

WatchGuard XTM eXtensible Threat Management

製品概要



2011年1月

株式会社ネットポイント

<http://www.netp.co.jp/> E-mail:info@netp.co.jp

WatchGuard Technologies社について



- 本社:シアトル 1996年設立
- 600,000以上の累積出荷台数 (日本国内:50,000台以上の実績)
- 販社数15,000 以上、120カ国以上での活動
- プロキシベースでのディープパケットインスペクション技術のパイオニア
- 日本法人:2000年に設立



WatchGuard XTM ラインアップ



WatchGuard XTM 2シリーズ

推奨ノード数: 10~50ノード



WatchGuard XTM 5シリーズ

推奨ノード数: 250~1500ノード



WatchGuard XTM 8シリーズ

推奨ノード数: 3000~5000ノード



WatchGuard XTM 1050

推奨ノード数: 10000ノード程度



WatchGuard XTM 製品の特徴

- 1 1500種類以上のアプリケーション*を検出・ブロックする機能を提供
- 2 アプリケーション・プロキシを搭載した強力なファイアーウォール機能を実装
- 3 速くて漏れの少ない高セキュリティ機能
- 4 簡単操作の充実した管理ツールを標準提供
- 5 ログ&レポート管理ツールを標準提供
- 6 多彩なVPN(IPsec方式、SSLVPN方式、PPTP方式)標準搭載
- 7 XTMを強力にサポートする2つのクラウドソリューション

※2011年1月リリース予定のXTM11.4では、アプリケーション検知機能が 1500 以上に拡大します。

1

1500種類以上のアプリケーション*を検出・ブロックする機能を提供

ファイアウォール機能では検出が難しいメッセージャーやP2Pアプリケーションの通信を検出し遮断することができます。また、XTMシリーズの最新バージョンであるVer11.4では、最新技術を用いた行動分析に基づき、送信先アドレスやL7プロトコルに関わらず通常のセキュリティ対策を通り抜けるように設計されている暗号化アプリケーションを含めて、ネットワークに進入を試みるアプリケーションを検出しブロックすることが可能となります。

SkypeやWinnyの通信もブロック可能



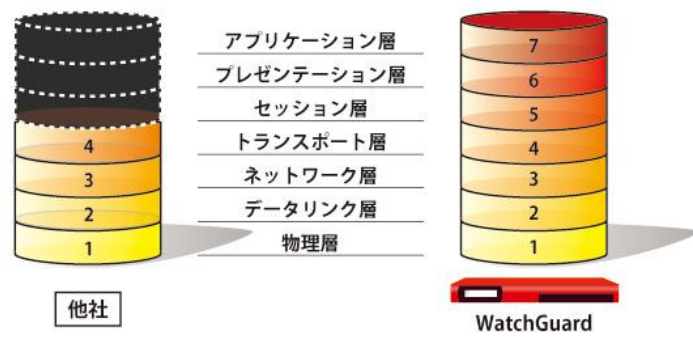
2

アプリケーション・プロキシを搭載した強力なファイアウォール機能を実装

多くのUTM・ファイアウォール製品は、初期攻撃を防御する仕組みに、パケットフィルタリング方式を採用しています。この方式では、流れているデータの中身を確認出来ず、セキュリティ製品としてアクセス制御が不十分であるといえます。WatchGuard(ウォッチガード)XTMは、パケットフィルタリング方式とアプリケーション・プロキシを組み合わせることにより、例えば、FTPによるファイル送信は許可するが、受信は許可しないといった制御や、メールで特定の添付ファイルを削除する等、細かなセキュリティ対策を施すことが可能となります。

ASICやパケットフィルタベースの製品では実現できない高いセキュリティ

※ステートフルインスペクションもパケットフィルタリングの発展形



3 速くて漏れの少ない高セキュリティ機能

WatchGuard ILS : Intelligent Layered Security



UTMをプロキシ機能に統合することで、UTM機能を無駄なく高速に処理します。

多くのUTM・ファイアウォール製品は、許可されているデータパケットを整理せずにそのままUTM機能でチェックしていることから、ハードウェアの高速化が常に求められています。また、専用カスタムプロセッサでも脅威の種類が増大している今日ではアーキテクチャーの限界から、検知できないことが多く、ソフトウェア処理でも同様の手法であれば、負荷が高くなる為、性能維持を理由に、途中から検知しなくなるということはよく知られているところです。



