

SAMSUNG SDI

電池システムの脆弱点公開ポリシー

(Vulnerability Disclosure Policy)

2025年08月27日



SAMSUNG SDI

1. 目的

SAMSUNG SDIは安全性と信頼を基盤に当社のシステムとアプリケーションで発生しうる。

潜在的なセキュリティ脆弱性について公開政策を策定し、顧客、研究者およびパートナーが脆弱点を発見時報告出来る窓口を通して受付から解決策まで内部Processに基づき円滑な解決を提供することを約束します。

これに対し本政策は当社の製品とサービスに関連する脆弱性を報告する方法とこれに対する当社の対応方針をご案内します。

2. 連絡先

エネルギー貯蔵製品の脆弱性が見つかりましたら、次の窓口にお問い合わせください。

- 専用メール: sdi.security.ess@samsung.com
- 専用電話: +81-(0)3-6369-6404 (平日 9:00~17:00 日本標準時間)
- 公式ウェブサイト: <https://www.samsungsdi.com/>
- 当社の窓口にお問い合わせの際、以下の情報をご連絡願います。
 - ※ 該当製品の型式 / バージョン
 - ※ 脆弱性関連詳細説明と影響範囲
 - ※ 再現手順 (Screen Shotまたは実証結果がある動画等)
 - ※ 報告者の連絡先 (御氏名、メール、連絡先)

SAMSUNG SDIは報告者の個人情報を保護します。

3. 脆弱性内容受付および処理プロセス

SAMSUNG SDIは脆弱性関連内容報告書を受付後、次段階に応じ対応し、進行状況は報告者に共有します。

- 受付確認: 受付後5営業日以内に受付確認し、返信します。
- 分析と検証: 脆弱性関連の影響範囲とリスク レベルを評価し、有効性を検証します。
- 解決および措置: ファームウェアの更新、パッチなどの適切な措置をとらせて頂きます。緊急性に応じて措置の優先順位を決定します。
- 公開: 修正完了後に報告者に結果を通知し、必要に応じてセキュリティ公告を公開させていただきます。

4. 脆弱性の処理と公開

脆弱性が完全に修正されるまでSAMSUNG SDIは使用者に危険状況と一時的な防御策をホームページを通じて公示します。脆弱性の報告が修正されると、公式ウェブサイトと個別のメールを通じて脆弱性の内容を公開します。

公開情報

- 脆弱性の概要（悪用可能な詳細情報を除く）
- 影響を受ける製品範囲およびバージョン
- アップデート手続きおよび対応方案

5. 脆弱性報告ガイドライン

当社は脆弱性の報告者に対し下記事項に対する協力を要請します。個人情報および顧客情報の侵害、データ破壊、サービス妨害、報告者に所有権のないデータの変更など業務を妨げる可能性のある行為を禁止してください。状況によっては脆弱性の問題解決のために時間がかかることもあることをご了承の上、問題の解決まで対外的な開示を行ってはなりません。

6. 免責事項

当社は、本政策を遵守する限り、善意の報告者に対して法的措置を取りません。

- 以上 -

SAMSUNG SDI

Vulnerability Disclosure Policy

August 27, 2025



1. Purpose

SAMSUNG SDI has established a Vulnerability Disclosure Policy based on safety and trust to address potential security vulnerabilities that may arise in our systems and applications. We are committed to providing a clear channel through which customers, researchers, and partners can report discovered vulnerabilities, and to ensuring smooth resolution from initial reporting to remediation in accordance with our internal processes.

Accordingly, this policy outlines how to report vulnerabilities related to our products and services, as well as our approach to responding to them.

2. Contact Information

If you have identified a vulnerability in our ESS products, please contact us through the following channels.

- Dedicated Email: sdi.security.ess@samsung.com
- Dedicated Phone: +81-(0)3-6369-6404 (Weekdays 9:00~17:00 JST)
- Official Website: <https://www.samsungsdi.com/>
- When contacting us, we kindly request that the following information be included.

- ※ Product model or version
- ※ Detailed description of the vulnerability and its potential impact
- ※ Steps to reproduce (e.g. screenshots or demonstration videos)
- ※ Reporter's contact information (e.g. name, email address, phone number)

SAMSUNG SDI ensures the protection of the reporter's personal information.

3. Submitting Vulnerability Reports and Handling Process

Upon receiving a vulnerability report, SAMSUNG SDI responds according to the following steps, and the progress will be shared with the reporter.

- Report Acknowledgement: Within 5 business days, we will acknowledge that your report has been received.
- Analysis and Verification: Assess the scope of impact and risk level of the reported vulnerability, and verify its validity.
- Resolution and Remediation: Take appropriate actions such as firmware updates or patches, and determine the priority of actions based on urgency.
- Disclosure: Notify the reporter once remediation is complete, and issue a security advisory if necessary.

4. Vulnerability Handling and Disclosure

Until a reported vulnerability is fully resolved, SAMSUNG SDI will notify users of the risk and provide temporary mitigations through its official website. Once the vulnerability has been remediated, the details will be disclosed via the official website and individual email notifications.

Disclosure Information

- Overview of the vulnerability (excluding details that could be exploited)
- Scope of affected products and versions
- Update procedures and mitigation measures

5. Vulnerability Report Guidelines

We kindly request the following cooperation from vulnerability reporters. Please refrain from any actions that may disrupt operations, such as compromising personal or customer information, destroying data, disrupting services, or altering data that does not belong to you. We also ask for your understanding that resolving vulnerabilities may take time depending on the situation, and request that you refrain from any public disclosure until the issue has been fully addressed.

6. Disclaimer

We will not take legal action against good-faith reporters who comply with this policy.

End of Document