不正侵入者に検知されることなくおとりデータ領域へと誘導するおとりシステムの設計

1S-05　　竹森 敬祐　　田中 俊昭　　中尾 康二

KDD 研究所

Email: {ke-takemori, tl-tanaka, ko-nakao}@kddi.com

1. はじめに

ISP(Internet Service Provider)が提供するホームページサービスに代表されるように、FTP を利用したWebサーバのリモート管理が多く実施されている中、ホームページの改竄に対する脅威が拡大している。これまで、様々なセキュリティ対策ツールが開発されてきたが、不正侵入者はこれらのツールを回避する新たな手法を考案し続けており、サーバ管理者は最新の侵入手法の把握や対策に努めなければならない。近年では、不正侵入者の行動ログを積極的に収集・追跡する方式が現れてきた[1]。

このような背景の中著者らは、外部不正侵入検知システムから通知を受けると、不正侵入者に気付かれないようにアクセス先をおとりデータ領域へと誘導し、起動したプロセスや実行したコマンド等の行動ログを収集して、その挙動を把握することで、以後の同様な手法を用いた不正侵入行為への対策を図る為のシステムを提案した[2]。

本稿では、[2]で提案したおとりデータ領域システムに関する具体的な設計手法について述べる。

2. おとりデータ領域とシステム構成要件

本システムは、Web ファイルの更新を、FTP を用いて行うシステムを対象とし、不正侵入者からの FTP と Web アプリケーションへのコマンドをリアルタイムに制御して、通信中のアクセス先をおとりデータ領域へと誘導する。

2.1 おとりデータ領域要件

詳細なログを収集するためには、アクセスしているデータがおとりであることが探知されないように、

- ファイルシステム／公開用の Web ファイル
- 証拠隠滅の標的にされるシステムログ

などについて、正規データ領域と整合性が保たれなければならない。用意するファイルシステムや Web ファイルは、改竄、削除されても構わないが、情報が盗まれたときのことを想定して、最小限もしくはダミーのものを用意するべきである。

"A Design of Non-detectable Session Switching Mechanisms using Decoy Directories", Keisuke TAKEMORI, Toshiaki TANAKA, Koji NAKAO, KDD R&D Laboratories inc.

2.2 システム構成要件

既存の通信アプリケーションを変更することなく、各不正侵入者のコマンドを監視・誘導するために、

- コマンドのアクセス先とレスポンス

を制御する通信アプリケーション・インターフェースの役割を果たす機能が必要である。また、全てのコマンドやプロセス状態を管理するための、

- 独自のログ

を収集する機能も必要となる。

また、本サーバが他のサイトへの攻撃の踏み台に利用されないように FTP port21 と HTTP port80 のみオープンすることや、プロセスを奪取されても問題ないように不正侵入者が起動するプロセスの uid、gid を非特権ユーザとする等の対策も必要となる。

3. 設計

3.1 システム構成と処理フロー

動作する OS 環境として Linux を想定する。

図1に、クライアントと通信アプリケーションとの間に、接続要求の受付ならびにログの管理を一括で行う通信管理プロセスと、クライアントと通信アプリケーションの接続ごとにコマンドを中継・不正侵入者のアクセス先をおとりデータ領域へ誘導するアクセス制御プロセスを新たに設置する本システムの基本構成を示す。本システムは、①クライアントからの接続要求を一括して通信管理プロセスで受付け、②アクセス制御プロセスを通じて、③通信アプリケーションへと通知、④この応答をアクセス制御

