InstaVR クラウドセキュリティ ホワイトペーパー

1.2 版

InstaVR 株式会社

本資料の所有権は InstaVR 株式会社に帰属します。
InstaVR 株式会社の許諾なく本資料の全部もしくは一部を対外的に参照・配布することはできません。

1. 利用者との責任分界点

当社の責任

当社は、クラウドサービスのご提供にあたり、以下の事項を実施いたします。

- クラウドサービスのセキュリティ対策（クラウドサービスの提供に利用するミドルウェア、OS、その他インフラのセキュリティ対策含む）
- クラウドサービスに保管されたクラウドサービスカスタマ・データの保護

当社は、上記を実施するにあたり、情報セキュリティ責任者およびシステム責任者を任命しています。

クラウドサービスカスタマの責任

クラウドサービスカスタマは、以下のセキュリティ対策を実施する必要があります。

- 各クラウドサービスユーザに付与されたパスワードの適切な管理
- クラウドサービスのアカウントの適切な管理（登録、削除、組織管理者権限の付与等）

2. データ保管場所

- クラウドサービスカスタマからお預かりしたデータは、既定の設定では、AWS の Region:us-east-1 (アメリカ合衆国バージニア州)に保管されます。
- クラウドサービスカスタマは当社に対して、Amazon Simple Storage Service (Amazon S3)が利用可能な AWS の Region へデータ保管場所を変更の申請をすることが可能です。

3. データの削除

- クラウドサービスの利用の終了時、クラウドサービスカスタマは、当社に対し、データの削除を申請することが可能です。クラウドサービスカスタマの申請があった場合、当社は、申請日から一か月以内に全てのデータの論理的削除を行います。
- クラウドサービスカスタマは、当社に対し、バックアップデータの削除を申請することができません。（保管期間等についての詳細は、11.バックアップの状況をご覧ください）

本資料の所有権は InstaVR 株式会社に帰属します。
InstaVR 株式会社の許諾なく本資料の全部もしくは一部を対外的に参照・配布することはできません。

- クラウドサービスカスタマは、当社に対し、ログの削除を申請することができません。（保管期間等についての詳細は、12.ログに関する情報をご覧ください）

4. ラベル付け機能

- 当社は、クラウドサービスカスタマに対して、情報及び関連資産を分離し、ラベル付けするための機能を提供しています。
- クラウドサービスカスタマは、クラウドサービス上の情報資産管理画面の情報資産（利用者コンテンツ）の一覧から、各情報資産に任意のラベルを設定することが可能です。

5. 利用者登録および削除

- クラウドサービスユーザによるクラウドサービスへのアクセスを、クラウドサービスカスタマが管理するため、当社は、クラウドサービスカスタマにアカウントの登録及び削除を行う機能を提供しています。
- クラウドサービスカスタマは、クラウドサービス上の新規アカウント登録画面からアカウントの登録を行うことができます。また、クラウドサービスカスタマは、サービス上の新規アカウント管理画面から購読を終了することで、アカウントの削除を行うことができます。

6. アクセス権の管理

- クラウドサービスユーザのクラウドサービスへのアクセス権を、クラウドサービスカスタマが管理するための特権（管理）アカウントを、当社はクラウドサービスカスタマに対して提供しています。
- 特権（管理）アカウントは、新規のクラウドサービスユーザを招待することができる他、組織の有償機能を購入、解約することができる機能を有します。特権（管理）アカウントは、メールアドレスに紐づけられます。
- クラウドサービスカスタマは、メールアドレス変更機能を使って、特権（管理）アカウントを別メールアドレスに紐づけることで権限の付与並びに削除を行うことができます。
- 当社は、クラウドサービスカスタマが特権（管理）アカウントにアクセスする際、二段階認証を提供しています。

本資料の所有権は InstaVR 株式会社に帰属します。
InstaVR 株式会社の許諾なく本資料の全部もしくは一部を対外的に参照・配布することはできません。

7. パスワードの配布方法

- 当社は、クラウドサービスカスタマの秘密認証情報の管理のための手順（秘密認証情報を割り当てる手順及び利用者認証手順を含む）についての情報を提供しています。
- 内容は以下の通りとなります。
  - ユーザーの初期パスワードは、最初からクラウドサービスユーザにウェブ画面から設定していただく方法を採用しています。
  - パスワード再発行手順については、クラウドサービスユーザがウェブ画面で再設定することができます。

