Fiery FS600 Pro/FS600 servers

Fiery Security White Paper

© 2024 Fiery, LLC. 本書に記載されている情報は、本製品の『法律上の注意』の対象となります。

45255438

2024 年 8 月 1 日

目次

本文書の概要

本文書は、セキュリティテクノロジーと機能を Fiery FS600 Pro/FS600 servers で実装する方法について詳しく記載するほか、ハードウェアセキュリティ、ネットワークセキュリティ、アクセス制御、オペレーティングシステム、およびデータセキュリティについて説明します。本文書の目的は、カスタマーが Fiery プラットフォームセキュリティテクノロジーを独自のポリシーと組み合わせて、特定のセキュリティ要件を満たせるようにサポートすることです。

用語の表記法

本書では、Fiery FS600 Pro/FS600 servers、プリンターおよび Fiery アプリケーションを参照するために、次の用語が使用されます。

用語/表記法	説明
Fiery server	Fiery FS600 Pro/FS600 servers
プリンター	プリンター、複写機、デジタルプレス、プレスまたは出力デバイス
Configure	Fiery Configure
Command WorkStation	Fiery Command WorkStation
WebTools	Fiery WebTools
QuickTouch	Fiery サーバーの LCD パネルで動作する Fiery QuickTouch ソフトウェア

FIERY のセキュリティ指針

FIERY は、セキュリティが世界中の企業やビジネスにとって、最も関心の高い問題の 1 つであることを理解しています。当社の製品は、会社資産を保護することを目的とする改善されたセキュリティ機能で頻繁に強化されています。 Fiery servers は、保管、輸送および処理の際にシステムデータを保護するために、セキュリティを中核として設計・製造されています。

グローバルなパートナーおよびサプライヤーと緊密に連携し、脅威の進化に対応するソリューションを提供してお客様を継続的にサポートします。システム全体のセキュリティを強化するために、Fiery セキュリティ機能を自社のセキュリティポリシーと組み合わせて、業界のベストプラクティス（セキュアパスワードや強固な物理的セキュリティ手順など）に従うことをお勧めします。

セキュリティに対する FIERY のアプローチ

FIERY セキュリティ機能は、次の 5 つの原則を指針としています。

- **データセキュリティ**：処理中、送信中または保存中（静止時）のデータが不正に公開されないこと。
- **使用可能性**：不正に操作されることのない、意図したとおりのパフォーマンスを実現する。
- **アクセス制御**：認可済みユーザーへのサービス運用妨害（DoS）が発生しないこと。
- **IT フレンドリーなメンテナンス**：セキュリティアップデートの自動通知と自動ダウンロード
- **コンプライアンス**：業界規制およびセキュリティフレームワークをサポートすること。

Fiery ソフトウェアセキュリティのアップデート

このセクションでは、Fiery server ソフトウェアセキュリティアップデート処理の概要について説明します。Microsoft® Windows™ OS セキュリティの脆弱性については、Microsoft が直接処理し、使用可能になった Windows アップデートを提供するため、記載されていません。マザーボード、プロセッサー、BIOS などのコア Fiery ハードウェア部品に影響を及ぼす可能性があるセキュリティ上の問題や脆弱性については、FIERY はメーカーと密接に連携して、必要なセキュリティアップデートを入手します。

- FIERY は、サイバーセキュリティおよびインフラストラクチャセキュリティ機関（CISA）が毎週更新する US-CERT Cyber Security Bulletin を確認しています。このセキュリティ情報では、アメリカ国立標準技術研究所（NIST）の脆弱性情報データベース（NVD）に記録されている新しい脆弱性の概要が紹介されています。脆弱性は、共通脆弱性識別子（CVE）命名標準に準拠しており、共通脆弱性評価システム（CVSS）によって決定される重大度（高、中、低）に従って整理されています。
- FIERY は、各 Fiery server プラットフォームのセキュリティ修正プログラムをできる限り早く提供します。
- Fiery ソフトウェアセキュリティアップデートは、承認を得るために FIERY パートナーに提供されます。
- パートナーが承認すると、Fiery ソフトウェアセキュリティアップデートがダウンロード可能になります。
- Fiery server でオプションが有効になっている場合、Fiery システムアップデートはセキュリティアップデートをダウンロードしてインストールします。デフォルトでこのオプションが有効になっているため、有効のままにすることをお勧めします。

Fiery servers を最適に作動させるためには、適切なタイミングでソフトウェアをアップデートすることが極めて重要です。Fiery および Windows オペレーティングシステムにソフトウェアのセキュリティアップデートをインストールすることは、指定された印刷環境で Fiery servers の安全を維持するために重要です。

メモ：Fiery ソフトウェアアップデートは、不正な変更（マルウェアの挿入を含む）を防ぐために、Secure Hash Algorithm（SHA-2）を使用してデジタル署名が行われています。

Fiery server セキュリティ機能の設定

Fiery servers セキュリティ機能の大半は、Configure を使用して管理できます。Configure は FieryWebTools にあり、Fiery servers セキュリティ設定を Fiery 管理者が調整できます。Configure には管理者権限が必要であり、FieryCommand WorkStation からもアクセスできます。

Fiery server の設定の詳細については、セキュア Fiery サーバー設定に関するガイドライン（32 ページ）を参照してください。

ハードウェアセキュリティ

Fiery server ハードウェアのセキュリティでは、電源障害が発生した場合、またはストレージデバイスのデータが不正にアクセスされた場合に、データが失われないようにすることを目的としています。

揮発性メモリ

揮発性 RAM に書き込まれるデータは、電源がオンになっている間のみ使用できます。電源がオフになると、すべてのデータが削除されます。

詳細については、表の「揮発性メモリ」セクション（23 ページ）を参照してください。

不揮発性メモリとデータストレージ

Fiery server は、電源がオフになっても、Fiery server 上にデータを保持する不揮発性データストレージテクノロジをいくつか使用しています。このデータには、システムのプログラミング情報や、ユーザーデータなどが含まれます。

詳細については、表の「不揮発性メモリ」セクション（23 ページ）を参照してください。

フラッシュメモリ

フラッシュメモリには、自己診断およびブートプログラム（BIOS）、一部のシステム設定データが保存されます。フラッシュメモリは工場でプログラミングされ、FIERY が作成した特別なパッチをインストールする場合にのみ再度プログラミングすることができます。データが破損したり削除されたりすると、Fiery server が起動しなくなります。

CMOS

電池式 CMOS メモリは、Fiery server のマシン設定を保存するために使用されます。この情報は、機密情報や非公開情報ではありません。CMOS メモリが取り付けられている場合、ユーザーは、モニター、キーボードおよびマウスを使用して、Windows 10 ベースのサーバーでこれらの設定にアクセスできます。

NVRAM

Fiery server には、システムの動作に必要なファームウェアを格納した小さな NVRAM が幾つか搭載されています。これらのデバイスには、ユーザー非依存の汎用的な動作情報が含まれています。ユーザーは、これらのデバイスに含まれているデータにはアクセスできません。

ハードディスクドライブおよびソリッドステートドライブ

通常の印刷やスキャン操作の間、およびジョブ管理情報を作成している間に、イメージデータは、ハードディスクドライブおよびソリッドステートドライブのランダムな領域に書き込まれます。

キュー内のイメージデータやジョブは、Command WorkStation またはその他のキュー操作（プリンター LCD からの操作など）からユーザーが手動で削除することができます。**サーバーの初期化**コマンドを使用するか、または印刷済みジョブの数が許可されたパラメーターを超えると、イメージデータとオブジェクトも自動的に削除されます。印刷済みキューを無効にすると、印刷済みジョブも削除されます。

