公開用

同時多発的DDoS攻撃への対応と即応体制の整備

～事例とISP等の情報共有･協調対処の取り組み～

2012年7月5日

NTTコミュニケーションズ株式会社

湯口 高司

説明内容

DDoS攻撃は大規模化／同時多発化の傾向にあり、インターネットの通信インフラを脅かす規模に変化している。

本説明では、NTTコミュニケーションズにおける同時多発的DDoS攻撃の事例と、ISP等の情報共有・協調対処を目的としたテレコム・アイザック推進会議（Telecom-ISAC Japan(以下、T-ISAC-J)）における「同時多発的DDoS攻撃への対応と即応体制の整備」の取り組みを紹介する。

- 同時多発的DDoS攻撃の事例紹介
  - ✓ 2010年9月 DDoS攻撃のNTTコミュニケーションズの観測状況
  - ✓ 2012年6月 Anonymousによる攻撃予告（#opJapan）
- Telecom-ISAC Japan DoS攻撃即応-WGの取り組み
  - ✓ DoS攻撃即応-WG発足の背景
  - ✓ DoS攻撃即応-WGの活動
  - ✓ 重要インフラ観測システム

同時多発的DDoS攻撃の事例紹介

2010年9月 DDoS攻撃の事例

Global ICT Partner
Innovative. Reliable. Seamless
NTT Communications

➢ サイバー攻撃の予告

毎日新聞　2010年9月13日

中国：最大ハッカー、日本政府機関サイト攻撃を予告（2010年9月13日 21:12 ）
【北京・成沢健一、浦松丈二】13日付の香港紙「明報」によると、中国最大のハッカー組織とされる「中国紅客連盟」は12日、日本政府機関のウェブサイトを18日まで攻撃する方針を発表した。日本の海上保安庁巡視船と衝突した中国漁船の船長が逮捕された事件に抗議するためといい、満州事変（1931年）の発端となった柳条湖事件から79年に当たる18日に最大規模の攻撃を仕掛けると表明している。

- ✓ **最大規模の攻撃**　2010年9月18日（土）　21時（9月18日は満州事変勃発日）
- ✓ **攻撃予告対象**　日本の各中央省庁サイト、各都道府県サイト、民間サイト
- ✓ **被害想定**　Webサイトの改ざん、大量パケットによる閲覧遅延

➢ サイバー攻撃の被害

毎日新聞　2010年9月18日

サイバー攻撃？：警察庁と防衛省HPが閲覧障害

警察庁のホームページ（HP）が16日夜から17日未明にかけて、防衛省のHPも15日夕にいずれも閲覧しにくい状態になったことが分かった。大量のデータを送りつけて機能障害に追い込む「DDoS攻撃」を受けた可能性がある。海上保安庁の巡視船と衝突した中国漁船の船長が逮捕された事件への抗議として中国のハッカー組織「中国紅客連盟」が日本政府機関のウェブサイトを攻撃すると表明したが、両省庁とも「関連は不明」としている。【鮎川耕史】

2012年6月 Anonymousによる攻撃予告（#opJapan）

Global ICT Partner
Innovative. Reliable. Seamless
NTT Communications

ハッカー集団「アノニマス」、日本を標的に
改正著作権法「ネットの自由侵害」

2012年6月28日 日本経済新聞

2012/6/28 0:22

小 中 大　印刷

財務省や最高裁、民主党などのホームページ（HP）が相次いでサイバー攻撃にさらされた。仕掛けたのは国際的なハッカー集団「アノニマス」。20日に成立した改正著作権法が自由なインターネット利用を侵害するとして、大規模な示威行動に打って出たとみられる。

日本政府などへの宣戦布告は25日だった。違法ダウンロードに刑事罰を科す改正著作権法に反対を表明。活動告知サイトなどを通じて「＃opJapan（オペレーションジャパン）」を開始すると宣言した。

サイバー攻撃は26日午前2時ごろに始まった。内閣官房情報セキュリティセンターがまず財務省のHPへの不正侵入に気付いた。財務省は不正な情報が書き込まれていることを確認したうえで、午後2時に「国有財産情報公開システム」のサイトを閉鎖した。

攻撃は続いた。最高裁によると、午後8時50分ごろから

アノニマスによる日本国内への攻撃

ネットの規制に抗議するアノニマスのメンバー＝ロイター

- 財務省のシステムに不正侵入（26日）
- 最高裁のサイトに障害（26日夜）
- 国交省の霞ケ浦河川事務所のホームページを改ざん（26日夜）
- 自民党のサイトに障害（26～27日）
- 民主党のサイト、接続が難しい状況に（27日）

画像の拡大

同時多発的DDoS攻撃への対応と即応体制の整備

～Telecom-ISAC Japan DoS攻撃即応-WGの取り組み～

2012年7月5日

NTTコミュニケーションズ株式会社
Telecom-ISAC Japan　ｽﾃｱﾘﾝｸﾞ･ｺﾐｯﾃｨｰ運営委員
Telecom-ISAC Japan　DoS攻撃即応-WG 副主査

湯口 高司

テレコム・アイザック推進会議の紹介

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

Members

緑文字はISP・通信事業者を示す

会員企業

会長: NECビッグローブ株式会社

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 、NTTデータ先端技術株式会社

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 、株式会社フォティーンフォティ技術研究所 、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) 他

DoS攻撃即応-WG発足の背景

DoS攻撃即応-WG発足の背景

- DDoS攻撃は大規模化／同時多発化の傾向
  - ✓ 諸外国において国家規模での通信断が発生する等、インターネットの通信インフラを脅かす規模に変化
    - 海外事例　　韓国DDoS攻撃（2009年7月、2011年3月）
    - 国内事例　　尖閣諸島問題を背景とした省庁等へのDDoS攻撃（2010年9月）
  - ✓ 被害企業やISP各社の努力により対策がなされているが、それぞれの会社の対応能力に依存

- T-ISAC-JでのDDoS攻撃対応の現状の課題
  - ✓ 会員企業からの自発的な情報提供がないと初動が取れない
  - ✓ 同時多発的な攻撃の全容を把握することができない
  - ✓ 国内から国内への攻撃事案への対応能力の限界 等

