Fiery FS700 Pro/FS700 servers

Security White Paper

45266132

2025 年 12 月 8 日

目次

はじめに

このドキュメントでは、Fiery サーバーのセキュリティ機能の概要について説明します。IT 管理者およびセキュリティ専門家に向けて、Fiery ソリューションが印刷環境をどのように保護しているかを伝えることが目的です。データの保護、ネットワークセキュリティの強化、システムの完全性維持のために Fiery サーバーで使用している原則や仕組みについて説明しています。

セキュリティの原則

Fiery servers は、業界のベストプラクティスに準拠するように細心の注意を払って設計されており、データ保護規制および企業のセキュリティ要件へのコンプライアンスを確保しています。この設計の基本原則は次のとおりです。

- データ保護：保存時と送信時のデータ暗号化
- ネットワークセキュリティ：アクセス制御、安全な通信プロトコル、認証メカニズム
- システムの完全性：ファームウェア検証、セキュアブート、セキュリティアップデート

Fiery はグローバルパートナーおよびサプライヤーと協力して、脅威が進化する中でも継続的なサポートを提供します。包括的なシステムセキュリティを確保するために、エンドユーザーは、Fiery のセキュリティ機能を自社のセキュリティポリシーと統合し、強固なパスワードや堅牢な物理的セキュリティ対策の実装を含む業界のベストプラクティスを遵守することを推奨します。

認証とアクセス制御

Fiery サーバーは、次のような複数の認証方法をサポートしています。

- ロールベースのアクセス制御（RBAC）
- LDAP/Active Directory との統合
- シングルサインオン（SSO）を利用して実装された多要素認証（MFA）

ユーザー認証

認証機能により、Fiery サーバーは次の機能を実行できます。

- 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 3 つのユーザー認証方式をサポートしています。

- Fiery サーバーで定義されているユーザーのローカル認証
- 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）
- 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、システム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。

グループ権限

Fiery サーバーは、所属するグループ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、カラー印刷やグレースケール印刷などの特定の権限セットが割り当てられています。グループメンバーは、与えられた権限の範囲内でのみアクションが可能です。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。

このユーザー認証方式で、グループごとに選択できる多様な権限は以下のとおりです。

- 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。この権限を持たないユーザーの場合、Fiery サーバー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 サーバーのカラー印刷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、ジョブの印刷は失敗し、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 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。

権限を強化されたシステム管理者は、これらの機能をカスタマイズして、不正アクセスを制限し、組織のセキュリティプロトコルを強制適用できます。

ローカルユーザー

Fiery サーバーソフトウェアは、Windows のユーザーやロールとは異なる、固有のユーザータイプと連携します。Fiery システム管理者は、初期インストールの直後にすべてのデフォルトパスワードを速やかに変更する必要があります。Fiery サーバーへのパスワードアクセスは厳重に管理する必要があります。

- **Configure** > **セキュリティ**を使用する場合、システム管理者およびオペレーターパスワードの最大文字数はともに 64 文字です。
- **Configure** > **ユーザーアカウント**を使用する場合、ローカルユーザーアカウントパスワードの最大文字数はともに 64 文字です。
- 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**で変更できます。

ローカル 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 サーバーの全機能を完全に管理でき、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、サーバーの設定とジョブログの削除は行えません。
- プレスオペレーター（Fiery XB サーバーのみ）：システム管理者によって付与された特定の権限を持ち、プレス上のジョブを管理します。
- Fiery サービス管理者（Windows サーバーのみ）：信頼済み証明書をインストールするための非表示アカウントで、Fiery サーバーにはログインできません。ネットワークスキャンツールには表示されますが、削除可能です。
- Fiery_SMB_ユーザー：デフォルトの Windows 印刷（SMB）アカウントで、ネットワークコンピュータを介して Fiery サーバーの印刷キューを表示します。
- 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、ジョブの編集、ステータス変更、プレビューは行えません。

LDAP 認証

Fiery サーバーは、企業内サーバーとの通信に LDAP バージョン 3（RFC 2251 準拠）を使用します。LDAPv3 を介して、スキャン機能向けのユーザーの電子メールアドレスや認証のためのユーザーおよびグループ情報を取得します。この機能は、Active Directory サーバーへの LDAP 接続の場合にのみサポートされます。

