ISO/IEC 27017

クラウドセキュリティホワイトペーパー

1.0 版

株式会社気象工学研究所

2026 年 6 月 1 日

1　目的

本ホワイトペーパー（以下、本書）は、クラウドセキュリティの国際規格（ISO/IEC 27017）で求められている要求事項に対して、当社がクラウドサービスプロバイダ(CSP)として実施するクラウドサービス固有の情報セキュリティ管理策および責任範囲をご理解いただくことを目的としています。

2　適用範囲

当社の ISO/IEC 27017 の適用範囲は、以下のサービス内容に対するものです。

ANPiS　：自社製品（気象情報提供・安否確認システム）

3　ANPiS 気象情報提供・安否確認システムついて

3.1　ANPiS 気象情報提供・安否確認システムとは

気象庁から配信された情報を自動で瞬時に一斉配信し、安否を確認するクラウドサービスです。 従業員の安否確認から、出社可否確認まで幅広くご利用いただけます。

3.2　責任分界点について

本サービスは責任共有モデルに基づき運用されます。
ANPiS 気象情報提供・安否確認システムの責任分界点は、以下になります。

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

JIS Q 27017:2016（ISO/IEC 27017:2015）が求める要求事項に対する管理策の項番の順番で本サービスの取り組みを記載いたします。

5.1.1 情報セキュリティのための方針群
本サービスでは、当社の情報セキュリティ基本方針（https://www.meci.jp/security.php）およびクラウドサービス情報セキュリティ方針（https://www.meci.jp/cloudsecurity.php）に従い、クラウドサービス固有の事項を考慮した情報セキュリティ対策を行っております。

6.1.1 情報セキュリティの役割および責任
「3.2.責任分界点について」 に記載しております。
本サービス利用については「一斉連絡・安否確認システム ASP サービス利用に関する規約」をご確認ください。

6.1.3 関係当局との連絡
関係当局からの要請および法令に基づく対応については、当社所定の手順に従い適切に対応します。
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「3.2.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「一斉連絡・安否確認システム ASP サービス利用に関する規約」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
本サービスに携わる当社サービス運営担当者に対し、クラウドサービスデータおよび派生データを取り扱うために情報セキュリティ要件やサービスの運用ルールの周知徹底と意識向上のための教育・訓練を定期的に実施しています。

8.1.1 資産目録
当社は、クラウドサービスデータ、クラウドサービス派生データおよびその保存先を情報資産として識別し資産管理を実施しています。

CLD.8.1.5 クラウドサービスカスタマの資産の除去
本サービスの提供が終了した場合に、サービス利用者様が作成・保存した情報資産（社員

情報、連絡設定、連絡履歴等）に関しては、契約終了から６０日以内に消去するものとする。 但し、サービス利用者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。

8.2.2 情報のラベル付け
本サービスでは、ユーザーをお客様自ら追加したグループにグルーピングする機能を提供しています。

9.2.1 利用者登録および登録削除
本サービスではユーザーのアカウントを登録・削除する機能をシステム管理者様に提供しています。

9.2.2 利用者アクセスの提供
システム管理者権限、配信権限ユーザー、一般ユーザーを管理する機能を提供しています。提供機能の詳細に関しては、各種マニュアルの「ご利用者の権限について」をご参照ください。

9.2.3 特権的アクセス権の管理
ログイン ID、パスワード認証に加え、Google 認証システム（Google Authenticator ）を利用した二要素認証機能を提供しています。また、管理者権限を有するアカウントについては二要素認証の利用を推奨しています。機能のご利用を希望されるお客様は当社 ANPiS サポートまでご連絡ください。

9.2.4 利用者の秘密認証情報の管理
本サービスはユーザーのログイン 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、変更等の手順は「ANPiS 操作マニュアル【システム管理者用】」および「ANPiS 操作マニュアル【一般ユーザー用】」を、パスワード要件は画面の表示をご参照ください。

9.4.1 情報へのアクセス制限
システム管理者権限を有するユーザー様によってシステム管理者権限ユーザー、配信権限ユーザー、一般ユーザーを設定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
本サービスにおいて、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。当社において、サービス運用保守するために保有する特権的ユーティリティプログラムについては、運用保守する要員を限定し、厳しく管理しています。

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、利用者団体ごとに論理的に分離し制御しています。

CLD.9.5.2 仮想マシンの要塞化
本サービスでは、以下のセキュリティ対策を実施しています。
・必要なポートだけを有効としています。
・必要なプロトコルだけを有効としています。
・マルウェア対策を実施しています。
・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
お客様よりお預かりしているメールアドレス、パスワードは、クラウドサーバ上で暗号化し管理しています。また。個人情報を扱う画面への Web アクセスはすべて暗号化通信を利用しています。

