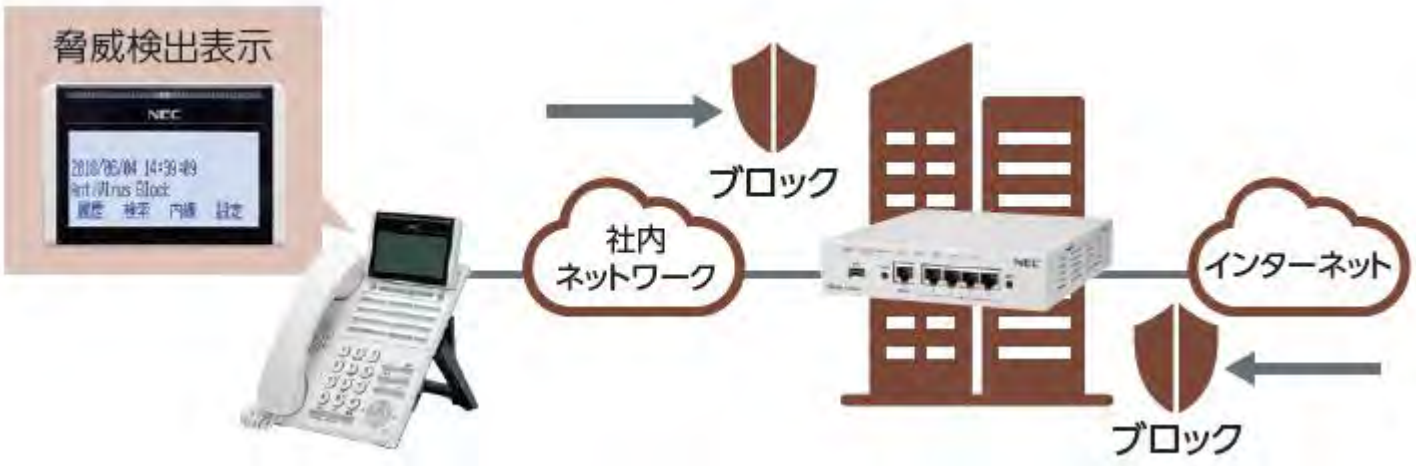
サイバーセキュリティ対策　(Aterm SA3500G)

セキュリティアプライアンス Aterm SA3500G

セキュリティアプライアンスAterm SA3500Gと連動させることで、脅威検出/ファームウェアアップデート/ライセンスの付加情報をファンクションボタンに表示でき、機器の状態を手元の多機能電話機で把握することができます。



POINT 2

・多機能電話機との連動で、よりわかりやすく運用することができます
・オフィスの出入口のセキュリティ対策も含め、安全なネットワーク環境をトータルで提案いたします

参考

セキュリティアプライアンス Aterm SA3500G

●セキュリティアプライアンス Aterm SA3500Gの特徴

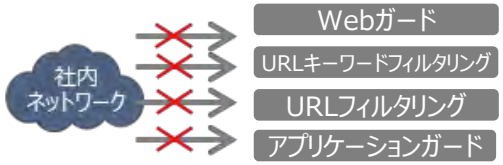
Aterm SA3500Gは、社内ネットワークとインターネット間のトラフィックを監視し、危険な通信を遮断することで、外部からの進入や攻撃を防ぎます。一般的なUTM製品では動作させると通信速度が大幅に遅くなるものがありますが、SA3500Gは高セキュリティエンジンで約700Mbps※を実現し、業務に影響なく快適に運用できます。

【サービス内容や詳細はこちら】
https://www.necplatforms.co.jp/product/security_ap/

特徴①　充実のセキュリティ機能

①**外部**からの脅威をブロック！

②**内部**からの脅威をブロック！



特徴②　快適通信

不正侵入防止やアンチウイルスを機能させても高速セキュリティエンジンを実現します。

約700Mbps※

特徴③　カンタン設置

既存ネットワークの構成を変えることなく、カンタンに設置することが可能です。

※当社、試験環境測定値

サイバーセキュリティ対策　(NA1000シリーズ)

無線LANアクセスポイント　NA1000シリーズ

高速で安定した無線LANの構築・運用を柔軟かつ容易に実現できます。一般的なパスワードによる接続認証等を使った対応に加え、無線LAN経由での不正侵入や不適切な設定による接続を検知・防止する「WIPS機能」も搭載し、社内ネットワークへの無線LANによる不正侵入や盗聴の被害を防ぎます。

