コンピュータセキュリティ　10－27
（2000．　7．25）

企業内不正アクセス対策情報サービスシステムの構築

寺田真敏 †　　萱島　信 †　　倉田盛彦 ‡
terada@sdl.hitachi.co.jp　　kayashi@sdl.hitachi.co.jp　　m-kurata@itd.hitachi.co.jp

† (株)日立製作所 システム開発研究所
〒224-0817　神奈川県横浜市戸塚区吉田町 292
‡ (株)日立製作所 情報システム事業部
〒100-8220　東京都千代田区丸の内 1-5-1

あらまし：不正アクセスによって引き起こされる企業情報システムへの被害は多大なものであり、企業内における不正アクセス対策の推進は重要な課題となっている。企業内での不正アクセス対策活動においては、部署の業務に則した不正アクセス対策活動を考慮するとともに、その活動を維持していく必要がある。本稿では、企業内での不正アクセス対策活動を支援するために構築した不正アクセス対策情報サービスシステムについて述べる。構築したシステムでは、ネットワーク管理者向けサービスとして不正アクセス動向把握のための統計情報、危険度/対策緊急度/対策解説を付加した脆弱性対策情報を、一般ユーザ向けサービスとして被害状況把握のための統計情報、不正アクセス事例情報やデモを提供する。
キーワード：不正アクセス、ネットワークセキュリティ、インシデントレスポンスチーム

Development of Enterprise Information Service System for Unauthorized Access Protection

Masato Terada †　　Makoto Kayashima †　　Morihiko Kurata ‡
terada@sdl.hitachi.co.jp　　kayashi@sdl.hitachi.co.jp　　m-kurata@itd.hitachi.co.jp

† Systems Development Laboratory, Hitachi Ltd.
292 Yoshida-cho, Totsuka-ku, Yokoham, 244-0817 Japan
‡ Information Technology Division, Hitachi Ltd.
1-5-1 Marunouchi, Chiyoda-ku, 100-8220 Japan

Abstract: Because unauthorized access causes a lot of damage to the enterprise information system, the promotion of the unauthorized access protection in the enterprise is an important subject. As for the unauthorized access protection activities in the enterprise, the each division promotes the activities and the level of activities are maintained. This paper described the overview of the information service system for unauthorized access protection activity. A built system provides statistics information for unauthorized access trend and the security advisory information which the risk level/urgent level/solution advice are provided as a service for the network administrator. Furthermore, statistics information for damage conditions by unauthorized access and the visible demonstration about unauthorized access are provided as a service for the general user.
key words: Unauthorized Access, Network Security, Incident Response Team

1. はじめに

インターネットに接続される計算機は7300万台に達し[1]、Web、電子メールを始めとするインターネットアプリケーションは、大学や企業だけではなく一般家庭にまで広がっている。このような利用範囲の広がりとともに悪意を持ったユーザによる計算機資源への不正アクセスの危険性は増大している。米国の調査によると、セキュリティインシデントの被害総額は1996年から毎年1億ドルを超えており、2000年の報告では総額として2億6559万ドルにのぼるとしている[2]。また、CERT/CC[*1]、JPCERT/CC[*2]の報告でも不正アクセスの発生件数は増加傾向にある[3][4]。

このような不正アクセスに対応するためには、ユーザ環境にあわせ、「回避/防止」「保証」「検知」「調査」の4つのフェーズからなる作業を継続的に繰り返しながらセキュリティ強化を図っていく必要があるとされているが(図 1.1)[5]、これらのフェーズを運用していくためには、該当するセキュリティ施策を導入するだけではなく、不正アクセスの動向把握、不正アクセスを未然に防ぐための脆弱性対策情報の収集と対策実施、不正アクセスの脅威分析や最新の不正アクセスにも早急に対処できる体制を整えていくことが必要となる。

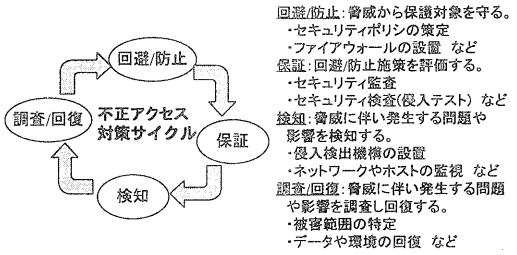

図 1.1 不正アクセス対策サイクル

インターネットの世界では、国レベル、企業レベルでネットワークセキュリティに関する問題を取り扱う不正アクセス対応機関を設置することにより、不正アクセス対策や対応に取り組んでいる[6]。しかし、国内においては、国レベルの不正アクセス対応機関である情報処理振興事業協会(IPA)[*3]、JPCERT/CCの活動に比べ、企業レベルでの活動は明確に確立されていないのが現状である。

