IIJ Internet Initiative Japan

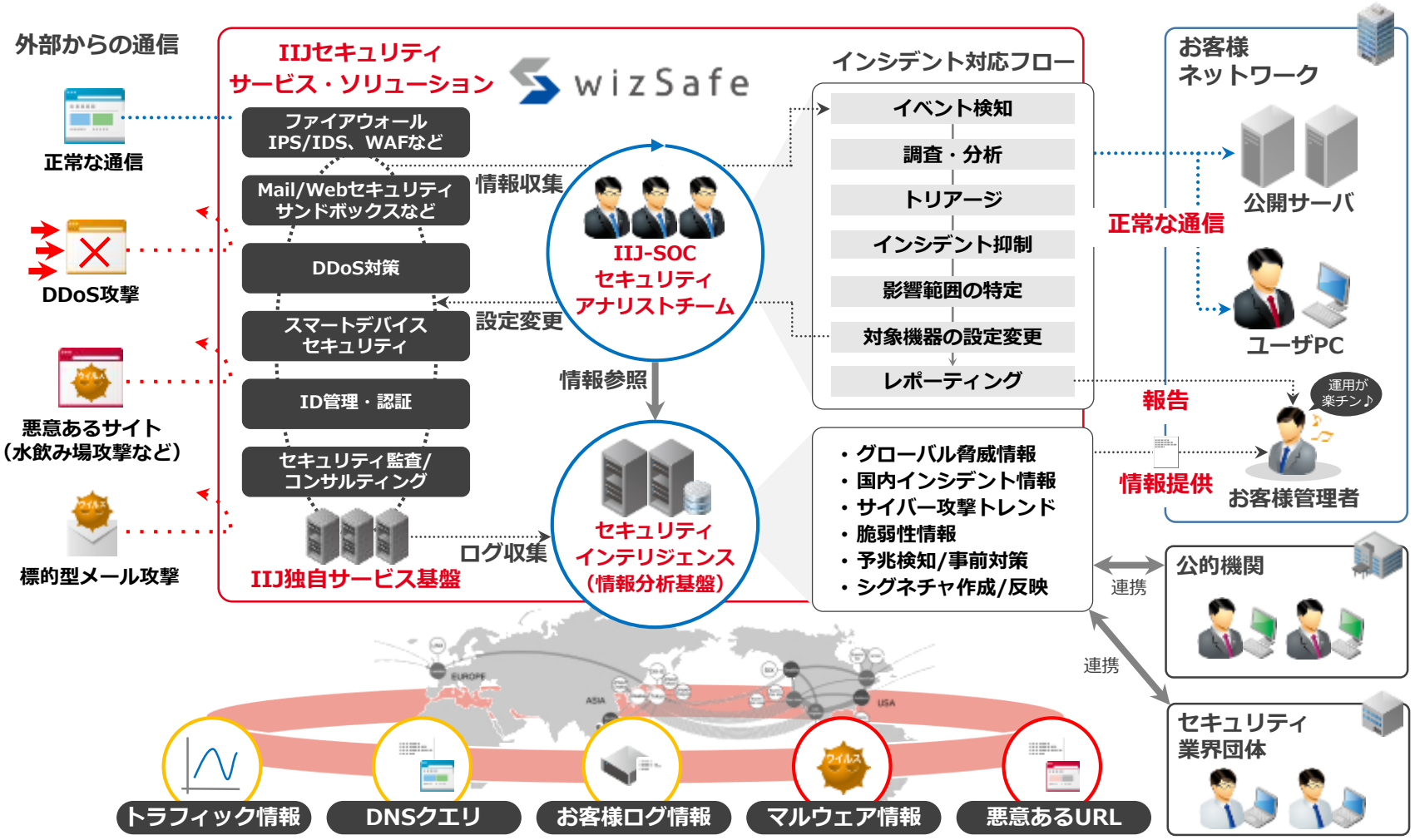
IIJ Technical DAY 2018
セキュリティ動向2018

安全をあたりまえに
wizSafe

2018/11/22
株式会社インターネットイニシアティブ
セキュリティ本部長
齋藤 衛

IIJ セキュリティ事業全体像

検知・防御・対処をIIJ-SOCを中心に24時間365日で実施し お客様のセキュリティ支援を行います。



“wizSafe Security Signal”での観測状況公開

wizSafe Security Signal

安心・安全への道標

https://wizsafe.iij.ad.jp/

HOME　お知らせ　観測レポート

タグ

2017/10/19 Release

- ✓ **情報分析基盤における観測情報・分析結果をもとにした脅威動向。**
- ✓ **新たな攻撃手法や脆弱性など緊急度の高い情報を発信。**
- ✓ **情報分析基盤に取り込むデータの拡大にともない、お客様にとってさらに有益となる情報を提供。**

2017.10.19　お知らせ　観測レポート

wizSafe Security Signal 2017年9月 観測レポート

執筆者：SOCチーム

「wizSafe Security Signal」の公開について IIJのセキュリティ事業を牽引する専門家による新しいセキュリティ情報発信サイト「wizSafe Security Signal（ウィズ…

Read More >

安全をあたりまえに
wizSafe

Agenda

クラウド利用に関連する攻撃

仮想通貨

IoT

DDoS攻撃

安全をあたりまえに
wizSafe

クラウド利用に関連する攻撃

クラウド利用に関連する攻撃

- オフィス環境の現状
  - 一部機能のクラウド利用が当たり前のこととなった
  - Microsoft Office365 など
  - クラウドに関連してオフィス環境のセキュリティを脅かす事件が発生
  - 主にサービス利用の認証情報を盗まれることから始まり、サービスそのもの設定を変更されたり、情報を盗まれたりする。

クラウド利用に関連する攻撃

- クラウドサービスが関連する事件(1)
  - 3月 マイクロソフトやフィッシング対策協議会から注意喚起。
  - 4/24 立命館大学 メールの不正転送
  - 5/6沖縄県立看護大学 メールの不正転送
    http://www.okinawa-nurs.ac.jp/oshirase/documents/H30kouhyoujian.pdf
  - 5/7 島根大学不正メール送信、不正転送
    https://www.shimane-u.ac.jp/docs/2018062200069/
  - 5/18 富山県立大学 メールの不正転送
    http://www.pu-toyama.ac.jp/wordpress/wp-content/uploads/2018/05/300530kaikensiryou.pdf
  - 5/23 弘前大学 メールの不正転送
    https://www.hirosaki-u.ac.jp/wordpress2014/wp-content/uploads/2018/06/300627_siryou.pdf
  - 6/6 横浜市立大　メールの不正転送
    https://www.yokohama-cu.ac.jp/news/2018/pr/dr3e64000000d0fh-att/180606_emailpressrelease.pdf
  - 6/7　文部科学省から注意喚起

クラウド利用に関連する攻撃

安全をあたりまえに wizSafe

- クラウドサービスが関連する事件(1)