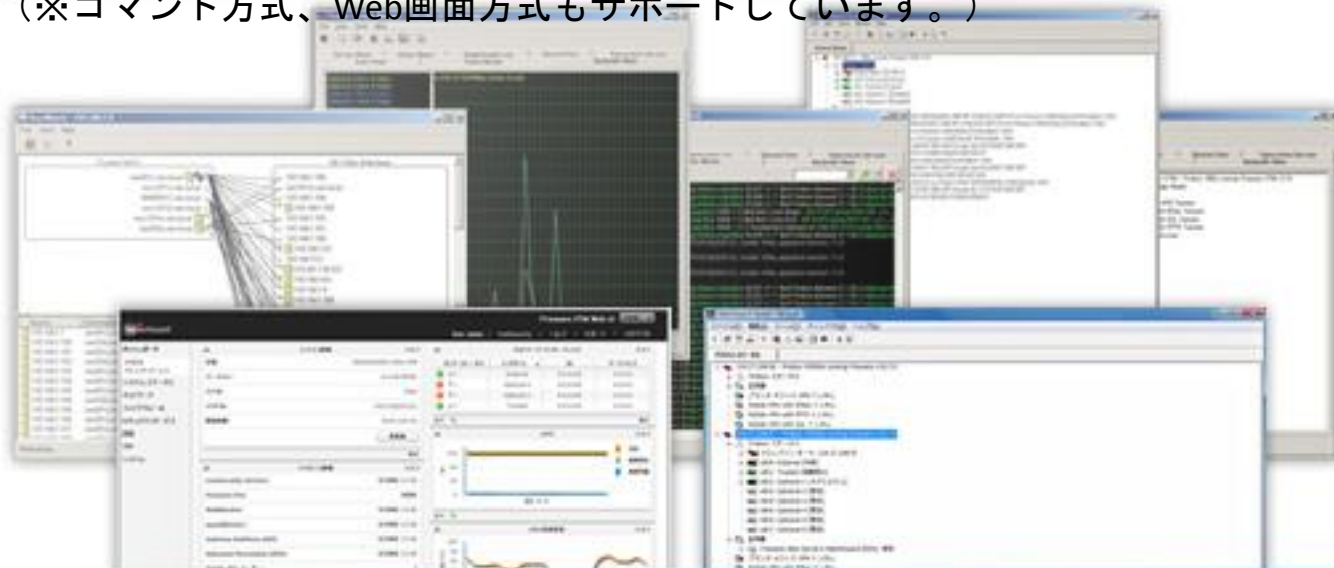
WatchGuard(ウォッチガード)XTMシリーズは「ソフトウェア処理による柔軟性」と「セッション別に分解によりすり抜けの禁止」と「セッション毎に必要なセキュリティを選択」することで負荷を減らし効率を上げることに成功しています。

4 簡単操作の充実した管理ツールを標準提供

多くのUTM・ファイアウォール製品は、ユーザインターフェースとしてコマンド方式やWeb画面からの設定・管理しか提供されていません。また、英語表示のみといった状況とされています。WatchGuard(ウォッチガード)社は初期の製品から、ユーザインターフェースに注力し、ネットワーク技術者でなくとも使いこなせるように設計したWindowsベースの日本語対応管理ツールを多数用意しています。

日本語管理ツール
標準提供

(※コマンド方式、Web画面方式もサポートしています。)



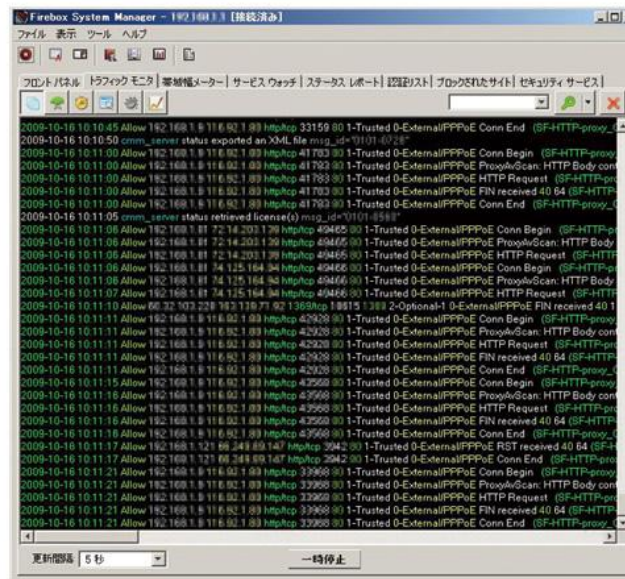
多言語対応(日本語,中国語,英語,韓国語,フランス語,スペイン語)