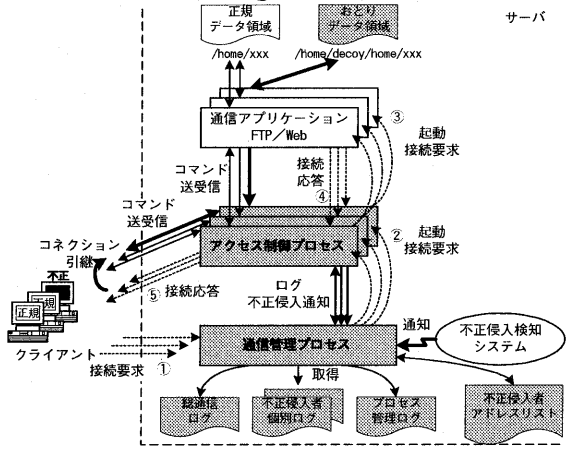

図1　システム構成

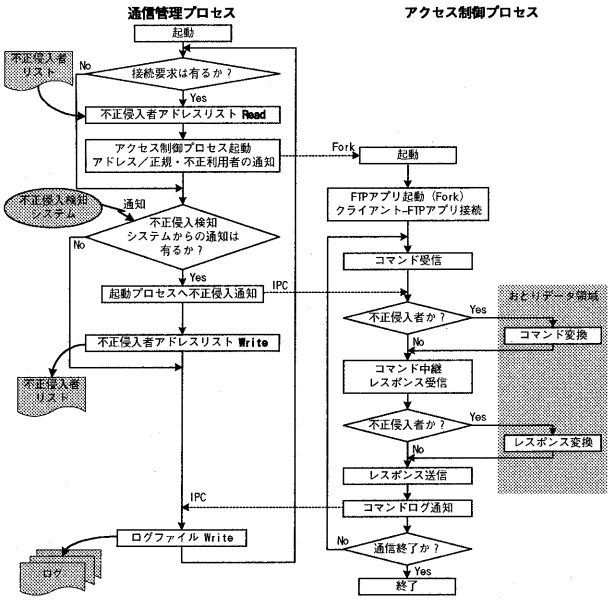

図2　処理フロー

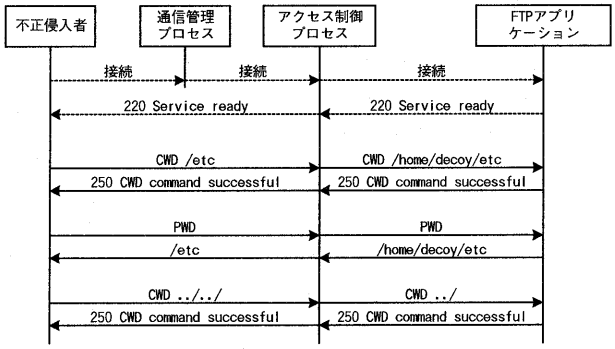

図3　FTPを利用した不正侵入者の通信シーケンス

プロセスへと返し、⑤ここから直接クライアントへと返信する。以後のクライアントと通信アプリケーション間の通信は、アクセス制御プロセスが引継ぐ。

図2に、FTPを想定したときの、通信管理プロセスとアクセス制御プロセスの処理連携フローを示す。

図3に、FTPを想定したときの、接続処理ならびに誘導シーケンスを示す。

3.2 通信管理プロセス

接続デーモンの役割を果たす通信管理プロセスは、クライアントからの接続要求を受け取ると、そのアドレスが不正侵入者リストに登録されているかをチェックする。チェックの結果とアドレスを持って、アクセス制御プロセスを生起する。アドレスと起動したプロセスIDを管理しておき、通信中に外部不正侵入検知システムから通知を受けた時、該当するアクセス制御プロセスへその旨を通知する。接続ごとに取得されるコマンドログ、通信に関ったプロセスの起動・終了ログについて、次の3つを管理する。

- 全てのコマンドログ　・・・・・・・・一括
- 不正侵入者コマンドログ　・・・・・・・・個別
- 関ったプロセスの起動・終了ログ・・・・・一括

3.3 アクセス制御プロセス

通信管理プロセスから受け取ったクライアントのアドレスを基に、通信アプリケーションと接続する。クライアントが正規利用者の場合、コマンドはそのまま通信アプリケーションへ中継され、レスポンスもそのままクライアントへ返信される。不正侵入者の場合、各コマンド中にあるディレクトリ部分を解析して、おとりデータ領域へアクセスするようにコマンド変換を行い、レスポンスについても、正規データ領域へアクセスしたかのように変換して、返信する(図3)。おとりデータ領域よりもさらに上のディレクトリへアクセスする矛盾したコマンドの場合、コマンド内容を再構成し、おとりデータ領域へ留まるようにする。

これら正規・不正利用者の全てのコマンドログは、プロセス間通信にて通信管理プロセスへ通知する。

3.4 おとりデータ領域

攻撃を許容できるファイルシステムやWebファイルを用意するが、cgiやperlの機能を実現するためのshやperlについてはセキュリティホールに繋がるため、これらは用意しない。ログイン履歴の残るwtmp、messagesと、FTP、Webアクセスの状況の残るxferlog、access_logについては、不正侵入者のログが記録されている個所と、おとりとしてのダミーのログを最小限コピーする。コピーは、初めてアクセスされるタイミングで行う。

4. おわりに

本稿では、Webサーバにおける不正侵入者のアクセス先をおとりデータ領域へと誘導し、行動ログを収集するシステムの設計手法について検討した。不正侵入者の挙動を把握して対策を図ることで、以後の同様な手法を用いた攻撃を許さないセキュリティレベルの高いWebサーバを構築できるようになる。

本設計では、通信管理プロセスに、i)ログ管理処理とii)不正侵入通知処理が集中している。今後は、負荷分散の面でこれらの処理を別プロセスとして管理させる設計について検討する必要がある。また、アクセス先をOSが制限するchrootコールを用いる手法も考えられるが、chrootを利用した誘導手法の設計についても今後の課題とする。

参考文献

[1] Amoroso, Edward G., "Intrusion Detection : An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response", Intrusion. Net Books, Sparta, NJ, 1999.

[2] 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", 情報処理学会第61回全国大会論文集, 5G-1, 2000.