そこで、本稿では、企業内における不正アクセス対応機関の活動の一環として、不正アクセス対策活動の推進を支援する、企業内不正アクセス対策情報サービスシステムを構築運用したので、その概要について述べる。

2. 企業内における不正アクセス対策活動の課題

企業内における不正アクセス対策活動は企業の業種やビジネス形態により異なる。ここでは、コンピュータメーカ／ベンダを対象に企業内における不正アクセス対策活動を取り上げてみると、以下の2つの側面が考えられる。

- メーカ／ベンダとしての立場から製品開発や顧客にサービスを提供する側面
- 企業自身が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

いずれの場合も企業のセキュリティポリシーのもと、各部署が業務に則した不正アクセス対策活動を進めていくことになる。また、このような企業内の不正アクセス対策活動を進めていく際には、各部署の不正アクセス対策活動を一定以上のレベルに維持していく必要があり、その不正アクセス対策活動を維持していくうえで必要となる対策情報の取扱いに関して、以下のような課題がある。

(1) 対策情報選別の迅速化

各部署は、必要となる脆弱性情報や対策情報をすばやく抽出し、対策実施につなげる必要がある。また、これらの抽出情報が各部署ごとに異なると整合性のとれていない対策を行ってしまうこととなるため、この点も考慮する必要がある。

(2) 対策情報理解の容易性確保

CERT/CC、CIAC[*4]をはじめとする主要な不正アクセス対応機関が発行するセキュリティアドバイザリ情報は重要な情報であるにもかかわらず英文であるために、多くのシステム管理者はこれらの

---

*1) Computer Emergency Response Team Coordination Center

*2) Japan Computer Emergency Response Team Coordination Center

*3) Information technology Promotion Agency, Japan

情報購読に躊躇してしまうことがある。必要となる情報をすばやく抽出しても購読時間や内容把握に時間を要すると、不正アクセス対策の開始が遅れることになる。また、対策情報によっては、一般ユーザの利用する計算機環境に関連するものもあり、一般ユーザに対しては、目に見えにくい不正アクセスの影響や危険性をわかりやすいものとして提示することにより、セキュリティに対する意識向上を図っていく必要がある。

(3) 対策レベルの整合性確保

脆弱性が与える影響を十分に把握できていないと、影響の大きい問題への対策が遅れたり、影響の小さい問題に対して過大に対策してしまう可能性がある。また、これらの評価が関連各部署に異なると整合性のとれていない対策を行ってしまうこととなる。したがって、対象となる脆弱性への適切な判断指標を提示する必要がある。

3. 企業内における不正アクセス対策活動

本章では、2章で述べた課題を解決するための企業内における不正アクセス対策活動について述べる。

3.1 企業内不正アクセス対応機関

企業内における不正アクセス対策活動にあたっては、企業内における不正アクセス対策活動を支援するための枠組みを用意し、その枠組みの中核の役割を果たす組織を企業内不正アクセス対応機関と定義する。

IPA や JPERT/CC など国レベルの不正アクセス対応機関の役割が不正アクセスの被害を受けた当事者やそれをサポートするサービスプロバイダやコンピュータメーカなど異なる組織間の協調を図り、被害に対して緊急対応が必要となる活動を円滑に運営していくことであるのに対し、企業内不正アクセス対応機関は、不正アクセス対策活動を推進する部署間の協調を図り、企業の不正アクセス対策活動の円滑な運営を支援することを目的とする。

3.2 企業内不正アクセス対策情報提供サービス

不正アクセス対策活動を推進していくうえで必要となる対策情報の取扱いの課題については、企業内不正アクセス対応機関を中心に、不正アクセス対策活動を進めるうえで必要となる情報、解説、対策のための適切な判断指標を提示することにより課題を解決する。これにより、各部署の不正アクセス対策活動のレベルを維持していくことができる。さらに、セキュリティ情報の提供目的を明確にすることと、対策情報理解の容易性を確保することから、以下のように対象ユーザを分け情報提供を行う。

