National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-94

侵入検知および侵入防止システム（IDPS）に関するガイド

米国国立標準技術研究所による勧告

Karen Scarfone
Peter Mell

この文書は下記団体によって翻訳監修されています

IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
NRI SECURE TECHNOLOGIES

NIST Special Publication 800-94

侵入検知および侵入防止システム（IDPS）に関するガイド

米国国立標準技術研究所による勧告

Karen Scarfone
Peter Mell

コンピュータ セキュリティ

米国国立標準技術研究所
情報技術ラボラトリ
コンピュータセキュリティ部門
Gaithersburg, MD 20899-8930

2007 年 2 月

米国商務省　長官

Carlos M. Gutierrez

技術管理局　技術担当商務次官

Robert C. Cresant

米国国立標準技術研究所　所長

William Jeffrey

コンピュータシステム技術に関する報告書

米国国立標準技術研究所（NIST：National Institute of Standards and Technology、以下、NIST と称する）の情報技術ラボラトリ（ITL：Information Technology Laboratory、以下、ITL と称す）は、国家の測定および標準基盤において技術的リーダーシップを提供することにより、米国の経済と公共福祉に貢献している。ITL は、テスト、テスト技法、参照データの作成、コンセプト実証のための実装、技術的分析を行い、情報技術の開発と生産的利用の拡大に努めている。ITL の責務は、連邦政府のコンピュータシステムにおいて費用対効果の高いセキュリティと取り扱いに注意を要する非機密扱い情報のプライバシを確保するための、技術的、物理的、および管理的標準とガイドラインを策定することにある。NIST Special Publication 800 シリーズでは、コンピュータセキュリティにおける ITL の調査、ガイダンス、成果を報告し、産業界、政府機関および教育機関との共同活動についても報告する。

米国国立標準技術研究所、Special Publication 800-94
米国国立標準技術研究所、Special Publication 800-94, 127 頁（2007 年 2 月）

謝辞

本書執筆陣である Karen Scarfone および Peter Mell（ともに NIST）は、本書草稿のレビューと技術内容に助言を与えてくれた同僚に感謝の意を表したい。まず、John Connor、Tim Grance、Anoop Singhal、Murugiah Souppaya（4 人ともに NIST）、Michael Gerdes、Ralph Martins、Angela Orebaugh、Mike Zeberlein（4 人ともに Booz Allen Hamilton）、および Steve Sharma（Project Performance Corporation）は、本書の作成全体にわたって、鋭く洞察に満ちた助言を与えてくれた。とりわけ Rebecca Bace（KSR）には、本書の入念なレビューと、既刊の NIST Special Publication 800-31『Intrusion Detection Systems』における功績に深い感謝を捧げる。また、特に貴重な意見や提案を寄せてくれたセキュリティ専門家の Andrew Balinsky（Cisco Systems）、Anton Chuvakin（LogLogic）、Jay Ennis（Network Chemistry）、John Jerrim（Lancope）、Kerry Long（Center for Intrusion Monitoring and Protection, Army Research Laboratory）ならびに、国務省および Gartner の代表の方々にもお礼を述べたい。この他の謝辞は、本書の正式版において加えさせていただくことにする。

商標

目次

付録

図

表

要旨

侵入検知とは、コンピュータシステムまたはネットワークに発生するイベントを監視し、それらを分析することによって、インシデントと考えられる兆候を検知するプロセスである。このインシデントとは、コンピュータのセキュリティポリシー、利用規定、標準セキュリティプラクティスに対する、違反または差し迫った違反の脅威を意味する。侵入防止とは、侵入検知を実施し、検知したインシデントと考えられるイベントを阻止することを試みるプロセスである。侵入検知および侵入防止システム（IDPS：Intrusion Detection and Prevention System）1は、インシデントと考えられるイベントを特定し、それらに関する情報をログに記録し、それらの阻止を試み、また、それらについてセキュリティ管理者に報告することを主な目的とするが、セキュリティポリシーに関する問題の特定、既存の脅威の文書化、個人のセキュリティポリシー違反抑止などといった別の用途にも使用される。ほとんどあらゆる組織にとって、IDPSはセキュリティインフラストラクチャに必要な追加要素となっている。

通常、IDPS は、観測したイベントに関連する情報の記録、観測した重要なイベントについてのセキュリティ管理者への通知、および報告の生成を行う。また、検知した脅威に対応して、それが成功するのを阻止するよう試みる機能を備えるものが多い。対応のためのテクノロジーとしては、IDPS によって攻撃自体を阻止する方法や、セキュリティ環境に変更を加える方法（ファイアウォールの設定変更など）、または攻撃の内容に変更を加える方法などいくつかの種類がある。

この文書では、各種 IDPS テクノロジーの特徴を説明し、それらを設計、導入、構成、保護、監視、保守する場合における推奨事項を示す。IDPS テクノロジーの種類を区別する最も大きな違いは、監視の対象とするイベントの種類と、テクノロジーの導入方法である。この文書で説明する IDPS テクノロジーは、次の 4 種類である。

- ネットワークベース：特定のネットワークセグメントまたはネットワーク装置のネットワークトラフィックを監視し、ネットワークプロトコルおよびアプリケーションプロトコルの活動を解析して疑わしい活動を特定する。
- 無線：無線ネットワークのトラフィックを監視および解析し、無線ネットワークプロトコル自体に関わる疑わしい活動を特定する。
- NBA（Network Behavior Analysis：ネットワーク挙動解析）：ネットワークトラフィックを検証し、通常と異なるトラフィックフローを生成する脅威を特定する。これにより、DDoS（Distributed Denial of Service：分散型サービス妨害）攻撃、特定の種類のマルウェア、およびポリシー違反（たとえば、クライアントシステムから他のシステムへのネットワークサービス提供）などを検知する。
- ホストベース：単一のホストの特性と、そのホストの内部で発生するイベントを監視し、疑わしい活動を特定する。

連邦政府の省庁および機関における IDPS 利用の効率と効果を高めるには、次に示す推奨事項を実施することが有効と考えられる。

---

[1] 侵入検知システム（IDS：Intrusion Detection System）は、侵入検知プロセスを自動化するソフトウェアである。侵入防止システム（IPS：Intrusion Prevention System）は、侵入検知システムのすべての機能に加え、インシデントと考えられるイベントを阻止することを試みる機能を備えたソフトウェアである。IDS テクノロジーと IPS テクノロジーは共通の機能を多く備えており、IPS 製品は通常、管理者の都合により侵入防止機能を無効にして IDS として使用することもできる。そこで、この文書では以降、記述を簡略にするため IDS テクノロジーと IPS テクノロジーの両方を総称して「侵入検知および侵入防止システム（IDPS）」と呼ぶことにする。

すべての IDPS 構成要素が正しくセキュリティ保護される状態を確保する

IDPS はしばしば攻撃の標的になるため、その構成要素を保護することは非常に重要である。攻撃者が IDPS を狙うのは、攻撃を検知されないようにするため、または、取り扱いに注意を要する IDPS 上の情報（ホスト構成、既知の脆弱性など）にアクセスするためである。IDPS は、センサーまたはエージェント、管理サーバ、データベースサーバ、ユーザ用および管理者用コンソール、管理ネットワークなど、いくつかの構成要素により構成される。そうしたすべての構成要素のオペレーティングシステムおよびアプリケーションを常に最新の状態に保ち、また、ソフトウェアベースの IDPS 構成要素はすべて、脅威に対する守りを強固にすべきである。具体的な保護策のうち特に重要な事項としては、IDPS の個々のユーザおよび管理者ごとに異なるアカウントを作成すること、IDPS の構成要素に対するネットワークアクセスを制限すること、IDPS の管理に関する通信を確実に正しく保護すること（暗号化や、伝送用ネットワークの物理的または論理的な分離）などが挙げられる。管理者は、継続的に IDPS 構成要素のセキュリティを維持し、その一環として、各種構成要素が意図したように機能していることの確認、構成要素に関するセキュリティ問題の監視、定期的な脆弱性アセスメント、IDPS 構成要素の脆弱性への適切な対処、IDPS に対する更新のテストおよび配備などを実行し続けなければならない。また、既存の設定が意図せずに失われることがないように、設定内容のバックアップを定期的に、また更新の適用前に作成することも必要である。

悪意ある活動の検出、防止をより網羅的かつ正確なものとするために、複数種類の IDPS テクノロジーの併用を検討する

4 種類の IDPS テクノロジー（ネットワークベース、無線、NBA、ホストベース）は、それぞれが根本的に異なる情報収集、ログ、検知、防止機能を提供する。イベントの種類によって、特定のテクノロジーでのみ検知可能であったり、特定のテクノロジーによる検知が他のテクノロジーよりも格段に正確であったりと、この 4 種類はそれぞれに異なる長所を備えている。多くの環境では、複数種類の IDPS テクノロジーを併用することなしには堅牢な IDPS ソリューションを実現できない。ほとんどの環境においては、実効性のある IDPS ソリューションを構築するには、ネットワークベースの IDPS とホストベースの IDPS の組み合わせが必須である。また、無線 IDPS テクノロジーは、組織として無線ネットワークの監視を強化する必要がある場合や、不正な無線ネットワークが組織内の施設で使用されることを確実に防ぎたい場合にも必要である。また、NBA テクノロジーは、DoS 攻撃やワーム、その他 NBA が特に優れた検知能力を示す脅威について検知を強化したい場合にも配備できる。IDPS テクノロジーの選定にあたっては、種類ごとの能力の違いやコスト対効果を考慮すべきである。

複数種類の IDPS テクノロジー、または同種テクノロジーの複数製品の使用を計画している場合は、それらの IDPS を統合する必要性の有無について検討する

単一ベンダーの IDPS 製品を複数使用する場合は、直接的な IDPS 統合により、複数製品を 1 つのコンソールで監視および管理することが多い。また、製品によっては相互にデータを共有できるため、分析プロセスの迅速化と脅威の優先順位付けに役立つ場合がある。直接的な IDPS 統合でも、ある IDPS 製品から提供されるデータを別の IDPS 製品で使用できるがその逆は不可能というように、場合によっては統合機能が限定されることがある。間接的な IDPS 統合は、通常、さまざまなセキュリティ関連ログを読み込んでイベントの相関関係を抽出する SIEM（security information and event management：セキュリティ情報およびイベント管理）ソフトウェアを使用して行われる。SIEM ソフトウェアを使用すると、異なるテクノロジーによって複数のログに記録されたイベントを相互に関連付けたり、さまざまなイベントソースのデータを表示したり、IDPS による警報の正確さをユーザが検証する作業を支

援するために他のソースから得た裏付け情報を提供したりと、いろいろな形で IDPS テクノロジーを補強できる。

IDPS 製品を評価する前に、採用する製品が満たすべき要件を定義しておく

対象組織のシステムやネットワークにおける注目すべきイベントを監視できる IDPS 製品を選定するために、評価者は、そのシステムおよびネットワーク環境が持つ特性を理解しておく必要がある。したがって、IDPS の使用により達成することを期待する目標や目的を明確に設定しておくべきである。たとえば、「一般的な攻撃を阻止すること」、「無線ネットワーク装置の構成の誤りを特定すること」、あるいは「組織のシステムおよびネットワークリソースの悪用を検知すること」などといった目標設定が考えられる。IDPS 製品に必要な機能の多くは、セキュリティポリシーによって規定されることになるため、評価者は既存のセキュリティポリシーの内容も確認しておくべきである。それに加え、対象組織が別の組織による監督または検査の対象となるかどうかについても確認し、該当する場合には、監督機関が IDPS あるいはその他特定のシステムセキュリティリソースの使用を義務付けているかどうかを確認する必要がある。さらに、使用可能なリソースの制約についても考慮しなければならない。また、次のような事項について、評価者は具体的な要件セットを定義する必要がある。

- セキュリティ機能：情報収集、ログの記録、検知、防止などについて
- パフォーマンス：最大処理能力およびパフォーマンスに関する特徴などについて
- 管理：設計と導入（信頼性、相互運用性、スケーラビリティ、製品セキュリティなど）、運用と保守（ソフトウェア更新など）、トレーニング、文書化、技術サポートなど
- ライフサイクルコスト：初期コストおよび維持コスト

IDPS 製品を評価する際は、評価対象製品の特性および能力に関するデータを複数の情報源から得ることを検討する

製品に関する一般的な情報源としては、検査機関または実際的な環境での製品テスト、ベンダーから提供される情報、第三者による製品レビュー、および、組織内の個人や別組織に属する信頼のおける個人による IDPS に関するこれまでの経験などがある。外部から提供されるデータは、どのようにして生成されたかについての説明がされていないことが多いため、データを参照する際には、その信頼性を考慮しなければならない。綿密かつ実際的な IDPS テストには、多くのリソースが必要になること、標準的なテストの方法論やテストスイートがないことなど、いくつかの大きな課題が伴うため、実施が現実的でない場合が多い。とはいえ、限定的な IDPS テストを行うだけでも、セキュリティ要件、パフォーマンス、運用および保守機能を評価する目的のためには有用である。

（本ページは意図的に白紙のままとする）

1. はじめに

1.1 作成機関

この文書は、Federal Information Security Management Act of 2002（2002 年施行の連邦情報セキュリティマネジメント法、以下、FISMA と称す）、公法 107-347 に基づくその法的責任を推進するために、米国国立標準技術研究所（National Institute of Standards and Technology、以下、NIST と称す）により作成された。

NIST は、すべての政府機関システムに十分な情報セキュリティを提供するための標準とガイドライン（最小限の要件を含む）を作成する責任を負うが、このような標準およびガイドラインは国家安全保障にかかわるシステムには適用されない。このガイドラインは、行政管理予算局（Office of Management and Budget、以下 OMB と称す）の通達（Circular）A-130 の第 8b（3）項『政府機関の情報システムの保護（Securing Agency Information Systems）』の要求事項と一致しており、これは A-130 の付録 IV「重要部門の分析（Analysis of Key Sections）」で分析されているとおりである。補足情報は、A-130 の付録 III に記載されている。

このガイドラインは、連邦政府機関による使用を目的として用意されたが、非政府組織が自己責任において使用することもできる。その場合は出自を明らかにすることが望ましいが、著作権の制約はない。

この文書におけるいっさいは、商務長官が法的権威に基づき連邦政府機関に対して義務付け、拘束力を有する標準およびガイドラインを否定するものではない。また、これらのガイドラインは、商務長官、行政管理予算局長、または他のすべての連邦政府当局者の既存の権威を変更したり、これらに取って代わったりするものと解釈してはならない。

1.2 目的と範囲

この文書は、侵入検知システム（IDS）および侵入防止システム（IPS）テクノロジーの理解を助け、組織における侵入検知および侵入防止システム（IDPS）の設計、導入、構成、セキュリティ保護、監視、および保守作業を支援することを目的とする。ネットワークベース、無線、NBA（ネットワーク挙動解析）、およびホストベースという IDPS 製品の 4 分類それぞれについて、実用的かつ現実的なガイダンスを示すものである。また、SIEM（セキュリティ情報およびイベント管理）ソフトウェア、ネットワークフォレンジック分析ツールなど、侵入の検知に使用できる補助テクノロジーについても概要を示す。この文書の記述は主として複合的な組織向け（エンタープライズ向け）の IDPS ソリューションを念頭におくが、大半の内容は、スタンドアロンおよび小規模配備の IDPS にも適用可能である。この文書は、従来の NIST Special Publication 800-31（SP 800-31）『*Intrusion Detection Systems*』を置き換えるものである。

1.3 対象とする読者

この文書は、コンピュータセキュリティのスタッフ、プログラム管理者、コンピュータセキュリティインシデント対応チーム（CSIRT：computer security incident response team）、システム管理者、ネットワーク管理者など、IDPS テクノロジーの管理または監視を担当する人々を対象として作成されている。読者が IDPS テクノロジーに関する経験を有することは前提としないが、情報セキュリティに関する経験を有することを前提とする。

1.4 構成

この文書のこれ以降の内容は、次の 9 つの主要セクションで構成されている。

- セクション 2 では、侵入検知および侵入防止に関する基本的な概念について説明する。
- セクション 3 では、IDPS テクノロジーの概要として、一般的な構成要素、検知の一般的な方法論、および、導入と運用に関するガイダンスを示す。
- セクション 4～7 では、各種の IDPS テクノロジーについて次のとおり詳細に説明する。
  - セクション 4：ネットワークベース
  - セクション 5：無線
  - セクション 6：NBA（ネットワーク挙動解析）
  - セクション 7：ホストベース
- セクション 8 では、IDPS の能力を有するその他のテクノロジーについて述べる。
- セクション 9 では、1 つの複合的な組織（エンタープライズ）内で複数の IDPS テクノロジーを併用および統合する場合の推奨事項を示す。
- セクション 10 では、IDPS 製品の選定に関するガイダンスを示す。

また、付録には参考情報を掲載している。付録 A および B には、それぞれ、用語集および略語の一覧を示す。付録 C には、IDPS について理解をさらに深めるために役立つ印刷物やオンラインツールおよびリソースの一覧を示す。付録 D には、この文書の索引を示す。

2. 侵入検知および侵入防止の原則

*侵入検知*とは、コンピュータシステムまたはネットワークに発生するイベントを監視し、それらを分析することによって、インシデントと考えられる兆候を検知するプロセスである。この*インシデント*とは、コンピュータのセキュリティポリシー、利用規定、標準セキュリティプラクティスに対する、違反または差し迫った違反の脅威を意味する。インシデントの原因はさまざまである。たとえば、マルウェア（ワーム、スパイウェアなど）、攻撃者によるインターネットからシステムへの不正なアクセスの他、システムの正当なユーザによる特権の悪用、あるいは正当なユーザによる、与えられた権限以上の追加的な特権の獲得の試みなどがある。インシデントの多くは本来悪意によるものであるが、そうでないものも少なくない。たとえば、ユーザがコンピュータのアドレスの入力を誤り、偶然に許可のないシステムへの接続を試みることがある。

侵入検知システム（IDS：Intrusion Detection System）は、侵入検知プロセスを自動化するソフトウェアである。*侵入防止システム*（IPS：Intrusion Prevention System）は、侵入検知システムのすべての機能に加え、インシデントと考えられるイベントを阻止することを試みる機能を備えたソフトウェアである。このセクションでは、以降の内容に関する基礎知識として、IDS および IPS テクノロジーの概要を説明する。まず始めに、両テクノロジーの可能な用途について説明し、次に、両テクノロジーの提供する主要機能と、検知に使用されている方法論について述べる。最後に、IDS および IPS と呼ばれるテクノロジーの主要な分類について概要を説明する。

IDSテクノロジーとIPSテクノロジーは共通の機能を多く備えており、管理者は通常、IPS製品の侵入防止機能を無効にしてIDSとして使用することができる。そこで、この文書ではこれ以降、記述を簡略にするためIDSテクノロジーとIPSテクノロジーの両方を総称して「*侵入検知および侵入防止システム（IDPS）*」と呼ぶことにする[2]。例外については随時述べる。

2.1 IDPSテクノロジーの用途

IDPSの主目的は、インシデントと考えられるイベントを特定することである。たとえば、システムの脆弱性を悪用して攻撃者がシステムの侵害に成功した場合、IDPSはそのことを検知する。その後、IDPSはこのインシデントをセキュリティ管理者に報告する。これを受けて、セキュリティ管理者はインシデントによる被害を最小限にとどめるべく、迅速にインシデント対応行動を開始する[3]。IDPSは、インシデント対応担当者の参考になると考えられる情報をログに記録することもできる[4]。また、セキュリティポリシー違反を認識するように設定することができるものも多い。たとえば、一部のIDPSはファイアウォールのルールセットの設定と同様の設定にすることができ、それを使用することで、組織のセキュリティポリシーや利用規定に違反するネットワークトラフィックを識別できる。また、IDPSによっては、ファイル転送を監視し、疑わしいと考えられる転送操作（大規模なデータベースをユーザのノートPCにコピーするなど）を特定できるものもある。

---

2 これは、この文書における便宜のために使用する用語であり、セキュリティコミュニティで広く通用するものではない。この用語をこのように使用する目的は、記述の簡略化のみであり、すでに定着している「IDS」および「IPS」の用語を置き換える意図はない。

3 IDPS が攻撃の阻止に成功した場合でも、セキュリティ管理者は攻撃があったことの通知を受け取る必要があると考えられる。特に、攻撃対象に既知の脆弱性があり、それが悪用された可能性がある場合はこのことが重要である。攻撃者が同じ脆弱性を対象に異なる攻撃を行うことも考えられ、それが IDPS によって認識されるとは限らないからである。

4 インシデント対応の詳しい説明は、この文書の対象外である。効果的なインシデント対応体制の確立に関するガイダンスは、NIST SP 800-61『*Computer Security Incident Handling Guide*（コンピュータセキュリティインシデント対応ガイド）』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

多くの IDPS には、間もなく行われる攻撃の前兆と考えられる偵察活動を特定する能力も備わっている。たとえば、ある種の攻撃ツールやマルウェア（特にワーム）は、本番の攻撃に先立って、攻撃目標を特定するために、ホストおよびポートスキャンなどの偵察活動を行う。そうした偵察活動を IDPS で阻止し、セキュリティ管理者に知らせれば、その他のセキュリティ管理策に必要に応じた変更を加えることで関連インシデントを回避できる可能性がある。偵察活動は、インターネット上で非常に頻繁に行われているため、偵察活動の検知は、主に保護されている組織内ネットワークにおいてしばしば使用される。

IDPS は、インシデントの特定およびそれに伴うインシデント対応活動の支援だけでなく、組織において次のような用途に使用されている。

- **セキュリティポリシーの問題の特定**：セキュリティポリシーの実施状況について、IDPS を使用してある程度の品質管理を行うことができる。たとえば、ファイアウォールと同じルールセットを設定し、ファイアウォールによって本来ブロックされるべきネットワークトラフィックが、ファイアウォールの設定エラーのためにブロックされていない場合に警報を発することができる。
- **組織が直面する既存の脅威の文書化**：IDPS で脅威が検知されると、それに関する情報がログに記録される。組織のコンピュータリソースが実際に受けている攻撃の頻度や特性を知ることは、リソースの保護にどのようなセキュリティ対策が必要かを的確に認識するために役立つ。また、組織が直面している脅威についてマネジメント層を教育するためにもこの情報が有用である。
- **個人のセキュリティポリシー違反抑止**：IDPS によって行動が監視されていることを意識させれば、各個人は自分のセキュリティポリシー違反行為が検知されるリスクを考慮して、違反行為におよぶ可能性が小さくなる。

情報システムに対する依存度がますます大きくなり、システムへの侵入が広範囲で発生していることと、侵入された場合の潜在的な影響の大きさから、ほとんどあらゆる組織にとって、IDPS はセキュリティインフラストラクチャに必要な追加要素となっている。

2.2 IDPSテクノロジーの主要機能

IDPS テクノロジーにはさまざまな種類があるが、それらの最も大きな違いは、認識できるイベントの種類と、インシデントを特定するための方法論である。あらゆる種類の IDPS テクノロジーは、イベントを監視および解析し、望ましくない活動を識別することに加え、次のような機能を備えている。

- **観測したイベントに関連する情報の記録**：情報は、通常ローカル環境に記録されるが、場合によっては、集中化ログサーバ、SIEM（セキュリティ情報およびイベント管理）ソリューション、エンタープライズ管理システムなど、別のシステムに送信される場合もある。
- **観測した重要なイベントのセキュリティ管理者への通知**：この通知は警報（アラート）とも呼ばれる。通知には、電子メール、ページャ、IDPS ユーザインタフェース上のメッセージ、SNMP（Simple Network Management Protocol）トラップ、syslog メッセージ、ユーザ定義のプログラムまたはスクリプトなど、いくつかの手段が使用される。多くの場合、通知メッセージにはイベントに関する基本的な情報しか含まれていないため、管理者が詳細情報を確認するには IDPS にアクセスする必要がある。
- **報告書の生成**：報告書には、監視対象イベントの概要や、注目すべき特定のイベントについての詳細情報が含まれる。

一部の IDPS は、新しい脅威を検知した場合に IDPS 自体のセキュリティプロファイルを変更する機能も備えている。これにより、たとえば、あるセッション内で悪意のある活動を検知した場合、以降は当該セッションについて通常よりも詳細な情報を収集することができる。また、特定の警報がトリガされた場合のための設定内容や、特定の脅威が検知された場合にそれ以降の警報に割り当てるべき優先度などを、IDPS が変更することもある。

IDS テクノロジーと IPS テクノロジーの違いは、検知した脅威に対応して、それが成功するのを阻止するよう試みる機能が備わっているかどうかであり、その機能を備えたものが IPS と呼ばれる。脅威への対応の方法はいくつかあるが、それらを分類すると次のようになる。

- **IPS が攻撃自体を阻止する**：これがいかにして行われるかについての例を次に示す。
  - 攻撃に使用されているネットワーク接続またはユーザセッションを終了させる
  - 攻撃者のユーザアカウントや IP アドレスあるいは他の攻撃者属性から標的への（または、標的にされる可能性がある対象への）アクセスを遮断する
  - 標的にされたホスト、サービス、アプリケーション、またはその他のリソースへのアクセスをすべて遮断する
- **IPS がセキュリティ環境に変更を加える**：攻撃を妨害するために、IPS が他のセキュリティ管理策の構成に変更を加える場合がある。たとえば、ネットワーク装置（ファイアウォール、ルータ、スイッチなど）の設定を変更して攻撃者からのアクセスあるいは、標的へのアクセスを遮断したり、標的ホスト上にあるホストベースのファイアウォールに変更を加えて外部からの攻撃を遮断したりするのが一般的である。IPS によっては、ホストに脆弱性が存在することを検知した場合に、パッチの適用を実行できるものもある。
- **IPS が攻撃の内容に変更を加える**：一部の IPS テクノロジーには、攻撃に含まれる悪質な部分を削除または置換して無害化する能力がある。単純な例では、電子メールからマルウェアに感染した添付ファイルを削除し、駆除済みの電子メールを受信者に届ける機能がこれに該当する。より複雑な例としては、IPS が一種のプロキシとして機能し、受信した要求の*正規化*を実行する場合がある。ここで正規化とは、プロキシが要求のペイロードをパッケージ化し直し、ヘッダ情報を廃棄することを意味する。ある種の攻撃は、この正規化プロセスによって排除される可能性がある。

各種の IDPS テクノロジーに共通するもう 1 つの性質は、検知を完全に正確に行うのは不可能ということである。害のない活動が IDPS によって悪意ある活動と誤認されると、*フォールスポジティブ*が発生する。反対に、悪意のある活動が IDPS によって検知されないと、*フォールスネガティブ*が発生する。フォールスポジティブやフォールスネガティブをすべて排除することは不可能であり、ほとんどの場合、いずれか一方の発生を抑えると他方の発生が増える。多くの組織では、フォールスネガティブを減らし、その代償としてフォールスポジティブの増加を受け入れることを選択している。これは、悪意のあるイベントがより多く検知される反面、フォールスポジティブと真に悪意のあるイベントを判別するための分析リソースがより多く必要となることを意味する。検知の正確さを向上させるために IDPS の設定を変更する作業は、*チューニング*と呼ばれる。

ほとんどの IDPS テクノロジーには、よく使用される回避テクニックに対処するための機能も備わっている。*回避*とは、悪意ある活動の効果をそのままに形式やタイミングを変え、その見かけを異なるものにすることである。攻撃者は、回避テクニックによって、攻撃が IDPS に検知されるのを防ごうとする。たとえば攻撃者は、IDPS には認識されないことを期待しながら、標的に届いたあとで認識されることを知っ

た上で、特定の方法を使用してテキスト文字列をエンコードする。ほとんどの IDPS テクノロジーでは、標的において実行される特定の処理を再現することにより、一般的な回避テクニックを克服している。標的において行われる活動を IDPS が同じように「観測」できれば、回避テクニックによる攻撃の隠蔽は概して失敗する。

2.3 一般的な検知方法

IDPS テクノロジーによるインシデント検知には、いろいろな方法が使用される。2.3.1 項～2.3.3 項では、主要な検知方法をシグネチャベース、アノマリベース、ステートフルプロトコル解析の 3 種類に大きく分け、それぞれについて説明する。ほとんどの IDPS テクノロジーでは、検知の幅と正確さを向上するために複数の検知方法を個別にあるいは、統合して使用する。

2.3.1 シグネチャベースの検知

*シグネチャ*とは、既知の脅威に対応するパターンである。*シグネチャベースの検知*は、観測したイベントとシグネチャとを比較してインシデントの可能性を特定するプロセスである [5]。シグネチャの例としては、次のようなものが考えられる。

- ユーザ名「root」による telnet の試みで、組織のセキュリティポリシー違反であるもの。
- 件名が「Free pictures!（無料画像）」、添付ファイル名が「freepics.exe」の電子メール。既知のマルウェア形態の 1 つにみられる特徴
- ステータスコード値 645 のオペレーティングシステムログ項目。当該ホストの監査機能が無効化されたことを示す

シグネチャベースの検知は、既知の脅威に対しては非常に有効であるが、まだ知られていない脅威、回避テクニックにより偽装された脅威、既知の脅威のさまざまな変種に対しては効果を発揮できないことが多い。たとえば、上で挙げた例のように、シグネチャに登録されているマルウェアのファイル名が「freepics.exe」である場合、攻撃者がマルウェアのファイル名を「freepics2.exe」に変更すると、このシグネチャでは検知できなくなる。

シグネチャベースの検知は、単に文字列比較操作を使用して現在の活動単位（パケット、ログ項目など）とシグネチャー覧を比較するだけの最も単純な検知方法である。ネットワークプロトコルやアプリケーションプロトコルを認識することはほとんどなく、複雑な通信については状態を追跡および認識することもできない。たとえば、要求とそれに対応する応答を結び付けられないため、ある特定の Web ページに対する要求の結果として応答ステータスコード 403（要求の処理をサーバが拒否したことを示す）が返されても、その対応関係を認識することができない。また、それまでに行われた要求を記憶しながら現在の要求を処理することもできない。この制約があるため、複数のイベントから構成される攻撃の場合、いずれか 1 つのイベントに明確な攻撃の形跡が含まれていない限り、シグネチャベースの方法では検知できない。

---

[5] シグネチャベースの検知は、*不正検知*とも呼ばれることがあるが、不正を検知する方法はシグネチャだけではないため、この文書では不正検知という用語を使用しない。また、シグネチャベースの検知は、2.3.3 項で説明するステートフルプロトコル解析をも包含する概念として説明される場合もある。この文書の目的上、シグネチャベースの検知の定義にステートフルプロトコル解析を含めないが、他の文書においてはこの点の定義が異なる可能性がある。

2.3.2 アノマリベースの検知

*アノマリベースの検知*は、観測したイベントと、正常とみなされる活動内容の定義とを比較し、重大な逸脱を特定するプロセスである。アノマリベースの検知を行う IDPS では、ユーザ、ホスト、ネットワーク接続、アプリケーションなどについての正常な挙動を*プロファイル*によって表現する。プロファイルは、通常の活動内容の特徴をある一定期間にわたって監視することにより作成される。たとえば、ネットワークのプロファイルに、通常の就業時間帯におけるインターネットとの境界で発生する Web 活動の割合が、平均でネットワーク帯域幅の 13%であるという情報が含まれていたとする。IDPS は、統計的な手法を用いて、現在の活動に見られる特徴と、このプロファイルに関連付けられているしきい値とを比較する。しきい値は、Web 活動の帯域幅が、予期される帯域幅を大幅に上回る場合にそれが検知され、管理者にアノマリの警報が通知されるように設定される。他にも、たとえば 1 人のユーザが送信する電子メールの件数、1 台のホストに対するログインの試みの失敗回数、1 台のホストにおける一定期間内のプロセッサ稼働率のレベルなど、挙動に関するさまざまな属性についてプロファイルを作成することができる。

アノマリベースの検知方法を使用する最大の利点は、未知の脅威の検知に対して非常に有効であることである。コンピュータが新種のマルウェアに感染した場合でも、それによってコンピュータの処理リソースが消費されたり、多数の電子メールが送信されたり、多数のネットワーク接続が開始されたりといった、当該コンピュータについて作成済みのプロファイルと大きく異なる動作が生じれば、アノマリベースの方法による検知が可能である。

最初のプロファイルは、一定期間（通常数日程度、場合により数週間）を経て生成される。この期間は、*トレーニング期間*とも呼ばれる。アノマリベースの検知に使用されるプロファイルには、静的なものと動的なものがある。静的プロファイルは、生成されたあとはそのまま使用され続け、IDPS が新しいプロファイルを生成するように明示的に指示されない限り変更されない。それに対し、動的プロファイルは、新しいイベントが観測されるにつれて常に内容が変化する。システムおよびネットワークは、時を経るにつれ変化するため、それに応じて正常な挙動の目安も変化する。静的プロファイルはいずれ実態に合わなくなるため、定期的に再生成する必要がある。動的プロファイルにはこの問題が生じない反面、攻撃者による回避の試みの影響を受けやすい。たとえば、攻撃者が、悪意のある活動を少量ずつ、間隔をおいて実行し、その量や頻度を徐々に引き上げていくとする。変化の速さが十分に緩やかであれば、悪意のある活動が IDPS には正常な活動内容と判断され、プロファイルに織り込まれる可能性がある。また、IDPS の最初のプロファイルを構築する期間内に悪意のある活動が行われる可能性もある。

悪意ある活動内容を意図に反してプロファイルに織り込んでしまうことは、アノマリベースの IDPS 製品によく発生する問題である（場合によっては、管理者がプロファイルに変更を加え、悪意のものと判明している活動を除外できることもある）。プロファイルの構築に関するもう 1 つの問題として、コンピュータの活動があまりにも複雑な場合には、正確なプロファイルの構築が困難になることがある。たとえば、大規模なファイル転送を伴う特定の保守作業が月に 1 回だけ行われる場合、この活動がトレーニング期間内に発生しない可能性がある。そうすると、月例の保守作業が行われたとき、プロファイルを大幅に逸脱した活動とみなされて警報が発される可能性が大きい。アノマリベースの IDPS 製品は、特に、より多様性に富んだ環境、または、より変化の大きな環境において、プロファイルから大幅に逸脱した正当な活動が原因となって、しばしばフォールスポジティブが多数発生する。また、イベントが複雑であり、多数のイベントが、警報が発生される原因となる可能性があることから、分析担当者にとって、特定の警報が発せられた理由を判断することや警報が正確であり、フォールスポジティブでないことを確認

することが困難な場合が多い。これもアノマリベースの検知技術の使用に際して指摘しておくべき問題の 1 つである。

2.3.3 ステートフルプロトコル解析

*Statef*ステートフルプロトコル解析は、個々のプロトコル状態に関し、無害なプロトコル活動として一般的に受容される内容の定義済みプロファイルと観測したイベントとを比較して逸脱を特定するプロセスである [6]。アノマリベースの検知では、ホストやネットワークごとに固有のプロファイルが使用されるのに対し、ステートフルプロトコル解析では、個別のプロトコルがどのように使用されるべきかおよび、どのように使用されるべきではないかをベンダーが指定した、ベンダーにより作成された汎用的なプロファイルが使用される。ステートフルプロトコル解析の「ステートフル」とは、状態（ステート）の概念を持ったネットワーク、トランスポート、およびアプリケーションプロトコルについて、IDPSがその状態を認識および追跡する能力を備えていることを意味する。たとえば、ユーザがFTPセッションを開始すると、当初そのセッションは未認証状態にある。この状態におかれている未認証ユーザは、ヘルプ情報の表示やユーザ名とパスワードの指定など少数のコマンド以外は実行すべきでない。状態を認識するための重要な要素の 1 つは、要求と応答の対応関係である。ユーザがFTPの認証を試みると、IDPSは対応するレスポンス中のステータスコードを見つけることにより、認証が成功したかどうかを判断する。認証が成功した場合、セッションは認証済み状態に移行し、ユーザは多数のコマンドから任意のものを実行できるようになる。これらコマンドは、未認証状態において実行された場合は疑わしいとみなされ得るものがほとんどであるが、認証済み状態において実行された場合はほとんどが無害と見なされる。

ステートフルプロトコル解析では、予期していないコマンドシーケンス（同じコマンドが何回も連続して実行されたり、先に必要なコマンドが実行されずに、後続のコマンドだけが実行されたりするなど）を識別することができる。状態追跡に関するステートフルプロトコル解析のもう一つの特徴は、認証を行うプロトコルについては、各セッションで使用された認証子を追跡し、疑わしい活動に使用された認証子を記録することができる点にある。これは、インシデントを調査する際に役立つ情報である。IDPS によっては、認証子の情報を使用して、許容される活動内容をユーザの種別や特定ユーザごとに分けて定義できるものもある。

ステートフルプロトコル解析の手法において実行される「プロトコル解析」には、主として、個別コマンドの妥当性チェック（たとえば、引数の長さの最大値と最小値など）が含まれる。あるコマンドが通常は 1 個のユーザ名を引数とし、ユーザ名の最大長は 20 文字であるとすれば、1000 文字の引数が指定された場合は疑わしいと考えられる。長い引数の内容にバイナリデータが含まれていたとすれば、よりいっそう疑わしい。

ステートフルプロトコル解析の手法においては、プロトコルモデルが使用される。それらは通常、ソフトウェアベンダーや標準化機関（Internet Engineering Task Force [IETF]、Request for Comments [RFC] など）により策定されたプロトコル標準に基づいているが、各プロトコルの実装における差異(variance)も考慮されているのが普通である。標準仕様は、プロトコルの詳細に関する定義に不徹底な部分がある場合が多いため、実装には差異が生じる。また、ベンダーが標準に従わなかったり、独自の機能（場

[6] 一部のベンダーは、ある種のステートフルプロトコル解析の実行を意味する DPI（Deep Packet Inspection）という用語を使用する。DPI は、悪意によるものと判定した通信を遮断するファイアウォール機能と組み合わせて提供されていることが多い。これがネットワークベースの活動だけを扱う場合に適した用語であるのに対し、「ステートフルプロトコル解析」はネットワークベースおよびホストベース両方の活動を解析する場合に適切な用語であるため、この文書では「ステートフルプロトコル解析」の用語を使用する。「Deep Packet Inspection」（パケットの深層検査）という表現の意味については、歴史的にもセキュリティコミュニティ内に共通認識が形成されたことはない。

合によっては標準仕様に取って代わる機能）を追加したりする場合も多い。ベンダー独自のプロトコルについては、完全な詳細仕様書を入手できないことが多く、IDPS テクノロジーによって網羅的かつ正確な解析を行うことが難しい場合がある。プロトコルの改訂やベンダーによるプロトコル実装の変更が行われれば、それを反映するために IDPS プロトコルモデルも更新する必要がある。

ステートフルプロトコル解析の手法を用いることの最大の難点は、解析の複雑さや、同時に多数のセッションの状態を追跡することで生じるオーバーヘッドのため、リソースの消費がきわめて大きいことである。また、一般に受容可能なプロトコル動作の特性に反しない攻撃方法（無害の活動を短時間に多数実行することによる DoS 攻撃など）を検知できないことも深刻な問題である。さらに、特定アプリケーションおよびオペレーティングシステムの特定バージョンにおけるプロトコル実装と IDPS で使用されるプロトコルモデルとのあいだに矛盾が発生する場合や、クライアントおよびサーバのそれぞれにおけるプロトコルの各種の実装が相互に通信する際に用いられる方法に矛盾が生じることも考えられる。

2.4 IDPSテクノロジーの種類

IDPS テクノロジーには多くの種類がある。この文書では、監視の対象とするイベントの種類とテクノロジーの導入方法に基づいて、それらの種類を次の 4 グループに分類する。

- **ネットワークベース**：特定のネットワークセグメントまたはネットワーク装置のネットワークトラフィックを監視し、ネットワークプロトコルおよびアプリケーションプロトコルの活動を解析して疑わしい活動を特定する。注目すべきさまざまな種類のイベントを識別することができる。ネットワーク間の境界（境界ファイアウォールまたはルータ、VPN サーバ、リモートアクセスサーバ、無線ネットワークなどの近く）に設置されるのが最も一般的である。セクション 4 に、ネットワークベースの IDPS テクノロジーに関する詳細情報を示す。

- **無線**：無線ネットワークのトラフィックを監視し、無線ネットワークプロトコルを解析して当該プロトコル自体に関わる疑わしい活動を特定する。無線ネットワークのトラフィックによって伝送される、アプリケーション層や上位層ネットワークプロトコル（TCP、UDP など）における疑わしい活動を特定することはできない。監視対象とする組織内無線ネットワークの通信可能範囲に設置されるのが最も一般的であるが、無許可の無線ネットワーク活動が行われている可能性がある場所に設置される場合もある。無線 IDPS に関する詳細情報は、セクション 5 に示す。

- **NBA（Network Behavior Analysis：ネットワーク挙動解析）**：ネットワークトラフィックを検証し、通常と異なるトラフィックフローを生成する脅威を特定する。これにより、分散サービス妨害(DDoS)攻撃、ある種のマルウェア（ワーム、バックドアなど）、およびポリシー違反（たとえば、クライアントシステムから他のシステムへのネットワークサービス提供）などを検知する。組織の内部ネットワークのトラフィックフローを監視するために設置されることが最も多いが、組織のネットワークと外部ネットワーク（インターネット、ビジネスパートナーのネットワークなど）のあいだに発生するフローを監視することができる場所に設置される場合もある。NBA 製品の詳細については、セクション 6 で説明する。

- **ホストベース**：単一のホストの特性と、そのホストの内部で発生するイベントを監視し、疑わしい活動を特定する。ホストベースの IDPS による監視の対象となる特性の例としては、ネットワークトラフィック（当該ホストのみ）、システムログ、実行中のプロセス、アプリケーション動作、ファイルに対するアクセスおよび変更、システムやアプリケーションの設定の変更などがある。一般に公開されているサーバや、機密情報が保存されているサーバなど、重要なホストに設置されるのが最も一般的である。ホストベースの IDPS に関する補足情報は、セクション 7 に示す。

ある種の形態の IDPS は、それ以外と比べてかなり以前から使用されているため、それだけ成熟度が高い。ネットワークベースの IDPS および一部のホストベースの IDPS は、10 年以上も前から商用製品として流通している。NBA ソフトウェアは、やや新しい形態の IDPS であり、DDoS 攻撃の検知を主目的とした製品から発展した部分と、内部ネットワークのトラフィックフローを監視することを目的とした製品から発展した部分を含んでいる。無線テクノロジーは、比較的新しい種類の IDPS であり、無線 LAN（WLAN）の普及と、WLAN および WLAN クライアントに対する脅威の増大に対応して開発されたものである。

2.5 まとめ

侵入検知とは、コンピュータシステムまたはネットワークに発生するイベントを監視し、それらを分析することによって、インシデントと考えられる兆候を検知するプロセスである。このインシデントとは、コンピュータのセキュリティポリシー、利用規定、標準セキュリティプラクティスに対する違反または差し迫った違反の脅威を意味する。侵入防止とは、侵入検知を実施し、検知したインシデントと考えられるイベントを阻止することを試みるプロセスである。侵入検知および侵入防止システム（IDPS：Intrusion Detection and Prevention System）は、インシデントと考えられるイベントを特定し、それらに関する情報をログに記録し、それらの阻止を試み、また、それらについてセキュリティ管理者に報告することを主な目的とするが、セキュリティポリシーに関する問題の特定、既存の脅威の文書化、個人のセキュリティポリシー違反抑止などといった別の用途にも使用される。ほとんどあらゆる組織にとって、IDPS はセキュリティインフラストラクチャに必要な追加要素となっている。

IDPS テクノロジーにはさまざまな種類があるが、それらの最も大きな違いは、認識できるイベントの種類と、発生し得るインシデントを特定するための方法論である。この文書で説明する IDPS テクノロジーは、次の 4 種類である。

- **ネットワークベース**：特定のネットワークセグメントまたはネットワーク装置のネットワークトラフィックを監視し、ネットワークプロトコルおよびアプリケーションプロトコルの活動を解析して疑わしい活動を特定する。
- **無線**：無線ネットワークのトラフィックを監視および解析し、無線ネットワークプロトコル自体に関わる疑わしい活動を特定する。
- **NBA（Network Behavior Analysis：ネットワーク挙動解析）**：ネットワークトラフィックを検証し、通常と異なるトラフィックフローを生成する脅威（DDoS 攻撃、スキャン、特定の種類のマルウェアなど）を特定する。
- **ホストベース**：単一のホストの特性と、そのホストの内部で発生するイベントを監視し、疑わしい活動を特定する。

通常、IDPS は、観測したイベントに関連する情報の記録、観測した重要なイベントについてのセキュリティ管理者への通知、および報告の生成を行う。また、検知した脅威に対応して、それが成功するのを阻止するよう試みる機能を備えるものが多い。対応のためのテクノロジーとしては、IDPS によって攻撃自体を阻止する方法や、セキュリティ環境に変更を加える方法（ファイアウォールの設定変更など）、または攻撃の内容に変更を加える方法などいくつかの種類がある。

IDPS による検知を完全に正確なものにすることは不可能であり、フォールスポジティブ（害のない活動を悪意ある活動と誤認すること）およびフォールスネガティブ（悪意ある活動を認識できないこと）が必

ず発生する。多くの組織では、フォールスネガティブを減らし、フォールスポジティブを増やすようにIDPS をチューニングしているが、そのためには、フォールスポジティブと真に悪意のあるイベントを区別するための追加的な分析リソースが必要となる。ほとんどの IDPS には、よく使用される回避テクニックに対処するための機能も備わっている。回避とは、悪意ある活動の効果をそのままに形式やタイミングを変え、その見かけを異なるものにして IDPS の検知を免れようとすることである。

ほとんどの IDPS では、検知の幅と正確さを向上するために複数の検知方法を個別に、あるいは、統合して使用する。検知方法は、大きく次のように分類される。

- **シグネチャベース**：観測したイベントと既知の脅威のシグネチャとを比較してインシデントを特定する。既知の脅威の検知については非常に高い効果を示すが、未知の脅威、および既知の脅威のさまざまな変種に対しては効果を発揮できないことが多い。複雑な通信については状態の追跡および認識ができないため、複数のイベントからなる攻撃の大半は検知することができない。

- **アノマリベース**：観測したイベントと、正常とみなされる活動内容の定義とを比較し、重大な逸脱を特定する。この方法では、通常の活動内容の特徴をある一定期間にわたって監視することにより作成されるプロファイルを使用する。IDPS は、現在の活動に見られる特徴と、プロファイルに関連付けられているしきい値とを比較する。この方法は、未知の脅威の検知について非常に優れた効果を示す。反面、悪意ある活動内容が意図に反してプロファイルに織り込まれたり、現実のコンピュータ活動を反映できる程度の十分な複雑さをもつプロファイルを作成することができなかったり、フォールスポジティブが多量に発生したりするといった問題がよく発生する。

