FUJIFILM

監査ログリファレンスガイド

もくじ

2021 年 9 月　GM1038J1-2 第 1 版　富士フイルムビジネスイノベーション株式会社

はじめに

このたびは、弊社製品をお買い上げいただき、まことにありがとうございます。

本書は、本機を管理するシステム管理者および機械管理者を対象に、監査ログの概要および監査ログの記録項目について説明しています。本機を使用する前に必ずこのマニュアルをお読みください。このマニュアルは、読み終わったあとも必ず保管してください。

なお、本書の内容は、お使いのパーソナルコンピューターの環境や、ネットワーク環境の基本的な知識や操作方法を習得されていることを前提に説明しています。お使いのパーソナルコンピューターの環境や、ネットワーク環境の基本的な知識や操作方法については、パーソナルコンピューター、オペレーティングシステム、ネットワークシステムなどに付属の説明書をお読みください。

富士フイルムビジネスイノベーション株式会社

本書の使い方

本書は、監査ログの機能やフォーマットについて記載しています。

本書の構成

本書は、次の構成になっています。

1 監査ログの概要

監査ログの概要、監査ログの機能について説明しています。

2 監査ログの保存項目

監査ログの記録項目について説明しています。

本書の表記

- 本文中では、説明する内容によって、次のマークを使用しています。

注記
- 必ず知っておいていただきたい情報、操作するときに必ず確認していただきたい情報を記載しています。

補足
- 操作の参考になる情報を記載しています。

参照
- 参照先を記載しています。

- 本文中では、次の記号を使用しています。

「　」	• 本書内にある参照先を表しています。 • メディア、機能、タッチパネルディスプレイのメッセージなどの名称や入力文字などを表しています。
[　]	• 本機のタッチパネルディスプレイに表示されるボタンやメニューなどの名称を表しています。

- お使いの製品によっては、保存される監査ログの項目や形式が異なることがあります。

1 監査ログの概要

1.1 監査ログとは

監査ログとは、障害、構成変更、ユーザー操作など、本体内で発生した重要な事象（以降、監査事象と呼びます）を、「いつ」、「何が（誰が）」、「どうした」、「その結果どうなったか」、を記録したものです。

監査ログ機能を使用すると、本体の不正使用や不正使用の試みを監視できます。

1.2 監査ログの機能

監査ログの保存

本体で発生した監査事象を、監査ログとして本体に記録します。

ログは最大で 15,000 件まで記録され、15,000 件を超えると日付の古いログから削除されます。

ストレージが取り付けられていない場合は、最大で 50 件のログが記録されます。

監査ログを記録するには、本体、またはインターネットサービスで監査ログの設定を有効にします。

監査ログの取り出し

本体に記録されている監査ログは、インターネットサービスからテキストファイル形式で取り出すことができます。

監査ログの Syslog 送信

本体に記録されている監査ログは、Syslog 送信（Syslog プロトコルを使ってネットワーク上の他のコンピューターに送信）することができます。

Syslog 送信は、本体で設定します。

参照

- 本体での設定は、本体のマニュアルを参照してください。
- インターネットサービスでの設定は、インターネットサービスのヘルプを参照してください。

1.3　取り出した監査ログのフォーマット

ヘッダ情報

項目	形式	説明
フォーマットバージョン	整数	設定値は「3」
デバイス IP アドレス	半角英数字（a ～ z、0 ～ 9）、ドット（.）、コロン（:）で構成された文字列	IP アドレス（IPv4、または IPv6）
符号化方式	文字列	UTF-8 に固定
タイムゾーン	-720 ～ 720	GMT を基準とした時差 単位は分、子午線より西まわりはマイナス値とします。
年月日フォーマット	YYYY/MM/DD、 MM/DD/YYYY、 または DD/MM/YYYY	

監査ログ情報

項目	形式	説明
ログ識別子（Log ID）	整数（1 ～ 60000）	監査事象発生時に割り振られる識別子
年月日（Date）	文字列	監査事象発生の年月日
時間（Time）	hh:mm:ss	監査事象発生の時間（時分秒）
監査事象識別子 (Audit Event ID)	16 進整数（0x0000 ～ 0xffff）	監査事象に対応する識別子
監査事象名 (Logged Events)	文字列	監査事象の種別を表す文字列
ユーザー名（User Name）	文字列	監査事象を発生させたユーザーを表す文字列 *
監査事象詳細 (Description)	文字列	監査事象の詳細
結果 / 状態（Status）	文字列	発生した監査事象の処理結果、または状態
個別保存項目 (Optionally Logged Items)	文字列	監査事象の個別保存情報

*：通常の場合：ユーザー ID
　　ユーザー ID が不明な場合：ユーザー名
　　ユーザー ID、ユーザー名が両方とも不明な場合：-
　　機械管理者：KO
　　カストマーエンジニア：CE
　　認証未登録ユーザー：Guest
　　システム内部動作に起因する場合：System
　　NMP 経由の場合：SNMP:admin

