CSIRT (Computer Security Incident Response Team) ～日立における CSIRT 活動～

公開日: 2006年5月25日

株式会社日立製作所
Hitachi Incident Response Team
チーフコーディネーションデザイナ 兼
システム開発研究所 主任研究員
寺田 真敏 氏著

はじめまして、Hitachi Incident Response Team (HIRT) に所属している寺田です。今回は、CSIRT (Computer Security Incident Response Team) と題して、日立の CSIRT 活動についてご紹介したいと思います。本題に入る前に、私自身を簡単に紹介をしますと、現在、日立に在籍しつつ、情報処理推進機構 (IPA) セキュリティセンターの非常勤研究員と JPCERT/CC の専門委員を兼務しています。主に日立では、HIRT の活動を企画しつつ、自ら手を動かすという生活を送っています。また、IPA とJPCERT/CC では、縁あって JVN(JP Vendor Status Notes) に関する研究開発に携わっています。

バックナンバー
- マイクロソフト セキュリティ ニュースレターで配信した日本オリジナル コラム

日立のCSIRT活動 = HIRT

まず、私の所属する HIRT の位置付けと組織体制についてご紹介します。

活動のはじまり

日立での CSIRT 活動は遡ること 8 年前の 1998 年 4 月に HIRT プロジェクトという名称で始まりました。その当時の報告書 (1998 年 HIRT プロジェクト活動報告書) を眺めてみますと、社外動向の章では、不正アクセス対策法案の整備に関して、1998 年 11 月 17 日警察庁は「不正アクセス対策法案の基本的考え方」を発表し、同年 11 月 25 日に郵政省が「電気通信システムに対する不正アクセス対策法制の在り方について」を発表したとあります。また、不正アクセスの動向の章では、imapd、popd、named、statd、mountd などのサーバプログラムを対象とするバッファオーバーフロー攻撃、Back Orifice、NetBus などのツールの流布とその探査活動の活発化、Windows 環境でネットワークを介して流布するRemote Explorer ウイルスの出現など、昨今のセキュリティ問題の先駆け? の頃だったようです。さらにその当時の活動を調べてみますと、かなり他人事のよう

な書き方ですが、1998 年 5 月 24 日社内向けに ""namedを攻撃対象とした不正アクセスの状況 (CERT Summary CS-98.04 - SPECIAL EDITIONから抜粋)"" という注意喚起情報の発行業務が HIRT としての最初の CSIRT 活動だったようです。せっかくですので、本題の活動のはじまりについても活動報告書から引用します。

> 不正アクセス対策ならびに、新たな脆弱性の発生に対処する社内組織体制を整備するために、日立版 CERT/CC (Computer Emergency Response Team / Coordination Center) に相当する組織として HIRT (Hitachi Incident Response Team) プロジェクトの活動を開始した。

HIRT の位置付け

このように始まった CSIRT 活動は、少しずつ活動範囲を広げながら、現在も HIRT (Hitachi Incident Response Team) という名称で継続しています。現在の HIRT の位置付けと役割を書き出しますと図 1 の通りとなります。活動開始当初との大きな違いは、HIRT の位置付けと活動目的が明確になったことと、会社組織の中に組み込まれたことです。

図 1
全画面表示

HIRT の組織編成

次に、HIRT の位置付けと役割で示した活動をどのような体制で進めているのかについてですが、試行錯誤の結果、日立の場合には、情報システム関連製品を開発する側面、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、そして、日立自身が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の 3 つがあることから、図 2 のように全体を 4 つの IRT (Incident Response Team) に分割し個々の IRT の役割を明確にしました。

