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

2020年1月
ALSOK

駆けつけ隊の稼働状況

クラウド型UTMの配備状況

クラウド型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次調査に必要となる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] ※12月28日現在

出動実績：3件（内容は次ページ）

駆けつけ対応の事例紹介

出動事例１

- 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し、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。

出動事例２

- 従業員が業務で使用しているPCに詐欺ソフトをインストールしてしまった恐れ。
- お助け隊コールセンターより要請を受けて、駆けつけ隊が出動して必要情報を取得。
- 取得した情報を解析した結果、詐欺ソフトがインストールされていること、インストールされた経緯が判明。解析結果および対処方法をお客様にご報告。
- 後日お客様で当該詐欺ソフトのアンインストールを実施。

駆けつけ対応実績の事例紹介

出動事例３

- 据置型UTMの配備先で、5台の端末からポートスキャンを検知。
- 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。
- 端末特定および必要情報の取得のため、駆けつけ隊の出動を実施。
- 駆けつけの結果、通信の発信元はPC2台、プリンタ2台、不明1台であった。うちPC2台から必要な情報を取得。
- しかし、取得した情報を解析するも不正な通信の原因となるプログラムの特定に至らず。現在も、別手法での調査の実施、専門会社への引き渡しの検討も含めて継続対応中。

駆けつけ隊の稼働状況

クラウド型UTMの配備状況

クラウド型UTMの利用終了および継続利用について

クラウド型UTMの配備・検知状況

[配備状況]※12月31日現在

当初配備予定	現在の配備予定 (12/31現在)	接続完了 (12/31現在)
100社	48社	28社

[アラート検知状況] ※12月28日現在

特になし

- クラウド型UTMには自動でアラートを発出し利用者に通知する機能を持ちません。
  代わりに週次レポートを電子メールで送信し、利用者の能動的アクションを可能にしています。
- 週次レポートは毎週月曜日に登録されたメールアドレスに対して送信します。
- 週次レポート内容について気になること、ご不明な点があれば以下にお問い合わせください。

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

クラウド型UTMで検知されたデータ

[外部→内部の通信]※12月28日現在

No.	プロトコル/ポート番号	検知件数
1	TCP/23	9,182
2	TCP/80	1,943
3	TCP/22	1,293
4	ICMP/-	947
合計		13,365

[内部→外部の通信]

