

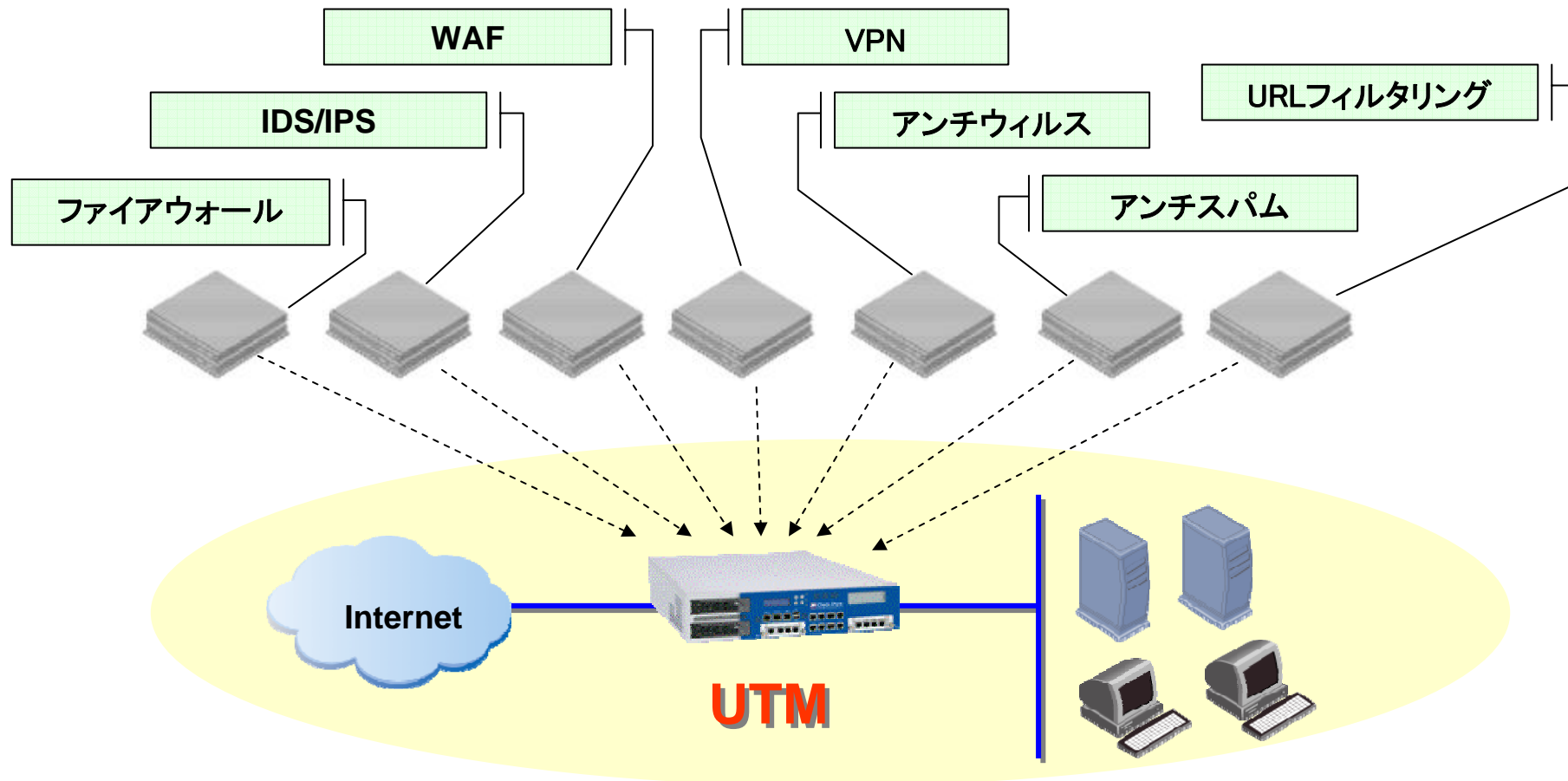


Check Point  
SOFTWARE TECHNOLOGIES LTD.

