ホストベースの IDS の概要と適用について

2002 年 6 月 24 日

Japan Network Security Association
Dynamic Defense Working Group

目次

このドキュメントの目的

近年インターネットの急速な普及と共に、インターネットやネットワークが社会的な基盤（インフラストラクチャ）としての重要度が増している。このため、ファィアウォール等によるアクセスコントロールや暗号化・認証といった、不正アクセスを防止するための技術に加えて、Web 改竄や、EC サイトに対する不正アクセスを迅速に検知し、対応する事が重要な課題となっている。

不正侵入検知においては、ネットワークベース IDS の必要性は認知されるようになったが、アプリケーションに対するアタックや、SSL などの暗号化された通信を使って行われるアタックは、ネットワークベース IDS での検知が難しい面がある。

これに対し、ホストベースの IDS は、セグメント全体を監視することはできない反面、アプリケーションが出力する各種のログから不正アクセスを検知する事や、暗号化された通信を経由した不正アクセスを検知する事が可能である。しかしながら、ホストベース IDS の利用は、ファイルの改竄防止対策程度の利用方法しか認識されておらず、効果的に利用されていることが少ないと思われる。

このドキュメントでは、ホストベース IDS の効果的な利用を促すことを目的として、以下の内容についてまとめたものである。

- **セキュリティ施策における IDS の位置付け**
- **IDS の分類と特長**
- **ホストベース IDS の特長と基本的な利用方法**
- **インシデント発生時の基本的な対応**
- **ホストベース IDS の利用例**

IDS（Intrusion Detection Systems：不正侵入検知装置）について

ホストベースの IDS についての考察を進めるにあたり、ＩＤＳ（Intrusion Detection System：不正侵入検知装置　以下 IDS）について整理する。

コンピュータセキュリティと IDS

IDS とは

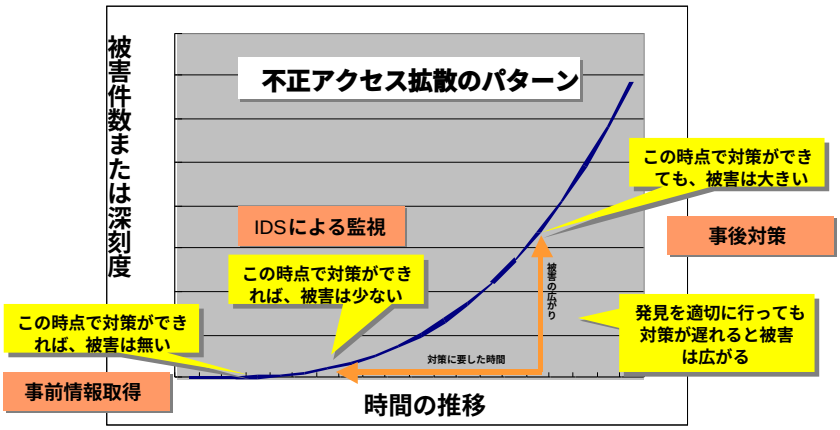
IDS とは **I**nstruction **D**etection **S**ystem の略称で、一般的に「侵入検知システム」と訳されており、コンピュータシステムやネットワークに起こるイベントを監視し、セキュリティ上問題となる兆候や行為を検出するものであり、近年のインターネットの普及とそれに伴うセキュリティ意識の向上により注目度が高まっている。

研究課題としては 20 年ほどの歴史を持っており、元々は記録されたログの監査システムを起源とするが、1990 年代はじめ頃にはネットワーク上を流れるパケットを監査対象とするタイプの IDS も生まれた。1990 年代終わり頃には、ホストベースの IDS とネットワークベース IDS の機能を併せ持つ IDS も出現している。

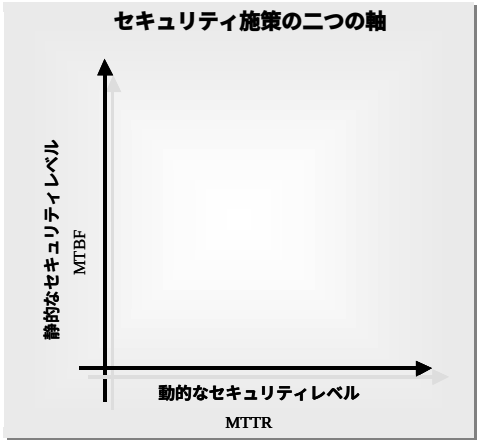
IDS の監視対象は、TCP/IP ネットワークに限定されるものではないが、このドキュメントでは、IDS を“ TCP/IP ネットワークにおける不正侵入を監視するシステム ”に限定して取り扱う。

ネットワークセキュリティにおける IDS の位置付け

不正アクセスによる被害は、時間と共に増加し、より深刻度を増す傾向にある。この傾向は、ワームによる不正アクセスが増加すると共に、より明確になってきている。
しかしながら、従来のコンピュータセキュリティ施策は、被害を発生させない事を第一の目的としており、不正アクセスが実施された場合の対応については、あまり考慮されていない傾向がある。



セキュリティ施策をシステムの信頼性という観点から見た場合、右図のように考えることができる。
ファィアウォール、暗号化、認証などによる不正アクセスを防止するためのセキュリティ施策を、セキュリティの MTBF(Meantime Between Failures)に関する施策、不正アクセスによる被害が発生した場合の対応の対応に関する施策をセキュリティの MTTR(Mean Time To Repair)に関する施策と考えることができる。



IDS は、基本的にセキュリティ MTTR を向上させる事を主たる目的とした技術と位置付けることができる。(IDS の動的な対応による MTBF の向上については、「ダイナミックディフェンスの概要と適用について」: JNSA を参照いただきたい)

ファイアウォール(パケットフィルタリング)との相互補完性

ファイアウォールはパケットフィルタリングやプロクシ (アプリケーションゲートウェイ)機能によりアクセス制御を行うシステムである。単なるネットワーク層でのアクセスコントロールに留まらず、アプリケーション層の情報からのフィルタリング・詳細な通信ログの取得・認証・暗号化通信等の機能を実装したものが主流になっている。

ファイアウォールは、ルール上許可されていない攻撃に対しては有効に防御を行えるが、ルールで許可しているプロトコルを利用した攻撃や、ファイアウォールを通過しない攻撃に対しては機能しない。

一方 IDS は通信の内容そのものや、通信の結果としてサーバに記録されるログを基に監視するため、ファイアウォールで許可された通信を利用した攻撃も監視することができる。また、IDS を適切に配置することで、ファイアウォールを通過しない攻撃を検出することも可能である。

最近は攻撃を検知した場合ファイアウォールと連携してその通信を遮断する機能を持つ IDS も多い。攻撃元からの通信は自動的に遮断するようファイアウォールのルールを動的に変更することで不正侵入に対する防御策を提供する。

サイト構築においては、セキュリティポリシー上許可する必要のない通信についてはファイアウォールでフィルタリングを行い、許可している通信とファイアウォールを通過しない通信については IDS で不正侵入を監視するというような役割分担が必要になる。

IDS の分類と特徴

IDS への入力（検知ターゲット）

IDS が検知する主なターゲットとして、「不正なパケットを利用した攻撃」、「ユーザの不正な振る舞い」、「システムの状態の変化」を上げることができる。

不正なパケットによる攻撃

・不正なパケットによる攻撃
　　ツールを使った攻撃
　　ワームによる走査/攻撃

一般にイメージされる不正アクセスの多くがこれに属する。攻撃の前兆としてのポートスキャンやアプリケーションの脆弱性を突いたバッファオーバーフロー攻撃がこれにあたる。CodeRed や Nimda 等のワームに感染したサーバからのスキャンが大量に発生し、インターネットのトラフィックに大幅な負荷をかけたという事件は記憶に新しい。特にシグニチャベースの IDS(後述)は、このような通信に特徴のある攻撃の検出を得意とする。

