害の軽減に役立つ場合があります。
- 構成ミスの問題を削減して稼働サービスを制限するために、組織がシステムとサービスの堅牢化ガイドラインに従っていることを徹底します。

非技術的推奨事項

- DDoS 攻撃に対する検出能力だけではなく対応能力についても、組織の理解を徹底します。
- 組織の事業継続計画と災害復旧計画の中に、DDoS 攻撃に対する説明を記載します。
- DDoS 攻撃によって組織の運営やサービスに生じる可能性のある財政的影響を評価します。
- 多くの場合、DDoS 攻撃はそれ以外の犯罪行為の隠ぺいに用いられます。万一 DDoS 攻撃が発生した場合には、発生している恐れのあるそれ以外の悪意のある行為（不正な電信送金、その他の脅威、他のネットワーク セグメントからのデータ流出）に対して、組織で警戒を続けることを徹底します。
- DDoS 攻撃の間にサポートを求める相手（SOC、ベンダー、ISP、インシデント対応チーム）を理解します。

「分散型サービス拒否攻撃」に関しては、以下の項目も参照してください。

DDoS 攻撃序論

分散型サービス拒否の種別分布のカレンダー形式表示

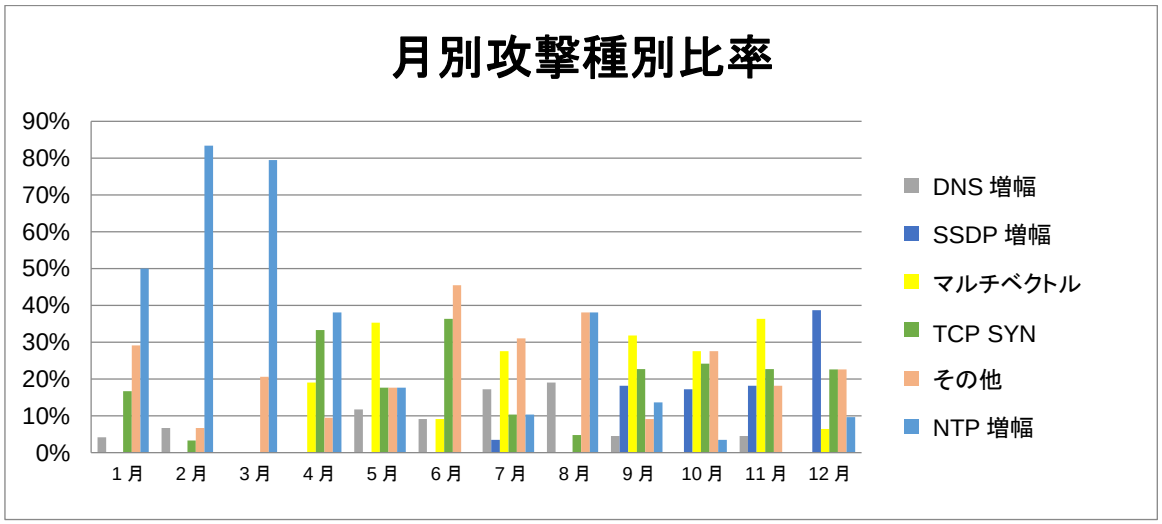
ケーススタディ：Web アプリケーション DDoS 攻撃

セクション F.3：分散型サービス拒否の種別分布のカレンダー形式表示

NTT グループでは、DDoS 攻撃のデータを分析して、2014 年に目撃した中で最も広く用いられている攻撃手法を調べました。年間を通じて、UDP プロトコル ベースの攻撃（NTP、DNS、SSDP など）が観測されています。2014 年に観測された中で、最も注目に値し、影響の大きな攻撃手法は、NTP 増幅攻撃と SSDP 増幅攻撃でした。

2014 年第 1 四半期に、DDoS 被害軽減プロバイダーと一般メディアは、NTP ベースの DDoS 活動に顕著な急上昇を認めました。NTT グループは、収集したデータの中に同一の結果を目にしました。次のグラフで表されているように、その年の NTP 増幅活動の半数以上は、2014 年の 1 月から 4 月までの期間に観測されました。第 4 四半期にも同じような攻撃が少しだけ再発しています。

NTP に関連する攻撃におけるこの劇的な増加の主な理由の 1 つは、ツールキットが入手可能であったことにより、攻撃者は、幅広いスキルが求められることなく強力な攻撃をしかけることが出来たためです。この機能を提供するツールキットの 1 つには「NTP-AMP」があります。