1.4 Syslog 送信のメッセージフォーマット

項目	形式	説明
Priority	整数	次の式で計算される整数 Facility << 3 ¦ Severity 補足 • Facility は本体で設定します。 • Severity は「6」に固定されています。
バージョン	1	「1」に固定
時刻	yyyy-mm-ddThh:mm:ssZ	監査事象発生の年月日および時間(時分秒) タイムゾーンは UTC です。
機械情報	FQDN、ホスト名の場合： 文字列 IPv4 アドレスの場合： nnn.nnn.nnn.nnn	ー
App-Name	-	「-」に固定
ProcId	-	「-」に固定
MsgId	-	「-」に固定
Structured-Data	-	「-」に固定
監査ログ ID	ID=nnnnnn	監査事象発生時に割り振られる識別子
ユーザー名	UserName= 文字列	監査事象を発生させたユーザーを表す文字列 参照 • 監査ログ情報（P.5）
監査事象名	Event= 文字列	監査事象に対応する識別子
監査事象詳細	Description= 文字列	監査事象の詳細
結果 / 状態	Status= 文字列	発生した監査事象の処理結果、または状態
個別記録項目	OptItems= 文字列	監査事象の個別記録情報

2 監査ログの保存項目

2.1 デバイスの状態変化

項目	説明
監査事象識別子（Audit Event ID）	0x0101
監査事象名（Logged Events）	「System Status」

デバイスの稼動開始および終了

通常ブートによるコールドスタート

項目	説明
年月日（Date）、時間（Time）	デバイスが Ready となった時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Started normally （cold boot）」
結果 / 状態（Status）	「-」
個別保存項目 （Optionally Logged Items）	「-」

通常ブートによるウォームスタート

項目	説明
年月日（Date）、時間（Time）	デバイスが Ready となった時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Started normally （warm boot）」
結果 / 状態（Status）	「-」
個別保存項目 （Optionally Logged Items）	「-」

強制ログ初期による立ち上げ

項目	説明
年月日（Date）、時間（Time）	デバイスが Ready となった時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Started （NVM initialized）」
結果 / 状態（Status）	「-」
個別保存項目 （Optionally Logged Items）	「-」

強制ストレージ初期化による立ち上げ

項目	説明
年月日（Date）、時間（Time）	デバイスが Ready となった時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Started （Storage initialized）」
結果 / 状態（Status）	「-」
個別保存項目 (Optionally Logged Items)	「-」

シャットダウン

項目	説明
年月日（Date）、時間（Time）	デバイスが電源のオフ要求を検出した時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Shutdown requested」
結果 / 状態（Status）	「-」
個別保存項目 (Optionally Logged Items)	**アクション** 最大 64 バイト（終端文字列を含まない） 障害を復旧した場合は「Recovered from failures」 それ以外の場合は「-」

セルフテスト

セルフテストの結果

項目	説明
年月日（Date）、時間（Time）	デバイスが Ready になる直前
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Self Test」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ROM Image1 のチェックサム値** **ROM Image2 のチェックサム値**

2.2 ログインおよびログアウト

項目	説明
監査事象識別子（Audit Event ID）	0x0201
監査事象名（Logged Events）	「Login/Logout」

ユーザー認証

ログイン

項目	説明
年月日（Date）、時間（Time）	ユーザーの認証結果が確定した時点
ユーザー名（User Name）	ログイン対象のユーザー ID
監査事象詳細（Description）	「Login」
結果 / 状態（Status）	「Successful」、「Failed（Invalid UserID）」、「Failed（Invalid Password）」、または「Failed」
個別保存項目 (Optionally Logged Items)	**アクセス方法** 「Local」、「Web User Interface」、または「Printer Driver」 **ホスト名** 最大 45 バイト（終端文字列を含まない） IP アドレス 補足 • IP アドレスが不明の場合、ローカルアクセスの場合、またはプライベートプリントの認証に失敗した場合は、「-」と記録されます。 **認証方法** 「Local」、「Remote」、または「Custom」 **役割** 「System Administrator」、「Accounting Administrator」、「Customer Engineer」、「Casual Operator」、または「-」 補足 • ログインに失敗した場合は「-」、機械管理者は「System Administrator」、カストマーエンジニアは「Customer Engineer」、一般ユーザーおよび認証未登録ユーザーは「Casual Operator」と記録されます。

補足

- プライベートプリントの認証に失敗した場合の監査ログは、次の条件をすべて満たしたときに記録されます。
  - プライベートプリントが有効で、[認証 / プライベートプリントの設定] が次のとおり
    - [受信制御] ：[プリンターの認証に従う]
    - [認証成功のジョブ] ：[プライベートプリントに保存]
    - [認証不正のジョブ] ：[ジョブを中止]
    - [User ID なしのジョブ] ：[ジョブを中止]
  - プリントジョブの種類が、次のどちらか
    - プリントジョブに付与されているユーザー情報のユーザー認証が失敗した
    - ユーザー情報が付与されていないプリントジョブ

