OKTA INC.

INFORMATION SECURITY DOCUMENTATION FOR OKTA COMMERCIAL SERVICES

(Last updated August 22, 2024)

1. Okta's Commitment to Security.

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

2. 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.

3. Covered Services.

This documentation describes the security controls and assurances that Okta has in place with respect to Okta's online services branded as Single Sign-On, Adaptive Single Sign-On, Multi-Factor Authentication, Adaptive Multi-Factor Authentication, Mobility Management, Lifecycle Management, Universal Directory, API Access Management, Directory Integration, Inbound Federation, Workflows, Advanced Server Access, Social Authentication, Okta Identity Governance, Okta Privileged Access, Customer Identity Cloud (formerly branded as "Auth0"), Fine Grained Authorization, and Okta Device Access (collectively, the "Service"). For avoidance of doubt, this documentation does not apply to Professional Services, Non-Okta Applications, Free Trials, or Limited Early Access or Early Access Subscriptions made available by Okta, and as such terms are defined in Okta's Master Subscription Agreement, available online at okta.com/agreements. The controls and assurances described herein are designed to ensure the integrity, confidentiality, and availability of all electronic data submitted by customers or on behalf of a customer to the Service ("Customer Data").

4. Service Architecture, Data Segregation & Data Processing.

The Service operates in a multitenant architecture that is designed to segregate Customer Data and restrict access to Customer Data based on business needs. The Okta architecture provides an effective logical separation of Customer Data for different customers via customer-specific "Organization[1] IDs," and allows for role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, such as for testing and production.

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.

5. Retrieval of Customer Data.[2]

Upon written request by a customer made prior to the effective date of termination or expiration of the customer's agreement, Okta will make available to the customer, at no cost, for thirty (30) days following the end of the agreement's term, for download a file of Customer Data (other than personal confidential information such as, but not limited to, User passwords which may not be included except in hashed format) in industry-standard format (e.g. and without limitation, .json or .csv). After such 30-day period, 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 expunging Customer's unique instance of the Service. During the term of the agreement, Customer may extract Customer Data from the Service in accordance with applicable Documentation.

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.

6. Secure Deletion of Customer Data.

Okta maintains policies and procedures regarding the deletion of Customer Data, taking into account available technology, so that Customer Data cannot be practically read or reconstructed. Customer Data is deleted using secure deletion methods materially in accordance with

---

[1] "Organization" may also be known as a "Tenant" (for Customer Identity Cloud) or "Team" (for Okta Privileged Access).

[2] For information related to flows, tables, execution data and history in Workflows, please refer to the Workflows help pages, located at: https://help.okta.com/wf/en-us/content/topics/workflows/workflows-main.htm.

applicable NIST guidelines.

7. Customer-Configurable 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 personnel will not set a defined password for a User. Each customer's Users are provided with a token that they can use to set their own password in accordance with the applicable customer's password policy. 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.

8. Information Security Policy ("ISP").

Okta maintains and implements a comprehensive information security management policy that establishes 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 ISP is reviewed annually, and may be updated if necessary, based on changes in legal and regulatory requirements related to data security practices and industry standards applicable to the Service.

9. Security Certifications.[3]

Okta maintains the following certifications, confirmation of which is available upon a customer's written request:

- ISO 27001, 27017, 27018
- CSA STAR Attestation (Level 2)

10. Security Audit Report.[4]

Okta will provide a customer, upon its written request, with a copy of Okta's then-current SOC2 Type II (or successor standard) Report which will be issued at least annually by an accredited third-party auditor, including information as to whether the audit revealed any material findings regarding the Service, and if so, the nature of each finding discovered.

11. Assigned Security Responsibility.

Okta assigns responsibility for the development, implementation, and maintenance of its security operations, including:

a) Designating a security official with overall responsibility; and

b) Defining roles and responsibilities for individuals with security obligations.

12. Relationship with Sub-processors.

Okta conducts reasonable due diligence and security assessments of sub-processors engaged by Okta to store and/or process Customer Data ("Sub-processors"). Okta's Sub-processors agree to similar or more stringent controls as those provided for in this Information Security Documentation.

