6Q-09

不正アクセス発信源追跡システムに対する多重化防御方式の検討*

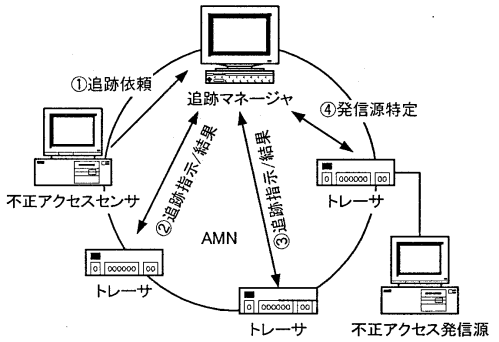
加藤幹一郎、 寺西俊晴、 横山義人、 飯田伸一
東日本電信電話株式会社 法人営業本部マルチメディア推進部
和氣弘明、 吉田一憲
NTT アドバンステクノロジ株式会社 ネットワークソリューション事業本部

1. はじめに

インターネット利用者の増加に伴い多発する不正アクセスに対して、その発信源を追跡する不正アクセス発信源追跡システム(以降、追跡システムと呼ぶ)の研究を行っている[1]。本稿では、追跡システムの可用性を高めるため、追跡システム自体に対する不正アクセスを多重化により防御する方式を検討する。

2. 不正アクセス発信源追跡システム

追跡システムは、不正アクセスのパケットに着目し、送信元 IP アドレスが偽造されていた場合でも、そのパケットが中継されてきたルータ等を一つ一つ遡ることによって、不正アクセスの発信源を特定するものである。主に不正アクセスセンサ、追跡マネージャ、トレーサから構成される(図1参照)。



AMN: Autonomous Management Network(自律管理ネットワーク)

図1. 不正アクセス発信源追跡システムの構成

3. 多重化防御方式

3. 1 防御対象

追跡システムにおいて追跡マネージャは追跡の全制御を担当しており、追跡マネージャへの不正アクセス等により機能を維持できなくなった場合、当該自律管理ネットワーク(AMN)内に関する全ての不正アクセスの発信源追跡が不可能になる。したがって、追跡マネージャの防御に関してはより厳重な防御施策を施す必要があり、その防御方式としてフォールトトレラント技術を応用した多重化防御方式を検討する。

なお、不正アクセスは外部からネットワークを経由して行われるものを対象とし、システム管理者の悪意等による内部犯行は対象外とする。

3. 2 防御方式概要

多重化防御方式は追跡マネージャとその搭載ホストを防御するものである。一般にあらゆる不正アクセスから追跡マネージャを完全に防御することは非常に困難なため、本方式では不正アクセスの基本的防御を行うと共に、万が一不正アクセスを受けた場合でも、その機能を維持することを目標とする。機能維持対策としては、追跡マネージャ搭載ホストを多重化し、不正アクセス等による異常発生時に予備に切り替えることで対応する。

3. 3 システム構成

追跡マネージャ搭載ホストを現用と待機(複数可)の多重構成とし、現用/待機ホスト間を内部ネットワークにより接続する(図2参照)。ただし、待機ホストは AMN 側ネットワークに接続しない配置(物理的に接続されているが、ネットワーク I/F は停止した状態)とする。

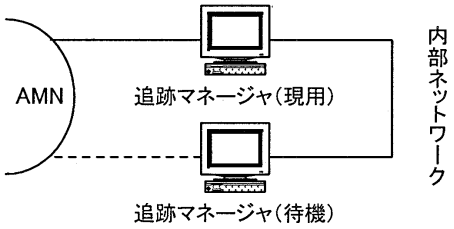


図2. 追跡マネージャサイトの構成

多重化防御方式は、アタック防御部、通信中継部、不正アクセス監視部からなる不正利用防止プログラムを用いて実現する(図3参照)。

---

* A Proposal of a Multi-Defense Method for Unauthorized Access Tracing System.
Kanichiro Kato, Toshiharu Teranishi, Yoshihito Yokoyama, Shinichi Iida, NTT East Corp.
Hiroaki Waki, Kazunori Yoshida, NTT Advanced Technology Corp.