ログアウト

項目	説明
年月日（Date）、時間（Time）	ユーザーのログアウト要求を検出した時点
ユーザー名（User Name）	ログイン対象のユーザー ID
監査事象詳細（Description）	「Logout」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**アクセス方法** 「Local」、または「Web User Interface」 **ホスト名** 最大 45 バイト（終端文字列を含まない） IP アドレス 補足 • IP アドレスが不明の場合、またはローカルアクセスの場合は、「-」と記録されます。

認証ロック

補足
- 検知タイミングによっては、対象となるログイン事象（失敗）より先に記録されることがあります。

項目	説明
年月日（Date）、時間（Time）	連続で認証に失敗した回数が、システムで設定した数に到達した時点
ユーザー名（User Name）	ログイン対象のユーザー ID
監査事象詳細（Description）	「Locked Authentication」
結果 / 状態（Status）	「-」
個別保存項目 (Optionally Logged Items)	ロックまでの認証エラー回数

不正侵入攻撃検知

補足
- 検知タイミングによっては、対象となるログイン事象（失敗）より先に記録されることがあります。

項目	説明
年月日（Date）、時間（Time）	規定時間内に、連続で認証に失敗した回数が、システムで設定した数に到達した時点
ユーザー名（User Name）	ログイン対象のユーザー ID
監査事象詳細（Description）	「Detected continuous Authentication Fail」
結果 / 状態（Status）	「-」
個別保存項目 (Optionally Logged Items)	**検知手段（プロトコル）** 「SNMPv3」、「Web User Interface」、または「-」 **不正攻撃認証までの連続認証エラー回数**

2.3　監査ポリシーの変更

項目	説明
監査事象識別子（Audit Event ID）	0x0301
監査事象名（Logged Events）	「Audit Policy」

重要データへのアクセス

監査ログ機能の有効化

項目	説明
年月日（Date）、時間（Time）	該当設定項目を設定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Audit Log」
結果 / 状態（Status）	「Enabled」
個別保存項目 （Optionally Logged Items）	「-」

監査ログ機能の無効化

項目	説明
年月日（Date）、時間（Time）	該当設定項目を設定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Audit Log」
結果 / 状態（Status）	「Disabled」
個別保存項目 （Optionally Logged Items）	「-」

2.4　ジョブの終了

項目	説明
監査事象識別子（Audit Event ID）	0x0401
監査事象名（Logged Events）	「Job Status」

ジョブ

プリンター

項目	説明
年月日（Date）、時間（Time）	ジョブが終了した時点
ユーザー名（User Name）	ジョブを実行したユーザーのユーザー ID、またはユーザー名
監査事象詳細（Description）	「Print」

項目	説明
結果 / 状態（Status）	「Completed」、「Completed with Warnings」、「Canceled by User」、「Canceled by Shutdown」、「Aborted」、または「Unknown」
個別保存項目 (Optionally Logged Items)	**root ジョブ UUID** 最大 36 バイト（終端文字列を含まない） **root ジョブ UUID と当該ジョブとの関連** 「Related」、または「Owned」 **Job Account ID** 最大 32 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 **アクション** 最大 64 バイト（終端文字列を含まない） 「強制印字一時解除」を実施した場合は「Released forced output」 それ以外の場合は「-」 **ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は、「-」と記録されます。 **ファイル名** 最大 64 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 **ジョブタイプ** 最大 16 バイト（終端文字列を含まない） 値が設定されていない場合は「-」

コピー

項目	説明
年月日（Date）、時間（Time）	ジョブが終了した時点
ユーザー名（User Name）	ジョブを実行したユーザーのユーザー ID、またはユーザー名
監査事象詳細（Description）	「Copy」
結果 / 状態（Status）	「Completed」、「Completed with Warnings」、「Canceled by User」、「Canceled by Shutdown」、「Aborted」、または「Unknown」
個別保存項目 (Optionally Logged Items)	**root ジョブ UUID** 最大 36 バイト（終端文字列を含まない） **root ジョブ UUID と当該ジョブとの関連** 「Related」、または「Owned」 **Job Account ID** 最大 32 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 **アクション** 最大 64 バイト（終端文字列を含まない） 「強制印字一時解除」を実施した場合は「Released forced output」 「制限コード検知一時解除」を実施した場合は「Ignored inhibited code」 それ以外の場合は「-」

スキャナー

項目	説明
年月日（Date）、時間（Time）	ジョブが終了した時点
ユーザー名（User Name）	ジョブを実行したユーザーのユーザー ID、またはユーザー名
監査事象詳細（Description）	「Scan」
結果 / 状態（Status）	「Completed」、「Completed with Warnings」、「Canceled by User」、「Canceled by Shutdown」、「Aborted」、または「Unknown」
個別保存項目 （Optionally Logged Items）	**root ジョブ UUID** 最大 36 バイト（終端文字列を含まない） **root ジョブ UUID と当該ジョブとの関連** 「Related」、または「Owned」 **Job Account ID** 最大 32 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 **アクション** 最大 64 バイト（終端文字列を含まない） 「制限コード検知一時解除」を実施した場合は「Ignored inhibited code」 「暗号化」を実施した場合は「Encrypted」 「署名」を実施した場合は「Signed」 どの操作も実施していない場合は「-」 **宛先名（to）** 最大 64 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 補足 • メールアドレスだけが設定されます。 **送信者名（from）** 最大 64 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 補足 • メールアドレスだけが設定されます。 **URL 送信文書 ID** 最大 10 バイト（終端文字列を含まない） 値が設定されていない場合は「-」

