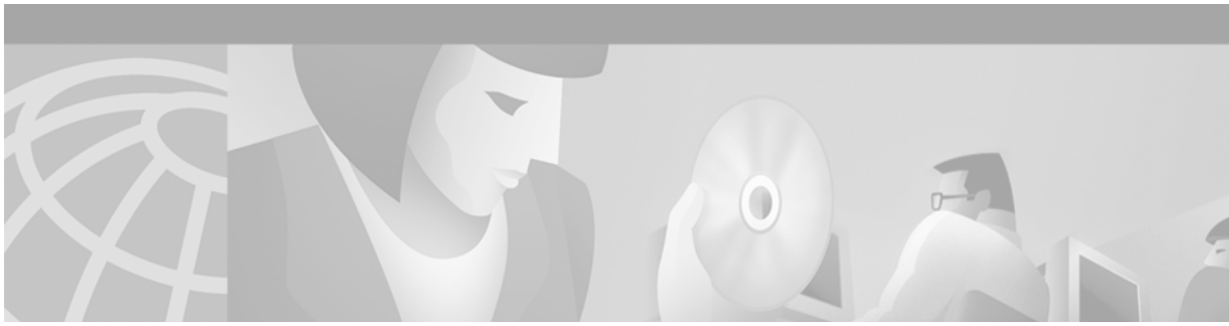


Cisco Intrusion Detection System Sensor インストレーション ノート

2002 年 5 月

このマニュアルでは、Cisco Intrusion Detection System（IDS）Sensor の概要と、ネットワークへの配置に関する情報、インストール手順、準処規定、および安全に関する情報について説明します。

目次

CISCO SYSTEMS

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

78-7016-04-J

安全に関する概要

安全上の警告は、このコンフィギュレーション ノート全体で、誤った操作がされたとき事故につながる可能性がある場合に表示されます。警告を意味する記号が各警告文の前に示されています。以下に、このノートで使用されている警告の記号について説明します。

警告について

警告

危険を意味します。怪我をする可能性があるので、装置を扱う前に電気回路に伴う障害に注意し、事故を防止するための標準手順を十分理解しておく必要があります。

Sensor の概要

Sensor（モデル IDS-4210、IDS-4220-E、IDS-4230-FE、IDS-4235、IDS-4250-TX、および IDS-4250-SX）は、高性能でプラグアンドプレイが可能な装置です。また、ネットワークベースのリアルタイム侵入検知システムのコンポーネントです。Sensor は、Cisco IDS Device Manager（IDM）、Cisco IDS Director for UNIX（IDD）、または Cisco Secure Policy Manager（CSPM）などの IDS マネージャーにより管理されます。Sensor と IDS マネージャー間に通信が確立すると、IDS マネージャーは Sensor を制御および構成します。Sensor は、ネットワーク トラフィックを取り込んで分析を行うとき、認識可能なシグニチャに対して応答するように設定することができます。この応答には、イベントのロギング、イベントの IDS マネージャーへの転送、TCP リセットの実行、IP ログの生成、およびルータの再構成が含まれます。

（注）次の Sensor モデルはレガシー モデルのため、このマニュアルではサポートされていません。NRS-2E、NRS-2E-DM、NRS-2FE、NRS-2FE-DM、NRS-TR、NRS-TR-DM、NRS-SFDDI、NRS-SFDDI-DM、NRS-DFDDI、NRS-DFDDI-DM、IDS-4220-TR、IDS-4230-SFDDI、IDS-4230-DFDDI。

ネットワークのキーポイントにインストールされると、膨大な埋め込み型シグニチャ ライブラリに基づいて異常および悪用を探すことで、Sensor がネットワーク トラフィックを監視しリアルタイム分析を実行します。システムが不正行為を検知した場合、Sensor は特定の接続を終了し、攻撃しているホストを永続的にブロックし、この事態を記録してアラームを IDS マネージャーに送信します。その他の正規の接続は、ネットワーク サービスまたはパフォーマンスが影響されることなく独立して動作が継続されます。

Sensor は、ネットワーク セキュリティ ポリシー違反を検知および報告するために、Cisco ルータからの syslog メッセージを監視および分析することも可能です。

Sensor は、特定のデータ レートに最適化されています。スイッチング環境においては、Sensor は、スイッチの Switched Port Analyzer（SPAN）ポートに接続される必要があります。IDM は Sensor を 3 台まで管理できます。スタンドアロンとして、または CSPM 内に設定された 1 つの IDD は、何十もの Sensor のアクティビティを集中的に管理することができます。さらに、複数の Director を階層構造に配置することで、システムを拡張し、最大規模の企業環境にも対処することができます。IDS マネージャー（複数可）および Sensor（複数可）の間の通信は、postoffice と呼ばれるシスコ独自のフォールト トレラントな通信システムによって提供されます。

Sensor の導入

ここでは、Sensor をネットワークにインストールする上で最適な場所の判別方法について説明します。次の項目があります。

ネットワーク トポロジの確認

Sensor を最も良い状態に配置および設定するには、使用中のネットワークについて次の点を注意深く調査する必要があります。

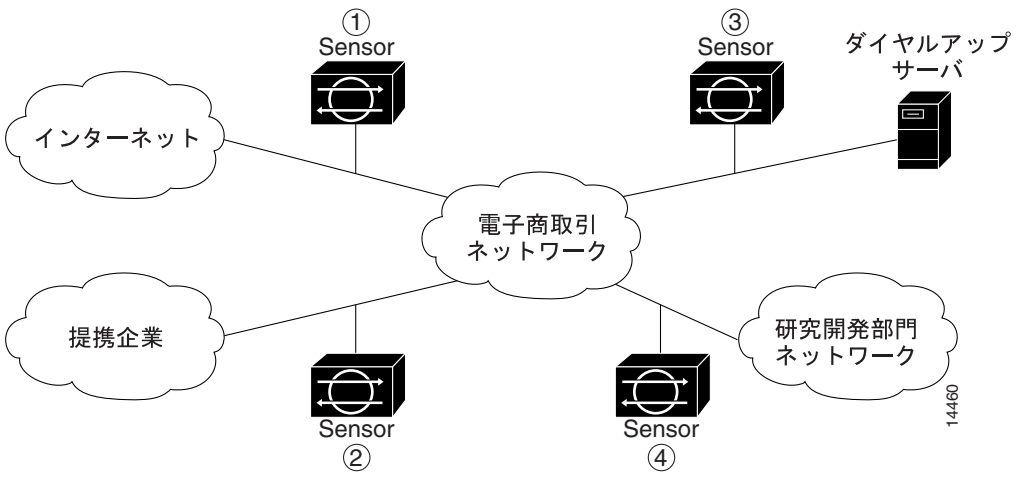
- 対象ネットワークの規模と複雑さ
- 対象ネットワークとほかのネットワーク（およびインターネット）間の接続状態
- 対象ネットワーク上のネットワーク トラフィックの量と種類

この 3 点を検討しておくと、必要な Sensor の数、各 Sensor のハードウェア構成（たとえば、ネットワーク インターフェイス カードのサイズと種類）、および必要な IDS 管理ワークステーションの数を決定する作業が容易になります。

（注） IDS の詳細情報については、次の Web サイトにある『*Intrusion Detection Planning Guide*』を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/index.htm

