# TOMS

TechnoBrave Onestop Medical Securityservice

TechnoBrave

## コンサルテーションからサービス提供まで、病院に本当に必要なセキュリティをセットにしてワンストップで提供する月額サービス

**コンサルテーション**

どこまで対応するのか？ お客様のご要望をお伺いし、最適なプランを検討、データバックアップ範囲などを決定致します。

**ご提案**

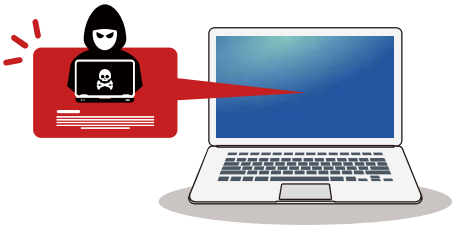
お客様のご要望に合った、最適なサービスを組み合わせて提供致します。

**セキュリティ対策監修** ＋ **ワンストップ（契約統一）** ＋ **サブスクリプション（定額販売）**

| 識別 | 防御 | 検知 | 対応 | 復旧 |
|---|---|---|---|---|
| VSR for TOMS | | SecureLoupe DPI for TOMS | | VDaP for TOMS |
| EPP/EDR+MDR for TOMS | | | SecureLoupe LOG for TOMS | Amazon S3 for TOMS |

## はじめに

急速に病院への攻撃が目立ってきているランサムウェア。規模や種類に関係なく、病院をターゲットにした攻撃が報告されています。最近では、診療停止やシステムの再構築など、経営に深刻なダメージを与えるインシデントが報道されています。このような状況の中、厚労省、内閣府、警察庁、自治体がセキュリティ対策を呼び掛けており、バックアップ、研修の実施、報告の義務化など、具体的な対応内容が提示されるに至りました。現在、下記の内容で法令対応が必要とされています。また、違反した際の罰則も強化されています。



### 個人情報保護法
### （２０２２年4月改正）

不正アクセス等による個人情報の漏えいは件数に関わらず、本人への通知を行うこと、個人情報保護委員会に報告することが義務化されました。

・速報は３～５日以内
・確報は３０日以内

上記日程で対応が必要。

### 診療報酬改定
### （２０２２年度）

４００床以上の保険医療機関は、下記の対応が必要です（移行措置あり）。

・専任のセキュリティ管理者の設置
・年１回のセキュリティ研修の実施
・毎年７月に指定された様式でバックアップ体制の状況を報告

### 厚労省の立入検査に関する通知

２０２２年５月２７日の通知「令和４年度の医療法第２５条第１項の規定に基づく立入検査の実施について」の中で下記項目の実施が明記されました。

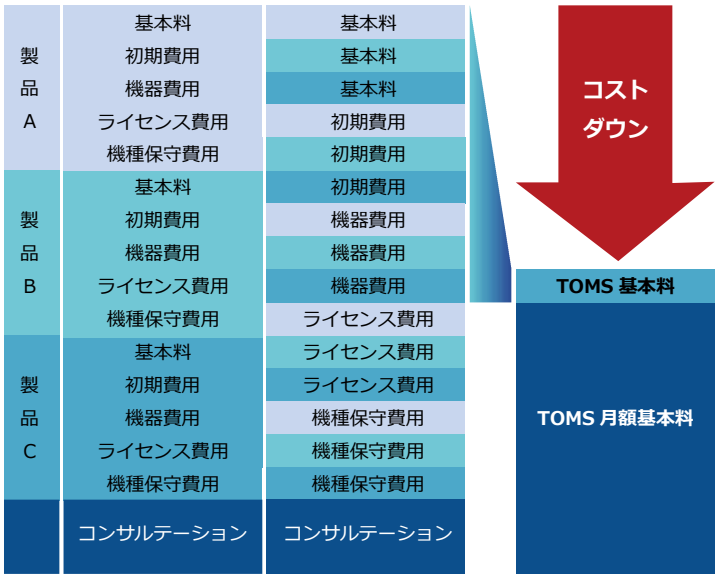
・脆弱性情報の収集と対策体制の確保
・バックアップの実施
・復旧手順の検討と攻撃時の訓練
・保守会社と厚労省への連絡体制確保

## 病院がまずやらなければならないこと

現在、病院のネットワークには様々な機器が接続されています（下記参照）。まずは、何が接続されているのかを正確に把握することが必要です。接続機器を一覧化したら、次は、それらのセキュリティ対策を確認します。どの端末がどのような方法で保護されているのか、また、権限管理はどうなっているのかを確認します。そして、通信ログを利用して、未確認の接続の有無を確認します。また、非常時に備えて、バックアップ対策を行うことも必要です。

