2015 年 HIRT 活動報告
HIRT: Annual Report 2015

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

〒140-0013 東京都品川区南大井 6-26-3 大森ベルポート D 館
OMORI BELLPORT Tower D, 6-26-3 Minamioi, Shinagawa, Tokyo, Japan 140-0013

1 はじめに

影響の大きなインシデントが発生すると，対策アプローチにも大きな変化が見られる．2006 年に発生したファイル共有ソフトによる情報漏えいは端末の Thin クライアント化, 2011 年の防衛産業企業他への標的型攻撃は出口対策の導入，そして，2015 年の同種のサイバー攻撃の多発は安全が確認できるまで止めるというリスク減算型対策の再認識である (図 1)．ここで安全が確認できるまで止めるというアプローチの意図するところは，潜在的な脅威残存期間とサービス停止時間を短くすることにある (図 2)．言い換えれば，攻撃者のサイバー攻撃スピードへの追従である．

しかも，2010 年以降注目を集めている APT (Advanced Persistent Threat ; 攻撃対象を狙い撃ちした高度な潜伏型攻撃) に代表される標的型攻撃は，

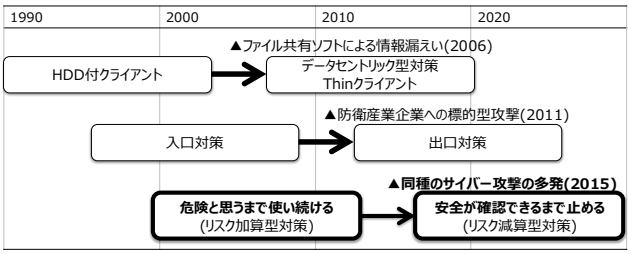


図 1：対策アプローチの変化

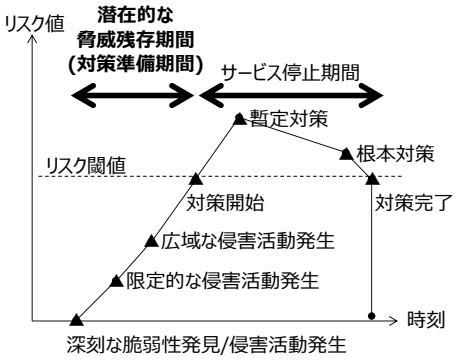


図 2：潜在的な脅威残存期間

侵害活動の成果が次の標的型攻撃に利用される踏み台型であり，最終目標となる特定組織への侵害活動につながっている．すなわち，セキュリティ対策やインシデント対応が，少なからず他組織に影響を与える／他組織の影響を受ける構図となっていることから，CSIRT を活用した組織間での専門的，実務的な連携にもスピードアップが求められてくることにもなる．

CSIRT (Computer/Cyber Security Incident Response /Readiness Team) としての HIRT (Hitachi Incident Response Team) の具体的な役割は，『脆弱性対策：サイバーセキュリティに脅威となる脆弱性を除去するための活動』と『インシデント対応：発生しているサイバー攻撃を回避並びに解決するための活動』を通じて，日立グループのサイバーセキュリティ対策活動を先導していくことに変わりはない．

また，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．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 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洩などのインシデント対応を先導すると共に，日立グループの CSIRT 統一窓口組織としての役割を担っている．

本稿では, 2015 年の HIRT 活動の報告として, 2015 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 2015 年の活動概要

本章では，2015 年の脅威と脆弱性の概況，HIRT

の活動を報告する．

2.1　脅威と脆弱性の概況

(1) 脅威の概況

標的型攻撃，Web サイトの侵害など，既知の脅威による被害は継続している状況にある．

2015 年のインシデントの特徴としては，インターネットバンキングを対象とした不正プログラムによる被害の深刻化が挙げられる．一方，攻撃手法としては，パソコン内のファイルを人質にとるランサムウェア攻撃，要求／応答のメッセージ増幅を利用した増幅攻撃 (いわゆる，リフレクター攻撃) の定常化が挙げられる．

- **インターネットバンキング**

警察庁の報告によれば，2015 年の国内の不正送金被害は計 1,495 件 (2014 年の 0.8 倍)，被害総額は約 30 億 7,300 万円 (2014 年の 1.05 倍) に上っている (図 3) [1]．特徴としては，信用金庫の法人口座被害が急増し，法人名義口座に係る被害額が過去最悪を記録した．

- **Web サイト侵害活動**

2013 年 3 月以降，国内 Web サイトでは，ホームページ誘導型マルウェア感染を意図したページ改ざん事案が続いている．報告件数を見ると，2009 年に発生したガンブラー (Gumblar) 事案のときよりも，多くの改ざんが発生している状況は継続している (図 4)．

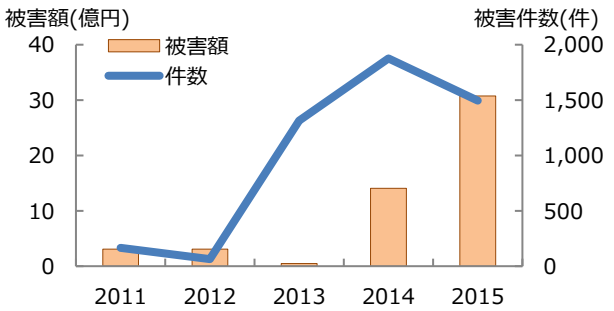


図 3：不正送金事案の年別被害件数と被害額
(出典：警察庁)

- **ランサムウェア**

ランサムウェアは，パソコン内のファイルを人質にとる不正プログラムの総称である．2015 年以降，特に，パソコン内のファイルを暗号化し，その暗号解除と引き換えに金銭を要求するランサムウェアは急増している．シマンテックの報告[2]によれば，64%がパソコン内のファイルを暗号化する暗号型，36%がパソコンへのアクセスを制限するロック型で，日本での発見件数は第 2 位としている．また，マカフィの報告[3]によれば，ランサムウェアの合計数は 2014 年よりも 127%増加，2015 年第 2 四半期だけで約 120 万の新たな検体が発見されたとしている．

重要なファイルがランサムウェアによって暗号化されてしまった場合には，事業継続に直接的影響を与えるため，バックアップの取得だけではなく，バックアップからの回復にも目を向けていく必要がある．