FIERY は、HDD ドライブからイメージデータを削除するために、セキュアイレース機能を提供します。Fiery のシステム管理者が Fiery セキュアイレースを有効にすると、選択された操作モードが適切なタイミングで実行されて、ハードディスクドライブ上のデータが安全に削除されています。現在、Fiery Secure Erase は HDD のみをサポートしています。ソリッドステートドライブ（SSD）の場合は、ドライブを廃棄する前に製造元にディスク消去オプションを確認してください。

メモ：セキュアイレースの詳細については、セキュアイレース（22 ページ）を参照してください。

物理ポート

ほとんどの Fiery サーバーで使用可能な一般的な物理ポート

Fiery のポート	機能	アクセス	アクセス制御
イーサネット RJ-45 コネクター	イーサネット接続	ネットワーク接続	Fiery の IP フィルタリングを使用してアクセス制御可能
プリンターのインターフェイスコネクター	印刷とスキャン	プリンターとの間の送受信専用	なし
USB ポート	USB デバイスの接続 システムソフトウェアのインストール	オプションのリムーバブルメディアデバイス用のプラグアンドプレイコネクター	• Windows ベースの Fiery サーバーの場合は、USB 印刷をオフにできます。 • USB ストレージデバイスへのアクセスは、Windows グループポリシーからオフにできます。 • USB ストレージは、Configure から無効にすることもできます。
光ファイバコネクター	10Gb イーサネット接続	ネットワーク接続	なし

ローカルインターフェイス

一部の Fiery servers では、ユーザーはタッチスクリーンディスプレイの Fiery QuickTouch ソフトウェア、または Fiery server に接続されているモニターから、Fiery NX Station モニターの Fiery 機能にアクセスできます。Fiery NX ステーションを使用した Fiery server 上でのセキュリティアクセスは、Windows のシステム管理者パ

スワードで制御されます。タッチスクリーンには、セキュリティリスクが生じる危険性のない限定的な機能のみが表示されます。

トラステッドプラットフォームモジュール（TPM）

FS600 Pro の Windows ベースの Fiery サーバーは、トラステッドプラットフォーム モジュール（TPM）をサポートしています。TPM は、オプションの有料セキュリティ機能を有効にするために使用されます。FS600 Pro の Fiery サーバーは、TPM を使用して、Fiery サーバーブートドライブ（C：ライブ）を暗号化/復号化します。また、ブートドライブの暗号化回復キーを安全に保存するためにも使用されます。Fiery TPM モジュールは、TPM 2.0 仕様、FIPS 140-2 およびコモンクライテリア標準に準拠しています。使用している Fiery DFE の Fiery セキュリティアップグレードキットと入手方法の詳細については、サービスプロバイダーに問い合わせてください。

Fiery ディスクドライブセキュリティキット

一部の Fiery servers は、セキュリティを強化するために、オプションのドライブドライブセキュリティキットに対応しています。このキットを使用すると、通常の運用時にはサーバーのドライブをシステムに固定しておき、Fiery server の電源を切った後はドライブを取り外して安全な場所に保管することができます。

Fiery XB サーバーの場合

ハードディスクドライブとソリッドステートドライブは、Fiery XB サーバーから取り外すことができます。ほとんどのハードディスクドライブとソリッドステートドライブは、RAID 設定でペアで使用されています。データ損失や新しいシステムソフトウェアのインストールを防ぐために、ドライブを元の場所に戻すことが重要です。

USB ポートをストレージに使用可能にする

Fiery servers の USB ポートには、マウス、キーボードまたは分光測色計を接続できます。USB ポートを無効にすると、ペンドライブなど外部 USB ストレージデバイスとの接続を防ぐことができます。このオプションは Configure で使用できます。無効にすると、外部 USB ドライブへのデータ書き込みを必要とする Fiery の機能は使用できません。

ネットワークセキュリティ

Fiery server には、ネットワークアクセスを制御および管理するためのさまざまなセキュリティ機能が含まれています。認可済みユーザーとグループのみが Fiery server にアクセスして、プリンターに印刷することができます。また、Fiery server は、指定された IP アドレスを使用したり、ネットワークポートやプロトコルを無効にしたりすることで、外部通信を制限または制御するように設定することができます。Fiery servers は、常に保護されたネットワーク環境に配置される必要があり、資格のある認定ネットワーク管理者が適切にアクセスの設定と管理を行う必要があります。

ネットワークポート

デフォルトでは、特定の Fiery サービスで使用されていないすべての TCP/IP ポートが無効になります。Fiery システム管理者は、ネットワークポートを有効/無効のどちらにするかを選択することができます。ネットワークポートを無効にした場合は、指定したポートを使用した外部接続がブロックされます。特定のポートが有効になっている場合、外部接続はそのポートを使用することで許可されます。

TCP/IP	UDP	ポート名	ポートを利用するサービス
20-21		FTP	FTP
80		HTTP	WebTools、IPP
135		MS RPC	Microsoft® RPC サービス SMB 関連のポイントおよび印刷サービスを提供するために、49152～65535 の範囲の追加ポートが開かれます。
137～139		NETBIOS	Windows 印刷
	161、162	SNMP	SNMP ベースのツール
	427	SLP	サービスロケーションプロトコル
443		HTTPS	WebTools、IPP/s
445		SMB/IP	SMB over TCP/IP
	500	ISAKMP	IPSec
515		LPD	LPR 印刷
631		IPP	IPP
3389		RDP	リモートデスクトップ（Windows Fiery サーバーのみ）
3702	3702	WS-Discovery	WSD WSD に対応したネットワークプリンターを検索します。このプリンターは Windows エクスプローラーでネットワークに表示され、ダブルクリックしてインストールできます。

TCP/IP	UDP	ポート名	ポートを利用するサービス
	4500	IPsec NAT トラバーサル	IPSec
	5353	マルチキャスト DNS（mDNS）	Bonjour
6310 8010 8021～8022 8090 9906 21030 50006～50025	9906	FIERY のポート	Command WorkStation、Fiery Central、Fiery SDK ベースのツール、Fiery Printer Driver、FieryWebTools、ダイレクトモバイル印刷、およびネイティブドキュメント変換
9100～9103		印刷ポート	ポート 9100

メモ：50006～50025 ポートは、Command WorkStation バージョン 6.2 以降で有効にされており、スタンドアロン Fiery server にインストールされています。

メモ：IPSec ポート（500 および 4500）は、FS600（Linux ベースの Fiery サーバー）でのみ設定できます。

Fiery パートナーが指定した特定のポートを除き、その他の TCP ポートは無効です。無効なポートを使用するサービスは、リモートアクセスができません。

Fiery システム管理者は、Fiery server が提供するさまざまなネットワークサービスを有効化および無効化することもできます。

IP フィルタリング

IP フィルタリングでは、定義された IP アドレスからの Fiery server への接続要求を許可または拒否します。システム管理者はデフォルトポリシーを定義して着信データパケットを許可または拒否することができます。また、接続要求を許可または拒否するために、最大 16 個の IP アドレスまたは範囲のフィルターを指定することもできます。

各 IP フィルター設定では、IP アドレスまたは IP アドレスの範囲と、対応するアクションを指定します。アクションが**拒否**された場合、指定されたアドレスに属すソースアドレスを持つパケットは破棄されます。アクションが**承認**されると、パケットは許可されます。

ネットワーク認証

SNMP v3

Fiery server は、最新の SNMPv3 標準をサポートしています。SNMPv3 の通信パケットは暗号化できるため、機密性やメッセージの完全性を確保できるほか、認証も行えます。

Fiery システム管理者は、低、中、高という 3 つの SNMP セキュリティレベルから選択できます。Fiery システム管理者は、SNMP トランザクションを許可する前に認証を要求したり、SNMP ユーザー名とパスワードを暗

