蓄電 IoT 統合システム製品の脆弱性公開に関するポリシー（ウェブ公開版）

一、 ポリシー概要

当社はプロフェッショナルな蓄電システムインテグレーション企業であり、蓄電システム全体の設計およびインテグレーションサービスを主軸事業としています。当社の**蓄電 IoT 統合システム（エッジゲートウェイ＋BMS 通信トポロジアーキテクチャ）**シリーズ製品のサイバーセキュリティリスク管理を規範化し、脆弱性の受け付け、検証、修正、開示、およびクローズドベース管理の標準化されたメカニズムを確立するため、また、蓄電現場の機器、通信リンク、バックエンド管理システムおよびユーザーデータの安全性を保障するため、JC STAR S1.1-05『脆弱性報告管理』の規範要件に基づき、本『蓄電 IoT 統合システム製品の脆弱性公開に関するポリシー』を特にお定めます。

本ポリシーは、セキュリティ研究者、業界パートナー、エンドオーナー、および保守運用者に向けて公開されるものであり、合法的なセキュリティ研究の境界、脆弱性の報告窓口、対応スピード、進捗の同期メカニズム、機密保持ウィンドウ期間、およびコンプライアンス免責規則を明確にし、蓄電システムのサイバーセキュリティ・コンプライアンス運営に対して、公開・透明化された制度的根拠を提供するものです。

二、 適用範囲

（一）適用製品およびシステムアーキテクチャ

本ポリシーは、当社が自社開発およびインテグレーションを行う蓄電 IoT 統合システム（エッジゲートウェイ＋BMS 通信トポロジアーキテクチャ）全シリーズの製品、およびこれらに付随するソフトウェア・ハードウェア、通信リンク、バックエンド服務に適用されます。具体的には以下を含みます：

- **蓄電システム全体のアーキテクチャ：** 工業用ルーターをエッジゲートウェイとし、BMS（バッテリーマネジメントシステム）をコアコントロールとする分散型/集中型蓄電システム。これには、バッテリークラスター、BMS システム、通信ゲートウェイ、エッジデータ収集機器、消防システム、冷却システムなどの現場機器一式が含まれます。
- **通信ネットワーク機器：** 蓄電専用の工業用ルーターであるエッジゲートウェイ、現場の通信ネットワーク構築機器、および対応する通信プロトコルサービス。
- **BMS（バッテリーマネジメントシステム）：** バッテリー状態の収集、バランス制御、過電圧/不足電圧/過電流保護、温度監視、故障アラート、データ報告、エッジゲートウェイを介したリモートコントロール、ローカル HMI ディ

スプレイへのログイン、ローカルパラメータ設定権限など、BMS のソフトウェア・ハードウェア機能モジュール一式。

- **全リンクのデータインタラクション：** ESS 現場機器とゲートウェイの間、およびゲートウェイとローカル EMS の間の通信リンク、データ転送プロトコル、暗号化認証メカニズム、およびビジネスロジック。
- **関連プラットフォームとサービス：** リモートデバッグシステム（EMS を通じて実現)、データ収集および報告インターフェース、ならびにサードパーティ連携サービス。

（二）非受理範囲

安全テストの境界を明確にするため、以下のシナリオは本ポリシーにおけるセキュリティ脆弱性の受理範囲に含めないものとします：

- 蓄電バッテリー、BMS ハードウェア、工業用ルーターに対して、物理的な分解、ハードウェアの改造、物理回線の破壊を行わなければ問題を再現できない場合。
- ユーザーが私的にネットワークトポロジを改造したり、機器を無断で接続したり、公式パラメータを変更したり、規約違反の保守運用操作を行ったりしたことに起因する安全リスク。
- 現在の最新安定版（最新スタブルバージョン）で修正済みの脆弱性。
- 一般的なネットワーク帯域の混雑、現場の施工環境の不具合、キャリア回線の中断など、製品設計に起因しない問題。
- サービス拒否攻撃（DoS/DDoS)、過度な負荷テスト（ストレスチェック)、トラフィック爆撃などの破壊的なテスト行為によって引き起こされたシステム異常。
- 一般的なブラウザの互換性の問題、ビジネス機能に関わらない UI 表示の問題など、権限、データ、制御権限に関わらない一般的な機能上の瑕疵。
- 当社に対する事前の書面による報告および授権（許可）を得ていない、悪意のあるペネトレーションテスト、データ窃取、バックドアの植え付け、ネットワーク内での横展開（ラテラルムーブメント）などの規約違反のテスト行為。

