SOFTBRAIN Co.,Ltd.

esm セキュリティホワイトペーパー

ソフトブレーン株式会社

第 1.1 版　2025 年 2 月 12 日　改訂版

目次

1.用語の定義

「セキュリティホワイトペーパー」（以下、本書）では、JIS Q 27017:2016（ISO/IEC 27017:2015）で定義されたクラウドサービスの用語の定義を原則として使用します。

1.1 用語

本書における当社独自の用語については、以下に定義します。

- クラウドサービス利用者（CSC：クラウドサービスカスタマー）
- クラウドサービス提供者（CSP:クラウドサービスプロバイダ）

1.2 略語

本書で用いる略語を、以下に示します。

IaaS インフラストラクチャアズアサービス（Infrastructure as a Service）

PaaS プラットフォームアズアサービス（Platform as a Service）

PII 個人を特定できる情報（Personally Identifiable Information）

SaaS ソフトウェアアズアサービス（Software as a Service）

SLA サービスレベル合意書（Service Level Agreement）

2.「セキュリティホワイトペーパー」の目的

「セキュリティホワイトペーパー」（以下、本書）は、クラウドセキュリティの国際規格（ISO/IEC 27017）で求められている要求事項に対して、ソフトブレーン株式会社（以下、当社）が、クラウドサービス提供者として実施する管理策をご確認いただくことを目的としています。

3.本書の適用範囲

本書の適用範囲は、当社が提供する以下のクラウドサービスとなります。

・esm（e セールスマネージャー） サービス

・esm store サービス

・esm marketing サービス

・esm linkage サービス

※Amazon Web Services（以下 AWS）上で当社にて運用管理する全ての有償提供環境が対象範囲となりますが、AWS 以外にてハウジングした物理サーバー上で個別提供している提供環境、当社が管理出来ない提供形態、無償提供されるデモ環境やテスト環境は、全てが適用範囲外と

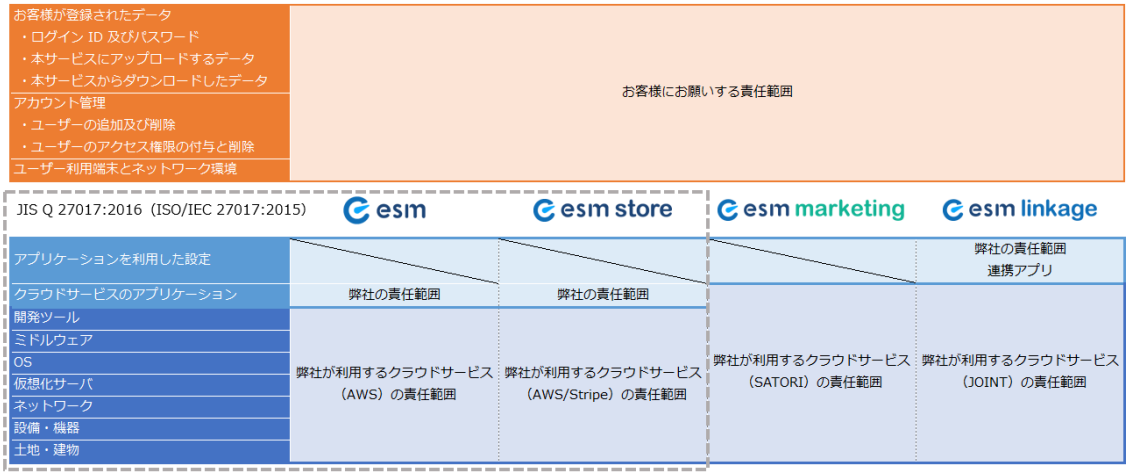
します。

なお、クラウドサービスで提供する機能の詳細に関しては、以下の「esm 活用支援サイト」（以下、「活用支援サイト」といいます。）をご参照ください。

活用支援サイト：https://esm-support.softbrain.com/

4.クラウドサービスの責任分界点について

当社が提供するクラウドサービスに関する責任分界点は、以下のように定めます。



4.1 当社の責任

当社は、以下のセキュリティ対策を実施します。

- 当社が提供するクラウドサービスのセキュリティ対策
- 上記サービスに保管された利用者データの保護
- 上記サービスの提供に利用するミドルウェア、OS、その他インフラのセキュリティ対策