5

ログ&レポート管理ツールを標準提供

多くのUTM・ファイアウォール製品は、IPアドレス、接続ポート番号、UTMチェック以外の情報をログとして出力する仕組みがないことから、詳細なレポート作成が難しく、またログも垂れ流しで安全に出力する仕組みそのものがないとされています。WatchGuard(ウォッチガード)XTMはアプリケーション・プロキシ機能による詳細ログも含め、安全に保管する為の専用設計のログサーバソフトとレポート用のサーバソフトが標準提供されておりますので、Windowsベースのハードウェアを用意頂く事で、簡単に導入することが可能です。

レポートソフト(英語)、
ログDBソフトも
標準提供



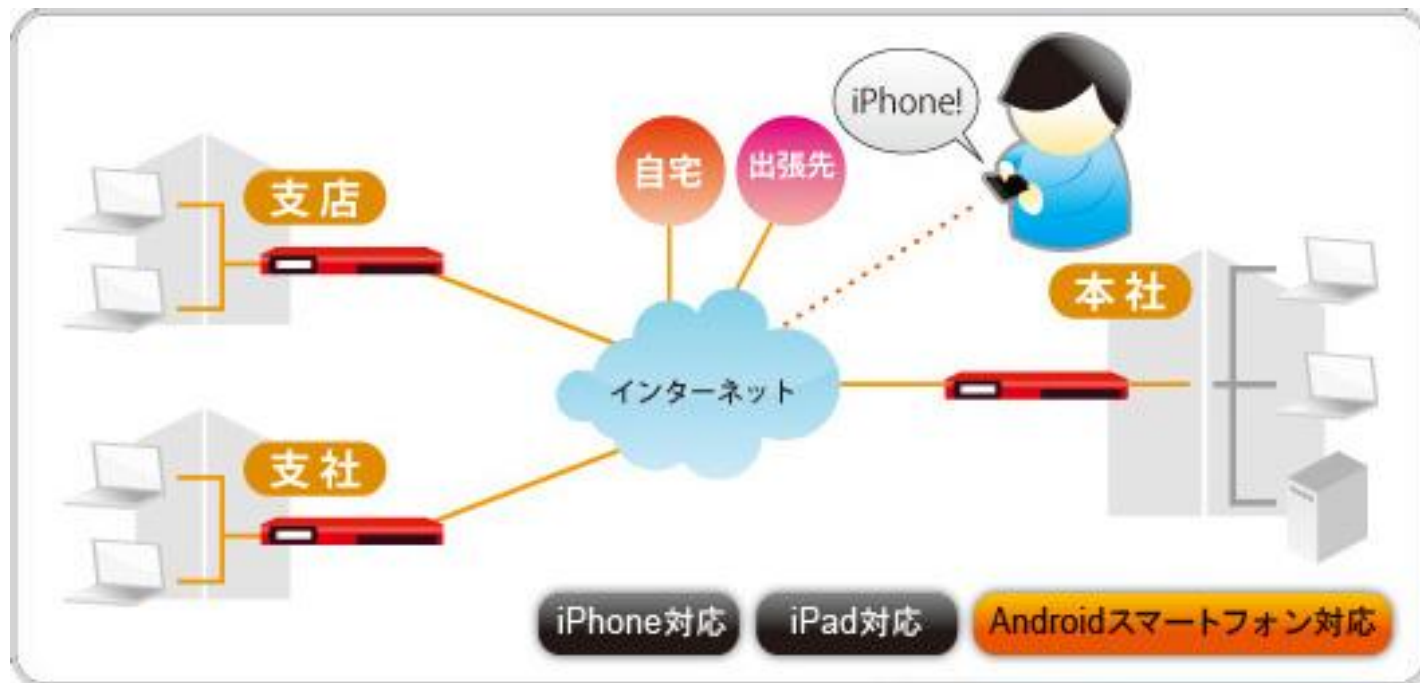
6

多彩なVPN(IPsec方式、SSLVPN方式、PPTP方式)標準搭載

VPN機能
(IPSEC,SSL,PPTP)全て
標準対応

WatchGuard(ウォッチガード)XTMは、IPSecにより拠点間VPNはもとより、ActiveDirectoryやRadius等、様々な認証システムと連携可能なくIPSECベースのクライアントVPNソフトを提供しています。またWindowsXP,VISTA,7(32/64Bit)対応や、MacOSX用SSL-VPNクライアント等充実したVPN環境を構築できます。

