RICOH Collaboration Board

セキュリティホワイトペーパー

Ver.1.2.1

2025年4月21日

株式会社リコー

＜目次＞

1. はじめに

1.1. 目的

本書は、RICOH Collaboration Board をお客様に安心して頂くためご利用いただくために、本システムのセキュリティ対策と仕組みについて説明することを目的としています。

1.2. 本書説明の対象となる範囲

本書は、RICOH Collaboration Board で利用しているアプリケーションおよびサーバーのセキュリティ対策を説明対象としています。

クラウドサービス事業者がクラウドサービスを提供する際に実施することが望ましい情報セキュリティ対策について、以下のガイドラインが公開されています。

クラウドサービス提供における情報セキュリティ対策ガイドライン [1]（第 3 版)

これは「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 2 版）」(2018 年 7 月)を基に、ISMAP 管理基準、ISO/IEC27017(2016)及び NIST SP800-53 Rev.5 を参考にして、クラウドサービス提供事業者が実施すべき情報セキュリティ対策を整理し/改定されたものであり、次章より説明する本システムのセキュリティ対策も上記ガイドラインに即したものとなっています。

また、リコーグループは、お客様に安心してご利用いただける製品・サービスを提供していくための不可欠な要素として、情報セキュリティマネージメントに取り組んでいます [2]。この取り組みにより、上記ガイドラインの組織・運用面の対策についてはその多くが網羅できているため、本書の対象外とし、主に物理的・技術的対策にフォーカスして説明しています。

リコーグループの情報セキュリティに関しては、こちら（https://jp.ricoh.com/security/management）を参照してください。

1.3. 用語定義

RICOH Collaboration Board：

ホワイトボード機能や外部入力表示機能を持ったアプリケーションおよび IFPD デバイス。

クラウドホワイトボード：

インターネット経由で他のデバイスと共有しながら書き込めるホワイトボード機能。

---

[1] 総務省 2021 年 9 月
https://www.soumu.go.jp/main_content/000771515.pdf

[2] リコーグループの情報セキュリティ、（適宜更新）
http://jp.ricoh.com/security/management/

1.4. 本書の構成

以下の章目次に示す通り、まずシステムの概要を把握いただくため、2 章でシステム構成、ユースケース、データフロー、通信プロトコルについて説明しています。そして、3～6 章でシステム全般および、各項目のセキュリティ対策について説明し、最後に製品を安全にお使いいただくための注意点を記載しています。

- 2 章 システム構成
- 3 章 システム全般のセキュリティ対策
- 4 章 データのセキュリティ対策
- 5 章 ネットワークのセキュリティ対策
- 6 章 データセンターのセキュリティ対策
- 7 章 安全にお使いいただくために

2. システム構成

2.1. 全体構成

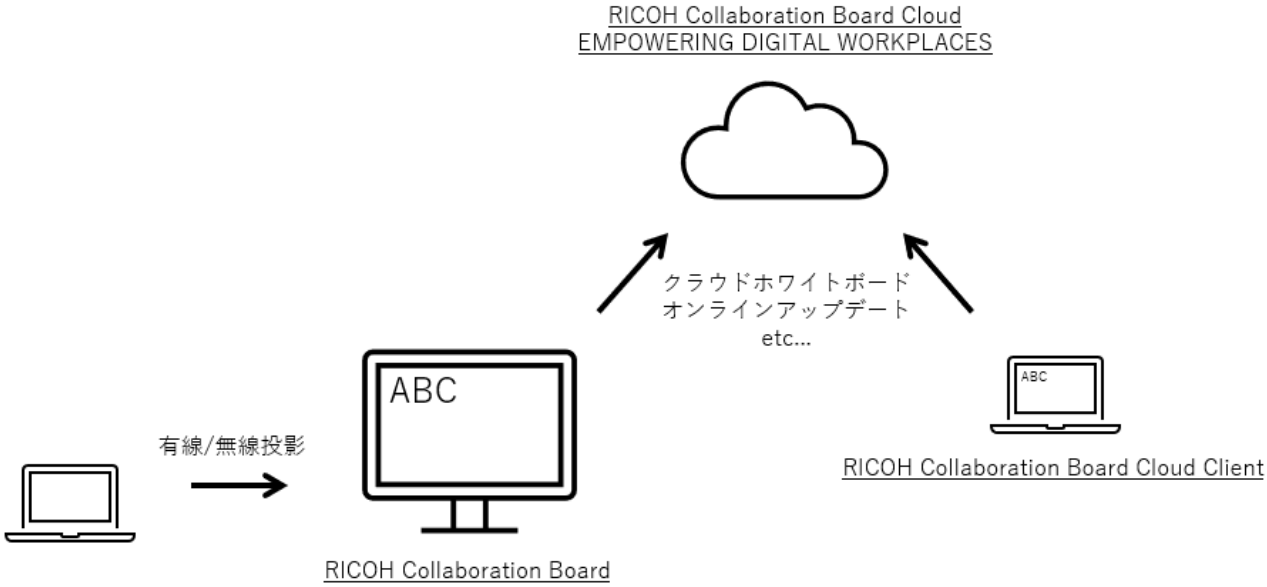


図 1 RICOH Collaboration Board システム構成図

RICOH Collaboration Board は、機器（RICOH Collaboration Board）と、お客様環境の PC 上で動作する PC クライアント（RICOH Collaboration Board Cloud Client）と、インターネット上に存在する RICOH Collaboration Board Cloud / EMPOWERING DIGITAL WORKPLACES プラットフォームで構成されます。
RICOH Collaboration Board Cloud はアプリサーバー（クラウドホワイトボード/アカウント設定サイト/管理者設定サイト）とバックエンドサーバー（RICOH Collaboration Board および RICOH Collaboration Board Cloud Client の機能提供用バックエンドサービス）から構成され、EMPOWERING DIGITAL WORKPLACES プラットフォームはアプリサーバー（ユーザー管理サイト）とバックエンドサーバー（MS365 連携を含む ID 管理、認証、会議情報管理バックエンドサービス）から構成されます。
PC クライアントは、バックエンドサーバーと通信し、クラウドホワイトボード等の機能提供を行います。
また、RICOH Collaboration Board は他の PC やスマホ等からの有線/無線での映像投影機能を持ちます。

2.2. 通信プロトコル

2.2.1. お客様環境から本サービスプラットフォームへの通信

RICOH Collaboration Board / RICOH Collaboration Board Cloud Client を利用する場合の、お客様環境から RICOH Collaboration Board Cloud / EMPOWERING DIGITAL WORKPLACES プラットフォームへの

通信については、以下の表 1 をご確認ください。

表 1 お客様環境からの通信

接続元	通信先ホスト	ポート	プロトコル
RICOH Collaboration Board	*.accounts.ricoh.com	443/TCP	HTTPS
	*.smart-integration.ricoh.com	443/TCP	HTTPS
	*.smart-integration.ricoh.com	443/TCP	WSS
	*.cs.rinfra.ricoh.com	443/TCP	HTTPS
	*.iot.us-west-2.amazonaws.com	443/TCP	HTTPS
	*.iot.us-west-2.amazonaws.com	443/TCP	WSS
	s3.ap-northeast-1.amazonaws.com	443/TCP	HTTPS
	*.s3.ap-northeast-1.amazonaws.com	443/TCP	HTTPS
RICOH Collaboration Board Cloud Client	*.accounts.ricoh.com	443/TCP	HTTPS
	*.smart-integration.ricoh.com	443/TCP	HTTPS
	*.smart-integration.ricoh.com	443/TCP	WSS
	*.cs.rinfra.ricoh.com	443/TCP	HTTPS
	*.iot.us-west-2.amazonaws.com	443/TCP	HTTPS
	*.iot.us-west-2.amazonaws.com	443/TCP	WSS

2.2.2. お客様環境から Microsoft Edge エンドポイントへの通信

RICOH Collaboration Board や Microsoft 社製アプリを安定的にご使用いただくためには、Microsoft Edge エンドポイントへの通信を全て許可していただく必要があります。これにより、アプリケーションが正常に機能し、最新のセキュリティアップデートや機能改善を適切に受け取ることができます。

詳細については、以下の Microsoft ドキュメントをご確認ください。
Microsoft Edge エンドポイントの許可リスト

また、上記エンドポイントへの通信許可が正しく設定されていても、グループポリシー設定により、正常にインストールがされない可能性があります。この場合、以下の Microsoft ドキュメントをご確認いただき、適切な設定を維持していただくようお願いします。
Edge のインストールおよび更新制御方法について

2.2.3. お客様環境から BYOM サービスへの通信

RICOH Collaboration Board の BYOM 機能を安定的にご使用いただくためには、以下の通信を全て許可していただく必要があります。これにより、アプリケーションが正常に機能し、最新のセキュリティアップデートや機能改善を適切に受け取ることができます。

表 2 BYOM サービスへの通信

接続元	通信先ホスト	ポート	プロトコル
RICOH Collaboration Board	amadeus-api.displaynote.com	443/TCP	HTTPS
	releases.displaynote.com	443/TCP	HTTPS

