組織間連携に向けたサイバーセキュリティ対策の取り組み

寺田 真敏 Terada Masato
藤原 将志 Fujiwara Masashi
沼田 亜希子 Numata Akiko
西川 由佳理 Nishikawa Yukari
久芳 瑠衣子 Kuba Ruiko

サイバー攻撃は変遷を続け，攻撃によるセキュリティインシデントは多様化し，情報システムや制御システムをベースにインターネットを活用して構築された社会インフラに与える影響は深刻なものとなっている。HIRTでは，インシデントオペレーションを通して日立グループのサイバーセキュリティ対策活動を先導するとともに，新たなアプローチとして，異なる組織のCSIRTどうしの情報共有を通して，侵害活動を鳥瞰し問題解決を図るサイバーセキュリティ対策に取り組んでいる。

1. はじめに

Heartbleed（ハートブリード），Shellshock（シェルショック），POODLE（Padding Oracle On Downgraded Legacy Encryption）（プードル）と，振り返れば，2014年は脆（ぜい）弱性対策の再考の年であった。これらは，いずれも脆弱性に付与された別名で，広範囲に影響を与え，注目を集めた脆弱性である。これら脆弱性は，情報システムや制御システムをベースにインターネットを活用して構築された社会インフラが，セキュリティインシデントにつながる脅威の一つとして，脆弱性という課題に直面していることを浮かび上がらせた。そして，日々のサイバーセキュリティ対策活動を通して，新たな脅威となりうる脆弱性という課題に立ち向かっていく必要があることを示唆した。

HIRT（Hitachi Incident Response Team）は，新たな脅威によって発生しうるセキュリティインシデントを日立グループ全体で予防し，万一インシデントが発生してしまった場合には迅速に対処することにより，顧客や社会の安心かつ安全な社会インフラの実現に寄与するための組織である。本稿では，HIRTが推進している組織間連携に向けたサイバーセキュリティ対策の取り組みについて述べる。

2. セキュリティインシデントの動向

2.1 概況

マルウェアを用いたサイバー攻撃は技術を継承しながら，活動形態を大きく変化させつつ進化してきている。1999年ごろはウイルス添付型メール，2001年ごろは脆弱性を利用するネットワーク型ワーム，2004年ごろは遠隔操作可能なボットが流布した。2008年ごろからは，ブラウザが利用するプラグインやアプリケーションの脆弱性を利用したWeb感染型が，2011年に入ると，電子メールと遠隔操作ツールとを組み合わせた組織内ネットワークへの侵害活動である標的型攻撃へと変遷してきた。侵害活動に利用される感染経路も，電子メール，Webアクセス，ソーシャルネットワークなど利用可能な通信インフラに合わせて広がっている。

2014年のサイバーセキュリティのトピックは，社会インフラのさまざまなセキュリティインシデントにつながる脅威の一つとして脆弱性問題（表1参照）が顕在化したこ

表1｜2014年に報告された代表的な脆弱性

脆弱性とは，不正アクセス，マルウェアなどの攻撃により，その機能，性能などを損なう原因となりうるセキュリティ上の欠陥のことである。

時　期	脆弱性の概要
2014年4月	Heartbleed（ハートブリード） OpenSSLの脆（ぜい）弱性
2014年9月	Shellshock（シェルショック） Bashの脆弱性
2014年10月	POODLE（プードル） SSL 3.0の脆弱性
2015年1月	GHOST（ゴースト） 汎用（はんよう）ライブラリglibcの脆弱性
2015年3月	FREAK（フリーク） 輸出グレード暗号使用の問題

注：略語説明　SSL（Secure Sockets Layer），
POODLE（Padding Oracle On Downgraded Legacy Encryption），
FREAK（Factoring attack on RSA-EXPORT Keys）

