

MRB-50



MRB-100



MRB-500



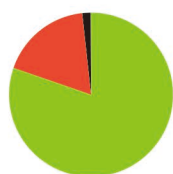
本当に
安全ですか？
セキュリティ
対策

企業がとらなければいけない 対策には問題が山積み！

急増する新しい未知の脅威

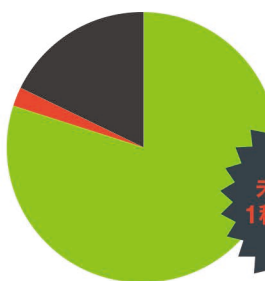
過去に比べ、現在膨大な量の脅威が発見されています。
それに比例して、未知の脅威が1秒に4～5個発生している状況です。

過去の脅威分布



■ 安全 ■ 既知の脅威 ■ 不明・未知

現在の脅威分布



急増する新しい未知の脅威は、とても膨大な量です。

1日に検出される新たな脅威の数



不正URL
25,000



悪質なIPアドレス
100,000



マルウェア
120,000



フィッシングサイト
6,000



未知のファイル
1,000,000

従来方式のセキュリティの限界

エクスプロイトキットが闇社会で簡単に入手できる昨今、
様々な新たな手法の未知の脅威がネットの世界に満ち溢れています。

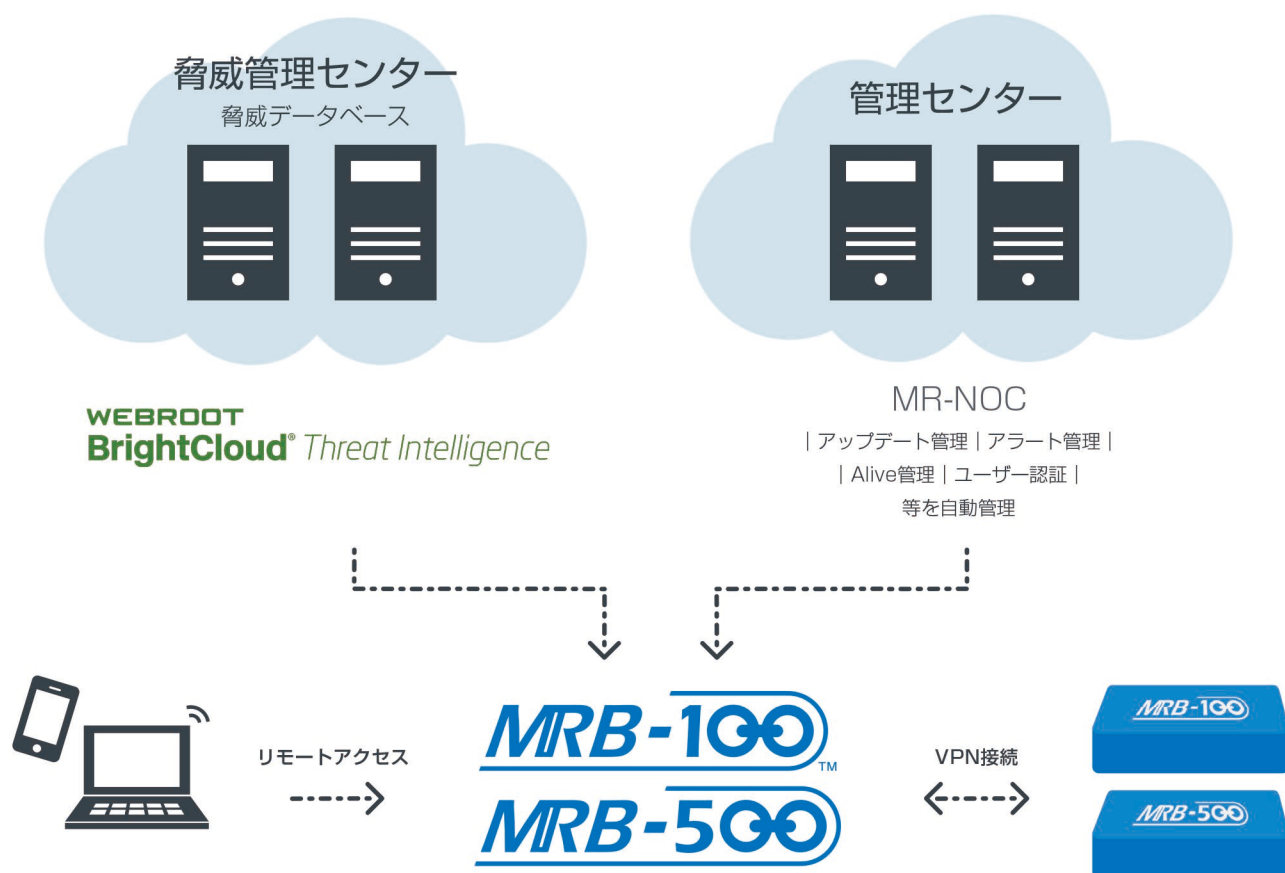
- 従来のAVソフトで検出出来ない未知のマルウェアやサイト改ざんによる感染リスクの増加
- 未知のマルウェア、攻撃ツールの取引、サポートサービス等を含んだCybercrime as a Serviceの増加
- 数日／数時間のみ存在、更に監視を逃れるため国内設置が増えるC&Cサーバの増加
- SSL通信の「見えない化」を隠れ蓑にするマルウェアや不正通信の増加
- シグネチャ方式の脅威への対応スピードの限界