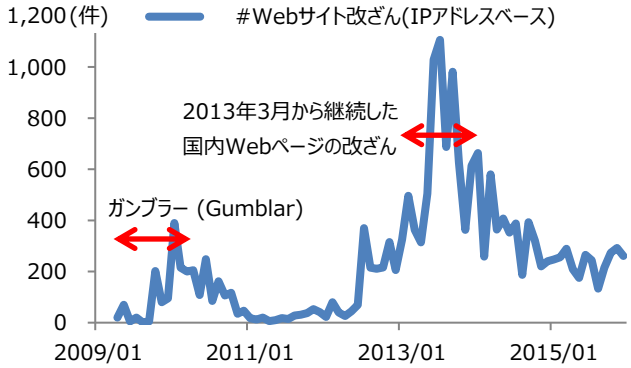


図 4：Web サイトのページ改ざんの報告件数
(出典：JPCERT/CC)

表 1：2013 年以降の代表的なランサムウェア

時期		ランサムウェア名
2013 年	9 月	CryptoLocker
	12 月	CryptoLocker 2.0
2014 年	2 月	CryptoDefense
	3 月	CryptoWall 1.0
	5 月	ANDROIDOS_LOCKER.HBT(Android 環境)
	7 月	CTB-Locker
	8 月	TorrentLocker
	10 月	CryptoWall 2.0
	11 月	Coinvault
2015 年	1 月	CryptoWall 3.0
	2 月	TeslaCrypt
	3 月	CRYPVAULT
	7 月	TeslaCrypt 2.0
	9 月	Chimera，TeslaCrypt 2.1
	11 月	CryptoWall 4.0，Linux.Encoder(Linux 環境)
	12 月	TeslaCrypt 2.2

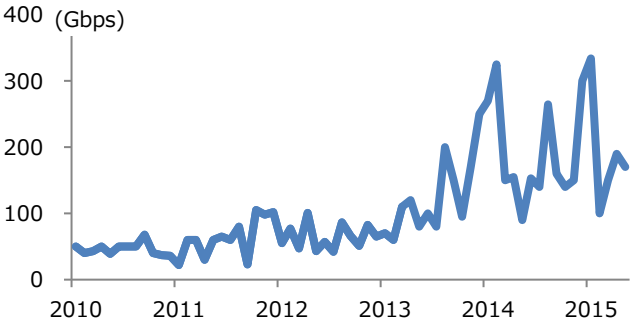


図 5：DDoS 攻撃のピークトラフィックの推移
(出典：Arbor Networks) [4]

● **リフレクター攻撃**

DDoS 攻撃のピークトラフィックは増加傾向にあり (図 5) , DDoS 攻撃の脅威は継続している. Arbor Networks の報告[4]によれば，1Gbps を超える攻撃が 2 割を超え，DrDoS (Distributed Reflective Denial of Service，分散リフレクター型のサービス不能) 攻撃については, 攻撃トラフィックは増加し, 特に, UPnP (Universal Plug and Play) 対応機器の SSDP (Simple Service Discovery Protocol) を用いた攻撃が顕在化してきたとしている.

また，サービス停止を意図して DDoS 攻撃を仕掛け，攻撃を停止する身代金としてビットコインを要求する DD4BC(DDos for Bitcoin)と呼ばれる攻撃においても, SSDP と NTP のリフレクター攻撃, Wordpress XML-RPC のリフレクター攻撃が利用されたとしている[5]. DD4BC は，2014 年半ばから各国で被害が目立ち始め，2015 年には，日本国内でも被害が報告されている.

(2) 脆弱性の概況

● **全体傾向**

米 NIST NVD (National Vulnerability Database) [6] に登録された 2015 年の脆弱性の総件数は 6,488 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 (1,319 件) を占めており (図 6)，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 7 割を占めるという状況が続いている (図 7). 同じく，IPA に報告された稼動中 Web サイトの脆弱性の報告件数は，例年に比べて減っているものの，約 6 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いる (図 8) [7].

● **制御システム製品**

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 10 件，126 件である (図 9).

脆弱性種別としては，スタックオーバーフロー (CWE-121)，クロスサイトスクリプティング (CWE-79)，入力データの検証が適切ではないこと (CWE-20) に起因する脆弱性が上位を占め，パスワードがハードコーディングされている問題 (CWE-798) も引き続き報告されている. また，アナログ伝送の信号に，デジタル信号を重畳して伝送する方式 HART (Highway Addressable Remote Transducer) を実装する DTM (Device Type Manager) 製品の脆弱性に関するものが 10 件, 医療分野では点滴システムの脆弱性に関するものが 6 件報告された.

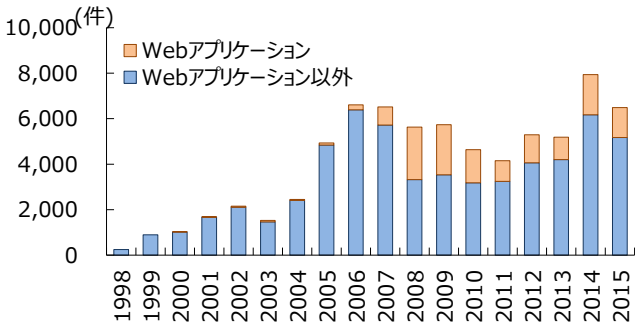


図 6：脆弱性報告件数の推移 (出典：NIST NVD)

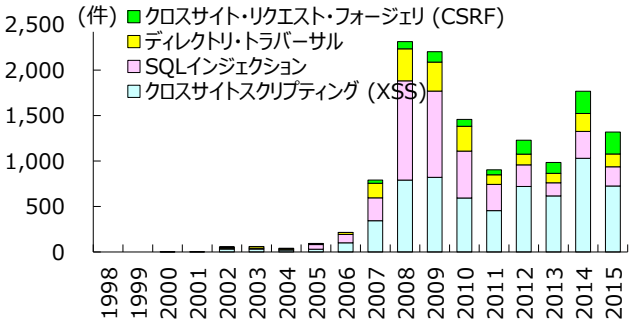


図 7：Web 系ソフトウェア製品の脆弱性報告件数の推移 (出典：NIST NVD)