マイクロソフトを装った不審メールの配信について

マイクロソフトを装った、下記のような件名の不審メールが、不特定多数のお客様に断続的に配信されています。

このメールはマイクロソフトから配信したものではなく、記載されている内容は事実ではありません。メールの受信を確認した場

メールを開いてしまった場合でも、本文中に記載の URL をクリックしないでください。URL をクリックすると、クレジットカード情
お願いいたします。

＜不審メール件名＞
『ご注意！！OFFICEのプロダクトキーが不正コピーされています。』
『警告！！マイクロソフトのプロダクトキーが不正コピーされている恐れがあります。』
『警告！！ご利用のマイクロソフトのプロダクトキーが何者かにコピーされています。』
『Microsoftアカウントの不審なサインイン』

※こちらはあくまで一例となり、類似した件名で配信される場合があります。

＜不審メール内容＞


2017/01/30 (月) 18:02
support@support-securityprotection-microsoft.com
ご注意！！OFFICEのプロダクトキーが不正コピーされています。
To
セキュリティ警告！！
お使いになっているオフィスソフトの授権が終了されてしまう可能性があります！！
日本マイクロソフトセキュリティチームはお使いのオフィスソフトのプロダクトキーが違法コピーをされた可能性があることを発見しています。
攻撃者はお使いのオフィスソフトのプロダクトキーを利用して他のオフィスソフトを起動しようと試みています。ご本人の操作なのかどうかが確定できないため、お手数ですが、直ちに検証作業をしてくださいますようお願いします。
検証作業をしていただけない場合、日本マイクロソフトはお使いのオフィスソフトのプロダクトキーの授権状態を終了させていただきますので、ご了承ください。
今すぐ認証
•ライセンス認証(マイクロソフトプロダクトアクティベーション)とは、不正コピーを防止するための技術で、手続きは、短時間で簡単に実行できます また、この手続きは匿名で行われるので、お客様の個人情報は保護されております。

https://www.microsoft.com/ja-jp/office/homeuse/attention3.aspx

クラウド利用に関連する攻撃

- クラウドサービスが関連する事件(2)
- 標的型攻撃

図 2 PDF ファイル風のアイコンを使ったフィッシングメール

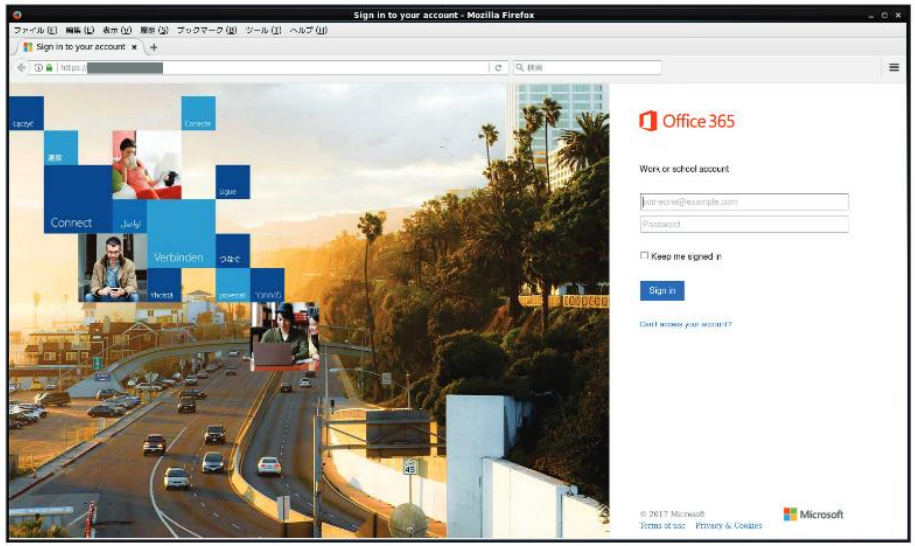


図 3 図 2 のメールから誘導されるフィッシングサイト

サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2017年7月～9月]
https://www.ipa.go.jp/files/000062172.pdf

クラウド利用に関連する攻撃

- クラウドサービスが関連する事件(2)

図 4 Word 文書ファイル風のアイコンを使ったフィッシングメール

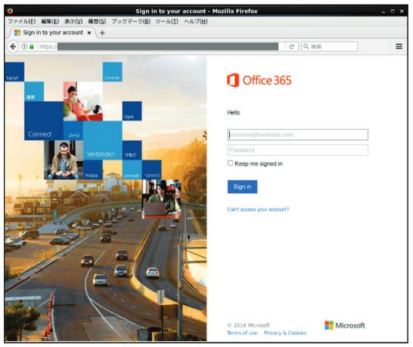


図 5 図 4 のメールから誘導されるフィッシングサイト

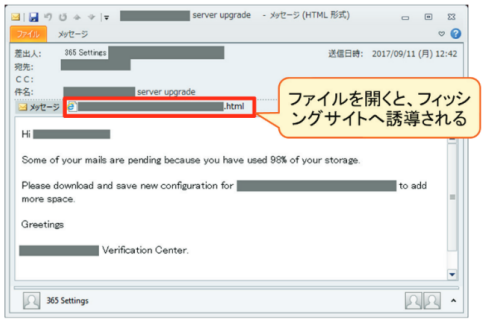
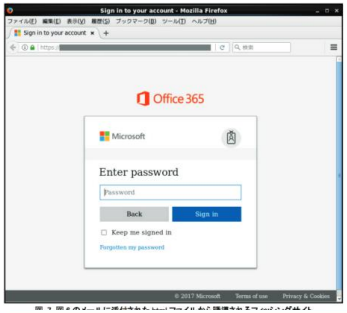


図 6 html ファイルを添付したフィッシングメール



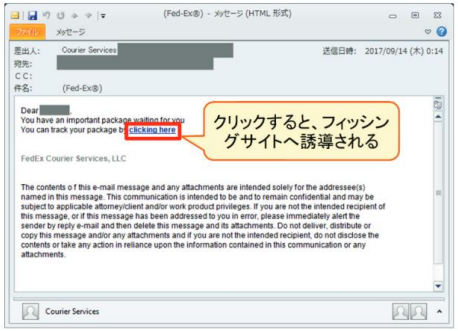


図 8 メール本文中に URL リンクがあるフィッシングメール

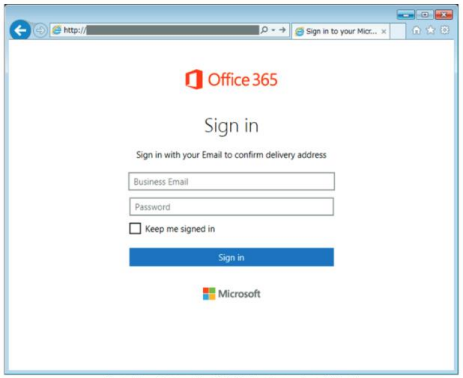


図 9 図 8 のメールから誘導されるフィッシングサイト

サイバー情報共有イニシアティブ（J-CSIP）運用状況 [2017年7月～9月]
https://www.ipa.go.jp/files/000062172.pdf