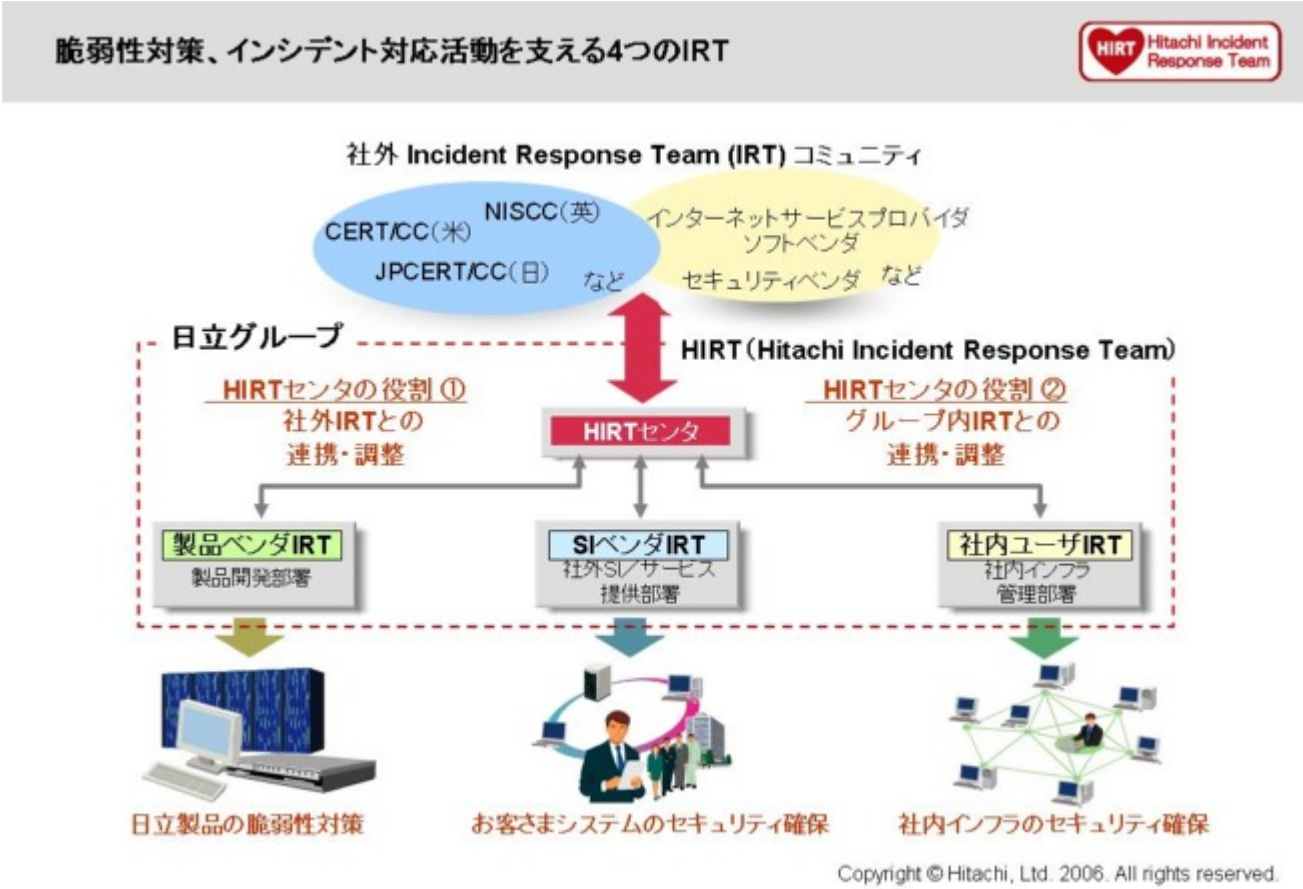

図2
全画面表示

これらを脆弱性対策、インシデント対応活動を支える 4 つの IRT と呼んでいます。4 つの IRT の役割分担は次のようになっています。

- HIRT/CC【 該当部署: HIRT センタ 】
  - JPCERT/CC, CERT/CC などの対外 IRT 組織との連絡窓口となる。

    - SI ベンダIRT、製品ベンダ IRT、社内ユーザIRT 間の連携調整を行なう。
- SIベンダIRT【 該当部署: SI/サービス提供部署 】
    - お客さまシステムを対象とした IRT 活動を推進する。
    - 公開された脆弱性について、お客さまシステムのセキュリティ確保を支援する。
- 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する。
    - 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。
- 社内ユーザ IRT【 該当部署: 社内インフラ提供部署 】
    - 日立サイトが不正アクセス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を推進する。