Fiery サーバーは、LDAP を使用して次の認証方法をサポートします。

- 自動
- SIMPLE
- GSSAPI

次の表に、さまざまな LDAP 認証方法を示します。

認証方法	説明	Active Directory サーバー
自動	LDAP サーバーがサポートする認証方法に基づいて、GSSAPI または SIMPLE を選択するオプションです。	サポート対象
SIMPLE	パスワードが必要です。LDAP over TLS が選択されている場合、パスワードは TLS で暗号化されます。	サポート対象
GSSAPI	この方法では、パスワードの代わりに Kerberos チケットが使用されるため、TLS は不要です。	サポート対象

シングルサインオン（SSO）

Fiery FS700 Pro サーバーは、Microsoft Entra ID（旧 Azure Active Directory）を使用したクラウドベースのシングルサインオン（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 Entra ID の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 管理方式により、Fiery サーバーはユーザーのパスワードをローカルに保存しないため、セキュリティが大幅に強化されます。

データセキュリティ対策

機密情報を保護するため、Fiery サーバーには次の対策が実装されています。

暗号化されたストレージ：印刷ジョブと設定データの保護

重要な顧客データを暗号化することで、パスワードや関連する設定情報を Fiery サーバー上で安全に保存します。これらの重要な情報は、最新のセキュリティ標準に準拠した AES-256 や SHA-2 などの暗号化アルゴリズムを使用して暗号化またはハッシュ化されます。

ディスク上に保存された顧客データは、ディスクを Fiery サーバーから取り外した場合でもアクセスできません。ユーザーデータの暗号化は、Windows ベースの Fiery サーバーでは有効または無効にできます。Linux ベースの Fiery サーバーでは暗号化機能が常に有効になっています。

データ復旧用のパスフレーズを忘れた場合、Fiery 側ではリセットできず、ソフトウェアを完全に再インストールする必要があります。

また、Windows ベースのサーバーでは、オペレーティングシステムを含むブートドライブを暗号化するオプションもあります。この暗号化により、Fiery サーバーへのオフライン攻撃を防ぎ、ブートドライブが別のデバイスで使用されることを防ぎます。

セキュアイレース：削除後にデータ復元を確実に防止する

Linux ベースの FS700 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。

この機能は、E600 および LX Pro ハードウェアプラットフォームを使用する組み込み型 Fiery サーバーではサポートされていません。これらのプラットフォームは、AES-256 方式で暗号化されたソリッドステートドライブ（SSD）に書類データを保存します。この暗号化は常に有効になっており、無効にはできません。

Windows ベースの FS700 Pro サーバーは、NIST 800-88 データ抹消処理（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。

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。

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

ワークフロー	セキュアイレース
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	×

ネットワークセキュリティ

Fiery サーバーは、ネットワーク通信を保護するために次のセキュリティメカニズムを採用しています。

- IP フィルタリングとポート管理
- ファイアウォールの構成
- SNMP v3 のサポートにより、安全なネットワーク監視および管理ツールを実現

サポートされているネットワークプロトコル

FS700/FS700 Pro は、業界標準のネットワークプロトコルを幅広くサポートしており、多様な環境での互換性、セキュリティ、効率的な通信を確保します。この機能には以下が含まれます。

- **コアプロトコル：**TCP/IP、IPv4、IPv6
- **Web プロトコル：**HTTP/1.1、HTTPS（TLS 1.2/1.3）
- **ファイルおよび印刷サービス：**FTP、LPR、IPP 2.0、SMB v2、SMB v3、ポート 9100
- **管理と監視：**SNMP v1、v2c、v3
- **リモートアクセス：**RDP（Windows ベースのサーバーのみ）
- **セキュリティと認証：**IPSec（IKEv2）、LDAP v3、IEEE 802.1X
- **ネットワークサービス：** DHCP、DNS
- **検出プロトコル：**WSD、Bonjour、SLP

ネットワークポート

デフォルトでは、未使用の TCP/IP ポートはすべて無効化されています。Fiery システム管理者は、ネットワークポートを有効または無効にできます。ポートを無効にすると、その特定のポートを使用する必要がある外部接続が効果的に防止されます。

インバウンドポート

Fiery サーバーは、受信ネットワーク接続を監視し管理しており、許可されたトラフィックのみがサーバーにアクセスできるようにすることで、不正アクセスや攻撃からサーバーを保護しています。