ユーザの不正な振る舞い

・ユーザの不正な振る舞い
　　なりすましユーザからの不正な通信
　　内部の正規ユーザからの不正な通信

ユーザアカウントを不正に取得したクラッカーが攻撃を仕掛けている場合、普段のそのユーザとは異なる振る舞いを行う場合がある。何度も su コマンドを失敗したり、いつもは行わないような時間帯にログインしたりといった具合である。また、正規ユーザであっても管理者権限のパスワードを探すために何度も su コマンドを試みたり、許可されていないディレクトリへのアクセス等の行為は監視する必要がある。

システム状態の変化

・システム状態の変化
　　ファイルの書き換え

リソースの使用状況

設定ファイルの不正な更新やバイナリファイルの置き換え、バックドアの配置などは常に監視する必要がある。またプロクシサーバやメールサーバに普段以上の負荷がかかっている場合、何らかの攻撃やワーム /ウィルスによる被害を受けている可能性があるため、注意する必要がある。

IDS の出力

前述の入力を基に IDS が提供する機能は以下のようなものがある。

基本機能
・システムに対する不正な侵入を検出する
・検出された不正侵入を管理者に通知する
・検出された不正侵入の記録を取る

付加機能
・不正な通信を遮断する
・ファイルやレジストリの復元
・他のアプリケーションとの連携

IDS はリアルタイムにシステムを監視することによって、不正な侵入者によるセキュリティ侵害行為を検知することができる。検出した不正侵入はコンソール表示やメール送信を通して管理者へ通知され、同時に時刻や侵入者の情報がログに記録される。
不正侵入の可能性があるという通知を受けた管理者は IDS に記録されたログを基に侵入元を突き止め警告を発したり、侵入されて不正に操作された可能性のあるサーバを切り離して被害状況を調査する等の対策を取ることができる。
また製品によってはファイアウォールとの連携やリセットパケットの送信により、不正な侵入に関わる通信そのものを遮断する機能を備えたものや、改竄されたファイルの復元機能を備えたものも存在し、より高度な防御を可能としている。

IDS の分類と特徴

現在入手可能な商用の IDS の多くは、ネットワークベース IDS (NIDS) と呼ばれる、ネットワーク監視による侵入発見の方式をとっている。
IDS の方式には、これ以外にも様々なバリエーションがあり、不正アクセス対策を効果的に行うためには、それらの特徴を十分に理解する必要がある。
前述したように、IDS はログ監査システムを起源とし、現在のネットワークベース IDS の登場に至ったわけであるが、それ以前の方式は古いから役に立たないというわけではない。各方式には、それぞれ得意不得意がある。効果的な侵入検知を行うためには、各方式の特徴を知り、目的に応じてそれらを相補的に使う必要がある。
以下では、どこで何を監視するかという観点を「ホストベース/ネットワークベース」で、侵入検出手法の観点を「不正検出/異常検出」で、時間に関する観点を「アクションをおこすまでの時間」で説明する。

ホストベース/ネットワークベース

IDS の種類には、大きく分けて、「ホストベース IDS」と「ネットワークベース IDS」がある。これらの違いを説明するとき、その名前と機能が、直観的につながりにくい点が問題となる。

ホストベースとネットワークベースの分類は、「どこに IDS をしかけるか」ではなく、「何を IDS に入力するか」で分けたものである。
何を IDS に入力して、侵入を監視するか、という観点で大きく分けると、ホスト上の OS やアプリケーションログなどを監視するタイプと、ネットワークを流れるパケットを監視するタイプに分類することができる。
一般的に、前者を「ホストベース IDS」、後者を「ネットワークベース IDS」と呼ぶ。

一方、どこに IDS をしかけるか、という観点でさらにネットワークベース IDS を分けると、ネットワーク全体を監視するタイプと、監視対象ホスト自身で送受信するパケットのみを監視するタイプに分類することができる。
ここでは、前者を「ネットワークに IDS をしかける方法」、後者を「ホストに IDS をしかける方法」と呼ぶことにする。後者は、ネットワークノード IDS (Network-Node IDS) とも呼ばれる。

以上をまとめると、IDS をつぎのように分類することができる。

[何を IDS に入力するかという観点で]

・ネットワークベース IDS (ネットワークベース IDS)
ネットワークを流れるパケットを監視
さらに以下のように分類可能
- ネットワーク全体の監視
- 監視対象ホスト自身で送受信するパケットのみを監視
・ホストベース IDS (ホストベース IDS)
監視対象ホスト自身で OS, アプリケーションのログなどを監視

[どこに IDS をしかけるかという観点で]

・ネットワークに IDS をしかける方法
- ネットワークベース IDS (ネットワークベース IDS)
ネットワーク全体の監視
・ホストに IDS をしかける方法
- ホストベース IDS (ホストベース IDS)
監視対象ホスト自身で OS, アプリケーションのログを監視
- ネットワークベース IDS (ネットワークベース IDS)
監視対象ホスト自身で送受信するパケットのみを監視
「ネットワークノード IDS (Network-Node IDS)」ともいう。

これを表にすると、以下のようになる。

		しかける場所	
		Network	Host
IDSへの入力	Network Traffic	ネットワーク IDS	ネットワーク・ノー IDS
	System Log		ホストIDS

次に、「どこに IDS をしかけるか」という観点で IDS を分類したときの、それぞれの利点(および欠点)を述べる。

ネットワークに IDS をしかける方法の利点

・低い監視コスト

ネットワークに IDS をしかける方法は、一つの IDS で監視対象ネットワーク全体を監視できるので、導入コストを低くおさえることができる。

一方ホストに IDS をしかける方法では、導入したホストしか監視できないため、全体を監視するには、全ホストに IDS を導入する必要があり、導入コストが高くなる傾向がある。

・監視対象に対する影響が少ない

ネットワークに IDS をしかける方法は、監視対象ネットワークに影響を与えない。

一方ホストに IDS をしかける方法では、監視対象ホストに IDS をインストールするため、OS との相性やパフォーマンスなど、ホストへの影響に注意する必要がある。

・IDS への侵入の可能性が低い

ネットワークベース IDS の場合、その存在自体をネットワークから隠蔽すること（スティルス監視）ができるため、ネットワークベース IDS が侵入を受ける可能性は低い。

これに対し、ホストベース IDS の場合は、監視対象ホストに直接導入することから、監視対象ホストへの侵入は、そのまま IDS への侵入を意味することになる。

ホストに IDS をしかける方法の利点

・多様な監視ソースが利用できる

ホストに IDS をしかける方法は、パケットの監視に加え、監視対象の OS, アプリケーションが出力するログなども監視できるため、より多様な情報から、不正アクセスを発見することができる。

・手法や行為ではなく結果に基づいた監視ができる

システムやアプリケーションのログを基に監視を行うホストベース IDS は、ネットワークベース IDS と異なり、実際に実行された結果に基づいて、判断を行う点に特徴がある。つまり、ネットワークベース IDS は攻撃の手法を監視するのに対し、ホストベース IDS は、攻撃の結果を監視すると考えることができる。このため、暗号化された通信、コンソールやシリアル接続からの直接的な通信、システム管理者が想定していない未知の経路を経由した不正アクセスについても、監視を行うことができる。