(1) ネットワーク管理者向けサービス

企業情報システムの運用に携わっている管理者は、不正アクセスの動向把握や脆弱性情報などの情報を収集し、次に収集した情報の分析を行い必要となる対策を策定した後、対策を実施する必要がある。また、顧客にサービスを提供する部門、製品開発をする部門においても、同様な活動が求められる。そこで、これらの活動を支援するために、不正アクセス動向把握のための統計情報、対策策定を支援するための危険度/対策緊急度/対策解説を付加した脆弱性対策情報を提供する。また、脆弱性対策情報については、遅延なくネットワーク管理者等の特定者に配信する。

(2) 一般ユーザ向けサービス

一般のユーザに対しては、セキュリティに関する倫理的な教育に加え、不正アクセス対策に関心を持たせ、さらに、セキュリティに対する意識向上を図っていくことが重要となる。そこで、不正アクセスによる被害状況把握のための統計情報、不正アクセス事例情報や不正アクセス自体がどのようなものであるのかを視覚的に理解してもらうためにビジュアル化した不正アクセスのデモを提供する。

3.3 実現例

企業内での不正アクセス活動を支援するために今回設置した企業内不正アクセス活動機関であるHIRT(Hitachi Incident Response Team)について、その位置付けと役割を一例として紹介する。

企業内不正アクセス対応機関として設置した

---

*4) Computer Incident Advisory Capability

HIRTは、企業内の不正アクセス対策活動を推進する部署間の協調を図り、企業内における不正アクセス対策活動の円滑な運営を支援することを目的とした組織である。

活動の中心である企業内の不正アクセス対策活動の支援では、課題である「対策情報選別の迅速化」「対策レベルの整合性確保」「対策情報理解の容易性確保」を解決することと、支援活動を通してインターネットセキュリティや不正アクセス対策技術のノウハウ蓄積を推進している。

(1) 情報収集活動
- インターネットセキュリティに関する技術情報、不正アクセスの動向情報や脆弱性情報などの収集

(2) 情報分析活動
- 不正アクセスの脅威分析
- 脆弱性対策の検討

(3) 情報提供活動
- 不正アクセス対策に関する情報や勧告の発行
- セキュリティツールの配布
- インターネットセキュリティ技術の教育活動

また、これらの支援活動の成果を、不正アクセス対策情報サービスとして各部署への提供を行っている。

4. 不正アクセス対策情報サービスシステム

本章では、支援活動の成果を提供する企業内不正アクセス対策情報サービスシステムについて述べる(図 4.1)。

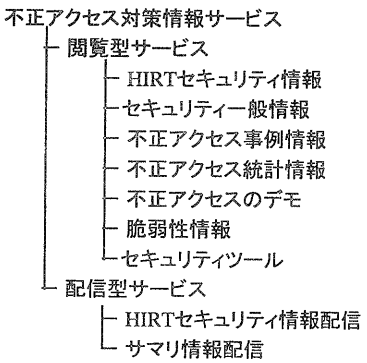

図 4.1 不正アクセス対策情報サービス

4.1 閲覧型サービス

閲覧型サービスでは、各ユーザの端末(Web 閲覧ソフト)から利用することのできるサービスを提供する。各サービスの概要は、以下の通りである。

(1) HIRT セキュリティ情報

HIRT セキュリティ情報には、外部の不正アクセス対応機関が提供するセキュリティ情報ならびに、ベンダが提供するセキュリティ情報に基づき発行する外部情報と、HIRT の独自調査により発行する内部情報とがある。外部情報の場合には、そのセキュリティ情報の危険度/対策緊急度/日本語による対策解説を付加している。危険度では不正アクセスの攻撃対象を明確にするとともに発生しうる脅威の指標を(表 4.1)、対策緊急度では対策の時期的な指標を提示している(表 4.2)。ここで、危険度/対策緊急度は対策レベルの整合性確保を、日本語による対策解説は対策情報理解の容易性確保を実現するものである。

