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

4F-03

竹森 敬祐　　田中 俊昭　　中尾 康二

(株) KDD 研究所

Email: {ke-takemori, tl-tanaka, ko-nakao}@kdd.co.jp

1. はじめに

近年、ホームページの改竄に代表されるような公開サーバへの不正侵入が痕を断たない。これに対するセキュリティ管理方式として、不正侵入を検出し、その通信セッションを切断、被害の拡大を防ぐ方式がある。また、不正行為に対する行動ログを収集すると伴に、侵入者を追跡する方式がある[1]。このような方式を組み合わせた不正侵入者への抑止力を持つ侵入検知・追跡システムが注目を集めている[2]。

有効な追跡・防御対策を施すには、IP アドレス、起動・終了したプロセス、実行したコマンド、キー入力に至るまでの不正侵入者の行動の詳細を記録することが重要である。しかしながら、行動ログを収集するために通信セッションを継続させることで、公開用データ領域に攻撃を加えられる恐れがある。

そこで本稿では、おとりを用いて公開用データ領域の安全性を保持しながら、不正侵入者の行動ログを収集できる新たな方式を提案する。

2. 攻撃手法とシステム要件

2.1. 対象とする攻撃手法

様々な方法を用いてシステムに対する不正侵入が行われているが、本稿では以下に示す最も一般的な手法についての対策を検討する。

① ターゲットシステムの探知
② セキュリティホールを衝いた管理者権限の取得
③ FTP や telnet による侵入:ファイルの改竄／盗難／削除
④ 痕跡隠蔽のためのログファイルの偽造／削除

2.2. システム要件

侵入検知・追跡システムに対する要件として、

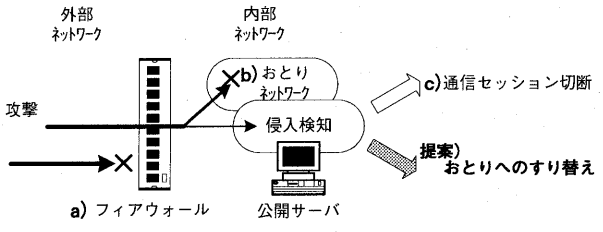

図1　様々なセキュリティ手法と提案手法

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

(1) 公開データ領域を保護する
(2) 不正侵入者に探知されない

が挙げられる。これまで、セキュリティ対策として、

a) ファイアウォールを用いて不正侵入を防ぐ
b) 仮想ホストからなるおとりネットワークへと誘き寄せる
c) 侵入検知システムによる通信セッションの切断

等が提案され、システムに適用されてきた。しかしながら、a)、b)、c)のいずれの対策においても、要件(1)、(2)を同時に満たすことができない。

本稿では図1に示すように、ファイアウォールやおとりネットワークをすり抜けて、公開サーバへ侵入された場合でも、この危険な通信セッションを不正侵入者に探知されることなく、おとりへとアクセス先をすり替え／引継ぎ、公開データ領域を保護しながら行動ログを収集できる手法について提案する。

3. 提案モデル

おとりモデルとして、アクセス先を仮想領域へすり替える手法があるが、不正侵入者に、より探知されにくくするためには、実データを用いたおとり手法が有効的であるとされている。そこで本稿では、公開サーバ上におとりデータ領域を設けるモデルと、おとりサーバを別に設けるモデルを提案する。

3.1 おとりデータ領域モデル

図2に、公開サーバ上におとりデータ領域を設けて、そこへ通信セッションをすり替えるときの構成、及び、不正侵入者、ルータ、公開サーバ間における正常コマンドと違反コマンドの通信シーケンスを示す。本モデルでは、TCP/IP レイヤと FTP や telnet などの通信プロセス間に、違反コマンドを検知しておとりデータ領域へとアクセス先をすり替える侵入検知／コマンド変換プロセスを新たに設置する。

正常コマンドの場合、不正侵入者からのコマンドは、そのまま通信プロセスまで到達し、応答もそのまま不正侵入者まで返信される。違反コマンドの場合、以下の手順に従う。

① 公開データ領域への侵入検知
② おとりデータ領域へアクセスするようにコマンドを変換
③ 公開データ領域からのレスポンスのように応答を変換
④ 以後、不正侵入者とおとり領域間での通信を継続

