サイバーセキュリティレポート

2025.04

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部　OSINT モニタリングチーム

目次

【1 ページサマリー】

当レポートでは 2025 年 4 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『セキュリティ・クリアランス制度について』

- 経済安全保障分野における「セキュリティ・クリアランス」制度を導入した法律「重要経済安保情報保護活用法」が、2025 年 5 月 16 日から施行される。
- セキュリティ・クリアランス制度は、政府が保有する安全保障上重要な情報へのアクセス権を、政府が信頼性の観点から認定した者に対してのみ付与するというものである。
- 民間事業者にとってセキュリティ・クリアランス制度は、重要インフラ等の事業への参加機会の維持・拡大や、自社の信頼性の向上によるビジネス機会の拡大といった面から、相応の対応を取る価値があるものと考えられる。

第 2 章『Oracle Cloud における認証情報の漏洩』

- ハッカーフォーラム上で「rose87168」と名乗るハッカーが、Oracle 社が提供するクラウドサービス「Oracle Cloud」を侵害して機密データを窃取したと主張し、その機密データを販売する旨の投稿を行った。
- Oracle 社は当初侵害を否定する声明を発表したが、最終的には「旧式の環境」が侵害されたと認めることとなった。
- サービスの問題に関してサービス提供者から公式見解が発表されない場合に備え、自社の判断でリスクを軽減できる体制を整えることを推奨する。

第 3 章『CVE 脆弱性情報管理に停止の危機』

- 2025 年 4 月 15 日、脆弱性情報管理に用いられ世界的なサイバーセキュリティのエコシステムの基礎になっている CVE が、継続困難の危機に立たされていることが突如明らかになった。
- これまで運営資金の提供を行ってきた米国政府の打ち切り通告によるもので、新規の発番やデータベース閲覧が不能になる等により、CVE 脆弱性情報管理に依存した世界中のセキュリティ対策全般に、大きな影響が出る可能性があった。
- 財団の設立、そして米国政府の資金提供の再開が決まり、CVE 発番等の停止はぎりぎりで回避された。

1. セキュリティ・クリアランス制度について

1.1. 概要

経済安全保障分野における「セキュリティ・クリアランス」制度を導入した法律「重要経済安保情報保護活用法」が、2025年５月 16 日から施行される[1]。セキュリティ・クリアランス制度は、政府が保有する安全保障上重要な情報へのアクセス権を、政府が信頼性の観点から認定した者に対してのみ付与するというものである[2]。これは、国家における情報保全措置のひとつで、情報指定、情報の厳格な管理・提供ルール、罰則という３つの骨格で構成されている[3]。

1.2. セキュリティ・クリアランス制度の目的

セキュリティ・クリアランス制度とは、国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として指定された情報にアクセスする必要がある者（政府職員及び必要に応じ民間事業者等の従業者）に対して政府による調査を実施し、当該者の信頼性を確認した上でアクセスを認める制度である[4]。今回施行される日本の「重要経済安保情報保護法」は、そのセキュリティ・クリアランスの新制度を含んでいる。

政府が保有する経済安全保障上重要な情報を「重要経済安保情報」とし、そのアクセスを信頼性が確認できた者に限定する事を定めている。情報漏洩の際の国の安全保障における支障がより大きい、重要なインフラや物資のサプライチェーンに関する情報が対象となっている。

従来、民間事業者を含めた政府の情報にアクセスできる者の、政府による選定については、法整備等が不十分で、円滑な経済安全保障分野の情報共有のためには、セキュリティ・クリアランス制度の確立が課題となっていた[5, 6]。

---

[1] 出典：内閣府『重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）』
https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html

[2] 出典：内閣官房『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議　参考資料（令和６年１月 17 日）』
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai10/sankou.pdf

[3] 出典：内閣官房『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議　参考資料（令和６年１月 17 日）』
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai10/sankou.pdf

[4] 出典：内閣官房『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議　最終とりまとめ』
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/torimatome.pdf

[5] 出典：内閣官房『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議　最終とりまとめ』
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/torimatome.pdf

[6] 出典：内閣府『重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）』
https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/hogokatsuyou.html