号化したりすることもできます。ローカルのシステム管理者は、SNMP の読み書き用のコミュニティ名や、その他のセキュリティ設定を定義できます。

詳細については、推奨設定（32 ページ）を参照してください。

IEEE 802.1x

802.1x は、ポートベースのネットワークアクセス制御のための IEEE 標準プロトコルです。このプロトコルは、Fiery server が LAN および LAN 内のリソースにアクセスする前に、認証メカニズムを提供します。

このプロトコルを有効にした場合、Fiery server では、802.1x 認証サーバーに対する認証に EAP MD5 チャレンジ型認証、PEAP-MSCHAPv2 認証または EAP-TLS 認証を使用するように設定できます。

Fiery server は、起動時またはイーサネットケーブルが切断されて再接続されたときに認証を行います。

ネットワーク暗号化

Internet Protocol Security（IPsec）

IPsec は、IP プロトコルを利用するすべてのアプリケーションに対して、各パケットを暗号化し認証することでセキュリティ機能を提供します。

Fiery server は事前共有鍵による認証を使用して、他のシステムとの間で IPsec による安全な接続を確立します。

クライアントコンピューターと Fiery server との間で IPsec を利用した安全な通信が確立されると、印刷ジョブを含むすべての通信内容がネットワーク上で安全に送信されます。

HTTPS

Fiery server では、クライアントと異なるサーバーコンポーネント間を安全に接続する必要があります。HTTPS over TLS は、2 つのエンドポイント間の通信を暗号化するために使用されます。WebTools と Fiery API から Fiery server に接続する場合は、HTTPS が必要です。これらの通信は、TLS 1.3 および TLS 1.2 で暗号化されます。

証明書管理

Fiery servers は、TLS 通信で使用される証明書を管理するためのインターフェイスを提供します。Fiery servers は X.509 証明書フォーマットをサポートします。

Fiery servers は 4096、3072、2048 ビットのキー長で RSA 証明書をサポートします。

Fiery システム管理者は、証明書管理で次の操作を行うことができます。

- 自己署名デジタル証明書の作成。
- Fiery server の証明書および対応する秘密鍵の追加。
- 信頼できる証明書権限からの証明書の追加、参照、表示および削除。

メモ：自己署名証明書は安全ではありません。信頼できる証明機関（CA）の証明書を使用することを強くお勧めします。

信頼できる証明機関によって署名された証明書を取得したら、WebTools の Configure セクションで証明書を Fiery server にアップロードできます。

E メールセキュリティ

Fiery server は、E メールが有効になっている場合、POP および SMTP E メール通信プロトコルをサポートします。（この機能はデフォルトでは無効にされています。）E メールサービスが攻撃されたり、不適切に使用されないように、Fiery システム管理者は、追加のセキュリティ機能を有効にすることができます。

POP before SMTP

E メールサーバーによっては、サポートしている SMTP プロトコルの安全性がまだ確保されておらず、誰でも認証なしに E メールを送信できるものがあります。不正なアクセスを防止するために、一部の E メールサーバーでは SMTP を使って E メールを送信する前に、E メールクライアントに対して POP 経由での認証を要求します。このような E メールサーバーを使用する場合、Fiery システム管理者は、POP before SMTP による認証を有効にする必要があります。

OP25B

アウトバウンドポート 25 ブロッキング（OP25B）は、ISP が、自社のルーター経由で 25 番ポートへ送信されるパケットをブロックするスパム対策の手段です。Fiery システム管理者は、E メール設定インターフェイスを使用して、別のポートを指定できます。

Fiery serverE メール印刷ワークフローの詳細については、E メール印刷（25 ページ）を参照してください。

サーバーメッセージブロック（SMB）

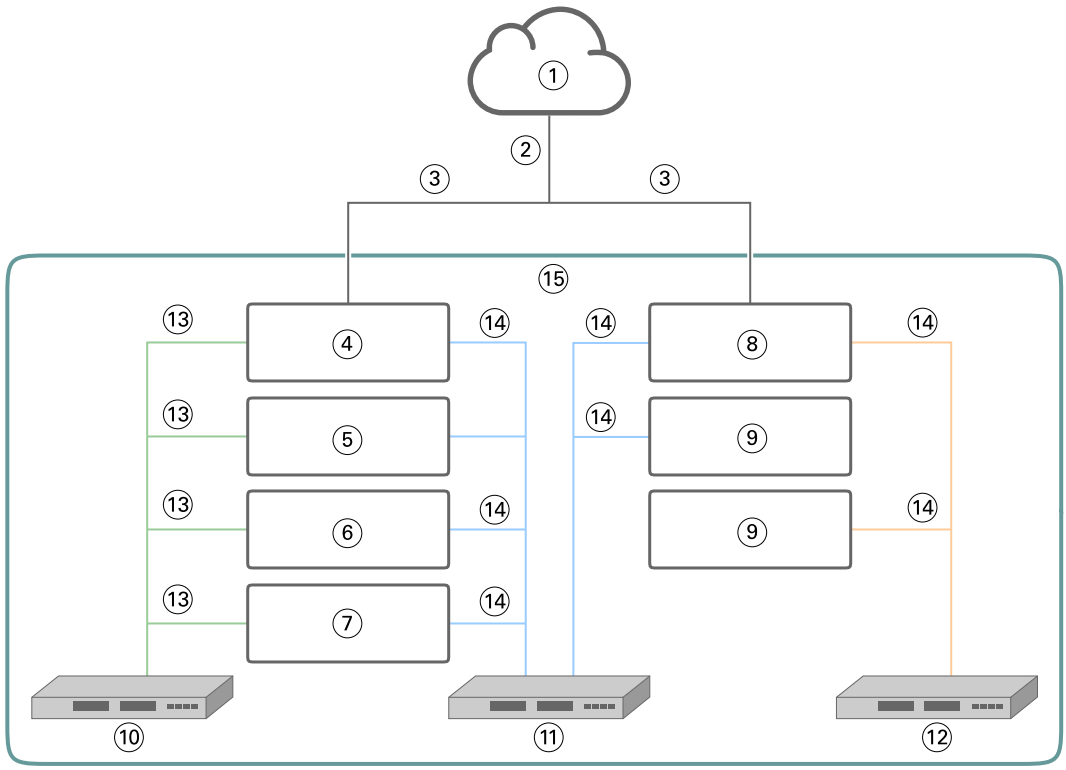
SMB は、ファイルやプリンターへの共有アクセスを提供するネットワークプロトコルです。SMB v1 は現在の業界セキュリティ標準を満たしていないため Fiery servers、SMB v1 は無効になっています。SMB v2 と v3 は引き続きサポートされています。

SMB 署名は、Fiery server で法的強制力を有します。SMB 署名では、受信者がパケットの真正性を確認して「中間の男」攻撃を防ぐために、デジタル署名されたパケットが必要です。SMB 認証が有効になっている場合、SMB フォルダーに格納されている SMB フォルダーとコンテンツにアクセスするには、ユーザーが SMB ユーザー名とパスワードを提供する必要があります。

メモ：SMB を使用した印刷またはファイルの共有は、Configure のパスワードを設定することで制限できます。

Fiery XB ネットワーク図

次の図は、Fiery XB サーバーと高速インクジェットプリンターをネットワークに接続する方法を示しています。



1	LAN	9	その他のプレスブレード（オプション）
2	ジョブ管理ネットワークトラフィック	10	10 GbE プライベートネットワーク
3	1 GbE DHCP またはスタティック	11	1 GbE プライベートネットワーク
4	Fiery メインブレード	12	1 GbE PLC プライベートネットワーク
5	Fiery RIP ブレード（オプション）	13	10 GbE
6	Fiery ブレード#1（オプション）	14	1 GbE
7	Fiery ブレード#2（オプション）	15	クローズ Fiery XB 環境
8	プレスブレード		