表 4.1 脆弱性に関する危険度の指標

レベル	対象	発生しうる脅威
高	サーバ	リモート/登録ユーザが管理者権限の不正取得、プログラム起動やシステムファイル操作が実施できる。
	クライアント	広範囲に影響を与える不正アクセス型ウィルスである。
中	サーバ	管理者以外のユーザ権限を不正に取得できる。 サーバ全体/特定サービスに影響を与えるサービス妨害である サーバ上のデータを不正に参照できる。
	クライアント	不正アクセス型ウィルスを利用し、クライアント上のデータを不正に参照できる。 リモートユーザがプログラム起動やシステムファイル操作が実施できる。
低	クライアント	ブラウザなどを利用し、クライアント上のデータを不正に参照できる。 クライアント全体/特定サービスに影響を与えるサービス妨害である。

表 4.2 脆弱性に関する対策緊急度

レベル	対策時期とアドバイス
即日	システムの運用を止めてでもすぐに対策を実施する必要がある
後日	他の対策との併用により，ある程度時期をみて対策を実施しても良い。 ただし、該当するサービスに対して、ファイアウォールやルータによるアクセス制御を実施している場合に限る。 ただし，登録ユーザを管理者だけに絞り込んでいる場合に限る。
	ある程度時期をみて対策を実施しても良い。ただし、サービス妨害などの攻撃を受けた場合、サービスの定常的な提供を実施できない。

(2) セキュリティ一般情報

HIRT セキュリティ情報で網羅することのできない不正アクセス対策関連の技術、製品ならびに、不正アクセス対応機関やベンダが提供するセキュリティ情報などを Web のリンク情報として提供する。

(3) 不正アクセス事例情報

事件として公開されている情報を Web のリンク情報として提供する。これまで提供してきた不正アクセスの事例には、以下のようなものがある。

- Web ページの書き換えに関する事例
- システムへの不正侵入に関する事例
- 不正アクセスにともなう被害統計や予測
- 内部情報ならびにプライバシ情報流出の事件など

(4) 不正アクセス統計情報

不正アクセス活動の傾向把握を目的とした情報と、不正アクセスの被害状況把握を目的した情報とがある。前者はネットワーク管理者を対象としており、後者は一般ユーザを対象としている。

(5) 不正アクセスのデモ

一般ユーザに不正アクセスの影響や危険性を理解してもらうために、目に見えにくい不正アクセス技術ならびにその影響を、以下のようなビジュアル化したデータとして提供する。これにより、一般ユーザは視覚的に不正アクセスの影響や危険性を知ることができる。

(6) 脆弱性情報

HIRT セキュリティ情報を発行する際に危険度や対策緊急度を検討するための情報であり、インターネット上に公開されている情報へのリンク情報、検証/検討結果などを提供する[7]

(7) セキュリティツール

不正アクセス対策活動を支援するためのセキュリティツールを提供する。これまでに、定義ファイルを用いたセキュリティ検査ツールを提供している[8]。

4.2 配信型サービス

配信型サービスでは、電子メールを用いて各ユーザに情報を直接配布する。HIRT セキュリティ情報や新たなサービス提供開始通知のような随時配信サービスと、定期的な配信サービスがある。

(1) HIRT セキュリティ情報

「対策情報選別の迅速化」「対策レベルの整合性確保」「対策情報理解の容易性確保」のいずれにおいても、脆弱性対策情報を遅延なくネットワーク管理者等の特定者に配信することが重要となる。この配信サービスでは、予め登録されたユーザを対象に HIRT セキュリティ情報の電子メール配信を行う。

(2) サマリ情報配信

電子メールを用いた情報配信では、配信数の増加を抑えながら必要となる不正アクセス対策情報を提供することが重要となる。この配信サービスでは、HIRT セキュリティ情報とセキュリティ一般情報の発行日付と題目のみを月 2 回(1 日、15 日)配信することにより、閲覧型ならびに配信型サービスの情報購読促進を補助する。

4.3 サービス提供実績と利用状況

構築したシステムのサービス提供実績と利用状況について述べる。

(1) 閲覧型サービス

セキュリティ一般情報は月平均 38 件、不正アクセス事例は月平均 14 件、統計情報は年 4 回の割合で更新を行っており、これに伴う閲覧型サービスの月別利用状況は図 4.2の通りである。

