OKTA INC.

INFORMATION SECURITY DOCUMENTATION FOR OKTA ACCESS GATEWAY

(last updated August 22, 2024)

Okta's Commitment to Security & Privacy

Okta is committed to achieving and preserving the trust of our customers, by providing a comprehensive security and privacy program that carefully considers data protection matters across our suite of products and services.

This documentation describes the security-related and privacy-related practices that Okta follows for the on-premise Okta Access Gateway software product and software updates or modifications ("Updates") to the foregoing (collectively, the "Software").

- Okta has commissioned a third-party review of the Software's code base, to verify the identity of third-party (including open source) components that are included in the Software. Okta commissions third-party reviews from time to time, as necessary in its discretion, to perform additional reviews of the Software's code base, if and to the extent that the Software is updated.

- If Okta elects to make any Updates available to customers, it may use a third-party platform provider, such as Amazon Web Services, to assist in doing so.

- Prior to being distributed or otherwise made available to customers, any Updates will be scanned to identify and remediate the Open Web Application Security Project's top ten application vulnerabilities, to the extent applicable to the Software. As of the drafting date of this document, those application vulnerabilities include: injection, broken authentication, sensitive data exposure, XML External Entities, broken access control, security misconfigurations, cross-site scripting, insecure deserialization, using components with known vulnerabilities, and insufficient logging and monitoring.

- Okta will perform penetration testing of the Software at least once annually.

Free Trials or Purchased Early Access Services.
Okta's services that are labeled 'Free Trial' or 'Purchased Early Access' may employ lesser or different security measures than those described in this document.

Usage Data.
Okta processes the data derived from the usage of its products and services, including data regarding service configurations and applications utilized in connection with the hosted Service, support data, operational data, log data and the performance results for the hosted Service ("Usage Data"). Okta may process Usage Data as outlined in the Data Processing Addendum ("DPA"), which is publicly available at https://www.okta.com/trustandcompliance, and for legitimate business purposes, such as to: (i) analyze application usage trends; (ii) detect, investigate, and combat fraud and cyber-attacks; (iii) detect, investigate, and combat security incidents, and other such deceptive, fraudulent or malicious behavior against Okta or its customers, including taking measures to improve Okta's overall security posture; (iv) improve service and product functionality; (v) retain and/or employ another service provider or contractor; and (vi) undertake any other specific business purpose authorized by the Customer. Okta may disclose Usage Data publicly and to other entities, and when doing so, will adhere to any applicable confidentiality obligations. Okta may retain, use, and disclose Usage Data in the normal course of business that is (i) deidentified when disclosed; or (ii) disclosed on an aggregated basis; for example, Okta may make available to the public information showing trends about the general use of the hosted service. For clarity, Okta owns Usage Data, which does not include Customer Data.

Language.
The governing language of this documentation is English. Any Japanese language version of this documentation is for reference purposes only. If there is any conflict between the English and Japanese version, the English version shall prevail.

OKTA, INC.

OKTA ACCESS GATEWAY向け情報セキュリティ文書

（最終更新日：2024年8月22日）

Oktaのセキュリティおよびプライバシーへの取り組み

Oktaは、お客様の信頼を獲得し、維持するために尽力するものであり、一連の製品およびサービス全体を通じてデータ保護の問題を慎重に考慮した、包括的なセキュリティおよびプライバシープログラムを提供する。

本文書ではオンプレミスのOkta Access Gatewayソフトウェア製品およびソフトウェア更新または変更（「更新」）の対象である前記ソフトウェア（総称して「ソフトウェア」）のセキュリティ関連およびプライバシー関連の慣行について説明する。

- Oktaはソフトウェアのコードベースのレビューを第三者に委託し、ソフトウェアに含まれる第三者（オープンソースを含む）のアイデンティティを検証している。ソフトウェアが更新される場合に限り、Oktaは必要に応じて独自の裁量で、適宜ソフトウェアのコードベースの追加レビューを第三者に委託する。

- お客様が更新を利用できるようにOktaが選択した場合は、更新作業を支援するために、第三者のプラットフォームプロバイダ、Amazon Web Servicesなどを利用できる。

- 配布または他の方法でお客様が利用できるようにする前に、すべての更新を、Open Web Application Security Project Top 10のアプリケーション脆弱性について、ソフトウェアに該当する範囲で、検証して、修復する。本文書の作成時点で、これらのアプリケーション脆弱性に含まれるのは、インジェクション、不適切な認証、機密データの露出、XML外部エンティティ、不適切なアクセス制御、セキュリティ設定のミス、クロスサイトスクリプティング、安全ではないシリアル化解除、既知の脆弱性を含むコンポーネントの使用、十分ではないログ記録および監視である。

- Oktaは少なくとも年1回、ソフトウェアの侵入テストを実施する。

無料トライアルまたは購入アーリーアクセスサービス。

「無料トライアル」または「購入アーリーアクセス」と表示されているOktaのサービスは、本文書に記載されたセキュリティ措置より劣るまたは異なる措置を採用している場合がある。

使用状況データ。

Okta は、その製品およびサービスの使用から得られるデータを処理する。データには、ホストされたサービスに関連して利用されるサービス構成およびアプリケーションに関するデータ、サポートデータ、運用データ、ログデータ、およびホストされたサービスのパフォーマンス結果 (「使用データ」) が含まれる。Oktaは、https://www.okta.com/trustandcompliance 上に公開されているデータ処理補遺（「DPA」）に概説されている通りおよび次のような正当なビジネスの目的で、使用状況データを処理することができる: (i) アプリケーションの使用傾向を分析する、(ii) 詐欺やサイバー攻撃を検出、調査、および対処する、(iii) セキュリティインシデントおよびその他のOktaまたはそのお客様に対する欺瞞的、詐欺的、または悪意のある行為を検出、調査、および対処する。これにはOktaの全体的なセキュリティ体制を改善するための対策を講じることが含まれる、(iv) サービスおよび製品の機能を改善する、(v) 別のサービスプロバイダーまたは請負業者を維持または雇用する、ならびに (vi) お客様が許可したその他の特定のビジネス目的を遂行する。Oktaは、使用状況データを公開および他の法人に開示することができるが、その場合、適用される守秘義務を遵守する。Oktaは、通常の業務の過程で、(i) 開示の時に匿名化された使用データ、または (ii) 集計ベースで開示される使用データを保持、使用および開示することがある。例えば、ホストされたサービスの一般的な使用状況に関する傾向を示す情報を一般に公開することがある。疑義の無いよう、使用状況データはOktaが所有するものであり、これにはお客様データは含まれない。

言語。

本文書の準拠言語は英語である。本文書の日本語版はすべて参照のみを目的としている。英語版と日本語版との間に矛盾がある場合、英語版が優先される。