ISO/IEC 27017 ホワイトペーパー

第 1 版

2024/7/26

ＣＨＲＯＦＹ株式会社

1. はじめに

このホワイトペーパー（以下、「本書」）は、ISMS クラウドセキュリティ認証「JIP-ISMS5517-1.0（ISO/IEC 27017:2015）」で求められている要求事項について、ＣＨＲＯＦＹ株式会社（以下「当社」）が提供する CHROFY（以下、「本サービス」）における具体的な取り組みをご理解いただくことを目的としています。

2. 適用範囲

本書は当社が提供する以下のサービスに適用されます。

・CHROFY

3. 用語の定義

本書における用語の定義は次の通りです。

a) クラウドコンピューティング
クラウド環境上でサーバー、ストレージ、ネットワークなどのサービスを利用することを指します。

b) クラウドサービスカスタマ
ここでは、本サービスをご利用いただくお客様を指します。

c) クラウドサービスプロバイダ
ここでは、本サービスを提供する当社を指します。

d) 特権的なユーティリティプログラム
ここでは、通常の認証手順を経ずに利用可能なプログラム（機能）を指します。

e) 仮想マシン
物理的なコンピュータ上に疑似的なコンピュータを作成することを指します。

f) クロック
情報システムにおける時刻を指します。

g) 供給者
ここでは、本サービスを提供するにあたり当社が利用している他事業者を指します。

h) ICT サプライチェーン

ここでは、情報通信技術（ICT）である本サービスを提供するにあたり当社が利用・調達している他事業者のサービス・製品（AWS 等）を指します。

4. ISO/IEC 27017

クラウドサービスに関する情報セキュリティ管理策のガイドライン規格であり、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である ISO/IEC 27001 の取り組みを ISO/IEC 27017 で強化することで、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することを目的としています。

5. 本サービスにおける責任分界

本サービスにおける当社及び当社及び他事業者とお客様との責任分界は次のようになります。

<table>
<tr><td>本サービス上に保存されたデータ</td><td rowspan="2">お客様の責任範囲</td></tr>
<tr><td>ネットワーク（インターネットへの接続）</td></tr>
<tr><td>アプリケーション</td><td rowspan="2">当社の責任範囲</td></tr>
<tr><td>他事業者（トレンドマイクロ）</td></tr>
<tr><td>仮想化層（ハイパーバイザー）</td><td rowspan="4">他事業者（当社が利用する IaaS など）の責任範囲</td></tr>
<tr><td>ネットワーク（バックボーン）</td></tr>
<tr><td>物理設備（サーバー、ネットワーク設備など）</td></tr>
<tr><td>土地・建物</td></tr>
</table>

6. 各管理策への対応

以下、ISO/IEC 27017 で求められている各管理策に関する当社の具体的な取り組みを記載します。管理策の項番は ISO/IEC 27017 に基づきますが、カッコ内の項番は ISO/IEC 27001:2022（ISO/IEC 27017 がまだ対応していない新規格）における対応項番を示しています。

5.1.1　情報セキュリティのための方針群（新規格 5.1）

当社は、当社の定めた情報セキュリティ方針に従ってサービスを運営します。詳細はこちらをご確認ください。

6.1.1　情報セキュリティの役割及び責任（新規格 5.2）

当社とお客様との間の責任分界は「５．本サービスにおける責任分界」でご説明しています。

6.1.3　関係当局との連絡（新規格 5.5）

当社の所在地は当社 HP をご確認ください。また、本サービスにおいて保存されるデータが保管される可能性のある国は日本国です。

CLD6.3.1　クラウドコンピューティング環境における役割及び責任の共有及び分担

本サービスに関する事項は CHROFY 利用規約をご確認ください。また、責任分界については「５．本サービスにおける責任分界」でご説明しています。

7.2.2　情報セキュリティの意識向上、教育及び訓練（新規格 6.3）

当社は本サービスの提供にあたり、当社の従業員に対して情報セキュリティの重要性を認識させるため、定期的な教育・訓練を実施しています。

8.1.1　資産目録（新規格 5.9）

当社内で整備している情報資産の目録において、本サービスを利用するお客様のデータ及びその派生データを識別し、管理しています。

CLD8.1.5　クラウドサービスカスタマの資産の除去

お客様が本サービスの利用を終了された場合、お客様のアカウント情報及びお客様が本サービスに保存されたデータは解約から 30 日以内に削除されます。但し、お客様の情報を含まないログデータ等は除外されます。

8.2.2　情報のラベル付け（新規格 5.13）

本サービスでは、お客様が保存されたデータに対してラベル付けを行うことのできる機能を提供していません。

9.2.1　利用者登録及び登録削除（新規格 5.16）

本サービス利用開始時に、お客様よりお申込み頂いた利用者数に応じて当社が ID を発行しています。利用者の登録・削除については、account-mgt@chrofy.co.jp 宛てにメールで受け付け、3 営業日以内に設定を完了します。

9.2.2　利用者アクセスの提供（新規格 5.18）

管理者権限によって、お客様が利用する領域に対するアクセス権限（管理者ユーザー、グループ会社閲覧ユーザー、一般閲覧ユーザー、データ更新ユーザー等）を操作することができます。詳細はご利用ガイドをご覧ください。