タイトル：月別の攻撃種別の比率

それほどの量ではありませんが、NTT グループでは 7 月に SSDP 増幅攻撃の増加を観測しました。第 4 四半期の間に増加を続けており、2014 年 12 月に最大となりました。

2014 年最終四半期における SSDP ベースの攻撃の増加は、急激で広範囲なものでした。この観測された攻撃の急増は、リフレクションに基づく DDoS 能力意識の可視性の向上と、これらの攻撃手法がサポートされているツールが入手可能であったことによるものでしょう。UPnP と SSDP が有効化された機器が世界中で入手できることから、我々は近い将来も SSDP ベースの攻撃を継続して観測するものと思われます。

特定の推奨事項や、このセクションで取り上げた DDoS 攻撃種別に関する詳細については、本レポートの「分散型サービス拒否の観測結果」のセクションも参照してください。

「分散型サービス拒否攻撃」に関しては、以下の項目も参照してください。

DDoS 攻撃序論

分散型サービス拒否の観測結果

ケーススタディ：Web アプリケーション DDoS 攻撃

セクション F.4：ケーススタディ：Web アプリケーション DDoS 攻撃

ケーススタディの教訓

攻撃を受ける「前に」DoS/DDoS 防御を確実に導入するのは、やるだけの価値があります。

概要

NTT グループのマネージド セキュリティ サービスのクライアントである XYZ 社（クライアントが特定されないように名前を変えてあります）は、分散型サービス拒否（DDoS）攻撃を受けました。その攻撃は、それまでほとんど使われていなかったアプリケーション レイヤ DDoS 攻撃であり、毎秒 1 メガビット未満の速度で Web アプリケーションを標的としていました。この現象は、顧客に提供したグローバル バックボーンにおいて、NTT が日々被害の軽減を行っている大規模な分散型攻撃のうち多くのものとは大きく異なる点でした。

イベントの時系列

日付	イベント
1 日目	アプリケーション DDoS 攻撃らしきものを検出
	インシデントを NTT の顧客にエスカレーション
	攻撃の兆候となるような遅延を生じる運用上の問題はチームによって確認されず
	顧客のインターネット サービス プロバイダー（ISP）からログの要求を受ける
	詳細な分析の結果、ある攻撃者が攻撃対象として悪意を持って WordPress 機能を使用していることが判明
	被害を軽減する手順が特定され、シグネチャの生成、試験、導入を実行
	クライアントが攻撃による被害を完全に緩和
	攻撃トラフィックに関係するサニタイズ済み詳細情報をエスカレーションとして DoS 防止ベンダーに送信
	このインシデントの合計所要時間：5.5 時間 ISP からログを受領してからの所要時間：1.5 時間
7 日目	ベンダーが新たな公式シグネチャを導入

イベントの説明

2014 年の春、NTT グループのセキュリティ オペレーション センター（SOC）所属のセキュリティ アナリストは、あるクライアントの監視付き環境内にあるさまざまなシステムからの異常な応答を観測することにより、DDoS 攻撃を発見しました。XYZ 社はもちろん、XYZ 社の IT サービス プロバイダーや ISP とも合同で、NTT グループはさらに進んだ調査を開始しました。このチームは、アプリケーションの性能に表れている遅延は、保守やネットワーク機器の故障によるものではないものとすぐに断定しました。NTT SOC チームは関連ログの提供を依頼しさらに調査を進めたところ、攻撃者は Pingback[6]という WordPress の正当な機能を用いて DDoS 攻撃を実行していることがわかりました。NTT グループのセキュリティ アナリストがこの攻撃の素性を割り出すやいなや、このチームは今後の攻撃による被害を緩和するシグネチャの開発、試験、導入を行いました。

[6] https://en.support.wordpress.com/comments/pingbacks/

被害の軽減が成功した後、インシデントと NTT グループによる攻撃の被害軽減方法について、DoS 防止ベンダーに伝えました。そのベンダーでは公式シグネチャの作成と導入を行い、他のどの顧客も入手可能なようにしました。

根本的原因

この攻撃はアプリケーション攻撃であり、目的は標的となった Web アプリケーションのリソースをすべて使い果たすことでした。しかし、攻撃量が少なかったために、Web サイトへのネットワーク アクセスには影響が及びませんでした。この現象はアプリケーション攻撃にはよくみられるものであり、このために通常の Web サイト トラフィックとの識別が困難となる場合があります。この帯域の狭さは、同一のインターネット アクセスを共有する他のアプリケーションは攻撃による影響を受けなかったということでもあります。