8. 暗号化の状況

- 当社のクラウドサービス上の情報は、Blowfish 暗号化方式によって保護されております。
- 上記暗号方式以外をご希望の場合であっても、別の暗号方式のご提供はございません。

9. 変更管理

- 当社は、クラウドサービスに悪影響を与える可能性のあるクラウドサービスの変更について、クラウドサービスカスタマに情報を提供しています。提供する情報は以下となります。
  1. 変更種別
  2. クラウド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
  3. 変更開始及び完了の通知
  4. 変更予定日及び予定時刻
- 当社は、通常の操作手順又はセキュリティ手順を回避することのできる特権的ユーティリティプログラムの利用について、利用できる要員を厳密に制限しております。特権的ユーティリティプログラムの利用権限については、年次で見直しを行っております。
- 当社は、クラウドサービスへの変更適用時に更新される「変更履歴」を通して、最新のクラウドサービスの変更内容および変更の適用状況をクラウドサービスカスタマに情報を提供します。

本資料の所有権は InstaVR 株式会社に帰属します。
InstaVR 株式会社の許諾なく本資料の全部もしくは一部を対外的に参照・配布することはできません。

10. 手順書の提供

- 当社は、クラウドサービスカスタマに対して、特に重要な操作である解約操作に関する手順をウェブ上で公表しています。

11. バックアップの状況

- システム及びユーザデータは、日次でバックアップを取得しています。バックアップの手法はフルバックアップとなります。バックアップは、7 世代分保管されます。バックアップの保管先は、AWS US-East1 (N. Virginia)となります。
- 利用者側でバックアップ/リストアできる機能を提供していません。原則、顧客データにアクセスしない運用としているため、利用者から申請があった場合でも、利用者の要望に合わせユーザデータを復旧する対応は致しません。
- 障害対応等でのリストア作業は弊社側で行います。作業を行う前には利用者にその旨事前に周知致します。

12. ログに関する情報

<u>イベントログの取得及び保護</u>

- 当社は、クラウドサービスのユーザに対し、管理者権限を持つユーザのみ、ログ確認機能を提供しております。取得したログは、クラウドサービス上で保管しております。保管の手法は、クラウドサービスカスタマに公開しています。
- 確認できるログの内容ですが、一般ユーザについては、クラウドサービスへのアクセスログ（一年間保管）がございます。特権操作のログについては、特権 ID 払出の際の記録、及びシステム側での記録(CloudTrail 等)がございます。InstaVR としてログを取得しているが、クラウドサービスカスタマに提供していないログはございません。
- 当社は、クラウドサービスカスタマに通常提供しているログ内容の範囲を超えるログ内容の提出を求められたとき、これに応じる義務は負いません。

本資料の所有権は InstaVR 株式会社に帰属します。
InstaVR 株式会社の許諾なく本資料の全部もしくは一部を対外的に参照・配布することはできません。

クラウドサービスの監視

- 当社は、クラウドサービスの監視機能を、クラウドサービスカスタマに対して提供しています。
- 当社は、ログインログ、および、ストレージ利用容量およびデータ通信量の監視を行っております。

クロックの同期

- サービス内で提供されるログの時間は、AWS と同期しています。
- AWS とログの時間を同期されたいクラウドサービスカスタマは、手順については Amazon Web Service ブログをご覧ください（https://aws.amazon.com/jp/blogs/news/keeping-time-with-amazon-time-sync-service/）

13. 脆弱性管理に関する情報

- 当社が実施している情報セキュリティ対策は以下となります。

- セキュリティパッチのタイミング：IPA や JPCERT/CC より脆弱性情報を入手し、当社で適用する必要があるか確認しております。緊急性の高い脆弱性に対しては、1 ヶ月以内にパッチ適用しております(それ以外の脆弱性は必要可否を判断し、必要であれば 3 ヶ月以内に適用しております)