最近では無線 LAN が急速に普及しているが、無線 LAN を利用した場合も、ネットワーク IDS で監視することが難しい面がある。特に、ホストそのものに無線 LAN の機能が組み込まれている場合、ネットワーク IDS で監視することはできない。

・監視精度を上げることができる

ネットワークベース IDS は、複数の監視対象を持つため、監視内容の一般化が不可欠であるのに対し、ホストベースIDSは、ネットワークモニタ、ホストベースIDSにかかわらず、多様な監視ソースが利用できる。これに加え、IDS を導入するホストに限定した監視を行うことができることから、精度の高い監視が可能となる。

・高トラフィック下での監視ができる

ネットワークに IDS をしかける方法では、Ethernet Switch などのスイッチング機器を流れるパケットすべてを、一つのミラーポートと一つの IDS で監視することが困難な場合がある。**※1**

一方ホストに IDS をしかける方法は、監視対象ホストが実際に受信したパケットを監視することから、高トラフィック化においても、取りこぼしのない監視を行うことができる。

・暗号化された通信を監視することができる

ネットワークに IDS をしかける方法では、暗号化されたパケットの中身を見ることができないため、SSL や VPN により暗号化された通信に含まれる、攻撃パケットを見つけることは困難である。**※2**

一方ホストに IDS をしかける方法は、上述したように手法によらない監視を行うことができるため、暗号化された通信についても監視を行うことができる。

なお、ネットワークモニタにおいても、パケットを受信して復号化した後に、監視することが可能なものもある。

・直接的な不正アクセスの対処ができる

IDS がホスト上で稼動していることから、改竄されたファイルの復旧や、疑わしいアカウントを停止させるなどの直接的な不正アクセスの対処が可能となる。

*1 スイッチング機器のミラーポートの性能によっては、影響を与えることがあるので注意が必要である。100Base-TX を 5port 持つ Ethernet Switch の通信をすべてミラーするには、単純計算で、100Mbps x 5 port x 2(全二重) で、1000Mbps の通信が可能なミラーポートが必要。

*2 ネットワークに IDS をしかける方法で、SSL で暗号化されたパケットの中身を見るためには、例えば Web サーバの手前に、別途 SSL の暗号化/復号化を行う機器を設置する方法が考えられる。しかし、他の IPsec-VPN や ssh による暗号化通信に対しては、また別のしくみが必要になる。

不正検出/異常検出

侵入のための攻撃をどのような手法で見つけるか、という観点で IDS を分けると、不正検出と異常検出に分類することができる。

1) 不正検出

いわゆるシグニチャマッチングによる、不正な攻撃を検出する手法である。
IDS が監視している情報の中に、あらかじめ登録しておいたシグニチャ(不正な攻撃の特徴情報)と一致するものが含まれているときに、侵入を発見するもので、商用の多くのネットワークベース IDS で、この手法を使っている。
この手法の特徴は、あらかじめ登録しておいた攻撃のみを発見することである。

2) 異常検出

あらかじめ決めておいた、システムの正常状態を基に、そこからのずれを検出することで、侵入を発見する手法である。
この方式の特徴は、不正な攻撃そのものを検出するのではなく、正常な状態からのずれを検出することである。これにより、未知の攻撃を発見することが可能となる。(したがって、不正検出のようなシグニチャは不要)
異常検出手法における、正常状態の決め方には色々な手法があるが、主に次のものがある。

プロファイルによる手法

システムやユーザの正常時のふるまいを、統計的な傾向としてプロファイル化したうえで保存し、実際のふるまいと比較する手法。
状況によって変化するユーザやシステムのふるまいから、いかにプロファイルを作るかがポイントになる。
DoS 攻撃やポートスキャンの検出は、この手法の一つということができる。

厳密な正常状態の定義ができるもの

仕様や運用ルールとして決まっている情報を基に、正常状態を決める手法。
状況によって正常状態が変化しないため、高い確率で攻撃を検出できる。
例えば、禁止されているプロトコルや、起きないはずのイベントを検出することで、侵入を発見する方法をとる。ファイルの改竄検出も、この手法の一つと言うことができる。
複雑なシステムの中で、変化しない正常状態をいかに決めるかがポイントとなる。

不正検出/異常検出の位置付け

不正検出と異常検出の手法の分類に関する一般的な分類について記載したが、シグニチャマッチングによる手法の IDS の中にも、異常検出手法をとりいれているものもあり、IDS を単純に分類することはできない。また、一般的にシグニチャマッチングによる手法は、異常検出手法と相対するものと考えられる事が多いが、必ずしも相対するものとは言えない面がある。

ここでは、不正検出と異常検出、プロファイルによる手法とシグニチャによる手法、という二つの分類方法は、直交した概念であるという考えにもとづき、IDS の新たな分類方法を提案する。

まず、IDS の手法を、表 1 のように定義する。

表 1 IDS の手法の定義

手法の名前	手法の特徴
不正検出(Misuse Detection)	不正パターンに一致することをもって不正と判断
異常検出(Anomaly Detection)	正常パターンからずれることをもって異常と判断
シグニチャベース(Signature-based)	厳密な判断基準(Signature)による手法
プロファイルベース(Profile-based)	幅がある判断基準(Profile)による手法

表 1 の手法による、IDS の分類のマトリックスを書くと、表 2 のようになる。

表 2 IDS の分類

	Misuse Detection/不正検出	Anomaly Detection/異常検出
Signature based	・不正 Signature と一致したとき、不正と判断 ・よくある Signature 方式	・正常 Signature と不一致のとき、異常と判断 ・厳密な異常検出方式 ・不許可のトラフィックや操作の検出など
Profile based	・不正 Profile に近いとき、不正と判断 あまり一般的ではない	・正常 Profile から遠いとき、異常と判断 ・よくある異常検出方式 ・一般的な DoS, portscan 検出, システム負荷の異常検出など

以上の観点を基に、利用する IDS がどこにあてはまるのか調べることで、IDS の機能を整理して理解することができる。

例えば 表 2 から言えることは、異常検出手法にも、シグニチャベースとプロファイルベースの二つの方式がある、ということである。

異常検出手法では、シグニチャは不要と言われることがあるが、例えば「HTTP と FTP 以外はこのネットワークには流れない」という定義は、表1 でいうところのシグニチャであり、このような手法は、シグニチャベースの異常検出であると言うことができる。

異常検出手法におけるシグニチャは、不正検出手法とは違って、世間で新たな攻撃手法が生

まれたことによって、更新する必要はないことが特長である。
一方、監視対象ネットワークの正常状態が、ユーザの都合などで変わったときは、異常検出手法におけるシグニチャやプロファイルを更新する必要がある。

アクションをおこすまでの時間

侵入を発見してから、アクションをおこすまでの時間の観点から IDS を分けると、次の二つに分類することができる。

短時間にアクションを要する監視（アラートによるインシデント対応）

常に侵入を監視し、発見しだい速やかに、管理者への通知や、ファイアウォールの設定変更などの対抗処置を行う。
商用のネットワークベース IDS の多くは、この方法をとっている。

ある程度時間をかける監視（解析・分析によるインシデント対応）

様々な情報を基に、ある程度時間をかけて分析し、関係する一連の攻撃を把握する (侵入相関分析等)。
侵入や攻撃による影響が、どの範囲に及んでいるかを特定し、システムの復旧計画や、セキュリティ対策の見直しに役立てる。
元々の起源であるログ監査システムを広義の IDS と定義すると、多くのログ監査システムがこの部類に該当する。