# 統合脅威管理(UTM)再考 - 導入効果を最大化する要件とは? -

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社  
北村 正義

UTM (Unified Threat Management)とは統合脅威管理と呼ばれ、一般的には以下のようなセキュリティ対策機能が**少なくとも2つ以上**統合されたソリューションを示します



現在は1つのセキュリティベンダーが1つのセキュリティ機能を提供する事は少なく、1つのセキュリティベンダーが複数のセキュリティ機能を持った製品をリリースしている

Check Point

Cisco

Juniper

Fortinet

SonicWall



MacAfee

Symantec

Trend Micro

Blue Coat

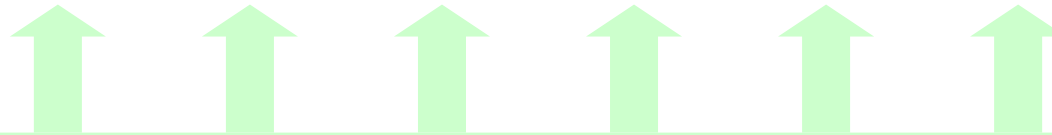
F5

また、この傾向はゲートウェイ製品だけではなく、エンドポイント製品も同様

セキュリティ技術のOEM化なども進み、違いは出身の違いだけのようにも見える

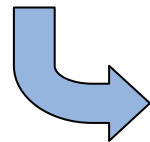
## UTMが求められる背景

次々と生まれる新たなセキュリティの脅威



都度個別にセキュリティ対策を構築

- ・ 導入コスト増大
- ・ 運用コスト増大
- ・ 導入した製品同士での競合



専門の知識を持った管理者を継続的に確保出来ない企業にとっては、次々と対策を講じる必要のあるセキュリティ対策を効率良く一元的に管理することが出来ない。

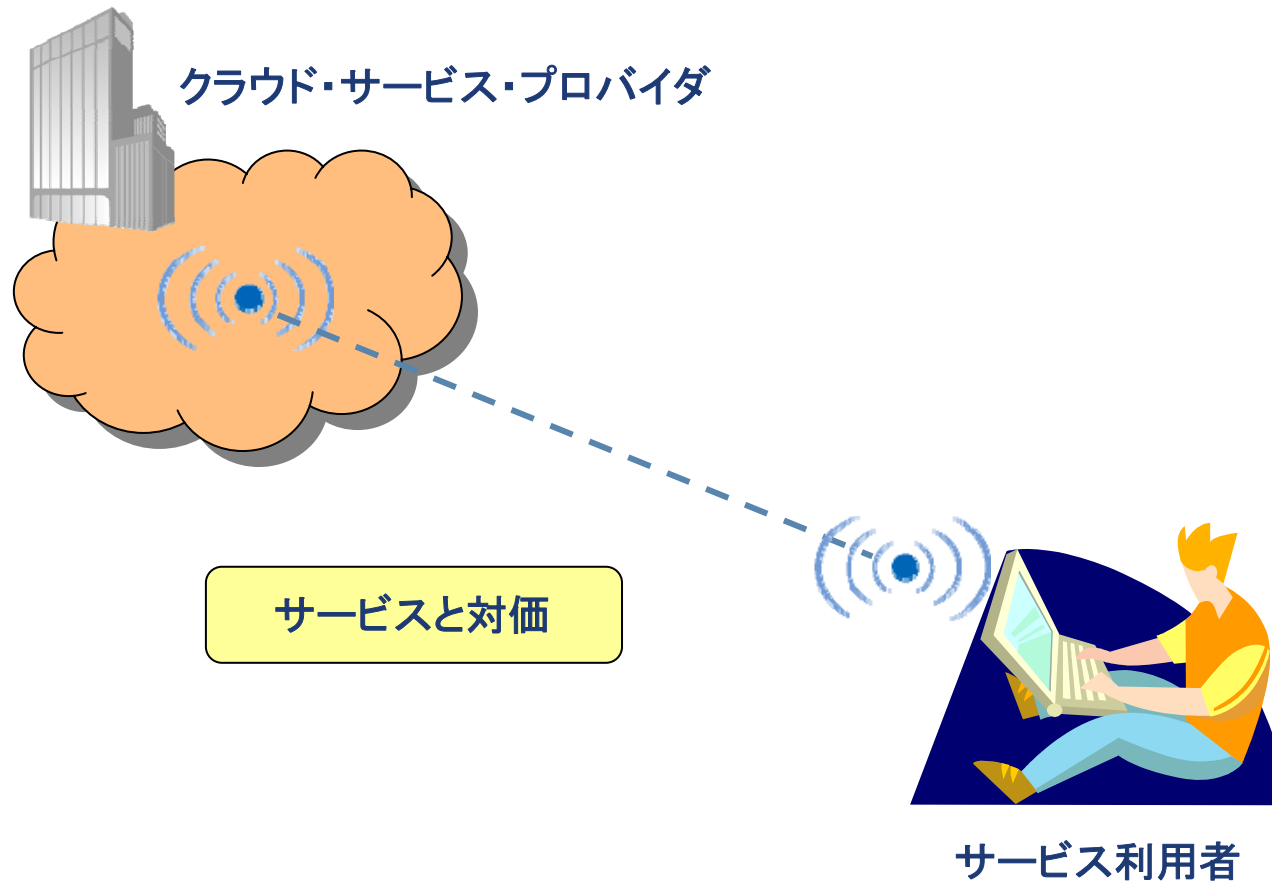
