4 DDoS 攻撃に対する通信事業者の取り組み

専

西部喜康（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 / NTT コミュニケーションズ（株））

テレコム・アイザック推進会議

近年，大規模な DDoS（Distributed Denial of Service）攻撃が世界各国で発生し，国際的な問題となっている[1]．日本国内でも，インターネット上のコミュニティ集団による大規模な攻撃が大きな脅威として認識されるとともに，ますます高度化・組織化されていく DDoS 攻撃への対応に関して情報通信業界としての一層の取り組みが求められている．本稿では，国内大手インターネットサービスプロバイダ（以降，ISP）や通信事業者などを会員とする情報セキュリティ推進組織であるテレコム・アイザック推進会議（以降，Telecom-ISAC Japan）でのサイバー攻撃，特に DDoS 攻撃への対応のための施策について紹介する．

Telecom-ISAC Japan は，2002 年 7 月，国内の主要通信事業者 7 社ほかが発起人となり，非営利任意団体「インシデント情報共有・分析センター」としてスタートした．通信サービスの安全かつ安心な運用の確立のため，会員企業が関連情報を共有・分析する仕組みを構築し，事業者単独では手に負えないサイバー脅威に対して共同で立ち向かうことを目的とした非営利会員制組織である．

2013 年 1 月末時点で，国内大手 ISP，移動体通信企業等を含む通信事業者等 19 社が会員企業となり，通信事業者を中心とする幅広い企業間の相互連携を図り，サイバー攻撃に関するインシデント情報の共有・分析をはじめとする情報セキュリティに資する活動を実施している．Telecom-ISAC Japan の活動を大別すると次の通りである．

1) ISP・通信業界の共通の問題解決に向けたワーキンググループ活動
2) 国内外のセキュリティ機関との連携・協調
3) 経路情報収集・分析システム（経路奉行システム☆1）の運用
4) サイバークリーンセンター（CCC : Cyber Clean Center）[2]，国際連携によるサイバー攻撃予知・即応技術の実証実験プロジェクト[3] 等への参画
5) セプターカウンシル☆2, [4] 等政府情報セキュリティ政策への参加・貢献
6) セミナおよびサイバー攻撃演習などイベント開催
7) その他（セキュリティ技術の普及・啓発・教育活動の主催・協力）

本稿では，この中から特に DDoS 攻撃の対応とかかわりを強く持つ DoS（Denial of Service）攻撃即応，サイバー攻撃即応スキーム検討，サイバー攻撃対応演習ワーキンググループの活動について紹介する．

DoS 攻撃即応ワーキンググループ（DoS 即応 WG）

ボットネットによる DDoS 攻撃は，個々の企業サイトに対する単発的な DDoS 攻撃だけではなく，同時に複数サイトを攻撃する同時多発的な DDoS 攻撃も発生しており，大規模化と複雑化の様相を呈している．

一方，DDoS 攻撃に対処する側は，攻撃対象となり得る個々の組織ならびに通信事業者の努力と能力

☆1 日本国内 ISP から提供される経路情報をもとに，インターネット運用に支障をきたす異常な経路情報の発生を監視するシステム．

☆2 内閣官房情報セキュリティセンターによって設立された，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組織体．

に応じた対応で，通信事業者間の連携は，自発的な情報提供や対応依頼によって対処しているのが現状である．しかし，同時多発的な DDoS 攻撃への対処を向上するためには，攻撃の全容を把握することが必要であり，このため，DDoS 攻撃の事後に個別団体からの情報を集約し，情報共有などを行う連携が急務となっている．このような中で，2011 年 3 月には，「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 版改定)[5] が公表されるなど，DDoS 攻撃を含む DoS 攻撃を検知した場合の通信事業者が実施できる内容についての一定の整理も試みられた．

Telecom-ISAC Japan では，サイバー攻撃全般に対して，通信事業者が連携ならびに協調して対応できる枠組みを目指し，まずは近々の課題である同時多発的な DDoS 攻撃への迅速な対応にフォーカスした DoS 攻撃即応ワーキンググループ（以降，DoS 即応 WG）を 2011 年 11 月に発足させた．

DoS 即応 WG では，複数の通信事業者が協調して対応することが必要な状況として，4 つの場面を想定している．

1) 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る場合
2) 発生している攻撃活動の発信元，送信先が通信事業者にまたがる場合
3) 攻撃活動にかかわる通信を伝播していることを知り得た場合
4) 攻撃活動にかかわる利用者を知り得た場合

