2003－CSEC－21 (7)
2003／5／15

Web マッパ(Web サービスポート／ホストマッピングシステム)の機能拡張と適用評価

寺田 真敏 † 磯川 弘実 † 永井 康彦 † 中原 亮 ‡
terada@sdl.hitachi.co.jp isokawa@sdl.hitachi.co.jp y-nagai@sdl.hitachi.co.jp mnakaha@itg.hitachi.co.jp

† (株)日立製作所 システム開発研究所
〒212-8567 神奈川県川崎市幸区鹿島田 890
‡ (株)日立製作所 情報・通信グループ
〒140-8570 東京都品川区南大井六丁目 23 番 15 号

あらまし：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、Web サービスを攻略するワーム流布時の課題のひとつに、「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の提供がある。この課題を解決するために、システムが相対している脅威レベルに応じて提供するサービスクラスを変更する Alternative Service Plane というフレームワークを導入すると共に、Web サービスを対象とした実現方式として、Web マッパ(Web サービスポート／ホストマッピングシステム)を位置付けている。本稿では、この Web マッパの拡張機能として HTTPS 対応、Web マッパの設定変更のための管理コンポーネント連携機能を試作し、イントラネットでの適用実験を行なったので、その概要について報告する。
キーワード：不正アクセス　ネットワークセキュリティ　ワーム　Web サービス

The Extensions and Evaluation of Web service port/host conversion system

Masato Terada † Hiromi Isokawa † Yasuhiko Nagai † Makoto Nakahara ‡
terada@sdl.hitachi.co.jp isokawa@sdl.hitachi.co.jp y-nagai@sdl.hitachi.co.jp mnakaha@itg.hitachi.co.jp

† Systems Development Laboratory, Hitachi Ltd.
890 Kashimada, Saiwai-ku, Kawasaki, 212-8567 Japan
‡ Information & Telecommunication Systems, Hitachi Ltd.
6-23-15 Minamioi, Shinagawa-ku, Tokyo, 140-8570 Japan

Abstract: We challenge the issue to tackle a problem about self-propagating worm of Web service based; how one can suppress Web service based worm propagation and support the stable Web service operation. We propose a "Alternative Service Plane" to provide multiple application service stage which responded with the threat type or level. Alternative Service Plane provides the framework for changing from one service stage to other service stage to reduce the threats. This paper described the extension of a proof-of-concept prototype "Web mapper (Web service port / host mapping system)" and the process for functional evaluation in our intranet environment.
key words: Unauthorized Access, Network Security, Worm, Web Service

1. はじめに

「回避/防止」「保証」「検知」「回復/調査」の 4 つのフェーズ(図 1.1)[1]からなる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ー策定などの管理面も整備すると共に、「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まだまだ検討の余地がある。

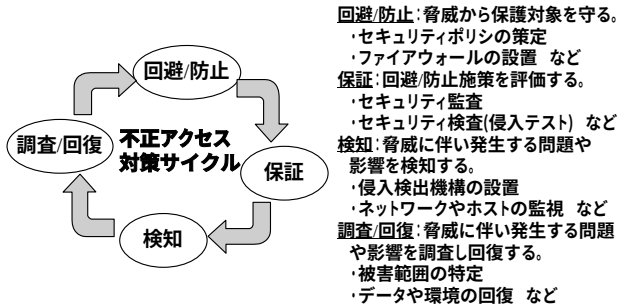


図 1.1 不正アクセス対策サイクル

本研究では、不正アクセス対策の「回復/調査」フェーズに対象を絞り、Web サービスを攻略するワーム流布時の施策について検討を進めている。報告者らが Web サービスを攻略するワーム流布時の施策で解決したい課題のひとつに、『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』の提供が挙げられる。この課題を解決するために、「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仕掛けとして、Web マッパ(Web サービスポート／ホストマッピングシステム)を提案している[2]。

本稿では、この Web マッパ(Web サービスポート／ホストマッピングシステム)の拡張機能として、HTTPS 対応、Web マッパの設定変更のための管理コンポーネント連携機能を試作すると共に、イントラネットでの適用実験を行なったので、その概要について報告する。

2. Alternative Service Plane

本章では、CodeRed, Nimda などのワーム流布時に、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 マッパの上位概念となる、Alternative Service Plane と呼ぶフレームワークについて述べる。

2.1 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共に、脆弱な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なうか、サービス自身を無効とすることである。

ところが、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伴ってしまう。

- 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、流布に伴うトラフィック増加を助長してしまう可能性がある。
- 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、システムが相対している脅威レベルに応じて提供するサービスクラスを変更する Alternative Service Plane というフレームワークを導入する。

