ISO/IEC 27017

セキュリティホワイトペーパー

第1.0版

2025年9月

キヤノンITソリューションズ株式会社

© Canon IT Solutions Inc.

目次

目次

1.はじめに 4
1.1 ホワイトペーパーの目的 4
1.2 本書の適用範囲 4
2.EDI-Master Cloudについて 5
2.1 EDI-Master Cloudとは 5
2.2 責任分界点について 5
3. ISO/IEC 27017：2015（JIS Q 27017：2016）への対応 6
3.1 管理策に関する見方の説明 6
3.2 各管理策への対応について 6
5.1.1 情報セキュリティのための方針群 6
6.1.1 情報セキュリティの役割および責任 6
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自覚、教育および訓練 7
8.1.1 資産目録 7
CLD.8.1.5 クラウドサービスカスタマの資産の除去 7
8.2.2 情報のラベル付け 7
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（provisioning） 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

© Canon IT Solutions Inc.

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または再利用 9
12.1.2 変更管理 9
12.1.3 容量・能力の管理 10
CLD.12.1.5 実務管理者の運用のセキュリティ 10
12.3.1 情報のバックアップ 10
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 技術的ぜい弱性の管理 11
13.1.3 ネットワークの分離 11
CLD.13.1.4 仮想および物理ネットワークのセキュリティ管理の整合 11
14.1.1 情報セキュリティ要求事項の分析および仕様化 11
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 12
15.1.3 ICT サプライチェーン 12
16.1.1 責任および手順 12
16.1.2 情報セキュリティ事象の報告 12
16.1.7 証拠の収集 12
18.1.1 適用法令および契約上の要求事項の特定 13
18.1.2 知的財産権 13
18.1.3 記録の保護 13
18.1.5 暗号化機能に対する規制 13
18.2.1 情報セキュリティの独立したレビュー 13
4.変更履歴 13

© Canon IT Solutions Inc.

1.はじめに

1.1 ホワイトペーパーの目的

「ISO/IEC27017 セキュリティホワイトペーパー」(以下、本書)は、クラウドセキュリティの国際規格(ISO/IEC27017)で求める要求事項に対して、キヤノンITソリューションズ株式会社(以下、当社)がクラウドサービスプロバイダ(CSP)として実施する管理策をご確認いただくことを目的としています。

1.2 本書の適用範囲

本書の適用範囲は、当社が提供するクラウドEDIサービス「EDI-Master Cloud」のサービス全体です。

© Canon IT Solutions Inc.

2.EDI-Master Cloudについて

2.1 EDI-Master Cloudとは

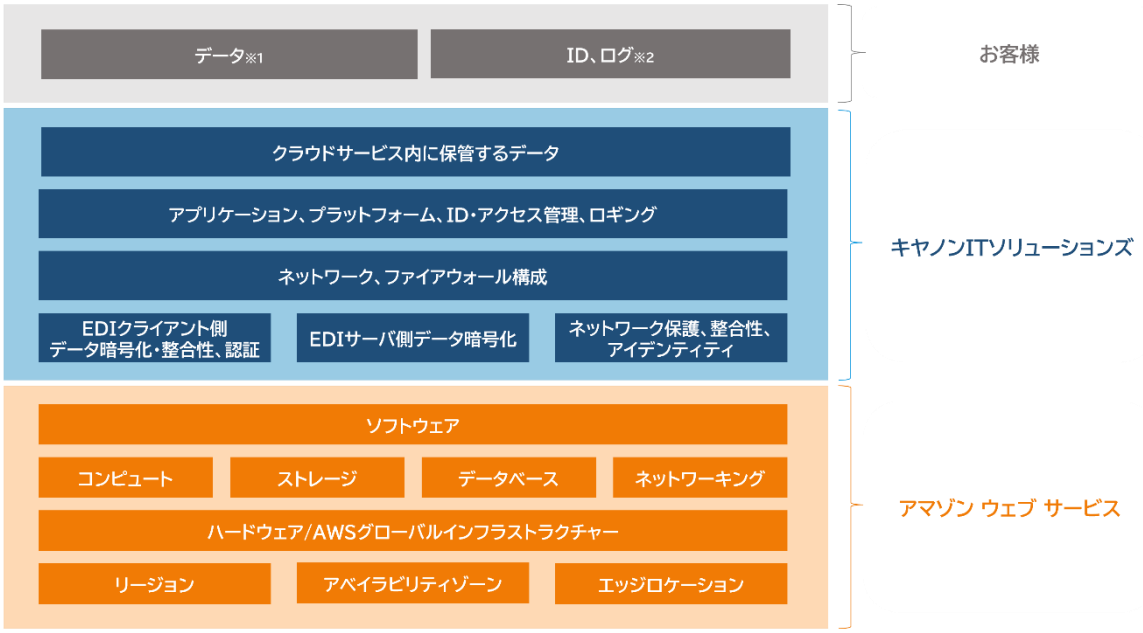
電子商取引(EDI)の各種機能をクラウド上で利用可能にするEDIサービス基盤です。通信・変換・運用管理機能を備える他、EDIの各種機能をWeb APIで提供し、Open APIを介して様々な製品/サービスとの連携を実現します。