Sensor は、所定のネットワーク セグメントを通過するトラフィックをすべて監視するように設計されています。そのことを念頭において、保護するネットワークに対する接続すべてを検討する必要があります。このような接続は、図 1 に示すように、4 つの基本的なカテゴリまたは位置に分類することができます。

図 1　　ネットワーク接続の主要方式



位置 1 では、Sensor が保護されたネットワークとインターネット間のトラフィックを監視するように配置されています。このような方法は一般に「周辺保護」と呼ばれており、最もよく使用される Sensor の導入方式です。この位置は、ファイアウォール保護と共有することができます。これについては P.5 の「ネットワークへの Sensor の導入」で説明します。

位置 2 では、Sensor が提携企業とのエクストラネット接続を監視します。多くの企業がこの形の接続の使用とセキュリティに対する方針を明確に規定していますが、提携企業のネットワークが十分に保護されているという保証はありません。したがって、外部の者が、この形の接続を通してネットワークに入り込む可能性があります。このようなエクストラネットも、ファイアウォールで保護することが可能です。

位置 3 では、Sensor がリモート アクセス サーバのネットワーク側を監視しています。この接続は、従業員専用に設けられたものですが、外部からの攻撃に弱いという問題があります。

位置 4 は、Sensor がイントラネット接続を監視します。たとえば、ある部門の保護されたネットワークには、電子商取引拠点が含まれ、これまで説明したアクセス方式がすべて要求される可能性があります。また別の部門のネットワークには、企業固有の研究開発情報およびその他の技術情報が含まれている可能性があり、一段と保護を強化する必要があります。

以上の情報を基に、ここで、保護するネットワークについて検討してみましょう。監視が必要なセグメントを決定します。各 Sensor が、監視するセグメントに対して設定されているセキュリティ ポリシーを保持していることを忘れないでください。このセキュリティ ポリシーは、組織全体に標準にすることも、各 Sensor に独自のものとすることもできます。ネットワーク トポロジを変更して、トラフィックが必ず、所定の監視下ネットワーク セグメントを通るようにすることも検討してください。ここでは常に、運用上のトレードオフも検討する必要があります。最終結果は、対象ネットワークの保護に必要な Sensor の数の概数に帰結します。

Sensor の動作の理解

ネットワーク保護の次のステップは、Sensor がどのようにしてネットワーク トラフィックを取り込むかを理解することです。

各 Sensor には、インターフェイスが 2 つあります。通常のインストールでは、1 つのインターフェイスが対象ネットワーク セグメントの監視に使用され、もう 1 つのインターフェイスが IDS 管理ワークステーションやほかのネットワーク デバイスとの通信に使用されます。モニタリング インターフェイスは識別不能モードになっており、IP アドレスを持たず、監視されているセグメント上では見えない状態になっています。

Sensor は、ネットワーク トラフィックを IP 層で取り込みます。したがって、MAC（メディア アクセス制御）層プロトコルを認識および解釈する必要があります。このプロトコルは、多くのネットワークがデータ パケットの転送に使用しています。

制御インターフェイスは、常に、イーサネットになります。制御インターフェイスには、IP アドレスが割り当てられており、IDS 管理ワークステーションまたはネットワーク デバイス（通常は、Cisco ルータ）と通信ができるようになっています。制御インターフェイスはセキュリティの点では「強化」されていますが、ネットワーク上では見える状態にあるので、保護することが必要です。

Sensor は攻撃に反応するとき、次のことを行います。

- モニタリング インターフェイスを介して TCP リセットを挿入する

（注） TCP リセット アクションは、TCP ベースのサービスに関連しているシグニチャで選択した場合に限り適切に動作します。非 TCP ベースのサービスのアクションとして選択した場合は、動作しません。さらに、TCP プロトコルには制限があるため、TCP リセットは違反するセッションの切断を保証していません。

- Sensor が管理するルータのアクセス コントロール リスト（ACL）を変更する

（注） ACL は、現在のトラフィックではなく、将来のトラフィックをブロックします。

- 制御インターフェイスを介してトラフィックをブロックする

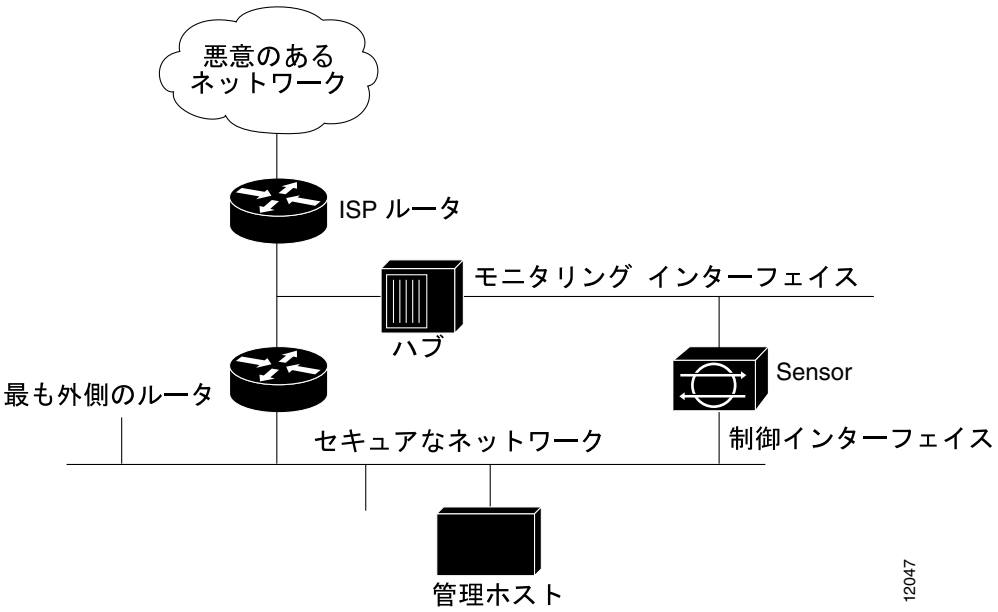
Sensor の動作を理解する最後のステップは、監視されるネットワーク上のデータ速度またはデータ負荷を理解することです。Sensor はデータ パス中にないため、ネットワーク パフォーマンスに対する影響は、無視できるほど小さくなります。しかし、Sensor が監視できるデータ速度には限界があります。

