セキュリティインシデントの動向と日立グループの取り組み

—HIRT活動—

寺田 真敏 Terada Masato
藤原 将志 Fujiwara Masashi
沼田 亜希子 Numata Akiko
妹尾 徹 Senoo Toru
石淵 一三 Ishibuchi Kazumi
宮崎 真理 Miyazaki Mari

サイバー攻撃は変遷を続けるとともに，攻撃によるセキュリティインシデントは多様化している。また，情報システムや制御システムをベースにインターネットを活用して構築された社会インフラに与える影響は，より深刻になりつつある。そうした事態に備えるためには，CSIRT体制の整備や技術継承が重要となる。HIRTは，日立グループ全体のインシデントオペレーションを推進するプロジェクトチームである。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ならびに解決するための活動）を通して，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る。

1. はじめに

情報システムや制御システムをベースにインターネットを活用して構築された社会インフラは，新たな脅威に直面しており，日々の脆（ぜい）弱性対策やインシデント対応を通して，脅威に打ち勝っていく必要がある。HIRT（Hitachi Incident Response Team）は，日立グループ全体で新たな脅威によって発生しうるセキュリティインシデントを予防し，万一インシデントが発生した場合には迅速に対処することにより，顧客や社会の安全かつ安心な社会インフラの実現に寄与するための組織である。

ここでは，近年のセキュリティインシデントの動向，HIRTセンタを中心とした日立グループにおけるCSIRT（Cyber Security Incident Readiness/Response Team：サイバーセキュリティにかかるインシデントに対処するための組織の総称や機能）活動について述べる。

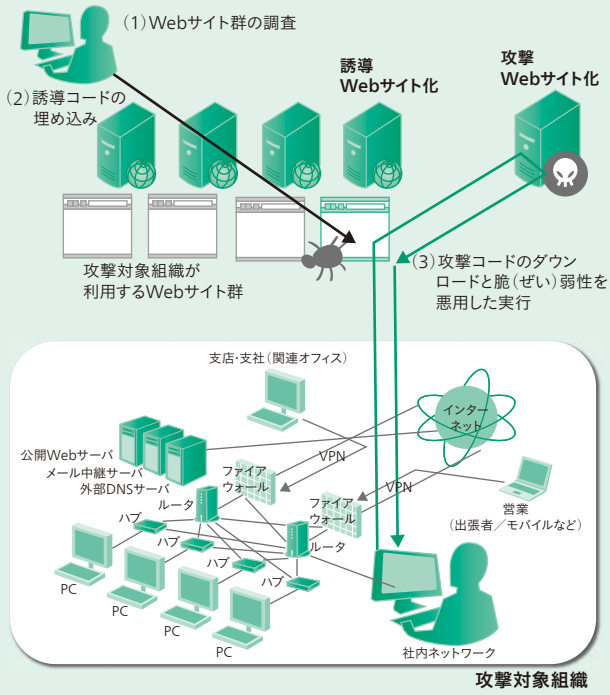
2. セキュリティインシデントの動向

2000年のラブレターウイルス以降，サイバー攻撃は変遷を続け，攻撃対象となる脆弱性は，オペレーティングシステムからアプリケーションへと広がってきている。不正プログラムも，ウイルス添付型メール，ネットワーク型ワーム，ボットなど，技術を継承しながら進化している。2008年ごろからは，Gumblar（ガンブラー）に代表されるホームページ誘導型マルウェアやUSB（Universal Serial Bus）メモリ型マルウェアのように，ユーザーの心理面や行動面の脆弱性を利用し，ユーザー自身をサイバー攻撃活動の渦中に巻き込む手法も一般化しつつある。

2010年以降，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が注目を集めているが，その目的は情報窃取だけではない。2010年7月に流布したマルウェアStuxnet（スタクスネット）は，原子力施設を攻撃対象とし，SCADA（Supervisory Control and Data Acquisition）ソフトウェアを通じて制御装置の動作に異常をきたす不正プログラムであった[1)]。