このうち 1) および 2) を当面の活動対象とし，活動を通じて日本国内における DDoS 攻撃発生の予測，早期検知，迅速かつ適切な対応の実現を目指している．2013 年 1 月末時点で，大手 ISP を中心として，10 の企業および 3 つの団体が参画している．

■ 活動概要

DoS 即応 WG で達成すべき課題の 1 つが，前述の『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』に基づいた対応の実現である．このガイドラインは，DDoS 攻撃を含む DoS 攻撃や迷惑メールなどの大量通信を受けた ISP が対処するにあたり，電気通信事業法で定める通信の秘密との関係で違法性が阻却されるための要件について，さまざまな実例を交えて解説している．

活動では，DDoS 攻撃発生時の状況確認と即応能力の向上を図るという視点から，DDoS 攻撃の過程を時間的流れに沿って，『予知』，『検知』，『協調対処』，『振り返り』に分け，各通信事業者が個別に対処すべきこと，DoS 即応 WG として協調して対処すべきことの課題や実現方法について検討している（図 -1）．また，それぞれのフェーズにおいて各通信事業者で実施するべき対応と協調することで，全体としても迅速かつ適切な対応が実現できるよう活動を進めている（表 -1）．

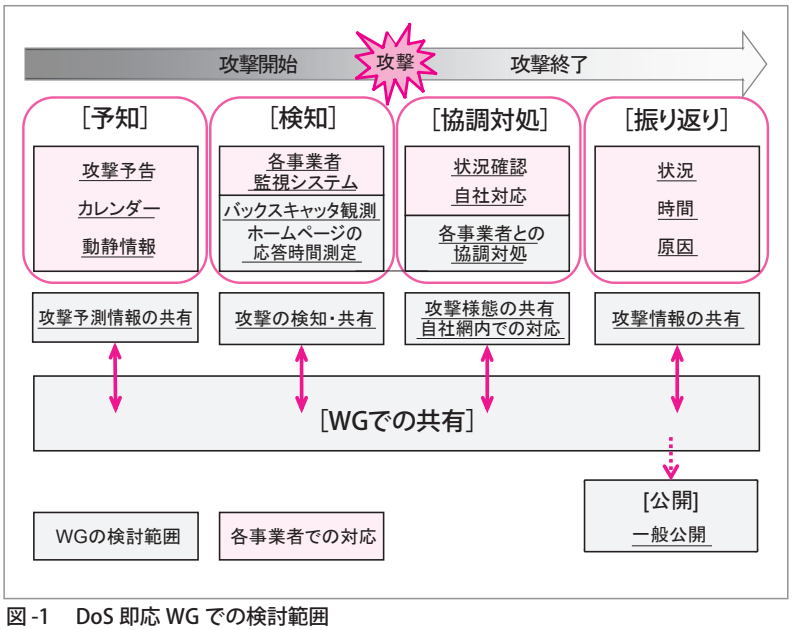

図 -1　DoS 即応 WG での検討範囲

予知

各通信事業者で掲示板，SNS（Social Networking Service），チャットルームやその他の情報源から DDoS 攻撃にかかわる情報を収集するとともにその情報を精査し，また，過去の DDoS 攻撃情報や社会情勢との関係から定期的／不定期的に起こり得る DDoS 攻撃の発生に関して予知・予測する．予

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** ✓ 攻撃予告の情報を事前に共有し，各社の対応の参考にする ✓ 会員企業間での情報共有内容 ・攻撃予告の内容，攻撃対象や攻撃者のプロファイルなど ✓ 外部や会員企業からの予告情報の募集／情報提供者への応答
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・対処の状況を共有し，自社の顧客への波及を検討 ✓ 会員企業間での情報共有内容 ・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，他社への波及状況の確認状況 ✓ DoS 攻撃即応 WG の観測状況
協調対処 （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** ✓ 個別の攻撃については，各事業者それぞれで対応 ✓ 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 ✓ 会員企業間での共有内容 ・攻撃様態，自社の対応，協調対処に対する品質（対処までの時間など）
振り返り	毎月～四半期	**攻撃情報の共有** ✓ 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） ✓ 振り返り会の開催　※ Telecom-ISAC Japan 主催のクローズな会員企業向けイベント ✓ Telecom-ISAC Japan からの情報公開

