「スマート公共ラボ with LINE SMART CITY GovTech プログラム」
「スマート公共ラボ電子申請」
ホワイトペーパー

2024 年 1 月

プレイネクストラボ株式会社

1. はじめに

1.1. 本書の目的

本書は、プレイネクストラボ株式会社（以降、当社と記載）のクラウドサービスについて、当社のセキュリティへの取り組みをご理解いただくとともに、当社クラウドサービスを安全にご利用いただくための留意事項をご確認いただくことを目的としています。

当社のサービスはSaaSとして提供し、インターネットからのアクセスとなります。顧客から取得したデータは重要情報として扱い、セキュリティに配慮されてクラウド上の環境にて厳密に管理しております。

1.2. 適用範囲

本書の適用範囲となる製品は以下の通りです。

スマート公共ラボ with LINE SMART CITY GovTech プログラム

地方自治体と住民との接点のDXソリューションでLINE公式アカウントの拡張システムを提供

スマート公共ラボ電子申請

LINEのアプリ内で各種行政手続きのオンライン化を実現するサービスの提供

2. セキュリティ方針

2.1. 情報セキュリティ方針

当社は情報セキュリティ方針を定め、クラウドサービスカスタマが安心して当社のクラウドサービスをご利用いただけるように取り組んでおります。
また、この情報セキュリティ方針及び関連する社内規則等は、毎年見直しております。
本書以外の情報セキュリティ関連の公開文書は以下をご確認ください。

	公開文書	リンク
1	情報セキュリティ方針	https://www.playnext-lab.co.jp/information-security-policy/
2	プライバシーポリシー	https://www.playnext-lab.co.jp/privacy-policy/

2.2. 責任分界点

当社は、利用者と当社の情報セキュリティの責任範囲について下記のとおり定義しております。

利用者の責任	1. ユーザー管理のデータ (1) ログイン ID 及びパスワード (2) 当社サービスにアップロードするデータ (3) 当社サービスからダウンロードしたデータ 2. 当社発行の管理者アカウントの運用 3. サービスの設定内容 4. インターネット環境 5. ユーザー端末
当社の責任	1. 管理者アカウントの発行 2. Web アプリケーション 3. LINE 上のアプリケーション 4. 保存データ(顧客情報、設定情報、各種ログデータ) 5. クラウドサービスプラットフォーム

＜補足＞
構築・運用サポートやインシデントが発生した際にお客様環境へログインを行い、作業をする場合がございます。

2.3. ICT サプライチェーン

当社は、クラウドサービスプラットフォーム(Amazon Web Services)を利用して環境を構築しています。

2.4. 個人情報保護

当社は、プライバシーポリシーに記載の通り、個人情報を保護しております。詳しくは 2.1 情報セキュリティ方針をご確認ください。

3. 利用者へのセキュリティ機能の提供

3.1. 情報資産の管理

3.1.1. 情報資産のラベル付け

当社は、利用者が情報を分類し、ラベル付けをするための機能を提供しております。具体的な操作手順はマニュアルをご覧下さい。

3.2. アクセス制御

3.2.1. 利用者登録及び登録削除

導入時に責任者のアカウントは当社が発行します。当社は、責任者もしくはユーザを追加可能な権限を持っている者がユーザーアカウントを登録および削除する機能を提供しております。

3.2.2. アカウント管理及びアクセス権の管理

当社はアカウントのアクセス保護のための仕組みとして ID とパスワードによる認証を提供しています。また、各ユーザの業務内容に合わせて、権限を変更し、アカウントを作成することが可能となっております。

3.2.3. IP アドレスの制限

当社は管理画面へのアクセスを提供先の要望に合わせて IP アドレスによるアクセス制限を実施しております。

3.3. 運用

3.3.1. アクセスログ取得

当社は、利用者のアカウントに対して、アクセスログを取得している。

3.3.2. 操作ログ取得

当社は、利用者のアカウントに対して、アプリケーションの操作ログを取得しております。

3.3.3. 利用状況の確認

当社は、利用状況を取得しております。

4.利用者へのセキュリティ情報の提供

4.1.当社の開発や運用における共通方針

4.1.1.技術的脆弱性の管理

当社は、クラウドサービスを開発・運用する際に、当社のセキュリティポリシーに従って定期的に脆弱性評価を実施しています。また、脆弱性情報を収集するとともに、脆弱性対策を実施しています。

4.1.2.クロックの同期

当社が提供するクラウドサービス内で提供する時刻情報は、タイムゾーン JST（UTC+9）で取得されます。ログの時間は、クラウドサービスプラットフォーム（AWS）が提供する NTP サービスに同期されています。

4.2.当社の開発方針

当社は、社内で定めた開発規定にしたがってクラウドサービスを開発しています。この規定に従い、開発時にはソースコードレビューを実施し、レビューを実施したソースコードしか本番環境に反映できない仕組みとすることで、開発したソースコードが開発規定に従っていることを確認しています。
また開発規定はセキュリティ上の注意点も含んでおり、脆弱性診断ツールなどを用いて、脆弱性を診断することで、安全性を確認しています。

4.2.1.通信の暗号化

当社は、通信内容を暗号化しております。

4.2.2.データの暗号化

当社は、利用者データをサーバー上に保存する際も暗号化をしております。

4.2.3.ネットワーク及び仮想コンピューティング環境における分離

当社は、利用者が別の利用者のデータを閲覧することができないよう、また当社の従業員が利用者のデータを必要以上に閲覧することができないように、適切に分離しております。

