セキュリティ研究者と連携するための協調的脆弱性開示プログラムの確立

公開日:2026年7月15日

米国サイバーセキュリティ・インフラセキュリティ庁(CISA)
米国国家安全保障局(NSA)
日本コンピュータ緊急対応チーム コーディネーションセンター(JPCERT/CC)
オランダ国家サイバーセキュリティセンター(NCSC-NL)
英国国家サイバーセキュリティセンター(NCSC-UK)

TLP:CLEAR

ガイダンスの概要

タイトル	セキュリティ研究者と連携するための協調的脆弱性開示プログラムの確立
初版公開日	2026年7月15日
エグゼクティブサマリー	本ガイダンスは、サプライヤーがセキュリティ研究者と効果的かつ透明性をもって連携し、脆弱性の報告と修復を行うための協調的脆弱性開示(CVD)プログラムを設計・実装する際のベストプラクティスを示すものである。
主な取り組み	• セキュリティ研究者に脆弱性の報告方法を案内する脆弱性開示ポリシー(VDP)を作成し、公開する。[1] • 報告された脆弱性が製品に影響する場合の、トリアージ、修復、共通脆弱性識別子(CVE)の付与に関するプロセスを定義し、脆弱性が迅速かつ適切に対処されるようにする。 • (各国のコンピュータセキュリティインシデント対応チームなどの)仲介機関を活用し、既存のCVDプログラムを代替または補完することで、セキュリティ研究者との連携を効果的に支援する。
想定読者	**組織:** ソフトウェア製造事業者およびオンラインサービス提供事業者。 **役割:** • National Initiative for Cybersecurity Education(NICE)フレームワークの職務区分:サイバーセキュリティ政策立案者、プログラムマネージャー、脆弱性アナリスト、セキュアソフトウェア開発者。 • その他の職務:プロダクトセキュリティインシデント対応チーム(PSIRT)マネージャー、PSIRTアナリスト、CVDマネージャー。

[1] 策定機関は、オープンソースソフトウェアのメンテナーについては、VDPの策定・維持に関する期待事項が異なることを認識している。

はじめに

ウェブサービスを運用する多くのソフトウェア製造事業者およびオンラインサービス提供事業者(以下「サプライヤー」という)[2]は、製品をリリースする前にセキュリティ上の脆弱性を特定し対処する社内チームを有している。しかし、社内の取り組みだけでは、あらゆる潜在的な脆弱性を発見するには不十分な場合がある。社内テストでは特定されないセキュリティ上の欠陥を洗い出す一助として、本ガイダンスでは、ソフトウェア、ネットワーク、ハードウェアにおけるセキュリティ上の弱点を発見することを専門とする外部のセキュリティ研究者の知見をサプライヤーがどのように活用できるかについて解説する。サプライヤーは、協調的脆弱性開示(CVD)プログラムを実装することで、これらの研究者と連携すべきである。[3] 強固なCVDプログラムにより、組織は脆弱性報告の頻度や質の変化に対応できるようになり、また、セキュリティ研究者に対しては、不当な法的措置や報復を恐れることなく脆弱性を報告する方法について明確な指針を提供することができる。

本ガイドは、米国サイバーセキュリティ・インフラセキュリティ庁(CISA)および国家安全保障局(NSA)、日本コンピュータ緊急対応チーム コーディネーションセンター(JPCERT/CC)、オランダ国家サイバーセキュリティセンター(NCSC-NL)、そして英国国家サイバーセキュリティセンター(NCSC-UK)(以下「策定機関」という)により作成されたものであり、サプライヤーがセキュリティ研究者と効果的に連携するためのCVDプログラムを設計・実装する際のベストプラクティスを示すものである。[4] 策定機関は、サプライヤー、特にソフトウェア製造事業者が、本共同ガイドで示すベストプラクティスに沿ったCVDプログラムを策定することを推奨する。

CVDプログラムを策定する

明確に定義され、体系化され、継続的に維持されるCVDプログラムは、サプライヤーがセキュリティ研究者と連携し、効率的に脆弱性へ対処する能力を高める。

CVDプログラムを設計する第一歩は、明確な脆弱性開示ポリシー(VDP)を作成し、公開することである。VDPは、報告のトリアージ、脆弱性の修復、共通脆弱性識別子(CVE)[5]の付与、および報告された脆弱性に関するCVEレコードの公開に関するプロセスを定義するものでなければならない。