2.2.4. お客様環境から RICOH Collaboration Board Add-on Service for Microsoft 365 への通信

RICOH Collaboration Board Add-on Service for Microsoft 365 をご使用いただくためには、以下の通信を全て許可していただく必要があります。

表 3 Add-on Service for Microsoft 365 への通信

接続元	通信先ホスト	ポート	プロトコル
RICOH Collaboration Board	graph.microsoft.com	443/TCP	HTTPS
	*.sharepoint.com	443/TCP	HTTPS
	*.box.com	443/TCP	HTTPS

2.2.5. お客様環境からその他のインターネット環境への通信

外部サービスとの連携は、外部サービスの仕様に従います。
Windows の既定のセキュリティ設定に加え、RICOH Collaboration Board の動作に必要なポートを開放する設定をしています。詳細は表 4 をご確認ください。
お客様がネットワーク通信を行うアプリケーションを追加した場合は、アプリケーションの要件に応じてネットワークポートの設定する必要があります。

表 24 RICOH Collaboration Board 使用ポート一覧

説明	ポート	通信方向
無線投影接続	1900/UDP	IN
	5000-5010/TCP	IN
	5353/UDP	IN
	7000/TCP	IN
	7100/TCP	IN
	7236/TCP	OUT
	7250/TCP	IN
	8008-8019/TCP	IN
	32768-65535/TCP	IN/OUT
	32768-65535/UDP	IN/OUT

2.2.6. マルチテナント対応

EMPOWERING DIGITAL WORKPLACES プラットフォームは複数の企業・組織に対してサービスを提供します。企業・組織など、サービスを提供する対象をテナントと呼び [3]、複数のテナントの情報を同一ハードウェア上で管理しています。システムは論理的にテナント間でのデータを分離しており、テナント間の独立性を確保しています [4]。データアクセスに関しては、4.1 データアクセス制御に記載しています。

テナントは、エンドユーザーが自身の属するテナントにライセンスされた EMPOWERING DIGITAL WORKPLACES プラットフォーム上のアプリケーションを利用するためのもので、他テナントの情報を参照することはできません。

[3] 複数の企業が合同で契約するような利用形態があるため、「企業」ではなく「テナント」と言う用語を使用しています。

[4] このようなシステム構成は、「マルチテナントアーキテクチャ」と呼ばれます。

3. システム全般のセキュリティ対策

3.1. 稼動監視、障害監視、パフォーマンス監視

24 時間 365 日でネットワーク、サーバー、アプリケーションなどの稼働状況、パフォーマンスを監視しており、万一不具合が発生した場合には迅速な対応を行う体制となっています。またキャパシティ管理 [5]を行い、十分な可用性を確保しています。

3.2. 脆弱性情報の定期的収集とパッチ適用

脆弱性情報の収集と対応は、リコー社内で定められたプロセスに従って運用しています。OS やミドルウェア等に対するセキュリティーパッチは重要性とシステムへの影響を判断した上で、開発環境にて検証後、実運用環境への実施を計画し適用しています。

また、脆弱性情報はリコー社内外から広く入手し、社内の脆弱性管理システムを利用してサービスへの影響度と対応有無を継続的に管理しています。

[5] テナント、ユーザー、機器、ライセンス、ジョブの想定数に対して、十分なストレージ容量を割り当て、また実際の使用量の監視を行っています。

3.3. 脆弱性診断

Web アプリケーションの脆弱性評価ツールとして IBM 社の AppScan を使用して、以下の項目について 3 ヶ月に 1 度確認を行い、既知の脆弱性が残されていないことを確認しています。

表 5　AppScan の脆弱性分類と対応する項目例

検査分類	具体的な検査項目
認証	・総当り攻撃 ・不適切な認証
認可	・インデクシング/セッションの推測 ・セッションの固定 ・不適切なセッション期限 ・不適切な許可
アプリケーション	・プライバシーテスト ・品質テスト
クライアント側攻撃	クロスサイトスクリプティング コンテンツの成りすまし
コマンドの実行	・LDAP インジェクション ・OS 命令 ・SQL インジェクション ・SSL インジェクション ・XPath インジェクション ・バッファオーバーフロー ・書式文字列攻撃
情報の開示	・ディレクトリインデクシング ・パストラバーサル ・情報遺漏 ・推測可能なリソース
論理攻撃	・サービスの拒否攻撃 ・機能の悪用

さらに、第三者評価として、Web アプリケーションの脆弱性評価ツールとして米 Rapid7 社の InsightVM を 1 ヶ月に 1 回適用し、既知の脆弱性が残されていないことを確認しています。

3.4. ログ

3.4.1. システム共通

サーバーのアプリケーションログは統合的に収集を行い、不正アクセス、システム障害の解析を一元的に行えるようにしており、各サーバー内のシステムログを含め、定期的にバックアップを行っています。なお、出力情報はリコー社内のルールに従って出力内容を適切に判断しており、全てのログにおいてパスワード情報は出力しておりません。

3.5. セキュリティ保証範囲

RICOH Collaboration Board ではオープンシステムを採用しており、お客様が自由に Windows OS をカスタマイズして利用することができます。
セキュリティの保証対象範囲は弊社が提供するアプリケーションのみです。お客様がインストールしたアプリケーション、接続したデバイス、Windows OS がシステム全体のセキュリティに与える影響に対して、弊社では責任を負いかねます。追加アプリケーションの使用に際しては、十分なセキュリティ対策を講じ、Windows OS を適切に管理するように運用してください。

4. データのセキュリティ対策

4.1. データアクセス制御

図 1 の EMPOWERING DIGITAL WORKPLACES プラットフォームで利用されるデータは、ユーザーやテナント単位で管理されており、各データにアクセスするためには、ユーザー認証で発行される認証チケットが必要となります。認証チケットによってアクセスできるデータを制御しているので、別企業のユーザー情報が目にふれることはありません。
EMPOWERING DIGITAL WORKPLACES プラットフォームで管理するデータは、AWS 上に存在し、インターネットから直接アクセスすることができず、EMPOWERING DIGITAL WORKPLACES プラットフォーム内に存在するエンドポイントを経由しない限りアクセスできません。
また、AWS にアクセスできるアカウントに対して AWS IAM でアクセス権限を設定しており、内部から業務上必要な範囲以外のデータにアクセスできないようになっています。

4.1.1. ユーザー認証

ログイン（ブラウザ、PC 共通）

図 1 の EMPOWERING DIGITAL WORKPLACES プラットフォーム にアクセスするには、テナント ID、ユーザー名、パスワード、または、メールアドレス、パスワードによるログイン(ユーザー認証)を行う必要があります。認証に成功しない限り、続く操作を実行することはできないようになっています。

テナント ID は 10 桁の数字列で、業務システムにより発行され、利用お申し込み後に、お客様に割り当てられます。ユーザー名は 1 文字以上 128 文字以下の文字列として登録することができます。

パスワードは、最大 128 文字(最小 6 文字)の任意のアスキー文字列として設定でき、ログイン時にパスワードを 5 回連続で間違えるとそのアカウントはロックされるため、ブルートフォース攻撃や辞書攻撃に対し、十分な耐性を有しています。アカウントがロックされた場合、管理者がユーザー管理画面から有効化するか、ユーザーがパスワードをリセットするか、24 時間後にシステムによって自動解除されるまでログインすることはできません。

登録されている テナント ID、ユーザー名、メールアドレス等のアカウント情報は、情報として漏洩することはないため、リバースブルートフォース攻撃に対する耐性も有しています。

ユーザーは、ユーザーサイトからパスワード変更できます。また、センター側でパスワードのハッシュ値のみを保存しているので、リコーはお客様のパスワードを入手することはできず、センター側からパスワードの文字列が漏えいすることはありません。
なお、ハッシュ値やユーザー情報のデータアクセスに関しても、適切なアクセス制限を行うことで、社内外からの不正アクセスを防いでいます(5.1 節参照)。

また、外部サービスのアカウントを利用したシングルサインオン機能も備えています。

デバイス（RICOH Collaboration Board）からのログイン

デバイス（RICOH Collaboration Board）からのログインは、ログイン(ブラウザ、PC 共通)に記載の方法の他に、IC カードログイン、または、デバイス（RICOH Collaboration Board）が連携している認証サーバー(Active Directory 等)のアカウント(ID/パスワード)でログインすることができます。これらのログインは登録されたデバイス（RICOH Collaboration Board）からのみ利用できるため、PC などの他のクライアントデバイスからログインすることはできません。

外部サービスへのシングルサインオン

デバイス（RICOH Collaboration Board）から EMPOWERING DIGITAL WORKPLACES プラットフォームにログインすると、外部サービスにアクセスできるようになります。例えば、Microsoft365 の OneDrive for Business や Outlook(Exchange Online)のスケジュール、Box のオンランストレージにアクセスできるようになります。

