EFI™ ホワイトペーパーシリーズ

Fiery® のセキュリティに関するホワイトペーパー

Fiery FS350 Pro/FS350 サーバー

発行日：
2020 年 7 月

目次

1. ドキュメント概要

このドキュメントでは、エンドユーザー向けに、Fiery® サーバーのアーキテクチャと機能的な側面について、Fiery FS350/FS350 Pro サーバーのデバイスのセキュリティに関連する事項の概要を説明します。具体的には、ハードウェア、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、データセキュリティについて説明します。

本文書は、エンドユーザーが、Fiery サーバーの有益なセキュリティ機能および潜在的な脆弱性について理解できるようにすることを目的としています。

1.1 EFI のセキュリティ指針

EFI™ は、今日、世界中のビジネスにおいてセキュリティが最大の関心事の 1 つであることを理解しています。そのため、Fiery サーバーには、企業の重要な資産を保護するための強力なセキュリティ機能が組み込まれています。また、当社では、世界中の Fiery パートナーおよび社内の機能横断型チームと積極的に協力し、企業が現在および将来必要とするセキュリティ要件を把握することで、当社の製品でセキュリティの問題が発生しないように努めています。さらに、従来通り、Fiery のセキュリティ機能と、その他のセキュリティ機構（安全なパスワードや、物理的に強力なセキュリティ手段など）を組み合わせて使用し、全体的にシステムのセキュリティを強化することをお勧めします。

1.2 Fiery Configure によるセキュリティ機能の設定

Fiery Command WorkStation® からシステム管理者ログインを使用して Fiery サーバーにアクセスする Fiery ユーザーは、Fiery Configure を使用して Fiery のすべての機能を設定できます。Fiery Configure は、Fiery Command WorkStation または WebTools® の Configure タブから起動できます。

2. ハードウェアと物理的なセキュリティ

2.1 揮発性メモリ

Fiery サーバーは、CPU のローカルメモリ、およびオペレーティングシステム、Fiery システムソフトウェア、イメージデータの作業メモリとして、揮発性 RAM を使用しています。RAM に書き込まれたデータは、電源がオンになっている間は保持されます。電源がオフになると、すべてのデータが削除されます。

2.2 不揮発性メモリとデータストレージ

Fiery サーバーは、電源がオフの間に Fiery サーバー上にデータを保持するための不揮発性データストレージテクノロジをいくつか利用しています。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。

2.2.1 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格納されます。このデバイス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、システムが起動しなくなります。

フラッシュメモリの一部は、Fiery ソフトウェアオプションをアクティブにするためのドングルの使用状況を記録するためにも使用されます。

このデバイスにはユーザーデータは格納されません。ユーザーは、このデバイスのデータにはアクセスできません。

2.2.2 CMOS

バッテリ電源が付属している CMOS メモリは、サーバーのマシン設定を格納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。ユーザーは、Windows 10 IoT Enterprise 2016 LTSB（Windows 10）サーバー上のこれらの設定に Fiery NX Station からモニター、キーボード、およびマウスを使用してアクセスできます（インストールされている場合）。

2.2.3 NVRAM

Fiery サーバーには、システムの動作に必要なファームウェアを格納した数多くの小さな NVRAM が搭載されています。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。

2.2.4 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

通常の印刷およびスキャン操作の間、およびジョブ管理情報を作成している間、イメージデータは、ハードディスクドライブ（HDD）およびソリッドステートドライブ（SSD）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およびジョブを Command WorkStation からユーザーが手動で削除したり、プリンターの LCD などの他のインターフェイスから他のキュー操作を実行したりできます。「サーバーの初期化」コマンドを使用して、または印刷済みジョブがキュー内のジョブ数の制限を超えた場合に、イメージデータとジョブを自動的に削除することもできます。印刷済みキューを無効にすると、印刷済みジョブが削除されます。

