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[††] 佐々木良一[†]

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るため，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，各部署が部署の業務に則した形で自律的に推進する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．本論文では，各部署の不正アクセス対策活動の支援ならびに，部署間にまたがった情報交換の場を提供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の有効性について検証する．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，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，一般ユーザ向けサービスとして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を視覚的に見ることのできるデモを提供する．本サービスシステムの運用を通して得られた利用実績とアンケート調査から，構築したシステムが実用的なシステムであることを確認した．

Development of Enterprise Information Service System for Unauthorized Access Protection

Masato Terada,[†] Makoto Kayashima,[†] Morihiko Kurata[††] and Ryoichi Sasaki[†]

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 implementation and evaluation 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. The validity of the built system was confirmed from the use conditions and the questionnaire investigation.

1. はじめに

近年，ネットワーク環境においては，データ破壊，改ざん，侵入，システム自身の稼動停止など，計算機資源への不正アクセス対策が重要になってきている．特にインターネットの普及により，遠隔からネットワークを経由して攻撃対象となる計算機への侵入や停止を目的とする不正アクセスが増えている．このような不正アクセスに対応するためには,「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実施することにより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[1)]．国内でも不正アクセス対策環境は徐々に整いつつあり，多くの組織が「回避/防止」としてファイアウォールをはじめとするアクセス制御システムを導入するに至っている．また，最近では,「回避/防止」としてセキュリティポリシーを策定したり,「保証」として不正アクセスシミュレータを用いた「セキュリティ検査」を行うなど不正アクセス対策の施策も広がりつつある．この４つ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

† 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi Ltd.
†† 株式会社日立製作所情報システム事業部
Information Technology Division, Hitachi Ltd.

必要となる．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[2]．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IPA☆1,3)，JPCERT/CC☆2,4)の活動に比べ，企業レベルでの不正アクセス対応機関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，本論文では，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，以下のような特徴を持つ企業内不正アクセス対策情報サービスシステムを構築し，そのサービスの有効性を検証する．

(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システム管理者，顧客にサービスを提供する部門，ならびに，製品開発を担当する部門を対象とし，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．

(2) 一般ユーザ向けサービス
企業情報システムを利用するユーザを対象とする．一般ユーザに対しては，セキュリティ教育の一環として，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のビジュアル化した不正アクセスのデモを提供する．

企業内不正アクセス対策情報サービスシステム構築にあたっては，顧客にサービスを提供する部門，製品開発をする部門と企業情報システムを運用管理する部門とが積極的に情報交換することのできる場を提供するために，企業内不正アクセス対応機関としてHIRT（Hitachi Incident Response Team）を設置するとともに，企業内における不正アクセス対応機関の役割と活動内容を明確にした．次に，部署間の情報交換ならびに不正アクセス対策活動を支援するために企業内不正アクセス対策情報サービスシステムを構築した．

以下，2章で企業内における不正アクセス対策活動の課題を，3章で企業内での不正アクセス対策活動について，4章で構築した企業内向けを対象とした不正アクセス対策情報サービスシステムについて示す．5章では不正アクセス対策情報サービスシステムの利用実績から構築したシステムの有効性を示す．

☆1 Information technology Promotion Agency, Japan
☆2 Japan Computer Emergency Response Team Coordination Center

2. 企業内における不正アクセス対策活動の課題

本章では，不正アクセス対策情報の取扱いの見地から，企業内における不正アクセス対策活動の課題について述べる．

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全体のセキュリティポリシーの下，各部署が部署の業務に則した形で自律的に不正アクセス対策活動を進めていくこととなる．しかしながら，このような企業内の自律的な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**
インターネットの普及と積極的な情報発信/公開活動の流れから，インターネット上には不正アクセスに関連する脆弱性情報や対策情報があふれている．これらの情報の中から不正アクセス対策活動を進めるうえで必要となる情報抽出に時間を要してしまうと，不正アクセス対策の開始が遅れることになる．したがって，各部署は，必要となる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☆3，CIAC☆4，AusCERT☆5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情報購読に躊躇してしまうことがある．必要とな

☆3 Computer Emergency Response Team Coordination Center
☆4 Computer Incident Advisory Capability
☆5 Australian Computer Emergency Response Team

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．したがって，抽出した情報をいかに早く購読し，内容把握するかが課題となる．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る．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分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

