

EPSON

ネットワークガイド

目次

商標	4	印刷機能を使う	23
		サーバークライアント型接続での印刷設定	24
		ピアツーピア型接続での印刷設定	27
マニュアルの見方	5	メールサーバーを設定する	27
マークの意味	5	メールサーバー設定項目	28
マニュアル記載の前提	5	メールサーバーとの接続を確認する	29
OS表記	5	システムの詳細を設定する	31
マニュアルのご注意	6	操作パネルの動作を設定する	31
		無操作時の省電力設定をする	32
		タイムサーバーと日付/時刻を同期する	32
はじめに	7	本体のセキュリティー編	33
マニュアルの構成	7	本体のセキュリティー機能の紹介	33
マニュアルで使用する用語	8	管理者パスワードの変更	33
用語	8	Web Configから管理者パスワードを変更する	33
ネットワーク環境の例	9	外部インターフェイスを無効にする	34
プリンター接続のタイプ	12		
プリンターの設定と管理	15	運用・管理編	35
プリンター設定、管理の流れ	15	管理者としてプリンターにログオンする	35
プリンターのネットワーク接続	16	Web Configで管理者としてログオンする	35
印刷機能設定	16	プリンターの情報を確認する	35
メールサーバー設定	16	操作パネルから情報を確認する	35
セキュリティー設定	16	Web Configから情報を確認する	36
運用・管理	17	イベント発生時にメール通知を受け取る	36
ネットワーク接続編	18	メール通知の概要	36
ネットワーク接続の前に	18	メール通知を設定する	36
接続設定情報の収集	18	ファームウェアのアップデート	37
IPアドレスの割り当て	18	プリンターをインターネットに接続しないで	
DNSサーバー、プロキシサーバーについて	19	ファームウェアをアップデートする	37
操作パネルでネットワークに接続する	19	設定のバックアップ	38
IPアドレスを設定する	19	設定をエクスポートする	38
有線LANに接続する	21	設定をインポートする	38
機能設定編	22	トラブルを解決する	40
設定に使うソフトウェア	22	トラブルを解決するための糸口	40
Web Config（デバイスのウェブページ）	22	プリンターの状態を確認する	40
		エラーメッセージを確認する	40
		通信状態を確認する	42
		接続テストをする	46

設定の初期化	47
トラブル事例	47
Web Configにアクセスできない	47
管理者パスワードを忘れた	48

付録49

ネットワーク関連のソフトウェア	49
Epson Device Admin	49
EpsonNet Config (Windowsのみ)	49
EpsonNet Print (Windowsのみ)	50
プリンターが使用するポート	50

エンタープライズセキュリティー設定 編52

セキュリティー設定と防止できる脅威	53
セキュリティー機能の設定	54
パスワードを暗号化する	54
プリンターとのSSL/TLS通信	54
使用できる電子証明書	54
CA署名証明書の取得とインポート	55
CA署名証明書を削除する	58
相手サーバー検証用CA証明書を設定する	58
利用するプロトコルを制御する	60
プロトコルを制御する	60
有効・無効が設定可能なプロトコル	60
プロトコルの設定項目	61
IPsec/IPフィルタリングで暗号化通信する	64
IPsec/IPフィルタリングの概要	64
基本ポリシーを設定する	64
個別ポリシーを設定する	68
IPsec/IPフィルタリングの設定例	74
IPsec/IPフィルタリングで使用する証明書を 設定する	75
IEEE802.1X環境にプリンターを接続する	75
IEEE802.1Xを設定する	75
IEEE802.1Xで使用する証明書を設定する	77
プリンターのIEEE802.1X状態表示	77
トラブルを解決する	78
セキュリティー設定の初期化	78
セキュア環境への接続時のトラブル	79
電子証明書使用時のトラブル	81

商標

- Microsoft、Windowsは、マイクロソフト グループの企業の商標です。
- Apple、Mac、macOS、OS X、Bonjourは米国およびその他の国で登録されたApple Inc.の商標です。
- その他の製品名は各社の商標または登録商標です。

マニュアルの見方

マークの意味

⚠ 注意 この内容を見逃して誤った取り扱いをすると、人が傷害を負う可能性および財産の損害の可能性が想定される内容を示しています。

！重要 必ず守っていただきたい内容を記載しています。この内容を見逃して誤った取り扱いをすると、本製品の故障や、動作不良の原因になる可能性があります。

参考 補足情報や参考情報を記載しています。

関連情報

➡ 関連したページにジャンプします。

マニュアル記載の前提

- 画面やイラストの詳細はお使いのプリンターとは異なることがありますが、操作方法は同じです。
- 画面はお使いのOSやバージョンにより異なることがあります。
- 機種や設定状況により画面の設定項目は異なることがあります。

OS表記

Windows

本書では、以下のOS（オペレーティングシステム）をそれぞれ「Windows 11」「Windows 10」「Windows 8.1」「Windows 8」「Windows 7」と表記しています。また、これらの総称として「Windows」を使用しています。

- Microsoft® Windows® 11 operating system 日本語版
- Microsoft® Windows® 10 operating system 日本語版
- Microsoft® Windows® 8.1 operating system 日本語版
- Microsoft® Windows® 8 operating system 日本語版
- Microsoft® Windows® 7 operating system 日本語版

Mac OS

本書では、「Mac OS X v10.9.5」以降の総称として「Mac OS」を使用しています。

マニュアルのご注意

- 本書の内容の一部または全部を無断転載することを禁止します。
- 本書の内容は将来予告なしに変更することがあります。
- 本書の内容にご不明な点や誤り、記載漏れなど、お気づきの点がございましたら弊社までご連絡ください。
- 運用した結果の影響については前項に関わらず責任を負いかねますのでご了承ください。
- 本製品が、本書の記載に従わずに取り扱われたり、不適當に使用されたり、弊社および弊社指定以外の、第三者によって修理や変更されたことなどに起因して生じた障害等の責任は負いかねますのでご了承ください。

©2025 Seiko Epson Corporation

はじめに

本書はシステム管理者向けに、プリンターを使用するための設定や運用、管理方法を記載した機種共通のマニュアルです。

共通マニュアルのため、機種によっては使用できない機能や表示されないメニューがあります。差分の情報は設定項目やメニューなどの近くで説明します。

それぞれの機能を使用する方法は『ユーザズガイド』をご覧ください。

マニュアルの構成

プリンターの設定と管理

プリンターのネットワーク設定～管理・運用までの流れを簡単な図で表します。

接続編

デバイスをネットワークに接続する方法を説明しています。プリンターが使用するポートやDNS、プロキシサーバーの設定も説明しています。

機能設定編

プリンターの各機能を使用するための設定を説明しています。

本体のセキュリティ編

管理者パスワードの設定や利用者制限などプリンター本体に設定する、基本的なセキュリティのことを説明しています。

運用・管理編

プリンターの情報確認や、イベント発生時の通知設定など、使用開始後の運用、管理を説明しています。

トラブルを解決する

設定の初期化とネットワークのトラブルシューティングを説明しています。

エンタープライズセキュリティ設定編

SSL/TLS通信やIPsec/IPフィルタリングなど、ネットワークで機能する高度なセキュリティ機能を説明しています。

マニュアルで使用する用語

用語

本書では以下の用語を使用しています。

システム管理者

企業や組織などでデバイスやネットワークに関して設置や設定をする権限を持つ人を指しています。小規模な組織ではネットワーク管理者、デバイス管理者を兼ねているケースがあります。大規模な組織では、部や課といった組織のグループ内のネットワークや機器に関しての権限を持つ人を指していて、インターネットなど組織外への通信設定の権限はネットワーク管理者が担います。

ネットワーク管理者

企業や組織などでネットワーク通信の制御を担当している人を指しています。ルーターやプロキシサーバー、DNSサーバー、メールサーバーなど、インターネットやネットワーク間の通信を制御している人です。

ユーザー（利用者）

プリンターやスキャナーなどのデバイスを使用するエンドユーザーを指しています。

サーバークライアント型接続（Windowsベースのプリントサーバーによるプリンター共有）

プリンターをWindowsベースのプリントサーバーにネットワークまたはUSBケーブルなどで接続し、サーバーで設定したプリントキューを共有する接続を指しています。プリンターとコンピューターの通信はサーバーを経由し、プリンターの制御をサーバーで行います。

ピアツーピア型接続（直接印刷）

プリンターとコンピューターがハブやアクセスポイントなどでネットワークに接続されていて、コンピューターから直接プリンターに印刷を実行する接続を指しています。

Web Config（デバイスのウェブページ）

デバイスに内蔵しているウェブサーバーです。Web Config（ウェブ コンフィグ）と表記しています。ネットワークからブラウザを使ってデバイスの情報確認や設定ができます。

プリントキュー

Windowsの場合、[デバイスとプリンター]にあるプリンターのポートごとに作られるアイコンを指しています。1台のプリンターでもStandard TCP/IPやWSDなどネットワークに接続しているポートにそれぞれのアイコンが作成されます。

ツール

Epson Device Admin（エプソン デバイス アドミン）やEpsonNet Config（エプソンネット コンフィグ）など、デバイスの設定や管理を行うソフトウェアの総称として使用しています。

ASCII（アスキー、American Standard Code for Information Interchange）

標準的な文字コードの一つです。アルファベット（a-z、A-Z）やアラビア数字（0-9）、記号、空白文字、制御文字などを収録した128文字が規定されています。本書で「ASCII文字」と表記している場合、下表にある0x20～0x7E（16進数）を指し、制御文字は含みません。

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
20	sp*	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
30	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
40	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
50	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
60	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
70	p	q	r	s	t	u	v	w	x	y	z	{		}	~	

* 空白文字（スペース）です。

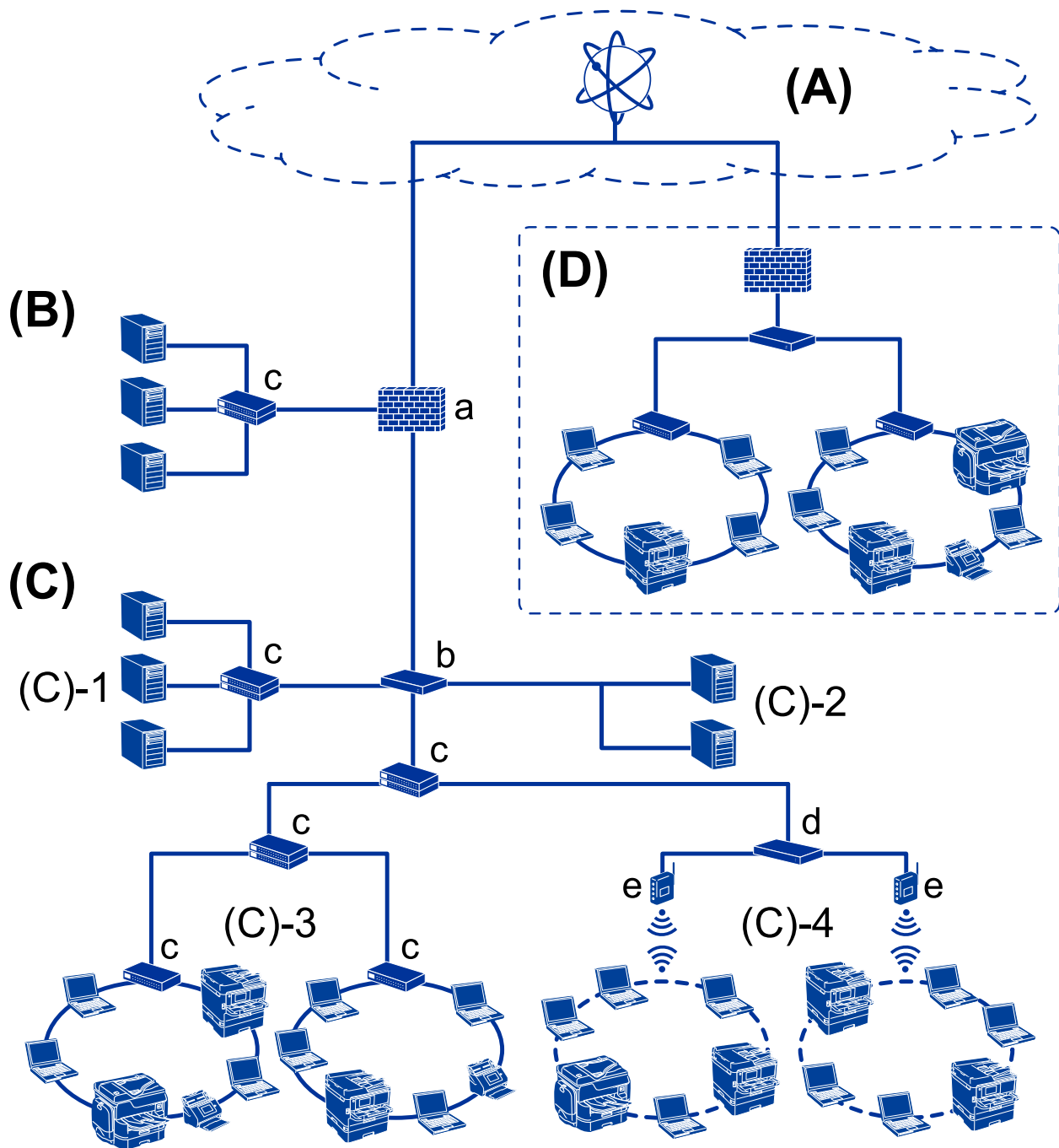
Unicode (UTF-8)

国際的な文字コード規格です。世界中の主な言語で主に使われる文字をカバーしています。「UTF-8」とある場合、UTF-8形式で符号化した文字を指します。

ネットワーク環境の例

製品を接続するネットワーク環境の例です。お使いの製品で利用できない機能やサービスが含まれている場合があります。

企業向けネットワークの例（中～大規模）



(A) : インターネット

プリンターがインターネットに接続できると、以下のようなサービスを利用できます。

- Epson Connect
メールプリント、リモートプリントなど
- クラウドサービス
Googleクラウドプリント、Evernoteなど
- エプソンのサイト
ドライバーやアプリケーションソフトのダウンロード、ファームウェアのアップデートなど

(B) : DMZ (非武装地帯)

内部ネットワーク（イントラネット）と外部ネットワーク（インターネット）の中間にあって、どちらからもファイアウォールで隔離されたセグメントです。一般的に外部へ公開するサーバーを配置します。外部からの脅威を内部ネットワークへ拡散することを防止できます。また、内部から公開サーバーへの不正アクセスも防止できます。

- DNSサーバー
- プロキシサーバー
- メール転送サーバー
- ウェブサーバー
- FTPサーバー

(C) : トラストゾーン（イントラネット）

ファイアウォールやUTM（総合脅威管理）で守られた信頼性のあるネットワークです。

- (C) -1 : イン트라ネット内サーバー
組織内のコンピューターに対してそれぞれのサービスを提供します。
 - DNSサーバー
 - DHCPサーバー
 - メールサーバー
 - Active Directoryサーバー／LDAPサーバー
 - ファイルサーバー
- (C) -2 : アプリケーションサーバー
組織内のコンピューターに以下のようなサーバーアプリケーションの機能を提供します。
 - Epson Print Admin
 - Document Capture Pro Server
- (C) -3 : 有線LAN (Ethernet) 、 (C) -4 : 無線LAN (Wi-Fi)
プリンターやスキャナー、コンピューターなどをLANケーブルや無線でLANに接続します。

