セキュリティプラクティス

SysCloud は、お客様のデータが常時安全で、利用可能で、アクセス可能であることを保証します。当社は、お客様のデータがプライベートで安全であることを確認するために、さまざまなセキュリティ対策を講じています。

1. バックアップアーカイブの保護

アクセス管理：一元化された ID およびアクセス管理が使用されます。アプリケーションとインフラストラクチャへのアクセスは最小特権の原則に従ってプロビジョニングされ、アクセスは知る必要がある場合にのみ提供されます。ロールベースのアクセス制御（RBAC）が実施され、インフラストラクチャとアプリケーションへのアクセスを制御するために、ユーザーに役割が付与されます。ユーザーアクセスは四半期ごとにレビューされ、ユーザーに付与されたアクセスの妥当性が再評価されます。

多要素認証：SysCloud は、本番環境とリソースへのすべてのアクセスに 2 要素（2 ステップ）認証メカニズムの使用を義務付けています。 ネットワークセキュリティ：SysCloud のアプリケーションは Virtual Private Network（VPN）上でホストされ、本番システムへのアクセスはパブリックインターネットからは制限されています。ネットワークのセグメンテーションにより、SysCloud は脅威行為者が本番システムに直接アクセスするのを防ぎます。

ログと監視：ログは監視され、セキュリティインシデントをリアルタイムで特定するためにアラートと警告が設定されています。インシデントは、インシデント管理ツールを通じて記録され、追跡されます。インシデントは、エスカレーションマトリックスに従ってエスカレーションされ、解決まで追跡されます。根本原因分析が実施され、是正措置と予防措置を特定します。

脆弱性とセキュリティのテスト：インフラストラクチャとアプリケーションの潜在的なセキュリティの脆弱性を積極的に特定し、修正するために、定期的に脆弱性とセキュリティのテストが実施されます。特定された脆弱性は、共通脆弱性採点システム（CVSS）を使用して評価されます。CVSS は、脆弱性報告を標準化し、脆弱性レベルの一貫した見解を提供する、信頼性の高いオープンなフレームワークです。アクションプランが特定され、脆弱性が解決するまで追跡されます。脆弱性が解決されたこ

とを確認するために、再テストが実施されます。

バックアップ：データはリアルタイムでバックアップされ、データの高い可用性を保証するために、定期的にリカバリ作業が行われ、バックアップの整合性を評価します。

パッチ：セキュリティパッチは、脅威行為者が根本的な脆弱性を悪用するのを防ぎます。パッチの更新は定期的にチェックされます。パッチはテスト環境でテストされ、デプロイメント前に承認されます。

第三者監査：SysCloud は、AWS から SOC 2 レポートを毎年取得し、AWS が実装する統制の設計と運用の有効性を評価しています。

2. SysCloud アプリケーションセキュリティの実践

ID とアクセス管理：SysCloud は、各従業員に固有のユーザーID の使用を義務付けています。認証にパスワードを使用する場合、パスワードの有効期限、パスワードの再使用の制限、十分なパスワード強度など、SysCloud のパスワードポリシーが強制されています。一元化されたロール管理は、本番システムとリソースに対するユーザーのロールベースアクセスコントロール（RBAC）を管理するために使用されます。

多要素認証：シスクラウドは、本番環境とリソースへのすべてのアクセスに 2 要素（2 ステップ）認証メカニズムの使用を義務付けています。

脆弱性管理： SysCloud のセキュリティチームは、脆弱性管理プログラムを管理しています。セキュリティチームは、主要なセキュリティツールを使用してセキュリティの脅威をスキャンし、自動および手動での侵入テスト、安全なアプリケーションと構成のレビューを実行します。セキュリティチームは、脆弱性の追跡とフォローアップを担当します。

脆弱性が特定されると、セキュリティチームはその脆弱性を記録し、重大性に応じて優先順位を付け、責任者を割り当てます。セキュリティチームは、脆弱性が修正され、再テストされるまで追跡します。

静止時および転送中のデータの保護：データは重要度と機密性の観点から分類されます。アクセス制御、トークン化、暗号化など、静止時および転送時のデータを保護するために複数のセキュリティ制御が行われます。SysCloud アプリケーションは、インターネット経由でアクセスされ、TLS（Transport Layer Security）で保護されています。

安全なソフトウェア開発ライフサイクル：SysCloud は、開発およびメンテナンス活動を管理するためのポリシーと手順を定義しています。プロジェクトごとにセキュリティリスクを評価し、対応する緩和策をドキュメント化しています。開発者はセキュアコーディングガイドラインのトレーニングを受けており、すべてのプロジェクトは、ピアコードレビューと多層的なセキュリティテストを受けます。すべての変更は、脆弱性を特定するための自動テストと手動テストを受けます。ソースコードの変更は開発者が行い、変更はバージョン管理システムに保存されます。すべての変更は、品質テストが成功した後にのみ本番環境に移行されます。

