

QNAPによるIT/OT セキュリティの強化

ストレージから多層防御まで、無停止運用を実現



IT/OTセキュリティは一步ずつ、着実かつ適切に

現代の企業では、ITシステムとOT(Operational Technology)環境が一体化しており、サイバー脅威の範囲はオフィスネットワークから生産現場まで拡大しています。多くの製造業にとって、OTセキュリティの実践は、リソースの問題ではなく、むしろ手法と実装の課題であることが多いのです。

QNAPは、企業がサイバーセキュリティを導入・実装する際に直面する、現実的な課題を深く理解しています。そのため、単発的なアプローチではなく、データの保存から保護までを一貫して「見えて・管理できて・適用できる」セキュリティ基盤の構築を提唱しています。これにより、中小企業もIT/OTセキュリティの実現に向けて、段階的かつ着実に一步一步進むことができます。

80%

の製造業企業が、2024年にセキュリティインシデントまたは侵害の増加を経験しました。

45%

が、こうした脅威に対処するための十分な備えがあると認識しました。

60%

が、OTセキュリティの複雑さを最大の懸念事項として挙げました。

情報源：

<https://www.telstrainternational.com/en/news-research/research/secure-manufacturing-the-challenges-of-IT-OT-convergence>

<https://www.paloaltonetworks.com/blog/network-security/state-of-ot-security-2024/>



QNAPは、ストレージ技術を強靱なサイバー防御力へと転換し、企業のIT/OTセキュリティの最前線を堅牢に守る

QNAPは、ストレージ、ネットワーキング、脅威検知、オフラインバックアップ、リモートアクセスなど、多岐にわたるソリューションを提供しています。

QNAPソリューションは、NIST CSFやIEC 62443といった主要なOTサイバーセキュリティフレームワークに準拠し、重要インフラ産業のセキュリティとコンプライアンスの確保を支援します。QNAPは、IT/OT環境全体で、可視性、レジリエンス（回復力）、そして復旧性を実現するセキュリティアーキテクチャの構築を支援します。





確かな指針(ブループリント)が 導くサイバーセキュリティ

NIST CSF 2.0に基づくIT/OT防御の段階的構築

- NISTサイバーセキュリティフレームワーク(CSF)は、企業、製造業、そして重要インフラで広く採用されています。2024年版のNIST CSF 2.0は、OT環境への実践的な適用性がさらに強化しています。
- 6つの主要機能(特定、防御、検知、対応、復旧、統治)が、企業に明確なサイバーセキュリティの指針(ブループリント)を提供します。
- このフレームワークは、多層防御、資産の可視化、インシデント対応、復旧能力を重視しており、QNAPのソリューションアーキテクチャと高いレベルで整合しています。
- 中小企業においては、NIST CSFは単なる標準にとどまらず、フェーズごとの導入のための実践的なロードマップとなります。
- QNAPは、NIST CSF 2.0を基盤として、NAS、ネットワーク機器、セキュリティアプリケーションを統合し、企業の実現可能なIT/OTサイバーセキュリティ防御構築を支援します。



標準から実践へ

QNAPソリューションは、NIST CSF 2.0の主要機能を完全にカバー

- 全製品ラインでサポート対応
- 特定の製品モデルのみサポート(全シリーズ対応ではありません)
- 非対応

機能力カテゴリー	課題	解決策	NAS	QHora/ルーター	ADRAスイッチ	QSWマネージドスイッチ
特定	多様なIT/OT環境デバイスにおける、資産インベントリの一元化欠如	デバイスの一元管理	●	●	●	●
		インベントリの可視化	●	●	●	●
		クラウドモニタリング	●	●	—	●
防御	レガシーの制御システムでは、最新の脅威に対抗できない	データ暗号化	●	●	—	—
		多層的なアクセス制御	●	●	—	●
		ネットワークセグメンテーション	●	●	●	●
検知	ネットワーク異常検知 IT/OT 環境での異常に対するリアルタイムモニタリングがない	デバイス異常の検出	●	●	●	●
		ログイン異常の検出	●	●	●	●
		ネットワーク異常の検出	●	●	●	●
対応	インシデント発生時の即時通知/レポート機能がない	即時アラート	●	●	●	●
		リモートアクセス	●	●	●	●
		クラウド管理	●	●	—	●
復旧	自動的なバックアップ機構がなく、ディザスタリカバリが困難	バックアップ機構	●	●	—	●
		データ整合性	●	—	—	—
		ディザスタリカバリ	●	—	—	—



