株式会社マネジメントソリューションズ

クラウドサービス

セキュリティホワイトペーパー

Ver. 1.2

初版制定日：2023 年 05 月 01 日

最終改訂日：2023 年 07 月 12 日

目次

Ⅰ. はじめに

1. ホワイトペーパーの目的

このホワイトペーパー（以下、本書）は、株式会社マネジメントソリューションズ（以下、「MSOL」または「当社」）が提供するクラウドサービス（以下、「PROEVER」）をご利用中の方およびご利用を検討される方（以下、「お客様」）に向けて、当社のクラウドセキュリティの取り組みや実施しているセキュリティ対策についてご理解いただくことを目的としています。

2. 本書の適用範囲

本書の適用範囲は PROEVER に限定しています。

3. 本書で使用する用語・項番について

本書は、ISMS クラウドセキュリティ認証である「ISO/IEC 27017:2015（JIP-ISMS517-1.0）」で求められる要求事項において、特にお客様に向けた情報開示が求められる事項に関し当社の取り組みを説明しています。

そのため、「ISO/IEC 27017:2015（JIP-ISMS517-1.0）」に記されている用語や項番について、一部をそのまま利用しております。

また、本書においてお客様による閲覧時の利便性を考慮し、項番の順番に沿って当社の取り組みに関し説明しております。

II.　PROEVER について

1.　サービス概要

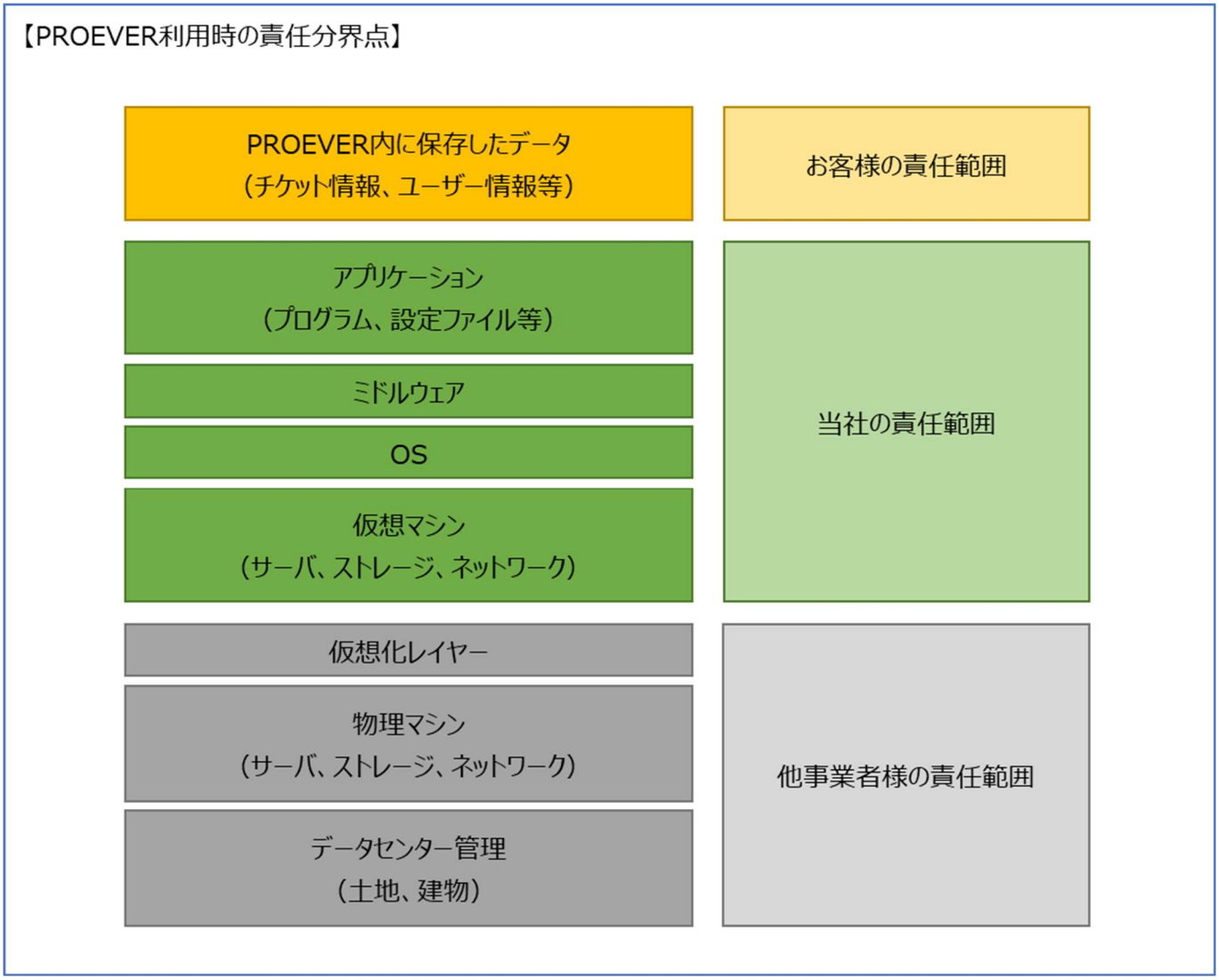
PROEVER はパブリッククラウドサービスに分類される SaaS（Software as a Service）型のサービスとなります。PROEVER を構成するインフラストラクチャーは日本マイクロソフト株式会社が提供する Microsoft Azure を採用しており、お客様のカスタマーデータは全て Microsoft Azure の東日本リージョンに保管されます。

