White Paper

SDGs プラットフォーム　BRIDGES

第 1.1 版

2023/7/31

株式会社ネイティブクリエイション

NC, Inc.

はじめに

White Paper の目的

当社が運営する SDGs プラットフォーム「BRIDGES」は、SDGs を推進する法人や、関心のある個人のお客様を支援するクラウドサービスです。本サービスでは、主に以下の機能を提供しています。

・SDGs 評価システム

・SDGs 市場のマッチングプラットフォーム

本ドキュメントは、BRIDGES 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

BRIDGES の導入を検討中の方

BRIDGES 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、お客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お客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、お客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。

第3者認証

ISO/IEC27001

当社は、全社を認証範囲として 2023 年 6 月に ISMS（Information Security Management System）の国際規格である ISO/IEC27001 を取得する予定です。

ISO/IEC27017

当社は、BRIDGES を認証範囲として 2023 年 6 月に国際規格である ISO/IEC27017（ISO/IEC 27017）ISMS クラウドセキュリティ認証を取得する予定です。

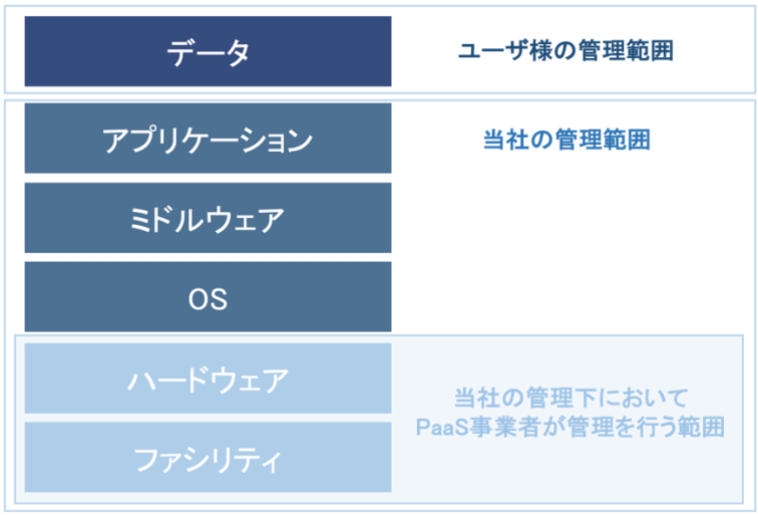
情報セキュリティのための組織(A.6)

責任分界点(A.6.1.1)

仮想レイヤーやファシリティ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、サプライヤーに対する当社の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、クラウドサービス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、お客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

・BRIDGES のセキュリティ対策

・BRIDGES に保管されたお客様情報の保護

お客様の責任

・アカウントの管理(登録、削除、権限設定、管理者設定など)

・パスワード等の利用者の秘密認証情報の管理

・お客様が取扱うデータに対してのバックアップ

地理的所在地(A.6.1.3)

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お客様のデータを保存する必要

性が生じた場合、お客様に事前に通知した上で行います。

資産の管理（A.8）

情報のラベル付け（A.8.2.2）

BRIDGES は、共有フォルダによるファイル管理機能を提供し、お客様のデータ分類をサポートします。任意のフォルダ名を指定して、ファイル保存・削除が出来ます。また、ファイルは 3 世代分のデータを保持し、復元が可能です。

サービス利用停止後のデータの扱い(CLD.8.1.5)

BRIDGES でお客様が作成・保存した、お客様のデータの除去に関しては以下の方針に従い完全に消去いたします。

・削除申請があった場合、申請受領後 7 営業日以内に DB から消去。

※サービス共通のアクセスログデータは、1 年後自動削除

※グループ管理者がグループを削除した場合、該当グループの関連データ（掲示板・共有フォルダ等）は、削除申請後 20 営業日以内に DB から消去。

※掲示板・共有フォルダへ、お客様が保存したデータについては、自動削除されません。データを除去したい場合は、利用停止前にご自身で削除ください。

なお、利用停止後、お客様のアカウント名は「サービス退会者」と表示されるため、アカウント名から個人が特定されることはありません。

アクセス制御（A.9）

利用者アクセスの管理(A.9.2.1)(A.9.2.2)

BRIDGES は、お客様がストレスなく、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。お客様は、簡単な操作によりアカウントの登録・削除・変更を行えます。

