NRIセキュアテクノロジーズ

第269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2018

～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～

2018年08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サービス開発部
セキュリティコンサルタント　原田　諭

Share the Next Values!

目次

「サイバーセキュリティ傾向分析レポート2018」について

■作成の経緯

- 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、企業などに対する脅威の現状を分析し、その結果を「サイバーセキュリティ傾向分析レポート」として公表
- このレポートは2005年度以降毎年発表しており、今回で14回目

■目的

- 企業や公的機関における情報セキュリティ対策の向上

■集計対象期間

- 2017年4月～2018年3月（一部例外あり）

■レポートの概要

- サイバー攻撃に関する「脅威の現状」および「企業などの対策状況」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P.28「ご参考」を参照

本年のレポートにおけるポイント

■1．意図せず外部開放されている不要ポートが攻撃者の標的になっている

- IoT機器を狙った攻撃が、telnet以外のポートにも分散
- サーバ・ネットワーク機器の不要ポートが、意図せず開放されている
- 意図せず外部開放される可能性を考慮して、自社のセキュリティ対策を検討するべき

■2．クラウドサービスの安全な利用を脅かす”シャドーIT”

- シャドーITは企業の情報漏えいの発生リスクを高めている
- 自社でクラウドサービスの利用実態を把握し、適切に利用を統制する必要がある
- 有効な対策の１つがCASBであり、今後導入が加速していくことが予想される

■3．仮想通貨のCryptojacking（クリプトジャッキング）が増加

- 仮想通貨のマイニングに他人のリソースを活用して、収益を得る方法が登場
- マイニングに関する対策や法整備が追いついておらず
  Webサイト閲覧者にマイニングを実施させる行為においては、今後の動向を注視するべき

目次

目次

1．意図せず外部開放されている不要ポートが攻撃者の標的に

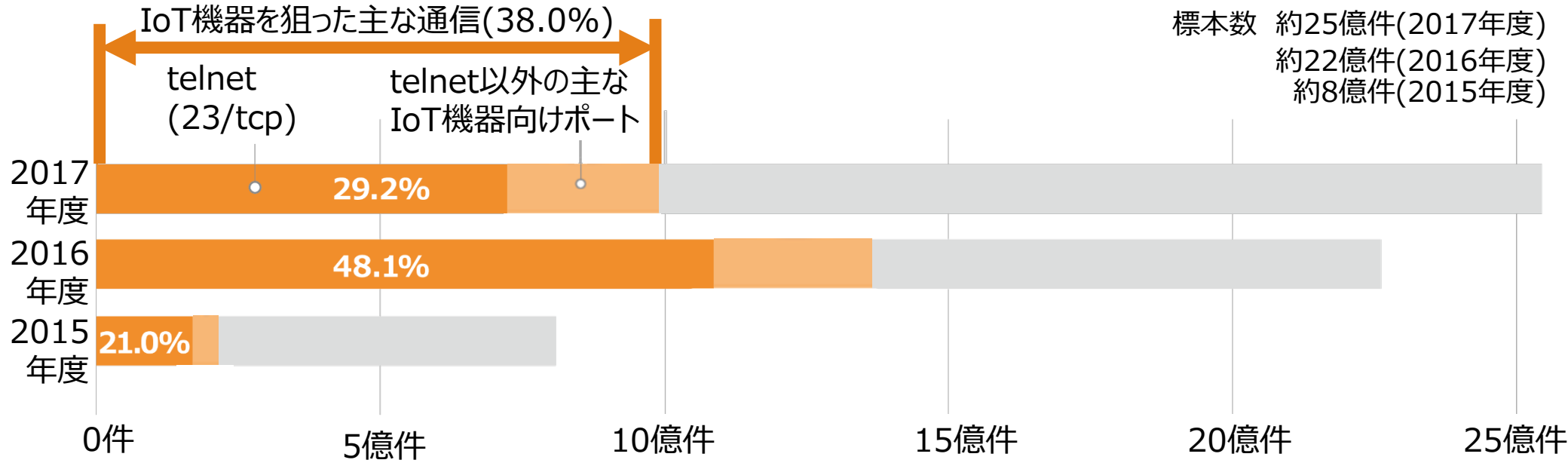
外部からのアクセスをファイアウォールでブロックした通信のうち telnet※1に対する通信割合は減少に転じているものの、依然として多く観測されている

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%→29.2%

（2015年度）　（2016年度）　(2017年度)

ファイアウォールでブロックした通信件数



※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

1．意図せず外部開放されている不要ポートが攻撃者の標的に

攻撃者が探索対象とするIoT機器のポートが分散しており全体では38.0%以上がIoT機器を狙った通信

- 2016年度には、telnetポートに対する攻撃の通信が多く観測された：
  IoT機器を狙ったMiraiマルウェアが背景
- 2017年度はIoT機器の探索行為が減少したのではなく、探索行為の対象ポートが**分散**
  - ファイアウォールでブロックした通信の総数は増加
  - ポートごとのブロック件数上位100種類のうち、
    IoT機器を狙ったポートの割合は2017年度全体の38.0%
- 脆弱性が存在する特定のIoT機器が狙われる
  - そもそも、外部公開する必要がないポートも攻撃対象に含まれる

IoT機器において探索行為の対象となったポートの例

ポート	脆弱性が存在することで攻撃者に狙われたサービスの概要
52869/tcp	特定ルータにおける、他のルータやネットワーク機器と相互接続するためのサービス
9000/tcp	海外製デジタルビデオレコーダにおける、メディア配信用サービス
8291/tcp	特定ルータにおける、管理画面への接続用サービス

脅威分析

セキュリティ設定が甘い状態のIoT機器が、攻撃者にとって格好の標的

- IoT機器は、インターネットに接続して、すぐ利用できるよう初期設定されている場合も多く、そのままでは攻撃を受けやすい
- 2016年のMiraiの登場以降、**攻撃者はIoT機器を格好の標的としている**
- 外部公開不要なポートが開放されているケースはIoT機器だけではない

