NRIセキュアテクノロジーズ

第257回NRIメディアフォーラム

サイバーセキュリティ傾向分析レポート2017

～“気軽なIT利用”が増大させるセキュリティリスク～

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サービス事業本部
サイバーセキュリティサービス開発部

上級セキュリティコンサルタント 内藤　陽介

〒100-0004
東京都千代田区大手町1-7-2 東京サンケイビル

目次

目次

「サイバーセキュリティ傾向分析レポート2017」について

経緯

- 当社が企業などに提供する、各種の情報セキュリティ対策サービスを通じて得たデータをもとに分析して、「サイバーセキュリティ傾向分析レポート2017」を作成
- このレポートは2005年度以降毎年発表しており、今回で13回目

目的

- 企業や公的機関におけるセキュリティ対策の向上

集計対象期間

- 2016年4月～2017年3月

レポートの概要

- サイバー攻撃に対する「企業などの対策状況」および「脅威の現状」を分析
- 分析結果を踏まえ、企業などが実施すべき対策を提示
- 分析対象のサービスおよび標本数については、次ページ及びP.28を参照

分析対象のサービスおよび標本数について

■ 分析対象サービス

- FNCセキュアインターネット接続サービス
  URLフィルタ20システム分、スパムフィルタリングサーバ26システム分のログ
- FNCセキュアWebネット管理サービス
  ファイアウォール96システム分、WAF 37システム分、次世代ファイアウォール41システム分のログ
- セキュリティログ監視サービス
  セキュリティインシデントに繋がるような攻撃かどうかを分析する必要があった918イベント
- プラットフォーム診断
  92システム分
- Webアプリケーション診断
  451システム分
- スマートフォンアプリケーション診断
  手動にて診断を実施した52アプリケーション（342指摘事項）
- Webサイト群探索棚卸サービス（GR360）
  4,039サイト
- プラットフォーム診断エクスプレスサービス
  1,090 IPアドレス分

本日の発表内容（今年のポイント）

- 脆弱なIoT機器を攻撃する通信が大幅に増加
  - ユーザー・メーカーともにIoT機器へのセキュリティ意識の向上を

- HTTPS通信とクラウドサービス利用の増加による新たな課題
  - 暗号化された通信に対してセキュリティを担保するための仕組みの検討が必要
    - SSLインターセプト
    - クライアントセキュリティ

- 4割の企業Webサイトは容易に攻撃可能
  - CMSの利用により増加傾向
  - 自社Webサイトの把握と適切な対応が有効

- 猛威を振るうマルウェアメール
  - 毎日のように新種マルウェアが届く時代
  - システム・ユーザーの両面で対策強化を

目次

目次

2-1. 脆弱なIoT機器を攻撃する通信が大幅に増加

telnet*1ポートへのアクセスを筆頭にIoT機器を標的とする通信を多数検知

- telnetを標的とした攻撃は、2016年度にはそれまで以上に大きく増加

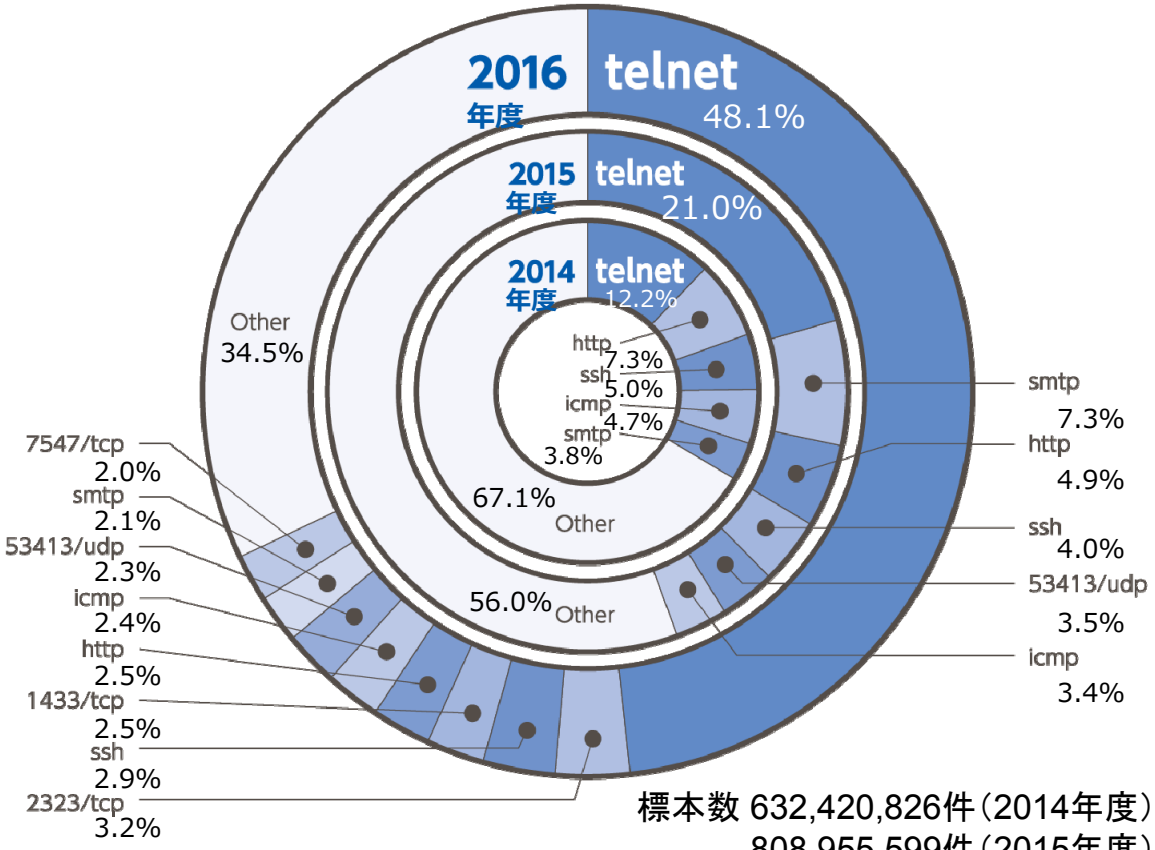
ファイアウォールでブロックした通信のうち、telnetポートへの通信の割合

21.0%→48.1%

（2015年度）　（2016年度）

- 過去にほとんど検出していなかった2323/tcpなどの通信も上位にランクイン
- IoT機器を標的とした攻撃が大きく増加している

■ファイアウォールでブロックした通信の件数(割合)



