製品仕様

モデル			S903
ハードウェア	インターフェース	イーサネット	10/100/1000Base-TX×6
		その他	USB×2　Console×1
	本体(突起部を除く)	寸法(mm)	232(W)×152(D)×44(H)
		重量	約1.1kg
	環境	温度	0℃～40℃
		湿度	10～85%(結露しないこと)
	電源	形状	ACアダプター
		周波数	50/60Hz
		電圧	100～240V
	スループット(双方向)	ユーザー数	35
		NAT	1.5Gbps
		ファイアウォール	800Mbps
		アンチウイルス	722Mbps
		IPS	524Mbps
		サンドストーム	524Mbps
		アンチウイルス+IPS+サンドストーム	455Mbps
		VPN	137Mbps
		FWセッション数	160,000

ソフトウェア	ネットワーク	PPPoE
		Router
		Transparent
		VLAN(EEE 802.1Q)
		QoS(帯域制御)
		VPN(PPTP IPSec SSL)
		HA
	機能	ファイアウォール・IPS
		ヒューリスティック分析・サンドストーム
		アンチウイルス
		SSLメールインスペクション
		アンチスパム
		URLフィルター
		アプリケーションコントロール
		アンチボット
		ARPスプーフィング防御
		リモートアシスタンス
	認証	POP3 RADIUS ActiveDirectory ローカルユーザー
	ログ	レポート
		シスログ

IPSec	IPSec Auto Key	SHA-1 MD5認証
	暗号化	DES AES 3DES
	その他	IPSec Dead Peer Detction
		ネットワークネイバー参照
SSL		サーバー
		証明書
VPN	IPSecトンネル数	500
	PPTPサーバー数	200
	PPTPクライアント数	200
	SSLトンネル数	50
	SSLアカウント数	300
	VPNポリシー数	200

注意事項

・本製品は株式会社ワイズが国内販売元となっています。
・本カタログに記載されている機能、性能等は全ての条件での動作を保証するものではありません。
・製品の色調は、印刷の都合上実際とは異なって見える場合があります。
・本製品に過大な負荷がかかりますと本機性能が低下する場合がありますのでご注意ください。
・IPoE/IPoE over IPv6には対応しておりません。
・本製品の故障、誤動作、不具合あるいは停電等の外部要因によって異常な動作が発生した場合、これによって生じた損害等につきましては一切その責任を負いかねますのであらかじめご注意ください。
・記載されている会社名、製品名は各社の商標または登録商標です。
・仕様、外観は予告なしに変更する場合があります。
・本カタログ記載の内容は2026年6月現在のものです。

安全に関するご注意

ご使用の際は取扱説明書をよくお読みの上、正しくお使いください。
表示された正しい電源・電圧でご使用ください。

国内総販売元

株式会社ワイズ　東京都千代田区神田須田町2-25 GYB秋葉原6F
TEL:03-5297-5470　FAX:03-5294-7959
E-mail:sales@stealthone.net　URL:https://www.stealthone.net

認定NPO法人
世界の子どもにワクチンを
日本委員会(JCV)

お問い合わせ

STEALTHONE
UTM/NGFW

S903

未来を見据えた進化するセキュリティ機器



製品概要

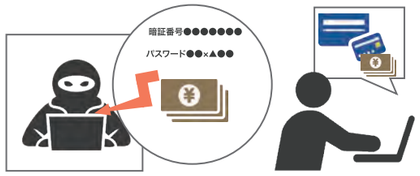
Qセキュリティって言うけど具体的にどうしたらいいの？

今やコンピュータにアンチウイルスソフトをインストールするのは常識となっています。
企業においてはコンピュータのウイルス対策だけでなく、アタック防御やWebフィルタリングなど総合的なゲートウェイセキュリティ対策が求められています。



