



高度セキュリティWi-Fi AP

WXA-1000

巧妙な高度継続攻撃 (APT) から
社内 Wi-Fi ネットワークを保護
暗号ファイルで持ち出しデータを安全に運用



社内ネットワークに潜むセキュリティの落とし穴

秒単位で発生する新種ウイルスと巧妙な侵入経路

- パターンマッチング方式の限界<ゼロデイ攻撃の驚異>
- 被害は、金銭損失・機会損失・信用失墜だけでなく、知らないうちに加害者にもなること
- Wi-Fi環境に潜むセキュリティリスク



毎秒4件、1日35万件の新種ウイルスが発生 ※AV-TEST2016/2017レポート

ウイルスが発見され、対策プログラムが配布されるまでのタイムラグを狙ったゼロデイ攻撃



ウイルス定義ファイルの更新は1日1回…
ということは毎日35万件の新種ウイルスにさらされている？

…更新ファイル開発期間を入れるともっと…



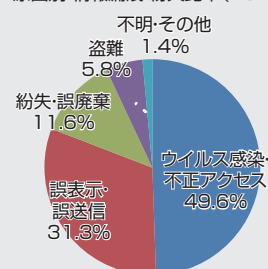
USBメモリやメールの使用を監視しているのに、社内情報が漏洩した

ウイルス感染したPCが、Wi-Fiを介して他のPCの情報を収集
C&Cサーバと呼ばれる攻撃者の管理するサーバーへ情報を送ります

機密データの情報窃盗を実行



原因別 情報漏洩・紛失比率(2021)



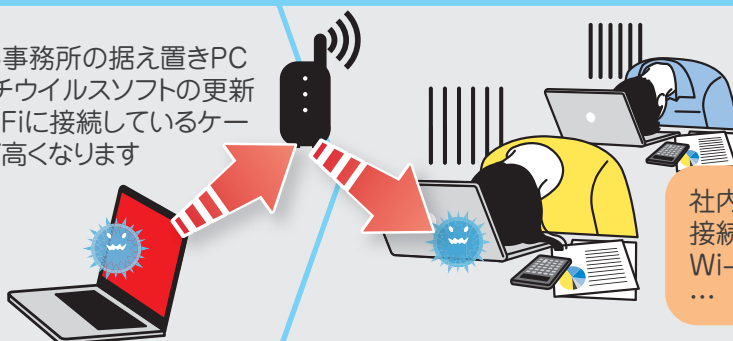
東京商工リサーチより引用



モバイルPCが、いつの間にか感染していた

UTMなどにより守られている事務所の据え置きPCと違って、モバイルPCはアンチウイルスソフトの更新頻度も長く、危険なフリーWi-Fiに接続しているケースもあり、セキュリティリスクが高くなります

