国軒高科日本株式会社管理制度

バッテリーマネジメントシステム（BMS）脆弱性開示ポリシー

発行日：2024 年 10 月 20 日

施行日：2024 年 10 月 20 日

掲載場所： https://www.gotionjapan.com/

発行者：国軒高科日本株式会社（Gotion Japan Co., Ltd.）

1. 総則

1.1 目的：

近年、バッテリーマネジメントシステム（以下「BMS」という）は、新エネルギー車、エネルギー貯蔵ステーション、携帯電子機器などの分野で広く応用されており、その安全性および安定性は、利用者の生命・財産の安全および産業エコシステム全体の安全に直接関わる重要な要素となっています。

本方針は、社内テストによって発見された、または外部から報告された BMS のセキュリティ脆弱性について、その報告・受付・評価・修復・状態更新などの全プロセス管理を標準化し、体系的な脆弱性対応メカニズムを確立することを目的とします。

これにより、BMS 製品ユーザーの情報セキュリティおよび装置運用の安全を確保し、セキュリティリスクの未然防止および低減を図るとともに、産業チェーンの上下流パートナーおよびエンドユーザーの正当な権益を保護いたします。

本方針は、国軒高科日本株式会社（以下「当社」という）が自社開発・委託製造・販売許諾を行うすべての BMS 製品に適用されます。具体的には車載用動力 BMS、大型エネルギー貯蔵 BMS、産業・商業用エネルギー貯蔵 BMS、携帯機器用 BMS、ならびにカスタム BMS ソリューションを含みます。

1.2 適用範囲：

本方針は、当社 BMS 製品に関するセキュリティ脆弱性を合法的に発見したすべての主体（セキュリティ研究機関、サイバーセキュリティ企業、大学・研究チーム、独立系セキュリティ研究員、一般ユーザー等、以下「外部報告者」という）を対象とします。

また、当社の社内テストチーム（研究開発テストグループ、セキュリティテストグループ、品質検査グループなどの専任チームおよび各事業部門の兼任テスト担当者、以下「内部テストチーム」という）にも適用されます。

本方針では、外部報告者および内部テストチームが脆弱性を報告する際の具体的な要件、当社における脆弱性の受付、評価、修復などの処理プロセスを明確に定義するとともに、脆弱性開示の各段階における関係主体の権利と義務を明示し、円滑な協力体制を確立するための指針を提供します。

1.3 基本原則：

当社は常に「透明性・効率性・協働・責任」の核心原則を持ち、オープンで包容力のある脆弱性開示エコシステムの構築を目指します。

外部報告者からの合理的な脆弱性報告および内部テストチームによる脆弱性発見に対し、当社は専門的リソースを動員して積極的かつ迅速に対応いたします。専用のコミュニケーションチャネルを通じて報告者と密接な連携を図り、専門的な提案を十分に取り入れることで、BMS 製品のセキュリティ防護能力を向上させます。

本方針に基づき、善意で脆弱性を報告し、脆弱性を利用した不正行為を行わなかった外部報告者および内部テストチームに対して、当社は法令および社内規定に則りその権利を保護します。

また、脆弱性の修復が完了するまでの間は、秘密保持の取り決めを遵守することを推奨し、市場秩序および当社の利益を共同で守ることを重視します。

2. 脆弱性報告の連絡先

2.1 公式ウェブサイト（外部報告者向け）：

外部報告者は、当社公式ウェブサイト内のセキュリティ特設ページにアクセスすることで、本脆弱性開示方針の全文、報告テンプレート、およびオンライン提出入口を確認できます。URL は https://www.gotionjapan.com/ です。

当該ページでは、脆弱性対応状況の最新情報やよくある質問への回答を随時更新しております。報告者は、オンラインフォーム内の指示に従って脆弱性情報を記入し、関連証拠資料を添付することができます。送信後、即時に受領確認が自動返信されます。

2.2 専用メールアドレス：

外部報告者の場合：

脆弱性に関する詳細情報を整理の上、当社の脆弱性専用受付メールアドレス (jp_admin@gotion.com) 宛に送付してください。処理効率向上のため、メール件名は

