NRI SECURE

Cyber Security Trend

Annual Review

2018

Cyber Security Trend Annual Review 2018

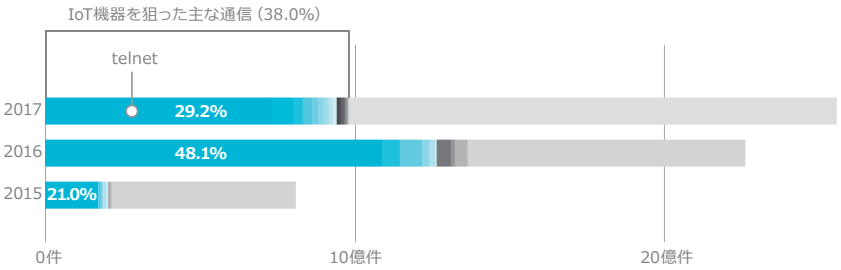
サイバーセキュリティ傾向分析レポート 2018

目次

エグゼクティブサマリ

攻撃対象が分散
全体の約4割がIoT機器宛の通信

■ファイアウォールでブロックした通信の件数



標本数 2,571,251,045件（2017年）
2,262,695,083件（2016年）
808,955,599件（2015年）

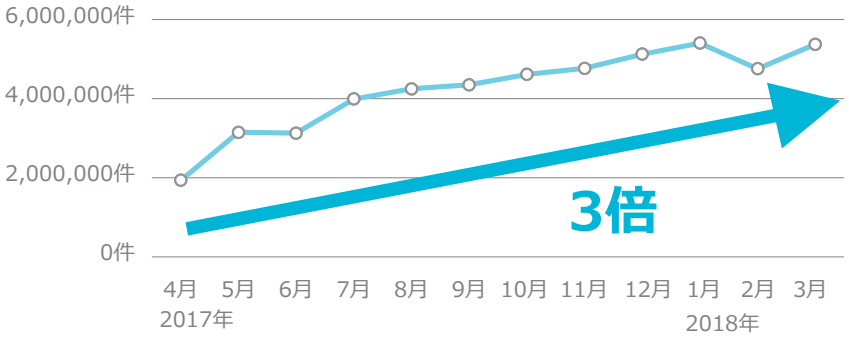
2017年4月～2018年3月にかけてFNCサービスにおけるファイアウォールでブロックした通信を分析したところ、IoT機器に対する探索行為の対象ポートが分散していることが分かりました。

telnetポートへのアクセスが2016年には大幅に増加していましたが、2017年は減少しています。一方上位100件にはtelnetポート以外にもIoT機器を狙った通信が複数あり、それらのポートを合わせると全体の約4割を占めています。

今後もIoT機器を狙った攻撃は増加していくと考えられます。IoT機器はインターネットに接続してすぐに利用できるように初期設定がなされている場合が多いことから、管理が疎かになりやすい側面があります。設置時および運用時の適切な設定管理が望まれます。

WannaCryから学ぶ、
自社での脆弱性管理の重要性

■ファイアウォールでブロックした通信（SMB宛）の件数



標本数 2,571,251,045件

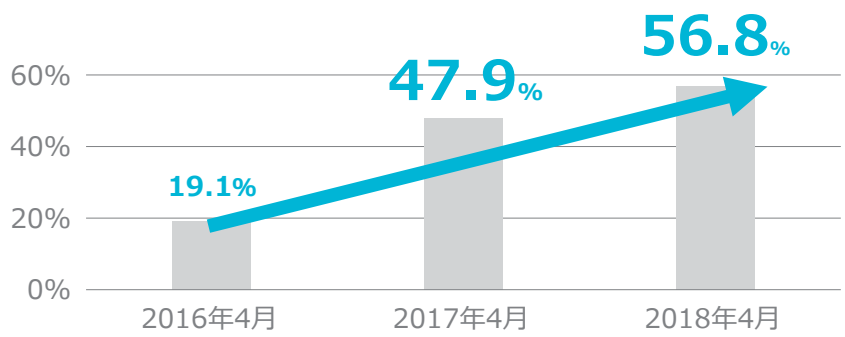
FNCサービスのファイアウォールでブロックした通信を分析したところ、ランサムウェアの一種であるWannaCryおよびその亜種（以降、これらをまとめてWannaCryと呼びます）による感染活動が2017年5月頃から増加し、2018年3月には2017年4月の3倍近くにもなりました。

WannaCryはWindows端末間でファイルを共有するためなどに利用するSMBの脆弱性を悪用しますが、多くの企業ではファイアウォールでインターネット側からのアクセスをブロックしていることなどから、企業内の端末の感染までには多少のハードルがあると考えられます。また、端末のパーソナルFWの設定によっては、企業内での感染拡大を防ぐことができると考えられます。

WannaCryへの主要な対策はパッチ適用であり、WannaCryに限らず恒常的なパッチ適用が重要であることは言うまでもありませんが、端末の利用状況によっては、本件への対応の緊急性は異なっていたと言えます。世間を騒がせる攻撃の手法や経路を理解し、自組織の環境に照らした時の影響有無や緊急性を判断することも、重要な活動であります。

"常時SSL化"における セキュリティ対策

■Webアクセスにおける HTTPS通信の割合



標本対象企業数　20社　20社　23社

FNCセキュアインターネット接続サービスで全Webアクセスに占めるHTTPS通信の割合を確認したところ、年々増加傾向にあり、2018年4月には56.8%に達しました。

HTTPSは通信の盗聴防止のみでなく、不正なサーバへの接続を防ぐ等のメリットがあるため、機密情報の有無にかかわらず、Webサイトの全通信を暗号化してHTTPSで通信（いわゆる“常時SSL化”）するサイトが増加しています。しかし、HTTPSによって暗号化された通信は通信経路上のセキュリティ対策では通信内容の一部しか検査を行うことができないため、マルウェア感染や情報漏えい等のリスクが高まる可能性があります。

そこで、通信経路上のセキュリティ機器でHTTPS通信を一度復号して内容を検査することや、通信経路上のセキュリティ機器で実装していたセキュリティ機能をクライアント端末上で実装し、暗号化の有無に関わらずセキュリティ機能を適用することが考えられます。

上記どちらの対応を行う場合でも導入後の運用まで考えた上でセキュリティ対策を整備していく必要があります。自社で導入済みのセキュリティ対策や構成を踏まえて、対応をご検討ください。

進まぬ Windows 10移行

■当社クリプト便サービスユーザの利用Windows OS種別割合

	Windows 7	Windows 10	Windows Vista	Windows XP
2018年3月	82.5%	10.6%	0.2%	0.5%
2017年4月	89.5%	4.1%	0.2%	1.1%

標本対象ユーザ数 352,980人(2018年3月延べ人数)
299,078人(2017年4月延べ人数)

当社クリプト便サービスユーザの利用 OS 種別を調査 *1 したところ、2018 年 3 月時点で Windows 7 を利用しているユーザが 80% を超えていたことが分かりました。2017 年 4 月～ 2018 年 3 月の1年間で、多少 Windows 10 の利用割合は増えましたが、依然として企業においては Windows 7 の利用が多くを占めており、移行は進んでいません。

Windows 10 は Windows 7 と比べてセキュリティ機能が大幅に強化されています。例えば、Windows Defender や Windows Firewall などの機能が Windows Defender セキュリティセンターとして統合され、Windows 7 では提供されていなかった機能が追加されました。

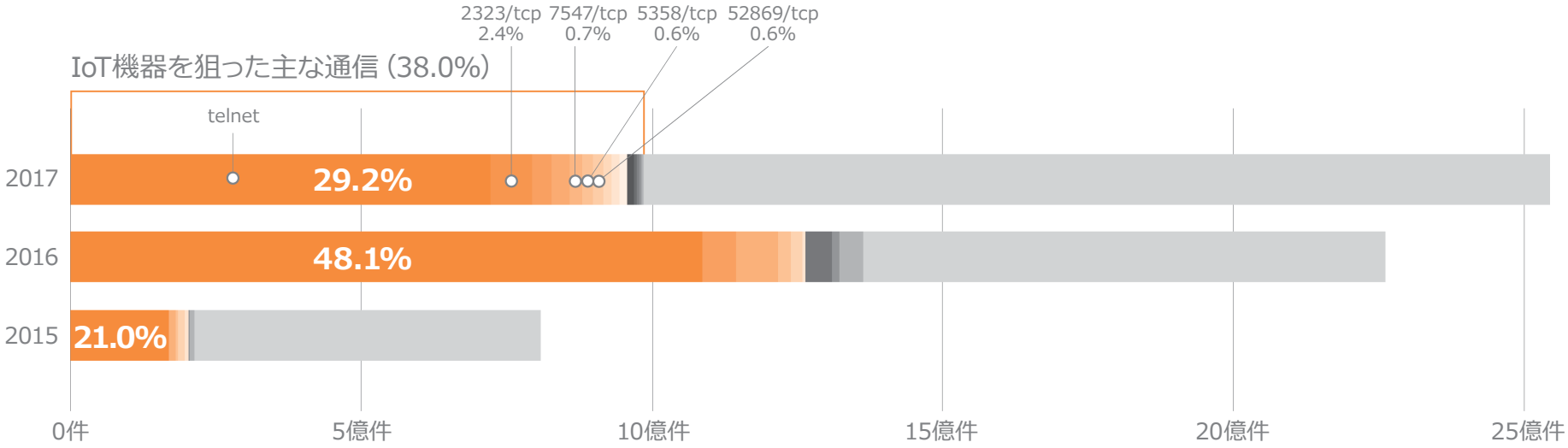
移行が進まない背景には、移行に必要な人的リソースやコスト不足が影響していると考えられますが、上記のとおり Windows 10 ではセキュリティ機能が大幅に強化されており、移行することにより大きなメリットがあります。Windows 7 のサポート終了日が迫っていることを踏まえ、早期に移行が進むことが望まれます。

*1　クリプト便利用ユーザの User-Agent ヘッダを基に集計しています。

ITサービスの提供者への脅威

攻撃対象が分散
全体の約4割がIoT機器宛の通信

■ファイアウォールでブロックした通信の件数



2017年4月～2018年3月にかけて、FNCサービスのファイアウォールでブロックした通信を分析したところ、telnetで利用される23/tcp宛の通信の割合は29.2%でした[*1]。IoT機器の増加に伴いIoT機器を探索する通信が増えたことで、2016年まではtelnet(23/tcp)宛の通信が急激な増加傾向にありましたが、今回の調査では減少に転じています。

