EdgeAI Station セキュリティガイド

> **セキュリティガイドライン**
> バージョン: 1.1
> 日付: 2025 年 10 月 31 日
> 作成者: Edgematrix
> モデル: EX3 / EX5 / EX7
> 機密レベル: 一般使用

凡例

> ℹ️ **注記**: 追加の有用な情報、ヒント、または説明を提供します。
>
> ⚠️ **警告**: 潜在的な問題を回避するために注意深い配慮が必要な注意点を示します。
>
> 🚨 **重要**: 重要な情報を示します。これを無視すると、深刻な問題（システム障害、データ損失、セキュリティ侵害など）を引き起こす可能性があります。

---

1. ファイアウォール設定

1.1. 統合と使用のために開放されたポート

開放されている外部ポートのリスト：

ポート	プロトコル	目的
443	HTTPS/WSS	セキュア Web UI および Websocket API アクセス
80	HTTP	互換性のため（HTTPS への自動リダイレクト）
123	UDP (NTP)	時刻同期

> ⚠️ **警告**: 現在フィルタリングされていない他のポートを通じたアクセスは提供されていません。デフォルトファイアウォールルールの強化は将来のバージョンに含まれる可能性があります。

1.2. Edgematrix サポートとフィルタリングされたサービス用の予約ポート

非公開ポートのリスト：

ポート	プロトコル	使用目的
22	SSH	Edgematrix リモートサポート（制限アクセス）
9100	HTTP	Node Exporter（メトリクス収集、内部専用 | フィルタリング済み）
9090	HTTP	Prometheus（ローカルメトリクス統合 | フィルタリング済み）

1.3. 内部マイクロサービスポート

これらのポートは、EdgeAI Station 内でのサービス間通信用です。外部からはアクセスできず、マイクロサービスの内部 DNS 名を使用してのみ到達できます。

その主な目的は、Node-RED などのコンポーネントがアクセストークンなどの外部認証メカニズムを必要とせずに内部 API と相互作用できるようにすることです。

例:

```
http://ms3_videostreaming:8000/api/stream/status
```

これは、Node-RED 内から ms3 API と通信してサービスにアクセスするために使用されます。

---

2. ネットワーク管理

2.1. ネットワーク統合

> 🚨 **重要**: EdgeAI Station を直接パブリックインターネットに公開しないでください。そうすることで、不正アクセス、データ侵害、サービス中断のリスクが大幅に増加します。

EdgeAI Station は、ファイアウォール、NAT ゲートウェイ、VPN の背後など、保護されたプライベートネットワーク内で動作するように設計されています。パブリックアクセスは、以下を含むより強力なセキュリティインフラストラクチャ設計を考慮せずに有効にすべきではありません：

- **厳格なファイアウォールルールと IP ホワイトリスト**
- **すべての公開サービスに対する署名済み TLS 暗号化プロキシトラフィック**
- **リモート操作のための VPN またはゼロトラストネットワークアクセス（ZTNA）メカニズム**
- **トレーサビリティのための外部到達可能エンドポイントの監査ログと監視**

2.2. Ethernet カードトラフィック分離

デフォルトでは、IP 転送が有効になっており（`ip_forward = true`）、ネットワークインターフェース間（例：eth0 と eth1 の間）でのトラフィックルーティングが可能です。

セキュリティ設計のこの部分を改善し、インターフェース間の不要な通信を防ぐ必要がある場合は、各 Ethernet ポートでネットワークトラフィックを分離するために**VLAN**を使用することをお勧めします。

この設定により、例えば、カメラトラフィックが EdgeAI Station の制御または管理トラフィックと分離されることが保証されます。

---

3. Edgematrix リモートメンテナンスサポート

3.1. パブリックリモートアクセス

> 🚨 **重要**: リモートアクセスは、お客様の明示的な同意がある場合にのみ確立でき、お客様が手動で開始する必要があります。Edgematrix は独立してリモート接続を開始することはできません。このアクセスは厳密に時間制限があり、リモートメンテナンスとサポート目的のためのみに意図されています。

EdgeAI Station へのパブリックリモートアクセスは、Edgematrix の AWS インフラストラクチャを通じて安全に管理およびプロビジョニングされる**ngrok トンネル**を介して有効になります。

この設定により、Edgematrix サポートエンジニアは、顧客デバイスに確立されたリバーストンネルを通じてデバイスにアクセスできます。リモートアクセストンネルは：

- ✅ **署名済み証明書を介した HTTPS 経由で暗号化**
- ✅ **Edgematrix バックエンドを通じて認証**
- ✅ **時間制限があり、オンデマンドのみ**

3.2. セッション管理

各リモートアクセスセッションには**デフォルト最大持続時間 6 時間**があります。

この期間が経過すると：

- ngrok トンネルが自動的に終了します
- 開いているセッションは正常に切断されます
- 新しいアクセスには再認証とユーザー承認が必要です

セキュリティを維持するため、セッションは期限切れ前に Edgematrix バックエンドまたはユーザーが直接 Web アプリケーションから手動で取り消すことができます。

---

4. ユーザーアカウントとロールベースアクセス制御

4.1. ユーザーアカウント

> 🚨 **重要**: デバイス初期化後、Web アプリケーションアカウントとリカバリアカウントの両方について**デフォルトパスワードを変更してください**（クイックスタートガイド -> 4.3. リカバリアカウント参照）。