ストレージからネットワーキングまで、 QNAPがIT/OTサイバーセキュリティを強化





NAS

IT/OT環境のための主要なストレージ、バックアップ、アプリケーション統合プラットフォーム

- AI分析、仮想化、QuFirewall、AMIZcloudの管理をサポート
- 一部のモデルは、過酷な環境に適した産業グレード設計のモデルをご用意(デスクトップ、ラックマウント、ウォールマウント、デュアル電源)を採用

エンタープライズクラスQuTS hero NAS：

- 信頼性の高いファイルストレージとバックアップ(スナップショット、イミュータブルバックアップ、WORM機能など)
- ダウンタイムリスクを最小化する高可用性(HA)アーキテクチャ



QHoraルーター

IT/OTクロスドメインのネットワークセキュリティと相互接続防御を実現

- ポリシーベース/マイクロセグメンテーションルーティング、L3~L7ファイアウォール、DPIパケットインスペクション、IPS侵入防御
- Qbelt(DTLS+AES-256)、WireGuard、OpenVPNによる安全なエンドツーエンド伝送をサポート
- WPA/WPA2/WPA3 Wi-Fiによる安全な無線アクセス
- Airgap+隔離バックアップによるランサムウェアの事前防止


QuWAN SD-WAN :

- マルチサイトの相互接続と一元管理
- WAN最適化と自動フェイルオーバーにより安定したリモート接続を実現

ADRA NDRスイッチ

悪意のあるトラフィックや異常な挙動に対するIT/OTネットワークのリアルタイム防御

- 数百台のデバイスに対応するAI異常検知、内部・外部の脅威を早期に検知
- 高度なトラフィック分析により攻撃を正確に遮断する、自動化されたインシデント対応と修復
- ラテラルムーブメントの防止、感染デバイスの隔離、不審なアクティビティのブロック
- SOC/SIEM統合により、NAS、PC、プリンタ、PoEデバイスを保護し、包括的なネットワーク防御体制を構築



QSWマネージドスイッチ

IT/OTシステム向けの長距離、広帯域、低遅延のバックボーン接続を提供

- 2.5GbE/10GbE/25GbE/100GbEファイバーおよび銅線接続、企業のコア・エッジネットワークに最適
- VLANおよびQoS管理により、さまざまなアプリケーションのトラフィックを最適化
- AMIZcloudによる一元監視と管理をサポート
- 一部のモデルは、デバイスへの電力供給を行うPoE機能を搭載し、過酷な環境向けに設計