- **ステートフルプロトコル解析**：個々のプロトコル状態に関し、無害なプロトコル活動として一般的に受容される内容の定義済みプロファイルと観測したイベントとを比較して逸脱を特定する。アノマリベースの検知では、ホストやネットワークごとに固有のプロファイルが使用されるのに対し、ステートフルプロトコル解析では、個別のプロトコルがどのように使用されるべきかおよび、どのように使用されるべきではないかをベンダーが指定した、ベンダーにより作成された汎用的なプロファイルが使用される。状態（ステート）の概念を持ったプロトコルについて、その状態を認識および追跡する能力があるため、他の方法では検知不可能な多くの攻撃を検知することができる。問題点としては、完全に正確なプロトコルモデルの作成が非常に困難または不可能な場合が多いこと、リソースの消費がきわめて大きいこと、一般に受容可能なプロトコル動作の特性に反しない攻撃を検知できないことなどがある。

3. IDPSテクノロジー

このセクションでは、IDPS テクノロジーの概要を示す。ここに示すのは、IDPS 製品のすべての種類に該当する情報である。各種類固有の追加情報については、セクション 4～7 に示す。このセクションでは、最初に IDPS テクノロジーの主要な構成要素を示し、それらの要素の導入に通常使用されるアーキテクチャについて説明する。また、疑わしい活動の特定に使用される方法論を含め、各テクノロジーのセキュリティ機能について概要を説明する。そのあとは、導入および運用に関する推奨事項の詳細を含め、各テクノロジーの管理機能について説明する。

3.1 構成要素とアーキテクチャ

この項では、IDPS ソリューションの主要な構成要素について説明し、それらの構成要素のための最も一般的なネットワークアーキテクチャを示す。

3.1.1 典型的な構成要素

IDPS ソリューションを構成する典型的な要素は、次のようなものである。

- **センサーまたはエージェント**: *センサー*およびエージェントは、活動を監視して分析する。センサーという用語は、ネットワークを監視する IDPS（ネットワークベース、無線、NBA）で使用されるのが普通である。エージェントという用語は、ホストベースの IDPS テクノロジーで使用されるのが普通である。
- **管理サーバ**: *管理サーバ*は、センサーまたはエージェントから送られる情報を受信し、管理する集中化された装置である[7]。一部の管理サーバには、センサーまたはエージェントから提供されたイベント情報を分析することにより、個別のセンサーまたはエージェントが認識できないイベントを特定する能力がある。複数のセンサーやエージェントからのイベント情報の対応付け（同一IPアドレスを発生元とする複数のイベントを見つけるなど）をすることを、*相関*という。管理サーバとして流通している製品には、アプライアンスと、ソフトウェアのみの両方の形態がある。小規模に導入されるIDPSでは、管理サーバをまったく使用しないこともあるが、使用する場合がほとんどである。大規模に導入されるIDPSには、複数の管理サーバが含まれることが多く、場合によっては管理サーバを 2 階層に構成することもある。
- **データベースサーバ**: *データベースサーバ*は、センサー、エージェント、または管理サーバによって記録されるイベント情報を保存するリポジトリである。多くの IDPS は、データベースサーバをサポートしている。
- **コンソール**: *コンソール*は、IDPS のユーザおよび管理者に対するインタフェースを提供するプログラムである。多くの場合、コンソールソフトウェアは標準的なデスクトップコンピュータまたはノート PC にインストールして使用する。コンソールによっては、IDPS 管理専用（センサーまたはエージェントの設定、ソフトウェア更新の適用など）のものや、厳密に監視および解析を行うためだけのものがある。一部の IDPS コンソールは、管理機能および監視機能の両方を備えている。

[7] この文書では、複合的な組織の IDPS の配備について取り上げているため、センサーとエージェントを管理サーバと併せて使用しているものと想定している。しかし、IDPS の一部の種類のセンサーとエージェントは、スタンドアロンで設置し、管理サーバを使わずに、管理者が直接管理したり監視したりできるものもある。

3.1.2 ネットワークアーキテクチャ

IDPS 構成要素相互の接続には、組織の標準ネットワークを使用する場合と、セキュリティソフトウェア管理専用として厳密に設計された別個のネットワーク（*管理ネットワーク*と呼ばれる）を使用する場合がある。管理ネットワークを使用する場合は、個々のセンサーまたはエージェントホストは、*管理インタフェース*と呼ばれる、管理ネットワーク接続用の追加的なネットワークインタフェースを持つ。また、いずれのセンサーまたはエージェントホストも、管理インタフェースとそれ以外のネットワークインタフェースの間でトラフィックをいっさい通過させることができない。管理サーバ、データベースサーバ、およびコンソールは、管理ネットワークにのみ接続する。このアーキテクチャにより、管理ネットワークは、業務用ネットワークから実質的に隔離される。こうした構成のメリットは、IDPS の存在と識別情報が攻撃者から隠蔽されること、IDPS を攻撃から保護できること、および、不都合な状況下（監視対象ネットワークがワーム攻撃や DDoS 攻撃を受けている場合など）でも IDPS が機能するのに十分な帯域幅を確保できることである。反面、管理ネットワークのデメリットとしては、ネットワーク機器やその他のハードウェア（コンソール用 PC など）のコストが増加することと、IDPS ユーザおよび管理者が IDPS の管理や監視に別のコンピュータを使用する必要があるため不便が生じることが挙げられる。

独立の管理ネットワークを使用せずに IDPS を導入する場合に、IDPS のセキュリティを向上させるもう 1 つの方法は、仮想ローカルエリアネットワーク（VLAN）による仮想的な管理ネットワークを標準ネットワーク内に構築することである。VLAN を使用すると IDPS の通信を保護することができるが、独立した管理ネットワークによって提供されるほどの保護効果は得られない。たとえば、VLAN の設定ミスが IDPS データの漏洩につながることなどがあり得る。また、DDoS 攻撃や深刻なマルウェアインシデントなどが発生する状況下では、組織の主ネットワークと VLAN で共用しているネットワーク装置が完全に飽和してしまい、IDPS の可用性とパフォーマンスに悪影響が生じる可能性がある。

3.2 セキュリティ機能

ほとんどの IDPS テクノロジーは、多種多様なセキュリティ機能を提供する能力を備えている。一般的なセキュリティ機能を、ここでは情報収集、ログの記録、検知、および防止の 4 つに分け、それぞれについて3.2.1項～3.2.4項で説明する。

3.2.1 情報収集機能

IDPS テクノロジーによっては、観測した活動内容からホストやネットワークに関する情報を収集する情報収集機能を備えているものがある。たとえば、ホストおよびオペレーティングシステムの特定、そこで使用されているアプリケーションの特定、ネットワークの全般的特徴の特定などが可能である。

3.2.2 ログ記録機能

IDPSは一般に、検知したイベントに関連するデータを詳細なログとして記録する。このデータは、警報の妥当性の確認、インシデントの調査、および、IDPSにおいて検知されたイベントとその他のログ生成ソースにおいて検知されたイベントとの相関をとるのに使用することができる。IDPSでよく使用されるデータフィールドとしては、イベント発生日時、イベントの種類、重要性のレベル（優先度、重大度、影響の程度、確実性など）、実行された防止措置（該当する場合）などがある。これらに加え、IDPSの種類に応じた特有のデータフィールドが付加されることがある（ネットワークベースのIDPSにおけるパケット採取、ホストベースのIDPSにおけるユーザID記録など）。管理者は、IDPSテクノロジーのログをローカルに保存するだけでなく、集中化ログサーバ（syslog、SIEMソフトウェアなど）にログのコピーを送信するこ

とができるのが普通である。一般に、データの完全性と可用性をサポートするため、ログはローカル環境と集中化サーバの両方に保存すべきである（IDPSが侵害された場合など、ログが攻撃者に改変または破壊される可能性がある）[8]。また、ログエントリのタイムスタンプを正確に合わせるために、各IDPSの時計を、Network Time Protocol（NTP）を使用するか頻繁に手動調整して同期させておくべきである[9]。

3.2.3 検知機能

IDPS テクノロジーには、詳細かつ広範な検知機能を備えるものが多い。ほとんどの製品では、検知の正確さとチューニングおよびカスタマイズの柔軟性を向上するために、複数の検知テクニックを組み合わせて使用している。検知されるイベントの種類と、検知の一般的な正確さは、IDPS テクノロジーの種類によって大きく異なる。ほとんどの IDPS では、検知の正確さ、使い勝手、実効性を向上させるために多少のチューニングおよびカスタマイズが必要となる（特定の警報に対応して実行させる防止措置の設定など）。チューニングおよびカスタマイズ機能の内容は、テクノロジーごとに大きく異なる。多くの場合、チューニングやカスタマイズの機能が強力な製品であるほど、検知の正確さをデフォルト設定よりも向上させることができる余地が大きい。製品の評価にあたっては、IDPS テクノロジーがどのようなチューニングおよびカスタマイズ機能を備えているかを注意深く検討すべきである。そうした機能の例を次に示す。

- **しきい値**：*しきい値*は、正常な動作と正常でない動作の境界を指定する値である。たとえば、60 秒間に試行された接続の失敗回数、ファイル名の文字数など、多くの場合は許容する最大値を指定する。しきい値は、アノマリベースの検知およびステートフルプロトコル解析で使用されることが最も多い。

- **ブラックリスト、ホワイトリスト**：*ブラックリスト*は、予め悪意のある活動に関連すると判定されている個別エンティティ（ホスト、TCP または UDP ポート番号、ICMP タイプまたはコード、アプリケーション、ユーザ名、URL、ファイル名、ファイル拡張子など）の一覧であり、*ホットリスト*とも呼ばれる。一般的に、悪意のものである確率が非常に高い活動を IDPS に認識させ阻止させるために使用するが、ブラックリストの項目に対応する警報により高い優先度を割り当てる目的で使用する場合もある。一部の IDPS は、最近検知された脅威（攻撃者の IP アドレスを起点とする活動など）を一時的に阻止するための動的なブラックリストを生成する。*ホワイトリスト*は、無害であることが知られている個別エンティティの一覧である。信頼のおけるホストを起点とする既知の害のない活動に対するフォールスポジティブの発生を抑制または無視するために、通常はプロトコルごとなどの粒度に基づいて使用される。ホワイトリストおよびブラックリストは、シグネチャベースの検知およびステートフルプロトコル解析で使用されることが最も多い。

- **警報の設定**：ほとんどの IDPS テクノロジーでは、警報の個々の種類を管理者がカスタマイズできる。たとえば、警報の個々の種類に対して次のような措置を実行できる。

---

[8] ログ管理の詳細については、NIST SP 800-92『*Guide to Computer Security Log Management*(コンピュータセキュリティログ管理ガイド)』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

[9] NIST SP 800-86『*Guide to Integrating Forensic Techniques into Incident Response*（インシデント対応へのフォレンジック技法の統合に関するガイド）』において、事象の調査および複数システム間で情報の相関をとるために時刻を同期させることの重要性について詳しく説明している。同文書は、http://csrc.nist.gov/publications/nistpubs/ から入手できる。

- 警報のオン／オフの切り替え [10]
- デフォルトの優先度または重大度レベルの設定
- 記録する情報の内容、使用する通知手段（電子メール、ページャなど）の指定
- 使用する防止機能の指定

製品によっては、攻撃により短期間に多数の警報が発生した場合に警報を抑制する機能や、攻撃者から発信される以後のトラフィックを一時的にすべて無視する機能を備えているものもある。これは、IDPS が警報によって飽和状態になるのを防ぐためである。

■ コードの表示および編集：一部の IDPS テクノロジーでは、検知に関連するコードの一部または全部を管理者が参照できる。通常、参照できる範囲はシグネチャに限られるが、他のコード（ステートフルプロトコル解析の実行に使用するプログラムなど）まで参照を許可しているテクノロジーもある。コードを確認できることは、特定の警報が生成された理由を分析担当者が判断するのを助け、警報の妥当性確認とフォールスポジティブの特定に役立つ。検知機能によっては、完全にカスタマイズするには、検知関連のすべてのコードを編集できることと、新規のコード（新しいシグネチャなど）を記述できることが不可欠である。たとえば、続けて発生した複数のイベントが複雑に関係し、いくつものコードモジュールが関与した結果として特定の警報が 1 つ生成されることがある。IDPS に組織固有の特性を認識させるための IDPS のカスタマイズは、コードを直接編集しなければ実現できない場合がある。コードを編集するには、プログラミングおよび侵入検知に関するスキルが必須である。また、IDPS によっては独自のプログラミング言語を採用しているため新しい言語の習得が必要となることもある。カスタマイズ作業によってコードのバグが持ち込まれると、IDPS が正常に機能しなくなったり、まったく動作しなくなったりする可能性があるため、管理者は、コードのカスタマイズについて、その他あらゆる業務システムのコードに変更を加える場合と同様に取り扱いに注意する必要がある。

管理者は、チューニングとカスタマイズの内容を正確に保つために、これらを定期的に見直すべきである。たとえば、ホワイトリストおよびブラックリストを定期的にチェックし、すべての項目について正確さと必要性を確認する。しきい値および警報設定は、環境と脅威の変化に応じて定期的な再調整を行う必要が生じることがある。検知コードが編集された場合には、製品が更新される（パッチ、更新などが適用される）たびに検知コードの複製が必要になる可能性がある。また、アノマリベースの検知を行うためのベースラインを収集する製品については、検知の正確さを保つために、必要に応じてベースラインの再構築を定期的に実行すべきである。

3.2.4 防止機能

ほとんどの IDPS は、複数の防止機能を備えている。その機能の具体的な内容は、IDPS テクノロジーの種類により異なる。通常、防止機能に関する設定は、警報の種類ごとに管理者が指定することができる。設定により指定できる事項には、防止の有効化／無効化の切り替えや、使用する防止機能の種類などがある。また、学習モードまたはシミュレーションモードを備えた IDPS センサーもある。これは、全ての防止措置を抑止し、その代わりに、防止措置が実行されるべき時点でその旨を示すモードであ

[10] 一部の IDPS テクノロジーでは、特定の警報をオフにするとそれに関連する検知機能まで無効になる。そうでない製品では、オフにしても検知プロセスは実行されるが警報メッセージは生成されない。前者に該当するテクノロジーの場合、不要な警報をオフにすることで IDPS の負荷を軽減できる。

る。このようなモードを利用することにより、管理者は防止機能を有効化する前に、監視を行いながら防止機能の設定を微調整することができ、害のない活動を誤って阻止してしまうリスクを低減できる。

3.3 管理

ほとんどの IDPS テクノロジーは、いずれもよく似た管理機能を備えている。この項では、管理の主要な側面（導入、運用、保守）について述べ、それらの作業を効果的かつ効率的に実行するための推奨事項を示す。また、IDPS の管理に必要な技能についても概略を述べ、技能習得のための推奨事項を示す。

3.3.1 導入

IDPS 製品を選定した場合、管理者がアーキテクチャの設計、IDPS 構成要素のテスト、構成要素に対するセキュリティ対策の実施を行った後に、IDPS を導入する必要がある。これらの作業の詳細については、3.3.1.1項～3.3.1.3項で述べる。

3.3.1.1 アーキテクチャ設計

IDPS 導入作業の最初のステップは、アーキテクチャの設計である。アーキテクチャに関しては、次のような考慮事項がある。

- センサーまたはエージェントをどこに配置するか
- ソリューションとしての信頼性がどの程度であるべきか、また、どのような方策によってそれを実現するか。たとえば、センサーの故障に備えて 1 つの活動を複数のセンサーで監視することや、複数の管理サーバを設置して主サーバの故障時には副サーバを使用できるようにすることなど
- 他の IDPS 構成要素（管理サーバ、データベースサーバ、コンソールなど）をどこに配置するか、また、必要な使い勝手、冗長性、負荷分散の目標を達成するにはそれぞれの構成要素がいくつ必要か
- 次のような他のシステムで、IDPS との相互運用が必要なものは何があるか
  - IDPS の提供するデータを受け取るシステム。たとえば、SIEM(security information and event management)ソフトウェア、集中化ログサーバ、電子メールサーバ、ページャシステムなど
  - IDPS の指示を受けて防止措置を開始するシステム。たとえば、ファイアウォール、ルータ、スイッチなど
  - IDPS 構成要素を管理するシステム。たとえば、ネットワーク管理ソフトウェア（管理ネットワーク用）、パッチ管理ソフトウェア（コンソールのオペレーティングシステムとアプリケーションを最新に保つため）など
- 管理ネットワークを使用するかどうか。使用する場合は、それをどのような設計にするか。使用しない場合は、標準ネットワーク上で IDPS の通信をどのように保護するか
- IDPS の導入に合わせて変更を加える必要がある他のセキュリティ管理策およびテクノロジー。たとえば、IDPS 要素間の通信を可能にするために必要なファイアウォールのルールセット変更など

3.3.1.2 構成要素のテストおよび配備

導入上の問題によって業務ネットワークに悪影響が生じる可能性を小さくするために、IDPS の構成要素は最初から実稼働環境に設置するのではなく、まずテスト環境に導入することを検討すべきである。実稼働環境に導入する際には、防止機能を無効化した少数の IDPS センサーまたはエージェントのみを有効にすることから始めるべきである。新しく導入された IDPS では、チューニングおよびカスタマイズが十分に行われるまでに、多数のフォールスポジティブが発生する可能性が大きいため、一度に多数のセンサーまたはエージェントを有効にした場合、管理サーバやコンソールが過負荷になり、チューニングおよびカスタマイズ作業が困難になることがある。他のセンサーまたはエージェントにおいても多数のフォールスポジティブが発生する確率が高いため、テスト実施時あるいは最初の少数のセンサーまたはエージェントの導入時に、そのようなフォールスポジティブを特定することは、それらを解決してから大規模な導入を行う上で役に立つ。センサーまたはエージェントを段階的に導入することは、スケーラビリティに関する潜在的な問題を明らかにするのにも役立つ。

IDPS を導入する際には、その構成要素をインストールするためにネットワークやシステムが一時的に使用できなくなる可能性がある。上述のようにテスト環境に導入することは、導入時に発生しやすい問題を特定し、実稼働環境への導入に際してそれらの問題に適切に対処できるようにするためには、非常に有効である。

アプライアンスベースの IDPS の構成要素は、多くの場合は単純な作業により導入することができる。場合によっては、IDPS のソフトウェアを最新の状態にするために、ソフトウェアやシグネチャの更新を適用する必要があるが、それ以外に管理者が行うべき作業は、一般的には、電源の供給、ネットワークケーブルの接続、アプライアンスの起動、および若干の基本的な設定作業（製品ライセンスキーの入力、センサー名の割り当てなど）である。

ソフトウェアベースの IDPS の構成要素は、アプライアンスベースの構成要素よりも導入に時間を要することが多い。まず、適切なハードウェアの調達が必要である。これには、広帯域ネットワークカードの購入や、ハードウェアの堅牢性が IDPS に用いるのに十分かどうかの確認作業などが含まれる場合がある。次に、使用する IDPS のソフトウェアと互換性のあるオペレーティングシステム（OS）を管理者がインストールし、当該ホストのセキュリティを可能な限り強固にする必要がある。セキュリティ強化作業には、OS、サービス、アプリケーション（IDPS ソフトウェアを含む）の更新作業が含まれる。また、アプライアンスベースの IDPS の構成要素と同様に、IDPS のソフトウェアの基本的な設定作業が必要となる。

アプライアンスベースまたはソフトウェアベースの IDPS の構成要素を導入したあとは、製品の検知機能および防止機能を設定する作業にかなりの手間がかかる可能性がある。必要な作業の内容は、導入する IDPS の種類によって異なる。この設定作業を行わないと、IDPS によっては能力が非常に限定され、以前から知られている検知の容易な少数の攻撃しか検知できなくなる場合がある。

3.3.1.3 IDPS構成要素のセキュリティ保護

IDPS は、しばしば攻撃の標的になるため、その構成要素を保護することは非常に重要である。IDPS が攻撃者に侵害されれば、以後、他のホストに対して行われる攻撃を検知できなくなる可能性がある。また、IDPS には、ホストの設定などの扱いに注意を要する情報や既知の脆弱性が存在することがよくあり、それらがさらなる攻撃の計画立案に利用される可能性がある。ソフトウェアベースの IDPS の構成要素のセキュリティを強固にし、すべての IDPS の構成要素を最新の状態に保つことに加え、管理者

は、IDPS の構成要素自体のセキュリティを適切に保つための追加的な対策を実施すべきである。具体的なセキュリティ上の推奨事項としては、次のようなことが挙げられる。

- IDPS の個々のユーザおよび管理者ごとに異なるアカウントを作成し、各アカウントに対し必要な権限だけを付与する。
- ファイアウォール、ルータ、その他のパケットフィルタ装置などを設定することにより、IDPS の全ての構成要素に対する直接的なアクセスを、そのようなアクセスを行う必要があるホストのみに限定する。
- IDPS管理に関するすべての通信が適切に保護されるようにする。そのために、物理的な分離（管理ネットワークなど）または論理的な分離（管理VLANなど）、あるいは、通信の暗号化を導入する。暗号化による保護を採用する場合は、FIPS承認済みの暗号化アルゴリズムを使用する[11]。多くの製品では通信の暗号化にTransport Layer Security（TLS）が採用されている。暗号化による保護が十分でない製品を使用する場合は、仮想プライベートネットワーク（VPN）またはその他の暗号化トンネリングによるトラフィック保護を検討すべきである。

組織によっては、IDPS の構成要素へのリモートアクセスのために強力な認証を必要とする（2 要素による認証など）。これにより、セキュリティが一段階強化される。

3.3.2 運用および保守

ほぼすべての IDPS 製品は、*コンソール*としても知られているグラフィカルユーザインタフェース（GUI）を使用して運用および保守の作業を実行するよう設計されている。コンソールでは一般に、管理者がセンサーや管理サーバの設定、更新、およびステータス（エージェントの故障、パケットの損失など）の監視を行うことができる。管理者は、他にもユーザアカウントの管理、報告のカスタマイズなど多くの機能をコンソールを使用して実行することができる。IDPS ユーザも、コンソールを使用して IDPS データの監視および解析、報告の生成など多くの機能を実行することができる。ほとんどの IDPS においては、管理者が各管理者およびユーザごとに個別のユーザアカウントを作成し、各人の役割に応じた必要な権限だけをアカウントごとに付与することができる。そのため、コンソールは、最新の認証されているアカウントに指定された役割に基づいて、ユーザごとに異なる内容のメニューやオプションを表示するようになっていることが多い。製品によっては、さらに細かいアクセス制御機能があり、いずれのセンサーやエージェントについて、監視、データの分析、報告の生成ができるかをユーザごとに指定したり、設定変更を特定の管理者に許可したりすることができる。このような機能により、大規模な IDPS の導入を運用上の目的に応じて論理的な単位に細分化することができる。

一部の IDPS 製品には、コマンドラインインタフェースも用意されている。GUI コンソールがセンサー、エージェント、管理サーバのリモート管理に使用されることが多いのに対し、CLI は、こうした構成要素のローカル管理に使用されることが多い。場合によっては、SSH などの手段で確立した暗号化接続によりリモートから CLI を使用できることもある。CLI は、コンソールよりも使いやすさがかなり劣るのが普通であり、また、コンソールにより提供される機能の一部しか使用できないことが多い。

---

[11] 連邦政府機関には、認可された暗号モジュールに含まれている FIPS 公認の暗号化アルゴリズムを使用することが義務付けられている。FIPS テストは、NIST の暗号モジュール検証プログラム（CMVP：Cryptographic Module Validation Program）に一元化されている。CMVP の Web サイトは、http://csrc.nist.gov/cryptval/ にある。FIPS 承認済みの対称鍵アルゴリズムの詳細については、http://csrc.nist.gov/cryptval/des.htmを参照のこと。FIPS 140-2『*Security Requirements for Cryptographic Modules*』は、http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdfで入手できる。

以降の内容は、IDPS の運用および保守に関する補足情報である。3.3.2.1項では、IDPS に関する日常的な作業においてコンソールを有効に使用する方法を説明する。3.3.2.2項では、IDPS テクノロジーの継続的な保守作業に関する詳細情報を示す。3.3.2.3項では、更新の入手および適用について述べる。

3.3.2.1 典型的な使用方法

ほとんどのIDPSコンソールには、ユーザの日常的な作業を支援する多数の機能がある。たとえば、ほとんどが備えているドリルダウン機能では、階層構造を掘り下げて警報に関する詳細情報を調べることができる[12]。ドリルダウンを使用することで、多数の警報に関する基本情報を一覧表示したり、特に注目すべき特定のイベントに関する追加情報を必要に応じて表示したりすることができる。製品によっては、採取したパケット（未加工およびプロトコルアナライザによる解析済み）、関連する警報（同じ発信元または送信先に関する別の警報など）、当該警報自体に関する文書など、広範な補足情報を表示する機能を持つものもある。一般に、IDPSが記録するデータが多いほど、分析担当者が、どのようなイベントが発生したのかを判断することが容易になる。一部のコンソールは、インシデント対応機能も備えており、たとえば、警報を基にしてインシデント事例を作成したり、警報の詳細を確認できるようにするために、警報に関する追加情報を文書化して特定のユーザやグループに対して送付することができるようにするワークフローメカニズムを提供したりするものがある。

ほとんどのコンソールには、さまざまな報告機能も備わっている。たとえば、所定の時刻に所定の報告を実行することや、報告を適切なユーザまたはホストに電子メールやファイル転送で送付することなどを、管理者またはユーザがコンソールを使用して行うことができる。ユーザの必要に応じた報告（特定のインシデントの報告を含む）を生成する機能や、報告の内容を必要に応じてカスタマイズする機能を持つコンソールも多い。データベースまたは解析しやすい形式のファイル（カンマで区切られた数値が記載されたテキストファイルなど）にログを保存するような IDPS 製品の場合は、データベース照会またはスクリプトの使用を通じて独自の報告を生成することもできる。これは、コンソールが報告をカスタマイズするための十分な能力を備えていない場合は、特に有用である。

3.3.2.2 ソリューションの継続的な保守

管理者は、IDPS を継続的に保守しなければならない。保守作業には、次のような内容が含まれる。

- IDPS の構成要素自体に関する運用上およびセキュリティ上の問題を監視する
- IDPSが正常に機能（イベントの処理、疑わしい活動に関する適切な警報の送信など）していることを定期的に確認する[13]
- 定期的に脆弱性アセスメントを実施する
- IDPS の構成要素（OS と、IDPS 以外のアプリケーションも含む）に関するセキュリティ上の問題についてベンダーからの連絡を受け取り、適切に対応する

---

[12] IDPS データの解析について詳しく説明することは、この文書のスコープ外である。詳細については、NIST SP 800-86『*Guide to Integrating Forensic Techniques into Incident Response*(インシデント対応へのフォレンジック技法の統合に関するガイド)』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。NIST SP 800-86 では、IDPS およびその他のセキュリティ事象に関する情報源から得られるデータの分析について論じている。

[13] 構成要素の機能を確認する一つの方法として、テスト環境または実稼動環境で IDPS を定期的にテストするという方法がある。ただし、そのようなテストを実稼働環境で実行すると、運用の妨げになることがある。IDPS テストの詳細については、セクション 9 を参照のこと。

■ IDPS ベンダーから更新に関する連絡を受け取り、更新のテストおよび導入を実行する。更新については、3.3.2.3項の説明を参照のこと。

3.3.2.3 更新の入手および適用

IDPS の更新には、ソフトウェア更新とシグネチャ更新の 2 種類がある。ソフトウェア更新は IDPS のソフトウェアのバグを修正したり新機能を追加したりするものであり、シグネチャ更新は新しい検知能力を追加したり既存の検知能力を向上（フォールスポジティブを減らすなど）したりするものである。ただし、シグネチャ更新においてプログラムコードの変更や置き換えが行われる IDPS も多く、その場合、シグネチャ更新はソフトウェア更新の特殊な形態である。それ以外の IDPS の場合、シグネチャはコード内に記述されておらず、シグネチャ更新は IDPS の設定データに変更を加えるものである。

ソフトウェア更新には、センサー、エージェント、管理サーバ、コンソールなど、IDPS の一部または全部の構成要素が含まれている可能性がある。センサーまたは管理サーバを対象とするソフトウェア更新（特にアプライアンスベースの装置の場合）は、以前の IDPS CD を新しいものと交換して装置を再起動する方法で適用されることが多い。多くの IDPS では、CD からソフトウェアが直接起動するため、ソフトウェアのインストールは不要である。その他の構成要素（エージェントなど）については、管理者がソフトウェアのインストールまたはパッチの適用を行う必要がある。これはホストごとに手作業で行われる場合と、IDPS の管理ソフトウェアにより自動的に行われる場合がある。ベンダーによっては、Web サイトまたはその他のサーバからのダウンロードによってソフトウェア更新やシグネチャ更新を提供しており、IDPS の管理者インタフェースがそのような更新のダウンロード・インストール機能を備えている場合も多い。

更新は、偶然または意図的に改変されているまたは差し替えられている可能性があるため、管理者は、更新を適用する前にその内容の完全性を確認すべきである。推奨される確認の方法は、更新の形式に応じて次のように異なる。

■ **Web サイトまたは FTP サイトからダウンロードしたファイル**：ベンダーから提供されたチェックサムと、ダウンロードしたファイルから計算したチェックサムを比較する。

■ **IDPS ユーザインタフェースによって自動的にダウンロードされた更新**：単独または複数のファイルとしてダウンロードされた場合は、ベンダーから提供されたチェックサムと管理者が生成したチェックサムを比較するか、IDPS ユーザインタフェース自体の機能によって何らかの完全性チェックを実行する。場合によっては、更新のダウンロードからインストールまでが、チェックサムの検証を除いて、一回の動作で実行されるようになっていることもある。その場合は、この動作の一部として、IDPS ユーザインタフェースによって個々の更新の完全性がチェックされるべきである。

■ **リムーバブルメディア（CD、DVD など）**：ベンダーから送付されたと考えられるリムーバブルメディアについて、内容の正当性を確認する具体的な方法がベンダーから提供されないことがある。メディアの正当性を確認することが関心事である場合は、管理者が確認方法をベンダーに問い合わせるべきである。確認するための方法としては、ベンダーから提供されたチェックサムとメディア上のファイルから計算したチェックサムを比較することや、メディアのコンテンツの正当性を確認するために、コンテンツのディジタル署名を検証することなどが考えられる。また、メディアをスキャンしてマルウェアが含まれていないかを確認することも検討すべきである。ただし、メディアに含まれているマルウェアを検知するための IDPS シグネチャによって、フォールスポジティブが発生する可能性があることにも注意すること。

一般に、IDPS は、ソフトウェア更新やシグネチャ更新によって既存のチューニングおよびカスタマイズ設定が影響を受けないように設計されている。ただし、重要な例外としてコードのカスタマイズがある。カスタマイズが行われている場合、ベンダーから提供されるコード更新のインストール後に、再度カスタマイズが必要になることが多い。どのような IDPS においても、不注意により既存の設定が失われることを防ぐために、定期的に、およびソフトウェア更新やシグネチャ更新の適用前に、設定内容のバックアップを行うべきである。

管理者は、ソフトウェア更新やシグネチャ更新を適用する前にそれらのテストを行うべきである（緊急時は除く。たとえば、組織に被害を与えつつある新しい拡散中の脅威を検知できるシグネチャがあり、それを適用する以外に検知あるいは阻止の方法がない場合など）。更新のテストだけを目的とした専用のセンサーまたはエージェントホストを少なくとも 1 基（エージェントの種類ごとに）用意しておくと便利である。新しい検知機能を追加すると大量の警報が発されるようになることが多いため、たとえ簡易なテストであっても（更新をロードし、通常の活動を監視する際に、IDPS がどのような動作をするかを観測するだけでも）、単独のセンサーまたはエージェントホストにおいてシグネチャ更新をテストすることは有用である。このテストを行うことで、問題を引き起こす可能性があって無効化することが望ましいシグネチャが特定しやすくなる。緊急対応を要しない状況では、ソフトウェア更新およびシグネチャ更新は、ファイアウォールやウイルス対策ソフトウェアなど他の重要なセキュリティ管理策の更新と同様の実践手法に従ってテスト・導入されるべきである。更新を実稼働環境へ導入する際には、管理者は、必要に応じて特定のシグネチャを無効にしたり、他の小規模な設定変更作業を実行したりするための準備を整えておくべきである。

3.3.3 技能の習得および維持

IDPS の導入、運用、保守には、次のようにさまざまな技能が必要である。

- IDPS の構成要素を導入する管理者には、システム管理、ネットワーク管理、情報セキュリティに関する基礎を理解しておく必要がある。
- IDPS のチューニングおよびカスタマイズを行う管理者には、情報セキュリティおよび IDPS の原則に関する相応の包括的知識が必要である。インシデント対応の原則と、組織のインシデント対応ポリシーおよび手続きについても理解しておくことが推奨される。また、IDPS の監視対象となるネットワークプロトコル、アプリケーション、オペレーティングシステムについても理解しておくべきである。
- 広範囲にわたるコードのカスタマイズ、報告書の作成、その他の作業のために、場合によってはプログラミングの技能も必要となる。

IDPS の原則に関する技能は、トレーニング、技術カンファレンス、書籍その他の技術文献、および指導教育プログラムなど多くの方法によって習得・維持することができる。また、特定の IDPS 製品に関する知識を得るには、次のような方法がある。

- **ベンダーによるトレーニング**：IDPS 製品ベンダーの多くは、将来、自社製品の管理者またはユーザになる人を対象に一つまたは複数のトレーニングコースを提供している。コース内容は、実習用の環境でテクノロジーの使用方法を実際に試して学べるようになっているものが多い。
- **製品に関する文書**：ほとんどの製品には、インストールガイド、ユーザガイド、管理者ガイドなどいくつかのマニュアルが用意されている。また、警報やシグネチャに関する補足情報が別冊のガイドやデータベースで提供される場合もある。

- **技術サポート**：ほとんどのベンダーは、顧客向けに技術サポートを提供している（製品を購入すると標準で利用できる場合もあれば、別途料金が必要な場合もある）。サポートは、主として、問題を解決し、ユーザや管理者に対して製品の機能を明らかにするために活用される。
- **プロフェッショナルサービス**：一部のベンダーは、プロフェッショナルサービスを提供する。これは、基本的にはベンダーによる有料のコンサルティングサービスである。たとえば、組織が、独自のシグネチャや報告書をベンダーに作成させる場合や、センサーのチューニングやカスタマイズを効果的に行うための方法を管理者が理解するのをベンダーに支援させる場合に利用することができる。
- **ユーザコミュニティ**：製品によっては活発なユーザコミュニティが形成され、通常は、メーリングリストやオンラインフォーラムなどの形態で運営されている。コミュニティでは、ユーザ同士が情報やコードを交換しあったり、問題のトラブルシューティングを相互に支援しあうことができる。したがって情報源として役立つ可能性はあるが、管理者およびユーザがユーザコミュニティを使用する際には注意も必要である。組織の IDPS の設定や問題に関する詳細情報をコミュニティに投稿することにより、組織のセキュリティインフラストラクチャ、システム、ネットワークなどに関する機密情報が、意図に反して開示されることになりかねないからである。

3.4 まとめ

IDPS ソリューションを構成する典型的な要素は、センサーまたはエージェント、管理サーバ、データベースサーバ、およびコンソールである。センサーおよびエージェントは、活動を監視および解析する要素であり、センサーはネットワークの監視に、エージェントはホストの監視に使用される。管理サーバは、センサーまたはエージェントから送られる情報を受信および管理する要素である。データベースサーバは、センサーまたはエージェントや管理サーバによって記録されるイベント情報を保存するリポジトリである。コンソールは、IDPS のユーザおよび管理者に対するインタフェースを提供するプログラムである。これら構成要素相互の接続には、組織の標準ネットワークを使用する場合と、セキュリティソフトウェア管理専用として厳密に設計された別個のネットワーク（管理ネットワークと呼ばれる）を使用する場合がある。管理ネットワークは、IDPS を攻撃から守り、不都合な状況下でも IDPS が機能するのに十分な帯域幅を確保するために役立つ。仮想ローカルエリアネットワーク（VLAN）を使用して仮想的な管理ネットワークを作成することもできる。その場合も IDPS の通信を保護することができるが、独立した管理ネットワークによって提供されるほどの保護効果は得られない。

ほとんどの IDPS は、多種多様なセキュリティ機能を提供する能力を備えている。製品によっては、観測した活動内容からホストやネットワークに関する情報を収集する情報収集機能を備えているものがある。また、IDPS は一般に、検知したイベントに関連するデータを詳細なログとして記録する。このデータは、警報の妥当性の確認、インシデントの調査、および、IDPS において検知されたイベントとその他のログ生成ソースにおいて検知されたイベントとの相関をとるのに使用することができる。一般に、データの完全性と可用性をサポートするため、ログはローカル環境と集中化サーバの両方に保存すべきである。

IDPS には、詳細かつ広範な検知機能を備えるものが多い。検知されるイベントの種類と、検知の一般的な正確さは、IDPS テクノロジーの種類によって大きく異なる。ほとんどの IDPS では、検知の正確さ、使い勝手、実効性を向上させるために多少のチューニングおよびカスタマイズが必要となる。多くの場合、チューニングやカスタマイズの機能が強力な製品であるほど、検知の正確さをデフォルト設定よりも向上させることができる余地が大きい。これらの機能の例としては、しきい値、ブラックリストおよびホワイトリスト、警報設定、コード編集などがある。製品の評価にあたっては、IDPS がどのようなチューニ

ングおよびカスタマイズ機能を備えているかを注意深く検討すべきである。管理者は、チューニングとカスタマイズの内容を正確に保つために、これらを定期的に見直すべきである。また、アノマリベースの検知を行うためのベースラインを収集する製品については、検知の正確さを保つために、必要に応じてベースラインの再構築を定期的に実行すべきである。

ほとんどの IDPS は、複数の防止機能を備えている。その機能の具体的な内容は、IDPS テクノロジーの種類により異なる。通常、防止機能に関する設定は、警報の種類ごとに管理者が指定することができる。設定により指定できる事項には、防止の有効化／無効化の切り替えや、使用する防止機能の種類などがある。

IDPS 製品を選定した場合、管理者がアーキテクチャの設計、IDPS 構成要素のテスト、構成要素に対するセキュリティ対策の実施を行った後に、IDPS を導入する必要がある。構成要素の配置、ソリューションの信頼性、他のシステムとの相互運用性、管理ネットワークアーキテクチャ、他のセキュリティ管理策に必要となる変更など、アーキテクチャに関しては多くの事項を考慮する必要がある。したがって、導入により発生した問題によって実稼働環境の運用が妨げられる可能性を低減するために、最初は実稼働環境ではなくテスト環境に IDPS の構成要素を導入することを検討すべきである。また、実稼働環境に導入する際には、少数の IDPS センサーまたはエージェントのみを有効にすることから始めるべきである。新しく導入された IDPS では、チューニングおよびカスタマイズが十分に行われるまでに、多数のフォールスポジティブが発生する可能性が大きいため、一度に多数のセンサーまたはエージェントを有効にした場合、管理サーバやコンソールが過負荷になり、チューニングおよびカスタマイズ作業が困難になることがある。

ソフトウェアベースの IDPS の構成要素のセキュリティを強固にし、すべての IDPS の構成要素を最新の状態に保つことに加え、管理者は、IDPS の構成要素自体のセキュリティを適切に保つための追加的な対策を実施すべきである。たとえば、IDPS の個々のユーザおよび管理者ごとに異なるアカウントを作成すること、IDPS の構成要素に対するネットワークアクセスを制限すること、IDPS の管理に関する通信を確実に正しく保護することなどが挙げられる。保護に使用する暗号化は、FIPS 承認済みの暗号化アルゴリズムのみを使用して行うべきである。

管理者は、IDPS を継続的に保守しなければならない。継続的な保守作業には、IDPS の構成要素の運用上およびセキュリティ上の問題の監視、定期的な脆弱性アセスメントの実施、IDPS の構成要素に存在する脆弱性への適切な対処、IDPS のソフトウェア更新およびシグネチャ更新のテストの実施および導入などが含まれる。更新は、偶然または意図的に改変されているまたは差し替えられている可能性があるため、管理者は、更新を適用する前にその内容の完全性を確認すべきである。また、緊急時を除いては、ソフトウェア更新やシグネチャ更新を適用する前にそれらのテストを行うべきである。既存の設定が意図せずに失われることがないように、設定内容のバックアップを定期的に、またソフトウェア更新やシグネチャ更新の適用前に作成することも必要である。

（本ページは意図的に白紙のままとする）

4. ネットワークベースのIDPS

ネットワークベースの IDPS は、特定のネットワークセグメントまたはネットワーク装置のネットワークトラフィックを監視し、ネットワーク、トランスポートおよびアプリケーションの各プロトコルを解析して疑わしい活動を特定する。このセクションでは、ネットワークベースの IDPS テクノロジーについて詳しく論じる。最初に、セクション 4 の残りの部分を理解するための背景知識として、TCP/IP について簡単な概説を示す。次に、ネットワークベースの IDPS の主要な構成要素を示し、それらの要素の導入に通常使用されるアーキテクチャについて説明する。また、疑わしい活動の特定に使用される方法を含め、各テクノロジーのセキュリティ機能について深く掘り下げる。そのあとは、各テクノロジーの管理機能について説明し、導入および運用に関する推奨事項を提示する。

4.1 ネットワーキングの概要

TCP/IP は、ネットワーク通信を提供するために全世界で広く使われている。TCP/IP の通信は、互いに連携する 4 つの層で構成されている。ユーザがネットワーク経由でデータを伝送するとき、データは最上層から中間層を経て最下層まで、各層において情報を追加されながら、渡されていく。最下層が、蓄積されたデータを物理ネットワーク経由で送信すると、そのデータは宛先に向かって順次上の層へ渡される。基本的には、ある層で作られたデータは、その下の層において、それよりも大きな入れ物に入れられカプセル化される。TCP/IP の 4 つの層を最上層から最下層の順に図 4-1 に示す。

アプリケーション層。この層は、DNS（Domain Name System）、HTTP（Hypertext Transfer Protocol）、SMTP（Simple Mail Transfer Protocol）など、特定のアプリケーションのためのデータを送受信する。
トランスポート層。この層は、ネットワーク間でアプリケーション層のサービスを伝送するためのコネクション指向またはコネクションレスのサービスを提供する。トランスポート層は、任意で通信の信頼性を保証することもできる。TCP（Transmission Control Protocl）および UDP（User Datagram Protocol）は、一般によく使われるトランスポート層のプロトコルである。
IP（Internet Protocol）層（ネットワーク層ともいう）。この層は、ネットワークを経由するパケットの経路を制御する。IPv4 が、TCP/IP における基礎的なネットワーク層プロトコルである。ネットワーク層においてよく使われる他のプロトコルとしては、IPv6、ICMP（Internet Control Message Protocol）および IGMP（Internet Group Management Protocol）がある。
ハードウェア層（データリンク層ともいう）。この層は、物理ネットワークの構成要素の通信を取り扱う。最もよく知られているデータリンク層のプロトコルは Ethernet である。

図 4-1. TCP/IP の各層

TCP/IP の 4 つの層は、互いに連携してホスト間でデータを伝送する。ネットワークベースの IDPS は一般に、大半の解析を、アプリケーション層を対象に行う。また、トランスポート層およびネットワーク層でも活動の解析を行い、それらの層での攻撃を特定したり、アプリケーション層の活動（TCP ポート番号が、使用されているアプリケーションを示すことがある）の解析を支援したりする。ネットワークベースの IDPS の一部には、ハードウェア層で限定的な解析を行うものもある。4.1.1 項～4.1.4 項では、各層についてさらに詳しく説明する。

4.1.1 アプリケーション層

アプリケーション層は、アプリケーションによる、アプリケーションサーバとクライアント間のデータ伝送を可能にする層である。アプリケーション層のプロトコルの例には、Web サーバと Web ブラウザとのあいだでデータを伝送する HTTP（Hypertext Transfer Protocol）がある。アプリケーション層の他の一般的なプロトコルには、DNS（Domain Name System）、FTP（File Transfer Protocol）、SMTP（Simple Mail Transfer Protocol）、SNMP（Simple Network Management Protocol）などがある。アプリケーション層に属する固有のプロトコルは、よく使われるものだけでも数百ある他、あまり一般的でないものも多数ある。使われるプロトコルを問わず、アプリケーションデータが生成され、さらなる処理のためにトランスポート層に渡される。

4.1.2 トランスポート層

トランスポート層は、データをホスト間で伝送できるようにパッケージ化する責任を負う。ネットワーク経由で通信するほとんどのアプリケーションは、データを確実に送るためにトランスポート層に依存している。一般に、これは TCP を使用して実現される。アプリケーションデータの一部が失われても問題がない場合（ストリーミングオーディオ、ビデオなど）、またはアプリケーション自身がデータの確実な送付を保証している場合は、UDP が一般的に使われる。UDP はコネクションレスであり、あるホストが予備的なネゴシエーションなしで単純に別のホストにデータを送る。TCP または UDP の各パケットには、送信元ポート番号と宛先ポート番号がある。ポートの 1 つは、一方のシステム上にあるサーバアプリケーションに関連付けられており、もう一方のポートは、他方のシステム上にある対応するクライアントアプリケーションに関連付けられている。クライアントシステムは一般に、アプリケーションが使用するための利用可能な任意のポート番号を選択するのに対し、サーバシステムは一般に、各アプリケーション専用の固定のポート番号を持っている。UDP および TCP のポートは非常によく似ているが、互いに異なるものであり、互いを代替することはできない。

4.1.3 ネットワーク層

ネットワーク層はIP層とも呼ばれ、トランスポート層から受け取ったデータのアドレス指定および経路制御を扱う責任を負う。ネットワーク層によってトランスポート層のデータがカプセル化された結果として得られる論理単位は「*パケット*」と呼ばれる。各パケットには、使用されているトランスポートプロトコルの特性を指定するさまざまな「フィールド」で構成される「*ヘッダ*」が含まれている。パケットには、アプリケーションデータを保持する「ペイロード」が含まれていることがある。IPヘッダには、IP Versionというフィールドがあるが、これはどのバージョンのIPが使用されているかを示す。一般にこれはIPv4 を示す 4 に設定されているが、IPv6 の使用が増えているので、このフィールドが代わりに 6 に設定されている可能性がある [14]。IPヘッダの他の重要なフィールドには、次のようなものがある。

- **発信元および宛先のIPアドレス。**これらは、通信のエンドポイントを示すことを目的とした、”from” アドレスと “to” アドレスである [15]。IIPアドレスの例：10.3.1.70（IPv4）および 1000::2F:8A:400:427:9BD1（IPv6）。

[14] 他のバージョンの IP も可能性としてはあるが、いずれも一般的には使われていない。IP Version フィールドの有効な値の正式なリストは、http://www.iana.org/assignments/version-numbersから入手できる。この文書では、別途明記しないかぎり、IPv4 の使用を前提とする。

[15] IP アドレスは多くの場合、通信の実際のエンドポイントを識別するには不正確だったり誤解を招くものであったりする。

■ **IPプロトコル番号。**これは、IPのペイロードに、どのネットワーク層プロトコルまたはトランスポート層プロトコルが含まれているかを示す[16]。よく使われるIP番号には、1（ICMP）、6（TCP）、17（UDP）、および 50（ESP：Encapsulating Security Payload）がある。

