# セキュリティステートメント

最終更新日：2025年4月

本書は、[日付] 時点で更新されたセキュリティステートメントの日本語版です。
セキュリティステートメントの英語版と日本語版の内容に相違がある場合には、
英語版が優先して適用されます。

## 概要

当社は、高いセキュリティ意識をもって設立・運営されるセキュリティ企業です。お客様のプライバシーを尊重し、お客様のデータを保護するため最大限の努力を払っています。そして、お客様のデータを当社のデータと同じように扱うことを徹底しています。

お客様のデータを安全に保つことは、KnowBe4にとって最重要事項です。KnowBe4は最大限の努力を払い、ご提供いただくすべてのデータを安全に保持しています。徹底したセキュリティのもとでKnowBe4のシステムとお客様のデータを保持することは、当社の事業基盤そのものです。ご利用の前に、当社の利用規約およびプライバシーポリシーをご確認ください。

## コンプライアンス

KnowBe4プラットフォーム（KSAT + PhishER）は、2023年11月14日よりFedRAMPのModerate ATO（中程度運用認可）を保持しています。

FedRAMP™

**Moderate ATO**

KnowBe4プラットフォーム（KSAT + PhishER）

KnowBe4の製品はすべて、SSAE18基準のSOC 2 Type 2の認証を取得しています。（KSAT、PhishER、SecurityCoachを含みます。）SOC 2 Type 2レポートの全文をご希望の場合は、営業担当者またはカスタマーサクセスマネージャーまでご連絡ください。SOC 3レポートを見る

**KnowBe4のSOC 2評価には、以下のすべてのトラストサービス基準が含まれます。**

- **セキュリティ**
- **処理のインテグリティ**
- **プライバシー**
- **可用性**
- **機密保持**

コンプライアンスの目的でブリッジレターをご希望の場合は、担当者またはカスタマーサクセスマネージャーまでご連絡ください。先日作成された当社のCAIQ（Consensus Assessment Initiative Questionnaire）は、クラウドセキュリティアライアンス（CSA）STARレジストリページでご覧いただけます

CYBER ESSENTIALS CERTIFIED

KnowBe4の製品はCyber Essentials 認証を取得しています。認証を確認する

国際標準化機構27001規格（ISO 27001）は、事業所、開発センター、サポートセンター、データセンターが安全に管理されていることを保証する情報セキュリティ規格です。KnowBe4は、独立した第三者機関である米国適合性認定機関（ANAB: ANSI-ASQ National Accreditation Board）認定の認証機関により、国際標準化機構27001（ISO 27001）の各種規格に則った監査を受けています。KnowBe4が監査を通過した基準は、以下の通りです。

- 国際標準化機構27001:2022規格（情報セキュリティ管理策）
- 国際標準化機構27701:2019規格（プライバシー情報マネジメント）
- 国際標準化機構27017:2015規格（クラウドコンピューティングにおける情報セキュリティ管理策）
- 国際標準化機構27018:2019規格（PII処理者としてのパブリッククラウドにおけるPII保護）

ISO/IEC 27701:2019 登録証明書

ISO/IEC 27001:2022 登録証明書

A-LIGN ISO 27701 CERTIFIED

A-LIGN ISO 27001 CERTIFIED

A-LIGN ISO 27018 CERTIFIED

A-LIGN ISO 27017 CERTIFIED

## Defend、Prevent、Protect（防御・予防・保護）

Defend、Prevent、Protectは、EgressのSOC 2 Type 2レポートおよびISO 27001認証の対象になります。

Caplinked上の当社情報セキュリティデューデリジェンスパッケージ（Defend、Prevent、Protectの各監査報告書および認証書を含む）へのアクセスをご希望の場合は、アカウント担当者までご連絡ください。

## 情報セキュリティ・データプライバシーチーム

KnowBe4の情報セキュリティ・データプライバシー専門チームは、関連する業界の以下の認定資格を保持しています。


## アクセス制御および認証制御

KnowBe4は、業務上必要な範囲に限定して、お客様のデータおよび機密データへのアクセスを許可しています。アクセス権は、組織内での役割に基づいて付与されます。KnowBe4は、機密データへアクセスする際は必ず多要素認証を行っています。必要に応じて、システムへのアクセスはIPアドレスによって制限されています。

## データの取扱いとデータプライバシー

- KnowBe4は、欧州連合の一般データ保護規則2016/679（GDPR）に準拠しています。
- 欧州経済領域（EEA）から米国へのデータ転送には、欧州委員会承認の標準契約条項を採用しています。適用されるあらゆるデータプライバシー法に準拠するためのポリシーおよび手順を整備しています。

