

駆けつけ対応状況および クラウド型UTM配備状況について

2019年10月
ALSOK

駆けつけ隊の稼働状況

クラウドUTMの配備状況

クラウドUTMの利用終了および継続利用について

駆けつけ隊の稼働状況

[概要]

- 実証事業期間中に、サイバーセキュリティに関する相談・有事の際の対応受付のため、ALSOKが現地へ駆けつけ、対応の支援を行うものです。
- お客様のPCから1次調査に必要なPCの情報を確保します。
 - 不正プログラムと疑われるプログラムのインストール履歴の調査
 - データの持ち出しと思われる操作の履歴調査 など

[駆けつけ隊 出動実績] ※10月1日現在

出動実績： 1 件（内容は次ページ）

駆けつけ対応実績の事例紹介

- 据置型UTMの配備先で、特定の端末から不正な通信先への通信を検知。
- お助け隊コールセンターより連絡、ご担当者と会話するも、当該端末を特定できず。
- 端末特定を目的に、駆けつけ隊の出動を実施。
- 自動でNW接続端末の一覧を作成する機器を設置し、社内には存在するIT機器の“見える化”を実施。
- 不正な通信は、社内無線LANに無断で接続された社員の私物スマートフォンであった。

[考えられる重篤な被害想定]

- 今回、検知した不正通信先は、過去にマルウェアの配布や、ランサムウェアの配布に利用されていることが確認されているC2サーバーでした。
- 今回はUTMによって通信がブロックされ、検知・保護されましたが、最悪の場合は…
 - マルウェア感染による情報漏えい、社内PCへの感染拡大
 - ランサムウェアへの感染などの被害発生が考えられます。

(参考)被害発生時に係るPC等の詳細調査価格例

1. PC詳細調査費用	1台	140万円
2. サーバ詳細解析費用	1台	170万円
3. Proxy詳細調査費用	1台	60万円

駆けつけ隊の稼働状況

クラウドUTMの配備状況

クラウドUTMの利用終了および継続利用について

クラウドUTMの配備・検知状況

[配備状況] ※10月11日現在

対象：66社（接続済:11社 ご案内済:23社 調整中:13社 申込書未受領:19社）

[アラート検知状況]

特になし

[クラウドUTM導入にあたってのお願い]

- 「MRB-Cloud登録申込用紙」を未提出の事業者は、早急にご提出をお願いします。
- 登録申込書の記載内容の不備による手戻りが多く発生しています。記載内容でご不明の点はお問い合わせください。
- クラウドUTMの導入にあたっては、ルータの設定変更作業およびケーブルの繋ぎ換え作業が発生します。作業時には変更内容を記録していただくようお願いします。
- 拠点間VPNをご利用中の事業者様は、事前にご相談ください。
- クラウドUTMの導入に当たって、不明点がありましたらお気軽にご相談ください。