HIRT の組織編成の経緯

実際に、この 4 つの IRT ができあがるまでには図 3 にある 4 段階ほどのステップを踏んでおり、3 つの IRT の大枠が決まった後に、社内外 IRT との調整役となる HIRT センタが組織としてできあがったという次第です。このあたりの組織編成の経緯を振り返りますと、それぞれの段階で活動を後押しするきっかけが存在しています。例えば、第 2 ステップの製品ベンダ IRT 立ち上げには CERTアドバイザリ CA-2002-03 で報告された SNMP の脆弱性報告が後押しになっています。また第 3 ステップの SI ベンダ IRT 立ち上げには 2004 年 7 月のソフトウエア製品等脆弱性関連情報取扱基準と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後押しになっています。CSIRT 活動そのものはかなり漠然としたもので摑み所がありませんが、きっかけを利用して問題の整理と解決、組織的な体制との連携を図るというのが、今のところ最善解のようです。

組織編成のことで、ひとつ言い忘れたことがあります。日立特有かもしれませんが、社内外 IRT との調整役となる HIRT センタは、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するために、バーチャルな組織体制をとっています。ちょっと分かりにくい説明ですね。簡単に言えば、メンバの多くは兼務職制となっています。これは、情報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という考え方に基づいています。社内向けには、縦軸の組織と横軸のコミュニティが連携することにより CSIRT 活動を推進するモデルですと説明しています。