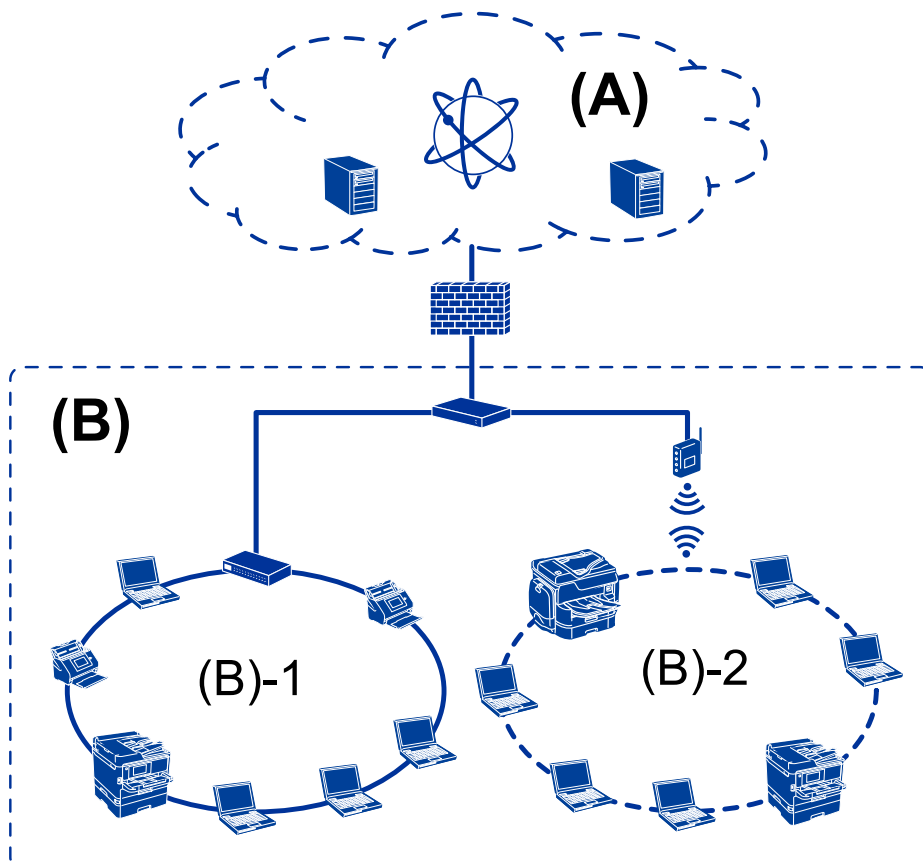
(D) : 他の拠点

他の拠点のネットワークです。インターネットや専用線などで拠点同士が接続されます。

ネットワーク装置

- a : ファイアウォール、UTM
- b : ルーター
- c : LANスイッチ
- d : 無線LANコントローラー
- e : アクセスポイント

企業向けネットワークの例（小規模）



(A) : インターネット

- Epson Connect
- クラウドサービス
- メールサーバー、FTPサーバー

(B) : トラストゾーン（イントラネット）

- (B) -1 : 有線LAN (Ethernet)
- (B) -2 : 無線LAN (Wi-Fi)

プリンター接続のタイプ

プリンターのネットワーク接続は主に以下の2つのタイプがあります。

- サーバークライアント型接続（Windowsベースのプリントサーバーによるプリンター共有）
- ピアツーピア型接続（直接印刷）

サーバークライアント型接続設定

サーバーになるコンピュータがプリンターを共有する接続です。プリンターにサーバー経由以外の通信を遮断すると、セキュリティを強化できます。

USBで接続するとネットワーク機能がないプリンターも共有できます。

接続方法：

プリンターをLANスイッチやアクセスポイントを介して直接ネットワークに接続します。

プリンターとサーバーをUSBケーブルで直接接続することもできます。

プリンタードライバー（通信ドライバー）：

Windowsベースのプリントサーバー上に、クライアントコンピュータのOSにおけるシステムの種類に対応したドライバーをインストールします。

Windowsベースのプリントサーバーにアクセスしてプリンターをリンクすると、クライアントコンピュータにインストールされて使用できるようになります。

特徴：

- プリンターやプリンタードライバー（通信ドライバー）を一括管理できます。
- 全ての印刷データはサーバーを経由するため、サーバーの能力によっては印刷開始までに時間がかかることがあります。
- Windowsベースのプリントサーバーが停止していると印刷できません。

関連情報

➡ [「用語」8ページ](#)

ピアツーピア型接続設定

プリンターとネットワーク上のコンピュータが直接通信する接続です。ネットワーク対応プリンターのみ接続できます。

接続方法：

プリンターをハブやアクセスポイントを介して直接ネットワークに接続します。

プリンタードライバー（通信ドライバー）：

- Windows：
プリンターに付属のEpson Edge Print PROなどのソフトウェアRIPと通信ドライバーをコンピュータにインストールします。
- Mac OS：
ソフトウェアRIPをコンピュータにインストールします。

Features:

- プリンターに直接印刷データを送るので、印刷開始までに時間がかかりません。
- プリンターが稼働していれば印刷できます。

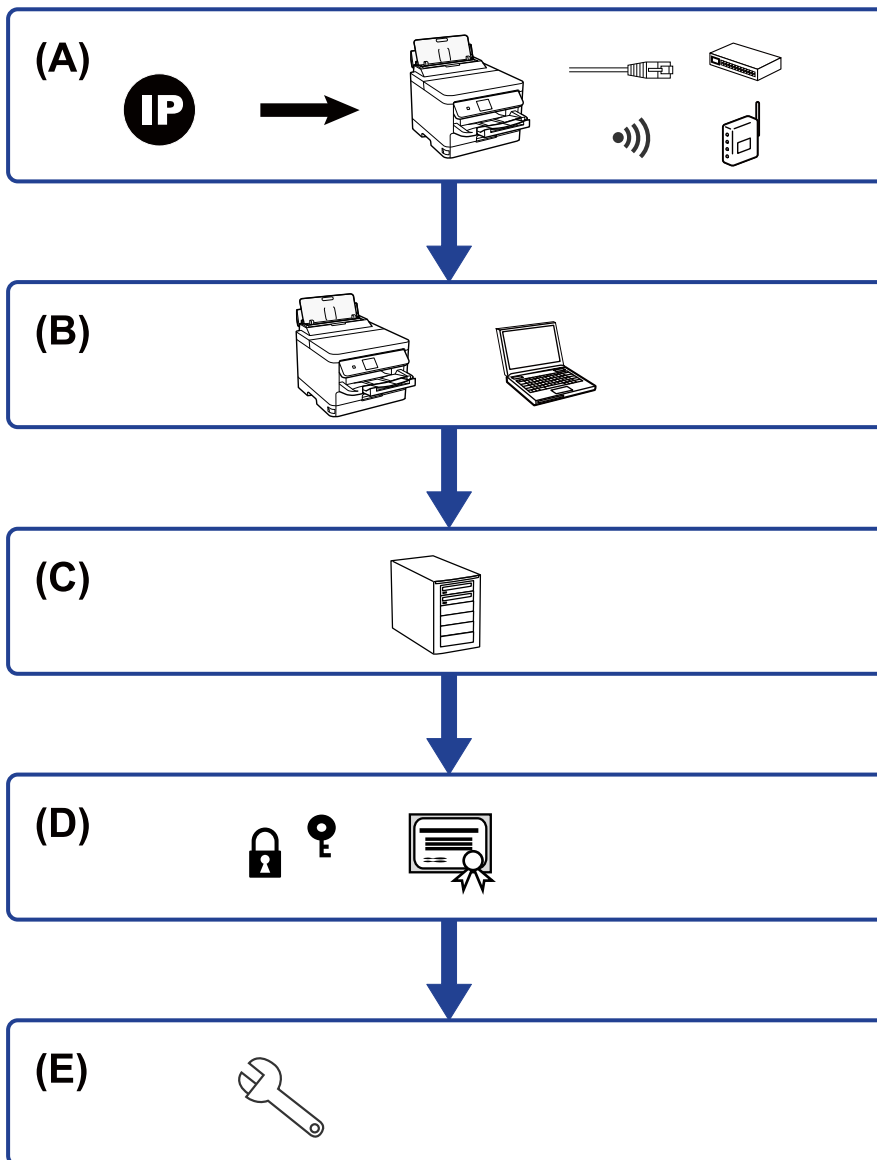
はじめに

関連情報

➡ [「用語」 8ページ](#)

プリンターの設定と管理

プリンター設定、管理の流れ



A	プリンターのネットワーク接続	B	印刷機能設定
C	サーバー設定	D	セキュリティ設定
E	運用・管理		

プリンターのネットワーク接続

プリンターにIPアドレスを設定して、ネットワークに接続します。

- IPアドレス設定
- ネットワークへの接続

関連情報

➡ [「ネットワーク接続編」18ページ](#)

印刷機能設定

印刷機能を使うための設定をします。

- サーバークライアント型接続での印刷設定
- ピアツーピア型接続での印刷設定

関連情報

➡ [「印刷機能を使う」23ページ](#)

メールサーバー設定

メール通知のためにメールサーバーを設定します。

- SMTPサーバー
- POP3サーバー

関連情報

➡ [「メールサーバーを設定する」27ページ](#)

セキュリティー設定

- 管理者パスワード設定
- 利用者制限設定
- プロトコル制御設定
- 高度なセキュリティー設定

関連情報

➡ [「本体のセキュリティー編」33ページ](#)

➡ [「エンタープライズセキュリティー設定編」52ページ](#)

運用・管理

- デバイスの状況確認
- イベント発生への対応
- デバイス設定のバックアップ

関連情報

➡ [「運用・管理編」35ページ](#)

ネットワーク接続編

この章では、プリンターをネットワークに接続するための手順を説明しています。

ネットワーク接続の前に

ネットワーク接続するには、接続方法と接続のための設定情報を事前に確認してください。

接続設定情報の収集

接続に必要な設定情報を用意します。事前に以下の情報を確認してください。

区分	項目	備考
LAN接続情報	<ul style="list-style-type: none"> IPアドレス サブネットマスク デフォルトゲートウェイ 	<p>プリンターに割り当てるIPアドレスを決定します。</p> <p>静的にIPアドレスを割り当てる場合は、全ての項目の値が必要です。DHCP機能で動的にIPアドレスを割り当てる場合は、自動設定されるのでLAN接続の情報は不要です。</p>
DNSサーバー情報	<ul style="list-style-type: none"> プライマリーDNSのIPアドレス セカンダリーDNSのIPアドレス 	<p>プリンターに静的IPアドレスを割り当てる場合に必要です。セカンダリーDNSはシステムを冗長構成にしてセカンダリーDNSサーバーがある場合に設定します。</p> <p>小規模なネットワークでDNSサーバーを構築していない場合は、ルーターのIPアドレスを設定します。</p>
プロキシサーバー情報	<ul style="list-style-type: none"> プロキシサーバー名 	<p>イントラネットからインターネットへの接続にプロキシサーバーを利用しているネットワーク環境において、プリンターが直接インターネットにアクセスする機能を使用する場合は設定してください。</p> <p>以下の機能はプリンターが直接インターネットにアクセスします。</p> <ul style="list-style-type: none"> ファームウェア更新
ポート番号情報	<ul style="list-style-type: none"> 開放するポート番号 	<p>プリンターやコンピューターが各機能で使用するポート番号を確認して、ファイアウォールでブロックされているポートを、必要に応じて開放してください。</p> <p>プリンターが使用するポート番号の情報は「付録」をご覧ください。</p>

IPアドレスの割り当て

IPアドレス（IPv4）の割り当てには、以下のタイプがあります。

固定IPアドレス：

あらかじめ決めたIPアドレスを手動でプリンター（ホスト）に割り当てます。

ネットワークに接続するための情報（サブネットマスク、デフォルトゲートウェイ、DNSサーバー設定など）を手動で設定する必要があります。

デバイスの電源を切ってもIPアドレスは変更されないので、IPアドレスの変更を追従できない環境やIPアドレスでデバイスを管理したい場合に利用できます。多数のコンピューターがアクセスする、プリンターやサーバーなどへの設定をお勧めします。また、IPsec/IPフィルタリングなどのセキュリティー機能を利用する場合は、IPアドレスが変更されないよう固定IPアドレスを割り当ててください。

DHCP機能による自動割り当て（動的IPアドレス）：

DHCPサーバーやルーターのDHCP機能を使って自動でIPアドレスをプリンター（ホスト）に割り当てます。ネットワークに接続するための情報（サブネットマスク、デフォルトゲートウェイ、DNSサーバー設定など）も自動で設定されるので、デバイスのネットワークへの接続が容易にできます。

デバイスやルーターの電源を切る、または、DHCPサーバーの設定により、再接続の際にIPアドレスが変更になる場合があります。

IPアドレス以外でのデバイス管理やIPアドレスを追従できるプロトコルでの通信をお勧めします。

 **参考** DHCPのIPアドレス予約機能を使用すると、常にデバイスに同じIPアドレスを割り当てることができます。

DNSサーバー、プロキシサーバーについて

DNSサーバーは、ホスト名やメールアドレスのドメイン名などとIPアドレスの情報を関連付けて持っています。コンピューターやプリンターがIP通信をするときに、ホスト名やドメイン名などで相手先を記述すると通信ができません。

その情報をDNSサーバーに問い合わせ、相手先のIPアドレスを取得します。この処理を名前解決と言います。これによりコンピューターやプリンターなどのデバイスは、IPアドレスを使って通信できるようになります。プリンターがメールを使ったり、インターネット接続をして通信したりするには、名前解決が必要です。これらの機能を使用するには、DNSサーバーの設定をしてください。

プリンターのIPアドレスをDHCPサーバーやルーターのDHCP機能で割り当てるとは自動設定されます。プロキシサーバーはネットワークとインターネットとの出入り口に配置され、コンピューターやプリンターとインターネット（相手サーバー）の代理でそれぞれのデバイスと通信します。相手サーバーはプロキシサーバーとだけ通信しているように見えます。よって、プリンターに設定されているIPアドレスやポート番号などの情報を読み取れなくなり、セキュリティーの向上が期待できます。プロキシサーバーを介してインターネット接続をしている場合は、プリンターにプロキシサーバーの設定をしてください。

操作パネルでネットワークに接続する

プリンターの操作パネルを使って、プリンターをネットワークに接続します。
操作パネルの詳細説明は『ユーザズガイド』をご覧ください。

IPアドレスを設定する

ホストアドレスやサブネットマスク、デフォルトゲートウェイなど、基本的なIPアドレス設定をします。
ここでは固定IPアドレスを設定する手順を説明します。

1. プリンターの電源を入れます。

2. 操作パネルのホーム画面でMenuを選択します。

3. [本体設定] - [ネットワーク設定] - [詳細設定] の順に選択します。

4. [TCP/IP] を選択します。

5. [TCP/IP設定方法] を [手動設定] にします。

IPアドレスをルーターなどのDHCP機能で自動設定する場合は [自動設定] にします。この場合は、手順6、7の [IPアドレス]、[サブネットマスク]、[デフォルトゲートウェイ] も自動設定になるので入力できません。手順8へ進んでください。

6. IPアドレスを入力します。

◀または▶を選択すると、ピリオドで区切られた前後の区切りにフォーカスが移動します。
戻った画面で入力した値が反映されていることを確認してください。

7. 同様に [サブネットマスク]、[デフォルトゲートウェイ] を設定します。

戻った画面で入力した値が反映されていることを確認してください。

！重要 IPアドレス、サブネットマスク、デフォルトゲートウェイの組み合わせが不正の場合、[設定を開始する] が有効にならず、設定を続けることができません。入力に間違いがないか確認してください。

8. プライマリーDNSサーバーのIPアドレスを入力します。

戻った画面で入力した値が反映されていることを確認してください。

参考 IPアドレスを [自動設定] にすると、DNSサーバー設定は [手動設定]、[自動設定] を選択できます。DNSサーバーのアドレスを自動取得できない場合に [手動設定] を選択して、DNSサーバーのIPアドレスを入力してください。引き続き、セカンダリーDNSサーバーのアドレスを直接入力します。[自動設定] を選択した場合は、手順10へ進んでください。

9. セカンダリーDNSサーバーのIPアドレスを入力します。

戻った画面で入力した値が反映されていることを確認してください。

10. [設定を開始する] をタップします。

プロキシサーバーを設定する

以下の両方に当てはまる場合は、プロキシサーバーを設定してください。

- インターネット接続用にプロキシサーバーを構築している
- 本体パネルまたはWeb Configから、インターネットを通じてプリンターファームウェアの更新を行う

1. ホーム画面でMenuを選択します。

IPアドレスの設定に続いて設定するときは、[詳細設定] 画面が表示されています。手順3に進んでください。

2. [本体設定] - [ネットワーク設定] - [詳細設定] の順に選択します。

3. [プロキシサーバー] を選択します。

4. 【プロキシサーバー使用設定】を【使用する】にします。
5. プロキシサーバーのアドレスを、IPv4アドレスまたはFQDN形式で入力します。
戻った画面で入力した値が反映されていることを確認してください。
6. プロキシサーバーのポート番号を入力します。
戻った画面で入力した値が反映されていることを確認してください。
7. 【設定を開始する】をタップします。