今までの常識では守りきれない脅威が日々生まれています。

MRBはクラウド上の最新の脅威データを常に参照。
世界中で起こっている

一つで
安心
セキュリティ
対策

最新の脅威に即座に対応！



BrightCloud® Threat Intelligence

- 世界中で発見された脅威を即座に共有
- 一日3回、世界中のIPアドレスをチェック。
脅威が潜むIPアドレスにアクセスさせません。
- 脅威が潜むURLはもちろん、
独自のスコアリング技術で
危険を予測しユーザーを守ります。

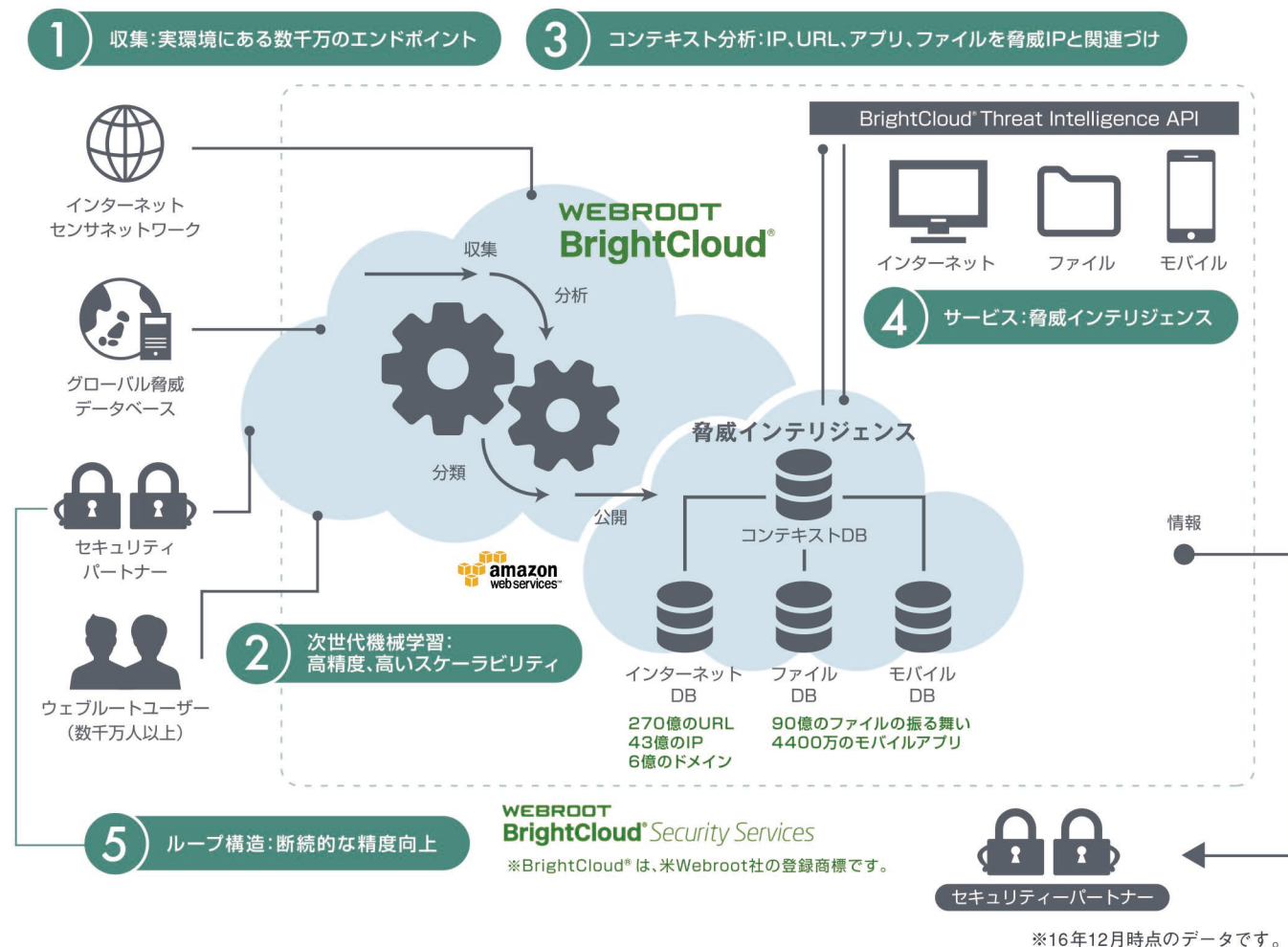
MR-NOC

- 機械の状態を常に監視
- ファームウェアの自動アップデート
- ファイアーウォール等設定の自動アップデート

