ALEXON

UTM（統合脅威管理）

NA-GP2000std

NA-GP2000std S （5年ライセンス）
NA-GP2000std M （6年ライセンス）
NA-GP2000std L （7年ライセンス）

Fire wall
IPS/IDS
Anti Virus
Anti Bot
Anti SPAM
URL Filter
Application Control
Report
1000Base GIGA
File Auto Encryption

ウイルス対策ソフトだけでは阻止できない脅威

拡大するネット不正送金被害・データ流出のニュースが絶えずヘッドラインを賑わしています。
なかでも近年のサイバー犯罪の主な目的は、金銭を窃取することです。
今やネットワークセキュリティは必須の課題であり、企業では効果的な対策を実施することが重要です。

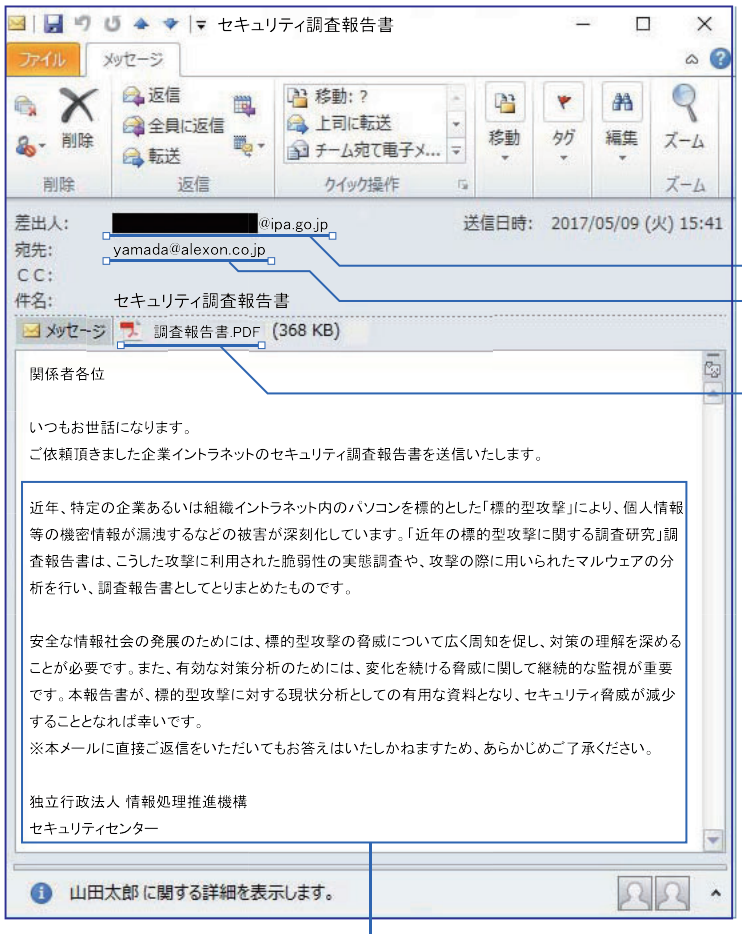
狙われる企業ネットワーク・巧妙化するサイバー犯罪の手口

企業の大小に係わらずセキュリティの甘い企業がターゲットにされています。

まずセキュリティの甘い企業に侵入。
ID、パスワードなどの**金融機関情報**や**顧客情報**などで換金できる**情報を抜き**去った後に、よりセキュリティの高い企業へ侵入するための**踏み台**とされます。

