STAFee ホワイトペーパー

第 1.0 版

2025年12月

新日本コンピュータマネジメント株式会社

目 次

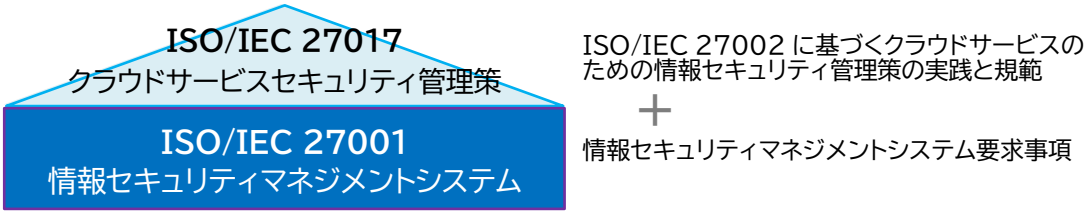
1 はじめに

1.1 ホワイトペーパーの目的

「STAFee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、実施する管理策をご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 (17 箇条を除く)に沿って管理策を記載しています。

当社は、全社を認証範囲として 2015 年 12 月 18 日に ISMS(Information Security Management System)の国際規格である ISO/IEC27001 を取得しています。



1.2 本書の適用範囲

本書の適用範囲は、STAFee(スタフィー)となります。
なお、STAFeeで提供する機能の詳細に関しては、以下サイトをご参照ください。

- STAFee機能紹介サイト
  https://stafee.scm-net.co.jp/function/

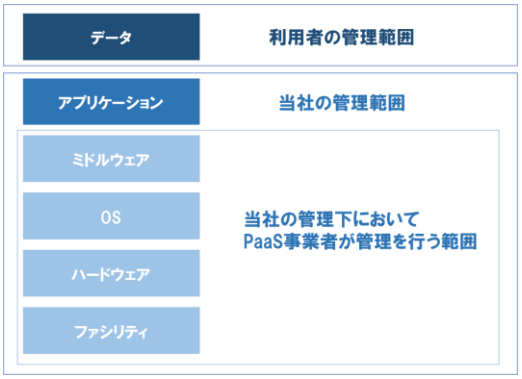
2 STAFeeについて

2.1 STAFee(スタフィー)とは

新日本コンピュータマネジメント株式会社が提供するSaaS(Software as a Service)型のクラウドサービスです。申請から承認まで電子化し、仕訳自動生成や会計ソフト連携機能で業務効率の向上とヒューマンエラーの防止に役立ちます。さらに、電子帳簿保存法にも対応し、法令遵守をサポートします。カスタマイズ性に優れ、多様な企業ニーズに対応し、総合的な業務改善を実現します。

2.2 責任分界点について

仮想レイヤーや施設におけるコンポーネントは、当社が基盤として利用するクラウドサービス事業者によって管理されます。当社は、当社のサプライヤーに対するセキュリティポリシーに従い、調達時のセキュリティ審査、及びパフォーマンスのモニタリングによりクラウドサービス事業者を管理します。
また、当社は、基盤上に構築したアプリケーションに対して責任を負います。
アプリケーション上のデータについては、お客様の責任において保護していただく必要があります。



当社の責任
・STAFeeのセキュリティ対策
・STAFeeに保管されたお客様情報の保護

お客様の責任
・利用者アカウントの管理(登録、削除、権限設定、管理者設定、アクセス権の設定など)
・パスワード等の利用者の秘密認証情報の管理
・お客様が取扱うデータに対してのバックアップ

3 ISO/IEC 27017：2015 への対応

3.1 STAFeeの管理策(3.2 節)に関する見方の説明

3.2 節で、ISO/IEC 27017:2015が求める要求事項に対する管理策を記載します。
「5.1.1 情報セキュリティのための方針群」などの番号・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)の小項目番号・要求事項原文を示し、後に続く内容は、STAFee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 STAFeeの管理策

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および利用に取り組むため、情報セキュリティ基本方針を拡充することが求められています。STAFeeでは、新日本コンピュータマネジメント株式会社 情報セキュリティ基本方針に従いサービスを運用しています。
・新日本コンピュータマネジメント株式会社 セキュリティ基本方針
https://www.scm-net.co.jp/security/

