Varonis
セキュリティ方針とプラクティス

もくじ

このホワイトペーパーでは、2023 年 7 月現在の Varonis のセキュリティの現状について説明しています。今後の機能や製品のローンチにより変更されることがあります。

2005 年に設立された Varonis のお客様には、大手金融会社、ヘルスケア、産業、保険、エネルギーおよび公共部門、テクノロジー、消費財および小売業、メディアおよびエンターテイメント、教育セクターが含まれています。

セキュリティへのアプローチ

哲学

組織は、提供する柔軟性や生産性を求めてクラウドソリューションを採用していますが、効率の向上はリスクの増大を伴うことがあります。Varonis では、ソフトウェア開発とセキュリティプラクティスに真剣に取り組んでいます。当社では、お客様に当社のソリューションとアプローチを信頼いただけるよう、磨きをかけたセキュリティプラクティスを共有しています。

Varonis はデータセキュリティと解析の先駆者で、データの保護、脅威の検出と脅威への対応、コンプライアンスに特化しています。Varonis では情報セキュリティ管理システム (ISMS) にリスクベースのアプローチを採用しています。このアプローチでは、情報資産の脆弱性と脅威を特定して、評価し、適切に軽減することが求められます。ISMS を展開することにより、認可されていない、事故、または意図的な情報の開示、改竄、処分のリスクを低減することができます。

当社のチーム

当社の経験豊富なチームは、情報セキュリティのあらゆる分野で活動しています:

- **CISO** ― グローバルセキュリティチームを率い、社内インフラストラクチャーとクラウド本番環境のセキュリティプログラムを担当しています。CISO はまた、情報セキュリティ方針、標準、ガイドラインの開発およびレビューを指揮し、監督します。
- **セキュリティオペレーションセンター (SOC) チーム** ― セキュリティインシデントの連絡窓口です。当社のグローバル SOC チームは、階層型組織になっており、システムの監視とサイバーセキュリティインシデントの調査を担当しています。また、運用上の脚本を作成し、脅威検出能力を向上するためのアラートの機能拡張を提案します。
- **製品セキュリティグループ** ― セキュアソフトウェア開発ライフサイクル (SSDLC) プログラムを主導します。このプログラムは、クラウドベースの本番環境を含む、すべての Varonis 製品ラインのセキュリティ管理策の設計、テスト、実装を担っています。
- **ガバナンス・リスク管理・コンプライアンス (GRC) チーム** ― お客様からの問い合わせやアセスメントに対応します。また、このチームは、セキュリティ意識向上プログラム、リスク

管理、外部セキュリティ監査、コンプライアンスプログラムについても責任を負っています。

- **社内セキュリティアーキテクト** – 当社の社内インフラストラクチャー、ネットワークとクラウドベースの IT ソリューションのセキュリティ要件を定義します。
- **開発、セキュリティおよび運用 (DevSecOps) チーム** – セキュリティプロトコルの実装と脆弱性の修正に責任を負っています。
- **セキュリティ調査およびフォレンジックチーム** – 監視対象のプラットフォーム上の新しいセキュリティ問題を特定し、新たな脅威を確実にカバーする製品ロードマップを定義します。

セキュリティプログラムの継続的な改善

当社は、優れたセキュリティプログラムには、インフラストラクチャーとクラウドのオファリングを改善するための継続的な取り組み、定期的な評価と更新が必要であることを理解しています。そのため、定期的に内部評価と外部評価を実施しており、ポリシーを継続的に更新および改善して、現行の管理体制が最も厳格なセキュリティ基準、プライバシー基準、およびコンプライアンス基準に準拠するようにしています。

自社環境の保護

セキュリティ設計

Varonis では、セキュリティは、すべてのシステム、プロジェクト、プロセスに組み込まれています。さらに、セキュリティ要件は、ソフトウェア開発のすべての段階に組み込まれています。

質の高いソフトウェアは、強固な基盤の上に構築されます。当社は、すべての新しいソフトウェアコンポーネントは、初めからセキュリティを念頭に置いて設計されるべきだと考えています。当社は、実績のある機能とフレームワークを使用してソフトウェアを開発しています。当社は、標準化されたセキュリティ管理策を使用しながら、そのコンポーネントを実装するための最善かつ最も安全な方法についてベンダーと相談しながら、仕様を設計しています。

優れたソフトウェア製品は絶えず進化を続けており、従って、セキュリティの問題を発見し、開発チーム間で追跡し続けるために、リスクと脅威の管理は重要です。共通脆弱性評価システム (CVSS) などのツールを活用することで、問題の評価と優先順位付けを行うことができます。

当社では初期段階からセキュリティを設計に組み込んでいます—すべての設計はセキュリティと安全性の危険性についてレビューされ、適切な緩和策が作成されます。特定された脅威は、さらなるセキュリティテストの基礎として使用されます。

お客様のデータ

Varonis ではデータとメタデータを区別しています:

1. お客様メタデータには、ユーザーID と名前、グループ名、フォルダー名とファイル名、電子メールの件名、ドメイン、ユーザーがアクセスする IP アドレスが含まれます。
2. お客様データには、ファイルや電子メールのコンテンツが含まれます。

Varonis のグローバル分類ポリシーにより、すべてのお客様メタデータは「confidential」に分類されます。お客様データは安全に保管し、お客様の環境での即時あるいは潜在的なリスクを特定するために監視されます。

Varonis SaaS Data Security Platform

Varonis のテクノロジーは、データソースをクロールして、お客様データを分類します。

お客様データは、それからお客様ネットワーク内にインストールされた Collector サーバーによって取得および処理されます。Varonis SaaS Data Security Platform はお客様データをクラウドに保管しません。[1]

メタデータとデータ分類結果は、お客様が利用できるようにするため、SaaS にアップロードされます。このデータは、さらに分析をし、お客様環境での即時あるいは潜在的なリスクを特定するために、保護されたストレージに収集および保管されます。生成されたアラートを含むこの情報は、Varonis SaaS のダッシュボードで簡単に見ることができます。すべてのお客様メタデータは常に暗号化された形式で保管および転送されます。

Varonis DatAdvantage Cloud

Varonis DatAdvantage Cloud は、Salesforce、Google Suite、Box などのクラウドデータソース専用です。

これらのデータソースの場合、Varonis は、Collector サーバーのインストールは必要なく、すべてのデータを DatAdvantage Cloud がデータソースから取得します。

