オフィス向け複合機（imageFORCE ／ imageRUNNER ADVANCE DX ／ imageRUNNER ADVANCE ／ imageRUNNER シリーズ）
プロダクション向け複合機（imagePRESS シリーズ）
不正アクセス防止対策について

重要　管理者の方は、必ずご一読ください。

平素より、キヤノン製品をご愛顧いただき、誠にありがとうございます。本文書ではオフィス向け複合機（imageFORCE ／ imageRUNNER ADVANCE DX ／ imageRUNNER ADVANCE ／ imageRUNNER シリーズ）ならびにプロダクション向け複合機（imagePRESSシリーズ）（以降、複合機）における外部ネットワークからの不正アクセス防止対策を取扱説明書の要約として記載いたします。管理者の方は、必ずご一読いただけますよう、よろしくお願い申し上げます。なお、オプションの imagePRESS Server ／ ColorPASS ／ imagePASS **については、各製品の取扱説明書を参照してください。**

はじめに

近年の複合機は多機能化が進み、従来のコピーやファクス、プリントといった機能に加え、ネットワーク経由での各種プロトコルによるアクセスを前提とした機能が多数搭載されるようになりました。キヤノンの複合機においても例外ではなく、HTTPプロトコルによるリモートUI、SMB ／ WebDAVプロトコルなどによるファイル共有など、さまざまな便利な機能が利用できるようになっています。以降では、キヤノンの複合機における、外部からの不正アクセス対策のポイントを紹介していきます。

お使いの機種によっては、紹介している機能に対応していないことがあります。各ポイントで必要となる複合機の操作／設定や、機能への対応状況については、お使いの機種の取扱説明書を参照してください。

外部からの不正アクセス対策のポイント

1. **プライベートIPアドレスで運用する**
2. **ファイアウォールで通信を制限する**
3. **複合機が持つ情報をパスワードで管理する**
4. **リモートUIの使用を制限する**
5. **SSL（TLS）暗号化通信を設定する**
6. **ファームウェアをアップデートする**
7. **ファームウェアの改ざんを検知する**
8. **監査ログを利用する**
9. **セキュリティーポリシーに従って管理する**

MEMO

リモートUI（User Interface）は、お手持ちのWebブラウザーからネットワークを経由して本機にアクセスし、本機の状況の確認やジョブの操作、各種設定などができるソフトウェアです。本機の前に行かなくても、離れた場所からコンピューターで本機を管理できます。Webブラウザーで本機のIPアドレスまたはホスト名を指定すると、リモートUIのポータルページが表示されます。

リモートUI利用上の注意：
Webブラウザーでリモート UIを開いている時には、他のWebサイトにアクセスしないようにしてください。また、リモートUIで設定変更を行っているコンピューターから離席する場合や設定変更が終了した場合は、Webブラウザーを必ず終了してください。