6.1.1 情報セキュリティの役割および責任

クラウドサービス契約書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。

6.1.3 関係当局との連絡

当社、新日本コンピュータマネジメント株式会社の本社所在地は東京都新宿区市谷本村町1番1号であり、STAFeeのサービス提供拠点は、大阪本社(大阪市北区堂島浜1丁目4番16号 アクア堂島NBFタワー8F)となります。また、STAFeeで保存頂くデータの所在は、日本国内のデータセンターとなります。

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

クラウドサービス契約書にて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。また、サービスに関するお問い合わせ先に関しては、当社営業日にメール・電話にて受け付けております。
なお、責任分界点に関しては前出の「2.2 責任分界点について」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。
また、STAFeeをご利用いただくにあたり、お客様によるセキュリティ意識向上のための教育・訓練の実施をおすすめいたします。

8.1.1 資産目録

お客様の情報資産(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、STAFee上にお客様が作成・保存する情報資産は、お客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

STAFeeの提供が終了した場合に、お客様が作成・保存した情報資産(保存データ)に関しては、解約日から30日が経過した日からさらに30日が経過するまでの期間内に全てのデータを消去いたします。当社にて取得した情報資産(保存データ)のバックアップについても合わせて破棄いたします。但し、お客様の情報資産を含まないサービス共通ログは対象外とします。

STAFeeの解約日までにデータの返還の申し入れがあった場合は、サービス解約日から30日が経過するまでの期間内に有償でデータの抽出および返還を行います。

8.2.2 情報のラベル付け

ご利用いただくSTAFeeの機能の詳細に関しては、各種マニュアル類も含めてSTAFeeマニュアルサイトにて公開しています。お客様情報資産を設定と運用方法によって分類することができ、閲覧権限も設定できる仕様になっています。

9.2.1 利用者登録および登録削除

STAFee利用開始時にご契約いただいた内容に従って、管理者権限を有する利用者IDを提供いたします。提供した利用者IDにて、STAFeeの運用に必要となる利用者の登録・更新・削除の機能がご利用頂けます。提供機能の利用にあたっては、STAFeeマニュアルサイトをご参照ください。

9.2.2 利用者アクセスの提供(provisioning)

STAFeeの機能として、利用者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

STAFeeの管理にあたっては、操作者ごとに一意の特権IDを設けております。
また、操作時のログの記録も行っています。

9.2.4 利用者の秘密認証情報の管理

STAFeeの初期利用時には、管理者権限を有する利用者ID・パスワードをメールにてご連絡しています。

初期パスワードは初回ログイン時に変更を求めるようになっています。パスワードの変更とパスワードポリシーの設定ついては、STAFeeマニュアルサイトをご参照ください。

9.4.1 情報へのアクセス制限

STAFeeのご利用にあたっては、管理者権限を有する利用者IDによって機能制限を行うことができます。また、接続が可能なIPアドレスを制限することができます。

9.4.4 特権的なユーティリティプログラムの使用

全ての機能においては、認証が必要となっており、セキュリティ手順を回避し各機能の利用を可能とするユーティリティプログラムは提供していません。

CLD.9.5.1 仮想コンピューティング環境における分離

STAFeeはマルチテナント環境でサービス提供していますが、お客様データはテナント毎に論理的に分離し、別テナントへの不正アクセスを抑止しています。

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アドレスの制限を実施しています。

10.1.1 暗号による管理策の利用方針

STAFeeのお客様パスワードは暗号化しています。STAFeeにてお客様データをやり取りする通信は、TLS 1.2以上の暗号化を強制する仕様を採用しています。また、データベースとストレージも暗号化しています。

11.2.7 装置のセキュリティを保った処分又は再利用

サービスを構成するクラウド事業者に対して、資源のセキュリティを保った処分または再利用のための方針および手順を確認したうえで、利用しています。

なお、サービスを構成する機器として、当社の物理的装置はありません。

12.1.2 変更管理

提供するサービスの変更を実施する場合、変更の内容と変更予定日時をメールにて通知します。提供サービスに変更が及ばない、定期メンテナンスの場合も通知します。

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、各テナント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、システムメンテナンスを実施します。

