セキュリティホワイトペーパー

当社が提供するSaaSにおける

ISO/IEC 27017 に基づくクラウドセキュリティへの取り組み

第1版

2026年11月26日

株式会社World Wide System

はじめに

クラウドサービスを利用する組織にとって、預けた情報がどのように守られているかは重要な関心事です。クラウドサービスの情報セキュリティについては、国際規格 ISO/IEC 27017 が、クラウドサービスの利用者と提供者が実施すべき管理策を定めています。本書では、株式会社World Wide System（以下「当社」）が提供する SaaS のうち、「サービス概要」に記載するサービス（以下「本サービス」）における、ISO/IEC 27017（以下「ISO27017」）に基づくクラウドセキュリティへの取り組みを説明します。本書が、本サービスを安心してご利用いただくための判断材料としてお役に立てば幸いです。なお、本書の内容は作成日時点のものです。各項目の詳細は、各項目に記載した公開資料（セキュリティチェックシート等）でご確認ください。

サービス概要

本書の対象は、当社が SaaS として提供する次のサービスです。各サービスの内容は、それぞれのサービスサイトをご覧ください。

MapPenguin（デジタルマップ作成システム。別プランの MapPenguin Business を含む）
https://www.mappenguin.com/

SmartKuji（くじ引きキャンペーンシステム）　https://kuji.smartpr.jp/

SmartE-Coupon（デジタルクーポンシステム。別プランの BeneTicket を含む）
https://e-coupon.smartpr.jp/

SmartStamprally（デジタルスタンプラリーシステム）　https://rally.smartpr.jp/

SmartReceico（レシート応募キャンペーンシステム）　https://receico.smartpr.jp/

SmartContest（コンテスト＆投票審査システム）　https://contest.smartpr.jp/

SmartStampCard（スタンプカードシステム）　https://receico.smartpr.jp/stamp/

本サービスは、利用規約に同意のうえ、利用申込書によりお申込みいただいたお客様に提供します。管理画面の操作方法は、サービスごとの操作説明書でご案内します。

ISO27017 の概要

ISO27017 は、情報セキュリティ管理策の実践のための規範である ISO/IEC 27002 を、クラウドサービス向けに補い、クラウドサービスに固有の管理策を加えた国際規格です。当社は、情報セキュリティマネジメントシステム（ISMS）の国際規格 ISO/IEC 27001 に基づく体制を運用しており、この体制に ISO27017 の管理策を加えることで、クラウドサービスの提供者および利用者としての情報セキュリティに取り組んでいます。当社の第三者認証の認証番号と有効期限は、当社Webサイトの「セキュリティ資料」ページ（https://ww-system.com/esg/security-materials/）で公開しています。

ISO/IEC 27017：クラウドサービスのための情報セキュリティ管理策の実践の規範

＋

ISO/IEC 27001：情報セキュリティマネジメントシステムの要求事項

ISO27017 に対する取り組み

1. 情報セキュリティのための方針群

1.1 情報セキュリティのための方針群

本サービスは、当社の「情報セキュリティ方針」「情報クラウドセキュリティ方針」「プライバシーポリシー」に従い、情報セキュリティを経営上の重要な事項として運営しています。これらの方針は当社Webサイトで公開しています。

情報セキュリティ方針　https://ww-system.com/esg/security/

情報クラウドセキュリティ方針　https://ww-system.com/esg/cloud-security/

プライバシーポリシー　https://ww-system.com/policy/privacy-policy/

方針に基づくデータ保護の内容、サービスの責任分界点、セキュリティチェックシート、サービスレベル目標（SLO）は、当社Webサイトの「セキュリティ資料」ページ（https://ww-system.com/esg/security-materials/）で公開しています。また、個人情報・秘密情報の取扱いと守秘義務は、利用規約（第29条・第30条）で定めています。

