UTMとは

提案資料

株式会社ビジョン
BNS事業部ﾋﾞｼﾞﾈｽﾌｫﾝﾕﾆｯﾄ

➢ UTMとは

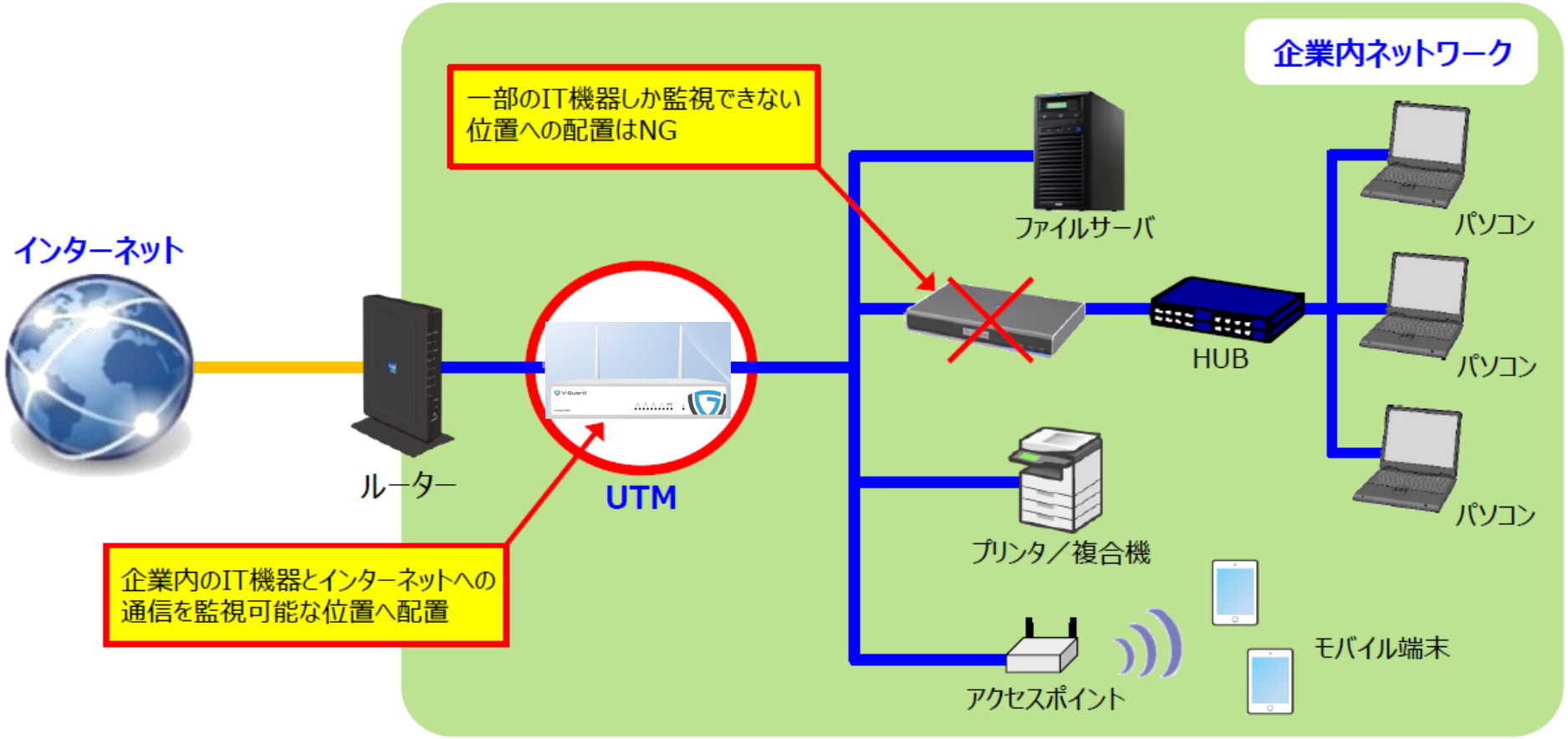
昨今のインターネットを通じた「脅威」は多様化しており、その「脅威」に対抗するためには、ファイヤウォールだけでなく、アンチウイルスやアンチスパム、IPS／IDSなどの様々なセキュリティ機能を駆使して対策を施す必要があります。