脆弱性開示ポリシーを作成し、公開する

VDPは、セキュリティ上の脆弱性を適切に報告する方法、脆弱性を調査してよい対象システム、許容されるテストの種類、および開示プロセスにおけるサプライヤーとセキュリティ研究者双方への期待事項について、研究者に指針を提供するものである。以下のガイドラインに従ってVDPを作成・公開することで、組織はセキュリティ研究者が適切に脆弱性を報告し、開示に関する期待事項を理解できるようなプロセスを定義することができる。これにより、脆弱性へ効果的に対処するための、研究者とのよりスムーズで効果的な連携を促進できる。

注: 米国政府の「拘束的運用指令(BOD)20-01」は、米国連邦文民行政機関(FCEB)に対し、脆弱性開示ポリシーの策定と公開を義務付けている。EUサイバーレジリエンス法(CRA)は、EU域内で事業を行うすべてのサプライヤーおよびその加盟国に対し、そのようなポリシーの維持を義務付けている。[6]

CISAの「Secure by Design」イニシアティブ

VDPの作成・公開は、ソフトウェア製造事業者に組織プロセスの透明性と説明責任の徹底を促す、CISAの「Secure by Design」イニシアティブにおける主要な製品開発上の実践事項である。

また、組織はCISAの「Secure by Design Pledge(誓約)」に参加することでセキュリティ研究を積極的に受け入れることができる。この誓約には、VDPの立ち上げが目標として含まれている。

顧客のセキュリティ成果へのコミットメントを示す

VDPを通じて、組織は秘密保持契約(NDA)やサイレント修正[7]といった包括的な開示制限を設けないことにより、顧客のセキュリティ成果に対するコミットメントを示すべきである。これにより、説明責任を示すことで透明性が高まり、明確でオープンなコミュニケーションが促進され、顧客、パートナー、およびセキュリティコミュニティとの信頼関係が強化される。

公開性を保つ

サプライヤーは自社ウェブサイトでVDPを公開し、脆弱性の報告が一般に開かれていることを明確に示すべきである。CVDプログラムへの参加は、セキュリティ研究者の国籍、年齢、その他の制限的な条件を根拠に制限すべきではない。ただし、サプライヤーが特定の政府による制裁の対象となる主体と連携できない場合はこの限りではない。

---

[2] 共通脆弱性識別子(CVE)の用語集は、「サプライヤー」を「製品を開発、維持、または提供する主体」であり、「通常、脆弱性報告を調査し、修正または低減策を講じる責任と能力を有する」ものと定義している。

[3] 本ガイダンスは、商用および公開されているオープンソースソフトウェアのサプライヤーに対し、公開のCVEレコードおよび脆弱性開示を伴うCVDプログラムの実装を推奨する。一方、政府専用市販ソフトウェア(GOTS)のサプライヤーについては、非公開の開示を伴うCVDプログラムの実装が望ましい。

[4] 国際標準化機構(ISO)/国際電気標準会議(IEC)「29147:2018:情報技術 — セキュリティ技術 — 脆弱性開示」、ISO、第2版、2018年10月。

[5] 脆弱性とは、悪用されうるソフトウェア、ハードウェア、または設定上の弱点をいう。CVEは、公に開示された特定の脆弱性に対する標準化された識別子およびレコードである(詳細はNIST SP 800-53 Rev.5を参照)。

[6] 欧州連合「デジタル要素を含む製品に関する水平的サイバーセキュリティ要件、および規則(EU)No 168/2013、規則(EU)No 2019/1020、指令(EU)2020/1828を改正する2024年10月23日付欧州議会および理事会規則(EU)2024/2847(サイバーレジリエンス法)」、欧州連合官報、2024年10月23日。