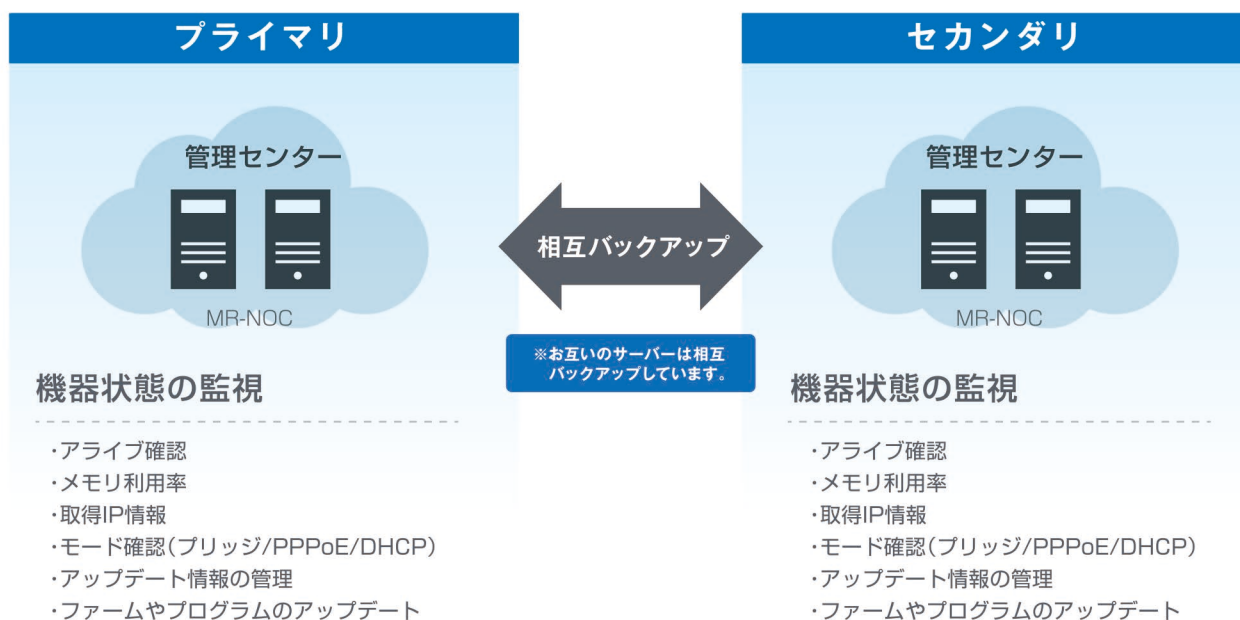
基本的な設定をするだけで、運用はお任せ！

脅威インテリジェンス

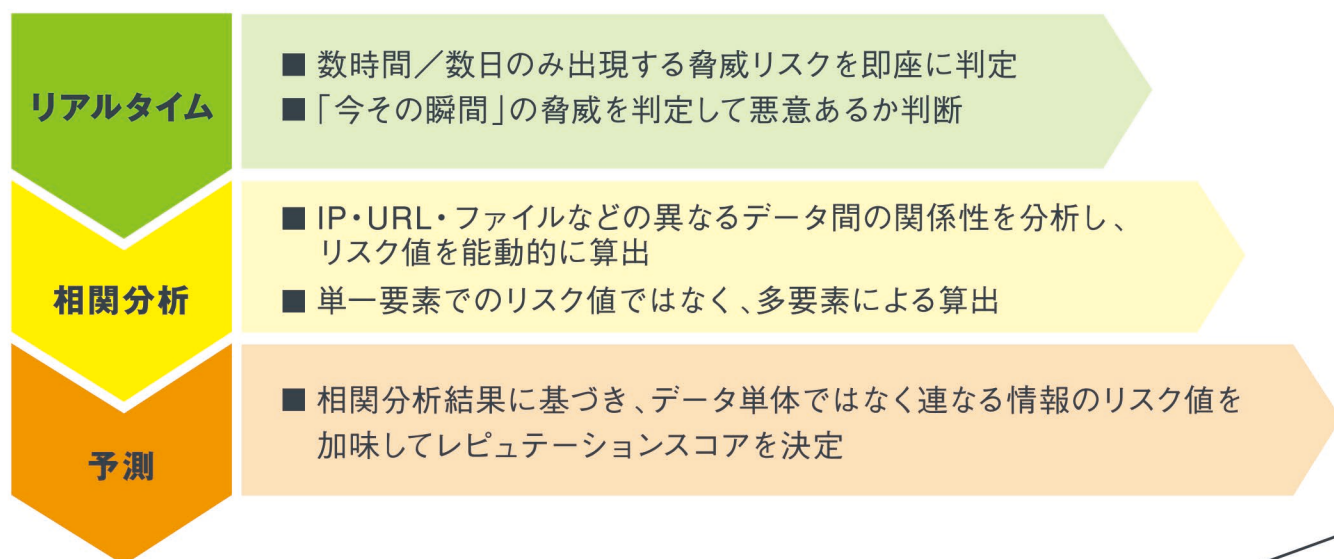
BrightCloud® Threat Intelligence; BCTI



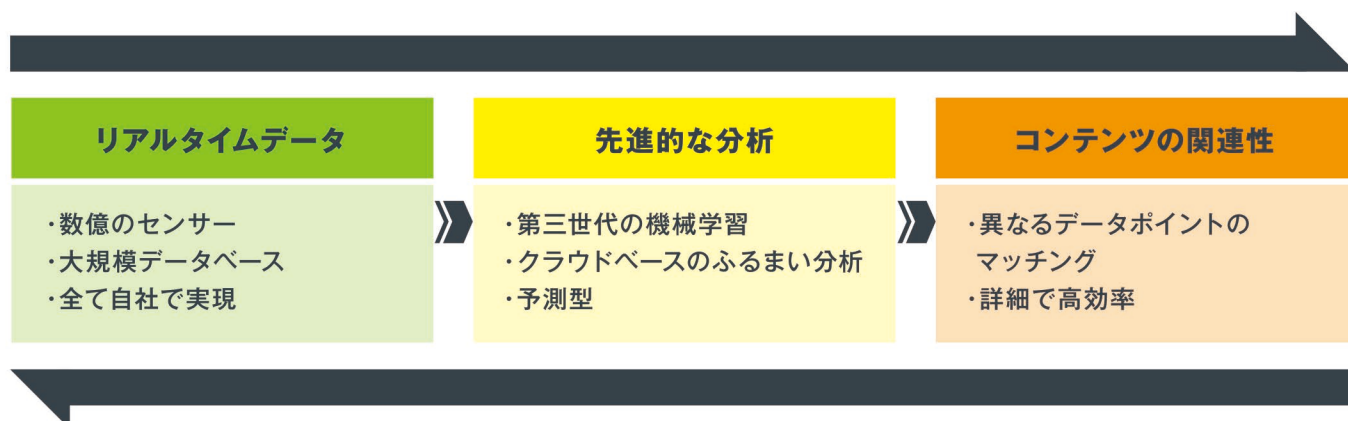
管理サーバーMR-NOC



予測型脅威インテリジェンスが 未知の脅威への対抗策に



脅威インテリジェンスBrightCloud® Threat Intelligenceは、
日々急増する脅威からお客様の情報を守ります。



従来のシグネチャベースの対応では、発見からシグネチャ発行のタイムラグがあり対応が遅れてしまいます。