1.3. セキュリティ・クリアランス制度の基本的な骨格

「重要経済安保情報保護活用法」におけるセキュリティ・クリアランス制度は、基本的に下図の通り 3 つの骨格で構成されている。

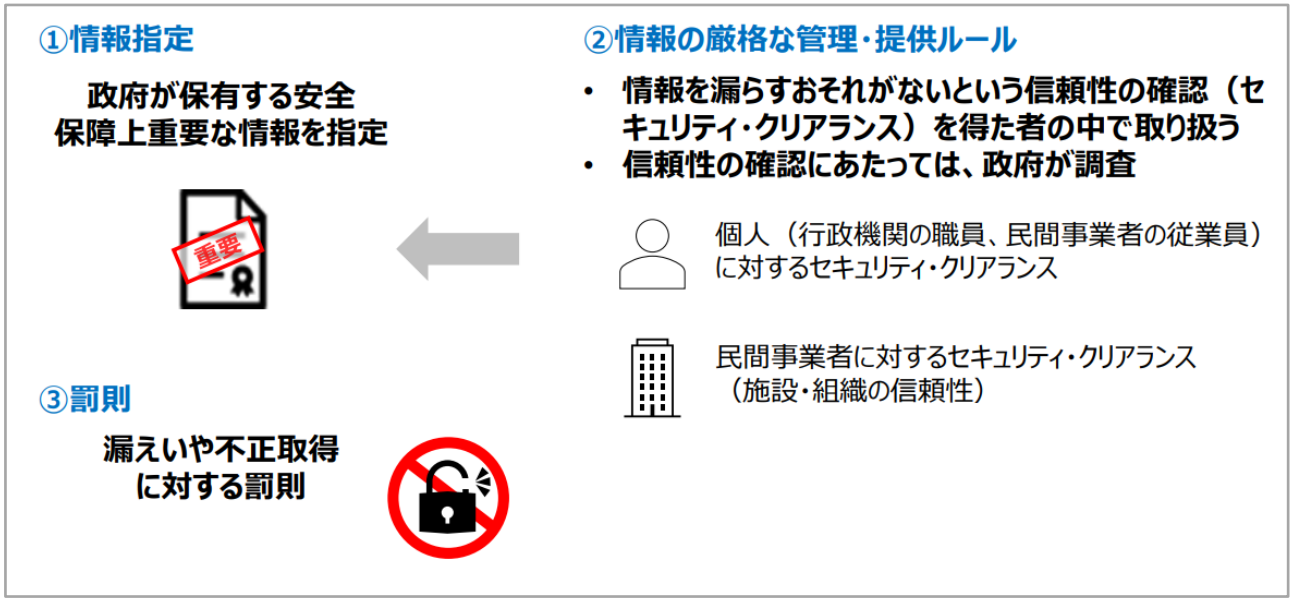


図 1 セキュリティ・クリアランス制度の概要(3 つの骨格：内閣官房の資料より)[7]

【① 情報指定（重要経済安保情報の指定）】

漏洩した場合に国の安全保障に支障をきたすおそれがある国家保有の情報を「重要経済安保情報」として指定する。指定の有効期限は 5 年以内で、延長しても原則 30 年を超えることはできない[8]。重要経済安保情報の候補には、サイバー関連情報や調査・分析・研究開発関連情報、国際協力関連情報等が挙げられている[9]。

【② 情報の厳格な管理・提供ルール（重要経済安保情報の取扱者の認定）】[10, 11]

民間事業者が重要経済安保情報の提供を受けるためには、情報漏洩の恐れがないことを行政機関から認定された上で、同機関と契約を締結する必要がある。

---

[7] 出典：内閣官房『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議　参考資料（令和 6 年 1 月 17 日）』 https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai10/sankou.pdf

[8] 出典：内閣府『重要経済安保情報の保護及び活用に関する法律の概要』 https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/gaiyo.pdf

[9] 出典：内閣官房『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議　参考資料（令和 6 年 1 月 17 日）』 https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai10/sankou.pdf

[10] 出典：内閣官房『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議　参考資料（令和 6 年 1 月 17 日）』 https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai10/sankou.pdf

[11] 出典：内閣府『重要経済安保情報の保護及び活用に関する法律概要』 https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/gaiyo_syousai.pdf

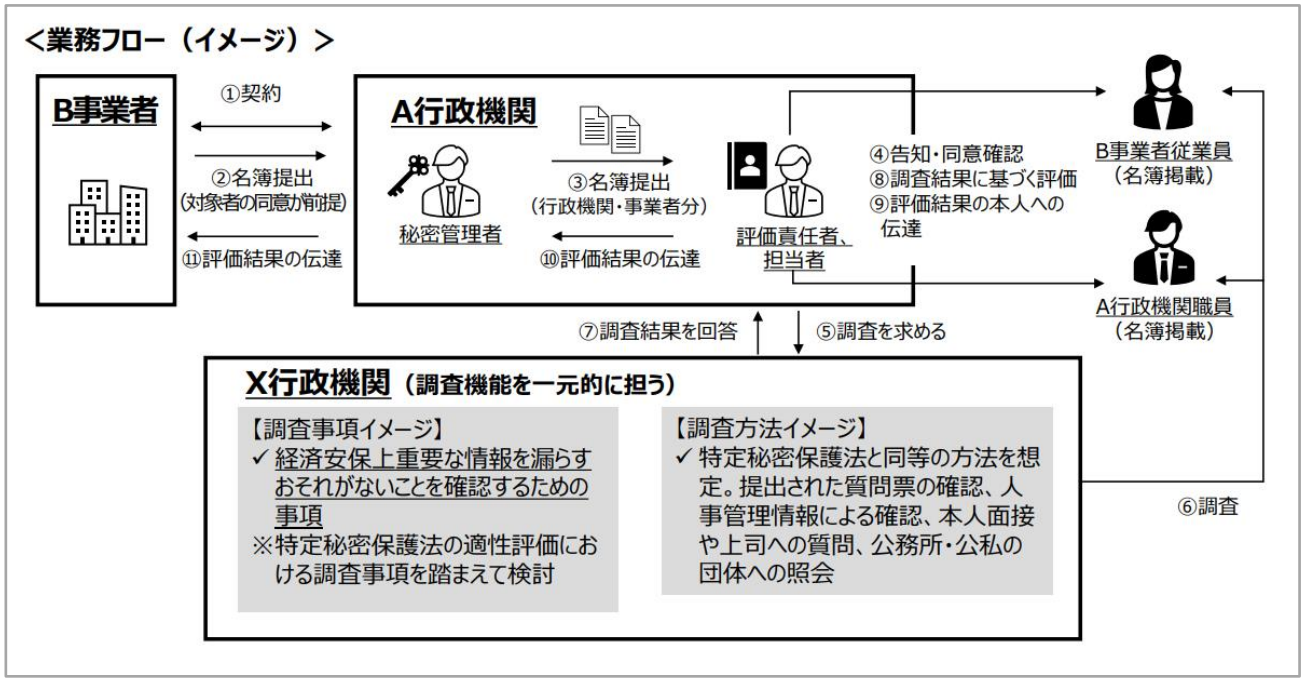


図 2 重要経済安保情報を取り扱うことができる個人や民間事業者の確認フロー[12]

