feature article

セキュリティインシデントへの日立グループの取り組み

HIRT（Hitachi Incident Response Team）活動

Activity for Computer Security Incident of Hitachi Group

寺田 真敏 Masato Terada
梅木 久志 Hisashi Umeki
藤原 将志 Masashi Fujiwara
石淵 一三 Kazumi Ishibuchi

**インターネットが基本的な社会インフラとなるに伴い，
セキュリティインシデントの発生頻度は増え，その影響はより深刻化している。
日立インシデントレスポンスチーム（HIRT）は，日立グループの情報セキュリティ活動を支援する組織である。
セキュリティインシデントの発生を予防し，
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，
顧客や社会の安全・安心なネットワーク環境の実現に寄与していく。**

1. はじめに

ワーム，フィッシング，スパイウェア，ボット，標的型攻撃など数多くのセキュリティ用語が生まれた状況からも，情報システムが直面する脅威は格段に広がり，侵害活動やその被害の形態も様相を変えてきていることが感じとれる。実際，2000年ごろから認知されはじめたWebサイトの改ざんは，当初はページの書き換えにとどまっていたが，2003年ごろからフィッシングを目的とした偽ページへの置き換えが目立つようになり，さらに2007年以降はマルウェア（悪質なソフトウェア）蔵置サイトに誘導する悪質なスクリプトプログラムの埋め込みも見られるようになった。

情報システムは新たな脅威に直面しており，日々の脆（ぜい）弱性対策やインシデント対応を通して，脅威に打ち勝っていく必要がある。「HIRT（Hitachi Incident Response Team）」は，日立グループ全体で新たな脅威によって発生しうるインシデントを予防し，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，顧客や社会の安全・安心なネットワーク環境の実現に寄与するための組織である。

ここでは，HIRTの活動モデルならびにHIRTセンタが推進している活動について述べる。

2. HIRTの概要

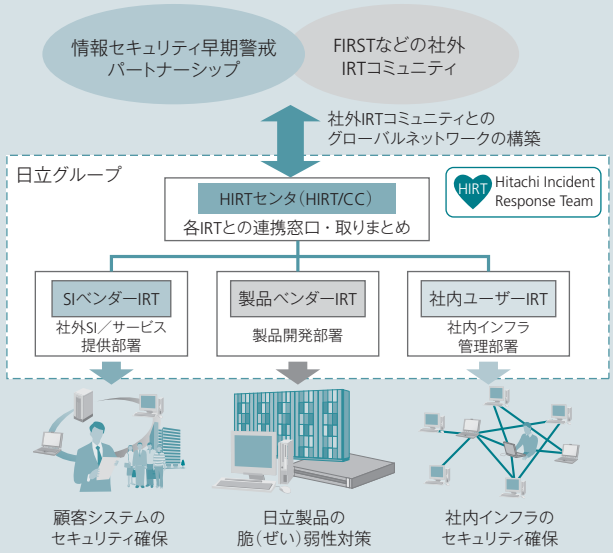
2.1 インシデントレスポンスチーム

コンピュータセキュリティインシデント（以下，インシデントと記す。）とは，コンピュータセキュリティに関係する人為的事象で，不正アクセス，サービス妨害行為，データの破壊などの行為（事象）を示す。

米国では，1988年12月のインターネットワーム（Morris Worm）の出現を契機に，コンピュータの脆弱性に対する脅威への認識が高まった。特に，インシデントの原因や対応方法に関する情報共有の重要性が認識され，緊急対応チームCERT/CC（Computer Emergency Response Team/Coordination Center）の設立に至った。また，1989年10月に出現したWankワームは，組織，国にまたがったコミュニケーションの欠落が適切な対応の推進を妨げたという教訓を残し，緊急対応チームの組織間ならびに国際間連携を目的としたFIRST（Forum of Incident Response and Security Teams）の組織化につながった。

国内では，1996年にJPCERT/CC（Japan Computer Emergency Response Team/Coordination Center）の活動開始を契機に，インシデント発生時には手順に沿って事後対処する「インシデントレスポンス」という考え方が普及した。さらに，2001年から2004年にかけて流布したCode Red，Slammer，Blasterなどのネットワーク型ワームの対処を通じて，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抑える「インシデントオペレーション」という考え方が生まれた。

インシデントレスポンスチームは，組織間ならびに国際間連携による問題解決のために，「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」という基本的な能力を持ち，「インシデントレスポンス」，「インシデ