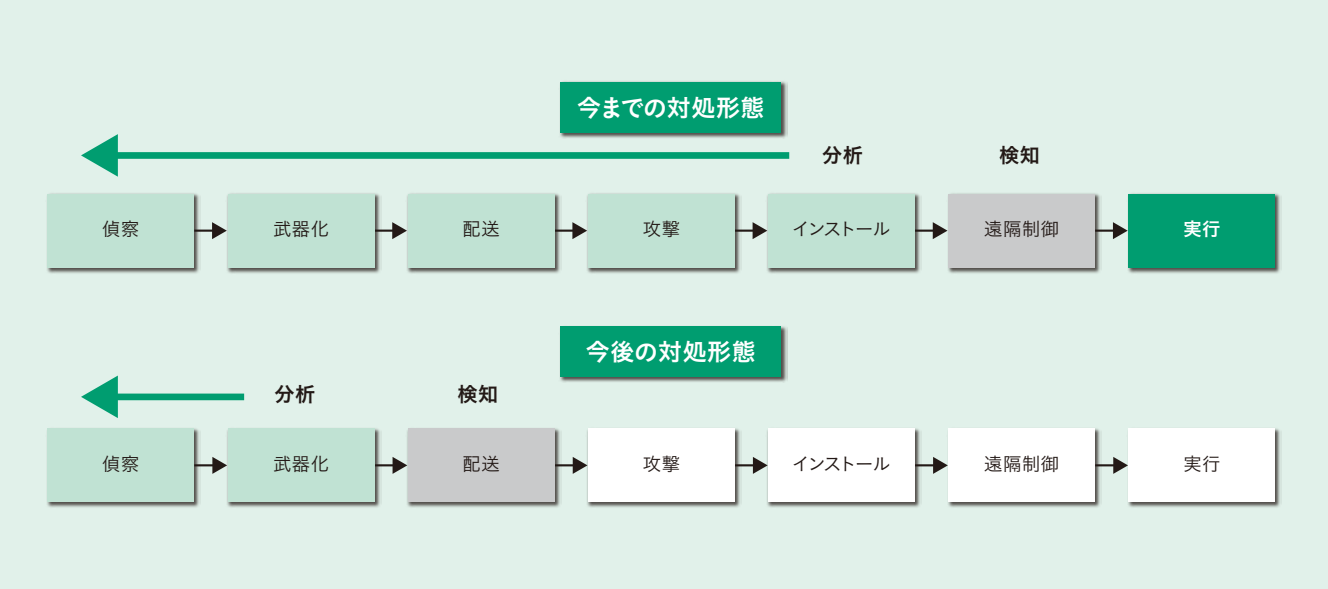


図1｜初期段階での対処の推進

上段は今までの対処形態，下段は今後の対処形態である。今後の対処形態では，配送段階での検知，武器化段階以前の分析と，攻撃者の意図，攻撃者のパターン，行動，TTP（Tactics, Techniques and Procedures）を明らかにする攻撃活動分析の必要性に言及している。

とである。セキュリティインシデントの特徴としては，インターネットバンキングを対象とした不正プログラムによる被害の深刻化，標的型攻撃やWebサイト侵害など，マルウェアを用いたサイバー攻撃による被害の定常化が挙げられる。特に，Webサイトへのサイバー攻撃は，アカウント情報を辞書化してさまざまなサイトに不正ログインを試みるパスワードリスト攻撃が一般化してきている。また，要求／応答のメッセージ増幅を利用した増幅型DoS（Denial of Service）攻撃やパソコン内のファイルを人質に取るランサムウェアなど，サイバー攻撃だけではなく，サイバー攻撃の回避と引き換えに攻撃者が金銭を要求する侵害活動も出始めてきた。ランサムウェアは，パソコン内のファイルを暗号化し，その暗号解除と引き換えに金銭を要求する不正プログラムの総称である。もし，事業上の重要なファイルがランサムウェアによって暗号化されてしまった場合には，事業継続に直接的影響を受ける可能性があり，サイバー攻撃対策も情報搾取だけではなく，情報破壊にも目を向けていく必要がある。

