通信の秘密とサイバーセキュリティ対策

2014年7月3日

テレコム・アイザック推進会議 会長
(株)ぐるなび　副社長
東京工業大学　客員教授

飯塚　久夫

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

本日のポイント

- 日本では、9.11事件が起きた後の米国事情も参考にして、2002年、主要通信事業者によって“テレコムISAC”が発足した。
- 特に2006年からはサイバー・クリーン・センター(CCC)をISAC内に設置し、2010年には日本が世界で最もウィルス感染率の低い国になった。
- しかしその後、日本でも新たなサイバーセキュリティ問題は深刻化する一方である。その実態例を概観してみよう。
- さらに、一昨年、サイバー事件でありながら、逮捕・立件は「偽計業務妨害罪」「ハイジャック防止法違反」とならざるを得ない事態(いわゆる“誤認逮捕事件”)まで起きた。
- 深刻化するセキュリティ問題に対処するには、ある日本的発想法・価値観の変化が必要かもしれない。
- サイバー攻撃に対処する場合の通信の秘密との関係についても、事業者の立場で検討を行い、総務省の研究会/WGに報告をした。
- 以上のことを、通信事業特有問題および社会論の視点から考察する(私見も多いがご容赦を！)

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

Telecom-ISAC Japanの概要

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

https://www.telecom-isac.jp/

- 2002年7月に日本で最初のISACとして発足
- 通信事業者の商用サービスの安全かつ安心な運用の確立を目的に、テレコム通信事業者を含む会員が関連情報を共有分析し、業界横断的な問題に対してタイムリーな対策をとる場を提供する活動を行う
- 世界に広がるサイバー空間の中で、「日本(jpドメイン)」が消失しないようサイバー脅威からネットワークを守る
- 事業者単独では手に負えない大規模なサイバー脅威に共同で立ち向かう「互助会型」の通信事業者連携
- ビジネス競合関係にある国内大手ISPが、会社の壁を越えて協力・連携するための会費会員制の民間組織

会員企業

赤文字はISPor通信事業者を示す

会長: 飯塚　久夫

副会長: NTT コミュニケーションズ株式会社、ニフティ株式会社、一般財団法人日本データ通信協会

会員企業: 日本電気株式会社 、NTTコミュニケーションズ株式会社 、KDDI株式会社 、株式会社NTTドコモ、株式会社インターネットイニシアティブ 、ニフティ株式会社、株式会社日立製作所、沖電気工業株式会社 ソフトバンクBB株式会社、東日本電信電話株式会社、西日本電信電話株式会社、日本電信電話株式会社 株式会社KDDI研究所 、ビッグローブ株式会社 、富士通株式会社 、インターネットマルチフィード株式会社 NTTコムテクノロジー株式会社 、エヌ・ティ・ティ・データ先端技術株式会社 、ソネット株式会社

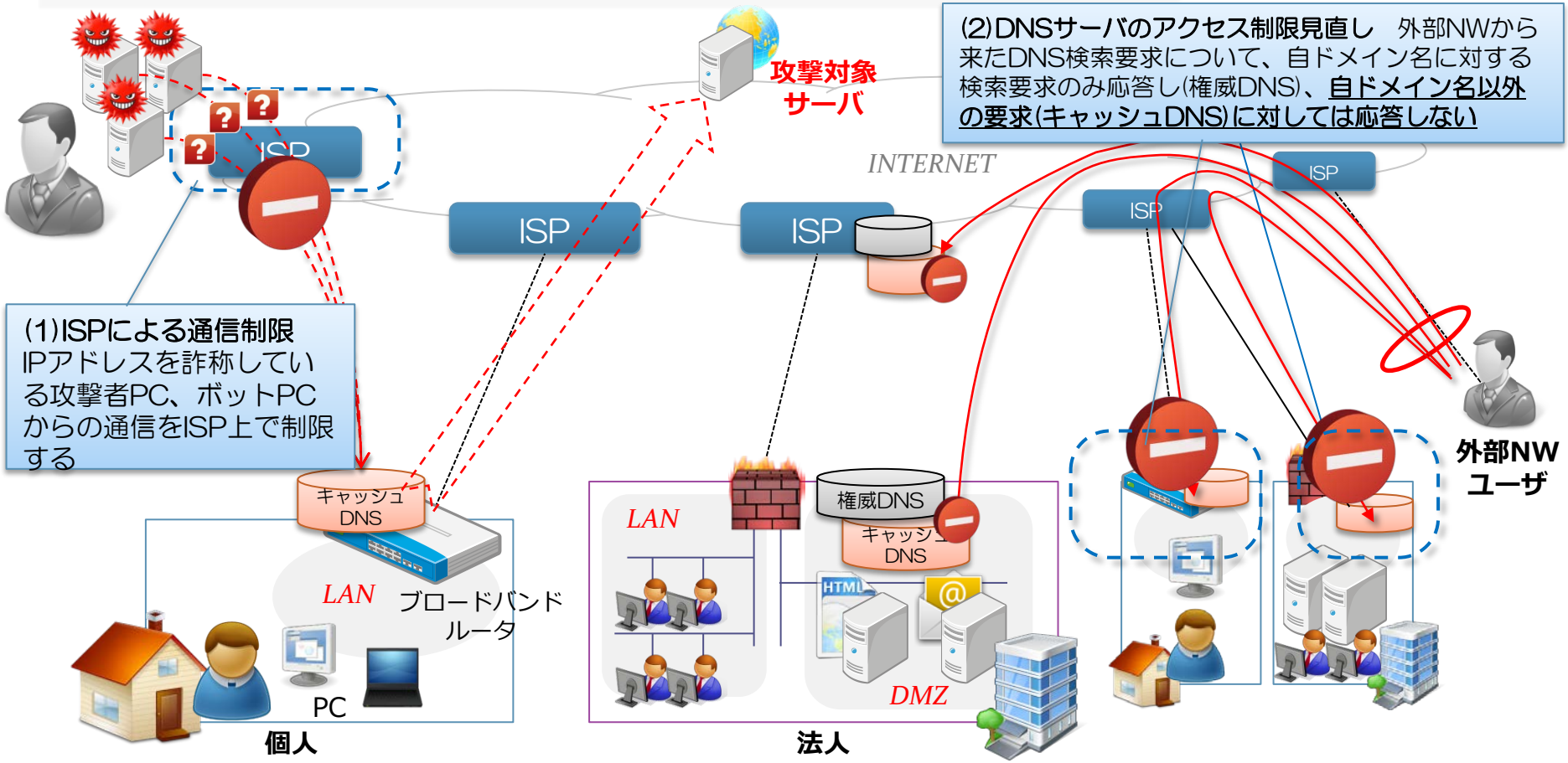
アライアンスメンバー: 株式会社ラック 、日本アイ・ビー・エム株式会社、トレンドマイクロ株式会社 マイクロソフト株式会社 、株式会社サイバーディフェンス研究所 株式会社FFRI、株式会社情報通信総合研究所 一般社団法人日本ネットワークインフォメーションセンター 、BBIX株式会社 日本インターネットエクスチェンジ株式会社、NRIセキュアテクノロジーズ株式会社

オブザーバー: 総務省、独立行政法人情報通信研究機構(NICT) 一般社団法人日本インターネットプロバイダ協会(JAIPA) 一般社団法人テレコムサービス協会、一般社団法人電気通信事業者協会(TCA)

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

大規模攻撃に対する事業者間の協調対処の必要性

非常に大規模な攻撃に対して1組織が単独で行える有効な手立てはない。
ISP・通信キャリア・DNS事業者・SOC事業者等の協調対処が必要になる。



一方、問題の根絶のためにはユーザ・端末側のセキュリティ対策向上が必須であり、
- **NW機器の脆弱性問題対応**
- **ユーザのセキュリティ・リテラシの向上、基本動作の徹底・励行**
- **PC/サーバのセキュリティ対策**(セキュリティ設定の強化、運用手順の見直し)

は喫緊の課題と言える。

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

Telecom-ISAC JapanのWG/SiGの設置状況

WG

1-1) ACCESS-WG　2007年4月設置
インターネットアクセスNWサービスの運用品質向上のための情報交換、ベストプラクティス共有や有識者を交えた意見交換

1-2) SoNAR-WG　2007年12月設置
ネットワークを利用した不正・不法行為対応(ABUSE対応)に関する情報の共有。インシデントの拡大を抑止するフレームワークの策定

1-3) DoS攻撃即応-WG　2011年10月設置
DoS攻撃への迅速な対応と複数事業者による協調対処の仕組みの検討。日本国内におけるDoS攻撃発生の、予測、早期検出、迅速かつ適切な対応の実現を目指す。

1-4) ルータ脆弱性問題-WG　2012年07月設置
危険な脆弱性を保有する特定ルータに対する具体的な対応の検討と調査を実施

1-5) 脆弱性保有ネットワークデバイス調査-WG　2013年05月設置
国内IPに接続されたネットワークデバイスの脆弱性保有状況の全容把握と調査を実施

1-6) サイバー攻撃への適正な対処検討のためのWG(仮称)　2013年12月設置
電気通信事業の業務を整理し通信の秘密に代表される法的な整理を行うことを目的とする

3-1) 経路情報共有-WG　2005年7月設置
ISP間の経路情報の共有、経路情報異常時の迅速な対応。および経路奉行システムの運用

4-1) サイバー攻撃即応スキーム検討WG(国際サイバーWG)　2011年12月設置
マルウェアやDDoSなどの様々なサイバー攻撃情報をISP間およびセキュリティ関連機関と共有し、予知・即応可能なサイバー攻撃対応スキームを検討

4-2) ACTIVE業務推進-WG　2013年07月設置
総務省ACTIVEプロジェクトの施策推進。マルウェアの感染防止、駆除を推進し、より安心・安全なインターネットの実現を目指す

4-3) WiFiリテラシー向上-WG　2013年09月設置
電波の有効利用(オフロード推進)を目的に、WiFiの利用および設置・運営において障壁となる情報セキュリティ課題の検討、対策の実施

6-1) サイバー攻撃対応演習-WG(CAE-WG)　2009年5月設置
電気通信事業者等の参加する、サイバー攻撃を想定した対応演習の企画、実施

SiG

DNS運用者連絡会-SiG　2008年6月設置
DNSに関わる、脆弱性対応・情報の共有、DNSSEC化に備えた情報交換

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

サイバー攻撃の推移と具体例

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

安心・安全なインターネット社会の実現を目指して

Telecom-ISAC Japanは安心・安全なインターネット社会の維持・発展のため、総務省支援の下、様々なプロジェクトを進めています。

マルウェアの変遷

より高度で多様なマルウェア

より高度で多様なマルウェアが次々と出現

Webを見ただけで感染するWeb感染型マルウェアが台頭

Drive-by-download

ボット

インターネットにつないだだけで、インターネット利用者の知らない間に感染する
ボットが主流

国際的な連携体制を構築。
海外からのサイバー攻撃情報を収集し、攻撃の予兆を捕捉。

総務省支援によるTelecom-ISAC Japanの活動

ACTIVE 2013～2018

マルウェア感染防止・駆除の取り組み

通信事業者・セキュリティベンダと連携し、マルウェア配布サイトのブロッキングによる感染防止や感染PCの注意喚起・駆除を行い、ネット環境の安全・安心を実現する

PRACTICE 2011～2016

国際連携によるサイバー攻撃予知・即応システムの実証実験

国際連携の下、様々なサイバー攻撃情報を収集・分析し、予知・即応する実証実験

RDB 2009～2012

マルウェア配布等危害サイト回避システムの実証実験

Webをみただけで感染するマルウェアから国民を守るため、マルウェア配布サイトをリスト化し、インターネット利用者が危害サイトにアクセスするのを防ぐ実証実験

Cyber Clean Center 2006～2011

ボット対策プロジェクト

インターネットにつないだだけで感染し、感染端末が悪意のある第三者に利用され、被害が発生するのを防ぐ活動
ISPと連携してボットを駆除

Telecom-ISAC Japanがサイバー攻撃対応に取組む背景

マルウェア作成配布の背景	マルウェア感染手法の変化	現在の社会状況
愉快犯目的から金銭目的へ変化	より高度で複雑な攻撃手法の出現	あらゆる社会活動がインターネットに依存

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

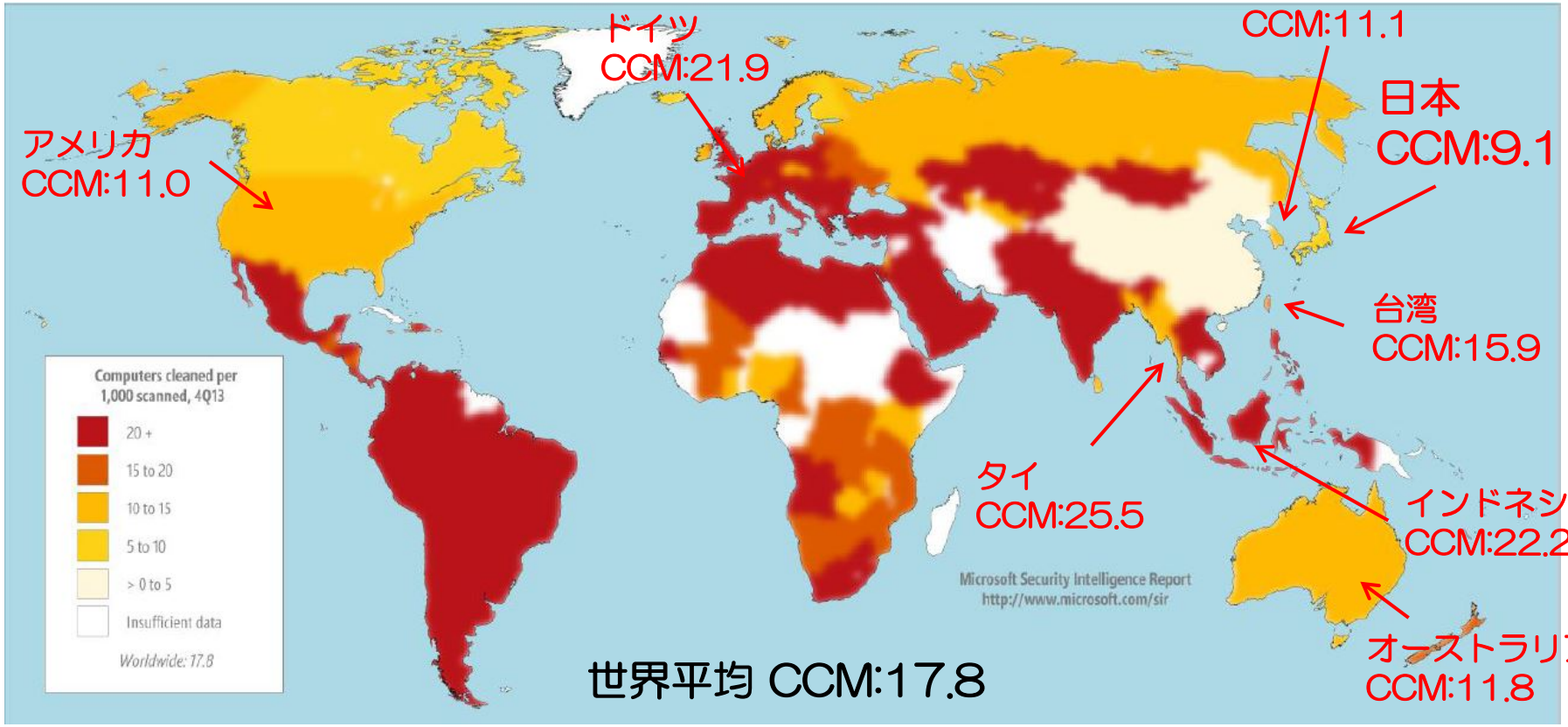
日本におけるマルウェア感染率は低下している

日本におけるマルウェアの感染率は、他国と比較すると低い

マイクロソフト セキュリティ インテリジェンス レポート第16版

2013年4Qの世界各地のマルウェア感染率

-Computers cleaned per mille (CCM) は、悪意のあるソフトウェアの削除ツール (MSRT) を実行している 1,000 台の一意のコンピューターのうち感染が除去されたコンピューターの台数として定義されている、感染率の指標



http://www.microsoft.com/ja-jp/security/resources/sir.aspx

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

しかし、次なる対策が必要

- 様々なサイバー攻撃手法が日々開発され、防御側は既存の対策では対応が難しくなっている
- サイバー攻撃被害を最小限に留めるため、サイバー攻撃を予知・即応できる仕組みの必要性が指摘されている
- サイバー攻撃は国境を越えて行われるが、現行法制度下では国外のサイバー攻撃を止めることは難しい
- こうした中、様々なレベル（事業者間、業界、官民、国際）での連携の必要性が提起されているが、具体的にどのような情報をどのレベルでどのように共有し、どのような連携をするのが効果的であるかは　まだ課題が残されている

まず、様々なサイバー攻撃を把握し、情報を共有することが基本！

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

近年のサイバー攻撃の発生状況

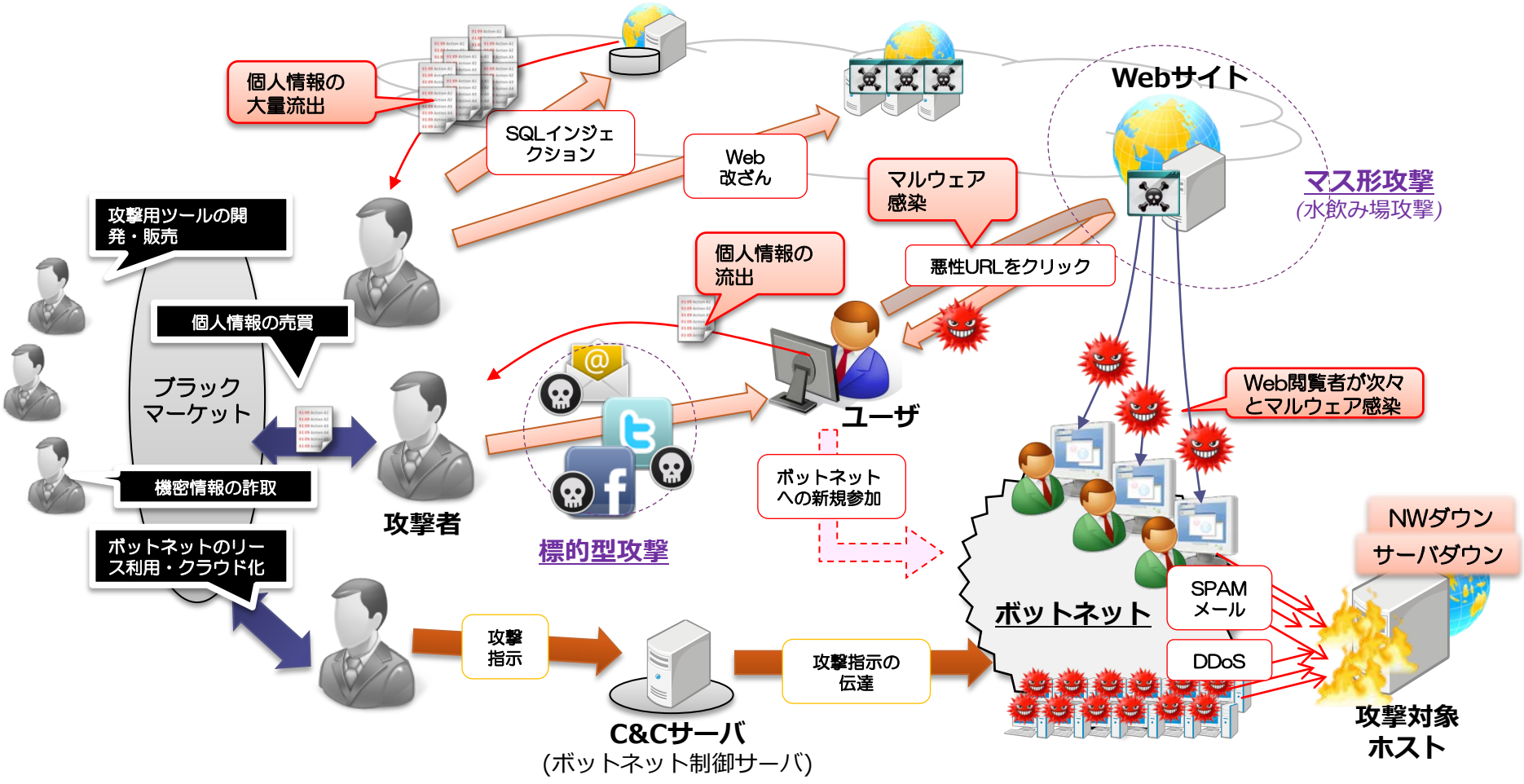
	2011年	2012年	2013年	
インシデント	・4月　SONY アノニマスによる大規模な抗議活動によるWeb閲覧停止 1億人超の個人情報流出	・6月　政府系Webサイト 違法ダウンロード罰則化抗議活動による改竄、閲覧停止	・3月　韓国内の銀行・放送局 3万台超のPC/サーバダウン	・1月　BaiduIME問題 クラウド型IMEによるユーザの意図しない情報漏洩の危険性
	・7～11月　衆参議院 標的型攻撃による情報漏洩	・9月　公共機関等Webサイト 尖閣諸島問題によるWeb改竄・閲覧停止	・3月　Spamhause DNSリフレクション攻撃による最大300Gbps超の大規模DoS攻撃	・2月　CloudFlare社顧客 NTPリフレクション攻撃による約400Gbps大規模DoS攻撃
	・9月　三菱重工 国家防衛機密漏えい事件	・10月～　各金融機関 ネットバンキングを中心に不正送金・出勤事件の多発	・5月～　Web改ざん多発 トヨタをはじめ、多数の国内Webサイトが改ざん被害	・4月　Y社等ルータ通信障害 海外からの不正パケット流入によるルータ故障発生
			・6月～ ネット銀行不正送金被害 マルウェア感染によるネット銀行利用者の不正送金被害が多発	
			・7月～ ISP会員向けサイト 不正アクセスにより約2万件超の会員情報流出の可能性	・5月～ mixi・LINE・はてな等 SNS等会員向けサイトにおいて大量不正ログインや一部金銭被害
攻撃傾向	ハクティビズムの台頭、攻撃者の組織化	マルウェア生成/攻撃ツールの充実によるサイバー攻撃のコスト低減・多様化		
	国家/競合企業間の情報戦争、標的型攻撃の増大	踏み台NW機器を利用したDDoS攻撃の大規模化	金銭目的の攻撃増加	