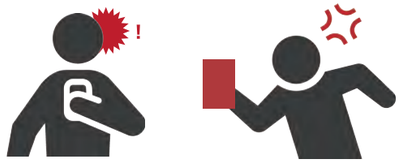
Qインターネットバンキングの不正利用が増えているようだけど・・・

インターネットを利用した便利なサービスは数多く存在します。
インターネットバンキングもその一つで、会社にいながら振込み手続きができたりと大変便利なサービスです。
パソコンに不正プログラムが侵入することで、IDやパスワードが盗まれてしまい、不正に送金されるといった被害が増加している傾向にあります。



Q情報漏えいが騒がれているけど、大丈夫・・・？

個人情報保護や企業倫理の観点から企業のコンプライアンスが注視されるようになってきました。
ゲートウェイでのコンテンツフィルタリングを活用することで、不要なウェブサイトにアクセスさせないなど、管理された環境を作ることも重要であると言われています。



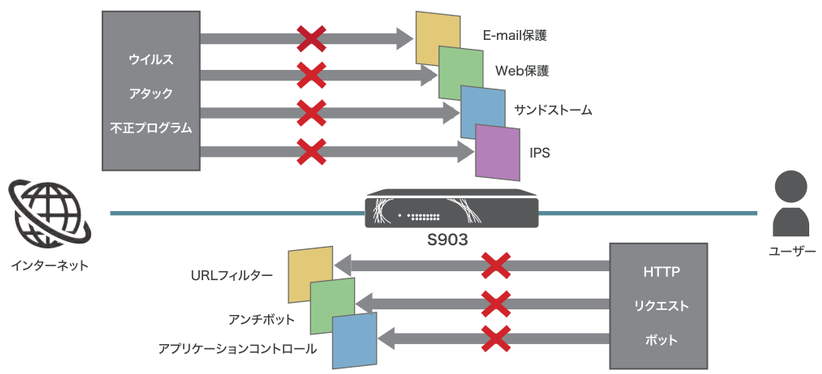
Q守るのはPCだけでいいの？

オフィスにはPCだけでなく、複合機やネットワークカメラ、スピーカーなどのIoT機器があります。
IoT機器の多くはインターネットに接続されているため、インターネットから悪意のある第三者にアクセスされる危険性があります。



S903が社内ネットワークを守る

S903は高性能で使いやすい統合脅威管理アプライアンスです。
企業において複雑化するさまざまなインターネットの脅威に対して、一つのソリューションで複数のセキュリティを展開します。脅威を未然に防ぎ、ネットワーク環境をクリーンに整えるだけでなく、強力に進化したフィルタリングエンジンによりユーザーの生産性を高めます。