アクセス制御

この章では、さまざまなユーザーグループに対してリソースへのアクセスを制御できるよう Fiery server を設定する方法について説明します。

ユーザー認証

ユーザー認証機能を使用して、Fiery server で次の操作を行うことができます。

- ユーザー認証
- ユーザー権限に基づくアクションの許可

Fiery server は次のユーザー認証方式をサポートしています：

1. Fiery サーバーで定義されているユーザーのローカル認証
2. LDAP（例：Microsoft Active Directory）を使用した外部 ネットワーク認証サーバー経由の単一要素認証（SFA）
3. シングルサインオン（SSO）を使用した多要素認証 (MFA)

使用する方法にかかわらず、管理者アカウントは常に認証が必要です。これを無効にすることはできません。

Fiery server は、グループのメンバーシップに基づいてユーザーアクションを許可します。各グループには一連の権限（グレースケールで印刷、カラー/グレースケールで印刷など）が関連付けられており、グループのメンバーのアクションは所属グループの権限に制限されます。Fiery システム管理者は、システム管理者およびオペレーターのアカウントを除く Fiery グループの権限を変更できます。

このバージョンのユーザー認証では、グループに対して、次のように別の権限を選択できます。

- **グレースケールで印刷**：グループのメンバーはジョブをグレースケールで印刷できます。ユーザーがこの権限を持たない場合、Fiery server はジョブを印刷しません。ジョブがカラージョブの場合、グレースケールで印刷されます。
- **カラー/グレースケールで印刷**：グループのメンバーは、Fiery server のカラーおよびグレースケール印刷機能をフルに使用してジョブを印刷できます。この権限またはグレースケールで印刷する権限がない場合、印刷ジョブに失敗し、ユーザーは FTP 経由でジョブを送信できません（カラーデバイスのみ）。
- **Fiery メールボックス**：グループのメンバーには、個別のメールボックスが与えられます。Fiery server は、メールボックス権限を持つユーザー名に対してメールボックスを作成します。このメールボックスには、メールボックスのユーザー名とパスワードを持つユーザーのみがアクセスできます。
- **キャリブレーション**：この権限を持つグループのメンバーは、カラーキャリブレーションを実行できます。
- **サーバープリセット作成**：グループメンバーがサーバープリセットを作成できます。グループのメンバーは、これらのサーバープリセットにアクセスできます。

- **ワークフローの管理**：この権限を持つグループのメンバーは、仮想プリンターを作成、公開または編集できます。
- **ジョブの編集**（Fiery XB サーバーのみ）：この権限を持つグループのメンバーは、キュー内のジョブを編集できます。

メモ：メンバー印刷およびグループ印刷機能は、ユーザー認証に置き換えられます。

Fiery ソフトウェアユーザー認証

Fiery server ソフトウェアは、さまざまなタイプのユーザーとやり取りをします。そうしたユーザーは、Fiery ソフトウェア固有のユーザーであり、Windows で定義されるユーザーや役割とは関係ありません。

Fiery システム管理者は、初回のインストール直後にすべてのデフォルトパスワードを変更することが推奨されます。Fiery サーバーへのアクセスにパスワードを使用することを強制する必要があります。

- システム管理者とオペレーターのパスワードの最大文字数は、**Configure** > **セキュリティ**を使用する場合、ともに 15 文字です。
- ローカルユーザーアカウントで **Configure** > **ユーザーアカウント**を使用する場合、パスワードの最大文字数は 64 文字です。
- システム管理者パスワードとオペレーターパスワードは、**Configure** > **ユーザーアカウント**で変更することができます。

ローカルな Fiery ユーザーアカウントとアクセス権限

- **システム管理者**：Fiery server のすべての機能を完全に制御できます。Fiery システム管理者は、システム管理者およびオペレーターのアカウントを除く Fiery グループの権限を変更できます。
- **オペレーター**：システム管理者と同じ権限がありますが、設定などの一部の Fiery server 機能にはアクセスできず、ジョブのログも削除できません。
- **プレスオペレーター**（Fiery XB サーバーのみ）：プレス上のジョブを管理できます。システム管理者は、このユーザータイプに特定の権限を追加できます。
- **Fiery サービス管理者**（Windows 上の Fiery servers のみ）：Windows サーバーに信頼された証明書をインストールするために使用される非表示の管理者アカウント。このアカウントでは、ユーザーは Fiery server（ローカルまたはリモート）にログインできません。このアカウントは、一部のネットワークスキャンツールに表示され、必要に応じて削除できます信頼できる証明書をインストールする場合は、別の標準の方法を使用できます。
- **Fiery_SMB_ユーザー**：Windows 印刷（SMB）のデフォルトユーザーアカウントです。Windows SMB ユーザーは「ネットワーク近傍」で Fiery サーバーを「見る」ことができます。
- **ゲスト**（デフォルト、パスワードなし）：オペレーターと同じ権限がありますが、ジョブログへのアクセス、印刷ジョブの編集、印刷ジョブのステータス変更またはジョブのプレビューを行うことはできません。

シングルサインオン（SSO）

FS600 Pro サーバーは、Microsoft Entra ID（Azure Active Directory）を使用したクラウドベースの SSO ユーザー認証用の OpenID Connect プロトコルをサポートしています。ユーザーは、既存の AAD ログイン情報を使用して Fiery server にログインできます。

この認証方法は、多要素認証（MFA）に対応しています。

この ID 管理アプローチを追加する利点は、Fiery サーバーがユーザーのパスワードをローカルに保存しないことから、セキュリティが向上するという点です。

Fiery セキュリティ監査ログ

組織のコンプライアンス要件を満たすために、Fiery システム管理者はセキュリティ関連のイベントを取得して分析し、セキュリティ監査ログに保存できます。

セキュリティ監査ログはデフォルトで有効になっています。

各セキュリティイベントは、情報、警告、エラーに分類されます。システム管理者に表示されるのは静的なログのみで、警告や通知は表示されません。

ログは一般的な SIEM ログ収集および分析ソリューションでサポートされる形式です。キャプチャされたイベントに関する情報は、NIST 特別刊行物 800-53、*Recommended Security Controls for Federal Information Systems*（SP800-53）に従って行われます。

Fiery システム管理者は、FIERY の介入なしにイベントを読み取ることができます。Windows ベースと Linux ベースの Fiery servers のイベントは JSON 形式で、任意のログ収集ツールで処理できます。Windows ベースの Fiery サーバーの場合、イベントは Windows イベントマネージャーで表示できます。Linux ベース Fiery servers のシステム管理者は、ログを中央ログ収集システム（SysLog）に転送できます。

セキュリティイベントは、割り当てられたディスクストレージ容量に基づいて保持されます。ログサイズが最大記憶域（400 MB）に達すると、古いイベントは削除されます。

オペレーティングシステム

FIERY は Fiery servers で使用されているオペレーティングシステムのメーカーと密接に連携して、コアな Fiery server コンポーネントに影響を及ぼす可能性がある必要なセキュリティアップデートを入手します。