国の安全保障の確保に貢献し、重要経済安保情報の保護のために必要な施設設備を設置しているなど、一定の基準を満たしていると行政に認められた事業者は、契約に基づき「適合事業者」として当該機密情報を扱えるようになる。ただし、この適合事業者に所属する従業員で、重要経済安保情報を取り扱うことができるセキュリティ・クリアランスの資格者となるためには、「適性評価」で認定を受ける必要がある。適性評価は、当該情報の漏洩を起こす恐れがない人物であることを確認するためのもので、本人の同意の上、以下の 7 項目が調査される。これらは評価対象者によって記入・提出された質問票や関係者への質問、面談、公的機関への照合等で判断される。

- 家族や配偶者、その他同居人の氏名や住所、国籍等を含む情報
- 犯罪や懲戒の経歴
- 情報の取り扱いに関する違反行為
- 薬物乱用等に関する情報
- 精神疾患に関する情報
- 飲酒の節度に関する情報
- 信用状態や経済的状況に関する情報

図 3 適性評価における調査の内容[13]

適性評価の有効期限は 10 年であるが、期限内でも懸念事項が生じた場合は、再度適性評価を受けることを求められる場合がある。

[12] 出典：内閣官房『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議　参考資料（令和６年１月 17 日）』 https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai10/sankou.pdf

[13] 出典：内閣府『重要経済安保情報の保護及び活用に関する法律概要』 https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/gaiyo_syousai.pdf

【③ 罰則】[14]

セキュリティ・クリアランスの資格を得た事業者およびその従業員には、機密情報を漏らしてはいけないという義務が生じる。そのような者が業務により知り得た重要経済安保情報を漏洩させた場合、主な罰則として、5 年以下の拘禁刑、もしくは 500 万円以下の罰金に処され、これらを併科される可能性もある。これは、重要経済安保情報の取扱いの業務から離れた後も同様で、未遂犯や過失も罰則の対象に該当する。また、両罰規定により事業者・従業員の双方について、罰則が適用される。

1.4. 民間事業者に対するセキュリティ・クリアランス資格

重要経済安保情報保護活用法が定めるセキュリティ・クリアランス制度は、国家の安全保障のために設けられたものであるが、民間事業者がこの制度を取り入れることでサイバーセキュリティの強化が期待できる。また、セキュリティ・クリアランス資格を保有することで事業者としての信頼性が向上し、取引先や顧客からの評価が高まる他、政府や国際機関が主催する会議や入札に参加できるようになり、ビジネスの機会を拡大することも可能となる。

なお、重要経済安保情報の提供を受ける者として、重要なインフラやサプライチェーンに関連する事業者等が想定される。重要経済安保情報保護活用法の施行により、情報管理者の選定や施設の保全体制の確認等、企業側での負担やコストが増加し、これらの事業者の業務に影響が出る可能性がある。なお、保護の対象となる重要経済安保情報は政府が保有するものであり、民間業者が保有する情報に様々な規制等が発生するわけではない[15, 16]。

1.5. 外国政府との安全保障上重要な情報のやりとり

安全保障に関する機密情報を外国政府と共有する場合も、その保全性を確保することが求められる。米国、英国、カナダ、オーストラリア、ニュージーランドの 5 カ国による機密情報共有の枠組みであるファイブ・アイズでも既にセキュリティ・クリアランス制度を導入しており、日本が国際競争力を高め、これらの国々と安全保障に関する情報共有を進めるためにも日本でのセキュリティ・クリアランスの運用は重要である[17]。

1.6. まとめ

民間事業者にとってセキュリティ・クリアランス制度は、重要インフラ等の事業への参加機会の維持・拡大や、自社の信頼性の向上によるビジネス機会の拡大といった面から、相応の対応を取る価値があるものと考えられる。その影響力は、国際社会

---

[14] 出典：内閣府『重要経済安保情報の保護及び活用に関する法律概要』
https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/gaiyo_syousai.pdf

[15] 出典：KPMG ジャパン『セキュリティ・クリアランス制度―新たな経済安保政策による機会とリスク』
https://kpmg.com/jp/ja/home/insights/2024/04/security-clearance.html

[16] 出典：内閣官房『経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議　最終とりまとめ』
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/pdf/torimatome.pdf

[17] 出典：トレンドマイクロ（JP）『セキュリティ・クリアランスとは？なぜ日本で必要性が高まっているのか？』
https://www.trendmicro.com/ja_jp/jp-security/23/d/securitytrend-20230410-01.html

においても同様と言え、この制度をめぐる国内外の動向を注視していくことが重要である。一方で、セキュリティ・クリアランスの導入は、組織や従業員に負荷となることもあり得る為、業務に過度な支障をきたさないような対応も考えておくべきである。