4.2 利用者の責任

利用者は、以下のセキュリティ対策を実施する必要があります。

- パスワードの適切な管理（利用するデバイスの適切な管理も含む）
- アカウントの適切な管理（登録、利用停止、管理権限の付与など）
- 登録された利用者データの適切な管理

5.情報セキュリティのための方針群

クラウドサービス提供者は、クラウドサービスの提供および利用に取り組むため、情報セキュリティ基本方針を拡充することが求められています。当社は、クラウドサービス提供者として、

当社の「情報セキュリティ宣言」ならびに「クラウドサービス情報セキュリティ基本方針」に従ってサービスを運用しています。

6.情報セキュリティの役割および責任

当社は、クラウドサービス提供者として、「eセールスマネージャー　サービス約款」（以下、「約款」といいます。）で契約やサービスの内容を定義し、サービス提供を実施しています。また、サービス利用中に発生する QA 等の問い合わせ対応に関しては、当社クラウドサービス利用時に合意いただいた約款でサービスの内容を定義し、サービス提供を実施しています。

約款は、以下の活用支援サイトをご参照ください。

約款：https://esm-support.softbrain.com/wp-content/uploads/e_セールスマネージャー-サービス約款.pdf

7.関係当局との連絡

当社は、クラウドサービス提供者として、クラウドサービス利用者に、クラウドサービスを運営している当社の地理的所在地と、クラウドサービス利用者の情報資産を保管する国を以下のとおり通知します。

① 本社所在地：東京都中央区銀座六丁目 18 番 2 号 野村不動産銀座ビル11階

② クラウドサービス利用者の情報資産の所在：

AWS　日本国内

Stripe APAC（バンガロール）

SATORI　日本国内

JOINT　日本国内

8.クラウドコンピューティング環境における役割および責任の共有および分担

当社は、クラウドサービス提供者として、約款でサービスの内容を定義し、クラウドサービス提供を実施しています。また、サービスに関するお問い合わせは、eセールスマネージャーストアにログイン後に表示されるお問い合わせフォームよりご連絡ください。 なお、責任分界点については、前出の「4.クラウドサービスの責任分界点について」をご参照ください。

約款とお問い合わせは、以下の活用支援サイトをご参照ください。

約款：https://esm-support.softbrain.com/wp-content/uploads/e_セールスマネージャー-サー

ビス約款.pdf

9.情報セキュリティの意識向上、教育及び訓練

当社は、クラウドサービス提供者として、情報セキュリティ要件の周知徹底とクラウドサービスの運営ルール徹底を目的として、クラウドサービスに従事する要員を対象とした教育・訓練および意識向上のためのセキュリティ対策を実施しています。

10.クラウドサービス利用者の資産の除去

当社は、クラウドサービス提供者として、クラウドサービス利用者が作成・保存した情報資産の除去に関して、クラウドサービス利用者が退会した時に、約款および「解約申請書」の合意内容に従い、解約日翌日より利用停止し、翌月末に環境を削除します。

約款は、以下の活用支援サイトをご参照ください。

約款：https://esm-support.softbrain.com/wp-content/uploads/e_セールスマネージャー-サービス約款.pdf

11.資産目録

当社は、クラウドサービス提供者として、クラウドサービス利用者の情報資産と当社が運営するための情報資産は明確に分離しています。なお、クラウド環境上にクラウドサービス利用者が作成・保存する情報資産（クラウドサービスカスタマーデータ）は、クラウドサービス利用者の管理範囲となります。

12.情報のラベル付け

当社は、クラウドサービス提供者として、クラウドサービス利用者に対して、当社のクラウドサービスに保存する情報資産を分類しラベル付けするためのサービス機能を提供しています。この機能は、クラウドサービス利用者の情報資産の分類（一般情報/個人情報/秘密情報の区別、利用者別権限設定）に、ご利用いただけます。

なお、クラウドサービスの提供機能の利用にあたっては、以下の活用支援サイトをご参照ください。

利用機能の制限: https://esm-support.softbrain.com/c001003/

データごとのアクセス可能者の制限：https://esm-support.softbrain.com/c020002/

13.利用者登録及び利用停止

当社は、クラウドサービス提供者として、クラウドサービス利用者に対して、当社のクラウドサービスへのアクセスを管理できるように、アカウントの登録や利用停止に関する機能を提供しています。

