IIJ Internet Initiative Japan

セキュリティ動向2017

2017/11/08
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

安全をあたりまえに
wizSafe

Agenda

マルウェアの活動
IoTボットの活動
DDoS攻撃とその対策
脆弱性対応の宿題

セキュリティに関する
IIJの取り組み

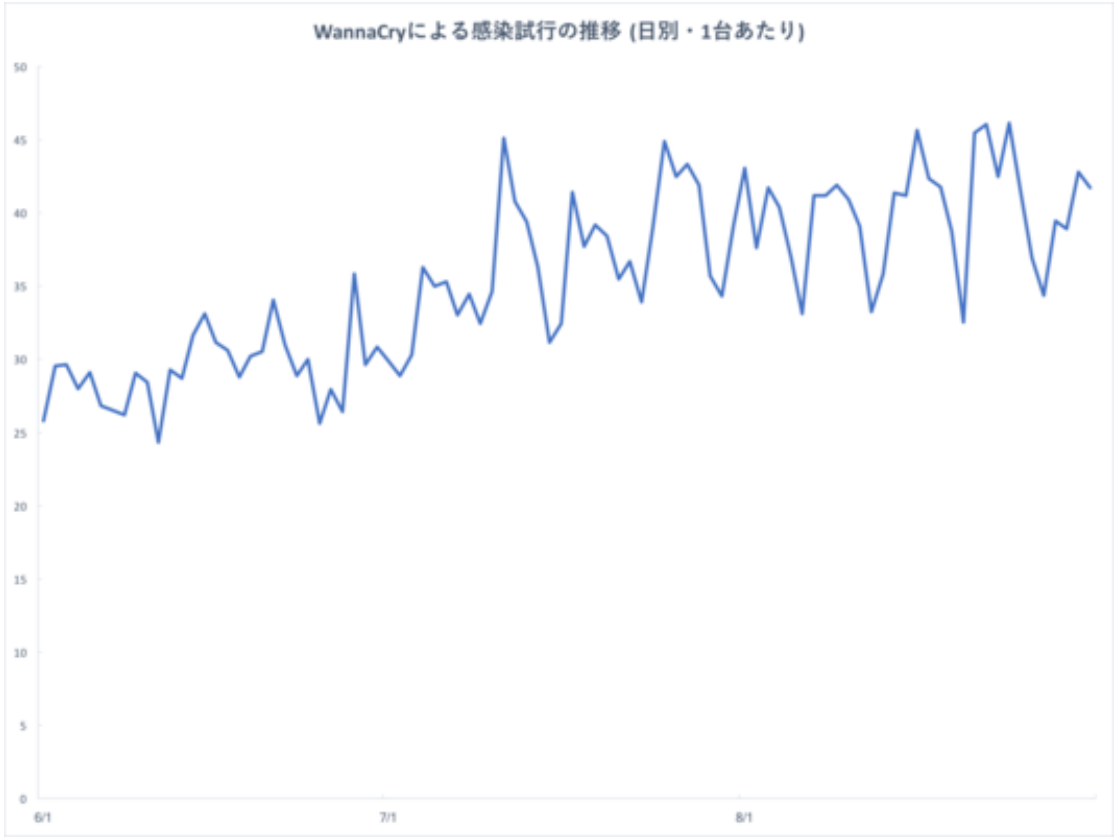
マルウェアの活動

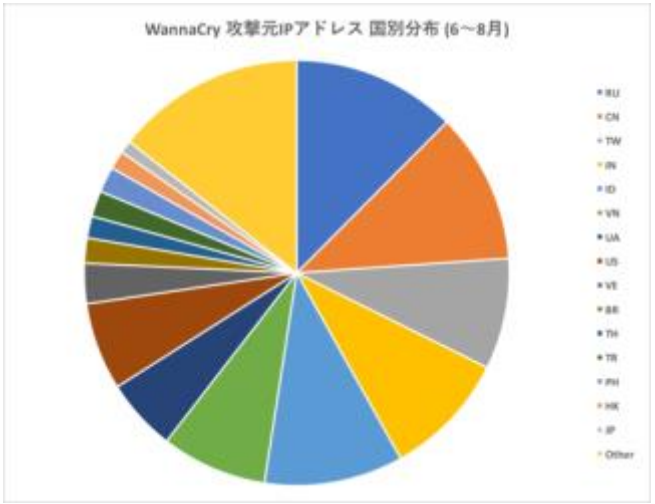
Wannacry

http://blog.trendmicro.co.jp/archives/15925yup

- HDDを暗号化して身代金を要求するランサムウェア。
- 5/12日頃より世界各国に感染を広げる、国内では大手企業で感染の報告。
- 3月のMSのパッチに含まれていたSMBv1の脆弱性を利用し感染を広げる。
  - 組織内ネットワークでの急速な感染。
- キルスイッチの存在。

Wannacry　(ワームとしての活動)

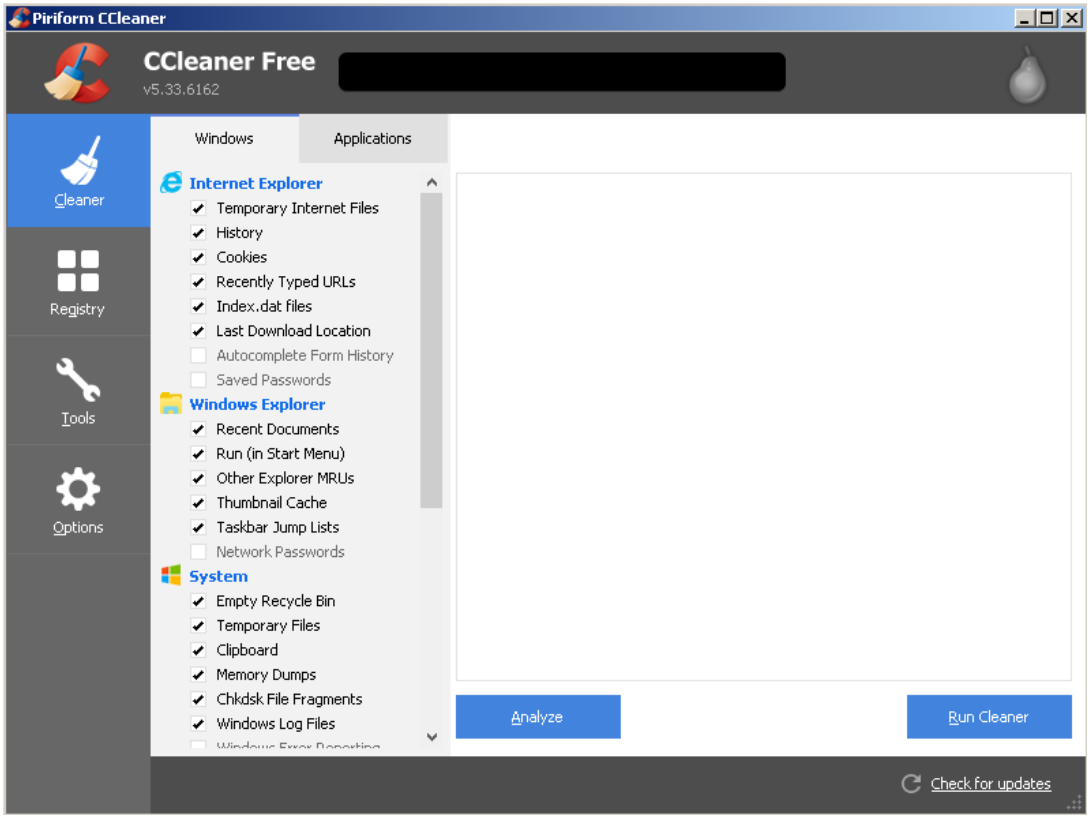




https://sect.iij.ad.jp/d/2017/09/192258.html

- IIJでは6月以降、ハニーポットでWannacryの亜種を観測しており、現在も活動が継続。
  - オリジナルと同じ脆弱性を利用、キルスイッチ機能が無効化。
  - 暗号化機能は動作せず感染を広げるのみ。
- 今年はPetya,NotPetya,BadRabbit等、破壊的な活動を行ったり、ワーム的な感染活動を行ったり、純粋なランサムウェアと呼ぶには微妙な活動が多い。