Alternative Service Plane とは、各ネットワークサービスごとに、脅威レベルごとに、事前に提供するサービスの条件を設定したクラスである。脅威レベルが上がるほど、提供するサービスに利用制約条件を付加することでサービスの稼動継続性を確保するという考え方に立っている。

例えば、電子メールサービスの場合には、定常状態はメール送信に際して特に制約事項を設けないが、ワームなどの流布によりメールサービスに対する脅威レベルが上がるに従い、「メール送信時にユーザ認証を行なう」「メールの件名に特定のキーワードが記載された場合のみ転送する」「インフラを運用

するシステム管理者向けのメールサービスのみを有効とし、一般ユーザのサービスを停止する」など段階的な制約の付いたサービスクラスを事前に準備しておく。

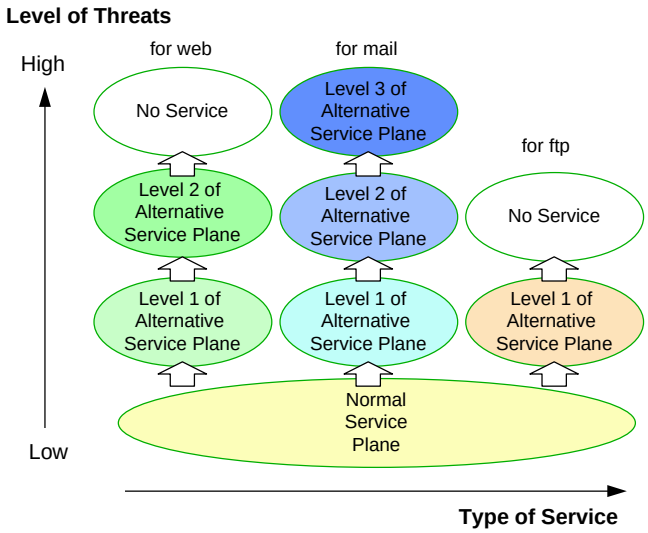


図 2.1　Alternative Service Plane の概要

また、Web サービスを攻略するワーム流布の場合には、以下のように事前定義したサービスクラスに移行することになる。

- 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 サービスへのトラフィックを遮断する。

- 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 サービスを代替ポートを用いて提供する。さらに、Web サービスが代替ポートに切り替わったことに伴う影響を最小限に留めるために、プロキシサーバにおいて、既存ポート番号と代替ポート番号とのマッピングを行なうなどの施策を適用する。

2.2　Web マッパ

Web マッパは、Web サービス向けの Alternative Service Plane を実現する方式のひとつであり、「ポートフィルタリングコンポーネント」「ポート切り替えコンポーネント」「ポート/ホスト変換コンポーネント」「管理コンポーネント」の 4 つのコンポーネントを用いて、以下の前提条件のもとでサービスを提供する。

- 同一の管理ドメインを適用対象とする。
- Web ブラウザからの Web アクセスは、全てプロキシサーバ経由とする。

2.3　Web マッパプロトタイプの機能拡張

本節では、Web マッパの 4 つのコンポーネントのうち、機能拡張を行なった「ポート／ホスト変換」「管理」コンポーネントについて述べる。

(1) 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(hwmapd)が持つ URL の rewriting 機能を拡張し HTTPS 対応とした。

- ポート／ホストマッピング機能

Web ブラウザから受信した HTTPS(CONNECT)要求に対して、定義ファイルに指定している変換定義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、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、転送を行なう (図 2.3)。