標本数 632,420,826件（2014年度）
808,955,599件（2015年度）
2,262,695,083件（2016年度）

*1: TCP/IPネットワークを通じて別のコンピュータにアクセスし、遠隔操作するためのプロトコルのひとつ

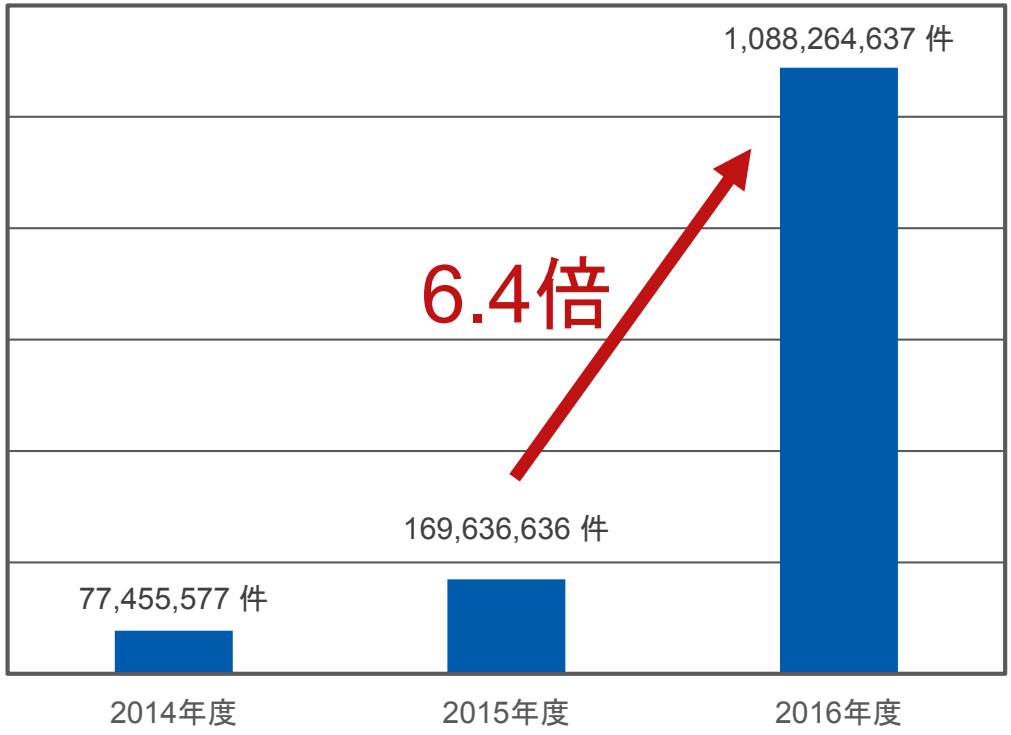
2-1. 脆弱なIoT機器を攻撃する通信が大幅に増加

件数ベースでは、telnetポートへのアクセスは2015年度比で約6.4倍に増加
背景に脆弱なIoT機器とそれを狙ったマルウェアの急増

- 従来の「コンピュータの世界」では、
  外部からのtelnetアクセスを
  遮断することは既に常識

- 「遮断は常識」なのに
  なぜ、通信が増え続けているのか？
  ⇒ 脆弱なIoT機器とそれを狙った
  マルウェア（IoTマルウェア）の急増

■ファイアウォールでtelnet通信をブロックした件数



2-1. 脆弱なIoT機器を攻撃する通信が大幅に増加

Miraiボットネットによる DDoS攻撃事例を皮切りに IoT機器を標的とするマルウェアを用いた大規模な攻撃を観測

■ Miraiボットネット
- 2016年9月に発生し、当時では史上最大*1のDDoS攻撃*2に使われたとされるボットネット*3
- PCではなくIoT機器に感染するマルウェア（IoTマルウェア）によって構成される
  - 感染機器は中国製Webカメラが多数を占めると言われる

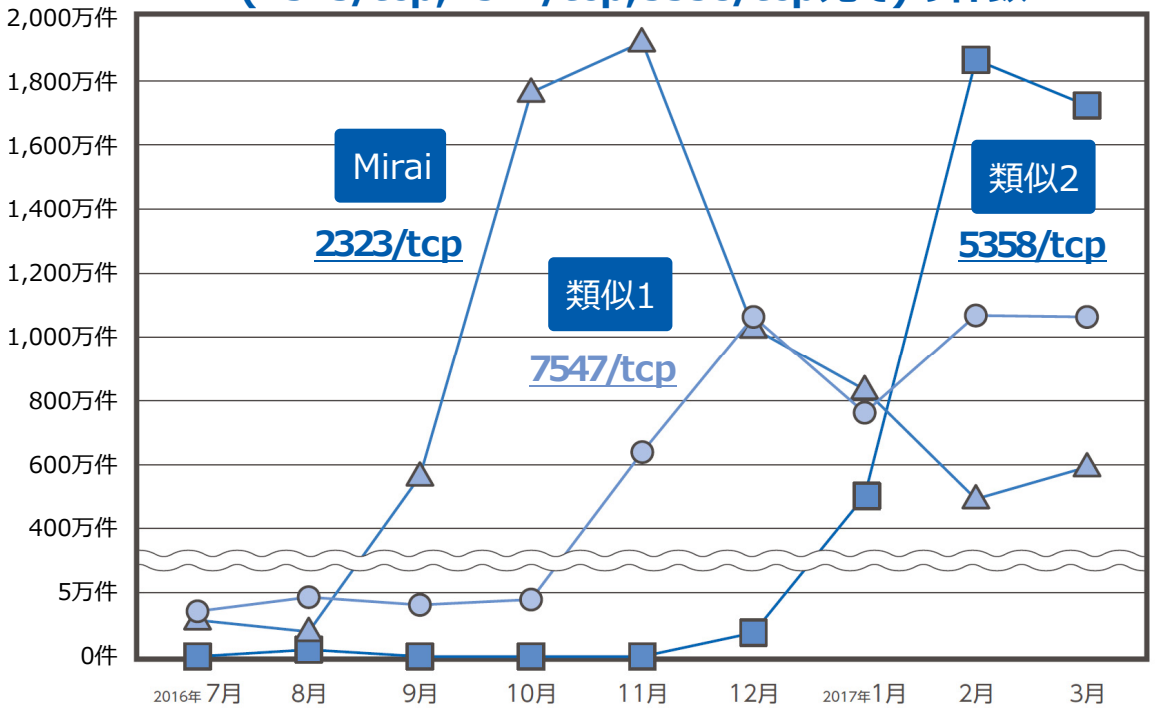
■ Miraiの感染経路
- telnetを用いて、ターゲットとなるIoT機器へ デフォルトパスワードなどの情報を用いて侵入
  - telnetのほか、TCP 2323番ポートも利用

