

【保険代理店／顧客向けセキュリティ対策の提案】

Step ① NTTによる無償セキュリティ診断を受けてみよう

▼ セキュリティ対策は、企業防衛の“新しい保険”

現在、サイバー攻撃は大企業だけでなく中小企業にも深刻な被害を及ぼしています。

特にランサムウェア、標的型攻撃、情報漏えいなどのリスクは年々増加傾向にあり、被害後には企業の信用失墜、取引停止、損害賠償といった連鎖的損失が発生することもあります。

保険による「事後対応」だけでなく、**UTM等による「事前防御」**も不可欠な時代です。

セキュリティ対策イメージ

サイバー攻撃～Dos/DDos攻撃

DoS攻撃:webサービスするサーバーに攻撃
▶ 金銭目的

複数の端末から意図的に大量のパケットを送信し相手のサーバーやネットワークへ膨大な負荷を掛ける

サーバーに対するDDoS/DoS攻撃の狙いはサーバーの「サービスを妨害すること」。

マルウェア感染したPC
情報の外部流出

マルウェア／メール攻撃

標的型攻撃の多くは、マルウェア(悪意のあるソフトウェアの総称)を忍ばせたメール攻撃によって、社内の情報を持出す。

入口対策

(ファイアウォール UTM など)
マルウェア(ウイルス)が自社のネットワーク内に侵入することを未然に防ぐための対策をする。

内部対策

(EDR:PCやサーバーの状況、通信内容などを監視)
自社内使用PCネットワークを監視し、怪しい動作をするプログラムを監視・停止する。
挙動パターンノックアウトリストを設定し、そのパターンに該当するマルウェアをブロック、検知したら通知・削除などの対策をする。

出口対策

(サイバー保険+DDH BOX など)
ハッカーが情報を抜き取る際に使用するC2サーバーをリスト化し出口で阻止する。

NTT無償セキュリティ診断

こんなお悩みありませんか？



- ・インターネットの速度が遅い
- ・Wi-Fi が途切れる
- ・パソコンの動きが悪い
- ・セキュリティが不安
- ・迷惑メールが多い

1 つでも当てはまる方は、**セキュリティ診断**を受けてみませんか？

診断を受けた企業のうち
セキュリティリスクが検出されたのは **80%**

NTT のセキュリティスペシャリストが
不正アクセスやウイルス感染状況などを遠隔で診断・可視化！
【所要時間：30 分～ 60 分程度】

無料で
6 項目を
チェック！

スピード
テスト

接続機器
の確認

ウイルス
チェック

メールアドレス
流出チェック

アクセスログ
チェック

Wi-Fi の状態
チェック

▼ NTTのネットワーク無料診断を活用した提案フロー

保険提案と並行して、NTTの無料ネットワークセキュリティ診断をご活用いただくことで、顧客の潜在的なリスクを可視化し、より説得力のある総合提案が可能になります。

<NTT無償セキュリティ診断内容>

1. インターネットのアップロードとダウンロードのスピード測定
2. ルーターに接続されている機器の確認
3. メールアドレスの漏洩チェック
4. 通信ログのチェック（不正通信）
5. ウィルス感染チェック