「BMS 脆弱性報告—製品型番—報告日」の形式を推奨します。

本文は「報告者情報—製品情報—脆弱性の詳細—証拠資料」という構成で記載し、テストコード、脆弱性再現動画、スクリーンショット等の添付も可能です。添付ファイルの容量は 200MB 以内を推奨します。

内部テストチームの場合：

脆弱性情報は内部専用の脆弱性管理メールアドレス (jp_admin@gotion.com) に送信してください。メール件名は「内部 BMS 脆弱性報告—製品型番—テストチーム—報告日」とし、本文は「テスター情報—製品情報—脆弱性の詳細—テストケース—リスク評価」の順で記載します。

2.3 連絡電話：

外部相談（外部報告者向け）：

平日（月～金、9:00～18:00、法定休日を除く）に、セキュリティ緊急対応電話 029-869-8262 までご連絡ください。報告手続に関する質問や、脆弱性処理進捗の確認などの一般相談を受け付けています。脆弱性の詳細情報を提出する場合は、記録保全のため、可能な限り公式ウェブサイトまたは専用メール経由での報告を推奨します。

内部連絡（内部テストチーム向け）：

内部テストチームは、セキュリティ部内線番号 029-869-8262 にて脆弱性報告および進捗確認に関するリアルタイム連絡が可能です。

2.4 郵送先（外部報告者向け）：

書面形式での脆弱性報告書を提出する場合は、以下の宛先までご郵送ください。

〒305-0005　茨城県つくば市天久保 2-17-5

国軒高科日本株式会社 セキュリティ部 脆弱性報告受付宛

法人の場合は社印を押印し、個人の場合は署名を記載してください。また、関連証拠資料の写しを同封してください。追跡可能な書留便または宅配便での送付を推奨いたします。

3. 脆弱性報告の要件

技術チームが迅速かつ正確に評価・処理を行えるよう、また報告内容の不備による対応遅延を防止するため、報告者は以下の主要情報を必ず含め、内容の真実性・正確性・完全性を確保してください。

3.1 報告者情報：

外部報告者：

法人による報告の場合は、機関名、法人番号（または統一社会信用コードに相当する番号)、担当者氏名および職位、有効な連絡先（固定電話、電子メール、携帯電話番号）を記載してください。

個人による報告の場合は、氏名、(任意で）身分証番号（本人確認目的)、有効な連絡先（メールアドレス、携帯電話番号）を記載してください。

正確な連絡先の提供は、当社が報告者に迅速にフィードバックおよび連絡を行うために不可欠です。

内部テストチーム：

テスト担当者の氏名、所属部門／テストグループ、社員番号、社内ネットワーク上の連絡先を明記してください。チームとしての成果報告の場合は、チームリーダーおよび参加メンバーを併記してください。

3.2 製品情報：

報告対象の BMS 製品の完全な型番（例：「GX_CN_BAMS_V1.01」）を明確に記載してください。また、次の情報を網羅することが求められます。

ハードウェアバージョン（装置本体または取扱説明書に記載）、ソフトウェアバージョン（管理画面等で確認可能）、ファームウェアバージョン、運用環境（電池セルの種類〔三元系リチウム、リン酸鉄リチウム等〕、電池パック容量、関連制御装置の型番および OS バージョン、使用シナリオ〔産業用蓄電、家庭用蓄電、新エネルギー車など〕）。

内部テストチームは、これらに加えてテスト機器番号、テスト環境の種別（シミュレーション環境または実機環境）を明記すること。

3.3 脆弱性の詳細：

外部報告者：

脆弱性の具体的な発生箇所（特定の機能モジュール、コードロジック、通信プロトコル等）、発生条件（特定の操作手順、入力パラメータ、環境設定など）および完全な再現手順を明確に説明してください。再現手順は実行可能であることが求められ、当社技術チームが記載内容に基づいて確実に再現できるレベルである必要があります。