来訪者に社内Wi-Fiを公開している場合もリスクは高くなります

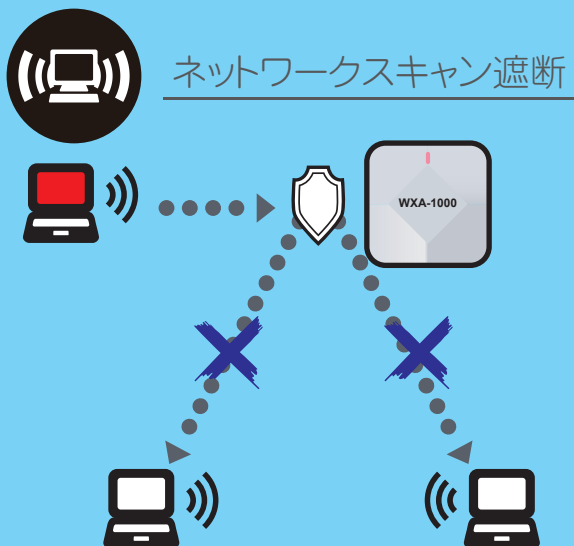


社内PCはすべてWi-Fi接続しているので、Wi-Fi経由で感染拡大…

WXA-1000は Wi-Fiセキュリティの砦

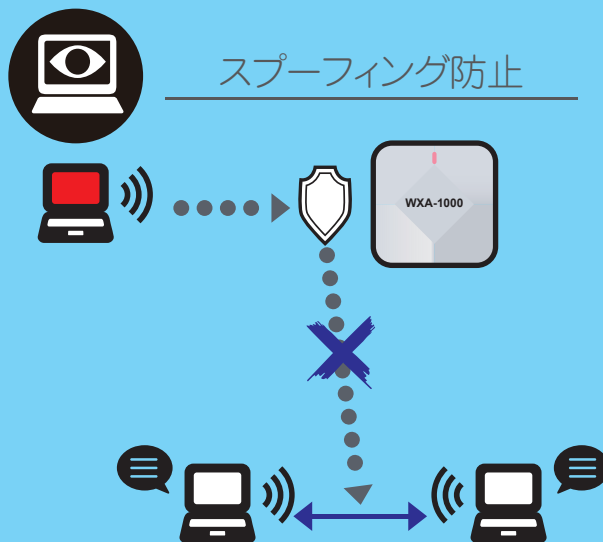
近年マルウェアの急激な増加により、入口対策のセキュリティが突破やWi-Fiなどの裏口からの感染リスクが高まっています。WXA-1000はWi-Fiによる感染拡大・攻撃の実行など攻撃者の最終目的を阻止します。

感染PCのネットワーク探索を阻止



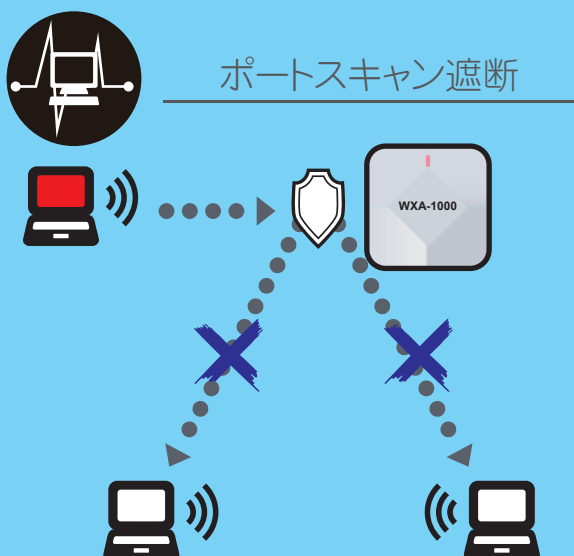
感染したPCが、より価値の高い情報を保存しているサーバやほかのPCにウイルスの感染を行うための事前ネットワーク調査を阻止します。

ネットワークでの盗聴を阻止



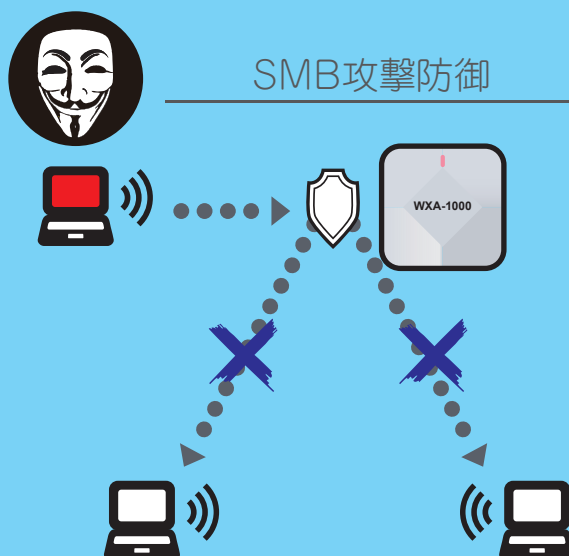
ネットワーク内の通信機器になりすまし、情報の盗聴やデータの改ざんが行われてしまうことを防止します。

