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（Prisma Access）

各社の機器のIPsecVPNも活用できるPrisma AccessのSASE※により、
外部へのNWアクセスも、リモートアクセスも統合化して管理します。

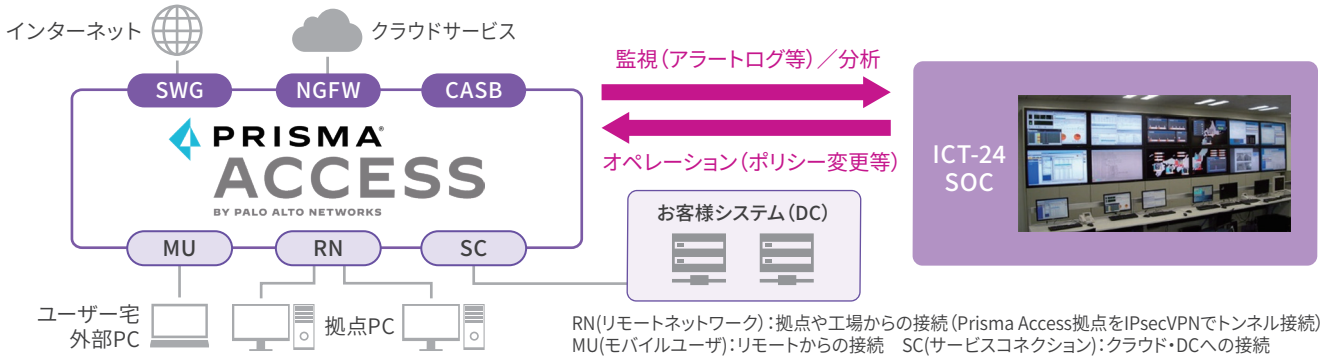
※SASE: Secure Access Service Edge

PRISMA® ACCESS BY PALO ALTO NETWORKS

境界型セキュリティに加えて リモート環境のセキュリティも対策 ＋ **運用業務の省力化や システムの複雑化を解消**

Prisma Accessによる統合的なセキュリティ対策を監視することにより、境界型セキュリティもリモートアクセス環境も含めて防御します。

外部サイトからの脆弱性スキャンや攻撃に対応するため、当社では外部と内部の境界通信に着目した境界型セキュリティ対策として、FortiGate SOCおよびPalo Alto SOCサービスを提供して来ましたが、近年、境界型セキュリティによる防御をすり抜ける攻撃が増加しており、加えて社内のリモートアクセス環境を経由した攻撃リスクも顕在化しています。その一方で、複数のセキュリティ対策を個別に導入・運用することは、運用業務の複雑化や管理負担の増大といった課題を招きます。その課題解決のため、複数のセキュリティ機能を統合的に管理し、システムの複雑化を抑えつつ運用効率を高めるPrisma Accessを活用したSASE（Secure Access Service Edge）ソリューションをご提案します。



RN(リモートネットワーク)：拠点や工場からの接続（Prisma Access拠点をIPsecVPNでトンネル接続）
MU(モバイルユーザ)：リモートからの接続　SC(サービスコネクション)：クラウド・DCへの接続

POINT 1
各社のIPsecVPNの機器を活用したSASE環境を監視

POINT 2
重要度の高いアラートのみを通知して運用負荷を削減

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/prismaaccess

サービスメニュー

サービスメニュー		サービス内容
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SASEのセキュリティポリシー設定を実施
	レポート作成支援	アラートサマリ、トラフィックサマリなどの状況を記載したレポート作成機能があり、その設定を支援
イベントハンドリング	アラーム分析・通知	危険度の高い攻撃検知についてお客様へメール通知
	設定変更	アラート分析からのフィードバックによる設定変更
	問い合わせ対応	お客様からの申告等に基づき、オペレータが対応。Prisma AcessSASE PaloAltoの仕様、操作方法、不具合対応などPrisma AcessSASE PaloAltoの機能に関する問い合わせは含んでいません。(ご契約頂いた運用メニューの範囲での回答となります。)
アナリティクス	インシデント初動対応	Prisma AcessSASE PaloAltoのログ分析で対応できる範囲でインシデント初動対応をリモートで支援

・現在、DLP、CASBの機能には非対応。
・Strata Cloud Manager Essentialsには非対応。Strata Cloud Manager Proまたは、Strata Cloud Manager Essentials + Strata Logging Serviceが必要です。

サービス開始までの流れ

		～6ヶ月前	5ヶ月前	4ヶ月週前	3ヶ月前	2ヶ月前	1ヶ月前
イベント		▲ヒアリング・導入準備開始				▲本格運用開始	
作業項目	ヒアリングおよび要件定義	▲機器構成ヒアリング					
	設計			▲設計			
	本番環境確認、構築、試験				▲本番環境構築、接続確認、試験		
	本番環境展開、本格運用開始(サービス開始)					▲エンドユーザへの本番環境展開、運用開始(サービス開始)	
	チューニング						▲チューニング

用語説明

・**SASE(Secure Access Service Edge):**
「ネットワーク機能」と「セキュリティ機能」を一つのクラウドサービスとして統合し、提供するモデル。場所やデバイスを問わず、どこからでも安全かつ快適に内部NW内のサービスやクラウドサービスにアクセスできる環境を実現する。
・**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/prismaaccess.html

NTTアドバンステクノロジ株式会社