可能な場合は、テストコード、脆弱性発生時のスクリーンショット（重要箇所の注記付）、再現過程の動画（説明テキスト付）などの証拠資料を提供することを推奨します。これにより評価効率が向上します。

内部テストチーム：

テストケース番号、テスト実施日時、脆弱性発生時のログファイル、製品設計仕様からの乖離点を明示してください。再現手順には、テスト環境の構築方法を含め、他のテスト担当者が 100％再現可能であるよう記載することが求められます。

3.4 リスク評価：

外部報告者：

専門的判断に基づき、当該脆弱性がもたらす影響について初期的な評価を行ってください。評価観点は以下に限定されません：

BMS の主要制御機能（充放電管理、過充・過放制御など）に対する影響、バッテリ安

全リスク（発火・爆発・膨張など）の有無、ユーザーの機微データ（運転データ、識別情報等）の流出可能性、装置の不正制御やサービス妨害（DoS）発生の有無等。

また、CVSS（共通脆弱性評価システム）に基づく暫定的リスクレベルの提示も推奨します。

内部テストチーム：

当社内部文書「BMS 脆弱性リスク評価細則」に準拠し、CVSS 3.1 基準に基づいてリスクレベルを算定してください。

併せて、脆弱性が製品ライフサイクルのどの段階（研究開発段階／量産段階／市販段階）で影響するかを明記します。

3.5 修復提案：

外部報告者：

発見した脆弱性に対する具体的な修復方針または提案を記載し、後続の対応作業の参考としてください。例として、コードレベルでの修正（入力検証の追加、権限管理の強化等）、設定面での改善（通信暗号化アルゴリズムの最適化、デフォルトパスワードポリシーの修正等）、ハードウェアの改善（セキュリティチップ追加等）、運用・管理面での暫定的回避策などが挙げられます。

内部テストチーム：

製品設計文書に基づき、実現可能な修復提案を提示してください。特に、暫定的な回避策によるリスク低減の可否、ならびに修復案が製品性能および互換性に与える潜在的影響について明示する必要があります。

4. 脆弱性対応プロセスおよび概要

4.1 報告の受領および確認（1〜3 営業日）

当社セキュリティ部は、脆弱性対応専任チームを設置し、報告受付および初期審査を

担当します。

外部報告：

当社は、脆弱性専用メールボックスおよび公式ウェブサイトのフィードバックチャネルを 24 時間 365 日体制で監視し、平日には電話および郵送による報告窓口も運用しています。

報告受領後、専任チームは 1〜3 営業日以内に初期審査を行い、情報の完全性、内容の明確性、当社製品に該当するか否かを確認します。

情報が十分で要件を満たす場合、報告者に対しセキュリティ部印の押された《脆弱性報告受領確認書》を発行し、その中で報告番号、脆弱性の概要、受付日時、今後の処理ステップを明記します。

情報が不十分または曖昧な場合、報告者の指定した連絡先に補足依頼リストを送付し、補完後に正式受付を行います。

内部報告：

内部テストチームから報告を受領後、1 営業日以内に審査を完了します。内容が完全な場合、即時に内部脆弱性番号を発行し、《内部脆弱性受領確認票》を報告チームへ送付します。

不完全な報告に対しては、社内メッセージツールを通じ補足案内を行い、追記後 1 営業日以内に確認を完了します。

4.2 脆弱性評価および分類（3〜5 営業日）

外部報告脆弱性：

セキュリティ部は、「脆弱性評価専門委員会」を招集します。委員会には、BMS 中核開発エンジニア、上級セキュリティテストエンジニア、システムアーキテクト、外部のサイバーセキュリティ専門家が参加し、報告済み脆弱性を総合的に技術評価します。

評価では、影響範囲（対象製品数・ユーザー規模)、危険度（安全・経済への影響)、悪用難度（必要とされる専門性やツールの有無)、既公開の攻撃コードの存在有無などを考慮し、CVSS 3.1 スコア体系に基づき定量評価を行い、高・中・低の 3 段階に分類します。

