Webサービスを攻略するワーム流布対策方式の提案

寺田真敏[†1,†2] 礒川弘実[†1] 永井康彦[†1]
倉田盛彦[†3] 土居範久[†2,†4]

マルウェアの流布を含む不正アクセス活動が活発化しており，また，その被害も広範囲かつ多岐にわたるようになってきている．特に情報システムがWebサービス主体に構成されているイントラネットにおいては，Webサービスを攻略するワームの流布にともなう影響は甚大である．Webサービスを攻略するワーム流布時の課題としては,「ワームの流布抑止」と「サービス稼動の継続性確保」の二面性を兼ね備えた施策が必要とされている．そこで，本論文では，この課題を解決するために，Webサーバ上のポート切替コンポーネントがWebサービスのポート番号を代替ポート番号にシフトさせることでワームの流布を抑止し，プロキシサーバ上のポート/ホスト変換コンポーネントが代替ポート番号へのシフトにともなうURL変更を隠蔽することでWebサービスの稼動継続性も確保するイントラネット向けのWebサービスポー/ホストマッピング方式を提案する．さらに，提案方式に基づき実装したシステムの評価を通じて，本提案方式の有効性を示す．

Proposal of the Countermeasure for the Web Service Based Worm Propagation

Masato Terada,[†1,†2] Hiromi Isokawa,[†1] Yasuhiko Nagai,[†1]
Morihiko Kurata[†3] and Norihisa Doi[†2,†4]

Unauthorized access containing Malware propagation is activated and causes a lot of damage. Especially, in the intranet information system which consists of Web service based, the influence accompanied by the self-propagating worm of Web service based becomes very large. Under the worm propagation, administrator is in the difficult stage — stop the worm and provide the service. In this work, we have taken up this issue. We have examined — how one can provide a continuous service to users, while reducing the damage of the worm propagation. This paper described a proof-of-concept prototype "Web mapper: the Web service port/host mapping system" for the intranet Web service. The functions of Web mapper are the followings to suppress the Web service based worm propagation and support the stable Web service operation. The port change component on the Web server shifts Web service port number to an alternative port number for suppression Web service based worm propagation. The port/host conversion component on proxy server hides the URL change accompanied by a shift for an alternative port number. We implemented our system to show the validity of our approach.

1. はじめに

インターネットの常時接続の普及にともない，マルウェア（ウイルス，ワーム，トロイの木馬などの有害な機能を持ったプログラムの総称)[1)] の流布を含む不正アクセス活動は活発化している．特に，2001年7月中旬の「Code Red I/IIの流布[2)]」，そして2001年9月中旬の「Nimdaの流布[3)]」による被害は広範囲かつ多岐にわたった．

不正アクセス対策は，ユーザ環境にあわせ,「回避/防止」「保証」「検知」「回復/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おり[4)]，国内でも不正アクセス対策環境は徐々に整いつつある．現状，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し，セキュリティポリシ策定などの管理面も整備するとともに，

†1 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi Ltd.
†2 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University
†3 株式会社日立製作所情報システム事業部
Information Technology Division, Hitachi Ltd.
†4 中央大学大学院理工学研究科
Graduate School of Science and Engineering, Chuo University

「保証」として計算機資源の脆弱性検査や「検知」として侵入検知システムの導入を進めている．しかし，情報システムの稼動性を確保するためには，「回復/調査」に関する検討も重要であり，実際にマルウェアが流布した際の施策については検討の余地がある．たとえば，Web サービスを攻略するワーム流布時の施策として，『ワーム流布の抑止と既存サービスの提供維持を実現するための機構』などがあげられる．

本論文では，イントラネットでの Web サービスを攻略するワーム流布時の施策に対象を絞り，「ワームの流布を抑止する施策」と「サービスの稼動継続性を確保する施策」を合わせて提供することを目的とした回復機構を提案する．提案方式は，Web サーバ上のポート切替コンポーネントが Web サービスのポート番号を代替ポート番号にシフトさせることでワームの流布を抑止し，プロキシサーバ上のポート/ホスト変換コンポーネントが代替ポート番号へのシフトにともなう URL 変更を隠蔽することで Web サービスの稼動継続性を確保する Web サービスポート/ホストマッピング方式である．

本論文の構成について述べる．2 章で Web サービスを攻略するワーム流布時の課題と解決のアプローチを示す．3 章で Web サービスポート/ホストマッピングの実現方式を記述した後，4 章で実装したシステムの評価を示す．5 章は結論である．

2. Web サービスを攻略するワームと流布時の課題

本章では，提案方式が対象とするワームの感染動作を示した後，Web サービスを攻略するワーム流布時の課題と，課題解決のアプローチについて述べる．

2.1 Web サービスを攻略するワーム

マルウェアは 1998 年末頃から電子メールを介して流布するようになり，2001 年に入ってからは電子メールを介して自己拡散するワームに加え，サーバプログラムの脆弱性を直接攻撃するワーム（CodeRed，Nimda など），クライアントの脆弱性を悪用したダイレクトアクション型ワーム（Nimda，Aliz，Klez など）も現れ，人手の介入を必要としない自己拡散の方法が主流となりはじめている．