有線LANに接続する

LANケーブルでネットワークに接続して、接続の確認をします。

1. プリンターとハブ（LANスイッチ）をLANケーブルで接続します。
2. ホーム画面でMenuを選択します。
3. 【本体設定】 - 【ネットワーク設定】の順に選択します。
4. 【接続診断】を選択します。
接続診断の結果が表示されます。正常に接続されていることを確認してください。
5. 【OK】をタップして終了します。
【接続診断結果を印刷する】をタップすると診断結果を印刷できます。画面の案内に従って印刷してください。

機能設定編

この章では、デバイスの各機能を使うために始めに設定する部分の説明をしています。

設定に使うソフトウェア

ここではWeb Configを使って、システム管理者のコンピューターから設定する手順を中心に紹介します。

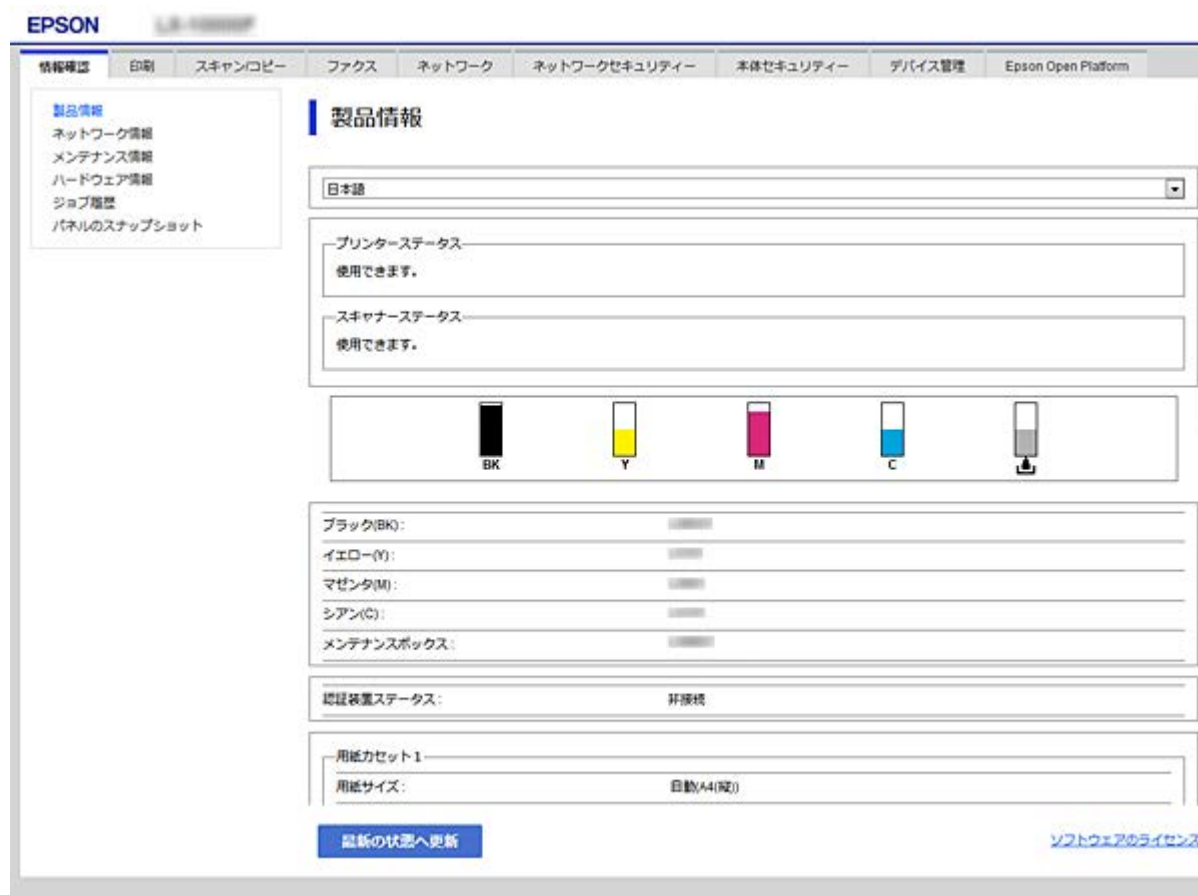
Web Config（デバイスのウェブページ）

Web Configの概要

Web Configは、プリンターの設定確認や変更がブラウザ上でできるプリンター内蔵のWebページです。ネットワークに接続されているプリンターを管理者のコンピューターから操作できます。

Web Configを使用するには、事前にプリンターにIPアドレスを設定しておく必要があります。

参考 プリンターに管理者パスワードを設定すると、管理者以外が設定を変更できないようにロックできます。



Web Configの起動

ネットワーク上のコンピューターやデバイスからブラウザを起動して、プリンターのIPアドレスを入力します。ブラウザのJavaScriptを有効にしてください。HTTPSアクセス時にプリンターが所有する自己署名証明書を使用するため、Web Configを起動するとブラウザに警告が表示されますが、問題ありません。

- HTTPSアクセス
IPv4 : `https://プリンターのIPアドレス`
IPv6 : `https://[プリンターのIPアドレス]`
- HTTPアクセス
IPv4 : `http://プリンターのIPアドレス`
IPv6 : `http://[プリンターのIPアドレス]`

記入例

- IPv4:
`https://192.0.2.111/`
`http://192.0.2.111/`
- IPv6:
`https://[2001:db8::1000:1]/`
`http://[2001:db8::1000:1]/`

参考 DNSにプリンター名を登録すると、IPアドレスの代わりにプリンター名が使用できます。

！重要

本機には管理者以外のユーザーに使用制限をかけられる機能があります。
管理者パスワードでログインすると、全ての機能を使用できます。管理者パスワードはあらかじめ設定されています。
使用開始後は管理者パスワードを初期パスワードのまま使用し続けず、任意のパスワードに変更することをお勧めします。

変更方法

[「管理者パスワードの変更」33ページ](#)

管理者ユーザー名の初期値は空白（何も入力していない状態）です。

関連情報

- ➡ [「プリンターとのSSL/TLS通信」54ページ](#)
- ➡ [「使用できる電子証明書」54ページ](#)

印刷機能を使う

ネットワーク接続でプリンターから印刷できるようにします。

ネットワークでプリンターを使用するには、プリンターのネットワーク接続以外に、コンピューターにネットワーク用のポート設定が必要です。

- サーバークライアント型の接続：サーバーコンピューター
サーバークライアント型の接続時に手動で設定する方法を説明します。
- ピアツーピア型の接続：それぞれのコンピューター
プリンターとコンピューターが一对一の関係になるピアツーピア型の接続では、製品のソフトウェアディスクのインストーラーやウェブインストーラーを使用して自動設定する方法を説明します。

サーバークライアント型接続での印刷設定

サーバークライアント型で接続したプリンターから印刷できるようにします。

サーバークライアント型の接続では、先にプリントサーバーのコンピューターから印刷できるように設定してから、プリンターをネットワークで共有してプリントサーバー経由で印刷できるようにします。

USBケーブルでサーバーに接続した場合も同様に、コンピューターからプリンターに印刷できるように設定してからプリンターをネットワークで共有します。

ネットワークポートを設定する

一般的なStandard TCP/IPを使用してプリントサーバーのコンピューターにネットワーク印刷用のプリントキューを作成し、ネットワークポートを設定します。

1. デバイスとプリンターの画面を開きます。

〔デスクトップ〕 - 〔設定〕 - 〔コントロールパネル〕 - 〔ハードウェアとサウンド〕（または〔ハードウェア〕） - 〔デバイスとプリンター〕の順に選択します。

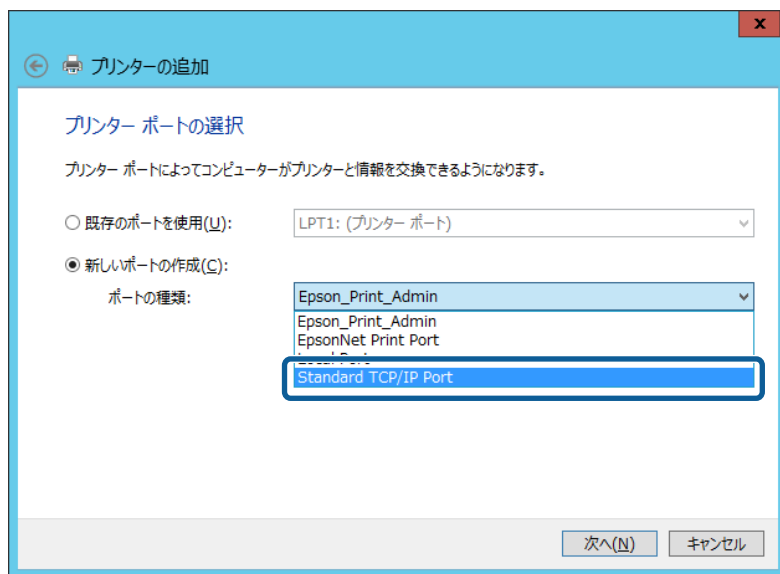
2. プリンターを追加します。

〔プリンターの追加〕をクリックして、表示される画面で〔探しているプリンターはこの一覧にはありません〕を選択します。

3. ローカルプリンターを追加します。

〔ローカルプリンターまたはネットワークプリンターを手動設定で追加する〕を選択して、〔次へ〕をクリックします。

4. 〔新しいポートの作成〕を選択し、ポートの種類から〔Standard TCP/IP Port〕を選択して、〔次へ〕をクリックします。



5. 〔ホスト名またはIP アドレス〕（または〔プリンター名またはIP アドレス〕）にプリンター名、またはプリンターのIP アドレスを入力して、〔次へ〕をクリックします。

記入例：

- プリンター名：EPSONA1A2B3C
- IPアドレス：192.0.2.111

〔ポート名〕 は変更しないでください。

〔ユーザーアカウント制御〕 画面が表示されたときは〔続行〕 をクリックします。

参考 名前で検索が可能なネットワークでプリンター名を指定した場合は、DHCPによってプリンターのIPアドレスが変更になっても追従ができます。プリンター名は、操作パネルのネットワーク情報表示またはネットワークステータスシートで確認できます。

6. プリンタードライバー（通信ドライバー）を設定します。

- 通信ドライバーとソフトウェアRIPがインストールされている場合:
〔製造元〕 - 〔プリンター〕 を選択します。〔次へ〕 をクリックします。
- 通信ドライバーとソフトウェアRIPがインストールされていない場合
お使いのプリンターの〔セットアップガイド〕 をご覧になり、通信ドライバーとソフトウェアRIPをインストールしてください。

7. この後は、画面の指示に従って操作します。

サーバークライアント型接続（Windowsベースのプリントサーバーによるプリンター共有）でプリンターを使用する場合は、続いてプリンターを共有設定します。

関連情報

➡ [「プリンターを共有する（Windowsのみ）」 26ページ](#)

ポート構成を確認する - Windows

プリントキューに適切なポートが設定されているか確認します。

1. デバイスとプリンターの画面を開きます。

〔デスクトップ〕 - 〔設定〕 - 〔コントロールパネル〕 - 〔ハードウェアとサウンド〕（または〔ハードウェア〕） - 〔デバイスとプリンター〕 の順に選択します。

2. プリンターのプロパティ画面を開きます。

対象プリンターのアイコンを右クリックして、[プリンターのプロパティ] をクリックします。

3. [ポート] タブをクリックし、[標準のTCP/IPポート] を選択して、[ポートの構成] をクリックします。

4. ポートの構成を確認します。

- RAWの場合
[プロトコル] で [Raw] が選択されていることを確認して、[OK] をクリックします。
- LPRの場合
[プロトコル] で [LPR] が選択されていることを確認します。[LPR 設定] の [キュー名] に「PASSTHRU」と入力します。[LPRバイトカウントを有効にする] をチェックして、[OK] をクリックします。

プリンターを共有する（Windowsのみ）

サーバークライアント型接続（Windowsベースのプリントサーバーによるプリンター共有）でプリンターを使用する場合は、プリントサーバーからプリンターを共有設定します。

1. プリントサーバーのコンピュータで [コントロールパネル] - [デバイスとプリンター] の順に選択します。
2. 共有したいプリンターアイコン（プリントキュー）を右クリックして、[プリンターのプロパティ] - [共有] タブを選択します。
3. [このプリンターを共有する] を選択して、[共有名] を入力します。

追加ドライバーをインストールする（Windowsのみ）

プリントサーバーのコンピュータとクライアントコンピュータが異なるバージョンのWindowsで動作している場合、それぞれのバージョンのプリンタードライバー（通信ドライバー）をプリントサーバーにインストールしておくことをお勧めします。

1. プリントサーバーのコンピュータで [コントロールパネル] - [デバイスとプリンター] の順に選択します。
2. 共有したいプリンターアイコン（プリントキュー）を右クリックして、[プリンターのプロパティ] - [共有] タブを選択します。
3. [追加ドライバー] をクリックします。
4. クライアントコンピュータのWindowsバージョン（プロセッサタイプ）を選択して、OKをクリックします。
5. プリンタードライバー（通信ドライバー）の情報ファイル (*.inf) を指定してドライバーをインストールします。

関連情報

➡ [「共有プリンターを使う - Windows」 27ページ](#)

共有プリンターを使う - Windows

プリンターの管理者は、クライアントコンピューターへのプリンター追加手順としてプリントサーバーに設定したコンピューター名をクライアントに連絡してください。追加ドライバーが設定されていない環境では、[デバイスとプリンター] からプリンターを追加する手順を案内してください。

以下は、プリントサーバーに追加ドライバーが設定されている場合の手順です。

1. プrintサーバーのコンピューター名を [エクスプローラー] で開きます。
2. 利用したいプリンターをダブルクリックします。

関連情報

- ➡ [「プリンターを共有する \(Windowsのみ\)」 26ページ](#)
- ➡ [「追加ドライバーをインストールする \(Windowsのみ\)」 26ページ](#)

ピアツーピア型接続での印刷設定

ピアツーピア型接続 (直接印刷) の場合、プリンターとクライアントコンピューターは一対一の関係になります。プリンターを使用するそれぞれのコンピューターにプリンタードライバー (通信ドライバー) をインストールします。

関連情報

- ➡ [「プリンタードライバー \(通信ドライバー\) を設定する」 27ページ](#)

プリンタードライバー (通信ドライバー) を設定する

小規模なネットワークの場合、それぞれのクライアントコンピューターにプリンタードライバー (通信ドライバー) とソフトウェアRIPをインストールすることをお勧めします。

インストールの方法は、お使いのプリンターの [セットアップガイド] をご覧ください。

メールサーバーを設定する

Web Configを使ってメールサーバーを設定します。

設定の前に以下を確認してください。

- プリンターがメールサーバーにアクセスできるネットワークに接続されているか
- プリンターと同じメールサーバーを使用するコンピューターのメール設定情報

参考 インターネット上のメールサーバーを利用する場合は、サービスを提供しているプロバイダーやウェブサイトから設定情報を確認してください。

1. Web Configで [ネットワーク] タブ - [メールサーバー] - [基本] を選択します。
2. 各項目を設定します。

3. 【設定】を選択します。

設定結果が表示されます。

メールサーバー設定項目

項目	設定値と説明	
認証方式	プリンターがメールサーバーにアクセスする際の認証方式を指定します。	
	認証しない	メールサーバーが認証を必要としない場合に設定します。
	SMTP認証	メール送信時にSMTPサーバー（メール送信サーバー）で認証をします。メールサーバーがSMTP認証に対応している必要があります。
	POP before SMTP	メール送信する前にPOP3サーバー（メール受信サーバー）で認証をします。選択した場合はPOP3サーバーの設定をしてください。
認証用アカウント	<p>【認証方式】に【SMTP認証】または【POP before SMTP】を選択した場合、認証用のアカウント名を入力します。入力できる文字は、ASCII (0x20-0x7E) の255文字以内です。</p> <p>【SMTP認証】を選択した場合、SMTPサーバーの認証用アカウントを入力してください。【POP before SMTP】を選択した場合、POP3サーバーの認証用アカウントを入力してください。</p>	
認証用パスワード	<p>【認証方式】に【SMTP認証】または【POP before SMTP】を選択した場合、認証用のパスワードを入力します。入力できる文字はASCII (0x20-0x7E) の20文字以内です。</p> <p>【SMTP認証】を選択した場合、SMTPサーバーの認証アカウントのパスワードを入力してください。【POP before SMTP】を選択した場合、POP3サーバーの認証アカウントのパスワードを入力してください。</p>	
送信元アドレス	システム管理者のアドレスなど送信元のメールアドレスを入力します。認証にも使用されるため、お使いのメールサーバーに登録されていて実際に送信できるアドレスを入力してください。入力できる文字は、: () < > [] ; ¥ を除くASCII (0x20-0x7E) で表せる255文字以内です。ただし、ピリオド (.) は先頭文字にできません。	
SMTPサーバーアドレス	A～Z a～z 0～9 . - を使用し、255文字以内で入力します。IPv4形式とFQDN形式での入力が可能です。	
SMTPサーバー ポート番号	1～65535までの範囲で、半角数字で入力します。	
セキュア接続	メールサーバーとの通信の暗号化方式を選択します。	
	なし	【認証方式】で【POP before SMTP】を選択した場合は暗号化しません。
	SSL/TLS	【認証方式】で【認証しない】または【SMTP認証】を選択したときに選択できます。通信の開始から暗号化します。
	STARTTLS	【認証方式】で【認証しない】または【SMTP認証】を選択したときに選択できます。通信の開始は暗号化せず、受信環境によってその後の通信を暗号化するかが変わります。

