2007 年 HIRT 活動報告
HIRT: Annual Report 2007

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

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』という考え方が普及し始めた．また，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 年に入ると，ネットワークワームのような大規模インシデントが影を潜め，特定の個人や組織に狙いを定めた標的型攻撃(Targeted Attack)やウイルス感染に伴うファイル交換ソフトウェアを介した情報の漏えいなど，被害発生が表面化しない事例や被害そのものを完全に収束できない事例が増加してきた．

このようなインシデントの変化は，IRT(Incident Response Team)に，情報セキュリティ対策活動として脆弱性対策やインシデント対応を推進するための『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，次のような役割も求め始めつつある．

『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，ウイルス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 IRT 統一窓口組織としての責務を負っている．

本稿では，2007 年の HIRT 活動の報告として，2007 年の脅威と脆弱性の概況と HIRT の活動トピックスについて報告する．

2 2007 年の活動概要

本章では，2007 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

2007 年は，PDF や MP3 などの添付ファイルを用いたスパムメールの出現[1]，Web サイトを流布媒体としたマルウェアの台頭など，侵害経路の多様化が見られた．また，Web サイトを流布媒体とするマルウェアの代表格 Storm Worm, Mpack に見られるように，ユーザの心理的な弱点を突くという手法が巧妙化した．

- Storm Worm

Storm Worm は，暴風雨が欧州を襲った 2007 年 1 月 19 日に欧州を中心に広がり始めた．初期の Storm Worm は，暴風雨に関する最新ニュースと見せかけ，添付された実行可能なファイルをユーザに実行するよう促す電子メールを介して流布した．亜種は，実行可能なファイルを電子メールに添付する形態だけではなく，電子メール中に URL を記載し不正 Web サイトに誘導する形態で流布した．Storm Worm のもうひとつの特徴は，注目ニュースやイベントに乗じて流布する手法を活用している．

- Mpack

2007 年 6 月に欧州を中心に被害が報告された．正規 Web サイトのページを改ざんし，マルウェアをダウンロードさせる不正 Web サイトを記載したタグを挿入する．正規 Web サイトにアクセスすると，挿入されたタグの誘導により自動的に不正 Web サイトにアクセスしてしまい，結果としてマルウェアをダウンロードし感染するという形態であった[2].

また，Web 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繰り返しダウンロードするための機能変更ダウンロードサイトとしても活用されており，不正活動の基点が Web サイト

に移りつつあると言える.

脆弱性については図 1に示す通り，NIST NVD(National Vulnerability Database)に登録された2007 年の脆弱性の総件数は 6,690 件(CERT/CC の報告は 7,236 件)である. その中で Web 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 10%，685 件となっている(図 2)[3].

また，IPA に報告された稼動中 Web サイトの脆弱性のうち，約 7 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年々増加している(図 3)[4].

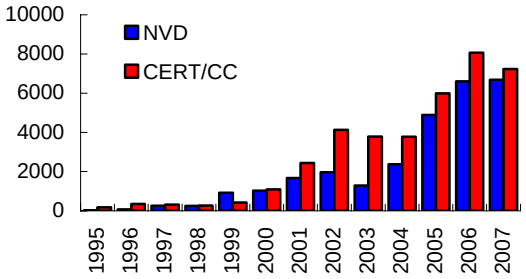


図 1：脆弱性報告件数の推移(出典：NIST NVD)

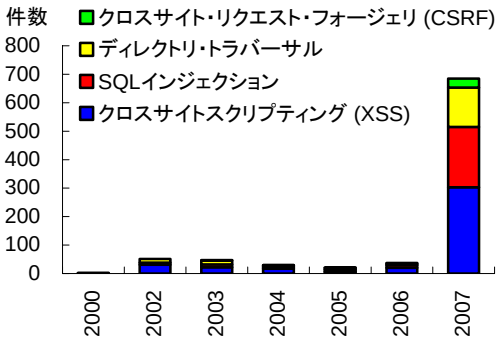


図 2：Web アプリケーション系ソフトウェア製品の脆弱性報告件数の推移(出典：NIST NVD)