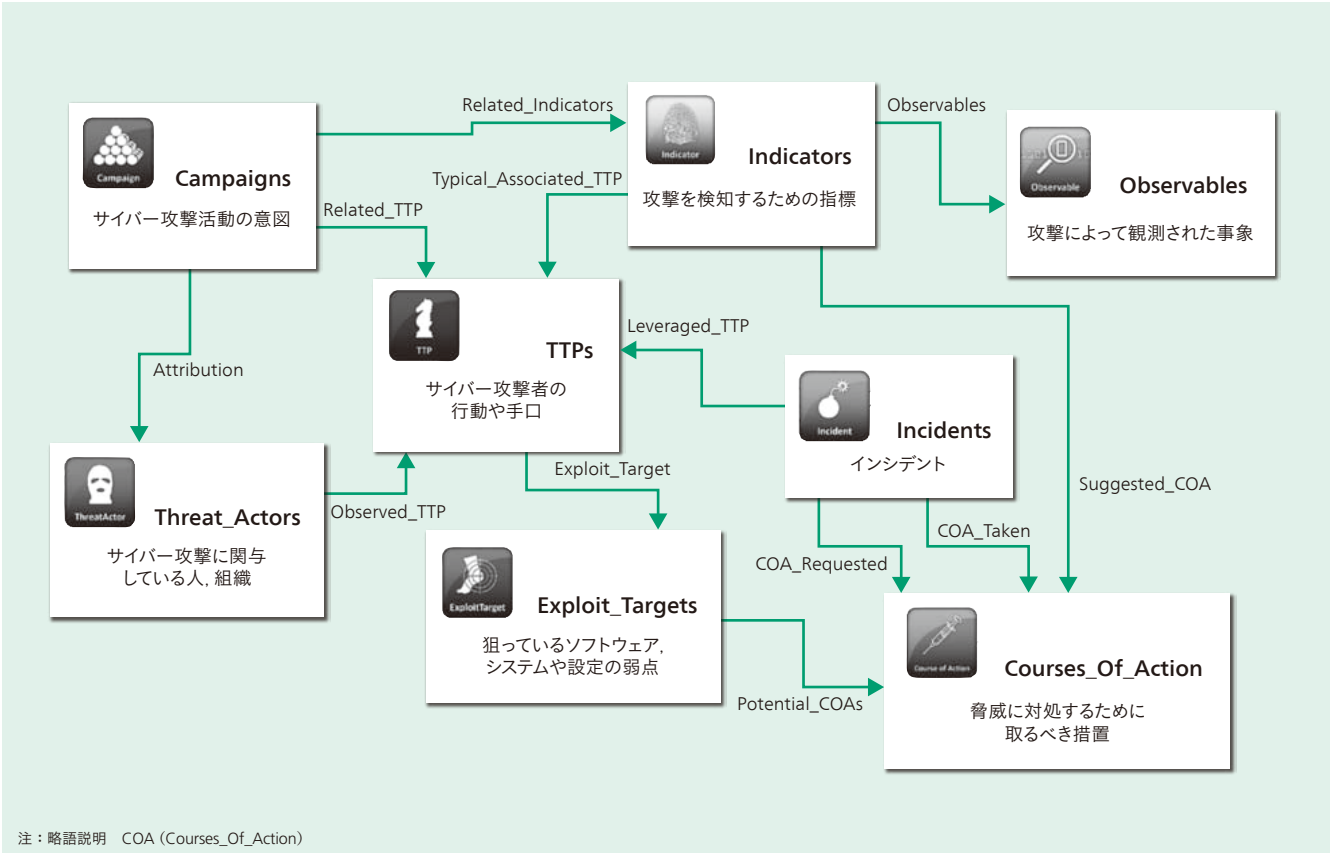
2.2　サイバー攻撃活動のモデル化

多様化と巧妙化するサイバー攻撃に対抗するため，サイバー攻撃活動をモデル化し，対策を検討する試みが行われている。例えば，攻撃対象となる組織に合う手法を選択し（標的型），組織内ネットワークを活動基点とした（潜伏型）侵害活動といわれている標的型攻撃については，その進行段階に着目したモデルがある[1), 2)]。文献2）では，米国空軍の軍事コンセプトであるKill Chain（F2T2EA）をサイバーに応用し，攻撃活動を対策視点でモデル化したCyber Kill Chainを提案している（図1参照）。このモデルは，Reconnaissance（偵察），Weaponization（武器化），Delivery（配送），Exploitation（攻撃），Installation（インストール），Command and Control（C2：遠隔制御），Actions on Objectives（実行）の7段階から成る。また，初期段階での対策として，配送段階での検知，武器化段階以前の分析と，攻撃者の意図，攻撃者のパターン，行動，TTP（Tactics, Techniques and Procedures：戦術，技術および手順）を明らかにする攻撃活動分析（Campaign Analysis）の必要性を示している。