提案方式が対象とするワームは，ポート番号 80 に対して直接 TCP コネクションを確立した後，Web サーバの脆弱性を攻略するワームであり，代表例として CodeRed I/II，Nimda がある．CodeRed I/II は，ランダムに選んだ IP アドレスのポート番号 80/tcp に対して TCP コネクションを確立する．確立に成功した場合には，特別な HTTP GET 要求を送信して，Microsoft Internet Information Server（以下，IIS）☆ の idq.dll の脆弱性[7] を攻略し感染を試みる．感染後は，ワームの自己伝播型の特質により，ランダムに選んだ他の計算機に対して同様な感染活動を行う．Nimda は，電子メール，共用ファイル，Web サーバ経由など複数の感染手法を持つ．このうち，Web サーバ経由の場合には，ランダムに選んだ IP アドレスのポート番号 80/tcp に対して TCP コネクションを確立し，Microsoft IIS の脆弱性「Web サーバーフォルダへの侵入」[8] の攻略を試みる．

イントラネット Web サイトから回収したアクセスログに基づき，対象とするワームである CodeRed II と Nimda の流布状況を示す．**図 1** は 2001 年 8 月 6 日の CodeRed II 流布開始当初からの累積アクセス数と累積感染ホスト数である．5 カ所のイントラネット Web サイトに記録された CodeRed II の HTTP GET 要求のアクセス件数と発信元 IP アドレス件数の平均値から作図している．流布状況は，流布開始直後から 2 時間で累積アクセス数が約 100 件となっていることから，10 分あたりに換算すると約 8 件のアクセスが発生していたことになる．また，**図 2** は 2001 年 9 月 19 日の Nimda 流布開始当初からの累積アクセス数と累積感染ホスト数である．Nimda の場合には，夜間から流布活動の痕跡を記録していたアクセスログと早朝から流布活動の痕跡を記録しはじめたアクセスログがあり，痕跡形態が夜間型と早朝型の 2 つにはっきりと分かれている．このため，Nimda の累積アクセス数と累積感染ホスト数については，6 カ所のイントラネット Web サイトのアクセスログを痕跡の記録開始時刻を用いて分類した後，記録された Nimda の HTTP GET 要求のアクセス件数と発信元 IP アドレス件数の平均値を算出して作図している．夜間型の流布状況は，CodeRed II と同じく流布開始直後から 2 時間で累積アクセス数が約 100 件となっていることから，10 分あたりに換算すると約 8 件のアクセスが発生していたことになる．

2.2 Web サービスを攻略するワーム流布時の課題と解決策の提案

(1) 既存対策の課題

ワームが流布した際の基本的な対策手段は，ウイルス対策ベンダの提供するアンチウイルスソフトウェアのウイルス定義ファイルを更新するとともに，脆弱な

☆ Microsoft Internet Information Server（IIS）は，米国およびその他の国における米国 Microsoft Corp. の登録商標です．

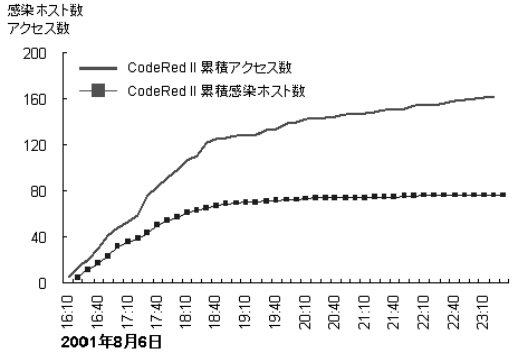

図 1 CodeRed II 累積アクセス数とホスト数
Fig. 1 Intranet Web servers compromised by CodeRed II.

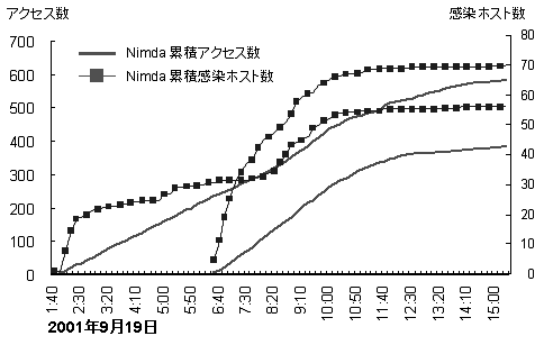

図 2 Nimda 累積アクセス数とホスト数
Fig. 2 Intranet Web servers compromised by Nimda.

