資料１－４

最近のサ イバーセキュリティに おける脅威動向について

中尾　康二

ICT－ISAC　理事
KDDI　株式会社　顧問
（NICT、横浜国大）

本日のトピック

最近のセキュリティ脅威（攻撃）の紹介

1）これまでの脅威（ボットネット中心）

2）金融系マルウェア

3）APTによる脅威

4）IoTによる脅威

サイバーセキュリティ対策の方向性　ー　まとめ

最近のセキュリティ脅威（攻撃）の紹介

1）これまでの脅威（ボットネット中心）
2）金融系マルウェア
3）APTによる脅威
4）IoTによる脅威

サイバー攻撃の変遷

- 20世紀：愉快犯/自己顕示

Richard Skrenta
世界初のウイルスElk Cloner
の作者（当時高校生）

- 21世紀：経済犯

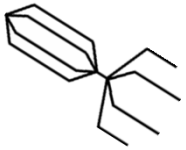
Anonymous

- 2010年代： 示威活動（Hacktivism）
  諜報活動（Cyber Espionage）

マルウェアの感染形態に着目した分類

●ウイルス（狭義のウイルス）

- ✓ 単体動作せず，自分自身を他のファイルやプログラムに寄生
- ✓ ブートセクタ感染型：ハードディスクなどのシステム領域に感染
- ✓ ファイル感染型：実行可能ファイルを主な感染対象



ウイルス

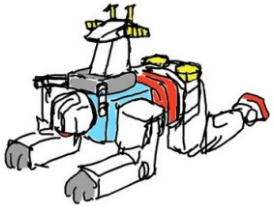
●ワーム

- ✓ 単体で動作し自己増殖を行う
- ✓ ウイルスに比べ高い感染力を有し，大規模感染を引き起こす
- ✓ 電子メールやリムーバブルメディア（USBメモリ等）を媒体とするもの
- ✓ Windowsのファイル共有やメッセージング機能を利用するもの
- ✓ OSやアプリケーションの脆弱性に対する攻撃コードを用いるもの

ワーム

●トロイの木馬

- ✓ 有用なプログラムやファイルに偽装
- ✓ ユーザ自身によるシステムへのインストールや起動を誘う
- ✓ 感染機能を持たないものが多い

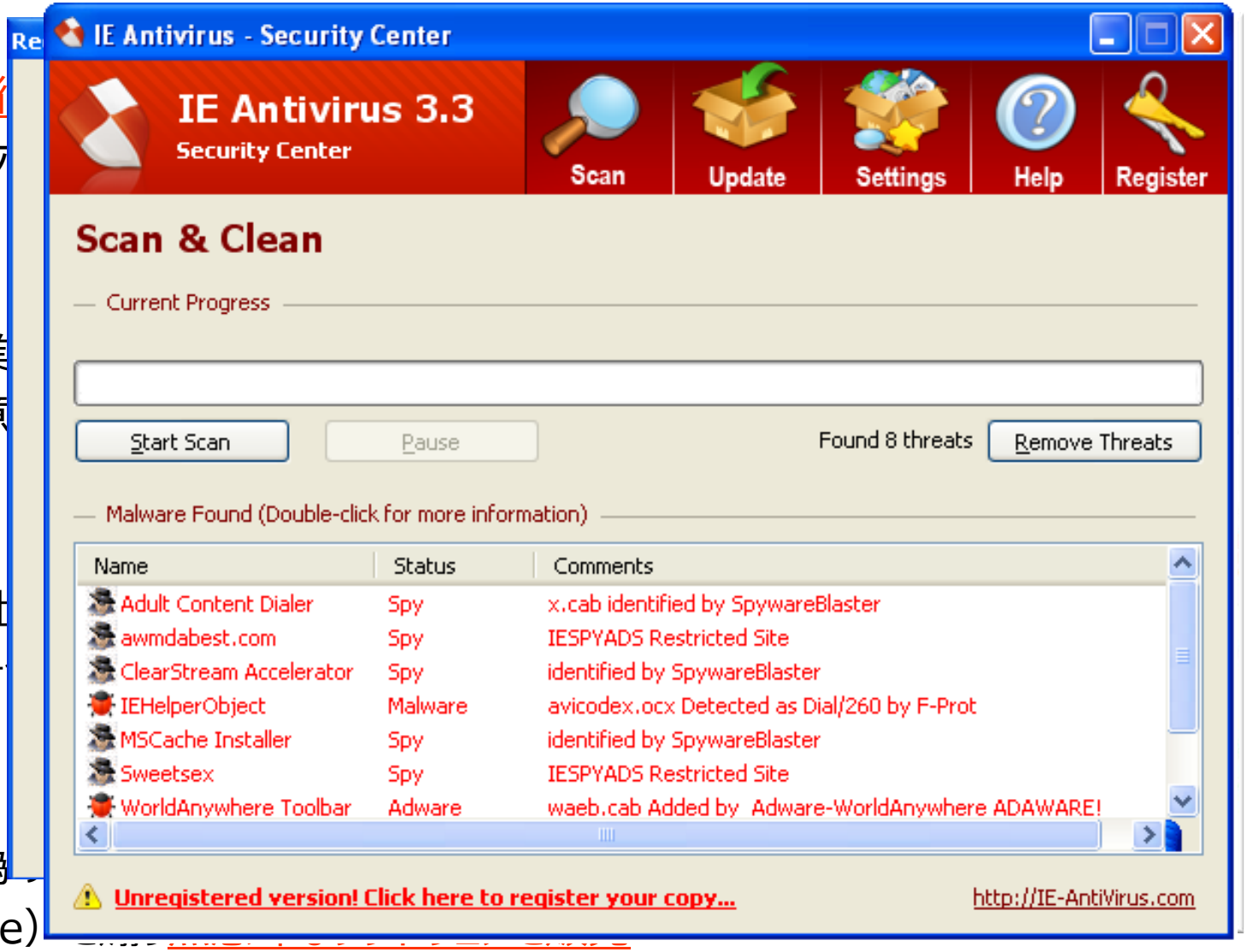


トロイの木馬

出典：GIZMODE Japan

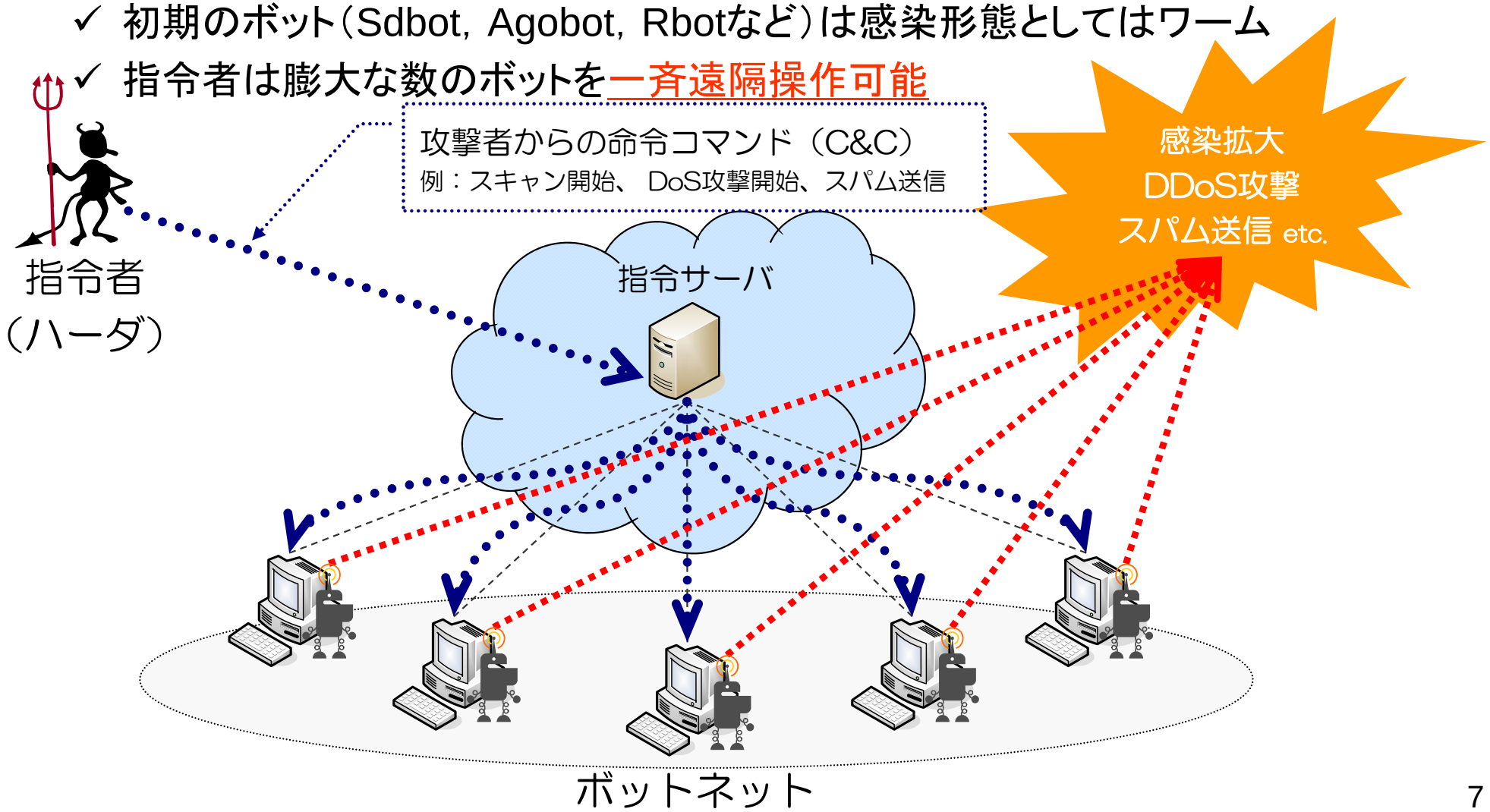
マルウェアの目的に着目した分類

- **スパイウェア**
  - ✓ 個人情報や行
  - ✓ ユーザのキー
- **アドウェア**
  - ✓ ユーザに企業
  - ✓ ユーザの同意
- **ランサムウェア**
  - ✓ ユーザのPC上
  - ✓ データの復号
- **スケアウェア**
  - ✓ ユーザに虚偽
  - ✓ 不安（scare）



単独攻撃から連携攻撃（ボットの出現）へ

- ✓ 指令者からの遠隔操作により多岐に渡る活動を行うマルウェア
- ✓ ボットネットと呼ばれるオーバレイネットワークを形成（数百～一千万台規模）
- ✓ 初期のボット（Sdbot，Agobot，Rbotなど）は感染形態としてはワーム
- ✓ 指令者は膨大な数のボットを一斉遠隔操作可能



ダークネットを用いて攻撃確認！

●ダークネット = 未使用IPアドレスブロック

✓パケットが飛んでくること自体おかしい

●ダークネットで見えるもの

✓インターネット上で何かを探す行為

- ワーム型マルウェアによるスキャン
- DRDoSのリフレクタ探索（DNS Open Resolver、NTP etc.）
- セキュリティ関連組織等による調査

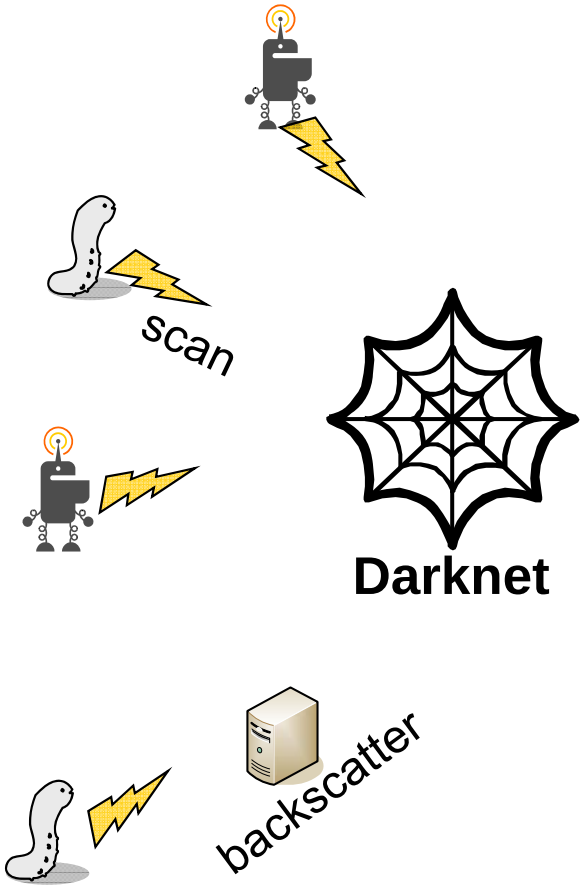
✓DoS攻撃の跳ね返り

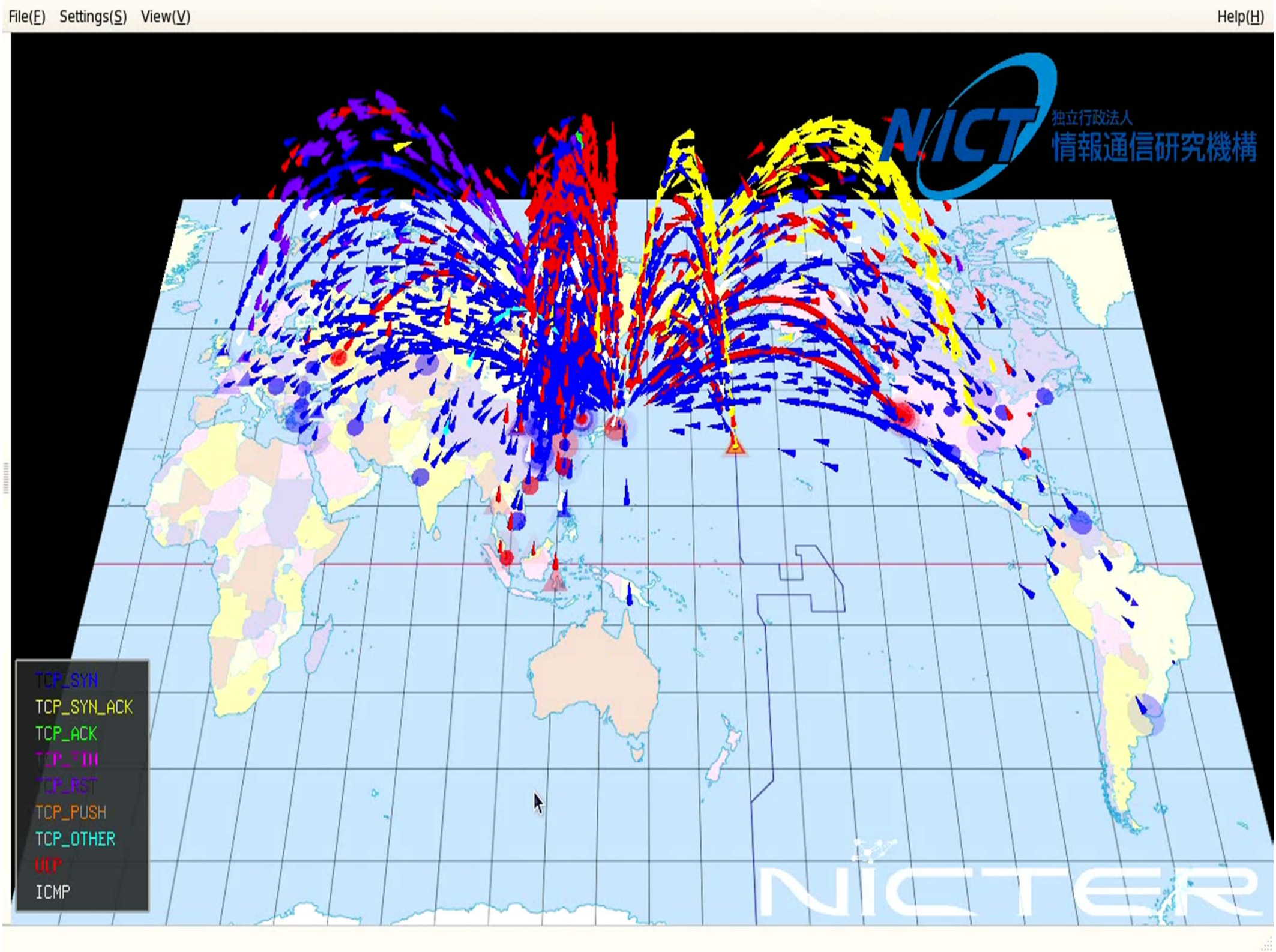
- DDoSバックスキャッタ

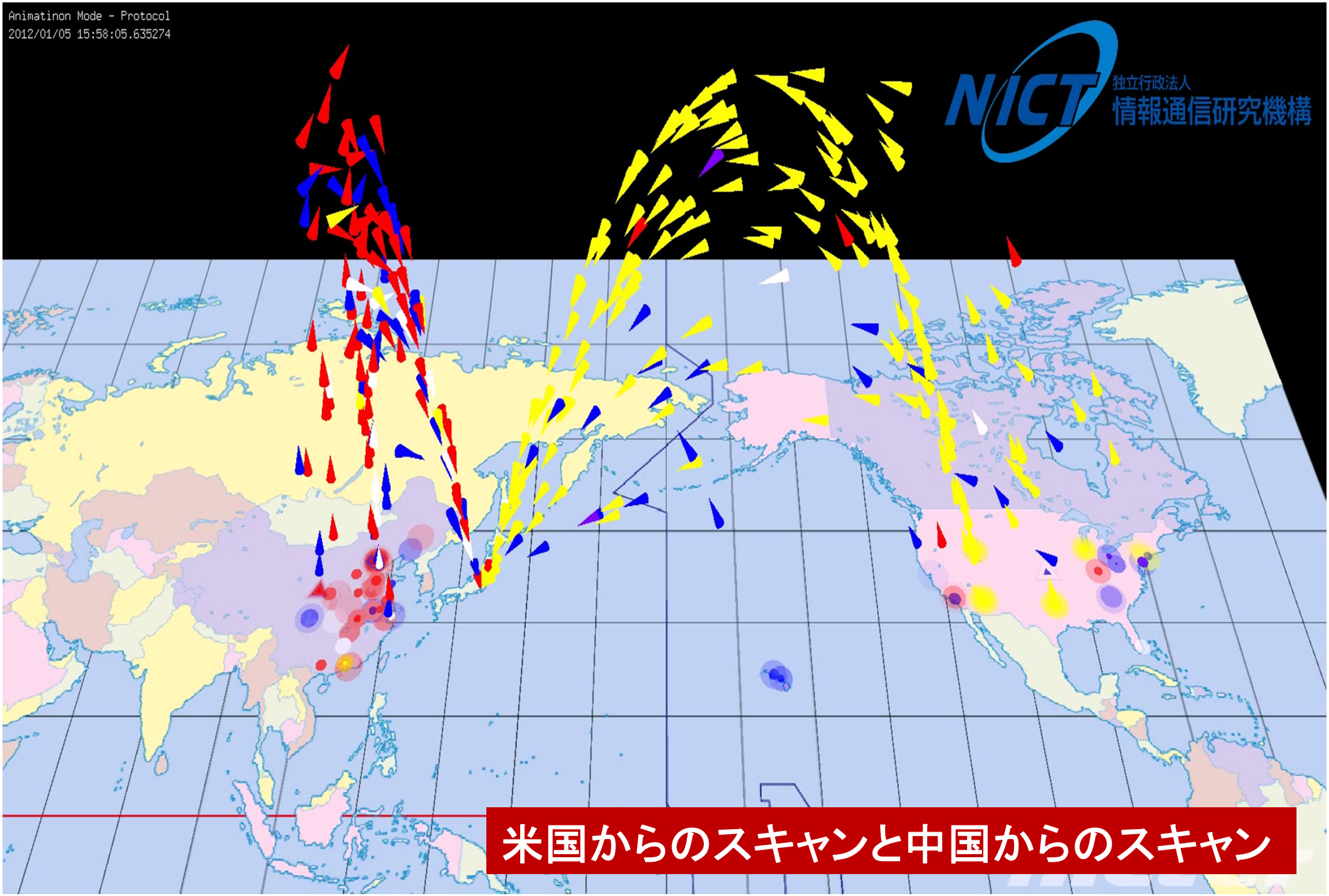
  ※ 送信元IPアドレス偽装されたSYN Floodへの応答
- DNS水責め攻撃のバックスキャッタ

