【NRI セキュアからのお知らせ】

2018 年 8 月 21 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 2018」を発表

～ 不要なポートの公開、シャドーIT、クリプトジャッキングへの対策を ～

NRI セキュアテクノロジーズ株式会社（以下「NRI セキュア」）は、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、サイバー攻撃などに関する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 2018（以下「本レポート」）」※2 としてまとめました。

今回の分析結果で注目すべき点は、以下の 3 つです。

■ 意図せず外部開放されたポートや経路から、IoT 機器やサーバ、Web サイトが狙われる

2017 年度中に、セキュリティ上のリスクからファイアウォールでブロックされた通信※3 を分析すると、ブロックされた通信件数が多い上位 100 種類のポートのうち、IoT 機器を狙ったものは 16 種あり、それらの通信件数の合計はブロックされた件数全体の 38.0%を占めました。とりわけ、telnet※4 ポートへの通信が全体の 29.2%を占め、昨年度の結果（48.1%）よりも減少しましたが、その一方で IoT 機器への侵入を図ろうとして探索行為を行うポートに分散傾向がみられました（図 1）。

また、サーバやネットワーク機器を診断したところ、それらの 24.9%が本来公開不要なポートをインターネットに開放していたほか、公開 Web サイトに関しては、12.2%がメンテナンス用経路※5 を開放していることが分かりました。

これらは意図せずに開放されていることが多く、外部から攻撃されてシステムそのものを乗っ取られてしまう危険性をはらんでいるため、アクセスを許可する対象を把握し、設定管理やアクセス制御を実施する必要があります。

■ 企業のクラウド利用を脅かす“シャドーIT”

情報システム利用に伴って生じるアクセスログに基づき、代表的な 3 つのクラウドサービスについて企業が利用している割合を調べたところ、2017 年 3 月時点と 2018 年 3 月時点では、各サービスともに 10 ポイント以上増加していました※6（図 2）。

クラウドサービスの利用普及に伴い、管理部門による許可・承認なしに、事業部門や従業員が IT 機器・サービスを利用する“シャドーIT”は増えていると推測されます。仮に、管理部門が把握していないところで社内文書がインターネット上にアップロードされ、更にファイルの公開設定に不備があって、第三者もそのファイルを閲覧できてしまうと、機密情報が漏洩するリスクが高まります。そのようなケースでは、対策面においても、「クラウドサービスの利用実態の把握が難しい」「定常的にモニタリングする仕組みの整備や、既存ゲ

ートウェイ機器での制御が難しい」「暗号化通信が、把握と制御を阻む」という、大きな課題があります。

有効とされる対策の一つは、クラウドサービスの利用を可視化・制御するためのツール「CASB（Cloud Access Security Broker）」の利用です。今後は、企業による CASB の導入が加速していくと考えられます。

■ クリプトジャッキングの事象が増加

仮想通貨のマイニング（採掘）ツールを Web サイトに設置し、サイト閲覧者の同意を得ないまま、その閲覧者の端末リソースを利用して、閲覧者が気づかないうちにマイニングを実行させることで、ツールの設置者が報酬を得る「クリプトジャッキング」が、2017 年 9 月以降増加しています。

NRI セキュアの次世代ファイアウォールを利用した企業について、クリプトジャッキングの可能性がある Web サイトへの月間アクセス件数を調査したところ、2017 年 8 月は約 1 万件でしたが、10 月には約 7 万件に急増しました※7（図 3）。

これらの Web サイトの中には、サイト管理者の意思でマイニングツールを設置したのではなく、攻撃者が Web サイトを改ざんして設置している可能性もあります。

クリプトジャッキングの事象については、対策や法整備が技術の進展に追いついていないため、今後の動向を注目していく必要があります。また、企業においては、自社の Web サイトを悪用されないため、日ごろからシステム全般の脆弱性に対して、迅速かつ適切な対応を取っていくことが今後一層求められます。

本レポートの詳細については、下記の Web サイトからご覧いただけます。

https://www.nri-secure.co.jp/report/2018/cstar2018.html

※1　ここでは、NRI セキュアが、2017 年度（2017 年 4 月 1 日～2018 年 3 月 31 日）に、顧客企業向け情報セキュリティ関連サービスから得られたデータを指す。