2013年のセキュリティインシデントの特徴は，Webサイトへのサイバー攻撃の定常化，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。特に，Webサイトへのサイバー攻撃は，水飲み場型攻撃（Watering Hole Attack）として，標的型攻撃の一部に組み込まれている。水飲み場型攻撃とは，攻撃対象組織が閲覧する可能性の高いWebサイト群に仕掛けを蔵置し，誘導Webサイトとして利用する手法である（**図1**参照）。

ここで使われているアプローチは，誘導Webサイトを閲覧すると，攻撃Webサイトに誘導されるというもので，技術的にはGumblarに代表されるWebページ誘導型マルウェアと同様の仕組みである。また，攻撃手法としては，アカウント情報をリスト化してさまざまなサイトに不正ロ



注：略語説明　DNS (Domain Name System)，VPN (Virtual Private Network)，PC (Personal Computer)

図1｜水飲み場型攻撃 (Watering Hole Attack)

攻撃対象組織の利用者が誘導Webサイトを閲覧するのを待ち受けることから，水飲み場で獲物を待ち伏せるライオンになぞらえ，水飲み場攻撃 (Watering Hole Attack) と呼ばれている。

グインを試みるリスト型攻撃，要求/応答のデータサイズ差を利用したDNS (Domain Name System)/NTP (Network Time Protocol) 増幅攻撃の顕在化が挙げられる[2]。DNS/NTPは，いずれもインターネット基盤として欠かすことのできない名前解決と時刻同期サービスであり，脅威の低減には，各所の協力が必要不可欠である。

3. 日立グループにおけるCSIRT活動

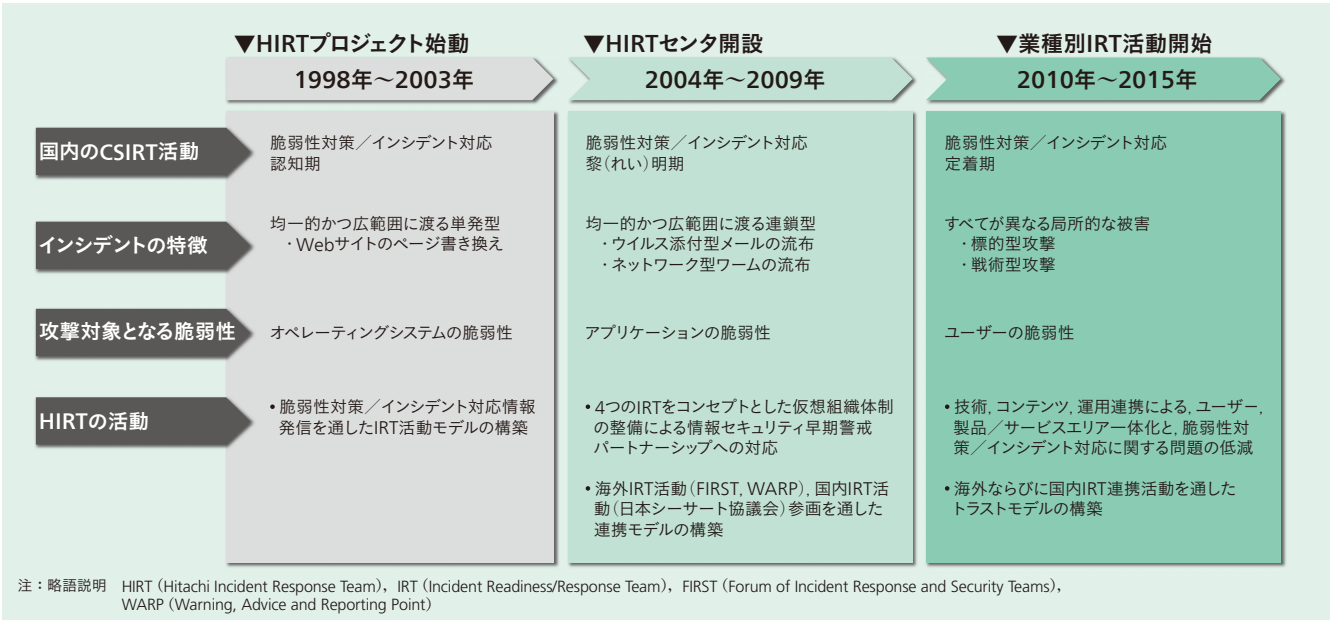
3.1 CSIRT(シーサート)