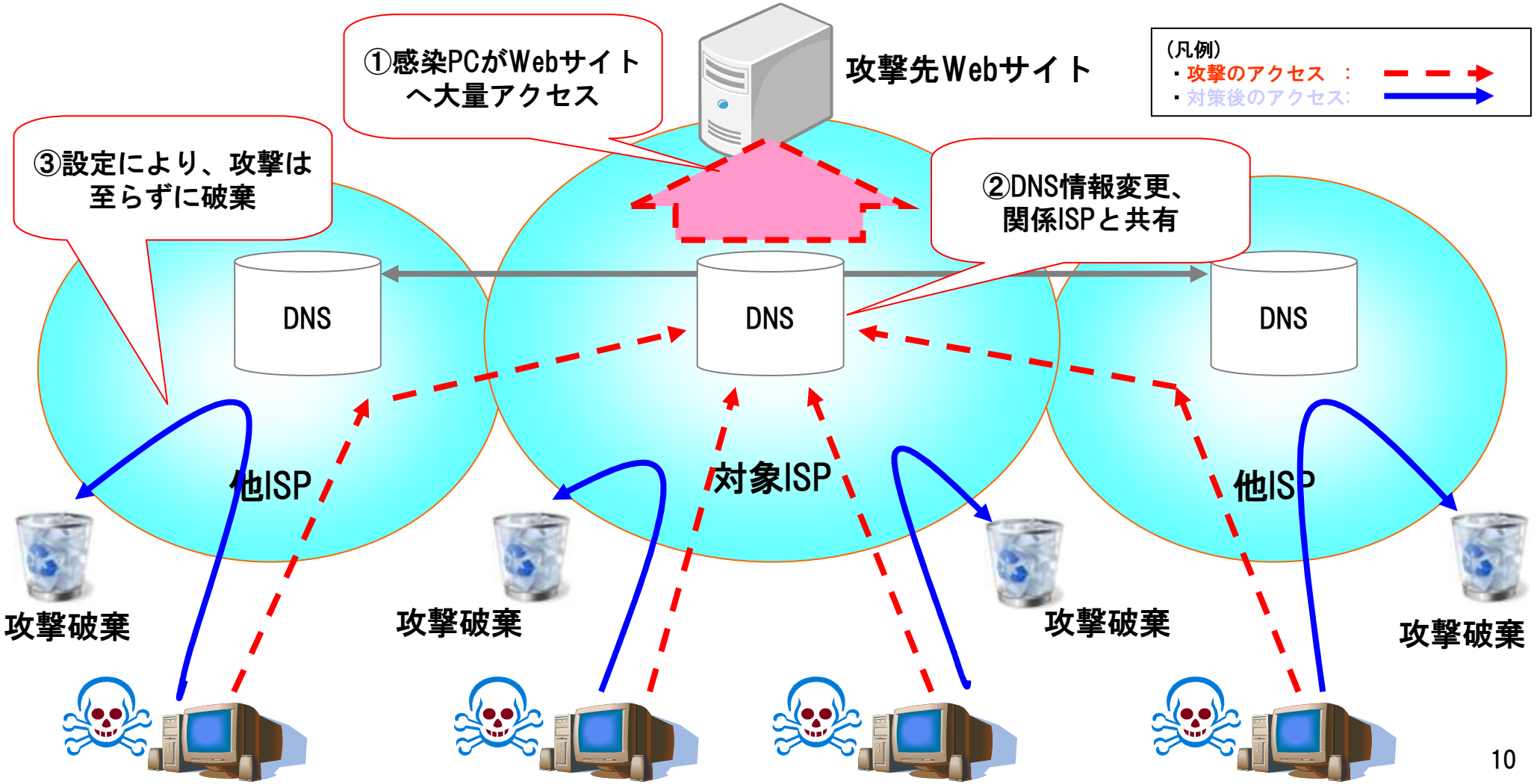
- 『電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン』
  - ✓ 2版改訂・公開（2011年3月）、T-ISAC-J含む5団体が制定
    http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf

- 三菱重工や衆議院等への標的型攻撃を契機とした官民連携
  - ✓ テレコム・アイザック官民協議会（2011年11月～）
    - 総務省、(独)情報通信研究機構（以下、NICT）、T-ISAC-Jによる日常的な情報共有
  - ✓ CEPTOAR間での連携強化(重要インフラ観測システムの運用開始)

T-ISAC-J関連施策

【参考①】T-ISAC-JでのDDoS攻撃への協調対処事例

①Antinnyウイルスに感染したPCが一斉に攻撃先WebサイトへDDoS攻撃発生　　－2004年4～6月－
②狙われたWebサーバのISPが、DNS情報(行き先情報)を書き換えて「ブラックホールIP」を設定、
　各ISPでもDNS情報を書き換え「ブラックホールIP」を設定
③各ISPで連携して設定したことにより、攻撃は「ブラックホールIP」へ向かされて破棄



DoS攻撃即応-WGの活動

DoS攻撃即応-WGの体制、活動目的

- 発足時期、体制
  - ✓ 2011年10月発足
  - ✓ 10社＋3団体が参画（2012年7月現在）
    - IIJ　齋藤衛（主査）
    - NTTコム 湯口高司、KDDI 三浦雄大 、SBB 松本勝之（副主査）
    - Nifty、NEC BIGLOBE、NTT東日本、BBIX、NTTコムテクノロジー、日立
    - 総務省(オブザーバー)、T-ISAC-J、NICT

- 活動目的
  - ✓ DDoS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を検討、実現

    [協調対処が必要な状況]
    - 日本の複数のサイトに対する同時多発的な攻撃予告があった場合
    - 既に発生した攻撃がお互いの利用者からの攻撃だった場合

    当面の検討範囲

    - 攻撃の通信をトランジットしていることを見つけた場合
    - 攻撃している利用者を見つけた場合

    [想定事例の検討例]
    - 2009年7月韓国DDoS攻撃と同様の攻撃（同時多発的DDoS攻撃）が日本で発生した場合の情報共有・協調対処をシミュレーション
  - ✓ 本活動を通じて、日本国内におけるDDoS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