- UTMのメリット = オールインワンであること

- ◎ 対策分野ごとにセキュリティ・ソリューションを選定する必要がない
- ◎ ハードウェア(場合によってはソフトウェア)投資の節約
- ◎ 容易な導入と運用
- ◎ ひとつの窓口にて提供されるサポート



小中規模のマーケットに対して最適なソリューション

クラウドコンピューティングとは、ユーザがコンピュータ処理に必要な機能を必要に応じてネットワーク(通常はインターネット)を通じてサービスとして利用する形態のこと。



- クラウドコンピューティングのメリット = コスト効果が高く、容易であること

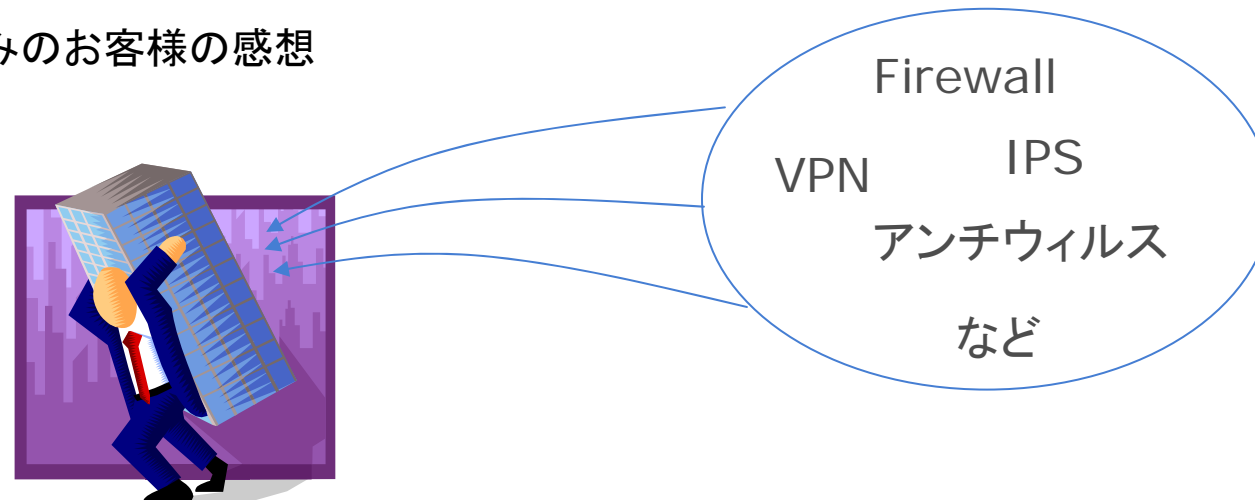
利用者側から見た場合

- ◎ 容易な導入
- ◎ 情報システムに対するコスト削減
- ◎ 高機能化、肥大化するシステムに専門の構築知識や運用知識を必要としない



小中規模のマーケットでは利用価値が高い

## UTM製品を導入済みのお客様の感想



- ・ UTMは便利だと思う(思ったけど)マシンに負荷がかかりすぎる
- ・ 1つ1つの機能が弱いように感じる
- ・ 管理機能が複雑で意図した機能を利用できない

結局、UTMとして購入したはずなのに

**特定のセキュリティ機能の専用機**

として使用するとといった状況を生み出している。

1. 導入機能の整理

2. 統合性、操作性

3. パフォーマンス

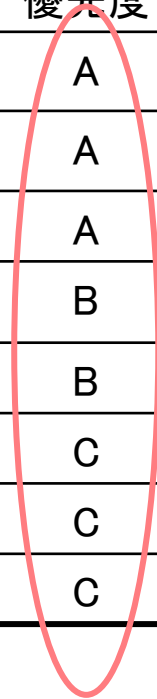
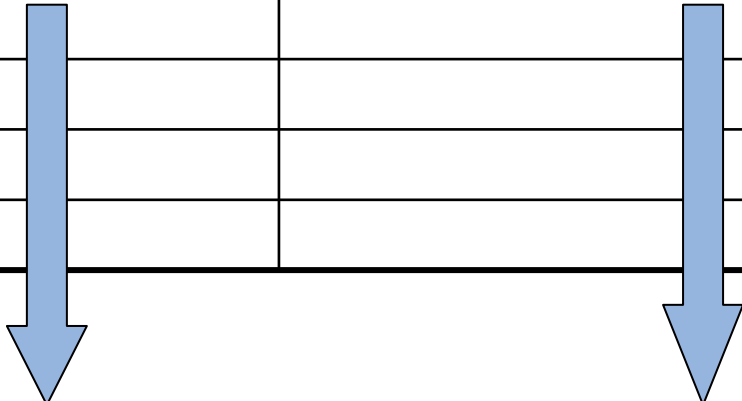
4. コスト