情報漏えいを阻止



感染PCが情報漏えいの前にLAN内の環境を探るポートスキャンを防止します。

ランサムウェアの拡散を阻止



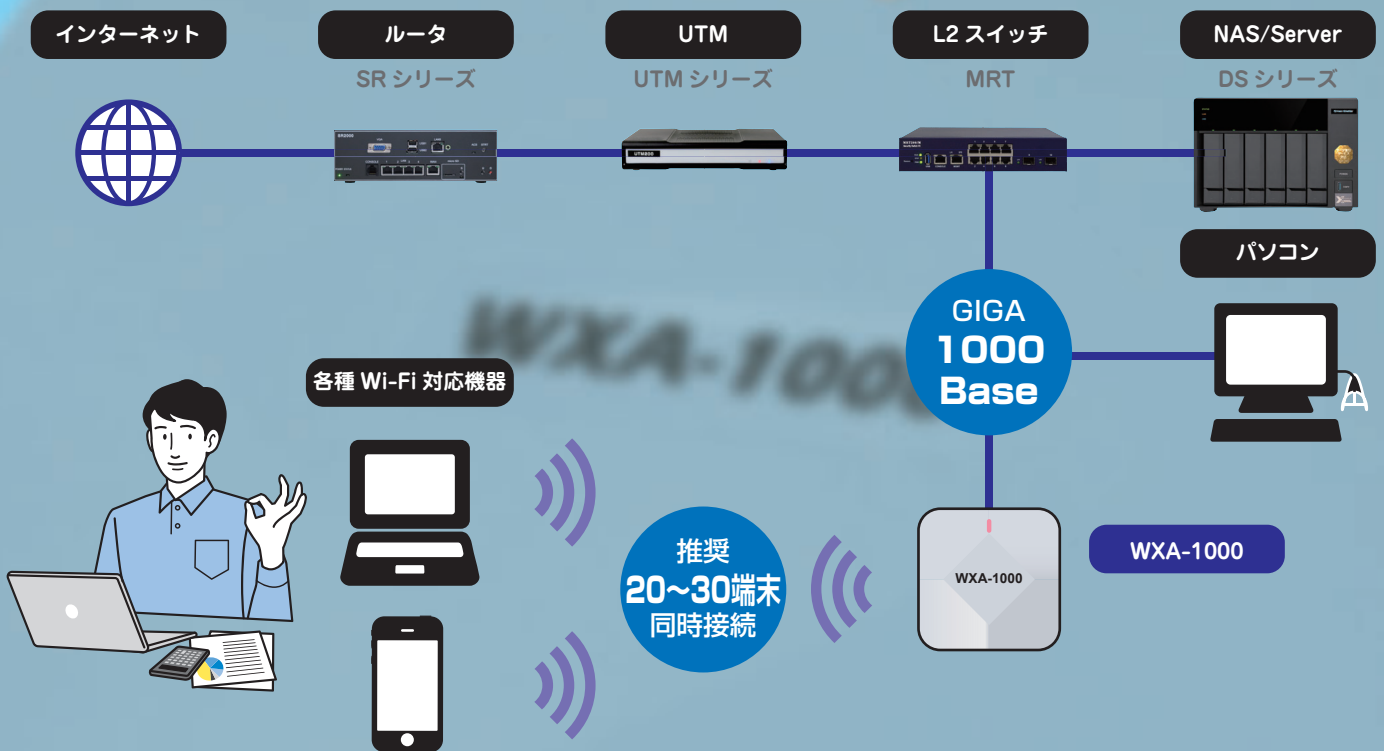
ランサムウェアを含めた各種マルウェアの社内PCへの拡散を防止します。

無線LAN(Wi-Fi)ソリューション

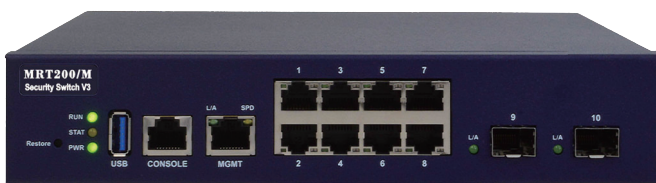
業務用のアクセスポイントとして充実の機能を搭載

- Wi-Fi接続台数が増えても安心の20~30端末(推奨)同時接続可能。
- 壁掛けに適したデザイン。PoE受電機能搭載で配線もスッキリ。※1
- 光回線を活かす1000Baseの高速有線LAN搭載。
- Wi-Fi通信のうち、サイバー攻撃の異常通信のみ遮断。
※マルウェア感染PCでも正常通信は可能。

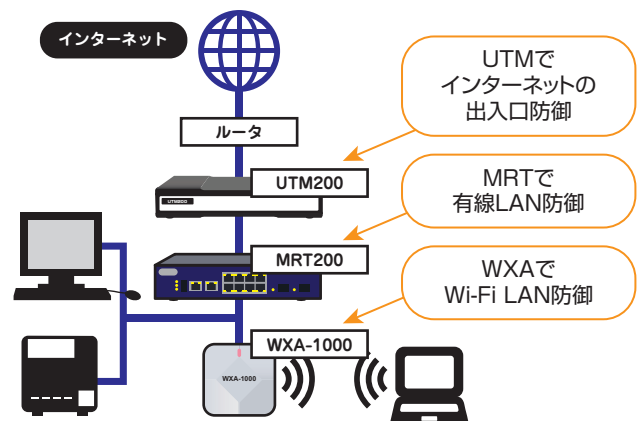
基本構成例



有線LANセキュリティは高度セキュリティスイッチMRT200がオススメ!