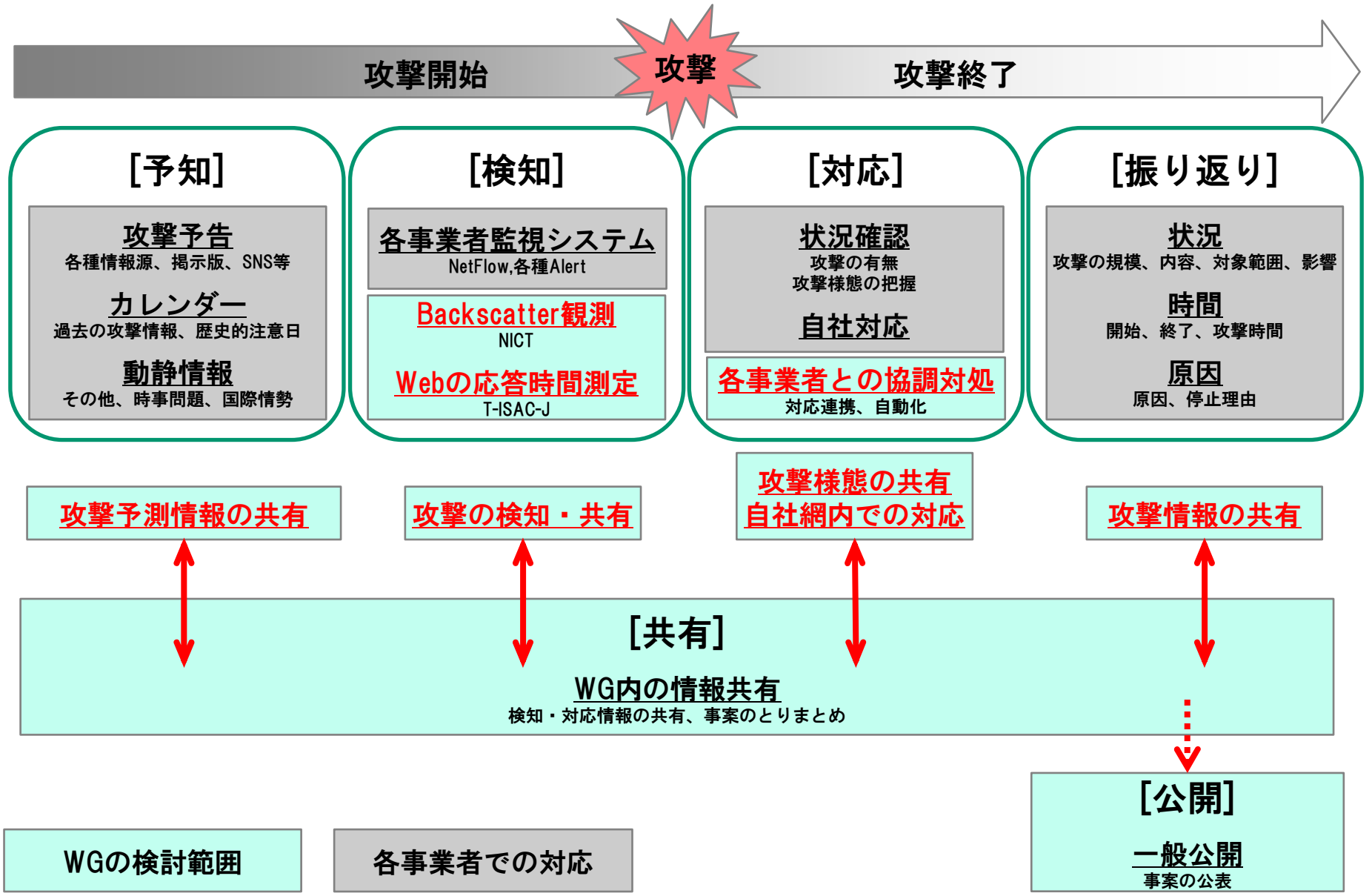
DoS攻撃即応-WGの活動概要

- 活動概要
  - ✓ 『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』に基づく対応の実現
  - ✓ DDoS攻撃発生状況の確認と即応能力の向上
    - ● 攻撃予告情報への対応
    - ● 攻撃発生状況の共有
    - ● 攻撃観測情報に基づいた状況確認
      - ・Backscatter観測（送信元IPアドレスを詐称した攻撃の跳ね返りパケットを観測）
      - ・重要インフラ事業者Webサイトの応答時間測定　T-ISAC-Jで新規構築・運用
    - ● 攻撃発生後の状況取りまとめと共有及び公開
  - ✓ DDoS攻撃対処能力の向上
    - ● 攻撃への自動対応方法の検討
    - ● 自社網内の攻撃者への対応の検討
    - ● その他の施策の検討

- 情報共有・協調対処確立に向けた現在の活動内容

  [前提] 個社の対応については、個社それぞれで対処する
  - ✓ 共有する情報の整理
  - ✓ 情報共有体制の構築
  - ✓ 『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』への還元

DoS攻撃即応-WGでの検討範囲



DoS攻撃即応-WGでの各フェーズ毎の情報共有、協調対処

フェーズ	想定時期	DoS攻撃即応-WGでの対処
予知	数日～2週間前	**攻撃予測情報の共有** ✓ 会員企業や外部から攻撃予告情報を事前に共有し、自社の対応の参考にする ✓ 情報共有内容 ・攻撃予告の内容、攻撃対象や攻撃者のプロファイル 等
検知	即時 (1時間～1日)	**攻撃の検知・共有** ✓ 会員企業間でDDoS攻撃の検知状況・対策を共有し、自社の顧客への波及を検討 ✓ 情報共有内容 ・攻撃予告どおりの攻撃が発生したか ・攻撃状況、動静情報の確認結果、他社への波及 等 ・DoS攻撃即応-WGの観測結果 - Backscatter観測 - 重要インフラWebサイトの応答時間測定
対応 (協調対処が必要時)	即時 (1時間～1日)	**攻撃様態や自社網内での対処を共有し、協調対処を促進** ✓ 攻撃者が会員企業内の他ISPにいた場合、攻撃通信の抑制に向けて協調対処 ✓ 協調対処のための共有内容 ・攻撃様態、自社の対応、協調対処に対する品質（対処までの時間 等）
振り返り	毎月～四半期	**攻撃情報を共有し、攻撃の全容を把握** ✓ 情報共有内容 ・攻撃情報の共有（攻撃者、攻撃手法、対処の状況、被害の有無 等） ✓ 振り返り会の開催　※T-ISAC-J主催のクローズな会員企業向けイベント ✓ T-ISAC-Jから外部への情報公開

過去事案に対するT-ISAC-J内情報共有・協調対処の実績

- DoS攻撃即応-WG発足前の実績
  - ✓ T-ISAC-JのMLやWGで共有
  - ✓ T-ISAC-J主催の業界横断的なサイバー攻撃対応演習等で共有・連携体制を検証

フェーズ	2004年 Antinnyウイルス対応	2010年9月 DDoS攻撃	2011年9月 DDoS攻撃
予知	✓ 特になし	✓ 攻撃予告情報等をMLで共有 （報道、JPCERT/CC、NISC、民間情報源 等） ✓ 公開情報等の考察	✓ 攻撃予告情報等をMLで共有 （報道、JPCERT/CC、NISC 等）
検知	✓ 各会員ISPのDNS負荷状況等を共有	✓ 攻撃状況の共有 （攻撃発生の有無、攻撃の状況、攻撃継続の状況 等）	✓ 攻撃状況の共有 （攻撃発生の有無 等）
対応 (協調対処が必要時)	✓ 各会員ISPのDNSにてブラックホールIPを設定 ✓ マイクロソフト社と連携し、Antinny感染PCの駆除を推進	✓ 本攻撃の協調対処なし ※各個社で対処	✓ 本攻撃の協調対処なし ※各個社で対処
振り返り	✓ T-ISAC-Jサイトで本取り組みや注意喚起を公開（計5回）	✓ 会員向けイベントで各ISPの攻撃状況を共有（2010年12月） ※今後の共有・協調対処を議論	✓ 会員向けイベントで各ISPの攻撃状況を共有（2011年10月） ※DoS攻撃即応-WG Kick Off