ネットワーク層は、エラー情報およびデータのアドレス指定と経路制御に関係するステータス情報の提供についても責任を負う。これはICMPを使用して行われる。ICMPは、そのエラーメッセージおよびステータスメッセージが宛先に到達することを保証するための試みを全く行わないコネクションレスプロトコルである。アプリケーションデータではなく、限定された情報を送信するように設計されているため、ICMPにはポートはない。その代わりに、各ICMPメッセージの目的を示すメッセージタイプがある[17]。メッセージタイプによっては、メッセージコードがあるものもある。これは、サブタイプであると考えてもよい。たとえば、Destination Unreachable（宛先に到達不能）というICMPメッセージタイプには、何（ネットワーク、ホスト、プロトコルなど）が到達不能だったのかを示すメッセージコードの候補がいくつかある。ほとんどのICMPメッセージタイプは、応答を求めることを目的としていない[18]。

4.1.4 ハードウェア層

ハードウェア層はデータリンク層とも呼ばれ、その名前が示すとおり、ケーブル、ルータ、スイッチ、およびNIC（ネットワークインタフェースカード）などネットワークの物理的な構成要素が関係する。また、ハードウェア層には各種のハードウェア層プロトコルが含まれ、なかでもEthernetが最も広く使われている。Ethernetは、MAC（Media Access Control：媒体アクセス制御）アドレスの概念に依拠している。これは、個々のNICに固定的に割り当てられる一意の 6 バイト値である（例：00-02-B4-DA-92-2C）[19]。個々の「*フレーム*」（ハードウェア層における論理単位）には 2 つのMACアドレスが含まれている。その 1 つは、当該フレームを転送してきた直前のNICのMACアドレス、もう 1 つはフレームの送信先となる次のNICのMACアドレスである。フレームが、送信元のホストから最終的な宛先のホストに向かう経路上でネットワーク装置（ルータやファイアウォールなど）を経由するたびに、ローカルの送信元と宛先を指し示すようにMACアドレスが更新される。ハードウェア層における複数の異なる伝送をリンクして、単独のネットワーク層における伝送にまとめることができる。

各フレームには、MACアドレスの他に、フレームのペイロードに含まれているプロトコル（通常は、IPまたはARP：Address Resolution Protocol）を示すEtherType値も含まれている[20]。IPが使用されている場合、それぞれのIPアドレスが特定のMACアドレスに対応する（複数のIPアドレスが単一のMACアドレスに対応することが可能なため、MACアドレスは必ずしも特定のIPアドレスを一意に特定するものではない）。

---

16 有効な IP プロトコル番号の正式なリストは、http://www.iana.org/assignments/protocol-numbersから入手できる。

17 ICMP の現在有効なタイプのリストは、http://www.iana.org/assignments/icmp-parametersから入手できる。

18 ICMP は、応答を特にエラーメッセージに限定するように設計されている。ICMP がこのように設計されていなければ、メッセージのループが発生する可能性がある。たとえば、ホスト A がホスト B から ICMP エラーメッセージを受け取り、それに対してエラーメッセージで応答し、ホスト B がそのエラーメッセージに対しエラーメッセージで応答したとする。両ホストは、互いにエラーメッセージに対してエラーメッセージを送信し続ける可能性がある。

19 MAC アドレスを偽装するようにシステムを設定するさまざまなソフトウェアユーティリティが一般に公開されている。また、メーカーが重複する MAC アドレスを持った NIC を誤って作成したケースもある。

20 0x0800 という EtherType 値は IP を表し、0x0806 は ARP を表す。EtherType 値の詳細については、http://www.iana.org/assignments/ethernet-numbersを参照のこと。

4.2 構成要素とアーキテクチャ

この項では、典型的なネットワークベースの IDPS の主要な構成要素について説明し、それらの構成要素のための最も一般的なネットワークアーキテクチャを示す。また、ネットワークベースの IDPS センサーの設置についての推奨事項を提示する。

4.2.1 典型的な構成要素

典型的なネットワークベースの IDPS は、センサー、1 基以上の管理サーバ、複数のコンソール、および任意で、1 基以上のデータベースサーバ（ネットワークベースの IDPS がその使用をサポートしている場合）により構成される。これらのうちセンサー以外の構成要素は、他の種類の IDPS テクノロジーのものと似ている。ネットワークベースの IDPS のセンサーは、1 つ以上のネットワークセグメントにおけるネットワーク活動の監視・解析を行う。監視を行うネットワークインタフェースカードは、*プロミスキャスモード*に設定される。これは、観測した着信パケットを、その意図する宛先に関係なくすべて受け入れる設定である。IDPS の導入においては、複数のセンサーを使用することがほとんどであり、大規模な場合にはセンサーが数百基にもなることがある。センサーは次の 2 つの形態のものが入手可能である。

- **アプライアンス**：アプライアンス型のセンサーは、専用のハードウェアとセンサーソフトウェアから成る。このハードウェアは一般にセンサーとして使用するために最適化されており、パケットを効率よく取得するための専用の NIC と NIC ドライバ、および解析を支援する専用のプロセッサまたはその他のハードウェア構成要素を含む。効率を高めるために、IDPS のソフトウェアの一部または全部がファームウェア内部に置かれることがある。アプライアンスには、管理者が直接アクセスすることを想定していない、カスタマイズによりセキュリティが強化されたオペレーティングシステム（OS）がしばしば使用される。
- **ソフトウェアのみ**：一部のベンダーは、アプライアンスのないセンサーソフトウェアを販売している。管理者は、特定の仕様を満たすホストにこのソフトウェアをインストールすることができる。センサーソフトウェアには、カスタマイズされた OS を含むものと、一般のアプリケーション同様に標準的な OS にインストールするものがある。

4.2.2 ネットワークアーキテクチャとセンサーの設置場所

ネットワークベースの IDPS を設置する場合には、可能なかぎり、管理ネットワークを使用すべきである。独立の管理ネットワークなしで IDPS を設置する場合は、IDPS の通信を保護するために VLAN が必要かどうかを検討すべきである。

構成要素に対して適切なネットワークを選択することに加え、管理者は IDPS センサーをどこに設置するかを決定しなければならない。センサーは、次の 2 つのいずれかのモードで導入することができる。

- **インライン**：*インラインセンサー*は、ファイアウォールに関連するトラフィックフローと同様に、監視対象のネットワークトラフィックがセンサーを必ず通過するように設置される。実のところ、一部のインラインセンサーは、ファイアウォールと IDPS 装置のハイブリッドである（そうでないものは単なる IDPS である）。IDPS センサーをインラインモードで設置する主な理由は、ネットワークトラフィックを遮断することによる攻撃阻止を可能にするためである。インラインセンサーは一般に、ネットワークファイアウォールおよびその他のネットワークセキュリティ装置が置かれる場所、つまり、外部ネットワークとの接続部および分離する必要がある個々の内部ネットワークの間の境界など、異なるネットワークを分ける境界部分に置かれる。ファイアウォールと IDPS のハイブリッド型装置でないイン

ラインセンサーは一般に、処理する必要があるトラフィックの量が少なくなるよう、ネットワークのより安全な側に設置される。図 4-2 にそのような設置の例を示す。ファイアウォールなどのネットワーク境界部に設置される装置を保護し、その装置に対する負荷を削減するために、センサーをネットワークのより安全性の低い側に置くこともできる。

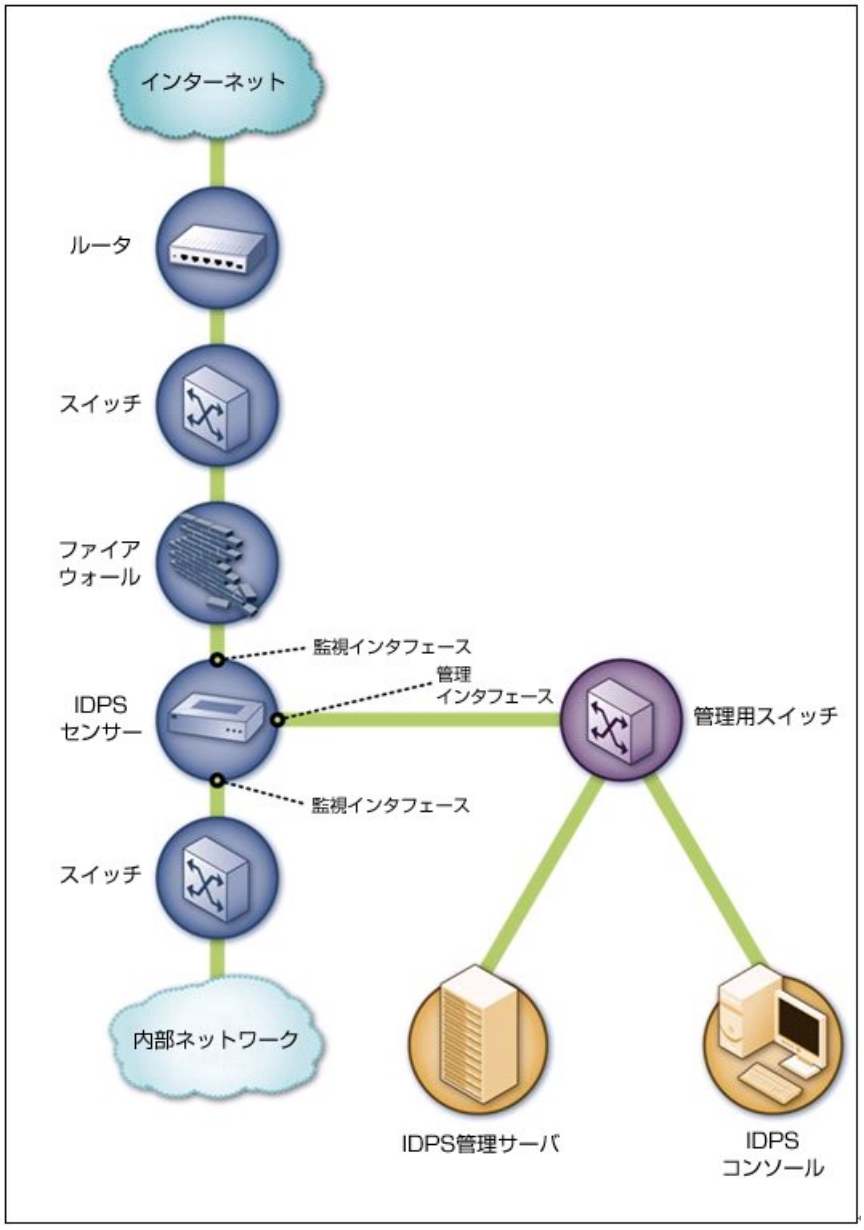

図 4-2. インライン型のネットワークベース IDPS センサーのアーキテクチャ例

■ **受動型**：*受動型センサー*は、実際のネットワークトラフィックのコピーを監視するような位置に設置される。実際のトラフィックは、センサーを通過しない。受動型センサーは一般に、ネットワークの境界部分などのネットワークの主要な場所、および DMZ（Demilitraized Zone：非武装地帯）サブネット

での活動など主要なネットワークセグメントの監視を行うことができるように設置される。受動型センサーでは、次のようにさまざまな方法でトラフィックを監視することができる。

– **スパニングポート**：多くのスイッチは、*スパニングポート*を備えている。これは、スイッチを通過するすべてのトラフィックを見ることのできるポートである。スパニングポートにセンサーを接続することにより、多数のホスト間で送受信されるトラフィックを監視することができる。この監視方式は、比較的簡単でコストも低いが、問題が生じる場合もある。スイッチを誤って設定または再設定した場合、スパニングポートで一部のトラフィックが見えなくなる可能性がある。スパニングポートを使用する場合のもう 1 つの問題は、リソースに負担をかけることがある点である。スイッチに高い負荷がかかっているとき、そのスパニングポートでトラフィックの一部が見えなくなる可能性がある。あるいは、スパニングが一時的に無効にされる場合がある。さらに、多くのスイッチはスパニングポートが 1 つしかないにも関わらず、ネットワーク監視ツール、ネットワークフォレンジック分析ツール、およびその他の IDPS センサーなど複数のテクノロジーで同じトラフィックを監視する必要があることがよくある。

– **ネットワークタップ**：*ネットワークタップ*は、センサーと、光ファイバケーブルなど物理ネットワーク媒体そのものとの直接的な接続である。タップは、媒体が伝送するすべてのネットワークトラフィックのコピーをセンサーに提供する。タップを設置する際は、ネットワークを一時的に停止する必要があり、タップに問題が生じた場合にも停止が必要となる可能性がある。また、スパニングポートは組織全体にすでに存在する場合が多いのに対し、ネットワークタップは、ネットワークへの追加要素として購入する必要がある。

– **IDS ロードバランサ**：*IDS ロードバランサ*は、ネットワークトラフィックを集約して IDPS センサーなどの監視システムに送り込む装置である。ロードバランサは、1 つ以上のスパニングポートまたはネットワークタップからネットワークトラフィックのコピーを受け取り、複数の異なるネットワークのトラフィックを集約することができる（2 つのネットワークに分割されたセッションを組み立て直すなど）。ロードバランサは、受信したトラフィックのコピーを、管理者によって設定されたルールセットに基づいて、IDPS センサーを含む 1 つ以上の監視装置に配信する。このルールは、どの種類のトラフィックをどの監視装置に提供するかをロードバランサに指示するものである。一般的な設定としては、次のようなものがある。

    - **すべてのトラフィックを複数の IDPS センサーに送る**：高可用性を確保する場合や、同じ活動を複数の種類の IDPS センサーで平行して解析する場合に使用する。

    - **量に応じてトラフィックを複数の IDPS センサーの間で動的に振り分ける**：一般に、トラフィックの処理とそれに対応する解析によってセンサーが過負荷になるのを防ぐための負荷分散を目的として使用する。

    - **IP アドレス、プロトコル、その他の特性に基づいて、トラフィックを複数の IDPS センサーに振り分ける**：1 台の IDPS センサーを Web 活動の監視専用にし、もう一台の IDPS センサーにその他のすべての活動を監視させるなど、負荷分散を目的として行われる。また、トラフィックの振り分けを使用して特定種類のトラフィック（たとえば、最も重要なホストが関係するトラフィック）をより詳しく解析することもできる。

  トラフィックを複数の IDPS センサーに振り分けると、関係する複数のイベントあるいは、単一のイベントが細分化されたものを異なるセンサーで監視することになり、検出の正確さが低下する可能性がある。たとえば、複数のステップにより構成される攻撃で、攻撃の各ステップ単体では

害がないが、二つのステップが順次実行されると悪意のある攻撃であるとみなされる場合、二台のセンサーがそれぞれ単体の攻撃ステップを観測すると、攻撃として認識されない可能性がある。

図 4-3 に、IDS ロードバランサ、ネットワークタップ、およびスパニングポートを使用して、監視対象ネットワークに接続された受動型センサーの例を示す。

4.3.4項で説明するように、センサーによって侵入を防止するテクニックでは、ほとんどの場合、受動型ではなくインラインモードでセンサーを設置する必要がある。受動型テクニックは、トラフィックのコピーを監視するため、一般に、センサーによってトラフィックが宛先に到達するのを防ぐための信頼性のある方法とはなり得ない。受動型センサーからネットワークにパケットを送ることにより、接続の妨害を試みることが可能な場合もあるが、そのような手法は一般にインラインによる方法よりも効果が低い。一般に、防止手段を使用する場合はセンサーをインラインで設置し、使用しない場合は受動型で設置すべきである。

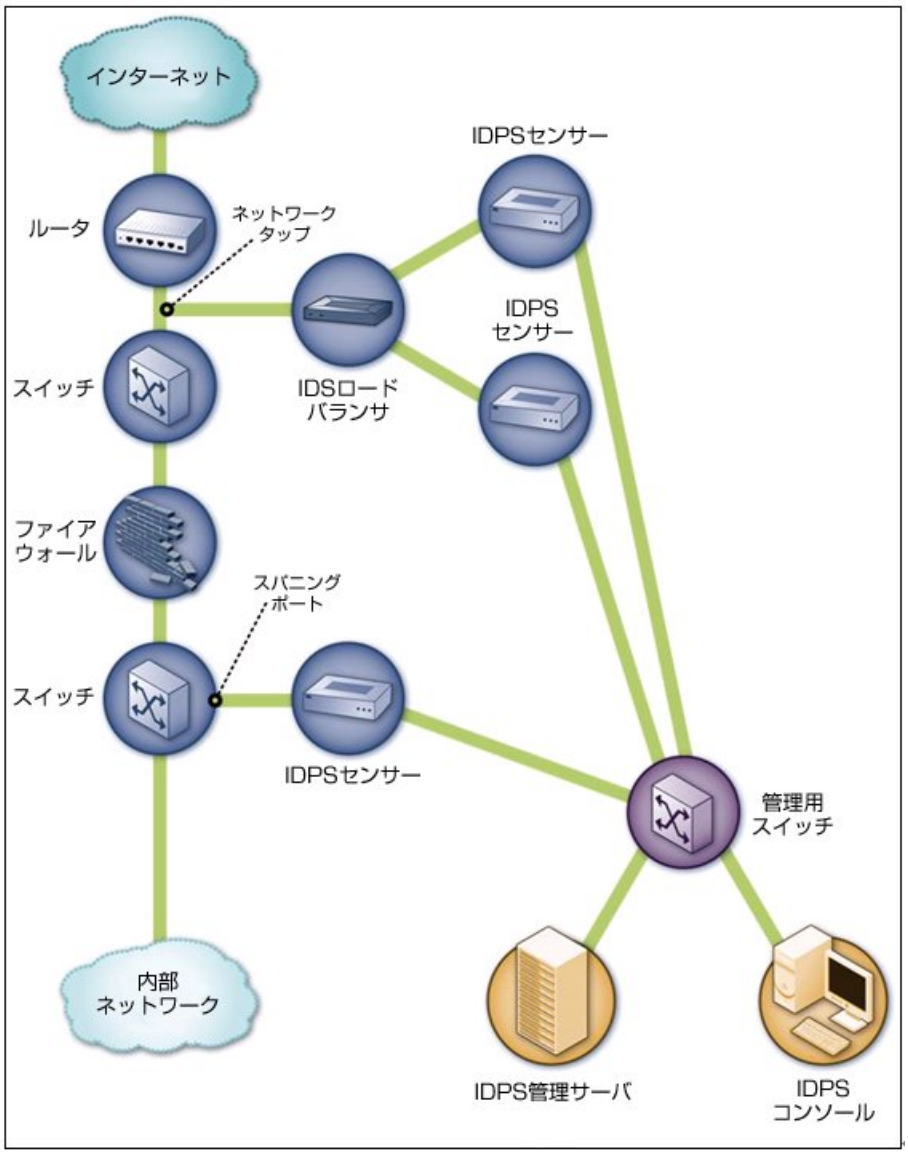

図 4-3. 受動型のネットワークベース IDPS センサーのアーキテクチャ例

4.3 セキュリティ機能

ネットワークベースの IDPS 製品は、多種多様なセキュリティ機能を提供する。一般的なセキュリティ機能を、ここでは情報収集、ログの記録、検知、および防止の 4 つに分け、それぞれについて4.3.1項～4.3.4項で説明する。IDPS 製品によっては、若干の SIEM（セキュリティ情報およびイベント管理）機能を持つものもある。SIEM の詳細については、8.2.2項を参照されたい。

4.3.1 情報収集機能

一部のネットワークベースの IDPS は、限定的な情報収集機能を備えており、ホストおよびそれらに関係するネットワーク活動についての情報を収集することができる。たとえば、次のような情報収集機能がある。

- **ホストの特定**：IDPS センサーによっては、組織のネットワーク上にあるホストを IP アドレスごとまたは MAC アドレスごとに示す一覧を作成する機能を備えている。この一覧は、ネットワークに接続されている新しいホストを特定するためのプロファイルとして使用することができる。
- **オペレーティングシステムの特定**：IDPS センサーによっては、組織内にあるホストで稼働している OS およびそのバージョンをさまざまな方法で特定する機能を備えている。たとえば、各ホストでどのポートが使用されているかを調べることにより具体的な OS または OS ファミリ（Windows、UNIX など）を特定できる場合がある。また、パケットヘッダを解析して、通常と異なる一定の性質や、特定の OS に見られる性質の組み合わせを識別する方法（*受動的フィンガープリンティング*と呼ばれる）もある。一部のセンサーでは、アプリケーションのバージョンを特定できるが（下記を参照）、場合によっては、この情報からどの OS が使用されているのかを特定できる。稼働している OS のバージョンを知ることは、潜在的に脆弱なホストを特定するために役立つ。
- **アプリケーションの特定**：一部のアプリケーションについては、使用ポートを追跡したりアプリケーションの通信の特徴を監視したりすることにより、使用されているアプリケーションのバージョンを IDPS センサーにより特定することができる。たとえば、クライアントからサーバへの接続が確立される際、稼働中のアプリケーションサーバソフトウェアのバージョンがサーバからクライアントに伝えられたり、その逆が行われたりすることがある。アプリケーションのバージョン情報は、潜在的な脆弱性のあるアプリケーションを特定することや、アプリケーションによっては不正使用を発見することに役立つ。
- **ネットワークの各種特性情報の特定**：一部の IDPS センサーは、各種ネットワーク装置およびホストの設定に関連するネットワークトラフィックに関する一般的な情報（装置間のホップ数など）を収集する機能を備えている。この情報を使用して、ネットワークの設定に加えられた変更を検出することができる。

4.3.2 ログ記録機能

ネットワークベースの IDPS は一般に、検知したイベントに関連するデータを詳細なログとして記録する。このデータは、警報の妥当性の確認、インシデントの調査、および、IDPS において検知されたイベントとその他のログ生成ソースにおいて検知されたイベントとの相関をとるのに使用することができる。ネットワークベースの IDPS のログに記録される一般的なデータフィールドとしては、次のようなものがある。

- タイムスタンプ（通常は日付および時刻）
- 接続 ID またはセッション ID（通常、個々の TCP 接続またはコネクションレスプロトコルにおけるパケットグループなどに割り当てられる通し番号または一意の番号）

- イベントまたは警報の種類 [21]
- 評価（優先度、重大度、影響の程度、確実性など）
- ネットワーク層、トランスポート層、アプリケーション層のプロトコル
- 送信元および宛先 IP アドレス
- 送信元および宛先の TCP または UDP ポート、あるいは ICMP タイプおよびコード
- 当該接続を介して伝送されたバイト数
- 復号したペイロードデータ（アプリケーションの要求／応答など）
- 状態に関する情報（認証されたユーザ名など）
- 実行された防止措置（該当する場合）

また、ほとんどのネットワークベースの IDPS ではパケット採取も行うことができる。一般に、これは何らかの警報が発生したあと、当該接続における以後の活動内容を記録することを目的として行われる。IDPS が警報発生までのパケットを一時的に保存している場合は、当該接続におけるすべての活動内容が記録される。

4.3.3 検知機能

ネットワークベースの IDPS には、詳細かつ広範な検知機能を備えるものが多い。ほとんどの製品では、シグネチャベースの検知、アノマリベースの検知、ステートフルプロトコル解析の手法を組み合わせることで、よく使用されるプロトコルの綿密な解析を実行している。ネットワークベースの IDPS を選定する際には、そのような技術を組み合わせて使用している製品を採用すべきである。通常、検知方法は緊密に絡み合っている。たとえば、活動内容がステートフルプロトコル解析エンジンによって要求と応答に分けられたあと、要求と応答のそれぞれに対して、アノマリの有無のチェックや、既知の悪意ある活動を示すシグネチャとの比較が行われるといった動作が考えられる。製品によっては、NBA（ネットワーク挙動解析）ソフトウェアと同じ手法を用い、同じ機能を提供するものもある。詳細については、セクション 6 を参照のこと。

この項では、次の観点から検知機能について説明する。

- 検知されるイベントの種類
- 検知の正確さ
- チューニングおよびカスタマイズ
- 技術的な制約

[21] イベントまたは警報の種類は、コンソールにおいて、特定の脆弱性や悪用方法に関する補足情報にリンクされることが多い。補足情報としては、たとえば、詳細情報の参照先や関連 CVE（Common Vulnerabilities and Exposures）番号などがある。

4.3.3.1 検知されるイベントの種類

ネットワークベースの IDPS によって最もよく検知されるイベントの種類には、次のようなものがある。

- **アプリケーション層の偵察および攻撃（バナーの取得、バッファオーバーフロー、書式文字列攻撃、パスワード推測、マルウェア伝送など）**：ネットワークベースのIDPSは、数十種類のアプリケーションプロトコルを解析できるものがほとんどである。解析対象として多いのは、DHCP（Dynamic Host Configuration Protocol）、DNS、Finger、FTP、HTTP[22]、IMAP（Internet Message Access Protocol）、IRC（Internet Relay Chat）、NFS（Network File System）、POP（Post Office Protocol）、rlogin／rsh、RPC（Remote Procedure Call）、SIP（Session Initiation Protocol）、SMB（Server Message Block）、SMTP、SNMP、Telnet、TFTP（Trivial File Transfer Protocol）の他、各種データベースプロトコル、インスタントメッセージングアプリケーション、ピアツーピアファイル共有ソフトウェアなどがある。

- **トランスポート層の偵察および攻撃（ポートスキャン、異常なパケット分割、SYN フラッディングなど）**：トランスポート層プロトコルでは、TCP および UDP が最も頻繁に解析対象となる。

- **ネットワーク層の偵察および攻撃（IPアドレスのなりすまし、不正なIPヘッダ値など）**：ネットワーク層プロトコルでは、IPv4、ICMP、IGMPが最も頻繁に解析対象となる他、多くの製品がIPv6 にも対応している。ネットワークベースのIDPSが実行できるIPv6 解析のレベルは、製品ごとの差がかなり大きい。製品によっては、IPv6 に対応していないものや、単にIPv6 活動があることを管理者に注意喚起することしかできないものがある。他の製品の中には、IPv6 およびトンネリングされたIPv6 トラフィックについての基本的な処理、つまり、送信元および宛先IPアドレスの記録や、綿密な調査のためのペイロード抽出（HTTP、SMTPなど）を行うことができるものがある。また、解析機能が完全にIPv6 に対応している製品では、IPv6 オプションの有効性確認などにより、プロトコルの使用方法が正常でない場合を特定することができる。現時点で、または将来的にIPv6 活動を監視する必要のある組織の場合、ネットワークベースのIDPS製品を評価する際には、IPv6 解析能力を入念に評価すべきである[23]。

- **予期していないアプリケーションサービス（トンネリングされたプロトコル、バックドア、許可されていないアプリケーションサービスが稼働しているホストなど）**：通常、これらの検知は、ステートフルプロトコル解析手法（ある接続における活動がそこで予期されるアプリケーションプロトコルと矛盾していないかを判定することができる）、またはアノマリベースの検知手法（ネットワークフローの変化や、ホストの開かれたポートに関する変化を特定することができる）によって行われる。

- **ポリシー違反（不適切な Web サイトの利用、禁止されているアプリケーションプロトコルの使用など）**：許可されるべきでない活動の特性（TCP または UDP ポート番号、IP アドレス、Web サイト名など、ネットワークトラフィックを調べることにより特定できるデータ）を管理者が指定することができる IDPS を使用することにより、ある種のセキュリティポリシー違反を検知することができる。

---

[22] HTTP プロトコルの活動は、ネットワークベース IDPS で監視できるが、SOAP（Simple Object Access Protocol）などによる Web サービス利用や、HTTP により伝送される XML（Extensible Markup Language）メッセージなどは解析できないのが普通である。そこで、Web サービス活動の解析を行うための、XML ゲートウェイまたは XML ファイアウォールと呼ばれるセキュリティテクノロジーが開発されている。この種のテクノロジーは、侵入防止機能に加え、ファイアウォール処理、認証／許可サービス、アクセス制御、監査ログといった機能を備えている。XML ゲートウェイの詳細については、NIST SP 800-95『*Guide to Web Services Security (DRAFT)*』（http://csrc.nist.gov/publications/drafts.html）を参照のこと。

[23] NIST SP 500-267『*A Profile for IPv6 in the U.S. Government, Version 1.0 (DRAFT)*』には、ネットワークベース IDPS 製品における IPv6 の取り扱いに関する推奨事項が示されている。当該文書（草稿）は、http://www.antd.nist.gov/で入手できる。

IDPS によっては、暗号化通信を確立する際の初期ネゴシエーションを監視し、クライアントまたはサーバソフトウェアに存在する既知の脆弱性や設定ミスを特定することができるものがある。監視対象には、SSH（Secure Shell）や SSL（Secure Sockets Layer）などのアプリケーション層プロトコルと、IPSec（IP Security）などネットワーク層の仮想プライベートネットワーク（VPN）プロトコルが含まれる。

ネットワークベースの IDPS センサーは、攻撃が成功する可能性が高いかどうかを判断できる場合が多い。たとえば、4.3.3.3 項で述べるように、センサーは、組織内の各 Web サーバで稼働している Web サーバソフトウェアのバージョンを知ることができる。Web サーバに攻撃が仕掛けられた場合、標的の Web サーバがその攻撃に対して脆弱でなければ、センサーは優先度の低い警報を発し、その攻撃に対して脆弱であると判断されれば、優先度の高い警報を発することが考えられる。IDPS センサーは一般に、攻撃が成功する可能性の高低に関わらず、攻撃を阻止するように設定されているが、IDPS は、攻撃が阻止されなかった場合に発生したであろうと想定される被害の大きさに応じて、異なる優先度レベルの活動のログを記録することがある。

4.3.3.2 検知の正確さ

ネットワークベースの IDPS は、歴史的に、フォールスポジティブおよびフォールスネガティブの発生率が高いものとされてきた。初期のテクノロジーのほとんどは、主としてシグネチャベースの検知に基づいていたが、この方法により単独で正確に検知できるのは、比較的単純なよく知られた脅威のみである。より新しいテクノロジーでは、複数の検知方法を組み合わせて使用することで、検知の正確さと幅が改善し、フォールスポジティブおよびフォールスネガティブの発生率も概ね減少した。ネットワークベースの IDPS の正確さに共通するもう 1 つの問題として、一般的に、監視対象となる環境の特性を反映させるチューニングおよびカスタマイズの作業に大きな手間がかかることが挙げられる。

監視対象の活動が複雑であるため、ネットワークベースの IDPS センサーのフォールスポジティブおよびフォールスネガティブは若干程度しか減少させることができない。1 基のセンサーで、内部および外部の数百、数千のホストに関するトラフィックを監視することも多い。監視対象のネットワークにおいて、膨大な数およびバリエーションの OS やアプリケーションが使用されている可能性がある。また、それらは、常に変更されている。したがって、観測する内容の全てをセンサーが把握することは不可能である。

それに加え、センサーは、サーバ／クライアントのさまざまな組み合わせにおける活動を監視しなければならない。たとえば、組織内で稼働する Web サーバの種類とバージョンが 10 通り存在し、そこにアクセスするユーザの使用する Web ブラウザの種類とバージョンが 50 通りあるといった状況が考えられる。ブラウザとサーバの個々の組み合わせごとに、通信は固有の性質（コマンドシーケンス、応答コードなど）を示す可能性があり、これが解析の正確さに影響することがある。また、ブラウザおよびサーバに適用される設定やカスタマイズの内容も一様とは限らない。ネットワークの活動を変化させるようなセキュリティ管理策（ファイアウォール、プロキシサーバなど）がサーバとクライアントの間に存在することも、センサーでの解析を困難にする要素となり得る。

理想としては、エンドポイントが行うのと同様の解釈を、ネットワークベースの IDPS がすべてのネットワーク活動について行えることが望ましい。たとえば、Web サーバの種類が異なれば、同じ Web 要求を受け付けても異なる解釈がされる可能性がある。ステートフルプロトコル解析技術では、一般的な種類のクライアントやサーバで行われる処理を複製することにより、異なる解釈を試みる。これにより、センサーにおける検知の正確さはわずかながら向上する。多くの攻撃者は、検知を回避するためのテクニックとして、攻撃の際に、特定のクライアントやサーバに固有の処理特性（文字エンコーディングの扱い

など）を利用する。したがって、このような一般的な回避テクニックに対処できるネットワークベースの IDPS を採用すべきである。

4.3.3.3 チューニングおよびカスタマイズ

4.3.3.2項で触れたように、ネットワークベースの IDPS では通常、検知の正確さを向上させるために詳細なチューニングおよびカスタマイズ作業が必要となる。チューニングおよびカスタマイズ機能の例としては、ポートスキャンやアプリケーション認証の試行(回数)に関するしきい値、ホスト IP アドレスやユーザ名に関するブラックリストとホワイトリスト、および警報の設定などがある。また、製品によってはコードの編集も可能である。一般に、編集できるコードはシグネチャに限られるが、それ以外のコード（ステートフルプロトコル解析の実行に使用するプログラムなど）を編集できる場合もある。

一部のネットワークベースの IDPS では、組織内にあるホストに関する情報を使用して検知の正確さを向上させることができる。たとえば、組織内の Web サーバ、メールサーバ、その他の一般的な種類のホストが使用している IP アドレスや、各ホストの提供するサービスの種類（各 Web サーバで実行されている Web サーバアプリケーションの種類およびバージョンなど）を、管理者が指定することができる場合、IDPS において警報の優先順位付けをより的確に行えるようになる。たとえば、Apache を狙った攻撃が Apache Web サーバに対して行われた場合は、同じ攻撃が異なる種類の Web サーバに仕掛けられた場合よりも高い優先度の警報を発することができる。また、一部のネットワークベースの IDPS は、脆弱性スキャンの結果を取り込み、それを用いて、遮断しなければ成功する可能性が高い攻撃がどれであるかを判断する機能を備えている。これにより、IDPS は、防止措置に関する判断と警報の優先順位付けをより正確に行うことができる。

4.3.3.4 技術的な制約

ネットワークベースの IDPS には、広範な検知能力がある一方、大きな制約がいくつかある。最も重要な制約として、暗号化されたネットワークトラフィックの解析に関するもの、高負荷トラフィックの扱いに関するもの、IDPS 自体に対する攻撃への耐性に関するものの 3 つが挙げられる。ここでは、これらの制約事項について述べる。

ネットワークベースの IDPS は、仮想プライベートネットワーク（VPN）接続、HTTPS（HTTP over SSL）および SSH セッションなど、暗号化されたネットワークトラフィックを経由して行われる攻撃を検知することができない。前述したとおり、一部のネットワークベースの IDPS には、暗号化接続の確立を分析することにより、クライアントまたはサーバのソフトウェアに既知の脆弱性があるのか、あるいは、それらの設定に誤りがあるのかを特定することができるものがある。暗号化されたネットワークトラフィック内のペイロードが十分に解析されるよう、暗号化前または復号後のペイロードを解析できる IDPS を使用すべきである。たとえば、暗号化されていないトラフィック（VPN ゲートウェイ経由で組織内に入り、ゲートウェイで復号されたトラフィックなど）を監視するためにネットワークベースの IDPS センサーを設置し、かつ、送信元または宛先ホスト上での活動を監視するためにホストベースの IDPS ソフトウェアを使用することが考えられる。

高負荷の条件下では、ネットワークベースの IDPS は十分な解析処理を実行できないことがある。特に、ステートフルプロトコル解析を使用している場合には、受動型 IDPS センサーが全てのパケットを処理することができず、インシデントの検知漏れにつながる可能性がある。インライン IDPS センサーでは、高負荷によりパケット処理のとりこぼしが発生してネットワークの可用性が阻害されることや、パケットの処理のために大きな遅延が発生して実用性が損なわれることが考えられる。こうした事態を避ける

ために、インライン IDPS センサーを使用する組織では、高負荷状態を認識することができ、特定の種類のネットワークトラフィックについては完全な解析を行うことなくセンサーを通過させることができる（部分的解析のみを行うか、解析を行わない）製品か、優先度の低いトラフィックを廃棄して負荷を軽減することができる製品を選択すべきである。多くのベンダーは、高負荷状態におけるパフォーマンスを向上させるためにセンサーを最適化する試みとして、専用ハードウェア（広帯域ネットワークカードなど）の使用、ソフトウェア構成要素の再コンパイルによる管理者設定やカスタマイズ内容の取り込みなどを行っている。ベンダーは一般に、処理可能な帯域幅の最大値によってセンサーの性能を示すが、どの製品についても、実質的な能力は、次のようないくつかの要素によって決まる。

- ネットワーク層、トランスポート層、アプリケーション層で使用されるプロトコルと、各プロトコルに対して実行される解析の綿密さ：ベンダーは、プロトコルの「典型的な」組み合わせに対して妥当な解析を実行する能力に基づいて、製品の評価を示すことが多い。個々の組織が行いたいと考える解析のレベルや、組織において実際に使用されるプロトコルの組み合わせは、ベンダーによってテストが実施された際の条件と大きく異なることがある。
- 接続の継続時間：たとえば、短時間の接続が複数回続けて発生するよりも、長時間の接続が 1 回だけ発生するほうが、センサーのオーバーヘッドは小さくなる場合がある。
- 同時接続の数：センサーには通例、状態を同時に追跡することができる接続の数に制限がある。

IDPS センサーは、さまざまな種類の攻撃を受ける可能性がある。攻撃者は、DDoS（分散型サービス妨害）攻撃のように極端に大量のトラフィックや、通常と異なる活動（異常なパケット分割など）を発生させ、センサーのリソース枯渇やクラッシュを引き起こそうと試みることがある。また、*目くらまし*と呼ばれる攻撃手法では、短期間に多数の警報を発生させる可能性のあるネットワークトラフィックを発生させる。このトラフィックは、IDPS センサーの一般的な設定を悪用するように特別に細工されているのが一般的である。多くの場合、目くらましのトラフィックは、特定の標的を実際に攻撃することを目的としていない。「真の」攻撃は、この目くらましのトラフィックと同時に、別途行われる。攻撃者が目くらましを行う意図は、IDPS を何らかの形で機能不全に陥らせるか、警報の数を極端に増やすことにより、真の攻撃に対する警報を見落とさせることである。一般的な DDoS 攻撃や目くらましのツールおよび手法が使用された場合、多くの IDPS センサーには、それを認識して管理者に警報を発し、以降の活動を無視してセンサーの負荷を軽減する機能がある。製品の選定時には、攻撃によって機能不全に陥ることを防ぐ機能を備えたものを採用すべきである。

4.3.4 防止機能

ネットワークベースの IDPS センサーは、さまざまな防止機能を備えている。それらをセンサーの種類別に示すと次のようになる。

- **受動型のみ**
  - **既存TCPセッションの終了**：受動型センサーは、既存セッションの両エンドポイントにTCPリセットパケットを送信してセッションの終了を試みることができる。この方法は、*セッションスナイピング（session sniping）*と呼ばれることもある[24]。これは双方のエンドポイントに対し、その反対側のエンドポイントが接続を終了しようとしているかのように見せかける手法である。攻撃の成功前

[24] インラインセンサーでもこの方法を使用することは可能だが、インラインセンサーで実行できる他の方法と比べて、はるかに効果が弱いため、実際にはインラインセンサーではほとんど使われない。

に、いずれかのエンドポイントが接続を終了すれば防止の目的は達成されるが、実際には、攻撃トラフィックを観測して解析し、攻撃を検知し、それからネットワークを経由してリセットパケットをエンドポイントに送信しなければならないため、パケットの到達が間に合わないことが多い。また、この手法を適用できるのはTCPのみであるため、UDPやICMPなど他の種類のパケットによって実行される攻撃に対しては使用できない。より新しい効果の高い防止機能が登場した現在では、セッションスナイピングはあまり使われていない。

■ **インラインのみ**

– **インラインファイアウォール処理の実行**：ほとんどのインライン IDPS センサーは、疑わしいネットワーク活動を廃棄または拒否するために使用することができるファイアウォール機能を備えている。

– **使用帯域幅の調整**：特定のプロトコルが不適切な目的（DoS 攻撃、マルウェア配布、ピアツーピアファイル交換など）に使用されている場合、インライン IDPS センサーによっては、当該プロトコルで使用できるネットワーク帯域幅を制限することができる。これにより、他のリソースの使用帯域が、そのような不適切な使用から悪影響を受けるのを防止できる。

– **悪意あるコンテンツの改変**：2.2項で説明したように、一部のインライン IDPS センサーには、パケットの一部分をサニタイズし（悪意のあるコンテンツを無害なコンテンツで置き換え）、無害化されたパケットを宛先に送る機能がある。プロキシとして動作するようなセンサーは、すべてのトラフィックを自動的に正規化（アプリケーションペイロードの再パッケージ化など）する場合がある。これには、パケットヘッダや一部のアプリケーションヘッダが関係する攻撃を（IDPS が検知しないものも含め）サニタイズする効果がある。また、センサーによっては、感染した添付ファイルを電子メールから除去したり、その他の悪意のあるコンテンツの個別の断片をネットワークトラフィックから削除したりすることもできる。

■ **受動、インラインの両方**

– **他のネットワークセキュリティ装置の設定変更**：多くの IDPS センサーは、ファイアウォール、ルータ、スイッチなどのネットワークセキュリティ装置に対し、特定の種類の活動を阻止したり別の場所へ誘導したりするように設定変更指示を出すことができる。これは、外部の攻撃者をネットワーク内に入らないようにする場合や、侵害された内部のホストを隔離（たとえば隔離用 VLAN に移動）する場合など、いくつかの状況において役立つ。ただし、この手法が有効なのは、ネットワークトラフィックのパケットヘッダにネットワークセキュリティ装置で通常認識できるような特徴（IP アドレス、ポート番号など）がある場合に限られる。

– **サードパーティ製プログラムまたはスクリプトの実行**：一部の IDPS センサーには、悪意ある特定の活動を検知した場合に、管理者が指定したスクリプトまたはプログラムを実行する機能がある。これにより、管理者が実行させたい任意の防止措置（他のセキュリティ装置の設定を変更して悪意のある活動を阻止するなど）を発動することができる。サードパーティ製プログラムやスクリプトは、管理者が必要としている防止措置を IDPS がサポートしていない場合に最もよく使用される。

ほとんどの IDPS センサーでは、警報の種類ごとに管理者が防止機能の設定を指定することができる。設定により指定できる事項には、防止の有効化／無効化の切り替えや、使用する防止機能の選択などがある。また、学習モードまたはシミュレーションモードを備えた IDPS センサーもある。これは、全ての防止措置を抑止し、その代わりに、防止措置が実行されるべき時点でその旨を示すモードである。こ

のようなモードを利用することにより、管理者は防止機能を有効化する前に、監視を行いながら防止機能の設定を微調整することができ、無害な活動を誤って阻止してしまうリスクを低減することができる。

4.4 管理

ほとんどのネットワークベースの IDPS テクノロジーは、いずれもよく似た管理機能を備えている。この項では、管理の主要な側面（導入、運用、保守）について述べ、それらの作業を効果的かつ効率的に実行するための推奨事項を示す。

4.4.1 導入

ネットワークベースの IDPS 製品を選定した場合、管理者がアーキテクチャの設計、IDPS 構成要素のテスト、構成要素に対するセキュリティ対策の実施を行った後に、IDPS を導入する必要がある。3.3.1項で示した内容に付け加える事項を次に示す。

- **アーキテクチャ設計**：ネットワークベースの IDPS に特有の考慮事項として、ネットワーク上のどこにセンサーを設置するかという問題がある。これには、必要なセンサーの個数、各センサーのモードをインライン／受動型のいずれにするか、および、受動型センサーをネットワークに接続する方法（IDS ロードバランサ、ネットワークタップ、スイッチのスパニングポートなど）の判断も含まれる。
- **構成要素のテストおよび設置**：ネットワークベースの IDPS を導入する際には、ネットワークを一時的に停止する必要が生じる可能性がある。これは主としてインラインセンサーを設置する場合であるが、場合によっては受動型センサーの設置時にもいくつかの理由により、同様のことが発生する可能性がある。たとえば、ネットワークタップや IDS ロードバランサを設置したり、スイッチの設定を変更してスパニングポート機能を有効化したりするためにネットワークを停止する必要がある場合がある。
- **IDPS の構成要素のセキュリティ保護**：受動型およびインライン型のいずれのセンサーについても、管理者は、ネットワークトラフィックの監視に使用するネットワークインタフェースに IP アドレスが割り当てられないようにすべきである（IDPS 管理用を兼ねるネットワークインタフェースを除く）。監視インタフェースに IP アドレスを割り当てることなくセンサーを稼働させる設定は、*ステルスモード*と呼ばれる。ステルスモードにすると、他のホストから IDPS センサーに対して接続を開始することができないため、センサーのセキュリティが向上する。これにより、センサーが攻撃者に見つけられるのを防ぎ、攻撃を受ける可能性を小さくすることができる。ただし、攻撃者が IDPS センサーの存在を知り、防止措置の特徴を分析することで具体的な製品まで特定する可能性もある。攻撃者による分析方法の例としては、保護されたネットワークを監視し、どのスキャンパターンが特定の反応を引き起こすかを判断したり、特定のパケットヘッダフィールドに設定される値を調べたりすることが考えられる。

4.4.2 運用および保守

ネットワークベースの IDPS の運用および保守作業は、3.3.2項に示した一般的な説明のとおりに行う。

4.5 まとめ

ネットワークベースの IDPS は、特定のネットワークセグメントまたはネットワーク装置のネットワークトラフィックを監視し、ネットワーク、トランスポートおよびアプリケーションの各プロトコルを解析して疑わし

い活動を特定する。ネットワークベースの IDPS を構成する要素のうちセンサー以外の要素は、他の種類の IDPS テクノロジーの要素と似ている。ネットワークベースの IDPS のセンサーは、1 つ以上のネットワークセグメントにおけるネットワーク活動の監視・解析を行う。センサーの形態としては、アプライアンスベースのセンサー（IDPS センサー用に最適化された専用ハードウェアおよびソフトウェアで構成される）とソフトウェアのみのセンサー（特定の仕様を満たすホストにインストールして使用する）の 2 種類がある。

ネットワークベースの IDPS を設置する場合には、可能なかぎり、管理ネットワークを使用すべきである。独立の管理ネットワークなしで IDPS を設置する場合は、IDPS の通信を保護するために VLAN が必要かどうかを検討すべきである。構成要素に対して適切なネットワークを選択することに加え、管理者は IDPS センサーをどこに設置するかを決定しなければならない。センサーの設置形態としては、インラインセンサー（監視対象ネットワークトラフィックが必ずセンサーを通過するように設置）と受動型センサー（実際のネットワークトラフィックのコピーを監視するように設置）の 2 種類のモードがある。一般に、防止手段を使用する場合はセンサーをインラインで設置し、使用しない場合は受動型で設置すべきである。