ネットワークへの Sensor の導入

Sensor は、ファイアウォールの前または後ろに置くことができます。各配置には、長所および短所があります。

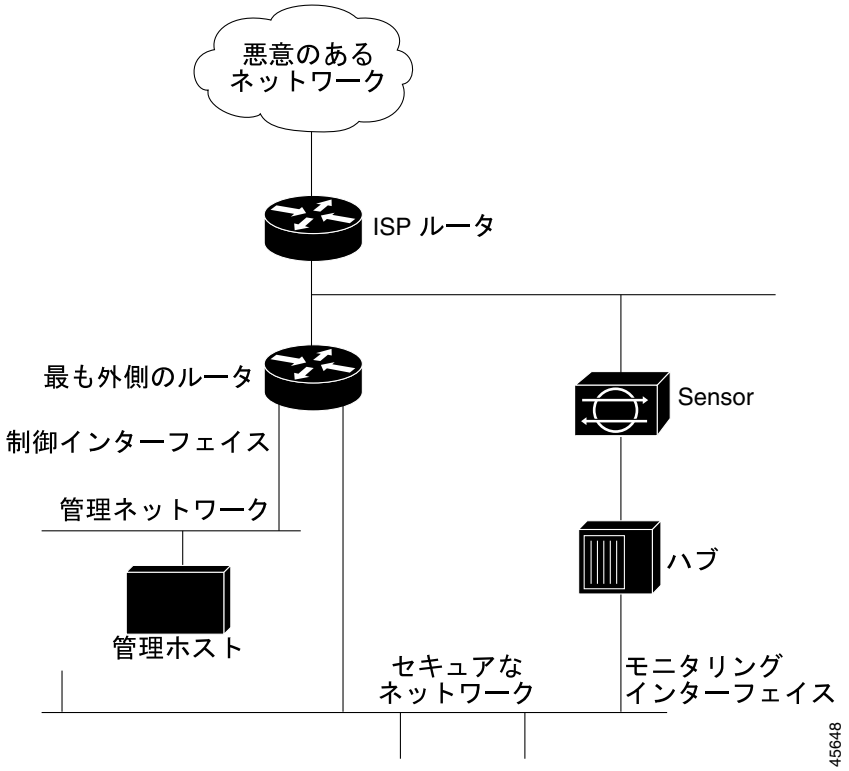
Sensor は、ファイアウォールの前に配置すると、発着信のネットワーク トラフィックすべてを監視することができます。ただし、この方法で設置した場合は、Sensor はネットワーク内部のトラフィックを通常に検出することができなくなります。ネットワーク サービスの弱点を悪用する内部の攻撃者は、外部 Sensor では検出できません（図 2）。

図 2　ファイアウォールの前に配置された Sensor



Sensor（モニタリング インターフェイスまたはスニファ インターフェイス）は、ファイアウォールの後ろに配置すると、ファイアウォールが拒否するポリシー違反すべてから防御されます（図 3 参照）。

図 3　　ファイアウォールの後ろに配置された Sensor



設置に関する検討事項

Sensor がルータとファイアウォールを利用するネットワーク構成を効果的に防御するには、次の事項を実行する必要があります。

- ルータ上で Telnet サービスをイネーブルにする。
- ルータを Sensor のデバイス管理リストに追加する（IDS マネージャーを介して）。
- 次のトラフィックを許可するようにファイアウォールを設定する。
  - Sensor の制御インターフェイスからルータへの Telnet トラフィック
  - ルータから Sensor への syslog（UDP ポート 514）トラフィック

（注）　ルータでのポリシー違反を認識するには、syslog メッセージを受け入れるように Sensor を設定する必要があります。

  - Sensor と任意の IDS 管理ワークステーション間の postoffice 通信（UDP ポート 45000）（Sensor と任意の IDS 管理ワークステーションの間にファイアウォールが存在する場合）

    本質的に、ファイアウォールは、ポリシー フィルタリングを実施します。Sensor は、Cisco ルータとファイアウォールの間のパケットを取り込み、動的に Cisco ルータの ACL を更新し、不正行為を拒否します。

インストール方法

ここでは、Sensor を使用中のネットワークに導入する方法について説明します。

警告 インストールに関する説明を読んでから、システムを電源に接続してください。

警告 訓練を受けた有資格の要員以外は、この機器の設置、交換、および保守は行わないでください。

警告 この装置は、TN 電源系で動作するように設計されています。

警告 オン / オフ スイッチのあるシステムに対して作業するときは、事前に電源を切り、電源コードを抜いてください。

警告 この製品は、ショート（過電流）保護をビルディング設備に依存しています。必ず、120 VAC、15A 以下（アメリカ合衆国の場合）または、240 VAC、10A 以下（アメリカ合衆国以外の場合）のヒューズまたはサーキット ブレーカを電圧線（電流が流れる導体すべて）に挿入してください。

警告 この装置は、アースすることになっています。ホストは、通常の使用時には、必ず接地してください。

警告 安全カバーは、製品の重要な一部です。安全カバーを取り付けない状態で装置を操作しないでください。安全カバーを所定の位置に取り付けずに装置を操作した場合、安全性の保証が保たれず、火災および電気事故の危険が生じます。

警告 ブランク前面プレートおよびカバー パネルには、次の 3 つの重要な機能があります。シャーシ内の危険な電圧および電流に対する照射を防ぐ、ほかの装置に対して影響を及ぼすような電磁干渉（EMI）を防ぐ、シャーシ内の冷却空気の流れを確保する、の 3 つです。必ず、すべてのカード、前面プレート、前面カバー、および背面カバーが正しく取り付けられた状態でシステムを動作してください。

警告 電源に接続されている装置に対して作業する場合は、事前に装身具（指輪、ネックレス、腕時計など）を外してください。このような金属製品が電圧がかかっている部分とアースに接触すると、金属が過熱して重度の火傷を負ったり、金属製品が端子に融着する恐れがあります。

警告 **雷が発生しているときは、システムに対する作業や、ケーブルの脱着を行わないようにしてください。**

警告 **電気ショックを回避するため、SELV（安全低電圧）回路を TNV（電話ネットワーク電圧）回路に接続しないでください。LAN ポートには SELV 回路があり、WAN ポートには TNV 回路があります。LAN ポートおよび WAN ポートによっては、両方とも RJ-45 コネクタを使用する場合があります。ケーブルを接続する祭は、注意してください。**

Sensor を組み立てるには、次の手順を実行します。

ステップ 1 Sensor をネットワーク上に配置します。

P.3 の「Sensor の導入」を参照して、Sensor を配置する最良の場所を検討してください。

（注） ネットワークにおける侵入検知の使用についての詳細情報は、次の Web サイトにある『*Intrusion Detection Planning Guide*』を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/index.htm

ステップ 2 電源コードを Sensor に接続し、電源に差し込みます（UPS を推奨）。

（注） IDS-4210、IDS-4235、または IDS-4250 Sensor を電源に接続するときは、一瞬で電源が入り、ネットワーク インターフェイス カード（NIC）のリンク ライトが点灯したまま電源が切れます。これは通常の動作です。電源スイッチを押してシステムをブートします。

ステップ 3 シリアル通信ケーブル（P/N 72-1847-01、アクセサリ キットに含まれる）を使用して、ラップトップを Sensor の COM1 ポートに接続するか、キーボードおよびモニタを Sensor に接続します（端末設定リストについては、表 1 を参照してください）。

表 1　端末設定

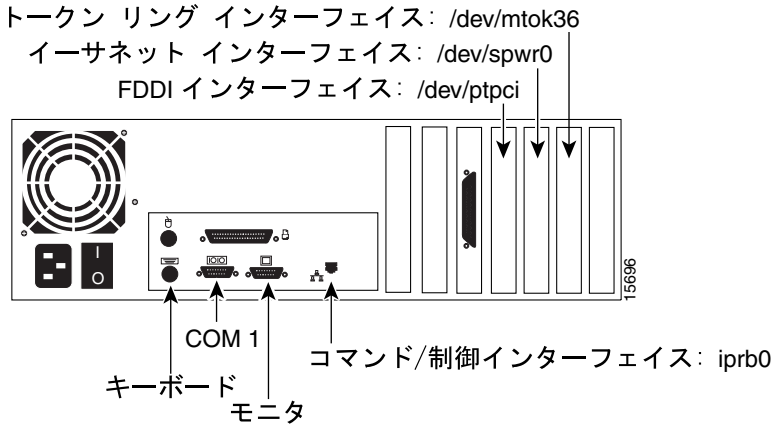
端末	設定
ビット / 秒	9600
データ ビット	8
パリティー	なし
ストップ ビット	1
フロー制御	ハードウェアまたは RTS/CTS