内部報告脆弱性：

セキュリティ部、開発責任者、テスト代表で構成される内部評価チームが同基準（高／中／低リスク）で評価します。

併せて、量産工程や既発売製品への影響の有無を確認します。開発段階のみで発生した脆弱性は、ユーザー告知手続を経ずに直接修復プロセスへ移行します。

脆弱性レベルの分類基準：

（1）高リスク（CVSS 9.0～10.0）：

BMS の充放電制御・熱管理等の中核機能が完全に停止し、発火・爆発・電解液漏出等の重大事故につながる可能性がある場合。

またはユーザー識別情報、稼働データ等の機密情報が大量に漏洩する場合、または、攻撃者がリモートでデバイスを不正制御できる場合。悪用が容易で拡散性が高いものを含む。

（2）中リスク（CVSS 6.0～8.9）：

BMS の一部機能（例：セルバランス管理、データ収集等）に障害が生じ、充放電効率低下や寿命短縮につながる場合。

構成情報・ログ等の非機密データ流出や、限定的条件下での部分的な性能劣化を引き起こす場合を含む。悪用には中程度の専門技術が必要。

（3）低リスク（CVSS 0.1～5.9）：

表示上の不具合、非重要パラメータの誤差など、軽微な問題に限られ、主要機能には

影響を与えない場合。

特殊な環境や設定を要し、実質的な攻撃価値が極めて低いものを含む。

評価完了後、当社は 3〜5 営業日以内に結果を通知します。

外部報告者には《脆弱性評価結果通知書》、内部テストチームには《内部脆弱性評価結果票》を発行し、脆弱性レベル、CVSS スコアと評価根拠、技術分析および潜在リスク、今後の修復予定概要を明確に記載します。

4.3 脆弱性修復および検証

（高リスク：7〜14 営業日／中リスク：15〜30 営業日／低リスク：30〜60 営業日）

（1）高リスク脆弱性：

即時に第 1 種緊急対応を発動し、技術責任者をリーダーとする緊急修復特別チームを設置します。非緊急案件を一時停止し、人員・リソースを優先投入します。

修復方針は、外部脆弱性の場合は評価専門委員会、内部脆弱性の場合は内部評価チームの承認を経て開発に着手します。

修復後、セキュリティテストチームが複数回の侵入・耐圧・シナリオ試験を実施し、完全修復と新たなリスク非発生を確認します。

開発段階で発見された高リスク脆弱性は、24 時間以内に修復を開始し、3〜7 営業日で検証を完了することを原則とします。

（2）中リスク脆弱性：

第 2 種対応を発動し、月次重点修復計画に組み込みます。開発部門が専任プロジェクトチームを編成し、部門技術責任者が修復方針を承認後、通常のセキュリティ試験および機能検証を行います。安定性を損なわず修復を完遂することを重視します。

（3）低リスク脆弱性：

第 3 種対応を発動し、製品のアップデートサイクルまたは四半期安全更新の中で段階的に修正を進めます。

修復コストが高く影響が軽微な場合は、外部報告者または内部利用部署に向けたリスク回避ガイドラインを作成・提供します。

後続バージョンにて改修を計画し、製品の継続的改善の中で最終修復を完了させます。

検証要件：

外部脆弱性の修復後は、セキュリティテストチームによる独立検証を実施します。

内部脆弱性修復後は、報告チームが一次検証を行い、その後セキュリティテストチームがクロス検証を行い、完全修復を確認します。

修復および検証完了後、当社は《脆弱性修復報告書》（外部用）または《内部脆弱性修復確認書》（内部用）を作成・保存します。報告書には、原報告内容、修復方針、開発・試験記録、修正後バージョン情報、更新手順等を網羅します。