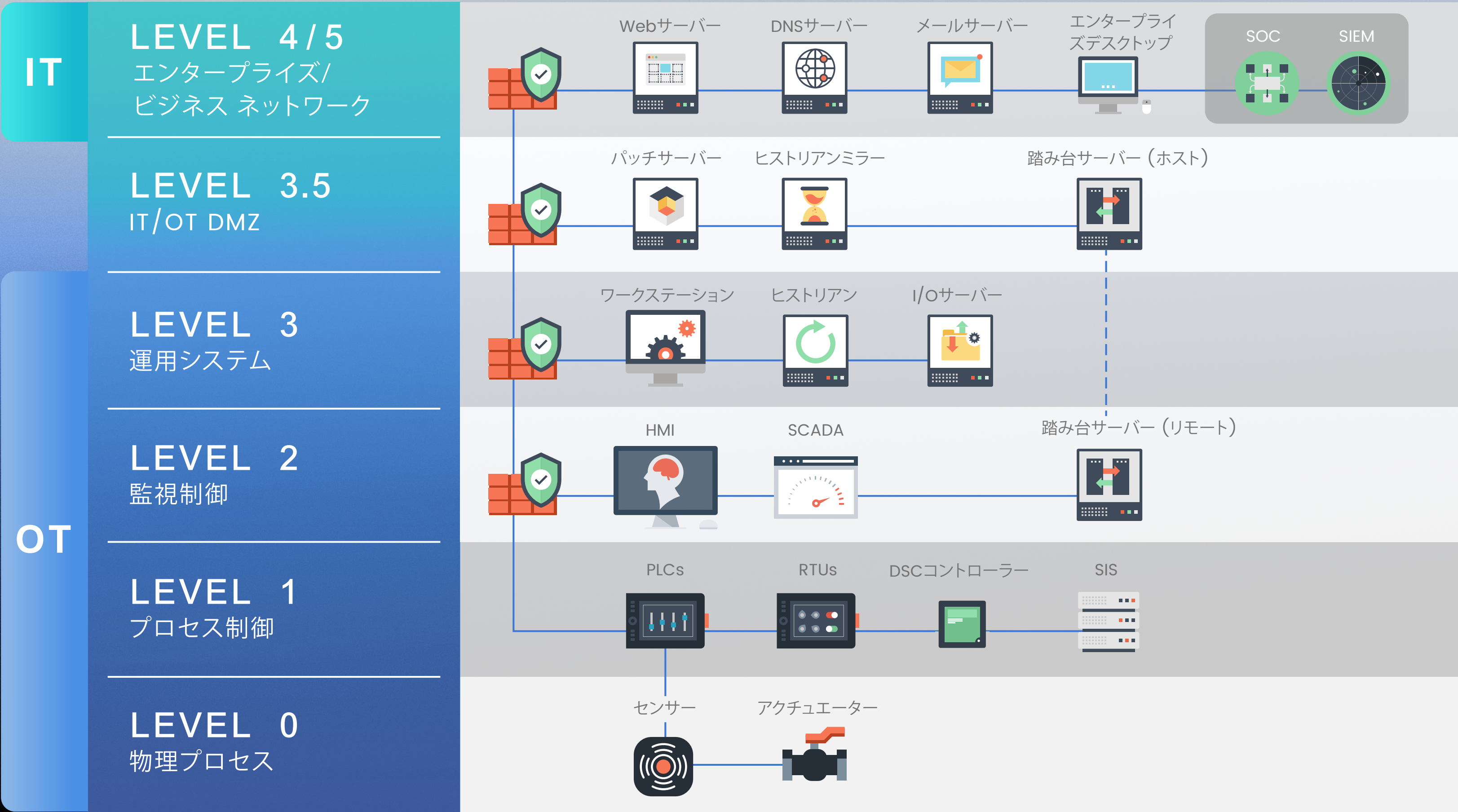
エンタープライズクラスのL3スイッチ：

- 内蔵のMC-LAG HAが24時間365日の無停止稼働を実現
- PTP IEEE ITU-T G.8273.3 Class Aによる100ns未満の時刻同期で、OT/産業用制御機器が要求する高精度に対応

Purdueモデルに基づく構築 — IT/OT運用の包括的な防御

企業は、国際的に認められているPurdueモデル*を階層化された産業用制御ネットワークアーキテクチャとして採用できます。ITとOTそれぞれの役割と境界を明確に定義することで、このモデルが強靱なサイバーセキュリティ防御体制の確立と、ドメイン間の連携を可能にする強固な基盤を提供します。