多数の標的に対して初歩的な攻撃手法が成立

■ Miraiのオリジナルマルウェアに引き続いて 異なる機器を標的とする類似マルウェアが出現

多数のIoTデバイスが 格好の標的であることが再認識された

■ファイアウォールでブロックした通信 （2323/tcp,7547/tcp,5358/tcp宛て）の件数



*1: 著名ジャーナリストBrian Krebs氏のサイト「Krebs on Security」に対するDDoS攻撃で、ピーク時のトラフィックは665Gbpsに達した。
*2: 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。
*3: マルウェアに感染したデバイスによって構成される、大規模なネットワーク。マルウェアメール配信やDDoS攻撃などに利用される。

標本数 218,003,655件

推奨対策

IoT機器のセキュリティ対策は未熟なものが多い
セキュリティ水準の確保には、機器のユーザーとメーカー双方の努力が必要

- ユーザーに求められる対応
  - 活用する機器がどのような外部アクセスを許すかを把握し、必要に応じてアクセス制限や機器の設定を変更
  - 機器選定条件に、セキュリティ的に問題がない（あるいは代替的な対応が可能である）ことを選定条件に入れる
- メーカーに求められる対応
  - ネットワーク経由での攻撃を受け得ることを認識し、ライフサイクルに運用フェーズを追加する
  - セキュリティレベルの維持のために、専門組織PSIRT*1を立ち上げる

■IoT機器のライフサイクルにおいて求められるセキュリティ対策

フェーズ	セキュリティ対策	概　要
企　画	ビジネスモデル構築	セキュリティ運用に要するコストを回収できるビジネスモデルの構築
	人材育成	セキュリティ開発・運用を行う組織作りおよび人材育成
開　発	工場セキュリティ	IoT機器を製造する工場自体のセキュリティ確保
	対策技術の策定	IoT機器が攻撃に対して一定のセキュリティレベルを維持するための対策を上流工程から策定
	要件・仕様のセキュリティ分析	セキュリティ対策が想定脅威に対して充足しているかセキュリティ分析を実施
	セキュアコーディング	開発時に脆弱性が作りこまれないようにセキュアコーディングを導入
	リリース時の評価技術	リリース前に攻撃者目線でセキュリティ対策状況を可視化する評価技術の導入
運　用	脆弱性管理（PSIRT）	構成情報を管理しつつ、該当する脆弱性情報を収集、評価し、対策の必要性を判断
	鍵管理・パッチ配信	クリティカルな問題についてパッチ配信・機器の認証を行うための鍵を定期的に更新するなど管理
	ログ管理	プライバシー情報の保護およびログ情報を用いた攻撃動向の可視化

*1: Product Security Incident Response Team の略。自社製品に対する脆弱性情報の管理と対策のハンドリングを行うチームのこと。

目次

2-2. HTTPS通信とクラウドサービス利用の増加による新たな課題

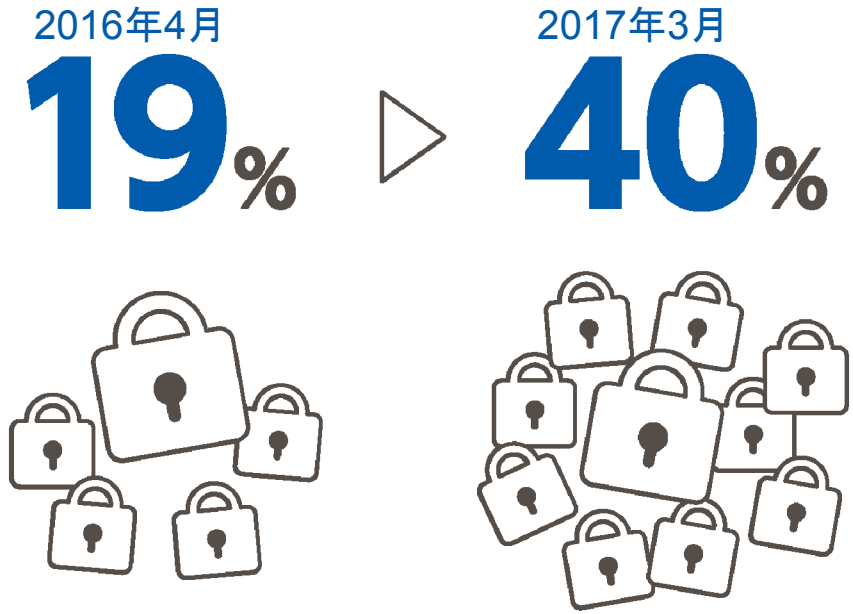
常時SSLの普及により、HTTPS化が急加速
全アクセスに占めるHTTPS通信の割合は1年で2倍となり、全体の40%を占める

■「常時SSL」とは
- 従来：ログイン画面や個人情報を取り扱う場面など、重要な情報をやりとりする画面のみを暗号化（HTTPS化）
- 常時SSL：重要情報の有無にかかわらず、サイト全体を暗号化

■ HTTPS化が急加速
- Googleなどが常時SSLを奨励する流れ
  - 検索順位に、HTTPS化を加点対象とする
- 大手サイトの常時SSL化推進
  - 日本でもYahoo! JAPANなどが常時SSL化を完了

