# Customers Mail Cloud

ISO/IEC 27017 ホワイトペーパー

HENNGE 株式会社
Messaging Business Division

2025 年 6 月 20 日（第 1 版）

# 目　次



Copyright © HENNGE K.K.

Copyright © HENNGE K.K.

# 1 はじめに

## 1.1 ホワイトペーパーの目的

「Customers Mail Cloud サービスホワイトペーパー」は、ISMS クラウド認証である(ISO/IEC 27017：2015)で求める要求事項に対して、当社がお客様に対して提供しているセキュリティ仕様について明確にするものです。
ISO/IEC 27017 は、ISO27001 のアドオン認証の位置付けであり、クラウドサービスの提供や利用に対して適用されるクラウドセキュリティの第三者認証に対するガイドライン規格となります。

## 1.2 本書の適用範囲

本書の適用範囲は、弊社の Customers Mail Cloud サービスとなります。

Copyright © HENNGE K.K.

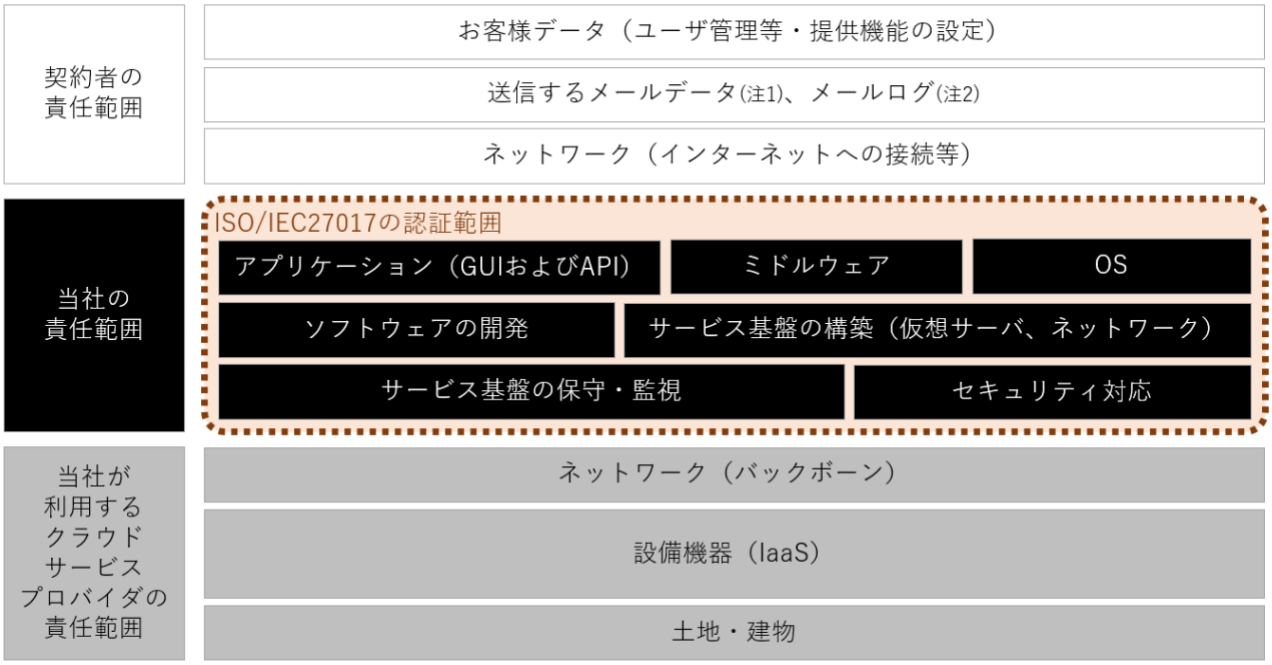
# 2 Customers Mail Cloud サービスについて

## 2.1 Customers Mail Cloud サービスとは

クラウドから簡単に、確実にメールを送信することができる SaaS 型メール配信サービスです。商品購入や予約完了の即時メールや、結果通知の一括・大量メールなど、 ユーザーに届けたい通知メールを高い到達率で配信することができます。

## 2.2 責任分界点について

Customers Mail Cloud に関する責任分界点は、以下になります。




注 1 :メールデータについては、送信後、システムから削除しています。

注 2 :メールログについては、インシデント対策のためシステム側で 40 日間保存していますが、それ以上の日数分を保存されたい場合は、管理画面、もしくは API を利用してダウンロードをおこなってください。

Copyright © HENNGE K.K.