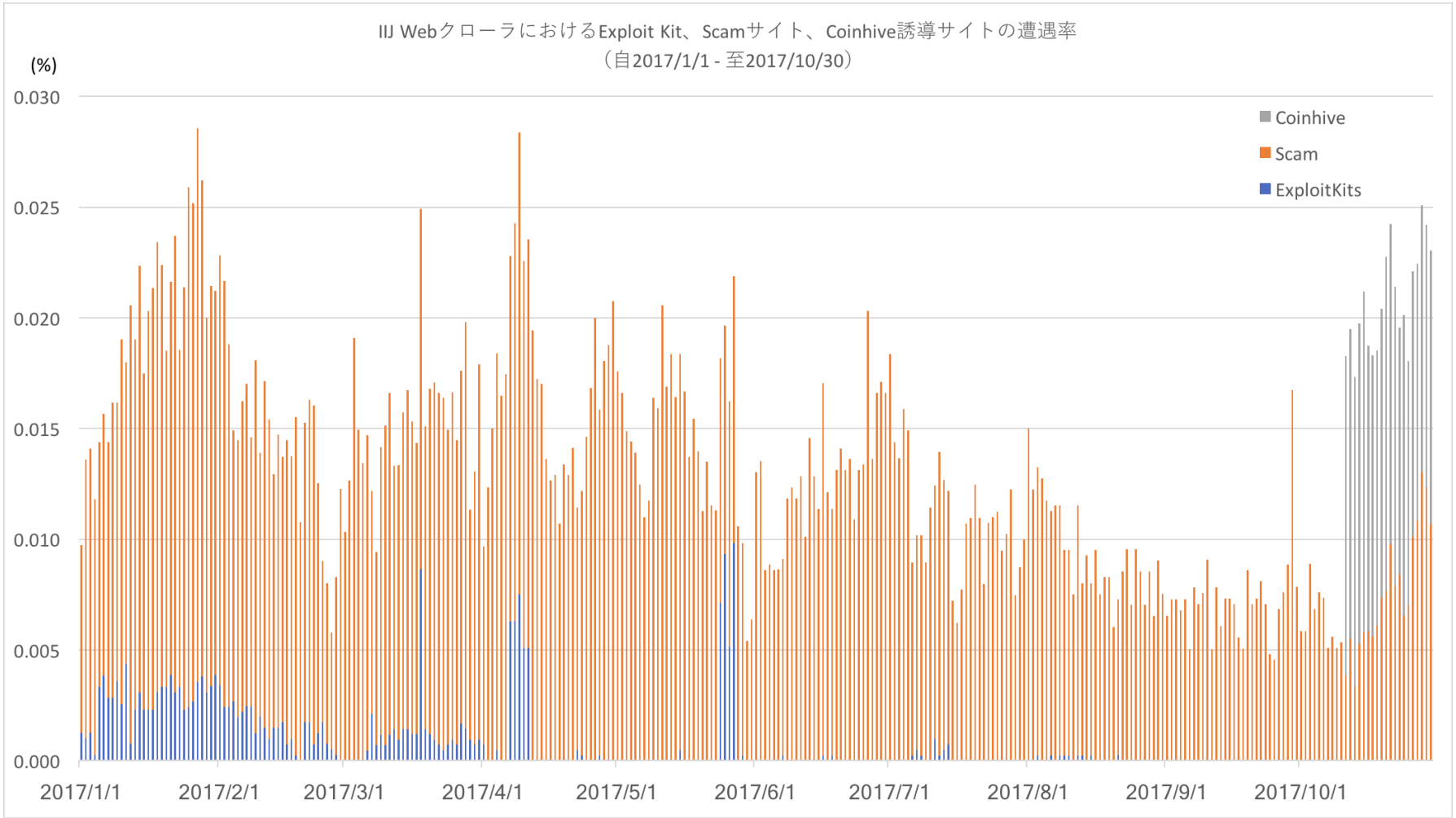
正当なソフトウェアへのマルウェアの混入



http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html

- Avast社傘下のPiriform社が作成しているシステムメンテナンスツールであるCCleaner及びCcleaner Cloudにマルウェアが混入。
- コンピュータ名、インストールソフト一覧などの情報が外部に送信される。
- 特定の企業内で感染した場合のみ新たなマルウェアをダウンロードして実行。

Web ExploitKitsによる感染活動の終焉



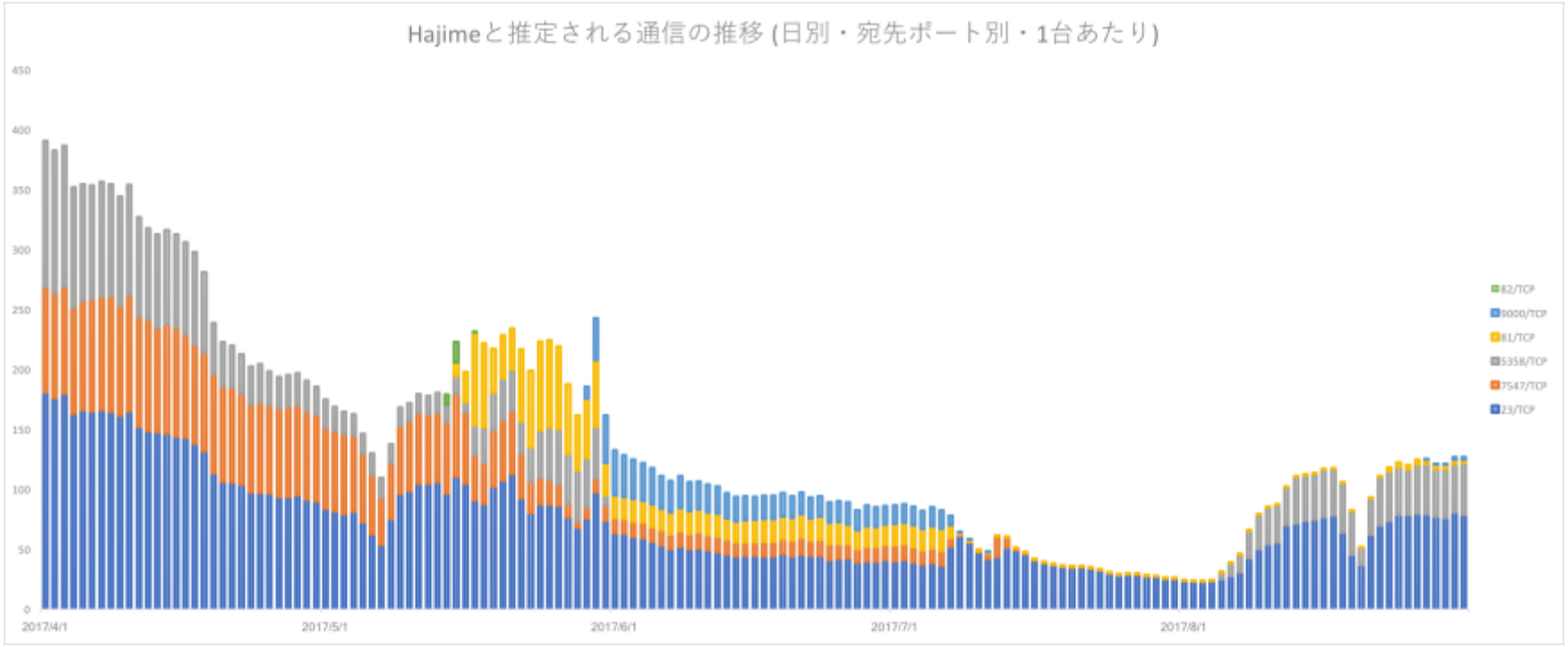
- ExploitKitsを使ってブラウザにマルウェアを感染させようとする試みの減少。
  - 悪用可能な脆弱性が減ったことに起因。
- Support Scamなど詐欺行為で不要なソフトウェアをインストールさせる行為に移行。
- 他の勢力として Coinhive（仮想通貨の掘削を行わせる行為）が登場。