ブロックされた通信の内訳を見てみると、同種の探索行為の対象ポートが分散していることが分かります。IoT機器を標的としたと考えられる23/tcp 宛以外のポート宛の通信も複数確認でき、上位100件に含まれるポートのうちIoT機器を狙ったポートを合わせると全体の38.0%を占めています。例として5358/tcp、7547/tcp、2323/tcp、52869/tcp宛の通信を挙げることができますが、これらのポートはIoT機器の管理コンソールや、ルータやプリンタの相互接続のために利用されるもので、いずれも脆弱性が存在する特定のIoT機器を標的としたものです[*2 *3]。

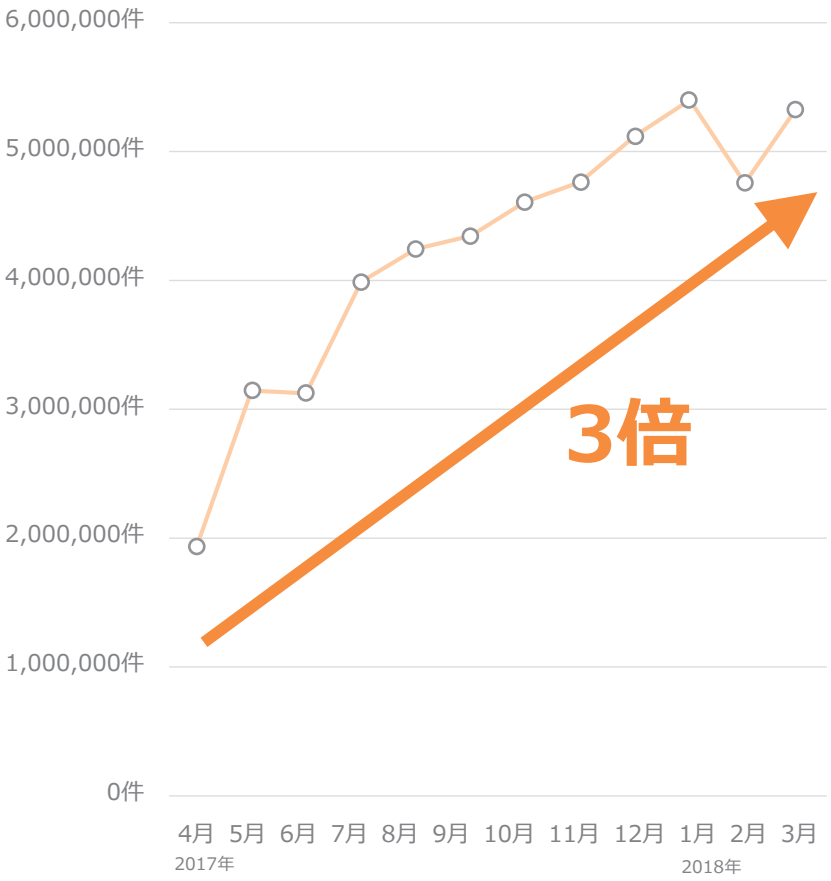
今後もIoT機器を狙った攻撃は増加していくと考えられます。IoT機器はインターネットに接続してすぐに利用できるように初期設定されている場合も多いことから、管理が疎かになりやすい側面があります。設置時および運用時の適切な設定管理が望まれます。

*1 当社のマネージドセキュリティサービス(MSS)で提供しているインターネット境界のファイアウォールにおいて、インターネットから内部へ流入する通信に絞って集計しています。ただし一部通信については当社の上位キャリアにてフィルタしているケースがあり、それらは集計に反映していません。
*2 平成29年観測資料, 警察庁, 2018
https://www.npa.go.jp/cyberpolice/detect/pdf/20180322_toukei.pdf
*3 脆弱性が存在するルータを標的とした宛先ポート 52869/TCP に対するアクセス及び日本国内からのTelnet による探索を実施するアクセスの観測等について, 警察庁, 2018
https://www.npa.go.jp/cyberpolice/detect/pdf/201712191.pdf

標本数　808,955,599件（2015年）
2,262,695,083件（2016年）
2,571,251,045件（2017年）

WannaCryから学ぶ、自社での脆弱性管理の重要性

■ファイアウォールでブロックした通信（445/tcp宛）の件数



2017 年 4 月～ 2018 年 3 月にかけて、FNC サービスのファイアウォールでブロックした通信を分析したところ、2017 年 5 月以降に 445/tcp 宛の通信が急上昇していました。これはランサムウェアの一種である WannaCry およびその亜種（以降、これらをまとめて WannaCry と呼びます）による感染活動と考えられます[*1]。445/tcp は Windows 端末間でファイルを共有するための SMB 通信等で利用されますが、WannaCry では感染拡大のために SMB の脆弱性を悪用します。この脆弱性を悪用する攻撃ツールが広く活用されたことで、世界中で大規模な感染に至ったと考えられます。当社でも感染活動と考えられる多くの通信を観測しましたが、攻撃経路を踏まえると、企業内の端末の感染までには多少のハードルがあります。

445/tcp は特別な事情がない限り、インターネットに公開する必要がないポートなので、多くの企業ではファイアウォールでブロックしています。また、仮に企業内の LAN 上に WannaCry 感染端末が存在したとしても、端末のパーソナル FW の設定によっては、感染拡大を防ぐことができたと考えられます。

WannaCry への主要な対策はパッチ適用であり、WannaCry に限らず恒常的なパッチ適用が重要であることは言うまでもありませんが、端末の利用状況によっては、本件への対応の緊急性は異なっていたと言えます。世間を騒がせる攻撃の手法や経路を理解し、自組織の環境に照らした時の影響有無や緊急性を判断することも、重要な活動であると言えます。

*1 ランサムウェア「WannaCry」の亜種に感染したPCからの感染活動とみられる445/TCPポート宛てアクセスの観測について, 警察庁, 2017
https://www.npa.go.jp/cyberpolice/detect/pdf/20170622.pdf

標本数 2,571,251,045件

仮想通貨の採掘を行う通信が急増

■CVE-2017-10271の脆弱性を狙った攻撃検知件数

2017年10月に、Oracle WebLogic Serverのサブコンポーネントであるwls Securityにおいて、リモートから任意のコードを実行可能な脆弱性の存在が公開されました*1。当社では遅くとも12月24日には攻撃コードが公開されていたことを確認しています。

過去の様々な脆弱性でも見受けられるように、攻撃コード公開以降は当該脆弱性を悪用しようとする攻撃が急増したことを観測しています。自社サーバを悪用されないためにも、基本的には脆弱性に対して迅速かつ適切な対応を行える仕組みや体制作りが必要となります。

また、本脆弱性には悪用のされ方に特徴的な点がありました。本脆弱性を悪用することで、攻撃者は遠隔から公開Webサーバの情報を改ざん可能であり、当社で観測した実際の攻撃通信では、公開Webサーバに仮想通貨を採掘するプログラム(マイニングツール)をダウンロードさせようとする攻撃を確認しました。このことは2017年9月にCoinHive*2が登場したことが関係しており、仮想通貨を採掘させた結果を利用して、攻撃者が収益を得ようとしていたと考えられます。

なお、本脆弱性は過去の様々な脆弱性と比較して、公開Webサーバに仮想通貨を採掘させるのに特別有用であったということではなく、単に仮想通貨の採掘が世の中に普及したタイミングで発見された深刻度が高い脆弱性であったと考えられます。

*1　CVE-2017-10271 https://www.ipa.go.jp/security/ciadr/vul/20180115_WebLogicServer.html
*2　Webサイト管理者が、Webサイトを閲覧したユーザ端末のリソースを利用して仮想通貨を採掘させて、その結果を基に収益を得るサービス。

標本対象企業数 48サイト

■仮想通貨を採掘させられる可能性があるURLへのアクセス件数

またFNCセキュアインターネット接続サービスにおいて2017年4月～2018年3月までのアクセス先URLを調査したところ、CoinHiveが登場した2017年9月以降、同様の目的を意図したサービス利用を示唆する通信が劇的に増加しました。

マイニングツールは、マルウェアに混入されたり、前頁のCVE-2017-10271(Oracle WebLogic Serverの脆弱性)におけるCoinHiveの利用のように、Webサイトを改竄してマイニングツール(スクリプト)を設置されたりするような例のほか、Webサイト管理者自身の意思でWebサイトの利用者に仮想通貨を採掘させるためのプログラムを設置する場合もあります。後者であれば、必ずしもWebサーバの特定の脆弱性を悪用したり、ユーザの端末をマルウェア感染させたりする必要はありません。JavaScriptを用いた採掘プログラムを設置すれば、多くのブラウザはデフォルトでJavaScriptが有効であることから、特に閲覧者の同意や特別な手順を要求することなく、仮想通貨を採掘させることが可能です。採掘させようとする立場としては、比較的容易に利益を上げる手段となり得ます[*1]。

仮想通貨の盛り上がりを反映するように、CoinHiveで利用されるようなマイニングツールは急激に流行しました。マイニングツールは実行させられても必ずしも目に見える被害を受けることがないという点でランサムウェア等とは異なりますが、次に流行する手段が同様に被害の小さいものであるとは限らず、今後の動向を注視していきたいと考えています。

*1 警察庁によって、閲覧者に明示せずにWebサイトにマイニングツールを設置することは、犯罪になる可能性があると指摘されています。仮想通貨を採掘するツール(マイニングツール)に関する注意喚起, 警察庁, 2018
http://www.npa.go.jp/cyber/policy/180614_2.html