[7] CERT®の「協調的脆弱性開示ガイド」の定義によれば、「サイレント修正とは、ベンダーが脆弱性を認識し修正しているにもかかわらず、その後のリリースノートにおいて当該脆弱性の存在に言及しないことをいう。その結果、サイレント修正は、明確に記載された修正に比べて広く展開される可能性が低くなる。」「公表への備え」、CERT®協調的脆弱性開示ガイド、カーネギーメロン大学 コンピュータ緊急対応チーム。

セキュリティテストの対象範囲を可能な限り広くする

サプライヤーは、セキュリティ研究者がサプライヤーのネットワーク内で脆弱性を発見するために、行ってよいこと・行ってはならないことを記したVDPガイドラインを提供すべきである。テスト対象とするIPアドレスの範囲を限定するといった恣意的な境界線は、悪意あるサイバー攻撃者を抑止するものではなく、セキュリティ研究者を制約すべきでもない。VDPガイドラインは、研究者が実際の脅威アクターの挙動を模した幅広いテスト手法を活用できるよう、十分に広い範囲を認めるべきである。ただし、これらのガイドラインは、脆弱性の存在を確認するために必要な最小限の範囲に、研究者による悪用を制限するものでもあるべきである。

禁止される行為を明確に示す

VDPにおいて、研究者に対し禁止される行為を明示すること。これらの禁止行為には、システム、データ、利用者の機密性、完全性、可用性を損なおうとするあらゆる行為を含めるべきである。禁止行為の例としては以下が挙げられる。

- システムへのマルウェアの持ち込み
- システム内のデータの複製、編集、削除
- システムへの変更
- システムへの反復的なアクセス、または他者とのアクセス権限の共有
- システムへのアクセス権取得を目的としたブルートフォース攻撃の実施
- サービス拒否(DoS)攻撃またはソーシャルエンジニアリングの実施

報告に必要な最低限の要件を明示する

VDPは、脆弱性の概要や概念実証(PoC)など、セキュリティ研究者が報告書に含めるべき最低限の情報について明確に記載すべきである。加えて、VDPには、理想的な報告書の内容(例:最小限に抑えたPoC、問題に関する説明資料、影響評価など)についても示すべきである。一部のセキュリティ研究者は身元の秘匿を望むため、匿名での報告受付についても検討すること。

脆弱性の報告方法を明確に定義する

VDPは、電子メール、ウェブプラットフォーム、あるいはCISAなどのサードパーティの仲介者を通じてなど、セキュリティ研究者が脆弱性を安全に報告する方法を明確に定義すべきである。策定機関は、ウェブサイトにおいて security.txt ファイルを使用し、セキュリティ研究者に脆弱性報告の明確な手順を提供することを推奨する。インターネット技術タスクフォース(IETF)のRequest for Comments(RFC)9116に記載されているとおり、この security.txt ファイルは、連絡先情報やポリシーへの容易なアクセスを提供することで、サプライヤーが効率的なCVDプログラムを運用する一助となる、機械可読かつ人間可読な仕組みとして定義されている。[8]

[8] Edwin Foudfil、Yakov Shafranovich「RFC 9116: A File Format to Aid in Security Vulnerability Disclosure」、インターネット技術タスクフォース(IETF)、2022年4月。

TLP:CLEAR

誠実に取り組む研究者に対してセーフハーバーを提供する

VDPには、組織が研究者の貢献を重視していることを保証する「セーフハーバー」に関する記述を含めるべきである。「セーフハーバー」の提供は、関連する「反ハッキング」法[9]の下で、VDPが(組織のポリシーと整合する形で)研究者の活動を許可するものであることを明確にするものである。セキュリティ研究者は、製品セキュリティの強化を目的とした誠実な研究活動を行いながらも、これまで様々な脅威に直面してきた。策定機関は、サプライヤーが自社の法律顧問と連携し、それぞれの管轄区域やリスクプロファイルに適した「セーフハーバー」文言をVDPに盛り込むよう策定することを推奨する。例示として、以下の文例がそのような条項の出発点となりうる。

> 「本ポリシーに従い誠実な努力をもってセキュリティ研究を行った場合、[サプライヤー名]は当該研究を許可されたものとみなし、問題を迅速に理解・解決するために貴殿と協力し、当該研究に関連して法的措置を推奨または追求することはありません。本ポリシーに従って行われた活動について第三者から法的措置が提起された場合には、当社はこの許可の事実を明らかにします。」

