Workday のセキュリティおよびデータ プライバシー

はじめに

ビジネス環境のデジタル化がますます進む昨今、IT 部門のリーダーは、顧客、従業員、知的財産に関わるデータの安全確保と保護を最優先で進めなければなりません。企業はより先鋭化したセキュリティの脅威に直面しており、サービスのあらゆる側面においてセキュリティおよびデータ プライバシーを担保することは喫緊の課題です。ここでは、IT プロフェッショナルの方を対象に、セキュリティおよびデータプライバシー分野における Workday の取り組みについてご紹介いたします。

法令遵守と認証

Workday と当社のお客様においては、プライバシーに関する多種多様な国際的な法規制を遵守しなければなりません。まず、国や地域を問わない共通のプライバシー方針があり、それにはプライバシーに関する通知、選択、アクセス、利用、開示、セキュリティなどが含まれています。そして、当社のアプリケーションは、設定の微調整ができるように設計されており、各国特有の法律に準拠できます。

Workday は、もとより国際的なプライバシー規制を遵守しています。包括的で、明文化された情報セキュリティ プログラムは、お客様データへの不正なアクセス、利用、開示を防御するよう設計されており、技術面および管理面でのセーフガードとなるものです。

外部監査：SOC 1 および SOC 2 レポート

Workday は、サービス プロバイダに求められる基準を満たしていること、あるいはその基準を超えていることを保証するために、業務、ポリシー、手順について定期的に外部機関による監査を受けています。Workday は、Service Organization Controls 1 (SOC1) TypeII レポートを発行しています。SOC 1 レポートは、内部統制の整備および運用に関する米国基準である SAS 70 の後継となるもので、米国保証業務基準書第 18 号 (SSAE 18) および国際保証業務基準第 3402 号 (ISAE 3402) に従って発行されます。

この 2 つの基準に準拠したレポートがあれば、Workday をはじめとするサービス プロバイダが適切な内部統制を遂行していることの証明となり、世界中の企業は安心してビジネスを遂行することができるようになります。財務諸表に影響を及ぼすような基幹業務を外部委託しているお客様は、その業務に対する内部統制を把握する必要があります。本レポートはそのようなお客様のために発行されています (サーベンス オクスリー法への準拠)。SOC 1 の対象は Workday 本番運用システムに限定されます。SOC 1 監査は、6 か月ごとに独立系の第三者監査法人によって実施され、Workday は監査終了後に、これらのレポートをお客様に開示しています。

Workday は、Service Organization Controls 2 (SOC 2) Type II レポートも発行しています。当社の SOC 2 レポートは、トラスト サービスの原則と基準 (セキュリティ、可用性、機密保持、処理のインテグリティ、プライバシー) をすべて網羅しています。SOC 2 の対象は、お客様によって入力されたデータが格納されている、Workday システムすべてに及びます。このレポートは、Workday のセキュリティに関する内部統制に関心をお持ちのお客様のために発行されています。SOC 2 の監査は年 1 回、独立系の第三者監査法人によって実施され、Workday は監査終了後に、これらのレポートをお客様に開示しています。

SOC 1 と SOC 2 の監査はいずれも、Workday の物理的安全対策および環境保全措置を審査するものです。審査対象は、本番運用データ センター、バックアップ/リカバリ手順、ソフトウェア開発プロセス、および論理的セキュリティ コントロールに関する内容となります。

ISO27001、ISO27017、ISO27018 認証

ISO 27001 は、2005 年に国際標準化機構 (ISO) および国際電気標準会議 (IEC) が公開した、情報セキュリティ マネジメント システム (ISMS) に関する規格であり、2013 年 9 月に、この 2005 年版の規格に代わる ISO 27001:2013 が公開されました。ISO 27001 は、国際基準として認められたセキュリティに対する規格ベースのアプローチで、組織の情報セキュリティ マネジメント システム (ISMS) に必要な要件の概要を示すものです。

2015 年に公開された ISO 27017 は、ISO 27001 の補完的な規格であり、クラウド サービスの提供や利用に適用される、情報セキュリティの管理および導入の指針となるものです。

ISO 27018 は、ISO および IEC が 2014 年に公開した補完的な規格で、個人情報を扱うクラウド サービスのプロバイダに適用するガイドラインを示しています。

