UPAS

ZERO TRUST ARCHITECTURE

全方位ゼロトラスト情報セキュリティソリューション

ZERO TRUST · TRUST UPAS

－ 製 品 カ タ ロ グ －

- APAC CIO Outlook -

TOP 5 / TOP 10
Cyber Security Solutions Provider
in Taiwan / APAC


ZERO TRUST
TRUST UPAS















UPAS

イントラネットセキュリティシステムリーダーブランド

1993年に設立されたUPASは、IP管理およびNACネットワークアクセス制御システム製品の研究開発から始まり、イントラネットセキュリティ制御システムのパイオニアおよびリーダーであり、長年にわたって情報セキュリティとネットワーク管理の分野に深く関与し、顧客に協力して全方位イントラネットセキュリティ管理システムを確立するのを支援し、企業イントラネットのセキュリティと管理の効率を向上させ、管理コストを削減し、情報セキュリティの回復力を強化している。

あなたのための専門的で誠実なサービス

UPAS は、イントラネットセキュリティのための最良のソリューションをお客様に提供することをお約束し、当社の使命は、お客様がイントラネット上のすべてのエンドポイントデバイスが安全でコンプライアンスに準拠し、ランサムウェアの侵入や機密データの漏洩を防ぐために、強固な境界保護を確立できるよう支援することです。
政府、重要インフラ、技術、製造、金融、医療機関、教育研究機関、一般企業などで豊富な経験を有しています。 これからもお客様の声に耳を傾け、お客様のニーズに合わせて製品の最適化を進め、お客様とともに情報セキュリティの道を歩んでまいります。

テクノロジーが世界をリード

台湾、中国、日本、東南アジアに拠点を持ち、大規模な多国籍企業、海外ブランド、国際ブランドのいずれであっても、UPASの専門知識は、お客様のニーズに合わせた完璧なソリューション、ゼロトラストセキュリティアーキテクチャ、強固なイントラネットセキュリティ保護を提供する。

あなたのネットワーク環境は以下の脅威にさらされているかもしれません



- 環境とデバイスの完全にチェックされておらず、ハッカーにつけ入るスキを与えている
- ルール違反のデバイスによる違法なアクセスにより、潜在的なリスクが形成されている
- IoT デバイス数の劇的な増加により、エージェントによる管理ができない



- Windowsパッチが更新されていないため、デバイスにバグが発生している
- パターンファイルが更新されていないため、新型のウィルスの好き勝手な侵入を許している
- 端末デバイスのソフトウェアにバグがあり、管理人がただちに修復できない
- GPOのルールに適合していない



- 重要なファイルの流出
- 従業員が私的なデバイスで勝手にネットワークに接続しデータを保存している
- 従業員が私的なUSBで重要情報を保存している



- 従業員はプライベートでHubやIP　ルーターに接続し、社内ネットワークに影響を与えた
- 外部ゲストが ID 認証未通過で直接ネットワークに接続している
- 端末デバイスのドメインからの私的な退出



- モバイルデバイスでの秘密情報の撮影、スクリーンショットの外部流出
- モバイルデバイスに勝手に違法なアプリケーションをインストールしている

様々なリスク防御とデバイス管理に、多くのソフトウェアは不要です。

UPAS ZTA が最も堅実なネットワークセキュリティのソリューションをお届けします。

UPAS 5S の主な利点

ZERO TRUST ARCHITECTURE

Simple

- NAPの特許取得済み技術を使用して、シンプルな展開アーキテクチャを備え、設置と構築が簡単
- 柔軟な導入機能を備えており、クラウド構築とオンプレミス構築の両方に適している
- モジュラーアーキテクチャ、自由で柔軟なアプリケーション、高いCP 値
- さまざまなブランドのSwitch、ウイルス対策ソフトウェア、およびネットワークアーキテクチャとの高い互換性
- 絶妙な UIデザイン 、フレンドリーな UX デザイン、ワンページ管理を使用したシステムのインストールと設定、ページ変換の削減、より使いやすく

Support

- ZTAシステム、単一プラットフォーム、単一Agent、一式はNAC、ITAM、IAM、IPAM、MDMなどを完成する
- AgentはWindows／Linux／macOS／Android／iOSなどの作業システム管理をサポートする
- Patchアップデート、ウイルス対策ソフトウェアのインストール、アプリケーションのインストール、ソフトウェアの無効化、USB管理、ソフトウェア脆弱性アップデート、GPOパッチ適用などは完全に自動化されている
- 統合された機能、syslog、APIなどのサポートを提供する
- NOCのホームページには明確なデータチャート分析があり、機器情報は高度に可視化されている
- 多様で豊富なレポート機能を提供し、さまざまなレポートを自動生成する

Smart

- 完了率、保守率、属性識別、Agent展開率、端末機器コンプライアンス検査率等はすべて98%以上に達し、システムのセキュリティを確保する
- ホワイトリストの自動参加、グループセグメンテーションの自動設定、Agentの自動配信、グループポリシーに従った自動コンプライアンスチェック、自動隔離とパッチ適用、自動接続回復など、インテリジェントで自動化された設計により、人員と時間を節約できる。

Safe

- 故障ByPass、エラー防止設計などの高度なセキュリティメカニズムを備えている

Stable

- 高い安定性、優れた性能、満足度が高く信頼度も高い

5つの情報セキュリティソリューション 20の機能を備えたモジュール

ネットワークに接続するすべてのデバイスの安全性とルール適合性を確保

ネットワークアクセス制御 NAC
Network Access Control

メインモジュール

ARP IP / MAC 管理モジュール
ARP Scanner アクセス制御

DAM デバイス認証モジュール
Device Authentication Management



IT 資産管理 ITAM
IT Asset Management



PM パッチ管理モジュール
Patch Management

DM デバイス管理モジュール
Device Management

ROM リモートメンテナンスおよびモジュール
Remote Operations Management

TIM 信頼判断モジュール
Trust Inference Management

GPO GPO 管理モジュール
GPO Management

VANS 脆弱性の警告と通知システム
Vulnerability Alert and Notification System



ID 認証管理 IAM
Identity and Access Management

AD AD アドバンスモジュール
ADVantage

ZERO TRUST ARCHITECTURE

ITスタッフ、MISスタッフのためにカスタマイズされたプロフェッショナルな管理用ツール

IPアドレス管理 IPAM
IP Address Management

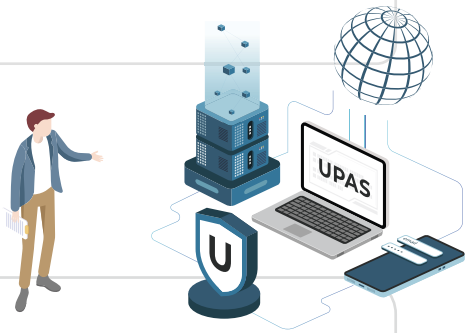
メインモジュール

ARP IP / MAC 管理モジュール
ARP Scanner　IP管理

モバイルデバイス管理 MDM
Mobile Device Management

MDM モバイルデバイス管理モジュール
Mobile Device Management

その他付加価値のあるマネジメントソリューション
Other Value-Added Functions



SIM セキュリティ統合管理モジュール
Security Integration Management

IPL IPアドレス解析モジュール
IP Locator

IPv6 IPv6 管理モジュール
IPv6 Management

IPAF IP 申請フォーム機能
IP Application Form Functionality

DHCP DHCP Server 整合機能
DHCP Server Integration Functionality

IPLI IP 使用記録整合機能
IP Usage Log Integration Functionality

IDC 認証モジュール
ID Checker

GAM 訪問者管理モジュール
Guest Access Management

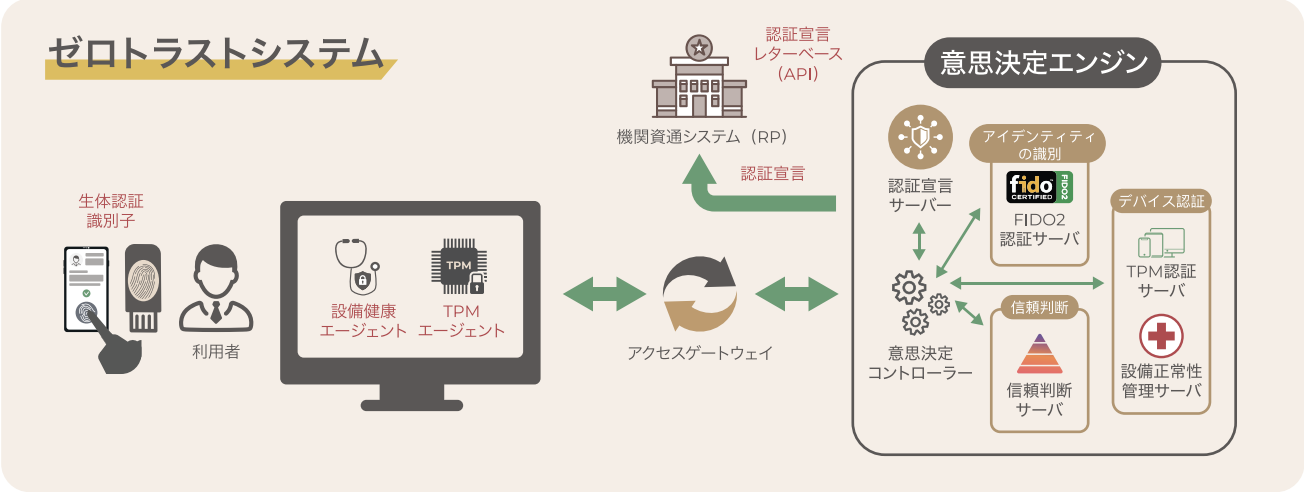
SCP システム中枢プラットフォーム
SCP Console

APP アクション管理 APP
UPAS Management App

UPAS ZTA 全方位実践 ゼロトラストアーキテクチャ

2020年、米国国家標準技術研究所(NIST)は、標準文書「NIST SP 800-207」を発行した、「NIST SP 800-207」の中、ゼロトラストの原則では、「組織は、資産、ネットワークインフラストラクチャ、および通信のステータスについてできるだけ多くの情報を収集し、その情報を使用してセキュリティ体制を改善する必要がある」と概説されていた。 UPASは、最初にイントラネット接続デバイスの資産と正常性をチェックし、次にデバイスの識別を実行して、偽造デバイスがイントラネットに侵入する可能性を防ぐのに役立っている。

▼ ゼロトラストフレーム



第1段階 アイデンティティの識別

FIDOでパスワードなしの二重因子認証を行う。

第2段階 デバイス認証

設備の信頼プラットフォームモジュール（TPM）に基づいて設備を検証し、設備の正常性管理を実行する。

第3段階 信頼判断

ユーザーコンテキストとデバイスの正常性状態に応じて、リソースアクセスの結果が動的に決定される。

UPAS ZTA モジュールの紹介

ゼロトラストアーキテクチャで構築されたUPASの5つの主要なソリューションは、1つのメインモジュールと異なる機能を持つ20のモジュールで構成されており、メインモジュールに一致する機能モジュールを自由に選択して、最適なソリューションを構築できる。

UPASの自社開発技術は、国内外の複数の特許を取得しており、違法な機器がイントラネットに接続するのをブロックし、イントラネットのセキュリティを常に監視するのに効果的である。さまざまなアラームメカニズム、ユーザーフレンドリーな操作インターフェイス、およびさまざまな豊富なレポートを備えており、エンドポイントセキュリティ保護とイントラネットセキュリティ制御を効果的に実現するのに役立っている。