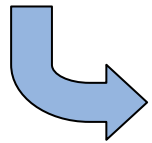
# 1. 導入機能の整理

- 具体的にどの機能を統合したいのか
- 使用機能の優先付け

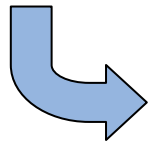
導入機能	現状	優先度
ファイアウォール	導入済み(XXXX社、xx年xx月保守終了予定)	A
IDS/IPS	導入済み(XXXX社)	A
サイト間 VPN	導入済み(XXXX社)	A
GWアンチウィルス	導入していない	B
		B
		C
		C
		C



## 比較のポイントの明確化

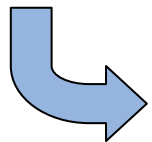


製品選定プロセスの簡略化



販売元の強みの見極め

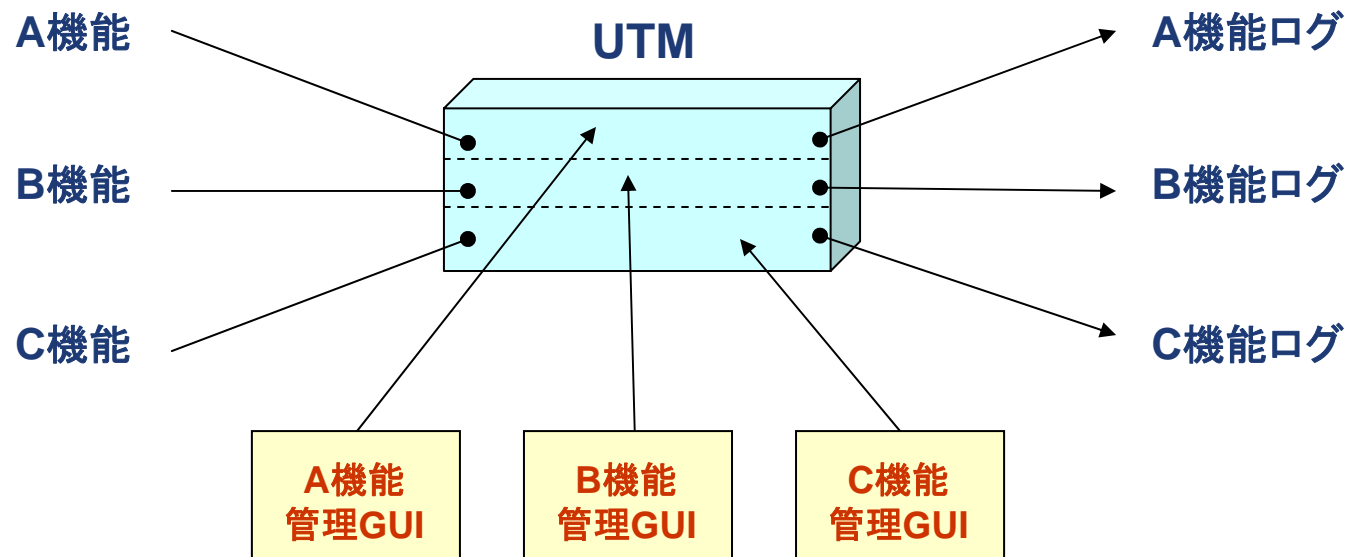
UTMの各機能については、OEMなどにより、その分野における最高レベルのセキュリティ機能を使っている可能性はあるが、サポートなどソフト面での対応には差が出る可能性はある



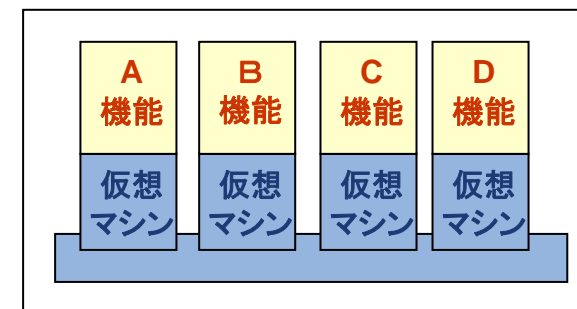
複数年での使用を考えた場合、パフォーマンスと機能の引き換えが発生する可能性も想定

