

# セキュリティホワイトペーパー

第 1.1 版

2026 年 1 月 1 日

～ 改訂履歴 ～

版番号	発行年月日	改訂内容	作成	承認
1.0	2025/10/01	初版作成		
1.1	2026/01/01	CLD.8.1.5 の削除時期を変更		

## 目次

1. 目的	5
2. 適用範囲について	5
3. 用語について	5
4. ISO/IEC 27017:2015 (JIS Q 27017:2016) への対応	6
5.1.1 情報セキュリティのための方針群	4
6.1.1 情報セキュリティの役割および責任	7
6.1.3 関係当局との連絡	7
CLD.6.3.1 クラウドコンピューティング環境における役割および責任の共有および分担	7
7.2.2 情報セキュリティの意識向上、教育および訓練	7
8.1.1 資産目録	8
CLD.8.1.5 クラウドサービス利用者の資産の除去	8
8.2.2 情報のラベル付け	8
9.2.1 利用者登録および登録削除	8
9.2.2 利用者アクセスの提供	8
9.2.3 特権的アクセス権の管理	8
9.2.4 利用者の秘密認証情報の管理	8
9.4.1 情報へのアクセス制限	8
9.4.4 特権的なユーティリティプログラムの使用	8
CLD.9.5.1 仮想コンピューティング環境における分離	9
CLD.9.5.2 仮想マシンの要塞化	9
10.1.1 暗号による管理策の利用方針	9
11.2.7 装置のセキュリティを保った処分又は再利用	9
12.1.2 変更管理	9
12.1.3 容量・能力の管理	9
CLD.12.1.5 実務管理者の運用のセキュリティ	9
12.3.1 情報のバックアップ	9
12.4.1 イベントログ取得	10
12.4.4 クロックの同期	10
CLD.12.4.5 クラウドサービスの監視	10
12.6.1 技術的脆弱性の管理	10

13.1.3 ネットワークの分離	10
14.1.1 情報セキュリティ要求事項の分析および仕様化	10
14.2.1 セキュリティに配慮した開発のための方針	11
15.1.2 供給者との合意におけるセキュリティの取扱い	11
15.1.3 ICT サプライチェーン	11
16.1.1 責任および手順	11
16.1.2 情報セキュリティ事象の報告	11
16.1.7 証拠の収集	11
18.1.1 適用法令および契約上の要求事項の特定	12
18.1.2 知的財産権	12
18.1.3 記録の保護	12
18.1.5 暗号化機能に対する規制	12
18.2.1 情報セキュリティの独立したレビュー	12

## 1. 目的

株式会社コムスクエアの提供するテレフォニーソリューション及び IT インフラ監視・運用ソリューション（以下、本サービス）のセキュリティホワイトペーパー（以下本書）は、ISMS（情報セキュリティマネジメントシステム）のクラウドセキュリティ認証である「ISO/IEC 27017：2015」で求められている要求事項の中で、当社がお客様に対し提供しているセキュリティの取組みについて明確にし、ご確認いただくことを目的としています。

### <ISO/IEC 27017 について>

ISO/IEC 27017 は、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を示した国際規格です。クラウドサービスに関する情報セキュリティ管理策の実践の規範として、ISO/IEC 27017 で、情報セキュリティ全般に関するマネジメントシステム規格 ISO/IEC 27001 の取組みを強化します。これにより、クラウドサービスにも対応した情報セキュリティ管理体制を構築し、その実践を支援します。

## 2. 適用範囲について

当社の ISO/IEC 27017 の適用範囲は、以下のサービス内容に対するものです。

- ・テレフォニーソリューション
- ・IT インフラ監視・運用ソリューション

### <お問い合わせの窓口：サポート窓口>

#### ①コールトラッカー お客様サポート

TEL：050-1860-5649

E-Mail：ct\_support@comsq.com

お問い合わせは 24 時間 365 日受け付けるが対応は弊社営業日の 9:00～18:00 となる

#### ②VoiceX お客様サポート

E-Mail：voicex\_support@comsq.com

TEL：050-1868-5196

営業時間：お問い合わせは 24 時間 365 日受け付けるが対応は弊社営業日の 9:00～18:00 となる

#### ③Patrolclarice Family お客様サポート

サポートサイト：[https://members.patrolclarice.jp/support\\_login/](https://members.patrolclarice.jp/support_login/)

営業時間：お問い合わせは 24 時間 365 日受け付けるが対応は弊社営業日の 9:00～18:00 となる

### **3. 用語について**

本書では ISO/IEC 27017:2015 (JIS Q 27017:2016)で記されている用語については、そのまま使用しています。

### **4. ISO/IEC 27017:2015 (JIS Q 27017:2016) への対応**

以下に ISO/IEC 27017:2015 (JIS Q27017:2016)が求める要求事項に対する管理策を記載します。  
番号・タイトルは、ISO/IEC 27017 が求める「情報セキュリティ管理策の実践の規範」 5～18（17を除く）の小項目番号・要求事項原文を示しています。

