LehmanSoft Japan 脆弱性開示ポリシー（VDP）

Version 1.2
制定日: 2026-05-11
最終更新日: 2026-10-30

発行者:
LehmanSoft Japan 株式会社

1. 目的

LehmanSoft Japan 株式会社（以下「当社」）は、「2. 対象範囲」に定める当社製品（以下「対象製品」）および関連するソフトウェア、設定ファイル、運用スクリプト、技術文書に関するサイバーセキュリティ上の問題を適切に受け付け、調査し、必要な修正または軽減策を提供するため、本脆弱性開示ポリシー（Vulnerability Disclosure Policy、以下「本ポリシー」）を定める。

本ポリシーは、善意のセキュリティ研究者、顧客、保守担当者、パートナー、およびその他の報告者が、対象製品に関する脆弱性またはその疑いを、安全かつ責任ある方法で報告できるようにすることを目的とする。

2. 対象範囲

本ポリシーの対象製品は以下の通りとする。

製品名	型番	ファームウェア名・バージョン	内部名称
LehmanSoft BESS Gateway	Lehman-EMS-STD-4414	LehmanSoft EMS v1.0.0 on MIL3	LS-FW 1.0.0
LehmanSoft EMS	LS-EMS-003	LehmanSoft EMS v1.0.0 on MIL3	LS-FW 1.0.0

本ポリシーの対象は、対象製品の以下に示すアプリケーション層および関連資産である。

- 上記の対象製品（Lehman-EMS-STD-4414、LS-EMS-003）
- 各対象製品のファームウェア（内部名称 LS-FW 1.0.0）およびその後継バージョン
- LS-FW に含まれるアプリケーションコード、設定ファイル、運用スクリプト
- /etc/ls/ 配下の設定構成に関する脆弱性
- /opt/ls/ 配下の LS-FW ソフトウェアに関する脆弱性
- docs/policies/ 配下のセキュリティ運用文書、サポート方針、更新手順、廃棄手順に関するセキュリティ上の不備
- 対象製品のセキュリティ機能、通信機能、認証情報管理、更新機能、データ削除機能に影響する問題

Lehman-EMS-STD-4414 は、Moxa UC-4414A-I-T および Moxa Industrial Linux 3 Standard 基盤上で動作する。LS-EMS-003 も、同じく Moxa UC-4414A-I-T および Moxa Industrial Linux 3 Standard 基盤上で動作する。Moxa Industrial Linux 3 Standard、Moxa UC-4414A-I-T、Moxa 提供の OS、ドライバ、

システムイメージ、SecureAPT　等の基盤層に係る脆弱性については、Moxa　の　Cybersecurity Vulnerability Management Policy および Moxa PSIRT の手順に従って対応する。

ただし、Moxa 基盤層の問題が対象製品のアプリケーション層、設定、運用、または顧客環境に影響する場合、当社は　Moxa　と連携し、影響範囲の確認、顧客通知、軽減策の提供、修正版の適用案内を行う。

3. 報告窓口

対象製品に関する脆弱性またはその疑いは、以下の窓口に報告することができる。

メールアドレス:
security@lehmansoft.co.jp

件名接頭辞:
[Lehman-EMS-STD-4414 VDP]（LehmanSoft BESS Gateway に関する報告）
[LS-EMS-003 VDP]（LehmanSoft EMS に関する報告）

対応言語:
日本語、英語、中国語（繁体・簡体）

security.txt:
https://lehmansoft.co.jp/.well-known/security.txt

公開ポリシー URL:
https://lehmansoft.co.jp/pdf/vulnerability-disclosure-policy.pdf

報告時には、可能な範囲で以下の情報を含めることを推奨する。

- 影響を受ける製品名、型番およびバージョン
- 例: Lehman-EMS-STD-4414 / LS-FW 1.0.0
- 例: LS-EMS-003 / LehmanSoft EMS v1.0.0 on MIL3
- 影響を受ける機能、設定、通信経路、API、ファイル、または手順
- 脆弱性の概要
- 再現手順
- 影響範囲の推定
- 攻撃に必要な前提条件
- 検証環境
- ログ、スクリーンショット、パケットキャプチャ、PoC 等の参考資料
- 報告者への連絡先
- 公開時の謝辞掲載を希望するかどうか