13. Background Checks.

Okta performs background checks on any employees who are to perform material aspects of the Service or have access to Customer Data. Where permitted under applicable law, background checks are also performed annually for employees with access to highly-sensitive information.

14. Security Awareness and Training.

All Okta employees must acknowledge in writing that they will comply with the ISP and protect Customer Data. For all of its employees, Okta mandates annual security awareness training programs that address their obligations related to the processing of personal data contained within Customer Data, as well as the implementation of and compliance with the ISP.

15. Identity and Access Management.

Okta has in place access management policies and procedures that are designed:

a) To limit access to its information systems and the facilities in which they are housed to properly-authorized persons;

[3] Customer Identity Cloud and Fine Grained Authorization currently do not have, but are in the process of acquiring, these certifications.
[4] Fine Grained Authorization and Okta Privileged Access currently do not have, but are in the process of acquiring, SOC2 Type II reports.

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 the following identity management controls:

a) Provisioning Okta personnel with access to Customer Data based on need-to-know criteria and the least-privilege principle;

b) Requirements that User identifiers (i.e., User IDs) be unique and readily identifiable to the Okta personnel to whom they are assigned, and no shared or group User IDs be used by Okta personnel for access to any Customer Data;

c) Password and other strong authentication controls, including addressing the number of invalid login requests before locking out, uniqueness, reset, termination after a period of inactivity, password reuse limitations, length, and expiration;

d) Periodic (no less than quarterly) reviews to ensure that those Okta personnel who have access to Customer Data still require access.

16. Physical and Environmental Security.

Okta maintains controls that provide reasonable assurance that access to Customer Data, at the production data center and other Okta-managed facilities, 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 maintain 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.

17. Data Encryption.

Okta uses strong encryption to protect Customer Data in-transit and at-rest. Customer Data at-rest is stored on environment(s) that are not accessible from the internet. Encrypted solutions and environments are utilized to protect all backups.

18. Business Continuity and Disaster Recovery.

Okta maintains policies and procedures for responding to an emergency or a force majeure event that causes or could cause Okta's infrastructure to experience a total, or unacceptably degraded, loss of service ("**DR/BC Event**"). Such procedures include:

a) Data Backups: A policy and process for performing periodic backups of production file systems and databases to meet the RPO and RTO, each from the time when a decision to restore backups is made, described below:

i. Recovery Point Objective ("**RPO**") is no more than 1 hour *(for CIC Private Cloud, the RPO is no more than 6 hours)*;

ii. Recovery Time Objective ("**RTO**") is no more than 24 hours to restoration of the full Service.

b) Business Continuity Plan ("**BCP**"): A formal process to address how a DR/BC Event that disrupts Okta's non-Service functions (i.e., corporate processes) might be managed in order to minimize loss of vital resources. The BCP, a copy of which is made available to a customer upon written request, is tested annually.

c) Disaster Recovery Plan ("**DRP**"): A formal process for the production environment that addresses how a DR/BC Event that disrupts Okta's Service might be managed to minimize loss of operations. The DRP includes requirements for testing on a regular basis, currently four times a year. Confirmation of such testing is available to a customer upon written request.

19. 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 / CIS Critical Security Controls;

b) Training: Okta provides employees responsible for secure application design, development, configuration, testing, and deployment the appropriate (based on role) technical training, on an annual basis, by the security team regarding secure

application development practices; and

c) Hardening of workstations used to develop the Service in alignment with US Government-approved frameworks.

20. 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.

21. Data Integrity and Management.

In addition to the data segregation measures described in Section 4 of this document, Okta maintains policies that ensure the following:

a) Back Up/Archival: Okta maintains full backups of the database(s) containing Customer Data as required to maintain the RPO on secure server(s) or on other commercially acceptable secure media; and

b) Data Integrity Checks: Okta implements automated and manual processes to ensure input and output integrity of Customer Data.