2.　責任分界点について

下図に PROEVER における当社とお客様の責任範囲の概要を記します。

PROEVER は SaaS 型のクラウドサービスであり、当社は PROEVER 利用に必要となるアプリケーション機能の提供、PROEVER に保管されたお客様データの保護等を責任範囲とします。

お客様は、PROEVRE 上に登録した業務データの適切な管理およびお客様自身の ID およびパスワード等の管理が責任範囲となります。



（図 I ：PROEVER 利用時の責任分界点）

III.　PROEVER におけるクラウドセキュリティ対策

1. 情報セキュリティのための方針群（5.1.1）

当社は、お客様にクラウドサービスを提供するクラウドサービスプロバイダとして、下記の通りクラウドセキュリティにおける個別方針を定めております。

- 情報セキュリティ基本方針（https://www.msols.com/security/）
- 情報セキュリティ個別方針（https://www.msols.com/security/kobetsu/）
- クラウドサービス情報セキュリティ方針（https://www.msols.com/security/cloudservice/）

2. 情報セキュリティの役割及び責任（6.1.1）

「PROEVER 利用規約」の第 4 章第 10 条「利用環境の整備・責任分界点」において役割及び責任を明記しており、これらについて PROEVER 利用開始時に利用規約として同意いただく事項となっております。

3. 関係当局との連絡（6.1.3）

地理的所在地は各契約書に定めています。なお、本書記載時点において、お客様のデータを保存する可能性のある国は日本国内のみとなっております。

4. 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（CLD.6.3.1）

PROEVER 利用における責任分界点につきましては、本書の第Ⅱ章第２項を参照ください。

5. クラウドサービスカスタマの資産の除去（CLD.8.1.5）

「PROEVER 利用規約」の第 6 章第 18 条に定める通り、お客様がサービスの利用を終了された場合、1 カ月以内を目途に当社にてお客様資産の削除を行わせていただきます。

サービス上に保存されている全ての資産が物理的に削除されるため、一度削除が行われた場合は復元することができません。よって、利用終了の際は必要に応じてデータのエクスポート等を実施ください。

6. 情報のラベル付け（8.2.2）

PROEVER では、「プロジェクト名」「フェーズ名」「チーム名」等のラベル付け機能を提供しております。ラベル付け機能の詳細につきましては、ご契約いただいたお客様にお渡ししている「PROEVER 操作マニュアル」に詳細な手順を記載しています。

