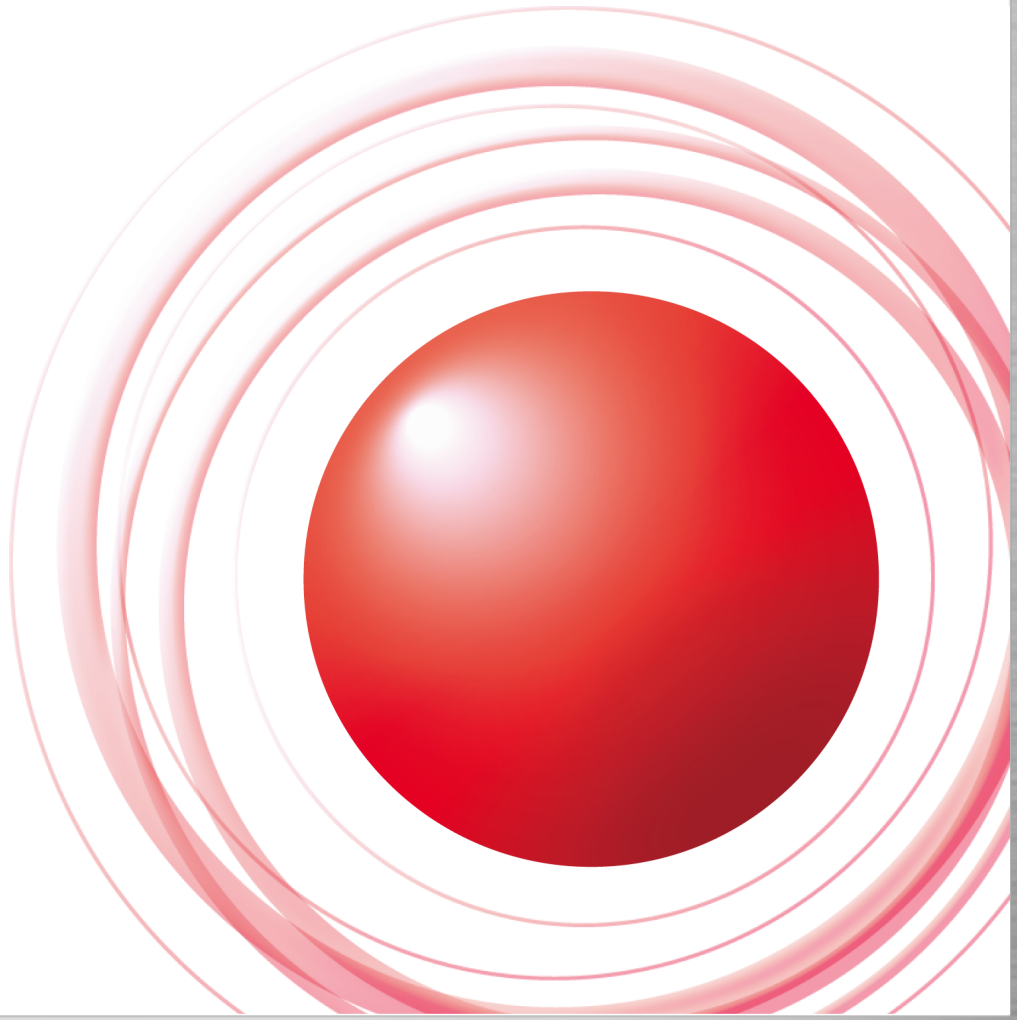
JANOG30　日本の現状と取り組みについて
Part.1 ~DDoS攻撃の状況~