表 -1　各フェーズごとの情報共有と協調対処

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）
協調対処 （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 ※各事業者で対処	✓ 本攻撃の協調対処なし ※各事業者で対処
振り返り	✓ Telecom-ISAC Japan 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・協調体制を議論	✓ 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 キックオフ

表 -2　Telecom-ISAC Japan での情報共有・協調対処事例

知・予測にあたっては，各通信事業者の持つ情報や判断だけで行うのではなく，広く通信事業者間で共有した情報に基づくことで精度の向上を図る．

検知

通信事業者は個々に DDoS 攻撃を感知できるシステムを保有しており，攻撃発生時に自身の感知範囲においてそれを知り得る．自身の感知範囲外で発生する攻撃については情報共有が必要となることから，通信事業者が共同して攻撃を感知できる観測システムの整備を進める．

協調対処

通信事業者個別の対処と，その対処による DDoS 攻撃の変化などの状況を共有することで，それぞれの対応品質の向上を可能とする連携を図る．

振り返り

攻撃終了後，DDoS 攻撃に使われた手法，攻撃への対応手法や有効性などの振り返り情報を持ち寄る．すり合わせを行うことでより正確に DDoS 攻撃の全容を把握し，今後起こり得る攻撃を想定した対処を検討することで，対応能力を高める．なお，DDoS 攻撃の過去事案における情報共有・協調対処事例については表 -2 を参考にしてほしい．

■ 重要インフラホームページ応答観測システム

ここでは，DoS 即応 WG の活動の一環として推

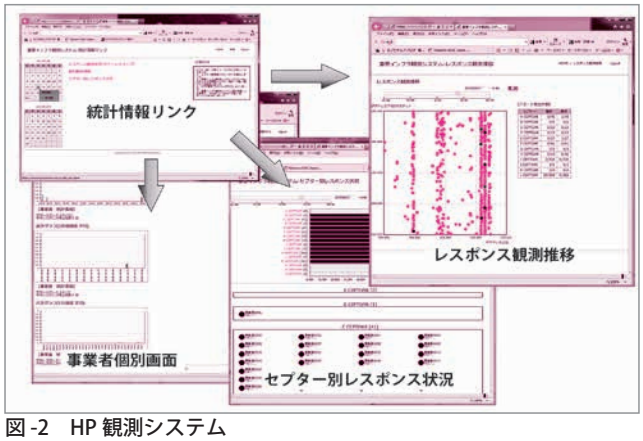

図 -2　HP 観測システム

進している事業者共同の DDoS 攻撃感知システム，通称：重要インフラホームページ応答観測システム（以降，HP 観測システム）について紹介する．

同時多発的な DDoS 攻撃において，各事業者は自身が持つ感知システムでの情報しか知り得ず，全体像を把握することが難しい．各事業者自身が持っている感知システムを補完するために，複数の事業者が共同でその外形を観測できるシステムの整備が望まれる．この課題を解決する 1 つの施策が，公開ホームページに外部から定期的にアクセスし，その応答状況から DDoS 攻撃の発生を俯瞰的に把握する観測システムの構築である．

重要インフラ事業者は，IT 障害の未然防止，IT 障害の拡大防止・迅速な復旧，IT 障害の分析・検証による再発防止のための情報共有の枠組みとしてセプターカウンシルの活動に参画している．DoS 即応 WG では，このセプターカウンシル内にある情報共有のための検討推進ワーキンググループに対し提案，承諾を得ることにより，重要インフラ事業者向けの DDoS 攻撃を俯瞰的に把握・共有する HP 観測システムを構築した．2013 年 1 月末時点で，9 セプター（事業分野），700 弱の被観測事業者が保有する約 1,600URL を観測しており，日々その観測対象数は増加している．このシステムでは，観測しているホームページの応答状況のリアルタイム表示だけではなく，IP アドレスでの統計化，分野ごとの集計などの応答状況について情報共有が可能である（図 -2）．

2012 年 1 月より観測を開始しており，2012 年 9 月のハッカー集団による日本国内サイトへの攻撃時には，ホームページの応答状況に変化を観測するなどの実績をあげつつある．幸いにして，重要インフラ事業者が対象となる同時多発的 DDoS 攻撃が発生していないため，複数事業者のホームページの応答が同じ時期に低下する事象はいまだ観測されていない．

