

Cloud型UTM **MRB-cloud** のご紹介

株式会社アンペール 2022年12月

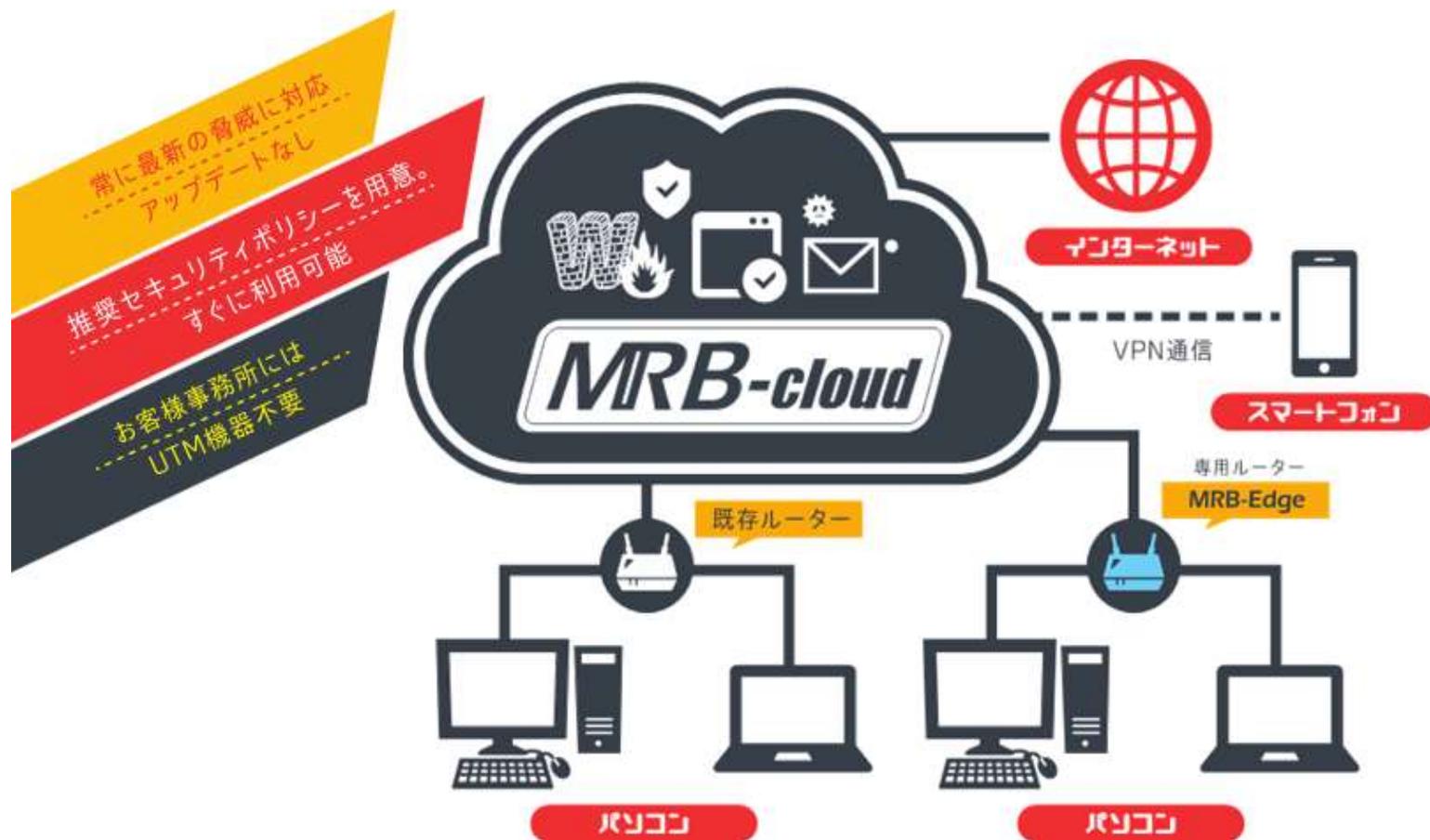


MRB-cloudの概要

MRB-cloudはクラウド上で使用するUTMサービスです。

お客様ネットワーク・PC・スマホ等からVPNで接続することで、インターネット上の脅威から保護します。

脅威インテリジェンスにWebroot社のBrightCloud®を使用する事で、常に最新のセキュリティを提供します。



MRB-Cloud 導入メリット

● 専用ハードウェア不要

既存のルーターがVPN接続できれば導入時の設定もらくらく。

