News Release

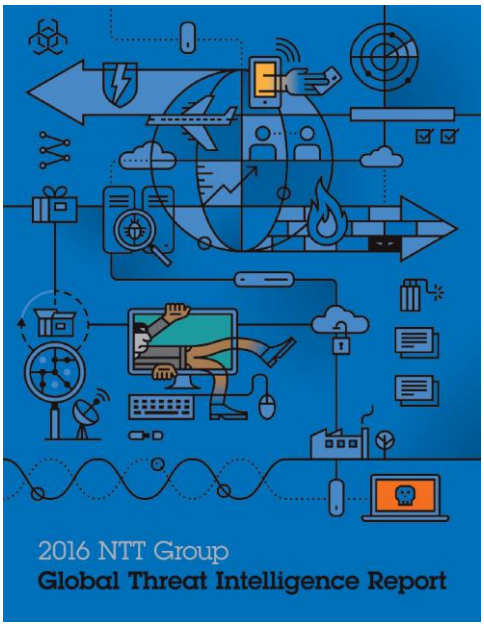
NTT Communications

2016 年 6 月 14 日

日本語版グローバル脅威インテリジェンス・レポートの公開

～自社でインシデントレスポンス対応能力がある企業は全体の 23%に留まる～

NTT コミュニケーションズ（略称：NTT Com）は、NTT グループにおけるセキュリティ関連各社が共同で編集、編纂した「グローバル脅威インテリジェンス・レポート 2016」の日本語版を本日公開します。



※本レポートは以下 URL よりダウンロード可能
WideAngle セキュリティリポートページ
http://www.ntt.com/business/services/security/security-management/wideangle/security-report.html

本レポートは、NTT Com Security AG、 Solutionary, Inc.、Dimension Data Holdings plc、NTT Data Inc.、NTT の研究所の協力を得て、NTT Innovation Institute（NTT I3）がとりまとめた[*1]、2015 年の IT セキュリティに関わる脅威のグローバル全体でのトレンド、対策方法、関連技術などを伝えるレポートで、2016 年 5 月 18 日に発表された英語版「2016 NTT Group Global Threat Intelligence Report」の全文日本語訳です。

NTT グループにて世界 24 カ所に展開しているセキュリティオペレーションセンターでの監視、100 カ国に設置したハニーポット[*2] およびサンドボックス[*3] によって脅威情報を収集し、３.５兆個のログと６２億件の攻撃データの分析を基に本レポートは制作されています。また、本レポートは４年目を迎え、有力な専門性の高い企業の協力を得て、脅威の実態を多角的に分析しています。

NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

NTT グループの全世界規模および各業界の顧客企業の基盤も対象に分析されたレポートであるため、海外に事業展開するあらゆる業種の日本企業にとって、情報セキュリティ対策導入を検討するための一助になると考え、本レポートの日本語版を作成しました。

NTT Com ならびに NTT グループは、今後も世界規模の分析およびレポートを定期的に発信していきます。

1. 「グローバル脅威インテリジェンス・レポート 2016」のポイント
―「あらゆる組織が日々、セキュリティ予算と資源を如何に最適に割り当てるべきかという決断に迫られています。マルウェアや攻撃、技術の進歩が状況を複雑にし、判断をより一層困難なものにしている。」（本文より）

セキュリティプログラムを進歩させて、限りある資源をより効果的に運用するには、ICT 環境全体に行き渡った包括的な解決策が求められます。
今回のレポートでは、「Lockheed Martin[*4] サイバーキルチェーン(CKC)[*5]」をベースとした各フェーズにて、「Center for Internet Security[*6]」の「クリティカルセキュリティコントロール[*7]」による有効な対策を確立し、実用的なセキュリティ強化策のケーススタディを紹介しています。
また、2015 年における顧客に対する攻撃と脆弱性情報を詳細に分析し、業種および地域別の観点で評価しています。