しかしながら複数のセキュリティ機能を導入するために、別々の製品・システムを導入するのではコストが積み重なり、企業にとって導入・維持が困難になります。

そこで登場したのが複数のセキュリティ機能を統合した「UTM（統合脅威管理）」です。
企業は「UTM」を導入することで、インターネットを通じた脅威を総合的に対策することができます。

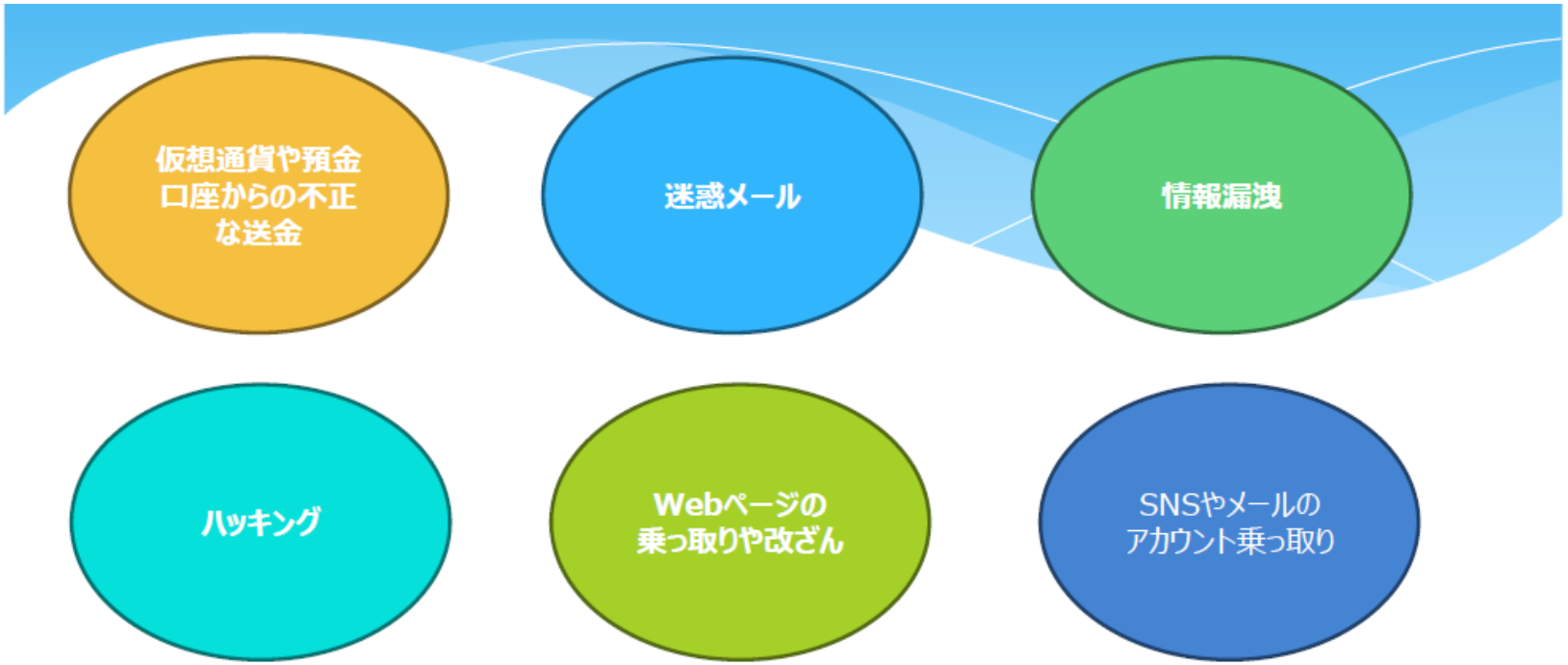
➢ UTMのネットワーク構成

UTMはインターネットからの通信と企業内ネットワークからの通信の両方を監視する装置です。
よって企業内ネットワークのルーター直下に設置する必要があります。



➢ ネットワークの脅威