現在、**3 つの事前定義されたアカウント**のみが利用可能です：

ユーザー	グループ	デバイスアクセス権限
`admin`	admin	すべてのデバイスページへの完全アクセス
`operator`	ops	デバイス情報、メディア、記録、パイプラインページなどへのアクセス、EdgeAI Station リソースの管理
`guest`	guest	ダッシュボードページのみにアクセス可能

4.2. アクセストークン（サービストークン）

サービストークンのアクセス範囲は以下の通りです：

エリア	m2m グループのアクセスレベル
監視・メトリクス	システム監視データとメトリクス API（未文書化）にアクセス可能
ログ	システムログ API（未文書化）にアクセス可能

エリア	m2m グループのアクセスレベル
ビデオストリーミング	ビデオストリーミング API にアクセス可能
デバイス管理	デバイス設定とデバイス情報 API を管理可能
ユーザー管理	ユーザーアカウントを管理可能（未文書化）
リモート管理	リモート管理機能にアクセス可能（未文書化）
基本デバイス情報	デバイスホスト名とセッションステータスにアクセス可能

4.3. リカバリアカウント接続

> 🚨 **重要**: デバイス初期化後、**デフォルトパスワードを変更してください**（クイックスタートガイド -> 4.3. リカバリアカウント参照）。

リカバリアカウント接続

仮想ターミナル（ヘッドレスモードのみ）に物理的にアクセスするには、**キーボード、マウス、およびスクリーン**が必要です。

コマンドリストと制限された特権

リカバリアカウントユーザー用の制限シェル（`rbash`）環境でアクセス可能なコマンドは以下の通りです：

ネットワーク管理コマンド:

- `nmtui`: ネットワーク設定
- `nmcli`: NetworkManager クライアント
- `mmcli`: ModemManager クライアント

スタック管理コマンド:

- `cx-manager stack up`: スタックを開始
- `cx-manager stack down`: スタックを停止
- `cx-manager stack status`: スタックの状態を表示
- `cx-manager status`: 全体の状態を表示

パスワード管理:

- `passwd`: ユーザーパスワードを変更

ヘルプコマンド:

- `help`: 利用可能なコマンドのリストを表示

---

5. ハードウェア暗号化

5.1. セキュアブートとフューズング

> 🚨 **重要**: Jetson モジュールのセキュアブートフューズは永続的に書き込まれ、システムを検証済みブートパスに制限します。これにより、Edgematrix 以外の署名されていないイメージのインストールが防止されます。

Edgematrix が提供するハードウェアは、**信頼された署名済みファームウェアと OS イメージ**のみをインストールできます。

5.2. ファイルシステム暗号化

> ℹ️ **情報**: LUKS 暗号化は特定のフォルダーだけでなく、ルートファイルシステム全体に適用され、フルディスクデータ保護を確保します。

EdgeAI Station は**LUKS（Linux Unified Key Setup）**を使用してルートファイルシステムを暗号化し、設定ファイル、ログ、モデル、記録されたメディアなど、保存されているすべてのデータが安全に保護されることを保証します。

起動時に、暗号化されたパーティションは、手動パスワード入力を必要とせずに、セキュアハードウェアに保存されたキーを使用して自動的にアンロックされます。これは、上記で説明した NVIDIA Jetson セキュアブートメカニズムとの統合によって可能になります。

動作方法

1. **システムパーティションは**現代的で安全な暗号化形式である LUKS2 で暗号化されます
2. **復号化キーは**Jetson モジュール上の信頼実行環境（TEE）に保存されます
3. **起動時に**、NVIDIA Secure Boot チェーンが復号化キーをリリースする前にブートローダーとカーネルの真正性を検証します
4. **ブートチェーンが改ざんされた場合**、キーはリリースされず、システムは起動に失敗し、データを保護します

したがって、デバイスが**物理的に盗まれたり改ざんされたりした場合**、暗号化されたデータはアクセスできません。

---

6. サービスアクセスと認証

6.1. Web サーバー用 TLS 証明書

> ℹ️ **情報**: 署名済みおよびプライベート証明書の使用は、将来のバージョンで提供される可能性があります。
>
> ⚠️ **警告**: EdgeAI Station の Web ページに初回アクセスすると、証明書が署名されていないことを示す警告メッセージが表示されます。ページに進むには、証明書の詳細を確認してホワイトリストに追加してください。

EdgeAI Station は、自己署名証明書で**Traefik**をリバースプロキシとして使用して、**TLS**でエンドポイントを保護します。証明書とその秘密鍵は、インストールプロセス中に EdgeAI Station システムファイルディレクトリに自動的に生成および保存されます。

6.2. PGP キー

デバイスの**PGP キー**は、EdgeAI Station インストールプロセス中に Edgematrix 認証局によって署名されます。

署名に使用される EdgeAI Station キータイプは**EDDSA（ed25519）で、暗号化に使用されるキータイプは**ECDH（cv25519）**です。

これらのキーは以下に必要です：

- ✅ **AIP セキュアパッケージの復号化**
- ✅ **デバイスバックアップの暗号化**
- ✅ **バックアップアーカイブの検証と署名**
- ✅ **Station Cloud Services バックエンドとの認証**