サービスが稼動している場合には，セキュリティ修正プログラムによる脆弱性の除去を行うか，サービス自体を無効化することである．また，システムがこれらのワームに感染してしまった場合には除去ツールを適用するか，初期からシステムを再構築することになる．ところが，現状のイントラネットにおける情報システムの多くが Web サービス主体に構成されている．このため，Web サービスを攻撃対象とするワームが流布した場合，対策が完全に完了するまでの間，以下のような対策上の課題をともなってしまい，この影響は甚大となる．

- Web によるサービスを提供していること自体がワームの流布ならびに，流布にともなうトラフィック増加を助長してしまう．
- ワームが Web サービスを攻撃対象としているために，Web による対策情報の発信や，既存 Web サービスの稼動が阻害されてしまう．

(2) 課題解決のアプローチ

上記課題を解決するためには，ワームの流布を抑止することと，サービスの稼動継続性を確保することの二面性を兼ね備えた対策が必要となる．そこで，対象とするワームが，「ポート番号 80/tcp に対して直接 TCP コネクションを確立した後，Web サーバの脆弱性を攻略する」という特徴に着目し，以下のような方法で解決を図る．

- ワームの流布を抑止する．
  ワームが攻撃対象としている Web サービス（80/tcp）へのトラフィックをルータやファイアウォールで遮断するか，Web サービスを TCP ポート番号 80 以外の代替ポート番号（たとえば，9999/tcp）に移動する．この施策により，ワームは Web サービス（80/tcp）に対して TCP コネクションを確立することができず，結果として感染活動を阻止できることになる．
- Web サービスの稼動継続性を確保する．
  ワームが攻撃対象としている Web サービス（80/tcp）を代替ポート番号（9999/tcp）を用いて稼動させることで，ワームの攻撃を回避しながら Web サービスを継続して提供できることになる．さらに，Web サービスが代替ポート番号に切り替わったことにともなう影響を最小限にとどめるために，中継経路上にあるプロキシサーバにおいて，既存ポート番号（80/tcp）へのアクセスを代替ポート番号（9999/tcp）へのアクセスに振り替える URL マッピング操作を実施する．この URL マッピング操作は，Web サービスの稼動継続性を提供するうえで，ポート番号の変更をユーザに意識させないようにするための施策となる．

3. Web サービスポート/ホストマッピング

本章では，CodeRed，Nimda などの Web サービスを攻略するワーム流布時に，ワームによるトラフィック増加の抑止と Web サービスの継続性を確保するための Web サービスポート/ホストマッピングシステム（以下，Web マッパ）について述べる．

3.1 Web マッパ適用にあたっての前提条件

- Web マッパの適用にあたってはネットワーク構成変更をともなうため，イントラネットなどの組織内ネットワークを対象とする．
- Web サービスを攻略するワームは，Web サービスの標準ポート番号 80/tcp に直接 TCP コネクションを確立して攻撃を仕掛ける CodeRed，Nimda タイプのワームを想定する．
- Web ブラウザからの Web アクセスは，すべてプロキシサーバ経由とする．なお，プロキシサーバを攻略するワームについては，本提案方式の適用対象外とする．

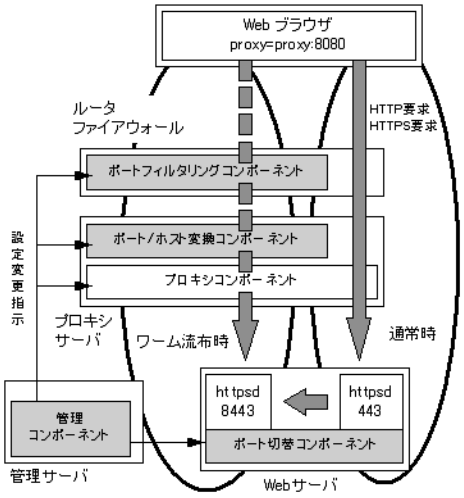

図 3 Web サービスポート/ホストマッピングシステム
Fig. 3 Web mapper: the Web service port/host mapping system.

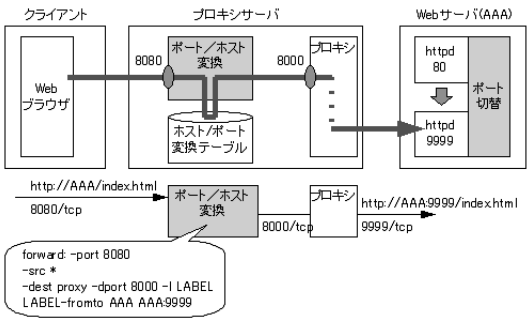

図 4 Web マッパ適用時の Web ブラウザから Web サーバまでのアクセス経路
Fig. 4 The operation outline of Web mapper.

