RemoteOn の情報セキュリティへの取り組みに関するホワイトペーパー

第 1.0 版

ジャパンメディアシステム株式会社

2024 年 1 月 12 日

目次

1. ホワイトペーパーの目的 3
2. 情報セキュリティへの取り組み 3
3. RemoteOn について 3
4. JIS Q 27017：2016（ISO/IEC27017：2015）への対応 4
5.1.1 情報セキュリティのための方針群 4
6.1.1 情報セキュリティの役割及び責任 4
6.1.3 関係当局との連絡 4
CLD6.3.1 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 4
7.2.2 情報セキュリティの意識向上、教育及び訓練 4
8.1.1 資産目録 4
CLD8.1.5 クラウドサービス利用者の資産の除去 4
8.2.2 情報のラベル付け 5
9.2.1 利用者登録及び登録削除 5
9.2.2 利用者アクセスの提供 5
9.2.3 特権的アクセス権の管理 5
9.2.4 利用者の秘密認証情報の管理 5
9.4.1 情報へのアクセス制限 5
9.4.4 特権的なユーティリティプログラムの利用 5
CLD9.5.1 仮想コンピューティング環境における分離 5
CLD9.5.2 仮想マシンの要塞化 5
10.1.1 暗号による管理策の利用方針 6
11.2.7 装置のセキュリティを保った処分又は再利用 6
12.1.2 変更管理 6
12.1.3 容量・能力の管理 6
CLD12.1.5 実務管理者の運用のセキュリティ 6
12.3.1 情報のバックアップ 6
12.4.1 イベントログ取得 6
12.4.4 クロックの同期 6
CLD12.4.5 クラウドサービスの監視 6
12.6.1 技術的ぜい弱性の管理 6
13.1.3 ネットワークの分離 7
CLD13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合 7
14.1.1 情報セキュリティ要求事項の分析及び仕様化 7
14.2.1 セキュリティに配慮した開発のための方針 7
15.1.2 供給者との合意におけるセキュリティの取扱い 7
15.1.3 ICT サプライチェーン 7
16.1.1 責任および手順 7
16.1.2 情報セキュリティ事象の報告 7

16.1.7　証拠の収集 8
18.1.1　適用法令及び契約上の要求事項の特定 8
18.1.2　知的財産権 8
18.1.3　記録の保護 8
18.1.5　暗号化機能に対する規制 8
18.2.1　情報セキュリティの独立したレビュー 8
5.　改訂履歴 9

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、ジャパンメディアシステム株式会社（以下、当社）が提供する「RemoteOn」における、セキュリティへの取り組みについて記載したものです。クラウドセキュリティの国際規格 ISO/IEC27017 の中で、特に利用者に向けて情報開示が求められる事項について、セキュリティへの取り組みをご確認いただくことを目的としております。
ISO/IEC27017 は、クラウドサービスに関する情報セキュリティ管理策のガイドライン規格となります。
本書では、ISO/IEC27017「情報セキュリティ管理策の実践の規範」の項番に沿って本サービスの管理策を記載しております。

2. 情報セキュリティへの取り組み

当社では、「情報セキュリティ基本方針」や「プライバシーポリシー」などを定めており、当社開発業務の遂行に関わる関係者に対して、定期的に情報セキュリティ教育・訓練を実施しております。
また、当社技術本部は、下記認証登録範囲の情報セキュリティマネジメントシステム（以下、ISMS）において、JIS Q 27001:2014（ISO／IEC 27001）と JIP-ISMS517-1.0（ISO／IEC27015:2015）の要求事項に適合し、認証登録番号「JP15／080358」と「JP21／080663」を保有しております。

＜ISMS 認証登録＞
https://web.liveon.ne.jp/isms/
＜情報セキュリティ基本方針＞
https://www.jm-s.co.jp/security/
＜プライバシーポリシー＞
https://www.jm-s.co.jp/privacy/

3. RemoteOn について

RemoteOn（以下、本サービス）は、インターネットを介して「勤務先など遠隔地の PC」を「自宅など手元の PC」で遠隔操作することができるテレワーク・在宅勤務に欠かせないリモートデスクトップサービスとなります。

4. JIS Q 27017：2016（ISO/IEC27017：2015）への対応

本項では、JIS Q 27017：2016（ISO/IEC 27015：2015）が求める要求事項に対する管理策を記載します。

「5.1.1 情報セキュリティのための方針群」などの番号・タイトルは、ISO27017 が求める“情報セキュリティ管理策の実践の規範”箇条 5～18（17 箇条を除く）の小項目番号・要求事項原文を示し、後に続く内容は、本サービスの要求事項に対する解釈及び管理策になります。