サイバー攻撃には大きく、DoS攻撃やWeb改ざん等示威行為に代表される**ハクティビズム**目的の攻撃と、国家/競合企業の機密情報や銀行口座/クレジットカード情報等の個人情報の**情報漏洩・詐取**といった**営利目的**の攻撃がある。攻撃手法はますます多様になっており、**標的型攻撃**による特定ターゲットへの攻撃が顕著になる一方で、マルウェア感染の拡大を狙う大量のSPAMメールや水飲み場攻撃などの**マス型攻撃**も続いており、またリスト型攻撃による**大量不正ログイン**被害も目立つ。ネット銀行不正送金や不正ログインによる金銭被害など**金銭目的**の攻撃も顕著になっている。

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

サイバー攻撃は広範、多岐に渡る

サイバー攻撃の高度化、多様化の背景として攻撃者の組織化、ブラックマーケットを介した個人情報売買の市場拡大、攻撃ツール・ボットネットの売買などが挙げられる



攻撃者側にとっての環境が充実したことによって、特別な知識を持たずともDoS攻撃やマルウェア作成ができるようになり、今日の多様なサイバー攻撃が生まれている

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ネットバンキング不正送金被害発生状況

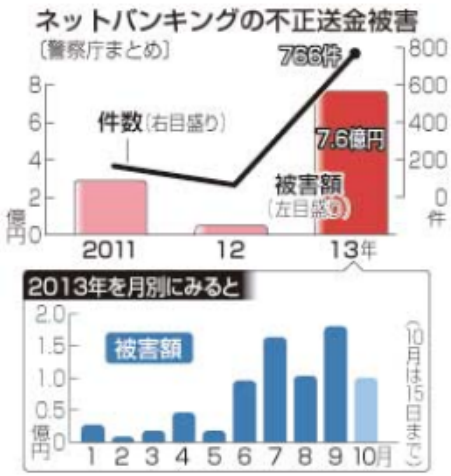
2013年10月15日時点の警察庁発表によると、ネットバンキング不正送金による被害が2013年1～10月の間に766件、約7億6千万円に上ったという。6月に急増した後に高い水準が続いており、過去最多だった2011年の約3億800万円の2．5倍にまで膨らんだ。

ネット銀被害7億円＝最悪11年の2．5倍－さらに拡大の恐れ・警察庁

警察庁は18日、インターネットバンキングで利用客のIDやパスワードが盗み取られ預貯金を不正に送金される事件の被害が、1月から今月15日までに約7億6000万円になったと発表した。被害は6月に急増した後、高い水準が続いており、過去最多だった2011年の約3億800万円の2．5倍に膨らんでいる。

不正送金の件数は15日時点で766件。11年の4．6倍に上る。今年は5月まで7～39件だったが、6月111件、7月194件、8月130件、9月150件で推移。今月も既に70件あり、5カ月連続で100件を上回るペースだ。

被害額は6月に約9580万円、7月以降は1億円を超え続けている。



被害者は、ゆうちょ、みずほ、楽天、三菱東京UFJなど19銀行の客で、地方銀行も9行ある。客の居住地は44都道府県に及んでいる。

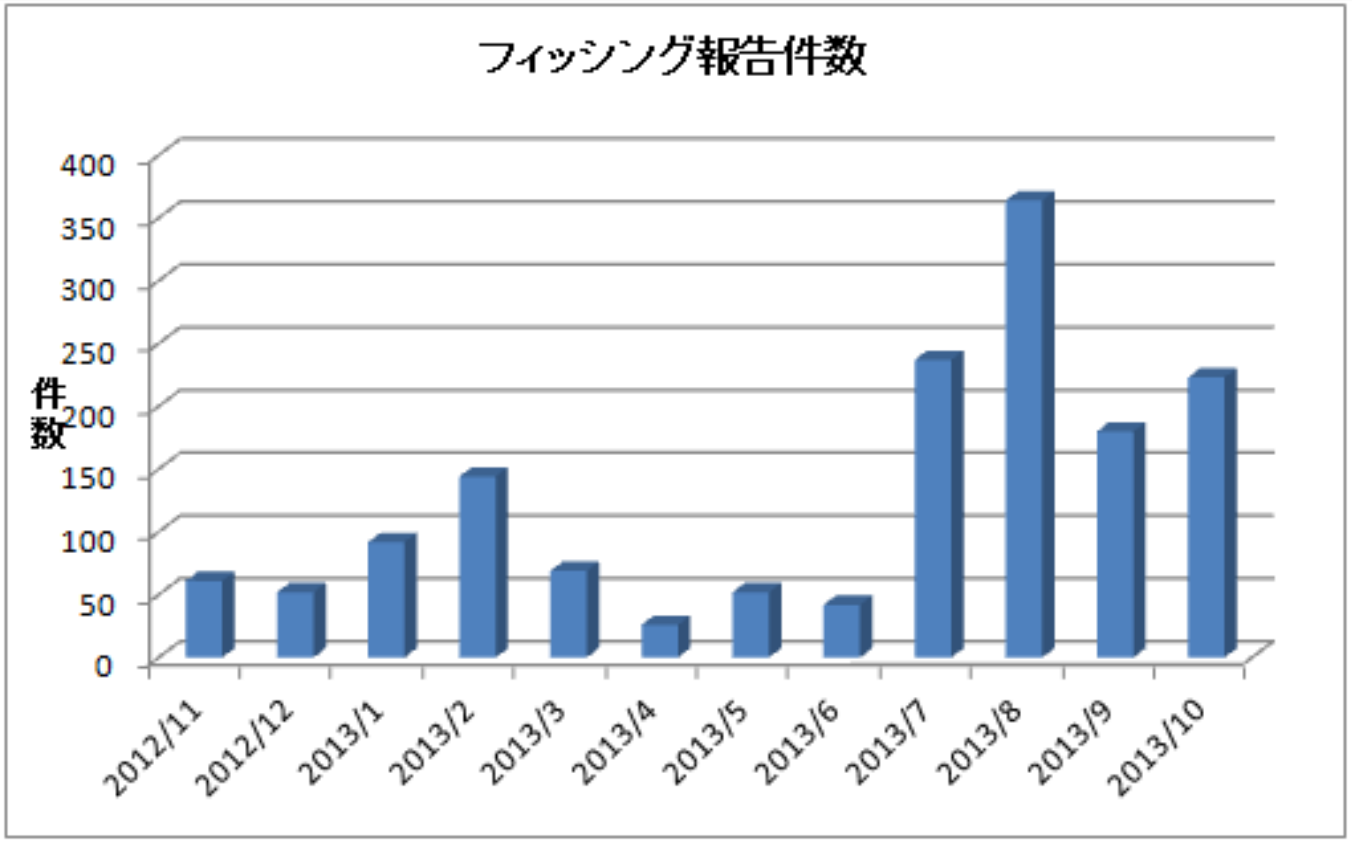
不正送金は利用客のパソコンをウイルス（不正プログラム）に感染させ、取引に使うIDとパスワードを盗んだ上で行われる。警察庁は「犯人がウイルスを仕込み終えて不正送金の機会をうかがっているパソコンが相当数あり、被害がさらに膨らむ恐れがある」とみている。（2013/10/18-19:08）

(出典) 時事ドットコム http://www.jiji.com/jc/zc?k=201310/2013101800537

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

フィッシング詐欺被害発生状況

ネットバンキング不正送金事案と並行して、従来のフィッシング詐欺も引き続き猛威をふるっている。



(参考)
https://www.antiphishing.jp/report/monthly/201310.html

フィッシング協議会の報告では、2013年7月以降とくに高い水準でフィッシング被害が報告されており、従来の金融系サイトのほか、クレジットカード・オンラインゲーム・その他サービスサイトを対象としたフィッシング詐欺が増えており、被害が拡大している。
現在、利用者が複数のオンラインサービス上でID/パスワードを使いまわす特性を利用したリスト型攻撃が流行していることもあり、フィッシング詐欺件数の上昇傾向はオンライン事業者全体の課題として認識する必要がある。

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

被害発生状況（フィッシング詐欺）

時期	経過
2013/12/27	三菱東京UFJ銀行をかたるフィッシング
2014/1/16	大学などで使用されているWebメール(Risumail)アカウントを狙うフィッシング
2014/2/6	セゾンNetアンサーをかたるフィッシング
2014/2/6	eoWEBメールをかたるフィッシング
2014/2/17	OMC Plus をかたるフィッシング
2014/2/17	ハンゲームをかたるフィッシング
2014/2/20	ゆうちょ銀行をかたるフィッシング
2014/3/25	NCSOFTをかたるフィッシング
2014/4/1	ゆうちょ銀行をかたるフィッシング
2014/4/15	お名前.comをかたるフィッシング
2014/4/30	三井住友カードをかたるフィッシング
2014/5/8	スクウェア・エニックス(FINAL FANTASY XIV)をかたるフィッシング
2014/6/10	三菱東京UFJ銀行をかたるフィッシング
2014/6/11	スクウェア・エニックス（ドラゴンクエストX）をかたるフィッシング
2014/6/16	りそな銀行をかたるフィッシング

（参考）フィッシング対策協議会 https://www.antiphishing.jp/news/database/

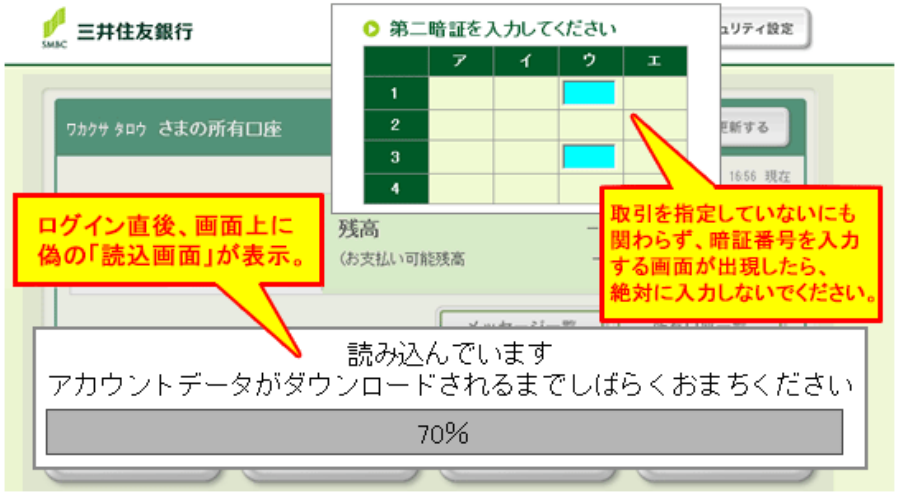
Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

偽装ポップアップ画面例

三菱東京UFJ銀行、三井住友銀行、みずほ銀行などで正規ホームページへの
ログイン過程において下記のように「暗証番号（コード）」や「秘密の合い言葉」の入力
を促す偽装ポップアップ（警告画面）が表示される

(三菱東京UFJ銀行)

(三井住友銀行)

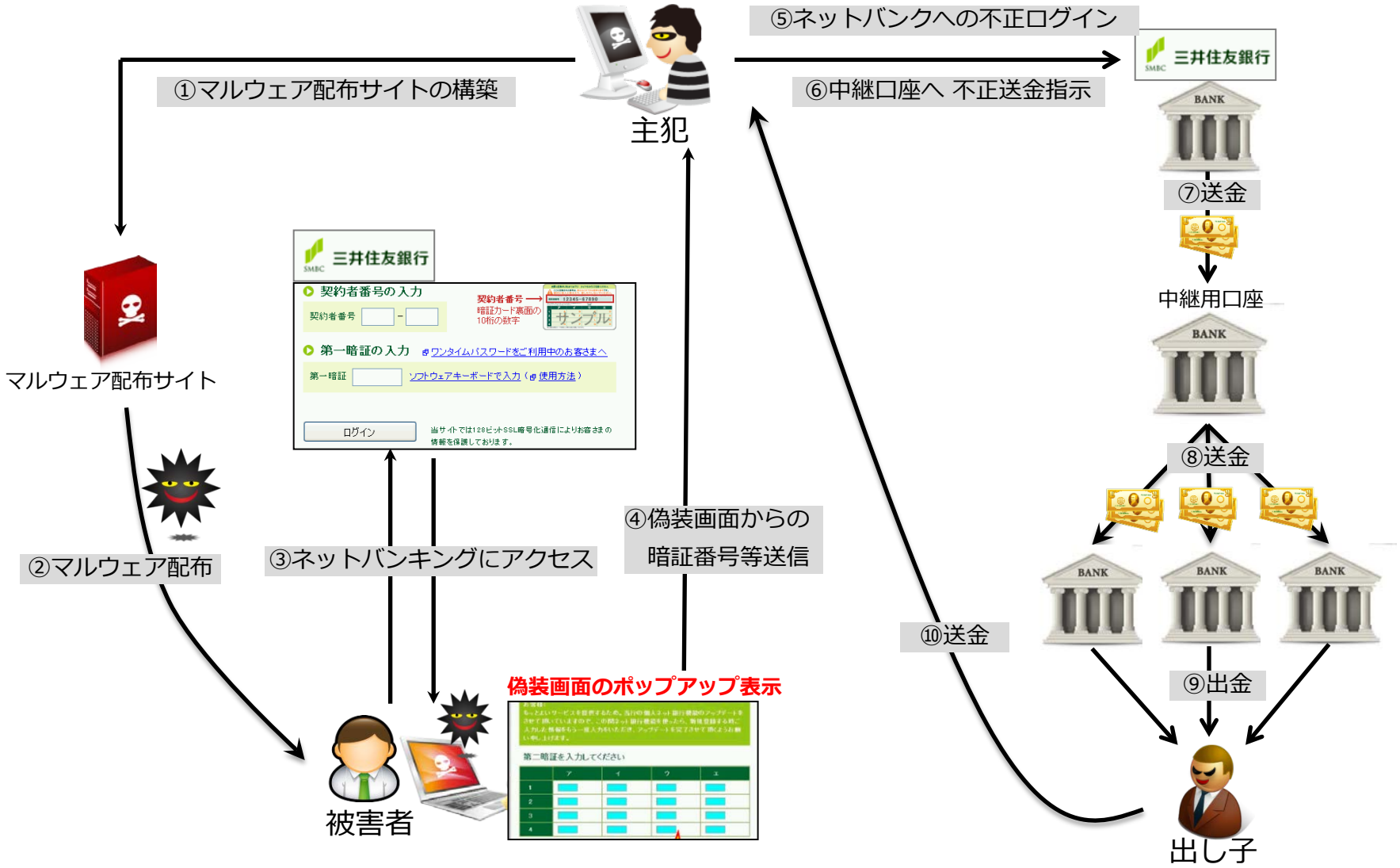


(みずほ銀行)

被害拡大防止のために、各行ともにログインまでに表示される正規の画面遷移について解説している

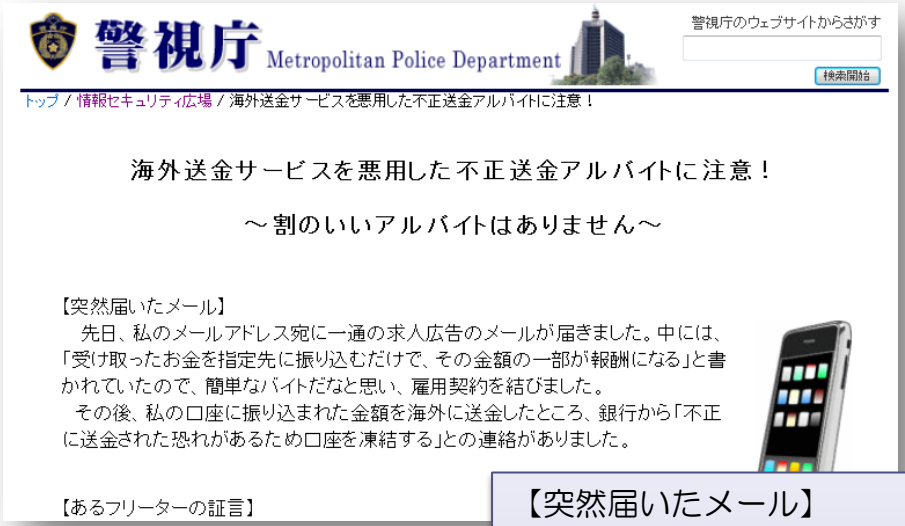
Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

偽装画面と不正送金の手口



Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

運び屋（マネー・ミュール）への誘い



警視庁 Metropolitan Police Department

警視庁のウェブサイトからさがす

検索開始

トップ / 情報セキュリティ広場 / 海外送金サービスを悪用した不正送金アルバイトに注意！

海外送金サービスを悪用した不正送金アルバイトに注意！

～割のいいアルバイトはありません～

【突然届いたメール】

先日、私のメールアドレス宛に一通の求人広告のメールが届きました。中には、「受け取ったお金を指定先に振り込むだけで、その金額の一部が報酬になる」と書かれていたので、簡単なバイトだなと思い、雇用契約を結びました。

その後、私の口座に振り込まれた金額を海外に送金したところ、銀行から「不正に送金された恐れがあるため口座を凍結する」との連絡がありました。

【あるフリーターの証言】

【突然届いたメール】
先日、私のメールアドレス宛に一通の求人広告のメールが届きました。中には、「受け取ったお金を指定先に振り込むだけで、その金額の一部が報酬になる」と書かれていたので、簡単なバイトだなと思い、雇用契約を結びました。
　その後、私の口座に振り込まれた金額を海外に送金したところ、銀行から「不正に送金された恐れがあるため口座を凍結する」との連絡がありました。

【あるフリーターの証言】
インターネットの求人サイトで「日本の客から海外送金するアルバイト」を見つけ、応募しました。
　ある日、送金依頼があり、翌日、私の口座に数十万円単位の入金があったので、私の取り分を差し引いた金額を引き出し、海外送金サービスを利用して送金しました。
　知人にこのアルバイトのことを話すと、怪しいと言われ、急に怖くなり、アルバイトをやめるメールを送りましたが、また数十万円が私の口座に振り込まれていました。

（警視庁HPより引用）

（参考） http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku430.htm

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

オンライン銀行詐欺ツールの流行

トレンドマイクロのレポートによると、**Citadel**と呼ばれるオンライン銀行詐欺ツールが流行しており、このツール被害の96%以上が日本であったという。また本ツールが情報詐欺の対象とする金融機関(6行)が全て国内銀行であったことからも、本ツールが国内を標的としていることが窺える。海外に対して比較的小規模に収まっていた国内でのオンライン銀行詐欺攻撃がより本格化してきている。

7月 23

オンライン銀行詐欺ツール「Citadel」：日本での被害増加を確認、国内で2万台以上の感染

by シニアスペシャリスト 岡本 勝之

(2 投票, 平均値/最大値: 4.00 / 5)　ブックマークへ追加　3 users　この記事を印刷

トレンドマイクロの脅威調査機関である「Forward-looking Threat Research(FTR)」では、さまざまな調査を行っていますが、その調査の中で、日本での被害が 96%以上を占めるオンライン銀行詐欺ツールの攻撃キャンペーンを確認しました。オンライン銀行詐欺ツールとは、オンライン銀行口座の不正操作による金銭窃取を最終的な目的とする不正プログラムの総称です。現在では、正規オンライン銀行Webページ上で各種認証情報の入力を促す偽のポップアップを表示し、情報を詐取する手口が中心的になっています。日本に特化したオンライン銀行詐欺ツールの攻撃については、2012年10月29日のブログ記事、2013年2月14日のブログ記事、「2013年第1四半期セキュリティラウンドアップ」などで触れていますが、今回確認された攻撃は、その後も継続して日本を狙う攻撃が拡大傾向にあることを示すものと言えます。

この攻撃で利用されたオンライン詐欺ツールは「Citadel」ファミリ(「TSPY_ZBOT」などとして検出)です。これらのツールが詐取情報をやりとりする遠隔操作用の C&Cサーバは、現時点で少なくとも 9つの IPアドレスを特定しており、地理的にはヨーロッパ、アメリカなどに分散していました。これらの C&Cサーバについてアクセス状況を監視したところ、アクセス元の96%以上が日本からのものと確認されました。この C&Cサーバへのアクセス発生は、既にユーザ環境に感染したオンライン銀行詐欺ツールの存在を示すものであり、感染被害のほとんどが日本国内で発生していることを意味します。

また、これらの C&Cサーバへアクセスするオンライン銀行詐欺ツール検体とその設定ファイルの解析から以下のことが確認できました。

- 情報詐取対象の 6つの金融機関はすべて日本国内のものであり、アクセス元の情報と併せて日本のみを狙った攻撃であることは明らかと言える
- 金融機関以外にも、Gmail、Yahooメール、Windows live(Hotmail)など、有名 Webメールも情報詐取対象となっている

出典:
2013/7/23 トレンドマイクロセキュリティブログ
http://blog.trendmicro.co.jp/archives/7547

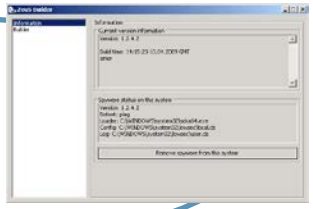
なお、ネットバンキング用アカウント情報のほか、GmailやYahooメール等のWebメールのアカウント情報も詐取する機能を持つといい、詐取したアカウント情報を他サイトへの攻撃へ転用するリスト型攻撃の温床となっている可能性もある（金融業界に限った脅威ではない）。

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

個人情報詐取マルウェア(開発ツール)

CitadelはZeusを元に開発されたマルウェア開発ツールであり、口座情報を詐取するマルウェアを作成するために多く利用されている。海外において既に500万台以上のPCへ感染、90カ国以上で5億ドル以上の被害が発生している。