2.2 責任分界点について

アマゾン ウェブ サービスと当社の間においては、責任共有モデル※が適用され、クラウドサービス提供上のセキュリティ責任はアマゾン ウェブ サービスと当社の間で共有されています。

お客様は、お客様の管理範囲において、情報セキュリティを含めた一切の責任を負うものとします。当社は、当社の管理範囲において、サービス提供・維持管理・セキュリティ対策を実施しています。

※アマゾン ウェブ サービスの責任共有モデル:
https://aws.amazon.com/jp/compliance/shared-responsibility-model/



※1:クラウドサービスにアップロードした元データ、またはクラウドサービスからダウンロードしたデータ
※2:クラウドサービスにアクセスするためのID、クラウドサービスにアクセスした際のクライアント側ログ

© Canon IT Solutions Inc.

3. ISO/IEC 27017 : 2015（JIS Q 27017 : 2016）への対応

3.1 管理策に関する見方の説明

ISO/IEC 27017:2015（JIS Q 27017:2016）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 、ISO27017 が求める”情報セキュリティ管理策の実践の規範”箇条 5～18（17 箇条を除く）の小項番番号・要求事項原文を示し、後に続く内容は、当社サービスの要求事項に対する解釈および管理策になります。

3.2 各管理策への対応について

ISO/IEC 27017 は、ISO/IEC27002 と共通する管理策について同じ項番が付与されていますので、ISO/IEC27001 付属書A の項番とも一致します。クラウド特有の拡張された管理策については、「付属書A（規定）クラウドサービス拡張管理集」として、頭に「CLD」がつく項番が指定されています。頭に「CLD」がつく管理策についても、そのあとに続く番号は、ISO/IEC 27001付属書 A およびISO/IEC 27002で定められた番号とも整合がとられています。

以下、項番の順に沿ってクラウドサービスプロバイダ（以下、クラウドサービス提供者）としての取り組みについて解説を行います。

5.1.1 情報セキュリティのための方針群

本サービスは、当社の定めた情報セキュリティ基本方針に従い、サービス運営を行います。

詳細は、情報セキュリティ基本方針
（https://corporate.jp.canon/sustainability/governance/security/policy）をご覧ください。

6.1.1 情報セキュリティの役割および責任

責任分界点については、本書の「2.2 責任分界点について」で明記しています。

© Canon IT Solutions Inc.

6.1.3 関係当局との連絡

当社の所在地は、ホームページ(https://www.canon-its.co.jp/)でご確認ください。

なお、当社が提供するクラウドサービスに保存された情報の所在は日本国内となります。

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

役割および責任は、本書の「2.2 責任分界点について」に記載しています。また、本サービス利用については、サービス約款をご確認ください。

7.2.2 情報セキュリティの自覚、教育および訓練

当社は、クラウドサービス提供者として、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、クラウド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ためのセキュリティ対策を実施しています。

8.1.1 資産目録

EDI-Master Cloudでは、お客様の情報資産(お客様データ)と、当社がサービスを運営するための情報は明確に分離しています。

CLD.8.1.5 クラウドサービスカスタマの資産の除去

本サービスの利用契約が終了した場合に、お客様が作成・保存した情報資産(お客様データ)に関して、約款および「解約申込書」の合意内容に従い、解約日翌日より利用停止し、30 日後に削除します。

8.2.2 情報のラベル付け

本サービスは、接続先毎の定義および接続先に紐づくファイル定義を設定・編集する機能を有しており、接続先定義・ファイル定義の分類・整理・識別が可能です。

© Canon IT Solutions Inc.