分類	役割
HIRT/CC	該当部署：HIRTセンタ FIRST, JPCERT/CC, CERT/CCなどの社外IRT組織との連携，SIベンダー・製品ベンダー・社内ユーザーIRT間の連携を通して脆弱性対策とインシデント対応活動を推進する。
SIベンダーIRT	該当部署：SI・サービス提供部署 公開された脆弱性について，社内システムと同様に顧客システムのセキュリティを確保するなど，顧客システムを対象とした脆弱性対策とインシデント対応活動の推進を支援する。
製品ベンダーIRT	該当部署：製品開発部署 公開された脆弱性について影響有無の調査を迅速に行い，該当する問題については，修正プログラムを提供するなど，日立製品の脆弱性対策の推進を支援する。
社内ユーザーIRT	該当部署：社内インフラ提供部署 日立グループサイトが侵害活動の基点とならないよう脆弱性対策とインシデント対応活動の推進を支援する。

注：略語説明　HIRT/CC（Hitachi Incident Response Team/Coordination Center），IRT（Incident Response Team），FIRST（Forum of Incident Response and Security Teams），JPCERT/CC（Japan Computer Emergency Response Team/Coordination Center），CERT/CC（Computer Emergency Response Team/Coordination Center），SI（System Integration）

図1　脆弱性対策，インシデント対応活動を支える四つのIRT
脆弱性対策，インシデント対応活動を推進するため，四つのIRT構成による組織編成モデルを採用している。

ントオペレーション」を通して，インシデントの予防と解決を先導するチームである。

次に，日立グループで実現しているインシデントレスポンスチームの活動モデルについて述べる。

2.2　HIRTの活動モデル

インシデントレスポンスチームとしてのHIRTの役割は，「脆弱性対策：情報セキュリティに関する脆弱性を除去するための活動」と「インシデント対応：発生している侵害行為を回避ならびに解決するための活動」を通じて，日立グループの情報セキュリティ活動を支援していくことである。さらに，「次の脅威をキャッチアップする」過程の中で早期に対策の展開を図ることで，安全・安心なインターネット社会の実現にも寄与することにある。

HIRTでは，脆弱性対策とインシデント対応とを推進するために，四つのIRT（Incident Response Team）という活動モデルを採用している（**図1**参照）。

四つのIRTとは，(1) 日立グループが，情報システム関連製品を開発する側面（製品ベンダーIRT），(2) その製品を用いたシステムの構築やサービスを提供する側面〔SI（System Integration）ベンダーIRT〕，(3) インターネットユーザーとして自身の企業情報システムを運用管理していく側面（社内ユーザーIRT）の三つとともに，(4) これらのIRT間の調整業務を行うHIRT/CCを設けることにより，各IRTの役割を明確にしつつ，IRT間の連携を図った効率的かつ効果的なセキュリティ対策活動を推進できると考えたモデルである。なお，HIRTという名称は，広義の意味では日立グループ全体のインシデントオペレーション活動を示し，狭義の意味では，HIRT/CC（HIRTセンタ）を示している。

また，HIRTセンタの組織編成上の特徴は，縦軸の組織と横軸のコミュニティが連携するモデルを採用しているところにある。具体的には，専属者と兼務者から構成されたバーチャルな組織体制をとることで，フラットかつ横断的な対応体制と機能分散による調整機能役を実現している。このような組織編成は，情報システムの構成品が多岐にわたっていることから，セキュリティ問題解決のためには，各部署の責務推進と部署間の協力が必要であるとの考えに基づいている。

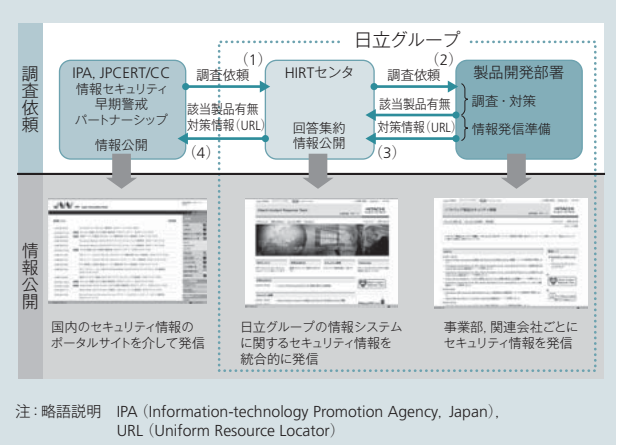
3.　HIRTセンタが推進する活動

HIRTセンタの主な活動には，組織内IRT活動として，制度面を先導する情報セキュリティ統括部門と品質保証部門との協力による制度・技術の両面での情報セキュリティ対策の推進，各事業部・グループ会社への脆弱性対策ならびにインシデント対応の支援がある。

