



Federal Office  
for Information Security

# 技術ガイドライン - TR03183 : 製造者及び製品に対する サイバーレジリエンス要件

パート 3 : 脆弱性レポートと通知



# 文書履歴

表 1 : 文書の履歴

バージョン	日付	説明
0.9.0	2024-09-20	初稿

連邦情報セキュリティ局

私書箱 20 03 63

53133 ボン

E メール TR03183@bsi.bund.de

インターネット : <https://bsi.bund.de/dok/TR-03183>

連邦情報セキュリティ局 2024

---

# 目次

<b>1 はじめに</b> .....	<b>5</b>
<b>2 要求言語</b> .....	<b>7</b>
<b>3 基本</b> .....	<b>8</b>
3.1 使用される用語.....	8
3.1.1 製造者.....	8
3.1.2 脆弱性.....	8
3.1.3 有効、妥当、検証された脆弱性.....	8
3.1.4 脆弱性の通知.....	9
3.1.5 セキュリティ勧告.....	9
3.1.6 脆弱性レポート.....	9
3.1.7 対応する CSIRT.....	9
3.1.8 匿名報告オプション.....	9
<b>4 脆弱性報告を受けるためのサイバーセキュリティ要件</b> .....	<b>10</b>
4.1 RFC 9116 に準拠した Security.txt ファイル.....	10
4.1.1 security.txt のローカライズ.....	10
4.1.2 連絡先情報.....	10
4.1.3 有効期限.....	11
4.1.4 OpenPGP 鍵.....	11
4.1.5 謝辞.....	11
4.1.6 好まれる言語.....	12
4.1.7 CVD 政策.....	12
4.1.8 仕事のオファー.....	12
4.1.9 セキュリティ勧告.....	12
4.1.10 デジタル署名.....	12
4.1.11 正規 URI.....	13
4.1.12 ウェブ・クローラーからの視認性.....	13
4.2 CVD プロセスの予備的対策.....	14
4.2.1 サイバーセキュリティ担当者の役割.....	14
4.2.2 脆弱性報告用ウェブフォーム.....	16
4.2.3 脆弱性報告の受信用ウェブページ.....	16
4.3 CVD 政策.....	16
4.3.1 全般.....	17
4.3.2 対応する CSIRT.....	17
4.3.3 連絡先.....	17
4.3.4 報告主体に対する製造者の保証.....	18
4.3.5 有効な脆弱性の要件.....	18

4.3.6 報告企業の行動規範.....	19
4.3.7 良好なコミュニケーション.....	19
4.3.8 応答時間の保証.....	19
4.3.9 匿名報告オプション.....	20
4.3.10 脆弱性の開示.....	20
4.3.11 CVD 工程の終了.....	20
4.4 脆弱性報告の受信用ウェブページ.....	21
4.4.1 全般.....	21
4.4.2 CVD ポリシーの公表.....	21
4.4.3 連絡先オプションの公表.....	21
<b>5 附属書.....</b>	<b>23</b>
5.1 更なる情報.....	23
5.1.1 "Handhabung von Schwachstellen v2.0 - Emphelungen for Hersteller" (シュワルツの取り扱い v2.0 - 販売業者への推奨事項) を参照。.....	23
5.1.2 脆弱性の開示に関するグッド・プラクティス・ガイド.....	23
5.1.3 調整された脆弱性情報開示のための CERT ガイド.....	23
5.1.4 DIN EN ISO/IEC 29147:2020-08 または ISO/IEC 29147:2018.....	23
5.1.5 DIN EN ISO/IEC 30111:2020-07 または ISO/IEC 30111:2019.....	23
5.1.6 SecureDrop.....	23

# 1 はじめに

脆弱性は、製品、そのユーザー、環境のセキュリティ、そしておそらく安全性にも影響を与える。しかし、ソフトウェアやハードウェアの開発において、脆弱性を避けることはできない。システムが複雑で、依存関係が多ければ多いほど、脆弱性の発生頻度は高くなる。さらに、集中的なテストを行っても、製品が市場に出る前にすべての脆弱性が発見されることはほとんどない。したがって、使用される各製品について、その前と使用期間中に脆弱性を処理するプロセスが必要となる。そのため、このプロセスでは少なくとも、影響を受ける製品に対する更新プログラムの作成、リリース、安全な配布とインストール、またはその他の緩和措置の実施が必要となる。

連邦情報セキュリティ局（BSI）による本技術ガイドラインの適用範囲は、悪用された場合に、影響を受けるコンポーネントまたはコンポーネントの機密性、完全性、可用性、真正性、否認防止、または信頼性に悪影響を及ぼす、サイバーセキュリティに関連する脆弱性のみである。また、本技術ガイドラインは、製造者がウェブサイトを運営していることを前提としている。

安全な開発・運用プロセスは製品の脆弱性の数を最小限に抑えるが、脆弱性がまったくないことを保証するものではない。従って、CVD（Coordinated Vulnerability Disclosure：脆弱性開示の調整）プロセスに準拠した、脆弱性報告に対する責任ある効率的な対応プロセスを確立することは、中心的な重要事項であり、脆弱性によって引き起こされる潜在的な被害とリスクを軽減するための第一歩である。

CVD プロセスを成功させるために、製造者は、寄せられる脆弱性報告に対して前向きに対応すべきであり、犯罪意図が明白でない限り、法的措置で脅すべきでない（セキュリティ研究者のための BSI CVD ガイドライン<sup>1</sup> を参照）。さらに、製造者は CVD プロセスに備える必要がある。CVD プロセスでは、関連部門が関与する全体的な内部プロセス、連絡先の指定と公表、連絡経路の確立、脆弱性報告への実際の対応が必要となる。CVD プロセス全体を通じて、製造者は報告主体との積極的なコミュニケーションを図り、社内プロセスの継続的な最適化に努めるべきである。