単一プラットフォーム・単一エージェント

ファンクションモジュールの自由な組合せ

ARP IP / MAC 管理モジュール

ARP Scanner アクセス制御

特許取得済みのARPパケット解析技術により、Agentをインストールすることなく、データ収集、デバイス識別、および高強度のアクセス制御を実行できる。100%の資産インベントリを実行して、IP/MAC管理、デバイスアクセス管理(ネットワークアクセス制御)、およびネットワークブロッキングを実現できる。

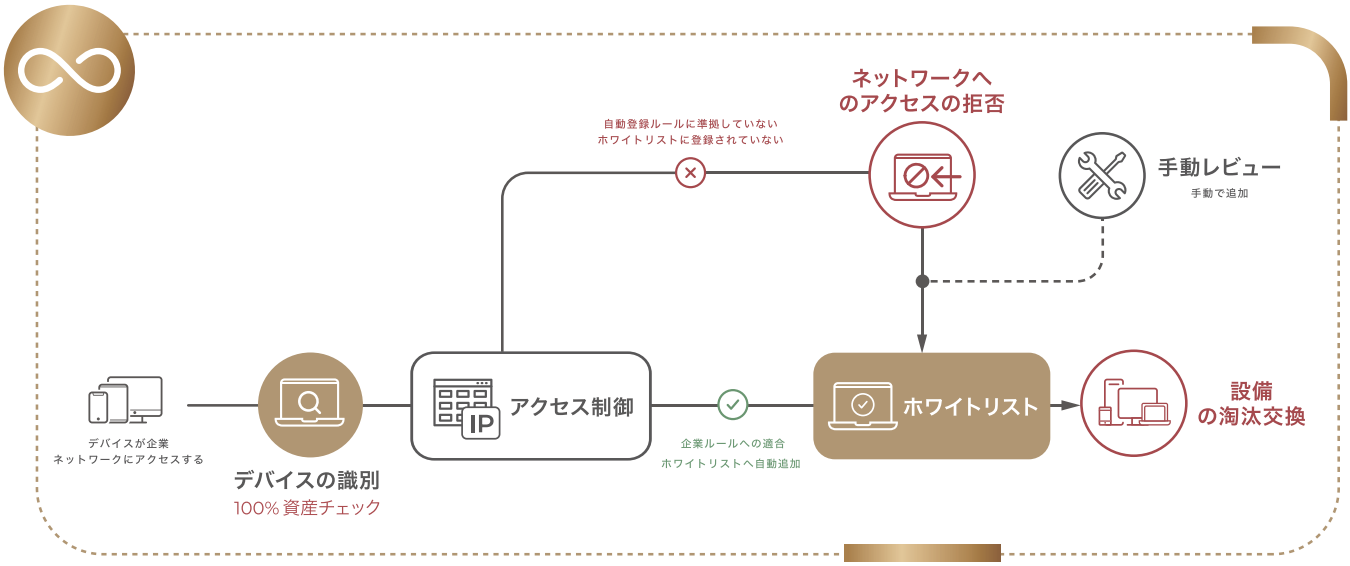
UPASシステムは、デバイスのホワイトリストを自動的に確立し、セキュリティポリシーを満たすデバイスのみにネットワークへのアクセスを許可し、許可されていない外部デバイスのアクセスを禁止し、リダイレクトページ、Agent UI、MSGなどのアラームメカニズムを提供して、イントラネットのセキュリティを根本的に確保できる。

DAM デバイス認証モジュール

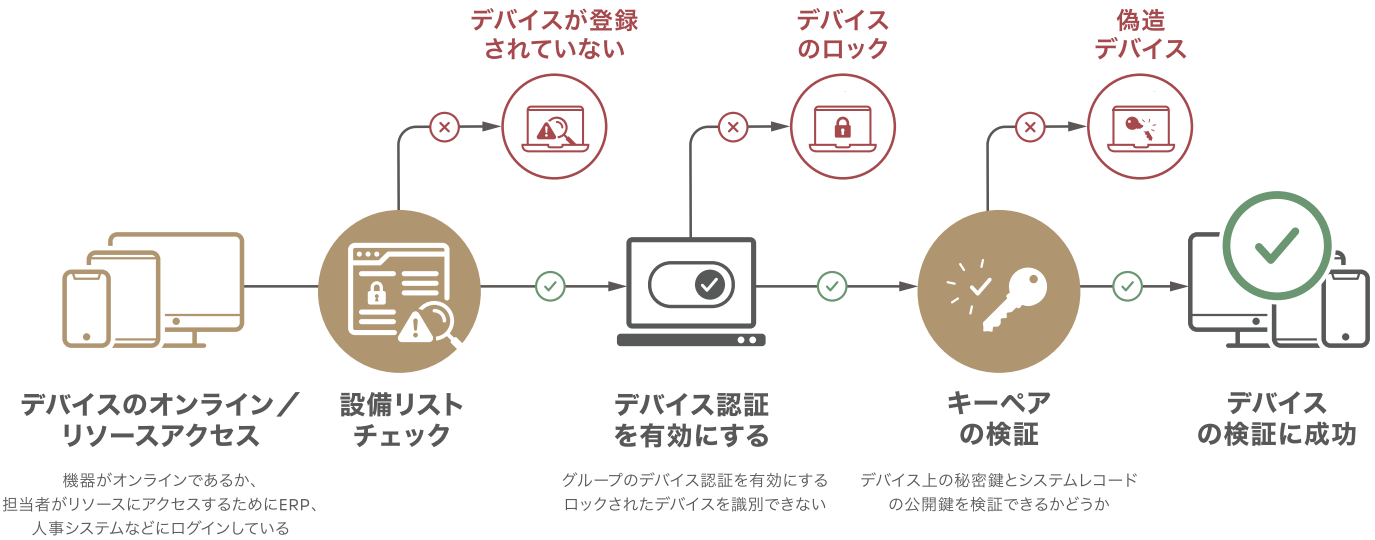
Device Authentication Management

DAMデバイス識別モジュールは、端末デバイスに展開されたAgentを介して、デバイスのハードウェアまたはソフトウェアの保護レベルを確認できる。デバイスがオンラインになったときに、ネットワーク接続されたデバイスが信頼できるデバイスであることを確認できるだけでなく、リソースアクセス状況にも適用できる。識別メーカーとの統合により、全面的なセキュリティ対策が提供される。

このモジュールは、デバイスの追加、ロック、削除などの管理機能、およびデバイスの正常性情報、ダッシュボード統計、および認証履歴クエリ機能を提供し、認証が失敗したときに事件を生成し管理者に通知する。



▲ ARP Scanner – IP / MAC 管理プロセス（アクセス制御）



▼ DAM – デバイス認証モジュール動作フロー

PM パッチ管理モジュール
Patch Management

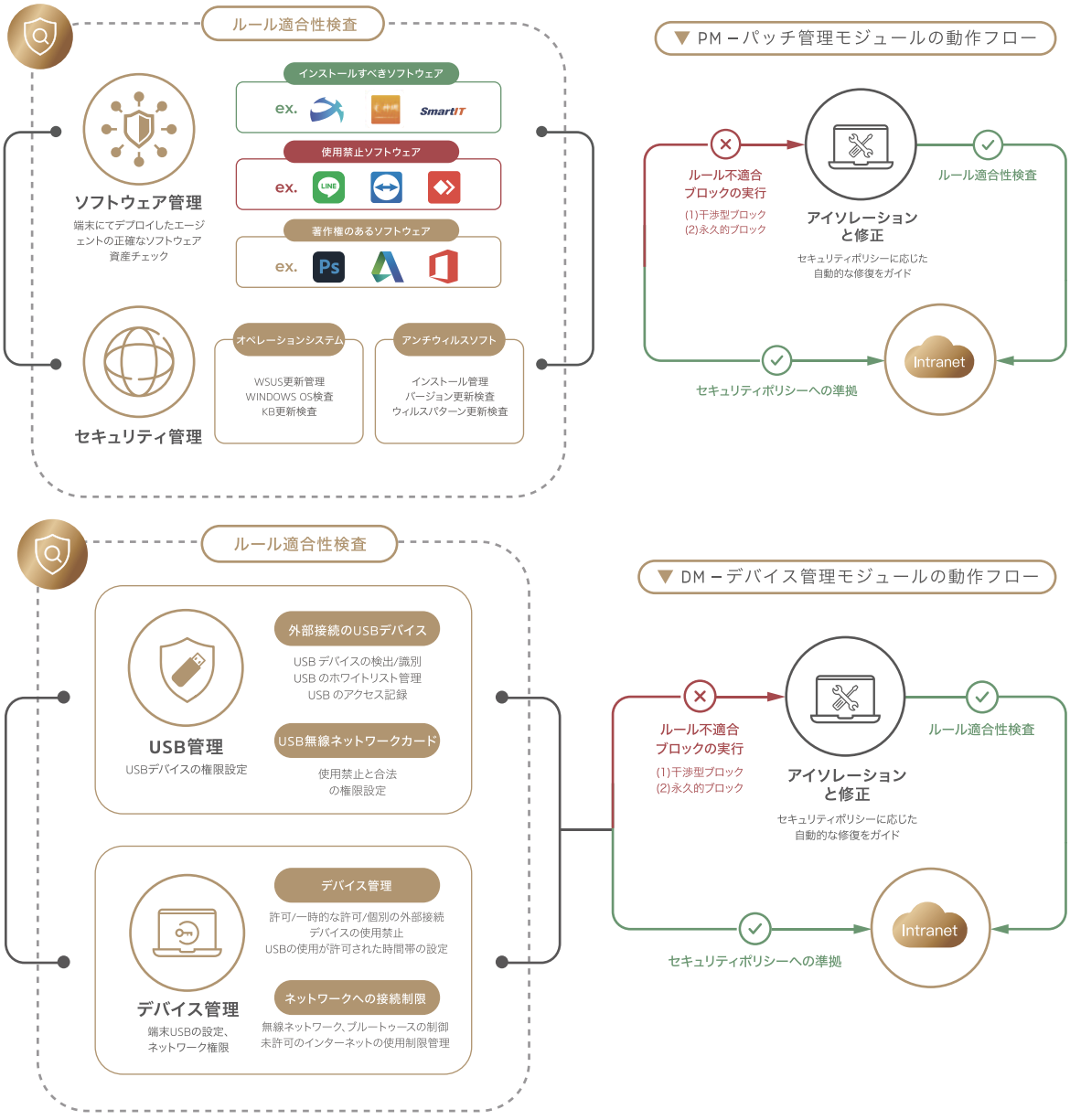
端末デバイスにエージェントをデプロイすることで、定時スキャンとネットワーク接続中のデバイスリスト、Windowsオペレーションシステムのバージョン/KB、アンチウィルスソフトの情報とパターンファイルのバージョンを獲得できます。ソフトウェアリストの検索と収集により、以下の検査を実行します：インストールすべきソフトウェア、使用禁止ソフトウェア、ソフトウェアのライセンス数、ソフトウェアバージョンなど。

ルール不一致イベントが発生した場合(インストールすべきなのにされていない、インストールすべきではないがインストールされている、海賊版ソフトウェアの使用、更新すべきだが更新されて、WSUS更新されていない)ネットワーク接続の切断及びリダイレクトページにより規制原因を通知します。デバイスを安定して運用するため、異なるレベルの権限制限を設定し、セキュリティーポリシーと適合させるための修正へとガイドできます。このほかROMモジュールとの連動により、管理者によるデバイスへの自動ソフトウェア修正の実施をサポートします。

DM デバイス管理モジュール
Device Management

端末デバイスにエージェントをデプロイすることで、USBストレージデバイス、メモリーカード、モバイルデバイス、USBネットワークカード及びCDドライブなどのUSB外付けデバイスを識別し制御します。デバイスが接続できるかどうか、修正権限があるかどうかなど、コンピュータへのデバイスの接続権限を設定することで秘密資料の流出を防止します。USBストレージデバイスのホワイトリスト作成により、認証を通過していない不明なUSBストレージデバイスによるデータ伝送と保管を防止します。