## 2. 統合性、操作性

- 管理機能や出力されるログデータはどこまで統合されているか
- 必要とされる機能とその操作性は充分か



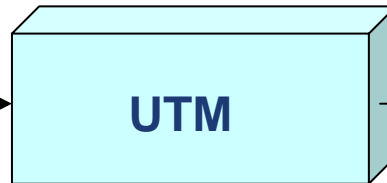
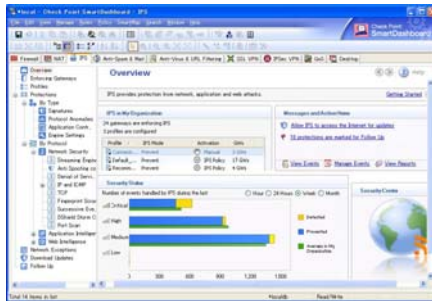
これはUTMというより仮想化システム？



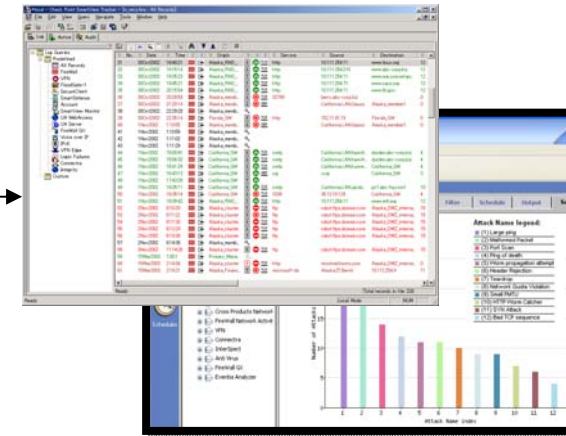
# UTMとして購入するメリットはあるか？

管理やログ機能などが統合出来ていないUTM製品を利用した場合、容易な運用というUTMの大きなメリットが失われます。  
運用負荷の軽減までを含めたUTM導入のメリットは薄れてしまうため、統合性の確認が必要です。

