2009 年 HIRT 活動報告
HIRT: Annual Report 2009

Hitachi Incident Response Team (HIRT)
http://www.hitachi.co.jp/hirt/

〒212-8567 神奈川県川崎市幸区鹿島田 890
Kashimada 890, Saiwai, Kawasaki, Kanagawa, 212-8567 Japan

1 はじめに

2005 年以降の情報漏えい被害を抑える情報保証対策が進む中，その影に隠れていたサイバー攻撃の技術変遷は著しい．この 10 年間のサイバー攻撃の変遷を見る限り，短いサイクルで新たな攻撃活動が生まれ，一度確立した攻撃活動は決してなくなることはない．攻撃活動を通した技術の継承と徹底したカスタマイズ化によって，攻撃活動の全容が見えないという状況が作り出されている．

特に，2008 年以降，サイバー攻撃の活動基点が怪しいから普通(怪しくない)に切り替わった．図 1は，日立に届いたコンピュータセキュリティシンポジウム 2008(CSS2008)の募集要項を装ったマルウェア添付の標的型メールである．受信した電子メールの本文に記載されている内容は，募集要項から切り貼りして作成された文面であり，怪しさをまったく感じさせない．図 2は，ホームページ誘導型マルウェアであるガンブラーが使用した攻撃サイトへの誘導方法である．正規ウェブサイトは，誘導コードを蔵置されてしまった場合，感染活動に加担してしまう．ユーザは，正規ウェブサイトにアクセスしているにも関わらず，蔵置された誘導コードにより，一連の攻撃活動(攻撃ウェブサイトへのアクセス，マルウェアのダウンロード，脆弱性を悪用したマルウェアへの感染まで)の渦中に巻き込まれてしまうことになる．

このようなサイバー攻撃によって発生するインシデントの変化は，対処側の考え方にも反映されている．1988 年のインターネットワームの出現を契機に，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，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』という考え方が確立した．2001 年から 2003 年にかけ流布したネットワーク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低減するために実施する一連のセキュリティ対策活動である『インシデントオペレーション』という考え方が生まれた．2006 年以降は，組織同志が相互に連携してインシデントに伴う被害を予測ならびに予防する組織相互連携オペレーションという新たな対処シナリオが検討されている．

さらに，インシデントの変化は，CSIRT(Computer Security Incident Response Team)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に加えて，サイバー攻撃の技術変遷への追従など，経験値を活かした次のような役割も求めている．

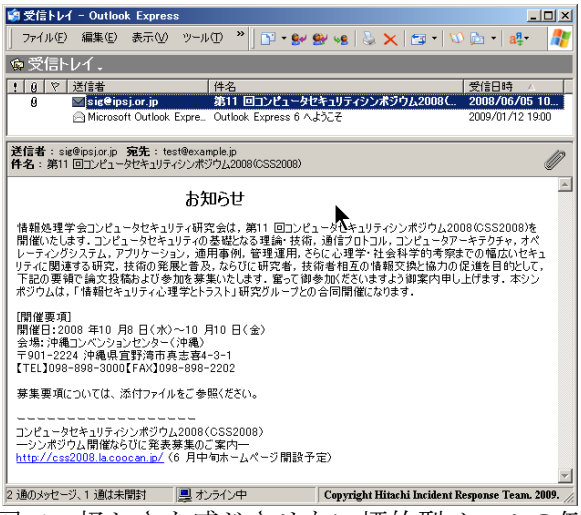


図 1：怪しさを感じさせない標的型メールの例

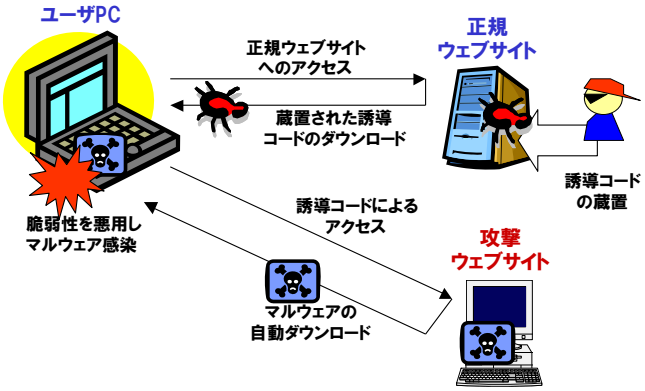


図 2：正規ウェブサイト感染活動への加担の例

『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．

HIRT(Hitachi Incident Response Team)は，これら能力ならびに役割を持った組織として，製品ならびにサービスの脆弱性対策，マルウェア被害や情報漏えいなどのインシデント対応を先導すると共に，セキュリティ分野での日立ブランドを向上するための活動，仕組みならびに体制を整備する日立グループのCSIRT統一窓口組織としての責務を負っている．

本稿では，2009年のHIRT活動の報告として，2009年の脆弱性と脅威の概況とHIRTの活動トピックスについて報告する．

2　2009年の活動概要

本章では，2009年のHIRTの活動トピックスを中心に報告する．

2.1　脅威と脆弱性の概況

(1) 脅威の概況

2009年は，USBメモリ型マルウェアの一種であるConficker(コンフッカー)やホームページ誘導型マルウェアの一種であるGumblar(ガンブラー)の流布活動にみられる通り，ウェブサイトを活動基盤とした受動型(誘導型)攻撃が一般化した．一般化と共に，ウェブサイトは，侵入したマルウェアが他の機能を持つプログラム群を入手するためのダウンロードサイトとしてだけではなく，感染拡大を誘発する窓口としても機能するようになった．特に，ホームページ誘導を用いたマルウェア感染活動に至っては，アカウント盗聴による感染拡大サイクルを組み込んだ攻撃活動基盤としてシステム化されつつある．

- **Conficker(コンフッカー)**

Conficker は，2008年11月頃からWindowsのServerサービスの脆弱性(MS08-067)を悪用するワームとして出現した．2008年12月にはいってから，USBメモリを介して感染する機能が追加されたことから，隔離されたネットワークにおいても，USBメモリという物理的な媒介手段を介して感染が広がった．USBメモリ型マルウェアは，2008年から流布しているが，2009年にはいってからは感染被害の報告件数が減少している(図 3)[1]．しかし，USBメモリ型マルウェアの一種であるConfickerについては，国内での感染活動の検知数は減少しているものの(図 4)[2]，Conficker Work Groupの観測によれば，ワールドワイドの感染台数はIPアドレスベースで約600万台と報告されている[3].

- **Gumblar(ガンブラー)**

Gumblarは，『いつも見ているホームページ』から攻撃サイトにアクセス誘導し，マルウェア感染被害を発生させるホームページ誘導型ウイルスの俗称である．この名前は，2009年5月に利用された攻撃サイトの名称が「gumblar.cn」であったことに由来する．Gumblarの感染活動の概要は次の通りである(図 6).

