

「UTM ソリューション」によるサイバーセキュリティ対策のご案内

■UTM とは

企業の IT セキュリティ対策として必要な、「ファイアウォール」や「ゲートウェイアンチウイルス」等、複数の機能が一台に集約されています。

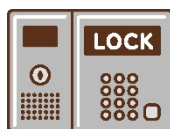
難しい技術的なことを理解しなくても、この一台の導入で、一定レベルのセキュリティを確保できます。専任担当者不要で、手間もコストもおさえられます。

例えるなら、UTM はオートロックのマンション。部屋の鍵とは別に、もうひとつ外で守ってくれる。



【部屋の鍵】

+



【マンション入口のオートロック】

■現状

- ・サイバーセキュリティ対策が必要なのはわかるが、情報がたくさんありすぎて、何から手を付けていいかわからない。
- ・大企業ではないため、通信ネットワークについて、技術的に詳しい専任担当者がいない。

■課題

- ・サイバーセキュリティ対策がとられていないまま放置され、危険な状態
- ・難しい技術的なことがわからなくても、ソリューションの導入等、具体的に取る必要がある

■背景

- ・サイバー犯罪による被害は大手企業のみならず中堅・中小企業にも広がっているのが現状です。
4、5 年前から状況は急速に悪化してきています。
- ・サイバー犯罪はビジネス化しており、単純にセキュリティ対策がとられていない企業が標的にされると言われています。
- ・それを受けて最近では、取引先間でも、セキュリティ対策の確認が入る等、具体的なセキュリティ対策についての取り組みが求められるようになりました。
- ・一方で、中堅・中小企業では、IT 人材不足も問題です。
社内に詳しい人がいないために何から手を付けたら良いかわからず、対応が放置されることで、犯罪者に狙われてしまう可能性もあります。

SonicWALL TZ/NSA シリーズ 「UTM ソリューション」

■「UTM ソリューション」とは

アーツネットワーク（以下、弊社）が提供する導入後保守サポート付きの UTM サービスです。セキュリティは、バランスも重要で、セキュリティをガチガチにしてしまうと、システムの動きが重くなったり使えなくなってしまう場合があります。

弊社のこれまでのノウハウ、経験を活かし、お客様に快適にご利用いただけるよう、バランスよく構築し、運用についてもサポートします。

■機種

SonicWALL TZ/NSA シリーズ

■機能

6つの機能を最新の定義ファイルに常に更新いたします。

ファイアウォール

- 不正侵入防止（IPアドレス、ポート番号等で特定して通信を遮断）

ゲートウェイアンチウイルス

- ウィルス、ワーム、トロイの木馬、フィッシング、新種の脅威、インターネットの悪用などのネットワークリスクから企業ネットワークを保護

アンチスパイウェア

- スパイウェア及びアドウェアを検出・除去

コンテンツフィルタリング

- 不適切・有害サイトやカテゴリごとのアクセスの許可/拒否

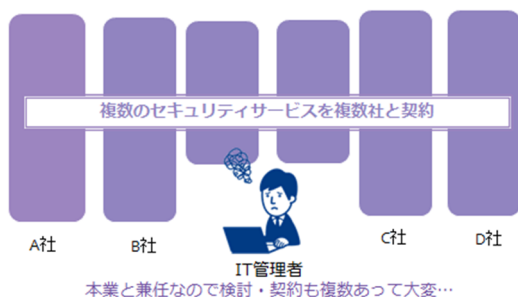
IDS/IPS

- 不正侵入検知/防御システム（DoS/DDoS攻撃等の悪意のある特徴を持つ通信を検知して遮断）

キャプチャATP（新機能）

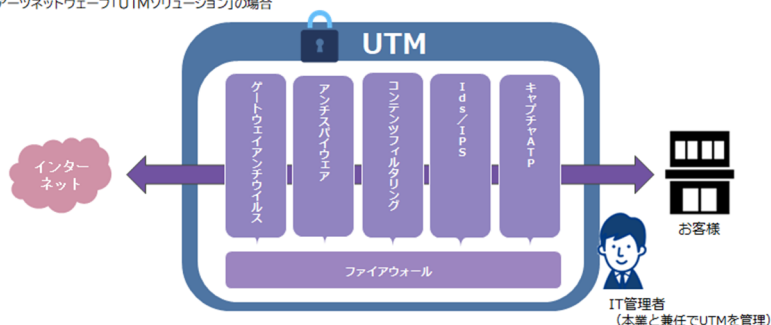
- これまで検知・ブロックが難しかった、SonicWALLのデータベースにまだ登録されていない未知のウィルスをリアルタイムで分析し、検知、ブロック。
（不知もしくは前段階で有害・無害の判断ができなかった場合、クラウド上のキャプチャATPサービスにファイルを転送し確認の上ダウンロードを実施）