項目	設定値と説明
証明書の検証	有効にするとメールサーバーの証明書の正当性をチェックします。[有効] にすることをお勧めします。設定するには、相手サーバー検証用CA証明書をプリンターにインポートする必要があります。
POP3サーバーアドレス	〔認証方式〕に〔POP before SMTP〕を選択した場合、POP3サーバーアドレスを入力します。入力できる文字は、A～Z a～z 0～9 . - で、255文字以内です。IPv4形式とFQDN形式での入力が可能です。
POP3サーバー ポート番号	〔認証方式〕で〔POP before SMTP〕を選択した場合にポート番号を指定します。入力できる文字は、1～65535の範囲で、半角数字で入力します。

メールサーバーとの接続を確認する

メールサーバーとの接続確認ができます。

1. Web Configで〔ネットワーク〕タブ - 〔メールサーバー〕 - 〔接続確認〕を選択します。
2. 〔確認開始〕を選択します。

メールサーバーとの接続診断が開始されます。接続テストが終了すると結果が表示されます。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)
- ➡ [「メールサーバー接続確認結果」 29ページ](#)

メールサーバー接続確認結果

メッセージ	原因
接続に成功しました。	サーバーとの接続に成功した場合に表示されます。
SMTPサーバーとの通信でエラーが発生しました。以下を確認してください。・ネットワーク設定	以下のような場合に通信エラーが表示されます。 <ul style="list-style-type: none"> • プリンターがネットワークに接続されていない • SMTPサーバーがダウンしている • 通信中にネットワークが切断された • 異常なデータを受信した
POP3サーバーとの通信でエラーが発生しました。以下を確認してください。・ネットワーク設定	以下のような場合に通信エラーが表示されます。 <ul style="list-style-type: none"> • プリンターがネットワークに接続されていない • POP3サーバーがダウンしている • 通信中にネットワークが切断された • 異常なデータを受信した

機能設定編

メッセージ	原因
SMTPサーバーとの接続に問題があります。以下を確認してください。・SMTPサーバーアドレス・DNSサーバー	以下のような場合に通信エラーが表示されます。 <ul style="list-style-type: none"> • DNSサーバーとの接続に失敗した • SMTPサーバーアドレスの名前解決に失敗した
POP3サーバーとの接続に問題があります。以下を確認してください。・POP3サーバーアドレス・DNSサーバー	以下のような場合に通信エラーが表示されます。 <ul style="list-style-type: none"> • DNSサーバーとの接続に失敗した • POP3サーバーアドレスの名前解決に失敗した
SMTPサーバーの認証に失敗しました。以下を確認してください。・認証方式・認証用アカウント・認証用パスワード	SMTPサーバーでの認証処理に失敗したときに表示されます。
POP3サーバーの認証に失敗しました。以下を確認してください。・認証方式・認証用アカウント・認証用パスワード	POP3サーバーでの認証処理に失敗したときに表示されます。
サポートしていない通信方式です。以下を確認してください。・SMTPサーバーアドレス・SMTPサーバーポート番号	プリンターがサポートしていないプロトコルで通信しようとした場合に表示されます。
SMTPサーバーとの接続に失敗しました。セキュア接続をなしに変更してください。	サーバーとクライアントでSMTPセキュア接続の設定が合っていない、またはサーバーがSMTPセキュア接続（SSL接続）をサポートしていない場合に表示されます。
SMTPサーバーとの接続に失敗しました。セキュア接続をSSL/TLSに変更してください。	サーバーとクライアントでSMTPセキュア接続の設定が合っていない、またはサーバーがSMTPセキュア接続にSSL/TLS接続することを要求してきている場合に表示されます。
SMTPサーバーとの接続に失敗しました。セキュア接続をSTARTTLSに変更してください。	サーバーとクライアントでSMTPセキュア接続の設定が合っていない、またはサーバーがSMTPセキュア接続にSTARTTLS接続することを要求してきている場合に表示されます。
サーバーの安全性が確認できませんでした。以下を確認してください。・日付/時刻	プリンターの日時設定が正しくない、またはサーバーに対応するルート証明書は保有しているが、期限切れの場合に表示されます。
サーバーの安全性が確認できませんでした。以下を確認してください。・相手サーバー検証用CA証明書	サーバーに対応するルート証明書をプリンターが保有していない、または相手サーバー検証用CA証明書がインポートされていない場合に表示されます。
サーバーの安全性が確認できませんでした。	サーバーから取得した証明書が壊れている場合などに表示されます。
SMTPサーバーの認証に失敗しました。認証方式をSMTP認証に変更してください。	サーバーとクライアントで認証方式が一致していない場合に表示されます。サーバーはSMTP認証をサポートしているのに、プリンターはSMTP認証を実行していません。
SMTPサーバーの認証に失敗しました。認証方式をPOP before SMTPに変更してください。	サーバーとクライアントで認証方式が一致していない場合に表示されます。サーバーはSMTP認証をしていないのに、プリンターはSMTP認証を実行しようとしています。
送信元アドレスが正しくありません。お使いのメールサービスで取得したアドレスに変更してください。	送信元アドレスの指定が間違っていた場合に表示されます。

メッセージ	原因
プリンターが処理動作中のためアクセスできません。	プリンターが動作中で接続設定ができなかったときに表示されます。

関連情報

➡ [「メールサーバーとの接続を確認する」 29ページ](#)

システムの詳細を設定する

操作パネルの動作を設定する

プリンターの操作パネルに関する設定をします。以下の設定ができます。

1. Web Configで【デバイス管理】タブ - 【パネル】を選択します。
2. 必要に応じて以下の項目を設定します。
 - 表示言語
操作パネルの表示言語を選択します。
 - パネルロック
【オン】にすると、操作パネルでシステム管理者権限が必要な操作をするときに管理者パスワードが必要になります。管理者パスワードを設定していないとパネルロックは無効になります。
 - 無操作タイマー設定
【オン】にすると、システム管理者としてログオンしている場合、設定した時間内に操作パネルの操作がなかったときに、自動でログオフして初期画面に移行します。
10秒～240分まで1秒単位で設定できます。

参考 プリンターの操作パネルからも設定できます。

- 表示言語：Menu - 【本体設定】 - 【基本設定】 - 【言語選択/Language】
- パネルロック：Menu - 【本体設定】 - 【管理者用設定】 - 【セキュリティー設定】 - 【管理者設定】 - 【管理者ロック】
- 無操作タイマー設定：Menu - 【本体設定】 - 【基本設定】 - 【無操作タイマー設定】（オン/オフのみ設定できます。）

3. 【設定】をクリックします。

関連情報

➡ [「Web Configの起動」 23ページ](#)

➡ [「Web Configで管理者としてログオンする」 35ページ](#)

無操作時の省電力設定をする

プリンターの操作パネルが一定時間操作されなかった場合に、節電モードへ移行する時間と自動で電源を切る時間を設定できます。使用する環境に合わせて時間を設定してください。

1. Web Configで「デバイス管理」タブ - 「省電力」を選択します。
2. 「スリープ移行時間設定」に操作パネル無操作時に節電モードへ移行する時間を設定します。



プリンターの操作パネルからも設定できます。

Menu - 「本体設定」 - 「基本設定」 - 「スリープ移行時間設定」

3. 「自動電源オフ時間」に電源が切れるまでの時間を選択します。



プリンターの操作パネルからも設定できます。

Menu - 「本体設定」 - 「基本設定」 - 「自動電源オフ」

4. 「設定」をクリックします。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)

タイムサーバーと日付/時刻を同期する

タイムサーバー（NTPサーバー）と連携すると、プリンターとネットワーク上のコンピューターとの時刻を同期できます。タイムサーバーは、組織内で運用している場合やインターネット上に公開している場合があります。CA証明書を使っている場合、連携すると時間に関するトラブルを防ぐことができます。

1. Web Configで「デバイス管理」タブ - 「日付/時刻」 - 「タイムサーバー」を選択します。
2. 「タイムサーバーを使用する」を「使用する」にします。
3. 「タイムサーバーアドレス」にタイムサーバーのアドレスを入力します。
IPv4、IPv6アドレスまたはFQDNが使用できます。252文字以内で入力します。指定しない場合は空白にします。
4. 「更新間隔（分）」を入力します。
1分単位で10,080分まで設定できます。
5. 「設定」をクリックします。



「タイムサーバーステータス」でサーバーとの接続状態を確認できます。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)

本体のセキュリティ編

この章では、デバイス本体のセキュリティ設定について説明しています。

本体のセキュリティ機能の紹介

本機に管理者以外のユーザーに使用制限をかけられる機能があります。
管理者パスワードでログオンをすると、全ての機能を使用できます。 管理者パスワードはあらかじめ設定されています。

！重要 使用開始後は管理者パスワードを初期パスワードのまま使用し続けず、任意のパスワードに変更することをお勧めします。
変更方法
[「管理者パスワードの変更」 33ページ](#)

Web Configでは、管理者パスワードでログオンすると全ての機能を使用できます。
[「管理者としてプリンターにログオンする」 35ページ](#)

管理者パスワードの変更

本機はあらかじめ管理者パスワードの初期パスワードが設定されています。初期パスワードはラベルに記載されています。詳細はプリンターのマニュアルをご覧ください。

使用開始後は初期パスワードのまま使用し続けず、任意のパスワードに変更することをお勧めします。

変更はWeb Config、操作パネル、ソフトウェア（Epson Device Admin）からできます。Epson Device Adminの操作方法についてはEpson Device Adminのマニュアルをご覧ください。

Epson Device Adminの起動方法

[「Epson Device Admin」 49ページ](#)

Web Configから管理者パスワードを変更する

Web Configを使って管理者パスワードを変更します。

1. Web Configで【本体セキュリティ】タブ - 【管理者パスワード変更】を選択します。
2. 【現在のパスワード】に現在のパスワードを入力します。
3. 【新しいパスワード】と【新しいパスワードの確認】に新しいパスワードを入力します。必要に応じてユーザー名を入力します。

4. **【設定】** を選択します。

参考

- ロックされている項目を設定、変更するには **【ログオン】** をクリックして管理者パスワードを入力します。
- 管理者パスワードを初期パスワードに戻すには、**【管理者パスワード変更】** 画面で **【購入時の設定に戻す】** をクリックします。

関連情報

➡ [「Web Configの起動」 23ページ](#)

➡ [「Web Configで管理者としてログオンする」 35ページ](#)

外部インターフェイスを無効にする

プリンターにデバイスを接続するインターフェイスを無効にできます。ネットワーク経由以外の印刷を制限する場合に設定します。

参考

プリンターの操作パネルからも設定できます。

- コンピューターのUSB接続：Menu - **【本体設定】** - **【プリンター設定】** - **【コンピューターのUSB接続】**

1. Web Configで **【本体セキュリティ】** タブ - **【外部インターフェイス】** を選択します。

2. 制限したい機能で **【無効】** を選択します。

制限を解除する場合は **【有効】** を選択してください。

- コンピューターのUSB接続
コンピューターからのUSB接続を制限できます。制限する場合は **【無効】** に設定します。

3. **【設定】** をクリックします。

4. 無効にしたポートが使用できなくなっているか確認します。

- コンピューターのUSB接続
確認するコンピューターにドライバーがインストールされている場合：
プリンターとコンピューターをUSBケーブルで接続し、印刷ができないことを確認します。
確認するコンピューターにドライバーがインストールされていない場合：
Windows)
デバイスマネージャーを表示したままプリンターをコンピューターにUSBケーブルで接続し、デバイスマネージャーの表示内容が変化しないことを確認します。
Mac OS)
プリンターをコンピューターにUSBケーブルで接続し、**【プリンターとスキャナー】** からプリンターを追加しようとしてもプリンターがリストに表示されないことを確認します。

関連情報

➡ [「Web Configの起動」 23ページ](#)

➡ [「Web Configで管理者としてログオンする」 35ページ](#)

運用・管理編

この章では、デバイスの日常的な運用や管理に関わる事項を説明しています。

管理者としてプリンターにログオンする

プリンターに管理者パスワードを設定している場合、Web Configでロックされている項目を操作するには管理者としてプリンターにログオンする必要があります。

Web Configで管理者としてログオンする

管理者としてWeb Configにログオンすると、管理者ロックされている項目を操作できます。

1. ブラウザーにプリンターのIPアドレスを入力してWeb Configを起動します。
2. [ログオン] をクリックします。
3. [ユーザー名] と [現在のパスワード] にユーザー名と管理者パスワードを入力します。
4. [確認] をクリックします。

認証されるとロックされている項目が表示され、[ログオフ] が表示されます。

ログオフするには [ログオフ] をクリックします。

参考 [デバイス管理] タブ - [パネル] - [無操作タイマー設定] を [オン] にすると、一定時間操作パネルを操作しない場合に自動でログオフします。

関連情報


➔ [\[Web Configの起動\] 23ページ](#)

プリンターの情報を確認する

操作パネルから情報を確認する

操作パネルから以下の情報の確認や印刷ができます。

- 消耗品
Menu - [消耗品情報]
インクやメンテナンスボックスの情報を確認できます。

- 本体ステータスシート
Menu - [情報確認/印刷] - [本体ステータスシートの印刷]
プリンター情報や消耗品情報などのステータスシートを印刷できます。
- ネットワーク情報
Menu - [本体設定] - [ネットワーク設定] - [ネットワーク情報]
Menu - [情報確認/印刷] - [ネットワーク]
ネットワーク接続状態などの確認とステータスシートの印刷ができます。
- ネットワーク接続状況
ホーム画面の  - [ルーター]
接続状況が確認できます。

Web Configから情報を確認する

Web Configの [情報確認] から、以下の情報を確認できます。

- 製品情報
言語、ステータス、製造番号、MACアドレスなどが確認できます。
- ネットワーク情報
ネットワーク接続状態、IPアドレス、DNSなどネットワークに関する情報が確認できます。
- ハードウェア情報
プリンターの各機能のステータスを確認できます。
- パネルのスナップショット
デバイスの操作パネルに表示されている画面イメージのスナップショットを表示します。

イベント発生時にメール通知を受け取る

メール通知の概要

印刷の停止やプリンターエラーなど、プリンターにイベントが発生したときに、指定したアドレスにメールで通知する機能です。

宛先は5つまで登録でき、それぞれに受け取りたい通知を設定できます。

この機能を使うには、設定前にメールサーバーの設定が必要です。

関連情報

➔ [「メールサーバーを設定する」27ページ](#)

メール通知を設定する

Web Configを使ってメール通知の設定をします。機種によって設定できる項目は異なります。

1. Web Configで [デバイス管理] タブ - [メール通知] を選択します。

2. メール通知の件名を設定します。

2つのプルダウンメニューで件名に表示する内容を選択します。

- 選択された内容が「件名」の横に表示されます。
- 左右に同じ内容は設定できません。
- 「ロケーション」の文字数が多い場合は、32バイト以降の文字が省略されます。

3. 通知メールを送信するメールアドレスを入力します。

A-Z a-z 0-9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @, を使用し、255文字以内で入力します。