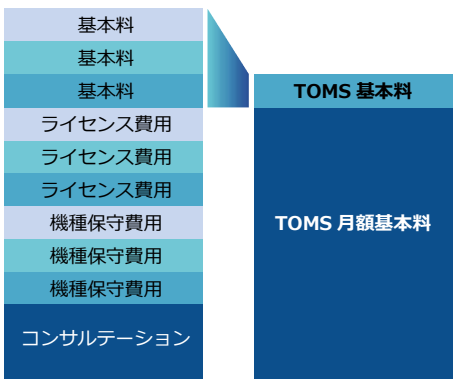
・電子カルテ更新時の端末
・病院調達の部門システム端末
・NW 利用医療機器
・BYOD デバイス
・患者持ち込み端末
・院内情報端末

## 月額固定のメリット




初年度のコスト比較

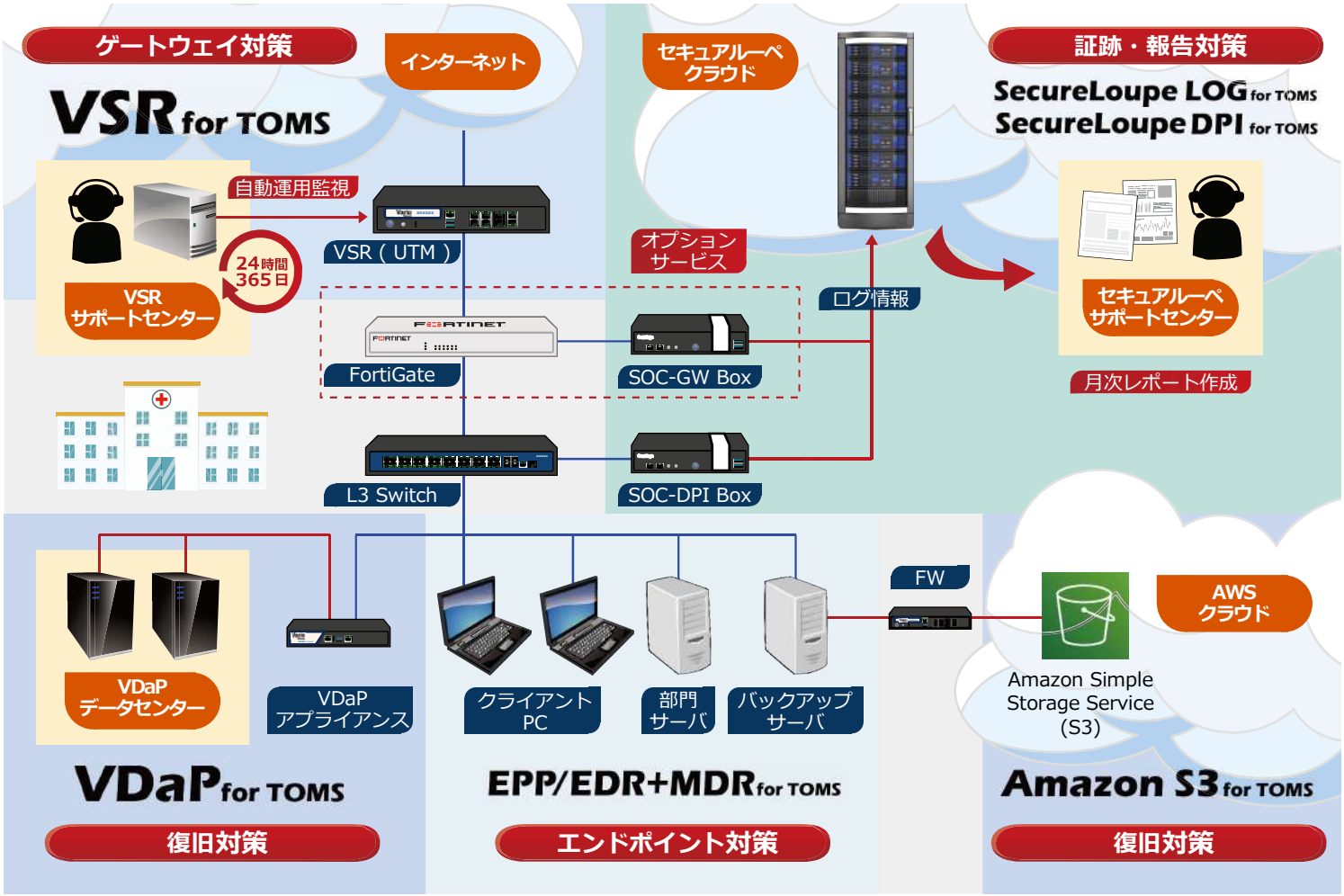
各種のセキュリティサービスを TOMS に一本化することで基本料金を削減することが可能です。また、月額固定に機器代が含まれますので、初期費用は構築費用のみになります。勿論、必要に応じて、機器構成の変更も可能です。




次年度以降

# TOMS セキュリティ全体図

TOMS では医療機関のニーズに応じて各種サービスを個別で提供できるように、４つのカテゴリーでセキュリティ対策をご紹介しています（ゲートウェイ対策 / 証跡・報告対策 / エンドポイント対策 / 復旧対策）。現在の環境が抱えている脆弱性を明確にして、それに対する解決策を必要なサービスのみ提供する形で実現致します。