サイバー攻撃即応スキーム検討ワーキンググループ（Practice-WG）

DDoS 攻撃を含むサイバー攻撃は多種多様化しており，その複雑性により，防御側は既存対策だけでの対応が難しくなってきている．その一方で，サイバー攻撃被害は最小限にとどめる必要があり，サイバー攻撃そのものを予知・即応できる仕組みが求められている．こうした中で，さまざまなレベル（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検討段階にある．

2011 年度より，さまざまなサイバー攻撃を把握し，情報を共有する仕組みを通した連携を実現すべく，総務省において国際連携によるサイバー攻撃の予知・即応に関する研究開発事業が進められている．Telecom-ISAC Japan のサイバー攻撃即応スキーム検討ワーキンググループ（Practice-WG / PRACTICE：Proactive Response Against Cyber-attacks Through International Collaborative Exchange）は，この事業と連携し会員企業である通信事業者のサイバー攻撃に関する前述の課題を解決するため活動している．

■ Practice-WG の役割

Practice-WG の目標は，国内外でのサイバー攻撃の実態を把握し，ISP や SOC（Security Operation Center）事業者，ホスティング事業者といった複数の事業者間で情報を共有し，有事の際に複数事業者の即応体制を確立することである．この目標は，

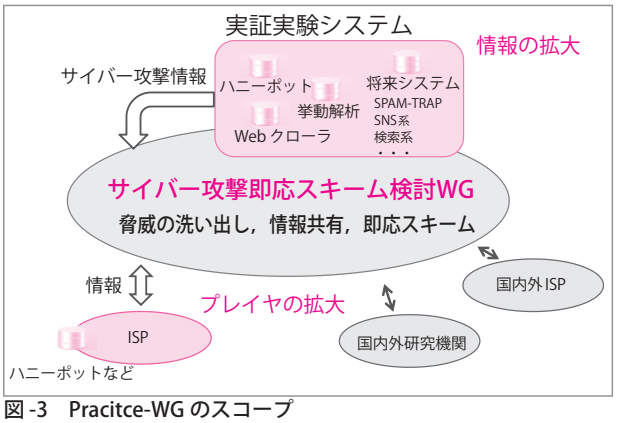

図-3　Pracitce-WGのスコープ

DoS即応WGの目的と重なる部分も多い．Practice-WGの活動上の特徴は，国内に存在するマルウェアの感染活動や感染状況を把握したり，国内外からサイバー攻撃に関する情報の入手と情報共有連携を通して，インターネット全体でのサイバー攻撃の実態把握に迫り，その中から即応しなければならない脅威を洗い出すとともに，共有すべき情報と共有方法を検討することにある（図-3）．ここでは，Practice-WGで実施したマルウェア感染活動の実態調査，特にDDoS攻撃にかかわるマルウェアについての調査状況を紹介する．

■ サイバー攻撃の予知と即応アプローチ

サイバー攻撃の予知と即応体制の確立にあたっては，リアルタイムにマルウェアの感染状況，感染活動，攻撃行動などを観測し，過去のサイバー攻撃の挙動と類似した初期行動を発見し，その後の挙動を推測し先手で対処するというアプローチで進めている．

過去のマルウェアの感染活動とDDoS攻撃の関連性の抽出

過去のマルウェアの挙動とDDoS攻撃の関連性を把握する事例として，2007年度～2011年度に総務省と経済産業省の共同プロジェクトで実施されたCCCプロジェクトのハニーポット群で収集したマルウェアを取り上げる．

図-4は，マルウェア検知推移とDDoS攻撃の発生時期を示すグラフで，国内外からCCCハニーポットに対するマルウェア感染活動を月別合計の棒グラフとして表している．この図を見る限り，マルウェア感染活動と，スポットで表したDDoS攻撃との関連性を見てとることはできない．次に，このマルウェアの中から指令サーバとしてIRC（Internet Relay Chat）を使用するIRCベースのボット型マルウェアを抽出し，その感染活動とDDoS攻撃に着目してみる．この場合，図-5で示すようにDDoS攻撃が実施された前後で感染活動が活発化しており，感染活動とDDoS攻撃になんらかの関係がありそうである．