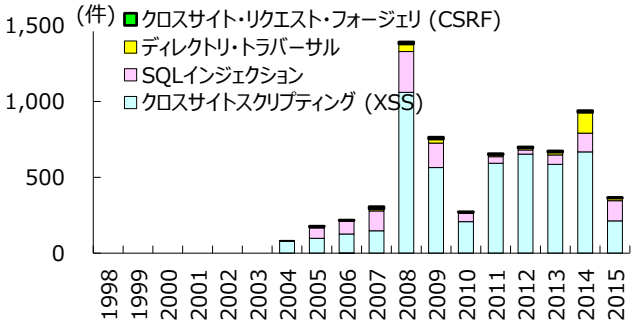


図 8：Web サイトの脆弱性報告件数の推移 (出典：IPA，JPCERT/CC)

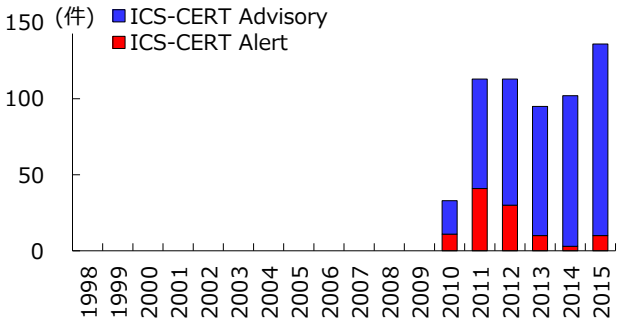


図 9：制御システム製品の脆弱性報告件数の推移 (出典：ICS-CERT)

2.2　HIRT の活動トピックス

(1) 日立グループ CSIRT 活動の向上 (フェーズ 3)

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)．6 年目となる 2015 年は，最終年として，バーチャルかつ横断的な対応体制 (HIRT センタ～IRT 窓口～IRT 連携支援メンバ) を実現するために規則面の強化を図った．具体的には，今後の運用を踏まえ，セキュリティインシデント対策の関連規則に，事業部 IRT の役割として，「セキュリティ対応体制の構築と維持」を規定するなどを推進した．

また，技術継承については，HIRT オープンミーティング『技術編』開催 (表 2) [*a]，IRT 連携支援メンバとの会合であるアドバンスド HIRT オープンミーティングの大甕地区開催に加えて，2014 年横浜研究所内に開設した HIRT ラボプロジェクトルームを利用し，標的型攻撃などのサイバー攻撃を調査するために構築した組織内ネットワークの擬似環境下で侵入後の攻撃者の行動を記録し分析する「動的活動観測」(図 10)，STIX/TAXII [*b]を用いた組織間でのサイバーセキュリティ情報活用[8]に取り組み始めた．

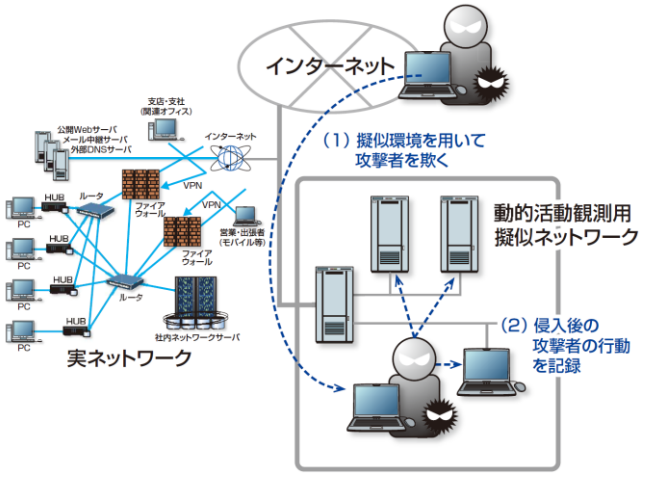
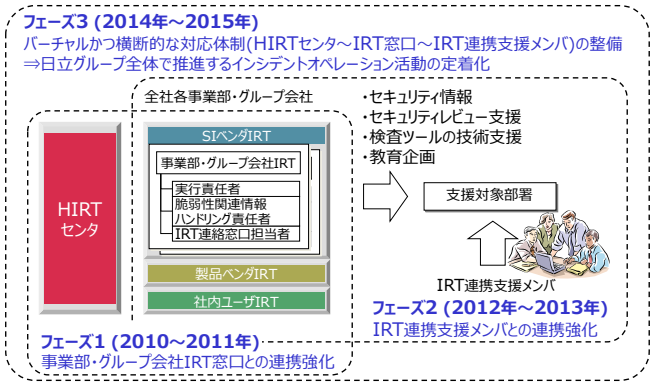


図 10：攻撃者の行動を記録する動的活動観測



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 2：HIRT オープンミーティング『技術編』

年月	概要
2015 年 1 月	アドバンスド HIRT オープンミーティング
	フォレンジック調査(体験編)のハンズオン
2015 年 2 月	【外部講師】 三井物産セキュアディレクション(株)　国分裕氏，寺田健氏 『脆弱性発見の立場から』
2015 年 3 月	アドバンスド HIRT オープンミーティング @大甕地区
2015 年 4 月	社外サーバの脆弱性検査における技術対策セミナー
2015 年 7 月	【外部講師】 一般社団法人 JPCERT コーディネーションセンター　Jack YS LIN (林 永熙) 氏 『「サイバー強国」になりうるか -中国-』
2015 年 8 月	アドバンスド HIRT オープンミーティング
2015 年 9 月	Windows イベントログ調査のハンズオン

(2) 分野別 IRT 活動の試行

- **HIRT-FIS におけるレディネス活動の推進**

分野別視点を取り込んだインシデントレスポンス＋レディネス 3 層サイクル (図 12) を実践するため，HIRT-FIS (Financial Industry Information Systems HIRT) が主体となり，金融分野における社内外のレディネス活動を推進した．社外対応としては，金融

*a) 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．

*b) STIX (Structured Threat Information eXpression: 脅威情報構造化記述形式)は，サイバー攻撃活動を記述するための XML 仕様．TAXII (Trusted Automated eXchange of Indicator Information: 検知指標情報自動交換手順)は，脅威情報を交換するための手順．情報活用基盤の仕様として注目されている．

系 CSIRT との連携を模索するための HIRT-FIS セキュリティノートの週次配信の拡大，金融系 CSIRT との意見交換会の実施を通して，日本シーサート協議会の加盟を支援した．