ロギングと監視：SysCloud 本番システム内の管理者とユーザーのアクティビティはログに記録されています。これらのログは、必要に応じてセキュリティチームが確認できます。本番環境へのすべての接続は、ネットワークレベルのコントロールによって強制されます。これらのコントロールは、本番環境への接続を集中的に監査し、本番アクセスに対するコントロールを可能にします。

3. SysCloud の企業セキュリティの実践

情報セキュリティ方針と手順：SysCloud は、情報セキュリティ方針と手順を定義しています。これらのポリシーは、企業ポリシーから各従業員が従うべきポリシーまで、セキュリティ関連の手順を幅広くカバーしています。これらのポリシーは、アクセス管理、インシデント管理、安全なソフトウェア開発と変更管理、事業継続と災害復旧などの分野をカバーしています。

情報セキュリティ機能とチーム：SysCloud には、専門家によって構成される情報セキュリティの専門部門があります。このチームは、会社のセキュリティポリシーと内部防御システムの設計、安全な開発とセキュリティレビューのプロセス、カスタマイズされたセキュリティインフラの構築を担当しています。

内部セキュリティチームが行う活動の一部をご紹介します：

- セキュリティ設計をレビューし、実装後のレベルレビューを実施し、プロジェクトのセキュリティリスクについて助言します。
- SysCloud のネットワーク上の不審な活動を監視します。
- 内部監査とセキュリティ評価を通じて、定義されたポリシーへのコンプライアンスを実施します。
- サイバーセキュリティのサブジェクトマターエキスパート（SME）と提携し、定期的にエンドポイントセキュリティテストを実施。
- 脆弱性管理プログラムの遵守と順守。脆弱性スキャンの一環として、特定された問題を修正するための社内チームのサポート。

人事セキュリティ：SysCloud で働くすべての従業員は、SysCloud の方針と手続きに書面で同意することが義務づけられています。従業員は、秘密保持契約を締結し、SysCloud の従業員ハンドブックを理解し、遵守していることを毎年再確認することが義務付けられています。

採用時、SysCloud は学歴、前職、犯罪歴を確認するため、独立した身元確認機関に依頼します。

情報セキュリティ教育：SysCloud では、情報セキュリティ教育プログラムを定めています。すべての従業員は、入社プロセスの一環としてセキュリティトレーニングを受けます。さらに、すべての従業員は毎年トレーニングを受け、職務の役割と責任に応じて、的を絞ったトレーニングプログラムを実施しています。従業員はまた、機密データのタグ付けや、顧客データの取り扱い時に従うべき手順についてもトレーニングを受けています。

アクセス管理：従業員は入社時に人事部によってユーザーID が割り当てられ、電子メールやドライブへのアクセスなど、限定された権限が付与されます。従業員には、職能、役割、責任に基づいて、アクセス権が付与されます。すべてのユーザーアクセスリクエストは、定義されたポリシーと手順に従い、適切な承認を受けた場合にのみ処理されます。さらに、アクセス権とレベルは、最小特権と知る必要性の原則に基づいています。離職すると、SysCloud のインフラストラクチャとアプリケーションへのユーザーアクセスは取り消されます。

インシデント管理：SysCloud は、セキュリティイベントのために定義されたインシデント管理プロセスを持っています。インシデント管理手順では、行動方針、エスカレーションの仕組み、コミュニケーションプロトコル、緩和策、文書化について説明します。

事業継続と災害復旧：SysCloud は、自然災害やその他のイベントによるサービスの中断を最小限に抑えるために、事業継続と災害復旧プログラムを定義しています。このプログラムは、アプリケーションデータを別の地域にリアルタイムで複製するなど、単一障害点のリスクを最小化する目的で定義されています。SysCloud は、地理的に分散された地域にバックアップを保存し、単一の地域で災害が発生した場合でも継続性を維持します。

バックアップの管理に加え、SysCloud はインドでの事業継続計画（BCP）を定めています。この計画は、お客様へのサービスを継続的に運営するための協調的な取り組みを可能にするように設計されています。

事業継続計画は毎年テストされます。テストは、範囲、目的、シナリオの設定など、定められた事業継続計画に従って実施されます。SysCloud は、卓上演習から実際のインシデントを想定した本格的なシミュレーションまで、さまざまな方法で BCP テストを実施します。テストの結果は分析され、望ましい復旧時間を達成するために復旧戦略が修正されます。