9.2.1 利用者登録および登録削除

ユーザーの登録・変更・削除の機能が、ご利用いただけます。提供機能の利用にあたっては、取扱説明書をご参照ください。

9.2.2 利用者アクセスの提供（provisioning）

ユーザー権限（機能制限設定）を管理する機能を提供しており、管理者の権限を有するユーザーが設定可能です。提供機能の利用にあたっては、取扱説明書をご参照ください。

9.2.3 特権的アクセス権の管理

ユーザーID／パスワード認証に加え、ワンタイムパスワードによる二要素認証機能を提供しています。

9.2.4 利用者の秘密認証情報の管理

本サービスは、クラウドサービス利用者のユーザーID、パスワードを管理する機能を提供しています。パスワードの発行、変更等の管理手順や、パスワード要件（桁数、文字の種類等）については、取扱説明書をご参照ください。

9.4.1 情報へのアクセス制限

管理者権限を有する利用者によってユーザーのアクセス権・機能制限の設定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

本サービスでは、特権的ユーティリティプログラムを利用する当社運用担当者を制限し、定期的にアクセスログのレビューを実施し、不正な利用がないことを確認しています。

本サービスにおいて、お客様へのユーティリティプログラムの提供はしていません。

© Canon IT Solutions Inc.

CLD.9.5.1 仮想コンピューティング環境における分離

本サービスでは、テナントIDによりお客様のデータを論理的に分離して管理しています。

CLD.9.5.2 仮想マシンの要塞化

当社は、クラウドサービス提供者として、構築するすべての仮想化環境で、以下のセキュリティ対策を実施しています。

① 必要なポートだけを有効としています。
② 必要なプロトコルだけを有効としています。
③ マルウェア対策を実施しています。
④ ログの取得を実施しています。

10.1.1 暗号による管理策の利用方針

本サービスでは、以下のとおり暗号化によるセキュリティ対策を適用しています。

① クラウドサービス利用者の各種情報
本サービスに入力・保存したデータは、バックアップデータを含め暗号化して保存されています。
② クラウドサービスとの通信
本サービス利用におけるデータ通信は、すべてTLSによる暗号化を使用した通信となります。

11.2.7 装置のセキュリティを保った処分または再利用

装置のセキュリティを保った処分又は再利用は、当社が本サービスの提供にあたり利用しているクラウドサービス提供事業者(アマゾン ウェブ サービス)の責任範囲となります。当社では、適切なプロセスで対応することを確認した上でサービスを利用しています。

12.1.2 変更管理

機能の動作や画面表示の大幅な変更を行う際にお客様に影響があると判断した場合には、事前にメールにて通知を行います。

© Canon IT Solutions Inc.

12.1.3 容量・能力の管理

容量・能力の監視は、当社が定める閾値を超えるとオートスケールする仕組みを設けています。

CLD.12.1.5 実務管理者の運用のセキュリティ

本サービスでは、サービスの利用に必要な操作方法を、各種「取扱説明書」として提供しています。

12.3.1 情報のバックアップ

本サービスでは、稼働中のリージョンとは異なるリージョン(国内)へのバックアップを日次で取得し、3年間保持しています。バックアップは、サービスのシステム障害や大規模災害発生時を想定し取得するもので、原則、個別の復旧依頼に応じるものではありません。お客様が実施可能なバックアップ機能は提供していません。

12.4.1 イベントログ取得

サービスの維持・管理に必要な範囲にて、適切なログを取得しています。また。テナント内でのイベントログ(操作履歴・実行履歴)を参照する機能を提供し、お客様による閲覧、検索が可能です。

12.4.4 クロックの同期

本サービスでは、アマゾン ウェブ サービスが提供するNTPサービス(Amazon Time Sync Service)を用いて時刻を同期しており、日本時間(JST, UTC+0900)で管理しています。

CLD.12.4.5 クラウドサービスの監視

安定的にサービスを提供するため、日々のサービスの監視および各種パフォーマンスの監視は、当社にて行っています。正常な動作をしていなかったことを検出した場合は、お客様に通知の上、対応することがあります。また、お客様においては、操作履歴の取得により不正操作の監視を実施することができます。

© Canon IT Solutions Inc.