ファクス

項目	説明
年月日（Date）、時間（Time）	ジョブが終了した時点
ユーザー名（User Name）	ジョブを実行したユーザーのユーザー ID、またはユーザー名
監査事象詳細（Description）	「Fax」
結果 / 状態（Status）	「Completed」、「Completed with Warnings」、「Canceled by User」、「Canceled by Shutdown」、「Aborted」、または「Unknown」

項目	説明
個別保存項目 (Optionally Logged Items)	**root ジョブ UUID** 最大 36 バイト（終端文字列を含まない） **root ジョブ UUID と当該ジョブとの関連** 「Related」、または「Owned」 **Job Account ID** 最大 32 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 **アクション** 最大 64 バイト（終端文字列を含まない） 「強制印字一時解除」を実施した場合は「Released forced output」 「制限コード検知一時解除」を実施した場合は「Ignored inhibited code」 どの操作も実施していない場合は「-」 **宛先名（to）** 宛先電話番号、またはアドレス帳の宛先名（宛先電話番号優先） 最大 64 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 **送信者名（from）** 最大 64 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 補足 • メールアドレスだけが設定されます。

ボックス

項目	説明
年月日（Date）、時間（Time）	ジョブが終了した時点
ユーザー名（User Name）	ジョブを実行したユーザーのユーザー ID、またはユーザー名
監査事象詳細（Description）	「Mailbox」
結果 / 状態（Status）	「Completed」、「Completed with Warnings」、「Canceled by User」、「Canceled by Shutdown」、「Aborted」、または「Unknown」
個別保存項目 (Optionally Logged Items)	**root ジョブ UUID** 最大 36 バイト（終端文字列を含まない） **root ジョブ UUID と当該ジョブとの関連** 「Related」、または「Owned」 **Job Account ID** 最大 32 バイト（終端文字列を含まない） 値が設定されていない場合は「-」 **アクション** 最大 64 バイト（終端文字列を含まない） 「強制印字一時解除」を実施した場合は「Released forced output」 それ以外の場合は「-」

レポート

項目	説明
年月日（Date）、時間（Time）	ジョブが終了した時点
ユーザー名（User Name）	ジョブを実行したユーザーのユーザー ID、またはユーザー名
監査事象詳細（Description）	「Print Reports」
結果 / 状態（Status）	「Completed」、「Completed with Warnings」、「Canceled by User」、「Canceled by Shutdown」、「Aborted」、または「Unknown」
個別保存項目 （Optionally Logged Items）	**root ジョブ UUID** 最大 36 バイト（終端文字列を含まない） **root ジョブ UUID と当該ジョブとの関連** 「Related」、または「Owned」 **Job Account ID** 最大 32 バイト（終端文字列を含まない） 値が設定されていない場合は「-」

ジョブフロー

項目	説明
年月日（Date）、時間（Time）	ジョブが終了した時点
ユーザー名（User Name）	ジョブを実行したユーザーのユーザー ID、またはユーザー名
監査事象詳細（Description）	「Job Flow Service」
結果 / 状態（Status）	「Completed」、「Completed with Warnings」、「Canceled by User」、「Canceled by Shutdown」、「Aborted」、または「Unknown」
個別保存項目 （Optionally Logged Items）	**root ジョブ UUID** 最大 36 バイト（終端文字列を含まない） **root ジョブ UUID と当該ジョブとの関連** 「Related」、または「Owned」 **Job Account ID** 最大 32 バイト（終端文字列を含まない） 値が設定されていない場合は「-」

その他

項目	説明
年月日（Date）、時間（Time）	ジョブが終了した時点
ユーザー名（User Name）	ジョブを実行したユーザーのユーザー ID、またはユーザー名
監査事象詳細（Description）	「-」
結果 / 状態（Status）	「Completed」、「Completed with Warnings」、「Canceled by User」、「Canceled by Shutdown」、「Aborted」、または「Unknown」
個別保存項目 （Optionally Logged Items）	**root ジョブ UUID** 最大 36 バイト（終端文字列を含まない） **root ジョブ UUID と当該ジョブとの関連** 「Related」、または「Owned」 **Job Account ID** 最大 32 バイト（終端文字列を含まない） 値が設定されていない場合は「-」