  ※送信元IPアドレス偽装されたランダムサブドメイン攻撃

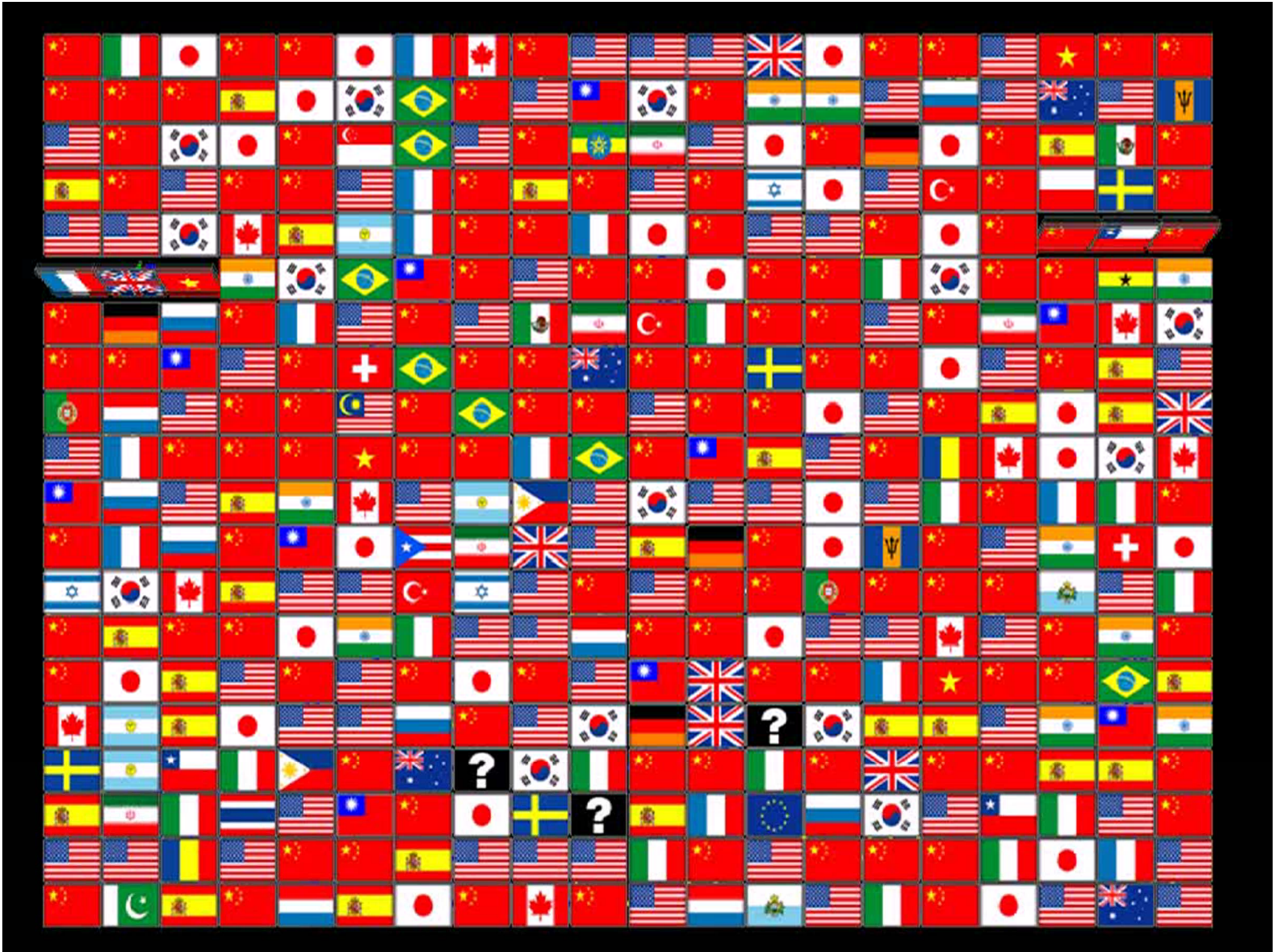
✓設定ミス




File(F) Settings(S) View(V)
Help(H)
NICT
独立行政法人
情報通信研究機構
TCP_SYN
TCP_SYN_ACK
TCP_ACK
TCP_FIN
TCP_RST
TCP_PUSH
TCP_OTHER
UDP
ICMP
NICTER

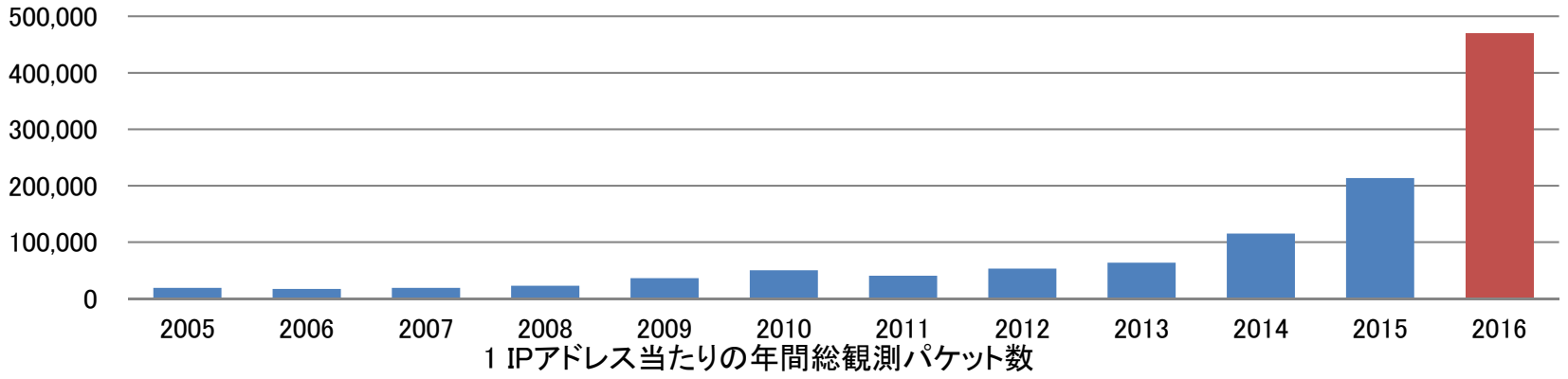

Animatinon Mode - Protocol
2012/01/05 15:58:05.635274
NICT
独立行政法人
情報通信研究機構
米国からのスキャンと中国からのスキャン


[Recv Count] ---------- [1120]pps
- Sampling Rate(1/1)--- < 0>
- Packet Loss --------- < 118>
[Packet Dropped]
- Not IPv4 ---------- (0)
- Other Proto ---------- (2)
- FragmentPkt ---------- (0)
- By Filter ---------- (0)
- CC Not Match --------- (0)
[Reg Count] ---------- [0]pps
Current fps - 30
Drawing Packet Num - 50
独立行政法人
情報通信研究機構
TCP_SYN
TCP_SYN_ACK
TCP_ACK
TCP_FIN
TCP_RST
TCP_PUSH
TCP_OTHER
UDP
ICMP
日本から日本へのスキャン

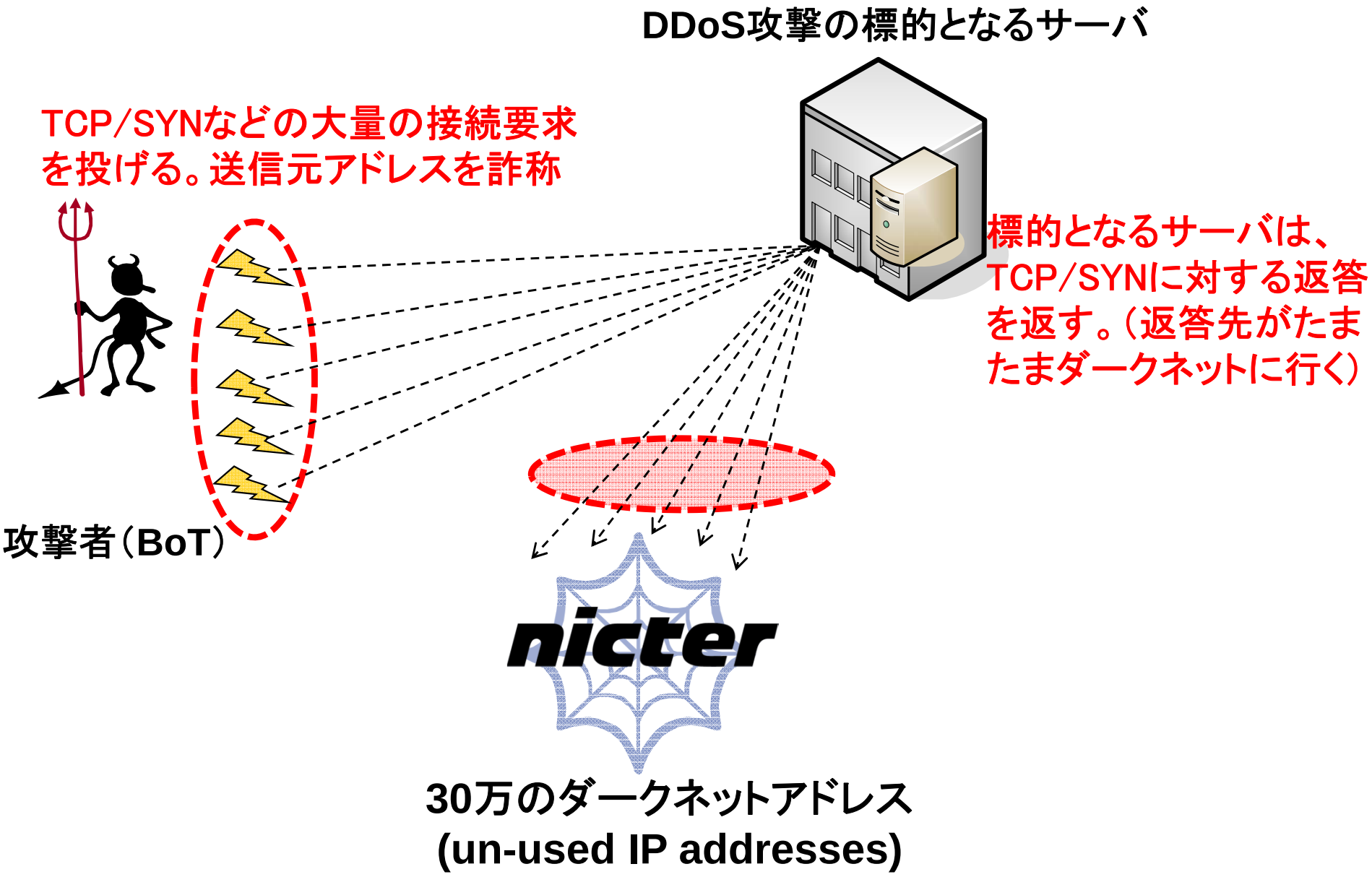


NICTERダークネット観測統計

年	年間 総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの 年間総観測パケット数
2005	約 3.1億	約1.6万	19,066
2006	約 8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104



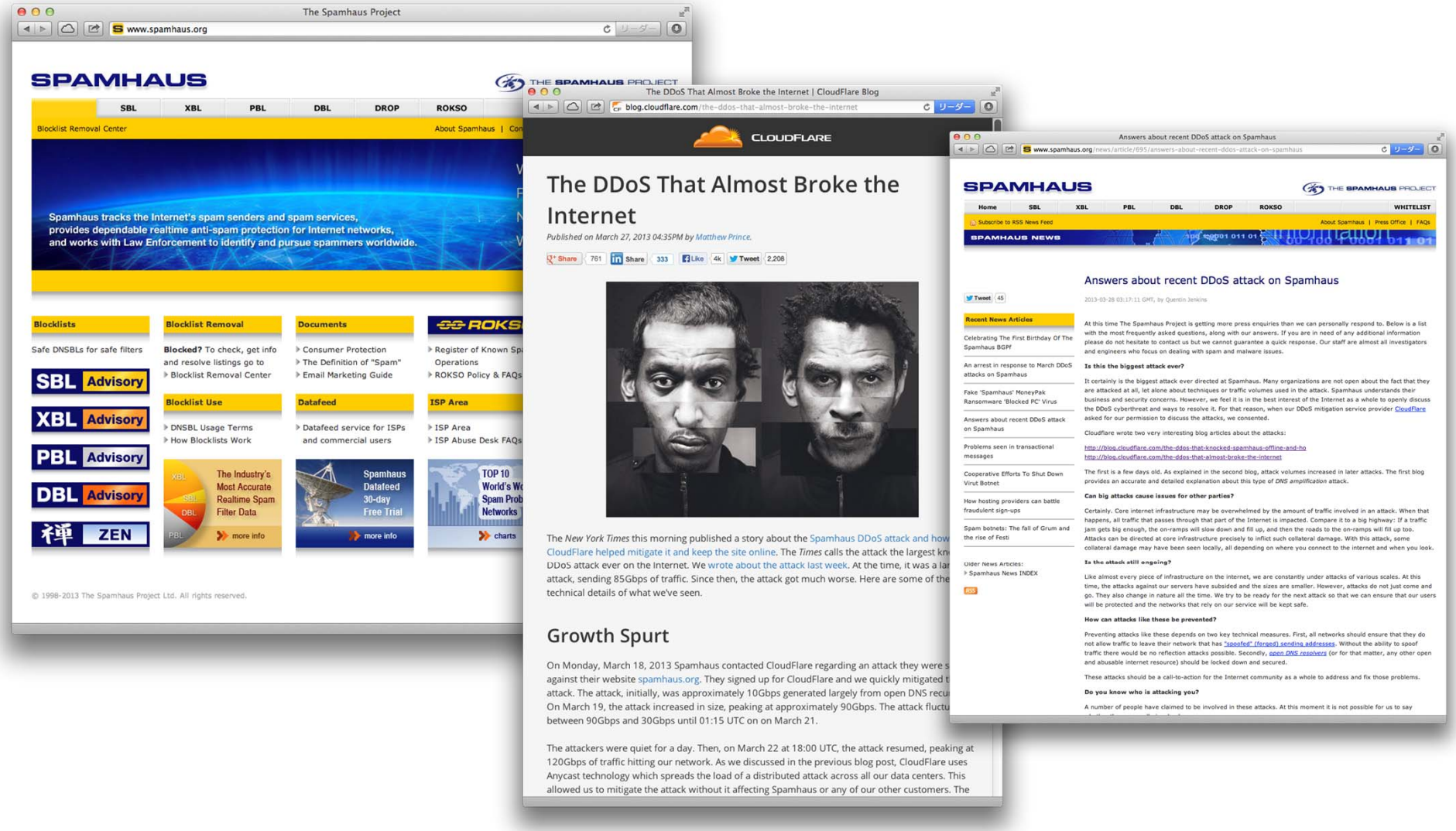
Backscatter: DDoS 攻撃の跳ね返り



2012年、SONYからのバックスキャッター

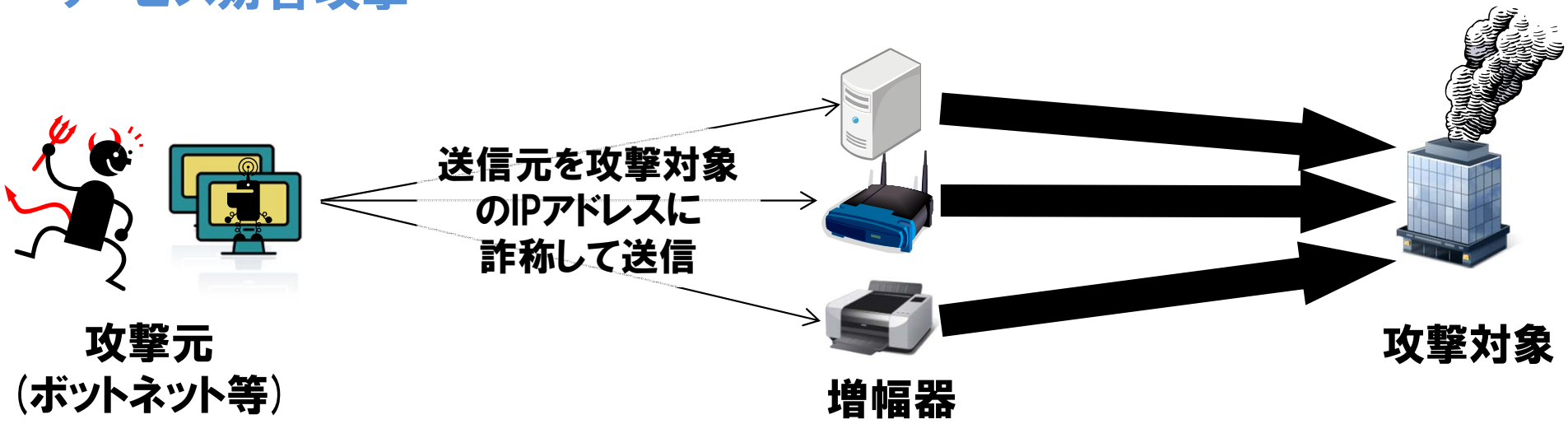
リフレクター攻撃（DRDoS）

- 2013年3月 SpamhausへのDDoS攻撃
- DNSをリフレクターにしたDRDoS攻撃（300Gbps）



新たなDR-DoS攻撃

- DR-DoS (Distributed Reflection Denial of Service) 攻撃
  インターネット上のサーバ・PC・ネットワーク機器等を増幅器として悪用したサービス妨害攻撃



