# 技術ガイドライン BSI TR-03183:

# 製造事業者および製品に対する

# サイバーレジリエンス要件

**第 3 部：脆弱性報告および通知**

# 文書履歴

表 *1*：文書履歴

| バージョン | 日付 | 説明 |
|---|---|---|
| 0.9.0 | 2024-09-20 | 初期ドラフト |
| 1.0.0 | 2025-08-20 | 初版公開時の BSI TR-03183-3 バージョン |

連邦情報セキュリティ庁

私書箱 20 03 63

53133 ボン

E-Mail: TR03183@bsi.bund.de

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

© 連邦情報セキュリティ庁 2024 - 2025

# 目次

**1 序論 ..... 5**
**2 要件言語 ..... 6**
**3 基本事項 ..... 7**
**3.1 使用用語 ..... 7**
3.1.1 製造事業者 ..... 7
3.1.2 脆弱性 ..... 7
3.1.3 有効、妥当性確認済み、確認済み、および積極的に悪用されている脆弱性 ..... 7
3.1.4 脆弱性通知 ..... 8
3.1.5 セキュリティアドバイザリ ..... 8
3.1.6 脆弱性レポート ..... 8
3.1.7 対応する国内 CSIRT ..... 8
3.1.8 匿名報告オプション ..... 8
**4 脆弱性報告の受領に関するサイバーセキュリティ要件 ..... 9**
**4.1 製造事業者のウェブサイト ..... 9**
4.1.1 概要 ..... 9
**4.2 RFC 9116 に準拠した Security.txt ファイル ..... 9**
4.2.1 security.txt の配置場所 ..... 9
4.2.2 正規 URI ..... 10
4.2.3 連絡先情報 ..... 10
4.2.4 OpenPGP 鍵 ..... 10
4.2.5 謝辞 ..... 10
4.2.6 優先言語 ..... 10
4.2.7 CVD ポリシー ..... 10
4.2.8 セキュリティ勧告 ..... 11
4.2.9 有効期限 ..... 11
4.2.10 デジタル署名 ..... 11
4.2.11 ウェブクローラーの可視性 ..... 12
**4.3 CVD プロセスの事前措置 ..... 12**
4.3.1 責任あるサイバーセキュリティ連絡担当者の役割 ..... 12
4.3.2 セキュリティ連絡先の暗号化オプションのプロバイダ ..... 14
4.3.3 脆弱性報告用ウェブフォーム ..... 14
4.3.4 脆弱性報告受付用ウェブページ ..... 14
**4.4 CVD ポリシー ..... 14**
4.4.1 概要 ..... 15
4.4.2 対応する国内 CSIRT ..... 15
4.4.3 連絡先詳細 ..... 15
4.4.4 報告事業体に対する製造事業者の保証 ..... 15
4.4.5 脆弱性ガイドライン ..... 16
4.4.6 報告事業体のための行動規範 ..... 16
4.4.7 良好なコミュニケーション ..... 16
4.4.8 保証された応答時間 ..... 17

4.4.9 匿名報告オプション ..... 17
4.4.10 脆弱性の開示 ..... 17
4.4.11 CVD プロセスの終了 ..... 17
**4.5 脆弱性報告受付用ウェブページ ..... 18**
4.5.1 概要 ..... 18
4.5.2 CVD ポリシーの公開 ..... 18
4.5.3 連絡先オプションの公開 ..... 19
**5. 附属書 ..... 20**
**5.1 追加情報 ..... 20**
5.1.1「脆弱性管理 v2.0 – メーカー向け推奨事項」 ..... 20
5.1.2 脆弱性開示に関するベストプラクティスガイド ..... 20
5.1.3 脆弱性開示の調整に関する CERT ガイド ..... 20
5.1.4 DIN EN ISO/IEC 29147:2020-08 または ISO/IEC 29147:2018 ..... 20
5.1.5 DIN EN ISO/IEC 30111:2020-07 または ISO/IEC 30111:2019 ..... 20
5.1.6 ISO/IEC 20153:2025 ..... 20
5.1.7 SecureDrop ..... 20
5.1.8 CSAF プロバイダ ..... 21

# 1 序論

脆弱性は、製品、そのユーザー、および環境のセキュリティ、ひいては安全性に影響を及ぼす可能性がある。しかし、ソフトウェアおよびハードウェアの開発において脆弱性を完全に回避することは不可能である。システムの複雑さや依存関係が増すほど、脆弱性が発生する頻度も高まる。さらに、徹底的なテストを実施した後であっても、製品が上市され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、各製品の使用前および使用期間中を通じて、脆弱性対応プロセスが必要となる。具体的には、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・インストール、またはその他の緩和策の実施が最低限求められる。

安全な開発・運用プロセスは製品内の脆弱性を最小化するが、製品に脆弱性が全く存在しないことを保証するものではない。したがって、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し、調整された脆弱性開示（CVD）プロセスに準拠することが極めて重要であり、脆弱性が引き起こす潜在的な危害とリスクを低減する第一歩となる。

CVD プロセスの成功のためには、製造事業者は脆弱性報告に対して前向きに対応し、犯罪意図が明らかでない限り法的措置をちらつかせるべきではない（セキュリティ研究者向け BSI CVD ガイドライン参照：[1]）さらに、製造事業者は CVD プロセスに備える必要がある。これには、関連部門を巻き込んだ包括的な内部プロセス、連絡先の指定と公表、コミュニケーションチャネルの確立、脆弱性報告への実際の対応が含まれる。CVD プロセス全体を通じて、製造事業者は報告事業体と積極的にコミュニケーションを取り、内部プロセスの継続的な最適化に努めるべきである。

