カブトテック株式会社 管理制度

KABUTO TECH

Battery Energy Storage System (BESS)

脆弱性開示ポリシー

公開場所：https://kabutotech.com/

公開日：2025 年 5 月 16 日

適用開始日： 2025 年 5 月 16 日

1. 総則

ESS（エネルギー貯蔵システム）が直面するサイバーセキュリティリスクを有効に防止・低減し、脆弱性の発見、評価、修正および開示プロセスを標準化し、機器の脆弱性に起因する重大な安全事故または広域停電事象を防止することを目的とします。

1.1 適用範囲

本ポリシーは、当社が調達、導入および運用保守するすべての電力系統向け／産業・商業向け ESS 蓄電システム、ならびに関連する BMS（バッテリーマネジメントシステム）、EMS（エネルギーマネジメントシステム）、PCS（パワーコンディショナ）およびクラウド監視プラットフォームに適用されます。また、すべての ESS 機器のソフトウェア・ハードウェアサプライヤーおよび第三者インテグレーターにも適用されます。

2. コンプライアンスおよび認証管理（JC-STAR フレームワークに基づく）

ESS 製品が基礎的なハードウェアレベルおよびネットワークレベルのセキュリティ保護能力を備えることを確保するため、基幹電力網に接続されるすべての ESS 機器は、以下の国際規格または業界標準を満たさなければなりません。

2.1 JC-STAR 認証の必須要求事項

サプライヤーは、ESS の中核となるネットワーク接続機器（例：ゲートウェイ、スマートコントローラー）について、日本の IPA（情報処理推進機構）による JC-STAR セキュリティ認証を申請し、取得しなければなりません。

- 認証レベル管理（Level Control）：本番環境に導入する機器の JC-STAR 認証レベルは、Level 1 を下回ってはなりません。
- 証明書有効期限の監視（Expiration Date Monitoring）：サプライヤーは、証明書の有効期限満了日の少なくとも 90 日前までに、更新または上位認証への移行手続きを開始する必要があります。期限切れ（Expired）または取消済み（Revoked）の機器型式については、新規プロジェクトでの調達を厳禁とし、既存機器については 1 か月以内にファームウェアのアップグレードまたは交換を完了しなければなりません。

- 状態追跡（Status Tracking）：日常の運用保守において、JC-STAR リスト上の機器ステータスを定期的に確認する必要があります。ステータスが Withdrawn（メーカーによる自主的な取下げ）または Revoked（取消し）に変更された場合、直ちに緊急対応を発動し、当該ロットの機器を隔離するとともに代替案を調査します。

3. 脆弱性報告の連絡方法

3.1 公式ウェブサイト（外部報告者向け）：

報告者は、当社公式ウェブサイト（https://kabutotech.com/）にアクセスすることで、脆弱性開示ポリシー全文、報告テンプレートおよびオンライン提出場所を確認できます。

同ページでは、脆弱性対応状況およびよくある質問を随時更新します。報告者はオンラインフォームを通じて脆弱性に関する連絡事項を提出し、関連する証明資料をアップロードできます。提出後、受付確認が即時に通知されます。

3.2 専用メールアドレス：

外部報告者は、脆弱性の詳細情報を整理したうえで、当社の脆弱性報告専用受付メールアドレス（Alex.Tei@kabutotech.com）に送付できます。処理効率を高めるため、メール件名は「BMS 脆弱性報告－製品型番－報告日」の形式に統一することを推奨します。また、メール本文は「報告者情報－製品情報－脆弱性の詳細－証明資料」の構成に従って記載してください。必要に応じて、テストコード、脆弱性再現動画、スクリーンショット等の資料を添付できます。添付ファイルの合計サイズは 200MB 以内に抑えることを推奨します。

内部テストチームは、脆弱性情報を内部脆弱性管理専用メールアドレス（Alex.Tei@kabutotech.com）に送付する必要があります。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」の形式に統一してください。本文は「テスト担当者情報－製品情報－脆弱性の詳細－テストケース－リスク評価」の構成に従って記載してください。