サイバー攻撃活動の進行段階のモデル化と共に，攻撃活動分析のための情報活用が検討されている。米MITRE社が開発した，脅威情報構造化記述形式STIX（Structured Threat Information Expression）[3)]は，サイバー攻撃活動の攻撃から対策までを記録するためのXML（Extensible Markup Language）仕様である。2010年に，US-CERT（United States Computer Emergency Readiness Team）とCERT※）/CC（Computer Emergency Response Team/Coordination Center）間での脅威情報の交換から検討が始まり，2013年4月にVer1.0がリリースされた。このSTIXでは，サイバー攻撃で狙っているソフトウェアやシステム，設定の弱点といった，攻撃を検知するための事象だけではなく，攻撃者の行動や手口，サイバー攻撃に関与している人，組織などを関係づけていくためのサイバー攻撃活動の構造化が試みられている（図2参照）。

これらサイバー攻撃活動のモデル化，構造化は，観測事

※）CERTは，CERT/CCの登録商標である。



注：略語説明　COA（Courses_Of_Action）

図2｜STIXによる脅威情報構造化

脅威情報構造化記述形式STIX（Structured Threat Information Expression）は，サイバー攻撃活動の攻撃から対策までを記録するためのXML（Extensible Markup Language）仕様である。

象（Observables：攻撃によって観測された事象），検知指標（Indicators：攻撃を検知するための指標）の情報共有を通じた組織間連携型のサイバー対策として注目され，各所での適用が試みられている。