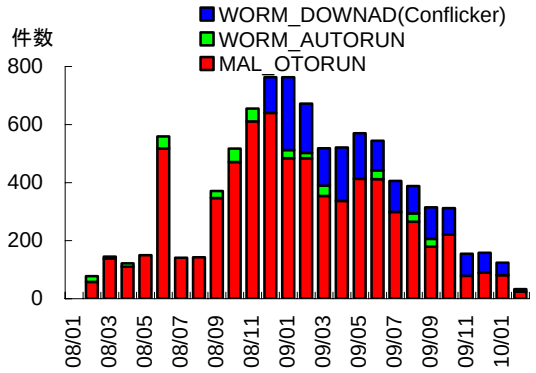


図 3：USBメモリ型マルウェアの感染数(/月)
(出典：トレンドマイクロ)

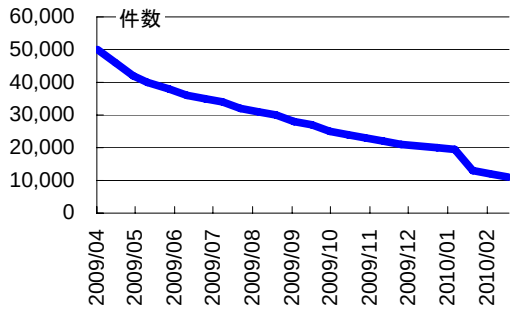


図 4：Conficker ワーム検知数(/日)の推移
(出典：IBM 東京 SOC)

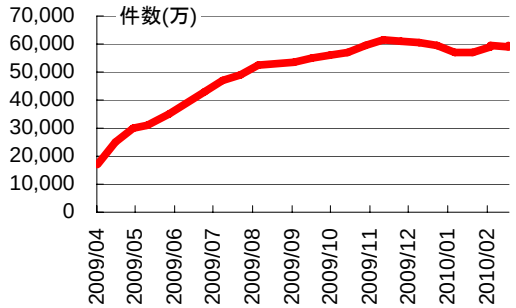
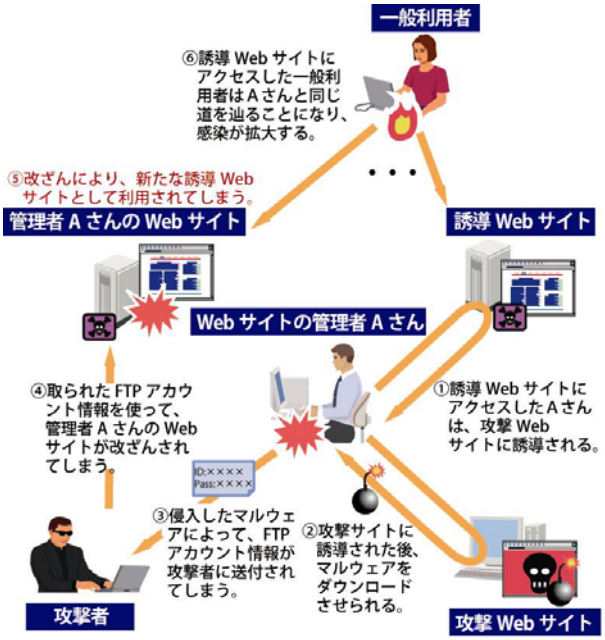


図 5：ConfickerA+B 感染台数(/日)の推移
(出典：Conficker Work Group)



①	誘導サイト：アクセスした利用者 A さんを，マルウェア感染を仕掛ける攻撃サイトに誘導する．
②	攻撃サイト：プログラムの脆弱性を悪用して A さんのパソコンを Gumblar に感染させる．
③	Gumblar：FTP アカウント情報を攻撃者に送付する．
④	攻撃者：FTP アカウント情報を使って，A さんの管理するウェブサイトに侵入する．
⑤	攻撃者：ホームページに不正なスクリプトを埋め込み，新たな誘導 Web サイトを作成する．
⑥	利用者：これら誘導 Web サイトにアクセスした一般利用者は A さんと同じ道を辿ることになり，感染活動がさらに拡大することになる．

図 6：マルウェアへの感染から
ウェブサイトの改ざんまでの流れ

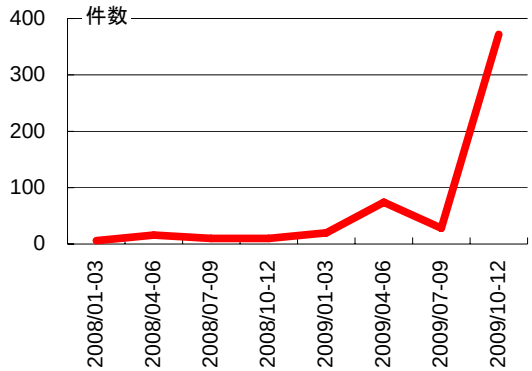


図 7：Web サイト改ざんの届出件数の推移
(出典：JPCERT/CC)

Gumblar の被害状況としては，2009 年 4 月～6 月に，国内ウェブサイトに不正なスクリプトを埋め込まれるホームページ改ざんが多数発生した．10 月～11 月には，亜種に感染したパソコンにおいて，電源を入れても正常に起動せず，画面が真っ暗になるなどの症状が発生した．12 月には，国内の大手ウェブサイトにおいて，不正なスクリプトを埋め込まれるホームページ改ざんが多数発生した(図 7)[4].

(2) 脆弱性の概況

脆弱性については図 8に示す通り，米 NIST NVD(National Vulnerability Database)に登録された 2009 年の脆弱性の総件数は 5,733 件で横ばい傾向にある．しかし，その中でウェブアプリケーション系ソフトウェア製品の脆弱性(クロスサイト・スクリプティング(XSS)，SQL インジェクション，ディレクトリ・トラバーサル，クロスサイト・リクエスト・フォージェリ(CSRF))が約 38%，2,202 件となっている(図 9)[5]．また，IPA に報告された稼動中ウェブサイトの脆弱性のうち，約 5 割がクロスサイト・スクリプティング(XSS)，SQL インジェクションによって占められており，これら脆弱性の報告件数も増加傾向にある(図 10)[6].

ウェブサイトを活動基盤とした受動型(誘導型)攻撃が一般化していることから，今後も，ウェブサイトが侵害活動の基点にならないよう，ウェブアプリケーション系ソフトウェア製品の開発ならびに，ウェブサイト運用の両面から脆弱性対策の推進が必要となっている．

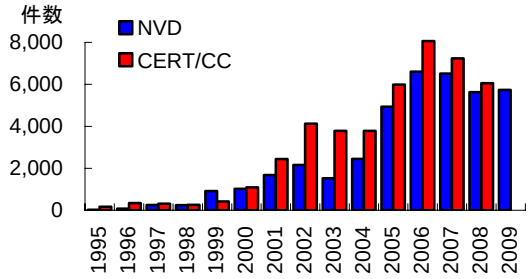


図 8：脆弱性報告件数の推移(出典：NIST NVD)

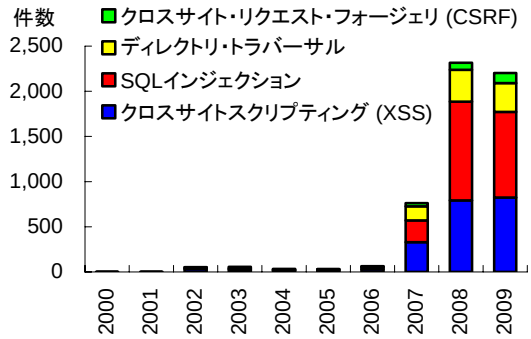


図 9：ウェブ系ソフトウェア製品の
脆弱性報告件数の推移(出典：NIST NVD)