3.2 Web マッパのコンポーネント

Web マッパは，課題解決のアプローチで示した方法を組み合わせることにより，Web サービスを攻略するワーム流布を回避するためのシステムであり，以下の 4 つのコンポーネントから構成する（**図 3**）．

(1) ポートフィルタリングコンポーネント

Web サービスを攻略するワームが流布した際に，Web サービスを提供しているポート番号（80/tcp）へのトラフィックをフィルタリングする．フィルタリングにあたっては，既存ネットワーク機器であるルータ，ファイアウォールを用いることを想定している．

(2) ポート切替コンポーネント

ワームが攻撃対象としている Web サービスを代替ポート番号（たとえば，9999/tcp）を用いて提供するためのポート番号切替えを行う．「Web サービスを代替ポート番号を用いて提供する」方法は，ワームが攻略しようとしているポート番号（80/tcp）での Web サービスを停止し，さらに代替ポート番号（9999/tcp）で Web サービスを提供することになるため，ワームの流布の抑止と Web サービスの稼動継続性の確保の双方に有効である．

(3) ポート/ホスト変換コンポーネント

Web サービスが代替ポート番号に切り替わったことをユーザに意識させないようにするために，既存ポート番号（80/tcp）へのアクセスを代替ポート番号（9999/tcp）へのアクセスに振り替える URL マッピング操作を行う．

(4) 管理コンポーネント

上記 3 コンポーネントに対して，フィルタリング，ポート切替え，ポートマッピングの変更指示を出す．管理者によるマニュアル操作や IDS（Intrusion Detection System）との連動を想定している．

次に，Web マッパを介した場合の Web ブラウザから Web サーバまでのアクセス経路概要を**図 4** に示す．

(a) Web ブラウザ－＞プロキシサーバ

Web ブラウザからのアクセスは，すべてプロキシサーバ経由であり，プロキシサーバのポート番号 8080/tcp に対して，HTTP 要求（例：GET http://AAA/index.html）を送信する．

(b) プロキシサーバ

プロキシサーバ上の「ポート/ホスト変換コンポーネント」では，HTTP 要求を定義ファイル（ポート/ホスト変換テーブル）に従い書き換え操作（URL マッピング操作）を行った後，プロキシコンポーネントに HTTP 要求（GET http://AAA:9999/index.html）を転送する．

(c) プロキシサーバ－＞ Web サーバ

プロキシコンポーネントでは，書き換え後の HTTP 要求（GET http://AAA:9999/index.html）に従い，Web サーバのポート番号 9999/tcp に対して HTTP 要求を送信する．

このように，Web マッパの基本的な仕組みは，プロキシサーバ上の「ポート/ホスト変換コンポーネント」と Web サーバ上の「ポート切替コンポーネント」が連動して Web サービスのポート番号（80/tcp）を代替ポート番号（9999/tcp）にシフトすることにより，ワームの流布を抑止し，Web サービスの稼動継続性を確保する．さらに，プロキシサーバ上の「ポート/ホスト変換コンポーネント」を利用して，代替ポート番号（9999/tcp）にシフトした URL 変更の隠蔽を行い，ユーザに対して既存 Web サービスの稼動環境の

```
' Move IIS Server PORT from 80 to 9999
Dim IisServerNum
Dim IisObjectPath
Dim IisObject
Dim IisSchemaObject
Dim IisPort
IisServerNum = 2
IisPort                    = ":9999:"
IisObjectPath = "IIS://LocalHost/W3SVC/" & IisServerNum
Set IisObject = GetObject(IisObjectPath)
Set IisSchemaObject ¥
                = GetObject("IIS://LocalHost/Schema/ServerBindings")
IisObject.Put "ServerBindings", IisPort
IisObject.SetInfo
```

図 5 IIS Web サーバ用のポート切替指示スクリプト
Fig. 5 Script for IIS re-configuration.

提供を維持する．

4. Web マッパの実装

本章では，提案した Web マッパを評価するために実装したシステムについて述べる．

4.1 実 現 方 式

Web マッパの 4 つのコンポーネントのうち，「ポート切替コンポーネント」「ポート/ホスト変換コンポーネント」「管理コンポーネント」について，実現方式の検討ならびに実装を行った．

(1) ポート切替コンポーネント

ポート切替コンポーネントについては，IIS[6] Web サーバ用としてポート番号を設定する VB スクリプト（**図 5**）を作成し，Apache[5]☆Web サーバ用として 2 種類のポート定義ファイルと切替え用スクリプトを準備した．

(2) ポート/ホスト変換コンポーネント

ポート/ホスト変換コンポーネントは URL の rewriting 機能であり，以下に示す機能を持つネットワークデーモン hwmapd として開発を行った．

- ポート/ホストマッピング機能

Web ブラウザから受信した HTTP/HTTPS 要求については，**表 1** に示す定義ファイルに従いポート番号ならびに，ホスト名の書き換えを行う．具体的には，HTTP 要求ヘッダのメソッド行と Host 行が，定義ファイルに指定された「変換前ホスト名：変換前ポート番号」に合致する場合，「変換後ホスト名：変換後ポート番号」に変換した後，転送を行う（**図 6** 上段）．また，HTTPS（CONNECT）要求については，HTTPS（CONNECT）要求ヘッダのメソッド行が定義ファイルに指定された「変換前ホスト名：変換前ポート番号」に合致する場合，「変換後ホスト名：変換後ポート番号」に変換した後，転送を行う（図 6 下段）．

☆ Apache は Apache Group の登録商標です．また，記載されている会社名，製品名は，それぞれの会社の商標もしくは登録商標です．

表 1 ポート/ホスト変換コンポーネント hwmapd の定義ファイル
Table 1 The configuration file of hwmapd.