全てのセキュリティをひとつに集約

ファイアウォール IPS
UTMに必要なファイアウォールだけでなく、IPSにより不正アクセスを検知します。

アンチウイルス
メール・WEB のウイルスを検出除去します。

アンチスパム
迷惑メールを自動判別します。ホワイト/ブラックリストへの登録が可能です。

URLフィルター
内部・外部データベース参照型のURLフィルター機能。
ホワイト/ブラックリストによる制御も可能です。

アプリケーションコントロール
データベース化されたアプリケーションから選択して特定のアプリケーションの通信を遮断します。

SSLメールインスペクション
SSLで暗号化されたメールをウイルススキャンすることができます。

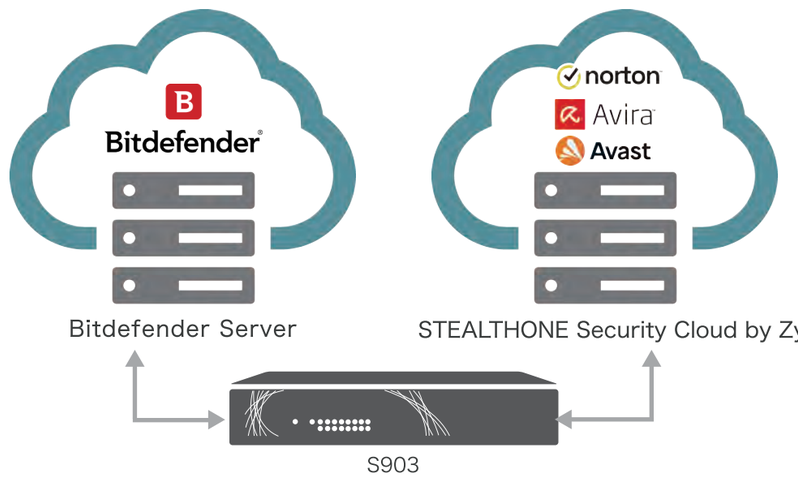
アンチボット
ボットに感染したPCがアウトバウンドに対して異常トラフィックを発生させると通信を遮断します。

ヒューリスティック分析/サンドストーム
未知の脅威に対してウイルス特有の挙動を検知し、ウイルスの発見を行います。

リモートサポート
設置されているS903に直接アクセスし、遠隔で保守対応をすることができます。

4つのセキュリティエンジンを搭載

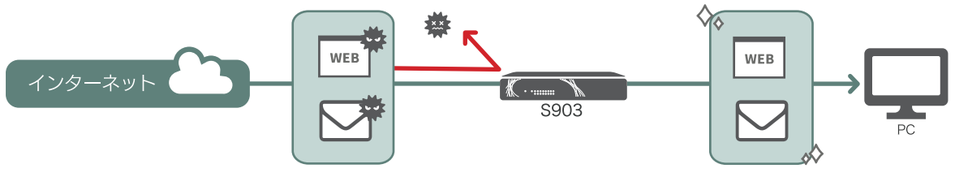
S903は、オリジナルエンジン「STEALTHONE Security Cloud by Zyxel」と「Bitdefender」を採用しています。「STEALTHONE Security Cloud by Zyxel」は「Norton」「Avira」「Avast」の協力のもとにネットワークの入口でウィルスやワーム、トロイの木馬といったマルウェアの侵入を防ぎます。



機能一覧

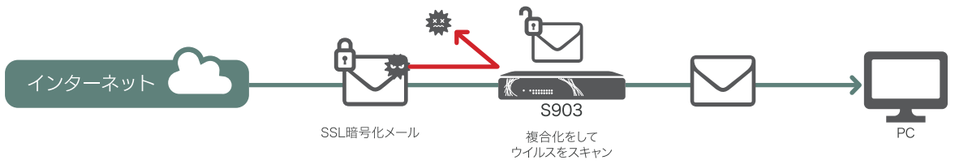
①アンチウイルス

メール・WEBのウイルスを検出駆除。
メールでは感染メールの処理方法も選択することができ、導入ネットワークのセキュリティポリシーに基づいた設定が可能です。



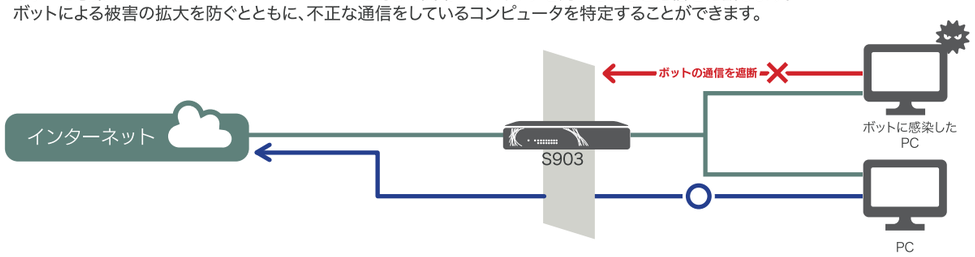
②SSLメールインスペクション

SSLで暗号化されたメールをウイルススキャンすることができます。
まず、SSLで暗号化されたメールに対してUTM内で中身を解析します。ウイルスの有無を調べた後ユーザーに安全なメールを届けます。