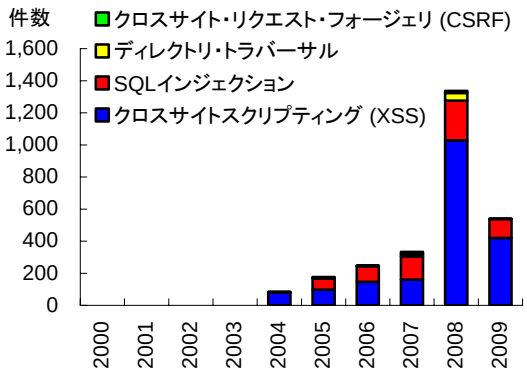


図 10：ウェブサイトの脆弱性報告件数の推移
(出典：IPA，JPCERT/CC)

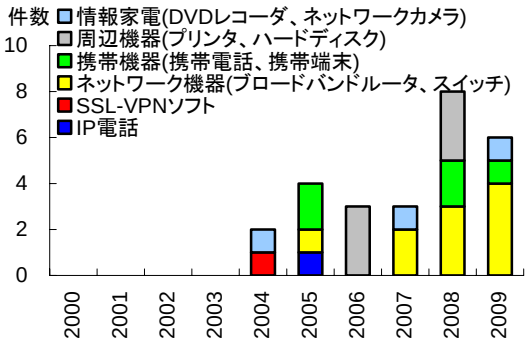


図 11：組込みソフトウェア製品の脆弱性報告件数の推移(出典：IPA，JPCERT/CC)

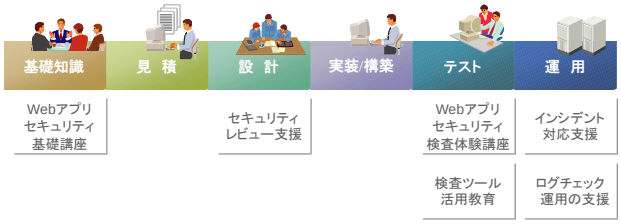


図 12：HIRT 支援活動の体系化
(ウェブアプリケーションのセキュリティ)

また，IPA に報告された組込み機器に関する脆弱性報告件数も少しずつ増加している傾向にあり，製品の開発段階から脆弱性を作り込まないよう脆弱性対策の一層の推進が必要となってきている(図 11).

2.2 HIRT の活動トピックス

本節では，2009 年の活動トピックについて述べる．

(1) 製品／サービスセキュリティ活動の開始

脆弱性対策とインシデント対応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ため，プロセス毎の HIRT 支援活動を開始した．支援活動が先行しているウェブ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(計 11 回，受講者：約 170 人)，セキュリティレビュー支援を実施した(図 12)．また，ウェブサイトの公開には，セキュリティ対策が常識と言われている現在でも，依然として，ウェブサイトの脆弱性を狙った事件や事故が後をたたない状況が続いている。このため，2009 年 7 月，(独)産業技術総合研究所の高木浩光氏を講師として招き，ウェブサイト／ウェブアプリケーションのセキュリティを確保するために考慮すべき視点についての講演会を開催した．

(2) セキュリティ技術者育成研修プログラムの実施

CSIRT 活動を活かしたセキュリティ技術者育成の一環として，グループ会社より研修生を受け入れ，ウェブシステムのセキュリティ対策を中心とした半年間の研修を実施した．また，研修生には，研修終了後，派遣元の開発者を対象に，ウェブシステムのセキュアな設計を題材とした教育の企画ならびに実施に協力してもらった．

(3) P2P ファイル交換ソフト環境で流通するマルウェアに関する調査

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えいについては，社外との組織間連携が必要であると考え，2008 年に引き続き，システム開発研究所と共に，総務省委託研究『ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発』に参画する安心・安全インターネット推進協議会 P2P 研究会の協力を得て調査を実施した[7][8]．特に，P2P ファイル交換ネットワーク環境 Winny に流通するマルウェアについては，依然として Antinny 型の情報漏えいを引き起こす既知マルウェアが多く流通していること，その多くが安全なコンテンツに見せかけた「アイコン偽装」を行い，巧妙にマルウェアを実行させる偽装を行っていることから，引き続き十分な注意が必要である．

- マルウェアは 20～30 ファイルに 1 つ(図 13)
- 流通量が多いアーカイブファイル(zip，lzh，rar)に限定すると，マルウェアは 5～7 ファイルに 1 つ
- 既知マルウェアの 7 割が情報漏えいを引き起こす Antinny とその亜種
- マルウェアのうち，フォルダなどの安全なコンテンツに見せかけたアイコン偽装を行っているマルウェアは約 9 割，さらに約 3 割がファイル名偽装

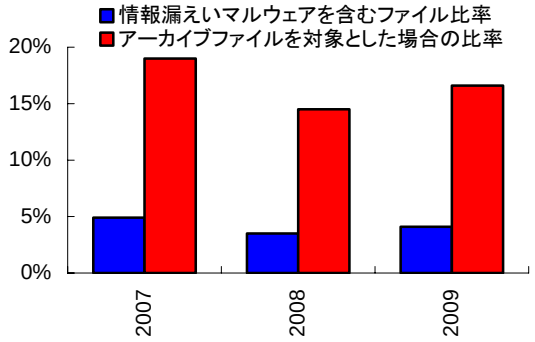


図 13 : Winny に流通する情報漏えいを引き起こすマルウェアの推移

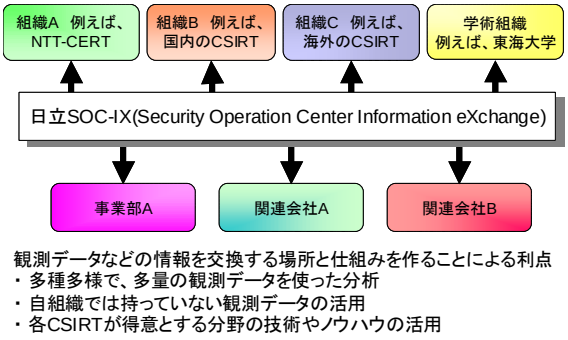


図 14 : 日立 SOC-IX の概念図

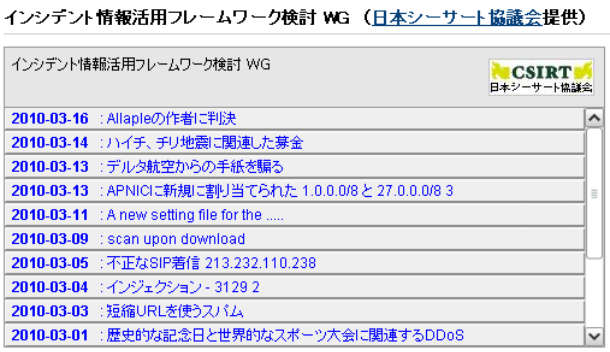


図 15 : セキュリティ情報統合サイトでの cNotes を活用した情報発信

表 1 : Publications コーナー掲載レポート

番号	題名
HIRT-PUB09008	2009 年ファイル交換ソフトによる情報漏えいに関する調査結果
HIRT-PUB09007	P2P ファイル交換ソフト環境で流通するマルウェア(2009 年)
HIRT-PUB09005	ファイル交換ソフトにおける流通ファイル数の推定
HIRT-PUB09003	USB メモリの自動再生／自動実行 -仮想体験デモ（2）-
HIRT-PUB09002	ウイルス添付メールの今と昔 -仮想体験デモ（1）-
HIRT-PUB09001	みんなで「情報セキュリティ」強化宣言！2009

(4) CSIRT コミュニティとの組織間連携の強化

組織間連携強化の具体的な活動として，2006 年から NTT-CERT[9]と定期的に会合を開催し，CSIRT 活動自身を改善するための情報交換を続けている．2009 年は，演習型 HIRT オープンミーティングで実施している教育メニュー改善を目的として，2 月に NTT-CERT 主催のワークショップで，NTT グループ向けにウェブアプリケーション開発の演習を実施した．

また，『脅威分析』に必要となる観測データなどの情報を組織間で相互活用していくためのフレームワークである『日立 SOC-IX(Security Operation Center Information eXchange)』(図 14)については，日本シーサート協議会のインシデント情報活用フレームワーク検討 WG と連携し、観測データに基づいた見える化を試みる cNotes(Current Status Notes)[10]を用いた情報発信を開始した(図 15).