三、 脆弱性の公式報告窓口

唯一の公式脆弱性受理メールアドレス：serviceess@tws.com

本メールアドレスは、当社の蓄電システム製品におけるセキュリティ脆弱性の唯一

の公式受理窓口であり、すべての脆弱性報告、安全に関する相談、ポリシーの確認、開示延期の申請は、本メールアドレスを通じて提出される必要があります。テキスト、リッチテキスト、添付の圧縮ファイル形式に対応しています。情報の安全性を保障するため、機密性の高い脆弱性資料は暗号化して提出することをお勧めします。

脆弱性報告に含めることを推奨する内容

- **脆弱性が所属する製品：** 蓄電 IoT 統合システムの型式、エッジゲートウェイ＋BMS トポロジに対応する機器モジュール、ファームウェア/ソフトウェアのバージョンを明記。
- **脆弱性の詳細な説明：** 問題の原理、トリガー条件、完全な再現手順、影響を受ける通信リンクおよび管理制御機能。
- **リスクと危害の説明：** BMS データの改ざん、機器の制御喪失、通信の乗っ取り、データ漏洩、リモート特権昇格（権限越え）、システムの機能停止などのリスクを招く可能性があるか否か。
- **裏付け資料：** 脆弱性のスクリーンショット、操作の録画画面、ログ記録、POC（概念実証）検証スクリプト、トポロジ問題の説明ドキュメントなど。
- **報告者の情報（任意）：** 氏名、所属機関、連絡先。匿名による報告も受け付けます。

添付ファイルの提出規範

- ZIP、7Z、GZIP などの一般的な安全な圧縮形式に対応しています。
- テストスクリプトや検証コードはアーカイブ（パック）してアップロードしてください。実行可能な悪意のあるプログラムを直接送信することは禁止します。
- アーカイブの作成、確認をスムーズに行うため、製品バージョンや脆弱性タイプを明記し、明確なファイル名を付けてください。

四、 脆弱性の受け付けおよび対応プロセス

当社は、JC STAR S1.1-05 の要件を厳格に遵守し、標準化された脆弱性対応のクローズドベースフローを構築し、対応スピードと各ノードを明確にすることで、脆弱性の追跡可能性、管理可能性、および修正可能性を保障します。

1. **5 営業日以内の受領確認：** 脆弱性の報告メールを受信後、当社のセキュリティチームは 5 営業日以内に受領受領書（受領確認メール）を返信し、報告の受信を確認して専任の担当者を割り当て、正式に対応プロセスを開始しま

す。

2. **脆弱性の有効性検証：** 蓄電 IoT 統合システムの通信トポロジ、BMS の管理制御ロジック、エッジゲートウェイの転送メカニズム、バックエンドの権限メカニズムを対象に技術的な再現と検証を行い、脆弱性の真実性、リスクレベル、および影響範囲を判定します。無効な問題やセキュリティに関わらない問題については、却下の理由および判定の根拠を明確に通知します。

3. **脆弱性の修正と是正：** 有効と確認された安全上の脆弱性に対して、エッジゲートウェイの通信ポリシー、BMS プロトコルの検証メカニズム、データの暗号化ロジック、権限アクセス制御、インターフェース保護、ファームウェアのセキュリティ強化などの観点から修正案を策定し、セキュリティファームウェア、システムパッチ、およびバージョンアップデートを繰り返しリリースします。

4. **検証のクローズおよびバージョンのリリース：** 修正完了後、内部テストおよび回帰検証を実施し、脆弱性が完全に修正されたことを確認した上で、正式にアップグレードバージョンをリリースし、製品のセキュリティ説明を同時に更新して、脆弱性対応をクローズします。

五、 脆弱性進捗の同期メカニズム

脆弱性修正の全ライフサイクルにおいて、当社は報告者に対して対応の進捗を継続的に同期します。主要なノードには、受領確認、脆弱性の検証結果、リスクレベルの判定、修正案のスケジュール、パッチ開発、内部テスト、正式リリースが含まれます。トポロジ情報、機器のバージョン、テスト環境資料の追加が必要な場合、当社から主体的にメールで連絡を取り、連携を図ります。