※ VPN接続 (IKEv2) ができて、インターネット通信をVPNに向けることができるルーターが条件となります。

● 常に最新のセキュリティを提供

ソフトウェアを導入したり定義ファイルデータを更新する手間はありません。

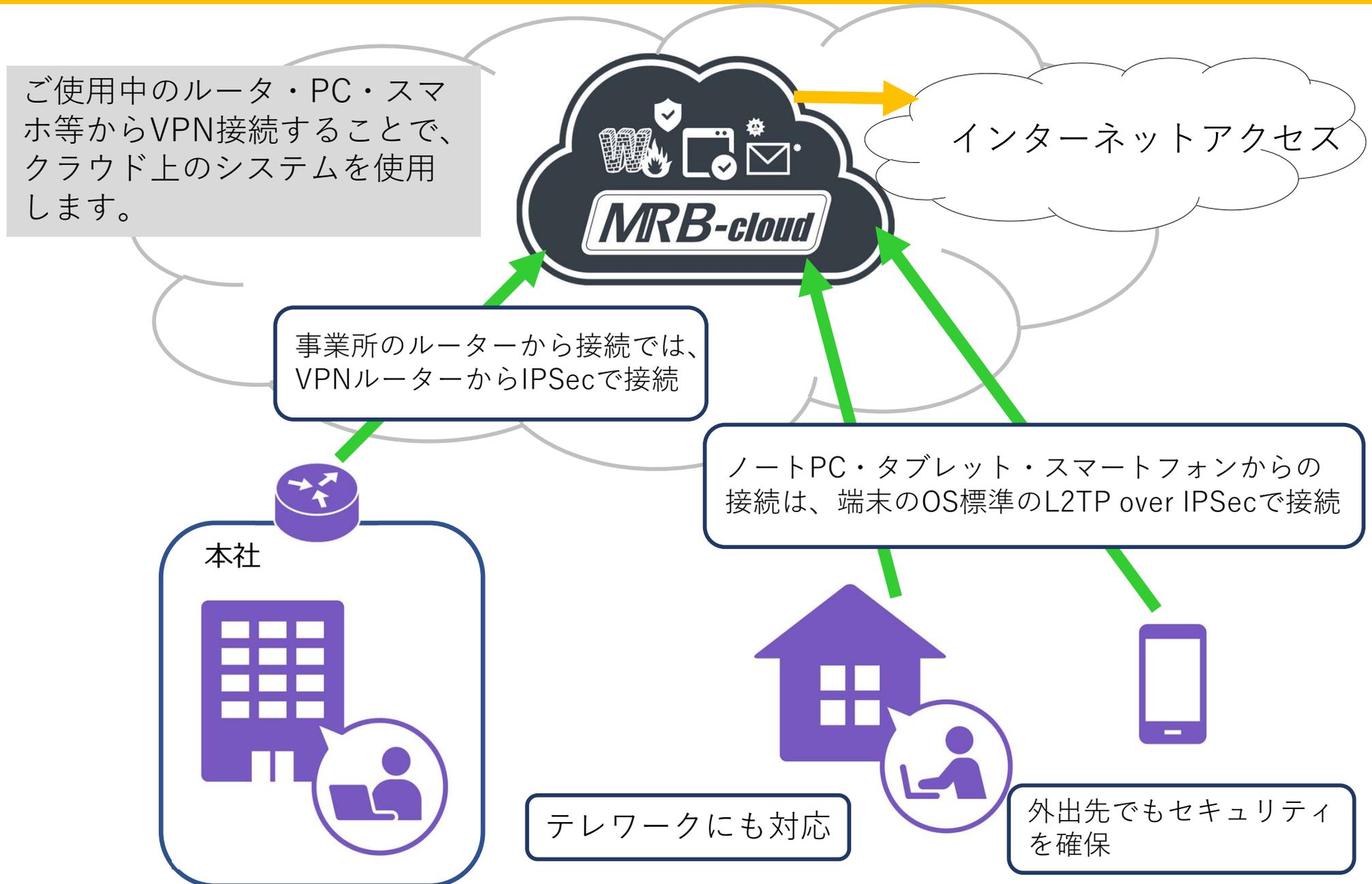
● 業務規模の変化に柔軟に対応可能

端末増加などの規模の拡大などに対してプラン変更で対応できます。

● 外出先でも、セキュリティを確保してインターネット通信が可能

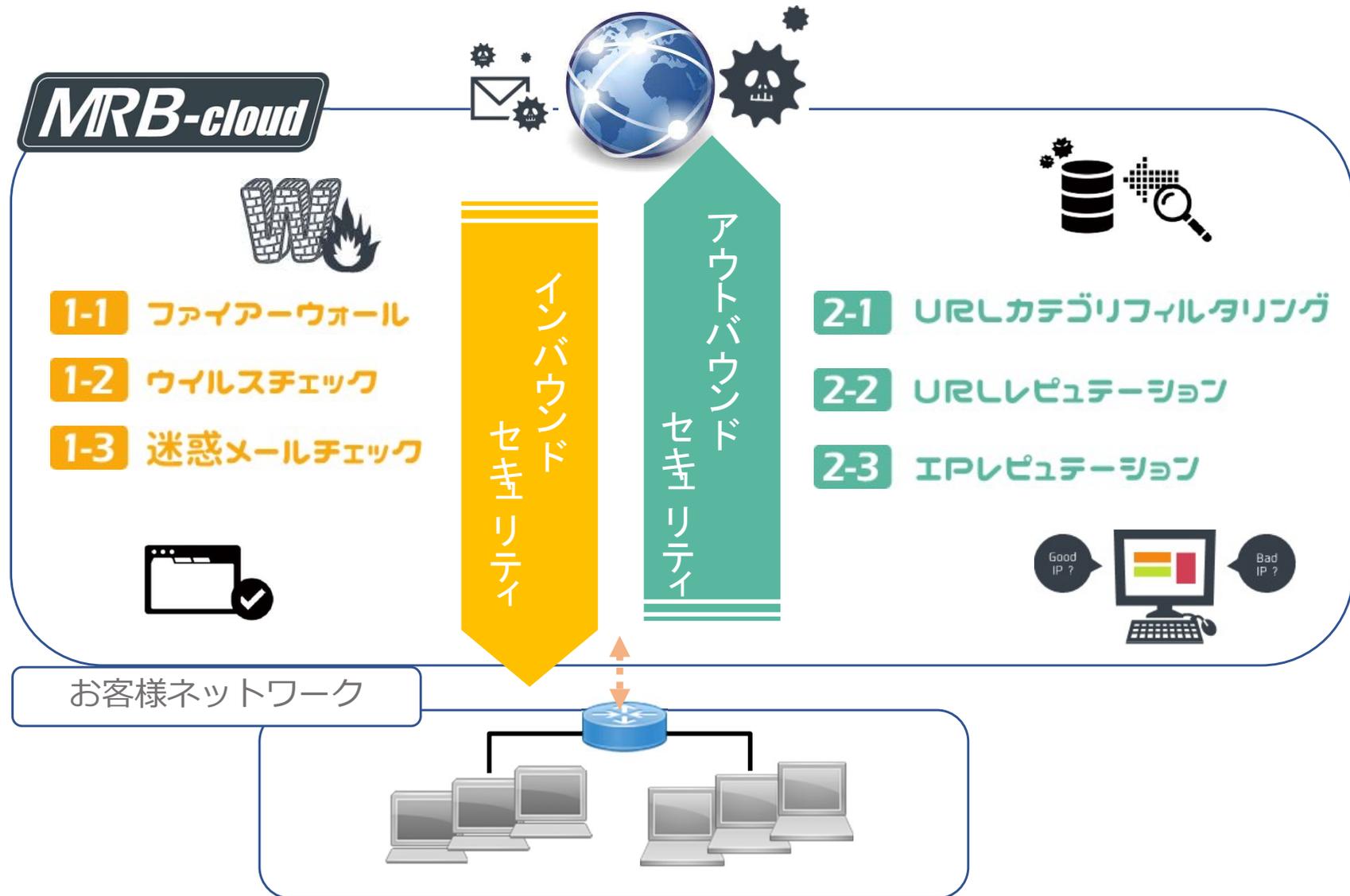
固定IPアドレスが無くても外出先から事務所にリモートアクセスが可能です。