(5) その他

- 日経 BP 社 ITpro CSIRT(Computer Security Incident Response Team)フォーラムに，脆弱性対策に関する記事「チェックしておきたい脆弱性情報」を寄稿した．
- 2009 FIRST Symposium, Riga において，P2P ファイル交換ソフトウェアが使用するファイル所在情報(キー情報)や通信を外的に制御することで発生しうる潜在的な脅威を明らかにすると共に，逆用によるオーバーレイネットワーク自身の制御可能性について報告した[11].
- 第 5 回 Annual WARP Forum 2009 において，日本での WARP 活動をスライドとビデオレターを用いて報告した[12].

3 HIRT

本章では, HIRT に対する理解を深めてもらうために，組織編成モデル，調整機関である HIRT センタの位置付け，ならびに現在 HIRT センタが推進している活動について述べる．

3.1 組織編成モデル

HIRT では, 4 つの IRT という組織編成モデルを採用している(図 16，表 2)．4 つの IRT とは，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 IRT), その製品を用いたシステムを構築やサービスを提供する側面(SI ベンダ IRT), そして，インターネットユーザ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 IRT)の 3 つがあること，これらの IRT 間の調整業務を行なう HIRT/CC(HIRT Coordination Center)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．

実際に，4 つの IRT が整備されるまでには表 3 にある 4 段階ほどのステップを踏んでおり，3 つの IRT の大枠が決まった後に，社内外の調整役となる HIRT センタが組織として構成されている．また，各段階においては組織編成を後押しするトリガが存在している．例えば，第 2 ステップの製品ベンダ IRT 立上げには CERT/CC から報告された SNMP の脆弱性[13]が多くの製品に影響を与えたこと，第 3 ステップの SI ベンダ IRT 立上げについては『情報セキュリティ早期警戒パートナーシップ』の運用開始が挙げられる．

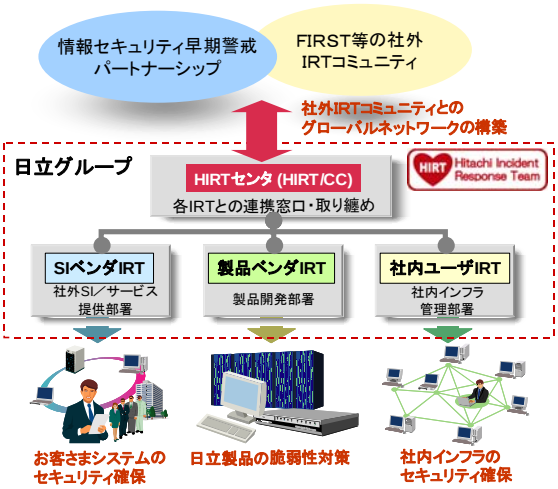


図 16：組織編成モデルとしての 4 つの IRT

表 2：各 IRT の役割

分類	役割
HIRT/CC	該当部署：HIRT センタ ➢ FIRST, JPCERT/CC, CERT/CC などの社外 CSIRT 組織との連絡窓口 ➢ SI ベンダ／製品ベンダ／社内ユーザ IRT 組織間の連携調整
SI ベンダ IRT	該当部署：SI／サービス提供部署 ➢ 顧客システムを対象とした CSIRT 活動の推進 ➢ 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
製品ベンダ IRT	該当部署：製品開発部署 ➢ 日立製品の脆弱性対策，対策情報公開の推進 ➢ 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，告知と修正プログラムの提供
社内ユーザ IRT	該当部署：社内インフラ提供部署 ➢ 侵害活動の基点とならないよう社内ネットワークのセキュリティ対策の推進

表 3：組織編成の経緯

ステップ	概要
1998 年 4 月	日立としての CSIRT 体制を整備するためのプロジェクトとして活動を開始
第 1 ステップ 社内ユーザ IRT の立上げ (1998 年～2002 年)	日立版 CSIRT を試行するために，日立グループに横断的なバーチャルチームを編成し，メーリングリストをベースに活動を開始．メンバ構成は主に社内セキュリティ有識者及び社内インフラ提供部門を中心に編成．
第 2 ステップ 製品ベンダ IRT の立上げ (2002 年～)	製品開発部門を中心に，社内セキュリティ有識者，社内インフラ提供部門，製品開発部門，品質保証部門等と共に，日立版 CSIRT としての本格活動に向け，関連事業所との体制整備を開始．
第 3 ステップ SI ベンダ IRT の立上げ (2004 年～)	SI／サービス提供部門と共に SI ベンダ IRT の立上げを開始．さらに，インターネットコミュニティとの連携による迅速な脆弱性対策とインシデント対応の実現に向け，HIRT の対外窓口ならびに社内の各 IRT との調整業務を担う HIRT/CC の整備を開始．
2004 年 10 月	HIRT/CC として HIRT センタを設立．

3.2 HIRT センタの位置付け

HIRT センタは，情報・通信グループ配下に設置された製品／サービスセキュリティ委員会の実行組織である．主な活動は，情報セキュリティ統括部，情報システム事業部と品質保証本部との相互協力による制度面／技術面でのセキュリティ対策活動の推進，各事業部／グループ会社への脆弱性対策とインシデント対応の支援，そして，日立グループの CSIRT 窓口として組織間連携によるセキュリティ対策活動の促進である(図 17)．

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の背景には，情報システムの構成品が多岐にわたっているため，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．

3.3 HIRT センタの主な活動内容

現在推進している HIRT センタの主な活動は，社内向けの CSIRT 活動(表 4)と，社外向けの CSIRT 活動(表 5)とがある．

社内向けの CSIRT 活動では，セキュリティ情報の収集／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すると共に，各種ガイドラインや支援ツールの形で製品開発プロセスにフィードバックする活動を推進中である．