HIRT-FIS セキュリティノートは，国内外で発生した金融関連のセキュリティインシデントや関連規則などの話題を取り上げた簡易レポートである(表 3，図 13)．

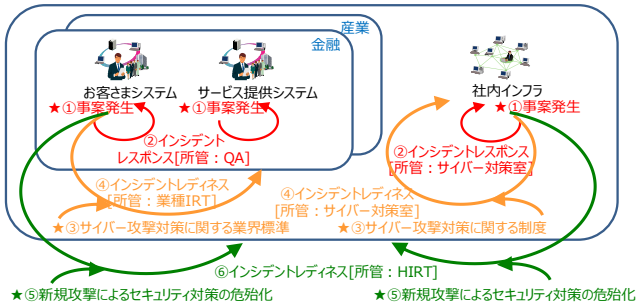


図 12:インシデントレスポンス＋レディネス 3 層サイクルの概念

表 3：HIRT-FIS セキュリティノート

項目	2013 年	2014 年	2015 年
発行数	10 件	48 件	48 件
受信者数	4 名	9 名	35 名
受信組織数	2 組織	5 組織	22 組織

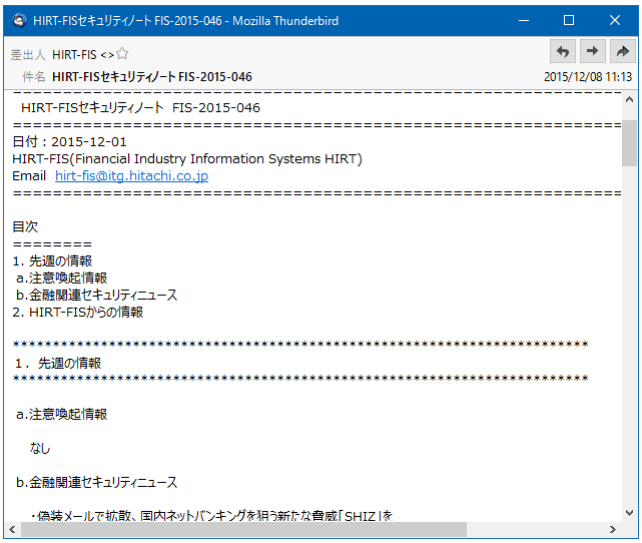


図 13：金融系 CSIRT 向けに週次配信している HIRT-FIS セキュリティノート

(3) CSIRT コミュニティとの組織間連携の強化

日本シーサート協議会への加盟を支援すると共に(表 4)，SSH サーバセキュリティ設定検討 WG と連携し「SSH サーバセキュリティ設定ガイド V1.0」を発行した[9].

表 4：日本シーサート協議会への加盟支援

加盟年月	加盟チーム名
2015 年 3 月	MY-SIRT (明治安田生命保険相互会社)
2015 年 10 月	AHIRU (アフラック)
2015 年 11 月	MELCO-CSIRT (三菱電機(株))

(4) 第 11 回「情報セキュリティ文化賞」受賞

他社に先駆けた企業内 CSIRT の立ち上げ，同分野の国際的なフォーラムである FIRST に国内メーカとして最初に加盟するなどの積極的な活動が評価され，情報セキュリティ大学院大学の「情報セキュリティ文化賞」を受賞しました[10].

(5) その他

- MWS (マルウェア対策研究人材育成ワークショップ) 2015 への参画[14]
  マルウェア対策の研究活動を支援していくと共に，支援を通して次世代の CSIRT コミュニティの醸成への寄与を目指している．
- 日経 BP 社 ITpro CSIRT 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[11]

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 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 14，表 5)．日立グループの企業活動をインシデント対応からみると，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おり，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』[33][34]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．

さらに，2010 年からは，バーチャルかつ横断的な対応体制を整備し，『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』を目標とした日立グループ CSIRT 活動の向上を推進している．

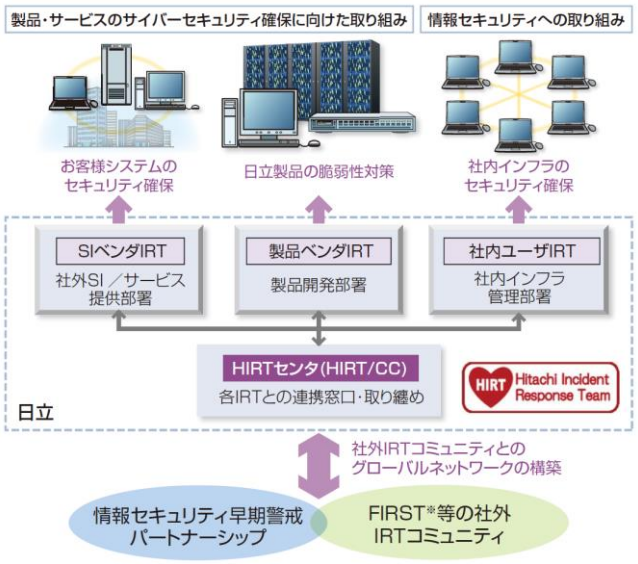


図 14：組織編成モデルとしての 4 つの IRT

表 5：各 IRT の役割

分類	役割
HIRT/CC	該当部署：HIRT センタ > FIRST，日本シーサート協議会, 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．
2010 年～	日立グループ CSIRT 活動の向上 目標：インシデントオペレーション活動の日立グループ全体への浸透

3.2 HIRT センタの位置付け

HIRT センタは，情報・通信システム社の配下に設置されているが，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．主な役割は，IT 戦略本部／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 15).