IIJ
Internet Initiative Japan



2012年7月6日
株式会社インターネットイニシアティブ
セキュリティ情報統括室
土屋　博英

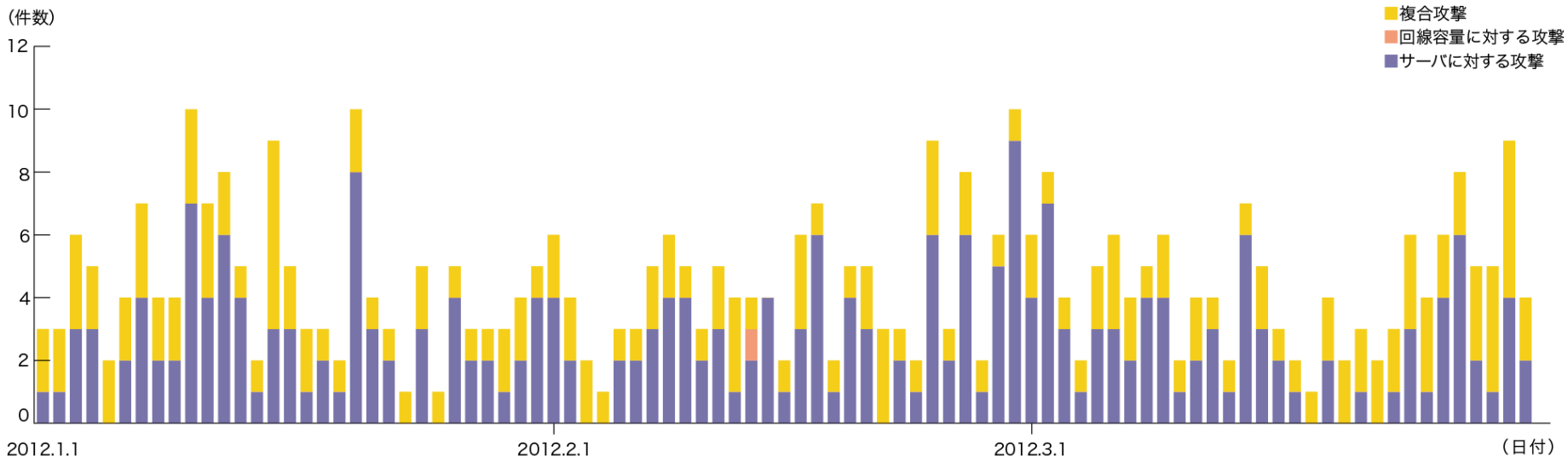
Ongoing Innovation

20th Anniversary

DDoS攻撃の状況（弊社観測状況）

DDoS発生件数（2012年1月～3月）

- 弊社DDoS対策サービスでの検知件数
  - 1日平均4.4件
  - 最大673Mbps
  - もっとも長い攻撃　4時間55分
  - サービス以外ではMax 4Gbps、75万ppsを観測



Internet Infrastructure Review (IIR) http://www.iij.ad.jp/company/development/report/iir/index.html