Workday は ISO 27001 認証を 2010 年 9 月に、ISO 27018 認証を 2015 年 10 月に、ISO 27017 認証を 2017 年 11 月に、それぞれ取得済みです。Workday が常に ISO 規格を遵守しているという評価を独立機関から得ることにより、ISO 認証が付与されます。ISO 認証の更新は 3 年ごとに行われ、認証を維持するためには、年 1 回の監査を受ける必要があります。これらの ISO 認証は、Workday がプライバシーとセキュリティの保護に注力していることの裏付けであり、当社の施策が効果的に実施されていることを示すものです。Workday の ISO 認証および 情報セキュリティ マネジメント システム (ISMS) の適合性評価は、常にお客様に開示されています。

国外へのデータの持ち出し

欧州経済領域 (EEA) から米国への個人データ持ち出しについては、データ保護に関する厳格な法規で規制されています。EEA 内で事業を推進しているお客様に対応し、この要件に準拠するよう、Workday は、欧州委員会 (EC) が承認した標準的契約条項 (SCC)、別名「モデル契約」を、当社のデータ保護規約に組み込みました。モデル契約とは、EEA から第三国への個人データの持ち出しを可能にする、「妥当性に関する要件」を満たすための契約の仕組みを示すものです。

Workday は、EU-U.S. Privacy Shield (EU-米国間プライバシー シールド) および、Swiss-U.S. Privacy Shield (スイス-米国間プライバシー シールド) に対して自己認証を行っています。プライバシー シールドはセーフハーバー協定に代わるもので、欧州司法裁判所がセーフハーバー協定を法的に無効と裁定する際に明らかにされた問題点に対応する目的で制定されました。Workday はプライバシー シールドに積極的に参加しています。プライバシー シールドに対する第三者による検証方法には TRUSTe を使用しています。

米国商務省のプライバシー シールド プログラムの詳細については、http://www.privacyshield.gov (英文のみ) でご覧いただけます。標準的契約条項 (SCC) の詳細については、http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (和文なし) でご覧いただけます。

Workday の顧客データ プライバシー管理およびプライバシー プログラムの詳細については「Workday Privacy Program」データシートをご覧ください。

EU 一般データ保護規則 (GDPR)

欧州連合 (EU) の法規制である GDPR は、EU データ保護指令 (95/46/EC) および各加盟国が実施している法令を改廃するものです。この規則は 2018 年 5 月 25 日に、EU に加盟する全 28 か国で発効され、全加盟各国のそれぞれのデータ保護法令が簡素化および統合されました。GDPR は、EU 内に拠点を置く企業と、拠点の有無にかかわらず EU 市民の個人データを処理または保管するすべての企業に適用されます。

Workday は GDPR 定義に則したデータ処理者です。当社は GDPR 要件を包括的に評価し、発効日初日からこの規則が定めるデータ処理者の基準を確実に満たすため、数多くのプライバシーおよびセキュリティ施策を実施してまいりました。これには以下の施策が含まれます。

- セキュリティおよびプライバシー施策に関する社員研修
- プライバシー影響評価の実施
- お客様への十分なデータ転送方法の提供
- 処理実施の記録の保持
- お客様にて設定可能なプライバシーおよびコンプライアンス機能の提供

さらに Workday のサービスは、プライバシー バイ デザインとプライバシー バイ デフォルトの考え方に基づいて設計されています。世界中のお客様にとって GDPR は重要なビジネス上の優先事項だと認識しているからこそ、当社は今後も欧州監督当局による GDPR のガイドラインが更新されていないか常に確認し、コンプライアンス プログラムを常に最新のものに更新いたします。

データ セキュリティ

物理的セキュリティ

Workday の本番運用システムは、完全な冗長化を施したサブシステムとコンパートメント化されたセキュリティ ゾーンを備えた、ミッションクリティカルなシステムのホスティングを念頭に設計された最先端のデータ センターに置かれています。さらに、次のような最も厳重な物理的対策が施されています。

- サーバー エリアへの立ち入りには、マルチレイヤーの認証が必要
- クリティカル エリアへの立ち入りには、2種類の生体認証が必要
- 内部・外部の重要な出入口には監視カメラ システムを配置
- セキュリティ担当者はデータ センターを 24 時間365日体制で監視
- データ センターのセキュリティ監視による不正アクセスの記録とモニタリング