Zeus



キーロガー、画面キャプチャ等の情報詐取機能を持つ。
2011年5月にソースコードがネットに流出し、亜種マルウェアが一気に拡大した。

SpyEye

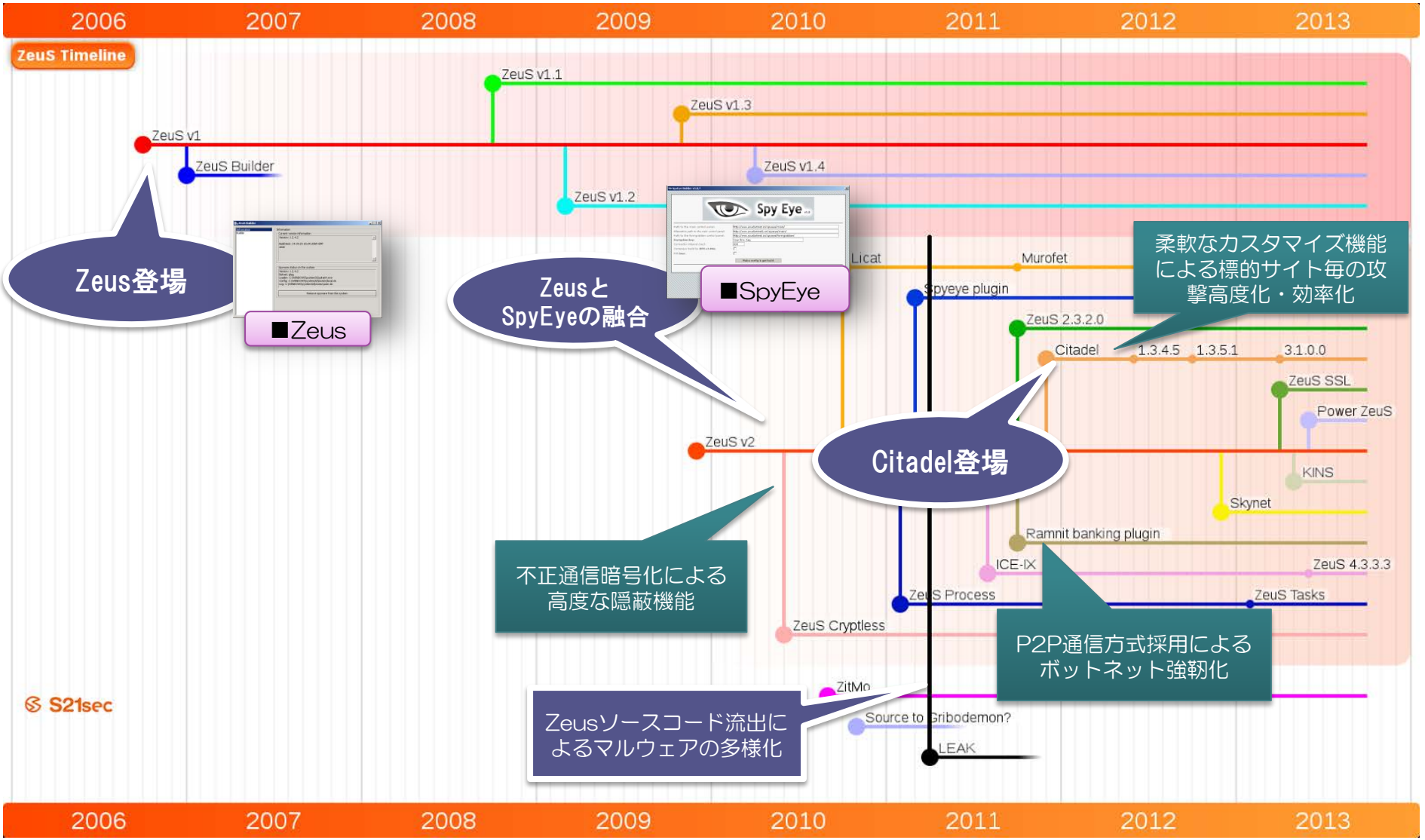
Zeusとならぶ代表的な個人情報収集マルウェア作成ツールキット。
中間者攻撃の機能等を提供。

後継ツール = 機能の進化

Citadelは自身の**高度な隠蔽化機能**を持つほか、「ダイナミック・コンフィグ」機能を含む**高度なボットネット管理・制御機能**を持つなど、従来のマルウェアに比べさらに洗練度が増している。
また、本ツールはアンダーグラウンドにおいて強固な開発環境・サポート体制を持っていると見られており、急拡大の一因に結び付いていると見られている。

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

個人情報詐取マルウェア(開発ツール)の変遷



(出典) S21sec http://securityblog.s21sec.com/2013/11/zeus-timeline-i.html

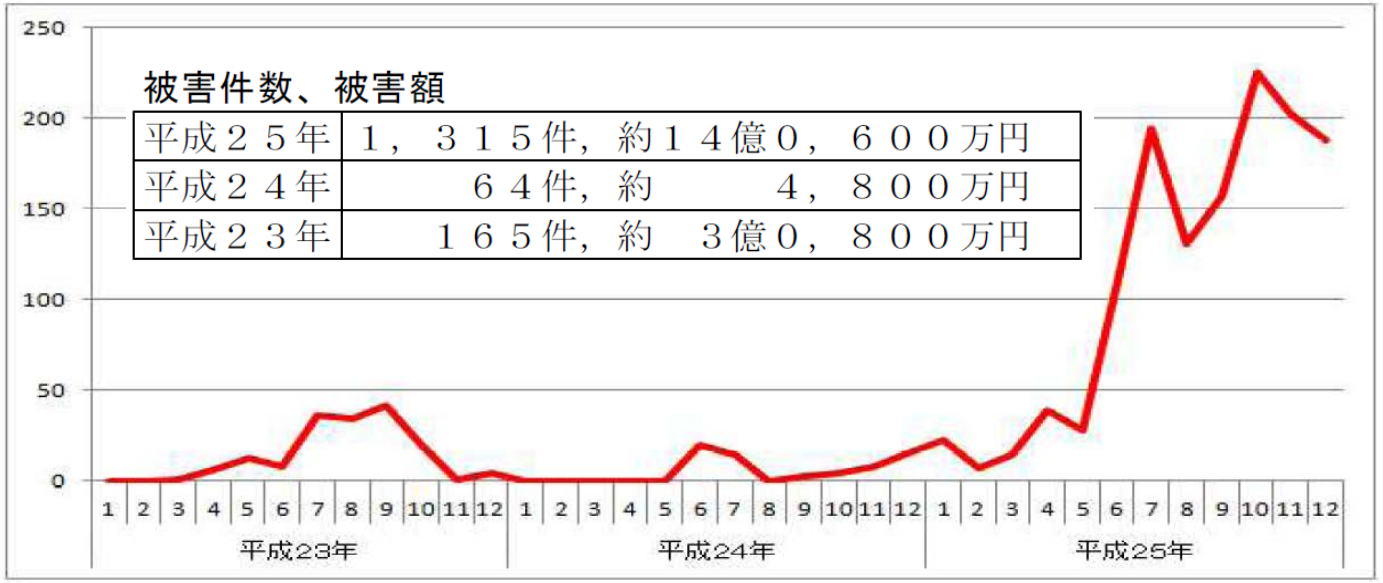
Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ネットバンキング不正送金被害

■ネットバンキングに係る不正送金被害（警察庁）

- 平成25年中の発生状況　（出典）http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf
  - 1,315件，約14億600万円と過去最大の被害。特に平成25年6月以降、急増
  - 被害に遭った銀行の数も月ごとに拡大
  - 犯行等の状況
    - ✓ 被害口座は個人名義がほとんど
    - ✓ 被害口座に係るパスワード等を入手する方法は、コンピュータウイルスで表示した不正画面に入力を求めるものが主
- 不正送金の被害額が今年1月から5月9日までに約14億1700万円に上り早くも平成25年を超す
  （出典）http://www.nikkei.com/article/DGXNZO71282200W4A510C1CR8000/

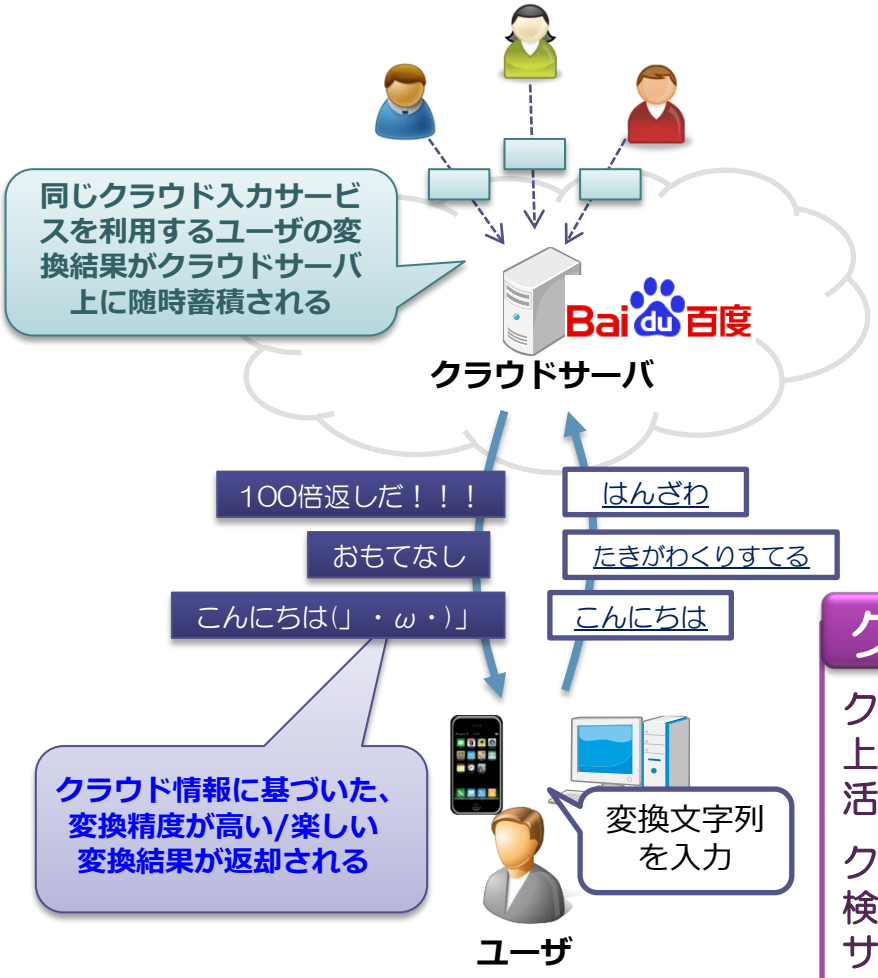
月別発生件数（平成２３年～平成２５年）



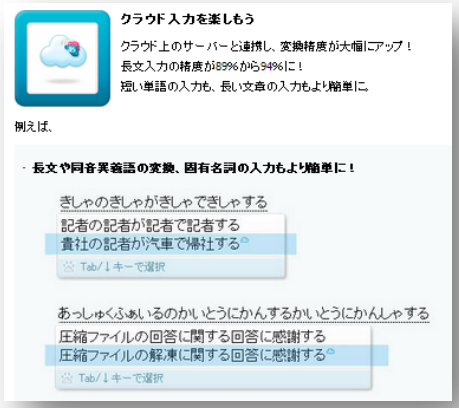
Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

クラウド利用によるサービスの実現とリスク

■Baidu IME/Simeji らクラウド入力**IME (Input Method Editor文字入力補助ソフト)**は**インターネット上に存在するクラウドサーバと通信を行い**、高精度な変換、または大量の変換候補文字列の提供を実現する。特に、顔文字、新語、流行語等リアルタイムに多くの変換結果を収集し活用するため、ユーザの人気を博している。



Baidu IME 入力変換例



http://love-guava.com/android-simeji-conversion/

Shimeji 入力変換例

http://love-guava.com/android-simeji-conversion/

クラウド入力IMEは強力な仕組み

クラウド入力IMEは多くのユーザの変換結果をクラウド上で収集・分析し、リアルタイムにIMEの辞書へ反映・活用できる効果の高い強力な仕組みである。

クラウド利用はIMEに留まらず、多くの顧客・拠点から検体を収集するセキュリティ製品の登場など、多くのサービス・アプリケーション等で活用が見込まれている。

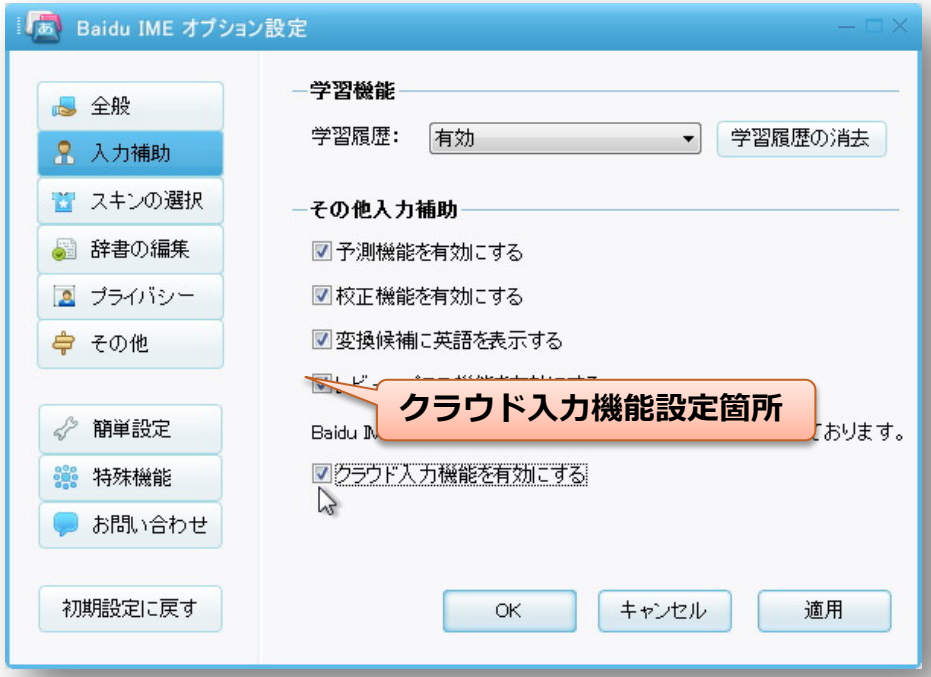
Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

Baidu IME/Simejiの問題点

（デフォルト設定とユーザ同意の確認）

■問題発覚前versionの Baidu/Simeji では、インストール時のデフォルト設定が**「クラウド入力機能を有効にする」**となっていたという。また、以前までユーザ規約文面では「クラウド入力機能によって個人情報が送信され得る」ことが読み取り難いとの指摘もあり、事実上「クラウドへの情報送信に同意していない(把握していない)状態で情報送信が行われる状態になっていたユーザが多かったと推測される。

図. Baidu IME(v2.3) 設定画面



(出典)
http://www.forest.impress.co.jp/img/wf/docs/493/253/html/image2.jpg.html

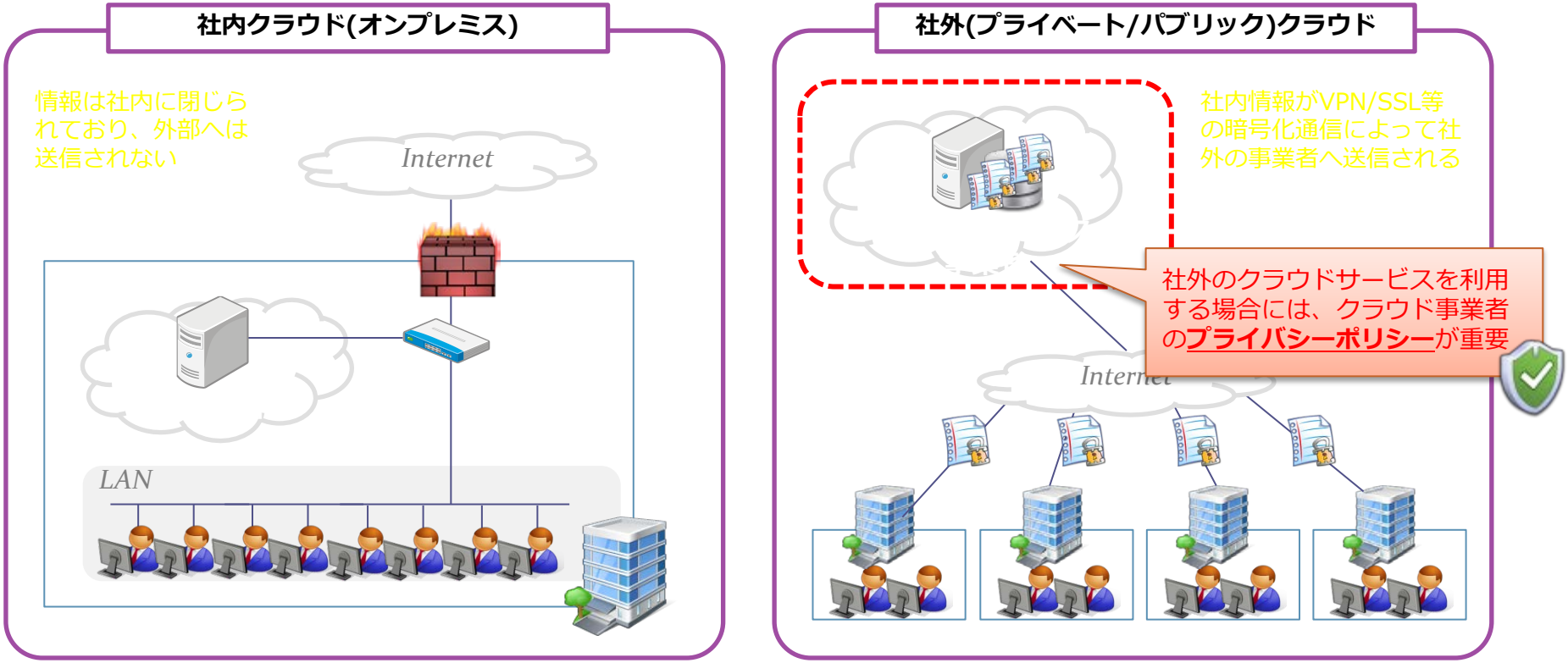
問題点

- **不明瞭なユーザ規約文面および同意取得**
- (事実上同意を得られていない状態での)
  不適切なデフォルト設定

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

クラウド利用における情報管理・保護の考え方

■本来、クラウド入力IMEを含むクラウドサービスの利用は大きなメリットを実現するものである。
各社の利用シーンや情報の重要度に応じて、適切なシステム形式やサービスを選択することで、その大きなメリットの享受を目指すことが肝要である。



多くのクラウド事業者ではセキュリティ・情報管理に重点を置いており、強固なセキュリティ対策を実施している。ユーザの条件によってはむしろ、クラウドサービスを利用することで自前でセキュリティ対策を実施するよりもスピーディかつ低コストで安全な環境を構築できるケースもある。

今回の事案に過敏に反応し、クラウドサービスの利用に対して過度な拒否反応を起こす必要はない！？

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

DNSオープンリゾルバー問題

（2013年3月に発生した大規模サイバー攻撃事例）

図： INTERNET Watch ネットを崩壊の瀬戸際に追い込んだ「史上最大のサイバー攻撃」が明るみに

ニュース

ネットを崩壊の瀬戸際に追い込んだ「史上最大のサイバー攻撃」が明るみに

～早急な対策が望まれるオープンリゾルバーDNS問題

今年の3月18日～22日ごろにかけて、インターネット上で大規模なDDoS攻撃が発生していた。ピーク時にはトラフィックが300Gbpsに達したと言われており、過去最大級の攻撃規模だったという。

今週多くの人は何も気がつかなかったが、「インターネットが破壊される瀬戸際」に追い込まれる程の攻撃、史上最大規模のDDoS攻撃が行われていたことが明らかになった。

スパム対策組織Spamhausと、同組織を支援した米セキュリティ企業Cloudflare社が発表し、発表内容をもとに米ニューヨーク・タイムズや英BBCが27日に大きく取り上げたことで、世間に広く知られるようになった。Cloudflare社は「ネットを崩壊の瀬戸際に追い込んだ」と攻撃を評している。

この攻撃は、欧州を中心としたインターネットに渋滞を引き起こし、ウェブサイトや動画ストリーミングサービスの使用が難しくなる時期があったが、現時点ではだいたい解決の方向に向かいつつあるという。しかし根本的問題は解決されておらず、様々な企業や組織がこの問題の根本的解決のために立ち上がっている。

インターネット利用者にとっても、ウェブサイト閲覧が遅くなったり、配信動画を見れない等といった影響を受けることもあった。

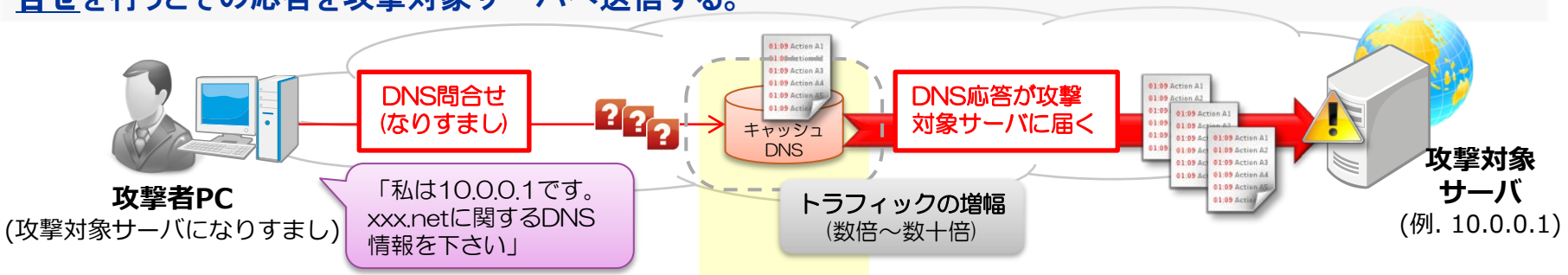
攻撃が始まったのは3月19

めSpamhausは米セキュリティ企業Cloudflareに攻撃緩和の支援を求めた。当初は攻撃の規模を別にすれば、攻撃手法は通常とさほど変わったものではなかった。

