Multi Security

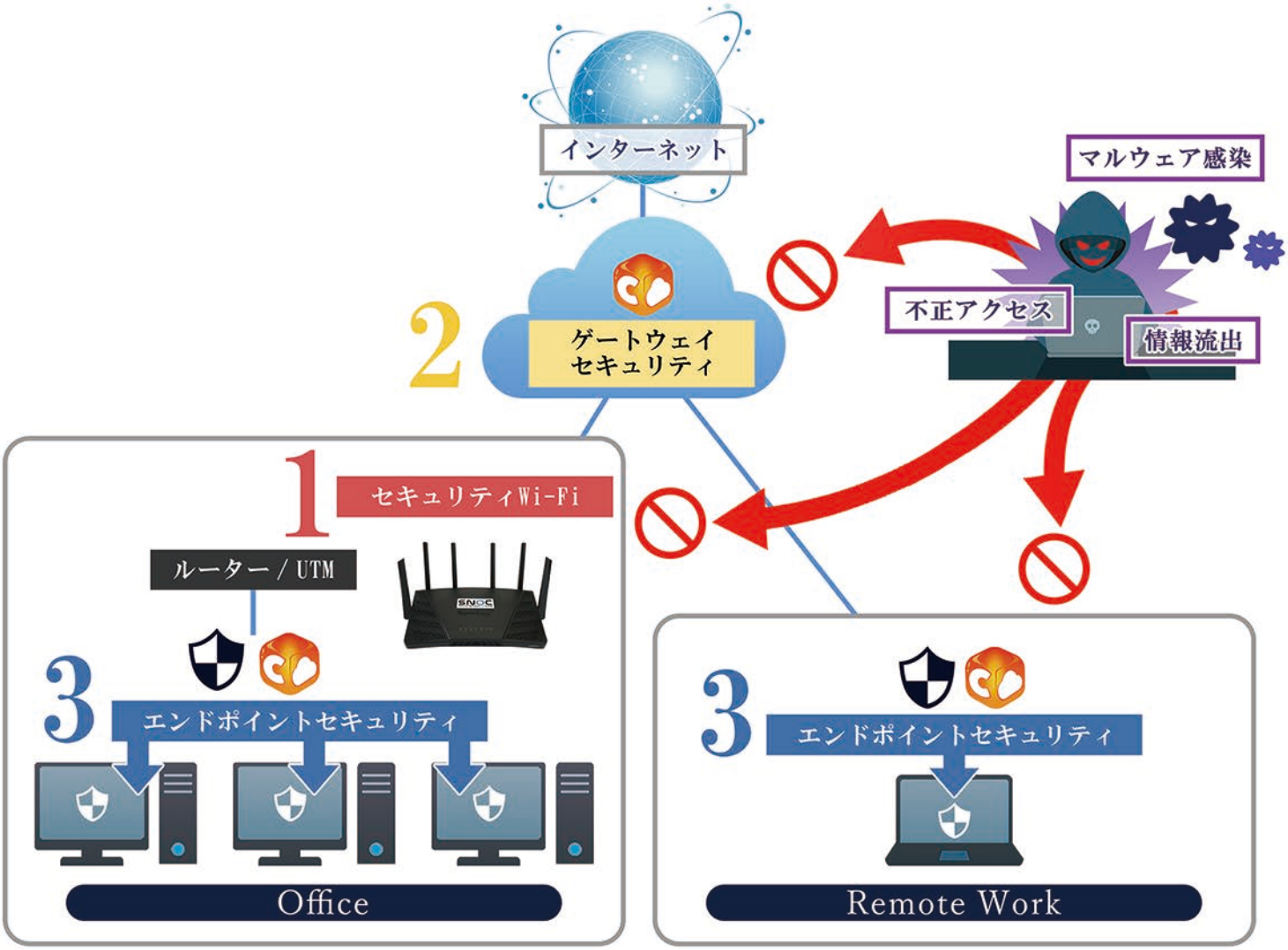
SNOC

Secure Network On Cube

超高速かつ多層防御で安全なネットワーク環境を実現

マルチセキュリティ

SNOCは、中小企業様に特化したセキュリティWi-Fiとゲートウェイセキュリティ、エンドポイントセキュリティで構成されてます。



多くの企業では在宅勤務やリモートワークが普及しつつも、社内ネットワークが必要なくなるというケースはまだ多くはありません。 企業では、ニューノーマルな働き方と従来のオフィスでの業務を併用する形に変化しています。そうした状況に合わせて既設のUTMを用いた境界型防御を維持しつつ、 在宅勤務やリモートワークへの対応としてゲートウェイセキュリティや、 エンドポイントセキュリティの導入などハイブリットな環境をSNOCで実現します。