# 書き換えを行うホスト名とポート番号を指定	
forward:	
-port	待ちポート番号
	HTTP 用の定義
-src	送信元 IP アドレス（アクセス制御用）
-dest	転送先サーバ IP アドレス
-dport	転送先サーバのポート番号
	HTTPS 用の定義
-ssrc	送信元 IP アドレス（アクセス制御用）
-sdest	転送先サーバ IP アドレス
-sdport	転送先サーバのポート番号
-l	マッピングルールラベル
#マッピングルールラベル	
-fromto	変換前 IP アドレス/ホスト名：ポート番号
/-sfromto	変換後 IP アドレス/ホスト名：ポート番号
# 定義ファイル例	
forward: -port 8080 -src * -dest proxy -dport 8080	
-ssrc * -sdest proxy -sdport 8080 -l LBL	
LBL-fromto tomato.hitachi.jp kiwi.hitachi.jp:9999	
LBL-sfromto tomato.hitachi.jp kiwi.hitachi.jp:8443	

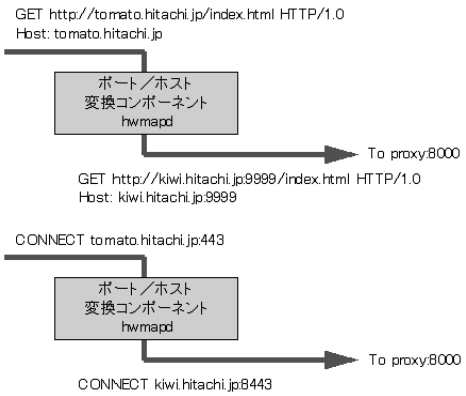

図 6 ポート/ホスト名変換処理
Fig. 6 Overview of hwmapd rewriting engine.

- 送信元に対するアクセス制御機能

許可されたクライアントからの HTTP/HTTPS 要求に対してのみ，ポート/ホストマッピングならびに，HTTP/HTTPS 要求の転送を行う．

- アクセスログ機能

ポート/ホストマッピング処理のログとして，送信元 IP アドレス/ホスト名，転送先 IP アドレス/ホスト名，時刻，HTTP/HTTPS 要求ヘッダのメソッド行を取得する．

(3) 管理コンポーネント

- マネジャ/エージェント機能

マネジャ/エージェント機能は，**図 7** に示す Web ベースの管理インタフェース，あるいは，IDS 連携機能の検知状態をトリガとして，「ポート切替え」「ポート/ホスト変換」コンポーネントに対して設定変更の指示を出す．マネジャ/エージェント間の通信ならびにコ

図 7 Web ベースの管理インタフェース
Fig. 7 Administrative Web interface.

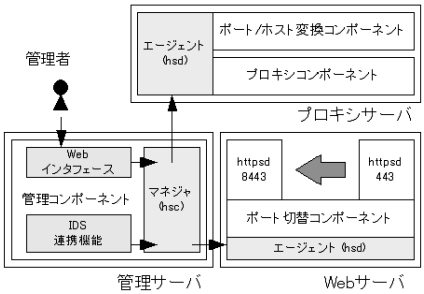

図 8 hsc/hsd を用いたコンポーネント間連携
Fig. 8 Manager/agent based administrative component.

ンポーネント間連携については，分散ネットワークサービス管理のためのセキュア通信基盤として開発してきた hsc/hsd（Hitachi Secure Socket Client/Daemon）を使用している（**図 8**）[9]．hsc/hsd は HTTP プロトコルを使用した軽量通信モジュールであり，hsc から hsd に対して CGI スクリプト指定形式でプログラム起動を行うことができ，通信内容も独自モジュールにより認証/暗号化している．

- IDS 連携機能

IDS と連携して Web サービスを攻略するワーム流布時に Web マッパの変更を行う．本システムでは，管理サーバ上のポート番号 80/tcp に立ち上げた HTTP サーバを簡易的なホスト IDS とした．イントラネットにおいては，明示的に Web サーバの公開を宣言していない限り，その Web サーバにアクセスが発生することはない．いい換えれば，管理サーバ上のポート番号 80/tcp にアクセスが発生すること自体が異常であると判断できる．本 HTTP サーバへの単位時間内のアクセスがしきい値を超過した場合，上記のマネジャ/エージェント機能経由で，コンポーネントに対して設定変更の指示を出す．