また，日立グループの対外的なインシデントレスポンスチーム窓口として，組織間IRT連携による情報セキュリティ対策の促進がある。

3.1　組織内IRT活動

組織内IRT活動では，セキュリティ情報の収集や分析を通して得られたノウハウを注意喚起やアドバイザリとして発行し，また，各種ガイドラインや支援ツールの形で製



注：略語説明 IPA（Information-technology Promotion Agency, Japan），URL（Uniform Resource Locator）

図2 セキュリティ情報の収集～調査分析～展開のための情報利活用基盤の整備

日立グループの製品・サービスのセキュリティ問題に関する情報を統合的にインターネット利用者に提供する。

品／サービス開発プロセスにフィードバックする。

(1) セキュリティ情報の収集・調査分析・展開

情報セキュリティ早期警戒パートナーシップの推進を通じた脆弱性対策ならびにインシデント対応に関する情報やノウハウを水平展開する。

(2) 情報利活用基盤の整備

統合Webサイトを活用したセキュリティ情報発信など，セキュリティ情報の収集～調査分析～展開のための情報利活用基盤を確立する（**図2**参照）。

(3) 製品・サービスのセキュリティ技術の向上

Webアプリケーションセキュリティの強化，情報家電・組込み系製品・制御系製品におけるセキュリティ施策の具体化，開発・管理プロセスの整備（開発～検査～運用管理のための各種ガイドラインなど）を推進する。

(4) 研究活動基盤の整備

「次の脅威のキャッチアップ」と早期の対策展開を図るための技術開発に向け，各研究所との共同研究体制を整備する。

3.2 組織間IRT活動

予兆や被害を隠蔽（ぺい）化する侵害活動の増加に合わせ，複数のインシデントレスポンスチームどうしが協調して新たな脅威に立ち向かうための組織間連携，互いのインシデント対応活動の改善に寄与できる協力関係の構築を推進している。

(1) IRT活動の国内連携の強化

JVN（Japan Vulnerability Notes）ならびにJVNRSS（JVN RDF Site Summary）を用いた情報利活用基盤の整備[1)]，情報セキュリティ早期警戒パートナーシップに基づく脆弱性対策活動の推進，日本シーサート協議会を通じた組織間IRTの連携がある。

(2) IRT活動の海外連携の強化

海外IRT組織・海外製品ベンダーIRTとの連携体制の整備，英国WARP（Warning, Advice and Reporting Point）活動の推進，CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子），CVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）など脆弱性関連の標準化への対応がある。

(3) 研究活動基盤の整備

学術組織との共同研究，マルウェア対策研究人材育成ワークショップなど学術系研究活動への参画を通して，専門知識を備えた研究者や実務者を育成する。

次に，具体的な組織内IRT活動，組織間IRT活動として，2008年の活動を紹介する。

4. 2008年の活動トピックス

(1) 製品・サービスセキュリティ活動の整備

脆弱性対策ならびに，インシデント対応などの活動を通じて得られたノウハウを製品・サービス開発プロセスにフィードバックするため，各プロセスに合ったHIRT支援活動の体系化を開始した。支援活動が先行しているWebアプリケーションのセキュリティについては，演習型HIRTオープンミーティングを取り込んだ体系化を進めている（**図3**参照）。

組込み系製品については，セキュリティを考慮した製品開発プロセスを整備していくために，セキュリティ評価に対する進め方やツール活用方法を対象とした支援活動を開始した。特に，セキュリティ検査に利用するツールについては，SIP（Session Initiation Protocol）など製品個別のセキュリティ検査ツールだけではなく，独立行政法人情報処理推進機構から提供されている「TCP/IP（Transmission Control Protocol/Internet Protocol）にかかわる既知の脆弱性検証ツール」などを活用することで，すでに公表されている脆弱性の再発を防ぐとともに，日立グループ内における情報家電・組込み系製品・制御系製品におけるセキュリティ施策の具体化を進めた。

(2) 演習型HIRTオープンミーティングの定着化

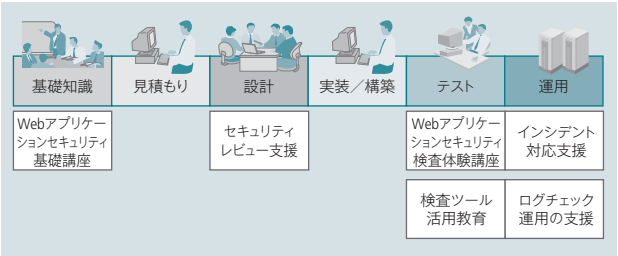


図3 HIRT支援活動の体系化

脆弱性対策ならびに，インシデント対応などの活動を通じて得られたノウハウを製品開発プロセスにフィードバックする。

HIRTオープンミーティングは，信頼関係に基づくHIRTコミュニティの拡大とともに，脆弱性対策・インシデント対応のノウハウを展開する活動である。2008年は，2007年から開始したWebアプリケーション開発を対象とした演習型HIRTオープンミーティングの定着化をめざし，計9回（参加者：約200名）のミーティングを開催した（**図4**参照）。

