2026年版

THALES
CYBERSECURITY

データ脅威レポート

国別データシート
日本

cpl.thalesgroup.com

#2026DataThreatReport

はじめに

企業が取り組んでいるAIの成功は、組織独自のデータソースへの一貫性のある制御されたアクセスにますます左右されるようになり、データセキュリティが中心的な課題として浮上しています。**2026年タレス　データ脅威レポート**は、組織がイノベーションを推進しつつ、最も貴重な資産であるデータを保護するために取り組むべき複雑な課題について検証しています。

AIとエージェント型運用の拡大は、データ管理とセキュリティへの負荷を増大させています。これは、AI専用に新たなセキュリティ予算を割り当てている回答者の割合が前年比で50%増加したことにも表れています。組織は、AIの価値創出の源となるデータへの安全なアクセスを提供しようとする中で、データ品質とセキュリティの確保に苦戦しています。エージェント型アプリケーションがより大量のデータにアクセスするようになる中で、AIが新たな内部脅威とならないよう、データセキュリティと管理手法を強化する必要があります。

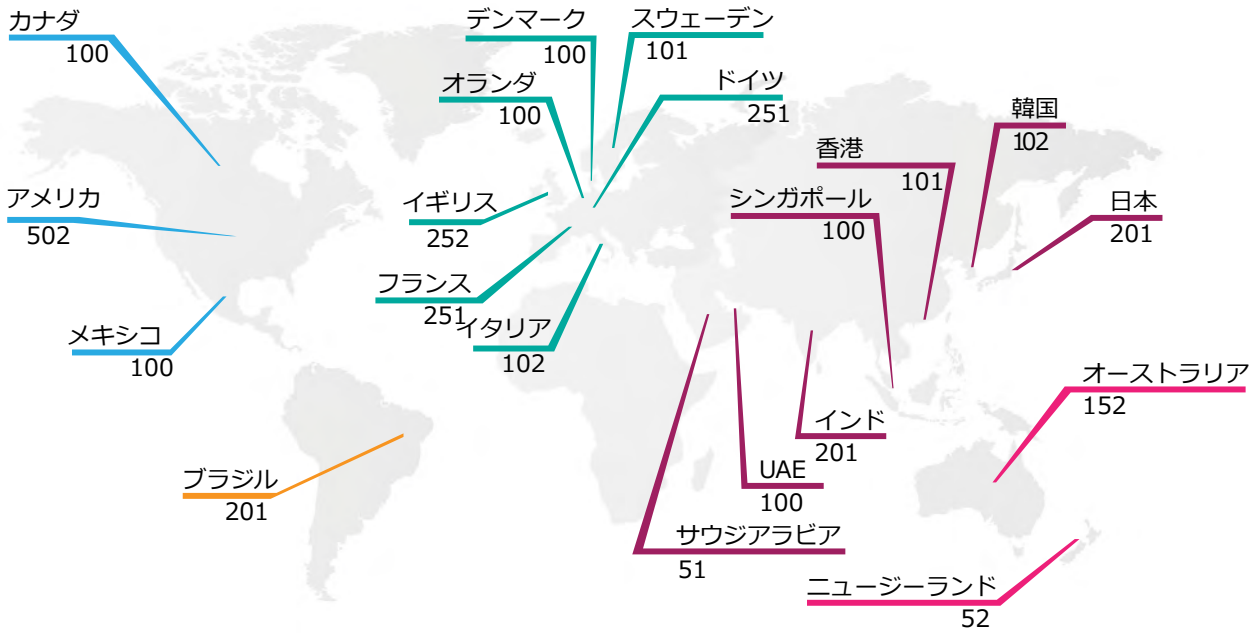
業務の加速を求められる一方で、セキュリティツールの乱立や、ますます複雑化するハイブリッドやマルチクラウドのITインフラによってセキュリティ運用が複雑化し、こうした取り組みは困難に直面しています。AIはチャットインターフェースやModel Context Protocol（MCP）サーバーといった新たな要素の統合を伴い、セキュリティチームはそれらの保護に苦戦しています。脅威環境も変化しており、攻撃者がAIを悪用し、量子コンピューティングのリスクがますます高まっています。さらに複雑なことに、AIエコシステムはセキュリティチームの足元で絶えず変化し続けています。

