



SECURITY & PRIVACY DOCUMENTATION FOR AUTH0

(last updated February 7, 2022)

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, including data submitted by customers to our online service ("Customer Data").

Covered Services

This documentation describes the security-related and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to, the Okta online services branded as Auth0 (collectively, the "Service"). For avoidance of doubt, the Service and this documentation does not apply to Professional Services, Non-Okta Applications, or Free Trial Services made available by Okta.

Architecture, Data Segregation, and Data Processing

The hosted Service is operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The Okta architecture provides an effective logical data separation for different customers via customer-specific "Organization IDs" and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, such as for testing and production.

The Service branded as Auth0 "Private Cloud" is operated in a single-tenant architecture, and if subscriptions for the Auth0 Private Cloud are purchased by the customer, such subscriptions are subject to the "Auth0 Private Cloud Terms" that form part of the customer's applicable Order Form(s).

Okta has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Okta and its sub-processors.

Retrieval of Customer Data

A customer may export Customer Data from the Service at any time during the term of its agreement, using the Service's standard functionality, and Okta's obligations to return Customer Data upon termination of an agreement may be fulfilled by permitting a customer to export Customer Data in this manner. After thirty (30) days following the end of the agreement's term, Okta shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, be entitled to delete all Customer Data by deletion of Customer's unique instance of the Service. Okta will not be required to remove copies of the Customer Data from its backup media and servers until such time as the backup copies are scheduled to be deleted in the normal course of business; provided further that in all cases Okta will continue to protect the Customer Data in accordance with the customer's agreement.

Security Controls

Okta's hosted Service includes a variety of configurable security controls that allow Okta customers to tailor the security of the Service for their own use. Okta strongly encourages all customers, where applicable in their configuration of the Service's security settings, to use the multi-factor authentication features made available by Okta.

Information Security Management Program (“ISMP”)

Okta maintains a comprehensive information security management program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of Okta’s business; (b) the amount of resources available to Okta; (c) the type of information that Okta will store and process; and (d) the need for security and protection from unauthorized disclosure of such Customer Data. The ISMP is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service.

Okta’s ISMP is designed to:

- Protect the integrity, availability, and prevent the unauthorized disclosure by Okta or its agents, of Customer Data in Okta’s possession or control;
- Protect against any anticipated threats or hazards to the integrity, and availability, and prevention of unauthorized disclosure of Customer Data by Okta or its agents;
- Protect against unauthorized access, use, alteration, or destruction of Customer Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Okta may be regulated.

1. **Security Standards.** Okta’s ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes:
 - a) Internal risk assessments;
 - b) ISO 27001 and 27018 certifications;
 - c) NIST guidance; and
 - d) SOC2 Type II (or successor standard) audits annually performed by accredited third-party auditors (“Audit Report”).
2. **Security Audit Report.** Okta provides its customers, upon their request, with a copy of Okta’s then-current Audit Report, including information as to whether the Security Audit revealed any material findings in the Service; and if so, the nature of each finding discovered.
3. **Assigned Security Responsibility.** Okta assigns responsibility for the development, implementation, and maintenance of its Information Security Management Program, including:
 - a) Designating a security official with overall responsibility; and
 - b) Defining security roles and responsibilities for individuals with security responsibilities.
4. **Relationship with Sub-processors.** Okta conducts reasonable due diligence and security assessments of sub-processors engaged by Okta in the storing and/or processing of Customer Data (“Sub-processors”), and enters into agreements with Sub-processors that contain provisions similar or more stringent than those provided for in this security and privacy documentation.
5. **Background Check.** Okta performs background checks on any employees who are to perform material aspects of the Service or have access to Customer Data.
6. **Security Policy, Confidentiality.** Okta requires all personnel to acknowledge in writing, at the time of hire, that they will comply with the ISMP and protect all Customer Data at all times.
7. **Privacy & Security Awareness and Training.** Okta has annual, mandatory privacy awareness and training programs for all Okta personnel that address their obligations related to the processing of personal data that is contained within Customer Data. Okta has annual, mandatory security awareness and training programs for all Okta personnel that address their implementation of and compliance with the ISMP.