欧州連合コンピュータセキュリティインシデント対応チーム（CSIRTs）ネットワーク<sup>2</sup> のメンバーは、コンピュータシステムのサイバーセキュリティインシデントに関連する予防的・事後的対策のための EU における中心的な窓口である。ドイツでは、指定された CSIRT はドイツ連邦当局のコンピュータ緊急対応チーム（CERT-Bund）<sup>3</sup> である。この CERT は、連邦サイバーセキュリティ当局であり、連邦政府内のサイバーセキュリティに関する唯一の窓口である BSI によって運営されている。BSI は、行政、企業、社会におけるサイバーセキュリティのレベルを高めることを目指している。したがって、CERT-Bund、ひいては BSI に通知され、検証された脆弱性は、製造者や製品所有

---

<sup>1</sup>[https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen\\_node.html](https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html)

<sup>2</sup>[https://csirtnetwork.eu/#network\\_members](https://csirtnetwork.eu/#network_members)

<sup>3</sup>[https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund\\_node.html](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html)

者と常に共有され、排除または軽減される。<sup>4</sup>

すべての CVD プロセスは脆弱性の報告から始まるため、外部とのコミュニケーションのための連絡先オプションと CVD 方針を公表することが不可欠である。製造者のウェブサイトには、セキュリティ情報専用のウェブページと、RFC 9116<sup>5</sup> に準拠した **security.txt**<sup>6</sup> を設けることで、この目的を果たすことができる。

---

<sup>4</sup><https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.html>

<sup>5</sup><https://www.rfc-editor.org/rfc/rfc9116>

<sup>6</sup><https://securitytxt.org/>

## 2 要求言語

本文書のキーワード "MUST"、"MUST NOT"、"REQUIRED"、"SHALL"、"SHALL NOT"、"SHOULD"、"SHOULD NOT"、"RECOMMENDED"、"NOT RECOMMENDED"、"MAY"、および "OPTIONAL" は、ここに示すように、すべて大文字で表示される場合に限り、BCP 14<sup>7</sup>（RFC 2119<sup>8</sup>、RFC 8174<sup>9</sup>）に記述されているとおりに解釈される。

---

<sup>7</sup><https://www.rfc-editor.org/info/bcp14>

<sup>8</sup> <https://www.rfc-editor.org/rfc/rfc2119>

<sup>9</sup><https://www.rfc-editor.org/rfc/rfc8174>

## 3 基本

### 3.1 使用される用語

#### 3.1.1 製造者

CRA は、「製造者」を、デジタル要素を含む製品を開発・製造する、またはデジタル要素を含む製品を設計・開発・製造させ、有償・無償を問わず、その名称または商標で販売する自然人または法人と定義している。

CRA は市場アクセス規制であるため、「製造者」は「ベンダー」と「クリエイター」の役割を兼ね備えていると解釈される。

「ベンダー」(独: "Anbieter") は、製品にデジタル要素を提供する主体の役割を表す。また、必ずしも商業的な背景があるわけではないが、「サプライヤー」(ドイツ語: "Lieferant") という用語も使われる。

「クリエイター」(ドイツ語では「Ersteller」) は、デジタル要素を含む製品をオーサリングまたは作成したエンティティの役割を表す。

本技術ガイドラインは、技術的要求事項を規定するものであるため、異なる用語を使用し、「製造者」を、機器等の有形財を製造する事業者と、ソフトウェア及びソフトウェア部品等の無形財を創造又は提供する事業者の組み合わせと解釈している。したがって、本技術指針では、「ディストリビューター」や「インポーター」という用語については言及しない。これらの技術的要求事項は、それを満たす役割とは無関係である。

#### 3.1.2 脆弱性

本技術ガイドラインでは、脆弱性とは、製品、(ウェブ)アプリケーション、またはサービスの欠陥や弱点であり、脅威源<sup>10</sup> によって悪用または誘発される可能性のあるものを指す。

#### 3.1.3 有効、妥当、検証された脆弱性

各エンティティは、何を有効な脆弱性とみなすかを定めることができる。これには、脆弱性の報告主体からの要求も含まれるかもしれない。これらに関する勧告は、4.3.5 節とセキュリティ研究者のための BSI CVD ガイドライン<sup>11</sup> にある。

製造者がその脆弱性が有効な脆弱性のルールに準拠していることを確認した後、この脆弱性は有効な脆弱性となる。

製造者が検証された脆弱性をその重大性と悪用可能性に関して評価した後、この脆弱性は検証され、確認された脆弱性となる。

---

<sup>10</sup><https://csrc.nist.gov/glossary/term/vulnerability>

<sup>11</sup>[https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen\\_node.html](https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html)

### 3.1.4 脆弱性の通知

本技術ガイドラインでは、脆弱性通知とは、脆弱性に関する一般的な情報であり、通常、当該製品の名称、暫定的な CVSS ベーススコアを含む初期評価を含むが、脆弱性に関する詳細な情報は含まない。一般的に、この通知は製造者から CSIRT または ENISA に送られ、非公開である。