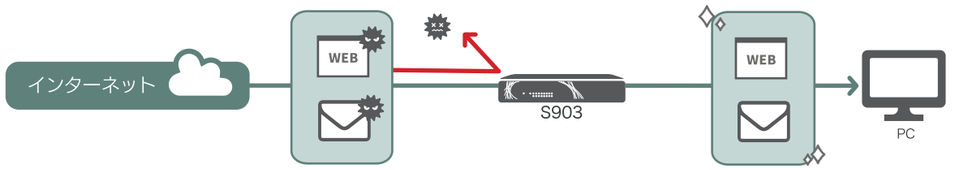
③アンチボット

ボットに感染したコンピュータがアウトバウンドに対して異常トラフィックを発生させると通信を遮断します。
ボットによる被害の拡大を防ぐとともに、不正な通信をしているコンピュータを特定することができます。



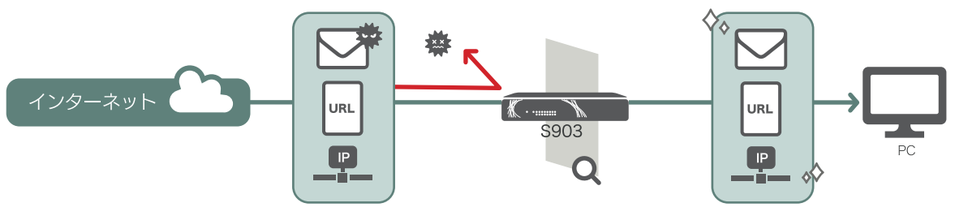
④ヒューリスティック分析

未知の脅威に対してウイルス特有の挙動を感知し、ウイルスを発見します。
また、世間に公表前の未知のウイルスや攻撃（ゼロデイ攻撃）に対しても有効です。



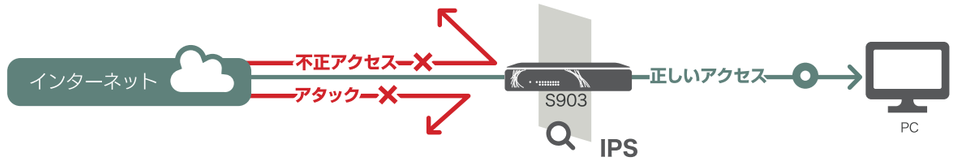
⑤サンドストーム

アンチスパム、フィルタリングおよびアンチウイルスエンジンとともに、電子メールの添付ファイル内のマルウェアや悪意あるプログラム、URL、IP等を識別します。URLまたはIPアドレスを入力して、悪意のあるプログラムやマルウェアが含まれていないかどうかをリアルタイムで確認できます。サンドボックスと比較して高速度で処理することができます。



⑥ファイアウォール/IPS

UTMに必須なファイアウォールだけでなく、IPSによって不正アクセスを検知します。
ファイアウォールによるポート制御で不正アクセスを遮断し、IPSでファイアウォールを通過したデータを検査し、不正な通信であればそのコネクションを切断します。