企業の現状

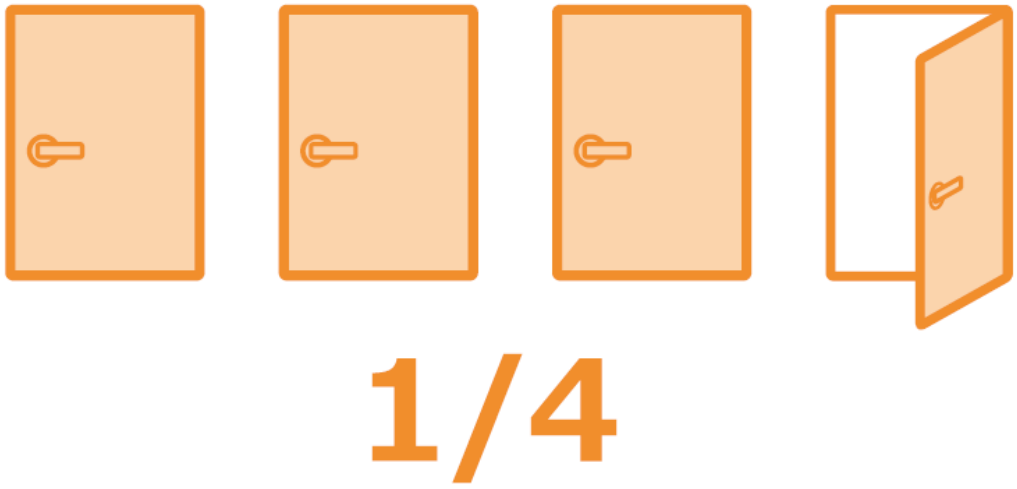
サーバやネットワーク機器の4分の1は メンテナンス用経路が外部開放されており、攻撃者の標的になる可能性

■「プラットフォーム診断エクスプレスサービス」の診断結果によると、
24.9%のサーバやネットワーク機器で、インターネットに公開する必要のないポートが外部開放されていた

■多くは**メンテナンス用**のポートが開放されていた

- システム構築時の考慮漏れ
- 設定変更作業時の戻し忘れ

インターネットに公開する必要のないポートが公開されていた機器の割合：24.9%



標本数　923 IPアドレス

企業の現状

Webサイトに関しては、約1割のサイトで メンテナンス用経路が外部開放されており、攻撃者の標的になる可能性

- 「Webサイト群探索棚卸しサービス(GR360)」の結果によると、**12.2%**の公開Webサイトがインターネットに公開する必要のない**メンテナンス用経路**を外部開放していた
- CMS※1などの管理ツールに見受けられる問題
  - バージョンアップされず、脆弱性が放置されている
  - 初期状態のパスワードや管理画面のパスが広く知られている
  - 公式マニュアルでは、堅牢化させるための情報が十分に提供されていない

公開Webサイトにおいてメンテナンス用の各経路が開放されていた割合

メンテナンスサービスの開放(8.8%)
www.example.com:**21**

管理用サブドメインの開放(2.0%)
manage.example.com

管理用ポートの開放(0.9%)
www.example.com:**8443**

コンテンツ管理用機能の開放(2.4%)
www.example.com/**admin**

標本対象サイト数 13,289サイト

※1: Content Management System の略。Webサイトを管理・構築するためのシステムで、これを利用すれば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となる。

1．意図せず外部開放されている不要ポートが攻撃者の標的に

提言

メンテナンス経路の管理は必須であり、導入時だけでなく運用時にも適切な設定管理とアクセス制御を行うべき

■どんな機器においても、メンテナンス経路のセキュリティ確保は極めて重要

- 外部からの攻撃を許してしまった場合、**システムそのものを乗っ取られてしまう**
- 設定不備によりメンテナンス経路を開放してしまった場合、脆弱性の悪用すら不要なこともある

対策の例

導入時	✓ 外部からのアクセスを許可する対象を特定し、ファイアウォールによるアクセス制限、機器の設定変更などを実施 ✓ 初期設定を確認し、不要な設定の無効化、パスワード変更などを実施
運用時	✓ 利用中の機器における脆弱性情報を把握し、バージョンアップなど必要な対策を実施 ➢ もしくはWAF(Webアプリケーションファイアウォール)やIPS(侵入防止システム)などで代替する ✓ Webサイトや機器の構築・運用に関する社内ルールを定める ✓ 人的ミス等による“穴”を見つけるため、診断サービスなどによる定期的な確認を管理フローに含める