11.2.7 装置のセキュリティを保った処分または再利用
機器の老朽化、故障等により交換した機器媒体については、当社では機器媒体の処分を行う場合は、サーバ等については、AWS またはさくらクラウドの施設、建物、および物理上のセキュリティに基づきます。

AWS クラウドにおける安全なデータの廃棄：
https://aws.amazon.com/jp/blogs/news/data_disposal/

さくらクラウドにおける安全なデータの廃棄：
https://cloud.sakura.ad.jp/news/2020/01/09/disk-data-erase/

12.1.2 変更管理
本サービスの利用者様に影響のある変更およびメンテナンスを実施する場合には、事前にシステム管理者様へメールにて通知いたします。また必要に応じて全てのご利用者様にも、ログイン画面にて通知いたします。

12.1.3 容量・能力の管理
安定的なサービスを提供するために、当社にてクラウドサービスのリソースを監視し、必要なキャパシティの増強を行っています。

CLD.12.1.5 実務管理者の運用のセキュリティ

提供機能に関して、操作マニュアル、ＦＡＱなどをサービス内で公開しています。

12.3.1 情報のバックアップ
本サービスでは、ユーザー情報やメールデータ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(送信設定削除、ユーザ削除など)によって生じたデータ消失に関しては、サービス障害復旧用バックアップからの個別復元は原則として実施しておりません。また以下のデータは、お客様自身でバックアップや、リストアできる仕組みを提供しています。
・従業員情報、所属情報、役職情報、最寄り事業所情報、連絡グループ

12.4.1 イベントログ取得
当社の責任範囲において、本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。必要あれば ANPiS サポートまでお問い合わせください。

12.4.4 クロックの同期
本サービスは 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。
本サービス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
ネットワークおよび CPU・メモリ等の使用率増加を検知する監視は、当社が実施しています。 監視結果が必要となる場合は ANPiS サポートまでご連絡ください。

12.6. 1 技術的脆弱性の管理
定期的に脆弱性情報の収集と検査を実施し、リスク評価の結果、対応が必要と判断された脆弱性については、定期または緊急メンテナンスにて対応を実施いたします。サービスを停止しての対応を伴う際には事前にシステム管理者様にメールにてご連絡いたします。

13.1.3 ネットワークの分離
本サービスでは、当社の社内ネットワークと本サービス側のネットワークとは、物理的に分離されています。

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
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
本サービスの主なセキュリティ機能は以下となります。

・ウィルスチェック機能
・ログ管理機能
・監視機能

14.2.1 セキュリティに配慮した開発のための方針
当社のコーディング規則に則ったシステム開発を行い、第三者による定期的なセキュリティ診断を実施しています。

15.1.2 供給者との合意におけるセキュリティの取扱い
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、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
本サービスの提供に必要となる構成要素(データセンターや機器等)の供給については、当社セキュリティ方針を満たすようリスク管理を実施しています。

16.1.1 責任および手順
セキュリティインシデントが発生した場合には、情報セキュリティ基本方針に則り、適切に対応いたします。また、確認できたセキュリティインシデントがサービス利用者様に重大な影響を及ぼす可能性がある場合には、ログインサイト及び対象のお客様の所属する団体のシステム管理者様に対し、ANPiS サポートより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
当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、ログインサイト及びメールにて通知します。
また、お客様から当社に情報セキュリティ事象を報告いただく場合は、ANPiS サポート窓口までメール・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
本サービスに関して、裁判所から開示請求など、法律に基づいた正当な開示請求が行われた場合、法令および当社規程に従い対応します。

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、日本国の法令となります。

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、当社ホームページからお問合せください。

18.1.3 記録の保護
当社の責任範囲において、お客様操作ログなどを１２ヶ月間取得しています。

18.1.5 暗号化機能に対する規制
本サービスへの Web アクセスにおいては、TLS 通信を行う機能を提供しています。 なお、輸出規制の対象となる暗号化の利用はございません。

18.2.1 情報セキュリティの独立したレビュー
当社は ISO/IEC 27001 に基づく ISMS 認証に加え、ISO/IEC 27017 に基づくクラウドセキュリティ認証要求事項に従い、クラウドサービス固有の情報セキュリティ対策を実施しています。
また、クラウドサービス固有の情報セキュリティ対策については、「ISO/IEC27017:2015 に基づく ISMS クラウドセキュリティ認証に関する要求事項（JIP-ISMS517-1.0）」に従い、情報セキュリティ対策を実施し、実施状況を定期的に内部監査にて確認しております。

5　改定履歴

版	改定日	改定内容
1.0	2026/6/1	初版発行