- ウィルス対策ソフトウェアの導入：当社の従業員の PC、及びサーバにマルウェア対策ソフトウェアを導入し、マルウェアから保護しております。マルウェア検知した場合、検知したマルウェアを隔離し、その後マルウェア対策ソフトウェアベンダーへ依頼し調査を実施しております。マルウェアを検知し、マルウェアの被害にあった場合、被害に遭う前の状態にリストアしております(バックアップ/リストア手順を用意しており、リストア可能な状態を保っております)。

- 第三者による脆弱性診断：年に 1 度、第三者機関による脆弱性診断を実施しております。

- サーバの適切な分離：ウェブサーバ、データベース及びバッチ処理システムを分離しております。

- 技術的脆弱性の監視状況：NATIONAL VULNERABILITY DATABASE の JSON フィードを定期チェックすることで、社内のぜい弱性監視体制（リソース監視体制）としております。当社が更新可能な

本資料の所有権は InstaVR 株式会社に帰属します。
InstaVR 株式会社の許諾なく本資料の全部もしくは一部を対外的に参照・配布することはできません。

SLA を超えたシステム停止、不正アクセス/情報漏えいを引き起こす可能性がある当社が重大と認識したセキュリティ脆弱性は、AWS などの外部クラウドサービスの技術的脆弱性の監視状況に準じてパッチ適用可能になり次第、最短で実施しております。

- ネットワークやサーバについての遵守事項：
  1. 仮想マシンを設定する際に、適切な側面からの要塞化（不要なポートを閉めること、及び、利用するプロトコルやサービスの制限）を実施しております。
  2. 利用する各仮想マシンへの適切な技術手段（マルウェア対策、及び、ログの取得）を実施しております。
  3. デフォルト値の変更、デフォルトアカウントの削除または無効化を実施しております。
  4. 異なるセキュリティレベルの機能を 1 つのサーバで管理しない施策(Web サーバと DB サーバを分離すること)を実施しております。

- 新しく入社する者に対しては、都度、情報セキュリティに関する教育を実施しております。また、会社員全員に対し、定期的(年に 1 回以上)に、情報セキュリティに関する教育を実施しております。いずれもテスト問題を用意しており、合格するまで受講するルールとしております。内部監査については、外部コンサルタントに参加してもらい、第三者が行うこととしております。認証取得後は年に 1 度外部審査対応を行います。

14. 資産の取り扱いに関する情報

- 当社は、お客様の情報資産を、データセンターのみに保管します。
- 例外的に SD カードがデータの保管先として使われた場合は、適切なアクセス制御された場所に保管し、作業が終わり次第、外部記憶媒体内のデータを消去し、再利用しております。

15. 開発におけるセキュリティ情報

- アプリケーションのプログラミングについては、開発標準を遵守しております。

本資料の所有権は InstaVR 株式会社に帰属します。
InstaVR 株式会社の許諾なく本資料の全部もしくは一部を対外的に参照・配布することはできません。

16. インシデント発生時の対応

- クラウドサービスカスタマまたはクラウドサービスユーザがセキュリティインシデント事象を発見したとき、当社にお問い合わせ・通知する機能として、コーポレートサイトにお問い合わせフォームをご提供しております。

- インシデントが発生した場合にクラウドサービスカスタマへ報告する範囲を、当社は以下のように定めております。
  - 当社がクラウドサービスカスタマに報告する情報セキュリティインシデントの範囲：①SLA を超えたシステム停止、②不正アクセス/情報漏えい、③当社が更新可能な、上記を引き起こす可能性があると当社が重大と認識したセキュリティ脆弱性
  - 当社がクラウドサービスカスタマに報告しない情報セキュリティインシデントの範囲：当社が制御できない AWS や Heroku などの外部クラウドサービスのセキュリティ脆弱性の対応状況