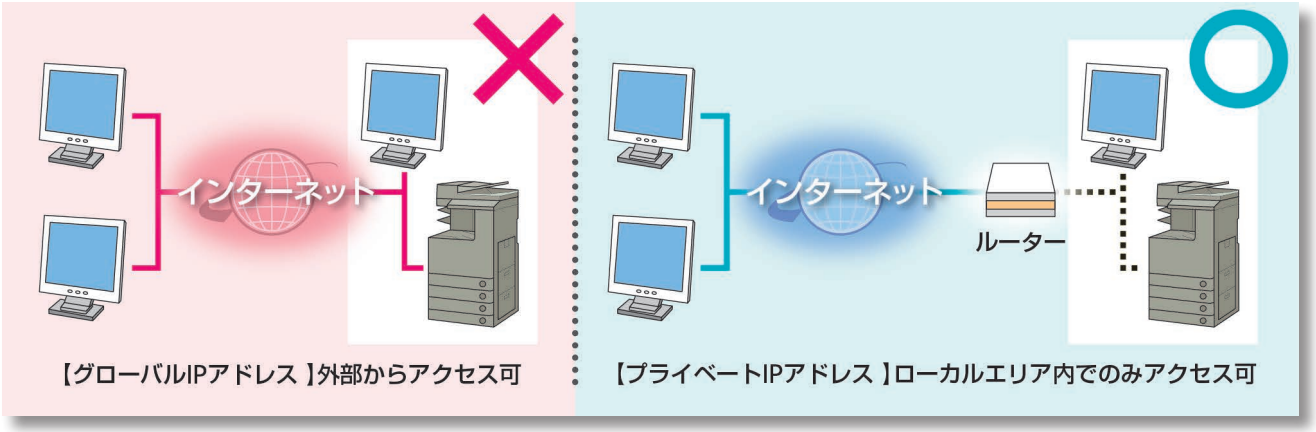
プライベートIPアドレスで運用する

IPアドレスとは、ネットワーク上の機器に割り当てられる番号のことで、インターネット接続に使われるIPアドレスを**「グローバルIPアドレス」**、社内LANなどのローカルエリアネットワークで使われるIPアドレスを**「プライベートIPアドレス」**と呼びます。複合機に設定されているIPアドレスがグローバルIPアドレスの場合は、インターネット上の不特定多数のユーザーからアクセス可能な状態であり、外部からの不正アクセスによる情報漏えいなどのリスクも高まります。一方で、プライベートIPアドレスが設定されている複合機なら、社内LANなどのローカルエリアネットワーク上のユーザーからしかアクセスすることができません。

基本的には、複合機のIPアドレスにはプライベートIPアドレスを設定して運用してください。プライベートIPアドレスには、以下のいずれかの範囲のアドレスが使用されます。お使いの複合機に設定されているIPアドレスがプライベートIPアドレスかどうかを確認するようにしてください。

プライベートIPアドレスの範囲

- 10.0.0.0　～　10.255.255.255
- 172.16.0.0　～　172.31.255.255
- 192.168.0.0　～　192.168.255.255



MEMO

複合機にグローバルIPアドレスが設定されていても、ファイアウォール等で外部からのアクセスを防御する環境を構築すれば、不正アクセスのリスクは軽減されます。複合機にグローバルIPアドレスを設定して運用したいときは、社内のネットワーク管理者にご相談ください。

■ IPアドレスの確認画面の例

本体操作パネル

本体操作パネル

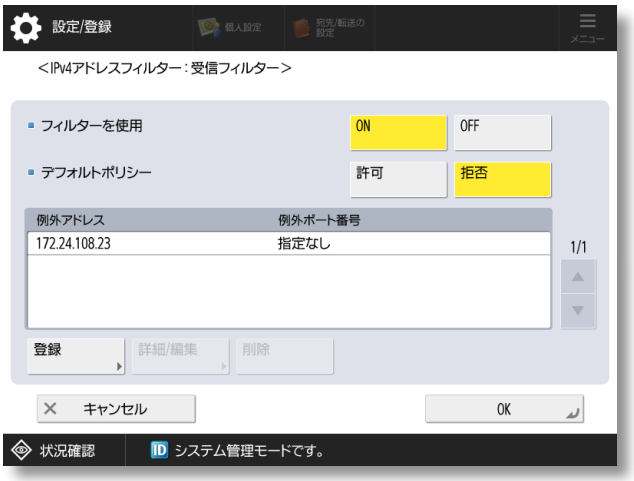
※お使いの機種により、画面が異なることがあります。

ファイアウォールで通信を制限する

ファイアウォールとは、外部ネットワークからの不正アクセスを防止し、ローカルエリア内のネットワークへの攻撃や侵入を防ぐシステムです。お使いのネットワーク環境で、特定の外部IPアドレスからの通信を制限することで、危険と思われる外部からのアクセスをあらかじめ遮断できます。キヤノンの複合機に搭載された機能でもIPアドレスのフィルタリングができます。

