資料3

サイバー攻撃対策の取り組みについて

～マルウェア対策と通信の秘密～

2013年11月29日

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
（Telecom-ISAC Japan）
小山覚

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

1.Telecom-ISAC Japanについて

2.サイバー攻撃の事例と課題

3.今後の取組み

1. Telecom-ISAC Japanの概要

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

緑文字は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 、NEC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 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) 、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、社団法人電気通信事業者協会（TCA）

Telecom-ISAC JapanのWG/SiGの設置状況

WG

④ 継続的に活動を実施
⑤ 仲間の醸成

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

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

③ 活動に厚みをつける
① 新たな課題の抽出
② 新たな連携の可能性を抽出

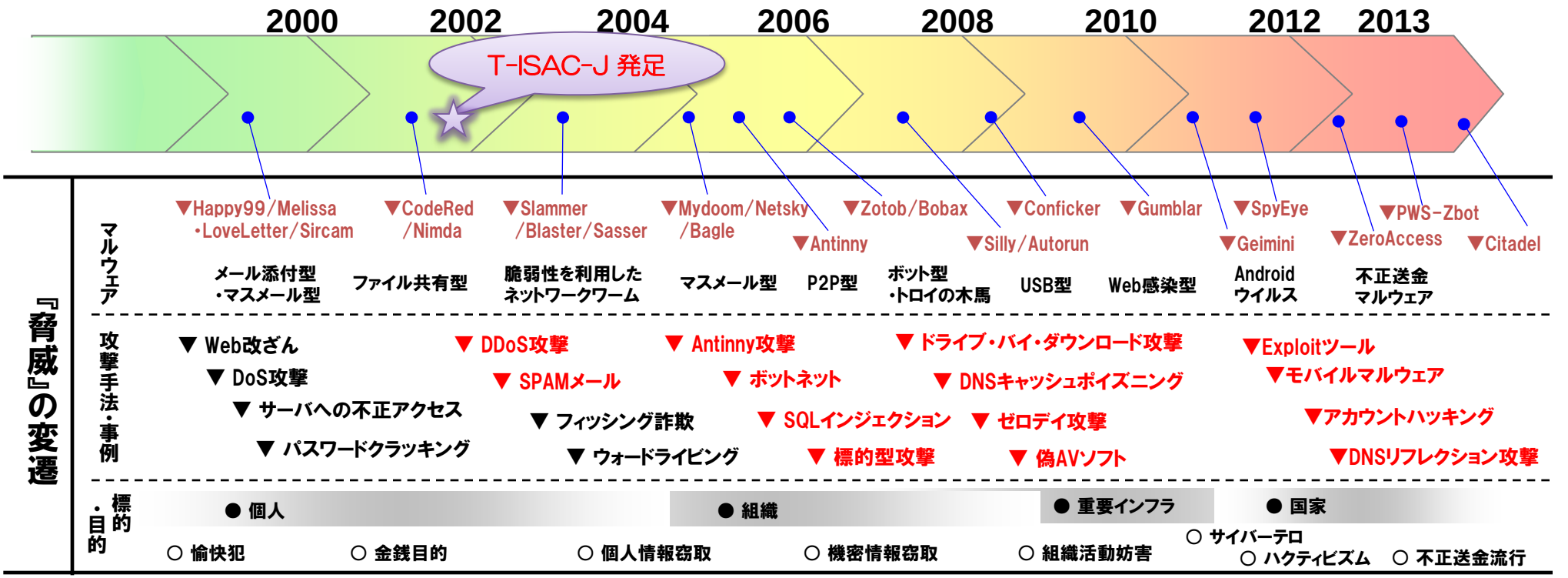
SiG

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

WG/SiG運営方針

- 課題解決型の多様な活動グループを運営
- 3社以上が参加意向を示した課題を対象とする
