STEALTHONE

SECURED BY Avira

SGW100

IoT Security Wi-Fi Router

IoT時代を見据えた
マルチプルデバイスセキュリティゲートウェイ

About STEALTHONE SGW100

近年、ネットワークに接続することで、今までになかった便利な機能を使えるようになった機器がたくさんあります。
これらIoTと呼ばれる機器は私たちを豊かにする反面、マルウェア感染や機器の乗っ取りなどのリスクに晒されることになります。
また、IoT機器の多くはコンピュータなどと異なりアプリケーションをインストールしてセキュリティを強化することができない為、サイバー犯罪のターゲットになりやすい傾向があります。

IoT機器に対するセキュリティはどうすればいいのでしょうか。

Q.

コンピュータやサーバー以外にもネットワークに接続している機器はたくさんあるが、セキュリティが心配。

Q.

知らないうちにWi-Fiが使われていたり、知らない機器が接続されていないか心配。

Q.

ネットワークに接続している機器が多すぎて管理が大変。手間を減らして一括管理がしたい。

A.

STEALTHONE SGW100は、
IoTセキュリティに特化したWi-Fiルーターですので、
そういったお客様に
便利と安心をお届けします。

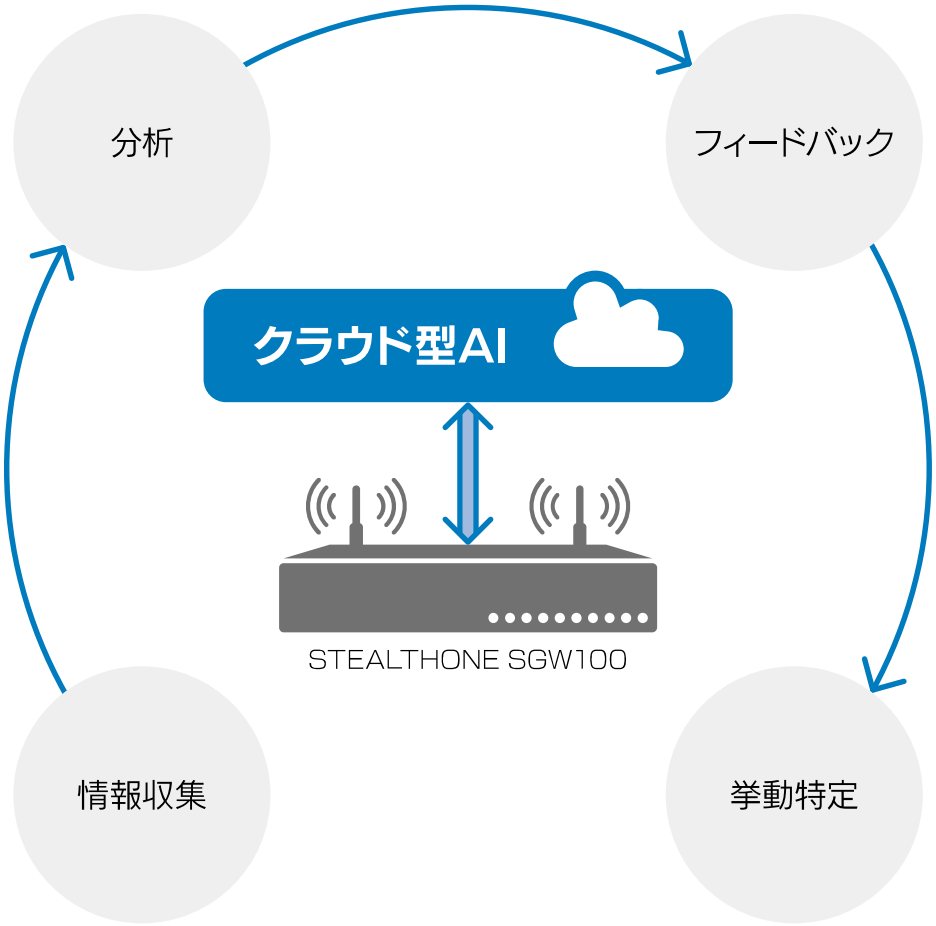
Avira SafeThings™ for StealthOne

About Avira SafeThings™ for StealthOne

STEALTHONE SGW100はセキュリティWi-Fiルーターとしての機能だけではなく、