■ 社内OA環境からのWebアクセスを対象とした
FNCサービスについてみると、
HTTPS通信の割合が1年で2倍以上、全体の40%に

■ **WebアクセスにおけるHTTPSリクエストの割合**

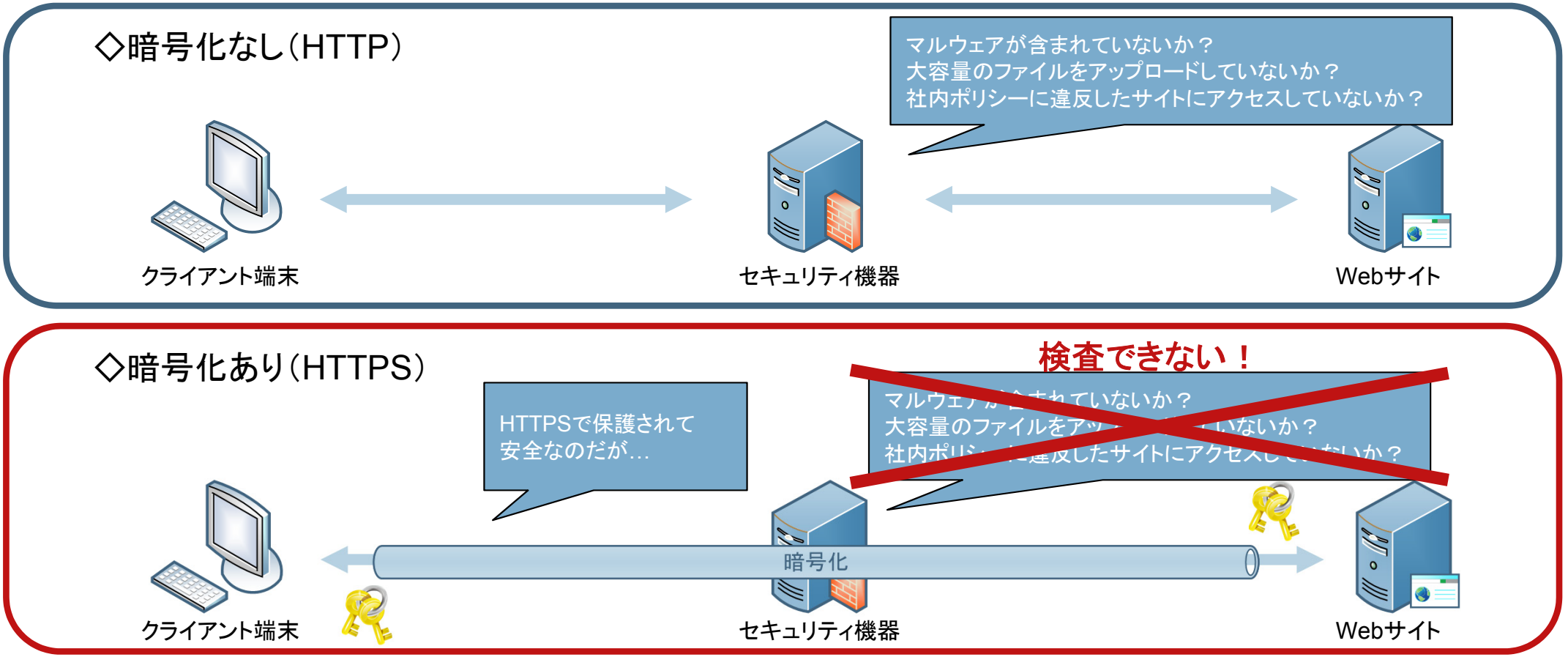


調査対象企業数 20社

企業の実態

HTTPS化がもたらすデメリット（1）
暗号化によるセキュリティ強化と引き替えに、通信経路でのセキュリティ対策が行えない

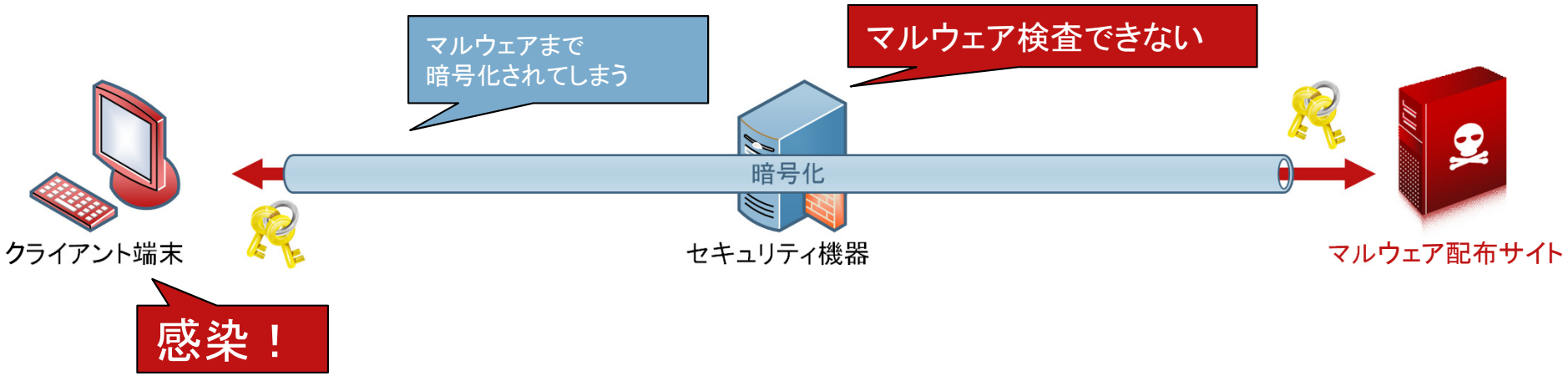
- HTTPSによって暗号化された通信は、通信経路上で内容の確認・変更を行うことができない
- プライバシーの保護や第三者による攻撃を防ぐという面では暗号化を行うことが望ましいが、従来行われてきた通信経路上のセキュリティ対策を行うことができなくなってしまう