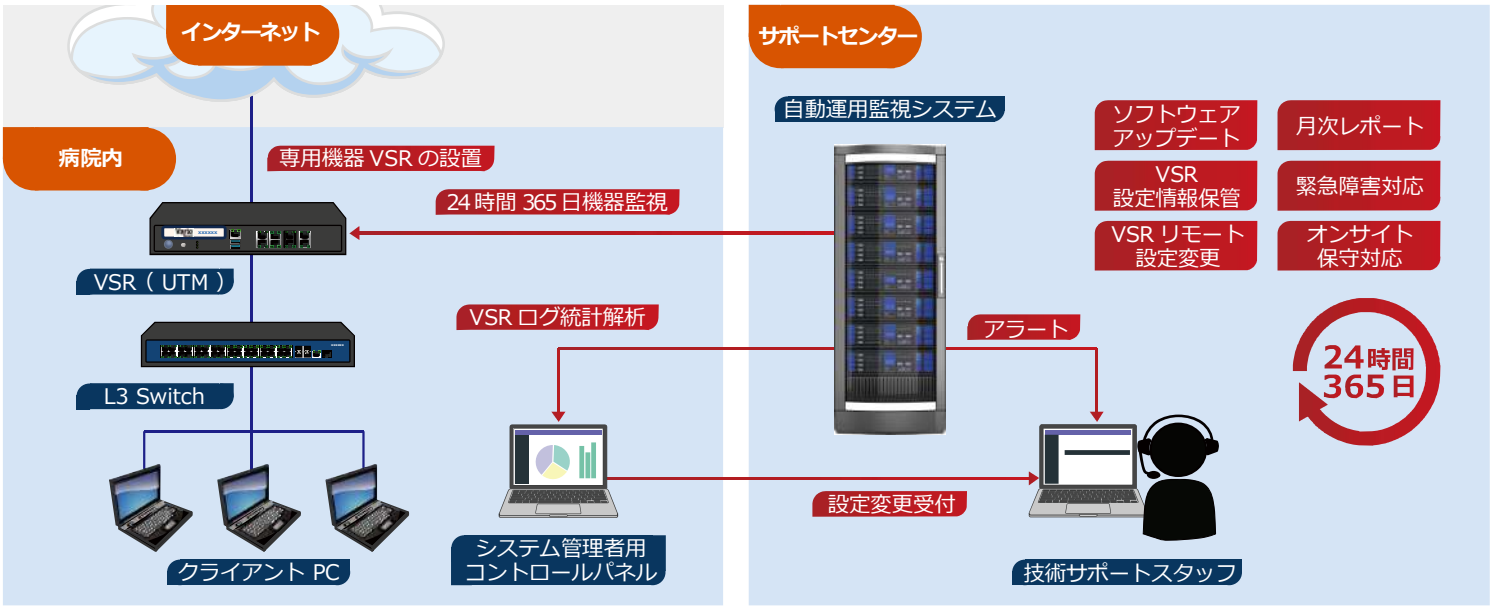

# TOMS サービス一覧

| 種別 | ソリューション | 内容 | NIST CSF 分類※1 | | | | |
|---|---|---|---|---|---|---|---|
| ゲートウェイ対策 | VSR for TOMS | VPN アカウントの管理 | 識別 | | | | |
| | | FortiGate の脆弱性対応 | | 防御 | | | |
| | | レポート作成 | | | | 対応 | |
| 証跡 / 報告対策 | Secure Loupe LOG for TOMS | 接続アカウントの管理 | 識別 | | | | |
| | | 外部通信の可視化 / 通信ログの保全 | | | | 対応 | |
| | | レポート作成 | | | | 対応 | |
| | | FortiGate アラート通知（簡易 SOC）オプション | | 防御 | | | |
| | Secure Loupe Forensic for TOMS | LAN 内通信の可視化 / 通信ログの保全 | | | | 対応 | |
| | | レポート作成 | | | | 対応 | |
| | | 異常通信とサーバ攻撃の検知 | | | 検知 | | |
| | | 脅威インテリジェンス（BCTI※2）+ Forti 連携 | | 防御 | | | |
| エンドポイント対策 | EPP/EDR+MDR for TOMS | PC とサーバの OS 及びアプリの管理 | 識別 | | | | |
| | | エンドポイントでの防御 | | 防御 | | 対応 | |
| | | ウイルスの検知と特定 | | | 検知 | 対応 | |
| | | 脅威の駆除 | | | | | 復旧 |
| データ復旧対策 | VDap for TOMS | 復旧のためのバックアップ | | | | | 復旧 |
| | AWS S3 for TOMS | | | | | | |

