5E-2

侵入検知システムの一考察

時庭康久† 永嶋規充† 後沢忍†

三菱電機(株)情報技術総合研究所†

1. まえがき

2003 年夏の MS ブラストの被害により、ネットワークセキュリティ装置は、組織外部からの侵入を防ぐという目的に加え、組織内部から発生する攻撃を防止するという目的が追加された。我々は、攻撃からネットワークを守るためにセキュリティデバイスを分散配置するシステムの研究開発を行っている。セキュリティデバイスはシグニチャを用いた IDP (Intrusion Detection & Prevention System)機能も実装しているが、IDP の世界ではシグニチャの増加に伴う処理量(負荷)増大が問題になっている。本稿では分散配置の特性を活かした IDP 機能の処理量低減の実現方式について述べる。

2. 基本概念

セキュリティデバイスの分散配置の目的は以下である。セキュリティデバイスをイントラネット内の複数の拠点や建屋の接続点、あるいは複数端末のグループやスイッチの幹線側ポートの接続点に分散配置し、端末の感染の広がりをセキュリティデバイスの境界点で局所化し被害を最小限に留め、復旧を早期実現することを目的としている。(図 1)

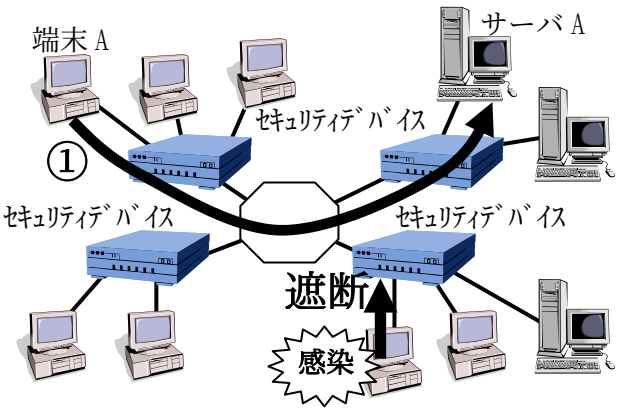

図 1. セキュリティデバイス分散配置

A Consideration of Intrusion Detection & Prevention System.
Yasuhisa TOKINIWA†, Norimitsu NAGASHIMA†, Shinobu USHIROZAWA†
† Information Technology R&D Center, Mitsubishi Electric Corporation 5-1-1 Ofuna, Kamakura, 247-8501 Japan

3. セキュリティデバイスの機能と課題

セキュリティデバイスは以下の 3 つの機能を実現する。

- シグニチャにより既知の攻撃を遮断する IDP 機能
- 不正端末を検出／遮断する検疫機能
- トラヒック解析により未知攻撃を検出する機能

イントラネットの高速化に伴い、セキュリティデバイスの性能向上も求められている。特に IDP 機能に関しては、前述のシグニチャの増加に伴う処理量の増大が課題となっている。我々は検索処理の高速化[1]とともに、分散配置のメリットを活かした IDP の処理量を減らす方法を検討した。

4. IDP 処理量削減の方式

セキュリティデバイスを分散配置することにより端末とサーバ間の通信において、通信路に複数のセキュリティデバイスが存在するケース(図 1 の①)がある。この複数台が処理を連係することにより 1 台当たりの IDP 処理量を減らす方式を考案した。以降にセキュリティデバイス経路探索方式と IDP 処理済み通知方式について述べる。

4.1 セキュリティデバイス経路探索方式

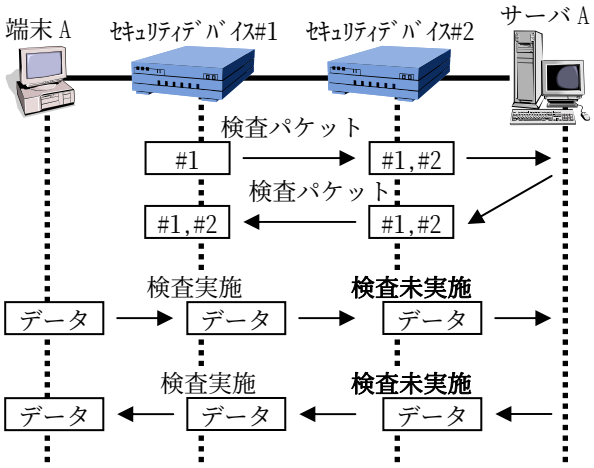

図 2.検査パケットによる探索

セキュリティデバイス経路探索方式は、(クライアント)端末とサーバ間の通信において、端末側のセキュリティデバイスからサーバまでの通信経路上に他のセキュリティデバイスが存在することを検査パケットの往復通信にて検出し、検査パケットの結果を学習し、端末側に一番近いセキュリティデバイスのみが IDP 処理を実施する方式である。