すべての CVD プロセスは脆弱性報告から始まるため、外部との連絡手段および CVD ポリシーを公開することが不可欠である。製造事業者のウェブサイト上に、セキュリティ情報専用のウェブページと、RFC 9116（[2]）に準拠した **security.txt（[3]）**を設置することで、この目的は達成される。

連邦情報セキュリティ庁（BSI）による本技術ガイドラインの対象範囲は、悪用された場合に影響を受けるコンポーネントの機密性、完全性、可用性、真正性、否認防止、信頼性に対して悪影響を及ぼすサイバーセキュリティ関連の脆弱性に限定される。

さらに、脆弱性は複数の EU 加盟国に影響を及ぼす可能性があり、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（CSIRT）ネットワーク[4]（NIS 指令第 12 条[5] および NIS2 指令第 15 条[6] 参照）が設立された。このネットワークの使命の一つは、EU 域内における脆弱性情報の交換を改善することである。したがって、各加盟国は、調整された脆弱性開示の目的のために、自国の CSIRT の一つを国家調整機関として指定する（NIS2 指令第 12 条参照）。ドイツでは、指定される見込みの国家 CSIRT は、ドイツ連邦当局向けコンピュータ緊急対応チーム（CERT-Bund）[7] である。これは、連邦サイバーセキュリティ機関であり、連邦行政機関内のサイバーセキュリティに関する単一窓口である 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水準の向上を目指している。したがって CERTBund、ひいては BSI は、脆弱性の排除または緩和を支援するため、報告された妥当な脆弱性情報を常に製造事業者と共有する[8]。

---

[1] https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html

[2] https://www.rfc-editor.org/rfc/rfc9116

[3] https://securitytxt.org/

[4] https://csirtsnetwork.eu/#network_members

[5] https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng

[6] https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[7] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/CyberSicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html

[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CVD/CVD-Leitlinie.html

# 2 要件言語

本ドキュメントにおけるキーワード「MUST」、「MUST NOT」、「REQUIRED」、「SHALL」、「SHALL NOT」、「推奨される」、「推奨されない」、「可能」、「任意」は、BCP 14[9] （RFC 2119[10] 、RFC 8174[11] ）で定義される通りに解釈される。ただし、これらがすべて大文字で表記されている場合に限る。

[9] https://www.rfc-editor.org/info/bcp14

[10] https://www.rfc-editor.org/rfc/rfc2119

[11] https://www.rfc-editor.org/rfc/rfc8174

# 3 基本事項

## 3.1 使用される用語

### 3.1.1 製造事業者

サイバーレジリエンス法（CRA）[12] は、第 3 条第 13 項において「製造事業者」を、デジタル要素を含む製品を開発または製造する、もしくはデジタル要素を含む製品の設計・開発・製造を委託し、有償・無償を問わず自社名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、「製造事業者」は「ベンダー」と「クリエイター」の役割を統合したものと解釈される。

「ベンダー」（ドイツ語：Anbieter）は、デジタル要素を含む製品を提供する事業体の役割を指す。代替的に、必ずしも商業的背景を伴わない場合、「サプライヤー」（ドイツ語：Lieferant）という用語が用いられる。

「クリエイター」（ドイツ語：Ersteller）は、デジタル要素を含む製品を制作または作成した事業体の役割を指します。

本技術ガイドラインは技術要件を規定するため、異なる用語体系を採用し、「製造事業者」を、デバイスなどの有形製品を生産する事業体と、ソフトウェアやソフトウェアコンポーネントなどの無形製品を創作・提供する事業体（通常「作者」と称される）の複合体として解釈する。したがって、本技術ガイドラインでは「頒布事業者」や「輸入事業者」という用語は言及しません。これらの当事者の役割は、ここで述べる技術要件とは無関係だからである。これらの技術要件は、それを満たす役割とは独立している。

### 3.1.2 脆弱性

NIS2 指令第 6 条第 15 項は、「脆弱性」を、サイバー脅威によって悪用される可能性のある ICT 製品または ICT サービスの弱点、感受性、欠陥と定義している。

### 3.1.3 有効な脆弱性、妥当性確認された脆弱性、確認済み脆弱性、および積極的に悪用されている脆弱性

各事業体は、自組織の脆弱性ガイドラインに基づき、有効な脆弱性をどう定義するかを決定できる。このガイドラインには、脆弱性を報告する事業体からの要求事項が含まれる場合がある。

このガイドラインの内容に関する要件は、セクション 4.4.5 およびセキュリティ研究者向け BSI CVD ガイドライン[13] に記載されている。

製造事業者 が当該脆弱性が自社の脆弱性ガイドラインの要件を満たすことを確認した後、この脆弱性は妥当性確認された脆弱性となる。

製造事業者が妥当性確認済みの脆弱性についてその深刻度と悪用可能性を評価した後、当該脆弱性は「妥当性確認済みかつ実証済み」または「妥当性確認済みだが実証未済」のいずれかとなる。

CRA は第 3 条第 42 項において、「積極的に悪用されている脆弱性」を、悪意のある行為者がシステム所有者の許可なくシステム内で悪用した信頼できる証拠が存在する脆弱性として定義している。