IoT Botの活動

IoT機器を狙ったマルウェア

- 監視カメラ、ルーター、DVRなどのIoT機器に感染。
- デフォルトで設定されているユーザID/パスワードを利用してログインし感染。
- 感染後に命令を受け、標的へDDoS攻撃を行うものも。

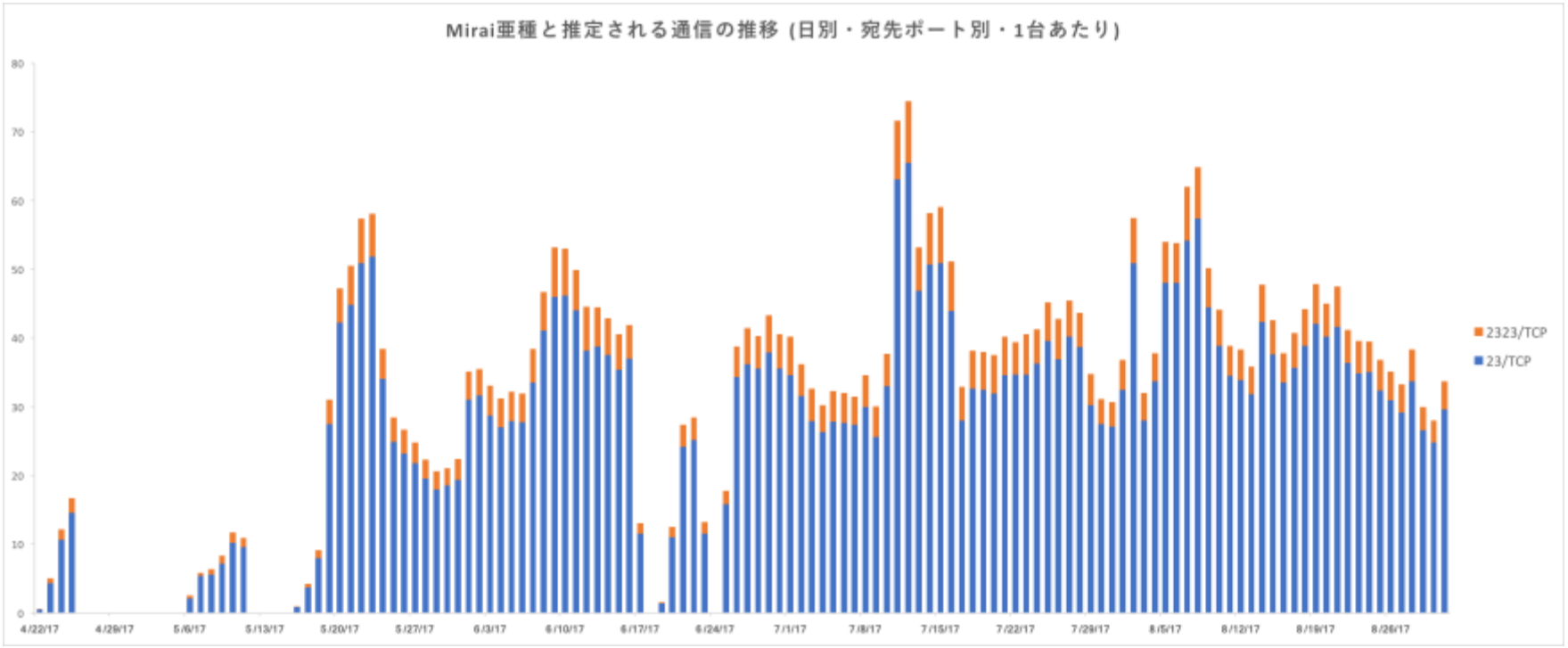
Hajime



https://sect.iij.ad.jp/d/2017/09/072602.html

- 2016年10月に最初に報告され、2017年に入ってから感染活動が活発化。
- Dos攻撃などは行わず感染活動のみを行う。
- 時期によりスキャンするポートが変化、23/tcp及び5358/tcpによる感染活動が現在は多い。

Mirai



https://sect.iij.ad.jp/d/2017/09/145930.html

- Miraiの亜種が出現。ソースコードが公開されたため同じ特徴を持つものが多いが、一致しない亜種の活動も活発化。
- 8月末時点で4万台程度がこのMirai亜種に感染していると推測。現在も活動は活発。
- その他11/1 からSatori/Okiru系ボットの活動が活性化。国内十万台規模。

Mirai の感染事例

- DDoS攻撃事案
  - 複数のアドレスからDDoS攻撃を受けたと苦情。
  - 利用者はすべて特定の企業（メーカ）。
  - 当該メーカの作成したIoTデバイスが、IoTボットに感染。
  - SIMを搭載したモバイル接続、全国で稼働していながら常時移動していることが判明。
- 対策
  - 幸いIoTボットの多くは電源断で消失する。
  - ISPはモバイル接続でフィルタリングをオファー（契約形態の変更）。
  - メーカにて自社作業による対策とISPのオファーを比べて対策検討、フィルタリングを採用。

- こういう装置が他にどのくらいの種類あるのか?

安全をあたりまえに
wizSafe

DDoS攻撃とその対策

DDoS攻撃の状況

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

In past, we launched one of the largest attacks in Switzerland's history. Use Google.

All network of [redacted] will be DDoS-ed starting [redacted]. if you don't pay 10 Bitcoins @ [redacted]

When we say all, we mean all - users will not be able to use any of your services.

Right now we will start 15 minutes attack on one of your IPs ([redacted]). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by [redacted], attack will start, price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long
time.

This is not a joke.

Our attacks are extremely powerful - our Mirai botnet can reach over 1 Tbps per second. So, no protection will help.