■ ファイアウォール設定画面の例

本体操作パネル



※お使いの機種により、画面が異なることがあります。

リモートUI

複合機が持つ情報をパスワードで管理する

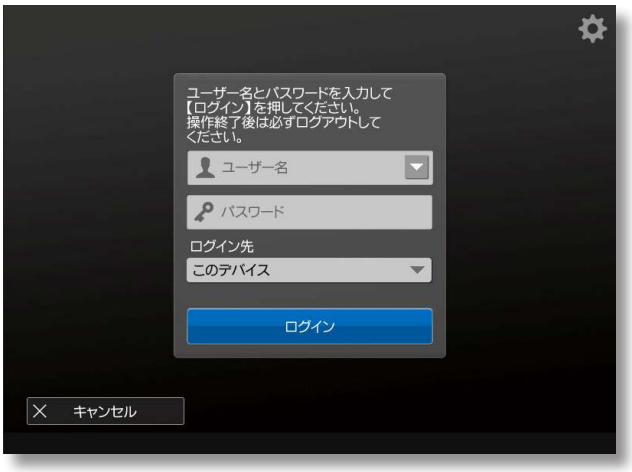
万が一、悪意のある第三者から不正アクセスを受けたとしても、複合機が持つさまざまな情報をパスワードで保護しておけば、情報漏えいによるリスクを大幅に軽減できます。キヤノンの複合機は、さまざまな情報がパスワードで保護できるようになっています。ここでご紹介する例以外の機能や情報においてもパスワードが設定できるものがあるので、必要に応じて適切に設定してください。

※各機能のパスワードは、本体操作パネルやリモートUIで設定できます。

■ パスワード入力画面の例

本体操作パネル

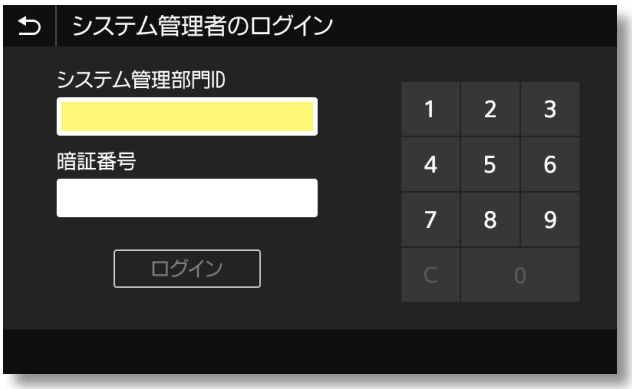
ユーザーログイン時のパスワード入力画面



※お使いの機種により、画面が異なることがあります。

本体操作パネル

システム管理項目のパスワード入力画面



MEMO

複合機はパスワードによる保護機能を備えていますが、パスワードの管理を行うことがセキュリティ対策において重要です。以下のポイントを参考に、パスワードを管理してください。

- 初期パスワードは必ず変更する
- 第三者が推測しやすいパスワードを設定しない
- 不用意に第三者に教えない

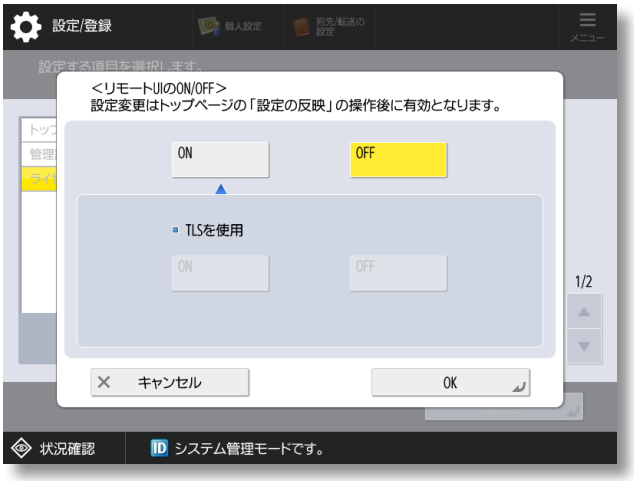
リモートUIの使用を制限する

リモートUIには、その使用を制限する機能が実装されています。

- リモートUIを利用するためには、システム管理暗証番号を初期値から変更する等の各種設定が必要となります。
- 一般ユーザーのリモートUIへのアクセス制限を設定できます。管理者権限、一般ユーザー権限のいずれの場合も、暗証番号（パスワード）の入力が必要となります。
  また、パスワードに加え、ワンタイムパスワードの入力が必要となる、二要素認証を使用することもできます。

