



- APAC CIO Outlook -
TOP 5 / TOP 10
Cyber Security Solutions Provider
in Taiwan / APAC



UPAS

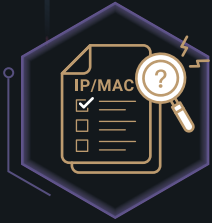
ZERO TRUST ARCHITECTURE

半導体サプライチェーンの情報セキュリティ弾力性を全面的に向上させる
IT/OTゼロトラストを実践し、SEMI E187コンプライアンスを実現する

FAB

FAB半導体/製造業のコンプライアンスソリューション

近年の多発する情報セキュリティ事件を鑑み、ここ数年、
国際の有名半導体メーカーの多くが操業停止を余儀なくされており、
最近では多くの業界企業の顧客情報の漏洩が発生している……



違法なデバイスをブロックするのは簡単ではない

ホホワイトリスト管理ポリシーは、イントラネットデバイス資産の数を明確に把握し、不正アクセスデバイスのネットワークをブロックする。



Agentの展開率が低い

Agentのインストールリスト管理、Agentの展開率を明確に把握し、行き止まりの防御をゼロにする。



設備の安全性が不足

Windows OS Patch、ウイルス対策バージョンなどの更新状態効果的に把握し、情報セキュリティ防御を向上させる。



不十分なソフトウェア管理

インストールすべきソフトウェアのポリシー、無効されているソフトウェア、ソフトウェアの著作権を管理し、脆弱性にタイムリーにパッチを適用して、リスク、損害、損失を軽減する。

UPAS 適用フィールド

Agentless

・ 完全な資産インベントリとデバイスアクセス管理 ・

UPASは、特許取得済みの独自のNAPテクノロジーを使用し、マルチVLAN環境をサポートし、Agentをインストールせずに100%の情報資産インベントリを実践でき、違法なデバイスを自動的にブロックし、リガイドページアラームを提供して、イントラネットに接続されているすべてのデバイスが安全でコンプライアンスに準拠していることを保証できる。

・ 自動管理、IoTデバイスの明確な把握 ・

OUI、相互接続されたDB、NMAP、DHCPパケット解析などの技術を用いて動的な資産属性収集し、IoT設備資産を識別する

Agent

・ サプライチェーン監査コンプライアンスは問題ない ・

設備の安全コンプライアンスを全面的に向上させ、Windows Patch更新率、ウイルス対策インストール更新率、インストールすべきソフトウェアコンプライアンス、ソフトウェア使用禁止政策及び違法ソフトウェア著作権検査などを行う。コンプライアンス「ISO 27001」、「NIST CSF」、「SEMI E 187」、サプライチェーン安全検査などの監査基準に協力する。

・ 複雑な工場環境に適応するクロスプラットフォームAgent ・

UPAS AgentはWindows、LINUX、MacOS、Android、iosなどのオペレーティングシステムをサポートし、工場の多様な作業環境を満たし、設備の納管率を高める。

UPAS を選択する必要があります

設置とセットアップが簡単、自動設計

特許取得済みのNAPテクノロジーにより、展開構造がシンプルになり、管理プロセスが自動化され、デバイスがホホワイトリストに自動的に追加され ➡ グループが自動的に割り当てられ ➡ Agentが自動的にディスプレイパッチされ ➡ グループポリシーに従ってコンプライアンスチェック ➡ 自動分離 ➡ 自動パッチ適用 ➡ コンプライアンス後にデバイスのネットワーク接続の復元を確保する
全面的なセキュリティチェック：
Windows Patchの更新、ウイルス対策ソフトウェアのインストール、ソフトウェアのインストール、無効化ソフトウェアのチェック、USB管理、ソフトウェア脆弱性アップデートなどが含まれる。

生産が中断 され確認されました。

違反が発生すると、従来のNACアーキテクチャでは、違法な機器の接続機能を直接ブロックし、工場エリアでの業務中断を引き起こし、生産ラインの稼働に影響を与え、莫大なビジネス損失を引き起こす恐れがある。