1日約 35万の新種ウイルスが発見されています。

【ウイルスメール例】



メールアドレスは、**簡単に詐称**できます。

yamada や ito など、よくあるアドレスから、ちょっと複雑なアドレスまで、攻撃者が独自のデータベースから**自動生成・自動送信**を行います。

ウイルス本体。
拡張子を変更することで**簡単に偽装**できます。

本文に関しては、詐称された組織のサイトから情報等を流用されたケースが多々あります。

NA-GP2000std の主な特長

攻撃者は、検出を避けるために、その攻撃方法を絶えず変更しています。
新たに出現するこれらの脅威からお客様のネットワークを保護します。

優れた防御力

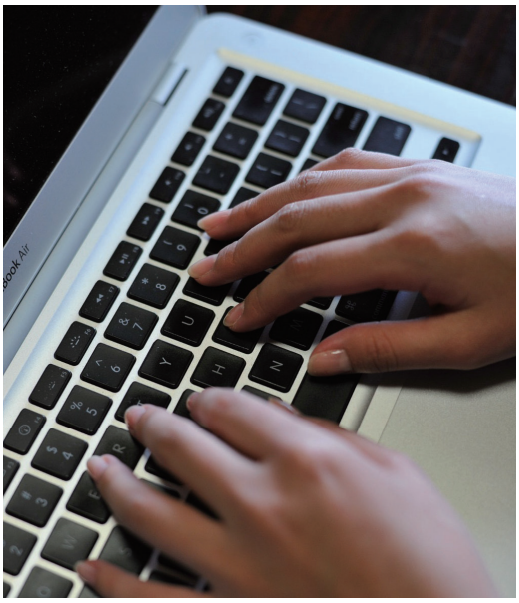
膨大な脅威データと豊富な経験を基盤として業界最多のウイルスデータベース・有害サイト情報を保持。

次世代ファイアウォール機能を搭載

従来型ファイアウォールを突破する不正な通信も制御。

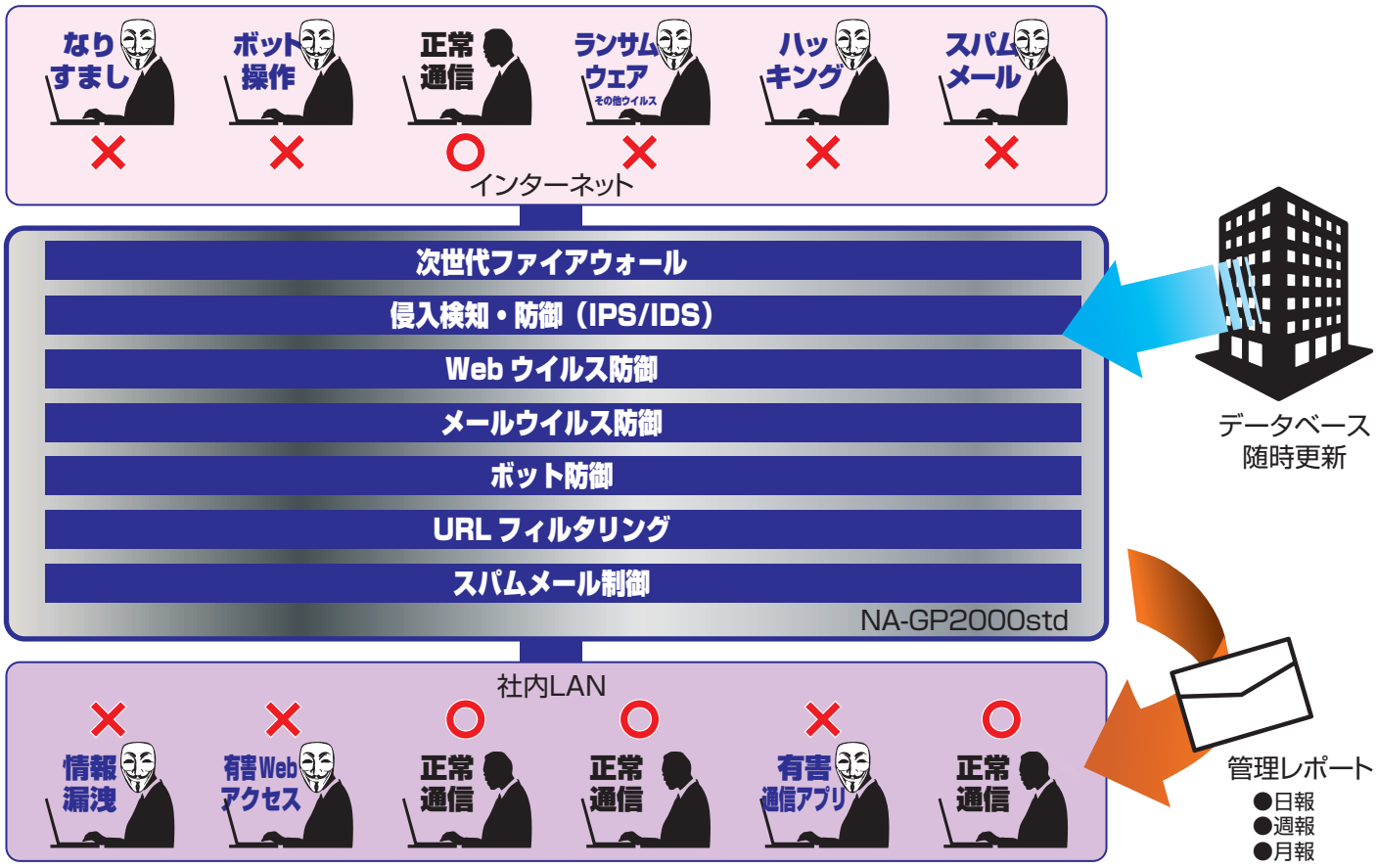
優れたユーザービリティ

定期的に NA-GP2000std 本体より発信する管理レポートにより社内ネットワークのセキュリティ状態を把握。
また、お客様の既存ネットワークを再構築することなく設置が可能です。