【保険代理店／顧客向けセキュリティ対策の提案】

Step ② 診断からセキュリティ対策～UTMの導入

▼ UTM（Unified Threat Management「統合脅威管理」）

昨今、様々な脆弱性を攻撃してくるマルウェアやウイルスなどの脅威に対抗する為、複数のセキュリティ機能が必要です。

今まで主流だったファイアウォールは通信のアドレスと種類だけで防御していましたが、昨今の標的型攻撃や外部から社内PCを乗っ取る攻撃には無力です。

UTMは通信の内容までチェックするため、ファイアウォールを通過してしまう攻撃のブロックが可能です。

<ファイアウォールと何が違うのか？>

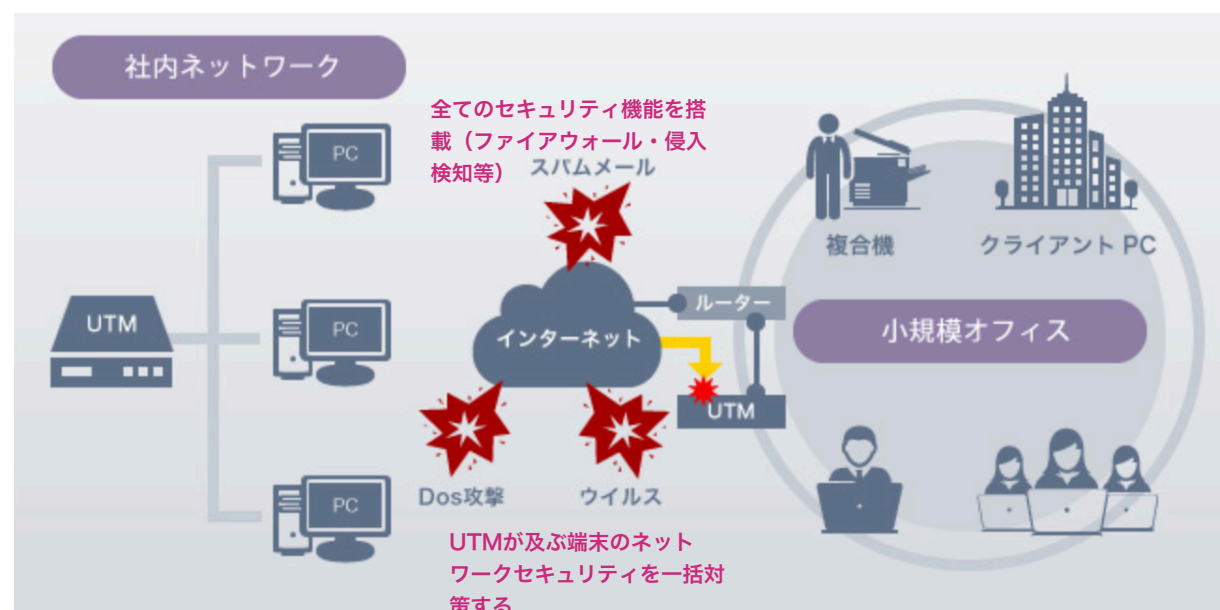
設置する場所がインターネットの出口に設置という意味では似ていますが、内部での動作（役割）は全然違います。

最も異なる点は、ファイアウォールは内部からの通信をほぼ全て許可しているため、ニュースなどで騒がれている「バックドア型」の侵入には効力を発揮しないのです。

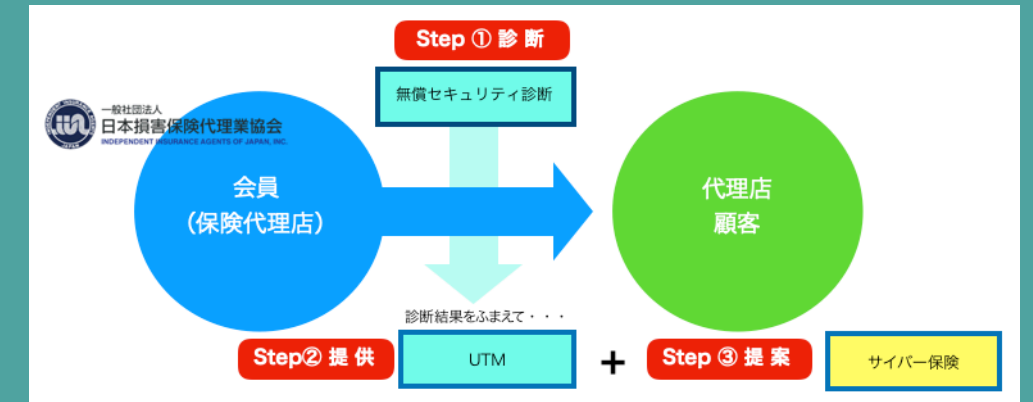
UTMは内部から外部に対しての通信も監視しており、万が一バックドアを設置されても不正アクセスをブロックします。