1998年以降，サイバー攻撃に対処するための日本国内のCSIRT活動は，3つの時期に分けられる (図2参照)。

第1期は認知期であり，米国で始まったCSIRT活動を参考にし，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」という考え方を導入した時期である。第2期は黎 (れい) 明期であり，2001年から2003年にかけて流布したネットワークワーム対処の経験値をフィードバックし，日本流のCSIRT活動が立ち上がり始めた。この黎明期には，2004年の情報セキュリティ早期警戒パートナーシップの始動，および脆弱性対策情報データベースJVN (Japan Vulnerability Notes) の開設，2007年の日本シーサート協議会の設立など，日本という地域性を考慮したCSIRT活動基盤が整備された。CSIRT活動の第3期にあたる2012年，サイバー攻撃対策において，インシデント対応の専門的な機能としてCSIRTを活用しようという流れが動き始めた。2011年の多様なセキュリティインシデント発生をきっかけとする面は大きいが，CSIRT活動を展開する定着期として，大きな一歩を踏み出した年であったと言える。

3.2 HIRT

1998年4月，HIRTは，日立グループにおけるCSIRT体制を整備するための研究プロジェクトとして活動を開始した。この活動の中では，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



注：略語説明　HIRT (Hitachi Incident Response Team)，IRT (Incident Readiness/Response Team)，FIRST (Forum of Incident Response and Security Teams)，WARP (Warning, Advice and Reporting Point)

図2｜インシデントの変遷とHIRTの活動概要

サイバー攻撃の変遷とともに，サイバー攻撃に対処するための日本国内のCSIRT (Cyber Security Incident Readiness/Response Team) 活動も成長を続けている。

feature articles

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をHIRTがCSIRTとして活動するための要件としている。また，そのミッションを，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）の経験値を生かして「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」としている。HIRTは，これらの能力ならびにミッションを持った組織として，日立グループの対外的なCSIRT統一窓口としての責務を負っている。

3.3　日立グループのCSIRT活動モデル

CSIRTとしてのHIRT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なら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支援していくことである。さらに，インシデントレスポンス（事後対処）などの実践的な活動経験を基に，インシデントレディネス（事前対処）を進めることで，安全・安心な社会インフラの実現に寄与することである。

HIRTでは，CSIRT活動を進めていくうえで，4つのIRT（Incident Readiness/Response Team）という組織編成モデルを採用している（**図3**参照）。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（製品ベンダー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（System Integration）ベンダーIRT］，そして，インターネットユーザーとして自身の企業を運用管理していく側面（社内ユーザーIRT）の3つがある。

4つのIRTでは，ここに，IRT間の調整業務を行うHIRTセンタを設けることで，各IRTの役割を明確にしつつ，IRT間の連携を図ったサイバーセキュリティ対策を推進するための体制モデルとしている。なお，HIRTという名称は，広義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，狭義ではHIRTセンタを示している。

4.　HIRTセンタが推進する活動

HIRTセンタの主な活動には，組織内IRT活動として，制度面を先導する部門との協力による制度・技術の両面でのサイバーセキュリティ対策の推進，各事業部・グループ会社への脆弱性対策ならびにインシデント対応の支援がある。また，組織間IRT活動として，日立グループの対外的なCSIRT窓口としてのサイバーセキュリティ対策の協力がある。

