2011 年 HIRT 活動報告
HIRT: Annual Report 2011

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 1-1-2
Kashimada 1-1-2, Saiwai, Kawasaki, Kanagawa, 212-8567 Japan

1 はじめに

2011 年，日本国内では多様なセキュリティインシデントが発生し，サイバー攻撃対策を見直す転換期となった(表 1).

表 1：代表的なセキュリティインシデント

時期	概要
2011 年 3 月	震災に便乗したウイルスメールの流布
2011 年 4 月	日本企業の海外 Web サイトを対象とした情報漏えいを伴う不正アクセス
2011 年 8 月	インターネットバンキングへの不正アクセス
2011 年 9 月	防衛産業企業への標的型攻撃
2011 年 11 月	クラウドへのサービス不能攻撃

特に，2011 年 4 月のインシデントは，実施すべきセキュリティ施策(特に脆弱性対策)の徹底，2011 年 9 月のインシデントは，情報保全を踏まえたセキュリティ施策(特に出口対策)の導入を再考させる事案となった.

これに伴い，日本における 2011 年のセキュリティ対策では，組織内システムの多層防御を実現する『出口対策』に注目が集まった．これまでのセキュリティ対策は，侵入を防ぐ入口対策にポイントが置かれていたが，『出口対策』を導入した多層防御では，3 つの視点からの対策推進がポイントとなる.

- 入口対策：侵入阻止を強化する.
- 拡散対策：侵入の可能性を考慮し，組織内ネットワークでの侵害活動の拡大を阻止する.
- 出口対策：侵入の可能性を考慮し，バックドア通信を介した侵害活動の進行や情報漏えいなどを阻止する.

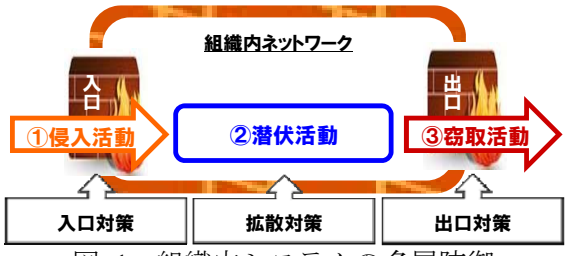


図 1：組織内システムの多層防御

このような対策の変化は，CSIRT(Computer Security Incident Readiness/Response Team；シーサート)の組織間での連携，特に情報交換にも，今後少なからず影響を与えるものと考えている.

我々の考える CSIRT の要件は，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である．これは，特別な要件を想定しているわけではない．その役割は，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)の経験値を活かして『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』ことにある.

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，2011 年の HIRT 活動の報告として，2011 年の脅威と脆弱性の概況，HIRT の活動トピックスについて報告する.

2 2011 年の活動概要

本章では，2011 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

日本国内では，標的型攻撃，Web サイトの侵害など，多様なセキュリティインシデントが発生した．この中で，Conficker(コンフィッカー)に代表される USB メモリを介した感染など，既知の脅威による被害は継続している状況にある.

また，2011 年の特徴としては，侵害活動による電子証明書の不正発行(2011 年 3 月，8 月)，窃取した電子証明書のマルウェアでの利用(2011 年 11 月)など，電子社会の基盤とも言うべき，電子証明書に関わるセキュリティインシデントが顕在化してきた．

- **標的型攻撃**

2011 年に報告された情報窃取を目的とした標的型攻撃のシナリオを図 2に示す．特徴としては，後述するソーシャルエンジニアリングを利用した標的型メール，Path the Hash 攻撃と呼ばれるハッシュ化した Windows パスワードを利用したシステム侵入, Poison Ivy などの RAT[*a]ツールを利用した感染 PC の遠隔制御が挙げられる．

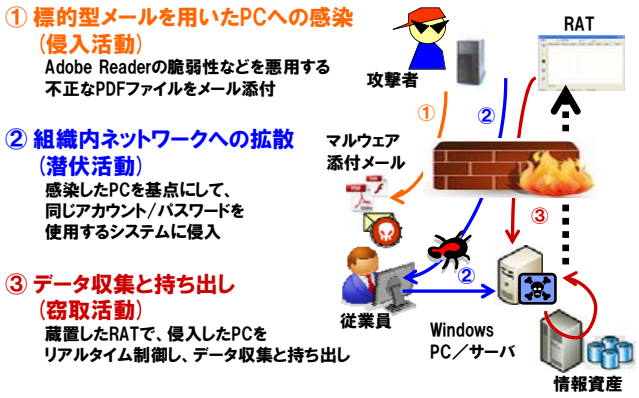


図 2：標的型攻撃のシナリオの例

特に，ソーシャルエンジニアリングを利用した標的型メールでは，アイコンとファイル名を偽装した単純な手法だけではなく，送付された電子メールを窃取し，添付ファイルに攻撃コードを埋め込んだ後，再送する手の込んだ手法の存在も報告された．