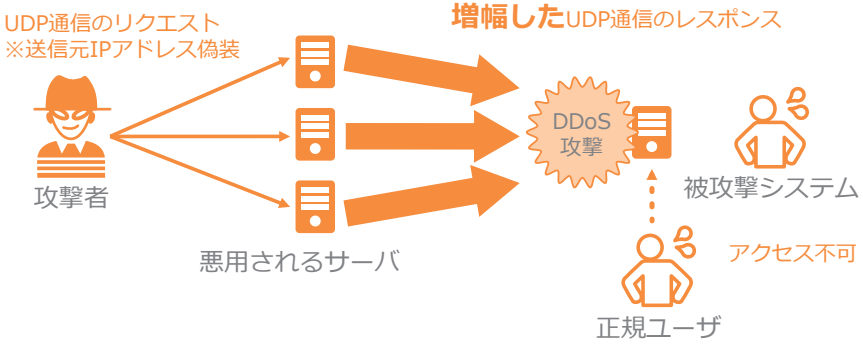
標本対象企業数 46サイト

DDoS攻撃に悪用されないためにできること

■ファイアウォールでブロックした通信（UDP増幅攻撃に利用可能なUDPサービス）の件数

順位	サービス	ポート	増幅率 *3 理論値	件数
1	DNS	53/UDP	28.0–54.0	100,405,804
2	SSDP	1900/UDP	30.8	28,911,633
3	SNMP	161/UDP	6.3	7,050,803
4	NTP	123/UDP	556.9	4,311,203
5	LDAP	389/UDP	46.0–55.0	3,802,301
・・・				
10	Memcached	11211/UDP	10,000.0–51,000.0	953,765

■UDP増幅攻撃の概要



2018年2月末にGitHub*1に対するDDoS攻撃が発生しました。攻撃発生時、GitHubの迅速な対応により被害は最小限に抑えられ、断続的なサービス停止があったのみでした。

この攻撃は、memcachedと呼ばれる分散型メモリキャッシュサーバに対するUDP増幅攻撃が原因とされ、攻撃発生時は1.35Tbpsのトラフィックが押し寄せたと言われています。memchached1.2.7～1.5.5を初期設定のまま使用して、11211/udpがサービス可動している場合、特定のリクエストに対して10,000倍以上のレスポンスサイズの応答を返すため、UDP増幅攻撃に使われやすく、攻撃者は低いコストで大きなトラフィックを発生させることが可能です。

FNCサービスではmemcachedによるDDoS攻撃の大きな被害は発生していませんが、2017年4月～2018年3月にかけてファイアウォールでブロックした通信を集計したところ、攻撃に使用可能な機器を探索していると考えられる11211/udp宛の通信が2018年2月以降急増したことを確認しています*2。

また左表のとおり、UDP増幅攻撃に利用可能なUDPサービスに対する通信はmemcached以外にも観測されています。自社の機器がUDP増幅攻撃に悪用されないためには、公開する機器とポートを限定したり、接続可能な機器を限定したりといった適切なアクセスコントロールを設計することが最も重要です。

特にDNSやNTPなど公開が必要なホストについては注意が必要です。DNSはキャッシュサーバとコンテンツサーバの分離や公開サーバの再帰問い合わせの無効化などが必要であり、NTPはmonlistと呼ばれるNTPサーバの状態を確認する機能を無効化することが必要です。

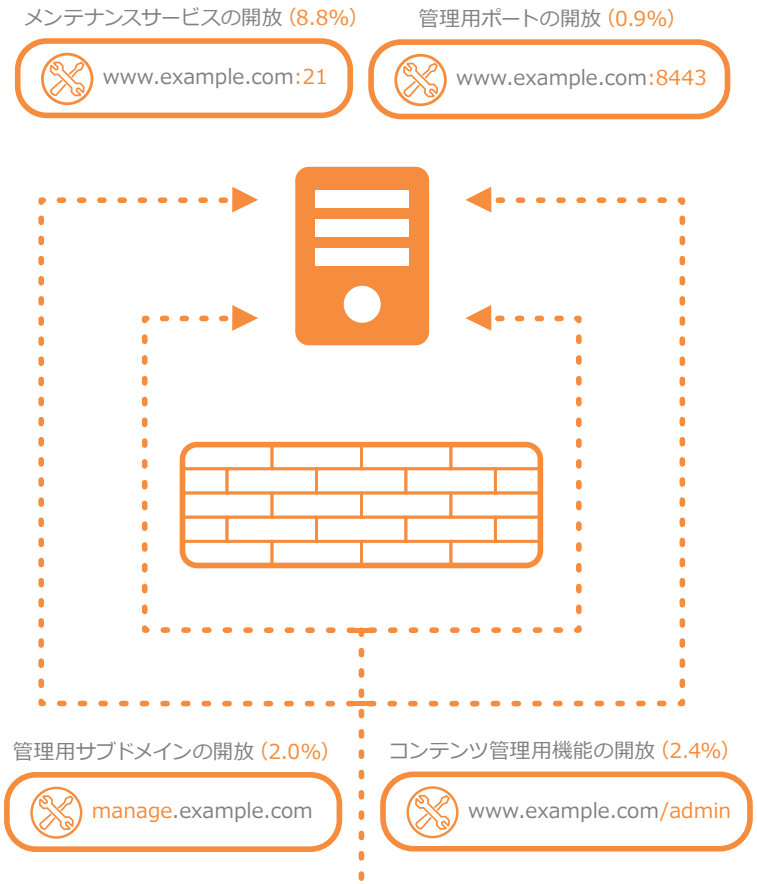
以上の対策はUDP増幅攻撃に悪用されないために必要なことですが、DDoS攻撃に悪用される機器は上記のようなサービスを提供するサーバに限ったことではありません。適切な管理がされていないネットワーク機器やIoT機器が存在すれば、悪用される可能性があります。自社の機器が想定外に外部へ公開されていないかなどを定期的に確認することも必要な対策です。

*1 ソフトウェア開発プロジェクト向けにソースコードやプログラムなどを共有できるWebサービス。
*2 memcached のアクセス制御に関する注意喚起, JPCERT/CC, 2018
https://www.jpcert.or.jp/at/2018/at180009.html
*3 UDP-Based Amplification Attacks, US-CERT ,2014
https://www.us-cert.gov/ncas/alerts/TA14-017A

標本数 2,571,251,045件

"裏口" の開いている公開システムが12%

■管理用の経路が開放されていた公開システムの割合



当社のWebサイト群探索棚卸サービス(GR360)で探索した公開システムのうち約12.2%において、管理用の一般公開を意図していない"裏口"経路が開放されていました。主な類型は以下のようなものであり、1つ以上の類型に合致しています。

● メンテナンスサービスの開放 (8.8%)
FTP(21/tcp) または SSH(22/tcp) サービスに該当します。

● 管理用サブドメインの開放 (2.0%)
例えば「manage」といった特定サブドメイン名に該当します。他にもリモートログインやバグトラッキングの製品/サービス/ベンダ名に基づくサブドメイン名などが見受けられます。

● 管理用ポートの開放 (0.9%)
HTTP代替サービス用のポート (8080, 8443/tcp など) において、サーバ管理ツールなどが稼働しているケースに該当します。

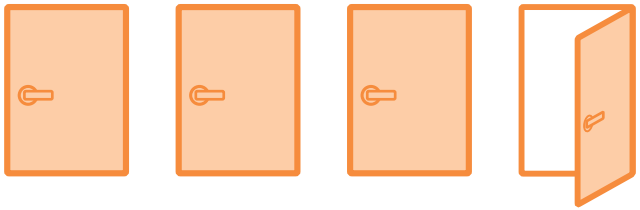
● コンテンツ管理用機能の開放 (2.4%)
例えば「/admin」といった特定のURLパスにおいて、コンテンツ管理機能などが稼働しているケースに該当します。多くはCMS (Content Management System) によって提供されており、さらにうち半数弱をWordPressが占めます。

何れも基本的にパスワード方式の認証のみで保護されており、パスワードを推測された場合に侵害されてしまう恐れがありました。また、得てしてこのような「裏口」で利用している製品はバージョンアップが行われておらず、既知の脆弱性を多数保有している状態でした。
このような攻撃表面の露呈はIPアドレスレベルのアクセス制御で最小限とすべきであり、次善策として認証については多要素認証を利用する、バージョンアップを適宜行う、といった対策が望ましいと言えます。

標本対象サイト数 13,289 サイト

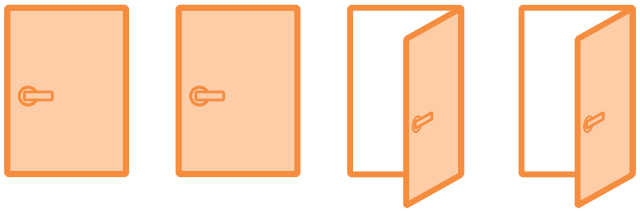
オープンポート管理できていますか?

■インターネット公開が望ましくないサービスが公開されていた機器の割合



1/4

セキュリティ診断を実施した機器全体



1/2

セキュリティ診断を実施した機器
海外に存在する機器のみ

Webサーバであれば80/tcpや443/tcp、メールサーバであれば25/tcpなど、サーバやネットワーク機器の用途に応じて必要なポートは限られています。また、システム管理者が利用する管理用のポート、例えばSSHやFTPなどはインターネット全てに対して公開せず、必要なアクセス元、例えばコンテンツ会社からのみアクセス可能なように設定するのが一般的です。

システムをセキュアに保つためには、サービス提供に必要なポートのみ公開し、不要なポートを公開しないオープンポートの管理が非常に重要となります。

しかし、当社のプラットフォーム診断エクスプレスサービスで診断を行った結果を確認すると、実に24.9%の機器で管理サービスや監視サービス等、本来インターネット公開が望ましくないサービスが検出されています。また海外のサイトでは不要なサービスが公開されている傾向がより顕著であり、49.5%の機器で本来インターネット公開が望ましくないサービスが検出されています。このような不要なポートが公開されていると、攻撃者に攻略されてサーバを乗っ取られてしまう可能性が高まります。実際に発生したインシデントの原因を調査すると、管理サービスや不必要に公開していたポートの脆弱性が原因で攻略されてしまった事例は多く見受けられます。

また、最近では公開状態となっているネットワーク機器やアプリケーションの管理用機能にアクセスし、その機能を悪用して機器を乗っ取ったりデータを盗もうとしたりする攻撃が多く観測されています[*1]。これらのオープンポート管理の不備については、システム構築時に考慮ができていないことが一番大きな原因ですが、機器のバージョンアップ時の仕様変更や設定作業のミスによって想定外のポートがオープンしてしまうこともあります。プラットフォーム診断の診断対象は前頁とは異なり、企業が存在を把握し、適切に管理されるべきものですが、それでも、適切な管理が行き届いていないことがわかります。

