

【用語の説明】

- **CERT/CC (Computer Emergency Response Team/Coordination Center)**
米国におけるセキュリティ事故情報、脆弱性情報の収集機関。
- **CPNI (Center for the Protection of National Infrastructure)**
英国におけるセキュリティ事故情報、脆弱性情報の収集機関。
- **CSIRT (Computer Security Incident Response Team)**
セキュリティ問題の発生に際して、それを検知し、関連組織と連絡をとり、被害拡大を防ぐと共に再発を防止するための原因究明と改善を行う組織。
- **FIRST (Forum of Incident Response and Security Teams)**
信頼関係に結ばれた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コミュニティ。現在では、59カ国274チームが加盟。
- **IPA (Information-technology Promotion Agency)**
「(独)情報処理推進機構」の略。汎用プログラムの開発／普及の促進、先進的な情報処理技術の研究開発、コンピュータウイルス対策、及び、情報基盤センターの整備／運営などを推進。
- **JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center)**
日本におけるセキュリティ事故情報、脆弱性情報の収集機関。
- **JVN (Japan Vulnerability Notes)**
経済産業省告示「ソフトウェア等脆弱性関連情報取扱基準」を受けて、日本国内の製品開発者の脆弱性対応状況を公開するサイト
- **NCA (Nippon CSIRT Association)**
「日本シーサート協議会」の略。国内のCSIRTが共通の問題を互いに協調して解決するための場を設けることを目的として、2007年3月に設立。
- **NISC (National Information Security Center)**
内閣官房内に設置された情報セキュリティに関するナショナル・センター。
- **WARP (Warning, Advice and Reporting Point)**
2002年に英国政府機関によって提唱されたセキュリティ情報、相互アドバイスと、インシデント情報の共有によるセキュリティ対策推進のための互助コミュニティ。
- **インシデント (コンピュータセキュリティインシデント)**
コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの。
- **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
ソフトウェア製品やWebサイトに見つかったセキュリティ問題を情報処理推進機構(IPA)が受け付け、製品開発ベンダやサイト運営者に修正や情報公開を促す制度。
- **脆弱性**
ソフトウェア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。ウェブアプリケーションにあたっては、ウェブサイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。
- **ソフトウェア等脆弱性関連情報取扱基準**
日本国内における脆弱性関連情報の受付と、情報の安全な流通を目的とした枠組み。



お問い合わせ先

株式会社 日立製作所 クラウドサービス事業部
HIRT (Hitachi Incident Response Team)

〒140-0013 東京都品川区南大井6丁目26番3号 (大森ベルポートD館)

■ 情報提供サイト : <http://www.hitachi.co.jp/hirt/>

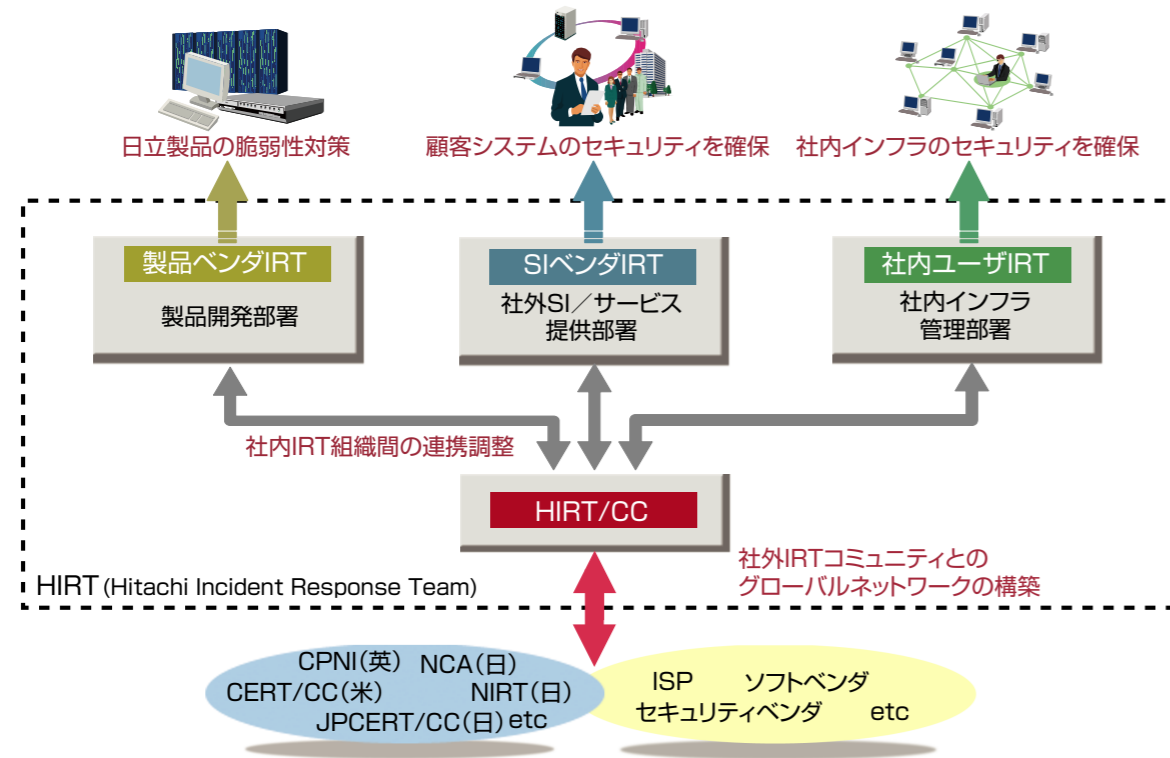
■ お問い合わせ : <http://www.hitachi.co.jp/hirt/ask.html>