Linux（FS600）

FS600 Linux ベースのサーバーは、クローズドシステムです。ネットワークの可視性を制限することで、不正アクセスを防ぎます。

Linux ベースの Fiery servers について

- オペレーティングシステムにアクセスできるローカルインターフェイスは含まれていません。
- SSH と Telnet はサポートされていないため、オペレーティングシステムのシェルにアクセスできません。
- システムの脆弱性を潜在的に晒す可能性のある不正なプログラムのインストールを許可しません。
- FS600 Fiery servers で使用される Linux オペレーティングシステムは、Fiery servers 専用にカスタマイズされたオペレーティングシステムです。Fiery server が必要とするすべてのオペレーティングシステムコンポーネントを備えていますが、一般的な Linux システムで見られる汎用コンポーネントやエンドユーザーアプリケーションは備えていません。
- プリンターコントロールパネルでの Fiery 設定または FieryWebTools の Configure での設定ができます。FieryWebTools は、Fiery server が Fiery システム管理者が設定やその他のシステム管理アクティビティにアクセスするために使用する、内部ブラウザーベースのアプリケーションです。FieryWebTools は、最新のセキュア web フレームワークで動作し、最新の web ブラウザーでサポートされています。

Windows 10（FS600 Pro）

FS600 Pro Fiery servers は、Windows 10 IoT Enterprise 2021 LTSC で動作します。この Windows 10 バージョンには、最新のセキュリティ保護が含まれており、Windows 10 バージョン 21H2 で提供される追加の拡張機能が含まれています。リリース後 10 年間にわたり、Microsoft から各 LTSC ビルドのセキュリティアップデートが提供されます。

メモ：Windows 10 IoT Enterprise 2021 LTSC は、Windows 10 Enterprise バージョン 21H2 に相当するバイナリです。

Windows 10 IoT Enterprise 2021 LTSC には、次の機能が含まれています。

- Fiery servers などの専用システムでの使用を目的としています。
- 脅威、情報、ID 保護のための多くのセキュリティ強化が組み込まれています。
- リリース後最長 10 年間のセキュリティアップデートを提供します。
- カレンダー、天気、写真などの消費者向けアプリケーションは含まれていません。

Microsoft Windows のアップデート

Microsoft は、オペレーティングシステムのセキュリティ上の脅威や脆弱性に対処するために、**Windows アップデート**からセキュリティパッチを定期的に発行します。Fiery servers の **Windows アップデート**のデフォルト設定では、パッチはダウンロードされず、新しいパッチがユーザーに通知されます。Windows の**コントロールパネル**の **Windows アップデート**で**アップデートの確認**を選択すると、自動アップデートが有効になり、アップデート処理が起動します。

Windows アップデートツール

Windows ベースの Fiery servers は、Microsoft の標準的な方法を使用して、適用されるすべての Microsoft セキュリティパッチをアップデートします。Fiery server は、セキュリティパッチを取得するためのサードパーティ製のその他のアップデートツールをサポートしていません。

Windows のウイルス対策ソフトウェア

Fiery servers は、Microsoft Defender ウイルス対策ソフトウェア使用して保護します。通常は、Fiery server でサードパーティのウイルス対策ソフトウェアを使用できます。ウイルス対策ソフトウェアにはさまざまな種類があり、脅威に対応するために数多くのコンポーネントや機能が組み込まれています。

ウイルス対策ソフトウェアは、Fiery server 自体にインストールして設定し、実行するのが最も有効です。ローカル設定のない Fiery servers でも、リモートクライアントコンピューターでウイルス対策ソフトウェアを起動し、共有 Fiery server ハードドライブをスキャンすることができます。ウイルス対策ソフトウェアの動作のサポートについて、Fiery システム管理者はソフトウェア製造元に直接問い合わせてる必要があります。

ウイルス対策エンジンのスキャン

Fiery server のウイルス対策エンジンのスキャンは、スキャンがスケジュールされている場合でも、Fiery パフォーマンスに影響を与える可能性があります。

スパイウェア対策

スパイウェア対策プログラムは、Fiery server にファイルを送信する際の性能に影響を与えることがあります。たとえば、印刷ジョブが送信されたとき、Fiery server システムのアップデート時にファイルがダウンロードされたとき、Fiery server で実行されているアプリケーションの自動アップデートが実行されたときなどに、性能に影響が出ることがあります。

組み込みのファイアウォール

Fiery server にはファイアウォールが実装されているため、通常、ウイルス対策用のファイアウォールは必要ありません。ウイルス対策ソフトウェアに付属のファイアウォールをインストールして実行する必要がある場合は、自社の IT 部門と協力して実行してください。使用可能なポートの一覧については、ネットワークポート（10 ページ）を参照してください。

スパム対策

Fiery server は、「E メール経由で印刷」および「スキャンして E メール」機能をサポートしています。そのため、サーバーベースの E メールスパムフィルタリングメカニズムを使用することをお勧めします。Fiery servers は、指定した E メールアドレスから書類を印刷するように設定することもできます。

ホスト侵入防止システム（HIPS）およびアプリケーション制御

ホスト侵入防止システム（HIPS）とアプリケーション制御は複雑な機能であるため、これらのいずれかの機能を使用する場合は、ウイルス対策設定をテストして、慎重に確認する必要があります。HIPS とアプリケー

ション制御は、適切に調整することで優れたセキュリティ対策の手段となり、Fiery server と共存することができます。ただし、HIPS パラメーター設定を誤ったり、不適切なファイル除外をしたりすると、Fiery server の問題を引き起こしやすい機能でもあります。多くの場合、「デフォルトの設定を受け入れる」ことにより問題が発生します。HIPS で選択されているオプションを確認するか、アプリケーション制御設定と Fiery server 設定（ネットワークポート、ネットワークプロトコル、アプリケーション実行可能ファイル、設定ファイル、一時ファイルなど）を確認してください。

セーフリストとブロックリスト

セーフリストとブロックリスト機能は、通常 Fiery server に悪い影響を与えません。FIERY では、Fiery モジュールがブロックされないよう、顧客がこれらの機能を設定することを強くお勧めします。

E メールウィルス

通常、E メール経由で伝播されるウィルスは、受信者が何らかの操作を実行することで感染します。PDL ファイル以外の添付ファイルは、Fiery server によって破棄されます。また、Fiery server は、RTF や HTML 形式の E メール、および組み込まれている JavaScript のコードをすべて無視します。受信したコマンドに基づいて特定のユーザーに対して送信される E メール応答を除き、E メールで受信したすべてのファイルは PDL ジョブとして処理されます。

メモ：Fiery server E メール印刷ワークフローの詳細については、E メール印刷（25 ページ）を参照してください。

データセキュリティ

このセクションでは、Fiery server に格納されているユーザーデータを保護するために設計されたセキュリティ管理、および送信中のデータについて説明します。

重要な情報の暗号化

重要な顧客データを暗号化することにより、すべてのパスワードおよび関連する設定情報を安全に Fiery server に保存できるようになります。重要な情報は暗号化またはハッシュ化されています。実装されている暗号化アルゴリズムは、AES256、Diffie-hellman および SHA-1 で、最新のセキュリティ標準に準拠して使用されています。

ディスクが Fiery server から除去されると、ディスクに保存されている顧客データを読み取ることはできません。ユーザーデータの暗号化は、Windows ベースの Fiery servers で Configure を使用して有効または無効にできます。Linux ベースの Fiery servers の場合、この機能は常に有効になっています。

データ復旧に使用するパスフレーズを忘れた場合、リセットする方法はなく、FIERY は復旧できません。この場合、ソフトウェアを再インストールする必要があります。

また、Windows ベースのサーバーには、ブートドライブを暗号化するオプションもあります。ブートドライブには、オペレーティングシステムと Fiery System ソフトウェアが含まれます。ブートドライブは暗号化されていることから、誰かが別のオペレーティングシステムで Fiery サーバーを起動するのを防いでおり、目的のオペレーティングシステムにおける強制ファイルパーミッションを簡単に回避できます。

標準印刷

Fiery server に送信されたジョブは、Fiery server によって公開されている次の印刷キューのいずれかに送信されます。

- 待機キュー
- 印刷キュー
- 送信順印刷キュー
- ダイレクトキューダイレクト接続
- 仮想プリンター（Fiery システム管理者が定義するカスタムキュー）