不要なポートの外部開放がないかをポートスキャンで確認するなど現状把握から始めてみることも選択肢の１つ

目次

企業の現状

管理部門が把握できていないクラウドサービスが存在する可能性

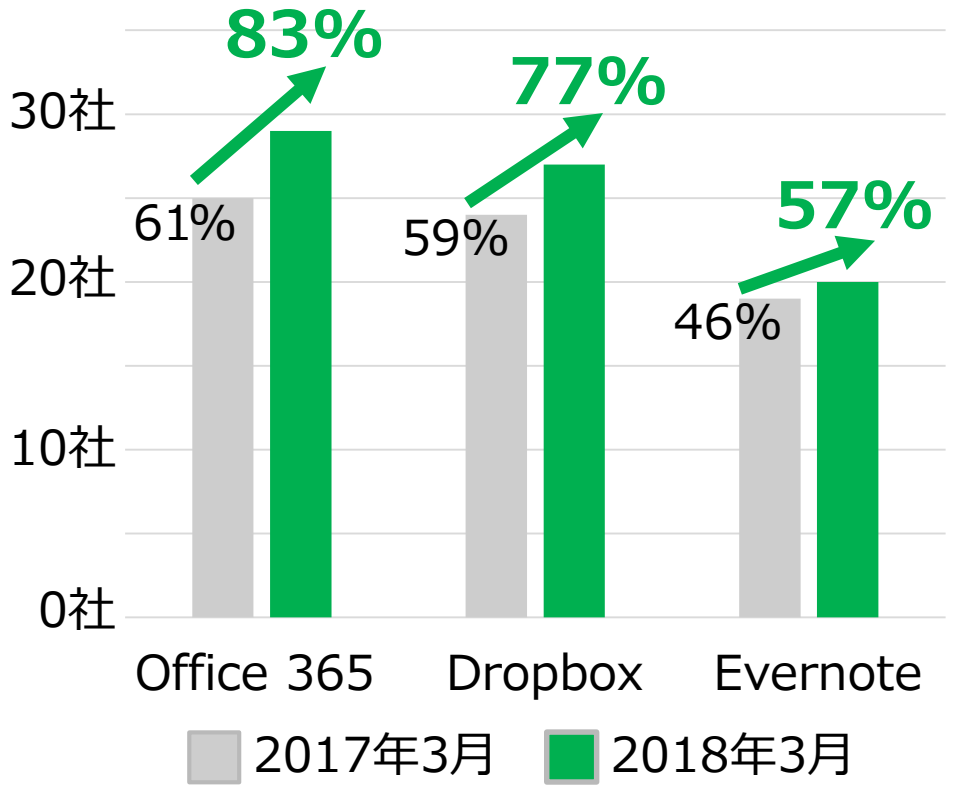
■クラウドサービスの利用率上昇

- 主なサービスについてみると
  昨年度比で**10ポイント以上**の増加

■管理部門は、自社が利用している
クラウドサービスの**全て**は把握できていない？

- 事業部門が勝手に契約
- 他社契約のサービスを利用
- 従業員が個人契約したものを利用

主なクラウドサービスを利用した企業の割合の推移※1



標本対象企業数 41社(2017年3月)
35社(2018年3月)

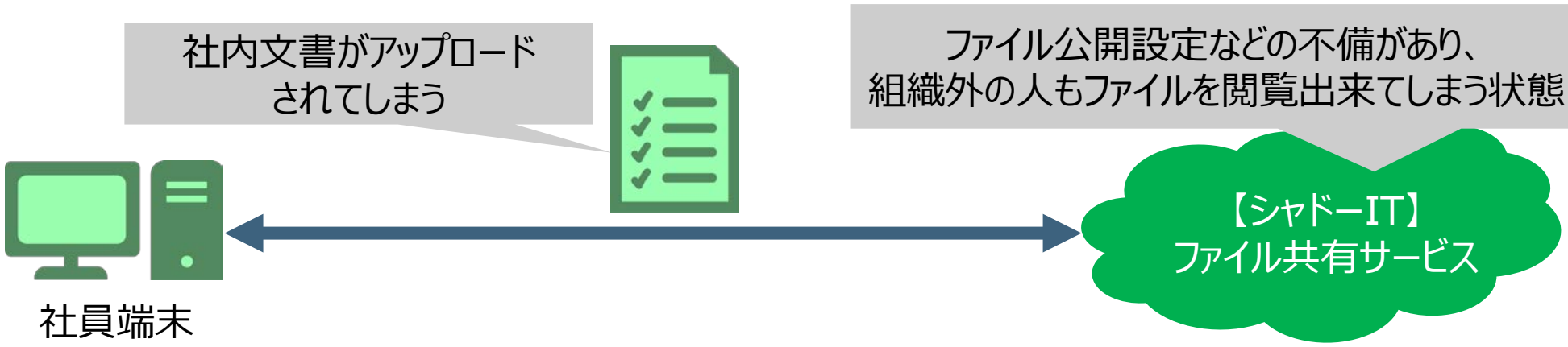
※1: インターネット接続環境において、1ヶ月の間に、
各サービスへ通信量1MB以上の通信が1回以上観測された企業の割合

企業の現状

シャドーITとは

- 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こと
- 適切にセキュリティ対策や利用ポリシーが定められていないIT(特にクラウドサービス)利用は、情報漏えいやマルウェア感染などの発生リスクを高める

把握できていないことが最大の問題
実態を把握し、適切なポリシーに基づいて管理することが肝要



2. クラウドサービスの安全な利用を脅かす”シャドーIT”