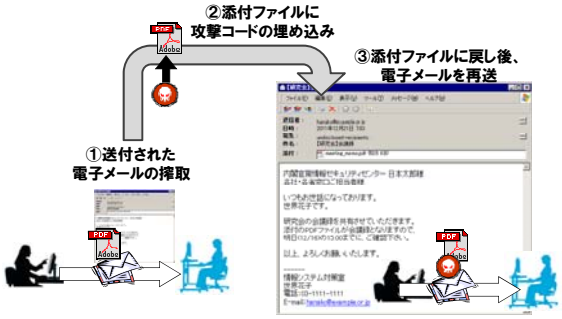


図 3：ソーシャルエンジニアリング攻撃
～本物を活用する～

- **Web サイトの侵害事案に見られた副次的な課題**

2011 年に報告された Web サイトの侵害事案の特徴として，攻撃者によって取得された情報が Web サイト上に公開されるという事例が挙げられる(表 2)．このような事案の副次的な課題としては，公開された情報が，前述の標的型攻撃などに利用される可能性にある．

表 2：漏洩情報の Web サイト公開の事例

時期	概要
2011 年 7 月	Booz Allen Hamilton 90,000 件規模のメールアドレス，パスワード
2011 年 11 月	OhMedia 60,000 件規模のメールアドレス，パスワード
2011 年 12 月	China Software Developer Network (CSDN) 600 万件規模のメールアドレス，パスワード
	Strategic Forecasting Inc.(Stratfor) 86 万件規模の顧客情報， 75,000 件規模のクレジットカード情報

- **Conficker (コンフィッカー)**

Conficker は，2008 年 11 月頃から Windows の『Server サービスの脆弱性 (MS08-067) 』を悪用するマルウェアとして出現した．2008 年 12 月，USB メモリを介して感染する機能が追加されたことにより，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の感染が広がった．2009 年にはいってからは，国内の USB メモリ型マルウェア感染被害の報告件数は減少している (図 4)[1]．しかし，Conficker Work Group の観測によれば，Conficker に感染している台数は，IP アドレスベースで約 300 万台と報告されている (図 5)[2].

(2) 脆弱性の概況

米 NIST NVD(National Vulnerability Database)[3]に登録された 2011 年の脆弱性の総件数は 4,151 件である．このうち，Web 系ソフトウェア製品の脆弱性が約 2 割(902 件)で(図 6)，その内訳は，クロスサイトスクリプティング(XSS)，SQL インジェクションが約 8 割を占めるという状況が続いている(図 7)．また，IPA に報告された稼動中 Web サイトの脆弱性のうち，約 6 割が 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 600 件/年を越えている状況にある(図 8)[4].

米 ICS-CERT(Industrial Control System-CERT)から発行された注意喚起(Alert)とアドバイザリはそれぞれ 37 件，64 件である(図 9)．このうち，制御システム製品に存在する ActiveX コントロールの脆弱性を指摘するアドバイザリが 12 件(19%)を占めている．

*a) RAT: Remote Access Trojan / Remote Administration Tool の略. 侵入したシステムを遠隔から操作するためのプログラムで，潜伏活動や窃取活動で利用されている．

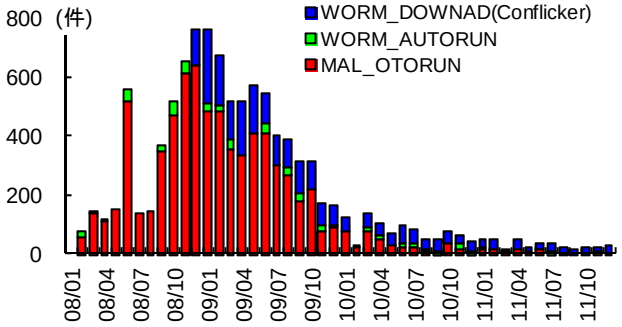


図 4：USB メモリ型マルウェアの感染被害(/月)
(出典：トレンドマイクロ)

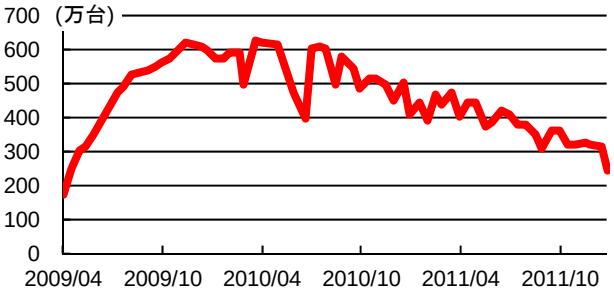


図 5：ConfickerA+B 感染台数(/日)の推移
(出典：Conficker Work Group)