Avira社から提供されたiOS/Androidアプリであるavira SafeThings™ for StealthOneという
IoTセキュリティサービスとの連携機能を搭載しています。
Avira SafeThings™ for StealthOneはネットワークに接続されたIoT機器を自動認識し、各デバイスの通信情報を収集します。
収集された情報はクラウド上の強力なAIにより分析され、端末の不審な挙動を特定することができます。
また、各IoT機器へのインストールは不要ですので、設定の手間がかからず管理を容易なものにします。

Cloud AI analyis

IoT端末の通信情報を収集するエージェントをSTEALTHONE SGW100に搭載しています。
収集された情報は、クラウドの強力なAIで分析され、不審な挙動を特定します。
各IoT端末へのインストールは不要ですので、設定の手間がかからず、管理が容易となります。



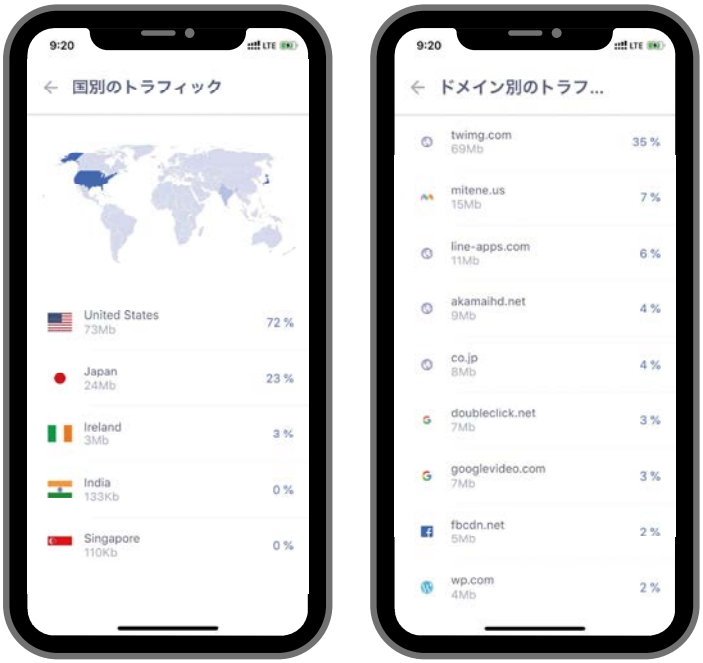
Avira SafeThings™ for StealthOne Functions

デバイスの自動認識

IoT機器にソフトウェアをインストールする事なく、ネットワーク内のIoT機器を自動的に認識します。
認識する端末は、コンピュータやスマートフォンだけでなくWebカメラやスマートテレビ、
アクセスポイント、スマートスピーカーなど多岐に渡ります。

通信の可視化・遮断

自動認識されたIoT機器の通信をスキャンし、トラフィックを可視化します。
可視化されたトラフィックは、国別、ドメイン別、直近24時間のトラフィック量で表示されるため、
どなたでも一元管理することができます。

