I. 概要

Panasonic Product Security Incident Response Team（Panasonic PSIRT）は、パナソニックグループが開発した製品に関して報告された脆弱性情報のコーディネーションを「パナソニック 脆弱性情報コーディネーションポリシー」に沿って実施します。

パナソニックグループが、脆弱性情報を公開する目的は、開発している製品のセキュリティを向上すること、および製品に含まれる脆弱性がもたらすリスクを軽減するための適切な対策をユーザに伝えることにあります。

パナソニックグループでは、報告された脆弱性に影響のある製品に対して脆弱性対策を施し、「パナソニック 脆弱性情報開示ポリシー」に従って公開します。

本ドキュメントには、パナソニックグループの脆弱性情報に関するコーディネーションおよび開示のポリシーが含まれています。

本ポリシーは予告なく変更されることがあります。

II. 脆弱性情報コーディネーションポリシー

A）脆弱性情報を Panasonic PSIRT に報告するには：

-脆弱性情報を product-security@gg.jp.panasonic.com まで送付

もしくは

-脆弱性報告フォーム https://www.panasonic.com/global/corporate/product-security/sec/psirt/jp.html を利用してください

メールによる送付には、PGP の利用を推奨しています。Panasonic PSIRT の PGP 鍵は以下の URL から入手できます：

Panasonic PSIRT PGP Public Key
https://www.first.org/members/teams/panasonic_psirt

上記の連絡方法で脆弱性情報の報告を受け付けてから 3 営業日以内に Panasonic PSIRT は報告者に受領した旨を連絡します。また、善意の報告には Panasonic PSIRT から報告者に対して訴えを起こすことはしません。

B）脆弱性の定義

本ポリシーにおいて、脆弱性とは、ソフトウエア、ハードウエア、ファームウエアなどの製品に含まれるプログラム上の不具合や設計上のミス（Computational Logic・演算ロジック）が原因で、機密性、完全性もしくは可用性に悪影響を与える攻撃可能なシナリオが一つ以上あるものと定義します。

C）脆弱性情報の報告に必要な事項

1. 影響を受けるソフトウエアもしくは製品モデルのバージョン（製品のリンクも含む）
2. 脆弱性の発見に至った経緯（使用したツールも含む）
3. 実証コード（PoC）もしくは脆弱性の再現手順
4. 脆弱性を悪用した際の影響もしくは脆弱性を悪用したシナリオを示す脅威モデル

脆弱性を報告する際、コーディネーションする上で留意すべき（カンファレンスなどでの講演や論文の公開のための)時間的制約があれば、併せてお伝えください。

報告された脆弱性情報を分析したのち、Panasonic PSIRT は脆弱性の影響を受けるパナソニックグループの開発部門とディスカッションを行い、コーディネーションの対象となる本ポリシーで定義されている脆弱性か否かを報告者に通知します。

報告された脆弱性情報は、コーディネーションの状況などを含め Panasonic PSIRT および パナソニックグループの開発部門で適切に管理します。

Panasonic PSIRT およびパナソニックグループの開発部門からの確認事項があれば報告者に質問を行う事があります。また、報告者からの問い合わせがあれば、適切に対応いたします。

D）報告された脆弱性がサードパーティ製のライブラリ・コンポーネントに起因した場合の Panasonic PSIRT の対応

報告された脆弱性を分析する中で、脆弱性による影響が（パナソニックグループ外の）サードパーティが開発するライブラリ・コンポーネントに起因することが発覚した場合、Panasonic PSIRT は、サードパーティのライブラリ・コーポーネントを使用したパナソニックグループの開発部門と連携して、該当のサードパーティとコーディネーションを行います。

Panasonic PSIRT は、必要に応じて調整機関と脆弱性情報のコーディネーションを行うこともあります。その際に Panasonic PSIRT は、報告者に対し事前に連絡を行います。

III. 脆弱性情報開示ポリシー

Panasonic PSIRT は報告された脆弱性情報に対し、該当するパナソニックグループの開発部門と公開に向けたコーディネーションを行います。パナソニックグループの事業部において脆弱性対策が準備出来次第、公開します。パナソニックグループでは、公開される情報の中に攻撃コードやハッカーなどの攻撃者に有利となる情報を含まないようにします。

脆弱性情報の報告者から要望があった場合、Panasonic PSIRT は MITRE Corporation もしくは別の CNA（CVE Numbering Authority / CVE 採番機関）と調整を行い、公開する脆弱性に対し CVE 番号を取得します。この CVE 番号は Panasonic PSIRT から報告者に伝えます。

[変更履歴]

2021/11/1	初版公開
2025/4/1	「II. 脆弱性情報コーディネーションポリシー」に追記・用語の統一
2025/5/8	「II. 脆弱性情報コーディネーションポリシー」に追記