現状の IDS の抱える問題点

IDS は、不正アクセスを検知する上で、重要な役割を果たすが、運用を行う上で注意を払うべきポイントがある。

ここでは、その代表的なポイントを取り上げる。

false positive と false negative

IDS を利用するにあたって、無視できない問題が誤検知である。誤検知にはフォールスポジティブ（false positive）とフォールスネガティブ（false negative）がある。フォールスポジティブは不正侵入ではない行為を不正と見なして検出してしまうことをいい、逆にフォールスネガティブは不正侵入が行われているにもかかわらずそれを検出できないことをいう。IDS を運用する上で問題になるのがこれらの誤検知である。

フォールスポジティブが高すぎる場合、運用担当者がアラートの多さに鈍感になり、本当の不正侵入に対して正しい対応ができなくなる危険があり、フォールスネガティブが発生した場合には、該当する不正侵入を検知できないことになる。これらの誤検出をいかに低く抑えるかが IDS を運用する上でのポイントになる。

未知の手法に対する防御

現状の IDS は、パケットに対してシグネチャのパターンマッチングを行う不正検出方法が主流になっている。この手法では既知の不正な攻撃に対してはどのような攻撃を受けているのかを容易に知ることができる反面、パターン化されていない未知の攻撃を検出することができない。ツール等の形で広く一般に知られている攻撃に対しては検出が容易であるが、新たに明らかになった特定のアプリケーションのセキュリティホールを突いた攻撃や、日々変種が現れるワームの攻撃は検知が難しい。一方、未知の攻撃に対する検知を可能とする「異常検出」の手法を実装した IDS も存在するが、こちらは「何の攻撃を受けているのか」、「どのような対策を取ればよいのか」を判断しにくいという問題も抱えている。

トラフィックの暗号化

通信の機密性や完全性を保証するための技術であり、SSL, IPSec, PGP, S/MIME など TCP/IP 各層での暗号化技術が実装されている。

パケットを監視する IDS において、SSL 等によりパケットデータが暗号化されている場合は、暗号化されたデータを解析できないため、不正アクセスの検出ができない。

ホストベース IDS による監視システムの構築

「ホストベースの侵入検知」は、ネットワークパケットが、ファイアウォールおよびネットワークベース IDS を通過し、侵入者が目的とするホストに到達した段階で機能することから、3番目の防御ラインと位置付けることができる。
先に述べたように、ホスト上への IDS の組み込み手法は、次の 2 種類に分類されるが、ここでは、ホストベース IDS（ホストモニタ）に関して記載し、ネットワークノード IDS については記載しない。

・ネットワークノード IDS（ネットワークモニタ：Network Monitor）
ホストへ入って来るパケットをモニターする。
ネットワークベース IDS が、ネットワーク上に流れるすべてのトラフィックを入力とするのに対し、ネットワークモニタは、IDS で監視するホストがやり取りするパケットだけを対象とする点が異なる。

・ホストベース IDS（ホストモニタ：Host Monitor：狭義のホストベース IDS)
サーバまたはその他のホスト上で、アクティビティを検査する。ログイン・アクティビィティのモニタリングや OS、ファイルシステム、レジストリ、アプリケーションが変更されると、アラートを発してログに記録する。

主な構築目的

ホストベース IDS を導入するにあたり、次のような構築目的があげられる。

・アカウントの不正利用監視
・権限の不正利用監視
・ファイル改竄検知（システムファイル、コンテンツ）
・その他システム異常の検知

また、不正アクセスの監視という本来の IDS の目的とは外れるが、以下のような目的で利用されることも多い。

・おとり（ハニーポット的な役割）
・研究
・趣味

これらの項目に加えて、不正アクセスにかかわる証拠として、監視ログを残す点も重要な項目としてあげることができる。
不正アクセスの検知を目的とした場合と、上記のような目的でホストベース IDS を利用する場合では、おのずと考え方が違ってくるため、ここでは、不正アクセスの検知を目的とした利用に限定して記載する。
なお、ホストベース IDS は、ネットワークベース IDS と比較すると、異常検知的な意味合いが強いため、ネットワークベース IDS のように、不正アクセスに焦点をあてることは難しい面がある。ここでは、このようなホストベース IDS の特徴を踏まえ、ホストベースを構築と運用にあたって、どのような事を考慮すれば良いかについて記載する。

ホストベース IDS による監視項目

ホストベース IDS（ホストモニタ）は、主にオペレーティングシステムやアプリケーションのログを監視して、不正アクセスを検知する。
ホストベース IDS の主な監視内容として以下の項目をあげることができる。

ファイルの改竄
アプリケーションのログを使った不正侵入検知
アタック（不正アクセス）の検知
システム稼動監視
管理者権限利用の監視
システム環境監視
管理ポリシとの適合性監視
監視環境監視

ホストベース IDS による監視内容

上記監視項目のうち、よく利用される監視項目を以下に記載する。

ファイルの改竄（変更）

本来書込みが行われる事がないファイルに対して、書込みやパーミッションの変更が行われた事を検出する目的で、ホストベース IDS を利用する場合、監視対象とするのファイルとして、以下のものが考えられる。

- Web のホームページ(index.html)
- Web 等のコンテンツディレクトリ
- システムプログラム
- システムファイル
- メールエーリアス
- .login 等の自動的に起動されるファイル
- .rhosts, /etc/hosts.quiv 等のホスト間の信頼関係に関するファイル
- root 実効権のあるファイル（特にスクリプト）

アカウント関連のアクティビティ

不正アクセスを行う場合、アカウントに対する操作が行われる事が多いため、ホストベース IDS による不正アクセス監視においては、アカウントに対する操作をアラートとして上げる必要がある。
アカウントに関連する項目として、以下のものを上げることができる。

- Brute Force（辞書攻撃、総当り攻撃によるアクセス権取得）
- システム管理者アカウントによるログイン
- システム管理者権限の奪取（su）
- アカウントの追加
- パスワードの変更

その他疑わしいアクティビティ

他の疑わしいアクティビティの例として、以下の項目を上げることができる。

- 未知のプロセスの稼動

- 未知のポートに対する Listen
- suid/sgid のセット
- プロセスの異常終了（core dump）
- ネットワークカードのプロミスキャスモード
- モデムの使用
- システムクロックの変更
- CPU の過負荷
- 通常は考えられないプロセス数
- ディスクの使用量の増加

ホストベース IDS の運用

IDS はネットワークベース、ホストベースにかかわらず、多数の正常な項目の中に含まれる異常を検知することが本質である。

いくつものサービスが無差別に稼動しており、誰がどのようにログインするか、いつホスト内で作業するか分からないホストに対して、IDS を導入しても、正常な挙動と異常な挙動を切り分けることは難しい。

たとえば、ユーザのログインを監視する場合においても、誰がログインを許可されたユーザなのか分からないような状態では、正規の挙動であるかを判断することは困難であり、さらに、盗難されたパスワードを使ったログインであることを見抜くことはきわめて難しい。

ファイル改竄を監視場合においても、いつ誰がファイルの更新やメンテナンスを行うかが決まっていない場合、正規の作業と不正アクセス行為を判別することはできない。

どちらの場合も、検出した項目について、毎回確認を取ればよいと考えることもできるが、このようなアプローチを取った場合、監視側ばかりでなく運用側に対する負担も無視できないものとなる。