※1 NIST CSF は米国国立標準技術研究所が策定したサイバーセキュリティに関する 5 段階のフレームワークです。脆弱性の明確化（識別）/ 保護対策の実施（防御）/ 監視警報システムの構築（検知）/ 報告と分析（対応）/ リカバリープランの実行（復旧）によって構成されます。

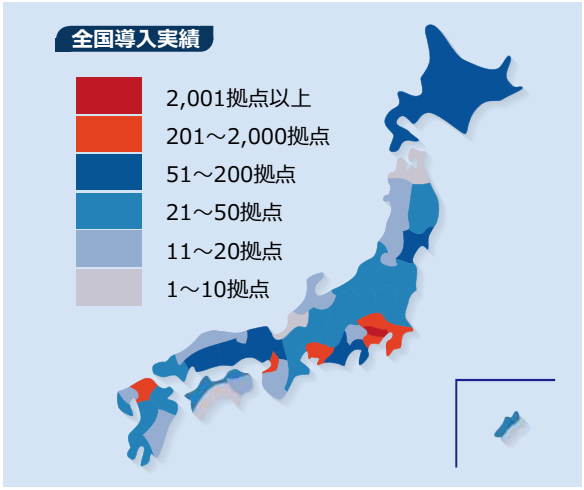
※2 オープンテキスト株式会社（旧ウェブルート）が提供する脅威インテリジェンス DB。８ペタバイト以上の膨大な情報（IP アドレス、URL 等）をリアルタイムに脅威判定する。

ゲートウェイの運用管理を一括アウトソース。機器を設置するだけで全て運用はお任せ下さい。運用監視、技術支援、緊急対応、原因分析を担当致します。



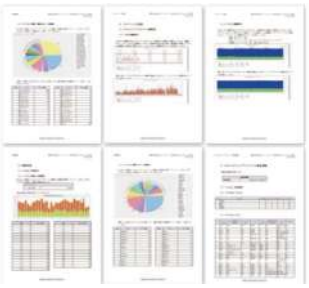

## 導入実績

- 国内中小企業におけるシェア大手メーカー製品
- 国内実績 2 千社以上（ 8 千台以上が稼働中）
- 多様なネットワークへの導入実績




## 製品特徴

- 日本メーカーによる国産 UTM
- 全国をカバーする運用・保守体制
- 24 時間 365 日対応のサポート体制
- 必要な機能を選択できるオーダーメイド UTM
- 月額定額で機器、運用、保守までを対応
- 自動セキュリティアップデート
- 月次の利用状況レポート（PDF）



## 基本サービス

- 初期設定・導入サポート
- ルータ機能
- 24時間365日運用監視
- 24時間365日オンサイト保守
- 24時間365日設定変更
- 専用コントロールパネル
- リソース監視 ※

※一部機能は提供機種により未対応となります。

## 導入メリット

下記の内容で管理負担を軽減

- ファームウェア更新
- 設定情報の保存・管理
- トラフィックとリソースの監視
- アクセスログの確認
- VPN 拠点との通信・機器管理
- 障害発生時の切り分け

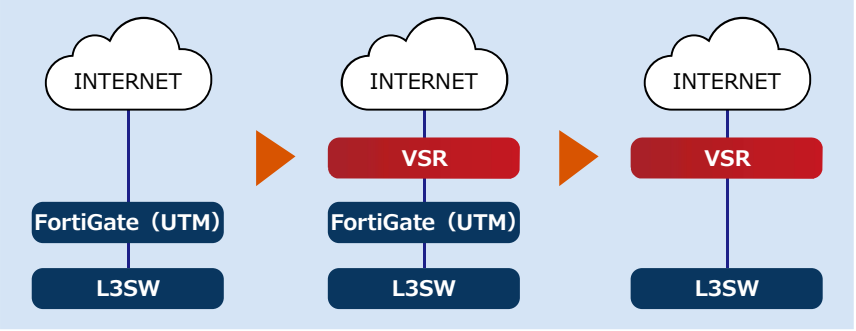
## 自動運用監視システム

国内複数拠点に設置された自動運用監視システムにより、24 時間 365 日体制でお客様のシステム内に設置されている VSR の運用と監視を行っています。万が一、VSR に障害が発生した場合は、リモートでの復旧作業と同時にオンサイトでの保守作業を行っています（月額に含む）。

| 24 時間 365 日対応 | | 営業時間内（9 ～ 18 時） |
|---|---|---|
| ■ 緊急サポートセンター | ■ オンサイト障害復旧対応 | ■ 技術サポート |
| ■ 障害自動検知 | ■ 機器設定変更対応 | ■ 障害対応・原因分析 |
| ■ リモート障害復旧対応 | – | – |