### 5.1.1 情報セキュリティのための方針群

クラウドサービスプロバイダ(CSP)は、クラウドサービスの提供および利用に取り組むため、情報セキュリティ方針を拡充することが求められています。本サービスでは、当社の情報セキュリティ方針に従いサービスを運用しています。

### 6.1.1 情報セキュリティの役割および責任

情報セキュリティの役割および責任、本サービスの責任分界点は下図のとおりです。



### 6.1.3 関係当局との連絡

本サービスに保存いただくデータの所在は日本国内になります。

#### CLD.6.3.1 クラウドコンピューティング環境における役割および責任の共有および分担

情報セキュリティの役割および責任、本サービスの責任分界点に関しては「6.1.1 情報セキュリティの役割および責任」をご参照ください。

### 7.2.2 情報セキュリティの意識向上、教育および訓練

情報セキュリティ要件の周知徹底とクラウドサービスの運営ルール徹底を目的として、サービスに従事する要員を対象とした教育・訓練および意識向上の策を実施しています。

### **8.1.1 資産目録**

利用者の情報資産(保存データ)とサービス提供者が運営するための情報資産は明確に分離しています。なお、利用者が本サービスに作成・保存する情報資産は、利用者の管理範囲となります。

### **CLD.8.1.5 クラウドサービス利用者の資産の除去**

利用者が本サービスを解約した場合、当社は利用者が本サービスで作成、保存した情報を削除します。削除については法令に基づく場合を除き解約日から 10 営業日で削除いたします。ただし、ログは対象外とします。

### **8.2.2 情報のラベル付け**

本サービスでは、保存データのラベル付けを行う機能は提供していません。

### **9.2.1 利用者登録および登録削除**

管理者権限を有する管理者アカウントにて利用者の登録・変更・削除をご利用いただけます。詳細は、管理者マニュアルにてご確認ください。

### **9.2.2 利用者アクセスの提供**

本サービスの参照範囲や機能実行範囲を定めるための権限管理機能を提供しています。

### **9.2.3 特権的アクセス権の管理**

特権的アクセス権は、お客様には提供していません。

### **9.2.4 利用者の秘密認証情報の管理**

本サービスメニューでユーザー登録後、対象者へアカウントを通知してください。

### **9.4.1 情報へのアクセス制限**

本サービスのご利用にあたっては、管理メニューの権限設定機能により、利用者の情報へのアクセス制限を行うことができます。

### **9.4.4 特権的なユーティリティプログラムの使用**

利用者に対し、セキュリティ手順を回避し各種サービス機能の利用を可能とする API 等のユーティリティプログラムの提供は行っておりません。

#### **CLD.9.5.1 仮想コンピューティング環境における分離**

マルチテナント環境で動作します。テナント毎の ID によるアクセス資源の分離を実施し、別テナントへのアクセス制御を実施しています。

#### **CLD.9.5.2 仮想マシンの要塞化**

構築するすべての仮想化環境はポート・プロトコルへの制限を実施し、不正アクセスを遮断して適切にログを保存しています。

#### **10.1.1 暗号による管理策の利用方針**

本サービスのデータ(アプリケーション及びデータベースのストレージ)は暗号化を行っており、鍵は当社で厳格に管理しています。お客様パスワードはハッシュ化して保管しています。本サービスにおいてお客様データをやり取りする通信は SSL/TLS (TLS 1.2/ TLS 1.3 対応) 通信を用いて暗号化しています。

#### **11.2.7 装置のセキュリティを保った処分又は再利用**

機器の老朽化、故障等により交換した機器媒体の処理については、当社では直接装置の処分を行うことはありません。AWS の施設、建物、および物理上のセキュリティに基づきます。

[https://aws.amazon.com/jp/blogs/news/data\\_disposal/](https://aws.amazon.com/jp/blogs/news/data_disposal/)

#### **12.1.2 変更管理**

提供するサービスの更新や定期メンテナンスを実施する場合、サポートサイトやメールで事前に通知いたします。

#### **12.1.3 容量・能力の管理**

安定的なサービス提供を行うため、各サーバーのリソースを監視し、必要に応じてキャパシティの増強を行っています。

#### **CLD.12.1.5 実務管理者の運用のセキュリティ**

本サービスの操作方法は、各種マニュアルを提供しています。

#### **12.3.1 情報のバックアップ**

本サービスでは、利用者が実施可能なバックアップ機能は提供していません。システムおよびお客様情報資産は、当社が日々の運用プロセスとしてバックアップの取得・管理を実施しています。障害復旧時点は前日バックアップ取得時点となります。バックアップデータは暗号化を行い保管しています。(10.1.1 暗号による管理策の利用方針に記載の通りです。)

