Fiery FS400 Pro/FS400 servers

セキュリティに関するホワイトペーパー

45204337

2019 年 12 月 16 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 FS400 Pro/FS400 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 FS400 Pro/FS400 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 FS400 Pro/FS400 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

EFI のセキュリティ指針

EFI 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。EFI 製品は、会社の資産を守るためのセキュリティ機能を強化し、常に改善を続けています。EFI Fiery servers は、保存時や送信中、および処理中の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および製造されています。

グローバルな EFI 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、エンドユーザーは、Fiery セキュリティ機能を自社のセキュリティポリシーおよび特定の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）と組み合わせて使用することをお勧めします。

EFI のセキュリティ目標

Fiery server のセキュリティ対策を実行する際、EFI では、以下を目標にしています。

- **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が利用可能になると、自動で通知とダウンロードを実施する。
- **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。

Fiery ソフトウェアセキュリティのアップデート

本セクションでは、Fiery server ソフトウェアセキュリティのアップデート処理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、EFI 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。

- EFI 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 を監視しています。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。
- EFI 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、承認を得るために特定の EFI 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できるようになります。
- 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で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には、指定された印刷環境で Fiery servers の安全を維持することが重要です。

Fiery server セキュリティ機能の設定

Configure は、Fiery servers のセキュリティ機能を設定するために使用される主なツールです。Fiery システム管理者は、Command WorkStation または WebTools から Configure にアクセスできます。

メモ：Configure にアクセスするには、ユーザーはシステム管理者権限が必要です。

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（28 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（24 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（24 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、EFI 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 IoT Enterprise 2016 または 2019 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。

イメージデータとジョブ管理情報は、オペレーターが削除することも、事前に設定した時間経過後に自動で削除することもできます。これにより、イメージデータにアクセスできなくなります。

イメージデータへの不正アクセスを防止するために、EFI はセキュアイレース機能を提供しています。Fiery のシステム管理者が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。セキュアイレースは、ソリッドステートドライブで設定できます。ただし、ハードディスクドライブと同じ方法では機能しません。

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

Fiery server は、次の表の外部ポートを使用して接続できます。

Fiery のポート	関数	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たアクセス制御
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	USB 印刷はオフにできます。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

ユーザーは、Fiery NX Station のモニター、Fiery servers の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 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。

リムーバブルハードディスクドライブキットオプション

一部の Fiery servers は、セキュリティを強化するために、取り外し可能なハードディスクドライブオプションキットをサポートしています。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。

スタンドアロンの Windows サーバーの場合

スタンドアロンの Windows ベースの Fiery servers は、リムーバブルハードディスクドライブオプションキットをサポートしています。このオプションキットが Fiery の製品に付属するかどうかは、EFI と個々の Fiery パートナーとの間で交わされる契約条項に応じて異なります。

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 ポートを使用して、マウス、キーボードまたは分光測色計を接続することができます、ただし、USB ストレージの有効化オプションが Configure で無効にされると、USB ストレージデバイスに接続できなくなります。このオプションは、デフォルトで有効にされています。このオプションが無効にされると、バックアップや復元など、USB の大容量ストレージ機能を必要とする Fiery 機能が無効になります。

ネットワークセキュリティ

Fiery server には、プリンターへのアクセスを制御および管理するためのさまざまなネットワーク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もできます。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（Windows 10 のみ）。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、49152～65536 の範囲の追加ポートが開かれます。
137～139		NETBIOS	Windows 印刷
	161、162	SNMP	Fiery Central、従来のユーティリティの一部、その他の SNMP ベースのツール
	427	SLP	SLP
443		HTTPS	WebTools、IPP/s
445		SMB/IP	SMB over TCP/IP
	500	ISAKMP	IPsec
515		LPD	LPR 印刷、従来のユーティリティの一部（旧バージョンの Command WorkStation）
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

TCP/IP	UDP	ポート名	ポートを利用するサービス
	4500	IPsec NAT	IPsec
	5353	Multicase DNS	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	EFI ポート	Command WorkStation 5 および 6、Fiery Central、EFI SDK ベースのツール、Fiery Printer Driver 双方向機能、WebTools、Fiery Direct Mobile Printing、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。

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。無効なポートを利用するサービスは、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（28 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、1.2 および 1.1 で暗号化されます。

証明書管理

Fiery servers は、SSL/TLS 通信で使用される証明書を管理するための証明書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 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。
- 信頼できる証明書ストアに対する証明書の追加、参照、表示、削除。

