CTC
Challenging Tomorrow's Changes

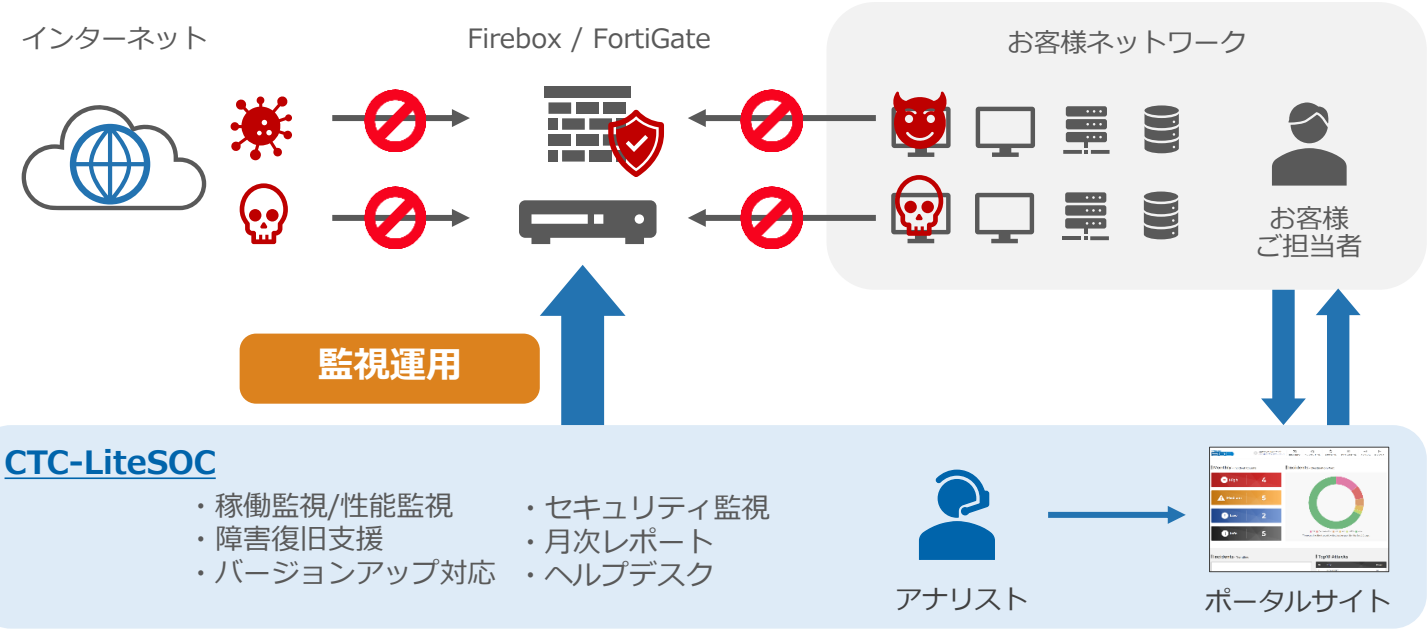
CTC-CSS
MSS

CTC-LiteSOC
for Fortigate のご紹介

伊藤忠テクノソリューションズ株式会社

サービス概要

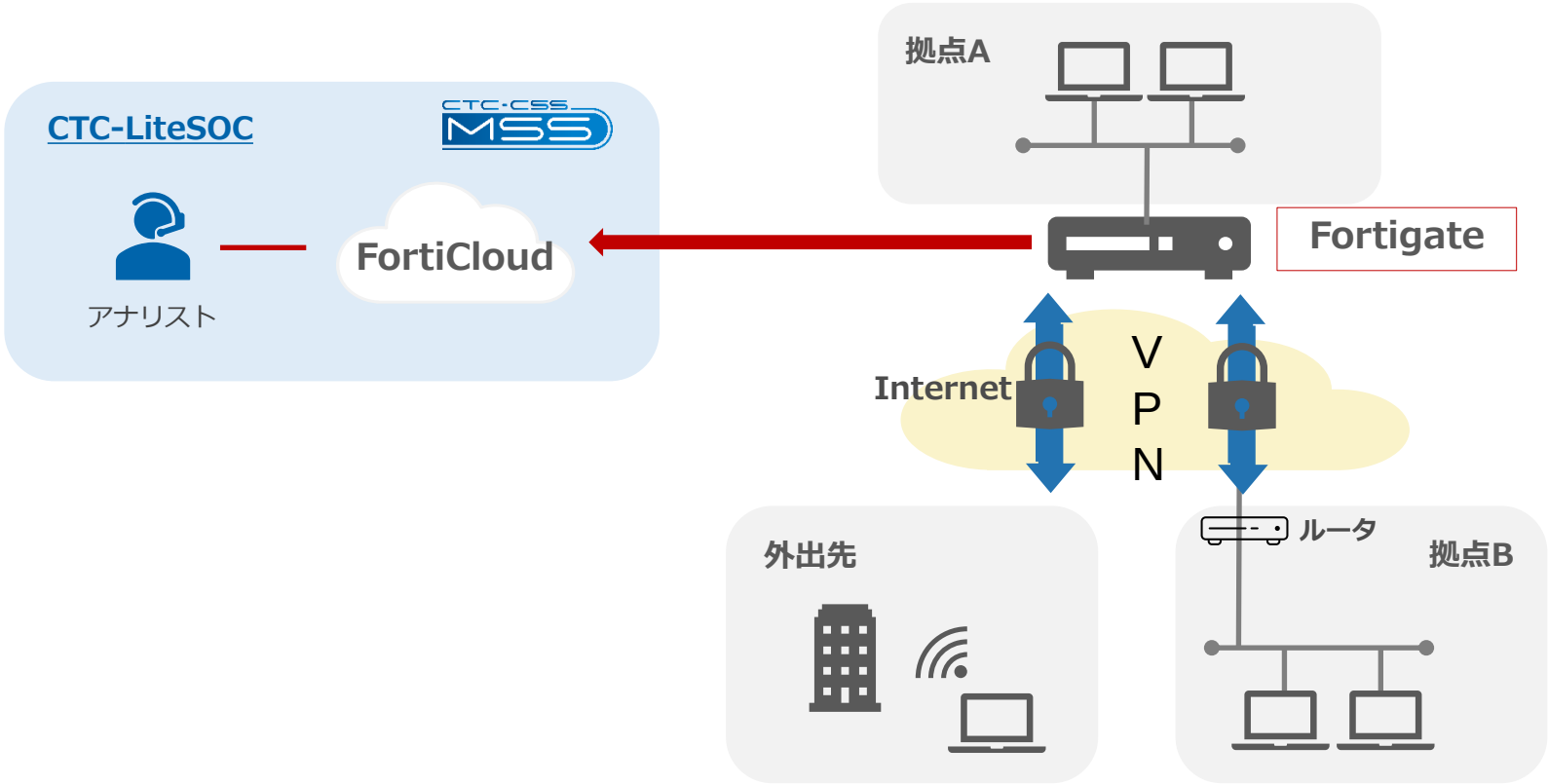
お客様環境のネットワークインフラを監視し、機器故障、通信障害、サイバー攻撃などをいち早く検知する総合セキュリティ運用サービスです。日々のシステム監視やセキュリティ運用はもちろん、機器の設定代行、ログ分析・リスク分析など、**月額の運用費用を抑えたい**お客様のセキュリティ運用を総合的に支援します。