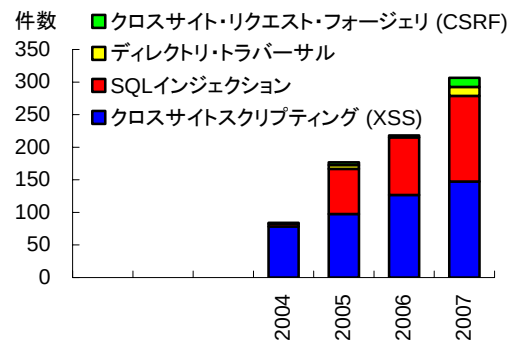


図 3：Web サイトの脆弱性報告件数の推移
(出典：IPA，JPCERT/CC)

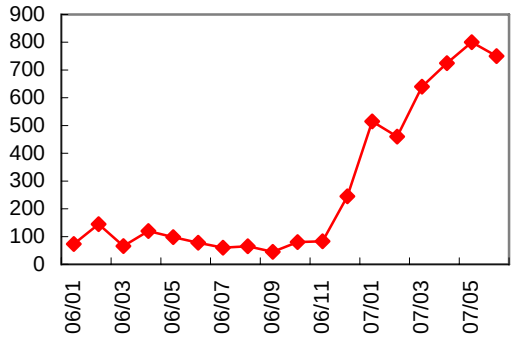


図 4：SQL インジェクション攻撃検知数の推移
(出典：LAC)

さらに，2007 年以降 SQL インジェクションに関する攻撃検知数が増加しているとの報告もあることから(図 4)[5]，Web サイトが不正活動の基点にならないよう，脆弱性対策の一層の推進が必要となっている.

全体としては，スパムメールやマルウェアなど不正なデータを情報システムに持ち込まないという防御だけではなく，内在する脅威を排除することで，重要なデータを情報システムの外に出さないという防御とを組合せて考えていく必要がでてきた.

2.2 HIRT の活動トピックス

本節では，2007 年の活動トピックについて述べる.

(1) 演習型 HIRT オープンミーティングの開始

HIRT オープンミーティングは, 信頼関係に基づく HIRT コミュニティを普及させるための活動である.『HIRT 活動に関して，HIRT センタに所属するメンバ同士が情報交換する場である』『HIRT センタの活動内容について，日立グループに広く知ってもらうことと, HIRT センタ以外からの意見を広く取り入れるために，情報交換する場を公開する』『公開の場を通じて，信頼関係に基づく HIRT コミュニティへの参加を募る』という方針に沿って開催している.

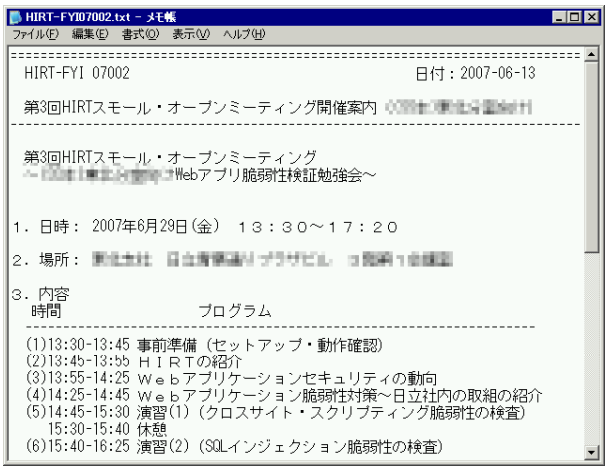
2007 年は，3 月，6 月の 2 回，Web アプリケーション開発者を対象に，演習型の HIRT オープンミーティングを開催し，ガイドライン『Web アプリケーションセキュリティガイド』のより実践的な展開を開始した(図 5).

