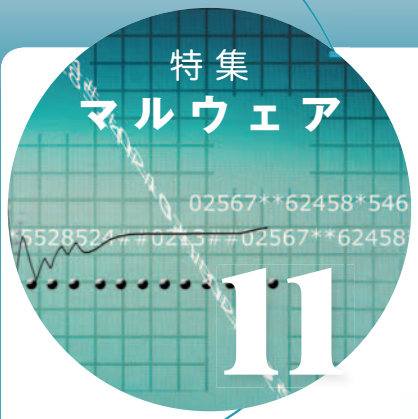

{コラム}

マルウェア対策に向けた国際連携

早貸淳子（JPCERT コーディネーションセンター）

CSIRT の国際連携

マルウェア対策等の情報セキュリティ対策にはグローバルな視点での取り組みが必要であることはいうまでもない．マルウェア対策に関する「国際連携」は，研究機関や民間事業者の間においてもさまざまな形で実施されているが，このコラムでは，特に，CSIRT（Computer Security Incident Response Team）間の国際連携に絞って紹介する．

CSIRT とは

「CSIRT（シーサート）」とは，あらかじめ定めた活動対象範囲において発生したコンピュータセキュリティインシデント（以降，インシデント）について，報告を受け取り，調査し，対応・連携活動を行う組織または機能の名称である．それぞれの CSIRT の活動内容は，活動対象範囲がどのように定められているかによって異なる．

企業等の組織やその顧客に関するインシデントに対応する CSIRT（組織内 CSIRT）や自社製品の脆弱性に対応する CSIRT（ベンダ CSIRT）もあれば，一国の全域を活動対象範囲とし，その国におけるコンタクトポイントとしてさまざまな CSIRT や関係機関とのインシデント対応の連携を図る CSIRT（National-CSIRT）等，さまざまな性質の CSIRT が存在する．

JPCERT コーディネーションセンター（以降，JPCERT/CC）は，日本の全域を活動対象範囲とし，日本のコンタクトポイント CSIRT として，インシデント対応のための関係機関間の調整（コーディネーション）を行っている．

CSIRT 連携の枠組み

多様な CSIRT によるグローバルな国際連携

このようなさまざまな性質の CSIRT がインシデントへの迅速な対応のための協力や情報共有の円滑化を目的として集う世界的規模の国際フォーラムが，1990 年に設立された FIRST（Forum of Incident Response and Security Teams）である．47 カ国から 205 のチームが参加し（2009 年末現在），マルウェア対策に限らず，インシデントへの対応に関するさまざまな観点の問題について情報共有が図られている．2009 年の年次会合は，6 月 28 日から 7 月 3 日の間，京都で開催され，50 を超える国から，400 名近い参加者を得た．2010 年の年次会合は，6 月 13 日から 18 日の間，マイアミで開催される予定であり，AGM（Annual General Meeting）を除き，FIRST 加盟チームのメンバでなくても参加できる [1]．

年次会合のほかにも，FIRST メンバ間の，脆弱性やインシデント等に関する情報共有を目的とする FIRST Technical Colloquia（以降，TC）が適時開催されている．2008 年 3 月には，日本から FIRST に加盟しているチームが共同で，マルウェアに関する問題を扱う TC を東京で開催している．

地域内連携

アジア太平洋地域の National-CSIRT を中心とする CSIRT 間における，円滑なインシデント対応や対策の実施協力のための連携の枠組みとして，APCERT（Asia Pacific Computer Emergency Response Team）が設立されている [2]．

この枠組みは，平成 14 年度から平成 17 年度における科学技術振興調整費「我が国の国際的リーダーシップの確保」プログラムにおいて「アジア太平洋地域インターネット防護体制の確立」のプロジェクトとして立ち上げられた．