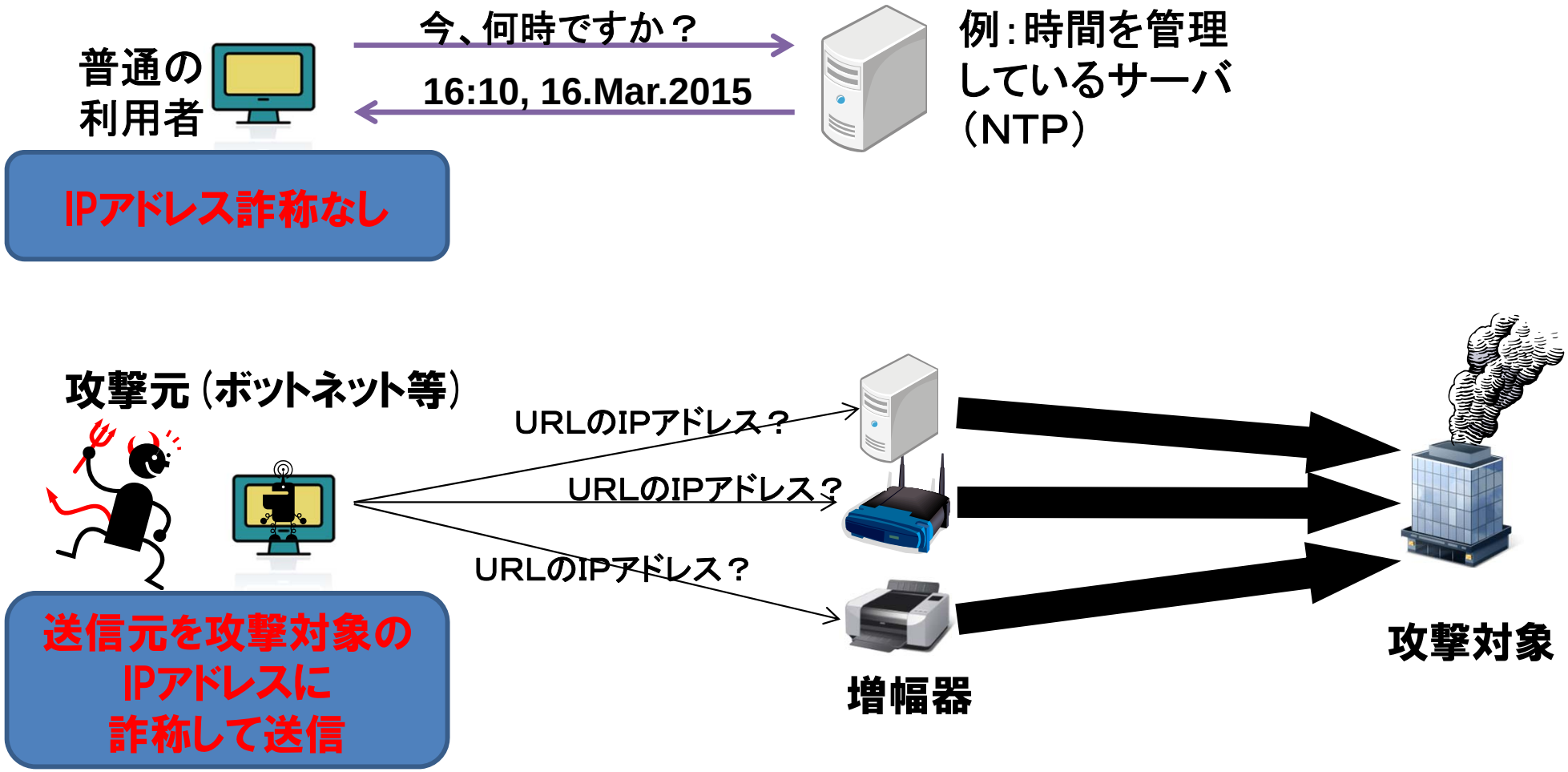
可視化

- 過去最大規模のサービス妨害攻撃の原因

  2013.3 スパム対策組織Spamhausへの攻撃 (300Gbps)

  2014.2 クラウドサービスプロバイダCloudFlareへの攻撃 (400Gbps)

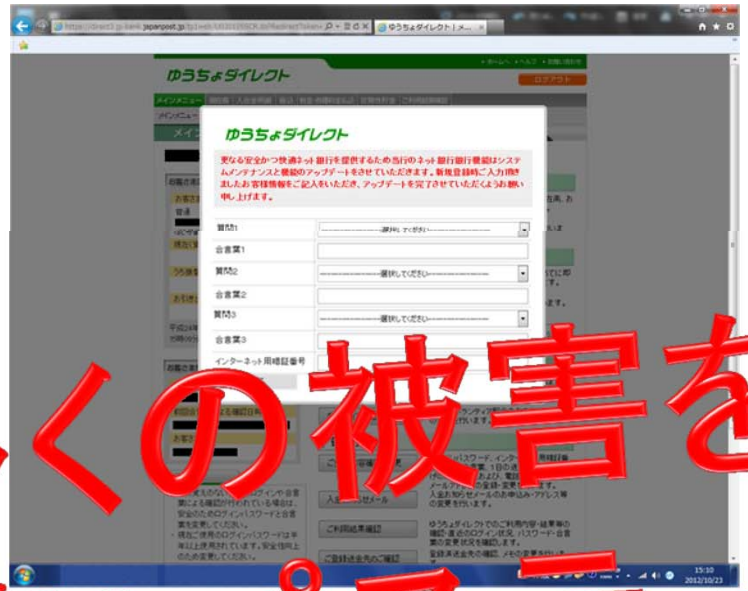
DR-DoSの原理


普通の
利用者
今、何時ですか？
16:10, 16.Mar.2015
例：時間を管理
しているサーバ
（NTP）
IPアドレス詐称なし
攻撃元（ボットネット等）
URLのIPアドレス？
URLのIPアドレス？
URLのIPアドレス？
送信元を攻撃対象の
IPアドレスに
詐称して送信
増幅器
攻撃対象

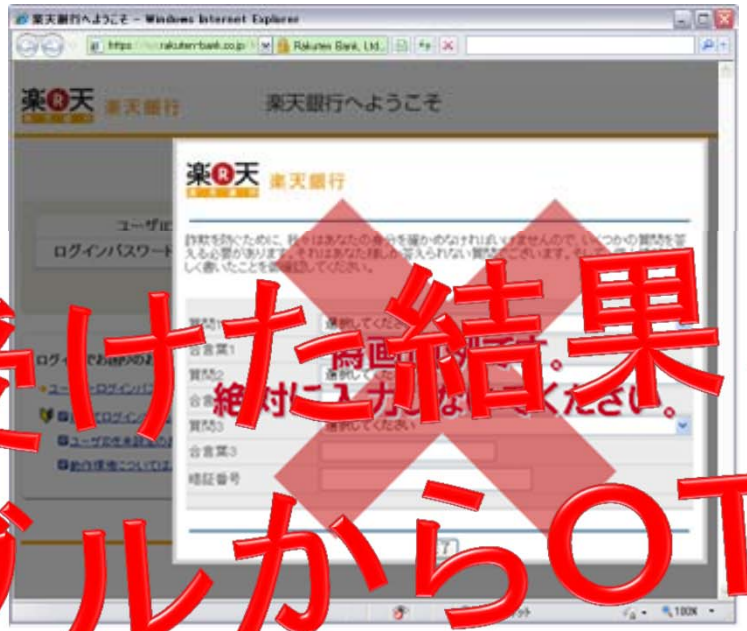
最近のセキュリティ脅威（攻撃）の紹介

1）これまでの脅威（ボットネット中心）
2）金融系マルウェア
3）APTによる脅威
4）IoTによる脅威

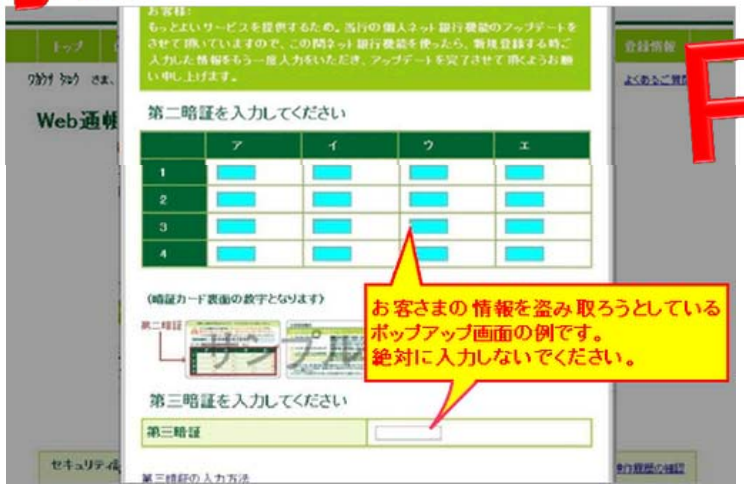
金融系マルウェアの啓蒙画面



出典：ゆうちょ銀行



出典：楽天銀行



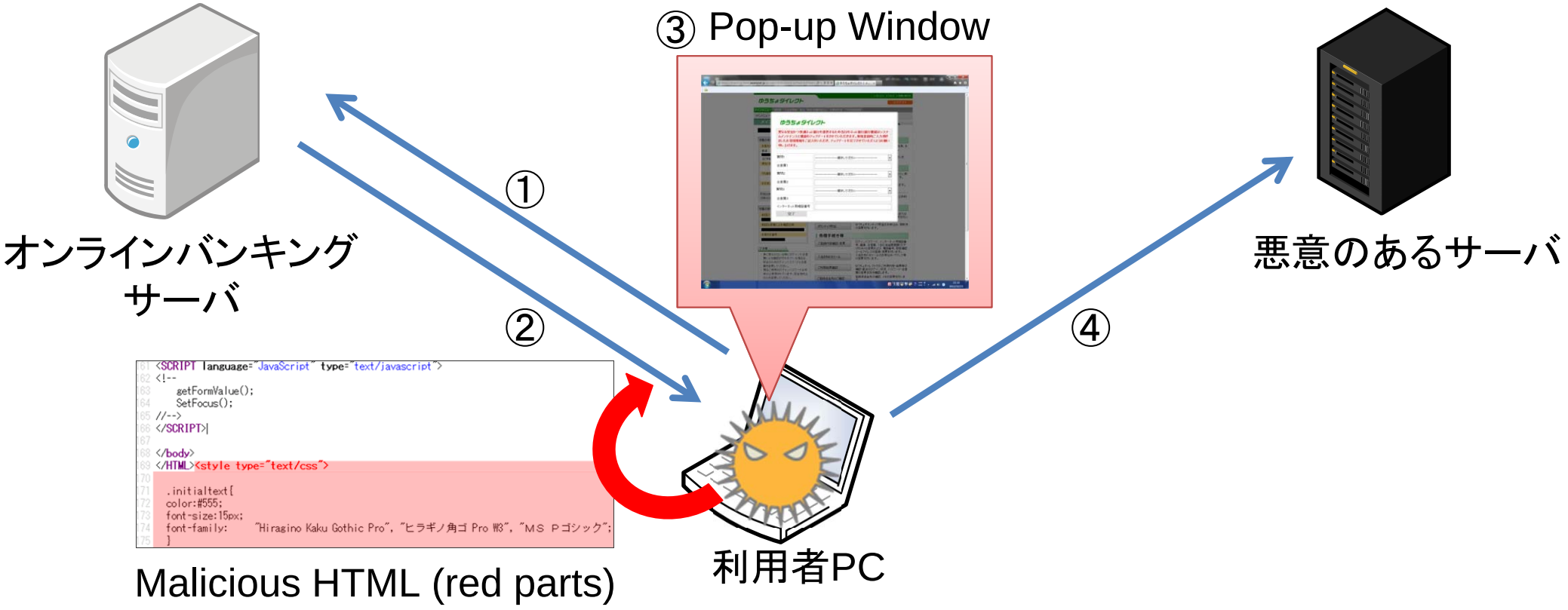
出典：三井住友銀行

出典：三菱東京UFJ銀行

多くの被害を受けた結果、
第2パステーブルからOTPへ

金融系マルウェアの大枠の流れ

① マルウェア感染PCが正規サイトにアクセス
② 正規コンテンツにマルウェアが不正なHTMLを追記
③ ユーザの画面上に不正なポップアップが表示される
④ ユーザが入力を完了すると外部サーバに情報送付

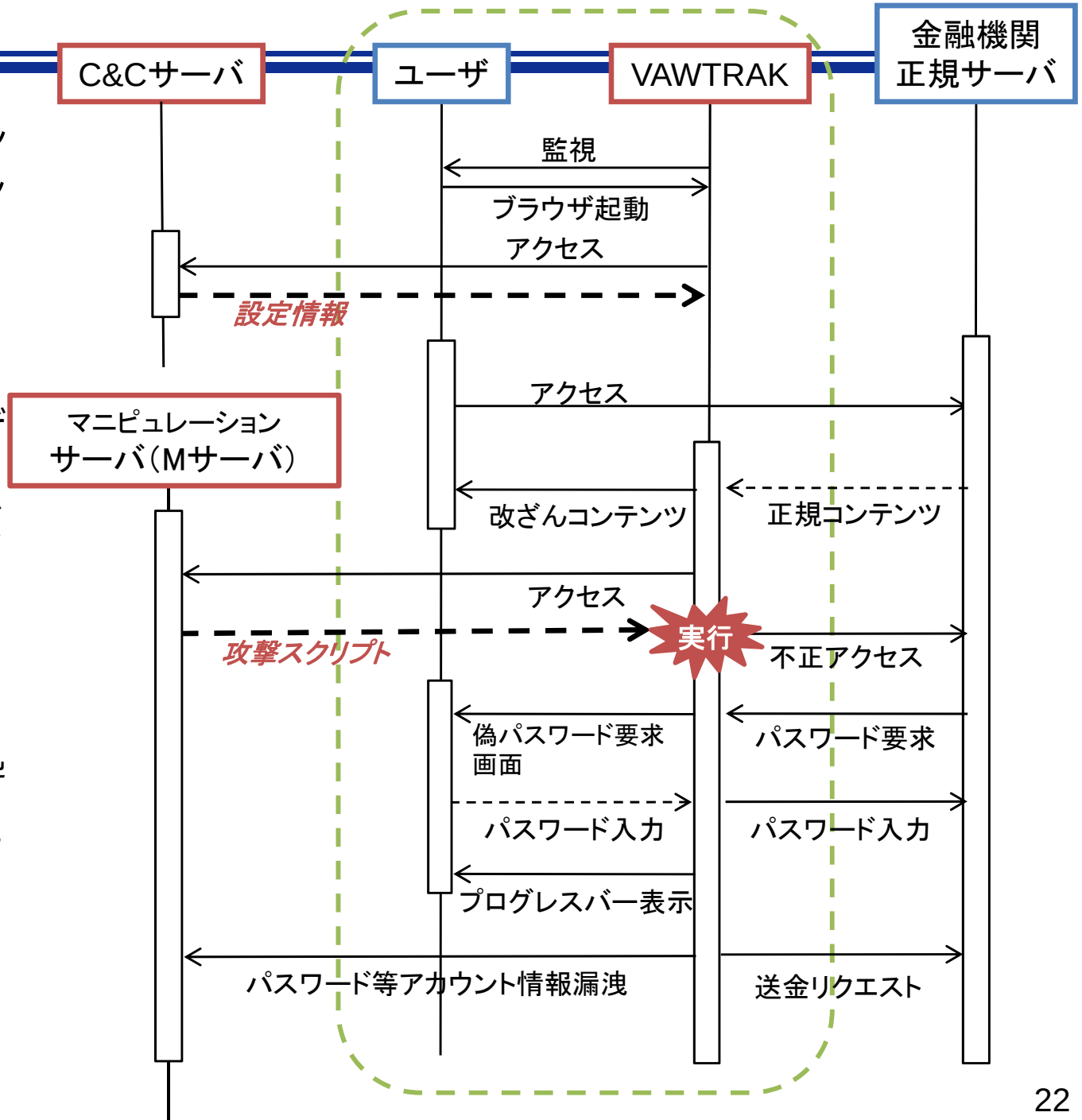


出典：セキュアブレイン「インターネットバンキング利用者を狙ったマルウェアの挙動を解析」2012-11-08

金融系マルウェアVAWTRAKの挙動観測例

金融系マルウェアの一例としてVAWTRAKの挙動を観測した結果を記載する。

① PCがVAWTRAKに感染。PC上でWEBブラウザが起動されると、Webブラウザを乗っ取る。
② VAWTRAKは、C&Cサーバから**設定情報を取得**。
③ VAWTRAKはユーザが攻撃対象となっているURL（金融機関)にアクセスすると、Webページの改ざん処理が行う。また、Mサーバから取得した**攻撃スクリプトを取得**し、実行。
④ **ログインフォーム入力情報の窃取や、ユーザPC上からの送金処理が行われる。**