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）

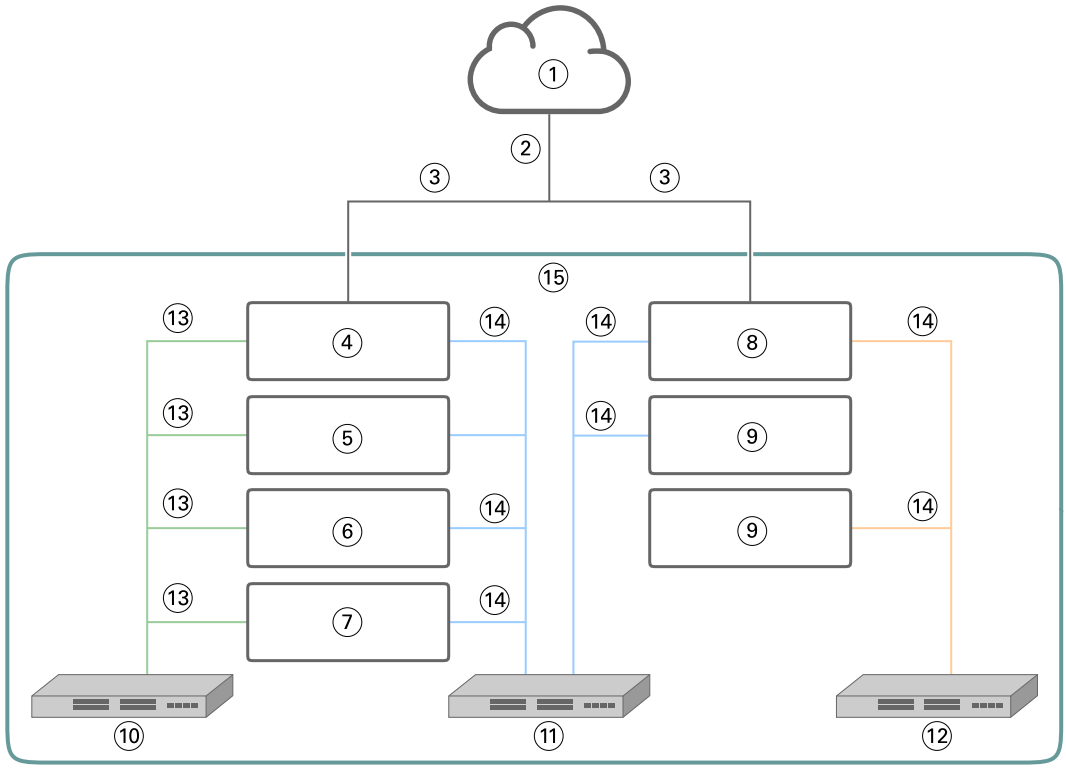
SMB は、ファイルやプリンターへの共有アクセスを提供するネットワークプロトコルです。SMB v1 は現在の業界セキュリティ標準を満たしていないため Fiery servers、SMB v1 は無効になっています。SMB v2 と v3 は引き続きサポートされています。

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のリソースへのアクセスを制御するよう 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、次のユーザーを認証することができます。

- ドメインベース：企業サーバーで定義され、LDAP を使用してアクセスされるユーザー
- Fiery ベース：Fiery server で定義されたユーザー

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**：この権限を使用すると、グループメンバーは Fiery server で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**：この権限を持つグループのメンバーは、Fiery server でジョブを印刷でき、Fiery server のカラーおよびグレースケール印刷機能をすべて利用できます。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**：この権限を持つ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の作成**：この権限を持つグループのメンバーは、一般的に使用されるジョブのプリセットに他の Fiery ユーザーがアクセスできるように、サーバープリセットを作成できます。
- **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 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 システム管理者が Fiery server にアクセスする場合は、パスワードを要求することをお勧めします。また、EFI は、Fiery システム管理者がデフォルトパスワードを変更して、その印刷環境のセキュリティ要件を満たすことを推奨します。

次に、さまざまな Fiery ユーザータイプに許可されている権限について説明します。

- **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**：システム管理者とほぼ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。

オペレーティングシステム

マザーボード、プロセッサー、BIOS などのコアな Fiery server コンポーネントに影響を及ぼす可能性があるセキュリティ上の問題や脆弱性については、EFI 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、必要なセキュリティアップデートを入手します。また、不正な変更（マルウェアの挿入を含む）を防ぐために、Fiery ソフトウェアアップデートは、EFI によってデジタル署名が行われています。

Linux（FS400）

FS400 Fiery servers は、クローズドアーキテクチャで設計された Linux ベースのサーバーです。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 の特性は次のとおりです。

- Linux ベースの Fiery servers には、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、Linux ベースの Fiery servers で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はアクセスできません。
- Linux ベースの Fiery servers は、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。
- FS400 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。このシステムは、Fiery server に必要なオペレーティングシステムコンポーネントをすべて備えていますが、Ubuntu や Fedora など、Linux システムの汎用コンポーネントの一部は含まれていません。

