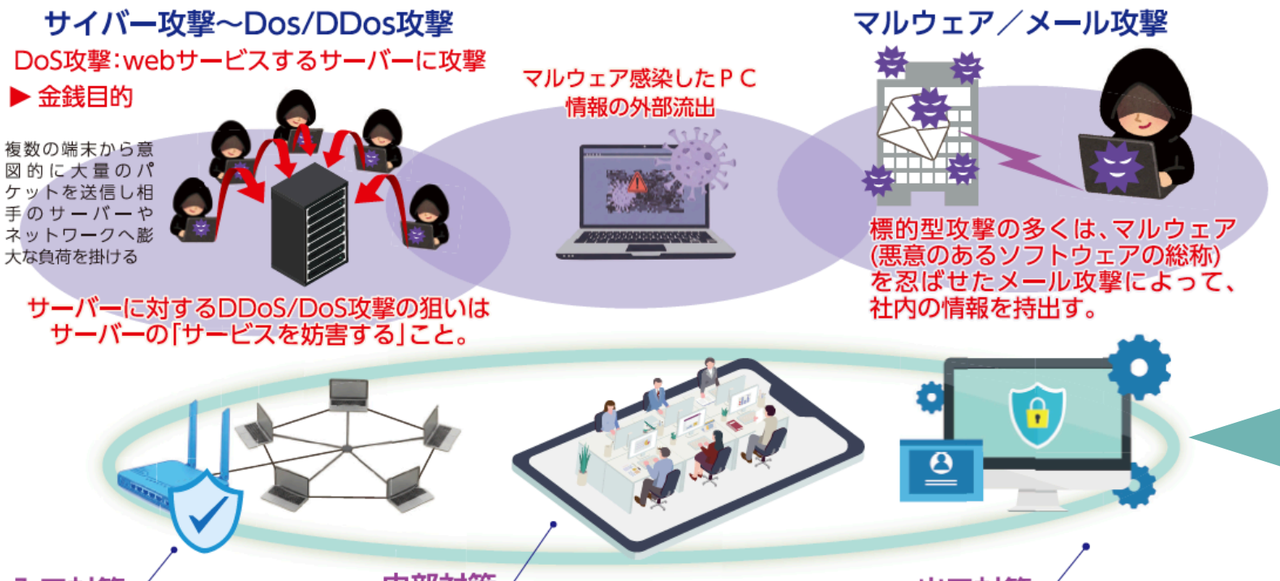
【保険代理店／顧客向けセキュリティ対策の提案】

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少なくありません。
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



NTT無償セキュリティ診断

▼ 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

日本メディアシステム株式会社
☎0120-050-530
https://www.n-media.co.jp

【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**ファイアー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、ファイアーウォールを通過してしまう攻撃のブロックが可能です。

＜ファイアーウォールと何が違うのか？＞

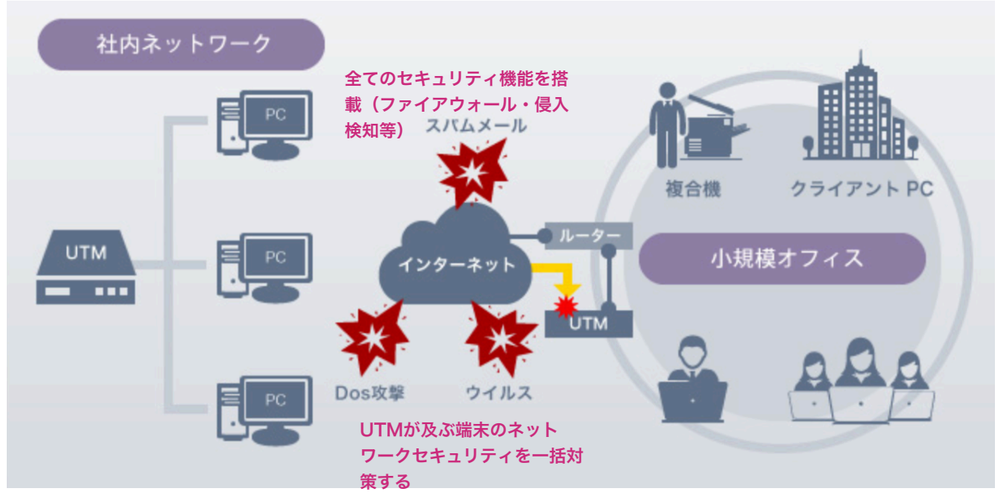
設置する場所がインターネットの出口に設置という意味では似ているかもしれませんが、内部での動作（役割）は全然違います。

最も異なる点は、ファイアー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。

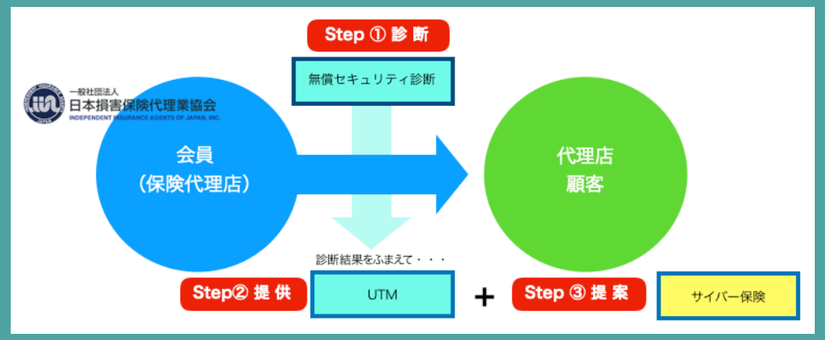
UTMは内部から外部に対しての通信も監視しており、万が一バックドアを設置されても不正アクセスをブロックします。