APCERT のミッションステイトメントには，メンバ間における，インシデントへの対応の協力のみならず，マルウェアに関する情報共有や技術交換など，マルウェア対策に向けての協力が規定されている（具体的な活動については，後述のマルウェア対策に向けた取り組みの部分で紹介する）．特に，利用している IP アドレス範囲が近い地域間での連携の意義は大きいことから，域内の CSIRT 機能未整備国に対する機能構築・運用支援や域内のインシデント対応演習等，活発な連携活動が進められている．

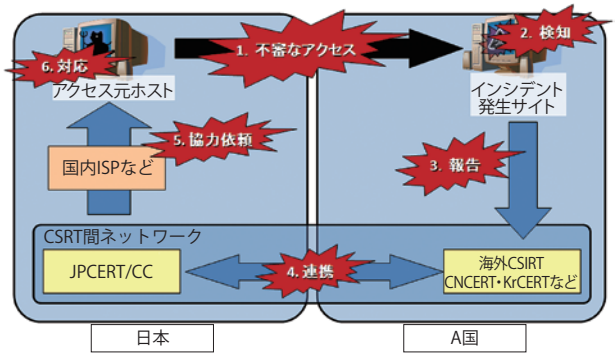

図 -1　インシデント対応に関する CSIRT 間協力

TLD	報告元	通知（対応依頼）先
.jp	2029	753
.jp 以外	7170	1450
合計	8199	2023

表 -1　2009 年 1 月から 12 月のインシデント対応件数

同様の理由により，欧州地域には TF-CSIRT[3]，中南米地域には CLARA WG-CSIRT，湾岸地域には GCC-CERT 等，他地域においても地域内連携の枠組みが存在しているだけではなく，地域連携間の協力も進められている．

National-CSIRT 連携

例年，FIRST の年次会合終了後に，National-CSIRT（CSIRTs with national responsibility）が参集する“Collaboration Meeting for CSIRTs with National Responsibility”が米国 CERT/CC 主催で開催されている．この会合では，共同プロジェクトに関する協力や National-CSIRT に固有の課題に関する意見交換などが行われている[4]．

マルウェア対策に向けた連携

マルウェア対策に向けた CSIRT 間の国際連携については，

(1) 国境を越えて発生したインシデントへの対応の調整のために必要となるマルウェアに関する情報の共有
(2) マルウェアの脅威分析に関する協力
(3) インシデント対応演習の実施
(4) マルウェアに関する分析能力の向上，人材育成のための協力

等がある．

●インシデント対応調整のためのマルウェア情報の共有

マルウェアに起因して発生するインシデントが報告された場合，JPCERT/CC では，被害の拡大抑止のため，報告に係るマルウェアを解析した結果に基づき，マルウェア配布サイトや，マルウェアが窃取した情報の送付先サイト等の活動を停止させるための調整活動を行う．

インシデントを引き起こす攻撃は国境を越えて行われる場合が多いことから，おのずとこのような調整を行う先も海外の組織になることが多い．対象となるサイトの管理者に直接依頼をする場合もあれば，対象となるサイトが存在する国の National-CSIRT に協力を依頼する場合もある．

逆に，日本国内に存在する PC やサーバが海外のユーザに対する攻撃に利用されている場合には，海外の関係機関から，その PC やサーバの活動停止を求める調整の依頼が寄せられ，JPCERT/CC から国内のサイト管理者などに対して調査や対応を依頼することになる（図 -1）．

海外からのインシデント報告（2009 年 1 年間における報告元のドメインは，「.my」「.br」等 33 種に及ぶ）については国内のサイトが調整先となる場合が多く，国内からの報告については海外のサイトが調整先となる場合が多い（同期間における調整先ドメインは，「.com」のほか「.cn」「.ru」「.br」等 47 種）（表 -1）．

いずれの場合についても，対応や調査を依頼するためには，その根拠を示す必要があることから，マルウェアの活動痕跡を示すアクセスログや，状況に応じてマルウェア検体の解析結果等の情報を合わせて提供することになる．