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，情報ならびに制御システムを構成する機器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 8) と社外向けの CSIRT 活動 (表 9) 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している．

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 7，図 16)．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．

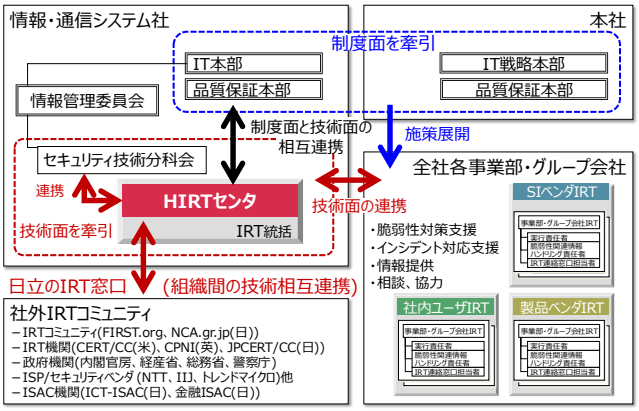


図 15：HIRT センタの位置付け

表 7：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．

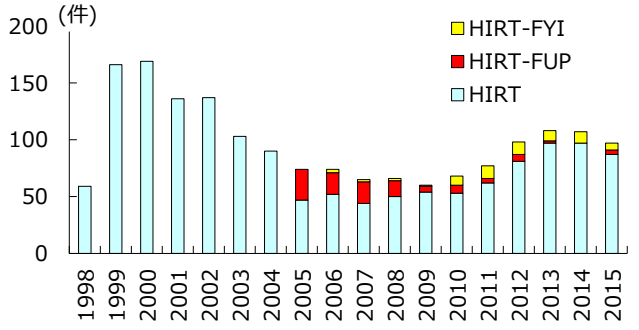


図 16：識別番号別セキュリティ情報の発行数

表 8　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) のコンセプト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 3) > 脆弱性対策とインシデント対応のための技術継承 > 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 (脆弱性対策を仕様，コード，設定の 3 つ視点からアプローチするとともに，先行事例作りを推進)
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 9　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 (Warning, Advice and Reporting Point) 関連活動の推進 > CVE (共通脆弱性識別子)，CVSS (共通脆弱性評価システム)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][13]
研究活動基盤の整備	> 明治大学 (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) [14] など学術系研究活動への参画

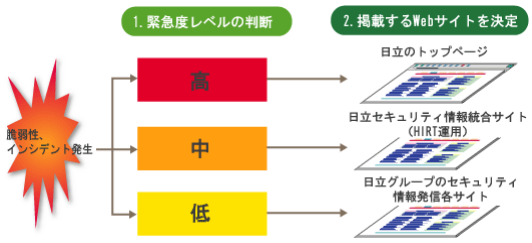


図 17：緊急度レベル×階層レベル型の情報発信

*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，2014 年 2 月，2013 年 11 月に IS 化が完了した．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) 』の標準化活動を推進してきた．

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．特に，社外向け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，情報の『緊急度レベル』×掲載 Web サイトの『階層レベル』を組合せた情報発信アプローチを併用している (図 17).

4　1998 年～2014 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について述べる．

4.1　2014 年

(1) 日立グループ CSIRT 活動の向上 (フェーズ 3)

5 年目となる 2014 年は，フェーズ 3 の開始年として，HIRT ラボプロジェクトルームを横浜研究所の施設内に開設した．このプロジェクトルームは，技術継承の場であり，支援活動ならびに研究所との協働の拠点として活用することを目的としている．

(2) 分野別 IRT 活動の試行

- **HIRT-FIS におけるレディネス活動の推進**

金融分野における社外レディネス活動として，HIRT-FIS セキュリティノートの週次配信の拡大，金融系 CSIRT との意見交換会の実施を通して，日本シーサート協議会の加盟を支援した．

- **制御システム製品向け脆弱性対策**

制御システム製品向け脆弱性対策として，仕様，コード，設定の 3 つ視点からの取り組みを開始した．

(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[15]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への加盟支援 (表 10)，SSH サーバセキュリティ設定検討 WG の立ち上げ，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[20].

- GNU bash の脆弱性 ～shellshock 問題～ について
- Struts: ClassLoader の操作を許してしまう脆弱性 (CVE-2014-0094, CVE-2014-0112, CVE-2014-0113) について
- OpenSSL 情報漏洩を許してしまう脆弱性 ～Heartbleed 問題～ について

表 10：日本シーサート協議会への加盟支援

加盟年月	加盟チーム名
2014 年 5 月	YMC-CSIRT (ヤマハ発動機(株))
2014 年 10 月	NISSAY IT CSIRT (ニッセイ情報テクノロジー(株))
2014 年 11 月	MS&AD-CSIRT (MS&AD インシュアランス グループホールディングス(株))

(5) 講演会

- 2014 年 2 月 : 一般社団法人 JPCERT コーディネーションセンター Jack YS LIN (林 永熙) 氏『中国のセキュリティ事情～DarKnight (中国黒客の夜明け) ～』
- 2014 年 3 月 : (株)インターネットイニシアティブ 根岸征史氏『監視されるインターネット』
- 2014 年 8 月 : トレンドマイクロ(株) 平原伸昭氏『標的型攻撃対策のための一般的な対応フローとビックデータを活用したプロアクティブな対処とプロファイリングとは?』

4.2　2013 年

(1) 日立グループ CSIRT 活動の向上 (フェーズ 2)

4 年目となる 2013 年は，フェーズ 2 の終了年として，HIRT 連携支援メンバ (HIRT センタと協力して，IRT 活動を積極的に推進するメンバ) と共に，サイバーセキュリティ対策のための技術継承の場の定着化を推進した．技術継承にあたっては，サイバー攻撃で使用されるマルウェアなどの動作の『解析』，記録された痕跡から事象を把握する『調査』，サイバー攻撃で対象となりえる脆弱性を明らかにする『評価』の 3 つとした．

(2) 分野別 IRT 活動の試行

- **HIRT-FIS におけるレディネス活動の推進**

金融分野における社外レディネス活動として，HIRT-FIS セキュリティノートの週次配信の試行を開始した．

- **制御システム製品向け脆弱性対策**

HIRT を対外的な窓口の基点とした脆弱性ハンドリング，インシデントハンドリングのための対応体制を整備した (図 18)[16].

(3) CSIRT コミュニティとの組織間連携の強化

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[20].

- 2013 年 3 月から継続している国内 Web サイトのページ改ざん事案について

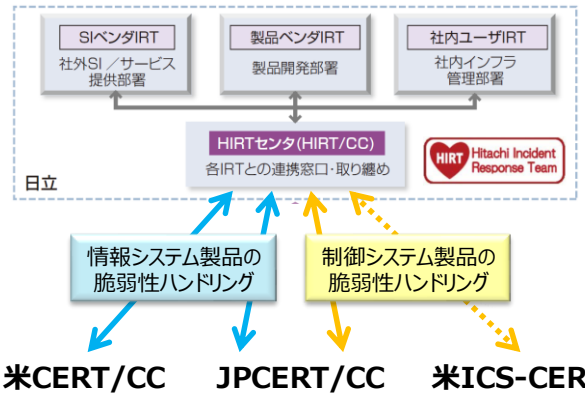


図 18：脆弱性ハンドリングのフレームワーク

(4) (ISC)² Asia-Pacific ISLA 2013 受賞

HIRT が携わっている JVN (Japan Vulnerability Notes) に関わる脆弱性対策活動への貢献が評価され，情報セキュリティ資格 CISSP を運営する (ISC)² の 2013 年アジア太平洋情報セキュリティリーダーシップアチーブメント ISLA (Information Security Leadership Achievements) の Senior Information Security Professional を受賞しました[17].