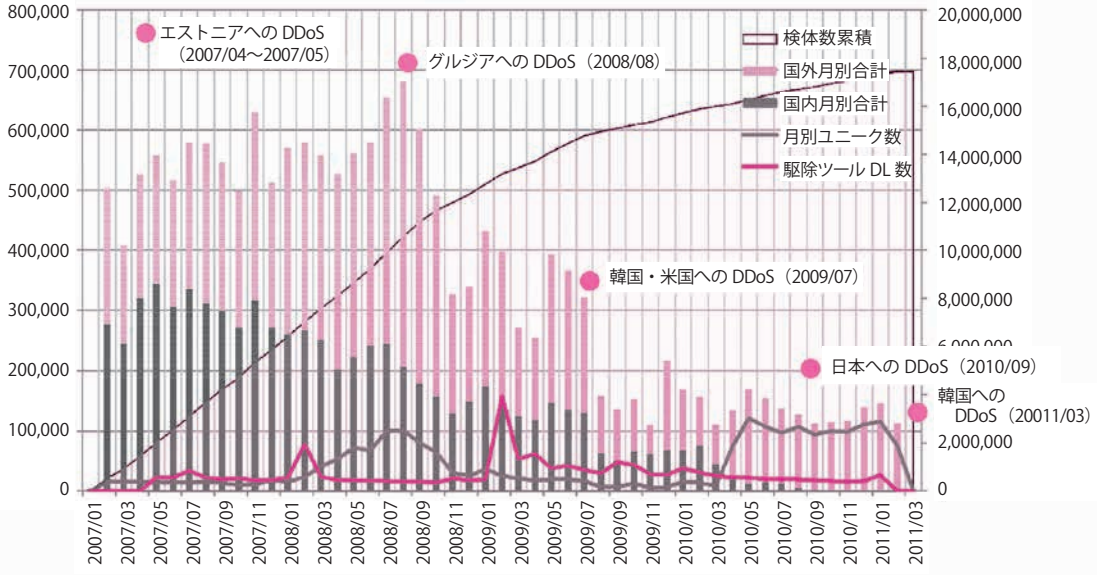

図-4　CCCハニーポットでのマルウェア検知とDDoS攻撃[6)～8)]

このほかの類似事例として，2007 年～ 2010 年の「W32.Mytob」「W32.Dozer」「Trojan.Dozer」「W32.Mydoom」の検知状況と DDoS 攻撃との関係性を図 -6 に示す．2008 年後半くらいから活発化しているこれらマルウェアの感染活動は，韓国・米国において 2009 年 7 月に起こった大規模な DDoS 攻撃の準備であったのではないかと推測される．このような実例を積み重ねていくことで，IRC ベースのボット型マルウェアの大規模な感染が起こった場合には，DDoS 攻撃発生の可能性を考慮すべきという知見を蓄えることができれば，予知と即応に役立てられるであろう．なお，実際の DDoS 攻撃において，これらのマルウェアが使用されたか否かなど，被攻撃者にかかわるファイアウォールや侵入検知のログなどを収集し関連性を調べていくことができれば，推測の確実性も向上すると考えられる．