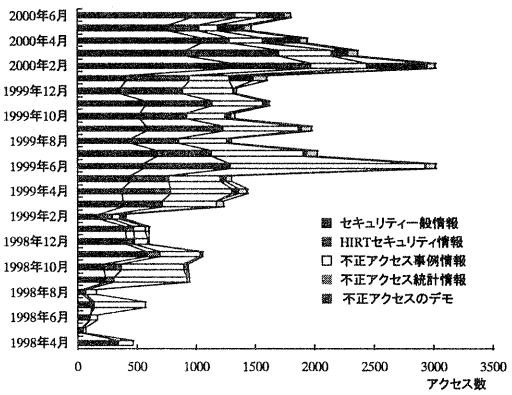

図 4.2 閲覧型サービスのアクセス状況

(2) 配信型サービス

配信型サービスの 1 次配信先は約 200 個所であり、サービスとして配布した HIRT セキュリティ

情報件数は、1998年で56件、1999年で166件、2000年は6月末までで80件、月平均10件の配信数となっている(図 4.3)。

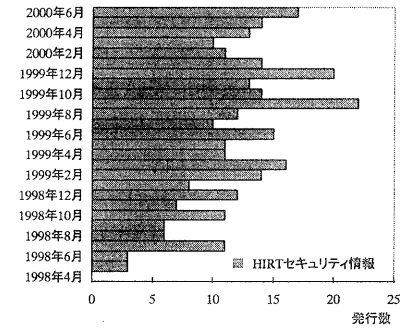

図 4.3 HIRTセキュリティ情報の発行状況

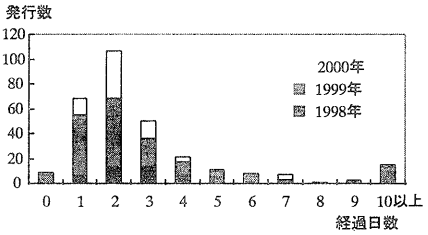

図 4.4 HIRTセキュリティ情報発行までの日数

また、HIRTセキュリティ情報のうち、外部情報に危険度/対策緊急度/日本語による対策解説を付加することによる配信遅延は、配信数の約8割が3日以内となっている(図 4.4)。情報提供元が海外の場合には、時差を考慮すると、ほぼ2日以内に最新の情報を配信していることになる。

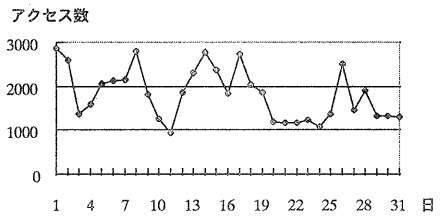

図 4.5 1ヶ月あたりの累積アクセス数の変位

サマリ情報配信にともなう閲覧型サービスのアクセス数の変位では、サマリ情報配信後の5日間の平均アクセス数は残りの日の約1.2倍となっており、サマリ情報配信が不正アクセス対策情報購読の促進に対して効果をあげている(図 4.5)。

5. おわりに

本稿では、企業内における不正アクセス対策活動において、企業内不正アクセス対応機関の役割を規定するとともに、対応機関の活動成果を提供する不正アクセス対策情報サービスシステムを構築運用した結果について述べた。

対策情報の取扱いの課題である「対策情報選別の迅速化」では閲覧型サービスで月平均38件、配信型サービスで月平均10件に絞り込みを行い、「対策情報理解の容易性確保」ならびに「対策レベルの整合性確保」では、危険度/対策緊急度/日本語による対策解説を付加する作業を経てユーザにHIRTセキュリティ情報として配信されるまでを2日以内としている。

今後の課題としては、部署やユーザに応じた木目細かな閲覧型/配信型サービスの実現や、不正アクセス対策情報サービスシステムと活用状況や対策実施状況の追跡調査機構とを連動させた対策活動の支援などが挙げられる。

参考文献

1) "Internet Domain Survey", January 2000, http://www.isc.org/
2) "2000 CSI/FBI Computer Crime and Security", 2000, http://www.gocsi.com/
3) CERT/CC Statistics 1988-1998, http://www.cert.org/stats/cert_stats.html
4) JPCERT/CC Statistics, http://www.jpcert.or.jp/anm/stats.html
5) 不正侵入はこう防げ, 日経コンピュータ, No.448, pp185-195, July 1998
6) Forum of Incident Response and Security Teams (FIRST), http://www.first.org/
7) 寺田, 甲斐, 熊谷：不正なTCPコネクション確立に関する一考察, 研究会報告 99-CSEC-6, pp.25-30, 情報処理学会 (Jul. 1999)
8) 寺田, 甲斐, 熊谷：定義ファイルを用いたセキュリティ検査システムの開発, CSS'99, pp.141-146, 情報処理学会 (Oct. 1999)