White Paper

プロセスマイニングソリューション

myInvenio Private Cloud

ハートコア株式会社

2022 年 8 月 17 日 (第 1.3 版)

はじめに

White Paper の目的

myInvenio Private Cloud はプロセスマイニングを実現する当社のクラウドサービスです。

本ドキュメントは、myInvenio 及び myInvenio の提供において基盤として利用するクラウドサービスにおけるセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMS クラウドセキュリティ認証である ISO/IEC 27017 の要求に従う公表を行うことを目的とします。

White Paper の対象

myInvenio の導入を検討中の方
myInvenio を利用中の方

クラウドコンピューティングのための情報セキュリティ方針

当社では、クラウドコンピューティングに関する情報セキュリティの方針を定め、ユーザ様に満足いただける機能的でセキュアなサービスの提供を目指しています。

当社は、クラウドコンピューティング環境におけるユーザ様の情報資産を情報セキュリティ上の脅威から保護するための措置を講じ、ユーザ様が安心してご利用いただけるセキュアなサービスを提供します。

当社の「情報セキュリティ方針」は以下の URL からご確認頂けます。
https://www.heartcore.co.jp/information_security/index.html

情報セキュリティ組織

当社では、情報セキュリティに関する統括責任者を任命し、情報セキュリティに関する統括責任と権限を与えています。また、情報セキュリティ委員会を設置し、情報セキュリティのマネジメントシステムの運用と継続的改善に取り組んでいます。

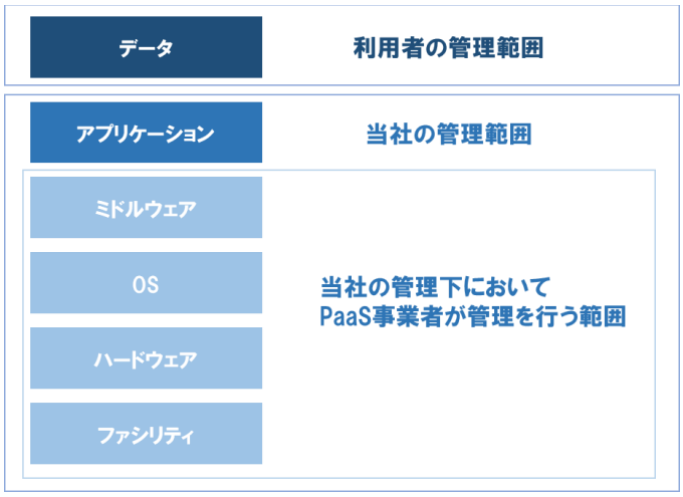
地理的所在地

当社の所在地、並びに当社がお客様のデータを保存する国は日本国となります。当社が基盤として利用するクラウドサービスにおいて、日本国以外のリージョンにユーザ様のデータを保存する必要性が生じた場合、ユーザ様に事前に通知したうえで行います。

責任範囲（共有 Model）

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、ユーザ様の責任において保護していただく必要があります。



※PaaS 事業者（アマゾン ウェブ サービス（以下 AWS））

情報セキュリティの意識向上，教育及び訓練

当社は、全従業員に対する定期的な情報セキュリティ教育を実施し、情報セキュリティに対する意識向上に努めています。また、クラウドコンピューティングに関する契約相手に対しても、同等レベルの教育を求めています。

情報セキュリティのパフォーマンス評価

当社では、定期的（最低でも年に一回）に情報セキュリティに関する内部監査を実施しています。定期的な内部監査以外に、組織、施設、技術、プロセス等の重大な変化にあわせて、独立した内部監査を行っています。

インシデント対応プロセス

当社では、ISO/IEC27001 に準拠した標準化された情報セキュリティインシデント対応プロセスを整備しています。情報セキュリティインシデントに関する報告、エスカレーションに関する全ての手順が文書化され、情報セキュリティ委員会により一元的に管理されています、報告されたインシデントはインパクトや緊急性に応じてハンドリングされています。

開発/調達

開発プロセス

当社の**クラウドサービス**の開発は、機能性とユーザビリティの確保はもちろんのこと、情報セキュリティについても配慮することを方針として行われます。開発は非機能要件としてのセキュリティ要件を定義し、厳格な承認プロセスを得たうえで実施されます。セキュリティ機能に関するソースコードはレビューされ、テストプロセスを経たうえでビルドされます。

また、リリース前のみならず、リリース後も定期的な脆弱性診断(システム開発元にて実施、必要に応じて診断結果を開示依頼)を行っています。

ブルーグリーンデプロイメント

当社の提供するクラウドサービスは、新バージョンのリリース時に、ブルーグリーンデプロイメントを採用しています。現バージョンの仮想環境（グリーン）と新バージョンの仮想環境（ブルー）を同時に用意し、アクセス先を切り替えることで、瞬時に新バージョンへの移行を可能としています。