4.2.4.仮想マシンの要塞化

当社は、クラウドサービスの提供に AWS を利用し、WAF による制御など、各種対策を実施しております。

4.2.5.情報のバックアップ

当社は、以下に従い、データのバックアップを取得しております。なお、バックアップデータからの復旧機能はユーザーに提供しておらず、当社がクラウドサービスを運用する中で必要と判断した場合にのみ、バックアップデータから復元を実施します。

4.3. 当社の運用方針

4.3.1. アプリケーションのサービスレベル

当社は、クラウドサービスのサービスレベルとして以下の指標として定めています。

項目	設定
サービス時間	1. Web 上で提供するサービス：24 時間 365 日 2. サポートサービス：9:00～17:30（土日祝日、年末年始、当社所定の休暇を除く） ※ 緊急時の場合は除く
計画停止	メンテナンスやバージョンアップ等の為、計画停止を行います。計画停止は年間 8.8 時間以内とし、可能な限り夜間に行います。但し、合理的な理由から早朝、日中帯で行う可能性もございます。
計画停止予告案内	14 日前までに電子メール、もしくはコミュニケーションツールなどで案内致します。 緊急停止セキュリティ危殆化等のやむを得ない場合は計画停止とは別途の緊急停止がありえます。また、当社は合理的な努力をもって管理を行い欠陥や障害に備えますが、本サービス用設備にやむを得ない故障や欠陥が認められた場合、サービスを停止する場合がございます。
サービス稼働率	99.9%以上 ※上述の計画停止時間を含みます。
アップデート	アップデートは都度当社が必要と判断した場合、実施します。

4.3.2. 変更管理

機能の変更や廃止、一時的なメンテナンスなど、利用者に影響を与える可能性が生じる場合は、電子メール、もしくはコミュニケーションツールなどにより利用者に通知します。

4.3.3. ネットワークセキュリティ管理の整合

仮想ネットワークの間で整合がとれなくなるような変更作業が行えないように、ネットワークセキュリティを管理しています。

4.3.4. 情報機器の処分または再利用

当社は、利用していた情報機器を廃棄及び再利用する際は、当社の取り決めに基づき適切に処理を行っています。

4.3.5. クラウドサービスカスタマの資産の除去

契約管理者が当社のクラウドサービスを解約された場合、解約後はクラウドサービス上の各種データをダウンロード不可となります。必要に応じて、解約前

にダウンロードして下さい。当社は、利用者がサービスの利用を終了した場合、当社所定の期間を経過後、アップロードデータ、生成データを削除します。消去したデータはいかなる場合でも復旧することはできません。

4.3.6. 容量・能力の提供

当社は、サービス提供のために利用しているリソースを監視し、必要に応じてリソースを増強します。

4.3.7. 障害対応と復旧までの目標時間

何らかの理由でクラウドサービスが停止した場合、当社は復旧計画に従ってサービスの普及を試みます。単一障害が発生した場合の目標復旧時間は 1 時間としています。複合障害が発生した場合の目標復旧時間は 24 時間を目指します。

4.4. 情報セキュリティインシデントの取り扱い

4.4.1. 報告するインシデントの範囲

情報インシデントのうち、利用者に明確な被害が及ぶ場合又はクラウドサービスの継続に影響を及ぼすと判断された場合を重大インシデントと定義して、利用者への報告対象とします。以下に示すようなものが重大インシデントに該当します。

1. クラウドサービスへの不正アクセスにより、サーバーに保存された情報が外部に流出した。
2. サーバーのウイルス感染により、サーバーに保存された情報が外部に流出した。
3. 外部からの攻撃により、クラウドサービスが利用できない状態となり、その状態が一定時間以上継続した。
4. なりすましサイトにより、クラウドサービスの利用者に被害が発生した。

4.4.2. インシデントの通知手順と通知までの目標時間

利用者に大きな影響を与える情報セキュリティインシデント（データの消失、長時間のシステム停止等）が発生した場合は、当社が情報セキュリティインシデントを発見してから１営業日以内を目標に電子メール、もしくはコミュニケーションツールなどにより利用者に通知します。なお、情報セキュリティインシデントに関する問合せは、サービス窓口より受け付けています。

4.5. コンプライアンス

4.5.1. 所在地及び利用者データの保存場所

当社は、日本の法人であり、本社所在地は東京都です。クラウドサービスの開発、運営は全て日本国内で行っております。
クラウドサービスは、AmazonWebServices（AWS）を利用して構築しており、システムが保管するデータ及びそのバックアップデータは、AWS が管理する日本国内のデータセンターに保管されています。

4.5.2. 適用法令

当社と利用者との間の契約における適用法令は適用される「準拠法」は「日本法」となります。

4.5.3. 証拠の収集

当社は、サービス内で収集されるデジタル証拠となりうるデータ（ログや利用者コンテンツなど）を第三者（警察や裁判所など）に提出する場合がございます。

4.5.4. 記録の保護

利用者データは、不正なアクセスや改ざんを防ぐため、許可された従業員しかアクセスできない、適切に管理されたアクセス権のもとで保管されます。

4.5.5. 情報セキュリティの独立したレビュー

当社は、JISQ27001（ISO/IEC27001）および JIS27017（ISO/IEC27017）について第三者による審査を受け、それぞれの認証を取得しております。

5. 改訂履歴

版数	日付	主な変更内容
1.0	2024 年 1 月 18 日	初版作成
1.1	2024 年 3 月 14 日	4.5.5 JIS27017（ISO/IEC27017）の取得を追記

■お問い合わせ
ご購入前のお客様からの、資料請求、お見積もり、ご購入、ご導入などついてのお問い合わせは下記にて承っております。
https://www.playnext-lab.co.jp/#contact