シングルサインオンは、予め、RICOH Collaboration Board Add-on Service 連携設定サイトで、Microsoft 365 や Box のアカウントと、EMPOWERING DIGITAL WORKPLACES プラットフォームのアカウントを紐づけておく必要があります。紐づけは、OAuth 認可を用いて行われます。

機器にログインした EMPOWERING DIGITAL WORKPLACES プラットフォームアカウントは、OAuth で認可されている範囲のデータにしかアクセスできません。

一般的にアカウントの紐づけ(SSO 設定)は外部サービスのアカウントを有するユーザーが自身のアカウントにログインし、認可されるデータの範囲を確認し承認することで行われます。

ログイン（デバイス）

システムの各種設定を実施するビルトイン管理者アカウントにサインインするためには、パスワード認証が必要です。

RICOH Collaboration Board では、既定の初期管理者パスワードは設定されておらず、初回起動時に必ず管理者パスワードを設定させることにより、既定パスワードを用いた不正アクセスを防止しています。

既定のパスワードポリシーは付録：RICOH Collaboration Board システムガイドの[設定済みのグループポリシー一覧]をご確認ください。

4.2. データ暗号化

RICOH Collaboration Board は、コントローラーに装着されている Trusted Platform Module(TPM)を使用して SSD を暗号化(BitLocker)することができます。この設定を有効にすることで万が一意図せず SSD が転用されても SSD 内のデータが読み取られることはないため、設定を有効にすることを強く推奨します。SSD 暗号化を有効にした場合、回復キーを確認することができます。この回復キーは、TPM が破損して自動復号に失敗した場合、Windows の構成変更が発生した場合の回復手段として必要です。例えば、Windows Update などにより Windows の構成変更が意図せずに起きることがあります。その場合は、回復キーを入力しない限り RICOH Collaboration Board が利用できなくなることがありますので、回復キーは必ず控えるようにしてください。

4.3. 不正改竄防止

RICOH Collaboration Board ではシステム更新の際、システム更新ファイルの正当性を検証し更新ファイルが改竄されていないか確認します。

4.4. マルウェア対策

RICOH Collaboration Board ではホワイトリスト方式のセキュリティ対策ソフトウェア(AppLocker)により、特定の条件のアプリケーションのみ動作します。また、万が一マルウェアが保存・インストールされた場合、ブラックリスト方式のセキュリティ対策ソフトウェア(Windows Defender)によりマルウェアの駆除が実行されます。ブラックリスト方式のセキュリティ対策ソフトウェアにより、ウィルス定義ファイル(ブラックリスト)に記載されているウィルスの駆除が実行されます。ブラックリストは Windows Update 時に更新されるため、最新のウィルスに対応することができます。
ホワイトリスト方式のセキュリティ対策ソフトウェアの既定の設定値は付録：RICOH Collaboration Board システムガイドの[設定済みのグループポリシー一覧]をご確認ください。

5. ネットワークのセキュリティ対策

5.1. アクセス制御

5.1.1. ネットワークのアクセス制御

インターネットから直接アクセスできるサーバーにはパスワードなどの機密情報は置かず、4.1 章の通りの AWS アカウント限定でアクセスできる場所に保管されます。インターネットからサーバーに対して直接ログインできないようにしています。また、AWS のセキュリティグループ（仮想ファイアウォール）で通信を許可するポート番号を設定することにより外部からの不正アクセスを防止しています。

保守業務は、リコー社内 LAN からインターネット回線でセンターサーバーに接続して行っています。AWS のセキュリティグループ（仮想ファイアウォール）で通信を許可する IP アドレス、および、ポート番号を設定することで、センターサーバーへのアクセスを、リコー社内 LAN からのみ、かつ特定プロトコルでの暗号化通信に限定していますので、第三者がインターネットから接続して、保守業務装いセンターサーバーにアクセスすることはできません。また、センターサーバーへの接続はパスワードではなく SSH 秘密鍵を使用しており、リコー社内からの接続者を、公開鍵を作成した関係者に限定することで、保守業務における顧客情報の漏洩や攻撃を防いでいます。

5.1.2. サーバー(OS)のアクセス制御

サーバーで保存しているデータについては種類によって適切なアクセス範囲を決め、業務上必要な範囲以外のデータにアクセスできないように AWS IAM でアカウントやサーバー毎にアクセス権限を設定しています。データアクセスに関する取り扱い手順を定めており、手順に従って承認を得た上でアクセスが行われます。サーバー管理者に対しては、事前にセキュリティ教育を実施し、また定期的に取り扱い手順の確認/徹底を行っています。

5.2. 通信経路の暗号化

5.2.1. ブラウザ、PC、機器とセンター間の通信

ブラウザ、PC、機器とセンター間の通信は、すべて HTTPS で通信経路を暗号化しています。センターのサーバー証明書には、ACM[6]を利用しており、暗号化には AWS のセキュリティポリシー[7]のうち ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04 を利用しています。HTTPS で用いるプロトコルとそのバージョンは、以下のものをサポートしています。

TLS 1.3

- TLS 1.2

5.2.2. 無線 BYOM ソフトウェア（RICOH Omni Client Powered by DisplayNote）の通信

RICOH Omni Client Powered by DisplayNote で使用する全てのデータは SRT プロトコルにより暗号化されています。

[6] AWS Certificate Manager
https://aws.amazon.com/jp/certificate-manager/

[7] AWS のセキュリティポリシー
https://docs.aws.amazon.com/ja_jp/elasticloadbalancing/latest/application/create-https-listener.html#describe-ssl-policies

6. データセンターのセキュリティ対策

サーバー群は、AWS の上に構成されます。データセンターのセキュリティ対策は AWS のセキュリティ対策によって行われています。[8]AWS 上のデータベースサーバーは、Multi-AZ で構成されており、障害が発生してもサービスを継続できるように設計されています。AWS 上のデータベース、ストレージで保存されるデータは、暗号化されております。ホワイトボードの情報を扱うサーバーは日本国内にあり、日本国内の法律および条令が適応されるよう対策されています。

[8] AWS セキュリティプロセスの概要：
日本語：https://d1.awsstatic.com/whitepapers/ja_JP/Security/AWS_Security_Whitepaper.pdf
English: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

7. 安全にお使いいただくために

共有機として RICOH Collaboration Board をご利用するシーンにおきましては、オープンシステムの特性上様々な脅威が想定されます。
安全にご利用していただくために、付録：RICOH Collaboration Board システムガイドの「専用アカウントについて」をご確認していただき、適切なアカウントで運用してください。

機器のセキュリティを確保するため以下の点に注意し、設置および設定を適切に行ってください。

1. 最新のファームウェアを適用する。
2. 最新のアプリケーションを利用する。（お客様が追加したアプリケーションやデバイスなど）
3. 最新の Windows Update を適用する。
4. 推測されにくいパスワードを設定する。
5. ファイヤーウォールで守られたネットワーク内で利用する。
6. 情報漏洩を防ぐため、ホワイトボードにはパスワードを設定し、会議終了後は終了する。
7. のぞき見による情報漏洩を防ぐため、利用時は周囲に配慮する。
8. SSD 暗号化機能(BitLocker)を有効にする。
9. 適切な OS の設定を維持する。

8. 付録：RICOH Collaboration Board システムガイド

「RICOH Collaboration Board システムガイド」では、主に RICOH Collaboration Board の Windows OS に対する設定内容について説明します。

8.1. Windows OS の主な設定・制限

設定項目	補足	標準アカウント	管理者アカウント
タスクバーを使用不可にしています	アプリ動作中のみ	o	x
機器をロック状態と休止状態にすることはできません	コンピューターの構成のグループポリシー	o	o
ユーザーの切り替えをすることはできません	コンピューターの構成のグループポリシー	o	o
ウィジェットを無効にしています	コンピューターの構成のグループポリシー	o	o
セキュリティオプション画面を禁止しています	ユーザーの構成のグループポリシー	o	x
タスクマネージャーの使用を禁止しています	ユーザーの構成のグループポリシー	o	x
スタートメニューで表示する項目を、サインアウト、シャットダウン、再起動、および OS 設定の表示に制限しています	ユーザーの構成のグループポリシー	o	x
OS 設定で設定できる項目を、表示言語設定、場所設定、Bluetooth 設定、カメラ設定、タッチ設定、ペン設定、プリンタ設定、メールへのアクセスに制限しています	ユーザーの構成のグループポリシー	o	x
アプリケーションのトースト通知を無効にしています	ユーザーの構成のグループポリシー	o	x

設定項目	補足	標準アカウント	管理者アカウント
デスクトップの機能を無効にしています	ユーザーの構成のグループポリシー	o	x
Windows インストーラーの使用を制限しています	ユーザーの構成のグループポリシー	o	x
Windows Update は配信されてから 7 日後に強制的に適用されます	コンピューターの構成のグループポリシー	o	X
サインアウト時に Microsoft Edge の閲覧データとキャッシュを削除します	ユーザーの構成のグループポリシー	o	X
Microsoft Edge でのパスワード保存を禁止しています	ユーザーの構成のグループポリシー	o	X