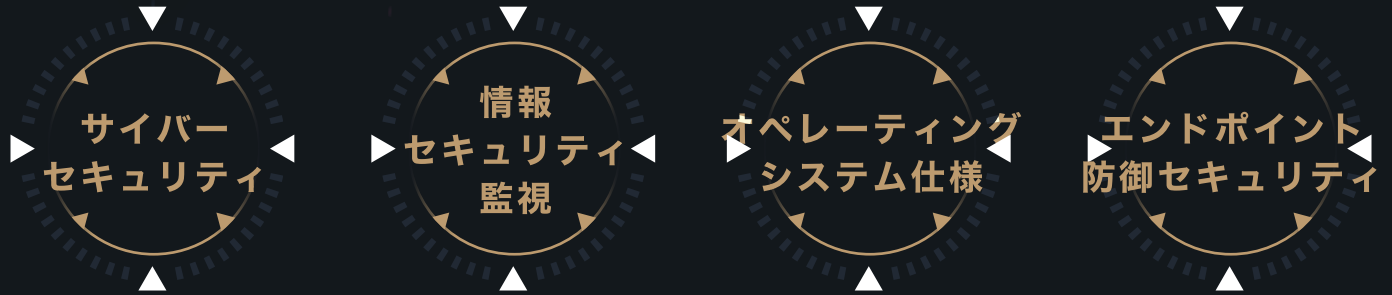
UPASは自社システムの安全性を非常に重視しており、エラー防止設計と故障ByPassを使用して、生産ラインが中断することなく稼働し続けることを保証する。

端末機器適合率の向上

UPASシステムは、NAPテクノロジーを使用して、イントラネットの情報資産リストを100%取得し、IP/MAC、デバイス属性、コンピュータ名、オペレーティングシステムなどの情報を識別する。Agent展開リストと相互比較して、網をすり抜ける魚の数を減らし、Agent展開率を強化する。機器端末のコンプライアンス率は98%に達する。

SEMI E187はどのように対応するか

2022年1月、台湾が主導した初の芝半導体製造ライン設備の情報セキュリティ標準仕様（SEMI E187）がSEMIの公式サイトで正式に発表され、規格策定の4つのポイントは以下の通り：



ZERO TRUST ARCHITECTURE 実践IT、OTゼロトラスト

UPAS 半導体供給チェーンのサイバーセキュリティと耐久性を向上させる

サイバーセキュリティ

SEMI E187

- ・ 設備の完全なインベントリし、識別
- ・ ネットワークアクセス制御
- ・ IPセグメント管理
- ・ IP保護、保持、回収
- ・ IP競合やMAC不正アクセスの防止

情報セキュリティ監視

SEMI E187

- ・ 24/7監視を継続
- ・ 情報セキュリティ事件、設備状態ログの生成
- ・ 多角度可視化データ提示

オペレーティングシステム仕様

SEMI E187

- ・ オペレーティングシステムバージョン管理
- ・ EOLオペレーティングシステムの採用を避ける
- ・ Windowsが定期的に更新されていることを確認する
- ・ ウイルス対策ソフトウェアウイルスコードの更新を確実にする

ネットワークにアクセスするすべてのデバイスの安全性とルール準拠を確保

設備コンプライアンスチェック

ID認証

エンドポイント防御セキュリティ

SEMI E187

- ・ ソフトウェアの無効化/ブロッキング
- ・ グループコンプライアンスの検出/適用
- ・ ソフトウェアの脆弱性のパッチ/デイスパッチ
- ・ リモートメンテナンス

プロで誠実 信頼できる

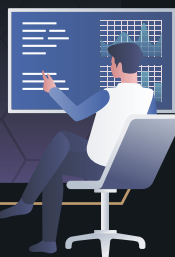
台湾の半導体大手メーカー 情報責任者

「まず、UPASがいち早く導入され、さらにUPASはイントラネット情報を効果的に統合でき、最高情報セキュリティ責任者に報告する際にイントラネットの運営方針を明示できるため、組織は脅威やリスクに効果的に集中することができます」



中央行政機関 情報スペシャリスト

「公務員のネットワーク機器やアクセス権が管理されており、ソフトウェアの無効化やUSBアクセスなど、デバイスごとに多くの制限がある。UPASは、限られた管理方法で私たちのニーズに応えることができる」



台湾の有名銀行 情報責任者

「政府には厳格な監査基準があり、各会社にはISO 27001やNIST CSFなどの準拠が必要な管理メカニズムがあり、UPASは管理責任を自動的に解決し、30種類以上のレポートを通じて監査の改善を支援する」



3800+

中央省庁、警察、防衛、地方政府、金融機関、半導体、テクノロジー産業、基幹インフラ、教育機関、小売業、一般企業などのお客様から信頼され、お客様のゼロトラストアーキテクチャを確立し、強力な情報セキュリティ防御を構築することに専門的かつ誠実である。

100+

10,000以上のIP数を持つ多国籍企業

米国のシリコンバレージャーナル『APAC CIO Outlook』を受賞

2023 TOP5 Cyber Security Solutions Provider in Taiwan 台湾情報セキュリティソリューション

2023 TOP10 Cyber Security Solutions Provider in APAC アジア太平洋情報セキュリティソリューション

UPAS

ZERO TRUST ARCHITECTURE