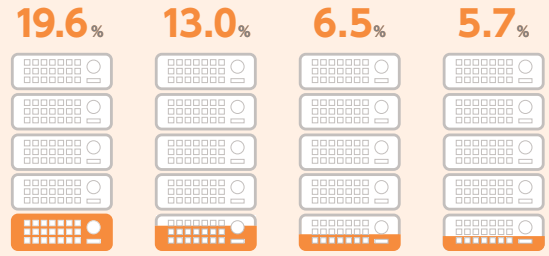
サービス提供に不要なポートをインターネット上に公開しないことは当然のことですが、今回の調査結果からその重要性を改めて知ることになりました。サービス提供しているポートに関してセキュリティを強化することに注力されがちですが、インターネットとの境界に思わぬ入口が空いていないかを継続的にチェックすることは基本的な活動であり、重要な活動であると言えます。

*1 NoSQLデータベース「Redis」に対する探索行為の増加等について, 警察庁, 2018
https://www.npa.go.jp/cyberpolice/detect/pdf/20180521.pdf

標本数 923 IPアドレス(うち、海外109 IPアドレス)

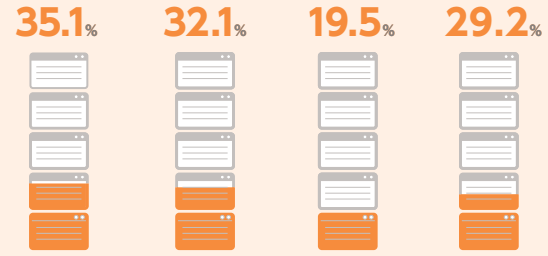
Column Webシステムの脆弱性傾向

■プラットフォーム診断にて危険と判断したシステム割合推移



標本対象システム数

■Webアプリケーション診断にて危険と判断したシステム割合推移



標本対象システム数

● プラットフォーム診断

2017年4月～2018年3月に実施したプラットフォーム診断では、危険と判定したシステム(即座に攻撃可能な問題を発見したシステム)が全体の5.7%を占めました。前年と同程度の割合となりましたが、企業がインターネットに公開するシステム基盤の脆弱性は、依然として一定の割合で残り続けていることが分かります。

危険と判断した問題のうち80.0%は、リモートから任意のコマンド実行が可能、あるいは情報の漏えいにつながるプロダクトの脆弱性に起因する問題でした。また、サポートが終了したソフトウェアを利用し続けているシステムが14.3%存在しており、パッチの適用やソフトウェアの更新による解決が可能な問題が多くを占めていることが分かりました。

● Webアプリケーション診断

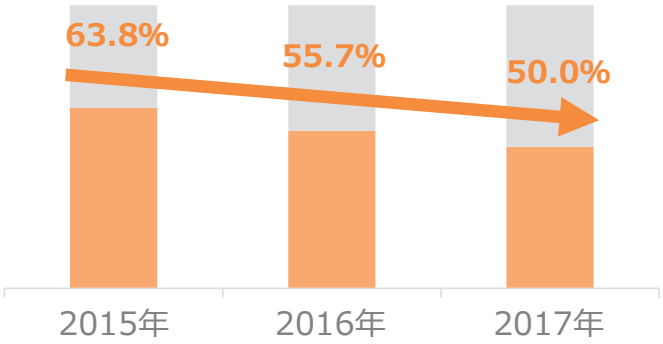
2017年4月～2018年3月に実施したWebアプリケーション診断では、危険と判定したシステム(重要情報に不正にアクセス可能な問題を発見したシステム)が全体の29.2%を占めました。前年は若干減少しましたが、この値は例年30%前後を推移しています。危険と判定した理由では、他のユーザへのなりすましが可能、あるいは一般ユーザが特権機能へアクセス可能である問題が最も多く、全体の73.4%を占めました。これらのような「アクセスコントロール」に関連する問題は、アプリケーション（以後、アプリ）の処理ロジックを理解した上で、その処理ロジック自体の問題を探す必要があることから、ツールによる機械的な検査では発見することが困難な問題です。また、この問題が占める割合が大きいのは例年と同様の傾向です。

クラウド利用や Business IT(BiT[*1])の促進によるビジネスのスピードアップにより、アプリの変更機会が増えていく傾向にあります。FaaS[*2]などのフレキシビリティの高いサーバレス環境においては、よりその傾向が顕著であり、アプリの変更機会が多くなれば意図しないバグが混入する機会も増え、結果として脆弱性が混入する機会も増えると想定されます。また、変更機会が増えることでセキュリティベンダによる検査/修正のリソース確保が困難になることが予想され、その結果、検査/修正に時間を要することが、ビジネスのスピードに影響を及ぼすことになります。一方、アプリのロジックに関する脆弱性検査の完全な自動化は、上述の通り現時点では困難であり、今後は検査ツールの活用等、タスクを可能な限り自動化しながら、開発プロセスにセキュリティを組み込む（DevSecOps[*3]）ことで、手戻りを防ぎ、脆弱性を作り込むリスクを低減していくことが重要になっていくと言えます。

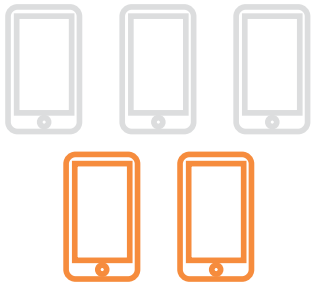
*1 企業のビジネスの拡大に直接貢献するIT。
*2 Function as a serviceの略。サーバレスでアプリを開発することが可能なサービスで、開発者はインフラ管理を気にすることなく、コード開発に集中することができる。
*3 開発 (Development)と運用 (Operations) が密に連携することで、開発期間を短縮し、リリース頻度を高める開発スタイルであるDevOpsに、セキュリティ (Security) を加えて、セキュリティを確保しつつビジネス対応スピードを高めるシステム開発スタイルのことを指す。

スマホアプリの4割はクラウド上に機微な情報をバックアップ

■危険度が中以上の問題を持つアプリ割合推移



■クラウドへのバックアップに機微な情報を含むアプリ



2/5 クラウドへのバックアップ設定がされているアプリのうち**40.5%**

● 危険度が中以上の問題を持つアプリ：50.0%

2017年4月～2018年3月に実施したスマートフォンアプリケーション診断では、50%のアプリケーション（以後、アプリ）に当社基準(高、中、低、参考の4段階の危険度)で危険度が中以上の問題が見つかりました。

今回見つかった危険度が中以上の問題の大半は危険度が中の問題であり、危険度が中と判定した問題には、サーバとアプリ間の通信に対して中間者攻撃が可能となる問題や重要情報をログに出力している問題等を含みます。これらの脆弱性を悪用するには、被害者となるユーザの端末に悪意のあるアプリをインストールさせる、端末を不正なアクセスポイントに誘導する等の端末への介入が前提条件となりますが、利用者をリスクにさらすことになるため、修正することが望ましい脆弱性です。これらは目新しいものではなく、アプリの脆弱性としては古典的なものです。

この割合は3年連続で減少しており、アプリを開発する上で注意すべきセキュリティ事項が浸透しつつあると考えられます。しかし、依然半数のアプリでは、前提条件付きとはいえ、悪用された場合に個人情報の漏えい等に繋がるような危険な問題が作りこまれていると言えます。

● クラウドへのバックアップに機微な情報を含むアプリの割合：40.5%
（クラウドへのバックアップ設定がされているアプリ中）

診断対象のうち96.2%のアプリでは、クラウド(Google DriveやiCloud)にデータがバックアップされる状態になっていました。これらのうち40.5%のアプリでは、アプリが端末内に保存している認証情報や個人情報を含む情報までもが、クラウドにアップロードされるようになっていました。アプリが端末に保存している情報をクラウドにバックアップする機能はOSにより提供されており、実際にバックアップされる情報の制御については、アプリを提供する事業者に委ねられています。

クラウドにこれらの情報をアップロードすることに直接的な問題があるわけではありませんが、仮に何らかの方法でクラウドのユーザ認証を突破された場合、クラウドに保存されたバックアップからアプリが端末に保存していた情報が漏えいする危険性があります。アプリに存在する問題の多くは、端末への介入が前提条件となりますが、この問題はユーザ端末のバックアップ設定に依るので、端末への介入は必要ありません。ユーザを無用なリスクにさらさないためには、不要な情報のアップロードは控えるべきでしょう。アプリを提供する事業者は、端末に情報を保存する際は意図せず機微な情報がクラウドにバックアップされないよう除外設定を行うなどの対策が必要です。

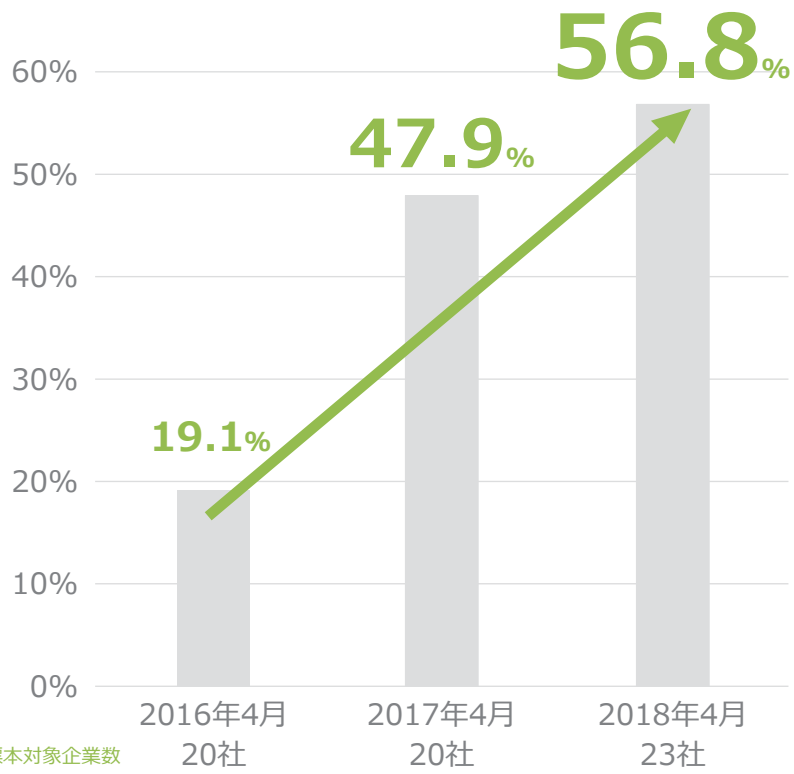
アプリのバックアップ対策を例に取り上げましたが、アプリを提供する事業者はこのようなOSの機能追加に追従したセキュリティ観点を設計時に含めることが必要と言えます。