3.　日立グループにおけるCSIRT活動

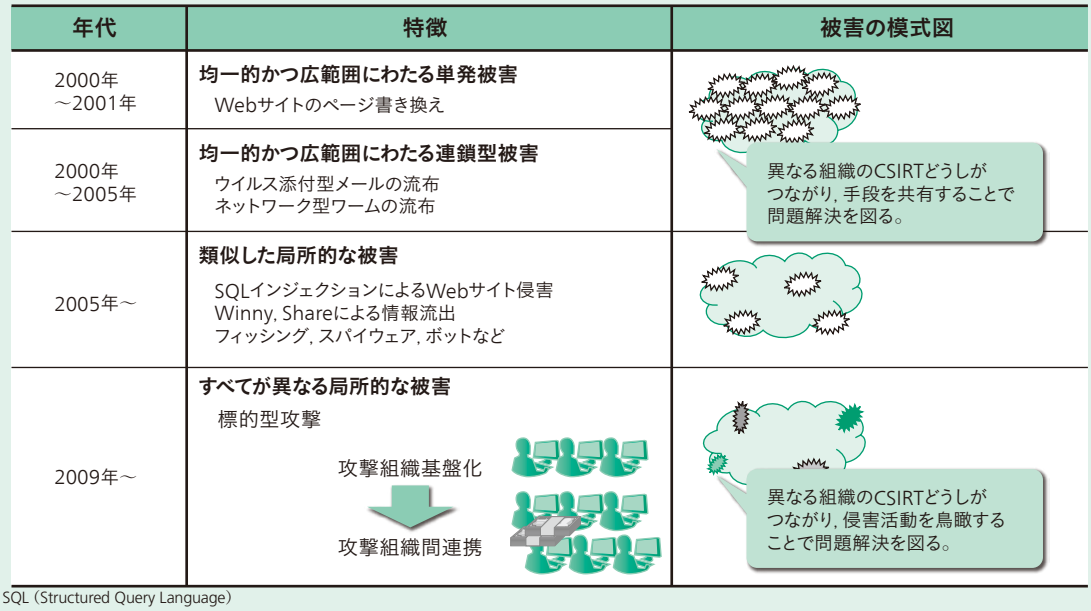
3.1　CSIRT（シーサート）

2012年以降，国内では，サイバー攻撃に対処するためのCSIRT（Computer Security Incident Response Team：サイバーセキュリティにかかるインシデントに対処するための組織の総称や機能）活動に注目が集まっている。CSIRTの主な活動の一つが，インシデントの原因や対応方法に関する情報共有を通して，あらかじめ決めておいた計画に沿って事後対処する「インシデントレスポンス」である。2005年ごろまでは，異なる組織のCSIRTどうしが手段を共有することで問題解決を図るアプローチが「インシデントレスポンス」においても有効であった。しかし，セキュリティインシデントやサイバー攻撃の変化は，対処側の考え方にも反映され，異なる組織のCSIRTどうしが，侵害活動を鳥瞰（かん）することで問題解決を図ることが求められてきている。これは，多様化と巧妙化するサイバー攻撃に対抗するためには，サイバー攻撃活動分析というレベルアップが必要であることに他ならない（図3参照）。

3.2　HIRT（Hitachi Incident Response Team）

1998年4月，HIRTは，日立グループとしてのCSIRT体制を整備するために研究プロジェクトとして活動を開始した。この活動の中で，脆弱性対策やインシデント対応を推進するにあたり，「技術的な視点で脅威を推し量り，伝達できること」，「技術的な調整活動ができること」，「技術面での対外的な協力ができること」という能力を備えていることをHIRTがCSIRTとして活動するための要件としている。また，そのミッションは，インシデントオペレーション（インシデントに伴う被害を予測ならびに予防し，インシデント発生後は被害の拡大を低減するために実施する一連のセキュリティ対策活動）の経験値を生かして「次の脅威をキャッチアップする過程の中で早期に対策展開を図る」としている。HIRTは，これら能力ならびにミッションを持った組織として，日立グループの対外的なCSIRT統一窓口としての責務を負っている。

HIRTでは，多様化と巧妙化するサイバー攻撃に対抗するため，攻撃者の行動観測を通してサイバー攻撃活動分析をすべく，攻撃者のアトリビューションに着目した動的活動観測を進めている。



注：略語説明　SQL（Structured Query Language）

図3｜セキュリティインシデントとサイバー攻撃の変遷

セキュリティインシデントとサイバー攻撃の変化により，異なる組織のCSIRTどうしの連携も，手段を共有することで問題解決を図るアプローチから侵害活動を鳥瞰（かん）することで問題解決を図るアプローチへと変わりつつある。