Prevent it all with just 10 BTC @ [redacted]

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

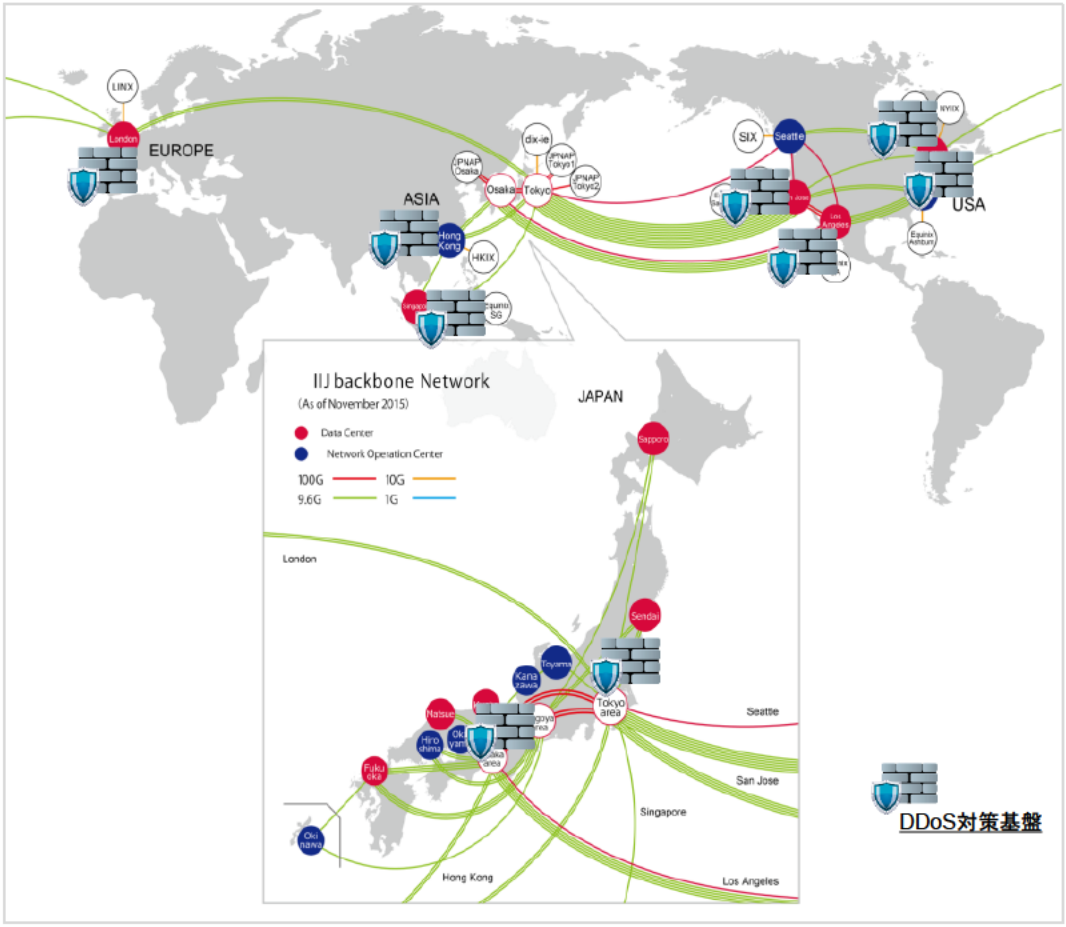
https://www.jpcert.or.jp/newsflash/2017062901.html

- DDoS恐喝事案やAnonymousによる攻撃、2チャンネル関連の攻撃が散発。
- 9月には、約20社の仮想通貨及びFX業者にDDoS攻撃が仕掛けられ、いくつかの会社には脅迫メールが届いたとの報告あり。
- 攻撃者の意図は、推測ではあるが、取引所間での価格差を人為的に生み出して裁定取引で利ざやを得る、あるいは不利益を被ったものの逆恨みなどの可能性が考えられる。

DDoS攻撃への対策（IIJ DDoSプロテクションサービス）

安全をあたりまえに wizSafe

- 網の中に対策装置を設置した場所がある状態から、網の出入り口すべてに対策装置がある状態へ。



安全をあたりまえに
wizSafe

脆弱性対応の宿題

脆弱性対応の宿題

- Bluetooth 脆弱性 BlueBorne
  - https://www.armis.com/blueborne/
  - Bluetooth接続した機器を制御することができる。
  - Android、Linux、iOS、Windowsのパッチはリリースされたが、あてていますか？
  - ペアリングする相手がパッチを当てているか確認できますか？
- WPA2の脆弱性KRACK
  - クライアント側パッチはリリースされたが、あてましたか？
  - 攻撃するためには無線が届く範囲にいる必要がある。
  - 特定のセッションに中間者（MITM）攻撃される(暗号鍵が盗まれるわけではない)。
  - 公衆無線LANなどで攻撃されている人がいるリスクは何でしょう？
- Infineon TechnologiesRSA ライブラリ
  - 鍵生成時のエントロピー不足。
  - エストニア e-residency ICカード。PCのTPMにも影響。
- Intel ATOM C2000エラッタ
  - ネットワーク機器などに影響の可能性。
  - https://www-ssl.intel.com/content/dam/www/public/us/en/documents/specification-updates/atom-c2000-family-spec-update.pdf
  - https://www.iad.gov/iad/library/ia-advisories-alerts/devices-with-intel-atom-c2000-series-processors.cfm