Fiery システム管理者は、印刷キューおよびダイレクトキューを無効にして、自動印刷を制限することができます。

待機、印刷および送信順印刷キュー

ジョブが印刷キューまたは待機キューに対して印刷された場合、ジョブは Fiery server のハードドライブにスプールされます。待機キューに送信されたジョブは、Command WorkStation などのジョブ管理ユーティリティを使用してジョブを印刷処理に送ったり、削除したりするまでの間、Fiery のハードディスクドライブに保持されます。

送信順印刷キューを使用すると、Fiery server は、ネットワークから送られる特定のジョブを順番通りに印刷することができます。ワークフローは「先入れ先出し」（FIFO）となり、ネットワーク経由で受信したジョブの順序が優先されます。送信順印刷キューが有効になっていない場合、Fiery server に送信された印刷ジョブは、さまざまな要因により、送信された順番通りに印刷されないことがあります。たとえば、Fiery server で大きなジョブをスプールしている間に、小さいジョブが先に印刷されることがあります。

印刷済みキュー

印刷キューに送信されるジョブは、印刷済みキューが有効になっている場合、印刷後に Fiery server の印刷済みキューに保存されます。システム管理者は、印刷済みキューで保持するジョブの数を定義できます。印刷済みキューが無効になっている場合、ジョブは、印刷後に自動的に削除されます。

ダイレクトキュー（ダイレクト接続）

ダイレクトキューは、フォントのダウンロード、および Fiery servers の PostScript モジュールに直接接続する必要があるアプリケーション用のキューです。

セキュリティ要件が高い環境では、ダイレクトキューで印刷しないことをお勧めします。Fiery server では、ダイレクト接続を利用して送信されたすべてのジョブが印刷後に削除されます。ただし、ジョブに関連するすべての一時ファイルが削除される保証はありません。

VDP（バリアブルデータ印刷）、PDF または TIFF ファイルタイプのジョブがダイレクトキューに送信された場合、これらのジョブは印刷キューに再ルーティングされます。ジョブが SMB ネットワークサービスでダイレクトキューに送信された場合、これらのジョブは印刷キューにルーティングされることがあります。

ジョブの削除

ジョブが Fiery server から自動的に削除された場合、または Fiery ツールを使用して消去した場合、ジョブを表示したり、取得したりすることはできません。ジョブが Fiery server のハードディスクドライブにスプールされた場合は、ジョブの要素がハードディスクドライブ上に残っていることがあるため、フォレンジックディスク分析ツールなどの特定の種類のツールを使用すると、理論的には復元することが可能な場合があります。

セキュアイレース

セキュアイレースを使用すると、Fiery 機能によってジョブ削除されたときに、送信されたジョブの内容が Fiery server ハードディスクドライブから削除されます。ジョブが削除されると、ジョブ情報は Fiery サーバーのハードドライブから回復できません。

Linux ベースの FS600 Fiery サーバーの場合、ジョブを削除すると、各ジョブのソースファイルは米国国防総省基準のデータ消去方法である DoD 5220.22-M に準拠したアルゴリズムを使用して 3 回上書きされます。

Windows ベースの FS600 Pro サーバーは、NIST 800-88 データサニタイズ標準に対応しています。Fiery システム管理者は、このオプションを 1 パスまたは 3 パスのイメージ上書き方法に設定できます。

ワークフロー	セキュアイレース
Fiery server ハードディスクドライブに保存されているジョブ。セキュアイレースは**オン**に設定されます。	はい
Fiery server ハードディスクドライブに保存されているジョブ。セキュアイレースは**オフ**に設定されます。	いいえ

ワークフロー	セキュアイレース
セキュアイレースを**オン**に設定した後、Fiery server で受信され、削除されたジョブ	はい
セキュアイレースを**オン**に設定する前に、Fiery server で受信されてから削除されたジョブ	いいえ
別の Fiery server に送信されるジョブのコピー（負荷分散）	いいえ
取り外し可能なメディアにアーカイブされるジョブ	いいえ
ネットワークドライブにアーカイブされるジョブ	いいえ
クライアントデバイス上にあるジョブ	いいえ
サーバーのクリアの実行	はい
別のジョブにマージまたはコピーされたページ（たとえば、Fiery Impose のジョブまたは組み合わされた PDF）	いいえ
SMB 接続から受信し、Fiery server ハードディスクドライブに保存されたジョブ	いいえ
ディスクスワップまたはキャッシュ処理の操作中に、Fiery server ハードディスクドライブに書き込まれたジョブの一部	いいえ
ジョブログエントリ	いいえ
サーバーのクリア実行後のジョブログエントリ	はい
ジョブの削除が完了する前に、Fiery server の電源をオフにする	いいえ
ジョブを削除する前に、Fiery server ハードディスクドライブを最適化する	×

メモ：セキュアイレース機能は、Fiery XB プラットフォームまたは SSD に保存されたユーザーデータでサポートされていません。

システムメモリ

ファイルの処理時に、一部のジョブデータがオペレーティングシステムのメモリに書き込まれることがあります。このメモリ上のデータがハードディスクドライブにスワップされ、上書きされないまま残ることがあります。

揮発性メモリ			
タイプ（SRAM、DRAM など）	**ユーザーが変更可能（はい/いいえ）**	**機能または使用**	**サニタイズ処理**
DRAM	はい	メインシステムメモリ（ダイレクトキューに送信されたジョブを受信）	Fiery server の電源オフ
SDRAM（ビデオカード上）	はい	ビデオメモリ	Fiery server の電源オフ

不揮発性メモリ			
タイプ（SRAM、DRAM など）	**ユーザーが変更可能（はい/いいえ）**	**機能または使用**	**サニタイズ処理**
BIOS	いいえ	BIOS 機能	ソケットから取り外して破棄しますが、システムは機能しなくなります。
イーサネット Eprom	いいえ	イーサネットチップファームウェア	デソルダーと破棄が行われますが、システムは機能しなくなります。
CMOS NVRAM	いいえ	BIOS 設定ストレージ	システムバッテリーを 30 秒間取り外します。
ハードディスクドライブ（HDD）またはソリッドステートドライブ（SSD）	はい	オペレーティングシステム Fiery アプリケーション（ユーザーデータを使用する可能性あり） Fiery システムソフトウェア ジョブの印刷、ジョブのスキャン、その他のユーザーデータ 工場出荷時のデフォルトのイメージバックアップ	システムソフトウェアを再インストールしてください。 ほとんどのジョブは、セキュアイレース機能*を使用して安全に削除することができます。サードパーティ製および Fiery パートナーのサニタイズツールを使用して、これらのデバイスでデータを完全に消去することができます。
メモ：揮発性メモリと RAM には、カスタマーデータの処理中にカスタマーデータを含めることができます。カスタマーデータは、BIOS、CMOS、NVRAM などの不揮発性メモリに保存されていません。 *SSD に保存されているジョブにマルチパス上書き方式を使用することは、メモリの磨耗により推奨されません。すべての SSD の書き込みサイクル数には限りがあり、何度も上書きするとドライブの動作寿命が大きく損なわれます。Fiery サーバーは、ジョブデータを HDD ドライブに保存します。			

セキュア印刷

セキュア印刷機能を使用する場合、ジョブを印刷するために、ユーザーは、ジョブ固有のパスワードを Fiery server とプリンターに入力する必要があります。

この機能を使用するには、プリンターのコントロールパネルにアクセスする必要があります。この機能の目的は、書類へのアクセスをジョブのパスワードを持ち、プリンターのコントロールパネルでローカルに入力できるユーザーに制限することです。