BrightCloud® は、ハッシュベースの脅威のチェックをしますので、脅威が見つかったから即座に

世界中のユーザーに脅威の情報を共有することができます。

搭載セキュリティソリューション

FW



外部ポートは閉じたまま、ステルス状態で通信をします。もちろん、外部からの一方的な通信は遮断しますので、ネットワークに対する攻撃から守ります。もちろん、管理は不要。MR-NOCでコントロールします。

File-Reputation



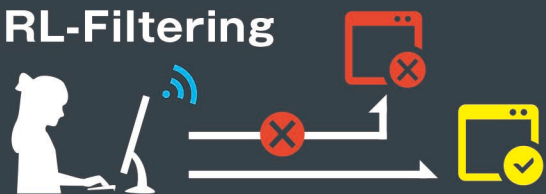
Web閲覧時に、マルウェアが含まれていないか、怪しい挙動をするファイルが潜んでいないかをチェックします。Webroot社のBCTI上の90億を超えるフレッシュなビッグデータを常に参照します。ですから、新しいマルウェアへの対応が非常にスピーディーです。

IP-Filtering



BCTI上の約43億個のIPのカテゴリや脅威のスコアを基に、アクセスして良い先かの判定をします。C&CサーバーのIPアドレスも監視しておりますので、通信が見つかると遮断します。また、メールのspam判定時には、送信元IPを判断してユーザーに危険をお知らせいたします。

URL-Filtering



BCTI上の約270億以上のURLのカテゴリや独自の脅威のスコアを基に、アクセスして良い先かの判定をします。Web閲覧時には、開いて良いURLかの判定はもちろん、ページ内にあるリンク先URLが危険であれば表示もさせません。また、メールのspam判定時には、本文中に含まれるURLのカテゴリやスコアを基にユーザーに危険をお知らせいたします。MRBは、予め危険が潜むサイトをブロックしてお客様を守ります。