ネットワークベースの IDPS は、多種多様なセキュリティ機能を提供する。製品によっては、ネットワークを介して通信を行うホストの稼働 OS やアプリケーションのバージョンなどといった情報を収集する機能がある。また、ネットワークベースの IDPS は、検知したイベントに関連するデータを詳細なログとして記録することができ、多くの製品ではパケットを採取することもできる。ネットワークベースの IDPS には、詳細かつ広範な検知機能を備えるものが多い。ほとんどの製品では、シグネチャベースの検知、アノマリベースの検知、ステートフルプロトコル解析を組み合わせることで、よく使用されるプロトコルの綿密な解析を実行している。複数の検知手法を組み合わせて使用することにより検知の正確さが向上するため、ネットワークベースの IDPS を使用する際には、そのような検知機能の組み合わせを提供する製品を採用すべきである。さらに、一般的な回避テクニックに対処できる能力も備え、いっそう正確な検知を可能にしたネットワークベースの IDPS を使用することが望まれる。

ネットワークベースの IDPS には、大きな制約がいくつかある。まず、暗号化されたネットワークトラフィックに含まれる攻撃は検出することができない。したがって、暗号化前または復号後のトラフィックを監視できる位置に設置するか、暗号化されていない活動を監視するためにエンドポイントにおいてホストベースの IDPS を併用すべきである。次に、高負荷の条件下では十分な解析処理を実行できないことが多い。したがって、インラインセンサーを使用する場合は、高負荷状態を認識することができ、特定種類のトラフィックについては十分な解析をせずにセンサーを通過させることや、優先度の低いトラフィックを廃棄して負荷を軽減させることができる製品を選択すべきである。さらに、ネットワークベースの IDPS はさまざまな種類の攻撃を受けやすく、攻撃のほとんどは、大量のトラフィックを伴うものである。攻撃によって機能不全に陥ることを防ぐ設計が施された製品を選択すべきである。また、受動型センサーおよびインラインセンサーのネットワークトラフィック監視用インタフェースには、IP アドレスを割り当てないようにすべきである（トラフィック監視用と IDPS 管理用を兼ねるネットワークインタフェースを除く）。

ネットワークベースの IDPS センサーは、さまざまな防止機能を備えている。多くの受動型センサーには、TCP リセットにより TCP セッションの終了を試みる機能があるが、この手法は対応が遅れることが多いのに加え、UDP や ICMP など TCP 以外のセッションに対応できない。インラインセンサーでのみ使用できる防止機能として、インラインファイアウォール処理、使用帯域幅の調整、悪意あるコンテンツの改変などがあり、いずれも特定の状況において効果的である。受動型およびインラインセンサーの

いずれにも、他のネットワークセキュリティ装置の設定を変更する機能や、付加的な防止措置を発動するためにサードパーティ製プログラムまたはスクリプトを起動する機能がある。

（本ページは意図的に白紙のままとする）

5. 無線IDPS

無線 IDPS は、無線ネットワークのトラフィックを監視し、無線ネットワークプロトコルを解析して、当該プロトコル自体に関わる疑わしい活動を特定する。このセクションでは、無線 IDPS テクノロジーについて詳しく論じる。まず、以降の内容を理解するための基礎知識として無線ネットワーキングの概要を説明する。次に、無線 IDPS の主要な構成要素を示し、それらの要素の導入に通常使用されるアーキテクチャについて説明する。また、疑わしい活動の特定および阻止に使用される方法を含め、各テクノロジーのセキュリティ機能について深く掘り下げる。そのあとは、導入および運用に関する推奨事項を含め、各テクノロジーの管理機能について説明する。

5.1 無線ネットワーキングの概要

*無線ネットワーキング*では、無線通信機能を備えた装置により、物理的にネットワークに接続することなくコンピューティングリソースを使用することができる。これらの装置は、無線ネットワークインフラストラクチャから特定の距離内（「範囲」と呼ばれる）にあればよい。無線 LAN（WLAN：Wireless Local Area Network）)は、無線通信によるデータ交換が可能な限定された地理的区域に含まれる無線ネットワークノードの集合である。一般に、WLAN はオフィスビル内や企業の敷地内などのかなり限定された範囲内にある装置によって使用され、ユーザの機動性を高めるために既存の有線 LAN の延長として導入される。

この項では、無線ネットワーキングの概要を説明する。5.1.1項では、広く使われている各種WLAN標準の概要を示す。5.1.2項では、WLANの基礎的構成要素について説明する。最後に、5.1.3項では、WLANが直面する主な脅威について簡単に述べる。ここでは、無線IDPSに関する以降の記述を理解するための基礎知識として、無線ネットワーキングの概略を示すにとどめる [25]。

5.1.1 WLANに関する標準

ほとんどのWLANでは、IEEE（Institute of Electrical and Electronics Engineers：米国電気電子学会）802.11 ファミリのWLAN規格が採用されている [26]。最も広く普及しているWLAN無線通信の標準は、IEEE 802.11b、IEEE 802.11g（ともに 2.4 GHz帯を使用）、およびIEEE 802.11a（5 GHz帯を使用）である。IEEE 802.11a／b／g規格は、総称的にWEP（Wired Equivalent Privacy）と呼ばれるセキュリティ面における特徴を有するが、WEPには、既に十分に文書としてまとめられているセキュリティ上の問題が存在する。それらへの対策として、IEEE 802.11a／b／gと組み合わせることにより動作するセキュリティ構成要素の仕様を定めたIEEE 802.11iが策定されている。

一方、WLAN機器・ソフトウェアのベンダーにより構成される非営利の業界団体Wi-Fi Allianceが、別のWLAN規格群を策定している [27]。IEEEが 802.11i正式版に向けた作業を進めている間に、Wi-Fi

---

[25] この文書では、WLAN 以外の無線ネットワーキング形態（Bluetooth など）に適用される IDPS テクノロジーについては説明しない。Bluetooth IDPS 製品はまだ提供され始めたばかりであり、2006 年後半の時点では提供される機能も少ない（機器の検出、サービスの列挙、限定的な脆弱性スキャンのみ）。また、WLAN の IEEE 802.11n 規格は 2006 年後半の時点では正式な内容が確定していないため、それに基づくテクノロジーについても言及しない。ただし、この項に示す推奨事項は、IEEE 802.11n ベースの WLAN に対応した無線 IDPS テクノロジーにも概ね適用できるものと考えられる。

[26] IEEE 802.11 規格の詳細と、無線ネットワークセキュリティに関するその他の側面については、NIST SP 800-97『*Establishing Wireless Robust Security Networks* (無線ロバストセキュリティネットワークの確立) *:A Guide to IEEE 802.11i*』および NIST SP 800-48『*Wireless Network Security: 802.11, Bluetooth and Handheld Devices*』（http://csrc.nist.gov/publications/nistpubs/index.html）を参照のこと。

[27] Wi-Fi Alliance の詳細については、同団体の Web サイト（http://www.wi-fi.org/）を参照のこと。

AllianceはWPA（Wi-Fi Protected Access）と呼ばれる暫定的なソリューションを策定した。2002 年 10 月に公開されたWPA規格の内容は、基本的には、その時点でIEEE 802.11i草案に盛り込まれていた要件のサブセットである。WPAでは、WLAN通信のセキュリティがWEPよりも強化されている。IEEE 802.11i修正案の承認と同時に、Wi-Fi Allianceは、IEEE 802.11iの要件に対応する能力を備えた相互運用可能な装置についての規定であるWPA2 を公開した。WPA2 のセキュリティ管理策は、WPAおよびWEPよりもさらに強化されている。

5.1.2 WLANの構成要素

IEEE 802.11 WLAN のアーキテクチャを構成する基本的な要素は次の 2 つである。

- **ステーション（STA）**：「*STA*」は、無線エンドポイント装置である。STA の典型例は、ノート型パソコン、PDA（personal digital assistant：携帯情報端末）、携帯電話、および IEEE 802.11 の機能を持つその他の家庭用電子機器である。
- **アクセスポイント（AP）**[28]：「*AP*」は、STAと*ディストリビューションシステム*（DS：Distribution System）を論理的に接続するものであり、通常、DSは組織の有線インフラストラクチャである。DSは、STAが組織の有線LANやインターネットなどの外部ネットワークと通信するための手段である。図 5-1 は、AP、STA、DSの関係を例示したものである。

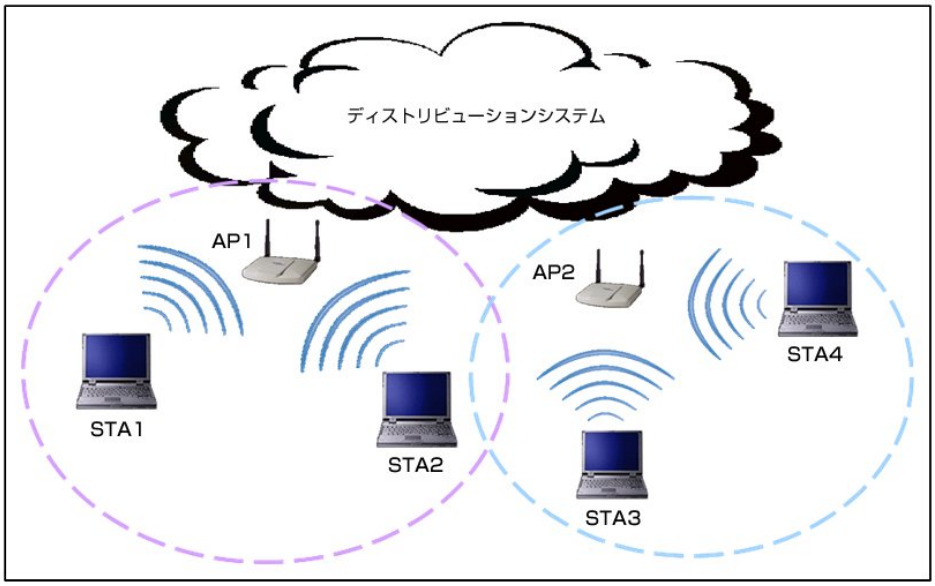

図 5-1. 無線 LAN アーキテクチャの例

WLAN の構成には無線スイッチが含まれることもある。「*無線スイッチ*」は、AP と DS の間を仲介する装置であり、管理者が WLAN インフラストラクチャの管理を行うのを支援することを目的としている。無線スイッチを使用しない WLAN では、AP が直接 DS に接続する。

また、IEEE 802.11 の標準では、次の 2 つの WLAN アーキテクチャが定義されている。

[28] 技術的には、AP も STA の一種である。文献によっては、AP STA と非 AP STA を区別している。この文書では、非 AP STA だけを STA と呼ぶことにする。

- **アドホックモード**：「*アドホックモード*」は、APを使用しないモードであり、「ピアツーピアモード」とも呼ばれる。このモードでは、2つ以上のSTAが直接、相互に通信を行う。
- **インフラストラクチャモード**：「*インフラストラクチャモード*」では、無線STAがAPによってDS（多くの場合は有線ネットワーク）に接続される。

WLAN上にある個々のAPおよびSTAは、それぞれの*MAC（Media Access Control：媒体アクセス制御）アドレス*によって識別される。MACアドレスは、無線ネットワークインタフェースカードに割り当てられる一意の48ビット値である。MACアドレスの一部分は、カードのベンダーを特定するために使用され、残りの部分は当該ベンダーにおけるシリアル番号として機能する。理想的には、すべての無線機器をMACアドレスで一意に識別できるはずであったが、実際には、MACアドレスの偽造は比較的容易である。

ほぼすべての組織において、WLANはインフラストラクチャモードで使用される。1つのWLANにある個々のAPには、*SSID*（Service Set Identifier：サービスセット識別子）と呼ばれる名前が割り当てられる。STAはSSIDによって、あるWLANと別のWLANを区別する。SSIDは、APによって平文でブロードキャストされるため、電波を受信している無線機器はすべて、その有効範囲内にある各WLANのSSIDを容易に知ることができる[29]。組織はWLANをいっさい持たない場合、1つのWLANを持つ場合、複数のWLANを持つ場合がある。また、ある組織の施設が別組織のWLANの有効範囲内にあることも多い。

5.1.3 WLANにとっての脅威

無線ネットワークと有線ネットワークが直面する脅威の種類は概ね同じであるが、一部の脅威の相対的なリスクは、無線と有線とでは大きく異なる。たとえば、無線の攻撃を仕掛けるには通常、攻撃者自身または攻撃者によって置かれた装置が、物理的に攻撃対象の無線ネットワークの近くに存在する必要がある。有線ネットワークに対する攻撃の多くは、遠く離れた任意の場所から実行可能である。ただし、認証を必要としないまたは弱い方式の認証だけでアクセスできるように設定されているWLANが多いため、そのようなWLANの近くにいる攻撃者にとって、いくつかの種類の攻撃（中間者攻撃など）を実行することは非常に容易である。

WLANに対する脅威は、STAとAPの間（または、アドホックモードにおける2つのSTA間）の無線リンクへのアクセスを有する攻撃者に関するものがほとんどである。多くの攻撃は、攻撃者がネットワーク通信を傍受する、あるいは、通信内容に別のメッセージを挿入する能力に依拠している。これは、無線LANの保護と有線LANの保護のあいだの最も大きな違いを浮き彫りにする。すなわち、ネットワーク通信へのアクセスおよびその改変のしやすさの違いである。有線LANの場合、攻撃者はLANに物理的にアクセスするか、リモートからLAN上のシステムに侵入する必要がある。ところが無線LANの場合は、単に攻撃の対象となるWLANインフラストラクチャの有効範囲内に入りさえすればよい[30]。

---

[29] 互いの圏内にある2つのWLANが同じSSIDを使用する場合がある。その場合、各WLANは、それぞれのAPのMACアドレスによって区別することができる。

[30] WLANに対する脅威の詳細については、NIST SP 800-97『*Establishing Wireless Robust Security Networks*（無線ロバストセキュリティネットワークの確立）*: A Guide to IEEE 802.11i*』およびNIST SP 800-48『*Wireless Network Security: 802.11, Bluetooth and Handheld Devices*』（http://csrc.nist.gov/publications/nistpubs/index.html）を参照のこと。

5.2 構成要素とアーキテクチャ

この項では、一般的な無線 IDPS ソリューションの主要な構成要素について説明し、それらの構成要素のための最も一般的なネットワークアーキテクチャを示す。また、特定の構成要素の設置についての推奨事項を提示する。

5.2.1 典型的な構成要素

無線 IDPS を構成する典型的な要素は、ネットワークベースの IDPS と同様で、コンソール、データベースサーバ（任意）、管理サーバ、およびセンサーである。これらのうちセンサー以外の構成要素が備える機能は、IDPS の両方の種類におけるものと基本的に同じである。無線センサーは、ネットワークベースの IDPS センサーと同様の基本的役割を担うが、無線通信を監視することの複雑さから、ネットワークベースの IDPS センサーとは大きく異なる方法で機能する。

ネットワークベースのIDPSが監視対象ネットワーク上の全てのパケットを観測できるのに対し、無線IDPSは、トラフィックをサンプリングすることにより動作する。監視すべき周波数帯は 2 つ（2.4 GHz、5 GHz）あり、それぞれが複数のチャネルに分割されている [31]。今のところ、ある周波数帯におけるすべてのトラフィックを同時に 1 基のセンサーで監視することは不可能であり、1 基のセンサーで同時に監視できるのは 1 チャネルのみである。異なるチャネルを監視するには、いったん無線の受信を停止し、チャネルを変更してから無線の受信を再開する必要がある。同じチャネルの監視を長く継続するほど、それ以外のチャネルで行われる悪意のある活動を見落とす可能性は大きくなる。見落としを防ぐために、センサーは頻繁にチャネルを変更し（「*チャネルスキャン*」という）、各チャネルを毎秒数回ずつ監視するのが一般的である。チャネルスキャンの必要性を減らすか、あるいはなくす手段として、複数の電波と高出力アンテナを使用（1 組の電波／アンテナで 1 つのチャネルを監視）する特殊なセンサーを利用することができる。高出力アンテナは感度が高いため、通常のアンテナよりも広い範囲を監視対象とすることもできる。また、IDPSの実装を工夫して、有効範囲を重複させた複数のセンサー間でスキャンパターンを調整することにより各センサーの監視対象チャネル数を減らす方法もある [32]。

利用可能な無線センサーには、次のようにいくつかの形態がある。

- **専用**：専用センサーは、無線 IDPS の機能を持つが、ネットワークトラフィックを送信元から宛先へと送る機能は持たない装置である。多くの場合は、完全に受動的に動作し、何らかの無線周波数

---

[31] IEEE 802.11b／g は 14 チャネルをサポートしている。そのうち 11 チャネルは、米国国内での使用を承認されたもの、残り 3 チャネルは国際的に使用を承認されたものである。IEEE 802.11a は、米国国内用として承認された 12 チャネルと、国際的に使用を承認された 4 チャネルをサポートしている。攻撃者によっては、標準以外のチャネルや IEEE 802.11 以外の周波数帯（900 MHz、4.9 GHz など）を使用することがある。WLAN の一般的な周波数帯およびチャネルと比べ、それらの周波数帯を使った活動が検知される可能性が小さいためである。たとえば、攻撃者が有線ネットワークに物理的に許可なくアクセスできる場合、無線機器を有線ネットワークに設置し、一般には使われない周波数帯を使用して、情報を組織から攻撃者に送信させるようにすることができる。スペクトラムアナライザ製品を使用すると、さまざまな周波数帯における活動を監視して攻撃を特定したり、悪意のない電波障害の原因（コードレスホン、電子レンジなど）を発見したりすることができる。2006 年中頃時点では、スペクトラムアナライザ機能を備える IDPS 製品はほとんどない。しかし、よく使用される周波数帯を監視できる携帯用スペクトラムアナライザがいくつかの企業から発売されている。そのような製品の詳細については、この文書では扱わない。

[32] どのチャネルを監視するかは、組織において決定する必要がある。前述のとおり、攻撃者は一般的でないチャネル（米国国内用として承認されていない IEEE 802.11a／b／g チャネルなど）を使用することが多い。そのようなチャネルを監視することにより、悪意のある活動を検知することができる反面、組織の WLAN と典型的な悪意の WLAN（不正アクセスポイントなど）の両方が使用するチャネルに対する監視時間の割合が低下する可能性もある。各組織において想定される脅威の可能性を考慮し、脅威に最もよく対処することができるチャネルスキャン計画を選択すべきである。

（RF）監視モードで無線ネットワークトラフィックを傍受する。センサー自身が監視対象のトラフィックを解析するものと、解析のためにネットワークトラフィックを管理サーバに転送するものがある。専用センサーは有線ネットワーク（たとえば、センサーとスイッチの間の Ethernet ケーブル）に接続されるのが一般的である。一般に、専用センサーは次のいずれかの設置方法を想定して設計されている。

- **固定** — 特定の場所に設置され、組織のインフラストラクチャ（電源、有線ネットワークなど）に依存する場合が多い [33]。通常、固定センサーはアプライアンスベースである。
- **モバイル** — 移動中でも使用できるように設計されている。たとえば、セキュリティ管理者が移動センサーを持って組織の建物内や敷地内を歩き回って不正APを探す場合に使用する。アプライアンスベースのものと、ソフトウェアベースのもの（RF監視機能を持つ無線NICを装備したノート型PCなどにインストールして使用）がある [34]。

■ **AP とのバンドル**：いくつかのベンダーが、IDPS 機能を付加した AP を提供している。バンドル AP の場合、ネットワークアクセスの提供と、複数のチャネルあるいは周波数帯を監視して悪意のある活動を検知する処理の両方を時分割で行う必要があるため、専用センサーと比べると検知能力は劣ることが多い。IDPS が監視する必要のある対象が 1 つの周波数帯およびチャネルだけであれば、バンドル製品でも実用に耐えるセキュリティとネットワークの可用性が得られる可能性がある。IDPS が、複数の周波数帯またはチャネルを監視する必要がある場合、センサーがチャネルスキャンを実行しなければならないために、主として使用する周波数帯やチャネルに対してセンサーを一時的に利用することができなくなり、センサーの AP としての機能が低下する。

■ **無線スイッチとのバンドル**：無線スイッチは、管理者による無線機器の管理および監視作業を支援するための装置であり、補助的な機能としてある程度の無線 IDPS 機能を備えているものもある。一般に、無線スイッチの検知能力は、AP にバンドルされたセンサーや専用センサーほど強力ではない。

専用センサーは、検知処理のみに専念でき、無線トラフィックを伝送する必要がないため、AP や無線スイッチにバンドルされた無線センサーよりも検知能力が高いのが一般的である。しかし、バンドルされたセンサーは既存ハードウェアにインストールできるのに比べ、専用センサーを使用するには新たにハードウェアやソフトウェアを調達する必要があるため、購入、インストール、保守のコストが高くなることが多い。そのため、無線 IDPS センサーの選定時にはセキュリティとコストの両面を考慮する必要がある。

ノート型 PC などの STA にインストールして使用するホストベースの無線 IDPS センサーソフトウェアも、一部のベンダーから提供されている。センサーソフトウェアは、当該 STA の有効範囲内で行われる攻撃や STA の設定ミスを検知し、その情報を管理サーバに報告する。また、当該 STA から無線インタフェースへのアクセスを制限するなど、STA に対するセキュリティポリシーの適用を行うことができる場合がある。ホストベースの IDPS 製品については、セクション7で詳しく述べる。

---

[33] 一部のセンサーでは、Power over Ethernet（PoE）と呼ばれる IEEE 802.3af プロトコルを使用することができる。このプロトコルにより、有線ネットワークの接続に使用する Ethernet ケーブルを通じた電力の供給が可能になる。PoE は、一部の専用センサーおよびアクセスポイントに実装されている。PoE の詳細については、http://www.ieee802.org/3/af/index.html を参照のこと。

[34] 移動センサーは、エンタープライズ向け無線 IDPS ソリューションの一部として提供される場合もあれば、管理者が直接管理および監視を行うスタンドアロン装置である場合もある。

5.2.2 ネットワークアーキテクチャ

無線 IDPS の構成要素は、図 5-2 のように有線ネットワークで相互に接続されるのが普通である。ネットワークベースの IDPS と同様、無線 IDPS の構成要素間の通信には、独立の管理ネットワークを使用することも、組織の標準ネットワークを使用することもできる。無線ネットワークと有線ネットワークは、すでに厳密な管理のもとに分離されていると考えられるため、無線 IDPS の構成要素間の接続に管理ネットワークと標準ネットワークのいずれを使用しても問題はないといえる。また、無線 IDPS センサーによっては（特にモバイルセンサー）、有線ネットワーク接続を必要とせずスタンドアロンで使用される場合もある。

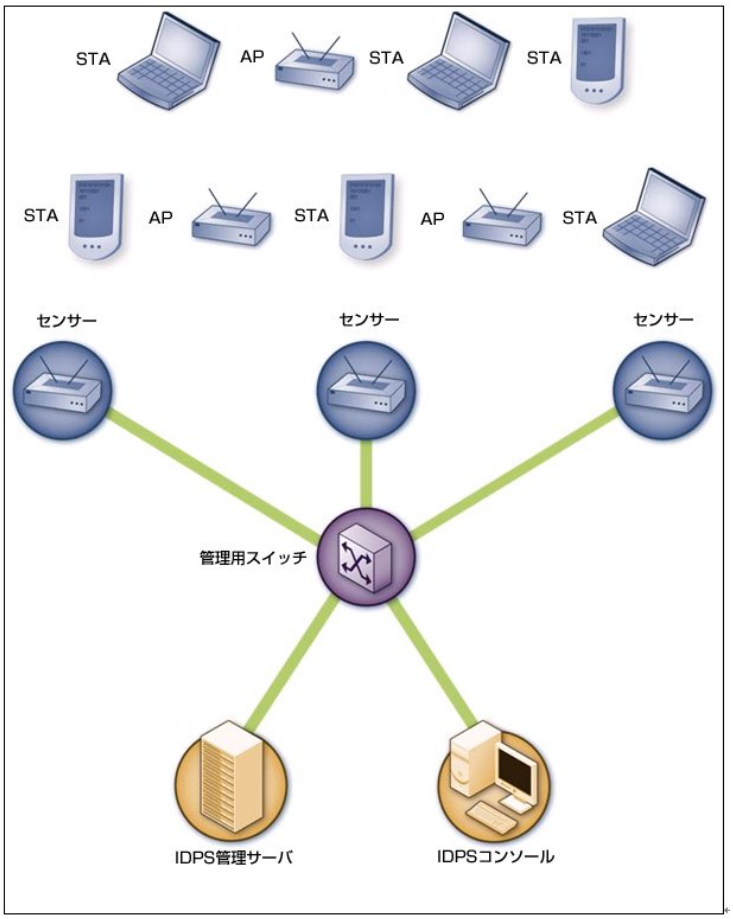

図 5-2. 無線 IDPS のアーキテクチャ

5.2.3 センサーの設置場所

無線 IDPS を導入する際にセンサーの設置場所を選択することは、他のあらゆる種類の IDPS センサーの設置場所を決めることとは本質的に異なる問題である。WLAN を使用する組織では、組織の WLAN（AP と STA の両方。ノート型 PC や PDA など可搬性のある要素を含むことも多い）が使用する無線周波数の有効範囲を監視するように、無線センサーを設置すべきである。また、多くの組織では、施設内で WLAN 活動がまったくないはずの物理的な場所や、組織の WLAN が使用しないはずのチ

ャネルおよび周波数帯を監視対象としたセンサーも設置して、不正 AP やアドホック WLAN を検知することも必要になる。他にも、無線センサーの設置場所を選択するときに、次のような考慮事項がある。

- **物理的セキュリティ**：センサーは、通常、閉鎖的な場所（配線室など）ではなく、開放的な場所（廊下の天井、会議室など）に設置される。そのほうが、はるかに広い範囲を監視できるためである。設置場所が屋外になることもある[35]。一般に、屋内の開放的な場所または屋外に設置されたセンサーは、そうでないものと比べて物理的な脅威にさらされやすい。物理的な脅威が深刻であると考えられる場合は、耐タンパ性のあるセンサーを採用するか、物理的にアクセスされる可能性がより小さい場所（監視カメラの視界内など）に設置するようにする必要がある。

- **センサーの有効範囲**：センサーの実際の有効範囲は、周囲の施設（壁、ドアなど）によって異なる。一部の無線 IDPS ベンダーは、建物の間取り図および壁、ドアなど建材の減衰特性を解析してセンサーの効果的な配置を決定するためのモデリングソフトウェアを提供している。また、センサーの有効範囲は、施設内の人間の居場所やその他の変動する特性によっても変化するため、センサーどうしの有効範囲がいくらか重なり合うように配置すべきである（たとえば、20%以上は重複させるなど）。

- **有線ネットワーク接続**：通常、センサーは有線ネットワークに接続する必要がある。有線ネットワークが敷設されていない場所にセンサーを配備する場合は、そこまで有線ネットワークを延長することが必要になる可能性がある。このことが問題になるのは、通常、組織の施設のうち WLAN の有効範囲外にある部分を監視する場合などに限られる。

- **コスト**：本来であれば、組織内にある施設のあらゆる場所にセンサーを設置して完全な無線監視を行うのが理想である。しかし、それには膨大な数のセンサーが必要となる可能性がある。特に、開放的な敷地が大きく広がる環境などでは、そうである。WLAN への脅威の大きさと、センサーの購入、配備、保守のコストとを比較して、リスクを許容可能なレベルに抑えられるようなソリューションを策定すべきである。たとえば、組織の WLAN の有効範囲全体には固定センサーを配備し、それ以外の場所についてはモバイルセンサーで定期的にチェックするといった方法が考えられる。

- **AP および無線スイッチの設置場所**：組織における他の要件をバンドルのソリューション（AP 上の無線 IDPS ソフトウェアなど）によって満たすことができる場合、AP および無線スイッチの設置場所が特に重要になる。これは、それらの装置に無線 IDPS ソフトウェアが導入される可能性があるためである。

5.3 セキュリティ機能

無線 IDPS は、いくつかの種類のセキュリティ機能を備えている。無線 IDPS は、比較的新しい形態の IDPS であるため、現状では製品によって機能に大きな差があるが、時間の経過に従い、しだいに製品の機能が整合してくるものと考えられる。一般的なセキュリティ機能を、ここでは情報収集、ログの記録、検知、および防止の 4 つに分け、それぞれについて5.3.1項～5.3.4項で説明する。

5.3.1 情報収集機能

ほとんどの無線 IDPS は、無線機器の情報を収集する機能を備えている。たとえば、次のような情報収集機能がある。

[35] 屋外向けに、環境的な脅威に対する耐性を通常よりも強化した特殊なセンサーも入手可能である。

- **WLAN機器の特定**：ほとんどのIDPSセンサーには、AP、WLANクライアント、アドホック（ピアツーピア）クライアントを含む観測されたWLAN機器のインベントリ（目録）を作成・維持する機能がある。このインベントリは一般に、SSIDおよび装置の無線ネットワークカードに割り当てられているMACアドレスに基づいて作成される。MACアドレスの最初の部分は、カードのベンダーを示す[36]。センサーによっては、なりすましの可能性があるMACの情報に頼らず、観測したトラフィックを対象にフィンガープリンティング手法も併用してベンダーを確認するものがある。インベントリは、新しいWLAN機器の追加や既存機器の取り外しを認識するためのプロファイルとして使用することができる。
- **WLAN の特定**：ほとんどの IDPS センサーには、観測した各 WLAN を SSID で識別し、それらの状態を追跡する機能がある。管理者は、識別された WLAN を承認済みの WLAN、近接する無害の WLAN（同じ建物にある別の組織など）、および不正 WLAN に分類することができる。この情報は、新しい WLAN を識別したり、特定したイベントへの対応の優先順位を決定したりするために使用することができる。

5.3.2 ログ記録機能

無線 IDPS は一般に、検知したイベントに関連するデータを詳細なログとして記録する。このデータは、警報の妥当性の確認、インシデントの調査、および、IDPS において検知されたイベントとその他のログ生成ソースにおいて検知されたイベントとの相関をとるのに使用することができる。無線 IDPS のログに記録される一般的なデータフィールドには、次のようなものがある。

- タイムスタンプ（通常は日付および時刻）
- イベントまたは警報の種類[37]
- 優先度または重大度のレベル
- 送信元 MAC アドレス（このアドレスからベンダーを特定できることが多い）
- チャネル番号
- 当該イベントを観測したセンサーの ID
- 実行された防止措置（該当する場合）

5.3.3 検知機能

無線 IDPS は、WLAN プロトコルレベル（主として IEEE 802.11a／b／g／i の各プロトコルの通信を検査することにより）における攻撃、設定ミス、ポリシー違反を検知する。それよりも上位レベルの通信（IP アドレス、アプリケーションペイロードなど）については関知しない。検知の方法は製品によって異なり、単純なシグネチャベースの検知だけを行うものと、シグネチャベースの検知、アノマリベースの検知、ステートフルプロトコル解析の手法を組み合わせて使用するものがある。より広範かつ正確な検知がで

[36] STA によっては、以前にアクセスした WLAN を特定しようとして複数の SSID を送信するものがある。

[37] 製品によっては Wireless Vulnerabilities and Exploits（WVE）データベースの ID を使用する。このデータベースには、無線プロトコルおよび無線製品の脆弱性、ならびに、それらの脆弱性に関する既知の悪用手法に関する情報が登録されている。WVE データベースは、http://www.wve.org/にある。

きるよう、複数の手法を組み合わせて使用する無線 IDPS 製品を採用すべきである。この項では、次の観点から検知機能について説明する。

- 検知されるイベントの種類
- 検知の正確さ
- チューニングおよびカスタマイズ
- 技術的な制約

5.3.3.1 検知されるイベントの種類

無線 IDPS センサーによって最もよく検知されるイベントの種類には、次のようなものがある。

- **無許可の WLAN および WLAN 機器**：ほとんどの無線 IDPS センサーは、その情報収集機能を使用して、不正 AP、無許可の STA、無許可の WLAN（インフラストラクチャモード、アドホックモードの両方）を検知できる。
- **セキュリティが十分に確保されていない WLAN 機器**：ほとんどの無線 IDPS センサーは、適切なセキュリティ管理策を実施していない AP および STA を特定することができる。これには、設定ミスおよびセキュリティの強力でない WLAN プロトコルやプロトコル実装が使用されていることを検知することも含まれる。検知は、暗号化、認証、データ転送速度、SSID 名、チャネルなどについての組織固有の設定に関するポリシーからの逸脱を特定することにより行われる。たとえば、センサーは、STA が WPA2 や IEEE 802.11i ではなく WEP を使用していることを検知することができる。無線 IDPS が検知することができるイベントの種類の大半は、この分類に属するものである。
- **通常と異なる使用パターン**：一部のセンサーは、アノマリベースの検知手法を使用して、通常と異なる WLAN の使用パターンを検知することができる。たとえば、特定の 1 基の AP を使用している STA の数が通常と比べて多すぎる場合や、ある STA と AP の間のネットワークトラフィックが通常に比べて大きすぎる場合には、装置のいずれかが侵害されたか、何者かが無許可で WLAN を使用している可能性があると考えられる。多くのセンサーは、WLAN に参加しようとして失敗した試みを識別することができ、短時間のあいだに数回にわたって行われ失敗した試みに対する警報を発する。これは、WLAN への不正アクセスの試みが行われたことを示すと考えられる。また、就業時間外に行われた WLAN 活動を検知した場合に警報を送信できるセンサーもある。
- **無線ネットワークスキャナの使用**（ウォードライビングツールなど）：このようなスキャナは、セキュリティが十分にまたは全く確保されていないWLANを見つけるために使用される。無線IDPSセンサーが検知できるのは、能動型スキャナ（無線ネットワークトラフィックを生成するスキャナ）が使用された場合のみである。単にトラフィックを監視し、観測したトラフィックを解析するだけの受動型スキャナを検知することはできない [38]。
- **サービス妨害（DoS）攻撃およびその判定条件**（ネットワーク干渉など）：DoS 攻撃には、*フラッディング*（多数のメッセージを短い間隔で AP に送信する攻撃）のような論理的攻撃と、*ジャミング*（WLAN の周波数帯に対して電磁エネルギーを放射し、その周波数帯を WLAN が使用することができなくする攻撃）のような物理的攻撃がある。DoS 攻撃の検知には、ステートフルプロトコル解

[38] 多くの場合、受動型スキャナの使用を特定する最も効果的な方法は、物理的なセキュリティ管理策を通じて行われる。つまり、組織の施設周辺でコンピュータとアンテナを持ち歩いている者を探すことなどである。

析およびアノマリベースの検知手法（観測される活動が予期される活動と矛盾していないかどうかを判定する）が有効であることが多い。多くの DoS 攻撃は、一定の時間内に発生するイベントの件数を数え、それがしきい値を超過した場合に警報を発するという方法により検知することができる。たとえば、無線ネットワークセッションの切断に関するイベントが大量に発生した場合、DoS 攻撃が行われた可能性がある。

- **なりすまし攻撃および中間者攻撃**：一部の無線 IDPS センサーには、特定の装置が別の装置の ID を使用してなりすましを試みた場合にそれを検知する機能がある。これは、活動の特徴（フレーム内の特定の値など）の差異を識別することにより行われる。

ほとんどの無線 IDPS センサーには、検知した脅威の物理的な位置を特定する*三角測量*機能があり、複数のセンサーが受信した脅威からの信号の強度に基づいて、各センサーから脅威までのおおよその距離を推定し、さらに、各センサーからの推定距離から、脅威の物理的な位置が算出される。物理的な位置が特定されれば、組織の物理セキュリティ要員をその場所に派遣して脅威に対処させることができる。無線 IDPS 製品の中には、建物の間取り図を使用し、脅威が屋内と屋外のいずれに存在するのか、あるいは、公共の場所と立ち入りの制限された区域のいずれに存在するのかについても判定できるものがある。このような情報は、脅威の発見および阻止だけでなく、脅威に対処する際の優先順位付けにも役立つ。無線 IDPS センサーは、警報の優先度を設定する際に、個々の脅威の存在場所を部分的な基準として使用することができる。固定センサーに三角測量機能がない場合や、脅威の存在場所が移動している場合には、脅威の正確な場所を特定するために携帯用 IDPS センサーを使用することも有効である。

5.3.3.2 検知の正確さ

無線 IDPS は、他の種類の IDPS よりも概して正確である。これは対象（無線ネットワークプロトコルの解析）が限定的であるという性質によるところが大きい。フォールスポジティブは、主としてアノマリベースの検知によって発生する（特に、しきい値の更新が適切に行われていない場合）。無害な活動（組織の WLAN の有効範囲内にある別組織の WLAN など）によって警報が多数発生する可能性があるが、それらは組織の施設内にある未知の WLAN を正しく検知した結果であるから、厳密な意味のフォールスポジティブではない。

5.3.3.3 チューニングおよびカスタマイズ

無線 IDPS テクノロジーでは通常、検知の正確さを向上させるために若干のチューニングおよびカスタマイズ作業が必要となる。主な作業は、承認されている WLAN、AP、STA を指定することと、無線 IDPS ソフトウェアにポリシーの各種特性を入力することである。無線 IDPS によって検証されるのは、より上位のプロトコル(アプリケーションなど）ではなく、無線ネットワークプロトコルのみであるため、一般に警報の種類は少なく、したがって、カスタマイズやチューニングが可能な項目も多くはない。一部の無線 IDPS には、業界別のテンプレートが用意されており、基本となるポリシーの確立に役立つ。

無線 IDPS には、ある程度のカスタマイズ機能があり、ほとんどの無線 IDPS は、アノマリベースの検知に使用するしきい値を設定することができる。ブラックリストおよびホワイトリストは、それぞれ、有害および無害であることが判明している WLAN 機器の一覧である。また、これらの一覧は承認済みまたは未承認の WLAN NIC ベンダーを記録するために使用することができ、承認リストにない NIC が AP や STA で使用された場合に警報を生成させることができる。個別の警報は、ネットワークベースの IDPS

の場合と同様にカスタマイズ可能である。コード編集ができる製品は少ないが、ベンダーによっては、特定の検知機能のチューニングを行うために複雑な論理表現を使用することができる場合がある。

チューニングとカスタマイズの内容を定期的に見直して正確さを保つことに加え、管理者は、建物の間取りに変更があった場合にも適宜それが確実に反映されるようにすべきである。これは、脅威の物理的な位置を正確に特定し、センサーの設置計画を正確に作成するために必要である。

5.3.3.4 技術的な制約

無線 IDPS には、堅牢な検知能力がある一方、大きな制約がいくつかある。最も重要な制約として、検知できない特定の種類の無線プロトコル攻撃があること、回避テクニックを用いられやすいこと、IDPS 自体に対する攻撃への耐性が弱いことの 3 つが挙げられる。ここでは、これらの制約事項について詳しく述べる。

無線 IDPS は、無線ネットワークを対象とした攻撃のうち、特定の種類のものを検知することができない。攻撃者は、無線トラフィックを受動的に監視することがあるが、そのような活動は無線 IDPS で検知することができない。使われているセキュリティ方式が強力でない場合（WEP など）、攻撃者は、トラフィックを収集してオフライン処理することにより無線トラフィックのセキュリティに使用されている暗号化鍵を特定することができる。この鍵を使うことにより、収集済みのトラフィックだけでなく、同じ WLAN から収集されるすべてのトラフィックの復号が可能になる。安全性の低い無線ネットワークプロトコルを無線 IDPS で完全には補完することはできない。

一部の無線 IDPS センサーは、回避テクニックへの対応能力に問題がある。攻撃者は、使用されている無線 IDPS 製品をさまざまな手段で特定することができる。たとえば、センサーが設置されている場所を物理的に調べる方法や、フィンガープリンティング手法によって、製品が用いている防止措置（防止の詳細については 5.3.4 項を参照）の特徴を見分け、使用されている製品を特定する方法などがある。製品を特定できれば、その製品のチャネルスキャン方法に見られる特徴を利用した回避テクニックの使用が可能となる。たとえば、監視の対象となるチャネルが切り替わるのに合わせ、その時点で監視されていない方のチャネルを使用して瞬間的にバースト的な攻撃を行うことが考えられる。また、2 つのチャネルに対して同時に攻撃を仕掛ける場合もある。無線 IDPS センサーが最初の攻撃を検知した場合、その次の攻撃については、監視対象のチャネルを切り替えない限り検知することができない。チャネルスキャンには、このような問題の他、ネットワークフォレンジックに与える影響に関する問題もある。個々のセンサーが観測できるのは、個々のチャネルにおける活動の断片だけであるため、フォレンジックデータとしては極めて不完全であり、解析作業は非常に困難なものとなる。

また、無線 IDPS センサーは攻撃の影響も受ける。WLAN に対するサービス妨害攻撃（論理的攻撃と物理的攻撃の両方）よって、センサーの機能も同時に妨害される。センサーは、廊下や会議室などの開放的な場所に設置されることが多いため、物理的な攻撃も非常に受けやすい。製品によっては、デザインを火災報知器や通常の AP に似せるなど、耐タンパ性を持たせることによって、攻撃を受ける可能性を低減している。無線周波数を妨害するジャミングなどの物理的攻撃はすべてのセンサーに影響する。これに対する防御策は、施設の周囲に物理的な境界を確保し、攻撃者がジャミングを実行できるほどには WLAN に近づくことができないようにするしかない。

5.3.4 防止機能

無線 IDPS センサーは、次の 2 種類の侵入防止機能を備えている。

- **無線**：一部のセンサーには、不正なまたは設定の正しくない STA と承認された AP との間の接続、または、承認された STA と不正なまたは設定の正しくない AP との間の接続を切断する機能がある。これは通常、現在のセッションを切断することを指示するメッセージを双方のエンドポイントに送信することにより行われる。以後、センサーは新しい接続の確立を拒否する。
- **有線**：一部のセンサーには、特定の STA または AP が関与するネットワーク活動を機器の MAC アドレスまたはスイッチポートに基づいて阻止するよう、有線ネットワーク上のスイッチに指示を出す機能がある。たとえば、ある STA から有線ネットワーク上のサーバに対して攻撃が送信された場合は、センサーが有線スイッチに指示を出すことにより、当該 STA が送受信するすべての活動を遮断することができる。この手法は、悪意のある STA または AP による有線ネットワーク通信のブロックにのみ有効である。STA または AP からの悪意ある活動が無線プロトコル経由で継続されることは阻止できない。

ほとんどの IDPS センサーでは、警報の種類ごとに管理者が防止機能の設定を指定することができる。設定により指定できる事項には、防止の有効化／無効化の切り替えや、使用する防止機能の種類などがある。また、学習モードまたはシミュレーションモードを備えた IDPS センサーもある。これは、全ての防止措置を抑止し、その代わりに、防止措置が実行されるべき時点でその旨を示すモードである。このようなモードを利用することにより、管理者は防止機能を有効化する前に、監視を行いながら防止機能の設定を微調整することができ、害のない活動に対して防止措置を実行してしまうリスクを低減することができる。

重要な検討事項の 1 つは、防止措置がセンサーによる監視に及ぼす影響である。たとえば、接続を切断するための信号をセンサーから送信する場合、その防止措置が完了するまで、センサーが他の通信を監視するためのチャネルスキャンを実行できなくなる可能性がある。この問題を軽減するために、センサーによっては 2 つの電波を使用し、一方で監視および検知を行いつつもう一方で防止措置を実行できるようにしている。センサーの選定時には、必要な防止措置の内容と、防止措置を実行する場合にセンサーの検知機能がどのような影響を受けるのかについて検討すべきである。

5.4 管理

ほとんどの無線 IDPS 製品は、いずれもよく似た管理機能を備えている。この項では、管理の主要な側面（導入、運用、保守）について述べ、それらの作業を効果的かつ効率的に実行するための推奨事項を示す。

5.4.1 導入

無線 IDPS 製品を選定した場合、管理者がアーキテクチャの設計、IDPS 構成要素のテスト、構成要素に対するセキュリティ対策の実施を行った後に、IDPS を導入する必要がある。3.3.1項で示した内容に付け加えるべき事項は、構成要素のテストおよび設置に関することである。無線 IDPS を導入する際、既存の AP または無線スイッチに対するアップグレードや IDPS ソフトウェアのインストールが必要であれば、無線ネットワークを短期間一時的に停止する必要が生じる可能性がある。一般に、専用センサーを設置する場合にネットワークを停止する必要はない。

5.4.2 運用および保守

無線 IDPS ソリューションの運用および保守作業は、ネットワークベースの IDPS ソリューションの場合とほぼ同じである。無線 IDPS コンソールが備える管理、監視、解析、報告の機能も同様である。大き

な違いとして、無線 IDPS コンソールは脅威の物理的な位置を表示する機能を備えていることがある。より小さな違いとしては、無線 IDPS センサーが検知するイベントの種類が他の種類の IDPS と比べて少ないため、シグネチャの更新頻度がより少ない傾向がある。

5.5 まとめ

無線 IDPS は、無線ネットワークのトラフィックを監視し、無線ネットワークプロトコルを解析して、疑わしい活動を特定する。無線 IDPS を構成する典型的な要素は、ネットワークベースの IDPS と同様で、コンソール、データベースサーバ（任意）、管理サーバ、およびセンサーである。ただし、ネットワークベースの IDPS センサーが監視対象ネットワーク上のすべてのパケットを観測できるのに対し、無線 IDPS センサーは一度に 1 チャネルしか監視できないため、トラフィックをサンプリングすることにより動作する。同じチャネルの監視を長く継続するほど、それ以外のチャネルで行われる悪意のある活動を見落とす可能性は大きくなる。見落としを防ぐために、センサーは頻繁にチャネルを変更しながら動作し、各チャネルを毎秒数回ずつ監視することが多い。

無線センサーにはいくつかの形態がある。専用センサーは、無線 IDPS の機能を持つが、ネットワークトラフィックを送信元から宛先へと送る機能は持たない、固定または携帯用の装置である。その他の形態として、アクセスポイント（AP）または無線スイッチにバンドルされた無線センサーがある。専用センサーは、検出処理のみに専念でき、無線トラフィックを伝送する必要がないため、アクセスポイントや無線スイッチにバンドルされた無線センサーよりも検知能力が高いのが一般的である。しかし、バンドルされたセンサーは、既存ハードウェアにインストールできるのに比べ、専用センサーを使用するには新たにハードウェアやソフトウェアを調達する必要があるため、購入、インストール、保守のコストが高くなることが多い。そのため、無線 IDPS センサーの選定時にはセキュリティとコストの両面を考慮する必要がある。

無線 IDPS の構成要素は一般的に、有線ネットワークで相互に接続される。無線ネットワークと有線ネットワークは、すでに厳密な管理のもとに分離されていると考えられるため、無線 IDPS の構成要素間の接続に管理ネットワークと標準ネットワークのいずれを使用しても問題はないといえる。無線 IDPS を導入する際にセンサーの設置場所を選択することは、他のあらゆる種類の IDPS センサーの設置場所を決めることとは本質的に異なる問題である。無線 LAN（WLAN）を使用する組織では、WLAN の有効範囲を監視するために、無線センサーを設置すべきである。また、多くの組織は、施設内で WLAN 活動がまったくないはずの区域や、組織の WLAN で使用しないはずのチャネルおよび周波数帯を監視するためのセンサーも導入したいと考える。センサーの設置場所を選択する際のその他の考慮事項としては、物理的セキュリティ、センサーの有効範囲、有線ネットワーク接続が利用可能かどうか、コスト、および、AP や無線スイッチの設置場所などがある。