【主な調査結果】
・全業種の中で最も攻撃されたのは小売業であり、次いで観光関連業であった。前者ではクレジットカード情報が、後者では個人情報がターゲットとなった。なお、NTT グループで対応したインシデントレスポンスの 22%が小売業であり、次いで金融業が 18%を占めた。
・攻撃の送信元として使用された IP アドレスの 65%が米国拠点のものであった。(同 IP アドレスは攻撃に利用されたものであり、米国人が攻撃者ということではない。)
・教育以外のすべての産業にてマルウェア検知数が 18%上昇した。
・顧客内部で攻撃に使用された脆弱性の 21%が、公表されてから 3 年以上放置されたものだった。
・Exploit[*8] で標的とされた脆弱性のうちトップ 10 は全て Adobe Flash 関連だった。
・企業顧客に対する DDoS/DoS 攻撃[*9] は 2014 年と比べて 39%低下する一方で、ブルートフォース攻撃[*10] は 2.4 倍になった。
・自社でのインシデントレスポンス対応能力があるのは、全体の 23%に留まっている。

２．「グローバル脅威インテリジェンス・レポート 2016」の掲載場所

WideAngle セキュリティリポートページ
http://www.ntt.com/business/services/security/security-management/wideangle/security-report.html

※「2016 Global Threat Intelligence Report」（英語版）は以下の URL よりダウンロード可能です。
https://www.nttcomsecurity.com/en/services/managed-security-services/threat-intelligence/

*1：日本電信電話株式会社より 2016 年 6 月 6 日に報道発表されたように、セキュリティ専門会社として NTT セキュリティ株式会社が設立され、NTT Com Security AG 及び Solutionary, Inc.は同社に統合、NTT コミュニケーションズ及び Dimension Data Holdings plc、NTT Innovation Institute（NTT I3）の高度分析基盤、セキュリティ脅威情報、セキュリティ専門技術も集約し、2016 年 8 月 1 日に事業開始予定です。（http://www.ntt.co.jp/news2016/1606/160606a.html）

*2：攻撃または攻撃者の情報を集めることや、攻撃者の目を会社のシステムからそらすことを目的とした、囮システム。

*3：高度に保護された領域で疑わしいコードを実行させてその動作を検証するソフトウェア。

*4：Lockheed Martin（ＬＭ）は、フォーチュン１０００社およびグローバル１０００社のために、開発、実装、保守、および重要インフラの保護に焦点を当てたサイバーセキュリティソリューションの世界的プロバイダーです。ＬＭのエンジニアは文字通り世界に広がり、５０の州と７５の国の６００拠点において、４,０００のプログラムを監督しています。当社は３,０００人以上のサイバーセキュリティのプロフェッショナルを雇用し、ＩＴとＯＴ技術の強固なパートナーシップを有しています。ライフサイクルに焦点を当てた当社の製品やプログラムは、当社の商業顧客のインフラ全体の成功と持続可能な保護ネットワークの両方を可能にします。当社のアプローチは、攻撃をしようとしている者の情報を活用し、それを彼らに対して使うことにフォーカスする Intelligence Driven Defense® の考え方に基づいています。（www.lockheedmartin.com）

*5：サイバー侵入に対抗するための分析と防御のためのフレームワーク。ロッキードマーティン社が２０１１年の論文で最初に論じた。

*6：The Center for Internet Security（ＣＩＳ）は米国の内国歳入法典第 501 条Ｃ項３号の規定に基づく非営利公益法人であり、公共および民間組織のサイバーセキュリティの備えと対策の強化を推進しています。業界と政府の強力なパートナーシップを活用し、ＣＩＳは地球規模でのサイバーセキュリティの課題の進化と戦い、サイバー攻撃に対する迅速かつ効果的な防御を達成するためのキーとなるベストプラクティスを、組織が適用することを支援します。ＣＩＳは、マルチステート情

報共有分析センター（ＭＳ－ＩＳＡＣ）、ＣＩＳセキュリティベンチマーク、およびＣＩＳクリティカルセキュリティコントロールを運営しています。（https://www.cisecurity.org/）

*7：米国ＣＩＳ（Center For Internet Security）が発行する、サイバー攻撃に対する推奨防御対策。

*8：セキュリティ上の脆弱性を攻撃するために作成された簡易プログラムの総称。

*9：コンピュータに対する攻撃の一種。コンピュータやネットワークのリソースを大量に消費して、本来のユーザが使えなくする。

*10：総当たり攻撃。暗号の解読やパスワードの割り出しなどに用いられる手法の一つで、割り出したい秘密の情報について、考えられるすべてのパターンをリストアップし、検証する方式。