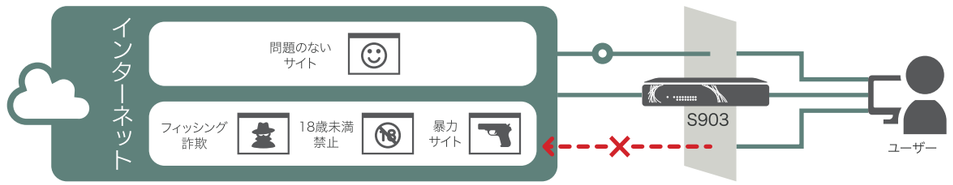
⑦アンチスパム

迷惑メールを自動判別。
ホワイト/ブラックリストへの登録が可能です。



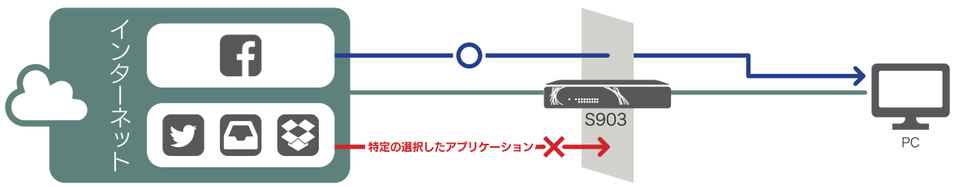
⑧URLフィルター

内部・外部データベース参照型のURLフィルター機能。HTTP通信においてアクセス可能なURLを制限します。
LIONIC社のデータベースに登録されたURLをブロックするだけでなく、ホワイト/ブラックリストによる制御も可能となっています。



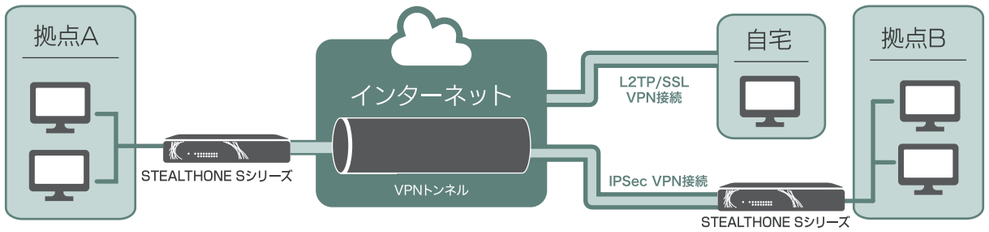
⑨アプリケーションコントロール

特定アプリケーションの通信を遮断。データベース化されたアプリケーションから選択して通信を遮断します。
WebメールやDropboxなどの情報流出にも利用されるアプリケーションにも対応しています。



⑩VPN構築

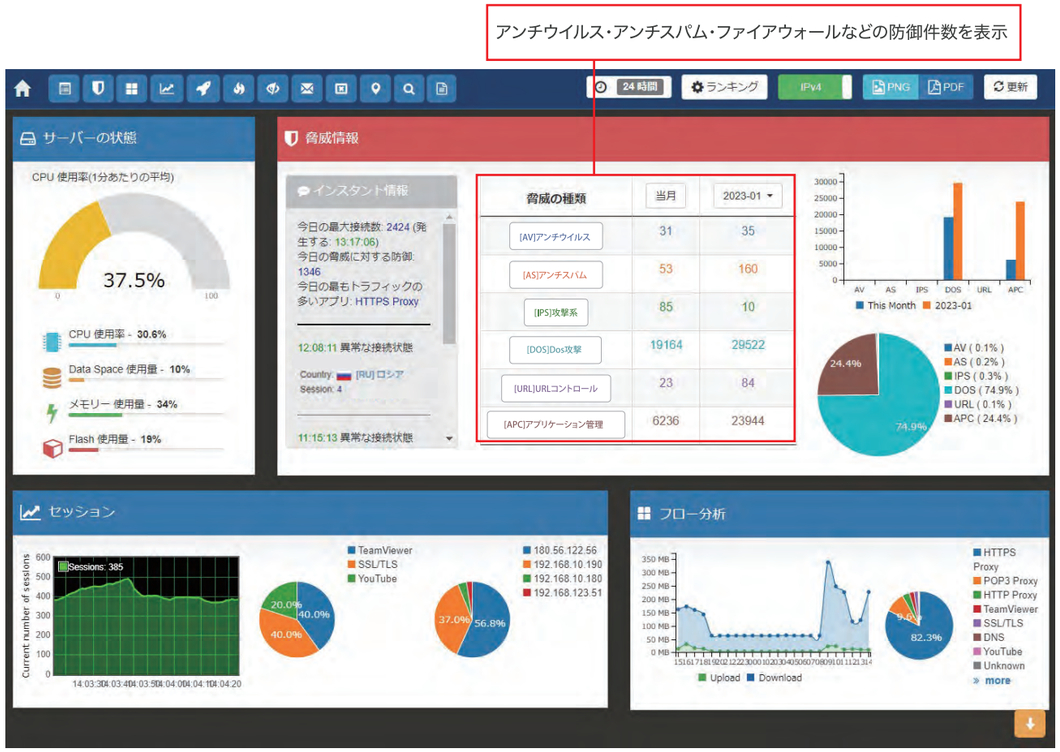
セキュアな仮想プライベートネットワーク。
PPTP・L2TP・IPSec・SSL VPNをサポートし、様々な環境で安全なVPN接続が可能となります。