無線 IDPS は、いくつかの種類のセキュリティ機能を備えている。ほとんどの製品には、観測した無線機器および WLAN に関する情報を収集し、イベントデータを詳細なログとして記録する機能がある。無線 IDPS は、WLAN プロトコルレベルにおける攻撃、設定ミス、ポリシー違反を検知することができる。組織で使用する無線 IDPS 製品の選定時には、より広範かつ正確な検知ができるよう、複数の検知手法を組み合わせて使用する製品を採用すべきである。無線 IDPS で検知されるイベントの例としては、無許可の WLAN または WLAN 機器、セキュリティ対策が十分でない WLAN 機器、通常と異なる使用パターン、能動型無線ネットワークスキャナの使用、サービス妨害（DoS）攻撃、なりすまし攻撃および中間者攻撃などがある。また、ほとんどの無線 IDPS センサーは、検知した脅威の物理的な位置を三角測量によって特定する機能を備えている。

無線 IDPS は、他の種類の IDPS よりも概して正確である。これは対象（無線ネットワークプロトコルの解析）が限定的であるという性質によるところが大きい。無線 IDPS は通常、検知の正確さを向上させるために若干のチューニングおよびカスタマイズ作業が必要となる。主な作業は、承認されている WLAN、AP、STA を指定することと、無線 IDPS ソフトウェアにポリシーの各種特性を入力することである。チューニングとカスタマイズの内容を定期的に見直して正確さを保つことに加え、管理者は、建物の間取りに変更があった場合にも適宜それが確実に反映されるようにすべきである。これは、脅威の物理的な位置を正確に特定し、センサーの設置計画を正確に作成するために必要である。

無線 IDPS には、堅牢な検知能力がある一方、大きな制約がいくつかある。無線ネットワークを対象とした攻撃の中には、無線 IDPS が検知できない種類のものがある。たとえば、無線トラフィックを受動的に監視してオフライン処理により解析を行う攻撃を検知することはできない。また、無線 IDPS は、特に、IDPS 製品のチャネルスキャン方法に関する知識を利用することにより、検知を回避されやすい。チャネルのスキャンにおいては、個々のセンサーが観測できるのが、個々のチャネルにおける活動の断片だけであるため、ネットワークフォレンジックに影響する可能性がある。また、無線 IDPS センサーは、サービス妨害（DoS）攻撃や物理的な攻撃も受けやすい。

無線 IDPS センサーは、さまざまな侵入防止機能を提供する。一部のセンサーには、両エンドポイントにセッションの切断を指示したり、新規セッションの確立を防止したりする機能がある。また、特定の無線エンドポイントに対するネットワーク活動を遮断するよう有線ネットワーク上のスイッチに指示する機能を持つセンサーもある。ただし、この方法で遮断できるのは有線ネットワークの通信だけであり、エンドポイントが無線プロトコル経由で引き続き悪意のある活動を行うことは阻止できない。ほとんどの IDPS センサーでは、警報の種類ごとに管理者が防止機能の設定を指定することができる。防止措置によりセンサーの監視機能に影響が生じる可能性がある。たとえば、接続を切断するための信号をセンサーから送信する場合、その防止措置が完了するまで、センサーが他の通信を監視するためのチャネルスキャンを実行できなくなる可能性がある。この問題を軽減するために、センサーによっては 2 つの電波を使用し、一方で監視および検知を行いつつもう一方で防止措置を実行できるようにしている。センサーの選定時には、必要な防止措置の内容と、防止措置を実行する場合にセンサーの検知機能がどのような影響を受けるのかについて検討すべきである。

（本ページは意図的に白紙のままとする）

6. ネットワーク挙動解析（NBA）システム

*NBA（Network Behavior Analysis：ネットワーク挙動解析）システム*は、ネットワークトラフィックまたはそれに関する統計データを解析し、通常と異なるトラフィックフロー、たとえば、DDoS（分散型サービス妨害）攻撃、ある種のマルウェア（ワーム、バックドアなど）、およびポリシー違反（たとえば、クライアントシステムから他のシステムへのネットワークサービス提供）などを識別する[39]。このセクションでは、NBAテクノロジーについて詳しく論じる。まず、NBAテクノロジーの主要な構成要素を示し、それらの要素の導入に通常使用されるアーキテクチャについて説明する。また、疑わしい活動の特定に使用される方法を含め、各テクノロジーのセキュリティ機能について深く掘り下げる。そのあとは、導入および運用に関する推奨事項を含め、各テクノロジーの管理機能について説明する。

6.1 構成要素とアーキテクチャ

この項では、典型的なNBAソリューションの主要な構成要素について説明し、それらの構成要素のための最も一般的なネットワークアーキテクチャを示す。また、特定の構成要素の設置についての推奨事項を提示する。

6.1.1 典型的な構成要素

NBAソリューションには一般にセンサーおよびコンソールが含まれ、さらに製品によっては管理サーバが提供される（管理サーバは「*アナライザ*」と呼ばれることがある）。NBAセンサーの提供形態は、通常はアプライアンスのみである。一部のセンサーは、1つまたはいくつかのネットワークセグメントのパケットを傍受してネットワーク活動を監視するという点において、ネットワークベースのIDPSセンサーに似ている。それ以外のNBAセンサーは、ネットワークを直接に監視することはせず、ルータまたはその他のネットワーク装置から供給されるネットワークフローに関する情報を使用する。「*フロー*」は、ホスト間に発生する特定の通信セッションを意味する。フローのデータ形式には、NetFlow[40]、sFlow[41]など多数の標準が存在する。侵入検知および侵入防止に関係する具体的なフローデータとしては次のようなものがある。

- 送信元および宛先IPアドレス
- 送信元および宛先のTCPまたはUDPポート、あるいはICMPタイプおよびコード
- セッションにおいて伝送されたパケット数およびバイト数
- セッション開始時および終了時のタイムスタンプ

6.1.2 ネットワークアーキテクチャ

ネットワークベースのIDPSと同様、NBA構成要素間の通信には、独立の管理ネットワークを使用することも、組織の標準ネットワークを使用することもできる。他の装置からネットワークフローデータの提供

---

39 ベンダーによっては、NBAテクノロジーという用語によって、「Network Behavior Anomaly Detection（NBAD：ネットワーク挙動異常検知）ソフトウェア」、「Network Behavior Analysis and Response（ネットワーク挙動解析および応答）ソフトウェア」、「Network Anomaly Detection（ネットワーク異常検知）ソフトウェア」などを意味していることがある。

40 NetFlowの詳細については、RFC 3954『*Cisco Systems NetFlow Services Export Version 9*』（http://www.ietf.org/rfc/rfc3954.txt）、およびCiscoのWebサイト（http://www.cisco.com/en/US/products/ps6645/products_ios_protocol_option_home.html）を参照のこと。

41 sFlowの詳細については、http://www.sflow.org/を参照のこと。

を受ける種類のセンサーを使用する場合は、NBA ソリューション全体を標準ネットワークから論理的に分離することができる。NBA ネットワークアーキテクチャの例を図 6-1 に示す。

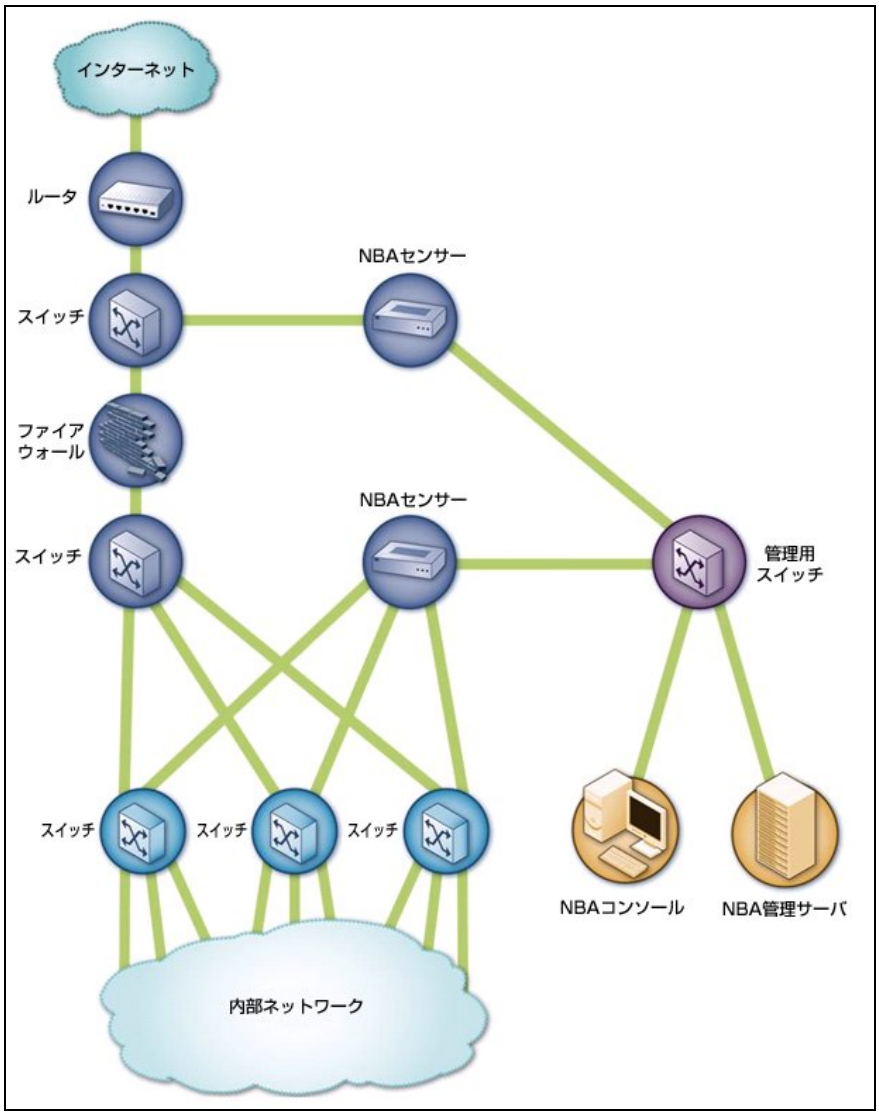

図 6-1. NBA センサーアーキテクチャの例

6.1.3 センサーの設置場所

構成要素に対して適切なネットワークを選択することに加え、管理者はセンサーをどこに配置するかを決定しなければならない。ほとんどの NBA センサーは、受動モードでのみ設置可能であり、ネットワークベースの IDPS と同様の方法（ネットワークタップ、スイッチスパニングポートなど）を使用して接続する。ネットワークを直接監視するタイプの受動型センサーは、ネットワーク間の境界など、ネットワークの重要な場所や、DMZ（非武装地帯）のサブネットなどの、重要なネットワークセグメントを監視できる位置に設置すべきである。インラインセンサーは通常、ネットワークの境界で使用されることを前提にしたものであり、ファイアウォールを過負荷にする可能性のある攻撃を制限するために、ファイアウォールのすぐ近く、多くの場合はファイアウォールとインターネット境界ルータの間に設置される。

6.2 セキュリティ機能

NBA 製品は、多様なセキュリティ機能を提供する。一般的なセキュリティ機能を、ここでは情報収集、ログの記録、検知、および防止の 4 つに分け、それぞれについて6.2.1項～6.2.4項で説明する。NBA 製品によっては、SIEM（セキュリティ情報およびイベント管理）機能を持つものもある。SIEM の詳細については、8.2.2項を参照のこと。

6.2.1 情報収集機能

ほとんどの NBA 製品で使用される検知手法では、組織内のホストの特性に関する知識が必要となるため、NBA テクノロジーは広範な情報収集機能を備えている。NBA センサーは、組織の監視対象ネットワーク上で通信を行っているホストの一覧を自動的に作成し、維持することができる。NBA センサーは、ポートの使用状況の監視、受動的フィンガープリンティングの実行などの手法を用いて、ホストの詳細情報を収集する（ほとんどの製品において管理者は、6.2.3.1 項で述べるように、ファイアウォールのルールセットに似た詳細なポリシーをホスト間通信について指定することができる。これによりたとえば、使用を許可または禁止するポート番号を指定することが可能である）。個々のホストについて収集する情報は、一般的に次のようなものである。

- IP アドレス
- オペレーティングシステム
- ホストが提供するサービスと、そのために使用する IP プロトコルおよび TCP／UDP ポート
- ホストが通信を行う他ホスト、また、ホストが他のホストのどのサービスを利用するのか、各ホストにコンタクトする際にどの IP プロトコルおよび TCP／UDP ポートを使用するのか

NBA センサーは、これらの情報を変更するために、ネットワーク活動を継続的に監視する。また、各ホストのフローに関する詳細情報も継続的に収集する。これについては6.2.3項を参照のこと。

6.2.2 ログ記録機能

N NBA テクノロジーは一般に、検知したイベントに関連するデータを詳細なログとして記録する。このデータは、警報の妥当性の確認、インシデントの調査、および、NBA ソリューションにおいて検知されたイベントとその他のログ生成ソースにおいて検知されたイベントとの相関をとるのに使用することができる。NBA ソフトウェアのログに記録される一般的なデータフィールドとしては、次のようなものがある。

- タイムスタンプ（通常は日付および時刻）
- イベントまたは警報の種類
- 評価（優先度、重大度、影響の程度、確実性など）
- ネットワーク層、トランスポート層、アプリケーション層のプロトコル
- 送信元および宛先 IP アドレス
- 送信元および宛先の TCP または UDP ポート、あるいは ICMP タイプおよびコード
- その他のパケットヘッダフィールド、たとえば IP TTL（time-to-live：存続時間）など

- 接続の送信元ホストおよび宛先ホストにより送信されたバイト数およびパケット数
- 実行された防止措置（該当する場合）

ネットワークトラフィックを直接監視する種類の NBA センサーの中には、パケットの限定的なペイロード情報（認証されたユーザの ID など）をログに記録する機能を備えているものがある。これにより、活動を追跡して、その活動がどのユーザアカウントによるものなのかを特定することができる。

6.2.3 検知機能

NBA テクノロジーは、いくつかのタイプの悪意ある活動を検知する機能を備えているのが一般的である。ほとんどの製品では、アノマリベースの検知を主体とし、それに若干のステートフルプロトコル解析手法を組み合わせて、ネットワークフローの解析を行う。シグネチャベースの検知機能を備えるものはほとんどない。ただし、管理者が手作業で設定するカスタムフィルタによって特定の脅威を検知および阻止する機能があり、これはシグネチャに相当する。この項では、次の観点から NBA ソフトウェアの検知機能について説明する。

- 検知されるイベントの種類
- 検知の正確さ
- チューニングおよびカスタマイズ
- 技術的な制約

6.2.3.1 検知されるイベントの種類

NBA センサーによって最もよく検知されるイベントの種類には、次のようなものがある。

- **サービス妨害（DoS）攻撃**（DDoS、すなわち分散型サービス妨害攻撃を含む）：この種の攻撃が行われると、一般に、帯域の使用量が大幅に増加するか、特定のホストとの間で送受信されるパケットの数または、特定のホストとの間での接続数が通常よりも極端に多くなる。アノマリベースの検知手法では、こうした特徴を監視し、観測された活動内容と、想定されている活動内容に大きな差異があるかどうかを判定する。NBA センサーの中には、よく使用される DoS ツールや手法の特徴を認識できるものがあり、脅威をより迅速に特定し、より正確な優先順位付けを行うために役立つ。
- **スキャン**：スキャンは、アプリケーション層（バナーの取得など）、トランスポート層（TCP／UDP ポートスキャンなど）、ネットワーク層（ICMP スキャンなど）で通常と異なるフローパターンを監視することにより検知できる。
- **ワーム**：ホストからホストへと伝染するワームを検知する方法はいくつかある。ワームによっては、迅速に伝染を広げ、帯域を大量に使用するものもある。ワームが原因で、通常通信を行わないホストどうしが互いに通信したり、ホストが通常使わないポートを使用したりするため、それらを監視することでも検知することが可能である。また、多くのワームはスキャンも実行するが、これは、前述の方法によって検知することが可能である。
- **予期されないアプリケーションサービス**（トンネリングされたプロトコル、バックドア、使用禁止のアプリケーションプロトコルなど）：通常、ステートフルプロトコル解析の手法（特定の接続において観測

される活動が、そこで予期されるアプリケーションプロトコルと矛盾していないかを判定する）により検知される。

- **ポリシー違反**：ほとんどの NBA センサーでは、詳細なポリシー（特定のシステムがどのホストまたはホストグループに対してコンタクトできるか、特定種類の活動が許可される時間帯や曜日の限定など）を管理者が指定することができる。また、ポリシー違反の可能性がある多くのイベント（たとえば、ポリシー上許可されない新しいホストや、ホストにおいて実行されている新しいサービスの検知など）についてもほとんどのセンサーは、自動的に検知する。

NBA センサーのほとんどは、観測した一連のイベントを再構成して脅威の発生源を特定する機能を備えている。たとえば、ネットワークにワームが感染した場合にワームのフローを解析し、組織のネットワーク上で他のホストへ最初にワームを伝送したホストを発見することができる。

6.2.3.2 検知の正確さ

NBA センサーは主として、通常の活動内容から大きく逸脱した活動を検知することにより機能する。したがって、短期間に大量のネットワーク活動が生じる攻撃（DDoS 攻撃など）や、通常と異なるフローパターンを示す攻撃（ホスト間を伝って広がるワームなど）を最も正確に検知する。反面、規模の小さい攻撃については検知の正確さが劣り、特に、緩慢に行われる攻撃や、管理者の設定したポリシーに違反しない攻撃（一般的なポートおよびプロトコルを使用する攻撃など）に対する検知能力は低い。

検知の正確さは、時間の経過によっても変化する。NBA テクノロジーは主としてアノマリベースの検知手法を使用するため、攻撃が予期される活動内容から大きな逸脱を示す状態に達するまでは検知できない場合が多い。DoS 攻撃が最初はゆっくりと開始され、時間を経るにつれてネットワーク活動の量が増える形で行われた場合、NBA センサーによって検知できる可能性は大きいが、攻撃のどの時点で検知するかは NBA 製品によって大きく異なることがある。アノマリ活動に対して敏感に反応するようセンサーを設定すると、攻撃の発生時に警報が発せられるタイミングは早まるが、フォールスポジティブが発生する可能性も大きくなる。逆に、アノマリ活動に対する感度が低くなるよう設定すると、フォールスポジティブの発生は減るが、警報のタイミングが遅くなり、攻撃が実行される期間は長くなる。

フォールスポジティブは、悪意によらない環境の変化に起因して発生することもある。たとえば、あるホストに新しいサービスが追加され、いくつかのホストがそれを利用し始めると、NBA センサーはそれをアノマリとして検知する可能性が大きい。ただし通常、こうした場合に発せられるのは優先度の低い警報であり、攻撃としては報告されないため、真のフォールスポジティブとみなすべきかどうかについては議論の余地がある。あるホストの重要なサービスを別のホストへ移動し、1000 台のホストが一日のうちにそのサービスを利用し始めるような場合には、意図しない警報が発せられることがある。

6.2.3.3 チューニングおよびカスタマイズ

NBA テクノロジーの機能は、主として、ネットワークトラフィックを観測することと、予期されるフローのベースラインおよびホスト特性のインベントリを作成することに依拠している。NBA 製品は、ベースラインを自動的に更新し続ける。そのため、通常はチューニングやカスタマイズの作業はあまり発生しないが、ファイアウォールのルールセットに似たポリシーはほとんどの製品に備わっており、その設定変更が必要となる場合がある。また、しきい値の設定（帯域の使用量がどの程度増加した場合に警報を発するかなど）についても、環境の変化を考慮して、管理者が定期的に変更する必要が生じることがある。しきい値は多くの場合、ホストごとに、あるいは、管理者が定義するホストグループに対して設定することができる。ほとんどの NBA 製品は、ホストおよびサービスに関するホワイトリストおよびブラックリスト

の機能も備える。その他の一般的な機能としては、個々の警報のカスタマイズ（警報によって起動される防止措置の指定など）がある。ネットワークベースの IDPS とは違い、通常の NBA 製品はコード編集には対応していない。

いくつかの NBA 製品は、限定的にシグネチャベースの検知を行う機能を備えている。対応しているシグネチャは一般に、非常に単純なものに限られており、主に IP、TCP、UDP または ICMP の特定のヘッダフィールドに特定の値が含まれているかどうかを調べる。この機能は、インライン NBA センサーにおいて最も役立つ。なぜなら、シグネチャを使用することにより、ファイアウォールやルータが阻止することができない可能性がある攻撃をセンサーが発見・阻止することができるからである。たとえば、細工された HTTP トラフィックを Web サーバに大量に送りつける DDoS 攻撃が行われた場合、ファイアウォールやルータでは、標的となった Web サーバに対する HTTP 活動をすべて遮断する以外に攻撃を阻止する方法がないことがある。そのような場合にも、攻撃の活動に特有の性質があれば、インライン NBA センサーのシグネチャをカスタマイズすることで、その攻撃活動だけを遮断できる可能性がある。また、インライン NBA センサーが攻撃のフローパターンを検知することにより、いずれにしろ攻撃を遮断する可能性がある。

チューニングとカスタマイズの内容を定期的に見直して正確さを保つことに加え、管理者は、組織内のホストに大幅な変更（ホストの追加、サービスの追加など）があった場合にも、それを NBA の設定に反映しなければならない。NBA システムを変更管理システムに自動的にリンクすることが現実的ではない場合でも、管理者は、フォールスポジティブの発生を防ぐために変更管理の記録を定期的にレビューして、NBA のホストインベントリ情報を調整することができる。

6.2.3.4 技術的な制約

NBA テクノロジーは、特定の種類の脅威に対して強力な検知能力を発揮する一方、大きな制約も抱えている。一部の制約については6.2.3.2項で説明したが、その他の重要な制約の 1 つは、攻撃の検知が遅れることである。ベースラインからの逸脱（帯域使用量の増加や接続試行数の追加など）に基づくアノマリベースの検知手法にとって、ある程度の遅延は本質的に避けられないものであるが、それに加え、NBA テクノロジーではデータソースによって遅延が発生する。特に、ルータまたはその他のネットワーク装置からフローデータの供給を受ける製品において顕著である。このデータは、バッチ処理で NBA システムへ転送されることが多いが、製品の能力やネットワーク容量、管理者の設定などによって、比較的頻繁に（たとえば 1～2 分ごと）転送が行われる場合もあれば、あまり頻繁でない（たとえば 15～30 分ごと）場合もある。このような遅延が存在するため、迅速な攻撃（マルウェア感染、DoS 攻撃など）が行われた場合、システムの妨害や破壊が行われるまで攻撃が検知されない可能性がある。

この遅延は、他の装置から供給されるフローデータに頼らず自身がパケットの採取および解析を行うセンサーを使用することにより避けられる。ただし、パケットを採取して解析する処理は、フローデータの解析と比べてはるかにリソースの消費量が大きい。1 台のセンサーにより実行可能なのは、多数のネットワークのフローデータを処理することか、あるいは、多くても少数のネットワークを対象とした、センサー自体による直接監視（パケット採取）である。したがって、フローデータを使用せずに直接監視を行うには、より強力なセンサーを購入する[とともに／か、あるいは]センサーの数を増やす必要が生じる場合がある。

6.2.4 防止機能

NBA センサーは、さまざまな侵入防止機能を備えている。それらをセンサーの種類別に示すと次のようになる。

■ **受動のみ**

– **既存 TCP セッションの終了**：受動型 NBA センサーは、既存セッションの両エンドポイントに TCP リセットパケットを送信してセッションの終了を試みることができる。

■ **インラインのみ**

– **インラインファイアウォール処理の実行**：ほとんどのインライン NBA センサーは、疑わしいネットワーク活動を通過させないまたは拒否するために使用することができるファイアウォール機能を備えている。

■ **受動、インラインの両方**

– **他のネットワークセキュリティ装置の設定変更**：多くの NBA センサーは、ファイアウォールやルータなどのネットワークセキュリティ装置に対し、特定の種類の活動を阻止したり別の場所（検疫用 VLAN など）へ誘導したりするように設定変更を行う指示を出すことができる。

– **サードパーティ製プログラムまたはスクリプトの実行**：一部の NBA センサーには、特定の悪意ある活動を検知した場合に、管理者が指定したスクリプトまたはプログラムを実行する機能がある。

ほとんどの NBA センサーでは、警報の種類ごとに管理者が防止機能の設定を指定することができる。設定により指定できる事項には、防止の有効化／無効化の切り替えや、使用する防止機能の種類などがある。フォールスポジティブの発生を避けるため、ほとんどの NBA システムの実装では、防止機能を限定的に使用するか、または全く使用しない。これは、わずか 1 件のフォールスポジティブの遮断が、ネットワーク通信の深刻な障害を招く可能性があるからである。NBA センサーで防止機能を使用するのはほとんどの場合、既知の特定の脅威（新種のワームなど）を阻止するためである。

6.3 管理

ほとんどの NBA 製品は、いずれもよく似た管理機能を備えている。この項では、管理の主要な側面（導入、運用、保守）について述べ、それらの作業を効果的かつ効率的に実行するための推奨事項を示す。

6.3.1 導入

NBA 製品を選定した場合、管理者がアーキテクチャの設計、NBA 構成要素のテスト、構成要素に対するセキュリティ対策の実施を行った後に、NBAを導入する必要がある。3.3.1項で示した内容に付け加えるべき事項は、構成要素のテストおよび配備に関することである。実稼働環境への配備の際には、インベントリの構築と初期ベースラインの生成がすべての構成要素について同時に行われるよう、比較的短時間でセンサーの設置を完了すべきである。導入期間中および運用の初期は、センサーが環境に関する情報を十分に持っていないため、センサーが数日～数週間程度にわたる環境の監視を完了するまでは、検知の正確さは低下する可能性が大きい。この点を除けば、NBA センサーおよびコン

ソールの配備作業は、ネットワークベースの IDPS センサーおよびコンソールの配備と基本的に同様である。

6.3.2 運用および保守

NBA 製品は、コンソールを使用して運用および保守作業を実行するよう設計されている。一般に、コンソールの機能は、ネットワークベースの IDPS のコンソールとよく似ている。大きな違いとして、NBA コンソールは、組織のネットワークを通じて攻撃のフローを表示する視覚化ツールを備えていることが多い。そのようなツールは、いずれのホストが攻撃の影響を受けたか、各ホストがどのような順序で攻撃の対象となったか、および、いずれのホストが最初に攻撃に巻き込まれたかをユーザに示すことができる。また、一部の NBA 製品には、コマンドラインインタフェースも用意されている。

NBA 製品についての継続的な保守作業も、ネットワークベースの IDPS の場合と非常によく似ている。主要な例外は、更新の適用作業である。ほとんどの NBA 製品はシグネチャを使用しないため、管理者は NBA ソフトウェア自体に対する更新についてのみ、テストおよび適用を実施すればよい。NBA センサーはアプライアンスベースであるため、更新作業は、現行の CD を交換してから、センサーを再起動するか、CD からソフトウェアをインストールするという方法によるのが一般的である。シグネチャ機能を備えた NBA 製品については、ネットワークベースの IDPS のシグネチャの更新を行う場合と同様の方法により、シグネチャの更新の入手・テスト・適用を行う必要がある。

6.4 まとめ

NBA（Network Behavior Analysis：ネットワーク挙動解析）システムは、ネットワークトラフィックまたはそれに関する統計データを解析し、通常と異なるトラフィックフローを識別する。NBA ソリューションには一般にセンサーおよびコンソールが含まれ、さらに製品によっては管理サーバが提供される。一部のセンサーは、1 つまたはいくつかのネットワークセグメントのパケットを傍受してネットワーク活動を監視するという点において、ネットワークベースの IDPS センサーに似ている。それ以外の NBA センサーは、ネットワークを直接に監視することはせず、ルータまたはその他のネットワーク装置から供給されるネットワークフローに関する情報を使用する。

ほとんどの NBA センサーは、受動モードでのみ設置可能であり、ネットワークベースの IDPS と同様の方法（ネットワークタップ、スイッチスパニングポートなど）を使用して接続する。ネットワークを直接監視するタイプの受動型センサーは、ネットワーク間の境界など、ネットワークの重要な場所や、DMZ（非武装地帯）のサブネットなどの、重要なネットワークセグメントを監視できる位置に設置すべきである。インラインセンサーは通常、ネットワークの境界で使用されることを前提にしたものであり、ファイアウォールを過負荷にする可能性のある攻撃を制限するために、ファイアウォールのすぐ近く、多くの場合は、外部ネットワーク側に設置する。

NBA 製品は、多様なセキュリティ機能を提供する。製品が提供する広範な情報収集機能によって、個々の観測対象ホストに関する詳細な情報の収集と、その情報の変化を検知するためのネットワーク活動の継続的な監視が行われる。NBA テクノロジーは一般に、検知したイベントに関連するデータを詳細なログとして記録する。また、いくつかのタイプの悪意ある活動（DoS 攻撃、スキャン、ワーム、予期していないアプリケーションサービスなど）およびポリシー違反（クライアントシステムから他のシステムへのネットワークサービス提供など）を検知する能力を備えているのが一般的である。NBA センサーは主として、通常の活動内容から大きく逸脱した活動を検知することにより機能する。したがって、短期間に大量のネットワーク活動が生じる攻撃や、通常と異なるフローパターンを示す攻撃を最も正確に

検知する。また、NBA センサーのほとんどは、観測した一連のイベントを再構成して脅威の発生源を特定する機能を備えている。

NBA 製品は、ベースラインを自動的に更新し続ける。そのため、通常はチューニングやカスタマイズの作業はあまり発生しないが、ほとんどの製品がサポートしている、ファイアウォールのルールセットに似たポリシーの更新が必要となる。いくつかの NBA 製品は、限定的にシグネチャのカスタマイズを行う機能を備えている。この機能はインライン NBA センサーにおいて最も役立つ。なぜなら、シグネチャを使用することにより、ファイアウォールやルータが阻止することができない可能性がある攻撃をセンサーが発見・阻止することができるからである。チューニングとカスタマイズの内容を定期的に見直して正確さを保つことに加え、管理者は、組織内のホストに大幅な変更（ホストの追加、サービスの追加など）があった場合にも、それが反映されるようにしなければならない。NBA システムを変更管理システムに自動的にリンクすることが現実的ではない場合が多いが、管理者は、フォールスポジティブの発生を防ぐために変更管理の記録を定期的にレビューして、NBA のホストインベントリ情報を調整することができる。

NBA テクノロジーには、大きな制約がいくつかある。まず、データソースとして何を利用するかによって、攻撃の検知が遅れるという問題がある。特に、ルータまたはその他のネットワーク装置からフローデータの供給を受ける製品において顕著である。外部から供給されるデータは、1 分に 1 回～1 時間に数回程度の頻度でバッチ処理により転送されることが多い。そのため、迅速な攻撃が行われた場合、システムの妨害や破壊が行われるまで攻撃が検知されない可能性がある。この遅延は、自身がパケットの採取および解析を行うセンサーを使用することにより避けられるが、フローデータの解析と比べてはるかにリソースの消費量が大きい。1 台のセンサーにより実行可能なのは、多数のネットワークのフローデータを処理することか、少数のネットワークを同時に直接監視することである。したがって、フローデータを使用せずに直接監視を行うには、より強力なセンサーを購入する[とともに／か、あるいは]、センサーの数を増やす必要が生じる場合がある。

7. ホストベースのIDPS

ホストベースの IDPS は、単一のホストの特性と、そのホストの内部で発生するイベントを監視し、疑わしい活動を検知する。監視の対象となる特性の例としては、有線および無線のネットワークトラフィック（当該ホストのみ）、システムログ、実行中のプロセス、ファイルに対するアクセスおよび変更、システムやアプリケーションの設定の変更などがある。このセクションでは、ホストベースの IDPS テクノロジーについて詳しく論じる。まず、テクノロジーの主要な構成要素を示し、それらの要素の導入に通常使用されるアーキテクチャについて説明する。また、疑わしい活動の特定に使用される方法を含め、各テクノロジーのセキュリティ機能について深く掘り下げる。そのあとは、導入および運用に関する推奨事項を含め、各テクノロジーの管理機能について説明する。

7.1 構成要素とアーキテクチャ

この項では、典型的なホストベースの IDPS の主要な構成要素について説明し、それらの構成要素のための最も一般的なネットワークアーキテクチャを示す。また、ホストベースの IDPS を使用すべきホストの選択についての推奨事項を提示する。さらに、ホストベースの IDPS がホストの内部アーキテクチャに及ぼす影響（プロセス呼び出しの捕捉など）についても説明する。

7.1.1 典型的な構成要素

ほとんどのホストベースのIDPSには、監視対象のホストにインストールされる「エージェント」と呼ばれる検知用ソフトウェアが含まれる。各エージェントは、1 つのホスト上で行われる活動を監視し、IDPS機能が有効になっている場合は防止措置も実行する。ホストベースのIDPSによる監視の対象となる活動の種類については、7.2.2項に示す。エージェントは、データを管理サーバへ転送し、管理サーバは、場合によってデータの保存にデータベースを使用する [42]。管理および監視には、コンソールが使用される。

ホストベースの IDPS によっては、個別のホストにはエージェントソフトウェアをインストールせず、エージェントソフトウェアが稼働する専用アプライアンスを使用するものがある。その場合、アプライアンスは特定ホストに出入りするネットワークトラフィックを監視できる場所に設置される。こうしたアプライアンスは、インラインに配備してネットワークトラフィックを監視するため、技術的にはネットワークベースの IDPS とみなすこともできるが、一般には特定の 1 種類のアプリケーション（Web サーバ、データベースサーバなど）に限って活動を監視するため、通常のネットワークベースの IDPS よりも用途が特化している。また、この種のアプライアンス上で稼働するソフトウェアは、ホストベースのエージェントと機能的に同じであるか類似していることが多い。以上の理由から、アプライアンスベースのエージェントを使用したホストベースの IDPS 製品についてもこの項で述べることにする。

個々のエージェントは一般に、次のいずれか 1 つを保護するよう設計されている。

- **サーバ**：サーバのオペレーティングシステム（OS）を監視する他、よく使用されるいくつかのアプリケーションも合わせて監視することがある。

[42] 本文書では、エンタープライズ規模の IDPS の導入を中心に説明するため、エージェントから管理サーバにデータが送られることを前提とする。エージェントによっては、管理サーバを使用せずホストの管理者が直接管理／監視するスタンドアロンによる導入が可能なものもある。

- **クライアントホスト（デスクトップまたはノート PC）**：ユーザホストの監視用として設計されたエージェントは、OS および一般的なクライアントアプリケーション（電子メールクライアント、Web ブラウザなど）を監視するのが普通である。
- **アプリケーションサービス**：エージェントによっては、特定のアプリケーションサービス（Web サーバプログラム、データベースサーバプログラムなど）だけを監視する。この種のエージェントは、*アプリケーションベース IDPS* とも呼ばれる。

ほとんどの製品には、これら以外のホスト（たとえば、ファイアウォール、ルータ、スイッチなどのネットワーク機器）を対象とするエージェントは含まれない。

7.1.2 ネットワークアーキテクチャ

一般に、ホストベースの IDPS を導入する際のネットワークアーキテクチャは非常に単純である。エージェントは、組織のネットワークに属する既存ホストに導入されるので、構成要素間の通信は通常、別個の管理ネットワークではなく、組織のネットワークを使用して行われる。ほとんどの製品は、通信を暗号化し、盗聴者が機密情報にアクセスするのを防止する。アプライアンスベースのエージェントは、通常、保護対象とするホストの直前の位置にインラインで導入される。ホストベースの IDPS の導入におけるネットワークアーキテクチャの例を図 7-1 に示す。

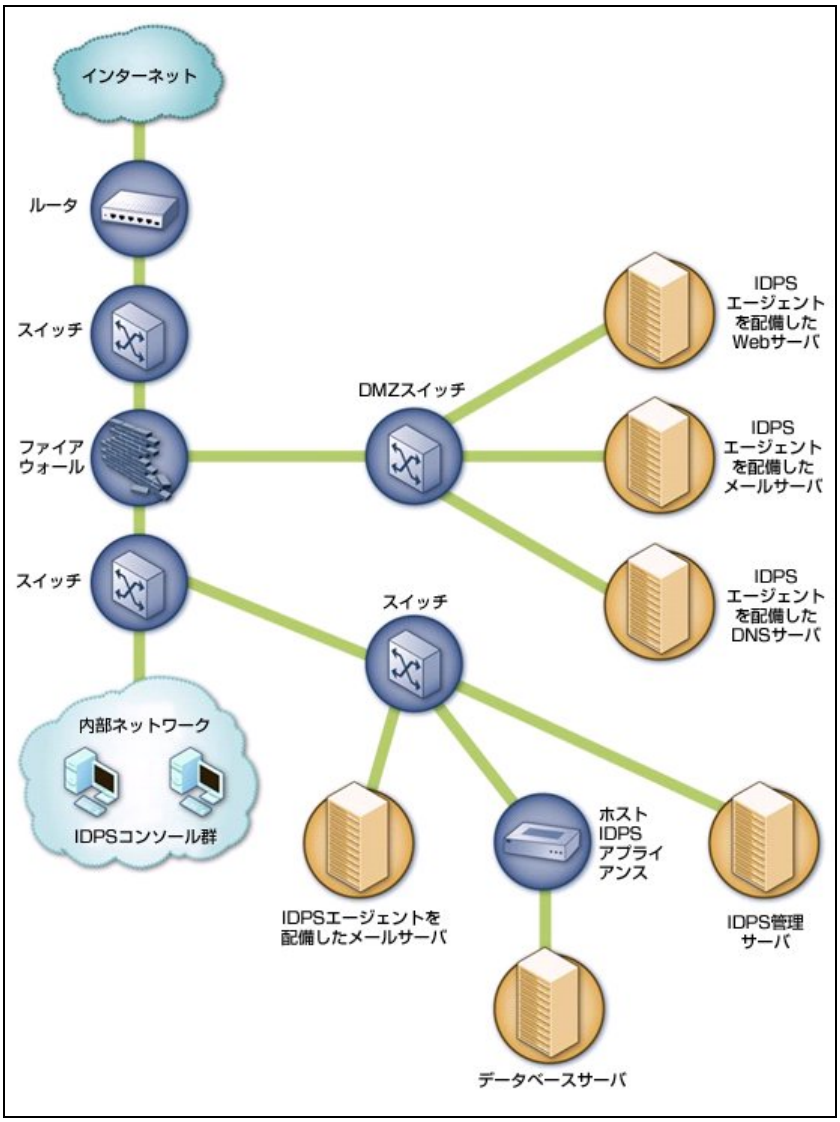

図 7-1. ホストベース IDPS エージェントの設置アーキテクチャ例

7.1.3 エージェントの配備場所

ホストベースの IDPS エージェントは、一般に公開されているサーバや、機密性の高い情報が保存されているサーバなど、重要なホストに導入されるのが最も一般的である。しかし、さまざまなサーバおよびデスクトップ／ノート PC 用オペレーティングシステムや特定のサーバアプリケーション向けにエージェントが用意されているため、必要があれば組織内のサーバやデスクトップ／ノート PC のほとんどにエージェントを導入することが可能である。一部の組織では、他のセキュリティ管理策では監視できない活動の解析を主目的としてホストベースの IDPS エージェントを使用している。たとえば、暗号化されたネットワーク通信を介して行われる活動は、ネットワークベースの IDPS センサーでは解析できないが、ホストベースの IDPS エージェントをエンドポイントにインストールすることにより、暗号化されていない活動を監視することができる。その他、エージェントを導入する場所の選定にあたっては、次の基準も考慮すべきである。

- エージェントの配備、保守、監視に要するコスト
- エージェントがサポートする OS およびアプリケーション
- ホストのデータまたはサービスの重要性
- インフラストラクチャがエージェントをサポートする能力（たとえば、エージェントから集中化サーバへ警報データを転送したり、集中化サーバからエージェントへソフトウェア更新やポリシー更新を転送したりするために十分なネットワーク帯域幅を確保できるか）

7.1.4 ホストのアーキテクチャ

IDPS エージェントがインストールされたホストでは、ほとんどの場合、侵入防止機能を提供するためにその内部アーキテクチャが変更される。これは通常、ホスト上の既存コード層の間に「シム」（くさび）と呼ばれるコード層を挿入することにより行われる。シムは、通常であれば、データがあるコードから別のコードへと渡されるポイントにおいて横取りし、解析することにより、そのデータを許容すべきか、拒否すべきかの判断を下す。ホストベースの IDPS エージェントでは、いくつかの種類のリソースに対してシムを使用することがある。たとえば、ネットワークトラフィック、ファイルシステムに関する活動、システムコール、Windows レジストリに関する活動、よく使用されるアプリケーション（電子メールや Web）などが対象となる。

一部のホストベースの IDPS エージェントは、ホストアーキテクチャを変更しない代わりにシムなしで活動を監視する、あるいは、活動による産物（ログの項目、ファイルに加えられた変更など）を解析する。このような方法は、ホストへの影響が少なく、IDPS がホストの通常の運用を妨げる可能性は小さい反面、脅威を正確に検知する能力が概して劣り、全く防止措置を実行することができない場合が多い。

ホストベースの IDPS ソリューションの選定における重要な意思決定事項の 1 つは、ホストにエージェントをインストールするのか、エージェントベースのアプライアンスを使用するのかのいずれを選択するかである。検知および防止の観点からは、ホストにエージェントをインストールするほうが一般に望ましいと考えられる。これは、ホストの各種特性にエージェントが直接アクセスすることにより、より網羅的かつ正確な検知／防止を実行することができるためである。ただし、エージェントは広く普及した少数の OS にのみ対応していることが多いため、ホストが、サポートされていない OS を使用している場合は、アプライアンスを配備することになる。また、パフォーマンス上の理由からアプライアンスを選択する場合もある。監視対象ホストにエージェントがインストールされることにより、当該ホストのパフォーマンスが過度に低下する場合は、負荷を軽減するためにエージェント機能をアプライアンスに移動せざるを得ないことがある。

7.2 セキュリティ機能

ホストベースの IDPS は、多様なセキュリティ機能を提供する。一般的なセキュリティ機能を、ここではログの記録、検知、防止、その他の 4 つに分け、それぞれについて7.2.1項～7.2.4項で説明する。

7.2.1 ログ記録機能

ホストベースの IDPS は一般に、検知したイベントに関連するデータを詳細なログとして記録する。このデータは、警報の妥当性の確認、インシデントの調査、および、ホストベースの IDPS において検知されたイベントとその他のログ生成ソースにおいて検知されたイベントとの相関をとるのに使用すること

ができる。ホストベースの IDPS のログに記録される一般的なデータフィールドとしては、次のようなものがある。

- タイムスタンプ（通常は日付および時刻）
- イベントまたは警報の種類
- 評価（優先度、重大度、影響の程度、確実性など）
- イベントの種類に応じた固有の詳細情報（IP アドレスおよびポート情報、アプリケーション情報、ファイル名およびパス、ユーザ ID など）
- 実行された防止措置（該当する場合）

7.2.2 検知機能

ほとんどのホストベースの IDPS は、いくつかのタイプの悪意ある活動を検知する機能を備えている。既知の攻撃を識別するシグネチャベースの検知手法と、ポリシーあるいはルールセットによって未知の攻撃を識別するアノマリベースの検知手法を組み合わせて使用するものが多い。この項では、次の観点からホストベースの IDPS の検知機能について説明する。

- 検知されるイベントの種類
- 検知の正確さ
- チューニングおよびカスタマイズ
- 技術的な制約.