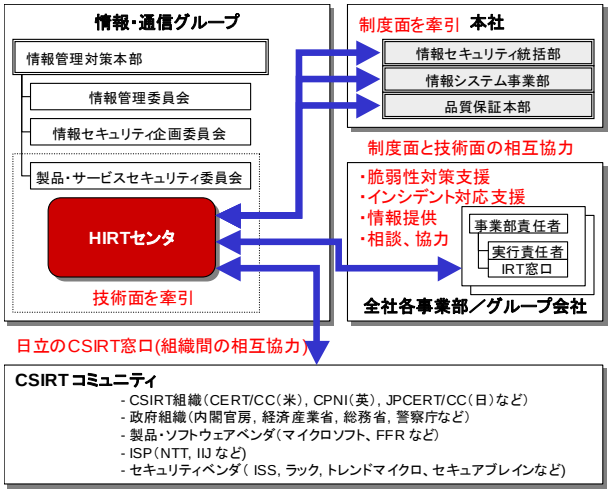


図 17：HIRT センタの位置付け

表 4　推進中のプロジェクト(社内対応)

分類	概要
セキュリティ情報の収集／分析／提供	➢ 情報セキュリティ早期警戒対応の推進(脆弱性対策ならびにインシデント対応に関する情報／ノウハウの水平展開) ➢ 日立 SOCIX(Security Operation Center Information eXchange)に基づく広域観測網の構築
製品／サービスの脆弱性対策とインシデント対応の推進	➢ 企業内セキュリティ対応部署向け教育による日立グループ内体制基盤強化 ➢ 脆弱性対策とインシデント対応のための技術ノウハウの蓄積と展開 ➢ セキュリティ情報統合サイトを活用した社外 Web サイトにおけるセキュリティ情報発信の推進
製品／サービスのセキュリティ技術の向上	➢ セキュリティ作り込みプロセスの整備(開発～検査～運用管理のための各種ガイドラインなど) ➢ 社内支援活動を通じた，支援内容・プロセスの強化・拡充 ➢ ウェブアプリケーションセキュリティの強化
研究活動基盤の整備	➢ システム開発研究所との共同研究体制の整備(P2P 観測関連など)

社内向けの注意喚起やアドバイザリの発行については，2005 年 6 月から HIRT セキュリティ情報を細分化した。注意喚起ならびに注目すべき情報を広く配布することを目的とした HIRT セキュリティ情報と，個別に対処依頼を通知する HIRT-FUP 情報とに分け，広報と優先度とを考慮した運用に移行している(表 6，図 18)．また，情報を効果的に展開するため，情報の集約化による発行数の低減と共に，情報セキュリティ統括部と品質保証本部と連動した情報発信を実施している．

製品／サービスの脆弱性対策とインシデント対応としては，セキュリティ情報統合サイトを用いて，日立グループの製品／サービスセキュリティに関する取り組みを広くインターネットユーザに展開する活動を推進中である．

表 5　推進中のプロジェクト(社外対応)

分類	概要
CSIRT 活動の国内連携の強化	➢ 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展開 ➢ 日本シーサート協議会関連活動との連携
CSIRT 活動の海外連携の強化	➢ FIRST カンファレンスでの講演／参画を通じた海外 CSIRT 組織／海外製品ベンダ IRT との連携体制の整備 ➢ 英国 WARP 関連活動の推進 ➢ CVE，CVSS など脆弱性対策とインシデント対応の標準化(ISO，ITU-T)への対応[*]
研究活動基盤の整備	➢ 東海大学(菊池教授)との共同研究の推進 ➢ 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

表 6：HIRT が発行するセキュリティ情報の分類

識別番号	用途
HIRT-FUPyynnn	優先度：緊急 配布先：関連部署のみ HIRT センタが日立グループ製品やウェブサイトの脆弱性を発見した場合や，その報告を受けた場合など，関連部署との連絡を必要とする際に利用する．
HIRT-yynnn	優先度：中～高 配布先：限定なし 広く脆弱性対策とインシデント対応の注意喚起を行なう際に利用する．
HIRT-FYIyynnn	優先度：低 配布先：限定なし HIRT オープンミーティング，講演会などの開催案内を通知する際に利用する．

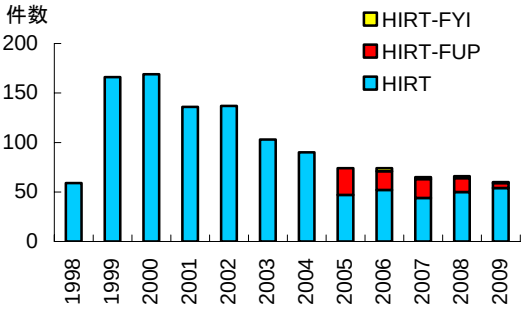


図 18：識別番号別セキュリティ情報の発行数

特に，社外向けの脆弱性対策とインシデント対応のセキュリティ情報の発信にあたっては，セキュリティ情報統合サイトを用いた定常的なセキュリティ情報の発信だけではなく，『緊急度のレベル』を判断し，次に情報掲載ウェブサイトの『階層レベル』を選択するという緊急度レベル×階層レベル型の情報発信アプローチも併用している(図 19)．

*) ISO SC27/WG3 では 2007 年から『責任ある脆弱性情報の開示(29147)』の検討を開始した。ITU-T SG17 Q.4 では 2009 年から CVE(共通脆弱性識別子)，CVSS(共通脆弱性評価システム)などの『サイバーセキュリティ情報交換フレームワーク(X.cybex)』の標準化活動を開始した。

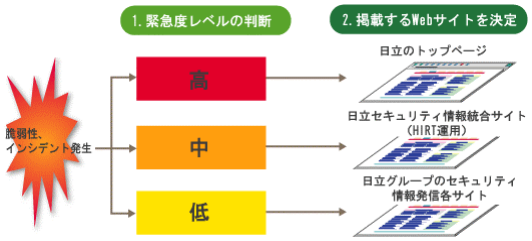


図 19:緊急度レベル×階層レベル型の情報発信の概念図

4 1998 年～2008 年の活動サマリ

本章では, HIRT プロジェクトとして活動を始めた 1998 年以降の各年の活動トピックスについて述べる.

4.1 2008 年

(1) DNS キャッシュポイズニングの対策

DNS キャッシュポイズニング対策として,『DNS の役割と関連ツールの使い方』説明会を開催した. また, 説明会用に作成した資料は, 国内の DNS キャッシュポイズニング対策に役立ててもらうため, 2009 年 1 月に IPA から発行された『DNS キャッシュポイズニング対策』[14]の資料素材として提供した.

(2) JWS2008 の開催

2008 年 3 月 25 日～28 日, 国内 FIRST 加盟チームと共に, FIRST 技術ミーティングである FIRST Technical Colloquium と国内 CSIRT の技術交流ワークショップ Joint Workshop on Security 2008, Tokyo(JWS2008)を開催した[15].

(3) 国内 COMCHECK Drill 2008 への参加

企業内の情報セキュリティ部署の対外向け連絡窓口のコミュニケーション確認を目的とした, 国内 COMCHECK Drill 2008(演習名:SHIWASU, 2008 年 12 月 4 日実施)に参加した.

(4) 経済産業省商務情報政策局長表彰(情報セキュリティ促進部門)受賞

2008 年 10 年 1 日に開催された, 情報化月間推進会議(経済産業省, 内閣府, 総務省, 財務省, 文部科学省, 国土交通省)主催の, 平成 20 年度情報化月間記念式典にて,『経済産業省商務情報政策局長表彰(情報セキュリティ促進部門)』を受賞しました[16].

(5) 講演会

- 2008 年 4 月:明治大学 経営学部教授 中西晶 氏『高信頼性組織のマネジメント』

(6) その他

新たな組織間連携の取り組みとして, 標的型攻撃の実態の一旦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募集要項を騙ったマルウェア添付メールの検体を関連組織に提供した.