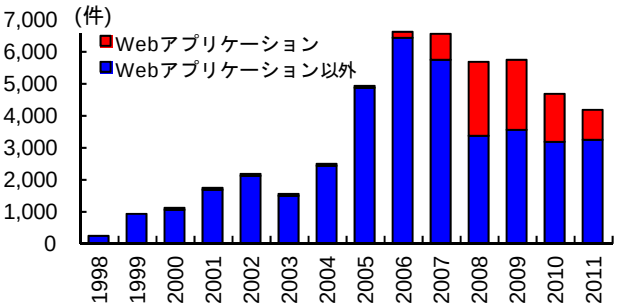


図 6：脆弱性報告件数の推移(出典：NIST NVD)

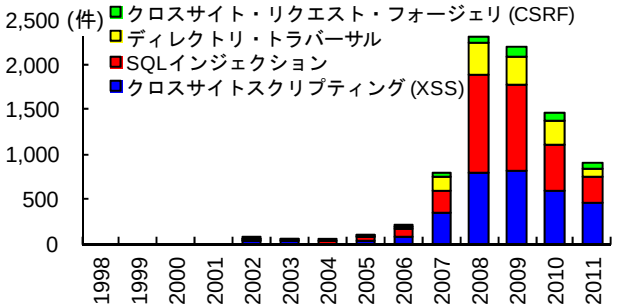


図 7：Web 系ソフトウェア製品の
脆弱性報告件数の推移(出典：NIST NVD)

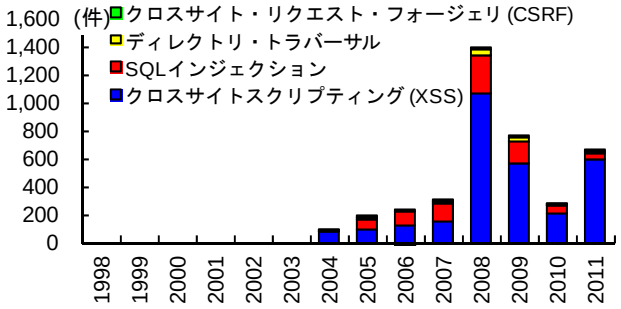


図 8：Web サイトの脆弱性報告件数の推移
(出典：IPA，JPCERT/CC)

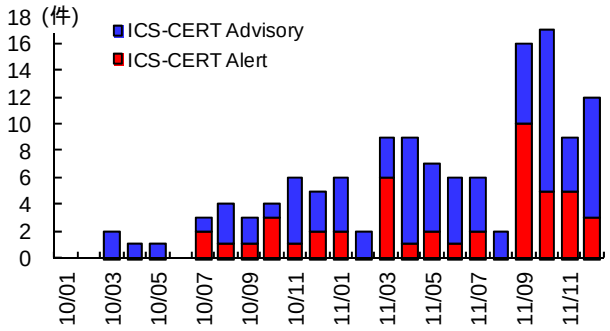


図 9：制御システム製品の脆弱性報告件数の推移
(出典：ICS-CERT)

2.2 HIRT の活動トピックス

本節では，2011 年の活動トピックについて述べる．

(1) 日立グループ CSIRT 活動の向上(フェーズ 1)

2010 年，『日立グループ全体にインシデントオペレーション活動を浸透させていくこと』を目標として日立グループ CSIRT 活動の向上を開始した(図 11)．2 年目となる 2011 年は，フェーズ 1 の終了年として，事業部・グループ会社 IRT と連携した支援活動サイクル(課題抽出，分析・対策検討，対策展開)の定着化に注力した(図 10)．

- **2010 年度再度確認しておきたいチェックポイントの作成**

サイクルの定着化にあたり，セキュリティレビューやインシデント対応支援を通して明らかとなった課題については，代表的な数項目に絞り込んだチェックポイントとしてまとめ，対策展開に利用した．

- **HIRT オープンミーティング『技術編』の拡充**

対策展開の一環として，既存ドキュメントの利活用を促すことを意図したセキュリティ基本仕様書作成ガイドの講習会，セキュリティ対策に対する取り組みを客観的に再考するという意味での外部講師による講演を中心に『技術編』の拡充を図った(表 3)[*b]．