今年のデータ脅威レポートには前向きな傾向も見られるものの、組織の最も機密性の高いデータを保護するためには、さらに多くの取り組みが必要です。本レポートは、20カ国、3,100人以上の回答者から得られた知見をまとめたものです。多くの組織は完全なマルチクラウド運用モデルを採用し、データとアプリケーションが複数のクラウドプロバイダーに分散していますが、この現実を積極的に受け入れている組織ばかりではありません。

今年の調査結果を過去の結果と比較すると、いくつかの注目すべき懸念事項が浮かび上がっています。クラウド上の機密性の高い大量のデータが、依然として暗号化されていないまま残されています。クラウドベースのアプリケーションやクラウド管理インフラは、攻撃者にとって主要な標的であり続けています。クラウドにおけるセキュリティ運用の複雑さは、特に人員面での制約がある中で対応が困難です。名称が示すとおり、クラウドセキュリティにはクラウド運用とセキュリティアプリケーションの両分野における専門知識が求められますが、どちらの能力も不足しています。これに加えて、AIアプリケーション向けに、より大量のデータと計算能力を提供しなければならないというプレッシャーが高まっています。エージェント型運用の時代を迎え、セキュリティ担当者は、アクセス、認証、認可をこれまで以上の規模で対処する必要があります。

調査方法

本調査は、セキュリティおよびITマネジメントの専門家を対象に、各国の対象集団に実施したWeb調査による、3,120人の回答者のグローバル調査に基づいています。調査のスクリーニング基準として、一般的なトピックに関する知識レベルの基準に加え、年間収益が1億米ドル未満、また主要国で1億～2億5千万米ドルの組織に属している回答者を除外しました。この調査は観察研究として実施されたものであり、因果関係を主張するものではありません。



収益	回答者数
1億ドル～2.499億ドル	213
2.5億ドル～4.999億ドル	701
5億ドル～7.499億ドル	799
7.5億ドル～9.999億ドル	774
10億ドル～14.9億ドル	265
15億ドル～19.9億ドル	137
20億ドル以上	231
合計	3,120

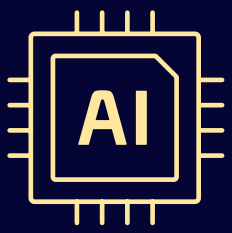
業種	回答者数	業種	回答者数
医療	263	旅行・ホスピタリティ	181
小売	255	eコマース	171
製造	251	自動車	166
金融サービス	237	教育	141
技術	222	バイオテクノロジー	124
エネルギー＆公益事業	213	防衛	115
政府	207	航空宇宙	80
運輸	189	電気通信	79
製薬	187	その他	28
合計			3,120