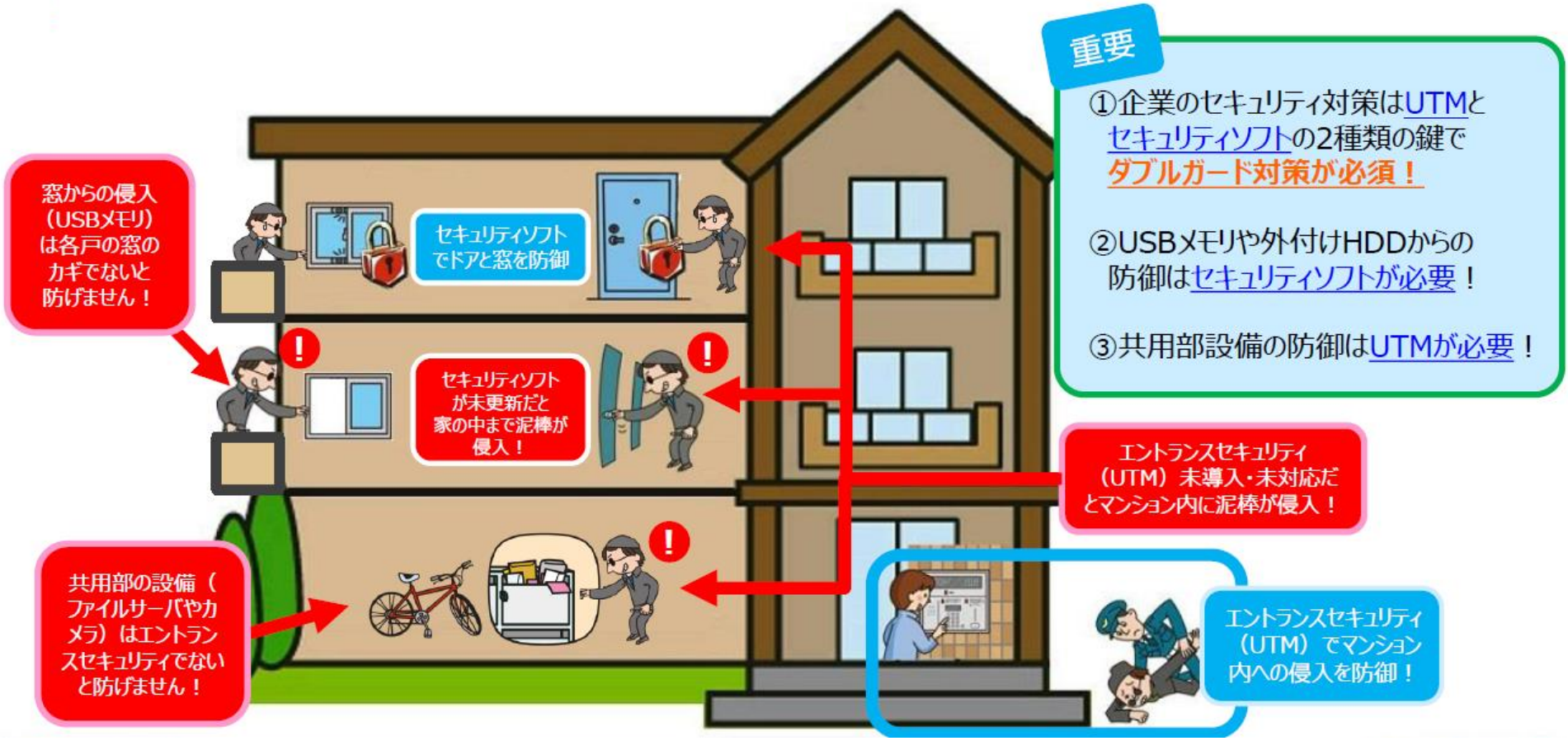
インターネット通信やネットワーク通信を利用する上で起こりうる脅威として下記が挙げられます。
IoTやスマホ等の移動体通信が主流になる今、セキュリティー対策も多層化を図ることが重要になっています。
また、外部からの脅威だけではなく社員の持ち出し、誤送信、デバイスの紛失など人的な要素も注意が必要です。



➢ セキュリティソフトとの違い

◆セキュリティソフトとの違い

UTMはパソコン本体をガードするセキュリティソフトとは違い、インターネットへの出入り口を監視する装置です。マンションで例えると、UTMはエントランスのセキュリティで、セキュリティソフトはマンション各戸のドアや窓の鍵になります。