不正アクセス技法が高度化するとともに，脆弱性の問題も多岐にわたってきている．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たり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．したがって，対象となる脆弱性が「何を対象としているのか？」「どの程度の危険性があるのか？」「対策の緊急性はどのくらいのものなのか？」など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

前章で，企業内における不正アクセス対策活動では，各部署が不正アクセス対策活動を推進しつつ，さらにその活動を一定以上のレベルに維持していくことの必要性について述べた．そこで，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することにより，各部署の不正アクセス対策活動の推進と維持を図る．このとき，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，自律的に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

次に，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，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，不正アクセス対策活動として，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，対策を実施するという継続的な活動が必要となる．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など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 HIRT での実現例

本節では，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．

(1) HIRT の役割

企業内不正アクセス対応機関として設置した HIRT では，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第 1 の目的としている．このため，外部の不正アクセス対応機関との協調ならびに社外ユーザの支援などの対外活動は該当関連部署が対応することとし，企業内の対策活動の支援に主体を置いた活動を行っている（**図 1**）．

(2) HIRT の活動内容

活動の中心である企業内の不正アクセス対策活動の支

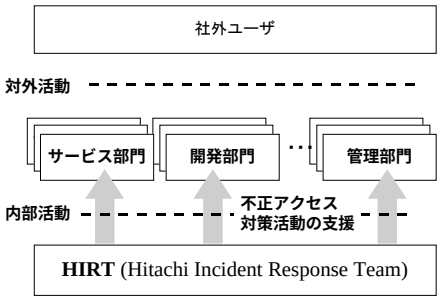

図 1 HIRT の位置付け
Fig. 1 Role of HIRT.

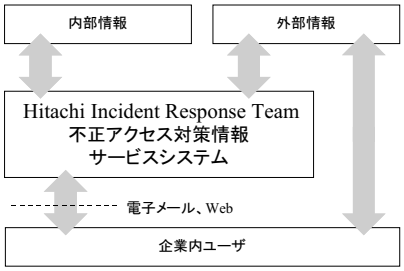

図 2 不正アクセス対策情報サービスの位置付け
Fig. 2 Role of the HIRT information service.

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ならびに共有を推進している．

(a) **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

(b) **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

(c) **情報配布活動**
- 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

(3) **HIRT 情報提供サービス**

上記の不正アクセス対策活動支援の一環として，不正アクセス対策情報サービスシステムを構築することにより，支援活動の成果を各部署で活用する形態をとっている（**図 2**）．ここで，不正アクセス対策情報サービスシステムが取り扱う情報には，外部情報と内部情報とがある．外部情報は主にインターネットなどから得られる公開情報があり，内部情報は独自に調査した

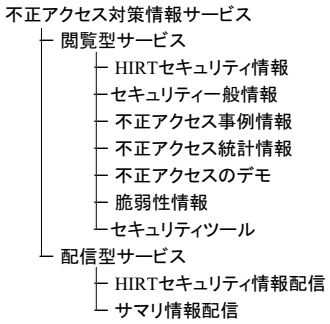

図 3 不正アクセス対策情報サービスの構成
Fig. 3 Structure of the HIRT information service.

内容や開発したセキュリティツールなどがある．また，サービス対象範囲は，企業内ユーザを対象とした Web による閲覧型サービスと電子メールによる配信型サービスを提供する．

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 3**）．

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．

(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（**表 1**）ならびに，ベンダが提供するセキュリティ情報（**表 2**）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，対策緊急度では対策の時期的な指標を提示している（**表 3**，**表 4**）．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．

(2) **セキュリティー般情報**

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，表 1，表 2 以外の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．情報の緊急度と重要度の違いを明確にするために，HIRT セキュリティ情報とセキュリティ一般情報の 2 段階の情報提供を行っている．

表 1 不正アクセス対応機関が提供するセキュリティ情報
Table 1 IRT's security information bulletin.

不正アクセス対応機関	発行セキュリティ情報
CERT/CC	・Advisory ・Summary ・Vulnerability Note ・Incident Note
JPCERT/CC	・緊急報告 ・ニュースレター
CIAC	・Information Bulletin
AusCERT	・Advisory ・Alert

表 2 ベンダが提供するセキュリティ情報
Table 2 Vendor's security information bulletin.