3.3 連絡電話：

外部問い合わせ（外部報告者向け）：営業日（月曜日から金曜日、9:00～18:00、祝日を除く）に、セキュリティ緊急連絡電話（080-3270-8504）へお問い合わせいただけます。主に、報告手続きに関する質問への回答、脆弱性対応状況の確認等の問い合わせ対応に使用します。脆弱性の詳細情報を提出する場合は、完全な資料を記録・保管できるよう、公式ウェブサイトまたは専用メールアドレスを優先して利用することを推奨します。

内部連絡（内部テストチーム向け）：内部テストチームは、情報セキュリティ部の内線窓口（080-3270-8504）へ連絡し、脆弱性報告および対応進捗について随時確認できます。

3.4 郵送先住所（外部報告者向け）：

紙媒体の脆弱性報告書を書面で提出する必要がある場合は、当社情報セキュリティ部門の専用受取住所宛に郵送できます。

〒305-0816

茨城県つくば市学園の森二丁目 13 番地 67

書面による報告書には、機関報告者の場合は所属機関の公印を押印し、個人報告者の場合は本人の署名を付してください。また、関連する証明資料の写しを添付してください。物流情報を追跡できるよう、書留郵便または宅配便での送付を推奨します。

3.5 内部管理システム（内部テストチーム向け）：

内部テストチームは、当社が自社開発した「ESS 脆弱性管理プラットフォーム」（https://kabutotech.com/）を通じて、オンラインで脆弱性報告を提出できます。システムには標準化テンプレートが組み込まれており、テストシナリオ、脆弱性再現手順、テストデータ等の情報を所定の要件に従って入力する必要があります。提出後、内部脆弱性番号が自動生成され、情報セキュリティ部に共有されます。

4. 脆弱性報告要求事項

技術チームが脆弱性を迅速かつ正確に評価し、効率的に処理できるようにし、情報不足による処理期間の長期化を避けるため、報告者が提出する脆弱性報告には、以下の主要情報を含め、内容の真実性、正確性および完全性を確保する必要があります。

4.1 報告者情報

外部報告者：法人または団体の報告者は、正式な団体名称、法人番号、連絡担当者の氏名および職務、有効な連絡先（固定電話、電子メール、携帯電話番号）を提供する必要があります。個人報告者は、実名、本人確認書類番号（任意）および有効な連絡先（電子メール、携帯電話番号）を提供する必要があります。正確な連絡先の提供は、当社が適時にフィードバックおよび連絡を行うための重要な条件です。

社内テストチーム：テスト担当者の氏名、所属部門／テストチーム、社員番号、社内ネットワーク上の連絡先を提供する必要があります。チームによるテスト成果である場合は、チーム責任者および参加者を明記する必要があります。

4.2 製品情報

関係する BMS 製品の完全な型番（例：「BX-XXXX」）、ハードウェアバージョン番号（通常は機器本体または取扱説明書に表示）、ソフトウェアバージョン番号（機器管理画面で確認可能）、ファームウェアバージョン番号および具体的な実行環境を明確に記載する必要があります。これには、対応する電池セルの種類（例：三元系リチウム、リン酸鉄リチウム）、電池パック容量、連携する主制御機器の型番および OS バージョン、利用シーン（例：産業用蓄電、家庭用蓄電、新エネルギー車）等の重要情報が含まれます。社内テストチームは、テスト機器番号およびテスト環境バージョン（例：シミュレーションテスト環境／実機テスト環境）も追加で記載する必要があります。

4.3 脆弱性の詳細

外部報告者：脆弱性の具体的な位置（例：特定の機能モジュール、特定のコードロジック、特定の通信プロトコル）、発生条件（例：特定の操作手順、特定の入力パラメータ、特定の環境設定）および完全な再現手順を、詳細かつ明確に記載する必要があります。再現手順は実行可能なものであり、当社技術チームが記載内容に従って脆弱性を再現できる必要があります。可能な場合は、関連するテストコード、脆弱性発生時のスクリーンショット（重要情報を注記）、再現過程の動画（説明文付き）等の証拠資料を提供し、脆弱性評価の効率向上に協力することを推奨します。