たとえば、このようなテストでは、IT システムや業務プロセスをオフラインにし、災害復旧計画に従って指定されたフェイルオーバー拠点にシステムやプロセスを移行させることで、地理的地域における災害をシミュレートします。テスト期間中、災害復旧拠点で業務およびオペレーションが可能であることが確認されます。テストの一環として特定された問題はすべて特定され、改善のために記録されます。

4. セキュリティ侵害やインシデントに対処するためのプロセス

インシデント管理ポリシー：SysCloud は、インシデント管理ポリシーと手順を定義しています。システムまたはデータの機密性、完全性、または可用性に影響を与えるセキュリティイベントは、インシデントとして分類されます。

インシデント・レスポンス・プログラムの一環として、以下が実施されます：

- セキュリティ運用とインシデント対応に関するユーザートレーニング
- 信頼性の高い一貫した対応を保証するためのプレイブックとガイドの定義
- テストは、インシデントレスポンスの有効性を評価するために、内部脅威やソフトウェアの脆弱性など、さまざまなシナリオを想定してシミュレートされます。
- 必要に応じてインシデント管理方針および手順の更新

インシデントの報告：インシデントの報告は、社内チームまたは顧客から incident@syscloud.com にインシデントを受信すると、SysCloud の内部チームは、インシデントを記録し、その重要度に応じて優先順位を付けて対応します。顧客に直接影響を与えるイベントは、最優先で処理されます。割り当てられたチームは、最初のトリアージを完了し、根本原因分析を実行し、是正措置と予防措置を特定します。各アクションプランに対して、責任者と目標タイムラインが割り当てられます。インシデントとアクションプランのステータスは、週単位で経営陣によってレビューされます。

データ漏洩が発生した場合、法務、テクノロジー、セキュリティの専門家からなるチームが関与し、さらに以下のステップが実行されます：

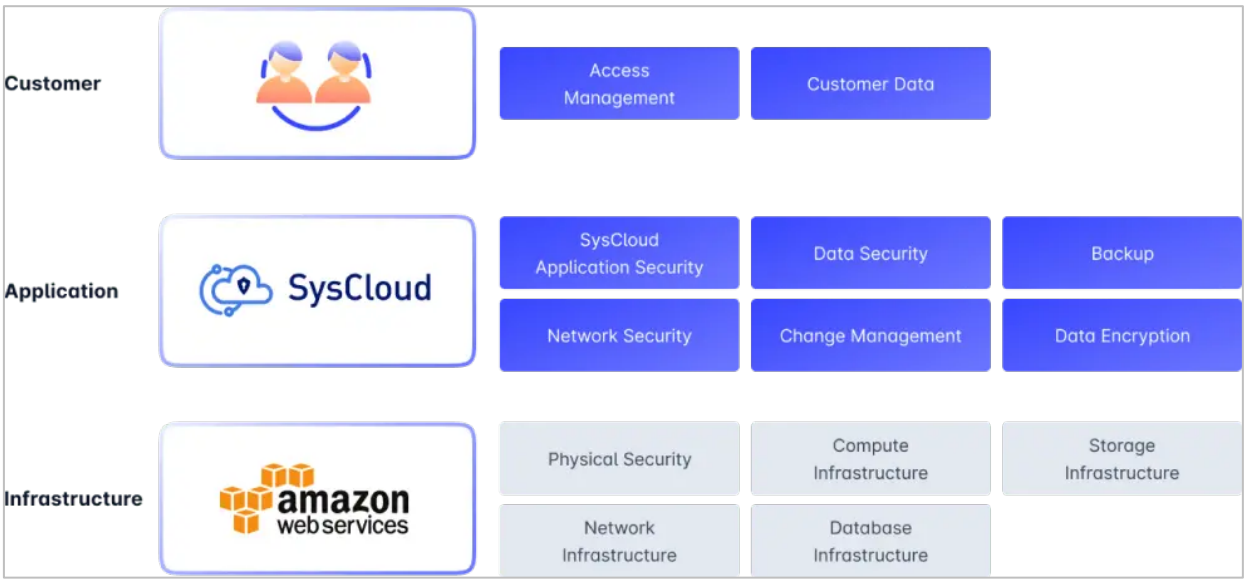
- 違反またはインシデント通知に関する契約上の義務を満たし、関連法規を遵守するため、影響を受ける顧客への通知を含む、社内外の関連ステークホルダーとのコミュニケーション
- 調査活動のための証拠の収集と保存

さらに、単一事象の根本原因や、複数の事象にまたがる長期的な傾向を把握し、同様の事象の再発防止に役立つ新たな戦略を開発するために、事故が収束した時点で事後調査を実施します。