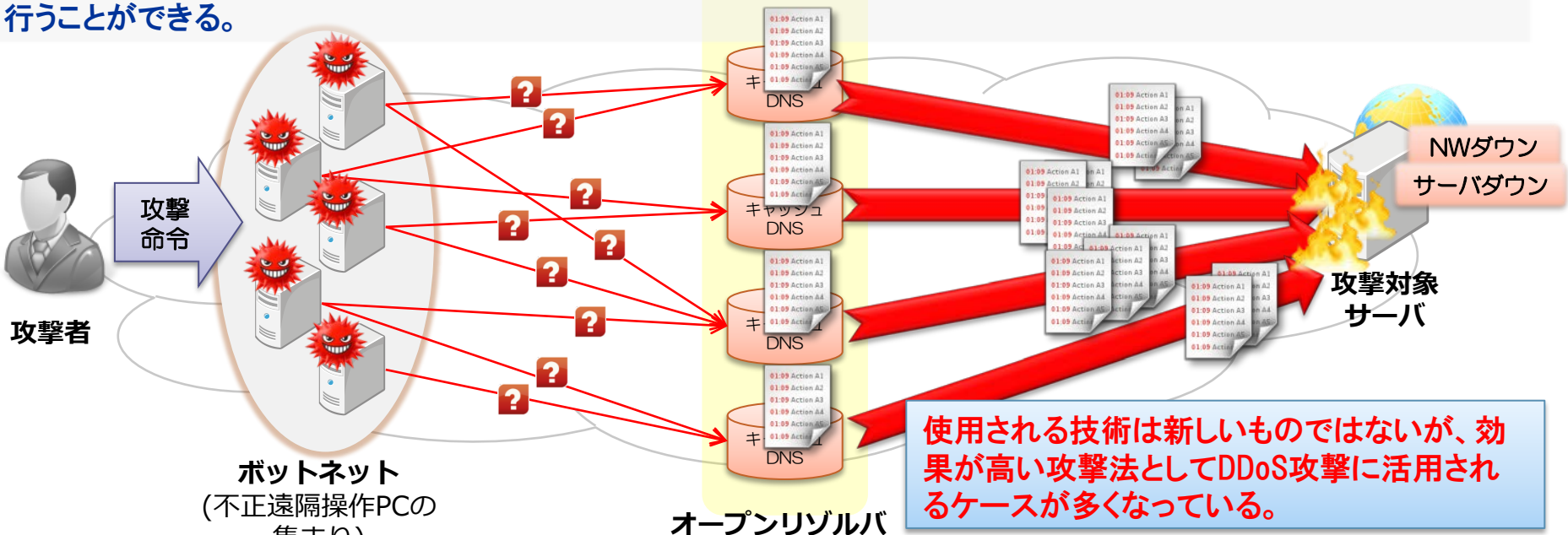
Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

DNSリフレクション攻撃の仕組み

■DNSのデータ増幅性・オープンリゾルバを悪用して、攻撃者はDoS攻撃の増幅を行う。具体的には、オープンリゾルバに対して**大容量のDNS応答を持つドメイン名を検索対象**とし、**攻撃対象サーバのIPアドレスを騙ったDNS問合せ**を行うとその応答を攻撃対象サーバへ送信する。



■実際には、攻撃者は**ボットネット**と呼ばれる(不正に)遠隔操作可能なPC群をまとめて制御し、各PCから攻撃対象サーバになりすましたDNS通信をオープンリゾルバに対して行うことで、攻撃対象サーバに対してより強大な攻撃を行うことができる。



Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

NTP Amp攻撃の発生

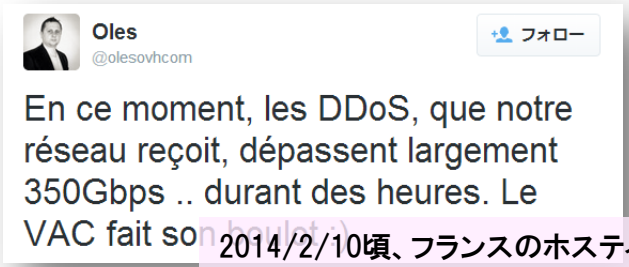
■昨年3月に発生した300GbpsのDDoS攻撃以降、DNS Amp攻撃という手法による大規模DDoS攻撃が頻発していたが、2014年に入り確認された以下の各攻撃では、NTP(時刻同期)サーバの機能を利用したNTP Amp攻撃という手法が使用されていたという。

2014年1月初頭、“*League of Legends*”等オンラインゲームサービスに対して、最大約**100 Gbps** のDDoS攻撃が発生

(出典) http://arstechnica.com/security/2014/01/new-dos-attacks-taking-down-game-sites-deliver-crippling-100-gbps-floods

2014/2/10頃、米国セキュリティ企業「CloudFlare」社の顧客に対し、約**400Gbps** におよぶ大規模DDoS攻撃が発生

(出典) http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack



2014/2/10頃、フランスのホスティング会社 OVH社に対し **350Gbps** のDDoS攻撃が発生

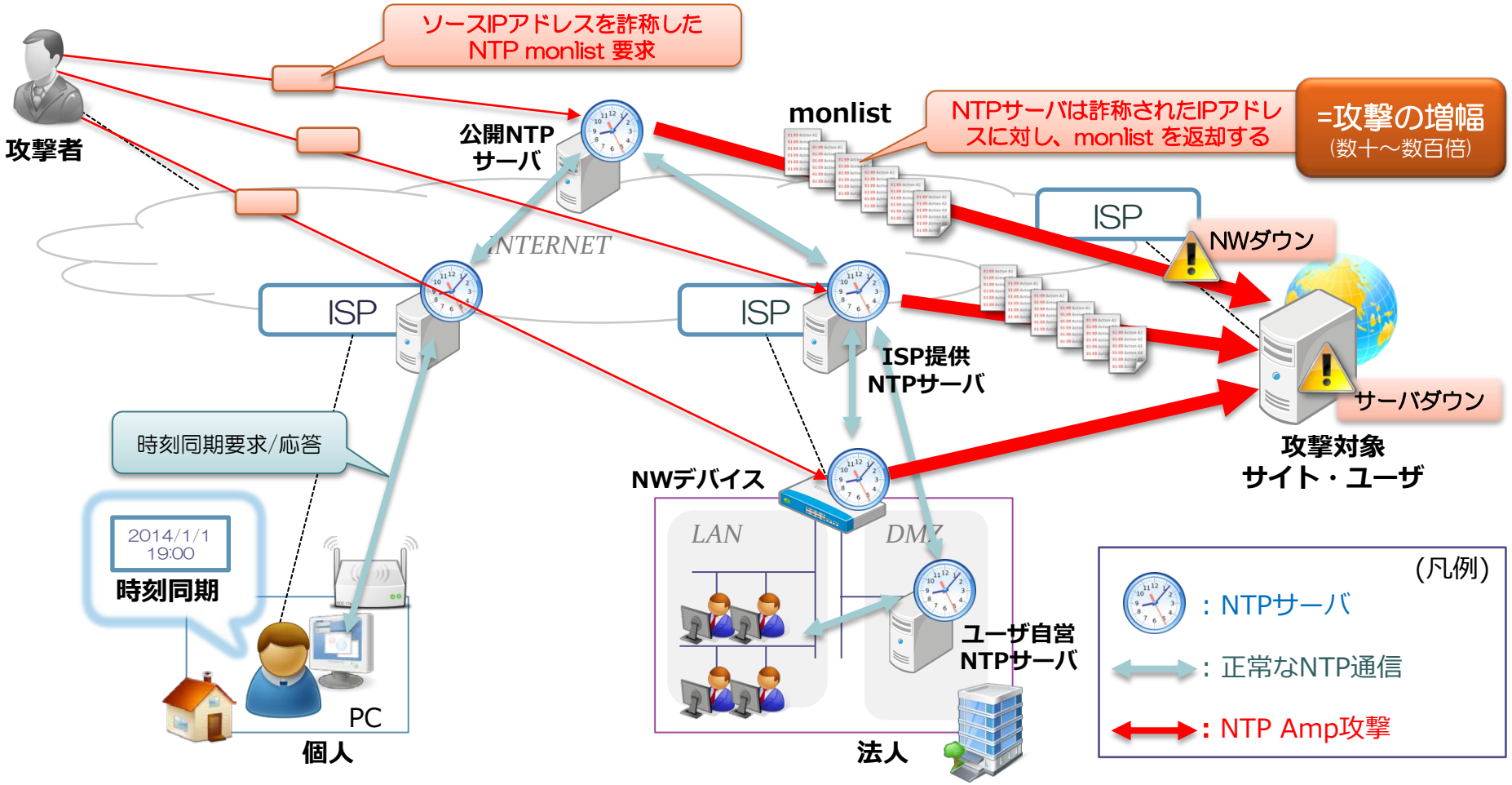
(出典)
https://twitter.com/olesovhcom/status/433036769924116481

NTP Amp攻撃が利用するNTP通信のトラフィック増幅性はDNSを越えるものであり、特にCloudFlare社が発表した2014年2月10日の事例では **約400Gbps** にまで及んだことが伝えられている。

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

NTPAmp攻撃の仕組み

■NTP(Network Time Protocol)はPCやサーバ等の時刻同期に利用される通信プロトコルである。NTPサービスは公的機関やISP等の公開NTPサーバで提供されている他、ユーザ側のサーバ・NWデバイス上で自営目的・または無意識の内に動作していることがある。



NTPサーバは通常の時刻同期を行う他、当該サーバへの接続履歴(monlist)を要求に応じて返却する機能を有する。攻撃者はこれを悪用し、「ソースIPアドレスを攻撃対象IPアドレスに詐称したNTP monlist要求」パケットを踏み台となる公開NTPサーバへ大量に送信し、monlist応答パケットを攻撃対象へ送信させることで 攻撃トラフィックの増幅を実現する。

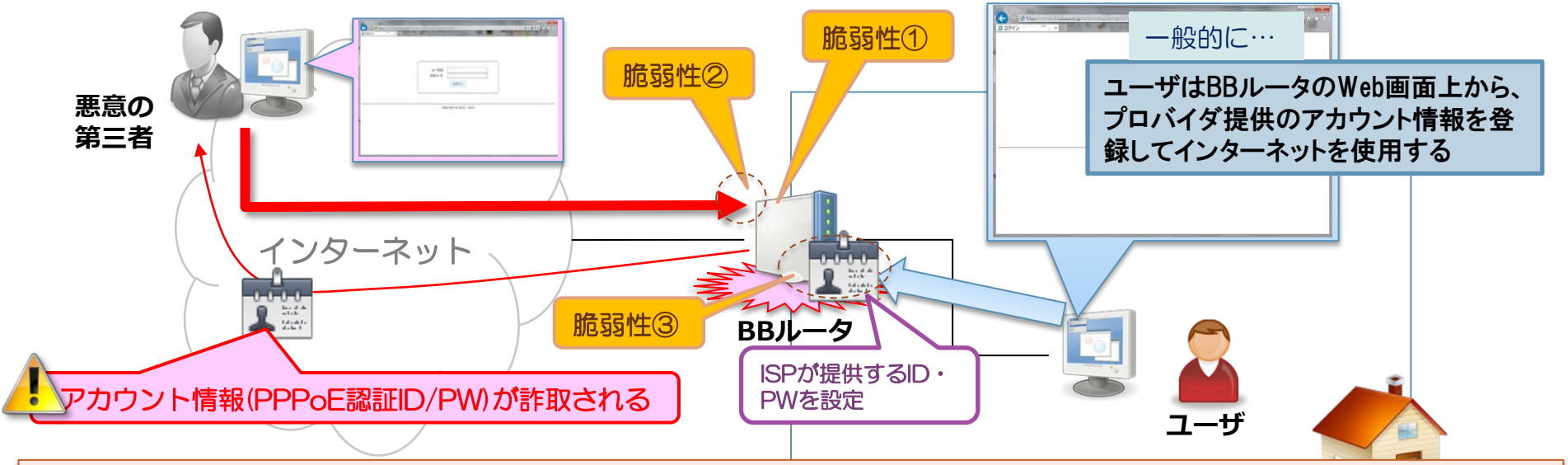
Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

NWデバイスの脆弱性問題

■攻撃パターン： 認証の脆弱性(デフォルトパスワード、平文保存等)

L社製ルータ問題に見られるケースで、多くのNWデバイスに搭載されているWeb管理画面のID/パスワードが周知のもの、もしくは容易に推測可能であることを利用して、悪意のユーザがNWデバイス管理画面へ不正アクセスを行うものである。

(出典)
http://www.logitec.co.jp/info/2012/0516.html?link_id=out_oshirase_20120516_2_2

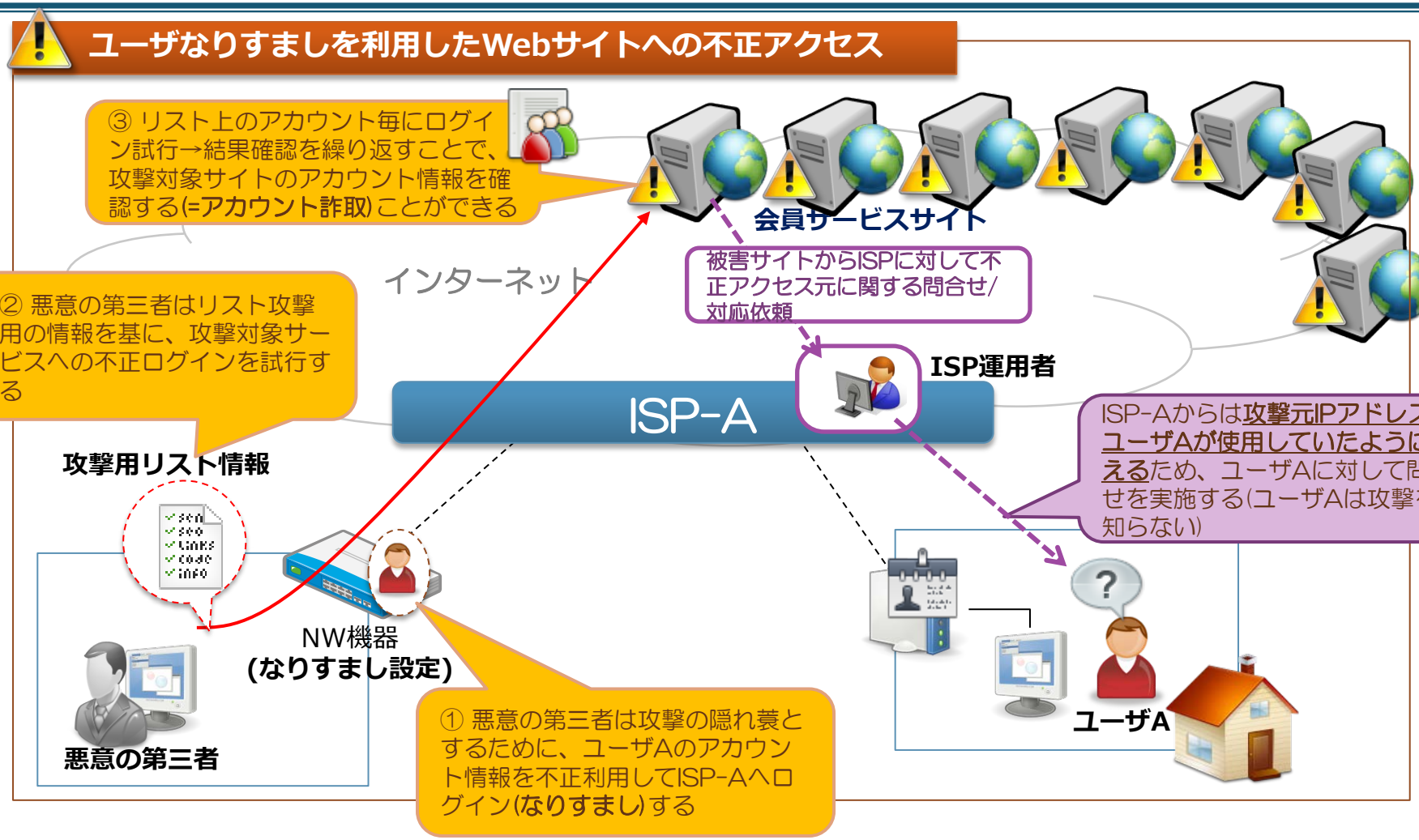


■BBルータのある機種に実在するセキュリティ脆弱性の例

① BBルータ管理画面の**初期ID/PWが"admin","password"のように平易**なもの
② **WAN(インターネット)側からBBルータ管理画面へアクセス可能**
③ BBルータ管理画面上において、設定されているISP提供の**PPPoEアカウント(ID/PW)情報が容易に読み取り可能な状態(平文)**で保存されている

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

参考：発生している被害概要（インシデント①）

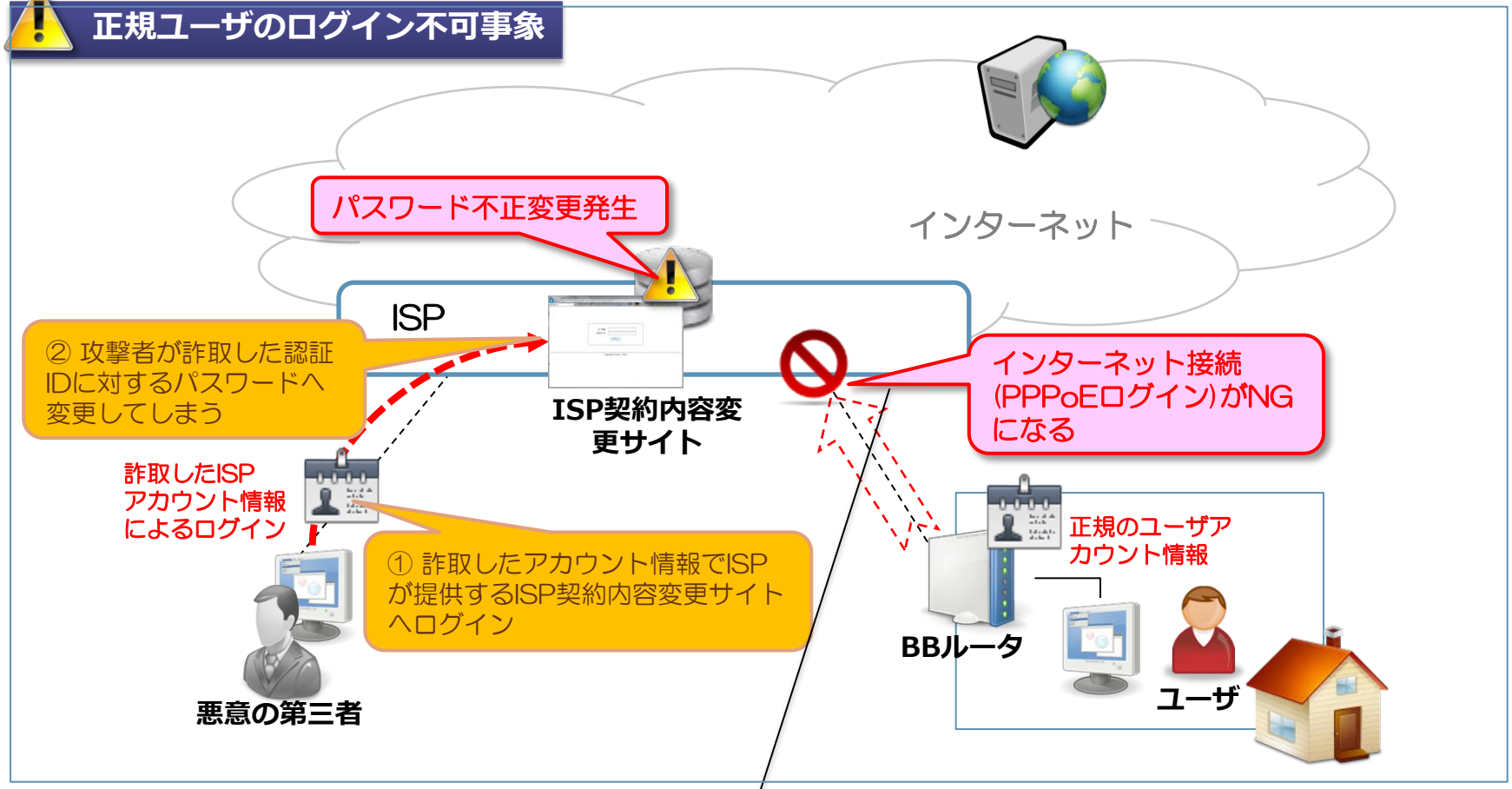


攻撃者がWebサイト不正アクセスを実行するにあたり、第三者の認証情報を利用することで(なりすましを行うことで)、攻撃者自身の特定を困難にしている。
※ 悪意の第三者の特定を困難にするための認証情報が簡単に取得できる環境が存在していることの危険性が存在している