MRB-cloud利用イメージ



MRB-Cloud セキュリティ機能

MRB-cloudは通信の入出力方向でチェックを行い、インターネットの脅威へ対処します。



MRB-cloudのセキュリティ機能

1 インバウンドセキュリティ

1-1 ファイアーウォール



外部ポートは閉じたまま、ステルス状態で通信します。
外部からの一方的な通信を遮断する事で、
ネットワークに対する攻撃から防御ます。

1-2 ウィルスチェック



約140億以上あるマルウェアのハッシュ情報を基に、お客様システムをマルウェアから守ります。
従来のシグネチャ方式に比べて、脅威が見つかったからの対応スピードが格段に速く、常に最新データを持つデータベースを参照しています。

1-3 迷惑メールチェック



受信メールの発信元サーバーのIPアドレスを ※BCTIに問い合わせします。
発信元サーバーのIPアドレスに脅威が潜んでいる場合には、件名に任意の文字列を付加しユーザーに危険をお知らせします。

MRB-cloudのセキュリティ機能

2 アウトバウンドセキュリティ

2-1 URLカテゴリフィルタリング



インターネットのサイトを、78のカテゴリに分類していきます。フィルタリングレベル「なし」「低」「中」「高」から選びます。一つ一つカテゴリを選択できる「カスタム」も選ぶこともできます。