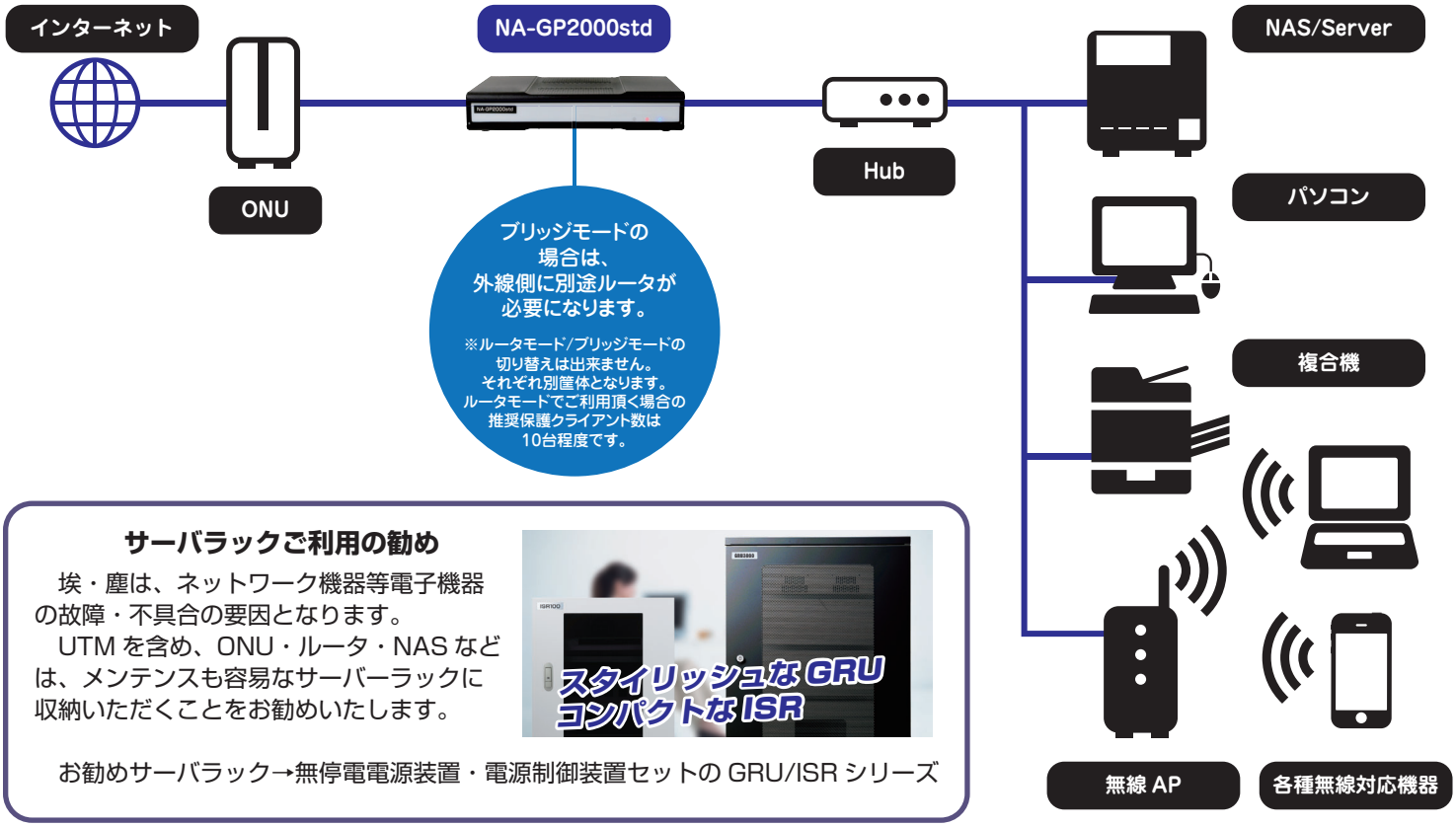


機能イメージ

NA-GP2000std は複数のネットワークセキュリティを 1 台にパッケージ化。
ユーザー様に運用・管理の負担が少ないシステムです。



NA-GP2000std（ルータモード）の接続構成



サーバラックご利用の勧め

埃・塵は、ネットワーク機器等電子機器の故障・不具合の要因となります。

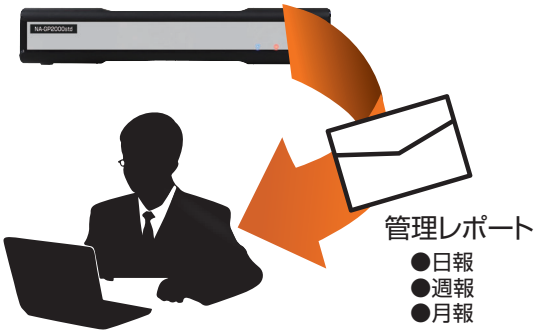
UTM を含め、ONU・ルータ・NAS などは、メンテンスも容易なサーバーラックに収納いただくことをお勧めいたします。

お勧めサーバラック→無停電電源装置・電源制御装置セットの GRU/ISR シリーズ

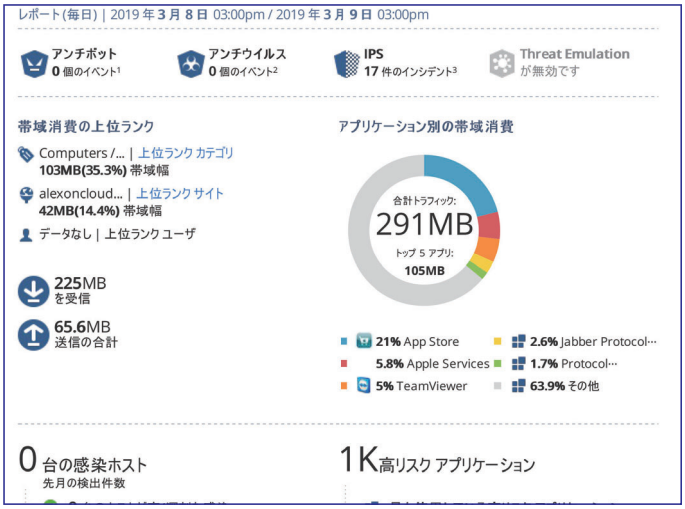
管理レポート

ひと目でネットワークの利用状況が把握できるグラフ形式のレポートでネットワークの状況を正確に把握できます。

※レポート設定は弊社よりリモートで行います。



【管理レポート（一部抜粋）】

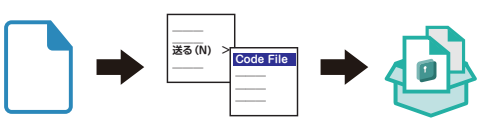


持ち出しデータを情報漏えいリスクから守る

自動暗号化ソリューション（Code File）