7.2.2.1 検知されるイベントの種類

ホストベースの IDPS によって検知されるイベントの種類は、使用する検知手法によって大きく異なる。数種類の検知手法を採用している IDPS 製品もあれば、少数または 1 つの手法しか使用しない製品もある。たとえば、製品によってはネットワークトラフィックの解析だけを行うものや、ホストの重要なファイルの完全性チェックだけを行うものがある。ホストベースの IDPS でよく使用される具体的な手法としては、次のようなものがある。

- **コード解析**：エージェントは、次のいずれか 1 つまたは複数の手法を用いて、コードの実行を試みる活動を解析することで悪意のある活動を特定する。いずれの手法も、マルウェアの阻止に有効であるだけでなく、その他の種類の攻撃（たとえば、無許可のアクセスやコード実行、権限昇格などを許可するもの）を防ぐのにも役立つ。
  - **コードの挙動解析**：コードをホスト上で普通に実行する前に、まず仮想環境またはサンドボックス内で実行して挙動を解析し、既知の無害または有害な挙動についてのプロファイルやルールと比較する。たとえば、特定の一まとまりのコードが実行された場合、管理者レベルの特権を獲得しようとする、あるいは、システムの実行可能ファイルを上書きしようとするかもしれない。
  - **バッファオーバーフロー検知**：スタックやヒープバッファにオーバーフローを発生させようとする試みを、その典型的な特徴（たとえば、特定の順序で命令が実行され、当該プロセスに割り当てられている領域以外のメモリにアクセスしようとするなど）を探すことによって検知する。

- **システムコールの監視**：エージェントは、どのような種類のアプリケーションおよびプロセスが、他のどのようなアプリケーションやプロセスを呼び出すべきか、あるいは、特定のアクションを実行するべきかを把握している。これにより、たとえばキーボード入力の傍受を試みるプロセス（キーロガーなど）を認識することができる。その他の例としては、COM（コンポーネントオブジェクトモデル）オブジェクトの読み込みを制限することにより、電子メールクライアントのアドレス帳に PDA アプリケーションからアクセスすることは許可し、他のアプリケーションからのアクセスを拒否するエージェントがある。また、ルートキットのインストールおよびその他の攻撃を防ぐために、読み込み可能なドライバを限定する方法も用いられる。
- **アプリケーションおよびライブラリの一覧**：ユーザあるいはプロセスが読み込もうとする個々のアプリケーションおよびライブラリ（DLL：ダイナミックリンクライブラリなど）をエージェントが監視して、許可済みまたは未許可のアプリケーションおよびライブラリの一覧と比較する。これにより、使用できるアプリケーションおよびライブラリの種類だけでなく、それらのバージョンを限定することもできる。

■ **ネットワークトラフィック解析**：これは、ネットワークベースの IDPS の機能と似たものであることが多い。製品によっては有線ネットワークおよび無線ネットワークのトラフィックを解析することができる。ネットワーク層、トランスポート層、アプリケーション層のプロトコルの解析の他、よく使用される電子メールクライアントなど一般的なアプリケーションに対する特別な処理もエージェントが行うことがある。また、電子メール、Web、ピアツーピアファイル共有などのアプリケーションによって転送されるファイルも、トラフィック解析により抽出してマルウェアのチェックを実行できる。

■ **ネットワークトラフィックのフィルタ処理**：エージェントの多くは、システム上のアプリケーションごとにトラフィックの出入りを制限するホストベースのファイアウォールを備えており、不正アクセスや利用規定違反（不適切な外部サービスの利用など）を防止することができる。このファイアウォール機能は、監視対象ホストが通信を行うべき相手ホスト（特に組織内のホスト）の一覧を生成および使用する能力を備える場合もある。

■ **ファイルシステム監視**：ファイルシステムを監視するための手法は、次に示すものを含めいくつかある。製品によっては、ファイル名に基づいて監視を行うものがあり、ユーザまたは攻撃者によってファイル名が変更されることにより、ファイルシステム監視手法が無効化される可能性があるため、管理者は注意する必要がある。

- **ファイルの完全性チェック**：重要なファイルのメッセージダイジェストまたはその他の暗号チェックサムを定期的に生成し、参照値と比較することで違いを検知する。ファイルの完全性チェックでは、すでに行われたファイル変更（トロイの木馬やルートキットによるシステムバイナリの置き換えなど）を事後に検知することのみ可能である。
- **ファイルの属性チェック**：重要なファイルの属性（所有者、アクセス許可など）に変更がないかを定期的にチェックする。ファイルの完全性チェックと同じく、すでに加えられた変更を事後にのみ検知できる。
- **ファイルアクセスの試み**：ファイルシステムのシムを使用するエージェントは、重要なファイル（システムバイナリなど）にアクセスしようとする操作をすべて監視し、疑わしいものを阻止することができる。エージェントが保持しているファイルアクセスのポリシーセットと、行われようとしているアクセスの特徴を比較し、どのようなユーザまたはアプリケーションが各ファイルへのアクセスを試みているか、どのような種類のアクセス（読み取り、書き込み、実行）が要求されたかなどに基

づいてアクセスの可否を判断する[43]。これにより、いくつかの形態のマルウェア（ルートキット、トロイの木馬など）がインストールされるのを防ぐ他、ファイルのアクセス、変更、置き換え、または削除を伴うさまざまなタイプの悪意のある活動を防止することができる。

- **ログ解析**：一部のエージェントには、OSおよびアプリケーションのログを監視・解析することで悪意のある活動を特定する機能がある[44]。解析対象のログに含まれている可能性がある情報の種類としては、システムイベント（システムのシャットダウンやサービスの開始など、OSの構成要素により実行される運用アクション）、監査記録（認証の成功／失敗やセキュリティポリシーの変更など、セキュリティイベントに関する情報）、アプリケーションイベント（アプリケーションの起動と終了、エラーによる停止、設定の大きな変更など、アプリケーションにより実行される重要な運用アクション）がある。
- **ネットワーク設定の監視**：一部のエージェントには、ホストの現在のネットワーク設定を監視して変更を検知する機能がある。一般に、有線、無線、仮想プライベートネットワーク（VPN）、およびモデムを含む、当該ホストのすべてのネットワークインタフェースが監視の対象となる。ネットワーク設定の大きな変更の例としては、プロミスキャスモードへのネットワークインタフェースの切り替え、ホスト上で使用されている TCP または UDP ポートの追加、使用されているネットワークプロトコル（たとえば IP 以外のプロトコル）の追加などがある。このような変化は、当該ホストがすでに侵害されており、以後の攻撃やデータ転送に備えて設定が変更されたことを示している可能性がある。

組織は、ホストのどのような側面を監視する必要があるかを判断し、そのための十分な監視および解析の機能を提供する IDPS 製品を選択すべきである。

ホストベースの IDPS は通常、ホストの特性および設定内容を詳細に把握しているため、ホストベースの IDPS のエージェントにおいて、あるホストに対する攻撃を阻止しなかった場合に攻撃が成功するかどうかを判断できることが多い。エージェントはこの知識に基づいて、実行する防止措置を選択したり、警報に適切な優先順位を設定したりすることができる。

7.2.2.2 検知の正確さ

他の IDPS テクノロジーと同様、ホストベースの IDPS においても、フォールスポジティブやフォールスネガティブはしばしば発生する。しかし、ホストベースの IDPS で使用できるいくつかの検知手法（ログ解析、ファイルシステム監視など）では、検知したイベントがどのような状況において発生したかを認識することができないため、正確な検知を行うことがより困難である。たとえば、ホストの再起動、新しいアプリケーションのインストール、システムファイルの置き換えといったアクションは、悪意ある活動による場合もあれば、ホストの正常な運用および保守の一環として行われる場合もある。こうしたイベント自体は正確に検知できても、それが無害であるか、悪意によるものかは、状況に関する情報を補わないと判断できない場合がある。製品によっては（特にデスクトップやノート PC 向け）、特定のアプリケーションのアップグレードを実行しようとしているかどうかなど、状況についてユーザに確認を求める。これに対してユーザの応答がないまま所定の時間（一般的には数分）が経過した場合、エージェントはデフォルトのアクション（許可または拒否）を実行する。

---

[43] Windows システムでは、多くの設定がレジストリと呼ばれる一連の特殊なファイルに格納されている。エージェントによっては、レジストリの重要な部分（特にマルウェアがよく利用する箇所）へのアクセスを制限する特殊なシムを備えるものがある。

[44] ログ解析およびログ管理（ログ統合など）だけを実行する製品もあり、これらはホストベースの IPS と呼ばれることが多いが、製品によっては、実際には SIEM（セキュリティ情報およびイベント管理）製品であるものもある。SIEM の詳細については、セクション 9 を参照のこと。

いくつかの検知手法を組み合わせて使用するホストベースの IDPS 製品のほうが、一つまたは 2～3 の手法を使用する製品よりも概して正確な検知能力を備えている。検知手法が異なれば、監視可能なホストの側面も異なるため、使用する手法が多いほど、発生している活動についてエージェントが収集できる情報の量も多くなる。それによってイベントの全体像をより的確に把握でき、場合によっては、特定のイベントの意図を知るために役立つ、状況に関する追加的な情報が得られることもある。

7.2.2.3 チューニングおよびカスタマイズ

ホストベースの IDPS では、通常、チューニングおよびカスタマイズの作業に大きな手間を要する。たとえば、多くの製品は、ホストの活動を観測して、予期される挙動のベースラインまたはプロファイルを作成することに依拠している。そうでない製品は、ホストにおいて実行される個々のアプリケーションがどのような挙動をすべきかを正確に定義した、詳細なポリシーにより設定する必要がある。ホストの環境に変更が生じた場合、管理者は、変更内容が反映されるようにホストベースの IDPS のポリシーを確実に更新しなければならない。ホストベースの IDPS システムを変更管理システムに自動的にリンクすることは現実的ではない場合が多いが、管理者は、フォールスポジティブの発生を防ぐために変更管理の記録を定期的にレビューして、ホストベースの IDPS のホストに関する設定やポリシー情報を調整することができる場合がある。

ポリシーは多くの場合、個別のホストまたはホストグループに対して柔軟に設定できる。製品によっては、1 つのホストに対して複数のポリシーを設定することもでき、複数の環境において動作するホスト（組織の内外で使用するノート PC など）においては非常に役に立つ。また、ホストベースの IDPS は、ホスト（監視対象ホストと通信できる相手先ホストの IP アドレスなど）、アプリケーション、ポート、ファイル名などのホストの特性に関するブラックリストとホワイトリストを設定することもできる。一部の製品は、他のエージェントで新しく検知された悪意のある活動に関する報告を受け、エージェントのホワイトリストおよびブラックリストの情報を最新の内容に自動的に更新する機能を備えている。ホストベースの IDPS のその他の一般的な機能としては、個々の警報のカスタマイズ（警報によって実行すべき対応措置の指定など）がある。

ホストベースの IDPS のシグネチャ機能が持つ能力の程度は、製品が使用する検知手法によって大きく異なる。

7.2.2.4 技術的な制約

ホストベースの IDPS には大きな制約がいくつかある。一部の制約については7.2.2.2項で説明したが、その他の重要な制約としては、次のようなものがある。

- **警報生成の遅れ**：ほとんどの検知手法においては警報がリアルタイムで生成されるが、すでに発生したイベントを特定するために、いくつかの手法が定期的に使用される。そのような検知手法は、1 時間に 1 回あるいは、1 日に数回程度しか適用されない場合もあるため、イベントの種類によっては特定が大幅に遅れる可能性がある。
- **集中化サーバへの報告の遅れ**：ほとんどのホストベースの IDPS では、管理サーバへの警報データ転送をリアルタイムではなく定期的に実行することが前提となっている。IDPS の構成要素とネットワークのオーバーヘッドを小さくするために、転送は 15～60 分おきにバッチ処理により行われるのが普通である。ホストベースの IDPS の小規模な導入においては、データ転送の頻度を上げることも可能であるが、大規模な導入の場合は、転送の頻度を下げるようベンダーが推奨することが一

般的である。そのため、対応措置の発動に遅れが生じ、特に、急速に拡大するようなインシデント（マルウェア感染など）が発生した場合の被害が大きくなる可能性がある。

- **ホストのリソース消費**：他の IDPS テクノロジーとは異なり、ホストベースの IDPS を使用する場合は監視対象のホストにおいてエージェントが動作する。エージェントは、メモリ、プロセッサ、ディスク領域などのホストリソースを大量に消費することがある。また、エージェントの動作（特にシム）によってネットワークやファイルシステムなどのパフォーマンスが低下する可能性もある。ホストベースの IDPS 製品の購入を検討する際には、ホストリソースの消費量に関するテストを行うべきである。

- **既存のセキュリティ管理策との競合**：エージェントをインストールすることにより、既存のホストセキュリティ管理策（パーソナルファイアウォールなど）が、当該エージェントにより提供される機能と重複すると判断されると、既存の管理策が自動的に無効化される場合がある。また、エージェントをインストールすることにより、他のセキュリティ管理策、特にシムを使用してホストの活動を傍受する管理策（パーソナルファイアウォール、VPN クライアントなど）との競合が発生する場合がある。ネットワーク用シムの使用が任意である製品もあるが、シムを使用すると防止措置などの機能が非常に強力になるメリットがある。実装の前には、エージェントが導入されるホストにおいて使用されているセキュリティ管理策と同じホストセキュリティ管理策を適用しているホストにおいてエージェントのテストを行い、競合が発生する可能性について確認すべきである。

- **ホストの再起動**：多くのホストベースの IDPS 製品では、エージェントのソフトウェアのアップグレードや、エージェントの設定変更により、監視対象ホストを再起動する必要が生じる。前述した問題と同様、製品の選定時にはこの点も考慮して綿密なテストを行い、再起動によって、エージェントの実効性にどのような影響があるかを検討すべきである（たとえば、再起動が許されない重要なホストであるために最新の脅威を検知できなくなるといった状況が考えられる）。

7.2.3 防止機能

ホストベースの IDPS のエージェントは、さまざまな侵入防止機能を備えている。防止機能は、製品で使用されている検知手法によって異なるため、個々の検知手法によって提供される防止機能を次に示す。

- **コード解析**：コード解析は、マルウェアや許可されていないアプリケーションなどのコードが実行されるのを防ぐ手法である。一部のホストベースの IDPS には、ネットワークアプリケーションによるシェルの起動（ある種の攻撃を試みるために使われることがある）を阻止する機能もある。設定とチューニングが適切であれば、コード解析は非常に効果的であり、特に未知の攻撃を阻止する上で有効である。

- **ネットワークトラフィック解析**：外部から着信するネットワークトラフィックがホストで処理されること、および、外部に出て行くネットワークトラフィックがホストから送り出されることを防ぐことができる。これは、ネットワーク層、トランスポート層、アプリケーション層で行われる攻撃（場合によっては無線ネットワークプロトコルに対する攻撃）や、許可されていないアプリケーションやプロトコルの使用を阻止するために行われる。また、解析によって、悪意のあるファイルのダウンロードあるいは転送を特定し、これらのファイルがホストに置かれることを防止することができる。ネットワークトラフィックの廃棄または拒否、疑わしいトラフィックに関連する付加的なトラフィックを締め出すことを目的としたホストのパーソナルファイアウォール（場合によってはエージェントに組み込まれているもの）の設定変更などが行われる。ネットワークトラフィック解析は、既知および未知のさまざまな攻撃を阻止する上で効果的である。

- **ネットワークトラフィックのフィルタ処理**：ホストベースのファイアウォールとして機能し、許可されていないアクセスおよび利用規定違反（不適切な外部サービスの利用など）を阻止する手法である。IP アドレス、TCP ポート、UDP ポート、または ICMP タイプ／コードによって特定できる活動に対してのみ効果がある。

- **ファイルシステム監視**：ファイルのアクセス、変更、置き換え、または削除を防ぐことができ、その結果としてマルウェア（トロイの木馬、ルートキットなど）のインストールや、不適切なファイルアクセスを伴うその他の攻撃を阻止することができる。ホスト上ですでに機能しているアクセス制御テクノロジーを補うための、追加的なアクセス制御層を提供することができる。

その他のホストベースの IDPS 検知手法（ログ解析、ネットワーク設定の監視、ファイルの完全性／属性チェックなど）は、イベントの発生後にイベントを特定するものであるため、一般に防止措置をサポートすることはできない。

7.2.4 その他の機能

一部のホストベースの IDPS は、IDPS 以外の機能（ウイルス対策ソフトウェア、スパムフィルタ、Web および電子メールのコンテンツフィルタ処理など）を備えている。これらの機能は、IDPS ソフトウェアに独立の製品をバンドルする形で提供されることが多く、本ガイドでは扱わない。この項では、ホストベースの IDPS 機能とより密接に結びついている、付加的な製品機能について述べる。次のような機能が、ホストベースの IDPS の付加機能として提供される場合がある。

- **リムーバブルメディアの使用制限**：一部の製品には、USB ベース（フラッシュドライブなど）および従来方式（CD、フロッピーディスクなど）のリムーバブルメディアの使用を制限する機能がある。これにより、マルウェアおよびその他の望まれないファイルがホストに転送されることや、機密性のあるファイルがホストからリムーバブルメディアにコピーされることを防止できる。

- **オーディオビジュアル装置の監視**：いくつかのホストベースの IDPS 製品には、ホストのオーディオビジュアル装置（マイク、カメラ、IP 電話など）が、いつ有効化または使用されたのかを検知する機能がある。このような事象は、ホストが攻撃者により侵害されたことを示す可能性がある。

- **ホストのセキュリティ強化**：一部のホストベースの IDPS には、継続してホストのセキュリティ強化を自動的に実施する機能がある。たとえば、あるアプリケーションの設定が変更され、特定のセキュリティ機能が無効になった場合に、変更を検知して当該機能を有効にすることができる。

- **プロセス状態の監視**：一部の製品には、ホスト上で動作しているプロセスまたはサービスの状態を監視し、それらが停止したことを検知すると自動的に再起動する機能がある。また、セキュリティプログラム（ウイルス対策ソフトウェアなど）の状態を監視できる製品もある。

- **ネットワークトラフィックのサニタイズ**：一部のエージェント（特にアプライアンスとして導入されるもの）には、監視対象のネットワークトラフィックをサニタイズする機能がある。たとえば、アプライアンスベースのエージェントがプロキシとして機能し、エージェントを経由するすべての要求／応答を再構築することができる。ある種の正常でない活動（特に、パケットヘッダおよびアプリケーションプロトコルヘッダ内で行われるもの）を無害化するために有効である。アプライアンスによるサニタイズ処理には、保護対象ホストに対して攻撃者が行うことができる偵察活動の量を削減する効果もある。サニタイズは、たとえばサーバ OS の特徴やアプリケーションのエラーメッセージを隠すことによる。製品によっては、機密性のある情報（社会保障番号、クレジットカード番号など）が Web サーバのページに表示されることを防止できるものもある。

7.3 管理

ほとんどのホストベースの IDPS は、いずれもよく似た管理機能を備えている。この項では、管理の主要な側面（導入、運用、保守）について述べ、それらの作業を効果的かつ効率的に実行するための推奨事項を示す。

7.3.1 導入

ホストベースの IDPS 製品を選定した場合、管理者がアーキテクチャの設計、IDPS 構成要素のテスト、構成要素に対するセキュリティ対策の実施を行った後に、IDPS を導入する必要がある。3.3.1項で示した内容への追加事項を次に示す。

- **構成要素のテストおよび配備**：テスト環境におけるホストベースの IDPS 構成要素の評価が完了したあと、実稼動環境に対して、小規模なパイロット導入を行うべきである。これによって、管理者は少数の実稼働ホスト群を対象としてチューニングやカスタマイズの作業を行うことができ、より大規模な導入に備えることができる。パイロット導入およびその後の実稼動環境における導入期間においては、エージェントのチューニングおよびカスタマイズが十分なものになるまで、防止機能を無効にしておくべきである。
- **構成要素のセキュリティ保護**：エージェントの管理やエージェントからのデータ収集を行う際に、管理サーバまたはコンソールが、個々のエージェントホストに対して、認証を通じて自身を証明する必要がある場合、認証メカニズムの適切な管理とセキュリティ確保が可能であることを確実にするべきである。たとえば、パスワードが必要な場合、すべてのエージェントホストに同一のパスワードを使用することはセキュリティ上問題がある。反面、個々のエージェントホストにすべて異なるパスワードを使用すると、エージェントの数が数百～数千にものぼる場合はパスワードの把握と管理が困難になる。認証に暗号鍵を使用する場合は、鍵の発行および配布において鍵管理が問題となり得る。

7.3.2 運用

ホストベースの IDPS の運用は、3.3.2項に示した推奨事項に従って行うべきである。ただし、エージェントの更新作業は唯一の例外である。エージェントによっては、定期的に管理サーバをチェックし、更新があれば自動的にそれを取得してインストールまたは適用する機能を備えている。この機能がないエージェントについては、更新の有無のチェック、転送、インストールまたは適用を管理者が行う必要がある。エージェントの更新機能は、多くの場合、エージェントが導入されるオペレーティングシステムの種類に関係している。

7.4 まとめ

ホストベースの IDPS は、単一のホストの特性と、そのホストの内部で発生するイベントを監視し、疑わしい活動を検知する。ホストベースの IDPS による監視の対象となる特性の例としては、有線および無線のネットワークトラフィック、システムログ、実行中のプロセス、ファイルに対するアクセスおよび変更、システムやアプリケーションの設定の変更などがある。ほとんどのホストベースの IDPS には、監視対象のホストにインストールされる「エージェント」と呼ばれる検知用ソフトウェアが含まれる。各エージェントは、1 つのホスト上で行われる活動を監視し、防止機能が有効になっている場合は防止措置も実行する。エージェントは、データを管理サーバへ送信する。個々のエージェントは一般に、特定のサーバ、デスクトップまたはノート PC、アプリケーションサービスを保護するように設計されている。

一般に、ホストベースの IDPS を導入する際のネットワークアーキテクチャは非常に単純である。エージェントは、組織のネットワークに属する既存ホストに導入されるので、構成要素間の通信は通常、管理ネットワークではなく、組織のネットワークを使用して行われる。ホストベースの IDPS エージェントは、一般に公開されているサーバや、機密性の高い情報が保存されているサーバなど、重要なホストに導入されるのが最も一般的である。しかし、さまざまなサーバおよびデスクトップ／ノート PC 用オペレーティングシステムや特定のサーバアプリケーション向けにエージェントが用意されているため、必要があれば組織内のサーバやデスクトップ／ノート PC のほとんどにエージェントを導入することが可能である。エージェントの導入場所を選定する際の基準としては、他のセキュリティ管理策で監視できない活動を解析することの必要性、エージェントの配備／保守／監視に要するコスト、エージェントのサポートしている OS およびアプリケーション、各ホストのデータまたはサービスの重要性、ネットワークインフラストラクチャがエージェントの通信をサポートする能力などがある。

ほとんどの IDPS のエージェントは、ホストの内部アーキテクチャに変更を加え、シムを通じてインストールされる。シムは、既存コード層の間に挿入されるコード層である。シムを使用しない監視方法のほうが、ホストへの影響が少なく、IDPS がホストの通常の運用を妨げる可能性は小さい反面、脅威を正確に検知する能力が概して劣り、効果的な防止措置も実行できない場合が多い。

ホストベースの IDPS は、多様なセキュリティ機能を提供する。一般に、検知したイベントに関連するデータを詳細なログとして記録する機能や、いくつかのタイプの悪意ある活動を検知する機能を持つものがある。使用される検知手法としては、コード解析、ネットワークトラフィック解析、ネットワークトラフィックのフィルタ処理、ファイルシステム監視、ログ解析、ネットワーク設定の監視などがある。検知手法が異なれば、監視可能なホストの特性も異なるため、いくつかの検知手法を組み合わせて使用するホストベースの IDPS 製品のほうが、一つまたは 2～3 の手法を使用する製品よりも概して正確な検知能力を備えている。どのような特性について監視する必要があるかを判断し、そのための十分な監視および解析の機能を提供する IDPS 製品を選択すべきである。

ホストベースの IDPS では、通常、チューニングおよびカスタマイズの作業に大きな手間をかける必要がある。たとえば、多くの製品は、ホストの活動を観測して、予期される挙動のベースラインまたはプロファイルを作成することに依拠している。そうでない製品の場合も、ホストにおいて実行される個々のアプリケーションがどのような挙動をすべきかを正確に定義した、詳細なポリシーにより設定する必要がある。ホストの環境に変更が生じた場合、管理者は、変更内容が反映されるように、ホストベースの IDPS のポリシーを確実に更新しなければならない。

ホストベースの IDPS には、大きな制約がいくつかある。一部の検知手法は、すでに発生したイベントを特定するためのものであり、1 時間に 1 回あるいは、1 日に数回程度しか適用されない場合もあるため、イベントの種類によっては特定が大幅に遅れる可能性がある。また、多くのホストベースの IDPS では、管理サーバへの警報データの転送を 1 時間に数回程度のバッチ処理で実行するため、対応措置の発動に遅れが生じる可能性がある。ホストベースの IDPS を使用する場合は、監視対象ホスト上でエージェントが動作するため、エージェントがホストのリソースを消費する結果、ホストのパフォーマンスに悪影響を及ぼす可能性がある。また、他のホストセキュリティ管理策（パーソナルファイアウォール、VPN クライアントなど）がすでに使用されている場合、エージェントをインストールすることにより、それらとの間で競合が発生する場合がある。エージェントのアップグレードや、いくつかの設定変更などが行われると、監視対象ホストを再起動する必要が生じる場合がある。

ホストベースの IDPS にはさまざまな侵入防止機能があり、それらは、製品で使用されている検知手法によって異なる。コード解析の手法は、コードが実行されるのを防ぐことができ、既知および未知の攻撃の阻止に非常に効果的である。ネットワークトラフィック解析の手法は、外部とやりとりされるネットワ

ークトラフィックを止めることによって、ネットワーク層、トランスポート層、アプリケーション層で行われる攻撃、無線ネットワークプロトコルに対する攻撃、アプリケーションやプロトコルの不正使用を阻止することができる。ネットワークトラフィックのフィルタ処理は、ホストベースのファイアウォールとして機能し、不正アクセスおよび利用規定違反を阻止する。ファイルシステムの監視は、ファイルのアクセス、変更、置き換え、または削除を防ぐ手法であり、マルウェアのインストールや、不適切なファイルアクセスを伴うその他の攻撃を阻止することができる。その他のホストベースの IDPS の検知手法は、イベントの発生後にイベントを特定するものであるため、一般に防止措置をサポートすることはできない。

一部のホストベースの IDPS は、侵入検知および侵入防止に関連する付加機能として、リムーバブルメディアの使用制限、オーディオビジュアル装置が有効化または使用されたことの検知、ホストの継続的なセキュリティ強化の自動的な実行、動作中のプロセスの状態監視および停止したプロセスの再起動、ネットワークトラフィックのサニタイズなどの機能を備えている。

（本ページは意図的に白紙のままとする）

8. 複数のIDPSテクノロジーの併用および統合

セクション 4～7 で説明したように、ネットワークベース、無線、NBA（ネットワーク挙動解析）、ホストベースという 4 種類の IDPS テクノロジーは、それぞれが根本的に異なる情報収集、ログ生成、検知、防止機能を提供する。イベントの種類によって、特定のテクノロジーでのみ検知可能であったり、特定のテクノロジーによる検知が他のテクノロジーよりも格段に正確であったり、あるいは、保護対象ホストのパフォーマンスを大きく低下させることなく綿密な解析を実行できたりと、この 4 種類はそれぞれに異なる長所を備えている。したがって、悪意ある活動の検知、防止をより網羅的かつ正確なものとし、フォールスポジティブやフォールスネガティブの発生をより低く抑えるためには、複数種類の IDPS テクノロジーの併用を検討すべきである。このセクションでは、複数の IDPS テクノロジーを併用していっそう広範な IDPS ソリューションを構築するためのガイダンスを示し、複数の IDPS テクノロジーを併用することのメリットおよびデメリットについて説明する。

複数種類の IDPS テクノロジー、または単一のテクノロジーに属する複数の製品の使用を計画している場合は、それらの IDPS 製品を何らかの形で統合する必要性の有無について検討すべきである。統合の方法には、製品同士を直接連携させる方法と、集中化ログ管理システムまたは SIEM（セキュリティ情報・イベント管理）システムに複数の IDPS 製品からデータを供給する方法の 2 通りがある。このセクションでは、異なる IDPS 製品を統合する方法と、統合のメリットおよび制約について説明する。また、IDPS テクノロジーを補完するその他のテクノロジーについて概略を示し、それらを IDPS ソリューションに取り入れることで検知／防止機能をさらに向上させる方法について述べる。

8.1 複数のIDPSテクノロジーを併用する必要性

多くの環境では、複数種類の IDPS テクノロジーを併用することなしには堅牢な IDPS ソリューションを実現することはできない。たとえば、ネットワークベースの IDPS では無線プロトコルを監視することはできず、無線 IDPS ではアプリケーションプロトコルの活動を監視することはできない。表 8-1 は、4 種類の主要な IDPS テクノロジーを概要レベルで比較したものである。長所の欄は、それぞれのテクノロジーが他のテクノロジーに比べて一般に優っている役割または状況を示す。テクノロジーによっては、他のテクノロジーにない特有の長所を備えていることがある。たとえば、他の IDPS によって記録された警報の妥当性確認に役立つ付加的なデータをログに記録するものや、他の IDPS ではテクノロジーの能力や設置場所（ネットワークではなくホストに設置されているなど）といった理由により対応できないような侵入を防止できるものがある。

表 8-1. 各種 IDPS テクノロジーの比較

IDPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor or Agent	Strengths
ネットワークベース	ネットワーク層、トランスポート層、アプリケーション TCP/IP 層の活動	複数のネットワークサブネットおよび複数のホストグループ	最も広範なアプリケーションプロトコルを解析することができる。多くのアプリケーションプロトコルは、この IDPS テクノロジーによってのみ完全な解析が可能
無線	無線プロトコルの活動。許可されていない無線 LAN（WLAN）の	複数の WLAN および無線クライアントグ	無線プロトコルの活動を監視可能な唯一の IDPS

	使用	ループ	
NBA	ネットワーク層、トランスポート層、アプリケーション TCP/IP 層において異常なネットワークフローを発生させる活動	複数のネットワークサブネットおよび複数のホストグループ	偵察スキャンおよび DoS 攻撃の識別、多数のマルウェア感染の再構成において、一般的に他のテクノロジーよりも効果的
ホストベース	ホストのアプリケーションおよびオペレーティングシステム（OS）の活動と、ネットワーク層、トランスポート層、アプリケーション TCP/IP 層の活動	単独のホスト	エンドツーエンドの暗号化通信を介して伝送される活動を解析することができる唯一の IDPS

実効性のある IDPS ソリューションを構築するには、ネットワークベースの IDPS とホストベースの IDPS を組み合わせて使用することが、ほとんどの環境において必須である。それに加え、無線 IDPS は、組織として無線ネットワークの監視を強化する必要がある場合や、不正な無線ネットワークが組織内の施設で使用されることを確実に防ぎたい場合にも必要である。また、NBA 製品は、DoS 攻撃やワームなど、セクション 6 で述べたような脅威についても検知を行いたい場合にも導入することができる。

組織によっては、複数種類の IDPS テクノロジーを併用するだけでなく、同じ IDPS テクノロジーに属する複数の製品を併用することがある。これは、検知能力を向上することを目的として行われる場合が多い。いずれの製品も、それぞれに異なる検知の方法を使用しており、他の製品で検知できないイベントを検知するため、複数製品を併用することで、発生し得るインシデントをより網羅的に検知できる可能性がある。また、複数製品（特に、いずれも同じ活動を監視するもの）が使用されていると、分析担当者が警報の妥当性を確認してフォールスポジティブを識別する作業が容易になる他、一つの製品が何らかの理由で停止した場合に備えて冗長性を確保することができる。

8.2 異なるIDPSテクノロジーの統合

複数の IDPS 製品を併用する組織は多数あり、多くの場合、組み合わされる製品は異なるベンダーのものである（ほとんどのベンダーは、特定の 1 種類の IDPS テクノロジーにのみ属する製品を開発している）。デフォルトでは、それらの製品は互いに完全に独立して機能する。このことには、1 つの IDPS 製品に障害や侵害が発生した場合に他の IDPS 製品が受ける影響を最小限にとどめるなどの点において重要なメリットをもたらす。しかし、製品が何らかの方法によって統合されていないと、導入された IDPS 全体としての実効性がいくらか限定されたものとなる可能性がある。製品がデータを共有できず、複数セットの製品の監視・管理を行うために、IDPS のユーザおよび管理者に余分な手間を強いることになる可能性がある。IDPS 製品の統合には、1 つの製品から別の製品へ警報データを供給するなど直接的に統合する方法と、すべての IDPS 製品の警報データを SIEM システムに供給するなど間接的に統合する方法がある。8.2.1 項および 8.2.2 項では、それぞれ直接統合および間接統合に関するメリットと制約について述べる。

8.2.1 直接的なIDPS統合

直接的な IDPS 統合は、単一のベンダーによって供給される複数の IDPS 製品を使用する組織において行われることが最も多い。たとえば、ベンダーによってはネットワークベース製品とホストベース製品の両方を提供している。そのようなベンダーでは、両方の種類の製品の管理・監視が可能な共通のコンソールをしばしば提供している。それにより、管理者およびユーザの作業が効率化され、大幅に時間を節約することができる可能性がある。また、データの共有が可能な製品もあり、たとえば、ネットワークベースの IDPS センサーにより検知された攻撃が成功したかどうかや、ネットワークベースの IDPS データによって阻止された攻撃が、仮に IDPS を通過していた場合に成功していたかどうかを、ホストベ

ースの IDPS のデータを使用して判定することができる。このような情報により、解析プロセスが迅速化されるとともに、ユーザによる脅威の優先順位付けに役立つ場合がある。全面的に統合されたソリューションの主要なデメリットは、1 つの障害または侵害によって、その統合ソリューションを構成するすべての IDPS テクノロジーに危険が及ぶ可能性があることである。

直接的な IDPS 統合のうち、より限定的な形態として、ある IDPS 製品から提供されるデータを別の IDPS 製品で使用するというものである。ある。前述のように、同じベンダーから提供される製品同士では、互いのデータを共有してイベント間の相関処理を行えることが多い。異なるベンダーの製品間でもデータの共有は可能であるが、一般的には、ある製品から得られるデータを単に別の製品の入力として使用できる程度のものである。たとえば、ネットワークベースの IDPS が、ネットワークフロー情報を NBA センサーに供給できる可能性がある。ホストベースの IDPS は、システム構成情報を NBA センサーまたはネットワークベースの IDPS センサーに供給できる可能性がある。このデータは、イベント間の相関処理や、警報のより正確な優先順位付けのために使用することができる。

8.2.2 間接的なIDPS統合

間接的なIDPS統合は、通常、SIEM（セキュリティ情報およびイベント管理）ソフトウェアを使用して行われる [45]。SIEMソフトウェアは、さまざまなセキュリティ関連ログから情報をインポートして、イベントの相関関係を抽出するよう設計されている [46]。SIEMソフトウェアによりサポートされる一般的なログの種類としては、IDPS、ファイアウォール、ウイルス対策ソフトウェア、その他のセキュリティソフトウェア、OS（監査ログなど）、アプリケーションサーバ（Webサーバ、電子メールサーバなど）、物理的セキュリティ装置（IDカードリーダなど）がある。SIEMソフトウェアの動作の概要は、ログ供給元ホストからセキュアなネットワークチャネルを経由してログのコピーを受信し、ログデータを標準的なフィールドおよび値に変換（*正規化*）し、さらに、IPアドレス、タイムスタンプ、ユーザ名などの特徴を照合して関連するイベントを特定するというものである [47]。SIEM製品は、攻撃やマルウェア感染など悪意のある活動と、システムおよびネットワークの誤用や不適切な使用も識別することができる。また、一部のSIEMソフトウェアには、指定されたイベントに対応して防止措置を発動する機能もある。SIEM製品は、一般に、元のイベントデータを生成しない代わりに、インポートしたイベントデータの分析結果に基づくメタイベントを生成する。

SIEM ソフトウェアは、次のような面で IDPS を補完する役割を果たす。

- 異なる複数のテクノロジーによって記録されるイベント間の相関を行う機能により、個別の IDPS では識別することができないある種のイベントを識別することができる。
- SIEM ソフトウェア用のコンソールにより、多数のソースから得られるデータを単一のインタフェース上で利用できるようにし、複数の IDPS を監視しなければならないユーザの作業時間を短縮する。また、IDPS コンソールに必ずしも備わっていない解析および報告のツールが SIEM コンソールによって提供される場合もある。

---

45 SIEM ソフトウェアおよびログ管理の詳細については、NIST SP 800-92『*Guide to Computer Security Log Management*(コンピュータセキュリティログ管理ガイド)』(http://csrc.nist.gov/publications/nistpubs/)を参照のこと。

46 SIEM は、セキュリティイベント管理（SEM：Eecurity Event Management）またはセキュリティ情報管理（SIM：Security Information Management）と呼ばれる場合もある。

47 IPS のログ形式またはデータフィールドについては、広く受け入れられている標準は存在しない。そのため、各種の IPS 製品はそれぞれ独自の形式でログを記録している。

- 個々の警報と、他のログから得られる補足情報とを関連づけることにより、ユーザは、IDPS 警報の正確さをより容易に確認することができるようになる。また、特定の攻撃が成功したかどうかの判定にも役立つ。

IDPS との関係における SIEM ソフトウェアの制約事項としては、次のようなものがある。

- イベントが開始した時点から、それに対応するログデータを SIEM が得るまでの間にしばしば大きな遅延が生じる。ログデータが、たとえば 5～10 分おきにバッチ処理でログ供給元から SIEM へと転送されたとする。その結果、悪意ある活動の警報は SIEM コンソールよりも先に IDPS コンソールに表示されることが多く、防止措置のタイミングはより遅くなる。
- SIEM 製品は通常、元のログに含まれる情報のうち一部のデータフィールドしか転送しない。たとえば、ネットワークベースの IDPS によりパケットが記録されても、帯域幅およびストレージの制約により、それらのパケットが SIEM に転送されない場合がある。また、ログ正規化プロセスによって個々のデータフィールドを標準的な形式に変換し、一貫性をもってデータを分類する過程で、データにエラーが発生したり一部のデータが失われたりする場合がある。幸い、SIEM 製品の多くは元のデータソースを改変しないため、必要に応じて元のデータを参照することにより、データの正確さを検証することができる。
- IDPS 製品によっては、それに対応する SIEM ソフトウェアのエージェントが提供されていないことがある。その場合、IDPS データを SIEM サーバへ転送するエージェントを管理者が作成するか、IDPS 側のログ記録を別のメカニズムを使用して行わせることにより、ログ形式を SIEM ソフトウェアが認識可能なものにするなどの必要がある。

SIEMソフトウェアを使用する他に、ログの集中化を実現する方法としては、主にsyslogプロトコルを基礎にしたソリューションを使用することが考えられる [48]。syslogはログの生成、保存、転送に関する単純な枠組みであり、これに対応して設計されたすべてのIDPSが使用することができる。IDPSによっては、ログの形式をsyslog形式に変換する機能を持つものもある。各syslog項目には、ログ生成元の任意の形式で情報を格納することができる内容フィールドがあり、ログ生成元にとっては非常に柔軟性の高い形式である。しかし、この柔軟性によって、ログデータの解析に問題が発生する。それぞれのIDPSが、多数の異なるログメッセージ形式を使用する可能性があるため、堅牢な解析プログラムには、各ログ形式を十分に理解し、それぞれの形式のフィールドに含まれるデータの意味を抽出できるようにすることが求められる。すべてのログメッセージの意味を理解することが現実的でない場合には、解析をキーワードやパターンの検索のみに限定することも考えられる。一般に、IDPSログを集中的に収集し、解析する手段としてsyslogを使用すると、インシデントの識別・対応作業をサポートする十分に強力な解析能力を得ることはできない。

8.3 IDPS機能を提供するその他のテクノロジー

多くの組織では、IDPS専用のテクノロジーを使用するだけでなく、ある程度のIDPS機能を持つ他の種類のテクノロジーをいくつか用意し、主要なIDPSを補完するために使用している。この項では、よく使用

[48] syslog は長年にわたって使用されているが、公式には標準化されていない。2001 年 8 月発行の RFC（Request for Comments）3164『*The BSD Syslog Protocol*』は、既存の実装において一般的に使用されている syslog メッセージ形式を説明した非公式 RFC の 1 つである（http://www.ietf.org/rfc/rfc3164.txt）。デフォルトでは、syslog の伝送メカニズムはひじょうに単純である。RFC 3164 では、「…UDP ポート 514 に送られるあらゆる IP パケットのペイロードは、有効な syslog メッセージとみなさなければならない」と述べている。2001 年 11 月発行の RFC 3195『*Reliable Delivery for Syslog*』では、syslog 用として複数の伝送メカニズムを定義している（http://www.ietf.org/rfc/rfc3195.txt）。

される補助テクノロジーとして、ネットワークフォレンジック分析ツール、マルウェア対策テクノロジー（ウイルス対策ソフトウェアとスパイウェア対策ソフトウェア）、ファイアウォールとルータ、およびハニーポットについて説明する[49]。このそれぞれについて、テクノロジーの概要と、侵入検知および侵入防止における用途、ならびにIDPSとの関係について説明する。また、補助テクノロジーをIDPSと組み合わせて使用する方法に関する推奨事項も必要に応じて示す。

8.3.1 ネットワークフォレンジック分析ツール（NFAT）ソフトウェア

ネットワークフォレンジック分析ツール（NFAT：Network Forensic Analysis Tool）は、有線ネットワークのトラフィックの収集・解析に主眼を置くソフトウェアである。ネットワークベースの IDPS が綿密な解析を実行して必要なネットワークトラフィックだけを保存するのに対し、NFAT は観測するトラフィックの大半またはすべてを保存し、保存されたトラフィックを対象に解析を実行するのが一般的である。NFAT ソフトウェアには、フォレンジック機能に加え、ネットワークトラフィックの解析に役立つ次のような機能がある。

- 個々のセッション（2 人のユーザ間のインスタントメッセージング（IM：instant messaging）など）からすべてのセッションにいたるまで、一定期間内の全てのネットワークトラフィックをツールの内部で再生することにより、イベントを再現する。一般的に、再生速度を必要に応じて調整できる。
- トラフィックの流れやホスト間の関係を視覚化する。ツールによっては、IP アドレス、ドメイン名、またはその他のデータを物理的な場所に結び付け、活動の地理的なマップを作成することもできる。
- 典型的な活動のプロファイルを作成し、そこからの大幅な逸脱を明らかにする。
- アプリケーションの内容からキーワード（たとえば、「confidential（機密）」、「proprietary（企業秘密）」など）を検索する。

このため、NFAT は一般的なネットワークベースの IDPS と比べて、ネットワークフォレンジックスにおける有用性が高い一方、侵入検知および侵入防止における有用性は低いといえる。

NFAT ソフトウェアは、次のような面で IDPS を補完する役割を果たす。

- パケットの広範なログを記録するため、ネットワークフォレンジックスにおいて、IDPS ソフトウェアよりも有用であることが多い。
- パケットのログ記録を NFAT ソフトウェアで実行することにより、ネットワークベースの IDPS センサーの負荷を軽減することができる。
- 一部の IDPS テクノロジーと比べてカスタマイズに適している場合がある（特に、キーワードなどによる内容検索を行う場合）。
- IDPS コンソールに備わっていない解析、視覚化、報告の機能が、一部の NFAT グラフィカルユーザインタフェース（GUI）に備わっている。

IDPS との関係における NFAT ソフトウェアの制約事項としては、次のようなものがある。

---

[49] 補助ツールの詳細については、NIST SP 800-86『*Guide to Integrating Forensic Techniques into Incident Response*(インシデント対応へのフォレンジック技法の統合に関するガイド)』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

- 通常、ネットワークベースの IDPS にあるような侵入検知機能を備えていない。
- 侵入防止機能を通常は備えていない。

8.3.2 マルウェア防止テクノロジー

マルウェアの脅威を軽減するための対策として最もよく使用されている技術的な管理策は、ウイルス対策ソフトウェアである。ウイルス対策ソフトウェアで検知できるマルウェアの種類としては、ウイルス、ワーム、トロイの木馬、悪意のあるモバイルコード、複合型脅威、および攻撃ツール（キーストロークロガー、バックドアなど）がある。一般に、ウイルス対策ソフトウェアは、重要な OS 構成要素、ファイルシステムおよびアプリケーションの活動を監視してマルウェアの形跡を探し、マルウェアを含んだファイルの感染除去または隔離を試みる。ほとんどの組織では、マルウェアの侵入口となる主要な媒介要素すべてを監視するために、ウイルス対策ソフトウェアを中央（電子メールサーバ、ファイアウォールなど）およびローカル（ファイルサーバ、デスクトップ、ノート PC など）の両方に導入している。

マルウェアによる脅威を軽減するためによく使用されているもう 1 つの管理策は、スパイウェア検出・駆除ユーティリティ（スパイウェア対策ソフトウェア）である。これはウイルス対策ソフトウェアに似ているが、マルウェア形態およびマルウェア以外の形態をとるスパイウェア（悪意のあるモバイルコードおよび追跡クッキー）、各種スパイウェアインストール手法（無許可の Web ブラウザプラグインインストールなど）、ポップアップ広告、Web ブラウザハイジャックの検知に主眼を置くものである。

ウイルス対策製品およびスパイウェア対策製品では、いずれも主としてシグネチャベースの解析によって脅威を検知する。また、未知の脅威を識別するために、特定の疑わしい特徴を示す活動を検出するヒューリスティック（発見的）技法も使用する。新種の脅威が出現すると、ベンダーは新しいシグネチャを作成・提供し、自社製品がその脅威を検知できるようにする。

ウイルス対策ソフトウェアおよびスパイウェア対策ソフトウェアは、次のような面で IDPS を補完する役割を果たす。

- IDPS が備えるマルウェアおよびスパイウェアの検知能力は限定的である（感染の広がったワームなど非常によく見られる脅威に検知対象が限られることが多い）ため、IDPS では検知することができない多数の脅威をウイルス対策ソフトウェアおよびスパイウェア対策ソフトウェアは検知することができる。
- NBA テクノロジーでは、通常とは異なるトラフィックフローに基づいてワームの感染を検知することができる可能性はあるが、ワームの種類まで特定できる可能性は小さい。ウイルス対策ソフトウェアは、当該脅威が既知のもので、それに対応するシグネチャを持っている限りは、ワームの具体的な種類を特定することができる。
- ウイルス対策ソフトウェアとスパイウェア対策ソフトウェア(ウイルス対策ソフトウェアより軽減の程度は小さいが)は、IDPS の負荷を軽減することができる。たとえば、特定のワームの識別をウイルス対策ソフトウェアで行うようにし、IDPS センサーのワーム用シグネチャを無効にすることによる。これは、特にマルウェア感染が広範囲に発生しているときに重要である。そのような場合に IDPS がワーム警報で飽和状態に陥ると、他の重要なイベントが同時に発生しても IDPS ユーザに通知されない可能性があるためである。

IDPS との関係におけるウイルス対策ソフトウェアおよびスパイウェア対策ソフトウェアの制約事項としては、次のようなものがある。

- マルウェアおよびスパイウェア以外の脅威は検知できない。
- ウイルス対策ソフトウェアの監視対象は、非常に一般的なアプリケーションプロトコルのみに限られることが多いため、ネットワークサービスワームを認識する能力は、しばしばネットワークベースの IDPS や NBA ソフトウェアの方が優れている。また、スパイウェア対策ソフトウェアは一般に、ネットワークサービスワームを検知することができない。通常、ネットワークベースの IDPS および NBA ソフトウェアは、すべてのプロトコルを監視することができる。
- 新種の脅威が出現した場合、ベンダーから新しいシグネチャが提供されて更新がインストールされるまで、ウイルス対策ソフトウェアとスパイウェア対策ソフトウェアは、その脅威を認識することができないことが多い。IDPS 管理者は、IDPS 用のシグネチャを独自に作成することもできるため、場合によっては（特に、脅威が容易に識別可能な性質を備えている場合など）、新しいシグネチャが提供されるまでの間に、IDPS が新種の脅威を検知することができる可能性がある。ウイルス対策ソフトウェアおよびスパイウェア対策ソフトウェアでは、管理者がシグネチャを独自に作成することは一般に認められていない。新種のワームについても、NBA ソフトウェアを使用すれば、その異常なトラフィックパターンにより認識できることが多い。

8.3.3 ファイアウォールとルータ

ファイアウォール（ネットワークベースおよびホストベース）とルータは、TCP/IP の特性、たとえば、送信元および送信先 IP アドレス、トランスポート層プロトコル（TCP、UDP、ICMP など）、基本的なプロトコル情報（たとえば、TCP または UDP のポート番号、ICMP のタイプおよびコード）などに基づいてネットワークトラフィックのフィルタ処理を行う。ほとんどのファイアウォールおよびルータでは、どの接続または接続の試みを遮断したのかについての情報をログに記録する。遮断された活動の多くは、自動化された攻撃ツール、ポートスキャン、マルウェアなどによる無許可のアクセスの試みによって発生するものである。一部のネットワークベースのファイアウォールは、プロキシとしても機能する。プロキシを使用すると、接続の試みが成功するたびに実際には 2 つの別々の接続が作成される。1 つはクライアントとプロキシサーバとの接続であり、もう 1 つはプロキシサーバと実際の接続先との接続である。多くのプロキシは特定のアプリケーション専用であり、実際に HTTP などの一般的なアプリケーションプロトコルの分析および検証を行うものもある。プロキシは、無効だと思われる（何らかの攻撃が含まれる可能性がある）クライアントの要求を拒否し、それらの要求に関する情報をログに記録する。

ファイアウォールおよびルータは、次のような面でIDPSを補完する役割を果たす [50]。

- ネットワークベースのファイアウォールおよびルータでは、NAT（Network Address Translation：ネットワークアドレス変換）処理がよく実行される。NAT は、あるネットワーク上のアドレスを別のネットワーク上のアドレスにマッピングする処理である。これは、内部ネットワークのプライベートアドレスを、インターネットに接続しているネットワーク上の 1 つ以上のパブリックアドレスにマッピングすることで行われる場合が最も多い。NAT を実行するファイアウォールおよびルータは、通常、個々の NAT アドレスおよびマッピングを記録している。NAT を実行する装置の先にあるホストの実際の IP アドレスを IDPS ユーザが特定するには、このマッピング情報を参照する必要がある。