データ センターへの物理的なアクセスは、すべて厳重に制限され、厳しく規制されています。Workday のデータ運用では、アクセスを「最小限」にするサーバー ハードニングや定期保守の実施など、さまざまなベスト プラクティスを取り入れてセキュリティの強化を図っています。

データの隔離

Workday は、マルチテナント型の SaaS (Software-as-a-Service) アプリケーションです。

マルチテナンシーは、Workday の重要なアーキテクチャです。テナントごとにお客様のアプリケーション データを分離する一方で、1 つの物理インスタンスを複数のお客様で共有することができます。こうした機能の実現には、Workday Object Management Server (OMS) が活用されています。ユーザーが Workday アプリケーションにアクセスする際には、特定のテナントに紐付いたユーザー ID を使用します。

組織や従業員といった各アプリケーション オブジェクトのインスタンスは、すべてテナントベースで管理され、新規オブジェクトが作成されるたびに、ユーザーのテナントに対して改変不可能なリンクが作られます。Workday は、これらのリンクを自動的に維持し、ユーザー ID およびテナントに基づいてあらゆるオブジェクトへのアクセスをコントロールしています。データが要求されると、テナントのリンクに基づいてフィルタが自動適用され、当該テナントに関連するデータのみが提供されます。

保管データの暗号化 (データベース セキュリティ)

Workday は、アプリケーション内に存在するお客様データの全属性を、データベースに格納する前に暗号化します。これは Workday テクノロジーの根幹をなす設計特性で、米国の新暗号規格である鍵長 256 ビットの AES (Advanced Encryption Standard) アルゴリズムが採用されています。Workday は、ディスクベースの RDBMS アプリケーションとは異なり、インメモリのオブジェクト指向アプリケーションであるため、この AES アルゴリズムを実装することができました。具体的には、Workday 内のメタデータを Workday OMS が識別してメモリに格納し、データの挿入、更新、削除はすべて、MySQL データベースの永続ストアに対して実行されます。この独自のアーキテクチャは、Workday が一度に扱うデータベース テーブルが数十に限定されることを意味します。RDBMS ベースのアプリケーションは、同時に数万ものテーブルにアクセスしなければならず、パフォーマンスを低下させる影響が大きくなり、データベースの完全な暗号化は実用的でないとされています。

転送中データの暗号化 (ネットワーク セキュリティ)

インターネット経由で Workday にアクセスする場合、通信は TLS (Transport Layer Security) によって保護されています。これにより、メッセージの受動的な傍受や意図的改ざん、もしくは偽装から、ネットワーク トラフィックを守ることができます。

Workday はさらに、境界防御システムやネットワーク侵入防止システムといった積極的なセキュリティ保護対策も実施しています。加えて、社内組織や外部の第三者機関によるネットワーク インフラストラクチャの脆弱性評価やペネトレーション テストも定期的に実行しています。

データのバックアップ

Workday の本稼働プライマリ データベースは、オフサイト データセンターにあるレプリカ データベースに、リアルタイムでレプリケーション (複製) されています。完全なバックアップ データが毎日このレプリカ データベースから作成されます。当社のデータベースバックアップ ポリシーは、データベースのバックアップとともにトランザクション ログの収集も義務づけています。このような対策を取ることにより、トランザクションの損失を最小限に抑え、実際の業務に支障のないレベルでデータベースをリカバリ (復旧) できるようにしています。トランザクション ログは、そのログの最後のエントリの後、バックアップを 2 回取得するまで保持されることになっています。インターフェイスを実装しているシステムについても、接続先のシステムをサポートする必要がある限り、データベースのバックアップの対象となります。その設定期間は、接続先のシステムにより異なります。お客様のデータを格納しているデータベースは、すべてバックアップおよびトランザクション ログを暗号化しています。

災害復旧

Workday は、標準のサービス品質保証契約 (SLA) によりサービスの品質を保証しています。SLA には、復旧時間目標 (RTO) を 12 時間以内、復旧時点目標 (RPO) を 1 時間以内とする、Workday 本番運用システムの災害復旧 (DR) プランが盛り込まれています。RTO は、Workday の本番運用システムに障害が発生してからサービス復旧までの時間です。RPO は、最初のトランザクションが消失した時点から本番運用システムがサービス不能になった時点までの時間です。