# 3 JIS Q 27017:27016(ISO/IEC 27017:27015)への対応

**Customers Mail Cloud サービス の管理策に関する見方の説明**

JIS Q 27017:27016(ISO/IEC 27017:27015)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、Customers Mail Cloud の要求事項に対する解釈および管理策になります。
小項目番号のみの管理策は、ISO27001 に対してクラウドサービス特有の要求事項を加えたものとなっており、CLD からはじまる管理策はクラウドサービス固有の管理策となります。

**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は，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を求められています。
Customers Mail Cloud サービス（以下、当サービスといいます）では、弊社の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。

情報セキュリティ基本方針
（https://hennge.com/jp/security-policy.html）
また、弊社が利用するクラウドサービスについては、利用のためのルールを作成し、適切に運用しています。

**6.1.1 情報セキュリティの役割及び責任**

当サービス サービス規約において契約やサービスの内容を定義し、サービス提供をおこなっています。これらについては利用開始時にサービス規約として同意いただく事項となります。

**6.1.3 関係当局との連絡**

弊社所在地は、東京都渋谷区南平台町 16-28 Daiwa 渋谷スクエアとなります。
当サービスで利用されるデータの所在地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**

当サービスサービス規約にてサービスの内容を定義し、弊社従業員に徹底したうえでサービス提供を実施しています。
責任分界点に関しては 2.2「責任分界点について」を参照ください。

Copyright © HENNGE K.K.

### 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定期的に実施しています。

### 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います。また、当サービス上にサービス利用者様が作成されたアカウント情報や各種設定情報、メールログは、サービス利用者様の管理範囲となります。

### CLD.8.1.5 クラウドサービスカスタマの資産の除去

1. サービス規約に記載していますように解約月の翌月末までに、サービスの管理者情報および配信ログおよび操作ログ等のご利用履歴を当社の責任において上書き消去を用いて全て復元できない状態で削除します。 2. 返却また削除できずに残存するデータはありません。 3. 物理装置（例えば、メモリ、ハードディスクなど）を再利用または廃棄する場合は、当社が利用するクラウドサービスプロバイダの取り決めに従い、適切なプロセスで処理しています。

### 8.2.2 情報のラベル付け

当サービスでは、電子メールを扱っており、ラベル付けとして API を利用して件名を指定いただくことが可能です。

(https://smtps.jp/docs/apiv2/es/emails/index.html#send)

### 9.2.1 利用者登録及び登録削除

当サービスはアカウント設定機能を提供しています。
管理者は、管理コンソールを利用し、ユーザーの登録や削除をおこなうことが可能です。
機能の利用にあたっては操作マニュアルをご覧ください。

(https://smtps.jp/docs/userguide/manage/account/index.html)

### 9.2.2 利用者アクセスの提供

当サービスはアクセス権限設定機能を提供しています。
管理者は、管理コンソールを利用し、ユーザー毎にアクセス権の追加・削除・管理が可能です。
機能の利用にあたっては操作マニュアルをご覧ください。

(https://smtps.jp/docs/userguide/manage/account/index.html)

Copyright © HENNGE K.K.

### 9.2.3 特権的アクセス権の管理

ID/パスワード認証以外に、ワンタイムパスワード(OTP)による二要素認証機能を提供しています。
管理者は、管理コンソールを利用し、ユーザー毎に OTP の機能利用を設定いただくことが可能です。
機能の利用にあたっては操作マニュアルをご覧ください。
（https://smtps.jp/docs/userguide/manage/account/index.html）

### 9.2.4 利用者の秘密認証情報の管理

管理者は、利用するユーザーの秘密認証情報の初期設定や変更が可能です。
設定や変更にあたっては操作マニュアルをご覧ください。
（https://smtps.jp/docs/userguide/manage/account/index.html）

### 9.4.1 情報へのアクセス権限

管理者は、管理コンソールを利用しユーザーの権限制限を行うことが可能です。
権限の設定や機能の利用にあたっては操作マニュアルをご覧ください。
（https://smtps.jp/docs/userguide/manage/account/index.html）

### 9.4.4 特権的なユーティリティプログラムの利用

管理コンソール、API の利用等すべてのサービス利用にあたっては、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おこなっていません。

### CLD.9.5.1 仮想コンピューティング環境における分離

適切な人が適切なリソースのみにアクセスするよう、ユーザーID によるアクセス資源の分離を実施し、別テナントへの不正アクセスを抑止しています。
尚、不正アクセス（別テナント ID でのアクセス）については第三者診断（脆弱性診断）を定期的に実施しています。

### 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、当サービスに必要となるポート・プロトコル・IP アドレスのみを有効としています。また、AWS Shield/Guard Duty/WAF による防御強化をおこなっています。

Copyright © HENNGE K.K.