データはクラウドに保管されず、データ分類の後、破棄されます。メタデータと分類結果は、お客様による分析ができるように、クラウドに保管されます。

アクセス制御と管理

本番環境アクセス権の保護

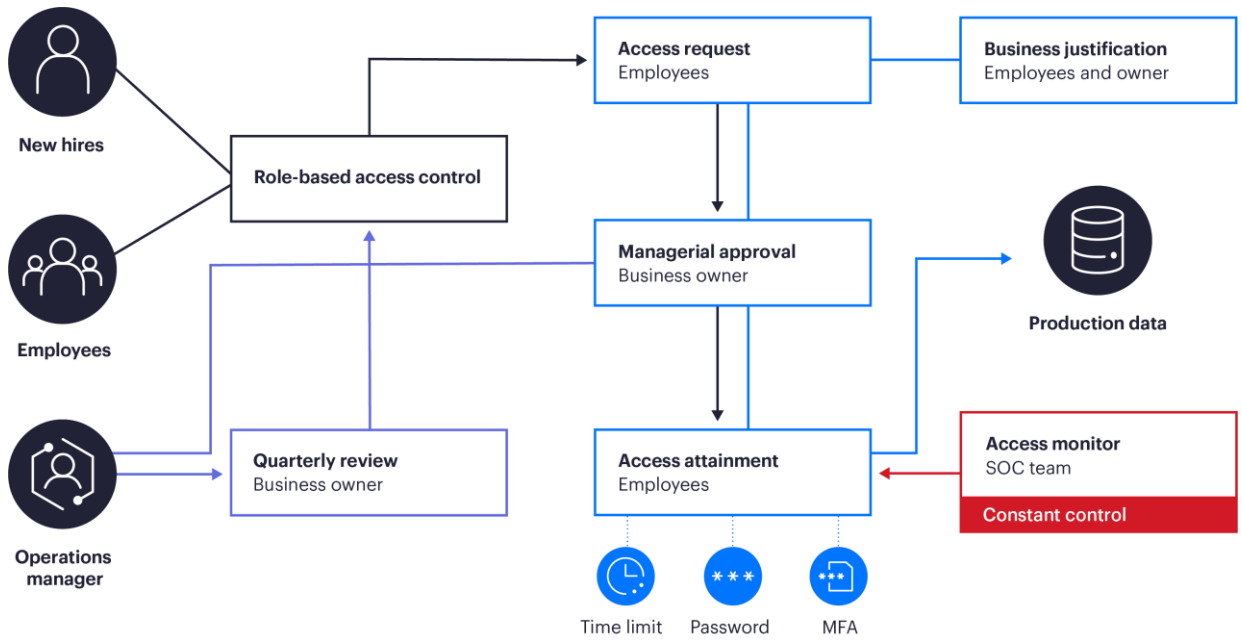
Varonis では、ユーザーのアクセス権をプロビジョニングするためのプロセスが定義されています。新規採用者には、社内での役割（つまり、役割ベースのアクセス制御 (RBAC)）と最小権限の原則に基づいて、リソースへのアクセス権が付与されます。本番環境へのアクセス権を申請できるのは、必要不可欠な従業員のみです。各アクセス権には、ビジネスオーナーの承認と業務上の必要性の文

---

1 お客様は、クラウドでオプションの「ファイル分析 (File Analysis)」ロールを有効にすることができます。有効にするとファイル分析ロールを承認されたお客様のユーザーは、ファイルを保存することなく、特定のファイルを SaaS 経由で取得することができます。

書化が必要です。アクセスは監査され、時間制限があり、常に SOC チームにより監視されています。多要素認証 (MFA) もセッションごとに必須となっています。

図 1: アクセス権の承認



アクセス権レビュー

すべての本番アカウントは、適切なレベルのアクセスおよびアクセス許可を持っていることを確認するために、ビジネスオーナーにより定期的に見直され、承認されます。Varonis 社員は MFA と強力な認証を使用して本番環境にアクセスしています。

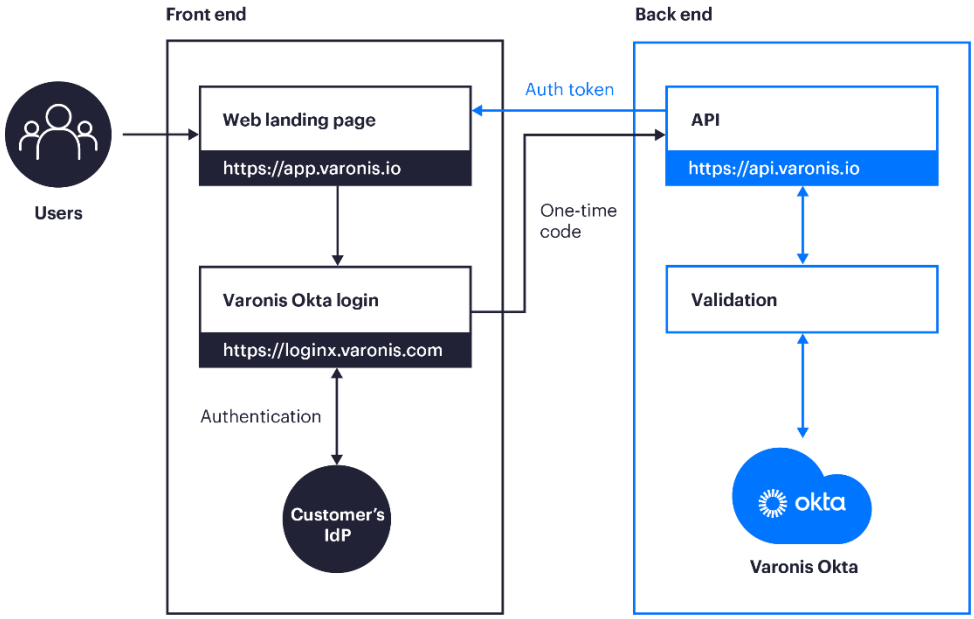
パスワード

Varonis のクラウドサービスには、業界のベストプラクティスとベンダーの推奨に従ったパスワードポリシーが定義されています。当社のアクセス承認プロセスでは、プロビジョニング、見直し、パスワードの強度がカバーされています。

ユーザー認証と認証連携

認証は OAuth 2.0 を使用して行われます。Varonis の IDP (Okta) を使用することも、お客様の IDP を使用してフェデレーションを構成することも可能です。後者では、お客様が MFA、パスワードの複雑さ、ロックアウトポリシー、ソース IP アドレスなどのログインポリシーを制御できます。

図 2: 認証連携のワークフロー



安全なアーキテクチャーとデータフロー

バックエンドプロセスは、お客様のクラウドサービスやオンプレミスのデータストア（NetApp ファイラーなど）にアクセスし、ファイル、フォルダー、ユーザー、グループ等のイベントとメタデータを取得します。収集したすべての情報は、テナントごとにパーティション化されて保管され、テナント間のアクセスの禁止を強制しています。この情報は、その後、認証されたユーザーのみが Web UI に表示させることができ、そのユーザーはログインしている特定のテナントのみにアクセスできます。すべてのデータは、外部転送中でも内部転送中でも、暗号化されています。