標本数　47アプリ(2015年)
52アプリ(2016年)
54アプリ(2017年)

ITサービスの利用者への脅威

"常時SSL化"におけるセキュリティ対策

■WebアクセスにおけるHTTPS通信の割合



FNCセキュアインターネット接続サービスのプロキシサーバのログから、全Webアクセスに占めるHTTPS通信の割合の推移を確認すると、2017年4月には47.9%でしたが、2018年4月には遂に50%を突破し56.8%に達していることが分かりました。

またブラウザベンダもHTTPS化の流れに対応しており、Chrome 68ではHTTPで表示される全てのWebページに対して、「安全ではない」ことの警告が表示される予定です。今後もWebサイト全体のHTTPからHTTPSへの移行（いわゆる“常時SSL[*1]化”）を促す動きは継続するものと考えられます。

HTTPSは一般的に、通信の盗聴を防いだり、不正なサーバへの接続を防ぐなど、メリットが多いものです。しかしながらHTTPSによって暗号化された通信は、通信経路上で通信内容の一部しか検査を行うことができません。したがって通信経路上にあるプロキシなどのセキュリティ機器で、ウイルスチェックやURLフィルタリングなどを実施していた企業にとっては、マルウェア感染や情報漏えい等のリスクが高まる可能性があります。

このような状況で考えられるセキュリティ対策としては、主に次の2つの方法があります。

● 通信経路上での一時的なHTTPS通信の復号
通信経路上のセキュリティ機器で通信を復号することで、HTTPS通信の内容を検査します。以前よりプロキシ製品などで実装されていましたが、導入の難易度や機器の計算リソースを大量に必要とするなどの理由から導入が進んでいませんでした。しかしながら、HTTPS化の流れとコンピュータの演算性能向上などを背景に導入事例が増えています。

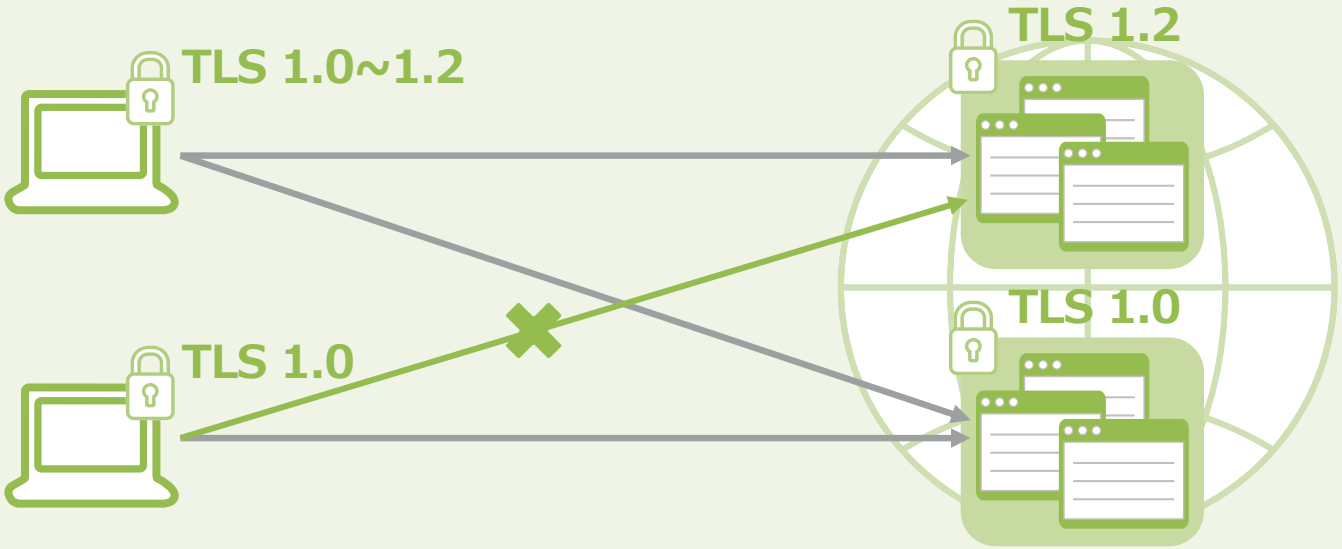
● クライアント端末の機能強化
通信経路上のセキュリティ機器で実装していたセキュリティ機能をクライアント端末上で実装して、暗号化の有無に関わらずセキュリティ機能を適用する方法です。

上記どちらの対応を行う場合でも導入後の運用までを考えた上で整備していく必要があります。自社で導入済みのセキュリティ対策や構成を踏まえて、対応をご検討ください。

*1 機密情報の有無にかかわらず、Webサイトの全通信をHTTPS化(暗号化)すること。SSLはHTTPSに採用されている暗号化方式の名称で、暗号強度や脆弱性の問題からすでにインターネット上ではあまり使われておらず、後継規格であるTLSに置き換えられていますが、未だSSL/TLSの双方を含む暗号化技術の総称としてSSLという言葉が使われることがあります。

Column

変化する暗号化技術に対応できていますか？



前頁にあるとおり、Web サイト全体が HTTP から HTTPS に移行していく流れ（いわゆる“常時 SSL 化”）が進行しており、全 Web アクセスに占める HTTPS 通信は増加傾向にあります。この常時 SSL 化が進行していく中で、もう 1 つ注目しておきたいことがあります。それは HTTPS を実装するために用いている暗号化技術です。

HTTPS には、TLS というプロトコルが用いられています。現在主に利用されているバージョンは TLS 1.0 ～ 1.2 ですが、TLS 1.0 および 1.1 では幾つかの脆弱性が発見されており、最近は 1.2 のみサポートする Web サイトが出てきています。例えば Yahoo! JAPAN や Microsoft Office365 は、TLS 1.0/1.1 のサポートを終了していくことを公表しています。Internet Explorer 8 より古いバージョンを使用している場合などは TLS 1.0 までしか利用できないため、TLS 1.0/1.1 をサポートしていない Web サイトにアクセス出来なくなります。

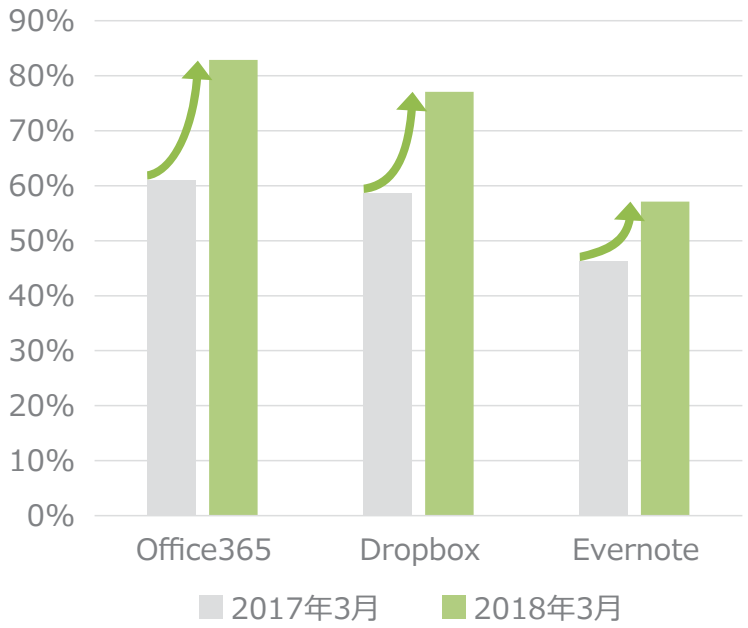
また現在、TLS 1.3 の標準化も進められています。TLS 1.3 では、通信の暗号化方式の強化が検討されています。その中には PFS（Perfect Forward Secrecy）と呼ばれる、セッション毎に異なる秘密鍵を暗号化に用いる手法を強制することで、万が一暗号化に用いた秘密鍵が漏えいしたとしてもその秘密鍵で暗号化した通信全てが復号されることを防ぐという内容があります [*1]。TLS 1.2 までは PFS の性質を持たない暗号化方式も許容されていましたが、TLS 1.3 では利用出来なくなります。これにより秘密鍵の漏えいによる被害影響は小さくなりますが、一方で企業のセキュリティ対策に影響が出る可能性があり、環境次第では今まで通信内容を監視できていたセキュリティ機器構成でも、TLS 1.3 では復号が出来ないということが考えられます。例えばセキュリティ機器を通信経路上ではなく、通信を複製するミラーリング方式で導入している場合には、暗号化に用いた秘密鍵を入手できないため復号出来ません。従って機器を通信経路上に移設して HTTPS 通信を復号し、HTTP 通信をそのセキュリティ機器が検査出来るようにする必要があると考えられます。

常時 SSL 化の流れが進行していくなかで、それを実装するための技術も見直されています。高度化するサイバー攻撃に対抗するために今後も見直されていく可能性があり、このような流れを把握して対応していくことは、企業として必要なことであると言えるでしょう。

*1 SSL/TLS暗号設定ガイドライン 6.3鍵交換で考慮すべきこと, IPA, 2018
https://www.ipa.go.jp/security/ipg/documents/ipa-cryptrec-gl-3001-2.0.pdf

クラウドサービスを安全に利用するために

■主なクラウドサービスの利用企業割合の推移



FNC セキュアインターネット接続サービスにおいて、2018 年 3 月の代表的なクラウドサービスの利用状況を調査したところ、82.6% の企業で Office 365 の、77.1% の企業で Dropbox の、57.1% の企業で Evernote の利用をそれぞれ確認しました *1。アンケート回答による企業のクラウドサービス利用状況では、一部でもクラウドサービスを利用していると回答した企業は 50% 未満であり、今年の数値を大きく下回っています *2。今回確認した数値の増大は、企業によるクラウドサービスの利用が進んでいることも一つの要因である可能性はありますが、実際には企業が把握しているよりも多くのクラウドサービスが利用されており、シャドー IT が多数含まれていると推測されます。