イメージデータへの不正アクセスを防止するため、EFI はセキュア消去機能を提供しています（セクション 6.2.5 を参照）。システム管理者がこの機能を有効にすると、選択された操作が適切なタイミングで実行されて、HDD 上のデータが安全に削除されます。セキュア消去機能は、SSD に保存されているデータに対してはサポートされていません。

2.2.5 物理ポート

Fiery サーバーは、次の外部ポートを通して接続できます。

FIERY のポート	関数	アクセス	アクセスコントロール
イーサネット RJ-45 コネクター [こねくた]	イーサネット接続	ネットワーク接続 [せつぞく]	Fiery の IP フィルタリングを使用してアクセスを制御
複写機インターフェイスコネクター [こねくた]	印刷 / スキャン	印刷エンジン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 のグループポリシーからオフにできます。
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

2.3 ローカルインターフェイス

ユーザーは、Fiery NX Station のモニターまたは Fiery サーバーの Fiery QuickTouch タッチスクリーンディスプレイから Fiery の機能にアクセスできます。Fiery NX Station を使用した Fiery サーバー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。Fiery QuickTouch タッチスクリーンディスプレイには、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。

2.4 Removable HDD キットオプション

Fiery サーバーでは、セキュリティを強化するために、Removable HDD 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、サーバー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。

2.4.1 外付型サーバー向け

Fiery サーバーでは、Removable HDD 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締結される開発および販売契約の条項に応じて異なります。

2.4.2 Fiery XB サーバーの場合

Fiery XB サーバーでは、HDD/SSD はリムーバブルです。ほとんどの HDD/SSD は RAID 設定でペアになっています。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。

3. ネットワークセキュリティ

Fiery サーバーの標準的なネットワークセキュリティ機能には、承認されたユーザーとグループにのみ出力デバイスへのアクセスと印刷を許可する機能、デバイスの通信を指定された IP アドレスに制限する機能、使用可能なネットワークプロトコルとポートを任意に制御できる機能などがあります。

Fiery サーバーにはさまざまなセキュリティ機能が備えられていますが、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内に配置してください。また、ネットワークシステム管理者は、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。

3.1 ネットワークポート

Fiery サーバーでは、ネットワークシステム管理者は、以下の IP ポートを選択的に有効化および無効化できます。これにより、特定の転送プロトコルを使用した不要なデバイス通信やシステムへのアクセスを効果的にブロックできます。

デフォルトでは、ポートフィルタリングが有効になっています。ポートをフィルタリングすると、Fiery サーバーの外部ユーザーが、指定したポートを使用して Fiery サーバーに接続できなくなります。ポートがブロックされていない場合、ユーザーはそのポートに接続することができます。

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。無効なポートを利用するサービスは、リモートアクセスができません。

TCP/IP	UDP	ポート名	ポートを利用するサービス
20 ～ 21		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	WebTools、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	
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（WebTools、旧バージョンの CWS など）
631		IPP	IPP
	4500	IPsec NAT	IPsec
	5353	Multicase DNS	Bonjour
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
8021、8022、9906	9906	EFI ポート	Command WorkStation 5 および 6、Fiery Central、Fiery Printer Driver 双方向機能、WebTools。
8010、6310			Fiery Direct Mobile Printing
21030			Fiery Image Viewer
8090			Fiery ソフトウェアライセンス
50006 ～ 50025*			Fiery XF
9100 ～ 9103	9906	印刷ポート	ポート 9100

* このポートは外付型 Fiery サーバーに Fiery Command WorkStation バージョン 6.2 以降がインストールされている場合に有効です。

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 サーバー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。

ローカルシステム管理者は、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。

3.2 IP フィルタリング

IP フィルタリングを使用すると、システム管理者はデフォルトポリシーを設定して、すべての着信パケットを許可または拒否することができます。また、デフォルトポリシーを上書きするように最大 16 個の IP アドレスまたは範囲を設定できます。「拒否」用のフィルターポリシーでは、IP フィルタールールに一致するパケットが破棄され、「許可」用のデフォルトポリシーがそのようなパケットを受け入れます。