注意 キーボードとモニタによっては、Sensor と互換性がないものがあるため、キーボードとモニタではなく、シリアル通信ケーブルの使用をお勧めします。互換性のあるモニタおよびキーボードのリストは P.11 の「推奨されるキーボードおよびモニタ」を参照してください。

ステップ 4 図 4、図 5 または図 6 に示す Sensor の背面パネルと比較して、使用中のネットワーク構成の種類を識別してください。

ステップ 5 それに従ってネットワーク ケーブルを接続します。

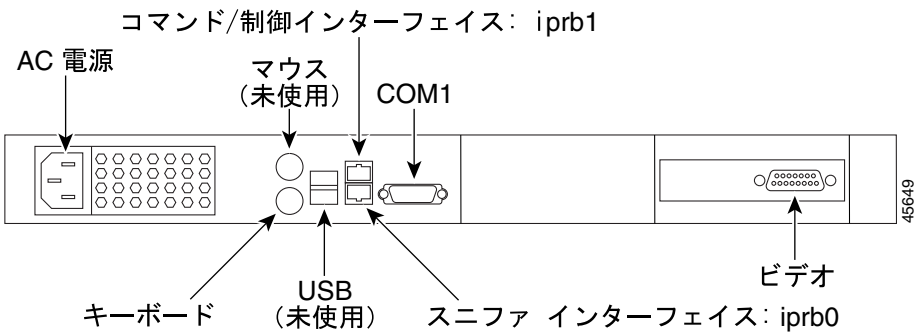
図 4　NRS シリーズ、IDS-4220（-E および -TR）、および IDS-4230（-FE、-SFDDI、-DFDDI）



- イーサネット ネットワーク構成またはファースト イーサネット ネットワーク構成の場合
  - iprb0 インターフェイスを、コマンドおよび制御用に使用します。
  - spwr0 インターフェイスを、監視下のネットワークからパケットを取り込むために使用します。
- トークン リング ネットワーク構成の場合
  - iprb0 インターフェイスを、コマンドおよび制御用に使用します。
  - mtok36 インターフェイスを、監視下のネットワークからパケットを取り込むために使用します。
- FDDI ネットワーク構成の場合
  - iprb0 インターフェイスを、コマンドおよび制御用に使用します。
  - ptpci インターフェイスを、監視下のネットワークからパケットを取り込むために使用します。

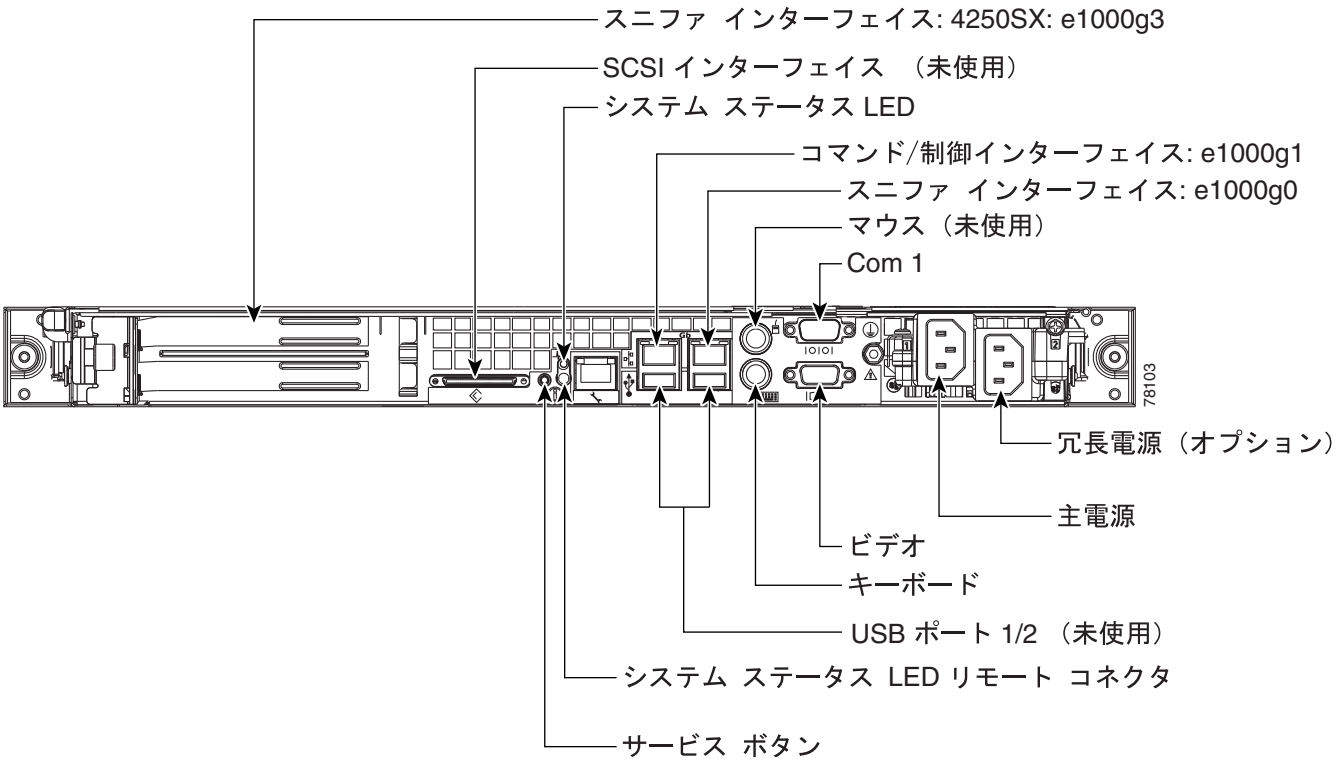
Multicast Media Access Control（MAC）トラフィックを IDS-4220-E または IDS-4230-FE Sensor で監視する場合にインターフェイスを切り替える手順については、P.12 の「Sensor 上でのインターフェイスの切り替え」を参照してください。

図 5　IDS-4210



- イーサネット ネットワーク構成の場合
  - iprb1 インターフェイスを、コマンドおよび制御用に使用します。
  - iprb0 インターフェイスを、パケットを取り込むために使用します。

図 6　IDS-4235、IDS-4250-SX、および IDS-4250-TX



- Command & Control（コマンドと制御）インターフェイス：e1000g1。
- スニッフィング インターフェイス（銅線、C&C の隣）：e1000g0（IDS-4235、IDS-4250-TX）。
- スニッフィング インターフェイス（光ファイバ、PCI アドオンカード）：e1000g3（IDS-4250-SX）。

ステップ 6　Sensor に電源を入れます。

これで Sensor を設定する準備が整いました。Sensor のセットアップに sysconfig-sensor を起動する方法については、該当する Sensor のコンフィギュレーション ノートを次の Web サイトで参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm

推奨されるキーボードおよびモニタ

一部のキーボードおよびモニタは Sensor との互換性がありません。このことは Sensor が正しく起動しない原因になる場合があります。Sensor には次のキーボードおよびモニタを使用することをお勧めします。

- キーボード
  - KeyTronic E03601QUS201-C
  - KeyTronic LT DESIGNER
- モニタ
  - MaxTech XT-7800
  - Dell D1025HT