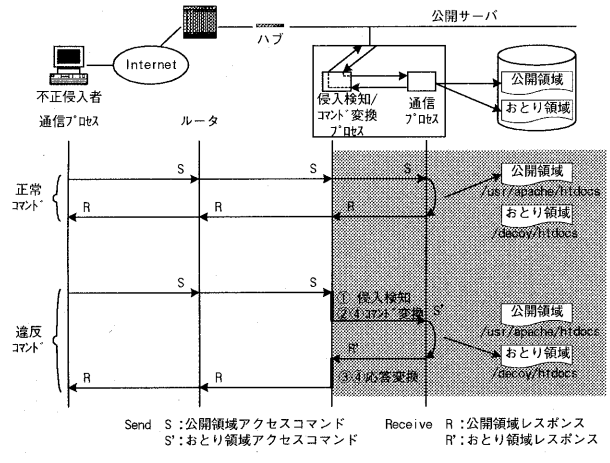

図2　おとりデータ領域モデルにおける通信シーケンス

3.2 おとりサーバモデル

おとりサーバを別に設ける場合、不正侵入者と公開サーバとの依存性を極力少なくする必要がある。すなわち、公開サーバにて侵入検知がなされた場合、一旦ルータに切り戻し、おとりサーバに再ルーティングする方式が優れており、本稿ではルータを用いた引継ぎ方式を提案する。図3に、おとりサーバを別に設けて、そこへ通信セッションを引継ぐときの構成、及び、不正侵入者、ルータ、公開サーバ、おとりサーバ間における正常コマンドと違反コマンドの通信シーケンスを示す。ルータには通信中にセッションの切替を行えるソフトウェアルータを適用する。公開サーバには不正コマンドを検出して通信セッションを切断する侵入検知プロセスを、おとりサーバには公開サーバ宛てのコマンドを取り込み通信プロセスへ通知する通信中継プロセスを、それぞれ設置する。不正侵入を検知した際、より迅速に引き継ぎ要求をルータに通知するため、専用の割込回線を用意する。おとりサーバは、通信セッションの引継ぎをスムーズに行うために、公開サーバの通信状態を模擬させておく。このため、通信シーケンスの揺らぎを吸収するためのバッファが必要になる。

正常コマンドの場合、コマンドはそのまま公開サーバの通信プロセスまで到達する。違反コマンドの場合、以下の手順に従う。

① おとりサーバにおいて公開サーバの通信状態を模擬
② 公開サーバへの侵入検知／通信セッションの終了
③ 公開サーバからルータへ通信セッションの引継ぎを要求
④ ルーティング情報の変更／おとりサーバへの引継ぎ
⑤ おとりサーバによる通信セッションの切替検知
⑥ おとりサーバから不正侵入者への応答開始
⑦ ルータから不正侵入者への応答元変換
⑧ 以後、不正侵入者とおとりサーバ間での通信を継続

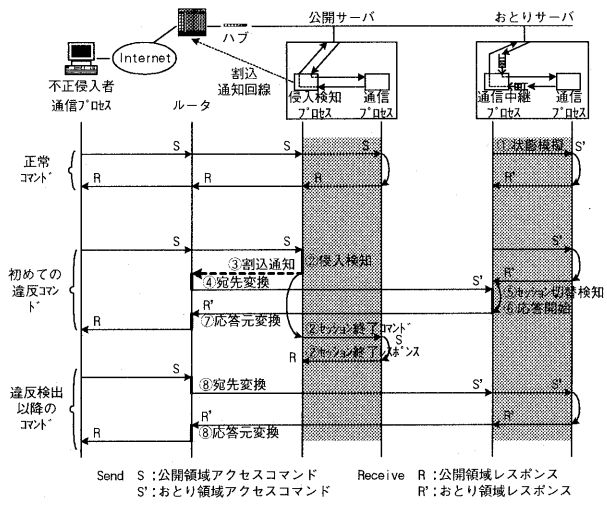

図3　おとりサーバモデルにおける通信シーケンス

4. 提案モデルの比較検討

提案した2つのモデルを各種ネットワークへ適用するときに考慮すべき特徴について表1に示す。

表1より、おとりデータ領域モデルの方が、ホスト側の負荷が大きくなるものの、開発規模が小さく、実装が容易であることが分かる。また、おとりサーバモデルでは、サーバ自体に対する攻撃には安全性が高いが、おとりサーバの通信状態を公開サーバと同期させるための仕組みが複雑となり、開発規模が大きくなる。これらの特徴を考慮して、セキュリティポリシィに従ったモデルを適用する。

表1　すり替え／引継ぎ方式の特徴比較

	おとりデータ領域モデル	おとりサーバモデル
安全性	サーバ自体への攻撃に対して公開領域に影響あり	サーバ自体への攻撃に対して公開サーバに影響なし
負荷	公開サーバ負荷の増加	ルータ負荷の増加
開発	公開サーバの開発	公開サーバ／おとりサーバ／ルータの開発

5. おわりに

本稿では、公開データ領域を保護するセキュリティ手法の一つとして、通信セッションを不正侵入者に探知されないように、おとりへとすり替え／引継ぐ手法について提案し、実装のための動作手順を検討した。また、各種ネットワークへの適用を考えたときの安全性や開発コストなどについても考察した。

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] 藤井, 大越, 辻, 小林, 太田, 勝山, "不正侵入検出手法に関する一考察", 情報処理学会第57回全国大会論文集, 6G-6, 1998.