暗号アルゴリズムは米国立標準技術研究所（NIST）選出のAES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



セキュリティ × パフォーマンス = NA-GP2000std

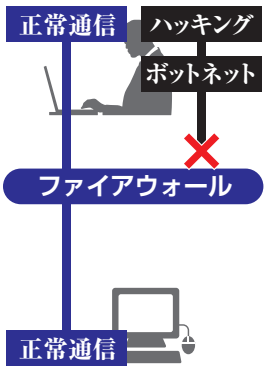
NA-GP2000std は、高度な脅威検出エンジンをバックボーンにしたセキュリティとハードウェアに最適化されたシステムで非常に優れたパフォーマンスを実現しています。

高度な攻撃や脅威の阻止に必要な機能を搭載し、信頼できるユーザーに対しては安全なネットワークアクセスを提供します。

ファイアウォール

ファイアウォールは、社内ネットワークとインターネットの間で決められたルールの下、出入りするデータを監視し、データの通過・破棄を行います。

NA-GP2000stdは、あらかじめ決められているルールを基にネットワークを保護し、セキュリティを高めます。



侵入検知･防御(IPS/IDS)

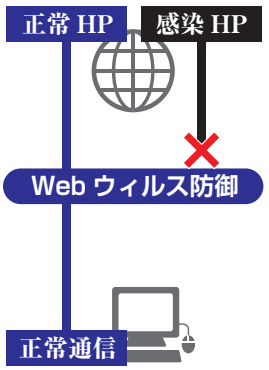
ファイアウォールだけでは阻止できない高度な攻撃や不正侵入･攻撃、またその兆候をもった通信を検知し、外部への情報流出を防御します。