2-2 URLレピュテーション



URLフィルタリングレベルと合わせて独自のスコアリングをします。レベルに応じたスコアに満たない場合はブロックします。

2-3 IPレピュテーション



ブラウジングだけでなく、インターネットに出る全ての通信のIPアドレスに危険がないかもチェックします。

MRB-Cloud セキュリティ機能

SSL通信検知機能



暗号化されたSSL通信でもMRB-Cloudにて復号処理を実施しセキュリティチェックが可能です。

対応メーカー：Outlook

対応ブラウザ：IE/FireFox/Chrome/safari

対応OS：Win7/Win10/Mac/iOS

※端末に証明書を設定する必要があります。

ログ機能

ログは2種類取得可能です。ログ保存期間は1ヶ月です。
通常ログ：リクエストがあった際のログを保持します。
検知ログ：ブロックしたログを保持します。

ユーザーログ - WEBアクセスログ

```
2018/08/14 01:08:04.0.100.192.188.1.209.69.192.229.149.25554.813.GET,"http://www
2018/08/14 01:08:04.0.100.192.188.1.209.202.229.2.83.25558.588.GET,"http://crl.m
2018/08/14 01:08:04.0.100.192.188.1.209.202.229.2.83.25558.521.GET,"http://crl.m
2018/08/14 01:08:04.0.100.192.188.1.209.202.229.2.83.25558.558.GET,"http://crl.m
2018/08/14 01:08:04.0.100.192.188.1.209.202.229.2.83.25558.530.GET,"http://crl.m
2018/08/14 01:25:58.0.100.192.188.1.209.202.229.2.130.25743.521.GET,"http://crl.r
2018/08/14 01:25:58.0.100.192.188.1.209.202.229.2.130.25743.530.GET,"http://crl.r
2018/08/14 01:25:58.0.100.192.188.1.209.202.229.2.130.25743.558.GET,"http://crl.r
2018/08/14 01:25:58.0.100.192.188.1.209.117.18.237.29.25751.471.GET,"http://ocsp
2018/08/14 02:10:37.0.100.192.188.1.209.172.217.31.131.26188.608.POST,"http://upc
2018/08/14 02:57:58.0.100.192.188.1.209.61.194.99.210.26822.521.GET,"http://crl.r
2018/08/14 02:57:58.0.100.192.188.1.209.61.194.99.210.26822.530.GET,"http://crl.r
2018/08/14 02:57:58.0.100.192.188.1.209.61.194.99.210.26822.558.GET,"http://crl.r
2018/08/14 03:31:40.0.100.192.188.1.209.61.194.99.211.26952.588.GET,"http://crl.r
2018/08/14 03:31:41.0.100.192.188.1.209.61.194.99.211.26952.521.GET,"http://crl.r
2018/08/14 03:31:41.0.100.192.188.1.209.61.194.99.211.26952.558.GET,"http://crl.r
2018/08/14 03:31:41.0.100.192.188.1.209.61.194.99.211.26952.530.GET,"http://crl.r
2018/08/14 03:59:58.0.100.192.188.1.209.61.194.99.211.27262.521.GET,"http://crl.r
2018/08/14 03:59:58.0.100.192.188.1.209.61.194.99.211.27262.530.GET,"http://crl.r
2018/08/14 03:59:58.0.100.192.188.1.209.61.194.99.211.27262.558.GET,"http://crl.r
2018/08/14 04:04:59:49.0.100.192.188.1.209.202.229.2.129.28123.19189.GET,"http://off
2018/08/14 04:04:59:49.0.100.192.188.1.209.202.229.2.129.28123.19115.GET,"http://off
2018/08/14 05:00:19.0.100.192.188.1.209.61.194.99.211.28145.588.GET,"http://crl.r
2018/08/14 05:00:20.0.100.192.188.1.209.61.194.99.211.28145.521.GET,"http://crl.r
2018/08/14 05:00:20.0.100.192.188.1.209.61.194.99.211.28145.558.GET,"http://crl.r
2018/08/14 05:00:20.0.100.192.188.1.209.61.194.99.211.28145.530.GET,"http://crl.r
2018/08/14 05:58:59.0.100.192.188.1.209.61.194.99.210.28712.521.GET,"http://crl.r
2018/08/14 05:58:59.0.100.192.188.1.209.61.194.99.210.28712.530.GET,"http://crl.r
2018/08/14 05:58:59.0.100.192.188.1.209.61.194.99.210.28712.558.GET,"http://crl.r
2018/08/14 07:11:17.0.100.192.188.1.209.172.217.31.131.29407.608.POST,"http://upc
2018/08/14 07:36:58.0.100.192.188.1.209.61.194.99.211.29676.521.GET,"http://crl.r
2018/08/14 07:36:58.0.100.192.188.1.209.61.194.99.211.29676.530.GET,"http://crl.r
2018/08/14 07:36:58.0.100.192.188.1.209.61.194.99.211.29676.558.GET,"http://crl.r
2018/08/14 07:36:58.0.100.192.188.1.209.61.194.99.211.29676.521.GET,"http://crl.r
```

ウイルスログ；	ウイルスチェックした際に記録
URLフィルタリングログ；	URLフィルタ及びレピュテーションでブロックされた際に記録
IPフィルタリングログ；	インターネット利用時に接続先のIPに危険が潜んでいてブロックした際に記録
アップロードログ；	データのアップロードの記録
ふるまいログ；	意図しない通信をブロックした際に記録