図 3: Varonis SaaS アーキテクチャー

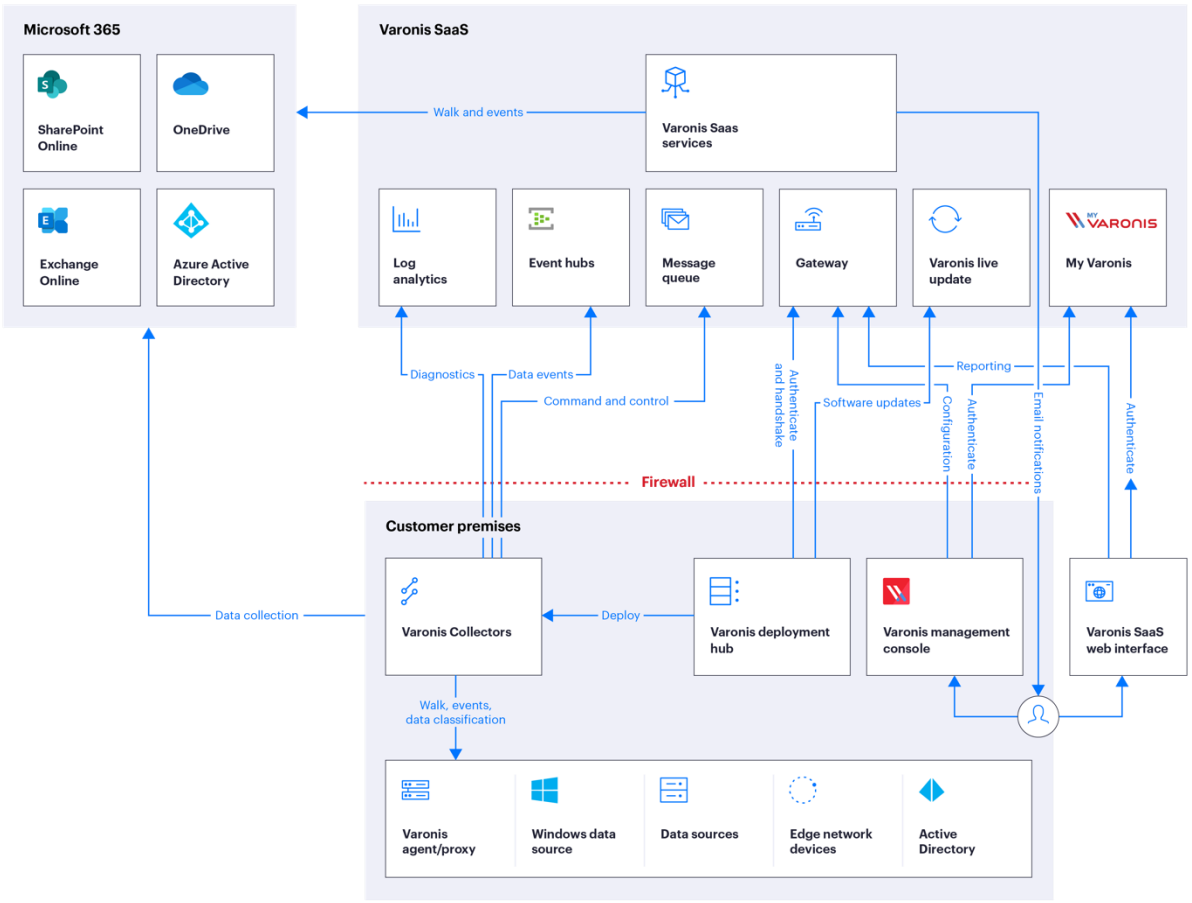
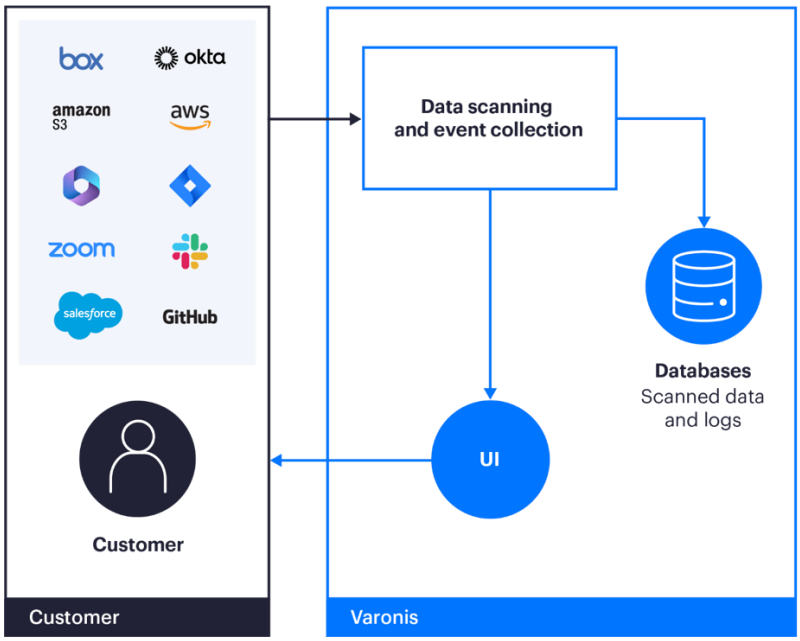


図 4: DatAdvantage Cloud アーキテクチャー



API アクセス許可

Varonis は役割へのユーザーの割り当てをサポートしています。Varonis は RBAC を実装しているため、API 呼び出しの都度、UI 経由でバックエンド API にアクセスしているユーザーが必要な役割を割り当てられているかを確認しています。

ネットワークアーキテクチャーへのセキュリティの組み込み

システムのユーザーは、リソースを使用する前に、割り当てられたユーザーの役割に従って識別され、認証されなければなりません。ネイティブのセキュリティシステムとアドオンソフトウェア製品がリソース保護を提供します; これらのシステムとソフトウェア製品は、ユーザーを識別および認証し、アクセス制御リスト上のユーザーの許可された役割と比較することによって、アクセス要求を検証します。監視は、作業アクティビティに関与していないスーパーバイザーや、他の部門の従業員など、関与していない担当者によって実施されます。

各システムには、構成基準が定められています。セキュリティアーキテクトがこれらの基準を定め、毎年、また必要に応じて、更新します。実装に先立ち、セキュリティ主任者とシステムアーキテクト主任者が構成基準をレビューし、承認します。

すべてのリソースは資産目録システムで管理され、各資産には所有者が割り当てられています。所有者は、リソースへのアクセスを承認し、役割ごとのアクセス権を定期的にレビューする責任を負います。