2. Oracle Cloud における認証情報の漏洩

2.1. 概要

ハッカーフォーラム上で「rose87168」と名乗るハッカーが、Oracle 社が提供するクラウドサービス「Oracle Cloud」から窃取したとする機密データを販売するという投稿を行った。Oracle 社は当初侵害を否定する声明を発表したが、最終的には「旧式の環境」が侵害されたと認めることとなった。本稿では、一連の騒動について振り返る。

2.2. 「Oracle Cloud」とは

「Oracle Cloud」は、Oracle 社が提供するパブリッククラウドサービスで、Oracle 社が管理するクラウド上でサーバー、データベース、ストレージなどを利用することができる。

パブリッククラウドの世界市場シェアでは、Oracle Cloud のシェアは 3%となっており、先行する三大クラウド Amazon Web Service (AWS)、Microsoft Azure、Google Cloud Platform (GCP)に水をあけられている[18]。一方、これまで Oracle 社がオンプレミス向けに提供してきたデータベースなどの製品をクラウドに移行する場合、Oracle Cloud ではスムーズな連携ができるため、有力な移行先となっている[19]。

また、日本政府が利用する共通クラウド基盤「ガバメントクラウド」のサービス提供事業者として選定されており[20]、地方公共団体での利用が進んでいる[21]。

2.3. 「rose87168」による Oracle Cloud 侵害の主張

2025 年 3 月 21 日、ハッカーフォーラム上で「rose87168」と名乗るハッカーが、「Oracle Cloud」を侵害して機密データを窃取したと主張し、その機密データを販売する旨の投稿を行った。機密データは約 600 万件にのぼり、暗号化されたシングルサインオンのパスワードなどが含まれていると、rose87168 は述べている[22]。

同投稿では、侵害の成功を裏付ける証拠として、影響を受けたとされる組織のドメインが約 14 万件記載されたリストなどが公開された。

---

[18] 出典：emma『Cloud Market Share Trends to Watch in 2025』
https://www.emma.ms/blog/cloud-market-share-trends

[19] 出典：Oracle『Migrate Oracle On-Premises Applications to Oracle Cloud Infrastructure』
https://www.oracle.com/cloud/migrate-applications-to-oracle-cloud/

[20] 出典：Oracle 日本『日本オラクル、ガバメント・クラウドのサービス提供事業者に選定』
https://www.oracle.com/jp/news/announcement/oracle-japan-selected-as-government-cloud-service-provider-2022-10-06/

[21] 出典：ITmedia NEWS『AWS 障害に Oracle 情報漏えい疑惑――リスク露呈したガバメントクラウド、デジタル庁の受け止めは』
https://www.itmedia.co.jp/news/articles/2505/08/news049.html

[22] 出典：BleepingComputer『Oracle customers confirm data stolen in alleged cloud breach is valid』
https://www.bleepingcomputer.com/news/security/oracle-customers-confirm-data-stolen-in-alleged-cloud-breach-is-valid/

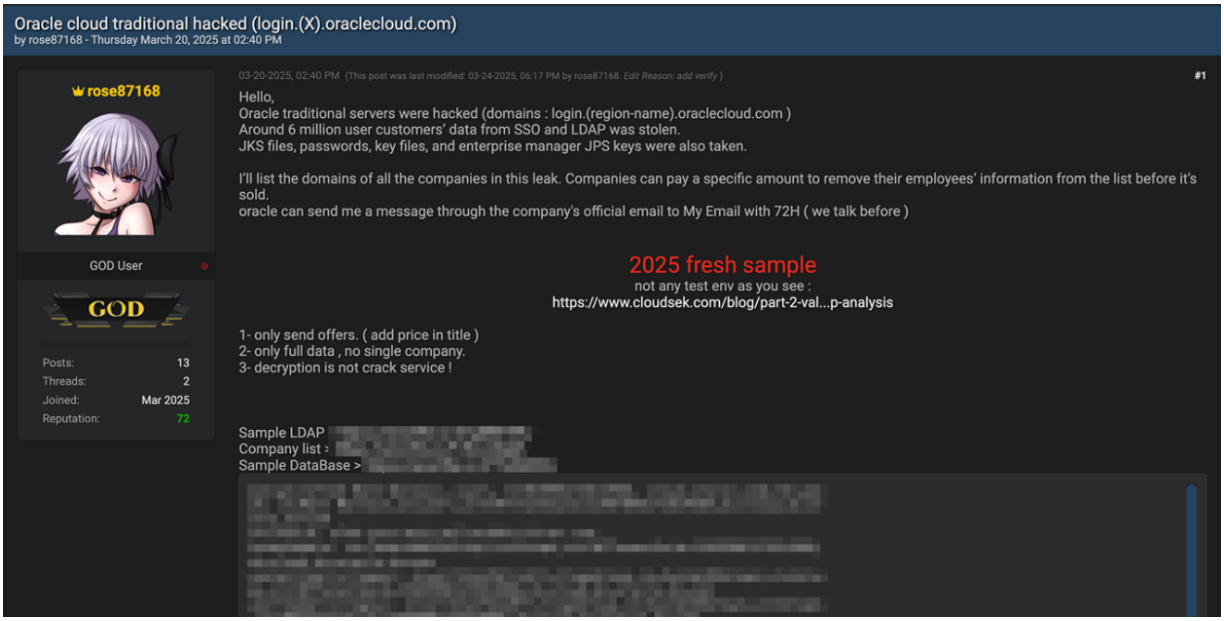


図 4 rose87168 のハッカーフォーラムでの投稿

さらなる裏付けとして、rose87168 は、自身のメールアドレスが表示されるよう、Oracle が管理するサーバーを改ざんし、当該サーバーの URL をメディアに共有した[23]。このハッキング実行の証拠により、自らの能力を誇示し、窃取したとされる機密データの正当性を高める狙いがあったとみられる。