またデバイスを検出し、デバイスに無線ネットワークまたはブルートゥースを使用禁止にすることで、企業ネットワークをバイパスにしたプライベートネットワークによるセンシティブなデータの伝送を防止します。



ROM リモートオペレーション管理モジュール
Remote Operations Management

端末デバイスにエージェントをデプロイすることで、デバイスのソフトウェア/ハードウェアの型番と仕様などの情報を検索・収集し、リモートオペレーション管理を実行します。

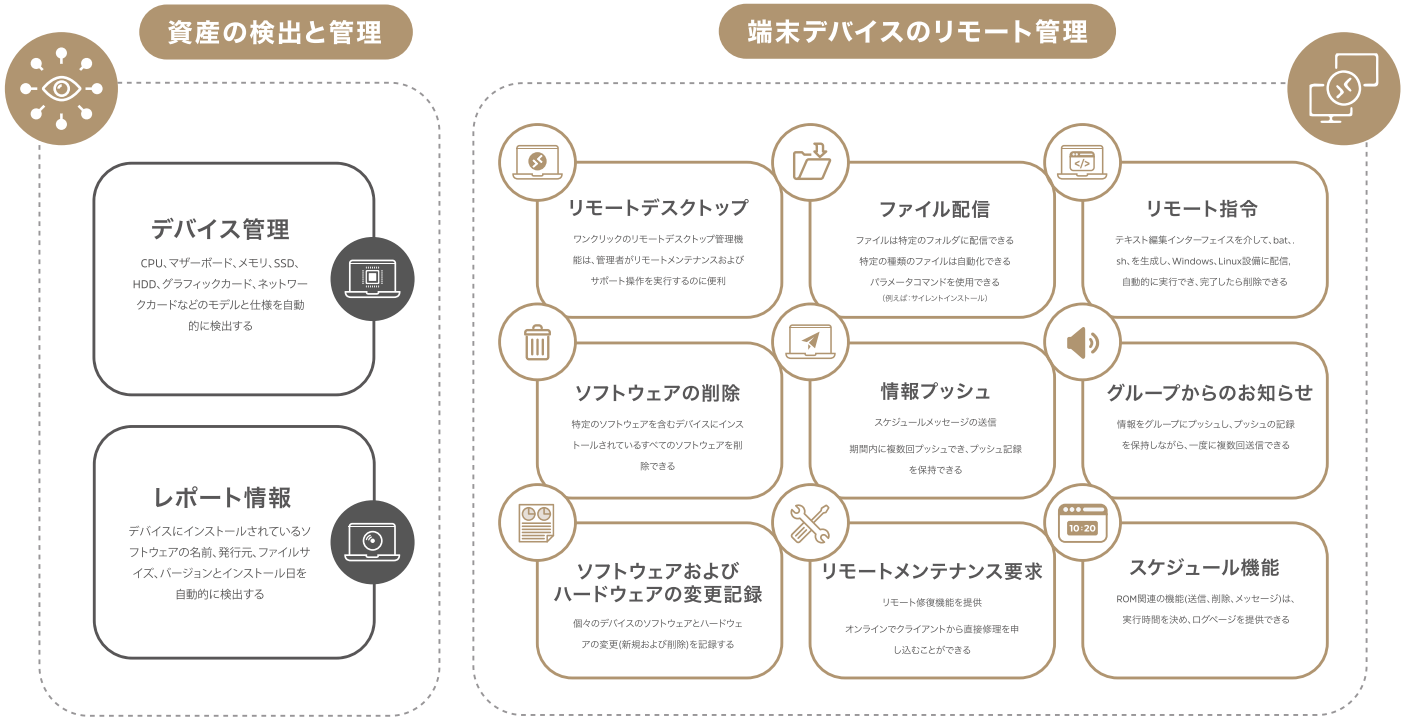
リモートデスクトップ管理機能とファイルの割り当、ソフトウエアの削除機能も備えています。パラメータやコマンドを組み合わせることで、ファイルのサイレントインストールを実行できます。このほか管理者が端末デバイスを管理・制御、メンテナンスしやすいよう、メッセージのプッシュ通知及びグループへのアナウンス機能も提供されています。ユーザー側からも管理者にリモートデスクトップのニーズを発信できます。エージェントUIを通して問題を説明することで、管理者によるタイムリーな処理をサポートします。

TIM 信頼判断モジュール
Trust Inference Management

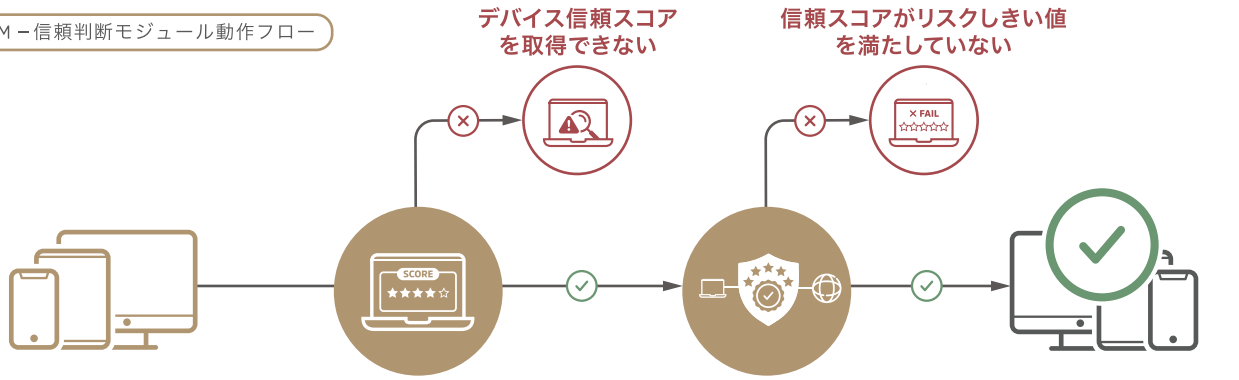
TIM信頼判断モジュールは、デバイス情報（OS、ウイルス対策、インストールされているソフトウェア、潜在的なリスクの脆弱性など）のインベントリを作成することにより、デバイスセキュリティ評価の基礎としてデバイスセキュリティ評価を行う。

収集されたセキュリティデータは、ID認証およびデバイス識別と組み合わされて、リソースにアクセスする際の信頼スコアを評価するための基準として使用でき、アクセス結果は意思決定コントローラーによって決定される。　このモジュールには、デバイスセキュリティビュー、信頼スコア情報、ダッシュボード統計、および履歴レコードがある。

▼ ROM－リモート運用管理モジュール機能の説明



▼ TIM－信頼判断モジュール動作フロー



デバイスのオンボード／リソースへのアクセス
機器がオンラインであるか、担当者がリソースにアクセスするためにERP、人事システムなどにログインしている

デバイスの信頼スコアを取得する
信頼判断アルゴリズムは、デバイスの現在の信頼スコアを取得するために使用される

リスクしきい値基準を満たす
信頼スコアがリスクしきい値の基準を満たしているかどうかを確認し、信頼スコアが基準を満たしていない場合、デバイスはリソースにアクセスできない

デバイスの信頼の推論フローを完了する

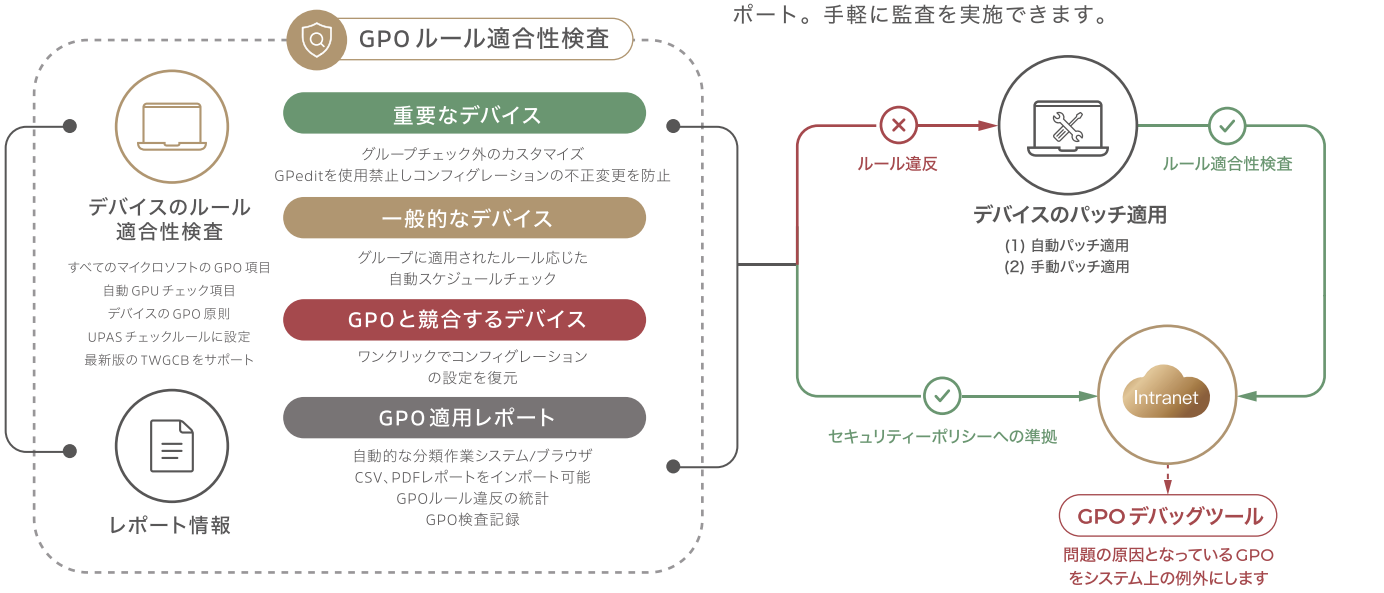
GPO GPO 管理モジュール
GPO Management

UPASのGPO管理モジュールは完成度の高い資産チェックで、WMIネットワークの最高権限を持たなくても、ドメイン内のデバイスに対しGPO適用チェックを実行できます。GPOに準拠していないデバイスに対し、自動修復または手動での修復を実行でき、自動的に適用結果をレポートし、修復記録を提供します。ワンクリックでのコンフィギュレーション復元機能を備え、デバイスをGPO適用前のコンフィギュレーションに復元することで、デバイスがGPO適用後に正常に運用できない状態を防止します。

VANS 脆弱性の警告と通知システム
Vulnerability Alert and Notification System

NVD脆弱性データベースを統合し、自動的に環境内のコンピュータのソフトウェア資産にNVDが公表するCVEのバグがあるかどうかを比較、企業のコンピュータのソフトウェア資産をまとめて検索します。

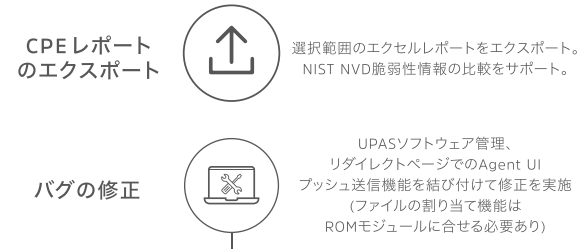
CVEによるマイクロソフト系の脆弱性及び非マイクロソフト系脆弱性チェック、またはデバイスのKBIDによる修復関連CVEの脆弱性のKBがデバイスにインストールされているかどうか、デバイスのソフトウェアチェックで何台のデバイスがCVEのバグがあるソフトウェアをインストールしているかをチェックし、ソフトウェアの更新検査、ソフトウェアの割り当て、エージェントUI、リダイレクトページなどによりバグを修復します。またCPEレポートのインポートをサポート。手軽に監査を実施できます。