22. Vulnerability Management.

Okta performs quarterly vulnerability scans on its (1) applications and (2) infrastructure components of its production and development environments. For applications, scans are also performed after any major feature changes or architectural modifications to the Service. Vulnerabilities are ranked using the Common Vulnerability Scoring System, and remediated on a risk basis that considers the types of applications and infrastructure systems on which they are found. Okta installs medium, high, and critical security patches for all components in its production and development environments as soon as commercially reasonable.

23. Penetration Testing.

Okta engages third parties to conduct annual penetration tests of the Service and issue a report of their findings, including confirmation that past findings have been remediated ("**Testing Report**"). Reports from Okta's then-current Testing Report, together with applicable remediation plans, are available to a customer upon its written request. Additionally, Okta's internal penetration testers regularly perform tests of the Service's production infrastructure and application source code.

Customer may, after signing a Penetration Testing Agreement provided by Okta, conduct its own penetration testing of a separate, fully-functioning Okta environment that simulates a distinct customer organization.

24. 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.

25. Intrusion Detection & Performance Assurance.

Okta implements intrusion, detection, and prevention controls to monitor 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.

26. Availability Incident Management.

System status information about the Service is available on the Okta Trust website, at https://trust.okta.com. Okta typically notifies customers of significant system incidents by email to the listed admin 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.

27. Security Breach Management.

a) Incident Response Plan: Okta has in place a security incident response plan ("IRP") that includes procedures to be followed in the event of any breach of security that causes the unlawful or accidental destruction, alteration or damage or loss, unauthorized

disclosure of, or access to, Customer Data, transmitted, stored or otherwise processed by Okta or its Sub-processors, of which Okta becomes aware ("Security Breach"). Okta's IRP addresses the following areas:

i. Roles and responsibilities: formation of an internal incident response team with a response leader;

ii. Investigation: assessing the risk the incident poses and determining who may be affected;

iii. Communication: internal reporting as well as a notification process in the event of a Security Breach;

iv. Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and

v. Audit: conducting and documenting a root cause analysis and remediation plan.

b) Notification: Upon its confirmation of a Security Breach, Okta notifies impacted customers to the extent permitted by applicable law, law enforcement directive or regulatory request. Notice shall be sent to the Security Contact that a customer designates in the Okta Admin Console, or, when a Security Contact is not designated, in accordance with the "Notices" section of an impacted customer's agreement. 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.

c) Remediation: In the event of a Security Breach, Okta shall, at its own expense, (i) investigate the actual or suspected Security Breach, (ii) provide any affected customer with a remediation plan to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents, (iii) remediate the effects of the Security Breach in accordance with such remediation plan, and (iv) reasonably cooperate with any affected customer and any law enforcement or regulatory official investigating such Security Breach.

28. Logs.[5]

Okta records activity in information systems containing or use electronic information, such as logins, connection attempts, privileged User access and actions, along with the source, date, time, and other relevant information for such activities. Okta (i) backs-up logs daily, (ii) implements commercially reasonable measures to protect such logs from unauthorized modification or erasure, and (iii) retains such logs in compliance with Okta's data retention policy. If there is suspicion of inappropriate access to the online Service, Okta may have the ability to provide customers log entry records to assist in forensic analysis. This service, if made available, will be provided to customers on a time-and-materials basis. A customer may access its own organization's system logs via the Okta Admin Console within the Service.

29. 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.

30. 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.

31. 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.

[5] This section does not apply to Okta Device Access when used offline, as logs can neither be configured nor stored.

OKTA, INC.