8. **Disciplinary Policy and Process.** Okta maintains a disciplinary policy and process in the event Okta personnel violate the ISMP.
9. **Access Controls.** Okta has in place policies, procedures, and logical controls that are designed:
- a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
 - b) To prevent personnel and others who should not have access from obtaining access; and
 - c) To remove access in a timely basis in the event of a change in job responsibilities or job status. Okta institutes:
 - a. Controls to ensure that only those Okta personnel with an actual need-to-know will have access to any Customer Data;
 - b. Controls to ensure that all Okta personnel who are granted access to any Customer Data are based on least-privilege principles;
 - c. Controls to require that user identifiers (User IDs) shall be unique and each shall readily identify the Okta person to whom it is assigned, and no shared or group User IDs shall be used for Okta personnel access to any Customer Data;
 - d. Password and other strong authentication controls that are made available to Okta customers, so that customers can configure the Service to be in compliance with NIST guidance addressing locking out, uniqueness, reset, expiration, termination after a period of inactivity, password reuse limitations, length, expiration, and the number of invalid login requests before locking out a user;
 - e. Periodic (no less than quarterly) access reviews to ensure that only those Okta personnel with access to Customer Data still require it.
10. **Physical and Environmental Security.** Okta maintains controls that provide reasonable assurance that access to physical servers at the production data center is limited to properly-authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include:
- a) Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;
 - b) Camera surveillance systems at critical internal and external entry points to the data center;
 - c) Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and
 - d) Uninterruptible Power Supply (UPS) modules and backup generators that provide back-up power in the event of an electrical failure.
11. **Data Encryption.**
- a) Encryption of Transmitted Data: Okta uses Internet-industry-standard secure encryption methods designed to encrypt communications between its server(s) and the customer browser(s), and between its servers and customer's server(s).
 - b) Encryption of At-Rest Data: Okta uses Internet-industry standard secure encryption methods designed to protect stored Customer Data at rest. Such information is stored on server(s) that are not accessible from the Internet.
 - c) Encryption of Backups: All offsite backups are encrypted. Okta uses disk storage that is encrypted at rest.
12. **Disaster Recovery.** Okta maintains policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain Customer Data. Such procedures include:
- a) Disaster Recovery: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis;

- b) **Business Continuity Plan:** A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

13. Secure Development Practices. Okta adheres to the following development controls:

- a) **Development Policies:** Okta follows secure application development policies, procedures, and standards that are aligned to industry-standard practices, such as the OWASP Top 10 and SANS Top 20 Critical Security Controls; and
- b) **Training:** Okta provides employees responsible for secure application design, development, configuration, testing, and deployment appropriate (based on role) training by the security team regarding Okta's secure application development practices.

14. Malware Control. Okta employs then-current industry-standard measures to test the Service to detect and remediate viruses, Trojan horses, worms, logic bombs, or other harmful code or programs designed to negatively impact the operation or performance of the Service.

15. Data Integrity and Management. Okta maintains policies that ensure the following:

- a) **Segregation of Data:** The Service includes logical controls, including encryption, to segregate each customer's Customer Data from that of other customers; and
- b) **Back Up/Archival:** Okta performs backups of the database(s) containing Customer Data for the Service using industry-standard measures.

16. Vulnerability Management. Okta will implement and maintain a vulnerability management program designed to identify and remediate vulnerabilities affecting networks and production systems for the Service in the form made available by Okta to Customer. Such program will include:

- a) Annual penetration tests conducted by an accredited third party on the Service. Upon Customer's reasonable written request, Okta will provide Customer with an executive summary of the test results, no more than annually. Customer will treat such information as Auth0's confidential information in accordance with the agreement; and
- b) Routine vulnerability scans on all infrastructure components of the Service and applications used by Okta to access Customer Data.

If vulnerabilities are detected from such tests and scans, Okta will remediate and apply applicable and necessary patches as soon as reasonably practicable and in accordance with a documented patching and response policy. Such policy will include factors for determining the scheduling of patches, including criticality of the Okta systems being updated, expected time taken to install the updates (and requirements for service outages, if any), degree of risk associated with any vulnerabilities that are closed by the updates, coordination of the updating of related components of the Service's infrastructure, and dependencies between updates.