*階層化された産業用制御ネットワークに広く用いられるフレームワークで、ISA/IEC 62443およびNIST 800-82標準に適用されています。



QNAPがIT/OT融合層のサイバーセキュリティを守る

エンタープライズネットワーク

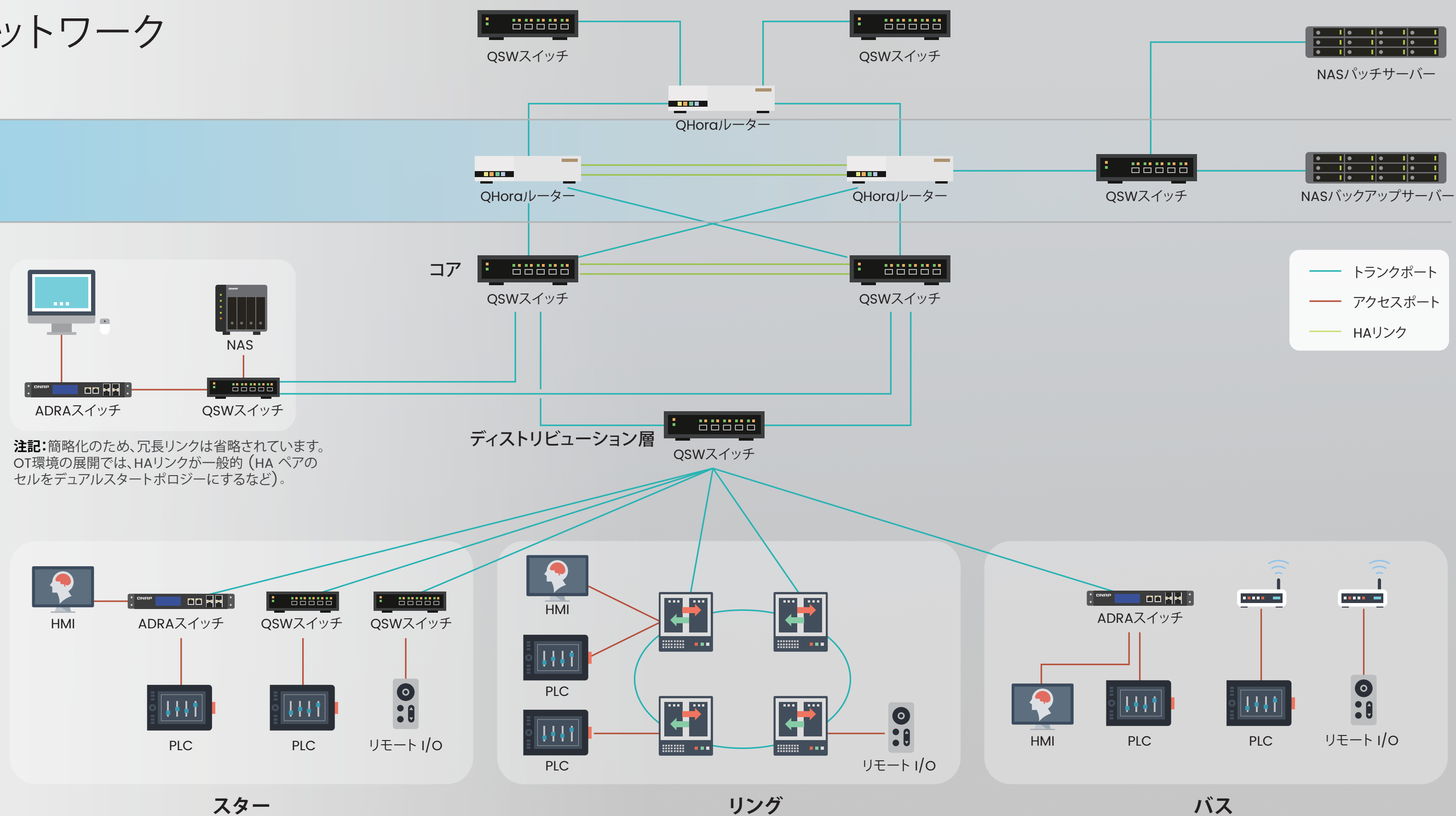
DMZ

▲ LEVEL 3.5

▼ LEVEL 0-3

OTネットワーク

▼ LEVEL 0-2



NIST CSF 2.0の主要5機能 の詳細解説 — 実践的なIT/ OTサイバーセキュリティ 防御の構築



特定

資産の可視化からユーザーの認識の向上まで — IT/OTセキュリティの基盤の構築

サイバーセキュリティの第一歩は、「何を保有しているかを知ること」です。しかし実際には、多くの企業が、資産管理の分断化、アカウントの分散、複雑な接続環境といった課題に直面しています。QNAPは、人、デバイス、ネットワーク、データにわたる識別とアクセス管理を実現することで、組織の効果的なリスク管理基盤の構築を支援します。