[12] https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[13] https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html

### 3.1.4 脆弱性通知

本技術ガイドラインにおいて、脆弱性通知とは脆弱性に関する一般的な情報を指し、通常は対象製品名を明記し暫定的な CVSS ベーススコアを含む初期アセスメントを含みますが、脆弱性の詳細な情報は含まれない。一般的に通知は製造事業者から各国の CSIRT または欧州連合サイバーセキュリティ機関（ENISA）[14] に送付され、非公開である。

### 3.1.5 セキュリティアドバイザリ

本技術ガイドラインにおいて、セキュリティアドバイザリも脆弱性に関する情報であり、通常は脆弱性通知の情報（検証済み CVSS ベーススコアを含む）に加え、脆弱性の修正・緩和策に焦点を当てた詳細情報を含む。一般的に、アドバイザリは製造事業者から当該製品の全ユーザーに送信され、公開される。推奨される配布方法は、共通セキュリティアドバイザリ枠組み（CSAF）[15] を適用した製造事業者ウェブサイトへの掲載である。

### 3.1.6 脆弱性報告

本技術ガイドラインにおいて、脆弱性報告とは脆弱性に関する情報を指す。通常、脆弱性通知の情報に加え、特定・悪用・再現方法（例：脆弱性の概念実証（POC））に焦点を当てた詳細情報を含む。一般的に、報告はセキュリティ研究者または国家 CSIRT から製品の製造事業者へ送信され、機密扱いとなる。

### 3.1.7 対応する国内 CSIRT

本技術ガイドラインに準拠するため、製造事業者は、協調的脆弱性開示の目的で自加盟国から調整機関として指定された国内 CSIRT の中から、対応する国内 CSIRT を選定しなければならない（CRA 第 3 条第 51 項と NIS2 指令第 12 条を参照）。対応する国内 CSIRT は、CRA 第 14 条第 7 項に基づき決定されなければならない。さらに、製造事業者は、対応する国内 CSIRT が対応を移管する場合を除き、有効な脆弱性個々の積極的な対応中は、対応する国内 CSIRT に留まらなければならない。加えて、製造事業者は、あらゆる脆弱性に関する連絡において、対応する国内 CSIRT として同一の国内 CSIRT を選択すべきである。

### 3.1.8 匿名報告オプション

本技術ガイドラインにおける匿名報告オプションは、報告事業体が匿名性を保持できる製造事業者への連絡手段を提供する。これは製造業者のウェブサイト上のウェブフォームであることが推奨される。このウェブフォームは、広告やトラッキングピクセルなどのサードパーティコンポーネントを含んではならない。データ入力時および本ウェブフォーム使用時のメタデータ記録は最小限に抑えなければならない。したがって、記録すべきでない情報には、報告事業体の IP アドレス、ブラウザ、またはコンピューターが含まれる。

[14] https://www.enisa.europa.eu/

[15] https://www.bsi.bund.de/dok/TR-03191-en

# 4 脆弱性報告受領に関する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受領プロセスを確立するためには、少なくとも以下の要件を満たさなければならない。これらの要件を満たすために実施された措置、全てのテスト手順、及び全てのテスト結果は記録されなければならない。明確化のため、本節の要件は脆弱性報告受領における最小限の要件とみなされる。したがって、**security.txt**（4.2 節参照）、脆弱性報告受付ウェブページ（4.5 節参照）、CVD ポリシー（4.4 節参照）における追加記述、および CVD プロセス向け追加事前措置（4.3 節参照）は許容される。

## 4.1 製造事業者のウェブサイト

製造事業者およびその製品に関するセキュリティ関連情報は、外部事業体が容易にアクセスできる状態で提供されるべきである。したがって、製造事業者は本情報を一般に容易にアクセス可能な状態で提供しなければならない。

### 4.1.1 概要

a. 製造事業者は、自社および自社製品に関するセキュリティ関連情報を少なくとも公開するためにウェブサイトを運営しなければならない。

b. このウェブサイトは、ログイン手続きやその他の制限（例：有料会員制）なしに完全にアクセス可能でなければならない。

c. 少なくとも、このウェブサイト上のすべてのセキュリティ関連情報（例：CVD ポリシー（4.4 節参照）および脆弱性報告受付ページ（4.5 節参照））は、ユーザーおよび市場監視当局が容易に理解できる言語で提供されなければならない。

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

脆弱性報告の適切な連絡先を報告事業体が容易に見つけられるようにするため、RFC 9116 に準拠した **security.**txt を作成し、製造事業者のウェブサイト上で公開しなければならない。**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「RFC 9116 に基づく security.txt によるセキュリティ連絡先指定」[16] および RFC 9116 自体で策定された推奨事項に基づいている。図 1 は、本節の要件に準拠した **security.txt** の例を示している。

### 4.2.1 security.txt の配置場所

a. 製造事業者は、/.well-known/ パス直下に **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 HTTP 1.1（RFC 7230[17] セクション 2.7.2 に準拠）またはそれ以降のバージョンを使用した HTTPS 経由でアクセス可能でなければならない。