脆弱性情報の共有に関する明確な期待事項を定める

VDPは、公開前において、適切な関係者のみが脆弱性を認識し、その調整に関与することを確実にするための、情報共有に関する期待事項を定めるべきである。

報告された脆弱性の修復・開示について合理的な期限を設ける

VDPにおいて、報告された脆弱性の修復および開示に関する期限を設定すること。この期限は、固定期間、最短または最長期間、あるいは交渉によって定める初期設定期間のいずれでもよい。サプライヤーと研究者は、(適切な修正の開発・テストを可能にするためなど)必要に応じて非公開期間を協力して調整し、不当な遅延なく報告された脆弱性を開示すべきである。

悪意ある攻撃者が独自に脆弱性を発見する可能性があるため、非公開期間を長くすることが必ずしもリスクを低減するとは限らない。加えて、関係者が多い非公開期間ほど、脆弱性を把握するいずれかの関係者が公表しうることから、意図せぬ情報漏えいにつながりやすい。

脆弱性アドバイザリの公開プロセスを明確に記述する

VDPは、研究者や、(CISAや各国のコンピュータセキュリティインシデント対応チームなどの)サードパーティのコーディネーターといった仲介者が、公開プロセスにおいてどのように協力できるかについて詳述すべきである。サプライヤーは、脆弱性アドバイザリにおいて研究者への謝辞を掲載することを検討すべきである。加えて、アドバイザリは容易にアクセスできるようにし、有料の壁の内側で公開してはならない。

[9] 米国におけるこのような法律の例として、Computer Fraud and Abuse Act(コンピュータ詐欺および濫用防止法)およびDigital Millennium Copyright Act(デジタルミレニアム著作権法)が挙げられる。

TLP:CLEAR

CVE IDに関するプロセスを定義する

確立されたVDPに加え、効果的なCVDプログラムには、製品に影響する報告された脆弱性についてのトリアージ、修復、CVE IDの付与に関する明確なプロセスが含まれる。これらのプロセスにより、サプライヤーはセキュリティ研究者から受け取った報告をトリアージし、脆弱性を迅速かつ適切に修復できるようになる。

脆弱性報告を管理するための明確な社内プロセスは、顧客のリスクを低減し、サイバーセキュリティへの積極的な取り組みを促進する一助となる。サプライヤーは、透明性を保ち、期限内の解決に対する信頼を維持するため、研究者に対して定期的かつ積極的に進捗状況を報告すべきである。

策定機関は、こうしたプロセスを実施するにあたり、以下の主要なステップの実施を推奨する。

セキュリティ研究者からの連絡を確認する

2~3営業日など、定めた期限内にセキュリティ研究者と連絡を取るための専用の仕組みを確立すること。

> **注:** 策定機関は、脆弱性の開示およびトリアージのプロセスを、既存のカスタマーサポート窓口とは分離することを推奨する。既存の窓口を利用すると、報告が見落とされたり軽視されたりするほか、意図せぬ開示につながるおそれがある。

報告された脆弱性のトリアージと深刻度評価を行う

CVDプログラム担当者に対し、報告された脆弱性が対象製品およびそのエンドユーザーにリスクをもたらすかどうかを評価するため、脆弱性報告書を確認するよう指示すること。サプライヤーは、報告の優先順位付けを支援するため、Stakeholder-Specific Vulnerability Categorization(SSVC)などのリスク評価・意思決定支援システムを活用すべきである。[10] 脆弱性のリスクを理解することは、修正開発のスケジュールを決定する上で重要である。判定されたリスクに応じて、新機能開発や通常のバグ修正リリースよりも脆弱性の修復を優先すること。さらに、リスクを評価する際には、顧客が既存の低減策や推奨される堅牢化ガイドラインを十分に実施していると想定してはならない。

報告された脆弱性への修正を開発する

報告された脆弱性に修正が必要な場合は、それに応じて修復を行うこと。適切な修復には、修正の発行や、設定変更・追加のセキュリティ管理策といったその他の低減策が含まれうる。ベストプラクティスとして、報告された脆弱性に確実に対処できているかを検証するため、低減策、修正、パッチの詳細を研究者と共有すること。通常の製品リリースサイクルから外れる場合であっても、VDPで定めた期限内に低減策または修復に関するガイダンスを公開すること。