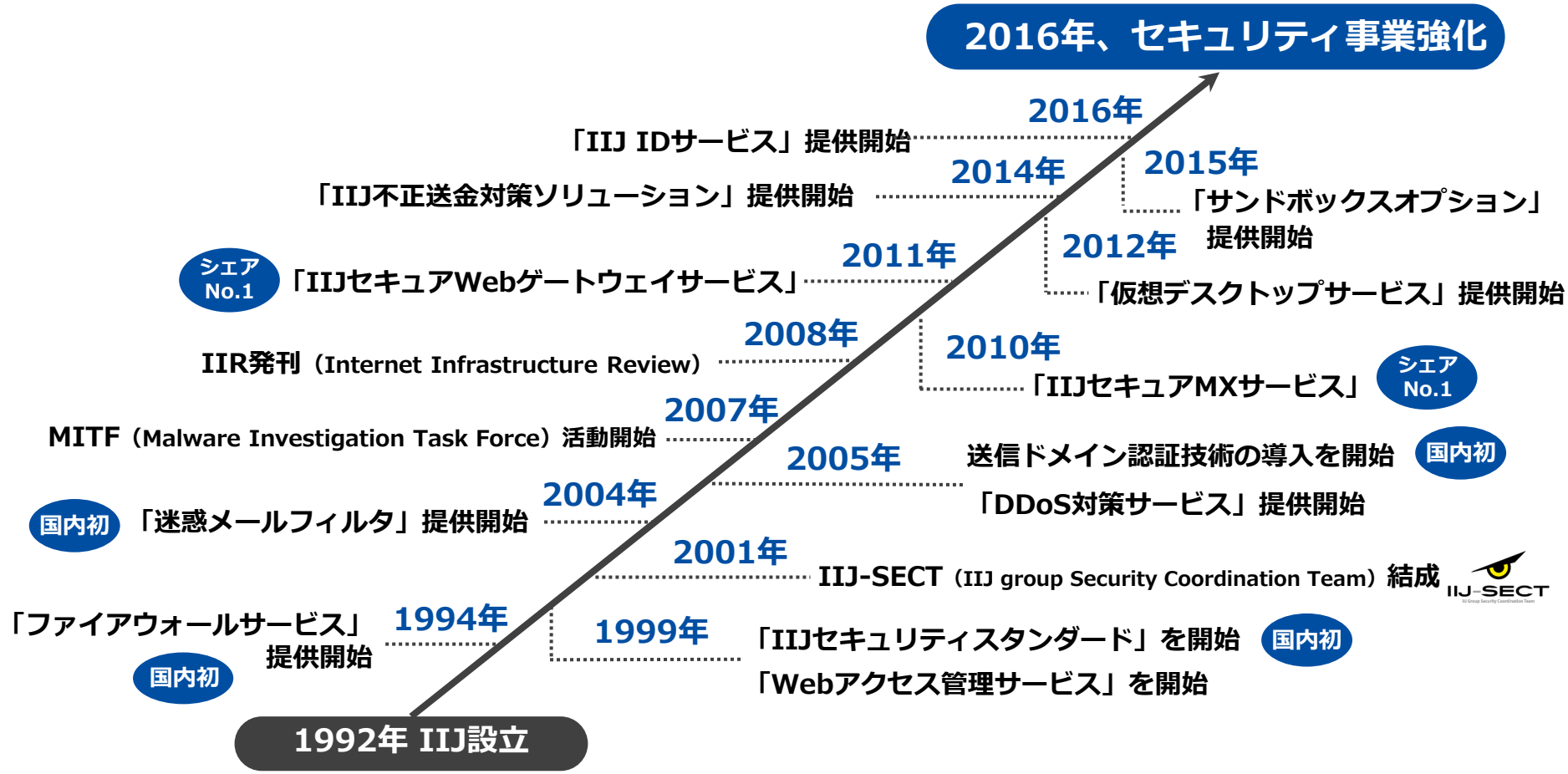
安全をあたりまえに
wizSafe

セキュリティに関する
IIJの取り組み

IIJセキュリティ事業の沿革

安全をあたりまえに wizSafe

1992年、IIJは国内初のISPとして創業。セキュリティに関しても技術面を中心にイニシアティブを取り続けてきました。



IIJセキュリティ事業の強化

より高度なセキュリティオペレーションを提供するために、「人材」「システム」「体制・設備」を強化しました。

wizSafe
安全をあたりまえに

1. 人材

・人材育成

2. システム

・情報分析基盤の刷新

3. 体制・設備

・セキュリティ本部
・オペレーションセンター

人材育成

社内はもとより社外においても、セキュリティに関して高い技術力、知識をもった人材の育成活動に力を入れています。

IIJ社内における セキュリティアナリストの育成

セキュリティ人材育成への貢献

役割と教育カリキュラム

日々進化する脅威に対抗するために練られたチーム編成と他部門との連携、それらを支える人材は、セキュリティだけではなく幅広い知識を身に付けます。

“IIJ C-SOCサービス”チーム

“セキュリティ、マルウェア、ビッグデータセキュリティ、フォレンジック”の各アナリスト、インシデントハンドラーなど

“アカウント対応（個別構築した案件担当）”チーム

アカウントエンジニア、セキュリティリサーチャーなど

“SOCインフラ”チーム

“ネットワーク、インフラ、ビッグデータ”の各エンジニアなど

“サービス運用”部門

サービス運用のスペシャリスト

“セキュリティリサーチ”部門

マルウェア解析、暗号などの調査・研究を行うスペシャリスト

教育カリキュラムの一例

- サーバの基礎知識 (Server Basics)
- ネットワークの基礎知識 (Network Basics)
- Webアプリの基礎知識 (WebApplication Basics)
- コンピュータに対する攻撃の基礎知識 (Exploit Basics)
- ネットワーク経由での攻撃の基礎知識 (Network Attack Basics)
- Webアプリに対する攻撃の基礎知識 (WebApplication Attack Basics)
- ログ分析 (Log Analysis)
- パケット分析 (Packet Analysis)
- マルウェアの動的解析 (Malware Dynamic Program Analysis)