各種機能

セキュリティWi-Fi

- WPA3対応
- Firewall/IPS
- VPNルーター
- 悪意のあるパケットをブロック
- 脅威データベースの更新
- クラウド管理による保守

ゲートウェイセキュリティ

- WEBプロキシサーバ
- ファイアウォール機能
- アンチマルウェア機能
- SSLインスペクション機能
- URLフィルタリング機能

エンドポイントセキュリティ

- エンドポイントセキュリティ
- アンチマルウェア機能
- ファイアウォール機能
- ソフトウェアアップデート機能
- デバイス制御

セキュリティWi-Fi

SNOCは、高速な無線接続と
ネットワークセキュリティを
併せ持ち、弊社独自の
セッティングと連動したサポートによって
より安心安全に利用することができます。

安定したWi-Fi

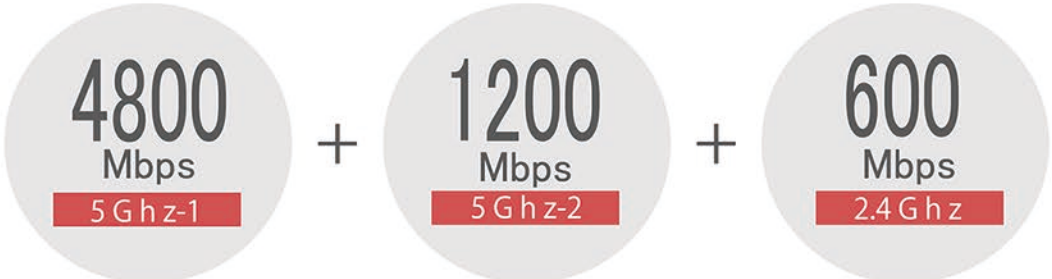
Wi-Fi6

通信速度の向上により、インターネットはもちろんリアルタイム性を求められるオンライン会議もスムーズに接続可能。