- サイバー攻撃独特の異常な通信だけを遮断
- ウィルス拡散、情報漏えいから社内LANを保護
- 高性能L2スイッチ内蔵



ファイル自動暗号化ソリューション

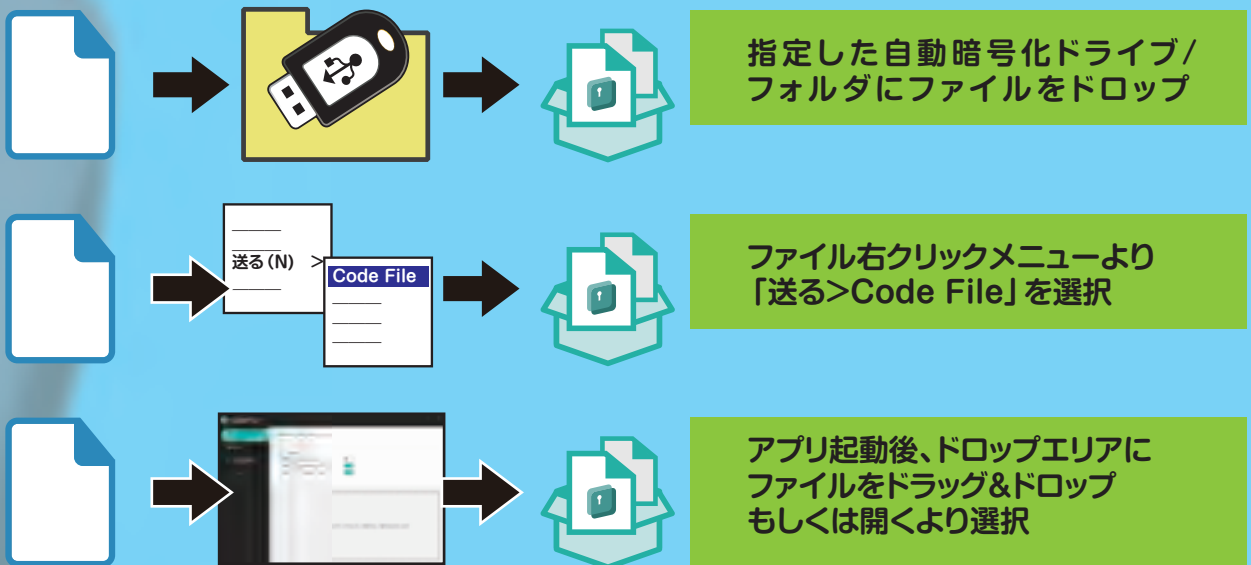
持ち出しデータを暗号化して情報漏えいリスクから守ります。

- 暗号アルゴリズムは米国立標準技術研究所(NIST)選出の中で最も強度のあるAES-256を採用。
- 自動暗号化フォルダや右クリックメニューで暗号化、生成暗号ファイルをメール送信。
- 専用のUSBメモリでなく、すべてのUSBメモリに新規保存したファイルを自動暗号化します。
- 復号パスワードは、自動生成! 暗号化後、自動で既定メーカーを起動してパスワードを記載。
- 復号PCに解凍ソフトは必要なし! 復号パスワードだけで復号できる自己解凍型ファイル。

※Code Fileオリジナル拡張子の暗号ファイル<AES-256>を復号する場合には、添付の専用復号アプリ(インストール容量約2MB)が必要です。

暗号化イメージ

暗号化



パスワード通知



- メーカー自動起動>新規メールに復号パスワード記述
- クリップボードに復号パスワード手動転送
- パスワードは自動生成。手動設定も可能

復号



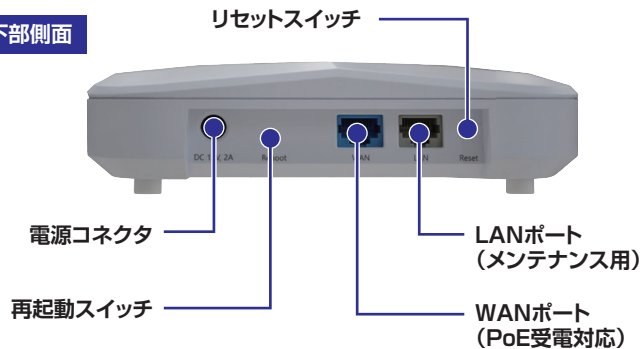
■外観図

正面



状態表示LED

下部側面



リセットスイッチ

電源コネクタ

再起動スイッチ

LANポート
(メンテナンス用)

WANポート
(PoE受電対応)