5.1.1　情報セキュリティのための方針群

本サービスは、当社の定めた情報セキュリティ基本方針に従い、サービス運営を行っております。
当社の情報セキュリティ基本方針（https://www.jm-s.co.jp/security/）をご覧ください。また、クラウドセキュリティ基本方針についても、併せてご覧ください。

6.1.1　情報セキュリティの役割及び責任

当社の情報セキュリティの役割及び責任分担については、RemoteOn サービス利用規約に記載しております。
※RemoteOn サービス利用規約（https://www.remoteon.ne.jp/terms/）

6.1.3　関係当局との連絡

当社の所在地は、当社 Web サイト（https://www.jm-s.co.jp/）をご確認ください。
また、本サービスで送受されるデータの保存は発生いたしません。

CLD6.3.1　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

RemoteOn サービス利用規約にて、役割及び責任を定義しております。また、情報セキュリティ基本方針やクラウドセキュリティ基本方針にも、当社が実施すべき役割・内容を記載しております。

7.2.2　情報セキュリティの意識向上、教育及び訓練

当社では、情報セキュリティ基本方針及びクラウドセキュリティ基本方針を定め、方針に従いサービスを運営しております。また、本サービスの開発・運用・保守に携わる社員に対する定期的な教育を実施しております。

8.1.1　資産目録

利用者の情報資産とサービス提供者が本サービスを運営するための情報資産は、明確に分離しております。なお、利用者の情報資産に関しては、利用者の管理範囲となります。

CLD8.1.5　クラウドサービス利用者の資産の除去

RemoteOn サービス利用規約にて、解約時のカスタマデータの返却・削除に関する内容を記載しております。

8.2.2　情報のラベル付け

仮想マシン上のデータに対して、ラベル付けを行う機能は提供しておりません。

9.2.1　利用者登録及び登録削除

ライセンスキー・パスワードをはじめとする利用者情報の登録機能は提供しておりますが、登録情報の削除機能は提供しておりません。

9.2.2　利用者アクセスの提供

本サービスは、Admintool（管理者）機能を標準で提供しており、ライセンスキーをはじめとする利用者情報の管理を行うことが可能です。

9.2.3　特権的アクセス権の管理

本サービスは、Admintool（管理者）機能を標準で提供しております。本機能をご利用いただくための URL は自動生成しており、セキュリティに配慮した複雑な URL を提供しております。

9.2.4　利用者の秘密認証情報の管理

RemoteOn 製品サイト上にて、秘密認証情報の設定に関する情報を提供しております。
なお、パスワードの設定はお客様のセキュリティポリシーに基づいて実施してください。管理者権限はお客様のセキュリティポリシーに従い厳重に管理することをお願いします。
※RemoteOn オンラインヘルプ（https://www.remoteon.ne.jp/help/）

9.4.1　情報へのアクセス制限

本サービスは、Admintool（管理者）機能を利用して、ライセンスキーの有効／無効の設定や任意のライセンスの強制切断が可能です。

9.4.4　特権的なユーティリティプログラムの利用

利用者に対し、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。

CLD9.5.1　仮想コンピューティング環境における分離

当社は、クラウドサービスプロバイダより提供されるマルチテナント環境を利用しております。本サービスは、ホスト側 PC とビューアー側 PC との 1 対 1 で使用するサービスとなるため、他の利用者にデータが共有されることはない仕様となっております。また、社内においても、クラウドサービス環境へは業務上アクセスの必要がある社員にのみアカウントを付与するなどのアクセス制御を実施しております。

CLD9.5.2　仮想マシンの要塞化

当社は、必要最小限の構成でサーバを構築して、不必要なサービスは起動しないようにしております。また、本サービスをご利用いただくのに必要なポートやプロトコルへのアクセス制限を実施しております。

10.1.1　暗号による管理策の利用方針

本サービスの通信データは、AES を使用して暗号化しております。また、Web の通信経路では、SSL／TLS による通信の暗号化を使用しております。

11.2.7　装置のセキュリティを保った処分又は再利用

当社は、クラウドサービスプロバイダより提供されるマルチテナント環境を使用しております。当社では直接、装置の処分を実施することはなく、クラウドサービスプロバイダ側の処分に依存しております。

12.1.2　変更管理

サービス変更がある場合には、リリースの 1 か月前にユーザー通知を実施しております。また、サービス変更の情報については、RemoteOn 製品サイトにて公開しております。

12.1.3　容量・能力の管理

安定的なサービス提供を行うため、CPU 利用率、サーバのディスク容量などを含むサービス利用状況の監視を実施しております。また、監視結果を参考に、必要に応じてリソース増強の検討及び実施を行っております。

CLD12.1.5　実務管理者の運用のセキュリティ

本サービスの操作方法に関しては、RemoteOn 製品サイト上にてオンラインヘルプを公開しております。また、各種問い合わせについては、問い合わせフォームやメール、電話にてお受けしております。

