



IoT時代の セキュリティ



Technol

MRB50/50LでIoT機器の 今までコスト面や環境の面で諦め



for example
工場でも

機械化が進み、さらにクラウドを活用するケースが増えています。通常のネットワークよりセキュリティ強化が必要なケースが増えてきました。



for example
SOHOオフィスでも

コストの面でセキュリティ機器の導入が難しいケースが多いのが現状です。昨今では企業の規模に関係なく脅威に晒されています。



for example
スマホ・タブレットでも

スマートフォンやタブレットが日常的に業務に使われています。さらに、企業内でも現在のセキュリティに加え部署によってセキュリティ強度を変える必要が出てきました。



for example
店舗でも

最近ではタブレットレジを使ったり、ネットショップを活用したりと、小売店でもインターネットが欠かせなくなってきました。



MRB-50

Wi-Fi モデル



利用シーンが広がります。 ていたセキュリティを提供します。

for example

現場事務所などでも

インターネットが必須の現場事務所ではタブレットの導入も進んでいます。加えて期間が短かったり工事が困難な場所も多くインターネット通信とセキュリティの確保が難しいことが多くありました。

for example

イベント会場でも

イベント会場では、タブレットを使った説明などが日常化しているだけではなくサービスのクラウド化も進んでいます。デモ環境にもセキュリティが必要なケースが増えてきております。

