サイバーセキュリティの脆弱性管理ポリシー

Moxa は、サイバーセキュリティに関する製品[i]の潜在的な脆弱性に確実に対応できるよう、確固としたプロセスを構築しています。私たちは、お客様がリスクを最小限に抑えることができるよう、信頼性の高いガイダンスとソリューションの提供に継続的に取り組んでいます。その一環として Moxa は、製品のサイバーセキュリティインシデントと Moxa 製品の潜在的な欠陥への対応を専門とする製品セキュリティインシデント対応チーム（PSIRT：Product Security Incident Response Team）を設立しました。Moxa は、オートメーション業界で世界的に採用、認識されている慣行と標準[ii]への対応を進めるとともに、潜在的なサイバーセキュリティの脆弱性に対処するため、最良のプロセスと対応策を確保しています。Moxa は産業用インターネットセキュリティを採用しており、すべてのお客様にとって信頼できるパートナーであり続けます。

製品サイバーセキュリティ脆弱性管理プロセス

Moxa の製品サイバーセキュリティ脆弱性管理プロセスは、以下に詳述する 5 つのステージから構成されています。Moxa は、各ステージのプロセスに注意深く従い、実施しています。

図 1. サイバーセキュリティの脆弱性に対する管理プロセス

- **インシデント発生直後の対応**：PSIRT が、Moxa 製品に関する外部からの脆弱性レポートを受け取り次第、最初の応答を 2 営業日以内に返します。
- **トリアージと分析**：PSIRT は、サイバーセキュリティの潜在的な脆弱性をトリアージ（優先順位付け）して分析し、Moxa 製品への影響を評価します。このステージで、脆弱性レポートの報告者に予備評価レポートを提出します。
- **調査**：PSIRT は製品開発チームと緊密に連携し、脆弱性の根本原因と、Moxa 製品への影響の程度や度合いを特定します。次に、PSIRT は問題を軽減および解決するためのソリューションを提供します。PSIRT は、このステージを通して継続的に、インシデントの報告者と連絡を取ります。
- **修復**：PSIRT は製品開発チームと緊密に連携し、最終的なソフトウェア/ファームウェアパッチを開発するか、または緩和策の最終調整を行います。また、PSIRT は関連する脆弱性に関する最新情報の追跡調

査を継続し、潜在的な影響を評価します。脆弱性がお客様に高いリスクをもたらし、最終パッチの開発にお客様にお待ちいただける以上に時間がかかる場合、Moxa は最終パッチの提供前に一時的な緩和策を提供いたします。

- **開示**：PSIRT は、製品のサイバーセキュリティに関する脆弱性の結果を、当社のウェブサイトのセキュリティアドバイザリセクションに公開します。レポートには、脆弱性の説明、影響を受ける製品とバージョン、緩和策、および適切な修復計画が記載されます。

Moxa の PSIRT および開発チームは、共通脆弱性評価システム（CVSS）と Moxa のリスクベースの脆弱性管理モデルを元に、インシデントの潜在的なリスクを評価します。PSIRT は、セキュリティの内容、脆弱性が悪用される可能性、考えられる影響、およびその他の要因など、いくつかの要因に基づいて問題に対処するためのタイムラインを作成します。

報告された脆弱性を分析後、Moxa は当該のテスト環境を直ちにセットアップして脆弱性の重大度を判断します。必要に応じて、Moxa は問題の報告者と連絡を取り続けます。根本原因と影響の重大度を特定した後、Moxa は修復策の分析に進み、解決策または緩和策を提供します。

セキュリティアドバイザリの更新と発表は、Moxa のウェブサイトのセキュリティアドバイザリセクションにて公開され、どなたでもセキュリティアドバイザリ RSS フィードを購読できます。特定の Moxa 製品における、最新のセキュリティアナウンスを受け取りたい場合は、始めに Moxa のウェブサイトでアカウントを作成してから、[Follow Updates]オプションをクリックしてください。

サイバーセキュリティの脆弱性に関するお問い合わせ方法

Moxa の製品に潜在的な脆弱性を見つけた場合は、直ちにご報告をお願いいたします。Moxa にとって、脆弱性を即時に特定することが、製品のセキュリティリスクを最小限に抑えるための鍵となります。Moxa 製品の潜在的なサイバーセキュリティの脆弱性を報告するには、PSIRT に電子メールを送信してください。その際、Moxa の PSIRT PGP キーを使用してファイルを暗号化してください。

リスク評価の実行と、その後の修復および緩和策の開発スピードを早めるため、サイバーセキュリティの脆弱性を報告する際は、以下の情報をご記入願います。

1. 製品名とモデル
2. ファームウェア/ソフトウェアバージョン
3. 問題の再現に必要な機器とソフトウェア
4. 問題を再現する手順（可能な場合は写真またはコードを添付してください）
5. 脆弱性実証のためのエクスプロイトコード
6. 攻撃者が脆弱性を攻撃する方法の説明

7. パケットのキャプチャ（Wireshark などのツールをご利用ください）
8. その他、関連すると思われる事物

- PSIRT のメールアドレス：PSIRT@moxa.com
- Moxa の PGP キーをダウンロード

免責条項

「サイバーセキュリティ脆弱性管理ポリシー」の内容は、特定の状況に応じて変更される場合があります。特定の問題または問題のカテゴリに対応することを保証するものではありません。このドキュメントにある情報、またはこのドキュメントからリンクされているコンテンツを使用する際にかかるリスクについては、お客様の責任となります。Moxa は、本書の内容を予告なしにいつでも変更できるものとします。本書の変更は、Moxa の公式ウェブサイトで公開されます。www.moxa.com/jp

[i] ここで言及されている「製品」とは、市場に出回っている標準的な Moxa 製品を指します。カスタマイズされた製品などの非標準製品の保守および欠陥に対する対応は、契約書の規定に従って履行されます。

[ii] Moxa は、以下をはじめとする数多くの基準に準拠しています。
- FIRST（Forum of Incident Response and Security Teams）による共通脆弱性評価システム
- FIRST の PSIRT Services Framework v1.1
- ISO/IEC 29147:2018 脆弱性開示