2.5 デバイス設定の変更 / 参照

項目	説明
監査事象識別子（Audit Event ID）	0x0501
監査事象名（Logged Events）	「Device Settings」

時刻設定

時刻設定（ローカルタイム）の変更

項目	説明
年月日（Date）、時間（Time）	設定変更結果が確定した時点
ユーザー名（User Name）	ジョブを実行したユーザーの、ユーザー ID
監査事象詳細（Description）	「Adjust Time」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	**旧日時** 監査事象発生の年月日および時間（時分秒） **手段** サービスによる時刻変更の場合は次のどれかの文字列 「Time change by system.」 「Time change by EPBB.」 「Time change by NTP.」 「Time change by SNMP.」 「Time change by XPJL.」 「Time change by SSMM.」 「Time change by unknown service.」 ユーザーによる時刻変更の場合は、「Time change by user」 **ホスト名、または IP アドレス** 時刻変更を行ったサービスが NTP サーバーの場合、追加でホスト名、または IP アドレス

ユーザー情報

ユーザー登録

項目	説明
年月日（Date）、時間（Time）	ユーザー登録結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Add User」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**対象ユーザーのユーザー ID** **対象ユーザーの役割** 「System Administrator」、「Accounting Administrator」、または「Casual Operator」 補足 • 認証未登録ユーザーの場合は「Casual Operator」が記録されます。

ユーザー登録内容変更

補足

• 認証モードが本体認証のときにだけ、記録されます。ただし、機械管理者ユーザーの登録内容が変更された場合は、認証モードが本体認証以外でも記録されます。

項目	説明
年月日（Date）、時間（Time）	ユーザー登録内容変更結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Edit User」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**対象ユーザーのユーザー ID** ユーザー ID 自身が変更された場合は、変更後のユーザー ID **対象ユーザーの役割** 「System Administrator」、「Accounting Administrator」、「Casual Operator」、または「-」 補足 • 役割自身が変更された場合は変更後の役割、一般ユーザー、および認証未登録ユーザーの場合は「Casual Operator」が記録されます。 **変更対象の属性** 「ID」、「Password」、「CardID」、「Name」、「Permission」、「Role」、「ICCardID」、および「Other」

ユーザー削除

項目	説明
年月日（Date）、時間（Time）	ユーザー削除結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Delete User」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**対象ユーザーのユーザー ID** ユーザー ID 自身が変更された場合は、変更後のユーザー ID **対象ユーザーの役割** 「System Administrator」、「Accounting Administrator」、「Casual Operator」

使用済みユーザー名管理テーブルフル

項目	説明
年月日（Date）、時間（Time）	使用済みユーザー管理テーブルのフルを検知した時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Deleted Username Queue Overflow」
結果 / 状態（Status）	「Successful」
個別保存項目 (Optionally Logged Items)	「-」

ボックス

ボックス登録

項目	説明
年月日（Date）、時間（Time）	ボックスの登録結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Create Mailbox」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」、操作パネルから実施した場合は「Local」と記録されます。 **BOX 番号** 左詰めで、最大 3 桁の半角数字表記（最上位桁から連続する 0 は省略されます）

ボックス削除

項目	説明
年月日（Date）、時間（Time）	ボックス削除結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Delete Mailbox」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」、操作パネルから実施した場合は「Local」と記録されます。 **BOX 番号** 左詰めで、最大 3 桁の半角数字表記（最上位桁から連続する 0 は省略されます）

認証モード

変更

項目	説明
年月日（Date）、時間（Time）	システムデータへの値設定が完了した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Switch Authentication Mode」
結果 / 状態（Status）	「Successful」
個別保存項目 (Optionally Logged Items)	**新設定値** 「Local is enabled」、「Network is enabled」、「Custom is enabled」、または「OFF is enabled」 **旧設定値** 「Local is enabled」、「Network is enabled」、「Custom is enabled」、または「OFF is enabled」

セキュリティ関連

変更

項目	説明
年月日（Date）、時間（Time）	該当設定項目を設定した時点 再起動後反映の設定変更であっても、値の変更時を保存タイミングとする
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Change Security Setting」
結果 / 状態（Status）	「Successful」
個別保存項目 (Optionally Logged Items)	**項目名** 「Authentication」 「Authorization」 「Accounting」 「Image Overwrite」 補足 • 「しない」から「3 回」に変更すると監査ログが二つ記録されます。 「Storage Encryption」 「S/MIME」 「IPSEC」 「SNMPv1/v2」 「SNMPv1/v2　(Read Only)」 「SNMPv3」 「SNMPv3　(Read Only)」 「802.1x」 「Certificate Verify Mode」 「Maintainer Password」 「IntelligentCard」 「FIPS140」 「Self Test」 「Auto Clear Timer」 「Service Rep. Restricted Operation」 「Print Reports Button」 「External Code Integrity Check」 「NFC」 「No Encrypt Ext App Install」 「CORS」 「ThinPrint」 「HTTP SSL/TLS」 「HTTP SSL/TLS Forced」 「IPP SSL/TLS Forced」 「SMTP SSL/TLS」 「LDAP SSL/TLS」 「ThinPrint SSL/TLS」 「Session Lock Timer」 「Authentication Operation Message」 「USB Port Management」 「Front USB-A」 「Rear USB-A」 「PC USB-B」