4. メール通知の言語を選択します。

5. 通知を受け取りたいイベントの行で、通知する宛先番号と重なるチェックボックスにチェックを付けます。

「通知設定」の番号は「宛先設定」の宛先の番号に対応しています。

設定例：

用紙がなくなった場合の通知を「宛先設定」の1に設定したアドレスに送信したいときは、「用紙なし」の行にある「1」の列のチェックボックスにチェックを付けます。

6. 「設定」をクリックします。

何らかのイベントを作って、メール通知が送信されることを確認してください。

例：用紙をセットしていない給紙方法を指定して印刷

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)

ファームウェアのアップデート

新しいファームウェアがある場合、プリンターのファームウェアをアップデートすると、機能が向上したり、不具合が解消されたりします。

プリンターをインターネットに接続しないでファームウェアをアップデートする

コンピュータでエプソンのウェブサイトから機種用のファームウェアをダウンロードし、USBケーブルで接続してアップデートすることもできます。ネットワーク経由でアップアップデートができない場合に、この方法をお使いください。

1. エプソンのウェブサイトアクセスして、ファームウェアをダウンロードします。

www.epson.jp/support/

2. ファームウェアをダウンロードしたコンピュータと、プリンターをUSBケーブルで接続します。

3. ダウンロードしたexeファイルをダブルクリックします。

Epson Firmware Updaterが起動します。

4. この後は、画面の指示に従って操作します。

設定のバックアップ

Web Configで設定した設定値をファイルにエクスポートできます。設定値のバックアップ、プリンターの置き換え時などに利用できます。

バイナリーファイルでエクスポートされるので編集できません。

設定をエクスポートする

プリンターの設定値をエクスポートします。

1. Web Configで【デバイス管理】タブ - 【設定のエクスポート/インポート】 - 【エクスポート】を選択します。

2. エクスポートしたい設定を選択します。

チェックが付いた項目の設定値がエクスポートされます。親のカテゴリーを選択すると、子のカテゴリーが同時に選択されます。ただし、IPアドレスなどネットワーク内に同じ設定値が複数あるとエラーになる項目は選択できないようになっています。

3. エクスポートファイルを暗号化するために任意のパスワードを入力します。

ここで指定したパスワードはインポートするときに必要になります。パスワードを指定しない場合は空白にします。

4. 【エクスポート】をクリックします。

！重要 デバイス名やIPv6アドレスなどのネットワーク情報を含めてエクスポートしたいときは【本体ごとの個別設定を選択可能にする】にチェックを付けて、項目を選択してください。なお、この項目をチェックしてから選択した設定値は、プリンターの置き換え時のみにお使いください。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)

設定をインポートする

Web Configの設定ファイルをプリンターにインポートします。

！重要 プリンター名やIPアドレスなどの個別情報を含む設定値をインポートするときは、同一のネットワーク内に同じIPアドレスを持つプリンターが存在しないことを確認してください。IPアドレスが重複する場合は、インポートしても内容は反映されません。

1. Web Configで［デバイス管理］タブ - ［設定のエクスポート/インポート］ - ［インポート］を選択します。
2. エクスポートされたファイルを選択し、暗号化パスワードを入力します。
3. ［次へ］をクリックします。
4. インポートする設定を選択して［次へ］をクリックします。
5. ［設定］をクリックします。

設定がプリンターに反映されます。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)

トラブルを解決する

トラブルを解決するための糸口

- エラーメッセージの確認
何らかのトラブルが発生した場合、始めにプリンターの操作パネルやお使いのアプリケーションなどにメッセージが出ていないか確認してください。通知メールを送信するように設定してあると、イベントが発生した場合に素早く状態を把握できます。
- 通信状態の確認
サーバーやクライアントコンピューターの通信状態をpingやipconfigなどのコマンドを使って確認します。
- 接続テスト
メールサーバーとの接続は、プリンターから接続テストをすることで確認できます。また、クライアントコンピューターからサーバーへの接続テストをして通信状態を確認します。
- 設定の初期化
設定や通信状態に問題がない場合、プリンターのネットワーク設定を無効にしたり、初期状態に戻して設定をやり直したりすると、トラブルが解消する場合があります。

プリンターの状態を確認する

トラブルの原因を特定するために、プリンターやネットワークの状況を確認します。

エラーメッセージを確認する

メール通知からエラー表示を確認する

メール通知を設定している場合、プリンターからエラーに関するメールが届いていないか確認します。対処方法が記載されている場合はそれに従ってください。

関連情報

➡ [「イベント発生時にメール通知を受け取る」 36ページ](#)

プリンター画面のメッセージを確認する

プリンターの画面にメッセージが表示されたら、画面の指示または以下の対処方法に従ってトラブルを解決してください。

トラブルを解決する

メッセージ	原因・対処方法
プリンターエラーが発生しました。電源を入れ直してください。詳しくはマニュアルをご覧ください。 エラーコード：XXXXXX	<ul style="list-style-type: none"> • 原因： プリンターの内部に異物が混入したか、プリンターエラーが発生しました。 • 対処方法： プリンター内部に用紙や保護材が入っていたら取り除いてください。電源を入れ直しても同じメッセージが表示される場合は、エラーコードを控えてから、エプソンの修理窓口にご連絡ください。
アドレスとサブネットマスクの組み合わせが有効ではありません。詳しくはマニュアルをご覧ください。	<ul style="list-style-type: none"> • 原因： 設定したIPアドレスの組み合わせが不正です。 • 対処方法： IPアドレス、またはデフォルトゲートウェイに正しい値を入力してください。
このサービスを利用するには、ルート証明書のアップデートが必要です。	<ul style="list-style-type: none"> • 原因： クラウドサービスに使用するルート証明書の期限が切れています。 • 対処方法： Web Configを起動して、以下からルート証明書を更新してください。 [ネットワークセキュリティ] - [ルート証明書更新]
Recovery Mode	<ul style="list-style-type: none"> • 原因： ファームウェアのアップデートに失敗し、通常モードに復帰できませんでした。 • 対処方法： ファームウェアのアップデートに失敗したため、リカバリーモードで起動しました。以下の手順でもう一度ファームウェアをアップデートしてください。 1. コンピューターとプリンターをUSB接続します（リカバリーモード中のアップデートは、ネットワーク接続ではできません）。 2. エプソンのウェブサイトから最新のファームウェアをダウンロードしてアップデートを開始します。 詳しくはダウンロードページの「アップデート方法」をご覧ください。

遠隔地にあるプリンターのパネル表示を確認する

Web Configを使って遠隔地にあるプリンターのパネル表示を確認できます。

1. 確認したいプリンターのWeb Configを起動します。

メール通知を受け取っている場合は、メールに記載されているURLからWeb Configを起動できます。

2. [情報確認] タブ - [パネルのスナップショット] の順に選択します。

プリンターの現在のパネルがWeb Configに表示されます。

更新する場合は、[最新の状態へ更新] をクリックします。

通信状態を確認する

プリンターやコンピューターのネットワーク接続、プリンターとコンピューター間の通信が正常かどうか確認し、トラブルの解決につなげます。

サーバーやネットワーク機器のログの確認

ネットワーク接続でのトラブル発生時は、メールサーバーやネットワーク機器のログ情報を確認したり、コマンドを使ってステータスを確認したりすると原因を特定できることがあります。

ネットワークステータスシートを印刷する

ネットワークステータスシートを印刷すると、プリンターのネットワーク情報や状態を確認できます。

1. 印刷用紙をセットします。
2. ホーム画面でMenuを選択します。
3. [本体設定] - [ネットワーク設定] - [ネットワーク情報] を選択します。
4. [ステータスシート印刷] を選択します。
5. メッセージを確認して、ネットワークステータスシートを印刷します。
6. 画面を閉じます。
一定時間経過すると自動で画面が閉じます。

デバイスとコンピューターの通信を確認する

コンピューターとの通信をPingで確認する - Windows

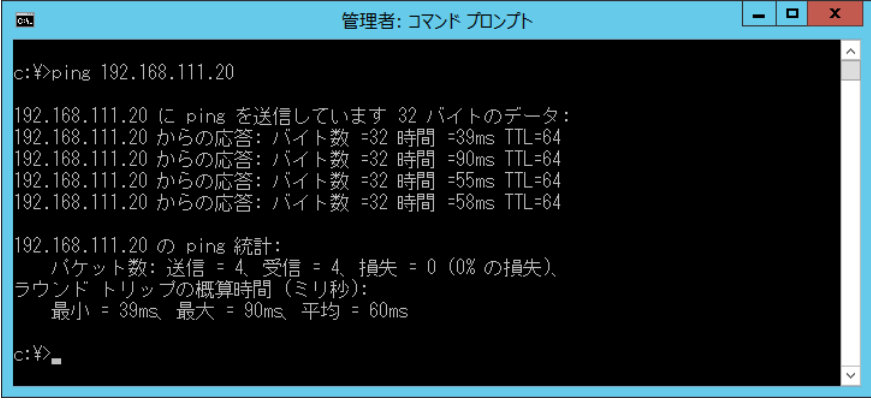
Pingを使ってコンピューターとプリンターが通信できているか確認します。以下の手順で通信を確認してください。

1. 通信を確認したいプリンターのIPアドレスを確認します。
操作パネルのネットワーク情報画面またはネットワークステータスシートの [IP Address] の項目で確認してください。
2. コンピューターのコマンドプロンプトを表示します。
アプリ画面を表示して、[コマンドプロンプト] を選択します。
3. 「ping xxx.xxx.xxx.xxx」と入力して、Enterキーを押します。
xxx.xxx.xxx.xxxにはプリンターのIPアドレスを入れてください。

トラブルを解決する

4. 通信状況を確認します。

プリンターとコンピューターが通信できていると以下のように表示されます。



```
管理者: コマンド プロンプト

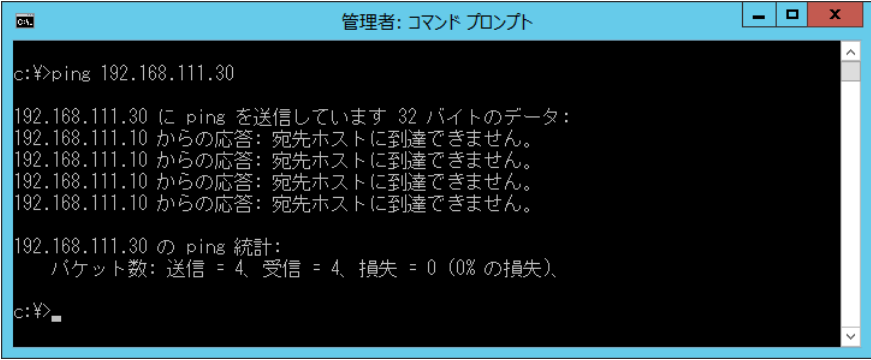
c:\>ping 192.168.111.20

192.168.111.20 に ping を送信しています 32 バイトのデータ:
192.168.111.20 からの応答: バイト数 =32 時間 =39ms TTL=64
192.168.111.20 からの応答: バイト数 =32 時間 =90ms TTL=64
192.168.111.20 からの応答: バイト数 =32 時間 =55ms TTL=64
192.168.111.20 からの応答: バイト数 =32 時間 =58ms TTL=64

192.168.111.20 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 39ms、最大 = 90ms、平均 = 60ms

c:\>
```

プリンターとコンピューターが通信できていないと以下のように表示されます。



```
管理者: コマンド プロンプト

c:\>ping 192.168.111.30

192.168.111.30 に ping を送信しています 32 バイトのデータ:
192.168.111.10 からの応答: 宛先ホストに到達できません。
192.168.111.10 からの応答: 宛先ホストに到達できません。
192.168.111.10 からの応答: 宛先ホストに到達できません。
192.168.111.10 からの応答: 宛先ホストに到達できません。

192.168.111.30 の ping 統計:
    パケット数: 送信 = 4、受信 = 0、損失 = 100% (100% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 0ms、最大 = 0ms、平均 = 0ms

c:\>
```

コンピューターとの通信をPingで確認する - Mac OS

Pingを使ってコンピューターとプリンターが通信できているか確認します。以下の手順で通信を確認してください。

1. 通信を確認したいプリンターのIPアドレスを確認します。

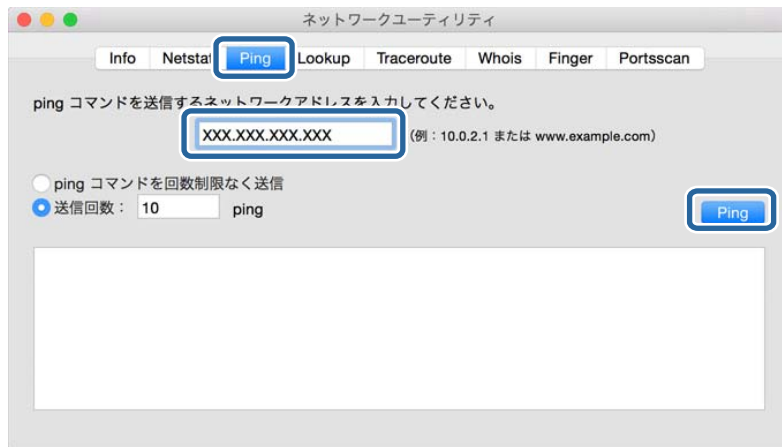
操作パネルのネットワーク情報画面またはネットワークステータスシートの「IP Address」の項目で確認してください。

2. ネットワークユーティリティを起動します。

[Spotlight] で「ネットワークユーティリティ」と入力して検索してください。

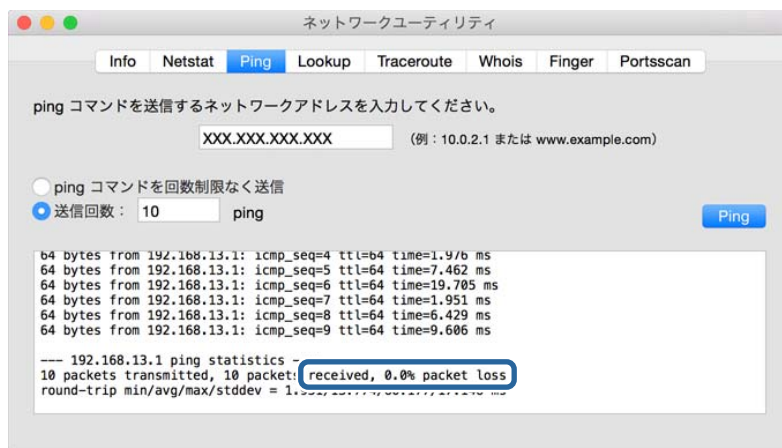
トラブルを解決する

3. [Ping] タブをクリックし、手順1で確認したIPアドレスを入力して、[Ping] をクリックします。

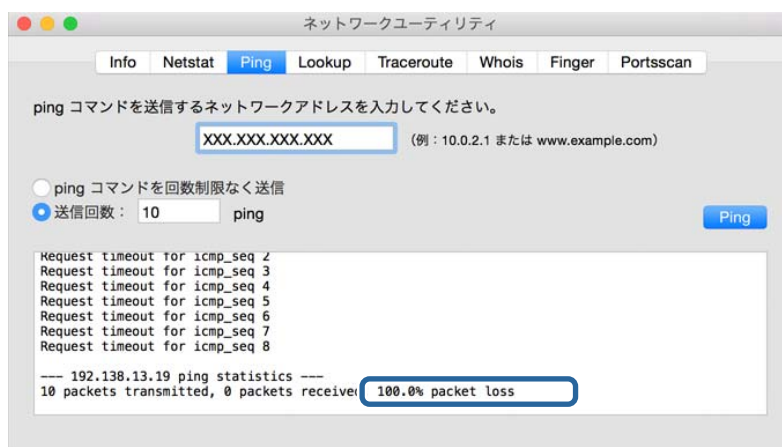


4. 通信状況を確認します。

プリンターとコンピューターが通信できていると以下のように表示されます。



プリンターとコンピューターが通信できていないと以下のように表示されます。



コンピューターのネットワークを確認する - Windows

Windowsのコマンドプロンプトからコマンドを使って、コンピューターの接続情報やプリンターとの接続経路などを確認します。トラブル解決につながります。

- ipconfigコマンド

コンピューターが現在使用しているネットワークインターフェースの接続状況を表示します。

実際に通信している情報と設定情報の差がないかを比較して、正常に接続されているかを確認できます。同じネットワークに複数のDHCPサーバーがあるような場合、コンピューターに割り当てられている実際のアドレスや、参照しているDNSサーバーなどを知ることができます。