1-71/71 件 1/1 ページ

ページ指定 前のページ 次のページ

2018/08/14

一覧に戻る 最新のログ 前日のログ 後日のログ

ダウンロード

MRB-Cloud セキュリティ機能

レポート機能

登録いただいたメールアドレスにレポートを配信します。

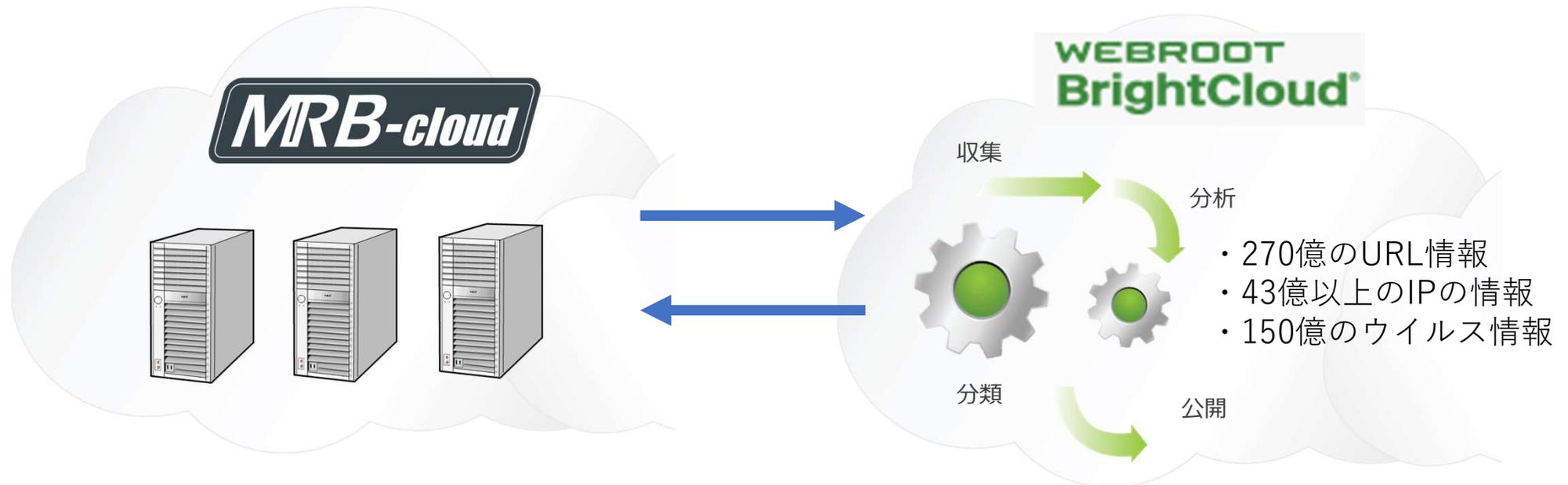
- 登録できるアドレス数：2つ
- レポート送出タイミング：週に1回

レポートサンプル

1. ウイルスブロックログ
 - ウェブ閲覧時 0回
 - ウイルスメール送受信 0回
 - 週間合計 0回
2. URLフィルタブロックログ
 - 週間合計 0回
 - ブロックカテゴリTOP5
 - 27 ギャンブル
 - 34 ゲーム
 - ブロックPC TOP5
 - 1.xxx.xxx.xxx
 - 2.xxx.xxx.xxx
3. IPフィルタブロックログ
 - 週間合計 0回
 - ブロック先IPアドレスTOP5
 - 1.xxx.xxx.xxx
 - 2.xxx.xxx.xxx
 - ブロックPC TOP5
 - 1.xxx.xxx.xxx
 - 2.xxx.xxx.xxx
4. 迷惑メール判定
 - メール総数 0通
 - 迷惑メール判定数 0通

脅威インテリジェンスについて

脅威インテリジェンスには、業界最大規模の脅威データベースと、AI・機械学習能力と情報提供体制を誇る、Webroot社のBrightCloud®を使用し、常に最新のセキュリティを提供します。



-BCTIについて-

Webroot BrightCloud® Threat Intelligence (BCTI)は、IPアドレス・URL・ファイル等の、膨大な脅威データベースをクラウド上に保有しています。