注意 一部の HP キーボードおよび IBM モデル G50 モニタを使用すると Sensor が正しく機能しません。

Sensor の制限

Sensor の使用と操作には、次の制限事項があります。

- Sensor は、汎用的なワークステーションではありません。
- シスコシステムズでは Cisco IDS の操作以外に Sensor を使用することを禁止しています。
- シスコシステムズでは、Cisco IDS の通常操作ではない、Sensor に対するいかなるハードウェアとソフトウェアの変更およびインストールを禁止しています。

Sensor 上でのインターフェイスの切り替え

Multicast MAC トラフィックを IDS-4220-E または IDS-4230-FE Sensor を使用して監視する場合は、インターフェイスを切り替える必要があります。

パスワードを変更するには、次の手順を実行します。

ステップ 1 root としてログインします。

ステップ 2 /usr/nr/etc/packetd.conf 内の NameOfPacketDevice トークンを次のように変更します。

```
/dev/iprb0
```

ステップ 3 次のコマンドを入力し、spwr インターフェイスを C&C（コマンドおよび制御）に設定します。

```
mv /etc/hostname.iprb0 /etc/hostname.spwr0
```

ステップ 4 ネットワーク ケーブルを交換します（iprb0<->spwr0）。

ステップ 5 Sensor を再度ブートして変更を有効にします。

欧州共同体（EC）、スイス、ノルウェー、アイスランドおよびリヒテンシュタイン

指令 93/68/EEC により改正された 指令 73/23/EEC および 89/336/EEC に関する適合宣言

この製品に関連する適合宣言は、次の URL でご確認いただけます。

http://www.ciscofax.com/

この機器は、指令 93/68/EEC により改正された指令 73/23/EEC および 89/336/EEC の必須条件およびその他の条件に準拠しています。

標準準拠規定

準拠規定、安全性、および EMC 承認要求を満たしている Sensor のリストを 表 2 に示します。EMC に関する注意事項および警告については、次の項を参照してください。

- EU 諸国で製品を設置する場合の EMC 環境条件（P.13）
- （FCC）クラス A に関する警告（P.14）
- クラス A に関する警告（カナダ）（P.14）
- CISPR 22 クラス A に関する警告（P.14）
- VCCI クラス A に関する警告（日本）（P.14）
- BSMI クラス A に関する警告（台湾）（P.14）
- クラス A に関する警告（ハンガリー）（P.15）
- Korean Class A Warning（P.15）

表 2　　標準準拠規定

仕様	説明
準拠規定	CE[1] マークが付いている製品は、89/366/EEC、73/23/EEC の指示に準拠していることを示しています。これには次の安全基準および EMC 標準が含まれます。
安全性	UL[2] 1950 CSA[3] --C22.2 No. 950 EN[4] 60950 IEC[5] 60950
EMC	FCC[6] Part 15 (CFR[7] 47) Class A EN55022 Class A CISPR22 Class A AS/NZS[8] 3548 Class A VCCI[9] Class A EN50082-1 EN-55024 EN61000-3-2 EN61000-3-3

1.CE= European Compliance
2.UL = Underwriters Laboratory
3.CSA = Canadian Standards Association
4.EN = European Norm
5.IEC = International Electrotechnical Commission
6.FCC = Federal Communications Commission
7.CFR = Code of Federal Regulations
8.AS/NZS = Standards Australia/Standards New Zealand
9.VCCI = Voluntary Control Council for Information Technology Equipment (Japan)

EU 諸国で製品を設置する場合の EMC 環境条件

この機器は、EMC に関して次の条件下で運用するように設定されています。

1. ユーザの管理下にある専用の設置場所
2. ETS 300 253 または CCITT K27 の要件に適合するアース接続およびボンディング
3. 該当する場合、AC 配源は TN-S および TN-C [IEC 364-3 に規定] のいずれかのタイプにする

また、住宅地で装置を運用する場合、干渉が発生することがあります。

（FCC）クラス A に関する警告

シスコの許可なしに機器を改造すると、機器がクラス A またはクラス B のディジタル装置に対する FCC 要件に適合しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で修正するように求められることがあります。

注：この装置はテスト済みであり、FCC ルール Part 15 に規定されたクラス A ディジタル装置の制限に適合していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオ / テレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

クラス A に関する警告（カナダ）

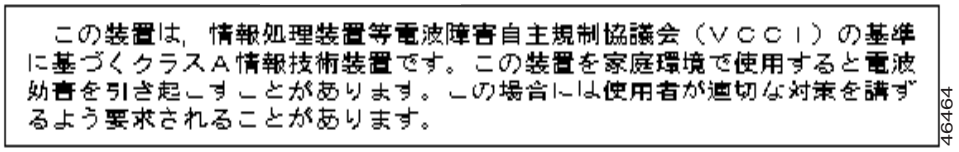
この装置は、Canadian ICES-003 に適合するクラス A ディジタル機器です。

Cet appareil numerique de la classe ‘A’ est conforme á la norme NMB-003 de Canada.

CISPR 22 クラス A に関する警告

この装置はクラス A 製品です。この装置を住宅地で使用した場合、ラジオ / テレビの受信障害が起こることがあります。その場合、ユーザが適切な防止措置を講じるように求められる場合があります。

VCCI クラス A に関する警告（日本）



BSMI クラス A に関する警告（台湾）

警告使用者　**這是甲類資訊產品，在居住環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。注意：產品的度量和檢驗標準局 (BSMI) 核准授權號碼在系統外殼的產品標籤上。**

この装置は、クラス A 製品です。この装置を住宅地で使用した場合、ラジオ / テレビの受信障害が起こることがあります。その場合には、ユーザが干渉防止措置を講じるよう求められる場合があります。

クラス A に関する警告（ハンガリー）

Figyelmeztetés a felhasználói kézikönyv számára: Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfeleloen kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelo kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelo speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.

この装置は、クラス A 製品であり、ハンガリーの EMC クラス A 要件（MSZ EN 55022）に従って適切に使用し、設置する必要があります。クラス A 装置は、設置と保護距離に対して特殊な条件が適用される、通常の商業環境用に作成されています。

Korean Class A Warning

주의 A급 기기 이 기기는 업무용으로 전자파 적합 등록을 한 기기이
오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약
잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

警告 **この装置はクラス A 製品であり、商業用の EMC 要件に登録されています。販売者または購入者はこのことに注意してください。このタイプの製品を誤って売却または購入した場合、家庭環境用タイプに交換する必要があります。**

安全上の警告

この項では、安全に関する警告について説明します。

インストール上の警告

警告　インストールに関する説明を読んでから、システムを電源に接続してください。

インストール上の警告

警告　訓練を受けた有資格の要員以外は、この機器の設置、交換、および保守は行わないでください。

TN 電源に関する警告

警告　この装置は、TN 電源系で動作するように設計されています。

電源切断に関する警告

警告　オン / オフ スイッチのあるシステムに対して作業するときは、事前に、電源を切り、電源コードを抜いてください。

サーキット ブレーカ（15A）に関する警告

警告　この製品は、ショート（過電流）保護をビルディング設備に依存しています。必ず、120 VAC、15A 以下（米国の場合）または、240VAC、10A 以下（米国以外の場合）のヒューズまたはサーキット ブレーカを電圧線（電流が流れる導体すべて）に挿入してください。

