レーザービームプリンター（Satera LBP シリーズ）
スモールオフィス向け複合機（Satera MFP 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。本書は、レーザービームプリンター Satera LBP シリーズ（以降、プリンター）ならびにスモールオフィス向け複合機 Satera MFP 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について記載しています。プリンター、複合機をネットワーク環境でお使いの方、管理者の方は、ご利用の前に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。

はじめに

近年のプリンター、複合機はネットワークに接続する事で、プリントやリモートUI における管理、さらに複合機においてはスキャン画像の送信といった、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、プリンター、複合機をネットワーク環境でお使いの際における、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。

本書ではリモートUIからの設定方法を記載しています。お使いのプリンター、複合機や各機能によっては本体操作パネルからも設定することが可能です。また、設定手順や図は一例であり、お使いのプリンター、複合機とは異なる場合があります。詳しくはプリンター、複合機同梱の取扱説明書も併せてご参照ください。

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. SSL暗号化通信を設定する
4. プリンター、複合機をパスワードで管理する
複合機が持つ情報をパスワードで管理する

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プリンター、複合機にアクセスし、本体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。本体の前に行かなくても、離れた場所からコンピューターで管理できます。Webブラウザーで本体の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の操作手順については、プリンター、複合機同梱の取扱説明書を参照してください。

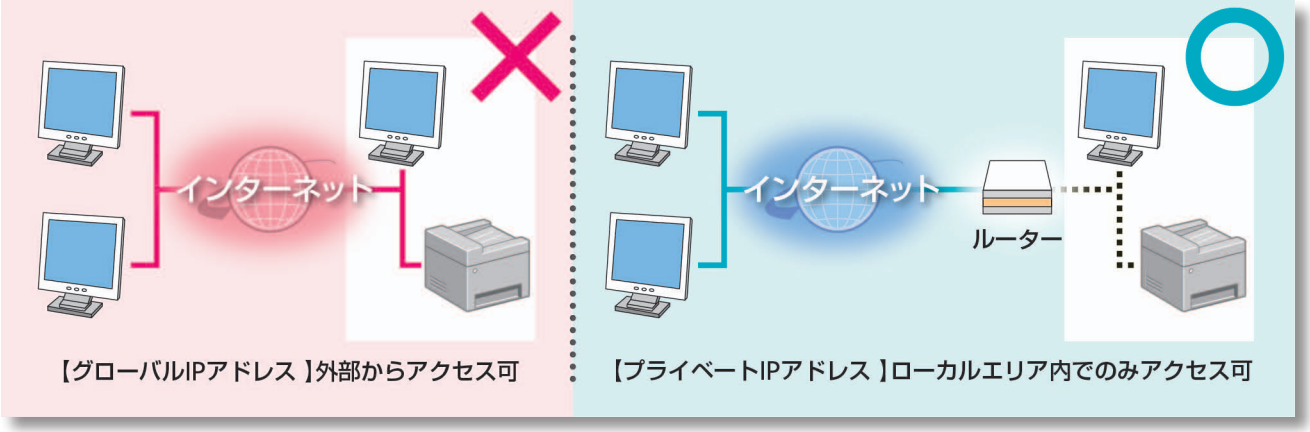
プライベートIPアドレスで運用する

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。プリンター、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プリンター、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、プリンター、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。お使いのプリンター、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

プリンター、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。プリンター、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

リモートUIを起動し、管理者モードでログインする
↓
[設定/登録]
↓
[ネットワーク設定]
↓
[TCP/IP設定]

※ IPアドレスの確認手順については、本体同梱の取扱説明書を参照してください。

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。キヤノンのプリンター、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。

■プリンター、複合機に搭載したIPアドレスフィルタリング画面

※ 設定手順については、本体同梱の取扱説明書を参照してください。

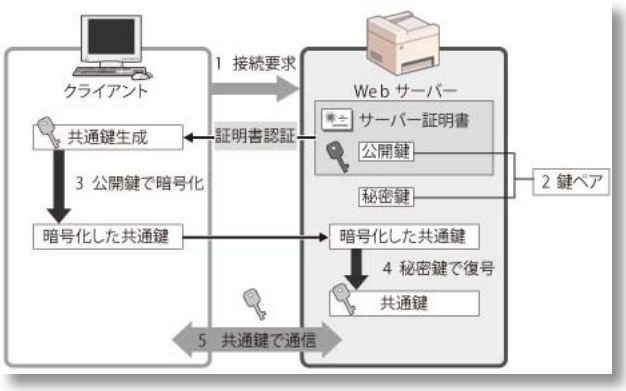
SSL暗号化通信を設定する

ユーザーがブラウザーを通してプリンター、複合機にアクセスする際に、プリンター、複合機にサーバー証明書を導入することで、SSL による安全な暗号化通信を実現できます。SSL 通信ではサーバー証明書と公開鍵を利用して、ユーザーとプリンター、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通信は、一部非対応の機種があります。非対応の機種については、外部ネットワークから接続できない環境でお使いになることをおすすめします。