4.1　組織内IRT活動

組織内IRT活動では，サイバーセキュリティ情報の収集や分析を通して得られたノウハウをアドバイザリーとして

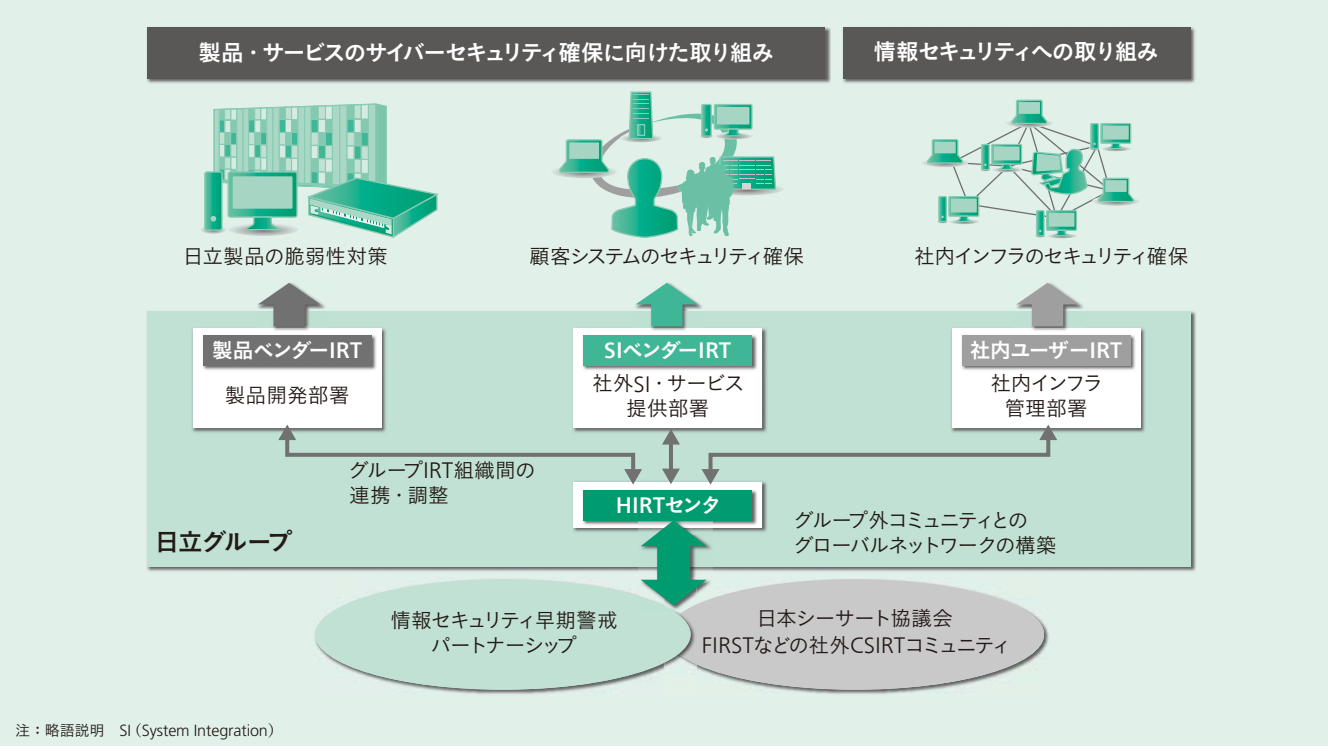


図3｜脆弱性対策とインシデント対応活動を支える4つのIRT
脆弱性対策，インシデント対応活動を推進するため，4つのIRT構成による組織編成モデルを採用している。

発行し，また，各種ガイドラインや支援ツールの形で製品・サービス開発プロセスにフィードバックする。

(1) セキュリティ情報の収集・調査分析・展開

脆弱性対策ならびにインシデント対応に関する情報やノウハウを水平展開する。

(2) 情報利活用基盤の整備

サイバーセキュリティ情報の収集～調査分析～展開のための情報利活用基盤を整備する。

(3) 製品・サービスのセキュリティ技術の向上

Webアプリケーションセキュリティの強化，情報家電・組込み系製品・制御系製品のセキュリティ施策の具体化，開発・管理プロセスの整備を推進する。

(4) 研究活動基盤の整備

早期の対策展開を図るための技術開発に向け，研究所との共同体制を整備する。

4.2 組織間IRT活動

予兆や被害を隠蔽化するサイバー攻撃の増加に合わせ，異なる組織のCSIRTどうしがつながり，サイバー攻撃を鳥瞰（かん）することで問題解決を図るための組織間連携，互いの活動の改善に寄与できる協力関係の構築を推進している。

(1) CSIRT活動の国内連携の強化

JVNおよびJVNRSS［JVN RDF（Resource Description Framework）Site Summary］を用いた情報利活用基盤の整備[3]，情報セキュリティ早期警戒パートナーシップに基づく脆弱性対策活動の推進，日本シーサート協議会を通じた組織間CSIRTの連携がある。