クラウド利用に関連する攻撃

- 対策
  - 多要素認証、多段階認証
  - ユーザ教育

- そもそも
  - そもそもクラウド事業者を信用してよいか？
  - そもそもクラウド側で提供される新しい機能、連携に対してセキュリティを設計しているか？
  - そもそも従来環境クラウド環境の違いを認識し、セキュリティを設計し直しているか？

安全をあたりまえに
wizSafe

仮想通貨

仮想通貨

- 仮想通貨とは
  - 「仮想通貨」とは、インターネット上でやりとりできる財産的価値であり、「資金決済に関する法律」において、次の性質をもつものと定義されています。

（1）不特定の者に対して、代金の支払い等に使用でき、かつ、法定通貨（日本円や米国ドル等）と相互に交換できる

（2）電子的に記録され、移転できる

（3）法定通貨または法定通貨建ての資産（プリペイドカード等）ではない

代表的な仮想通貨には、ビットコインやイーサリウムなどがあります。

（教えて！にちぎん https://www.boj.or.jp/announcements/education/oshiete/money/c27.htm/）

- いくつかの仮想通貨では
  - ゲームによる通貨の発見（採掘：マイニング）
  - ブロックチェーンによる取引記録

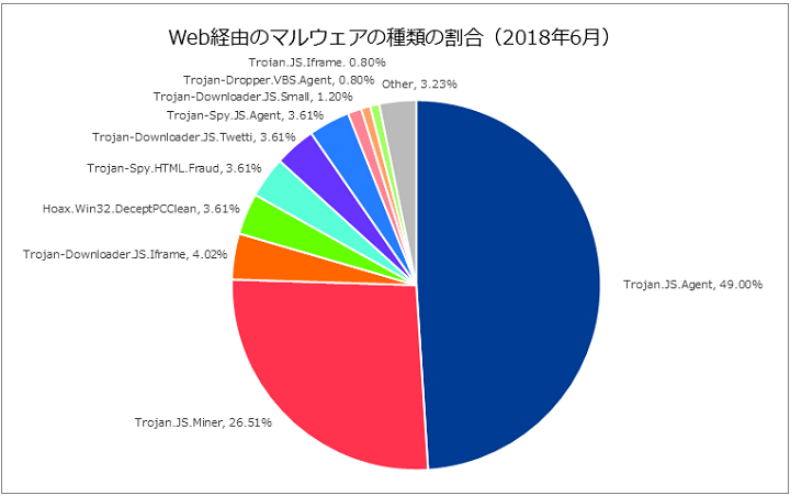
仮想通貨

安全をあたりまえに wizSafe

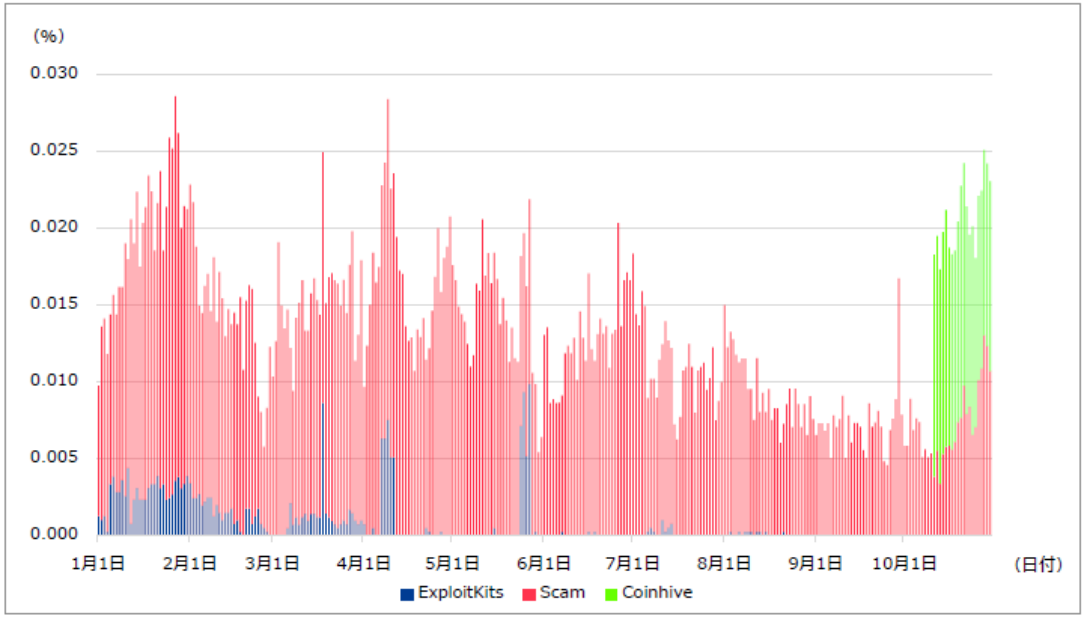
- 仮想通貨の盗難
  - 1/26 CoinCheck 約580億円相当
  - 9/14 Zaif 約67億円相当
- 金融庁の動き
  - 行政処分、指導
  - 仮想通貨交換業者の登録制度

仮想通貨

- コインマイナー
  - 仮想通貨のマイニング（採掘）を行うプログラム
- Coinhive
  - Webサーバにマイニングを行うスクリプトを蔵置し、アクセスしてきたブラウザに仮想通貨の採掘を行わせるためのフレームワーク
    - 広告などと同様にWebコンテンツのオーナによって設置される場合
    - 不正に設置される場合



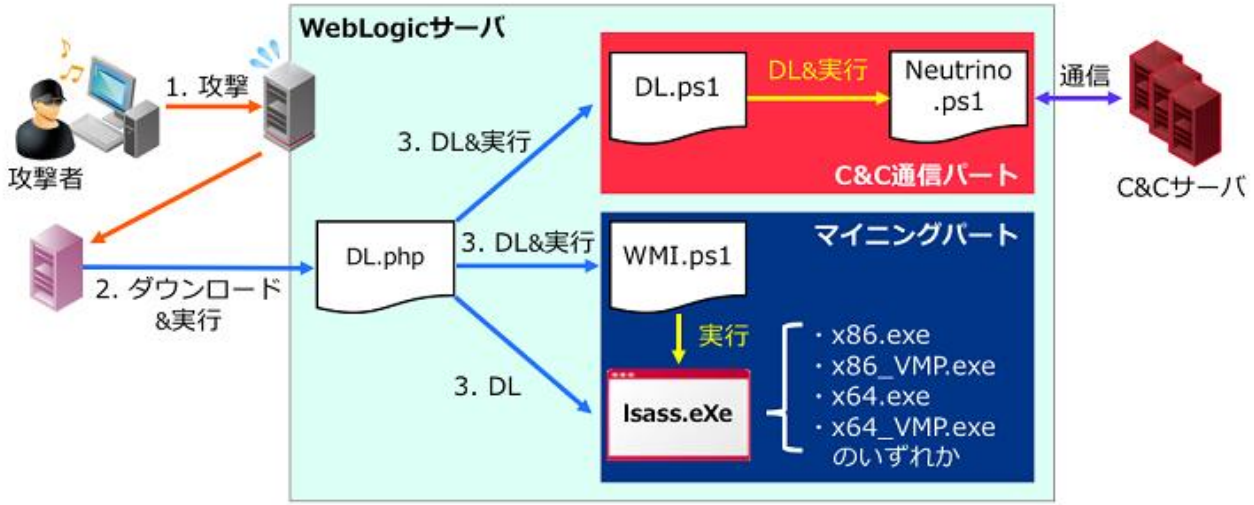
https://wizsafe.iij.ad.jp/2018/07/412/



Exploit KitおよびScamサイトの衰退とCoinhiveの台頭
https://wizsafe.iij.ad.jp/2017/11/120/

仮想通貨

- Webサーバ自身でコインマイナーを動作させようとする試み
  - クラウドプラットフォーム
  - PHPのCGIモード脆弱性、Oracle Weblogic の脆弱性、CMSの脆弱性
  - ３月GhostMiner攻撃キャンペーン