社内テストチーム：テストケース番号、テスト実施時間、脆弱性発生時のログファイル、製品設計仕様からの逸脱点の説明を追加で提供する必要があります。再現手順にはテスト環境構築の詳細を含め、他のテスト担当者が 100%再現できるようにする必要があります。

4.4 リスク評価

外部報告者：自身の専門的判断に基づき、脆弱性がもたらし得る影響について初期評価を行うことができます。評価観点には、BMS の中核制御機能（充放電管理、過充電・過放電保護等）への影響、電池安全リスク（発火、爆発、膨張等）の有無、ユーザーの機微データ（電池運転データ、ユーザー識別情報等）の漏えいの有無、機器の不正制御またはサービス拒否につながる可能性等が含まれますが、これらに限定されません。また、CVSS 評価体系を参考に、初期的なリスクレベルを提示することができます。

社内テストチーム：会社の「BMS 脆弱性リスク評価細則」（社内文書）を厳格に参照し、CVSS 3.1 評価体系と組み合わせてリスクレベルを提示する必要があります。また、当該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／市場投入済み段階等）に影響するかを説明する必要があります。

4.5 修正提案

外部報告者：当該脆弱性に対して、具体的な修正方針または提案を提示することができます。例として、コードレベルの修正案（入力検証の追加、権限制御の改善等）、設定レベルの最適化措置（通信暗号化アルゴリズムの調整、デフォルトパスワードポリシーの変更等）、ハードウェアレベルの改善提案（セキュリティチップの追加等）または管理面の回避策等が含まれ、後続の修正作業の参考となります。

社内テストチーム：製品設計文書に基づき、実行可能な修正提案を提示する必要があります。暫定的な回避策によってリスク低減が可能かどうか、および修正案が製品性能や互換性に与える潜在的影響を優先的に明記します。

5. 脆弱性処理プロセスおよび概要

5.1 報告の受付および確認（1〜3 営業日）

当社情報セキュリティ部は脆弱性対応専門チームを設置し、専任者を指定して脆弱性報告の受付および初期審査を担当します。

外部報告：脆弱性専用メールおよび公式ウェブサイトのフィードバック窓口を 24 時間 365 日監視し、営業日には連絡電話および郵送先も併せて確認します。脆弱性報告を受領後、専門チームは 1〜3 営業日以内に初期審査を完了します。審査内容には、報告情報の完全性、脆弱性説明の明確性、当社製品の範囲に該当するか等が含まれます。報告情報が完全で要求を満たす場合、報告者に対し、当社情報セキュリティ部の公印を付した「脆弱性報告受領確認書」を送付します。同書には、報告番号、脆弱性の初期説明、受付時刻および後続処理プロセスの主要な節目を明記します。情報が不完全または曖昧な場合は、報告者が提供した優先連絡先を通じて、補足が必要な具体的情報リストを通知し、報告者による補足完了後に正式な受付確認を行います。

内部報告：社内テストチームから脆弱性報告を受領後、1 営業日以内に審査を完了します。情報が完全な場合は直ちに内部脆弱性番号を生成し、「内部脆弱性受領確認票」をテストチームに送付します。情報が不完全な場合は、社内ネットワークのインスタントメッセージツールを通じて補足要求を通知し、補足完了後 1 営業日以内に確認を完了します。

5.2 脆弱性評価および分類（3〜5 営業日）

外部脆弱性：情報セキュリティ部は脆弱性評価専門委員会を組織します。委員会の構成員には、BMS 中核研究開発エンジニア、シニアセキュリティテストエンジニア、システムアーキテクトおよび外部委託のサイバーセキュリティ専門家が含まれ、受領確認済みの脆弱性について包括的な技術評価を実施します。評価では、脆弱性の影響範囲（関係製品数、ユーザー規模等）、影響の重大性（人身安全への影響、経済的損失等）、悪用難易度（専門技術や特殊ツールの必要性等）、公開された悪用コードの有無

