ALSI

INTERSAFE Gateway Connection

# クラウドセキュリティホワイトペーパー

第 5 版

2024 年 10 月 発行

目次

**1. このホワイトペーパーについて ..... 1**

**2. 本書の適応範囲について ..... 2**

**3. ISO/IEC 27017 について ..... 3**

**4. クラウドサービスの管理策 ..... 4**

A.5.1.1 情報セキュリティのための方針群 ..... 4
A.6.1.1 情報セキュティの役割及び責任 ..... 4
A.6.1.3 関係当局との連絡 ..... 4
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及び責任の共有及び分担 ..... 5
A.7.2.2 情報セキュリティの意識向上、教育及び訓練 ..... 5
A.8.1.1 資産目録 ..... 5
CLD.8.1.5 クラウドサービスカスタマの資産の除去 ..... 5
A.8.2.2 情報のラベル付け ..... 6
A.9.2.1 お客様登録及び登録 ..... 6
A.9.2.2 お客様アクセスの提供 ..... 6
A.9.2.3 特権的アクセス権の管理 ..... 6
A.9.2.4 お客様の秘密認証情報の管理 ..... 6
A.9.4.1 情報へのアクセス制限 ..... 6
A.9.4.4 特権的なユーティリティプログラムの使用 ..... 6
CLD.9.5.1 仮想コンピューティング環境における分離 ..... 7
CLD.9.5.2 仮想マシンの要塞化 ..... 7
A.10.1.1 暗号による管理策の利用方針 ..... 7
A.11.2.7 装置のセキュリティを保った処分又は再利用 ..... 7
A.12.1.2 変更管理 ..... 7
A.12.1.3 容量・能力の管理 ..... 7
CLD.12.1.5 実務管理者の運用のセキュリティ ..... 8
A.12.3.1 情報のバックアップ ..... 8
A.12.4.1 イベントログ取得 ..... 8
A.12.4.3 実務管理者及び運用担当者の作業ログ ..... 8
A.12.4.4 クロックの同期 ..... 8

CLD.12.4.5 クラウドサービスの監視 ..... 8
A.12.6.1 技術的脆弱性の管理 ..... 9
A.13.1.3 ネットワークの分離 ..... 9
CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合 ..... 9
A.14.1.1 情報セキュリティ要求事項の分析及び仕様化 ..... 9
A.14.2.1 セキュリティに配慮した開発のための方針 ..... 9
A.15.1.2 供給者との合意におけるセキュリティの取扱い ..... 9
A.15.1.3 ICT サプライチェーン ..... 9
A.16.1.1 責任及び手順 ..... 10
A.16.1.2 情報セキュリティ事象の報告 ..... 10
A.16.1.7 証拠の収集 ..... 10
A.18.1.1 適用法令及び契約上の要求事項の特定 ..... 10
A.18.1.2 知的財産権 ..... 10
A.18.1.3 記録の保護 ..... 10
A.18.1.5 暗号化機能に対する規制 ..... 10
A.18.2.1 情報セキュリティの独立したレビュー ..... 10

**5. 改定履歴 ..... 11**

# 1. このホワイトペーパーについて

このホワイトペーパー(以下、本書)は、アルプスシステムインテグレーション株式会社(以下、当社)が提供するクラウドサービスにおける、セキュリティへの取り組みについて理解を深めていただくためのものです。クラウドセキュリティの国際規格 ISO/IEC27017 の中で、お客様に向けて情報開示が求められる事項について、セキュリティの取り組みをご確認いただくことができます。

# 2. 本書の適応範囲について

本書は、当社の提供するクラウド型次世代 Web フィルタリングサービス、InterSafe GatewayConnection(以下、ISGC)が適用範囲となります。

# 3. ISO/IEC 27017 について

ISO/IEC27017 は、国際標準化機構 と国際電気標準会議 の下に設置された ISO/IEC JTC 1/SC 27 小委員会により公開された、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を示した国際規格です。

クラウドサービスに関する情報セキュリティ管理策の実践の規範として、ISO/IEC 27017 で、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 ISO/IEC 27001 の取り組みを強化します。これにより、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し、その実践を支援します。