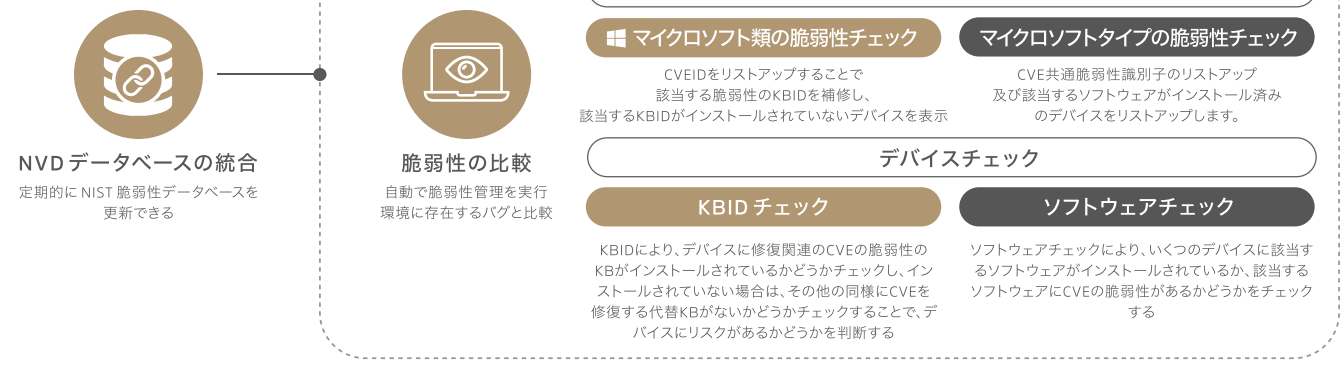


▲ GPO – GPO 管理モジュールの動作フロー



▼ VANS – 脆弱性アラートおよび通知システムの動作フロー





AD 管理模組
ADVantage

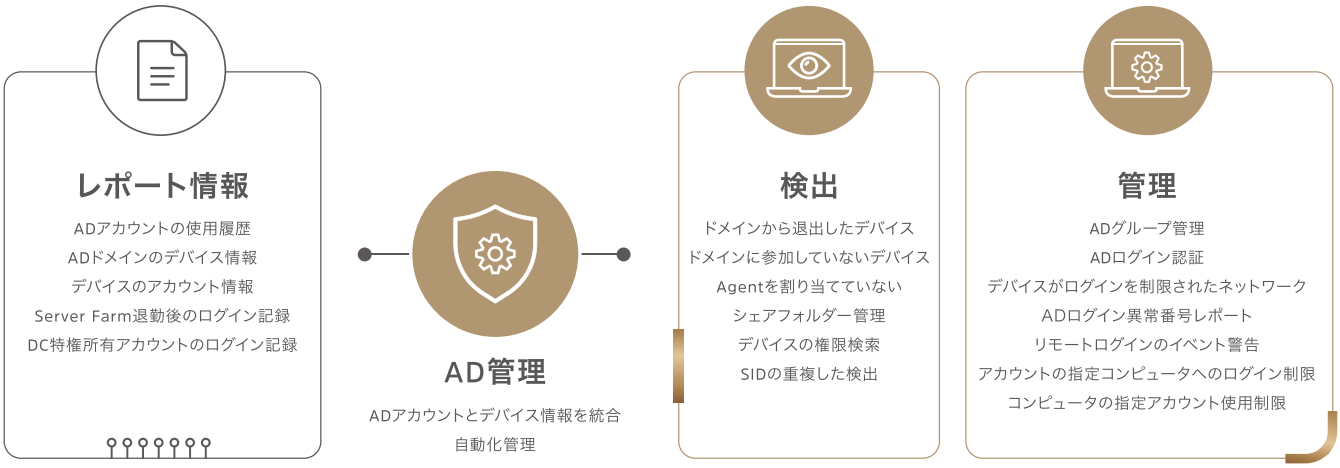
ADアドレスとコンピュータの連動、使用しているデバイスでのログインの禁止、ドメインからの私的な退出などの方式により、強制的にすべてのコンピュータに企業のセキュリティーポリシーを遵守させます。特定のADアカウントで特定のPCにログインします。セキュリティポリシー及び管理ではすべてのWindows搭載デバイスがカバーされ、20個以上のAD情報とデバイス情報を統合し、アカウントの使用履歴を提供します。

シェアフォルダーへのファイルの検出及び異動が可能です。SID重複イベントを検出し、特権を持つアカウントのログイン/ログアウト記録と使用しているデバイスのアカウントなどの情報を作製し、異常な行動を管理者が発見できるようサポートすることで、すべてのADドメインに参加すべきデバイスを制御できます。

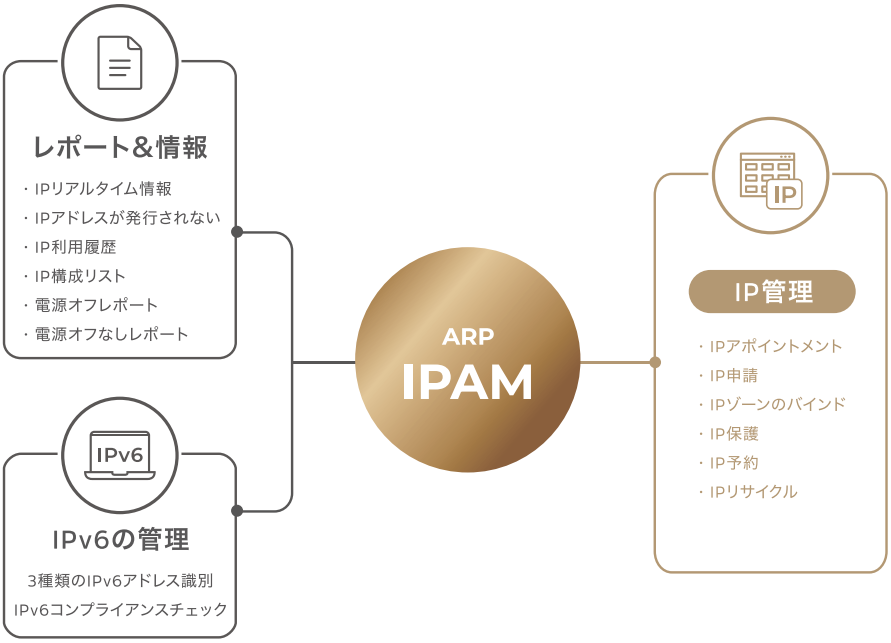
IP / MAC 管理モジュール
ARP Scanner　IP管理

IP/MAC/DHCPセグメント/コンピューター名/ハードウェア指紋(UUID)間の複数のバインディングを接続されているすべてのデバイスで実行して、IP保護、IP予約、IPリサイクル、IP競合防止、MAC偽造防止などの機能を実現できる。

同時に、UPASは出力できる:割り当てられていないIPリスト、IP構成リスト、IP使用状況レコード、オフになっていないレポート、オンになっていないレポート、その他のイントラネット統計リスト、管理者がイントラネット資産とIP使用状況を完全に把握するのに役立ち、関連する設定を1ページで行うことができ、マネージャーがイントラネットIPリソースとデバイスをタイムリーかつ簡単に管理するのに役立つ。



▲ AD – AD管理モジュールの動作フロ



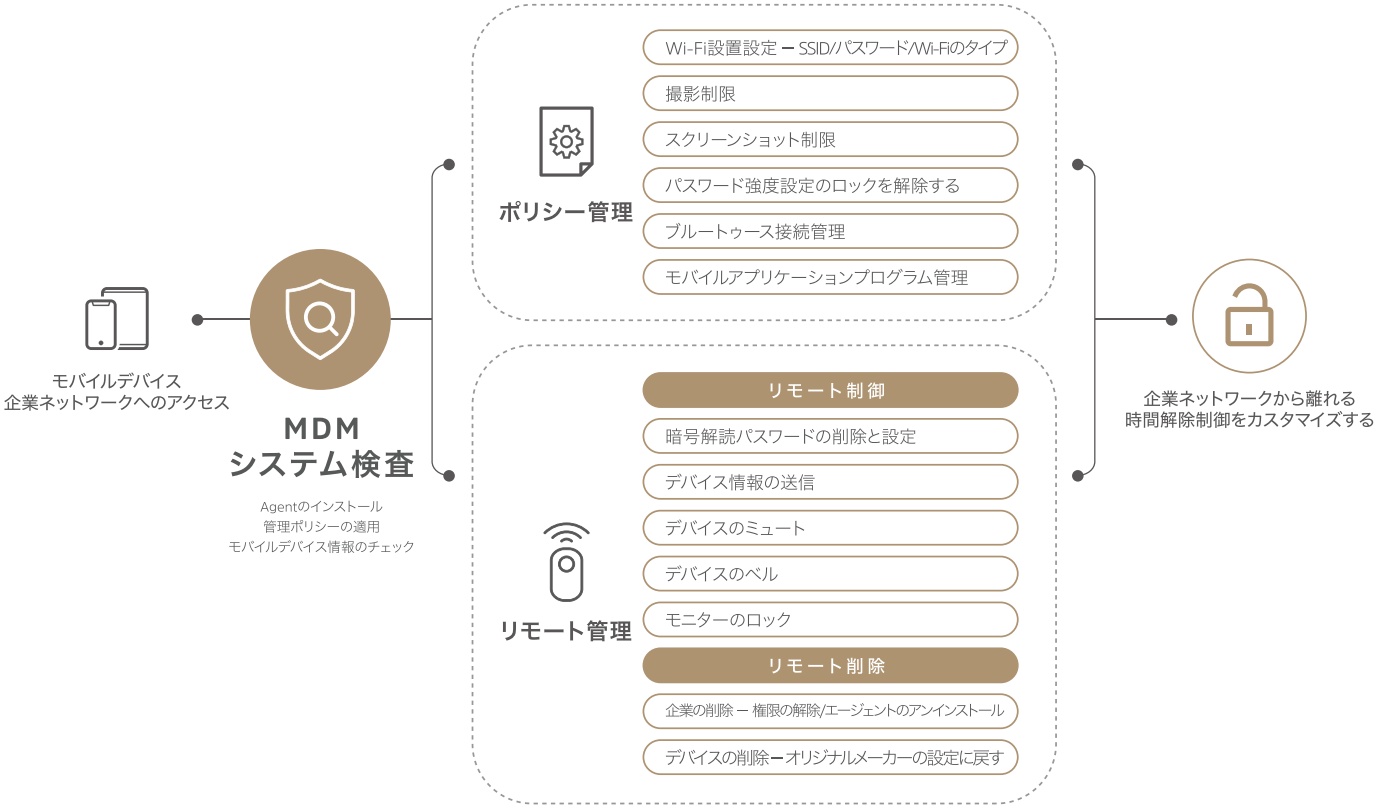
▶ ARP Scanner – IP/MAC管理プロセス(IP管理)

MDM モバイルデバイス管理モジュール
Mobile Device Management

端末デバイスへのエージェントのデプロイ、またはiOS　MDMサーバーの構築により、IP/MAC/アカウント/スマートフォンの型番/OSの詳細なバージョン/製造メーカー/ローミングのステータス/前回のオンライン時間などの情報を検索・収集できます。またWi-Fiとブルートゥースによるオンライン管理、解読用パスワードの強度設定、写真撮影とスクリーンショットの制限、アプリケーション管理及びリモートでのモニターロック、ロック解除、解読用パスワードの再設定機能を実行できます。