3.3 ネットワーク暗号化

3.3.1 IPsec

インターネットプロトコルのセキュリティである 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 サーバー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 サーバーとの間に 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。

FS350

3.3.2 SSL および TLS

Fiery サーバーでは、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。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 サーバーに接続する場合は、HTTPS over TLS が必要です。これらの通信は、TLS 1.2 および TLS 1.1 で暗号化されます。TLS 1.0 および SSL v3 は無効にされており、これらのプロトコルを使用しているすべての着信接続要求が拒否されます。

3.3.3 証明書管理

Fiery サーバーは、さまざまな SSL/TLS 通信で使用される証明書を管理するための証明書管理インターフェイスを備えています。X.509 証明書フォーマットをサポートしています。

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 サーバー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

3.4 SMB

SMB（Server Message Block）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 は安全でないため、Fiery サーバーで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。

3.6 SNMP v3

Fiery サーバーは、IP ネットワーク上のデバイスを管理するための安全なネットワークプロトコルである SNMPv3 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、機密性を確保できます。また、メッセージの完全性が確保され、認証も可能です。

Fiery システム管理者は、SNMPv3 に用意されている 3 つの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。

3.7 E メールセキュリティ

Fiery サーバーは、POP および SMTP プロトコルをサポートしています。E メールサービスが攻撃を受けたり、不適切に利用されたりしないように、Fiery システム管理者は、次のような追加のセキュリティ機能を有効化できます。

3.7.1 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。

3.7.2 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。

3.8 Fiery XB ネットワーク図

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の詳細は、付録 1 を参照してください。

4. アクセス制御

4.1 ユーザー認証

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

- ユーザー認証
- ユーザーの権限に基づくアクションの許可

Fiery サーバーは、次のユーザーを認証できます。

- ドメインベース：企業サーバーに定義され、LDAP によってアクセスされるユーザー
- Fiery ベース：Fiery サーバーに定義されたユーザー

Fiery サーバーは、ユーザーがどのグループに所属しているかに応じてユーザーの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する」、「カラー / グレースケールで印刷する」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、オペレーター、ゲストのアカウントを除き、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、グループを編集して、次の権限レベルを選択できます。

- グレースケールで印刷する：この権限を持つグループのメンバーは、Fiery サーバーでジョブの印刷を行うことができます。ユーザーが「カラー / グレースケールで印刷する」権限を持っていない場合、Fiery サーバーでは、ジョブが強制的にグレースケールでの印刷になります。
- カラー / グレースケールで印刷する：この権限を持つグループのメンバーは、Fiery サーバーでジョブを印刷でき、Fiery サーバーのカラー印刷機能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 サーバーは、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、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。

注意：メンバー印刷 / グループ印刷機能は、ユーザー認証に置き換えられました。

4.2 Fiery ソフトウェア認証

Fiery サーバーは、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。システム管理者が Fiery サーバーにアクセスする場合には、パスワードを要求することをお勧めします。

また、システム管理者のデフォルトパスワードは、印刷環境のセキュリティ要件に適合するパスワードに変更することをお勧めします。

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 サーバーのすべての機能にアクセスできます。
- オペレーター：システム管理者とほとんど同じ権限を持っていますが、設定などの一部のサーバー機能にはアクセスできず、ジョブ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するための権限を持っています。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。
- ゲスト（デフォルト、パスワードなし）：オペレーターとほとんど同じ権限を持っていますが、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、ジョブのプレビューを行うことはできません。

5. ソフトウェアセキュリティアップデート

5.1 セキュリティアップデートサービス

Fiery サーバーを最適に稼働させるためには、タイムリーなソフトウェア更新がきわめて重要です。どの印刷環境でも Fiery サーバーの安全を維持するには、Fiery および Windows オペレーティングシステムのソフトウェアセキュリティアップデートをインストールすることが重要です。