セキュア印刷ワークフロー

ユーザーは、Fiery ドライバーの**セキュア印刷**フィールドにパスワードを入力します。このジョブが Fiery server の印刷キューまたは待機キューに送信されると、ジョブはキューに登録され、パスワードが入力されるまで保留されます。

メモ：セキュア印刷パスワードを使用して送信されたジョブは、Command WorkStation から表示できません。

プリンターのコントロールパネルから、ユーザーはセキュア印刷ウィンドウにアクセスしてパスワードを入力します。その後ユーザーは、そのパスワードを使用して送信されたジョブの場所を特定してそのジョブを印刷してから削除することができます。

印刷済みセキュアジョブは印刷済みキューに移動されず、印刷後に自動的に削除されます。

メモ：ただし、オペレーティングシステムファイルにデータの一部が一時的に残る場合があります。

E メール印刷

この機能では、Fiery server は E メールで送信されたジョブを受信して、印刷します。システム管理者は、Fiery server 上に、許可された E メールアドレスのリストを保存できます。許可された E メールアドレスのリストに含まれていない E メールアドレスから受信した E メールは削除されます。E メール印刷機能は、デフォルトでオフになっています。システム管理者は、E メール印刷機能をオン/オフにできます。

ジョブ管理

Fiery server に送信されるジョブに対してジョブアクションを実行するには、システム管理者またはオペレーターのいずれかが、 Fiery ジョブ管理ユーティリティを使用する必要があります。

ジョブログ

ジョブログは、Fiery server に保存されます。ジョブログの個別のレコードを削除することはできません。ジョブログには、ジョブを開始したユーザー、ジョブの実行時刻、使用された用紙やカラーなどのジョブの特性など、印刷やスキャンのジョブ情報が含まれています。ジョブログを使用して、Fiery server のジョブアクティビティを調べることができます。

オペレーターとしてのアクセス権を持つユーザーは、Command WorkStation からジョブログを参照、エクスポート、または印刷できます。システム管理者としてのアクセス権を持つユーザーは、Command WorkStation からジョブログを削除できます。

Fiery サーバーが FIERY IQ に接続されている場合、リモートユーザーは会社の IQ ポータルテナントでジョブログを確認できます。

設定

設定を行うには、システム管理者パスワードが必要です。Fiery server は、FieryWebTools の Configure、Fiery Command WorkStation またはプリンターのコントロールパネルの設定機能から設定できます。

スキャン

Fiery server を使用して、プリンターの原稿台ガラスに置かれたスキャンする画像を、スキャンを開始したワークステーションに戻すことができます。ワークステーションからスキャン機能を開始すると、生のビットマップイメージが直接ワークステーションに送信されます。

ユーザーは書類を Fiery server にスキャンして、配布、保管および取得することができます。すべてのスキャン済み書類は、ディスクに書き込まれます。システム管理者は、事前に定義した一定時間が経過すると、スキャンジョブが自動的に削除されるように Fiery server を設定できます。

スキャンジョブの配布

スキャンジョブは、さまざまな方法で提供されます。

E メール

スキャンジョブの添付ファイルがある E メールはメールサーバーに送信され、そのメールサーバーから任意の宛先にルーティングされます。

メモ：ファイルサイズが、システム管理者が定義した最大サイズよりも大きい場合、ジョブは Fiery server のハードディスクドライブに保存され、URL からアクセスできるようになります。

FTP

ファイルは FTP の宛先に送信されます。宛先を含む転送のレコードは FTP ログに保持され、プリンターのコントロールパネルのページの印刷コマンドからアクセスできます。ジョブをファイアウォール経由で送信するために FTP プロキシサーバーを定義することができます。

Fiery server 待機キュー

ファイルは Fiery server 待機キューに送信され、スキャンジョブとして保持されません。

待機キューの Fiery server の詳細については、待機、印刷および送信順印刷キュー（21 ページ）を参照してください。

インターネットファックス

ファイルはメールサーバーに送信され、メールサーバーから目的のインターネットファックスの宛先にルーティングされます。

メールボックス

ファイルはメールボックスのコード番号を付加されて Fiery server に保存されます。保存されたスキャンジョブにユーザーがアクセスするには、正しいメールボックス番号を入力する必要があります。ユーザーには、不正アクセスに対するスキャンメールボックスの内容を保護するための、パスワードの設定オプションが用意されています。スキャンジョブは、URL を通して取得できます。

Fiery のクラウドサービスとの通信

Fiery 内部サービスおよび Fiery アプリケーションの中には、外部のクラウドベースサービスとの通信が必要なものがあります。たとえば、Fiery セキュリティアップデートのダウンロードやライセンスアクティベーションなどです。

次の情報は、IT またはネットワーク管理者を対象としており、企業のファイアウォールの背後にある Fiery server を設定するために使用します。

#	Fiery サービス/アプリケーション	リモートサーバーの完全修飾ドメイン名（FQDN）	ポート	使用する
1	システムアップデート	https://liveupdate.efi.com	443	Fiery パッチのダウンロード
2	OFA	https://xbis.efi.com	443	ライセンスアクティベーション用
3	IQ	https://iq.efi.com	443	Fiery IQ との通信
4	LINQ	https://ews.efi.com	443	分析
5	Microsoft 社のユニバーサルプリント	https://portal.azure.com https://print.print.microsoft.com https://notification.print.microsoft.com https://discovery.print.microsoft.com https://graph.print.microsoft.com	443	Microsoft 社の Universal Print との通信
6	シングルサインオン（SSO）	https://login.microsoft.com	443	シングルサインオン（SSO）

#	Fiery サービス/アプリケーション	リモートサーバーの完全修飾ドメイン名（FQDN）	ポート	使用する
7	Windows アップデート	https://windowsupdate.microsoft.com http://*.windowsupdate.microsoft.com https://*.windowsupdate.microsoft.com http://*.update.microsoft.com https://*.update.microsoft.com http://*.windowsupdate.com http://download.windowsupdate.com https://download.microsoft.com http://*.download.windowsupdate.com http://wustat.windows.com http://ntservicepack.microsoft.com http://go.microsoft.com http://dl.delivery.mp.microsoft.com https://dl.delivery.mp.microsoft.com http://*.dl.delivery.mp.microsoft.com https://*.dl.delivery.mp.microsoft.com	80 443	Windows アップデート
8	Command WorkStation	http://help.efi.com https://learning.efi.com https://communities.efi.com http://resources.efi.com https://liveupdate.efi.com http://www.efi.com http://product-redirect.efi.com https://iq.efi.com https://services.efi.com https://services-test.efi.com http://w3.efi.com	80 443	Fiery のサービス/リソースにアクセス
9	Fiery Driver	https://help.efi.com	443	Fiery オンラインヘルプリソース
10	Fiery アップデート	https://liveupdate.efi.com	443	Command WorkStation からの Fiery アップデートの確認

#	Fiery サービス/アプリケーション	リモートサーバーの完全修飾ドメイン名（FQDN）	ポート	使用する
11	Fiery Software Manager	https://kuveupdate.efi.com https://www.efi.com https://estore.efi.com	443	ソフトウェアアップデートの確認
12	Fiery Software Manager	https://diumxs9ckzarso.cloudfront.net	443	Fiery アプリケーションのダウンロード
13	Fiery JobFlow	https://xbis.efi.com https://www.efinotifications.com http://help.efi.com http://fiery.efi.com/jobflow/support https://ews.efi.com/api/v1/analytics http://fiery.efi.com/jobflow-cookbook http://resource.efi.com/jobflow http://www.efi.com http://product-redirect.efi.com	80 443	Fiery のサービス/リソースにアクセス