(2) 静的解析と製品セキュリティ

プログラムのセキュリティ問題を調査する方法として，ソースコードを調査するホワイトボックス方式，さまざまなテストケースを用意しトライ&エラーを繰り返すブラックボックス方式がある. 特に，2006 年から総当り的に例外的なデータの入力を試行し，プログラムの欠陥を発見する Fazzing

ツールが普及し始め，多くの脆弱性を発見するに至っている．しかし，総当り的な方法では見落としが発生しやすいことから，ソースコードが無くても調査可能で，脆弱性の見落としが少ない静的解析を製品のセキュリティ問題を調査する方法として検討する必要がでてきた．

このような背景から，2007 年 8 月，フォティーンフォティ技術研究所の鵜飼裕司氏を講師として招き，製品の脆弱性検査に静的解析技術がどのように利用されているのかなど，開発サイドでの活用策についての講演会を開催した．


HIRT-FYI07002.txt - メモ帳

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

HIRT-FYI 07002 日付：2007-06-13

第3回HIRTスモール・オープンミーティング開催案内

第3回HIRTスモール・オープンミーティング
～Webアプリ脆弱性検証勉強会～

1．日時： 2007年6月29日(金) １３：３０～１７：２０

2．場所：

3．内容
時間 プログラム
(1)13:30-13:45 事前準備（セットアップ・動作確認）
(2)13:45-13:55 ＨＩＲＴの紹介
(3)13:55-14:25 Ｗｅｂアプリケーションセキュリティの動向
(4)14:25-14:45 Ｗｅｂアプリケーション脆弱性対策～日立社内の取組の紹介
(5)14:45-15:30 演習(1)（クロスサイト・スクリプティング脆弱性の検査）
15:30-15:40 休憩
(6)15:40-16:25 演習(2)（SQLインジェクション脆弱性の検査）

図 5：演習型の HIRT オープンミーティング開催案内

(3) 日本シーサート協議会の設立

2007 年 4 月，単独の IRT では解決が困難な事態に対して IRT 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)，SBB-SIRT(ソフトバンク BB)と共に，日本シーサート協議会を設立した[6]．また，日本シーサート協議会においては，個別の IRT が抱える課題や技術情報，対応手法などの情報をより高いレベルで共有していくために，ワーキンググループ毎の問題解決活動を開始した．

(4) 英 WARP 加盟

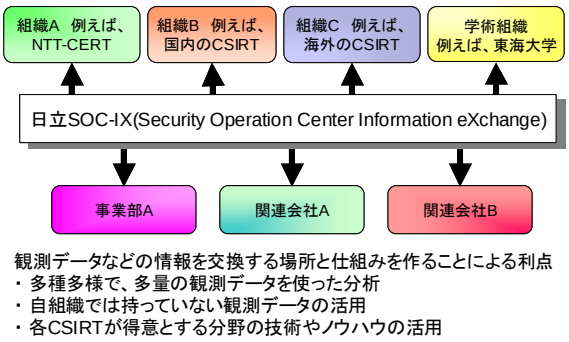
IRT 活動の海外連携強化のため，英国政府のセキュリティ機関 CPNI(The Centre for the Protection of the National Infrastructure) が推進する WARP (Warning, Advice and Reporting Point)に加盟を申請し，2007 年 5 月 16 日申請が認可された[7]．WARP は，英国政府のセキュリティ機関が推進する脆弱性対策ならびにインシデント対応推進のためのフレームワークであり，また，そのフレームワークに加盟したグループから構成されたコミュニティである．

(5) IRT 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[8]と定期的に会合を開催し，IRT 活動自身を改善するための情報交換を続けている．2007 年は，NTT-CERT とのボット観測の相互協力関係を整備するため，観測データの相互利用の検討を実施した．

また，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，状況把握ならびに対処を含め，社外との組織間連携が必要であると考え，総務省「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」に参画するコンピュータソフトウェア著作権協会の協力を得て，ファイル交換ネットワーク環境の調査活動を実施した[9][10]．

今後，上記の組織間連携活動は，次の脅威をキャッチアップするために，「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)」に繋げていく予定である(図 6)．



観測データなどの情報を交換する場所と仕組みを作ることによる利点
・多種多様で、多量の観測データを使った分析
・自組織では持っていない観測データの活用
・各CSIRTが得意とする分野の技術やノウハウの活用

図 6：日立 SOC-IX の概念図

(6) IRT 活動の広報

IRT の活動を伝えていくことも，情報セキュリティ対策の推進に必要であると考え，2007 年 1 月から，HIRT で推進している取り組みをレポート形式にまとめて報告する Publications コーナー (http://www.hitachi.co.jp/hirt/publications/)を設置した．また，2007 年のレポートとして 6 件(英語サイトは 3 件)を掲載した(表 1)．