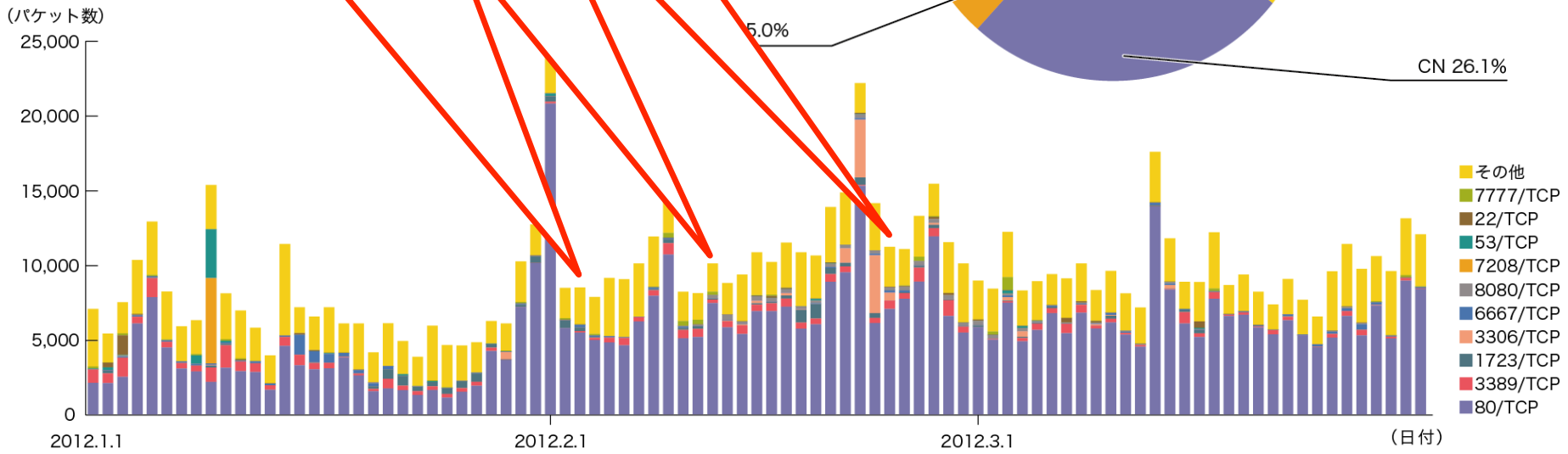
DDoS攻撃の状況（弊社観測状況）

DDoS攻撃によるBackscatter観測（2012年1月～3月）

ロシアのニュースサイト

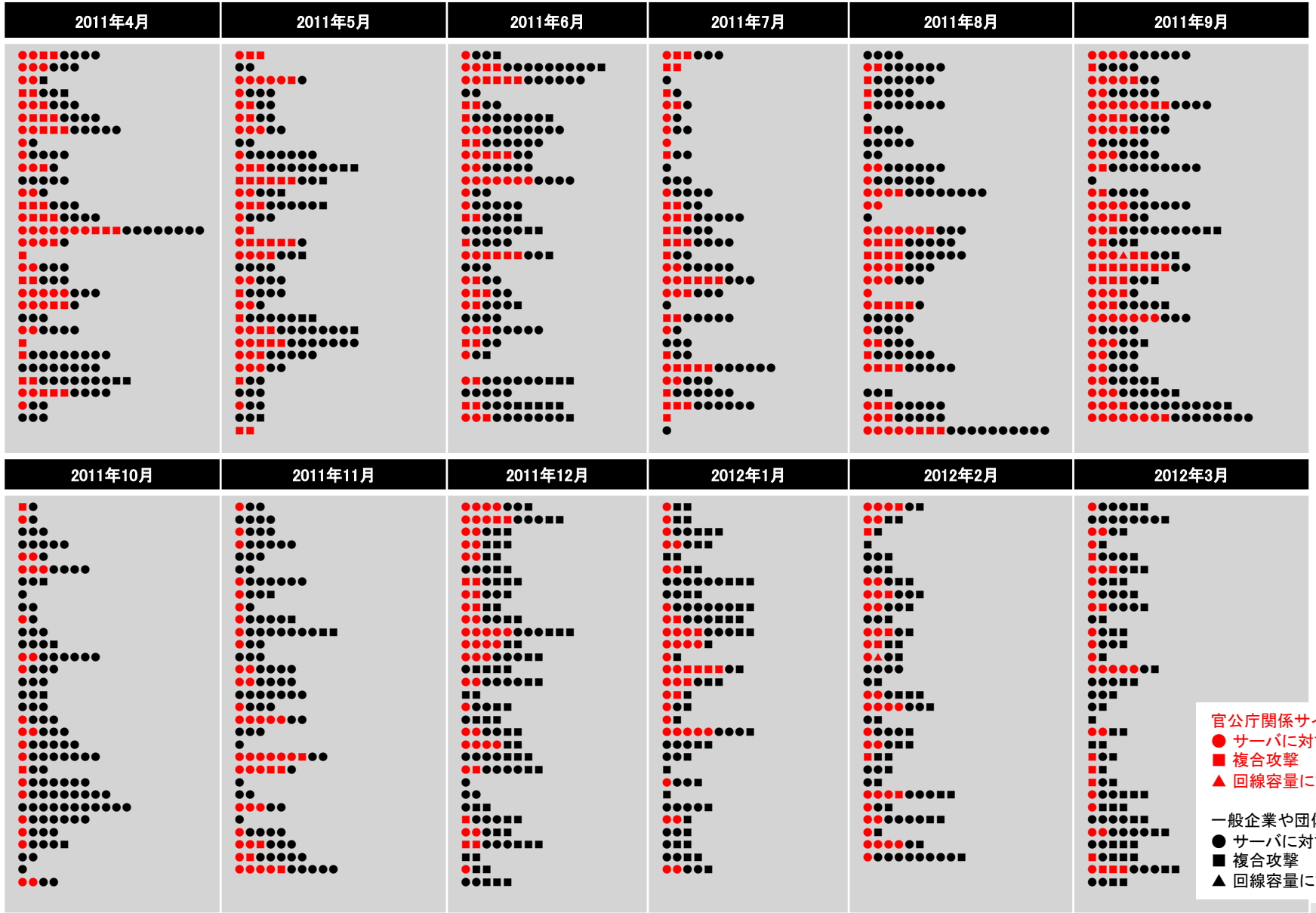
Anonymous　sweaden

Anonymous　Brasil



Internet Infrastructure Review (IIR) http://www.iij.ad.jp/company/development/report/iir/index.html

