1S-04

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評価*

飯田伸一、建部英輔

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

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

不正アクセス発信源追跡システム(以下、追跡システム)[1]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追跡マネージャの多重化により防御する方式を検討した[2]。本稿では、多重化防御方式の実用性についての評価結果を述べる。

2. 多重化防御方式

2. 1 防御方式概要

多重化防御方式は、万が一、追跡マネージャとその搭載ホスト(以下、追跡マネージャ)が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的とする。機能維持対策としては、追跡マネージャの動作異常の監視と多重化により、不正アクセス等による異常発生時には予備に切り替えることで対応する。

2. 2 システム構成

追跡マネージャを現用と外部ネットワークインタフェースを休止した状態の待機(複数可)の多重構成とし、現用と待機ホスト間を内部ネットワークにより接続する。

2. 3 異常監視

異常監視用プログラムは追跡マネージャの動作を常に監視する。以下の監視項目の組合せにより全ての不正アクセスに対応するものとする。

①プロセス監視:プロセステーブルを一定周期ごとに監視することにより、起動許可された規定プロセス群以外の異常プロセス起動の検出、および規定プロセスのダウンを監視する。

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異常監視用プログラム等の機能異常を監視する。具体的には、被監視プロセスとの相互認証によりプロセスの機能異常を検出する。

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・削除を監視する。

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。(市販品流用予定)

⑤異常監視用プログラム監視:待機側から内部ネットワーク経由で現用側の異常監視用プログラムの生存/機能異常を監視する(現用ホストの生存確認含)。機能的には②と同様。

2. 4 追跡マネージャの切替

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。切替の際、待機ホストは外部ネットワークインタフェースを起動し、現用ホストをシャットダウンする。

3. 実用性評価

3. 1 評価の観点

異常監視周期(所要時間)と切替時間を合わせた動作時間が、追跡処理所要時間(5 分を想定)に比べて十分短ければ、実用上問題ないものとする(追跡処理所要時間の 15%、概ね 45 秒以内を想定)。ただし、プロセス監視では、不正プロセス稼動中に検出を行わなければ検知できないため、できるだけ細かい周期で検出を行うことが望ましい。したがって、本評価では最小監視周期を見極めることとする。

(1)異常監視

①プロセス監視:監視対象プロセス数をパラメータとして、指定した監視対象プロセス全ての検査に要する時間を測定する。

②プロセス機能監視:監視対象プロセス数をパラメータとして、指定した機能テスト対象プロセス全ての検査に要する時間を測定する。

③ファイル改竄監視:指定された監視ファイルリストにおいて、監視対象ファイルのファイルサイズをパラメータと

---

* An Evaluation of a Multi-Defense Method for Unauthorized Access Tracing System.
Shinichi Iida and Eisuke Tatebe, NTT East Corp.
Hiroaki Waki, NTT Advanced Technology Corp.

して、監視所要時間を測定する。

(2)追跡マネージャの切替: 追跡マネージャの異常検出後、待機から現用に切り替わるまでの時間を測定する。

3.2 評価環境

評価環境の構成図を図1に示す。

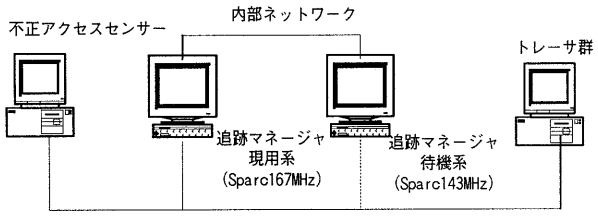

図 1 評価環境構成図

3.3 評価結果

(1)異常監視

①プロセス監視: プロセス監視所要時間を表1に示す。

②プロセス機能監視: プロセス機能監視所要時間を表1に示す。

③ファイル改竄監視: ファイル改竄監視の監視所要時間を表2に示す。

表 1 プロセス/プロセス機能テスト監視時間測定結果

	対象プロセス数 [個]	測定値 [sec.]	備考
プロセス監視	初期プロセス + 0	0.454	初期プロセス:多重化防御方式に最低限必要なプロセス
	初期プロセス + 30	0.928	
	初期プロセス + 50	1.12	
プロセス機能監視	22	0.311	
	33	0.378	
	44	1.838	

表 2 ファイル改竄監視時間測定結果

監視ファイルサイズ [Byte]	測定値 [sec.]	備考
100K	9.482	監視対象ファイル 100 個を 10 個の監視プロセスで分担
1M	27.661	
100M	184.121	

(2)追跡マネージャの切替: 切替時間の測定結果については、平均で 14.176[sec]となった。

3.4 考察

(1)異常監視

①プロセス監視: 追跡マネージャは専用マシンであることを考えると、初期プロセス(異常監視用プロセス含む)に加えてさらに多数のプロセスが増える状況はほとんどないと思われる。表1より初期プロセス+30 個の場合でも監視所要時間は高々1秒であり、実用上全く問題ない時間で監視が行えている。しかし、異常監視周期としては、1 秒程度が限界と思われる。

②プロセス機能監視: 表 1 より、監視対象プロセス数 44 個でも、所要時間は高々2秒であり、実用上全く問題ない時間で監視が行えている。追跡マネージャ自体や監視用プロセス、OS のコアプロセス等重要なもののみを監視するとしても、監視プロセス数は 40 個もあれば十分と考えられる。

③ファイル改竄監視: 表2と切替時間測定結果とを併せると、監視ファイルサイズは1MB 程度が実用上の限界と思われる。しかし、実際の設定ファイルは数 KB 以下が大半であるため、設定ファイルを中心に検査することを想定すると、監視ファイルサイズは 1MB 程度もあれば十分と考えられる。

(2)追跡マネージャの切替: 目標動作時間に対し、監視所要時間と合わせても、実用上問題ないと考えられる。

以上より、動作時間は目標に対して実用上全く問題ないと判断する。なお、プロセス監視では検知できない場合のある起動時間 1 秒以下の不正プロセスに対しても、その結果としての異常は他の監視項目により検出可能であるため、問題ないと考える。

4 おわりに

この評価により本方式の有効性を確認した。今後は他の防御技術との連携を含めた追跡システムの可用性向上を図りたい。

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.