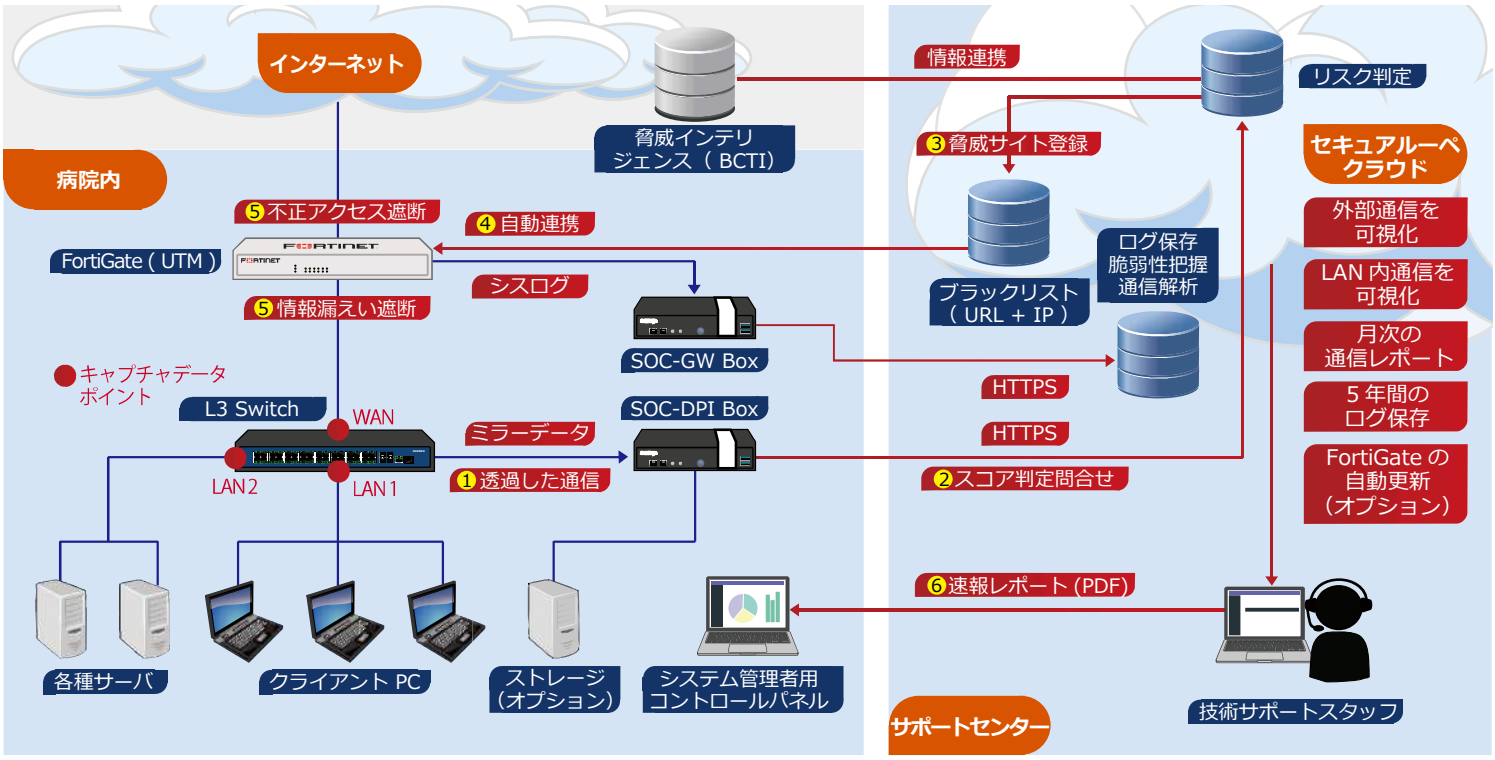
## FortiGate の脆弱性対策について

同社の製品に関しては、世界的なシェアが大きいために標的にされることが多いという脆弱性の問題が存在しております。そのような状況の中、行政側からは、保守内容の確認、通信ログの保全、最新バージョンへの更新、異常時の報告等を病院側の必要な対応として要求されています。TOMS では、お客様のご都合に合わせて、同社製 UTM の外側に VSR を追加することを推奨しております。RVPN を VSR 側に担当させることで脆弱性の解消を図ります。



## SecureLoupe LOG for TOMS + SecureLoupe DPI for TOMS　製品概要　証跡・報告対策

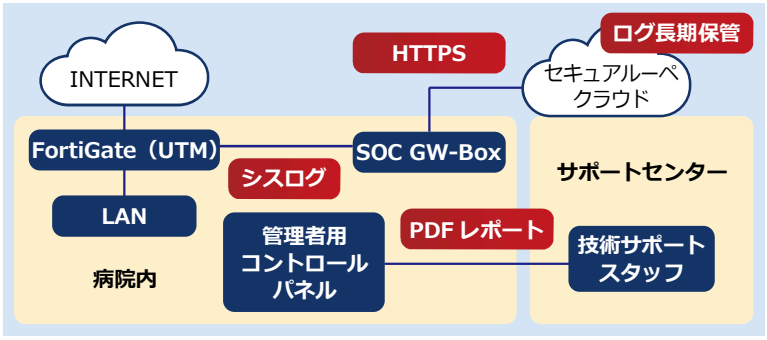
専用機器により外部と LAN 内部の通信ログを取得、分析して、可視化致します。ログの長期保管によりフォレンジックを支援、法令に対応するデータを作成して報告致します。