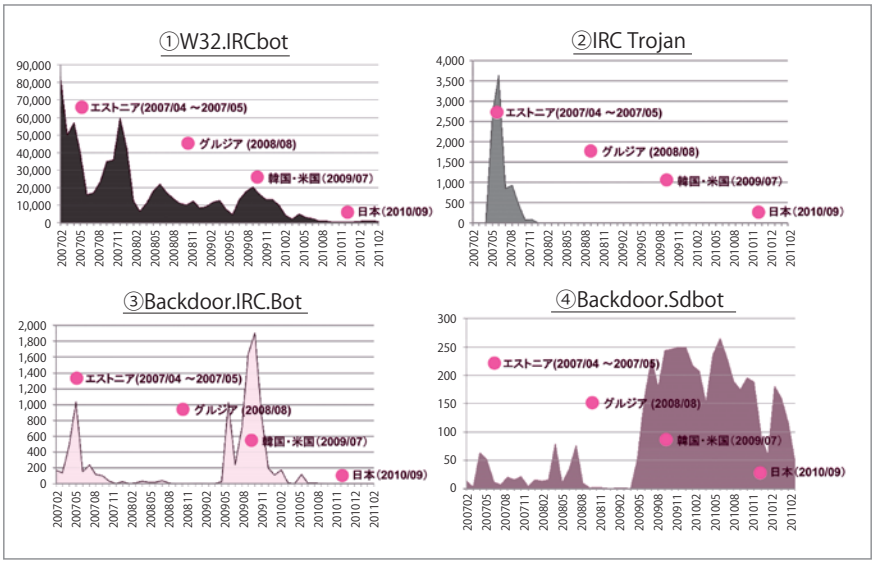

図 -5　IRC ベースのボット別のマルウェア検知と DDoS 攻撃

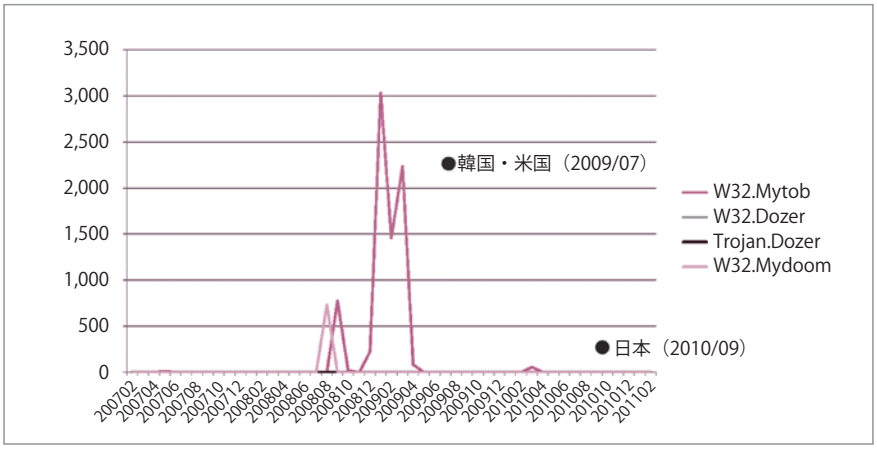

図 -6　「W32.Mytob」「W32.Dozer」「Trojan.Dozer」「W32.Mydoom」の検知状況

サイバー攻撃対応演習ワーキンググループ（CAE-WG）

DDoS 攻撃に関して対応を行う通信事業者の担当者が，DDoS 攻撃に対する理解を深め，対応を迅速に行うためには，有事に備えた訓練は有効である．ここでは，訓練を中心として活動しているサイバー攻撃対応演習ワーキンググループ（CAE-WG）を紹介をする．

Telecom-ISAC Japan では 2006 年度から総務省主催のサイバー演習に参加してきた．2009 年度からは，サイバー攻撃対応演習の継続的な実施の重要性，参加事業者の拡大および連携した対処の実現，より運用に近いシナリオでの演習などの観点から，CAE-WG を中心に，毎年，民間の通信事業者主体の独自演習を実施してきた．

■ サイバー攻撃対応演習

サイバー攻撃対応演習は，1）通信事業者間の連携の確認，2）人材育成，3）課題認識について，それぞれの参加者が後述の役割に従い，実際に組織的対応や活動ができるかについて討議をベースに訓練する机上演習となっている．

1）通信事業者間の連携の確認：通信事業者個別で対応できない状況が発生した場合，通信事業者間で連携した対応が行えるか，どのような連携を取るべきかを確認する．

名称	主な役割
ディレクタ	演習全体を統括し，演習参加各グループの状況を把握する． 各グループに対してイベントの配布を行う．
コントローラ	プレイヤにイベントや他組織からの情報の理解を促させ，討議を促しアクションを決定づけるよう指導する．
評価者	グループ内の議論の内容や決定したアクションに関する記録と評価を行う．
プレイヤ	演習の中心となる参加者で，演習では実際のアクションを起こす当事者である．