情報分析基盤の刷新

膨大な情報の分析から、セキュリティインテリジェンスを生成。

ISPだからこそ得られる情報

・バックボーントラフィック
・DNSクエリ　　etc

IIJセキュリティサービスの情報

・ファイアウォール
・IPS/IDS
・メール
・DDoS対策　　etc

IIJ独自調査/研究で得られた情報

・独自の調査で得られた情報
・研究で得られた情報 etc

公開情報

・ホワイトペーパー
・脅威/事故事例 etc

ビッグデータ解析

- リアルタイム脅威検知
- 最新の攻撃に対する研究

情報分析基盤

情報参照

SOC
セキュリティ
アナリストチーム

セキュリティインテリジェンス

C&Cサーバなど攻撃元の
レピュテーション情報

攻撃者プロフィールや手法等
将来の攻撃に備えるための指針となる情報

対策実装に必要とされる
脅威情報や攻撃トレンド

広く安全を実現するための
脅威情報の公開と提供

ISPならではの膨大な量の情報ソース

膨大なセキュリティ機器のログやバックボーントラフィック、DNSクエリなどに、外部情報を加え、ビッグデータ解析を行っています。


トラフィック/DNS


ファイアウォール


Web


メール


DDoS対策


アンチウイルス


サンドボックス


IPS/IDS

900億行/月
のWebアクセスログ

38億行/月
のメールアクセスログ

1,700億行/月
のセキュリティ機器ログ

40万サイト以上/日
のWebクローラ調査サイト数

情報分析基盤

Mailゲートウェイ

SecureMX

約 **172万** アカウント

Webゲートウェイ

Secure Web Gateway

約 **116万** アカウント

システム運用実績

IIJ GIO

サーバ数：約 **21,000**

監視ノード数：約 **48,000**

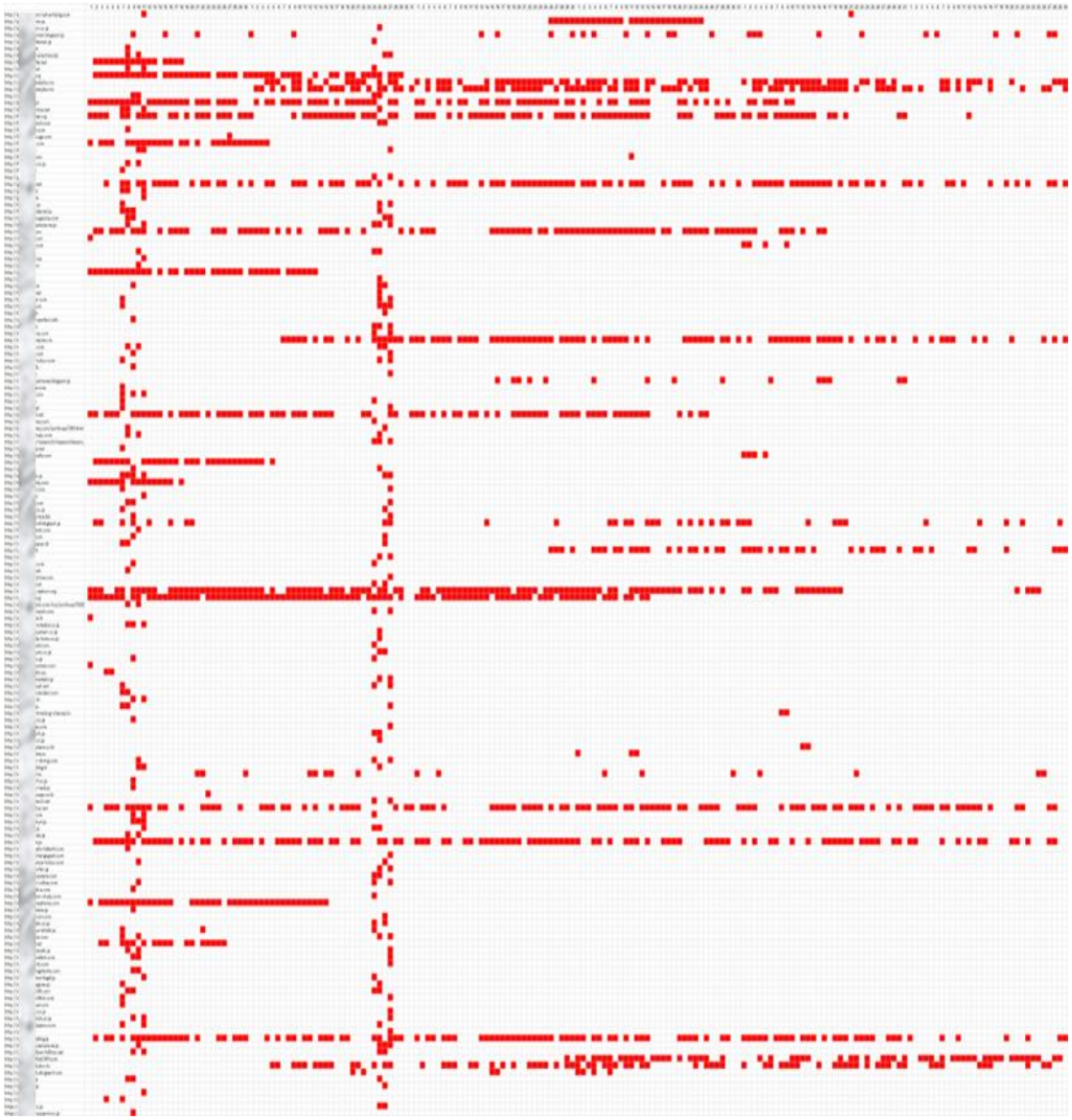
【形を変えながら運用を続け21年。IIJのシステム運用実績】

TbpsクラスのDDoS攻撃に対応する設備

地球を一周する日本最大級のバックボーン

*数字は2017年1月末時点の情報です

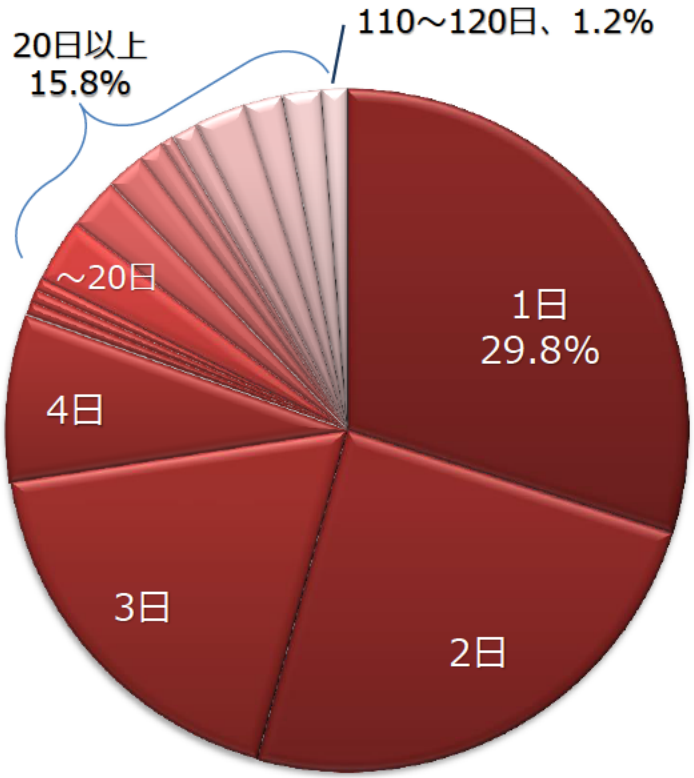
クライアントハニーポットによるWeb改ざん検出データ



- クライアントハニーポットによる(マルウェア配布悪用)Web改ざんの検出状況（IIJ調査結果 2017/4～9）
- 表の見方
  - 横軸：調査期間日
  - 縦軸：Webサイト名称
  - 表中：改ざん検出結果（赤色が検出）
- 赤色の横線：**マルウェア配布やScamの温床として継続**
- 赤色の縦線：キャンペーンによる複数サイトが改ざん

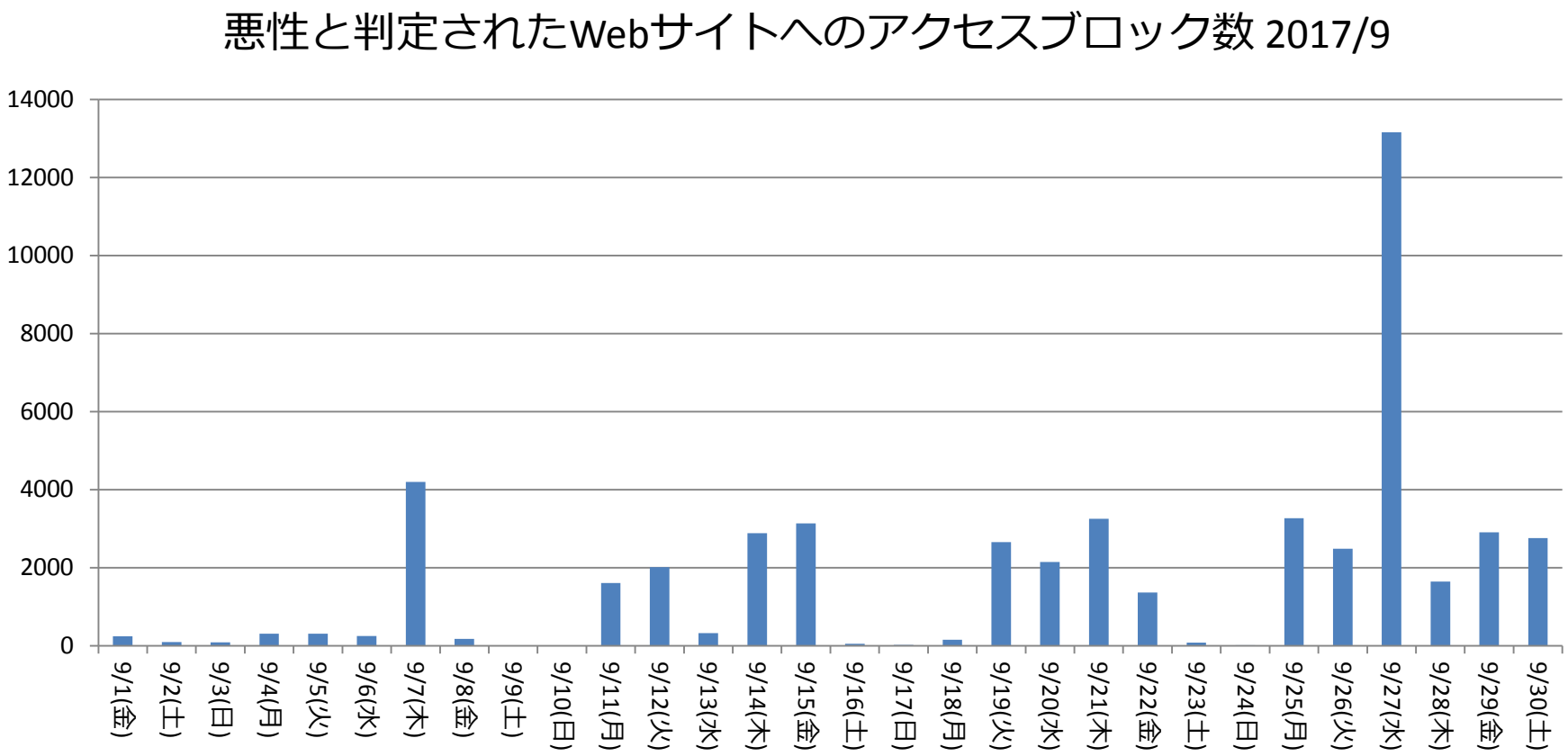
Web改ざんの検出頻度

- Web改ざんとして検出されたサイトのうち断続的に**２日以上検出されたWebサイトは7割以上**となった
- 調査期間中、断続的に**20日以上検出されたWebサイトは15.8%**になった
- １日しか検出されないWebサイトも29.8%存在した