シャドー IT は統制の効いていない外部サービスの利用です。「何が起きているのか把握できていない」という状況は、情報漏えいやマルウェア流入などのセキュリティインシデント発生リスクが非常に高いものと捉えられます。クラウドサービスの利用をセキュアにコントロールするためには、まずシャドー IT の状態にあるサービスの利用を把握し、サービスごとに個別に禁止または認可といった対応を検討するべきです。

ゲートウェイ機器のログを用いたクラウド通信のモニタリングは、このプロセスの起点として非常に有用です。しかし、ログの集計は元々手間がかかるものである上に、クラウドサービスの利用判別においては、そのクラウドサービスが持つ特性やリスクの調査を行わなければならず、しかも定期的にレビューを行わなければならないことから、なかなか定常的な運用を行うのは難しいかもしれません。当社のアンケート調査によると、シャドー IT 対策として通信のモニタリングを行っていると答えた企業は 16.8% にとどまりました *3。

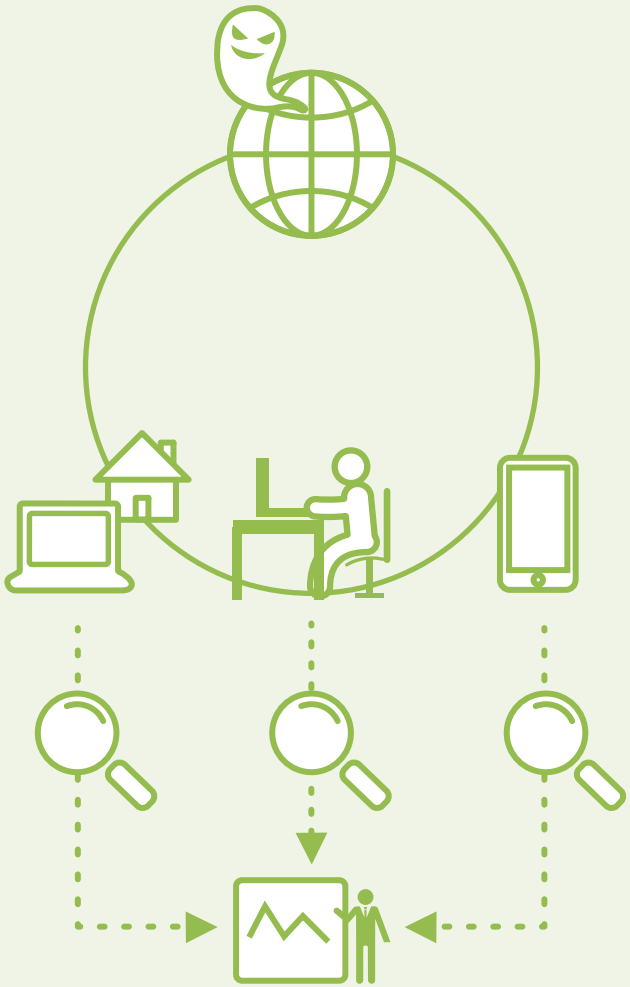
クラウドサービスの利用を効果的にコントロールするためのツールとして CASB(Cloud Access Security Broker) があります。CASB には、ゲートウェイのログを集計してクラウドサービスの利用状況を可視化する機能や、個別のクラウドサービスについて、CASB ベンダによる個々のクラウドサービスの概要やリスクの調査結果を表示する機能もあります。これらを用いれば、効果的にクラウドの利用状況を把握できます。さらに、利用許可したアプリケーションについても、個別のクラウドサービスの利用状況を把握したり、クラウドサービスごとに情報のアップロード禁止や外部公開禁止といった、ポリシーを適用したりすることも可能です。

クラウドサービスはビジネスに必須のものであるといっても過言ではない状況となりました。CASB などの有用なセキュリティツールも用いつつ、セキュアに、かつ効率的にクラウドサービスを利用していきたいものです。

*1 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、当該サービスの利用があったと判断しました。
*2 平成29年版 情報通信白書 第2部 基本データと政策動向 第2節 ICTサービスの利用動向 (4)企業におけるクラウドサービスの利用状況, 総務省, 2017 http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc262140.html
*3 NRIセキュアテクノロジーズ「NRI Secure Insight 2018」より

標本対象企業数 41社(2017年3月)
35社(2018年3月)

Column 働き方改革に勧めるマルウェア感染対策



厚生労働省が主導で行っている「働き方改革 *1」の一つとして、働く環境にとらわれないテレワーク（リモートワーク、モバイルワーク）が推進されています。テレワークを実現する方法として、社員は自宅やカフェなど好きな場所からインターネットを経由して企業のクラウドサービスや社内システムなどに接続して業務を行う機会が増えています。

これまで、企業の社員が社内システムやインターネットに接続する場合、関連する社内のネットワークに対するアクセス規制や監視などのセキュリティ対策が導入されていましたが、テレワークの普及に伴い、社員は多様な環境から多様な経路で企業のクラウドサービスや社内システムに接続するため、従来の仕組みでは十分なセキュリティ対策ができない状況が考えられます。

例えば、端末がマルウェアに感染してしまった場合、社内の端末であれば、直接端末から LAN ケーブルを抜いたり、ネットワーク側で処置したりといった対応が比較的容易にできました。しかしながらテレワークの端末は社外にあるケースがほとんどで、このような対処が社内の端末に比べて非常に困難であると言えます。またテレワークの端末は、公衆無線 LAN や自宅のインターネット回線など、接続するネットワークの統制が取りづらいという点でも、社内の端末に比べてマルウェアの流入などセキュリティリスクがより高まると考えられます。

テレワークでもこれまでと同等以上のセキュリティを担保する解決手段の 1 つとして、EDR（Endpoint Detection and Response）によるエンドポイントセキュリティ対策の強化が挙げられます。

多くの EDR 製品の特長として、社内・社外という端末の環境に依存せずにマルウェアの侵害に対して迅速に調査や対処が行える機能を持ちます。EDR では端末上で発生したイベント、操作ログ、プロセスのアクションなどあらゆる端末情報を常時収集・分析し、管理画面上でその端末に何が起こっているのかを可視化できます。また、管理画面からリモートで端末を論理的にネットワーク接続不能な状態にすることで、物理的な対処をせずとも感染端末を迅速に隔離することも可能です。

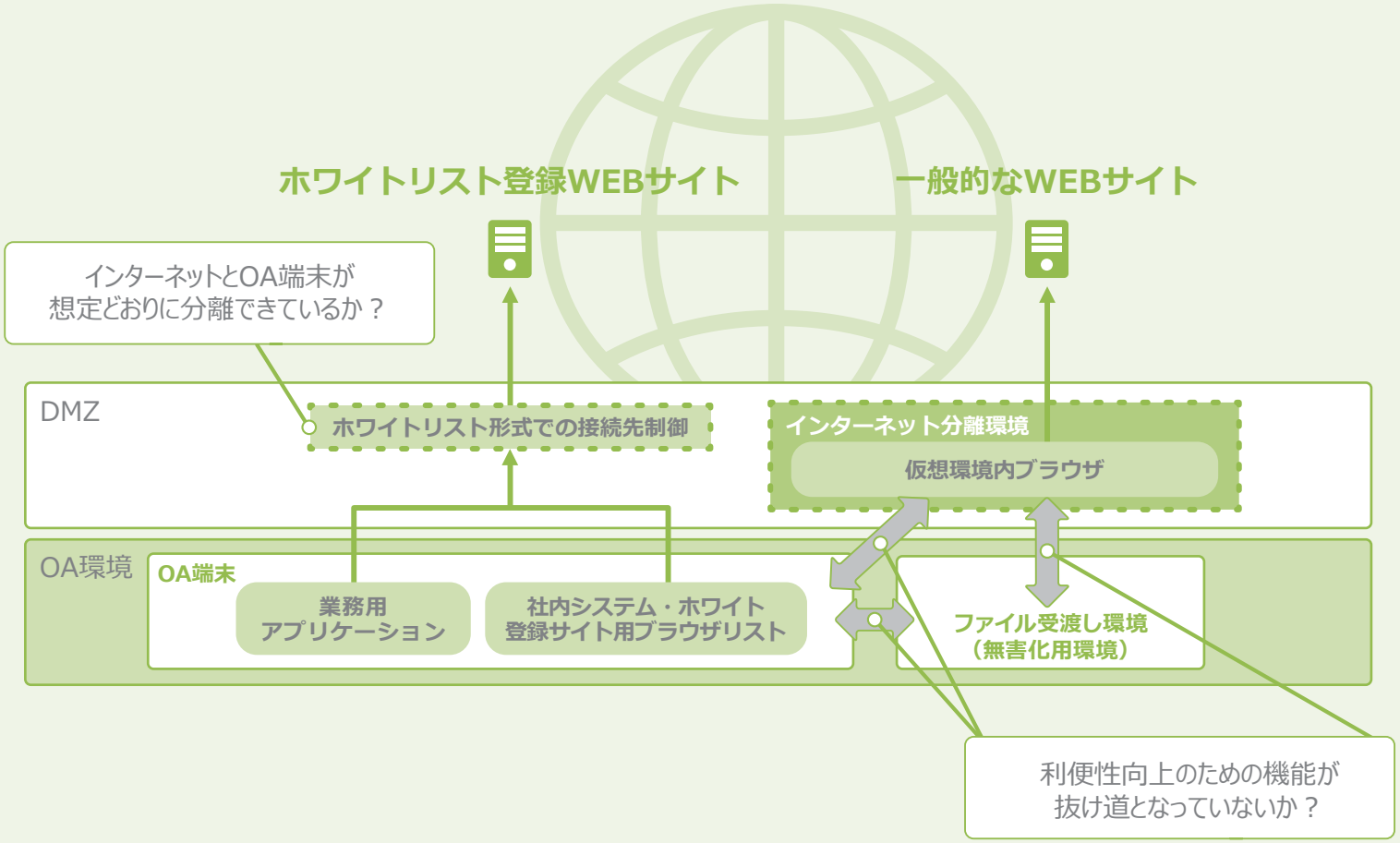
この EDR を新たに組込み、端末側のセキュリティ対策を強化することで、多様な環境で端末を利用するテレワークにおいても、マルウェア感染に対してこれまでと同等以上のセキュリティを担保することが可能になると言えます。

