不正アクセス発信源追跡システムに対する不正利用防止アーキテクチャの提案*

3H－07

建部　英輔、田中　美穂、千喜良　和明
東日本電信電話株式会社

1. はじめに

不正アクセス発信源追跡システム（以下、追跡システム）の研究開発[1]の一環として、想定されるインターネットからの脅威の分析から、それぞれの脅威に対する防御技術や方式の検討を行ってきた。本稿では、追跡システムに対する不正利用を防止する為の防御技術とその方式（枠組み）を、不正利用防止アーキテクチャとして提案する。

2. 防御対象と脅威

一般的に、様々な手法による不正利用の脅威が存在するが、本稿では、追跡システム内の保護すべき対象を整理する事で、脅威への対策を網羅した。

追跡システムは、攻撃者からの攻撃を不正アクセスセンサが検知後、追跡マネージャへ追跡依頼を行い、追跡マネージャがネットワーク上に配置されたトレーサの持つ情報を元に不正アクセスの発信源まで遡るシステムである[1]。追跡システムについて、保護すべき対象（以下防御対象）は、構成要素間を流れる通信データや設定ファイルやログの保持データという「データ」部分と、上記不正アクセスセンサ、トレーサ、追跡マネージャの構成要素や搭載デバイス、その上で動作する追跡プログラムの「システム」部分に分類できる。

(1) データ（保持データ/通信データ）

脅威としては、データの改竄、盗聴/漏洩（不正読みだし）、虚偽の追跡依頼が挙げられる。これに対し、保持データについては、不正読みだし/改竄防止や原本性保証の対策が必要である。同様に、通信データについても、原本性保証や内容隠蔽の対策が必要である。

(2) システム（構成要素/搭載ﾃﾞﾊﾞｲｽ/追跡ﾌﾟﾛｸﾞﾗﾑ）

脅威としては、サービス妨害、デバイスへの侵入やそれによるデバイスや追跡プログラムの停止、改竄が挙げられ、防御対象の可用性向上の対策が必要である。特に、追跡マネージャは追跡制御の要であるため、より強固な対策が必要である。

3. 提案する対策技術

(1)保持データ：不正読みだし/改竄防止

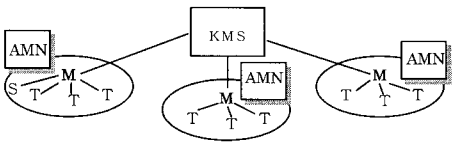
保持データとして、ログ等の証拠データは、ネットワークから侵入/読み出しが不可能であると同時に追記が可能である必要が有るため、構成要素とは別にログマシンを RS-232C で代表されるシリアル接続等で接続しログ出力することで、インターネット側からのログ参照を遮断する、「シリアルロギング方式」を提案する。

(2)通信データ：原本性保証/内容隠蔽

盗聴や虚偽の依頼を防ぐための方法として、通信箇所の特性別に鍵管理から検討した暗号・認証技術の適用について、以下のように提案する[2]。

暗号方式については、通信毎に鍵を変えることによる安全性、暗号用鍵の生成/更新の効率性、処理速度を考慮し、Diffie-Hellman 方式（以下 DH 方式）で鍵を共有し、共通鍵方式で暗号化する方式を提案する。

認証方式については、AMN 内は不正アクセスセンサ/トレーサから見て通信相手が限定されているため、暗号と認証用の鍵を共通化してメッセージ認証（共通鍵方式）を使用することによって、デジタル署名（公開鍵方式）と比較して鍵管理の簡素化と処理速度の向上が図れる。しかし、AMN 間では、インターネット上で通信相手が散在しており、相手毎の共通鍵交換等の鍵管理が困難であるため、メッセージ認証は適さない。従ってデジタル署名を使用することとし、鍵の管理としては、「鍵管理機構」を介在させ、AMN 間追跡の都度、相手の公開鍵を鍵管理機構から取得し認証に用いる方法を提案する。（図1）



追跡マネージャ：M　不正アクセスセンサ：S　トレーサ：T　鍵管理機構：KMS
図1　各構成要素の関係

* “Proposal about the preventions of illegal use for unauthorized access tracing system”: Eisuke Tatebe,Miho Tanaka, Kazuaki Chikira, NTT East Corp.

以上より、適用箇所別に提案する技術を表 1に示す。

表 1 通信箇所と暗号・認証方式

	AMN 間		AMN 内	
	M-KMS	M-M	M－S	M－T
暗号	－	共通鍵	共通鍵	共通鍵
認証	デジタル署名（公開鍵）	デジタル署名（公開鍵）	メッセージ認証（共通鍵）	メッセージ認証（共通鍵）

(3)システム：可用性向上

システムの可用性向上としては、認証/アクセス制御やパーミッション設定、パッチ施工といった一般的なセキュリティ対策が必須である。さらに、追跡マネージャのように機能不能になると追跡システムの動作全体に影響を被るような構成要素は、上記対策をすり抜ける未知攻撃等の不測の事態に対する可用性の更なる確保が必要である。対策として、未知の異常を含む何らかの異常状態の検出機能を設け、異常を検出したら直ちに現用系をネットワークから切り離し待機系へ切替を実現する、「多重化防御方式」を新たに提案する。

また、暗号/認証方式の適用に当たり、追跡システムの機能/処理を妨げず維持するには、(a)鍵/鍵生成情報の破損時や、(b)漏洩/解読/方式弱体化時にもオンライン状態を継続する必要がある。そこで、(a)鍵/鍵生成情報のコピー情報、(b)別の鍵/暗号方式、を用意しこれらへ切り替える、秘密情報二重化方式を提案する。

4. 多重化防御方式

追跡マネージャに適用する多重化防御方式は、追跡マネージャの重要性を踏まえ、可用性向上を目的に提案する技術である[3]。本方式は、未知の不正による異常の監視機能と、異常検知後待機系への切替作業を行う切替機能で構成される。

一般的な冗長系との違いは、切り替わる待機系への連続攻撃を回避するために、現用系とは違うIPアドレスで起動し、クライアントからの再接続によって復帰する部分である。

異常検出をするための監視機能は、①プロセス監視、②プロセス機能監視、③ファイル改竄監視、④監査ログ監視の4種類で構成され、現用側内部では①～④を、待機側から現用側への監視では、②を行う。

発生する異常を監視することの妥当性を検証するため、CVE リストより 726 件の攻撃事例を無作為抽出し、上記監視方法の机上比較調査を行った。(図 2, 図 3)

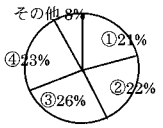


図 2 発生する異常の割合

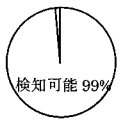


図 3 検知可否の割合

発生する異常において、提案する検知項目に直接当てはまらないものが1割弱あるが、異常状態に至る一歩手前の状態(権限取得等)が殆どである。このケースは、後で①～④の状態に陥った状態で検出できる為、検出可能に分類すると、監視機能①～④によって、実用上問題ないレベルで検出できると言える。

5. おわりに

追跡システムに対する不正利用を防止する為の防御技術とその方式について、防御対象から整理し、各々の対策技術を整理、提案することで、不正利用防止アーキテクチャとして示した。特に、日々悪質化する不正手法からも追跡マネージャを防御する多重化防御方式方式を提案した。

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] 田中他："不正アクセス発信源追跡システムにおける暗号通信方式及び鍵管理方式の検討"、情処 63 全大、1G-06、Sep.2001

[3] 加藤他："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"、情処 60 全大、6Q-09、Mar.2000