■ リモートUIのON/OFF設定画面の例

本体操作パネル



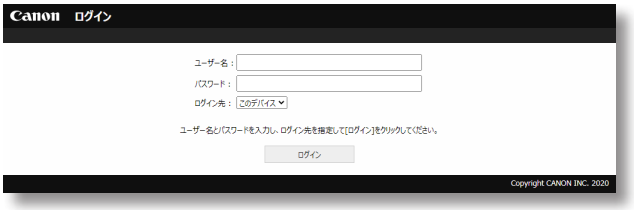
※お使いの機種により、画面が異なることがあります。

本体操作パネル

■ リモートUIログイン画面の例

お使いの機種・設定により、ログイン画面が異なります。

ログイン画面①



管理者・一般ユーザーに関わらず、ユーザー名／パスワードが求められます。

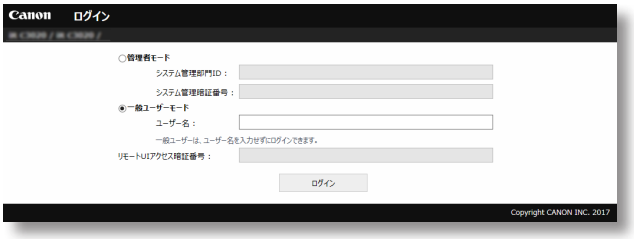
ログイン画面②

管理者はシステム管理部門ID／暗証番号の入力を、一般ユーザーは暗証番号の入力を求められます。

ログイン画面③

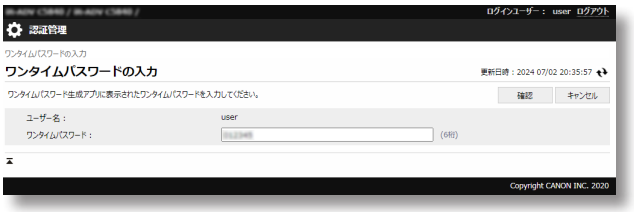
部門別ID管理が設定されている場合、登録されている部門ID／暗証番号の入力を求められます。

ログイン画面④



部門別ID管理が設定されていない場合、管理者はシステム管理部門ID／暗証番号の入力を、一般ユーザーは暗証番号の入力を求められます。

ログイン画面⑤



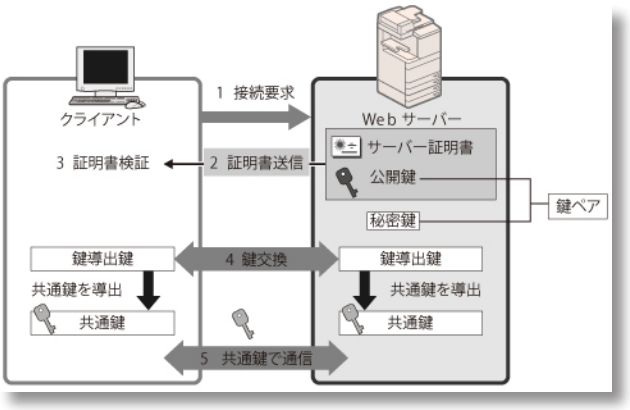
二要素認証が設定されている場合、ユーザー名／パスワード入力後に、ワンタイムパスワードの入力が求められます。

SSL（TLS）暗号化通信を設定する

ユーザーがブラウザーを通して複合機にアクセスする際に、複合機にサーバー証明書を導入することで、SSL（TLS）による安全な暗号化通信を実現できます。SSL（TLS）通信ではサーバー証明書と公開鍵を利用して、ユーザーと複合機の双方のみで使用できる共通鍵を互いに生成します。それにより、外部ネットワークからの不正アクセスを防ぐことができます。

