2021年11月3日更新

# クラウドサービスのセキュリティ条件

クラウドサービスに関するこれらのセキュリティ条件（「クラウドセキュリティ条件」）は、本言及により、Genesysとの本契約に組み込まれ、本契約に基づき顧客がGenesysからライセンスを受けたクラウドサービスの提供に関連し、Genesysが顧客に提供する情報セキュリティに関する契約上の要件を記載します。これらの条件は、Genesysが顧客データにアクセスし、かつコントロールできる範囲で適用されます。

1. セキュリティプログラム

1.1 セキュリティ基準。Genesysは、提供されるクラウドサービスの性質および範囲に応じ、顧客データを保護するように設計され、ISO27001規格に具現化された、一般的に認められているシステム・セキュリティ原則に準拠した情報セキュリティプログラムを実施し、維持します。

1.2 セキュリティアウェアネスおよびトレーニング。Genesysは、雇用または契約開始時およびその後毎年、すべての従業員および適切な請負業者に提供される情報セキュリティおよびアウェアネスプログラムを開発し、維持します。アウェアネスプログラムは電子的に提供され、合格するための最低限の要件を備えたテストの側面を含みます。具体的には、顧客データアクセスに関して、年次コンプライアンス、情報セキュリティ、プライバシー、HIPAAセキュリティおよびプライバシー、およびPCIトレーニングを含みます。Genesysのコードリポジトリへのアクセスには、安全な開発における追加の年次トレーニングが必要です。

1.3 ポリシーおよび手続き。Genesysは、情報セキュリティプログラムをサポートするための適切なポリシー及び手続きを維持します。ポリシーおよび手続きは、毎年見直され、必要に応じて更新されます。

1.4 変更管理。Genesysは、クラウドサービス環境のすべての変更が適切にレビューされ、テストされ、かつ承認されることを保証するために、業界標準に基づく変更管理プロセスを活用します。

1.5 データの保存とバックアップ。Genesysは重要な顧客データのバックアップを作成します。顧客データは、クラウドプロバイダベースのサーバサイド暗号化（SSE）を使用して保存および維持されます。バックアップデータはポータブルメディアに保存されません。顧客データのバックアップは、不正アクセスから保護されます。

1.6 アンチウイルスおよびアンチマルウェア。業界標準のアンチウイルスおよびアンチマルウェア保護ソリューションが、悪意のあるソフトウェア（トロイの木馬、ウイルス、ワームなど）からクラウドサービスをサポートするインフラストラクチャを保護するために、マルウェアにより一般に影響を受けるシステムで使用されます。Genesysは、システムアクセスおよびコマンド使用の堅牢な監視だけでなく、すべてのプロダクションシステムにファイル整合性管理（FIM）ソリューションを配備しています。クラウドサービス・サーバインスタンスは、主にLinuxであり、一般にマルウェアの影響を受けないシステムです。Windowsベースのサーバーインスタンスが使用されている場合は、業界標準マルウェア対策ソフトウェアが配備されます。

1.7 脆弱性およびパッチ管理。Genesysは、業界標準の遵守を保証する脆弱性管理プログラムを維持します。Genesysは、クラウドサービスのプロダクション環境に対するすべての重大な脆弱性について、アクセス／ベクタの複雑性、認証、影響、完全性、可用性について評価します。結果として生じるリスクが、Genesysによって顧客データにとって「重大」とみなされる場合、Genesysは、7営業日以内に影響を受けるシステムにパッチを適用または緩和するよう努力します。特定のステートフルシステムは、相互依存性および顧客の影響により、迅速にパッチを適用することはできませんが、可能な限り迅速に修正されます。

1.8 データの削除および破棄。Genesysは、使われなくなったデータを削除し、かつ、以前顧客データを保持していた使用済み機器を除去または破棄するために、サブプロセッサが業界標準のプロセスに従うことを保証します。記録保持ポリシーは、顧客によって決定され、記録されたやり取りのための日常的な削除プロセスの一部として使用することができます。たとえば、記録保存ポリシーを作成して、一定の日にちの範囲内で発生した会話を削除することができます。クラウドサービス内のすべての削除は、単純な削除です。セキュアデータの削除は、仮想ディスク環境では適用されません。