### 10.1.1 暗号による管理策の利用方針

ログイン ID のパスワードは、SHA256 方式にてハッシュ化しています。サービス内に保存するメールアドレスは AES 暗号化(128bit)によって暗号化しています。管理コンソール、API、および、SMTP の通信については、TLS バージョン 1.2 による暗号化通信が利用できます。

### 11.2.7 装置のセキュリティを保った処分又は再利用

当サービスは、弊社が契約するクラウドサービスプロバイダ（アマゾンウェブサービス、及びさくらのクラウド）が構築する仮想化環境上で提供しており、弊社が直接処分、又は再利用する資源（装置、ストレージ、メモリ等）は保有していません。弊社が契約するクラウドサービスプロバイダが、契約に基づき資源の処分または再利用を適切に実施していることを定期的に確認しています。

### 12.1.2 変更管理

サービス規約第 13 条で定めているとおり、サービス仕様の変更について、その旨を変更の 60 日前までに契約者に通知するものとします。また、ユーザインタフェースの大幅な変更およびサービス URL の変更等、契約者の操作方法に変更が生じる場合ならびに契約者が本サービス 利用のための環境を変更する必要が生じる場合には、当社は、その旨を変更の 30 日前までに契約者に通知するものとします。ただし、緊急またはやむを得ない事由によるサービスの変更等の場合はこの限りではありません。

### 12.1.3 容量・能力の管理

弊社が契約しているクラウドサービスプロバイダ提供のクラウド環境上の資源において CPU やストレージ等、ハードウェア資源の処理能力やデータ保存容量について監視しており、必要に応じ適切なタイミングでシステムの増強を行なっています。

### CLD.12.1.5 実務管理者の運用セキュリティ

サービス内で発生する重要な操作に関する手順につきましては、各種ドキュメントを提供しています。

(https://smtps.jp/docs/service/index.html)

### 12.3.1 情報のバックアップ

暗号化した上で 1 時間ごとに 20 日分（480 世代）バックアップしております。目標復旧時点（RPO）は、障害発生 1 時間前の取得時点となります。また、センターレベルで隔地保管をおこなっております。

Copyright © HENNGE K.K.

※お客様のメール本文および添付ファイルにつきましては保存およびバックアップを行なっていません。

### 12.4.1 イベントログ取得

メールログ、管理コンソールへのログインログ、操作ログを取得しており、管理コンソール、及び API を利用して閲覧できます。操作方法については操作マニュアルをご覧ください。
尚、ログインログ、及び操作ログは 5 年間、（メールログは 40 日間）保存していますが、ユーザー権限でダウンロード可能な期間は 90 日間となります。随時、ダウンロードいただき保存をおこなってください。
（https://smtps.jp/docs/userguide/manage/log/）

### 12.4.4 クロックの同期

NTP による時刻同期の仕組みを有しています。
タイムゾーンは日本時間（JST)となります。

### 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等のパフォーマンスや攻撃を検知する監視は、弊社が実施していますが、現在、その結果を公開できるサービス機能はありません。メールログ、管理コンソールへのログインログ、操作ログは管理コンソール及び API を利用して閲覧が可能です。操作方法については操作マニュアルをご覧ください。

### 12.6.1 技術的ぜい弱性の管理

非公開情報を含め、脆弱性情報を常時収集しています。 収集した情報を元に、サービス設備への影響を評価し、弊社の責任範囲において影響がある場合は、速やかに対応しており、必要に応じて当サービスブログ、及びメールにて報告をおこないます。
また、外部第三者機関による脆弱性診断を年 2 回実施しています。診断の結果、改善が必要となる事項に対しては速やかに対応し必要に応じて当サービスブログ、及びメールにて報告をおこないます。

### 13.1.3 ネットワークの分離

お客様毎のテナント間は完全に分離されており、また弊社管理用ネットワークからも分離されています。
尚、第三者によるテナントを跨いだアクセスについて定期的に診断も実施しています。

Copyright © HENNGE K.K.