WordPress のこの機能を用いることで、攻撃者は定評あるサードパーティーの正当なサーバーを悪用して、正当な HTTP リクエストらしく見えるものを生成して被害者の Web サーバーに送り込むことができました。被害者の Web サイトでは、WordPress は動作していませんでした。

Pingback は、WordPress にてデフォルトで有効となっており、ブログ同志の相互参照に用いられます。攻撃者はデスティネーション URL を捏造して、WordPress サイトが被害者の Web サイトにアクセスして、pingback が実際にそこから発せられたものか確認するように仕向けることが可能です。Pingback 攻撃は正当な HTTP リクエストを利用しますが、そのクエリにはリクエストのたびに変化する任意の値が含まれています。この任意のリクエストが攻撃の有効性の鍵となりますが、それは、Web サイトがリクエストを受け取るたびに Web ページのリロードを余儀なくされることによります。これによって、Web サーバー上の負荷を軽減するために用意されたバッファ記憶装置やキャッシュは、すべてバイパスされます。このようなリロード動作は、アプリケーションのリソースを非常に大量に消費し、影響を受けた Web サイト上にサービス拒否（DoS）状態を引き起こすことができます。リクエストされた Web ページのファイルサイズが大きく、大量のコンテンツを含んでいるメディア リッチなものである場合には、特にその傾向が強くなります。

この種の WordPress 攻撃では、正当な WordPress サイトが無実な被害者に襲い掛かるように仕向けられます。WordPress 攻撃は In-the-Wild ウイルスリストに掲載されており、場合によっては、16 万以上の WordPress サイトを使って、 1 箇所の被害者サイトに pingback リクエストを送信することもあります。

数か月後、攻撃者は、何社かの金融会社や運輸会社に加えて、同じクライアントに対して同じタイプの WordPress DDoS 攻撃を仕掛けました。金融機関 1 社の Web サイトが 1 時間以上にわたって使用不能となり、他の会社でも最大 12 時間、さまざまな程度の影響を被りました。NTT グループのクライアントでは、測定可能なほどの業務への影響はありませんでした。

インシデントのコスト

クライアントである XYZ 社とのやり取りに基づき、インシデントの発見と被害の軽減が迅速に行われたことで、このイベントの実際のコストはかなり低かったものと NTT グループでは推定しています。このインシデントに伴うコストの大半は、調整、連絡、文書化、教訓学習に関するものです。

品目	コスト
上記の調査、改善、および専門家によるインシデント サポートの実コスト	$2000 未満
法律および広告宣伝に関するサポートの実コスト	$0
Web サイト停止による実損失額	少額
イベントに直接関連する実コスト総額	$2000 未満
その後の攻撃による実コスト総額（シグネチャ導入後）	$0

タイトル：被害緩和に成功した DDoS イベントのコスト

ケーススタディのまとめ

NTT グループのデータによると、オンラインビジネスで存在感を示している企業にとって、サービス拒否攻撃は一般的でかつ脅威をもたらすものであり続けることは明らかです。特にこのケースにおいては、XYZ 社では、DoS/DDoS 攻撃に対する防御への投資が先手を打って行なわれていました。攻撃が発見された時点で、専門家は Web アプリケーション攻撃による被害を即座に軽減する準備が整っていました。熟練した SOC アナリストが効果的な恒久防御策の検討と導入を行いました。その後、新たな WordPress 攻撃の標的と再びなった際には、XYZ 社にはサービス停止時間が発生しませんでした。

脅威による被害の軽減 — Web アプリケーション DoS/DDoS 攻撃

サービス停止時間は顧客のインタラクションに影響するだけではなく、どの企業においてもその評判に重大な衝撃を及ぼします。DoS/DDoS 攻撃の種類と手法はさまざまですので、それらすべてを止めるただ 1 つのソリューションというものは存在しません。しかし、適切なガイドラインに従って先手を打った階層的防御によって、これらの攻撃を防ぎ、影響を最小限に抑えることは可能です。次の推奨事項は、DoS/DDoS 攻撃の影響を軽減するためのものです。