ファイアウォールは通信の内容までは把握できないが、UTMは危険なWebサイトへの通信を遮断したり、ファイル交換ソフトの通信を禁止するなど、昨今危険といわれている通信の制御が可能です。

<UTMのイメージ>



UTMの提案フロー



【提案フロー】

- 1 NTTの無料ネットワーク診断のご案内
→ 現状のセキュリティリスクを“見える化”
- 2 診断結果に基づき、UTM機器導入の必要性をご説明
- 3 UTM機器の御見積をご提示
- 4 保険代理店様からサイバー保険をご提案

▼ 保険とセキュリティの“両輪”提案で差別化

- ▶ NTT診断 → リスクの可視化
- ▶▶ 日本メディアシステム → セキュリティ機器の提案

Step ③ ▶▶▶ 保険代理店 → サイバー保険の提案

このような3者連携によるトータルサポートは、顧客への信頼性向上・解約防止にもつながります。

ご紹介や共同提案など、ご興味ございましたらお気軽にお声がけください。資料・提案書のご提供も可能です。

必要に応じて、この文面を営業資料やメール案内用に再フォーマットもできます。ご希望あればお知らせください。

【保険代理店／顧客向けセキュリティ対策の提案】

Step ② 診断からセキュリティ対策～裏口対策



裏口対策 × 横感染防止とは？

会社のネットワーク環境では・・・

社内では「業務用ノートPC」や「タブレット」「スマホ」などで、WiFiを通してインターネットに接続しています。

一部の端末（例：従業員スマホ、来客用タブレットなど）では、セキュリティレベルが低いデバイスで、接続している可能性があります。

Android は世界のスマホの約7割を占める OS シェア（世界）

Android 約70～75%

iOS (iPhone) 約25～30%（※地域差、年度により多少前後する。）

- ▶日本ではiPhoneのシェアが高い（50%以上）が、
- ▶世界全体では圧倒的にAndroidが主流

サイバー攻撃者の心理

「10万人にウイルスをばらまくなら、Androidを狙う方が効率がいい！」

→ 開発コストが安く済むし、感染も広がりやすい

その結果

- ▶Android向けのマルウェア・ウイルスが大量に作られる
- ▶Google Playにも偽アプリが紛れ込むことがある
- ▶個人だけでなく企業の業務端末にも被害が波及

このように感染端末から安全PCへ感染が展開するリスクが生じる

そこでサブゲートAPの出番！

サブゲートAPは「部屋を分けるドア」のような存在です

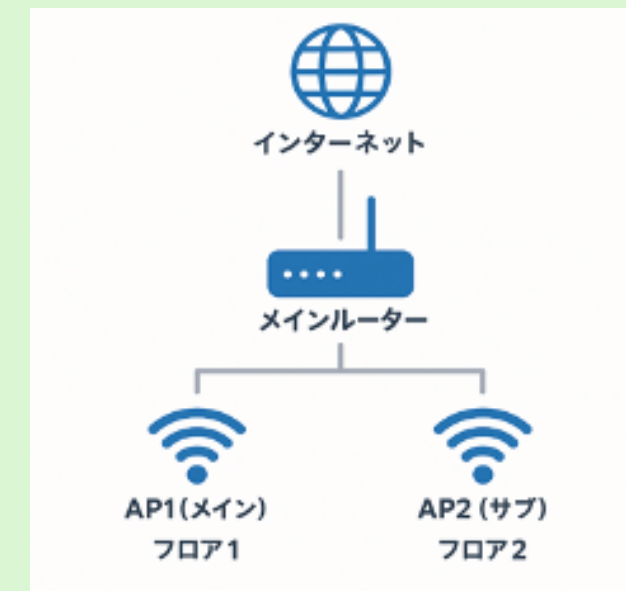
- ・信頼できる端末（業務PC）→メインAPへ接続
- ・外部性がある端末（貸出タブレットなど）→サブゲートAPへ接続
ネットワークを分離（VLANなどで）します。