4.4 コミュニケーションおよび免責事項

コミュニケーション：

当社は、対応全期間を通じて専用の連絡体制を維持します。

外部報告者とはメール／電話にて連絡を取り、高リスク脆弱性は 3 営業日ごと、中・低リスクは 7 営業日ごとに進捗を報告します。

内部テストチームは、「BMS 脆弱性管理プラットフォーム」で進捗をリアルタイム確認でき、高リスクは毎日、中・低リスクは 3 営業日ごとに更新されます。

報告者からの合理的な質問や追加提案には、担当者が 2 営業日以内に回答します。

免責事項：

当社は、善意に基づき本方針を遵守し、第三者への情報漏洩や不正利用を行わなかった外部報告者に対して、正当な脆弱性検証行為によって生じた法的責任を追及しません。

内部テストチームが適法かつ社内規定に従い脆弱性を発見・報告した場合、それは職務遂行として扱い、テスト過程における正規操作に関して責任を問わないものとします。

ただし、故意に装置を損壊させる、脆弱性情報を悪意の第三者へ漏洩する、または脆弱性を悪用して不正なデータ取得・システム破壊を行った場合には、当社は証拠を収集し、民事・行政・刑事すべての法的手段によって責任を追及します。

内部関係者が該当する場合は、社内規程《社員違反処分規定》に基づき懲戒処分の対象となります。

5. 修復前の脆弱性状態更新プロセスおよび概要

5.1 脆弱性調査および対応開始（評価完了後 1 営業日以内）

評価結果が確定次第、当社セキュリティ部は 1 営業日以内に開発部門・生産部門・販売部門等と連携し、対象調査を開始します。

外部脆弱性および量産／上市済み内部脆弱性の場合：

生産記録を遡り、該当する製品ロット、生産日、販売地域を特定します。

顧客管理システムを通じて影響を受けるユーザー数および具体情報を統計し、技術解析により脆弱性発生確率および潜在的影響範囲を精査します。

高リスク脆弱性に対しては直ちに緊急対応メカニズムを発動し、暫定保護措置（緊急設定変更ガイドラインの提示・リスクポートの閉鎖・一部危険機能の一時停止等）を策定します。

中・低リスクの場合は、実際のリスクレベルに応じて調査スケジュールおよび対応計画を立案し、リスクの制御を確保します。

開発段階における内部脆弱性の場合：

追加調査として、テスト工程上の漏れや検証手順の欠陥有無を確認します。

その結果をまとめた《テストプロセス最適化提案書》を品質管理部に報告し、再発防止策を講じます。

5.2 状態管理および社内共有

当社は電子台帳および紙台帳の二重管理による脆弱性状態管理体制を構築します。

電子台帳は暗号化データベースで管理し、報告番号、報告者情報、製品情報、評価結果、修復進捗、暫定措置、影響範囲、ユーザー告知状況などの主要情報をリアルタイムで記録します。

更新・保守はセキュリティ部の専任担当者が毎日実施します。

台帳内では「内部発見脆弱性」と「外部報告脆弱性」を区別し、内部脆弱性の発見工程別統計、修復率、再テスト合格率を個別に集計します。

毎週月曜日午前に《脆弱性対応週次進捗報告書》を作成し、開発・生産・販売・カスタマーサポート・品質管理など各部門責任者に共有します。

これにより、各部門が脆弱性情報を即時に把握し、ユーザー告知、アフターサポート、プロセス改善などに連携できるようにし、情報断絶を防ぎます。

5.3 状態公開およびユーザーへの告知

（1）高リスク脆弱性（外部および上市済み内部）：

評価完了および暫定措置策定後 2 営業日以内に、以下の複数チャネルを通じて対象ユーザーに通知します：

公式ウェブサイトのセキュリティ告知欄（最上段掲示）、製品アプリのプッシュ通知（強制ポップアップ形式）、SMS 通知（登録済み携帯番号宛）、企業ユーザーへのメール通知。

通知内容には、脆弱性の概要、潜在リスク、暫定保護措置（操作手順・設定変更方法)、修復進捗計画等を含めます。

以後、修復完了までの間、3 営業日ごとに同様のチャネルを通じて最新進捗を更新します。

（2）中リスク脆弱性（外部および上市済み内部）：

評価完了後 5 営業日以内に、公式ウェブサイト告知欄および製品アプリのメッセージセンターを通じて概要を通知します。

通知内容には、脆弱性の概要（タイプ・影響範囲）と修復計画（完了予定時期・更新方法）を明記します。

その後は 7 営業日ごとに公式ウェブサイト上で進捗を更新します。

（3）低リスク脆弱性（外部および上市済み内部）：

軽微な UI 表示不具合など、ユーザー使用に実質的影響のない場合は、修復後に公式ウェブサイトで四半期ごとのセキュリティアップデート総括告知を行い、修復概要を一括公開します。