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。非コメント部分には ASCII 文字 0x20 から 0x7E のみを使用しなければならない。

d. 製造事業者は、このファイル内のすべての情報について、RFC 9116 の各フォーマット仕様に準拠しなければならない。

[16] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSICS_149.html

[17] https://www.rfc-editor.org/rfc/rfc7230

### 4.2.2 正規 URI

a. 製造事業者は **security.txt** の正規 URI を指定しなければならない。

b. この正規 URI は、RFC 7230 セクション 2.7.2 に準拠した Web URI でなければならない。

c. この正規 URI は、権威あるファイルの真の場所を反映し、リダイレクトなしでアクセス可能でなければならない。

d. この記述は、コメント「**# 当社の正規 URI**」で導入することが推奨される。

### 4.2.3 連絡先情報

a. 製造事業者は脆弱性報告用の連絡先オプション一覧を提供しなければならない。

b. 最初の連絡先オプションの宣言は、RFC 6068[18] に準拠した、製造事業者の製品セキュリティインシデントレスポンスチーム（PSIRT）（セクション 4.3.1 参照）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。

c. 第二の連絡先オプションの宣言は、RFC 6068 に準拠した製造事業者の CSIRT（セクション 4.3.1 参照）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。

d. 次の連絡先は、RFC 7230 および RFC 3986[19] に準拠し、脆弱性報告受付用製造事業者ウェブページ（セクション 4.5 参照）の Web URI（RFC 7230 セクション 2.7.2 準拠）でなければならない。

e. このリストは、コメント「**# 当社のセキュリティ連絡先**」で導入されるべきである。

### 4.2.4 OpenPGP 鍵

a. 製造事業者は、セクション 4.2.3 で提供される連絡先リストの暗号化オプションを提供しなければならない。

したがって、セクション 4.3.2 の要件を適用しなければならない。

b. このリストにはコメント「**# 弊社の OpenPGP 鍵**」を付記することが推奨される。

### 4.2.5 謝辞

a. 製造事業者は、脆弱性報告用ウェブページの謝辞のウェブ URI（RFC 7230 2.7.2 節に準拠）を提供すべきである。

b. このリストは、コメント「**# 当社のセキュリティ謝辞ページ**」で導入すべきである。

### 4.2.6 推奨言語

a. 製造事業者は、脆弱性報告の送信に際して推奨される言語を明示しなければならない。

b. 少なくとも英語の言語タグ (en) は指定しなければならない。

c. このリストには、コメント「**# 推奨言語**」を付記することが推奨される。

### 4.2.7 CVD ポリシー

a. 製造事業者は、自社の CVD ポリシーのウェブページへのウェブ URI（RFC 7230 セクション 2.7.2 に準拠）を提供しなければならない。

[18] https://www.rfc-editor.org/rfc/rfc6068

[19] https://www.rfc-editor.org/rfc/rfc3986

b. これはコメント**「# 当社のセキュリティポリシー」**と共に導入されるべきである。

### 4.2.8 セキュリティアドバイザリ

a. 製造事業者は、CSAF 文書[20] 用のファイル**プロバイダ-メタデータ.json の** Web URI（RFC 7230 セクション 2.7.2 に準拠）を提供すべきである。

b. この記述は必ず **CSAF** タグで開始しなければならない **:**

c. この記述はコメント**「# 当社のセキュリティアドバイザリ」**で導入されるべきである。

### 4.2.9 有効期限

a. 製造事業者は、RFC 3339[21] に従い、**security.txt** の有効期限を指定しなければならない。区切り文字「T」は大文字でなければならない。他の区切り文字は使用してはならない。該当する場合、タイムゾーン指標「Z」も大文字でなければならない。

b. この値は、最大で 1 年先の将来の日付であることが望ましい。

c. 製造事業者は、少なくとも四半期ごとに **security.txt** の情報を確認し、必要に応じて修正または補足しなければならない。

### 4.2.10 デジタル署名

a. 製造事業者は、RFC 9580[22] に準拠した OpenPGP を用いて security**.txt に**デジタル署名を行わなければならない。注記: RFC 9580 は、RFC 4880[23] （「OpenPGP メッセージ形式」）、RFC 5581[24] （「OpenPGP におけるカメリア暗号」）、および RFC 6637[25] （「OpenPGP における楕円曲線暗号（ECC）」）を廃止する。

b. 製造事業者は、RFC 9580 に従い **security.txt** の署名に専用の OpenPGP 鍵を使用すべきである。

c. 対応する OpenPGP 公開鍵は提供されなければならない（4.5.3 節参照）。

d. 製造事業者は、デジタル署名が現行の BSI TR-03116 Part 4[26] または現行の ECCG 合意暗号メカニズム[27] の要件に準拠していることを保証しなければならない。注記：ECCG 合意暗号メカニズム - バージョン 2 は、SOG-IS 合意暗号メカニズム[28] に基づいている。

e. b で言及された鍵の有効期間が、現行の BSI TR-03116 Part 4 または現行の ECCG 合意暗号メカニズムで別段の定めがない限り、5 年を超えてはならない。

[20] https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html#718-requirement-8-securitytxt

[21] https://www.rfc-editor.org/rfc/rfc3339

[22] https://www.rfc-editor.org/rfc/rfc9580

[23] https://www.rfc-editor.org/rfc/rfc4880

[24] https://www.rfc-editor.org/rfc/rfc5581

[25] https://www.rfc-editor.org/rfc/rfc6637

[26] https://www.bsi.bund.de/dok/TR-03116-en

[27] https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

[28] https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf

### 4.2.11 ウェブクローラーへの可視性

製造事業者は、**security.txt** が自動的に検出可能であることを保証しなければならない（例：findsecuritycontacts.com[29] や internet.nl[30] などのウェブクローラーによる検出）。したがって、該当する場合は、ファイアウォール規則や DDoS 保護規則を適宜調整する必要がある。