[50] 一部のファイアウォールやルータでは、IDPS ソフトウェアを実行することもできる。この項では、ファイアウォールおよびルータの中心的な機能にのみ着目し、アドオン IDPS 機能については扱わない。

- ネットワークを経由して伝送される新種の脅威（ネットワークサービスワーム、サービス妨害攻撃など）を、IDPS およびその他のセキュリティ管理策（ウイルス対策ソフトウェアなど）によって阻止することができない場合には、そのような脅威を遮断するためにファイアウォールまたはルータの設定を一時的に変更する必要が生じることがある。
- セクション 4～7 で触れたように、多くの IDPS には、特定の脅威を阻止するためにファイアウォールやルータの設定を変更する機能がある。
- ルータは、NBA 導入におけるデータソースとしてよく使用される。

IDPS との関係におけるファイアウォールおよびルータの制約事項としては、次のようなものがある。

- ファイアウォールおよびルータでは、ほとんどの種類の悪意ある活動は検知できない。
- ファイアウォールおよびルータがログに記録する情報は比較的少ない。たとえば、拒否された接続の試みに関する基本的な特性のみに限られることなどが多く、パケットの内容を記録することはほとんどない。NBA テクノロジーおよび一部のネットワークベースの IDPS は、ネットワークトラフィックに関して、ファイアウォールやルータが記録するよりもはるかに豊富な情報を記録することができる。

8.3.4 ハニーポット

組織によっては、広範囲に拡大するインシデント（新種の深刻なワームなど）の最も初期の兆候をも検知することが非常に重要であると考え、このような脅威に関するデータをより多く収集するために、ハニーポットなどの偽装手段を採用している。*ハニーポット*は、業務上の機能をいっさい果たさないため、ハニーポット管理者以外に権限を有するユーザを持たないホストである。これらのホストに対して行われるすべての活動は疑わしいものとみなされる。攻撃者のスキャンや攻撃はハニーポットに対しても行われるため、管理者は新しい傾向や攻撃ツール（特にマルウェア）に関するデータを入手することができる。ただし、ハニーポットはあくまで補助的なものであり、侵入検知および侵入防止システムなど他のセキュリティ管理策を代替することはできない。ハニーポットを使用する組織では、インシデント対応および侵入検知分析の資格を持つ担当者がハニーポットを管理すべきである。ハニーポットの合法性はまだ完全に確立していないため、ハニーポットの導入を計画する際に、法律上の副次的影響について慎重に検討するべきである。

8.4 まとめ

4 種類の IDPS テクノロジー（ネットワークベース、無線、NBA、ホストベース）は、それぞれが根本的に異なる情報収集、ログ、検知、防止機能を提供する。イベントの種類によって、特定のテクノロジーでのみ検知可能であったり、特定のテクノロジーによる検知が他のテクノロジーよりも格段に正確であったりと、この 4 種類はそれぞれに異なる長所を備えている。したがって、悪意ある活動の検知、防止をより網羅的かつ正確なものとするために、複数種類の IDPS テクノロジーの併用を検討すべきである。多くの環境では、複数種類の IDPS テクノロジーを併用することなしには堅牢な IDPS ソリューションを実現することはできない。実効性のある IDPS ソリューションを構築するには、ネットワークベースの IDPS とホストベースの IDPS を組み合わせて使用することが、ほとんどの環境において必須である。それに加え、無線 IDPS は、組織として無線ネットワークの監視を強化する必要がある場合や、不正な無線ネットワークが組織内の施設で使用されることを確実に防ぎたい場合にも必要である。また、NBA テクノロジーは、DoS 攻撃やワーム、その他 NBA が特に優れた検知能力を示す脅威について脅威についても検知を行いたい場合にも導入することができる。

複数種類の IDPS テクノロジー、または単一のテクノロジーに属する複数の製品の使用を計画している場合は、それらの IDPS 製品を何らかの形で統合する必要性の有無について検討すべきである。単一ベンダーの IDPS 製品を複数使用する場合は、直接的な IDPS 統合により、複数の製品を 1 つのコンソールで監視・管理できることが多い。また、製品によってはデータを共有できるため、解析プロセスが迅速化されるとともに、ユーザによる脅威の優先順位付けに役立つ場合がある。直接的な IDPS 統合のうち、より限定的な形態として、ある IDPS 製品から提供されるデータを別の IDPS 製品で使用する（たとえば、ネットワークベースの IDPS が、ネットワークフロー情報を NBA センサーに供給する）というものがある。

間接的な IDPS 統合は、通常、さまざまなセキュリティ関連ログから情報をインポートして、イベントの相関関係を抽出する SIEM（security information and event management：セキュリティ情報およびイベント管理）ソフトウェアを使用して行われる。SIEM ソフトウェアは、異なるテクノロジーによって複数のログに記録されたイベントを相互に関連付ける、多数のイベントソースのデータを表示する、IDPS による警報の正確さをユーザが検証する作業を支援するために他のソースから得た裏付け情報を提供するというように、いくつかの方法で IDPS を補完する。SIEM ソフトウェアを使用する他に、ログの集中化を実現する方法としては、syslog プロトコルがある。syslog は、ログの生成、保存、転送に関する単純な標準的枠組みであり、これに対応して設計されたすべての IDPS が使用することができる。各 syslog 項目には、ログ生成元の任意の形式で情報を格納することができる内容フィールドがあり、ログ生成元にとっては非常に柔軟性の高い形式である。しかし、この柔軟性によって、ログデータの解析に問題が発生する。それぞれの IDPS が多数の異なるログメッセージ形式を使用する可能性があるため、堅牢な解析プログラムには、各ログ形式を十分に理解し、それぞれの形式のフィールドに含まれるデータの意味を抽出できるようにすることが求められる。一般に、IDPS ログを集中的に収集し、解析する手段として syslog を使用すると、インシデントの識別・対応作業をサポートする十分に強力な解析能力を得ることはできない。

多くの組織では、専用の IDPS を使用するだけでなく、いくつかの IDPS 機能を持つ他の種類のテクノロジーをいくつか用意し、主要な IDPS を（代替ではなく）補完するために使用している。補助テクノロジーとしては、ネットワークフォレンジック分析ツール、マルウェア対策テクノロジー（ウイルス対策ソフトウェアとスパイウェア対策ソフトウェア）、ファイアウォールやルータなどがある。

9. IDPS製品の選定

このセクションでは、IDPS 製品の選定に関するガイダンスを示す。まず、IDPS 製品が満たすべき一般的な要件を明確にする。次に、IDPS テクノロジーが持つ 4 つの側面（セキュリティ機能、パフォーマンス、管理、ライフサイクルコスト）を評価するための基準セットを示す。最後に、実地および書類での製品評価作業と、それぞれの評価方法が最も適している場合について簡単に述べる。IDPS テクノロジーの 4 分類（ネットワークベース、無線、NBA、ホストベース）のうち、組織としていずれを必要としているかは、ここではすでに決定しているものとする。実際のニーズに適したテクノロジーを選定する場合に有用な、それぞれのテクノロジーの比較については、セクション 8 を参照のこと。

組織として受容可能なレベルまでリスクを低減するために必要なセキュリティ管理策を明らかにするには、リスクマネジメントの手法を用いるべきである。安易に製品を選びがちであるが、リスクマネジメントのプロセスに従って最も効果的な管理策の組み合わせを採用すれば、組織のセキュリティ体制をより強力なものとすることができる。リスクマネジメントプロセスの詳細については、この文書では説明しない。NIST SP 800-30『Risk Management Guide for Information Technology Systems（IT システムのためのリスクマネジメントガイド）』を参照のこと。

9.1 一般要件

IDPS 製品の評価にあたっては、まず、IDPS ソリューションおよび IDPS 製品が満たすべき全般的な要件をあらかじめ定義しておくべきである。IDPS 製品が提供する機能およびそれらが使用する手法は、製品によって大きく異なるため、ある組織の要件に最もよく合致する製品が別の組織の要件を満たすのに適しているとは限らない。また、1 つの IDPS 製品が、組織が特定の種類の IDPS テクノロジー（たとえばネットワークベース）に課しているすべての要件を満たせない可能性があるため、場合によっては、1 種類のテクノロジーに属する複数の製品を使用する必要がある。そのような状況は、大規模な環境や、IDPS テクノロジーが複数の運用目的に使われるような環境において最も生じやすい。

9.1.1 システム環境およびネットワーク環境

対象組織のシステムやネットワークと互換性があり、かつ、システム・ネットワーク上の注目すべきイベントを監視することができる IDPS 製品を選定するために、評価者は、まずシステムおよびネットワーク環境が持つ特性を理解しておく必要がある。この知識は、IDPS ソリューションを設計し、必要な構成要素（センサー、エージェントなど）の数およびそれらを設置する場所（IDPS エージェントを実行するシステム、監視するネットワークセグメントなど）を決定するためにも必要である。考慮すべき特性としては、次のようなものがある。

- **IT 環境の技術的仕様**：これは、たとえば次のような事項である。
  - ネットワークの（論理的および地理的）アーキテクチャを示す構成図およびマップ。他のネットワークへの全ての接続と、ホストの数および設置されている場所の情報もこれに含む。
  - IDPSの保護対象となる可能性がある各ホストにおいて実行されているオペレーティングシステム（OS）、ネットワークサービス、およびアプリケーション [51]。

[51] 場合によっては（特に一部のホストベースの IDPS において）、保護が必要となるアプリケーションのバージョンを特定し、IDPS がそれらのバージョンをサポートしていることを確認する必要がある場合もある。

- IDPS と統合する必要が生じる可能性があるセキュリティ関連以外のシステム（ネットワーク管理システムなど）の各種属性。

■ **既存のセキュリティ保護策の技術的仕様**：たとえば次のような保護策が該当する。

- 既存の IDPS 実装
- 集中化ログサーバおよび SIEM ソフトウェア
- マルウェア対策ソフトウェア（ウイルス対策およびスパイウェア対策のソフトウェアなど）
- コンテンツフィルタリングソフトウェア（スパム対策ソフトウェアを含む）
- ネットワークファイアウォール、ルータ、プロキシ、および、その他のパケットフィルタ処理装置およびソフトウェア
- リンク暗号化装置、VPN（仮想プライベートネットワーク）、SSL（Secure Sockets Layer）／TLS（Transport Layer Security）など、各種の通信暗号化サービス。

9.1.2 目標および目的

既存のシステム環境およびネットワーク環境を十分に把握したあと、評価者は、IDPS を使用して達成したいと考えている技術上、運用上、業務上の目標および目的を明文化すべきである。この領域において検討すべき事項は、次のとおりである。

■ **IDPS による保護が提供されるべき脅威はどのようなものか**：**評価者は、**組織として懸念を持っている脅威の種類(組織外からもたらされる脅威と、組織内で発生する脅威（内部者による脅威）の両方を含む)を可能な限り具体的に明記する。内部者による脅威には、システムを内側から攻撃するユーザだけでなく、正当なユーザが権限を逸脱して組織のセキュリティポリシーや法律に違反する行動をとる場合も含む。

■ **利用規定違反あるいは、セキュリティ以外の理由でシステムやネットワークの使用状況を監視する必要があるかどうか**：組織によっては、システムセキュリティ上の問題ではなく人事管理上の問題とみなし得るユーザ行動を対象としたシステム利用規定を定めている。そのような行動には、たとえば、品位や価値に疑問のある内容（ポルノグラフィなど）を提供する Web サイトにアクセスする、あるいは、組織のシステムを使用して個人を攻撃する電子メールやその他のメッセージを送りつけるといったものが該当する。一部の IDPS は、このようなイベントの検知に対応した機能を備えている。使用状況を監視することは、システムやネットワークの能力が限界に達したことにより、それらのアップグレードまたは交換が必要になる時期を判断するのにも役立つ可能性がある。

9.1.3 セキュリティおよびその他のITポリシー

評価者は、製品を選定する前に、既存のセキュリティポリシーおよびその他のITポリシーの内容を確認すべきである。これは、ポリシーが、IDPS製品に必要な機能の多くを規定する一種の仕様書として機能するためである [52]。IDPS製品の選定に役立つ情報は、たとえば次のようなポリシー要素に含まれている。

[52] どのような種類の活動を許可または拒否すべかについて、十分な情報が既存のポリシーに盛り込まれていない場合は、ポリシーの実施に必要となる IDPS 製品を選定する前に、まずポリシーの改定が必要と考えられる。

- **ポリシーの目標**：ポリシーに述べられている目標を、標準的なセキュリティ目標（完全性、機密性、可用性）と、より一般的な管理目標（プライバシ、法的責任からの保護、管理のしやすさ）の両方の観点から明文化することは有用である。

- **利用規定またはその他の管理規定**：前述のように、多くの組織では、セキュリティポリシーやその他の IT ポリシーの中にシステム利用規定を盛り込んでいる。

- **具体的なポリシー違反への対処のプロセス**：IDPS がポリシー違反を検知した場合の組織としての対応方針を明確化しておくことは有用である。組織にそのような違反への対応措置をとる意図がないのであれば、違反を検知するように IDPS を設定する意味はない。組織として違反に対処する意思がある場合は、違反を検知できる IDPS 製品を選定する必要があり、場合によっては、違反を阻止するための対応措置を自動的に行うことも必要である。

9.1.4 外的要件

評価者は、組織が別の組織による監督または検査の対象となるかどうか、また、近い将来に新たな形態の監督の対象となる予定があるかどうかを把握しておく必要がある。このいずれかに該当する場合には、評価者は、監督機関が IDPS やその他の特定のセキュリティリソースの使用を要求しているかどうかの判断を行う必要がある。外的要件の例としては、次のようなものが考えられる。

- **法律に基づく、セキュリティに特有の要件**：たとえば、システムに保存されている個人を特定し得る情報（所得情報、医療記録など）の保護については法的な要件が定められていることがある。また、そのような情報を漏えいするまたは危険にさらすようなセキュリティ違反の調査についても法的な要件が定められていることがある。

- **セキュリティ上のベストプラクティスまたは善管注意義務に関する監査要件**：IDPS で必ず提供またはサポートしなければならない機能が、監査要件によって指定されていることがある。一部の IDPS は、特定の業界や市場ニッチの特殊なニーズを満たす機能を備えている（たとえば、医療施設や金融機関の法的要件を満たすよう設計された報告機能など）。

- **システム運用認可要件**：組織のシステムが運用認可の対象となる場合、評価者は、IDPS またはその他のセキュリティ保護策について運用認可機関が定める要件を把握し、考慮する必要がある。

- **法執行当局のセキュリティインシデント調査および解決に関する要件**：法執行当局が IDPS の機能について追加要件（特に、証拠としての IDPS のログの収集および保護に関するもの）を定めていることがある。

- **独立のプロセスによる評価を受けた製品の購入に関する要件**：たとえば、何らかの評価機関から特定の評価を受けた製品を購入することが組織として要求されている、あるいは、推奨されていることがある。

- **暗号の要件**：たとえば、連邦政府機関は、ネットワーク通信の保護および扱いに注意を要するデータの保存に関して、FIPS 承認済みの暗号化アルゴリズムを使用する製品を購入することが義務付けられている。また、何らかの IDPS 構成要素を国外に設置する予定がある場合、評価者は、IDPS に組み込まれている暗号要素の導入または使用に影響を及ぼし得るすべての規制や制約について考慮すべきである。

9.1.5 リソースの制約

IDPS を使用すると組織のシステムを保護することができるが、一定のコストがかかる。IDPS の使用に見合う十分なシステムおよび人員を持たない組織では、IDPS 機能のために支出を増やす意味はほとんどないといえる。したがって、評価者は次のことを考慮すべきである。

- **IDPS ハードウェア、ソフトウェア、インフラストラクチャの調達とライフサイクルサポートに要する予算**：IDPS の総所有コストは、調達コストをはるかに上回る。その他のコストとしては、ソフトウェア構成要素を実行するシステムの調達コスト、追加ネットワークの導入コスト、IDPS データ保存用の十分なストレージ確保に要するコスト、システムのインストールと設定のために専門家の支援を受けるコスト、人員の教育コストなどがある。ライフサイクルコストの詳細については、9.5 項を参照のこと。
- **IDPSの監視および保守に必要なスタッフ**：IDPSによっては、監視および保守を行う人員を 24 時間体制で配置することを前提に設計されているものがある。そのような人員の確保を期待できない場合、評価者は、常時監視を必要としないシステムや無人運用向けに設計されたシステムを探すか、IDPSの監視を（場合によっては保守も）外部委託する可能性を検討する必要がある [53]。

9.2 セキュリティ機能の要件

9.1 項で述べた一般要件に加え、評価者は、各種の目的に特化した要件セットも定義する必要がある。この項では、セキュリティ機能に関する要件を取り上げる。9.3 項～9.5 項では、それぞれ、パフォーマンス、管理、およびライフサイクルコストに関する要件について論じる。各項に示す基準は、考えられる評価基準の例であり、製品評価の際にこのまま使用することを想定したものではない。実際の組織においては、これらを参考にしつつ、組織の環境、ポリシー、および既存のセキュリティとネットワークのインフラストラクチャを考慮に入れて、実際の組織に適した独自の基準セットを策定することができる。9.6 項では、IDPS の評価作業の実施についての追加情報を示す。

個々の IDPS 製品が備えるセキュリティ機能を評価することは、いうまでもなく非常に重要である。必要な機能を備えていなければ、その製品は単体ではセキュリティ管理策として不十分であり、他の製品を選択するか、他のセキュリティ管理策（別の IDPS 製品など）と併用する必要があることになる。この項では、IDPS のセキュリティ機能に関する検討事項を、情報収集、ログの記録、検知、および防止の 4 つのカテゴリに分けて説明する。評価作業における IDPS セキュリティ機能データの収集については、9.6 項にガイダンスを示す。

9.2.1 情報収集機能

各組織は、採用する IDPS の検知手法および解析機能がどのような情報収集能力を必要とするかを明らかにし、検討している IDPS 製品のそれぞれが該当する能力を備えているかどうかを評価しなければならない。IDPS テクノロジーの各タイプが有する情報収集機能については、セクション 4～7 で示したとおりである。

[53] IDPS を部分的に外部委託する、あるいはその可能性がある場合、各組織は、委託業者が実施することができる措置の制限や、それらの措置に対する監査の実施などの外部委託固有の要件を、製品の要件に確実に反映すべきである。

9.2.2 ログ記録機能

評価対象の各IDPSソリューションが、イベントおよび警報についてどのようなログ記録機能を備えているかを慎重に調査すべきである。ログの品質（網羅性と精度の両方）は、組織が解析を行い、警報の正確さを確認し、また、記録されたイベントと他のログ生成ソース（他のセキュリティ管理策、OSのログなど）で記録されたイベントとの相関関係を見つけるための能力に影響する。したがって、少なくとも、検知したイベントの基本的な情報（タイムスタンプ、イベントの種類、イベントの発生元、イベントを検知したセンサーまたはエージェントなど）を記録できるIDPS製品を選択しなければならない。また、使用する各IDPS製品が、イベントの詳細に関する補助データを記録する機能も備えているべきである。補助データフィールドは、IDPS製品の種類ごとに固有であるが、一般的なデータフィールドについてはセクション 4～7 で示したとおりである。さらに、ユーザが、個々のログ項目とそれに対応する外部の参照情報とを関連付けるための仕組みも提供することが望まれる。参照情報としては、脆弱性を識別するための世界共通のIDであるCVE（Common Vulnerabilities and Exposures）番号 [54]や、ベンダーによるセキュリティ勧告などが考えられる。

9.2.3 検知機能

各組織は、評価対象の各 IDPS ソリューションが備える検知機能を慎重に評価するべきである。検知機能は、多くの導入環境にとって最も重要な機能である。通常、各製品はそれぞれに異なる方法論を使用して、互いにいくらか異なるイベントセットを検知するので、検知機能の比較検討は複雑な作業となる。IDPS の評価において考慮すべき事項としては、次のようなものがある。

- 評価時点でどのような活動を完全に解析し、どのような活動を部分的に解析するか。また、将来的にどのような解析機能の追加が予定されているか。たとえば次のような事項である。
  - ネットワークベースの IDPS の場合は、ネットワーク層、トランスポート層、アプリケーション層の解析対象プロトコルの一覧と、各プロトコルに対する解析処理（シグネチャベースの検知、アノマリベースの検知、ステートフルプロトコル解析など）の量に関する説明。
  - ホストベースの IDPS の場合は、具体的な監視可能リソース（ログファイル、システムファイル、ネットワークインタフェースなど）の一覧と、各種リソースの監視方法に関する説明（事後の変更検知、ファイルアクセス要求に対する能動的な処理、TCP/IP スタック監視など）。
- どのような種類のインシデントを特定できるか。たとえば、サービス妨害（DoS）攻撃、バックドア、ポリシー違反、ポートスキャン、マルウェア（ワーム、トロイの木馬、ルートキット、悪意のあるモバイルコードなど）、無許可でのアプリケーション／プロトコルの使用など。
- 識別できるインシデントの種類ごとに、どの程度網羅的な検知を行えるか（ワームの数、DoS 攻撃の種類の数など）。
- 初期設定のままのデフォルト設定がどの程度有効であるか。IDPS 製品を初めて起動したとき、そのデフォルト設定は妥当なものであることが望まれる。たとえば、大量のフォールスポジティブが生じやすい内容のシグネチャやポリシーは無効に、また、最新の重要な攻撃を識別できる信頼性の高いシグネチャやポリシーは有効になっているのが妥当である。検知のしきい値（たとえば、「y 分間に x 件を検知」といった設定）には、フォールスポジティブとフォールスネガティブのバランスを配

[54] CVE の詳細については、NIST SP 800-51『*Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*』（http://csrc.nist.gov/publications/nistpubs/）、および CVE の Web サイト（http://cve.mitre.org/）を参照のこと。

慮した値が設定されるべきである。また、特にリソースを多く使用する機能は無効になっていることが望ましい。

- 既知の悪意あるイベント（攻撃、スキャン、マルウェアなど）をどの程度効果的に検知できるか。既知のイベントの認識においては、一般的にアノマリベースの検知やステートフルプロトコル解析よりもシグネチャベースの検知手法のほうが優れている。この能力には、使用された悪用手段や標的にされた脆弱性の情報（CVE 参照番号など）を的確に示す機能があるかどうかも含めて検討すべきである。

- 未知の悪意あるイベント（新種の攻撃、既知の攻撃の変種など）を、IDPS の設定変更や更新をすることなく、どの程度効果的に検知できるか。未知のイベントの認識においては、一般的にシグネチャベースの検知手法よりもアノマリベースの検知およびステートフルプロトコル解析手法のほうが優れている。

- 回避テクニックによって隠蔽された既知または未知の悪意あるイベントをどの程度効果的に検知できるか。回避テクニックには、異常な IP パケット分割、標準的でないアプリケーションポートの使用、代替文字セットや異なる文字エンコーディングの使用などの方法がある。

- 攻撃の成功または失敗をどの程度正確に判定できるか。

- どのような対応メカニズムを備えているか。ただし、防止措置（9.2.4 項を参照）を除く。これには、たとえばログへのイベント情報の記録（ローカルおよびリモートログサーバの両方に）、コンソールへの警報表示、SNMP（Simple Network Management Protocol）トラップ、電子メール、テキストメッセージ、ページャ呼び出しの送信などが含まれる。また、イベントの優先順位付けを効果的に行えるかどうかもこの基準に含まれる（たとえば、特定の種類のイベントが発生した場合や、イベントに特定のシステムまたはサービスが関与した場合に異なる措置を実行できるかなど）。

- 管理者がシグネチャやポリシーなどの設定項目に変更を加えて、検知機能をどの程度カスタマイズできるか。カスタマイズの例としては、ホワイトリスト、ブラックリスト、しきい値の変更、コードのカスタマイズによるフォールスポジティブ、フォールスネガティブの削減、独自のシグネチャやポリシーの作成（完全な新規作成、サンプルや枠組みに基づいた作成）などがある。カスタマイズ作業の容易さについても評価すべきである（GUI を使用するか、テキストファイルを編集するかなど）。さらに、カスタマイズを行うためにプログラミング言語の知識が要求される場合は、次のような事項も検討する。

  - 一般によく知られている言語を使用しているか、それとも、管理者が新たに習得する必要がある特殊なまたは独自の言語か
  - 言語の複雑さ、強力さはどの程度か
  - カスタマイズを支援する開発環境その他のツールが製品に含まれているか（構文チェックツールや、カスタマイズ内容を導入する前にテストを実施することができる仮想マシンなど）
  - 製品の更新時またはアップグレード時に、コードのカスタマイズ内容はどのように保存されるか

- 他の情報源から得られるデータ（脆弱性スキャンの結果や、他の IDPS のログなど）を、イベント間の相関処理や警報の的確な優先順位付けのためにどの程度有効に活用できるか。

9.2.4 防止機能

IDPS ソリューションが防止措置を実行する必要があるかどうかについては、組織としての将来的なニーズも含めた必要性の有無を決定したうえで、採用候補製品それぞれに備わる防止機能を評価すべきである。防止機能のほとんどは、IDPS の種類ごとに固有のものである。共通する機能については、IDPS 製品の種類ごとにセクション 4～7 で示したとおりである。防止手法の種類によっては、特定の状況において他の手法よりも防止効果が向上または低下することがあるため、一般的には、可能であれば 1 つではなく複数の防止機能を備えた製品を採用することが望ましい。すべての IDPS 製品には、防止手法の設定オプションでかなり粒度の細かい設定が可能であることが望まれる。たとえば、特定の警報だけを有効化／無効化したり、ホワイトリストに登録したホストに対して防止手法を実行しないようにしたり、管理者が使用する防止手法を個々の警報ごとに指定したり（複数の手法を使用できる場合）することができる能力があることが望ましい。一部の製品には、さらに粒度の細かい設定が用意されており（特定のシステムが攻撃された場合に限り防止措置を実行するなど）、場合によって有用である。

9.3 パフォーマンス要件

IDPS 製品のパフォーマンスを比較することには、次のような理由により困難が伴う。

- 各製品の設定やチューニングによってパフォーマンスが大幅に変化する。それぞれの製品のデフォルト設定のままでテストを実行することも考えられるが、製品によっては、使用する前に広範なカスタマイズおよびチューニング作業を行うことを前提に設計されているものがある。
- パフォーマンスと検知能力はトレードオフの関係にあることが多い。提供する検知機能が複雑、堅牢であるほど、そのために必要な処理能力やメモリ量も多くなり、パフォーマンスの面ではしばしば不利になる。
- 多くの IDPS 構成要素はアプライアンスベースで、数多くのハードウェアモデルや設定が用意されており、それぞれパフォーマンス特性が異なる。アプライアンスベースでない IDPS 構成要素については、ハードウェア、OS、および OS 構成が非常に多岐に渡り、それらの違いがすべてパフォーマンスに影響する。
- パフォーマンスのテストに関する公開標準は存在しない。また、広く入手可能かつ網羅的で最新の内容を持つテストスイートも存在しない。

したがって、評価は IDPS 製品の全般的なパフォーマンス特性に主眼を置いて行うべきであり、報告されたパフォーマンスのわずかな違いによって製品の評価を左右させるべきではない。ベンダーが自社製品の評価を示す際には、能力の最大値を示すのが普通である。これは、ネットワークベースの IDPS の場合、たとえば 1 秒あたりに監視可能なネットワークトラフィック量やパケット数などであり、ホストベースの IDPS の場合は 1 秒あたりに監視可能なイベント数などである。また、NBA システムの場合は 1 秒あたりに監視可能なフロー数やプロファイルが可能なホスト数などである。評価作業における IDPS パフォーマンスデータの収集については、9.6 項にガイダンスを示す。主張されている性能の最大値を評価する際、評価者は次の事項を考慮すべきである。

- 性能の最大値は、解析対象となる活動内容を反映したものであるか、あるいは監視対象ではあるが必ずしも解析対象とならない活動によるものであるか。たとえば、ネットワークベースの IDPS は、

使用されるアプリケーションプロトコルによっては解析処理をほとんどあるいは全く実行しない場合がある。

- 性能は、どのような性質の活動を使用して計測されたものであるか。この情報があると、テストが評価者の使用する実際の環境に近い条件で行われたか、あるいはテストにパフォーマンスに影響する可能性のある大きな違いがあるかを判断しやすくなる。確認すべき事項としては、次のようなものがある。
  - テストに使用された活動はどのような方法で生成されたか。
  - どのような種類の悪意ある活動がテストに含まれていたか。IDPS によって監視されたイベントのうち、悪意ある活動の割合はどの程度であったか。最大の負荷をかけた条件下で、悪意あるイベントのうちどの程度の割合が IDPS により検知されたか。
  - ネットワークトラフィックについて、どのようなプロトコルがおよそどのような比率で使用されたか。ホストベースの活動について、どのようなアプリケーションが実行され、その他のイベント発生源として何が使用されたか。
  - テストに使用された活動には、実稼働環境における実際の条件がどの程度正確に反映されているか。
- IDPS の設定内容はどのようであったか。デフォルト設定が使用されたか。そうでない場合、どの検知機能、ログ記録機能、その他の機能がデフォルトと異なる状態に有効化／無効化されたか。
- アプライアンス形態以外の構成要素について、どのようなハードウェア、OS、アプリケーションまたはサービスが使用されたか。
- テストを実施した主体はだれか。
- テストはいつ実施されたか。

検討対象の各 IDPS が備えているパフォーマンス機能についても考慮すべきである。パフォーマンス機能について確認すべき事項としては、たとえば次のようなものがある。

- 何らかのパフォーマンスチューニング機能（手動設定または自動実装）があるか。たとえば、活動が大量に発生して IDPS が飽和しそうになった場合、検知機能を変更して、すべてのトラフィックに対する解析処理の範囲を一時的に狭めたり、低リスクのトラフィックの解析処理を停止したりすることは可能か。
- 状態の追跡機能（ネットワーク接続のステートフルプロトコル解析など）を備えた製品について、同時に何件の活動（接続など）に関する状態を並行して追跡することができるか。平常時および最大負荷時において、状態情報が保持される期間はどの程度か。
- インラインのネットワークベースの IDPS センサーなど、実際のイベントを処理する製品（イベントのコピーを扱う製品でないもの）について、処理によってどの程度の遅延が発生するか。たとえば、ネットワークベースの IDPS センサーがパケットを受信してから、それを宛先に向けて再送出するまでに、50 マイクロ秒の遅延が発生する可能性がある。ホストベースの IDPS においても、同様に短時間ながらシステムコールの実行に遅延が生じる可能性がある。高負荷時には IDPS 製品にきわめ

て大きな遅延が発生することがあるため、平常時と負荷が極端に大きい場合の両方における遅延を考慮することが重要である。

- 受動型のネットワークベースの IDPS センサーや、ルータから供給されるネットワークフローのログを解析する NBA ソフトウェアなど、イベントのコピーを処理する製品について、イベントが発生してから、IDPS がそれを検知・報告するまでにどの程度の時間がかかるか。

9.4 管理の要件

各 IDPS 製品の管理機能を評価することは非常に重要である。なぜなら、管理が困難な製品や必要な管理機能を備えていない製品は、当初想定していたほどには、有効に使用されない可能性が高いからである。この項では、IDPS の管理機能に関する検討事項を、次の 3 つに分けて説明する。

- 設計および導入
- 運用および保守
- トレーニング、文書化、技術サポート

評価作業における IDPS 管理機能データの収集については、9.6 項にガイダンスを示す。

9.4.1 設計および導入

IDPS の設計および導入に関するほとんどの側面には、IDPS テクノロジーの種類ごとに固有の性質がある。設計および導入に関して考慮すべき事項はセクション 4～7 に示したが、それらに加え、信頼性、相互運用性、スケーラビリティ、セキュリティに関する一般的な基準も考慮すべきである。

9.4.1.1 信頼性

採用する IDPS 製品は、組織の持つ要件を満たすことにおいて十分な信頼性を備えていなければならない。信頼性について確認すべき事項としては、たとえば次のようなものがある。

- アプライアンスに対し、どのようなハードウェア冗長性が提供されているか（標準装備または別途）。たとえば、電源、ネットワークインタフェースカード、ストレージ装置（ハードディスク、フラッシュ ROM）、CPU などが二重化されているか。
- 特にエージェントやセンサーについて、どのようなソフトウェア冗長性機能が製品に組み込まれているか。たとえば、エージェントやセンサーが停止した時に、エージェントやセンサー自身や補助サービスを自動的に再起動する機能があるか。
- 複数の管理サーバを使用し、1 基の管理サーバが故障しても、センサーまたはエージェントがフェイルオーバーによって自動的に別の管理サーバに切り替わることはできるか。フェイルオーバープロセスによって、運用にどの程度の支障が生じるか。
- 同一の活動を監視する複数のセンサーを配備し、1 基のセンサーが停止した場合に別のセンサーにその担当機能を引き継がせることはできるか。フェイルオーバープロセスによって、運用にどの程度の支障が生じるか（状態追跡情報の引き継ぎができない、しきい値を超えたイベントのカウント数の引き継ぎができないなど）。

■ センサーが停止した場合、その設定内容を別のセンサーへ容易に転送することができるか（たとえば、センサーCD と設定情報フロッピーを転送して、転送先のセンサーを再起動するなど）。

9.4.1.2 相互運用性

採用する IDPS 製品は、所望のシステムとの間で相互運用を効果的に行うことができなければならない。IDPS との相互運用が必要なシステムとしては、次のようなものが考えられる。

■ データ供給ソース：他の IDPS 製品、ログファイル、脆弱性スキャン結果など

■ ログ解析／管理ソフトウェア：syslog その他のログサーバ、SIEM ソフトウェア、ネットワーク管理ソフトウェアなど

■ 防止措置によって設定変更の対象となるシステム：ファイアウォール、ルータなど

9.4.1.3 スケーラビリティ

IDPS 製品を評価する際は、組織の現時点でのニーズだけでなく将来的に予想されるニーズも考慮し、十分なスケーラビリティを備えた製品を採用できるようにすべきである。スケーラビリティについて検討すべき事項としては、たとえば次のようなものがある。

■ 単一の論理的実装の一部として考えることができる、センサーまたはエージェント、管理サーバ、コンソール、その他の IDPS 構成要素の数。

■ 単一の管理サーバがサポートすることができるセンサー／エージェントの数。

■ アプライアンスベースの IDPS 構成要素について、利用できるアプライアンスの範囲（能力が異なるさまざまなアプライアンス装置が提供されているかなど）と、アプライアンスを拡張するための能力（メモリ、NIC、ストレージ装置の追加など）。

■ 1 つのネットワークまたはシステムに対する監視機能を複数のセンサーまたはエージェントで共有できるかどうか。これには、負荷分散装置を別途使用することなく負荷を分散できるかどうかを含む。

■ ネットワークベースの IDPS、無線 IDPS または NBA センサーが同時にいくつのネットワークを監視できるか。ホストベースのエージェントが同時にいくつのネットワークインタフェースを監視できるか。

■ IDPS のストレージ機能をどのように拡張または強化することができるか（古いデータの自動アーカイブ、外部ストレージ装置の使用など）。

■ 個々の IDPS 構成要素がどのようなレベルの活動（ネットワークトラフィック、システムコール、ログ項目など）をサポートすることができるか。

■ IDPS ソリューションに、複数のセンサーまたはエージェント、管理サーバ、その他の構成要素に対する管理および監視機能をどの程度うまく統合することができるか。

■ 個々のスケーラビリティオプションのコストおよびそれに必要なリソース。

9.4.1.4 セキュリティ

IDPS 製品の評価にあたっては、IDPS ソリューション自体のセキュリティ要件も考慮しなければならない。評価者は、NIST SP 800-53『*Recommended Security Controls for Federal Information Systems*（連邦政府情報システムにおける推奨セキュリティ管理策）』に記載されているセキュリティ管理策を参考にして、組織の IDPS に関するセキュリティ基準にどのような管理策を盛り込むべきであるかを検討すべきである。セキュリティに関しては、たとえば次のような検討事項がある。

- 保存されているデータ（ログを含む）および全ての IDPS 構成要素間の通信をどのように保護するか。たとえば、データの機密性および完全性が要求される場合に、これをサポートするために、代替データチャネルまたは FIPS 承認済みの暗号化アルゴリズムおよびディジタル署名アルゴリズムを使用するなど。
- IDPS の使用および管理のために、どのような認証、アクセス制御、監査機能を実行するか。
- IDPS への攻撃（目くらまし、DoS 攻撃など）に対して、IDPS がどの程度の耐性を備えているか。

9.4.2 運用および保守

この基準は、IDPS を継続的に管理するためのユーザおよび管理者用インタフェースの要件に関するものである。これには、日常的な監視、解析、報告活動、IDPS の保守管理、更新の適用に関する作業の容易さを含む。これらの各領域についての考えられる具体的な基準を以下に示す。また、各製品の使用と保守にどの程度の技術上およびセキュリティ上の専門的知識が必要とされるかを判断するために、評価者はベンダー、アナリスト、その他信頼のおける相手に意見を求めるべきである。製品を使用するユーザや管理者にどのような技能が期待されているかについて評価者は、ベンダーに確認する必要がある。

9.4.2.1 日常的な使用

セキュリティイベントの監視、着目したイベントの解析、報告書の生成といった日常的な作業において、どのように IDPS ソリューションを使用する必要があるかを組織は検討すべきである。これら 3 つの活動はしばしば、相互に関連しているため、多くの場合は一度に評価するのが最も容易である。日常の IDPS 使用について確認すべき事項としては、たとえば次のようなものがある。

- イベントや警報がユーザに対してどのように表示されるか。解析を支援する機能としてはどのようなものがあるか（ドリルダウン機能、サポート 情報へのリンク、複数センサーまたはエージェント間のイベント相関、警報の重大度／優先度を示す色分け表示など）。ユーザが視点や絞り込みをカスタマイズして、イベントや警報の表示を変更する機能にはどのようなものがあるか。
- IDPS の状態に関する情報はユーザおよび管理者に対してどのように表示されるか（センサーが停止した場合の通知方法など）。
- 深刻なセキュリティイベントや IDPS の障害と運用に関するその他の問題の両方についての情報が、ユーザおよび管理者に対してどのように通知されるか。
- イベントに関して、どの程度詳細な補足情報が記録されるか（たとえば、発生したイベントの内容を分析担当者が判断するために十分な情報が記録されるか）。

- 日常的に使用する機能に関して、インタフェース／プログラムがいくつ必要か（たとえば、IDPS ユーザにとって必要なすべての機能が単一の GUI によって提供されるか）。
- 同時にいくつのインタフェースを並行してサポートできるか。
- デフォルトでどのような報告書式が用意されているか（テキスト、CSV、HTML、XML、PDF、Microsoft Word、Microsoft Excel など）。IDPS データ、ログ、報告を保管しておくためにどのようなデータ保存形式がサポートされているか。
- 報告書のカスタマイズに関してはどのような機能があるか（既存の報告書の変更、新しい報告書の作成の両方について）。
- 報告書の自動生成機能があるか（所定のスケジュールで生成、特定イベントの発生時に生成など）。報告書の配布に関してはどのような機能があるか（管理者への電子メール送付など）。配布される報告書はどのように保護されるか（ファイル暗号化など）。
- ワークフロー追跡機能があるか（インシデントの追跡など）。

9.4.2.2 保守

IDPS 製品を評価する際には、IDPS ソリューションおよびその構成要素の保守を組織としてどのような方法で行うべきかをまず検討し、保守の要件に基づいて評価作業を行うべきである。保守について確認すべき事項としては、次のようなものがある。

- センサーまたはエージェントを個別に管理する方法と管理サーバ経由で行う方法の両方が可能か。また、そのような作業のアクセスはログに記録されるか。
- どのようなローカルおよびリモートの保守メカニズムを使用できるか（ローカル環境にインストールされた GUI、Web ベースのコンソール、コマンドラインインタフェース(CLI)、サードパーティ製ツールなど）。それぞれのメカニズムの間に機能的な差異がある場合、それはどのような違いか。
- それぞれの保守メカニズムを使用してどの構成要素の保守作業をローカルおよびリモートで実行できるか。
- それぞれの保守メカニズムについて、どのようなセキュリティ保護が提供されるか（ネットワークトラフィックの強力な暗号化など）。
- 構成要素の設定内容はどのような方法でバックアップおよび復元することができるか。また、設定内容をどのような方法で代替構成要素に転送することができるか（ハードウェア故障のためセンサーアプライアンスを交換する場合など）。
- 構成要素の状態情報（ディスク領域の不足、CPU の高負荷など）、運用上の障害、および保守作業が必要となる可能性のあるその他のイベントをログに記録する処理がどの程度確実に実行されるか。
- 十分に堅牢なログ管理ツールを提供するか。しない場合、管理者がそれを補う手段があるか（スクリプトを作成する、サードパーティ製ツールを調達するなど）。

9.4.2.3 更新

評価対象とする各 IDPS 製品のベンダーによる更新の提供状況についても慎重に検討すべきである。検討すべき事項としては、次のようなものがある。

- どの程度の頻度で、それぞれの構成要素（センサー、管理サーバ、コンソールなど）に対して、定期的な大規模および小規模な更新が提供されるか。
- 新規の重大な脅威の出現に対応して検知機能の更新が提供される頻度はどの程度か。また、新たな脅威が特定されてからそれに対応した更新が提供されるまでの期間は通常どの程度か。
- どのような種類の更新を適用する際に、IDPS 構成要素の再起動や再スタートがしばしば、または時折必要となるか。
- それぞれの種類の更新をベンダーからどのような方法で受け取るか（たとえば、センサーの更新は CD で配布され、シグネチャの更新はコンソールを使用してダウンロードするかベンダーの技術サポート Web サイトにアクセスしてダウンロードするなど）。
- 更新の真正性および完全性はどのような方法で確認できるか（暗号チェックサムなど）。
- 更新を IDPS 構成要素（センサー、コンソールなど）にどのように配布するか（自動処理、手動インストールなど）。
- 更新のインストール作業が IDPS の既存の設定内容やカスタマイズ内容にどのように影響を及ぼすか。

9.4.3 トレーニング、文書化、技術サポート

組織は、IDPS の管理者およびユーザが IDPS の機能や特性について学ぶために利用可能なリソースおよび、問題発生時に支援を得るために利用可能なリソースを検討すべきである。トレーニング、文書化、技術サポートの各リソースは、管理者およびユーザの両方のニーズだけではなく、さまざまな経験レベルのニーズを考慮したものであることが望まれる。

- **トレーニング.** ほとんどの IDPS ベンダーは、自社の製品に関するトレーニングクラスを開講している。ベンダーによって、製品ごとに 1 つのクラスのみ用意されている場合と、ユーザおよび管理者向けに別々のクラスが用意されている場合がある。また、特定の IDPS 構成要素（コンソール、管理サーバなど）や特定の作業（コードのカスタマイズ、報告書の作成など）について別のクラスが用意されていることもある。一部のベンダーは、IDPS の原理についてユーザの理解を深めるための IDPS 概論クラスも開講している。IDPS 概論および具体的ないくつかの IDPS 製品については、サードパーティ業者の開講しているクラスも利用できる。こうした選択肢の中から、組織のニーズに合ったトレーニング内容、提供形態（講師による指導、オンライン、コンピュータベーストレーニング[CBT]など）、開催場所（IDPS ベンダー本社、地域拠点、顧客先オンサイトなど）はどのようなものであるかを検討すべきである。講師による指導を受けるクラスの場合は、さらに、実験環境での実習あるいは他の実践演習など、ユーザが実際の IDPS 機器を使用することができる内容が含まれているかどうかについても確認する必要がある。
- **文書.** 通常、IDPS 製品には印刷物または電子データの形式で文書が付属する。たとえば、インストールガイド、ユーザガイド、管理者ガイド、シグネチャ／ポリシー開発ガイドなどがある。電子データ

形式のガイドは、全文検索が可能であることが多い。一部の製品は、コンソール上で利用できる状況検知式ヘルプを備えており、ユーザは、特定のコンソール機能やセキュリティイベントの種類に応じた文書を容易に参照することができる。ガイド類が印刷物でしか提供されない場合は、複製の可否と、複製不可であれば追加コピーを入手する方法について確認する必要がある。

- **技術サポート.** ほとんどの IDPS ベンダーは、複数の技術サポート契約形態を用意している。たとえば、ある契約では「通常業務時間内のみ電話、電子メール、Web によるサポート、応答は 1 時間以内」などといった内容が、別の契約では「上級サポートスタッフに 24 時間連絡可能、応答は 15 分以内、年に一度のオンサイト出張およびコンサルティングサービス込み」といった内容が考えられる。契約にどのような活動内容が含まれ、何が含まれないかを慎重に判断すべきである。たとえば、チューニングおよびカスタマイズ（シグネチャの作成、報告書のカスタマイズなど）などは、技術サポート契約に含まれない可能性がある。通常、ベンダーのサポート契約には複数の選択肢があり、顧客がそれぞれにとって費用対効果のよい契約を選択できるようになっている。製品によっては、ユーザグループ、メーリングリスト、フォーラム、その他の手段による無償の技術サポートを利用することもできる。

9.5 ライフサイクルコスト

コストの面では、評価対象の各ソリューションに関する見込みライフサイクルコストと、IDPS ソリューションのために組織として用意することができる予算とを比較すべきである。ただし、IDPS ソリューションのコストには環境特有のさまざまな要因が影響を与え、また、IDPS によってもたらされるコスト面のメリットを把握することが通常は困難であるため、ライフサイクルコストの定量化は難しい。以下に示す基準は、もっぱら IDPS ソリューション自体の基本的なコストに関するものであり、IDPS の使用によって実現され得るコスト節減効果を勘案してはいない。

- **初期コスト**：ソリューションを調達および導入するための初期コストには、一般に、次の要素が含まれる。
  - ハードウェア（アプライアンスを含む）、追加ネットワーク設備（管理ネットワーク、ネットワークタップ、IDS ロードバランサなど）、非アプライアンス構成要素用のホスト（コンソール用など）
  - IDPS 構成要素および補助ソフトウェア（報告ツール、データベースソフトウェアなど）のソフトウェア費用およびライセンス費用
  - インストールおよび初期設定作業コスト（外部の支援、内部の人件費を含む）
  - カスタマイズコスト（プログラマによるカスタムスクリプトや報告書式の開発など）
  - トレーニングコスト（ハードウェアおよびソフトウェアの初期購入費用に必要なトレーニングが含まれていない場合）
- **保守コスト**：IDPS ソリューションに対して見込まれる保守コストには、通常、次の要素が含まれる。
  - 人件費：IDPS の管理および解析作業を行うスタッフのコストを含む。
  - ソフトウェアライセンス費用、サブスクリプション費用、または保守契約：IDPS のソフトウェア更新およびシグネチャ更新の提供を受けるための費用。通常、年単位で発生する。