また、このような状態が続いた場合、緊張感が薄れ、確認作業に漏れやミスが発生する可能性が高くなり、本当に危険な状況を見逃す事につながってしまう。つまり、「異常な状態をほとんど起こさない環境」を構築することが、IDS による不正アクセス監視を効果的に行う上での最も重要なポイントとなる。特に、ホストベース IDS の場合は、システム運用と密接な関係があるため、ネットワークベース IDS による監視に比べ、より高い精度で実現する必要がある。

ホストベース IDS 導入条件

ホストベース IDS は、ネットワークベース IDS と異なり、ホストで稼動している業務や、運用に対して影響を与える可能性がある。ホストベース IDS を適切に構築し、運用するためには、ホストの利用目的や運用内容を的確に理解し、ホストの運用業務を行う部門・担当者との十分な相互理解が不可欠といえる。

以下に、ホストベース IDS を導入し適切に運用するためのポイントとなる点を記載する。

・監視目的の明確化

どのようなセキュリティ対策ソフトウェアにもよく言われているように、ホストベース IDS を利用することで、セキュリティ上のすべての問題が解決することはありえない。

導入の目的を明確にし、ホストベース IDS でカバーする領域、カバーできない領域を明確にした上で、カバーできない領域については他の手段で補うことを考慮した構築と運用を行う必要がある。

・監視対象ホストの適切な運用

ホストベース IDS は OS のログを監視しているため、サーバ上で不用意な操作を行った場合、不正アクセスとして検知されることになる。このような検知が行われた場合、サーバの運用に支障をきたす可能性がある。

また、運用上の日常動作が不正アクセスとして検知されることが続くと、実際の不正アクセスが誤検知に埋もれてしまい、見過ごされてしまう危険がある。

ホストベース IDS を導入するにあたっては、日常的なシステム運用を意識し、システムを実際に運用する部隊との調整を行いながらの構築が必要となる。

特に、アカウント管理や、ホームページ等の更新等の頻繁に変更が行われる可能性のある操作について配慮が必要となる。

・適切なログの運用

ホストベース IDS の監視を行う際には、監視ソースとなるシステムやアプリケーションのログが大量に記録されることになる。これに加えて、ホストベース IDS 自体のログも記録されるため、HDD が逼迫することが多い。

ホストベース IDS を導入するにあたっては、ログによる HDD の圧迫を考慮に入れたシステム構成の検討と各種ログに対する適切な管理と運用を行う必要がある。

・適切なセキュリティレベルの構築（要塞化）

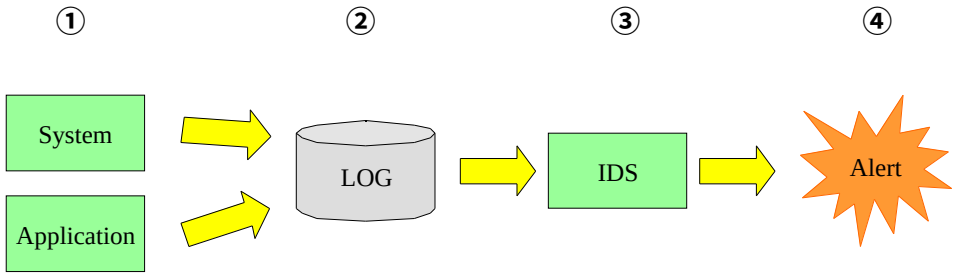
ホストベース IDS の主たる機能は、不正アクセスの防止ではなく、不正アクセスの検知にある。このため、基本的なセキュリティ対策が確立していないホストに対して、ホストベ

ース IDS を使った監視を行っても、セキュリティ施策上のバランスが悪く、コストに見合った成果・効果をあげることは難しい。
また、ホストベースの IDS の場合、ネットワークベースの IDS と異なり、監視ターゲット（ホスト）上で動作するため、ホストへの侵入を受けた場合、検知システムが変更され、二次的な侵入行為が捕らえられなくなる可能性がある。
これらの観点から、ホストベース IDS を導入するにあたっては、監視対象ホストのセキュリティレベルを十分に高める必要がある。

検知の精度向上

IDS を運用する上で、誤検知は避けて通ることのできない問題である。適切な運用を行うためには、できる限り誤検知を低減する必要がある。
前述のように、誤検知には False Positive と、False Negative がある。IDS の運用を行う際には、False Positive を知ることはできるが、False Negative を知ることはできない。このため、本来は、False Negative をいかになくすかが重要となる。しかしながら、ホストベース IDS を使った監視を行うにあたっては、False Positive の対応が監視の成否を分ける側面がある。
このため、ここでは、False Positive / False Negative の双方について考察を行う。

ホストベース IDS の場合は、前述のように、システムやアプリケーションの実行結果に基づいて検知を行うため、ネットワーク IDS とは違ったアプローチが必要となる。
システムやアプリケーションのログを利用してホストベース IDS が稼動する際の一連の流れを図に示す。この図に基づき、ホストベース IDS の基本的な考え方と、False Positive / False Negative 軽減のための手法について記載する。



解析ソースの生成（①−②）について

この図からわかるように、本質的な問題として、ログに適切な記録が行われていない場合、ホストベース IDS は不正アクセスを検知することができない。たとえば、システムのオーディト（監査）機能が適切に設定されていない場合、ファイルの変更記録がログに出力されないため、改竄を検知することはできない。
また、あるアプリケーションでログインの失敗をログに記録していない場合、このアプリケーションを使ったアクセス権取得の試みを検出することはできない。同様にディスクの空きがなくなってしまい、ログを出力できない場合も、IDS は異常や不正アクセスを検知することができない。
つまり、ホストベース IDS を使った不正アクセス監視を行う際には、適切なログを出力することが第一条件となる。

ログの出力が適切に行われない事が原因となり、適切な IDS による監視が行えない例として、IIS(Microsoft Internet Information Server)の例を紹介する。
HTTPS でやり取りをされているパケットは、基本的にネットワーク IDS で解析することができないため、Web サーバのエラーログやアクセスログに対するパターンマッチングを使って、アタックを検出することがある。Apache 等の Web サーバは、アクセスログがほぼリアルタイムでログに出力されるため、この機能を効果的に利用することができる。しかし、IIS を Web サーバとして利用しているケースは、アクセスログがファイルに書き出されるタイミングが限定されているため、リアルタイムで監視を行うことができない。つまり、IIS を使って Web アクセスのログを監視する場合、リアルタイムの監視ではなく、バッチ処理として実行されることになる。

ソースの解析（②−③）について

ホストベース IDS は、システムやアプリケーションの実行結果として記録されたログ（②）に対する監視であるため、正規の行為であるか不正行為であるかにかかわらず、監視項目として定めたものはすべてアラートとして検出することになる。
例えば、ユーザのログインを監視対象とする場合、root や Administrator といった特権ユーザのログインは、正規・不正を問わずに、特権ユーザのログインとして検出することになる。正規のログインと、不正なログインを区別するためには、ログイン失敗の履歴や、どのネットワークからログインを行ったかといったポイントに着目することが必要となる。つまり、ひとつのシグニチャだけで切り分けを行うことは難しく、複数のシグニチャの組み合わせから、正規のアクセスと不正なアクセスを切り分ける必要がある点に注意を払わなければならない。
また、ファイルの改竄についても、ファイルが変更されたことは検知できるが、それが正規の変更であるのか、不正な変更であるかを切り分けるためには、関連するアラートの総合的な判断と、作業の届出に基づいた運用面の判断が必要となる。