(2) CSIRT活動の海外連携の強化

海外CSIRT組織との連携体制の整備，英国WARP（Warning, Advice and Reporting Point）活動の推進，サイバーセキュリティ情報交換フレームワーク（CYBEX：Cybersecurity Information Exchange Techniques）などの標準化への対応がある。

(3) 研究活動基盤の整備

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

4.3 主な活動

2010年から，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，日立グループCSIRT活動の向上プロジェクトを開始した（**表1**参照）。ここでは，フェーズ2までの活動の中から業種別IRT活動の試行，制御システム製品向け脆弱性対策の取り組みについて報告する。

表1｜日立グループCSIRT活動の向上プロジェクト

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活動である。

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連携支援メンバーとの連携強化** • IRT連携支援メンバー（事業部・グループ会社）制度の試行 • IRT連携支援メンバーを起点とした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連携支援メンバーによる各種支援活動の推進 • ユーザー連携モデル（フェーズ1，2）と組織連携モデル（フェーズ3）の融合による広義のHIRT（バーチャル組織体制）の構築

4.3.1 業種別IRT活動の試行

(1) インシデントレスポンス+レディネス3層サイクル

サイバー攻撃対策において，発生した事案解決のためのインシデントレスポンスはもちろん重要であるが，インシデントや動向を踏まえたレディネスの推進も欠かせない。そこで，業種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を取ることで，部門との役割分担と連携を明らかにしつつ，業種別のレディネスを推進することとした（**図4**参照）。

(2) HIRT-FIS：金融分野における先行的な取り組み

2012年10月，金融システム部門内にHIRT-FIS（Financial Industry Information Systems HIRT）を設置した。HIRT-FISは，HIRTの分野別サブセットとして位置づけ，金融分野に特化した先行的なCSIRTプロフェッショナルチームをめざしている（**図5**参照）。これは，インシデントレスポンス＋レディネス3層サイクルを具体化する取り組みの1つでもある。特に，サイバー攻撃対策に

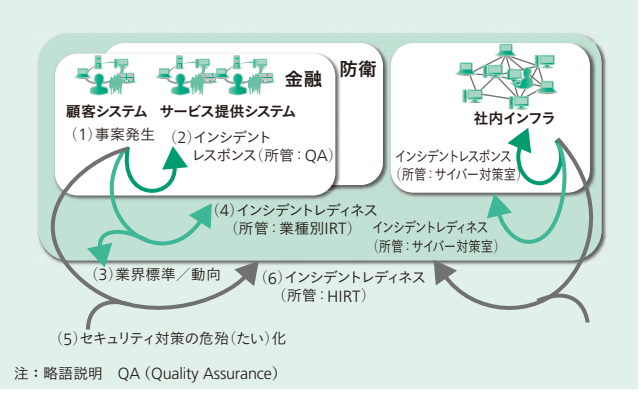


図4｜インシデントレスポンス+レディネス3層サイクルの概念

サイバー攻撃対策において，発生した事案解決のためのインシデントレスポンス（事後対処）とともに，インシデントの経験値や業種別視点を取り込んだ動向を踏まえてレディネス（事前対処）を推進する。

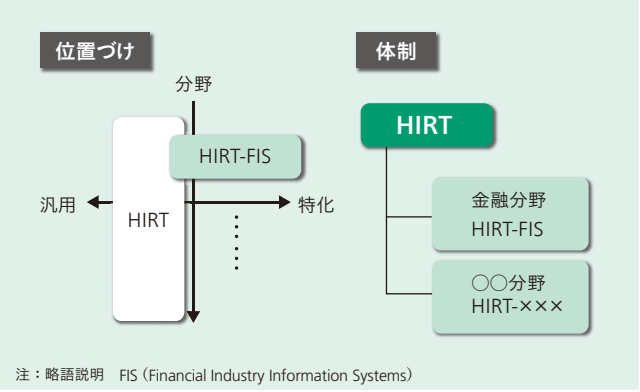


図5｜業種別IRT活動の位置づけと体制

インシデントレスポンス＋レディネス3層サイクルを具体化する取り組みの1つであるHIRT-FISは，金融分野に特化した先行的なCSIRTプロフェッショナルチームをめざしている。