- 書式 : ipconfig /all
- 例 :

```

c:\¥>ipconfig /all

Windows IP 構成

ホスト名 . . . . . : WIN2012R2
プライマリ DNS サフィックス . . . . . : pubs.net
ノード タイプ . . . . . : ハイブリッド
IP ルーティング有効 . . . . . : いいえ
WINS プロキシ有効 . . . . . : いいえ
DNS サフィックス検索一覧 . . . . . : pubs.net

イーサネット アダプター イーサネット :

    接続固有の DNS サフィックス . . . . . :
    説明 . . . . . : Gigabit Network Connection
    物理アドレス . . . . . : xx-xx-xx-xx-xx-xx
    DHCP 有効 . . . . . : いいえ
    自動構成有効 . . . . . : はい
    リンクローカル IPv6 アドレス . . . . . : fe80::38fb:7546:18a8:d20e%13(優先)
    IPv4 アドレス . . . . . : 192.168.111.10(優先)
    サブネット マスク . . . . . : 255.255.255.0
    デフォルト ゲートウェイ . . . . . : 192.168.111.1
    DHCPv6 IAID . . . . . : 283142549
    DHCPv6 クライアント DUID . . . . . : 00-01-00-01-21-0A-D4-46-E0-69-95-3C-91-49
    DNS サーバー . . . . . : 192.168.111.2
    NetBIOS over TCP/IP . . . . . : 有効

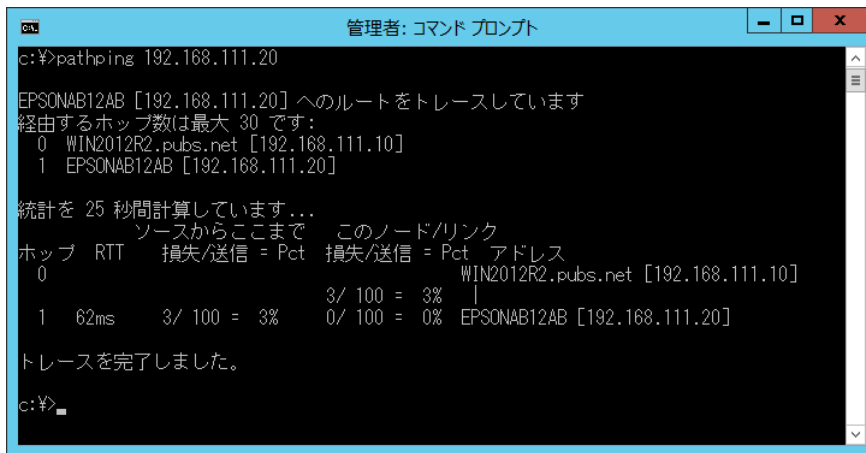
Tunnel adapter isatap.{12345678-ABCD-EFGH-IJKL-MNOPQRSTUVWXYZ}:

    メディアの状態 . . . . . : メディアは接続されていません
    接続固有の DNS サフィックス . . . . . :
    説明 . . . . . : Microsoft ISATAP Adapter #2
    物理アドレス . . . . . : 00-00-00-00-00-00-E0
    DHCP 有効 . . . . . : いいえ
    自動構成有効 . . . . . : はい

c:\¥>
  
```

トラブルを解決する

- pathpingコマンド
宛先ホストまでに通過するルーターのリストや通信のルーティングを確認できます。
- 書式：pathping xxx.xxx.xxx.xxx
- 例：pathping 192.0.2.222



```
c:\>pathping 192.168.111.20

EPSONAB12AB [192.168.111.20] へのルートをトレースしています
経由するホップ数は最大 30 です:
  0  WIN2012R2.pubs.net [192.168.111.10]
  1  EPSONAB12AB [192.168.111.20]

統計を 25 秒間計算しています...
      ソースからここまで      このノード/リンク
ホップ  RTT      損失/送信 = Pct  損失/送信 = Pct  アドレス
  0                                WIN2012R2.pubs.net [192.168.111.10]
  1   62ms      3/ 100 = 3%      0/ 100 = 0%  EPSONAB12AB [192.168.111.20]

トレースを完了しました。

c:\>
```

接続テストをする

プリンターやプリンターと同じセグメントに接続されているコンピューターから、サーバーやフォルダーとの接続が正常かを確認し、トラブルの解決につなげます。

メールサーバー

プリンターとメールサーバーの接続をプリンターのテスト機能で確認できます。

関連情報

➡ [「メールサーバーとの接続を確認する」29ページ](#)

DNSサーバー

コンピューターで参照しているDNSサーバーを確認します。プリンターと同じネットワークセグメント上にあるコンピューターのネットワークアダプターの状態を確認して、プリンターのDNS設定と同じかどうか確認してください。コンピューターのDNS設定は以下で確認できます。

- Windows：[コントロール パネル] - [ネットワークとインターネット] - [ネットワークと共有センター] - [アダプターの設定の変更]
複数のネットワークI/Fがある場合は、コマンドプロンプトでipconfig /allを入力して確認することもできます。
- Mac OS：[システム環境設定] - [ネットワーク] - [詳細] - [DNS] を選択します。

設定の初期化

操作パネルからネットワーク設定を初期の状態に戻す

ネットワーク設定全てを初期の状態に戻します。

1. ホーム画面でMenuを選択します。
2. [本体設定] - [管理者用設定] - [初期設定に戻す] - [ネットワーク設定] を選択します。
3. メッセージを確認して、[はい] を選択します。
4. 完了メッセージが表示されたら、画面を閉じます。
一定時間経過すると自動で画面が閉じます。

トラブル事例

Web Configにアクセスできない

プリンターのIPアドレスが設定されていない

プリンターに有効なIPアドレスが設定されていない可能性があります。プリンターの操作パネルでIPアドレスを設定してください。現在の設定は、ネットワークステータスシートやプリンターの操作パネルで確認できます。

WebブラウザがSSL/TLSの暗号強度に対応していない

SSL/TLSには暗号強度があります。Web Configは以下のメッセージ暗号化をサポートしているブラウザで起動できます。ブラウザの暗号強度の対応ビットをご確認ください。

- 80bit: AES256/AES128/3DES
- 112bit: AES256/AES128/3DES
- 128bit: AES256/AES128
- 192bit: AES256
- 256bit: AES256

CA署名証明書の有効期限が切れた

証明書の有効期限に問題がある場合、Web ConfigにSSL/TLS通信（https）で接続したときに「有効期限が切れている」と表示されます。証明書の有効期限内に表示されるときは、プリンターの時刻が正しく設定されているか確認してください。

証明書とプリンターのコモンネームが一致していない

コモンネームの不一致が起こると、Web ConfigにSSL/TLS通信（https）で接続したときに「セキュリティ証明書の名前が一致しません...」と表示されます。これは以下のIPアドレスが一致していないために発生します。

トラブルを解決する

- 自己署名証明書の作成や更新時、CSRの作成時にコモンネームで記述したIPアドレス
- Web Configの起動時にブラウザーに入力したIPアドレス

自己署名証明書の場合はプリンター名を変更してください。証明書が更新されて接続できるようになります。
CA署名証明書の場合は該当のプリンター用に証明書を取得し直してください。

ブラウザーにローカルアドレスのプロキシサーバー設定がされていない

プリンターでプロキシサーバーを使用する設定にしている場合、ブラウザーでローカルアドレスへの接続にプロキシサーバーを経由しないよう設定します。

- Windows :
[コントロールパネル] - [ネットワークとインターネット] - [インターネットオプション] - [接続] - [LANの設定] の [プロキシ サーバー] で、LAN (ローカルアドレス) にプロキシサーバーを使わない設定にします。
- Mac OS :
[システム環境設定] - [ネットワーク] - [詳細] - [プロキシ] で [プロキシ設定を使用しないホストとドメイン] にローカルアドレスを登録します。
記入例 :
ローカルアドレス192.168.1.XXX、サブネットマスク255.255.255.0 の場合 : 192.168.1.*
ローカルアドレス192.168.XXX.XXX、サブネットマスク255.255.0.0 の場合 : 192.168.*.*

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「IPアドレスを設定する」 19ページ](#)

管理者パスワードを忘れた

設定した管理者パスワードを忘れたときは、エプソンソリューションコールセンターにご相談ください。

付録

ネットワーク関連のソフトウェア

デバイスの設定、管理用のソフトウェアを紹介します。

Epson Device Admin


Epson Device Adminは、ネットワーク上のデバイスの管理を行う多機能なアプリケーションソフトです。以下のような機能があります。

- セグメントを越えて1台から2000台のプリンターやスキャナーの監視、管理
- 消耗品やステータスの詳細なレポート機能
- ファームアップデート機能
- デバイスのネットワークへの導入
- 複数デバイスへの同じ設定値の適用

Epson Device Adminはエプソンのウェブサイトからダウンロードしてください。詳細はEpson Device Adminのヘルプやマニュアルをご覧ください。

Epson Device Adminの起動（Windowsのみ）

[すべてのプログラム] - [EPSON] - [Epson Device Admin] から [Epson Device Admin] を選択します。

 **参考** Windowsファイアウォールの警告画面が表示された場合は、Epson Device Adminを例外のプログラムに登録してください。

EpsonNet Config（Windowsのみ）

EpsonNet Configはネットワーク上のデバイスの設定ができるアプリケーションソフトです。有線でネットワークに接続されていれば、IPアドレスのないデバイスでもIPアドレスの設定や接続形態の変更ができます。LCDパネルのないデバイスのネットワーク設定も容易に行えます。

詳細はEpsonNet Configのヘルプやマニュアルをご覧ください。



EpsonNet Configの起動 - Windows

[すべてのプログラム] - [EpsonNet] - [EpsonNet Config SE] から [EpsonNet Config] を選択します。

参考 Windowsファイアウォールの警告画面が表示された場合は、EpsonNet Configを例外のプログラムに登録してください。

EpsonNet Print (Windowsのみ)

TCP/IP上でネットワーク印刷するためのソフトウェアです。インストーラーからプリンタードライバー（通信ドライバー）などと共にインストールされます。ネットワーク印刷にはEpsonNet Printポートを作成します。

- スプーラー画面にプリンターのステータスが表示できます。
- DHCP機能によって変更されたIPアドレスを自動追従します。
- ルーターを越えた場所（別セグメント）のプリンターも使用できます。
- 印刷データの送信プロトコルが使い分けられます。
- IPv6アドレスには対応していません。

プリンターが使用するポート

プリンターは以下のポートを使用します。必要に応じてあらかじめネットワーク管理者にポート使用を許可してもらいます。

付録

送信元（クライアント）	用途	送信先（サーバー）	プロトコル	ポート番号
プリンター	メール送信（プリンター本体のメール通知機能利用時）	SMTPサーバー	SMTP（TCP）	25
			SMTP SSL/TLS（TCP）	465
			SMTP STARTTLS（TCP）	587
	POP before SMTP接続（プリンター本体のメール通知機能利用時）	POPサーバー	POP3（TCP）	110
	WSDの制御	クライアントコンピュータ	WSD（TCP）	5357
クライアントコンピュータ	ファイル送信（プリンター本体のFTP印刷利用時）	プリンター	FTP（TCP）	20
				21
	EpsonNet Configなどのアプリケーションソフト、プリンタードライバー（通信ドライバー）からのプリンター探索	プリンター	ENPC（UDP）	3289
	EpsonNet Configなどのアプリケーションソフト、エプソンのプリンタードライバー（通信ドライバー）からのプリンターMIB情報の取得と設定	プリンター	SNMP（UDP）	161
	LPRデータの転送	プリンター	LPR（TCP）	515
	RAWデータの転送	プリンター	RAW（Port9100）（TCP）	9100
	WSDのプリンター探索	プリンター	WS-Discovery（UDP）	3702
	Web Config	プリンター	HTTP（TCP）	80
			HTTPS（TCP）	443

エンタープライズセキュリティ設定編

この章では、高度なセキュリティ機能を説明しています。

セキュリティ設定と防止できる脅威

ネットワークにプリンターを接続すると、離れた場所からアクセスして使用できます。また、プリンターを共有してたくさんの人が使用でき、業務効率や利便性の向上に役立ちます。反面、不正アクセスや不正使用、データの改ざんなどのリスクも高くなります。インターネットにアクセスできる環境の場合はさらにリスクが高まります。

外部からのアクセスの保護を施していないプリンターは、本体に記憶している印刷履歴などをインターネットから読み取ることができてしまいます。

リスクを回避するため、エプソン製プリンターにはさまざまなセキュリティ技術を搭載しています。

お客様の情報環境での条件に合わせて、必要なセキュリティ設定をしてください。

機能名	どんな機能が	何を設定するのか	何を防止できるのか
パスワードの暗号化	プリンターに記録されている機密情報（全てのパスワード、証明書秘密鍵）を暗号化します。	パスワードの暗号化を設定して、暗号鍵をバックアップします。	暗号鍵はプリンター外部からアクセスできないため、暗号化した機密情報を守ることができます。
SSL/TLS通信	ブラウザー経由でのコンピューターとの通信やファームウェアアップデートなどプリンターからインターネット上のエプソンサーバーにアクセスするような場合に通信内容がSSL/TLS通信で暗号化されます。	CA署名証明書をCA局から取得し、プリンターにインポートします。	CA署名証明書によってプリンターの身分が明確になることで、なりすましや不正アクセスを防げます。また、通信内容がSSL/TLSによって保護されるため、設定情報や印刷データ内容の漏えいが防げます。
プロトコルの制御	プリンターやコンピューター間の通信で使用するプロトコルやサービスを制御して、機能を有効、無効にします。	機能に対応したプロトコルやサービスを個別に許可、禁止します。	不要な機能を使用できなくすることで、意図されない利用によるセキュリティリスクを軽減できます。
IPsec/IPフィルタリング	特定のクライアントからのデータや、特定の種類のデータだけを通過、遮断する設定ができます。IPsecはIP パケット単位で保護（暗号化および認証）するため、セキュアでないプロトコルも安全に通信できます。	基本ポリシー、個別ポリシーを作成し、プリンターにアクセスできるクライアントやデータの種類を設定します。	プリンターへの不正アクセス、通信データの傍受や改ざんを防止できます。
IEEE802.1X	有線LAN へ認証された利用者だけに接続を許可します。許可された利用者だけがプリンターを使用できるようにします。	RADIUS サーバー（認証サーバー）への認証設定をします。	不正なプリンターへのアクセスや使用を防止できます。

関連情報

- ➡ [「パスワードを暗号化する」 54ページ](#)
- ➡ [「プリンターとのSSL/TLS通信」 54ページ](#)
- ➡ [「利用するプロトコルを制御する」 60ページ](#)
- ➡ [「IPsec/IPフィルタリングで暗号化通信する」 64ページ](#)
- ➡ [「IEEE802.1X環境にプリンターを接続する」 75ページ](#)

セキュリティ機能の設定

IPsec/IPフィルタリングやIEEE802.1Xなどの設定は、改ざん、傍受などセキュリティのリスク低減のために、SSL/TLS通信でWeb Configにアクセスして設定することをお勧めします。

また、設定に使うコンピューターは、プリンターとLANケーブルで直結し、ブラウザでIPアドレスを入力してWeb Configを起動して設定できます。セキュリティ設定が完了してからプリンターをセキュアな環境へ接続できます。

パスワードを暗号化する

パスワード暗号化を使用すると、プリンターに保存されている機密情報（全てのパスワード、証明書の秘密鍵）を暗号化できます。

1. ブラウザーにプリンターのIPアドレスを入力してWeb Configを起動します。

プリンターと同じネットワークに接続されたコンピューターから、プリンターのIPアドレスを入力してください。IPアドレスは操作パネルの以下のメニュー項目から確認できます。

[Menu] - [本体設定] - [ネットワーク設定] - [ネットワーク情報] - [有線・無線接続状態]

2. 管理者としてログオンするために、管理者パスワードを入力します。

3. 以下の順に選択します。

[本体セキュリティ] タブ - [パスワード暗号化]



デバイスの操作パネルからも設定できます。

[Menu] - [本体設定] - [管理者用設定] - [セキュリティ設定] - [パスワード暗号化]