POINT 2

・安心できる無線LAN環境を手軽に構築できます
・安全なネットワーク環境をトータルで提案いたします

参考

無線LANアクセスポイント　NA1000シリーズ

●無線LANアクセスポイント　NA1000シリーズの特徴

優れたコストパフォーマンスで、安心できる無線LAN環境の構築を実現する導入・運用が容易な法人向け無線LANアクセスポイントです。

【サービス内容や詳細はこちら】
http://www.necplatforms.co.jp/product/na/

特徴①　安心できる無線LAN環境構築

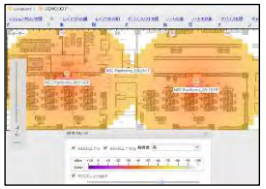
業界トップクラスのWirelessIPS機能で無線LANを見える化し、
不正アクセスなどの脅威をブロックします。

特徴②　優れたコストパフォーマンス

優れた通信性能を低価格で提供します。
学校など40台以上の端末が同時に接続しても安定した通信品質を保つことが可能です。

特徴③　導入・運用がカンタン

わかりやすいGUI画面から、少ないステップで設定可能です。
管理コンソールの導入で、複数台のNA1000を統合管理できます。電波範囲の見える化もでき、設置設計作業を支援します。



ヒートマップ(電波範囲の見える化)

特徴④　Made in Japan

開発・製造拠点が国内のため、素早い保守サポートが可能です。

サイバーセキュリティ対策　(不正アクセス検出オプション)

不正アクセス検出オプション

システムを経由する外線発信を監視し、規定したルールに反した異常な動作を検出。
管理者へEメールで通知することができます。さらに、管理者がEメールに返信することで当該発信を規制することができ、セキュリティレベルを高めることが可能です。

POINT 2

・専用サーバの構築が不要で、Aspire WXにライセンスの投入だけで利用できます
・電話システムに関わる脅威に対して、セキュリティを向上させることが可能です

参考　不正アクセス検出オプション　詳細

●検出・通知・規制について

①検出

検出するための監視ルールは2種類あります。
両方の監視ルールを設定することや、複数の条件を設定することも可能です。

監視ルール	効果	動作条件
特定ダイヤルの発信監視	**[不正アクセス発信]** 指定した電話番号(ex.010)等への発信を規制する。	指定した電話番号への外線発信が一定時間内に一定回数を超えて発生したかどうか。
内線の発信監視	**[なりすまし]** 内線電話機に対して発信規制をかける。	内線電話機からの外線発信が一定時間内に一定回数を超えて発生したかどうか。

②通知

不正アクセス検出オプションにEメール通知に関する設定を入れることにより、検出された時点で、Eメールが通知されます。

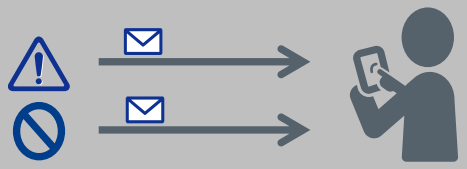
事前設定

・メールサーバ情報
・メール通知先情報
　（TO,CC,BCC,件名）
※宛先を複数指定する場合は、カンマ(,)区切りとしてください。セミコロン(;)では動作しません。