- **企業のリスク評価を実施**：自組織で重要なデータおよびアプリケーションと、さまざまな攻撃が組織に及ぼす恐れのある潜在的な影響を特定します。攻撃によって、測定可能な影響を事業に与える機能停止が発生する恐れがあるのであれば、DoS/DDoS 被害軽減戦略を自組織のセキュリティ計画に盛り込みます。
- **公式な DoS/DDoS インシデント対応計画の作成**：インシデント対応計画に、DoS/DDoS 攻撃に対する準備と対応のガイドラインが含まれていることを確認します。
- **階層化された DoS/DDoS 防御戦略の導入**：自分の環境のあらゆる側面を検討して、オンサイト、クラウド、ISP ベースの各ソリューションを見直します。すべての DoS/DDoS 攻撃が同じものではありません。低帯域で低速なアプリケーション攻撃には、ネットワーク層をオーバーフローさせるレートベースのリフレクション攻撃とは異なる対応方法が必要となります。
- **ISP によるオプションの理解**：ISP およびサードパーティーすべての担当者名と電話番号が正確に記載された連絡先リストを作成して、すぐに連絡を取って協力を求めることが出来るようにします。DoS/DDoS の検出や被害の軽減を行うサポート オプションについて、実際にこのようなサービスが必要となる前に ISP と相談しておきます。
- **教訓の再検討**：DoS/DDoS 攻撃の後には、その攻撃が成功であったか否かによらず、そこから得られた教訓を再検討して将来的な攻撃の管理に役立てます。
- **環境の試験**：攻撃を受ける前に公開されているシステムの試験を行い、システムの限界と弱点を見つけて、被害を軽減します。
- **監視付きマネージド セキュリティ サービスの活用**：お使いのマネージド セキュリティ サービス プロバイダーが提供する DoS/DDoS による被害の軽減と評価に関するあらゆるサービスの製品評価を行います。その機能の理解と、サードパーティーのサービスがそれ以外に利用可能なリソースをいかに補完可能であるかの理解を、積極的に行います。

「分散型サービス拒否攻撃」に関しては、以下の項目も参照してください。

DDoS 攻撃序論

分散型サービス拒否の観測結果

分散型サービス拒否の種別分布のカレンダー形式表示

セクション G：NTT グループのリソース情報

セクション G.1：NTT グループのセキュリティ関連会社

NTT グループのセキュリティ企業（NYSE: NTT）である Solutionary は、マネージド セキュリティ サービスとグローバルな脅威インテリジェンスの提供に重点を置く、次世代マネージド セキュリティ サービス プロバイダー（MSSP）です。包括的な Solutionary のセキュリティ監視サービスおよびセキュリティ機器管理サービスは、従来型およびバーチャル型の IT インフラストラクチャ、クラウド環境、そしてモバイル データに対する保護を提供します。Solutionary のクライアントであれば、現行のセキュリティ プログラムの最適化を行い、十分な情報を得た上でセキュリティに関する決定を下すことが可能となります。さらに、規制上のコンプライアンスを確保し、コストを抑えることが可能です。特許取得済みのクラウドベースによる ActiveGuard® MSSP プラットフォームでは、複数の検出技術と最新の分析論を用いて最新型の脅威からの防御を行います。Solutionary のセキュリティ エンジニアリング 研究チーム（SERT）では、グローバルな脅威領域の研究を進めており、実利的な脅威インテリジェンス、強化された脅威検出・被害軽減コントロールの提供を行っています。経験豊富で有資格の Solutionary のセキュリティ専門家は、クライアントの社内チームの追加戦力として機能し、金融サービス、ヘルスケア、小売り、政府などを含む広範囲な業界におけるグローバル企業やミッド マーケットのクライアントに業界最先端のクライアント サービスの提供を行っています。複数地点にある最高技術水準のセキュリティ オペレーション センター（SOC）を通じ、24 時間体制でサービスの提供を行っています。

Solutionary がセキュリティを高め、効率を改善し、コンプライアンスの負担を軽減します。詳細については、Solutionary の認定パートナーか、866-333-2133、info@solutionary.com、www.solutionary.com のいずれかから Solutionary に直接ご連絡ください。

NTT グループのセキュリティ企業（NYSE: NTT）である NTT コムセキュリティでは、情報セキュリティおよびリスク管理に関する全ての広範な業務を行っています。コンサルティング サービス、マネージド セキュリティ サービス、技術サービスが含まれる WideAngle サービスをお選びいただいたクライアントは、NTT コムセキュリティがリスク管理に集中する中で、ビジネスチャンスに自由に集中出来るようになります。