ベンダ	発行セキュリティ情報
Cisco	・Field Notice ・Internet Security Advisory
Hewlett-Packard	・Daily Security Bulletins Digest
Microsoft	・Security Bulletin
日本マイクロソフト	・Security Advisor（日本語） ・新着サポート技術情報
Netscape	・Security Note
Sun Microsystems	・Security Bulletin

(3) 不正アクセス事例情報

不正アクセスの事例では，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

不正アクセスの統計情報では，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，JPCERT/CC が定期的に発行する「活動概要：不正アクセスの動向」[5]をグラフ化した後，CERT/CC が発行するセキュリティ情報公開時期を併記した統計情報（**図 4**）などがある☆．このような時系列的なグラフ化により，脆弱性の公開時期と不正アクセス活動との関連性が分かりやすくなる．また，後者は一般ユーザを対象としており，イン

☆ JPCERT/CC（http://www.jpcert.or.jp/）の公開資料（JPCERT-E-NL-98-0001-01，JPCERT-E-NL-98-0002-01，JPCERT-E-NL-98-0003-01，JPCERT-E-NL-98-0004-01）を基に作成．

表 3 脆弱性に関する危険度の指標
Table 3 Definition of the risk level.

レベル	対象	発生しうる脅威
高	サーバ	・リモート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． ・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を実施できる．
	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 脆弱性に関する対策緊急度
Table 4 Definition of emergency level for countermeasure.

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よい． ・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よい． ・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．

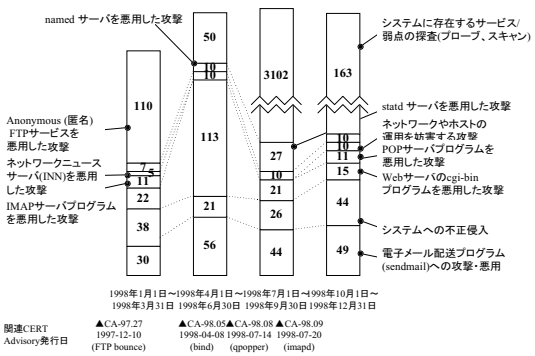

図 4 統計情報の例：不正アクセスの動向
Fig. 4 Trend of unauthorized access.

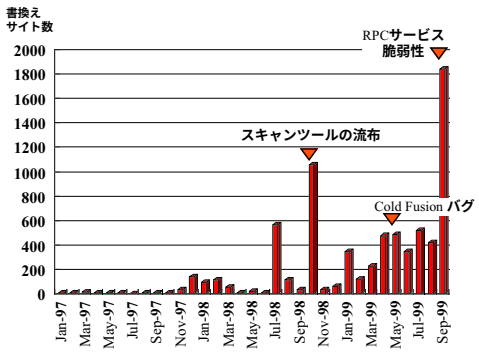

図 5 統計情報の例：Web サイトの書き換え（1）
Fig. 5 Web site defaced (1).

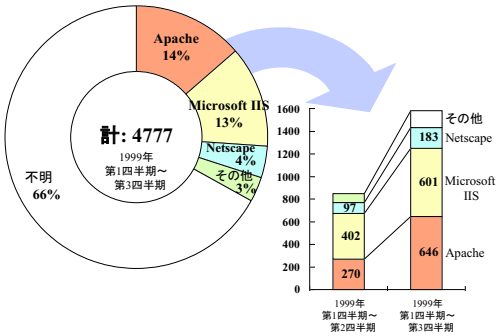

図 6 統計情報の例：Web サイトの書換え（2）
Fig. 6 Web site defaced (2).

ターネット上で不正アクセスに関する情報発信を活発に行っている多数の Web サイトを調査し，その調査結果に基づき作成した Web サイトの書き換え発生状況の統計情報（**図 5**）や，書き換えの発生した Web サイトのサーバプログラムの状況を独自に調査した統計情報（**図 6**）などがある．

(5) **不正アクセスのデモ**

不正アクセスのデモは，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．

- デモ内容の説明資料
- 不正アクセスの様子を録画した画面データ

録画データの作成は，Windows☆環境で動作するスクリーン録画再生ソフトウェア ScreenCam☆☆を用いており，また，不正アクセスを助長させることのないよう手口が直接的に見えないような構成としている．これまでに提供してきた不正アクセスのデモを**表 5** に示す．

表 5 不正アクセスのデモ例
Table 5 Example of the unauthorized access demonstration.