動作

Eメールは、2段階（警告・規制）の通知となります。

1段階目：警告メール
2段階目：規制メール



参考　不正アクセス検出オプション　詳細

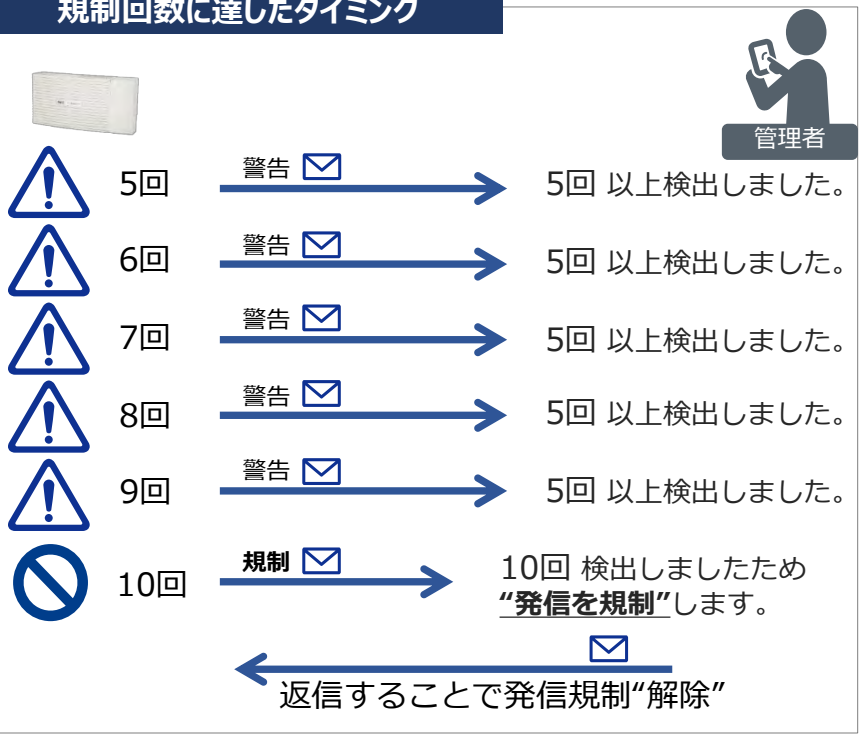
●検出・通知・規制について

③規制

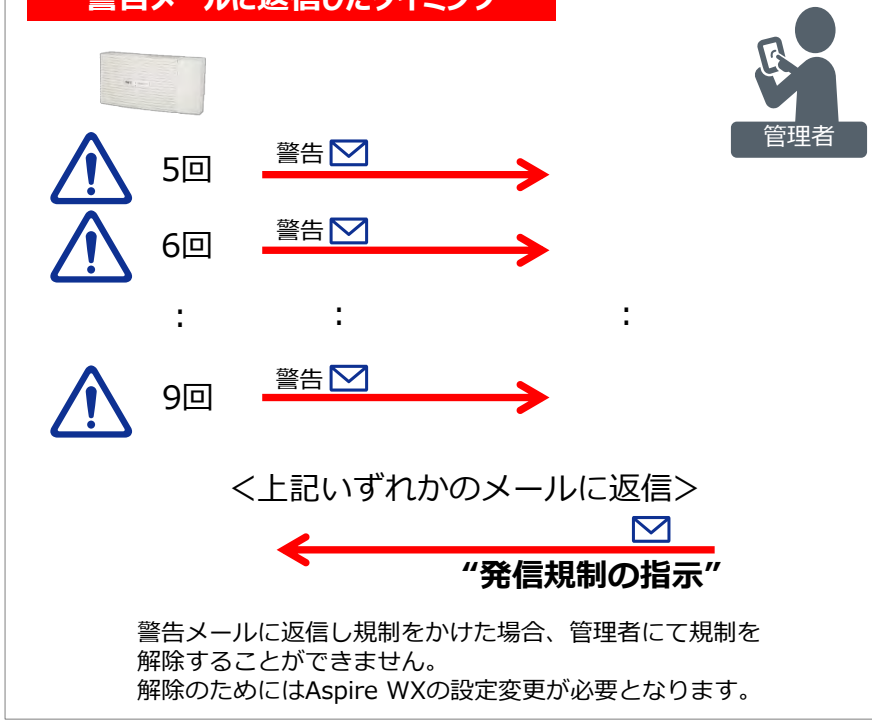
不正発信が検出され、管理者へEメールが送信された後に規制をかけますが、規制するタイミングは、2回あります。以下のように監視ルールを設定した場合の例にて示します。

<監視ルール設定例>
24時間365日監視し、“010”から始まる電話番号への外線発信が、1分間に5回発生した場合に“警告”メールを送信し、さらに5回（計10回）発生した時点で、発信の規制をかけるとともに“規制”メールを送信する。

規制回数に達したタイミング



警告メールに返信したタイミング



警告メールに返信し規制をかけた場合、管理者にて規制を解除することができません。
解除のためにはAspire WXの設定変更が必要となります。

返信メール

管理者が受信したEメールには、毎回異なる“コード”が本文に記載されます。その“コード”をもって返信を認識するため、“コード”がもれなく記載された状態で送信してください。それ以外の署名や本文が入力されていても影響はありません。