一般的に、システムのログに対する異常パターンの検出は、ホストベース IDS の基本機能として組み込まれていることが多い。このため、システムの監視については、組み込みの機能を基にすることで、ある程度対応ができる場合が多い。
ただし、システムの監視においても、シグニチャが相互に関連している場合があるため、必ず検証を行った上で運用を始める必要がある。例えば、繰り返しログインが失敗したことを検知するシグニチャの場合、単純なログインの失敗を IDS に処理をさせないと、このシグニチャは稼動しない(False Negative)。同様に管理者権限の取得に対しても、管理者権限取得の失敗を記録しない限り、繰り返し管理者権限を取得しようとしている動きを捉えることができない点に注意が必要となる。

一方、アプリケーションログを監視する場合、ホストベース IDS の基本機能としては用意されていない場合が多い。このため、アプリケーションのログを監視するためには、利用者が独自に検出パターンを記載する必要がある。
このような利用上の難しさがある反面、ホストベース IDS を使うことで、ユーザが独自に開発したアプリケーションの監視を行うことも可能となる。例えば、基幹業務で利用しているアプリケーションのログから、システムの異常を検知することも可能である。

アプリケーションログを使った監視の精度を向上させる上で、ホストベース IDS がステートレスで稼動するのか、ステートフルで稼動するのかが大きなポイントとなる。
ホストベース IDS が単純なパターンマッチングしか持たない場合（ステートレス）、繰り返し発生するイベントをサマライズした検出（連続したログイン失敗の検出等）を行うことができない。
これに対して、検出の履歴を何らかの方法で記録できる場合（ステートフル）、繰り返し発生するイベントや、一連のイベントの組み合わせを使った、高度な監視を行うことが可能となる。一般的にユーザ定義イベントに対するステートフル監視機能は、何らかの言語を用いてインプリメントされることになるため、アプリケーションログの監視を行う場合は、言語の限界を把握し、機械的な判断を行う領域と、運用上の判断を行う領域を切り分ける必要がある。複雑なプログラミングを行った場合、False Negative の発生が増す可能性がある。

解析結果に基づくアクション（③−④）について

前述のように、ホストベース IDS を使った監視においては、イベント単体で不正アクセスを判断することが難しい面がある。このため、IDS が検出した一連のイベントを、どのように分類（クラス化）するかが、監視を行う上での重要なポイントとなる。
基本的には、以下のアプローチを取る必要がある。

> **システムに対して影響が大きいものは、正規/不正にかかわらず高いレベルでアラートをあげる**
> **上記アラートが発生した際に、問題の切り分けに必要なイベントを、次のレベルのアラートとする**
> **リアルタイムでは判断できないが、疑わしいアクティビティを検出するために必要となる情報を、もっとも低いレベルのアラートとし、後日解析を行う際の基礎データとする。**

なお、監視側の努力だけでは、適切な監視を行う事は難しい。適切にコントロールされた運用下において、初めて適切な監視が可能となる。

アラートが発生した場合の対応

IDS は、種類にかかわらず、不正アクセスを迅速に検知し、被害が発生する前に対処を行うか、被害を最小限にとどめることを目的としている。
この目的を実現するためには、単に IDS を導入するだけでは不十分であり、IDS が不正アクセスを検知した際に迅速な対処が行えるような、運用手順や体制を確立することが必要となる。
ここでは、不正アクセスを検知した際に必要な対処を、フェーズに分けて解説する。

事前準備

インシデント対応を行うにあたっての運用体制を明確にする。
運用体制が決められている場合においても、単なる書面上のもので実際には機能しない事も多いため、実効性のある体制を確保する事が重要となる。
運用体制を構築する際に、調査項目表や報告項目表を作成し、調査・対応内容が確実にエスカレーションされ、記録として残るようにする。
また、システムの通常の動作を理解し、インシデントを検出するための仕組みを適切に設計・実装するとととともに、インシデント対処を行うために必要なログ等を適切に収集し、バックアップを行う必要がある。
なお、ここでは、IDS のアラートがインシデント対応のトリガと想定しているが、実際の運用においては、ユーザや社内からのクレーム、掲示板での情報の発見など、トリガとなる情報ソースが多数存在する。これらのソースに対しても迅速な対応ができるようにすることが重要である。

インシデント確認

教科書通りの言葉になってしまうが、まず「落ち着く」ことが重要である。焦ってし まっては事態をさらに混乱したものにしてしまう可能性がある。
この上で、まずは、「本当に侵入されたのか？」を明らかにする。単純な IDS の誤検知である場合や、正規ユーザの正当な行為がアラートとして検出されている可能性がある。
以下にインシデントを確認する際の一般的な項目を以下に記載する。

ネットワークレベルの確認

- 該当システムおよびサービスの稼動確認と正常性確認

該当サーバおよびサービスが稼動しているのか、停止しているのかを明らかにする。
システムに対する ping による稼動確認、該当サービスに対するアクセスによる稼動確認を行う。
例えば、Web サーバのように、容易にクライアントで確認ができる場合は、クライアントを使って確認する。

クライアントによる確認が難しい場合は、TELNET クライアントを使って、該当サービスに対して接続確認を行う。
例えば Web サーバのように正当性確認が容易である場合は、改竄の調査などの正当性確認を行う。

- 周辺サーバの確認

該当サーバの周辺のサーバが影響を受けている可能性があるため、最低限同一セグメントのサーバに対して、該当サーバと同様の確認を行う。
この段階で、サービスが停止している事が判明した場合、速やかにエスカレーションを行う。

これらの確認作業の多くは、一般的な稼動監視システムにおいて網羅されていることが多い。既に稼動監視システムが導入されているのであれば、稼動監視システムから上記内容を確認することで、いち早く状況を把握することができる。

ホストレベルの確認

システムに残されている侵入痕跡を調べる。まず、現在ログインしているユーザを確認する。/etc/utmp ファイルによるログインしたユーザの洗いだしや、last ログなどによる su の使用状況、who、ps コマンドによる接続元の調査などを行う。また、setuid されたファイルは、管理者権限を容易に取得できる可能性があるため、真っ先にチェックする必要のあるファイルといえる。
なお、後述するようにシステム自体に手を加えられており、これらのコマンドが正しい情報を出力しているとは限らない可能性を考慮する。

侵入に対する暫定対応（一次対応）

侵入が行われた可能性がある場合や、侵入が明らかになった場合には、「関係者への周知と召集」、「重要度確認」、「証拠保全」、「暫定対処」といったタスクを平行して実施する必要がある。
得られた被害状況情報をもとに、コンピュータ資源の安全確保、侵入者の特定、復旧計画などについてどのような方針で以後の対応を進めるかを決定する。
決定した対処方針に基づいて対応を進める。

関係者への周知と召集

侵入された可能性が濃厚な場合には事前に定められた担当者や関係者に連絡をとる。また、事態によって影響を受ける他の管理者やユーザなどにも通知を行う。この際、闇雲に連絡をとると、事態が混乱し収拾が難しくなる場合があるため、誰にどのような連絡を行うかについては、慎重に判断する必要がある。（通常は、対応責任者の判断が必要）

重要度確認

インシデントの重要度・影響度を判断する。
この段階の判断においては、技術的な側面だけではなく、業務面、経営面での重要度を判定する。例えば、技術的に深刻な侵入があった場合でも、業務面に影響がなければ、重要度は低いと判断し、技術的には、さほど重要でない場合においても、業務面に影響をあたえる場合は、重要度は高いと判断する。なお、業務に支障もなく技術的に重要でないとしても、影響範囲が広く復旧に時間を要する場合には影響度は高いと判断できる。