サービスメニュー一覧

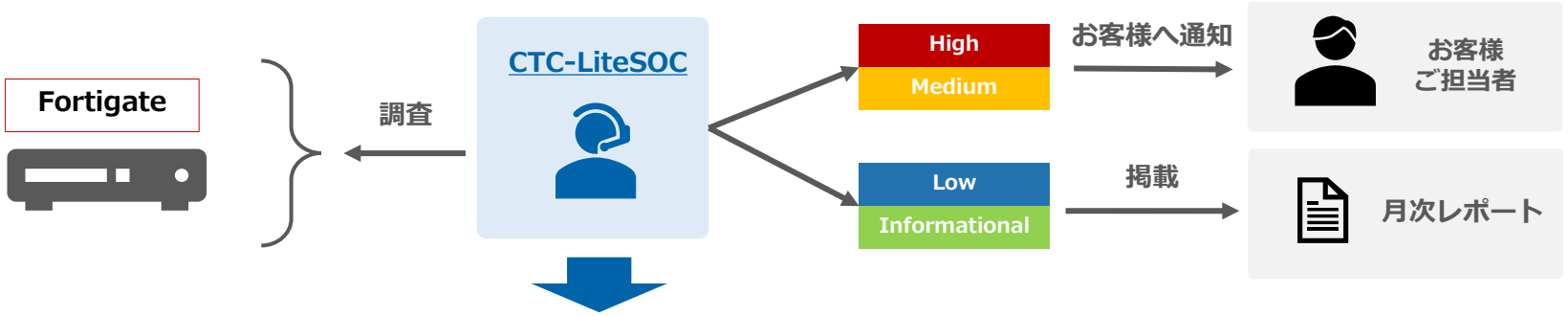
サービスメニュー		概要
セキュリティ監視		お客様環境のFortigateにて検知したセキュリティアラートを監視・分析し、お客様へ影響度や推奨対応について通知を実施します。
システム運用支援	セキュリティ機能の設定変更	Port設定、Webフィルタの解除、config世代管理、IPS設定変更などを対応します。
	稼働状況監視	死活監視、リソース（メモリ監視、CPU監視）監視を実施します。
	障害復旧支援	障害調査、機器故障判断の場合の保守ベンダへの連携を行います。
	ファームウェア管理	重大な脆弱性が見つかったタイミング等、バージョンアップ対応を実施します。
	製品サポート連携	FortiGate の設定、操作、不具合などのお問い合せの受付およびサポート窓口への連携を実施します。
お客様専用ポータルサイトのご提供		セキュリティインシデント情報の閲覧、各種ご依頼やお問い合わせが可能です。ご契約1件につき４つまでアカウントを提供します。（アカウントの増設はオプション契約にて可能です）

提供構成イメージ



セキュリティ監視

お客様環境のFortigateのアラートを監視し、分析・調査を実施します。重要度に応じてお客様に通知します。
通知の際は、影響度や推奨策を併せてお伝えします。



●アラートの内容及び調査結果
発報されたアラートを深堀調査した結果の内容を記載いたします。
※調査の結果、誤検知の可能性が高い場合は、その旨もご報告いたします。

●推奨事項
お客様にて対応頂きたい推奨事項を記載致します。

●その他補足情報
検知されたファイルやログの状態などの補足情報を追記致します。

セキュリティ監視　-　インシデントレベル

セキュリティインシデントを4段階に分類し、インシデントレベルを判定後、規定の通知方法にてご連絡します。

レベル	インシデント定義	通知方法
High	サイバー攻撃が成功している可能性が高く、早期対応が必要と判断したセキュリティアラート	メール通知 詳細はポータルサイト掲載
Medium	サイバー攻撃が成功している、あるいは成功する可能性があり、攻撃対象の状況確認もしくは追加調査が必要と判断したセキュリティアラート	メール通知 詳細はポータルサイト掲載
Low	直接サイバー攻撃の被害は発生していないが、今後の攻撃につながる可能性があるセキュリティアラート	月次レポートにて通知
Informational	直接サイバー攻撃の被害は発生しておらず、今後の攻撃につながる可能性も低いセキュリティアラート	月次レポートにて通知

セキュリティ監視

通知サンプル

【Medium】インシデントを通知致します。
検知されたUTMアラートをもとに調査しましたところ、下記の情報が判明しております。
ご確認のほど、よろしくお願いいたします。

発生日時：
202x/xx/xx　12:00

送信元：
xx.xx.xx.xx

宛先：
xx.xx.xx.xx

インシデントレベル：
Medium

内容：
・UTMアラートでは「xxx(High) 」が検知されています。
・アウトバウンド通信です。宛先は「xx.xx.xx.xx」、Geoは「エジプト」を指し示しております。
・UTM側にてブロックされておりますので、本通信による攻撃自体は成功していません。
・但し、同じ送信元から本ブロックアラートがhh:mm～hh:mmの間にxx件発生しております。
・送信元端末において何らか悪性のファイルが動いている可能性があるため、追加調査が必要としてMediumとして通知させて頂きます。

お客様での対応：
・送信元端末（クライアントホスト名：）において再度ウィルスソフトのスキャンを実施ください。
・送信元端末の該当時間帯において、ユーザにてどのような操作を実施されたかご確認ください。
　（資産管理ソフトやEDR等で動きを確認頂く形でも問題ありません）

