6Q－08　　不正アクセス発信源追跡システムの不正利用防止アーキテクチャの検討*

巻田　政好、寺西　俊晴、○建部　英輔、牛川　陽子
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
豊元　厚一、永吉　孝行
東日本電信電話株式会社　研究開発センタ

1．はじめに

本稿は、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、追跡システム自身に対する不正利用を防御するために、トランザクションデータの原本性及び非盗聴性を確保し、更に、本システムの可用性向上に有効な方式条件(不正利用防止アーキテクチャ)について検討するものである。

2. 防御対象と脅威

2．1　防御対象

追跡システムは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、その構成要素をインターネット上に分散配置したものである。

防御対象はシステム構成要素の搭載デバイス(以下デバイス)・追跡プログラム等のシステム部分と、各要素上の記録情報や各構成要素間の通信データ等のデータ部分に大別される。以上を図1に示す。

尚、本稿では、システム外部からの不正利用のみを対象とする。

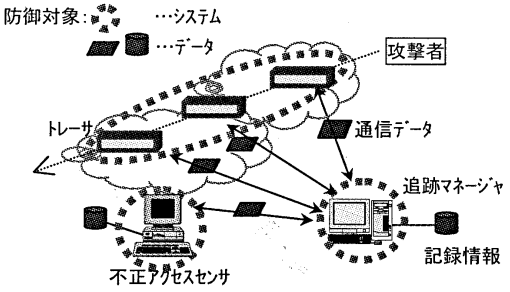

図1．追跡システムの防御対象

2．2　想定される脅威

(1) システム

デバイスへの攻撃については、特に、追跡マネージャ搭載デバイスが停止されると、その追跡マネージャが管理するネットワークに関連する追跡が不能となるため影響が大きい。追跡プログラムへの攻撃の場合も同様であり、十分な防御が必要である。

通信路への攻撃としては、通信路自体への直接攻撃よりも、それに接続されるホストへの攻撃による通信路への影響が主である。通信路自体の過負荷により追跡システムがその機能を果たせなくなる、といった問題も考えられるが、これに関しては、インターネットでの利用を前提とするため本稿の対象外とする。

(2) データ

追跡プログラム(不正アクセスセンサ・追跡マネージャ)によって保持される記録情報は不正アクセスの証拠となるため、改ざんの検出や破壊行為の防御を行わなければならない。また、不正に読み出した情報を解析してデバイスやプログラムを攻撃したり、IPアドレス等の個人情報を入手して不正に利用する、といったことも考慮しなければならない。

通信データについては、インターネットを通信路とすることからデータが第三者に盗聴されたり改ざんされたりする危険性は避けられない。例えば、盗聴により入手した情報を元にプロトコルが解析された場合、虚偽の追跡指示が送信されて、正規のアクセス者が攻撃者として誤認されることも考えられる。従って、データの漏洩やプロトコル解析がなされないようにするため、通信データ自体に十分な対策を施す必要がある。

以上の分析を表1に示す。

3．脅威に対する防御策の検討

2.2 の分析に基づき、それぞれの防御策の検討を行う。

(1) **システム**(デバイス／追跡プログラム)

デバイスや追跡プログラムに対する攻撃はアクセス制御、セキュリティホール対策などの防御方法が適用可

---

* "Discussion about the preventions of illegal use for unauthorized access tracing system: Masayoshi Makita, Toshiharu Teranishi, Eisuke Tatebe, Yoko Ushikawa, Koichi Toyomoto, and Takayuki Nagayoshi, NTT East Corp.

表1. 防御対象と脅威

防御対象		脅威の種別	想定される脅威概要
システム	システム構成要素の搭載デバイス	サービス妨害/デバイス停止/デバイスへの侵入	デバイスの停止による追跡阻止 デバイス停止中の不正アクセス行為
	追跡プログラム	サービス妨害/追跡プログラムの停止/改ざん	プログラム停止による追跡阻止 プログラム改ざんによる誤追跡(誤認)
	追跡プログラム間の通信路	サービス妨害/NW停止・過負荷	通信データ送信不能による追跡阻止
データ	追跡プログラムの保持する記録情報 (不正アクセスセンサ・追跡マネージャ)	改ざん/破壊	証拠データの改ざん・破壊による不正行為の否認
		漏洩(不正読み出し)	データ解析に基づく攻撃
	追跡プログラム間の通信データ ・不正アクセスセンサ～追跡マネージャ	盗聴	追跡記録情報の漏洩/プロトコルの解析による攻撃
		改ざん	追跡依頼の改ざんによる誤追跡(誤認)
	・追跡マネージャ～トレーサ ・追跡マネージャ～追跡マネージャ	虚偽の追跡依頼	存在しない追跡依頼による誤追跡(誤認) 追跡指示の偽装発信によるNW過負荷→追跡不能化

能である。しかし、これらの防御が破られ、攻撃が直接デバイスに到達する危険性を否定することは出来ない。よって、攻撃されたデバイス自体の可用性を確保する新たな方式開発が必要である(詳細は[2]参照)。

(2) データ(記録情報・通信データ)

暗号認証技術・電子署名技術・アクセス制御等により、改ざんの防止・検出が可能であるが、これだけでは破壊行為自体の防御には不充分である。よって、破壊行為に耐えうる追記専用の記録・保存方法を検討する。該当する方法としては「①Write Once メディア(帳票・CD-R等)に保存する方法」や「②外部からネットワーク経由で直接アクセスできない装置を接続して収集する方法」「③カーネルセキュリティレベルを設けて、管理者権限を不正に取得された場合でも操作出来ないように保護する方法」等があげられる。

攻撃者による不正な読み出しや破壊、改ざんの可否等の条件を勘案すると、追記専用で読み出し不可能な上記②の記録方法が望ましい。但し、この方法を適用する場合は、別途装置を準備する必要がある。

追跡プログラム間の通信データについては、防御手段として暗号や電子署名技術の導入は不可欠である。追跡システムでは、通信データサイズが小さく、処理の発生頻度が低いといった特徴があり[3]、公開鍵を含めた暗号方式選定の上での制限は少ない。

不正アクセスセンサ～追跡マネージャ間、追跡マネージャ～トレーサ間の通信は、同じ自律管理ネットワーク内で認証を行い、電子署名を施した暗号化通信を行う。追跡マネージャ～追跡マネージャ間の通信は複数の自律管理ネットワークに跨るため、それを勘案した相互認証の仕組みが必要となる。

更に、各構成要素の追加／削除等の要求条件を考慮すると、これらに柔軟に対応できる鍵管理・認証局の設置が具体化の際の重要な課題となる。

4. おわりに

追跡システムに関する防御対象を特定し、これらに対する脅威の分析と防御の為の方式条件を明確化した。

今後は、デバイスの可用性を確保する新たな方式、効率的な認証や鍵管理を具体化することを目的としたプロトタイプを構築し、実証評価を進める予定である。

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] 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

[3] 竹爪他:“不正アクセス発信源追跡アーキテクチャの一検討”、情処60全大、6Q-06、Mar.2000