

管理者向け：通信・認証・更新

法人向け導入検討ガイドの別紙 / v1.18.3

通信経路

Windowsアプリ同士は、操作するPCから接続先PCのTCPポートへ直接接続します。既定はTCP 55510で変更できます。接続先はIPv4の全インターフェースで待ち受け、標準設定ではLAN/VPN向けの接続元アドレス範囲を検査します。これは利用者本人を識別する仕組みではありません。初期状態では待ち受けはオフです。管理者が許可する端末・経路に通信を絞ってください。

ClearRemote自身の中継サーバー・オンラインライセンス認証はありません。社外からは既存VPN等の経路が別途必要です。VPN製品側の外部通信・中継の有無はその構成に依存します。インターネットへのポート開放を導入手順にはしません。

認証と暗号化

Windowsアプリ間ではECDH P-256で鍵交換し、AES-256-CBCとHMAC-SHA256で通信を保護します。パスワードは任意で初期値は空です。**法人評価では接続用パスワードを設定してください。** 未設定時にも通信は暗号化されますが、暗号化だけでは接続相手の本人確認になりません。パスワード設定時は双方がその知識を検証します。

ブラウザ接続は同じポートのHTTP/WebSocketで、**通信は暗号化されません。** ブラウザ用パスワードは別設定で、空ならブラウザ接続は無効です。ブラウザを使う場合はVPNなどで通信路を保護してください。本紙の初回評価はWindowsアプリ同士を対象にします。

更新と配布元の確認

v1.18.3はコード署名付きとして10月1日に公開されています。署名があってもSmartScreen等の警告が出ない保証にはなりません。取得元、署名、公開ページのSHA-256を管理者が確認してください。

更新は指定したフォルダ（既定はexeの起動元。共有フォルダも可）にある更新マニフェストとexeを使います。マニフェストの署名とexeのSHA-256を確認します。自動更新の設定があります。インターネットから最新版を自動取得する仕組みではなく、管理者が公開版を確認して配布フォルダへ置く運用です。Windowsのコード署名と更新マニフェストの署名は別のものです。

導入時の確認欄

- ☐ 操作されるPCだけ待ち受けを有効化し、接続用パスワードを設定した。
- ☐ 接続先ごとにWindows・他社製ファイアウォールを確認した。VPNの変動IPを単一の一時IPに固定していない。
- ☐ 社内の利用ルールに従い、クリップボード・ファイル転送の利用可否を決めた。
- ☐ 更新フォルダの書込担当と配布の承認手順を決めた。
- ☐ 実際のCAD等で操作感、使用許諾、フォルダ転送を評価した。

フォルダ転送は相手→手元がコピー＆貼り付け（空フォルダも対応）、手元→相手がドラッグ＆ドロップ（空フォルダは非対応）。1回約4,000件・深さ32まで。OneDriveオンライン専用ファイルやNAS越しの大きなフォルダは、この版の実機確認が未完了です。

本紙は導入審査の補助です。SSO・MFA・集中管理・監査証跡を備えるとの保証はしていません。通常の動作ログはありますが、監査要件への適合は別に確認が必要です。VPN設定・個別導入作業はお客様の管理担当者の範囲です。

問い合わせ：clearremote@shimadagiken.jp