SYNCDOT MailAuditSaaS
ホワイトペーパー

第 1.7 版

2024 年 3 月

富士通 Japan(株)

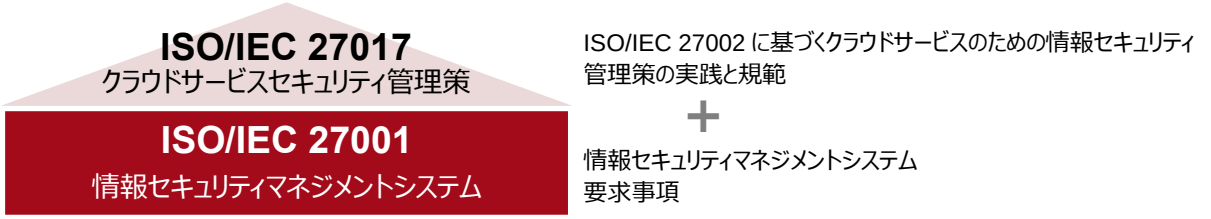
目　次

1 はじめに

1.1 ホワイトペーパーの目的

このホワイトペーパー(以下、本書)は、クラウドセキュリティの国際規格(ISO/IEC 27017 : 2015)で求める要求事項に対して、実施する管理策を確認いただくことを目的としています。

ISO/IEC 27017 は、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 で強化した管理策のガイドライン規格になります。本書では、このガイドラインの”情報セキュリティ管理策の実践の規範”箇条 5～18 に沿って管理策を記載しています。



1.2 本書の適用範囲

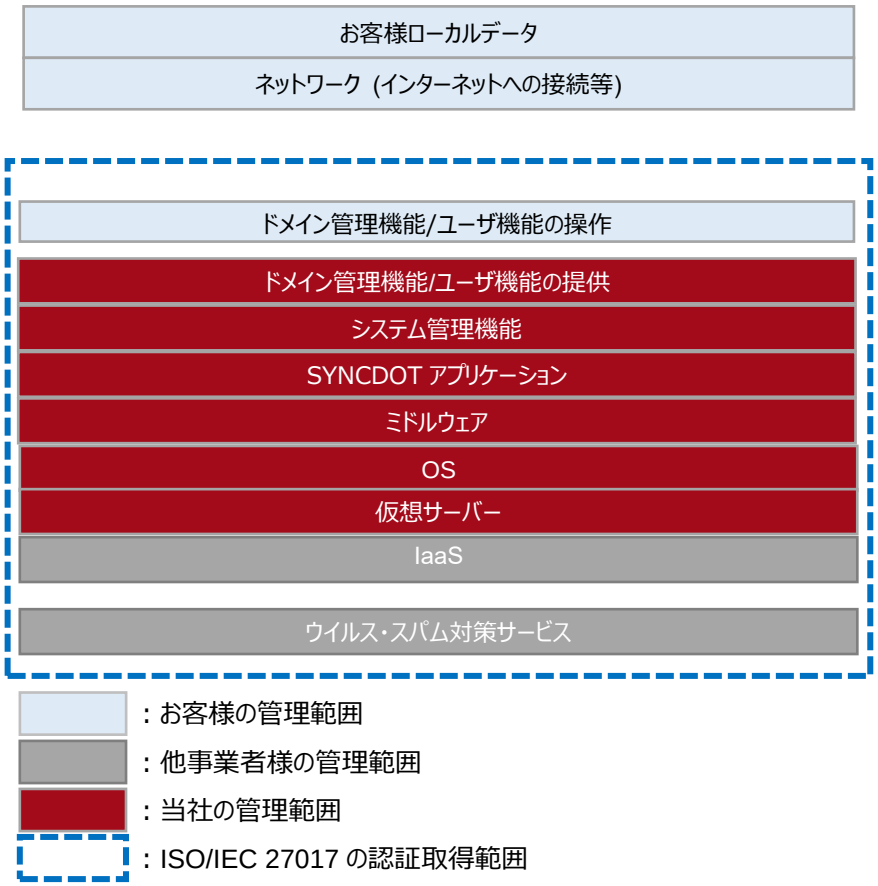
本書の適用範囲は、以下のクラウドサービスとなります。

- SYNCDOT MailAudit SaaS……SaaS 型メールアーカイブ、メールコンプライアンス対策サービス

機能概要は以下サイトを参照ください。
https://www.fujitsu.com/jp/solutions/enterprise-solutions/business-applications/syncdot/mailaudit/
機能の詳細に関しては、各種マニュアルをご参照下さい。
サポートサイト→マニュアル