DoS攻撃即応-WG発足後の活動実績

➢ 情報共有・協調対処の実績

フェーズ	2012年5月25日 Anonymous攻撃予告	2012年6月25日 Anonymous攻撃予告（#opJapan）
予知	✓ 攻撃予告情報等をMLで共有 （Anonymous関連サイト 等） ✓ 公開情報等の考察	✓ 攻撃予告情報、攻撃ツール等をMLで共有 （Anonymous関連サイト、IRC 等） ✓ 攻撃者のプロファイルを共有
検知	✓ 各社でDoS攻撃を検知していないことを共有 ✓ Backscatterの観測がないことを共有（NICT）	✓ 各社の攻撃状況等の共有 ✓ Backscatterの観測状況を共有（NICT） ✓ 重要インフラ観測システムの観測（T-ISAC-J）
対応 （協調対処が必要時）	✓ 本攻撃の協調対処なし ※各個社で対処	✓ 現時点で、本攻撃の協調対処なし ※各個社で対処
振り返り	✓ 攻撃が軽微なため未実施	✓ 各社の観測状況等を中間報告 （2012年6月28日 第8回DoS攻撃即応-WG）

➢ DoS攻撃即応-WGの定期的な開催（月１回）

➢ DDoS／DoS攻撃に関する勉強会の開催

- ✓ 各社のDDoS／DoS攻撃の観測状況や対応を共有し、同時多発的DDoS攻撃発生時の協調対処の検討に役立てる
- ✓ 各社が持ち回りで説明（第１回 IIJ社、第２回 NTTコミュニケーションズ予定）

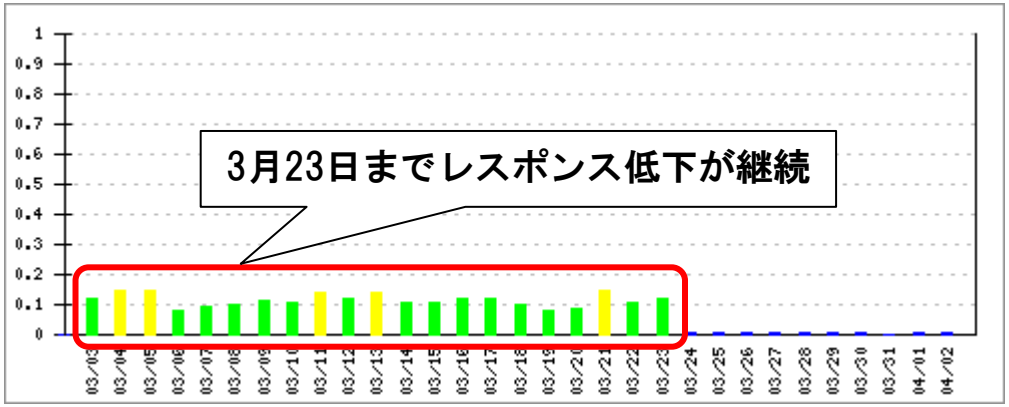
重要インフラ観測システム

重要インフラ観測システム

- 重要インフラ観測システムの概要
  - ✓ 重要インフラ事業者へのDDoS攻撃を俯瞰的に把握・共有することを目的に、T-ISAC-J（T-CEPTOAR）からCEPTOARカウンシル情報共有WGへ提案し、実現
  - ✓ 重要インフラ事業者の関連するWebサイトを外部から定期的にアクセスし、 Webサイトのレスポンス低下を検知・情報共有するシステム
    - ● 登録Webサイトへ15分間隔でHTTP HEADリクエストを送信

- 参加事業者数：405、観測対象URL：479 URL
- 今までの観測結果（2012年1月～7月）
  - ✓ 同時多発的なWebサイトの遅延を観測せず

◆ある重要インフラ事業者Webサイトのレスポンス観測状況（2012年3月）

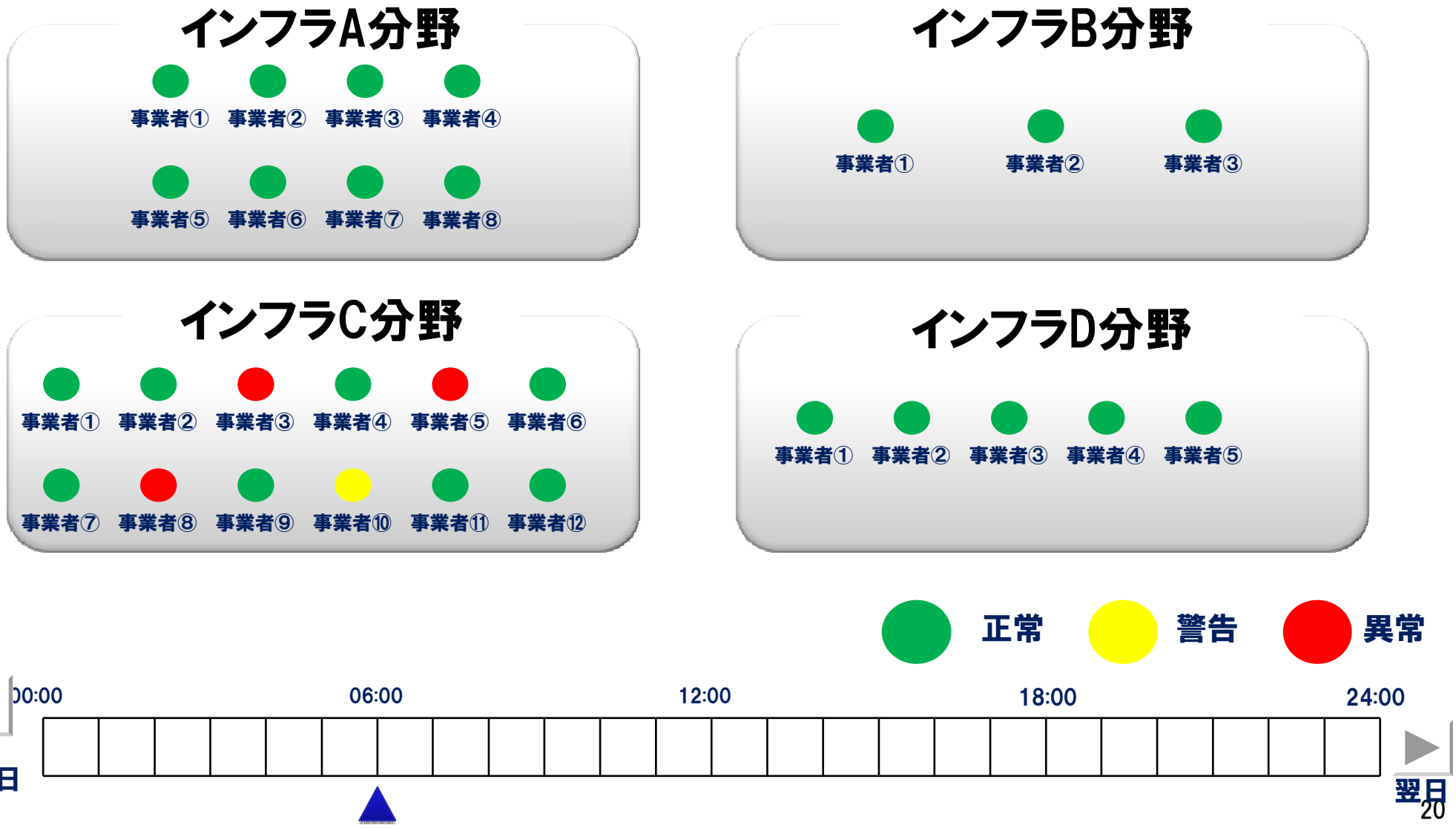


◆CEPTOAR別参加事業者数(2012年7月)