データの種類および利用目的に関する詳細は、当社プライバシーポリシーの製品タブをご参照ください。

## データの暗号化

KnowBe4は、転送中のデータ暗号化（TLS）および保存データの暗号化（AES-GCM 256）にAWSを利用しています。現在KnowBe4は、TLS 1.2以降をサポートするロードバランサーおよびCloudFrontセキュリティポリシーを使用しています。当社の全製品において保存時のデータ暗号化を実現するため、AWS Key Management Service（KMS）を採用しています。データベース（RDS）内のデータおよびS3内に保存されたデータの暗号化にこれを使用します。

AWS KMSは、256ビットの秘密鍵を用いたガロア／カウンターモード（GCM）のAES（Advanced Encryption Standard）アルゴリズムを使用します。

## データセンターの場所

KnowBe4はAmazon Web Services（AWS）内で運用されています。AWSは責任共有モデルを遵守します。AWSはクラウドのセキュリティに責任を負い、KnowBe4はクラウド内でのセキュリティに責任を負います。AWSデータセンターのコンプライアンスに関する情報は、AWSコンプライアンスウェブサイトでご覧いただけます。データセンターのSOCレポートをご覧になる必要がある場合は、最新のAWS SOC 3レポートをご確認ください。

# KnowBe4が使用するAWSの地域

データローカリゼーション要件に基づき、データの保存場所を選択することができます。現在は、米国、欧州、英国、カナダでデータセンターを運営しています。ただし、特定の機能において補助サービスを利用していることから、これらのサービスがデータを別の場所に保存することがありますのでご了承ください。サブプロセッサを見る

| 製品 | プロダクション・データベース | ディザスタリカバリ・データベース |
|---|---|---|
| **KSATおよびPhishER（オプション1）**<br>*データを米国に保存することを希望されるお客様 | Amazon AWSデータセンター（米国、バージニア州北部（us-east-1）） | Amazon AWSデータセンター（米国、オレゴン州（us-west-2）） |
| **KSATおよびPhishER（オプション2）**<br>*データをアイルランド（EU）に長期保存することを希望されるお客様 | ヨーロッパのAmazon AWSデータセンター（アイルランド、ダブリン（eu-west-1）） | Amazon AWSデータセンター（ドイツ、フランクフルト（eu-central-1）） |
| **KSATおよびPhishER（オプション3）**<br>*データをカナダに長期保存することを希望されるお客様 | Amazon AWSデータセンター（カナダ、モントリオール（central）） | ヨーロッパのAmazonAWSデータセンター（アイルランド、ダブリン（eu-west-1）） |
| **KSATおよびPhishER（オプション4）**<br>*データを英国に長期保存することを希望されるお客様 | Amazon AWSデータセンター（英国、ロンドン（eu-west-2）） | ヨーロッパのAmazonAWSデータセンター（アイルランド、ダブリン（eu-west-1）） |
| **KSATおよびPhishER（オプション5）**<br>*データをドイツ（EU）に長期保存することを希望されるお客様 | Amazon AWSデータセンター（ドイツ、フランクフルト（eu-central-1）） | ヨーロッパのAmazonAWSデータセンター（アイルランド、ダブリン（eu-west-1）） |
| **KCM GRC（オプション1）**<br>*データを米国に保存することを希望されるお客様 | Amazon AWSデータセンター（米国、バージニア州北部（us-east-1）） | Amazon AWSデータセンター（us-west-1） |
| **KCM GRC（オプション2）**<br>*データをEEAおよび／または英国に保存することを希望されるお客様 | ヨーロッパのAmazon AWSデータセンター（ロンドン（eu-west-2）） | Amazon AWSデータセンター（アイルランド、ダブリン（eu-west-1）） |

データセンター間でデータを共有することはありません。各地域でアカウントをリクエストできますが、これらは互いに独立しており、アカウント間でデータは同期されません。

## データバックアップとデータ保持

KnowBe4はデータベースのバックアップを1年間、監査ログおよびアプリケーションログを3年間保持します。これらのバックアップは、上記のデータ暗号化セクションに記載されている方法に従い、暗号化されて保存されます。データ削除のリクエストを送信する場合は、営業担当者またはカスタマーサクセスマネージャーまでご連絡ください。

## 意識向上とトレーニング

KnowBe4の従業員は全員、採用時および年1回以上、必修のセキュリティ意識向上およびプライバシートレーニングを修了します。当社では、月に1回以上、フィッシングおよびソーシャルエンジニアリングの模擬テストを継続的に実施しています。nowBe4の全従業員および契約社員は、採用時および会社または顧客データへのアクセス前に、秘密保持契約および守秘義務契約に署名します。