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

Expires: 2026-07-01T00:00:00.000Z
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.4

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

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

## 4.3 CVD プロセスに向けた事前措置

脆弱性報告に対する効率的かつ効果的な対応プロセスを実現するには、事前に体制を整える必要がある。これには少なくとも以下の事項が含まれる。

### 4.3.1 責任あるサイバーセキュリティ連絡担当者の役割

a. 製造事業者は、少なくとも 2 つの責任あるサイバーセキュリティ連絡窓口の役割、すなわち PSIRT（製品セキュリティインシデント対応チーム）と CSIRT（サイバーセキュリティインシデント対応チーム）を設置しなければならない。

[29]https://findsecuritycontacts.com/

[30]https://internet.nl/

b. 製造事業者が零細企業（CRA 第 3 条第 19 項参照）でない限り、これらの役割は単一の人物に割り当ててはならず、複数の異なる個人に分割して割り当てる必要がある。

c. 製造事業者は、両方の役割に機能メールボックスを割り当てる必要があり、これらの役割に関わる個人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。

d. これら二つの役割は、その割り当てに基づいて分離されなければならない。

e. これら 2 つの役割は緊密に連携し、相互に情報を共有するとともに、他方の役割が関与する事案については脆弱性事例を内部で相互転送しなければならない。

f. 最初のサイバーセキュリティ連絡窓口は、製造事業者の製品およびサービスの脆弱性対応を扱う製造事業者の PSIRT でなければならない。

g. 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す必要がある。したがって、メールのローカル部分（メールプレフィックス）は「psirt」とすることを推奨する（例：psirt@example.com）。

h. 第二のサイバーセキュリティ連絡先は、製造事業者の CSIRT でなければならない。これは製造事業者のインフラストラクチャの脆弱性対応を扱う。

i. 製造事業者の 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す必要がある。したがって、メールのローカル部分（メールプレフィックス）は「csirt」であることが望ましい。例：

   csirt@example.com。

j. 製造事業者は、現行の BSI TR-03116 Part 4 または現行の ECCG 合意暗号化メカニズムの仕様に従い、機能別メールボックスの各メールアドレスに対して RFC 9580 に基づく専用の OpenPGP 鍵を使用し、これらの鍵を用いた暗号化および署名付き通信を提供しなければならない。

k. 製造事業者は、現行の BSI TR-03116 Part 4 または現行の ECCG 合意暗号メカニズムの仕様に基づき、機能メールボックスの対応するメールアドレスに対して追加の暗号化オプションを提供してもよい。

   現行の ECCG 合意暗号メカニズムの仕様に基づき、機能メールボックスの対応する電子メールアドレスに対して追加の暗号化オプションを提供し、これらの鍵を用いた暗号化および署名付きコミュニケーション（例：S/MIME）を提供してもよい。

l. j および k で言及された鍵/証明書の有効期間が、現行の BSI TR-03116 Part 4 または現行の ECCG 合意暗号メカニズムにおいて別段の定めがない限り、5 年を超えてはならない。

m. 製造事業者が零細企業でない限り、製造事業者は両役割に対し、欠員を補填し CVD ポリシー（4.4 節参照）の応答時間と保証を確実にする十分なリソースを提供すべきである。

n. 製造事業者は、両役割において脆弱性報告が少なくとも英語で受信・処理可能であることを保証しなければならない。

o. 製造事業者は、両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。

p. 製造事業者は、両役割に関与する者の任務を明確に定義しなければならない。

q. 製造事業者は、機能メールボックスのメールアドレスがメール受信に高い準備態勢にあることを確保すべきである。これは少なくとも、外部メールアドレスから毎日（自動的に）機能メールボックスへメールを送信することでテストすべきである。

### 4.3.2 セキュリティ連絡先の暗号化オプションの提供

製造事業者が役割別連絡オプションのメールアドレス（4.3.1 節参照）を自社ウェブサイトのどこかに提供する場合、**例えば security.txt**（4.2.3 節と 4.2.4 節を参照）、CVD ポリシー（4.4.3 節参照）、または脆弱性報告受付ページ（4.5.3 節参照）に提供する場合:

a. 製造事業者は、これらのメールアドレスに対応する OpenPGP 公開鍵（4.3.1 j 項で言及）の直接ダウンロード場所の Web URI（RFC 7230 セクション 2.7.2 に準拠）を、RFC 9580 に準拠した ASCII アーマー形式の**.asc** ファイルとして提供しなければならない。

b. 製造事業者は、これらのメールアドレスに対応する OpenPGP 公開鍵のフィンガープリントを引用しなければならない。

c. 追加の暗号化オプション（4.3.1k 項に記載）が存在する場合は、製造事業者はこれらの追加暗号化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場所の Web URI（RFC 7230 セクション 2.7.2 に準拠）を提供し、それらのフィンガープリントを引用すべきである。

d. a および c で言及された Web URI は、公開鍵または証明書に直接リンクしなければならず、公開鍵または証明書のダウンロードオプションがある Web ページにリンクしてはならない。