OKTAコマーシャルサービス向け

情報セキュリティ文書

（最終更新日：2024年8月22日）

1. Oktaのセキュリティへの取り組み

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、包括的な情報セキュリティプログラムを提供する。

2. 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。

3. 対象サービス

本文書では、Oktaの各種オンラインサービスに関するセキュリティ統制および確約について記載する。ここで言うOktaオンラインサービスとは、シングルサインオン、アダプティブシングルサインオン、多要素認証、アダプティブ多要素認証、モビリティ管理、ライフサイクル管理、ユニバーサルディレクトリ、APIアクセス管理、ディレクトリ統合、インバウンドフェデレーション、Workflows、Advanced Server Access、ソーシャル認証、Okta Identity Governance、Okta Privileged Access、Customer Identity Cloud（かつての「Auth0」ブランド）、Fine Grained Authorization、およびOkta Device Access としてそれぞれで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、本文書は、Oktaが提供するプロフェッショナルサービス、非Oktaアプリケーション、無料トライアルまたは限定アーリーアクセス、またはアーリーアクセスサブスクリプションには適用されない。これらに適用される条件は、オンラインでhttps://okta.com/agreements上で提供されているOktaのマスターサブスクリプション契約に規定されている。ここに記載されている統制および確約は、お客様がまたはお客様に代わって本サービスに入力したすべての電子データ（以下「お客様データ」）の完全性、機密性、および可用性を確保するために設計されている。

4. サービスアーキテクチャ、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、お客様データを分離し、お客様データへのアクセスを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[1] ID」を介して、様々なお客様に効果的なお客様データ論理的分離を行い、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、様々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。

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。

5. お客様データの取得[2]

お客様との契約の解約または期間満了の発効日より前に行われたお客様からの書面による要求に応じて、Oktaは、契約期間終了から30日間、お客様が無料で（ハッシュ形式によるもの以外に含めることができないユーザーパスワードなどを含むがこれらに限定されない、個人の機密情報を除く）お客様データのファイルを、業界標準形式（これらに限定されない例、.jsonまたは.csv）でダウンロードできるようにする。かかる30日間の経過後、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消去することで、すべてのお客様データを削除する権利を有する。契約期間中、お客様は、適用される関連文書に従って、本サービスからお客様データを抽出することができる。

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

---

[1]「組織」とは、「テナント」（Customer Identity Cloudの場合）または「チーム」（Okta Privileged Accessの場合）である。

[2]Workflowsにおけるフロー、テーブル、実行データおよび履歴の詳細については、Workflowsヘルプページ（https://help.okta.com/wf/ja-jp/content/topics/workflows/workflows-main.htm）を参照。

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。

6. お客様データの安全な削除

Oktaは、利用可能な技術を考慮し、お客様データの削除に関するポリシーおよび手順を維持しており、これによりお客様データが実際的に読み取りまたは再構築することができないようにしている。お客様データは、適用されるNISTガイドラインに実質的に従った安全な削除方法を用いて削除される。

7. お客様による設定可能なセキュリティ管理

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の人員がユーザーのために事前定義されたパスワードを設定することはない。お客様の各ユーザーにはお客様のパスワードポリシーに従った、独自のパスワードを設定できるトークンが提供される。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。

8. 情報セキュリティポリシー（「ISP」）

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確立する、包括的な情報セキュリティ管理ポリシーを維持し、これを実施している。(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、セキュリティと保護の必要性。ISPは毎年見直され、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、必要に応じて更新されることがある。

9. セキュリティ認証[3]

Oktaは、以下の認証、確認を維持しており、お客様からの書面による要求に応じて提供することができる：

- ISO 27001、27017、27018
- CSA STAR 認証（レベル2）

10. セキュリティ監査報告書[4]

Oktaは、お客様からの書面による要求に応じて、その時点で最新のOktaのSOC2 Type II（または後継基準）報告書のコピーを提供する。かかる報告書は認定された第三者監査人により最低年1回発行され、これには監査により、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が含まれる。

11. セキュリティ上の責任の割り当て

Oktaは、以下を含む同社のセキュリティ運用の開発、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) セキュリティの義務を負う個人の役割と責任を定義。

12. 復処理者との関係

Oktaはお客様データを保存し処理するために、Oktaが利用する復処理者（「復処理者」）に対して合理的なデューデリジェンスおよびセキュリティ評価を実行する。Oktaの復処理者は、本情報セキュリティ文書に記載されるものと同等または厳格な統制に合意している。

13. 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。また、適用される法令で認められている場合、機密性の高い情報にアクセスできる従業員については、毎年身元調査を実施している。