2. 情報セキュリティのための組織

2.1 情報セキュリティの役割及び責任

お客様と当社の役割・責任の分担は、「サービスの責任分界点」と利用規約で定め、当社Webサイトで公開しています。

サービスの責任分界点　https://ww-system.com/data/terms/pdf/boundary.pdf

利用規約　https://ww-system.com/data/terms/pdf/terms.pdf

また、本サービスを支える供給者との役割は契約で定めており、物理設備・ネットワーク基盤はクラウド事業者（Amazon Web Services）、サーバーのOS・ミドルウェアの運用保守と監視は運用委託先、Webサイト・アプリケーションの開発・保守は当社が担っています。

2.2 関係当局との連絡

本サービスのデータは、Amazon Web Services の東京リージョン（日本国内）に保管しています。ただし、SmartReceico でレシート画像の読み取りに外部の AI サービス（Google Gemini API）を選択した場合、画像の処理場所は日本国外となる場合があります（画像は Google 側に保存されません）。また、SmartContest の応募動画は外部の動画配信サービス（Cloudflare Stream）に保存され、保存場所は日本国外となる場合があります。これらは、各サービスのセキュリティチェックシートでもお知らせしています。当社の所在地は、当社Webサイトの会社概要ページ（https://ww-system.com/company/）に記載しています。

2.3 クラウドコンピューティング環境における役割及び責任の共有及び分担

お客様には、お申込みの際に、利用申込書の「利用規約への同意」欄で、利用規約と「サービスの責任分界点」をご確認のうえ、同意してお申込みいただいています。本サービスは、この同意を前提に提供しています。

3. 人的資源のセキュリティ

3.1 情報セキュリティの意識向上、教育及び訓練

当社は、情報セキュリティ方針（https://ww-system.com/esg/security/）に従って本サービスを運営しています。お客様のデータ（クラウドサービスカスタマデータ）と、本サービスの利用に伴って生じるデータ（クラウドサービス派生データ）を取り扱う従業者には、その取扱いについて定期的に教育を行っています。また、本サービスの運用を担当する従業者には、着任時に、本番環境の操作や認証情報の管理に関する注意事項を説明しています。運用委託先の従業者に対する教育は、委託先の評価の際に確認しています。

4. 資産の管理

4.1 資産目録

本サービスの基盤設備と、お客様のデータを保管するシステムは、当社の情報資産台帳に記載して管理しています。お客様から預かったデータと、本サービスの運用で当社が生成するデータ（アクセスログ・操作ログ等）は、台帳上で区別して管理しています。

4.2 クラウドサービスカスタマの資産の除去

契約終了時のデータの返却と削除の取決めは、利用規約（第24条）と利用申込書で定め、お申込みの際に同意をいただいています。お客様は、契約終了前に、管理画面からデータを CSV 形式でダウンロードできます。当社はデータを返却する義務を負いませんが、個別にご依頼いただいた場合は、データの保存・出力を有償で承ります。契約終了後は、利用申込書に定める期日までに、お客様ごとのデータベースを含むすべてのデータを、復旧できない状態に削除します。バックアップは、保管期間の経過とともに自動的に消去されます。ご希望があれば、データ消去証明書を発行します。詳細は、セキュリティチェックシート（SLO 3.4・3.5・3.9、総務省版 #12・#13・#14）でご確認ください。

4.3 情報のラベル付け

一部のサービスでは、お客様が自らのデータを分類・管理できるよう、データへのタグ付け機能と、管理者ごとに閲覧できるデータの範囲を分ける権限設定機能を提供しています。機能の有無と使い方は、サービスごとのサービス説明資料と操作説明書でご案内しています。

5. アクセス制御

5.1 利用者登録及び登録削除

最初の管理者アカウントは、利用申込書の「管理画面ログインアカウント」欄に記載いただいた管理者をもとに、当社が発行します。その後の管理者アカウントの追加・削除は、お客様の管理者が管理画面で行えます。操作方法は、サービスごとの操作説明書でご案内しています。契約終了時は、管理者アカウントもデータとあわせて削除します。