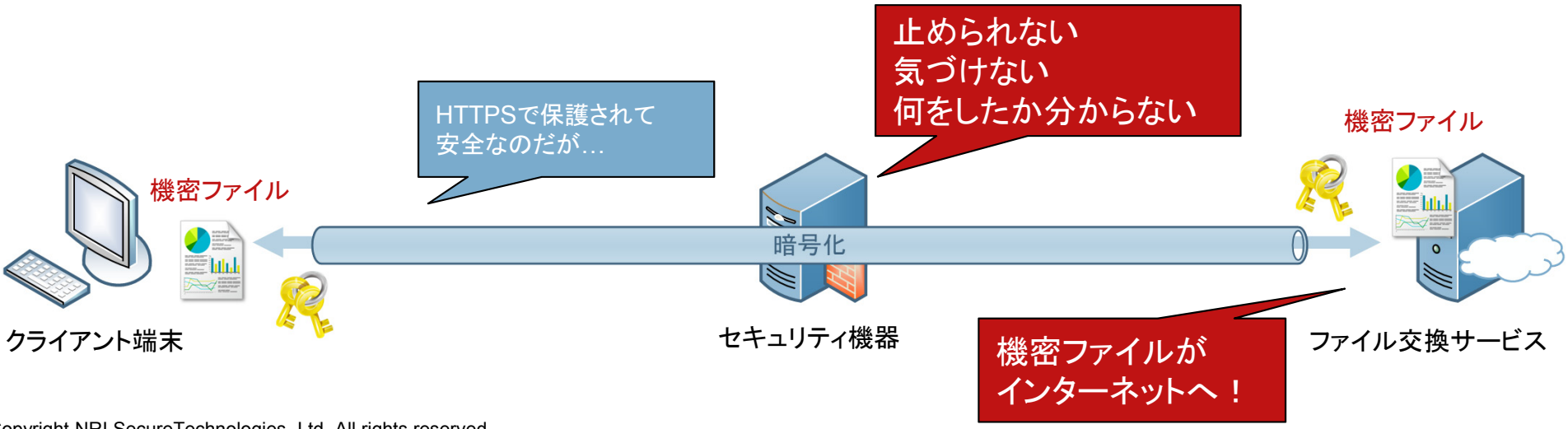
企業の実態

HTTPS化がもたらすデメリット(2)
通信経路上で実現できなくなるセキュリティ対策の例

■ 悪意のあるWebサイトがHTTPSを利用していたら…



■ ファイル交換サービスがHTTPSを利用していたら…



企業の実態

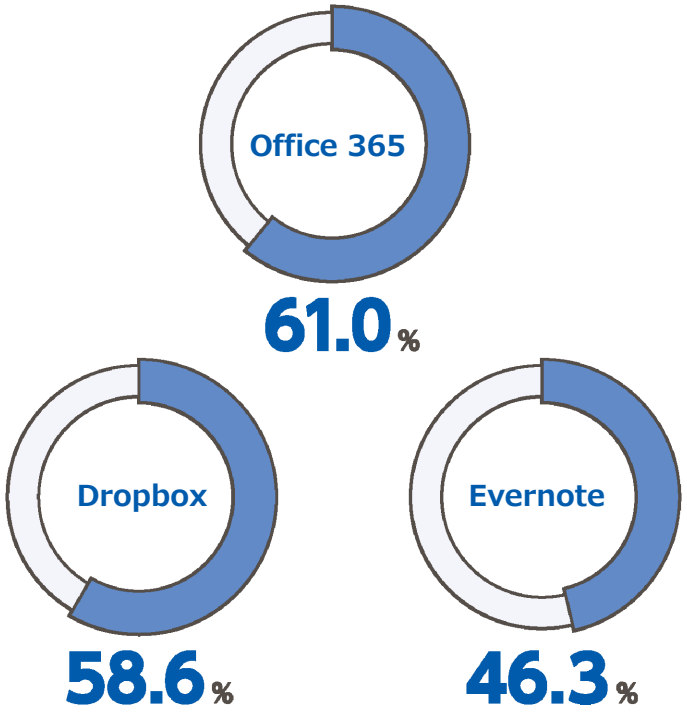
クラウドサービスの利用は企業の管理部門が把握しているよりもずっと多い Shadow ITの問題は、今後大きくなっていく

- Office 365、Dropbox、Evernoteといったクラウド（SaaS[*1]）サービスの普及が進んでいる
- 上記SaaSサービスへのアクセスは、管理部門が把握しているものよりも明らかに多い
  - 企業向けアンケート調査[*2]によれば、「SaaSサービスを利用している」と回答した企業は40.4%
  - 今回の分析結果では、上記3つサービスともに、単体で40.4%を上回っている

- Shadow IT問題
  - 事業部門や従業員が管理部門の認可・承認なしでクラウドサービスを利用し、情報流出のリスクにつながってしまうという問題
    - 事業部門が自社で定められた承認を受けずにサービスを契約
    - 他社契約下のサービスを利用
    - 従業員が個人的にサービスを契約・利用

- 大手クラウドサービス事業者は積極的に常時SSL化を推進しており、通信経路上での制御が難しいことも
  - たとえば、自社契約下のサービスのみ利用を認めるというような制御が難しい

■ 2017年3月に各サービスへ通信量1MB以上の通信が1回以上観測された企業の割合



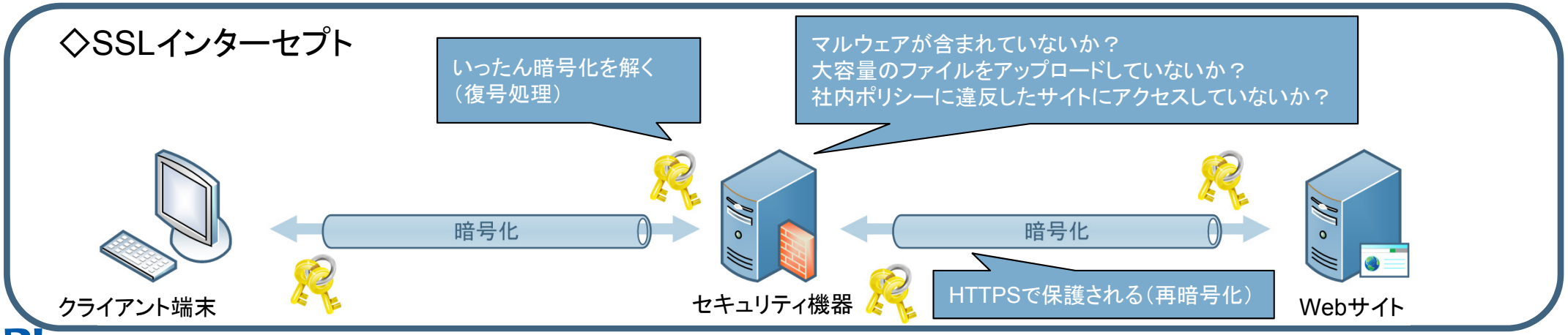
調査対象企業数　41社

*1: Software as a Serviceの略。インターネット上でソフトウェアを必要な分だけ利用できるようにするクラウドサービスの形態。
*2: NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査　2017」より。

推奨対策

HTTPS・クラウド時代への対応は必須
自社のニーズに合ったセキュリティ対策の選択を

- SSLインターセプト
  - HTTPS通信をいったんセキュリティ機器で復号し、再度暗号化を行ってWebサーバと通信する
  - HTTPS通信であっても、HTTPと同様の検査を行うことが可能
  - 実施の上で課題があるため、十分な検討の上での導入を推奨
- CASB（Cloud Access Security Broker）
  - クラウド利用の可視化・制御・セキュリティ保護を行うサービス
- クライアントの機能強化
  - 従来通信経路上で実施していたセキュリティ機能をクライアント上のソフトウェアで実施する
  - 暗号化の有無に関係なくセキュリティ機能の適用が可能
  - 全端末に対してソフトウェアのインストール・管理が必要