振る舞い(行き先)検知機能



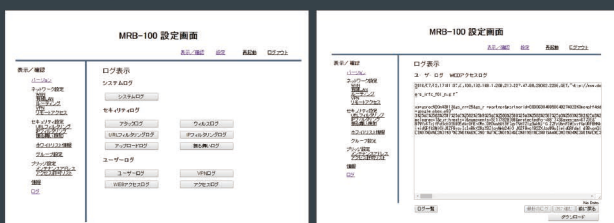
アウトバウンド通信全ポートを監視している機能です。IP-ReputationやURL-Reputation/Classificationをコントロールすることで、知らず知らずに外に通信されていても、危険が含まれる先への通信は遮断します。

※振る舞い検知機能は、17年夏に搭載予定

グループ設定

MRB-100 設定画面					
設定					
セキュリティ設定					
グループ設定					
優先度	詳細	編集	クリア		
グループ	グループ	グループ	グループ	グループ	グループ
グループ1	0	0設定	0	0	0
グループ2	1	0設定	0	0	0
グループ3	2	0設定	0	0	0
グループ4	3	0設定	0	0	0
グループ5	100	全て	0	0	0

ログ機能



各種ログ機能を搭載しております。ウイルスログやアタックログ等を確認できます。また、1週間の機械の稼働状況をメールで報告します。

配下の情報端末を、グループ分けしてそれぞれでセキュリティ設定を変更することができます。業務に併せたセキュリティ強度を設定することができます。また、オプションの『コレダケトオス』を使うことで、必要最小限の通信だけ許可することができますので、人事部門等重要データを扱うことが多い部署の情報を守ることでもあります。

セキュリティソリューションを組み合わせ、 様々な脅威から情報を守ります。

ユーザーが外部と通信していないとき



外部からの一方的な通信要求は、すべてブロック。

ポートが開いていないステルスファイアウォールですので、インターネットの世界から姿を消します。

Webページを見るとき



Webページを閲覧するときは、

① 閲覧先のIPアドレスに脅威が潜んでいるかをチェックします。

② URLをチェックし脅威が潜んでいるか、スコアリングがどうかをチェックします。

更にMRBは

③ 接続先のページに貼り付けてある画像等のリンク先のURLやIPアドレスもすべてチェックします。

脅威が潜んでいる場合そのリンクを表示させません。ですので、若干ページビューが遅れる場合がありますが、ダウンロード等の実際のスループットに影響はありません。

意識しない通信は…



マルウェア感染をしたり、リモートツールを仕掛けられた際等、気付かないうちにC&Cサーバーにアクセスされて操られたり、情報を盗られてしまいます。MRBは、インターネットに向けたすべての通信を監視しています。

ですから、Webページの閲覧の際と同様、お客様が意識することなく悪意のあるサイトに情報が出されようとした場合でも脅威情報を基にその通信をブロックします。

Mail security



メール受信の際は、MRB独自のセキュリティを提供します。メール情報を見て、

① 送信元サーバーのIPアドレスが脅威が潜むサーバーかの情報をBCTIに問い合わせます。

② メール本文にあるURLにフィッシング等の脅威が含まれるかを判定します。

①②の判定結果によって脅威が見つかった場合は件名に『任意の文字列』表記をします。

③ 最後に添付ファイルにマルウェアなどの脅威が含まれている場合は、削除します。

※POP/POPS/IMAP/IMAPSに対応。POPS/IMAPSの対応メーラーは16年12月現在MicrosoftOutLookです。
その他のメーラーは順次対応予定です。