🏠 家にたとえると・・・

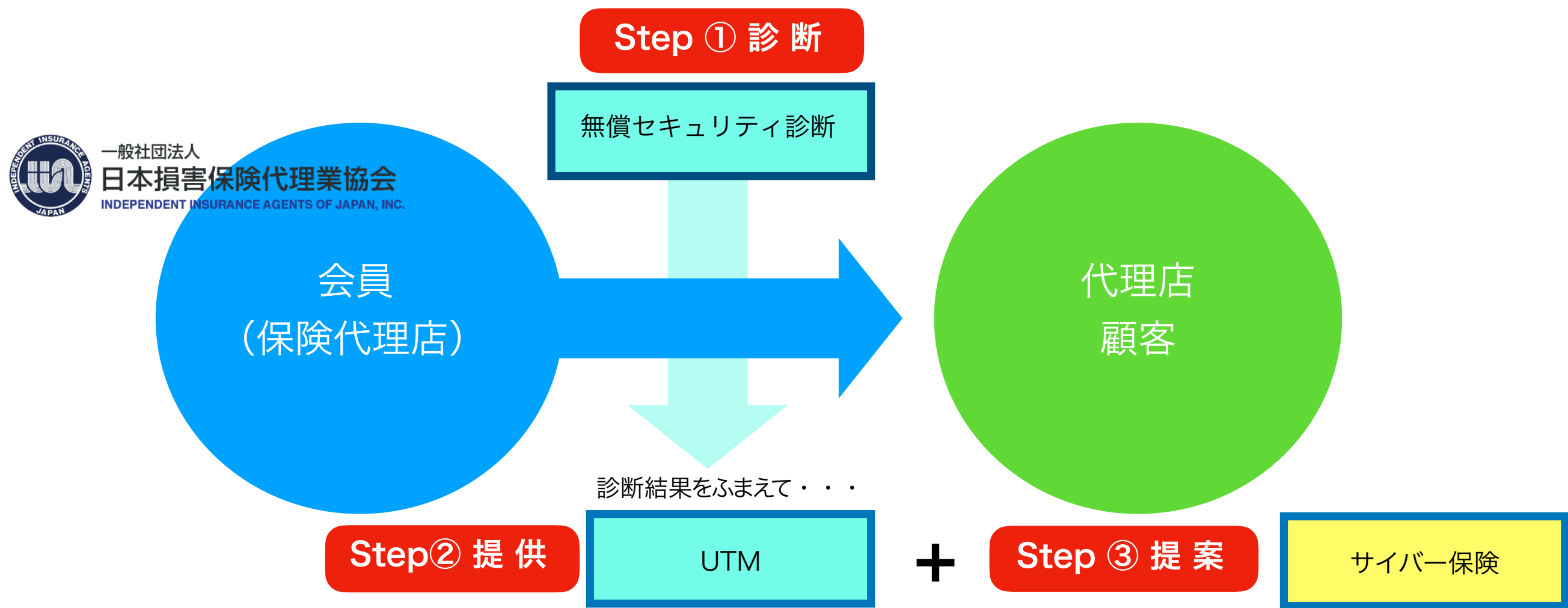
- ・家の「リビング」は家族だけが入れる場所（業務ネットワーク）
 - ・「玄関先」は宅配や来客が通るだけの場所（ゲストネットワーク）
- サブゲートAPは、この玄関先（ゲストエリア）専用のWi-Fi出入口をつくるようなイメージです。

まとめ

- ・サブゲートAPは「Wi-Fiの裏口専用通路」
- ・信頼できない端末を完全に別の空間（ネットワーク）に隔離
- ・結果として、社内ネットワークの安全を守る盾になる



【保険代理店／顧客向けセキュリティ対策の提案】



【UTM 販売手数料について】				
対策箇所	販売価格	機器代金	手数料（7.5%）	月額リース料（6年）
出入口全体対策	¥ 1,154,000—	¥ 998,000—	¥74,800—	約 ¥18,000—
入口対策のみ	¥ 553,000—	¥ 545,000—	¥40,875—	約 ¥9,000—
裏口対策のみ	¥ 733,000—	¥ 613,000—	¥45,975—	約 ¥12,000—