システムへのアクセス

Linux ベースの Fiery servers は、プリンターのコントロールパネルの Fiery 設定から、または WebTools の Configure から設定することができます。WebTools は、Fiery システム管理者が設定のために Fiery server へアクセスしたり、アクティビティと関連性のある他のシステム管理者にアクセスしたりすることができるブラウザーベースのページです。WebTools は、最新の Web ブラウザーでサポートされている最新のセキュア Web フレームワーク上で実行されます。

Windows 10（FS400 Pro）

FS400 Pro スタンドアロン Fiery servers は、Windows 10 IoT ENTERPRISE 2019 LTSC をオペレーティングシステムとして使用します。この Windows 版には、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 1703、1709、1803 および 1809 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 2019 LTSC は、Windows 10 Enterprise バージョン 1809 に相当するバイナリです。これらの 2 つのバージョンの主な違いは、ライセンスとディストリビューションモデルです。

Windows 10 IoT Enterprise 2019 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、および 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。
- セキュリティアップデートを多数提供します。
- Edge ブラウザー、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 ウイルス対策ソフトウェアおよび Windows 10 Defender を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。ただし、ウイルス対策ソフトウェアの動作のサポートについては、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ください。

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することを推奨します。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（11 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。Fiery server では、Outlook などの E メールクライアントを別途動作させることはできないため、スパム対策コンポーネントはありません。

HIPS と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、適切に調整すると、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、不適切なファイルを除外したりすると、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、アプリケーション制御設定、および 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）を合わせて確認する必要があります。

ホワイトリストおよびブラックリスト

ホワイトリストおよびブラックリスト機能は、通常、Fiery server に悪い影響を与えません。EFI では、Fiery モジュールがブラックリストに登録されないよう、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のセキュリティ制御について説明します。

重要な情報の暗号化

Fiery server 内の重要な情報を暗号化することによって、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。最新のセキュリティ基準に準拠するために、暗号化アルゴリズムとして、AES256、Diffie-hellman および SHA-1 が使用されています。

ディスクが Fiery server から削除されると場合、ディスクに保存されているユーザー情報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。

回復データに入力するパスフレーズを忘れた場合、リセットする方法はないため、EFI は回復できません。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。

メモ：データ暗号化を使用した場合、ディスクはパーティション分割され、ユーザーデータのパーティションのみが暗号化されます。オペレーティングシステムのパーティションは暗号化できません。

高度な暗号化標準（AES）

Fiery server は、不正アクセスから残りのデータを保護します。256 ビット AES アルゴリズムを使用して、ジョブ、画像、カスタマーデータを暗号化します。

AES は、幅広いデバイスやアプリケーションに適した、小型かつ高速でクラックのない暗号化標準です。AES により、企業のセキュリティポリシーに準拠しながら、データ盗難に対する保護をさらに強化することができます。

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。

印刷にはダイレクトキューを使用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確実に削除されることは保証されません。

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、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「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。

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
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	いいえ

メモ：セキュアイレース機能は、Fiery XB プラットフォームでは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。

*ソリッドステートドライブは、メモリの磨耗マッピングが行われるため、セキュアイレースマルチパス上書き方法によって完全にサニタイズすることはできません。また、サニタイズを実行しようとすると、ソリッドステートドライブの稼働寿命も大幅に低下させます。この機能は、Fiery XB プラットフォームではサポートされていません。

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。

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、ジョブがキューに登録されて、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。すると、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。

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、WebTools または Command WorkStation の Configure ツールから、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（22 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。

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。システム管理者のデフォルトパスワードは、初めて設定する際は Fiery 設定ウィザードで変更する必要があります。最初の設定後のシステム管理者およびオペレーターのパスワードは、WebTools で次のように変更できます。 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）。パスワード設定は、ユーザーアカウントからもアクセスできます。

システム管理者パスワードを使用してログインすると、ユーザーは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

- SNMP の最高セキュリティレベル（ネットワーク > SNMP）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 を使用すると、SNMP のコミュニティ名の読み込みとコミュニティ名の書き込みフィールドの値を WebTools（Configure > ネットワーク > SNMP）およびプリンターのコントロールパネル（ネットワーク > SNMP）から変更できます。
- 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。
- TCP/IP ポートフィルターを セキュリティ > TCP/IP ポートフィルタリングで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。

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設定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	使用可能
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	使用不可

EFI 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

EFI は、どのような環境のお客様に対しても、包括的でカスタマイズ可能なセキュリティソリューションを提供できるように、一連の堅牢な標準機能およびオプションセキュリティ機能を Fiery server で提供しています。EFI は、お客様が自社で最大限効率よく操作できるように、悪意を持った使用や意図しない使用に対する脆弱性から、Fiery server を効果的に保護するように取り組んでいます。