(5) 講演会

- 2013 年 6 月：ソニーデジタルネットワークアプリケーションズ(株) 松並勝氏『Android アプリのセキュリティとソフトウェア開発現場のセキュリティ活動』
- 2013 年 9 月：(株)サイバーディフェンス研究所 ラウリ コルツパルン氏『制御システムのセキュリティ ～情報系と制御系システムとの融合世代に向けた積極的なアプローチの提案～』

4.3 2012 年

(1) 日立グループ CSIRT 活動の向上 (フェーズ 2)

3 年目となる 2012 年は，HIRT 連携支援メンバを通じた日立グループ内連携の強化を図るフェーズ 2 を開始した.

- HIRT オープンミーティング『技術編』を活用した対策展開
- アドバンスド HIRT オープンミーティングの開始

(2) 分野別 IRT 活動の試行

分野別視点を取り込んだインシデントレスポンス＋レディネス 3 層サイクルというアプローチ (図 12) を取るため，分野別 IRT 活動の試行を開始した. また，金融分野における先行的な取り組みとして，2012 年 10 月 1 日，金融部門内に，HIRT-FIS を設置した (図 19).

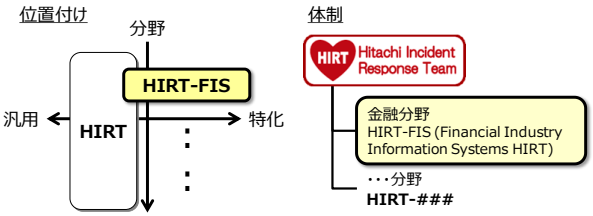


図 19：分野別 IRT 活動の位置付けと体制

(3) CSIRT コミュニティとの組織間連携の強化

- 2012 年 2 月 29 日，CSIRT 活動に関心のある企業担当者を対象に，企業の CSIRT についての意見交換会の場として，CSIRT ワークショップ 2012 を開催[18]
- 2012 年 11 月 13 日～15 日，国内 FIRST 加盟チームと共に，FIRST 技術会議 2012 京都を京都市国際交流会館にて開催[19]
- FIRST 技術会議 2012 京都で取り上げた『脆弱性情報のグローバルな取り扱い』を継続的に検討していくため，FIRST 内に Vulnerability Reporting and Data eXchange SIG (Special Interest Group) を設置

(4) 講演会

- 2012 年 3 月：S&J コンサルティング(株) 三輪信雄氏『組織におけるセキュリティ対策の推進体制』
- 2012 年 8 月：日本オラクル(株) 北野晴人氏『データベース・セキュリティの要素と実装』
- 2012 年 9 月：(独)情報通信研究機構 井上大介氏『サイバー攻撃の動向とサイバーセキュリティ研究の最先端』
- 2012 年 11 月：NPO 情報セキュリティ研究所 上原哲太郎氏『遠隔操作事案・ファーストサーバ問題・うるう秒問題を振り返る』

4.4 2011 年

(1) 日立グループ CSIRT 活動の向上 (フェーズ 1)

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.

(2) 制御システム製品の脆弱性情報の発信

制御システム製品の脆弱性報告件数が増えてきたことと，定常的に報告されている脆弱性の傾向を把握するため，制御システム製品の脆弱性を HIRT セキュリティ情報で取り上げることとした.

(3) CSIRT コミュニティとの組織間連携の強化

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 と連携し情報発信した[20].

- 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) 講演会

- 2011 年 7 月 : 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 : 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 12 月 : (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) 』

(5) その他

- 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

4.5 2010 年

(1) 日立グループ CSIRT 活動の向上 (フェーズ 1) の始動

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』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[20].

- 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[21]
- 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[22]
  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 型の情報漏洩を引き起こす既知マルウェアが多く流通している (図 20).

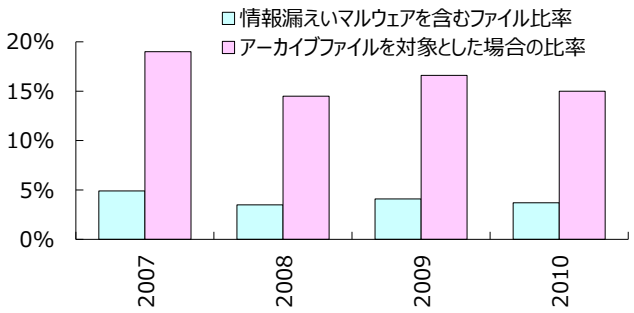


図 20 : Winny に流通する情報漏洩を引き起こすマルウェアの推移

4.6 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 21).

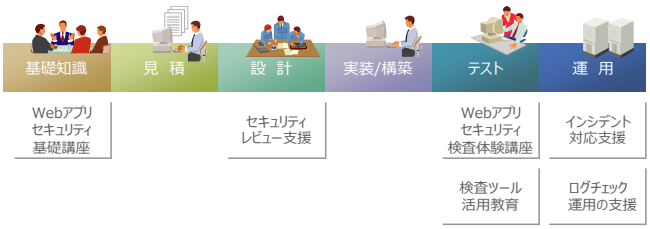


図 21 : HIRT 支援活動の体系化

(2) セキュリティ技術者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研修の一環として, 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[23]
- 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) [24]を用いた情報発信を開始

4.7 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．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』[25]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[26]．

(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，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おいて，『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[27]．

(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[28]．

4.8 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[29]．2015 年 12 月現在，106 チームが加盟している (図 22)．