※o：該当 / X：非該当

8.2. 設定済みのグループポリシー一覧

コンピューターの構成のグループポリシー

設定項目	設定値	説明	設定のパス
スタートアップ	c:¥vender-tools¥script¥startup.bat c:¥vender-tools¥script¥startup.ps1	起動時に登録したスクリプトが実行されます **startup.bat と startup.ps1 は RCB のシステム設定用のため、編集・削除しないでください**	コンピューターの構成>Windows の設定>コントロールパネル>スクリプト(スタートアップ/シャットダウン)
シャットダウン	c:¥vender-tools¥script¥shutdown.bat c:¥vender-tools¥script¥shutdonw.ps1	シャットダウン時に登録したスクリプトが実行されます **shutdown.bat と shutdown.ps1 は RCB のシステム設定用のため、編集・削除しないでください**	コンピューターの構成>Windows の設定>コントロールパネル>スクリプト(スタートアップ/シャットダウン)

設定項目	設定値	説明	設定のパス
Windows インストーラーをオフにする	1(管理されていないアプリケーションのみ)	標準アカウントでは Windows インストーラーを起動できなくなります	コンピューターの構成>管理テンプレート>Windows コンポーネント>Windows インストーラー
ユーザーの簡易切り替えのエントリ ポイントを非表示にする	1(有効にする)	ログオン UI、[スタート] メニュー、およびタスク マネージャーで [ユーザーの切り替え] が非表示になります	コンピューターの構成>管理テンプレート>システム>ログオン
電源オプションメニューに休止状態を表示する	無効にする	電源メニューで休止状態を選択できなくなります	コンピューターの構成>管理テンプレート>Windows コンポーネント>エクスプローラー
システム休止タイムアウトを指定する (電源接続時)	有効にして、休止タイムアウト値に 0 を指定する	指定時間経過後に休止状態になる機能が無効になります（電源メニューでスタートする）	コンピューターの構成>管理テンプレート>システム>電源の管理 >スリープの設定
システム休止タイムアウトを指定する (バッテリ使用時)	有効にして、休止タイムアウト値に 0 を指定する	指定時間経過後に休止状態になる機能が無効になります（電源メニューでスタートする）	コンピューターの構成>管理テンプレート>システム>電源の管理 >スリープの設定
既定のアカウントの画像をすべてのユーザーに適用する	有効	スタートメニュー内の[アカウント設定を変更]を非表示にします	コンピューターの構成>管理テンプレート>コントロールパネル>ユーザーアカウント
自動更新と再起動の期限を指定する	有効にして、期限を 7 日、猶予期限を 0 日を指定する	Windows Update が配信 7 日後に強制的に適用されます	コンピューターの構成>管理テンプレート>Windows Update>エンド ユーザー エクスペリエンスの管理

設定項目	設定値	説明	設定のパス
パスワードの長さ	8 を指定する	パスワードを 8 文字以上に強制します	コンピューターの構成>Windows の設定>セキュリティの設定>アカウントポリシー>パスワードのポリシー
パスワードの最終文字数の監査	8 を指定する	8 文字未満のパスワードが設定されたとき、監査イベントをログを記録します	コンピューターの構成>Windows の設定>セキュリティの設定>アカウントポリシー>パスワードのポリシー
実行可能ファイルの規則	既定の規則の許可	すべてのアカウントで Program Files フォルダ配下のファイルの実行を許可、すべてのアカウントで Windows フォルダ配下のファイルの実行を許可、および管理者グループアカウントですべてのファイルの実行を許可、が設定されます 設定後、AppLocker のプロパティで[実行可能ファイルの規則]を構成済みにチェックしてください	コンピューターの構成>Windows の設定>セキュリティの設定>アプリケーションの制限ポリシー>AppLocker
実行可能ファイルの規則	署名されたファイルの許可	信頼された証明書で署名されたファイルの実行の許可が設定されます	コンピューターの構成>Windows の設定>セキュリティの設定>アプリケーションの制限ポリシー>AppLocker
パッケージアプリの規則	既定の規則の許可	署名されたすべてのパッケージアプリ実行を許可、が設定されます 設定後、AppLocker のプロパティで[パッケージ アプリの規則]を構成済みにチェックしてください	コンピューターの構成>Windows の設定>セキュリティの設定>アプリケーションの制限ポリシー>AppLocker
ウィジェット	ウィジェットを許可する	デバイスでウィジェット機能を使用できるかどうかを指定します	コンピューターの構成>管理用テンプレート

設定項目	設定値	説明	設定のパス
			>Windows コンポーネント>ウィジェット

※AppLocker を動作させるため、Application Identity サービスの自動起動を設定しています。

ユーザーの構成のグループポリシー

非管理者グループポリシーボブジェクトおよび管理者グループポリシーオブジェクトに対して設定しています。非管理者グループポリシーオブジェクトの設定はすべての標準アカウントを含むすべての非管理者アカウントに適用されます。管理者グループポリシーオブジェクトの設定はすべての管理者アカウントに適用されます。

