Intrusion Trap Systemの設計および実装

2G−1

竹森 敬祐　力武 健次　清本 晋作　田中 俊昭　中尾 康二

（株）KDDI研究所

Email: {takemori, kenji, kiyomoto, toshi, nakao}@kddilabs.jp

1. はじめに

日々多様化する攻撃手法の把握は、セキュリティ確保の面で重要である。最近では、侵入手法を収集する方式として、a)脆弱な機器をおとりにして誘き寄せる方式[1]、b)疑わしいと判断された時点でTrap Serverへと強制誘導する方式[2]-[4]が研究されている。b)についてはVLANを適用する応用技術も検討されている[5]。本稿では、b)方式のシステムをIntrusion Trap System（ITS）と呼ぶ。

これまで、著者らはITSについて、i)一台のサーバ内部に正規領域とおとり領域を設けるシステムと、ii)正規サーバと独立におとりサーバを設ける手法について提案してきた[3]。i)の手法について、実装評価を行った結果、コマンド変換処理が複雑となる問題点が明らかになった。

本稿では、ii)の手法に基づくシステム設計、実装を行うことにより、最も現実的なITSソリューションについて、性能評価を交えて検討する。

2. おとりサーバを分離したITSのシステム要件

2.1. 本稿で想定するITSの定義

ITSは、侵入者が様々な手法を試しながら攻撃している過程において、その中にIDSによって検知される既知の攻撃が含まれてことを想定し、その攻撃の検知をトリガとして、攻撃者を正規サーバ（RS: Regular Server）からおとりサーバ（SMS: Security Mirror Server）に誘導し、侵入者の試す未知の攻撃手法の入手のため、行動ログを記録するシステムと定義する。記録された行動ログは、今後の新たな侵入手法の解析のために用いられ、その結果を早期にIDSへ反映させるものである。

2.2. システム設計のための要件

要件1）既存のRSを変更なく利用できること

要件2）疑わしい行為が検知されたセッションについてはRSから隔離すること

要件3）解析のための行動ログは、攻撃者からの不正なログ改竄に備えてSMSの外部装置に管理されること

要件4）誘導先のSMSのRoot権限が奪取された場合でも、踏み台にされないこと

要件5）応答性の観点からITSが仕掛けられていることが露呈しないこと

3. 設計および実装

3.1. ITSの機能モジュールと構成設計

ITSを構成する機能モジュールとしては、RS／SMS、誘導機能（IDSとの連携機能も含む）、行動ログ記録、分析機能、IDSが考えられる。これら機能から、ITSの構成設計を示す。

1）RSは無改修（要件1）。

2）誘導機能をRSとは独立に設計（要件2）。

3）行動ログ記録／分析機能をSMSとは独立に構築（要件3）。

4）上記独立の両機能を、速度性と秘匿性の観点から一つのホスト上に外部アクセス制御装置(AC: Access Controller）として設計。

5）すべての通信セッションは、上記ACを必ず経由するものとし、必要なアクセス制限（e.g.中継機能の禁止等）をACにて提供（要件4）。

3.2. AC設計

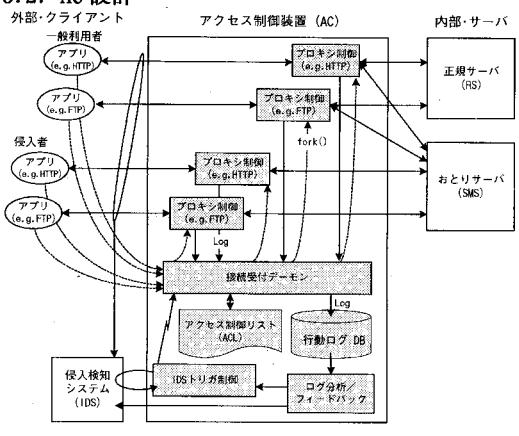

図1. ACの基本設計

図1にACの基本設計を示す。以下に、各種モジュールについて説明する。

a) *アクセス制御リスト（ACL）*：既知の侵入者IPな

Design and Implementation of Intrusion Trap System

Kosuke TAKEMORI, Kenji RIKITAKE, Shinsaku KIYOMOTO, Toshiaki TANAKA, Koji NAKAO

KDDI R&D Laboratories inc.