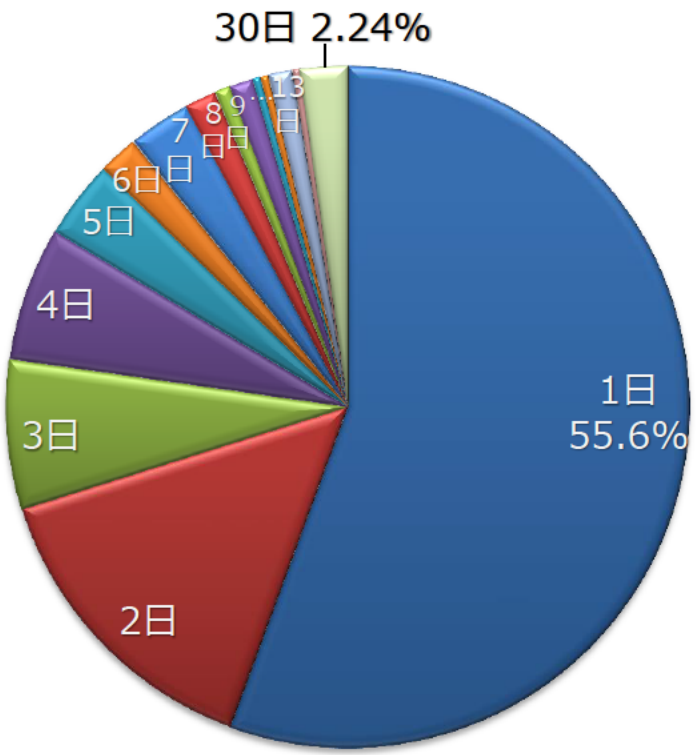
Web改ざん検出頻度（断続的日数）2017/4～9

IIJセキュアWebゲートウェイサービスでの脅威防御



- 悪性と判定されたWebサイトへのアクセスは実際に発生している
- 2017年9月のデータでは、多いときは10,000件を超えるアクセスを防御

Apache Struts 2を狙った攻撃元IPアドレス

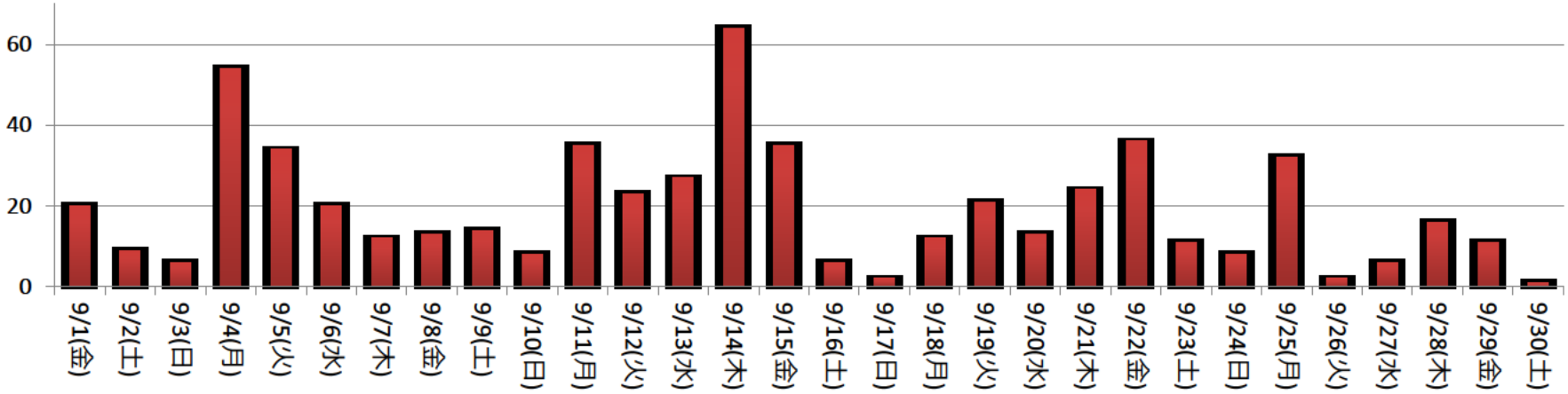


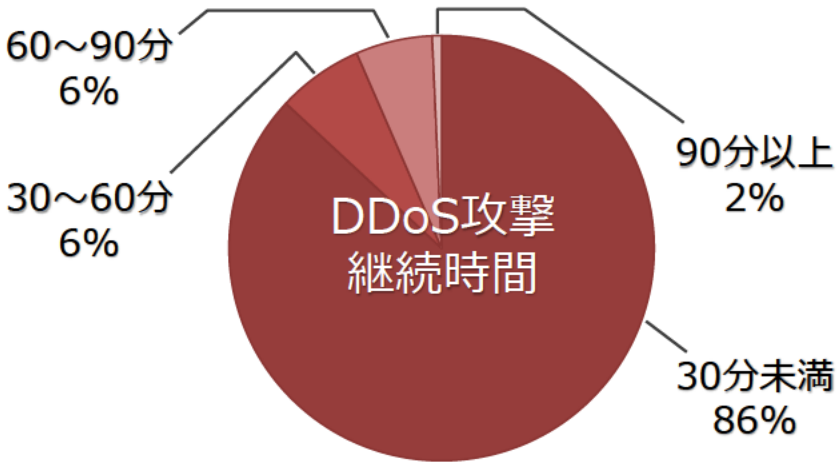
攻撃元IPアドレス出現頻度

- 2017年9月において、Apache Struts 2の脆弱性を悪用する攻撃の検出データから攻撃元IPアドレスの検出頻度割合を集計
- 同一の攻撃元IPアドレスから断続的に**2日～30日間継続した攻撃は全体の4割を超えていた**
- 攻撃を**30日間連続して継続していたIPアドレスが 2.24%**あった

※ これらのIPアドレスが攻撃以外の活動をしているかは不明

2017年9月のDDoS攻撃の状況

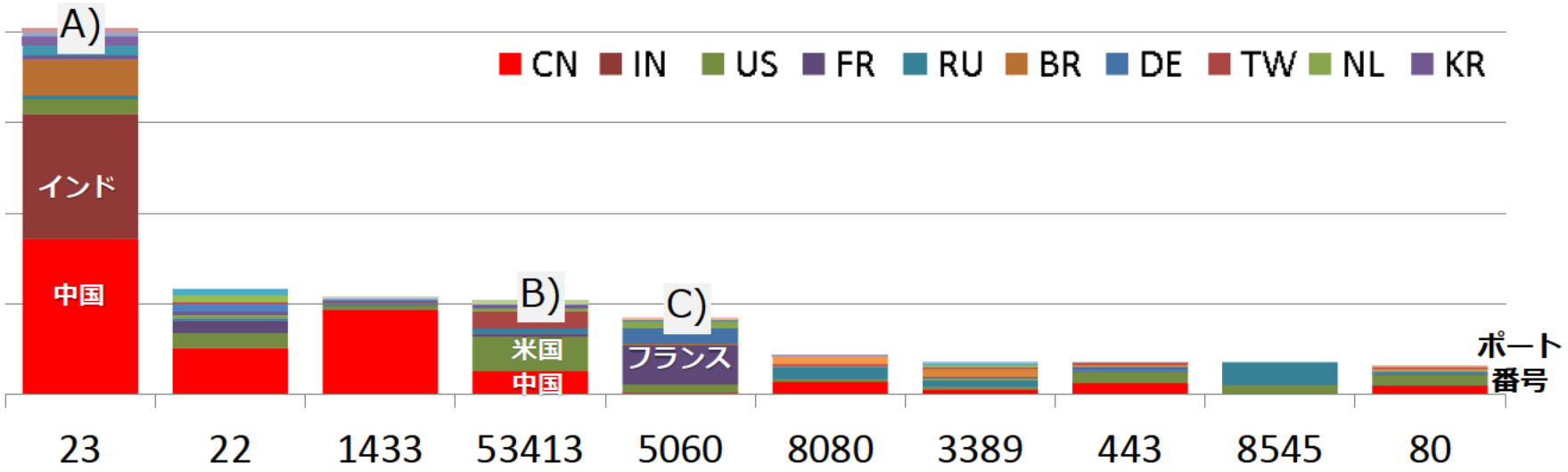




- 2017年9月の**DDoS攻撃検出件数 575件**
  1日あたり19.16件
- **最大攻撃規模 12.06Gbps**
- **30分以上継続する攻撃が14%**、最大継続時間 46時間57分
- DDoS攻撃が発生しやすい**9月18日前後**での発生件数は多くなかった