NTT コムセキュリティのガバナンス、リスク、コンプライアンス（GRC）対応、革新的なマネージド セキュリティ サービス、実用的な技術導入が広範囲であることは、クライアントと独自の視点を共有して、プロジェクトの優先順位の設定や標準化の推進の支援が可能であることを示しています。いつでも的確で客観的なアドバイスを提供できることが NTT コムセキュリティの願いです。

また、マネジドセキュリティサービスにおいては、自社開発による高度な相関分析エンジンとリスクアナリストによる脅威の迅速な検知、報告、セキュリティ防御機器等の管理サービスを通じた回復措置並びに防御への対応をグローバルに展開しています。この根幹となるセキュリティオペレーションセンタは世界 7 カ国に設置しており、グローバルでの脅威検知と対応と、地域に密着し他国へ情報が漏出しないオペレーションの双方を実現しています。

ビジネスにおいて、差別化要因として情報セキュリティとリスク管理の価値が増していることを基本理念として、NTT コムセキュリティのグローバルな手法は、コストと複雑性を排除するように設計されています。革新的な企業である NTT コムセキュリティは、NTT コミュニケーションズ グループの一員であり、アメリカ、欧州、APAC（アジア パシフィック）にオフィス、セキュリティオペレーションセンター及びコンサルティング拠点を展開しています。

NTT コムセキュリティと、情報セキュリティとリスク管理に対する独自サービスである WideAngle の詳細については、アカウント営業担当者にお問い合わせください。地域別連絡先については、www.nttcomsecurity.com に記載されています。

NTT グループのセキュリティ企業（NYSE: NTT）であり、世界最大のセキュリティ システム インテグレーターの 1 社であるディメンションデータでは、ネットワーキング、セキュリティ、通信およびコラボレーション、データ センター、仮想化、**エンドユーザ** コンピューティングなどのさまざまな IT 領域を網羅する、幅広い技術的知見とインテグレーション技術の提供を行っています。ディメンションデータは 14,000 人を超える従業員にて 5 大陸の 52 ヶ国で事業を展開しており、5 箇所のグローバル サービス センターにおいて、24 時間体制で 125 億 US ドルを超えるネットワーク インフラストラクチャの管理を 16 言語以上で行っています。金融サービス、通信、ヘルスケア、製造、政府、教育を含むあらゆる産業部門において、6,000 以上のセキュリティ クライアントにサービスを提供しています。ディメンションデータのリアルタイムなセキュリティ情報イベント管理アーキテクチャは、複数のセキュリティ技術コントロールからのセキュリティ情報を相互に関係づけることにより、SOC アナリストが攻撃、脅威、露出を集中管理可能な、全社的リスク管理ソリューションをベースとしています。このソリューションにより、ディメンションデータのアナリストは、本当のセキュリティ脅威を迅速に特定して効果的で効率的な対応を行う一方で、疑陽性現象などのノイズ要因を取り除くことが可能となります。有資格のセキュリティ専門家から構成されるディメンションデータのチームは、5 大陸に跨るセキュリティ オペレーション センター（SOC）に属しており、他に並ぶもののないサイバーセキュリティの経験により、クライアントの IT 組織の知識ベースの増強を行います。ディメンションデータでは、どのようなサイバーセキュリティの脅威にも、クライアントを支援して対応と影響の軽減を行う用意が出来ている熟練した技術者により安心を提供します。取得済みの認証としては、ISO 9001、ISO 27001、ASD Protected Gateway、PCI DSS、Cisco MSCP、ACSI 33、ASIO T4 などがあります。

詳細については、お近くのディメンションデータのオフィスまでお問い合わせいただくか、www.dimensiondata.com をご覧ください。

NTT Innovation Institute, Inc.（NTT i3）は、シリコンバレーに拠点を置く、NTT グループのイノベーションと応用研究開発のセンターです。この研究所は NTT の事業会社およびその世界中のクライアントと密接に連動し、市場主導型でクライアントに焦点を合わせたソリューションとサービスの開発を行っています。NTT i3 は、年間 25 億ドル以上の研究開発投資を行う NTT グループの膨大な知的資本の上に構築されています。NTT i3 とそれが抱える世界有数の科学者と技術者は、著名なテクノロジー企業やスタートアップ企業と提携し、グローバル規模で戦略、