表 -3　演習参加者の役割

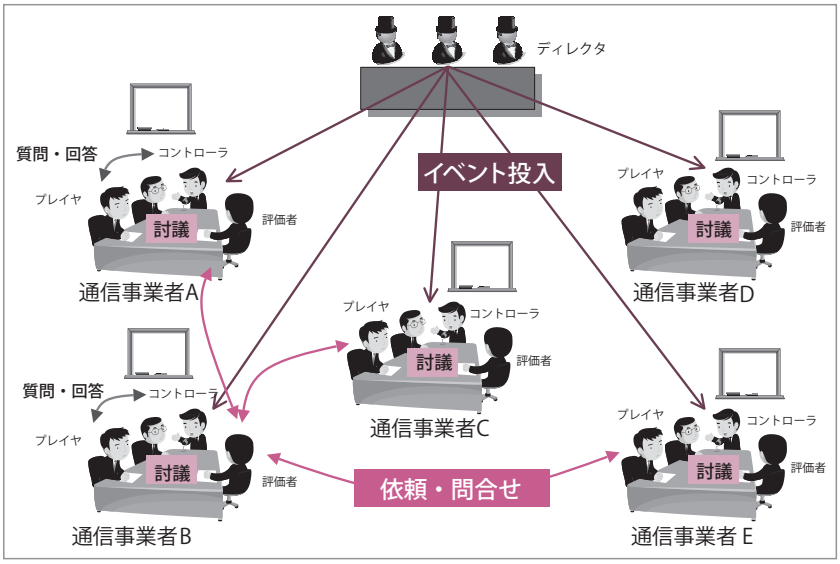

図 -7　演習の流れ

2) 人材育成：通常のオペレーションでは経験しにくいサイバー攻撃発生時の状況を演習を通じて体験し，サイバー攻撃に対応できる人材を育成する．

3) 課題認識：演習に参加した各組織の課題および協調対処の課題を認識し改善する．

さらに，演習を通じて，ほかの通信事業者の運用体制への理解を深め，担当者とのコミュニケーションの活性化を図り，人と人とのつながりを強化することで，有事の際に通信事業者間連携が円滑に進むことを期待している．大規模化，高度化，複雑化する DDoS 攻撃を含むサイバー攻撃が発生した際，演習での経験を踏まえた迅速な対応を行うことで実際の被害や影響を極小化する効果が生まれるものと考えられる．

■ サイバー攻撃対応演習の仕組み

演習のためのサイバー攻撃のシナリオは，表 -3 に示す演習参加者の役割を踏まえ，通信事業者の通常業務内で実際に起こり得る実践的なシナリオとなるよう，半年以上の時間をかけて作成している．さらに作成にあたっては，できるだけ演習の目的にそった大規模かつ複合インシデントへの対応，他社との連携能力の向上に即したものとなるように考慮している．

演習当日は，図 -7 に示す通り，演習全体のすべてを統括する「ディレクタ」のもと，演習参加者は，通信事業者ごとのグループに分かれて演習に臨むことになる．各グループには，コントローラ，プレイヤ，評価者が配置され，ディレクタから投入されたイベント，たとえば，「現在，○○サイトの Web 閲覧ができなくなっている模様です」といったイベントに従い，プレイヤはアクションを起こさなければならない．

各グループのコントローラは，プレイヤに正しいアクションを起こさせるよう，自グループのプレイヤに質問することや，イベントの大元となっているインシデント対応についての討議を行い，正しいアクションへの理解を促す．また，自グループ状況を判断しながら必要に応じてシナリオの進捗などをディレクタと調整する．

プレイヤが起こしたアクションについては，評価者が，自グループ内の議論の内容や，プレイヤが決定したアクションについて記録し，プレイヤに対し客観的な評価を行う．この評価は総括と呼ばれるものであり，個々のプレイヤの評価を集約することで，その中から課題や改善点を見出す．このような仕組みの演習を行うことで，プレイヤやコントローラは，

より実際のサイバー攻撃対応に近い形を模擬的に経験できる．

■ 2012 年度の演習

第 7 回目にあたる 2012 年度サイバー攻撃対応演習は，2013 年 1 月 18 日，表 -4 に示す架空のハッカー集団からの攻撃予告を皮切りに，DoS 攻撃によるインターネット基盤への通信容量の急増，DNS サーバの長時間ダウン，BGP（Border Gateway Protocol）☆3 経路ハイジャック，Web サイトのページ改ざん等が同時並行的に起こるシナリオで実施した．約 2 時間半の演習本番，1 時間の総括というスケジュールである．参加組織は，国内大手通信事業社 8 社だけではなく，重要インフラ事業者 2 社も加わり，参加人数は約 150 人規模となった．この規模での複数事業者にまたがる演習としては，国内最大級のものである（図 -8）．

参加者からは，シナリオや他事業者との連携シミュレーションが実践の場で役立つとの声を多数聞いており，今後も継続を求める声および継続参加の意思が多数示された．Telecom-ISAC Japan では，DDoS 攻撃を含むサイバー攻撃が発生した際に，通信事業者各社において迅速な連携，迅速な対応が可能となるよう，今後も定期的なサイバー攻撃対応演習の実施を通じて，インターネット環境のセキュリティ向上を支援していく．