1.3 責任分界点について

責任分界点は、以下になります。



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

5.1.1 情報セキュリティのための方針群

クラウドサービスの提供及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。

富士通グループの基本方針に従います。

情報セキュリティ基本方針 https://www.fujitsu.com/jp/about/csr/security/

6.1.1 情報セキュリティの役割及び責任

サービス仕様書及び利用規約にて契約やサービスの内容を定義し、サービス提供を実施しています。サービスの責任については「利用規約 第 19 条」セキュリティの確保については「利用規約第 24 条」に記載しています。

また、サービスご利用中に発生したセキュリティ等の問い合わせ対応に関しては、サポートサイトからお問い合わせいただくことができます。

6.1.3 関係当局との連絡

弊社の本社所在地は、 東京都港区東新橋 1-5-2 (汐留シティセンター)であり、
運用拠点は、長野県長野市鶴賀緑町 1415 大通りセンタービルです。

本サービスで保存されるデータの所在は FJcloud-V（旧名称：ニフクラ、ニフティクラウド）上にあり、全て日本国内です。

CLD.6.3.1 クラウドコンピューティング環境内の役割分担及び責任

責任分界点に関しては前出の「責任分界点について」を参照下さい。

弊社責任範囲でサービスの機密性、完全性、可用性を保つように最善を尽くします。

7.2.2 情報セキュリティの意識向上、教育及び訓練

情報セキュリティ要件やサービスの運用ルール周知徹底を目的として、サービスに従事する要員を対象とし、意識向上のための教育・訓練を実施しています。

また、本サービスをご利用するにあたって、お客様にもセキュリティ意識向上のための教育・訓練などを実施していただくことを望みます。

8.1.1 資産目録

サービス利用者様の情報資産(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おります。なお、サービス上に利用者様が作成・保存する情報資産は、利用者様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

本サービス利用によって生成されたデータの除去に関しては、サービス解約から 30 日以内に実施されます。

データのバックアップ等が必要となる場合には、サービス解約までに対応を実施して下さい。

但し、「18.1.3 記録の保護」に記載の通り、お客様操作ログなどはサービス解約後も 3 ヶ月間保存されます。

8.2.2 情報のラベル付け

メールにコメント を付与する機能などを提供しています。 機能の詳 細に関しては、 サポートサイト→マニュアル→ SYNCDOT MailAudit Viewer 利用者ガイド 4.4 メールを監査する をご参

照ください。

9.2.1 利用者登録及び登録削除

利用者を管理するドメイン管理者権限を提供します。管理者権限にて利用者の登録、削除を実施していただくことができます。

9.2.2 利用者アクセスの提供(provisioning)

管理権限、承認権限、閲覧 権限、 一般権限など、 利用者の権限 を 管理 する 機能を提供しています。機 能の詳 細に関しては、サポートサイト→マニュアル→ SYNCDOT MailAudit 管理者ガイド【組織管理者編】 3.2.2 利用者を追加する をご参照ください。

9.2.3 特権的アクセス権の管理

サービスの利用にあたって、ID/パスワードによる認証だけでなく、多要素認証を提供しています。機能の詳細に関しては、サポートサイト→マニュアル→各種 Web ログイン時 MFA 認証機能マニュアルをご参照ください。