2011年4月から2012年3月までのDDoS攻撃の発生状況



DDoS攻撃の状況（世界）

World Wide Infrastructure Security Report 2011 Volume VII (Arbor Networks)

- Hacktivismなどイデオロギーに基づく攻撃の増加
- 10Gbpsクラスの攻撃が常態化 (最大 60Gbps)
- Layer 7 DDoS攻撃の増加

World Infrastructure Security Report 2011 Volume VII（http://www.arbornetworks.com/report）

Prolexic Attack Report Q1 2012 (Prolexic Technologies)

- 前年同期比で攻撃総数が25%増加、平均 6.1Gbps
- 73%がインフラへの攻撃(Layer 3,4)、27%がアプリケーションへの攻撃(Layer 7)
- 2011年11月に最大 45Gbps / 6900万ppsの DDoS攻撃を観測 (複数の異なる手法による複合攻撃)

Prolexic Attack Report（http://www.prolexic.com/attackreports/index.html）

DDoS攻撃の状況（世界）

日本からの攻撃?

CNCERT/CC 2011 Annual Report

- 中国国内への攻撃発信元 (DDoS以外も含む)
  1位 日本 (22.8%) 2位 米国 (20.4%)

http://www.cert.org.cn/UserFiles/File/201203192011annualreport(1).pdf

Prolexic Attack Report Q4 2011
(Prolexic Technologies)

- 2011年第4四半期 DDoS攻撃の発信元
  1位 日本 (35.0%) 2位 中国 (18.65%)

Prolexic Attack Report（http://www.prolexic.com/attackreports/index.html）

最近のDDoS攻撃事例

- ロシアの市民ジャーナリストのUstream妨害
- WikiLeaks, The Pirate Bayへの攻撃
- 韓国で小学生を含むグループが政府系サイトを攻撃
- ロシアの大統領選挙に関連する攻撃
- Anonymousによる米政府系サイトへの攻撃
- Anonymousによる日本サイトへの攻撃

#opjapan
元々は日本のAnonymousが計画していたACTAへの抗議活動だったが、海外のAnonopsが参加したことで、著作権法改正（刑事罰化）への反対運動として、Webサイト改ざんやDDoS攻撃などが行われた。

世界中から日本が標的とされた事例

攻撃方法

- 人海戦術 (F5アタック)
- DDoS攻撃ツール (大量通信発生、IPアドレス詐称)
- DDoS攻撃機能をもつマルウェア、ボットネット
- DDoS攻撃代行サイト、DDoSサービス
- Javascriptによるブラウザベースの攻撃ツール
  (Twitter等で攻撃用サイトの短縮URLを拡散)

例：Anonymousで利用されているとされるツール類
[hping]-[OS: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOS X, Windows]
[Slowloris]-[OS: Linux]
[HOIC]-[OS: Windows]
[Pyloris]-[OS: Windows, MacOS X, Linux]
[THC-SSL-DOS]-[OS: Windows, Linux]
[Torshammer]-[OS: Linux]

まとめ

- DDoS攻撃の状況
  - DDoS攻撃は日常的に発生しており、攻撃件数も増加傾向にある。攻撃理由も様々で、何の前触れもなく攻撃されることが多い。
  - 攻撃ツールが一般に公開されていて、容易に入手できるため、誰でも攻撃に参加可能。
  - ネットワークへの攻撃は規模が年々増大し、アプリケーションへの攻撃は効果的な攻撃が多くなってきている。また、これらを組み合わせた複合攻撃が増えている。