専用機器を設置して外部通信データを UTM から、LAN 内部通信データを L3SW から取得します（PC 以外の医療系デバイスに対応）。通信状況を月次で PDF にてレポート致します。また、UTM が FortiGate の場合には、バージョンやパッチの自動更新に対応することが可能です（オプション）。

## SecureLoupe LOG for TOMS　製品概要　証跡・報告対策

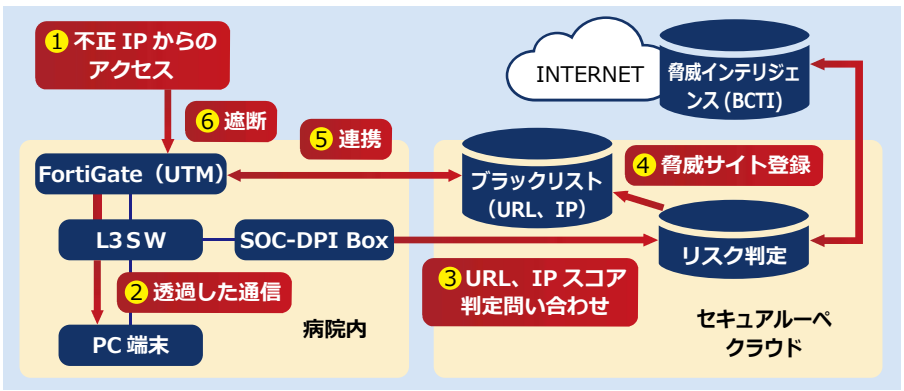
FortiGate 向けログ収集ソリューション。厚生労働省や内閣サイバーセキュリティセンターから通達や注意喚起がされている VPN 装置の脆弱性の調査や、ログの保全にすぐ役立つソリューション。




- FortiGate（UTM）に専用機器を追加して外部との通信を可視化
- ログのクラウド退避（1 時間に 1 回の頻度で帯域は微小）
- FortiGate 機器のバージョンやパッチの適用状況を把握
- 月次の通信レポート（PDF）
- 個人情報漏えい時の報告対策（詳細オプション）
- 医療法による立入検査への対応（VPN の脆弱性情報の収集）

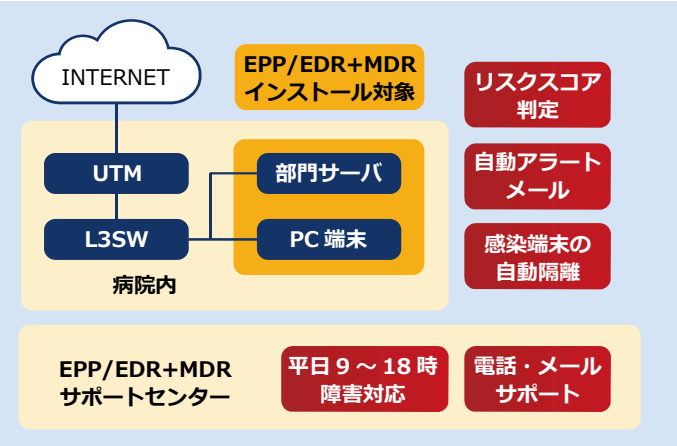
## SecureLoupe DPI for TOMS　製品概要　証跡・報告対策

院内ログ収集ソリューション。院内の PC 端末だけでなく、医療機器やその他の通信にも対応。LAN 内の通信を可視化するソリューション。個人情報保護法において必須となる情報漏えい時の速報に対応。不審な通信のホスト特定による漏えい先の追跡や社内の影響範囲の把握が可能です。




- L3SW に専用機器を追加して LAN 内通信を可視化
- 医療機器等の PC 以外の通信にも対応
- FortiGate の FW 機能と連携して不正アクセスを遮断（独自リストをブラックリストに追加）
- FW を通過した通信に対して、クラウド側でリスク判定を行い、リスクのあるものはブラックリストに自動追加
- ログ解析の PDF レポート作成
- 個人情報漏えい時の報告対策（速報対応）
- 医療法による立入検査への対応（PC の脆弱性情報の収集）

最新攻撃に対応した検知システム。PC 内の不審な挙動を検知して、調査します。プロセスの関連性や振る舞いに対して、AI 解析、及び、リスクスコア判定を実施。セキュリティアナリストがプロセスの正常性や異常通信を確認して報告致します。国内導入実績 15,000 ライセンス以上。