※初期設定アプリで作成される専用標準アカウントは非管理者アカウントに含まれます。

設定項目	設定値	説明	設定のパス	非管理者	管理者
デスクトップ上のすべてのアイコンを非表示にして無効にする	有効	デスクトップのすべてのアイコンとコンテキストメニューが非表示になります	ユーザーの構成>管理テンプレート>Windows コンポーネント>デスクトップ	o	x
ログオン	%ProgramFiles%¥RICOH¥RicohCollaborationBoard¥tools¥startup.bat c:¥vender-tools¥script¥logon.bat c:¥vender-tools¥script¥logon.ps1	サインイン時に登録したスクリプトが実行されます startup.bat が実行さると、RCB アプリが自動起動します **logon.bat と logon.ps1 は RCB のシステム設定用のため、編集・削除しないでください**	ユーザーの構成>Windows の設定>コントロールパネル>スクリプト(ログオン/ログオフ)	o	x
ログオフ	c:¥vender-tools¥script¥logoff.bat c:¥vender-tools¥script¥logoff.ps1	サインアウト時に登録したスクリプトが実行されます **logoff.bat と logoff.ps1 は RCB のシステム設定用の**	ユーザーの構成>Windows の設定>コントロールパネル>スクリプト(ログオン/ログオフ)	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
		ため、編集・削除しないでください			
特定のテーマを読み込む	c:¥vender-tools¥themes¥rcb.theme	専用の背景画像が適用され、サウンド設定がなしになります	ユーザーの構成>管理テンプテート>コントロールパネル>個人用設定	o	o
パスワードの変更を削除する	有効	セキュリティオプション画面でパスワードの変更を実行できなくなります	ユーザーの構成>管理テンプレート>システム>Ctrl + Alt + Del オプション	o	x
コンピューターのロックを削除する	有効	セキュリティオプション画面でコンピューターのロックを実行できなくなります	ユーザーの構成>管理テンプレート>システム>Ctrl + Alt + Del オプション	o	x
ログオフを削除する	有効	セキュリティオプション画面でログオフを実行できなくなります	ユーザーの構成>管理テンプレート>システム>Ctrl + Alt + Del オプション	o	x
トースト通知をオフにする	有効	アプリケーションはトースト通知を表示できません	ユーザーの構成>管理テンプレート>タスクバーと[スタート]メニュー>通知	o	x
タイル通知をオフにする	有効	アプリケーションおよびシステムの機能はスタート画面のタイル	ユーザーの構成>管理用テンプレート>タスクバーと[ス	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
		およびタイルバッジを更新できません	タート]メニュー>通知		
ロック画面のトースト通知をオフにする	有効	アプリケーションおよびシステムの機能でロック画面にトースト通知を表示できません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー>通知	o	x
通知のミラーリングをオフにする	有効	アプリケーションおよびシステムからの通知は他のデバイスにミラーリングされません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー>通知	o	x
[コンピューターの検索]リンクを削除する	有効	スタートメニューの検索結果にコンピュータのリンクを含めません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]に[別のユーザーとして実行]を表示する	無効	[スタート]アプリケーションバーで[別のユーザーとして実行]を非表示にします	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[おすすめ]セクションを削除する	有効	[スタート]メニューの[おすすめ]セクションに追加できないようにします	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[お気に入り]を削除する	有効	[スタート]メニューの[お気に入り]に追加できないようにします既定では[お気に入り]メニュー	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
		は[スタート]メニューには表示されません			
[スタート]メニューから[ゲーム]アイコンを削除する	有効	[スタート]メニューに[ゲーム]フォルダーへのリンクが表示されなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[コンピューターの装着解除]ボタンを削除する	有効	[コンピューターの装着解除]ボタンが削除され、ユーザーはコンピューターの装着を解除できなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[すべてのプログラム]を削除する	有効にして、**削除して設定を無効にする**を選択する	[スタート]メニューからすべてのアプリの一覧が削除されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[ダウンロード]リンクを削除する	有効	[スタート]メニューに[ダウンロード]フォルダーへのリンクが表示されなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[ドキュメント]を削除する	有効	[スタート]メニューそのサブメニューに[ドキュメント]アイコンが表示されなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[ネットワーク接続]を削除する	有効	[スタート]メニューで[ネットワーク接続] フォルダーを開くことはできなくなり、ユーザーは[ネットワーク接続]を実行できません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
[スタート]メニューから[ネットワーク]アイコンを削除する	有効	[スタート]メニューから[ネットワーク]アイコンが利用できなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[ピクチャ]アイコンを削除する	有効	[スタート]メニューから[ピクチャ]アイコンが利用できなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[ビデオ]リンクを削除する	有効	[スタート]メニューにビデオライブラリへのリンクが表示されなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[ファイル名を指定して実行]を削除する	有効	[ファイル名を指定して実行]が[スタート]メニューから削除されます [Win]キー+R キーを押下しても、[ファイル名を指定して実行] は表示できません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[ヘルプ]を削除する	有効	[スタート]メニューから[ヘルプ]が削除されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[ホームグループ]リンクを削除する	有効	[スタート]メニューにホームグループへのリンクが表示されません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
[スタート]メニューから[ミュージック]アイコンを削除する	有効	[スタート]メニューから[ミュージック]アイコンが利用できなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[よく使う]の一覧を表示または非表示にする	有効にして、**非表示**を選択する	"最も使用されている"リストが強制的に非表示になります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[既定のプログラム]を削除する	有効	[スタート]メニューから[既定のプログラム]が削除されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[検索]を削除する	有効	[スタート]メニューおよび[スタート]メニューを右クリックすると表示されるショートカットメニューから[検索]が削除されます また、ユーザーが Win キー)+F キーを押してもシステムからの応答はありません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[最近使ったファイル]を削除する	有効	[スタート]メニューから[最近使った項目]を削除します	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから[録画一覧]リンクを削除する	有効	[スタート]メニューに[録画一覧]ライブラリへのリンクが表示されなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
[スタート]メニューからピンされたプログラムを削除する	無効	[スタート]メニューに[ピンされたプログラム] の一覧が表示されます ユーザーは[スタート]メニューでプログラムを固定または固定解除できます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューからユーザーフォルダーを削除する	有効	[スタート]メニューにユーザーの保存フォルダーへのリンクが表示されなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューからユーザーのフォルダーを削除する	有効	[スタート]メニューのユーザー専用部分(上部)にあるフォルダーを非表示にします	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューからユーザー名を削除する	無効	[スタート]メニューにユーザー名ラベルが表示されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから共通プログラムグループを削除する	有効	ユーザーのプロファイルの項目のみが[プログラム]メニューに表示されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューから頻繁に利用するプログラムの一覧を削除する	有効	頻繁に利用するプログラムの一覧が[スタート]メニューから削除されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
[スタート]メニューに[インターネットの検索]リンクを追加する	無効	ユーザーが[スタート]メニューの検索ボックスで検索を行うときに[インターネットの検索]リンクは表示されません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューに[ファイル名を指定して実行]コマンドを追加する	無効	[ファイル名を指定して実行]コマンドは[スタート]メニューには表示されません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューに[ログオフ]を追加する	有効	[<ユーザー名>のログオフ]が[スタート]メニューに表示されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニューの[ログオフ]を削除する	無効	[<ユーザー名>のログオフ]が[スタート]メニューに表示されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[スタート]メニュー項目のバルーンヒントを削除する	有効	[スタート]メニューと通知領域のポップアップテキストを非表示にします	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[セキュリティとメンテナンス]のアイコンを削除する	有効	システム通知領域に[セキュリティとメンテナンス]のアイコンが表示されません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[検索結果の続きを表示]/[すべての場所の検索]リンクを削除する	有効	ユーザーが[スタート]メニューの検索ボックスで検索を行うときに、[検索結果の続きを表	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
		示]/[すべての場所の検索]リンクが表示されません			
[今すぐ会議]アイコンを削除します	有効	[今すぐ会議]アイコンがシステム通知領域に表示されません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[設定]メニューのプログラムを削除する	有効	[スタート]メニューの [設定]、[マイ コンピューター]およびエクスプローラーから、コントロールパネル、[プリンター]および[ネットワーク接続]が削除されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
[別のメモリ領域で実行する]チェックボックスを[ファイル名を指定して実行]ダイアログボックスに追加する	無効	[ファイル名を指定して実行]ダイアログボックスに	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニューに[別のメモリ領域で実行する]チェックボックスが表示されません	o	x
Windows Update へのリンクとアクセスを削除する	有効	ユーザーは Windows Update の Web サイトにアクセスできなくなります また、[スタート]メニューおよび Internet Explorer の[ツール]メニューから Windows Update のハイパーリンクが削除されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
Windows ストアアプリをタスクバーに表示する	無効	Windows ストアアプリはタスクバーに表示されません	ユーザーの構成>管理用テンプレー	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
			ト>タスクバーと[スタート]メニュー		
インストール時にアプリをスタートにピン留めする	無効	AppID によって一覧に含まれているアプリをインストールしたとき、[スタート]メニューにピン留めしません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
インターネットを検索しない	有効	[スタート]メニューの検索ボックスによるインターネットの履歴またはお気に入りの検索は行われなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
カスタマイズメニューをオフにする	有効	メニューはカスタマイズされません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
サインイン時にスタート画面ではなくデスクトップに移動する	有効	ユーザーはサインイン時に常にデスクトップに移動します	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
システム通知領域に時刻を表示しない	有効	システムの通知領域に時刻が表示されません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
スタートメニューから[最近追加されたもの]の一覧を削除する	有効	[スタート]メニューに[最近追加されたもの]の一覧は表示されません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x

設定項目	設定値	説明	設定のパス	非管理者	管理者
スタートメニューの[推奨事項]セクションから個人用 Web サイトのおすすめ候補を削除する	有効	[スタート]メニューの[推奨事項]セクションから個人用 Web サイトのおすすめ候補を削除します	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
スタートメニューのショートカットメニューを無効にする	有効	[スタート]メニュー内でのコンテキストメニューの呼び出しは無視されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
すべてのタスクバー設定をロックする	有効	ユーザーはタスクバーのコントロールパネルにアクセスできません また、タスクバー上のツールバーを、サイズ変更、移動、および整理することもできません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
タスクバーからの People バーを削除する	有効	People アイコンがタスクバーから削除され、対応する設定の切り替えがタスクバー設定ページから削除されます	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
タスクバーから固定されたプログラムを削除する	有効	固定されたプログラムはタスクバーに表示されません	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
タスクバーと[スタート]メニューの設定を変更できないようにする	有効	ユーザーはタスクバーの[プロパティ]ダイアログボックスを開くことができなくなります	ユーザーの構成>管理用テンプレート>タスクバーと[スタート]メニュー	o	x
ユーザーに[スタート]からアプリケーションをアン	有効	ユーザーは[スタート]からアプリをアンインストールできません	ユーザーの構成>管理用テンプレー	o	x

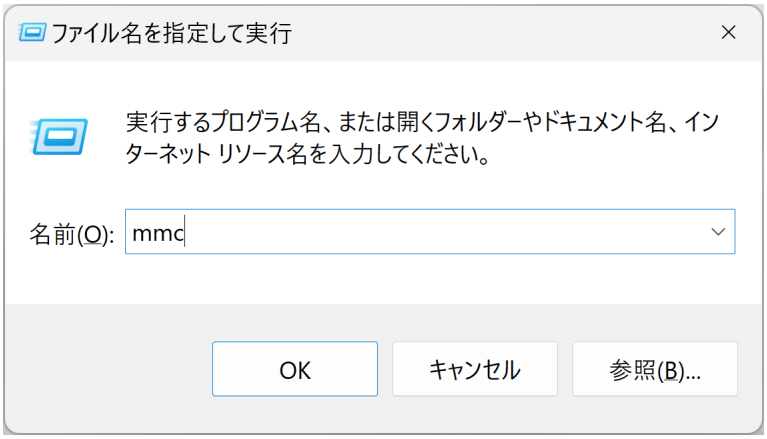
設定項目	設定値	説明	設定のパス	非管理者	管理者
インストールさせないようにする			ト>タスクバーと[スタート]メニュー		
設定ページの表示	有効にして、下記設定値を指定する showonly: regionlanguage- setdisplaylanguage; regionformatting;bluetooth; connecteddevices; camera; pen;printers;devices-touch	設定アプリでは以下のページのみ使用可能になります 表示言語の設定、リージョン、Bluetooth、接続されたデバイス、カメラの設定、ペンとWindows Ink、プリンターとスキャナー、Touch	ユーザーの構成> 管理用テンプレート>コントロールパネル	o	x
Microsoft Edge を閉じるときに閲覧データを消去する	有効	Microsoft Edge を終了するたびにすべての閲覧データが削除されます 閲覧データには、フォームやパスワードに入力した情報が含まれています またアクセスした Web サイトで入力した情報も含まれています	ユーザーの構成> 管理用テンプレート>Microsoft Edge	o	x
Microsoft Edge を閉じるときに、キャッシュされた画像とファイルを消去する	有効	Microsoft Edge を終了するたびに、キャッシュされた画像とファイルが削除されます	ユーザーの構成> 管理用テンプレート>Microsoft Edge	o	x
パスワード マネージャーへのパスワードの保存を有効にする	無効	ユーザーは Microsoft Edge でパスワードを保存できません	ユーザーの構成> 管理用テンプレート>Microsoft Edge>パスワードマネージャーと保護	o	x