項目	説明
個別保存項目 (Optionally Logged Items)	「Deleted User Account Names Days of Restriction」 「Maximum Number of Reusable Sequential Characters」 「Number of Password Generations Required」 「ID Token Validation　(Azure Active Directory)」 「Certificate Verify Mode　(Azure Active Directory)」 「Invalid User Deletion　(Azure Active Directory)」 「Syslog」 「Download Disable Flag」 「Firmware Download via Network」 「Web UI Timer」 「SSL Protocol Information」 「CSRF Check」 「Runtime System Protection」 「Device Ceritificate Enrollment」 「Startup Integrity Check」 「POP3 with OAuth Authentication」 「Common Criteria Function」 「Universal Print」 「Certificate Verify Mode (FujiFilm BI Direct)」 「ID Token Validation (FujiFilm BI Direct)」 **変更内容** 有効 / 無効の設定を変更した場合は「is enabled」、または「is disabled」 有効 / 無効以外の設定を変更した場合は「is configured」

参照

項目	説明
年月日（Date）、時間（Time）	インターネットサービスから参照した場合は、対象となるデータを含む HTML を取得したタイミング 操作パネルから参照した場合は、［設定］画面に入ったタイミング
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「View Security Setting」
結果 / 状態（Status）	「Successful」
個別保存項目 (Optionally Logged Items)	**アクセス方法** 「Local」、または「Web User Interface」 **ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合、またはローカルアクセスの場合は「-」と記録されます。

ジョブ関連

変更

項目	説明
年月日（Date）、時間（Time）	該当設定項目を設定した時刻
ユーザー名（User Name）	「CE」
監査事象詳細（Description）	「Change Job Setting」
結果 / 状態（Status）	「Successful」
個別保存項目 (Optionally Logged Items)	**機能名** 「Delay Print」、または「Private Print」

XCP プラグイン

XCP プラグインの起動 / 停止

項目	説明
年月日（Date）、時間（Time）	XCP プラグインの起動および停止時
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Activate Embedded Plug-in」、または 「Deactivate Embedded Plug-in」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**XCP プラグイン名および要求元のホスト情報**

2.6 デバイス格納データへのアクセス

項目	説明
監査事象識別子（Audit Event ID）	0x0601
監査事象名（Logged Events）	「Device Data」

証明書

証明書登録

項目	説明
年月日（Date）、時間（Time）	証明書の登録結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Import Certificate」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	**カテゴリ** 「RootCA」、「DeviceEE」、または「SSCEE」 **鍵長** 「512」から「2048」まで **発行者 DN** 文字列最大 150 バイト **シリアル番号** 最大 40 バイト

証明書抹消

項目	説明
年月日（Date）、時間（Time）	証明書の抹消結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Delete Certificate」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	**カテゴリ** 「RootCA」、「DeviceEE」、または「SSCEE」 **鍵長** 「512」から「2048」まで **発行者 DN** 文字列最大 150 バイト **シリアル番号** 最大 40 バイト

証明書オンライン登録

項目	説明
年月日（Date）、時間（Time）	証明書のオンライン登録をした時刻
ユーザー名（User Name）	「System」
監査事象詳細（Description）	「Device Ceritificate Enrollment」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**証明書の所有者 DN**

アドレス帳

宛先追加

項目	説明
年月日（Date）、時間（Time）	宛先追加結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Add Address Entry」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」、操作パネルから実施された場合は「Local」と記録されます。 **登録番号** 左詰めで、最大 4 桁の半角数字表記（最上位桁から連続する 0 は省略されます）

宛先削除

項目	説明
年月日（Date）、時間（Time）	宛先削除結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Delete Address Entry」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」、操作パネルから実施された場合は「Local」と記録されます。 **登録番号** 左詰めで、最大 4 桁の半角数字表記（最上位桁から連続する 0 は省略されます）

宛先変更

項目	説明
年月日（Date）、時間（Time）	宛先変更結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Edit Address Entry」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」、操作パネルから実施された場合は「Local」と記録されます。 **登録番号** 左詰めで、最大 4 桁の半角数字表記（最上位桁から連続する 0 は省略されます）

リモートクライアントからアップロード（全体）

項目	説明
年月日（Date）、時間（Time）	リモートクライアントからのアップロード結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Import Address Entry」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」と記録されます。

リモートクライアントへのダウンロード（全体）

項目	説明
年月日（Date）、時間（Time）	リモートクライアントへのダウンロード結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Export Address Entry」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」と記録されます。

宛先全削除

項目	説明
年月日（Date）、時間（Time）	全宛先削除結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Clear Address Entry」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」と記録されます。

監査ログ

リモートクライアントへのダウンロード（全体）

項目	説明
年月日（Date）、時間（Time）	ダウンロード結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Export Audit Log」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」と記録されます。

文書

スキャン送信文書のリモートクライアントへの送信

補足

- スキャン送信で保存された文書だけが対象となります。

項目	説明
年月日（Date）、時間（Time）	リモートクライアントへの送信結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Retrieve scanned image」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」と記録されます。 **URL 送信文書 ID** 最大 10 バイト（終端文字列を含まない）