業務アプリケーション、データ、インフラストラクチャに跨り、市場をリードするソリューションの提供を行っています。

NTT i^3 の詳細については、www.ntti3.com をご覧ください。

「NTT グループのリソース情報」に関しては、以下の項目も参照してください。

NTT のグローバル データ分析手法

デジタル ビジネスの世界におけるグローバルな脅威インテリジェンスの勃興

GTIR 用語集

セクション G.2：NTT のグローバル データ分析手法

2014 年版のグローバル脅威情報レポートには、NTT グループのセキュリティ関連各社が 2014 年の 1 月 1 日から 12 月 31 日の間に収集したグローバルな攻撃データが収録されています。この分析は、クライアントならびにハニーポットやサンドボックスなどの NTT の研究環境から得られたログ、イベント、攻撃、インシデント、および脆弱性に関するデータに基づいており、数兆件のログと 60 億件以上の攻撃からのデータの概要が示されています。さらに、Web サイトには、2014 年の履歴データと、2015 年からは NTT グローバル脅威情報プラットフォーム（GTIP）によって毎日提供されている生データも掲載されています。

NTT グループでは、セキュリティ ログ、アラート、イベント、および攻撃に関する情報の収集を行い、背景情報がわかるように質を高めた上で、その背景情報と関連づけられたデータの分析を行っています。このプロセスによって、グローバルでのリアルタイムな脅威のインテリジェンスと警報出しが可能になります。18,000 を超えるクライアント数の規模と多様性があることによって、NTT グループでは、大半の組織が遭遇した脅威を正確に代表するセキュリティ情報の集合が可能となっています。

このデータは、イベントの種別または頻度から攻撃を特定する、世界中でロギングされたイベントから導出されています。生のログデータやネットワーク トラフィックではなく、確認された攻撃イベントを用いることで、実際の攻撃回数をより正確に表現可能です。この手法により、結果データに信頼性が加わります。攻撃イベントの適切なカテゴリー分けがないと、不相応に多いネットワーク情報収集トラフィック、疑陽性の現象、正当なセキュリティ スキャン、セキュリティ オペレーション センター（SOC）で能動的に監視された大量の DDoS などが邪魔をして、攻撃の実際の発生率の特定が困難になります。

最終的に、NTT グループのセキュリティ関連各社からのデータを取り込むことで、世界中の脅威の現状をより正確に表すことが可能になります。

「NTT グループのリソース情報」に関しては、以下の項目も参照してください。

NTT グループのセキュリティ関連会社

デジタル ビジネスの世界におけるグローバルな脅威インテリジェンスの勃興

GTIR 用語集

セクション G.3：記事: デジタル ビジネスの世界におけるグローバルな脅威インテリジェンスの勃興

NTT グループのセキュリティ チームは、グローバル脅威情報レポート（GTIR）の作成に、NTT のインフラストラクチャ全体に対するマネージド セキュリティ サービス、プロフェッショナル サービス対応、カスタマー インシデント、および NTT の新たなグローバル 脅威インテリジェンス プラットフォーム（GTIP）などの大規模なデータ収集を行うツールと技術を使用しました。この中には、ディメンションデータ、NTT データ、NTT コムセキュリティ、Solutionary、NTT Innovation Institute（NTT i3）から提供されたデータや分析内容も含まれています。

IT に対する課題

NTT では、最近のセキュリティ状況では標準的なものであるさまざまな攻撃を取得するために、データ収集の対象を広く取りました。本レポートでは、NTT はこの広範なデータセットを用いて攻撃の分析を行いました。実際に、この同一の課題というのは各 IT 部門が毎日直面しているものであり、これと同じ種類の攻撃に対応しなければなりません。

組織的 IT は、オンプレミスならびにクラウドのサービスに、攻撃の状況が多様なものとなる SaaS ベース サービスを組み合わせたハイブリッド モデルの中に存在します。それと同時に、コンプライアンスや法規が支配的な業界の IT 部門では、既存のミッション クリティカルなシステムに対して高いレベルのセキュリティを維持する必要があることから、「バイモーダル」な世界を構築しています。

インフラストラクチャの多様性によって、セキュリティ業務の管理の複雑性が劇的に増大し、ローカルなインフラストラクチャのみには限られない分析が求められています。サイバー犯罪は、グローバルな組織化が行われており、豊富な資金と熟練度を有していますが、さらには、大半の組織のセキュリティ担当者に対しても余裕で数的に勝っています。

この課題にはいろいろな側面がありますが、その理由は以下のものです。

- 新規技術を学習する負担
- ROI の回収が難しいコストの増加
- 熟練した技術者と専門家の世界的な不足
- さまざまな必要製品間で不統一なユーザー体験
- 製品階層間のインテグレーションにおける互換性の無さや不十分さ