4.2 2007 年

(1) 演習型 HIRT オープンミーティングの開始

2007 年は, 3 月, 6 月の 2 回, ウェブアプリケーション開発者を対象に, 演習型の HIRT オープンミーティングを開催し, ガイドライン『Web アプリケーションセキュリティガイド』のより実践的な展開を実施した.

(2) 日本シーサート協議会の設立

2007 年 4 月, 単独の CSIRT では解決が困難な事態に対して CSIRT 間の強い信頼関係に基づいた迅速かつ最適な対応を実施する体制作りを整備するため, IIJ-SECT(IIJ), JPCERT/CC, JSOC(ラック), NTT-CERT(NTT), SBCSIRT(ソフトバンク)と共に, 日本シーサート協議会を設立した[17].

(3) 英 WARP 加盟

2007 年 5 月, CSIRT 活動の海外連携強化のため, 英国政府のセキュリティ機関 CPNI(The Centre for the Protection of the National Infrastructure)が推進する WARP(Warning, Advice and Reporting Point)に加盟した[18].

(4) 講演会

- 2007 年 8 月:フォティーンフォティ技術研究所 鵜飼裕司氏『静的解析による脆弱性検査』

4.3 2006 年

(1) 脆弱性届出統合窓口の設置

2006 年 11 月, 日立グループにおいて脆弱性関連情報を適切に流通させ, 日立のソフトウェア製品およびウェブサイトの脆弱性対策を推進するために, ソフトウェア製品およびウェブアプリケーションに関する脆弱性もしくは不具合を発見した場合の日立グループ向け脆弱性届出統合窓口を設置した.

(2) ウェブアプリケーションセキュリティの強化

2006 年 10 月, 日立グループにおけるウェブアプリケーションセキュリティ施策の一環として, ガイドラインとチェックリストを整備すると共に, 日立グループ内への展開を支援した. ガイドライン『Web アプリケーションセキュリティガイド(開発編)V2.0』では, LDAP インジェクション, XML インジェクションなどの新たな脆弱性項目と脆弱性有無の確認方法を追記し改訂を行った.

(3) ファイル交換ソフトによる情報漏えいに関する注意喚起

Antinny は，2003 年 8 月に出現したファイル交換ソフトウェア『Winny』を通じて流布するマルウェアである．感染すると情報漏えいや特定サイトへの攻撃活動を発症する．HIRT では，これら脅威の状況を踏まえ，2006 年 4 月に資料『～ウィニーによる情報漏えいの防止と将来発生する危険から身を守るために～』による注意喚起を行った．

(4) 情報家電／組込み系の製品セキュリティ活動の立上げ

情報家電／組込み系の製品セキュリティ活動の立上げを開始した．HIRT では，インターネット電話などで用いられる通話制御プロトコルのひとつである SIP(Session Initiation Protocol)に注目し，関連するセキュリティツールならびにセキュリティ対策の状況を調査報告としてまとめた．

(5) CSIRT コミュニティとの組織間連携の強化

2006 年 3 月，NTT-CERT 主催の NTT グループ向けワークショップで日立の CSIRT 活動を紹介し，CSIRT 活動を相互に改善するための情報交換を行なった．

(6) 講演会

- 2006 年 5 月 : eEye Digital Security 鵜飼裕司氏『組込みシステムのセキュリティ』
- 2006 年 9 月 : Telecom-ISAC Japan 小山覚氏『Telecom-ISAC Japan におけるボットネット対策』

(7) その他

- HIRT から発信する技術文書(PDF ファイル)にデジタル署名を付加する活動の開始[19]

4.4 2005 年

(1) FIRST 加盟

2005 年 1 月，各国の CSIRT 組織と連携可能なインシデント対応体制を作りながら，CSIRT 活動の実績を積むため，世界におけるコンピュータ・インシデント対応チームの国際的なコミュニティである Forum of Incident Response and Security Teams(FIRST)に加盟した[20]．加盟にあたっては，加盟済み 2 チームによる推薦が必要であり，約 1 年の準備期間を要した．

2010 年 2 月現在，日本からは，CDI-CERT(サイバーディフェンス研究所)，CFC(警察庁情報通信局)，HIRT(日立)，IIJ-SECT(IIJ)，IPA-CERT(情報処理推進機構)，JPCERT/CC，JSOC(ラック)，KKCSIRT(カカクコム)，MIXIRT(ミクシィ)，NCSIRT(NRI セキュアテクノロジーズ)，NISC(内閣官房情報セキュリティセンタ)，NTT-CERT(NTT)，Rakuten-CERT(楽天)，RicohPSIRT(リコー)，SBCSIRT(ソフトバンク)，YIRD(ヤフー)の 16 チームが加盟している(図 20)．

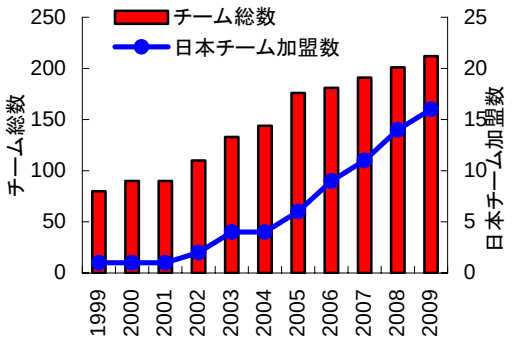


図 20：FIRST 加盟チーム数の推移

(2) セキュリティ情報統合サイトの開設

2005 年 9 月，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ため，各事業部ならびにグループ会社のウェブサイトから発信されているセキュリティ情報を統合する窓口ページを開設した(図 21)．これにあわせ，セキュリティ情報発信ガイドとして『社外向け Web セキュリティ情報発信サイトの発信ガイド V1.0』を作成した．

セキュリティ情報統合サイト
日本語　http://www.hitachi.co.jp/hirt/
英語　http://www.hitachi.com/hirt/

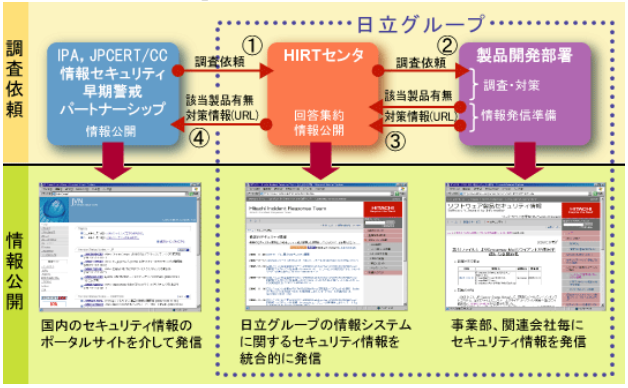


図 21：統合サイトでのセキュリティ情報発信

(3) CSIRT 活動の国内連携強化

CSIRT 活動の国内連携強化として，FIRST 加盟済み国内チームとの意見交換会，NTT-CERT ならびにマイクロソフト PST(Product Security Team)との個別に意見交換会を実施すると共に，ウェブサイト改ざん発見時の通知などの連絡網を整備した．