※o：該当 / X：非該当

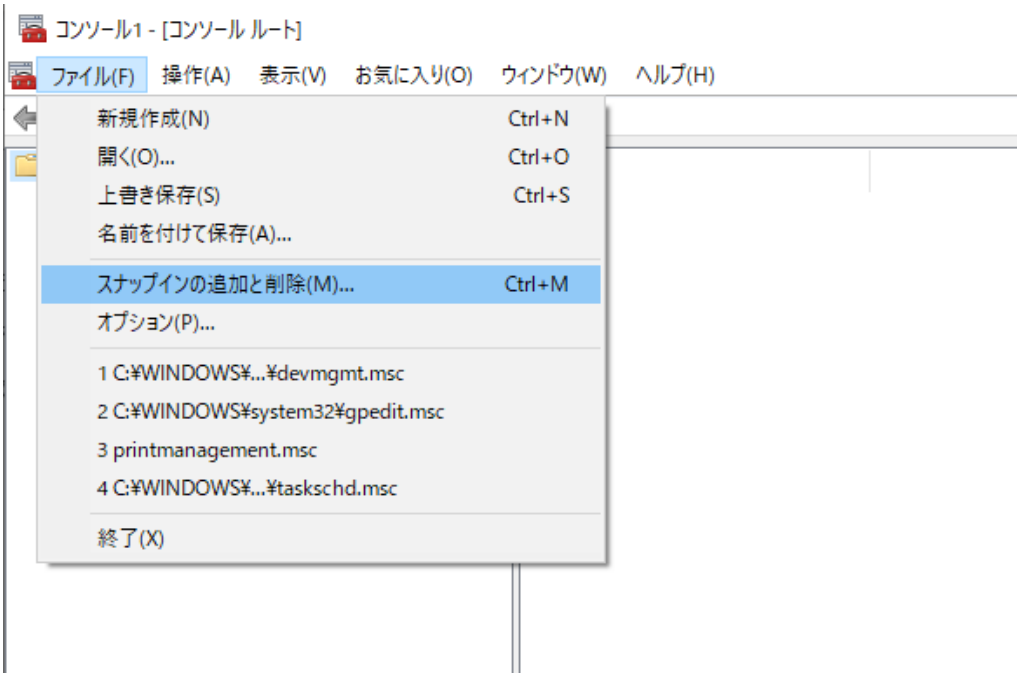
8.3. グループポリシーの設定方法

■グループポリシーエディターを開く■

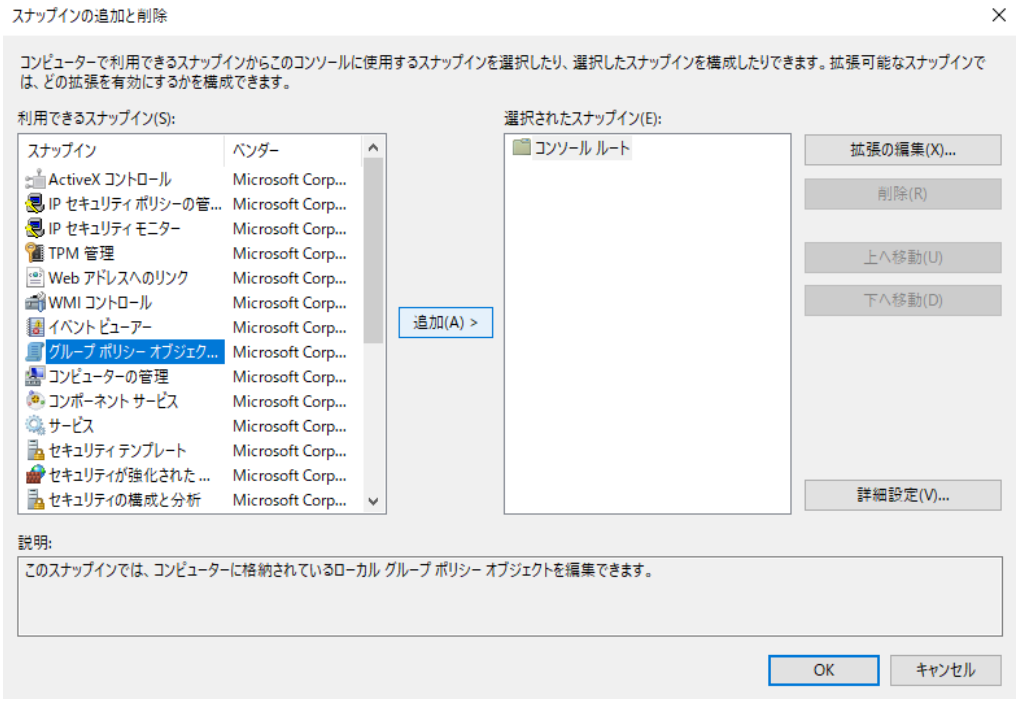
1. 管理者アカウントにサインインする。
2. Win キーと r キーを同時押しし、[ファイル名を指定して実行]を開く。
3. [mmc]と入力して OK を押し、管理コンソールを開く。（この際、ユーザーアカウント制御のダイアログが表示された場合は[はい]を押す）



