企業向けサイバーセキュリティソリューション

SASE SOCサービス（FortiSASE）

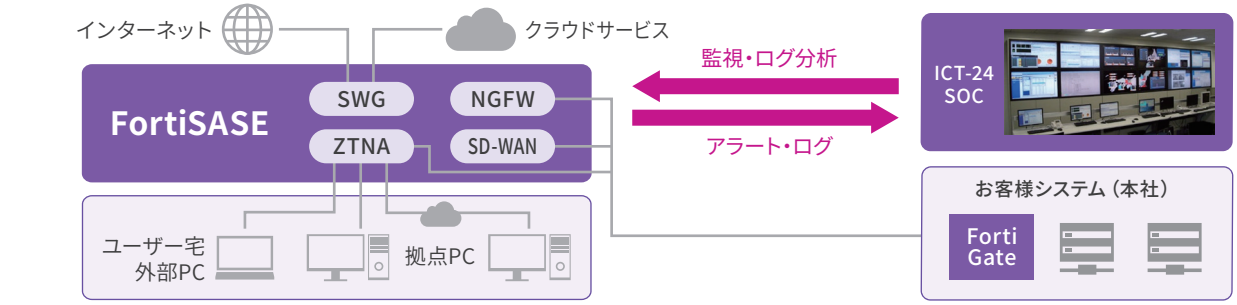
FortiGateを用いた境界型セキュリティ対策を、

SASE※により、リモートアクセスも統合化して管理します。

※SASE: Secure Access Service Edge

境界型セキュリティ対策のFortiGateSOCサービスに加えて、さらにFortSASEで監視することにより、リモートアクセス環境も含めて防御します。

外部からの脆弱性スキャンや攻撃に対応するため、外部と内部の通信を監視する境界型セキュリティ対策として「FortiGate SOCサービス」が有効でしたが、ここ最近では、このような従来型の防御をすり抜ける新たな攻撃が増えており、リモート環境の普及により社内ネットワークへの侵入経路も多様化しています。また、複数のセキュリティ対策を個別に運用することで管理が煩雑になり、負担も増しています。そこで、新たに複数のセキュリティ機能を統合することにより、より効率的に運用できる「SASE（Secure Access Service Edge）」ソリューションをご用意しました。