異なる工場エリア/作業エリアに応じたそれぞれの管理ポリシーを設定できます。OSのバージョン/使用されているIPセグメントなどの情報に応じて、所属グループを自動的に分配。グループのセキュリティポリシーを適用することで、管理員の作業負担を軽減します。

Androidのデバイスにはデータのオリジナルメーカーの設定への復元、サイレントモードの起動、デバイスのベル、メッセージの送信などのリモート機能を追加しました。またポジションとオフラインの補助的な判断の提供により、モバイルデバイスが制御エリアを離れた後、制御を解除するよう確保することで、従業員が制御エリアを離れたと見せかけて制御から逃れること、さらには秘密情報の盗み取りを防止します。



▲ MDM – モバイルデバイス管理モジュールの動作フロー

SIM セキュリティ統合管理モジュール
Security Integration Management

端末デバイスへのエージェントのインストールは不要。ただちにWSUSメインマシン、様々なアンチウィルスソフト（Trend Micro/Macfee/Kaspersky/360Safeguard）と資産管理ソフト（神網資訊デバイス管理システム/WinMatrix/X-FORT/IP-guard/SmartIT/Ivanti/SCOM/SCCM）を結び付けた、統合性のある管理を実現します。多項目のルール適合検査を実行し、ネットワーク接続の切断及びリダイレクトページによって、強制的にユーザーがルールに適合するよう修正します。ルール不適合のデバイスに対しては、異なるレベルの権限制限を設定できます。

IP/MACシステムにより約100%のWSUSマネジメント率、アンチウィルスソフトのインストール・更新率と資産管理ソフトのインストール/更新率を実現することで、端末デバイスを企業のセキュリティーポリシーに適合させています。

IPL IPアドレス解析モジュール
IP Locator

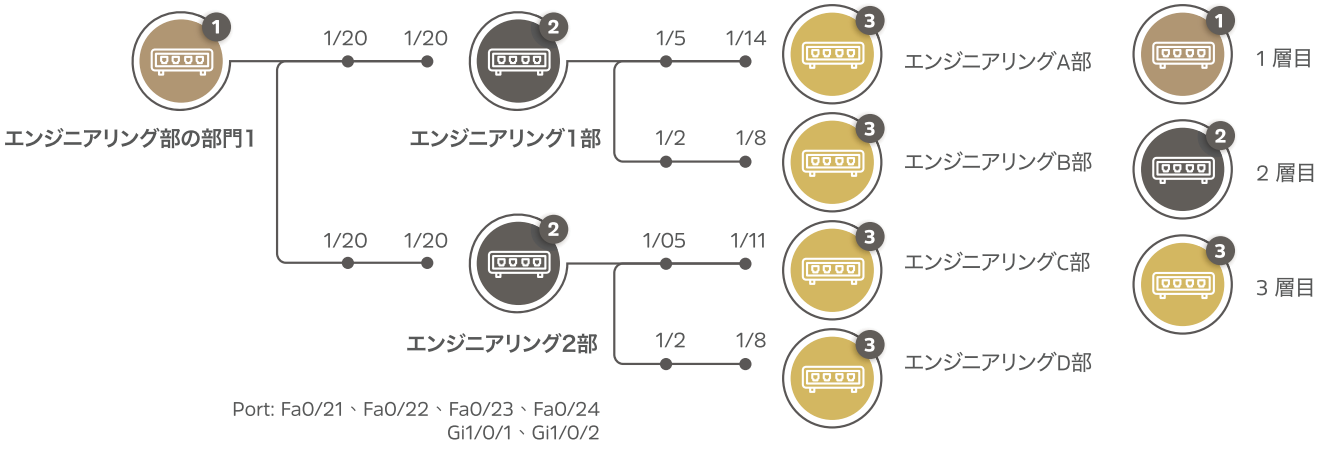
SNMPにより自動的に上下スイッチを結び付ける関連性を構築します。デバイスIPの実体アドレスを識別して自動的にネットワークトポロジーを作成し、MAC/IP/スイッチ/ポート/VLAN ID の履歴を提供します。市販されているほとんどのブランドのスイッチをサポートしています。Windows/Linux/macOS/Android/iOSなどの様々なプラットフォームのデバイス情報を取得できます。

管理者による資産チェックと統計をサポートし、単一ポート複数MACリストや、MAC/ポートの連動設定を構築できます。いかなる私的アクセスのデバイスによるイベントが発生した場合も、システムは自動的に警告を発して修正のヒントが表示されることで、ネットワークセキュリティとネットワークの正常な運営を確保します。

▼ SIM – セキュリティ統合管理モジュールの説明



▼ IPL – IPアドレス解析モジュールアーキテクチャの概略



IPv6 IPv6管理モジュール
IPv6 Management

エージェントのインストールは不要。ただちに全面的なIPv6管理のサポートします。ユニキャストやマルチキャスト、いかなるキャスト方式でも3種類のIPv6アドレスを検出できます。IPv6デバイスにルール適合検査を実行することで、IPv6を使用する外部デバイスをブロックします。

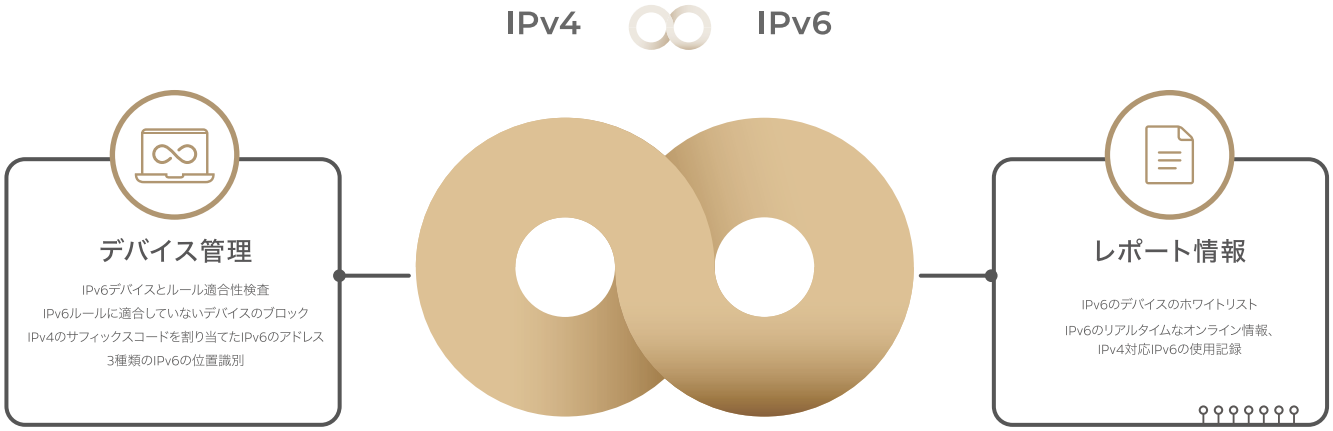
IPv6ホワイトリスト自動構築機能により、一時的及び永久的なIPvホワイトリストを提供します。またIPv6デバイスリストをインポート/エクスポートできます。IPv6の管理上のニーズに応じて、異なる管理状況に対するホワイトリスト設定し、IPv6及びMACアドレスのマルチ連動機能を提供します。

このほかIPv6リアルタイム情報、履歴及びIPv4アドレス対応リストも提供しています。

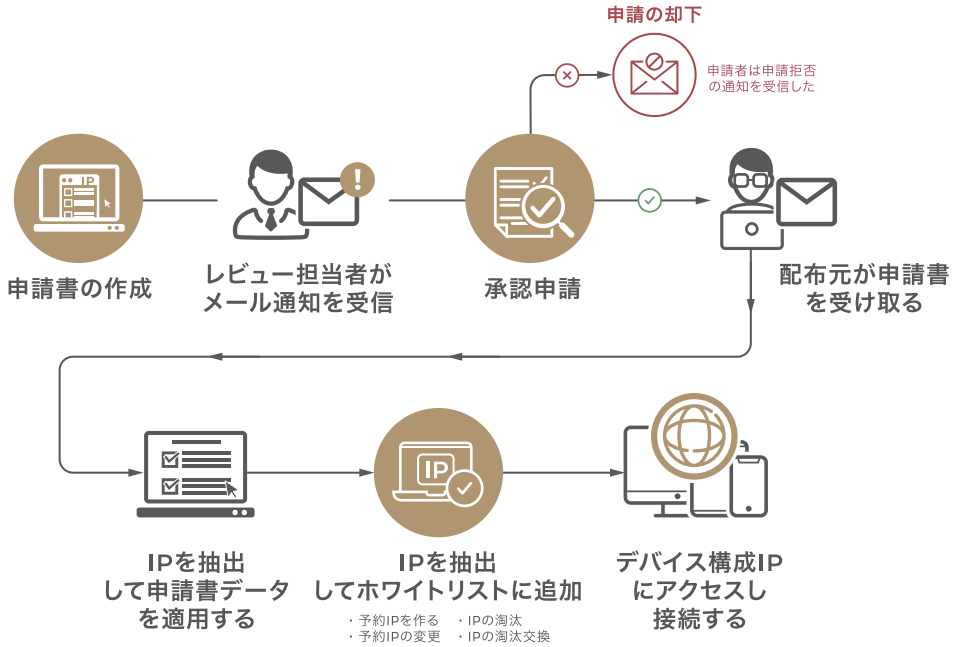
IPAF IP申請フォーム機能
IP Application Form Functionality

オンラインIP申請フォームをカスタマイズすることにより、さまざまなユニットの申請者は、煩雑な紙の承認プロセスを排除し、全面的な電子操作を実現しながら、IP申請を簡単に完了できる。また、IPページでは検索機能を利用することができ、ユーザーは同じページで利用可能なIPをすばやく検索できる。

ユーザーが使用するIPアドレスを確認すると、システムが関連するIP申請情報を取り込み、申請者は申請の進捗状況を簡単に追跡し、必要に応じてすべての操作の状態を確認でき、これらの記録は申請記録ページに記録される。 同時に、エクスポート機能も備えているため、申請者は関連するすべてのアプリケーション情報をエクスポートして、保存および照会を行うことができる。 データのセキュリティが確保されるだけでなく、将来の確認と管理も容易になる。



▲ IPv6 – IPv6 管理モジュールの動作フロー



IPAF – IP 申請フォーム機能動作フロー ▶

DHCP DHCP Server整合機能

DHCP Server Integration Functionality

配信のホワイトリストを介してMACアドレスと同期できる。 ホワイトリストが作成されると、ホワイトリストがDHCPサーバに同期され、システムはホワイトリスト内のIPアドレスとMACアドレスの組み合わせをDHCPサーバの予約領域に自動的に同期する。ホワイトリストからIPアドレスを削除すると、対応するIPアドレスとMACアドレスがDHCPサーバの予約領域から自動的に削除される。