5. SysCloud 上のバックアップアーカイブを保護するためのお客様の義務

セキュリティとコンプライアンスは、SysCloud とお客様の間で共有される責任です。この共有モデルは、お客様の義務を理解するのに役立ちます。お客様は、SysCloud アプリケーション内のデータとユーザーのアクセスに対する責任と管理を負います。SysCloud は、アプリケーション、オペレーティングシステム（アップデートとセキュリティパッチを含む）、および関連するインフラストラクチャを管理します。

下図に示すように、SysCloud とお客様の間での責任の所在が明確になります：



SysCloud は、当社の管理下にあるアプリケーションの各側面を保護する責任を持つ一方で、お客様は、自社内のチームとデータの保護と安全を確保する上で重要な役割を果たします。SysCloud バックアップアプリケーションの管理者として、組織のセキュリティ、プライバシー、およびコンプライアンスのニーズを満たす方法でアカウントを設定、運用、および監視する能力を持っています。

この、お客様と SysCloud の責任共有モデルは、IT 統制にも適用されます。IT 環境の運用責任が SysCloud とお客様の間で共有されているように、IT 統制の管理、運用、検証も共有されています。

お客様には以下の責任を負っていただきます：

ユーザー管理： ユーザーの割り当てやロールの変更など、管理者コンソールによる設定の構成。設定をカスタマイズし、ユーザーの適切なアクセスレベルと権限を選択します。許可されたユーザーのみが SysCloud アプリケーションにアクセスできるようにします。

認証：SysCloud アプリケーションへの認証を管理し、強力なパスワードセキュリティ制御を実施します。ユーザー認証情報の共有は避けてください。

データ管理：バックアップするデータの選択、データの包含と除外の制御、クロスユーザーリストアの実行、および管理コンソールからのデータに関するその他のすべての機能。

バックアップ設定：データの保持期間、バックアップ対象データのカテゴリ、ユーザーがデータを削除できないように制限する設定などのバックアップ設定の構成。

規制およびコンプライアンス適合性の評価：SysCloud のセキュリティプラクティスがお客様のコンプライアンスプログラムに適合しているかどうかを判断します。SysCloud のバックアップとデータ保護アプリケーションは、SOC 1 Type 2 および SOC 1 Type 2 Attest レポートの対象です。また、お客様が十分な情報を得た上で判断できるように、秘密保持契約に基づいて追加の文書にアクセスすることもできます。これには、HIPAA、COPPA、および FERPA の要件と当社の内部プラクティスのマッピングが含まれます。

6. セキュリティ認証について

SystemandOrganizationControls（SOC）

System and Organization Controls（SOC）レポートは、他の事業体にサービスを提供するサービス組織が、独立した公認会計士によるレポートを通じて、実施されたサービスおよび関連する統制に対する信頼と信用を構築することを目的としています。

SOC1 Type2 レポートは、サービス機関における財務報告に係る内部統制の整備及び運用の有効性に関する保証を提供します。

SOC 2 Type2 レポート - SOC 2 レポートは、セキュリティ、機密性、およびプライバシーのトラストサービス基準をカバーしています。SOC 2 レポートは、SysCloud のコントロールが 2017 年の信頼性サービス基準を満たすように設計され、効果的に運用されていることを確認します。

HIPAA

HIPAA とは、Health Insurance Portability and Accountability Act（医療保険の 相互運用性と説明責任に関する法律、1996 年）のことです。HIPAA は、医療データのセキュリティとプライバシーを保護することを目的としています。HIPAA には公式な認証はありません。 HITRUST は、医療業界の代表者

によって運営されている組織です。HITRUST は、HIPAA と HITECH 法を基礎とする共通セキュリティフレームワーク（CSF）を作成し、維持しています。SysCloud は、SOC 2 にマッピングされた HITRUST CSF を活用しており、SOC 2 レポートの一部となっています。

FERPA

Family Educational Rights and Privacy Act (FERPA)は、個人を特定できる情報や名簿情報を含む、学生の教育記録のプライバシーを保護することを目的とした連邦法です。 この法律は、学校、学区、および米国教育省から資金提供を受けているその他の機関に適用され、事実上、すべての公立の幼稚園から高校までの学校と学区、および公立と私立の両方のほとんどの中等教育機関に適用されます。SysCloud は、評価を実施し、FERPA の主要なコンプライアンス要件を SOC 2 コントロールにマッピングし、SOC 2 レポートに含まれています。

COPPA

1998 年児童オンラインプライバシー保護法（COPPA）は、13 歳未満の児童からの個人情報の収集を規制することを目的とした連邦法です。COPPA は、ウェブサイトやオンラインサービスの運営者に顧客情報を保護するためのさまざまな要件を課しています。 SysCloud は、評価を実施し、COPPA の主要なコンプライアンス要件を SOC 2 統制にマッピングし、SOC 2 レポートに含まれています。