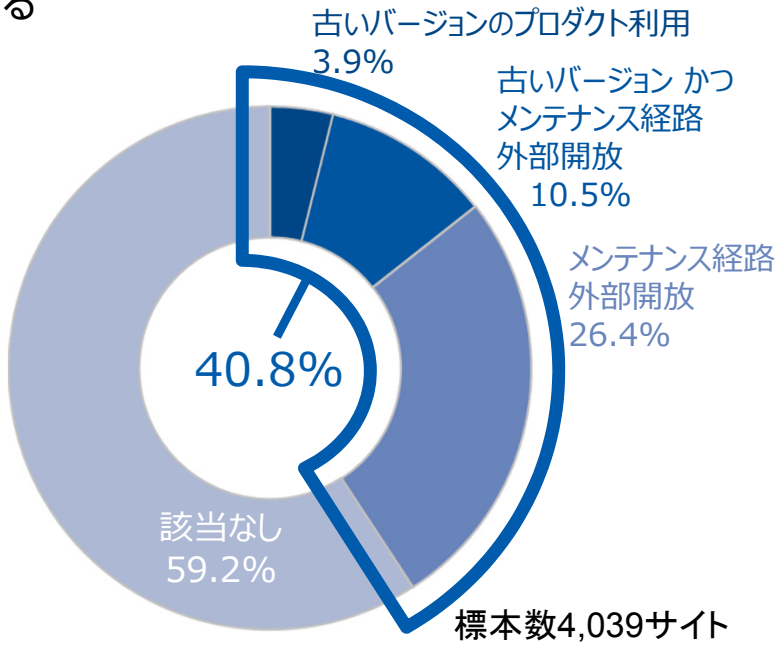
目次

2-3. 4割の企業Webサイトは容易に攻撃可能

4割の企業Webサイトは容易に攻撃可能
この傾向はCMSの利用増により加速

- 「Webサイト群棚卸しサービス」によって、管理部門が把握しきれていないWebサイトが発見される
  - 事業部門や海外現地法人などが独自に構築したサイトなど
- 発見したWebサイトすべて（企業が元々把握していたものを含む）を対象として調べた結果、外部から容易に攻撃可能となる下記の2つの問題について、少なくとも片方が露呈していたケースは全体の40.8%
  - 古いバージョンのプロダクト利用: 14.4%
    - 古いバージョンの利用は、既知の脆弱性を放置していることを意味する
    - 古いバージョンを利用し、かつファイアウォール・WAF[*1]などによって代替的な対策を行わない場合、容易に攻撃可能
  - メンテナンス経路の外部開放: 36.9%
    - メンテナンス用のサービス（telnet・SSH・FTP・Webコンソールなど）に対して、外部からアクセス可能
    - ID/パスワードのみで制御されている（二要素認証などの高度な方式が利用されていない）
    - 特にデフォルトID/パスワードがそのまま利用されている場合非常に危険
- CMS[*2]の利用増によりこの傾向は加速される傾向にある

■容易に攻撃可能な問題が検出されたサイトの割合



標本数4,039サイト

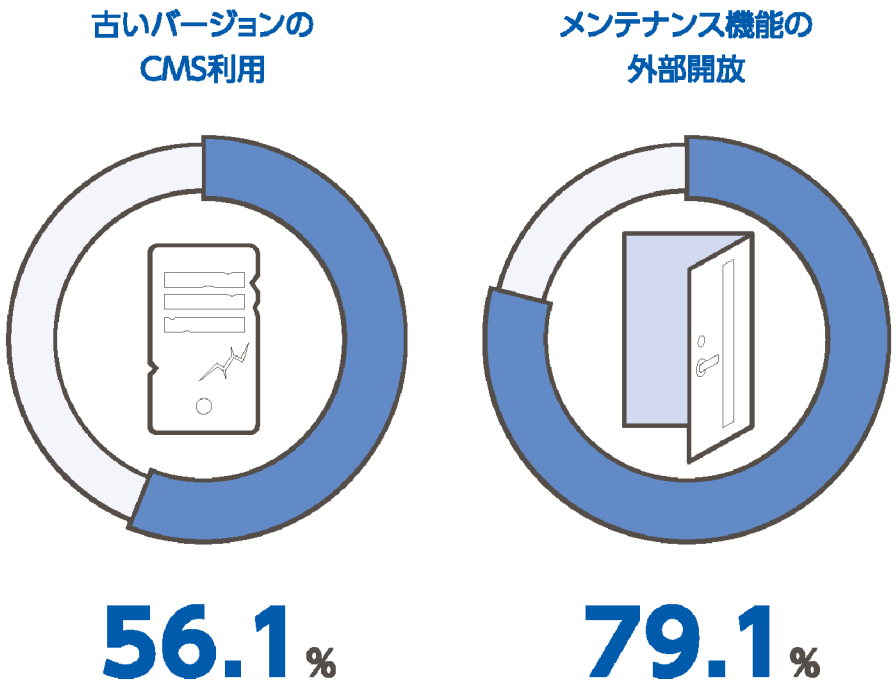
*1: Web Application Firewall の略。アプリケーションに対する攻撃を防御する為のソリューション。
*2: Content Management System の略。Webサイトを管理・構築するためのシステムで、専門的な知識をそれほど必要とせずにWebサイトの運営が可能。

2-3. 4割の企業Webサイトは容易に攻撃可能

CMS利用サイトの大半は堅牢化が行われていない
簡単にWebサイトを作れることが、安易なサイトリリースに繋がっている

- CMS利用サイトについては、前述の「容易に攻撃可能」な状態になっている割合が非常に高い
- 低コストで見栄えの良いWebサイトが構築できるため、Webサイト全体への予算も小さく、セキュリティ対策に十分なリソースが割かれないことも多いと推測される
- 多くのCMSは既定設定が十分に堅牢ではない上、堅牢化のためのノウハウが公式マニュアルでは十分に提供されていないことも多い

■CMS利用サイトにおいて、容易に攻撃可能な問題が検出されたサイトの割合



標本数173サイト

推奨対策

自社Webサイトの現状を把握し
一元管理によるセキュリティ水準の底上げを

- まずは現状を把握する
  - Webサイトの存在を把握できていなければ、脆弱性が存在していても対処のしようがない
  - 自社に関連するWebサイトを探索するソリューションを「支援策」として活用することも一つの選択肢
    - 発見したWebサイトをひとつひとつ地道に評価し、対策を検討していくことが結局は近道

- Webサイトを把握し、一元管理するための王道は、管轄部門を定めてWebサイトの構築・運用に関わるルールを設定し、PDCAサイクルを回していくこと
  - CMSサイトについても共通ルールを設定し、運用することで確実に堅牢化を実施

- 利用中のプロダクトにおける脆弱性情報を収集し、該当するWebサイトについては適切な対応を実施する
  - プロダクトのバージョンを最新化する
  - WAFなどによって代替的な対策を行う