https://wizsafe.iij.ad.jp/2018/04/323/

仮想通貨

安全をあたりまえに wizSafe

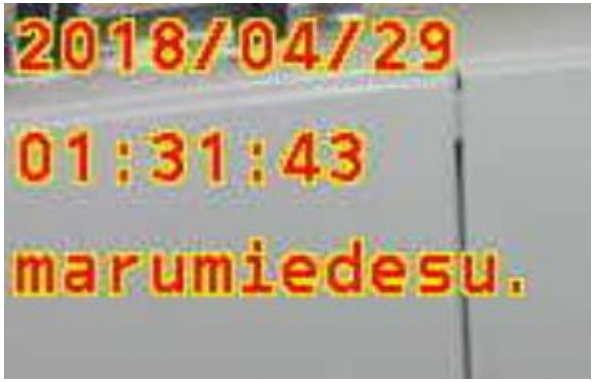
- 対策
- ブラウザでコインマイナーの是非
  - 不正に蔵置されたものは悪
  - 正当に蔵置されたものは？

- サーバでは脆弱性対策を

安全をあたりまえに
wizSafe

IoT

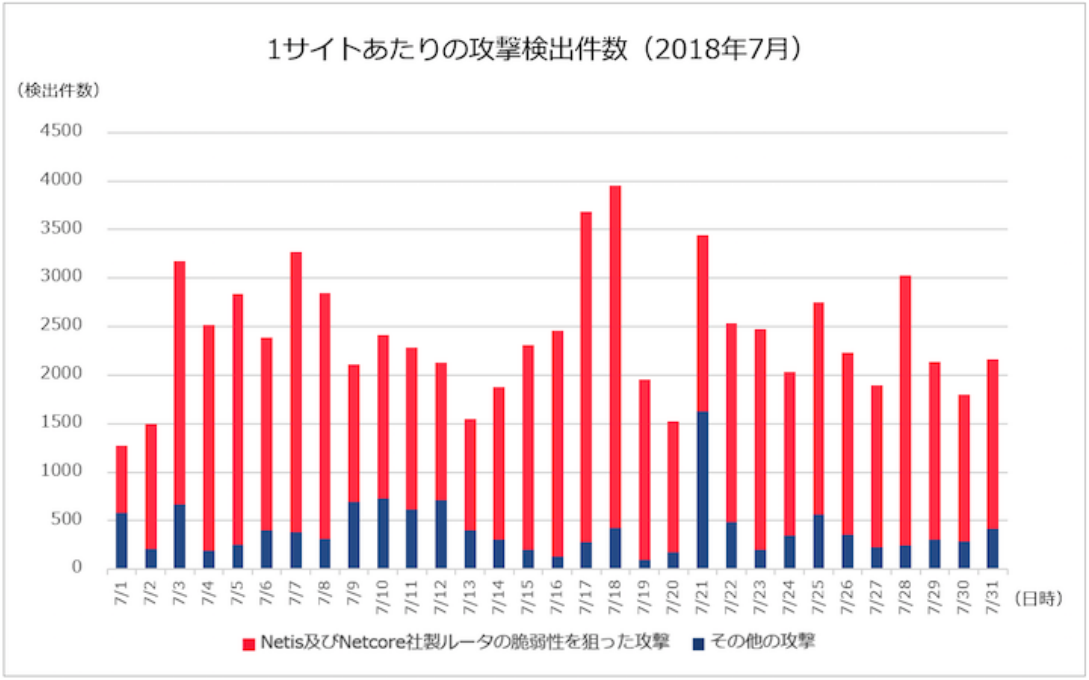
- IoTに関する事件
  - 4月 全国60台ほどの監視カメラが不正に操作されコメントなどを改ざんのうえ公開される
  - キヤノン「ネットワークカメラの不正アクセス防止対策について」
    https://cweb.canon.jp/caution/180426.html



IoT

- IoTに関する事件
  - ホームルータのDNS設定を書き換えられ、Webアクセスを偽のサイトに誘導される。
  - 結果として偽のアプリケーションパッケージ「facebook拡張ツールパッケージ」（facebook.apk,chrome.apk）をAndroidにインストールさせようとする。
  - 複数のルータのデフォルトのIDとパスワードが悪用された。
    Logitec LAN-W300N/R, LAN-W301NR,
    Buffalo WHR-1166DHP4,WHR-G301N,
    NTT東西 Netcommunity OG410Xa,OG410Xi,
    OG810Xa, OG810Xi

- IoTに関する事件
  - Netis,Netcore, D-Link, Huawei, Realtek製ルータなどを狙ったIoTボット感染活動（Mirai botの亜種）