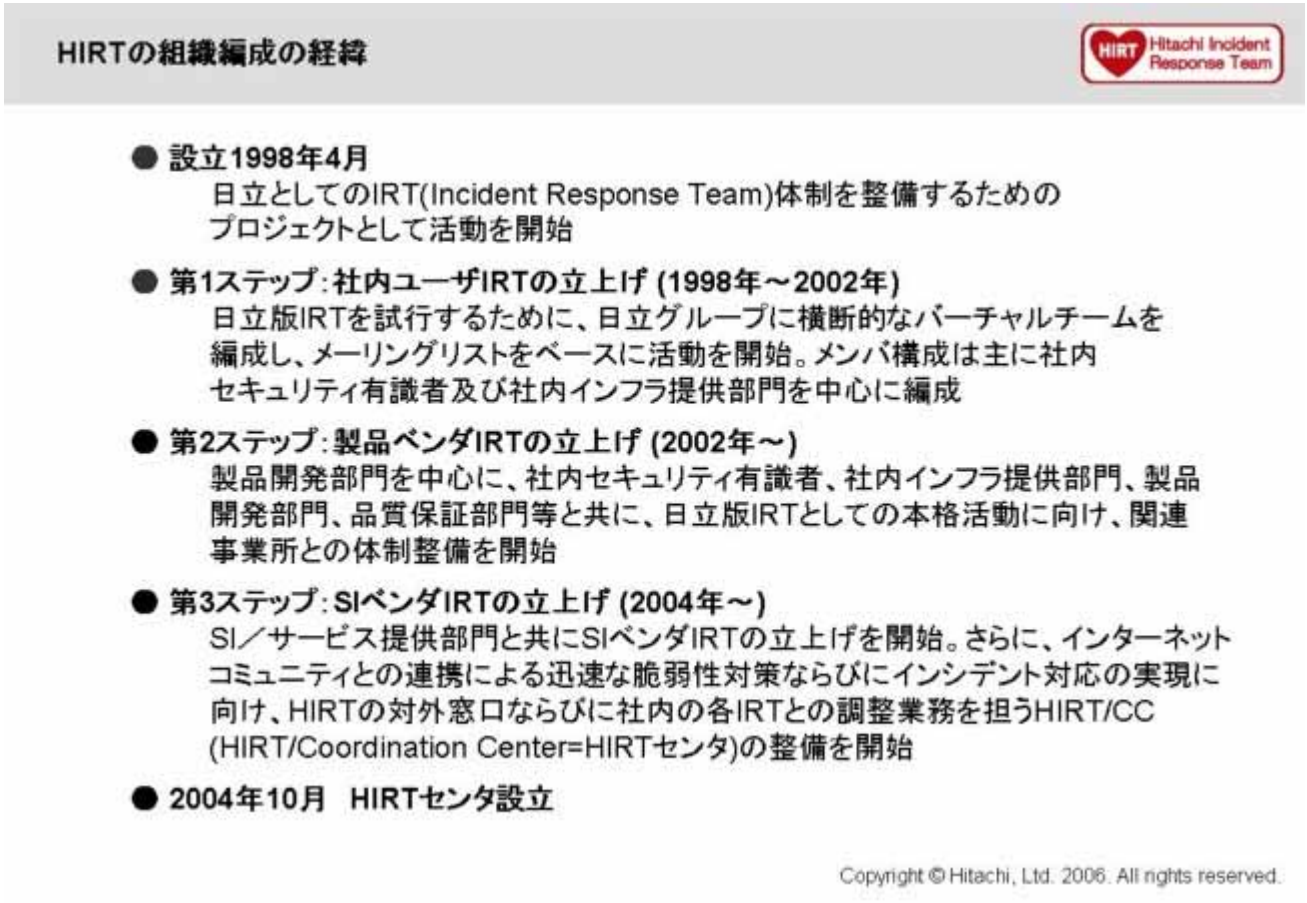

図3
全画面表示

脆弱性対策活動

HIRT の組織体制の話も一通り済みましたので、ここでは、CSIRT 活動の中から製品ベンダ IRT の活動を取り上げることにします。特に、情報セキュリティ早期警戒パートナーシップのソフトウエア製品に係る脆弱性関連情報の取扱を中心にご紹介します。なお、ソフトウエア製品に係る脆弱性関連情報の取扱全般については、ぜひ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を参照してください。

ソフトウエア製品に係る脆弱性関連情報の取扱のうち、JPCERT/CC から製品開発者である日立にソフトウエア製品の脆弱性関連情報が通知され、その影響有無ならびに対策情報を回答するまでのフローを図 4 に示します。取り組みに関する特徴は、次の通りです。

- 全体を把握しながら対策を推進するために、JPCERT/CC と各製品開発部署との間に HIRT センタが介在し、調査展開する窓口集約型モデルで運用しています。

- 脆弱性対策情報の発信ならびに広報活動も脆弱性対策活動の重要な一項目と考え、調査活動と情報公開活動をセットにした脆弱性対策活動を推進しています。具体的には、HIRT センタでは、窓口集約に加え、情報発信の集約として、2005 年 9 月 12 日から

http://www.hitachi.co.jp/hirt/、http://www.hitachi.com/hirt/ において、事業部や関連会社の発信する日立関連のセキュリティ情報へのリンクを掲載する活動を開始しました。

また、図 4 のフローには記載されていない部分ですが、日立が他社にも影響範囲が及ぶ脆弱性を発見した場合には「情報セキュリティ早期警戒パートナーシップ」の趣旨に沿い、IPA に報告し問題解決に寄与することになっています。何度か JVN に HIRT という名前が掲載されているのは、この活動の推進記録ということになります。

