

製品構成



- リモートアクセスの受け側、拠点間アクセスなど
- 拠点内のデバイスが多い
- 複合機など、SDP Client のインストールが不可能で、守りたいデバイスが多数ある
- モバイルワーク / テレワークを実施する端末
Windows/macOS/Android/iOS/Linuxに対応
- 規模の小さい拠点やサテライトオフィスの端末
- インターネットアクセス、クラウドアクセスのみの場合

機能一覧

機能	概要
FWaaS (Firewall as a Service)	ファイアウォール機能をクラウドで提供する機能です。拠点を問わず全ての通信を共通のセキュリティポリシーで制御することで、安全性を強化することができます。
拠点間アクセス	拠点間のアクセスが必要な環境でも、各拠点間の通信もインターネット通信と同様のCato FWaaSポリシーでシンプルに管理することができます。
SWG (Secure Web Gateway)	悪意のあるサイトや不適切なコンテンツへのアクセス制御を提供する機能です。Catoでは、80以上のデフォルトカテゴリや任意に作成可能なカスタムカテゴリを用いて、お客様の要件に沿った柔軟なアクセス制御が可能です。
DNSプロテクション	DNSトラフィックを検査し、悪意のあるドメインや危険性の高いドメインなどへの接続を防ぐことができる機能です。
TLSインスペクション	TLS (SSL) によって暗号化された通信 (HTTPSなど) を安全に復号化し、アンチマルウェアやIPSなどの脅威保護サービスが完全な性能を発揮できるようにします。
アンチマルウェア (AM/NGAM)	ランサムウェアやマルウェアなどの悪意のあるファイルがネットワークに侵入するのを防ぐためのセキュリティポリシーです。既知のファイルシグネチャとヒューリスティック分析に基づいたアンチマルウェアレイヤーと、機械学習予測モデルにより未知のファイルを分類する次世代アンチマルウェアレイヤーによって構成されます。
IPS	既知および未知の 익스プロイト を利用した高度な脅威や攻撃に対するリアルタイムの保護を提供します。IPS保護は、インターネット、WAN、クラウドを含むすべてのトラフィックに適用され、機械学習モデルを統合したリアルタイム検査エンジンによって、ランサムウェアの配信と伝播、データの盗難を防ぎます。
CASB	認可、未認可 (シャドールー) 問わず、クラウドアプリケーションの利用状況を可視化し、アプリケーションやユーザ、デバイスのリスク状態などに基づいたアクセス制御を提供します。
DLP	社内のデバイスから、オンプレミスやクラウドへと送られる機密データについて、アクセスポリシーによる制御や可視化ができる機能です。
QoS	帯域が圧迫された状態でも、業務に必要な通信を優先するように制御できる機能です。デフォルトで、Web会議などのリアルタイム性の高い通信が優先されるようにプリセットされています。また、特定の通信が帯域を圧迫してしまわないように帯域上限を設けるなどの制御も可能です。
CMA (Cato Management Application)	単一の統合された管理コンソールです。設定、分析、ネットワークやセキュリティのダッシュボード、アカウントの管理など多岐の機能を提供します。

CATO
NETWORKS

— 次世代セキュリティプラットフォーム —
Cato SASE Cloud

datacontrol
株式会社データコントロール
(英文: Datacontrol Co., Ltd.)



本社 〒543-0028 大阪府大阪市天王寺区小橋町11-19
TEL 06-6763-2662 FAX 06-6763-2696

東京事業所 〒141-0031 東京都品川区西五反田1-1-8 NMF五反田駅前ビル5F
TEL 03-5434-2331 (代) FAX 03-5434-2332
メール cato-sales@datacontrol.co.jp