9.2.4 利用者の秘密認証情報の管理

サービス開始時の管理権限については、サービス開始時に PDF で送付する「ご利用情報」に記載し、パスワード暗号化したうえでメールにて送付いたします。

お客様管理の利用者情報及び認証情報の登録/削除手順についてはサポートサイト→ご利用の手引き→[メールアドレスの登録/削除]をご参照ください。

尚、サーバに保持されたパスワード情報は AES256 で暗号化されています。

9.4.1 情報へのアクセス制限

サービスのご利用にあたっては、ドメイン管理権限を有している利用者によって、適切に各種機能を利用するユーザのアクセス制限を行う機能を提供しています。

9.4.4 特権的なユーティリティプログラムの使用

全てのサービス利用においては、認証が必要となっており、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

アプリケーションのマルチドメイン機能によって、各お客様のドメインが論理的に分離されており、分離されたドメインによるセキュリティ影響がないよう設計されています。

CLD.9.5.2 仮想マシンの要塞化

サービスの仮想化環境は、必要なポート、プロトコル、サービスだけを有効としています。
ファイアウォール機能などにより、ポート・プロトコル・IP アクセスの制限を実施しています。
また、必要なログを取得し３ヶ月保存しています。

10.1.1 暗号による管理策の利用方針

各機能への Web アクセスは SSL 暗号化通信を利用しています。
また、メールの添付ファイルを自動で ZIP 暗号化する機能を提供しています。

11.2.7 装置のセキュリティを保った処分又は再利用

サービスを構成する IaaS 事業者に対して、資源のセキュリティを保った処分又は再利用のため

の方針及び手順を確認したうえで、利用しています。
尚、サービスを構成する機器として、弊社の物理的装置はありません。

12.1.2 変更管理

サービスに悪影響を与える可能性のあるサービスの変更について、次のような事項をサポートサイト及びメールにて通知します。

・変更種別
・変更予定日及び予定時刻
・サービス及びその基礎にあるシステムの変更についての技術的な説明
・変更開始及び完了の通知

12.1.3 容量・能力の管理

安定的にサービスを提供するため、各サーバのキャパシティを明確にし、日々の運用プロセスの中で稼働監視を行っています。監視の結果としてシステムの増強が必要と判断された場合には、適切なタイミングにて、システムの増強を実施します。

CLD.12.1.5 管理者の運用セキュリティ

提供機能に関して、操作マニュアル、ご利用の手引き、ＦＡＱ、利用規約などをサポートサイトにて公開しています。

12.3.1 情報のバックアップ

サービス提供元としてメールデータやユーザ情報などを都度バックアップしていますが、これはサービス障害時の復旧に利用するバックアップです。
お客様操作メール削除、ユーザ削除など に よって生じたデータ消失に関しては、サービス提供元からの復元は実施いたしませんので、お客様責任でのバックアップをお願いします。

管理しているユーザ情報は CSV にてバックアップ可能です。
詳細は、サポートサイト→マニュアル→ SYNCDOT MailAudit 管理者ガイド【組織管理者編】→ 3.3 組織情報を CSV ファイルに抽出する をご参照ください。

メールデータはエクスポート機能によってバックアップ可能です。
詳細は、サポートサイト→マニュアル→ SYNCDOT MailAudit Viewer 利用者ガイド→ 8.1 メールのエクスポート をご参照ください。

12.4.1 イベントログ取得

弊社の責任範囲において、サービスの維持管理に必要となるログ、お客様操作ログ、メール送受信ログなどを取得していますが、そのログをお客様が取得する機能は提供していません。
お客様操作ログなどの確認が必要な場合はサポートサイトからお問い合わせください。

12.4.4 クロックの同期

サービスで利用する、仮想サーバーは適切な NTP サーバーを参照することで時刻を同期しています。システムのタイムゾーンは JST です。

CLD.12.4.5 クラウドサービスの監視

サービスの各種パフォーマンスや攻撃などの監視は、弊社が実施しておりますが、現在、結果をサービス利用者様に公開できるサービス機能は提供しておりません。確認結果が必要となる場合には、サポートサイトからお問い合わせください。

12.6.1 技術的ぜい弱性の管理

定期的にぜい弱性情報の収集を実施しています。
サービス側で対応が必要になった場合には、サポートサイト及びメールにて通知いたします。
また、利用者側で対応が必要となるぜい弱性情報があった場合にも、サポートサイト及びメールにて通知いたします。

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。
SaaS 型共用サービスのため、サービスを利用するためのネットワークはドメイン間で共有しています。