4. 報告後の対応手順

当社は、受領した脆弱性報告について、以下の手順で対応する。

4.1 受領確認

当社は、脆弱性報告を受領した後、原則として 5 営業日以内に報告者へ受領確認を行う。

受領確認では、報告を受け付けたこと、今後の確認方針、および追加情報が必要な場合の依頼事項を通知する。

4.2 初期トリアージ

当社は、報告受領後、原則として 14 営業日以内を目標に初期トリアージを行う。

初期トリアージでは、以下を確認する。

- 報告内容が本ポリシーの対象範囲に含まれるか
- 再現可能性
- 影響を受ける製品、バージョン、設定、運用条件
- 攻撃に必要な前提条件
- 守るべき情報資産への影響
- 外部ネットワークから悪用可能か
- 認証なしで悪用可能か
- 既知の軽減策が存在するか
- Moxa 基盤層との関連有無

4.3 重大度判定

当社は、脆弱性の重大度判定に CVSS v3.x を使用する。

重大度区分は以下を目安とする。

- Critical: CVSS 9.0 以上
- High: CVSS 7.0 以上 8.9 以下
- Medium: CVSS 4.0 以上 6.9 以下
- Low: CVSS 4.0 未満

CVSS による評価に加え、以下の観点も考慮して、セキュリティアップデートの優先度を決定する。

- ネットワーク経由で悪用可能か
- 認証なしで悪用可能か
- MQTT 認証情報、mTLS 秘密鍵、証明書、通信設定、セキュリティ設定への影響
- 計測値、制御コマンド、設定情報への影響
- BESS / PCS / PLC の運用安全性への影響
- サービス停止、誤制御、情報漏えい、権限昇格、改ざんの可能性
- 実運用環境における攻撃成立可能性
- 一時的な軽減策または設定変更でリスクを低減できるか
- Moxa 基盤層、Debian パッケージ、SecureAPT、systemd 設定との関連性

5. 修正および軽減策の提供方針

当社は、確認された脆弱性について、重大度および影響範囲に応じて、以下のいずれか、または複数の対応を行う。

- LS-FW の修正版提供
- 設定変更手順の提供

- 軽減策の提供
- Moxa 基盤層更新の適用案内
- SecureAPT / APT 経由での更新案内
- リリースノートまたはサポートポータルでの advisory 公開
- 登録顧客へのメール通知
- 影響なしまたは適用対象外であることの説明

Critical または High と判定された脆弱性については、初期トリアージ完了後、90 日以内を目標として、軽減策または恒久対策を提供する。

ただし、以下の場合は、報告者および影響を受ける顧客との調整により、対応期間が変更されることがある。

- Moxa 基盤層の修正を待つ必要がある場合
- 複数のステークホルダー間で調整が必要な場合
- 安全な修正確認に追加期間が必要な場合
- 公開により利用者へ過度なリスクが発生する可能性がある場合
- 実運用環境での検証が必要な場合

6. 状況更新

当社は、対応中の脆弱性について、原則として 30 日ごとに報告者へ状況更新を行う。

状況更新には、可能な範囲で以下を含める。

- 調査状況
- 再現確認の状況
- 重大度判定の状況
- 修正または軽減策の検討状況
- Moxa 等の外部ステークホルダーとの連携状況
- 修正版または advisory 公開の見込み

報告者への個別連絡とは別に、顧客への通知が必要と判断した場合、当社はリリースノート、サポートポータル、または登録顧客へのメール通知を通じて情報提供を行う。

7. セキュリティアップデート通知

当社は、対象製品に関するセキュリティアップデートを公開する場合、アップデートの内容、必要性、未適用時の影響、および緩和されるリスクを利用者に通知する。

通知媒体は以下の通りとする。

- 各対象製品のリリースノート
- 各対象製品のサポートポータル
- 登録顧客へのメール通知
- 必要に応じた個別サポート連絡

重大度別の通知方針は以下の通りとする。

- Critical: 修正版提供後 5 営業日以内に登録サポート連絡先へ通知する。

- High: 修正版提供後 10 営業日以内に登録サポート連絡先へ通知する。
- Medium: 次回定例リリースノートに記載する。
- Low: リリースノートに記載する。