1.9 侵入テスト。少なくとも年1回、Genesysは、独立した適格なベンダーとの間で、脆弱性評価および侵入テスト業務を実施します。かかる業務の間に特定された問題は、問題の特定されたリスクレベルに見合った合理的な期間内に適切に対処されます。テスト結果は、書面の要求に応じて顧客に提供され、かつ秘密保

持契約に従うものとします。

2. 製品アーキテクチャのセキュリティ

2.1 論理分離コントロール。Genesysは、顧客データが、クラウドサービス環境内において、他の顧客データから論理的に分離されることを保証するために、業界標準に基づく効果的な論理分離コントロールを採用します。

2.2 ファイアウォールサービス。Genesysはファイアウォールサービスを使用し、クラウドサービスインフラストラクチャを保護します。Genesysは、粒度の細かいイングレスおよびエグレスに関するルールを維持し、かつ、変更はGenesysの変更管理システムを通じて承認されなければなりません。ルールセットは半年ごとに見直されます。

2.3 侵入検知システム。Genesysは、クラウドサービス環境全体にPCI DSS要件を満たす侵入検知を実装しています。

2.4 ワイヤレスネットワークなし。Genesysは、クラウドサービス環境内でワイヤレスネットワークを使用しません。

2.5 顧客とクラウドサービス環境との間のデータ接続。ブラウザ、モバイルアプリ、およびその他のコンポーネントへのすべての接続は、パブリックインターネット経由のハイパーテキスト転送プロトコルセキュア（HTTPS）およびトランスポート層セキュリティ（TLS v1.2）を介して保護されます（一部のクラウド音声テレフォニーはキャリアの制限のために保護できないことに注意してください）。

2.6 クラウドサービス環境と第三者間のデータ接続。顧客データの顧客およびGenesysベンダーとの伝送または交換は、安全な方法（例：TLS1.2、HTTPS、SFTP）を用いて行われます。

2.7 暗号化された記録。Genesysは、通話録音およびチャットセッションを暗号化します。
顧客は、ローカルキー暗号化を実施し、かつ音声およびスクリーン記録のために顧客自身のキーを維持することを選択することができます。適用される法令または顧客のポリシーで要求される範囲において、顧客は、適用されるセキュリティ機能またはGenesysが提供するその他のツールを使用して、レコーディングの内容に責任を負い、かつPCIセンシティブ（機密）認証データが記録されないことを保証します。

2.8 暗号化保護。Genesysは、AESおよびTLS1.2を使用した暗号化をサポートするために業界標準方策をとります。
デジタル記録の暗号化については、2.7項と7.6項に記載されます。

2.9 ロギングと監視。Genesysは、顧客にクラウドサービスを提供するすべてのインフラストラクチャの運用上の観点からセキュリティイベントを記録（ログ）します。Genesysは、セキュリティ上のインシデントまたは問題を示す可能性のあるイベントを監視および調査します。イベント記録は、少なくとも1年間保存されます。限定された監査データは、ユーザ・インターフェース（UI）およびアプリケーション・プログラミング・インターフェース（API）を介して顧客がアクセスできます。

3. ユーザアクセスコントロール

3.1 アクセスコントロール。Genesysは、許可されたユーザのみがクラウドサービス環境内の顧客データにアクセスできるように、適切なアクセスコントロールを実装します。

3.2 顧客のユーザアクセス。顧客は、アプリケーション内のユーザアクセスコントロールを管理する責任を負います。クラウドサービス・アプリケーションのパスワード要件は、最小の長さ、最小文字数、最小数字、最小の特定の文字数、パスワードの有効期限、および最小経過時間について、顧客が設定できます。Genesysは、数回の無効な試みの後、ロックアウト期間を設けています。ほとんどのユーザは、5回の失敗後にロックアウト期間を経験しますが、5分以内に自動的に再試行することができます。これらの設定は構成できません。顧客は、きめ細かいアクセス権限モデルでユーザ名とロールを定義します。顧客は、自ら、その代理人、請負業者または従業員（そのすべてのユーザを含みますが、これらに限定されません）が、自己の制御下にあるすべてのユーザ名、パスワードおよびその他のアカウント情報のセキュリティを維持しなかった場合、全責任を負います。Genesysの重大な過失または故意の作為または不

作為に起因するセキュリティ失効の場合を除き、顧客は、顧客のユーザ名およびパスワード（顧客により承認されているか否かを問いません）を通じてのクラウドサービスのすべての使用および当該使用に起因するすべての料金に全責任を負います。顧客は、顧客がクラウドサービスの不正使用を認識した場合、直ちに、Genesysに通知することとします。