機能一覧

管理画面

Webページ上で管理画面にログインすると、脅威からの防御状況を確認できます。



サイバー保険サービス

S903にはサイバー保険サービスが標準付帯されています。
サイバー攻撃等でS903を通過してウイルス感染をしてしまった場合に情報漏洩の損害賠償やシステム復旧費用として最大100万円を補償します。

第三者へ負担する
損害賠償金や争訟費用等

謝罪文作成・
送付費用等

超過勤務手当・
臨時雇入れ費用等

弁護士相談費用等

補償項目・対象となる損害		保険金の概要	1請求/1事故・および期間中のお支払い限度額	損害に対してお支払いする割合	自己負担額
サイバー保険特約条項	賠償責任	サイバーインシデントや情報漏えい、業務遂行上のシステム利用等に起因して定期された損害賠償請求について、貴社(被保険者)が負担する損害賠償金、争訴費用等	1事故あたり最大100万円(補償期間:3年)	100%	0円
	費用	・損害賠償請求が発生する恐れがある場合に、その事故に対応するため、貴社(被保険者)が支出した情報漏洩対応費用、謝罪文作成・送付費用、使用人等の超過勤務手当て・臨時雇入れ費用、弁護士相談費用等 ・サイバーインシデントのおそれが発見されたことにより、サイバーインシデント等の有無を判断するために支出した外部調査機関への調査依頼費用等	1事故あたり最大100万円(補償期間:3年)	100%	0円

万一の事故の際は下記代理店へご連絡をお願い致します。
代理店名:ブロードマインド株式会社
連絡先:0120-917-066

SOMPO 損害保険ジャパン株式会社

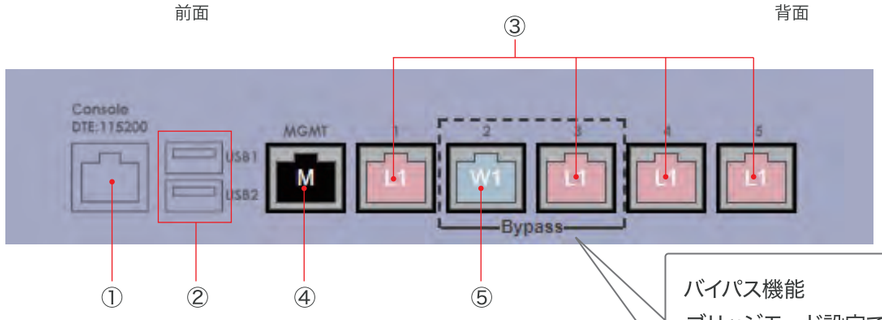
イメージ図



ハードウェア仕様



前面　　背面



①コンソールポート:メンテナンスポートです。
②USBポート:設置の際にデータのアップ・ダウンロードに使用します。
③LANポート(3のみバイパス機能有り):1000BASE-Tポートです。
④管理用ポート:管理者の設定用ポートです。
⑤WANポート(バイパス機能有り):上部ネットワークと接続をするためのポートです。

バイパス機能
ブリッジモード設定で電源が切られている場合、WANポートと直接接続される機能です。故障をしたとき、通信をバイパス(迂回)してネットワークの通信停止を回避します。