### 4.3.3 脆弱性報告用ウェブフォーム

a. 製造事業者は、脆弱性報告用のウェブフォームを連絡手段として設定しなければならない。したがって、自社ウェブサイト上にこのウェブフォームを備えたウェブページを作成する必要がある。

b. このウェブフォームを備えたウェブページは、製造事業者サイトのひとつでなければならない.

c. このウェブフォームは、脆弱性報告を匿名で送信できるものでなければならない。

d. 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。

e. このウェブフォームは、必須情報の完全な入力が保証されるよう、構造化された方法で脆弱性報告をユーザーに案内すべきである。

f. このウェブフォームは高可用性を有すべきである。少なくとも毎日（自動的に）フォームに入力・送信するテストを実施すべきである。

### 4.3.4 脆弱性報告受付用ウェブページ

製造事業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（4.5 節参照）。

## 4.4 CVD ポリシー

CVD ポリシーは、CVD プロセス全体の支援、改善、標準化、迅速化を目的としている。本ポリシーは脆弱性報告の取り扱い方法を定義します。これには、報告事業体に対する製造事業者保証、報告の処理方法、および CVD プロセスの成功に必要な要件が含まれる。したがって、製造事業者の CVD ポリシーは、少なくとも下記の要件を満たす必要がある。これらは特に「BSI セキュリティ 研究者向け CVD ガイドライン」[31] 、「国家調整脆弱性開示ポリシー実施ガイドライン」[32] 、および ETSI TR 103 838 V1.1.1[33] に基づいている。

[31] https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html

[32] https://ec.europa.eu/newsroom/dae/redirection/document/99973

[33]

インセンティブの提供は、製造事業者製品やインフラにおける脆弱性報告の意欲を高める可能性がある。「栄誉の殿堂」ウェブページを設けることは、製造事業者が脆弱性報告を行った事業体に対して公に感謝を示す一つの方法である。脆弱性を発見した者に対する金銭的報酬（バグ報奨金プログラム）を確立することで、製造事業者は感謝の意を表し、積極的なインセンティブ構造を構築できる。したがって、CVD ポリシーへの報奨プログラム追加は推奨される（CRA の前文 76 項参照）。

### 4.4.1 概要

a. 製造事業者は、CVD ポリシーの最終更新日（初版の場合は作成日）が明確に表示されることを保証しなければならない。

b. 製造事業者は、CVD ポリシーが製造事業者へ明確に帰属することを保証しなければならない。

c. 製造事業者は、CVD ポリシーが最新であることを確認するため、少なくとも年 1 回レビューを行わなければならない。

### 4.4.2 対応する国内 CSIRT

製造事業者の製品または製造事業者のインフラに影響を与える脆弱性が積極的に悪用されている場合、

a. 製造事業者は、これを知った時点で遅滞なく、対応する国内 CSIRT（セクション 3.1.7 参照）に通知し、

b. 製造事業者は、新たな情報、緩和措置及びそのスケジュールについて、対応する国内 CSIRT に通知し、これらを対応する国内 CSIRT と調整しなければならない。

### 4.4.3 連絡先詳細

製造事業者は、役割別連絡オプション（4.3.1 節参照）の機能別メールボックスのメールアドレスを提供しなければならない。したがって、4.3.2 節の要件を適用しなければならない。

### 4.4.4 報告事業体に対する製造事業者の保証

a. 製造事業者は、法律で認められる範囲で、受信した脆弱性報告を機密扱いすることを保証しなければならない。ただし、脆弱性の公開開示に必要な情報（4.4.10 節参照）は除外される。

b. 製造事業者は、報告事業体の明示的な同意なしに、報告事業体の個人データをサードパーティに開示しないことを保証しなければならない。

c. 製造事業者は、各脆弱性報告または既提出脆弱性報告の更新に対し、保証された対応時間内（4.4.8 節参照）に回答を提供しなければならない。

d. 製造事業者は、通知事業体が本方針及びその原則を遵守している限り、報告事業体に対して刑事訴追を行わないことを保証しなければならない。ただし、明らかな犯罪意図が認められる場合はこの限りではない。

e. 製造事業者は、CVD プロセス全体を通じて信頼できる情報交換の窓口として対応可能であることを保証しなければならない。

f. 製造事業者は、報告事業体から要請があった場合、有効な脆弱性を報告し CVD プロセスが完了した後、製造事業者の CVD ポリシーに従い、報告事業体の名称/別名および希望する参照情報を製造事業者の承認ウェブページ（栄誉の殿堂）に掲載することを推奨する。

g. 製造事業者は、報告事業体に対し秘密保持契約（NDA）への署名を要求してはならない。

h. 製造事業者は、機密情報の伝送に暗号化およびデジタル署名付き電子メールの使用を報告事業体に推奨しなければならない。

### 4.4.5 脆弱性ガイドライン

製造事業者は、CVD ポリシーの一部として脆弱性ガイドラインを公開し、有効な脆弱性の定義を定めるものとする。有効な脆弱性の分類においては、以下の要件のみを考慮すべきである：

a. 脆弱性は、製造事業者の製品または製造事業者インフラストラクチャのいずれかに影響を与えなければならない。

b. 脆弱性報告は、公に知られていない情報に関連しているべきである。

c. 脆弱性報告は、裏付けとなる文書がない自動ツールやスキャンによる結果であってはならない。

### 4.4.6 報告事業体向け行動規範

善意に基づく目的で悪意のない報告者のみを報奨するため、製造事業者は、報告事業体に期待される行動規範と非遵守の結果を定めた行動規範を公表してもよい。ただし、製造事業者は、非遵守事業体の報告についても可能な限り最善の対応を保証しなければならない。行動規範には以下の点を含めてもよい：