for example

農場でも

農業や養鶏業などでは現在害獣駆除やセンサー、WebカメラなどIoT機器の設置がどんどん広がっています。



MRB-50L

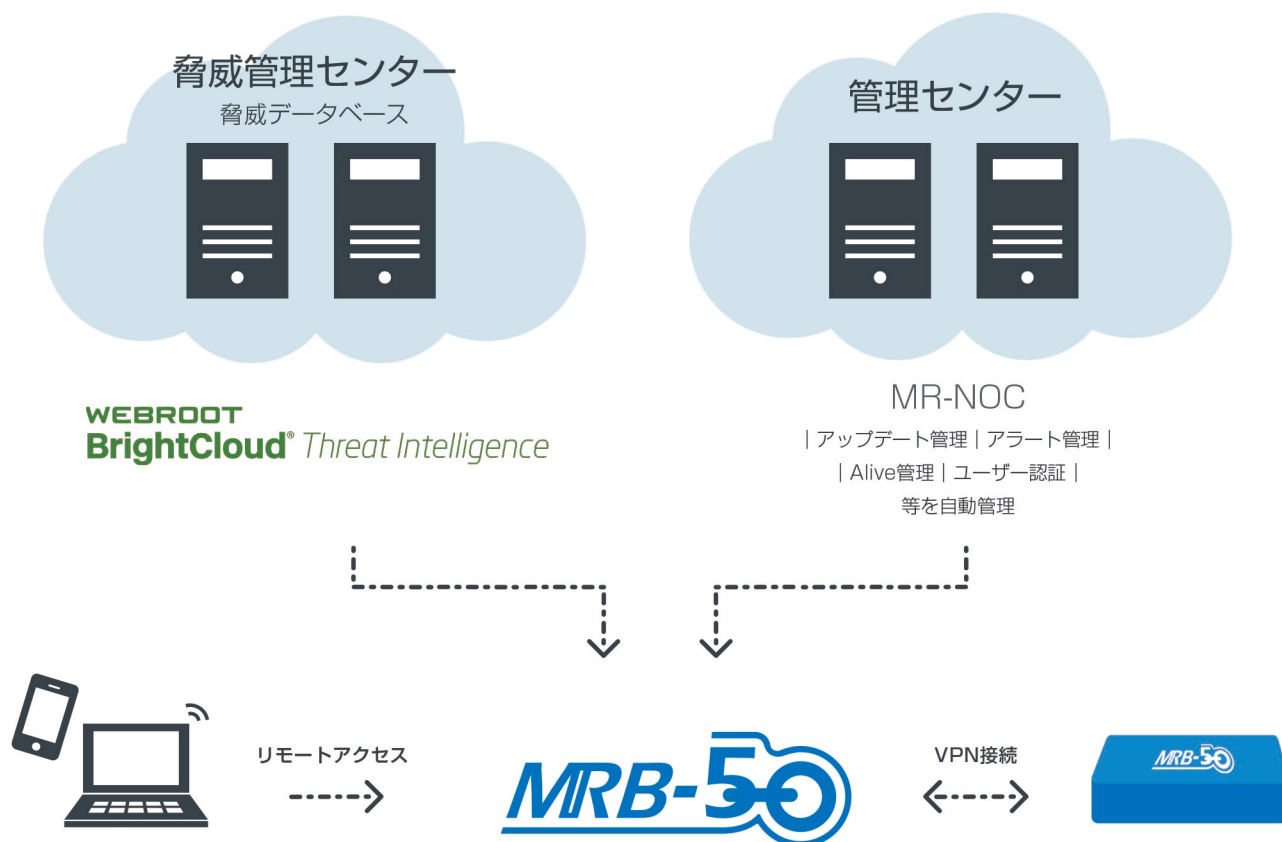
WiFi モデル
SIM搭載
モデル

※実際のものには2本アンテナが付属いたします。

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。

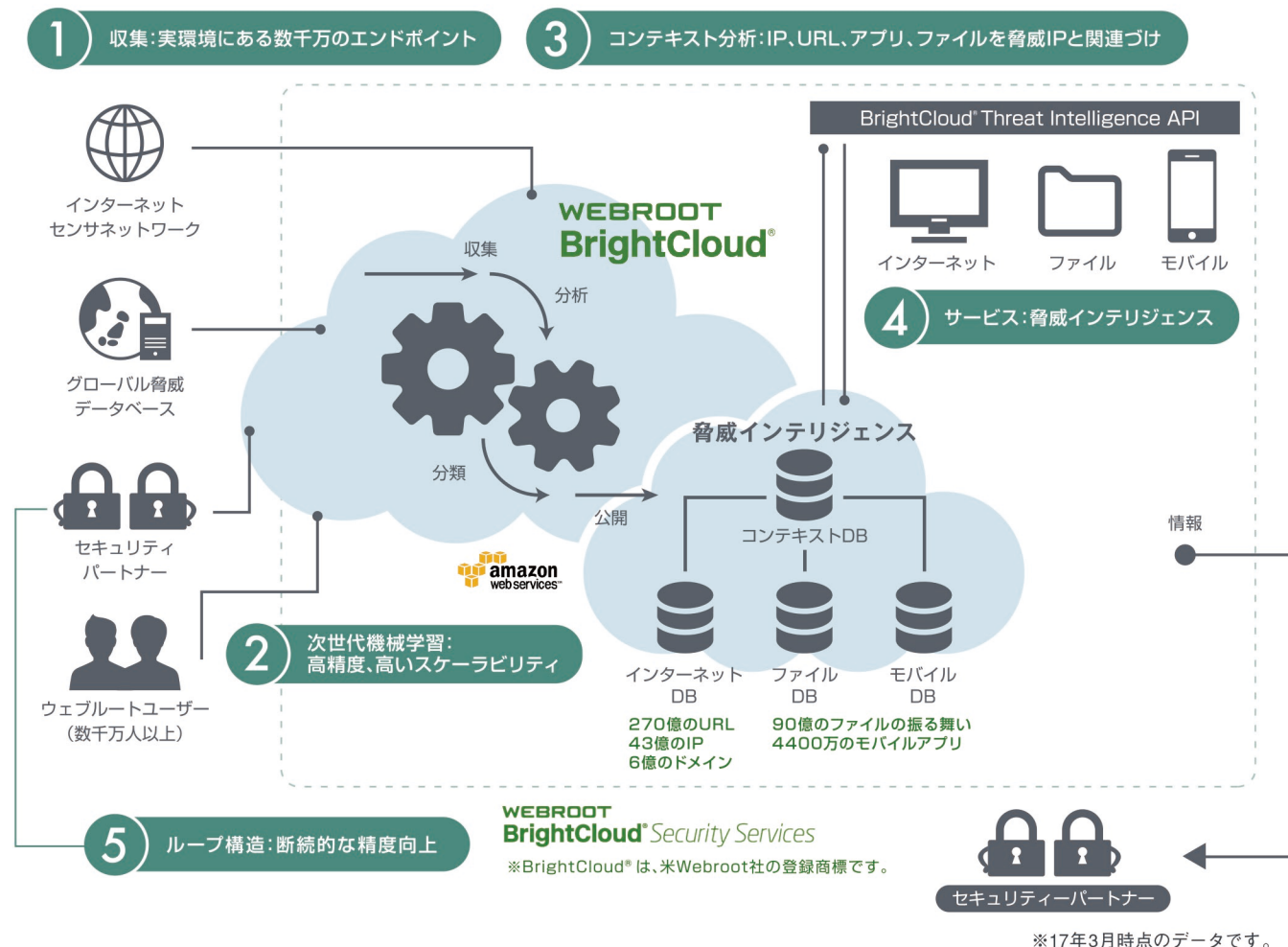
MR-NOC

- 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