ネットワークセキュリティ

当社は、さまざまな技術や監視ツール、安全なネットワークアーキテクチャーによって、社外および社内のネットワークを保護しています:

- 社内のセグメント化はサービスごとに行われています。
- システムエラーの影響を軽減するために、本番システムには高可用性配列と負荷分散配列が設置されています。
- Web アプリケーションファイアウォールがクラウドベースソリューションと企業インフラストラクチャーの前面にあり、悪意のある Web 攻撃や制裁対象国をブロックするための強制ルールが適用されています。

- Microsoft Azure と Amazon AWS のパブリッククラウドインフラストラクチャーにより、DDoS に対する全体的なネットワーク保護が提供されています。ネットワークセキュリティ攻撃とアラートは、セキュリティオペレーションセンターにより継続的に監視されています。

Varonis エンドポイントデバイスの保護

エンドポイントセキュリティは、Varonis の徹底したセキュリティ防御アプローチの極めて重要なメカニズムです。

当社は次のような手法を使用して、エンドポイントへの脅威を最小限に抑えています。

- **マルウェアからの保護** ― 当社の企業インフラストラクチャー内では、SOC チームが監視している内部サーバー上の対応ソリューションに加えて、Varonis のセキュリティチームによりマルウェア対策とエンドポイント検出を導入されました。
- **パッチ管理** ― 当社のパッチ管理ポリシーでは、セキュリティ更新を速やかにインストールすることが義務付けられています。すべてのデバイスは継続的に脆弱性スキャンを受けます。
- **構成管理** ― 当社では自社サーバー向けのハードニングポリシーを開発しました。
- **モバイルデバイス管理** ― 当社はすべての企業デバイスと認証されたデバイスに、MDM（モバイルデバイス管理）ソリューションを利用して、暗号化、パスワード保護、セッションタイムアウト、監査、スマートフォンやモノのインターネット（IoT）による本番データへのアクセスを禁止するなどしています。
- **監視** ―当社の SOC チームは、継続的に資産を監視し、サーバーやエンドポイントデバイスからの異常、不審、または悪意のあるアクティビティに対応します。SOC は様々なセキュリティシステムからアラートを受け取ります。SOC チームは常に脅威検出能力を向上させ、サービスプロバイダーと連携してルールを微調整し、新しい検出方法や対応方法を積極的に模索しています。

運用セキュリティ

構成および変更の管理

当社の環境内すべての変更は構造化された変更管理手順の対象となります。変更は、設計および影響の分析を受け、継続的に監視されます。当社のすべてのプロセスと同様に、変更管理手順は、年次外部監査（SOC 2 および ISO/IEC 27000 シリーズ）の対象となっています。

ソフトウェアコードの変更

当社のチェックイン (CI) / チェックアウト (CO) プロセスは、本番環境の変更プロセスと完全に統合されています。これらのプロセスには、プログラマーによるピアコードレビュー（変更に対して責任を負わないユーザーにより実施）とコミットされた各変更の承認が含まれます。新しく開発されたコードは、その後、回帰テスト、単体テスト、セキュリティテスト、統合テストなど、品質保証のいくつかのプロセスを経ます。候補ビルドは、その後、文書化されたテスト計画に基づいて、手動テストおよび自動テストを受けます。テストを完了すると、新しい候補ビルドは、関連するマネージャーによってレビューされ、承認されます。当社では、マルチテナントアプリケーションにも同じプロセスを適用します。すべての変更はバージョン管理システムにログが記録され、文書化されます。

インフラストラクチャーとその他の変更

当社では他のすべての種類の変更について、影響分析、セキュリティチームとビジネスオーナーによる承認、文書化、テスト、代替プラン、必要な場合のお客様への通知などを含む、文書化されたプロセスを確立しています。

変更の通知

Varonis は、お客様のクラウド環境に悪影響を及ぼす可能性のあるクラウドサービスのアップグレードと変更をお客様に通知し、情報を提供します。すべてのソフトウェア更新パッケージは、アップグレードの一部として配布され、デジタル署名が含まれています。

データのテスト

データをテストする際には、当社は以下のプラクティスに従います:

- 規制対象のデータをテスト目的で使用することは禁止されています。
- 個人識別情報 (PII) またはその他の機密情報がテスト目的で使用される場合、すべての機密詳細およびコンテンツは匿名化されます。
- お客様データをテスト目的で使用することは禁止されています。

ログ取得と監視

IT インフラストラクチャーとクラウドベースのセキュリティソリューションによる包括的なログ記録と監視により、情報システムやデータへの不適切なアクセスや使用を、あるいはその両方を検出し、対応します。

すべてのクラウドオファリングと企業インフラストラクチャー環境から詳細な監査ログが収集されています。当社のセキュリティオペレーションセンターとクラウドオペレーションチームは、ログを監視し、パフォーマンスの問題やセキュリティインシデントに対して自動通知や脚本を使用しています。

事業継続と災害復旧管理

お客様のサポートと回復力は Varonis の最優先事項です。当社の事業継続 (BC) 計画は、お客様やパートナーに対する混乱を回避するための対策をまとめたものです。事業継続計画には、重要な機能とプロセスを特定するための影響分析とリスクアセスメントが含まれています。

また、当社では以下のような事業継続計画を策定しています:

- 企業インフラストラクチャー

- リモートワーク
- サイバーインシデントレスポンス対応
- パンデミックへの準備

当社のクラウド環境はクラウド運用チームとインシデントレスポンスチームにより監視されています。当社では、お客様にダウン時間を通知するためのプロセスを確立しています。

高可用性アーキテクチャー

高可用性の一環として、当社のクラウド本番インフラストラクチャーとサービスは完全に冗長化されており、単一障害点やダウン時間を回避しています。

クラウドホスティングの回復力機能

Microsoft Azure と Amazon AWS サービスは、冗長化されたデータセンター、電力供給、インターネット回線などを備え、デフォルトで回復力のあるクラウドホスティングサービスを提供しています。お客様データについては、高可用性、データ損失や破損が発生した場合でも復旧できることを確実にするため、物理的および論理的な制御を行っています。当社のクラウドプロバイダーは、データセンターの耐障害性を継続的にテストし、全体的なセキュリティアーキテクチャーを継続的に改善し、最高水準のセキュリティ基準を満たしていることを検証しています。

監視

クラウドインフラストラクチャーは、当社のエンジニアによって継続的に監視され、いかなる障害についても検知して即座に対応できるように安全に設計されています。お客様ログは、迅速な解決とダウン時間の回避のために、データそのものと同じデータセンターに保存されています。当社では、また、お客様にダウン時間を通知するためのプロセスを確立しています。可用性管理は、SOC 2 および ISO27000 の監査時に毎年テストされています。