図 2 では、セキュリティデバイス#1 がサーバ A 宛ての検査パケットを送信する。セキュリティデバイス#2 は、検査パケットから(クライアント)端末 A とサーバ A 間の通信では、端末側にセキュリティデバイス#1 が存在することを学習する。通信経路上のセキュリティデバイス#2 は、(クライアント)端末 A とサーバ A 間の通信データの IDP 検査を実施しない。セキュリティデバイス#1 のみが(クライアント)端末 A とサーバ A 間の通信データの IDP 検査を実施する。

検査パケットは ICMP の echo パケットの往復通信でも良いし[2]、サーバに UDP 上のアプリケーションを実装しセキュリティデバイスとサーバ間の UDP の往復通信でも良い。検査パケットの往復通信には暗号化とハッシュ関数による改ざんチェックを加えてセキュリティ向上を図ることも可能である。

4.2 IDP 処理済み通知方式

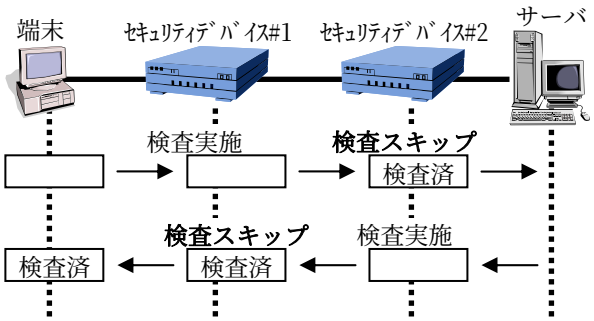

図 3．検査済み通知のパケット通信

IDP 処理済み通知方式は、実通信データ(パケット)内の空き領域に"検査済みフラグ"を設けるか、または通信データの形式変更にて、他のセキュリティデバイスへ IDP 処理実施済みを通知する方式である。セキュリティデバイスは、外部からパケットを受信した場合、パケットに検査済みフラグが有るかを調べて、検査済みの場合には中継し、検査済みで無い場合には、パケットの検査を実施する。検査が OK である場合には検査済みフラグを設定してパケットを中継し、検査が NG の場合にはパケットを廃棄する。

上記検査済みの通知方法では、2 台あるいは、N 台による直列処理方法が考えられる。2 台の例を図 3 に示す。2 台をネットワーク上に直列接続し、お互いに検査済みを他方に知らせる。これによりネットワーク構成によらず処理負荷を容易に軽減できる。N 台のメッシュ構成ネットワークにも適用可能である。

検査済みフラグの実装例と注意点を以下に示す。

(1)特定の VLAN タグを検査済みフラグとして設定
VLAN を使用しているネットワークの場合、実運用している VLAN と整合性をとるためのネットワーク設計が必要となる。

(2)IP ヘッダの TOS フィールドに特定の値を検査済みフラグとして設定
帯域制御などに TOS フィールドが使われている場合、整合をとる必要がある。

(3)IP エンカプセルによる検査済み通知
通信データの形式変更にて"検査済みフラグ"と同等と位置付ける。
(3)-1 IPsec のエンカプセル
(3)-2 独自形式のエンカプセル
IP エンカプセル化では、エンカプセルを実行する装置と解く装置の 2 台構成を基本として、3 台以上の構成では両端でない装置は中継のみ実施する。

(4)TCP のサーバ側の well known ポート番号変換(NAPT 機能)により検査済みフラグ通知
検査したセキュリティデバイスでポート番号を変換し、サーバ手前のセキュリティデバイスで再びポート番号を変換し元に戻す。

5. まとめ

侵入検知システムの一考察として IDP 機能の処理量低減について検討結果を述べた。今後は、実際に作成し検討結果を評価していく所存である。

参考文献

[1]貞包他“侵入検知システムの高速化の一考察”，信学会 2004 年ソサイエティ大会
[2]日本国 特許第３５９５１４５号
【発明の名称】暗号通信システム