

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

- $\cdot 10.0.0.0 \sim 10.255.255.255$
- 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



#### ※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

Ð	設定確認			
自動取得		: ON		
プロトコル選択		: DHCP		
Auto	) IP	: ON		
IPア	ドレス	: 192.168.74.130		
サフ	ブネットマスク	: 255.255.255.0		
ゲー	ートウェイアドレス	: 192.168.74.2		

# 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

■ ファイアウォール設定画面の例

### 本体操作パネル

₩ 設定/登録	9 個人設定	第二章 第二章 第二章	έØ		= ×==-
<ipv4アドレスフィルター:受< td=""><td>信フィルター</td><td>&gt;</td><td></td><td></td><td></td></ipv4アドレスフィルター:受<>	信フィルター	>			
■ フィルターを使用			ON	OFF	
■ デフォルトポリシー			許可	拒否	
例外アドレス	f	列外ポート番号	3		
172.24.108.23	ţ	指定なし			1/1
登録 ▶ 詳細/編集	▶				
× キャンセル				C	K J
状況確認	テム管理モー	ドです。			

※お使いの機種により、画面が異なることがあります。

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。

リモートリ
-------

aparent #O		*-9/~	19491-9-:	7654521 09791
※)設定/登録				管理者へメール
國境設定	設定/登録:環境設定:ネットワーク	2設定 > ファイアウォール設定 > IPv4アドレス:送信フ	ィルターの編集	
用紙設定	IPv4アドレス:送信	フィルターの編集		
表示設定	以下のように設定を変更します。 設定変更は次回宇電源ON時より#	めとなります。	ОК	キャンセル
94マー設定	送信フィルターの設定			
ネットワーク設定	☑フィルターを使用する			
外部インターフェイス設定	デフォルトポリシー :	<ul> <li>● 拒否</li> <li>● 許可</li> </ul>		
アクセシビリティー設定	例外アドレス			
音量調整	登録するアドレス:			違加
>>クション部定 共通設定 ンピー設定 プリンター設定 送信設定 受信(形法送定 ファイル発存/利用設定 せるこアプリン特定	* 300,000,000,000,000,000,000,000,000,000	のほうにいインノでさなと、達成するロアドルスを一度に設定 をと、カンパクス発生性性できます。(カンパックス長10~3) 用金	₹2)	
CH-4797971BOE				
よく使う設定	T			

# 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



5 システム管理者のログイン				
システム管理部門ID	1	2	3	
暗証番号	4	5	6	
	7	8	9	
ログイン				

※お使いの機種により、画面が異なることがあります。

#### 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。

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

- 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

# リモートリの使用を制限する

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。

## ■ リモートUIのON/OFF 設定画面の例

### 本体操作パネル

🔅 設定	/登録	19 個人設定	E 宛先/転送の 設定			≡ ×=⊐-
設定す	くリモートUIの01 設定変更はトップ	す。 V/OFF> ブページの「設定	の反映」の操作後に	こ有効となります	۲.	
トッフ 管理 ライ	0	N	OFF			
	•	TLSを使用				
ш						1/2
<u> </u>	× キャンセ	יעני		ОК	L.	V
◈ 状況確	認 🕕 シ	ステム管理モート	ヾです。		an-7-04	

※お使いの機種により、画面が異なることがあります。

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。

本体操作パネル
---------

I

OFF ON
OFF ON

# ■ リモートリログイン画面の例

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

ログイン画面③

Canon ログイン



ログイン画面2



#### ログイン画面④

いいの ログイン	Canon ロヴィン
3620 / IK C3620 /	m (3620 / m (3620 /
8월10 : 북한철육 : 0742 Copyright CANON INC. 2017	○館等長モード システム世球部に当時、 ・システム世球部に当時、 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
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。	07<> Copyright CANON INC. 2017
	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