削除

補足

- ボックスの保存文書、およびプライベートプリントの保存文書が削除された場合に記録されます。
  次の場合は記録されません。
  - ボックスの削除（「ボックス削除」の監査ログが記録されます）
  - WebDAV、カスタムサービスコンテンツから実施された場合
  - 時間経過による文書削除
  - ボックスとプライベートプリント以外の保存文書（たとえば、ファクスポーリング予約で［ポーリング予約ボックス］に保存した文書、時刻指定プリント）の削除

項目	説明
年月日（Date）、時間（Time）	文書削除結果が確定した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Delete Document」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 (Optionally Logged Items)	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」、操作パネルから実施された場合は「Local」と記録されます。 **ボックス番号** 左詰めで、最大3桁の半角数字（冒頭に0がある場合は省略されます） **文書番号** 左詰めで、最大4桁の半角数字（冒頭に0がある場合は省略されます）

カスタムサービス

インストール

項目	説明
年月日（Date）、時間（Time）	インストールが終了した時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Install Custom Service」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	**カスタムサービスコンテンツ名（name）** （例）「CS_RM_00108」 不明の場合は「-」 **失敗理由を指す文字列（失敗の場合に記録する）** 原因がインスタンス作成時、指定のカスタムサービス名がすでにデバイス上に存在する場合は、「Application already exists.」 それ以外の場合は、「RegApp regist failed to management service.」

不正なカスタムサービスコンテンツ登録

項目	説明
年月日（Date）、時間（Time）	カスタムサービスコンテンツファイルの署名検証に失敗した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Install Custom Service」
結果 / 状態（Status）	「Failed」
個別保存項目 （Optionally Logged Items）	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」、CPIM 経由の場合は、パッケージ取得先サーバーの FQDN が記録されます。 **カスタムサービスコンテンツ名** 最大 63 バイト（終端文字列を含まない） 取得できない場合（取得エラーの場合も含む）は「-」

アンインストール

項目	説明
年月日（Date）、時間（Time）	アンインストールが終了した時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Uninstall Custom Service」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	**カスタムサービスコンテンツ名（name）** （例）「CS_RM_00108」 不明の場合は「-」 **失敗理由を指す文字列（失敗の場合に記録する）** 「Failed to delete RegApp from management service.」

XCP プラグイン

インストール

項目	説明
年月日（Date）、時間（Time）	インストールが終了した時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Install Embedded Plug-in」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	**XCP プラグイン名** 不明の場合は「-」

不正な XCP プラグイン登録

項目	説明
年月日（Date）、時間（Time）	XCP プラグインファイルの署名検証に失敗した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Install Embedded Plug-in」
結果 / 状態（Status）	「Failed」
個別保存項目 （Optionally Logged Items）	**ホスト名** 最大 45 バイト（終端文字列を含まない） 補足 • ホスト名が不明の場合は IP アドレス、ホスト名と IP アドレスの両方が不明の場合は「-」、CPIM 経由の場合は、パッケージ取得先サーバーの FQDN が記録されます。 **プラグインファイル名** CPIM 経由の場合は、ダウンロードしたファイルのダウンロード名 最大 63 バイト（終端文字列を含まない） 取得できない場合（取得エラーの場合も含む）は「-」

アンインストール

項目	説明
年月日（Date）、時間（Time）	アンインストールが終了した時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Uninstall Embedded Plug-in」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	**XCP プラグイン名** 不明の場合は「-」

設定情報の複製

エクスポート

項目	説明
年月日（Date）、時間（Time）	エクスポートが終了した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Export Cloning Data」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	「-」

インポート

項目	説明
年月日（Date）、時間（Time）	インポートが終了した時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Import Cloning Data」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	「-」

改ざん検知

ホワイトリストで許可されていないファイルへのアクセスおよび実行の検知

項目	説明
年月日（Date）、時間（Time）	ホワイトリストで許可されていないファイルへのアクセスおよび実行を検知した時点
ユーザー名（User Name）	「System」
監査事象詳細（Description）	「Illegal Access Detection」
結果 / 状態（Status）	「Successful」
個別保存項目 （Optionally Logged Items）	**アクセス種別** （例）「write」 **アクセスされたファイル名** **アクセスされたプログラム名**

起動時改ざん検知および自動修復

起動時改ざん検知

項目	説明
年月日（Date）、時間（Time）	起動時改ざん検知機能が動作した時点
ユーザー名（User Name）	「System」
監査事象詳細（Description）	「Startup Integrity Check」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	**OS** **アプリケーション**

Software 自動復旧

項目	説明
年月日（Date）、時間（Time）	SoftWare 自動修復機能が動作した時点
ユーザー名（User Name）	「System」
監査事象詳細（Description）	「System Software Recovery」
結果 / 状態（Status）	「Successful」、または「Failed」
個別保存項目 （Optionally Logged Items）	「-」