### 3.1.5 セキュリティ勧告

本技術ガイドラインでは、セキュリティアドバイザリもまた、脆弱性に関する情報であり、通常、レビューされた CVSS Base Score を含む脆弱性通知の情報と、脆弱性の修正と緩和を中心とした詳細が含まれる。一般的に、アドバイザリは製造者から製品の全ユーザーに送られ、一般に公開される。推奨される配布方法は、Common Security Advisory Framework (CSAF) 文書<sup>12</sup> を適用して、製造者のウェブサイト上で公表することである。

### 3.1.6 脆弱性レポート

本技術ガイドラインでは、脆弱性報告書とは、脆弱性に関する情報であり、通常、脆弱性通知の情報と、脆弱性の特定、悪用、再現（例えば、概念実証(POC)）に焦点を当てた詳細な情報が含まれる。一般的に、脆弱性報告書は、セキュリティ研究者や CSIRT から製品の製造者に送られ、機密情報として扱われる。

### 3.1.7 対応する CSIRT

本技術ガイドラインを遵守するために、製造者は、欧州連合 CSIRTs ネットワークのいずれかの CSIRT を脆弱性届出対応 CSIRT として選択しなければならない。対応する CSIRT は、第 14 条 (7)CRA に従って決定されなければならない。さらに、製造者は、対応する CSIRT が処理を移管する場合を除き、有効な脆弱性のアクティブな処理の間、対応する CSIRT に留まらなければならない。さらに、製造者は、各脆弱性に関するコミュニケーションのために、同じ CSIRT を対応する CSIRT として選択するべきである。

### 3.1.8 匿名報告オプション

本技術ガイドラインでは、匿名報告オプションは、報告主体が匿名を保てるような製造者との連絡オプションを提供する。これは、製造者のウェブサイト上のウェブフォームであるべきである (SHOULD)。このウェブフォームは、広告やトラッキング 픽セルなどのサードパーティ製コンポーネントを含んではならない。データを入力し、このウェブフォームを使用する間、メタデータのロギングは最小限に抑えなければならない (MUST)。したがって、ログに記録してはならない情報には、報告者の IP アドレス、ブラウザ、コンピュータが含まれる。

---

<sup>12</sup>[https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technik-Richtlinien/TR-各-テーマ-ソート/TR03191/TR-03191\\_node.html](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technik-Richtlinien/TR-各-テーマ-ソート/TR03191/TR-03191_node.html)

## 4 脆弱性報告を受けるためのサイバーセキュリティ要件

本技術ガイドラインに準拠した脆弱性報告書の受領プロセスを確立するためには、少なくとも以下の要求事項を満たさなければならない。これらの要求事項を満たすために実施された対策、すべてのテスト手順、すべてのテスト結果を記録しなければならない。明確化のため、本項の要件は、脆弱性報告を受領するための最小限の要件とみなされる。したがって、例えば、**security.txt** (4.1 項参照)、脆弱性報告受理用ウェブページ (4.4 項参照)、CVD ポリシー (4.3 項参照)、CVD プロセスのための追加的な予備措置 (4.2 項参照) において、さらなる記述が許される。

### 4.1 RFC 9116 に準拠した Security.txt ファイル

報告主体が脆弱性報告の適切な連絡先を見つけやすくするため、RFC9116 に準拠した security.txt を作成し、製造者のウェブサイトで利用できるようにしなければならない (MUST)。**security.txt** のセキュリティ要件は、BSI のサイバーセキュリティ勧告 "Sicherheitskontakte mit Hilfe einer security.txt nach RFC 9116 angeben"<sup>13</sup>、RFC 9116 自体に策定された勧告に基づいている。推奨される security.txt を図 1 に例として示す。

#### 4.1.1 security.txt のローカライズ

- a. 製造者は、/.well-known/パスに **security.txt** という名前のファイルを作成しなければならない (例: /.well-known/security.txt)。
- b. このファイルは、少なくとも RFC 7230<sup>14</sup> に従った HTTP 1.1 またはそれ以上のバージョンを使用して、HTTPS 経由でアクセスできなければならない[MUST]。
- c. このファイルは、ASCII または UTF-8 エンコーディングのプレーンテキストファイルでなければならない (MUST)、コメント以外には ASCII 文字 0x20 から 0x7E のみを使用しなければならない (MUST)。
- d. 製造者は、このファイル内のすべての情報について、RFC9116 の各フォーマット仕様に準拠しなければならない (MUST)。

#### 4.1.2 連絡先情報

- a. 製造者は、脆弱性を報告するための連絡先リストを、**#Our security addresses (私たちのセキュリティアドレス)** というコメントとともに紹介すべきである (SHOULD)。
- b. 最初の連絡先オプションの宣言は、RFC 6068<sup>15</sup> (4.2.1 節参照)に従って、製造者の製品セキュリティインシデント対応チーム(PSIRT)の機能メールボックスの電子メールアドレスでなければならない[MUST]。

---

<sup>13</sup>[https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI\\_CS\\_149.html](https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI_CS_149.html)

<sup>14</sup><https://www.rfc-editor.org/rfc/rfc7230>

<sup>15</sup><https://www.rfc-editor.org/rfc/rfc6068>

- c. 最初のコンタクトオプションの宣言は、RFC6068(4.2.1 節参照)に従った製造者の CSIRT の機能メールボックスのメールアドレスでなければならない(MUST)。
- d. 次の接点は、RFC 7230 および RFC 3986<sup>16</sup> に従った、脆弱性報告 (セクション 4.4 参照) を受け付ける製造者のウェブページの URL でなければならない (MUST)。