https://wizsafe.iij.ad.jp/2018/08/428/

- 対策
  - 有効な対策手法は（まだ）ない。

安全をあたりまえに
wizSafe

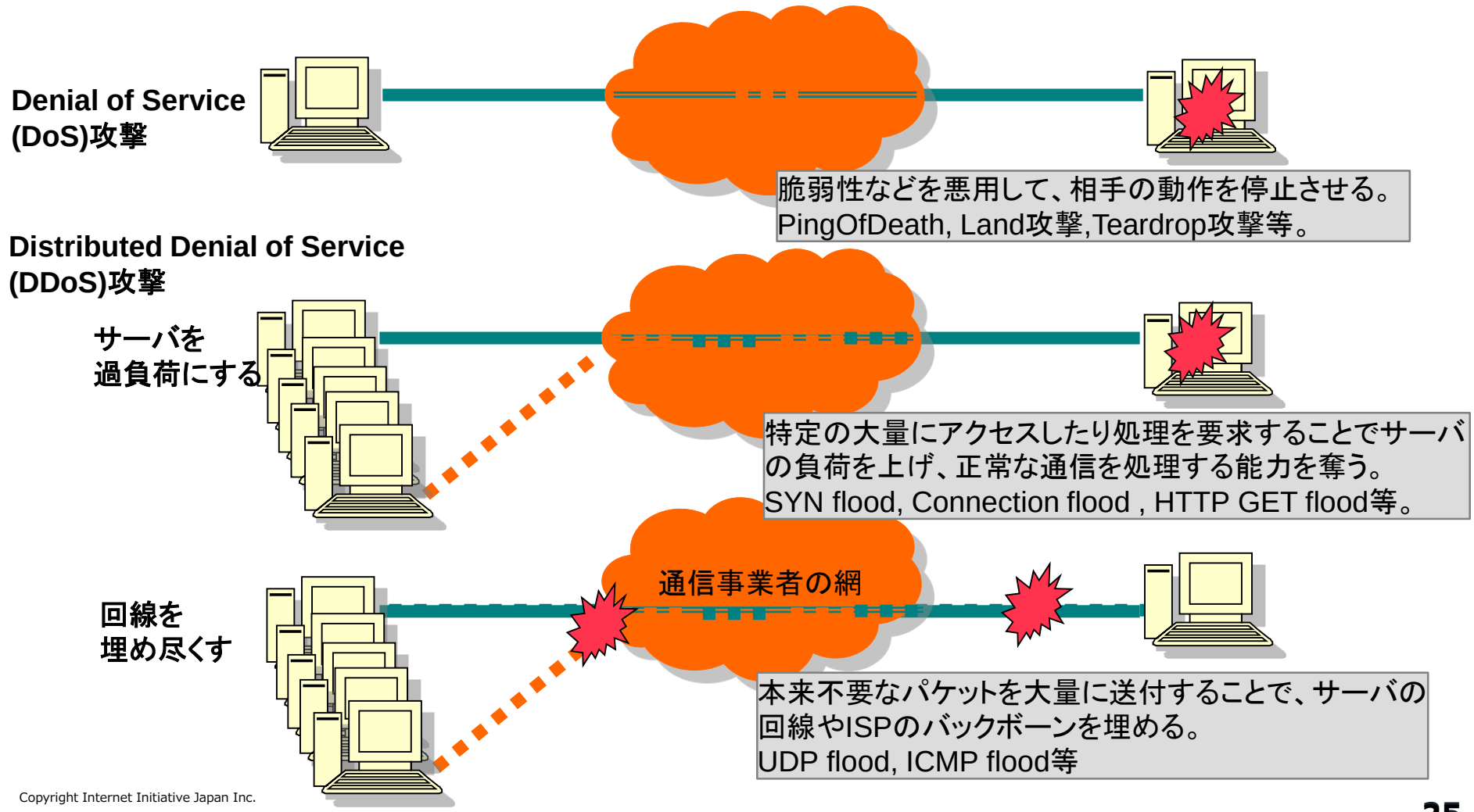
DDoS攻撃について

DDoS攻撃について

- DDoS攻撃とは
  - 特定の宛先に大量の通信を送付することで、攻撃先のサーバの処理能力や回線容量を無駄に浪費させることで、正常な処理を行えなくする攻撃。
- 大量の通信の作り方
  - 多人数で通信行う、専用攻撃ツール、PCのマルウェアやボット、リフレクション（反射型）攻撃、IoTボット

DDoS攻撃とは

DoS攻撃とDDoS攻撃:2つの種類



DoS攻撃：大量の通信の発生方法

- 人海戦術
- DDoS攻撃ツール(多くホストに埋め込み、同時に動かすもの)
- DDoS攻撃機能を持つマルウェア
- ボットネット(指令に従い同時に多数が動作するマルウェア)
- DDoS攻撃ツール(１台で大量通信発生、IPアドレスの詐称)
- DDoS攻撃代行サイト
- 設定のあまいホームルータなどの踏み台
- IoTボット

DDoS攻撃代行サイトの例

DDoS攻撃ツールの例

DDoS攻撃について

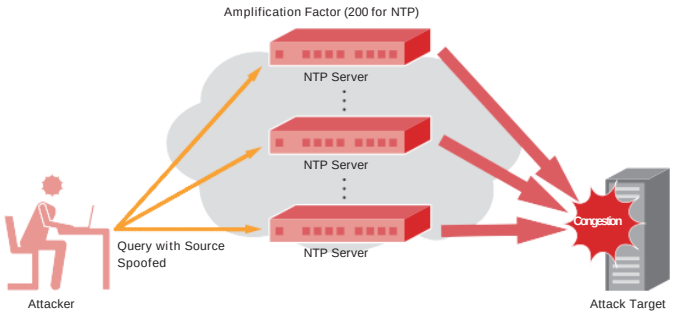
2018年攻撃の傾向

- 自警団的攻撃、オレオレ正義の味方
  - Anonymous
  - ダークネス玉葱君
- ワイドショー型攻撃
  - ワイドショーなどで話題になった悪者に対する攻撃。
  - （おそらく）行為者と被害者の間に利害関係はない
- ゲームのミドルウェア
  - 複数のゲーム、Xbox,PS4などが関係するUDPポートへの攻撃

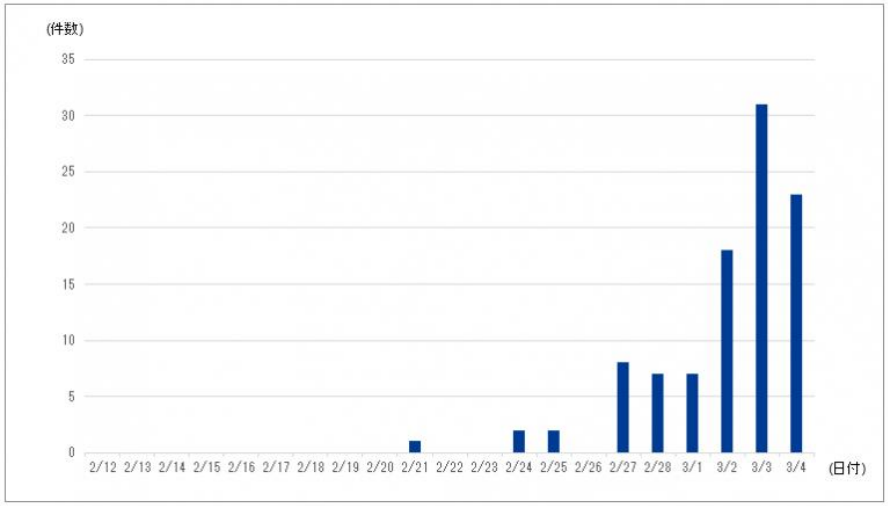
DDoS攻撃について

あたらしい攻撃手法(1)

- Memcachedによるリフレクション攻撃
  - 大規模Webアプリケーションなどで利用される分散キャッシュ技術
  - 数万倍という高い増幅率
  - 3月Githubに対しこの手法で1Tbpsの攻撃が発生
  - 結果として一部クラウド事業者が影響を受けたが、多くの国内ISPでは問題とならなかった。



Internet Initiative Japan Inc., Internet Infrastructure Review (IIR) Vol.23, 1.4.2 DrDoS Attacks and Countermeasures (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol23_EN.pdf)