※2　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 14 回目となる。

※3　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、ファイアウォールでブロックした件数を指す。分析に使用した全標本数は、25 億件に達する。

※4　telnet とは、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。ここでは最も使われることの多い 23 番ポートへの通信を指す（23/tcp）。

※5　メンテナンス用経路には、FTP(21/tcp) または SSH(22/tcp) サービス、管理用ポート、管理用サブドメイン、コンテンツ管理用機能が含まれる。

※6　FNC セキュアインターネット接続サービスにおいて、1 ヶ月の間に、1 セッションの通信量が 1MB を越える通信が確認できたものについて、当該クラウドサービスの利用があったと判断してその件数を集計している。今回調査したクラウドサービスは、「Microsoft Office365」「Dropbox」「Evernote」。2017 年 3 月時点の調査対象企業数は 41 社。2018 年 3 月時点は、35 社。

※7　FNC セキュアインターネット接続サービスにおいて、2017 年度に次世代ファイアウォールを利用し

た企業 39 社のアクセス先 URL を調査。なお、クリプトジャッキングの可能性がある Web サイトかどうかについては、2018 年 4 月時点でのサイト情報をもとに調査した。

【お知らせ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　広報担当

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

【ご参考】

図 1:ファイアウォールでブロックした通信件数

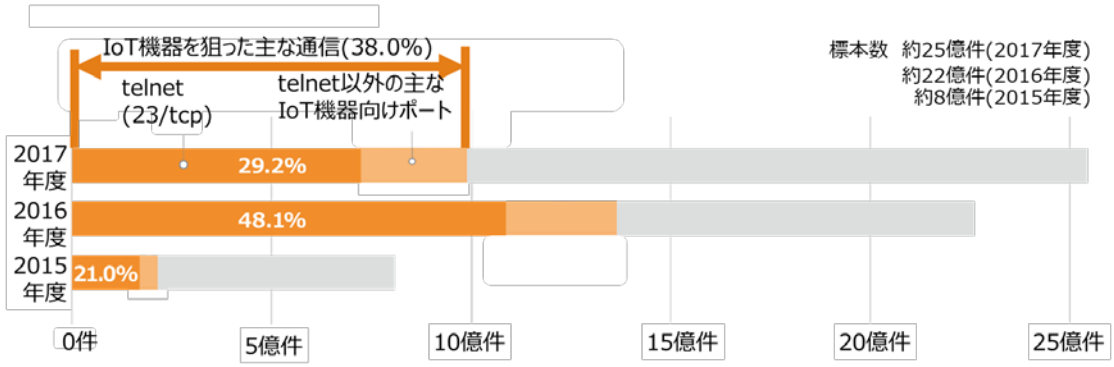

図 2:主なクラウドサービスを利用した企業の割合

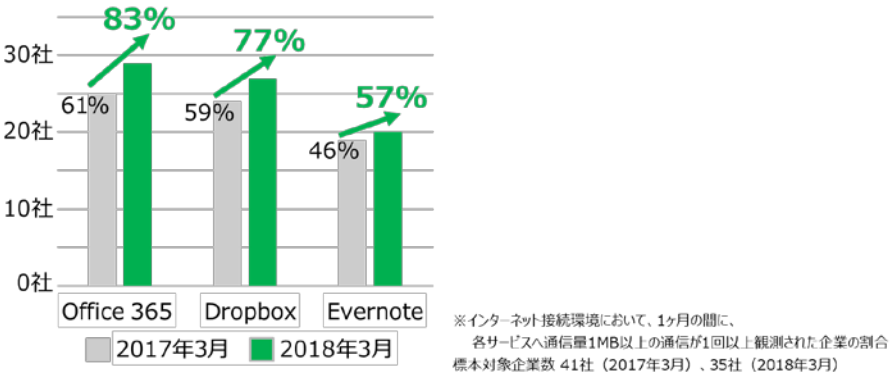

図 3:Web サイト閲覧者にマイニングを実施させる可能性がある URL へのアクセス件数