※お客様が、企業アカウントを作成される場合は、事務局へ申請が必要です。申請後、事務局からアカウント登録内容をご案内します。

認証情報の管理(A.9.2.3)(A.9.2.4)

BRIDGES の登録画面でアカウントの仮登録完了後、登録したメールアドレスに対し、一定時間のみ有効なパスワード設定用 URL が記載されたメールが届きます。メールの URL をクリックして、画面指示に従ってパスワードを設定すると本登録が完了します。

パスワードの設定はお客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。パスワードの設定は 16 文字以上　英数字混在　大小文字を組み合わせて設定してください。

管理ユーザの扱いは、お客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。

暗号（A.10）

暗号化(A.10.1.1)

データベースに保管されるお客様データは、AES-256 暗号化アルゴリズムを使用して暗号化しています。
お客様のパスワードは、そのままのコードで保存せず、不可逆のハッシュ化をしています。
BRIDGES とお客様との間での通信は、TLS1.2/1.3 で暗号化し、情報の盗聴等のリスクに対処しています。

運用のセキュリティ（A.12）

変更(A.12.1.2)

お客様に影響を与える BRIDGES の変更は、ご登録頂いたメールアドレス宛に事前通知します。また、TOP 画面で変更に関する情報を確認することができます。

バックアップ(A12.3.1)

システム及びお客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、お客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いません。

ログ(A.12.4.1)(A.12.4.4)

BRIDGES の維持管理に必要となる適切なログを取得しています。
お客様が必要となる場合は、当社の BRIDGES 事務局までご相談ください。

BRIDGES 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時刻同期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。

技術的脆弱性の管理(A.12.6.1)

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で、利用者に影響を与える可能性のある脆弱性が検知された場合、BRIDGES のトップ画面等で通知し、速やかに影響調査を行います。
検出した脆弱性については必要な対策を講じ、対策の状況は随時、BRIDGES のトップ画面にて公表します。

管理者用手順(CLD12.1.5)

管理画面のヘルプ(予定)より、サービスの利用に必要な操作手順を提供致します。

クラウドサービスの監視(CLD12.4.5)

当社は、BRIDGES の稼働状況並びに障害発生状況について監視を行っています。
監視結果をお客様に公開できるサービス機能は有しておりません。監視結果が必要な場合は、当社の BRIDGES 事務局までご相談ください。

通信のセキュリティ（A.13）

ネットワーク(A.13.1.3)

BRIDGES は、クラウドサービスのネットワーク仮想化技術を利用して、他サービスとのネットワークの分離を適切に行っています。
また、お客様に提供するインターフェイス環境と、当社の管理用環境を別のネットワークセグメントとして分離しています。

システムの取得、開発及び保守（A.14）

情報セキュリティ機能(A.14.1.1)

主にお客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

開発プロセス(A.14.2.1)

当社のクラウドサービスの開発は、商用とは異なる独立した開発・検証環境で行われ、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。セキュリティ機能はレビューとテストを経たうえで公開されます。

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
・契約により機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。

情報セキュリティインシデントの管理（A.16）

インシデント対応プロセス(A.16.1.1)

当社では、適切な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。

インシデント対応

BRIDGES 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、長時間のシステム停止等のお客様に大きな影響を及ぼす可能性のある情報セキュ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お客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、TOP 画面 （必要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	BRIDGES 事務局
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お客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、お客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、BRIDGES 内のお問合せ窓口、又は当社 BRIDGES 事務局からご連絡ください。

証跡の収集(A.16.1.7)

法令または裁判所の命令に基づき開示が義務付けられた際、お客様への通知または同意を得ることなく開示することがあります。詳細は、利用規約をご確認ください。

順守（A.18）

適用法令及び契約上の要求事項(A.18.1.1)

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。

暗号化機能に対する規制(A.18.1.5)

BRIDGES 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。

情報セキュリティのパフォーマンス評価(A.18.2.1)

ISO/IEC27001 と ISO/IEC27017 について第三者による審査を受け、認証の取得状況を弊社ウェブサイトで公開しています。
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。
監査結果に関しては、BRIDGES 事務局までご連絡下さい。

BRIDGES に関するお問い合わせ

メール：info@ncinc.jp

更新履歴

版数	日付	更新内容
第 1.0 版	2023/4/12	初版
第 1.1 版	2023/7/31	A.8.1.5、A.16.1.1 の内容修正、 A.16.1.7 の新規追加