項目	シナリオの概要
攻撃予告	架空のハッカー集団による攻撃予告が行われる．
インターネットの障害（1）	日本の国内外から大規模なサイバー攻撃が行われ，インターネット上のさまざまなサービスに障害が発生する．
インターネットの障害（2）	通信経路上で通信量の急増や障害が発生するなどし，正常な通信が行えなくなる．
インターネットの障害（3）	DNS などインターネットを利用する上で基本となるシステムにも障害が発生する．
Web 改ざん	Web サイトの改ざんにより，自社の Web ページにアクセスしたユーザの PC がマルウェアに代表される不正なソフトウェアに感染し，偽サイトへの誘導事案が発生する．
終息	架空のハッカー集団の中心メンバが逮捕されたことが報道される．

表 -4　シナリオ概要

図 -8　サイバー攻撃演習実施模様

次の戦いに向けて

本稿では，国内大手 ISP や通信事業者などを会員とする情報セキュリティ推進組織である Telecom-ISAC Japan でのサイバー攻撃への対応，特に DDoS 攻撃への対応として，DoS 攻撃即応，サイバー攻撃即応スキーム検討，サイバー攻撃対応演習ワーキンググループの活動を紹介した．

Telecom-ISAC Japan では，本稿で紹介している 3 つのワーキンググループ以外にも，アクセスライン，BGP 運用，カスタマーコントロール，Abuse ☆4 に関連したワーキンググループ活動を進めている．これらワーキンググループでは，ISP を中心とした通

☆3　インターネットの通信経路情報を交換するための手順．

☆4　Abuse（アビュース）は不正使用や乱用を意味する英単語である．このワーキンググループでは，ネットワークを利用した不正・不法行為対応に関する情報を共有し，インシデントの拡大を抑止するフレームワークを策定している．

信事業者にかかわるさまざまな問題を，ビジネス競合の壁を越えて集まり，協調して問題の解決を図っている．また，これらワーキンググループの活動は，昨今の国内外インターネットで起こる DDoS/DoS 攻撃を含むサイバー攻撃が，大規模化，高度化，複雑化している現状において，より密接な連携が必要となってきている．

Telecom-ISAC Japan では，大規模化，高度化，複雑化してきているサイバー攻撃に対して，ワーキンググループの活動を連携させるだけではなく，複数の事業者，複数の組織，複数の観点から対応できる強固な連携，高い対応能力の実現を通して，インターネットを含む通信事業の健全性を高める努力を継続的に実施する．また，日本のインターネットユーザにより安心・より安全なインターネット環境を提供する努力をし続ける組織を目指していく．

参考文献

1) IPA：「サービス妨害攻撃の対策等調査」報告書，http://www.ipa.go.jp/security/fy22/reports/isec-dos/index.html
2) Cyber Clean Center, http://www.ccc.go.jp/
3) 総務省報道発表資料，http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000036.html
4) セプターカウンシル事務局報道発表資料，http://www.nisc.go.jp/press/pdf/ceptoar_council20090226_press.pdf
5) （社）日本インターネットプロバイダー協会，（社）電気通信事業者協会，（社）テレコムサービス協会，（社）日本ケーブルテレビ連盟，（財）日本データ通信協会：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，テレコム・アイザック推進会議，http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf
6) 防衛省：防衛省・自衛隊におけるサイバー攻撃対処について，新たな時代の安全保障と防衛力に関する懇談会第七回配布資料，http://www.kantei.go.jp/jp/singi/shin-ampobouei2010/dai7/siryou3.pdf
7) 名和利男：最新のサイバー攻撃の発生メカニズムと，対策のあるべき姿，NICT 情報通信セキュリティシンポジウム 2012，http://www2.nict.go.jp/nsri/plan/H24-symposium/pdf/04.Nawa_presentation.pdf
8) IIJ : Internet Infrastructure Review, http://www.iij.ad.jp/company/development/report/iir/index.html

（2013 年 2 月 18 日受付）

謝辞　本稿は，Telecom-ISAC Japan で日々行っている活動について，DDoS 攻撃対応の観点でまとめ，紹介したものである．日頃より，Telecom-ISAC Japan の活動についてご理解・ご協力をいただいている会員企業各社および活動に参加していただいている各会員企業社員各位，また，さまざまなご指導をいただいている一般財団法人日本データ通信協会幹部各位，Telecom-ISAC Japan 飯塚会長，伊藤副会長，林副会長，大島副会長，ステアリングコミッティ運営委員各位に感謝するとともに，本稿を作成するにあたり各種データのとりまとめに関してご協力をいただいた NRI セキュアテクノロジーズの初谷良輔氏に御礼申し上げたい．

■西部喜康　nishibe@telecom-isac.jp

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企画調整部部長．