SSL（TLS）通信の仕組み（右図）

1. ユーザーのコンピューターから本機へアクセスするとき、SSL（TLS）のサーバー証明書を要求します。
2. 本機からユーザーのコンピューターへ証明書が送られます。
3. ユーザーのコンピューターでサーバーから受け取った証明書を検証します。
4. 共通鍵を確立するため、ユーザーのコンピューターと本機で鍵交換を実施します。
5. これによりユーザーのコンピューターと本機の双方で共通鍵を所有することになり、互いに共通鍵を使用してのデータのやり取りができるようになります。

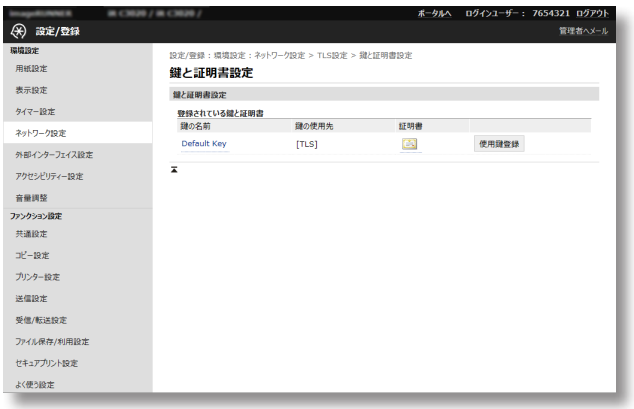


■ SSL(TLS) 設定画面の例

本体操作パネル

※お使いの機種により、画面が異なることがあります。

リモートUI



MEMO

セキュリティー設定をより強固なものにするために、セキュリティポリシー設定の［通信の運用ポリシー］を有効にすることを推奨します。

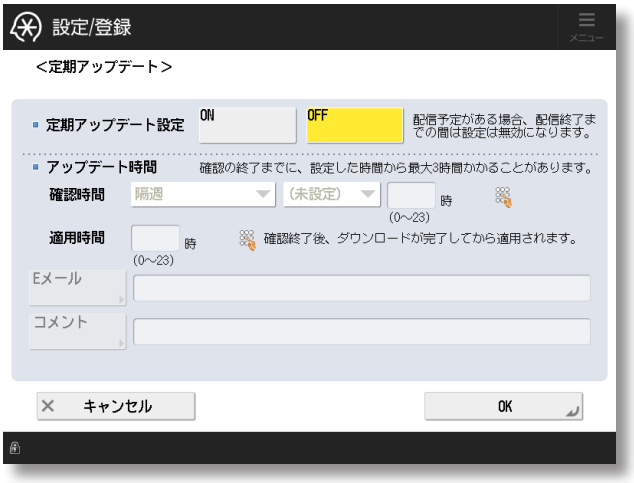
※［通信の運用ポリシー］の詳細については、各製品の取扱説明書を参照してください。

ファームウェアをアップデートする

機能が追加されたり、機能に不具合があったときなどにファームウェアは更新されます。
定期的に新しいファームウェアをチェックして、自動的にアップデートするための設定を行うことができます。