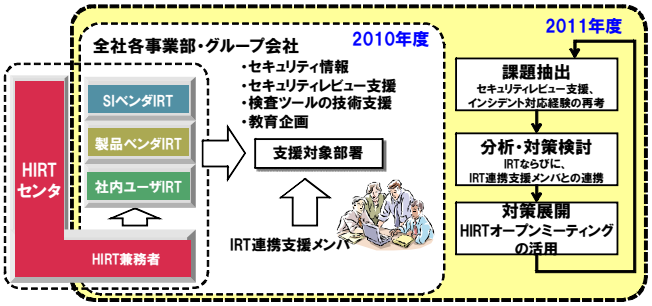
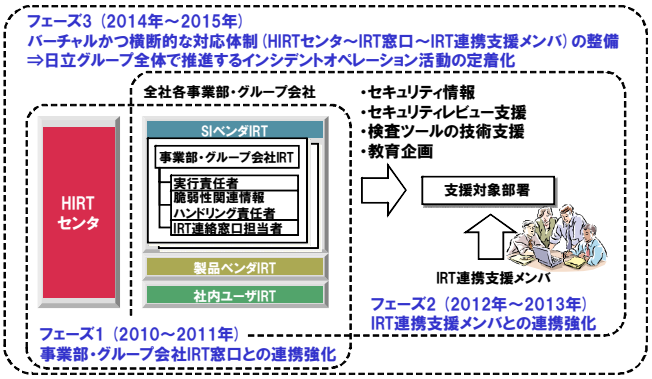


図 10：フェーズ 1 の活動



分類	具体的な施策
フェーズ 1 (2010 年～2011 年)	事業部／グループ会社 IRT 窓口との連携強化 ➢ 事業部／グループ会社 IRT と HIRT センタ連携による各種支援活動の推進 ➢ HIRT オープンミーティングを活用した，IRT 連携の運営体制，技術ノウハウの展開体制の整備 ➢ セキュリティレビュー支援などから得られた課題の解決に向けた対策展開
フェーズ 2 (2012 年～2013 年)	IRT 連携支援メンバとの連携強化 ➢ IRT 連携支援メンバ(事業部・グループ会社)制度の試行 ➢ IRT 連携支援メンバを起点とした IRT 活動のボトムアップ
フェーズ 3 (2014 年～2015 年)	バーチャルかつ横断的な対応体制の整備 ➢ HIRT センタ～IRT 窓口～IRT 連携支援メンバによる各種支援活動の推進 ➢ ユーザ連携モデル(フェーズ 1, 2) と組織連携モデル(フェーズ 3) 融合による広義の HIRT(バーチャル組織体制) の構築

図 11：日立グループ CSIRT 活動の向上

表 3：2011 年 HIRT オープンミーティング『技術編』

年月	概要
2011 年 4 月	[演習] USB ウィルス感染のフォレンジック
2011 年 6 月	セキュリティ基本仕様書作成ガイド：導入編 ～基本仕様書作成ガイドの概要とその使い方～
2011 年 7 月	[演習] セキュリティ基本仕様書作成ガイド：実践編 ～ワークシート 1 を用いたグループ討議～
	セキュリティ基本仕様書作成ガイド：応用編 【外部講師】 HASH コンサルティング(株) 徳丸浩氏 『Web アプリ開発のセキュリティ要件定義』
2011 年 9 月	【外部講師】 日本アイ・ビー・エム(株) 徳田敏文氏 『情報漏洩対策現場の苦労と実務 ～悪意ある情報拡散犯の追跡～』
2011 年 11 月	脆弱性情報の見方と効果的な活用方法
2011 年 12 月	【外部講師】 (株)Kaspersky Labs Japan 前田典彦氏 『Android を取り巻く状況(Android マルウェアの動向)』

(2) 制御システム系製品の脆弱性情報の発信

米 ICS-CERT の注意喚起とアドバイザリ発行活動が 2 年目に入り，制御システム系製品の脆弱性報告件数が増えてきたこととと，定常的に報告されている脆弱性の傾向を把握するため，2011 年 9 月から社内向けの情報発信活動において，制御システム系製品の脆弱性を月例で取り上げることとした．これにより，HIRT セキュリティ情報の発行件数が微増している(図 14).

(3) 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[5]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．また，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 と連携し情報発信を実施した[6].