目次

2-4. 猛威を振るうマルウェアメール

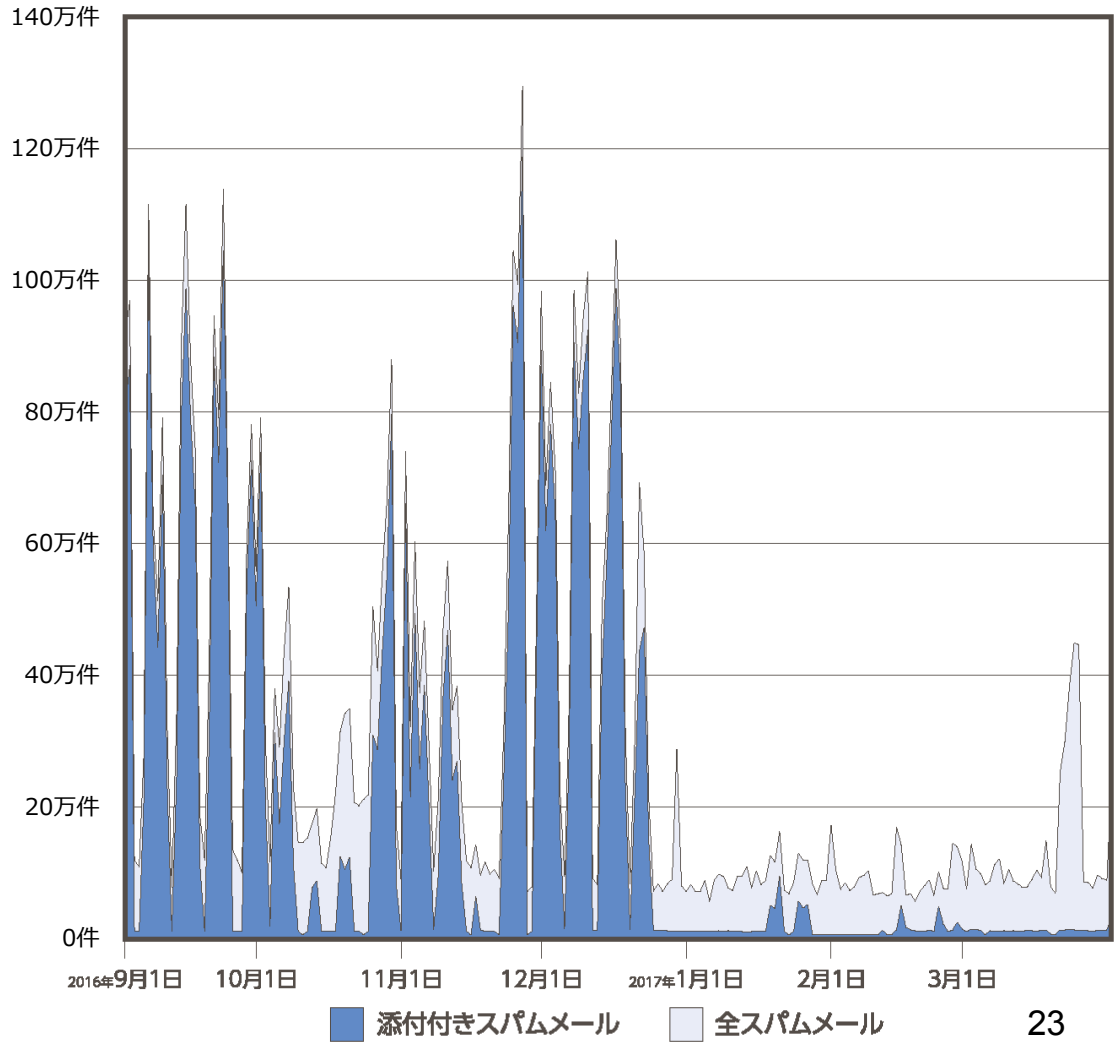
バラマキ型メールが猛威を振るう
2016年度後半にいったん落ち着いたが、再び激化の兆しあり

- 2016年度初頭から12月頃まで、大量のバラマキ型マルウェアメールを毎日のように検出

- バラマキ型マルウェアメールとは
  - マルウェアが添付されたスパムメール
    - ランサムウェア拡散にも利用される
  - 一度に大量の組織・アドレスに向かって配信される
    - 配信の都度マルウェアに変更が加えられるため、ウイルス検査をすり抜けてしまうことが多い
  - いわゆる標的型攻撃ではない
    - 本文の内容から、特定の業種を想定ターゲットとしていると考えられるものはある
  - 高度な攻撃ではないが、標的が多数に及ぶため全従業員に対して、不審なメールを開かないように教育することが有効

- 2016年末にいったん激減
  - 配布に使われていたボットネットの停止による
  - 2017年度に入って、激化の兆し

■スパムメール検出数推移



メール訓練における、危険メールの開封率は1桁台へ 継続的な実施により、低開封率の維持を図るべき

- 標的型メール訓練におけるメール開封率は低下を続けている
  - 2016年度のメール開封率は9.2%
  - ユーザーの不審メールへの関心が高まっている
  - 繰り返し訓練を実施することにより教育の結果が出ている
- 当社の経験上、メール訓練の継続実施により開封率は低下するものの、最終的には5%程度以下には下がらない

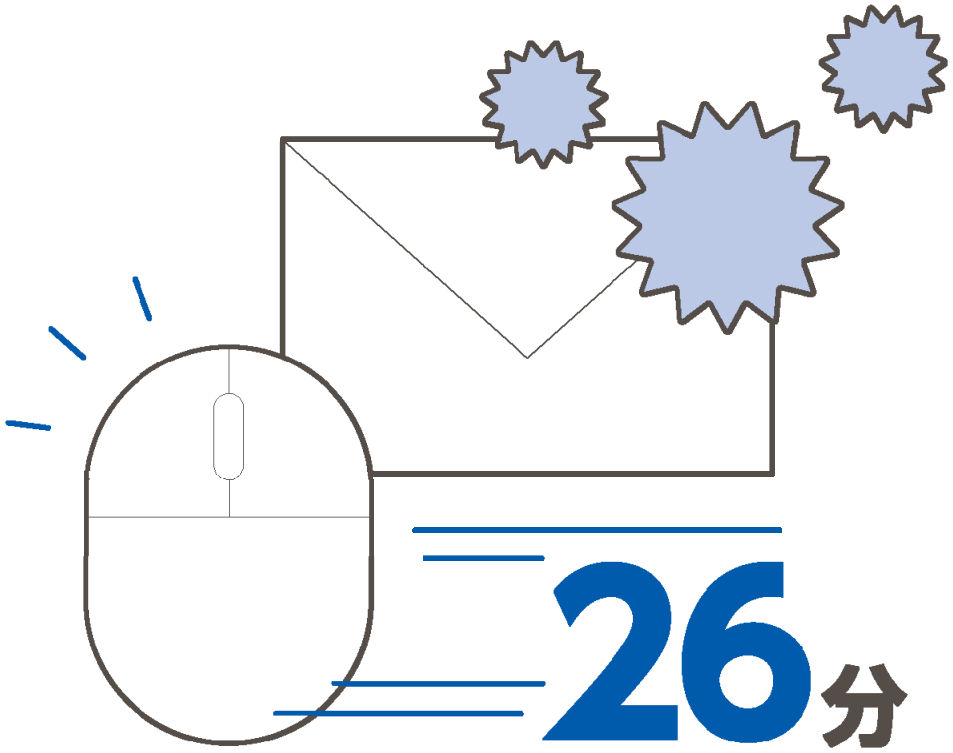
■メール訓練における添付ファイル実行・URLへのアクセス率

集計期間	アクセス率
2012年 (2012年4月～2013年3月) 標本数：164,974人	22.5%
2013年 (2013年4月～2014年3月) 標本数：101,326人	15.6%
2014年 (2014年4月～2015年3月) 標本数：190,730人	15.3%
2015年 (2015年4月～2016年3月) 標本数：565,115人	12.8%
2016年 (2016年4月～2017年3月) 標本数：837,703人	**9.2%**