CLD.12.1.5 管理者の運用セキュリティ

ご利用いただくSTAFeeの操作方法に関しては、STAFeeマニュアルサイトにて公開しています。

12.3.1 情報のバックアップ

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。システムおよびお客様情報資産のバックアップに関しては、当社が日々の運用プロセスとして実施し、バックアップの取得状況は月次サイクルで確認しています。世代管理は7世代、障害復旧時点は前日バックアップ取得時点となり、目標復旧時間は24時間以内としています。また、バックアップの取得方法、復元方法については、手順書を作成し、管理者が適切に保管しています。なお、バックアップデータは、STAFeeが稼働するリージョンとは異なる国内のリージョンに保存しています。

12.4.1 イベントログ取得

当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、お客様の操作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。必要な場合は、当社のお問い合わせ窓口までご相談ください。

12.4.4 クロックの同期

STAFeeで利用する仮想サーバーは、NTPによる時刻同期を行っており、日本時間(JST)で管理しています。STAFeeで記録される時刻は、すべて時刻同期に基づいて記録しています。

CLD.12.4.5 クラウドサービスの監視

ネットワークのトラフィックおよび、CPU・メモリ・ディスクアクセスの使用率増加を検知する監視は、当社が実施しております。現在、結果をお客様に公開できるサービス機能は提供していません。確認結果についてお客様から求めがあった場合、当社の裁量判断により、お知らせの可否、ならびに、お知らせ可能な事項および範囲を決定いたします。

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、お客様で対応が必要となるぜい弱性情報があった場合には、メールにて通知いたします。

STAFee側での対応が必要になった場合には、定期・緊急メンテナンスにて対応を実施し、メンテナンス前後で対応内容および対策後の結果をメールにて通知いたします。

また、年1回第三者機関によるぜい弱性診断を受けており、指摘事項があった場合は速やかに対策を講じています。

13.1.3 ネットワークの分離

STAFeeでは、開発・構築時にネットワークセキュリティ要件を決定し、用途別にネットワークを分離しており、お客様側のネットワーク環境とSTAFeeのネットワーク環境は分離されています。

また、当社の社内ネットワーク環境とSTAFeeのネットワーク環境も分離されています。

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性がとれるように設計、構築、管理を徹底しています。

14.1.1 情報セキュリティ要求事項の分析および仕様化

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、クラウドサービス利用契約書、当ホワイトペーパーに記載しています。

下記に主なセキュリティ機能を記載します。詳細は当ホワイトペーパー該当項番をご参照ください。

・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

開発時には、当社が定めるセキュリティ方針に基づいたコードレビューを実施し、コードにバグやパフォーマンスの問題、安全でないコーディングパターンが潜在していないか検出に努めています。

また、年1回の第三者機関による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

STAFeeは、SaaS(Software as a Service)型のクラウドサービスとなり、責任分界点の詳細に関しては前出の「2.2 責任分界点について」をご参照ください。

また、STAFeeのセキュリティ対策に関しても「2.2 責任分岐点について」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、STAFee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。

https://aws.amazon.com/jp/compliance/
https://learn.microsoft.com/ja-jp/azure/compliance/

16.1.1 責任および手順

当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。確認できた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おいては、検知から3営業日以内を目標にメールにて通知いたします。また、当社に起因するセキュリティインシデントでお客様に重大な影響を及ぼすものは、適用可能なあらゆる対処を実施します。

16.1.2 情報セキュリティ事象の報告

お客様からの問い合わせや報告は、当社のお問い合わせ窓口にてお受けします。
当社で確認した情報セキュリティ事象がお客様に影響を及ぼす可能性がある場合には、メールにて通知します。

16.1.7 証拠の収集

お客様は、クラウドサービス利用契約の締結をもって、お客様情報資産および派生データが、国内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承諾されたものとします。

18.1.1 適用法令および契約上の要求事項の特定

STAFee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

知的財産権などに必要な情報の問い合わせは、当社のお問い合わせ窓口にてお受けします。

18.1.3 記録の保護

当社の責任範囲において、お客様のアクセスログを取得しています。必要な場合は、当社のお問い合わせ窓口にてお受けします。

18.1.5 暗号化機能に対する規制

STAFeeでは、SSL/TLS による通信の暗号化を使用しています。なお、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

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のISMS 認証取得、プライバシーマークの取得において第三者による審査を受け、情報セキュリティに対する取り組みを行うことで、常に安全なセキュリティレベルを確保しています。内部監査の結果が必要な場合は、当社のお問い合わせ窓口までご相談ください。

4 更新履歴

版数	日付	更新内容
第 1.0 版	2026/2/17	初版公開