調整の相手方 CSIRT がマルウェア検体の収集能力や解析能力を有している場合には，マルウェア検体のハッシュ値を提供するだけで，攻撃の影響や対応に必要となる情報を共有できることも多い．しかし，調整先がそのような体制を有していない場合や，優先度を上げた迅速な対応を求める必要がある場合には，マルウェア検体や詳細解析で得られた情報を提供する必要が生じる．

このような情報は，悪用されるとユーザの脅威を増すことにつながってしまうため，提供に当たっては，情報を提供する相手方が関連情報を適切に取り扱うことができる組織であることの確認や，このような情報を共有した場合の取り扱いに関する合意が形成されている必要がある．インシデントが発生してからこのような確認や合意形成をしているようでは，その間にも被害が拡大してしまうことから，CSIRT 間では，上述の CSIRT 間連携の枠組みなども利用しつつ，平素からの信頼関係の醸成や対応ポリシーの確認，覚書／秘密保持契約の締結等，いざというときに迅速な連携対応を行うための関係を構築している．

●マルウェアの脅威分析に関する協力

CSIRT 間の国際連携においては，発生したインシデ

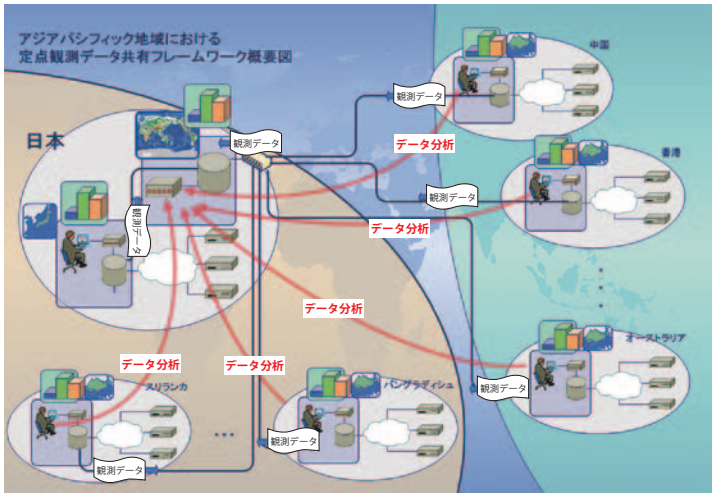

図 - 2　TSUBAME プロジェクト概念図

ントへの対応のみならず，平素からの，脅威情報の収集・共有，および収集した情報の分析による攻撃手法・目的の変化の予測，事前対策の検討等の分野においても連携を深めることが重要である．

日本国内での報告が目立ち始めたマルウェアについて，他国での出現状況に関する情報を共有することで攻撃者の意図の分析につなげたり，（日本からの攻撃の状況を確認することで）国内における感染の広がりの分析につなげたりすることができる．

また，インターネット上での攻撃活動を把握するインターネット定点観測についても，国内だけでなく海外にもセンサを設置してデータを集約することにより，(1) 日本から各国に向けて発せられている攻撃（日本国内の情報システムの感染実態）や (2) 第三国間における攻撃の状況の把握が可能になる．

このような観測の相互補完を目的として，2008 年から，APCERT 加盟チーム等が連携し，アジア太平洋地域各国に観測システムのセンサを設置して，観測データを一元的に集約し，参加各国で共有する枠組み（アジア太平洋地域インターネット観測データ共有フレームワーク：TSUBAME プロジェクト）の運用を開始している（図 -2）．

各国の CSIRT が同じ手法で各国から集められた観測データを，各々または共同で解析するとともに，確認された異常値と国内で発生している事象を組み合わせて分析することで，自国への影響の分析に資する情報を収集できる．また，分析手法や結果等の共有を進めることで，分析活動自体の共有・連携も図ることが可能となる．

