Hitachi Incident Response Team
2016.10.25 10:20:32 +09'00'

HITACHI
Inspire the Next

【用語の説明】

- CERT/CC (CERT Coordination Center)
  米国におけるサイバーセキュリティの調査、調整機関。
- 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。
- IPA (Information-technology Promotion Agency)/(独)情報処理推進機構
  情報や制御システムのセキュリティ確保やサイバー攻撃対策を推進する公的機関。
- JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center)
  日本におけるサイバーセキュリティの調査、調整機関。
- JVN (Japan Vulnerability Notes)
  情報セキュリティ早期警戒パートナーシップで報告された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
  信頼関係に結ばれたコンピュータインシデント対応チームの日本国内のコミュニティ。2007年3月設立。
- STIX (Structured Threat Information Expression)/脅威情報構造化記述形式
  サイバー脅威情報を記述するための言語。
- インシデント (サイバーセキュリティインシデント)
  サイバー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
  ソフトウェア製品およびWebサイトに関する脆弱性関連情報の円滑な流通、および対策の普及を図るための官民の連携体制。
- 脆弱性
  ソフトウェア等において、サイバー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。

HIRT Hitachi Incident Response Team

お問い合わせ先

株式会社 日立製作所 ICT事業統括本部 サービスプラットフォーム事業本部
HIRT（Hitachi Incident Response Team）

〒140-8572　東京都品川区南大井6丁目27番18号（日立大森第二別館）
■ 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

2016.10

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、日立のサイバーセキュリティ対策活動を支援する組織です。セキュリティインシデントの発生を予防し、万一発生した場合は迅速に対処することにより、お客様や社会の安全・安心なネットワーク環境の実現に寄与します。また、日立グループのCSIRT(Computer Security Incident Response Team)連絡窓口としてFIRST、日本シーサート協議会などのCSIRTコミュニティに積極的に参画し、サイバーセキュリティの向上に貢献してまいります。

HIRTの役割は、「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、「組織単体活動:自身の企業情報システムを対象とする『情報セキュリティへの取り組み』」象とする『製品・サービスのサイバーセキュリティ確保に向けた取り組み』」の視点から、日立のサイバーセキュリティ対策活動を支援していくことにあります。さらには、「次の脅威をキャッチアップする」過程の中で早期に対策の展開を図ることによって、安全・安心なインターネット社会の実現に寄与することにあります。

HIRTは、脆弱性対策とインシデント対応とを推進するために、下記のように、4つのIRT(Incident Response Team)という活動モデルを採用しています。

4つのIRTとは、

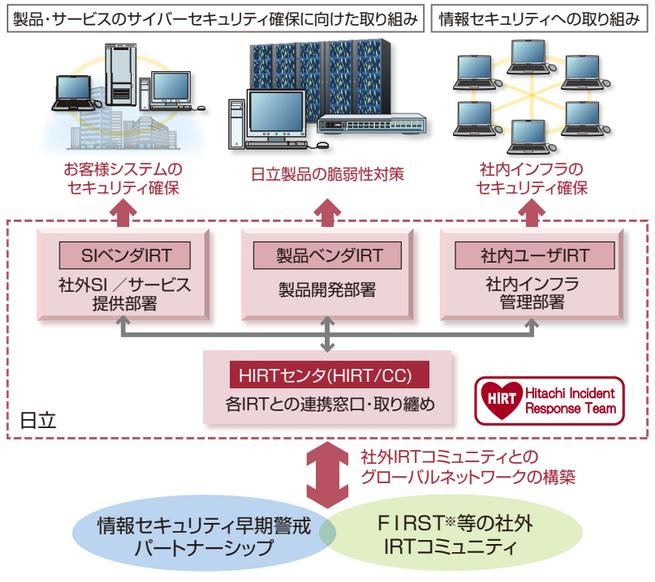
(1)情報システムや制御システム関連製品を開発する側面(製品ベンダIRT)

(2)その製品を用いてシステムの構築やサービスを提供する側面〔SI(System Integration)ベンダIRT〕

(3)インターネットユーザーとして自身の企業情報システムを運用管理する側面(社内ユーザIRT)

の3つとともに、

(4)これらのIRT間の調整業務を行うHIRT/CC(HIRTセンタ)を設け、各IRTの役割を明確にしつつ、IRT間の連携を図る効率的かつ効果的なセキュリティ対策活動を推進するモデルです。