報告者の書面による許可がない限り、当社は報告者のプライバシー情報を外部に開示することはありません。必要であり、かつ授権（許可）を得ていることを前提とする場合に限り、影響を受ける顧客や保守運用ユニットに対して、対応する蓄電システムのリスクおよびアップグレード案を同期します。

六、 脆弱性の機密保持および公開ウィンドウ期間の規則

当社が脆弱性の受領確認メールを発信した当日から起算して、デフォルトで 120 日間の公式機密保持ウィンドウ期間を設定します。ウィンドウ期間中、報告側はいかなる第三者、公開コミュニティ、オンラインプラットフォームに対しても、当該脆弱性の完全な技術的詳細、再現方法、およびリスクの原理を開示してはなりません。

ウィンドウ期間内に当社が脆弱性の修正を完了し、正式なセキュリティバージョンをリリースした場合、双方で協議の上、合意に達した後に脆弱性情報を外部に公開

することができます。120 日間のウィンドウ期間内に繰り上げて開示する必要がある場合は、必ず事前に当社に書面による申請を提出し、公式な正式同意を得た上で公開しなければなりません。

七、 セキュリティ研究の行動規範および免責事項

（一）許容される善意のセキュリティ研究行為

非破壊的な前提において、当社の公開テスト環境にある蓄電 IoT 統合システム（エッジゲートウェイ＋BMS 通信トポロジ）を対象にコンプライアンスに則った脆弱性検証を行うことに限定されます。これは脆弱性の存在を確認することのみを目的とするものであり、悪意のある攻撃、不法な制御、およびデータの窃取に用いてはなりません。

（二）厳格に禁止される行為

- 蓄電現場の機器の稼働を破壊すること、BMS の正常な管理制御ロジックを妨害すること、エッジゲートウェイの通信を遮断すること、およびシステムを停止させること。
- 蓄電システムの稼働データ、バッテリーの状態データ、ユーザーの設定情報を改ざん、削除、または窃取すること。
- 機器、ゲートウェイ、システム内に悪意のあるプログラムを植え付けること、持続的なバックドアを構築すること、および社内ネットワークへ横展開（ラテラルムーブメント）すること。
- ソーシャルエンジニアリングによるフィッシング、嫌がらせ、詐欺類のテスト行為を行うこと。
- 許可なく、未修正の蓄電システムの脆弱性の詳細を事前に公開または拡散すること。

（三）コンプライアンス免責

セキュリティ研究者が本ポリシーの境界を厳格に遵守し、善意を持って報告を行い、脆弱性情報を事前に漏洩せず、業務や機器に損失を与えていない場合、当社はその研究行為がコンプライアンスに準拠していると認め、関連する法的責任を追及しません。

八、 知的財産権およびデータに関する義務

報告者が提出した脆弱性報告書、技術文書、検証材料について、デフォルトで当社に対し、永久的、無償、非独占的であり、製品の最適化、修正・改善、コンプライアンス公示に使用できる使用権を授与するものとします。提出される材料は、第三

者の知的財産権に関する紛争がないことを保証する必要があり、侵害問題が発生した場合は、提出側が自らその責任を負うものとします。

テストの過程で一時的に取得した非公開データは、今回の脆弱性検証のみに使用し、研究終了後は直ちに完全に削除しなければならず、私的に保存、転送、または公開してはなりません。

九、 ポリシーに関する相談および確認

テストの境界、脆弱性の受理範囲、開示ウィンドウ期間、コンプライアンスに関する疑問については、すべて公式の脆弱性メールアドレスを通じて相談を立ち上げることができます。セキュリティテストを開始する前に、コンプライアンスに準拠しているか確認できない場合は、コンプライアンスリスクを回避するため、必ず事前にメールで確認を行ってください。

十、 ポリシーの効力に関する説明

本ポリシーは日本地域の関係者を対象とするものであり、日本語版のみで外部に公示されます。当社は、製品のアップデートやコンプライアンスの要件に基づき、本ポリシーを改定・更新する権利を留保します。