Fiery ソフトウェアをアップデートするには、Fiery サーバーが定期的に EFI クラウドサービスに接続して最新のアップデートを確認し、必要なアップデートをダウンロードします。

EFI は、次のような Fiery ソフトウェアアップデートを処理するための専用システムツールを備えています。

- Command WorkStation の Fiery アップデート：システム管理者は、承認を受けてリリースされた Fiery システムアップデートの通知、ダウンロード、およびインストールを取得します。
- Fiery Software Manager：このクライアントアプリケーションは、Fiery クライアントソフトウェアアプリケーションのアップデートを自動的に確認してダウンロードします。
- システムアップデート：この機能を使用すると、承認を受けてリリースされた Fiery システムアップデートの通知、ダウンロード、およびインストールを行うことができます。

5.2 Linux

Linux システムには、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。

5.2.1 Linux のウイルス対策ソフトウェア

組み込み型 Fiery サーバーで使用される Linux オペレーティングシステムは、Fiery サーバー専用の OS です。Fiery サーバーに必要な OS コンポーネントはすべて備えていますが、Ubuntu など、Linux システムの汎用目的コンポーネントの一部は含まれていません。この専用 OS は、性能が高く、汎用目的の Linux システムや Microsoft OS のようなウイルスに対する脆弱性もありません。汎用目的の Linux OS のためのウイルス対策ソフトウェアは、Fiery サーバー上では動作しない場合があります。

5.3 Windows 10

外付型 Fiery サーバーには、最新のセキュリティ保護機能が含まれている Windows 10 IoT Enterprise 2016 LTSB エディション（Windows 10）が搭載されています。

- Windows 10 には、ドメインに参加している Fiery サーバーへの中間者攻撃を軽減できる SYSVOL および NETLOGON 共有の SMB 強化が組み込まれています。
- Windows 10 では、メモリの悪用を防止するために、ヒープおよびカーネルプールのメモリ保護が強化されています。
- Windows Defender SmartScreen 機能を有効にすると、悪意のあるアプリケーションのダウンロードが防止されます。この追加のセキュリティ機能は、Fiery サーバーのパフォーマンスに影響を与える可能性があり、デフォルトではオフになっています。
- エンタープライズ証明書のピニングは、中間者攻撃の防止に役立ちます。これはエンタープライズ向けの機能です。この機能を有効にするには、Fiery サーバーをドメインに参加させる必要があります。
- Windows Defender Antivirus は、デバイスをウイルスやその他のマルウェアから保護します。Fiery サーバーではこの機能がオンになっていますが、パフォーマンスへの影響を最小限に抑えるために、デフォルトで e:\ ではなく c:\ をスキャンするよう設定されています。必要に応じて、e:\ をスキャンするように Windows Defender を設定してください。
- Windows プログラムとサービスに対する Windows データ実行防止（DEP）を有効化すると、マルウェアがメモリ操作手法を使用するのを防ぐことができます。

5.3.1 Microsoft Windows アップデート

Microsoft は、Windows 10 オペレーティングシステムの潜在的なセキュリティホールの問題に対応するために、定期的にセキュリティパッチを発行しています。Fiery サーバーの 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。アップデートを確認をクリックすると、自動アップデートが有効になり、アップデートが即座に開始されます。

5.3.2 Windows アップデートツール

Windows ベースの Fiery サーバーは、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 サーバーは、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。

5.3.3 Windows のウイルス対策ソフトウェア

Fiery サーバーでは、Microsoft のウイルス対策ソフトウェアである Windows 10 Defender を使用して、Fiery サーバーを保護します。通常は、Fiery サーバーで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、個別の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。

次に、お客様がウイルス対策ソフトウェアを選ぶ際の指針をいくつか示します。ウィルス対策ソフトウェアは、Fiery サーバー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 サーバーでも、リモート PC でウイルス対策ソフトウェアを起動し、Fiery サーバーの共有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。