図 5 rose87168 が改ざんしたと主張するサーバーのアーカイブ

ハッキングフォーラムへの最初の投稿から数日後、rose87168 は非公開の機密情報の一部データを複数のメディアに共有した。各メディアはデータに記載されていた複数の企業に対して取材を行い、共有されたデータが本物であることを確認した。

2.4. Oracle 社の対応

一部の脅威インテリジェンスベンダーやメディアが機密データの正当性を主張する一方で、報道直後、Oracle 社は Oracle Cloud への侵害を否定する声明を発表した[24]。

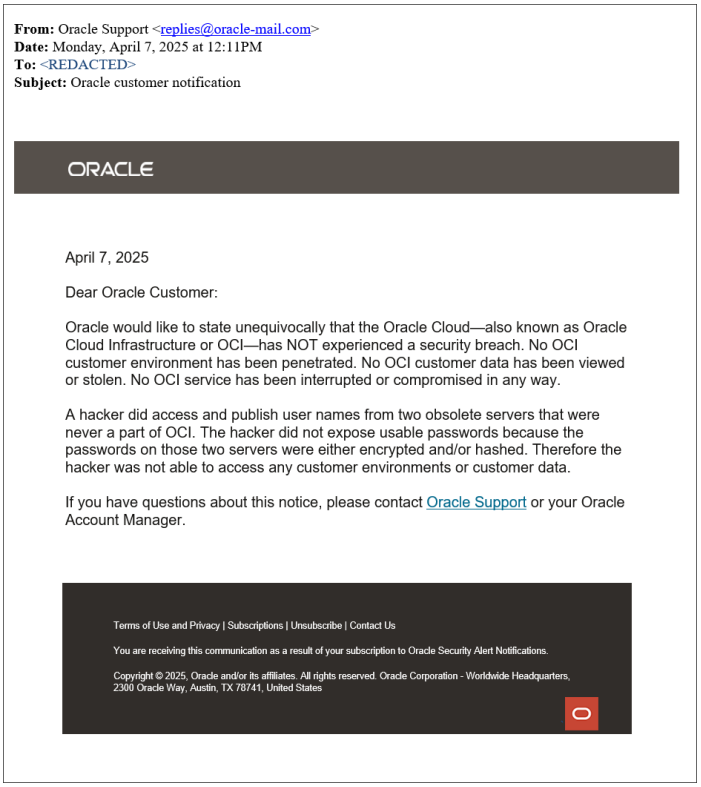
しかし、4 月 2 日になって、Oracle 社は、ハッカーが「2 つの旧式のサーバー」から認証に関わる情報を盗んだことを顧客に

[23] 出典：CloudSEK『The Biggest Supply Chain Hack Of 2025: 6M Records Exfiltrated from Oracle Cloud affecting over 140k Tenants』
https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants

[24] 出典：The Register『Oracle Cloud says it's not true someone broke into its login servers and stole data』
https://www.theregister.com/2025/03/23/oracle_cloud_customers_keys_credentials/

対してメールで通知した[25]。さらに FBI とセキュリティベンダーの CrowdStrike が侵害の調査を実施していることが明らかになった。

この顧客への通知で、侵害を受けたのは「Oracle Cloud Classic」という旧式の環境のサーバーであり、「Oracle Cloud」は侵害されていないと Oracle 社が説明したことに関して、一部のメディアは「言葉遊び」と批判している[26]。



From: Oracle Support <replies@oracle-mail.com>
Date: Monday, April 7, 2025 at 12:11PM
To: <REDACTED>
Subject: Oracle customer notification

ORACLE

April 7, 2025

Dear Oracle Customer:

Oracle would like to state unequivocally that the Oracle Cloud—also known as Oracle Cloud Infrastructure or OCI—has NOT experienced a security breach. No OCI customer environment has been penetrated. No OCI customer data has been viewed or stolen. No OCI service has been interrupted or compromised in any way.

A hacker did access and publish user names from two obsolete servers that were never a part of OCI. The hacker did not expose usable passwords because the passwords on those two servers were either encrypted and/or hashed. Therefore the hacker was not able to access any customer environments or customer data.

If you have questions about this notice, please contact Oracle Support or your Oracle Account Manager.

Terms of Use and Privacy | Subscriptions | Unsubscribe | Contact Us

You are receiving this communication as a result of your subscription to Oracle Security Alert Notifications.

Copyright © 2025, Oracle and/or its affiliates. All rights reserved. Oracle Corporation - Worldwide Headquarters, 2300 Oracle Way, Austin, TX 78741, United States

図 6 Oracle 社による顧客への通知メール

4 月 16 日、米サイバーセキュリティ・インフラセキュリティ庁(CISA)は、同侵害による認証情報の漏えいが、組織・個人のユーザーに対してリスクをもたらす恐れがあるとして、ガイダンスを発表した[27]。ガイダンスでは潜在的な脅威を軽減するために、パスワードのリセット、多要素認証の導入などの実施を推奨している。

2.5. まとめ

今回の一連の騒動では、Oracle 社の対応を巡り、透明性の欠如と責任回避の姿勢に批判が集中することとなり、ユーザー企業は自社が影響を受けるのか自ら調査し、対応の要否を判断する必要があった。