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

参考：発生している被害概要（インシデント②）

詐取したPPPoE認証ID/PWを利用したPPPoE認証IDに対するPWの変更行為



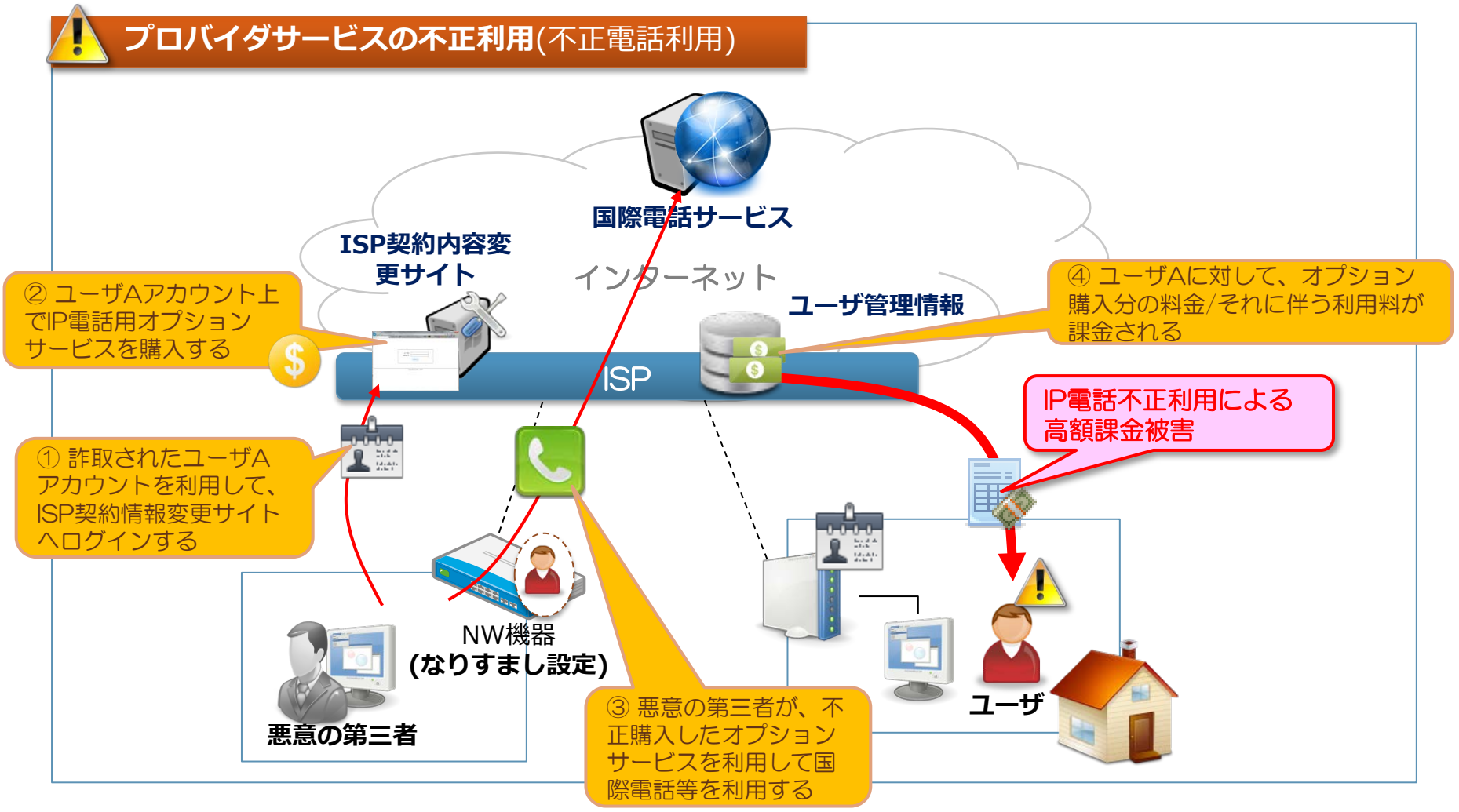
意図せずネット接続がNGとなり、ユーザはISPへ問合せを行う。
※ただし、既に確立済みPPPoEセッションが不正変更後もそのまま残っているケースもあり、不正変更に気づかないユーザも存在

ユーザ問合せによって、アカウント詐取事象が発覚！

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

参考：発生している被害概要（インシデント③）

ログイン不可事象ばかりではなく、アカウント情報詐取によって金銭被害につながるインシデントも発生



Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ロジテック社製品(BBルータ)の脆弱性に起因するISPユーザの接続に関する
インシデントが発生
本脆弱性を悪用したサイバー攻撃者は、不正アクセスのインフラとして利用

Telecom-ISAC Japanおよび本施策に対し賛同した会員ISPで、

① ロジテック社製脆弱性保有ルータをネットワーク側から調査を実施し	T-ISAC-Jで実施
② スキャン結果とISPが保有するユーザ接続情報を照らし合わせることで	ISPで実施
③ 該当脆弱性保有ルータの利用者を特定し、	ISPで実施
④ 特定した利用者に対し、手紙、電子メール等を利用して注意喚起を行うとともに脆弱性対応をお願い	ISPで実施

脆弱性対応依頼 = ルータ ファームウェアのバージョンアップ
+ PPPoE認証ID / PW の変更

Telecom-ISAC Japan、会員ISP、製品メーカ(エレコム/ロジテック)
との合意の下に本施策を実施

※ 製品メーカとの協議においては一部合意されていない事項も有

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

参考：警視庁による悪用者の摘発

ルーターの欠陥を悪用

今回、摘発されたサーバー管理会社(中都商事)は、一般家庭から盗まれたインターネットの接続IDとパスワードを使って、ネットに接続できるようにしていた。
この一般家庭からのID/PWの詐取は、今回のルータの脆弱性を悪用したものである。

今回摘発された被疑者は、本脆弱性悪用者の氷山の一角と考えられること、また、摘発の対象となった中継サーバ運用団体の全容もつかめていない状況と推測することができ、今後も本問題に関しては継続した捜査が行われると考えられる。

NHK NEWSWEB　2014年（平成26年）2月14日［金曜日］

トップページ › 社会ニュース一覧 › 中国の顧客に日本に不正接続させたか

ニュース詳細

中国の顧客に日本に不正接続させたか

2月13日 18時40分

東京・池袋のサーバー管理会社の社長ら２人が、不正に入手した他人のＩＤやパスワードを使って、中国国内の顧客に日本のインターネットに不正に接続させていたとして逮捕されました。
この会社のサーバーは、国内で起きた不正アクセス事件やサイバー攻撃に使われていて、警視庁で実態の解明を進めています。
２人は容疑を否認しているということです。

逮捕されたのは、東京・豊島区のサーバー管理会社「中都商事」の社長で、中国人の劉傳聞容疑者（３４）ら２人です。
警視庁によりますと、劉容疑者らは去年１０月、不正に入手した神奈川県内の男性のＩＤとパスワードを使って、中国の顧客に自分の会社のサーバーから日本国内のインターネットに接続させたとして、不正アクセス禁止法違反の疑いがもたれています。
この会社は、中国国内で顧客を募り、プロキシサーバーと呼ばれるインターネットへの接続を仲介するサーバーを通じて日本のインターネットに接続させるサービスを提供し

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

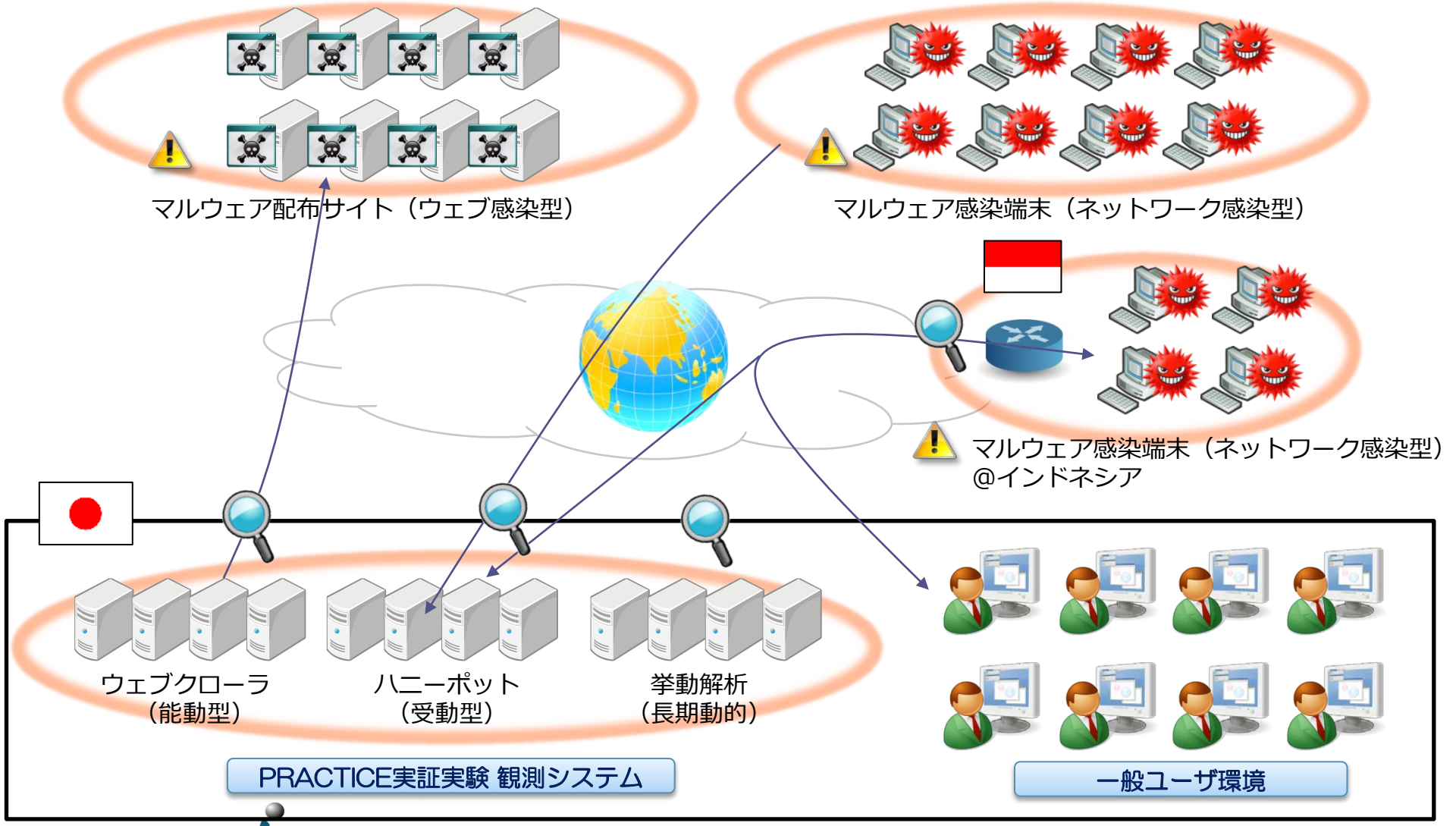
サイバー攻撃対応プロジェクトと今後に向けた考察

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

PRACTICE

(Proactive Response Against Cyber-attacks Through International Collaborative Exchange)

総務省「国際連携によるサイバー攻撃予知・即応に関する実証実験」



Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

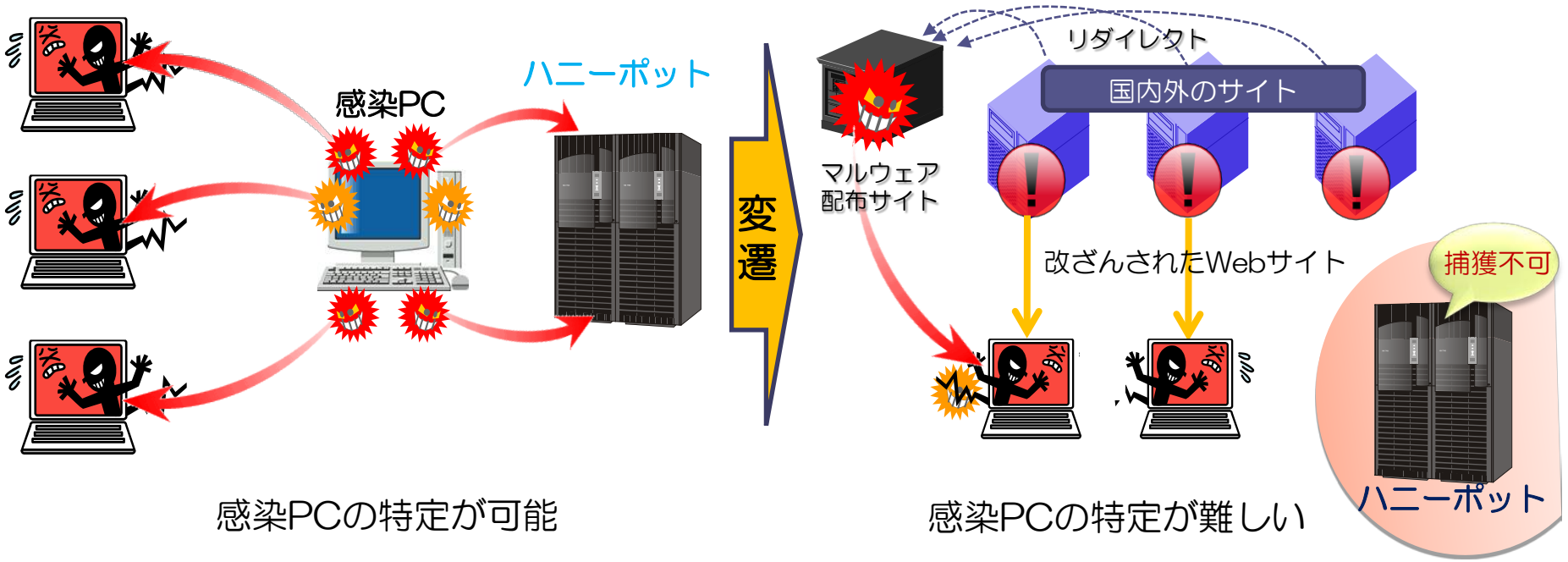
マルウェア感染経路の変遷

ネットワーク感染型マルウェア

- ネットワーク経由で感染するマルウェア
- OSの脆弱性を攻撃して感染
- ハニーポットにて捕獲可能であり、Cyber Clean Centerの取り組み(2006～2010年度)の駆除対象

Web感染型マルウェア

- Webサイトの閲覧により感染するマルウェア
- ブラウザまたはブラウザのプラグインの脆弱性を攻撃して感染
- ACTIVEでは<u>ネットワーク感染型の他、この対応も注力していく</u>



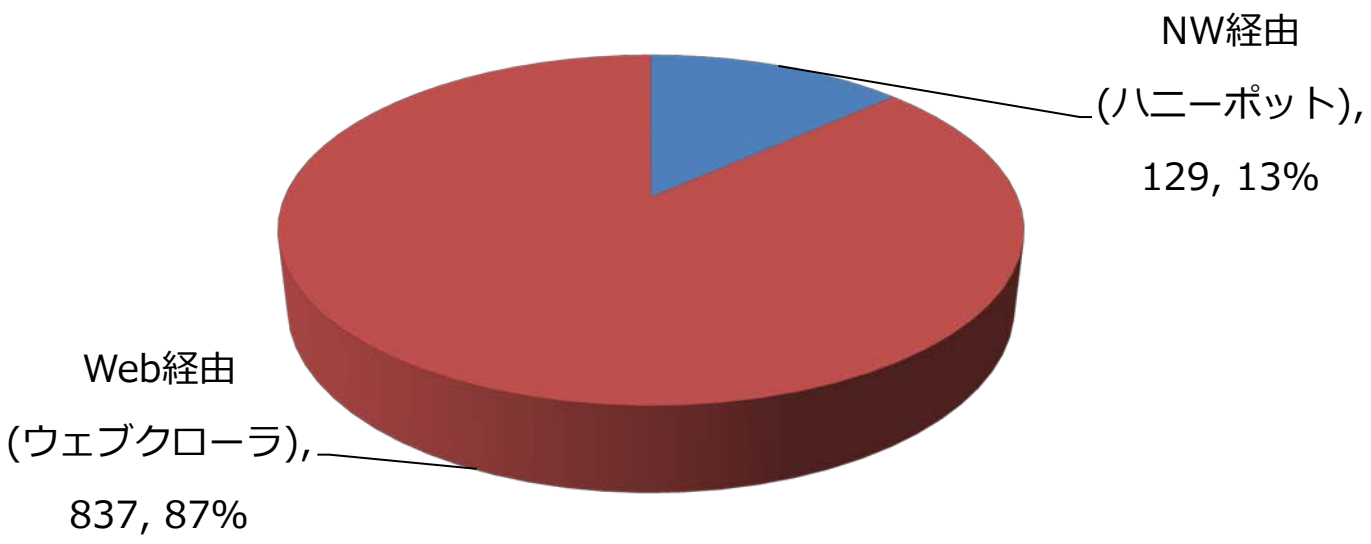
Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

Zeus/Zbot系マルウェアの感染経路

■Zeus/Zbot関連マルウェアの感染経路

【収集期間：2012/2/1～2013/11/14】

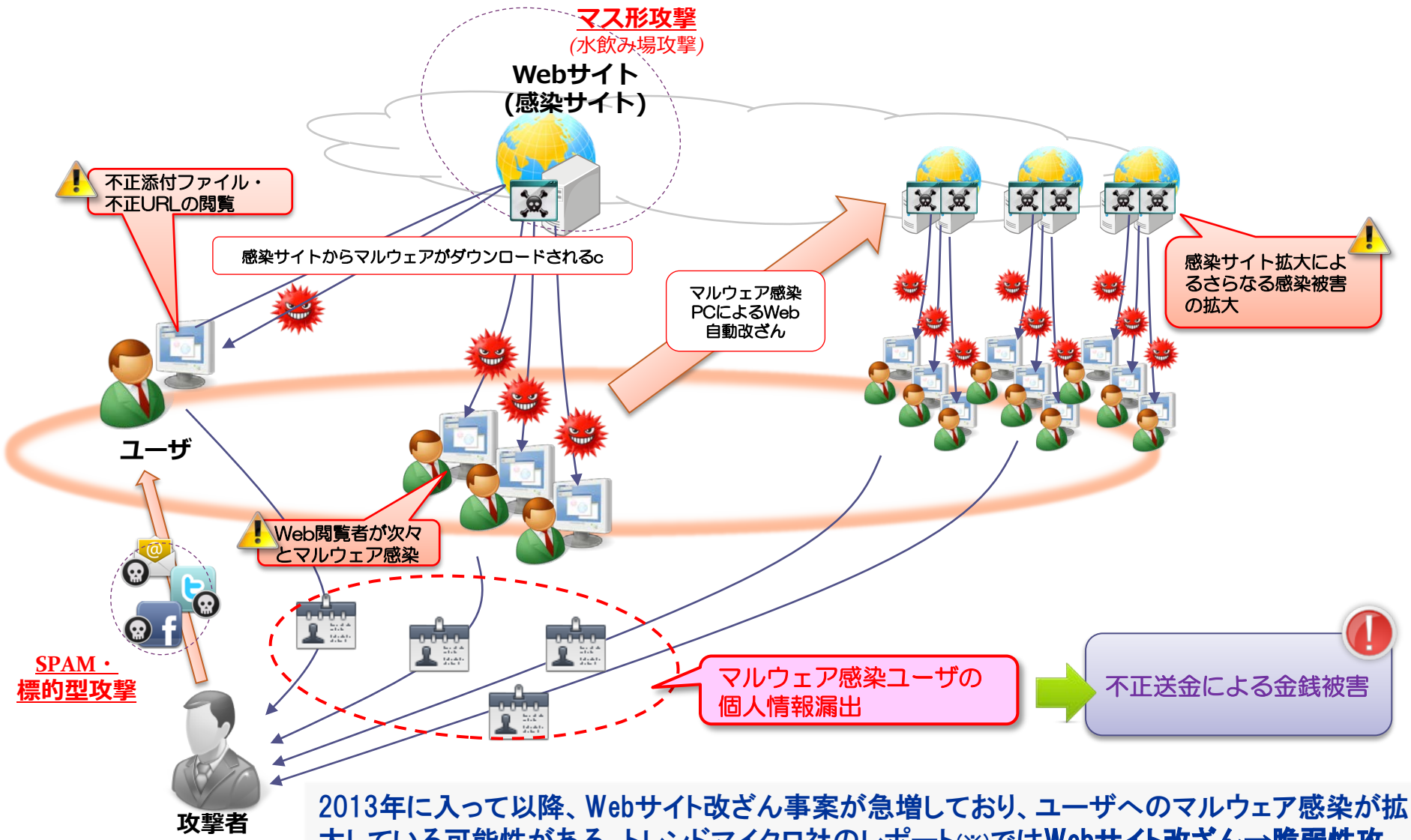
感染経路	NW経由 (ハニーポット)	Web経由 (ウェブクローラ)	合計
*ZBOT*と判定された検体	129	837	966



マルウェアの感染経路としては、Webサイト経由が87%を占め主な感染源になっている

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

Web改ざん多発事案によるマルウェア感染拡大との関連



2013年に入って以降、Webサイト改ざん事案が急増しており、ユーザへのマルウェア感染が拡大している可能性がある。トレンドマイクロ社のレポート(※)ではWebサイト改ざん→脆弱性攻撃→金銭詐取と連鎖する攻撃を国内で確認しているという。

※参考 TrendLabs 2013年第1四半期セキュリティラウンドアップ　http://www.47news.jp/CN/201308/CN2013080201001719.html

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ACTIVEプロジェクト

■ ACTIVE(Advanced Cyber Threats response InitiatiVE)

- 総務省主管の国民のマルウェア対策支援プロジェクト

  http://www.active.go.jp/

  - 2013年11月1日開始
  - 目的:マルウェア感染の削減等により、安心・安全なインターネットの実現を目指す
  - マルウェア感染防止から駆除まで一貫して取り組む総合的なマルウェア感染対策であり、官民連携により行う同様のプロジェクトは世界初の試み

マルウェア感染防止の取り組み

① マルウェア配布サイト等のURL情報をリスト化
② マルウェア配布サイト等にアクセスしようとする利用者に注意喚起
③ マルウェア配布サイト等の管理者に対しても適切な対策を取るように注意喚起

マルウェア駆除の取り組み

① マルウェアに感染した利用者のPCを特定
② 利用者に適切な対策を取るように注意喚起
③ 利用者は、注意喚起の内容に従いPCからマルウェアを駆除

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ACTIVEプロジェクトの背景

多種多様なマルウェア感染経路が存在

- ネットワーク感染(ボット型)
- Web経由の感染
- メール経由の感染
- USB経由の感染　など

マルウェア感染時にはさまざまな脅威が存在

- 不正アクセスインシデント
- 他人のPCを踏み台にしたサイバー攻撃
- フィッシング、SPAMメール
- PCの破壊活動　など

・昨今、マルウェア感染による国家機密の情報窃取等、サイバー攻撃の脅威が増大
・悪性サイトの閲覧によりマルウェア感染するなど、その感染手法が巧妙化し、利用者が自力で検知することが困難