システム運用支援

セキュリティ機能の設定変更

Port設定、Webフィルタの解除、IPS設定変更などを対応します。 設定に伴いconfigの世代管理も行います。

稼働状況監視

死活監視、リソース（メモリ監視、CPU監視）監視を実施します。

障害復旧支援

障害調査、機器故障判断の場合の保守ベンダへの連絡及び調整をします。

ファームウェア管理

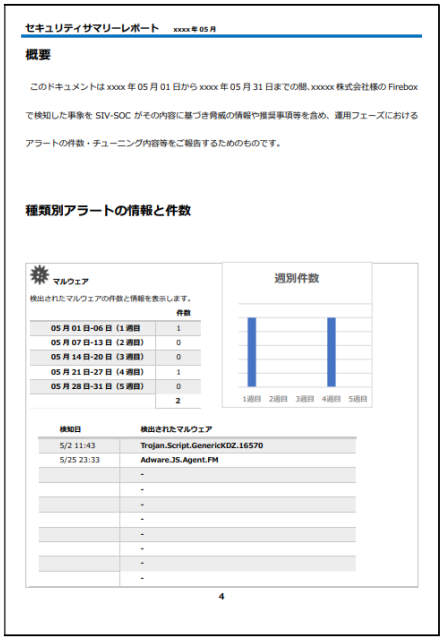
重大な脆弱性が見つかったタイミング等、バージョンアップ対応を実施します。

製品サポート連携

FortiGate の設定、操作、不具合などのお問い合せの受付およびサポート窓口への連携を実施します。

月次レポート

アラートの統計情報や対応作業のサマリレポートを月次でご提供します。


セキュリティサマリーレポート xxxx年05月

概要

このドキュメントは xxxx 年 05 月 01 日から xxxx 年 05 月 31 日までの間、xxxxx 株式会社様の Firebox で検知した事象を SIV-SOC がその内容に基づき脅威の情報や推奨事項等を含め、運用フェーズにおけるアラートの件数・チューニング内容等をご報告するためのものです。

種類別アラートの情報と件数

マルウェア

検出されたマルウェアの件数と情報を表示します。

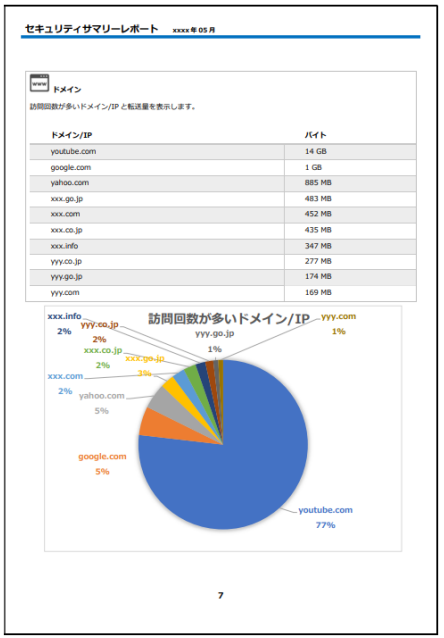
	件数
05 月 01 日-06 日 (1 週目	1
05 月 07 日-13 日 (2 週目)	0
05 月 14 日-20 日 (3 週目)	0
05 月 21 日-27 日 (4 週目)	1
05 月 28 日-31 日 (5 週目)	0
	2

週別件数

1週目 2週目 3週目 4週目 5週目

検知日	検出されたマルウェア
5/2 11:43	Trojan.Script.GenericKDZ.16570
5/25 23:33	Adware.JS.Agent.FM
	-
	-
	-
	-
	-
	-
	-
	-