(7) その他

- 日経 NETWORK「ネットワーク検定 2007」の問題作成に協力
- 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を寄稿
- 警察庁セキュリティポータルサイト@police に，「脆弱性対策情報を提供しているサイトの活用方法」に関する記事を寄稿[11]

表 1：Publications コーナー掲載レポート

番号	題名
HIRT-PUB07012	2007 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-PUB07007	諸外国のセキュリティコミュニティの形　－英国の WARP とは？
HIRT-PUB07004	ワームが送信するパケットの動きをみてみよう
HIRT-PUB07003	みんなで「情報セキュリティ」強化宣言！
HIRT-PUB07002	RSS ディレクトリを用いた日立セキュリティ情報の発信
HIRT-PUB07001	HIRT 活動紹介アニメを作ってみました

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 7，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 IRT(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 センタ(HIRT/CC)を示していることに留意して欲しい.

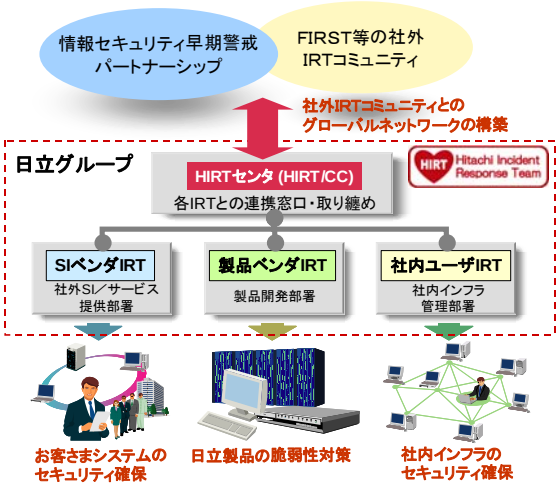


図 7：組織編成モデルとしての 4 つの IRT

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 などの対外 IRT 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 IRT 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を支援 ➢ 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 ➢ 日立サイトが不正アクセス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を支援

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 IRT 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 IRT 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 IRT 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ならびに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 センタ設立.

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 IRT との調整役となる 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[12]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.

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ならびにインシデント対応の支援，そして，日立グループの IRT 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となっている(図 8).

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．

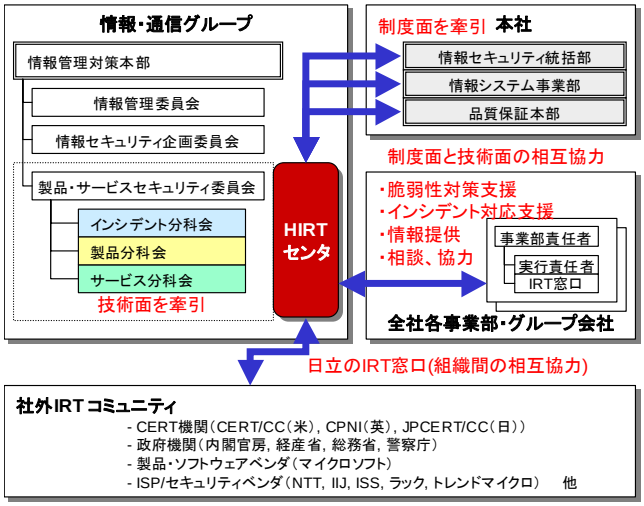


図 8：HIRT センタの位置付け

3.3 HIRT センタの主な活動内容

現在推進している HIRT センタの主な活動内容を表 4に示す．定常的な活動は，IRT 活動の国内ならびに海外連携と，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各種ガイドライン，利用可能な支援ツールの形で開発プロセス整備にフィードバックする，注意喚起やアドバイザリとして発行するという社内向けの活動と，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認知してもらうために，セキュリティ情報統合サイトを用いた社外向けの活動とに分かれている．

特に，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 セキュリティ情報の細分化として，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 5，図 9)．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．

