

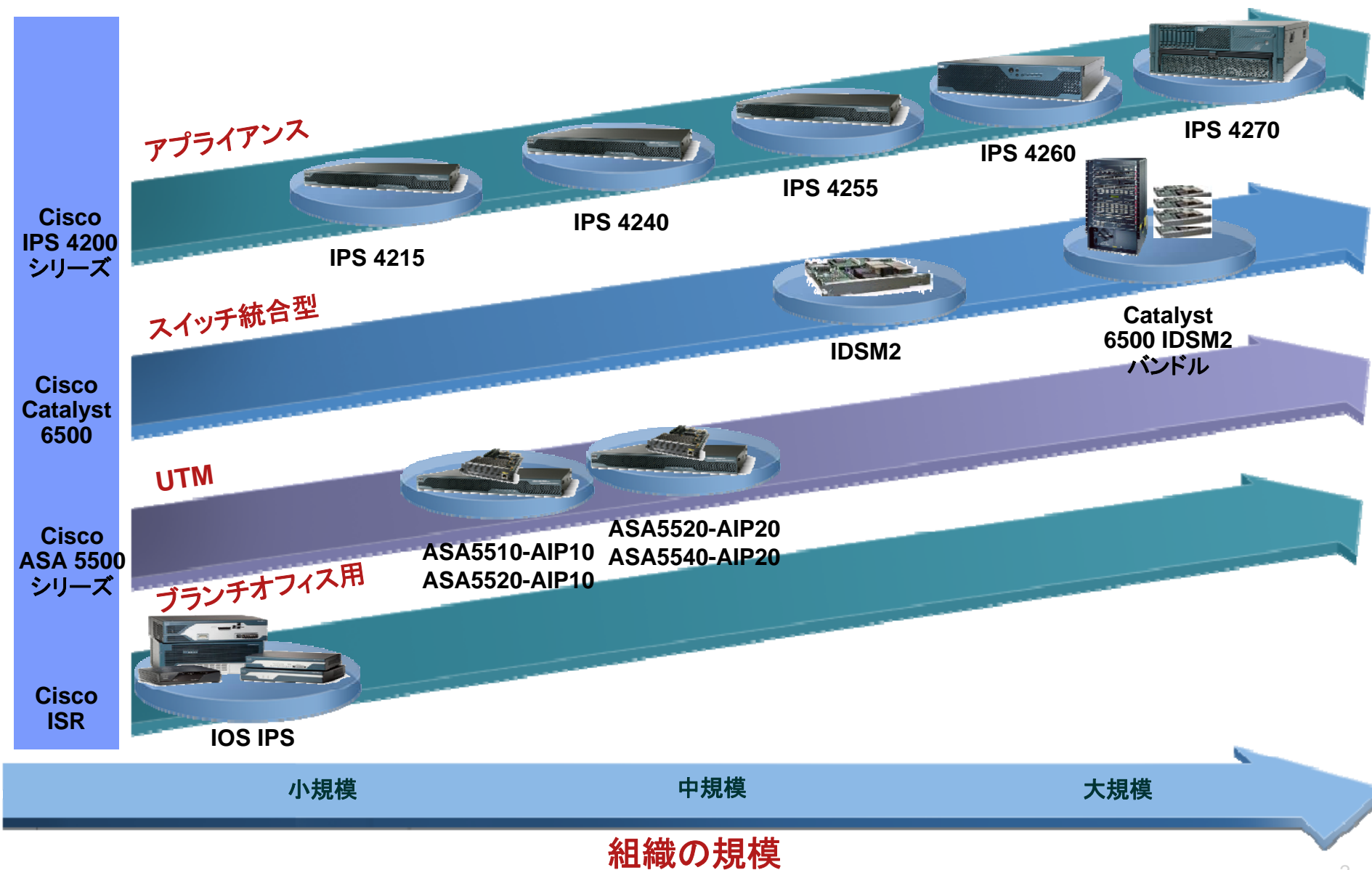


# Cisco IPS 4270による マルチギガビット侵入防御サービス



**Oct. 2007**

# Cisco IPS プロダクトラインナップ



# ヒューマン ネットワークを加速するパフォーマンスを

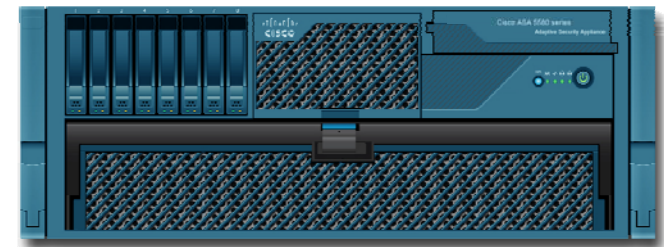


# New Cisco IPS 4270-20 センサー

## 妥協のないパフォーマンス

### プロダクトハイライト:

- 最大 4-Gbps のパフォーマンス
  - 4 Gbps (メディアリッチ環境)
  - 2 Gbps (高トランザクション環境)
- 最大16 のGigabit Ethernetインターフェイス (銅線 および 光ファイバ)
- 最大 4 つの 10 Gigabit Ethernet インターフェイスへの対応を予定
- 数千の論理インターフェイスをサポート
- ホットスワップ可能な冗長化電源
- IPS Device Manager によるGUI上でのデバイス管理 (IDM/IEV)
- Cisco Security Manager and Cisco® Security MARS による複数デバイス管理