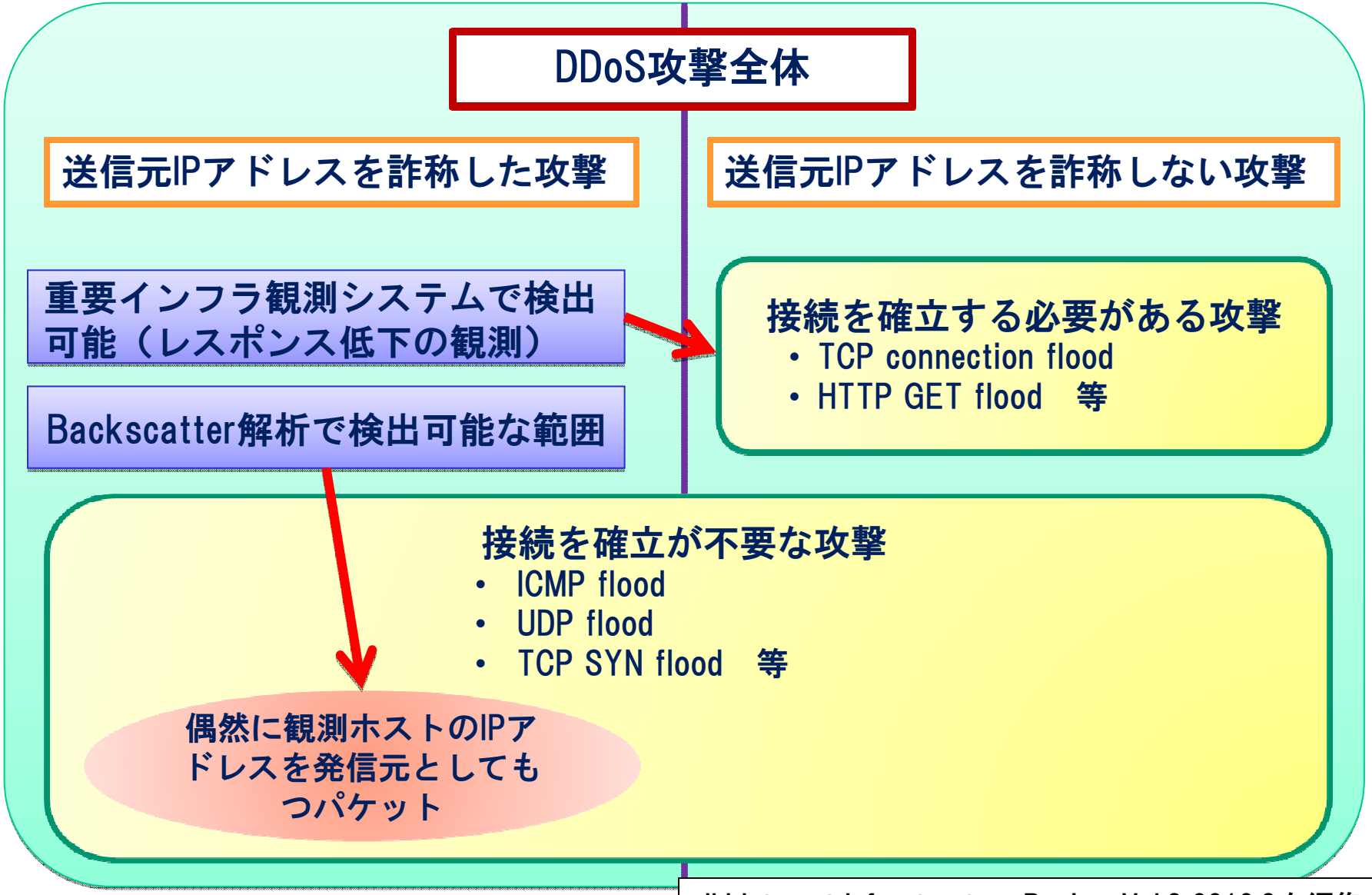
CEPTOAR	参加事業者数
航空	2
証券	39
生保	20
損保	20
電力	15
物流	5
ガス	40
通信	1
銀行	262
NISC	1