17. Change and Configuration Management. Okta maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

- a) A process for documenting, testing and approving the promotion of changes into production;
- b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and
- c) A process for Okta to perform security assessments of changes into production.

18. Secure Deletion. Okta maintains policies and procedures regarding the deletion of Customer Data in compliance with applicable NIST guidance and data protection laws, taking into account available technology so that Customer Data cannot be practicably read or reconstructed. Customer Data submitted to the Service is deleted using techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media

Sanitization”).

- 19. Intrusion Detection & Performance Assurance.** Okta monitors the Service generally for unauthorized intrusions using traffic and activity-based monitoring systems, and may analyze and share data, such as data collected by users’ web browsers (for example, device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) and authentication event data (collectively, “Threat Information”) for security purposes, including to detect compromised browsers and to help customers detect fraudulent authentications, and to ensure that the Service functions properly. For clarity, Threat Information: (1) is only shared if it is derived from evidenced unauthorized attempt(s) to access and/or use the Service; and (2) does not constitute Customer Data.
- 20. Incident Management.** Okta has in place a security incident response plan that includes procedures to be followed in the event of any unauthorized disclosure of Customer Data by Okta or its agents of which Okta becomes aware to the extent permitted by law (such unauthorized disclosure defined herein as a “Security Breach”). The procedures in Okta’s security incident response plan include:
- a) Roles and responsibilities: formation of an internal incident response team with a response leader;
 - b) Investigation: assessing the risk the incident poses and determining who may be affected;
 - c) Communication: internal reporting as well as a notification process in the event of a Security Breach;
 - d) Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and
 - e) Audit: conducting and documenting a root cause analysis and remediation plan.

Okta publishes security bulletin information regarding the Service at <https://auth0.com/docs/security/security-bulletins>. Okta typically notifies customers of significant system incidents by email to the listed contact, and for availability incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and Okta’s response.

21. Security Breach Management.

- a) Notification: In the event of a Security Breach, Okta notifies impacted customers of such Security Breach. Okta cooperates with an impacted customer’s reasonable request for information regarding such Security Breach, and Okta provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.
 - b) Remediation: In the event of a Security Breach, Okta, at its own expense, (i) investigates the actual or suspected Security Breach, (ii) provides any affected customer with a remediation plan, to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents, (iii) remediates the effects of the Security Breach in accordance with such remediation plan, and (iv) reasonably cooperates with any affected customer and any law enforcement or regulatory official investigating such Security Breach.
- 22. Logs.** Okta will regularly log and monitor the details of its personnel’s access to Customer Data submitted to the Service on networks, systems, and devices that are used to provide the Service. Such logs will be maintained by Okta in accordance with its data retention policies.
- 23. Communications with Users.** Separate from and as a complement to the Service, Okta may provide Users access to online communities that provide technical support resources and communicate with Users from time to time, including to send announcements and details about Okta’s products, services, industry events, professional certifications, and other relevant information that Users may find useful. Administrator Users who do not want their organization’s Users to receive such communications may, on behalf of their organizations, update their communications preferences by visiting their Okta Admin console and adjusting the “Okta User Communications” setting.
- 24. Language.** The governing language of this Security and Privacy Documentation is English. Any Japanese language version of this Security and Privacy Documentation is for reference purposes only. If there is any conflict between the English and Japanese version, the English version shall prevail.



Auth0 用セキュリティおよびプライバシーに関する文書

(最終更新日: 2022 年 2 月 7 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、具体的には、一連の製品およびサービス全体を通じて、お客様から Okta のオンラインサービスに送信されたデータ(「お客様データ」)を含む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。

対象サービス

本文書では、各種 Okta オンラインサービスに対するセキュリティ関連およびプライバシー関連の監査と認証、およびその管理上、技術上、および物理上の統制について記載する。ここで言う Okta オンラインサービスとは、Auth0 ブランドとして展開されているサービス(総称して「本サービス」)を指す。疑義の無いよう、本サービスおよび本文書は、Okta が提供するプロフェッショナルサービス、Okta 以外のアプリケーション、または無償トライアルサービスには適用されない。