表 4 推進中のプロジェクト

分類	概要
セキュリティ情報の収集・分析・提供	➢ 注意喚起やアドバイザリの発行 ➢ 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
IRT 活動の国内連携の強化	➢ IRT 組織間連携活動の推進(インシデント対応時の相談窓口の提供など) ➢ FIRST 加入済み国内 IRT(NTT-CERT, IIJ, JPCERT/CC 他)チームミーティングの定着化
IRT 活動の海外連携の強化	➢ 日立グループ海外拠点との連携体制の整備 ➢ 海外製品ベンダ IRT との連携体制の整備(FIRST PST ミーティングの活用) ➢ CVE, CVSS など脆弱性関連の標準化への対応
日立グループ会社との連携強化による製品脆弱性対策・情報発信の推進	➢ 日立製品ならびに日立関連サイトに脆弱性があった場合など，日立グループにおける脆弱性対策ならびにインシデント対応の社内外の対応調整 ➢ ソフトウェア製品，組込み系製品，サービスにおける管理プロセスの事例共有・開発プロセスの整備 ➢ セキュアなソフトウェア／システム開発のための各種ガイドラインの整備，利用可能な支援ツールの拡充と日立グループ内への展開 ➢ 日立製品に関する脆弱性対策情報の社外公開，情報流通の促進(セキュリティ情報統合サイトの活用)
社外向け Web サイト・アプリケーションの脆弱性対策の徹底	➢ セキュリティ文化定着化に向けたセキュリティ啓発活動 ➢ Web サイト開発プロセスの整備(開発～検査～運用管理のための各種ガイドラインなど)
日立のセキュリティプレゼンス向上	➢ 東海大学(菊池教授)と HIRT との共同研究体制の整備 ➢ 日立 SOCIX(Security Operation Center Information eXchange)の付加価値創造 ➢ 社外向け IRT 活動コンテンツの充実

表 5：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 メンバが日立グループ製品や Web サイトの脆弱性を発見した場合，または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 広く脆弱性対策ならびに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．

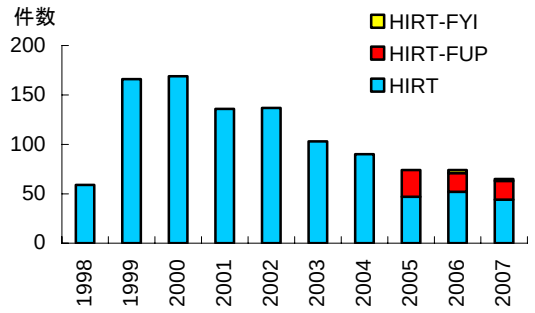


図 9：識別番号別セキュリティ情報の発行数

4　1998 年～2006 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　2006 年

(1) 脆弱性届出統合窓口の設置

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 Web サイトの脆弱性対策を推進するために, 2006 年 11 月, ソフトウェア製品および Web 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脆弱性届出統合窓口を設置した(図 10).

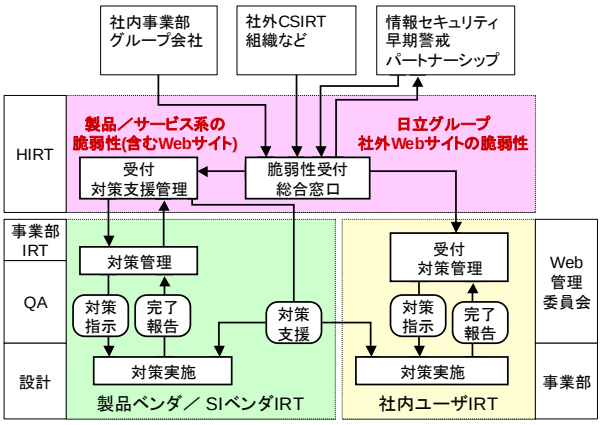


図 10：統合窓口と情報展開

(2) Web 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 Web 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』を通じて流布するウイルスであり, 感染に伴う情報漏えいや特定サイトへの攻撃が継続的に発生している. HIRT では, 昨今の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～』を作成すると共に, 注意喚起を行った.