お客様は https://varonisprod.statuspage.io/ から、障害に関するプロアクティブなコミュニケーションを申し込むことができます。

バックアップと復元

Varonis は、システムのバックアップと復旧アクティビティの担当者をガイドするためにポリシーを文書化しています。可用性と完全性を確保するため、毎日バックアップを行い、定期的に復旧テストを実施しています。お客様データは Amazon AWS と Microsoft Azure のデータセンターに保存され、デフォルトで遠隔のアベイラビリティゾーンに複製されます。当社では、データサーバーを自動的に構築するために、infrastructure-as-a-code（コードとしてのインフラストラクチャー）を使用しています。これにより、災害時にインフラストラクチャーを迅速に再構築することもできるようにしています。

物理セキュリティ

Varonis は業界のベストプラクティスに沿った物理セキュリティポリシーを持っています。このポリシーでは、全世界のオフィスの安全確保、建物やオフィスへのアクセス制限、バッジによる入室、定期的な入室審査、職場の継続的な監視の手順が詳細に記されています。

当社の SOC 2 準拠のパートナーデータセンターはさまざまな物理セキュリティと環境管理に対応します。当社は毎年、コンプライアンス証明書と認証レポートを確認し、一貫した保護レベルを確保しています。

サードパーティのデータセンターへのアクセス

当社はクラウドベースのソリューションのサービスプロバイダーとして、Amazon AWS と Microsoft Azure を使用しています。両組織とも、監視、検知システム、その他の電子的手段を使用してデータセンターの安全性を確保するために、十分な物理アクセス制御システムとセキュリティ要員を備えています。

Varonis 施設の物理セキュリティ

物理アクセス保護の仕組みには、アクセスカードや監視カメラで管理される入口や、その他の環境的なセキュリティ管理が含まれています。従業員は Varonis の施設内では ID バッジを身に着けていなければならず、バッジを他人と共有することもできません。アクセス権限は最小特権モデルに基づいて付与されます。退職した要員、異動した要員、あるいは情報システムが存在している施設にアクセスする必要がなくなった要員のアクセス権限は速やかに削除されます。アクセス権限は施設

管理者により定期的に見直され、承認されます。Varonis の施設は、監視カメラや鍵、ID カード、物理的な存在（警備員や会社の職員）によって監視され、保護されています。

お客様データの安全な保管

暗号化

パブリックネットワーク経由で転送されるお客様データは ー 少なくとも ー トランスポート層セキュリティ (TLS) 1.2 以降を使用して暗号化されます（後方互換性のために TLS 1.1 をサポートすることも可能です）。Varonis は、可能な限り、より長い鍵と FIPS 準拠の暗号を備えた強力な暗号を使用します。また、定期的に使用されている暗号とアルゴリズムを監視し、非推奨のバージョンが使用されていないことを確認しています。

許可された従業員は Varonis クラウドソリューションに VPN（仮想プライベートネットワーク）と MFA を使用してアクセスすることができます。Varonis はパブリックネットワーク上でデータを送信する際にデータを暗号化するための安全なデータ転送プロトコルを実装しました。暗号化は、保存中のデータベースおよびデータのバックアップでも有効になっています。境界間の通信は暗号化されます。外部ゾーン境界（インターネットに面するサービス）は TLS を介して公開されます。

保存データの暗号化はすべてのテナントとサーバーでクラウドサービスプロバイダーによりデフォルトで強制されています。保存中のデータは Advanced Encryption Standard (AES) 256 ビット暗号化を使用して暗号化されます。

鍵管理

Varonis ではシークレットと資格情報の管理に Azure Key Vault ソリューションを使用しています。この保管庫にはアクセス制限が適用され、ユーザーへのアクセス権は提供されません。鍵保管庫を含むインフラストラクチャーの一部にアクセスするためには、システムユーザーには利用できないアクセス許可が必要となります。

インフラストラクチャーへのアクセス試行はすべて監査されます。

データセンター

当社では、DatAdvantage Cloud に Amazon AWS、Varonis SaaS に Microsoft Azure を選定していますが、両社ともにガートナー社の「クラウド・インフラストラクチャ／プラットフォーム・サービスの

マジック·クアドラント」においてリーダーに選べています。Varonis SaaS および DatAdvantage Cloud は米国内の複数のアベイラビリティゾーンでホストされています。当社のデータセンターはさまざまなセキュリティ業界標準の認定を受けています。

マルチテナントのセキュリティ

テナントを分離し、他のお客様のデータやテナントを危険にさらすことを避けるために、論理的なセキュリティが実装されています。

- お客様ごとに、個別の役割、シークレット、データベースパーティションがあります。
- お客様データベースに接続するトークンなど、すべてのシークレットは、管理された鍵保管庫ソリューションに保管されます。テナントのシークレットへのアクセスには、個別の役割が使用されます。
- アクセス認証および承認のセクションで説明しているように、従業員の本番環境へのアクセスは制限され、管理者の承認により、オンデマンドで特定の従業員に対してのみ、短時間の間、許可されます。
- 本番環境は、ステージング環境や開発環境から完全に分離されており、個別のアクセス制御とセグメント化されたネットワークが用意されています。

お客様データの管理責任の共有

Varonis のシステムは、システムのユーザーによって管理される責任を共有するように設計されています。お客様による管理は、Varonis の管理を補完するためにユーザーエンティティーで運用されることが期待されています。

お客様は以下の項目について責任を負います:

- 強力なパスワードポリシーの確保
- ID プロバイダー接続して、以下を強制すること:
  - シングルサインオン
  - 認証
  - MFA
  - パスワードポリシー

- お客様の ID プロバイダー (IDP) との My Varonis のフェデレーション構成
- ユーザーのアクセス権が不要になった場合に、従業員のユーザーアカウントを適時に削除することを確実にすること
- オンプレミスコンポーネントの保護
  - パッチ管理プロセスの確保
  - オンプレミスのコンポーネントへのアクセス制限
  - ディスク暗号化
  - アンチマルウェア/EDR ソリューションでの頻繁なシグネチャーの更新とアラートの監視
  - 関連するシステムコンポーネントの継続的な監視
- 最小権限アクセスモデルに基づいてお客様の従業員に対するアプリケーションの役割を設定
- 強固なパスワードポリシーによる初期テナントアカウントの保護
- 監視対象のプラットフォームとの安全な統合
  - データソースへのアクセスには強力なシークレットを使用
  - 定期的なシークレットのローテーション
- データソースへのアクセスには暗号化された接続のみを使用
- テナントの場所の選定

データ保持

お客様データは、お客様の求めに応じて、あるいは、お客様にお伝えしているライフサイクルポリシーに基づいて、削除されます。お客様データの保持は、ソフトウェアプライバシーポリシー内（「収集した情報の保持期間 (How long do we retain the information we collect?) 」セクション以下）で説明されています。