---

[3]Customer Identity CloudおよびFine Grained Authorizationは、現在これらの認証を取得していないが、取得のプロセスを進めている。
[4]Fine Grained AuthorizationおよびOkta Privileged Accessについては現在SOC2 Type II報告書は無いが、その取得を進めている。

14. セキュリティの意識向上およびトレーニング

Oktaのすべての従業員は、ISPを遵守すること、およびお客様データを保護することを書面で確約しなくてはならない。Oktaは、そのすべての従業員に、お客様データに含まれる個人データの処理に関連する責任およびISPの実施および遵守に関するOktaの全従業員を対象とした、年1回の必須のセキュリティ意識向上トレーニングを義務付けている。

15. アイデンティティおよびアクセス制御

Oktaには、以下のために設計されたアクセス管理方針および手順を設けている:

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、以下のアイデンティティ管理統制を設けている:

a) 知る必要があるという基準および最小権限の原則に基づいて、Okta人員にお客様データへのアクセスを付与する

b) ユーザー識別子(すなわち、ユーザーID)が一意であり、それが割り当てられているOkta担当者が容易に特定できること、かつOkta担当者がお客様データにアクセスするために共有またはグループのユーザーIDを用いないとする要件

c) ロックアウトまでの無効なログイン要求の回数、一意性、リセット、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、およびパスワードの有効期限を含むパスワードおよびその他の強力な認証制御

d) お客様データにアクセスできるOkta担当者が依然としてアクセスを必要としていることを確保するための、定期的な(最低、四半期ごとの)調査。

16. **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およびその他Oktaが管理する施設でのお客様データへのアクセスが、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維持するシステム、および

d) 電気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。

17. **データ暗号化**

Oktaは、強力な暗号化を使用することにより送信中および保存されているお客様データを保護している。保存されているお客様データはインターネットからアクセスすることができない環境に保管されている。すべてのバックアップの保護に暗号化ソリューションおよび環境を利用している。

18. 事業継続および災害からの復旧

Oktaは、Oktaのインフラストラクチャに完全な、または許容できないほど劣化したサービスの喪失を引き起こす、または引き起こす可能性のある緊急事態または不可抗事象(「**DR/BCイベント**」)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) データのバックアップ: 以下に説明される、バックアップの復元を決定した時点からの、RPOおよびRTOを満たすため、本番ファイルシステムとデータベースの定期的なバックアップを実行する方針および手順。

i. 目標復旧ポイント(「**RPO**」)1時間以内 *(CIC Private Cloudでは、RPOは6時間以内)*、

ii. 本サービスの完全な復旧までの目標復旧時間(「**RTO**」)は24時間以内。

b) 事業継続計画(「**BCP**」): 重要なリソースの損失を最小限に抑えるために、Oktaの本サービス外の機能(すなわち、企業内プロセス)を中断させるDR/BCイベントを、どのように管理するかという正式なプロセス。お客様の書面による要請に応じてコピーが提供される、BCPは毎年テストされる。

c) 災害からの復旧計画(「**DRP**」): Oktaの本サービスに支障をきたすDR/BCイベントが発生した場合、運用の喪失を最小限に抑えるためにどのように管理するかという、本番環境向けの正式なプロセス。DRPには、定期的にテストを行う要件が含まれており、現在は年4回実施している。かかるテストの確認は、書面による要求に応じて、お客様に提供される。

19. 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/CIS 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)テクニカルトレーニングを年に1回提供する。

c) 米国政府が承認したフレームワークに沿った、本サービスの開発に使用するワークステーションの強化。

20. 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。

21. データの完全性と管理

本文書の第4条に記述されているデータ分離措置に加えて、Oktaは、以下を確保する方針を維持している:

a) バックアップ/アーカイブ: Oktaは、RPOを維持するために必要なお客様データを含むデータベースの完全バックアップを、安全なサーバー上、または他の商業的に許容できる安全な媒体上でのアーカイブ保管を実行している、および