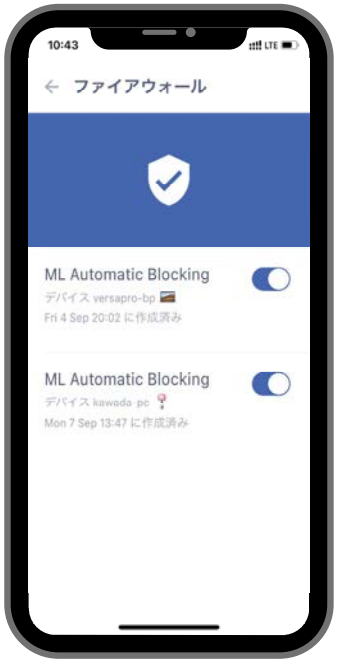


脆弱性のスキャン

自動認識されたIoT機器の脆弱性（ポート）を検出します。
検出結果は具体的なポート番号で表示され、管理者は存在するリスクを把握することができます。

ファイアウォール

予め設定されているアタックを自動的に防御し、
そのログを表示します。
ログにはアクセス元も表示されるため、
誤検知などの場合はブロックを解除することもできます。



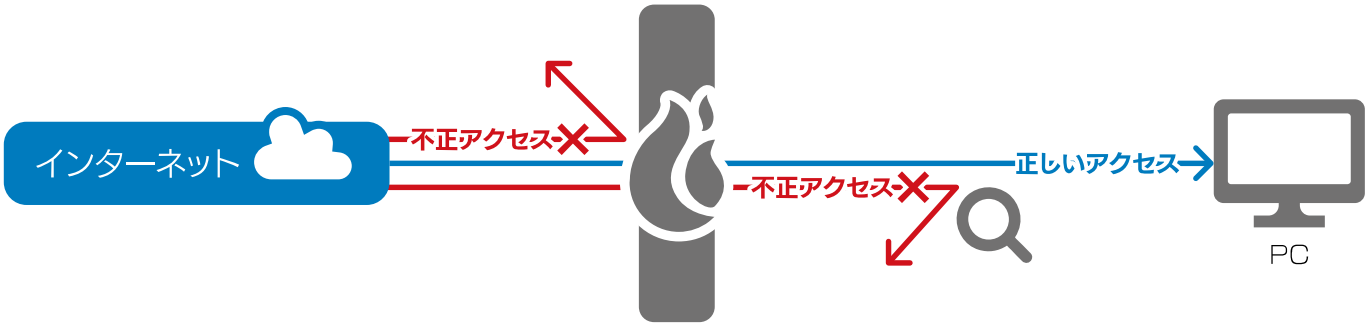
ユーザー管理

自動認識したIoT機器を
グループで管理することができます。

Other Functions

FW / IPS

通信ポートの管理に必須なファイアウォールと、不正な侵入を検知するIPSを搭載。
