

ネットワーク接続等仕様書

佐賀県情報系ネットワークへの接続については、以下の仕様を満たすこと。

1	佐賀県情報系ネットワーク上でネットワークプリンタ、ネットワークスキャナ及びネットワークファクスとして機能すること。
2	別途サーバ機器を必要とせずに、佐賀県情報系ネットワーク上のパソコンからの印刷ができること。
3	・別途サーバ機器を必要とせずに、複合機でスキャンしたデータを佐賀県情報系ネットワーク上の共有フォルダ等に保存できること。 ・ネットワークスキャナの設定を複合機に行うこと。
4	・別途サーバ機器を必要とせずに、ネットワークからファクス送信できること(複合機の直接操作によるファックス送信と同等機能)。 ・ネットワークよりファックス送信完了時、送信完了結果を指定したメールアドレス宛てに通知できること。 ・受信したファクスは、佐賀県情報系ネットワーク上の共有フォルダ等にファイルとして保存できること。 - また、指定したメールアドレス宛てにFAX受信したことを通知できること。
5	複合機で取り扱う各種データ(プリンタ、スキャナ利用時等)についてアクセス制御及び通信時の暗号化ができること。
6	複合機の設定(複合機を識別するための複合機名(例:A5001)、IPアドレス、スキャンデータの保存先等)は、現行複合機の設定を踏襲すること。
7	・職員用端末のドライバ更新について、下記要件に対応可能なツール及び手順書を作成し、配布することで対応を行うこと。 ○現行複合機のドライバ削除 →削除対象のドライバ情報は県から提示を行う。 ○納入複合機のドライバインストール →職員用端末には一律、納入複合機の種類分のプリンタドライバ、納入通知書用プリンタドライバ、FAXドライバのインストールを想定している。 ・更新作業時は、問い合わせ等に対応できる体制を構築すること。
8	・複合機名のテプラの作成、複合機への貼付けを行うこと。 ・複合機名の一覧は県から提示を行う。
9	・各機能(プリントアウト(納入通知書含む)/スキャン/FAX等)の操作説明のマニュアルを提供すること。 ・ほか、別途県が職員用端末や共有フォルダ等の運用を委託している業者が必要とする手順、マニュアル等を提供すること。詳細は県と協議のうえ、決定することとする。
10	・セキュアプリント(sesame: セサミ)に対応している複合機、ドライバであること。 ・現行複合機において、セキュアプリント用のカードリーダーが取り付けられている場合は、該当カードリーダーを納入複合機に移設すること。複合機への取り付け方法は現行の取り付け方法を踏襲すること。
11	県が提示する複合機管理用の台帳に必要情報(複合機名、シリアル番号、MACアドレス等の機器情報等)を記入し納品物として納品すること。

【仕 様】

区 分	項 目	仕 様 内 容
プリンタ	対応OS	Windows 11 Windows Server 2019
	ネットワークプロトコル	TCP/IP (IPv4,IPv6)
	プリンタ用インターフェース	Ethernet 1000BASE-T/100BASE-TX/10BASE-T USB2.0以上
	解像度	600dpi×600dpi以上の解像度を有し、かつ、高精細化技術等により、2400dpi×600dpi以上若しくは1200dpi×1200dpi以上相当の解像度が実現できること
	その他	PDFファイル上のOCR-Bフォントの印刷が可能であること PDFファイル上のEAN128規格バーコードのイメージデータの印刷が可能であること
スキャナ	対応OS	Windows 11 Windows Server 2019
	ネットワークプロトコル	TCP/IP (IPv4,IPv6)
	スキャナ用インターフェース	Ethernet 1000BASE-T/100BASE-TX/10BASE-T
	出力フォーマット	モノクロ: TIFF,PDF グレースケール/カラー: TIFF,JPEG,PDF
	ファイル送信(パソコン保存)	対応プロトコル: SMBv2以上,FTP 出力フォーマット: TIFF,JPEG,PDF
	メール送信	対応プロトコル: SMTP 出力フォーマット: TIFF,JPEG,PDF
	読取解像度	600dpi以上の読取解像度をサポートし、かつ、複数の読取解像度に対応すること(例: 600dpi,400dpi,300dpi,200dpi 対応など)
	その他	TWAIN対応
認証機能・セキュリティ	本体認証	複合機に登録したユーザー情報による簡易な認証機能を有すること
	外部認証	以下の認証機能を有し、佐賀県情報系ネットワーク上のActive Directoryに接続して認証が可能な機能を有すること ・Windows認証(Kerberos認証) ・LDAP認証 なお、将来的にICカードを利用した認証について拡張が可能なこと
	通信データのセキュリティ	以下の暗号化通信に対応すること ・SSL ・IPsec ・SNMPv3
	蓄積データのセキュリティ	・記憶装置に蓄積されたデータを上書き消去できること ・記憶装置に蓄積されたデータを暗号化できること
	スキャン時のセキュリティ	パスワード設定や暗号化したPDF文書を作成できること
	プリント時のセキュリティ	本体に一旦蓄積したデータを、利用者が設定したパスワードを入力することによってプリントできること
	不正コピー防止	プリント時に特殊な紋様等を埋め込み、複写時に埋め込んだ紋様等を浮かび上がらせることができること
	ファクス誤送信防止	・宛先2回(確認)入力対応 ・宛先リスト等からの選択入力対応 等
そ の 他	各インターフェースのポート数	ネットワークインターフェース:1ポート以上 USBインターフェース:1ポート以上