最近のセキュリティ脅威（攻撃）の紹介

1）これまでの脅威（ボットネット中心）
2）金融系マルウェア
3）APTによる脅威
4）IoTによる脅威

新しい攻撃：APTによる攻撃の現状

Advanced	---	高度で
Persistent	---	執拗な
Threat:	---	脅威

- APTによる攻撃の定義

  APTによる攻撃とは、特定の相手に狙いを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数か月から数年にわたって継続するサイバー攻撃のこと。

これまでのAPTによる攻撃の事例

公表時期	標的	攻撃の概要
2010年1月	米グーグルなど30数社	これは米国のグーグルなど33社がInternet Explorerのゼロデイぜい弱性を突く攻撃を受け、各企業が保有するソフトウェアのソースコード等の知的財産などが狙われたとされる。グーグルではメールサービス「Gmail」のアカウントやパスワードの一部が漏えいするなどの被害が確認された。
2010年11月	イランの核施設	ウラン濃縮用の遠心分離機の論理制御装置を乗っ取り、回転数を通常よりも過大に設定して、遠心分離機を意図的に故障させたといわれる。Windowsなどの複数のぜい弱性を突く、Stuxnetウイルスが使われた。
2011年2月	世界の石油・ガス関連企業5社	2009年11月以降、世界の石油・ガス関連企業の油田・ガス生産システムや現地調査入札関連の情報が盗み出された。中国のハッカー集団「ナイト・ドラゴン」によるものとされる。
2011年3月	米EMC	米国EMCの2要素認証製品であるSecureIDのワンタイムパスワードの生成に関する技術情報が流出。その後、米国ロッキード・マーチンへのサイバー攻撃にSecureIDのパスワード生成の情報が利用され、同社のシステムに不正侵入されたことが同年5月に明らかに。
2011年8月	世界70以上の企業や政府機関	2006年から2010年9月にかけて、重工業からエレクトロニクス企業、IT企業、オリンピック委員会など（日本は2組織）世界の70以上の企業や政府機関のコンピュータにRAT（Remote Administration Tool / Remote Access Trojan）が組み込まれ、情報が窃取された。
2011年8月	オランダ認証局のデジノター	オランダ・デジノターのSSL認証局システムが不正侵入されていたことが2011年7月に明らかになり、続いてGmailを含む多数のサイト向けのSSL証明書が不正に発行されていたことが同年8月に判明。
2011年9月	三菱重工ほかイスラエル、インド、米国の防衛産業	Flash PlayerやAdobe Readerのぜい弱性を突いた攻撃を受けた。PDFファイル付きメールを開けたPCがウイルスに感染、ネットワーク構成やファイルの所在を特定された上で、一部の端末にRATを組み込まれた。
2011年10月	外務省在外公館	日本の国外9ヶ国にある外務省在外公館の職員が使用するコンピュータ等が、情報窃取を目的とする不正プログラムに感染。不正プログラムは外務省のネットワークシステムを標的にした特殊なものとされる。
2011年10月	衆議院	情報窃取を目的とする不正プログラムに感染し、11月には全衆議院議員のID・パスワードが流出、最大15日間にわたってメールが盗聴されていたおそれがあることが判明。
2011年11月	参議院	メールに添付されたウイルスによって参議院のサーバが感染し、全参議院議員・秘書の計約千件のパスワードが流出した可能性が判明、その一部は実際の流出が確認された。

APTによる攻撃と従来の攻撃の相違

	APTによる攻撃（発見が困難）	従来の攻撃
攻撃目的	情報の収奪（スパイ行為）	多様な目的
	情報を盗むことを目的とする。動機は軍事・政治目的や経済目的など様々。	政治目的・経済目的等に加えて、いやがらせや自身が目立つためという目的もある
攻撃の重要な拠点	対象システムの内部	対象システムの外部
	目的を達成するために、対象とするコンピュータシステムの中に拠点を作り、そこから本格的な攻撃に取り掛かる	ボットネットなどを用いて、主に外部から攻撃する
攻撃ツール	特別仕様・手動ツール	標準的ツール・既成ウイルス
	目的に合わせ手作り。マニュアル（手動）操作も用いる	出来合いのツールを使う。ウイルスも闇で市販されているものが多い。
攻撃の手順	段階的で変幻自在	直線的で定型的
	対象システムの情報を入手し、それにあわせて手口を変える	標準ツール等で攻略できる範囲しか行わない
攻撃の痕跡の改ざん・消去	偽装・改ざん（痕跡なし）	痕跡にこだわらない
	発覚を遅くするために、痕跡を残さないようにする	自ら攻撃成功を誇ることがなるなど、発覚に問題がない為、頓着しない

日本年金機構への標的型攻撃

- 2015年6月1日
  - ✓ 日本年金機構が125万件の年金情報の漏洩を発表
- 標的型攻撃メールが起点となりマルウェア『Emdivi』に感染

http://blogos.com/news/Japan_Pension_Service/

事例（2015年）

日本年金機構への標的型攻撃

- 2015年6月1日 125万件の年金情報の漏洩を発表
- 標的型攻撃メールが起点となり『Emdivi』に感染

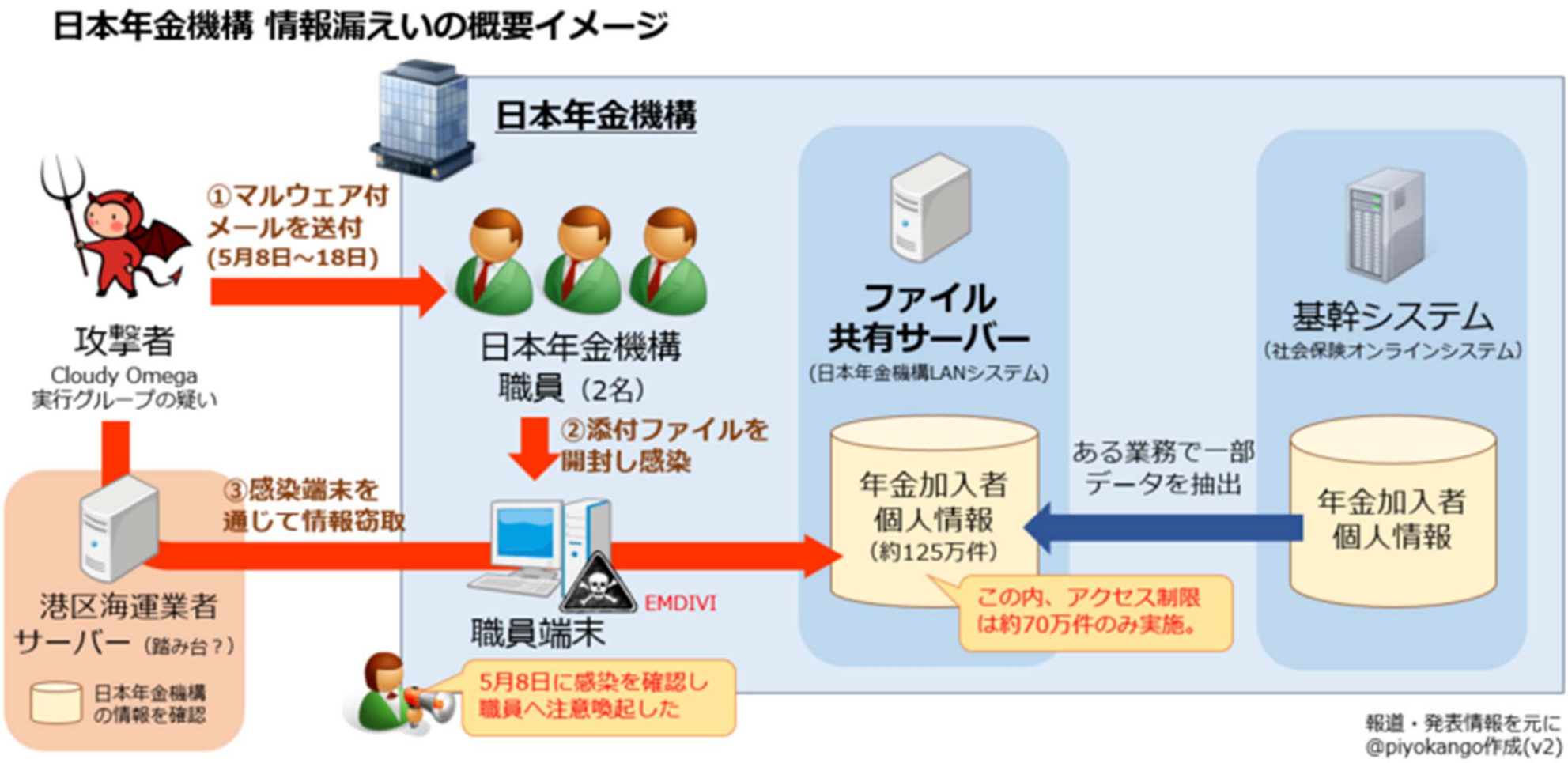
日本年金機構への標的型攻撃メール

番号	受信日	不審メールの概要
Ⅰ	5月8日(金)	件名：「厚生年金基金制度の見直しについて(試案)に関する意見」 宛先：公開メールアドレス(2) リンク：商用オンラインストレージ
Ⅱ	5月18日(月)	件名：給付研究委員会オープンセミナーのご案内 宛先：非公開の個人メールアドレス(98) 添付ファイル：給付研究委員会オープンセミナーのご案内.lzh
Ⅲ	5月18日(月) ～ 5月19日(火)	件名：厚生年金徴収関係研修資料 宛先：非公開の個人メールアドレス(20) 添付ファイル：厚生年金徴収関係研修資料(150331厚生年金徴収支援G).lzh(16) リンク：商用オンラインストレージ(4)
Ⅳ	5月20日(水)	件名：【医療費通知】 宛先：公開メールアドレス(3) 添付ファイル：医療費通知のお知らせ.lzh

※ 表中の括弧内の数字はメールの件数を表す。

（NISC「日本年金機構における個人情報流出事案に関する原因究明調査結果」）

日本年金機構への攻撃手法



（出典：piyolog http://d.hatena.ne.jp/Kango/20150601/1433166675）

2016年に起きた主なAPT攻撃の事例

- 慶應義塾大学への攻撃（文科省なりすまし）
  - –実際のメールの文面が使いまわされた事例
- JTBへの攻撃
  - –大規模な情報漏えいの事例
- 富山大学への攻撃
  - –メール受信からインシデント発覚までに時間を要した（半年ほど要した）事例

慶應義塾大学への攻撃
（文科省なりすまし）

メール受信日	2016/05/25
標的となった組織	慶應義塾大学 （同様のメールが2016/05/25-2016/05/27にかけて以下の大学にも送られていた） 東京工業大学、中央大学、首都大学東京、早稲田大学、青山学院大学、上智大学
差出人	yahoo.co.jpの複数メールアドレス
件名	【文科省（ご連絡）】新学術領域研究の中間・事後評価について
メール本文	右図 （文科省が過去に送ったものを流用）
添付ファイル	中間-事後評価に係る様式20160524.zip 中間-事後評価に係る様式201605.zip （zipを展開したものはPlugXと思われる）
実行日	実行せず
検知日	実行されなかったので，感染していない

参考：http://www.sfc.itc.keio.ac.jp/ja/news_targeted_mail_20160524.html
http://d.hatena.ne.jp/Kango/20160526/1464278965

使用されたメール（事例）

平成26・27・28年度採択研究領域の領域代表者各位

お世話になっております。
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

本年度、中間・事後評価のスキームを見直すとともに、
評価報告書の様式の見直しを実施いたしましたので、
来年又は再来年に中間評価又は事後評価を実施することになります
先生方に、本変更点についてご報告させていただきます。
変更点につきましては、添付の事務連絡をご参照ください。

また、
実際の評価時期に作成依頼する際には変更の可能性がございますが、
本年度は使用いたしました様式をご参考までに添付いたします。
特に、今回より追加いたしました別添の"データシート"については、
来年以降は"全研究期間"について記載いただくことを予定しておりますので、
現時点よりデータ収集・整理についてご準備いただけますようお願いいたします。

なお、評価に関する例年のスケジュールは以下の通りとなっております。
5月半ば　　評価報告書(添付のもの)の作成を依頼（領域代表者←文科省）

JTBへの攻撃

メール受信日	2016/03/15
標的となった組織	JTB
差出人	全日空を装った差出人
件名	「航空券控え 添付のご連絡」
メール本文	本文は不明，特徴を右に記載
添付ファイル	圧縮ファイル （ELIRKSやPlugXが含まれていた？）
受信＆感染者	問い合わせ窓口代表のメールアドレス
実行日	2016/03/19
検知日	2016/03/19
マルウェア通信先	不明
漏洩した恐れがある情報	個人情報（約680万人）

メール本文の特徴として以下のものが報道されている

- 「お客様の旅行内容を確認したい」旨が記載
- 「eチケットの確認をお願いしたい」旨が記載
  - 上記は共に不自然な文面ではない
- 実在する取引先の会社名，部署名，担当者名が署名に記載
- 日本語挨拶の定型文が記載
  - 「お世話になっております」の一文が含まれていた

参考：
http://www.jtbcorp.jp/jp/160824.html
http://d.hatena.ne.jp/Kango/20160614/1465925330#20160614f28

富山大学への攻撃

メール受信日	2015/11/5, 11/17, 11/24（複数回）
標的となった組織	富山大学 研究推進機構 水素同位体科学研究センター
差出人	yahoo.co.jpのメールアドレス（自称学生）
件名	不明
メール本文	次頁
添付ファイル	document.zip （zip展開したものはAsruexと思われる）
受信＆ 感染者	トリチウム理工学専門の非常勤職員
実行日	2015/11/24
検知日	2016/06/14
マルウェア通信先	supportservice247.com requestword.com enewsdatabank.com housemarket21.com
漏洩した恐れがある	共同研究関係者の個人情報（約1,500件）

使用されたメール（事例）

こんにちは、先生。
前回の学会でお目にかかった〇〇と申します。
学会では短い時間お話ししただけですが、ずっと尊敬に思っていた先生にお会いすることができてすごく嬉しかったです。
実は、僕が今研究しているプロゼックトに関して少しお伺いしたいことがありまして失礼ながらもメールお送りします。
詳細な質問は添付いたします。
この分野に詳しい先生から僕のプロゼックトについてご意見を伺いできればこれからの研究に大きな力になると思います。
お忙しいなか、突然のメールで申し訳ございませんが、何卒よろしくお願いいたします。
ありがとうございます。
早稲田大学　〇〇〇〇〇
〇〇〇〇〇@yahoo.co.jp

↑ 赤字部分の日本語が不自然

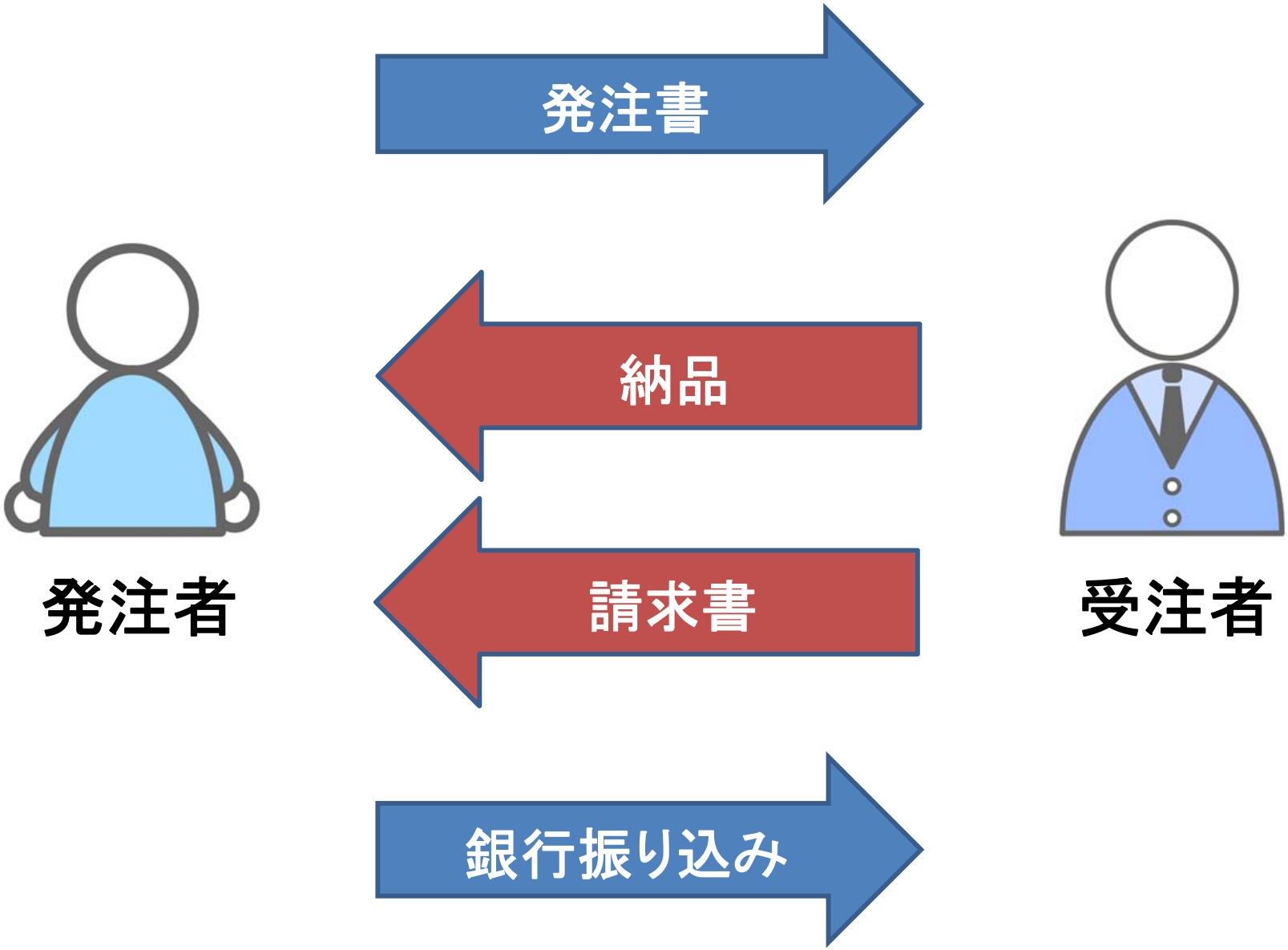
参考：
https://www.u-toyama.ac.jp/news/2016/1010.html
http://d.hatena.ne.jp/Kango/20161010/1476110179