ファイアウォールとIPSの2段構えで不正なアクセスや侵入をブロックします。



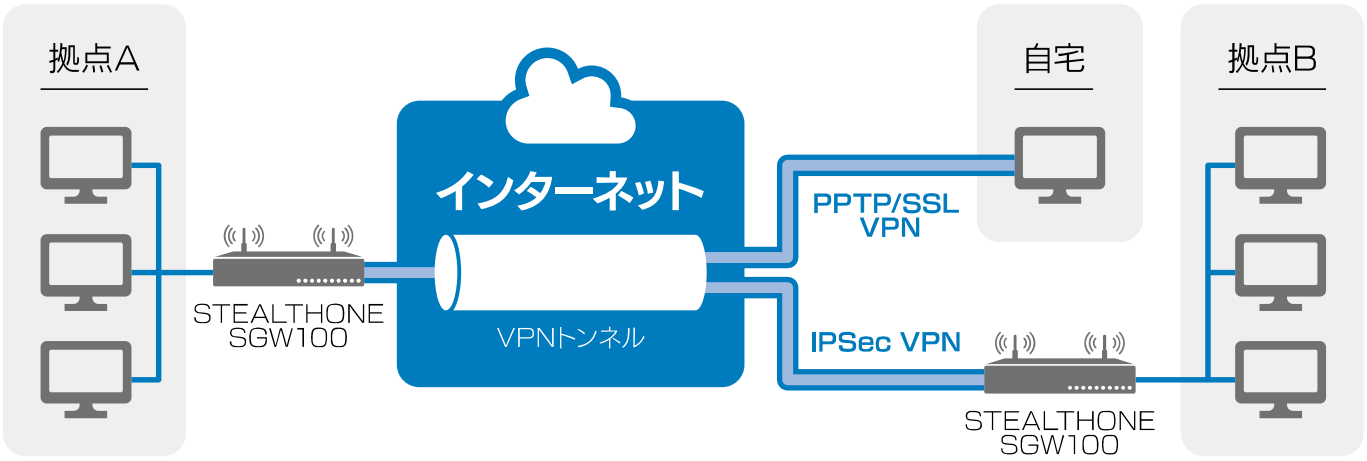
USB SIM連携

USBスティックタイプのモバイルルーター*1を直接接続し、インターネットを利用することができますので、
様々なインターネット接続環境にも対応することができます。

*1 全てのUSBモバイルルーターの動作を保証するものではありません。

VPN

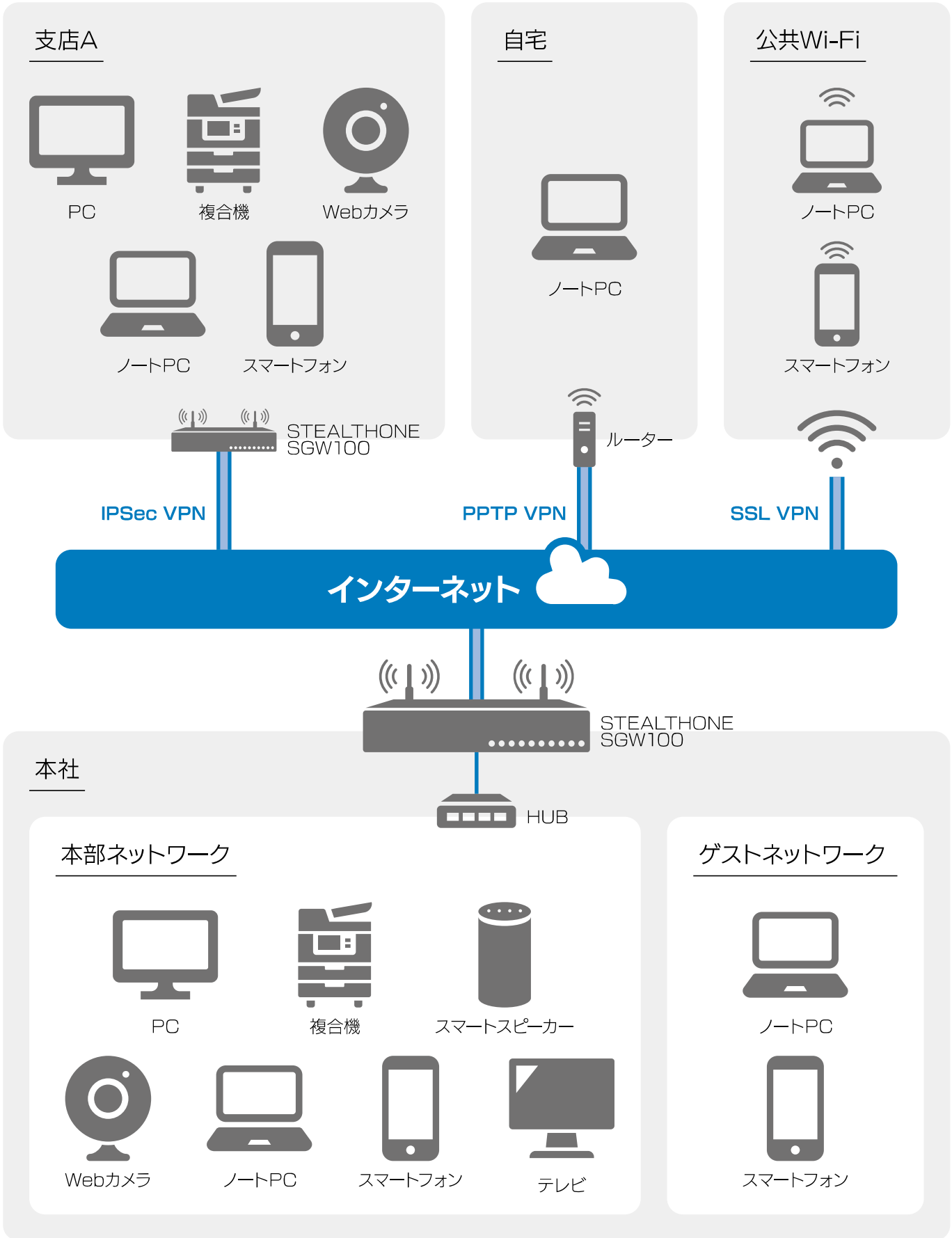
PPTP(端末型)・IPSec(拠点間接続)・L2TP・SSLに対応したVPNを構築することができ、
ニーズが高まるリモートワークにも対応する事ができます。
また、DDNS(sotokara.com*1)も利用することができます。