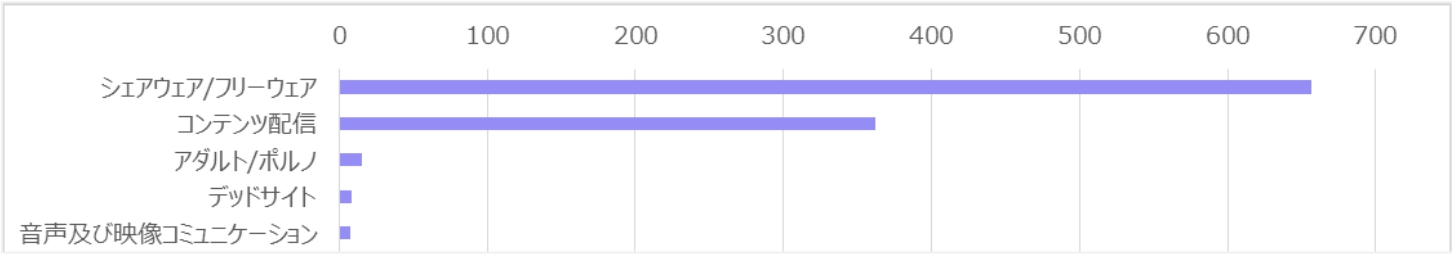


図. URLフィルタリングの検知状況（11月上位5項目）

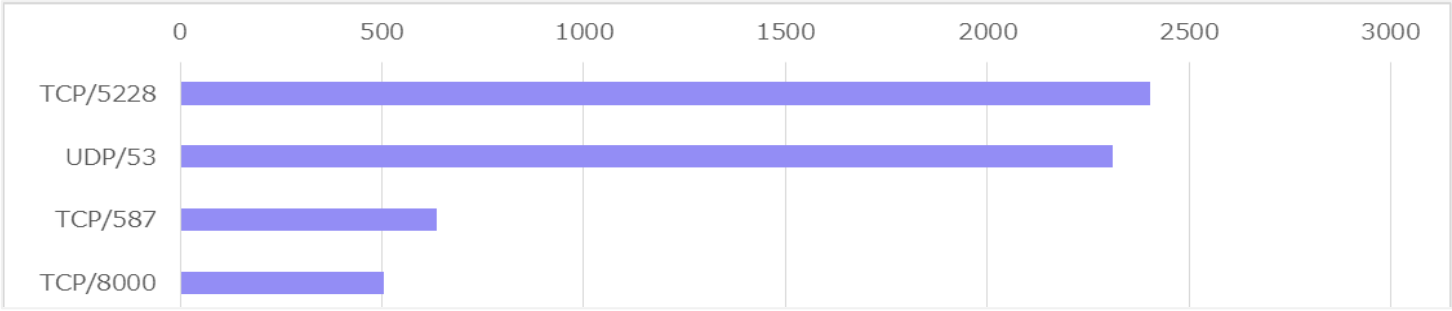


図. 振る舞い検知状況（11月上位5項目）

駆けつけ隊の稼働状況

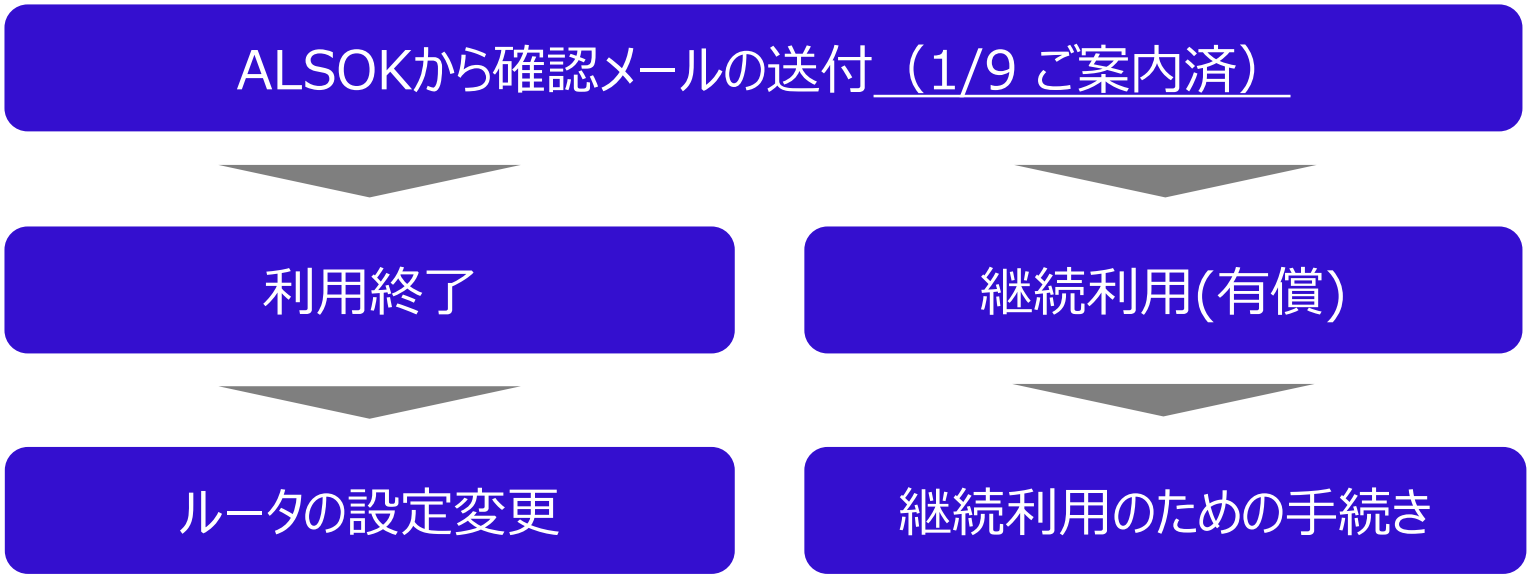
クラウド型UTMの配備状況

クラウド型UTMの利用終了および継続利用について

クラウド型UTMの利用終了および継続利用について

クラウド型UTMの無償配備は、実証事業期間中のみとなります。

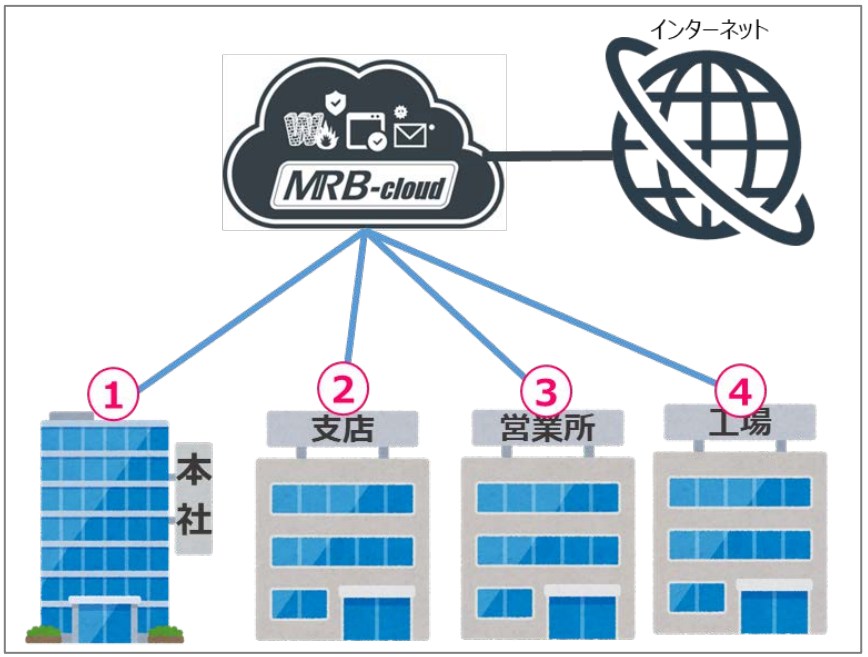
- 実証事業終了後のクラウド型UTMの利用については、**「利用終了」**または**「継続利用」**のいずれかを選択いただけます。
- 実証事業終了後にどちらを選択されるかについては、ALSOKよりご案内を電子メールにて送付いたします。
- 案内受領後は、ご回答うえ、速やかにお手続きをお願いいたします。（1/20〆切）



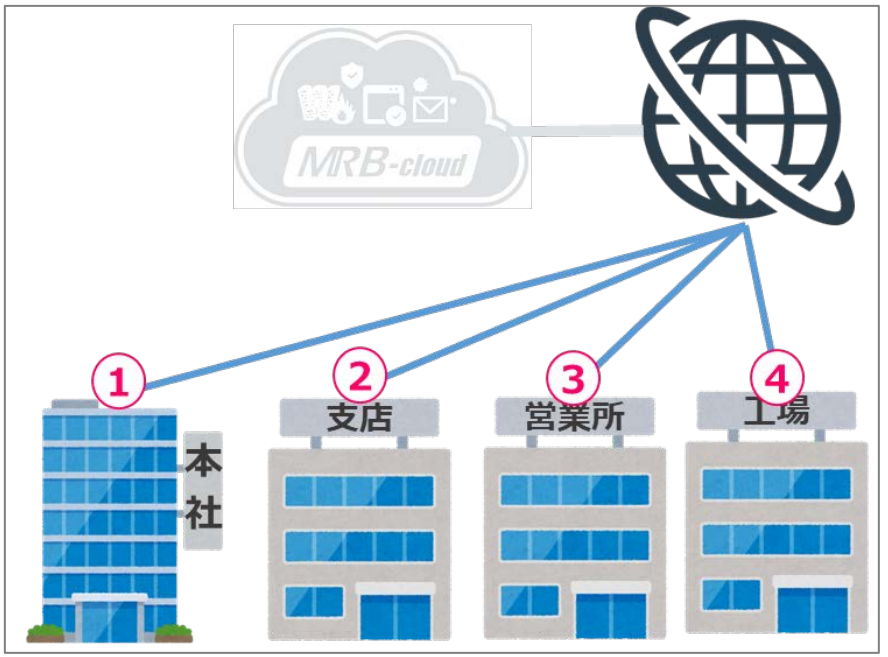
クラウド型UTMの利用終了について①

- クラウド型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。（クラウド型UTMへ接続する設定の削除）
- クラウド型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型UTMを利用された場合、クラウド型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。

クラウド型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。
- クラウド型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下さい。
- 回収時期については、個別にお知らせいたします。

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　宛~~

送付先、送付方法については、
別途ご案内いたします。

クラウド型UTMの継続利用について

- クラウド型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手続き方法を別途ご案内いたします。
- クラウド型UTMを継続利用される場合は、以下の価格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。

クラウド型UTM　価格(税別)

ご利用規模	初期費用※1	月額料金
1～5台	0円	2,400円
6～10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 価格(税別)

販売価格	年額保守費用
58,000円	12,000円

※1 実証事業期間中にクラウド型UTMへの接続が完了している企業向け価格です。実証事業期間後にクラウド型UTMに接続する場合は初期費用が発生します。

※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。（※クラウド型UTMのご契約者様に限ります）