ISP等 = お客さま対応、インシデント対応の観点から**マルウェアの感染率の低下**を実施する必要性がある

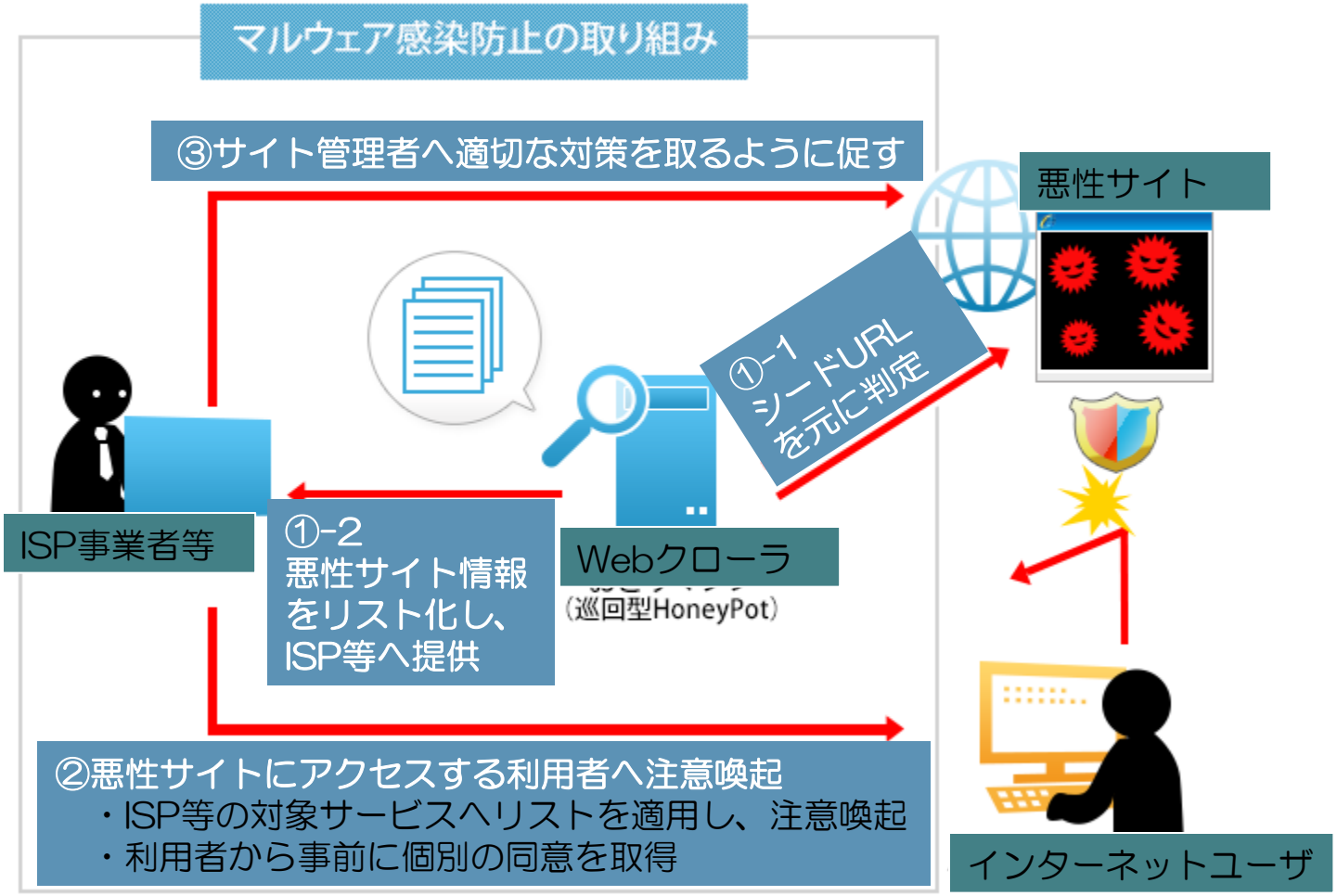
行政 = 安心・安全なインターネットの利用環境の向上、維持の観点から**マルウェアの感染率の低下**が望まれる

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ACTIVEプロジェクトの概要(１)

■ マルウェア感染防止の取り組み

✓ 各社の対象サービスに対して、利用者から事前に個別の同意を取得



Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

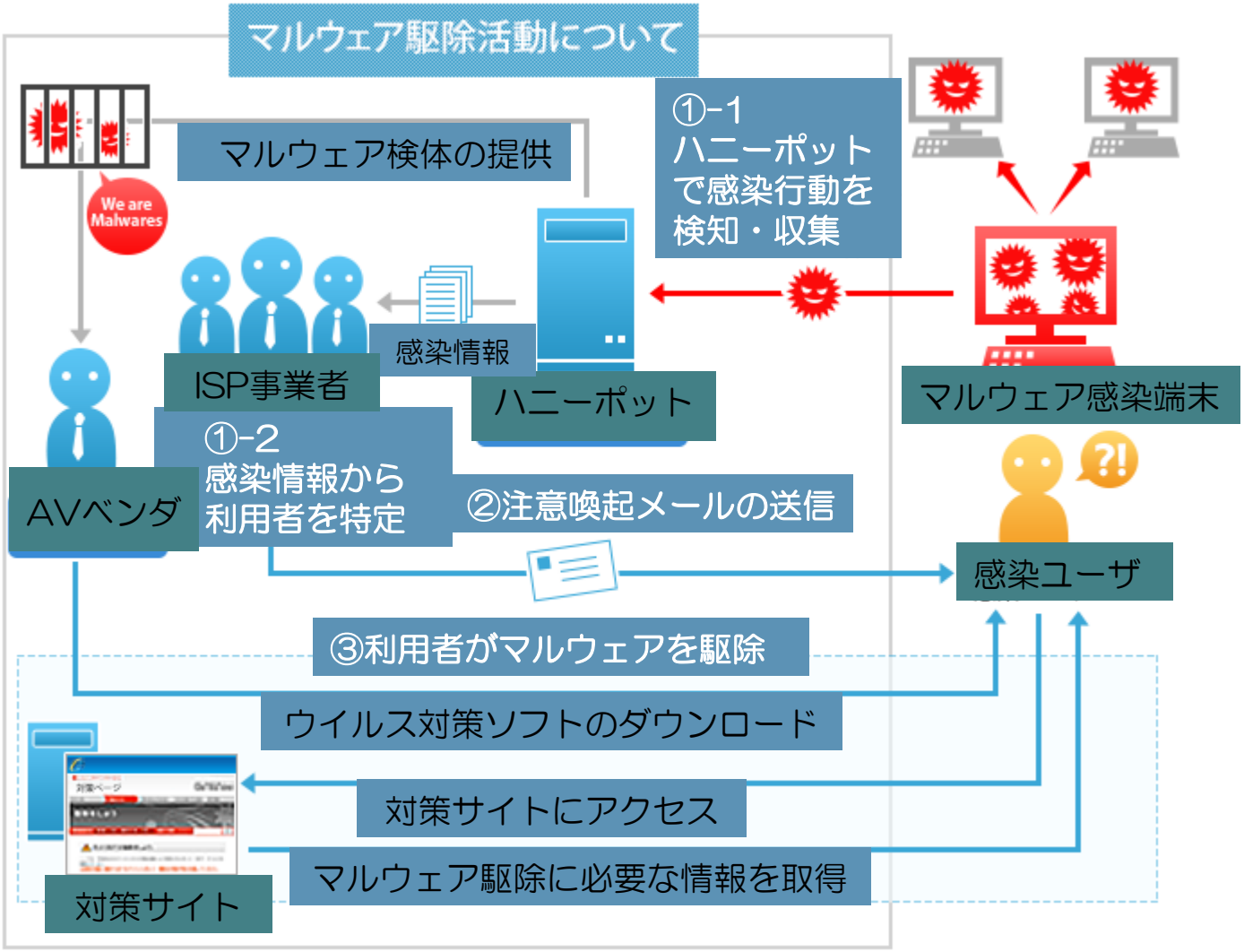
マルウェア感染防止の取り組み

■ 悪性サイトにアクセス時の注意喚起（例：gooスティック）

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ACTIVEプロジェクトの概要(２)

■ マルウェア駆除の取り組み



Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ACTIVEプロジェクト体制（2013年11月現在）

■ ISP等の通信事業者やセキュリティベンダなどが参画

総務省

財政支援、全体支援

Telecom-ISAC Japan

主査　：エヌ・ティ・ティ・コミュニケーションズ株式会社
副主査：ニフティ株式会社、T-ISAC-J企画調整部

参画事業者間の調整

NECビッグローブ株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社
エヌ・ティ・ティレゾナント株式会社
株式会社NTTぷらら
株式会社インターネットイニシアティブ
株式会社エヌ・ティ・ティピー・シーコミュニケーションズ
株式会社ハイホー
KDDI株式会社
ソネット株式会社
ソフトバンクBB株式会社
ソフトバンクテレコム株式会社
ニフティ株式会社

インターネットサービスプロバイダー など

NTTコムテクノロジー株式会社
NRIセキュアテクノロジーズ株式会社
エヌ・ティ・ティ・コムチェオ株式会社
エヌ・ティ・ティ・ソフトウェア株式会社
エヌ・ティ・ティラーニングシステムズ株式会社
株式会社FFRI
株式会社カスペルスキー
株式会社日立製作所
トレンドマイクロ株式会社
日本電信電話株式会社
日本マイクロソフト株式会社
マカフィー株式会社

マルウェア収集・駆除のための技術支援

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ここで “誤認逮捕事件” の教訓…まず経過・時系列

6月	7月	8月	9月	10月

6/29
●横浜市小学校襲撃予告

7/29
●大阪市HP大量殺人予告

8/1
●JAL航空機爆破予告

9/10
●伊勢神宮破壊予告
●任天堂破壊予告

8/27
●お茶の水女子大付属幼稚園襲撃予告
●芦田愛菜への脅迫

8/29
●AKB48握手会襲撃予告

10/9～10
●犯行声明メール
(10/9 落合弁護士 宛)
(10/10 TBSラジオ「Dig」宛)

※安倍総裁殺害予告

7/1
●杉並区男性(19)逮捕

8/15
●保護観察処分

10/17
●再聴取

10/23
●処分取消申し立て

8/26
●吹田市男性(42)逮捕

9/14 ●起訴　9/21 ●釈放

10/19
●起訴取消

9/1
●福岡市男性(28)逮捕

9/21 ●釈放 ●再逮捕

9/27 ●釈放

10/23
●不起訴処分

9/14
●津市男性(28)逮捕

9/21
●釈放

10/23
●不起訴処分

9/18
●津市男性PCのウイルス感染判明

2chへの書き込み　●7/27タイマーソフト偽造 ●8/24クリップボード監視ソフト偽造
●8/28テキストエディタ偽造 ●9/10exif情報編集ソフト偽造

10/18●警察庁長官誤認逮捕会見

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

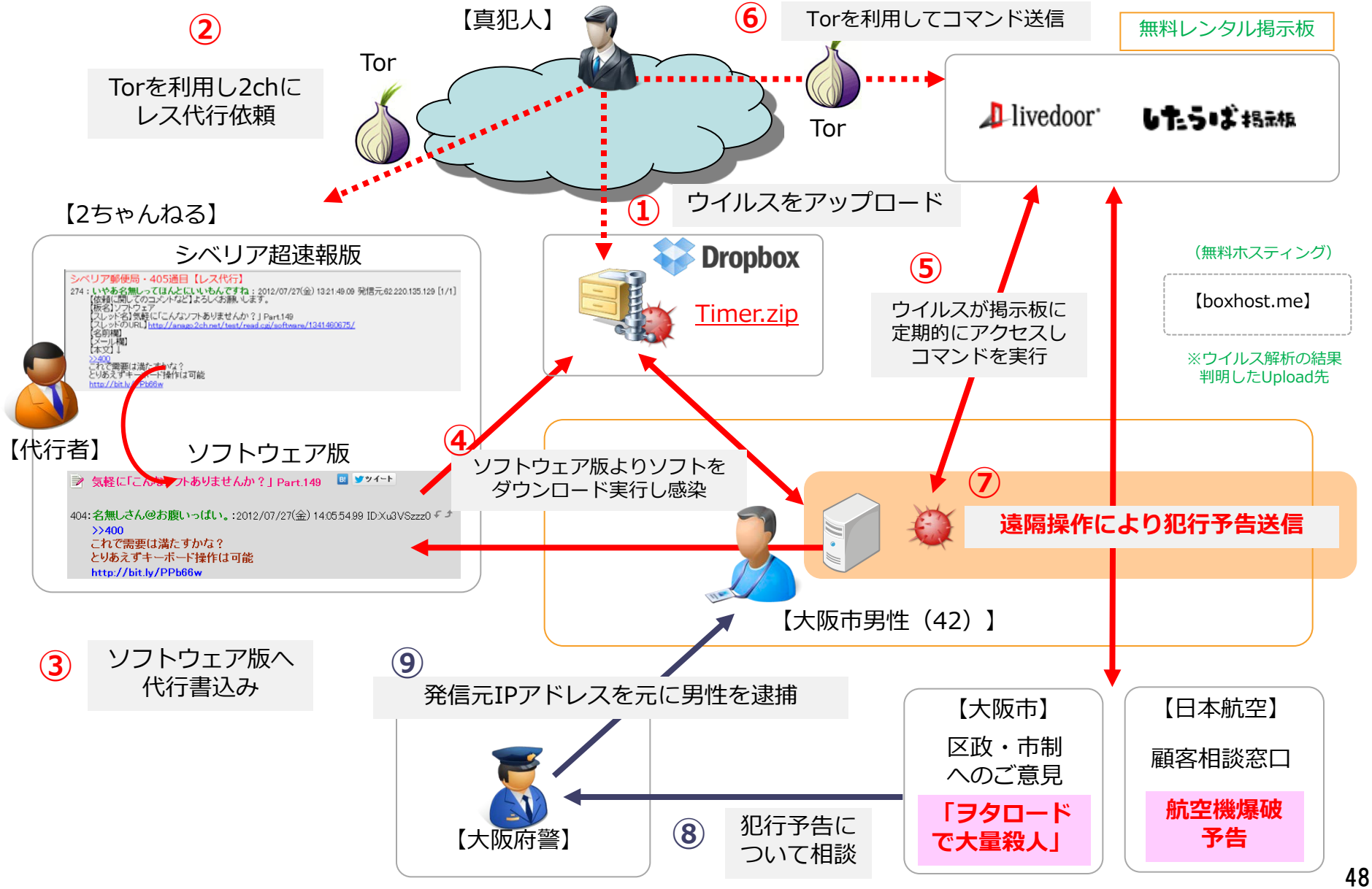
犯行予告

＜犯行声明で関与が記載された犯行予告事件＞

	日時	犯行予告対象	遠隔操作の対象	犯行予告先	手法	捜査担当
1	6月29日	横浜市 市立小学校襲撃予告	杉並区男性(19)	メールフォーム	CSRF	神奈川県警
2	7月29日	大阪日本橋 大量殺人予告	吹田市男性(42)	メールフォーム	ウイルス	大阪府警
3	7月29日	皇居ランナー大量殺人予告	〃	不明	ウイルス	届出なし
4	8月1日	日本航空機爆破予告	〃	メールフォーム	ウイルス	警視庁
5	8月9日	コミックマーケット大量殺人予告	愛知会社員	2ちゃんねる	ウイルス	不明
6	8月9日	天皇陛下殺害予告	〃	2ちゃんねる	ウイルス	不明
7	8月27日	お茶の水女子大付属幼稚園襲撃予告	福岡市男性(28)	メール	ウイルス	警視庁
8	8月27日	芸能プロダクション脅迫	〃	メール	ウイルス	警視庁
9	8月27日	学習院初等科襲撃予告	〃	メール	ウイルス	届出なし
10	8月27日	部落解放同盟襲撃予告	〃	メール	ウイルス	届出なし
11	8月29日	AKB48握手会襲撃予告	〃	2ちゃんねる	ウイルス	警視庁
12	9月10日	伊勢神宮破壊予告	津市男性(27)	2ちゃんねる	ウイルス	三重県警
13	9月10日	任天堂本社破壊予告	〃	2ちゃんねる	ウイルス	三重県警

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

遠隔操作ウイルスの犯行手口（大阪市のケース）



Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

遠隔操作ウイルスの機能

- ユーザのキー入力操作情報およびマウスの操作の記録
（いわゆるキーロガー、入力したパスワードなどはすべて筒抜け）
- 隠しブラウザで特定のURLを操作および開く
- ファイルのダウンロード
（この機能によって感染したパソコンの持ち主が誰なのかといった情報を収集可能）
- ファイルのアップロード
（児童ポルノ画像でも何でも送りつけることができるのでさらなる犯人として捏造しようと思えば可能）
- スクリーンショットの取得（これによってもそのパソコンの持ち主の情報をいろいろと得ることが可能）
- ファイルおよびフォルダの列挙（重要なファイルを見つけてダウンロードされてしまう）
- ファイルの実行（ファイルのコピーや削除も自由自在ということ）
- デフォルトのインターネットブラウザの取得
- 自身のアップデート（アンチウイルスソフトが更新される前に自分自身を更新し続けることで検知されないようにすることも可能になるような機能で、もっと高機能なボットやバックドアではよくある機能）
- 環境設定ファイルの更新（遠隔操作用）
- 利用した掲示板のスレッドの更新（遠隔操作用）
- コンピュータを一定の時間スリープする
- コンピュータから自身を削除する（自分自身を削除することで証拠を一切無くすことができる）

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

“通信の秘密”

日本国憲法第21条第2項
検閲は、これをしてはならない。通信の秘密はこれを侵してはならない

電気通信事業法第4条
電気通信事業者の取り扱いに係る通信の秘密は、侵してはならない

（有線電気通信法第9条と電波法第59条にも、同趣旨の規定）

インターネット時代の今日、クラウドやビッグデータの扱いが技術面、サービス面で一般化しており、個人情報をベースに便利で満足度の高いサービスがいわゆるネット企業によって提供されるようになっています。通信事業者は通信の秘密保護の刑罰規定で通信の取り扱い中の秘密を守ることが規定されているのに対し、通信事業者ではない、いわゆるネット企業にはこの種の規定はなく、バランスを欠いた状況です。もちろん、個人情報等の機密保持は事業者の契約上の責務であり、民事上の責任を負っています。

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

ネット企業において、個人情報を得て（引き換えに）検索や情報提供などのサービスを提供することが、クラウド技術やビッグデータ解析によって一層便利に、素早く、快適に行われるようになっています。ところが、通信事業者に対しては、通信の秘密について厳しい刑事罰をもって臨み、ネット企業に対しては約款内容を含めて十分な吟味がなされていないといった不均衡状態が生じています。

当然のことですが、現行憲法の下で長い間、通信事業者によって厳格に守られてきた通信の秘密を、個人情報の利活用を優先するあまり、無視してよいと言っている訳ではありません。

ネット企業との極端な不均衡、国内外企業による適用の有無の差、さらには一部にある厳格であるが故の当事者個人の契約約款への無関心、サービス提供者の約款整備の遅れなどの現実を踏まえて、これを是正するために通信事業者に対する刑事罰適用領域の運用面の明確化を求めたいと思います。

（情報通信総合研究所　相談役　平田正之）

Copyright©2004-2014 Telecom-ISAC Japan. All Rights Reserved.