*1 sotokara.comは株式会社ワイズが運用するダイナミックDNSサービスです。
本機再起動直後からDDNSの更新まで接続できない時間帯がありますので、VPNの確実な接続を保証するものではありません。

Diagram

ネットワーク構成図



Product Specifications

本体仕様

インターフェース	イーサネット	10 / 100 / 1000 Base-TX ×4
	その他	USB ×2, Console×1
本体	寸法(mm)	190(W)×120(D)×44(H)
	重量	約1.2kg
環境	温度	-20~75℃
	湿度	10~85%　結露しない事
電源	形状	ACアダプター
	周波数	50/60Hz
	電圧	100-240V
認証	機器本体	CE/FCC/VCCI
	無線部分	技適(TELEC)
推奨最大接続クライアント数	75	

前面

背面

VPN Client

	PPTP	L2TP	SSL-VPN
Windows10	○	○	○
MacOS	×	○	×
iOS	×	○	×
Android	○	△*1	×

*1 接続は可能ですが、機器やOSによっては不安定になる場合があります。

VPN仕様

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

Wi-Fi仕様

無線規格	2.4GHz:IEEE802.11 g/n mixed, g/n mixed, b/n mixed, g, b
	5GHz:IEEE802.11 a/n mixed, ac
ピークスピード	867Mbps
セキュリティ	WPA_PSL / WPA2_PSK
アンテナ	2本(2T2R)
最大接続機器数	16

注意:5GHz(W52,W53)の帯域は、電波法により屋内での使用に限定されます。

機能一覧

- ファイアウォール
- IPS(不正侵入検知防御)
- VPN(IPSec・PPTP・L2TP・SSL)
- Avira Safething™ for StealthOne
- Wi-Fi(2.4GHz・5GHz)
- USB SIM連携

注意事項

- 本製品は株式会社ワイズが国内総販売元となっています。
  本製品はAvira GmbH & Co.KG(以下、Avira)(https://www.avira.com/ja)が提供するAvira SafeThings™ for StealthOneというIoTセキュリティサービスを利用するためのソフトウェアを搭載しています。
- Avira SafeThings™ for StealthOneモバイルアプリのインストール・利用方法はインストレーションガイドを参照してください。
- Avira SafeThings™ for StealthOneにつきましては、https://safethings.avira.com/を確認してください。なお、管理対象となる全てのデバイスのデータはAviraのクラウドセンターで保管・解析され、本製品内には保存されません。
- 本製品はIoT機器を含むネットワーク上に存在する端末に対するリスクを低減するための製品です。
- ライセンスの有効期限を過ぎますと、アップデートは停止し、脅威への効果が低下することになりますのでご注意ください。
- 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。
- 本カタログで使用している図はイメージ図です。
- 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。
- 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2021年2月現在のものです。

日本総販売元
株式会社ワイズ　東京都千代田区外神田2-2-19 丸和ビル
TEL: 03-5297-5470　FAX: 03-5294-7959
E-mail: sales@stealthone.net　　URL: https://www.stealthone.net

お問い合わせ