NA-GP2000stdは、IPS(侵入防御システム)とDoS攻撃防止機能により、外的攻撃からシステムを保護します。

Webウイルス防御

ウイルス感染はメールだけではなく、ウイルスを仕込まれたサイトにアクセスするだけで感染する場合があります。

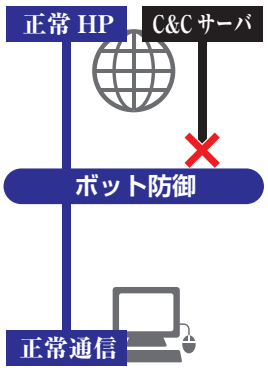
NA-GP2000stdは、ウイルスサイトを保持した情報で見破り、アクセスをさせない様にします。



ボット防御

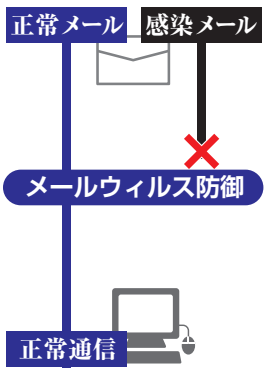
ボットとは、他人のPCをリモート操作する不正ソフトウェアの一種です。

NA-GP2000std は、ボット化された PC と指令（C&C）サーバの通信を遮断してボット化によるリモート操作を防ぎます。



ウイルスメール防御

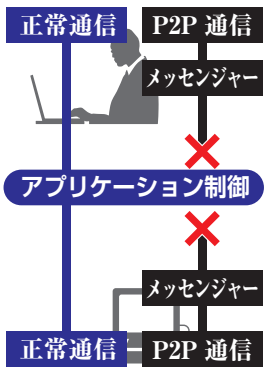
ウイルス添付メールは、NA-GP2000std上でブロックし、機密データの安全を確保します。パソコンには、ウイルスメールをブロックした旨をメールで通知します。



アプリケーション制御

サーバを介さず暗号により1対1の匿名通信を行うP2Pソフトや特定の相手にメッセージや添付ファイルを送ることができるメッセンジャーは、情報漏えいの温床になります。

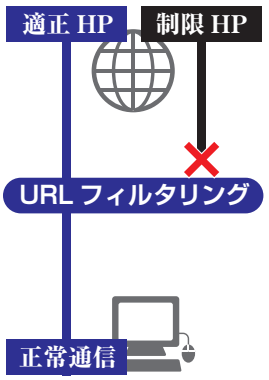
NA-GP2000std は、LAN内のパソコンからの通信を監視し、該当の通信を遮断します。



URLフィルタリング

業務には不要なサイトへのアクセスをブロックし、業務効率向上を図ることができます。

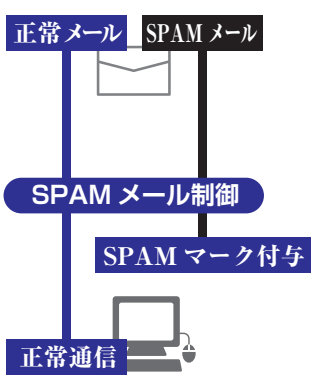
URLデータベース内のサイト情報を活用して、不適切なコンテンツの閲覧を排除します。