#### 4.1.3 有効期限

- a. 製造者は、RFC 3339<sup>17</sup> に従って、**security.txt** の有効期限を指定しなければならない [MUST]。セパレーター「T」は大文字でなければならない[MUST]。他のセパレーターは使用してはならない[MUST NOT]。タイムゾーン指示子「Z」も、該当する場合は大文字にしなければならない[MUST]。
- b. この値は最大で 1 年先までとすべきである。
- c. 製造者は、少なくとも四半期に一度は **security.txt** の情報をチェックし、必要であれば修正または補足しなければならない (MUST)。

#### 4.1.4 OpenPGP 鍵

- a. 製造者は、脆弱性報告(4.2.1 節参照)を受信するためのメールアドレスの公開 OpenPGP 鍵をダウンロードするための URI を提供しなければならない[MUST]。4.2.1 節で述べられている追加のセキュリティオプションが存在する場合、製造者はそれらをダウンロードするための URL を提供すべきである[SHOULD]。
- b. 対応する OpenPGP 公開鍵の直接ダウンロード場所の URI を、RFC 4880<sup>18</sup> に従って ASCII Armor で **.asc-files** として指定しなければならない[MUST]。
- c. 対応する OpenPGP 鍵ファイルのダウンロードオプションを持つ Web ページの URL を指定してはならない[MUST NOT]。
- d. このリストには、**# Our OpenPGP keys** というコメントを付けるべきである[SHOULD]。

#### 4.1.5 謝辞

- a. 製造者は、脆弱性報告に対する謝辞のウェブページの URL を提供すべきである (SHOULD)。
- b. このリストは、**# Our security acknowledgements page (私たちのセキュリティに関する謝辞のページ)** というコメントとともに紹介されるべきである (SHOULD)。

---

<sup>16</sup><https://www.rfc-editor.org/rfc/rfc3986>

<sup>17</sup><https://www.rfc-editor.org/rfc/rfc3339>

<sup>18</sup><https://www.rfc-editor.org/rfc/rfc4880>

#### 4.1.6 好まれる言語

- a. 製造者は、脆弱性通知の優先言語を指定しなければならない (MUST)。
- b. 少なくとも英語 (en) の言語タグを指定しなければならない。
- c. このリストには、**# Our preferred languages** というコメントを付けるべきである (SHOULD)。

#### 4.1.7 CVD 政策

- a. 製造者は、CVD ポリシーのウェブページの URL を提供しなければならない (MUST)。
- b. これは、**# Our security policy (私たちのセキュ リティポリシー)** というコメントとともに紹介されるべきである (SHOULD)。

#### 4.1.8 仕事のオファー

- a. 製造者は、現在の求人情報を掲載したウェブページの URL を提供してもよい。
- b. **というコメント**とともに紹介されるべきである。

#### 4.1.9 セキュリティ勧告

- a. 製造者は、CSAF 文書<sup>19</sup> に対して、**providermetadata.json** ファイルの URI (RFC 7230 に従う) を提供すべきである (SHOULD)。
- b. この文章は、**CSAF というタグ**で始めなければならない (MUST) :  
この記述には、**# Our security advisories.**というコメントを付けなければならない (MUST)。

#### 4.1.10 デジタル署名

- a. 製造者は、RFC 4880 に従って、OpenPGP を使用して **security.txt** にデジタル署名しなければならない[MUST]。
- b. 製造者は、RFC 4880 に従って、**security.txt** の署名に専用の OpenPGP サブキー(同じ OpenPGP の「ID キー」)を使用しなければならない[MUST]。
- c. この鍵は利用可能にしなければならない(MUST) (4.4.3 節参照)。
- d. 製造者は、電子署名が現行の TR-03116 Part 4<sup>20</sup> または現行の SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms<sup>21</sup> の要件に準拠していることを保証しなければならない。

---

<sup>19</sup><https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html#718-requirement-8-securitytxt>

<sup>20</sup>[https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-  
認証/技術-リヒトリ/TR-各-テーマ-ソート/TR03116/TR-03116\\_node.html](https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-<br/>認証/技術-リヒトリ/TR-各-テーマ-ソート/TR03116/TR-03116_node.html)

<sup>21</sup><https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf>

#### 4.1.11 正規 URI

- a. 製造者は **security.txt** の正規 URI を指定しなければならない[MUST]。
- b. このステートメントには、**# Our canonical URI** というコメントを付けるべきである [SHOULD]。

#### 4.1.12 ウェブ・クローラーからの視認性

- a. 製造者は、**security.txt** が自動的に（たとえば [findsecuritycontacts.com](https://findsecuritycontacts.com/)<sup>22</sup> や [internet.nl](https://internet.nl/)<sup>23</sup> などのウェブクローラによって）見つかるようにしなければならない。従って、ファイアウォールルールや DDoS 防御ルールが適用される場合は、それに応じて適合させなければならない。

---

<sup>22</sup><https://findsecuritycontacts.com/>

<sup>23</sup><https://internet.nl/>

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

# Our canonical URI
Canonical: https://www.example.com/.well-known/security.txt

# Our security addresses
Contact: mailto:psirt@example.com
Contact: mailto:csirt@example.com
Contact: https://www.example.com/Security-Contact

# Our OpenPGP keys
Encryption: https://www.example.com/openpgp-key_psirt.asc
Encryption: https://www.example.com/openpgp-key_csirt.asc

# Our security acknowledgments page
Acknowledgments: https://www.example.com/hall-of-fame.html

# Our preferred languages
Preferred-Languages: en

# Our security policy
Policy: https://www.example.com/security-policy.html

# Our vacancies
Hiring: https://www.example.com/Jobs

# Our security advisories
CSAF: https://www.example.com/.well-known/csaf/provider-metadata.json

Expires: 2025-01-01T00:00:00.000Z
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.2