証拠保全

侵入された可能性のある場合には、被害を受けたシステムのコマンドヒストリのコピーを作成し、その後の操作で以前に実行されたコマンドのヒストリが上書されないように処置しておく。コマンドヒストリに限らず、必要なログはできる限り早い段階で、リムーバブルメディア（テープ等）か別のシステムにバックアップを行う。
また侵入に関して法的な処置、あるいは追跡調査のため、発見直後の状態を保存しておく 必要があると考えられる。システムのハードディスクをディスクイメージとして別のメディアに保存するか、ディスクそのものを保管するなどの処置をとることができればなお良い。

暫定対処

システムへの侵入形跡が確認された場合は、被害拡大を防止するため、可能な限りシステムをネットワークから切り離した上で侵入に対応する。情報漏洩や被害拡大の危険性が高い場合はネットワークからの遮断を行うのが望ましい。

侵入元とのコンタクトを行う場合

DoS 攻撃などを継続して受けている場合、攻撃を停止させるためには、攻撃元とのコンタクトが必要となる場合がある。コンタクトを取る際には、相手が悪意を持ったアタッカと断定せず、以下の可能性を考慮にいれて対処する。

- 攻撃元が偽装（スプーフィング）されている
- アタックのように見えるが、正常な通信である
- 機器の故障によりアタックと類似の現象が発生している

また、自社または攻撃元のネットワークにおいて、侵入者による電子メールの盗聴や、他のサーバへ転送されるように設定されている可能性もあるので、これらの連絡は別系統のネットワークがない限り（物理的に切り離されているネットワークを指す）電話、Fax など別の手段を利用が安全である。

インシデントの対処

暫定的な対処により、被害の拡大に対する対策の目処がついた段階で、インシデントの本質的な調査と対応へ移行する。

アタッカが侵入に成功した場合、色々な手段で、その痕跡を隠蔽する。例えば、ログを改竄することで侵入の形跡を隠蔽したり、共有ライブラリを差し替える事で、バックドアツールがコマンドでは見つけられないような処置を行う。調査の段階においては、システムが既にこのような影響を受けている可能性を考慮する必要がある。

被害状況の調査

侵入調査の手法としては、ログに着目する方法と、ファイルの内容等に着目する方法がある。被害の状況を調査する段階においては、これらの手法を効果的に組み合わせる。

改竄されていないことを確認できるシステムやバイナリを用いて、システムの部分復旧あるいは再構築を行う。復旧を開始する前には、バックアップにバックドアや盗聴ソフトが動作している可能性もあるので、以後の調査のために動作中のプロセスを記録する。

コマンドや設定ファイルなどが改竄されていない事を確認するためには、ファイル等のハッシュ値を基に整合性チェックを行うツールを用いて確認するというのも一つの手段である。

要因・侵入経路の分析

調査結果に基づいて、侵入経路を特定する。

侵入にあたっては、踏み台を利用していることが多いため、最終的な犯人を見つけることが難しい面がある。

要因・侵入経路の分析を行うにあたっては、再発を防止するための基礎データを収集することを主たる目的とすることが、二次的被害を防ぐ上で重要な視点となる。

システムの浄化・復旧

調査結果から、システムがどの程度侵入されているかを評価し、部分的に修復を行うのか、システム全体をインストールを行うのか、部分的な対応を行うのかを判断する。

最も確実な方法は、システム全体を再インストールすることであり、影響範囲が特定できない場合は、システムを再構築するべきである。

再発防止策の立案と実施

ワーム等による被害にあった場合は、抜本的な対策を行わないと、繰り返す同じ被害にあうことになる。同じ被害が再発しないような対策を立案し、技術レベル、運用レベルでそれぞれ実装する必要がある。

対策の立案にあたっては、以下の内容を考慮する。

- 同じ手法による侵入を許さないための対策
- 類似の手法による侵入を許さないための対策
- 他の手法で侵入される可能性についての調査と対策

侵入者の分析・特定

各種ログから侵入に関わる情報を抽出する作業を行う。侵入元の特定にあたっては、常に他のシステムが踏み台になっている可能性や、IP アドレスがスプーフィング（偽装）されている可能性があることを考慮に入れる。

ログから得られた情報をもとに、侵入者像を分析し。侵入者に対して法的責任を問うか、どこまで追跡調査するのかを決定する。また、侵入の原因となったセキュリティ上の問題や、侵入者の動機についても分析を行う。

アナウンスおよび届出

被害の内容により、警察等への公的な機関への届出を行うかどうかを判断する。また、顧客に対して影響が出た際には、どのようにアナウンスを行うかを検討し、実施する必要がある。

いずれについても、技術的な視点ではなく、経営・管理面を含めたサイトとしてのリスクコントロールという視点で対応する必要がある。

ホストベース IDS を中心とした IDS の構成

この章ではホストベース IDS を中心とした構成について 考えてみる。
前述のようにホストベース IDS を運用するには、異常な状態をほとんど起こさない環境が構築されており、適切に運用されている必要があるが、仮にそのような状態であれば、インターネットから直接アクセス可能であるか否かを問わず、サービスにおいて重要だと思われるサーバにはインストールすべきであると考える。
しかしながら、ホストベース IDS と他のソフトウェアの相性に問題がある場合や極端にパフォーマンスを気にしなければいけない場合などに関してはこの限りではない。
例えばパフォーマンスについては、ネットワークベース IDS とくらべ使用するリソースが少ないものの、IDS の設定や監査対象とするログなどの出力量によって多少リソースを消費させられるのは否めない。
また、Solaris 対応の商用のホストベース IDS には SunSHIELD BSM を利用してログ解析する製品がいくつかあるが、BSM による監査を有効にするだけでも 5% 程度のパフォーマンスダウンがあると言われており、BSM の監査対象の設定によっては、対象ホストがメインで行っているサービスのパフォーマンスを損なうことがあり得る。
ホストベース IDS によるシステムパフォーマンスの低下が問題となるような場合は、監視対象ホストに影響を与えないと言う特徴を持っているネットワーク IDS を使って監視を行うことが適切と考えられる。

ここで、実際の構成例を考察する前に、もう一度ホストベース IDS とネットワークベース IDS の長所、短所について確認してみる。
一般的な不正侵入の手法をモデルにすると、攻撃者はまずポートスキャンなどで対象のネットワークやサーバの状態を確認する事が多い。アプリケーションログなどを入力情報とするホストベース IDS では TCP コネクションを確立しないステルススキャンと呼ばれるポートスキャンを一般的に検知できないが、ネットワークベース IDS ではこれらの探査活動をモニターすることが可能である。
しかしながら、実際の攻撃であるアプリケーションのバグをついたエクスプロイトを実行した時点では、ネットワークベース IDS ではエクスプロイトが実行されたことを検知できるが、その結果対象ホストに対する攻撃が、成功したのか失敗したのか判断することは難しく、侵入後に攻撃者が対象ホストに対する操作を知ることも困難である。これに対し、ホストベース IDS の場合、システム内で稼動することから、攻撃の成否やその後の侵入行為の追跡などを行うことが可能である。

このようにネットワークベース、ホストベース両方の IDS を配置することによりお互いの限界を補完することが可能で、それぞれの IDS で検知した結果、不正アクセスを総合的に判断した