- Web サービス連携を使用した Web サイト経由での攻撃 mstmp について

(4) ITU-T サイバーセキュリティ情報交換フレームワーク CYBEX 標準化活動への協力

国際電気通信連合 標準化部門 ITU-T では，脆弱性対策情報ならびにインシデント対応に関連するフォーマット，番号体系などの技術仕様 CYBEX(Cyber security information exchange framework)シリーズの標準化を進めている．これら技術仕様の普及により，脆弱性対策ならびにインシデント対応の機械処理を推進できる．一方，国内では，2008 年から MyJVN[7]が，CYBEX シリーズの一部を構成する SCAP(Security Content Automation Protocol)を用いた脆弱性対策のため機械処理基盤の整備を進めている．脆弱性対策のための機械処理基

*b) HIRT オープンミーティング
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．『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．
HIRT オープンミーティング『技術編』
HIRT オープンミーティングの主旨の下，設計者，システムエンジニアや技術ノウハウの展開に協力して頂ける方を対象に，製品・サービスセキュリティの作り込みに必要となる技術ノウハウを展開するための会合である．

盤の整備に協力すべく，X.cybex(X.1500)[8]の付録にユースケースとして，米国の FDCC(Federal Desktop Core Configuration：連邦政府共通デスクトップ基準)の取り組みと共に，日本での JVN，MyJVN の取り組みの掲載を推進した．

(5) その他

- FIRST 加盟のスポンサー(推薦チーム) として，MBSD-SIRT(三井物産セキュアディレクション)，MUFG-CERT(三菱 UFJ フィナンシャルグループ)の加盟を支援
- 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[9].
- HIRT で推進している取り組みをレポート形式にまとめてセキュリティ情報統合サイトに掲載(表 4).

表 4：セキュリティ情報統合サイト掲載レポート

番号	題名
HIRT-PUB10008 (英語版)	Hitachi Vulnerability Disclosure Process
HIRT-PUB11003	P2P ファイル交換ソフト環境で流通するマルウェア(2011 年)
HIRT-PUB11002	2010 年 HIRT 活動報告(HIRT: Annual Report 2010)
HIRT-PUB11001	ゼロディに関する対応経緯(2011 年)

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 12，表 5)．日立グループの場合には，情報システムや制御システムなどの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．4 つの IRT では，ここに，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で推進する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，4 つの IRT が整備されるまでには，表 6にある 4 段階ほどのステップを踏んでいる．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おり，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[10]が多くの製品に影響を与えたことが後押しとなった．また，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．HIRT センタは，3 つの IRT の大枠が決まった後に，社内外の調整役を担う組織として構成されたという経緯がある．

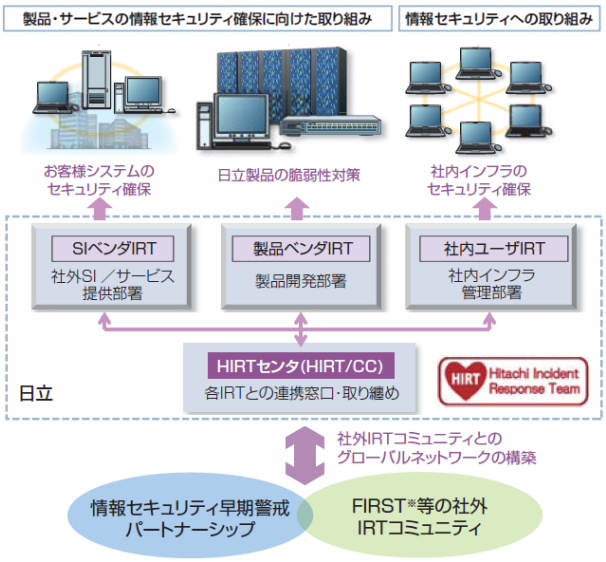


図 12：組織編成モデルとしての 4 つの IRT

表 5：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 6：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・通信システム社配下に設置されており，社内外の調整役だけではなく，セキュリティの技術面を牽引する役割を担っている．主な活動は，製品／サービスセキュリティ委員会活動の技術支援，IT 戦略本部／情報システム事業部／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 13).

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，情報システムや制御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

HIRT センタの主な活動には，社内向けの CSIRT 活動(表 7)と，社外向けの CSIRT 活動(表 8)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．

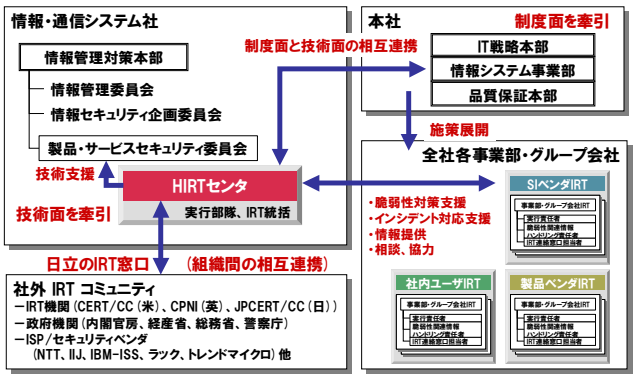


図 13：HIRT センタの位置付け

表 7　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	➢ 事業部／グループ会社 IRT 窓口との連携強化(フェーズ 1) ➢ 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 ➢ Web 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	➢ 横浜研究所との共同研究体制の整備

表 8　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[*c]
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(MWS)[11] など学術系研究活動への参画

*c) ISO SC27/WG3 では 2007 年から『脆弱性情報の開示(29147)』，2010 年から『脆弱性対応手順(30111)』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(CYBEX)』の標準化活動を開始した.