ファイアー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。

日本メディアシステム株式会社 ☎0120-050-530
https://www.n-media.co.jp

【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

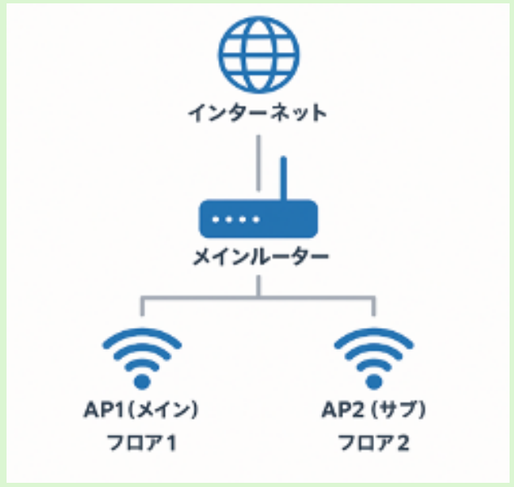
サイバー攻撃者の心理
「10 万人にウイルスをばらまくなら、Android を狙う方が効率がいい！」
→ 開発コストが安く済むし、感染も広がりやすい
その結果
▶Android 向けのマルウェア・ウイルスが大量に作られる
▶ Google Play にも偽アプリが紛れ込むことがある
▶個人だけでなく企業の業務端末にも被害が波及

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。

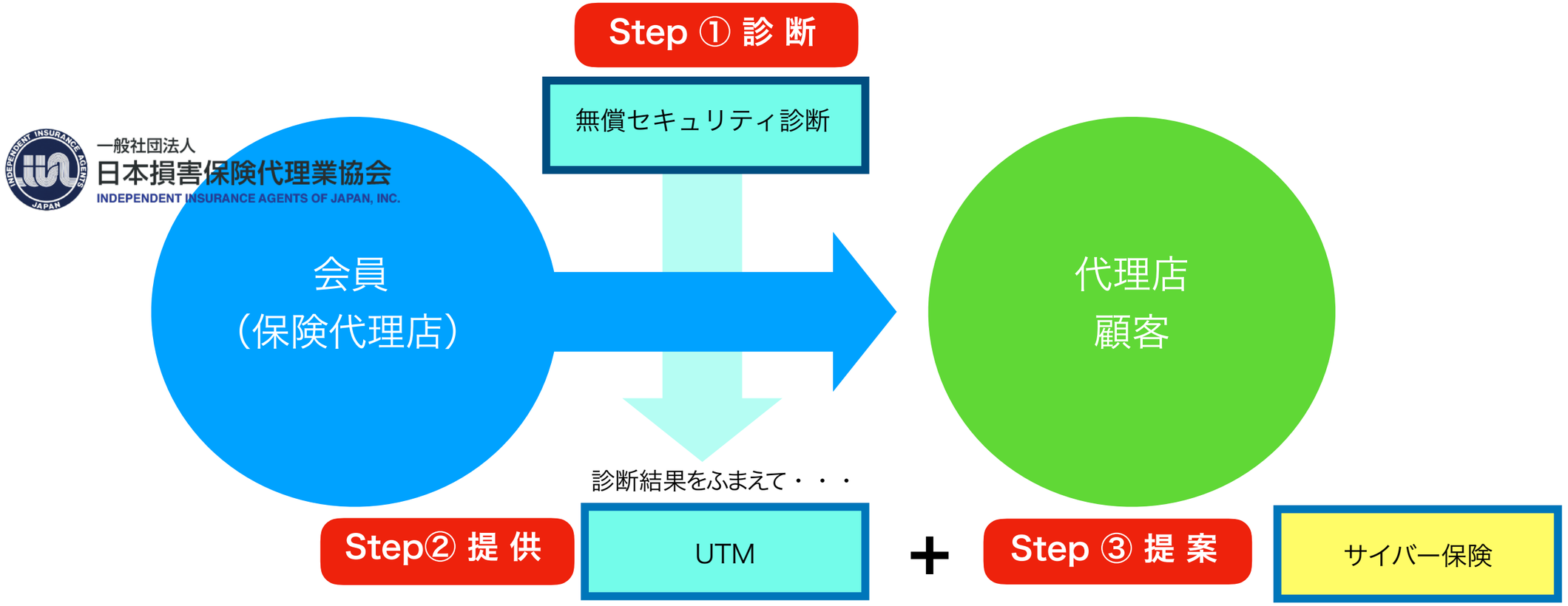
🏠 家にたとえると…
・家の「リビング」は家族だけが入れる場所（業務ネットワーク）
・「玄関先」は宅配や来客が通るだけの場所（ゲストネットワーク）
サブゲートAP は、この玄関先（ゲストエリア）専用のWi-Fi 出入口をつくるようなイメージです。

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



日本メディアシステム株式会社 ☎0120-050-530
https://www.n-media.co.jp

【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―