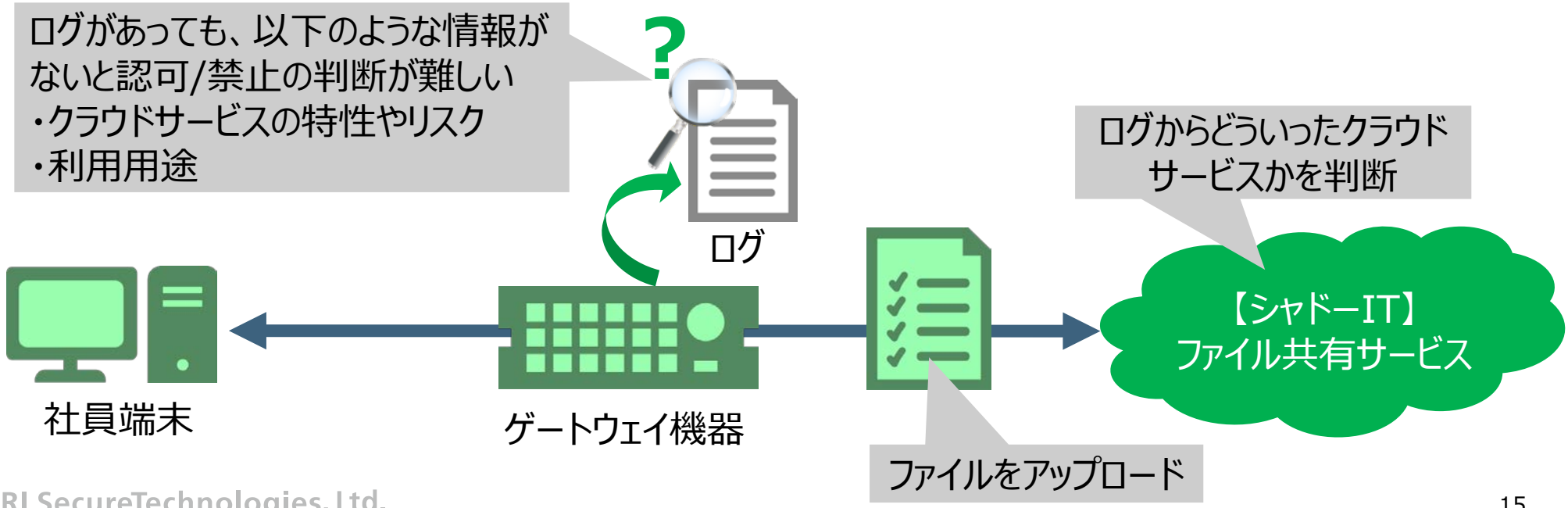
シャドーIT対策における課題
課題１：実態の把握が困難

■ゲートウェイ機器のアクセスログを定常的にモニタリングすることが有用

- シャドーIT対策のために、通信のモニタリングを行っている企業は**16.8%**にとどまる※1

■利用認可・禁止の判断のためには
クラウドサービスに関する情報(宛先URL・特性・リスクなど)が必要