装置のアースに関する警告

警告　この装置は、アースすることになっています。ホストは、通常の使用時には、必ず接地してください。

安全カバーに関する説明

警告　安全カバーは、製品の重要な一部です。安全カバーを取り付けない状態で装置を操作しないでください。安全カバーを所定の位置に取り付けずに装置を操作した場合、安全性の保証が保たれず、火災および電気事故の危険が生じます。

前面プレートおよびカバー パネルに関する説明

警告　ブランク前面プレートおよびカバー パネルには、次の 3 つの重要な機能があります。シャーシ内の危険な電圧および電流に対する照射を防ぐ、ほかの装置に対して影響を及ぼすような電磁干渉（EMI）を防ぐ、シャーシ内の冷却空気の流れを確保する、の 3 つです。必ず、すべてのカード、前面プレート、前面カバー、および背面カバーが正しく取り付けられた状態でシステムを動作してください。

装身具に関する警告

警告　電源に接続されている装置に対して作業する場合は、事前に装身具（指輪、ネックレス、腕時計など）を外してください。このような金属製品が電圧がかかっている部分とアースに接触すると、金属が過熱して重度の火傷を負ったり、金属製品が端子に融着する恐れがあります。

雷に関する警告

警告　雷が発生しているときは、システムに対する作業や、ケーブルの脱着を行わないようにしてください。

SELV 回路に関する警告

警告　電気ショックを回避するため、SELV（安全低電圧）回路を TNV（電話ネットワーク電圧）回路に接続しないでください。LAN ポートには SELV 回路があり、WAN ポートには TNV 回路があります。LAN ポートおよび WAN ポートによっては、両方とも RJ-45 コネクタを使用する場合があります。ケーブルを接続する祭は、注意してください。

用語集

次に、Cisco IDS に関連する用語を解説します。

数字

3DES Triple Data Encryption Standard の略。SSH v.1 のデフォルトの暗号化方式であった DES をより強化したバージョンです。

A

AAA 認証、許可、アカウンティング（authentication, authorization, and accounting）。ユーザがルータまたは PIX Firewall にログインする方法を制御する Cisco IOS ソフトウェアおよび PIX Firewall のコマンドです。

ACE アクセス コントロール エントリ。指定されたアドレスまたはプロトコルに対して実行するアクションを記述する ACL のエントリです。

ACK あるネットワーク デバイスからほかのネットワークデバイスへ送信される、イベントの発生（たとえば、メッセージの受信）を確認する通知。

ACL アクセス コントロール リスト。サービスへのアクセスおよびアクセス拒否を制御する手段です。リストには、利用可能なサービスと、そのサービスの使用が許可されているホストが列挙されています。

アクティブ ACL Device Management（*managed*）によって作成および保守されている ACL で、ルータ ブロック インターフェイスに適用されます。

アラーム 現在ネットワークで行われている不正利用または潜在的なセキュリティ問題の発生を通知するために、内部的に使用される IDS メッセージです。

攻撃 技術的な脅威から派生する、システム セキュリティに対する攻撃。たとえば、巧妙な手段で故意に（特に手法や技術を駆使して）セキュリティ サービスを回避したり、システムのセキュリティ ポリシーに違反したりする行為を指します。

認証 ユーザを識別する方式を提供します。ログインダイアログとパスワードダイアログ、チャレンジとレスポンス、メッセージ処理サポート、暗号化等が含まれます。

B

良性トリガー シグニチャが正しく発行され、トラフィックが悪性ではない状況。

ブロッキング ネットワーク デバイスを使用して特定のネットワーク ホスト またはネットワーク全体へのエントリを拒否する Sensor の機能。「シャニング」を参照。

C

CA 認証局。デジタル認証（特に X.509 認証）を発行し、証明書内のデータ項目との間の拘束力を保証するエンティティです。

CA 証明書 ある CA がその他の CA に発行した証明書。

C & C Command & Control（コマンドと制御）。Sensor 上のネットワーク インターフェイスを通して管理されます。

暗号キー 暗号化キーの値。Data Encryption Standard（DES）での有効な暗号化キーは、16 バイトの 16 進数値です。

CiscoFusion 最新のルーティング技術によるスケーラビリティ、安定性、セキュリティの利点を、ATM および LAN スイッチングのパフォーマンスや VLAN による管理の利点と融合（fuse）する、シスコのインターネットワーキング アーキテクチャ。「Cisco IOS ソフトウェア」を参照。

Cisco IOS ソフトウェア Cisco Internetworking Operating System。アーキテクチャに基づくすべての製品に共通の機能性、スケーラビリティ、セキュリティを提供する Cisco Systems のソフトウェアです。Cisco IOS ソフトウェアでは、広範なプロトコル、メディア、サービス、プラットフォームのサポートを保証しながら、インターネットワークのインストールと管理についての集中化、自動化を実現しています。「CiscoFusion」を参照。

Cisco Secure Policy Manager Cisco Secure Policy Manager は、スケーラブルで包括的なセキュリティ ポリシー管理システムです。

構成管理 Configuration Management は、Sensor の設定をリモートで管理する IDS マネージャーの機能です。この機能を使用すると、ネットワーク セキュリティ担当者は、企業全体に配置されている Sensor をすべて集中して管理できます。

制御インターフェイス Device Management（*managed*）が Telnet または SSH セッションをネットワーク ルーティング デバイスとで開く場合、そのデバイスのいずれかのルーティング インターフェイスをリモート IP アドレスとして使用します。これが制御インターフェイスです。

カウンターメジャー（対抗手段） ネットワークにおける脅威、脆弱性、および攻撃を減少させるアクション、デバイス、プロシージャ、または技術を言います。脅威、脆弱性などを排除および妨害したり、発生する可能性を最小限にしたり、訂正アクションを実行できるように発見、報告したりします。

D

デーモン / サービス デーモンまたはサービスは、特有の機能、たとえばログ ファイルの記述、IP トラフィックの分析、またはイベントの処理を実行します。

DES Data Encryption Standard の略。アルゴリズムよりも 56 ビット キーに強度がある、強力な暗号化方式。

デバイス管理 Device Management は、ネットワーク デバイスと対話するための Sensor の機能です。たとえば、ルータの ACL を動的に再構成して攻撃者をブロックできます。Device Management は *managed* サービスによって制御されます。

Director Director は、UNIX ベースの IDS マネージャーです。1 つの Director で Sensor をまとめて管理および監視できるので、セキュリティ担当者は、中央コンソールからネットワークのセキュリティを確保することができます。

DNS Domain Name System の略。IP アドレスをマッピングするインターネット規模のホスト名です。DNS を利用すると、人間が読み取り可能な名前を、ネットワーク パケットに必要な IP アドレスに変換できます。

DoS Denial of Service（サービス拒絶）。DoS 攻撃は、特定のシステムまたはネットワークを使用不能にすることが目的の攻撃です。

E

暗号化 特殊なアルゴリズムのアプリケーションで、データを理解できない表示にし、権限がなければ情報を参照できないようにします。

エンジン ある 1 つのカテゴリで多数のシグニチャをサポートするように設計された Sensor のコンポーネント。各エンジンには、シグニチャの作成や既存のシグニチャのチューニングに使用できるパラメータがあります。

エンタープライズ ネットワーク 企業などの組織において主要なポイントをほぼ接続する、大規模で多様なネットワーク。WAN とは異なり、私的に所有および維持されます。