Workday は、SLA が保証するサービスを維持するため、本番運用システムの完全なレプリケーションである災害復旧環境を整えています。不測のシステム停止が発生し、停止時間が指定した範囲を超えると予想された場合、Workday は DR プランを実行に移します。この DR プランについては、最低でも 6 か月に 1 回の定期的なテストを実施しています。

ひとつのセキュリティ モデル

Workday は、これまでのレガシー ERP システムとは異なり、単一のセキュリティ モデルによって、ユーザー アクセス、システム インテグレーション、レポート作成、モバイル デバイス、IT アクセスを監視しています。すべての Workday ユーザーは、ログイン時に Workday のセキュリティ モデルに基づいて認可を受けなければなりません。これに対してレガシー ERP システムは、通常アプリケーションごとにセキュリティ層が分かれています。このため、IT 担当者やデータベース管理者は、セキュリティ層をバイパスし、直接データベース内のデータにアクセスできる仕組みになっています。Workdayでは、このようなバイパスを行うことは不可能です。Workday は、暗号化された永続データ ストアを利用したオブジェクト指向のインメモリ システムであるため、アプリケーションへのアクセスおよび変更は、すべて確実に追跡、監視できます。この他に類を見ない堅牢な統合セキュリティ モデルと自動化機能により、あらゆるデータ更新が日時情報とともに記録および監視されるため、ガバナンスやコンプライアンスに要する時間とコストの削減だけでなく、セキュリティ リスクも軽減できます。

認証

Workday のセキュリティ アクセスはロール ベースで、シングル サインオン (SSO) 機能のための SAML、およびユーザー管理と Web サービスの統合のための x509 証明書認証にも対応しています。お客様は、ユーザーのグループごとに異なる認証要件を設定できます。

お客様が地理的にも組織的にも広範囲にわたって活動しており、ユーザーの認証に複数の認証タイプを導入することを希望する場合、ユーザーは認証の種類を選択することもできます。

シングル サインオンのサポート

LDAP はユーザー名とパスワードの組み合わせでユーザーを認証しますが、SAML は、さらに進化したエンタープライズ シングル サインオン (SSO) を実現します。SAML は、お客様の社内アイデンティティおよびアクセス管理 (IAM) ソリューションと Workday の間でシームレスな SSO エクスペリエンスを提供します。

Workday へのネイティブ ログイン

ネイティブ ログインの利用をご希望の場合、Workday は通常のプレーン テキスト形式ではなくハッシュ形式でパスワードを保存します。失敗したログインの履歴や、成功したログイン/ログアウトの履歴も監査情報として記録されます。アクティブでないユーザーのセッションは、指定の時間が経過した後にタイムアウトとなり自動的に切断されます。切断までの時間を、ユーザーごとに設定することもできます。またパスワードの長さ、複雑さ、有効期限といったパスワード ルールの設定も可能です。

多要素認証

Workday では、お客様に多要素認証 (MFA) をお使いいただくことを推奨し、ご提供もしております。お客様は、タイムベース ワンタイム パスワード (TOTP) アルゴリズムによるあらゆる認証アプリを利用できます。この設定を行うと、お客様は Workday へのネイティブ ログインに MFA プロバイダを簡単に統合することができます。Workday ではさらに、E メールから SMS へのゲートウェイを介してエンド ユーザーにワンタイム パスワードを配信することが可能です。追加のメカニズムとして、ユーザーのアイデンティティを証明するためのチャレンジ クエスチョンにも対応しています。

信頼できるデバイス

Workday は、お客様とそのエンド ユーザーがお使いのデバイスを Workday テナントにアクセス可能な信頼できるデバイスとして登録できる機能を備えています。未登録のモバイル デバイスがエンド ユーザーのアカウントにアクセスしようとした場合、そのユーザーに通知が届きます。ユーザーは、使用しなくなったデバイスの登録を削除することができます。管理者には、信頼できるデバイスのリストが確認のために提供されます。この機能を設定するには、まず管理者がテナントに対して機能を有効にします。エンド ユーザーは、信頼できるデバイスがブラウザのクッキーにより追跡されることに同意する必要があります。