Windows 向けウイルス対策ソフトウェアの各コンポーネントについて、EFI では次のガイドラインを示しています。

- **ウイルス対策エンジン**
  ウイルス対策エンジンが Fiery サーバーをスキャンする場合、スケジュールされたスキャンであるかどうかを問わず、Fiery の性能に影響を与えることがあります。
- **スパイウェア対策**
  スパイウェア対策プログラムは、ファイルが Fiery サーバーに追加されるときに Fiery 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 システムの更新時にファイルがダウンロードされたとき、Fiery サーバー上で実行されているアプリケーションの自動更新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 サーバーにはファイアウォールが備えられているため、通常は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組み込み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、このドキュメントのセクション 3.1 を参照してください。
- **スパム対策**
  Fiery では、E メール経由で印刷する機能、およびスキャンした結果を E メールに送信する機能がサポートされています。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 サーバーは、指定した E メールアドレスからドキュメントを印刷するように設定することもできます。Fiery サーバーでは、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必要ありません。
- **ホワイトリストとブラックリスト**
  ホワイトリストおよびブラックリスト機能は、通常は Fiery サーバーに悪影響を与えません。ホワイトリストおよびブラックリストを設定する場合は、Fiery モジュールの機能が阻害されないようにすることを強くお勧めします。
- **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 サーバー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、サーバー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、そして Fiery サーバーの設定（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）をあわせて確認する必要があります。

5.4 E メールウイルス

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 ファイルでない添付ファイルは、Fiery サーバーによって破棄されます。また、Fiery サーバーは、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。詳細については、このドキュメントのセクション 6.4 に示した、Fiery の E メール印刷ワークフローを参照してください。

6. データセキュリティ

6.1 重要な情報の暗号化

Fiery サーバー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 サーバーに保存できるようになります。NIST 2010 準拠の暗号アルゴリズムが使用されます。

6.2 標準印刷

Fiery サーバーに送信されたジョブは、Fiery サーバー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。Fiery サーバーでパスワードを有効にすることで、Fiery のオペレーターとシステム管理者のみが印刷できるようにユーザーを制限することができます。

6.2.1 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 サーバー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、Fiery 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 のハードドライブに保持されます。

送信順印刷キューでは、ネットワークから送られる特定のジョブを順番どお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 に送信された印刷ジョブは、さまざまな要因で、送信された順番どおりには印刷されないことがあります。たとえば、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。

6.2.2 印刷済みキュー

印刷キューに送信されたジョブは、印刷済みキューが有効な場合、印刷後に Fiery サーバーの印刷済みキューに格納されます。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。

6.2.3 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 サーバーの 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。ダイレクト接続を利用して送信されたすべてのジョブは、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、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経由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。

6.2.4 ジョブの削除

ジョブが Fiery サーバーから自動的に削除されたり、Fiery ツールを使用して削除されたりした場合、そのジョブは、Fiery ツールを使用して参照または取得できなくなります。ジョブが Fiery HDD にスプールされた場合は、ジョブの要素が HDD 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。

6.2.5 セキュア消去

セキュア消去機能を使用すると、Fiery 機能によってジョブが削除されたときに、送信されたジョブの内容が Fiery HDD から削除されます。削除時に、各ジョブのソースファイルが、米国防総省の仕様 DoD5220.22M に基づくアルゴリズムを使用して 3 回上書きされます。