4. 管理コンソールで[ファイル]>[スナップインの追加と削除]を押す。

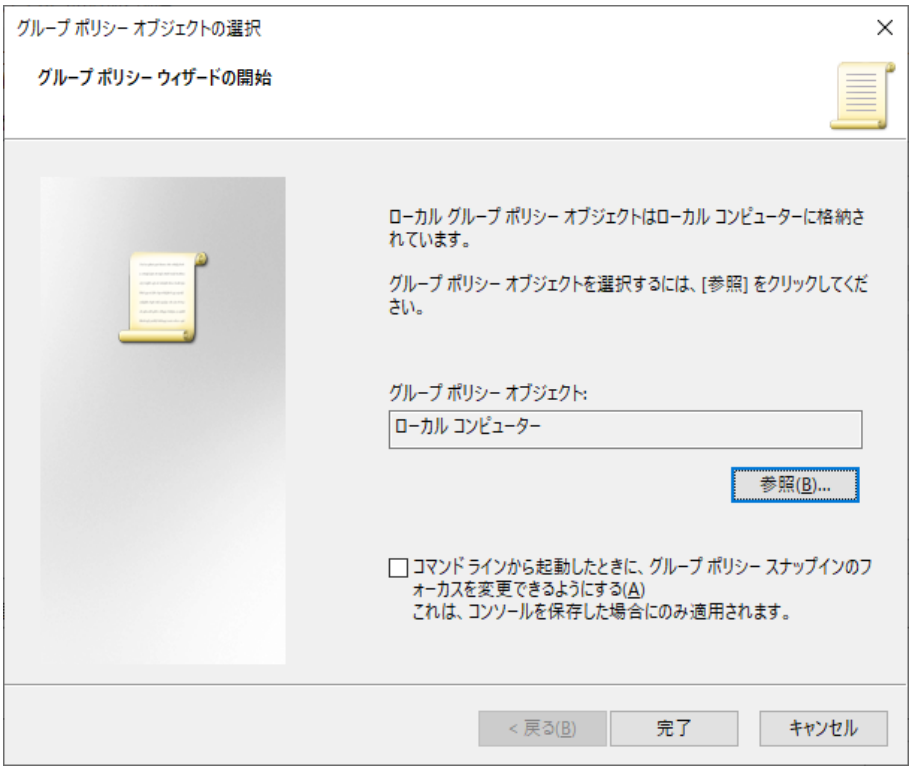


5. [グループポリシーオブジェクト]を選択し、[追加]を押す。



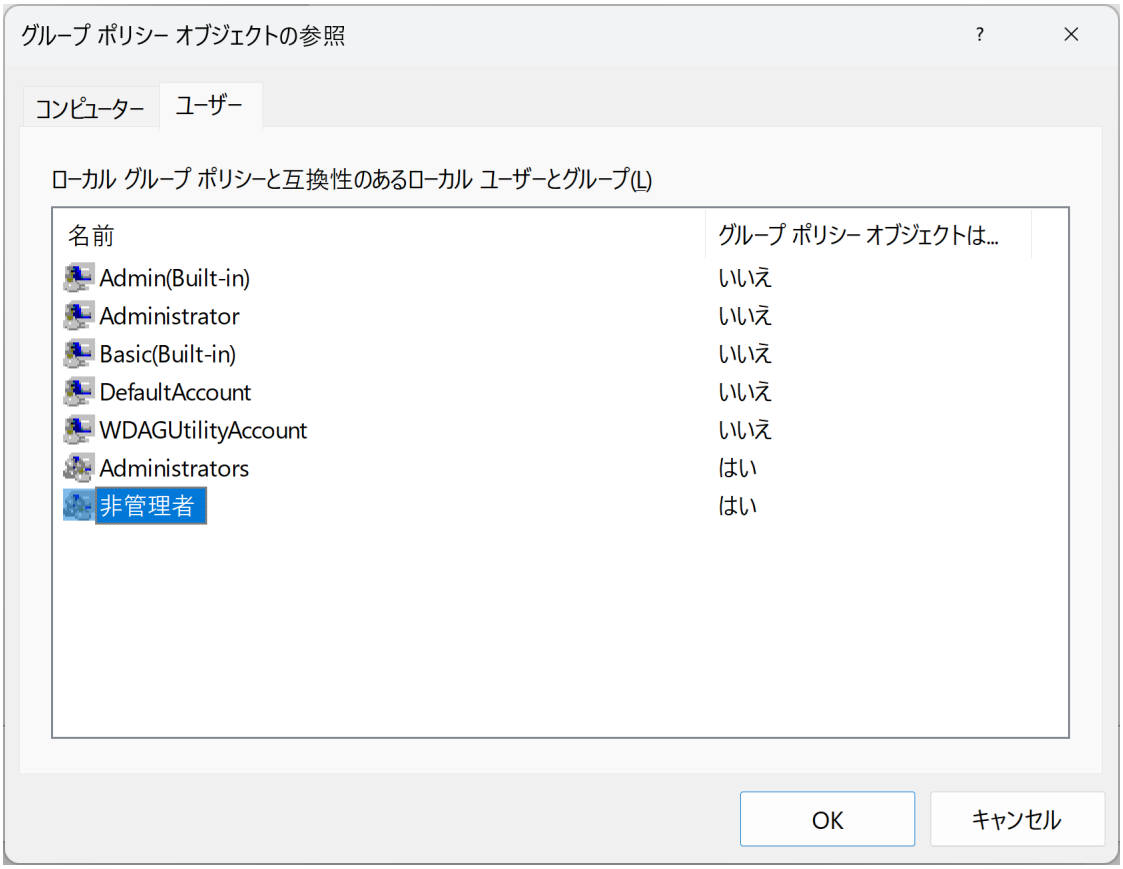
6. ①コンピューターの構成を変更する場合：

[グループポリシーオブジェクトの選択] で[ローカルコンピューター]が選択された状態のまま[完了]を押す。

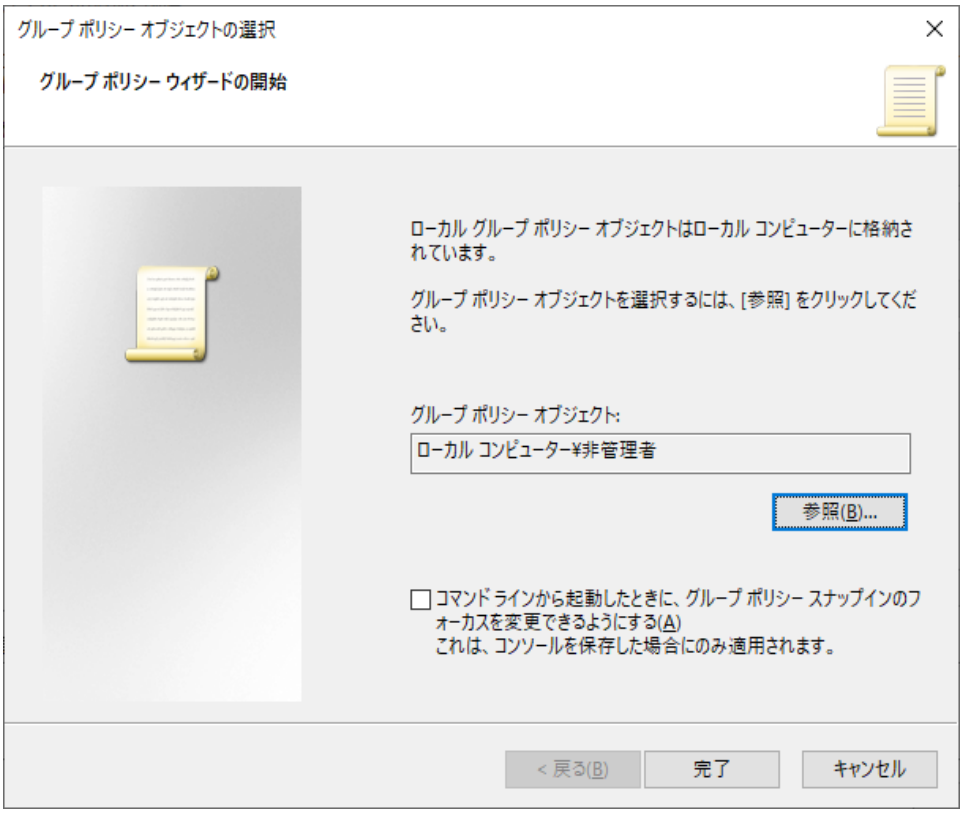


②ユーザーの構成を変更する場合：

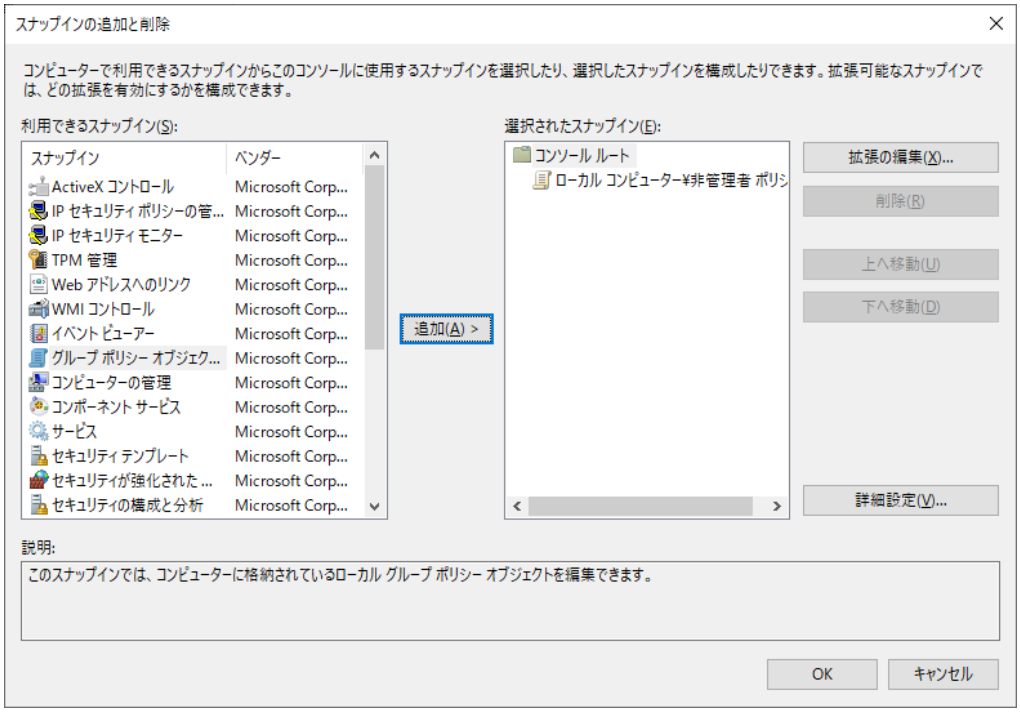
[グループポリシーオブジェクトの選択]で[参照]を押し、[ユーザー]タブの[非管理者]を選択し、[OK]を押す。