CLD.13.1.4 仮想及び物理ネットワークのためのセキュリティ管理の整合

物理ネットワークと論理ネットワークの整合がとれるよう設計したうえで、管理ルール・プロセスを徹底しています。

14.1.1 情報セキュリティ要求事項の分析及び仕様化

情報セキュリティに関しましては、情報セキュリティ基本方針および、サービス仕様書、当ホワイトペーパーに記載しています。
セキュリティ機能として以下のような機能を提供しています。
□フィルタルール　□上司承認　□添付ファイル難読化　□保存・監査
機能の詳細に関しては、サポートサイトの各種マニュアルなどで公開しています。

14.2.1 セキュリティに配慮した開発のための方針

本サービスは、富士通が定めるセキュリティ問診・診断を実施後、サービスを提供しています。また、提供中サービスにおいても年 1 回の定期診断にてセキュリティ対策を実施しています。

15.1.2 供給者との合意におけるセキュリティの取扱い

サービス契約時にサービス仕様書及び利用規約にて定義された事項に合意いただいたものとします。
責任分界点に関しては前出の「責任分界点について」を参照下さい。

15.1.3 ICT サプライチェーン

弊社が供給を受けている他事業者のサービスについて、供給者に対して、情報セキュリティ基本方針を示し、同等の情報セキュリティ水準を達成するための活動の実施を要求しています。

16.1.1 責任及び手順

弊社で確認できた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、適切に対応しております。
また、確認できたセキュリティインシデントがお客様に影響を及ぼす可能性がある場合においては、サポートサイト及びメールにて通知いたします。

16.1.2 情報セキュリティ事象の報告

弊社で確認したセキュリティインシデントがお客様に影響を及ぼす可能性がある場合には、サポートサイト及びメールにて通知します。
また、お客様から弊社に情報セキュリティ事象を報告いただく場合は、サポートサイトのお問い合わせから報告いただくことができます。

16.1.7 証拠の収集

「利用規約第 26 条」で定めている通り、利用者固有データが、国内外の関係法令に基づき参照、閲覧される可能性があることを合意いただくものとします。

18.1.1 適用法令及び契約上の要求事項の特定

「利用規約 第 31 条」で定めている通り、準拠法は原則として日本法とします。

18.1.2 知的財産権

知的財産権などに必要な情報の問い合わせは、サポートサイトからお問い合わせください。

18.1.3 記録の保護

弊社の責任範囲において、お客様操作ログなどを３ヶ月間取得しています。

また、お客様の契約情報の保護や廃棄については、社内規定に定め、定期的に検査を実施し、適切に管理しております。また、その利用については「利用規約 第 27 条」に定めています。

18.1.5 暗号化機能に対する規制

サービスで利用している暗号化機能において、輸出規制の対象となる暗号化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

プライバシーマーク、ISO/IEC 27001、ISO/IEC27017 の認証取得において第三者による審査を受け、それぞれの認証を取得していることで、情報セキュリティに対する取り組みの証憑としています。

3 改版履歴

版数	日付	更新内容
第 1.0 版	2019/09/01	初版公開
第 1.1 版	2019/09/25	軽微な文言修正
第 1.2 版	2020/07/20	5.1.1 情報セキュリティ基本方針の URL を修正
第 1.3 版	2021/04/01	・表紙の社名を変更 ・1.2 本書の適用範囲 サービス紹介サイトへのリンクを削除 ・5.1.1 情報セキュリティのための方針群 FJAS の記述を削除 ・10.1.1 暗号による管理策の利用方針 RC4,3DES の通信について明記 ・14.1.1 情報セキュリティ要求事項の分析及び仕様化 サービス紹介サイトへのリンクを削除
第 1.4 版	2021/10/01	・表紙の社名を変更 ・6.1.3 関係当局との連絡 本社所在地を修正
第 1.5 版	2022/08/01	・9.2.3 特権的アクセス権の管理 MFA 認証機能を追加
第 1.6 版	2023/09/01	・1.2 本書の適用範囲 SYNCDOT SaaS,SYNCDOT Communication SaaS の記載を削除 ・10.1.1 暗号による管理策の利用方針 RC4,3DES の制限について削除
第 1.7 版	2024/03/27	・名称表記見直（ニフクラ→FJcloud-V）