働き方改革によりテレワークが推進されていくことで、新たなセキュリティ上の懸念が生まれてきます。自社の働き方を見直すと共に、自社のセキュリティ対策も見直してみてはいかがでしょうか。

*1 「働き方改革」の実現に向けて、厚生労働省
http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000148322.html

Column

インターネット分離ソリューション導入時に気をつけたいポイント



インターネット接続環境とOA環境を分離することにより、OA端末をマルウェアなどの脅威から守るための対策として近年注目されているインターネット分離（Web分離）。導入に際してはOA端末からインターネットへの接続経路を変更する必要があるため、業務内容や現状のOA環境の構成に合わせて適切な方式を選択する必要があります。また、導入に伴う利用者への影響が大きいことから、業務影響も考慮する必要があり、とても難しい判断が必要です。しかし、業務影響を考慮しすぎたために対策の抜け漏れが生じてしまっている環境を目にすることがあります。インターネット分離ソリューション導入時に気をつけたいポイントとして、以下をご紹介します。

● インターネットとOA端末が想定どおりに分離できているか？

企業内からのインターネットへの接続はWebブラウズやメール送受信だけでなく、OS・アプリケーションの更新やテレビ会議など、特に利用者に意識させずにインターネットとデータをやり取りしているケースもあります。また、Web閲覧時の検索フォームに値を入力する際のコピー＆ペーストもその一つです。これらを全て分離してしまうと業務に支障が出る可能性があります。このように、ブラウザとOA端末の分離、Webブラウザ以外のアプリケーションの通信を遮断する影響は大きく、一般的にはインターネットへの接続を仮想環境経由のみとすることはできません。

このような背景から、インターネット分離導入時には、OA端末からもホワイトリストに登録したWebサイトへはアクセス可能な迂回路を構築するケースが多数です。「インターネットから分離する」といっても、やみくもに迂回路を作れば迂回路経由のマルウェア感染・情報漏えいの可能性は残ってしまいます。迂回を許可するホワイトリストの登録と削除を、適切に運用することが大切です。

● 利便性を向上するための機能が抜け道となっていないか？

インターネット分離環境（仮想デスクトップや仮想ブラウザ）とOA端末間で、何らかの手段でファイルをやり取り可能とする必要がある場合、インターネット分離環境からOA環境にファイルを持ち込むためのファイル受渡し環境を用意しているケースがあります。

このような環境では、ファイル受渡し環境を経由すればインターネットと情報をやり取り可能であるため、インターネット分離の効果をすり抜ける抜け道となりえます。インターネット分離を導入していない環境に比べればマルウェア感染や情報漏えいのリスクを減らすことはできるかもしれませんが、ゼロにすることはできないことを念頭におき、転送ファイルの検査・無害化・検疫をするなどの対策も合わせて検討する必要があります。

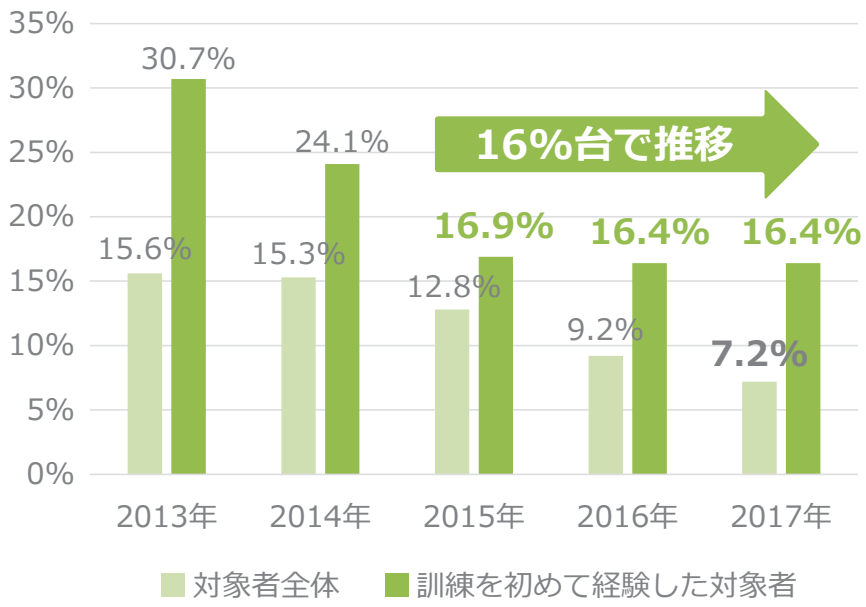
● まとめ：安全なOA環境を実現するためのすすめ

業務影響を考慮しながらインターネット分離を実現するために迂回路などを併せて導入した場合、インターネット接続が可能であることに伴うリスクが残存することとなります。このような中でセキュリティを確保するためには、迂回路を通す接続先の評価やホワイトリスト運用、ファイル転送時の無害化の仕組み、ファイル転送経路での不正アップロードへの対策等、多層防御の観点がより重要となります。

また、対策導入後には想定した効果が得られているか、OA環境構成を大きく変更したことにより想定外の対策漏れがないかを、脅威ベースのペネトレーションテストなどの手段を用いて、効果測定することをお勧めします。

経験者と未経験者でアクセス率に明確な差

■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



2017年4月～2018年3月までに実施した標的型攻撃メール訓練（以下：メール訓練）の対象者全体の添付ファイル実行・URLリンクへのアクセス率は7.2%であり、過去5年の当社統計上、最も低い値となりました。年次のイベントとしてメール訓練を取り入れている企業は多く、繰り返して実施していることで、普段の受信メールに対する注意力が向上している結果であると考えています。

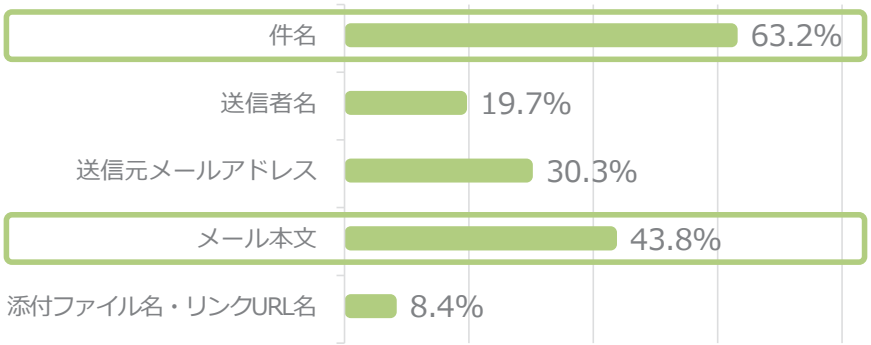
一方、初めて訓練を経験した対象者においては、直近の3年間は16%台を推移しており、およそ6人に1人がアクセスしていることが分かりました。初回経験者のアクセス率が低下傾向にあるのは、メールに起因する攻撃についての研修など、知識の全体的な向上による影響であると考えていますが、それでもメール訓練経験者と未経験者の間のアクセス率には明確な差を確認できます。

メール訓練によって従業員の注意を惹く効果は永続的なものではなく、経験者・未経験者問わず、メール訓練を継続的に実施して、セキュリティに対する啓発活動を行うことは重要であると言えます。実施方法については、対象者をサンプリングしての実施、全従業員を対象に一斉に実施など、企業によって特色がありますが、特に新入社員や中途社員など、未経験あるいは実施経験数の少ない従業員は、積極的にメール訓練の対象者として取り入れていくのが良いでしょう。

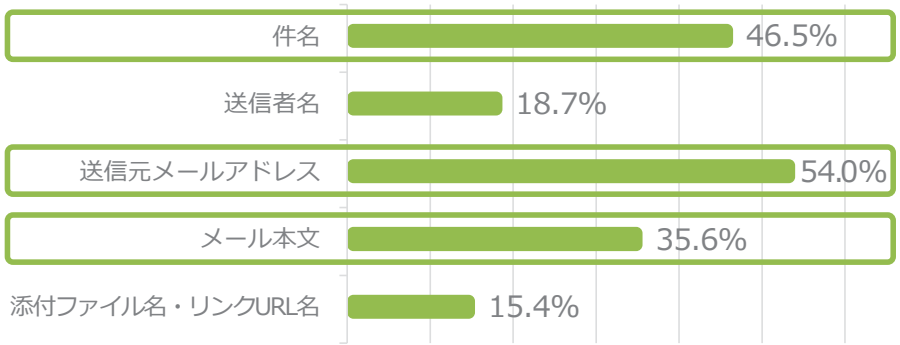
標本対象者数　101,326アドレス（2013年）
190,730アドレス（2014年）
565,376アドレス（2015年）
837,703アドレス（2016年）
646,256アドレス（2017年）

不審なメールに気付く人、気付かない人の特徴

訓練メールを正しいと思った人が、正しいと思ったポイント【複数回答可】



訓練メールを不審だと思った人が、不審だと思ったポイント【複数回答可】



2017年4月～2018年3月の間に、メール訓練対象者に実施したアンケートによると、訓練メールが不審であると気付かなかった対象者の多くが、主に「件名」や「メール本文」に着目していたのに対し、不審であると気付いた対象者は、「件名」「メール本文」に加え、「送信元メールアドレス」にも着目していることが分かりました。訓練メールの本文、件名、送信元メールアドレス、またその内容は、訓練実施企業によって異なるので一概には言えませんが、それでも、不審メールに気付く対象者は、普段の受信メールの取り扱いにおいて、より多くの箇所に注意を払っていることが分かります。

近年、不特定多数の組織を対象に繰り広げられている「ばらまき型」攻撃により、バンキングマルウェアやランサムウェア等の感染被害に遭う組織が後をたちません。かつてこの攻撃に用いられた日本語のメールは、表現や記載が不自然なものがほとんどでしたが、従業員が日常的に受信するメールを騙り、自然な日本語を用いたメール[*1]も多く確認されるようになりました。内容や表現が自然な攻撃メールを受信した場合、「件名」や「本文」のみの情報を頼りに、不審であることに気付くのは困難です。