【拠点への接続】SD-WAN・ZTNA・NGFW
【クラウドへの接続】FortiSASEによるNGFW・SWG・CASB（安全なクラウドはLBOで接続）

【拠点からの接続】FortiGateによるSD-WAN・ZTNA・NGFW（安全なクラウドはLBOで接続）

POINT 1

FortiGateの境界型防御に加え、SASEによりリモートアクセスも防御

POINT 2

お客様のニーズに合わせて監視項目を取捨選択可能

POINT 3

他EDR製品と組み合わせた分析も可能（オプション）

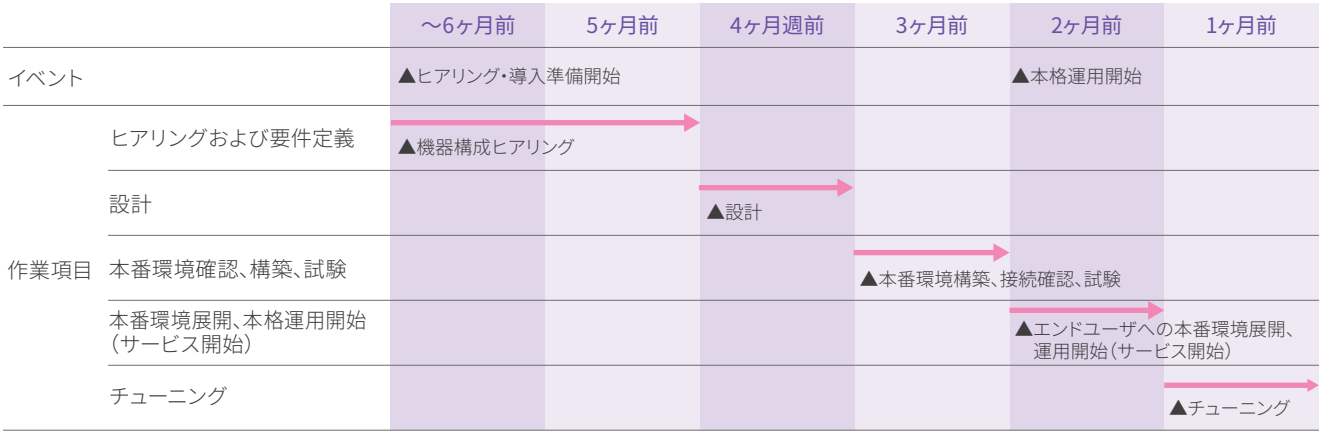
セキュリティ Security

https://www.ntt-at.co.jp/product/sase-soc/fortisase

サービスメニュー

サービスメニュー		サービス内容
FortiGate機器メンテナンス	コンテンツアップデート	FortiGate機器の最新シグネチャへの定期的な更新確認
	正常稼働監視	FortiGate機器の正常稼働を監視、切り分け、原因調査
	イベント管理	FortiGate機器のセキュリティログを過去3ヶ月分保持 ※対象はWarning以上のセキュリティログとし、トラフィックログは含まず
	設定バックアップ	FortiGateのポリシー設定時に、過去一世代分のConfigをバックアップ
	FortiGateポリシー設定変更	ユーザーからの依頼をうけて、FortiGateのセキュリティ設定（ポリシー）の設定変更
SASE設定	SASEポリシー設定変更	ユーザーからのリクエストを受けて実施（弊社業務時間帯・チケット制）
	レポート作成支援	未知の攻撃・不審な通信を分析し、インシデントの可能性がある場合はメールで通知
イベントハンドリング	アラーム分析・通知	発生したアラートについてICT-24 SOCにて分析し、危険度が高いイベントは即時にお客さまへ通知 ※ICT-24 SOCの対応は、FortiSASEからのアラートを受信してからの対応
	設定変更	アラート分析後、必要であれば異常な通信の遮断設定など、FortiSASEやFortiGateに対して必要なセキュリティ設定（ポリシー）の設定変更
	問い合わせ対応	ユーザーからのセキュリティに関する問い合わせ対応　※FortiSASE、FortiGateの仕様、操作方法、不具合対応など FortiSASE、Gateの機能に関する問い合わせは含まず。（ご契約頂いた運用メニューの範囲内での回答）
アナリティクス	インシデント初動対応	リモートでFortiSASE,FortiGateのログ分析で対応できる範囲で、インシデントの初動対応を支援（1年間に2回まで）
オプションサービス	・EDRオプション ・サイバーセキュリティインシデント対応支援サービス ・デジタルフォレンジックサービス	・EDRオプションでは、端末のマルウェア感染時に、EDRを使用して、端末で起きた事象をリモートで監視・分析 ・サイバーセキュリティインシデント対応支援サービスは、事故発生直後の初動対応から事態収束、さらに改善・再発防止まで、あらゆる段階でご支援 ・デジタルフォレンジックサービスでは、端末でのファイル削除の痕跡など、端末のHDDやSSDなどを物理的に詳細解析

サービス開始までの流れ



用語説明

- **SD-WAN（Software Defined Wide Area Network）：**
  拠点間やクラウドとのネットワークをソフトウェアで制御するNetwork
- **ZTNA（Zero Trust Network Access）：**
  「すべての通信を信頼しない」ことを前提にアプリケーションやデータ資産へのアクセス許可を制御する方式
- **SWG（Secure Web Gateway）：**
  ユーザーが社外ネットワークへのアクセスを安全に行うための、主にクラウド型として提供されるプロキシ（代理中継サーバー）
- **CASB（Cloud Access Security Broker）：**
  ユーザーとクラウドサービスの間に入り、クラウドサービスの利用状況を可視化して監視し、各種制御を行う
- **NGFW（Next Generation FireWall）：**
  従来のFireWallの機能に加え、アプリケーションの通信データ内容を解析し、不正アクセスの侵入を探知して防止
- **LBO（Local Break Out）：**
  特定の安全なサイトへの通信を、セキュリティ機能をつけず通信することで、クラウドサービスなどへの快適なアクセスを確保

お問い合わせ　**https://www.ntt-at.co.jp/product/sase-soc/fortisase**

NTTアドバンステクノロジ株式会社