たとえば，2009 年 7 月に Oracle データベースが使うポート（Oracle TNS Listener：1521/TCP）に対する中国からのスキャン（ポートの稼働を探索する活動）の急増が観測され始めた（図 -3）．これと同時期に，そのポートをスキャンする機能と攻撃する機能とを兼ね備えたツール ”Oracle Auto Attacker” の公開が確認されており，これらの情報を合わせて分析することで，攻撃ツールの拡散範囲等を検討することが可能となる．

アジア太平洋地域内での展開を優先させている意図としては，APCERT という連携基盤がすでに存在していることに加え，利用している IP アドレス範囲が隣接していることが挙げられる．利用している IP アドレス範囲が隣接する各国間においては，攻撃の傾向に類似性があったり，逆に IP アドレス範囲が隣接しているにもかかわらず異なった状況が発生したりする場合がある．このような視点での分析は，攻撃者の目的の解明につながる可能性が高くなる等，脅威情報の共有・分析活動の連携効果も大きい．

2010 年 1 月末現在，14 カ国／経済地域のチームが TSUBAME プロジェクトに参加している．国や経済地域によってインターネット利用の規模が異なることから，現在，どのようにセンサを配置すれば，より意味のある観測データを収集できるか等，適切なセンサの配置について継続して検討を進めている．

●インシデント対応演習の実施

インシデント対応演習は，実際にインシデントが発生した場合に備え，円滑なマルウェアの分析協力やインシデントへの対応調整を行うための CSIRT 間連携の枠組みが有効に機能することを確認するため，定期的に実施している．

ACID 2009

2009 年 7 月 23 日に，ASEAN 加盟国の CSIRT に，CNCERT/CC（中国），KrCERT/CC（韓国）および JPCERT/CC（日本）等の連携先 CSIRT を加えた 13 経済地域／ 14 チームが参加して，“ASEAN CERT Incident Drill（ACID）2009” が実施された．ACID の演習は，今回が 3 年目（3 回目）で，ボットによる攻撃の調査と対応をテーマに，パケットの分析，ログの解析，ボットネットの指令サーバの追跡と閉鎖までを演習シナリオとして実施した．

APCERT 演習 2009

2010 年 1 月 28 日に，16 チームの参加を得て，6 年目（6 回目）を数える APCERT 演習を実施した．

今年は，金融機関に対するマルウェアを利用した攻撃への対処を想定した．パケットの解析から，マルウェア配布サイトへの誘導やマルウェア配布サイトの特定，サイトの閉鎖依頼等の流れに応じ，実際に各チームにおいて解析等の作業を行いつつ，解析結果の共有やサイト閉

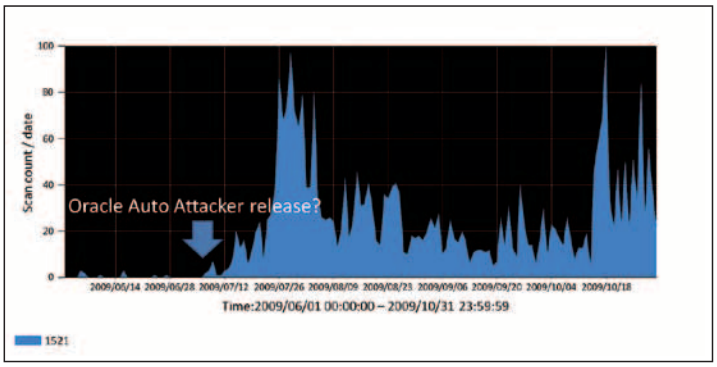

図 -3　Oracle TNS Listener への攻撃活動の観測

鎖に関する連絡までの実施手順の確認を行った．

過去の演習においては，各国内における ISP 等の関係組織との間の情報連携の確認をテーマに，国内 ISP 事業者各社にもご協力をいただいた．しかし，昨今のマルウェアによる攻撃活動の複雑化により，演習シナリオについても CSIRT 内での解析作業の比率が高まり，限られた時間の演習において，国内における情報連携／共有への展開を組み込むことが難しくなる傾向にある．演習に一層の実効性を持たせるためには，国内関係組織への展開等，連携の広がりを持たせることが今後の課題となる．