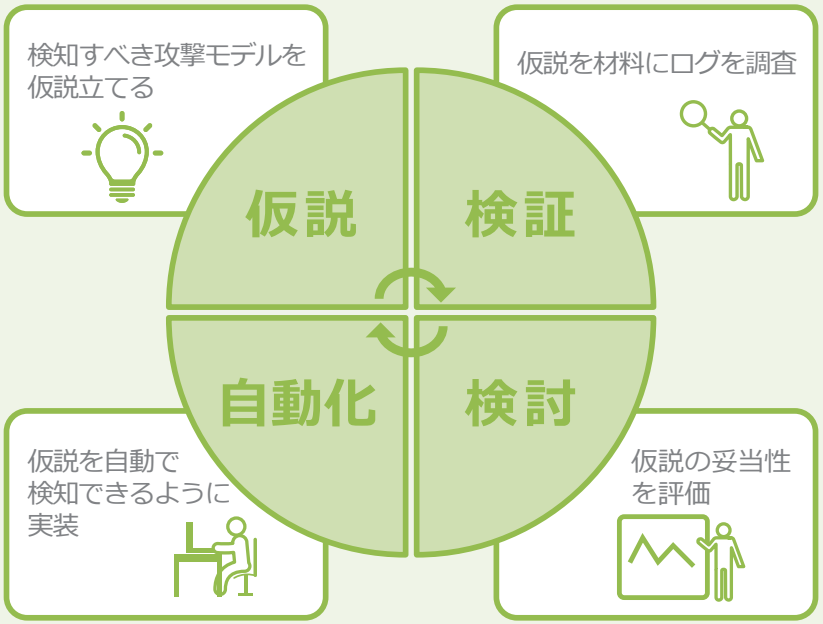
メール訓練では、攻撃手法の全てを再現して従業員に体験させることはできません。ただし、疑似体験を通じて身に覚えのないメールの添付ファイルやURLリンクをクリックしないといった基本動作はもちろん、「件名」や「本文」だけで正しいメールであると判断することなく、「差出人の情報」や「受信した時期」等、を総合的に勘案して違和感に気付く習慣を身につけさせることに役立ちます。また、メールがコミュニケーションの主要な手段であり続ける限り、今後も攻撃手法はますます巧妙化していくと考えられ、巧妙化する攻撃手法の特徴を1人1人に理解させるための取り組みとして、メール訓練はこれからも組織にとって重要な施策の一つであり続けるのではないでしょうか。

*1 例:著名な企業やブランドが日常的に配信するメールを装ったり、内容をシンプルにして不自然さを取り除いたりしたメール等。

標本数　18,870件

Column 潜伏した脅威を狩る「スレット・ハンティング」

■スレット・ハンティング（Threat Hunting）の運用サイクル



スレット・ハンティング（Threat Hunting）という言葉を耳にしたことがあるでしょうか。スレット・ハンティングとは「アナリストが攻撃者に侵入された痕跡がないかを能動的に探索し、それを運用化する」行為を指します。昨今の高度化した攻撃手法によって従来のセキュリティ機器による対策ではインシデントを検知出来ないケースが増えてきたため、注目を集めるようになりました。スレット・ハンティングは、このような検知出来ていないインシデントをアナリストが能動的に分析して発見することで、侵害から検知までの期間をできる限り短縮する目的で行われます。

スレット・ハンティングには、EDR(Endpoint Detection and Response) などが取得するエンドポイントのログや、ファイアウォール、プロキシなどのネットワークのログが必要ですが、それらを相関分析可能なツールである SIEM(Security Information and Event Management) があるとより詳細な分析が可能となります。また効果的にスレット・ハンティングを実施するために、攻撃者に狙われる可能性の高い情報資産や、組織で侵害されると重大なインパクトとなる資産など、「守るべき資産の選定」を行います。そして選定した資産に対し、「仮説→検証→検討→自動化」のサイクルを回します。

1. 仮説：日々情報収集を行い、攻撃者が侵入するために用いる検知すべき攻撃モデルを仮説立てします。例えば、不審な PowerShell 実行があればマルウェアに感染している可能性がある、などと仮説立てします。

2. 検証：仮説について当てはまるログがあるか調査します。例えば PowerShell 実行を検知した場合、ログから実行コマンドの内容が確認できるようになっていると、より明確な不審性の判断が可能です。インターネット上のファイルをダウンロードし実行を試みている場合は、インシデントの可能性を疑います。

3. 検討（仮説の評価）：検証から一定期間が経過した仮説は、その検出率や妥当性を評価します。インシデントの発見率や誤検知の多さなどを鑑み、条件を絞って精度を高めることや、不要として捨てる検討など、調査コストと発見率の見合いを考え運用化可能か考えます。ここでは潜伏している脅威を探索するという性質上、やや擬陽性の検知が発生する程度が適していると評価すべきです。

4. 自動化（運用化）：1 ～ 3 のプロセスにより、運用化された仮説は、同種の被害を検出できるようセキュリティ機器や SIEM への適用や、独自のスクリプトを作成することで自動化を検討します。

スレット・ハンティングを効果的に行うには、仮説と検証の質が肝要です。そして仮説に使われる攻撃モデル情報である IoA(Indicator of attack) が如何に充実しているかがスレット・ハンティング活動全体に関わります。またスレット・ハンティングは従来の検知・防御技術に取って代わるものではなく共存・補完関係にあります。攻撃技術や攻撃手法に関する日々の情報収集から得られた知見を、EDR での探索手順や SIEM ルールなど既存の仕組みに適用したり、機械学習に活用したりするなど、能動的に活動することが重要です。

進まぬWindows 10移行

■当社クリプト便サービスユーザの利用Windows OS種別割合

	Windows 7	Windows 10	Windows Vista	Windows XP
延長サポート終了日	2020年1月14日	-	2017年4月11日	2014年4月8日
2018年3月	82.5%	10.6%	0.2%	0.5%
2017年4月	89.5%	4.1%	0.2%	1.1%

当社クリプト便サービスユーザの利用 OS 種別を調査 *1 したところ、2018 年 3 月時点で Windows 7 を利用しているユーザが 80% を超えていたことが分かりました。
2017 年 4 月～2018 年 3 月の1年間で、多少 Windows 10 の利用割合は増えましたが、依然として企業においては Windows 7 の利用が多くを占めており、移行は進んでいません。
Microsoft より、2020 年 1 月 14 日をもって Window 7 のサポートを終了することが発表されており、Windows 10 への移行が推奨されていますが、既にサポートが終了している Windows XP(2014 年 4 月 8 日にサポート終了)、Windows Vista (2017 年 4 月 11 日にサポート終了) を利用しているユーザがそれぞれ 0.5%、0.2% いたことも確認しました。
Windows 10 は Windows 7 と比べてセキュリティ機能が大幅に強化されています。例えば、Windows Defender や Windows Firewall などの機能が Windows Defender セキュリティセンターとして統合され、Windows 7 では提供されていなかった機能が追加されました。ユーザの資格情報を保護する目的として不正なアプリケーションによる読取りを防止したり、マルウェア感染対策としてユーザ端末に対する脅威をリアルタイムに検知して、インシデントレスポンスを可能とするなどの機能が含まれます。
移行が進まない背景には、移行に必要な人的リソースやコスト不足が影響していると考えられますが、上記のとおり Windows 10 ではセキュリティ機能が大幅に強化されており、移行することにより大きなメリットがあります。Windows 7 のサポート終了日が迫っていることを踏まえ、早期に移行が進むことが望まれます。

*1 クリプト便利用ユーザの User-Agent ヘッダを基に集計しています。

標本対象ユーザ数　352,980人(2018年3月延べ人数)
299,078人(2017年4月延べ人数)

調査概要

● 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23社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105サイト分、WAF48サイト分、次世代ファイアウォール46サイト分のログを集計対象としています。

● セキュアファイル交換サービス

・クリプト便
インターネットを介した電子ファイルのやり取りを、安全かつ確実に実現するファイル転送ソリューションです。本レポートでは2017年4月～2018年3月にクリプト便を利用したユーザ3,882,271人(延べ人数)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サービス
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2017年4月～2018年3月に、インターネット経由で診断した70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サービス
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2017年4月～2018年3月に診断を実施した407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サービス
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2017年4月～2018年3月に手動にて診断を実施した54アプリケーション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2017年4月～2018年3月に簡易なセキュリティチェックを実施した13,289サイトを集計対象としています。

・不審メール対応訓練サービス
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リンクを記載した訓練メールを送付し、対象者へ不審メールに対する意識づけを行うと共に、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、不審メールに対する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2017年4月～2018年3月に送信した646,256アドレス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 2017 年 4 月～ 2018 年 3 月に、インターネット経由で診断した 923 IP アドレス (うち、海外 109 IP アドレス) 分を集計対象としています。

Cyber Security Trend Annual Review 2018

サイバーセキュリティ傾向分析レポート2018

データ収集・分析　浅野 岳史、石川 朝久、佐藤 元樹、関戸 亮介、月岡 稚恵

執筆　曽谷 祐一、高梨 素良、根岸 大宙、藤原 健、天野 一輝
大塚 淳平、小屋松 美佳、竹森 和也、柏村 卓哉、竹内 和輝
末澤 裕希

編集　原田 諭、内藤 陽介、西 はる菜、西田 助宏、山田 朋美

協力　小田島 潤、菅谷 光啓、佐藤 健、観堂 剛太郎、岡 博文
木内 雄章、吉田 修、西谷 昌紀、中山 潤一、野口 大輔
宮尾 紘太、伊藤 耕介、菅 智彦、田篭 照博、根本 仁美
安福 広

発行　NRIセキュアテクノロジーズ株式会社
〒100-0004　東京都千代田区大手町1-7-2　東京サンケイビル
TEL：03-6706-0622　E-Mail：info@nri-secure.co.jp
ホームページ： https://www.nri-secure.co.jp/

NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ株式会社

〒100-0004　東京都千代田区大手町 1-7-2　東京サンケイビル
E-Mail：info@nri-secure.co.jp　https://www.nri-secure.co.jp/