り、誤検知の判断をしたりすることが可能である。

ホストベース IDS の中にはホストに出入りするパケットも監視するハイブリッド型の IDS も存在し、ネットワークベース IDS が従来から苦手としてきたスイッチングネットワーク環境における監視や IPSec などの暗号化トラフィックの監視などが可能となって来ている。
IDS を使った監視をする際には、これら IDS の特徴と監視対象の制約事項などを加味した上で配置を考える必要がある。

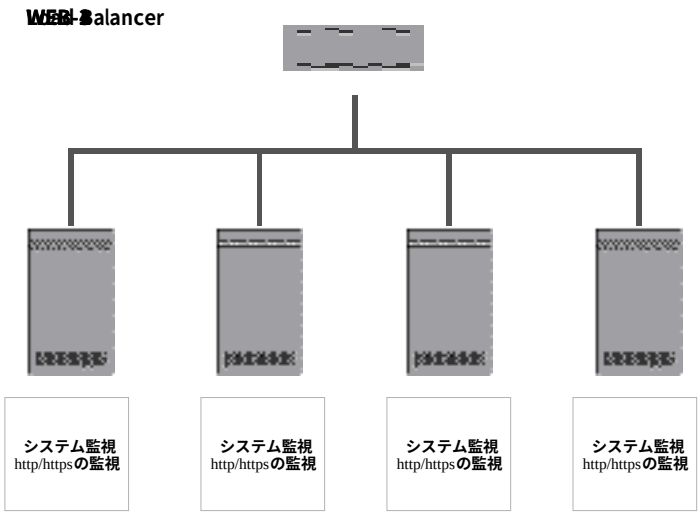
ロードバランシングされた Web サーバへの適用

ネットワークベース IDS でロードバランシングされたサーバに対して監視を行う場合、たとえ不正アクセスを検知したとしても、どのサーバに対してアタックが行われたかを特定することが難しいため、すべてのシステムをしらみつぶしに調べる必要がある。

また、このようなケースでは、大量のトラフィックが処理されていることが多く、ネットワークベース IDS の処理性能限界に達する可能性も高い。

これに対して、ホストベース IDS をそれぞれのサーバに導入した場合、どのサーバに対して不正アクセスが行われたかを、直接知ることができるため、初動を迅速に行うことが可能となる。

また、ロードバランシングするサーバを増加させた場合においても、各サーバで処理するトラフィックは変わらないため、安定した性能を維持することができる。



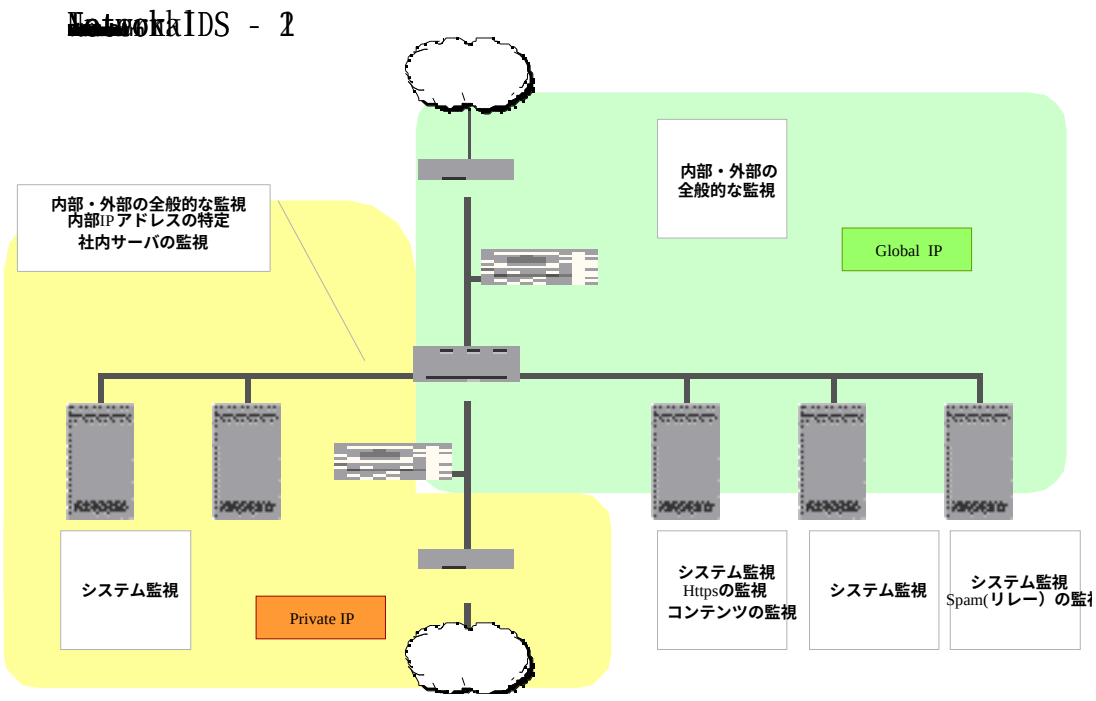
複数の IDS による監視分担の例

企業ネットワークにおいては、社内ネットワークはプライベート IP アドレスで運用し、外部との通信においては、ファィアウォール などでアドレス変換を行っている場合が多い。

この図の Network IDS-1 のように、ルータ直下に ネットワークベース IDS を設置した場合、たとえば社内から外部に対してワームによるアタックが発生した場合に、すべてのソースアドレスがファィアウォールのアドレスとなってしまうため、ワームに感染しているコンピュータを特定することが難しい面がある。このため、この点を補うことを目的として、プライベート IP アドレス領域に別のネットワークベース IDS を設置することがある。

DMZ(公開セグメント)に目を向けると、暗号化が行われていない不正アクセスについては、Network IDS-1 で検出することが可能だが、HTTPS 等の暗号化された通信を監視することができない。この点を補うため、各ホストにホストベース IDS を導入する。

また、このホストベース IDS を適切に設定することにより、各サーバ特有の危険な内容について監視を行うようにすることが可能となる。



最後に

インターネットを中心としたネットワークが、社会活動のインフラストラクチャとしての位置付けられるに従い、ネットワークやサーバの重要性が増している。　その一方で、不正アクセスに関する情報が容易に手に入るようになり、特別な技術や知識がなくても攻撃が実施できるようになっている。

このような状況において、システムの運用とセキュリティ面の双方への対応を求められるシステム管理者の負担は、増加する傾向にある。

今回取り上げたホストベース IDS は、このような状況下にあるシステム管理者に対して、セキュリティ上の対応をある程度自動化し、補助することができる。逆の言い方をすれば、このような仕組みがない環境で、セキュリティ面を含めたシステム管理を行うことは、事実上不可能であると言える。

このドキュメントにおいて記載したように、ホストベース IDS は不正アクセスに対する特効薬ではない。しかしながら、機能と限界を適切に把握し構築・運用を行うことで、効果的なセキュリティ管理を行うことが可能である。また、仮に最適な IDS の設定が行えないとしても、ホストベース IDS の導入は、システムがどのように稼動しているのかを理解する大きな助けとなる。

このドキュメントを、それぞれのサイトにおけるセキュリティ技術の向上に利用していただければ幸いである。

JNSA　IDS ワーキンググループ

新日鉄ソリューションズ（株）	武井 辰徳
	圓田 哲也
	寺島 弘明
インターネット総合研究所	佐藤　友治
横河電機(株)	武智 洋
	清水 孝祥
	田中 貴志
	星野 浩志
（株）ラック	岩井 博樹
	谷田　総生
インターネットセキュリティシステムズ（株）	高橋　正和