■主な仕様

機種名		WXA-1000/S	WXA-1000/M	WXA-1000/L
無線LAN (Wi-Fi)	規格	IEEE802.11 a/b/g/n/ac		
	MIMO	MU-MIMO 対応		
	アンテナ	内蔵アンテナ (2T2R x 2)		
	認証・暗号化方式	WEP(64/128bit)、IEEE802.1X(Personal、Enterprise)、WPA-mixed(Personal、Enterprise)、WPA(Personal、Enterprise)、WPA2(Personal、Enterprise)		
	対応チャンネル	5GHz : [W52] [W53] [W56]※W52/W53は屋外使用禁止※DFS 対応 / 2.4GHz : 1~13ch		
	最大接続数	推奨 20 ~ 30 台		
セキュリティ	フラッディング	TCP syn flooding / TCP ack flooding / UDP flooding / ICMP flooding / ARP flooding / IP-Spoofed		
	ネットワークスキャン	TCP / UDP / ICMP / Non-echo-ICMP / ARP		
	ポートスキャン	TCP syn / TCP ack / UDP / Stealth		
	スプーフィング	ARP スプーフィング		
	SMB scan	SMB scan		
管理		クラウド一元管理・イベントログ		
ハードウェア	インターフェース	10/100/1000 BASE-T RJ-45 x 2 (WAN・LAN<メンテナンス用使用不可>) WAN : PoE 対応		
	定格電圧 / 最大消費電力	100~240V AC, 50/60Hz / 12W (PoE : 36V DC ~ 57V DC)		
	サイズ (mm) / 質量	W170 X D170 X H40 / 360g		
	温度 / 湿度	0 ~ 50℃ / 20 ~ 90% (但し結露なきこと)		
	TELEC 認証	○		
	RoHS 対応	○		
自動暗号化 Code File	暗号アルゴリズム	AES-256 <オリジナル拡張子あり> / ZipCrypto		
	暗号化方式	●自動方式(自動暗号化機能)>論理ドライブ/フォルダ<最大指定数:3> ●手動方式>ドロップ機能(ドロップフィールド)・SendTo機能(右クリックメニュー)		
	暗号化ファイルのメール自動貼付	自動設定可<最大添付容量20MB※2 メールプレート機能つき>		
	元ファイル削除	ON/OFF可		
	復号化パスワード	●手動(使用可能文字種:英数記号)●自動生成(メーラー自動起動パスワード記載/クリップボード)		
	ライセンス数	20ライセンス <10ごとライセンス追加可能>		
	対応メーラー / 対応OS	Outlook(ストアアプリ版[Microsoft Outlook]は非対応)、Thunderbird / 日本語版Windows8.1、10(32/64bit)		
ライセンス期間	5年	6年	7年	
構成	本体、ACアダプタ、簡易マニュアル(本体・Code File)、CD-ROM、壁掛けブラケット、ネジx4種			

安全上のご注意



- 正しく安全にお使いいただくために、ご使用前には「取扱説明書」をよくお読みください。
- 水、湿気、ほこり、油煙等の多い場所や密閉された状態で設置しないでください。火災、感電、故障等の原因となることがあります。

●本製品は、内部Wi-Fiネットワーク (LAN) 内における通信を監視し制御する機器であり、インターネットなど外部ネットワークからの通信を監視・制御する機器ではありません。●本製品は、ゼロディ攻撃や未知の攻撃等に対して100%の防御を保証するものではありません。●本紙掲載の会社名および商品名等は、各社の商標または登録商標です。●製品改良等により予告なく仕様、デザインを変更することがあります。●本カタログに掲載している製品の価格には消費税、配送設置工事・接続調整費等の費用は含まれておりません。●本機は屋内専用です。屋外での使用は避けてください。●暗号化ファイル生成直後であれば、アプリに暗号化ファイルをドラッグ&ドロップすることで復号可能です。(最大履歴20個) ●暗号化可能なファイルおよびフォルダの合計サイズは最大3.5GBです。●本機に落下等の強い衝撃を与えないでください。●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や、異常動作の発生により生じた損害等の純粋経済損失につきましては、一切その責任を負いかねますので、あらかじめご了承ください。●本紙は2022年06月現在のものです。仕様および内容は予告なく変更する場合があります。※1 : PoE受電機能をご利用するには別途PoE Hubが必要です。※2 : 最大添付容量は利用メールサーバ制限も影響します。



株式会社 アレクソン

ビジネスパートナー部 営業一課
〒103-0013 東京都中央区日本橋人形町2-25-13 リンレイ日本橋ビル5F
TEL 03-3667-2276 FAX 03-3667-5329

ビジネスパートナー部 営業二課
〒541-0052 大阪府大阪市中央区安土町1-8-6 大永ビル4F
TEL 06-6121-6048 FAX 06-6121-6049

ビジネスパートナー部 営業三課 福岡営業所 ※福岡営業所はISO14001範囲外です
〒819-0025 福岡県福岡市西区石丸2丁目40番8号
TEL 092-892-9677 FAX 092-892-9678

ホームページ <https://www.alexon.co.jp/>



お問い合わせ