通信の秘密等に配慮した新たな取り組み

■ 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000074.html

✓ ACTIVEを推進するための通信の秘密の整理についても、本研究会で新たに取り組み済

	検討課題	通信の秘密との関係等の考え方
1	マルウェア配布サイトへのアクセスに対する注意喚起	利用者が、一旦契約約款に同意した後も、随時、同意内容を変更できる（オプトアウトできる）こと等を条件に、契約約款に基づく事前の包括同意であっても有効な同意と整理
2	マルウェア感染駆除の拡大	C&Cサーバに蓄積されている、同サーバとマルウェアに感染したPC等の端末に係る通信履歴からマルウェアの感染者を特定し、注意喚起を実施することは、当該端末が正常かつ安全に機能することに対する現在の危難を避けるための緊急避難として許容される
3	新たなDDoS攻撃であるDNSAmp攻撃の防止	利用者が設置しているブロードバンドルータ等のゲートウェイに対するインターネット側からの名前解決要求に係る通信を遮断することは、電気通信役務の安定的提供を図るための正当業務行為として許容される
4	SMTP認証の情報（ID及びパスワード）を悪用したSPAMメールへの対処	他人のID・パスワードを悪用して送信されるSPAMメールへの対処として、 当該IDの一時停止や、正規の利用者への注意喚起等を実施することは、電気通信役務の安定的提供を図るための正当業務行為として許容される

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

（参考）

通信の秘密に関する同意についての基本的な考え方

通信当事者の同意がある場合には、通信当事者の意思に反しないため、通信の秘密の侵害に当たらない。もっとも、以下の理由から、契約約款等に基づく事前の包括同意のみでは、一般的に有効な同意と解されていない。

① 約款は当事者の同意が推定可能な事項を定める性質であり、通信の秘密の利益を放棄させる内容はその性質になじまない

② 事前の包括同意は将来の事実に対する予測に基づくため対象・範囲が不明確となる

（平成22年5月総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会（※）」第二次提言より）

※ 総務省主催の研究会として平成21年4月から開催。

通信の秘密侵害に関する違法性阻却事由についての基本的な考え方

○ 緊急時に行われる対策については、一般的に、正当防衛、緊急避難（※）の要件を満たす場合には通信の秘密の侵害について違法性が阻却される。

※ 「正当防衛」として違法性が阻却されるためには、①急迫不正の侵害に対して、②自己又は他人の権利を防衛ために、③やむを得ずした行為であること、の全ての要件を満たすことが必要。
「緊急避難」として違法性が阻却されるためには、①現在の危難の存在、②法益の権衡、③補充性の全ての要件を満たすことが必要。

○ 常時行われる対策については、急迫性、現在の危難といった要件を満たさないものと思われるため、正当業務行為（※）に当たる場合には違法性が阻却される。

※ 電気通信事業者による通信の秘密の侵害行為が正当業務行為となる場合については、実務上の運用事例を通じて一定の考え方が整理されてきている。これまでに正当業務行為が認められた事例は、ア．通信事業者が課金・料金請求目的で顧客の通信履歴を利用する行為、イ．ISP がルータで通信のヘッダ情報を用いて経路を制御する行為等の通信事業を維持・継続する上で必要な行為に加え、ウ．ネットワークの安定的運用に必要な措置であって、目的の正当性や行為の必要性、手段の相当性から相当と認められる行為（大量通信に対する帯域制御等）といったものが挙げられる。こうした事例の根底にある基本的な考え方は、国民全体が共有する社会インフラとしての通信サービスの特質を踏まえ、利用者である国民全体にとっての電気通信役務の円滑な提供という見地から正当・必要と考えられる措置を正当業務行為として認めるものである（平成22年5月総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言より）。

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

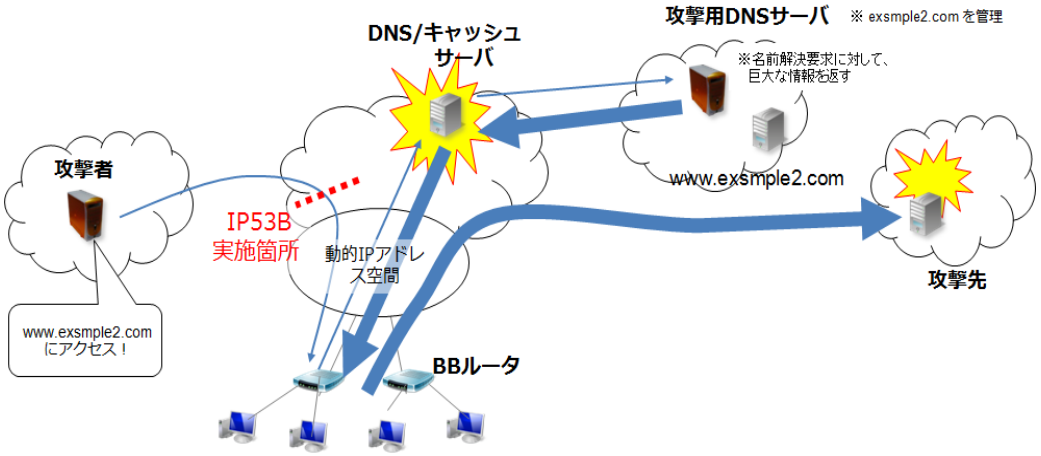
正当業務行為

○ 常時行われる対策については、急迫性、現在の危難といった要件を満たさないものと思われるため、正当業務行為に当たる場合には違法性が阻却される。

DNSAmp攻撃防止(IP53B)に関する違法性阻却の考え方

目的の正当性	攻撃に依る回線逼迫やDNSサーバの過負荷は利用者の電気通信役務利用を妨げるため、目的は妥当
行為の必要性	踏み台DNSサーバを全て発見して対策することは現実的でない。通常通信と攻撃通信の区別が難しいことからISPでの常時ブロッキングは必要
手段の相当性	通秘の侵害範囲は、宛先IPアドレス及びポート番号程度。ユーザ向けのDNSクエリは通常想定されない通信で、ブロックは影響少ない

正当業務行為の例(IP53B)



正当業務行為で行われる対策の例

- ✓SPAMメール送信ブロック (IP25B/OP25B)
- ✓DNSリフレクション攻撃ブロック (IP53B)
- ✓NTPリフレクション攻撃ブロック (IP123B)

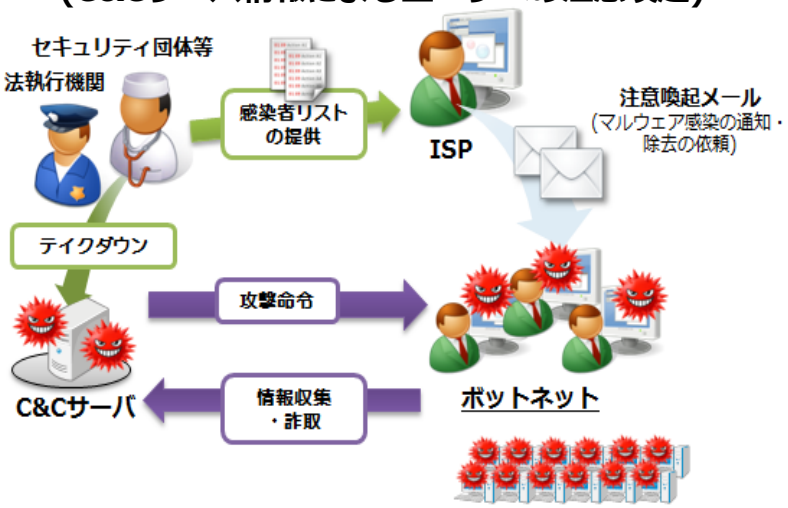
Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

緊急避難

○ 緊急時に行われる対策については、一般的に、正当防衛、緊急避難の要件を満たす場合には通信の秘密の侵害について違法性が阻却される。

C&Cサーバ蓄積情報に基づくマルウェア感染ユーザへの注意喚起に関する違法性阻却の考え方	
現在の危難の存在	C&Cサーバと通信している端末はマルウェア感染しており、C&Cサーバによる制御が実際に行われていることから現在の危難が存在する
法益の権衡	前項に示すような看過しがたい害に対し、侵害される範囲はIPアドレス・時刻から該当利用者を割り出す程度
補充性	本対策以外に有効性が認められる手立てはない

緊急避難の例
(C&Cサーバ情報によるユーザへの注意喚起)



緊急避難による対策の例

✓ユーザ申告に基づく、特定ユーザへ向けた大量通信(DDoS攻撃等)のブロッキング

✓大量ユーザへ影響を及ぼし得るISP設備への緊急的な大量通信のブロッキング

✓テイクダウンしたC&Cサーバ内情報に基づくマルウェア感染被疑ユーザへの注意喚起

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

Telecom-ISAC Japanでの通信の秘密に対する活動

サイバー攻撃対策WGを立ち上げ下記の活動を実施

- 総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会、並びにワーキンググループ（以下、総務省研究会/WG）」と連動し、マルウェア等の攻撃に対処する場合に予め考慮すべき「通信の秘密侵害罪に関する違法性阻却事由」について、事業者の立場で検討しその成果を総務省研究会/WGに報告

- 総務省WGメンバ等が検討する「マルウェア等の攻撃に対処する場合の通信の秘密との関係」について検討会を開催し、技術的・運用的視点からのアドバイスを行い、通信業界のビジネス拡大に資する検討

- 総務省「取りまとめ結果」を受けて、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン（以下、大量通信等ガイドライン）」の見直しを行い、第3版を作成

Copyright©2004-2013 Telecom-ISAC Japan All Rights Reserv

サイバー攻撃対策WGの取組み

● 総務省研究会/WGの構成員としてT-ISAC会員企業が参加し、サイバー攻撃対策と「通信の秘密」の考え方について議論、具体的な検討課題は本WGで検討を重ね、総務省研究会/WGにフィードバックするなど貢献

		12月	1月	2月	3月
総務省	研究会	11/29 第1回 ・キックオフ		2/19 第2回 ・とりまとめ案の審議	パブコメ 第3回 ・とりまとめ
	WG	12/11 第1回 ・検討の方向性の確認 ・ヒアリング	1/30 第2回 ・整理の方向性の審議	2/14 第3回 ・とりまとめ案の審議	

	12月	1月	2月	3月	4月
T-ISAC 本WG	12/19 第1回 12/26 第2回	1/16 第3回	2/14 第4回		第5回 大量通信ガイドライン改訂作業着手

5月	6月	7月	8月	9月	10月
	ガイドライン改訂作業			意見募集 反映	大量通信ガイドライン 第3版公開

Copyright©2004-2013 Telecom-ISAC Japan All Rights Reserv

ACTIVEにおける「通信の秘密」との関係

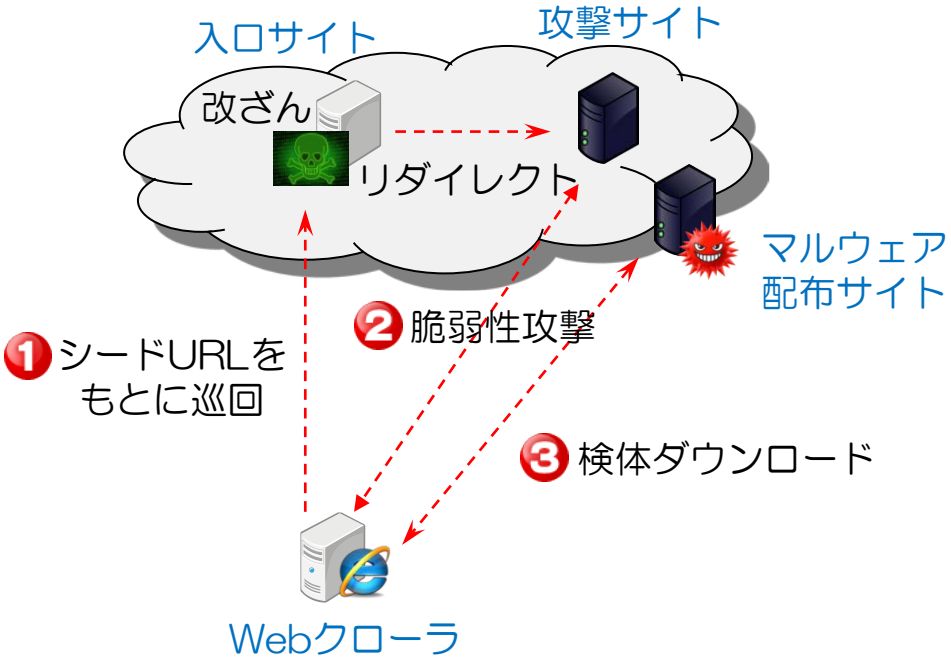
マルウェア感染防止の取り組み

- Webクローラを用いてシードURLを元に当該サイトURLの悪性判定を実施
- 利用者から事前に個別の同意を取得する

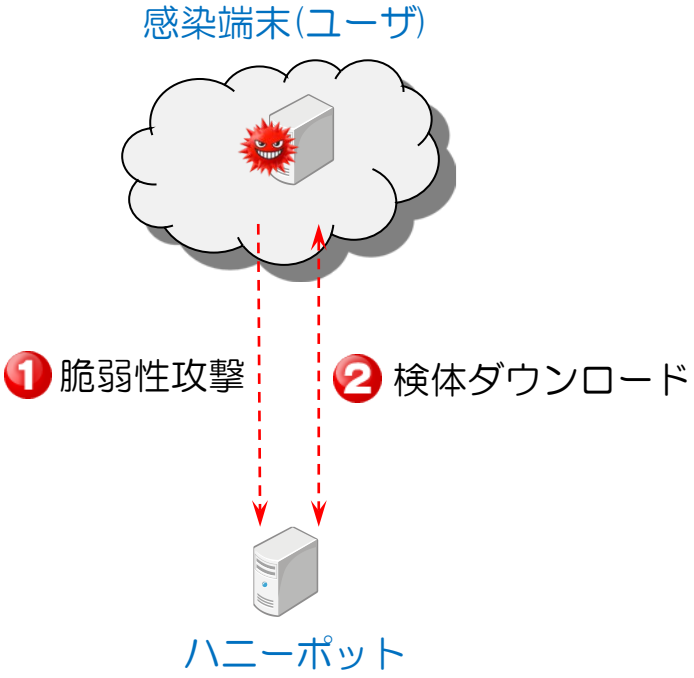
マルウェア駆除の取り組み

- ハニーポットを用いて攻撃情報を収集し、攻撃の発信元を特定
- 通信当事者として、発信元(感染ユーザ)へ注意喚起を行う

【Web感染型マルウェアの攻撃情報を収集】



【NW感染型マルウェアの攻撃情報を収集】



Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

ACTIVEにおける「通信の秘密」との関係

■ ACTIVEにおける「通信の秘密」との関係

総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」の公開資料抜粋
http://www.soumu.go.jp/main_content/000264105.pdf

（１）マルウェア感染防止の取組

① マルウェア配布サイトのURL情報をリスト化。
② マルウェア配布サイトにアクセスしようとする利用者に注意喚起。
③ マルウェア配布サイトの管理者に対しても適切な対策を取るよう注意喚起。

通信の秘密との関係

ISP等が、利用者がアクセスしようとするサイトのURLの情報を知得し、注意喚起を行うことについては、利用者の同意に基づいて行われており、通信の秘密の侵害にあたらない。

（２）マルウェア駆除の取組

① マルウェアに感染した利用者のPCを特定。
② 利用者に適切な対策を取るよう注意喚起。
③ 注意喚起の内容に従いPCからマルウェアを駆除。

通信の秘密との関係

① ACTIVE事務局が、マルウェア感染パソコンからハニーポットに来た通信における送信元IPアドレスを、当該IPアドレスの割当てを行っているISPに提供することは、ACTIVE事務局は当該通信を受信する一方当事者であり、通信の秘密の侵害にあたらないと考えられる。

② 上記ISPが、当該IPアドレスをどの契約者に割り当てたか顧客情報と突合し、該当契約者を割り出す行為は、マルウェア感染パソコンに対する現在の危難を避けるための緊急避難として、通信の秘密の侵害に係る違法性は阻却されると考えられる。

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

「通信の秘密」各国比較調査研究

- 先進諸国においては「通信の秘密」は基本的人権の一つとして保護され、その侵害に対しては、刑事罰が科せられる。
- 「通信の秘密」の根拠は、プライバシー保護の一環だとする考え方が一般的である。
- しかしプライバシー保護のあり方については、国ごとに歴史的・文化的な差があるため、保護の仕方や範囲などに微妙な差が生じている。

⇒米国・英国・オーストラリアという英米法系の国と、ドイツ・フランスという大陸法系の国、さらに隣国である韓国を加えて、それぞれの国ごとの実情を調査するとともに横断比較を行ない、わが国への教訓を探ることとした。

「インターネットと通信の秘密」研究会
構成メンバー:NTT コミュニケーションズ株式会社、株式会社KDDI総研 、ソネット株式会社 、ニフティ株式会社、ビッグローブ株式会社 、ヤフー株式会社 、一般財団法人日本データ通信協会テレコム・アイザック推進会議
調査メンバー:桐蔭横浜大学 、情報通信総合研究所 、城所 岩生(米国弁護士)、曽我部 真裕(京都大学法科大学院)、高橋 郁夫(弁護士)、松前 恵環 (駒澤大学)、吉田 一雄 (清和大学)、モバイルコンピューティング推進コンソーシアム・モバイルセキュリティ委員会
協賛メンバー: キヤノングローバル戦略研究所
事務局:林 紘一郎 、田川 義博 (情報セキュリティ大学院大学)、橋本 清貴 (桐蔭横浜大学)

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

「通信の秘密」各国比較調査研究

- 「通信の秘密」は絶対的保障を受けるわけではなく、「公共の福祉」の観点から、より高位の法益があれば制限される場合があることは、共通した理解である。
- わが国も理論的には同じ理解に立っていると思われるが、実際の運用は極めて厳格で、明確な「違法性阻却事由」がない限り「通信の秘密」が守られるとしている点は、先進諸国の間では「保護の程度が高い」類型になる。
- 「公共の福祉」の観点から、通信傍受などが違法性を阻却されるケースは、大きく分けて以下のように分けられる。

(a) 事業者のネットワーク制御に伴うもの

(b) 公権力の関与に伴うもの
- (b-1) 犯罪捜査に伴うもの
- (b-2)国家安全保障にかかわるもの

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

「通信の秘密」各国比較調査研究

- 本調査では、(a)事業者のネットワーク制御に伴うものについて、ISPが関与する以下の5つの個別事項に関して、各国での実施状況・法的規定・利用者の同意の3点について、調査を行った。①迷惑メールのフィルタリング(ブロッキング)、②帯域制御、③サイバー攻撃などに対する情報セキュリティ対策、④違法コンテンツサイトへのアクセスブロッキング、⑤行動ターゲティング広告。

- その結果、これらの事項は調査対象のいずれの国においても何らかの形で実施されているが、「各国ともほぼ同じようなレベルで実施されているもの」と「実施されているが、ISPが関与する程度が異なるもの」がある。また関与を認める法的根拠や実際の運用についても、必ずしも各国で足並みが揃っているわけではない。

- このように一般的な傾向が明確でない中で、各国のISPの関与について強いて大きな分類をすれば、EU型においては「ネットワーク中立性」が重視され、事業者の裁量が制限されているのに対して、アメリカ型ではネットワーク事業者の自由度が高いという対照があるように思われる。なお、ここでネットワーク事業者というのは電気通信事業者に限らず、コンピュータ・サービス提供者を含めた概念であり、後者において営業の自由度が高いのは「インターネット非規制政策」を取ってきた同国の特徴と考えられる。電気通信事業者に限って言えば、アメリカ型でも「ネットワーク中立性」の議論がある。

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

参考:「通信の秘密」各国比較調査研究

■「サイバー攻撃などに対する情報セキュリティ対策」に関する比較

①実施状況:各国とも実施、②法的規定、③利用者の同意については以下の通り若干の違いがある。

	情報セキュリティ対策に関する法的規定と利用者の同意
米国	通信傍受法(18USC2511条(2)(a)(i)は、事業者の権利、財産を保護するために社員に通信傍受を認める規定。 ペンレジスター法(18USC3121条(b)は、事業者の権利、財産の保護に加えて、サービスの濫用や違法使用から加入者を保護するために、ペンレジスター（通話を追跡するが、録音はできない装置）の設置を認める規定。 注：ECPA（電子通信プライバシー法）は、三つの部分からなっており、上記の法はいずれもECPAに含まれている法規定であ
英国	電気通信法2003一般契約条項「通信プロバイダにおいてセキュリティまたはインテグリティのインシデント、脅威、脆弱性に対する手法のタイプ」として、利用者への情報提供が求められる。ISPがそのような環境で一方的な行動を取る権利は利用約款で与えられているので、利用者の同意は一般的に求められていない。
ドイツ	電気通信法109条1節では、ISPは「通信の秘密」の保護対象であるデータ・コンテンツを保護するために十分な技術的安全性を保障する義務がある。 同法100条では、上記の保護を行うためにトラフィックデータや登録データを収集、処理することを認めている。 データ・コンテンツ保護のためのステップが適切であれば、利用者の同意は不要。

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

参考:「通信の秘密」各国比較調査研究

	情報セキュリティ対策に関する法的規定と利用者の同意
フランス	トラフィックブロッキングは、帯域制御の一つ。電子プライバシー法4条で、ISPにサービスのセキュリティ確保のための対策を取るように求めている。
オーストラリア	法的な規定はない。利用者の同意は不要。
韓国	情報通信網利用促進法46条の2 利用者の同意は、利用約款による包括同意で良い。

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

ここで、不幸な日本の国民共通番号の歴史（石川宏NTT-AT元社長資料）

- 1968年佐藤栄作内閣が「各省庁統一個人コード連絡研究会議」を設置
  大蔵、警察、外務、厚生、運輸など12省庁が国民総背番号制の導入を目指したが頓挫した
- 1980年「グリーンカード（少額貯蓄等利用者カード）法案」が可決
  1985年、「海外への資金流出」、「プライバシー保護」などの反対運動により、同法廃止
- 2002年「住民基本台帳ネットワーク」
  さまざまな反対の中で稼働
- 2007年「消えた年金問題」発覚
  氏名や住所の異動を管理する台帳の裏づけが無い番号を使っていたため、年金の納付記録が行方不明に
- 2008年麻生太郎内閣「定額給付金政策」発表
  すべての国民の所得捕捉ができていないために、所得制限をかけることができず、莫大な経費をかけて全ての国民に給付
- 2010年「消えた高齢者問題」発覚
  「死亡届」が出されない限り生存していることを前提とした住基台帳制度の機能不全
- 2011年「東日本大震災」
  死亡確認ができない。避難所が全国に、被災者支援ができない

Copyright©2004-2013 Telecom-ISAC Japan All Rights Reserv

日本の個人番号の現状 （石川宏NTT-AT元社長資料より）

- 漢字の姓名だけでは、名寄せができない

わたなべ　様 ⟹ 渡辺？渡部？渡邊？渡邉？

邉邉邉邉邉邉邉邉邉邊邊邊邊邊邊邊邊邊
邉邉邉邉邊邊邊邊邊邊邊 ？？？？？？？？？

- 一人にたくさんの公的ID番号
- 結果として膨大な不整合作業による非効率とユーザの不便

運転免許：
パスポート：
住基カード：
基礎年金番号：
介護保険：
国税納税システム：
健康保険：　etc.