## 事業継続／ディザスタリカバリ

KnowBe4では、高度にスケーラブルかつ耐障害性の高い製品アーキテクチャがAWS内に設計されています。当社の製品は高度な攻撃に耐えるとともに、高い適応性を備えています。製品アーキテクチャ内における当社システムのパフォーマンスは主要指標に基づき監視されており、いずれのシステムへの負荷も許容範囲内に収まるよう管理されています。万一、コンポーネントに過負荷や障害が発生した場合、自動化されたプロセスが実行され、別の一時システムをオンライン化するか、既存システムを新しいシステムに切り替える対応が取られます。KnowBe4のアーキテクチャには自動化機能が組み込まれているため、必要に応じて、システム監視、アップデート、および修正措置がダウンタイムなしで実行されます。
ステータスおよびアップタイムのモニタリング

KnowBe4のリスク管理プログラムは、KnowBe4で年に一度行われる第三者監査（FedRAMP、ISO 27001、およびSOC2）の一環で評価されます。KnowBe4のリスク管理プログラムの全概要を見る

## コードセキュリティとコードアップデート

KnowBe4の研究開発（R&D）部門は、コードデプロイメントの管理に継続的インテグレーション／継続的デリバリー（CI/CD）パイプラインを活用しています。コード変更はピアレビューを経て、別のQAスタッフによる承認を受け、本番環境にプッシュされる前にステージング環境でテストされます。ステージング環境と本番環境は論理的に分離されており、両環境間でデータが共有されることはありません。

## ロギングおよびモニタリング：

KnowBe4は、すべてのシステムから監査ログとアプリケーションログを収集します。これらのログは、ログを生成するシステムとは別の集中ログファシリティに暗号化されて保存されます。ログエントリは、監査証跡に関する業界標準に準拠しています。KnowBe4は、過去のシステム活動を調査する目的で、これらのログを3年間保持します。

## 脆弱性管理

KnowBe4の情報セキュリティチームは、毎月ウェブアプリケーションの脆弱性スキャンを実施しています。これらのスキャンは認証済みスキャンとして実行されるよう設定されています。これらのスキャン中またはその他の脆弱性発見作業で発見された脆弱性は、脆弱性追跡システムに追加されます。そこで、脆弱性は検証・分類され、実際のリスクについて評価されます。なお、脆弱性は以下のスケジュールに従って修正されます。

以下のSLAは、CVSS（共通脆弱性評価システム）に基づく脆弱性発見に対して適用されます。Snyk Priority Score（Snyk優先度スコア）が800未満の場合、SnykはCVSSスコアのみを使用して優先度の決定は行いません。Snyk Priority Score（Snyk優先度スコア）は、CVSSスコア、修正プログラムの有無、既知の悪用手法、脆弱性の新しさ、到達可能性の有無などの複数の要素を処理する包括的なスコアリングシステムです。

| 重大度 | 重大／高 | 中 | 低 | 情報提供 |
|---|---|---|---|---|
| 修復期間 | 30日未満 | 90日未満 | 180日未満 | 任意 |

以下のSLAは、CVSSに基づく脆弱性発見に対して適用されます。

Snyk Priority Score（Snyk優先度スコア）が800以上の場合、リスクスコアのあるCVSSスコア未評価の脆弱性は、OWASPリスク評価手法（リスク＝発生確率 × 影響度）を用いて決定されます。

| 重大度 | 重大／高 | 中 | 低 | 情報提供 |
|---|---|---|---|---|
| 修復期間 | < 14 Days | 30日未満 | 180日未満 | 任意 |

## ペネトレーションテスト／バグバウンティ／セキュリティ脆弱性の報告

KnowBe4は、審査済みの第三者調査機関が当社製品に対して継続的なペネトレーションテストを実施する、有料の非公開バグバウンティプログラムに参加しています。当社のシステムにセキュリティ上の欠陥を発見したと思われる場合は、プログラムに登録していただければ、参加をご招待いたします。バグバウンティプログラムを通じて、またはKnowBe4セキュリティチームinfosec@knowbe4.comに直接連絡して、脆弱性を報告していただけます。テストを実行し、発見をぜひ当社にお知らせください。この非公開プログラム以外でのセキュリティテストは許可されていません。また、本プログラムでは自動スキャンを一切許可しておりません。調査機関には、混乱を招かないよう手動でのテストを実施するようお願いしています。