4.5　2004 年

(1) 情報セキュリティ早期警戒パートナーシップへの参画

2004 年 7 月『ソフトウェア等脆弱性関連情報取扱基準』の施行にあわせて，情報セキュリティ早期警戒パートナーシップ制度が始動した[21][22]，日立グループでは，パートナーシップに製品開発ベンダとして登録(HIRT を連絡窓口)すると共に，Japan Vulnerability Notes(JVN)[23]への脆弱性対策の状況掲載を開始した．

(2) ウェブアプリケーションセキュリティの強化

2004 年 11 月，ウェブアプリケーションの設計／開発時に留意すべき，代表的な問題点とその対策方法の概要についてまとめた『Web アプリケーションセキュリティガイド(開発編)V1.0』を作成し，日立グループ全体に展開した．

(3) 講演会

- 2004 年 1 月 : ISS(Internet Security Systems)Tom Noonan 氏 『Blaster 以降の米国セキュリティビジネス事情』

4.6　2003 年

(1) ウェブアプリケーションセキュリティ活動の立上げ

ウェブアプリケーションセキュリティ強化活動の検討を開始すると共に，事業部と共同で，『Web アプリケーション開発に伴うセキュリティ対策基準の作成手順 V1.0』を作成した．

(2) NISCC からの脆弱性関連情報の社内展開

2002 年の CERT/CC 脆弱性関連情報の社内展開に続き，NISCC(現 CPNI)Vulnerability Disclosure Policy に基づく脆弱性関連情報入手と情報掲載を開始した．活動開始以降，日立製品の情報が NISCC Vulnerability Advisory に最初に掲載されたのは 2004 年 1 月の 006489/H323 である[24].

表 7：連絡窓口情報

名称	"HIRT": Hitachi Incident Response Team.
所在地	〒212-8567 神奈川県川崎市幸区鹿島田 890
電子メールアドレス	hirt@hitachi.co.jp
公開鍵 PGP key	KeyID = 2301A5FA Key fingerprint 7BE3 ECBF 173E 3106 F55A 011D F6CD EB6B 2301 A5FA pub 1024D/ 2003-09-17 HIRT: Hitachi Incident Response Team < hirt@hitachi.co.jp >

(3) HIRT 社外向け連絡窓口の整備

脆弱性発見に伴う関連機関への報告と公開に関する活動[25][26][27]の活発化にあわせ，日立製品ならびに日立が関与するサイトに対して脆弱性の存在や侵害活動の要因などが指摘された場合の対処窓口として，表 7に示す連絡窓口を設置した．

4.7　2002 年

(1) CERT/CC 脆弱性関連情報の社内展開

2002 年に CERT/CC から報告された SNMP の脆弱性[13]は，多くのソフトウェアや装置に影響を与えた．この脆弱性報告をきっかけに，HIRT では，製品ベンダ IRT の立上げ，CERT/CC Vulnerability Disclosure Policy に基づく脆弱性関連情報入手と情報掲載を開始した[28]．活動開始以降，日立製品の情報が CERT/CC Vulnerability Notes Database に最初に掲載されたのは 2002 年 10 月の VU#459371 である[29].

(2) JPCERT/CC Vendor Status Notes の構築と運用支援

国内のセキュリティ情報流通改善の試みとして，2003 年 2 月，試行サイト JPCERT/CC Vendor Status Notes(JVN)の(http://jvn.doi.ics.keio.ac.jp/)の構築と運用を支援した(図 22)[30][31]．なお，試行サイトは，2004 年 7 月の『ソフトウェア等脆弱性関連情報取扱基準』の施行に伴い，報告された脆弱性を公表する Japan Vulnerability Notes(JVN)サイト(http://jvn.jp/)にその役割を引き継いでいる．

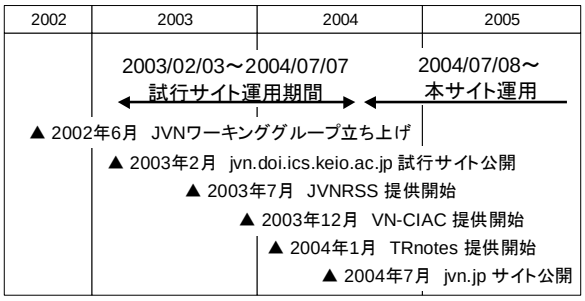


図 22：JVN 試行サイトの構築ならびに運用

4.8　2001 年

(1) ウェブサーバを攻撃対象とするワームの活動状況調査

インターネット上に公開しているウェブサーバから回収したログデータをもとに，2001 年に流布したウェブサーバを攻撃対象とするワームである，CodeRed I，CodeRed II，Nimda の活動状況について状況調査を実施した(2001 年 7 月 15 日～2002 年 6 月 30 日)．特に，国内で被害の大きかった CodeRed II，Nimda(図 23)については，最初の痕跡記録時刻

から最頻数となった日までわずか 2 日間程度であり，ワームによる被害波及が短期間かつ広範囲に渡っていた．

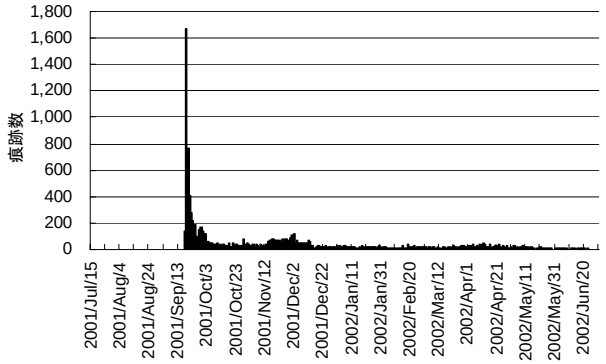


図 23：観測期間内の痕跡数変位(Nimda)

4.9 2000 年

(1) 脆弱性の深刻度に関する指標調査

侵害活動などに利用される脆弱性の深刻度を図るために，関連機関が提示している脆弱性の深刻度の指標を調査した．

CERT/CC では，脆弱性毎に Vulnerability Notes[32]と呼ぶメモを作成し，その中で脆弱性の深刻度を示す Severity Metrics を算出している[33]. CVE(共通脆弱性識別子)では脆弱性を『通常考えられる一般的なセキュリティポリシーを侵害する“Vulnerability”』と『個々の環境に依存し，個別のセキュリティポリシーを侵害する“Exposure”』の 2 つに区別し, Vulnerability を脆弱性として取り扱う[34]．また，NIST では，NVD の前身である ICAT Metabase[35]において，CERT アドバイザリならびに CVE の発行有無を脆弱性の深刻度判定の目安とし，3 段階の分類を行っている．

なお，各組織で使用する脆弱性の深刻度指標が異なっていることから，2004 年，脆弱性の深刻度を包括的かつ汎用的に評価する共通指標として CVSS(共通脆弱性評価システム)[36]が利用され始めた．

4.10 1999 年

(1) hirt.hitachi.co.jp ドメイン稼動開始

日立グループへのセキュリティ情報提供の改善を図るため，1999 年 12 月，HIRT プロジェクト用の社内向けドメインを用意し，ウェブサイト hirt.hitachi.co.jp を立上げた．

(2) ウェブサイト書き換えの調査

1996 年に米国でウェブサイトのページ書き換えが発生してからネットワークワーム世代(2001 年～2004 年)までの間, ウェブサイトのページ書き換えが代表的なインシデントとなった．1999 年～2002 年にかけ，侵害活動の発生状況を把握するために，ウェブサイトのページ書き換えに関する調査を行なった(図 24).