「ビジネス　E－mail詐欺（BEC）」

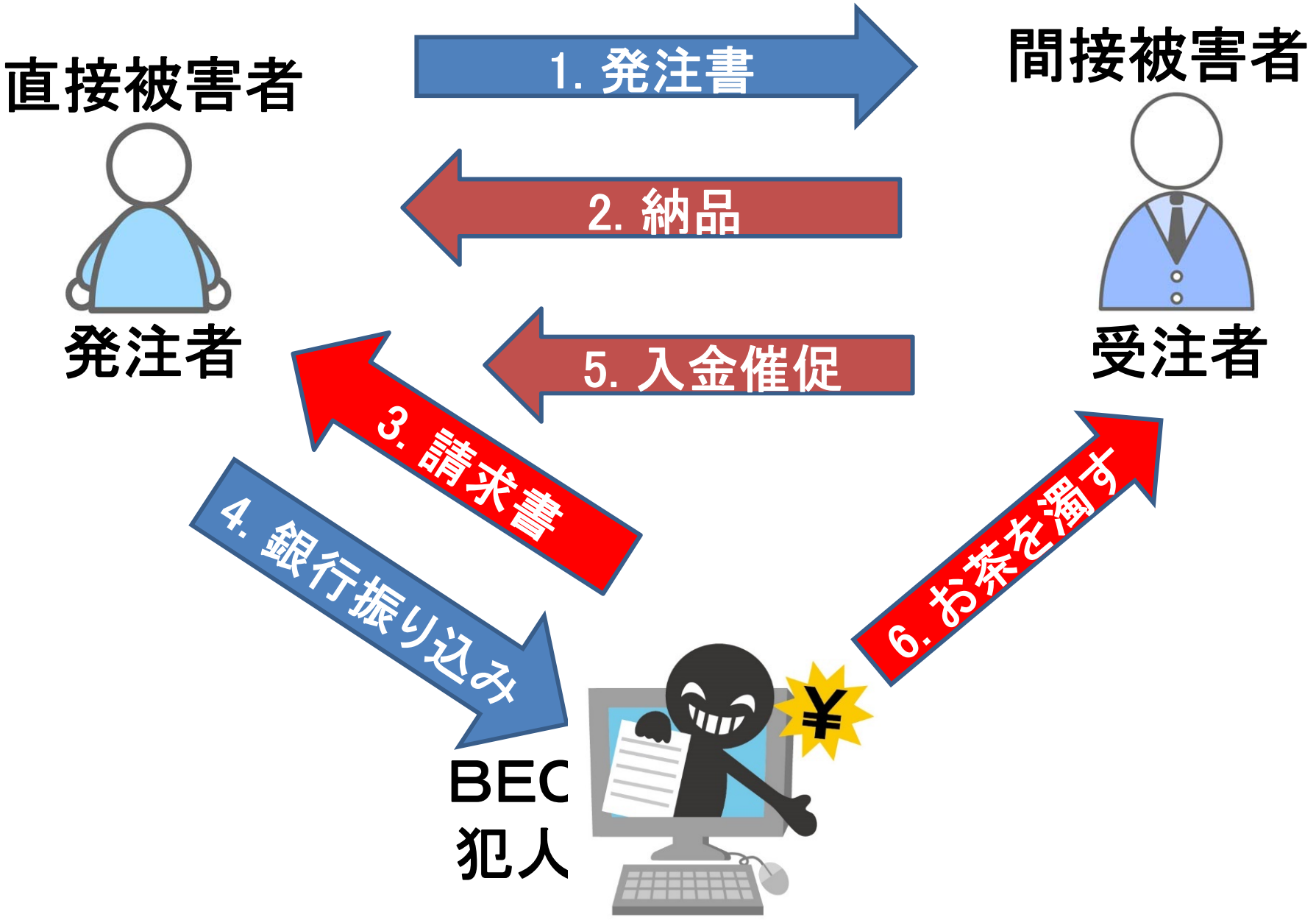
2016年に米国を中心に被害があった。世界中で3500億円以上の被害。
Business E-mail Compromise (BEC)

BECは既に日本にも上陸中

ビジネスの受発注における通常のやりとり



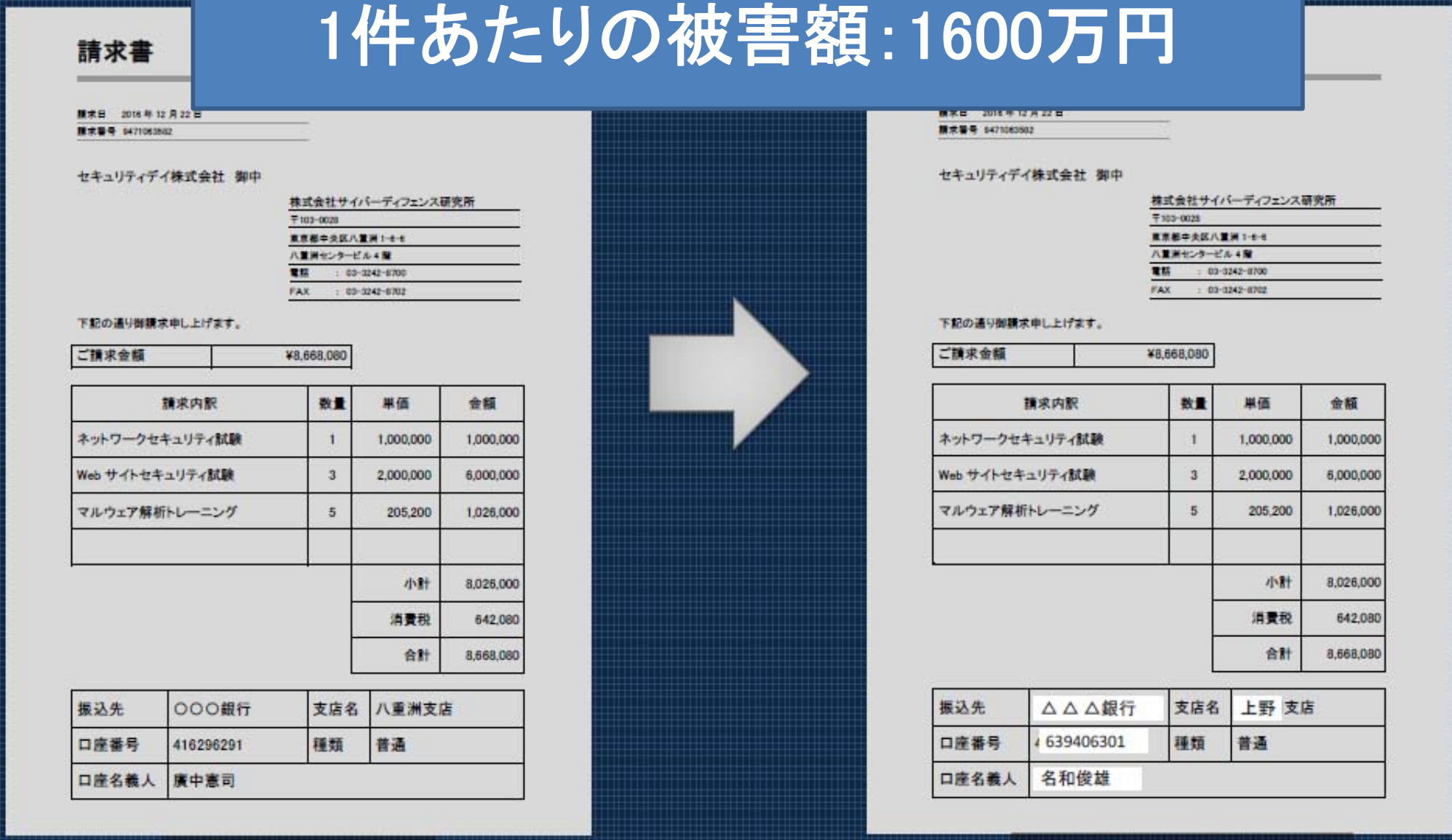
ビジネスメール詐欺（BEC）の場合



請求書偽造の手口

イメージCG

1件あたりの被害額：1600万円



請求書

請求日　2016 年 12 月 22 日
請求番号　9471063502

セキュリティデイ株式会社　御中

株式会社サイバーディフェンス研究所
〒103-0028
東京都中央区八重洲 1-6-6
八重洲センタービル 4 階
電話　：03-3242-8700
FAX　：03-3242-8702

下記の通り御請求申し上げます。

ご請求金額	¥8,668,080

請求内訳	数量	単価	金額
ネットワークセキュリティ試験	1	1,000,000	1,000,000
Web サイトセキュリティ試験	3	2,000,000	6,000,000
マルウェア解析トレーニング	5	205,200	1,026,000
		小計	8,026,000
		消費税	642,080
		合計	8,668,080

振込先	○○○銀行	支店名	八重洲支店
口座番号	416296291	種類	普通
口座名義人	廣中憲司		

正規の請求書

請求日　2016 年 12 月 22 日
請求番号　9471063502

セキュリティデイ株式会社　御中

株式会社サイバーディフェンス研究所
〒103-0028
東京都中央区八重洲 1-6-6
八重洲センタービル 4 階
電話　：03-3242-8700
FAX　：03-3242-8702

下記の通り御請求申し上げます。

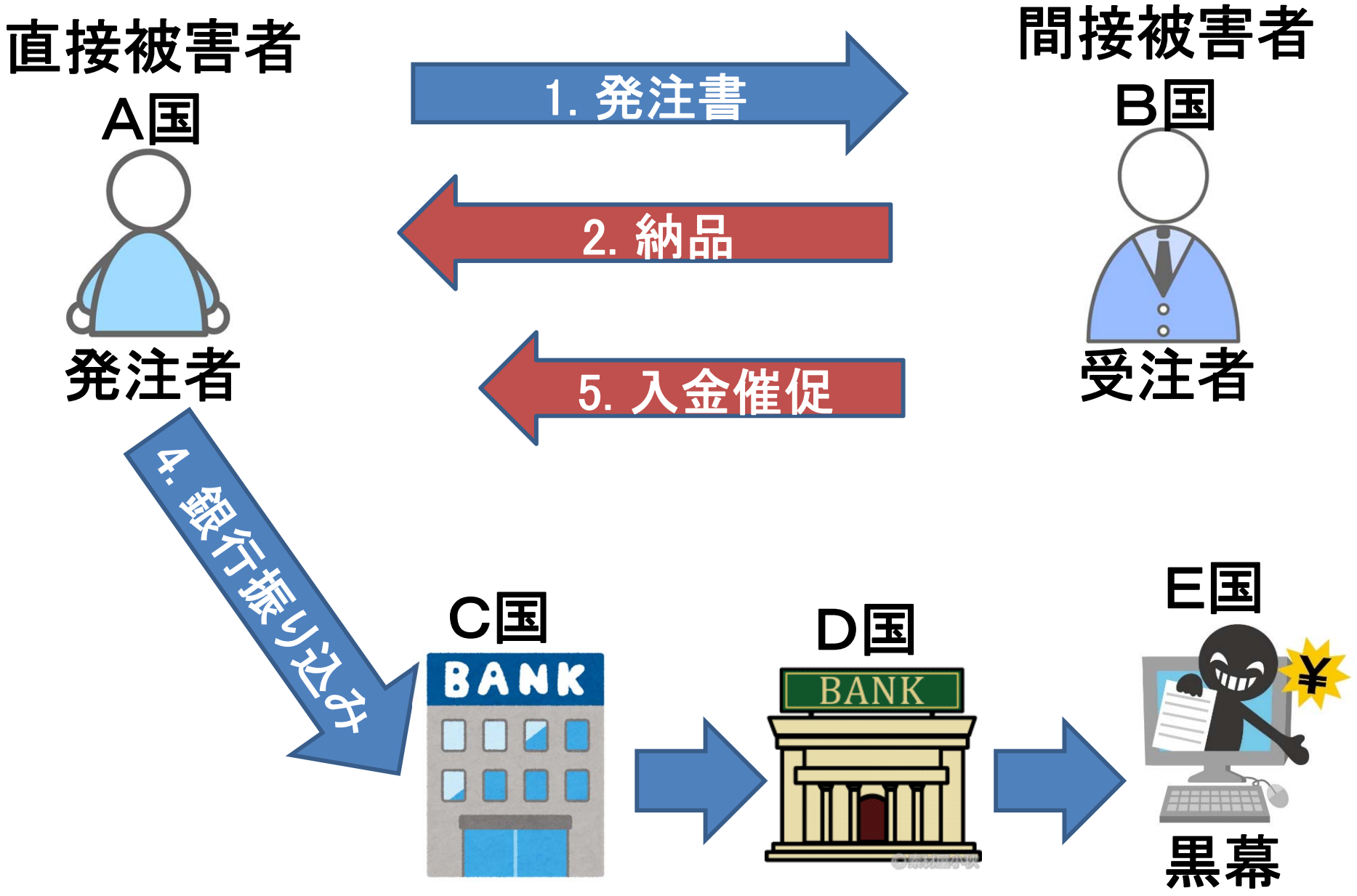
ご請求金額	¥8,668,080

請求内訳	数量	単価	金額
ネットワークセキュリティ試験	1	1,000,000	1,000,000
Web サイトセキュリティ試験	3	2,000,000	6,000,000
マルウェア解析トレーニング	5	205,200	1,026,000
		小計	8,026,000
		消費税	642,080
		合計	8,668,080

振込先	△△△銀行	支店名	上野 支店
口座番号	639406301	種類	普通
口座名義人	名和俊雄		

偽造された請求書

ビジネスメール詐欺（BEC）の場合（国を跨る）



最近のセキュリティ脅威（攻撃）の紹介

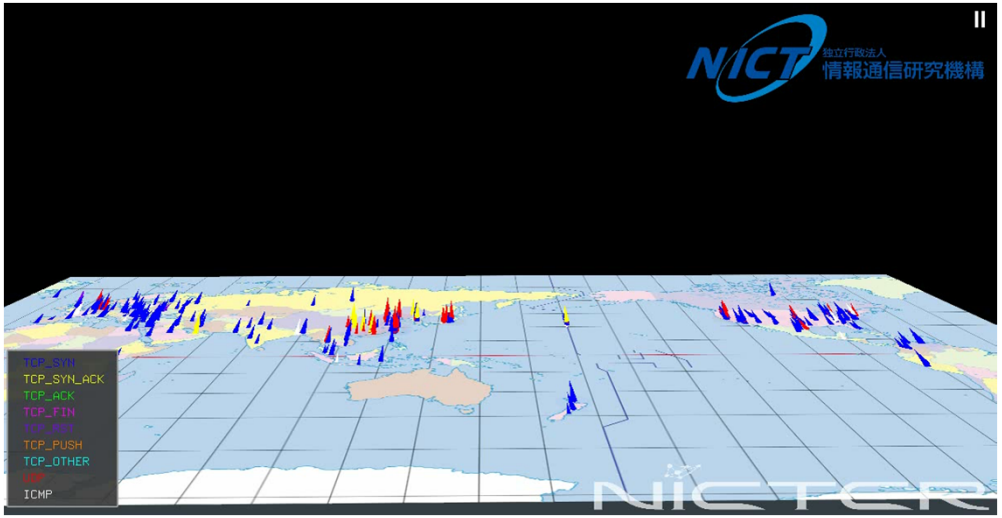
1）これまでの脅威（ボットネット中心）
2）金融系マルウェア
3）APTによる脅威
4）IoTによる脅威

nicter-Atlasによるスキャンの現状把握

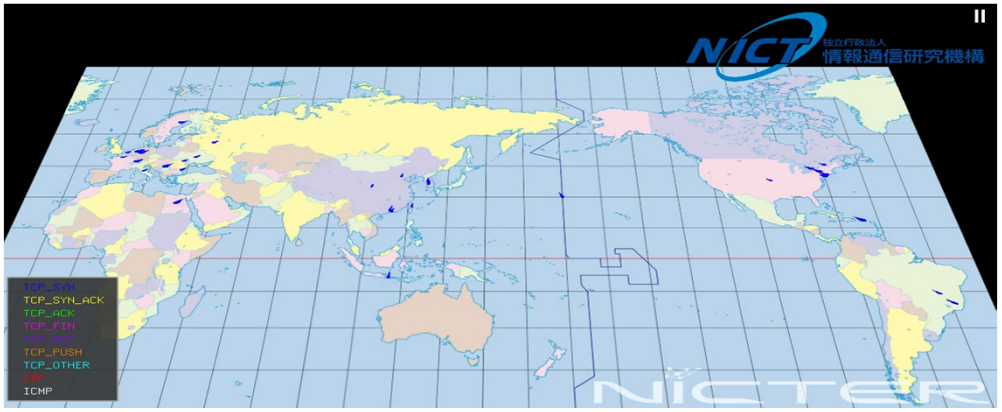
最近は, “Port 23 (telenet)へのスキャン” が増えている!!