7. 利用者登録及び登録削除（9.2.1）

お客様ご自身で PROEVER の利用者を管理可能な機能を提供しております。登録、変更、削除を含む全ての利用者管理をお客様ご自身で実施いただくことが可能です。

マスタ管理やシステム設定を含めた管理者権限を含め、クラウドサービスカスタマであるお客様

自身で管理可能となっているため、お客様の定める規定に従い運用いただくことができます。

8. 利用者アクセスの提供（9.2.2）

PROEVER へのアクセス権について、お客様の管理者アカウントがマスタ管理者となり、各アカウントの権限設定を行うことが可能です。また、PROEVER 上のプロジェクトを分離することで、特定のデータに対しアクセス可能なアカウントを分離することが可能です。

9. 特権的アクセス権の管理（9.2.3）

ID およびパスワードによる認証の他、有効期限付きの認証コードによる認証が必須となっております。また、お客様の PROEVER テナントに限定し、アクセス元の IP アドレスを制限することも可能となっております。

10. 利用者の秘密認証情報の管理（9.2.4）

アカウントの登録手順及び秘密認証情報の管理手順につきましては、ご契約いただいたお客様にお渡ししている「PROEVER 操作マニュアル」に詳細な手順を記載しています。
認証コードによる認証を実施するため、アカウントの登録に際しメールアドレスのご登録が必須となっております。登録いただいたメールアドレス宛にパスワード設定用 URL が記載されたメールが届きますので、画面の指示に従ってパスワードの設定を行ってください。

また、PROEVER におけるパスワードポリシーは下記の通りとなっております。

- 英字小文字、英字大文字、数字、記号の 3 つ以上を組み合わせた 8～16 文字
  使用できる記号　@ # $ % ^ & * - _ + = [ ] { } | ¥ : ’ , ? / ` ~ ” ( ) ; .
- パスワードの有効期限：3 カ月

11. 情報へのアクセス制御（9.4.1）

PROEVER へのアクセスについては、管理者権限を持つお客様アカウントによるクラウドサービス機能へのアクセス制限や、特定のデータアクセスを制限する運用が可能となっております。
また、お客様の PROEVER テナントに限定し、アクセス元の IP アドレスを制限することも可能となっております。

12. 特権的なユーティリティプログラムの使用（9.4.4）

PROEVER において、通常の認証を回避可能なユーティリティプログラムの提供は行っておりません。

13. 仮想コンピューティング環境における分離（CLD.9.5.1）

お客様が利用する PROEVER テナントは、他テナントとは論理的に分離されています。

14. 仮想マシンの要塞化（CLD.9.5.2）

Microsoft Azure 上で提供される各種のセキュリティ機能を有効化し、適切な側面からの要塞化を実施しております。また、当社が PROEVER のサービス提供のために利用する各仮想マシンへの適切な技術手段（例えば、定期的な OS アップデートやログ取得）を確実に実施するために、セキュリティソリューション上の検査結果の定期的な確認を実施しております。

15. 暗号による管理策の利用方針（10.1.1）

データベースに保管される利用者の各種情報（氏名やメールアドレス、入力情報等）は暗号化されませんが、適切なアクセス権のもとで保管されています。
また、お客様の端末を当社が提供するサービス間の通信は TLSv1.2 によって暗号化されています。

16. 装置のセキュリティを保った処分又は再利用（11.2.7）

お客様のサービス利用終了に合わせ、原則として 1 カ月以内にお客様データを再利用不可能な形で削除いたします。削除はお客様専用のデータベースを物理的に削除するため、当社であっても一切復旧することができません。

ただし、お客様の利用によって派生的に生じた以下のクラウドサービス派生データに関しては所定の期間を過ぎた後に削除されるため、サービス利用終了後も一定期間残ります。

- バックアップデータ：7 日間を経過した後、8 日目に削除されます。
- 監査ログ（アクセスログ、操作ログ）：3 カ月を経過した後に削除されます。

17. 変更管理（12.1.2）

お客様に何らかの悪影響を与える可能性のある変更お呼びシステム作業に関しては、事前にお客様への通知を行います。通知方法は PROEVER のサービスダッシュボード上に表示される他、当社担当者からお客様への直接の連絡をもって行われます。

18. 容量・能力の管理（12.1.3）

お客様へのサービス提供において支障がないよう、リソース等のメトリクスに対して適切な運用監視を行っております。また、リソースが枯渇した際は自動スケールアップによる解消が図られるよう、適切なサービス設計を行っております。