ボットが狙うポートの状況（2017年9月）

IIJマネージドサービスで観測したボットの不許可アクセス



A) IoTボットとして有名なMiraiのScan対象でもある23/TCPポートへの探査行為が最も多くなっている（多くは国外からであり、中国とインドが大半を占める）

B) 米国、中国からのアクセスが目立つ53413/UDPは、Netis製ルータの脆弱性を狙ったアクセスであると考えられる

C) 5060/UDPのアクセスがフランスから多く観測されており、SIPサーバー/機器を狙ったスキャン行為と考えられる

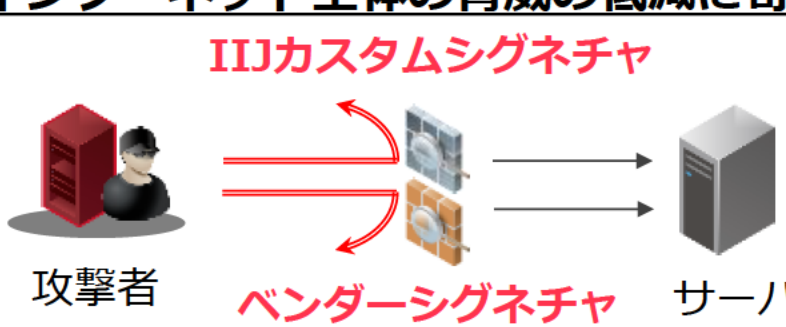
情報分析基盤の活用によるセキュリティ品質の向上

Apache Struts2脆弱性（CVE-2017-5638）での対応例。

- 脆弱性公開
- IIJカスタムシグネチャ緊急リリース
- Struts2攻撃情報解析（情報分析基盤）
- ベンダーシグネチャ公開
- ベンダーシグネチャ改善点発見と修正依頼
- ベンダーシグネチャ修正版リリース

IIJカスタムシグネチャによる防御と解析

インターネット全体の脅威の低減に寄与



情報分析基盤による解析で、適切なカスタムシグネチャを提供。
ベンダへの情報提供等、インターネット全体の脅威の低減に寄与。

“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 >

IIJ セキュリティオペレーションセンターの刷新

安全をあたりまえに wizSafe

業務に「集中」できる独立した作業スペースと高度化する脅威に対して「協調」し対処するため、専用に設計した設備です。

分離

マルウェアなどリスクの高い分析を行うために業務ネットワークから

独立したネットワーク環境

集中

より複雑化・高度化した脅威を監視し続け、分析を行うための

集中できる環境

保全

フォレンジックの分析結果やお預かりする証拠品保護のための

セキュリティゾーニング

協調

同時多発的なものや高度なインシデントに対処するための

コラボレーション促進

IIJ セキュリティオペレーションセンター　エントランス

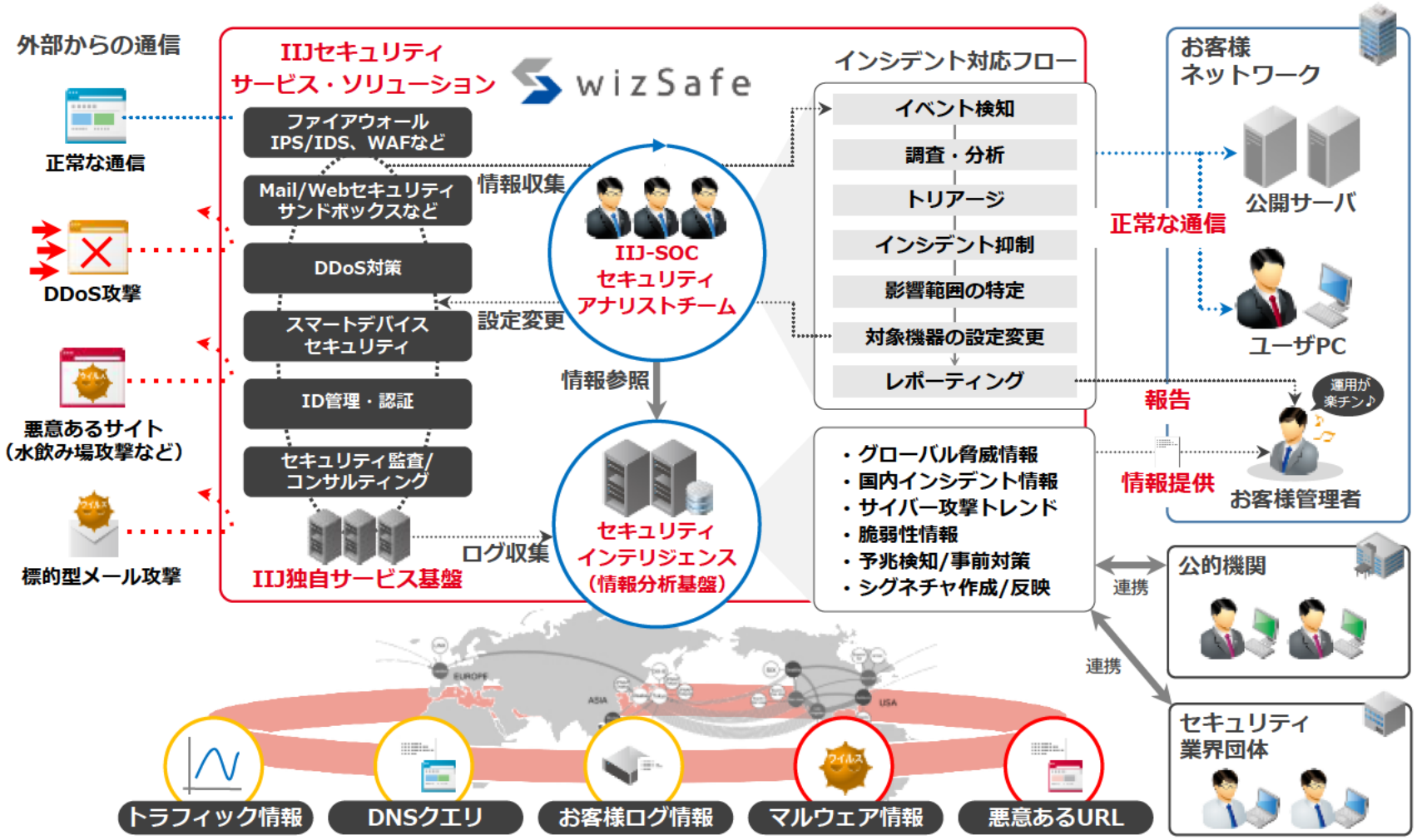
IIJ セキュリティオペレーションセンター　オペレーションルーム


IIJ セキュリティオペレーションセンター　セキュリティラボ

IIJ セキュリティ事業全体像

安全をあたりまえに wizSafe

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

安全をあたりまえに