- ダークネットに来るパケットを実時間で捕捉。
- 可視化におけるパケット色は、プロトコルタイプを表現。

- UDP
- TCP SYN
- TCP SYN/ACK
- TCP Other
- ICMP



Atlas All view



Atlas only port23

NICT National Institute of Information and Communications Technology

ダークネットへのTelnet攻撃の急増

パケット数

TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	2,699,639	45%
22	461,738	8%
8	3,07	6%
1433	208,460	3%
3	9,37	3%
3	5	3%
8080	145,657	2%
4	4,80	2%
9200	116,255	2%
25	94,901	2%

観測される
攻撃パケットの
約4～5割が
Telnet狙い

TCP 宛先ポート別パケット数 Top 10

宛先ポート	パケット数	割合
23	11,727,894	65%
1433	791,485	4%
22	559,059	3%
3389	247,547	1%
80	247,159	1%
8080	184,132	1%
443	147,434	1%
3306	128,382	1%
4028	116,029	1%
54628	78,378	0%

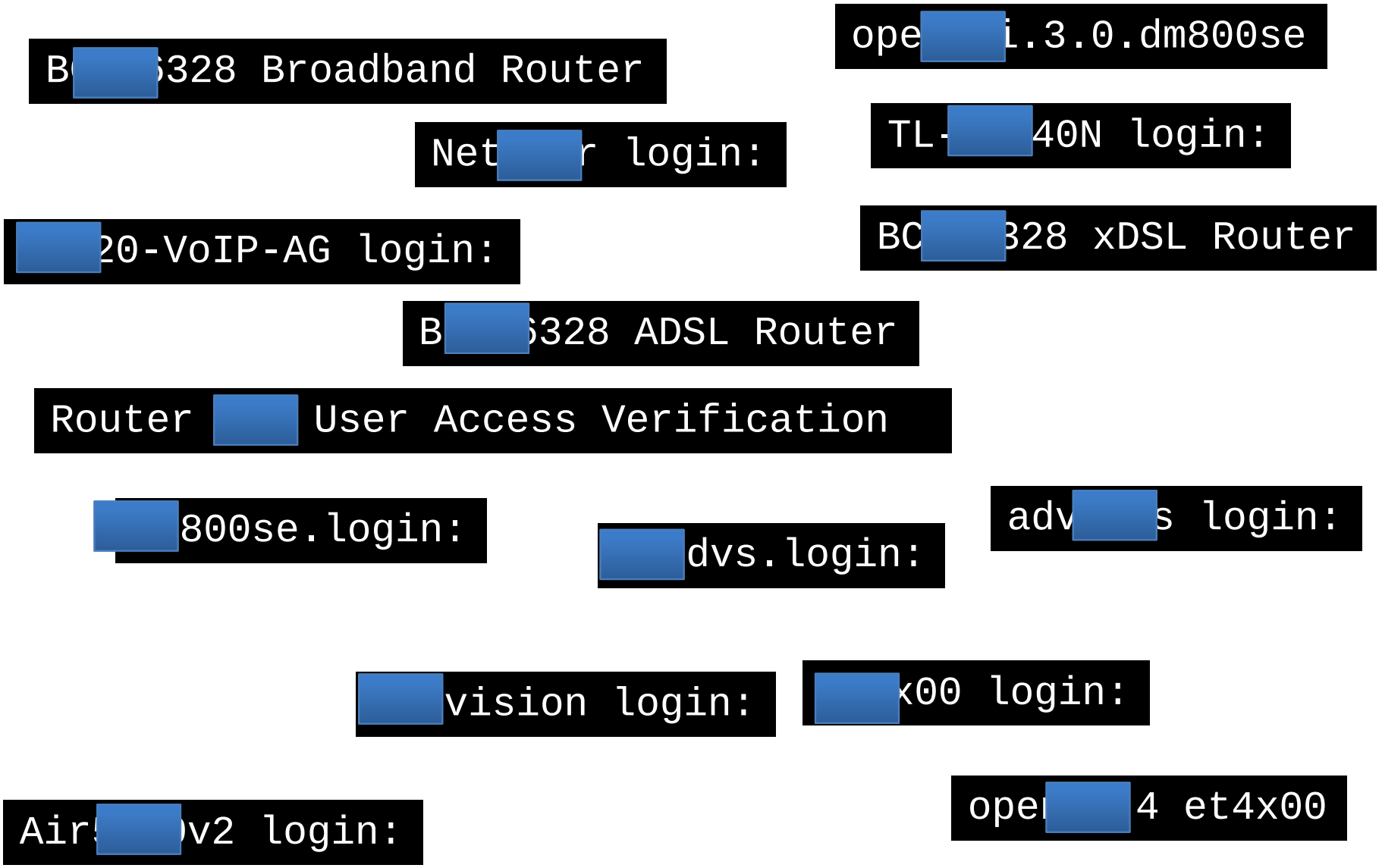
1/1/2005 1/1/2006 1/1/2007 1/1/2008 1/1/2009

日時

情報通信研究機構NICTERにおける過去10年間の観測結果（23/tcpのみ）

NICT National Institute of Information and Communications Technology

調べると、多くの機器で動いています



しかも多くは
デフォルト/弱いパスワードで

```
[shogo@www9058up ~]$ telnet x.x.243.13
Trying x.x.243.13...
Connected to x.x.243.13.
Escape character is '^]'.

[redacted]i.3.0.dm800s
[redacted]e.login: root
Password: 12345
```

リモートログイン成功

```
BusyBox v1.1.2 (2007.05.09-01:19+0000) Built-
in shell (ash)
Enter 'help' for a list of built-in commands.
```

2016年1月～6月の6ヶ月で横浜国大に攻撃をしてきたマルウェア感染IoT機器

感染機器の種別（2015年9月時点）

- 監視カメラ等
  - IP カメラ
  - デジタルビデオレコーダ

- 制御システム
  - ソリッドステートレコーダ
  - インターネット接続モジュール

IoT機器の
大量マルウェア感染が既に
発生している

- 駐車管理システム
- LEDディスプレイ制御システム

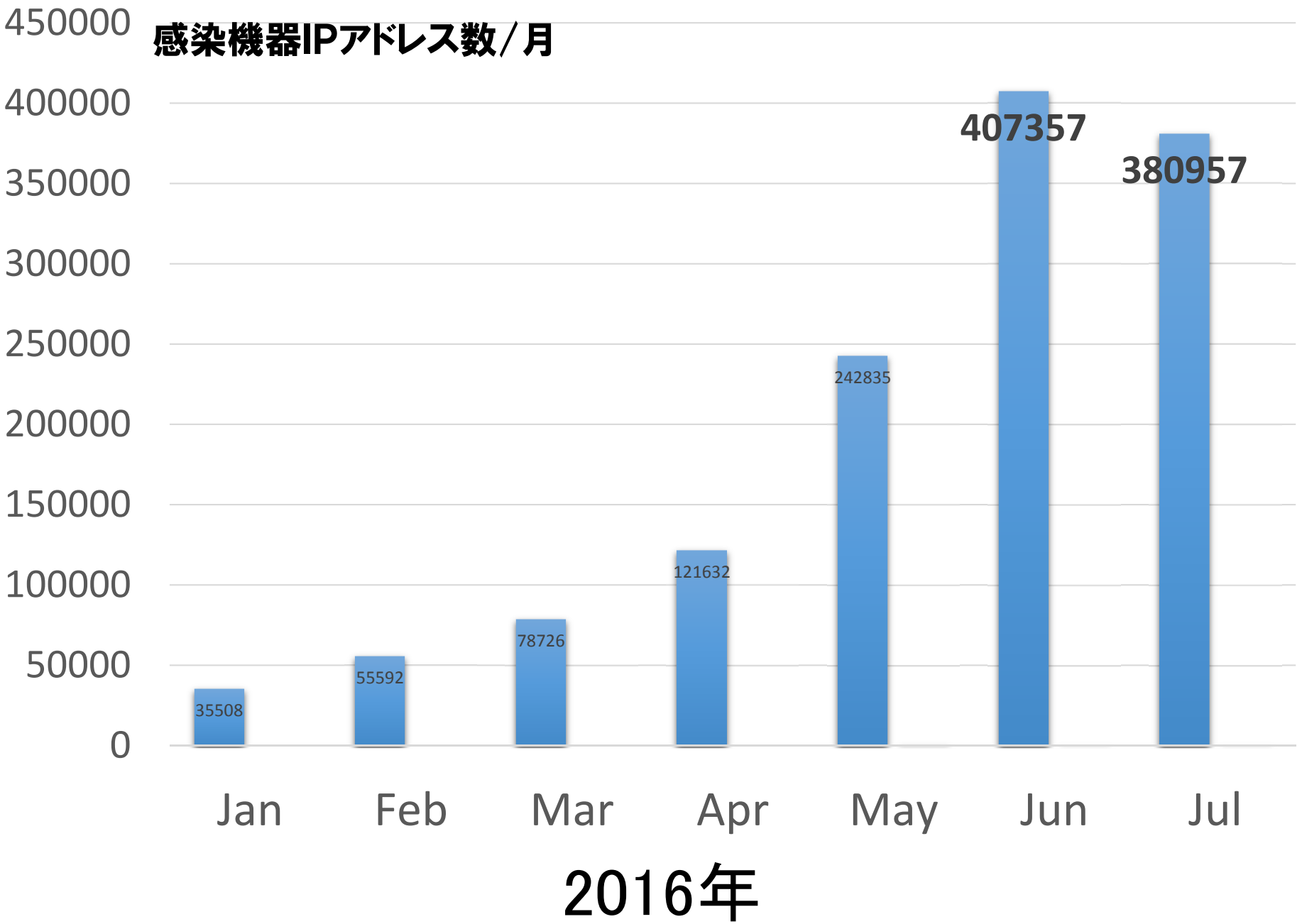
- 火災報知システム
- ディスク型記憶装置
- 指紋スキャナ

デバイスはWebおよびTelnetの応答から判断しています.

なぜIoT 機器が感染？？

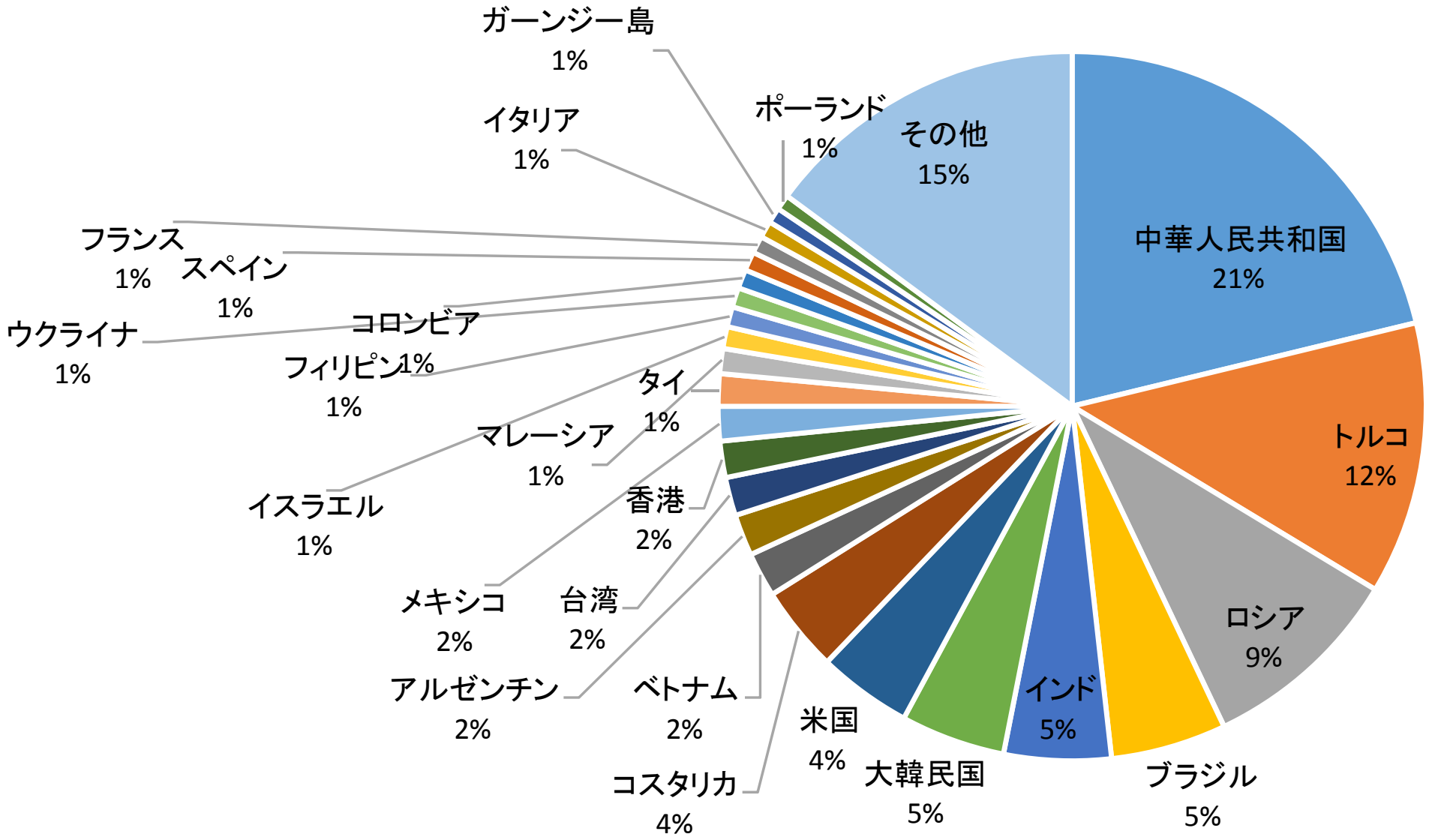
- 24/7 オンライン
- AVがない
- 弱い/デフォルトのID/PWの使用
- グローバル IP を持ち、インターネットへの接続を開いている