SPAMメール制御

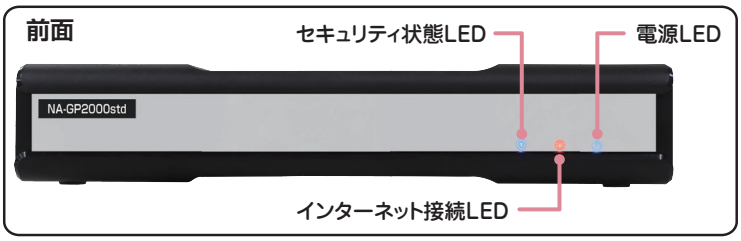
最新の解析情報を利用し、新種･未知のスパムを検出。

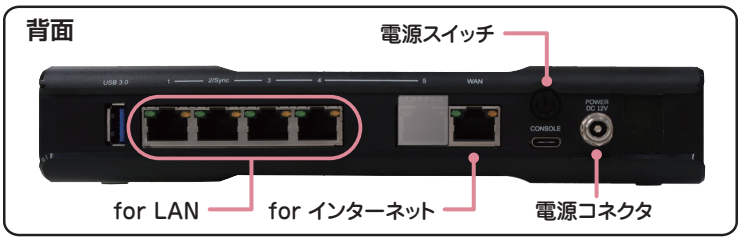
検出したスパムメールには件名にスパムマークが追加されます。



主要機能	NA-GP2000std/S	NA-GP2000std/M	NA-GP2000std/L
Firewall 送受信時データチェック	●	●	●
IPS / IDS 不正侵入検知・防御	●	●	●
Application Control アプリケーション制御	●	●	●
URL Filtering アクセスURL制限	●	●	●
Anti Virus ウイルス防御	●	●	●
Anti Bot ボット防御	●	●	●
Anti Spam スパムメール制御	●	●	●
Client 保護クライアント数	推奨 25	推奨 25	推奨 25
License UTM ライセンス期間	5年	6 年	7 年

外観図





仕様概要

		NA-GP2000std
セキュリティ	保護クライアント数	推奨25ユーザー
	通信プロトコル	IPv4
	ファイアウォール※1	●
	侵入検知・防御(IPS/IDS)	●
	ウイルスメール防御	●
	対応プロトコル	POP3(110)
	Webウイルス防御	●
	対応プロトコル	FTP※2,HTTP
	ボット防御	●
	URLフィルタリング※3	●
	ブロック対象	指定アドレス
	スパイウェア防御	●
	アプリケーション制御※1	●
	スパムメール制御※4	●
	管理レポート	日報・週報・月報　送信先最大5メールアドレス
自動暗号化	暗号アルゴリズム	AES-256<オリジナル拡張子あり※5> / ZipCrypto
	暗号化方式	●自動(論理ドライブ/フォルダ)<最大指定数:3> ●手動(ドロップ機能・SendTo機能[右クリックメニュー])
	暗号化ファイルのメール※6自動貼付	自動設定可<最大添付容量20MB※7メールテンプレート機能つき>
	元ファイル削除	ON/OFF可
	復号化パスワード	●自動生成(メーラー※6記載/クリップボード<手動>) ●手動(使用可能文字列:英数記号)
	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OS	Windows8.1、10(32/64bit)

		NA-GP2000std
ルータ機能	対応回線及びサービス網	FTTH(光ファイバー)
	ルーティング対象プロトコル	IPv4
	WANプロトコル	PPPoE(IPv4のみ)
	VPN機能※8※9(対地数)	クライアントVPN<専用アプリ>(10)
	VLAN機能※9	ポートVLAN
	その他ルータ機能	DHCPサーバ、ポート転送ほか
ハードウェア仕様	ファイアウォールスループット	1000Mbps
	LANインターフェース	10/100/1000Base TX ×4
	WANインターフェース	10/100/1000Base TX ×1
	メンテナンスポート	USB-A、USB-C、RJ-45　各1ポート
	外部電源	100-240V-1.5A 50-60Hz (専用AC)
	周波数 / 消費電力	50-60Hz / 最大17.92W
	外形寸法	210(W)×160(D)×37.5(H)mm(突起物を除く)
	質量	約0.43kg
	使用環境	温度0～40℃、湿度5～95%(但し結露なきこと)
	取得認定	[JATE]D200016020、VCCI ClassB

安全上のご注意

●正しく安全にお使いいただくために、ご使用の前には「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。

●ルータモード/ブリッジモードは、それぞれ専用の筐体となります。●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。●本製品は機器構成によっては接続出来ない場合がありますので、あらかじめご了承ください。●本製品を医療機器の近くでは使用しないでください。●本資料は2022年2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。●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正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。

※1：初期値透過モードです。有効化するにはユーザー様ごとの設定が必要になります。※2：初期値無効です。※3：ユーザー様ごとの設定が必要になります。※4：メール件名にSPAMマークが追加されます。※5：オリジナル拡張子の暗号ファイルの復号には別途付属の復号化アプリ（インストール容量約2MB）が必要です。※6：指定メーラーは、Outlook（ストアアプリ版［Microsoft Outlook］は非対応）またはThunderbirdとなります。※7：最大添付容量は利用メールサーバ制限も影響します。※8：VPNをご利用の場合は、別途ご利用ISPの固定IPサービスをお申し込みください。※9：VPNとVLANの機能ついては、すべての環境で動作を保証するものではありません。お客様の環境で十分な検証を行ってからご使用ください。

ALEXON
株式会社 アレクソン
ISO14001

ビジネスパートナー部 営業1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2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2課 福岡営業所
〒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/