White Paper

ECAI

第 1.0 版

2021 年 3 月 23 日

株式会社バイモソフト

はじめに

White Paper の目的

本ドキュメントは、ＥＣＡＩ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

ＥＣＡＩの導入を検討中の方
ＥＣＡＩ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。

> **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方針**
> 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://baimosoft.co.jp/pdf/i_security_policy.pdf

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

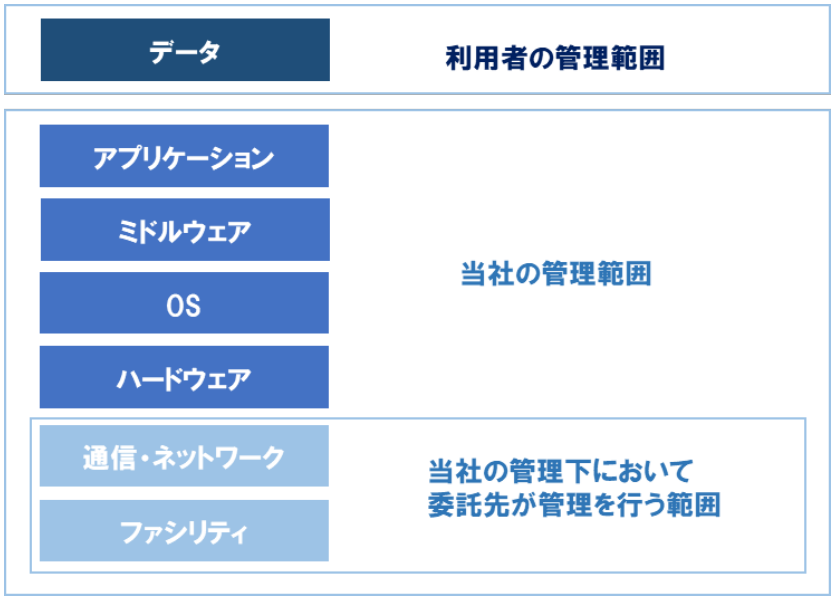
当社の所在地、並びに当社がお客さのデータを保存する国は日本国となります。当社が基盤として利用するクラウドサービスにおいて、日本国以外のリージョンにユーザ様のデータを保存する必要性が生じた場合、ユーザ様に事前に通知したうえで行います。

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。



当社の責任

・ＥＣＡＩのセキュリティ対策

・ＥＣＡＩに保管されたユーザ様情報の保護（バックアップも含む）

ユーザ様の責任

・利用者アカウントの管理（登録、削除、権限設定、管理者設定、アクセス権の設定など）

・パスワード等の利用者の秘密認証情報の管理

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。
内部監査結果をユーザ様が必要となる場合は、問合せ窓口のチャットワークサポートまでご相談ください。

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、修正時にはテスト仕様に準じたペネトレーションテストを行っています。

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

情報セキュリティ機能

主にユーザ様が検討される情報セキュリティ機能として、本ホワイトペーパーは以下を記述しています。

機能（ISO/IEC27017 の管理策）	本ホワイトペーパーの記述
A.9.2.1 利用者登録及び登録削除	利用者アクセスの管理
A.9.2.2 利用者アクセスの提供	利用者アクセスの管理
A.9.2.3 特権的アクセス権の管理	認証情報の管理
A.9.2.4 利用者の秘密認証情報の管理	認証情報の管理
A.9.4.1 情報へのアクセス制限	利用者アクセスの管理
A.10.1.1 暗号による管理策の利用方針	暗号化
A.12.3.1 情報のバックアップ	バックアップ
A.12.4.1 イベントログ取得	ログ
CLD.12.4.5 クラウドサービスの監視	クラウドサービスの監視

