SECURITY & PRIVACY DOCUMENTATION FOR ADVANCED SERVER ACCESS

(last updated June 14, 2021)

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 or on behalf of 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 Advanced Server Access (hereinafter, the "Service"). This documentation does not apply to free trial services made available by Okta.

Architecture, Data Segregation, and Data Processing

The 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.

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.

Security Controls

The 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.

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, 27002 and 27018 certifications;
    c) NIST guidance; and
    d) SOC2 Type I and II (or successor standard) audits annually performed by accredited third-party auditors ("Audit Report").

As of this documentation's last update date, Okta and its accredited third-party auditors are in the process of testing for compliance with the standards set forth in sections 1(b) and 1(d), above.

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. **Security Awareness and Training**. Okta has 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 readily identify 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 and access to stored backups is restricted. Okta uses volume encryption for backup 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) Data Backups: A policy for performing periodic backups of production file systems and databases to meet the Recovery Point Objective described below;

b) 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, currently four times a year;

c) RPO / RTO: Recovery Point Objective is no more than 1 hour and Recovery Time Objective is no more than 24 hours;

d) 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 regardingOkta'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 full backups of the database(s) containing Customer Data no less than once per day and archival storage on no less than a weekly basis on secure server(s) or on other commercially acceptable secure media.

16. **Vulnerability Management**. Okta maintains security measures to monitor the network and production systems, including error logs on servers, disks and security events for any potential problems. Such measuresinclude:

a) Infrastructure Scans: Okta performs quarterly vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis. Okta installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

b) Application Scans: Okta performs quarterly (as well as after making any major feature change or architectural modification to the Service) application vulnerability scans. Vulnerabilities are remediated on a risk basis. Okta installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

c) External Application Vulnerability Assessment: Okta engages third parties to perform network vulnerability assessments and penetration testing on an annual basis ("Vulnerability Assessment"). Reports from Okta's then-current Vulnerability Assessment, together with any applicable remediation plans, will be made available to customers on written request, after such Vulnerability Assessment becomes available.

Vulnerabilities are remediated on a risk basis. Okta installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible.

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 is deleted using secure deletion methods including digital shredding of encryption keys and hardware destruction in accordance with NIST SP800-88 guidelines.

19. **Intrusion Detection.** Okta monitors the Service generally for unauthorized intrusions using traffic and activity-based monitoring systems. Okta may analyze data collected by users' web browsers (e.g., device type,screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers,to help customers detect fraudulent authentications, and to ensure that the Service functions properly.

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 system status information 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 incidentslasting 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 suchSecurity 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 provides procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports. Okta (i) backs-up logs on a daily

basis, (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 Service, Okta has the ability to provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.

23. **Communications with Administrators.** Separate from and as a complement to the Service, we may provide Okta administrator users ("Admins") access to Okta help and support communities, or communicate with Admins from time to time, including to send announcements and details about our products, services, or other relevant information that Admins' organizations may find useful. Admins who do not want to receive such communications on behalf of their organizations may update their communications preferences by visiting our subscription center, which is available through their admin panel.

24. **Language.** The governing language of this Security and Privacy Documentation for Advanced Server Access is English. Any Japanese language version of this Security and Privacy Documentation for Advanced Server Access is for reference purposes only. If there is any conflict between the English and Japanese version, the English version shall prevail.

Advanced Server Access の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：2019 年 6 月 14 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、お客様からまたはお客様に代わって Okta のオンラインサービスに送信されたデータ（「顧客データ」）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、Okta のオンラインサービスである Advanced Server Access(以下、「本サービス」)について取得したセキュリティ関連およびプライバシー関連の監査および認証、ならびに本サービスに適用される管理上、技術上および物理上の統制について記述する。本文書は、Okta が提供する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顧客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、様々なお客様の効果的な論理データの分離を行い、お客様および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、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チェーン全体を通じ、顧客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された手順を実装した。

セキュリティ管理

本サービスには、Okta のお客様が自社用途に合わせて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、適用される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。

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上、技術上、および物理上の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、および(d)顧客データの不正開示が起きないよう、セキュリティおよび保護の必要性。ISMP は文書化され、プライバシーおよびデータセキュリティ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 が保有または管理している顧客データの不正開示を防止すること
- 完全性および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、ならびに Okta またはその代理人による顧客データの不正開示を防止すること
- 顧客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
- 顧客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順守と定期的なテストが含まれており、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。かかるテストには次のものが含まれる：
   a) 内部リスク評価
   b) ISO 27001、 27002、27017 および 27018 認証
   c) NIST ガイダンス、および
   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 I および II (または後継規格) 監査（「監査報告書」）