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 9，図 14)．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，IT 戦略本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 9：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 Web 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．

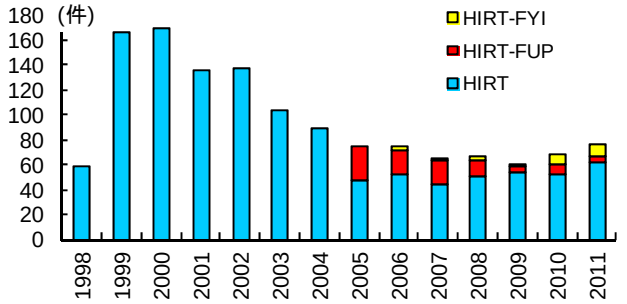


図 14：識別番号別セキュリティ情報の発行数

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 Web 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 15).

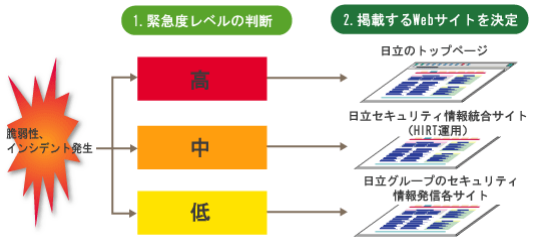


図 15：緊急度レベル×階層レベル型の情報発信の概念図

4 1998 年～2010 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 2010 年

(1) 日立グループ CSIRT 活動の向上(フェーズ 1)の始動

日立グループ CSIRT 活動の向上として，『日立グループ全体にインシデントオペレーション活動を浸透させていくこと』を目標に，フェーズ 1 の活動を開始した．フェーズ 1 の初年度となる 2010 年は，脆弱性関連情報ハンドリング責任者／IRT 連絡窓口担当者連絡会『事務編』『技術編』開催の定着に注力した．

- 事務編(1 回／期)：脆弱性関連情報ハンドリング責任者，IRT 連絡窓口担当者を対象に，IRT 活動に必要となる運営ノウハウの共有ならびに継承を目的とした会合
- 技術編(2～4 回／期)：設計者，システムエンジニアや技術ノウハウの展開に協力して頂ける方を対象に，製品・サービスセキュリティの作り込みに必要となる技術ノウハウを展開するための会合

(2) CSIRT コミュニティとの組織間連携の強化

2010 年 12 月に，日本シーサート協議会の国際連携ワークショップ開催を支援した．また，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 と連携し情報発信を実施した[6].

- ガンブラーウイルス対策まとめサイト
- ボットネット PushDo による SSL 接続攻撃
- マルウェア Stuxnet(スタクスネット) について

(3) その他

- 2010 年 7 月，インドネシアの学術系 CSIRT 活動を支援するため，JPCERT/CC と協力して，ワークショップ『Academy CERT Meeting』の開催を後援[12]
- 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[13]

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，2007 年以降，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(図 16).

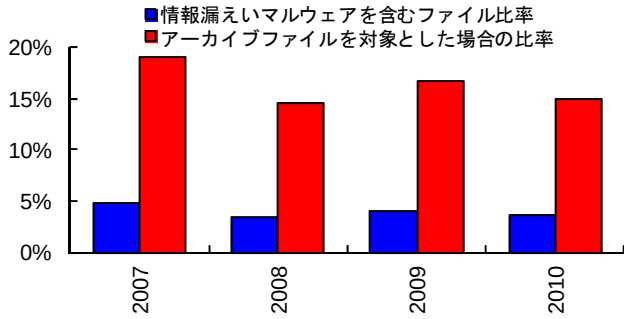


図 16：Winny に流通する情報漏えいを引き起こすマルウェアの推移

4.2 2009 年

(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(図 17).

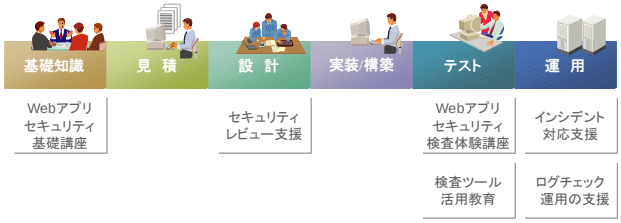


図 17：HIRT 支援活動の体系化
(Web アプリケーションのセキュリティ)

(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，Web 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.