Memcachedの探索
https://wizsafe.iij.ad.jp/2018/03/269/

DDoS攻撃について

あたらしい攻撃手法

- SYN/ACK攻撃(2)
  - 9 /26 特定のホストから攻撃されているという複数のtweet。
  - のちのそのホストが被害者であることが判明。
  - Webサーバが大量にあることを悪用した、増幅を伴わないリフレクション攻撃。

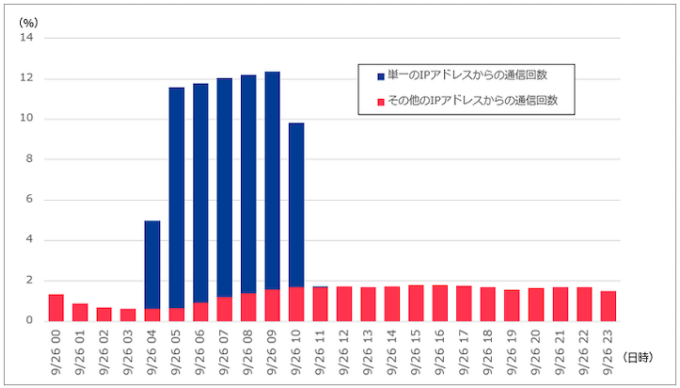


図-11 単一のIPアドレスから80/tcpへの通信の増加

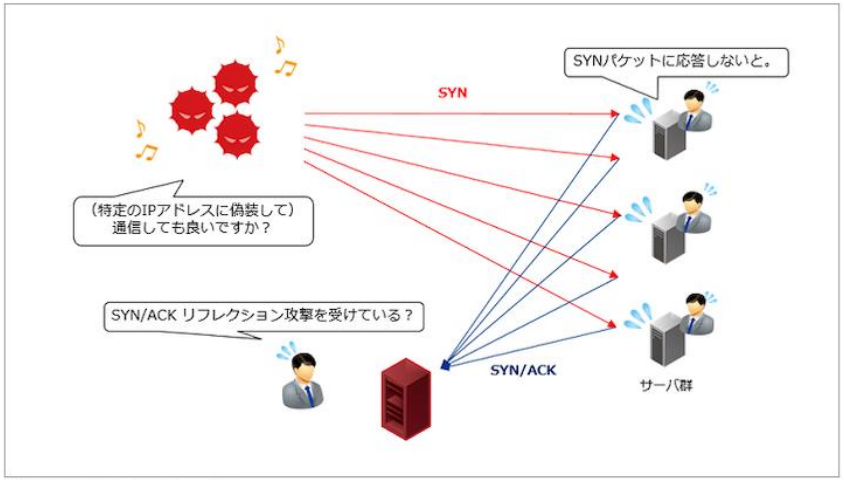


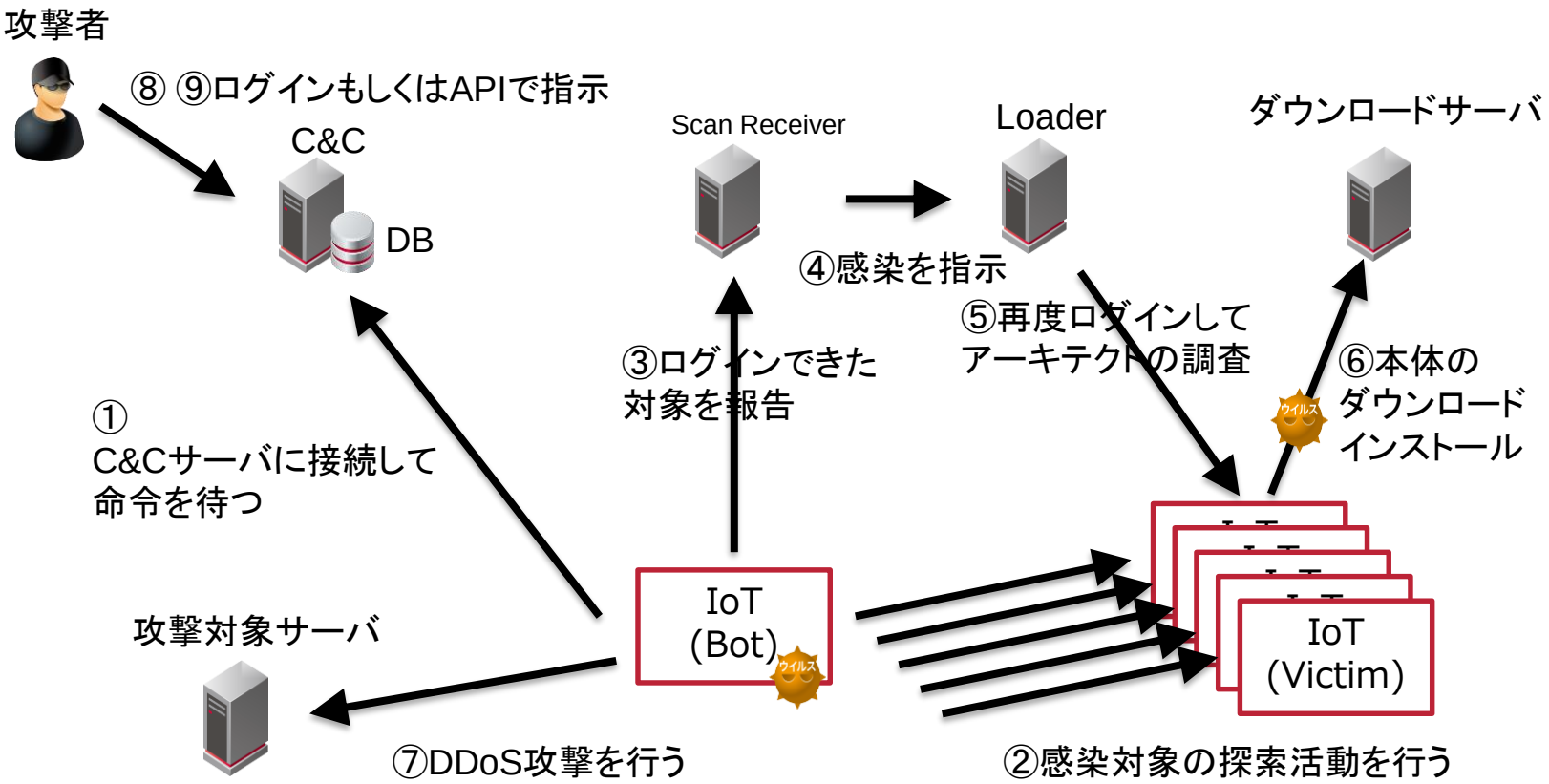
図-12 SYN/ACK リフレクション攻撃

https://wizsafe.iij.ad.jp/2018/10/470/

DDoS攻撃について

IoT ボット: Mirai ボットについて

※詳細はIIR Vol33 (2016年12月上旬公開)にて紹介



DDoS攻撃について

DDoS攻撃の状況の変化(2016年～)