a. 報告事業体による報告された脆弱性の悪用がないこと。これは、報告された脆弱性を超える損害が生じていないことを意味する。

b. 報告事業体による製造事業者 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、（分散型）DoS 攻撃、「ブルートフォース」攻撃など）は行われていないこと。

c. 報告事業体によるサードパーティのシステムまたはデータの操作、侵害、改変が行われていないこと。

d. 報告事業体が、ダークネット市場などで、サードパーティが犯罪を犯すために使用できる脆弱性悪用ツールを有償または無償で提供していないこと。

e. 報告事業体による第 4.4.7 項 c の違反行為（例：製造事業者への謝辞掲載ページにおける氏名/別名、または掲載希望の参照情報）は存在しない。

非準拠の結果として、以下の点が生じる可能性がある：

a. 報告事業体は、バグ報奨金プログラムなどからの報酬を受け取れません。

b. 報告事業体は謝辞掲載ページ（栄誉の殿堂）に掲載されない。

### 4.4.7 良好なコミュニケーション

a. 製造事業者は、既に修正済みの脆弱性に関する報告情報であっても、CVD プロセスの一部として追加処理の対象とならない場合でも、当該情報が確実に受領・確認されるよう確保すべきである。

b. 製造事業者は、脆弱性報告において良好なコミュニケーションが重要であることを説明し、報告事業体が問い合わせ用に少なくとも 1 つの有効な連絡先（できればメールアドレス）を提供すべきであることを伝えるべきである。

c. 製造事業者は、すべての関係事業体が互いを尊重し合うこと、および差別、性差別、侮辱などの容認できない行為の余地がないことを明確に強調すべきである。

d. 製造事業者は、どの連絡手段を受け入れるかを宣言すべきである。

e. 製造事業者は、少なくともメールアドレスと電話番号を有効な連絡手段として受け入れる必要がある。

f. 製造事業者は、報告事業体からの脆弱性報告状況に関する問い合わせを歓迎することを明示すべきである。

g. 製造事業者は、すべての報告が可能な限り最善の方法で処理され、単一のアナリストによって閉じられないことを保証しなければならない。

### 4.4.8 保証された応答時間

a. 製造事業者は、脆弱性報告または既存報告の更新に対する簡易応答を、匿名で報告された脆弱性（ ）を除き、5 営業日以内に提供しなければならない。この簡易応答は自動応答であってはならない。

b. 製造事業者は、匿名で報告された脆弱性でない限り、追加分析後の詳細なフィードバックを 10 営業日以内に提供しなければならない。

c. この詳細なフィードバックには、少なくとも以下のいずれかを含めなければならない：

- 報告された脆弱性を確認するか否かの製造事業者による声明、
- 報告された脆弱性を理解するための有意義な質問、または
- 報告された脆弱性の調査に時間がかかる理由の説明、および 10 営業日以内に更新情報を提供する約束。

### 4.4.9 匿名報告オプション

a. 製造事業者は、脆弱性報告を匿名で提出するための容易に見つけられるオプションを提供しなければならない。これは脆弱性報告用ウェブフォームであるべきである（4.3.3 節参照）。

b. 製造事業者は、特に複雑な問題の場合、追加の説明や文書が必要となる可能性があることを明記すべきである。

c. 報告事業体が技術的または内容に関する問い合わせに対応しない場合、対応する脆弱性報告は限定的にしか処理されないか、あるいは全く処理されない可能性があることを製造事業者は明示すべきである。

d. 製造事業者は、技術的または内容に関する問い合わせを要求する手段が欠如しているため、匿名報告は限定的にしか処理されないか、あるいは全く処理されない可能性があることを明確に述べなければならない。

### 4.4.10 脆弱性の開示

a. 製造事業者は、妥当性確認かつ確認済みの脆弱性について、影響を受ける製品が上市される前に脆弱性を認識し修正した場合を除き、90 日以内に公開開示す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延について正当な理由と説明がある場合、対応する国内 CSIRT と緊密に協議の上、開示までの期間を一度に限りさらに 90 日間延長できる。例外として、製造事業者の要請に基づき、対応する国内 CSIRT が公的開示までの期間をさらに延長できる。

b. この公開開示は、製造事業者の要請に基づき、対応する国内 CSIRT または ENISA と協議の上、少なくとも ENISA が維持する欧州脆弱性データベース（EUVD）[34] において行わなければならない。

### 4.4.11 CVD プロセスの終了

a. 製造事業者は、CVD プロセスが完了したとみなされる条件を明確かつ公に表明しなければならない。

[34] https://euvd.enisa.europa.eu/

b. 製造事業者は、脆弱性が匿名で報告された場合を除き、報告事業体に対し不当な遅延なく CVD プロセスの終了を通知すべきである。

c. 製造事業者は、脆弱性報告の指摘が根拠のないものである場合、CVD プロセスが完了したとみなすべきである。

d. サービス（例：Web サービス）の脆弱性が修正され、かつ公開された場合、製造事業者は CVD プロセスが完了したとみなすべきである。

e. 製造事業者は、脆弱性が適切なパッチによって緩和または修正され、かつ公開された場合、CVD プロセスが完了したとみなすべきである。

f. 報告事業体が技術的または内容に関する問い合わせに対して少なくとも 30 日間対応せず、その結果、対応する脆弱性報告が限定的にしか処理できない、あるいは全く処理できない場合、製造事業者は CVD プロセスが完了したとみなすことができる。

g. 製造事業者は、脆弱性が公に開示され、かつ対応する国内 CSIRT との協議により、当該脆弱性が緩和または修正されるとはもはや想定できない場合、CVD プロセスが完了したとみなすことができる。