- 送信元に対するアクセス制御機能

定義ファイルにて許可されたクライアントからの HTTPS(CONNECT)要求に対してのみ、ポート／ホストマッピングならびに、HTTPS 要求の転送を行なう。

- アクセスログ機能

ポート／ホストマッピング機能で処理した HTTPS 要求のログを取得する。

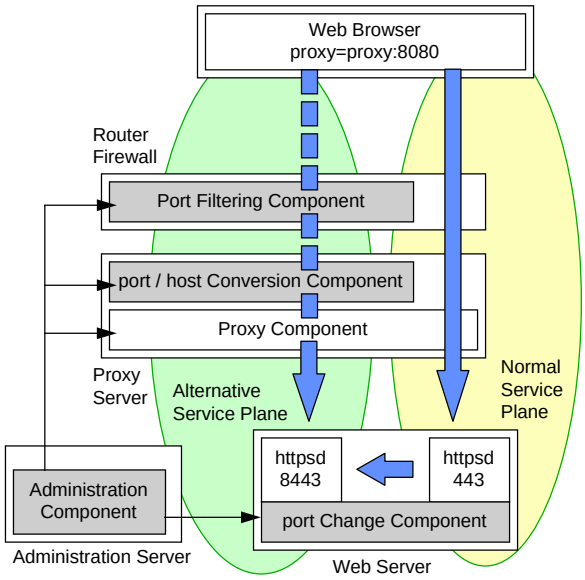


図 2.2　Web サービスポート/ホストマッピングシステムの概要

```
# 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
   -src  送信元IPアドレス                    ┐
   -dest  転送先サーバIPアドレス             │HTTP用
   -dport  転送先サーバのポート番号          ┘
   -ssrc  送信元IPアドレス                   ┐
   -sdest  転送先サーバIPアドレス            │HTTPS用
   -sdport  転送先サーバのポート番号         ┘
   -l  ルールラベル
ルールラベル
   -fromto/-sfromto  変換前IPアドレス/ホスト名：ポート番号
                     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.sdl.hitachi.co.jp    kiwi.sdl.hitachi.co.jp:9999
LBL-sfromto tomato.sdl.hitachi.co.jp    kiwi.sdl.hitachi.co.jp:8443
```

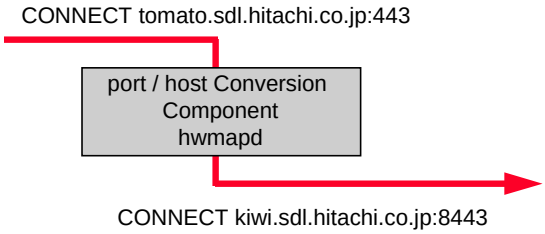


図 2.3　ポート/ホスト変換コンポーネント(hwmapd)の定義ファイルと書き換え処理

(2) 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 2.4に示すWebベースの管理インタフェースを介して、「ポート切り替え」「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 2.5)[3]。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なうことができ、通信内容も日立独自モジュールにより認証/暗号化できる。

● 簡易 IDS 機能

管理サーバ上に、ポート番号 80/TCP で稼働するダミーの HTTP サーバを立ち上げる形態とし、単位時間内のアクセスが規定値を超過した場合、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仕様としている。

図 2.4　Web ベースの管理インタフェース

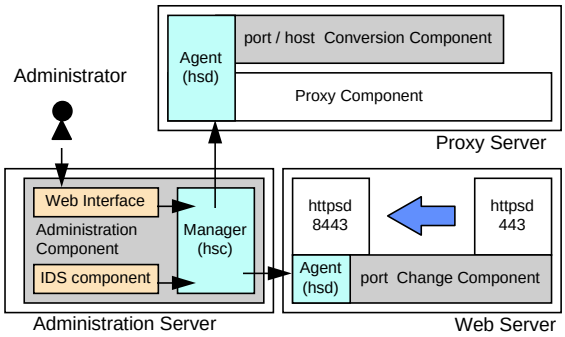


図 2.5　hsc/hsd を用いたコンポーネント間連携

2.4　プロトタイプの機能確認

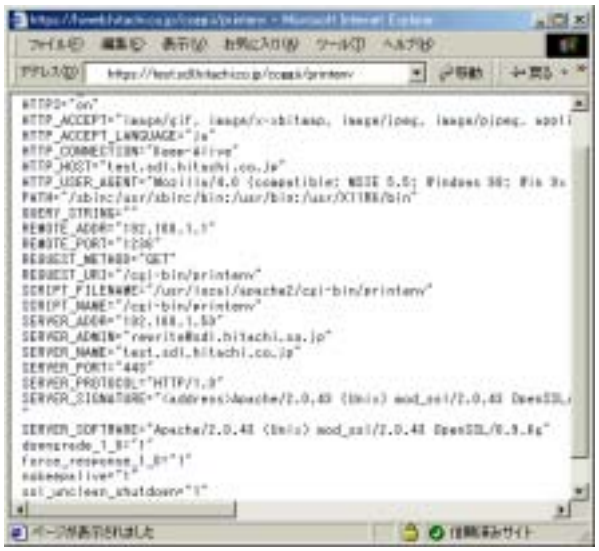
(1) HTTPS における URL 変更の隠蔽について

代替ポート番号(8443/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なった結果、図 2.6に示す通り、標準ポート番号(443/tcp)へのアクセスで代替ポート番号にアクセスし、いずれの場合も代替ポート番号にシフトしたことによる URL 変更を、ポート/ホスト変換コンポーネント hwmapd により隠蔽できていることを確認した。

- CGI(GET/POST)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、URL 変更をドメイン名部分にまで適用した場合には、図 2.7に示す警告ダイアログを表示するが、