潜在的影響がわずかにある場合は、評価完了後 10 営業日以内に公式サイトで概要および修復計画を告知し、高頻度更新は不要とします。

（4）未上市段階の内部脆弱性（開発・量産フェーズ）：

外部通知は不要です。「BMS 脆弱性管理プラットフォーム」および《脆弱性対応週次報告書》上で内部共有し、関連部門が情報を把握できるようにします。

5.4 報告者へのフィードバック

修復着手前の段階においても、当社は報告者に対し次の内容を定期的に報告します：

外部報告者：

調査段階で判明した影響製品数・範囲の統計結果、暫定保護策の内容と効果、修復方針の検討経過・審査状況、開発進度および技術的課題について共有します。

内部テストチーム：

追加で、テストプロセス改善提案の実施状況および関連テストケースの更新進捗を報告します。

報告者から状態に関する問い合わせがあった場合、担当者は 2 営業日以内に適切なチャンネルを通じて詳細に回答し、処理段階証明資料を提供します。修復完了後、外部報告者には《脆弱性修復完了通知書》、内部チームには《内部脆弱性修復完了確認書》を即時送付し、修復報告サマリーを添付のうえ再検証を正式依頼します。報告者からの検証意見は、最終クローズ手続きの重要資料として反映されます。

6. 製品公開における技術サポート期間

6.1 適用範囲：

本条項は、当社が自社開発・委託製造・販売許諾を行うすべての BMS 製品に適用されます。対象には、車載用動力 BMS、大規模エネルギー貯蔵 BMS、産業・商業用 BMS、携帯機器用 BMS、ならびにカスタム BMS ソリューションが含まれます。これらすべての製品のライフサイクル全期間にわたり、技術サポートおよび脆弱性修復の提供期間を本条項で明確に定めます。

6.2 技術サポート期間の区分：

（1）製品サポート期間：

製品の初回市場販売日から起算して 5 年間を製品サポート期間とします。この期間中、当社は以下の技術支援を包括的に提供します：脆弱性修復、安全アップデート、技術相談、トラブルシューティング。高リスク／中リスク脆弱性については、本方針第 4 章および第 5 章の要件に基づき優先的に修復し、ユーザーへの進捗通知を実施します。低リスク脆弱性は四半期単位の更新計画に組み込み修復を完了させます。あわ

せて、無償のファームウェア更新、安全設定最適化指導等の技術サポートを提供します。

（2）サポート終了期間：

製品サポート期間終了後、当社は当該製品に対する公開技術サポートを正式に終了し、新たな脆弱性報告の受付、修復サービス、技術相談の提供を行いません。ただし、製品安全使用ガイドラインおよび技術文書のアーカイブ参照サービス（公式ウェブサイトでのダウンロード提供）は継続します。

6.3 特殊ケースの調整：

（1）カスタム BMS ソリューション：

技術サポート期間は、当社と顧客との間で締結する協定書において別途定めることができます。合意された期間は標準サポート期間（5 年）より短くしてはならず、延長期間については協議の上、契約条項で明示します。

（2）製品の販売終了／生産終了：

製品がサポート期間内に販売終了または生産停止となる場合、当社は追加で 1 年間の技術サポートを提供します。この期間中に既知の脆弱性修復およびユーザー告知を完了させることを保証します。販売終了告知には技術サポート期間延長の詳細を明記し、公式ウェブサイトや顧客チャネルを通じてすべての影響ユーザーに通知します。

6.4 サポート期間の公表およびユーザー通知：

（1） 当社は公式ウェブサイト（https://www.gotionjapan.com/）内の製品詳細ページおよびセキュリティ特設セクションにて、販売中のすべての BMS 製品の基本サポート期間および延長サポート期間の開始・終了日を公表します。また、販売終了・生産終了製品のサポート期間変更情報を毎月更新・掲載します。