アーキテクチャ、データ分離、およびデータ処理

本サービスは、ビジネスニーズに基づきお客様データへのアクセスを分離および制限するように設計されたマルチテナントアーキテクチャで運用されている。Okta アーキテクチャはお客様固有の「組織 ID」を介して、様々なお客様に効果的な論理データの分離を行い、お客様およびそのユーザーのロールベースのアクセス権限を使用可能にしている。テストや本番環境など、さまざまな機能ごとに個別の環境を提供することにより、追加のデータ分離が確保されている。

Auth0 「プライベートクラウド」ブランドの本サービスは、シングルテナントアーキテクチャで運用されており、お客様が Auth0 プライベートクラウドのサブスクリプションを購入された場合、かかるサブスクリプションにはお客様に該当する注文書の一部を構成する「Auth0 プラットフォーム上のプライベートクラウド条件」が適用される。

Okta は、Okta およびその復処理者による処理業務のチェーン全体を通じ、お客様データがお客様の指示に従ってのみ処理されるよう設計する手順を実装した。

お客様データの取得

お客様は、その契約期間中いつでも、本サービスの標準機能を使用して、お客様データを本サービスからエクスポートすることができる。契約の終了時に Okta がお客様データを返還する義務は、かかる態様によりお客様がお客様データをエクスポートできるようにすることをもって、履行したことになる。契約期間終了から 30 日経過後、Okta はお客様データを維持または提供する義務を負わないものとし、その後は法的に禁止されていない限り、お客様の利用するサービスの一意のインスタンスを削除することで、すべてのお客様データを削除する権利を有する。Okta は、通常業務の過程でバックアップコピーが削除される予定の期日になるまで、バックアップメディアとサーバーからお客様データのコピーを削除する必要はない。ただし、いかなる場合も、Okta が引き続き、お客様との契約に従ってお客様データを保護することを条件とする。

セキュリティ管理

Okta のホステッドサービスには、Okta のお客様が自社用途に合わせてサービスのセキュリティを調整できるよう、設定可能な各種のセキュリティ制御が含まれている。Okta はすべてのお客様に、サービスのセキュリティ設定の構成において該当する場合、Okta が提供する多要素認証機能を使用することを強く奨励している。

情報セキュリティ管理プログラム(「ISMP」)

Okta は、以下に対して適切な管理的、技術的、および物理的な保護手段を定める、包括的な情報セキュリティ管理プログラムを維持している。(a) Okta の事業の規模、範囲、および種類、(b) Okta が利用できるリソースの量、(c) Okta が保存および処理する情報の種類、(d) お客様データの不正開示が起きないように、セキュリティと保護の必要性。ISMP は文書化され、プライバシーとデータセキュリティの慣行および本サービスに適用される業界標準に関連する法律上および規制上の要件の変更に基づき、更新されている。

Okta の ISMP は、次の目的で設計されている：

- 完全性、可用性を保護し、Okta またはその代理人による、Okta が所有または管理しているお客様データの不正開示を防止すること
- 完全性と可用性に対して予想される脅威や危険から保護すること、および Okta またはその代理人によるお客様データの不正開示を防止すること
- お客様データを不正アクセス、使用、変更、または破壊から保護すること
- お客様データの偶発的な損失や破壊、または損傷から保護すること、および
- Okta が規制を受ける可能性のある地方、州、または連邦の規制に定めるとおり情報を防御すること。

1. **セキュリティ基準** Okta の ISMP には、ISMP の主要な制御、システム、および手順の遵守と定期的な検査が含まれている。これにより、主要な制御、システム、および手順が適切に実装され、特定された脅威とリスクに対処する際に効果的であることを検証している。かかる検査には次のものが含まれる：

- a) 内部リスク評価
- b) ISO 27001 および 27018 認証
- c) NIST ガイダンス
- d) 認定された第三者監査人によって毎年実施される SOC2 Type II (または後継規格) 監査(「監査報告書」)

2. **セキュリティ監査報告書** Okta はお客様の要求に応じて、セキュリティ監査により、本サービスの重要な指摘事項が判明したか否か、判明した場合は、その指摘事項の性質に関する情報を含む、Okta のその時点における最新の監査報告書のコピーを提供する。