Copyright©2004-2013 Telecom-ISAC Japan All Rights Reserv

日本のICT産業活性化のためにも…

- 「通信の秘密」の原点（真の自由と公益）に立ち返り
  行き過ぎた「個人情報保護法」を見直し
  先進国の中でも日本が最も遅れをとっている

マイナンバー（国民共通番号ID）

を早く官民分野ともに導入し（**16年1月必守**）
悪平等でなく、真に公平な社会を改めて実現することが、
技術者のインセンティブ向上、
世界の中における日本のICT産業復活、
そして（今後益々増大する）ネット犯罪抑制につながる！

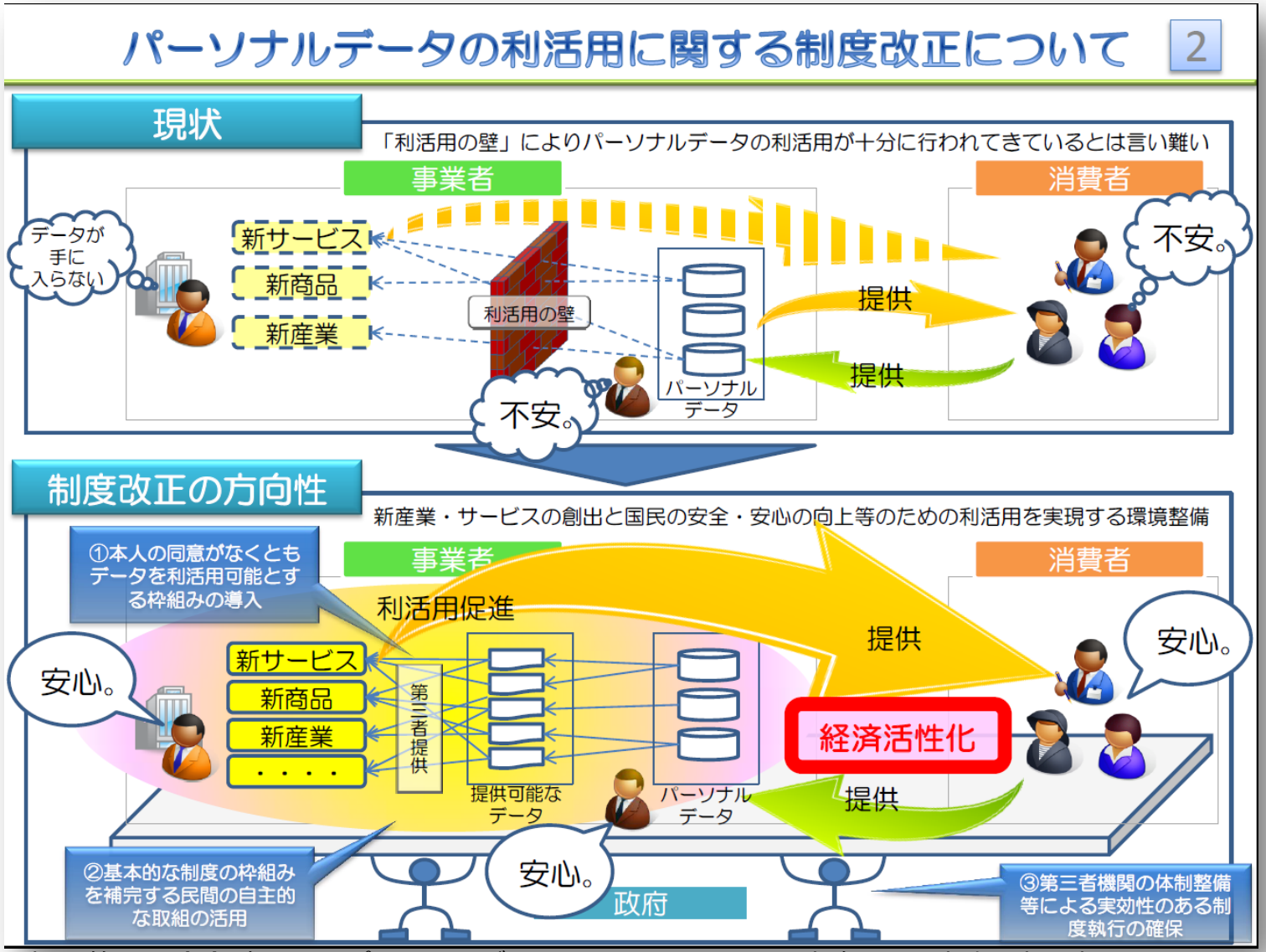
「過度のプライバシー保護」⇒　国民の「自己確立の未熟さ」

↓

日本も今や真の成熟国家へ！

Copyright©2004-2013 Telecom-ISAC Japan All Rights Reserv

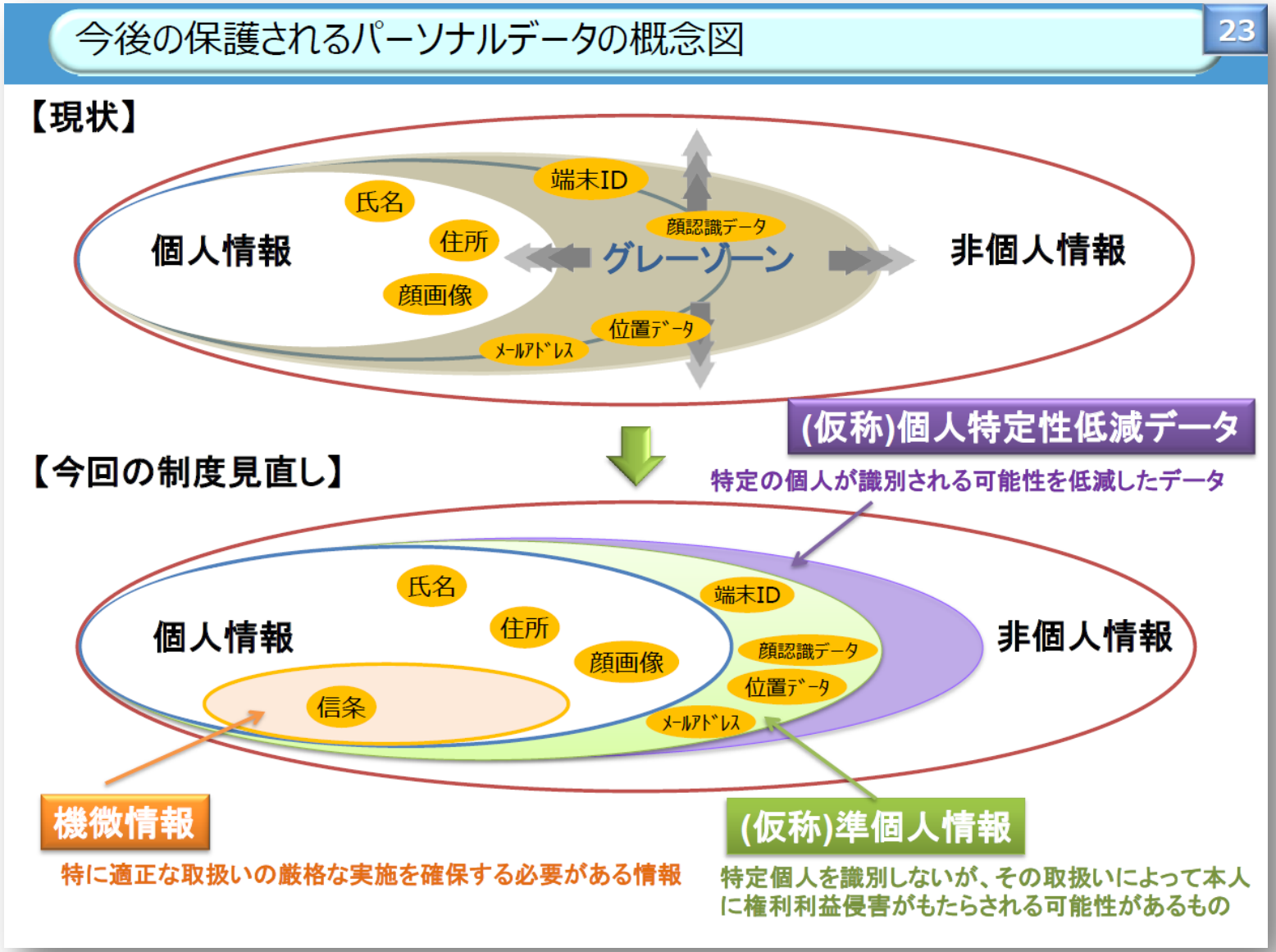
パーソナルデータ研究会の制度改正の基本的な考え方について



(引用) 第10回会合 資料4-1 パーソナルデータの利活用に関する制度改正の基本的な考え方について(2014/5/29)

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

パーソナルデータ研究会が検討するパーソナルデータの概念図



(引用) 第7回会合 資料1 「個人情報」等の定義と 「個人情報取扱事業者」等の義務について （事務局案）(2014/4/16)

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

パーソナルデータ利活用に関する制度見直し

Ⅰ パーソナルデータの利活用に関する制度見直しの背景及び趣旨

今年で個人情報保護法の制定から10年を迎えたが、情報通信技術の進展は、多種多様かつ膨大なデータ、いわゆるビッグデータを収集・分析することを可能とし、これにより新事業・サービスの創出や我が国を取り巻く諸課題の解決に大きく貢献する等、我が国発のイノベーション創出に寄与するものと期待されている。特に利用価値が高いとされているパーソナルデータについては、個人情報保護法制定当時には想定されていなかった利活用が行われるようになってきており、個人情報及びプライバシーに関する社会的な状況は大きく変化している。

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

その中で、個人情報及びプライバシーという概念が広く認識され、消費者のプライバシー意識が高まってきている一方で、事業者が個人情報保護法上の義務を遵守していたとしても、プライバシーに係る社会的な批判を受けるケースも見受けられるところである。また、パーソナルデータの利活用ルールの曖昧さから、事業者がその利活用に躊躇するケースも多いとの意見もある。

さらに、企業活動がグローバル化する中、情報通信技術の普及により、クラウドサービス等国境を越えた情報の流通が極めて容易になってきている。国内に世界中のデータが集積し得る事業環境の整備を進めるためにも、海外における情報の利用・流通とプライバシー保護の双方を確保するための取組に配慮し、制度の国際的な調和を図る必要がある。

EU:「データ保護規則」提案、
米国:「消費者プライバシー権利章典」公表、
OECD:「OECDプライバシーガイドライン」改正等

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

このような状況の変化を踏まえ、平成25年６月に決定された「世界最先端IT国家創造宣言」において、

IT・データの利活用は、グローバルな競争を勝ち抜く鍵であり、その戦略的な利活用により、新たな付加価値を創造するサービスや革新的な新産業・サービスの創出と全産業の成長を促進する社会を実現するもの

とされていることから、個人情報及びプライバシーの保護を前提としつつ、パーソナルデータの利活用により民間の力を最大限引き出し、新ビジネスや新サービスの創出、既存産業の活性化を促進するとともに公益利用にも資する環境を整備する。さらに、事業者の負担に配慮しつつ、国際的に見て遜色のないパーソナルデータの利活用ルールの明確化と制度の見直しを早急に進めることが必要である。

内閣府　IT戦略本部　パーソナルデータ検討会
（2013．12．10）

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

提言(１)

サイバー攻撃は複雑多様化しており、組織にとってもはやIT部門のような一部署だけで対応できる範疇を超えている。セキュリティは全組織的な影響を及ぼす「課題」として取り組むべきである

- **リスク評価・リスクマネジメントの必要性**
  - ・組織の守るべき情報資産と漏洩・流出した場合のコストを算出
  - ・コストに見合うセキュリティ対策を講じるべき
    - ⇒絶対破られないセキュリティは無い
      - インシデント発生時にどこまでリスクを許容できるか決めておくべき
  - ・コストは1次被害（賠償金・被害復旧費用）と2次被害（サービス・業務停止による機会損失、信用低下）がある。2次被害の方が大きなコストになることも多い

端緒：

・情報流出: 2005年5月、米国のクレジットカード処理会社から約390万件のカード情報漏洩
　→ **日本人も約1億1000万円の被害**
・情報流出: 2006年3月、複数のインターネットショッピング加盟店で、顧客情報がWinnyのネットワークに流出
　→ **インターネット上の店舗が休店**
・不正な侵入: 2005年5月、インターネットで情報提供事業を行う企業のHPで不正改竄、閲覧者がマルウェア感染
　→**ホームページ上の事業が10日間ストップ**

出典: JPCERT/CC 経営リスクと情報セキュリティ ～ CSIRT：緊急対応体制が必要な理由 ～

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

提言(2)

- **サイバー攻撃の危険はすぐ身近にある**

シマンテックによると、2011年ですら標的型攻撃を受けた組織の従業員規模毎の内訳は以下の通り

> 100人以下…15%強
> 101～500人以下、501～1500人以下、1501～5000人以下…いずれも25%

上記のデータからも「中小組織だから狙われない」ということは全くないといえる

中小組織が狙われる理由として、

・革新的な知的財産を保有している

・大組織と取引があり、セキュリティの甘い中小組織を攻撃のとっかかりとして狙う

- **セキュリティ基本動作励行**

サイバー攻撃の多くは既知のソフトウェア脆弱性を利用して攻撃してくる

ソフトウェア最新化は重要かつ効果的

-サーバ管理者はOS・ミドルウェアの脆弱性情報を欠かさずチェックする

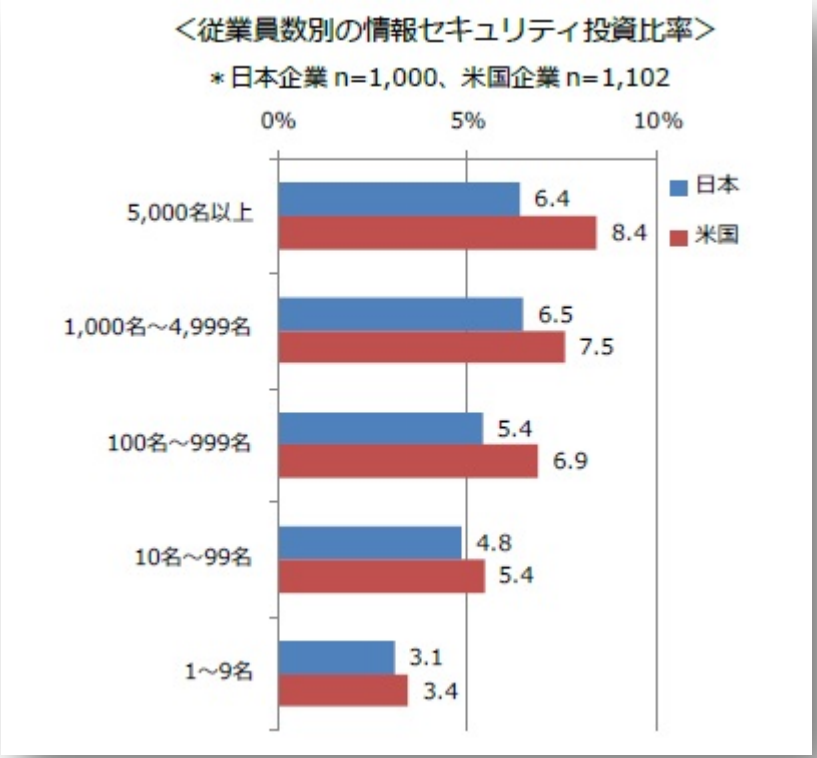
-PC/サーバのセキュリティソフトの定義ファイルを常に最新化する

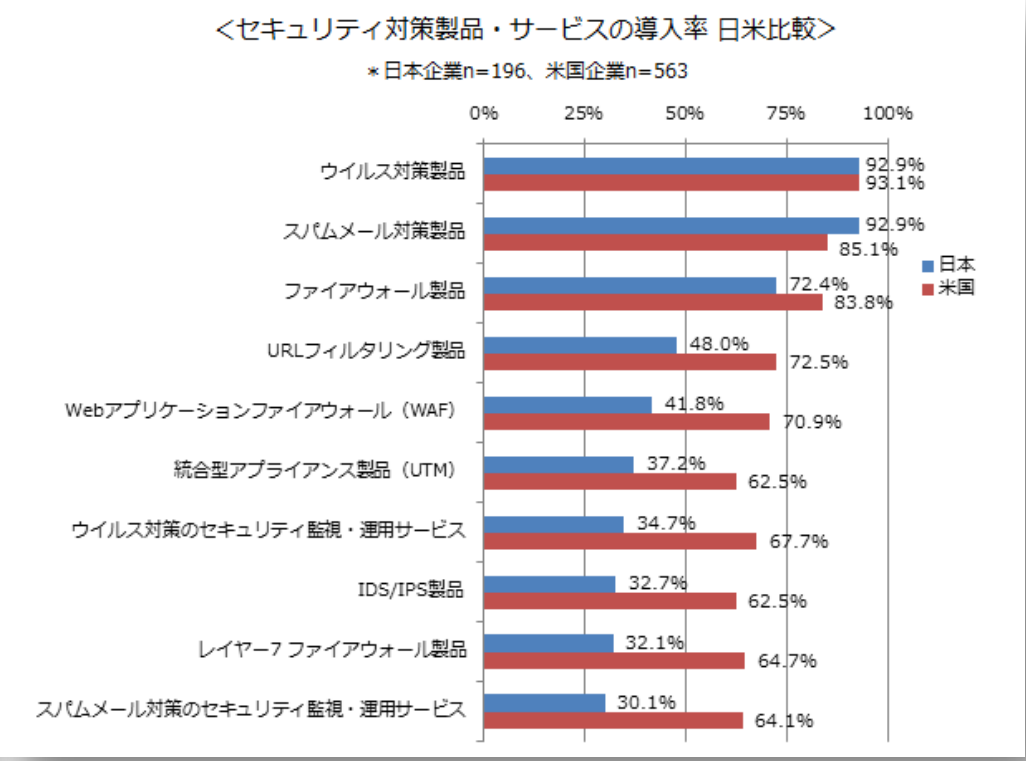
-Windows端末を使っている人はWindowsUpdateも欠かさず実施する

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

セキュリティ投資にみる日米比較

日米企業に行ったセキュリティ投資関連に関する調査結果によると、日米ともに情報セキュリティに関して「重要と考えている」傾向はみられるものの、実際の投資額には大きな開きが見られる。





(出典) http://www.m2ri.jp/newsreleases/main.php?id=010120131226500

Copyright©2004-2013 Telecom-ISAC Japan All Rights Reserv

これからどうすればいいのか？

『受動的な無責任』改めよ

多くの人が「安全・安心」を強調する。しかし、大事なのは安全の確保であって、安心の確保ではない…国民が安心を求め、リスクをゼロにせよといえば、政府はこれに答えて、リスクはゼロだという。こういうフィクションはやめるべきだ。人生はリスクに満ちている。リスクを直視し、これをできるだけ減らすように様々な努力をし、あとはリスクを取って行動することが必要だ。日本の経済発展の停滞も根源にあるのはリスクを取らない精神ではないだろうか。

（北岡伸一　国際大学学長）

© NEC BIGLOBE, Ltd. 2011

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

「安全・安心」は誰かが与えてくれるという観念

↓

「自己確立・自己責任」社会になれるか？

その象徴《日本人のリスク観形成要因》

奈良由美子『生活とリスク』(2007)より

日本人はリスクに極めて敏感で、ゼロリスクを志向するが、無理な場合は、安心がとたんに不安に変わる。リスクを小さくしようとするのでなく、しょうがないとあきらめることで気持ちの折り合いをつける

リスクを程度でなく、イチかゼロで捕らえる傾向が強い

＜日本＞

ひとびとのリスク不安に最大限の対処しよう(してもらおう)とする　安心優先のリスク管理が顕著になる

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

＜米国＞

外国との軍事緊張、多文化・他民族、多様な価値観が作り出す社会的　葛藤を抱えている国では、社会の内部に異質な要素を含みながら　社会的合意を形成しなければならない。リスクに対する配慮よりも、本来の課題遂行や目的達成を重視する。この結果、リスクを受け入れやすい風土が形成される。この場合、リスクは回避でなく、低減すべき対象となる

＜日本人のリスク観形成要因＞

不確実性の回避傾向

ある文化の成員が不確実な（何が起こるか、それが何か、いつ、どの位起こるかが分からない）状況や未知の状況に対して脅威を感じることが強い

現状肯定的心情

日本人には、与えられた現実を受け止めるという伝統的な思考や態度がある（自然をコントロールするという欧米的自然観に対して、自然に人間が合わせることは日本人の伝統的な生き方）　⇒平穏な現状維持を求めながら、そうでない変化が生じた場合には受け入れる。この思考が、リスクに対してあきらめるという観念の形成に関わっている

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

＜日本人のリスク対応＞

・論理的・合理的・統計的なリスク対応が不得手

・異常を背景の中に埋没させてしまったり、他者が行動するまで何もせず行動が鈍くなる傾向

・日本社会の同化構造があり、社会通念から逸脱せずに、雰囲気も壊さないで、皆と一緒であろうとする

・自助努力より公助・共助によるリスク引き受け

・従って、個人が自分で事前にリスクを発見したり、そのための準備を行ったりすることは必要なかった

・しかし、相互扶助システムは崩壊しつつあり、自己責任・自助努力が求められる程度が大きくなっている

＜リスク文化の転換＞

・文化の問題でもあり、個々人のリスク観やリスク対応を変えることはそう簡単ではない

・しかし、目的を達成するための方法は、多様であり、個々の社会のリスク文化を尊重し、認め合い、良いところはきちんと学ぶ姿勢は可能であろう！

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

最後にラジカルな“私的意見”と“公共哲学”の復権

- OTT(Over The Top)企業はネットワーク・インフラ事業者の利益をはるかに上回っており、そのご利益（りやく）は特定企業に偏在し海外にも流出
- 一方、インフラの重要性はナショナル・セキュリティ上からも不変
- 国の安全は軍事ネットワークだけでは対応不可能であり、官民連携の重要性を見せつけたのが“９．１１”
- 産官民学の連携によるICT利活用の飛躍的復活とそれを支えるインフラの“復権”なしには日本（情報通信産業）の将来はない！
- 癒着防止という建前のためか、日本弱体化戦略？に負けたのか、「産官学一体戦略」と「強いものをより強くして世界に立ち向かう作戦」不在で来た日本の不幸
- “情報通信審議会”もやっとNTTグループの固定・移動統合サービス容認で国力回復？に乗り出したが、
- 「独占回帰論」「光ファイバー分岐貸し」という“プロパガンダ”とNTTによる「光ファイバー卸し提供」という“背水の陣”とのせめぎあいがどうなるか興味津々！

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.

ハーバード大学マイケル・サンデル教授の言葉

過去30年間、米国では行き過ぎた「市場勝利（原理）主義」が席巻してきた…政治が正義、平等・不平等、家族・コミュニティーの存在意義などを巡る問題に取り組まなくなった…それこそ米国、日本などの国々に共通する人々の不満の源泉となっている…この問題と向き合う唯一の方法は、市場が扱う品物について公的な議論を重ねることだ…市場が生み出す公的なサービスとそうではないものについて、開かれた議論をしなければならない…大きな政府でも自由放任（＝小さな政府）でもない、代替案はある。それは公共的な社会を創設することだ…そこに暮らす人々が確かな絆を感じ、相互に責任感を持てるような社会だ…ここで重要なのは社会的な多元性を評価することだ．．．

（日経新聞）

Copyright©2004-2013 Telecom-ISAC Japan. All Rights Reserved.