[signature]
-----END PGP SIGNATURE-----
```

図 1 : 本技術ガイドラインに準拠した *security.txt* の例

## 4.2 CVD プロセスの予備的対策

脆弱性報告に対する効率的かつ効果的な対応プロセスのためには、事前に整理しておく必要がある。これには少なくとも以下のことが含まれる。

### 4.2.1 サイバーセキュリティ担当者の役割

- a. 製造者は、責任あるサイバーセキュリティ担当者の役割を 2 つ作成しなければならない (MUST)。これらの役割は一人の担当者に割り当ててはならない (MUST NOT)。
- b. 製造者は、両方の役割に機能メールボックスを割り当てなければならず [MUST]、これらの役割に携わる者が対応する機能メールボックスにアクセスできることを保証しなければならない [MUST]。

- c. この2つの役割は、割り当てに基づいて分けられなければならない (MUST)。
- d. これら2つの役割は緊密に連絡を取り合い、互いの情報を共有し、脆弱性事例がもう一方の役割の割り当てに関係する場合は、相互に内部転送しなければならない (MUST)。
- e. サイバーセキュリティの最初の連絡先は、製造者の PSIRT でなければならない。PSIRT は、製造者の製品の脆弱性対応を担当する。
- f. PSIRT 機能メールボックスのメールアドレスは、その機能を明確に示さなければならない (MUST)。そのため、電子メールのローカル部分(電子メールのプレフィックス)は、"psirt " としなければならない(MUST)。さらに、少なくとも "productcert "と "vulnerability "をメールのローカル部分とする追加のメールボックスを作成しなければならない(MUST)。これらの追加メールボックスへの着信メールは、PSIRT の機能メールボックスにリダイレクトされなければならない(MUST)。
- g. 第二のサイバーセキュリティの連絡先は、製造者の CSIRT でなければならない。CSIRT は製造者のインフラの脆弱性対応を担当する。
- h. CSIRT 機能メールボックスのメールアドレスは、その機能を明確に示さなければならない。そのため、メールのローカル部分 (メールのプレフィックス) は、"csirt" (例: [csirt@example.com](mailto:csirt@example.com)) としなければならない (MUST)。さらに、少なくとも "cert "と "security "をメールのローカル部分とする追加のメールボックスを作成しなければならない (MUST)。これらの追加メールボックスへの着信メールは、PSIRT の機能メールボックスにリダイレクトされなければならない(MUST)。
- i. 製造者は、そのウェブサイトの「Contact Us」ウェブページに機能的メールボックスの電子メールアドレスがあれば、それを公表しなければならない。
- j. 製造者は、現行の TR-03116 Part 4 または現行の SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms の仕様に従って、機能メールボックスの電子メールアドレスに RFC 4880<sup>24</sup> に従った専用の OpenPGP サブキー(同じ OpenPGP の "identity key")を使用し、これらのサブキーを使用した暗号化され署名された通信を提供しなければならない(MUST)。
- k. 製造者は、現行の TR-03116 Part 4 または現行の SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms の仕様に従って、機能メールボックスの電子メールアドレスに追加のセキュリティオプションを提供し、RFC 6637<sup>25</sup> に従った S/MIME または OpenPGP など、これらの鍵による暗号化通信と署名通信を提供してもよい。
- l. 製造者は、欠勤を補い、CVD ポリシー (4.3 項参照) の応答時間と保証を保証するために、両方の役割に十分なリソースを提供しなければならない。

---

<sup>24</sup><https://www.rfc-editor.org/rfc/rfc4880>

<sup>25</sup><https://www.rfc-editor.org/rfc/rfc6637>

- m. 製造者は、両方の役割について、少なくとも英語で脆弱性報告書を受領し、処理できることを保証しなければならない (MUST)。
- n. 製造者は、両方の役割について、これらの役割に関与する者の権限を明確に定義しなければならない。
- o. 製造者は、両方の役割に携わる者のタスクを明確に定義しなければならない。
- p. 製造者は、機能メールボックスの E メールアドレスが E メールを受信する高い準備性を持っていることを保証すべきである (SHOULD)。これは、少なくとも毎日外部の電子メールアドレスから機能メールボックスに電子メールを (自動的に) 送信することによってテストされるべきである (SHOULD)。

#### 4.2.2 脆弱性報告用ウェブフォーム

- a. 製造者は、連絡先オプションとして、脆弱性報告用のウェブフォームを設定しなければならない。そのため、このウェブフォームを備えたウェブページをウェブサイトを作成しなければならない。
- b. このウェブフォームは、匿名で脆弱性報告を提出できるようにしなければならない (MUST)。
- c. このウェブフォームはローカライズされなければならない。少なくとも英語版を提供しなければならない。
- d. このウェブフォームは、すべての必須情報が確実に入力されるよう、構造化された方法で脆弱性報告を通じてユーザーを導くべきである (SHOULD)。
- e. このウェブフォームは高い可用性を持つべきである。これは、少なくとも毎日(自動的に)ウェブフォームに入力し、送信することでテストされるべきである (SHOULD)。

#### 4.2.3 脆弱性報告の受信用ウェブページ

- a. 製造者は、脆弱性報告のための中央ウェブページを作成しなければならない (4.4 項参照)。
- b. このウェブページには、JavaScript を有効にしなくても、製造者のウェブサイトのトップページにある見つけやすいリンクからアクセスできなければならない。