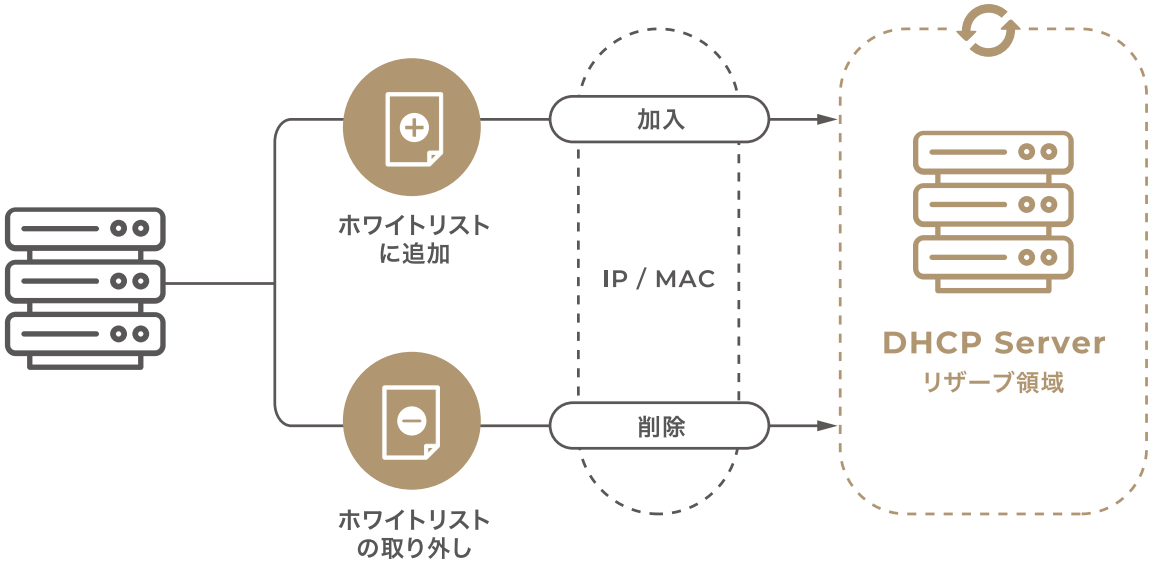
IPアドレスが同じでMACアドレスが異なる場合、システムはDHCPサーバの予約領域のIPアドレスに対応するMACアドレスをホワイトリストのMACアドレスに自動的に変更し、一貫性を維持する。 DHCP サーバに予約エリアはあるが、ホワイトリストにはない場合、システムは予約エリアからIPアドレスを削除して、ホワイトリストで指定された IPアドレスとMACアドレスだけが予約エリアに保持されるようにする。

IPLI IP使用記録統合機能

IP Usage Log Integration Functionality

UPASは、アップストリームIPアドレスとオフラインIPアドレスの使用情報と記録を指定されたsyslogホストに同期できるため、ネットワーク上のIPアクティビティをリアルタイムで追跡および監視できる。　この機能は、ネットワークのセキュリティを確保し、ネットワークの運用と管理を最適化するためのより完全な監視および分析ツールを提供するのに役立つ。情報をSyslogホストに同期することで、リスク評価、インシデント調査、コンプライアンスコンプライアンスのために履歴データを簡単に保存および取得することもできる。

▲ DHCP – DHCP サーバー統合機能の運用プロセス





IPLI – IP 使用記録統合機能の動作フロー ▶

IDC ID認証モジュール
ID Checker

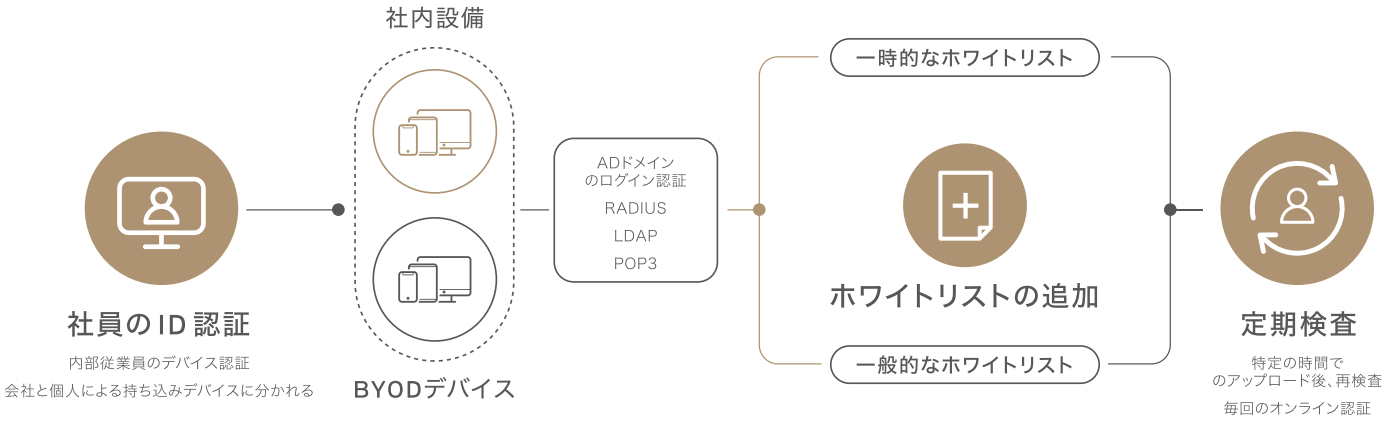
AD/LDAP/POP3/RADIUSサーバーを利用し、私的な持ち込みデバイス(BYOD)のID認証を実行します。すみやかにデバイスを識別してオンライン許可を管理し、人員とデバイスのゼロトラストセキュリティを構築します。

企業または政府のネットワークに接続後、システムはただちにリダイレクトページに誘導し認証を実行します。企業のセキュリティーポリシーに応じたID認証実行後、システムは自動的に対応するアクセス権限(インターネット/イントラネット/特定のセグメント)及び有効期限を与えます。またデバイスに一定時間ごとに定期的な認証を実行するようリクエストすることも可能です。

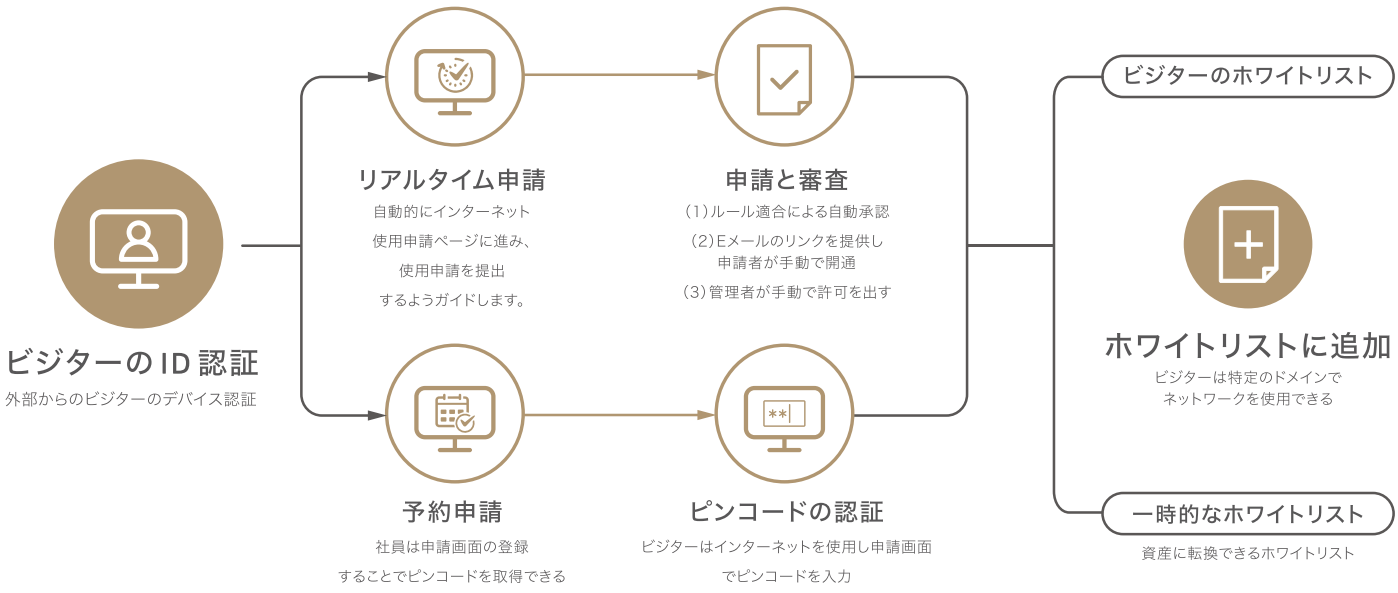
GAM 訪問者管理モジュール
Guest Access Management

訪問者の外部デバイスが企業ネットワークに入ると、訪問者管理モジュールは、自動訪問者予約アプリケーションを提供することができ、ネットワークは、自動許可、手動許可、および応答許可によって開くことができる。

予約アプリを使用する訪問者は事前にPIN Codeを取得し、企業のネットワークに入った後、アプリケーション接続ページでPIN Codeを入力してネットワークを開くと、すべての訪問者がイントラネットとエクストラネットのアクセス権とアクセス時間制限を設定でき、制限時間が経過するとシステムが自動的に許可を取り消す。自動化されたメカニズムにより、訪問者の定義と管理が容易になり、監査用の詳細な記録が生成される。



▲ IDC – ID認証モジュールの動作フロー



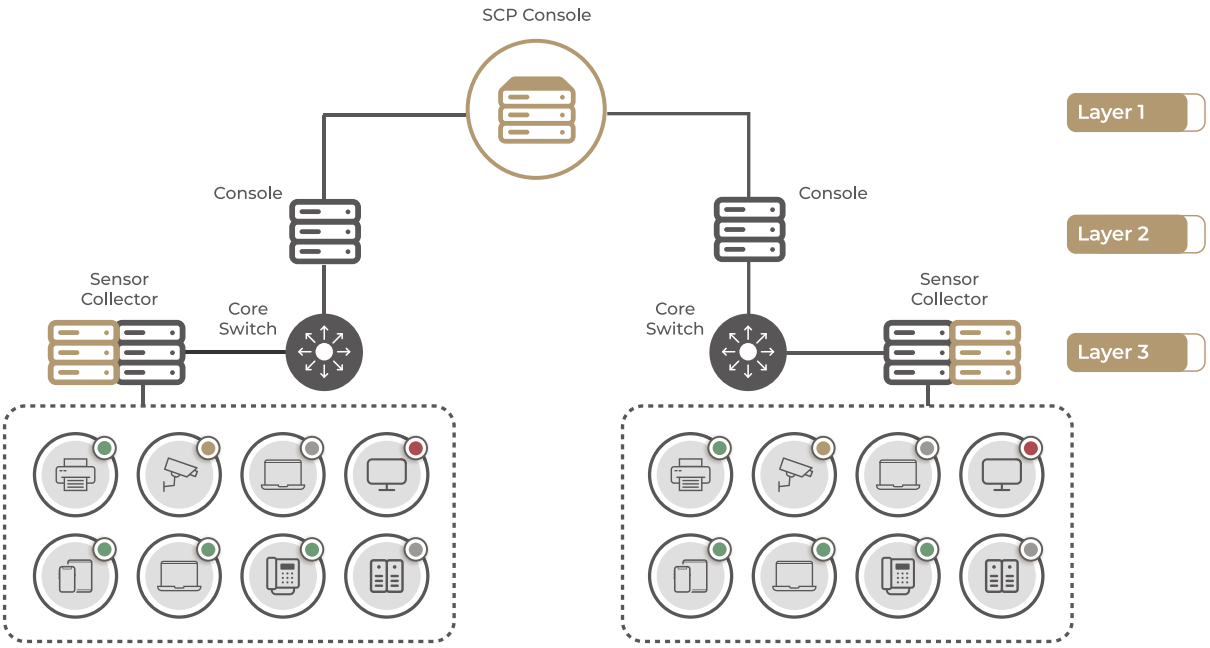
▼ GAM – 訪問者管理モジュールの動作フロー

SCP システム中枢プラットフォーム
SCP Console

5,000セット以上のIP/MACアドレスを持つ大企業が国境を越えた、地域を越えた管理を完了するための支援、本社にSCP　Console/子Console/Sensorを設置して他の地域を統一的に管理し、さまざまな地域でのコンソール接続の異常を防止し、各地域のネットワーク状況をリアルタイムで表示し、グローバルな内部データを統合し、管理者がローカルイベントの傾向とセキュリティ管理ポリシーを分析するのを支援する。