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

TCP/IP	UDP	ポート名	ポートを利用するサービス
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。NetBIOS は安全性が低いため、これらのポートはデフォルトで閉じられています。
	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を指します。このポートはデフォルトでブロックされています。SLP は安全性が低いためです。
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 ベースの Fiery サーバーのみ）
3702	3702	WS-Discovery	Web Services for Devices（WSD）。WSD を介して Fiery サーバーの検出と印刷を可能にします。
	4500	IPsec NAT トラバーサル	IPSec
	5353	マルチキャスト DNS（mDNS）	Bonjour
6310		DMP ポート	ダイレクトモバイル印刷
8010		FIERY のポート	JDF
8021～8022		FIERY のポート	Fiery Harmony、Fiery HotFolders、Fiery Command WorkStation
8090		FIERY のポート	OFA
9100～9103		印刷ポート	ポート 9100
	9906	FIERY のポート	Harmony 検出
21030		FIERY のポート	Fiery Image Viewer

メモ：IPSec ポート（500 および 4500）は、FS700（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。無効なポートに依存するサービスは、リモートアクセスができません。

また Fiery システム管理者は、Fiery サーバーが提供するさまざまなポート依存サービスを有効化または無効化できます。

アウトバウンドポート

Fiery サーバーは、アウトバウンドネットワークトラフィックを管理および制限して、許可された通信のみがデバイスから外部に発信されるようにします。これにより、外部の脅威にさらされるリスクを低減します。

アウトバウンドポート	目的	デフォルト/オン設定
53	DNS	デフォルト
67	DHCP	デフォルト
80、443	Fiery System アップデート、JDF、PrintMe、その他のクラウド通信	デフォルト
161、162	SNMP	デュアル IP 構成時
21	FTP スキャン	オン設定
123	NTP	オン設定
389/636	LDAP サービス	オン設定
445	スキャンして SMB に送信/JobLog を SMB に送信/JDF 共通グローバルパス	オン設定
500/4500	IPSEC	オン設定
8080/8443	HTTP/HTTPS/FTP プロキシポート	オン設定

クラウドサービスとの通信

このリストは、外部のクラウドベースサービスとの通信が必要な Fiery サービスおよびアプリケーションを列挙しています。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がこれに該当します。このドキュメントは、すべての外部通信を無効にしている顧客が、社内ファイアウォールの例外設定を試みている場合に特に役立ちます。

Fiery サービス/アプリケーション	完全修飾ドメイン名	ポート	サーバー所在地	利用用途
システムアップデート	https://liveupdate.fiery.com/des/hypatia.asmx	443	Fiery	Fiery セキュリティアップデートのダウンロード
OFA	https://flexlicensing.fiery.com	443	Fiery	ライセンスアクティベーション
IQ	https://iq.fiery.com/iq	443	AWS	Fiery IQ クラウド
LINQ	https://ews.fiery.com	443	Azure	分析

Fiery サービス/アプリケーション	完全修飾ドメイン名	ポート	サーバー所在地	利用用途
ユニバーサルプリント	複数のドメイン： • portal.azure.com • print.print.microsoft.com • notification.print.microsoft.com • discovery.print.microsoft.com • graph.print.microsoft.com	80/443	Azure	IPP プロキシとユニバーサルプリントサービス
SSO	login.microsoft.com	80/443	Microsoft	シングルサインオン
Windows Server Update Services（WSUS）	複数のドメイン： • http://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://.delivery.mp.microsoft.com • https://.delivery.mp.microsoft.com	80/443	Microsoft	Windows アップデート
Command WorkStation	複数のドメイン： • https://help.fiery.com • https://learning.fiery.com • https://communities.fiery.com/s/ • https://liveupdate.fiery.com • https://iq.fiery.com	443	Fiery	

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、事前に定義された IP アドレスに基づいて Fiery サーバーへの接続要求を制御できます。デフォルトポリシーを定義することで、システム管理者は受信データパケットを許可するか拒否するかを指定できます。さらに、最大 16 個の IP アドレスまたは範囲ごとにフィルターを作成し、それに応じて接続要求を許可または拒否できます。

各 IP フィルター設定では、IP アドレスまたは IP アドレスの範囲および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る送信元からのパケットは破棄されます。一方アクションが許可された場合は、パケットは受け入れられます。