## 統合インターフェース



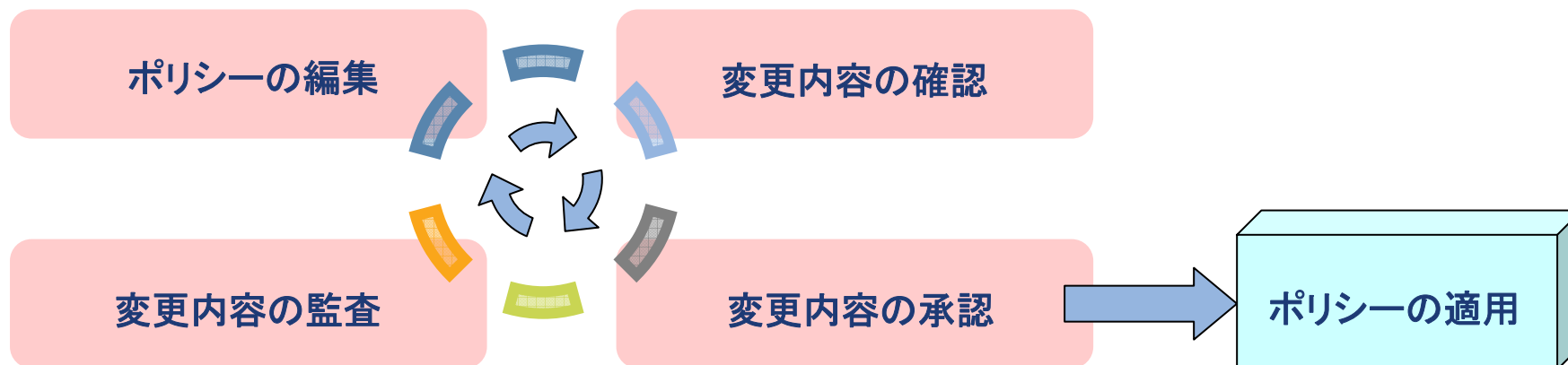
## 統合ログやレポート



統合性、操作性(見え方や使い安さ)を確認

## Check Pointのポリシー変更管理機能「SmartWorkflow Blade」

### SmartWorkflow機能のライフサイクル



リスクの緩和



可視化とコントロール

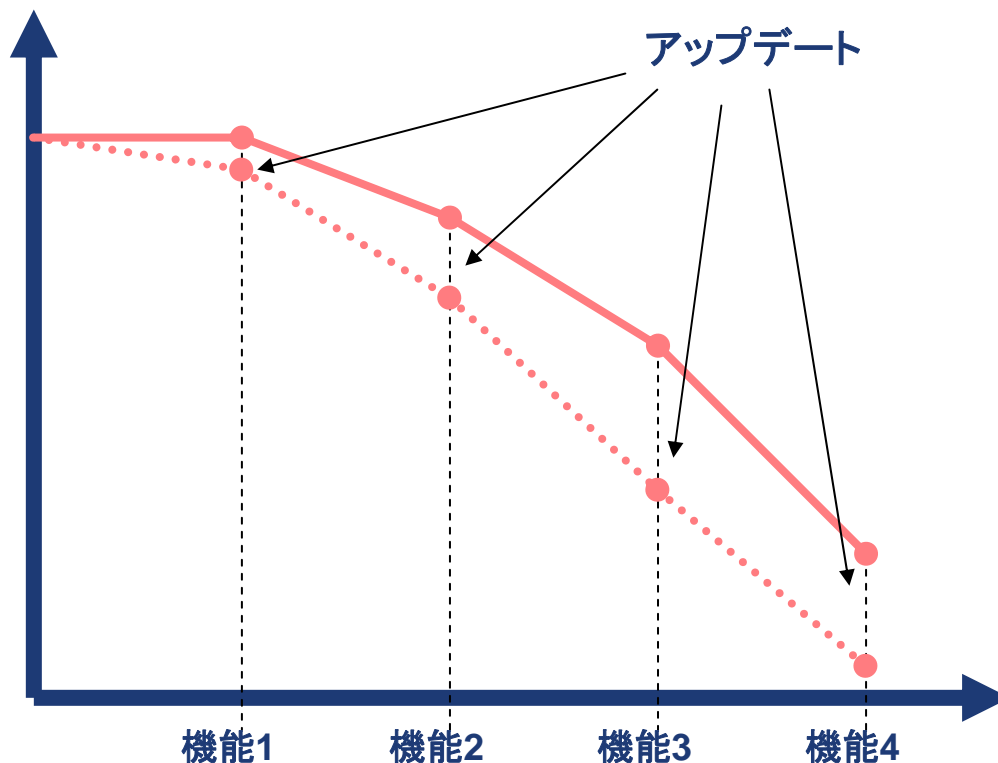


コンプライアンス



### 3. パフォーマンス

- 現在必要なパフォーマンス、将来必要なパフォーマンス