人事のセキュリティプラクティス

技術的な手段に加えて、情報セキュリティでは人間による強制と適用が必要となります。当社の人事 (HR) セキュリティプラクティスは、従業員のセキュリティリスクを軽減する管理策に対応して

います。当社の雇用ライフサイクルポリシーは、すべての人事セキュリティトピックが含まれており、すべての従業員、スタッフの役割変更、および各地域の再委託先に適用されます。

雇用

- 法律により適用可能な場合かつ Varonis のポリシーに基づいて、すべての採用候補者および委託先について身元確認が実施されます。
- 機密性の高い役割と、特権アクセスまたはお客様データへのアクセス権を持つ従業員については、追加の検証チェックが必要となります。
- 従業員は、秘密保持契約 (NDA) に署名の上、セキュリティポリシーと当社の行動規範を確認する必要があります。
- ユーザーには関連する役割とアクセス許可のみが割り当てられます。

在職中

- すべての従業員が、毎年、セキュリティとプライバシーの研修を受けます。このプログラムには、CISO による現在の業界の脅威の状況の指導や、定期的なフィッシングシミュレーションが含まれています。
- 開発者向けには定期的に役割ベースのセキュリティトレーニングを実施します。
- 役割の変更があれば、アクセス許可はレビューされ、変更されます。

アカウントの停止

- Varonis には、すべての論理的および物理的アクセス権に取り消し手順があり、従業員の退職後に Varonis から提供されたすべてのコンピューティングデバイスの返却を義務付けています。
- 人事部門が退職手続きを開始すると、関連部門で即座に必要なアクションがトリガーされます。

セキュリティ意識向上トレーニング

すべての従業員は、各自の役割に関連する組織の方針および手順の定期的な更新に加え、適切なセキュリティとプライバシーに関する意識向上トレーニングを受けます。

従業員のセキュリティトレーニングはセキュリティチームの責任です。これは継続的なプログラムであり、すべての従業員が、社内の職務と地位に関連するセキュリティ問題について、常にトレーニングを受ける必要があります。

トレーニングは、各従業員の職務レベルに関連する必要があり、以下の内容で構成されます:

- 全従業員を対象とした一般的なセキュリティトレーニング
- PII にアクセス権を持つ従業員向けのプライバシートレーニング
- 開発者向けのセキュアコードトレーニング

その他の要件:

- 従業員ガイドラインが配布され、インターネットポータルにアップロードされています。
- CISO の決定に従って、従業員に最新情報やニュースレターが送信されます。
- 新入社員は、教育パッケージを読んで署名しなければなりません。
- 各従業員は、関連するセキュリティポリシーの年次レビューと確認が必要です。

ソリューションの安全性

SSDLC フレームワークによるセキュアな設計

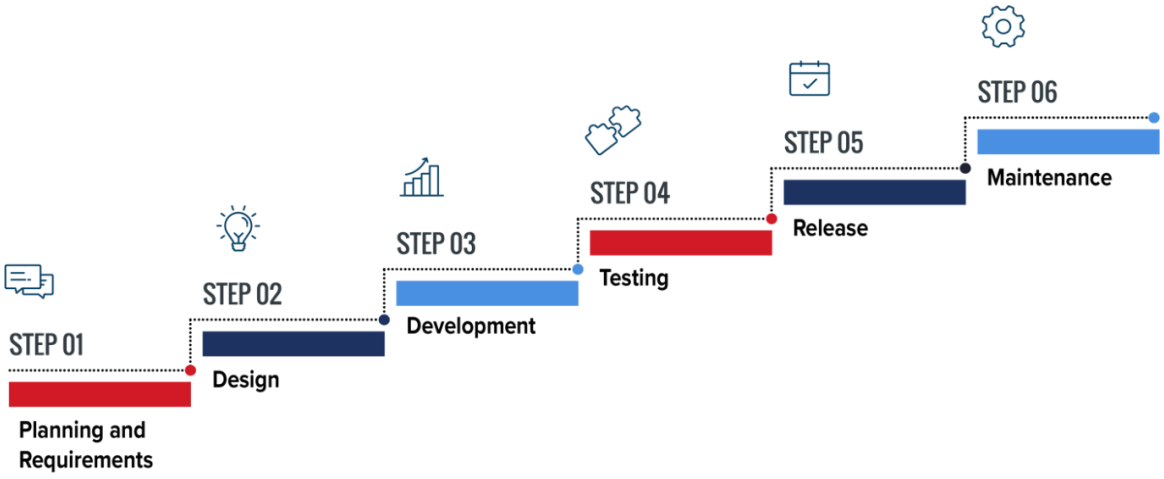
Varonis は、総合的な開発アプローチの一環として SSDLC フレームワークを採用しました。この実証済みのアプローチは、標準的な SDLC（ソフトウェア開発ライフサイクル方針）にセキュリティを追加し、SDLC の各フェーズの主要な構成要素としてセキュリティを組み込むことに重点を置いています。この方法論を使用することにより、Varonis は安全なアプリケーションと IT システムをより迅速に構築し、手戻りのコストを削減し、潜在的なセキュリティ問題を事前に特定して対処することができるため、この方法は組織にとって有効な投資になります。

以下の図 5 に示すように、このアプローチには次の 6 つのフェーズがあります:

- **計画と要件** — これはプロセスの基本的かつ重要なフェーズであり、構想しているシステムに対する組織のニーズが、お客様との実質的なフィードバックとやり取りによって特定されます。このフェーズでは、システムの目的や期待に関する関連情報が収集され、製品やサービスの実現可能性を判断するために使用されます。このフェーズの最後で、すべての曖昧さが解決され、構想しているソリューションの機能が正式に文書化されます。
- **設計** — 要件（ビジネス、機能、必須セキュリティ）を収集し、設計に組み込みます。機能要件によって何が起こるべきかを定義し、セキュリティ要件によって何が起こってはならないかを定義します。
- **開発** — 指定された要件に従ってシステムやサービスを購入するかカスタム構築するかを決定することにより、代替案を特定し利害関係者のニーズを満たすための最善のアプローチを決定します。確立された安全なコーディングのガイドラインとともに、ゼロからコードを書く場合とオープンソースの既存のコードを活用する場合のいずれの場合にも、ガイドライン正しく守られていることを再確認するコードレビューを使用します。
- **テスト** — 当初の設計とセキュリティ要件に照らして、リリース前テストを実施します。テスト結果が満足のいくものであり、お客様から正式な承認が得られない限り、アプリケーションを配備する準備は完了しません。