12.6.1 技術的ぜい弱性の管理

OS、ミドルウェア、OSS等のセキュリティ情報を収集し、リスクに応じてパッチ適用を実施しています。

脆弱性が検出された場合は、重要度に応じてお客様窓口に対してメール連絡およびサービス管理画面で通知します。

13.1.3 ネットワークの分離

サービス提供者用の管理ネットワークと利用者がサービス機能を利用するネットワークは、適切に分離されています。

CLD.13.1.4 仮想および物理ネットワークのセキュリティ管理の整合

当社は、アマゾン ウェブ サービスが提供している環境を利用した SaaS 型のクラウドサービスを提供しています。

14.1.1 情報セキュリティ要求事項の分析および仕様化

当社のクラウドサービスで実装している情報セキュリティ対策および機能は、当セキュリティホワイトペーパーに記載しています。

8.2.2 情報のラベル付け
9.2.1 利用者登録及び登録削除
9.2.2 利用者アクセスの提供
9.2.3 特権的アクセス権の管理
9.2.4 利用者の秘密認証情報の管理
9.4.1 情報へのアクセス制限
9.4.4 特権的なユーティリティプログラムの使用

14.2.1 セキュリティに配慮した開発のための方針

当社で取り決められたガイドライン(コーディング規約)に従ったプログラム開発、およびレビューを実施しています。また、提供中のサービスにおいても第三者機関による脆弱性診断を実施しています。

© Canon IT Solutions Inc.

15.1.2 供給者との合意におけるセキュリティの取扱い

責任分界点の詳細に関しては本書の「2.2 責任分界点について」をご参照ください。

また、セキュリティ対策に関しても「2.2 責任分界点について」に記載する当社サービスの提供範囲において必要なセキュリティ対策を実施しています。

15.1.3 ICT サプライチェーン

当社は、本サービスの提供にあたり利用しているクラウドサービス提供事業者(アマゾン ウェブ サービス)の情報セキュリティ水準を把握した上で、当社の「情報セキュリティ基本方針」に則り、適切なリスク管理を実施しています。

16.1.1 責任および手順

当社で確認できた情報セキュリティインシデントに関しては、情報セキュリティ基本方針に則り、適切に対応しています。また、確認できた情報セキュリティインシデントがお客様に重大な影響を及ぼす可能性がある場合には、当社公開基準に従い、検知から1営業日を目標に発生事象と対処方法についてサポートセンターからお客様窓口に対してEDI-Master Cloudお知らせ画面、サポートサイトおよびメールで通知を行います。

16.1.2 情報セキュリティ事象の報告

情報セキュリティインシデントが発生した場合には、サポートセンターよりEDI-Master Cloudお知らせ画面、サポートサイトおよびメールでお客様窓口に報告いたします。また、お客様が発見した情報セキュリティインシデントの報告、情報セキュリティインシデントに関するお問い合わせはサポートセンターまでホームページ・電話のいずれかの方法でご連絡ください。

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、お客様の情報資産を開示することについて、利用規約に合意いただく必要があります。

© Canon IT Solutions Inc.

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。

18.1.2 知的財産権

知的財産権に関わるお問い合わせは、当社サポートセンターへお問い合わせください。

18.1.3 記録の保護

各種アクセスログについて、原則として当日を含む過去365日分の記録をお客様にて参照できる機能を提供しています。

18.1.5 暗号化機能に対する規制

本サービス利用におけるデータ通信は、すべてTLSによる暗号化機能を使用した通信となります。

なお、輸出規制の対象となる暗号化機能の利用はありません。

18.2.1 情報セキュリティの独立したレビュー

当社では、情報セキュリティの有効性を確認するために、本サービスの提供部門とは独立した別部門による内部監査を年1回実施しています。あわせて、ISO/IEC 27001およびISO/IEC 27017に基づく第三者機関による定期的な審査を受け、認証を維持しています。

4.変更履歴

版数	日付	変更内容
第1.0版	2025/9/1	初版公開

© Canon IT Solutions Inc.