- IoTボットなどの大規模ボットネットが一夜にして構成される。
- IoT機器への脆弱性対策の仕組みなどが醸成されていない。
  - Logitec製ルータ３３万台の脆弱性対策に２年以上かかった。
- 1Tbpsを越えるDDoS攻撃がIoTボットによって引き起こされている。
- 東京オリンピックなど大規模イベントを見据えたサイバー攻撃対策の強化が必要。

- 今起こっている事案に即応できる仕組みが必要である。

DDoS攻撃について

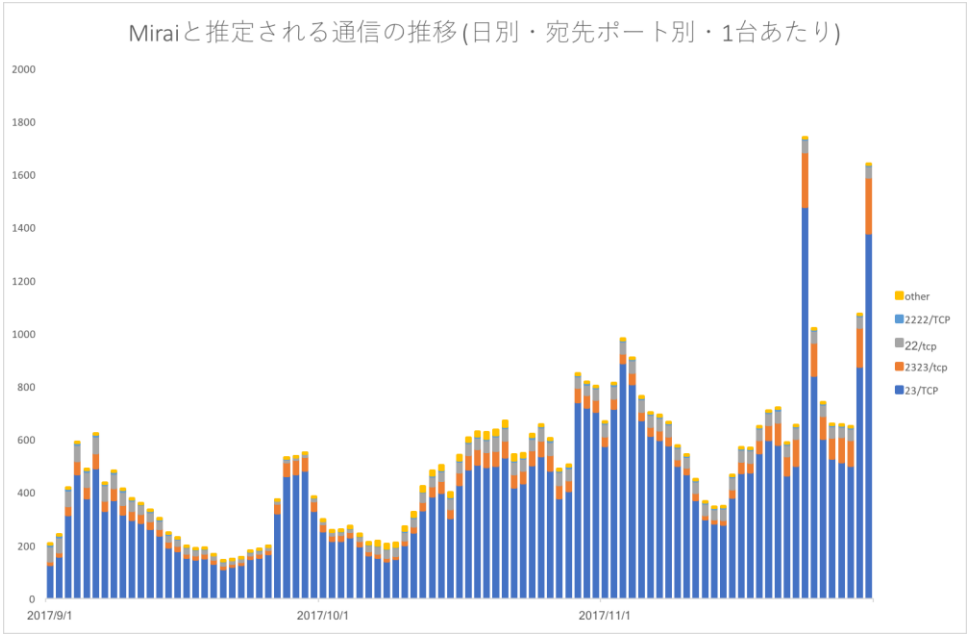
安全をあたりまえに wizSafe

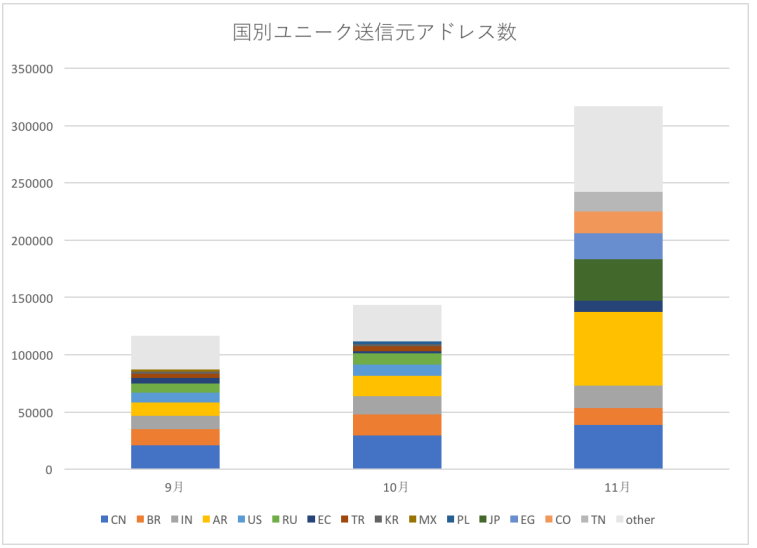
状況の変化
11月におけるMirai亜種感染の拡大

- ICT-ISAC DoS即応WGのMLにて
  - 11/7 NICTからMirai Botの特長を持つ通信の増加の報告と問合わせ
    - 11月に入ってから急増、国内16,000台
    - コネクトバックしてもセッションが確立しない
    - ケーブルテレビなどで多い
  - 11/7 IIJから観測情報をもとに呼応
    - satori/okiru系Miraiの亜種による
    - IIJ観測では12,000、海外数十万台
    - 検体解析結果の共有（対応アーキテクチャ、C&Cサーバ等）
  - いくつかの会員からIPアドレス提供依頼、調査

DDoS攻撃について

11月におけるMirai亜種感染の拡大(2)





国内における Mirai 亜種の感染急増 (2017年11月の観測状況) https://sect.iij.ad.jp/d/2017/12/074702.html

DDoS攻撃について

状況の変化
Mirai亜種感染への対応

- 2017/12/06 答え合わせ会（ICT-ISAC Japan DoS即応WG）
  - 会員から
    - ロジテックが多いのでは？
  - IIJから
    - 11/1の波、11/16日の波、悪用された脆弱性などの様子
    - 感染活動を組み込んだボットと、オリジナルMiraiのように分離している場合
    - ボットに組み込まれた感染活動（上の両者のどちらか）と、関連脆弱性をスキャンしているだけの活動
    - Huaweiを対象とした別の亜種もある
  - NiCTから
    - 脆弱性スキャンのボットへの組み込みの話題
    - 国別の話題 netlab.360のブログ（アルゼンチンが増えたといいながら日本が多い）
    - Huaweiの脆弱性スキャンについて、0-day攻撃だった
  - JPCERT/CCから
    - もともとインシデントにロジテックルータ関係する場合が増えているとの認識
    - 独自観測システムの観測情報による日本の感染活動の特長
    - ロジテックと話している。少なくとも4機種以上が対象。
    - SHODANの情報からわかること。

DDoS攻撃について

安全をあたりまえに wizSafe

状況の変化
Mirai亜種感染への対応（２）

- 2017/12/19注意喚起
  - JPCERT/CC
    - Mirai 亜種の感染活動に関する注意喚起
    - https://www.jpcert.or.jp/at/2017/at170049.html
  - NICT
    - NICTER 観測レポートルータ製品の脆弱性を悪用して感染を広げるMiraiの亜種に関する活動(2017-12-19)
    - http://www.nicter.jp/report/2017-01_mirai_52869_37215.pdf
    - Realtek社脆弱性の記載。
  - IIJ
    - wizSafeSecuritySignal Mirai亜種の感染拡大に伴う注意喚起
    - https://wizsafe.iij.ad.jp/2017/12/175/
  - ロジテック製 300Mbps 無線LAN ブロードバンドルータおよびセットモデル (全11モデル)に関する重要なお知らせとお願い
    - http://www.logitec.co.jp/info/2017/1219.html

DDoS攻撃について

- 電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律

電気通信事業法の一部改正について

4

- サイバー攻撃を行う**マルウェア**※**感染機器**やそれらに**指令を出すサーバへの対処を促進**するため、**第三者機関**を中心として**通信事業者が必要な情報共有をする**ための制度を整備。