企業の実態

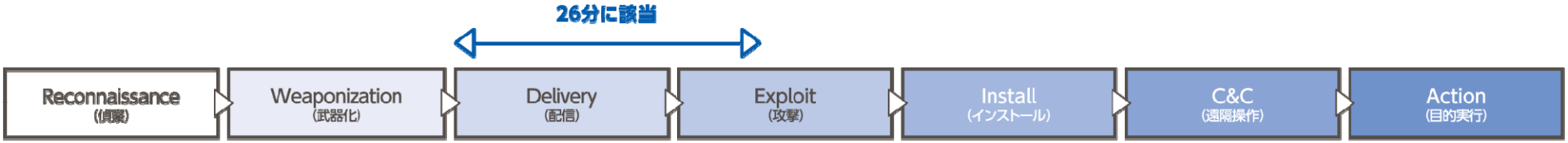
攻撃メールの着信から、添付ファイルの開封もしくはURLリンクのクリックまで平均26分 開封前に対策を行うことが理想的

- 訓練メールの配信開始から
  最初の開封者が出るまでの平均時間は約26分
- 「26分間のうちに最初の対策を取ること」を
  一つの目安値として考えることができる
- 開封者が出ないうちに対策を行うことで
  被害を発生させない（理想的な対応）



標本数460配信

■サイバーキルチェーン(サイバー攻撃者の行動パターン)のモデル



推奨対策

標的型メール攻撃やバラマキ型マルウェアメールから企業を守るためには システム的・人的な多層防御が重要

システム的対策

- システムレベルの防御力の強化
  - 新型ソリューションの導入（振舞検知*1、EDR*2……）
  - 既存セキュリティ製品・設定の見直し
    - ファイルタイプ（拡張子）規制によって遮断できるマルウェアメールも多数ある

人・組織的対策

- 訓練の継続的な実施
  - 継続的な訓練により、教育の効果が上昇
- 従業員をセキュリティリソースに変える
  - 「不審なメールを受信したり、開封してしまったときにはすぐに報告」を習慣づける
  - 従業員からの報告をうまく扱えるような仕組みを作ることで、より効率的なハンドリングも検討できる

*1: ファイル実行時の動作を解析し、マルウェアであるかどうかを判断するソリューション。
*2: Endpoint Detection and Response の略。エンドポイント（端末）の情報を分析し、不正な挙動の検知や感染発覚後の対策を迅速に行うためのソリューション。

目次

ご参考

分析対象としたNRIセキュアテクノロジーズのサービス

◆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

メールゲートウェイ、プロキシサーバ、リモートアクセスなど、お客様の社内ネットワークとインターネットを安全に接続するために必要となるセキュリティ対策のアウトソーシングサービスです。本レポートではFNCセキュアインターネット接続サービスで管理しているゲートウェイサーバのうち、URLフィルタ20システム分、スパムフィルタリングサーバ26システム分、次世代ファイアウォール41システム分のログを集計対象としています。

○FNCセキュアWebネット管理サービス

お客様のWebサイトを、外部からの不正アクセスの脅威から守るセキュリティ対策のアウトソーシングサービスです。ファイアウォール（FW）や侵入検知システム（IDS）の他、侵入防御システム（IPS）やWebアプリケーションファイアウォール（WAF）等のセキュリティデバイスを24時間365日監視しています。本レポートではFNCセキュアWebネット管理サービスで管理しているセキュリティデバイスのうち、ファイアウォール96システム分、WAF 37システム分のログを集計対象としています。

○セキュリティログ監視サービス

お客様環境より収集した各種プロダクトのイベントログをSIEMに取り込み、リアルタイムに監視、分析するサービスです。本レポートでは2016年4月～2017年3月にセキュリティログ監視サービスにおいて、セキュリティインシデントに繋がるような攻撃かどうかを分析する必要があった918イベントを集計対象としています。

◆セキュリティ診断サービス

○プラットフォーム診断

ネットワークの外側（インターネット）あるいは内側のLANから、サーバやネットワーク機器等のシステム基盤のセキュリティホールや設定状況について検査を行い、発見された問題に対して当社独自の基準により危険性を評価して報告するサービスです。本レポートでは2016年4月～2017年3月に、インターネット経由で診断した92システム分を集計対象としています。

○Webアプリケーション診断

Webアプリケーションの実装方式、開発言語、利用プラットフォームなどを考慮し、Webアプリケーションに潜在するセキュリティ上の問題点を洗い出し、発見された問題に対して当社独自の基準により危険性を評価して報告するサービスです。本レポートでは2016年4月～2017年3月に診断を実施した451システム分を集計対象としています。

○スマートフォン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の実装方式、開発言語、利用プラットフォームなどを考慮し、スマートフォンアプリケーションに潜在するセキュリティ上の問題点を洗い出し、発見された問題に対して当社独自の基準により危険性を評価して報告するサービスです。本レポートでは2016年4月～2017年3月に手動にて診断を実施した52アプリケーション（342指摘事項）を集計対象としています。

○Webサイト群探索棚卸サービス（GR360）

独自アルゴリズムにより、インターネットに公開されている特定企業関連のWebサイトを探索し、発見されたWebサイトに対して簡易なセキュリティチェックを行って、Webサイト群全体に対するセキュリティレベルの可視化を行うサービスです。本レポートでは2016年4月～2017年3月に簡易なセキュリティチェックを実施した4,039サイトを集計対象としています。

○標的型メール攻撃シミュレーション

疑似攻撃ファイルを添付、あるいは疑似攻撃サイトへのURLリンクを記載した標的型メールを送付し、対象者へ標的型メール攻撃に対する意識付けを行うと共に、対象者のファイル実行、あるいはリンクのクリック状況を確認することで、標的型メール攻撃へ耐性をチェックして報告するサービスです。本レポートでは2016年4月～2017年3月に送信した837,703通を集計対象としています。

○プラットフォーム診断エクスプレスサービス

診断ツールを用いてインターネット経由でサーバやネットワーク機器等のシステム基盤のセキュリティホールや設定状況について検査を行い、発見された問題を報告するサービスです。本レポートでは2016年4月～2017年3月に、インターネット経由で診断した1,090 IPアドレス分を集計対象としています。

NRIセキュアテクノロジーズ

NRI SecureTechnologies