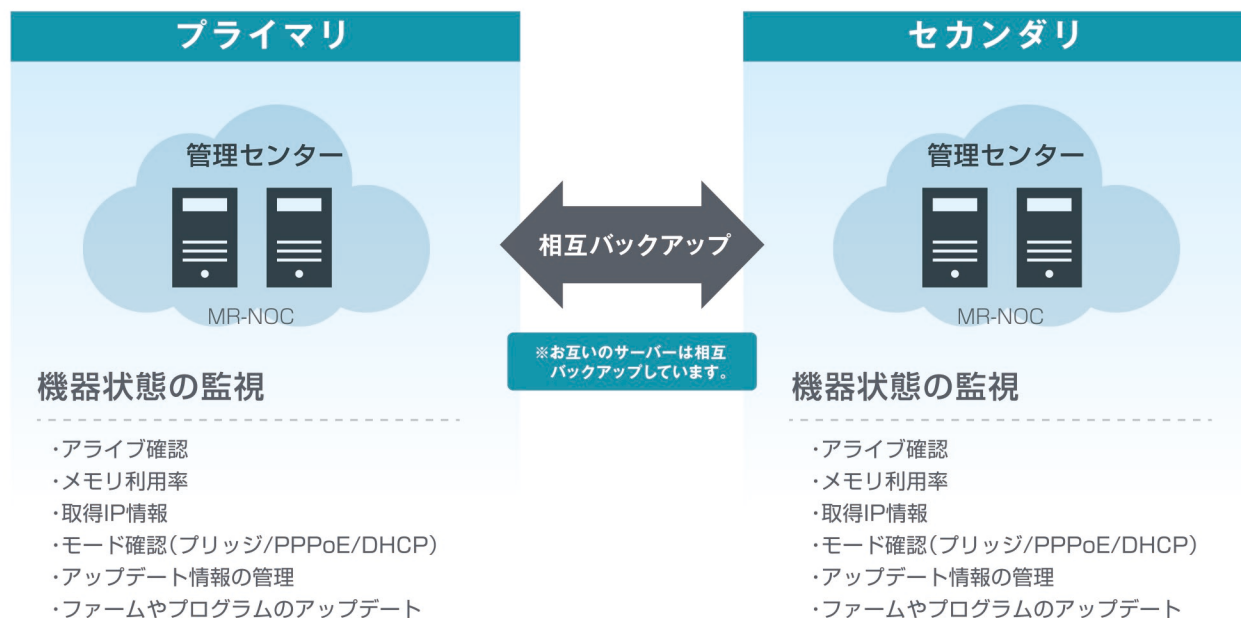
基本的な設定をするだけで、運用はお任せ！

脅威インテリジェンス

BrightCloud® Threat Intelligence; BCTI



管理サーバーMR-NOC



搭載セキュリティソリューション

FW



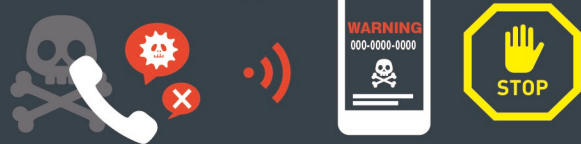
外部ポートは閉じたまま、ステルス状態で通信をします。もちろん、外部からの一方的な通信は遮断しますので、ネットワークに対する攻撃から守ります。もちろん、管理は不要。MR-NOCでコントロールします。