4


セキュリティサマリーレポート xxxx年05月

ドメイン

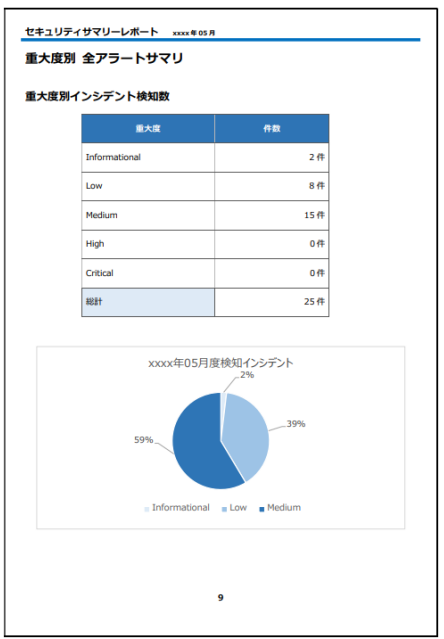
訪問回数が多いドメイン/IP と転送量を表示します。

ドメイン/IP	バイト
youtube.com	14 GB
google.com	1 GB
yahoo.com	885 MB
xxx.go.jp	483 MB
xxx.com	452 MB
xxx.co.jp	435 MB
xxx.info	347 MB
yyy.co.jp	277 MB
yyy.go.jp	174 MB
yyy.com	169 MB

訪問回数が多いドメイン/IP

xxx.info 2%
yyy.co.jp 2%
xxx.co.jp 2%
xxx.go.jp 3%
xxx.com 2%
yahoo.com 5%
google.com 5%
youtube.com 77%
yyy.go.jp 1%
yyy.com 1%

7


セキュリティサマリーレポート xxxx年05月

重大度別 全アラートサマリ

重大度別インシデント検知数

重大度	件数
Informational	2 件
Low	8 件
Medium	15 件
High	0 件
Critical	0 件
総計	25 件

xxxx年05月度検知インシデント

2%
39%
59%
Informational Low Medium

9

サービス提供体制

サービス窓口

本サービスでは、お客様ごとにポータルサイトをご用意しています。
お客様からの各種お問い合わせやご依頼は全てポータルサイトにて受付いたします。

サービス提供時間

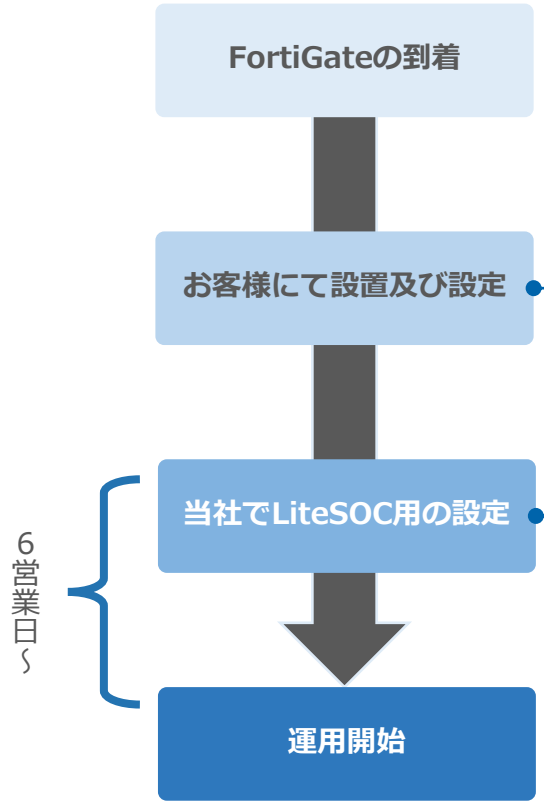
サービス提供時間は以下のとおりです。

ご提供内容	対応時間
本サービスのご提供	弊社営業日　09：00～17：30
ポータルサイトからのお問い合わせ受付	24時間365日

その他ご利用条件等

- FortiCloudを利用できること
- FortiGateに管理者権限でWebUIにアクセスできること
- FortiCloudに登録したいFortigateに固定グローバルIPが降られていること
- 当社ポリシーにてセキュリティ機能を設定できること（IPS機能の有効化など）
- 最低利用期間は1年間となります

サービス導入までの流れ



【お客様にて事前に対応頂きたいこと】
- FortiGateは、インターネットへ繋がる状態まで設定をお願いします。
- FortiGateのWebコンソール画面に入れるように、当社の固定IPからのアクセス許可をご設定ください。
- 当社がWebコンソール画面へアクセスする専用のアカウントを作成ください。
- 当社用のFortiCloudのアカウントを新規登録し、連携ください。
- お客様へのアラート通知先のメールアドレス情報を連携ください

【当社にて対応】
- 各種セキュリティ機能の設定変更（推奨ポリシーへの移行）
  ※IDS/IPSポリシーの設定変更などを想定
- 該当のFortiGateへFortiCloudのアカウントを登録