12.3.1　情報のバックアップ

本サービスは、バックアップ機能を提供しておりません。

12.4.1　イベントログ取得

利用者は、Admintool（管理者）機能より、ログイン履歴や使用帯域などの利用者管理に関わるログを取得することが可能です。機能の情報は、オンラインヘルプにて公開しております。
なお、これらのログ情報を確認できる期間は、過去 1 年間となります。

12.4.4　クロックの同期

Amazon Linux の NTP デーモンを利用して、時刻同期を行っております。

CLD12.4.5　クラウドサービスの監視

本サービスでは、Admintool（管理者）機能より、ログイン履歴や使用帯域などの利用者管理情報を確認する機能を提供しております。

12.6.1　技術的ぜい弱性の管理

定期的に脆弱性情報を収集して、本サービスへの影響度合いを検討し、必要に応じて対応を実施して

おります。

13.1.3　ネットワークの分離

クラウドサービス上の環境については、ライセンスキーごとに分離させております。また、クラウドサービスと当社内部ネットワークについても、分離させております。

CLD13.1.4　仮想及び物理ネットワークのセキュリティ管理の整合

物理ネットワーク上に仮想マシンを構築する際は、物理ネットワークと仮想ネットワーク間の整合性を確保するようにしております。

14.1.1　情報セキュリティ要求事項の分析及び仕様化

セキュリティ関連機能の仕様については、オンラインヘルプや本書にて公開しております。

・アクセス制御関連（9.4.1 情報へのアクセス制限、CLD9.5.2 仮想マシンの要塞化）
・通信の暗号化関連（10.1.1 暗号による管理策の利用方針）
・ログ情報関連（12.4.1 イベントログ取得）

14.2.1　セキュリティに配慮した開発のための方針

情報セキュリティ基本方針やクラウドセキュリティ基本方針に基づき、情報セキュリティを維持する責任を自覚させるためのセキュリティ教育を受けた社員で開発を行っております。

15.1.2　供給者との合意におけるセキュリティの取扱い

RemoteOn サービス利用規約にて、サービス利用における当社の役割及び責任について記載しております。また、提供しているセキュリティ機能に関する情報については、RemoteOn 製品サイト上にて公開しております。

15.1.3　ICT サプライチェーン

本サービスの提供に関連する供給者に対しては、情報セキュリティリスクに対処することを要求する方針を定めております。

16.1.1　責任および手順

本サービスのインシデント発生やサービス内容の変更に関しては、クラウドセキュリティ基本方針に則り、お知らせやメール通知を通じてお客様に対し情報を提供しております。なお、情報セキュリティの責任分担については、RemoteOn サービス利用規約に記載しております。

16.1.2　情報セキュリティ事象の報告

本サービスのインシデント発生やサービス内容の変更に関しては、クラウドセキュリティ基本方針に則り、お知らせやメール通知を通じてお客様に対し情報を提供しております。また、本サービスにおいて発生したインシデントについては、RemoteOn 製品サイト上にて情報を公開して、お客様がインシデント情報を監視及び追跡できるようにしております。
お客様からのお問い合わせについては、メールや電話、問い合わせフォームなどよりお受けしており

ます。

16.1.7　証拠の収集

法令や裁判所などの命令に基づき開示請求が行われ、当社が必要であると判断した場合の第三者への情報開示については、RemoteOn サービス利用規約に記載しております。

18.1.1　適用法令及び契約上の要求事項の特定

本サービスにおいて適用される準拠法は、日本法となります。準拠法に関する情報については、RemoteOn サービス利用規約にも記載しております。

18.1.2　知的財産権

当社の情報セキュリティの役割及び責任分担については、RemoteOn サービス利用規約に記載しております。個人情報に関するお問い合わせについては、プライバシーポリシーにて公開しております。

18.1.3　記録の保護

本サービスでは、利用状況履歴を一定期間システム内に保存しております。当社が保存する情報や保存期間については、RemoteOn サービス利用規約にも記載しております。なお、保存している情報には、業務上アクセスの必要がある社員のみがアクセスできるよう制御しております。

18.1.5　暗号化機能に対する規制

本サービスにおける暗号の利用については、「10.1.1 暗号による管理策の利用方針」に記載しております。なお、輸出規制の対象となる暗号化の利用はありません。

18.2.1　情報セキュリティの独立したレビュー

当社は、ISO／IEC27001 と ISO／IEC27017 について、第三者の認証機関による審査を受け、認証を取得しております。なお、認証取得状況については、RemoteOn 製品サイト上にて公開しております。

5. 改訂履歴

版 数	日 付	改訂内容
第 1.0 版	2024/01/12	初版