なお、クラウドサービスの提供機能の利用にあたっては、以下の活用支援サイトをご参照ください。

社員の登録：https://esm-support.softbrain.com/c012003/

社員の変更：https://esm-support.softbrain.com/c012006/

14.利用者アクセスの提供

当社は、クラウドサービス提供者として、クラウドサービス利用者に対して、当社のクラウドサービスへのアクセス権を管理できる機能（セキュリティポリシーの設定・変更機能）を提供しています。

なお、クラウドサービスの提供機能の利用にあたっては、以下の活用支援サイトをご参照ください。

データごとのアクセス可能者の制限：https://esm-support.softbrain.com/c020002/

15.特権的アクセス権の管理

当社は、クラウドサービス提供者として、クラウドサービス利用者に対して、当社のクラウドサービスで特権的アクセス権が付与されている利用者アカウントを十分に強固なパスワードポリシーにより保護します。

・最小文字数の指定
・有効期限
・複数文字種
・認証エラー回数によるアカウントロック

16.利用者の秘密認証情報の管理

当社は、クラウドサービス提供者として、クラウドサービス利用者の秘密認証情報（パスワー

ドなど)を次のように管理します。

・初期パスワードはユーザー登録時の招待メールにて通知します

・有効期限は 90 日間です。

・3 回連続で認証エラーをした場合アカウントロックされます

その場合はパスワード再設定を行う必要があります。

・パスワードの再設定は登録メールアドレスに送付される有効期限付きの一時 URL から再設定が可能です。

17.情報へのアクセス制限

当社は、クラウドサービス提供者として、クラウドサービスへのアクセス権、クラウドサービス機能へのアクセス権、クラウドサービス利用者の情報資産へのアクセス権を、クラウドサービス利用者が制限できるように、アクセス制御機能（セキュリティポリシーの設定・変更機能）を提供しています。

なお、クラウドサービスの提供機能の利用にあたっては、以下の活用支援サイトをご参照ください。

利用機能の制限: https://esm-support.softbrain.com/c001003/

データごとのアクセス可能者の制限: https://esm-support.softbrain.com/c020002/

18.特権的なユーティリティプログラムの使用

当社のクラウドサービスは、全てのサービス利用において、認証が必要となっており、セキュリティ手順を回避し各種サービス機能の利用を可能とするユーティリティプログラムの提供は行っておりません。

19.仮想コンピューティング環境における分離

当社は、クラウドサービス提供者として、クラウドサービス利用者ごとのユーザーID によるアクセス資源の分離を実施し、別テナントへの不正アクセスを抑止することで、クラウド環境の論理的分離を確実に実施しています。

20.仮想マシンの要塞化

当社は、クラウドサービス提供者として、構築するすべての仮想化環境で、以下のセキュリティ対

策を実施しています。

① 必要なポートだけを有効としています。

② 必要なプロトコルだけを有効としています。

③ マルウェア対策を実施しています。

④ ログの取得を実施しています。

21.暗号による管理策の利用方針

当サービスではストレージ、データベース、通信(TLS1.3 対応)の暗号化を実施しておりま す。

22.装置のセキュリティを保った処分又は再利用

機器の老朽化、故障等により交換した機器媒体の処理については、当社では直接装置 の処分を行うことはありません。AWS の施設、建物、および物理上のセキュリティに基づき ます。

https://aws.amazon.com/jp/blogs/news/data_disposal/

23.変更管理

当社は、クラウドサービス提供者として、クラウドサービス利用者のセキュリティに悪影響を与える可能性のあるクラウドサービスの変更を実施する前に、活用支援サイトを通じて変更内容の連絡を行います。また、提供サービスの定期システムメンテナンスの場合も連絡を行います。

以下の活用支援サイトをご参照ください。

活用支援サイト: https://esm-support.softbrain.com/

24.容量・能力の管理

当社は、クラウドサービス提供者として、安定的にクラウドサービスを提供するために、各テナントのキャパシティを明確にし、日々の運用プロセスの中で稼働監視を行っています。また、監視の結果として必要と判断した場合は、適切なタイミングで、システムメンテナンスを実施します。システムメンテナンスの実施は、活用支援サイトを通じて連絡を行います。