等を考慮し、CVSS 3.1 評価体系を厳格に参照して定量評価を行い、最終的に高・中・低の 3 段階に分類します。

内部脆弱性：情報セキュリティ部、研究開発責任者およびテストチーム代表による評価チームを構成します。分類基準は外部脆弱性と同一（高／中／低リスク）ですが、当該脆弱性が量産工程または市場投入済み製品に影響するかを追加で評価する必要があります。研究開発段階の脆弱性である場合、分類後ただちに研究開発修正プロセスに移行し、ユーザー通知手続きは開始しません。

脆弱性レベルの分類基準：

（1）高リスク：CVSS スコアが 9.0～10.0 であり、BMS の充放電制御、熱管理等の中核機能が完全に失効し、電池の発火・爆発、電解液漏えい等の安全事故を直接引き起こす可能性があるもの。または、ユーザー識別情報、電池運転の中核データ等の機微情報が大規模に漏えいするもの。または、攻撃者が遠隔から未認可で機器を制御し、悪意ある操作を実行でき、かつ悪用難易度が低く、広範な拡散リスクを有するもの。

（2）中リスク：CVSS スコアが 6.0～8.9 であり、BMS の均衡管理、データ取得等の一部機能に異常を生じ、電池の充放電効率低下、寿命短縮等の問題を引き起こす可能性があるもの。または、中核ではない機器運転ログ、基本設定情報等のデータ漏えいにつながるもの。または、特定条件下でのみ機器の局所的性能低下を引き起こし、悪用難易度が中程度で一定の専門技術能力を要するもの。

（3）低リスク：CVSS スコアが 0.1～5.9 であり、BMS 画面表示異常、非重要パラメータの誤差等の軽微な機能不備にとどまり、中核安全機能に影響しないもの。または、極めて特殊なハードウェア設定、ソフトウェア環境および操作手順下でのみ発生する可能性があり、システム全体の安全性への影響が極めて小さく、悪用難易度が非常に高く、実質的な攻撃価値をほとんど有しないもの。

評価完了後、当社は 3～5 営業日以内に、対応する窓口を通じて報告者へ評価結果を通知します。外部報告者には「脆弱性評価結果通知書」を、社内テストチームには「内部脆弱性評価結果票」を送付します。文書には、脆弱性レベル、CVSS の具体的スコアおよび根拠、脆弱性の技術分析結論、潜在的リスク分析ならびに後続修正作業の初期スケジュールを詳細に記載します。

5.3 脆弱性の修正および検証（脆弱性レベルに応じて決定：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）

当社は、脆弱性のレベルに応じて、対応する優先順位の修正プロセスを開始します。

（1）高リスク脆弱性：直ちにレベル 1 緊急対応を開始し、会社技術責任者が主導して緊急修正専門チームを設置します。非緊急の研究開発業務を一時停止し、中核研究開発・テストリソースを優先的に配

分して脆弱性修正を行います。修正案は、評価専門委員会（外部脆弱性）または評価チーム（内部脆弱性）の審査承認を経た後に開発段階へ進めます。修正開発完了後、情報セキュリティテストチームが複数回のペネトレーションテスト、ストレステストおよびシナリオシミュレーションテストを実施し、脆弱性が完全に解消され、新たなセキュリティリスクが発生していないことを確認します。社内テストで発見された研究開発段階の高リスク脆弱性については、研究開発チームが 24 時間以内に修正を開始し、3〜7 営業日以内に検証を完了する必要があります。