JANOG30　日本の現状と取り組みについて

Part.2～Telecom-ISAC Japan DoS攻撃即応-WGの取り組み～

2012年7月6日

Telecom-ISAC-Japan　DoS攻撃即応-WG
株式会社インターネットイニシアティブ
セキュリティ情報統括室
土屋　博英

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

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について実例を交えて解説

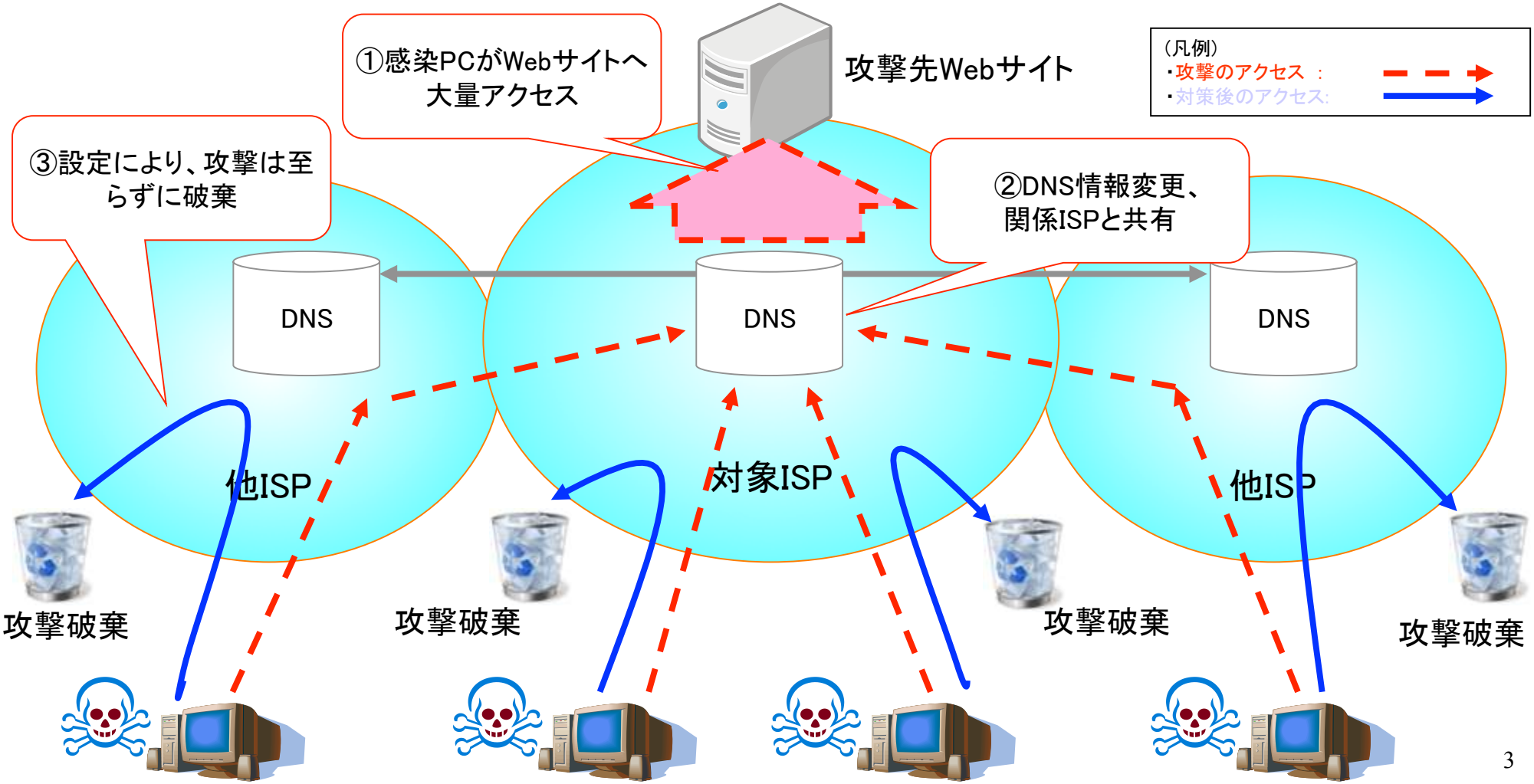
第1章　総則（*目的*、総論、*定義*、*通信の秘密とISPの対処に関する基本的な考え方*、*見直し*）
第2章　各論
- ◆ 大量通信等について
  - (1) 大量通信等に係る通信の遮断
    - ア　被害者から申告があった場合
    - イ　事業者設備に支障が生じる場合
    - ウ　送信元設備の所有者の意思と関係なく送信される大量通信等の場合
  - (2) 送信元詐称通信の遮断
  - (3) 壊れたパケット等の破棄
  - (4) マルウェア等トラヒックの増大の原因となる通信の遮断
  - (5) 受信側の設備等に意図しない影響を及ぼす通信等
  - (6) 網内トラヒックの現状把握
  - (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