BADY CBRD / BADY CBRD /		ログインユーザー: user <u>ログアウト</u>
<ul> <li>シッシュビロセ</li> <li>ワンタイムパスワードの入力</li> </ul>		更新日時:2024 07/02 20:35:57 📢
ワンタイムパスワード生成アプリに表示されたワンタイムパスワードをス	わしていださい。	確認 キャンセル
ユーザー名: ワンタイムバスワード:	user (688)	
×		
		Copyright CANON INC. 2020
二要素認証が設定 ワード入力後に、 られます。	されている場合、ユーサ ワンタイムパスワードの	「一名/パス )入力が求め

# 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

	第先/転送の 設定		
<鍵と証明書>			
鍵の名前	使用状況	証明書	
Default Key		E3	
AMS	使用中		
🔎 key1	使用中	<b>E</b>	
Device Signature Key	使用中		1/1
			$\mathbf{\nabla}$
使用鍵に 設定 → 証明書 詳細情報 → 使用先 表示	£	,	
		ОК	لد
☆ 状況確認	<sup>、</sup> です。		

※お使いの機種により、画面が異なることがあります。

### 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。

#### リモートリ

image/EDM/NE R	B C3620 / B	C3620 /		ボータルへ	ログインユーザー: 7654321 ログアウト
(米) 設定/登録					管理者へメール
環境設定		設定/登録:環境設定:ネ	ットワーク設定 > TLS設定 > 我	比証明書設定	
用紙設定		鍵と証明書設定			
表示設定		鍵と証明書設定			
タイマー設定		登録されている鍵と証明書			
ネットワーク設定		鍵の名前	鍵の使用先	証明書	
外部インターフェイス設定		Default Key	[TLS]	100	使用減量錄
アクセシビリティー設定		*			
音量调整					
ファンクション設定					
共通設定					
コピー19定					
プリンター設定					
送信設定					
受信/転送設定					
ファイル保存/利用設定					
セキュアプリント設定					
F/48319**					

# 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	本体操作パネル	
	□ ホーム	
<定期アップデート>	))	1
<ul> <li>定期アップデート設定</li> <li>ON</li> <li>OFF</li> <li>配信予定がある場合、配信終了までの間は設定は無効になります。</li> </ul>	● 「 ● 「 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	アーム
<ul> <li>アップデート時間 確認の終了までに、設定した時間から最大3時間かかることがあります。</li> </ul>		- ゲ 史፣
<ul> <li>確認時間 隔週 ▼ (未設定) ▼</li></ul>	<b>†</b>	
(0~23) Eメール	操作ガイド	
× キャンセル OK 」		
£		

カウンター確認

IDカー

♦ 状況確認

※お使いの機種により、画面が異なることがあります。

# 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

<ul> <li></li></ul>	宛先/転送の 設定		= ×==-
<ul> <li>              記動時のシステム検証      </li> </ul>	ON	OFF	
■ ランタイムシステム保護			
<ul> <li>× キャンセル</li> <li>◇ 状況確認</li> <li>● システム管理モードで</li> </ul>	<b>す</b> 。	OK	له

※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

### リモートリ

<b></b>			ポータルヘ ログイン	ンユーザー: 1 <u>ログアウト</u>
	ህፖ			
← デバイス管理 監査ログのエクスポート/クリア 監査ログ情報	監査ログのエクスポート/クリア:監査ログ情報	査ログ情報	更新日時 : 2	2022 06/07 18:31:14 📢
監査ログの目動エクスボート設定	監査ログの収集:	停止 開始		
監査ログのエクスポート 監査ログの刑除 Syslog設定	現在のログ保存件数: ログの最終収集日時: ログの最終保存日時: 目動エクスポートの利用: Syslog送信の利用:	0 OFF OFF		
	自動エクスポートの実行状況			
	実行日時	状况	詳細	
	Syslogの送信エラー状況			
	送信日時	状況	詳細	
	Ŧ			
				Copyright CANON INC. 2020

※お使いの機種により、画面が異なることがあります。

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

#### 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。

### ■ セキュリティーポリシー設定画面の例



※お使いの機種により、画面が異なることがあります。

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。

[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。