※iPhone,iPadはPPTP方式によるVPN接続に対応しています。

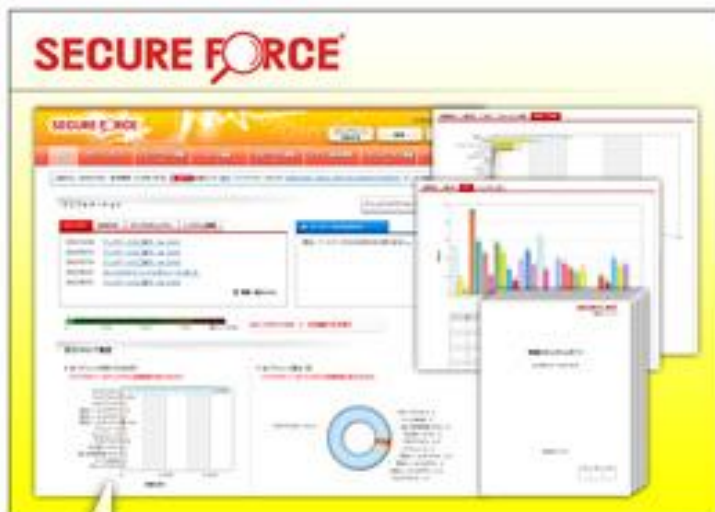


7

XTMを強力にサポートする2つのクラウドソリューション

WatchGuard XTM製品群は、高度なセキュリティ機能と管理者に使いやすいインターフェースに定評があります。株式会社アイバックスはその魅力をさらに充実したものにするために、IT管理者でない人でも、導入効果や情報漏洩対策に有効なログ情報から、状況を簡単に把握できるログ管理サービスの「SECUREFORCE」と、XTM製品の動作を決定する重要な設定情報を、簡単な操作で設定報告書を自動作成するツール「ConfigReporter」を開発・提供しています。※いずれもオプションサービスとなります。