- 最新攻撃に対応した検知システム
- PC 内の不審な挙動を監視、検知、調査
- レピュテーション、サンドボックス、ふるまい検知を標準装備
- 解析結果に応じたリスクスコア判定
- アラートメール（英語）の自動送信
- 調査報告メール（日本語）の送信（重要度が高い場合に、高リスクなプログラムの正常性、及び、通信先を確認して管理者様にメールで報告）
- 感染端末を遠隔操作で自動または手動隔離
- セキュリティパッチ・ソフトウェアパッチの適応管理
- 動作が非常に軽いソフトウェア
- テレワーク端末に対応
- 高い検知率を継続中（業界紙での高い評価）

## EPP と EDR+MDR の役目

**一般化された脅威　軽微な損害**

- ランサムウェアなどのマルウェア
- スパムとフィッシングキャンペーン
- 1 億以上の新たなマルウェアサンプル

**EPP で対応（多くの企業が導入）**

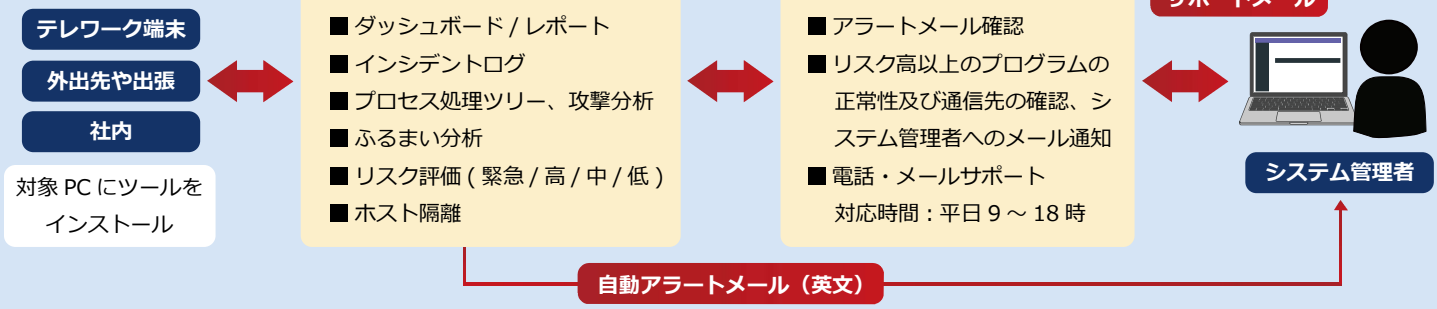
**重大な損害　高度な標的型サイバー攻撃**

- 人によるフィッシングおよびエクスプロイト
- システム内部の使用
- リモート管理ツールとハッキングツール
- 隠されたコマンドおよび制御トラフィック

**EDR+MDR で対応可能（自動隔離に対応）**

## EDR サービス構成

自動アラートメールとサポートメールの 2 階建て構成

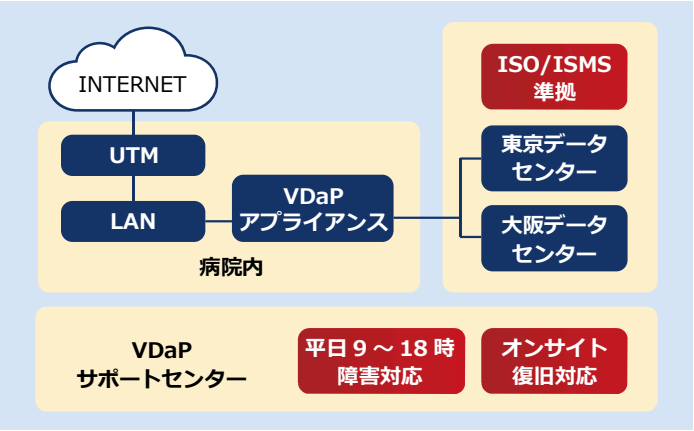



## アラートメールに関して

| | |
|---|---|
| **クラウドからの自動アラートメール（英文）** | リスクレベルに従い、アラートがリアルタイムで通知されます。件名にリスクレベル、本文に検知カテゴリとホスト名を報告します。メールは全て英文になります。 |
| **サポートからの調査報告メール** | リスクレベルが高または最大の場合は EDR サポートが調査して日本語のメールで報告します。調査メールの対応時間は平日の 9 ～ 18 時です。 |
| **PC 端末の隔離** | EDR の判定において必要と判断された場合には、手動または自動で対象の PC 端末を遠隔操作で隔離します。管理情報に必要なプロセスやプロトコルの通信は残して、ネットワークから切り離します。 |
| **管理者はどこからでも状況を把握** | EPP と EDR の状況はブラウザベースの管理ポータルから確認可能です。ご利用に必要なインストールツールは EPP と EDR で共通です。 |

## VDaP for TOMS　製品概要　復旧対策

データバックアップの実行、管理、復旧までを一括アウトソース。病院に設置するバックアップ専用機器はバックアップエージェントや SSH 接続により、最大 20 台の Windows/Linux サーバや、MacOS、NAS などのバックアップに対応可能です。