開発チームには、報告された脆弱性を修正するだけでなく、特にMITREの2007年の論文「Unforgivable Vulnerabilities(許されざる脆弱性)」に記載されているような、同じ種類の脆弱性の他の事例についても確認するよう徹底すること。

---

[10] CISAは、FCEB機関における脆弱性修復の優先順位付けを支援するためにSSVCを使用している。

これらの種類に該当する社内で発見された脆弱性についても、CVE IDを付与すべきである。詳細は、NCSC-UKの報告書「『許される』脆弱性と『許されない』脆弱性を評価する手法」を参照のこと。[11]

加えて、組織のプロセスに従い、組織の製品に繰り返し現れる脆弱性の種類について、経営幹部に正式に報告すべきである。こうした種類の脆弱性を排除する計画の必要性を示すため、明確な指標やトレンドを用いること。詳細はCISAの「Secure by Design Alert」シリーズを参照のこと。

CVE IDを付与し、レコードを公開する

報告がCVE IDの付与に値するかどうかを判断する際には、CVEプログラムの運用規則を参照すること。CVEレコードは、米国政府の脆弱性対応およびリスク低減の取り組みにとって前提条件となるものである。CVEはまた、ソフトウェアサプライチェーン全体での認知度を高めることにより、顧客との透明性も向上させる。サプライヤーは、社内・社外いずれで発見されたかを問わず、自社製品において発見された脆弱性にCVE IDを付与すべきである。

CVE番号採番機関(CNA)がCVEレコードを発行する。自組織がCNAでない場合は、CNAとなることを検討されたい。サプライヤーは、自社製品に影響する脆弱性についてCVE IDを直接付与し、CVEレコードを公開するのに最も適した立場にある。CNAになる方法の詳細については、cna@cisa.dhs.gov まで問い合わせること。

CVE IDの付与が必要であり、自組織・研究者いずれもCNAでない場合は、CVEプログラムの「Request a CVE ID」ページに記載された手順を参照すること。

CVEレコードの完全性、正確性、適時性を確保する

顧客および一般に対し、脆弱性の実際の性質やそれに伴うリスクについての理解を提供するため、CVEレコードには十分かつ正確な詳細を記載すること。脆弱性の根本原因を伝えるCommon Weakness Enumeration(CWE)の項目、および技術的影響や悪用可能性を推定するForum of Incident Response and Security Teams(FIRST)のCVSS仕様書に基づくベクトル文字列を記載すること。[12]

脆弱性が確認され低減された後は、不要な遅延なく、速やかにCVEレコードを付与・公開すること。CVE ID付与に関する詳細は、CVE番号採番機関(CNA)運用規則を参照のこと。

顧客向けのコミュニケーションを作成する

脆弱性、その深刻度スコア、および必要な低減措置に関する公開情報を顧客に対して公表すること。サプライヤーは、この情報を(ログインを必要としないなど)制限のない自社ウェブサイト上の場所で提供すべきである。機械可読な形でセキュリティアドバイザリを公開するための標準化された枠組みを提供する、Common Security Advisory Framework(CSAF)[13]を用いてアドバイザリを公開すること。これにより、

[11] National Cyber Security Centre(NCSC)「A Method to Assess Forgivable vs Unforgivable Vulnerabilities」、2025年1月28日。

[12] 「Common Vulnerability Scoring System Version 4.0: Specification Document」、FIRST、最終更新2024年6月18日。

[13] 詳細はCommon Security Advisory Framework(CSAF)を参照。

TLP:CLEAR

脆弱性情報の自動分析が可能となる。サプライヤーが自社ウェブサイトで公開できない場合には、仲介機関を活用して代わりに公開することができる。理想的には、脆弱性の公開情報には以下を含めるべきである。

- 脆弱性に関する包括的かつ正確な説明
- 判明している影響を受ける製品およびバージョン
- CWE識別子など、脆弱性の根本原因
- 顧客が自社インフラへのリスクを評価するための情報(例:CVSS)
- 悪用状況および侵害の兆候
- 修復策
- 低減策
- CVE ID
- (研究者が許諾した場合)研究者への謝辞