アイバックスが開発・提供しています。

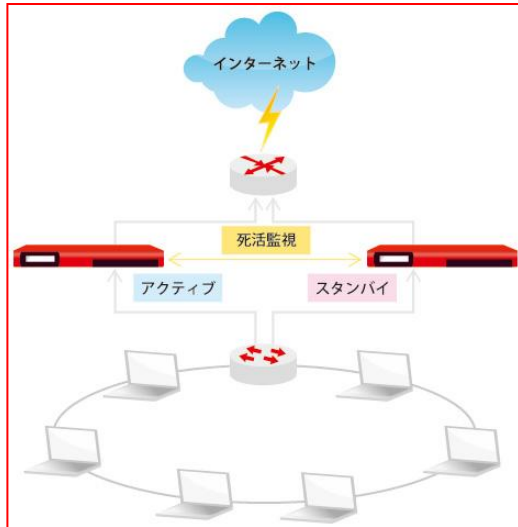


セキュリティの「見える化」を実現

Firewall設定報告書をワンクリックでPDF化



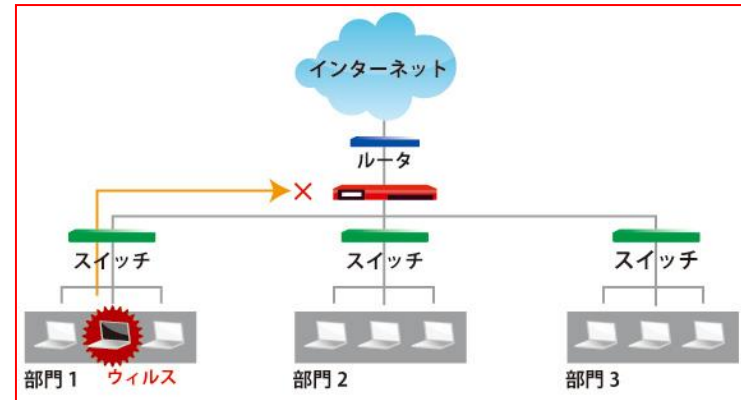
その他特徴



冗長化

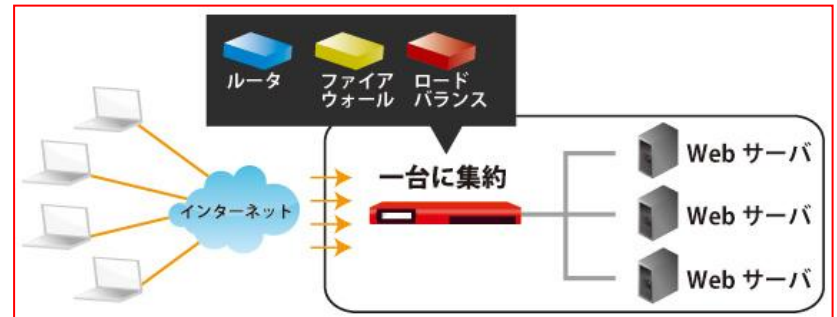
- ・Active/Active、Active/Standbyいずれにも対応
- ※冗長化を行う際には、オプションのFireware XTM Proライセンスが必要となります。

多彩な構成に対応でき
全体コスト削減にも
つながります。



VLAN機能

- ・VLAN (802.1Q)に対応
- スイッチをWatchGuard XTMに置き換えることでウィルス感染したネットワークから他のネットワークへの感染拡大を未然に防ぎます。



ロードバランス機能+サーバの負荷分散

- ・WatchGuardは、ルータ機能+FW/UTM+ロードバランス機能を一台で提供できます。既存サーバの負荷低減を低コスト、低い運用負荷で実現できます。

検疫サーバー(スパムメール、ウィルスメール対応隔離ツール) ※標準添付ソフトウェア

検疫サーバー(WatchGuard Quarantine Server)は、スパムであると疑わしかったり、ウイルスを含む疑わしい電子メールを一時保留し、受信ユーザーに確認をほどこす事が可能となります。