3.3 Genesysのユーザアクセス。Genesysは、クラウドサービス環境内で顧客データまたは顧客のシステムにアクセスする必要のある業務を有する各従業員のために、個々のユーザアカウントを作成します。Genesysのユーザアカウント管理に関して、以下のガイドラインに従います：

3.3.1 ユーザアカウントは、Genesysのマネジメントによって要求され、かつ承認されます。

3.3.2 強力なパスワード管理が体系的に実施されています。

3.3.3 接続は、90日ごとに期限切れになる強力なパスワードおよびマルチファクター認証を使用して、安全なVPN経由でなされる必要があります。

3.3.4 セッションのタイムアウトは、体系的に実施されます。

3.3.5 ユーザアカウントは、アクセスの有効なビジネス上の必要性を排する従業員の終了または役割の移転時に速やかに無効化されます。

4. ビジネス継続性・災害復旧

4.1 破壊防止。クラウドサービスは、クラウドサービスの最適な可用性を提供するために、高可用性設計で展開かつ構成され、かつ別々のデータセンターに展開されます。クラウドサービス環境は、企業環境に関わる中断イベントがクラウドサービスの可用性に影響を及ぼさないように、Genesysの企業ネットワーク環境から物理的に分離されています。

4.2 事業継続。Genesysは、企業環境に関わる混乱事態が発生した場合でも、継続中の監視およびサポートサービスが継続されるよう設計された、企業の事業継続計画を維持します。

4.3 災害復旧。クラウドサービスプラットフォームは、インフラストラクチャの分散された性質を利用して、複数の可能性ゾーン（「AZ」）（互いに隔離されるように設計された別個の場所で）において動作することにより、完全なマルチサイトの災害復旧を可能にします。独立したアプリケーション・スタックは、複数のAZで実行されます。単一のAZまたはデータセンターが失われた場合、残りのクラウドサービスは動作し続け、失われたシステム容量を置き換えるために自動スケールするように設計されます。

5. セキュリティインシデント対応

5.1 セキュリティインシデント対応プログラム。Genesysは、顧客データに関わるセキュリティインシデントを特定し、対応するために設計された業界標準に基づくセキュリティインシデント対応プログラムを維持します。プログラムは、少なくとも年1回、レビュー、テスト、および、必要に応じ、更新されます。セキュリティインシデントとは、顧客データの不正使用、削除、変更、開示またはアクセスをもたらす確認されたイベントを意味します。

5.2 通知。適用法令に基づく通知を必要とするセキュリティインシデントまたはその他のセキュリティインシデントが発生した場合、Genesysは、24時間以内に顧客に通知し、当該インシデントに関連する必要な通知を顧客が行うことができるよう、合理的な協力をするものとします。ただし、Genesysが、法執行機関または裁判所により、そのようにしないよう特に要求された場合はその限りではありません。

5.3 通知の詳細。Genesysは、顧客に対し、セキュリティインシデントに関する以下の詳細を提供します。（i）セキュリティインシデントが特定され、確認された日付、（ii）セキュリティインシデントの性質および影響、（iii）Genesysが既に講じた措置、（iv）講じるべき是正措置、および（v）代替策および次の措置の評価。

5.4 継続的コミュニケーション。Genesysは、セキュリティインシデントの解決に関する顧客への適切な状況報告を継続し、セキュリティインシデントの是正および将来のセキュリティインシデントの防止のた

め、継続的に誠実に取り組みます。Genesysは、顧客から合理的に要求される場合、セキュリティインシデントをさらに調査し、かつ解決するために協力します。

6. データセンターの保護。Genesysは、サービスとしてのプラットフォーム（PaaS）のためデータセンターと契約します。データセンターのセキュリティおよびコンプライアンスの認証および／またはアテステーションレポートは、データセンターから直接入手しなければなりません。データセンターは、顧客に対し、追加の秘密保持契約の締結を要求することがあります。

7. クラウドサービスの利用

7.1 使用制限。顧客は、以下のいずれかのため、クラウドサービスを使用し、かつ他者にその使用を許可または承認しません。（i）適用法令に違反すること、（ii）悪意のあるコードを送信すること、（iii）911または緊急サービスを送信すること（または、かかる使用をサポートまたは提供するために再構成すること）、（iv）クラウドサービスまたは、それらに含まれる第三者データの完全性または性能を妨害し、不当に負担させ、または、中断させること、（v）システムまたはネットワークへの不正アクセスを得ることを試みること、または（vi）再販、ライセンス、貸与またはリースを含む、ユーザ以外の第三者にクラウドサービスを提供すること。