(3) DNSキャッシュポイズニングの対策支援

インターネット上の多くのネットワークサービスがDNS（Domain Name System）を前提としているにもかかわらず，DNSの動作や関連ツールの情報はあまり知られていない。このため，DNSの動作やツールの使い方に踏み込んだ「DNSの役割と関連ツールの使い方」資料を作成し，HIRTオープンミーティングを通じて展開した。また，国内のDNSキャッシュポイズニング対策の推進に役立ててもらうため，2009年1月に独立行政法人情報処理推進機構から発行された「DNSキャッシュポイズニング対策」の資料素材として提供した[2)]。

(4) IRTコミュニティとの組織間連携の強化

組織間連携では，NTT-CERT（NTT Computer Security Incident Response and Readiness Coordination Team）とのIRT活動改善のための定期的な情報交換会に加え，マルウェア捕獲システムの相互利用とその調査結果について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て報告した。

継続的に発生しているファイル交換ソフトウェアを介した情報漏洩（えい）については，2007年に引き続き，システム開発研究所，「安心・安全インターネット推進協議会P2P研究会」の協力を得て，漏洩要因となるファイル交換ネットワーク環境のマルウェアの流布状況について調査し，その調査結果をWebサイトにて公開した。

新たな組織間連携の取り組みとして，標的型攻撃の実態を明らかにすべく，情報処理学会コンピュータセキュリティ研究会が主催するシンポジウムのCFP（Call for Papers）を騙（かた）ったウイルス添付メールの検体を関連組織に提供するとともに，ウイルス添付メール受信を安全に体験可能な仮想体験デモを提供した。

タイムテーブル	
(1) Webアプリケーションセキュリティの動向	(10分)
(2) 日立グループでの取り組み状況／演習の目的	(20分)
(3) Webアプリケーションの脆弱性の解説	(60分)
(4) 脆弱性検査演習（各自演習）	(70分)
(5) 脆弱性報告書の作成（各自演習）	(30分)
(6) Webアプリケーションセキュリティガイドおよび機能要件チェックリストの紹介	(30分)
(7) SQLインジェクションログチェックツール紹介	(10分)

注：略語説明　SQL（Structured Query Language）

図4　演習型HIRTオープンミーティング
演習を通して，技術者の育成と信頼関係に基づくHIRTコミュニティを普及させる。

5. おわりに

ここでは，HIRTの活動モデルならびにHIRTセンタが推進している活動について述べた。

ここ数年間のインシデントの変遷を見る限り，短いサイクルで新たな侵害活動が生まれ，一度流布した侵害活動は決してなくならず，さらに侵害活動を通して攻撃技術が継承されていることがわかる。このような状況下においては，各IRTが保有する情報収集・観測機能，状況分析機能ならびに対処機能を連携させて，問題事象の把握と解決を図っていくことが必要である。

HIRTでは，今後とも，情報セキュリティ早期警戒パートナーシップを活用した脆弱性対策の推進，複数のIRTどうしが協調して新たな脅威に立ち向かうための組織間連携を通して，安全・安心なインターネット社会の実現に寄与していく。

参考文献など

1) 寺田，外：脆弱性対策情報データベースJVNの提案，情報処理学会論文誌，Vol.46，No.5，p.1256～1265（2005.5）
2) 独立行政法人情報処理推進機構：DNS（Domain Name System）の役割と関連ツールの使い方，http://www.ipa.go.jp/security/vuln/DNS_security.html

執筆者紹介

寺田 真敏
1986年日立製作所入社，情報・通信システム社 情報・通信グループ セキュリティ・トレーサビリティ事業部 HIRTセンタ 所属 システム開発研究所 兼務
現在，インシデントオペレーション関連技術の研究開発，IRT活動の連携に従事
博士（工学）
情報処理学会会員

梅木 久志
1989年日立製作所入社，情報・通信システム社 情報・通信グループ セキュリティ・トレーサビリティ事業部 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情報利活用基盤の整備に従事

藤原 将志
2006年日立製作所入社，情報・通信システム社 情報・通信グループ セキュリティ・トレーサビリティ事業部 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

石淵 一三
1994年日立製作所入社，情報・通信システム社 情報・通信グループ セキュリティ・トレーサビリティ事業部 HIRTセンタ 所属 ソフトウェア事業部 兼務
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