

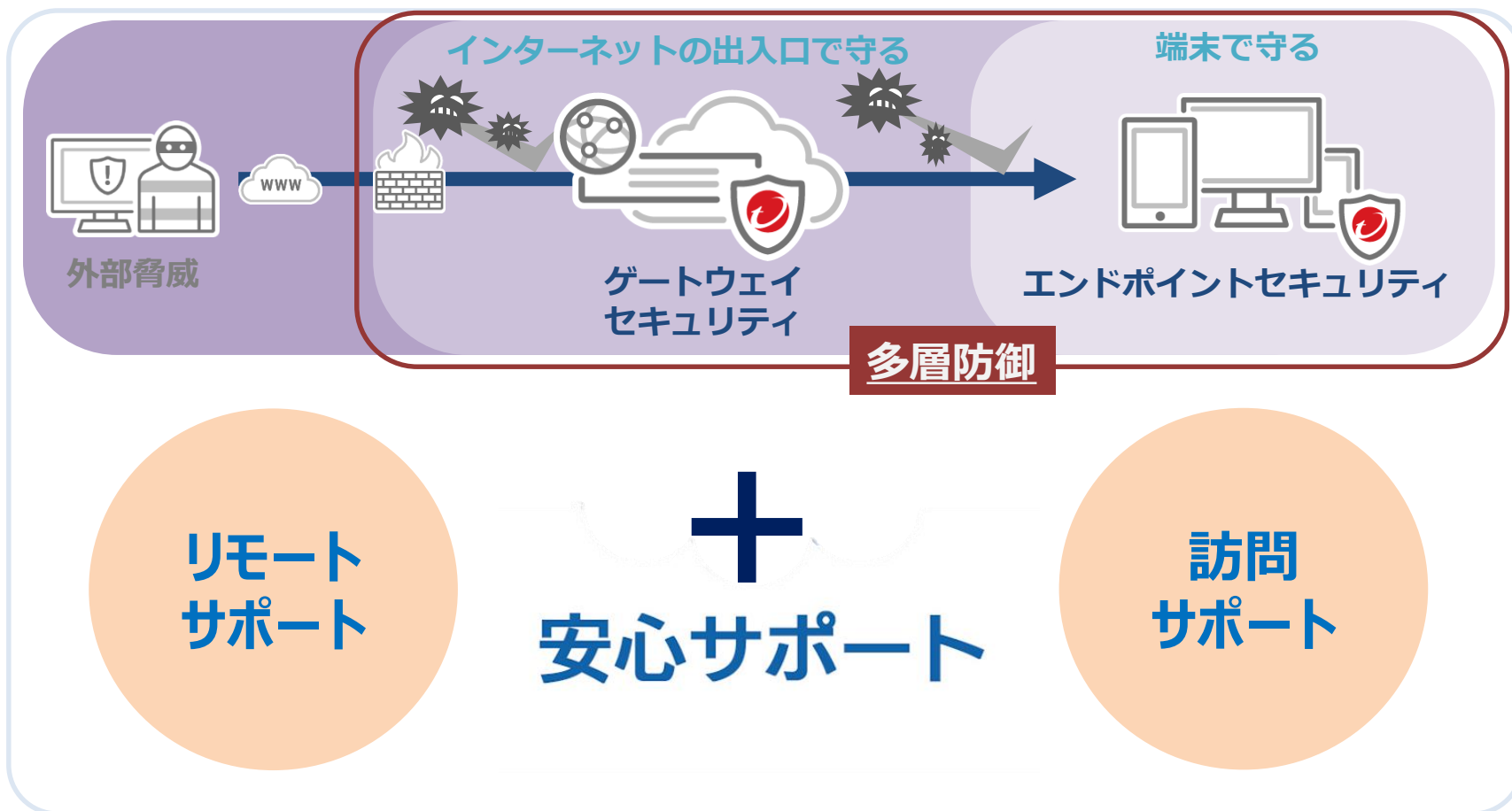
そのお悩みを「MINATOおまかせインターネットセキュリティーサポート」が解決します！