#### **12.4.1 イベントログ取得**

当社の責任範囲において、本サービスの維持管理に必要な適切なログを取得しています。問題が発生し、ログが必要な場合は、本サービスサポート窓口までお問い合わせください。

#### **12.4.4 クロックの同期**

本サービスでは NTP サーバーを参照することで時刻を同期（日本標準時）しています。

#### **CLD.12.4.5 クラウドサービスの監視**

ネットワークおよび CPU・メモリ等の使用率増加を検知する監視は、当社が実施しています。

#### **12.6.1 技術的脆弱性の管理**

定期的に脆弱性情報の収集を実施し、当社の責任の範囲で対応が必要となった場合には、定期または緊急メンテナンスにて対応を実施します。メンテナンス情報はサポートサイトやメールで通知いたします。

#### **13.1.3 ネットワークの分離**

本サービスの管理者は、専用のテナント経由でのみ本サービスにアクセスし、他の利用者のネットワークと分離しています。

#### **14.1.1 情報セキュリティ要求事項の分析および仕様化**

当社では、情報セキュリティ方針の下で、お客様が要求される情報セキュリティを維持、提供しています。主にお客様が検討される情報セキュリティの機能の仕様として、当ホワイトペーパーは以下の項目を記載しています。

- ・ アクセス制限機能（9.4.1 情報へのアクセス制限、CLD.9.5.2 仮想マシンの要塞化）
- ・ 通信暗号化機能（10.1.1 暗号による管理策の利用方針）
- ・ バックアップ機能（12.3.1 情報のバックアップ）
- ・ ログ取得機能（12.4.1 イベントログ取得）

#### **14.2.1 セキュリティに配慮した開発のための方針**

当社では、セキュリティに配慮した開発方針として、開発時点からセキュリティに関するリスク対応、脆弱性対応を行い、初期リリース時及び大幅な変更を伴うメンテナンス時に脆弱性診断、及びネットワーク診断を行っています。

#### **15.1.2 供給者との合意におけるセキュリティの取扱い**

情報セキュリティにおける役割及び責任、本サービスの責任分界点に関しては「6.1.1 情報セキュリティの役割および責任」をご参照ください。

#### **15.1.3 ICT サプライチェーン**

当社が利用するクラウドサービスプロバイダの情報セキュリティ水準を把握し、本サービスの情報セキュリティとの整合性が取れていることを確認しています。本サービスは、AWS をクラウドサービスプロバイダとして運用しています。AWS のコンプライアンス状況については下記をご参照下さい。

<https://aws.amazon.com/jp/compliance/>

#### **16.1.1 責任および手順**

利用者に大きな影響を与えるセキュリティインシデント(データの消失、長時間のシステム停止等)が発生した場合は、サービスレベルに基づきメールで通知いたします。サービスレベルについては本サービス利用規約、SLA についてをご確認ください。セキュリティインシデントに関する問合せは、本サービスサポート窓口で受け付けています。

#### **16.1.2 情報セキュリティ事象の報告**

サポートサイトで掲載いたします。また個別のお問い合わせは、本サービスサポート窓口で受け付けています。

#### **16.1.7 証拠の収集**

裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、利用者の同意なく、利用者のデータを当該機関に開示することがあります。詳細は、本サービス利用規約をご確認ください。なお、お客様に重要なインシデントが発生し、実態調査を目的としたログ情報等が必要な場合には本サービスサポート窓口までお問い合わせください。

### **18.1.1 適用法令および契約上の要求事項の特定**

本サービスの利用に関して、適用される「準拠法」は「日本法」となります。本サービス運用に関連する各種法令に関しては関連法規管理要領に従い、法的準拠するように努めています。

### **18.1.2 知的財産権**

本サービスをご利用いただく上で知的財産権に関わるお問い合わせは、本サービスサポート窓口までお問い合わせください。

### **18.1.3 記録の保護**

利用者の本サービスご利用に関して蓄積された記録に対しては、不正アクセス・改ざんなどを防ぐためアクセス制限を実施しています。

### **18.1.5 暗号化機能に対する規制**

本サービスでは、SSL/TLS（TLS 1.2/TLS 1.3 対応）による通信の暗号化を使用しています。

### **18.2.1 情報セキュリティの独立したレビュー**

当社では、社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、ISO/IEC 27001、ISO/IEC27017 に基づく第三者による認証審査を受け、情報セキュリティに対する取り組みを行うことで、安全なセキュリティレベルを確保します。

（2026年4月 ISO/IEC27017 認証取得予定）