19. 実務管理者の運用のセキュリティ（CLD.12.1.5）

ご契約いただいたお客様に対し、「PROEVER 操作マニュアル」を提供しております。また、操作方法の詳細やご利用方法に関するご相談を承れるよう、カスタマサポート窓口を提供しております。

20. 情報のバックアップ（12.3.1）

原則として、全てのお客様データを日次でバックアップしており、バックアップデータは 7 世代まで保持されております。バックアップは Microsoft Azure によって提供される機能を利用しており、お客様のバックアップデータは同サービス上に保管されています。
ただし、バックアップデータはサービス全体の復旧を目的としており、個々のお客様データを個別に復旧することはできません。また、何らかの障害等によってバックアップデータによるロールバックが必要となった場合、原則として 7 日以内（※）にバックアップによる復旧を行います。

※ 上記日数はあくまで目標とする復旧日数であり、期日以内の確実な復旧をお約束するものではございません。

21. イベントログ取得（12.4.1）

利用者が行った特定機能に対する操作ログを PROEVER 上で確認することが可能です。データの登録、変更、削除の操作ログに関して、操作を行ったアカウント名や日時を確認することができます。
また、お客様から要望に対して当社が必要であると判断した場合は、上記以外のアクセスログ（IP アドレスを含むログイン履歴等）をお客様へ提供いたします。

22. クロックの同期（12.4.4）

当社が提供する PROEVER は、サービス内は全て Microsoft Azure が提供する NTP サービスによって同期しております。PROEVER 側のサーバー時間は日本標準時（JST(UTC+9)）で取得されており、ユーザーごとにこれを変更することはできません。

クロックの同期を行う場合、お客様が PROEVER にアクセスする環境のクロックを日本標準時に同期させることによって、PROEVER のクロックと同期させることが可能です。

23. クラウドサービスの監視（CLD.12.4.5）

お客様ご自身で特定機能に対する操作ログを監視できるよう、PROEVER 上で専用機能を提供しております。監視機能の利用方法につきましては、ご契約いただいたお客様にお渡ししている「PROEVER 操作マニュアル」に詳細が記載されております。
また、当社責任範囲であるネットワークや CPU、メモリ等の各メトリクスの監視は当社が行っており、お客様には監視機能を提供しておりません。

24. **技術的ぜい弱性の管理（12.6.1）**

当社では技術的なぜい弱性情報を常時収集しております。収集した情報をもとに、お客様への影響を判断のうえ、お客様への通知を行います。通知方法は PROEVER のサービスダッシュボード上に表示される他、当社担当者からお客様への直接の連絡をもって行われます。

25. **ネットワークの分離（13.1.3）**

お客様のテナント間のネットワーク分離は適切に実施しております。

26. **仮想及び物理ネットワークのセキュリティ管理の整合（CLD.13.1.4）**

PROEVER のサービス提供に際し、信頼性の高い仮想化サービス（Microsoft Azure）を利用するとともに、当該サービスが第三者認証等によって当社の求めるセキュリティ水準が確保されたサービスであることを確認しております。

27. **情報セキュリティ要求事項の分析及び仕様化（14.1.1）**

本書へ記載するとともに、ご契約をいただいたお客様に提供する「PROEVER 操作マニュアル」に PROEVER に関する仕様詳細を記載しております。

28. **セキュリティに配慮した開発のための方針（14.2.1）**

開発プロセスに沿ったコードレビューの実施等により、基本的なぜい弱性への対応ができているか等の確認を行っております。また、PROEVER のサービス提供に必要な各種のライブラリ群について、定期的なバージョンアップを実施し、ぜい弱性への対応を行っております。

29. **供給者との合意におけるセキュリティの取扱い（15.1.2）**

お客様から事前の了承をいただいた場合を除き、当社カスタマサポートチームがお客様の情報に許可なくアクセスすることはございません。カスタマサポートサービスや障害対応のためにアクセスが必要になった場合、お客様からの了承を前提としアクセスさせていただく場合がございます。