Critical または High の通知には、以下の情報を含める。

- 対象製品および対象バージョン
- 脆弱性の概要
- 重大度
- 影響範囲
- アップデートの必要性
- 未適用時に想定されるリスク
- 修正版の適用手順
- 一時的な軽減策
- 必要な設定変更
- Moxa 基盤層更新が必要な場合の適用案内

8. 公開および調整

当社は、脆弱性情報の公開について、報告者、顧客、Moxa 等の関係者と必要に応じて調整する。

当社は、利用者へのリスクを低減するため、修正版または軽減策の準備が整った後に、リリースノートまたはサポートポータルで advisory を公開することを基本方針とする。

報告者が独自に公開を希望する場合は、事前に当社へ連絡し、公開時期および公開内容について調整することを推奨する。

9. Safe Harbor

当社は、本ポリシーに従い、善意で、かつ安全な範囲で脆弱性の調査および報告を行う報告者に対して、原則として法的措置を求めない。

Safe Harbor の対象となるためには、報告者は以下を遵守する必要がある。

- 本ポリシーの対象範囲内で調査すること
- 実運用中の顧客環境に影響を与えないこと
- データの破壊、改ざん、削除、外部送信を行わないこと
- 個人情報、認証情報、秘密鍵、証明書、営業秘密等を取得、保存、共有しないこと
- サービス停止、DoS、過負荷、制御異常を発生させないこと
- 発見した脆弱性を第三者へ公開する前に当社へ報告すること
- 報告後、当社と合理的な調整を行うこと

本ポリシーに違反する行為、悪意ある行為、または顧客・第三者に損害を与える行為については、Safe Harbor の対象外とする。

10. 禁止されるテスト

以下の行為は禁止する。

- 顧客環境、本番環境、第三者環境への無断アクセス
- DoS、DDoS、過負荷試験
- BESS、PCS、PLC、蓄電池制御、電力取引システム、または現場設備の安全性に影響する操作
- 実際の制御コマンド送信による設備動作への影響
- 認証情報、秘密鍵、証明書、個人情報、営業秘密の取得または外部送信
- 物理的破壊、分解、改造
- ソーシャルエンジニアリング
- フィッシング
- スパム送信
- マルウェアの設置
- 永続的なバックドア、アカウント、鍵、設定変更の作成
- ログ削除または証跡隠蔽
- 法令または契約に違反する行為

11. 対象外の報告

以下の報告は、原則として本ポリシーに基づく脆弱性対応の対象外とする場合がある。

- 実際のセキュリティ影響が確認できない報告
- バージョン情報の公開のみを問題とする報告
- 一般的なベストプラクティスの提案のみで、具体的な脆弱性を伴わない報告
- 既知であり、すでに修正予定または対応済みの問題
- サポート終了後の製品に関する問題
- 改造済み、非公式パッケージ導入済み、またはサポート範囲外の構成に限定される問題
- Moxa 基盤層のみの問題であり、対象製品のアプリケーション層に影響しないもの

ただし、対象外と判断した場合でも、当社は必要に応じて報告者へ理由を説明する。

12. Moxa 基盤層との連携

対象製品（Lehman-EMS-STD-4414、LS-EMS-003）は、いずれも Moxa UC-4414A-I-T および Moxa Industrial Linux 3 Standard 基盤上で動作する。

以下に該当する脆弱性については、Moxa の Cybersecurity Vulnerability Management Policy および Moxa PSIRT の手順に従って対応する。