本文書の最終更新日現在、Okta およびその認定された第三者監査人は、上記 1(b)および 1(d)の規格遵守をテストしているところである。

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 のその時点によ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、顧客データの保存や処理のために 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等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、または顧客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 を遵守すること、およびすべての顧客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. **セキュリティの意識向上およびトレーニング**　Okta には、ISMP の実装および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. **懲戒方針およびプロセス**　Okta は、Okta の人員が ISMP に違反した場合の懲戒方針および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. いかなる顧客データにも、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. 顧客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. ユーザー識別し（ユーザーID）が一意であり、そ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 の担当者が顧客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 が無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 ガイダ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. 顧客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) 電気的故障の場合に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、保存された顧客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、保存されたバックアップへのアクセスは制限されている。Okta は、保存時のバックアップにボリューム暗号化を使用している。

12. **災害からの復旧**　Okta は、顧客データまたは顧客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) データのバックアップ：以下に説明する目標復旧ポイントを満たすため、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。

b) 災害からの復旧：本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（現在は年４回）災害計画をテストする要件が含まれる。

c) RPO / RTO： 目標復旧ポイント（RPO）は１時間以内であり、目標復旧時間（RTO）は 24 時間以内である。

d) 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 および SANS Top 20 Critical Security Controls などの、業界標準に沿った安全な開発方針、手順、および標準に従う。

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、ウィルス、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. **データの完全性および管理**　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顧客データを他のお客様の顧客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) バックアップとアーカイブ：Okta は、顧客データを含むデータベースの完全バックアップを、１日１回以上の頻度、および少なくとも週単位で安全なサーバー上、または他の商業的に許容される安全な媒体上でのアーカイブ保管を実行している。

16. **脆弱性管理**　Okta は、潜在的な問題についてのサーバー、ディスク、セキュリティイベントのエラーログを含む、ネットワークと本番システムを監視するためのセキュリティ対策を維持している。そうした措置には以下が含まれる：

a) インフラストラクチャのスキャン：Okta は、四半期ごとに、その本番および開発環境の全インフラストラクチャコンポーネントに対して脆弱性スキャンを実行する。脆弱性はリスクに基づき修正される。Okta は、本番および開発環境のすべてのコンポーネントに、中、高、および重大なセキュリティパッチをすべて商業的に可能な限り速やかにインストールする。

b) アプリケーションスキャン：Okta は、四半期ごと（および本サービスに大幅な機能の変更またはアーキテクチャの修正を加えた後）に、アプリケーションの脆弱性スキャンを実行する。脆弱性はリスクに基づき修正される。Okta は、本番および開発環境のすべてのコンポーネントに、中、高、および重大なセキュリティパッチをすべて商業的に可能な限り速やかにインストールする。

c) 外部アプリケーション脆弱性評価：Okta は毎年、ネットワークの脆弱性評価と侵入テストを実行するために第三者と契約している（「脆弱性評価」）。Okta が行ったその時点で最新の脆弱性評価の報告書は、かかる脆弱性評価が提供可能となった後、該当する修復計画とともに、書面による要求に基づいてお客様に提供される。

脆弱性はリスクに基づき修正される。Okta は、本番および開発環境のすべてのコンポーネントに、中、高、および重大なセキュリティパッチをすべて商業的に可能な限り速やかにインストールする。

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、顧客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 ガイダンスおよびデータ保護法令に準拠して、利用可能な技術を考慮し、顧客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。顧客データは、NIST SP800-88 ガイドラインに準拠した暗号化キーのデジタルシュレッダーやハードウェア破壊を含む、安全な削除方法で削除される。

19. **侵入検知**　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。Okta は、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）を分析する場合がある。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することを支援し、本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。

20. **インシデント管理**　Okta は、Okta または Okta の代理人による顧客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を「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がのある人を判断

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社内報告および通知プロセス

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：根本原因の分析および修復計画の実施および文書化

Okta はウェブサイト「Okta Trust」（https://trust.okta.com）でシステムステータス情報を公開している。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、インシデントと Okta の対応について説明する電話会議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の要求に協力し、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) 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是正計画を提出する、(iii)セキュリティ違反の影響をかかる是正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、然るべきログやレポートはじめとする電子情報を含む、または使用する、情報システムの活動を記録および調査するための手続上の仕組みを規定する。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。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めに、お客様にログエントリレコードを提供することができる。このサービスは、実費精算ベースでお客様に提供される。

23. 管理者とのコミュニケーション　本サービスとは別に、また本サービスを補完するものとして、当社は Okta 管理者ユーザー（「管理者」）に Okta ヘルプおよびサポートコミュニティへのアクセスを提供する、または、管理者の組織に有用と思われる当社の製品、サービス、その他の関連情報に関するお知らせや詳細を送信するなど、随時管理者と連絡を取ることがある。その組織を代表して、かかる連絡の受け取りを望まない管理者は、管理パネルから利用可能な当社のサブスクリプションセンターにアクセスして、連絡の設定を更新することができる。

24. 言語　本 Advanced Server Access の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 Advanced Server Access の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。