（2）中リスク脆弱性：レベル 2 対応を開始し、月次重点修正計画に組み込みます。研究開発部門が専任プロジェクトチームを指定して修正作業を担当します。修正案は部門技術責任者の審査を受け、開発完了後に通常のセキュリティテストおよび機能検証を実施し、修正効果を確保するとともに、製品の既存機能の安定性に影響しないことを確認します。

（3）低リスク脆弱性：レベル 3 対応を開始し、製品の改良計画または四半期ごとのセキュリティ更新と組み合わせて段階的に修正します。脆弱性の修正コストが高く、影響が極めて小さい場合は、詳細なリスク回避ガイドを作成し、ユーザー（外部脆弱性）または社内利用部門（内部脆弱性）に提供することができます。後続製品にバージョン更新計画がある場合は、脆弱性修正を更新内容に組み込み、製品反復の過程で改善を完了します。

検証要件：外部脆弱性の修正完了後は、情報セキュリティテストチームが独立して検証を行います。内部脆弱性の修正完了後は、脆弱性を提出したテストチームが一次検証を行い、検証通過後に情報セキュリティテストチームが二次のクロス検証を実施して、脆弱性が完全に修正されたことを確認します。修正および検証の完了後、当社は正式な「脆弱性修正報告書」（外部脆弱性）または「内部脆弱性修正確認報告書」（内部脆弱性）を作成します。報告書には、脆弱性の元情報、修正案の詳細説明、開発過程記録、テスト計画およびテスト結果、修正後のバージョン情報、導入・更新ガイド等の完全な資料を含め、情報セキュリティ部が保管します。

5.4 コミュニケーション・フィードバックおよび免責説明

コミュニケーション・フィードバック：脆弱性処理の全過程において、当社は専用のコミュニケーション体制を構築します。外部報告者とは電子メール／電話で連絡を維持し、高リスク脆弱性については 3 営業日ごとに修正進捗をフィードバックし、中・低リスク脆弱性については 7 営業日ごとにフィードバックします。社内テストチームは「BMS 脆弱性管理プラットフォーム」を通じて進捗をリアルタイムで確認でき、高リスクの内部脆弱性については毎日修正進捗を同期し、中・低リスク脆弱性については 3 営業日ごとに同期します。報告者から合理的な質問または補足提案があった場合、担当窓口は 2 営業日以内に詳細に回答します。

免責説明：本ポリシーの要求事項を厳格に遵守し、脆弱性報告提出後に第三者へ脆弱性情報を漏えいせず、脆弱性を利用した攻撃テストまたは不正な利益取得を行わない善意の外部報告者について、当社は、脆弱性発見過程における合法的なテストに起因する関連法的責任を追及しないことを約束します。社内テストチームが合法かつ適法なテスト範囲内で脆弱性を発見し報告した場合は、通常の職務遂行とみなし、会社は規範に沿った機器操作に関する責任を追及しません。外部報告者または社内テスト担当者が、機器を故意に破壊する、悪意ある第三者に脆弱性情報を漏えいする、脆弱性を利用して不正にデータを取得する、またはシステム運用を破壊する等の行為を行った場合、当社は関連証拠を収集し、民事、行政または刑事責任を追及する権利を留保します（社内関係者については会社の「従業員違反処理規程」に従って併せて責任を追及します）。

6. 脆弱性修正前の状態更新処理プロセスおよび概要

6.1 脆弱性調査および対応開始（評価完了後 1 営業日以内）

脆弱性評価結果が確定した後、当社情報セキュリティ部は 1 営業日以内に、研究開発、生産、販売等の部門と連携して、対象を絞った調査を開始します。

外部脆弱性および社内で発見され量産工程または市場投入済み製品に影響する脆弱性：生産記録を通じて、脆弱性に関係する製品ロット、生産日および販売地域を追跡します。ユーザー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集計します。技術分析を通じて、脆弱性の発生確率および潜在的影響範囲を明確にします。高リスク脆弱性については直ちに緊急対応体制を開始し、専門チームが暫定的な防護措置を策定します。これには、緊急設定変更ガイドの提供、関連するリスクポートの閉鎖、一部高リスク機能の一時停止等が含まれます。中・低リスク脆弱性については、実際のリスク程度に応じて詳細な調査スケジュールおよび対応案を策定し、リスクを管理可能な範囲に保ちます。