- インシデントを検知する手段およびクラウドサービスカスタマに開示する情報について、当社は以下のように定めております。
  - SLA を超えたシステム停止：第三者の通知システムによって検知し、停止時間および復旧状況についての情報を開示いたします。
  - 不正アクセス/情報漏えい：DB へのアクセスログからの通知によって検知し、影響する顧客範囲およびデータ範囲についての情報を開示したします。
  - 当社が更新可能な、上記を引き起こす可能性がある 当社が重大と認識したセキュリティ脆弱性：定時レビューによって検知し、対応予定および対応状況についての情報を開示いたします。

- インシデントに関する通知を行う目標時間について、当社は以下のように定めております。
  - SLA を超えたシステム停止：停止を検知した後、SLA を超え次第に通知を行うことを目標といたします。また復旧次第の通知を目標といたします。
  - 不正アクセス/情報漏えい/アカウント乗っ取り(なりすまし)/迷惑メール送信：事象を検知した後、影響範囲が判明し次第に通知を行うことを目標といたします。
  - 当社が更新可能な、上記を引き起こす可能性がある 当社が重大と認識したセキュリティ脆弱性：事象を検知した後 5 営業日以内の通知を目標といたします。また対応が完了し次第に通知を行うことを目標といたします。

本資料の所有権は InstaVR 株式会社に帰属します。
InstaVR 株式会社の許諾なく本資料の全部もしくは一部を対外的に参照・配布することはできません。

- 上記のほか、天災等によるシステム停止に関して、非災害地域でバックアップから復旧をおこなう場合があります。

17. 認証

- 当社は、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS 適合性評価制度における ISMS 認証を取得しています。（https://isms.jp/lst/ind/）
- 当社は、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS 適合性評価制度における ISMS クラウドセキュリティ認証（https://isms.jp/isms-cls/lst/ind/）を取得しています。
- InstaVR は第三者の外部機関から、独立した監査を年に一度受けております。また、脆弱性の診断についても年に一度受けております。クラウドサービスカスタマ（見込含む）からご要望があった場合、開示可能な範囲で情報を提供します。（19.サービスに関するお問い合わせで記載があるフォームからお問い合わせください）

18. 外部クラウドサービスの利用

- 当社では、外部のクラウドサービスである AWS（Amazon Web Services 社提供）及びピアクラウドサービスとして Heroku（株式会社セールスフォース・ドットコム社提供）を利用しています。

19. サービスに関するお問い合わせ

- 当社コーポレートサイトのフォームよりお問い合わせください。（当社情報セキュリティ管理者又はシステム責任者へのお問い合わせも、同様のフォームよりお問い合わせください）

20. 当セキュリティホワイトペーパーの改定

- 当セキュリティホワイトペーパーの記載内容に変更があった場合は、すみやかにクラウドサービスカスタマに電子メール等の手段で通知いたします。

本資料の所有権は InstaVR 株式会社に帰属します。
InstaVR 株式会社の許諾なく本資料の全部もしくは一部を対外的に参照・配布することはできません。

改定履歴

版	改定年月日	改定内容（概要）
1.0	2019/05/15	初版
1.1	2019/06/13	3. データの削除：バックアップデータおよびログデータの削除のお取り扱いのご案内を追記 8. 暗号化の状況：Blowfish 暗号化方式以外のお取り扱いのご案内を追記 12. ログに関する情報：AWS のクロックとの同期方法について追記 14. 資産の取扱いに関する情報：例外的に取り扱われる SD カードの再利用の手順のご案内を追記 15. 開発におけるセキュリティ情報：開発標準に関する記載を追記 17. 認証：第三者機関による監査の情報及び請求の方法追記 19. サービスに関するお問い合わせ：当社情報セキュリティ管理者およびシステム責任者へのお問い合わせ方法を追記
1.2	2021/03/22	9. 変更管理：クラウドサービスの変更内容及び変更の適用状況についての情報提供方法を明記 13. 脆弱性管理に関する情報：技術的脆弱性の監視状況についての記載を追記及び外部監査の実施について記載を追記 16. インシデント発生時の対応：セキュリティ脆弱性の定義を追記 17. 認証：認証の取得に伴い取得状況を追記 18. 外部クラウドサービスの利用：ピアクラウドサービスの Heroku を追記