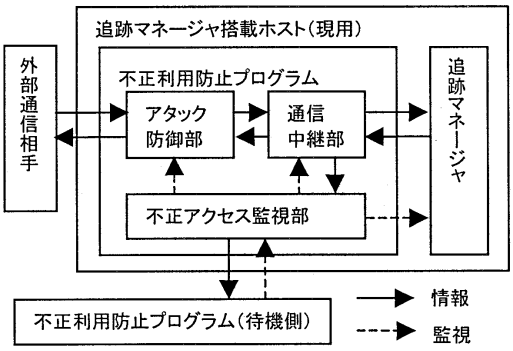


図3. ソフトウエア構成

アタック防御部は、ファイアウォールと同様のアクセス制御を行う。通信中継部は、不正アクセスセンサやトレーサなど追跡マネージャと接続する全ての外部通信を中継し、接続時に認証を行う。

3.4 不正アクセスの監視

防御機構を突破された場合を想定し、不正アクセス監視部は、追跡マネージャとその搭載ホストへの不正アクセスを常に監視する。以下に監視項目を示す。このうち、(1)～(4)は現用ホスト内、(5)は待機ホストが現用ホストに対して行うもので、これらにより、システム異常を検出することとする。

(1)プロセス監視: 規定プロセスの稼動、および規定外プロセスの稼動を監視する。

(2)プロセス機能監視: バッファオーバーフロー攻撃等による追跡マネージャや不正利用防止プログラム等の機能異常を監視する。

(3)ファイル改竄監視: 追跡システム関連ファイルや OS 設定ファイル等の改竄を監視する。

(4)監査ログ監視: 監査ログを基に規定外の操作(ログイン、コマンド実行等)を監視する。

(5)不正利用防止プログラム監視: 待機側から内部ネットワーク経由で現用側の不正利用防止プログラムの生存/機能異常を監視する(現用ホストの生存確認含)。

3.5 追跡マネージャ搭載ホストの切替

現用ホストの異常を検出した場合、待機ホストに切り替えることで機能を維持する。ただし、切替により IP アドレスを変えるため(再アタック低減策)、不正アクセスセンサは現用ホストへの接続に失敗した場合、待機ホストに接続を試みる。以下に切替手順を示す。

(1)現用ホスト内で異常を検出した場合

①不正アクセス監視部が自ら現用ホストをダウン

②待機ホストは現用ホストダウン検知後、AMN 側ネットワーク I/F を起動し、現用に移行

(2)待機ホストが現用ホストの異常を検出した場合

①待機ホストは現用ホストを強制的にダウン

②待機ホストはネットワーク I/F を起動し現用に移行

3.6 追跡処理中の切替

追跡処理中に異常を検出し、切替が発生した場合でも途中から追跡を再開できるように、追跡の進行状況を追跡情報として現用から待機に送信し、待機ホスト側で保存する。待機ホストは現用に移行後、追跡情報を元に途中から追跡を再開する。図4は追跡中にトレーサ2へ追跡指示を出し、結果を待つ時点で切替が生じた例を示す。待機ホストは、追跡情報により①～④までの情報を保持しているため、トレーサ2への追跡指示を出す処理から再開が可能となる。

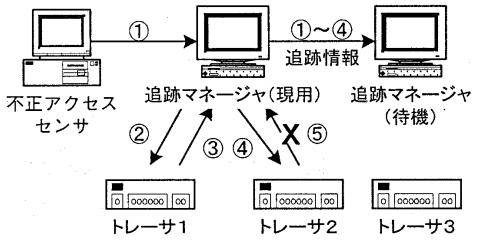


図4. 追跡処理中の切替

4. おわりに

不正アクセス発信源追跡システムにおいて、追跡マネージャを多重化することによる防御方式を示した。今後はプロトタイプを作成し、監視機能や切替処理等の適用性評価を行う予定である。

謝辞

本研究は、通信・放送機構(TAO)の委託研究テーマ「不正アクセス発信源追跡技術に関する研究開発」の一環として行われているものである。

参考文献

[1] 小久保他:“不正アクセス発信源追跡システムのモデル検討”, 情処 60 全大, 6Q-04, Mar. 2000.

[2] “フォールトトレランス特集”, 日本信頼性学会誌, Jun. 1998.