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。

セキュアイレースには、次の制限や制約事項が適用されます。

- 次のような Fiery サーバー以外のシステムにあるジョブファイルには適用されません。
  - 別の Fiery サーバーに負荷分散されたジョブのコピー
  - メディアまたはネットワークドライブにアーカイブされたジョブのコピー
  - クライアントワークステーション上にあるジョブのコピー
  - 別のジョブに完全にマージまたはコピーされたジョブのページ
- エントリはジョブログから削除されません。
- ジョブの削除が完了する前に手動でシステムの電源がオフにされた場合、ジョブが完全に削除されないことがあります。
- この機能が有効になる前に削除されたジョブは、安全に削除されません。
- ディスクスワップによってディスクに書き込まれた可能性のあるジョブデータは削除されません。
- Windows OS での自動デフラグを無効にします。有効にした場合、OS はジョブデータをデフラグによって移動させることができます。その場合、元の場所にあるジョブデータの一部がセキュアイレースで上書きされないことがあります。
- FTP サーバーを通して送信されたジョブは、Fiery システムソフトウェアに送られる前に FTP クライアントに保存されることがあります。Fiery システムソフトウェアはこのプロセスを制御できないため、FTP クライアントが保存したジョブは安全に削除されません。
- SMB から印刷されたジョブは、Fiery のスプーラーを経由しますが、このときにジョブがディスクに保存されます。Fiery システムソフトウェアはこのプロセスに関与できないため、これらのジョブについては安全に削除することができません。

注意：ディスクスワップは、物理メモリよりも多くの仮想メモリを作成するために実行されます。この処理はオペレーティングシステムのレイヤーで行われるため、Fiery サーバーで制御できません。ただし、さまざまなメモリセグメントがメモリとディスク間でやり取りされるため、ディスクのスワップ領域は、オペレーティングシステムの操作によって定期的に書き換えられます。この処理により、一部のジョブセグメントが一時的にディスクに保存される場合があります

6.2.6 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 HDD 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。

6.3 セキュア印刷

セキュア印刷機能を使用した場合、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 サーバーに入力する必要があります。

この機能には、プリンターのコントロールパネルからアクセスする必要があります。この機能の目的は、(a) ジョブのパスワードを持っていて、(b) プリンターのコントロールパネルにローカルでそのパスワードを入力できるユーザーのみがドキュメントにアクセスできるようにすることです。

6.3.1 ワークフロー

ユーザーは、Fiery Driver 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 サーバー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、パスワードを入力するまで保留状態となります。

注意：セキュア印刷パスワードが設定されて送信されたジョブは、Fiery Command WorkStation から参照することはできません。

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を表示してパスワードを入力します。パスワードを入力すると、ユーザーは、このパスワードが設定されて送信されたジョブにアクセスして、そのジョブの印刷や削除を行えます。

印刷されたセキュアジョブは、印刷済みキューに移動しません。このジョブは、印刷終了後、自動的に削除されます。

6.4 E メール印刷

この機能では、Fiery サーバーは 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 サーバー上に、許可された E メールアドレスのリストを格納できます。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。システム管理者は、E メール印刷機能をオフにできます。E メール印刷機能は、デフォルトでオフになっています。

6.5 ジョブ管理

Fiery サーバーに送信されたジョブは、システム管理者またはオペレーターとしてのアクセス権を持つユーザーが Fiery のジョブ管理ユーティリティを使用した場合にのみ操作できます。

6.6 ジョブログ

ジョブログは、Fiery サーバーに格納されます。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。ジョブログを使用すると、Fiery サーバーのジョブアクティビティを検査できます。

オペレーターとしてのアクセス権を持つユーザーは、Fiery 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、Fiery Command WorkStation からジョブログを削除できます。

6.7 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 サーバーは、Fiery Configure ツールから、または Fiery QuickTouch インターフェイスの設定機能から設定できます Fiery Configure ツールは、Fiery WebTools および Fiery Command WorkStation から起動できます。

6.8 スキャン

Fiery サーバーでは、複写機のガラス面に置いたイメージをスキャンし、Fiery TWAIN プラグインを使用して、スキャンを開始したワークステーションに直接取り込むことができます。このプラグインは、Adobe® Photoshop および Textbridge アプリケーションでサポートされています。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、ドキュメントを Fiery サーバーにスキャンして、配布、保管、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 サーバーを設定できます。スキャンジョブは、次の方法で配信できます。