2016年4月以降感染機器数が急増
（IoT用ハニーポットでの観測によると）

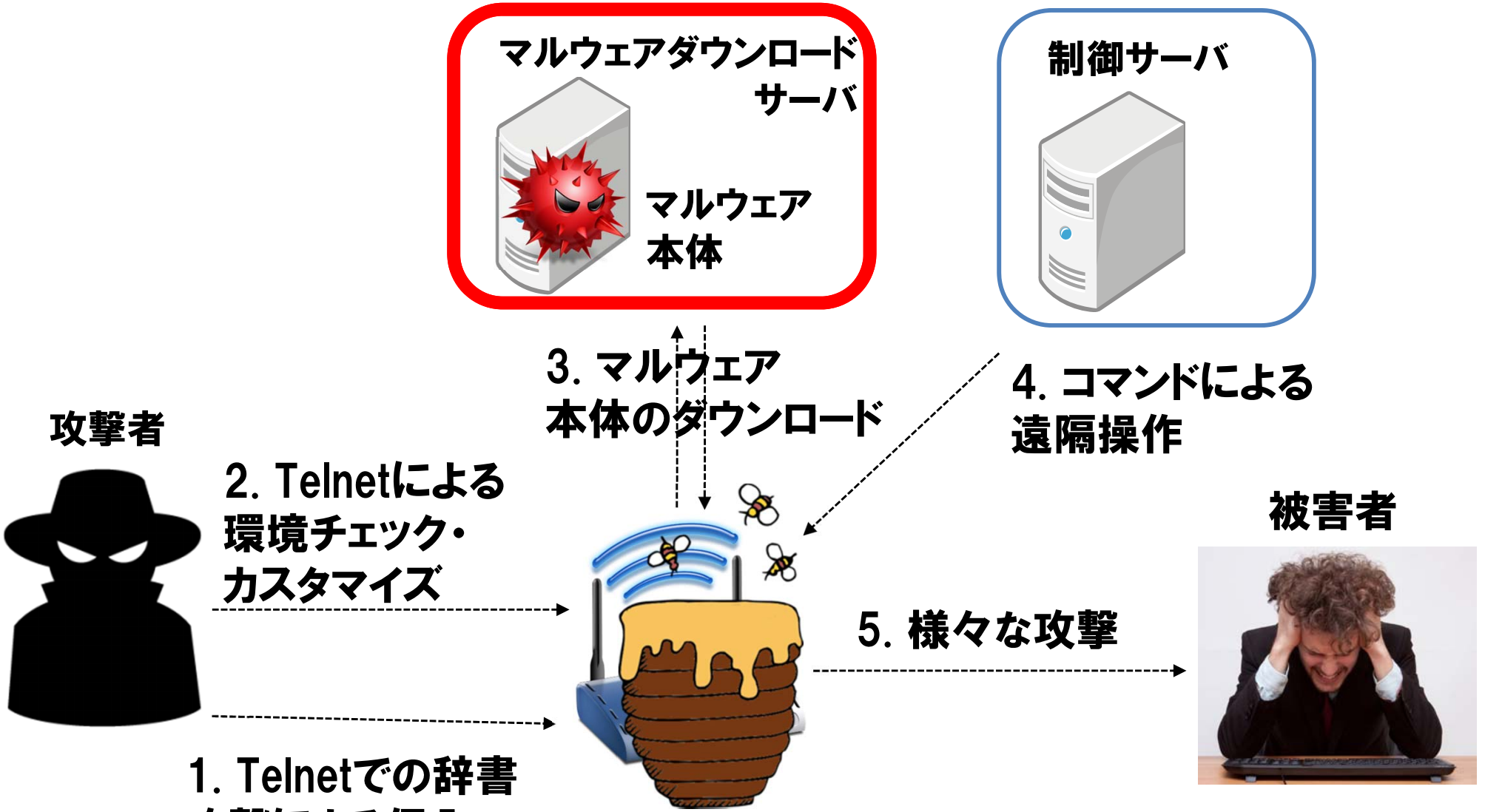


国別の感染状況

分析対象期間:2015/05/01 - 2016/02/21



Telnetベースのマルウェア感染の流れ



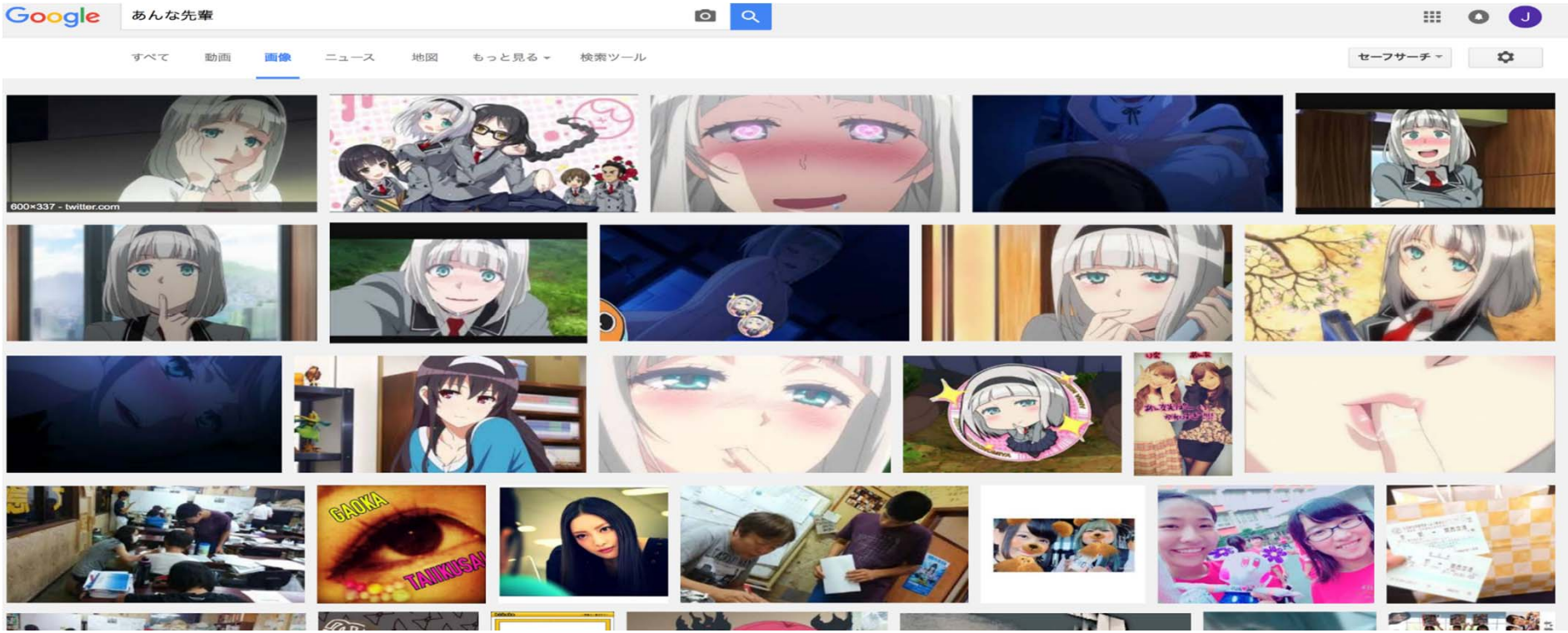
最近の事象
Mirai（IoTマルウェア）及び、その亜種について

最新IoT機器のマルウェア

- Mirai
  - telnetサービスを使って500,000以上のIoT機器に感染
  - 特徴は
    - 23/TCP，2323/TCPへスキャン
    - 辞書攻撃
    - スキャン先IPアドレスとTCPシーケンス番号が同一
    - 送信先，windowサイズ，送信ポートはランダム（多分）
  - 2016年9月にAnna-senpaiと名乗る人物がHackforumsにソースコードを公開（その後GitHubにも公開）

【余談】Anna-senpaiとは

- アニメ:「下ネタという概念が存在しない退屈な世界」
- 2015年7月より9月まで放送
  - –ATX(アニメ専門チャンネル)
  - –東京MX



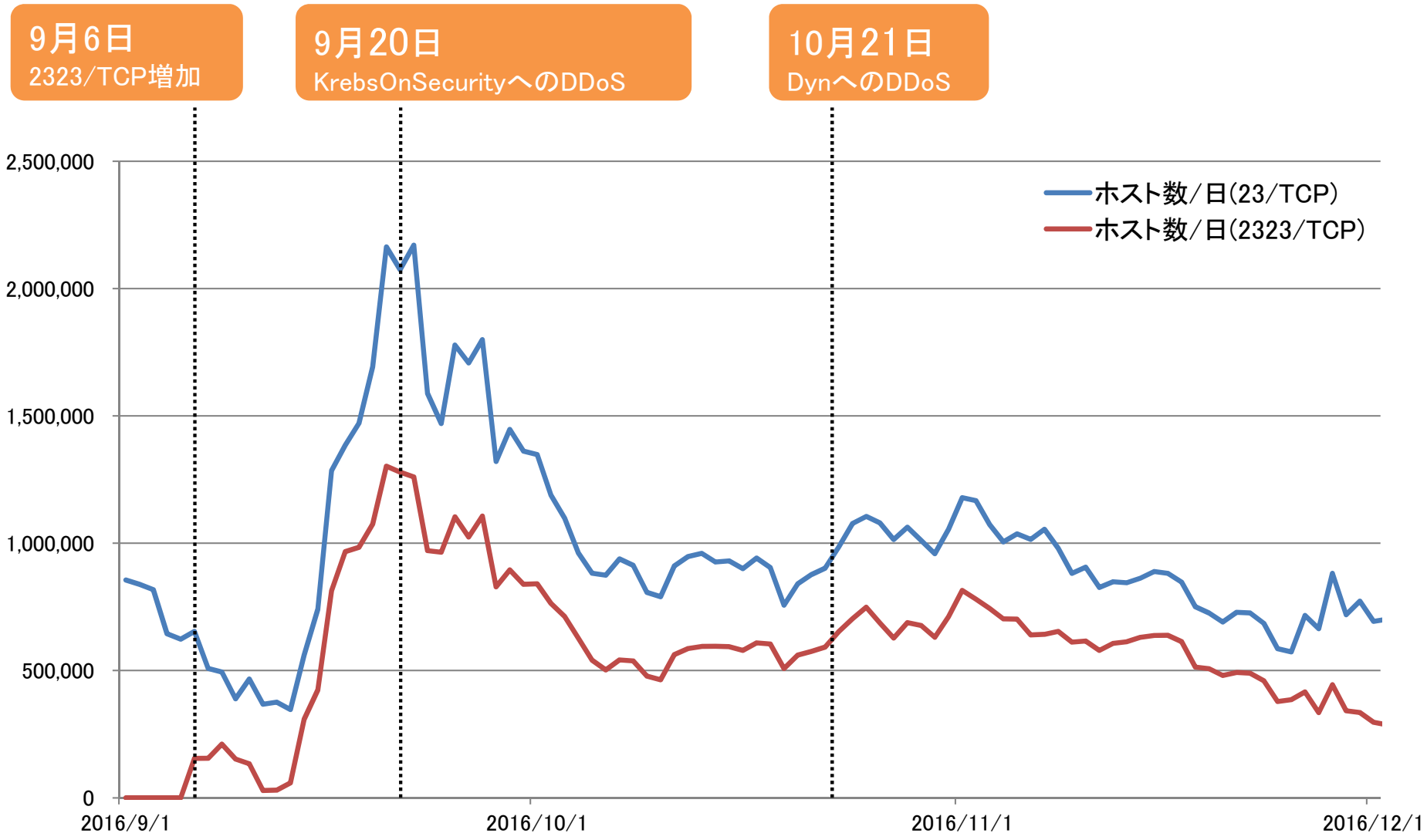
Mirai(2)

DDoS攻撃

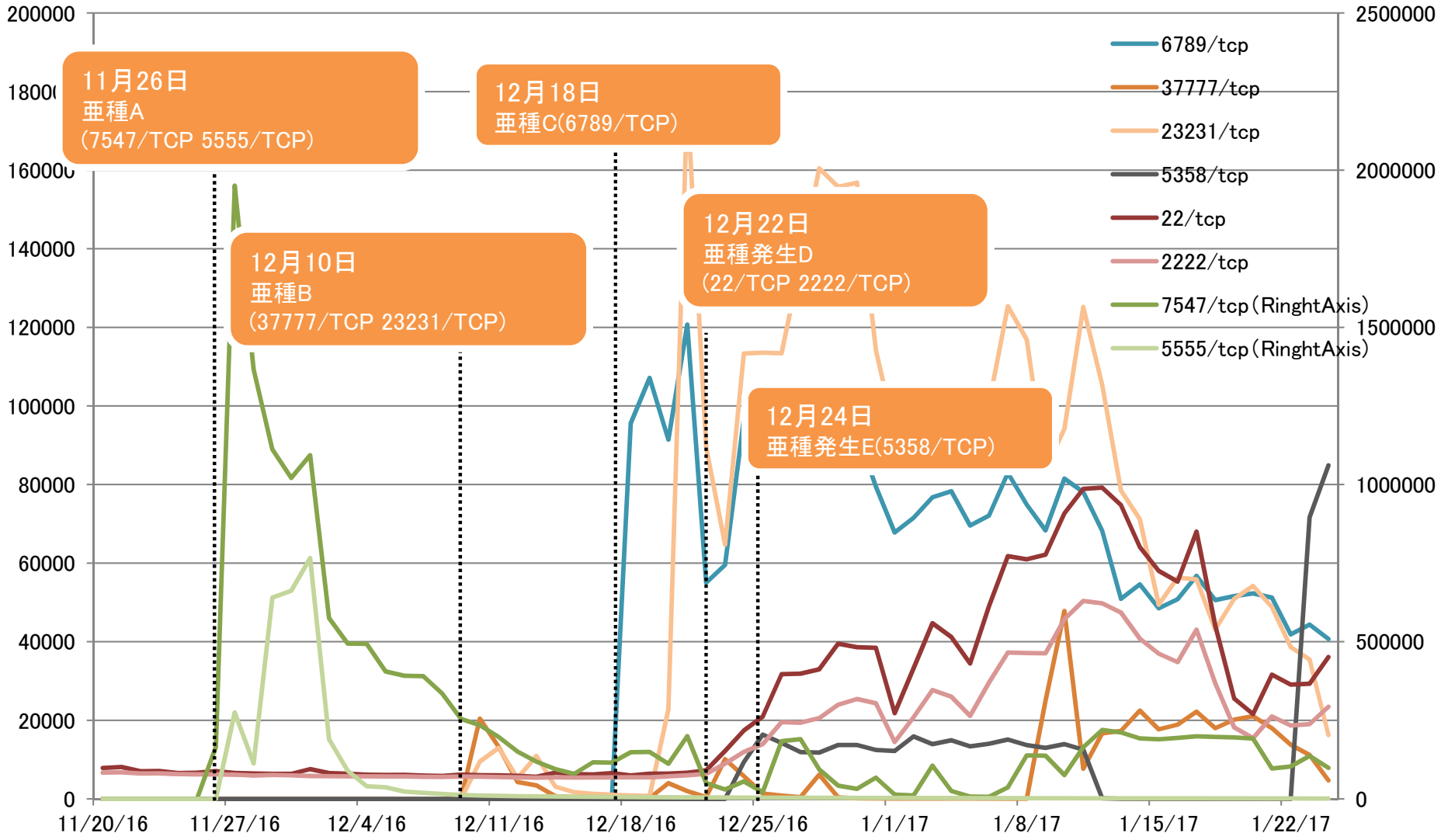
- Krebs on Security(16/9/20)
  - –Akamaiサービス
- DYN社DNSサーバ(16/10/21)
  - –Netflix
  - –Twitter
  - –Amazon

- 感染機器
  - –プリンタ
  - –カメラ
  - –ルータ
  - –DVR
- 対応アーキテクチャ
  - –ARM
  - –ARM7
  - –MIPS
  - –PowerPC
  - –SH4
  - –SPARC
  - –X86

ダークネットによるMiraiの観測状況



続々と登場するMirai亜種



続々と登場するMirai亜種

- NICTERWEB（www.nicter.jp）

Top 10 List

2017/01/19のデータを表示中

国別ユニークホスト数 Top 10

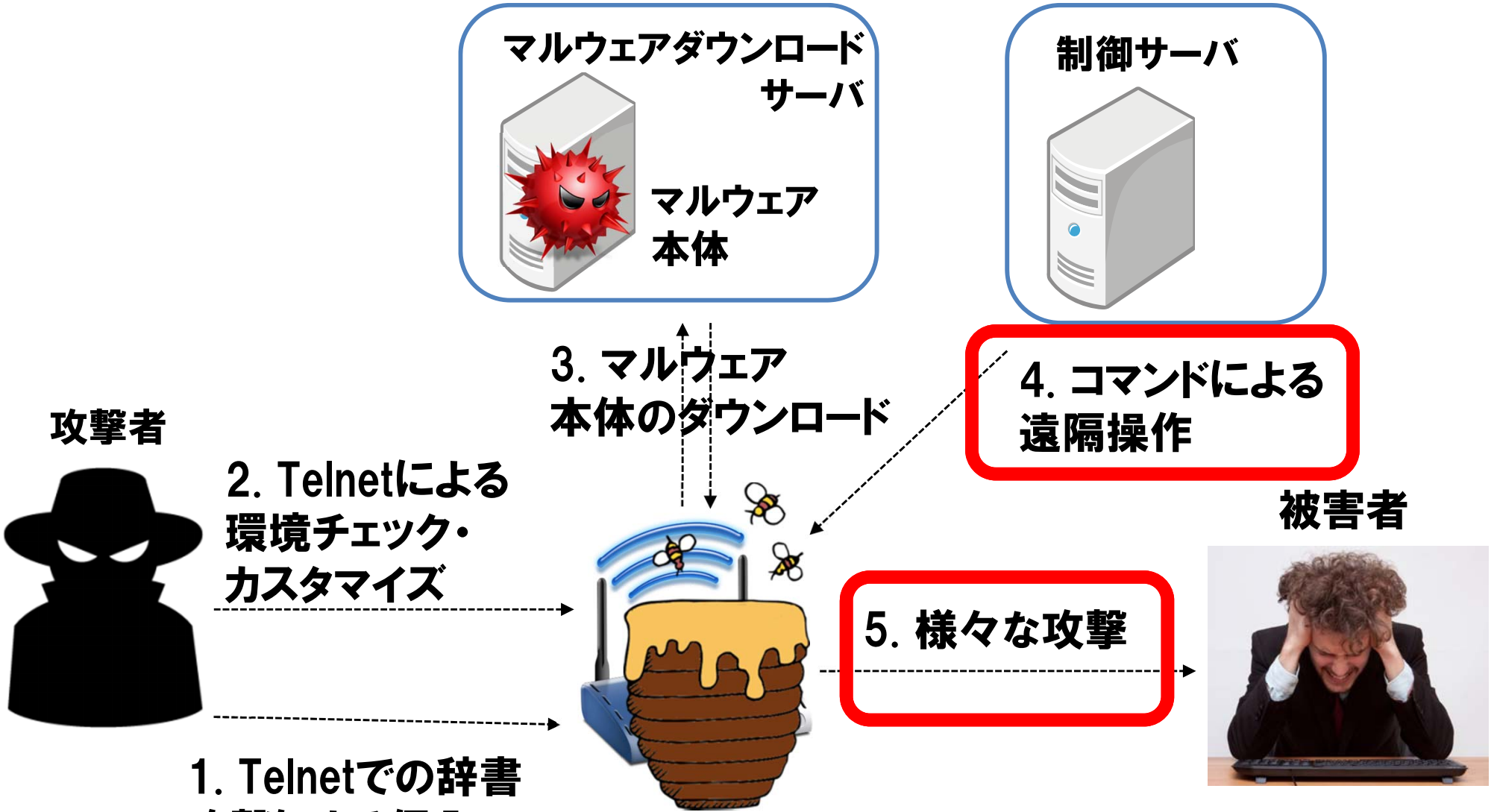
国名(国コード)	ホスト数	割合
中国(CN)	94,492	12%
イラン・イスラム共和国(IR)	83,082	11%
ブラジル(BR)	72,249	9%
インド(IN)	57,330	7%
ベトナム(VN)	48,019	6%
トルコ(TR)	35,665	5%
メキシコ(MX)	34,196	4%
ロシア連邦(RU)	33,234	4%
韓国(KR)	27,384	4%
イタリア(IT)	23,393	3%

TCP 宛先ポート別ユニークホスト数 Top 10

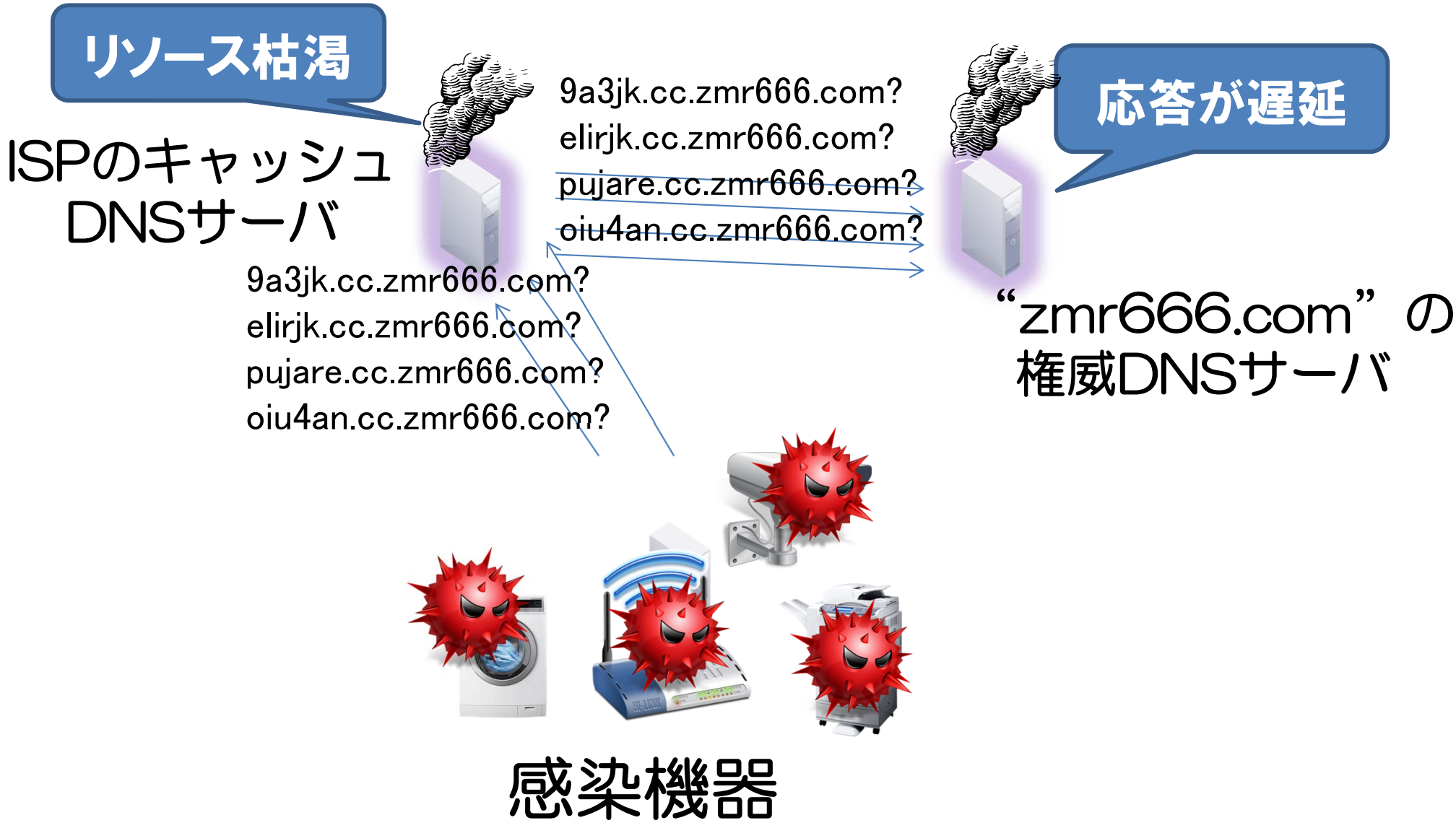
宛先ポート	ホスト数	割合	
23	554,795	38%	Mirai (9/6)
7547	169,985	12%	Mirai亜種 (11/26)
2323	134,841	9%	Mirai (9/6)
23231	46,333	3%	Mirai亜種 (12/10)
6789	45,351	3%	Mirai亜種 (12/18)
22	21,289	1%	Mirai亜種 (12/22)
37777	18,638	1%	Mirai亜種 (12/10)
2222	14,196	1%	Mirai亜種 (12/22)
21	10,814	1%	
80	8,147	1%	