ネットワーク認証

SNMP v3

Fiery サーバーは最新の SNMPv3 標準に対応しており、通信パケットの暗号化を促進することで、機密性、メッセージの完全性、認証を保証します。

Fiery システム管理者は、SNMP のセキュリティレベルを低、中、高という 3 つのレベルから選択できます。これらのレベルでは、パスワードは SHA-1 や SHA-256 などのアルゴリズムでハッシュ化され、SNMP メッセージ全体が暗号化されます。さらに、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構成できます。

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 標準であり、ローカルネットワークとそのリソースにアクセスする前にデバイスが認証されるようにします。Fiery サーバーでは、サーバーベース認証用に EAP MD5 Challenge または PEAP MSCHAPv2 を、さらに強化されたセキュリティを実現する証明書ベース認証用に EAPTLS を使用するように 802.1X を設定できます。Fiery サーバーは、EAP-TLS 証明書ベースの認証でユーザー証明書（デバイス証明書はサポートしない）のみをサポートします。

Fiery サーバーは、起動時またはネットワーク接続が切断された後に再接続されるたびに、認証を実行します。

ネットワーク暗号化

インターネットプロトコルセキュリティ（IPsec）

IPsec は、ネットワークレイヤーで各パケットを暗号化および認証することにより、IP ベースの通信のセキュリティを強化し、IP を使用するすべてのアプリケーションの通信データを保護します。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 を介した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 を利用した通信が確立されると、印刷ジョブを含むすべての通信がネットワーク上で安全に送信されます。

HTTPS

Fiery サーバーは、クライアントとサーバーコンポーネント間の安全な通信を HTTPS over TLS によって保護します。これにより、印刷ジョブ、ジョブ状況の更新、管理コマンドなど、送信されるすべてのデータが転送中に暗号化され、傍受や改ざんから保護されます。Fiery サーバーは TLS 1.3 と TLS 1.2 に対応しており、強力な暗号化保護と最新のセキュリティ機能を提供します。WebTools および Fiery API への接続には HTTPS が必須であり、管理および運用トラフィックの安全な送信を保証します。

証明書管理

Fiery サーバーは、TLS 通信中に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ています。Fiery サーバーは、4096、3072、2048 ビット長の RSA キーを使用して、Base64 でエンコードされた PEM 形式の X.509 証明書をサポートします。

Fiery システム管理者は、証明書管理により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生成
- Fiery サーバーの証明書およびそれに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

自己署名デジタル証明書は暗号化を提供しますが、自動的な信頼検証は行われません。安全な展開のためには、適切な ID 検証を行うために、信頼できる認証局（CA）によって発行された証明書の使用を推奨します。

信頼できる CA により署名された証明書は、WebTools の Configure セクションから Fiery サーバーにアップロードできます。

サーバーメッセージブロック（SMB）

SMBv1 は、ファイルとプリンター共有のための従来のプロトコルですが、既知のセキュリティ脆弱性により、Fiery サーバーでは無効化されています。Fiery サーバーは、SMBv2 と SMBv3 をサポートしています。SMB 署名が強制され、中間者攻撃を防ぐためにすべてのパケットがデジタル署名されます。SMB 認証が有効な場合、ユーザーは共有フォルダーやコンテンツにアクセスするために有効なユーザー名とパスワードを入力する必要があります。また、ゲストアカウントに対する SMB 経由の印刷やファイル共有も、Fiery Configure でパスワードを設定することにより制限可能です。

ハードウェアセキュリティ

Fiery サーバーは、エンタープライズグレードのハードウェアセキュリティを念頭に設計されています。機密情報の保護は、ソフトウェア制御に限らず、ハードウェアコンポーネントもシステムの完全性とデータの機密性を維持する上で重要な役割を果たします。主要なハードウェア要素とそのセキュリティ対策の概要を以下に示します。

揮発性メモリ（RAM）

Fiery サーバーは、アクティブな操作中に一時的にデータを格納するために揮発性メモリ（RAM）を使用しています。データ漏洩のリスクを軽減するには、次の対策が講じられています。

- RAM 内の機密情報は、使用後またはシステムのシャットダウン時に直ちに消去されます。
- 残留データが残らないように、メモリスクラビング技術が適用されます。
- プロセッサーとオペレーティングシステムによる特権分離により、RAM へのアクセスが制限されます。