脆弱性の詳細を公開する

脆弱性の低減策とコミュニケーション内容を策定した後、研究者または仲介機関と共同で一般公開のタイムラインを決定すること。一般公開には、CVEレコードの発行のほか、顧客への通知、ブログ投稿、ソーシャルメディアといったその他の公表も含まれる。このタイムラインは多くの場合、セキュリティ研究者とサプライヤー双方の合意により決定されるが、特定の要件を策定する規制当局など、他の主体が関与する場合もある。例えば、策定機関は、脆弱性と低減策に関する認知度向上のため、各機関のウェブサイトでアドバイザリをさらに広めることが多い。

CVDプログラムのレビューと更新

以下の推奨ステップに従い、CVDプログラムを定期的にレビュー・更新すること。

- CVDプログラムをレビューし、過去の実績に基づいて調整するための、継続的改善プロセスとその実施頻度を確立する。
  - プログラムの有効性を評価しプロセスを改善するため、机上演習を活用する。
  - 外部からの報告件数とその特性(質や完全性など)を評価する。
- プログラムの改善方法について研究者からフィードバックを募り、その回答に共通する傾向を探る。
  - 研究者へのフィードバック提供を検討する。
- 脆弱性研究や報告を促進するため、公的な謝辞やバグバウンティの提供を検討する。
  - バグバウンティプログラムを社内で運用するか、外部サービス提供事業者に委託する。[14]

[14] NIST用語集は、バグバウンティを「セキュリティの悪用や脆弱性を許すおそれのあるソフトウェアの誤り、欠陥、不具合(『バグ』)を報告した個人に対して報酬を支払う仕組み」と定義している。

- 開発チームの特定における困難さや対応の迅速さも含め、自組織の社内対応時間を評価する。
  - 外部からの報告が開発チームや経営幹部の即時対応を必要とする場合に、CVDプログラムが定められたエスカレーション経路と整合し、対応づけられていることを確認する。
- プログラムの定量的・定性的分析および改善点を含む、主要な調査結果やトレンドを経営陣へ報告する実施頻度を確立する。

報告のトリアージ、脆弱性の修復、CVE IDの付与に関するプロセスを定義することは、CVDプログラムに不可欠な要素である。顧客のリスクを最小限に抑え、セキュリティ研究者との協調的な連携を確実にするため、上記のベストプラクティスを遵守すること。

CVDプログラムを代替・補完するための仲介機関の活用

サプライヤーのニーズや担当者のスキルセットに応じて、(CISAや各国のコンピュータセキュリティインシデント対応チームなどのサードパーティのコーディネーターといった)仲介機関を活用することで、CVDプログラムを効果的に代替または補完することができる。仲介機関は、コミュニケーションを効率化し、潜在的な脆弱性へ迅速に対応することで、研究者にとっての主要な窓口として機能することができる。また、脆弱性の評価、自らのCNAとしての範囲に応じたCVE IDの付与、責任ある開示の確保も行うことができる。CISAなどのサードパーティのコーディネーターは、複雑な多者間案件の調整に特有の強みを持つ。[15] CISAは、産業用制御システム、モノのインターネット(IoT)機器、医療機器、ITシステムに影響するものを含め、ソフトウェアおよびハードウェアにおけるサイバーセキュリティ上の脆弱性の修復と一般公開の調整を行っている。

CISAのCVDプログラムの一環として、CISAの脆弱性開示プラットフォームは、複数の関係者間での安全かつ体系的な連携・調整を可能にしている。これにより、(サプライヤー、ソフトウェア製造事業者、メンテナー、ベンダー、サービス提供事業者、脆弱性報告者を含む)すべての関係者を支援し、脆弱性および実行可能な修復策の一般への同時開示を、適時かつ協調的な形で行うことができる。詳細はCISAの「協調的脆弱性開示プログラム」を参照のこと。