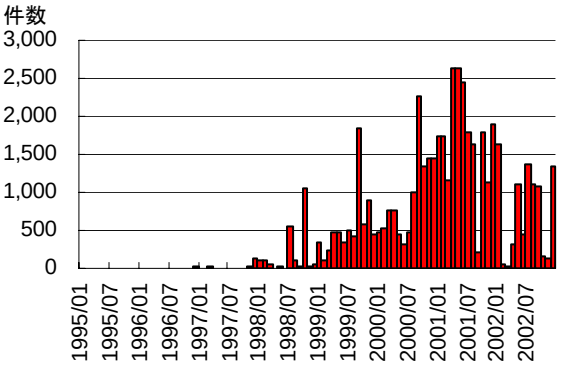


図 24：ウェブサイトの書き換え件数の推移

4.11 1998 年

(1) HIRT セキュリティ情報のサービス開始

1998 年 4 月，CERT/CC，JPCERT/CC や製品ベンダ(シスコ，ヒューレッド・パッカード，マイクロソフト，ネットスケープ，サン・マイクロシステムズなど)が発行するセキュリティ情報を元に社内メーリングリストと HIRT プロジェクト用の社内ウェブサイトにて対策情報の提供を開始した．

(2) ネットワークセキュリティセミナー開催

1998 年 6 月 25 日～26 日，米セキュリティカンファレンス DEFCON[37]にスピーカとしても参加している米国技術者を講師に迎え, 日立向けに『ネットワークセキュリティ』教育を実施した．

5 おわりに

サイバー攻撃活動はシステム化され，派生するインシデントは，対処の複雑さを増している．このような新たな脅威に対してこそ，各組織が保有する観測機能，状況分析機能ならびに対処機能を連携させることによって問題事象を解決できると考えている．

HIRT では，インシデントの状況変化を踏まえ，『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る活動を進めていく。また，複数の CSIRT 同士が協調して新たな脅威に立ち向かうための組織間連携や観測データに基づく見える化など，今後共、国内の脆弱性対策とインシデント対応活動に寄与できる協力関係の構築を進めていく予定である．

(2010 年 3 月 23 日)

参考文献

1) トレンドマイクロ：インターネット脅威レポート,
http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/index.html
2) IBM Tokyo SOC Report: Conficker ワームの検知状況(2009 年 4 月～2010 年 2 月),
https://www.ibm.com/blogs/tokyo-soc/entry/conficker-201002
3) Conficker Work Group - ANY - InfectionTracking,
http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking
4) JPCERT/CC Alert 2010-01-07:：Web サイト改ざん及びいわゆる Gumblar ウイルス感染拡大に関する注意喚起, http://www.jpcert.or.jp/at/2010/at100001.txt
5) NIST NVD (National Vulnerability Database),
http://nvd.nist.gov/
6) (独)情報処理推進機構：脆弱性関連情報に関する届出状況, http://www.ipa.go.jp/security/vuln/report/press.html
7) 2009 年ファイル交換ソフトによる情報漏えいに関する調査結果 (2009/12),
http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html
8) P2P ファイル交換ソフト環境で流通するマルウェア(2009 年) (2010/3),
http://www.hitachi.co.jp/hirt/publications/hirt-pub09007/index.html
9) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team),
http://www.ntt-cert.org/
10) cNotes: Current Status Notes,
http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi
11) Feasibility Study of DoS attack with P2P System (2009/1), http://www.first.org/events/symposium/riga-2009/program/
12) Annual WARP Forum Report September 2009 (2009/9), http://www.warp.gov.uk/Index/Forum/5th Annual WARP Forum v1.0.pdf
13) CERT Advisory CA-2002-03, “Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)” (2002/2),
http://www.cert.org/advisories/CA-2002-03.html
14) (独)情報処理推進機構：DNS キャッシュポイズニング対策 (2009/2),
http://www.ipa.go.jp/security/vuln/DNS_security.html
15) Joint Workshop on Security 2008, Tokyo 開催記録サイト (2008/3), http://www.nca.gr.jp/jws2008/index.html
16) 情報化月間 2008-平成 20 年度情報化促進貢献企業等表彰 (2008/10),
http://www.jipdec.or.jp/gekkan/ceremony/prize02.html
17) CSIRT - 日本シーサート協議会,
http://www.nca.gr.jp/
18) WARP (Warning, Advice and Reporting Point),
http://www.warp.gov.uk/
19) GlobalSign Adobe Certified Document Services,
http://jp.globalsign.com/solution/example/hitachi.html
20) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/
21) 経済産業省告示第 235 号：ソフトウエア等脆弱性関連情報取扱基準 (2004/7),
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
22) (独)情報処理推進機構：情報セキュリティ早期警戒パートナーシップガイドライン (2004/7),
http://www.ipa.go.jp/security/ciadr/partnership_guide.html
23) JVN (Japan Vulnerability Notes), http://jvn.jp/
24) NISCC: NISCC Vulnerability Advisory 006489/H323: Vulnerability Issues in Implementations of the H.323 Protocol (2004/1),
http://www.kb.cert.org/vuls/id/JSHA-5V6H7S
25) Organization for Internet Safety: Guidelines for Security Vulnerability Reporting and Response V2.0 (2004/9),
http://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf
26) (独)情報処理推進機構：セキュリティ脆弱性情報等の公開ポリシーに関する資料 (2003/9),
http://www.ipa.go.jp/security/awareness/vendor/vulnerability200309012.pdf
27) (株)ラック：脆弱性報告と公開のポリシー (2003/8),
http://www.lac.co.jp/info/advisory/pdf/vulnerability_reporting_and_disclosure.pdf
28) CERT/CC Vulnerability Disclosure Policy,
http://www.cert.org/kb/vul_disclosure.html
29) US-CERT: Vulnerability Note VU#459371: Multiple IPsec implementations do not adequately validate authentication data” (2002/10),
http://www.kb.cert.org/vuls/id/459371
30) JPCERT/CC Vendor Status Notes DB 構築に関する検討, CSS2002 (2002/10),
http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf
31) セキュリティ情報流通を支援する JVN の構築 (2005/5), http://www.hitachi.co.jp/rd/sdl/people/jvn/index.html
32) CERT/CC Vulnerability Notes Database,
http://www.kb.cert.org/vuls
33) CERT/CC Vulnerability Note Field Descriptions,
http://www.kb.cert.org/vuls/html/fieldhelp
34) CVE (Common Vulnerabilities and Exposures),
http://cve.mitre.org/
35) ICAT, http://icat.nist.gov/
36) CVSS (Common Vulnerability Scoring System),
http://www.first.org/cvss/
37) DEFCON, http://www.defcon.org/

執筆者
寺田真敏（てらだ まさと）
1998 年に HIRT の試行活動を立ち上げて以降，2002 年に JVN(http://jvn.jp/)の前身となる研究サイト(http://jvn.doi.ics.keio.ac.jp/)の立ち上げ，2005 年には HIRT の窓口として CSIRT の国際団体である FIRST への加盟など対外的な CSIRT 活動を推進．現在，JPCERT コーディネーションセンター専門委員，(独)情報処理推進機構研究員，日本シーサート協議会の副運営委員長を務める．