- Moxa Industrial Linux 3 Standard の OS 層
- Moxa UC-4414A-I-T のハードウェアおよびファームウェア
- Moxa 提供のシステムイメージ
- SecureAPT / APT リポジトリ
- Moxa 提供の SSH、NTS 等の基盤機能
- Moxa 提供パッケージに含まれる既知 CVE

Moxa 基盤層の脆弱性が対象製品の利用者、アプリケーション層、通信機能、セキュリティ機能、または運用に影響する場合、当社は Moxa と連携し、以下を行う。

- 影響範囲の確認
- 一時的な軽減策の検討
- 顧客通知
- Moxa 提供修正版の適用案内
- LS-FW 側で必要な設定変更または手順変更
- リリースノートまたはサポートポータルでの情報提供

アプリケーション層と基盤層の双方に影響する問題については、当社と Moxa の各方針を照合し、利用者への影響を最小化するため、より早い対応期限を採用する。

13. サポート期間

対象製品の標準サポート期間は以下の通りとする。

項目	Lehman-EMS-STD-4414	LS-EMS-003
初回リリース日	2026-05-11	2026-10-01
標準サポート期間終了日	2031-05-11	2031-10-01
標準サポート期間	5 年間	5 年間

延長サポート:
個別契約により最大 2 年

End-of-Life 通知:
標準サポート期間終了の少なくとも 12 か月前までに公式通知を行う。

当社は、標準サポート期間中、対象製品に関するセキュリティアップデート、軽減策、または運用上の注意喚起を必要に応じて提供する。

サポート期間終了後は、原則としてセキュリティアップデートを提供しない。ただし、個別契約に基づく延長サポートがある場合は、その契約条件に従う。

14. 報告者への謝辞

当社は、報告者が希望し、かつ公開内容について合意した場合、リリースノート、advisory、またはサポートポータルにおいて、報告者への謝辞を記載することがある。

謝辞の掲載は、以下を前提とする。

- 報告者が本ポリシーを遵守していること
- 報告者が謝辞掲載に同意していること
- 顧客、第三者、Moxa、またはその他関係者の機密情報を含まないこと
- 修正版または軽減策が提供可能であること

15. 個人情報および機密情報の取扱い

報告者は、調査中に個人情報、認証情報、秘密鍵、証明書、顧客情報、営業秘密、またはその他の機密情報へアクセスした場合、ただちに調査を停止し、当社へ報告すること。

報告者は、これらの情報を保存、複製、共有、公開、または第三者へ送信してはならない。

当社は、脆弱性報告に含まれる報告者の連絡先情報を、脆弱性対応、連絡、調査、謝辞掲載の確認、および必要な管理目的に限定して利用する。

16. 免責

当社は、本ポリシーに基づく報告を誠実に受け付け、調査および対応に努める。ただし、すべての報告について修正、報奨、謝辞掲載、または個別回答を保証するものではない。

当社は、報告内容、影響範囲、製品のサポート状態、実運用環境への影響、Moxa 基盤層との関連性、またはその他の事情により、対応方法を決定する。

本ポリシーは、報告者に対して製品、システム、ネットワーク、データ、または第三者環境へのアクセス権限を付与するものではない。

17. 連絡先

対象製品に関する脆弱性報告、セキュリティアップデート、または本ポリシーに関する問い合わせは、以下に連絡すること。

LehmanSoft Japan 株式会社 セキュリティ窓口
security@lehmansoft.co.jp

件名接頭辞:
[Lehman-EMS-STD-4414 VDP]（LehmanSoft BESS Gateway に関する報告）
[LS-EMS-003 VDP]（LehmanSoft EMS に関する報告）

公開ポリシー:
https://lehmansoft.co.jp/pdf/vulnerability-disclosure-policy.pdf

security.txt:
https://lehmansoft.co.jp/.well-known/security.txt

18. 改訂履歴

版	改訂日	改訂内容
1.0	2026-05-11	制定（対象製品: Lehman-EMS-STD-4414）
1.1	2026-10-27	対象製品に LehmanSoft EMS（型番 LS-EMS-003）を追加
1.2	2026-10-30	記載内容の一部訂正