9.2.3　特権的アクセス権の管理（新規格 8.2）

ID・パスワードによる認証方法に加え、二段階認証等の認証方法をご利用いただくことが可能です。

9.2.4　利用者の秘密認証情報の管理（新規格 5.17）

本サービス利用開始時に、管理者権限を有した ID を提供しています。

9.4.1　情報へのアクセス制限（新規格 8.3）

管理者権限によって、CHROFY が生成する分析結果（ダッシュボード）に対するアクセス制限を行うことができます。詳細はご利用ガイドをご覧ください。

9.4.4　特権的なユーティリティプログラムの利用（新規格 8.18）

本サービスの利用を支援する特権的なユーティリティプログラムはありません。

CLD9.5.1　仮想コンピューティング環境における分離

本サービスにおいてお客様が利用する仮想マシンやネットワークは、仮想化技術等を通してお客様ごとに論理的な分離を行っています。

CLD9.5.2　仮想マシンの要塞化

仮想マシンの要塞化については当社が利用するクラウドサービス（ＡＷＳ）のポリシーに基づいて実施されています。

10.1.1　暗号による管理策の利用方針（新規格 8.24）

本サービス利用における通信は SSL/TLS 通信を利用可能です。サービス上のデータに対しては AWS KMS（Key Management Service）によって暗号化されます。

11.2.7　装置のセキュリティを保った処分又は再利用（新規格 7.14）

故障などにより交換となった記憶媒体の処理については、AWS のポリシーに基づき適切に処分されます。

12.1.2　変更管理（新規格 8.32）

お客様に何らかの影響を及ぼす可能性のあるサービスの変更については、事前に通知を行っています。

12.1.3　容量・能力の管理（新規格 8.6）

各種リソースについては当社内で日々監視を行うか、又は自動的に増強・増設を行っております。

CLD12.1.5　実務管理者の運用のセキュリティ

本サービスでは以下のマニュアルをご用意しております。
・CHROFY 運用手順

12.3.1　情報のバックアップ（新規格 8.13）

本サービスの提供に用いている仮想環境は、日次又は週次でバックアップを取得しており、最低 1 カ月以上世代保管しております。

12.4.1　イベントログ取得（新規格 8.15）

本サービスにおけるイベントログは、当社側で取得・管理しており、現時点ではお客様への開示は行っておりません。

12.4.4　クロックの同期（新規格 8.17）

本サービスに関わるシステムは NTP により単一の参照時刻源と同期させています。

CLD12.4.5　クラウドサービスの監視

本サービスに関わるネットワーク及びメモリ・ストレージ等の監視は当社において日々実施しております。

12.6.1　技術的脆弱性の管理（新規格 8.8）

当社では定期的に本サービスに関わる脆弱性情報の収集・分析を行い対策を行っています。

13.1.3　ネットワークの分離（新規格 8.22）

本サービスではサーバレスを採用しているため、お客様毎のネットワーク分離は行っておりません。

CLD13.1.4　仮想及び物理ネットワークのセキュリティ管理の整合

物理ネットワークと仮想ネットワークの整合が取れるよう、当社の定める管理手順に基づき設計・構築・管理を行っています。

14.1.1　情報セキュリティ要求事項の分析及び仕様化（新規格 5.8）

本サービスの仕様については CHROFY 情報セキュリティ仕様をご覧ください。

14.2.1　セキュリティに配慮した開発のための方針（新規格 8.25）

当社の定める開発手順に則った開発を行うとともに、定期的な脆弱性診断などを実施しています。

15.1.2　供給者との合意におけるセキュリティの取扱い（新規格 5.20）

責任分界については「5．本サービスにおける責任分界」でご説明しています。その他の詳細は CHROFY 利用規約をご覧ください。

15.1,3　ICT サプライチェーン（新規格 5.21）

本サービスの提供に必要となる構成要素について外部から供給を受ける場合、当社のセキュリティポリシーに基づき当社と同等のセキュリティ水準を満たすことを確認しています。

16.1.1　責任及び手順（新規格 5.24）

当社で確認したセキュリティインシデントについては、当社のインシデント対応手順に基づき速やかに対応します。発生したインシデントがお客様に重大な影響を及ぼすと判断した場合はお客様に通知を行っています。

16.1.2　情報セキュリティ事象の報告（新規格 6.8）

お客様が発見されたセキュリティ事象についてはお問い合わせ窓口にて報告いただくことができます。

16.1.7　証拠の収集（新規格 5.28）

法令等に基づき捜査機関・裁判所等から情報の開示を求められた場合、お客様への通知又は同意を得ることなく開示することがあります。この点について、CHROFY 利用規約において合意を頂いております。

18.1.1　適用法令及び契約上の要求事項の特定（新規格 5.31）

本サービスの利用に関して適用される法令は「日本法」です。

18.1.2　知的財産権（新規格 5.32）

知的財産権に関するお問い合わせはお問い合わせ窓口をご利用ください。

18.1.3　記録の保護（新規格 5.33）

当社の責任範囲内で、必要なログを取得しています。

18.1.5　暗号化に対する規制（新規格 8.24）

本サービスへのアクセスについては SSL/TLS 通信が利用可能です。輸出規制の対象となる暗号化機能は提供しておりません。

18.2.1　情報セキュリティの独立したレビュー（新規格 5.35）

ISO/IEC 27001 及び ISO27017 に基づく内部監査を定期的に実施しており、その他外部審査機関による認証審査を毎年受審しています。