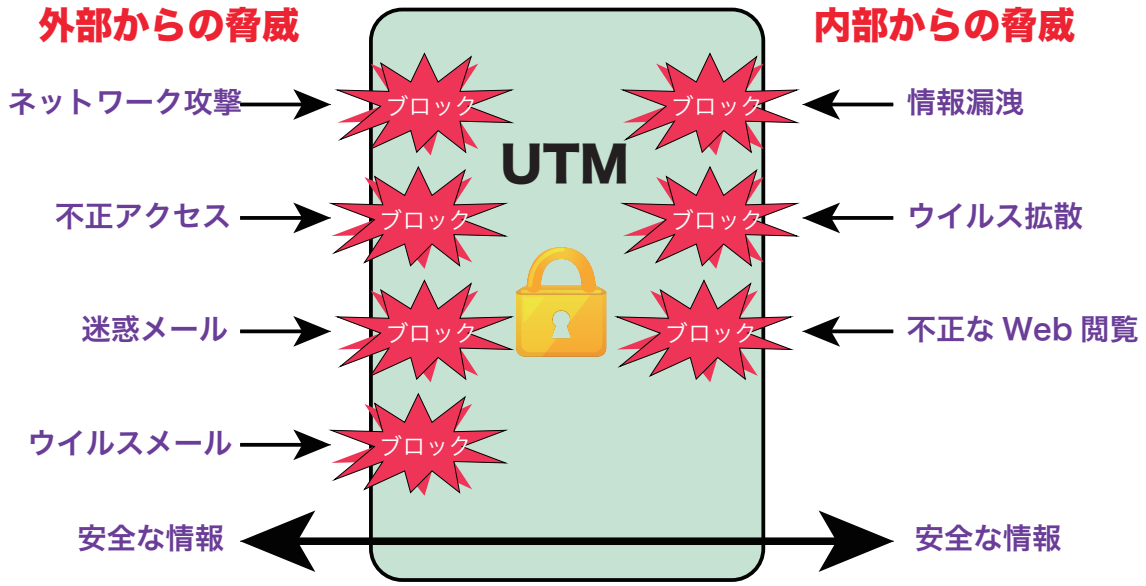
UTM（Unified Threat Management）統合脅威管理

UTM とは、複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理を行う、つまり統合脅威管理 (Unified Threat Management) を行う機器のことを指します。
ま、簡単に言うとウイルス対策とファイアウォールを 1 台にまとめたようなものです。
ウイルスを生み出すハッカーは世界中に数多くおり、1 日に新しく作られるウイルスは 120 ～ 130 万個とも言われ、様々な脆弱性を攻撃してくるワームやウイルスなど、企業ネットワークは新たな脅威にさらされています。過去に発見されたウイルスのパターンをもとに検知する**従来のウイルス対策ソフトだけでは不十分**になってきています。ウイルス対策ソフトが検知できるのは、攻撃してくるウイルスの半分くらいだとも言われています。
そうした脅威に対抗するためには、ファイアウォールのみならず、IDS/IPS やアンチウィルス、アンチスパム、Web フィルタリングなどを駆使し、総合的なセキュリティ対策を施さなければなりません。しかし、侵入防止のために複数の機器を導入したり、すべての端末にウイルス対策ソフトを入れたり、それらを管理したりするのは、手間もコストもかかります。
外部からの脅威と内部からの脅威を、いろいろな階層で防御することを「多層防御」と呼びます。
多層防御とは

- 危険なサイトに行かせない（URL フィルタリング）
- 危険なメールを防ぐ（アンチスパム）
- ウイルスの侵入を防ぐ（アンチウイルス）
- 危険な通信を社内に侵入させない（ファイアウォール、IPS）
- 内部からの危険な通信を外に出さない（ファイアウォール、IPS）

といったことを制御することを指し、これらのことを**1 台の機器で実現するのが「UTM」**なのです。



そして VPN（Virtual Private Network）機能を併せ持った UTM を使うことによって、安全なテレワーク環境を構築することが出来ます。

**シスポートでは、外部からの不正侵入や内部からの不正なデータ流出を防ぎ、
快適で安全なテレワーク環境の構築に欠かせない UTM の導入をお薦めしています。**

プライベートクラウドに対応しているＱシリーズ
(はんばいＱ、こうじＱなど）と共に導入をご検討
下さい。