4.2 評価と考察

評価にあたっては，Web サービスが代替ポート番号にシフトしたことによるトラフィックの抑止効果，URL 変更の隠蔽，管理コンポーネントとの連動に加え，実イントラネット環境での実験的な利用により行った．

(1) トラフィックの抑止効果について

CodeRed I/II，Nimda の送出する TCP パケット数は，ポート切替えの前後で**表 2** のとおりとなり，ワームの流布にともなうトラフィック抑止においても効果がある．

(2) HTTP における URL 変更の隠蔽について

代替ポート番号（9999/tcp）でサービスを提供している Web サーバに対して，ポート/ホスト変換コンポーネント hwmapd を介して，下記の 5 つの形態でのアクセスを行った結果，**図 9** に示すとおり，標準ポート番号 80/tcp）の URL 指定で代替ポート番号（9999/tcp）にアクセスしていることと，代替ポート番号へのシフトによる URL 変更を，ポート/ホスト変換コンポーネント hwmapd が隠蔽していることを確認した．

- 環境変数表示用 CGI プログラムへのアクセス
- 相対パス記述の URL へのアクセス
- 絶対パス記述の URL へのアクセス
- ホスト名+ポート番号記述の URL へのアクセス
- JavaScript によるホスト名記述の URL へのアクセス

また，今回，今後の機能拡張を考慮し「ポート/ホスト変換コンポーネント」として hwmapd の開発を行ったが，同等の機能は Apache の既存機能（rewrite, proxy 機能）により実現できることも確認した．

(3) HTTPS における URL 変更の隠蔽について

HTTP アクセスと同様に 5 つの形態でのアクセスを行った結果，標準ポート番号（443/tcp）の URL 指定

表 2 ワームが送出する TCP パケット数の比較
Table 2 Comparison of TCP packet counts.

	ポート切替前	ポート切替後
CodeRed I	13 パケット SYN, SYN+ACK, ACK, HTTP 要求（1/3, ACK, HTTP 要求（2/3), ACK, HTTP 要求（3/3), ACK, HTTP 応答, FIN+ACK, RST, RST	6 パケット SYN, RST（3 回再送されるため, 2×3 パケットとなる）
CodeRed II	13 パケット 同上	6 パケット 同上
Nimda	128 パケット SYN, SYN+ACK, RST, ACK, HTTP 要求, HTTP 応答, FIN+ACK, RST（16 個の HTTP 要求が送信されるため 8×16 パケットとなる）	96 パケット SYN, RST（16 個の HTTP 要求の送信が 3 回再送されるため 2×16×3 パケットとなる）

（注）実測条件：TCP セグメントの最大サイズ=1460 バイト.

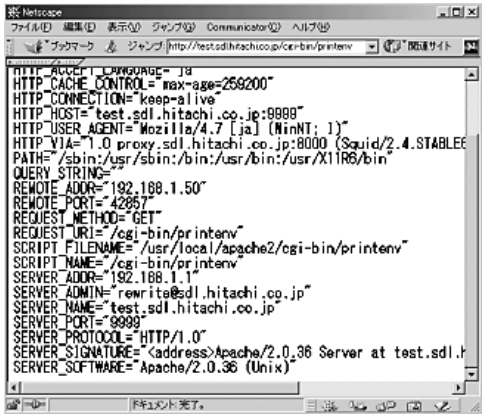

図 9 hwmapd を介した環境変数表示用 CGI プログラムへのアクセス結果
Fig. 9 Access to CGI printenv program via hwmapd.

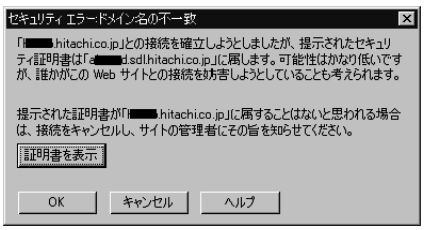

図 10 異なるホスト名に書き換えた場合の警告ダイアログ
Fig. 10 Dialog of security error: Un-match domain name.

で代替ポート番号（8443/tcp）にアクセスしていることと，代替ポート番号にシフトしたことによる URL 変更を隠蔽していることを確認した．さらに，ポート/ホスト名変換の対象範囲をドメイン名部分にまで適用した場合には，**図 10** に示す警告ダイアログ「セキュリティエラー：ドメイン名の不一致」を表示するが，ディレクトリパスはサーバに格納されているディレクトリパスに従いアクセスできることを確認した．

(4) 管理コンポーネントとの連動について

(a) 手動による設定変更

Web ベースの管理インタフェースから hsc/hsd 経由でポート切替スクリプトを起動することにより，対象となるすべてのコンポーネントの通常時ポート/緊急時ポートの相互切替えを確認した．

(b) IDS 連携機能からの設定変更

マネジャ機能は，定期的に簡易的なホスト IDS へのアクセス数をカウントし，単位時間内のアクセスがしきい値を超過した場合，エージェント経由で「ポート切替え」「ポート/ホスト変換」コンポーネントの設定変更を指示する．IDS 連携機能からの設定変更についても，すべての設定変更が終了した時点で Web ベースの管理インタフェースに完了報告を上げることを確認した（**図 11**）．なお，単位時間内のしきい値は，調査事例を参考に 10 分間あたり 8 アクセスとしたが，流布の規模をふまえたしきい値の設定については，今後の課題である．

図 11 IDS 連携機能指示による切替の完了報告
Fig. 11 The message of automatic operation with the portable IDS.