資産台帳とデバイスの一元管理

- QuWAN Orchestrator：SD-WANクラウド
オーケストレーションシステムにより、QNAPデバイスが配置された企業ネットワークセグメントのIPアドレス、モデル、デバイス状態を自動認識し、一元管理を実現します。
- ADRA NDRスイッチのデバイスインベントリ：パケット分析を通じて、ネットワークに接続されているデバイスのMAC アドレス、IP アドレス、ホスト名、状態などを自動認識します。

ディザスタリカバリ機能：

- スナップショットにより、システムを正常な状態に迅速に復元でき、ダウンタイムを最小化し、人的エラーや悪意のある攻撃によるリスクを軽減します。

包括的なデータバックアップ・復旧ソリューション：

- QNAPは、Windows® PC、サーバー、SaaSクラウドデータ、仮想マシン(VM)を包括するバックアップソリューションを提供し、データ損失リスクを最小化し、業務継続性を確保します。



防御

多層防御機構：システム、データ、ネットワークを包括的に保護

OT環境では、最新の攻撃に対抗するためには、単一の防御策に頼るだけでは不十分です。QNAPは、システムからデータ、内部ネットワークからネットワーク管理までを網羅する多層防御機構を提供し、インフラのレジリエンス強化と、途切れることのない生産・業務の継続を実現します。

NASシステムの保護：

多要素認証(MFA)と組み込みファイアウォールで、不正アクセスや悪意のある操作を防止し、NASの安定性と可用性を確保します。

データセキュリティ&イミュータブルストレージ：

AES-256暗号化とイミュータブルストレージ(WORM、オブジェクトロック)により、データの整合性を保護します。Airgap+隔離バックアップと組み合わせることで、ランサムウェアからデータを保護し、バックアップデバイスのネットワーク曝露時間を最小限に抑えます。

内部脅威の隔離：

ADRA NDRが悪意のあるOTネットワークトラフィックを迅速に検知・フィルタリングし、ラテラルムーブメントやマルウェアの拡散を監視。攻撃の拡大や機密データの外部流出を効果的に阻止します。

ネットワークセグメンテーション&アクセス制御：

QNAPスイッチは、VLANとACLを活用して生産・監視・管理ネットワークをセグメント化し、クロスドメインのリスクを低減してセキュアな隔離を強化します。



検知

監視システムを導入し、ネットワークトラフィックとユーザー動作を分析

OTネットワークの異常トラフィックや行動をリアルタイムで監視できないと、脅威が温存され、深刻な被害につながります。QNAPは、システム、ネットワーク、トラフィックの振る舞いを包括的にリアルタイム監視し、異常の迅速な検知、対応時間の短縮、生産・業務の安全確保を実現します。

システムと稼働状況の監視：

NASは、システム状態、ファイルアクティビティ、アクセスログを継続的に監視し、不正アクセスや異常ログイン、疑わしい行動を迅速に特定します。AMIZcloudによる一元管理とQuWANオーケストレーションにより、管理者は全QNAPデバイスの稼働状況とリスクを完全に可視化・把握できます。