広く利用されているサービスの問題に関して、必ずしもサービス提供者から公式見解が発表されるとは限らない。その場合、

[25] 出典：Reuters『Oracle tells clients of second recent hack, log-in data stolen, Bloomberg News reports』
https://www.reuters.com/technology/cybersecurity/oracle-tells-clients-second-recent-hack-log-in-data-stolen-bloomberg-news-2025-04-02/

[26] 出典：BleepingComputer『Oracle says "obsolete servers" hacked, denies cloud breach』
https://www.bleepingcomputer.com/news/security/oracle-says-obsolete-servers-hacked-denies-cloud-breach/

[27] 出典：CISA『CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise』
https://www.cisa.gov/news-events/alerts/2025/04/16/cisa-releases-guidance-credential-risks-associated-potential-legacy-oracle-cloud-compromise

問題となったサービスを自社内で利用しているか調査し、利用していることを確認でき次第、自社の判断でリスクの軽減を図る必要がある。平素からガバナンスを強化して、シャドーIT を抑制・検知し、自社で利用しているサービスを把握していることが望ましい。また、高い可用性が求められるサービスに対しては代替手段を用意するなど、サイバーレジリエンスを高める備えをすることも推奨する。

3. CVE 脆弱性情報管理に停止の危機

3.1. 概要

脆弱性対応において、「Common Vulnerabilities and Exposures」（共通脆弱性識別子、以下、略称の CVE で表記）は重要な情報源である。

2025 年 4 月 15 日、これまで CVE 発番等をする運営組織を資金援助してきた米国政府機関が、トランプ大統領への政権移行に伴う予算削減を進める中で援助を打ち切ることが明らかになった。これにより翌 17 日以降、CVE の新規発番やデータベース公開等が停止の危機に直面し、国家だけではなく民間のセキュリティ対策全般に大きな影響が出る可能性があった。

この事態を受けて、直ちに独立した財団が設立された。また、米国政府機関の支援延長も決まったため、これでひとまず CVE の運営継続は確保された。

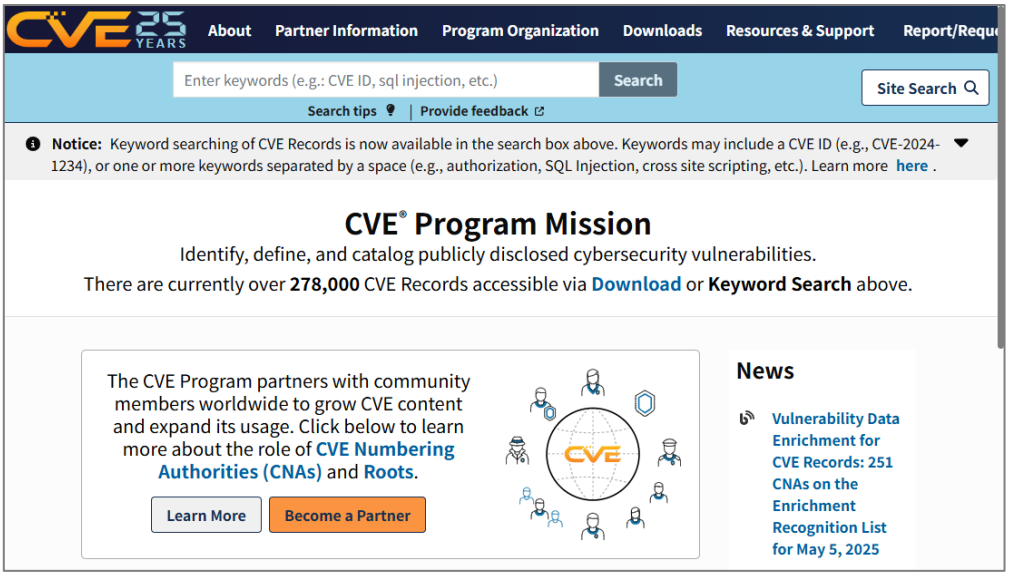


図 7 CVE の公式サイト（www.cve.org）[28]

3.2.「Common Vulnerabilities and Exposures (CVE)」とは [29]

CVE は、個別のソフトウェア製品中の脆弱性を対象とした識別子である。脆弱性に対し、「CVE-2025-xxxx」といった CVE 識別番号（CVE-ID）を付与することで、異なる組織が発行する脆弱性対策情報を相互に参照・関連付けることができるようになっている。公開された脆弱性を特定し、CVE 識別番号を付与してカタログ化する、国際的なコミュニティ主導の取り組みが CVE プログラムである[30]。

---

[28] 出典：CVE『CVE Common Vulnerabilities and Exposures』
https://www.cve.org/

[29] 出典：IPA『共通脆弱性識別子 CVE 概説』
https://www.ipa.go.jp/security/vuln/scap/cve.html

[30] 出典：CVE『CVE: Common Vulnerabilities and Exposures』
https://www.cve.org/ResourcesSupport/Glossary