➢ UTMのメリット・デメリット

◆UTMのメリット

①UTMのほとんどがアプライアンス製品のため、ソフトウェアのインストールが不要となり、導入が容易。

②1台で複数のセキュリティ機能を導入できるので、導入コストを抑えることができる。

③1台で複数のセキュリティ機能を提供しているので、保守サポートを1社から受けられる。

④複数の製品で構成されているセキュリティ機能より、ネットワーク接続問題が発生した場合の調査が簡単。（UTMの撤去もしくは他製品への入替で問題の切り分けが可能）

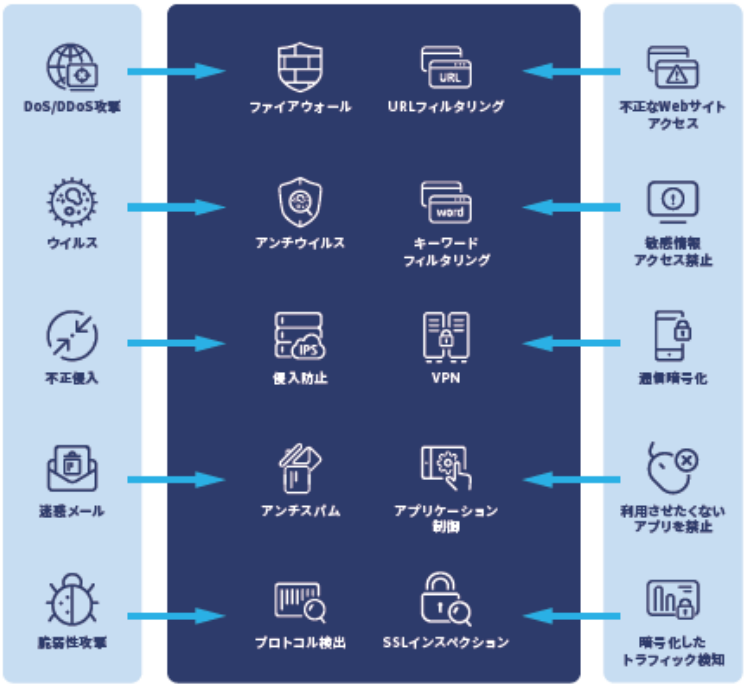
◆UTMのデメリット

⑤セキュリティ機能を1つにまとめているため、システムダウン時にインターネットへの接続が出来ない。

⑥製品によって対応しているセキュリティ機能やその性能がまちまちであり、一部の機能だけ拡張するなどの対応が取りづらく、導入時の製品選択が重要となる。

⑦インターネットと社内の通信を監視する役割なので、PCへ直接接続するUSBメモリからのウイルス感染などは防げない。（PCのセキュリティソフトも合わせて導入が必須）

➢ V-Guad2000 機能一覧



➢ ファイアウォール

◆ファイアウォールとは？

ファイアウォールとは、ネットワーク通信に含まれる「送信元のIPアドレスとポート」「送信先のIPアドレスとポート」を監視し、その通信を通過させるかどうかをポートの開け閉めで制御しています。

ポートはインターネットとの通信を行うドアのようなもので0から65535まであり、ファイアウォールは通常使用しないポートを閉じることで不正な通信を遮断します。

◆ファイアウォールが無いとどうなるか？

パソコンにインストールされるソフトウェアの中には、P2Pファイル共有ソフトのように、通信を待ち受けている機能（サーバ機能）を持つものがあります。その場合、常にポート（ドア）が開いている状態となり、ソフトウェア側に脆弱性があると、それを悪用してパソコンの情報を盗み出されたり、パソコンを乗っ取られてしまうことがあります。

➢ アンチウィルス①

◆アンチウイルスとは？

UTMにおけるアンチウイルスとは、コンピューターに感染することでプログラムやファイルを破壊してしまうコンピュータウイルスをダウンロードしたり、インターネットに拡散することを未然に防ぐ機能です。

コンピュータウイルスにはいくつもの種類や亜種があり、全世界のネットワーク上で日々増加しています。UTMなどのセキュリティ機器は、この増加に対応できるようパターンファイル（シグネチャ）を自動更新する機能を兼ね備えています。

◆コンピュータウイルスの感染経路

ウイルスの感染経路として多いのは、インターネットの不正なサイトからダウンロードしたものによる感染やメールの添付ファイルによるものです。UTMはインターネットとの通信を監視しますのでパターンファイルにマッチングしたコンピュータウイルスの通信を阻害することが可能です。

なおコンピュータウイルスには、OSやソフトウェアのセキュリティホール（システムの欠陥）をついてコンピューターに侵入するタイプもあり、UTMでは阻害できないケースもあるため、最新バージョンのOSやソフトウェアを使用することもセキュリティ上必須の対策となります。
（Windows XPは使用しない、OSの更新プログラムを最新にする、など）