- **リリース** – 稼働開始、運用、保守、変更。将来のリリース、アップグレード／アップデート、システム機能拡張などの形式でのフィードバックに基づいて、アプリケーション機能の変更が計画されます。
- **保守** – 保守フェーズでは、Varonis はソフトウェアに対してセキュリティ脆弱性を修正するためのアップデートを提供します。保守フェーズが終了した後も、Varonis は通常、例外的な状況が発生しない限り、セキュリティの提供を停止しません。

図 5: Varonis SSDLC モデル



コード分析

Varonis では、手動および自動のセキュアコードレビュー技術を使用して、アプリケーションのソースコードを検査します。この検査の目的は、既存のセキュリティ上の欠陥や脆弱性を特定することです。コードレビュー中に、開発者は、特に論理エラーを探し、実装を検証し、スタイルガイドラインをチェックします。自動コードレビューでは、Varonis は商用ツールを使用してアプリケーションのソースコードを自動的にレビューし、事前に定義されたルールセットを使用して品質の悪いコードを見つけます。

脅威の特定、保護、対応

セキュリティテスト

Varonis では、当社の製品、サービス、インフラストラクチャーのセキュリティ管理およびプロセスをテストすることにより、当社のセキュリティ態勢を厳格かつ継続的に評価しています。当社は脆弱性や設定ミスをスキャンし、問題を迅速に修正します。

当社のセキュリティテスト手法の概要は次の通りです:

- **侵入テスト** — 自動スキャナーの実行に加えて、外部および内部の侵入テストチームによるテストを実施します。テスト結果は、機密保持契約に基づいて、ご要望に応じて提供可能です。
- **内部セキュリティテスト** — 当社の製品チームは特定の機能に関するセキュリティテストを実施します。
- **Web セキュリティアセスメント** — このアセスメントでは Web サービスや Web ベースのアプリケーションの脆弱性を特定します。
- **手動プロセス** — 新しいコードのコミットは毎回チェックされ、承認されます。製品セキュリティチームは、ソースコードの品質とセキュリティをレビューします。検証の後、後続のフェーズである自動化プロセスを使用したテストに進みます。
- **ネットワークスキャン** — このスキャンは、アクティブなサービス、開いているポート、環境全体で実行されているアプリケーション、加えてネットワークレベルでの脆弱性の脆弱性を特定するのに役立ちます。
- **外部資産の調査** — 利用可能な最新のツールを継続的に検討し、脆弱性検出機能を強化できると判断した場合には、システムに統合します。
- **お客様からの報告およびチケット** — 当社製品のユーザーによって脆弱性が特定された場合には、連絡を受け入れ、迅速に対応します。
- **バグ修正ポリシー** — 当社には、当社製品のさまざまな重大度のセキュリティ問題を解決するための期間を定義している、文書化されたバグ修正ポリシーがあります。

脆弱性開示プログラム

Varonis は HackerOne と提携し、公開の脆弱性開示プログラム (VDP) を運営しています。当社の VDP は、HackerOne のセキュリティ研究者の大規模なネットワークに対し、当社の資産の評価や、発見した脆弱性を修正のために当社のチームへ報告することを奨励するものです。当社は、新しい脅威を積極的に特定し、当社のお客様、パートナー、供給者、従業員、そして会社全体のセキュリティ向上のために、コミュニティとの関係を育んでいます。当社の脆弱性開示プログラムの詳細については、こちらをご覧ください。

インシデントレスポンス

Varonis には、すべてのセキュリティ関連のイベントやインシデントの一元的な調整と監視 – と対応 – のための構造化された一貫したフレームワークがあります。当社のセキュリティオペレーションセンターは、すべての環境からのイベントを継続的に監視し、ログの関連付けと統合を行い、さまざまな種類のインシデントに対応する自動化され文書化された脚本を作成します。脅威インテリジェンスチームは、外部リソースから積極的に情報を収集します。当社のインシデントレスポンス計画には、疑わしいイベントへの対応やイベントの集約を行うための、以下のような段階的な手順が含まれています:

- 検出と分析
- カテゴリー化
- 封じ込め
- 駆除
- 回復
- 教訓

当社はレッドチームとブルーチームで自社のレスポンス計画を定期的にテストしています。高度な資格と経験を有するセキュリティ専門家とフォレンジック専門家からなる当社のインシデントレスポンスチームは、あらゆるセキュリティインシデントを検出して迅速に対応できるよう訓練されています。

当社のインシデントレスポンス計画には通知ワークフローが含まれています。お客様のデータやテナントがインシデントに巻き込まれた場合には、利害関係者に速やかに通知されます。調査が完了

すると、事後処理会議を開催し、プロセスの改善と今後のインシデント防止について話し合います。

リスク管理とコンプライアンスプログラム

リスク管理プログラム

Varonis には、リスクの特定、分析、コミュニケーションと報告、処置、監視を含んだ、リスク管理方針とプラクティスがあります。各リスクは、潜在的な影響のレベルに基づいて評価され、処置計画は、関連するすべての Varonis の部門による継続的な取り組みとなります。

企業リスク管理プログラム

当社のセキュリティとプライバシーリスク管理プログラムにはいくつかの構成要素があります。企業全体のリスクは、内部監査人が実施し、上級管理職および取締役会の監査委員会に提示される、年次企業リスク評価でカバーされます。CISO は、サイバー脅威を伝え、その後、緩和計画を作成し、それを遂行します。

サイバーリスクアセスメント

当社は、ソフトウェア開発、クラウド本番環境、企業およびクラウドインフラストラクチャーに関する技術的なリスク評価を定期的に実施しています。セキュリティ部門は、実質的なリスクがすべて修正されるまで、そのような取り組みの進捗状況を監視します。CISO と上級管理職は修正計画を提案し、セキュリティ運営委員会が対処計画を決定します。

サードパーティリスク管理

他のすべてのプロセスと同様に、サードパーティの供給者との契約は、セキュリティリスク評価を受けます。Varonis は、ベンダーのセキュリティと態勢を徹底的に審査し、提供能力を有し、固有のセキュリティリスクを認識していることを確かめています。当社は、サードパーティのセキュリティ、コンプライアンス、プライバシー慣行を徹底的に確認することにより、お客様に対して、お客様のデータが保護されていることを保証しています。データを新しいサードパーティと共有するたびに、お客様に通知し、ベンダーリストを更新します。お客様データを保持するリスクの高いサードパーティは、定期的なレビューを受けます。潜在的に PII を開示する各契約は、プライバシー評価と双務的なデータ処理追加条項への署名を必要とします。また、NDA およびセキュリティ契約も必要です。

法律、規制、標準の遵守

Varonis が維持するセキュリティ方針は、当社のすべてのクラウドソリューションを対象としています。当社のコンプライアンスプログラムは、クラウドインフラストラクチャー、ポリシー、基準を業界のベストプラクティスに合わせて更新され、常に進化しています。このコンプライアンスには、また、セキュリティ、プライバシー、コンプライアンス管理策と手順を確実にするための定期的な独立したがイブ監査も含まれます。