5.2 利用者アクセスの提供

すべてのサービスで、お客様の管理者が管理画面から、管理者アカウントの追加・削除と、IPアドレス制限の設定を行えます（IPアドレス制限が標準機能にないサービスでは、オプションで提供しています）。各機能が標準かオプションかは、セキュリティチェックシートで公開しています。

5.3 特権的アクセス権の管理

お客様の管理者が、管理画面へのログインをリスクに応じて強化できるよう、多要素認証、IPアドレス制限、Basic認証、ロックアウト機能を提供しています。多要素認証を提供していないサービスでは、IPアドレス制限を標準機能として提供し、接続元を限定できるようにしています。サービスごとの機能と提供形態は、セキュリティチェックシート（総務省版 #49、経産省版 6-19・6-29）で公開しています。また、当社の運用者用アカウントには、多要素認証が使えるサービスでは多要素認証を設定しています。

5.4 利用者の秘密認証情報の管理

初期パスワードは推測されにくいものを発行し、ログインIDとは別のメールでお送りします。パスワードの強度はシステムで強制し（条件はサービスにより異なります）、パスワードは暗号化（ハッシュ化）して保存しています。発行後のログイン情報の管理・変更は、利用規約（第24条）に基づきお客様の責任で行っていただきます。変更の方法は、サービスごとの操作説明書でご案内しています。

5.5 情報へのアクセス制限

お客様が自社の方針に従って、本サービスの機能とデータへのアクセスを制限できるよう、管理者アカウントの追加・削除、ログイン認証の強化を提供しています。一部のサービスでは、管理者ごとに閲覧できるデータの範囲を分ける権限設定も提供しています。サービスごとの機能はセキュリティチェックシートで公開し、設定方法は操作説明書でご案内しています。

5.6 特権的なユーティリティプログラムの使用

本サービスでお客様がお使いいただけるのは管理画面のみであり、セキュリティ手順を回避してサーバーやデータベースに直接接続できるユーティリティプログラムは、お客様に提供していません。当社がサーバーの管理に使う管理用のツールは、本サービスを担当するエンジニアのみが使用し、接続は社内VPN経由に限っています。使用者のアクセス権は定期的に見直し、特権IDによる操作のログを取得して確認しています。

5.7 仮想コンピューティング環境における分離

本サービスは、複数のお客様のデータや処理環境が混在しないよう、共通基盤上で論理的に分離しています。お客様ごとに個別のデータベースを割り当て、サーバー上の実行環境を分けて、お客様が互いのデータにアクセスできないようにしています。新規のご提供では、お客様ごとに専用のサブドメインを割り当てています。詳細は、セキュリティチェックシート（SLO 3.7・4.5、経産省版 6-20）でご確認ください。

5.8 仮想マシンの要塞化

本サービスは SaaS として提供しており、お客様に仮想マシンは提供していません。本サービスを提供する当社の仮想マシンには、通信の制限、不正プログラム対策・侵入防御、ログの取得と監視、修正プログラムの適用、不要なポート・サービスの確認といった対策を行っています。

6. 暗号

6.1 暗号による管理策の利用方針

本サービスでは、通信を TLS（HTTPS）で暗号化し、データベースに保存するデータを暗号化しています。利用者・管理者のパスワードは、暗号化（ハッシュ化）して保存しています。暗号化の範囲はサービスにより異なり、セキュリティチェックシート（SLO 3.6、総務省版 #40・#51、経産省

版 6-31）で公開しています。なお、お客様がご自身でデータの暗号化を設定する機能は提供しておらず、お客様がご利用になる暗号の機能は、TLS による通信の暗号化です。

6.2 鍵管理

データベースの暗号化に使う暗号鍵は、クラウド事業者（Amazon Web Services）が管理する鍵を使用しています。お客様が暗号鍵を管理する必要はありません。