# 4. クラウドサービスの管理策

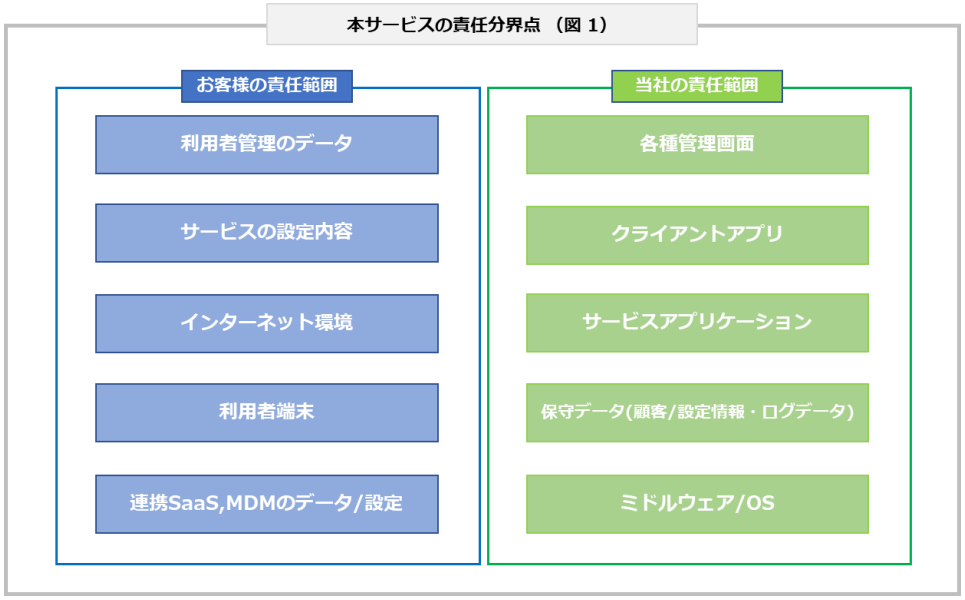
本項では、ISO/IEC27017 管理策の実践の規範の項番に沿って本サービスの管理策を記載します。本サービスにおける ISO/IEC27017 の定める管理項目への管理策は以下のとおりです。

### A.5.1.1 情報セキュリティのための方針群

・当社はセキュリティポリシーの中に、「クラウドセキュリティ基本方針」を定め、お客様が安心してご利用いただけるように取り組んでおります。また、本基本方針及び関連する社内規則等は、毎年の ISMS 活動の中で、年に 1 回、見直しております。

### A.6.1.1 情報セキュリティの役割及び責任

・本サービスは、お客様と当社の情報セキュリティの責任範囲について、図 1 の責任分界点のとおり定義しております。




### A.6.1.3 関係当局との連絡

・当社の所在地は、当社ウェブサイトでご確認ください。「https://www.alsi.co.jp/company/」

・本サービスにて保存されるデータの所在は、日本国内のデータセンターです。

### 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及び責任の共有及び分担

・本サービスは、サービスの提供環境における役割及び責任について利用規約に定めサービスを提供します。

・本サービスの責任分界点については、「6.1.1 情報セキュリティの役割及び責任」をご確認ください。

### A.7.2.2 情報セキュリティの意識向上、教育及び訓練

・本サービスでは、サービス運営担当者に対し、当社が定めたセキュリティ教育に加え、クラウドセキュリティ基本方針に定めた管理事項の運営に必要な教育を実施しています。

### A.8.1.1 資産目録

・本サービスでは、お客様の情報資産（お客様が保存されるデータ）と、当社がサービスを運営するための情報を、明確に分離しています。

・お客様の情報資産（お客様が保存されるデータ）に関しては、お客様の管理範囲です。

### CLD.8.1.5 クラウドサービスカスタマの資産の除去

・お客様が当社のクラウドサービスを解約された場合、解約後はサービス利用に関する下記データをダウンロードできなくなります。必要に応じて、解約前にダウンロードしてください。

・ユーザアカウントデータ

・アクセスログ

・フィルタリング設定データ

・違反検出履歴データ

・キッティング完了デバイスデータ

・当社は、お客様がサービスの利用を終了した場合、当該サービスの解約後 90 日以内に消去します。

・本サービスでは、下記の消去したデータはいかなる場合でも復旧することはできません。ただし、お客様の情報資産を含まない、システムのイベントログ等の当社がサービスを運営するための情報は対象外とします。