サプライチェーン

当社のクラウドサービスの提供に関連するサプライヤー、及びサプライチェーンは以下の手段により管理することを方針としています。

・情報セキュリティ水準を当社と同等又はそれ以上に保つことを事前の審査により確実にする
・契約により秘密保持の確保を担保する
・サプライヤーがサプライチェーンを形成しサービス提供している場合、サプライヤーのサプライチェーンメンバーに対するセキュリティ管理の能力について審査する

アプリケーションのセキュリティ機能

情報セキュリティプラットフォーム

myInvenio システムの情報セキュリティは、プラットフォームとして使用するクラウドサービス事業者（AWS）の情報セキュリティ機能に依存します。当社は、クラウドサービス事業者（AWS）から提供される情報セキュリティがベストプラクティスであることを確認のうえ、プラットフォームとして採用しています。
https://d1.awsstatic.com/International/ja_JP/Whitepapers/AWS_Security_Best_Practices.pdf

情報セキュリティ機能

myInvenio システムがアプリ―ケーションとして実装する情報セキュリティ機能は「ユーザマニュアル」をご参照ください。
ユーザ様は、「責任範囲」に基づき、myInvenio システムにて取扱うデータに対してバックアップやアクセス権の設定などの対策を行う責任があります。

情報のラベル付け

myInvenio はユーザが任意の名前で作成した「プロセス」と呼ばれるエリアに対してユーザが指定したファイルを取り込みます。「プロセス」に対して、ユーザもしくはユーザグループを指定したアクセス制限設定が可能です。使用方法の詳細は「ユーザマニュアル」をご参照ください。

利用者アクセスの管理

myInvenio は、ユーザ様がストレスなく、安全に利用者アクセスの管理を行うためのユーザインターフェイスと機能を提供します。お客さまは管理者画面から簡単な操作によりアカウント登録・削除を行い、またユーザに対する権限の割り当てを行うことが出来ます。使用方法の詳細は「ユーザマニュアル」をご参照ください。

認証情報の管理

初期のアカウント登録手順は「ユーザマニュアル」をご参照ください。ユーザ様管理者により新規アカウント作成と初期パスワードの設定を行います。新規アカウントユーザは管理者により設定された初期パスワードを使用して初期ログインを行うと、ユーザ様独自のパスワード変更を行うよう指示されますので、パスワードの設定を行っていただきます。

パスワードの設定はユーザ様のセキュリティポリシーにもとづいて実施してください。また、myInvenio のユーザアカウントは 2 段階認証が可能です。

管理者権限はユーザ様のセキュリティポリシーに従い厳重に管理することをお願いします。

ユーティリティプログラム

ユーティリティプログラムは管理者権限に限定して利用可能です。管理者権限を厳重に管理することによりユーティリティプログラムの使用制限につながります。
ユーティリティプログラムは AWS コンソール及びコマンドプロンプトが該当します。

暗号化

myInvenio では、ユーザ様との間での通信を SSL/TLS1.2 により暗号化し、情報の盗聴等のリスクに対処しています。
データベースに保管されるユーザ様データは、AES256 暗号化アルゴリズムを使用して暗号化しています。

SSH のクライアント側のキーペアファイル（秘密鍵）はユーザ様の責任にて厳重に管理してください。

運用

変更

ユーザ様に影響を与える myInvenio の変更は、ご契約時のメールアドレス宛に事前通知します。
変更に伴うサービスレベルの取扱いについては「利用規約」に従うものとします。

バックアップ

当社のクラウドサービスでは、仮想マシンイメージの snapshot を取得しています。月次で Disk To Disk によるバックアップを取得しており、1 年間保持しています。ユーザ様のご要望に応じて、オンデマンドバックアップのご提供も可能です。バックアップ結果については、目視で確認する運用を行っています。異常が検知された際はクラウド担当者にて対応を行います。
また、バックアップ検証用サーバにて年一回バックアップリストア試験を行います。
尚、仮想マシン内の個別データのバックアップはユーザ様の責任において実施してください。

ログ

myInvenio は管理者権限、及びユーザの操作に関連したログを取得します。一定期間(1 日)のログは管理者画面から確認することができます。サービス提供中における操作ログは内部データベースに全て保持されます。サービス終了後の保存が必要な場合、CSV ファイルとして出力のうえ、ユーザ様の内部環境にて保管してください。

myInvenio は、基盤として利用するクラウドサービス事業者が提供するマネージドサービスを利用し、協定世界時 (UTC)への時刻同期を行っています。

技術的脆弱性の管理

アプリケーションを構築する上で使用するソフトウェアに脆弱性が検知された場合、myInvenio のトップ画面等で通知し、速やかに影響調査を行います。
脆弱性情報の収集は以下の手段により行います。
・JPCERT コーディネーションセンターから公開される脆弱性情報
・当社関係者による検知
・ユーザ様、基盤を提供するクラウドサービス事業者等の外部からの情報提供