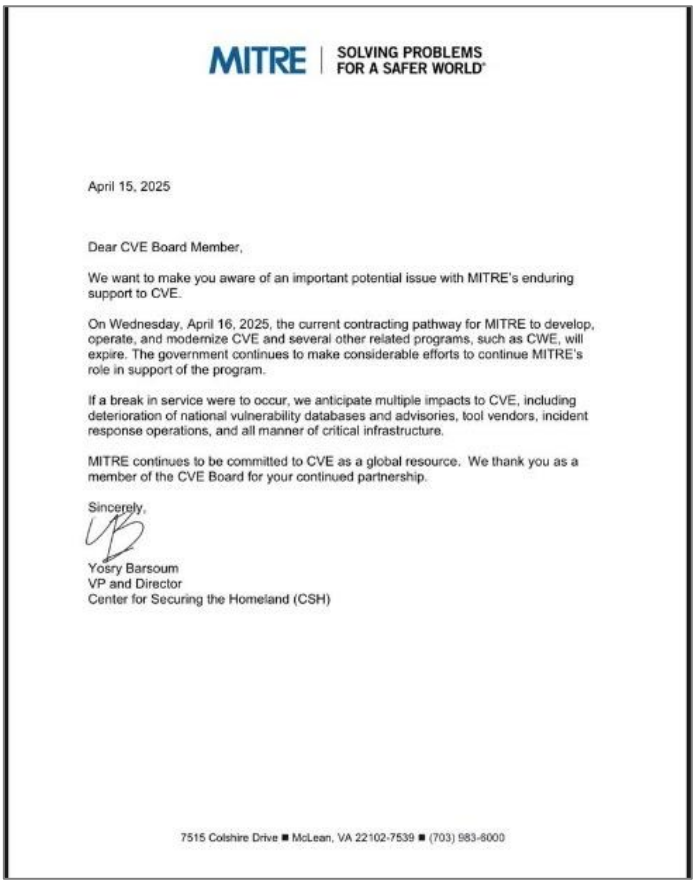
CVE プログラムは、非営利団体の MITRE 社が、米国政府機関である国土安全保障省（DHS）とサイバーセキュリティ・インフラセキュリティ庁(CISA)からの資金援助を受け運営している。CERT/CC、HP、IBM、OSVDB、Red Hat 等の主要な脆弱性情報サイトとの連携により、CVE プログラムは脆弱性情報を網羅している。

CVE の取り組みは、1999 年 1 月に開催された脆弱性情報管理のワークショップにおける、MITRE 社の提案から始まった。以来約 25 年間、世界的な脆弱性情報管理等のサイバーセキュリティ・エコシステムにおける基礎になっている。脆弱性検査や脆弱性情報提供等、多くのツールやサービスが CVE を利用している。

3.3. CVE プログラム閉鎖騒動

【米国政府、CVE プログラム支援を更新せず】

米国政府は MITRE 社に、CVE プログラムへの資金援助契約を、更新期限の 2025 年 4 月 16 日を迎えても延長しない旨、通知した。理由は述べられていないが、トランプ大統領への政権移行に伴う、政府予算削減のあおりを受けたものとみられている[31]。



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

April 15, 2025

Dear CVE Board Member,

We want to make you aware of an important potential issue with MITRE's enduring support to CVE.

On Wednesday, April 16, 2025, the current contracting pathway for MITRE to develop, operate, and modernize CVE and several other related programs, such as CWE, will expire. The government continues to make considerable efforts to continue MITRE's role in support of the program.

If a break in service were to occur, we anticipate multiple impacts to CVE, including deterioration of national vulnerability databases and advisories, tool vendors, incident response operations, and all manner of critical infrastructure.

MITRE continues to be committed to CVE as a global resource. We thank you as a member of the CVE Board for your continued partnership.

Sincerely,

Yosry Barsoum
VP and Director
Center for Securing the Homeland (CSH)

7515 Colshire Drive ■ McLean, VA 22102-7539 ■ (703) 983-6000

図 8 MITRE 社から CVE 理事会への書簡 [32]

[31] 出典：Forbes『CVE Program Funding Reinstated—What It Means And What To Do Next』
https://www.forbes.com/sites/kateoflahertyuk/2025/04/16/cve-program-funding-cut-what-it-means-and-what-to-do-next/

[32] 出典：BlueSky『@tib3rius.bsky.social』
https://bsky.app/profile/tib3rius.bsky.social/post/3lmulrbygoe2g

これを受け MITRE 社は CVE プログラムの理事会のメンバーに宛て、運営が困難になったことを通告した（**図 8**）。この書簡が SNS で公開されて CVE プログラム継続の危機が明らかになると、新規の CVE 発番や CVE のデータベースが閲覧できなくなる等の影響が予想されたことから、多くのサイバーセキュリティの専門家やコミュニティのリーダーたちが不安を表明した[33]。一部のセキュリティ研究者らは壊滅的な損失に備えて 27 万 5,000 件の CVE の脆弱性情報全体をアーカイブする取り組みを、迅速に開始した[34]。

【CVE Foundation の設立】

支援打ち切りの報の直後、CVE 理事会メンバーを中心として、CVE プログラムの財政的な基盤となる「CVE Foundation」が設立された（**図 9**）[35]。

CVE 理事会ではもともと、米国政府に依存した CVE プログラムの在り方を、持続可能性と中立性の観点から問題視しており、その解決策として 1 年ほど前から財団設立を模索していた。CVE Foundation は、政府に依存せず独立した形で資金調達することを志向している。そして、サイバーセキュリティコミュニティと協力し、脆弱性情報の収集、管理、提供を継続すると発表している[36]。

