Agent Orchestration セキュリティホワイトペーパー / Agent Orchestration Security White Paper

※本セキュリティホワイトペーパーは、他の言語に翻訳され、日本語による本セキュリティホワイトペーパーとその他の言語による翻訳版の間に相違がある場合には、日本語による記述があらゆる点について優先します。
*If this Security White Paper is translated into other languages, and there is any discrepancy between the Japanese version of the Security White Paper and any translated version in any other language, the Japanese version shall prevail in all respects.

改訂履歴 / Revision History

版数 / Revision	発行日 / Date of Issue	変更内容 / Changes
初版 / Rev. 1.0	July 1st, 2026	

この Agent Orchestrationセキュリティホワイトペーパー（以下「本書」といいます。）は、 株式会社セゾンテクノロジー（以下「当社」といいます。）が提供するAI 業務実行基盤「Agent Orchestration」のインフラストラクチャー及びアプリケーションにどのようなセキュリティ対策を施しているかを紹介するドキュメントです。

1. 当社の取組み

⑴ 情報セキュリティ方針

当社は、情報セキュリティ基本方針を定めております。詳細は下記URLをご確認ください。

https://www.saison-technology.com/security

また、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/IEC27001:2013認証を取得しています。

⑵ 情報セキュリティインシデント対応体制

情報セキュリティインシデント発生時、連絡窓口、社内の責任体制と対応手順を定めています。

2. Agent Orchestrationに関するセキュリティ対応

⑴ クラウドコンピューティング 環境

Agent Orchestration はクラウドコンピューティング環境として Amazon Web Services（「AWS」）の Amazon Elastic Container Service（ECS）を採用しています。

クラ ウドコンピューティング環境のセキュリティ対策については、下記URLをご確認ください。

AWS Security Center

http://aws.amazon.com/security/

⑵ 機密性

Agent Orchestrationは通信の機密性を確保するために、Agent Orchestrationとクライアント間の通信においてSSL/TLSによる通信データの暗号化を常時適用します。

登録済みアカウントや接続情報の不正利用を防ぐ目的でAgent Orchestrationはサインインに使用するアカウントパスワードを認証基盤上で適切に保護します。また、接続情報等の機密情報は、暗号化して保管します。

⑶ 可用性

Agent Orchestrationは、万が一稼働中のデータセンター（AZ）で障害が発生した場合は、別AZにてアプリケーションを再起動し、速やかにサービスを復旧可能な構成としています。

⑷ 開発工程におけるセキュリティ対策

Agent Orchestrationの開発は当社が指定したセキュリティの担保された環境下で行っています。

ソースコードの脆弱性を早期に発見するために、開発工程において 静的ソース解析ツール及び疑似攻撃型脆弱性診断ツールによる検証を実施しています。 開発環境、ステージング環境、プロダクション環境（お客様がご利用になる環境） をそれぞれ用意し、未検証のアプリケーションをプロダクション環境にデプロイしない仕組みを導入しています。また、定期的な脆弱性検査および対応の実施を開発プロセスに取り入れています。

3. オペレーション対応

⑴ ペネトレーションテスト

Agent Orchestrationでは、メジャーリリース時等、必要に応じてペネトレーションテストを実施しています。実施インターバルはメジャーリリースごとです。

⑵ モニタリング

当社は、 Agent Orchestrationを構成する共通システムの監視(死活監視、CPU/メモリ監視)を行います。 自動モニタリングシステムを活用して、異常検知時または警戒閾値を越えた場合、当社の運用担当者及び開発者に情報の通知を行い、内容に応じ当社よりお客様にご連絡します。

⑶ インシデント管理

Agent Orchestrationにおいて重大障害等インシデントが発生した場合、通常の問い合わせ・運用対応時のものとは別にインシデント管理手順により対応します。必要に応じて、当社所定の方法によりお客様に情報を提供します。

アクセスコントロール

① お客様情報の保管

お客様の情報はAgent Orchestration内に暗号化され保管されています。外部からアクセス可能なゾーンへの配置はありません。

② 不正アクセス対策

事前に許可されたユーザーだけが Agent Orchestrationにアクセスできる仕組みとなり、パスワード認証の他、スマートフォンを利用した多要素認証を導入しています。また、管理サーバへのアクセスを当社内からの通信に限定することで、 故意・過失による不正アクセスの可能性を抑制しています。

③ 当社従業員の管理

当社全ての従業員（協力会社社員含めて）に対して入社時（受入れ時）のセキュリティ教育および定期的なセキュリティ教育を行っています。事務所への入退出管理など物理的なセキュリティ対策を実施し、情報処理装置を保護しています。

4. データの取扱い

⑴ バックアップ

サービスに格納される主要なデータストアには継続的な自動バックアップを適用しています

⑵ 解約後の取扱い

お客様が契約解除をされた場合、契約終了日以降は本サービスにアクセスできなくなります。契約終了時点で本サービス内に残ったデータは契約終了日以降に削除されます。再度、契約され利用を再開された場合も元に戻すことはできません。