7. 物理的及び環境的セキュリティ

7.1 装置のセキュリティを保った処分又は再利用

本サービスのサーバーの記憶媒体など、物理的な資源の処分・再利用は、クラウド事業者（Amazon Web Services）が行っています。当社は、クラウド事業者が ISO/IEC 27017 の認証を取得していることを確認しています。お客様のデータの削除については、「4.2 クラウドサービスカスタマの資産の除去」をご覧ください。

8. 運用のセキュリティ

8.1 変更管理

お客様に影響を与え得る変更は、事前にお知らせします。メンテナンス・アップデートは、事前にメールで通知し、当社Webサイトの「NEWS&TOPICS」（https://ww-system.com/list/news/）にも掲載します。サービス内容・料金の変更、サービスの廃止、利用規約の変更は、利用規約（第3条・第11条・第17条）に定める時期までに NEWS&TOPICS に掲載し、必要に応じてメールでもお知らせします。通知には、変更の種類、予定日時、内容を記載し、作業の完了も NEWS&TOPICS でお知らせします。なお、緊急の保守や障害対応で事前にお知らせできない場合があることは、利用規約（第10条・第16条）で定めています。通知の方法は、セキュリティチェックシート（SLO 1.2）でも公開しています。

8.2 容量・能力の管理

本サービス全体の容量・処理能力を監視し、資源不足によるサービスの停止を防いでいます。サーバー基盤は運用委託先が監視し、しきい値を超えた場合は当社に通知され、必要に応じて容量を拡張します。また、利用状況の推移と大規模なご利用の予定をもとに、増強の計画を立てています。監視項目は、セキュリティチェックシート（SLO 1.13、総務省版 #31、経産省版 6-5）で公開しています。お客様には、利用申込書で参加者数の上限の目安をお示ししています。大規模な告知を行う場合は、事前に当社へご連絡ください。

8.3 実務管理者の運用のセキュリティ

お客様が管理画面で行う操作のうち、元に戻せない操作（データ・キャンペーンの削除、参加者一覧の削除、管理者アカウントの削除など）の手順と注意点は、サービスごとの操作説明書に記載し

ています。お客様の操作で削除したデータは復旧できない場合があることを、利用申込書と利用規約（第24条）でお示ししています。

8.4 情報のバックアップ

バックアップの方法、取得のタイミング、保存期間、世代数、冗長化の状況、復旧の検証は、サービスごとにセキュリティチェックシート（SLO 1.11・3.1・3.2・3.3・3.5、総務省版 #25・#26・#27、経産省版 6-8・9-2）で公開しています。バックアップは、サーバーの障害や災害に備えるためのものであり、お客様の誤操作などによるデータの紛失の復旧には用いません。必要なデータは、お客様ご自身でも保存していただくよう、利用規約（第24条）と利用申込書でお願いしています。バックアップの保管場所は、「2.2 関係当局との連絡」をご覧ください。

8.5 イベントログ

システムのログは、当社が改ざん防止の措置を講じて保管しています。管理画面でお客様がログを確認する機能は提供していません。ログは通常、お客様へ提供していませんが、事故の調査などで必要な場合は、提供可能な範囲で抜き出して提供します。ログの種類、保管期間、提供の条件は、セキュリティチェックシート（総務省版 #36・#37、経産省版 6-13）で公開しています。

8.6 クロックの同期

本サービスのサーバーは、NTP により正確な時刻源と同期しています。詳細は、セキュリティチェックシート（総務省版 #32、経産省版 6-14）でご確認ください。

8.7 クラウドサービスの監視

お客様は、管理画面で自社の利用状況（参加者数、応募数など。内容はサービスにより異なります）を確認できます。管理画面で確認できるのは、自社のデータだけです。サービスの稼働率の目標は、セキュリティチェックシート（SLO 1.5）で公開しています。障害が発生した場合は、当社Webサイトの NEWS&TOPICS に速報を掲載し、必要に応じてメールでお知らせします。