すべて、“シーケンス番号＝宛先IPアドレス”の特徴をもつ

Telnetベースのマルウェア感染の流れ



サービス妨害攻撃への加担



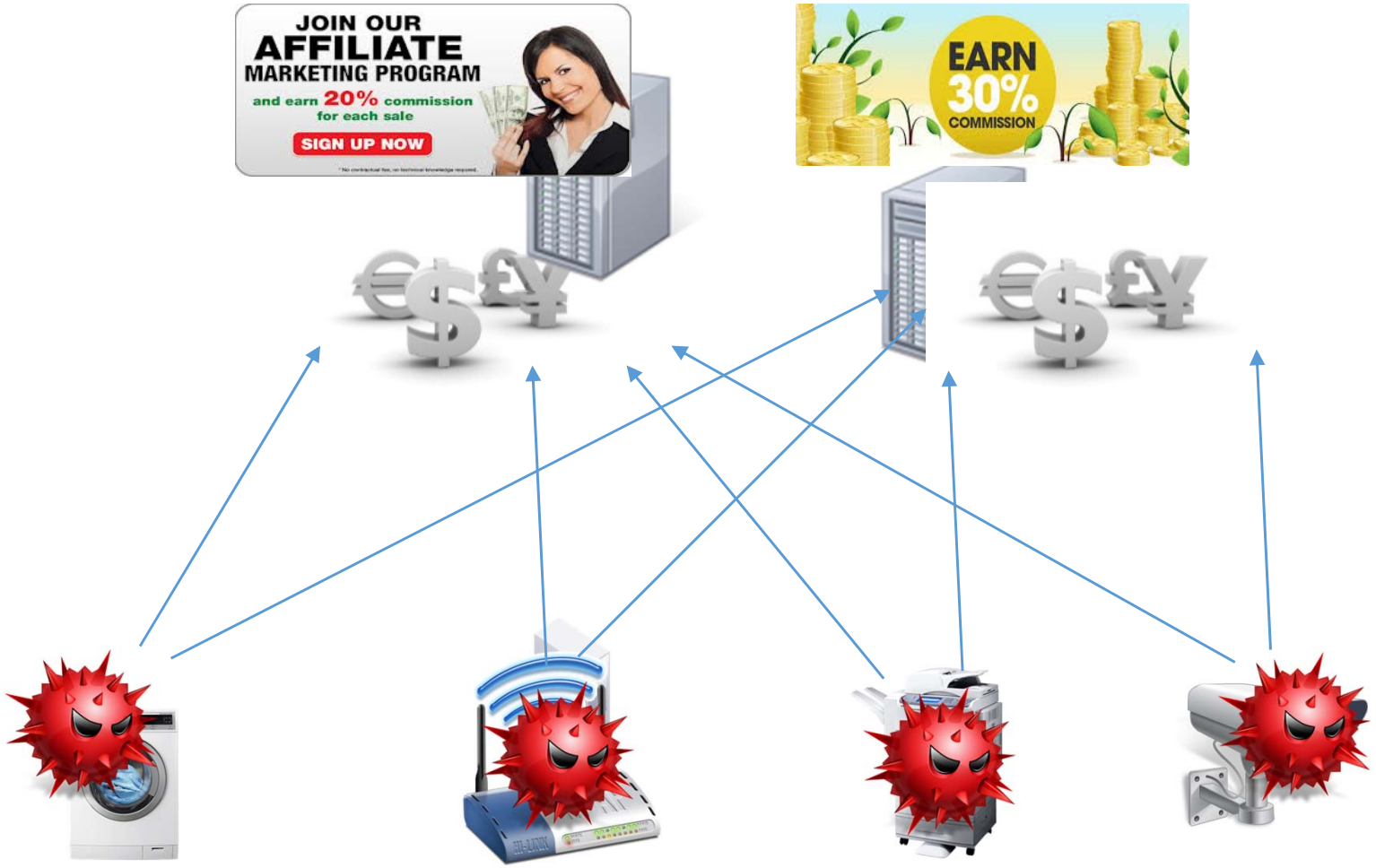
他の機器の探索・感染

同様のTelnetサービスが動作する機器を探索し感染を広める

感染機器

クリック詐欺(Affiliate)

感染機器が広告サイトへユーザクリックを模倣する



PPV(Pay Per View)の資格証明書(credential)を盗む

特定のセットトップボックス(set top boxes、dreambox等)が攻撃のターゲットになっている

感染機器の種別（2016.9時点）

- 監視カメラ等
  - IP カメラ
  - デジタルビデオレコーダ
- ネットワーク機器
  - ルータ・ゲートウェイ
  - モデム、ブリッジ
  - 無線ルータ
  - ネットワークストレージ
  - セキュリティアプライアンス
- 電話関連機器
  - VoIPゲートウェイ
  - IP電話







- 制御システム
  - ソリッドステートレコーダ
  - インターネット接続モジュール
  - センサ監視装置
  - ビル制御システム
- 家庭・個人向け
  - Webカメラ、ビデオレコーダ
  - ホームオートメーションGW
  - 太陽光発電管理システム
  - 電力需要監視システム
- 放送関連機器
  - 映像配信システム




ーダ
デコーダ
ス・アンテナ

国内メーカの機器の感染事例も複数確認
感染機器情報はJPCERT/CC，内閣サイバーセキュリティセンターに情報提供、または、メーカに直接情報提供済

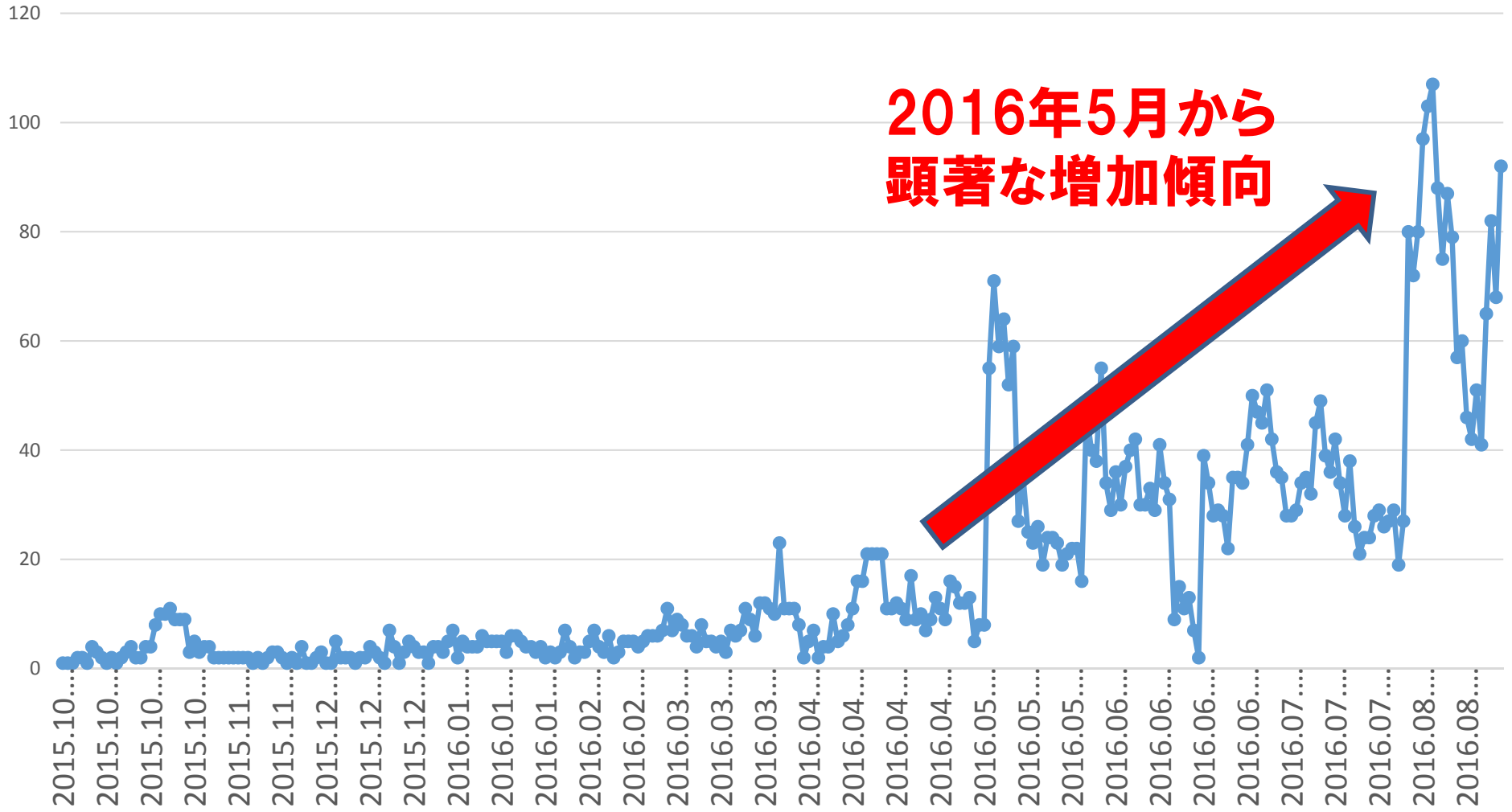


デバイスはWebおよびTelnetの応答から判断しています.

- ディスク型記憶装置
- 医療機器（MRI）
- 指紋スキャナ

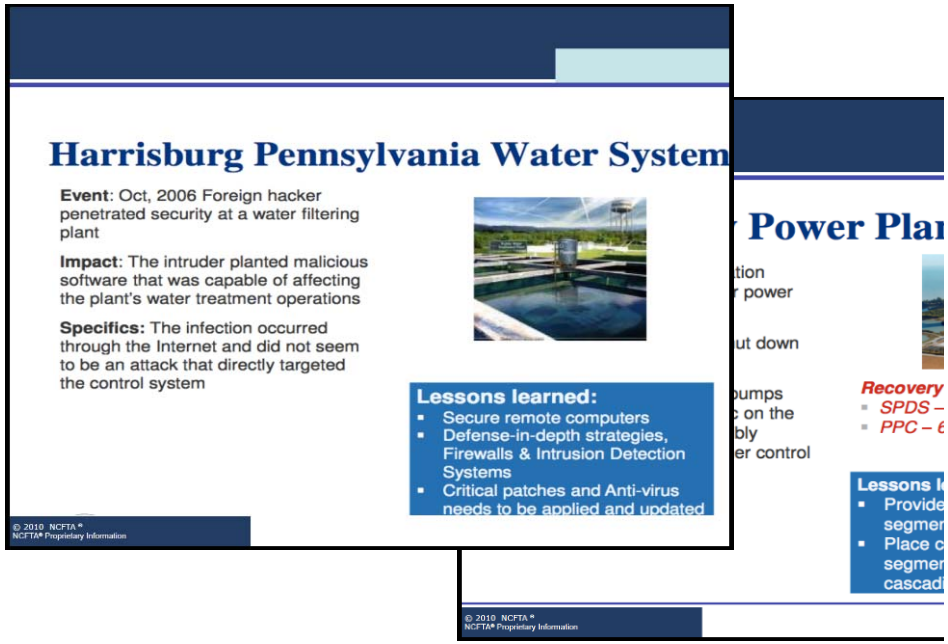
日本国内 感染機器台数（日毎にカウント）

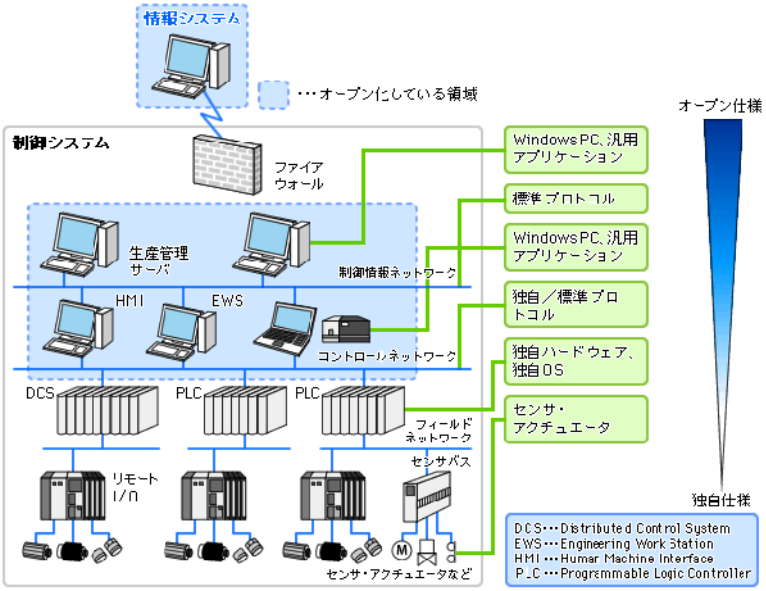
IPアドレス/日



その他の注目すべき脅威

- ランサムウェア、またはランサム活動
- 環境の変化に関係する脅威（BigData, Cloud　Computing・・・）
- 重要インフラに対する脅威





サイバーセキュリティ対策の方向性

－ まとめ －

サイバーセキュリティの構成要素は？

1. サイバーにおける技術的な要件

・既存の技術：境界防御、AVなど
・研究的視点（AIの活用）、日本独自の成果発掘
・イベントベース、観測→分析→対策のプロセスサイクル→知識蓄積

2. サイバーにおける運用的な要件

・ガイドライン化による運用精度向上
・他ステークフォルダー（ISP等）との連携による運用向上

3. サイバーにおけるシステム的な要件

・システムの脆弱性診断
・脅威・攻撃の研究とシステム診断、認定

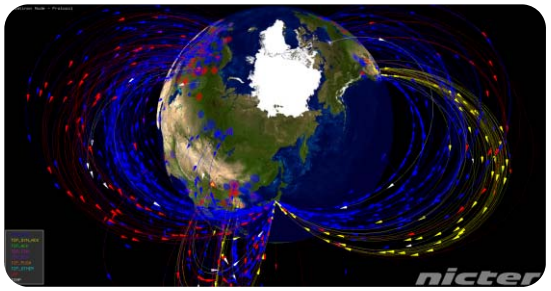
4. サイバーにおけるマネジメント的な要件

・脅威分析、ポリシー策定、対策整備・実施、効果測定。対策改善のサイクル

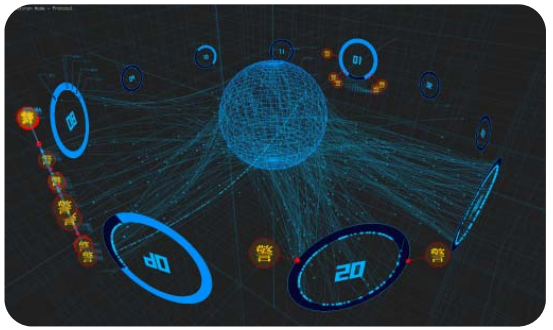
5. サイバーにおける法制度など整備に関する要件

nicterとそのスピンオフ技術たち

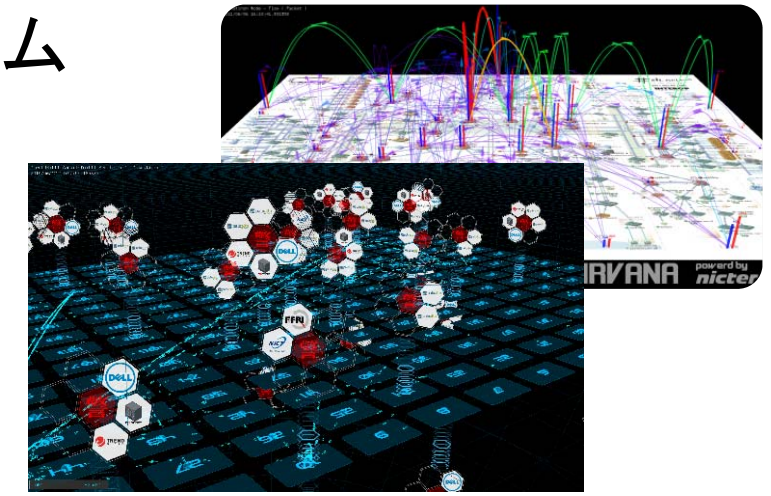
1. インシデント分析センター
   nicter



2. 対サイバー攻撃アラートシステム
   DAEDALUS



3. ネットワークリアルタイム可視化システム
   NIRVANA、NIRVANA改



ご静聴、ありがとうございました。