3. **セキュリティ上の責任の割り当て** Okta は、以下を含む同社の情報セキュリティ管理プログラムの開発、実装、および保守のための責任を割り当てる：

- a) 全体的な責任を担うセキュリティ担当者を指名、および
- b) セキュリティの責任を担う個人のセキュリティの役割と責任を定義。

4. **復処理者との関係** Okta は、お客様データの保存や処理に対して Okta が採用する復処理者(「復処理者」)について、合理的なデューデリジェンスとセキュリティ評価を実施し、また、復処理者とは、本セキュリティおよびプライバシーに関する文書で規定されているものと同様またはより厳格な規定が含まれた契約を締結している。

5. **身元調査** Okta は、本サービスの重要な側面を実行する、またはお客様データにアクセスできる従業員の身元調査を行っている。
6. **セキュリティ方針、機密保持** Okta は、すべての人員に対して、採用時点で常に ISMP に準拠すること、およびすべてのお客様データを保護することを書面で確約することを求めている。
7. **プライバシーおよびセキュリティの意識向上とトレーニング** Okta には、お客様データに含まれる個人データの処理に関連する義務に関するすべての Okta の人員を対象とした、年1回の必須のプライバシー意識向上およびトレーニングがある。Okta には、ISMP の実装とコンプライアンスに対応するすべての Okta の人員を対象とした、年1回の必須のセキュリティ意識向上およびトレーニングプログラムがある。
8. **懲戒方針とプロセス** Okta は、Okta の人員が ISMP に違反した場合の懲戒方針とプロセスを維持している。
9. **アクセス制御** Okta には、以下のために設計された方針、手順、および論理的制御を設けている：
 - a) 適切な許可を得た人のみに、Okta の情報システムおよびそれを収容する、施設へのアクセスを制限すること
 - b) アクセスすべきでない人員によるアクセスの取得を防止すること、および
 - c) 職責または職位が変更された場合に、タイムリーにアクセスを削除すること。

Okta は、以下を制定する：

- a. いかなるお客様データにも、実際に知る必要のある Okta 担当者のみがアクセスできる状態を確保するための制御
 - b. お客様データへのアクセスを許可されているすべての Okta 担当者が、最小権限の原則に基づいている状態を確保するための管理
 - c. ユーザー識別子(ユーザーID)が一意であり、それぞれが割り当てられている Okta の人物を容易に特定できること、かつ Okta の担当者がお客様データにアクセスするために使用される共有またはグループのユーザーIDがないことを要求する制御
 - d. ロックアウト、一意性、リセット、有効期限、非アクティブ期間後の終了、パスワード再利用の制限、パスワードの長さ、パスワードの有効期限、およびユーザーのロックアウトに紐づく無効なログイン要求の回数に対応する NIST ガイドランスに準拠するためにお客様が本サービスを設定できるよう、Okta のお客様が利用できるパスワードおよびその他の強力な認証制御
 - e. お客様データにアクセスする必要が依然としてある Okta の担当者のみがアクセスできる状態を確保するための、定期的な(最低でも四半期ごとの)アクセスレビュー。
10. **物理的および環境的なセキュリティ** Okta は、本番データセンターでの物理サーバーへのアクセスが、適切な許可を得た個人に限定され、かつ極端な環境による破壊を検出、防止、制御するための環境管理が確立されている合理的な確証を提供する制御を維持している。こうした制御には、次のものが含まれる：
 - a) データセンターのセキュリティ担当者によるデータセンターへの不正アクセス試行のログ記録と監視
 - b) データセンターへの重要な内部および外部エントリポイントでのカメラ監視システム
 - c) 電子機器に適切な水準で気温と湿度を監視および制御するシステム、および
 - d) 電氣的故障の場合バックアップ電源を提供する、無停電電源装置(UPS)モジュールおよびバックアップ発電機。

11. データ暗号化

- a) 送信データの暗号化: Okta は、同社サーバーとお客様ブラウザとの間、および同社サーバーとお客様サーバーとの間での通信を暗号化するために設計された、インターネット業界標準の安全な暗号化方式を使用している。
- b) 保存データの暗号化: Okta は、保管されたお客様データを保護するよう設計された、インターネット業界標準の安全な暗号化方式を使用している。かかる情報は、インターネットからはアクセスできないサーバーに保存される。
- c) バックアップの暗号化: すべてのオフサイトバックアップは暗号化されている。Okta は、休止時に暗号化されるディスクストレージを使用している。