従来の典型的なフレームワークは、全く異なる戦いのために設計されたものです。これらのフレームワークは、各種のネットワーク アクセス ポイント、プロセスおよび製品の制御と防御を行うために、さまざまベンダーが提供するさまざまな製品を数多く必要としています。セキュリティ コントロールは、ネットワークの周りに「壁」を築いて、エンドポイントとサーバーばかりではなく貴重なデータと情報をも保護するために、ネットワークと製品の階層構造を用いて実現されています。

危機インテリジェンスの概観

危機インテリジェンスによって、企業は、世界の広範な背景情報に基づく、確認済みで実利的なライブの裏付けデータを用いて、顧客のセキュリティ上の問題に対応可能となります。グローバルなセキュリティ コミュニティ、顧客、ベンダー、業界フォーラム、および政府との密接な共同作業により、入手できるセキュリティ情報の品質は向上しています。最も必要なものは、入手可能なセキュリティ情報を効果的に取り込んだ後に、背景情報を意識した分析を応用することにより純粋なインテリジェンスへと変換するフレームワークです。

この新たなフレームワークによって、製品、サービス、インテリジェンスが統合された階層構造を用いてセキュリティ コントロールを提供する業界の能力が強化されることでしょう。各組織が自分たちにとって意味のあるインテリジェンスを考えることが可能となり、自己環境に対する意識との組み合わせにより、リスク管理と適切なコントロールの適用がより上手に行えるようになります。最終的な「侵入に対する回復力の高い」フレームワークによって、サイバー犯罪、国家から資金提供を受けている攻撃、そしてハクティビズムといった、今日のデジタル ワールドからの圧力に対応できるように特別に設計された柔軟なセキュリティの中に、最新版が提供されることでしょう。

最良の脅威インテリジェンスによって、次のものに対してセキュリティの柔軟性と統合化が達成されます。

- 予防的防御
- 攻撃が開始される前の脅威による影響の緩和
- 仮に攻撃を受けた場合にも損害の最小化
- 損害からの迅速な回復
- 継続的に進歩するセキュリティ業務

脅威インテリジェンスは発展途上のセキュリティ能力であり、数多くのベンダーが市場に参入しつつあります。ベンダー各社では、自社のインストールベースやカスタマー サービス対応からのデータを活用しています。市場の脅威インテリジェンスは、配信技術、情報源の性質、データの信憑性、地理的範囲による制約を受けています。

NTT グローバル脅威インテリジェンス プラットフォーム（GTIP）

脅威インテリジェンスの世界の中、NTT の GTIP では、NTT が保有するグローバル インフラストラクチャ、脅威センサー ネットワーク、およびグローバル規模のパートナーからの脅威情報の収集、分析、交換、そして使用を行っています。GTIP によって、NTT のセキュリティ専門家は、サイバーセキュリティの脅威を最小限に抑え、損害を軽減し、迅速な復旧を行ってビジネス上の混乱を効果的に抑制できる実利的な見識の提供が可能となります。この脅威インテリジェンスにより、NTT グループでは、NTT クラウド サーバー上で稼働するクラウドやアプリケーションに対する危機監視などの新たに強化された予防的セキュリティ サービスの提供が可能となっています。

「NTT グループのリソース情報」に関しては、以下の項目も参照してください。

NTT グループのセキュリティ関連会社

NTT のグローバル データ分析手法

GTIR 用語集

セクション G.4：GTIR 用語集

以下の用語が GTIR の中で使用されています。

ゼロデイ攻撃：それまで知られていなかったソフトウェアの脆弱性をエクスプロイトする攻撃

APT（持続的標的型攻撃）：長期的な目標を持ち、高度な技量と豊富な資金を有する攻撃者であり、通常は政府や組織的犯罪によるもの。通常、APT は最大の便益を得るために複数の技術を用いた複合的攻撃となる。

ボットネット：同時に指令やコマンドの受信が可能な、攻撃者が制御する複数のシステム。多くの場合、ボットネットは DDoS などの種類のサイバー犯罪活動の中で使用されているものが観測される。