SSL通信の仕組み（右図）

1. ユーザーのコンピューターからプリンター、複合機へアクセスするとき、SSLのサーバー証明書とサーバーの公開鍵を要求します。
2. プリンター、複合機からユーザーのコンピューターへ証明書と公開鍵が送られます。
3. サーバーから受け取った公開鍵を使用して、コンピューター内で独自に生成した共通鍵を暗号化します。
4. 暗号化した共通鍵をプリンター、複合機に送ります。
5. プリンターで秘密鍵を使用し、暗号化された共通鍵を復号する。
6. これによりユーザーのコンピューターとプリンター、複合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設定画面

※ SSL通信の設定手順については、本体同梱の取扱説明書を参照してください。

プリンター、複合機をパスワードで管理する
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、プリンター、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。キヤノンのプリンター、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。

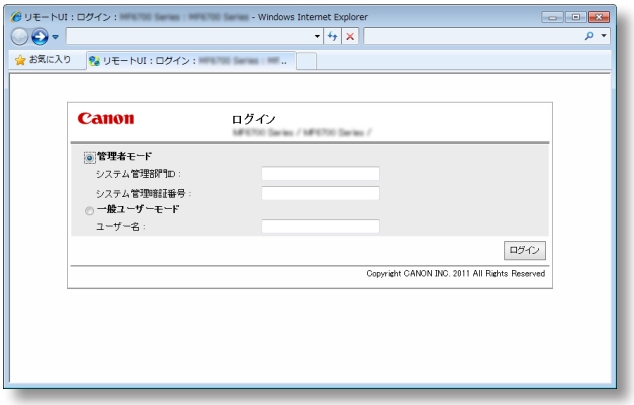
ここでご紹介する例以外の機能や情報においてもパスワードが設定できるものがあるので、必要に応じて適切に設定してください。

※ 各機能のパスワード設定手順については、本体同梱の取扱説明書を参照してください。

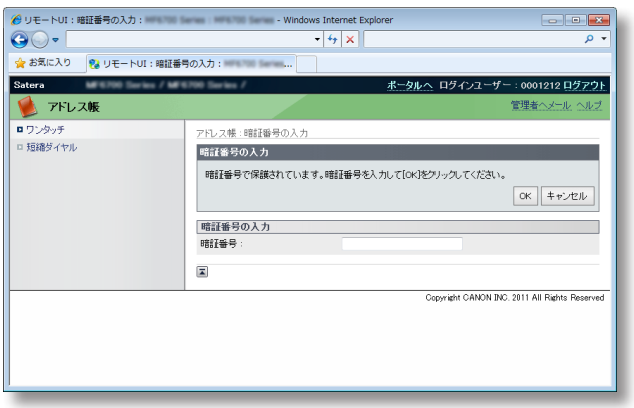
※ 各機能のパスワードは、リモートUIで設定できます。

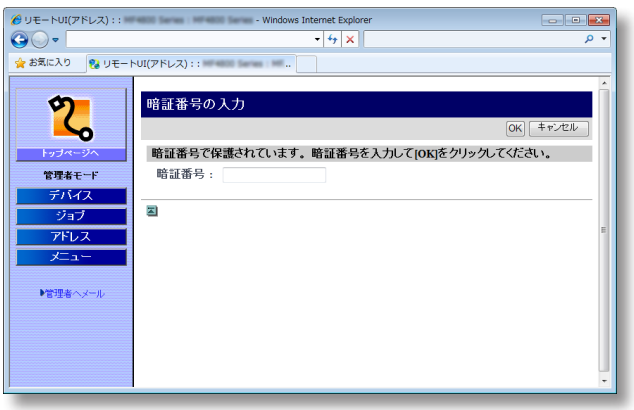
■各種画面

・ システム管理項目のパスワード入力画面



・ アドレス帳アクセス時のパスワード入力画面





その他

■リモートUI利用上での注意

Webブラウザーでプリンターのリモート 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。