社内研究開発段階の脆弱性：当該脆弱性が前段階のテストで見落とされたか、対応するテスト工程にプロセス上の欠陥があるかを追加で調査し、「テストプロセス最適化提案」を作成して品質管理部へ共有し、同種問題の再発を防止します。

6.2 状態管理および社内同期

電子台帳と紙台帳による二重管理の脆弱性状態記録体系を構築します。電子台帳は暗号化データベースで保存し、脆弱性の報告番号、報告者情報、製品情報、評価結果、修正進捗、暫定防護措置、影響範囲、ユーザー通知状況等の重要情報をリアルタイムで記録します。情報セキュリティ部の専任者が毎日更新・維持を担当します。電子台帳では「内部発見脆弱性」と「外部報告脆弱性」を区分し、内部脆弱性の発見工程、修正率、再テスト通過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」を作成し、研究開発、生産、販売、カスタマーサービス、品質管理等の関連部門責任者へ共有します。これにより、各部門が脆弱性状況を適時に把握し、ユーザー通知、アフターサポート、プロセス最適化等の対応を連携して実施し、情報の分断を防止します。

6.3 状態公開およびユーザー通知

（1）高リスク脆弱性（外部脆弱性および社内で発見された市場投入済み高リスク脆弱性）：評価完了後、暫定防護措置を策定してから 2 営業日以内に、公式ウェブサイトのセキュリティ告知欄（上部固定表示）、製品アプリのプッシュ通知（強制ポップアップ通知）、SMS 通知（携帯電話番号を登録済みのユーザー向け）、電子メール通知（法人ユーザー向け）等の複数チャネルを通じて、影響を受けるユーザーへ脆弱性状況を同時に通知します。通知内容には、脆弱性の基本説明、潜在的リスク、暫定防護措置（操作手順、設定変更方法等）および修正進捗の予定節目を含めます。その後、脆弱性修正完了まで、同一チャネルで 3 営業日ごとに修正進捗を更新します。

（2）中リスク脆弱性（外部脆弱性および社内で発見された市場投入済み中リスク脆弱性）：評価完了後 5 営業日以内に、公式ウェブサイトのセキュリティ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、脆弱性の概要（脆弱性の種類および影響の簡潔な説明）および修正計画（予定修正完了時期、更新方法を含む）をユーザーへ通知します。その後、7 営業日ごとに公式ウェブサイトで進捗を更新し、ユーザーが容易に確認できるようにします。

（3）低リスク脆弱性（外部脆弱性および社内で発見された市場投入済み低リスク脆弱性）：脆弱性が軽微な画面不備にとどまり、ユーザー利用に実質的影響を与えない場合、修正完了後に公式ウェブサイトで四半期セキュリティ更新の一括告知を発行し、脆弱性修正状況を一括して説明することができます。一定の潜在的影響があるもののリスクが低い場合は、評価完了後 10 営業日以内に公式ウェブサイトのセキュリティ告知欄で基本状況および修正予定をユーザーへ通知し、高頻度の更新は不要とします。

（4）社内研究開発／量産段階で市場投入前の脆弱性：外部ユーザーへの通知は不要とし、「BMS 脆弱性管理プラットフォーム」および「脆弱性対応週次進捗報告」で状態を同期し、社内関連部門が情報を把握できるようにします。

6.4 報告者へのフィードバック

脆弱性修正前に、当社は所定のコミュニケーション頻度に従い、報告者へ詳細な脆弱性処理進捗をフィードバックします。

外部報告者：フィードバック内容には、調査段階における製品影響範囲の集計結果、暫定防護措置の具体内容および実施効果、修正案の策定方針および審査状況、開発進捗ならびに発生している技術的課題等が含まれます。