分類	デモ概要
ネットワーク	・**不正パケット送信**：不正なパケットの送付によりネットワーク機能をハングアップさせる．
ブラウザ	・**JavaScript，ActiveX 悪用による情報送信**：JavaScript，ActiveX を利用してクライアント上のデータを不正に取得する． ・**Hostile Applet**：サービス不能を目的とした Java アプレット
パスワード解読	・辞書を利用したパスワードクラッキング
アプリケーション	・**IMAP サーバへの不正アクセス**：不正なデータの送付によりシステムに侵入する． ・**HTTP サーバへの不正アクセス**：不正なデータの送付によりシステムデータを参照する．

(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[6]．

(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[7]．

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など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，あらかじ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っている．

(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

☆ Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標である．

☆☆ ScreenCam は，米国およびその他の国における米国 Lotus Development Corp. の登録商標である．

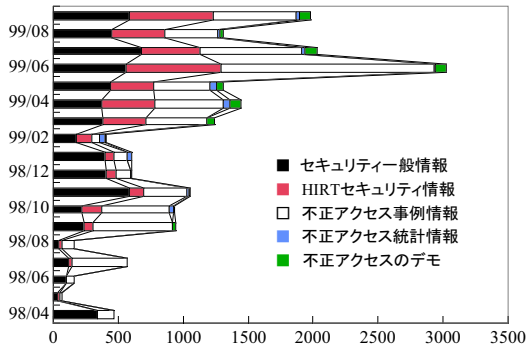

図 7 Web システムのアクセスの状況
Fig. 7 Access count of Web system.

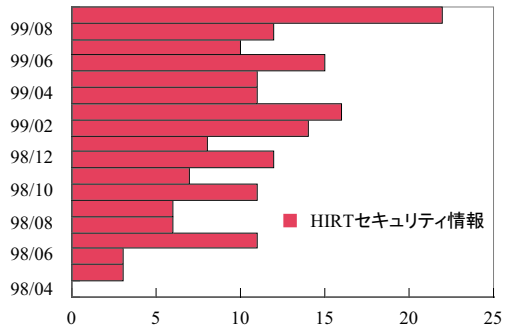

図 8 HIRT セキュリティ情報の発行状況
Fig. 8 Reported counts of HIRT security advisory.

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．

5. 不正アクセス対策情報サービスシステムの有効性

本章では，提供実績ならびに利用実績の見地から，システムの有効性を検証する．

5.1 サービス提供実績と利用実績

(1) 閲覧型サービス

セキュリティ一般情報は月平均 30 件，不正アクセスの事例は月平均 8 件，統計情報は年 4 回の割合で更新を行っている．閲覧型サービスの月別利用状況を**図 7** に示す．閲覧型サービスの利用はこの 1 年間で約 3 倍近く増加していることが分かる．

(2) 配信型サービス

配信型サービスの 1 次配信先は約 150 カ所であり，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 年は 9 月末までで 119 件（**図 8**），月平均 10 件の配信数となっている．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 9**）．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．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上げている（**図 10**）．

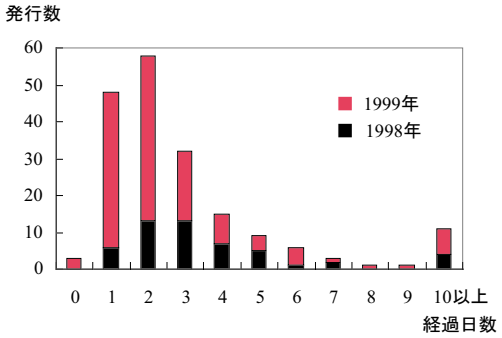

図 9 HIRT セキュリティ情報発行までの経過日数
Fig. 9 Required days of HIRT security advisory publication.

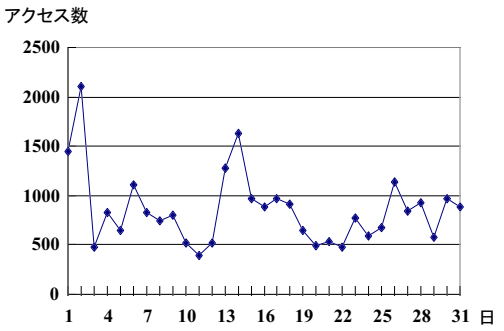

図 10 1 カ月あたりの累積アクセス数の変位
Fig. 10 Accumulated access count of Web per month.