(3) 講演会

- 2009 年 7 月：(独)産業技術総合研究所 高木浩光氏『Web アプリケーションセキュリティ』
- 2009 年 7 月：NTT-CERT 吉田尊彦氏『NTT-CERT の活動取り組み』

(4) その他

- 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[14]
- 2009 年 2 月：NTT-CERT 主催のワークショップにおいて，NTT グループ向けに Web アプリケーション開発の演習を実施
- 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)[15]を用いた情報発信を開始.

4.3 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』[16]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[17].

(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[18].

(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.

4.4 2007 年

(1) 演習型 HIRT オープンミーティングの開始

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図るため，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[19]．2011 年 4 月現在，27 チームが加盟している(図 18).

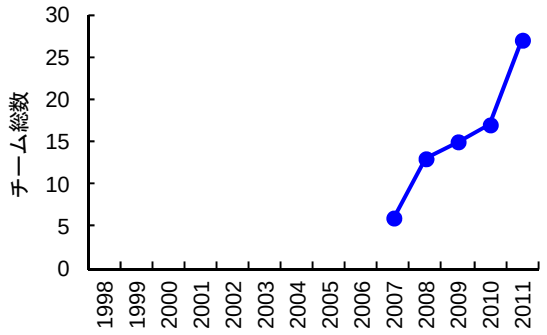


図 18：日本シーサート協議会加盟チーム数の推移

(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[20].

(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』

4.5 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 Web 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 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日立グループ向けの脆弱性届出統合窓口を設置した.

(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を開始[21]

4.6 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[22]．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.

2012 年 4 月現在，計 252 チームが加盟している．日本からは，CDI-CIRT(サイバーディフェンス研究所)，CFC(警察庁情報通信局)，FJC-CERT(富士通)，HIRT(日立)，IIJ-SECT(IIJ)，IPA-CERT(情報処理推進機構), JPCERT/CC, JSOC(ラック), KDDI-SOC(KDDI), KKCSIRT(カカクコム)，MBSD-SIRT(三井物産セキュアディレクション)，MIXIRT(ミクシィ)，MUFG-CERT(三菱 UFJ フィナンシャルグループ),

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)，NTTDATA-CERT(NTT データ)，Panasonic PSIRT(パナソニック)，Rakuten-CERT(楽天)，RicohPSIRT(リコー)，SBCSIRT(ソフトバンク)，YIRD(ヤフー)の 22 チームが加盟している(図 19).

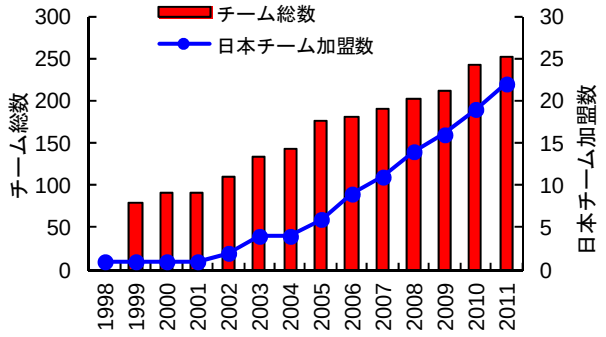


図 19：FIRST 加盟チーム数の推移

(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 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 20). 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/

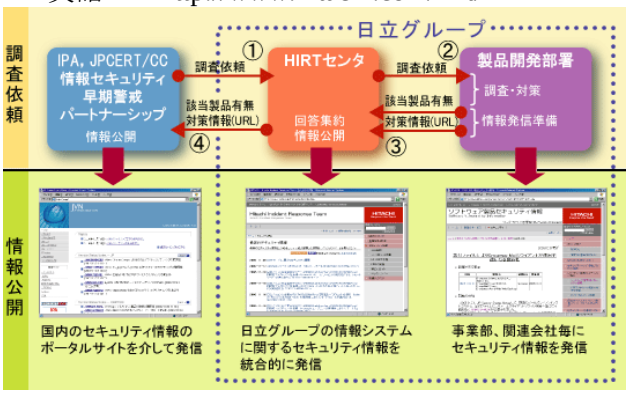


図 20：統合サイトでのセキュリティ情報発信

(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，Web サイト改ざん発見時の通知などの連絡網を整備した.

4.7 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[23][24], 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)[25]への脆弱性対策の状況掲載を開始した.

(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) 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』

4.8 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[26].