境界ネットワークの脅威検出：

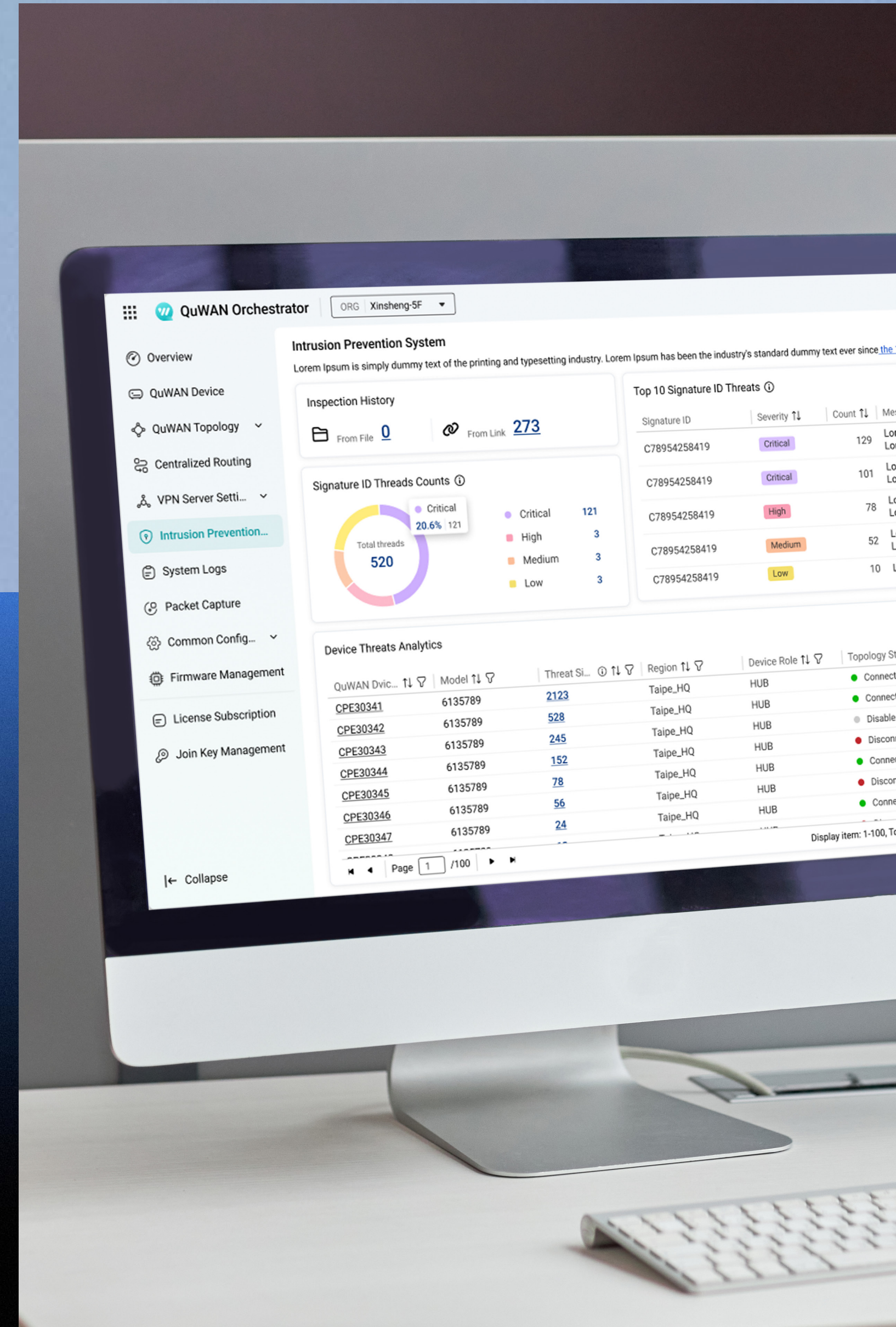
QHoraルーターは、侵入防止システム(IPS)とディープパケットインスペクション機能を備え、悪意のあるトラフィックを特定・ブロックすることで、OT/IT境界のセキュリティを強化します。

マルウェアの検出と駆除：

NAS上で定期的にアンチウイルススキャンを実施し、悪意のあるソフトウェアを検出・排除します。QNAPは、定期的に更新されるウイルス定義により、常に最新の保護を提供します。さらに、ADRA NDR Trapがマルウェアの早期検出とアラートを提供し、プロアクティブな防御を支援します。

内部ネットワークの行動分析： コントロール：

ADRA NDRは、OTトラフィックと内部行動のディープ分析を実施し、継続的な監視により不審なアクティビティを自動検出。ラテラルムーブメントによる脅威の伝播を阻止します。



対応

リアルタイムアラート、封じ込め、リモート更新で脅威を効果的に阻止

OT環境において、セキュリティインシデントへの対応の遅れや不手際は、生産ラインの停止や重大な事故につながりかねません。

QNAPは、即時通知と迅速な封じ込め機能を提供し、脅威の拡散前に食い止めます。

リアルタイムイベント通知：監視：

通知センターは、異常イベントを複数のチャネル(メール、SMS、Syslog、Webhookなど)に同時にプッシュ通知し、セキュリティチームや現場スタッフへの即時情報伝達を実現します。