接続台数の増加による通信の不安定さも解消されます。

OFDMA（直交周波数分割多元接続）と呼ばれる技術が採用されておりWi-Fiルーターに
複数の端末が接続していても安定した通信を実現

トライバンド

2.4GHz 帯と 2 つの 5GHz 帯により、端末台数の増加によるネットワーク負荷に強く同時接続時の速度低下も軽減。



エンタープライズ向けのハイレベルなセキュリティ機能搭載

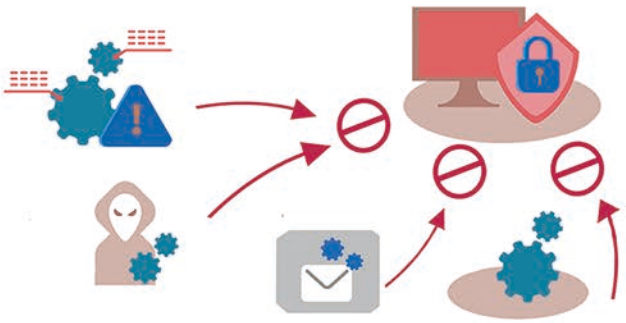
WPA3

最新の通信暗号化技術である WPA3 に対応。機密情報や個人情報など、重要性の高い情報を保護します。

Threat Prevention

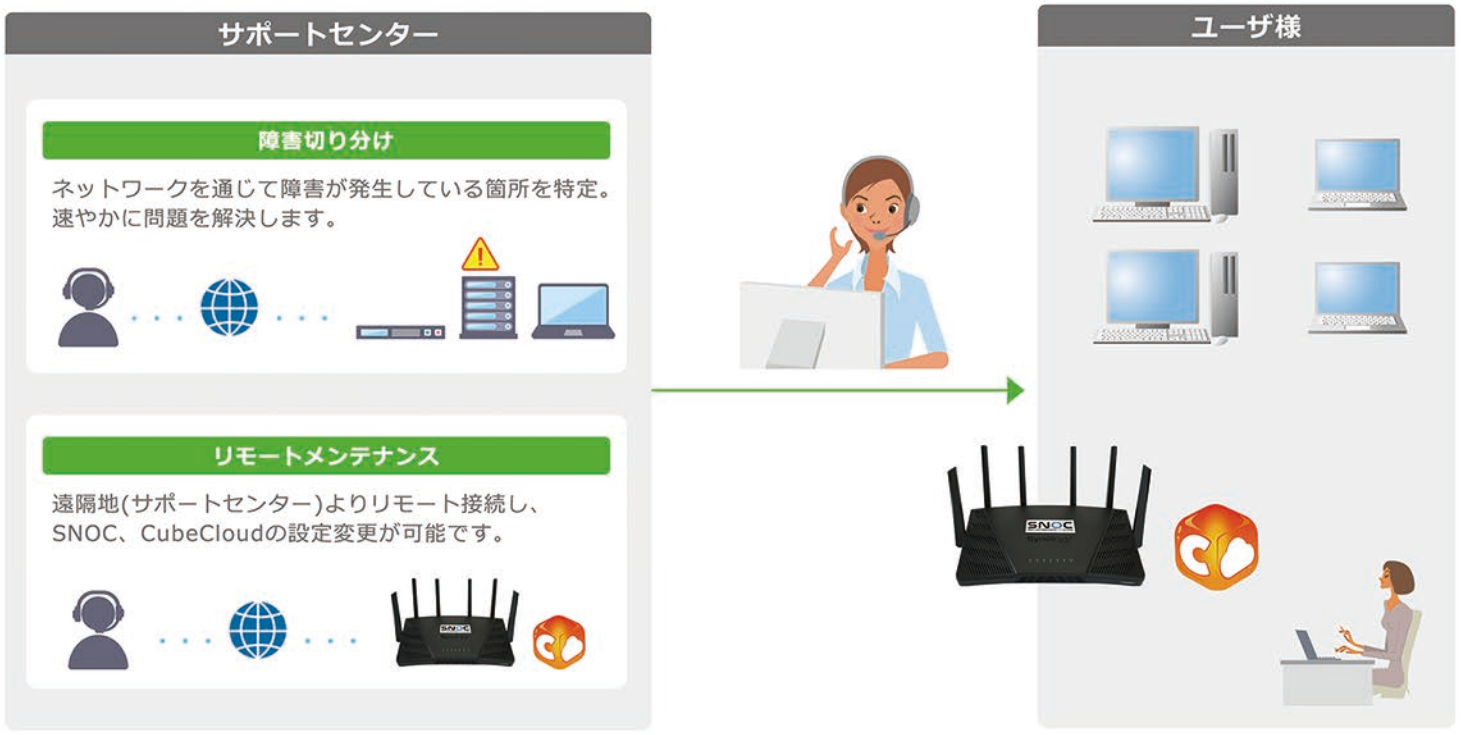
Threat Prevention は、SNOC や、その下位のデバイスのネットワーク セキュリティを以下の方法で動的に保護します。