また、ホワイトリストのデバイス情報と出張のホワイトリストをさまざまな地域のサブコンソールにリアルタイムで同期できるため、出張者の権限の管理が簡素化され、グローバルに更新される。

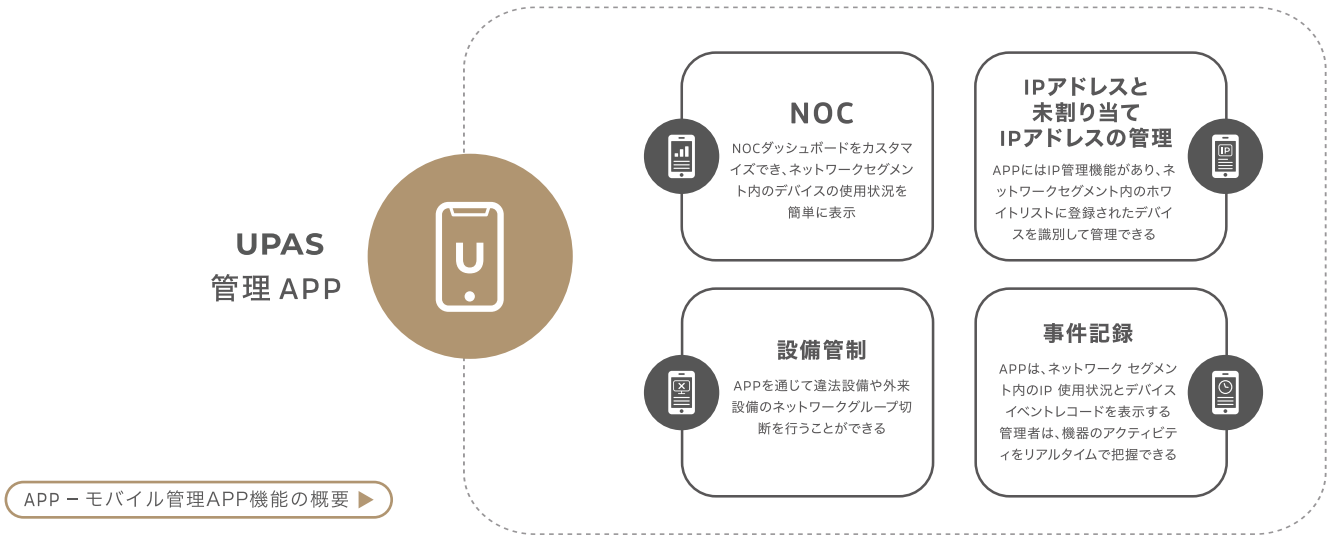
▼ SCP – システム中枢プラットフォームアーキテクチャの概略



APP アクション管理APP
UPAS Management App

モバイル管理アプリは、UPASの実用的な機能を統合し、管理者がいつでもどこでもエンタープライズネットワークセグメントとデバイスの使用状況を把握できるようにする。カスタマイズされたNOCダッシュボードを使用すると、ネットワークセグメント内のデバイスの使用状況を簡単に確認できる。

さらに、このアプリはIP管理機能を提供し、ネットワークセグメント内のホワイトリストに登録されたデバイスを簡単に識別して管理できる。　機器制御機能により、違法な機器や外国機器のネットワークを効果的にブロックできる。同時に、APPはネットワークセグメント内のIP使用状況とデバイスイベントレコードも表示するため、管理者は各デバイスのアクティビティステータスを完全に把握し、潜在的な問題にタイムリーに対応できる。

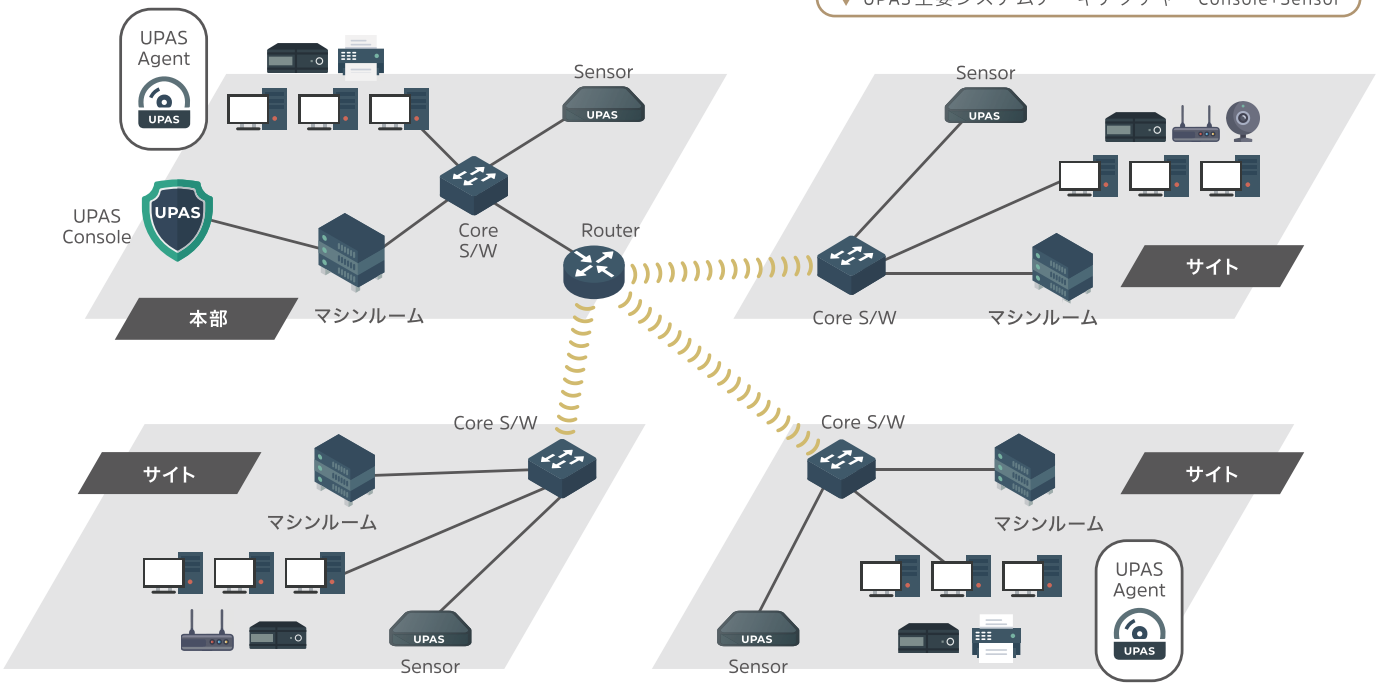


APP – モバイル管理APP機能の概要 ▶

UPAS 主要システム アーキテクチャ - Console + Sensor (+Agent)

オブザーバビリティを備えたデプロイの採用により、顧客側のネットワークアーキテクチャを変更する必要がありません。無線、有線のネットワーク環境のどちらにも適用できます。センサーを顧客の環境のCore　S/Wに接続するだけで、Trunk　Portよりネットワークパケットを受け取れます。すべてのオンラインデバイスのチェックを実行し、コンソールによりID認証とネットワークへのアクセス制御を実行します。

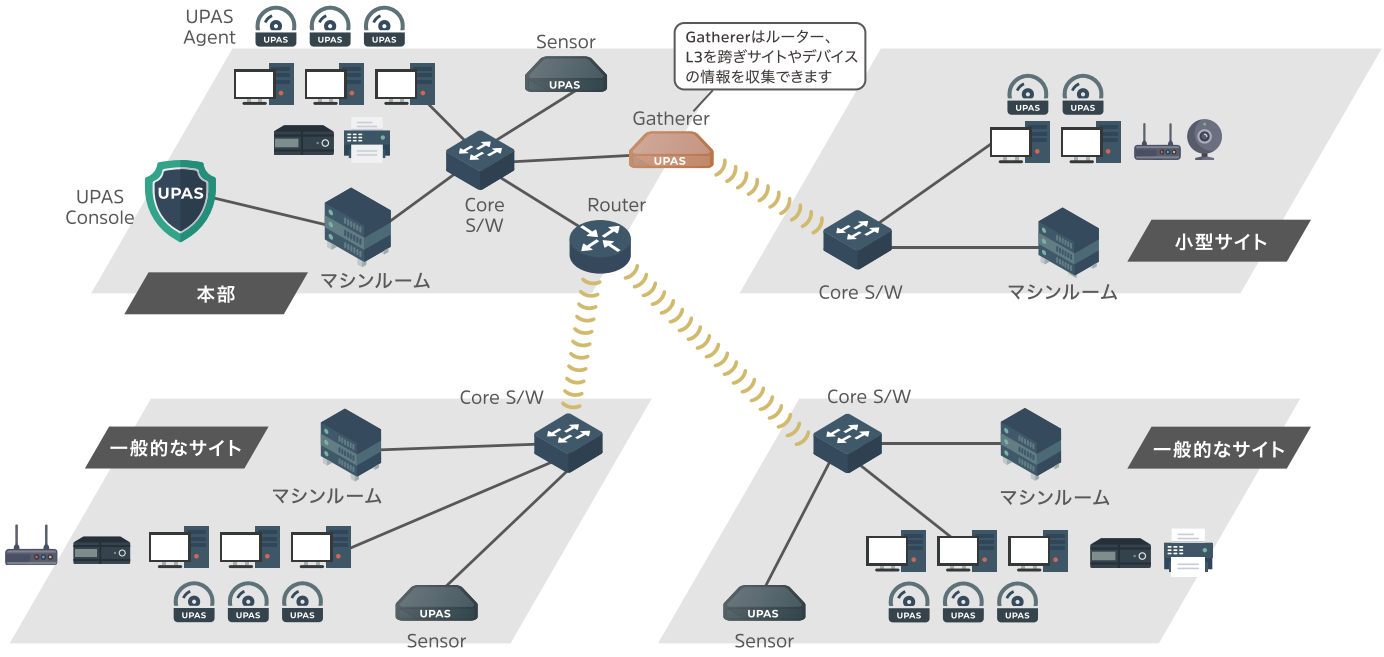
▼ UPAS主要システムアーキテクチャーConsole+Sensor



Gatherer フレーム

センサー+Gathererのコンビプランでは、同時にアクセス制御とアドバンス資産管理のニーズを満足できます。特にサイト数が非常に多い環境では、本部にGathererを設置するだけで、ルーター、ファイアウォールを跨いだ管理を実行できることから、システムの構築コストが大幅に削減されます。

▼ Sensor+Gatherer フレーム



UPAS ZTA プラットフォーム全体ですべての主要なオペレーティングシステムをサポートする

Windows システムのサポート
MacOS システムのサポート
Linux システムのサポート

ZERO TRUST ARCHITECTURE

- 著作権ソフトウェアの管理
- インストールされているソフトウェアの概要
- ファイル/指令の配信
- ソフトウェアとプログラムのチェックを無効にする
- USB外部デバイス管理
- ソフトウェアの削除
- ソフトウェアとバージョンチェックをインストールする必要がある
- USBホワイトリスト
- リモートデスクトップ
- 設備ソフトウェア変更記録
- ワイヤレスネットワーク管理
- ユーザーがリモートサービスの要求を開始する
- オートコンプリメンテーション
- ソフトウェアおよびハードウェアの資
- 情報プッシュ/グループブロードキャスト