※1: NRIセキュアテクノロジーズ 「NRI Secure Insight 2018」より

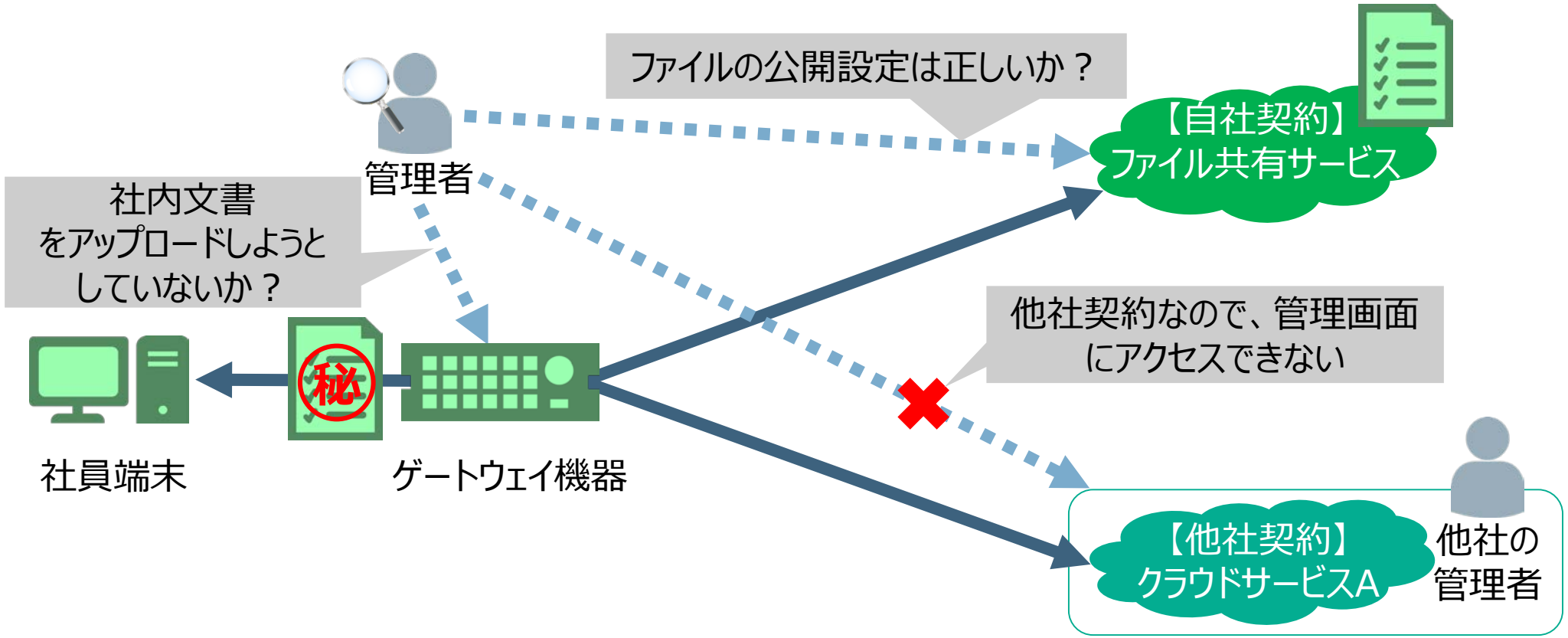


企業の現状

シャドーIT対策における課題

課題２：クラウドサービスの制御が、運用面および技術面で実施困難（1/2）

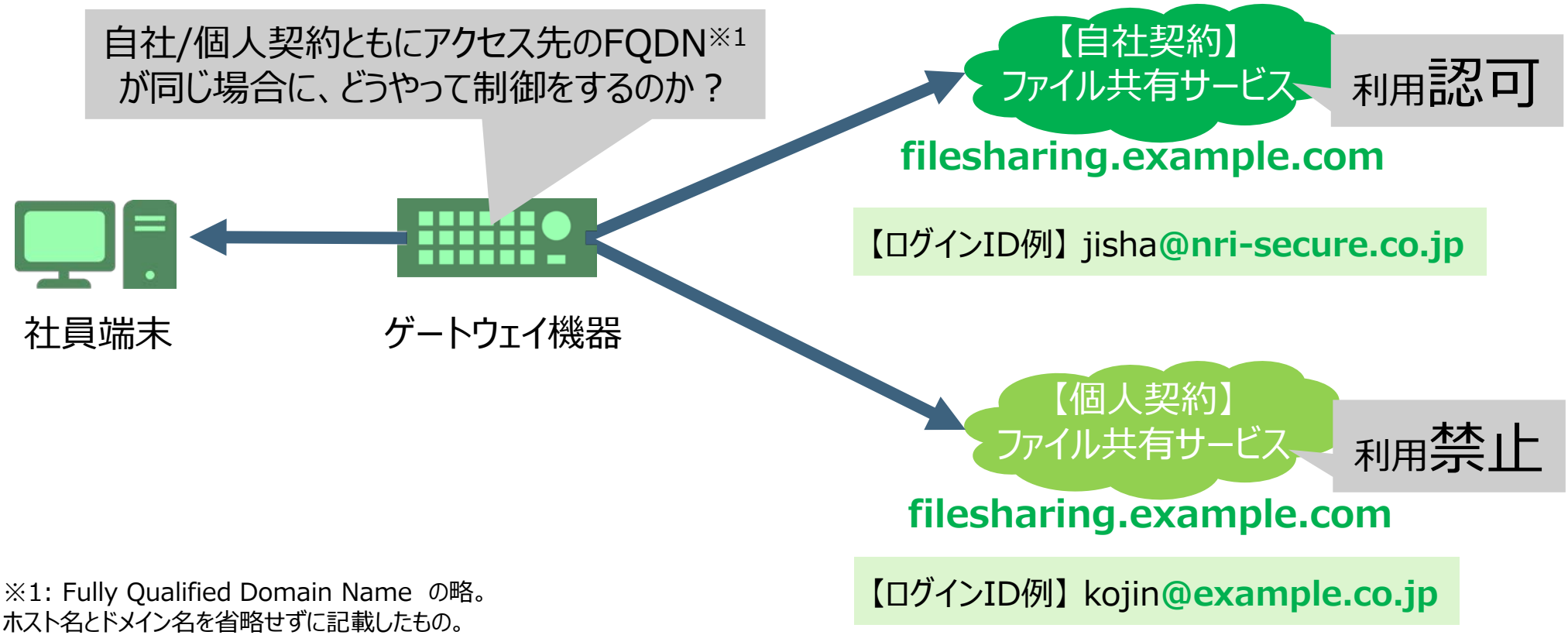
■**運用面：**想定通りに利用されていることを
定常的にモニタリング出来る仕組みを整備することが困難