不揮発性メモリとデータストレージ

不揮発性メモリにはハードドライブ、ソリッドステートドライブ（SSD）、その他の永続的ストレージが含まれ、システムの電源がオフになってもデータを保持します。セキュリティ対策としては、以下が挙げられます。

- 保存されたデータを保護するためのユーザーデータ暗号化（UDE）
- ファイルが削除されたときに機密情報を復元不能にする安全な削除方法

フラッシュメモリ

フラッシュメモリは、ファームウェア、設定ファイル、システム設定の保存に使用されます。セキュリティを維持するために、以下が実施されています。

- 改ざん防止のためのファームウェアのデジタル署名
- インストール前の暗号チェックサムによるファームウェア更新の検証
- 実行時における不正な変更を防止するための書き込み保護メカニズム

CMOS および NVRAM

ハードウェア構成やブート設定などの重要なシステムパラメーターは、CMOS と不揮発性 RAM（NVRAM）に保存されます。このデータを安全に保護するために、以下の対策が講じられています。

- アクセスは、許可された管理プロセスに制限されています。
- セキュアブートメカニズムにより、信頼されたファームウェアのみがこれらの領域を読み書きします。
- 重要な NVRAM 変数はバックアップされ、完全性がチェックされており、破損や悪意のある改変を防止しています。

ストレージドライブ

Fiery サーバーは、オペレーティングシステムとシステムファイルの保存にストレージドライブを使用します。これらのドライブは、ジョブのスプール、ログ、一時ファイルにも使用されます。

顧客データを保護するために、次のセキュリティ機能が提供されています。

- ドライブレベルの暗号化
- アクセス制御リスト (ACL) による許可されていない読み取り/書き込み操作の制限
- ディスクドライブセキュリティキット（外部 Fiery サーバー用オプション）による通常操作中のサーバードライブの安全にロックを通じたシステムのセキュリティ強化

物理ポート

USB、ネットワークインターフェイス、サービスコネクターなどの物理ポートは、不正アクセスの潜在的な経路となります。Fiery のハードウェアセキュリティは、このリスクに対して次の対策を講じています。

- 未使用ポートをハードウェアレベルまたはファームウェアレベルで無効化
- 外部デバイスを接続する際に管理者権限を要求
- 重要な物理インターフェイスとのすべてのやり取りを監視およびログに記録

これらのハードウェアセキュリティ対策をソフトウェアおよびネットワーク保護と組み合わせることで、Fiery サーバーは包括的な多層防御戦略を提供し、印刷環境における機密データの機密性、完全性、および可用性を確保します。

システムの完全性と安全なアップデート

システムの完全性を維持することは、セキュリティを確保するために最も重要です。Fiery サーバーは、次のサポートを提供しています。

- セキュリティ監査ログ
- セキュアブート：信頼済みソフトウェアのみがロードされることの保証
- デジタル署名付きアップデート：ソフトウェアアップデートの改ざんを防止
- 自動化されたセキュリティアップデート管理：セキュリティアップデートの適用プロセスを簡素化

セキュリティ監査ログ

権限を強化されたシステム管理者は、セキュリティ監査ログに記録されたセキュリティイベントにアクセスして精査することができます。このログはデフォルトで有効です。

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。システム管理者に警告や通知は届きません。代わりに、静的なログとして表示されます。

このログは、一般的にログの収集や分析に用いられるセキュリティ情報およびイベント管理（SIEM）ツールと互換性のあるフォーマットで作成されています。キャプチャされたすべてのイベントデータは、NIST SP 800-53 で概説されている基準に準拠しています。

Fiery システム管理者は、Fiery の介入を必要とせずセキュリティ監査ログにアクセスできます。Linux ベースのサーバーのログは、Syslog 形式（RFC 5424 または RFC 3164）で提供されます。Windows ベースのサーバーの場合、ログは標準の Windows EVTX フォーマットで保存され、Windows イベントログマネージャーや、Windows イベントログ API を使用する多くの利用可能な市販のソリューションで閲覧可能です。Linux ベースの Fiery サーバーには、Syslog などの中央集約型の収集システムにログを転送するオプションも提供しています。

セキュリティログの保管期間は、割り当てられたローカルストレージ容量に依存します。ログサイズが事前設定された記憶域（400MB）を超えると、古いイベントから順に自動的に削除されます。