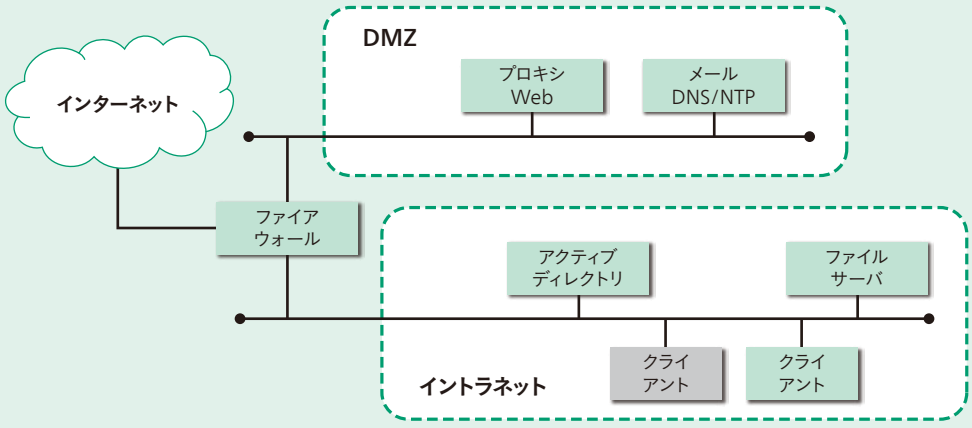
4.　攻撃者のアトリビューションに着目した動的活動観測

4.1　目的

サイバー攻撃の分野において，アトリビューションとは，攻撃者や攻撃仲介者の同一性や場所の特定を意味する[4]。これまで，マルウェア検体の静的／動的解析は，マルウェアの挙動に着目したものであった。例えば，C2サーバ接続，情報窃取，バックドアなどの機能の存在や挙動把握に重点が置かれており，これら機能のいずれを使ったのかなど，攻撃者の行動という視点で把握や解析されることは少なかった。多くの場合，攻撃者の行動＝マルウェアの挙動という想定の下，静的／動的解析によって対応してきた。しかし，組織内ネットワークへの侵害活動である標的型攻撃のサイバー攻撃活動分析においては，サイバー攻撃活動の構造化でも示されているとおり，攻撃者の存在を意識する必要がある。そこで，動的活動観測では，アトリビューションの一部として，マルウェアの挙動に加えて，どのような操作をしたのか，どのようなファイルにアクセスしたのかなど攻撃者の行動と組み合わせていくことで，攻撃者行動視点で脅威の特徴づけを試みている。

4.2　動的活動観測環境

動的活動観測では，組織内ネットワーク自身を模擬した観測環境を構築している（**図4**参照）。この環境は，組織



注：略語説明　DMZ（Demilitarized Zone），DNS（Domain Name Server），NTP（Network Time Protocol）

図4｜動的活動観測環境の概要図

動的活動観測環境は，組織内ネットワークを模擬した環境を保有し，攻撃者が組織内ネットワークで試みるサイバー攻撃活動を観測するためのシステムとなっている。

内ネットワークのパソコンにおいてマルウェア感染が発生した以降，すなわち，進行段階モデルの攻撃以降を対象に，実インターネット上の攻撃者が組織内ネットワークで試みるサイバー攻撃活動を観測するシステムとなっている。クライアントは，標的型攻撃メールに添付されたマルウェア検体を実行するパソコンであり，プロキシ経由／プロキシ経由なしのいずれかの形態で，実インターネットへのアクセスが可能である。

4.3　観測事例

観測事例として，2014年9月中旬ごろに流布した医療費通知の偽装メールでの観測事例を紹介する。医療費通知の偽装メールは，健康保険組合などからの医療費通知メールを偽装し，ユーザーのパソコンを遠隔操作可能な不正プログラム（検出名：Emdivi）に感染させようとする攻撃であった。