お問い合わせ窓口

ALSOK 情報警備監視センター

電話：0120-6845-74 メール：info@i-sec.alsok.co.jp

駆けつけ隊の稼働状況

クラウドUTMの配備状況

クラウドUTMの利用終了および継続利用について

クラウドUTMの利用終了および継続利用について

クラウドUTMの無償配備は、実証事業期間中のみとなります。

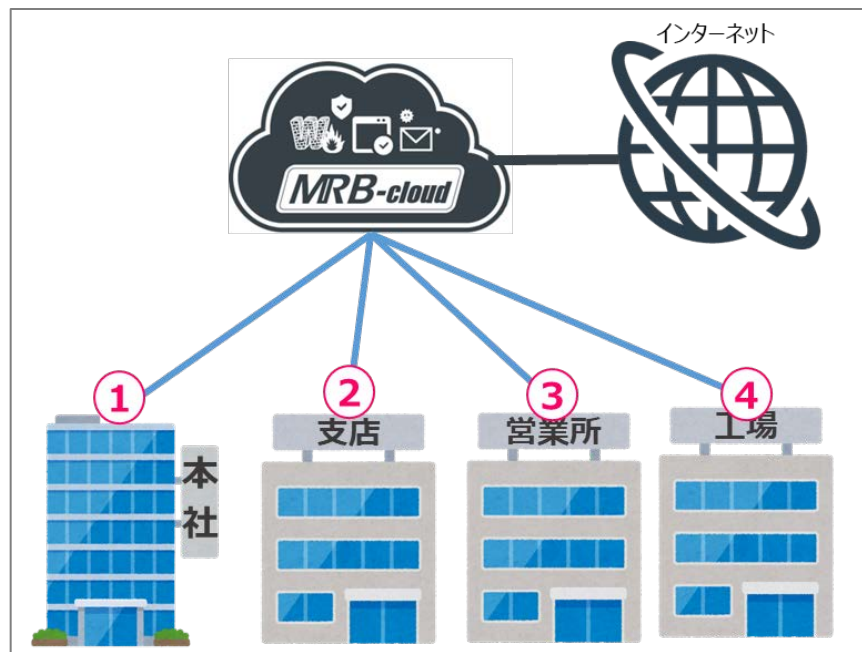
- 実証事業終了後のクラウドUTMの利用については、**「利用終了」**または**「継続利用」**のいずれかを選択いただけます。
- 実証事業終了後にどちらを選択されるかについては、ALSOKよりご案内を電子メールにて送付いたします。
- 案内受領後は、ご回答うえ、速やかにお手続きをお願いいたします。



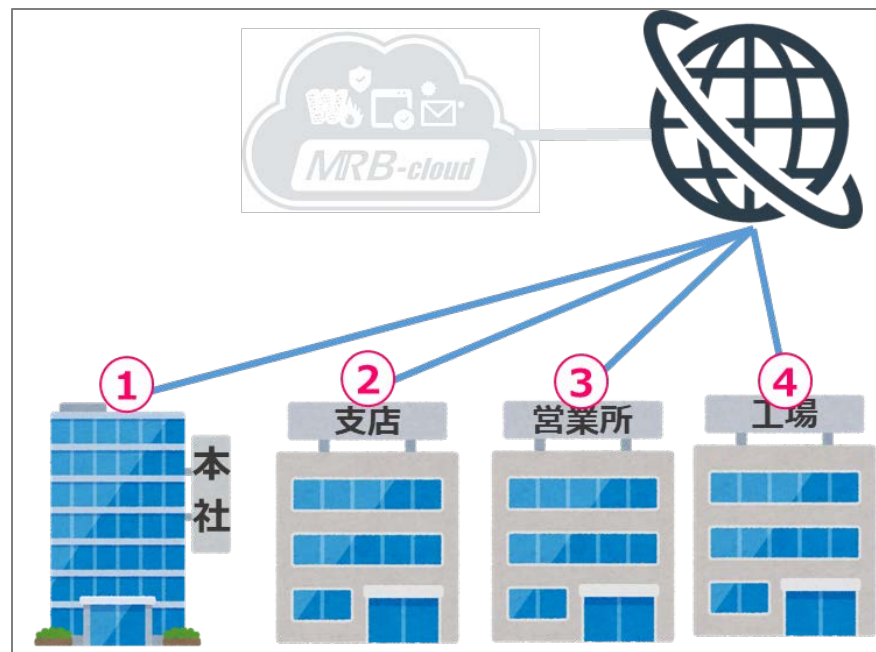
クラウドUTMの利用終了について①

- クラウドUTMの利用を終了する場合、実証事業期間終了後、速やかにルータ等の設定変更をお願いします。（クラウドUTMへ接続する設定の削除）
- クラウドUTMの利用継続手続きをしていただけないまま、実証事業期間後もクラウドUTMを利用された場合、クラウドUTM側でサービスを停止する、もしくはご利用料金を請求するなどの対応をとらせていただきますので、ご注意ください。