8.8 技術的ぜい弱性の管理

本サービスの技術的脆弱性は、脆弱性情報の定期的な確認、深刻度に応じた修正プログラムの適用、侵入防御、外部の脆弱性診断によって管理しています。管理の方法は、セキュリティチェックシート（総務省版 #39・#47、経産省版 6-4・6-6、SLO 4.2）で公開しています。外部の脆弱性診断の結果は開示していませんが、個別にご確認のご依頼があった場合は、診断の実施状況をお答えします。修正プログラムの適用でサービスを停止する場合は、事前にメールでお知らせし、NEWS&TOPICS にも掲載します。緊急の場合は、利用規約（第10条）に基づき、事前のお知らせなく行うことがあります。

9. 通信のセキュリティ

9.1 ネットワークの分離

お客様どうしの分離は、「5.7 仮想コンピューティング環境における分離」のとおりです。また、当社が運用に使う接続経路は、お客様がお使いになる管理画面とは分けています。お客様は Web の管理画面のみをお使いいただき、当社の運用者は社内VPN経由の別の経路を使います。サーバー基盤のネットワークは、運用委託先が管理しています。

9.2 仮想及び物理ネットワークのセキュリティ管理の整合

仮想ネットワークは、物理ネットワークと同じ考え方（通信の制限、ネットワークの分離、接続元の制限）で設定しています。物理ネットワークとデータセンターはクラウド事業者（Amazon Web Services）が管理しており、当社は、クラウド事業者が ISO/IEC 27017 の認証を取得していることを確認しています。仮想ネットワークでは、運用委託先が、サーバーとデータベースごとに通信を制御する設定（セキュリティグループ）で必要な通信だけを許可し、監視しています。本サービスへの Web の通信は、Web アプリケーションファイアウォール（AWS WAF）とサーバーの侵入防御の仕組みで保護しています。

10. システムの取得、開発及び保守

10.1 情報セキュリティ要求事項の分析及び仕様化

本サービスが提供する情報セキュリティの機能（IPアドレス制限、Basic認証、ロックアウト機能、多要素認証、通信の暗号化〈TLS〉、管理者アカウントの管理など）について、サービスごとに提供する機能と提供形態（標準・オプション）を、セキュリティチェックシートで公開しています。お客様の情報セキュリティの要求に合うかどうかの評価にお役立てください。設定方法は、サービスごとの操作説明書でご案内しています。なお、当社は原則としてお客様の管理画面にログインしません。設定代行・運用支援・導入支援をお申込みいただいた場合に限り、当社の運用者用アカウントでログインします。

10.2 セキュリティに配慮した開発のための方針

本サービスは、独立行政法人情報処理推進機構（IPA）の「安全なウェブサイトの作り方」に準拠して開発しています。また、開発・テスト・本番の環境を分け、脆弱性診断を行っています。これらは「情報クラウドセキュリティ方針」（https://ww-system.com/esg/cloud-security/）でも公開しています。脆弱性診断は、外部の診断を定期的に受けるほか、その他の期間も社内のコードレビューと脆弱性スキャンツールで確認しています。診断の方針は、セキュリティチェックシート（SLO 4.2、経産省版 6-6・10-6）で公開しています。外部の診断の結果の扱いは、「8.8 技術的ぜい弱性の管理」をご覧ください。

11. 供給者関係

11.1 供給者との合意におけるセキュリティの取扱い

お客様と当社の間の情報セキュリティに関する取決めは、利用規約で定めています。双方の秘密保持義務は第30条、個人情報の取扱いは第29条、再委託先の管理は第18条に定めています。お預かりした情報に事故が起きた場合は、速やかにお客様にお知らせします。このことは、「情報クラウドセキュリティ方針」とセキュリティチェックシートで公開しています。事故の際は、委託元であるお客様にお知らせし、その指示に従って対応します。