- E メール：このプロセスでは、E メールがメールサーバーに送信され、メールサーバーから適切な宛先にルーティングされます。注意：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 HDD に保存され、URL からアクセスできます。
- FTP：ファイルは FTP の宛先に送信されます。宛先を含む転送レコードは FTP ログに保持され、LCD 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 待機キュー：ファイルは Fiery 待機キュー（上記セクション 6.2.1 参照）に送信されて、スキャンジョブとしては保持されません。
- 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 サーバーに保管されます。保管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。一部のバージョンの Fiery サーバーでは、パスワードも必要です。スキャンジョブは、URL を通して取得できます。

7. Fiery のセキュア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 サーバーを設定する際に、セキュリティを向上させるのに役立ちます。

- 組織内のパスワードポリシーに準拠するように、セキュリティで Fiery システム管理者のデフォルトのパスワードを変更します。
- ネットワーク -> SNMP の SNMP：
  （a）最高セキュリティを選択した場合、Fiery サーバーでは SNMP v3 のみがサポートされます。
  （b）SNMP マネージャーが SNMP v1/v2c でのみ動作する場合は、デフォルトの読み取り用のコミュニティ名を変更します。
- ジョブ送信での FTP 印刷は、不要な場合、無効にします。
- 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。
- ポートをブロックします（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 を選択解除します）。

OS レベルでの保護のほかに、Fiery サーバーには、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。

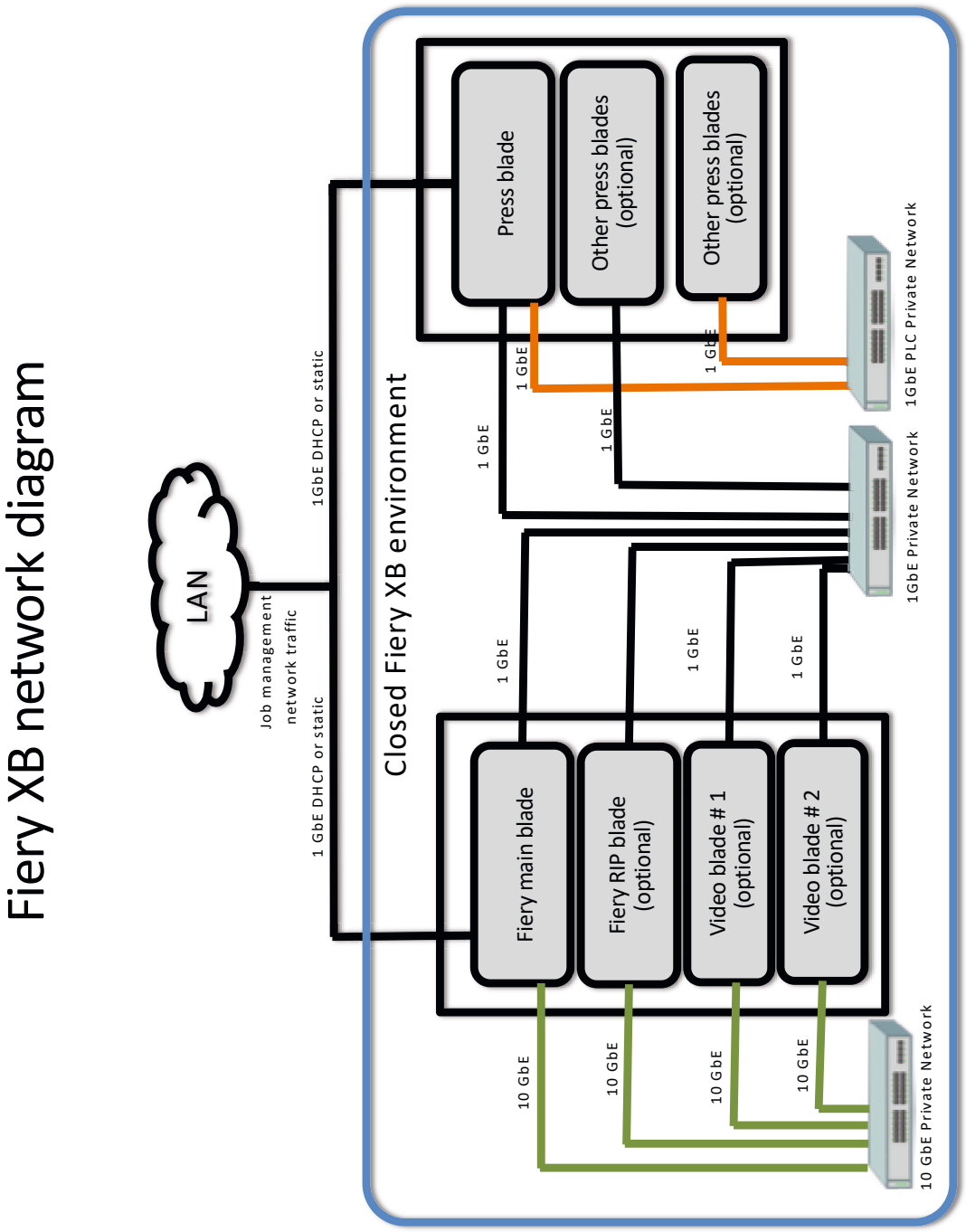
- Fiery サーバーには、ユーザーが印刷したものをユーザー自身が確実に回収できるセキュア印刷機能があります。
- Fiery は、主要なジョブアカウンティングソリューションと統合して、フォローミー印刷を使用してセキュリティを強化することができます。