> **注:** 策定機関はサードパーティのコーディネーターおよび外部でホストされるバグバウンティプログラムの活用を推奨する一方で、サプライヤーに対し、NDAなどの仕組みを通じてCVDを妨げないことなど、本文書に示すベストプラクティスに沿ったものであるかを確認するため、コーディネーターおよびプログラムのポリシーを注意深く確認することも推奨する。

結論

本ガイドで示すベストプラクティスに沿った強固なCVDプログラムを策定・維持することは、顧客のセキュリティと信頼の保護に取り組むすべてのサプライヤーにとって不可欠である。

[15] FIRSTの「Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure」では、複数の関係者が関与する脆弱性調整に関する詳細情報や事例が示されている。

TLP:CLEAR

(社内で運用する場合でも仲介機関を通じて運用する場合でも)体系化されたCVDプログラムは、セキュリティ研究者との連携における明確な枠組みを構築し、連携を促進するとともに、脆弱性の特定と効果的な対処を確実にする。これにより、サプライヤーはリスクをより適切に評価し、製品のセキュリティを向上させるための十分な情報に基づいた意思決定を行うことができるようになる。

CVDプログラムを策定しないことは、顧客のセキュリティを危険にさらし、セキュリティコミュニティ内での信頼を損なうおそれがある。CVDプログラムを通じてセキュリティ研究者と透明性をもって協力しながら脆弱性の修復に取り組むことにより、サプライヤーは建設的な関係を構築し、脆弱性管理プロセスを改善し、製品セキュリティを強化し、顧客保護への取り組みを示すことができる。

連絡先情報

脆弱性を報告するには:

- **米国の組織**は、CISA(cvd@cisa.dhs.gov)まで連絡すること。
- **日本の組織**は、JPCERT/CC(vuls@jpcert.or.jp)まで連絡すること。
- **オランダの組織**は、NCSC-NL の CVD 報告フォームを利用して連絡すること。
- **英国の組織**は、「Report a Cyber Incident」サービスを利用してインシデントまたは悪意ある活動を報告し、詳細な助言についてはNCSCのウェブサイトを参照すること。

参考資料

- CERT® 協調的脆弱性開示ガイド:「公表への備え」
- FIRST:「Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure」
- NCSC-UK:「Vulnerability Disclosure Toolkit」
- NCSC-UK:「『許される』脆弱性と『許されない』脆弱性を評価する手法」

免責事項

本レポートに記載された情報は、情報提供のみを目的として「現状のまま」提供されるものである。CISAおよび策定機関は、本文書内でリンクされている事業者、製品、サービスを含め、いかなる商用事業者、製品、企業、サービスについても推奨するものではない。特定の商用事業者、製品、プロセス、またはサービスへの言及は、サービスマーク、商標、製造事業者名などによるものであっても、CISAおよび策定機関による推奨や支持を意味するものではない。

謝辞

本ガイダンスの作成には、CERT@VDE、CrowdStrike、Dragos、Mandiant、Palo Alto Networksが協力した。

版歴

2026年7月15日: 初版。

TLP:CLEAR

参考文献

CERT® 協調的脆弱性開示ガイド。「公表への備え」。カーネギーメロン大学 コンピュータ緊急対応チーム。2025年12月10日アクセス。

欧州連合。「デジタル要素を含む製品に関する水平的サイバーセキュリティ要件、および規則(EU)No 168/2013、規則(EU)No 2019/1020、指令(EU)2020/1828を改正する2024年10月23日付欧州議会および理事会規則(EU)2024/2847(サイバーレジリエンス法)」。欧州連合官報。2024年10月23日。

FIRST。「Common Vulnerability Scoring System Version 4.0: Specification Document」。最終更新2024年6月18日。

FIRST。「Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure」。2025年12月10日アクセス。

Foudfil, Edwin, および Yakov Shafranovich。「RFC 9116: A File Format to Aid in Security Vulnerability Disclosure」。インターネット技術タスクフォース(IETF)。2022年4月。

国際標準化機構(ISO)/国際電気標準会議(IEC)。「29147:2018:情報技術 — セキュリティ技術 — 脆弱性開示」。ISO。第2版。2018年10月。

National Cyber Security Centre(NCSC)。「A Method to Assess Forgivable vs Unforgivable Vulnerabilities」。2025年1月28日。

TLP:CLEAR