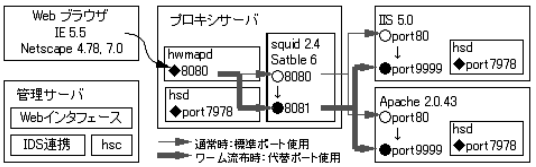

図 12 適用評価の構成概要
Fig. 12 A part of system configuration in Intranet environment.

表 3 適用評価の環境
Table 3 Overview of Intranet environment.

項目	内容
ユーザ利用テストで確認した Web サーバ台数	イントラネットに接続する 10 サイト（注）
セッション制御動作テストで確認した Web サーバ台数	同上
切替テストで確認した Web サーバ台数	イントラネットに接続する 3 サイト

（注）10 サイトのうち，代替ポート番号を準備して確認を行ったサイトは 3 サイトであり，残りの 7 サイトについては Web ブラウザの URL で代替ポート番号（http://host:9999）を指定する形態で確認を行った．

(5) 実イントラネット環境での実験的な利用

図 12，**表 3** に示す実イントラネット環境下において，実装システムの適用可能性を検討した．適用評価のシステム構成では，管理コンポーネント用としてポート番号 7978/tcp，プロキシサーバ用としてポート番号 8080/tcp を固定的に割り当てている．また，プロキシサーバ内部では，通常時にはプロキシコンポーネントとして使用した Squid のポート番号 8080 経由で，緊急時には Squid のポート番号 8081 経由で代替ポート番号（9999/tcp）にアクセスする形態を用いて，下記に示す項目についての確認を行った．

- ポート切替えによる Web サービスの提供
  実環境下において，ポート切替えにともなう Web

表 4 確認項目
Table 4 Functional evaluation lists.

分類	確認内容
(a) ユーザ利用テスト	ポート/ホスト変換コンポーネントを有効としたプロキシサーバを介して Web サーバにアクセスした場合に，ページが表示されないなどの問題がない．
	ポート/ホスト変換コンポーネントの定義対象外となる Web サーバ，たとえば，インターネットならびに，他サイトのページについては，これまでどおりアクセスすることができ，ページが表示されないなどの問題がない．
(b) セッション制御動作テスト	Web サーバのポート切替後（80 → 9999）も，ユーザの追加操作なく，Web サーバ（Apache，IIS）を継続して利用可能である．
	Web サーバのポート切替後（80 → 9999）も，ユーザの追加操作なく，Cookie を用いてセッション制御を行っているアプリケーション，URL を用いてセッション制御を行っているアプリケーションを継続して利用可能である．
(c) 切替テスト	Web ベースの管理インタフェースからの指示に従い，Web サーバのポート番号の切替え，ポート/ホスト変換コンポーネントの有効化が可能である．
	IDS 連携機能からの指示に従い，Web サーバのポート番号の切替え，ポート/ホスト変換コンポーネントの有効化が可能である．

サービスへの影響有無を確認する（**表 4**：(a) ユーザ利用テスト，(b) セッション制御動作テスト）．

- IDS 検知機能と連動したポートの自動切替え
  深夜の運用支援を想定し，IDS などの検知機構と連動したポート切替えを対象に動作確認を行う（表 4：(c) 切替えテスト）．

結果として，ユーザ利用，セッション制御動作のいずれのテストにおいてもページが表示されないなど，Web サービスの継続利用を妨げる問題はなかった．また，HTTP において「ポート/ホスト変換コンポーネント」として同等の機能を持つ Apache の既存機能（rewrite，proxy 機能）についても同様の結果が得られた．HTTP 要求/応答の 1 トランザクションごとに測定を行った場合，ポート/ホスト変換コンポーネント hwmapd 経由の性能は**表 5** のとおりである．ただし，Web ブラウザにおいて画像が多数リンクされた Web ページを表示する際に 1 分近く要する場合もあり，hwmapd への同時アクセスにともなう性能改善を検討していく必要がある．

また，切替テストについても動作自身にトラブルはなく，管理コンポーネントによる設定変更指示から完了報告までの時間にばらつきはあるが，1 サイトあたり約 15 秒前後での切替えができている（**表 6**）．ただし，約 1 分/サイトを要する場合もあり，イントラネット全体への適用を想定した場合には，設定変更指示方法の改良，並行処理ならびにサイト単位での分散処理を検討していく必要のあることが分かった．

表 5 HTTP 要求/応答の 1 トランザクションごとの応答性能
Table 5 Evaluation of HTTP response time.