b) データ完全性のチェック: Oktaは、お客様データの入力および出力の完全性を確保するために、自動およびマニュアルのプロセスを実施している。

22. 脆弱性管理

Oktaは、四半期ごとの脆弱性スキャンを (1) そのアプリケーションおよび (2) 本番環境および開発環境のインフラストラクチャコンポーネントに対し実行している。アプリケーションに対しては、いかなる本サービスに大きな機能変更またはアーキテクチャの変更の場合にもスキャンが実施される。脆弱性は、共通脆弱性スコアリングシステムを用いてランク付けされ、脆弱性が発見されたアプリケーションおよびインフラストラクチャシステムの種類を考慮したリスクベースで修正される。Oktaは本番環境および開発環境のすべてのコンポーネントに、中、高、および重大ランクのセキュリティパッチを商業上合理的な最短時間でインストールする。

23. 侵入テスト

Oktaは第三者と契約し、本サービスの侵入テストを毎年実施し、過去に発見された問題が修正されたことの確認を含む調査結果の報告書(「**テストレポート**」)を発行する。Oktaの最新のテストレポートからの報告は、該当する改善計画とともに、お客様からの書面による要求に応じて提供される。さらに、Oktaの内部侵入テスト担当者は、定期的に本サービスの本番インフラおよびアプリケーションのソースコードのテストを実施している。

お客様は、Oktaが提供する侵入テスト契約書に署名した後、個別のお客様組織を模した、完全に機能するOkta環境に対して、独自の侵入テストを実施することができる。

24. 変更およびコンフィグレーション管理

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および手順を維持している。かかる方針と手順には、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

25. 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するための侵入、検出、防止制御を実施し、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。

26. 可用性インシデント管理

本サービスに関するシステムステータス情報は、Okta Trustウェブサイト（https://trust.okta.com）上で提供されている。Oktaは通常、重大なシステムインシデントをリストされている管理者の電子メール連絡先に通知する。また、可用性インシデントが1時間以上続く場合、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。

27. セキュリティ違反管理

a) インシデント対応計画： Oktaは、OktaまたはOktaの復処理者が伝送、保存、処理した、お客様データの不正開示や不正アクセス、不法行為または事故による破壊、変更、損害または損失を引き起こすセキュリティ違反で、Oktaが認識したもの（「セキュリティ違反」）が発生した場合に、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（「IRP」）を策定している。OktaのIRPは次の分野に関するものである：

   i. 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

   ii. 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

   iii. 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

   iv. 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

   v. 監査： 根本原因の分析と修復計画の実施と文書化

b) 通知： セキュリティ違反を確認した場合、Oktaは、適用される法律、法執行機関の指示、または規制上の要求によって許可される範囲内で、影響を受けるお客様に通知する。通知は、お客様がOktaアドミンコンソール内で指定したセキュリティコンタクト、またはセキュリティコンタクトが指定されていない場合は、影響を受けたお客様との契約書の「通知」条項に従って送付される。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。

c) 是正措置： 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。

28. ログ記録[5]

Oktaは、ログイン、接続試行、特権ユーザーアクセスおよびアクションなどの電子情報を含む、または使用する情報システム上のアクティビティを、かかるアクティビティのソース、日付、時間、およびその他の関連情報とともに記録している。Oktaは、以下を行う： (i) 毎日のログのバックアップ、(ii) かかるログを不正な変更または消去から保護するための、商業上合理的な措置の実施、および (iii) かかるログをOktaのデータ保持方針に従って保持。オンラインの本サービスへの不適切なアクセスの疑いがある場合、Oktaはフォレンジック調査を支援するた

[5]このセクションはOkta Device Accessオフラインで使用するときには適用されない。ログが構成されず、保存されないためである。

めに、お客様にログエントリレコードを提供できることがある。このサービスは、提供された場合、実費精算ベースでお客様に提供される。お客様は、本サービス内のOktaアドミンコンソール経由で、自らの組織システムログにアクセスすることができる。

29. ユーザーとのコミュニケーション

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。

30. 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。

31. 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。