（2） 製品初回販売時には、取扱説明書および保証書に技術サポート期間と提供内容を明記します。

（3） 基本サポート期間または延長サポート期間の満了 3 か月前には、製品アプリ通知、SMS、メール（登録済みユーザー宛）を通じ、サポート終了予定および今後のサ

ービス提供方針をユーザーへ通知します。

6.5 責任の範囲：

（1） サポート期間内において、当社は本方針に従い脆弱性修復および技術支援の義務を誠実に履行します。公開サポート期間を超過した製品について、当社は脆弱性修復および技術サポートの法的義務を負いません。ユーザーは任意で脆弱性報告を提出できますが、当該報告は参考情報として扱い、正式な処理プロセスには含めません。

（2） ユーザーが修復パッチを適時適用しなかった場合、または当社が提供する暫定保護措置に従わなかったことによって発生したセキュリティリスク、もしくは技術サポート期間終了後の製品における安全問題に対して、当社は一切の責任を負いません。

7. その他の説明

7.1 方針更新：

本方針は、BMS 技術の進化（新規通信プロトコルの導入、スマート機能拡張など）、関連法令・業界標準の改訂、運用経験および社内検証プロセス改善ニーズに応じて適宜改訂します。

改訂前に技術・法務・マーケティング・品質管理・テスト・外部セキュリティ専門家の意見を聴取し、改訂後は公式ウェブサイトセキュリティセクションおよび社内イントラネットで更新告知を行います。

改訂内容と発効日を明示し、告知日をもって新方針を施行、旧版は同時に廃止します。ユーザー、外部報告者、従業員が最新情報を適時に把握できるようにします。

7.2 脆弱性開示の証明書類：

脆弱性開示方針の公開を計画する場合、評価機関に対し以下の証憑資料（Evidence）を提出し、必要記録を完備します。

（1）公開予定日：

政策公開日は製品上市日より少なくとも 7 営業日前であることを示す文書を添付し、社内承認済の製品上市計画書（公開日付を記載）を併せて提出します。

（2）公開方法・掲載位置：

当社公式ウェブサイト（https://www.gotionjapan.com/）内のセキュリティ専用ページを主要公開チャネルとし、製品取扱説明書等でも方針リンクを併せて告知する旨を明示します。

（3）公開予定の方針案：

現行方針と同構成の草案全文を提出し、対象製品の特性に応じて調整箇所と理由を明示した別添説明資料を添付します。

問い合わせ窓口：

本方針の条項内容・運用プロセス・具体的操作に関して不明点がある場合、外部報告者およびユーザーは、第 2 章で示した各連絡チャネル（公式ウェブサイト、専用メール、電話）を通じてセキュリティ部にお問い合わせください。

社内関係者およびテストチームは、内線電話、社内メッセージ、または「BMS 脆弱性管理プラットフォーム」上の相談窓口を利用できます。

セキュリティ部は 2 営業日以内に分類処理を行い、複雑な事項については専門会議の上で正式回答を行います。

7.4 社内インセンティブ制度：

内部テストチームが高リスク・重大脆弱性を発見した場合、当社は《開発およびテスト評価奨励規程》に基づき、金銭報酬・業績加点・表彰優先資格などを付与します。

また、発見件数・修復検証効率・テストプロセス改善貢献が基準値を満たしたチームには、四半期ごとに特別報奨を授与し、BMS セキュリティ防御活動への積極参加を奨励します。

7.5 サプライチェーン管理

本社 BMS 製品は第三者企業からの供給部品を含むため、Gotion Japan がサプライチェーン全体を直接管理しています。サプライチェーンに関する連絡・調整については、Gotion Japan の BMS チームがサプライチェーン責任者と直接連携する体制を構築しています。現在の主な連絡窓口は以下のとおりです。

サプライチェーン責任者：方 佳麗

連絡先：（+86）130-9331-3537