●マルウェアの分析能力向上，人材育成に関する協力

マルウェアに起因するインシデントへの対応調整は，国境を越えて行われることが多く，そのために CSIRT 間で国際連携の強化が図られていることは上述のとおりである．ただし，各国の窓口となる CSIRT の機能が立ち上がっていない場合には，その国に対する実際の対応調整が円滑に進まないこととなってしまう．そのような事態を回避するため，窓口 CSIRT の機能の構築が遅れている国に対する支援活動が，JPCERT/CC のみならず，KrCERT/CC（韓国）や CNCERT/CC（中国）等の各国 CSIRT や，APCERT，TF-CSIRT（欧州）のような地域 CSIRT 連携の枠組み，ITU 等の国際機関によっても積極的に実施されている．

JPCERT/CC においても，アジア太平洋地域の各国のほか，湾岸地域，アフリカ地域等において，CSIRT 機能構築や運用技術支援セミナの講師を務め，（独）国際協力機構（JICA）のプロジェクトによる短期専門家を派遣してカンボディアの National-CSIRT の機能構築を支援する等の活動を推進している．

最近では，（財）海外技術者研修協会（AOTS）が，“The Program on Information Security - Strengthening of CSIRT” と題する，アジア地域の National-CSIRT や組織内 CSIRT のスタッフ等を対象とする呼び寄せ研修を始めている．今年は，2009 年 1 月 13 日から 22 日までの間東京で実施し，カンボディア，インドネシア，フィリピン，ヴィエトナムおよびタイから 25 名が参加した．

今年の研修は，3 回目となることから，より専門的なコースとして，マルウェア解析やインターネット定点観測情報の分析の演習を多く盛り込んだほか，分析・解析作業が必要となるインシデント対応調整演習も実施した．

今後の課題

昨今のマルウェアを用いた攻撃活動の複雑化により，攻撃に利用されるサイトの閉鎖等の対応調整を行うための分析・解析の作業負担は日に日に増している．CISRT 間でのリソース共有等を図る努力は進めているが，それだけでは到底十分とは言えない．インシデントへの対応に平素からご協力をいただいている ISP 事業者各社，インシデントの報告にご協力をいただいているセキュリティベンダ各社を始め，研究機関や「マルウェア対策研究人材育成ワークショップ」で培われた大学等の研究体制との連携をも取り込んだ形での国際連携の展開の必要性を強く感じる毎日である．

日本におけるマルウェア対策研究人材育成ワークショップの成功をアジア太平洋地域などにも展開することができれば，マルウェア対策研究の土壌が広がり，奥行きの深い国際連携の実現に繋がり得ること，さらには，それにより，インシデント対応調整や被害拡散抑止に関する国際連携がより効率的で，実効性の高いものとなっていくのではないかと期待している．

この場をお借りして，マルウェア対策をはじめとするコンピュータセキュリティインシデントやソフトウェア等の脆弱性への対応の調整にご協力をいただいている関係組織の皆様にお礼申し上げます．

参考文献

1）Annual FIRST Conference：http://conference.first.org/
2）Asia Pacific Computer Emergency Response Team
http://www.apcert.org/index.html
3）TF-CSIRT：http://www.terena.org/activities/tf-csirt/
4）Collaboration Meeting for CSIRTs with National Responsibility
http://www.cert.org/csirts/national/conference.html

（平成 22 年 1 月 29 日受付）

早貸淳子（正会員）
office@jpcert.or.jp
法務省，経済産業省等において電子商取引基盤の構築等に関する施策等を担当の後，（独）情報処理推進機構（IPA）セキュリティセンター長等を経て，2006 年から JPCERT/CC 常務理事．