(4) 情報家電・組込みソフトウェアにおける製品セキュリティ活動の立上げ

情報家電・組込みソフトウェアにおける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) IRT コミュニティとの組織間連携の強化

2006 年 3 月, NTT-CERT 主催のワークショップで日立の IRT 活動を紹介し, IRT 活動自身を相互に改善するための情報交換を行なった.

(6) 社外接続サイトのセキュリティ向上と脆弱性対策の推進

2006 年 11 月, 事業部のセキュリティ管理者, サーバ管理者を対象に, 『社外接続サイトのセキュリティ向上と脆弱性対策の推進』を目的とした HIRT オープンミーティングを開催し, 月例の脆弱性検査で検出されている脆弱性の説明や対策方法についての解説を実施した.

(7) 2006 年に実施した講演会

- 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」

(8) その他

- (独)情報処理推進機構ウェブアプリケーション開発者向けセキュリティ実装講座での講演[13]
- 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[14]
- マイクロソフトセキュリティコラム, FIRST Conference への寄稿ならびに投稿[15][16]

4.2　2005 年

(1) FIRST 加盟

2005 年 1 月, IRT 活動の実績を積み, 各国の組織との連携可能なインシデント対応体制を作りな

がら，より正確かつ迅速な情報収集を目指すため，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[17]．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．

2008 年 1 月現在，日本からは，CFC(警察庁情報通信局)，HIRT(日立)，IIJ-SECT(IIJ)，JPCERT/CC，JSOC(ラック)，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)，SBB-SIRT(ソフトバンク BB)，RicohPSIRT(リコー)，YIRD(ヤフー)の 11 チームが加盟している(図 11).

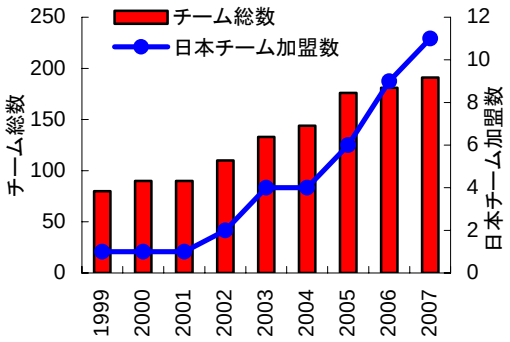


図 11：FIRST 加盟チーム数の推移

(2) セキュリティ情報用の統合窓口ページ(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 Web 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 12)．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/

(3) IRT 活動の国内連携強化

IRT 活動の国内連携強化として，FIRST 加盟済み国内チームとのミーティング，NTT-CERT ならびにマイクロソフト PST(Product Security Team)との個別チームミーティングを実施すると共に，Web サイト改ざん発見時の通知などの連絡網を整備した．

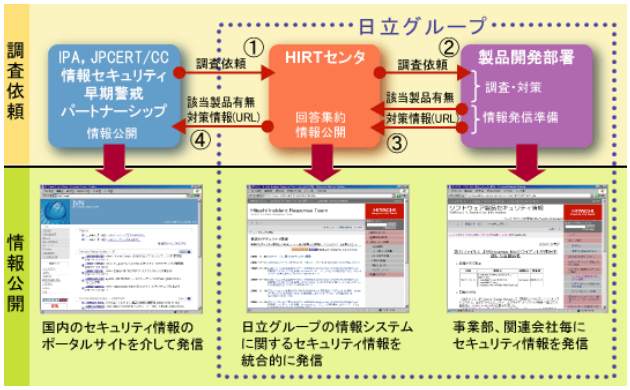


図 12：統合サイトでのセキュリティ情報発信

4.3　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[18][19]，日立グループでは，パートナーシップに HIRT を窓口として製品開発ベンダ登録を行なうと共に，JP Vendor Status Notes(JVN)[20]への製品脆弱性対応状況の掲載を開始した．

(2) Web アプリケーションセキュリティの強化

2004 年 11 月，Web 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) 2004 年に実施した講演会

- 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」

4.4　2003 年

(1) Web アプリケーションセキュリティ活動の立上げ

Web アプリケーションセキュリティ強化スキーム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 からの脆弱性確認情報の社内展開

2002 年の CERT/CC から脆弱性確認情報の社内展開に続き，NISCC(現 CPNI)から Vulnerability Disclosure Policy に基づく情報入手を開始した．活動開始以降，日立製品の情報が最初に NISCC Vulnerability Advisory に掲載されたのは 2004 年 1 月の 006489/H323 である[21].