12. 災害からの復旧

Okta は、お客様データまたはお客様データを含む本番システムに損害を及ぼす恐れのある緊急事態または不可抗力事象に対応するための方針と手順を維持している。その手順は以下を含む:

- a) 災害からの復旧: サービスの中断を最小限に抑えるように設計された、本番環境用の正式な災害復旧計画で、これには定期的に災害計画をテストする要件が含まれる。
- b) BCP(事業継続計画): 重要なリソースの損失を最小限に抑える手段として、計画外の事象を管理するための枠組みに対処する正式なプロセスである。

13. 安全な開発手法

Okta は、次の開発管理を遵守している:

- a) 開発方針: Okta は、OWASP Top 10 や SANS Top 20 Critical Security Controls などの、業界標準に沿った安全なアプリケーション開発方針、手順、標準に従う。
- b) トレーニング: Okta は、安全なアプリケーションの設計、開発、構成、テスト、および導入を担当する従業員に、Okta の安全なアプリケーション開発手法に関して、セキュリティチームによる適切な(役割に基づく)トレーニングを提供する。

14. マルウェア制御

Okta は、その時点で最新の業界標準の対策を採用して、ウイルス、トロイの木馬、ワーム、論理爆弾、その他の本サービスの運用またはパフォーマンスに悪影響を与えるよう設計されている有害なコードやプログラムを検出して修復する本サービスのテストを行っている。

15. データの完全性と管理

Okta は、以下を確保する方針を維持している:

- a) データの分離: 本サービスには、各お客様のお客様データを他のお客様のデータから分離する暗号化を含む論理制御が含まれている、および
- b) バックアップ/アーカイブ: Okta は、お客様データを含む本サービス用のデータベースのバックアップを業界標準措置により実行している。

16. 脆弱性管理

Okta は、本サービスのネットワークおよび本番システムに影響を与える脆弱性を特定および修正するために設計された脆弱性管理プログラムを、Okta がお客様に提供する形で実施および維持する。かかるプログラムは、以下を含む。

- a) 認定された第三者によって本サービスに対して実施される年 1 回のペネトレーションテスト。お客様の合理的な書面による要請があった場合、Okta はお客様にテスト結果の要旨(年 1 回を上限とする)を提供する。お客様は、かかる情報を本契約に従って Auth0 の機密情報として取り扱うものとする。および

b) Okta がお客様データにアクセスするために使用する本サービスのすべてのインフラコンポーネントおよびアプリケーションに対する定期的な脆弱性スキャン。

かかるテストおよびスキャンから脆弱性が検出された場合、Okta は、可及的速やかに、文書化されたパッチおよびレスポンスポリシーに従って修正し、適用すべき必要なパッチを適用する。かかるポリシーには、更新される Okta システムの重要性、更新のインストールにかかる予想時間（およびサービス停止がある場合はその要件）、更新によって閉じられる脆弱性に関連するリスクの程度、サービスのインフラの関連コンポーネントの更新の調整、および更新間の依存関係など、パッチのスケジュールを決定するための要因が含まれる。

17. 変更および構成管理 Okta は本番システム、アプリケーション、およびデータベースへの変更を管理するための方針と手順を維持している。そうした方針と手順には、次のものが含まれる：

- a) 本番環境への変更の反映を文書化、テスト、承認するプロセス
- b) リスク分析に基づき適時にシステムにパッチを適用する必要があるセキュリティパッチ適用プロセス、および
- c) Okta が本番環境に行う変更のセキュリティ評価を実行するためのプロセス

18. 安全な削除 Okta は、お客様データの削除についての方針と手順を維持している。この方針と手順は、適用される NIST ガイドランスおよびデータ保護法に準拠して、利用可能な技術を考慮し、お客様データを実現可能な限り読み取ったり再構築したりできないようにする。本サービスに入力されたお客様データは、DoD 5220.22-M 国家産業保全プログラム運用マニュアル (“National Industrial Security Program Operating Manual”) または NIST SP800-88 (記憶媒体のサニタイズに関するガイドライン) に詳述される方法を用いて削除される。