ディレクトリパスはURL変更後の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。



Webサーバの稼働ポートは8443であるが、環境変数表示用CGIプログラムprintenvにアクセスした場合SERVER_PORTは443として表示される。

図 2.6　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

図 2.7　異なるホスト名に書き換えた場合の警告ダイアログ

(2) 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

ポート切り替えコンポーネントとして、図 2.8に示すようなポート切り替えスクリプトを用意し、Webベースの管理インタフェースからhsc/hsd経由で起動することにより、通常時のポート／緊急時のポートの相互に切り替えを確認した。

(b) 簡易IDSからの設定変更

マネジャ機能は、定期的に簡易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規定値を超過した場合、エージェント経由で「ポート切り替え」「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。簡易IDS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 2.9)。

```
' 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.Setinfol
```

図 2.8　hsdからIISサーバへのポート切り替え指示

図 2.9　簡易IDS指示による切り替えの完了報告

3. プロトタイプの適用評価

(1) 適用評価の目的

イントラネットにおいて、同提案方式の適用可能性を検討すべく、下記に示す項目について確認を行なった。

(a) ポート番号切り替えによるWebサービスの提供

実環境下において、ポート番号切り替えに伴うWebサービスへの影響有無を確認する(表 3.1：①ユーザ利用テスト、②セッション制御動作テスト)。

(b) 検知機構と連動したポート番号の自動切換え

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番号切り替えを対象に動作確認を行なう(表 3.1：③切り替えテスト)。

(2) 適用評価の環境

図 3.1、表 3.2に示すイントラネット実環境下で適用評価を行なった。

(3) 結果と考察

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のWebサー

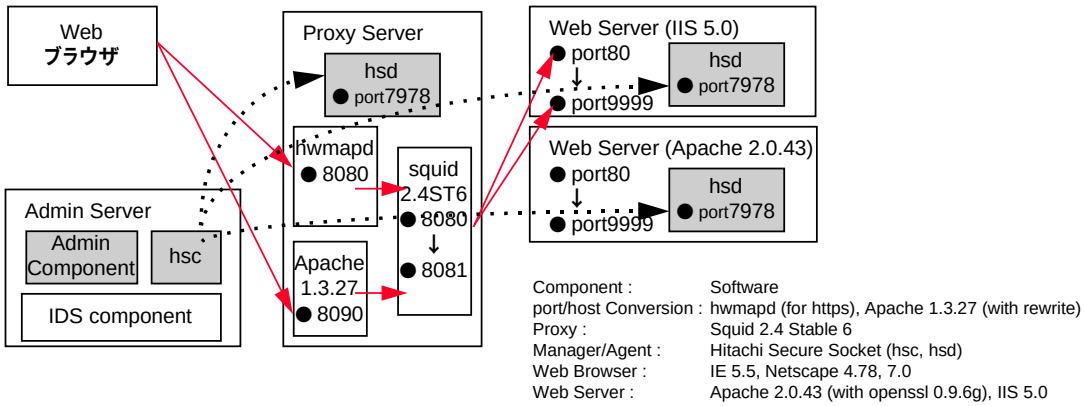


図 3.1　適用評価の構成概要

表 3.1　確認項目

分類	確認内容
① 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 Proxy 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はない。
	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、例えば、インターネットならびに、他サイトのページについては、これまで通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。
② セッション制御動作テスト	Web サーバのポート切り替え後(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。
	ポート切り替え後(80=>9999)も、ユーザの追加操作なく、Cookie セッション制御アプリケーション, URL セッション制御アプリケーションを継続して利用可能である。
③ 切り替えテスト	Web ベースの管理インターフェース(http://admin:20021/) からの指示に従い、Web サーバのポート番号の切り替え、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。
	簡易 IDS からの指示に従い、Web サーバのポート番号の切り替え、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。

表 3.2　適用評価の環境

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
切り替えテストで確認した 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、代替ポートを準備して確認を行なったサイトは 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なった。

ビス継続利用を妨げる問題はなかった。また、「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。ただし、切り替えテストについては、切り替え動作自身にはトラブルはなかったが、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に約 1 分/サイトを要しており、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がある。

4. おわりに

本稿では、Web マッパの上位概念である Alternative Service Plane と呼ぶフレームワークについて述べると共に、Web マッパの機能拡張とイントラネットで実施した適用評価について述べた。今後は、適用評価で得られた知見を元に機能改善を図り、Web マッパの試行運用へとつなげて行く予定である。

参考文献

1) 不正侵入はこう防げ, 日経コンピュータ, No.448, pp185-195, July 1998

2) 寺田真敏、永井康彦、倉田盛彦：「Web サービスを対象とするワーム流布対策方式の検討」, 研究報告 コンピュータセキュリティ No.018 - 014 (2002.07)

3) 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)