Varonis には、さまざまなセキュリティ領域をカバーする 30 種類近くのセキュリティポリシーがあり、ポリシーをさまざまな ISO/IEC 標準（27001、27017、27018、27701）、NIST 800-53、AICPA（米国公認会計士協会）およびその他のプライバシー規制に準拠させています。

規制コンプライアンス認証

Varonis は以下の認証を取得しています。

- **ISO/IEC 27001:2013** は、ISMS の要求事項を規定する最もよく知られている標準規格です。
- **ISO/IEC 27017:2015** は、クラウドサービスの提供と利用に適用される情報セキュリティの管理策のガイドラインを提供します。
- **ISO/IEC 27018:2019** は、ISO/IEC 29100 に記載されているパブリッククラウドのコンピューティング環境のプライバシー原則に従って、共通して受け入れられている管理目標や、管理策、ガイドラインを確立するものです。

- **ISO/IEC 27701:2019** は、プライバシー情報管理システム (PIMS) を確立し、実施し、維持し、継続的に改善するための要求事項を規定しているプライバシー指向の標準規格です。ISO 27701 は、ISO 27001 の条件、管理目標、管理策に基づいています。この標準規格は、セキュリティ管理策とプライバシー管理策を整合させ、カリフォルニア州消費者プライバシー法 (CCPA)、EU 一般データ保護規則 (GDPR)、ニューヨーク州 SHIELD 法など、グローバルなプライバシー標準規格をサポートするための強力な統合ポイントを作成します。
- **SOC 2 タイプ 2** は、セキュリティ、可用性、機密性、プライバシーに関する意見に関するトラストサービスの基準です。
- **CSA Star 認証**は、Varonis が CSA の STAR レベル 1 セキュリティ自己評価を完了したことを証明するものです。
- **Cyber Essentials** は英国政府が支援するプログラムで、一般的なさまざまなサイバー攻撃から組織を保護するのに役立ちます。
- **テキサス州リスクおよび認可管理プログラム (TX-RAMP)** は、テキサス州政府機関にデータを送信するクラウド製品やサービスのセキュリティ対策のレビューを提供するプログラムです。Varonis SaaS と DatAdvantage Cloud は、TX-RAMP からサードパーティによる監査／認証レビューを通じて、暫定認証を取得しました。

当社のポリシープログラムは年次レビュー、改善プロセス、CISO および上級管理職による評価が必要です。従業員は定期的にポリシーを読む必要があります。Varonis のポリシーは社内ポータルで確認することができます。

Varonis におけるプライバシーポリシーとプラクティス

当社はプライバシーに真剣に取り組んでいます。Varonis では、データ保護に関する法律と規制を遵守し、自社のプライバシー情報マネジメントシステム (PIMS) において適切な手順を維持しています。当社のプライバシープログラムは、GDPR や CCPA などのグローバルプライバシー標準に準拠しています。

当社は、当社に提供される個人情報の適切な保護と管理の必要性を認識しています。Varonis には、以下のようなポリシーとプラクティスがあります:

- プライバシーホワイトペーパー
- ソフトウェアプライバシーポリシー

- SaaS のお客様向けのデータ処理に関する追加条項

当社のデータプライバシーに関する主な原則は以下の通りです:

- **データの保持と最小化** – 当社は必要不可欠な情報のみを収集し、必要最小限の期間、保持します。
- **目的の制限** – 当社は、データの処理を、特定された目的に対して適切で、関連性があり、必要とされるものに制限しています。
- **データ処理に関する追加条項** – 関連するすべてのサードパーティデータ処理者は Varonis のポリシーと条件に従わなければなりません。
- **データ主体の権利** – 当社には、関連するすべてのデータ主体からの要求を迅速に処理するためのプロセスがあります。
- **侵害の通知** – 当社のインシデントレスポンスポリシーには、プライバシー侵害ワークフローが含まれており、関連するすべての利害関係者に速やかに通知することを義務付けています。
- **研修** – すべての従業員が、GDPR やその他のプライバシー規制に対する意識向上と遵守のため、当社のプライバシーポリシーおよび手順の研修を受けています。
- **プライバシー評価** – 個人識別情報 (PII) へのアクセス権を持つすべてのサードパーティに対してプライバシー評価を行うこととしています。

データ所在地

オンボーディングプロセスに際して、お客様はテナントの所在地を選択することができます。以下は、Varonis のクラウドオファリングのデータセンターホスティング拠点です。

クラウドオファリング	クラウドホスティングプロバイダー	米国データセンター	欧州データセンター	カナダデータセンター	豪州データセンター
DatAdvantage Cloud	Amazon AWS	米国東部	中央ヨーロッパ		
Varonis SaaS Data Security Platform	Microsoft Azure	米国東部 2	西ヨーロッパ	カナダ中部	豪州東部

内部監査および外部監査

Varonis は、その事業活動を合法的に、コンプライアンス義務に合致する方法で行うことを、約束するとともに実践します。これには、法的義務、規制、セキュリティ方針、知的財産権、記録の保護、情報セキュリティの独立したレビュー、セキュリティポリシーと基準の遵守、契約上の要件、適用されるプライバシー規制、業界標準、および Varonis の社内ポリシー、標準、手順が含まれます。

Varonis は、定期的なセキュリティ評価、ビジネスツールレポート、内部監査や外部監査を含むがこれらに限定されないさまざまな方法で標準への準拠を検証します。

当社は少なくとも年 1 回、有名な監査法人による包括的なセキュリティ監査を実施しています。「高リスク」と見做される分野では追加の内部監査が実施され、Varonis 取締役会の監査委員会に報告されます。監査結果はすべて継続的な改善サイクルに反映し、セキュリティプログラム全体を常に研ぎ澄ますために役立てています。

法執行機関および政府からのデータ要求

Varonis では法務部門を介在させるプロセスが定義されており、法執行機関や政府からのデータの要求に対応しつつ、法律に準拠してお客様の機密を保持することを確実にしています。

Varonis ではお客様のプライバシーを大切にしています

当社は、お客様のデータプライバシーおよび権利の保護に努めています。当社はまた、当社の管理下にあるデータの管理責任者として、データおよびプライバシーの収集、使用、開示を規制する適用されるすべてのデータ保護法を遵守します。

連絡窓口

脆弱性の報告

https://hackerone.com/varonis

セキュリティ問題の報告

soc@varonis.com

プライバシーに関するお問い合わせ

privacy@varonis.com

個人情報の情報処理の中止あるいは削除の要求

dl-privacy-request@varonis.com