また、当社とお客様の責任分界点は、本書の第Ⅱ章第２項を参照ください。

30. **ICT サプライチェーン（15.1.3）**

当社は、PROEVER のサービス提供に際し日本マイクロソフト株式会社が提供する Microsoft Azure を利用しております。当該サービスが当社の要求するセキュリティ水準を満たしていることを確認するとともに、当該サービスの利用に際し必要なリスクマネジメント活動を実施しております。

31.　責任及び手順（16.1.1）

当社の責任範囲において重大な情報セキュリティインシデント（お客様情報の漏洩等）を検知した場合、原則として 24 時間以内（※）にお客様へ発生事象およびそれによるお客様影響に関し第一報連絡を行います。通知方法は PROEVER のサービスダッシュボード上に表示される他、当社担当者からお客様への直接の連絡をもって行われます。

また、上記に類する情報セキュリティインシデントの相談・報告窓口として、以下連絡先を提供しております。

- 連絡先メールアドレス：proever.support@msols.com

※　上記時間はあくまで目標とする連絡時間であり、時間内の確実な報告をお約束するものではございません。

32.　情報セキュリティ事象の報告（16.1.2）

情報セキュリティ事故が発生した場合は、ROEVER のサービスダッシュボード上に表示される他、当社担当者からお客様への直接の連絡をもって行われます。
また、お客様からの事象報告はお問い合わせ窓口にて承っております。ご連絡をいただいた後、当社担当者よりメールにてご連絡をさせていただきます。

33.　証拠の収集（16.1.7）

お客様責任範囲におけるイベントログ等の収集は、お客様ご自身で行っていただけるよう、機能の提供を行っております。当社責任範囲でのアクセスログ等のディジタル証拠が必要な場合は、個別に対応していますため、都度当社へご相談ください。
なお、「PROEVER 利用規約」の第 7 章第 21 条に定める通り、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経ることなくお客様の情報を開示することがございます。

34.　適用法令及び契約上の要求事項の特定（18.1.1）

「PROEVER 利用規約」の第 8 章第 28 条に定める通り、準拠法は日本法と定めております。
また、当社はプライバシーマーク制度による認証を取得しており、個人情報保護法に基づいてお客様の個人情報を適切に保護しております。

35.　知的財産権（18.1.2）

知的財産権に関するお問い合わせは、下記の通りとなっております。また、当社ポータルサイトのお問い合わせ窓口からも受付を行っております。

- 苦情の受付窓口：所定のメールアドレス（proever.support@msols.com）
- 苦情の受付方法：当社指定のメールアドレス宛への連絡
- 苦情の対応部門：PROEVER 事業部（カスタマーサポートチーム）

36. 記録の保護（18.1.3）

各種アクセスログについて、原則として当日を含む過去 30 日分の記録を提供しております。30 日を超えた記録に関しては、一部のログを提供できない場合がございます。

また、お客様の記録は Microsoft Azure 内のサービスを利用し、記録の収集と保護を行っております。当該サービスが当社の要求するセキュリティ水準を満たしていることを確認するとともに、当該サービスの利用に際しアクセス制御等を実施することで、お客様の記録の保護を行っております。

37. 暗号化機能に対する規制（18.1.5）

お客様の端末と当社が提供するサービス間の通信は TLSv1.2 によって暗号化されています。

38. 情報セキュリティの独立したレビュー（18.2.1）

情報セキュリティが自社の方針及び手順に従って実施されていることを確認する目的で、独立したレビュー、監査を実施しております。お客様から提供の依頼があった場合に限り、監査結果をお客様に開示いたします。

IV.　改訂履歴

版数	改定日	主な改定内容
1.0	2023/05/01	初版発行
1.1	2023/05/15	・「情報のラベル付け（8.2.2)」の変更 ・「特権的アクセス権の管理（9.2.3)」の変更 ・「利用者の秘密認証情報の管理（9.2.4)」の変更 ・「適用法令及び契約上の要求事項の特定（18.1.1)」の変更 ・「記録の保護（18.1.3)」の変更 ・「情報セキュリティの独立したレビュー（18.2.1)」の変更
1.2	2023/07/12	・誤字の修正