- 各グループが月1回以上の会合・勉強会を実施
- 共同連携の実施など

ネットワーク脅威とTelecom-ISAC Japan



DoS/DDoS 協調対応2004~

Cyber Clean Center 2006~2011

NWディバイス調査 2012~

RDB 2009~2012

PRACTICE 2011~2016

ACTIVE 2013~

近年の特徴

●攻撃側のリスクが低くコストが安い「マルウェア」を活用する傾向

●簡単に乗っ取れるWebサイトから、ユーザPC(デバイス)にマルウェアを感染させ悪用

●クレジットカード情報など金銭目的の①情報窃取と、②DDoS攻撃などの迷惑・妨害行為に大別
①企業機密・重要インフラ情報・国家機密など深層情報へのアクセスが目的に
②DNS等を踏み台にしたDDoS攻撃などの事例も増加(攻撃の効率化)

1.Telecom-ISAC Japanについて

2.サイバー攻撃の事例と課題

3.今後の取組み

1. 感染したマルウェアの主な動作

パソコンに感染したマルウェアは、感染したPCの利用者が被害を受けるだけでなく、関係の無い第三者や企業等にも悪影響を及ぼす可能性がある。

■アカウント/個人情報不正取得 (Zbot/SpyEye等)

・偽Webサイト画面を表示し、**口座番号/暗証番号/クレジットカード番号を不正取得**する
・サーバやPC内を探索し、保存された**アカウント情報**を不正取得する

■ボットPC化による遠隔不正操作

-マルウェアによってボットネットに接続され、**攻撃者によって遠隔操作可能**なボットＰＣとなり、**DDoS攻撃やSPAMメール送信等の不正行為に利用される**

口座番号
暗証番号
クレジットカード番号
アカウント情報

DDoS攻撃
SPAMメール
不正クリック

攻撃対象
Webサイト等

攻撃者

■偽ウィルス対策ソフトの画面表示

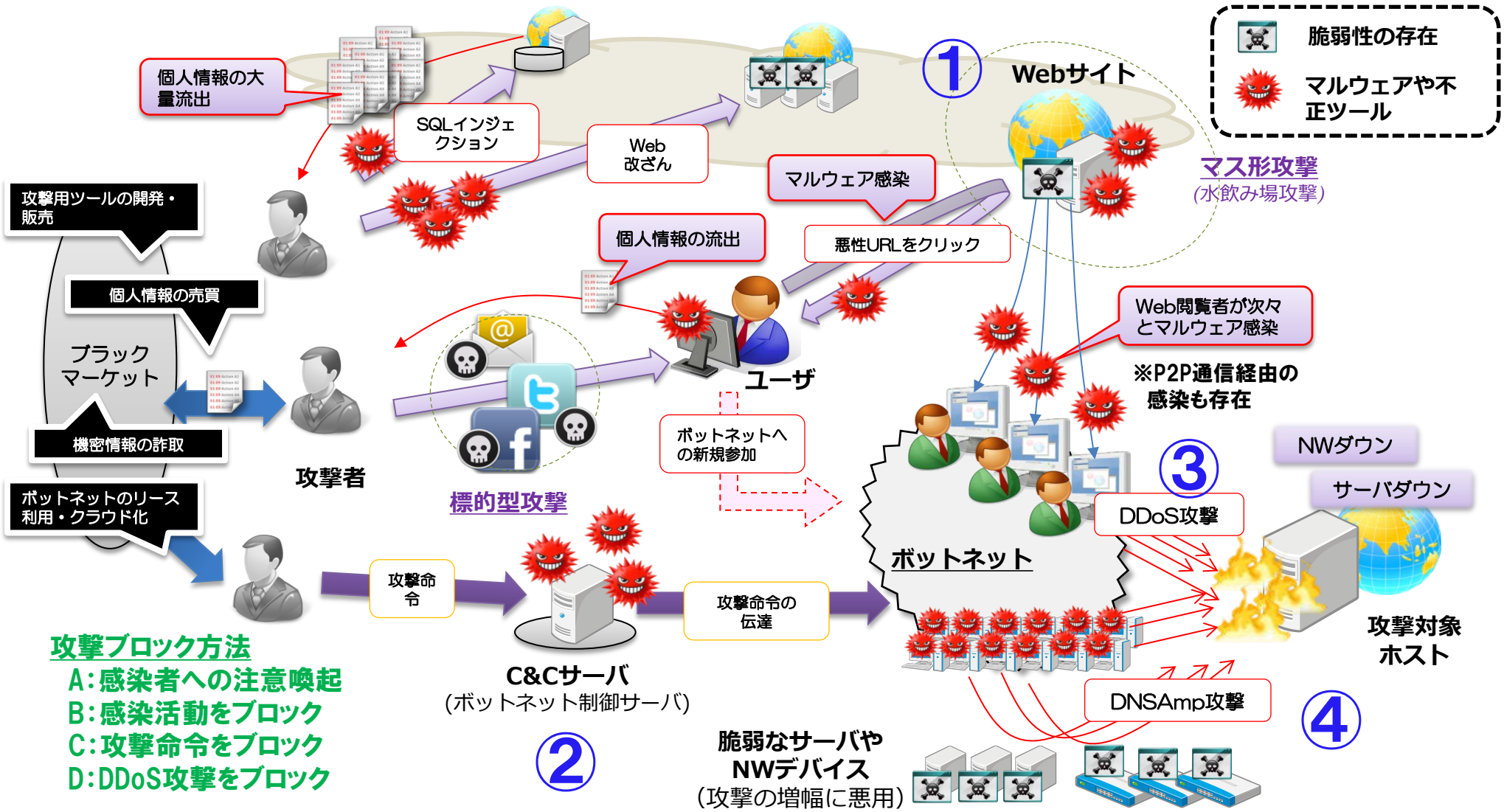
-ウィルス感染を注意喚起する画面を表示し、ウィルス対策ソフト購入に見せかけた画面で**クレジットカード番号を不正取得**する