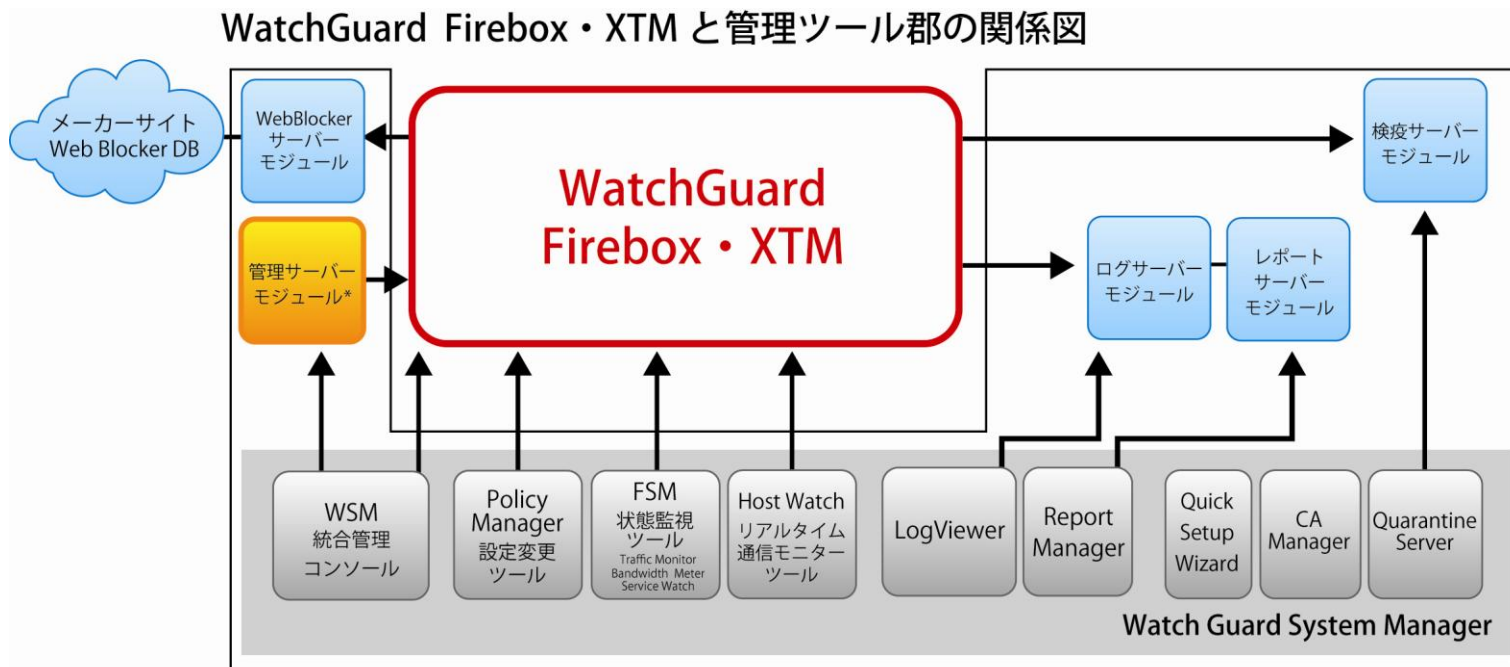
メッセージ (すべて): 12464 メッセージ

ユーザー	検疫のステータス	送信者	件名
suzuki@zing.dnsdojo.com	Confirmed spam	268467@ret.c.sweethea...	Subject: K・
suzuki@zing.dnsdojo.com	Confirmed spam	268467@ret.c.sweethea...	Subject: K・
suzuki@zing.dnsdojo.com	Confirmed spam	268467@ret.c.sweethea...	Subject: K・
suzuki@zing.dnsdojo.com	Confirmed spam	268467@ret.c.sweethea...	Subject: K・
suzuki@zing.dnsdojo.com	Confirmed spam	264676@ret.d.sweethea...	Subject: 違・
suzuki@zing.dnsdojo.com	Confirmed spam	264676@ret.d.sweethea...	Subject: 違・
suzuki@zing.dnsdojo.com	Confirmed spam	268467@ret.c.sweethea...	Subject: くる

疑わしいスパムメール
スパムメール
バルクメール
ウィルスメール
疑わしいウィルスメール

:スパムの可能性があるが、情報不足により断定できない。
:間違いなくスパムである。
:商業バルクメールの一部である。
:ウイルスが含まれる可能性が高い。
:ウイルスが含まれる可能性がある。

【参考】管理ツール群とWatchGuard XTM製品の関係



□ は WatchGuard System Manager インストーラーに全て含まれており、個別にインストール可能です。
尚、管理サーバーモジュールは別途ライセンスが必要です。

これだけの管理・便利
ツールがどの製品にも
利用ライセンス付き

【参考】ASICテクノロジーベースUTM製品の比較

WatchGuardは「多層防御」ファイアウォールを提供できる唯一のベンダー



ディープ・パケット・インスペクション

ステートフル・パケット・インスペクション

プロキシ・プロテクション

某ASICテクノロジーベースUTM製品

ディープ・パケット・インスペクション

ステートフル・パケット・インスペクション

WatchGuardは全てのセキュリティ・サービスが稼働している際、
同等のASICベースUTM機器に比べて、格段に早いパフォーマンスを実現



全UTM機能を稼働した際のスループット速度

※メーカー独自調査

約30%ダウン ※

某ASICテクノロジーベースUTM製品

約90%ダウン ※

WatchGuardは、インテルのチップセット技術を採用
ASICベースUTM機器は自社開発のチップセットに縛られている



インテル

最新技術

高い信頼性

素早く、高機能で、強力に
次世代ネットワーク脅威をブロック

某ASICテクノロジーベースUTM製品

自社開発

陳腐化する可能性

最新のネットワーク脅威に対応不可

【参考】ASICテクノロジーベースUTM製品の比較

- ASIC テクノロジー:
 - **GOOD** Firewallパフォーマンス
 - POOR コンテンツセキュリティパフォーマンス
- セキュリティ:
 - 弱セキュリティSPIFirewall
 - DoS攻撃防御無し
 - VoIPセキュリティ無し
- 管理・モニタリング:
 - リアルタイムモニタリング機能無し
(HostWatch、トラフィックモニター)
 - ドラッグアンドドロップVPN管理機能無し
 - 貧弱なレポート機能 見えないセキュリティ