企業の現状

シャドーIT対策における課題
課題２：クラウドサービスの制御が、運用面および技術面で実施困難（2/2）

■**技術面：**制御したい内容次第では、既存のゲートウェイ機器で対応できない



※1: Fully Qualified Domain Name の略。
ホスト名とドメイン名を省略せずに記載したもの。

企業の現状

シャドーIT対策における課題

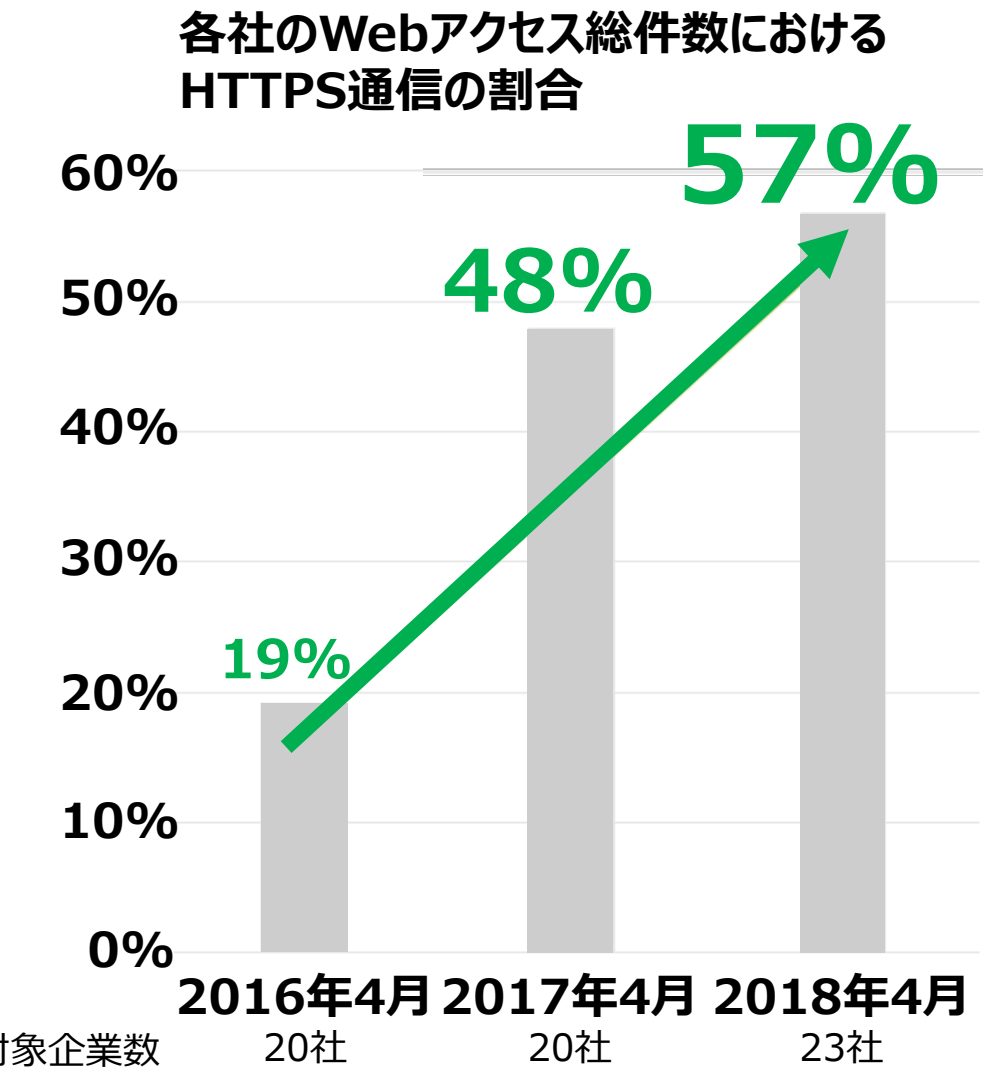
課題３：暗号化通信によりクラウドサービスの利用実態の把握と制御ができない

■HTTPSにより暗号化された通信の割合が増加し続けている

- Webアクセスにおける HTTPS通信の割合は **50%を超えている**
- ほとんどのクラウドサービスは HTTPSを採用している

■暗号化された通信は経路上で内容を把握することができない

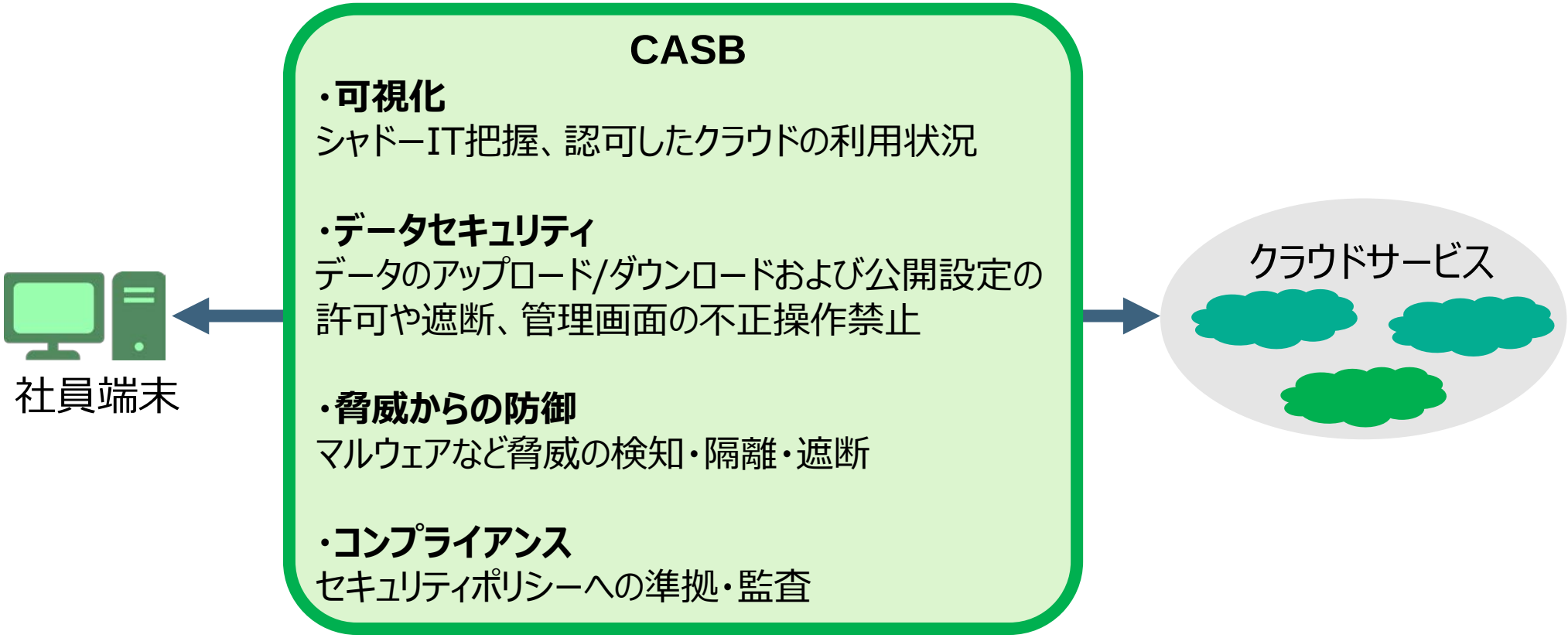
許可したクラウドサービスを制御できず また利用実態も把握できない



提言

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 Cloud Access Security Broker（CASB）製品が注目を集めている