・管理画面で設定可能な全ての情報

・導入時/オプション設定時にご提供頂いた情報

・環境構築時/運用時に生成されるデータ

- 違反検出履歴データ

- キッティング完了デバイスデータ
- Web アクセスログ

### A.8.2.2 情報のラベル付け

・お客様は、ユーザをお客様自ら追加したグループにグルーピングすることが可能です。

### A.9.2.1 お客様登録及び登録

・本サービスの契約管理者のアカウントは当社が発行します。

・当社は、契約管理者がユーザーアカウントを登録、及び削除する機能を提供しています。具体的な操作手順は製品の操作マニュアルをご参照ください。

### A.9.2.2 お客様アクセスの提供

・本サービスは、ユーザ権限を管理する機能（アクセス権）を提供しており、管理者が設定可能となります。提供機能の利用にあたっては、操作マニュアルをご参照ください。

### A.9.2.3 特権的アクセス権の管理

・本サービスは、ID／パスワード認証に加え、アクセス元 IP アドレス制限を設定できるオプションを提供しています。

### A.9.2.4 お客様の秘密認証情報の管理

・本サービスは、サービス利用開始時に管理者権限を有するお客様 ID をメールにて提供します。パスワード変更にあたっては、操作マニュアルをご参照ください。

### A.9.4.1 情報へのアクセス制限

・本サービスは、管理者権限を有するお客様によって、機能制限を行うことができます。

### A.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、通常の操作手順またはセキュリティ手順を回避することのできるユーティリティプログラムの提供はありません。

### CLD.9.5.1 仮想コンピューティング環境における分離

・本サービスでは、仮想化技術やネットワークセキュリティ技術を利用し、サーバやネットワーク、ストレージをお客様ごとに論理的に分離しています。

### CLD.9.5.2 仮想マシンの要塞化

・お客様が利用するサービスの提供に用いる仮想環境は、必要最小限の構成でサーバを構築して、不必要なサービスは起動しないようにしております。また、本サービスをご利用いただくのに必要なポートやプロトコルへのアクセス制限を実施しております。

### A.10.1.1 暗号による管理策の利用方針

・本サービスのご利用において、お客様の端末と、サービスプラットフォーム間のインターネット通信は、基本的に HTTPS(TLS1.2)により暗号化されます。

・例外としてプロキシ利用時は HTTP を利用しています。

・下記情報は記載の暗号化方式にて暗号化されます。

- グループおよびユーザの情報[暗号化方式：3DES]
- システム稼働に必要となる機密データ（パスワードなど）[暗号化方式：3DES]
- アプリへ配布するための設定データ（エージェント設定ファイル）[暗号化方式：RSA]
- アプリがクラウドからダウンロードする設定データ（アプリポリシー）[暗号化方式：RSA]

### A.11.2.7 装置のセキュリティを保った処分又は再利用

・本サービスでは、サービス提供に利用するクラウドサービスのデータの処分状況を正しく把握し、適切なプロセスでデータ管理を行っています。

### A.12.1.2 変更管理

・本サービスでは、機能の変更や廃止、一時的なメンテナンスなど、お客様に影響を与える可能性のある変更が生じる場合は、メールやサポート情報サイトにおいて通知します。

### A.12.1.3 容量・能力の管理

・本サービスでは、サービス提供に利用するクラウドサービスの監視を行い、状況に応じてリソース増強を行うなど適切な運用管理を行っています。

### 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手順を、マニュアルなどのドキュメントとしてダウンロードサイトにて提供しています。

### A.12.3.1 情報のバックアップ

本サービスでは、サービスの設定情報およびユーザーデータのバックアップを日次で取得/保持しています。

・バックアップ対象：
グループ/ユーザアカウントデータ、通知先メールアドレス、フィルタリング設定データ、お客様の認証局証明書データ、キッティング完了デバイスデータ、違反検出履歴データ、Web アクセスログ、システムのイベントログ