ステップアップ認証

Workday は、機密性の高いリソースへのアクセスに対して、より強固な認証方法としてステップアップ認証をご提供いたします。認証タイプとして SAML をお使いのお客様は、Workday に格納されているアイテムの中で非常に重要とみなされているものへの不正アクセスを防ぎ、確実にデータを保護できます。これにより、こうした重要なアイテムにアクセスする場合、ユーザーに第 2 の認証要素を義務付けることが可能になります。

認可

Workday アプリケーションは、グループごとに設定されたポリシーに従ってセキュリティ認可を行います。アプリケーションのユーザーが本番運用データベースに直接アクセスすることはできません。Workday が提供するセキュリティ グループおよびお客様が作成するセキュリティ グループは、事前に定義されたセキュリティ ポリシーとの組み合わせにより、ユーザーごとに機能、ビジネス プロセス、レポート、データに対するアクセスを、アクセス手段 (オンラインまたは Web サービス経由) を問わず許可あるいは制限します。

セキュリティ グループは、ユーザー、ロール、職務、組織、事業地階層、事業拠点などに基づいて、お客様が柔軟に設定できます。また、セキュリティ グループを他のグループと組み合わせて新しいセキュリティ グループを作ることができます。新しく作られたセキュリティ グループでは論理的にその中のグループを外したり追加することができます。一方、システム間のアクセスは、インテグレーション システム セキュリティ グループで定義します。こうしたグループやポリシーの定義にお客様のニーズを十分に反映させることで、グローバル導入において避けては通れない複雑なグループ構成に適合した、詳細なアクセス権限の設定が可能となります。

また、採用や契約終了などの各種ビジネス プロセスに応じて自動更新されるセキュリティ グループも提供されます。こうした当社提供のセキュリティ グループは、単体でも、他の Workday 標準のグループまたはお客様が作成したグループと組み合わせても使用でき、セキュリティ ポリシーに基づいてアクセス可否を決定できます。

パブリック クラウド

Workday は、Amazon Web Services (AWS) のパブリック クラウド サービスを利用して Workday Media Cloud にコンテンツを保管し、処理しています。お客様のコンテンツは、他のお客様のコンテンツとは論理的に隔離されます。すべての Workday Media Cloud のコンテンツは、保存時に AWS サーバーサイドで安全に暗号化されます。Workday が AWS に保管する各オブジェクトは、独自の 256 ビット暗号キーを用いた AES で暗号化されます。

Workday では、AWS クラウドの論理的に隔離されたセクションである Amazon Virtual Private Cloud (Amazon VPC) を使用しています。エンド ユーザーと Workday データ センターや Workday Amazon VPC サービスとのすべての通信は、トランスポート層において暗号化されます。さらに、Workday Amzon VPC サービスから Workday データ センターへの通信、あるいはその逆方向の通信も同様に暗号化されます。Workday は、TLS プロトコルを使用して、安全な暗号のみを用いてすべてのトラフィックを暗号化します。

常時監査

Workday は、ビジネス データに対するすべての変更をアプリケーション レベルで追跡しています。このアプリケーション監査情報をもとに、Workday システムの随所で目にする監査およびコンプライアンスのレポートが作成されます。Workday は、ユーザーが成功したログインとログアウトだけでなく、失敗したログイン試行も記録し、この情報を Workday の監査レポートに提供します。Workday のシステムのアップデートは非破壊型なので、データが上書きされることはなく、テナントが有効である限り保持されます。このため、お客様は任意の値の完全な監査履歴を取得できます。Workday の監査機能は、ビジネス オブジェクトやトランザクションに対する変更履歴を追跡するために必要な情報を監査人に提供します。

Workday について

Workday は、財務・人事向けエンタープライズ クラウド アプリケーションの代表的なプロバイダです。

2005 年に設立されて以来、世界で最大規模の組織や教育機関、政府機関を念頭に設計された財務管理、人財管理、およびアナリティクスのためのアプリケーションを提供しています。中規模企業から Fortune 50 にランクインするような大企業まで、Workday はさまざまな企業から選ばれています。

workday. ワークデイ株式会社 | 代表: 03 4572 1200 | workday.co.jp

© 2019. Workday, Inc. All rights reserved. Workday および Workday のロゴは Workday, Inc. の登録商標です。その他のすべてのブランドおよび製品名は、それぞれの所有者の商標または登録商標です。20190128SECURDATAPRIV-JP