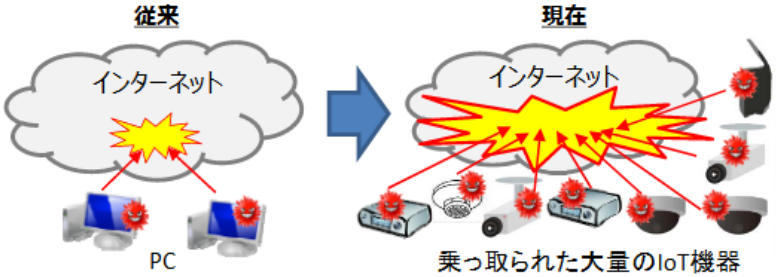
※悪意あるソフトウェアの総称であり、コンピュータに感染することによって、サイバー攻撃などの遠隔操作を自動的に実行するプログラムのこと。

現　状

インターネットの障害の深刻化

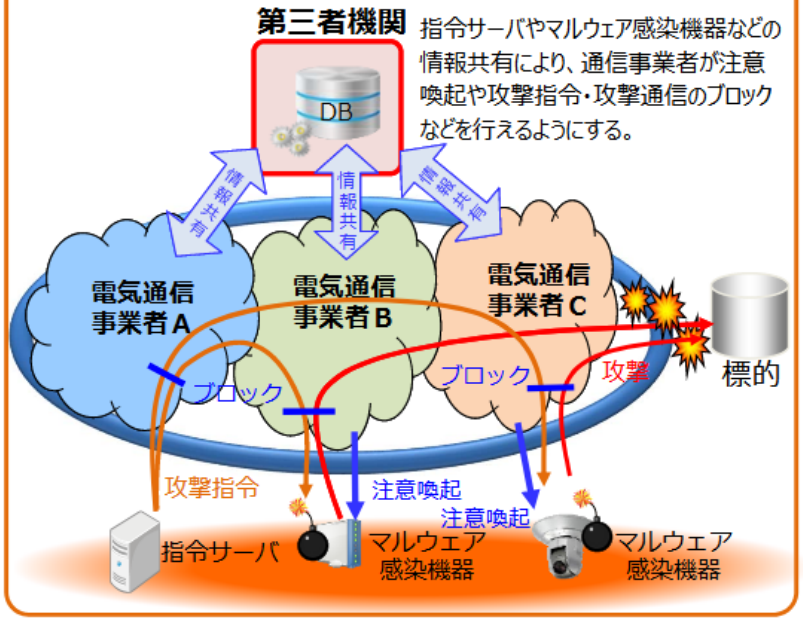
- サイバー攻撃によるインターネットの障害が発生し、国民生活や社会経済活動に影響
- 増加するIoT機器※を悪用したサイバー攻撃によりインターネットに重大な障害が発生
- 2020年の東京オリンピック・パラリンピック競技大会に際して、日本に対する大規模なサイバー攻撃の発生の懸念

※インターネットに接続される家庭用機器や業務用センサーなどの機器



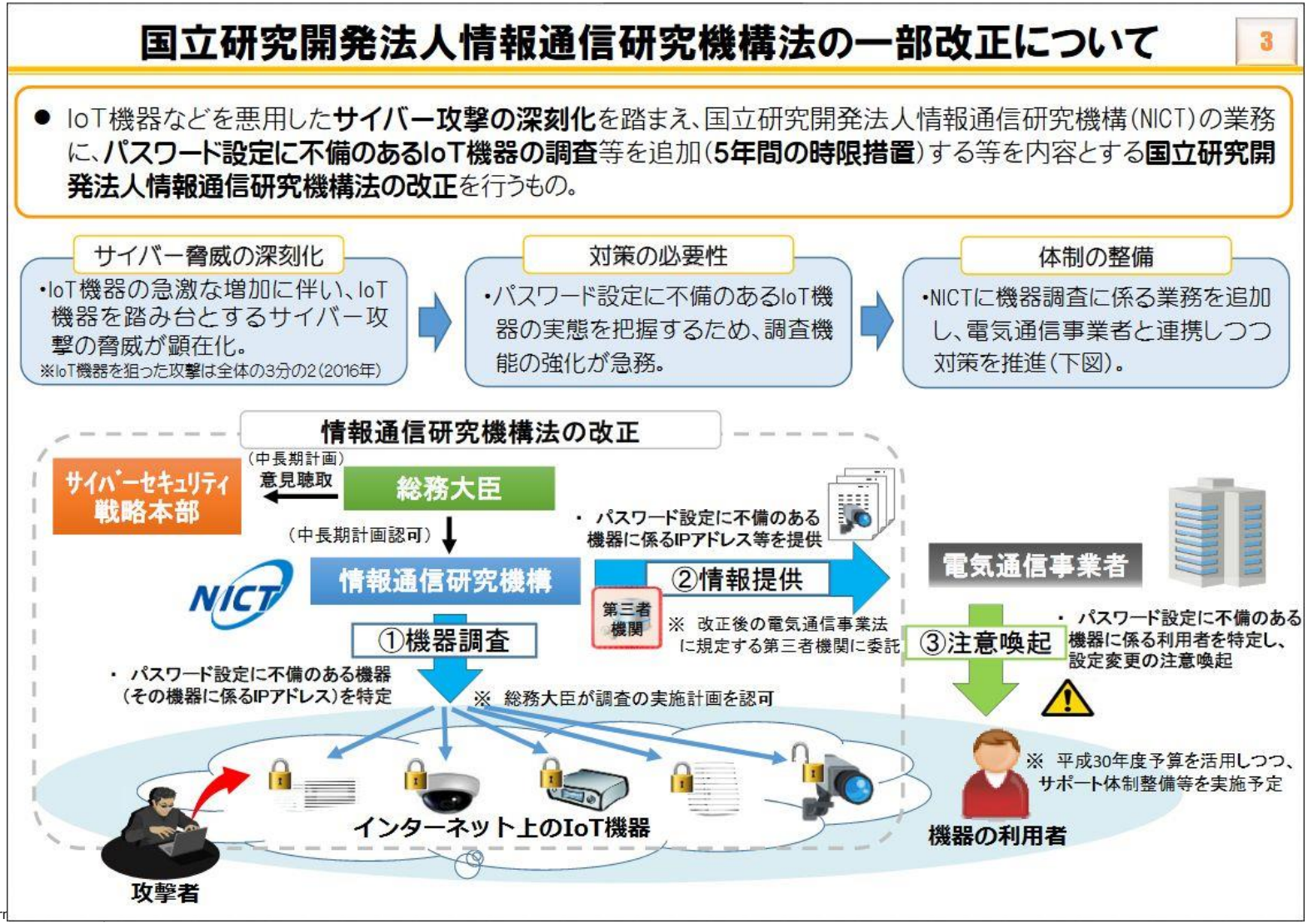
制度整備（イメージ）

第三者機関を中心とした情報共有基盤の構築



DDoS攻撃について

- 電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律



wizSafe

安全をあたりまえに