情報のラベル付け

ＥＣＡＩは、以下の機能を提供し、ユーザ様のデータ分類をサポートします。

・アドレス登録データへのタグ付けによるグルーピング

・ユーザに任意に付帯情報を追加

使用方法の詳細はサービス内のマニュアルサイトをご参照ください。

認証情報の管理

ＥＣＡＩの利用にあたって以下の手順でマスタアカウントを登録いただきます。

１．申込フォームにメールアドレスを登録いただきます。

２．登録頂いたメールアドレス宛にクレジット決済用 URL　が記載されたメールが届きますので、画面の指示に従い決済を行っていただきます。

３．決済の正常終了で、登録頂いたメールアドレスに認証コードをお送りし、さらに登録画面に遷移します。

４．登録画面にて、画面の指示に従い認証コードの入力、パスワードの設定等を行っていただきます。設定後にシステムを自動構築します。

５．構築完了後に登録頂いたメールアドレス宛にアカウント情報及び問合せ窓口のチャットワークサポートのアカウント情報をお送りします。

利用者アクセスの管理

ＥＣＡＩは、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。お客さまはマスタアカウント画面から簡単な操作により利用者のアカウント登録・削除を行い、また利用者に対する権限の割り当てを行うことが出来ます。使用方法の詳細はサービス内のマニュアルサイトをご参照ください。

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マスタアカウントに限定して利用可能です。マスタアカウント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。

暗号化

ＥＣＡＩとユーザ様との間での通信は、SSL/TLS で暗号化し、情報の盗聴等のリスクに対処しています。

運用

変更

ユーザ様に影響を与えるＥＣＡＩの変更は、情報提供用のチャットワークグループにより事前通知します。
また、各種の変更管理に関する情報はシステムログイン時のダッシュボード画面より、確認することができます。

管理者用手順

サービス内のマニュアルサイトの提供に加え、チャットワークによる質問対応をしています。

バックアップ

システム及びユーザ様データのバックアップは、日次で７世代分のデータを保持します。
ただし、ユーザ様からのバックアップデータの復元等に関するご要望には対応してせん。

ログ

ＥＣＡＩの維持管理に必要となる適切なログを取得しています。
ユーザ様が必要となる場合は、問合せ窓口のチャットワークサポートまでご相談ください。
尚、配信の履歴はユーザ様で確認ができます。確認方法の詳細はサービス内のマニュアルサイトをご参照ください。

ＥＣＡＩは、「NICT インターネット時刻供給サービス」を利用し時刻同期を行っています。
ログは、日本標準時（UTC＋９）で提供されます。

クラウドサービスの監視

当社は、ＥＣＡＩが正常に提供され、他社を攻撃する基盤として使用される等に不正に使用されていないこと、データの漏洩が発生していなか等の監視を行っています。
監視結果をユーザ様に公開できるサービス機能は有しておいません。監視結果が必要な場合は、問合せ窓口のチャットワークサポートまでご相談ください。

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、チャットワークサポート等で通知し、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、チャットワークサポートにて通知します。

ネットワーク

ＥＣＡＩ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。

ＥＣＡＩは、他のユーザ様との分離を適切に行っています。専用サーバは、サーバ単位で、共有サーバはスキーマをデータベース単位で、Web サーバ　のデイレクトリ単位で分離しています。
また、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。

負荷分散/冗長化

ＥＣＡＩ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

ＥＣＡＩ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、以下の内容で速やかに通知します。

項目	内容

報告する範囲	データの消失、サービス停止等のユーザ様に大きな影響を及ぼす可能性のある情報セキィリティインシデント
対応の開示レベル	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、すべて同等のレベルで対処します。
通知を行う目標時間	検知から 72 時間以内を目標に通知します。
通知手順	ご登録頂いたメールアドレス宛、管理者画面 （必用に応じて電話等の手段を使用する場合もあります。）
問合せ窓口	お問合せ窓口
適用可能な対処	当社に起因する情報セキュリティインシデントでユーザ様に影響があるものは、あらゆる手段を講じて対処します。

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、ＥＣＡＩ内の問合せ窓口のチャットワークサポートからご連絡ください。

サービス利用停止後のデータの扱い

ＥＣＡＩで利用者様が作成・保存した利用者様のデータの除去に関しては、解約後 30 日以内に以下の様に消去いたします。ただし、利用者様のデータを含まないサービス共通のログデータは対象外になります。

・専有サーバ：完全に消去
・共有サーバ：ユーザの OS の機能によるファイルを削除

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

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。

記録の保護

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を一定期間保存します。

暗号化機能に対する規制

ＥＣＡＩにおいて暗号化の規制対象になる地域にはサービスを提供していません。

ＥＣＡＩに関するお問い合わせ

チャットワークサポートにて対応します。

※　チェットワークサポートは事前登録が必要です。

更新履歴

版数	日付	更新内容
第 1.0 版	2021 年 3 月 23 日	初版