NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ
NRI SecureTechnologies

News Release

2017 年 7 月 26 日
NRI セキュアテクノロジーズ株式会社

「サイバーセキュリティ傾向分析レポート 2017」を発表

～ “気軽な IT 利用”が増大させるセキュリティリスク ～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：小田島 潤、以下「NRI セキュア」）は、顧客企業に提供した情報セキュリティ対策サービスを通じて蓄積したデータ※1 を元に、最新の動向分析と推奨する対策を、「サイバーセキュリティ傾向分析レポート 2017（以下「本レポート」）」としてまとめました。本レポートは、企業や公的機関の情報セキュリティ対策の推進を支援する目的で、2005 年度以降毎年発表しており、今回で 13 回目となります。

今回のレポートで注目される点は、以下の 3 つです。

■ セキュリティ対策が十分でない IoT 機器への攻撃が大幅に増加

NRI セキュアが提供するマネージドセキュリティサービスにおいて、2016 年度中にファイアウォールでブロックした通信（全標本数 22.6 億件）のうち、48.1%（10.9 億件）が遠隔操作に用いられる telnet※2 ポートへの通信でした。2015 年度の 1.7 億件に比べると、約 6.4 倍に増加しました。

現在、多くの企業では、外部から telnet ポートへの通信を許可しないことが一般的です。それにも関わらず、上記の通信が急増した背景として、アクセス制限が行われていない Web カメラやルーターなどの IoT 機器を探索し、侵入しようとする通信が増えたことが大きな要因と考えられます。気軽に使えるようになったこれらの機器が脆弱な状態にあると、DDoS 攻撃※3 の踏み台となるなど、悪用される可能性があります。

IoT 機器の利用者は、使用前にアクセス制限や機器そのものの設定などを適切に行うことが推奨されます。また機器メーカーは、標準仕様で必要なセキュリティ機能を持たせることや、販売後においても脆弱性が発覚した時には、速やかに対応できる体制を整えることが必須になっていくと考えられます。

■ HTTPS 通信（暗号化通信）への移行が加速する一方、新たな問題が浮上

「FNC セキュアインターネット接続サービス」において、Web アクセスに関するログ（調査対象企業数 20 社）を集計したところ、HTTPS 通信の割合が 2016 年 4 月の 19%程度から、2017 年 3 月には 40%にまで増えたことがわかりました。

従来 HTTPS は、Web サイト内にあるログイン画面や個人情報など、機密性の高い情報を扱うページの暗号化のために利用されてきました。ところが昨今、大手インターネットサービス会社の全ページが HTTPS に移行されるなど、重要情報の有無に関わらず、サイト全体

を暗号化する企業が増えています。

HTTPS が広く使われるようになったことにより、セキュリティ強化が期待される一方、暗号化された通信は通信経路上で内容の検査ができず、従来行われてきた通信経路上のセキュリティ対策ができなくなる問題が浮上しています。また、多くのクラウドサービスが HTTPS 通信で暗号化されているために、サービスを利用する企業では、従業員の利用状況の可視化や統制がしづらくなるという問題も出てきています。HTTPS 化の流れが進む中、企業はこの問題を認識し、HTTPS 化に対応したセキュリティ対策の実施が求められます。

■ 企業 Web サイトのうち、4 割が容易に攻撃可能な状態

世界中に点在している、顧客企業に関連する Web サイトを探索し、棚卸しするサービス「Web サイト群探索棚卸サービス GR360（ジーアール 360）」で、NRI セキュアが 2016 年度に調査した Web サイト（全標本数 4,039 サイト）のうち、4 割が容易に攻撃される可能性があることがわかりました。

古いバージョンのソフトウェアを使用し続けていたり、ID とパスワードの単純な認証だけで保護されているメンテナンス用インターフェースが外部に公開されていたりすると、その Web サイトでは容易に攻撃が成立する可能性があります。これはマーケティングキャンペーンのサイトや、中小企業のコーポレートサイトに多くみられます。背景には CMS※4 を利用することで、専門的な知識をそれほど必要とせず、比較的容易に Web サイトを構築できる反面、セキュリティの堅牢化に関するノウハウが十分に提供されていないことが挙げられます。

企業全体の Web サイトのセキュリティ水準を維持するためには、まず、自社の Web サイトの存在をセキュリティの管轄部門が把握することが重要です。その上で、一元的な管理を行い、サイトの安全性が一定の水準を満たしているか検証することが望ましいと言えます。

「サイバーセキュリティ傾向分析レポート 2017」の詳細については、下記の Web サイトを参照ください。

http://www.nri-secure.co.jp/security/report/2017/cstar.html

※1　本レポートで分析対象としたデータ：NRI セキュアが、2016 年度（2016 年 4 月 1 日～2017 年 3 月 31 日）に、顧客企業へ提供した情報セキュリティ関連サービスから得られたデータ。分析対象としたサービスは、マネージドセキュリティサービス（FNC セキュアインターネット接続サービス、FNC セキュア Web ネット管理サービス、セキュリティログ監視サービス）、セキュリティ診断サービス（プラットフォーム診断、Web アプリケーション診断、スマートフォンアプリケーション診断、Web サイト群探索棚卸（GR360）、標的型メール攻撃シミュレーション、プラットフォーム診断エクスプレスサービス）

※2　telnet：ネットワークに接続された機器を遠隔操作するために使用するプロトコルのひとつ。例えば別室にあるルーターなどの IoT 機器を自席のパソコン上で操作できる。ここでは 23 番ポートへの通

信を指す（23/tcp）。通信の暗号化や証明書を利用した接続先の正当性を確認する機能を持たない。

※3　DDoS 攻撃：Distributed Denial of Service の略。大量の通信を発生させ、標的をサービス不能に陥らせる攻撃。

※4　CMS：Contents Management System の略で、HTML や CSS などの知識がなくても Web サイトのコンテンツを作成・管理できるシステム。

【ニュースリリースに関するお問い合わせ】

株式会社野村総合研究所　コーポレートコミュニケーション部　日下部、松本

TEL：03-5877-7100　E-mail：kouhou@nri.co.jp

【レポートに関するお問い合わせ】

NRI セキュアテクノロジーズ株式会社

サイバーセキュリティサービス開発部　内藤、西田

広報　根本

TEL：03-6706-0622　E-mail：info@nri-secure.co.jp