➢ アンチウィルス②

◆コンピューターウイルスに感染すると・・・

一旦ウイルスに感染するとパソコンに様々な異常が起きるケースが多くあります。
例えば、いつも使用しているソフトウェアや業務ファイルの表示がおかしくなったり、開けなくなったり、
いつの間にか削除されていることもあり、企業に多大な被害を与えることになります。

また見た目は何も異常は起きなくとも、ウイルスの添付されたメールを取引先やお客様に勝手に
送りつけたり、パソコンに保存されているファイルの情報が外部に流出することもあり、この場合は
感染したことに気づくのが遅れて、被害が拡大するケースも多くあります。

◆ウイルスの増加対策

ウイルスは全世界で日々増加しており、増加したウイルスに対応するためにはパターンファイルを更新す
ることで対応していますがイタチゴッコです。
パターンファイルやOSのセキュリティパッチが適用される前にうける攻撃のことを「ゼロデイ攻撃」と呼び、
被害も大きくなる傾向があります。

これに対してセキュリティ機器側でも、ウイルスの特有の挙動を検知する「ヒューリスティック検知」や
攻撃されてもいい仮想環境でファイルを動作させて挙動を分析する「サンドボックス」といった
未知のウイルスを検出するセキュリティ機能があります。

※「ヒューリスティック」「サンドボックス」は未知のウイルスを100%検知できるものではありません。

➢ アンチスパム

◆スパムメールとは？

スパムメールとは、受信者の意向を無視して無差別に送信されるメールのことです。インターネットの普及に合わせて宣伝目的で広く使われており、メール使用者にとっては通常のメールよりもはるかに多く届くなどの問題で、社会問題となっています。

またスパムメールの内容は有料サイトや不正なサイトであるフィッシングサイト（詐欺）への誘導であったり、アクセスすることでスパイウエア（情報収集用のウイルス）をダウンロードしてしまうなどセキュリティ上の問題が多々あります。

※スパムメールのメール削除依頼や、配信停止の連絡は逆効果です。そのメールアドレスが有効であることを伝える行為となります。

◆アンチスパムとは？

アンチスパムとはスパムメールを特定し処理する機能のことです。UTMの場合、メールの題名にスパムメールであることを追記処理し、ユーザが使用しているメーラーの自動振り分け機能で、通常のメールとスパムメールをフォルダ分けすることが可能になります。（スパムメールの削除はしません）

➢ Webフィルタリング

◆Webフィルタリング（URLフィルタリング）とは？

Webフィルタリング機能とは、危険なWebサイトや業務に関係ない不適切なWebサイトへのアクセスを制限する機能です。
制限する方法については１つ１つのWebサイトを登録する「ブラックリスト」方式だけでなく、
特定のカテゴリでまとめて一括設定するなど、設定する方が容易に対応できる仕組みとなっています。

【カテゴリ例】
アダルト／脆弱性のあるサイト／金融／ギャンブル／ゲーム／フィッシングサイト／スパムサイト／ショッピング／ソーシャルネットワーク（SNS）／違法なサイト／P2P／チャット／掲示板etc..

◆Webフィルタリングの効果！

Webフィルタリングの効果としては、以下のものが挙げられます。

■Webサイト閲覧からのウイルスやスパイウェアの侵入を減らせた
■従業員が業務へ集中できるようになり作業効率がアップした
■従業員が悪質なネット犯罪に巻き込まれる心配が減った
■動画サイトを禁止したことでネットワーク負荷が減って、ネットワークアクセスが早くなった
■家庭のネットワークと共用のため、子供にアクセスして欲しくないアダルトサイトを禁止にした

➢ アプリケーション制御

◆アプリケーション制御とは？

アプリケーション制御機能とは、パソコンにインストールした特定のアプリがインターネットと通信することを識別し禁止することができる機能です。
例えばWinnyやShare、PerfectDarkといったP2Pソフト（ファイル共有ソフト）や動画アプリのネットワーク通信を阻害することでアプリを正常に動かなくすることができます。

【アプリケーション制御例】
P2Pソフト／ネットワークゲーム／ネットバンキング／リモートデスクトップ／SNSソフト／メッセンジャーソフトetc..