・保持期間：31 日

・バックアップデータ保管場所：日本

### A.12.4.1 イベントログ取得

・本サービスでは、サービスの維持管理に必要となる適切なログを取得しています。また、管理権限を有しているお客様へログのダウンロード機能を提供しています。

・ログのダウンロードに必要な操作手順は、マニュアルなどのドキュメントとして提供しています。

### A.12.4.3 実務管理者及び運用担当者の作業ログ

・本サービスでは、サービスの提供に関わる作業及び結果を記録し、レビューを実施しています

### A.12.4.4 クロックの同期

・本サービスでは、サービス提供に必要なシステムのクロック同期を、NTP などの技術を用いて実施しています。

### CLD.12.4.5 クラウドサービスの監視

・本サービスでは、サーバの死活監視、サービスプロセス監視、サービスポート監視、リソース監視、サービス外形監視を 1～5 分ごと監視しています。

・アラート発生時には運用部門への通知が行われ、影響がある場合には、速やかに対処します。

### A.12.6.1 技術的脆弱性の管理

・本サービスでは、脆弱性情報を収集し、収集した情報を元にサービスへの影響を評価し、当社の責任範囲において影響がある場合には、速やかに対応します。

### A.13.1.3 ネットワークの分離

・本サービスでは、お客様ごとに論理的にネットワークを分離し、サービス運営で必要となる管理ネットワークに関しても、お客様のネットワークと分離しています。

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

・本サービスでは、サービス提供に利用するクラウドサービスにおける仮想および物理ネットワークの整合を確認しています。

### A.14.1.1 情報セキュリティ要求事項の分析及び仕様化

・本サービスでは、以下のセキュリティ機能を使用しています。

- WAF（Web アプリケーショファイアウォール）

### A.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、当社にて定めた規定に則ったセキュリティに配慮した開発を行っています。

・また、開発を外部に委託する際も、これに準じた契約のもと開発が行われます。

### A.15.1.2 供給者との合意におけるセキュリティの取扱い

・本サービスは、サービスの提供環境における役割及び責任について利用規約に定めサービスを提供します。

・本サービスの責任分界点については、「A.6.1.1 情報セキュリティの役割及び責任」をご確認ください。

### A.15.1.3 ICT サプライチェーン

・本サービスでは、ピアクラウドサービスプロバイダに対して当社の情報セキュリティ方針を示し、自社のセキュリティ水準と同等かそれ以上であることを確認しています。

### A.16.1.1 責任及び手順

・本サービスは、当社が確認し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場合、確認より24 時間以内を目標にお客様管理者様へメールにて通知を行います。

・ 情報セキュリティインシデントに関する問合せは、InterSafe GatewayConnection サポート窓口でお受けいたします。

### A.16.1.2 情報セキュリティ事象の報告

・本サービスでは、ALSI サポート窓口へのお問い合わせで、相互に情報のやりとりができる仕組みを提供しています。

### A.16.1.7 証拠の収集

・当社は、サービス内で収集するデジタル証拠となりうるデータ（ログなど）、及びそれらのデータを第三者（警察や裁判所など）に提出する情報や条件なども利用規約に記載しています。

### A.18.1.1 適用法令及び契約上の要求事項の特定

・本サービスのご利用に関して、適用される準拠法は日本国の法令です。

### A.18.1.2 知的財産権

・本サービスをご利用いただく上での知的財産権に関わるご相談は、当社窓口までお問い合わせください。

### A.18.1.3 記録の保護

・本サービスのお客様に関するデータは、不正アクセスや改ざんを防ぐため、許可された従業員しかアクセスできない適切に管理されたアクセス権のもとで保管されます。

### A.18.1.5 暗号化機能に対する規制

・本サービスでは、輸出規制の対象となる暗号化の利用はありません。

### A.18.2.1 情報セキュリティの独立したレビュー

・当社は、ISO/IEC 27001 と ISO/IEC 27017 について第三者による審査を受け、認証の取得状況を当社ウェブサイトで公開しています。

# 5.　改定履歴

| 版数 | 改訂日 | 改訂内容 |
|---|---|---|
| 1 | 2024/04/01 | 初版作成 |
| 2 | 2024/05/14 | 表紙の画像と文言を更新 |
| 3 | 2024/08/01 | A.18.2.1 情報セキュリティの独立したレビューを更新 |
| 4 | 2024/09/09 | 下記内容を更新<br>CLD.8.1.5 クラウドサービスカスタマの資産の除去<br>A.10.1.1 暗号による管理策の利用方針<br>A.12.3.1 情報のバックアップ<br>A.14.1.1 情報セキュリティ要求事項の分析及び仕様化 |
| 4 | 2024/10/24 | 下記内容を更新<br>A.8.2.2 情報のラベル付け<br>A.18.2.1 情報セキュリティの独立したレビュー |

**InterSafe GatewayConnection　情報セキュリティホワイトペーパー**

---

2024 年 10 月 第 5 版

作成 / 発行 / 企画　　アルプスシステムインテグレーション株式会社

〒145-0067 東京都大田区雪谷大塚町 1-7

---

・ 記載されている会社名および商品名は、各社の商標もしくは登録商標です。

・ 本書の内容は将来予告なしに変更することがあります。

・ 本書の内容の一部、または全部を無断で転載、あるいは複写することを禁じます。

・ 本書の内容については万全を期して作成いたしましたが、万一記載に誤りや不完全な点がございましたらご容赦ください。