11.2 ICTサプライチェーン

本サービスで利用する他社のクラウドサービス（Amazon Web Services、Google Gemini API、Cloudflare Stream など）は、当社の委託先として評価し、責任範囲、アクセス制限、データセンターの場所、障害時の連携などを確認して、当社と同等以上のセキュリティ水準であることを確かめています。運用委託先を通じて利用するクラウド基盤も、運用委託先の評価の中で確認しています。また、運用委託先には、再委託先にも当社と同等の要求事項を伝えるよう求めています。

12. 情報セキュリティインシデント管理

12.1 責任及び手順

本サービスで事故や障害が発生した場合は、検知後速やかに当社Webサイトの「NEWS&TOPICS」（https://ww-system.com/list/news/）に速報を掲載し、その後、必要に応じてメールでお知らせします。当社は、委託元であるお客様への通知や関係機関への報告を含む対応の手順を、社内の規程で定めています。通知の方法と時期は、「情報クラウドセキュリティ方針」とセキュリティチェックシート（総務省版 #58）で公開しています。

12.2 情報セキュリティ事象の報告

お客様は、当社Webサイトの問い合わせ窓口（https://ww-system.com/inquiry/）から、メールまたは電話で、事故や障害、セキュリティ上の懸念をご報告いただけます。いただいた報告は、当社の情報セキュリティ及びプライバシー管理責任者に報告し、インシデントにあたるかを判断して対応します。回答と対応状況は、受け付けた窓口（メール・電話）でお知らせします。窓口、受付時間、連絡手段は、セキュリティチェックシート（総務省版 #52・#53・#55）で公開しています。

12.3 証拠の収集

システムのログは、改ざん防止の措置を講じて保管しています。インシデントが発生した場合は、社内の手順に従い、ログを証拠として保存します。事故の調査などでお客様から求められた場合は、提供可能な範囲でログを抜き出して提供します。

13. 順守

13.1 適用法令及び契約上の要求事項の特定

本サービスの利用契約の準拠法は日本法とし、管轄裁判所は利用規約（第7条）で定めています。お客様が本サービスで個人情報を取り扱う際に個人情報の保護に関する法律の義務を守っていただくことは、利用規約（第29条）でお示ししています。データの保管場所は、「2.2 関係当局との連絡」をご覧ください。また、法令等の順守の取組みとして、ISO/IEC 27001 の認証とプライバシーマークを取得しており、セキュリティチェックシートで公開しています。

13.2 知的財産権

本サービスに関する第三者の知的財産権の苦情は、当社の営業担当が受け付けます。利用規約では、第三者の知的財産権の侵害を禁止しています（第25条・第26条）。苦情があった場合は、侵害行為の停止、コンテンツの変更、当事者間の協議をご契約者に求め、必要に応じて、データの削除、利用の制限、契約の解除を行います（第15条・第26条・第27条）。

13.3 記録の保護

お客様からお預かりする記録の保護に関する情報（ログの保管期間と改ざん防止、バックアップの頻度と世代数、暗号化の範囲、データの保管期間、解約時の削除とデータ消去証明書の発行）は、サービスごとのセキュリティチェックシートと利用申込書で開示しています。

13.4 暗号化機能に対する規制

本サービスで実装している暗号による管理策（TLS による通信の暗号化、データベースに保存するデータの暗号化、パスワードのハッシュ化）は、「6. 暗号」のとおりです。本サービスで使用している暗号は、ブラウザ等に標準で備わる TLS による通信の暗号化と、クラウド基盤の標準機能によるデータベースの暗号化であり、暗号機能を持つプログラムをお客様に配布することはありません。

13.5 情報セキュリティの独立したレビュー

当社の第三者認証（ISO/IEC 27001、プライバシーマーク）の認証番号と有効期限は、当社Webサイトの「セキュリティ資料」ページ（https://ww-system.com/esg/security-materials/）とセキュリティチェックシートで公開しています。第三者機関による脆弱性診断の結果は開示していませんが、個別にご確認のご依頼があった場合は、診断の実施状況をお答えします。