◆アプリケーション制御の効果！

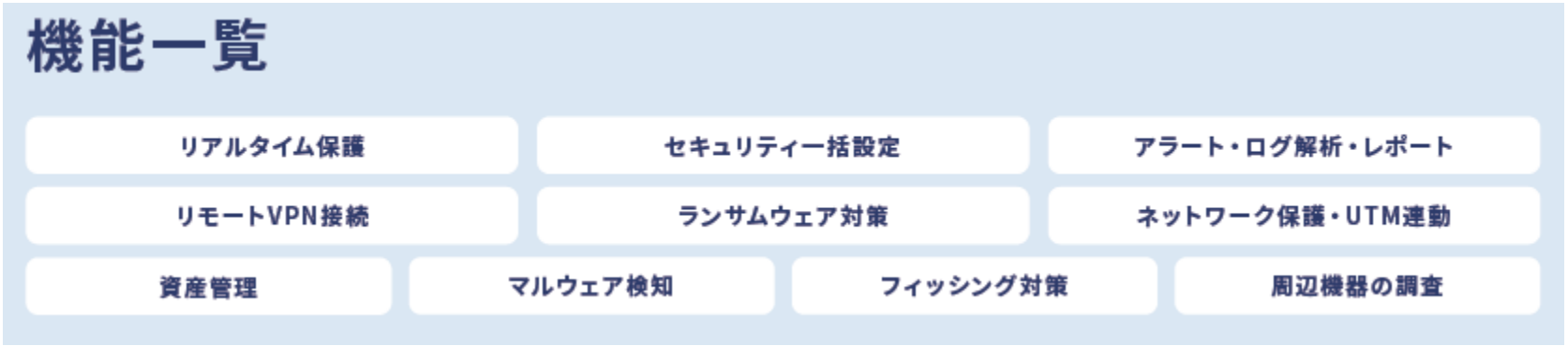
アプリケーション制御の効果としては、以下のものが挙げられます。

- ファイル交換によるウイルスやスパイウェアの侵入リスクを除外できた
- ファイル交換による個人情報や企業機密情報の漏えい対策になった
- 従業員が業務へ集中できるようになり作業効率がアップした
- 動画アプリを禁止したことでネットワーク負荷が減って、ネットワークアクセスが早くなった
- 家庭のパソコンが業務と共用のため、子供が勝手にファイル共有ソフトを使用することでの情報漏洩リスクを除外できた

※Webフィルタリングと同じような効果ですが、インターネットに接続する手段が異なりますので企業のセキュリティとしては両方の対策がより効果的です。

➢ NISE(エンドポイントセキュリティ製品)

NISEでは、アンチマルウェアやランサムウェアの防止・管理・対策といった EPP ・ EDR セキュリティ機能の他、リモートデスクトップ機能やソフトウェアや端末の利用状況などを管理する資産管理ソリューションも備えた総合セキュリティーソフトです。
V-Guard との連携することで、より詳細な出入口対策を提供することが可能になります。



導入メリット

・リアルタイム保護（PC常駐）とクラウド脅威情報を用いた検知で、新種のウイルスや未知の脅威も見逃しません。
・PCの脆弱性診断と自動修復の実施で万全なセキュリティ強化対策を実施します。
・UTMと情報連携することで、ネットワークの出入口の防御だけではなく、
社内LANを含む全体の多重化セキュリティ対策を実現します。
・リモート接続によって、感染リスクのあるPCの調査、手動隔離、メンテナンス保守が簡単に実施できます。
・感染後の自動対処、自動隔離、アラート通知とレポート分析によって、運用負担を軽減します。
・クラウド管理で社内資産を一覧化し、セキュリティレベルやカテゴリー分類によって効率よいセキュリティ運用が
可能となります。

➢ サイバー保険

V-Guard 2000には、サイバーセキュリティ事故や情報漏えいによる各種損害を補償する「サイバー保険」が付帯されています。

SOMPO
損保ジャパン

【補償概要】
・賠償責任に関する補償
・事故対応に関する費用
事故につき合わせて100万円

損害賠償責任への対応費用

- お詫び状送付費用
- 被害者への見舞金・見舞品
- 賠償金支払い
- 情報漏えいのモニタリング

など

他人に対する損害

事故発生時の各種対応費用

- 事故原因調査・影響範囲調査
- 会見・マスコミ対応・コールセンター設置
- データ復旧・情報機器復旧
- 再発防止コンサルティング
- 専門コンサルタントへの相談費用
- 文書作成や報告に要する費用
- 証拠収集費用・翻訳費用

など

事故対応に要する諸費用

➢ 保守・サポートについて

「V- Guard2000」をご利用のお客様を対象としたサービスです。
動作不良時のハードウェアの無償交換及び、お困り事など何でもご相談いただける
オンラインサポートのセット保守となります。


Vision
More vision, More success.