■クリック報酬型広告の不正クリック (ZeroAccess)

-ボットPCを遠隔操作し、対象のクリック報酬型広告に不正クリックの通信を大量に送信することで、広告主から不正に報酬を獲得する

2. マルウェアの感染経路と感染防止方法（総論）

マルウェアに感染したユーザ（PC・サーバ）への注意喚起や啓蒙に加え、マルウェア特有の感染活動(Exploit攻撃)や攻撃命令など検知し、当該IPアドレスからの通信をブロックすることで、攻撃の軽減と二次被害の防止が期待できる。
ただし、このような攻撃ブロック方法については、その実現可能性について検討が必要。



1.Telecom-ISAC Japanについて

2.サイバー攻撃の事例と課題

3.今後の取組み

ISPによるサイバー攻撃対応の現状と今後の取組み

● 自社設備に影響のある攻撃には「大量通信ガイドライン」を参考に能動的に対応しているが、ユーザ設備に対する攻撃への対応は課題が多い

	攻撃種別			記事
	DDoS攻撃（DNSAmpも含む）	マルウェア感染	不正侵入	
1.サーバなど事業者設備に影響がある場合	○	○	○	DoS攻撃対策は、大量通信ガイドラインが奏功
2.PCなどユーザ設備に影響がある場合	△～×	×	×	業界のコンセンサスが得られず、対策の方向性が定まっていない領域

※全てのISPが同じ対応をしている訳ではありません。

○：予防的対策と事後対応の両方が一定レベルで実現
△：通信設備影響発生時など、事後対策で対応中
×：ユーザの要請に基づいて対応

今後WGで検討したい事項→ガイドラインに反映したい

攻撃ブロック方法の検討事項

- A:感染者への注意喚起 ： 効果的な方法の検討、テイクダウンしたサーバ情報の活用
- B:感染活動をブロック ： 同意の取得の緩和の可能性について検討、脆弱性攻撃と正当な通信の適正な区別可能性について検討
- C:攻撃命令をブロック ： OP25Bを参考にした攻撃のブロッキングを検討
- D:DDoS攻撃をブロック ： ISP業界横断的な連携対処

ご清聴ありがとうございました