セキュアブート

この機能は、デジタル署名され信頼されたコンポーネントのみが読み込まれるようにすることで、起動時にオペレーティングシステムのファイルの完全性を確保します。Fiery サーバーでは、起動中に不正なコードや悪意のあるコードが実行されるのを防ぎ、セキュリティを強化し、侵害のリスクを低減します。デフォルトでは、セキュアブートが無効になっています。

デジタル署名付きアップデート

Fiery サーバーは、すべてのソフトウェアおよびファームウェアについてインストールの完全性と真正性を確保するため、デジタル署名されたアップデートを使用しています。各アップデートは、Fiery またはその認定パートナーによって暗号的に署名されており、サーバーは内容の変更または改ざんがないことを検証できます。このプロセスにより、悪意のあるコードの混入が防止され、信頼できるアップデートのみが適用されることが保証されるため、システムのセキュリティと信頼性が維持されます。

自動化されたセキュリティアップデート管理

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。すべて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、あらゆる印刷環境で Fiery サーバーの安全性を維持する上で重要です。

Fiery システムアップデートは、Fiery サーバーでオプションが有効になっている場合、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。

Microsoft® Windows™ OS セキュリティの脆弱性については Microsoft によって直接管理され、使用可能になり次第 **Windows 更新プログラム**を通じてお客様に配布されるため、本書では詳細を記載しません。

マザーボード、プロセッサー、ファームウェアなどのコア 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対応するため、Fiery は製造元と緊密に連携し、必要なセキュリティアップデートを入手しています。これらのセキュリティアップデートは、その後、必要に応じてお客様に提供されます。

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 サーバーソフトウェアのセキュリティアップデート

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。最新の Fiery サーバーソフトウェアのセキュリティアップデートを適用することで、システムの完全性が保たれ、脆弱性が軽減されることで業界のセキュリティ標準への準拠が維持されます。

Fiery サーバーセキュリティチームは、次のような信頼できる複数の情報源の包括的なネットワークを通じて、セキュリティの脆弱性を注意深く監視および追跡しています。

- 米国サイバーセキュリティ・インフラストラクチャセキュリティ庁 (CISA) の警告とアドバイザリ
- 米国国立標準技術研究所（NIST）の国立脆弱性データベース
- 共通脆弱性識別子（CVE）レコード
- ソフトウェアおよびハードウェアの脆弱性に関する CERT コーディネーションセンター（CERT/CC）のレポートとアドバイザリ
- 地方自治体および規制当局
- ソフトウェアおよびハードウェアベンダーのセキュリティアドバイザリ

Fiery では、共通脆弱性評価システム（CVSS）によって決定される重大度（重大、高、中、低）に基づいてセキュリティ修正に優先順位を付けます。これらの修正プログラムは、OEM パートナーから対応する承認を得た後にリリースされます。承認後、Fiery ソフトウェアセキュリティアップデートはダウンロード可能になります。すべての Fiery ソフトウェアアップデートは、マルウェアの混入を含む不正な改変を防ぐために、Secure Hash Algorithm（SHA-2）を使用してデジタル署名が行われています。

有効にすると、Fiery システムアップデートは Fiery サーバー上でセキュリティアップデートを自動的にダウンロードしてインストールします。デフォルトでは、このオプションが有効になっており、顧客にはこの状況を維持することを強くお勧めします。

コンプライアンスとベストプラクティス

堅牢なセキュリティの実装は、次のような基本的な業界標準と規制フレームワークに準拠しています。

- 一般データ保護規則（GDPR）、EU データ法
- ISO/IEC 27001（FS700 Pro のみ）
- FIPS 140-2
- NIST 800-88、媒体のデータ抹消処理（サニタイズ）に関するガイドライン（FS700 Pro のみ）
- NIST 800-52、トランスポート層セキュリティ（TLS）実装の選択、構成、および使用のためのガイドライン
- NIST 800-171、非連邦政府組織およびシステムにおける管理対象非機密情報 CUI の保護（FS700 Pro のみ）
- 米国国防総省によるサイバーセキュリティ成熟度モデル認証のフレームワーク（CMMC）レベル 2：管理された非機密情報（CUI）の広範な保護（FS700 Pro のみ）
- NIST 800-193、プラットフォームファームウェアのレジリエンスに関するガイドライン（FS700 Pro のみ）
- NIST 800-53、組織と情報システムのためのセキュリティおよびプライバシー管理策
- 汎用オペレーティングシステムのコモンクライテリアプロテクションプロファイル（FS700 Pro のみ）