- パフォーマンス・アーキテクチャ



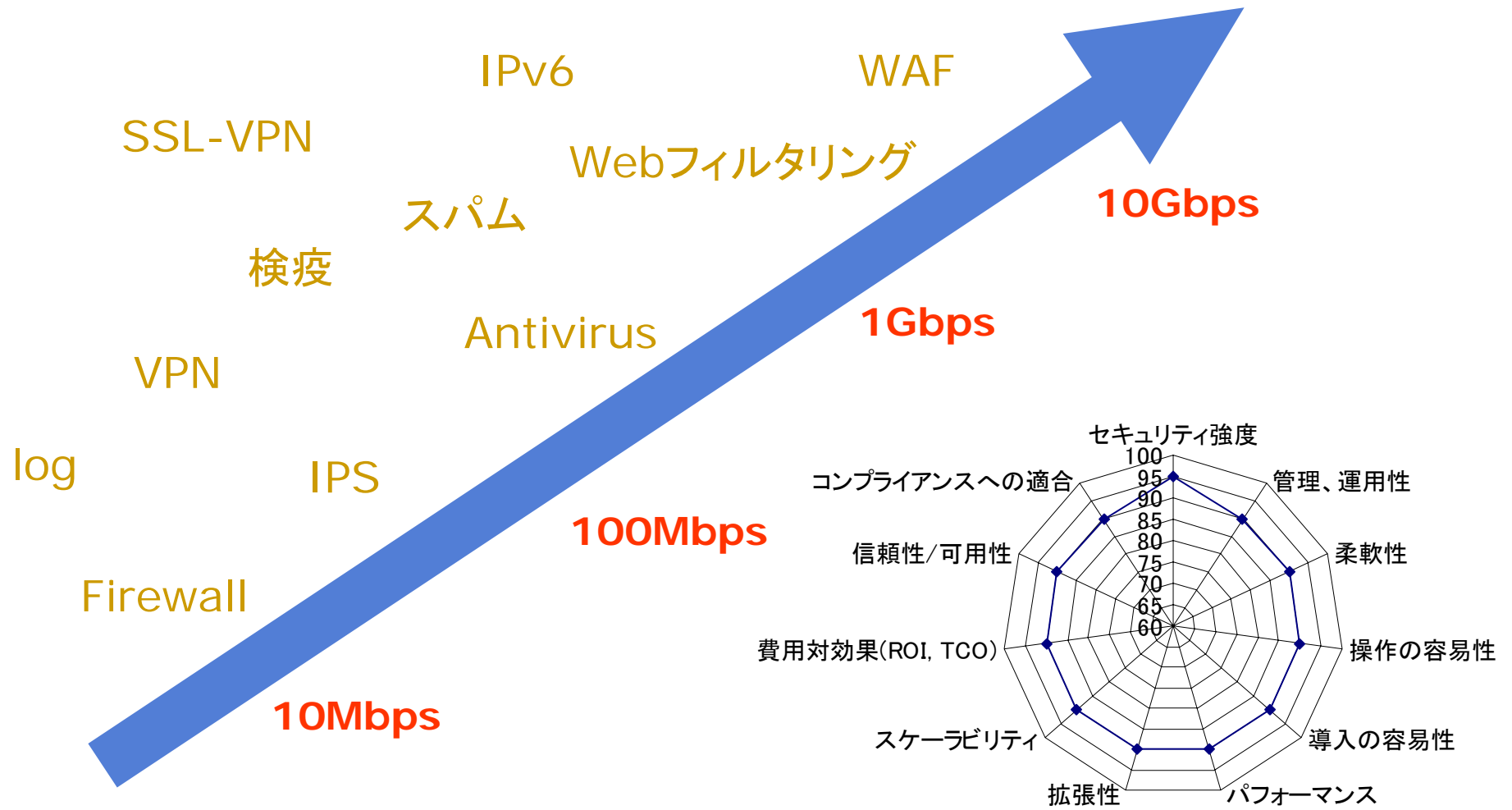
UTM製品は非常に  
負荷のかかる製品





パフォーマンスの高いベースプラットフォームと  
高いアーキテクチャを有している必要がある

# 多様化するニーズ

強く求められるセキュリティ機能とパフォーマンス要件の両立



- 3つのコア技術によるセキュリティパフォーマンスの向上:
  - » SecureXL – ソフトウェアにおけるアクセラレーション
  - » ClusterXL – 冗長化/負荷共有のためのクラスタ技術
  - » CoreXL – 複数のコアを効率的に利用
  