7.2 顧客テストの制限。顧客は、クラウドサービスのプロダクション、テスト、または開発に対して、いかなる種類の侵入テスト、脆弱性評価、またはサービス拒否攻撃も行わないこととします。

7.3 使用禁止。顧客は、ユーザによるあらゆる禁止された使用を防止し、または、それらを阻止するために、商業的に合理的な努力を払うこととします。

7.4 顧客セーフガード。顧客は、そのアカウントID、パスワード、アンチウィルスおよびファイアウォールの保護、クラウドサービスとの接続性に関して、合理的かつ適切な管理レベル、物理レベル、および技術レベルのセキュリティを維持します。

7.5 VoIPサービス回線。顧客は、すべてのVoIPサービスライン上で厳重なセキュリティを維持するものとします。顧客は、Genesysが顧客に911またはその他の緊急サービスに到達する能力を提供していないことを確認し、かつ、顧客は、クラウドサービスが利用されている場所にいる可能性のある、またはクラウドサービスを使用する個人に、911またはその他の緊急ダイヤルが利用できないことを通知することに同意します。

7.6 セキュリティ機能。クラウドサービスが個人データの送信または処理に使用される場合、顧客は、すべての個人データがGenesysにより提供されるセキュリティ機能の使用を介してのみ取得され、かつ使用されることを保証します。

7.7 記録。顧客は、レコーディングの使用が専ら顧客の裁量およびコントロールの範囲内であることを認識します。上記を制限することなく、（i）本顧客は、すべての適用法令に遵守するような記録の実施方法および方法を決定し、かつ適切にクラウドサービスを設定および使用することに単独で責任を負います。（ii）本顧客は、すべての適用法令により要求される目的および／または遵守する目的のためにのみ、記録が行われることを保証します。顧客は、（a）全ての適用法令で許可される場合を除き、記録には、銀行口座番号、クレジットカード番号、認証コード、社会保障番号または個人データが意図的に含まれないこと、または、（v）記録が常に暗号化されること、を保証することとします。顧客は、クラウドサービス内の記録暗号化機能を変更、無効化または回避してはなりません。

8. 業界固有の認証。Genesysのセキュリティおよび運用管理は、業界標準プラクティスに基づいており、PCI、SOC2Type2、ISO27001、およびHIPAAのガイドラインを満たすことが認定されています。それにもかかわらず、顧客は、顧客のビジネスに必要な業界固有の認証を取得し、維持する責任を単独で負います。

9. 監査。顧客または顧客が選択した適任の第三者は、Genesysの合理的な秘密および情報セキュリティポリシーに従い、顧客がGenesysが遵守していないと合理的に信じていることを証明した場合、年に1回を超えない範囲内で、かつ、30日前の書面通知をもって、これらのクラウドセキュリティ条件の条件をGenesysが遵守しているか否かのセキュリティ評価を行う権利を有するものとします。通常の営業時間中、顧客またはその正式な代理人は、これらのクラウドセキュリティ条件を遵守するために実施されたGenesysのポリシーおよび実務を検査することができ、これにはサイト訪問および合理的な裏付け書類のレビューが含まれることがあります

が、ただし、顧客は、当該権利にGenesysの第三者のホスティング施設および設備を含むGenesysの下請業者の立入検査または監査の権利は含まれないことに同意します。かかる評価は、他の顧客またはパートナーに対するGenesysの守秘義務に違反しないものとし、またはGenesysの知的財産を開示しないものとします。本条に基づいて実施されるあらゆる評価は、の事業の正常な遂行を妨げるものではありません。Genesysは、当該評価の過程で顧客が行った合理的な要求に協力するものとします。Genesysは、顧客の評価に関連して発生したGenesysの費用（費やした内部的な時間を含みます）について、評価が遠隔的に実施されたか現場で実施されたかを問わず、合理的な料金を顧客に請求する権利を有します。

10. プライバシー。Genesysは、Genesysのコントロール下で顧客データを尊重かつ保護するために設計されたプライバシー・プログラムを開発し、かつ維持します。