F

false negative 不正なトラフィックが検出されたときにシグニチャが発行されない状況。

false positive シグニチャが不適切に発行される状況。

フィルタリング ルータ セキュリティ ポリシーに従ってデータ パケットの通過を選択的に妨げるインターネットワーク ルータ。

ファイアウォール ネットワーク境界を保護するセキュリティ デバイス。

フラグメンテーション IP フラグメンテーションは、単一の IP パケットを複数のセグメントに分割し、すべてネットワークの最大伝送サイズより小さいサイズにします。

H

HTTP Hypertext Transfer Protocol の略。Web サイトで Web ユーザへの情報の搬送に使用される標準プロトコル。デフォルトでは TCP ポート 80 が使用されます。

HTTPS 標準 HTTP プロトコルの拡張機能で、Web サイトからのトラフィックを暗号化し、機密性を提供します。このプロトコルは、デフォルトでは TCP ポート 443 を使用します。

I

ICMP Internet Control Message Protocol の略。エラーの報告や IP パケット処理に関連する情報の提供を行う、ネットワーク層のインターネット プロトコル。RFC 792 に記載されています。

IETF インターネット技術特別調査委員会（Internet Engineering Task Force）。インターネット基準の開発を担う 80 の作業グループで構成されています。IETF は ISOC の賛助により機能しています。

侵入検知 システムのイベントを監視および分析するセキュリティ サービスです。未許可の方法でのシステム リソースへのアクセスを、リアルタイムまたはほぼリアルタイムで発見して妨ぎます。

Intrusion Detection Planning Guide 侵入検知テクノロジーについて説明し、ネットワーク展開の基本的な設計計画とシナリオについて紹介しているマニュアルです。

IDM Intrusion Detection System Device Manager の略。Sensor の Web ベースのデバイス マネージャー。IDM は基本構成および管理機能を提供します。

IDS MC Management Center for IDS Sensors の略。Web ベースの IDS マネージャーは Sensor の構成を 300 まで管理できます。

IDV Intrusion Detection System Device Viewer の略。IDV は、Web ベースの IDM を補完する基本的なモニタリングおよびレポート機能を提供します。

IP アドレス TCP/IP を使用するホストに割り当てられる 32 ビットのアドレス。IP アドレスは 5 つのクラス（A、B、C、D、または E）のいずれかに属し、ピリオドで区切られた 4 オクテット（ドット付き 10 進形式）で表します。各アドレスはネットワーク番号とサブネットワーク番号（オプション）およびホスト番号から成ります。ネットワーク番号とサブネットワーク番号は、どちらもルーティングに使用されます。ホスト番号は、ネットワークまたはサブネットワーク内にある個々のホストのアドレスに使用されます。サブネット マスクは、ネットワークおよびサブネットワークの情報を IP アドレスから抽出します。

IPSec IP Security Protocol の略。データの機密性、データの整合性、およびデータの認証を提供する、公開規格のフレームワークです。IPSec は、これらのセキュリティ サービスを IP 層で提供します。IPSec は IKE を使用して、プロトコルおよびアルゴリズムのネゴシエーションをローカル ポリシーに基づいて処理し、IPSec で使用する暗号化キーおよび認証キーを生成します。IPSec は、2 つのホスト間、2 つのセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護します。

IP スプーフィング IP スプーフィング攻撃は、ネットワークの外にいる攻撃者が信頼されているユーザになりすます場合に発生します。その方法として、ネットワークの IP アドレス範囲内の IP アドレスの使用や、ネットワーク内の特定のリソースへのアクセスを提供する、信頼されていて許可のある外部の IP アドレスの使用があります。IPSec セキュリティ パラメータへのアクセスを獲得した攻撃者は、企業ネットワークへの接続を許可されているリモート ユーザを装うことができます。

ISOC インターネット学会。1992 年に設立された、インターネットの発展とその利用についての活動を行う国際的非営利団体。ISOC は IAB などの関連の下部機関に権限を委任しています。本部は米国バージニア州のレストンです。

L

ロギング セキュリティ情報のロギングは、2 つのレベルで実行されます。イベントのロギング（たとえば、IDS コマンド、エラー、およびアラーム）、および個々の IP セッション情報のロギングです。

M

マネージャー IDS Sensor を管理するノード（たとえば、IDS Director、CSPM、IDM、または IDS MC）を言います。

managed ネットワーク デバイス（ルータおよびパケット フィルタ）の管理およびモニタリングを行うサービス。

MTU 最大伝送ユニット。ネットワーク セグメントが処理できる最大パケットサイズを表します。パケットが MTU よりも大きい場合、送信ホストはパケットを複数フレームに分割してからネットワークを介して送信し、宛先ホストでフレームが再構成されます。

N

ネットワーク デバイス ルータ またはパケット フィルタ。特に Sensor とともに機能して未認証の接続をブロックまたは切断するものを指します。

nrConfigure IDS Director で使用される、リモート Sensor の構成管理を集中化する Java ベースのツール。

NSDB Network Security Database の略。IDS が使用するシグニチャと、そのシグニチャに基づく脆弱性を示すセキュリティ情報のデータベースです。

P

packetd 侵入検知を行うサービス。「*packetd*」は Sensor 自体がネットワークから直接パケットを取得している場合に使用されます。

PIX Firewall Private Internet Exchange Firewall の略。ネットワーク間のアドレスまたはポートについて、許可または拒否する機能がプログラムされている シスコのネットワーク セキュリティ デバイスです。

postoffice ネットワークを介して IDS サービス間の通信を維持する専用プロトコル。

R

正規表現 ストリームまたはファイルにある、指定した文字シーケンスの検索方法を定義できるメカニズム。

RPC リモート プロシージャ コール。クライアント / サーバ コンピューティングの基礎となった技術です。RPC はクライアントによって構築または指定されたプロシージャ コールで、サーバ上で実行され、結果はネットワークを経由してクライアントに返されます。

RSA 技術の提唱者である Rivest、Shamir、Adelman の各氏の頭文字を取った略語。暗号化と認証に使用される公開キー暗号化システムです。

S

SA セキュリティ結合。データ フローに適用されるセキュリティ ポリシーおよびキーイング情報のインスタンスです。

Security Monitor セキュリティの Monitoring Center。ネットワーク デバイスのイベント収集、表示、報告を行います。IDS MC と使用されます。

Sensor Sensor は侵入検出エンジンです。ネットワークのトラフィックを分析し、不正行為の徴候を探索します。

Sensor の忠実度 Sensor の高い忠実度が達成されるのは、false positive または false negative を示さずに、true positive および true negative、および最小限の良性トリガーを示す場合です。忠実度を達成するには、シグニチャのしきい値のチューニングが必要です。

シャニング ネットワーク デバイスを使用して、特定のネットワーク ホストまたはネットワーク全体への侵入を拒否する Sensor の機能。「ブロッキング」を参照。

シグニチャ シグニチャは、ネットワーク情報を抽出し、一般的な侵入アクティビティを定義したルール セットとその情報を比較します。

シグニチャ インスペクタ 既知のシグニチャの集約トラフィックを検査するサブシステム。

SPAN Switched Port Analyzer。Catalyst 5000 スイッチの機能で、既存のネットワーク アナライザの監視機能を、スイッチド イーサネット環境にまで拡張します。SPAN は、1 つのスイッチ対象セグメントを、事前に定義された SPAN ポートにミラーリングします。SPAN に接続されたネットワーク アナライザは、任意の Catalyst スイッチド ポートからのトラフィックを監視することができます。