過去に危険もしくは怪しい行動（攻撃元、踏み台、マルウェア配布など）が確認されたブラックリストだけではなく、将来的な攻撃の発生リスクを数値化する予測型インテリジェンスを提供しています。

MRB-cloudに係る費用について

■ MRB-cloudと一般的なUTM製品の料金体系比較

	MRB-cloud	一般的なUTM製品（参考）
初期費用	<ul style="list-style-type: none">・ 初期登録費用・ 年間ライセンス（1年分） <p>※機器設定変更を弊社実施の場合は別途費用が発生します</p>	<ul style="list-style-type: none">・ 本体価格・ 構築費用・ 保守費用（1年分）
次年度以降年間費用	<ul style="list-style-type: none">・ 年間ライセンス	<ul style="list-style-type: none">・ ライセンス費用・ 保守費用
更新期間	契約中は継続して利用可能	一般的に5年程度でリプレイスが必要

■ MRB-cloud料金の特徴

- ・ 年間ライセンス費用を使用機器台数で計算
 - ☞ 機器を導入する場合と費用の考え方が異なります。
 - 拠点数が多い・端末数が少ない等のケースでは、大幅に費用を抑える事ができます。
- ・ 機器リプレイスが不要
 - ☞ 何年使用しても更新費用が発生しません。

導入例（製造業）

	導入前の課題	導入後の効果
Case 1	<u>ルータのみで拠点間通信をしておりセキュリティ対策を早急にする必要があった。</u>	導入規模：2拠点100端末 注文から 3営業日で運用開始 （セキュリティ強化）ができた。
Case 2	既存UTMのサポート切れに伴うリプレイス及び運用 <u>工数削減したい。</u>	導入規模：3拠点200端末 管理画面がシンプルで分かり易いので、運用に関して 専任の担当者が不要になった。
Case 3	<u>事業拡大(拠点含む)にともなうサイジングやコストが読めず困っていた。</u>	導入規模：2拠点50端末 拠点/クライアントが増えても モデルチェンジが不要なく、結果コスト削減となった。 また、運用工数も削減につながった。

導入例（出版業）

	導入前の課題	導入後の効果
Case 4	5年ごとにアプライアンス型UTM機器の入替導入していたが、価格改定（値上）もありコスト増に困っていた。	<p>導入規模：3拠点50端末</p> <p>5年毎にUTM機器の入替費用が発生していたが、クラウドサービスに切り替えることで<u>機器入替の費用を抑える</u>ことが出来るようになった。</p> <p>検討から導入までの時間に余裕がなかったが、MRB-cloudであれば数日で導入できることがわかり導入を決めた。</p> <p>実際<u>3営業日程度</u>で導入完了できた。</p>

導入例（医療関係）

	導入前の課題	導入後の効果
Case 5	NW環境の見直しに合わせて、セキュリティ強化をしたい。 なお導入後の <u>運用管理が容易なものを</u> 探していた。	導入規模： 1拠点20端末 クラウドサービスを選択したことにより <u>ファームアップを含むメンテナンス工数が削減された。</u>

導入例（物流業）

	導入前の課題	導入後の効果
Case 6	もともとアプライアンス型のUTMを各拠点に配備していたが、複数毎の管理工数や導入/運用費用を <u>セキュリティレベルは維持しつつ、コスト削減をしたかった。</u>	<p>導入規模： 5拠点50端末</p> <p>クラウド型のサービスということもあり、導入時に端末側の設定変更はなく、容易に切り替えができた。 定期的なレポートによる通知機能があるので、ネットワークの見える化で安心を得ることができた。</p> <p>MRB-cloud導入後は、今までの運用コストと比較して 50%程度削減することができ、セキュリティレベルも維持できた。</p>

MRB-cloud トライアル



トライアルの利用を用意しています。
弊社担当営業までお問い合わせください。

【お問い合わせ先】

株式会社アンペール 情報機器部

TEL : 03-5330-6802

E-Mail : it-sales@ampere.co.jp

<https://www.ampere.co.jp/it/network/mrb-cloud/>