セキュリティ体制強化のため、IT 管理者は次の対策を取ることが求められます。

- セキュリティアップデートの定期的な適用
- 強固な認証ポリシーの適用
- 定期的なセキュリティ監査の実施
- 印刷環境におけるネットワーク分離の実施

セキュアな Fiery サーバー設定のためのガイドライン

Fiery システム管理者は、Fiery サーバーの設定時にセキュリティを強化するために、次のガイドラインに従うことができます。

管理者パスワードの変更

Fiery サーバーは工場出荷時に、システム管理者アカウント用のデフォルトパスワードが設定されています。このパスワードにより、ローカルおよびリモートクライアントの両方から Fiery サーバーへの完全なアクセスが可能となります。このアクセスには以下が含まれますが、これに限定されるものではありません。

- ファイルシステム（Windows 上の Fiery サーバーのみ）
- システムのセキュリティ設定
- アプリケーション設定
- レジストリエントリ

インストール後すぐにデフォルトのパスワードを変更し、その後も組織のセキュリティポリシーに従い定期的に Fiery 管理者パスワードを変更することを強く推奨します。Fiery 管理者パスワードは、Fiery プラットフォーム内で変更する必要があります。

安全で効率的な運用のベストプラクティス

- セキュリティを最大限に高めるために、SNMP をバージョン 3 に限定する
- WSD が印刷ワークフローで使用されることを防止するためにジョブ送信用の WSD を無効化する
- 明示的な必要性がない限り、Windows 印刷プロトコル（LPR、ポート 9100、IPP）を無効に化する
- 未使用のポートをブロックしてリスクを軽減するために TCP/IP ポートフィルタリングを有効化する
- Windows 印刷またはファイル共有も必要がない限り、ポート 137〜139 および 445 を閉じる
- セキュリティで保護されていない通信を防止するためにポート 80 の HTTP を無効化する
- ジョブの所有者のみが印刷ジョブをリリースできるようにセキュア印刷を有効化する

高度なセキュリティ環境

権限を強化されたシステム管理者は、**WebTools** > **Configure** > **セキュリティ**内で使用可能な高セキュリティプロファイルを選択することで、高度なセキュリティ設定を簡単に構成できます。

まとめ

Fiery サーバーは、強固なセキュリティ機能を備えていますが、インターネットに接続することを目的として設計されているわけではありません。そのため、ネットワーク管理者によってアクセスが厳密に制御された安全なネットワーク環境内に導入する必要があります。最新の業界標準に準拠して構築された Fiery サーバーは、エンタープライズグレードのセキュリティを提供し、進化するサイバー脅威から印刷環境を保護します。システム管理者は、Fiery のセキュリティ機能をフルに活用することで、コンプライアンスを確保し、機密データを保護することができます。

FS700、FS700 Pro の新機能

- セキュリティの脆弱性に対応するため、コアシステムモジュールがアップデートされました。
- E メール経由の攻撃を防ぎセキュリティ規制への対応を強化するために、E メール機能が廃止されました。
- Fiery サーバーとのすべての通信を TLS 1.3 で暗号化できるようになりました。Windows 10 を実行している Fiery サーバーへのリモートデスクトップ接続は、現在 TLS 1.2 をサポートしています。
- 次の Fiery アプリケーションおよびモジュールに、TLS 1.3 のサポートが追加されました。
  - サーバーおよびクライアントコンポーネントのライセンス管理
  - IPP プロキシ：Microsoft ユニバーサルプリントに必要
  - 802.1x ネットワーク認証プロトコル
  - EFI LINQ：Fiery サーバーのクラッシュレポート用
  - JDF
  - システムアップデート
  - FCC‐Fiery Cloud Connector
- Linux サーバーで使用されていた IPsec ツールが、より安全な新しいツールに刷新されました。
- SNMPv3 通信に Advanced Encryption Standard（AES）のサポートが追加され、AES 128 が新しいデフォルトになりました。
  - AES 128（デフォルト）
  - AES 192（Configure からユーザーが選択可能）
  - AES 256（Configure からユーザーが選択可能）
  - DES も引き続きサポートされていますが、デフォルトのオプションではなくなりました。必要に応じてユーザーが選択できます。