■大手クラウドベンダとの連携や、独自に収集した情報
（各クラウドサービスの特性やリスクなど）をベースとしたセキュリティ機能を提供



提言

CASBにより、シャドーITの把握と制御における課題の解決が可能
今後、日本企業のCASB導入が加速

■課題１（シャドーITの把握）への対応

- アクセスログを集計してクラウドサービスの利用状況を可視化
- CASBベンダによる個々のクラウドサービスの概要や利用状況を評価したレポートを表示

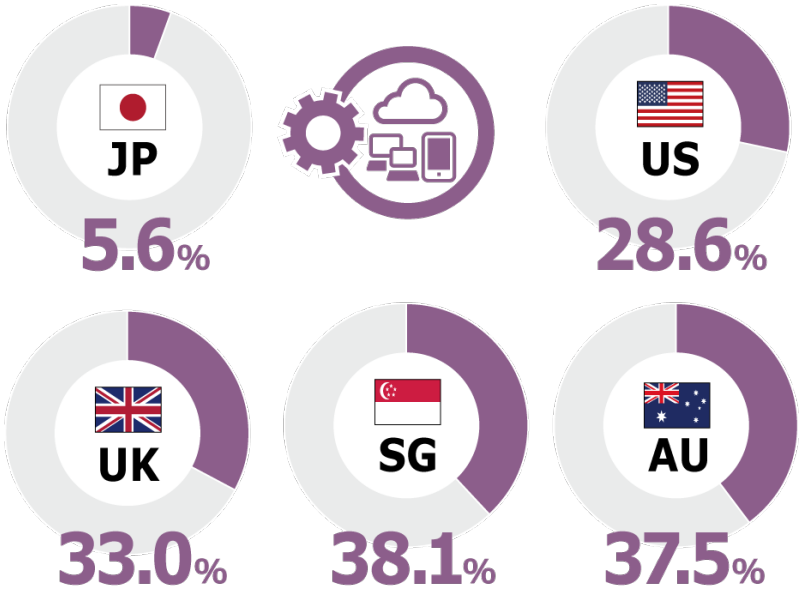
■課題２（クラウドサービス利用制御）への対応

- 多数のクラウドへのアクセスを一元的に制御
- 各クラウドサービス単体では不足している
  セキュリティ機能をCASBが提供できる場合も

■課題３（暗号化通信）への対応

- HTTPS通信の復号が可能

シャドーIT 対策としてCASB等のシステムを導入している企業の割合※1

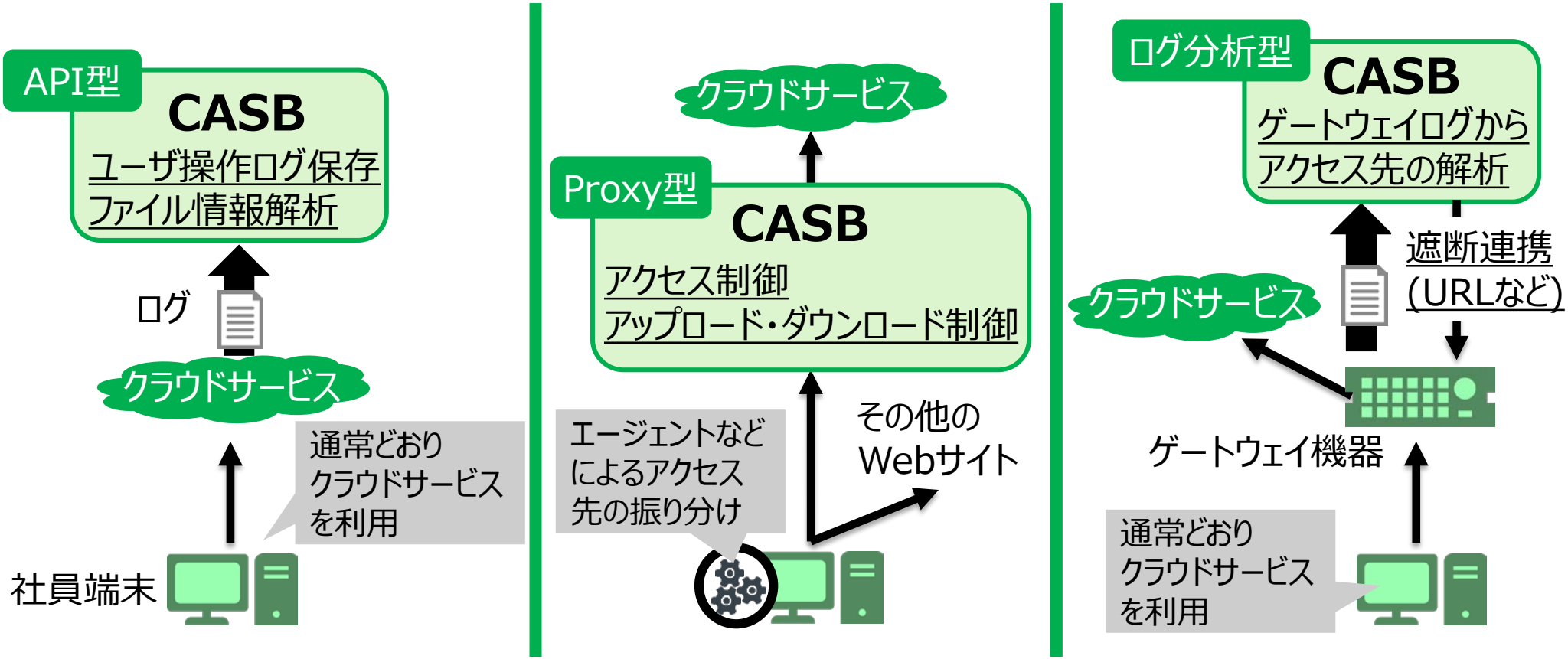


※1: NRIセキュアテクノロジーズ「NRI Secure Insight 2018」より

提言

CASBの導入にあたり、自社として実現したい制御内容を明確にした上で製品を選定すべき

■製品の導入形態（API、Proxyなど）により、実現可能な機能が異なる

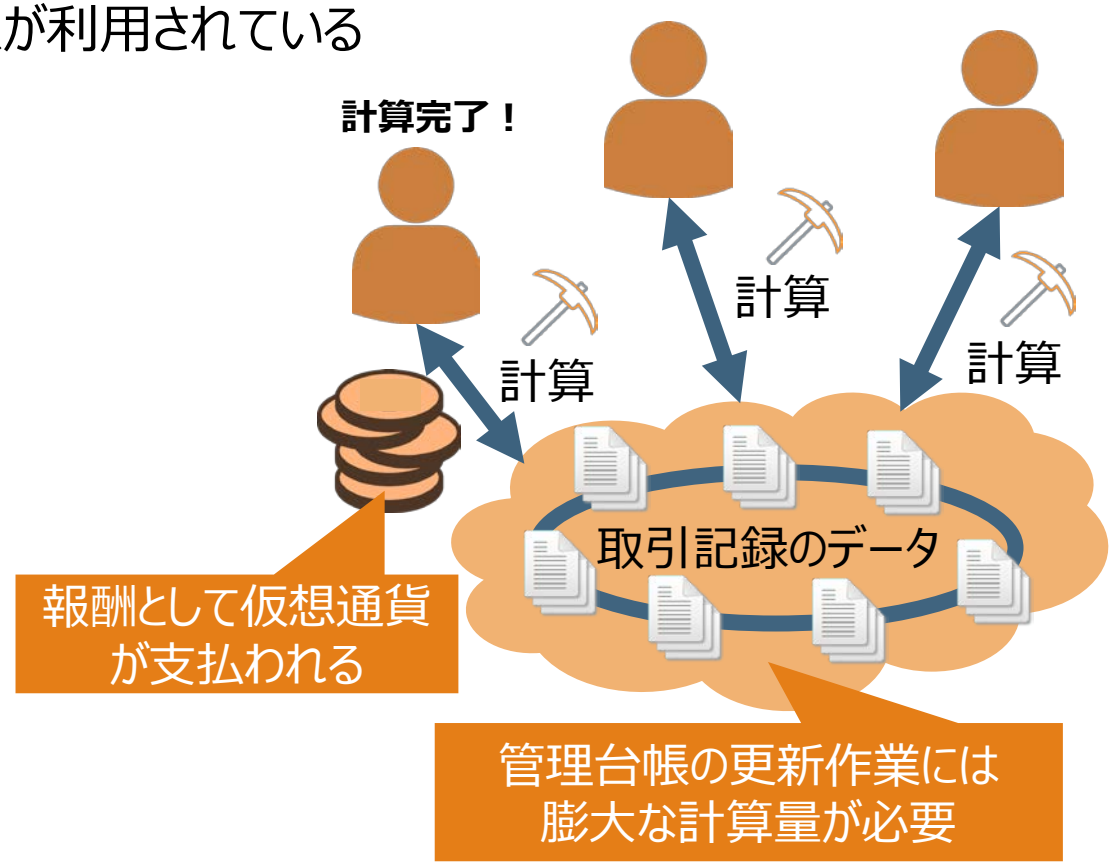


目次

脅威分析

仮想通貨の採掘（マイニング）で報酬が得られるようになっている

- 過去の仮想通貨による取引記録のデータは、分散してインターネット上で管理されている
- 分散したデータの更新に必要な計算作業には、
  個人もしくは組織の端末やサーバリソースが利用されている
- 計算作業に協力した人のうち、
  最も早く正しい計算を完了させた人に
  報酬として仮想通貨が支払われる
- 一連の流れを採掘（マイニング）と呼ぶ
  （仮想通貨の種類によっては
  一番早くなくても報酬がもらえる）