19. 侵入検知および性能保証 Okta は、トラフィックおよびアクティビティベースの監視システムを使用し、本サービス全般に不正侵入がないか否かを監視し、セキュリティ保護の目的で、ユーザーのウェブブラウザによって収集されたデータ (例えば、デバイスの種類、画面解像度、タイムゾーン、オペレーティングシステムのバージョン、ブラウザの種類とバージョン、システムフォント、インストールされているブラウザプラグイン、有効な MIME タイプなど) および認証イベントデータ (総称して、「脅威情報」) を分析しデータを共有する場合がある。この目的には、侵入に利用されたブラウザの検出およびお客様が不正な認証を検出し、サービスが適切に機能することを確保することが含まれる。疑義の無いよう、脅威情報は、(1)本サービスへのアクセスまたはその使用の明らかに不正な試みから生じた場合にのみ共有され、および(2)お客様データを構成するものではない。

20. インシデント管理 Okta は、Okta または Okta の代理人によるお客様データの不正開示が発生した場合に、法律で許可されている範囲で従うべき手順を含むセキュリティインシデント対応計画を策定している (本書では、かかる不正な開示は「セキュリティ違反」とする)。Okta のセキュリティインシデント対応計画の手順は次のとおりである：

- a) 役割と責任: 対応リーダーを筆頭とする内部インシデント対応チームの編成
- b) 調査: インシデントがもたらすリスクを評価し、影響を受ける可能性のある人を判断
- c) コミュニケーション: セキュリティ違反が発生した場合の内部報告と通知プロセス
- d) 記録管理: 実施したこと、および誰がそれを実施したのかをその後の分析を支援するために記録
- e) 監査: 根本原因の分析と修復計画の実施と文書化

Okta は、Okta は、本サービスに関するセキュリティ情報のお知らせを <https://auth0.com/docs/security/security-bulletins> で公開している。Okta は通常、重大なシステムインシデントについて、リストされている連絡先へ電子メールによりお客様に通知する。また、可用性インシデントが 1 時間を超えて継続する場合、影響を受けるお客様を、インシデントおよび Okta の対応について説明する電話会議に参加するよう招待することがある。

21. セキュリティ違反管理

- a) **通知:** セキュリティ違反が発生した場合、Okta は、影響を受けるお客様にかかるセキュリティ違反を通知する。Okta は、影響を受けるお客様からのかかるセキュリティ違反に関する合理的な情報要求に協力し、かつ Okta は、かかるセキュリティ違反、および講じた調査措置や是正措置について、定期的に最新情報を提供する。
- b) **救済措置:** セキュリティ違反が発生した場合、Okta は自費で以下を行う。(i) 実際のまたは疑わしいセキュリティ違反を調査する、(ii) 影響を受けるお客様に、セキュリティ違反に対処し、インシデントの影響を軽減し、それ以上のインシデントを合理的に防止する修復計画を提出する、(iii) セキュリティ違反の影響をかかるとして修復計画に従って修正する、(iv) 影響を受けるお客様、およびかかるセキュリティ違反の捜査に当たる法執行機関または規制当局と合理的に協力する。

22. **ログ** Okta は、本サービスを提供するために使用されるネットワーク、システム、およびデバイス上で、本サービスに力されたお客様データへの社員によるアクセスの詳細を定期的に記録し、監視します。かかるログは、Okta のデータ保持ポリシーに従って Okta によって保持されます。

23. **ユーザーとの連絡** 本サービスとは別に、これを補完するものとして、Okta はユーザーにオンラインコミュニティへのアクセスを付与することがあり、これによりテクニカルサポートリソースを提供し、Okta 製品、サービス、業界イベント、プロフェッショナル認定、およびユーザーに役立つと思われるその他の関連情報の告知および詳細を含む、ユーザーへの連絡を適宜取ることがあります。組織のユーザーがそのような連絡を受けることを希望しないアドミニストレータユーザーは、その組織を代表して、Okta アドミンコンソールに行き、「Okta ユーザーコミュニケーション」設定を調整することによりコミュニケーションの選択を更新することができる。

24. **言語** 本セキュリティおよびプライバシーに関する文書の準拠言語は英語である。本セキュリティおよびプライバシーに関する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。