– 技術サポート費用：多くの組織は、IDPS 製品に対する技術サポート契約を購入する。契約は、年単位で更新されるのが一般的である。組織によっては、年間契約ではなく技術サポートへの問い合わせ 1 件ごとに料金を支払う場合もある。

– トレーニングコスト：IDPS 製品の新バージョンを導入する準備や、新しい IDPS ユーザおよび管理者のために、定期的にトレーニングを実施する必要が生じる可能性がある。場合によっては、IDPS 製品のうち、組織にとって最も重要な構成要素に主眼を置き、組織固有の環境やニーズに関する特定の側面を反映するよう、トレーニングクラスの内容をカスタマイズすることも必要となる。

– カスタマイズコスト：IDPS 製品を使用している間に、ユーザや管理者が、製品のさらなるカスタマイズを必要性とする可能性がある。たとえば、プログラマが報告書式の追加や、既存の報告書式の変更を行うことができるようにしたり、プログラマまたは管理者が独自のアナライザやシグネチャを作成したりすることができるようにする。

– 技術サポート契約に含まれないプロフェッショナルサービスまたは技術サポート：たとえば、IDPS 導入の設計、製品のインストール作業、センサーまたはエージェントのチューニング、報告書の作成およびカスタマイズ、インシデント対応作業支援などである。組織が自らこのようなサービスを提供することができる場合もあれば、IDPS ベンダーまたはサードパーティからサービスを購入する場合もある。

9.6 製品の評価

要件を収集して評価基準を決定したら、評価対象製品に関する情報源を探す必要がある。製品に関する一般的な情報源としては、次のようなものがある。

- 検査機関または、選択したいくつかの IDPS 製品の実環境におけるテスト
- 組織内の個人、または、別組織に属する信頼のおける個人が IDPS に関してこれまでに実地で経験したこと
- ベンダーから提供される情報（製品のマニュアル、データシート、ホワイトペーパー、製品デモ、ベンダーの社員との話し合いなど）
- 第三者による製品レビュー（個別製品のレビュー、複数製品の比較など）

9.6.1項では、評価作業の一環として IDPS 製品のテストを実施することに関する課題について述べる。9.6.2項では、評価実施時に上記のような情報源を利用する場合の推奨事項を示す。

9.6.1 IDPSテストの実施に関する課題

組織自身がIDPS製品の綿密かつ実際的なテストを行えば、理想的には、個々の製品がどの程度ニーズに合っているかを正確に示す総合的なデータが得られるはずである。しかし、IDPSのテストを適切に行うことが困難であり、しかもテストには多大なリソースを要するため、現実的には、データが得られない場合が多い。そのような問題が生じる大きな原因のいくつかを次に示す[55]。

[55] IDPS のテスト実施の課題の詳細については、NIST Interagency Report（IR：省庁間報告書）7007『*An Overview of Issues in Testing Intrusion Detection Systems*』（http://csrc.nist.gov/publications/nistir/nistir-7007.pdf）を参照のこと。主としてネット

- **テストの方法論**：IDPS のテストには標準的な方法論が存在しない。また、商業的に行われる評価作業において用いられる方法論のほとんどは、詳細な内容が明らかにされていない。IDPS のテストを実施する組織は、独自に方法論を確立するか、既存の方法論に関する情報を収集して最もニーズに適すると思われるものを選び、それに基づいてテストプロセスを設計および実装する必要がある。また、IDPS テクノロジーの種類ごとに、異なる方法論（テスト環境およびテストスイートを含む）が必要である。

- **複数の環境**：IDPS のテストは、現実の環境と、実験用環境の両方において実施すべきである。現実の環境でのテストは、実稼働環境において製品がどの程度有効に機能するかを知るのに役立つ。一方、製品が備える検知および防止の能力をより正確に評価するには、実験用環境でのテストが適している。現実の環境で発生する活動にはさまざまな種類の悪意ある活動が含まれ、検知した活動が実際に悪意のものであるかどうかが明確でないこともあるため、そのような活動を監視して得られる検知結果は理解しにくいものになる可能性がある。一般に防止機能のテストを現実の環境で行わないのは、害のない活動を中断させる可能性が高いからである。実験用に隔離した環境で現実の環境を模倣することは非常に難しいため、IDPS のテストを実施する場合は、2 つの環境それぞれにおいてテストを行う必要がある。

- **テストツールの入手性**：標準のIDPSテストスイートといえるものは存在しない。テストを行うには、悪意のある活動（製品の検知能力を調べるため）および害のない活動（平常時または高負荷時と同様の条件を作り出すため）の両方をどのような手段で生成するかを考える必要がある。悪意のある活動の内容には、組織のシステムおよびネットワークが最近直面している脅威の構成内容を正確に反映させなければならないため、それらの脅威を特定し、そのテスト手段を獲得するにはかなりの時間を要する。また、一般に個々の検知手法の実効性を正しく評価するには、それぞれの手法ごとに異なる種類のテストが必要であるため、当該IDPSで使用されているすべての検知手法を考慮する必要がある[56]。多くの場合、妥当な内容のテストスイートを構築するには、慎重に選択されたツール群と、独自に作成した攻撃スクリプトの組み合わせが必要である。個々のツールおよびスクリプトのレビューとテストを行い、テストが適切に実施されることを確認しなければならない。

- **実験用環境のリソース**：実験用環境で IDPS をテストするには、一般に、環境の構築に大量のリソースを投じる必要がある。攻撃側および攻撃を受ける側のシステムのセットアップと設定を行う必要がある。攻撃を受ける側のシステムでは、攻撃の標的となる OS、サービス、アプリケーションを稼働させる必要がある。IDPS で使用される手法に応じて、攻撃を受ける側のシステムに、攻撃者が悪用するすべての脆弱性を用意する必要がある場合がある。IDPS によっては、攻撃が成功すると考えられる場合にしか警報を発しないことがある。また、攻撃の側も、悪用できる脆弱性を検知できない場合には実行を中止することがある。評価者は、IDPS の能力についても注意を払う必要がある。たとえば、IDPS がいくつかの攻撃が同一の攻撃者のシステムから行われたことを検知すると、防止措置を自動的に実行し、以後そのシステムから行われるすべての攻撃を阻止する可能性がある。

- **製品の同等性**：ほとんどの IDPS 製品は、組織の要件に合わせるためにチューニングおよびカスタマイズが必要である。各製品のデフォルト設定は、互いに若干異なるため、テストを実施する際には、チューニングおよびカスタマイズによって、各製品が可能な限り同等になるようにするべきであ

ワークベースの IDPS を扱った文書であるが、テスト実施に関する課題を論じている内容のほとんどは、あらゆる種類の IDPS テクノロジーに当てはまる。

[56] 問題を複雑にするもう一つの要因として、個々の製品が実際にどの手法を採用しているかが明確でないことが多く、必要なテストの種類を知ることが難しいことが挙げられる。

る。たとえば、各種のしきい値（一定期間内に許容するログイン試行失敗の回数など）をいずれの製品でも同じ値に設定し、各種検知機能の有効化／無効化についても、すべての IDPS で統一すべきである。しかし、多くの場合、これらのことを実際に行うのは非常に困難である。たとえば、シグネチャベースの検知を行う製品は、使用される個々の悪用手段に基づいて設定がされる傾向があるのに対し、ステートフルプロトコル解析を行う製品は、悪用される個々の脆弱性に基づいて設定されることが多い。どのようにすれば異なる IDPS 製品が同等の設定になるかを判断するために、評価者は、悪用手段と脆弱性の対応関係を把握する必要がある。

9.6.2 IDPS評価作業の実施に関する推奨事項

IDPS 製品に対して綿密かつ実際的なテストを実施するためには、多くの課題があり、現実的でない場合が多い。とはいえ、IDPS テストをいくらかでも実施することは、セキュリティ機能、パフォーマンス、運用および保守に関する組織の要件を対象製品がどの程度満たしているかを評価するためには、非常に有用であることが多い。また、製品の持つ能力と、組織の環境における保守および監視の作業に必要な労力について、現実的な見通しを立てるための参考にもなる。したがって、各組織において IDPS 製品を評価する際には、限定的な製品テストの他、ベンダーから提供される情報、第三者による製品レビュー、個人による IDPS に関するこれまでの経験など、いくつかの情報源を組み合わせて利用するとよい。たとえば、テスト以外の情報に基づいて採用候補製品の数をいくつかに絞り込み、それらの製品を対象として限定的なテストを実施することなどが考えられる。時間とリソースの制約により製品テストを省略する必要がある場合、書類のみで製品を評価せざるを得ないこともあるが、たとえ少しでもテストを取り入れるほうが、概して評価作業がよい結果につながりやすいといえる。

外部から提供されるデータを参照する際には、その信頼性の程度を考慮しなければならない。能力の上限値や検知の正確さなどといったデータは、導出方法の詳しい説明なしに示されていることがしばしばある。こうしたデータのまとめ方について標準的な方法は確立されておらず、異なる情報源から得られるデータを比較する際には、それらのデータが根本的に異なる方法によって計測されている可能性があるため、注意が必要である。

実地のIDPSテストを行う場合は、有効な結果を得られる可能性が最も高いテスト手法を採用すべきである。また、テスト実施者は、テストが組織の業務の妨げにならないよう注意することも必要である。以降の各項では、テスト実施に関するガイダンスをIDPS製品の種類ごとに示す。テストの完了後は、IDPSベンダーから借り受けたハードウェアに搭載されているすべての書き込み可能メディアを適切な方法でサニタイズし、組織に関するデータの消去を確認すべきである[57]。

9.6.2.1 ネットワークベース

現実の環境における IDPS テストを実施することにより、ネットワークベースの IDPS のセキュリティ機能（特に、検知の正確さとチューニング）、組織のネットワークトラフィックに対するパフォーマンス、IDPS の運用および保守に関する貴重な見識を得ることができる。ただし、IDPS が業務に悪影響（遅延の増大など）を及ぼしたり、IDPS の脆弱性が攻撃者に悪用されたりすることのないよう、テスト時は IDPS と実稼働環境の間にある程度の分離を保っておくのが賢明である。IDS ロードバランサを使用すると、ネットワークトラフィックの同一内容のコピーを同時に複数のセンサーに送ることができるので、センサーを隔離して実稼働環境に破壊的な影響が及ぶのを防ぐと同時に（ロードバランサは一方向しかトラフィ

[57] メディアのサニタイズ処理の詳細については、NIST SP 800-88『*Guidelines for Media Sanitization*(メディアのサニタイズに関するガイドライン)』（http://csrc.nist.gov/publications/nistpubs/）を参照のこと。

ックを通さない）、複数製品を並べてそれらの挙動を確認することができる。ネットワークアーキテクチャによっては、インラインセンサーのネットワークインタフェースが存在するであろう場所のトラフィックを複製し、そのトラフィックをインラインセンサーのインタフェースに送ることにより、インラインに設置されているセンサーをテストできる可能性がある。そうでない場合も、ほとんどのインラインセンサーは受動モードで設置し、受動モードでテストすることが可能である。実稼働環境のトラフィックに対するインラインモードでのテストには、センサーのパフォーマンスを把握することができるというメリットがある。

ネットワークベースの IDPS のテストを実験用環境で行う最大のメリットは、次の事項を評価しやすいことである。

- **製品の提供する防止機能**：テストシステム（攻撃を実行するシステムおよびその標的）を用意し、攻撃を生成して、各 IDPS が実行する防止措置の実効性を監視する。
- **導入したインラインセンサーのパフォーマンス**：現実の環境でのテストが実施できない場合は、ネットワークトラフィック生成ツールを使用するか、事前に記録したトラフィックを再生することにより、センサーを通過する活動を生成する。
- **設計および導入に関する特性**：製品の信頼性をテストする方法として、導入中の複数のセンサーや管理サーバをフェイルオーバーの状態に設定し、それらに処理させるトラフィックを生成しながら、意図的に 1 つの構成要素を停止させることにより、結果的に生じる製品の挙動を監視するというものがある。相互運用性をテストするには、IDPS との相互運用が必要な製品を模したテストシステムを設定し、両製品を協働して動作させるような活動を生成する。IDPS 自体のセキュリティについても、脆弱性スキャン、ペネトレーションテスト、その他の方法を用いてテストすることができる。

9.6.2.2 無線

無線 IDPS のテストに使用する手法は、主として、テスト対象となる無線 IDPS センサーの形態に基づいて選択すべきである。

- **移動センサー、固定センサー、APにバンドルされたセンサー**[58]：セキュリティ機能、パフォーマンス、および運用・保守の一部の側面に関するテストは、通常は実稼働環境でセンサーを使用することにより実行できるが、その場合は防止機能を無効にしておくべきである。防止機能の評価は、テスト用以外の全ての無線LANの有効範囲の外にある隔離したテスト環境において実行することができる。テスト環境には、テスト用アクセスポイントと、それらを使用するテスト用無線クライアントを配置する。無線ネットワーク通信を生成するために、無線クライアントのアクセス先となるテストシステムのセットアップが必要となる場合もある。攻撃は 1 つまたは複数の無線クライアントから行い、必要に応じて不正アクセスポイントをテスト環境内に配備してもよい。センサーをIDPSインフラストラクチャに統合することを予定している場合、実稼働中のインフラストラクチャを危険にさらすことなくパフォーマンス、運用および保守、ならびに設計および導入上の特性を評価するために、統合に関わる全てのテストは、テスト環境内で実行すべきである（たとえば、IDPSセンサーに脆弱性が存在すると、センサー有効の範囲内にいる攻撃者によって悪用される可能性がある）。

[58] AP にバンドルされたセンサーについては、これらのテストに関する説明は、テストに実稼働環境では使用しない AP を使用することを前提としている。実稼働中の AP 上にテスト目的でセンサーソフトウェアを導入することは、業務の運用を妨げる可能性があるため推奨しない。

- **無線スイッチにバンドルされたセンサー**：一般に、このテストはセンサーソフトウェアを搭載したテストスイッチをテスト環境内に用意して実行する。これは、他の形態の無線センサーの場合（上記）と同様である。また、実行すべきテストの種類も上記と同様である。

9.6.2.3 NBA

NBA 製品でネットワークトラフィックを直接監視する場合は、ネットワークベースの IDPS のテストに関するガイダンスに基づき、現実の環境および実験用環境で当該の監視機能をテストすべきである。他の装置から供給されるネットワークフローログを NBA 製品で監視する場合、現実の環境におけるテストを行うには、独立のネットワークを用意し、監視対象となる装置のログをこのネットワークを経由して NBA センサーに転送するのが望ましい。このようにすれば NBA ソリューションが保護され、ソリューションの使用する帯域幅を容易に計測することができる。独立のネットワークではなく実稼働中のネットワークを使用する場合は、大量のログでネットワークを飽和させることがないよう格別の注意を払う必要がある（特に、複数の NBA 製品を同時にテストする場合）。また、実稼働環境から生成したログのコピーを実験用環境内の NBA 製品に供給することによりテストを行う方法もある。テストを実験用環境で行うことは、ネットワークベースの IDPS の場合と同様に、防止機能、インラインセンサーのパフォーマンス、製品の設計および導入の特性に関する評価が容易になるというメリットがある。

9.6.2.4 ホストベース

ホストベースの IDPS を現実の環境でテストすることは、通常、他の種類の IDPS の場合よりも困難である。エージェントは、監視対象のホストに変更を加え、ホストのパフォーマンスや機能に悪影響を与える可能性がある（IDPS シムが他のアプリケーションの妨げとなるため）。アプライアンスベースの IDPS も、実稼働システムの手前の位置にインラインで設置することになるためリスクがある。ホストベースの IDPS のテストに使用する手法は、主として、保護対象となるホストの役割に基づいて選択すべきである。

- **サーバ（サーバ上の単一アプリケーションサービスが対象の場合も含む）**：テスト環境でのみテストを行う。これには、たとえば実稼働サーバを模倣するテストサーバ（実物の予備機でもよい）を用意することが考えられる。このサーバに対する通常の活動（無害の活動と悪意のある活動の両方）をテストシステムで生成（たとえば、スクリプトまたはツールで HTTP 要求を生成）し、それをホストベースの IDPS で監視する。テスト環境であれば、実稼働システムを危険にさらすことなくテストサーバに攻撃を仕掛け、防止措置が実行される様子を監視することができる。また、ホストベースの IDPS がサーバのパフォーマンスに及ぼす影響を測定したり、ホストベースの IDPS に対する妨害を試みて信頼性やセキュリティを評価したりすることもできる。

- **クライアントホスト（デスクトップまたはノート PC）**：ホストベースの IDPS によってパフォーマンスや機能性に深刻な問題が発生する可能性を調べるために、初期のテストはテスト環境内で実行すべきである。IDPS の信頼性およびセキュリティに対する評価もテスト環境内で行うことができる。IDPS が異常停止しても、実稼働環境に与えるリスクは非常に小さいと考えられるため、エージェントのセキュリティ機能、防止措置、その他の特性に関するテストは、テスト環境および実稼働環境の両方で実施してよい。ホストに対する攻撃はテスト環境内のみで行うべきであるが、害のない活動に対するエージェントの挙動については、現実の環境でテストするのが最も簡単である。たとえば、数人のテスト担当者が自発的に自分の実稼働デスクトップに IDPS エージェントをインストールして 1～2 週間程度使用し、エージェントの挙動やエージェントが原因で発生した問題などを文書化するといった方法が考えられる。このような方法により、本当の意味で現実の環境を使用したエー

ジェントのテストを行うことができる。ユーザとの対話操作を必要とするようなエージェント（活動の許可あるいは拒否に関する問い合わせへの対応など）については、テスト環境または実稼働環境においてエンドユーザテストも実施することが望ましい。

ホストベースの IDPS のテストにおいては、最もよく使用される OS および重要な OS と、保護の必要があるアプリケーションに対しては必ずテストを実行すべきである。OS やアプリケーションのアーキテクチャはそれぞれに異なるため、たとえ同じ製品であっても、異なるプラットフォーム上ではまったく違った挙動を示す可能性がある。

9.7 まとめ

IDPS 製品の評価にあたっては、まず、製品が満たすべき全般的な要件をあらかじめ定義しておくべきである。IDPS 製品が提供する機能およびそれらが使用する手法は、製品によって大きく異なるため、ある組織の要件に最もよく合致する製品が別の組織の要件を満たすのに適しているとは限らない。対象組織のシステムやネットワークと互換性があり、かつ、システム・ネットワーク上の注目すべきイベントを監視することができる IDPS 製品を選定するために、評価者は、組織のシステムおよびネットワーク環境が持つ特性について、近い将来の変更予定も含めて理解しておく必要がある。この知識は IDPS ソリューションを設計するためにも必要である。既存のシステム環境およびネットワーク環境を十分に把握したあと、評価者は、IDPS を使用して達成したいと考える目標および目的を明文化すべきである。また、既存のセキュリティポリシーおよびその他の IT ポリシーの内容についても、製品を選定する前に再確認すべきである。これは、ポリシーが IDPS 製品に必要な機能の多くを規定する一種の仕様書として機能するためである。それに加え、対象組織が別の組織による監督または検査の対象となるかどうかについても確認し、該当する場合には、監督機関が IDPS あるいはその他特定のシステムセキュリティリソースの使用を義務付けているかどうかを確認する必要がある。さらに、使用可能なリソースの制約についても考慮しなければならない。

一般要件に加え、評価者は、次のような各種の目的に特化した要件セットも定義する必要がある。

- セキュリティ機能：情報収集、ログの記録、検知、防止などについて
- パフォーマンス：最大処理能力およびパフォーマンスに関する特徴などについて
- 管理：設計と導入、運用と保守、トレーニング、文書化、技術サポートなど
- ライフサイクルコスト：初期コストおよび維持コスト

実際の組織においては、これらの基準を参考にしつつ、組織の環境、ポリシー、および既存のセキュリティとネットワークのインフラストラクチャを考慮に入れて、実際の組織に適した独自の基準セットを策定することができる。要件を収集して評価基準を決定したら、評価対象製品に関する情報源を探す必要がある。製品に関する一般的な情報源としては、検査機関または実際的な環境での製品テスト、ベンダーから提供される情報、第三者による製品レビュー、および、組織内の個人や別組織に属する信頼のおける個人による IDPS に関するこれまでの経験などがある。

綿密かつ実際的な IDPS テストは、大きな困難を伴い、満足のいく結果を得ることも難しいため、実施は現実的でない場合が多い。限定的な IDPS テストの結果を参考にするだけでも、ほとんどの組織にとっては、日常の使い勝手、相互運用性、セキュリティ要件を評価するために役立つ。IDPS 製品を評価するにあたっては、複数の情報源からデータを得ることを検討すべきである。外部から提供されるデー

タは、どのようにして生成されたかについての説明がされていないことが多いため、データを参照する際には、その信頼性を考慮しなければならない。実地の IDPS テストを行う場合は、有効な結果を得られる可能性が最も高いテスト手法を採用し、組織の業務の妨げになる可能性の高いテスト手法は避けるべきである。

付録 A—用語集

『*侵入検知および侵入防止システム（IDPS）に関するガイド*』で使用している用語について、その一部の定義を以下に示す。

エージェント（Agent）：ホストベースの侵入検知および侵入防止プログラム。活動の監視および解析を行い、場合により防止措置も実行する。

警報（Alert）：観測した重要なイベントについての通知。

アノマリベースの検知（Anomaly-Based Detection）：観測したイベントと、正常とみなされる活動内容の定義とを比較し、重大な逸脱を特定するプロセス。

ウイルス対策ソフトウェア（Antivirus Software）：コンピュータやネットワークを監視し、主要な種類のマルウェアをすべて識別して、マルウェアインシデントの防止や封じ込めを行うプログラム。

アプリケーションベースの侵入検知および侵入防止システム（Application-Based Intrusion Detection and Prevention System）：ホストベースの侵入検知および侵入防止システム。特定のアプリケーションサービス（Web サーバプログラム、データベースサーバプログラムなど）だけを監視する。

ブラックリスト（Blacklist）：予め悪意のある活動に関連すると判定されている個別エンティティ（ホスト、アプリケーションなど）の一覧。

目くらまし（Blinding）：「真の」攻撃によって発生する警報を隠蔽するために、同時に、短期間に多数の警報を発生させる可能性が大きいネットワークトラフィックを生成すること。

チャネルスキャン（Channel Scanning）：無線侵入検知および侵入防止システムによる監視対象チャネルを変更すること。

コンソール（Console）：IDPS のユーザおよび管理者に対するインタフェースを提供するプログラム。

データベースサーバ（Database Server）：センサー、エージェント、または管理サーバによって記録されるイベント情報を保存するリポジトリ。

回避（Evasion）：悪意ある活動を、標的に対する効果はそのままに形式やタイミングを変え、その見かけを異なるものにすること。

フォールスネガティブ（False Negative）：侵入検知および侵入防止テクノロジーが、悪意のある活動を、悪意あるものとして特定できないこと。

フォールスポジティブ（False Positive）：侵入検知および侵入防止テクノロジーが、実際には害のない活動を、悪意のある活動と誤って認識すること。

フラッディング（Flooding）：多数のメッセージを短い間隔でホストまたはネットワークに送付すること。この文書では、特に無線アクセスポイントに関わるものとしている。

フロー（Flow）：ホスト間に発生する特定のネットワーク通信セッション。

ホストベースの侵入検知および侵入防止システム（Host-Based Intrusion Detection and Prevention System）：単一のホストの特性と、そのホストの内部で発生するイベントを監視し、疑わしい活動を特定して阻止するプログラム。

インシデント（Incident）：コンピュータのセキュリティポリシー、利用規定、または標準セキュリティプラクティスに対する、違反または差し迫った違反の脅威。

インラインセンサー（Inline Sensor）：監視対象となるネットワークトラフィックが必ず通過するように設置されるセンサー。

侵入検知（Intrusion Detection）：コンピュータシステムまたはネットワークに発生するイベントを監視し、それらを分析することによって、インシデントと考えられる兆候を検知するプロセス。

侵入検知および侵入防止（Intrusion Detection and Prevention）：コンピュータシステムまたはネットワークに発生するイベントを監視し、それらを分析することによって、インシデントと考えられる兆候を検知し、検知したインシデントと考えられるイベントを阻止することを試みるプロセス。「侵入防止」*も参照*。

侵入検知システムロードバランサ（Intrusion Detection System Load Balancer）：ネットワークトラフィックを集約して、侵入検知および侵入防止センサーなどの監視システムに送り込む装置。

侵入検知システム（Intrusion Detection System）：侵入検知プロセスを自動化するソフトウェア。

侵入防止（Intrusion Prevention）：コンピュータシステムまたはネットワークに発生するイベントを監視し、それらを分析することによって、インシデントと考えられる兆候を検知し、検知したインシデントと考えられるイベントを阻止することを試みるプロセス。「侵入検知および侵入防止」*も参照*。

侵入防止システム（Intrusion Prevention System）：侵入検知システムのすべての機能に加え、インシデントと考えられるイベントを阻止することを試みる機能を備えたソフトウェア。「侵入検知および侵入防止システム」とも呼ばれる。

ジャミング（Jamming）：無線ネットワークの周波数帯に対して電磁エネルギーを放射し、その周波数帯をネットワークが使用することができないようにすること。

マルウェア（Malware）：被害者のデータ、アプリケーション、またはオペレーティングシステムの機密性、完全性、または可用性を損なわせる目的で、あるいは被害者を困らせたり混乱させたりする目的で、通常は気づかれないようにシステムに挿入されるプログラム。

管理ネットワーク（Management Network）：セキュリティソフトウェアの管理専用に設計された独立のネットワーク。

管理サーバ（Management Server）：センサーまたはエージェントから送られる情報を受信し、管理する集中化された装置。

ネットワークベースの侵入検知および侵入防止システム（Network-Based Intrusion Detection and Prevention System）：侵入検知および侵入防止システムの一種。特定のネットワークセグメントまたはネットワーク装置のネットワークトラフィックを監視し、ネットワークプロトコルおよびアプリケーションプロトコルの活動を解析して疑わしい活動を特定して阻止する。

ネットワーク挙動解析システム（Network Behavior Analysis System）：侵入検知および侵入防止システムの一種。ネットワークトラフィックを検証し、通常と異なるトラフィックフローを生成する脅威を特定して阻止する。

ネットワークタップ（Network Tap）：センサーと、光ファイバケーブルなど物理ネットワーク媒体そのものとの直接的な接続。

受動的フィンガープリンティング（Passive Fingerprinting）：パケットヘッダを解析して、通常と異なる特定の性質や、特定のオペレーティングシステムまたはアプリケーションに見られる特有の性質の組み合わせを識別すること。

受動型センサー（Passive Sensor）：実際のネットワークトラフィックのコピーを監視するように設置されるセンサー。

プロミスキャスモード（Promiscuous Mode）：ネットワークインタフェースカードの設定の一種。観測した着信パケットを、その意図する宛先に関係なくすべて受け取る設定。

センサー（Sensor）：侵入検知および侵入防止システムの構成要素。ネットワーク活動を監視および解析し、場合により防止措置も実行する。

シム（Shim）：ホストの既存コード層の間に配置され、データを傍受・解析する、ホストベースの侵入検知および侵入防止のコード層。

シグネチャ（Signature）：既知の脅威に対応するパターン。

シグネチャベースの検知（Signature-Based Detection）：観測したイベントとシグネチャとを照合してインシデントの可能性を特定するプロセス。

スパニングポート（Spanning Port）：スイッチを通過するすべてのネットワークトラフィックを観測することができるスイッチポート。

ステートフルプロトコル解析（Stateful Protocol Analysis）：個々のプロトコル状態に関し、無害なプロトコル活動として一般的に受容される内容の定義済みプロファイルと観測したイベントとを比較して逸脱を特定するプロセス。

ステルスモード（Stealth Mode）：侵入検知および侵入防止センサーを、その監視ネットワークインタフェースに IP アドレスを割り当てることなく運用する設定。

しきい値（Threshold）：正常な動作と正常でない動作の境界を指定する値。

三角測量（Triangulation）：無線ネットワークにおいて検知した脅威の物理的な位置を複数の無線センサーで特定する方法。受信する脅威からの信号の強度に基づいて、各センサーから脅威までのおおよその距離を推定し、さらに、各センサーからの推定距離から、脅威の物理的な位置を算出する。

チューニング（Tuning）：侵入検知および侵入防止システムの設定を変更して検知の正確さを向上させる作業。

ホワイトリスト（Whitelist）：無害であることが判明している個別エンティティ（ホスト、アプリケーションなど）の一覧。

無線侵入検知および侵入防止システム（Wireless Intrusion Detection and Prevention System）：侵入検知および侵入防止システムの一種。無線ネットワークのトラフィックを監視し、無線ネットワークプロトコルを解析して、当該プロトコル自体に関わる疑わしい活動を特定し、阻止する。

（本ページは意図的に白紙のままとする）

付録 B—略語

『*侵入検知および侵入防止システム（IDPS）に関するガイド*』で使用している略語について、その一部の定義を以下に示す。

AP Access Point（アクセスポイント）
ARP Address Resolution Protocol（アドレス解決プロトコル）

CAIDA Cooperative Association for Internet Data Analysis（インターネットデータ解析協会）
CIAC Computer Incident Advisory Capability（コンピュータインシデント情報勧告機関）
CLI Command-Line Interface（コマンドラインインタフェース）
CMVP Cryptographic Module Validation Program（暗号化モジュール有効性確認プログラム）
COM Component Object Model（コンポーネントオブジェクトモデル）
CPU Central Processing Unit（中央処理装置）
CSIRT Computer Security Incident Response Team（コンピュータセキュリティインシデント対応チーム）
CSRC Computer Security Resource Center（コンピュータセキュリティリソースセンター）
CSV Comma Separated Values（カンマ区切りデータ形式）
CVE Common Vulnerabilities and Exposures（一般的な脆弱性と暴露性）

DDoS Distributed Denial of Service（分散型サービス妨害）
DHCP Dynamic Host Configuration Protocol（動的ホスト設定プロトコル）
DLL Dynamic Link Library（ダイナミックリンクライブラリ）
DMZ Demilitarized Zone（非武装地帯）
DNS Domain Name System（ドメインネームシステム）
DoS Denial of Service（サービス妨害）
DS Distribution System（ディストリビューションシステム）
DShield Distributed Intrusion Detection System（分散化侵入検知システム）

EICAR European Institute for Computer Antivirus Research（欧州コンピュータウイルス対策研究所）
ESP Encapsulating Security Payload（暗号ペイロード）

FIPS Federal Information Processing Standards（連邦情報処理規格）
FISMA Federal Information Security Management Act（連邦情報セキュリティマネジメント法）
FTP File Transfer Protocol（ファイル転送プロトコル）

GHz Gigahertz（ギガヘルツ）
GUI Graphical User Interface（グラフィカルユーザインタフェース）

HTTP Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）
HTTPS Hypertext Transfer Protocol over SSL（SSL 経由のハイパーテキスト転送プロトコル）

ICMP Internet Control Message Protocol（インターネット制御通知プロトコル）
IDPS Intrusion Detection and Prevention System（侵入検知および侵入防止システム）
IDS Intrusion Detection System（侵入検知システム）

IEEE Institute of Electrical and Electronics Engineers（電気電子技術者学会）
IETF Internet Engineering Task Force（インターネット技術特別調査委員会）
IGMP Internet Group Management Protocol（インターネットグループ管理プロトコル）
IM Instant Messaging（インスタントメッセージング）
IMAP Internet Message Access Protocol（インターネットメッセージアクセスプロトコル）
IP Internet Protocol（インターネットプロトコル）
IPS Intrusion Prevention System（侵入防止システム）
IPsec Internet Protocol Security（インターネットプロトコルセキュリティ）
IRC Internet Relay Chat
ISC Internet Storm Center（インターネット上の脅威に関する情報サイト）
IT Information Technology（情報技術）
ITL Information Technology Laboratory（情報技術ラボラトリ）

LAN Local Area Network（ローカルエリアネットワーク）

MAC Media Access Control（媒体アクセス制御）

NBA Network Behavior Analysis（ネットワーク挙動解析）
NBAD Network Behavior Anomaly Detection（ネットワーク異常状況検知）
NFAT Network Forensic Analysis Tool（ネットワークフォレンジック分析ツール）
NFS Network File System（ネットワークファイルシステム）
NIC Network Interface Card（ネットワークインタフェースカード）
NIST National Institute of Standards and Technology（米国国立標準技術研究所）
NTP Network Time Protocol（ネットワークタイムプロトコル）
NVD National Vulnerability Database（脆弱性データベース）

OMB Office of Management and Budget（行政管理予算局）
OS Operating System（オペレーティングシステム）

PDA Personal Digital Assistant（携帯情報端末）
PoE Power over Ethernet（イーサネット配線による電力供給）
POP Post Office Protocol（ポストオフィスプロトコル）

RF Radio Frequency（無線周波数）
RFC Request for Comment（インターネット技術に関する IETF 発行文書）
ROM Read-Only Memory（読み取り専用メモリ）
RPC Remote Procedure Call（リモートプロシージャコール）

SEM Security Event Management（セキュリティイベント管理）
SIEM Security Information and Event Management（セキュリティ情報およびイベント管理）
SIM Security Information Management（セキュリティ情報管理）
SIP Session Initiation Protocol（セッションイニシエーションプロトコル）
SMB Server Message Block（サーバメッセージブロック）
SMTP Simple Mail Transfer Protocol（簡易メール転送プロトコル）
SNMP Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
SP Special Publication（特別刊行物）

SSH Secure Shell（セキュアシェル）
SSID Service Set Identifier（サービスセット識別子）
SSL Secure Sockets Layer（セキュアソケットレイヤ）
STA Station（ステーション）

TCP Transmission Control Protocol（伝送制御プロトコル）
TCP/IP Transmission Control Protocol/Internet Protocol（伝送制御プロトコル／インターネットプロトコル）
TFTP Trivial File Transfer Protocol（簡易ファイル転送プロトコル）
TLS Transport Layer Security（トランスポート層セキュリティ）
TTL Time to Live（存続時間）

UDP User Datagram Protocol（ユーザデータグラムプロトコル）
USB Universal Serial Bus（ユニバーサルシリアルバス）
US-CERT United States Computer Emergency Readiness Team（米国コンピュータ緊急対応チーム）

VLAN Virtual Local Area Network（仮想ローカルエリアネットワーク）
VPN Virtual Private Network（仮想プライベートネットワーク）

WEP Wired Equivalent Privacy（有線ネットワークと同等のプライバシ）
WLAN Wireless Local Area Network（無線ローカルエリアネットワーク）
WPA Wi-Fi Protected Access（アクセス保護付き Wi-Fi）
WVE Wireless Vulnerabilities and Exploits（無線関連の脆弱性および悪用情報サイト）

XML Extensible Markup Language（拡張可能マークアップ言語）

（本ページは意図的に白紙のままとする）

付録 C—ツールおよびリソース

以下の一覧には、役に立つツールとリソースの例を示す。

印刷資料

Bace, Rebecca, Intrusion Detection, Macmillan Technical Publishing, 2000.

Bejtlich, Richard, Extrusion Detection, Addison-Wesley, 2005.

Bejtlich, Richard, The Tao of Network Security Monitoring: Beyond Intrusion Detection, Addison-Wesley, 2004.

Crothers, Tim, Implementing Intrusion Detection Systems: A Hands-On Guide for Securing the Network, 2002.

Endorf, Carl et al, Intrusion Detection and Prevention, McGraw-Hill Osborne Media, 2003.

Kruegel, Chris et al, *Intrusion Detection and Correlation: Challenges and Solutions*, Springer, 2004.

Nazario, Jose, Defense and Detection Strategies Against Internet Worms, Artech House Publishers, 2003.

Northcutt, Stephen and Novak, Judy, Network Intrusion Detection: An Analyst's Handbook, Third Edition, New Riders, 2003.

Rash, Michael et al, Intrusion Prevention and Active Response: Deployment Network and Host IPS, Syngress, 2005.

組織

組織名	URL
Computer Incident Advisory Capability (CIAC)	http://www.ciac.org/ciac/
Cooperative Association for Internet Data Analysis (CAIDA)	http://www.caida.org/home/
Distributed Intrusion Detection System (DShield)	http://dshield.org/indexd.html
European Institute for Computer Antivirus Research (EICAR)	http://www.eicar.org/
IETF Intrusion Detection Exchange Format (idwg) Working Group	http://www.ietf.org/html.charters/OLD/idwg-charter.html
Internet Storm Center (ISC)	http://isc.incidents.org/
SANS Institute	http://www.sans.org/
United States Computer Emergency Readiness Team (US-CERT)	http://www.us-cert.gov/
Virus Bulletin	http://www.virusbtn.com/index
Viruslist.com	http://www.viruslist.com/en/
WildList Organization International	http://www.wildlist.org/

技術資料サイト

資料名	URL
CSRC—Practices & Checklist/Implementation Guides	http://csrc.nist.gov/pcig/cig.html
Unassigned IP Address Ranges	http://www.cymru.com/Documents/bogon-list.html
一般的リソースおよびネットワークベースの IDPS に関するリソース	
An Introduction to Intrusion Detection Systems	http://www.securityfocus.com/infocus/1520
Comparison of Firewall, Intrusion Prevention and Antivirus Technologies	http://www.juniper.net/solutions/literature/white_papers/200063.pdf
Evaluating Intrusion Prevention Systems	http://www.cioupdate.com/article.php/3563306
IDS: Intrusion Detection System	http://www.javvin.com/networksecurity/ids.html
Intrusion Detection System Frequently Asked Questions	http://www.sans.org/resources/idfaq/
Intrusion Detection System Overview	http://www.webopedia.com/TERM/I/intrusion_detection_system.html
Intrusion Detection: Implementation and Operational Issues	http://www.stsc.hill.af.mil/crosstalk/2001/01/mchugh.html
Intrusion Prevention Systems	http://www.nfr.com/resource/downloads/SentivistIPS-WP.pdf
Intrusion Prevention Systems (IPS)	http://www.securecomputing.com/pdf/Intru-Preven-WP1-Aug03-vF.pdf
Intrusion Prevention Systems (IPS)	http://hosteddocs.ittoolbox.com/BW013004.pdf
Intrusion Prevention Systems: the Next Step in the Evolution of IDS	http://www.securityfocus.com/infocus/1670
Recommendations for Deploying an Intrusion-Detection System	http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci781471,00.html
SANS Glossary of Terms Used in Security and Intrusion Detection	http://www.sans.org/resources/glossary.php
State of the Practice of Intrusion Detection Technologies	http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr028.pdf
The Evolution of Intrusion Detection Systems	http://www.securityfocus.com/infocus/1514
無線 IDPS に関するリソース	
Wireless IDSes Defend Your Airspace	http://www.eweek.com/article2/0,1895,1630842,00.asp
Wireless Intrusion Detection and Response	http://users.ece.gatech.edu/~owen/Research/Conference%20Publications/wireless_IAW2003.pdf
Wireless Intrusion Detection Systems	http://www.securityfocus.com/infocus/1742
Wireless Intrusion Detection Systems: GIAC Security Essentials	http://www.sans.org/rr/whitepapers/wireless/1543.php
NBA IDPS に関するリソース	
Anomaly Detection Can Prevent Network Attacks	http://www.techworld.com/networking/features/index.cfm?featureid=2338&pagtype=samecat
Anomaly Detection in IP Networks	http://users.ece.gatech.edu/~jic/sig03.pdf
Design and Implementation of an Anomaly Detection System: an Empirical Approach	http://luca.ntop.org/ADS.pdf
IDS: Signature Versus Anomaly Detection	http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1092691,00.html?track=IDSLG
Packet vs Flow-Based Anomaly Detection	http://www.esphion.com/pdf/ESP_WP_4_PACKET_V_FLOWS.pdf
The State of Anomaly Detection	http://www.securityfocus.com/infocus/1600

資料名	URL
ホストベースの IDPS に関するリソース	
Host-Based IDS vs Network-Based IDS	http://www.windowsecurity.com/articles/Hids_vs_Nids_Part1.html
Host-Based IDSs Add to Security Policy	http://www.networkworld.com/news/tech/2003/0915techupdate.html
Host-Based Intrusion Detection System Definition	http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
Host-Based Intrusion Detection Systems	http://staff.science.uva.nl/~delaat/snb-2004-2005/p19/report.pdf
What Is Host-Based Intrusion Detection?	http://www.sans.org/resources/idfaq/host_based.php

メーリングリストと通知サービス

メーリングリスト／通知サービス名	URL
Incidents	http://www.securityfocus.com/cgi-bin/index.cgi?c=11&op=display_threads&ListID=75&limit=30&offset=0&date=2007-01-16&mode=threaded
Security Focus	http://www.securityfocus.com/ids
SecurityTracker.com	http://securitytracker.com/

その他の技術資料文書

資料名	URL
IETF, RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing*	http://www.ietf.org/rfc/rfc2267.txt
NIST, SP 500-267, *A Profile for IPv6 in the U.S. Government, Version 1.0 (DRAFT)*	http://www.antd.nist.gov/
NIST, SP 800-31, *Intrusion Detection Systems*	http://csrc.nist.gov/publications/nistpubs/
NIST, SP 800-42, Guideline on Network Security Testing	*http://csrc.nist.gov/publications/nistpubs/*
NIST, SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*	http://csrc.nist.gov/publications/nistpubs/
NIST, SP 800-53, *Recommended Security Controls for Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/
NIST, SP 800-61, *Computer Security Incident Handling Guide*	http://csrc.nist.gov/publications/nistpubs/
NIST, SP 800-70, *Security Configuration Checklists Program for IT Products*	http://csrc.nist.gov/checklists/
NIST, SP 800-83, *Guide to Malware Incident Prevention and Handling*	http://csrc.nist.gov/publications/nistpubs/
NIST, SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*	http://csrc.nist.gov/publications/nistpubs/
NIST, SP 800-88, *Guidelines for Media Sanitization*	http://csrc.nist.gov/publications/nistpubs/
NIST, SP 800-92, *Guide to Computer Security Log Management*	http://csrc.nist.gov/publications/nistpubs/
NIST, SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*	http://csrc.nist.gov/publications/nistpubs/

一般的なエンタープライズ向けネットワークベース IDPS

製品系列	ベンダー	URL
Attack Mitigator	Top Layer Networks	http://www.toplayer.com/content/products/index.jsp
BBX	DeepNines	http://www.deepnines.com/bbx.php
Bro	Vern Paxson	http://bro-ids.org/
Cisco IPS	Cisco Systems	http://www.cisco.com/en/US/products/hw/vpndevc/index.html
Cyclops	e-Cop.net	http://www.e-cop.net/
DefensePro	Radware, Ltd.	http://www.radware.com/content/products/dp/default.asp
Dragon	Enterasys Networks, Inc.	http://www.enterasys.com/products/ids/
eTrust Intrusion Detection	Computer Associates	http://www3.ca.com/solutions/Product.aspx?ID=163
Juniper Networks IDP	Juniper Networks	https://www.juniper.net/products/intrusion/
IntruShield	Network Associates	http://www.mcafee.com/us/enterprise/products/network_intrusion_prevention/index.html
iPolicy	iPolicy Networks	http://www.ipolicynetworks.com/products/ipf.html
Proventia	Internet Security Systems	http://www.iss.net/products/product_sections/Intrusion_Prevention.html
SecureNet	Intrusion	http://www.intrusion.com/
Sentivist	Check Point Software Technologies	http://www.nfr.com/solutions/sentivist-ips.php
Snort	Sourcefire	http://www.snort.org/
Sourcefire	Sourcefire	http://www.sourcefire.com/products/is.html
StoneGate	StoneSoft Corporation	http://www.stonesoft.com/en/products_and_solutions/products/ips/
Strata Guard	StillSecure	http://www.stillsecure.com/strataguard/index.php
Symantec Network Security	Symantec Corporation	http://www.symantec.com/enterprise/products/index.jsp
UnityOne	TippingPoint Technologies	http://www.tippingpoint.com/products_ips.html

一般的なエンタープライズ向け無線 IDPS

製品系列	ベンダー	URL
AirDefense	AirDefense	http://www.airdefense.net/products/index.php
AirMagnet	AirMagnet	http://www.airmagnet.com/products/
AiroPeek	WildPackets	http://www.wildpackets.com/products/airopeek/overview
BlueSecure	BlueSocket	http://www.bluesocket.com/products/centralized_intrusion.html
Highwall	Highwall Technologies	http://www.highwalltech.com/products.cfm
Red-Detect	Red-M	http://www.red-m.com/products-and-services/red-detect.html
RFprotect	Network Chemistry	http://networkchemistry.com/products/
SpectraGuard	AirTight Networks	http://www.airtightnetworks.net/products/products_overview.html

一般的なエンタープライズ向け NBA システム

製品系列	ベンダー	URL
Arbor Peakflow X	Arbor Networks	http://www.arbornetworks.com/products_x.php
Cisco Guard, Cisco Traffic Anomaly Detector	Cisco Systems	http://www.cisco.com/en/US/products/hw/vpndevc/index.html
GraniteEdge ESP	GraniteEdge Networks	http://www.graniteedgenetworks.com/products
OrcaFlow	Cetacea Networks	http://www.orcaflow.ca/features-overview.php
Profiler	Mazu	http://www.mazunetworks.com/products/index.php
Proventia Network Anomaly Detection System (ADS)	Internet Security Systems	http://www.iss.net/products/Proventia_Network_Anomaly_Detection_System/product_main_page.html
QRadar	Q1 Labs	http://www.q1labs.com/content.php?id=175
StealthWatch	Lancope	http://www.lancope.com/products/

一般的なエンタープライズ向けホストベース IDPS

製品系列	ベンダー	URL
BlackIce	Internet Security Systems	http://www.iss.net/products/product_sections/Server_Protection.html http://www.iss.net/products/product_sections/Desktop_Protection.html
Blink	eEye Digital Security	http://www.eeye.com/html/products/blink/index.html
Cisco Security Agent	Cisco Systems	http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html
Deep Security	Third Brigade	http://www.thirdbrigade.com/
DefenseWall HIPS	SoftSphere Technologies	http://www.softsphere.com/programs/
Intrusion SecureHost	Intrusion	http://www.intrusion.com/
McAfee Host Intrusion Prevention	McAfee	http://www.mcafee.com/us/enterprise/products/host_intrusion_prevention/index.html
Primary Response	Sana Security	http://www.sanasecurity.com/products/pr/index.php
Proventia	Internet Security Systems	http://www.iss.net/products/product_sections/Server_Protection.html http://www.iss.net/products/product_sections/Desktop_Protection.html
RealSecure	Internet Security Systems	http://www.iss.net/products/product_sections/Server_Protection.html http://www.iss.net/products/product_sections/Desktop_Protection.html
SecureIIS Web Server Protection	eEye Digital Security	http://www.eeye.com/html/products/secureiis/index.html
Symantec Critical System Protection	Symantec	http://www.symantec.com/enterprise/products/index.jsp

（本ページは意図的に白紙のままとする）

付録 D—索引

こ

さ

し

す

せ

そ

ち

て

と

な

に

ね

は

ふ

へ

ほ

ま

む

め

ゆ

り

る

ろ

わ