社内テストチーム：テストプロセス最適化提案の実施状況、脆弱性に関連するテストケースの更新進捗を追加でフィードバックします。

報告者が脆弱性状態について自発的に問い合わせた場合、担当窓口は 2 営業日以内に対応チャネルを通じて詳細に回答し、具体的な処理段階を示す証明資料を提供します。脆弱性修正完了後は、速やかに報告者へ「脆弱性修正完了通知書」（外部）または「内部脆弱性修正完了確認書」（内部）を送付し、修正報告書の要約を添付するとともに、修正効果の検証を正式に依頼します。報告者からの検証意見は、最終的なクローズ処理の重要な根拠とします。

7. その他の説明

7.1 ポリシー更新

本ポリシーは、BMS 技術の進展（新型通信プロトコルの適用、スマート機能の高度化等）、サイバーセキュリティ関連法令および業界標準の変化、会社の実際の運用過程における経験、ならびに社内テストプロセス最適化の必要性に応じて適時改訂します。改訂前には、社内の技術、法務、市場、品質管理、テストチームおよび外部セキュリティ専門家の意見を求めます。改訂完了後は、公式ウェブサイトのセキュリティ専用セクションおよび社内ネットワークで更新のお知らせを発行し、改訂内容および発効日を明記します。改訂後のポリシーは公開日から発効し、旧ポリシーは同時に廃止され、ユーザー、外部報告者および社内従業員がポリシー変更を適時に把握できるようにします。

7.2 脆弱性開示に関する説明

脆弱性開示ポリシーの公開を予定する場合、評価機関に対し、証拠（Evidence）として以下の資料を提供し、評価要件を満たすための関連記録を完了する必要があります。

（1）公開予定日：明確なポリシー公開日を提示する必要があります。当該日は、製品の正式市場投入・販売日の少なくとも 7 営業日前でなければなりません。また、会社内部で承認済みの製品市場投入計画文書の写し（公開日を注記）を添付します。

（2）公開方法および場所：当社公式ウェブサイト［https://kabutotech.com/］のセキュリティ専用セクションを主要公開チャネルとすることを明確に説明します。併せて、製品市場投入時の取扱説明書を同期配信し、ユーザーが容易に取得できるようにすることを補足できます。

（3）公開予定の脆弱性開示ポリシー：完全なポリシー草案を提供する必要があります。草案内容は本ポリシーの中核フレームワークと一致している必要があり、公開予定の対象製品については、草案内で調整箇所および理由を明確に記載し、必要に応じて調整根拠を説明する別添資料を添付できます。

7.3 連絡先および問い合わせ

本ポリシーの条項理解、実行プロセスまたは具体的な操作について疑問がある場合、外部報告者およびユーザーは、本ポリシーに記載された公式ウェブサイトのお問合せフォーム、専用メールアドレス、電話等のいずれかのチャネルを通じて当社情報セキュリティ部に連絡できます。社内従業員およびテストチームは、情報セキュリティ部の内線、社内ネットワークのメッセージまたは「BMS 脆弱性管理プラットフォーム」の問い合わせセクションを通じて連絡できます。情報セキュリティ部は 2 営業日以内に問い合わせ内容を分類処理し、複雑な問題については専門的な検討を組織した上で回答し、問い合わせに適切に対応します。

7.4 社内インセンティブ制度

社内テストチームが高リスクまたは重大なセキュリティ脆弱性を発見した場合、会社は「研究開発およびテストインセンティブ規程」に基づき、現金報奨、業績評価加点または表彰選考での優先資格を付与します。脆弱性発見件数、修正検証効率、テストプロセス最適化への貢献が基準を満たしたチームには、四半期ごとに特別報奨を支給し、社内テストチームが BMS セキュリティ保護業務へ主体的に参加することを促進し、製品のセキュリティ品質を向上させます。

カブトテック株式会社

法定代表者／権限代表者署名：　當眞大貴　