■ ファームウェアアップデート設定画面の例

本体操作パネル



※お使いの機種により、画面が異なることがあります。

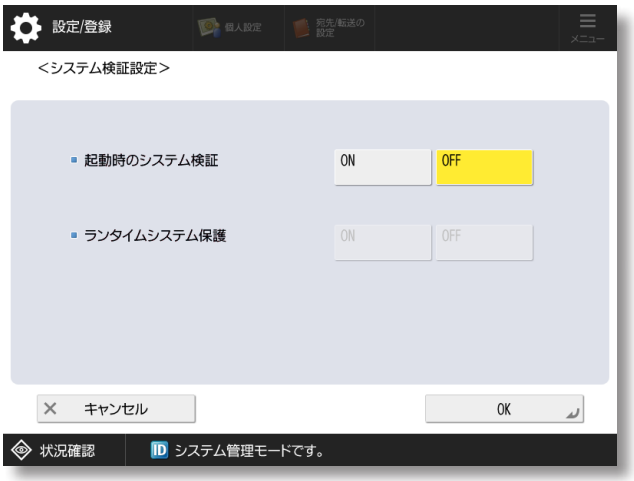
本体操作パネル

ファームウェアの改ざんを検知する

ファームウェアの安全性をさらに高めるために、複合機の起動時および稼働時にファームウェアの改ざんを検知することができます。

■ ファームウェア改ざん検知設定画面の例

本体操作パネル



※お使いの機種により、画面が異なることがあります。

監査ログを利用する

複合機がどのように使用されているかを確認／分析するために、ログを活用することができます。ログには操作日時、ユーザー名、操作の種類、機能の種類、操作結果などの情報が記録されます。

ログの種類

- ユーザー認証ログ
- ジョブログ
- 送受信ログ
- アドバンスドボックス保存ログ
- ボックス操作ログ
- ボックス認証ログ
- アドバンスドボックス操作ログ
- 本体管理ログ
- ネットワーク認証ログ
- 一括エクスポート／インポートログ
- ボックスバックアップログ
- アプリケーション／ソフトウェア管理画面での操作ログ
- セキュリティーポリシーログ
- グループ管理ログ
- システムメンテナンスログ
- 認証プリントログ
- 設定の同期のログ
- 監査ログ管理機能のログ

ログの取得方法

- 自動エクスポート（SMBサーバー指定フォルダへの自動エクスポート）
- 手動エクスポート（リモートUIからエクスポート）
- 逐次送信（Syslog/SIEMサーバーへの送信）

■ ログ設定画面の例

リモートUI

※お使いの機種により、画面が異なることがあります。

セキュリティーポリシーに従って管理する

情報セキュリティーの基本方針や対策基準といったセキュリティーポリシーは多くの組織で定められており、パソコンや複合機などの情報機器はこれに従って運用することが望まれます。本機では、セキュリティーポリシーに関連する複数の設定を一括管理し、情報セキュリティーの担当者だけが設定を変更できるようにすることができます。

セキュリティーポリシーの設定項目

［インターフェイス］

- 無線ポリシー
  無線接続を禁止することで、不特定多数のアクセスを抑止します。
- USBポリシー
  USB接続を禁止することで、不正な接続やデータの持ち出しを防ぎます。

［認証］

- 認証の運用ポリシー
  ユーザー認証を徹底することにより、未登録ユーザーによる不正な操作を回避します。
- パスワードの運用ポリシー
  パスワードの運用方法を厳しく制限します。
- パスワードの設定ポリシー
  ユーザー認証で使用するパスワードに一定の複雑さや有効期間を設定し、第三者が容易に推測できないようにします。
- ロックアウトのポリシー
  入力したパスワードによるログイン操作が一定回数連続で失敗した場合、しばらくの間はログインできないようにします。

［鍵/証明書］

弱い暗号を使用できないようにしたり、ユーザーのパスワードと鍵を特定のハードウェア内で暗号化したりして大切なデータを保護します。

［ネットワーク］

- 通信の運用ポリシー
  署名や証明書の検証を必須にすることで、より安全に通信できます。
- ポートの利用ポリシー
  使用しないポートを閉じることで、外部からの侵入を防ぎます。

［ログ］

ログの記録を必須にすることで、定期的に監査できるようにします。

［ジョブ］

- 印刷のポリシー
  印刷による情報漏えいを抑止します。
- 送受信のポリシー
  送信時の宛先操作や受信データの処理方法を制限します。

［ストレージ］

ハードディスク内の不要なデータを削除することで、情報漏えいを防ぎます。

■ セキュリティーポリシー設定画面の例

リモートUI

※お使いの機種により、画面が異なることがあります。

USRM2-8572-03
Copyright CANON INC. 2025