Power Integrations サプライヤー・サイバーセキュリティ・ポリシー

ポリシー 改訂日: 2026年1月

The online version of this manual is the updated version and takes precedence over any printed copy
このマニュアルのオンライン版は最新版であり、印刷版よりも優先されます。

1. 目的と範囲

本ポリシーは、Power Integrationsの機密データ（以下「PICD」）を取り扱う、またはPower Integrationsのシステムに接続するすべてのサプライヤーに対する、最低限のサイバーセキュリティ要件を定めるものです。これらの要件は、Power Integrationsのサプライチェーン全体において、事業継続性を確保し、独自の情報を保護することを目的としています。

2. 侵害通知の要件

サプライヤーは、PICDまたはPower Integrationsのシステムに影響を及ぼす、あるいは及ぼす可能性があるセキュリティ・インシデントが発生した場合、可能な限り速やかに、かつ発見から**72時間以内**にPower Integrationsに通知しなければなりません。

- **初期通知（24時間以内）：** 予備的な事実関係および封じ込め措置。
- **詳細な更新（72時間以内）：** 範囲、影響を受けたシステム、予想される影響、および次のステップ。
- **必須情報：** 発見日時、インシデントの種類、PICD関与の状況（確定または疑い）、および主要なインシデント連絡先詳細。

3. データの暗号化と管理

サプライヤーは、文書化された暗号化および鍵管理ポリシーを維持しなければなりません。PICDは、強力かつ現代的な暗号アルゴリズムを使用して保護される必要があります。

- **転送中：** すべてのサービス、API、および安全なファイル転送（SFTP/FTPS/HTTPS）において、TLS 1.2または1.3を使用すること。
- **保管時：** PICDを含むストレージおよびバックアップに対して、AES-256（または同等）を使用すること。
- **鍵管理：** 暗号鍵へのアクセスは制限、ログ記録され、ポリシーに従ってローテーションされなければなりません。

4. 最低限のセキュリティ・ベースライン要件

サプライヤーは、業界をリードする管理、物理、および技術的保護策を実装しなければなりません。

- **アイデンティティとアクセス管理**：「最小権限の原則」を徹底すること。
- PICDを取り扱うシステムへのすべての特権アクセス、リモートアクセス、およびインターネットに公開されたアクセスに対して、**多要素認証（MFA）**が義務付けられます。
- **脆弱性およびパッチ管理**：定期的な脆弱性スキャンを維持すること（四半期ごとを推奨）。インターネットに公開されたシステムについては、重大なリスク（Critical）が発見された場合、72時間以内に修正すること。
- **ログ記録と監視**：調査および監査を可能にするため、セキュリティログを最低90日間保持すること。

- **エンドポイント保護**: PICDにアクセスするすべてのシステムに、アンチマルウェアおよびエンドポイント検出・応答（EDR）コントロールを導入すること。
- **AI/生成AIの制限**: サプライヤーは、Power Integrationsからの事前の書面による承認なしに、AI/MLモデルのトレーニングにPICDを使用したり、パブリックAIツールにPICDをアップロードしたりしてはなりません。
- **下請け業者の責任**: サプライヤーは、下請け業者を雇用する場合でもコンプライアンスに対する責任を負います。
- 事前の通知と承認なしに、第三者にPICDへのアクセス権を提供してはなりません。

5. サプライヤーの承認と証明

サプライヤーは、本ポリシーの受領と理解を確認し、必要な管理策が実施されていることを証明します。

A. **コンプライアンス証明**
   - [ ] 文書化されたインシデント対応計画が策定されている。
   - [ ] 72時間の侵害通知期間を承諾する。
   - [ ] 暗号化規格（AES-256/TLS 1.2以上）を満たしている。
   - [ ] MFAおよび最小権限アクセスが徹底されている。
   - [ ] 脆弱性スキャンおよびタイムリーなパッチ適用が実施されている。
   - [ ] 調査のためのセキュリティログが保持されている。

Power Integrations インシデント報告連絡先: Breach-notify@power.com