規制およびフレームワークのコンプライアンス

次の表は、FS600 Pro/FS600 システムソフトウェアを実行している Fiery サーバーの規制およびフレームワークのコンプライアンスを示しています。

規制/フレームワーク	適用範囲	NX シリーズ（FS600 Pro）	A/E シリーズ（FS600）
FIPS 140-2	• アメリカ、カナダ • 暗号化モジュールのセキュリティ要件	適合 Windows 10 2021 LTSC	非適合
CIS ベンチマーク	• システムを安全に設定するための設定ベースラインとベストプラクティス	適合 Microsoft Windows 10 Enterprise（リリース 21H2）ベンチマーク	なし*
セキュリティ技術実装ガイド（STIG）	米国国防総省（DOD）機関が使用するハードウェアおよびソフトウェアのセキュリティ設定標準。	適合 Windows 10 STIG バージョン 2、R4	なし*
共通基準	• IT セキュリティに関する情報技術セキュリティ手法の評価基準	適合	非適合
セイフガードコンピューターセキュリティ評価マトリックス（SCSEM）	• 米国政府（連邦および州） • 連邦政府、州および地方省庁の税務情報セキュリティガイドライン	適合 抵抗および検出の要件にはオプションの Fiery ディスクドライブセキュリティキットが必要	非適合
DoD 522.22-M	データサニタイズ標準	なし	適合 3 パス
NIST 800-88	データサニタイズ標準	適合 1 パスまたは 3 パス	非適合

*規制やフレームワークの適用範囲外。A および E シリーズの Linux ベースサーバーは、ファイルシステムに直接アクセスしないクローズドシステムです。ネットワークの可視性を制限することで、不正アクセスを防ぎます。

FIPS 140-2 準拠

Windows 10 2021 LTSC で FS600 Pro を実行している Fiery サーバーは、正しく設定されていれば、FIPS 140-2 データ暗号化ガイドラインに準拠できます。*FIPS 140-2 モード*の Fiery サーバーは、米国連邦政府の暗号化アルゴリズム検証プログラム（CAVP）で検証および認証された暗号化アルゴリズムのみを使用し、保存中および送信中のデータを暗号化します。

Fiery で *FIPS 140-2 モード*を有効にするには、認定された Fiery プロフェッショナルハードニングサービスが必要です。

セキュア Fiery サーバー設定に関するガイドライン

次のガイドラインは、Fiery システム管理者が Fiery server を設定する際に、セキュリティを向上させるのに役立ちます。

システム管理者パスワードの変更

インストール時に Fiery システム管理者のデフォルトパスワードを変更し、組織のセキュリティポリシーに従って定期的に変更することをお勧めします。Fiery サーバーを初めて設定する際に、**Fiery 設定ウィザード**でシステム管理者のデフォルトパスワードを変更する必要があります。システム管理者のパスワードとオペレーターのパスワードは、初回設定の後に WebTools の **Configure** > **セキュリティ** > **システム管理者パスワード**（またはオペレーター）で変更できます。パスワード設定は、**Configure** > **ユーザーアカウント** > **Fiery 連絡先リスト**からも行うことができます。

システム管理者パスワードで、ローカルでまたはリモートクライアントから Fiery server にフルアクセスできます。フルアクセス可能な対象：

- ファイルシステム
- システムセキュリティポリシー
- レジストリエントリ
- システム管理者パスワードを設定すると、匿名のユーザーが Fiery server にアクセスするのを拒否することができます。

推奨設定

- **ネットワーク** > **SNMP** で、SNMP に**最高**セキュリティレベルを選択します。

  最高セキュリティ制限を選択した場合、Fiery server のサポートは SNMP v3 のみに制限されます。

  SNMP マネージャーが SNMP v1/v2c でのみ動作する場合は、**コミュニティ名の読み込み**フィールドの値を変更します。Fiery server により WebTools から、SNMP **コミュニティ名の読み込み**および**コミュニティ名の書き込み**フィールドの値を変更できます（**Configure** > **ネットワーク** > **SNMP**）。また、プリンターコントロールパネルの値も変更できます（**ネットワーク** > **SNMP**）。
- ジョブ送信で WSD を無効にします。
- lpr、ポート 9100 または IPP を使用して印刷する場合は、ジョブ送信での Windows 印刷を無効にします。
- **セキュリティ** > **TCP/IP** ポートフィルタリングで、TCP/IP ポートフィルターを有効にしてポートをブロックします。

  Windows 印刷を使用しておらず、ファイルフォルダーへのアクセスや共有が不要な場合は、ポート 137～139 および 445 を削除します。セキュリティで保護されていないポート 80（HTTP）通信を無効にします。

オペレーティングシステムレベルでの保護の他に、Fiery server には、データの保護に役立つ次のセキュリティ機能もあります。

- Fiery servers のセキュア印刷を使用して、ユーザーが各自の印刷ジョブのみを選択していることを確認します。
- Fiery servers は、主要なジョブアカウンティングソリューションと統合して、フォローミー印刷を使用してセキュリティを強化することができます。

Fiery servers には多数のセキュリティ機能が備わっていますが、インターネット接続向けのサーバーではありません。Fiery サーバーは保護された環境に配置する必要があります。また、ネットワークのシステム管理者は、サーバーへのアクセスを適切に管理する必要があります。

高セキュリティプロファイルの選択

Fiery server は、さまざまなリスクや脅威レベル（**標準**、**高**、**現在の設定**）に基づいて、事前に定義されたセキュリティ推奨事項を提供します。この機能は**セキュリティプロファイル**と呼ばれ、次の場所からアクセスできます。

- Fiery ソフトウェアウィザード
- **WebTools** > **Configure** > **セキュリティ**

高セキュリティプロファイルを使用すると、Fiery server をよりセキュアにすることができ、最も一般的に使用されているセキュリティ機能を使用できます。

オプション	高
TCP/IP ポートフィルタリング	使用可能
Service Location Protocol（SLP）	使用不可
Bonjour	使用不可
セキュアイレース	使用可能
リモートデスクトップ	使用不可
SMB パスワード	使用可能
USB ストレージデバイス	使用不可
PostScript セキュリティ	使用可能
ポート 9100	無効
LPD	使用可能
Windows 印刷	使用不可
IPP	使用可能
Web Services for Devices（WSD）	使用不可
E メール印刷	使用不可

オプション	高
FTP 印刷	使用不可
ダイレクトモバイル印刷	無効

FIERY は、セキュリティ要件が最も高い環境で、**高**セキュリティプロファイルを使用することを推奨します。

まとめ

FIERY は、Fiery サーバー向けに堅牢な標準およびオプションのセキュリティ機能を提供しています。このような包括的かつカスタマイズ可能なセキュリティ機能は、セキュリティ要件が厳しいお客様をはじめ、あらゆる規模のお客様に適しています。FIERY は、脆弱性、悪意のある使用、意図しない使用から Fiery サーバーを保護し、効率に影響を及ぼすことなく顧客データを保護するために、高度なセキュリティ機能を提供しています。

著作権情報

Copyright ©2024 Fiery, LLC. 無断複写、転載を禁じます。

本書は著作権法によって保護され、すべての権利が留保されています。ここで明示的に許可されている場合を除き、本書のいかなる部分も、形式、方法、目的を問わず、Fiery, LLC の事前の書面による合意なしに複製または公開できません。

本書に記載されている製品仕様、外観、その他の詳細は、発行日現在のもので、変更される可能性があり、Fiery が約束するものではありません。ここに記載される内容は、Fiery, LLC の製品とサービスに付属して明示された保証書に追加する保証にはなりません。

Fiery、Fiery ロゴ、 FieryCommand WorkStation、QuickTouch および WebTools は、米国および/またはその他の国の、Fiery, LLC および/またはその完全に所有する子会社の商標または登録商標です。その他の用語や製品名は各社の商標や登録商標である可能性があります。