2.7　デバイス構成の変更 / 復旧

項目	説明
監査事象識別子（Audit Event ID）	0x0701
監査事象名（Logged Events）	「Device Config」

重要パーツ

重要パーツ交換

項目	説明
年月日（Date）、時間（Time）	重要パーツの交換が検出された時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Important Parts」
結果 / 状態（Status）	「Replaced」
個別保存項目 （Optionally Logged Items）	「-」

ストレージ

ストレージ交換検知

項目	説明
年月日（Date）、時間（Time）	ストレージをシステムが認識した時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Storage」
結果 / 状態（Status）	「Installed」、「Removed」、または「Replaced」
個別保存項目 （Optionally Logged Items）	「-」

ROM

ROM バージョン変更

項目	説明
年月日（Date）、時間（Time）	前回起動時の ROM バージョンと、現在起動中の ROM バージョンの差を検知した時点 補足 • バージョンを検知するタイミングは、ROM ごとに異なります。 • NVM 初期化時、オプションの追加 / 削除時には記録されません。
ユーザー名（User Name）	ユーザー ID 補足 • EP - BB センターから指示された場合は「System」と記録されます。
監査事象詳細（Description）	「Software」
結果 / 状態（Status）	「Updated」
個別保存項目 （Optionally Logged Items）	**ROM 種別** （例）「IOT」、「Controller+PS」、「FAX」 **新バージョン** **旧バージョン**

2.8 通信結果

項目	説明
監査事象識別子（Audit Event ID）	0x0801
監査事象名（Logged Events）	「Communication」

信頼性通信

信頼性通信エラー

項目	説明
年月日（Date）、時間（Time）	定期チェックで信頼性通信エラーを検出した時点
ユーザー名（User Name）	「-」
監査事象詳細（Description）	「Trusted Communication」
結果 / 状態（Status）	「Failed」
個別保存項目 （Optionally Logged Items）	**プロトコル名** 「SSL/TLS」、「IPSEC」、または「S/MIME」 **通信先** 最大 45 バイト（終端文字列を含まない） ホスト名、または IP アドレス 補足 • ホスト名と IP アドレスの両方が不明の場合、または S/MIME の場合は「-」が記録されます。 • 通信先の記録例は、次のとおりです。 - IPv6：「[3ffe:0200:0000:010a:0000:0000:0000:0001]」 - IPv4：「129.249.79.100」 - ホスト名：「host.fujifilm.co.jp」 • 45 バイトを超える場合は、一部が切り捨てられます。 **失敗回数** **失敗理由** 補足 • 個別保存項目（Optionally Logged Items）の表示例は、次のとおりです。 - 「SSL/TLS, [3ffe:0200:0000:010a:0000:0000:0000:0001],3,Certificate verification failed」 - 「IPSEC,[3ffe:0200:0000:010a:0000:0000:0000:0001],23,IKE negotiation failed」 • 複数のエラーが発生した場合は、1 つのエラーにつき 1 行記録されます。1 行は最大 69 バイトです。 • 発生したエラーが 50 件を超えた場合は、50 件目以降のエラーが「+」と記録されます。

NTP

信頼性通信エラー

項目	説明
年月日（Date）、時間（Time）	NTP サーバーとの通信失敗を検出した時点
ユーザー名（User Name）	「System」
監査事象詳細（Description）	「NTP Communication」
結果 / 状態（Status）	「Failed」
個別保存項目 （Optionally Logged Items）	**通信先** 最大 45 バイト（終端文字列を含まない） ホスト名（FQDN）、または IP アドレス 補足 • ホスト名と IP アドレスの両方が不明の場合は「-」、ホスト名の名前解決に失敗した場合はホスト名が記録されます。 • 通信先の記録例は、次のとおりです。 - IPv6：「[3ffe:0200:0000:010a:0000:0000:0000:0001]」 - IPv4：「129.249.79.100」 - ホスト名：「host.fujifilm.co.jp」 • 45 バイトを超える場合は、一部が切り捨てられます。 **失敗理由** サーバー通信の場合は「NTP negotiation failed」、DNS 通信の場合は「jp,dns name resolution failed」 補足 • 個別保存項目（Optionally Logged Items）の表示例は、次のとおりです。 - 「[3ffe:0200:0000:010a:0000:0000:0000:0001],NTP negotiation failed」 - 「ntp.fujifilm.co.jp,dns name resolution failed 」 • 複数のエラーが発生した場合は、1 つのエラーにつき 1 行記録されます。1 行は最大 69 バイトです。 • 発生したエラーが 50 件を超えた場合は、50 件目以降のエラーが「+」と記録されます。

EWB（Embedded Web Browser）

EWB からの WEB アクセス

項目	説明
年月日（Date）、時間（Time）	EWB からアクセスした時点
ユーザー名（User Name）	ユーザー ID
監査事象詳細（Description）	「Web Access」
結果 / 状態（Status）	「Successful」
個別保存項目 （Optionally Logged Items）	**アクセス URL**