らびに保証された管理者 IP を登録しておき、通信開始時点での誘導制御に利用する。

b) *行動ログ DB*：解析に必要な項目を記録する。

c) *接続受付デーモン*：クライアントからの接続要求の受付ならびに行動ログの管理を一括で行う。内部から第三者の外部ホストへの接続要求は受け付けない。

d) *プロキシ制御*：クライアント-サーバ間のセッション毎に fork されて、コマンドを中継する。

e) *IDS トリガ制御*：IDS のログを監視、分析して誘導トリガを発行する。

f) *ログ分析／フィードバック*：攻撃ログを抽出し、IDS へフィードバックする。

3.3. 同期制御と誘導制御

RS と SMS の状態同期を図る制御ならびに侵入者の誘導制御は、d)のプロキシ制御が行う（要件 5，性能については 4 章にて検証）。

クライアントが侵入者と判定されるまでの RS と SMS の同期は、プロキシ制御が RS と SMS の両者へ、クライアントからのコマンドを送信し、この両者からのレスポンスを待って、RS からのレスポンスをクライアントへ送信することで実現する。

侵入者の誘導は、ACL もしくは IDS トリガ制御から、接続受付デーモンがトリガを受け取ると、該当するプロキシ制御へ通知して、RS とのセッションを即座に切断、、以後は SMS からのレスポンスのみを侵入者へ送信することで実現する。

3.4. 実装

ここでは AC による誘導制御と同期制御を評価するため a)から d)について、Linux OS 上で実装した。e)については手動制御によって模擬した。AC は C 言語を用いて開発し、gcc でコンパイル・実装した。各プロセスのステップ数を表 1 に示す。

表 1. AC 上のプロセス・ステップ数

プロセス名	接続受付デーモン	FTPプロキシ	HTTPプロキシ
ステップ数	1970 ステップ	1940 ステップ	1400 ステップ

4. 性能評価

ここでは、最も大きな処理時間が予想される、RS と SMS の両方との同期を図る AC のコマンド中継処理に注目する。なお、誘導処理については、RS とのセッションを切断して、代わりに SMS からのレスポンスを返信するのみであり、十分高速な応答性が見込まれるため、ここでは評価しない。試験は、図 2 の環境で行い、侵入者が利用すると思われるコマンドについて評価する。このときの結果を図 3 に示す。

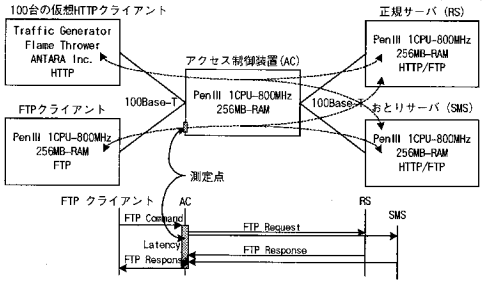

図 2. 処理速度評価環境

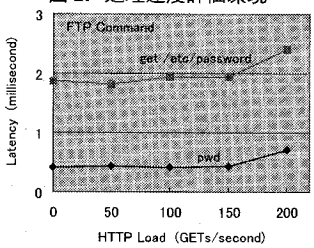

図 3. HTTP 負荷を加えた時の FTP コマンド遅延特性

HTTP-GET のバックグランド負荷が 200GET/秒以内であれば、FTP コマンド・レスポンスが数ミリ秒程度で処理できることを確認した。処理速度の面で、ITS の存在を検知されることはないと言える（要件 5）。

5. おわりに

本稿では、プロキシの役割を担う AC を導入することで、既存の RS を変更することなく ITS を構築する手法について述べた。今回の実装では、FTP を用いた Web データ管理を想定した ITS に絞ったが、本手法は、その他の応用においても基本的に流用可能である。同期制御と誘導制御について詳細な検討を行い、同期制御については十分な高速性が実現されていることを評価、確認した。

今後は、IDS トリガ制御の自動化と行動ログの分析・フィードバック機能について開発を進める。

参考文献

[1] Honeynet Project, http://project.honeynet.org/project.html

[2] E. G. Amoroso, “Intrusion Detection : An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response”, Intrusion. Net Books, Sparta, NJ, 1999.

[3] 竹森，田中，中尾，“不正侵入者に探知されない通信セッションのおとりサーバへの引継ぎ方式の検討”，情処 第 61 回全国大会論文集，5G-1，2000.

[4] 竹森，田中，清本，中尾，“不正侵入者に探知されることなくおとりのデータ領域へと誘導するおとりシステムの実装評価”，情処 CSEC，pp79-84，2001 年 2 月.

[5] 宮川，稲田，後沢，“不正侵入者を外部ネットワークに設置したおとりサーバへ誘導するセキュリティシステムの検討”，情処 CSEC，pp225-230，2001 年 7 月.