実測環境	hwmapd 経由	hwmapd 経由なし
応答値が最小の Web サイト	36 ミリ秒	33 ミリ秒
応答値が最大の Web サイト	3.2 秒	2.2 秒

ユーザ利用テストで使用した Web サイトにアクセスし，その応答時間を測定した．測定値は 20 回行って平均をとった．

表 6 コンポーネント切替の所要時間
Table 6 Evaluation of Web mapper component shift.

実測環境	Web ベースの管理インタフェース経由
切替時間	15.7 秒

Web ベースの管理インタフェースを用いて対象とする 3 サイトの切替えが完了するまでの総時間を測定した．測定値は 20 回行って平均をとった．

5. おわりに

本論文では，イントラネットにおいて Web サービスを攻略するワーム流布時の施策として，Web サービスポート/ホストマッピング方式を提案した．まず，ワームの流布を抑止することと，サービスの稼動継続性を確保することの二面性を兼ね備えた対策として，Web サービスの標準ポート番号を代替ポート番号にシフトし，その変更をプロキシサーバで隠蔽する方式を提示した．さらに，提案方式に基づき実装したシステムの評価を通じて，ワーム流布の抑止と既存サービスの提供維持を実現できることを示した．このような対策方法を開示することで，その対策方法を回避するワームの出現は予想しうることではあるが，さまざまな対策方法を用意し，それらの対策を組み合わせていくことのできる環境作りが重要であると考えている．今後は，適用評価で得られた知見をもとに機能ならびに性能改善を図るとともに，本提案方式だけでは回避することのできない Web サービスを攻略するワーム，たとえば，プロキシサーバ自身を攻撃対象としたワームやプロキシサーバを乗り越えて Web サービスを攻略するワームへの対処方法を検討していく．

参考文献

1) EICAR99 (European Institute for Computer Anti-Virus Research). http://www.ipa.go.jp/security/fy10/contents/virus/3_1_3.html
2) CERT Advisory CA-2001-19: “Code Red” Worm Exploiting Buffer Overflow In IIS Indexing Service DLL. http://www.cert.org/advisories/CA-2001-19.html

3) CERT Advisory CA-2001-26: Nimda Worm. http://www.cert.org/advisories/CA-2001-26.html
4) 不正侵入はこう防げ，日経コンピュータ，No.448, pp.185–195 (July 1998).
5) The Apache Software Foundation. http://www.apache.org/
6) Microsoft Internet Information Server. http://www.microsoft.com/japan/products/iis/
7) Index Server ISAPI エクステンションの未チェックのバッファにより Web サーバーが攻撃される（MS01-033），http://www.microsoft.com/japan/technet/security/bulletin/ms01-033.asp
8) 「Web サーバーフォルダへの侵入」の脆弱性に対する対策（MS00-078）．http://www.microsoft.com/japan/technet/security/bulletin/ms00-078.asp
9) 中野喜之，礒川弘実，萱島　信，寺田真敏，山崎隆行：「分散ネットワークサービス管理のためのセキュア通信基盤の開発」研究報告，コンピュータセキュリティ，No.007-003 (1999.01).

(平成 15 年 9 月 9 日受付)
(平成 16 年 10 月 4 日採録)

寺田　真敏（正会員）

1986 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．システム開発研究所にてネットワークセキュリティの研究に従事．2004 年 4 月から中央大学研究開発機構客員研究員を兼務．

礒川　弘実（正会員）

1996 年九州大学大学院工学研究科修士課程修了．同年（株）日立製作所に入社，システム開発研究所に配属．以来，ネットワーク管理システム，セキュリティ管理システムの研究開発に従事．

永井　康彦（正会員）

1983 年日本大学理工学部航空宇宙工学科卒業．1985 年同大学大学院理工学研究科修士課程修了．同年（株）日立製作所入社．システム開発研究所勤務．情報セキュリテイ，ネットワーク管理システム，グループウエア等の研究開発に従事．現在同研究所セキュリティシステム研究部主任研究員．電子情報通信学会，電気学会各会員．

倉田　盛彦

1981 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．1994 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・運用に従事．電子情報通信学会，IEEE 各会員．

土居　範久（正会員）

1969 年慶應義塾大学大学院博士課程単位取得退学．慶應義塾大学理工学部教授を経て，2003 年より中央大学理工学部教授，慶應義塾大学名誉教授．工学博士．現在，文部科学省科学技術・学術審議会委員，総務省情報通信審議会委員，世界科学会議〔International Council for Science（ICSU）〕Priority Area Assessment Panel of Scientific Data and Information メンバー，科学技術振興機構（JST）社会技術システムミッションプログラム「情報セキュリティ」研究統括，特定非営利活動法人日本セキュリティ監査協会会長，国際計算機学会（ACM）日本支部長，等．専門はソフトウェアを中心とした計算機科学．