重要インフラ観測システム

➢ CEPTOAR別グループ観測（イメージ）



重要インフラ観測システムで検出できるDDoS攻撃の範囲

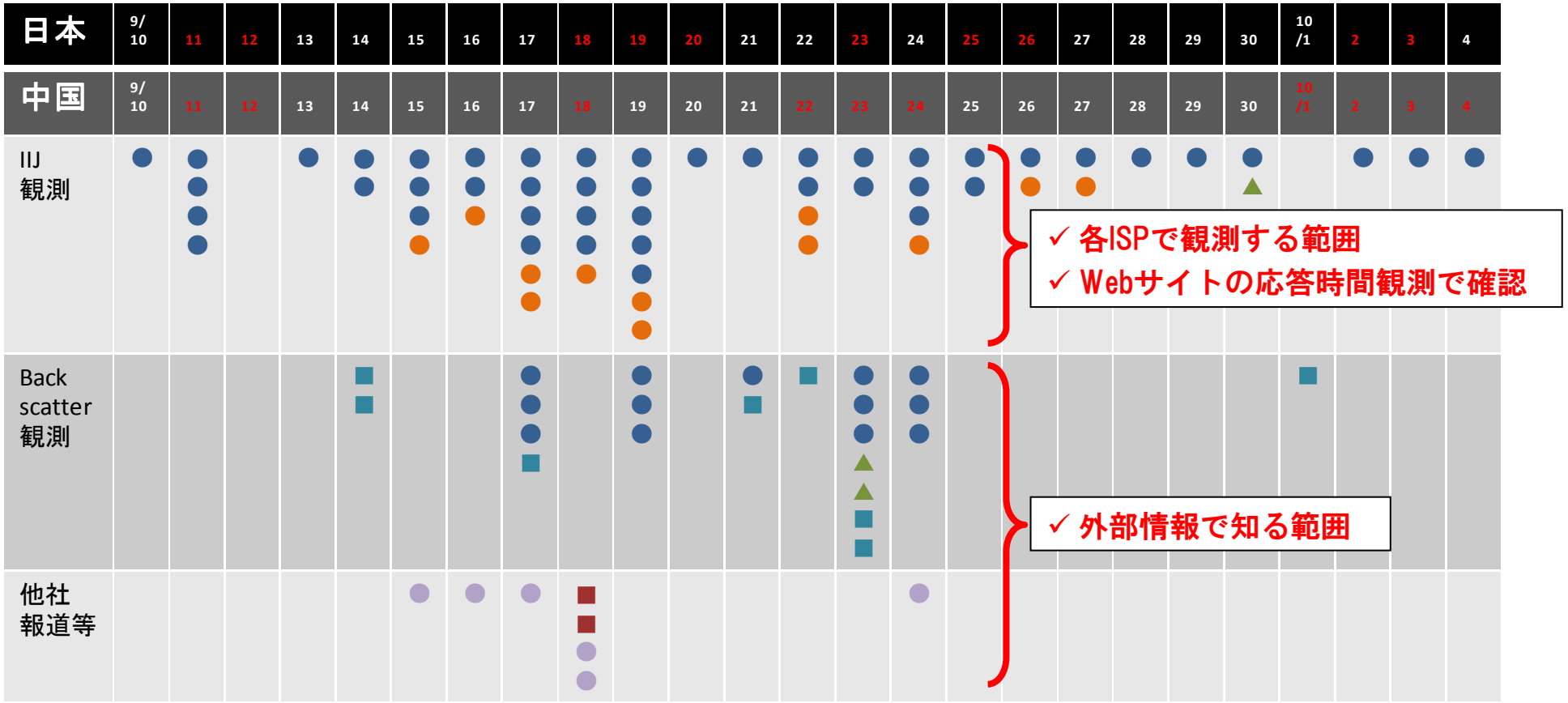


IIJ Internet Infrastructure Review Vol.8 2010.8を編集

【参考②】2010年9月DDoS攻撃の全体像（IIJ社調査）

Telecom SAC Japan

➢ 観測方法の多様化によりDDoS攻撃の全体像の把握が可能



特定のサイトに攻撃が発生した日にマークしている。1つのサイトに1日で複数攻撃が発生していてもマークは一つ。「IIJ観測」はIIJが対処した顧客に対する攻撃を示す。「Backscatter観測」はIPアドレスを詐称された他者に対する攻撃を示す[*49]。「他社報道等」は外部情報によるもの。
「改竄」には報道等外部情報による改竄事件の情報と、IIJの運用するサーバに対する改竄の試みの情報を示している。なお、期間中IIJの運用するサーバではコンテンツ改ざんの成功は確認していない。

INTEROP Tokyo 2011 NC-25　IIJ 齋藤氏資料を編集

凡例
- ●：政府官公庁関係／リソース消費型
- ●：政府官公庁関係／帯域消費型
- ●：政府官公庁関係／攻撃種別不明
- ▲：教育関係／リソース消費型
- ■：一般企業・団体等／リソース消費型
- ■：一般企業・団体等／攻撃種別不明

まとめ

- 同時多発的DDoS攻撃の事例
  - ✓ 近年、日本においても、政治情勢等の影響による政府系サイト等を標的とした同時多発的DDoS攻撃が発生している。2010年9月の尖閣諸島問題を背景としたサイバー攻撃では、日本の複数の政府系サイトが狙われたことを観測している。
  - ✓ 2012年6月25日から発生しているハッカー集団「Anonymous」による日本の政府系サイトへのサイバー攻撃は、今後の情勢により大規模化し、単独の組織のみでは対処できないものに拡大する可能性がある。
- Telecom-ISAC Japan DoS攻撃即応-WGの取り組み
  - ✓ Telecom-ISAC Japanでは、会員企業やISP間の協調対処を推進し、日本におけるインターネットの安全・安心な利用に寄与すべく、DoS攻撃即応-WGを発足した。
  - ✓ DoS攻撃即応-WG活動を通じて、DDoS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を検討・実現し、日本国内におけるDDoS攻撃発生の予測、早期検出、迅速かつ適切な対応を目指す。
  - ✓ 重要インフラ観測システムを用いて、重要インフラ事業者のWebサイトに対するレスポンスを定点観測し、同時多発的なDDoS攻撃発生時の影響を俯瞰的に把握できるようになった。Backscatter観測結果と合わせて、日本国内におけるDDoS攻撃の全容を把握し、個社の対応や企業間の協調対処の連携強化に活用していく。

ご清聴ありがとうございました。

【補足①】大量通信等への対処に関するガイドライン

➢ 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
- ✓ http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf （2011年3月25日、第2版）
- ✓ 民間の自主的なガイドラインという位置づけ
- ✓ DDoS攻撃等の大量通信を受けたISPが対処するに際し、電気通信事業法で定める「通信の秘密」との関係で、正当業務行為となるかどうかの判断できるかどうかを実例を交えて解説

第1章　総則（*目的*、総論、*定義*、*通信の秘密とISPの対処に関する基本的な考え方*、*見直し*）
第2章　各論
- ◆ 大量通信等について
  - (1) 大量通信等に係る通信の遮断
    - ア 被害者から申告があった場合
    - イ 事業者設備に支障が生じる場合
    - ウ 送信元設備の所有者の意思と関係なく送信される大量通信等の場合
  - (2) 送信元詐称通信の遮断
  - (3) 壊れたパケット等の破棄
  - (4) マルウェア等トラヒックの増大の原因となる通信の遮断
  - (5) 受信側の設備等に意図しない影響を及ぼす通信等
  - (6) 網内トラヒックの現状把握
  - (7) ***大量通信等への共同対処***
- ◆ 迷惑メール等
  - (1) 送信元詐称メールの受信拒否
  - (2) Black Listとの突合に基づくユーザへの注意喚起
  - (3) 迷惑メールフィルタリングサービスにおけるフィルタ定義の共有
- ◆ その他の情報共有・情報把握について
  - (1) 踏み台端末や攻撃中継機器への対処
  - (2) レピュテーションDBの活用

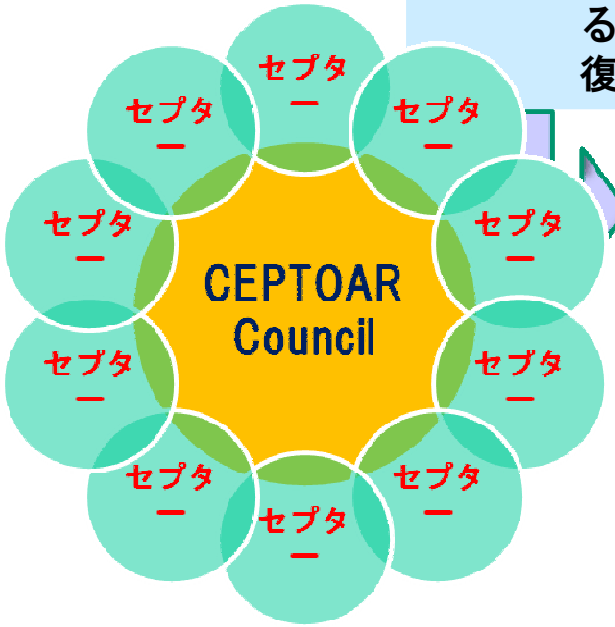
※*下線斜め文字*
第2版の主な改正点

【補足②-1】CEPTOAR(セプター)の概要

「重要インフラの情報セキュリティ対策に係る行動計画」
(2005年12月13日情報セキュリティ政策会議決定)