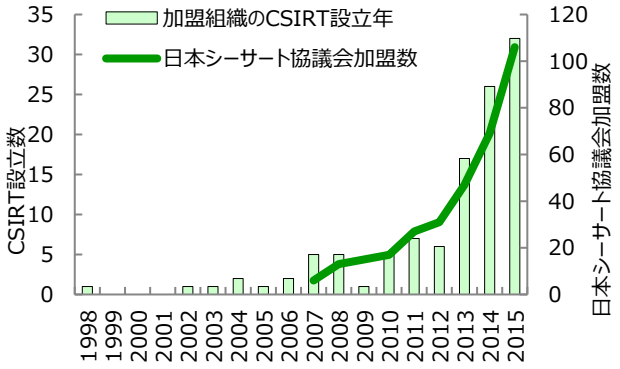


図 22：日本シーサート協議会加盟数の推移

(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[30]．

(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』

4.9 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改訂すると共に，日立グループ内への展開を支援した．

(3) ファイル交換ソフトによる情報漏洩に関する注意喚起

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．感染すると情報漏洩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洩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[31]

4.10 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フォーラムである Forum of Incident Response and Security Teams (FIRST) に加盟した[32]．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．

2015 年 12 月現在，計 345 チームで，日本からは 25 チームが加盟している (図 23) [*d].

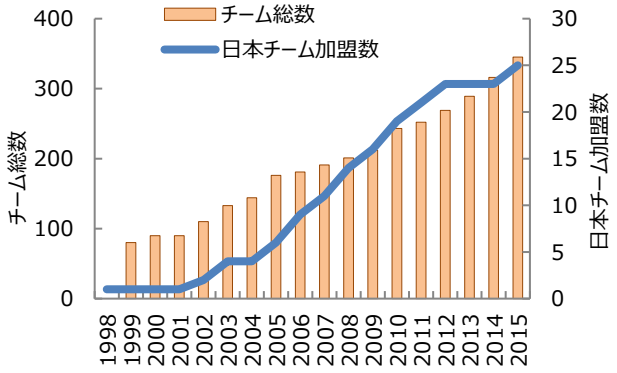


図 23：FIRST 加盟チーム数の推移

(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 24)．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/

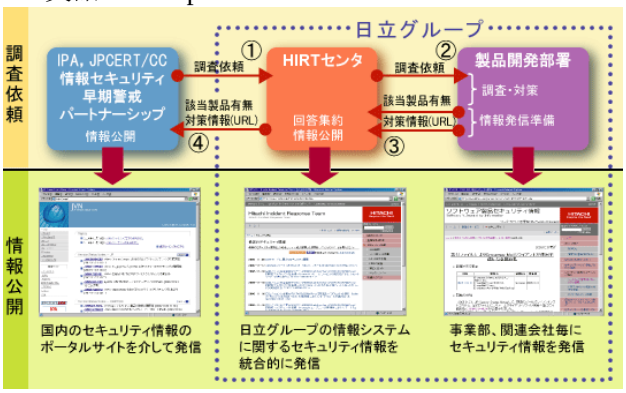


図 24：統合サイトでのセキュリティ情報発信

(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．

4.11 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

*d) CDI-CIRT (サイバーディフェンス研究所)，CFC (警察庁情報通信局)，DeNA CERT (DeNA)，DT-CIRT (デロイトトーマツ)，FJC-CERT (富士通)，Fuji Xerox-CERT (富士ゼロックス)，HIRT (日立)，IIJ-SECT (IIJ)，IPA-CERT (情報処理推進機構)，JPCERT/CC，JSOC (ラック)，KDDI-CSIRT (KDDI)，KKCSIRT (カカクコム)，LINE-CSIRT (LINE)，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 (内閣サイバー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)

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[33][34]，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，JVN (Japan Vulnerability Notes) [35]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』

4.12 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』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[36].

(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 11 に示す連絡窓口を設置した．

表 11：連絡窓口情報

名称	"HIRT": Hitachi Incident Response Team.
所在地	〒140-8572 東京都品川区南大井 6-27-18 日立大森第二別館 10 階
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 HIRT: Hitachi Incident Response Team < hirt@hitachi.co.jp >

4.13 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[12]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[37]．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[38].

(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 25) [39][40]．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．

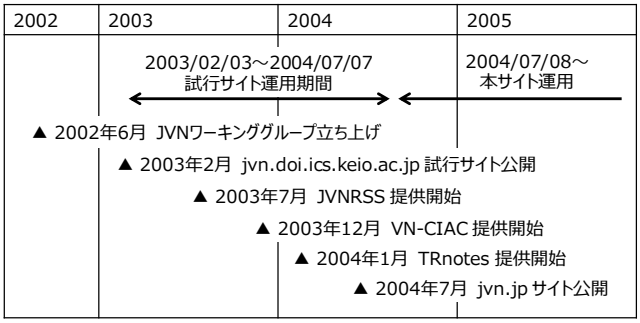


図 25：JVN 試行サイトの構築ならびに運用

4.14 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 26) 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．

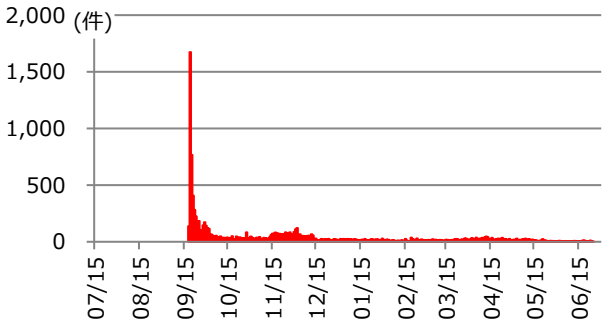


図 26：観測期間内の痕跡数変位 (Nimda)

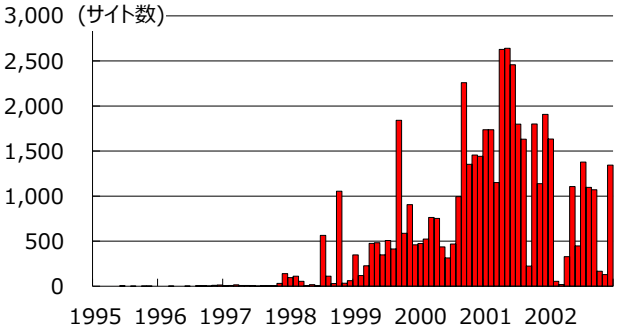


図 27：Web サイトの書き換え件数の推移

4.15 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[41]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[42]．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[43]．また，NIST では，NVD の前身である ICAT Metabase[44]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) [45]が利用され始めた．