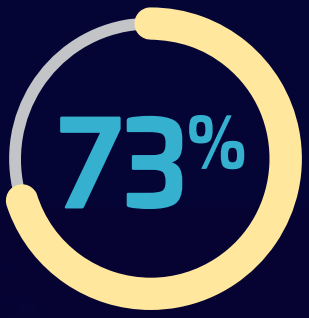
主な調査結果　-　日本

AIによってセキュリティの優先順位が変化

AIセキュリティへの支出は増加していない –

24% 組織がAIセキュリティ専用の予算を確保している（前年の25%から減少）。57%が既存のセキュリティ予算を使用してAIセキュリティに投資している。





AIエコシステムの変化の速さは、AIセキュリティの最大の懸念事項であり、68%が最大のAIリスクとして挙げている。

62%

自社のAIアプリケーションが攻撃対象になっていると回答しており、機密データが主要な標的となっている。

AIを悪用した攻撃が顕著な脅威として浮上 – 55%がディープフェイク攻撃を経験し

48%

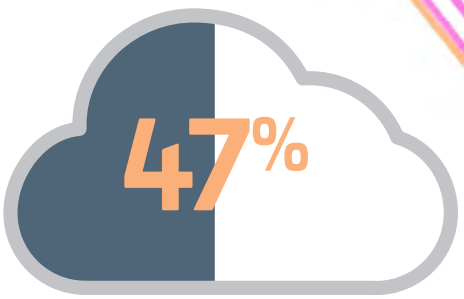
がAI生成の偽情報によって評判を傷つけられたと回答している。

AI生成の偽情性やディープフェイクが攻撃増加のだ2位と報告している。

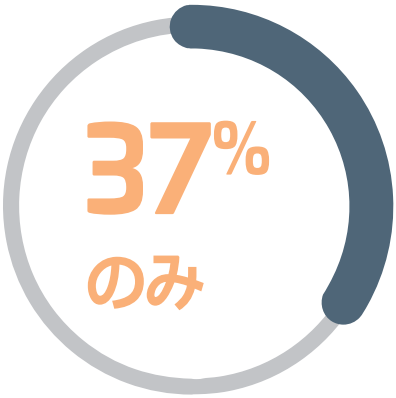
データ保護はAI時代に極めて重要

35%

最も緊急性の高いセキュリティ分野としてID・アクセス管理を挙げており、これは攻撃者による認証情報の悪用が進んでいるためである。



機密性の高いクラウドデータの約半数しか暗号化されていない。



自社データの保存場所を完全に把握している。

41%

アプリケーションセキュリティにおける最大の懸念としてシークレット管理を挙げている。

複雑さがデータセキュリティ態勢の可視性を阻害

セキュリティの複雑さがリスクを増大させている –

ツール数は多く、**73%**が5つ以上のデータ保護ツールを使用している。

41% 5つ以上の鍵管理システムを使用

42% データセキュリティツールの理解度に自信があると回答

30% データ侵害の主な原因としてヒューマンエラーを挙げているが、48%が最も懸念される脅威要因の上位3つに、国家主導の攻撃者を挙げている。

クラウドが主要な攻撃対象

クラウド資産が上位3つの攻撃対象を占める –

回答者の

45% クラウドストレージ、 **30%** クラウドアプリケーション、 **35%** クラウド管理インフラ

上位3つを攻撃対象として挙げている。

認証情報の窃取はクラウドインフラに対する主要な攻撃手法である –

66% 認証情報の窃取と不正取得されたシークレットの増加を確認している。

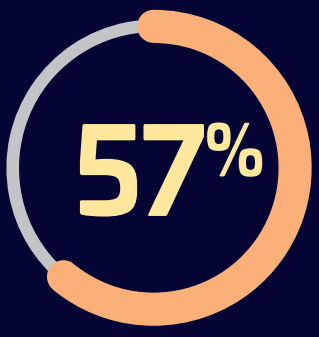
地政学的リスクの高まりがデータ主権を再形成

50% データ主権の目的を達成するための主要な焦点としてアプリケーションとデータアーキテクチャの再構築およびリファクタリングを推進している。

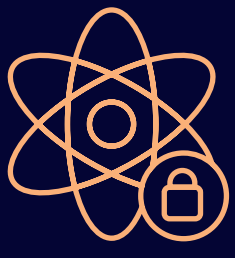
36% 暗号化や鍵管理といった暗号保護だけでデータ主権を達成できると考えている。

将来のリスクはすでに現実化

量子コンピューティングに関する懸念は、現在のデータの将来的な解読（HNDL）という現実的な脅威へと移行しており、



最も懸念されるセキュリティ脅威として挙げている。



組織は量子リスクの軽減に向けて動き始めている

51%

ポスト量子暗号（PQC）アルゴリズムのプロトタイピングと評価を行っている。

THALES

CYBERSECURITY

cpl.thalesgroup.com/ja/data-threat-report

お問い合わせ先

全てのオフィスの所在地と連絡先情報につきましては、
cpl.thalesgroup.com/ja/contact-us をご覧ください。