UPAS ZTA 推奨仕様

	Console		Sensor	
CPU	< 1,000 U	4C8T	BOX: <500	J3160 (4C4T)
	1,000 ~ 3,000 U	8C16T	BOXi7: <1,000	i7-8550U (4C8T)
	3,000 ~ 5,000 U	12C24T	1U: 2,000	E3-12XX (4C8T)
RAM	< 1,000 U	8 GB	BOX: <500	4 GB
	1,000~3,000 U	16 GB	BOXi7: <1,000	8 GB
	3,000~5,000 U	32 GB	1U: 2,000	8 GB
HDD	< 1,000 U	250 GB SSD X4 Raid5	BOX: <500	250 GB SSD X1
	1,000~3,000 U	250 GB SSD X4 Raid5	BOXi7: <1,000	250 GB SSD X1
	3,000~5,000 U	250 GB SSD X5 Raid10	1U: 2,000	250 GB SSD X1
コメント	5000 U 以上は別途ご確認ください		シングル NIC 2000 U / VLAN 20個 / ドメイン制限20個	

UPAS ZTA 5 つの主要な情報セキュリティソリューション

お客様の管理ニーズに合わせたカスタマイズ
一般的な使用シナリオを一度に確認

UPASは、企業が直面するイントラネットの情報セキュリティと管理の主な問題に対応して、UPAS　ZTAの20の強力なモジュール機能を統合した5つのソリューションを提供している。



NAC ネットワークアクセス制御

承認されていないデバイスがイントラネットに接続されていないことを確認する

ARP　DAM

適用シーン

ネットワークにアクセスするデバイスの種類と数が劇的に増加するにつれて、企業や政府はこれらのデバイスのセキュリティリスクを考慮する必要がある。

1. エージェントをインストールせずに全面的なデバイスインベントリとメモリ取得制御を実現し、ネットワークセキュリティを確保する方法は?
2. セキュリティポリシーに基づいてデバイスのホワイトリストを自動的に確立し、要件を満たしていないデバイスのイントラネットへのアクセスを禁止する必要がある。
3. デバイスがオンラインになったときに、信頼できるデバイスを検証できるようにしながら、全面的なデバイスセキュリティを提供する必要がある。

ソリューション

- UPASのNACシステムは、ARPの特許取得済みのパケット解決技術を使用して、エージェントレスのデータ収集、デバイス識別、および高強度のアクセス制御を実現し、IP/MAC管理やネットワークアクセス制御を含む100%の資産インベントリを実現する。
- UPASシステムは、要件に基づいてアクセスルールを策定し、セキュリティポリシーに準拠したデバイスのホワイトリストを自動的に作成し、外部デバイスへの不正アクセスを禁止する。 同時に、イントラネットのセキュリティを確保するために、リガイドページ、Agent UI、MSGなどのアラームメカニズムが提供される。
- DAMデバイス識別モジュールは、デバイスの正常性情報や識別履歴クエリ機能など、ハードウェアまたはソフトウェアの保護レベルのチェックを実行できる。 識別に失敗すると、システムはマネージャに通知する事件を生成する。



ITAM IT 資産管理

ウイルスを完全に防御し、脆弱性を修復
コンプライアンスに悩まず、設備の健康度を確保

PM　DM　ROM
TIM　GPO　VANS

適用シーン

エージェントソフトウェアをインストールするためのエンドポイントセキュリティソリューションにはまだデッドスポットがあり、ほとんどのエンタープライズ環境で完全にインストールできないデバイスの数は増え続けている。

1. 企業内の多くのオンラインデバイスは定期的に更新されないことが多く、外部侵入ノードを形成しやすいため、企業のウイルス対策ソフトウェアとアプリケーションが正常に動作できるようにするにはどうすればよいですか?

2. データアクセス用の不明な外部デバイス(USBなど)により、機密データの漏洩や恐喝の大きなリスクが生じる。

3. 企業やユニットの内部機器が政府の規制を満たしていることを確認し、それらの正常性を管理する方法

ソリューション

- UPASは包括的な資産管理とセキュリティ監視を提供し、端末デバイスを自動スキャンし、ソフトウェアやシステム情報を収集します。USBや外部デバイスも監視し、データ漏洩を防止するための権限を設定します。脆弱性データベースを統合し、システムの脆弱性を自動的に識別して修正し、セキュリティを向上させます。

- リモートオペレーションと管理機能を提供し、リモートデスクトップ管理やファイル配信を容易にし、管理者が遠隔操作とメンテナンスを行えるよう支援します。メッセージプッシュやグループブロードキャスト機能も提供し、デバイスの効果的な管理とメンテナンスを支援します。

- 信頼評価とアクセス制御を強化し、デバイスのセキュリティデータと身元確認に基づいてアクセス時の信頼スコアを評価し、アクセス権限を決定します。また、デバイスのセキュリティ検査、信頼スコア情報、アクセス履歴レコードを提供し、管理者が適切なアクセス決定を支援します。

IAM アイデンティティ識別管理

設備人員の身分がすべて検証に合格することを確保する

AD

適用シーン

内部ネットワークに入るデバイスは、ID　に基づいて最小限の特権を付与して識別および管理し、マネージャーがデジタル ID を可視化できるようにする必要がある。

1. 企業は、特定のADアカウントを使用した特定のPCへのログインや、すべての　　Windowsデバイスの制御など、すべてのコンピューターに企業のセキュリティ　ポリシーを適用したいと考えている。

2. 企業は、共有フォルダ内のファイル移動を監視し、潜在的なセキュリティリスクと異常な動作を検出する必要がある。

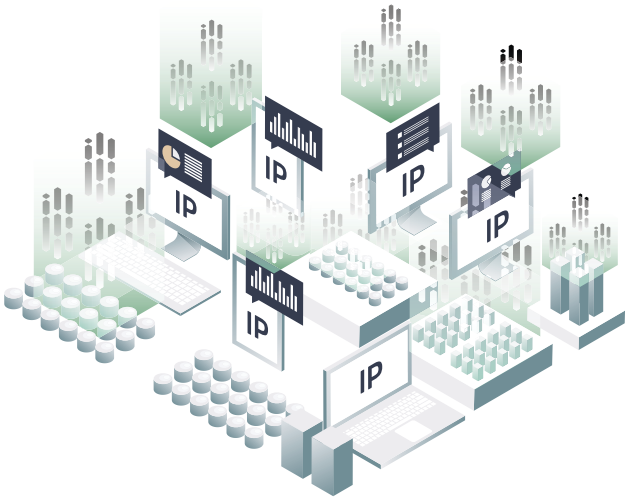


ソリューション

- UPASは、ADアカウントをコンピュータにバインドし、ローカルログインを禁止し、プライベートドメインの引き出しを禁止し、特定のADアカウントを使用して特定のPCにログインするようにし、AD情報とデバイス情報を統合してアカウント使用記録を提供することで、すべてのコンピュータにエンタープライズセキュリティポリシーへの準拠を強制できる。

- 共有フォルダの場合、追加、変更、削除などのファイル変更を監視し、潜在的なセキュリティリスクを適時に検出して、企業データのセキュリティを保護できる。

- SIDリピートイベント、特権アカウントのログインおよびログアウトレコード、およびローカルアカウントを検出することで、管理者は異常な動作を検出して対応し、ADドメインに追加する必要があるすべてのデバイスを制御することができる。



IPAM IP アドレス管理

IP管理が容易で便利

ARP

適用シーン

企業や政府機関の拡大に伴い、それらが持つ巨大で複雑なネットワークリソースを効果的に管理および適用する必要がある。

1. IPアドレスの混乱による管理上のトラブルは、通常の運用に影響を与えるだけでなく、管理担当者が基本的なメンテナンスに費やす時間を大幅に増加させる。

2. インシデントが発生すると、MIS担当者は問題を見つけるのに時間と労力がかかり、最良の救助の機会を逃す。

ソリューション

- IPAMは、デバイス属性を自動的に識別し、IP/MAC情報を表示でき、接続されているすべてのデバイスのIP/MAC/DHCPセグメント/コンピューター名/ハードウェアフィンガープリント(UUID)間で複数のバインディングを実行できる複数のバインディング機能を備えており、IPの保護、保持、リサイクルを実現し、IPの競合やMACの偽造を防ぐ。

- UPAS は、関連する機能を1つのページで管理でき、さまざまなイントラネット統計リストを生成して、管理者がイントラネット資産とIPの使用状況を完全に把握し、管理者がイントラネット IP リソースとデバイスをタイムリーに管理できるように支援できる。

MDM モバイルデバイス管理

モバイルデバイスと機密データを安全に保つ

MDM

適用シーン

スマートフォンやタブレットなどのデバイスが普及し、ネットワーク環境が使用権はもっと問題になるはず。

1. 厳しい規制のないモバイルデバイスのアプリケーション開発のシステムのオープン性と利便性は、情報セキュリティリスクを警告し、データ漏洩のリスクを高める。

2. BYOD/COPEはどのように管理基準を開発しているか?

ソリューション

- MDMは、モバイルデバイスが組織のネットワークに入ったときにコンプライアンスチェックとID認識を実行し、グループ設定に従って制御ポリシーを適用することで、組織の情報セキュリティを厳密に保護するネットワークアクセス制御テクノロジーを組み合わせている。

- 管理者は、Wi-Fi接続設定、カメラの無効化、パスワード強度設定のロック解除、スクリーンショット設定の無効化など、フィールドに応じて管理ポリシーを策定でき、管理インターフェイスはデバイスをリモートで制御して、画面のロック、エージェントのアンインストール、設定の初期化、ロック解除パスワードの設定とクリア、呼び出し音のミュートとプッシュメッセージも実行できる。

- iOS/Android操作システムをサポートする。



ZERO TRUST

TRUST UPAS

UPAS 導入効果



NAC – イントラネット境界保護の確立

安全性と運用上のリスクを効果的に低減する。データ漏洩やウイルストロイの木馬の侵入など、プライベートデバイスによって引き起こされるリスクを防ぐ。



資産インベントリ – 機器の可視性の向上

IoT資産のインベントリを確立して、デバイスの可視性を高め、アイドル状態のデバイスを回避する。 また、デバイス属性、OS、場所、ユーザー情報などのイントラネットデバイス データも識別する。



ルール適合検査-ネットワーク内の適合率をアップ

AD管理完備率

Windows Patch 更新率

ウイルス対策ソフトのインストール率、更新率

ソフトウェアのインストール率と、インストールする必要があるソフトウェアの更新率



ソフトウェアおよびハードウェア管理ポリシーの完備

禁止されているソフトウェアの管理と違法な著作権チェックにより、メーカーによる違法な著作権の主張を防ぎ、USB外部デバイスの管理を制御してWi-Fiの使用を制限し、1つのデバイスが2つのネットワークで動作するのを防ぐ。



IP管理プロセスを完備する

IP回収、IP保留、IP保護、IP使用記録、IP構成リスト、シャットダウン済みレポート、シャットダウンしていないレポート。



規制や情報セキュリティ監査の通過を支援する

『ISO27001』、『NIST CSF』、『情報セキュリティ管理法』、サプライチェーンセキュリティ検査などの監査基準を遵守する。

台湾を拠点に・グローバルに活動する
豊富な実績・好評を証拠に



30年

台湾オリジナルメーカー

自社でのプロフェッショナルな
研究開発経験

7つの

産業への応用

政府｜テクノロジー｜製造｜金融｜医療
教育｜一般企業｜重要インフラ

3800+

顧客による証明と信頼

100+

10000 IP以上の
大規模な企業

アメリカ・シリコンバレーのジャーナル《APAC CIO Outlook》にて評価を獲得

Top 10 Cyber Security Solutions Providers in APAC 2023
Top 5 Cyber Security Solutions Providers in Taiwan 2023

UPAS

ZERO TRUST ARCHITECTURE

最適なセキュリティ管理ソリューションの詳細をご覧ください

Website

Facebook

LINE

Medium

LinkedIn