- c. このウェブページの URL のパスは、例えば <https://www.example.com/Security-Contact> のように、その機能を明確に示さなければならない (MUST)。製造者のウェブサイトの別の URL へのリダイレクトは許可される。

### 4.3 CVD 政策

CVD ポリシーは、CVD プロセス全体を支援、改善、標準化、迅速化することを目的としている。脆弱性報告の取り扱いを定義している。これには、報告主体に対する製造者の保証、報告がどのように取り扱われるか、CVD プロセスを成功させるために必要なことが含まれる。したがって、製造者の CVD ポリシーは、少なくとも以下の特徴を持たなければならない (MUST)。CVD ポリシーの要件

は、特に「BSI CVD guideline for security researchers<sup>26</sup>」、「Guidelines on implementing national Coordinated Vulnerability Disclosure (CVD) policies<sup>27</sup>」、「ETSI TR 103 838 V1.1.1<sup>28</sup>」に基づいている。

インセンティブを与えることで、製造者製品の脆弱性を報告する意欲を高めることができる。殿堂入り」ウェブページを提供することは、製造者が報告主体からの脆弱性報告に対して公に感謝する方法の一つの方法である。脆弱性を発見した者に対して金銭的な報奨金（バグ報奨金プログラム）を設けることで、メーカーは感謝の意を表し、前向きなインセンティブ構造を作ることができる。本技術ガイドラインでは、報奨金制度は CVD ポリシーのオプション的な要素と考えている。

#### 4.3.1 全般

- a. 製造者は、CVD ポリシーの最終修正日（最初のバージョンでは作成日）が明確にわかるようにしなければならない。
- b. 製造者は、CVD 方針を明確に自社に譲渡できるようにしなければならない。
- c. 製造者は、CVD 方針が最新のものであることを確認するために、少なくとも 1 年に 1 回は CVD 方針を見直さなければならない (MUST)。

#### 4.3.2 対応する CSIRT

- a. 製造者は、対応する CSIRT(3.1.2 項参照)に対し、認識した全ての有効な脆弱性を過度な遅延なく通知しなければならない(MUST)。
- b. 有効性が確認され、検証された脆弱性の場合、製造者は、対応する CSIRT にすべての新情報、緩和策及びそのスケジュールを通知し、対応する CSIRT と調整しなければならない。

#### 4.3.3 連絡先

- a. 製造者は、役割指向のコンタクトオプションの機能メールボックスの E メールアドレスを命名しなければならない(MUST)(4.2.1 項参照)。
- b. 製造者は、対応する OpenPGP 公開鍵(セクション 4.1.10 と 4.2.1 参照)の直接ダウンロード場所の URI を、RFC 4880 に従って ASCII Armor で.ascfiles として提供しなければならない[MUST]。
- c. 製造者は、対応する OpenPGP 鍵のフィンガープリントを引用しなければならない[MUST] (セクション 4.1.10 と 4.2.1 参照)。

---

<sup>26</sup>[https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen\\_node.html](https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html)

<sup>27</sup><https://ec.europa.eu/newsroom/dae/redirection/document/99973>

<sup>28</sup> [https://www.etsi.org/deliver/etsi\\_tr/103800\\_103899/103838/01.01.01\\_60/tr\\_103838v010101p.pdf](https://www.etsi.org/deliver/etsi_tr/103800_103899/103838/01.01.01_60/tr_103838v010101p.pdf)

- d. 製造者は、(セクション 4.2.1 で述べられている)追加セキュリティオプションの公開鍵または証明書が存在する場合、それを直接ダウンロードする場所の URI を提供するべきである [SHOULD]。
- e. コンタクトオプションの有効期限は、有効期限が切れる前に十分な余裕をもって 指定し、更新しなければならない[MUST]。この有効期限は、最大で 1 年先までとすべきである [SHOULD]。

#### 4.3.4 報告主体に対する製造者の保証

- a. 製造者は、各脆弱性報告書が法律で許される範囲内で秘密保持されることを保証しなければならない。
- b. 製造者は、報告主体の明示的な同意なしに個人データを第三者に開示しないことを保証しなければならない。
- c. 製造者は、各脆弱性報告に対する回答が、保証された回答時間（4.3.8 項参照）内に提供されることを保証しなければならない。
- d. 製造者は、本方針とその原則が通知主体によって遵守されている限り、報告主体に対して刑事責任を追究されないことを保証しなければならない (MUST)。このことは、犯罪的意図が認識され、または追求されている場合には適用されない。
- e. 製造者は、CVD の全過程を通じて、信頼できるやりとりの窓口であることを保証しなければならない。
- f. 製造者は、有効な脆弱性を報告し、CVD プロセスを完了した後、報告主体から要請があれば、報告主体の名前／別名および希望する参照先を製造者の謝辞のウェブページ（殿堂）に掲載することを保証しなければならない (MUST)。その際、すべての関係主体が互いに敬意をもって接し、EU 域内では差別、性差別、人種差別、ナチズム、暴力の賛美、ポルノ、侮辱、中傷、名誉毀損などの不法行為が許されないことを明確に強調すべきである。この点で違反があった場合、その機関は公表を差し控えなければならない。
- g. 製造者は、非開示契約 (NDA) に署名することを報告事業者に求めてはならない (MUST NOT)。
- h. 製造者は、報告主体に対し、機密情報の送信に暗号化され電子署名された E メールを使用するよう推奨しなければならない (MUST)。

#### 4.3.5 有効な脆弱性の要件

- a. 製造者は、以下の場合を除き、有効な脆弱性の報告を要求すべきではない (SHOULD NOT) :  