表 10：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 1-1-2
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[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 10に示す連絡窓口を設置した．

4.9 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[10]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 の立上げと，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)(http://jvn.doi.ics.keio.ac.jp/) の構築と運用を支援した(図 21)[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がれている．

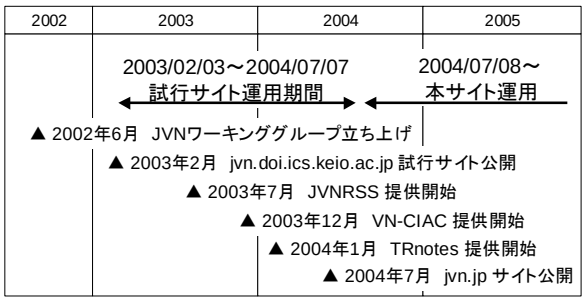


図 21：JVN 試行サイトの構築ならびに運用

4.10 2001 年

(1) Web 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 Web 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 Web 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 22) 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．

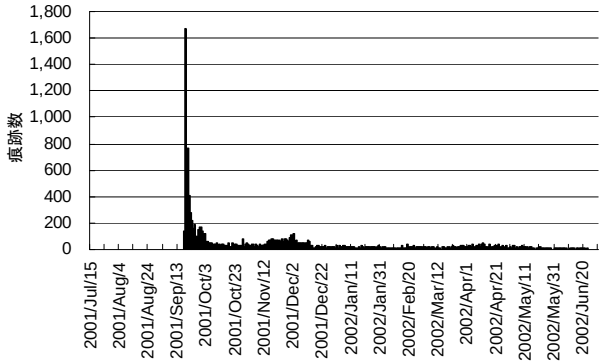


図 22：観測期間内の痕跡数変位(Nimda)

4.11 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]. MITRE が推進する 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 FIRST が推進する CVSS(共通脆弱性評価システム)[36]が利用され始めた．

4.12 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，Web サイト 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．1999 年～2002 年にかけ，侵害活動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 23).

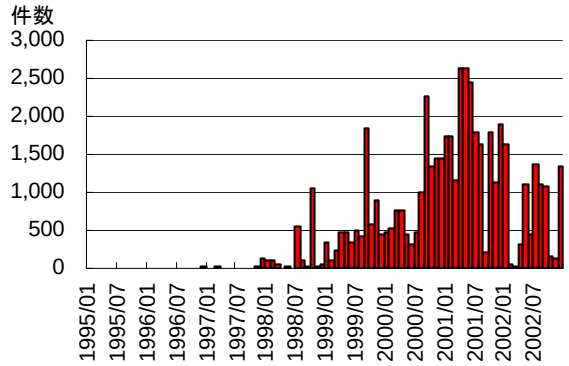


図 23：Web サイトの書き換え件数の推移

4.13 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 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[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

情報セキュリティ施策の全てを強固にすれば自由度が下がり，ビジネススピードに対応できず，また，情報セキュリティ施策を自己責任の下，個々の対応とすれば，ひとつの破綻が連鎖的なセキュリティインシデントにつながる．バランスの取れたサイバー攻撃対策の実現手段の一つとして，CSIRT を活用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, CSIRT コミュニティでの先導的な活動を通して，サイバー攻撃対策における CSIRT の活用を具現化していく予定である．

(2013 年 4 月 30 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/monthlyreport/index.html
2) Conficker Work Group - ANY - InfectionTracking, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking
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) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), http://www.ntt-cert.org/
6) 日本シーサート協議会：インシデント対応まとめサイト, http://www.nca.gr.jp/2010/incidentresponse.html
7) (独)情報処理推進機構： 脆弱性対策情報共有フレームワーク, http://jvndb.jvn.jp/apis/myjvn/index.html
8) ITU-T X.1500 : Overview of cybersecurity information exchange, http://www.itu.int/rec/T-REC-X.1500-201104-I
9) ITpro セキュリティ, http://itpro.nikkeibp.co.jp/security/
10) 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
11)マルウェア対策研究人材育成ワークショップ, http://www.iwsec.org/mws/2011/
12) SGU MIT Workshop Academy CERT Meeting (2010/7), http://idsirtii.or.id/academy-cert-meeting/
13) P2P ファイル交換ソフト環境で流通するマルウェア(2011 年) (2011/9), http://www.hitachi.co.jp/hirt/publications/hirt-pub11003/index.html
14) 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
15) cNotes: Current Status Notes, http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi
16) (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
17) Joint Workshop on Security 2008, Tokyo 開催記録サイト (2008/3), http://www.nca.gr.jp/jws2008/index.html
18) 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/archives/project/gekkan/2008/ceremony/prize02.html
19) 日本シーサート協議会, http://www.nca.gr.jp/
20) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/
21) GlobalSign Adobe Certified Document Services, http://jp.globalsign.com/solution/example/hitachi.html
22) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/
23) 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
24) (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
25) JVN (Japan Vulnerability Notes), http://jvn.jp/
26) 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
27) (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
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/yrl/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/ (not available)
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，テレコム・アイザック推進会議運営委員，日本シーサート協議会の副運営委員長を務める．