セプター (CEPTOAR)

- Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略称
- 各重要インフラ分野におけるIT障害に関して、情報共有体制を強化するための「情報共有・分析機能」のこと。
- CEPTOARは、IT障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有する。これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。



セプターカウンシル (CEPTOAR Council)

- 2009年2月に重要インフラ各分野のセプターが連携して設立された、重要インフラのセキュリティ向上に向けた分野横断的な情報共有のための協議会
- 重要インフラとして位置づけられている10分野について、IT障害への対策向上のための機能
- 10分野とは、情報通信、金融、航空、鉄道、電力、ガス、政府・行政、医療、水道、物流

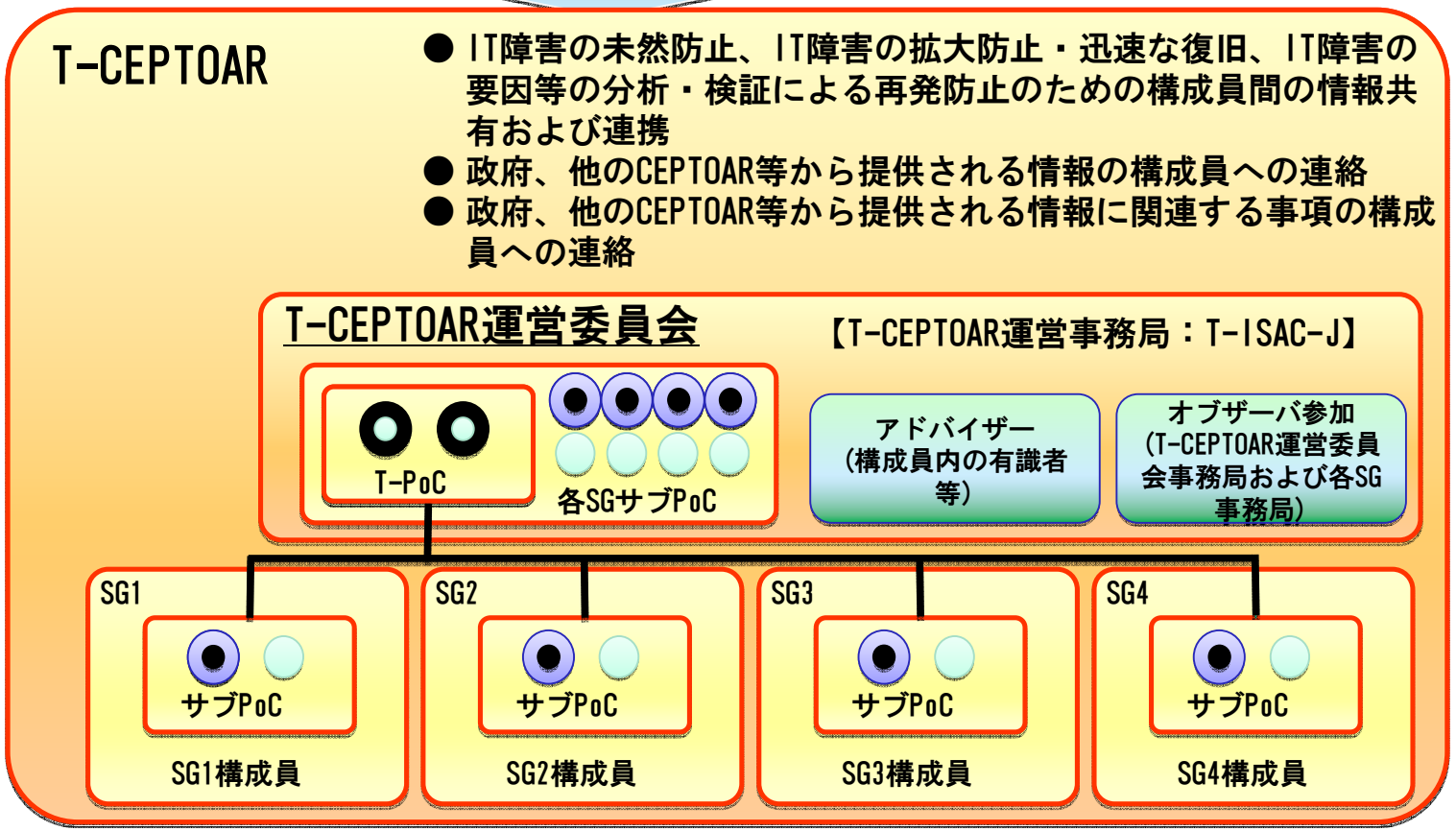
https://www.telecom-isac.jp/public/t-ceptoar.html

【補足②-2】T-CEPTOAR(ティー・セプター)の概要

内閣官房情報セキュリティセンター(NISC)