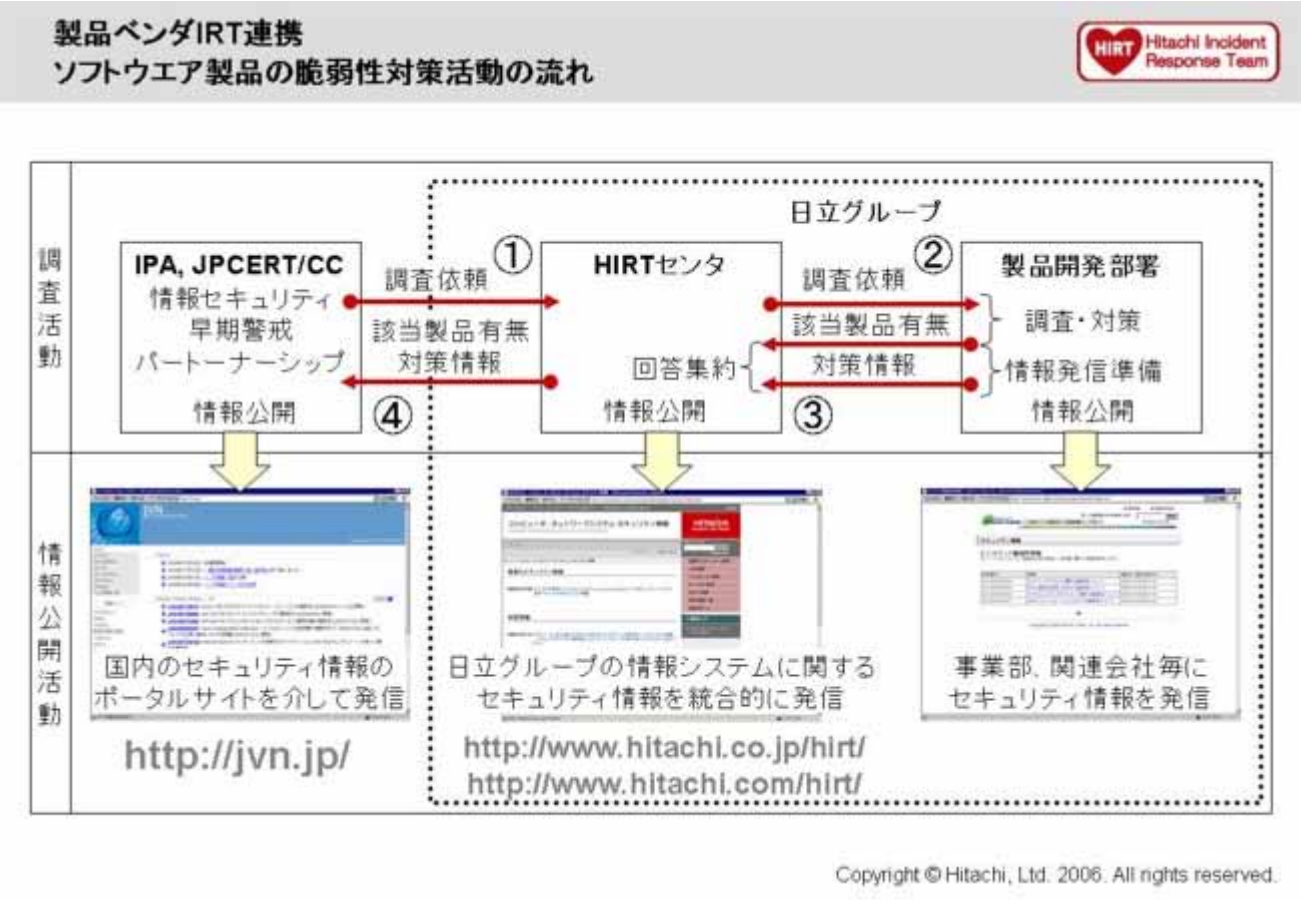

図4
全画面表示

さて、せっかくの機会ですので、このような脆弱性対策活動を通して私自身が得た経験値をいくつかご紹介したいと思います。

- 経験値 (1): ワールドワイドで利用されているソフトウエアであっても、そのソフトウエアを取り込んで開発された製品で、しかも国内向けに販売されている製品の場合、製品開発者がその販売地域に向けて対策を実施する必要があります。例えば、Web サーバとして著名な Apache を取込んで開発された国内向け製品や、MS SQL Server および Microsoft SQL Server Database Engine (MSDE) を利用した国内向け会計ソフトウエアなど数え上げると限りなく存在します。

- 経験値 (2): 国内を対象として販売される製品の脆弱性対策情報が CERT アドバイザリや CERT Vulnerability Notes Database に掲載されていることはほとんどありません。これは掲載可能な国内の製品開発者が少ないだけではなく、国内向けに製品開発する製品開発者にとって、海外展開していない製品の脆弱性対策情報を掲載する利点は少ないということにも起因しています。

- 経験値 (3): 国内の商用サービスによる脆弱性対策情報の多くは、英語圏の情報が翻訳され提供されているのが実情のようです。たとえば、国内向け製品の脆弱性対策情報を英語版として公開すると、英語圏のセキュリティ情報ベンダがその情報を拾い上げ、商用サービスが英語を日本語に再翻訳して提供しています。さらに、この経路の方が国内への情報の展開が速いようです。

以上の経験値から言えることは、脆弱性対策には言語という地域性だけではなく、製品販売という地域性も伴うということです。このような地域性に対しては、今後も情報セキュリティ早期警戒パートナーシップとJVNの活用が重要なポイントになってくると考えています。

ページのトップへ

インシデント対応活動

脆弱性対策活動の話が終われば、次はインシデント対応活動となるわけですが、ここでは、インシデント対応活動をも含むインシデントオペレーションという考え方についてご紹介します。