その脆弱性は、製造者のいずれかの製品に影響しなければならない。
- b. 脆弱性報告書は、公に知られていない情報に関するものである。
- c. 脆弱性の通知は、自動化ツールやスキャンによる結果ではなく、裏付けとなる文書がない。

#### 4.3.6 報告企業の行動規範

- a. 善意の目的のために悪意がない報告者のみに報いるために、製造者は、報告主体に期待される行動と、違反した場合の結果を示した行動規範を公表してもよい (MAY)。しかし製造者は、非遵守主体からの報告が可能な限り最良に扱われることを保証しなければならない (MUST)。行動規範には、以下の点を含めてもよい (MAY) :  
報告された脆弱性は、報告主体によって悪用されていない。つまり、報告された脆弱性以上の被害は生じていない。
- b. 報告主体による、製造者の IT システムまたはインフラに対する攻撃（ソーシャルエンジニアリング、スパム、(分散) DoS または「総当たり」攻撃など）は行われていない。
- c. 報告企業によって、第三者の可能性のあるシステムやデータの操作、危殆化、変更が行われたことはない。
- d. 報告主体がダークネット市場などで、第三者が犯罪に利用できるような、脆弱性を悪用するためのツールを有料または無料で提供していない。

不順守の結果 (MAY) には以下の点が含まれる :

- a. 報告企業は、(バグ報奨金プログラムなどの) 報奨金を受け取っていない。
- b. 報告主体は、謝辞のウェブページ (殿堂入り) には掲載されない。

#### 4.3.7 良好なコミュニケーション

- a. 製造者は、報告された脆弱性情報が CVD プロセスの一部として更なる処理を行う資格がない場合であっても、既に是正された脆弱性について報告された情報を受信し、チェックすることを保証すべきである (SHOULD)。
- b. 製造者は、脆弱性報告には良好なコミュニケーションが重要であること、また、問合せのために、少なくとも一つの有効な連絡先 (できれば電子メールアドレス) を報告主体から提供されるべきであることを説明すべきである。
- c. 製造者は、どのような接点オプションが受け入れられるかを宣言すべきである (SHOULD)。
- d. 製造者は、少なくとも電子メールアドレスと電話番号を有効な連絡先として認めなければならない。
- e. 製造者は、報告された脆弱性の状況について報告主体からの問い合わせを歓迎することを指摘すべきである。

#### 4.3.8 応答時間の保証

- a. 製造者は、脆弱性が匿名で報告された場合を除き、脆弱性報告に対する簡易な回答を 5 営業日以内に提供することを保証しなければならない (MUST)。この簡単な回答は、自動化された回答であってはならない (MUST NOT)。
- b. 製造者は、脆弱性が匿名で報告された場合を除き、さらなる分析後の詳細なフィードバックを 10 営業日以内に提供することを保証しなければならない。

- c. 製造者は、脆弱性が匿名で報告された場合を除き、報告された脆弱性が 10 営業日以内に確認されるか拒否されることを保証しなければならない。

#### 4.3.9 匿名報告オプション

- a. 製造者は、脆弱性報告を匿名で提出するための見つけやすいオプションを提供しなければならない(MUST)。これは、4.2.2 節で述べた脆弱性報告用のウェブフォームであるべきである(SHOULD)。
- b. 製造者は、特に複雑な問題の場合、さらなる説明と文書化が必要になる可能性があることを明確にすべきである。
- c. 製造者は、報告主体が技術的または内容に関連する問合せに応じない場合、対応する脆弱性報告は限定的な範囲でしか処理できないか、場合によっては全く処理できないことを明確にすべきである(SHOULD)。
- d. 製造者は、技術的または内容的な問い合わせを要求するオプションがないため、匿名レポートが限られた範囲でしか処理できないか、まったく処理できない可能性があることを明示しなければならない(MUST)。
- e. 製造者は、有効な脆弱性を見落としを避けるため、匿名報告が可能な限り最善の範囲内で扱われ、一人のアナリストによってクローズされることがないようにしなければならない(MUST)。

#### 4.3.10 脆弱性の開示

- a. 製造者は、検証され報告された脆弱性が 90 日以内に公開されることを保証しなければならない。ただし、脆弱性の緩和または修正の遅れについて正当な理由と説明がある場合、対応する CSIRT と緊密に協議の上、公開までの期間を 90 日間延長することができる。例外として、製造者の要求があれば、対応する CSIRT は公開までの期間をさらに延長することができる。
- b. 製造者は、対応する CSIRT と協議の上、例えば NIST（米国国立標準技術研究所）の NVD（National Vulnerability Database）<sup>29</sup>、脆弱性が公表されることを保証しなければならない(MUST)。

#### 4.3.11 CVD 工程の終了

- a. 製造者は、CVD プロセスがいつ完了したとみなされるかを明確に公示しなければならない。
- b. 製造者は、脆弱性が匿名で報告された場合を除き、報告主体に対し、過度な遅延なく CVD プロセスの終了を伝えるべきである(SHOULD)。

---

<sup>29</sup><https://nvd.nist.gov/>

- c. 製造者は、脆弱性報告の指摘に根拠がない場合、CVD プロセスは完了したとみなすべきである。
- d. 製造者は、サービス（ウェブサービスなど）の脆弱性が修正され、一般に公開された場合、CVD プロセスが完了したとみなすべきである（SHOULD）。
- e. 製造者は、その脆弱性が適切なパッチによって緩和または修正され、公に開示された場合、CVD プロセスが完了したとみなすべきである（SHOULD）。
- f. 製造者は、脆弱性が公表され、対応する CSIRT と協議の上、脆弱性が緩和または修正されることがもはや 想定できない場合、CVD プロセスが完了したとみなしてもよい。

#### 4.4 脆弱性報告の受信用ウェブページ

外部事業者は、脆弱性報告書の提出に関するすべての重要な情報を、製造者のウェブサイト上の一元的なポイントで見つけるべきである。そのため、脆弱性報告書を受け付けるウェブページには、少なくとも以下の機能を持たせるべきである。