# IPS-4270の利用環境

アプリケーションとコンテンツの環境に応じた高速サービスの提供

## メディアリッチ環境

ビデオコンテンツ  
高解像度イメージ  
Webでのマルチメディア  
など、大容量データ環境で

最大4Gbpsの処理性能



## 高トランザクション環境

受発注システム  
在庫管理システム  
トレーディングシステム  
など、トランザクションレート  
の高い環境においても

2万transaction/Sec  
2Gbpsの処理性能



## 次世代データセンター

高速インターフェイス対応  
VLANトランクIF対応  
IPS/IDS両モードに対応  
仮想IPSで複数ポリシー  
管理に対応



# シスコIPSによるマルチベクタの脅威認識

## 広範囲なアタックと、マルウェアの通信に対抗が可能

### スパイウェア／アドウェア

- マルウェアのインストール防止および、外部への二次攻撃の回避
- ネットワーク帯域の開放
- Winnyなどの許可されないプログラムによる、機密データ漏えいの防止

### ネットワークワーム & ウイルス

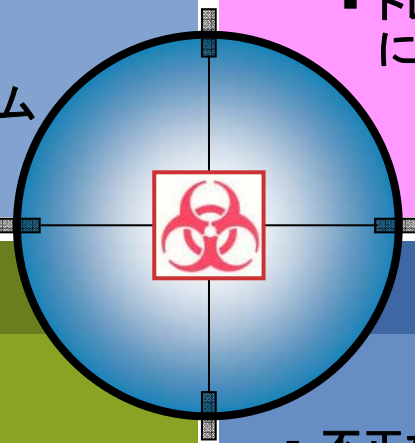
- 感染の防止とマルウェア配信の防止
- トレンドマイクロ社とのパートナーシップによる開発体制

### 直接攻撃

- 社内スパイ活動の監視、抑制
- Webアタックによるサイト改ざんの防止
- ゾンビ、バックドア、ボットによるネットワーク停止攻撃(DoSアタック)の防止

### トラフィック クリーニング

- 不正なトラフィック(TPCセグメントやフラグメントの上書き、矛盾したTTLなど)の排除
- エンドホストの挙動のシミュレートによる検知精度の向上



# Cisco IPSの特徴

## ■ インテリジェントな検知

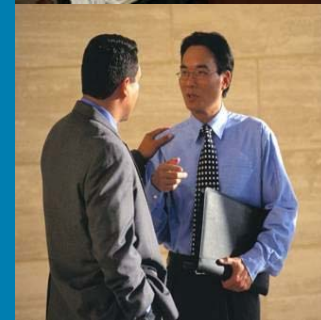
様々な脆弱性および攻撃法に対応したシグネチャ  
トラフィックとプロトコル アノーマリの検知と学習  
ヒューリスティック検知 (統計ベースのアルゴリズム)

## ■ 検知精度の向上

複数要素のリスク率の複合分析によるポリシー適用  
メタ イベント ジェネレータによる複数イベントの関連付け  
収集したエンドポイントの属性、信頼性情報を反映

## ■ 柔軟な導入

パッシブ (IDS) / インライン (IPS) での動作  
センサー ポリシーの仮想化  
物理 / 論理インターフェイスのサポート



# Cisco IPS インテリジェントな検出機能:

## 脆弱性、攻撃手法に対応したシグネチャ

### アドウェア／スパイウェア

- Perfect Keylogger Activity
- Hotbar Activity

### DDoS/DoS

- ICMP/UDP/TCP Floods

### セキュア Voice

- SIP
- H323
- H225

### Web サーバ

- Apache
- Internet Information Server (IIS)

### ネットワーク攻撃 (L2/3/4)

- BGP
- DHCP
- DNS
- TCP/UDP
- IP
- IP Fragment

### ワーム／ウイルス／トロイの木馬

- Blaster
- Nimda
- Sasser
- Code Red
- Slammer
- Backdoor Frenzy
- Backdoor Beast
- Backdoor Ghost
- Backdoor Illusion
- Backdoor Trojan Spirit
- Backdoor Beast
- Fatso Worm
- Kelvir Worm



### P2P/IM

- AIM/ICQ
- AOL
- MSN
- Sametime
- Yahoo
- BitTorrent
- Kazaa
- eDonkey
- Jabber
- Winny

### 偵察

- ICMP host sweeps
- TCP Port Sweeps
- TCP/UDP Combo Sweeps
- UDP Port Sweeps

### Email

- POP
- IMAP
- SMTP
- Microsoft Exchange