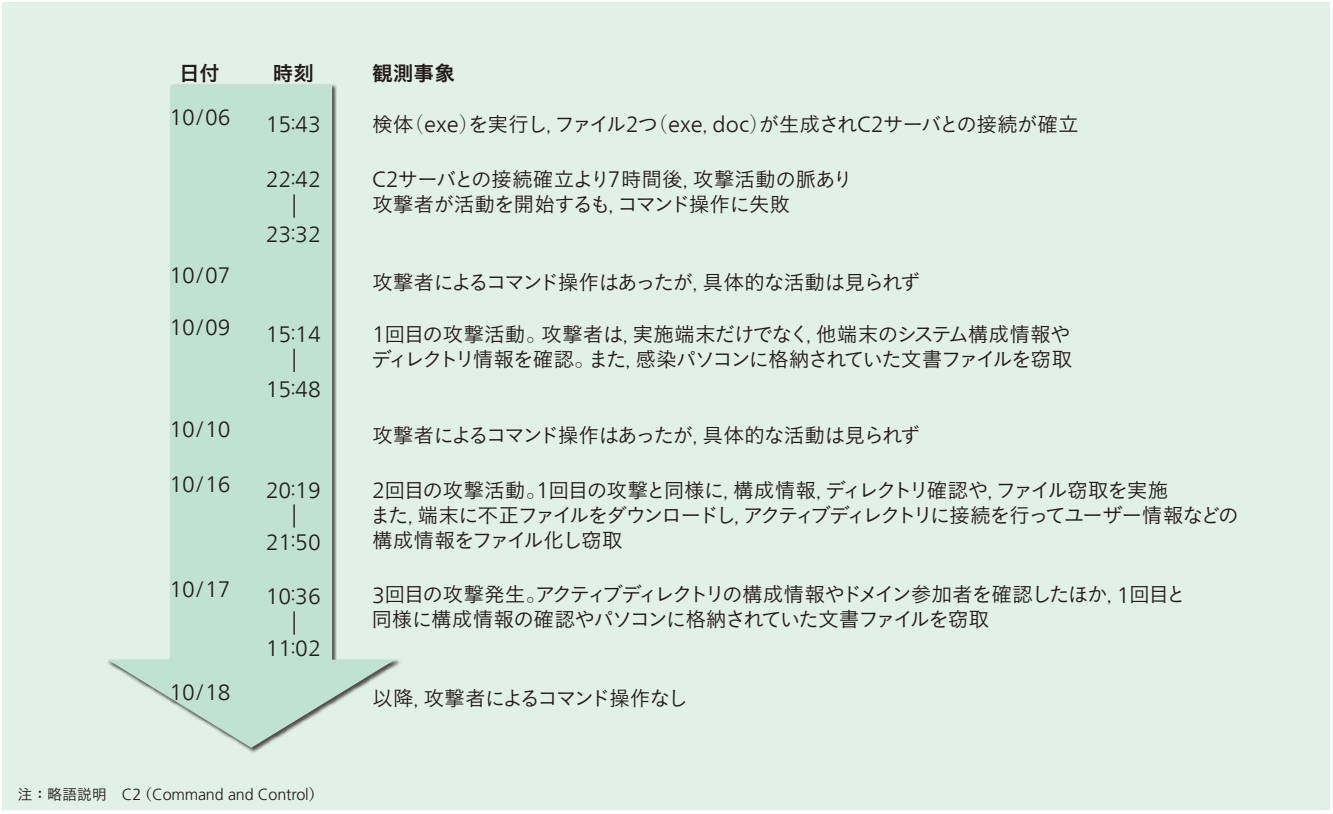
医療費通知メールの添付ファイルには，文書アイコンに偽装された実行形式の不正プログラムが含まれていた。動的観測環境では，パソコンが不正プログラムに感染した後，約7時間すると攻撃者が観測環境を訪れ侵害活動を開始し，活動を停止するまでの12日間のあいだに，3回，計3時間ほどの活動を通して，システム構成やディレクトリ情報の確認，感染パソコンなどからのファイルの窃取などを行う様子を確認している（**図5**参照）。

このような動的活動観測は，試行段階のレベルではあるが，攻撃者の行動，サイバー攻撃活動を明らかにしていくことで，サイバー攻撃活動分析や標的型攻撃対策につながると考えている。

4.4　マルウェア対策研究人材育成ワークショップとの連携

動的活動観測には，もう1つの果たすべき目的がある。それは，異なる組織のCSIRTどうしがつながり，情報共有を通して侵害活動を鳥瞰することで問題解決を図るためのアプローチを整備していくことである。