##### 4.4.1 全般

- a. 製造者は、すべての情報を含むこのウェブページが、有効化された JavaScript なしで、またログイン手順やその他の制限（例えばペイウォールの後ろなど）なしに、完全にアクセス可能であることを保証しなければならない。
- b. このウェブページの情報は、明確に構成され、外部組織にとって見つけやすいものでなければならない。
- c. 製造者は、そのプライバシーポリシーのうち、個人データの送信に関する項目（例えば、報告事業者の連絡先詳細）の近くを示すべきである（SHOULD）。

##### 4.4.2 CVD ポリシーの公表

- a. 製造者は、このウェブページに、CVD 方針が掲載されているウェブページへのリダイレクト、転送、ルーティングが簡単にできるリンクを貼らなければならない。従って、製造者は、CVD 方針を掲載したウェブページを作成しなければならない（MUST）。
- b. 製造者は、CVD 方針が掲載されているウェブページ<sup>(30)</sup>において、CVD 方針を PDF/A-2a 形式で無料でダウンロードできるようにすることができる。

##### 4.4.3 連絡先オプションの公表

- a. 製造者は、役割に応じたコンタクトオプションの E メールアドレスを提供しなければならない(MUST) (4.2.1 項参照)。

---

<sup>30</sup>ISO 32000-1:2008 - 文書管理 - ポータブル文書フォーマット - 第 1 部 : PDF 1.7

- b. 製造者は、対応する OpenPGP 公開鍵の直接ダウンロード先の URI を、RFC 4880 に準拠した ASCII アーマーで、**.asc-files** として a.に記載された E メールアドレスに提供しなければならない[MUST]。
- c. 製造者は、a.に記載されたメールアドレスの OpenPGP 鍵のフィンガープリントを提示しなければならない。
- d. 製造者は、**security.txt**(セクション 4.1.10 参照)に署名するために、対応する OpenPGP 公開鍵の直接ダウンロード場所の URI を、RFC 4880 に従って ASCII Armor で**.asc-file** として提供しなければならない[MUST]。
- e. 製造者は、**security.txt** ファイルに署名するための OpenPGP 鍵のフィンガープリントを引用しなければならない[MUST](セクション 4.1.10 参照)。
- f. 製造者が a に記載された電子メールアドレスに追加セキュリティオプション (4.2.1 節に従う) を提供する場合、製造者は、これらの追加セキュリティオプションに関連する公開鍵または証明書 の直接ダウンロード先の URI を提供し、そのフィンガープリントを引用しなければならない。
- g. 製造者は、4.2.2 節で述べた脆弱性報告用ウェブフォームの URL を提供しなければならない(MUST)。
- h. コンタクトオプションの有効期限は、有効期限が切れる前に十分な余裕をもって 指定し、更新しなければならない[MUST]。この有効期限は、最大で 1 年先までとすべきである [SHOULD]。

---

## 5 附属書

このセクションでは、補足的な説明をしている。

### 5.1 更なる情報

#### 5.1.1 "Handhabung von Schwachstellen v2.0 - Empfehlungen for Hersteller" (シュワルツの取り扱い v2.0 - 販売業者への推奨事項) を参照。

BSI は、脆弱性に正しく対処する方法について、製造者向けの推奨事項を発表している。  
[https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS\\_019.pdf](https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf)

#### 5.1.2 脆弱性の開示に関するグッド・プラクティス・ガイド

ENISA は、脆弱性開示の課題とグッドプラクティスを明らかにするため、本調査を発表した。  
<https://www.enisa.europa.eu/publications/vulnerability-ディスクロージャー>

#### 5.1.3 調整された脆弱性情報開示のための CERT ガイド

CERT コーディネーションセンター (CERT/CC) は、カーネギーメロン大学ソフトウェア工学研究所 (Software Engineering Institute of the Carnegie Mellon University) により発行された『CERT Guide to Coordinated Vulnerability Disclosure』のウェブ版を発行した。

ウェブ版 : <https://certcc.github.io/CERT-Guide-to-CVD/>

原文 : <https://insights.sei.cmu.edu/library/the-cert-guide-to-coordinated-vulnerability-開示-2/>

#### 5.1.4 DIN EN ISO/IEC 29147:2020-08 または ISO/IEC 29147:2018

この ISO 規格は、脆弱性の開示に関するさらなる推奨事項と要求事項を記述している。

<https://www.iso.org/standard/72311.html>

<https://www.dinmedia.de/de/norm/din-エン-iso-iec-29147/324674445>

#### 5.1.5 DIN EN ISO/IEC 30111:2020-07 または ISO/IEC 30111:2019

この ISO 規格は、脆弱性処理プロセスに関するさらなる推奨事項と要求事項を記述している。

<https://www.iso.org/standard/69725.html>

<https://www.dinmedia.de/de/norm/din-エン-iso-iec-30111/324674587>

#### 5.1.6 SecureDrop

これは、匿名の情報源から文書を受け取り、なおかつ彼らとコミュニケーションをとるためのオープ

ンソースソフトウェアである。

<https://securedrop.org/>

<https://github.com/freedomofpress/securedrop>