構成例



クラウドUTM利用中



クラウドUTM利用終了後

※設定漏れのないよう、ご注意ください。

クラウドUTMの利用終了について②

- レンタルルータをご利用中のお客様は、ルータの設定変更後、ご返却をお願いします。
- クラウドUTMの利用継続手続きをしていただけないまま、実証事業期間後もレンタルルータをご返却いただけない場合は、買取とさせていただくこともありますのでご注意ください。
- 回収時期については、別途お知らせします。



レンタルルータ

レンタルルータは以下の宛先に送付をお願いいたします。

〒031-0072

青森県八戸市城下1丁目10-15

株式会社テクノル IS推進部

クラウドUTMの継続利用について

- クラウドUTMを継続利用される場合は、ALSOKと直接契約するための手続きが必要となります。継続利用をご希望のお客様には別途ご案内いたします。
- クラウドUTMを継続利用される場合は、以下の価格（予定）でご利用いただくことができます。
- レンタルルータの継続利用は買取とさせていただきます。

クラウドUTM 参考価格(税別) ※1

ご利用規模	初期費用	月額料金
1～5台	0円	2,400円
6～11台	0円	3,000円
11～50台	0円	7,800円
51～100台	0円	15,600円
101～200台 ※2	0円	31,200円

レンタルルーター 参考価格 ※2

予定価格	年額保守費用
58,000円	12,000円

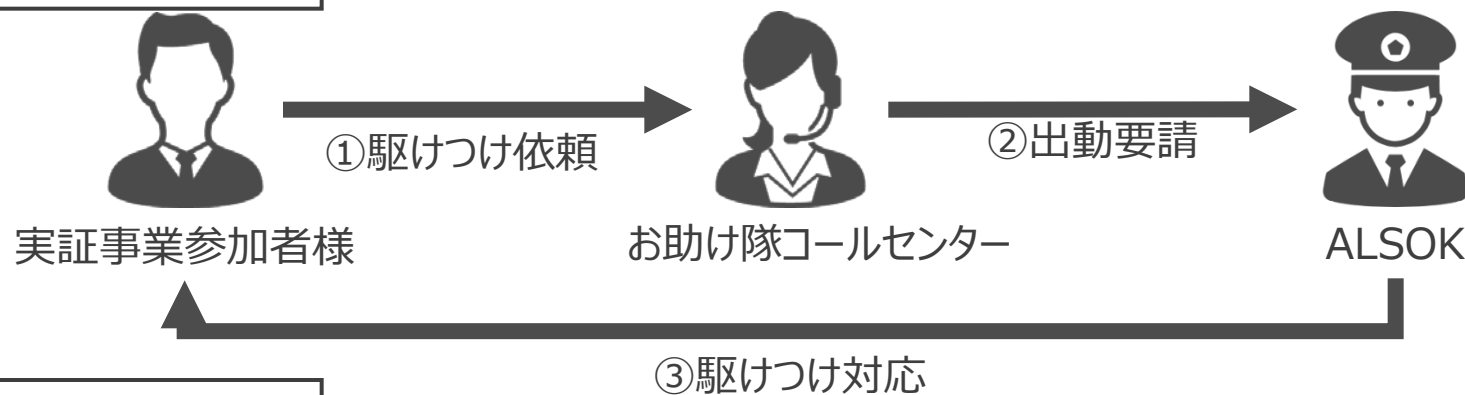
※1 上記価格は現時点での参考価格であり、今後変更となる可能性があります。

※2 端末台数200台超の場合は、別途お見積りとなります。

実証事業終了後の駆けつけ隊のサービス提供について

- 実証事業終了をもって、駆けつけ隊のサービス提供は終了します。
- 駆けつけ隊とお助け隊コールセンターの連携も終了しますのでご注意ください。
- 実証事業終了後、インシデント対応をご希望されるお客様は、ALSOK情報警備監視センターにて相談をお受けし、状況をお伺いしたうえで専門会社をご紹介します。（※クラウドUTMのご契約者様に限りです）

実証事業期間中



実証事業終了後