File-Reputation



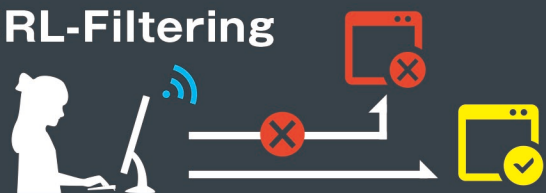
Web閲覧時に、マルウェアが含まれていないか、怪しい挙動をするファイルが潜んでいないかをチェックします。Webroot社のBCTI上の90億を超えるフレッシュなビッグデータを常に参照します。ですから、新しいマルウェアへの対応が非常にスピーディーです。

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、通信が見つかりと遮断します。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



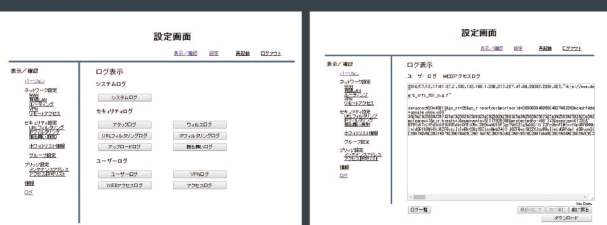
アウトバウンド通信全ポートを監視している機能です。IP-ReputationやURL-Reputation/Classificationをコントロールすることで、知らず知らずに外に通信されていても、危険が含まれる先への通信は遮断します。

※IPS機能は、17年秋に搭載予定

グループ設定

設定画面				
表示 / 確認 設定 再起動 ログアウト				
設定	ネットワーク設定	セキュリティ設定		
	グループ	グループ設定		
	グループ1	優先度	詳細	編集 / クリア
	グループ2	0	0設定	
	グループ3	1	0設定	
	グループ4	2	0設定	
	グループ5	3	0設定	
	グループ6	4	0設定	
	グループ7	5	0設定	
	グループ8	6	0設定	
	グループ9	7	0設定	
	グループ10	8	0設定	
	グループ11	9	0設定	
	グループ12	10	全て	

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『コレダクトオス』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、検知して件名に任意の文字列を入れます。

※POP/POPS/IMAP/IMAPSに対応。POPS/IMAPSの対応メーラーは17年3月現在MicrosoftOutLookです。
その他のメーラーは順次対応予定です。

HW仕様

	MRB-50
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)
メモリ	NAND FLASH 256MB、DRAM1GB、NOR FLASH 2MB、EEPROM 2kByte
ストレージ	8GB(SD)
イーサネット	10BASE-T/100BASE-TX/1000BASE-T × 2ポート
Wi-fi	○(802.11b/a/g, 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)
スループット(全機能稼動)	最大160Mbps(有線利用時)
VPN接続台数	～5台程度 ※MRB-50同士の場合
対象端末台数	～5台程度
リモートアクセス	最大5台(同時接続)
大きさ	174.0mm(W)×111.0mm(D)×33.0mm(H)(アンテナ含まず)
重量	400g
使用電源・電源形状	DC12V ±10%
消費電力	計測中
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)

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))は検知のみ)
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
リモートアクセス	3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『コレダケトオス』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。

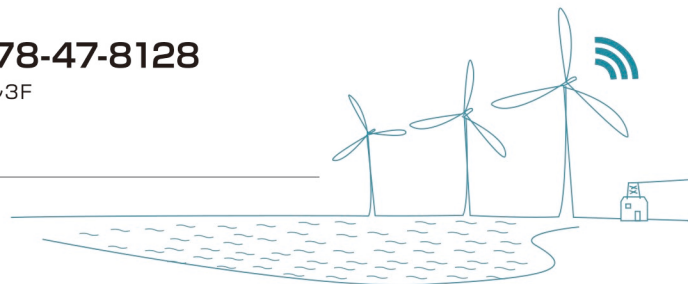
Technol

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®