4. [オン] を選択すると、暗号化が有効になります。

5. [設定] をクリックします。

プリンターとのSSL/TLS通信

SSL/TLS (Secure Sockets Layer/Transport Layer Security) 通信でプリンターにサーバー証明書を設定して、コンピューターとの通信経路を暗号化できます。なりすましや不正アクセスを防ぎたいときに設定してください。

使用できる電子証明書

- CA署名証明書

認証機関（CA局）によって署名された証明書です。CA局に申請して取得します。この証明書はプリンターの実在性を証明し、SSL/TLS通信に使用されるため、データ通信の安全が確保できます。

SSL/TLS通信に使用する場合は、サーバー証明書として利用されます。

IPsec/IPフィルタリング、IEEE802.1Xに設定する場合は、クライアント証明書として利用されます。

- CA証明書

CA署名証明書のチェーン内の証明書で、中間CA証明書とも呼ばれます。相手サーバーまたはWeb Configにアクセスするブラウザが、プリンターの証明書パスを検証するために使用されます。

相手サーバー検証用のCA証明書は、プリンターからアクセスするサーバーの証明書パスを検証する場合に設定します。プリンターでは、SSL/TLS通信用のCA署名証明書の証明書パスを証明するために設定します。

プリンターのCA証明書は、CA署名証明書を発行したCA局から入手できます。

また、相手サーバー検証に使用するCA署名証明書は、相手サーバーのCA署名証明書を発行したCA局から入手できます。

- 自己署名証明書

プリンター自らが署名し、発行した証明書です。ルート証明書とも呼ばれます。発行者が自分自身を証明しているので、証明書として信頼性がなく、なりすましは防げません。

セキュリティ設定をする際にCA署名証明書なしで簡易的にSSL/TLS通信を行う場合に使用してください。

ブラウザに証明書の登録がないために、SSL/TLS通信でプリンターにアクセスするとセキュリティ警告が出る場合があります。自己署名証明書はSSL通信のみで使用できます。

関連情報

- ➡ [「CA署名証明書の取得とインポート」 55ページ](#)
- ➡ [「CA署名証明書を削除する」 58ページ](#)
- ➡ [「自己署名証明書を更新する」 59ページ](#)

CA署名証明書の取得とインポート

CA署名証明書を取得する

CA署名証明書を取得するにはCSR（証明書発行要求）を生成し、CA局に申請します。CSRはWeb Configかコンピューターで生成してください。

ここではWeb Configから取得する方法を説明します。Web Configで生成したCSRの証明書はPEM/DER形式です。

1. Web Configで【ネットワークセキュリティ】タブを選択し、【SSL/TLS】 - 【証明書】または【IPsec/IPフィルタリング】 - 【クライアント証明書】または【IEEE802.1X】 - 【クライアント証明書】を選択します。

どれを選択しても同じ証明書が取得でき、共通で使用できます。

2. 【CSR】の【生成】をクリックします。

CSR生成画面が開きます。

3. 各項目を設定します。



対応している公開鍵長や省略の可否はCA局によって異なる場合があります。申請するCA局のルールに従って記載してください。

4. 【設定】をクリックします。

生成されると完了メッセージが表示されます。

5. 【ネットワークセキュリティ】タブを選択し、【SSL/TLS】 - 【証明書】または【IPsec/IPフィルタリング】 - 【クライアント証明書】または【IEEE802.1X】 - 【クライアント証明書】を選択します。

6. CA局規定のファイル形式に従い [CSR] のダウンロードボタンをクリックして、CSRをコンピューターにダウンロードします。

！重要 再度CSRを生成しないでください。交付されたCA署名証明書がインポートできなくなります。

7. 保存したCSRをCA局に送付し、CA署名証明書を入手します。
送付方法や送付形態は、CA局の規定に従ってください。
8. 入手したCA署名証明書を、プリンターに接続しているコンピューターに保存します。
指定場所にCA署名証明書ファイルが保存されたら完了です。

CSRの設定項目

項目	設定値と説明
公開鍵長	CSRIに使用する公開鍵長を選択します。
コモンネーム	1～128文字以内で入力できます。IPアドレスを指定するときは、固定のIPアドレスを設定します。IPv4アドレス、IPv6アドレス、ホスト名、FQDNを「.」カンマで区切って1～5個入力できます。 先頭の要素がコモンネームに格納され、その他の要素は証明書のサブジェクトの別名フィールドに格納されます。 記入例： プリンターのIPアドレス：192.0.2.123、プリンター名：EPSONA1B2C3 コモンネーム：EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
組織名/ 部署名/ 市町村名/ 都道府県名	ASCII (0x20-0x7E)で表せる0～64文字以内で入力できます。識別名 (CN) はカンマで分割できます。
国コード	ISO-3166で規定している2文字の国コードを入力します。
送信元アドレス	メールサーバー設定の送信元アドレスを入力できます。[ネットワーク] タブ - [メールサーバー] - [基本] の [送信元アドレス] と同じメールアドレスを入力してください。

CA署名証明書をインポートする

取得したCA署名証明書をプリンターにインポートします。

- ！重要**
- プリンターの日付と時刻が正しく設定されていることを確認してください。証明書が無効になる場合があります。
 - Web Configで生成したCSRで証明書を取得した場合、証明書をインポートできるのは一度だけです。

1. Web Configで [ネットワークセキュリティ] タブを選択し、[SSL/TLS] - [証明書] または [IPsec/IPフィルタリング] - [クライアント証明書] または [IEEE802.1X] - [クライアント証明書] を選択します。
2. [インポート] をクリックします。
証明書インポート設定画面が開きます。


3. 各項目を設定します。[CA証明書1]、[CA証明書2] はプリンターにアクセスするブラウザで証明書のパスを検証する場合に設定してください。

インポートの設定内容は、CSRの生成場所や証明書のファイル形式によって異なります。以下を参考にして入力が必要な項目を設定してください。

- Web Configから取得したPEM/DER形式の証明書
 - [秘密鍵]：プリンターで保持しているため設定しない
 - [パスワード]：設定しない
 - [CA証明書1] / [CA証明書2]：任意
- コンピューターから取得したPEM/DER形式の証明書
 - [秘密鍵]：設定する
 - [パスワード]：設定しない
 - [CA証明書1] / [CA証明書2]：任意
- コンピューターから取得したPKCS#12形式の証明書
 - [秘密鍵]：設定しない
 - [パスワード]：任意
 - [CA証明書1] / [CA証明書2]：設定しない

4. [設定] をクリックします。

インポートされると完了メッセージが表示されます。

 **参考** [表示] をクリックするとインポートした証明書の情報が確認できます。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)
- ➡ [「CA署名証明書のインポート設定項目」 57ページ](#)

CA署名証明書のインポート設定項目

項目	設定値と説明
サーバー証明書 または クライアント証明書	取得したCA署名証明書のファイル形式を選択し、ファイルを指定します。 SSL/TLSの場合、サーバー証明書になります。 IPsec/IP フィルタリング、IEEE802.1Xの場合はクライアント証明書になります。
秘密鍵	コンピューターで生成したCSRでPEM/DER形式の証明書を取得した場合、証明書と対になった秘密鍵ファイルを指定します。
パスワード	ファイル形式が[秘密鍵付き証明書 (PKCS#12)] の場合、証明書取得時に設定した秘密鍵暗号化のパスワードを入力します。
CA証明書1	ファイル形式が[証明書 (PEM/DER)] の場合、サーバー証明書として使うCA署名証明書を発行したCA局の証明書をインポートします。必要に応じて設定してください。

項目	設定値と説明
CA証明書2	ファイル形式が「証明書（PEM/DER）」の場合、CA証明書1を発行した機関の証明書をインポートします。必要に応じて設定してください。

関連情報

➡ [「CA署名証明書をインポートする」 56ページ](#)

CA署名証明書を削除する

サービスが無効になった証明書や使用していない証明書は削除できます。

！重要 Web Configで生成したCSRで取得した証明書は、一度削除すると再インポートができません。必要な場合はCSRを再生成して取得し直してください。

1. Web Configで「ネットワークセキュリティ」タブを選択します。[SSL/TLS] - 「証明書」または [IPsec/IPフィルタリング] - 「クライアント証明書」または [IEEE802.1X] - 「クライアント証明書」を選択します。
2. 「削除」をクリックします。
3. 確認のメッセージを確認して、削除します。

相手サーバー検証用CA証明書を設定する

相手サーバー検証用CA証明書を設定すると、プリンターがアクセスするサーバーのCA証明書のパスを検証できます。これによってなりすましを防止できます。

相手サーバー検証用CA証明書は相手サーバーのCA署名証明書を発行したCA局から入手できます。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)
- ➡ [「CSRの設定項目」 56ページ](#)
- ➡ [「CA署名証明書をインポートする」 56ページ](#)

相手サーバー検証用CA証明書をインポートする

相手サーバー検証用CA証明書をプリンターにインポートします。

1. Web Configで「ネットワークセキュリティ」タブ - 「相手サーバー検証用CA証明書」を選択します。
2. 「インポート」をクリックします。

3. インポートする相手サーバー検証用CA証明書ファイルを指定します。

4. **【設定】** をクリックします。

インポートされると**【相手サーバー検証用CA証明書】**に戻り、インポートされた相手サーバー検証用CA証明書の情報が表示されます。

相手サーバー検証用CA証明書を削除する

インポート済みの相手サーバー検証用CA証明書を削除します。

1. Web Configで**【ネットワークセキュリティ】** タブ - **【相手サーバー検証用CA証明書】** を選択します。
2. 削除したい相手サーバー検証用CA証明書の**【削除】** をクリックします。
3. 確認のメッセージを確認して、削除します。
4. **【ネットワーク再起動】** をクリックし、更新された画面で削除したCA証明書が一覧にないことを確認してください。

関連情報

➡ [「Web Configの起動」 23ページ](#)

➡ [「Web Configで管理者としてログオンする」 35ページ](#)

自己署名証明書を更新する

自己署名証明書はプリンターが発行しているので、有効期限が切れた場合や記載している内容に変更があった場合などに更新できます。

1. Web Configで**【ネットワークセキュリティ】** タブ - **【SSL/TLS】** - **【証明書】** を選択します。

2. **【更新】** をクリックします。

3. **【コモンネーム】** を入力します。

IPv4アドレス、IPv6アドレス、ホスト名、FQDNを「.」カンマで区切って5個まで、1～128文字以内で入力できます。先頭の要素がコモンネームに格納され、その他の要素は証明書のサブジェクトの別名フィールドに格納されます。

記入例：

プリンターのIPアドレス：192.0.2.123、プリンター名：EPSONA1B2C3

コモンネーム：EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. 証明書の有効期間を選択します。

5. **【次へ】** をクリックします。

確認画面が表示されます。

6. 「設定」をクリックします。

設定がプリンターに反映されます。

参考 「ネットワークセキュリティ」タブ - 「SSL/TLS」 - 「証明書」 - 「自己署名証明書」にある「表示」をクリックすると証明書の情報が確認できます。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)

利用するプロトコルを制御する

プリンターに印刷する場合、いろいろな経路やプロトコルから印刷できます。
使わない機能やプロトコル、サービスを無効にすることで意図しない経路からの不正なアクセスや印刷などのセキュリティリスクを軽減できます。

プロトコルを制御する

プリンターが対応している制御可能なプロトコルの設定をします。

1. Web Configで「ネットワークセキュリティ」タブ - 「プロトコル」を選択します。
2. 各項目を設定します。
3. 「次へ」をクリックします。
4. 「設定」をクリックします。

設定がプリンターに反映されます。

有効・無効が設定可能なプロトコル

プロトコル	説明
Bonjour設定	Bonjourを使用するかを指定できます。Bonjourは機器の検索や印刷などに使われます。
SLP設定	SLP機能の有効・無効が設定できます。SLPはエプソンプリンターではプッシュスキャン機能やEpsonNet Configでのネットワーク探索に使われます。
WSD設定	WSD機能の有効・無効が設定できます。WSDデバイスの追加やWSDポートからの印刷ができるようになります。
LLTD設定	LLTDの有効・無効が設定できます。有効にするとWindowsのネットワークマップに表示されるようになります。

プロトコル	説明
LLMNR設定	LLMNRの有効・無効が設定できます。有効にするとDNSが使えない状況でもNetBIOSを使用せずに名前解決ができるようになります。
LPR設定	LPR印刷を許可するかを指定できます。有効にするとLPRポートからの印刷ができるようになります。
RAW (Port9100) 設定	RAWポート (Port9100) からの印刷を許可するかを指定できます。有効にするとRAWポート (Port9100) からの印刷ができるようになります。
IPP設定	IPPからの印刷を許可するかを指定できます。有効にするとインターネット経由の印刷ができるようになります。
FTP設定	FTP印刷を許可するかを指定できます。有効にするとFTPサーバーからの印刷ができるようになります。
SNMPv1/v2c設定	SNMPv1/v2cの有効・無効を指定できます。エプソンプリンターでは機器の設定や監視などに使われます。
SNMPv3設定	SNMPv3の有効・無効を指定できます。エプソンプリンターでは暗号化した機器の設定や監視などの通信で使われます。

プロトコルの設定項目

Bonjour設定

項目	設定値と説明
Bonjourを使用する	チェックを入れるとBonjourで機器を検索または使用することを許可します。
Bonjour名	Bonjour名が表示されます。
Bonjourサービス名	Bonjourサービス名が表示されます。
ロケーション	Bonjourのロケーションが表示されます。
最優先プロトコル	Bonjour印刷の最優先プロトコルを選択します。
Wide-Area Bonjour	Wide-Area Bonjourを使用するかどうか設定します。

SLP設定

項目	設定値と説明
SLP機能を有効にする	チェックを入れるとSLP機能が有効になります。 EpsonNet Configでのネットワーク探索に使われます。

WSD設定

エンタープライズセキュリティ設定編

項目	設定値と説明
WSDを有効にする	チェックを入れるとWSDによるデバイス追加が有効になります。本製品をデバイス検索をさせないようにしたい場合は、この項目を無効にし、あわせて「IPPを有効にする」の項目も無効にしてください。
印刷タイムアウト (秒)	WSD印刷の通信タイムアウト時間を3～3600秒の範囲で入力します。
デバイス名	WSDのデバイス名が表示されます。
ロケーション	WSDのロケーションが表示されます。

LLTD設定

項目	設定値と説明
LLTDを有効にする	チェックを入れるとLLTDが有効になります。有効にするとWindowsのネットワークマップに表示されるようになります。
デバイス名	LLTDのデバイス名が表示されます。

LLMNR設定

項目	設定値と説明
LLMNRを有効にする	チェックを入れるとLLMNRが有効になります。有効にするとDNSが使えない状況でもNetBIOSを使用せずに名前解決ができるようになります。

LPR設定

項目	設定値と説明
LPRポートからの印刷を許可する	チェックを入れるとLPRポートからの印刷を許可します。
印刷タイムアウト (秒)	LPR印刷の通信のタイムアウト時間を0～3600秒の範囲で入力します。「0」はタイムアウトなしを表します。

RAW (Port9100) 設定

項目	設定値と説明
RAWポート(Port9100)からの印刷を許可する	チェックを入れるとRAWポート (Port9100) からの印刷を許可します。
印刷タイムアウト (秒)	RAW (Port9100) 印刷の通信タイムアウト時間を0～3600秒の範囲で入力します。「0」はタイムアウトなしを表します。

IPP設定

エンタープライズセキュリティ設定編

項目	設定値と説明
IPPを有効にする	チェックを入れるとIPP通信が有効になります。有効にすると、インターネット経由で印刷できるようになります。ネットワーク上でデバイスを探索するときにも表示されます。IPPをサポートしているプリンターのみ表示されます。
非セキュア通信を許可する	〔許可する〕を選択すると非セキュア（IPP）で通信します。
通信タイムアウト（秒）	IPP印刷の通信のタイムアウト時間を0～3600秒の範囲で入力します。「0」はタイムアウトなしを表します。
URL（ネットワーク）	ネットワークに接続されている場合にIPPのURL（httpとhttps）が併記されます。URLはプリンターのIPアドレスとポート番号とIPPのプリンター名が組み合わされた値です。
プリンター名	IPPのプリンター名が表示されます。
ロケーション	IPPのロケーションが表示されます。

FTP設定

項目	設定値と説明
FTPサーバーを有効にする	チェックを入れるとFTP通信が有効になります。FTP印刷をサポートしているプリンターのみ表示されます。
通信タイムアウト（秒）	FTP印刷の通信のタイムアウト時間を0～3600秒の範囲で入力します。「0」はタイムアウトなしを表します。