SPI Security Parameter Index の略。受信側の SA を一意に識別するために使用される 32 ビット エンティティです。値の範囲は 0x100 ～ 0xffff ffff（数値）です。

SSH Secure Shell の略。リモート セキュア C & C インターフェイスを提供するユーティリティです。リモート ユーザを Sensor にネットワーク接続するための平文のユーザ名やパスワードを表示することなく Sensor が構成できます。

SSL Secure Socket Layer。電子商取引におけるクレジット カード番号の送信など、安全なトランザクションの実現に使用される Web の暗号化技術です。

サブシグニチャ 一般的なシグニチャよりも細分化されたシグニチャ。通常は、さらに広いスコープのシグニチャを定義します。

sysconfig-sensor Sensor を初期化し、Sensor と IDS Manager 間の通信を設定するために使用されるプログラム。

SYN フラッド プロトコル実装の処理量を超える大量の TCP SYN パケット（同期化シーケンス番号を要求、接続を開始するときに使用する）をホストに送信する DoS 攻撃。

T

TACACS Terminal Access Controller Access Control System の略。DDN コミュニティによって開発された認証プロトコルです。リモート アクセスのための認証およびイベント ロギングのような関連サービスを可能にします。ユーザ パスワードを個々のルータではなく中央データベースにおいて管理することで、ネットワークセキュリティに関する簡便でスケーラブルなソリューションを提供します。

TACACS+ Terminal Access Controller Access Control System Plus の略。TACACS に対するシスコ独自の拡張版。認証、許可、アカウンティングなどのサポート機能が追加されています。

TCP Transmission Control Protocol。コネクション型のトランスポート層プロトコル。信頼性の高い全二重データ転送を提供します。TCP は TCP/IP プロトコル スタックの一部です。

Telnet TCP/IP プロトコル スタックの標準的なターミナル エミュレーション プロトコル。ユーザはネットワークを介して遠隔地のホストにログインし、自分のデスク上のマシンを操作するようにそのホストを操作することができます。Telnet は RFC 854 で定義されています。

しきい値 アラームを送信するまでの最大 / 最小の許容条件を定義する上限または下限の値。

TLS Transport Layer Security の略。SSL に次ぐ将来の IETF プロトコル。

トラフィック分析 データ フローの特性を観察して得られる情報を推察すること。データが暗号化されていたり、直接にはアクセスできない場合にも実行することができます。取得される特性には、送信元および送信先の ID とロケーション、およびトラフィック発生の有無、トラフィック量、発生頻度が含まれます。

true negative 不正なトラフィックが検出されたときにシグニチャが発行されない状況。

true positive 不正なトラフィックが検出されたときにシグニチャが適切に発行される状況。

U

UDP User Datagram Protocol。TCP/IP スタックに含まれるコネクションレス型のトランスポート層プロトコル。UDP は確認応答あるいは配送保証なしにデータグラムを交換するシンプルなプロトコルで、エラー処理および再転送はほかのプロトコルによって行う必要があります。UDP は RFC 768 で定義されています。

V

VACL VLAN ACL の略。スイッチを通過するすべてのパケット（VLAN 内 と VLAN 間の両方）をフィルタにかける ACL。Security ACL としても知られています。

VLAN 仮想 LAN。LAN を、異なるブロードキャスト ドメインに、論理的に分割したグループです。

脆弱性 コンピュータまたはネットワークのアトリビュートで、それがあるために、何かを原因としてコンピュータまたはネットワークでさまざまな形の誤動作が起きることを言います。

関連マニュアル

Cisco Intrusion Detection System に関する追加情報については、次の Web サイトで次のマニュアルを参照してください。

- *Cisco Intrusion Detection System Sensor Configuration Note Version 3,0*
  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids6/index.htm
- *Release Notes for Cisco Intrusion Detection System Sensor Version 3.0(1)S4*
  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids6/index.htm
- *Cisco Intrusion Detection System Director for UNIX Configuration and Operations Guide Version 2.2.3*
  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids7/index.htm
- *Release Notes for Cisco Intrusion Detection System Director for UNIX Version 2.2.3*
  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids7/index.htm
- *Cisco Secure Intrusion Detection System Internal Architecture*
  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/0866_02.htm
- *Intrusion Detection Planning Guide*
  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/index.htm

マニュアルの入手

シスコからマニュアルを入手する方法について紹介します。

World Wide Web

最新のマニュアルは World Wide Web の次の URL で参照いただけます。

http://www.cisco.com

翻訳版は、次の URL で入手できます。

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

シスコのマニュアルおよびその他の資料は、製品に付属している Cisco Documentation CD-ROM パッケージでご利用いただけます。Documentation CD-ROM は毎月更新されるので、印刷資料よりも新しい情報が得られます。この CD-ROM パッケージは、1 つのパッケージごとでも年間契約という形でもご利用いただけます。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると妨害電波を引き起こすことがあります。この場合には使用者が適切な対応を講ずるよう要求されることがあります。

このマニュアルは、「関連マニュアル」でリストされているマニュアルと併せて使用してください。

CCIP、Cisco Arrow のロゴ、Cisco Powered Network のマーク、Cisco Systems Verified のロゴ、Cisco Unity、Follow Me Browsing、FormShare、Internet Quotient、iQ Breakthrough、iQ Expertise、iQ FastTrack、iQ のロゴ、iQ Net Readiness Scorecard、Networking Academy、ScriptShare、SMARTnet、TransPath、および Voice LAN は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、Discover All That's Possible、The Fastest Way to Increase Your Internet Quotient、および iQuick Study は、Cisco Systems, Inc. のサービス マークです。Aironet、ASIST、BPX、Catalyst、CCDA、CCDP、CCIE、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco IOS のロゴ、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Empowering the Internet Generation、Enterprise/Solver、EtherChannel、EtherSwitch、Fast Step、GigaStack、IOS、IP/TV、LightStream、MGX、MICA、Networkers のロゴ、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、RateMUX、Registrar、SlideCast、StrataView Plus、Stratm、SwitchProbe、TeleRouter、および VCO は、米国および一部の国における Cisco Systems, Inc. または関連会社の登録商標です。

このマニュアルまたは Web サイトで言及されているその他の商標はすべて、それぞれの所有者のものです。「パートナー」という語の使用は、シスコシステムズと他社との提携関係を意味するものではありません。（0206R）

Copyright © 2002, Cisco Systems, Inc.
All rights reserved.

お問い合わせは、購入された各代理店へご連絡ください。

シスコシステムズでは以下のURLで最新の日本語マニュアルを公開しております。
本書とあわせてご利用下さい。

Cisco Connection Online Japan
http://www.cisco.com/japanese/manuals/

日本語マニュアルの購入を希望される方は、以下のURLからお申し込みいただけます。

シスコシステムズマニュアルセンター
http://www2.hipri.com/cisco/

上記の両サイトで、日本語マニュアルの記述内容に関するご意見もお受けいたしますので、
どうぞご利用下さい。

なお、技術内容に関するご質問は、製品を購入された各代理店へお問い合せください。

Copyright © 2002, Cisco Systems Inc.

CISCO SYSTEMS

シスコシステムズ株式会社
URL:http://www.cisco.com/jp/
問合せ URL:http://www.cisco.com/jp/service/contactcenter/
〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL.03-5549-6500　FAX.03-5549-6501

DOC-J-787016=
78-7016-04-J