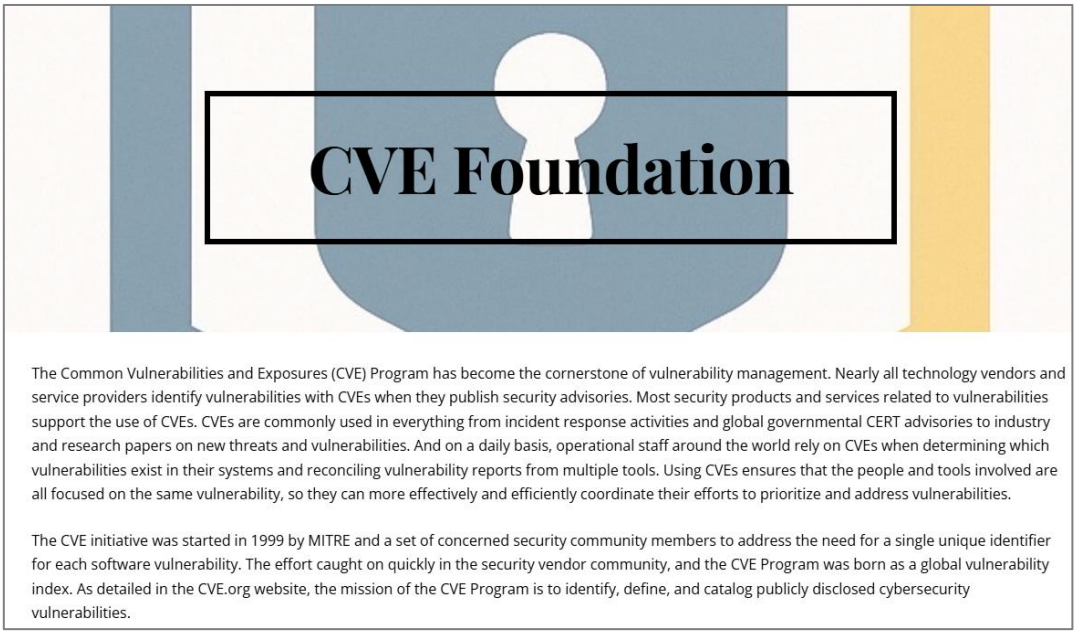


図 9 CVE Foundation 設立に伴い開設された、同財団の Web サイト [37]

[33] 出典：BleepingComputer『MITRE warns that funding for critical CVE program expires today』 https://www.bleepingcomputer.com/news/security/mitre-warns-that-funding-for-critical-cve-program-expires-today/

[34] 出典：Cybernews『Screw gov't funding, we're going nonprofit, CVE Board declares after database debacle』 https://cybernews.com/security/cve-database-foundation-established-nonprofit-funding-board/

[35] 出典：BleepingComputer『CISA extends funding to ensure 'no lapse in critical CVE services'』 https://www.bleepingcomputer.com/news/security/cisa-extends-funding-to-ensure-no-lapse-in-critical-cve-services/

[36] 出典：Cybernews『Screw gov't funding, we're going nonprofit, CVE Board declares after database debacle』 https://cybernews.com/security/cve-database-foundation-established-nonprofit-funding-board/

[37] 出典：CVE Foundation『CVE Foundation』 https://www.thecvefoundation.org/

【CISA、CVE プログラムの契約を延長】

CVE Foundation の設立直後の 4 月 16 日、CISA が MITRE への資金援助を延長すると発表した[38]。これにより契約が 11 か月延長され[39]、CVE プログラムの停止は免れた。CISA は「CVE プログラムはサイバーコミュニティにとって非常に重要であり、CISA の優先事項である」とメディア取材に対して述べ、サイバーセキュリティにおける CVE プログラムの意義を重視していることをアピールしている。

3.4. まとめ

CVE プログラムによる CVE の提供継続が決まり、世界的なサイバーセキュリティ・エコシステムの危機は回避された。事後の 4 月 25 日には CISA と CVE Foundation の会談が行われ、歩み寄りも見られる[40]。だが、11 か月後に CISA の契約は更新されるのか、CVE Foundation は今後も継続可能なのかまだ定かではなく、先行きの不透明さが不安視されている[41]。

これまで、脆弱性が明らかになるとすぐに CVE が発番される CVE プログラムの活動は、セキュリティ業界にとって有って当たり前のものとされてきた。だが、米国政府の政策変更により大きく揺らぎ、当たり前ではないことが明らかになった。欧州サイバーセキュリティ機関（ENISA）も欧州脆弱性データベース（EUVD）[42]を立ち上げているが、まだベータ版であること等、直ちに CVE の代替になるものではない。サイバーセキュリティ対策のエコシステムには、長年の慣習の中で米国政府に依存していることにより単一障害点が存在することを、再認識させられる出来事であった。

以上

[38] 出典：CISA『CISA Statement on CVE Program』
https://www.cisa.gov/news-events/news/cisa-statement-cve-program

[39] 出典：BleepingComputer『CISA extends funding to ensure 'no lapse in critical CVE services'』
https://www.bleepingcomputer.com/news/security/cisa-extends-funding-to-ensure-no-lapse-in-critical-cve-services/

[40] 出典：CVE Foundation『News』
https://www.thecvefoundation.org/news

[41] 出典：ZDNET Japan『米国で脆弱性情報の管理体制に混乱--新組織発足でも既存体制は当面維持』
https://japan.zdnet.com/article/35231923/

[42] 出典：ENISA『Vulnerability Database』
https://euvd.enisa.europa.eu/

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

プロフェッショナルサービス部　OSINT モニタリングチーム
メールアドレス：nsj-co-osint-monitoring@security.ntt