以下の活用支援サイトをご参照ください。

活用支援サイト: https://esm-support.softbrain.com/

25.実務管理者の運用セキュリティ

当社は、クラウドサービス提供者として、クラウドサービス利用者にとって重要な当社のクラウドサービスの操作方法に関して、活用支援サイトで各種マニュアルを提供しています。
以下の活用支援サイトをご参照ください。
活用支援サイト: https://esm-support.softbrain.com/

26.情報のバックアップ

クラウドサービス利用者が実施可能なバックアップ機能は、提供しておりません。
当社は、クラウドサービス提供者として、クラウドサービスのシステムおよびクラウドサービス利用者の情報資産のバックアップを日々実施しています。

・対象データ:登録されたデータおよびファイル
・頻度:1 日 1 回
・保持期間:7 世代

27.イベントログ取得

当社は、クラウドサービス提供者として、当社の責任範囲において、クラウドサービスの維持管理に必要となる適切なイベントログを取得し、クラウドサービス利用者からの要求に応じて、以下のログを提供しています。

- 監査ログ・・・「誰が」、「いつ」、「どこから」顧客データにアクセスしたかが記録されるログ

28.クロックの同期

当社のクラウドサービスでは AWS が提供する Time Sync Service を基準に時刻を同期しています。

29.クラウドサービスの監視

当社は、クラウドサービス提供者としてサービスの状況に関するログの取得及び監視を実施しています。

・サーバーの状態監視:状態のロギング及び監視

・システムの死活監視：状態のロギング及び監視
・リソース監視：状態のロギング及び監視
・外部からの攻撃の監視：複数回のログイン試行など攻撃の可能性を含むアクセスの監視

30.技術的脆弱性の管理

当社は、クラウドサービス提供者として、定期的にぜい弱性情報の収集を実施し、クラウドサービス利用者で対応が必要となる脆弱性情報があった場合には、クラウドサービス利用者に通知連絡します。当社のクラウドサービス側での対応が必要になった場合には、定期または緊急メンテナンスで対応を実施し、メンテナンス前後での対応内容および対策後の結果を活用支援サイトを通じて通知連絡します。
以下の活用支援サイトをご参照ください。
活用支援サイト：https://esm-support.softbrain.com/

31.ネットワークの分離

当社は、クラウドサービス提供者として、他のクラウドサービス利用者とのネットワーク環境を適切に分離しています。さらに、当社の社内ネットワークと、クラウドサービス利用者に提供するクラウドサービスそのものも分離しています。

32.仮想および物理ネットワークのためのセキュリティ管理の整合

当社は、IaaS として AWS を利用して、SaaS としてクラウドサービスを提供しています。AWS のインフラストラクチャセキュリティに関する情報は、AWS 公式サイトをご参照ください。
https://aws.amazon.com/jp/whitepapers/?whitepapers-main.sort-by=item.additionalFields.sortDate&whitepapers-main.sort-order=desc&awsf.whitepapers-content-type=*all&awsf.whitepapers-global-methodology=*all&awsf.whitepapers-tech-category=*all&awsf.whitepapers-industries=*all&awsf.whitepapers-business-category=*all

33.情報セキュリティ要求事項の分析および仕様化

当社は、クラウドサービス提供者として、当社のクラウドサービスで実装している情報セキュリティ対策および機能を本書に記載しています。以下に示す主なセキュリティ機能の詳細は、本書の該当項番をご参照ください。

- アクセス制限機能【17.情報へのアクセス制限】

- アクセス制限機能【20.仮想マシンの要塞化】
- 通信暗号化機能【21. 暗号による管理策の利用方針】
- バックアップ機能【26.情報のバックアップ】
- ログ取得機能【27.イベントログの取得】

34.セキュリティに配慮した開発のための方針

当社は、クラウドサービス提供者として、IPA（情報処理推進機構）が発行する「安全なウェブサイトの作り方」を参考に開発し、 第三者によるセキュリティ診断を実施後にサービスを提供しています。また、提供中のクラウドサービスにおいても、年 1 回の脆弱性診断にてセキュリティ対策を実施しています。