## 4.5 脆弱性報告受付用ウェブページ

外部事業体は、脆弱性報告の提出に関する重要な情報をすべて、製造事業者ウェブサイト上の中心的な場所で入手できる必要がある。したがって、脆弱性報告受付用ウェブページは、少なくとも以下の機能を備えていなければなりません。

### 4.5.1 概要

a. 脆弱性報告受付ウェブページは、製造事業者のウェブサイトの一部でなければならない。

b. このウェブページは、JavaScript やその他のクライアントサイド実行スクリプトを有効化せずに、製造事業者のウェブサイトのホームページ上で容易に見つけられるリンクを通じて少なくともアクセス可能でなければならない.

c. このウェブページのウェブ URI（RFC 7230 セクション 2.7.2 に準拠）のパスは、その機能を明確に示すものでなければならない。例：https://www.example.com/security-contact。製造事業者サイトの別のウェブ URI（RFC 7230 セクション 2.7.2 に準拠）へのリダイレクトは許可される。

d. 製造事業者は、JavaScript やその他のクライアントサイド実行スクリプトを有効化せず、ログイン手続きやその他の制限（例：ペイウォール）なしに、本ウェブページ上の全情報へ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。

e. このウェブページの情報は明確に構造化されなければならない。

f. 製造事業者は、個人データの送信に関するセクション（例：報告事業体の連絡先詳細）の近くに、自社のプライバシーポリシーへのリンクを掲載すべきである。

### 4.5.2 CVD ポリシーの公開

a. 製造事業者は、CVD ポリシーが公開されているウェブページへリダイレクト、転送、またはルーティングするための見つけやすいリンクを本ウェブページに設置しなければならない。したがって、製造事業者は CVD ポリシーを掲載したウェブページを作成しなければならない。

b. 要件 4.5.1 a、d、および e は、CVD ポリシーウェブページにも適用される。

### 4.5.3 連絡先オプションの公開

a. 製造事業者は、役割別連絡先オプション（4.3.1 節参照）のメールアドレスを提供しなければならない。したがって、4.3.2 節の要求事項を適用しなければならない。

b. 製造事業者は、これらのアドレスを自社ウェブサイトの「お問い合わせ」ページに追加で公開してもよい。

c. 製造事業者は、**security.txt の**署名用として、対応する OpenPGP 公開鍵の直接ダウンロード場所の Web URI（RFC 7230 セクション 2.7.2 に準拠）を、RFC 9580 に準拠した ASCII アーマー形式の**.**asc ファイルとして提供しなければならない（セクション 4.2.10 参照）。

d. 製造事業者は、**security.txt の**署名用 OpenPGP 公開鍵のフィンガープリントを引用しなければならない（4.2.10 節参照）。

e. 製造事業者は、脆弱性報告用ウェブフォームへのウェブ URI（RFC 7230 セクション 2.7.2 に準拠）を提供しなければならない（セクション 4.3.2 参照）。

f. 連絡先オプションの有効期限は、期限切れ前に十分な余裕をもって指定および更新されなければならない。この有効期限は、最大でも 1 年先とすべきである。

# 5. 附属書

本節では補足説明情報を提供する。

## 5.1 詳細情報

### 5.1.1「脆弱性対応 v2.0 – 製造業者向け推奨事項」

BSI は、脆弱性を適切に扱う方法に関する製造事業者向け推奨事項をドイツ語で公開している。
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf

### 5.1.2 脆弱性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優良事例を識別するため、本調査を公表した。

https://www.enisa.europa.eu/publications/脆弱性-disclosure

### 5.1.3 脆弱性開示の調整に関する CERT ガイド

カーネギーメロン大学ソフトウェア工学研究所が当初発行した「CERT 協調的脆弱性開示ガイド」のウェブ版を、CERT 調整センター（CERT/CC）が公開した。

Web 版： https://certcc.github.io/CERT-Guide-to-CVD/

原典： https://insights.sei.cmu.edu/library/the-cert-guide-to-coordinated-vulnerabilitydisclosure-2/

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

この ISO 標準は、脆弱性の開示に関するさらなる推奨事項と要求事項を規定している。

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

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

この ISO 標準は、脆弱性対応プロセスに関するさらなる推奨事項と要求事項を規定している。

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

### 5.1.6 ISO/IEC 20153:2025

この ISO 標準は、OASIS CSAF v2.0 仕様に基づく自動化および機械可読セキュリティアドバイザリの形式と配布について規定する。

https://www.iso.org/standard/89986.htmlhttps://webstore.iec.ch/en/publication/105858

### 5.1.7 SecureDrop

これは、匿名の情報源から文書を受け取り、かつ彼らとコミュニケーションす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

### 5.1.8 CSAF プロバイダ

これは、標準に準拠した CSAF 文書を提供するために必要なすべてのメタデータと構造を自動生成するためのオープンソースツールである。

https://github.com/gocsaf/csaf/blob/main/docs/csaf_provider.md