※メールのウイルスチェックと本文URLチェックは、17年2月に対応予定です。

HW仕様

	MRB-50	MRB-100	MRB-500
CPU	テキサスインスツルメンツ社 Sitara AM3352 (ARMCortex-A8 core) 1GHz (300MHz~1GHz動的切り替え対応)	テキサスインスツルメンツ社 Sitara AM3352 (ARMCortex-A8 core) 1GHz (300MHz~1GHz動的切り替え対応)	Intel® Atom™ BayTrail-I プロセッサー E3845 QC 1.91 GHz
メモリ	NAND FLASH 256MB, DRAM1GB, NOR FLASH 2MB, EEPROM 2kByte	NAND FLASH 256MB, DRAM1GB, NOR FLASH 2MB, EEPROM 2kByte	DDR3L 1066・1333MHz 4GB Memory Down ECC Support
ストレージ	8GB(SD)	8GB(SD)	16GB(mSATA)
イーサネット	10BASE-T/100BASE-TX/1000BASE-T × 2ポート	10BASE-T/100BASE-TX/1000BASE-T × 2ポート	10BASE-T/100BASE-TX/1000BASE-T × 3ポートx1
Wi-fi	○(802.11b/a/a, 802.11a)	×	×
SIMスロット	○(MRB-50L: シムスロット搭載モデル)	×	×
USB/IF	USB 2.0 ホスト× 1ポート(TYPE-Aコネクタ)	USB 2.0 ホスト× 1ポート(TYPE-Aコネクタ)	USB3.0×1, USB2.0 ×3
スループット(全機能稼動)	最大90Mbps	最大90Mbps	最大200Mbps
VPN接続台数	~5台程度 ※MRB-50同士の場合	~5台程度 ※MRB-100同士の場合	~20台程度
対象端末台数	~10台程度	~10台程度	~50台程度
リモートアクセス	最大5台(同時接続)	最大5台(同時接続)	最大20台(同時接続)
大きさ	174.0mm(W)×111.0mm(D)×33.0mm(H) (アンテナ含まず)	81.0mm(W)×137.0mm(D)×28.7mm(H)	178.0mm(W)×48.0mm(H)×110.0mm(D)
重量	400g	380g	1Kg
使用電源・電源形状	DC12V ±10%	DC +12V ※ DCジャック (ACアダプタ)	DC+12V (9.0V~19.2V)
消費電力	計測中	待機時: 2.0W, 最大負荷時: 4.5W	待機時: 6.8W, 最大負荷時: 12.8W
本体動作条件	CPU 1GHz/1000BASE-Tリンク時: -20℃~60℃ CPU 300MHz/100BASE-TXリンク時: -20℃~65℃ 20~90%(結露なきこと)	CPU 1GHz/1000BASE-Tリンク時: -20℃~60℃ CPU 300MHz/100BASE-TXリンク時: -20℃~65℃ 20~90%(結露なきこと)	20℃~50℃ ACアダプターは、0~+40℃

搭載機能	詳細	
ファイアーウォール	ステートフルインスペクション	
ウイルスチェック	HTTP (POP(S)/IMAP(S))は17年2月対応予定です	
IPフィルタリング	低中高で設定可能、その他任意のカテゴリをカスタマイズ設定可能	
URLフィルタリング	低中高で設定可能 (83カテゴリに分類)	
Spamメール判定機能	・送信元IPアドレスによるチェック ・対象メールに任意の文言付加をします。	・対応プロトコルPOP(S)/IMAP(S)
VPN	最大30Mbps AES256bit	最大70Mbps AES256bit
リモートアクセス	5台まで(L2TP ver IPsec; 1ルーター1台のみ)	20台まで(L2TP ver IPsec; 1ルーター1台のみ)
デバイス別設定	最大3グループ、オプションで『コレダクトオス』機能あり	
ログ機能	システムログ2種類、ユーザーログ1種類、セキュリティログ6種類、週間稼動レポート	

※掲載内容は、2017年3月現在のものです。予告なく変更する場合がございます。
※商品の色調はフィルム、印刷インクの性質上、実際の色とは異なって見える場合がありますので、予め御了承ください。

Technol

株式会社テクノ TEL 0178-47-8128
青森県八戸市廿三日町2番地 YSビル3F
Mail : mr5@mamottaro.net

お問い合わせは _____

POWERED BY
WEBROOT®