- ✓ **インターネットトラフィックを検査し、悪意のあるパケットを検出してブロック**
  脆弱性攻撃、ウイルス、スパイウェア等をまとめて検査する
- ✓ **ネットワークイベントを記録し、悪意のあるソースに関する統計的分析を提供**
  重要度の高いイベントを表示
  アクセス場所や日時も指定して確認できる
- ✓ **アラート通知を提供**
- ✓ **手動および自動更新を許可してネットワークセキュリティを強化**



リモートによるサポート体制

導入後も安心してご利用いただくため専門スタッフによるサポートサービスを展開
管理者がいなくても故障相談や設定変更などの対応が可能

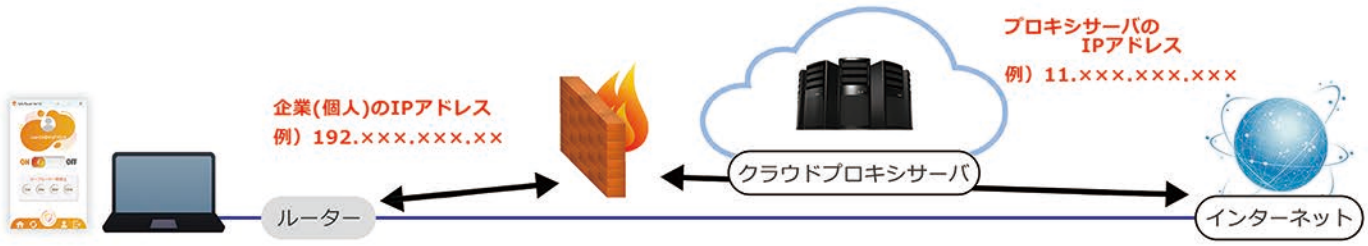


ゲートウェイセキュリティ

CubeCloudを利用することで、外出先や自宅でもオフィスと同等のセキュリティ環境が再現可能となります。

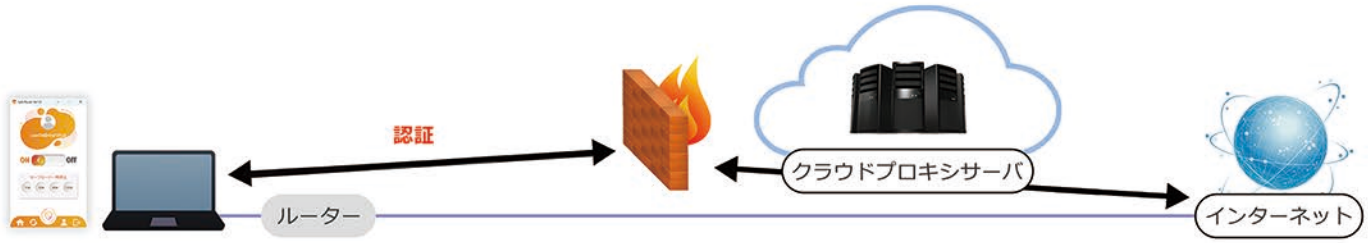
WEBプロキシサーバ

プロキシサーバの使用により、企業(個人)ではなくプロキシサーバのIPアドレスのみが送信されることになります。企業(個人)のIPアドレスが特定されにくくなり、悪用やサイバー犯罪の攻撃対象となる可能性を未然に防止します。



デバイス認証

利用のデバイスに対してそれぞれID・パスワードを発行して登録された端末で認証を行うことによりオフィス、自宅、外出先問わず安心してWEB閲覧できるようになります。なりすましや許可されていないデバイスでの接続を制限することができます。