インシデントオペレーション

インシデントレスポンスという用語を聞いたことはあっても、インシデントオペレーションという用語ははじめて！という方も多いかと思います。インシデントレスポンスとは、事業継続に大きな影響を及ぼすような事象が発生した際に、あらかじめ決めておいた計画に沿って対処する事後処置を意味します。具体的には、各サイトは、サイトのセキュリティポリシーに応じたセキュリティ技術や製品を導入して、それらを適切に運用するとともに、近い将来発生し得るセキュリティインシデントに備えて、事前に対応手順を明確にします。また、インシデント発生時には、その対応手順に従った運用をおこない、その被害の拡大を最小限にするための行動がインシデントレスポンスとなります。

しかし、2001 年 8 月の Code Red、9 月の Nimda の流布、2003 年 1 月の Slammer、8 月の Blaster などの流布によって、イントラネットならびにインターネットに接続する多数のシステムが感染し、ネットワークサービスが一時的に停止状態に陥るなどの影響がでたことがきっかけとなり、事後処置を中心とした対処であるインシデントレスポンスに加えて、事前処置をも含んだ一連の対処活動が必要となってきました。事前ならびに事後処置から成る一連の対処活動がインシデントオペレーションであり、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と言うことができると思います。

Sasser を対象としたインシデントオペレーション

では、インシデントオペレーションについて、具体的な流れを見ていきましょう。ちょっと古い事例ですが、ここではネットワークワーム Sasser への対処を取り上げてみます。

ネットワークワームを対象としたインシデントオペレーションは、脆弱性ならびに修正プログラムの公開からネットワークワームが出現するまでの "脆弱性対策活動" とネットワークワームが出現した後の "インシデント対応活動" から構成することができます。ここで、脆弱性対策活動とは "セキュリティに関する何らかの問題を引き起こす脆弱性を除去するための活動" であり、"インシデント対応活動" とは "実際に発生している侵害活動の回避やセキュリティに関する問題事象を解決するための活動" を意味しています。そして、"脆弱性対策活動／インシデント対応活動" と Sasser 出現までの経過を対応付けると図 5 のようになります。次に、"脆弱性対策活動／インシデント対応活動" の中身として、活動内容を 6 つの段階、準備、警戒、予兆、対処、監視、収束にわけると共に、各段階の実施すべき活動と具体的な対応事例を表 1 に示します。