5.2 サービスの有効性

課題に対するサービス提供実績と不正アクセス対策情報サービスを活用するユーザへのアンケート調査に

よりサービスの有効性を検証した．

［**サービス提供実績**］

- 「対策情報選別の迅速化」については，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 件に絞り込んでいる．
- 「対策情報理解の容易性確保」については，ネットワーク管理者向けに，CERT/CC，CIAC などのセキュリティ情報に日本語による対策解説を記載して 2 日以内に HIRT セキュリティ情報として配信を行っている．また，一般ユーザ向けに，不正アクセスの影響や危険性を理解してもらうための不正アクセスのデモを提供している．
- 「対策レベルの整合性確保」に対しては，危険度/対策緊急度を提示した HIRT セキュリティ情報の配信を行っている．

［**アンケート 調査方法**］

配信型サービス利用者に対して，記名式のアンケート調査により実施した．回答者は 16 名であり，その内訳は，一般ユーザ 8 名，ネットワーク管理者 7 名（うち，セキュリティ関連業務担当 4 名）であった．

［**アンケート 回答結果**］

Q1. 提供情報内容について
(1) 十分：11 件 (2) 普通：1 件 (3) 偏りあり：2 件
Q2. 提供情報量について
(1) 多い：3 件 (2) 普通：13 件 (3) 少ない：0 件
Q3. 情報提供のタイミングについて
(1) 早い：7 件 (2) 普通：6 件 (3) 遅い：0 件
Q4. 提供情報は，業務に役立ちましたか？
(1) はい：15 件 (2) いいえ：1 件
・デモはとても分かりやすくて有用
Q5. 今後も，情報提供は，
(1) あるべき：10 件 (2) あったほうが良い：5 件
(3) なくても良い：0 件

上記のサービス提供実績に対して良好なアンケート回答が得られており，構築したシステムが有用であることを確認した．

6. むすび

本論文では，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．

まず，企業内不正アクセス対応機関の役割を，部署間の協調を図り企業の不正アクセス対策活動を円滑に運営していくこととした．次にその活動内容を情報収集/情報分析/情報配布活動とし，その活動成果を不正アクセス対策情報サービスシステムとして提供した．「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．この結果，閲覧型サービスの利用はこの 1 年間で 3 倍近く増加し，またアンケート調査からいずれの課題に対しても良好な回答を得ることができた．これにより，構築したシステムが実用的であることと，各部署が推進する不正アクセス対策活動を支援できることを確認した．

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あげられる．

参考文献

1) Stepnenson, P.: Intrusion Management, *NetSec '98*, InfoSec Technologies.
2) Forum of Incident Response and Security Teams (FIRST): http://www.first.org/
3) IPA（情報処理振興事業協会）: http://www.ipa.go.jp/
4) JPCERT/CC（コンピュータ緊急対応センター）: http://www.jpcert.or.jp/
5) JPCERT/CC ニュースレター：http://www.jpcert.or.jp/nl/
6) 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，情報処理学会研究報告，99-CSEC-6, pp.25–30 (Jul. 1999).
7) 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).

(平成 11 年 12 月 3 日受付)
(平成 12 年 6 月 1 日採録)

寺田　真敏（正会員）

昭和 61 年千葉大学大学院工学研究科写真工学専攻修士課程修了．同年（株）日立製作所入社．平成 6 年 10 月より平成 9 年 11 月まで情報処理振興事業協会技術センター非常勤研究員．現在,（株）日立製作所システム開発研究所にてインターネット，ネットワークセキュリティの研究に従事．

萱島　　信（正会員）

昭和 62 年横浜国立大学工学部電気工学科卒業．平成元年同大学院修士課程修了．同年（株）日立製作所入社．以来システム開発研究所にて AI 技術，オブジェクト指向技術，ネットワーク技術，セキュリティ技術等の研究に従事．現在，同研究所研究員．

倉田　盛彦

昭和 56 年新潟大学大学院工学研究科修士課程修了．同年（株）日立製作所入社．以来電話交換機，時分割多重化伝送装置の開発に従事．平成 6 年より，インターネット接続・セキュリティ管理を中心とした企業内ネットワークの開発に従事．電子情報通信学会会員，IEEE 各会員．

佐々木良一（正会員）

昭和 46 年東京大学医学部保健学科卒業．同年（株）日立製作所入所．以来システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．現在，同研究所主管研究長兼セキュリティシステム研究センタ長．工学博士（東京大学）．昭和 58 年電気学会論文賞受賞．平成 10 年電気学会著作賞受賞．著書に「インターネットセキュリティ基礎と対策技術」（共著，オーム社，1996 年),「インターネットセキュリティ入門」（岩波新書，1999 年）等．IEEE，電子情報通信学会，電気学会等会員．