おいては，分野の背景や動向を踏まえた対応が必要になると考えており，分野に特化したCSIRT活動の検討とその推進を先導することを目的としている。今後，状況を見ながら，制御システム，防衛などの業種別IRTを分野別サブセットとして立ち上げていく予定である。

4.3.2　制御システム製品向け脆弱性対策

これまで推進してきたHIRT活動の経験値を制御システム分野に展開するというアプローチであり，3つの取り組みを進めている。

(1) 制御システムにおける最新の動向や製品の脆弱性，インシデント事例などのセキュリティに関する情報収集は，HIRTセキュリティ情報を活用する。

(2) 脆弱性ハンドリング，インシデントハンドリングに対応するため，HIRTを対外的な窓口の基点とした体制整備を推進していく。

(3) 制御装置や制御システムの脆弱性対策では，具体的な展開を視野に入れた脆弱性対策の推進として，仕様，コード，設定の3つ視点から脆弱性対策にアプローチするとともに，制御装置と制御システムでの先行事例づくりの検討を開始した。

5.　おわりに

ここでは，近年のセキュリティインシデントの動向，HIRTセンタを中心とした日立グループにおけるCSIRT活動について述べた。

既知の脅威による被害が継続する一方で，新たなサイバー攻撃によって脅威が生み出され，被害が発生している。さらに，サイバー攻撃による被害が，異なる組織間で少なからず影響し合う構図が鮮明になってきている。このような状況において，CSIRTを活用した組織間での専門的かつ実務的な連携の具現化は必要不可欠である。

HIRTでは，状況変化を捉え，「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，業種などの分野に特化したCSIRT活動の推進，次世代のCSIRTコミュニティにつながる学術系人材の育成に取り組むことで，安全・安心な社会インフラの実現につながるものと考える。

参考文献など

1)　独立行政法人情報処理推進機構：IPAテクニカルウォッチ『新しいタイプの攻撃』に関するレポート，http://www.ipa.go.jp/about/technicalwatch/20101217.html
2)　JPCERT/CC：DNSの再帰的な問い合わせを使ったDDoS 攻撃に関する注意喚起，https://www.jpcert.or.jp/at/2013/at130022.html
3)　寺田，外：脆弱性対策情報データベースJVNの提案，情報処理学会論文誌，Vol. 46，No. 5，pp. 1256-1265 (2005.5)

執筆者紹介


寺田 真敏
日立製作所 情報・通信システム社 サービスプロデュース統括本部 セキュリティ先端技術本部 HIRTセンタ 兼 横浜研究所 情報サービス研究センタ エンタープライズシステム研究部 所属
現在，インシデントオペレーションに向けたCSIRT組織間連携活動に従事
博士（工学）
情報処理学会会員


藤原 将志
日立製作所 情報・通信システム社 サービスプロデュース統括本部 セキュリティ先端技術本部 HIRTセンタ 所属
現在，製品・サービスの脆弱性対策ならびにインシデント対応に従事


沼田 亜希子
日立製作所 情報・通信システム社 サービスプロデュース統括本部 セキュリティ先端技術本部 HIRTセンタ 所属
現在，脆弱性対策・インシデント対応における技術継承企画業務に従事


妹尾 徹
日立製作所 情報・通信システム社 ITプラットフォーム事業本部 開発統括本部 開発基盤本部 ソフトウェア生産技術部 兼 サービスプロデュース統括本部 セキュリティ先端技術本部 HIRTセンタ 所属
現在，制御システム製品向け脆弱性対策の取り組みに従事


石淵 一三
日立製作所 情報・通信システム社 ITプラットフォーム事業本部 開発統括本部 開発基盤本部 ソフトウェア生産技術部 兼 サービスプロデュース統括本部 セキュリティ先端技術本部 HIRTセンタ 所属
現在，サイバーセキュリティ情報の調査分析に従事


宮崎 真理
日立製作所 情報・通信システム社 金融システム事業部 事業推進本部 システム統括部 所属
現在，HIRT-FISにおいてCSIRT活動に従事