(3) HIRT 社外向け連絡窓口の整備

脆弱性発見に伴う報告と公開に関する活動[22][23][24]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の指摘された場合の対処窓口として，表 6に示す連絡窓口を用意した．

表 6：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 >

4.5 2002 年

(1) CERT/CC からの脆弱性確認情報の社内展開

2002 年に CERT/CC から報告された SNMP の脆弱性[12]は，多くのソフトウェアや装置に広範囲にわたって影響を与えた．この脆弱性報告をきっかけに，製品ベンダ IRT の立上げと共に，CERT/CC から Vulnerability Disclosure Policy に基づく情報入手を開始した[25]．活動開始以降，日立製品の情報が最初に CERT/CC Vulnerability Notes Database に掲載されたのは 2002 年 10 月の VU#459371 である[26]．

(2) JPCERT/CC Vendor Status Notes の構築支援

JPCERT/CC Vendor Status Notes(JVN)は，2003 年 2 月に試行サイト(http://jvn.doi.ics.keio.ac.jp/)として公開された(図 13)[27][28]．また，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サイト(http://jvn.jp/)にその役割を引き継いでいる．

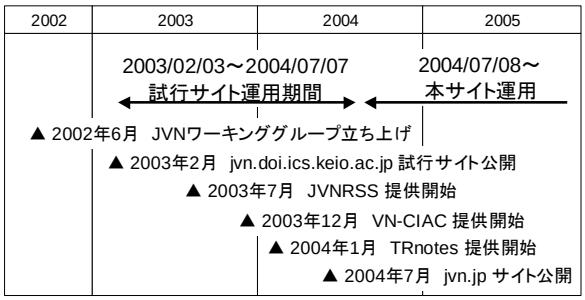


図 13：JVN 試行サイトの構築ならびに運用

4.6 2001 年

(1) Web サービス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 Web サイトから回収したログデータをもとに，2001 年に流布した Web サービス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 14)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．

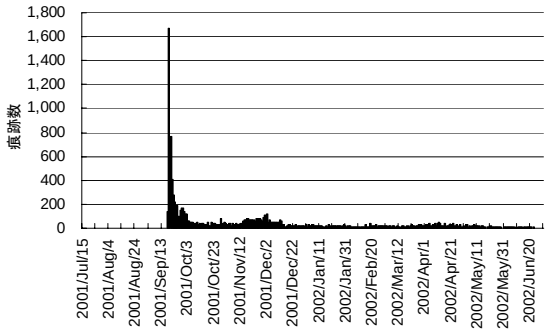


図 14：観測期間内の痕跡数変位(Nimda)

4.7 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，調査報告としてまとめた．

CERT/CC では，脆弱性毎に Vulnerability Notes[29]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[30]．CVE(Common Vulnerabilities and Exposures)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[31]．また，NIST では，NVD の前身である ICAT Metabase[32]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言語として CVSS(Common Vulnerability Scoring System)[33]が提案された．

4.8　1999 年

(1) hirt.hitachi.co.jp 稼動開始

日立グループへのセキュリティ情報提供，ならびに事業所設備点検に伴う停電時のサービス改善を図るため，1999 年 12 月，社内向け HIRT プロジェクトメイン Web サイトとして hirt.hitachi.co.jp を立上げた．

(2) Web サイト書き換えの調査

1996 年に米国で Web 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，Web 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ことから，1999 年～2002 年にかけ，不正アクセスの発生状況を把握するために，Web サイトのページ書き換えに関する調査を行なった(図 15).