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
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

－2004年4～6月－



2010年9月DDoS攻撃の全体像（弊社調査）

Telecom ISAC 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　弊社 齋藤の資料を編集

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

DoS攻撃即応-WG発足の背景

- 『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

- 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

- 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

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6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
    - 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

    当面の検討範囲

    [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

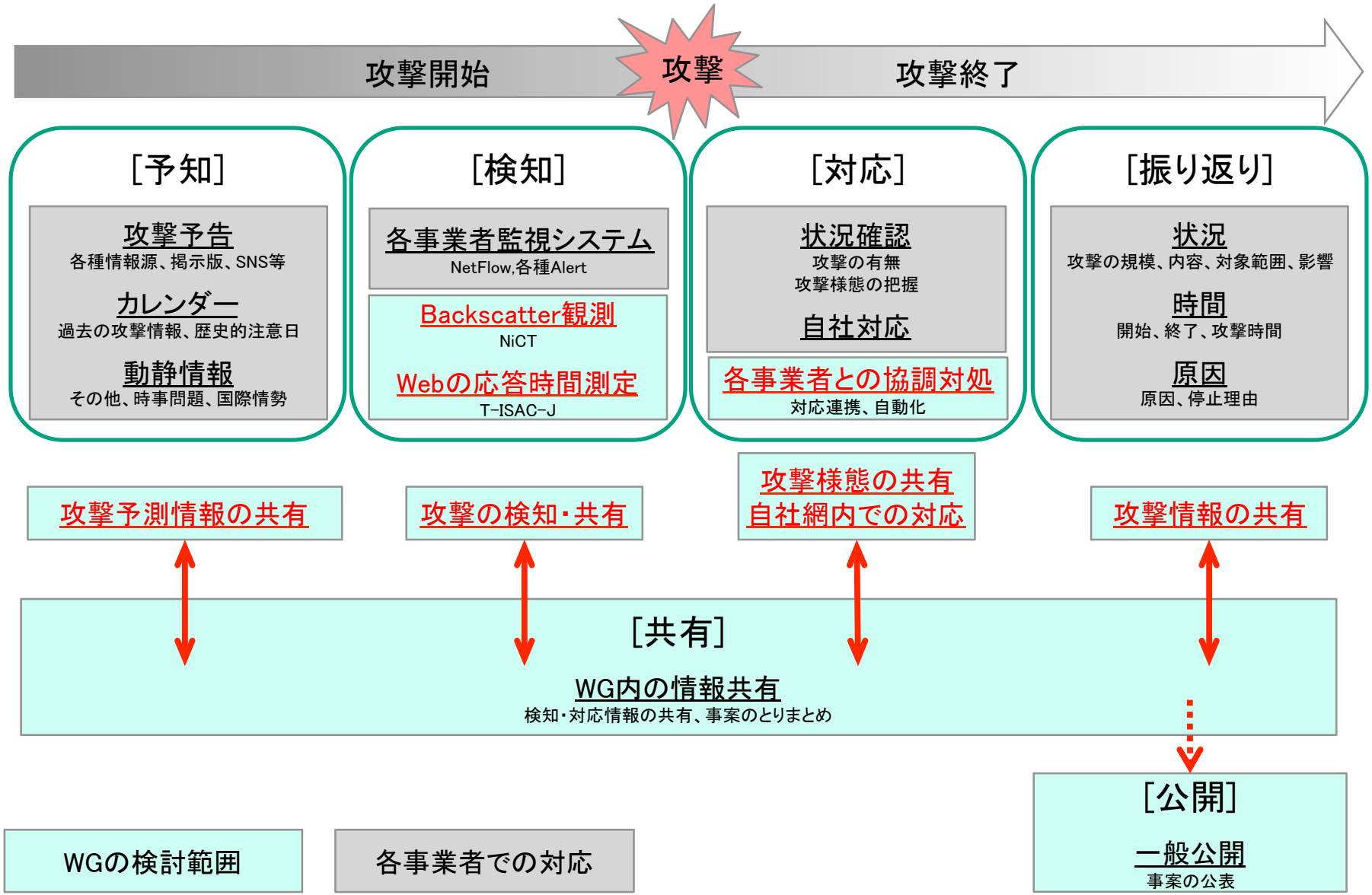
DoS攻撃即応-WGの活動概要

➢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）NiCT他
    - ・ 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