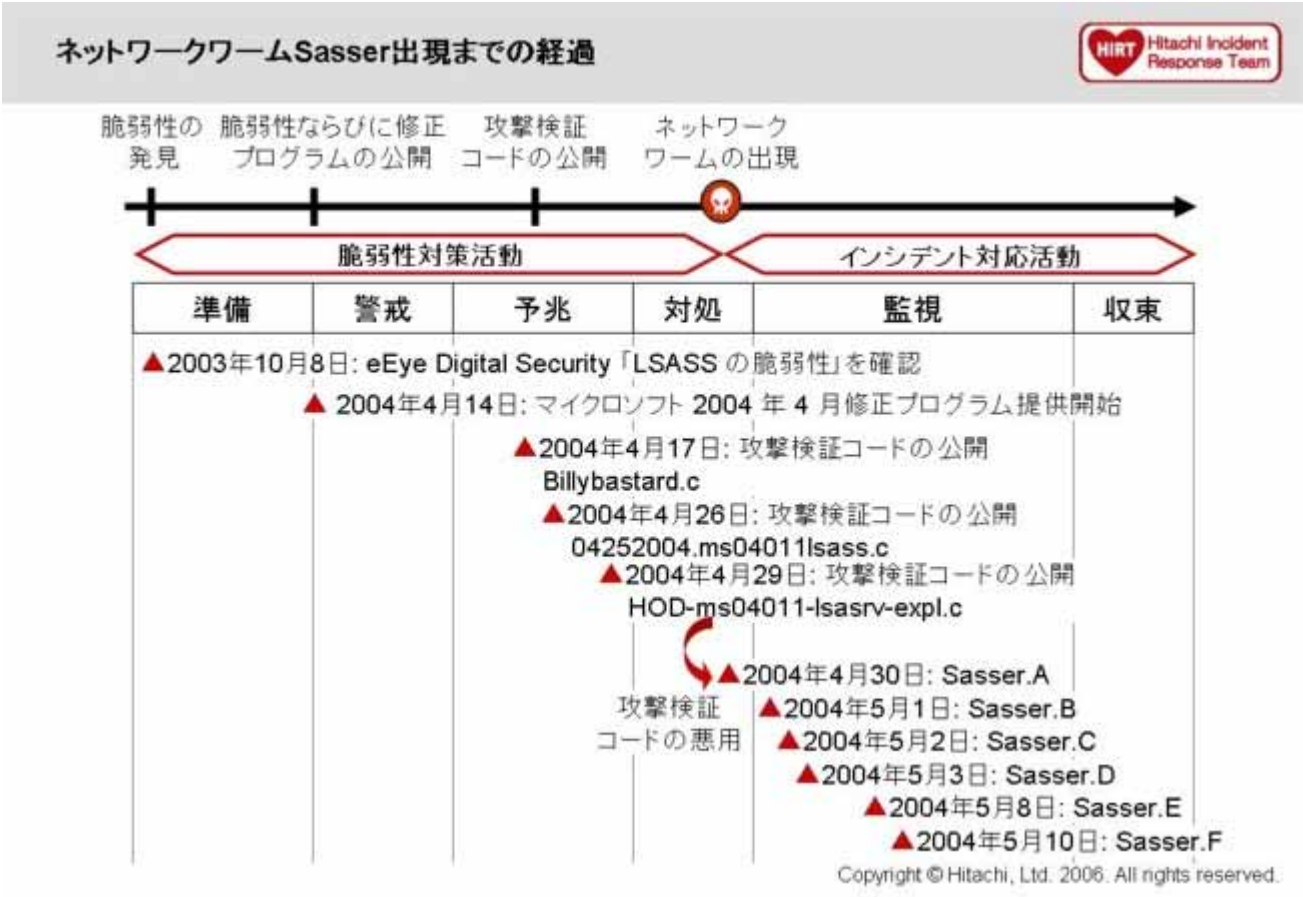

図5
全画面表示

表 1: ネットワークワーム対処のための 6 つの段階

段階	実施すべき活動	Sasser の場合の具体的な事例
準備段階	発見された脆弱性の解析を行なうことにより、脆弱性が与える影響、脆弱性への攻撃容易性を検討します。さらに、脆弱性を悪用された場合のインシデントシナリオを想定作成します。	Sasser の攻略対象とした MS04-011 のLSASS (Local Security Authority Subsystem Service) の脆弱性は、リモートから任意のコードを実行可能な脆弱性であり、マイクロソフトが MS04-011 で提示した深刻度は "緊急" でした。
警戒段階	修正プログラムの実機検証を行なうと共に、脆弱性公開に伴う各組織の対応を把握することにより、現時点でとりうる脆弱性の対策を判断します。	Sasser の場合、MS04-011 の公開に伴い、CERT/CC 、IPA、@police から Windows システム脆弱性対策に関する注意喚起がなされました。
予兆段階	攻撃検証コードの公開を監視する期間です。攻撃検証コー	予兆段階において、MS04-011 の PCT (Private Communications

	ドが公開された場合には、攻撃検証コードの解析により、実際に発生する影響 (DoS、任意のコード実行、権限昇格など)、動作適用範囲 (OS、言語、バージョンやサービスパック依存性など) と転用の可能性 (インシデントシナリオの修正) を検討し、脆弱性への攻撃容易性を再検討します。	Transport) の脆弱性に関する攻撃検証コードが先に公開されたために、LSASS の脆弱性への注目度が少し低下しました。また、PCT の脆弱性の攻撃検証コードが公開されたことと、大型連休を控えていたことから、経産省、総務省、警察庁が合同で Windows システム脆弱性対策に関する注意喚起を発行しました。
対処段階	攻撃検証コードから派生した侵害活動ならびにネットワークワームなどの出現期間です。侵害活動痕跡の調査ならびにネットワークワームの挙動解析により、これら侵害活動が与える影響、動作適用範囲 (言語依存性、サービスパックやバージョン依存性など) の確認を行なうと共に、侵害活動発生に伴う観測データを分析します。	Sasser は、2004 年 4 月 29 日に "houseofdabus" によって公開された攻撃検証コードを利用していました。この攻撃検証コードは英語版とロシア語版 Windows 2000 Professional と Windows 2000 Server、そして Windows XP Professional に対して攻撃を成功させることが確認されました。一方、日本語版 Windows 2000 に対しては攻撃が失敗することと、他言語版の Windows 2000 においても同様に攻撃は失敗する可能性があることが確認されました。
監視段階	ネットワークワームの亜種出現の兆候に関する監視強化、観測データの状況推移に関する監視強化を行ないます。また、急速な被害拡大を防止するための機能やシステムの稼動確認をおこない、緊急時に備えた体制を準備します。特に、ネットワークワームの亜種は、動作不良の解決、動作適用範囲の拡大、機能拡張などがおこなわれている場合もありますので、亜種出現時には対処段階と同様、ネットワークワームの挙動解析を行なう必要があります。	2004 年 4 月 30 日の Sasser.A に続き、Sasser.B (5 月 1 日)、Sasser.C (5 月2日)、Sasser.D (5 月 3 日)、Sasser.E (5 月8日)、Sasser.F (5 月 10 日) が亜種として出現しました。
収束段階	ネットワークワームの出現に伴い実施した一連の活動内容を関連組織間で整理すると共に、課題を確認し、その結果を次回以降のインシデントオペレーションにフィードバックします。	2004 年 5 月 8 日に Sasser 作成の容疑者が逮捕されました。Sasser に関する一連の活動は、Sasser.F (5 月 10 日) の出現後にほぼ収束したと言えます。