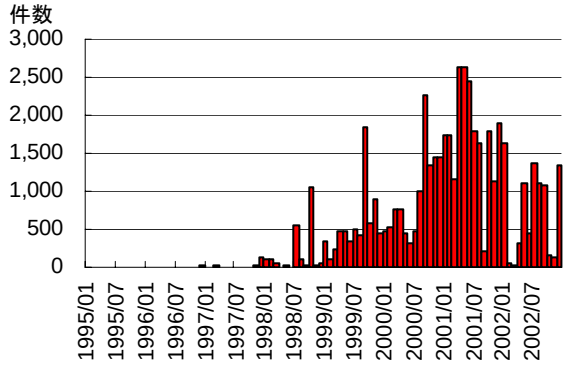


図 15：Web サイトの書き換え件数の推移

4.9　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(Cisco, HP, Microsoft, Netscape, Sun Microsystems 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 プロジェクト用社内 Web 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[34]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

インシデントは，予兆や被害が表面化しない新たなフェーズに入っている．このような新たな脅威に対しても，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組織として連携させることによって問題事象の解決を図ることができると考えている．

HIRT では，このようなインシデントの状況変化を踏まえ，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 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，お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進めていく予定である．

(2008 年 1 月 29 日記)

参考文献

1) Symantec: The State of Spam, A Monthly Report – December 2007 (2007/12), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Spam_Report_-_December_2007.pdf

2) トレンドマイクロ(株)：続・大規模な「Web からの脅威」(2007/6), http://blog.trendmicro.co.jp/archives/24

3) NIST NVD (National Vulnerability Database), http://nvd.nist.gov/

4) (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

5) (株)ラック：侵入傾向分析レポート Vol.9 (2007/11), http://www.lac.co.jp/business/sns/intelligence/report/20071101lac_report.pdf

6) CSIRT - 日本シーサート協議会, http://www.nca.gr.jp/

7) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/

8) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), http://www.ntt-cert.org/

9) クローリング手法を用いた P2P ネットワークの観測, 情報処理 CSEC 研究報告 Vol.2007 No.48. (2007/5)

10) 2007 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, http://www.hitachi.co.jp/hirt/publications/hirt-pub07012/index.html

11) @police：セキュリティ解説：脆弱性対策情報を提供しているサイトの活用方法, http://www.cyberpolice.go.jp/column/explanation21.html

12) 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

13 (独)情報処理推進機構：H18 年度ウェブアプリケーション開発者向けセキュリティ実装講座の開催について, http://www.ipa.go.jp/security/vuln/event/200612.html

14) GlobalSign Adobe Certified Document Services, http://www.globalsign.com/adobe-cds/index.htm

15) CSIRT (Computer Security Incident Response Team) ～日立における CSIRT 活動～ (2006/5), http://www.microsoft.com/japan/technet/security/secnews/columns/column060525.mspx

16) Proposal of RSS Extension for Security Information Exchange (2006/6), http://www.first.org/conference/2006/program/presentations.html - p198

17) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/

18) 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/downloadfiles/vulhandlingG.pdf

19) (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, http://www.ipa.go.jp/security/ciadr/partnership_guide.html

20) JVN (JP Vendor Status Notes), http://jvn.jp/

21) NISCC: NISCC Vulnerability Advisory 006489/H323: Vulnerability Issues in Implementations of the H.323 Protocol, http://www.cpni.gov.uk/docs/re-20040113-00387.pdf?lang=en

22) Organization for Internet Safety: Draft Security Vulnerability Reporting and Response Process (2003/7), http://www.oisafety.org/resources.html

23) (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

24) (株)ラック：脆弱性報告と公開のポリシー (2003/8), http://www.lac.co.jp/business/sns/intelligence/SNSadvisory/SNSpolicy.html

25) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html

26) US-CERT: Vulnerability Note VU#459371: Multiple IPsec implementations do not adequately validate authentication data”, http://www.kb.cert.org/vuls/id/459371

27) 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

28) セキュリティ情報流通を支援する JVN の構築 (2005/5), http://www.sdl.hitachi.co.jp/japanese/people/jvn/

29) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls

30) CERT/CC Vulnerability Note Field Descriptions, http://www.kb.cert.org/vuls/html/fieldhelp

31) CVE (Common Vulnerabilities and Exposures), http://cve.mitre.org/

32) ICAT, http://icat.nist.gov/

33) CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/

34) DEFCON, http://www.defcon.org/