35.供給者との合意におけるセキュリティの取扱い

当社のクラウドサービスは、SaaS 型のクラウドサービスであり、責任分界点の詳細は、前出の「4. クラウドサービスの責任分界点について」をご参照ください。また、当社のクラウドサービスの情報セキュリティ対策に関しても、「4. クラウドサービスの責任分界点について」で定めた当社クラウドサービスの提供範囲において、必要な情報セキュリティ対策を実施しています。

36.ICT サプライチェーン

当社は、SaaS 事業者として、AWS が提供するクラウドサービスを利用して、当社のクラウドサービスを実現しています。このため、クラウドサービスの供給者関係において、当社はクラウドサービス提供者であるとともにクラウドサービス利用者でもあります。従って、当社の「情報セキュリティ基本方針」ならびに「クラウドサービス情報セキュリティ基本方針」に則り、当社のクラウドサービス提供に必要となる構成要素について、適切なリスク管理を実施しています。

37.責任および手順

当社は、クラウドサービス提供者として、当社で確認できたセキュリティインシデントに関して、情報セキュリティ基本方針に則り、適切に対応します。また、確認できたセキュリティインシデントがクラウドサービス利用者に重大な影響を及ぼす可能性がある場合は、公開基準を定め、検知から 7営業日を目標に クラウドサービス利用者に通知します。なお、クラウドサービス利用者への通知は、当社クラウドサービス利用時に合意いただいた約款で定めた方法で実施します。

約款は、以下をご参照ください。
約款:https://esm-support.softbrain.com/wp-content/uploads/e セールスマネージャー-サービス約款.pdf

38.情報セキュリティ事象の報告

当社は、クラウドサービス提供者として、セキュリティインシデントに関するお問い合わせ窓口を設置して、クラウドサービス利用者が発見したセキュリティインシデントの報告を行えるようにし、双方向での情報のやり取りを可能とする仕組みを提供しています。
なお、セキュリティインシデントに関するお問い合わせは、活用支援サイトのお問い合わせから、お問い合わせフォームで、当社までご連絡ください。
以下の活用支援サイトをご参照ください。
お問い合わせ:https://esm-support.softbrain.com/

39.証拠の収集

当社は、クラウドサービス提供者として、裁判所、捜査機関または監督官庁からの開示請求など、法律に基づいた正当な開示請求が行われた場合、クラウドサービス利用者の同意なく、クラウドサービス利用者の情報資産を第三者に開示することがあります。なお、クラウドサービス利用者への通知および同意を経ることなく、当該機関にクラウドサービス利用者の情報資産を開示することについては、約款で契約時に合意します。
約款は、以下の活用支援サイトをご参照ください。
約款: https://esm-support.softbrain.com/wp-content/uploads/e セールスマネージャー-サービス約款.pdf

40. 適用法令および契約上の要求事項の特定

当社のクラウドサービスの利用に関して、適用される準拠法は日本法となります。

41.知的財産権

当社のクラウドサービス上でサービスをご利用いただく上で、知的財産権に関わるお問い合わせは、活用支援サイトのお問い合わせから、お問い合わせフォームで、当社までご連絡ください。
以下の活用支援サイトをご参照ください。
お問い合わせ: https://esm-support.softbrain.com/

42.記録の保護

当社は、クラウドサービス提供者として、当社の責任範囲において、クラウドサービス利用者のイベントログを取得しており、クラウドサービス利用者の要求に応じて、イベントログ（呼称：監査ログ）を提供しています。クラウドサービス利用者の監査ログ保存期間は 6 ヶ月間となります。

43.暗号化機能に対する規制

サービスで利用している暗号化機能において、輸出規制の対象となる暗号化の利用はありません。

44.情報セキュリティの独立したレビュー

社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、JIS Q 27001、JIS Q 27017:2016（ISO/IEC 27017:2015）の ISMS 認証取得において第三者による審査を受け、情報セキュリティに対する取り組みを行うことで、常に安全なセキュリティレベルを確保しています。

改訂履歴

版	日付	改訂内容
1.0	2024/11/1	―
1.1	2025/2/12	3.本書の適用範囲 esm marketing esm linkage を追加
		4.クラウドサービスの責任分界点について 責任分界点を修正
		7.関係当局との連絡 クラウドサービス利用者の情報資産の所在に SATORI/JOINT を追加