システム管理者は、インストール時にパスワードを変更することをお勧めします。また、組織の IT ポリシーに従って、定期的にパスワードを変更することを強くお勧めします。システム管理者パスワードを使用してログインすると、ローカルまたはリモートクライアントから Fiery サーバーのすべての機能にアクセスできます。ファイルシステム、システムのセキュリティポリシー、レジストリのエントリなどへのアクセスが可能になります。さらに、システム管理者パスワードを使用してログインした場合は、システム管理者パスワードを変更して、他のユーザーが Fiery サーバーにアクセスできないようにすることもできます。

8. まとめ

Fiery サーバーは、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を備えています。EFI は、お客様のビジネスの効率性を最大限向上させ、Fiery サーバーを悪意のある使用や意図しない使用による脆弱性から効果的に保護するための施策に力を入れています。そのため、EFI では、Fiery サーバーに包括的で信頼できるセキュリティソリューションを提供する新しいテクノロジーを日々開発しています。

付録 1


Fiery XB network diagram
LAN
Job management network traffic
1GbE DHCP or static
1 GbE DHCP or static
Closed Fiery XB environment
Press blade
Other press blades (optional)
Other press blades (optional)
Fiery main blade
Fiery RIP blade (optional)
Video blade # 1 (optional)
Video blade # 2 (optional)
1 GbE
10 GbE
1GbE PLC Private Network
1GbE Private Network
10 GbE Private Network

付録 2

Windows 10 IoT Enterprise 2019 LTSC

2019 年以降、一部の Fiery サーバーには、オペレーティングシステムとして Windows 10 IoT Enterprise 2019 LTSC が搭載されています。

この Windows エディションには、最新のセキュリティ保護と、Windows 10 バージョン 1703、1709、1803、および 1809 で提供された累積的な機能強化が含まれています。

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。

注意：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 サーバー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。

EFIはお客様のビジネスの発展をお手伝いします

EFIは看板・パッケージ・繊維製品・セラミックタイル・パーソナライズされた書類の制作のための革新的テクノロジーを開発しています。EFIの提供する様々なプリンター・インク・デジタルフロントエンド・総合的ビジネスソリューション及び生産ワークフローにより、生産プロセスを改良・簡素化することで、印刷業界で圧倒的な競争力と高い生産性を手に入れることができます。詳細は： http://www.efi.co.jp まで。

FTL_061.06.20_JP