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発足後の実績
  - ✓ 2012年5月25日 アノニマスの攻撃予告では、予知・検知情報を共有
  - ✓ 2012年6月25日 アノニマスの#opjapanでも情報共有を行い、適切な対応が行えるように備えている

現在の活動内容

➢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

➢協調対処に向けた検討（これから）

✓協調対処に向けた技術的検討

・ 現状の対策技術のおさらい

・ どういった技術的手段が利用できるかの検討

✓そのためにクリアする必要のある課題

✓法律

✓規約・契約

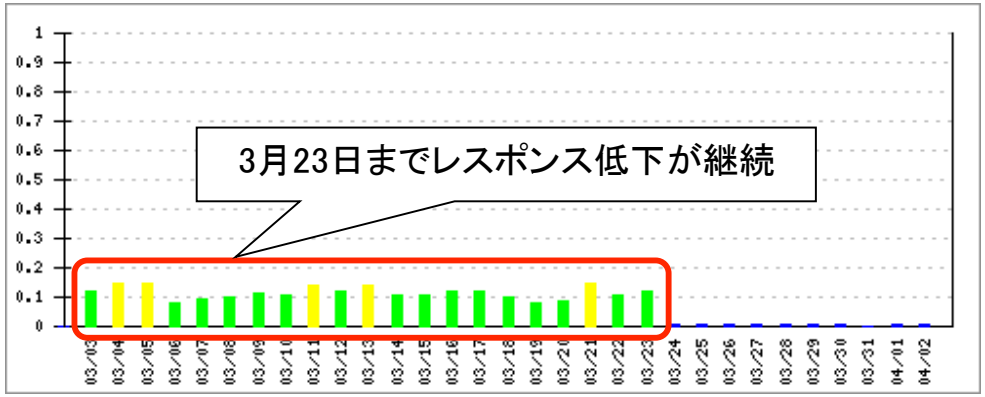
✓社内体制

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：409、観測対象URL：476 URL
- 今までの観測結果（2012年1月～6月）
  - ✓ 同時多発的なWebサイトの遅延を観測せず