SSLインスペクション

HTTPSがWEBの大半を占めている今、避けては通れないSSLに対してのセキュリティ対策としてSSLインスペクションでSSL通信を見逃しません。

エンドポイントセキュリティ

ヒューリスティック・行動分析（振る舞い検知）

シグネチャーのデータベースに頼らずに、巧妙なマルウェアを特定しブロックします。

リアルタイム脅威情報

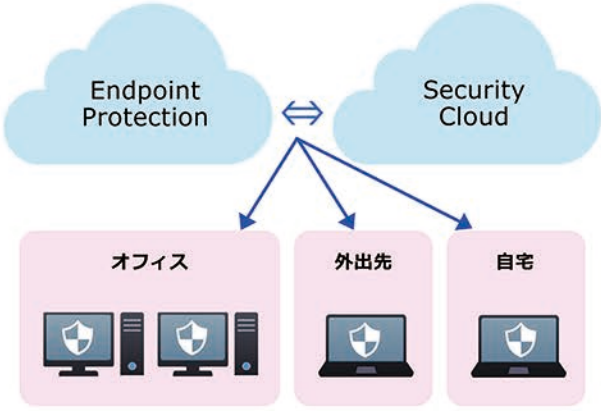
独自のクラウドベースで新しく出現してくる脅威を特定、分析、防止します。

マルチエンジン構成

悪質な攻撃の特徴、パターン、傾向をさらに広い範囲で検出します。

デバイスの脆弱性を防ぐアップデート

アップデートの欠落をスキャン、欠落しているパッチをもとに脆弱性のレポートを作成し、アップデートを自動的にないしは手動で行います。



デバイスの一元運用管理

ロケーションフリーにて運用が可能となります。本社や拠点、外出先、自宅などどこでも、インターネット接続ができる環境であれば、最新脅威情報やセキュリティクラウドとの連携により、未知のウイルス検知、振る舞い検知防御が可能となります。また各デバイスのWindowsアップデートやOffice、ブラウザ、Adobeなどのアプリケーションでの脆弱性対策に有効化なアップデート管理が一元的に運用できます。

アプライアンス仕様

【ハードウェア】

型名	SNOC
CPU	クアッド - コア 1.8GHz
ハードウェア L7 エンジン	あり
メモリ	DDR3　1GB
アンテナタイプ	2T2R + 4T4R 無指向性ハイゲイン ダイポール (2.4GHz/5GHz)
LAN ポート	・2.5GbE (RJ-45) x 1　・Gigabit (RJ-45) x 3
WAN ポート	・Gigabit (RJ-45) x 1　・2.5 GbE (RJ-45) x 1 (Dual WAN)
外部ポート	USB 3.2 Gen 1 (タイプ A) x 1
サイズ (H×W×D)	175 mm x 320 mm x 200 mm (アンテナ直立状態)
重量	1.6 kg
AC 入力電源電圧	100V ～ 240VAC
消費電力	・11.11 W (アクセス)・6.77 W (無作動)
電源周波数	50/60 Hz, 単相
動作温度	5℃～ 40℃ (40°F ～ 104°F)

【無線仕様】

ワイヤレス規格	・IEEE 802.11 a/n/ac/ax 同時トライバンド ・802.11k/v/r ローミングサポート
最大データ速度	・2.4GHz：最大 600Mbps　・5GHz-1：最大 4800 Mbps　・5GHz-2：最大 1200Mbps
Wi-Fi 暗号化	WPA/WPA2-Personal、WPA/WPA2-Enterprise、WPA2/WPA3-Personal、WPA3-Personal/Enterprise、 Wi-Fi Enhanced Open (OWE)、Wi-FiProtected Setup (WPS) 2.0

【システム要件】

エンドポイントセキュリティ	Windows　10, 11 MacOS　13, 14, 15
ゲートウェイセキュリティ	Windows　10, 11

※各 OS のサポート終了に伴い、予告なく終了する可能性がありますのでご了承ください。

株式会社AUS
〒135-0023
東京都江東区平野2-16-12
TEL 03-5875-8255　FAX 03-5875-9770
URL https://www.aus-inc.co.jp/

■お問い合わせ先

202404