迅速な脅威の封じ込め：

インシデント発生時、ADRA NDRスイッチは脅威の発生源を迅速に特定し、侵害されたデバイスを隔離することで、悪意のあるトラフィックの拡散を阻止します。これにより、他のOTシステムの継続稼働を確保し、全体的な影響を最小化します。

リモートデバイスアップデート：

AMIZcloudとQuWAN SD-WANを利用し、管理者はQNAPデバイスをリモートから管理し、シャットダウン、再起動、システムアップデートといった操作を実行できます。これにより、パッチ展開を加速し、脆弱性を速やかに解消することで、人的エラーのリスクを低減します。

マルウェアの駆除：

マルウェアの定期駆除機能により、感染プロセスは直ちに強制終了され、システムやデータへの被害拡大を防止します。



復旧

ディザスタリカバリとデータ保全バックアップ アーキテクチャの導入

OT環境の核となる目標は、「無停止稼働」です。

QNAPは、迅速なディザスタリカバリとデータ整合性の維持に注力し、通常運用への早期復旧を実現します。

高可用性バックアップアーキテクチャ (サーバー・ネットワーク)：

NAS HA(アクティブ/パッシブ高可用性)とスイッチMC-LAGにより、障害発生時にシステムが自動的にバックアップ機器へフェイルオーバーし、事業継続性を維持し、OT制御システムの中断を防止します。

ディザスタリカバリ機能：

スナップショットにより、システムを正常な状態に迅速に復元でき、ダウンタイムを最小化し、人的エラーや悪意のある攻撃によるリスクを軽減します。

高可用性バックアップアーキテクチャ (複数拠点)：

QuWANを組み合わせたQHoraルーターが、OT環境における複数拠点WANバックアップを実現します。クロスサイトのフェイルオーバー機能が、代替のノードおよび経路への自動切り替えを実行します。デュアルWAN構成により、ローカルからクラウドへのリンクがシームレスにフェイルオーバーし、リモート/クラウドサービスの無停止稼働を実現します。

包括的なデータバックアップ・復旧 ソリューション：

QNAPは、Windows® PC、サーバー、SaaSクラウドデータ、仮想マシン(VM)を包括するバックアップソリューションを提供し、データ損失リスクを最小化し、業務継続性を確保します。



サイバーセキュリティは、すべてを一度に達成する必要はありません。 しかし、必ず始めなければなりません。

QNAPのソリューションにより、IT/OTのセキュリティ変革を自信を持って推進し、ストレージからサイバーセキュリティまで完全な保護を提供し、レジリエンスの高い業務運用を実現します。

デバイスからアクセス制御まで —
企業資産とユーザー行動の完全な可視化

展開から脅威の緩和まで —
セキュリティ防御と運用効率を効果的に統合

脅威の防止から復旧まで —
業務の安定運用を包括的に保護



詳細は

QNAPは、お客様の既存インフラを基盤として、IT/OTセキュリティ実現への第一歩を支援します。

お客様の環境に最適なソリューションをお探しですか？
導入支援や技術相談をご希望ですか？

お問い合わせ



QNAP株式会社

Tokyo
Email: jpsales@qnap.com
Tel: +81-3-5901-9735

QNAP Systems, Inc.

New Taipei City
Email: sales@qnap.com
Tel: +886 2 2641 2000

QNAP Inc. (USA)

Pomona CA
Email: usasales@qnap.com
Tel: +1-909-595-2782

QNAP Inc. (Canada)

Markham, Ontario
Email: canadasales@qnap.com
Tel: +1-905-947-1000

QNAP GmbH (Germany)

Willich
Email: desales@qnap.com
Tel: +49-2154-88428-0

QNAP SRL (Italy)

Roma
Email: eusales@qnap.com
Tel: +39-(0)687-738456

QNAP UK Limited

Swindon
Email: uksales@qnap.com
Tel: +44-(0)333-344-2522

QNAP Korea

Seoul
Email: krsales@qnap.com