Sasser の場合には、予兆段階での攻撃検証コードの動作適用範囲の検証確認と、対処段階でのネットワークワームへの攻撃検証コードの流用についての検証確認がポイントとなります。具体的には、攻撃検証コードが日本語版 Windows 2000 に対しては攻撃が失敗することと、Sasser.A がその攻撃検証コードを取り込んでいることから、Sasser.A が日本語版 Windows 2000 を介して感染拡大する可能性がなく、日本語版 Windows XP に対する脆弱性対策の推進が被害拡大の低減につながるという判断ができたということです。

私自身がこの事例から得た経験値は次の通りです。

- ネットワークワームを対象とするインシデントオペレーションにおいては、脆弱性からネットワークワームへの発展を可能な限り早期に弁別し事前処置することが、インシデント発生後の被害拡大の低減につながります。

この経験値をつきつめていくと、インシデントオペレーションとは、対処判断のために必要となる正確な情報を入手する活動と言うことができるかもしれません。そして、かなり強引な導き方ですが、このような活動の実現には、"組織相互連携型のインシデントオペレーション"、すなわち、HIRT の組織編成のところで述べた "縦軸の組織と横軸のコミュニティが連携することにより CSIRT活動を推進するモデル" を外部の組織間にも当てはめるのが適しているのではないかと考えています。

ページのトップへ

最後に

日立における CSIRT 活動の締めくくりとして、私が JVN に関わるきっかけをお話することで CSIRT 活動の別な役割をご紹介したいと思います。

2004 年 7 月 8 日に施行された、経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」以降、JVN というサイトを知ることとなった方も多いかと思います。JVN 自身は、2002 年に JPCERT/CC Vendor Status Notes ワーキンググループとして産声を上げ、2003 年 2 月に試行サイト (http://jvn.doi.ics.keio.ac.jp) として公開されました。そして、2004 年 7 月の「ソフトウエア等脆弱性関連情報取扱基準」にあわせて、報告された脆弱性を公表するサイト (http://jvn.jp) にその役割を引き継いでいます。実は、JPCERT/CC Vendor Status Notes ワーキンググループとして活動を開始したきっかけは、私自身が日立における CSIRT 活動を通して感じていた疑問の投げかけだったのです。

> 様々な国内での教育活動で紹介されている CERT アドバイザリに国内を販売対象とするソフトウエア製品に関する対策情報が掲載されていない。CERT アドバイザリで脆弱性に関する存在を知ることはできても、対策情報としての情報は不足していることになる。つまり、自らが生活する国内の対策情報源がないということは、十分な脆弱性対策活動を進めることができない。

CSIRT 活動を通して感じた疑問の投げかけも、CSIRT の役割なのかもしれません。

最後となりますが、今後も、『HIRT (Hitachi Incident Response Team) は、インターネットコミュニティとの連携による迅速なインシデントオペレーション (脆弱性対策ならびにインシデント対応) を通して、安心かつ安全なネットワーク環境の実現に寄与することを目的とした日立グループの活動組織です。』の実行を通して、情報社会の発展に寄与していきたいと考えています。