[完了]を押す。

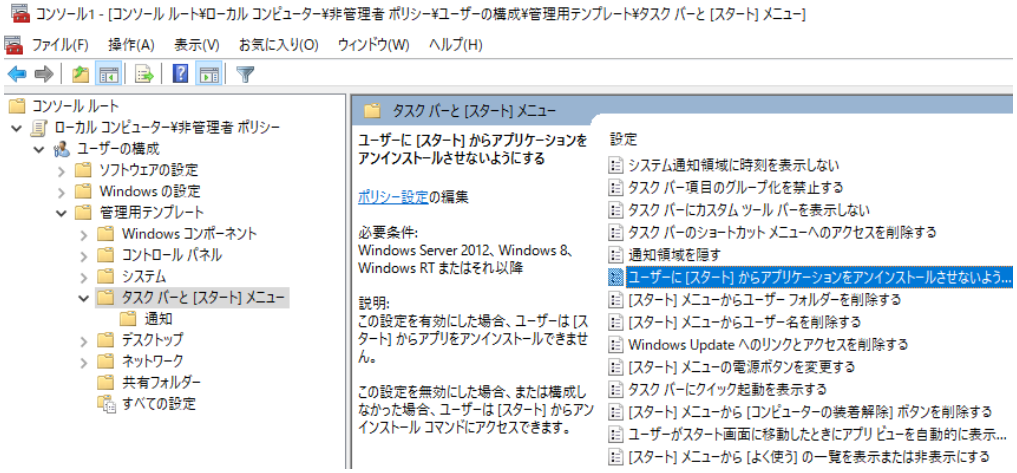


7. [OK]を押す

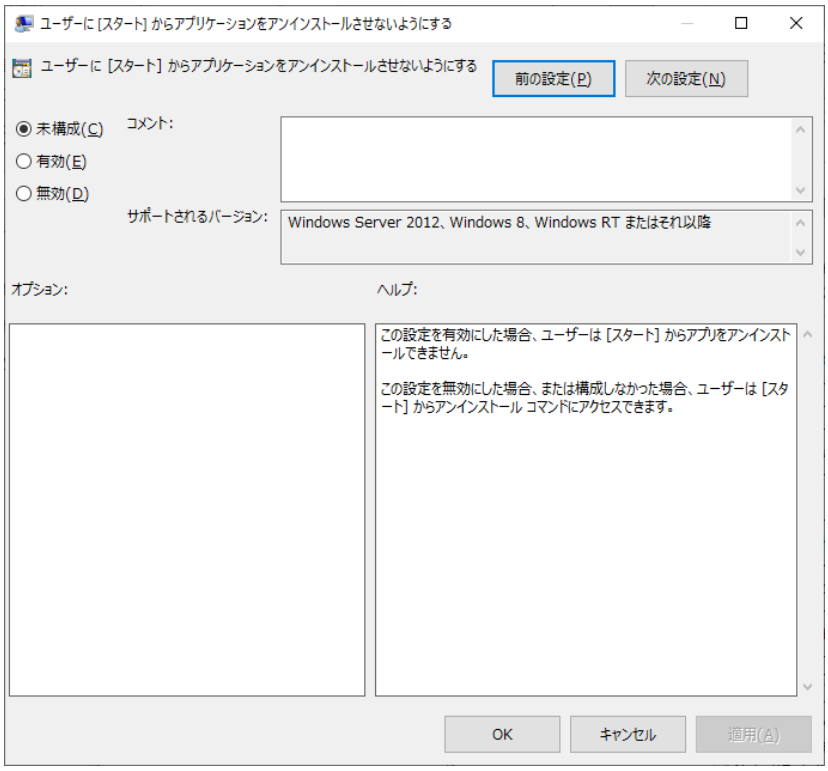

スナップインの追加と削除
コンピューターで利用できるスナップインからこのコンソールに使用するスナップインを選択したり、選択したスナップインを構成したりできます。拡張可能なスナップインでは、どの拡張を有効にするかを構成できます。
利用できるスナップイン(S):
スナップイン
ベンダー
ActiveX コントロール Microsoft Corp...
IP セキュリティ ポリシーの管... Microsoft Corp...
IP セキュリティ モニター Microsoft Corp...
TPM 管理 Microsoft Corp...
Web アドレスへのリンク Microsoft Corp...
WMI コントロール Microsoft Corp...
イベント ビューアー Microsoft Corp...
グループ ポリシー オブジェク... Microsoft Corp...
コンピューターの管理 Microsoft Corp...
コンポーネント サービス Microsoft Corp...
サービス Microsoft Corp...
セキュリティ テンプレート Microsoft Corp...
セキュリティが強化された ... Microsoft Corp...
セキュリティの構成と分析 Microsoft Corp...
追加(A) >
選択されたスナップイン(E):
コンソール ルート
ローカル コンピューター¥非管理者 ポリシ
拡張の編集(X)...
削除(R)
上へ移動(U)
下へ移動(D)
詳細設定(V)...
説明:
このスナップインでは、コンピューターに格納されているローカル グループ ポリシー オブジェクトを編集できます。
OK
キャンセル

■グループポリシーを変更する■

1. 任意のグループポリシー設定を開く。



2. 任意の設定に変更する。



※注意点

設定値を持つグループポリシー設定においては、一度未構成/無効にすると設定内容が消えてしまうため、元に戻す際に備えて設定値を控えておくことを推奨する。

3. 管理コンソールを終了する。（終了時に保存ダイアログが表示されるが、保存は不要）

8.4. 専用アカウントについて

RICOH Collaboration Board では下記 2 つの専用アカウントを用意しています。専用管理者アカウントは出荷時の状態で作成済みです。専用標準アカウントは初期設定アプリを使って作成することができます。専用標準アカウントを作

成すると自動的に自動サインイン設定も適用されるため、電源をいれるだけですぐに機器を使うことができます。

アカウント名	グループ	説明
Admin(Built-in)	Administrators	管理者グループポリシーオブジェクトの設定が適用されます。
Basic(Built-in)	Users	非管理者グループポリシーオブジェクトの設定が適用されます。 自動サインインします。

補足：Windows で使用するアカウントのセキュリティ上の脅威と留意事項

RICOH Collaboration Board では使いやすくご利用いただける専用標準アカウントを作成する初期設定アプリを提供しています。専用標準アカウントではいくつかの機能をグループポリシーで制限していますが、セキュリティの向上を目的にしておりません。グループポリシーの変更は、お客様の判断と責任において実施してください。

また、RICOH Collaboration Board では基本的に専用標準アカウントでの使用を想定しておりますが、通常の標準アカウント（お客様が追加で作成したアカウント）、および共有 PC モードで使用するゲストアカウントでの使用も想定しています。使用するアカウント毎の主なセキュリティ上の脅威と留意事項を以下に記載します。

想定脅威	専用標準アカウント	標準アカウント（個人毎にサインイン）	共有 PC モード	留意事項
機器に保存したファイルを他のユーザーに閲覧・改ざんされる。 各種履歴などの情報を他のユーザーに閲覧される。	該当	非該当	非該当	ファイルを保存する場合は USB メモリ等に保存し、機器本体に保存しない。 ブラウザ等で個人認証することは避ける。もし履歴に残してしまった場合は履歴を削除する。
悪意のあるアプリを配置/実行され、機器上で操作した内容が漏洩・改ざんされる。	該当	該当	非該当（利用開始直前にサインインすることで非該当となる）	Windows 標準のウイルス対策ソフト、およびグループポリシー（AppLocker）による実行可能条件の制限により、基本的な対策は実施済み。さらなる対策としては、悪意のあるアプリが起動されないようにするため、実行可能なアプリケーションを AppLocker 使ってさらに制限する。（既定以上に制限した場合はサードパーティ製アプリなどに影響する可能性もあるため、管理

想定脅威	専用標準アカウント	標準アカウント（個人毎にサインイン）	共有 PC モード	留意事項
				者の責任において実施すること） 実行をトレースするため Windows のログを監査することも有効だが、「誰が」までトレースするには個人毎にサインインする必要がある。

8.5. システムの復元機能について

Windows OS では、何らかの原因でシステムの動作が不安定になった場合、システムの復元機能を使用することで安定動作していた状態に戻すことができます。ここでは、RICOH Collaboration Board でのシステムの復元の使い方について説明します。なお、システムの復元の詳細は Microsoft 社の技術情報などを参照してください。

RICOH Collaboration Board では出荷時の状態でシステムの復元機能を有効にしています。システムの復元機能は Windows OS の[システムのプロパティ]の[システムの保護]で操作します。[システムの保護]タブ内の[システムの復元…]ボタンを押下することで、作成されている復元ポイントの状態にシステムを戻すことができます。操作方法の詳細は Microsoft 社の技術情報などを参照してください。なお、[システムのプロパティ]ダイアログは、Windows OS の設定画面から開くか、管理者権限でターミナルを起動し、sysdm.cpl を実行することで表示できます。また、[設定]>[システム]>[回復]から[PC をリセットする]を実行することで、Windows OS 自体を再インストールすることができますが、本機能を実行した場合、製品保証が失効されるため、絶対に実行しないでください。

なお、Windows OS は下記のイベントの発生時に復元ポイントを作成します。

1．システム復元に準拠したインストーラーを使用してアプリケーションをインストールしたとき
　※RICOH Collaboration Board のシステム更新も対象になります
2．Windows Update を適用したとき
3．システムの保護タブで復元ポイントを手動作成したとき

9. 商標

- Windows®、Microsoft 365®、OneDrive®、Outlook®は Microsoft 社の米国および、その他の国における商標または登録商標です。
- Box は Box, Inc.の商標または登録商標です。
- Amazon Web Services、AWS、Powered by AWS ロゴ、[およびかかる資料で使用されるその他の AWS 商標] は、Amazon.com, Inc. またはその関連会社の商標です。
- InsightVM は.Rapid7 社の米国その他の諸国における商標または登録商標です。

変更履歴

Rev.	改版日	改版内容
1.0	2024.07.31	初版作成
1.1	2025.01.23	RICOH Collaboration Board V1.1 の内容を反映 グループポリシーの変更方法を追記
1.2	2025.03.07	お客様環境から Microsoft Edge エンドポイントへの通信を追加
1.2.1	2025.04.21	無線 BYOM 機能（Omni）のセキュリティに関する記載を追加 ログアップロード機能を利用するために必要な通信先ホストを追加 Add-on for MS365 を利用するために必要な通信先ホストを追加