- 上記以外のセキュリティパフォーマンスの向上:
  - » カーネル・レイヤーでの検査
  - » 検査手法の置き換え
  - » 検査オーバーヘッドの最小化

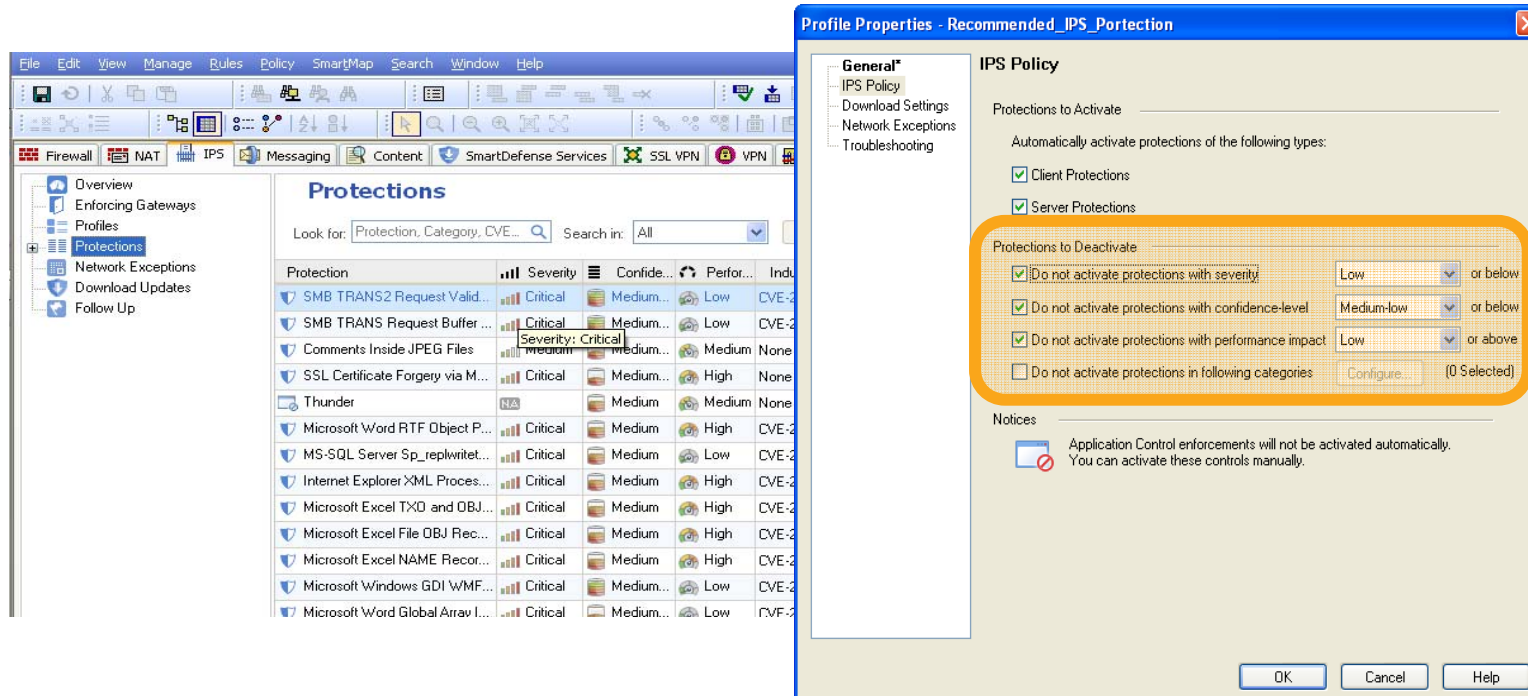
	2007年		2008年	
UTM-1 1050	1.0Gbps	→	1.2Gbps	
UTM-1 2050	2.0Gbps	→	2.4Gbps	

Firewall機能において、20%スループットの向上を実現



最新バージョンであるR70では、IPS機能において10倍以上のパフォーマンス向上も実現

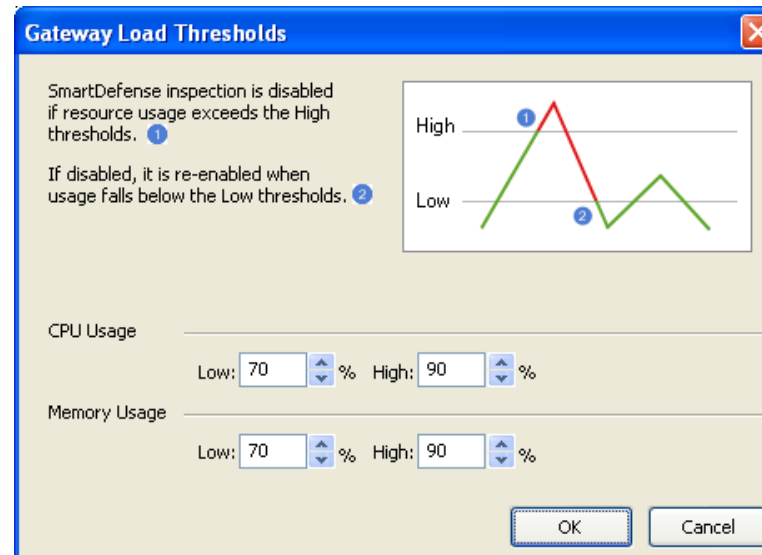
- 設定は生き物



- ・ セキュリティ緊急度(重要度)とパフォーマンスに対する影響との比較
- ・ 実施内容と自社ネットワークの状況の比較

## ■ IPS機能に対するソフトウェア・フェイルオープン

CPUまたはメモリ使用率がHighで指定された閾値を越えた場合、IPS機能を自動的に無効にすることでパフォーマンスを確保し。IPS機能はLowで指定された閾値以下に低下した場合、再び有効化される。



システムに余裕がある場合は深い検査を実施するというアプローチ

## 1. 導入機能の整理

- 具体的にどの機能を統合したいのか
- 使用機能の優先付け

## 2. 統合性、操作性

- 管理機能や出力されるログデータはどこまで統合されているか
- 必要とされる機能とその操作性は充分か

## 3. パフォーマンス

- 現在必要なパフォーマンス、将来必要なパフォーマンス
- パフォーマンス・アーキテクチャ

## 4. コスト