この目的を達成するために，動的活動観測で得られた観測事例の通信観測データ，プロセス観測データを研究用データセットBOS（Behavior Observable System）として，一般社団法人情報処理学会コンピュータセキュリティ研究会に設置されたマルウェア対策研究人材育成ワークショップ［MWS（anti-Malware engineering Work Shop）］組織委員会を介して情報共有を図っている。MWSは，研究用データセットの提供，研究成果の共有ならびに切磋琢磨する環境の提供を通して，マルウェアに関する知識を備えた研究者，技術者，実務者を育成するための産学官連携のコミュニティをベースとした活動フレームワークであり，アプローチの整備を試行する場として活用している。



注：略語説明　C2（Command and Control）

図5｜動的活動観測環境での観測事例

攻撃者は，活動を停止するまでの12日間のあいだに，3回，計3時間ほどの活動を通して，システム構成やディレクトリ情報の確認，感染パソコンなどからのファイルの窃取などを行った。

5. おわりに

既知の脅威による被害は継続し，その一方で，新たなサイバー攻撃により脅威が生み出され，被害が発生している。HIRTでは，このような状況変化を捉え，「次の脅威をキャッチアップする」過程の中で，早期に対策展開を図っていく。

特に，対策展開においては，異なる組織のCSIRTどうしがつながり，情報共有を通して侵害活動を鳥瞰し問題解決を図っていく活動を先導していく。具体的には，進行段階に着目したモデル化，サイバー攻撃活動の構造化で想定している，観測事象（Observables：攻撃によって観測された事象）と検知指標（Indicators：攻撃を検知するための指標）を用いた組織間連携型の情報共有によるサイバー攻撃への対処である。

さらに，MWSなど次世代のCSIRTコミュニティにつながる学術系人材育成活動との連携を通して，安心，安全な社会インフラの実現に寄与していく。

謝辞

動的活動観測は総務省実証事業「サイバー攻撃解析・防御モデル実践演習の実証実験」の請負で実施したものである。動的活動観測を進めるにあたって有益な助言と協力をいただいた関係各位に深く感謝申し上げる。

参考文献など

1) 独立行政法人情報処理推進機構：「『高度標的型攻撃』対策に向けたシステム設計ガイド」の概要（2014.9），
https://www.ipa.go.jp/security/vuln/newattack.html
2) Eric M. Hutchins, et al.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains（ICIW2011）（2011.3）
3) STIX，
http://stix.mitre.org/
4) David A. Wheeler, et al.: Techniques for Cyber Attack Attribution（Institute for Defense Analysis, IDA Paper）（2003.10）
5) マルウェア対策研究人材育成ワークショップ2015（MWS2015），
http://www.iwsec.org/mws/2015/

執筆者紹介

寺田 真敏
日立製作所 研究開発グループ システムイノベーションセンタ所属，
情報・通信システム社 クラウドサービス事業部
セキュリティ先端技術本部 HIRTセンタ 兼務
現在，インシデントオペレーションに向けたCSIRT組織間連携活動に従事
博士（工学）
情報処理学会会員

藤原 将志
日立製作所 情報・通信システム社 クラウドサービス事業部
セキュリティ先端技術本部 HIRTセンタ 所属
現在，製品・サービスの脆弱性対策ならびにインシデント対応に従事

沼田 亜希子
日立製作所 情報・通信システム社 クラウドサービス事業部
セキュリティ先端技術本部 HIRTセンタ 所属
現在，脆弱性対策・インシデント対応における技術継承に従事

西川 由佳理
日立製作所 情報・通信システム社 クラウドサービス事業部
セキュリティ先端技術本部 HIRTセンタ 所属
現在，情報共有を通じたCSIRT活動の推進に従事

久芳 瑠衣子
日立製作所 情報・通信システム社 クラウドサービス事業部
セキュリティ先端技術本部 HIRTセンタ 所属
現在，情報共有への脅威情報構造化記述形式STIX適用業務に従事