重要インフラ監督官庁：総務省

各種関連情報 復旧手法
早期警戒情報 等



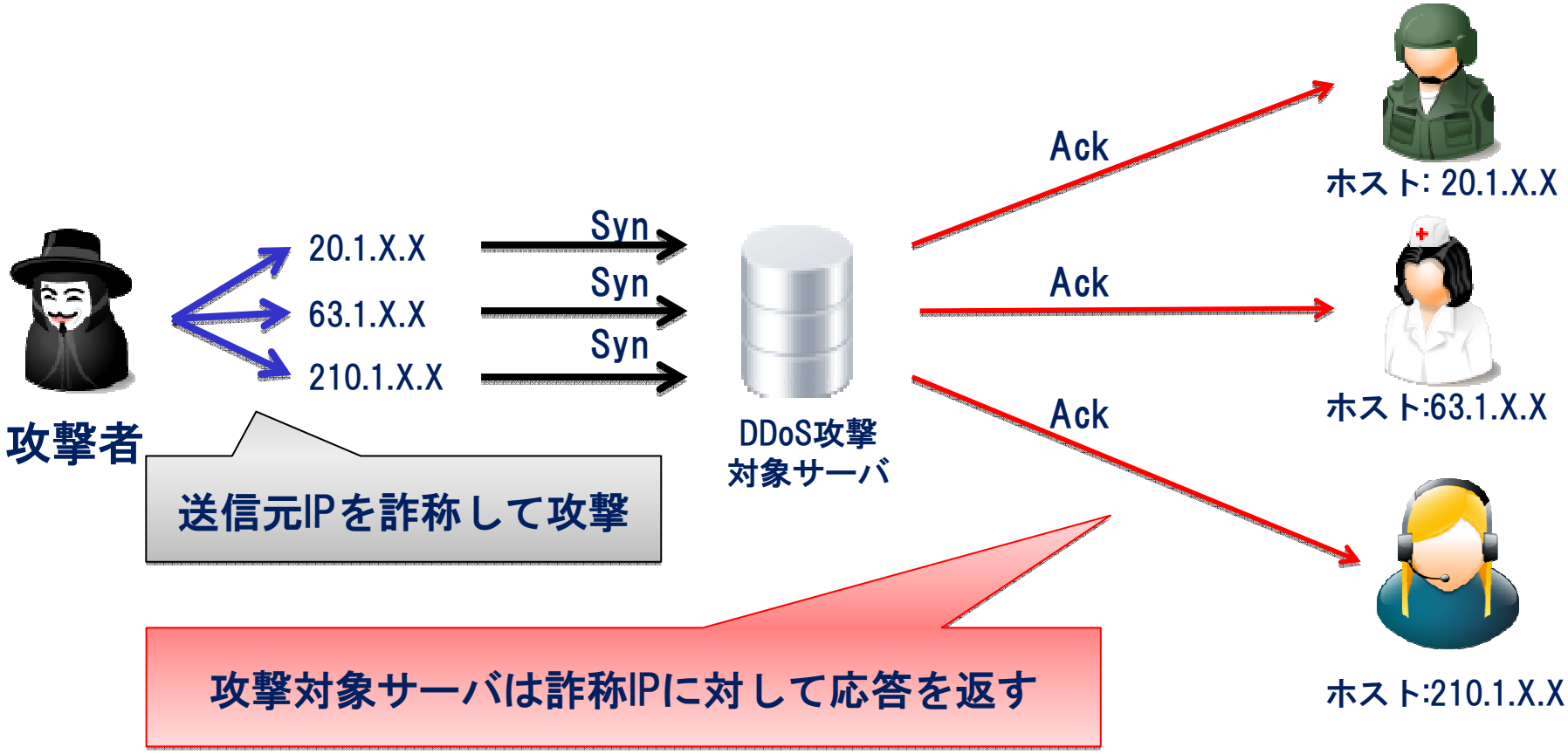
SG1：固定NWインフラを設置する電気通信事業者等
SG2：アクセス系の電気通信事業者等
SG3：ISP事業者等
SG4：携帯電話事業者等

https://www.telecom-isac.jp/public/t-ceptoar.html

【補足③-1】送信元IPアドレス詐称攻撃とBackscatter

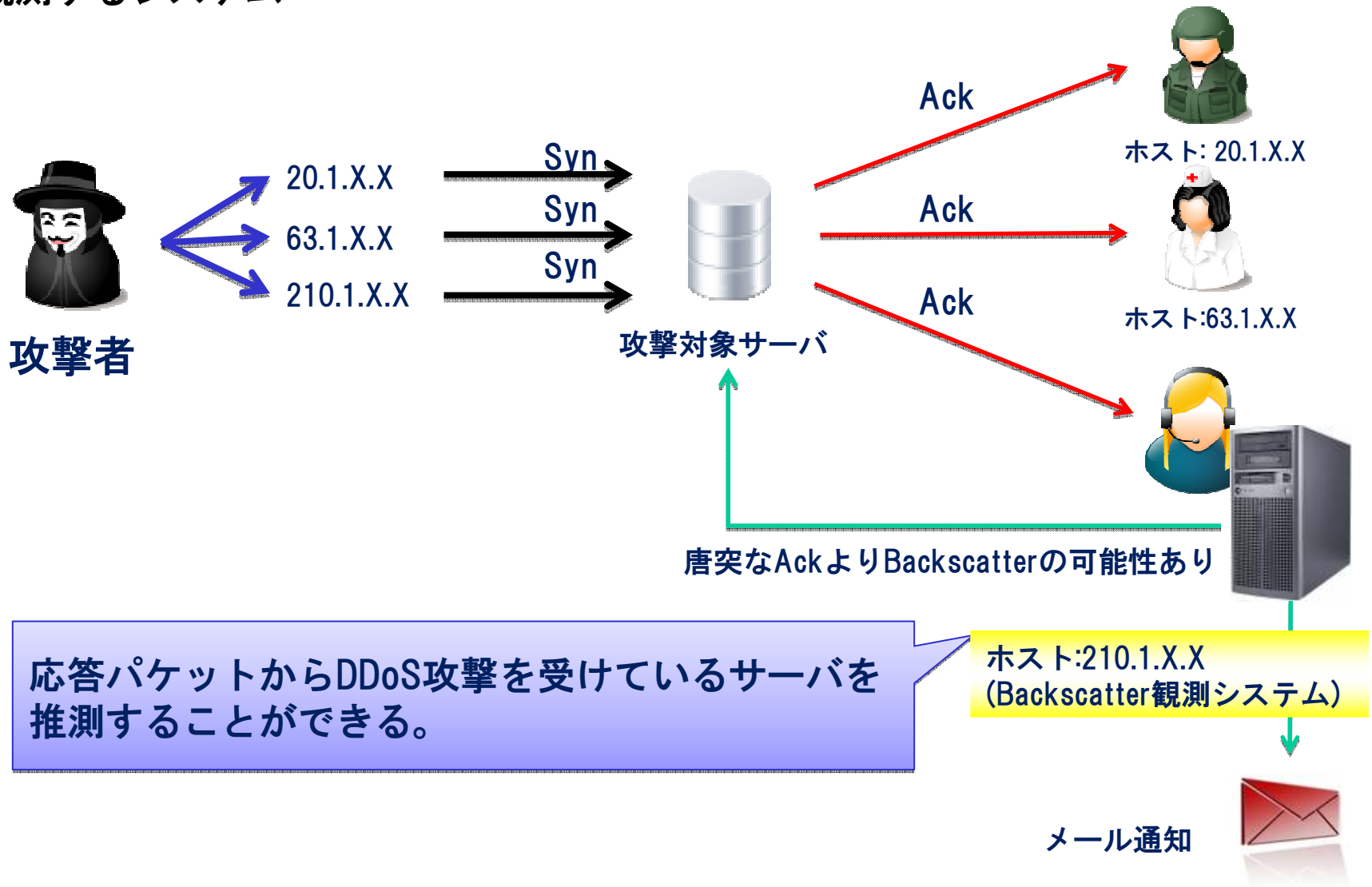
Backscatterとは

✓ 攻撃者が送信元IPアドレスを詐称してDDoS攻撃を行っている場合、応答パケットが攻撃者IPアドレスにではなく詐称IPアドレスへ返送される事象



【補足③-2】Backscatter観測システム

発生したBackscatterを検知し、DDoS攻撃の対象となっている可能性のあるサーバIPを観測するシステム



応答パケットからDDoS攻撃を受けているサーバを推測することができる。