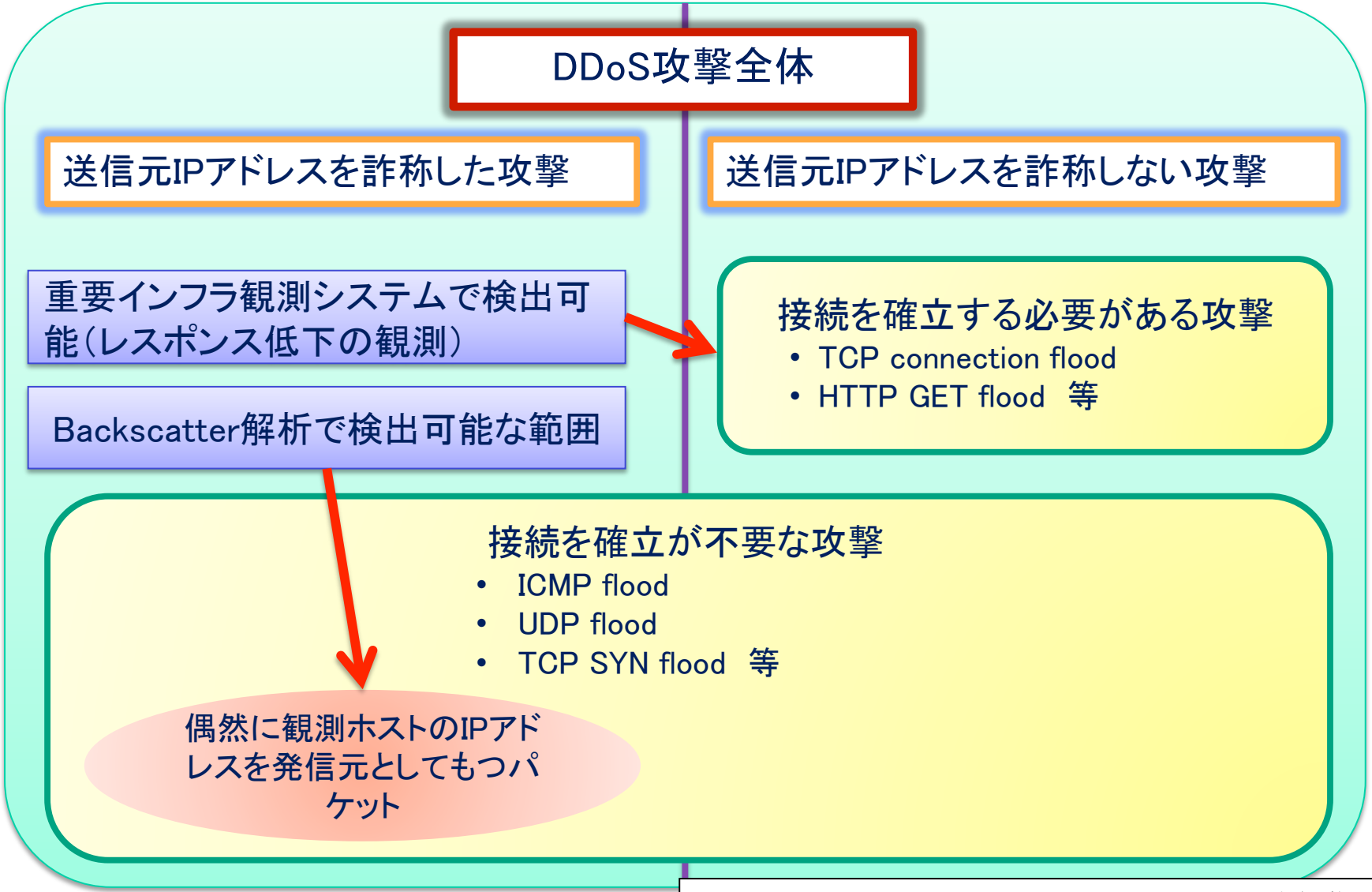
◆ある重要インフラ事業者Webサイトのレスポンス観測状況（2012年3月）



◆CEPTOAR別参加事業者数（2012年6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
放送	6
銀行	262

重要インフラ観測システムなどで検出できるDDoS攻撃の範囲



IIJ Internet Infrastructure Review Vol.8 2010.8を編集

まとめ

- 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。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。

- Telecom-ISAC Japan DoS攻撃即応-WGの活動
  - ✓ 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。
  - ✓ 今までも同時多発的なDDoS攻撃が発生した際、Telecom-ISAC Japanの各種枠組みを活用して情報共有や協調対処を実施してきた。より大規模かつ同時多発的なDDoS攻撃が発生した場合（2009年7月 韓国DDoS攻撃と同様の攻撃が日本国内で発生した場合 等）を想定して、情報共有体制や協調対処を高度化していく。

- 重要インフラ観測システム
  - ✓ 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、会員企業の個社の対応や会員企業間の協調対処の連携強化に活用していく。

最後に

DoS攻撃即応-WG設立の思い

■近い将来、協調対処が必要な状況は必ず発生

- 韓国DDoS攻撃（7・7 DDoS）と同様の攻撃（同時多発的DDoS攻撃）が日本で発生したら
- 国内同士でお互い(ISP)がお互い(ISP)を攻撃する状況が発生したら

韓国と比べて、通信インフラの整っている日本では、よりひどいことが起こる可能性が十分に想定できる。対処が遅くなれば状況はより悪化する。

■大規模な攻撃に対する適切な対応をあらかじめ用意しておく

- 「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」に沿った対応の実現

日本のインターネット全体の問題として考えることが重要

攻撃の全体像を把握するためには、複数事業者による情報共有や協調対処といった連携が重要となる。ISP各社で協力して対処しなければいけない時に迅速に動くため、まずは限られた枠内（WG）で協調対処の仕組みを作り、コンセンサスを得る。

ご清聴ありがとうございました。