5. リスクマネジメントと保険

当社は、IT業務賠償責任保険を付保しています。

6. 通知

本書は、本書の発行日時点での情報を記述しており、これらは事前通知なく変更される場合があります。最新の情報については、下記URLをご確認ください。

Agent Orchestrationサービス仕様書 別添６「セキュリティホワイトペーパー」
https://www.saison-technology.com/service/.assets/agent-orchestration-security-white-paper.pdf

お客様は、本書の情報およびAgent Orchestrationの使用について独自に評価する責任を負うものとします。これらの情報は明示または黙示を問わずいかなる保証も伴うことなく「現状のまま」提供されるものです。

以上

This Agent Orchestration Security White Paper (“this document”) is a document that introduces the security measures implemented in the infrastructure and applications of “Agent Orchestration,” the AI operations execution platform provided by Saison Technology Co., Ltd. (“the Company”).

1. The Company’s Initiatives

(1) Information Security Policies

The Company has established a basic policy for information security. Please refer to the following URL for details.
https://www.saison-technology.com/security (Japanese only)
In addition, the Company has obtained ISO/IEC27001:2013" certification, the international standard for ISMS (Information Security Management System) accreditation.

(2) Information Security Incident Handling

In the event of an information security incident, the Company has established a contact point, internal responsibility structure, and response procedures.

2. Security Measures for Agent Orchestration

(1) Cloud Computing Environment

Agent Orchestration utilizes Amazon Elastic Container Service (ECS) on Amazon Web Services (AWS) as its cloud computing environment.
Please refer to the following URL for security measures of the cloud computing environment.
AWS Security Center
http://aws.amazon.com/security/

(2) Confidentiality

To ensure the confidentiality of communications, Agent Orchestration always applies SSL/TLS encryption to data transmitted between Agent Orchestration and clients.
To prevent unauthorized use of registered accounts and connection information, Agent Orchestration appropriately protects account passwords used for sign-in on the authentication platform. Additionally, confidential information such as connection details is stored in encrypted form.

(3) Availability

Agent Orchestration is configured so that, in the unlikely event of a failure in the active data center (AZ), the application can be restarted in a different AZ to quickly restore service.

(4) Security Measures in the Development Process

Agent Orchestration is developed in a secure environment specified by the Company.
To detect vulnerabilities in source code at an early stage, we conduct verification using static source analysis tools and pseudo-attack type vulnerability diagnostic tools during the development process. We provide a development environment, a staging environment, and a production environment (customer's environment); a mechanism is introduced to prevent deploying untested applications to the production environment. We also incorporate regular vulnerability inspections and handling into our development process.

3. Operation

(1) Penetration Test

Agent Orchestration conducts penetration tests as needed, such as during major releases. These

tests are performed at the interval of each major release.

(2) Monitoring

We monitor the common systems that make up Agent Orchestration (dead/alive monitoring, CPU/memory monitoring). Using an automated monitoring system, we notify our operations staff and developers when anomalies are detected or warning thresholds are exceeded, and we contact the customer as appropriate based on the situation.

(3) Incident Management

In the event of a significant failure or other incident at Agent Orchestration, the incident will be handled in accordance with the incident management procedures separate from those used for normal inquiries and operational support. Information will be sent to customers as necessary, in accordance with our established procedures.

(4) Access Control

① Storage of Customer Information

Customer information is encrypted and stored within Agent Orchestration. It is not placed in an externally accessible zone.

② Measures Against Unauthorized Access

Only pre-approved users can access Agent Orchestration. Password authentication, as well as multi-factor authentication using smartphones, are introduced. In addition, limiting access to the management server to communications from internal sites reduces the possibility of unauthorized access due to intentional or negligent acts.

③ Management of Employees

The Company provides security education to all the employees (including employees of subcontractors) when they join the Company (upon receiving their employment) and regularly. We implement physical security measures such as access control to the office to protect information processing equipment.

4. Data

(1) Backups

We apply continuous automatic backups to the primary data stores stored on the service.

(2) After Termination

If a customer cancels the contract, the customer will not be able to access the service after the contract termination date. Any data remaining in the service at the time of contract termination will be deleted after the contract termination date. The data cannot be restored even if the customer resumes the contract and resumes the use of the service.

5. Risk Management and Insurance

The Company carries IT business liability insurance.

6. Notification

This document describes information as of the publication date, which is subject to change without prior notice. Please refer to the following URL for the latest information.

Agent Orchestration Service Specifications, Appendix 6: "Security White Paper"
https://www.saison-technology.com/service/.assets/agent-orchestration-security-white-paper.pdf

Customers are solely responsible for their independent evaluation of the information in this document and their use of Agent Orchestration. This information is provided "as is" without warranty, either express or implied.

End