4.16 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 27)．

4.17 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[46]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

セキュリティ対策やインシデント対応が，少なからず他組織に影響を与える／他組織の影響を受ける構図となり、CSIRT を活用した組織間での専門的，実務的な連携にもスピードアップが求められるだけではなく、物理的な影響を伴う被害も顕在化し始めてきている。次の克服すべき課題は、攻撃者のサイバー攻撃スピードへの追従と、サイバーとフィジカル両面からのインシデント対応体制であろう。

HIRT では，この新たな脅威の状況に対処していくため，「日立グループ CSIRT 活動の向上～6 ヵ年計画～」に続き、「分野別 CSIRT 活動の推進～6 ヵ年計画～」を開始すると共に、『次の脅威をキャッチアップする』過程の中で，早期に対策展開を図る活動を進めていく．

(2016 年 8 月 14 日)

参考文献

1) 警察庁，平成 27 年中のインターネットバンキングに係る不正送金事犯の発生状況等について，
http://www.npa.go.jp/cyber/pdf/H280303_banking.pdf

2) シマンテック, The evolution of ransomware (Aug. 2015), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
3) マカフィ, 脅威レポート (Aug. 2015), http://www.mcafee.com/jp/resources/reports/rp-quarterly-threat-q2-2015.pdf
4) Arbor Networks, ATLAS Q2 2015 Global DDoS Attack Trends, http://www.slideshare.net/Arbor_Networks/atlas-q2-2015final
5) Arbor Networks, ASERT Threat Intelligence Report 2015-04; "DD4BC DDoS Extortion Threat Activity", http://pages.arbornetworks.com/rs/082-KNA-087/images/ATIB2015-04DD4BC.pdf
6) NIST, NVD (National Vulnerability Database), http://nvd.nist.gov/
7) (独)情報処理推進機構, 脆弱性関連情報に関する届出状況, https://www.ipa.go.jp/security/vuln/report/press.html
8) 日立と HP がサイバー脅威に関するデータ共有の試行を開始, http://www.hitachi.co.jp/New/cnews/month/2015/10/1006a.html
9) 日本シーサート協議会, SSH サーバセキュリティ設定検討 WG, http://www.nca.gr.jp/activity/sshconfig-wg.html
10) 情報セキュリティ大学院大学, 第 11 回「情報セキュリティ文化賞」, https://www.iisec.ac.jp/news/20150210culsec_11th.html
11) ITpro セキュリティ, http://itpro.nikkeibp.co.jp/security/
12) CERT Advisory CA-2002-03, "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)" (Feb. 2002), http://www.cert.org/advisories/CA-2002-03.html
13) HIRT-PUB14008: サイバーセキュリティ情報交換フレームワーク CYBEX, http://www.hitachi.co.jp/hirt/publications/hirt-pub14008/index.html
14) 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/2015/
15) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), http://www.ntt-cert.org/
16) HIRT-PUB10008： 日立グループにおける製品脆弱性情報の開示プロセス (Sep. 2010), http://www.hitachi.co.jp/hirt/publications/hirt-pub10008/index.html
17) (ISC)^{2,} Information Security Leadership Achievements (ISLA)プログラム, https://www.isc2.org/japan/isla.html
18) CSIRT ワークショップ 2012, http://www.hitachi.co.jp/hirt/topics/20120229.html
19) Kyoto 2012 FIRST Technical Colloquium, http://www.first.org/events/colloquia/kyoto2012
20) 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
21) SGU MIT Workshop Academy CERT Meeting (Jul. 2010), http://academy-cert-indonesia.blogspot.jp/2010/06/academy-cert-meeting.html
22) 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)(Sep. 2011), http://www.hitachi.co.jp/hirt/publications/hirt-pub11003/index.html
23) 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 (Dec. 2009), http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html
24) cNotes: Current Status Notes, http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi
25) (独)情報処理推進機構, DNS キャッシュポイズニング対策 (Feb. 2009), https://www.ipa.go.jp/security/vuln/DNS_security.html
26) Joint Workshop on Security 2008, Tokyo 開催記録サイト (Mar. 2008), http://www.nca.gr.jp/jws2008/index.html
27) 情報化月間 2008-平成 20 年度情報化促進貢献企業等表彰 (Oct. 2008), http://www.meti.go.jp/policy/it_policy/gekkan/#gekkan_kako
28) (一社)情報処理学会, 情報処理: マルウェア: 5. コラム：標的型メールがやってきた (May. 2010), https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=69232&file_id=1
29) 日本シーサート協議会, http://www.nca.gr.jp/
30) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/
31) GlobalSign Adobe Certified Document Services, https://jp.globalsign.com/solution/example/hitachi.html
32) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/
33) 経済産業省告示第 235 号, ソフトウェア等脆弱性関連情報取扱基準 (Jul. 2004), http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
34)(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 (Jul. 2004), https://www.ipa.go.jp/security/ciadr/partnership_guide.html
35) JVN (Japan Vulnerability Notes), http://jvn.jp/
36) NISCC, NISCC Vulnerability Advisory 006489/H323: Vulnerability Issues in Implementations of the H.323 Protocol (Jan. 2004), http://www.kb.cert.org/vuls/id/JSHA-5V6H7S
37) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html
38) US-CERT, Vulnerability Note VU#459371: "Multiple IPsec implementations do not adequately validate authentication data" (Oct. 2002), http://www.kb.cert.org/vuls/id/459371
39) JPCERT/CC Vendor Status Notes DB 構築に関する検討, CSS2002 (Oct. 2002), http://www8.cao.go.jp/cstp/project/export/ITPT-B/ITPT1/shiryo.1-6.pdf
40) セキュリティ情報流通を支援する JVN の構築 (May. 2005), http://www.hitachi.co.jp/hirt/csirt/jvn/index.html
41) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls
42) CERT/CC Vulnerability Note Field Descriptions, http://www.kb.cert.org/vuls/html/fieldhelp
43) CVE (Common Vulnerabilities and Exposures), http://cve.mitre.org/
44) ICAT, http://icat.nist.gov/ (not available)
45) CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/
46) DEFCON, http://www.defcon.org/

執筆者
寺田真敏(てらだ まさと)
1998 年に HIRT の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運営委員長を務める．