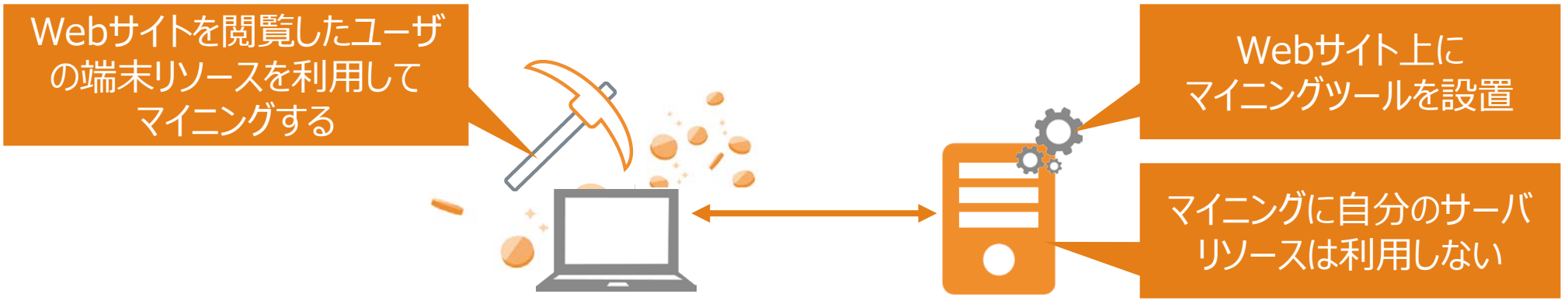


脅威分析

マイニングにあたって、他人の端末リソースを活用することもできる

■仮想通貨を採掘するプログラム(マイニングツール)をWebサイト上に設置し、
そのWebサイト閲覧者の端末リソースを利用してマイニングするサービス
「CoinHive」が2017年9月に登場

マイニングツールが設置してあるWebサイトを、ユーザが閲覧するだけでマイニングが行える
⇒**仮にWebサイト閲覧者の同意や操作がなくても**
マイニングは実行される: Cryptojacking



脅威分析

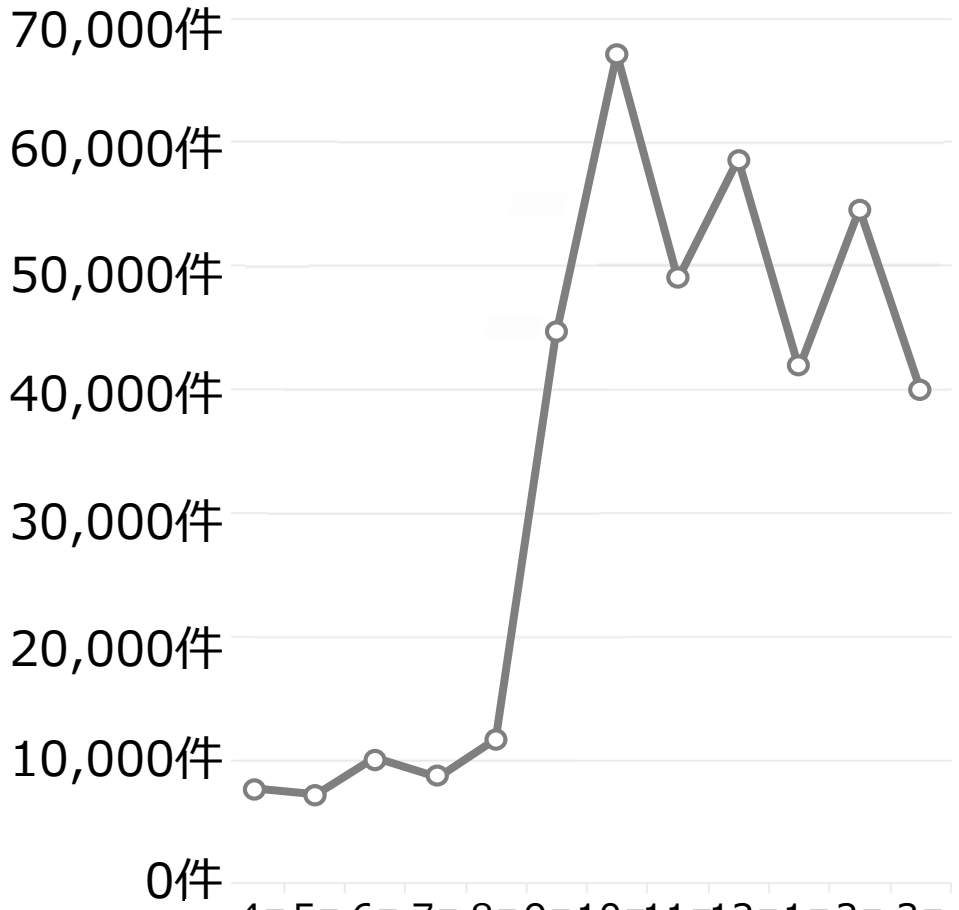
Webサイト閲覧者にマイニングを実施させる可能性があるURLに、多くのアクセス

■CoinHiveの登場以降にアクセスを**多数検出**

- マイニングツールが世の中に認知されて直ぐに、多くのWebサイトがマイニングツールを設置したと考えられる

■多くの場合、
閲覧者は**マイニングを実施している(させられている)ことに気付かない**

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※1



※1:2018年4月時点でのWebサイト情報をもとに集計

標本対象企業数 39社

脅威分析

公開Webサーバに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

- 2017年10月、Oracle WebLogic Serverの脆弱性（CVE-2017-10271）公開
- 脆弱性の悪用方法が特徴的
  - 公開Webサーバに対して、**マイニングツールをダウンロード**させ、成功した場合はそのサーバにマイニングを実施させて、攻撃者が収益を得ようとしていたと考えられる
- 他の脆弱性よりも、マイニングを実施させるのに特別有用であったということではない
  - 単にマイニング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

脆弱性を利用して、攻撃者が収益を得るための新しい手段

CVE-2017-10271の脆弱性を狙った攻撃検知件数

標本対象数 48サイト

提言

Webサイト閲覧者にマイニングを実施させる行為について

■脆弱性を利用して**他人のWebサイト**にマイニングツールを設置する場合

- 設置のためにサイト改ざんを行っている

■**自分のWebサイト**にマイニングツールを設置する場合

- 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※1されており、逮捕事例※2も出ている
- 閲覧者から悪い印象を持たれるリスク

■**今後、マイニングに関する動向が変わる可能性もあり、注視していく必要がある**

- 法整備が進む可能性
- 攻撃者にとって、より、魅力的なマネタイズ方式が登場することで、Cryptojacking自体が廃れていく可能性も

など

※1: 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

※2:「仮想通貨、無断『採掘』の疑い　10県警が16人摘発」, 日本経済新聞電子版, 2018
https://www.nikkei.com/article/DGXMZO31770490140620 18CC1000/

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23社分、次世代ファイアウォール39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。

NRIセキュアテクノロジーズ
NRI SecureTechnologies