セキュリティ対策をしようとすると



UTMなら

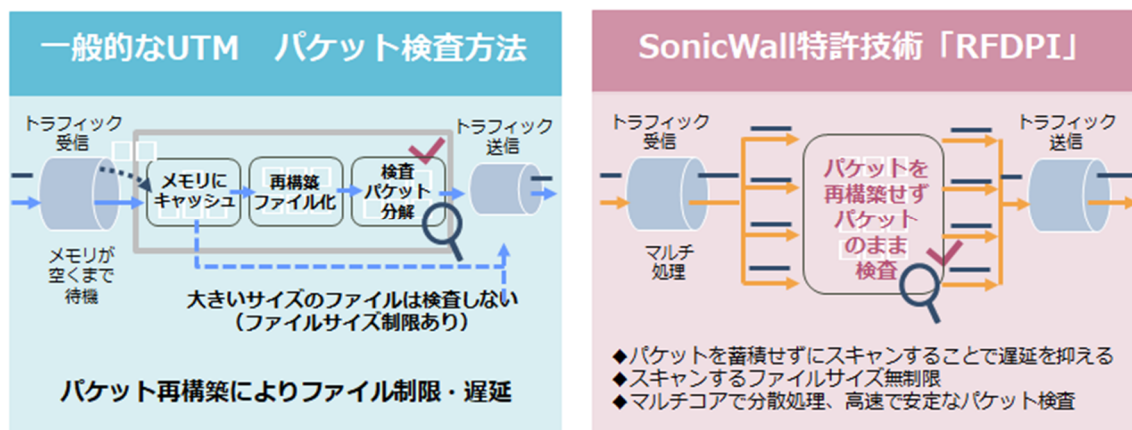
※アーツネットワーク「UTMソリューション」の場合



■高速処理を実現

「UTM ソリューション」で使用する SonicWall UTM は、特許技術「RFDPI」により、脅威保護が、高速かつ安定的に行えます。

一般的な UTM では時間がかかったり、サイズが大きすぎて通信を止めてしまう大きなファイルでも、SonicWall はこの特許技術で検知可能で、ネットワークセキュリティを高速処理で実現します。



■ファームウェア更新も確実に対応

サイバー攻撃を受けるリスクを減らすためにファームウェアの更新を適切に行っていただく必要性が高まっています。機器提供元が更新を必要と判断したファームウェアが発表されたタイミングで、お客様と日程調整の上、弊社がリモートで機器ファームウェアを更新します。

■オプション

リモートアクセス VPN サービス「SSL-VPN」

場所を選ばず、事務所 PC にアクセスすることが可能になります。

ライセンス数はご利用人数にあわせてお選びいただけます。

「SSL-VPN」をより安心してご利用いただくために

- ・ 2 段階認証

本人にのみ確認できるアドレスを登録することでセキュリティを高めることができる 2 段階認証。スマートフォンや手元のパソコンで確認できるアドレスである必要があります。

- ・ 定期パスワード変更

SSL-VPN で使用するパスワードを接続者が定期的に変更必要のようにする定期パスワード変更。これによりセキュリティの向上を図ることができます。(別途お申込みが必要です)

機器故障に備えた通信障害対策 UTM 機器2台構成「ホットスタンバイ」

万が一 UTM 機器が故障してしまった場合、インターネットや VPN の通信ができなくなり、業務がストップしてしまいます。

「ホットスタンバイ」オプションをご利用いただくと、常に 2 台の UTM 機器が稼働し、万が一の機器故障が起こったときにも、もう片方の UTM 機器に自動で通信を切り替えるため、お客様の業務を止め

ずに済みます。

(別途お申し込みが必要です)

このような2台構成の場合、弊社「UTM ソリューション」 SonicWALL では、機器費用は2台分必要ですが、ライセンス、保守は1台分で運用可能です。初年度のみ、2台構成「ホットスタンバイ」を可能にするための「STATEFUL HA UPGRADE ライセンス」のご購入が必要です。

3～5年の総所有コストにおいて、ソフトウェアライセンスは大きな部分を占めます。ご検討の際は、初期費用だけでなく、3～5年の総所有コストもご確認ください。

「ホットスタンバイ」オプション対応機種については、弊社までお問い合わせください。オプションのご利用には弊社までお申し込みが必要です。



企業ネットワークをトータルで提案

インターネット回線の冗長化やローカルブレイクアウト機能を使って、トラフィック分散も可能となり、通信環境でも速度対策ができます。

速度が遅くなることを理由に導入をあきらめていた方にもぜひご検討いただきたいサービスです。

■注意事項

- ・ UTM はすべてのコンピューターウイルス、スパイウェア、不正アクセス等への対応を保証するものではありません
- ・ アーツネットワーク提供の「UTM ソリューション」では「アンチスパムメール」には対応していません。ご利用のメールサーバ側や端末ごとのウイルス対策ソフト等で対応が必要になります。
- ・ オプション「ホットスタンバイ」をご利用頂く場合、LAN 側が1ポートとなりますので、HUBが必ず必要です。また、LAN 側 IP アドレスは3つ必要です。

ご検討、どうぞよろしくお願いいたします。