### 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。 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。

| セキュリティ機能 | 内容 |
|---|---|
| アクセス制御機能 | (9.2.1 利用者登録及び登録削除) |
| アクセス制御機能 | (9.2.2 利用者アクセスの提供) |
| アクセス制御機能 | (9.4.1 情報へのアクセス制限) |
| 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

当社で定める情報システム開発保守細則、および IPA「安全なウェブサイトの作り方 改訂第 7 版」に基づきセキュアな開発をおこなっています。

### 15.1.2 供給者との合意におけるセキュリティの取扱い

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。

### 15.1.3 ICT サプライチェーン

弊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、弊社が適用するクラウドサービスと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。

### 16.1.1 責任及び手順

弊社で確認したインシデントについては、以下の責任および手順に従い、情報提供および対策を実施します。

| | |
|---|---|
| 情報セキュリティインシデントの範囲 | DDoS 等によるサービスへの攻撃、不正アクセス、ソフトウエアに確認した脆弱性、情報漏洩など。 |
| 検出及びそれに伴う開示レベル | ネットワークモニタリング、ログモニタリング、脆弱性データベース参照等により検出し、当社の判断において契約者に影響があると判断した場合に　これを開示します。 |
| 通知を行う目標時間 | 検出から 6 営業時間以内に第一報を通知します。 |

Copyright © HENNGE K.K.

| | |
|---|---|
| 通知手順 | 契約者のメールアドレス宛にメールにて通知します。 |
| 取り扱いの窓口 | 管理コンソールの「問い合わせ」フォーム、または、以下のサポート窓口宛の電子メールにてお問合せを受け付けます。<br>hde-cm@hennge.com |
| 発生した場合の対処 | 不正な通信遮断、セキュリティパッチの適用、証拠の保全、外部機関への　報告など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

弊社で検知した情報セキュリティ事象（インシデント）について、お客様に影響の可能性があると判断した場合は、ご契約時に登録いただいたメールアドレス宛にメールにより報告をおこないます。
お客様で情報セキュリティ事象を検知した場合には、サポート窓口までご連絡ください。

### 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、お客様の同意なく、お客様のデータを第三者に開示することがあります。
このことは、サービス規約第 24 条第 4 項に定められており、お客様の合意を得られたものとします。

### 18.1.1 適用法令及び契約上の要求事項の特定

サービス規約第 30 条のとおり、準拠法を日本国法として本サービスを提供します。
本サービスはインターネットを介して、電子メールの送信に係るサービスを提供するため、当社は当社および契約者に以下の法令に順守を要求することとします。
（1）特定電子メールの送信の適正化等に関する法律
（2）個人情報の保護に関する法律
（3）不正アクセス行為の禁止等に関する法律

### 18.1.2 知的財産権

サービス規約第 27 条で定めているとおり、本サービスおよび本サービスを提供するためのウェブコンテンツ、ドキュメント、プログラム、その他の著作物および技術等に関する著作権、特許権、商標権、その他一切の権利は、当社または原権利者に帰属します。
知的財産権に関する問い合わせは、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

前出の 12.4.1.イベントログ取得に記載していますとおり、ログを取得しています。

Copyright © HENNGE K.K.

また、取得したログの保護や廃棄につきましては、社内の運用規定に定め、定期的に監査を実施し適切に管理しています。
また、このことはサービス規約第 24 条に定めています。

### 18.1.5 暗号化機能に対する規制

ログイン ID のパスワードは、SHA256 方式にてハッシュ化しています。サービス内に保存するメールアドレスは AES 暗号化(128bit)によって暗号化しています。ご利用いただける暗号化通信の TLS バージョンは以下 の通りです。

（1）管理コンソール（UI / API）：TLS1.2
（2）新規メールサーバー（SMTP / API）：TLS1.2
（3）既存メールサーバー（SMTP / API）：TLS1.2

又、当サービスにおいて、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

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 の ISMS 認証取得において第三者による審査を受け、各々の認証を取得していることをもって、弊社がセキュリティ対策を確実に実施している証跡としています。
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についても実施しており、常に安全なセキュリティレベルを確保しています。

Copyright © HENNGE K.K.

## 4改訂履歴

| 版数 | 日付 | 更新内容 |
|---|---|---|
| 第 1.0 版 | 2025/6/20 | 初版公開 |

Copyright © HENNGE K.K.