- ゲートウェイセキュリティ（UTM）と、エンドポイントセキュリティの**多層防御**により、お客さまのインターネット環境をしっかりと**防御**します。
- トラブル時にはサポートセンターが異常を**検知**し、ウイルス駆除等の**対処、回復**をサポートします。

防御

検知

対処・回復



※訪問サポートは追加費用を頂く場合がございます。

多層防御でブロック！ 安心のサポート

ポイント 1

多層防御

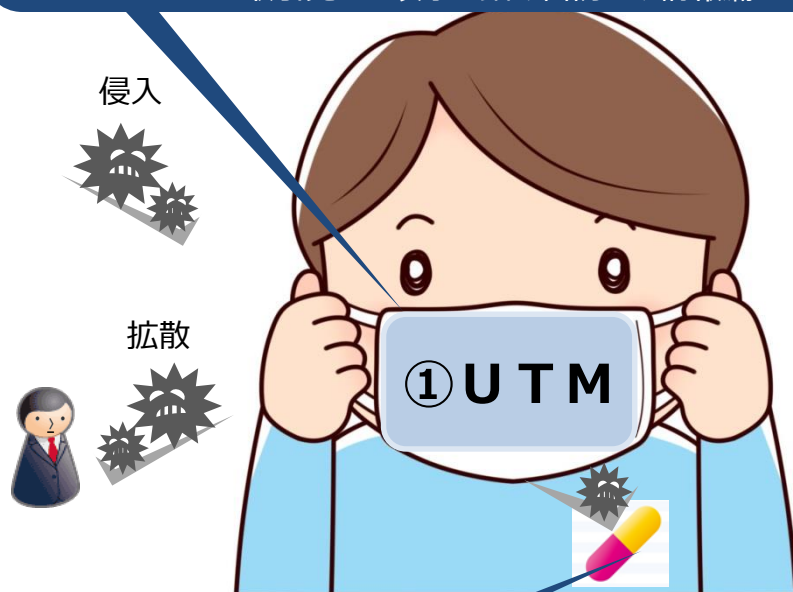
① マスク≡ゲートウェイセキュリティ (UTM)

入口対策：ウイルスの体内への侵入をブロック

⇒不正通信、ウイルス侵入防止等

出口対策：ウイルスの拡散

⇒取引先への攻撃の踏み台防止、情報漏えい防止等



② インポイントセキュリティ

② ワクチン≡エンドポイントセキュリティ

入口対策：ウイルス感染を防ぐ⇒ウイルス検知・駆除等

防御

ポイント 2

充実のサポート体制

③ 遠隔サポート



監視・検知

運用監視レポート

セキュリティ相談

④ 訪問サポート (オプション)



通信環境の復旧

検知・対処・回復

楽々

担当者様の負担を軽減！

異常検知時はセンターからメール/電話でご連絡

9:00-21:00まで営業
土日祝日も対応 ※年末年始除く

通知メールは24時間
365日送付

リモート
サポート



↑管理画面

管理画面を通じて遠隔で駆除支援等を行います。

OS初期化作業が必要な際は、現地作業を代行

訪問
サポート

24時間
365日訪問

年1回
最大100台
無償対応※

機器故障修理



OS初期化作業

全国約200カ所の保守拠点がサポートします。







※指定のゲートウェイセキュリティをご利用されていない場合は有償になります。

※無償台数の上限はご利用の機種により異なります。





※機器故障対応は24時間365日対応しますが、OS初期化作業は9:00-17:00の対応となります。

【参考】ゲートウェイセキュリティ 防御機能一覧

<cloud scanサーバでの提供機能>

機能名	提供内容
 不正プログラム対策	ゲートウェイセキュリティ本体でのエンジン検索とクラウドデータを利用した検索を使い分け、高い不正プログラム検出率を維持しながら高スループットを実現します。
 メールセキュリティ対策	E-mailレピュテーションとゲートウェイセキュリティ本体のエンジンを利用し、不正プログラム付メール、スパムメールをブロックします。 また、コンテンツフィルタリングにより、不適切なメールを検知します。
 機械学習型検索（添付ファイル）	メール攻撃で侵入する添付ファイルを、A I 技術を利用して特徴を元に判断することで、従来の検出技術では検出できなかった未知のマルウェアにも迅速に対処することができます。
 Webレピュテーション	約16億URLの情報を持つトレンドマイクロ社のデータベースを利用して、接続先URLをリアルタイムに評価します。
 URLフィルタリング	約80のカテゴリでURLをフィルタリングします。 ブラックリスト/ホワイトリストの設定も可能です。
 E-mailレピュテーション	スパムメール対策として使用します。 受信メールメッセージのIPアドレスを検証して、スパムおよびフィッシングの送信元を特定し阻止します。