検出した脆弱性については、速やかに影響調査を行い、必要な対策を講じます。対策の状況は随時、myInvenio のトップ画面にて公表します。

ネットワーク

myInvenio 専用の仮想ネットワークを構築し、入口への侵入を IDS/ IPS により監視することによりセキュリティを確保しています。

myInvenio は、お客様のテナント毎にネットワーク設定を行います。お客様ご指定のネットワーク以外からはアクセス遮断の設定を行う事で、他のユーザ様とのネットワークの分離を適切に行っています。
myInvenio は、ユーザ様に提供するクラウドコンピューティング環境と、当社の管理用環境を別セグメントとして分離しています。

容量・能力の管理

当社は、サーバリソース、及びネットワークリソースを監視しています。またリソースの増減は GUI から瞬時に実行することができます。サーバリソースはインスタンスの構成を変更せずにスケールアップによることを原則としていますが、将来的なニーズに照らして、必要があればスケールアウトによる対応も行います。
監視には監視ツールを利用し、監視ログは 5 年間保有しています。

負荷分散/冗長化

myInvenio は基盤を提供するクラウドサービス事業者のマネジメントサービスを使用し、複数の仮想サーバに処理を振り分ける、ロードバランバランシングを採用しています。

また、アプリケーションの構成はマシンイメージとして保存し、即時に複製が可能な状態を整えています。

インシデント対応

myInvenio に関連した情報セキュリティインシデントを検出した場合、当該インシデントによるユーザ様への影響が懸念される場合は、速やかにご契約時のメールアドレス宛に通知します。

また、ユーザ様において情報セキュリティインシデントを検出された場合、またはその疑いをもたれた場合は、弊社サポートサイトのお問合せページ、又は当社カスタマーセンターへご連絡ください。

サポートサイト: https://support.heartcore.co.jp
メール: support-desk-dx@heartcore.co.jp

サービス利用停止後のデータの扱い

myInvenio の利用契約終了後のデータの取扱いは、「利用規約」に従います。保持が必要なデータ等が存在する場合、ユーザ様の責任において、利用契約終了前にダウンロード等をお願い致します。
ただし、クラウドサービス派生データのうち、仮想ネットワークへのアクセスに関するログ、サービスのバージョンアップに関する内部要員による作業ログ、及びコマンドログ以外は削除します。

装置のセキュリティを保った処分又は再利用

当社は、情報システム管理者に装置の処分又は再利用に関する役割を集中し、従業員による個別対応を排除することで、セキュア且つ確実な装置の処分又は再利用を実現しています。

その他

証拠の収集

法令また権限のある官公庁からの要求により myInvenio 上にあるデータ等の情報を、当該官公庁またはその指定先に開示もしくは提出することがあります。合意について別途、「利用規約」をご参照ください。

適用法令及び契約上の要求事項

利用契約に関する準拠法は、日本法とします。別途、「利用規約」をご参照ください。

知的財産権

本サービスを構成する有形または無形の構成物（プログラム、データベース、画像、マニュアル等の関連ドキュメントを含むがこれらに限られない）に関する著作権を含む一切の知的財産権その他の権利は当社に帰属します。別途、「利用規約」をご参照ください。

記録の保護

アプリケーションにおけるデータ操作等のログはユーザ様にて保護して頂く必要があります。当社は、仮想ネットワークへのアクセスに関するログ、及びサービスのバージョンアップに関する内部要員による作業ログ及びコマンドログを一定期間(毎月 5 営業日までに、前月分のログを取得する、ファイルサーバにて 1 年間保管)保存します。

暗号化機能に対する規制

myInvenio において暗号化の規制対象になる国は存在しません。

第3者認証

ISO/IEC27001

当社は、全社を認証範囲として 2018 年 8 月 11 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。]

ISO/IEC27017

当社は、プロセスマイニングサービス(myInvenio Private Cloud)を認証範囲として 2021 年 1 月 10 日に ISMS クラウドセキュリティの国際規格である ISO/IEC27017 を取得しています。

改定履歴

改訂日	版数	内容	承認	作成
2020/10/26	1.0	新規制定	宮田	三宅
2020/12/15	1.1	バックアップ仕様の追記 情報セキュリティプラットフォームの追記	宮田	三宅
2021/6/29	1.2	開発プロセスの追記 ログの追記 記録の保護の追記 暗号化アルゴリズム記載誤り修正	保坂	宮田
2022/8/17	1.3	サービス利用停止後のデータの扱いの追記 ユーティリティの追記 容量・能力の管理の追記 第 3 者認証の追記	宮田	後藤