分　類	役　割
HIRT/CC※	該当部署:HIRTセンタ FIRST、JPCERT/CC※、CERT/CC※などの社外IRT組織との連携、SIベンダ・製品ベンダ・社内ユーザIRT間の連携を通して脆弱性対策とインシデント対応活動を推進する。
SIベンダIRT	該当部署:SI・サービス提供部署 公開された脆弱性について、社内システムと同様にお客様システムのセキュリティを確保するなど、お客様システムを対象とする脆弱性対策とインシデント対応活動を支援する。
製品ベンダIRT	該当部署:製品開発部署 公開された脆弱性について影響の有無を迅速に調査し、該当する問題について、修正プログラムを提供するなど、日立製品の脆弱性対策を支援する。
社内ユーザIRT	該当部署:社内インフラ提供部署 日立サイトが侵害活動の基点とならないよう脆弱性対策とインシデント対応活動の推進を支援する。

※HIRT/CC: HIRT Coordination Center
FIRST: Forum of Incident Response and Security Teams
JPCERT/CC: Japan Computer Emergency Response Team/Coordination Center
CERT/CC: CERT Coordination Center
SI: System Integration

脆弱性対策、インシデント対応活動を支える4つのIRT

HIRTセンタが推進する活動

HIRTセンタの活動には、組織内IRT活動として、制度面を先導する情報セキュリティ統括部門と、品質保証部門との協力による制度・技術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ります。また、日立の対外的なIRT窓口として、組織間のIRT連携によるサイバーセキュリティ対策を推進しています。

組織内IRT活動

組織内IRT活動では、セキュリティ情報の収集や分析を通じ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ともに、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します。

(1)セキュリティ情報の収集・調査分析・展開

情報セキュリティ早期警戒パートナーシップの推進などを通じて、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組織内に展開しています。

(2)研究活動基盤の整備

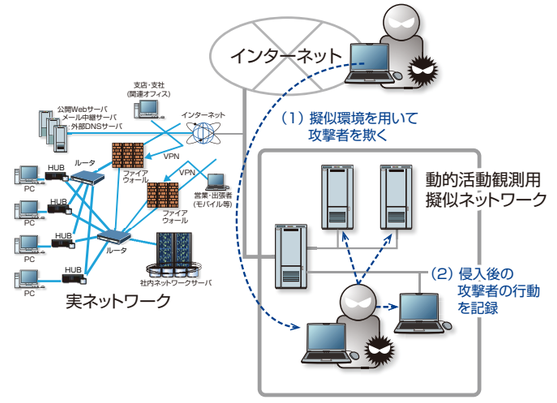
「次の脅威のキャッチアップ」と早期に対策展開を図るための技術として「動的活動観測」に取り組んでいます。動的活動観測は、標的型攻撃などのサイバー攻撃を調査するために構築した組織内ネットワークの擬似環境下で、侵入後の攻撃者の行動を記録し分析する観測手法です。

(3)製品・サービスのセキュリティ技術の向上

情報システムならびに制御システム関連製品に対するセキュリティ施策の具体化、開発・管理プロセスの整備、エキスパート人材への技術継承を推進しています。

(4)分野別IRT活動の実践

分野ごとの背景や動向を踏まえた対応を具体化していくため、分野に特化したIRT活動の検討と整備を進めています。



攻撃者の行動を記録する動的活動観測システム

組織間IRT活動

組織間IRT活動では、複数のIRTが協調して、新たな脅威に立ち向かうための組織間連携、互いのIRT活動の改善に寄与できる協力関係の構築を推進しています。

(1)IRT活動の国内連携の強化

JPCERTコーディネーションセンターと独立行政法人情報処理推進機構(IPA)が共同運営するJVNを用いた情報利活用基盤の整備、日本シーサート協議会を通じた組織間IRTの連携を推進しています。

(2)IRT活動の海外連携の強化

FIRST活動を活用した海外IRT組織ならびに海外製品ベンダIRTとの連携体制の整備、脅威情報構造化記述形式STIXなどを活用したインシデントオペレーションを推進しています。

(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研究活動への参画を通じて、人材育成の場の醸成、専門知識を備えた研究者や実務者の育成を推進しています。