<UTM本体での提供機能>

機能名	提供内容
 アプリケーションコントロール	1,000以上のアプリケーションをサポートし、利用可否を制御できます。 一部アプリケーションでは、機能単位の制御も可能です。
 侵入防御（IPS）	6500を超えるルールにより脆弱性対策が可能です。
 ファイアウォール	攻撃をブロックし、適切なアプリケーショントラフィックのみを通過させます。
 コンテンツフィルタ (マイナンバー情報漏えい防止機能)	メールのコンテンツフィルタリングを行います。 「マイナンバーによるフィルタ」をONにすると、メール本文に記載されたマイナンバーを検知することが可能です。

【参考】サポート内容詳細

機能		提供内容	
監視	①インシデント発生時の連絡 ※即時通知を保証するものではありません	内容	以下のセキュリティ脅威イベント発生時のシステム管理者への電話連絡 <ゲートウェイセキュリティをご利用の場合> ・C&Cサーバ通信検知時 ・ゲートウェイ機器電源断 <エンドポイントセキュリティをご利用の場合> ・ウィルス駆除 & 隔離不可事象発生時
		連絡方法	電話および電子メール
		提供時間	電子メールによるご連絡: 24時間365日 電話によるご連絡: 9:00から21:00 (年末年始を除く)
	②レポート機能	内容	セキュリティ脅威の検知状況をまとめたレポートの提供
		提供方法	電子メール
		提供時間	月1回配信
対処	③セキュリティに関する問い合わせ対応	内容	・セキュリティ全般に関する問い合わせ対応 ・本サービスで提供するセキュリティ対策機器やアンチウイルスソフトの機能問い合わせ ※本サービスで提供していないセキュリティ機器やアンチウイルスソフト等のセキュリティソフトウェアに関するお問い合わせ、操作支援についてはお受けすることができません。
		受付方法	電話
		提供時間	電話によるご連絡: 9:00から21:00(年末年始を除く)
	④インシデント発生時の遠隔支援	内容	・セキュリティインシデント発生端末の探索支援 ・マルウェア等感染状況の確認およびエンドポイントセキュリティツールによる駆除支援 ・未知のウィルス対策ソフトに対する専用ツールでのログ取得支援・解析 ・本サービスで提供するセキュリティ対策機器やアンチウイルスソフトの設定変更支援
		提供時間	電話によるご連絡: 9:00から21:00(年末年始を除く)
	⑤インシデント発生時の現地支援	内容	・OSリカバリ支援 ※CE50/100契約者は、1年間に1回無償で対応 (台数上限はCE50の場合50台/CE100の場合は100台まで) ※年間2回目以降は有償です。 ※ゲートウェイセキュリティ対策機能を未契約の場合は有償対応になります。
		提供時間	9:00から17:00(年末年始を除く)
	⑥ゲートウェイセキュリティ機器の故障時の交換対応 (ゲートウェイセキュリティご契約の場合)	内容	ゲートウェイセキュリティ機器の訪問による故障交換対応 ※翌営業日以降にお伺いする場合があります。
		提供時間	24時間365日

【参考】エンドポイントセキュリティ OS別機能一覧

機能		Windows	Mac OS	Android	iOS
セキュリティ対策	ウイルス対策	○	○	○	
	スパイウェア対策	○	○	○	
	Webレピュテーション	○	○	○	
	ファイアウォール	○			
	挙動監視	○			
	USBデバイスコントロール	○			
	URLフィルタリング	○			
集中管理	ポリシー管理	○	○	○	○
	管理ログ	○	○	○	○
	管理者への通知	○	○	○	○
	レポート	○	○	○	
	モバイルデバイス管理			○	○