HIRTとは…

日立グループでは、1998年4月より、日立としてのIRT(Incident Response Team)体制を整備するためにプロジェクトとしてHIRT(Hitachi Incident Response Team)の活動を開始しました。

HIRTは、日立グループの各部門に対して、脆弱性対策／インシデント対応情報を展開し、お客様のシステムを不正アクセスなどのインシデントから守るための対策を支援する組織です。HIRTでは、日立グループ全体でセキュリティインシデントの発生を予防し、万一インシデントが発生してしまった場合には迅速に対処することにより、お客様や社会の安心かつ安全なネットワーク環境の実現に寄与していきます。また、日立グループのCSIRT(Computer Security Incident Response Team)連絡窓口としてFIRST、NCAなどのCSIRTコミュニティに積極的に参画し、情報セキュリティ全体の向上に貢献してまいります。

● 脆弱性対策／インシデント対応活動を支える4つのIRT



■ HIRT/CC(HIRT/Coordination Center) 【該当部署:HIRTセンタ】

FIRST, NCA, JPCERT/CC, CERT/CC などの対外CSIRT組織との連絡窓口であり、日立グループの SIベンダ/製品ベンダ/社内ユーザ IRT 組織間の連携調整を行います。

■ 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活動を推進します。公開された脆弱性やインシデント発生について、顧客システムのセキュリティを確保することに努めます。

■ 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、対策情報公開を推進します。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、告知ならびに修正プログラムを提供することで、コンピュータウイルス、コンピュータ不正アクセス等により、インターネットにおいて発生しうる被害(インシデント)を予防します。

■ 社内ユーザIRT 【該当部署:社内インフラ提供部署】

日立関連サイトがインターネットに対して脅威を与えるような侵害活動の基点とならないよう社内システムのセキュリティ対策を推進します。

活動内容

インターネットが基本的な社会インフラとなるにともない、セキュリティインシデントの発生頻度は増え、その影響はより深刻化しています。さまざまなシステムがネットワークで結ばれ、社会で、組織で、家庭で、手軽な情報流通や便利なサービスが実現される時代になっていますが、その反面では、ソフトウェアやWebアプリケーションの脆弱性を利用した不正アクセス、情報漏洩などが大きな問題となっています。

今やインターネットに関わる問題は、組織全体、社会全体の問題として考える必要があり、インシデント対応機関を通じ、各組織さらには国家間が連携して対処することが重要となっています。

このような背景のもと、HIRTでは、「脆弱性対策:セキュリティに関する脆弱性を除去するための活動」「インシデント対応:発生している侵害活動を回避するための活動」を通じて、日立グループの情報セキュリティ活動を支援していくとともに、安心、安全なインターネット社会の樹立、維持、発展に寄与してまいります。

● IRT活動の国内&海外連携の強化

2003年のBlasterワーム以降、発覚を逃れるための工夫をこらした侵害活動や特定組織を対象とした侵害活動など、インシデントの形態も急速に変化しています。このような変化に伴い、脆弱性対策／インシデント対応活動に必要な情報収集や分析、さらには実際の対応などもCSIRT同士が協力して解決する必要性が高まっています。

HIRTでは、CSIRT同士の協力体制を確立するため、2005年1月に国際的なCSIRTフォーラムであるFIRSTに、2007年3月に国内のCSIRTコミュニティであるNCAに、2007年5月に英国のセキュリティコミュニティであるWARPに加盟しました。今後共、FIRSTをはじめ他の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／インシデント対応を通じて、安心かつ安全なネットワーク環境の実現に寄与していきます。

● セキュリティ情報流通の促進

HIRTは、日立グループのCSIRT連絡窓口として、「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」に沿った日立グループ内外との調整、インシデントを回避するための日立グループ内外との調整を行っています。脆弱性対策／インシデント対応の関連情報を適切に流通させることにより、コンピュータウイルスなどの侵害活動による被害発生抑制ならびに、発生後は、その被害収束に努めていきます。

日立グループのシーサート(CSIRT)向上活動

HIRTセンタとの連携を深めるため、日立グループ内の各事業部/グループ会社にIRTを設置しています。

■ 組織内IRT活動

■ セキュリティ情報共有

日立グループでの情報セキュリティ問題解決のため、メーリングリスト、Webを用いて、日立グループ向けのセキュリティ情報(脆弱性対策情報、インシデント対応のための注意喚起情報)の提供と共有を推進します。

■ セキュリティに関する相談窓口/対応調整

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外ならびに社内の対応調整を行います。

■ セキュリティ教育支援

IRT活動を通じて蓄積したノウハウを基に、セキュリティ教育/セキュリティ技術者育成を支援します。

■ HIRTコミュニティ展開活動

■ HIRTオープンミーティング

HIRTセンタと各IRTとが連携した脆弱性対策ならびにインシデント対応支援を推進するための情報交換の場です。人の輪でつながったHIRTコミュニティを日立グループ内に展開する場としても活用しています。

■ アドバンスドHIRTオープンミーティング

HIRTセンタと協力して、CSIRT活動を先導するメンバー(連携支援メンバー)との情報交換の場です。より技術的、より先進的な情報交換の場として活用しています。