脅威：ネットワークやシステムが不正利用されることにより、組織のデータが盗まれたり公開されたりするサイバー攻撃

BYOD（Bring Your Own Device）：企業の作業環境の中で従業員に個人所有のモバイル機器の資料を認める慣行

C&C（コマンド コントロール）：ボットネット内のボットに指令を与えたり、管理上のタスクを実行したりするために攻撃者が使用する通信インフラストラクチャ

CVE（共通脆弱性識別子）：一般に知られている脆弱性のカタログ

サイバー攻撃：コンピューター ネットワーク システムに損害を与えたり、混乱させたり、破壊したりしようとするハッカーによる企て

サイバー犯罪：コンピューターやネットワークが関係する法規違反

サイバー犯罪人：ツールもしくは標的、またはその両方としてコンピューターを使用してサイバー犯罪を犯す個人またはグループ

サイバー脅威：コンピューターのネットワークやシステムを混乱させるための悪意ある企ての可能性

ダークウェブ：一般にはアクセスできないプライベートなネットワーク。多くの場合、これらのネットワークは無法な目的や不正な目的のために利用される。

DoS（サービス拒否）および DDoS（分散型サービス拒否）：マシン リソースまたはネットワーク リソースを意図したユーザーには利用できなくする攻撃。DDoS 攻撃は、同時に多くの機器から発生する。

流出：ある組織からのデータの不正な抽出

エクスプロイト キット：悪意のあるツールキットであり、多くの場合はソフトウェア アプリケーションの脆弱性をエクスプロイトするためにサイバー犯罪で用いられる。

ファイアウォール：事前に定められたルールセットに基づき、データ パケットを分析してそれが許されるべきものかどうかを判定することで、流入と流出のネットワーク トラフィックを制御するように設計されたソフトウェアまたはハードウェア

ハクティビスト：活動（ハクティビズム）が社会的な主張や政治的な主張を推進することを狙っているハッカー

ハニーポット：攻撃や攻撃者に関する情報を収集するため、そして場合によっては、攻撃を企業環境からそらすために設定されるおとりシステム

IDS（侵入検知システム）：通常、ネットワークをベースとし、潜在的に悪意のあるネットワーク異常の発見にシグネチャや発見的方法に依存する。

インシデント対応プログラム：サイバー攻撃に対処し、その影響を制御するための組織の計画

注入：受信側システムが有効なクエリとして扱うものに悪意のあるコードやデータを挿入することにより行う攻撃

IP レピュレーション：ホストのマルウェアから信頼されるか否かによって IP アドレスを区分するデータベース

IPS（侵入予防システム）：潜在的に悪質と特定されたトラフィックをブロックする追加のステップを利用することを除いては、一般的にネットワークをベースとするもので、IDS に類似している。

IRC：インターネット リレー チャット

ISP：インターネット サービス プロバイダー

マルウェア：ウイルス、ウォーム、トロイの木馬、スパイウェアなどの悪意のあるソフトウェアに対する一般的用語

NTP（ネットワーク タイム プロトコル）：システム クロックの同期を保つために、時刻情報を交換するプロトコル

OWASP：オープン Web アプリケーション セキュリティ プロジェクト

パッチ管理：ベンダーから提供を受けたソフトウェア パッチをインストールする系統的プロセス

防衛ライン：ある組織をインターネットに接続するインターフェース システム

フィッシング：電子的通信（電子メール）において信頼できるエンティティになりすますことにより、ユーザー名、パスワード、クレジットカードの詳細情報（さらには間接的に金銭も）などの情報を取得しようとする企て

ランサムウェア：被害者のデータを暗号化し、暗号キーとの交換でランサム支払いを要求するマルウェア

ソーシャル エンジニアリング：個人的な訪問、電話通話、ソーシャル メディア Web サイトなどの手法により不正なアクセスを獲得すること。この攻撃は主として人間を標的とし、セキュリティに関連する人的な弱点を活用する。

スピア フィッシング：特定の個人や組織に対する知識を用いて、高度に標的が設定されたフィッシング攻撃

標的攻撃：特定の個人、会社、組織に向けられた攻撃

トロイの木馬：正規のファイルや有用なプログラムのように見せかけられているが、無法行為のために設計されたマルウェアの種類

脆弱性ライフサイクル管理（VLM）：脆弱性の発見、文書化、追跡、修理を行う系統的プロセス

WAF：Web アプリケーション ファイアウォール

「NTT グループのリソース情報」に関しては、以下の項目も参照してください。

NTT グループのセキュリティ関連会社

NTT のグローバル データ分析手法

デジタル ビジネスの世界におけるグローバルな脅威インテリジェンスの勃興