- 国産バックアップ専用機器（ VDaP アプライアンス ）
- コネクタソフトをサーバや PC にインストールして最小負荷で VDaP にデータを転送
- 転送データの暗号化処理
- VPN によるデータ転送
- ローカル、東京 DC と大阪 DC の 3 拠点でデータを保存
- ３１世代までの世代管理に対応
- 最大２０台、５００GB ～１０TB に対応
- Windows / Linux / Mac OS / NAS / Hyper-V 対応
- ハード故障時の無償交換
- 緊急障害対応

### VDaP の強固なセキュリティ

- VDaP アプライアンス及び専用クラウド間通信は SSL/TLS で守られており、通信先を限定しています。
- VDaP アプライアンスの場合、不要なポートは閉じていますので、エージェントソフト以外からの通信には応答しません。
- データは VDaP 内で暗号化します。従って、取り込んだデータが感染していた場合でも VDaP 内では発症しません。感染前のデータをしっかり保護しています。
- VDaP アプライアンスのログイン権限はコントロールパネルのみです。VDaP アプライアンスには直接ログインできません。

### コントロールパネルに関して

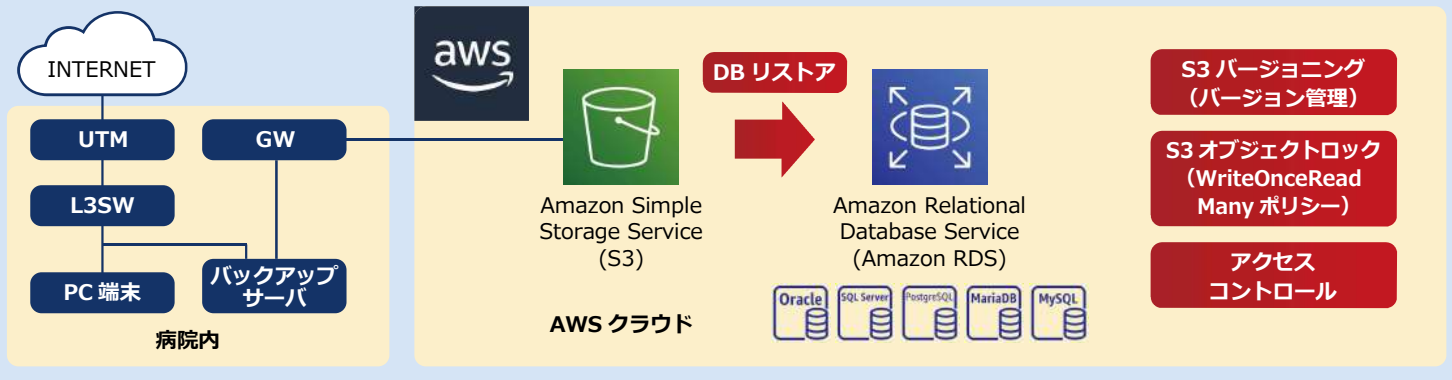
- システム管理者向けにコントロールパネルとして、ブラウザーベースの管理ポータルを用意しております。
- エージェントソフト～ VDaP アプライアンス～クラウド間の通信状態が全て把握できます。
  - ・バックアップポリシーの定義・実行
  - ・バックアップ状態ステータス確認
  - ・バックアップログ表示
  - ・リストア設定・実行
  - ・エージェントソフトのダウンロード
  - ・管理者情報設定
- バックアップサーバの台数が複数でも管理画面は１つで対応できます。

### 製品仕様

- バックアップ方式
  ファイルバックアップ (1 回 /1 日バックアップ実行、初回はフルバックアップ、翌日以降は差分バックアップ )
- バックアップ対象
  Windows 10、Windows Server 2012 以降、Hyper-V( ゲスト OS+ データ )
  CensOS、RHEL や MacOS
  汎用 NAS など (SSH 方式、SMB 方式に対応 )
  クラウドサービスの 2 次バックアップ
- 世代管理
  7/15/31 世代 / 直近 7 日分 + 過去 3 回分の金曜日分
- データ保管先
  VDaP 機器 + 東京 DC+ 大阪 DC の計 3 か所
  ( リストアは 3 か所のどこからでも可能 )

## Amazon S3 for TOMS　製品概要　復旧対策

まずはバックアップを取りたいというお客様には AWS のソリューションをご提案致します。新しい退避先として S3 を利用。安全性を担保する WORM 保存。




追加予定サービス：BCP・訓練用冗長性サービス / SS-MIX BCP ビュワーサービス

＜ お問い合わせ先 ＞
テクノブレイブ株式会社
東京都千代田区内神田１丁目２-８ 楠本第２ビル２ F
TEL: 03-5577-2102
https://www.tbrave.com/product/toms/
( お問い合わせは下記の専用フォームをご利用下さい )
https://tayori.com/f/tomstoiawase/

2023.3 01 版