One Security One Policy One Network

究極のゼロトラスト・セキュリティ「Cato SASEクラウド」で 実現する全方位のセキュリティ対策

グローバル SASE サービス

最寄りのSASE PoPに接続するだけで、場所を問わず均一のパフォーマンス、セキュリティ、キャパシティ、可用性を得ることができます。

クラウドネイティブ

セルフメンテナンス、ロケーションフリー、新機能の追加、スケールアウトなどオンプレミス環境で抱えていた日々の運用負荷やリスクを低減します。

Security as a Service

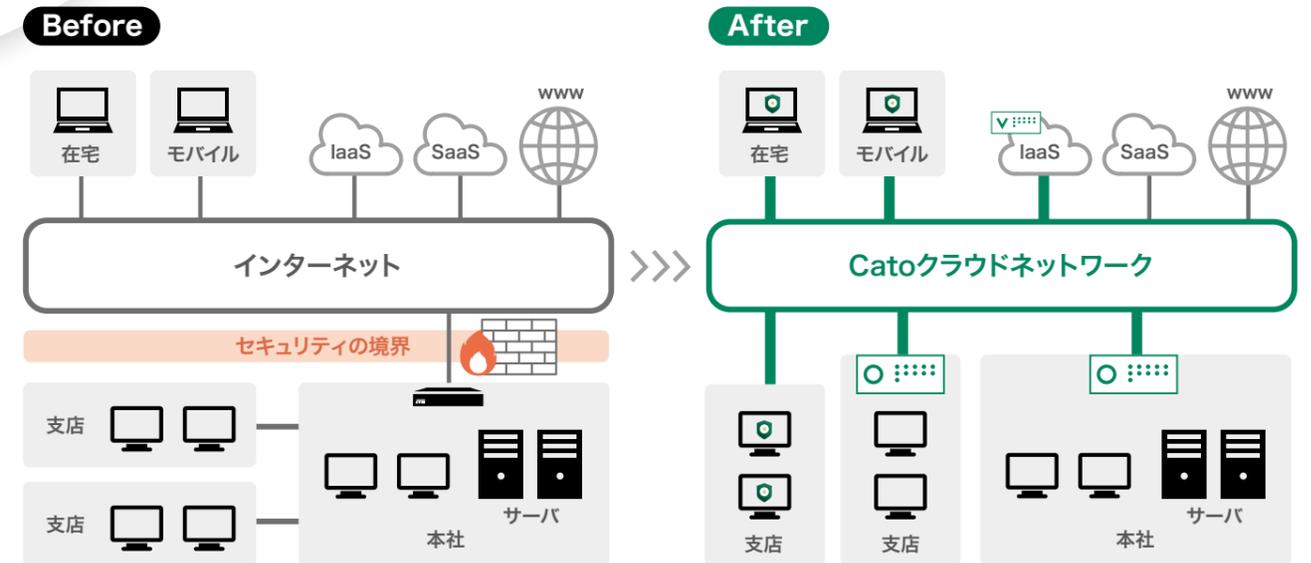
FWaaS、脅威防御(SWG、IPS、NGAMほか)をはじめ、アプリケーションとデータの保護(CASB、DLP、ZTNA)までをカバー、脅威毎の対策が不要になります。



Cato SASEクラウドの利点

すべてをつなげる、あらゆる場所を守る

Catoは、セキュリティ機能にネットワーク機能を統合させた全く新しいコンセプトのクラウドサービスです。インターネットアクセス回線さえあれば、どこからでもCatoクラウドネットワークへつながり通信が保護されます。



- 物理的な拠点を中心としたレガシーネットワーク
- アクセス集中によるスピード低下
- リモートワークの安全性、信頼性の確保
- セキュリティ管理の断片化と複雑化

- アクセス回線さえあれば、どこからでも接続可能
- 安全に分散アクセスが可能
- あらゆる場所から閉域アクセスが可能
- 簡単にポリシーを統一

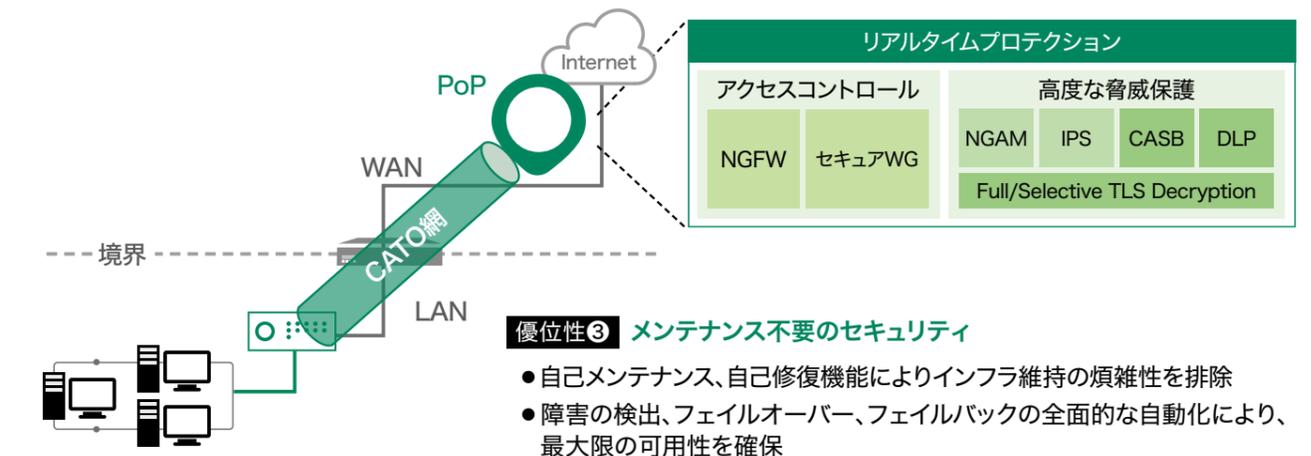
Cato SASEクラウドの優位性

優位性① 高セキュアなネットワーク

- 全ての通信は完全に閉じられたグローバルプライベートバックボーン内で完結
- 専用のVPNインフラを導入する必要なし
- リモート環境など境界の外にある対象も保護

優位性② 即座にセキュリティ機能を導入

- 複雑な統合、キャパシティ計画、複数の管理コンソールが不要
- 将来追加されるセキュリティ機能を利用できる
- 全てのセキュリティポリシーおよび分析を単一画面で管理可能
- ポイントソリューションのコスト、複雑さを排除



優位性③ メンテナンス不要のセキュリティ

- 自己メンテナンス、自己修復機能によりインフラ維持の煩雑性を排除
- 障害の検出、フェイルオーバー、フェイルバックの全面的な自動化により、最大限の可用性を確保

Catoのクラウドネットワーク

世界最大 グローバルプライベートバックボーン



グローバルトラフィックの最適化