SNMPv1/v2c設定

項目	設定値と説明
SNMPv1を有効にする	チェックを入れるとSNMPv1が有効になります。
SNMPv2cを有効にする	チェックを入れるとSNMPv2cが有効になります。
アクセス権限	SNMPv1またはSNMPv2cを有効にした場合にアクセス権限を設定します。〔読み込み専用〕または〔読み書き可能〕を選択します。
コミュニティ名（読み込み専用）	ASCII（0x20～0x7E）で表せる32文字以内で入力します。指定しない場合は空白にします。
コミュニティ名（読み書き可能）	ASCII（0x20～0x7E）で表せる32文字以内で入力します。指定しない場合は空白にします。
Epsonツールからのアクセスを許可する	Epson Device AdminなどのEpsonツールからの書き込みを許可するかどうかを設定します。

SNMPv3設定

項目	設定値と説明
SNMPv3を有効にする	チェックを入れるとSNMPv3が有効になります。

項目		設定値と説明
ユーザー名		1バイト文字を使って1～32文字以内で入力します。
認証設定		
	アルゴリズム	SNMPv3の認証用のアルゴリズムを選択します。
	パスワード	SNMPv3の認証パスワードを入力します。 ASCII (0x20-0x7E)で表せる32文字以内で入力します。指定しない場合は空白にします。
	パスワード確認入力	確認のため、入力したパスワードをもう一度入力します。
暗号化設定		
	アルゴリズム	暗号化アルゴリズムを選択します。
	パスワード	暗号化パスワードを入力します。 ASCII (0x20-0x7E)で表せる32文字以内で入力します。指定しない場合は空白にします。
	パスワード確認入力	確認のため、入力したパスワードをもう一度入力します。
コンテキスト名		Unicode (UTF-8) で表せる32文字以内で入力します。指定しない場合は空白にします。言語によって扱える文字数は異なります。

IPsec/IPフィルタリングで暗号化通信する

IPsec/IPフィルタリングの概要

IPsec/IPフィルタリング機能を使用すると、IPアドレス、サービスの種類、受信や送信ポートなどをフィルタリングできます。これらを組み合わせることによって、特定のクライアントからのデータや特定の種類のデータを通過させたり、遮断したりできます。IPsecと組み合わせることによってさらに強固なセキュリティ通信ができます。

基本ポリシーを設定する

フィルタリングのために基本ポリシーを設定します。基本ポリシーはプリンターにアクセスする全てのクライアントに影響します。より細かくアクセスを制御するには、個別ポリシーを設定します。

1. Web Configで「ネットワークセキュリティ」タブ - 「IPsec/IPフィルタリング」 - 「基本」を選択します。
2. 各項目を設定します。

3. [次へ] をクリックします。

確認画面が表示されます。

4. [設定] をクリックします。

設定がプリンターに反映されます。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)
- ➡ [「基本ポリシーの設定項目」 65ページ](#)

基本ポリシーの設定項目

[基本ポリシー]

項目	設定値と説明
IPsec/IPフィルタリング	IPsec/IPフィルタリング機能を有効または無効にします。

- [通信処理]
IP通信の制御方法を設定します。

項目	設定値と説明
通信を通過	IPパケットの通過を許可するときに選択します。
通信を遮断	IPパケットを遮断したいときに選択します。
IPsecの使用	IPsecで送られたパケットの通過を許可するときに選択します。

- [IKEバージョン]
[IKEバージョン] で [IKEv1] または [IKEv2] を選択します。プリンターを接続する機器に合わせて選択してください。
- IKEv1
[IKEバージョン] で [IKEv1] を選択すると表示されます。

項目	設定値と説明
認証方式	CA署名証明書をインポートすると [証明書] が選択できるようになります。
事前共有キー	[認証方式] で [事前共有キー] を選択した場合、1～127文字以内で事前共有キーを設定します。
事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

- IKEv2
[IKEバージョン] で [IKEv2] を選択すると表示されます。

項目		設定値と説明
ローカル認証	認証方式	CA署名証明書をインポートすると「証明書」が選択できるようになります。
	IDの種類	「認証方式」で「事前共有キー」を選択した場合、プリンターを何のIDで認証させるか選択します。
	ID	IDの種類に合わせてプリンターのIDを入力します。 いずれの場合も先頭に@#=は使用できません。 「識別名」：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。=を含めてください。 「IPアドレス」：IPv4またはIPv6形式で入力します。 「FQDN」：半角英数字、ドット、ハイフンを組み合わせて1～255文字以内で入力します。 「メールアドレス」：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。@を含めてください。 「任意の文字列」：ASCII（0x20～0x7E）で表せる1バイト文字で1～255文字以内で入力します。
	事前共有キー	「認証方式」で「事前共有キー」を選択した場合、1～127文字以内で事前共有キーを設定します。
	事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

項目		設定値と説明
リモート認証	認証方式	CA署名証明書をインポートすると「証明書」が選択できるようになります。
	IDの種類	「認証方式」で「事前共有キー」を選択した場合、認証相手を表すIDの種類を選択します。
	ID	IDの種類に合わせてプリンターのIDを入力します。 いずれの場合も先頭に@#=は使用できません。 「識別名」：ASCII (0x20～0x7E) で表せる1バイト文字で1～255文字以内で入力します。=を含めてください。 「IPアドレス」：IPv4またはIPv6形式で入力します。 「FQDN」：半角英数字、ドット、ハイフンを組み合わせて1～255文字以内で入力します。 「メールアドレス」：ASCII (0x20～0x7E) で表せる1バイト文字で1～255文字以内で入力します。@を含めてください。 「任意の文字列」：ASCII (0x20～0x7E) で表せる1バイト文字で1～255文字以内で入力します。
	事前共有キー	「認証方式」で「事前共有キー」を選択した場合、1～127文字以内で事前共有キーを設定します。
	事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

- 「カプセル化」
「通信処理」で「IPsecの使用」を選択した場合、IPsecの通信モードを設定します。

項目	設定値と説明
トランスポートモード	主に同じLAN内だけでプリンターとIPsec通信をする場合に選択します。IPパケットのレイヤー4以上のデータ部のみが暗号化されます。
トンネルモード	主にIPsec-VPNのようなインターネットが有効なネットワークでプリンターを接続するときに選択します。IPパケットのヘッダーとデータが暗号化されます。 「リモートゲートウェイアドレス(トンネルモード)」：「カプセル化」で「トンネルモード」を選択した場合、1～39文字以内でゲートウェイアドレスを設定します。

- 「セキュリティプロトコル」
「通信処理」で「IPsecの使用」を選択した場合、IPsecのセキュリティプロトコルを選択します。

項目	設定値と説明
ESP	認証とデータの完全性の保証に加えてデータ全体を暗号化します。
AH	認証とデータの完全性の保証をします。データの暗号化が禁止されていてもIPsec通信ができます。

- [アルゴリズム設定]

全ての設定で[任意]を選択するか、個別に[任意]以外を選択することをお勧めします。一部のアルゴリズム設定[任意]にして、一部を[任意]以外で選択した場合、相手の設定によっては通信ができない場合があります。

項目		設定値と説明
IKE	暗号化アルゴリズム	IKEで利用する暗号化アルゴリズムを選択します。 IKEのバージョンで選択できる項目が異なります。
	認証アルゴリズム	IKEで利用する認証アルゴリズムを選択します。
	鍵交換アルゴリズム	IKEで利用する鍵交換アルゴリズムを選択します。 IKEのバージョンで選択できる項目が異なります。
ESP	暗号化アルゴリズム	ESPで利用する暗号化アルゴリズムを選択します。 [セキュリティプロトコル]が[ESP]のときに選択できます。
	認証アルゴリズム	ESPで利用する認証アルゴリズムを選択します。 [セキュリティプロトコル]が[ESP]のときに選択できます。
AH	認証アルゴリズム	AHで利用する認証アルゴリズムを選択します。 [セキュリティプロトコル]が[AH]のときに選択できます。

関連情報

➡ [「基本ポリシーを設定する」64ページ](#)

個別ポリシーを設定する

個別ポリシーは、プリンターへの各アクセスに適用されるルールです。IPパケットを受け取ったプリンターはポリシーを参照し、IPパケットを制御します。ポリシーは、個別ポリシー1、個別ポリシー2と順に適用され、最後に基本ポリシーが適用されます。

1. Web Configで[ネットワークセキュリティ] タブ - [IPsec/IPフィルタリング] - [基本] を選択します。
2. 設定したい番号のタブをクリックします。
3. 各項目を設定します。
4. [次へ] をクリックします。
確認画面が表示されます。
5. [設定] をクリックします。
設定がプリンターに反映されます。

関連情報

- ➡ [「Web Configの起動」23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」35ページ](#)
- ➡ [「個別ポリシーのサービス名一覧」73ページ](#)

個別ポリシーの設定項目

項目	設定値と説明
この個別ポリシーを有効にする	選択している個別ポリシーを有効または無効にします。

〔通信処理〕

IP通信の制御方法を設定します。

項目	設定値と説明
通信を通過	IPパケットの通過を許可するときに選択します。
通信を遮断	IPパケットを遮断したいときに選択します。
IPsecの使用	IPsecで送られたパケットの通過を許可するときに選択します。

〔ローカルアドレス（プリンター）〕

お使いの環境に合ったIPv4アドレスまたはIPv6アドレスを選択します。IPアドレスの取得方法が自動の場合は、〔自動取得したIPv4アドレスを使用する〕が選択できます。

参考 IPv6アドレスが自動取得の場合、リースや有効期限切れで通信できなくなることがあります。固定のIPv6アドレスを設定してください。

〔リモートアドレス（ホスト）〕

通信を制御する機器のIPアドレスを入力します。IPアドレスは43文字以内で入力してください。何も入力しないと、全てのIPアドレスが制御の対象になります。

参考 IPアドレスがDHCPや自動取得（IPv6）の場合、リースや有効期限切れで通信できなくなることがあります。固定のIPアドレスを設定してください。

〔ポート指定方法〕

ポートの指定方法を設定します。

- サービス名
〔ポート指定方法〕で〔サービス名〕を選択した場合、IPsecのセキュリティプロトコルを選択します。
- トランスポートプロトコル
〔ポート指定方法〕で〔ポート番号〕を選択した場合、IPsecの通信モードを設定します。

項目	設定値と説明
全てのプロトコル	全てのプロトコルタイプを制御したい場合に選択します。
TCP	ユニキャストのデータを制御したい場合などに選択します。
UDP	ブロードキャストやマルチキャストのデータを制御したい場合などに選択します。
ICMPv4	pingコマンドを制御したい場合などに選択します。

- ローカルポート番号
〔ポート指定方法〕で〔ポート番号〕を選択し、かつ〔トランスポートプロトコル〕で〔TCP〕または〔UDP〕を選択した場合は、受信パケットを制御するポート番号をカンマで区切って記述します。最大10個指定できます。
記入例：20,80,119,5220
何も記述しないと、全てのポートが制御の対象になります。

- リモートポート番号

〔ポート指定方法〕で〔ポート番号〕を選択し、かつ〔トランスポートプロトコル〕で〔TCP〕または〔UDP〕を選択した場合は、送信パケットを制御するポート番号をカンマで区切って記述します。最大10個指定できます。

記入例：25,80,143,5220

何も記述しないと、全てのポートが制御の対象になります。

〔IKEバージョン〕

〔IKEバージョン〕で〔IKEv1〕または〔IKEv2〕を選択します。プリンターを接続する機器に合わせて選択してください。

- IKEv1

〔IKEバージョン〕で〔IKEv1〕を選択すると表示されます。

項目	設定値と説明
認証方式	〔通信処理〕で〔IPsecの使用〕を選択した場合、IPsecのセキュリティプロトコルを選択します。この証明書は基本ポリシーで設定したCA署名証明書と共通です。
事前共有キー	〔認証方式〕で〔事前共有キー〕を選択した場合、1～127文字以内で事前共有キーを設定します。
事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

- IKEv2
[IKEバージョン] で [IKEv2] を選択すると表示されます。

項目		設定値と説明
ローカル認証	認証方式	[通信処理] で [IPsecの使用] を選択した場合、IPsecのセキュリティプロトコルを選択します。この証明書は基本ポリシーで設定したCA署名証明書と共通です。
	IDの種類	[認証方式] で [事前共有キー] を選択した場合、プリンターを何のIDで認証させるか選択します。
	ID	IDの種類に合わせてプリンターのIDを入力します。 いずれの場合も先頭に@#=は使用できません。 [識別名] : ASCII (0x20～0x7E) で表せる1バイト文字で0～255文字以内で入力します。=を含めてください。 [IPアドレス] : IPv4またはIPv6形式で入力します。 [FQDN] : 半角英数字、ドット、ハイフンを組み合わせて1～255文字以内で入力します。 [メールアドレス] : ASCII (0x20～0x7E) で表せる1バイト文字で0～255文字以内で入力します。@を含めてください。 [任意の文字列] : ASCII (0x20～0x7E) で表せる1バイト文字で0～255文字以内で入力します。
	事前共有キー	[認証方式] で [事前共有キー] を選択した場合、1～127文字以内で事前共有キーを設定します。
	事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。
リモート認証	認証方式	[通信処理] で [IPsecの使用] を選択した場合、IPsecのセキュリティプロトコルを選択します。この証明書は基本ポリシーで設定したCA署名証明書と共通です。
	IDの種類	[認証方式] で [事前共有キー] を選択した場合、認証相手を表すIDの種類を選択します。
	ID	IDの種類に合わせてプリンターのIDを入力します。 いずれの場合も先頭に@#=は使用できません。 [識別名] : ASCII (0x20～0x7E) で表せる1バイト文字で0～255文字以内で入力します。=を含めてください。 [IPアドレス] : IPv4またはIPv6形式で入力します。 [FQDN] : 半角英数字、ドット、ハイフンを組み合わせて1～255文字以内で入力します。 [メールアドレス] : ASCII (0x20～0x7E) で表せる1バイト文字で0～255文字以内で入力します。@を含めてください。 [任意の文字列] : ASCII (0x20～0x7E) で表せる1バイト文字で0～255文字以内で入力します。
	事前共有キー	[認証方式] で [事前共有キー] を選択した場合、1～127文字以内で事前共有キーを設定します。
	事前共有キー確認入力	確認のため、設定したキーをもう一度入力します。

[カプセル化]

[通信処理] で [IPsecの使用] を選択した場合、IPsecの通信モードを設定します。

エンタープライズセキュリティ設定編

項目	設定値と説明
トランスポートモード	主に同じLAN内だけでプリンターとIPsec通信をする場合に選択します。IPパケットのレイヤー4以上のデータ部のみが暗号化されます。
トンネルモード	主にIPsec-VPNのようなインターネットが有効なネットワークでプリンターを接続するときに選択します。IPパケットのヘッダーとデータが暗号化されます。 [リモートゲートウェイアドレス(トンネルモード)] : [カプセル化] で [トンネルモード] を選択した場合、1～39文字以内でゲートウェイアドレスを設定します。

[セキュリティプロトコル]

[通信処理] で [IPsecの使用] を選択した場合、IPsecのセキュリティプロトコルを選択します。

項目	設定値と説明
ESP	認証とデータの完全性の保証に加えてデータ全体を暗号化します。
AH	認証とデータの完全性の保証をします。データの暗号化が禁止されていてもIPsec通信ができます。

[アルゴリズム設定]

全ての設定で [任意] を選択するか、全て個別に選択することをお勧めします。一部のアルゴリズム設定を [任意] にして一部を選択した場合、相手の設定によっては通信ができない場合があります。

項目		設定値と説明
IKE	暗号化アルゴリズム	IKEで利用する暗号化アルゴリズムを選択します。 IKEのバージョンで選択できる項目が異なります。
	認証アルゴリズム	IKEで利用する認証アルゴリズムを選択します。
	鍵交換アルゴリズム	IKEで利用する鍵交換アルゴリズムを選択します。 IKEのバージョンで選択できる項目が異なります。
ESP	暗号化アルゴリズム	ESPで利用する暗号化アルゴリズムを選択します。 [セキュリティプロトコル] が [ESP] のときに選択できます。
	認証アルゴリズム	ESPで利用する認証アルゴリズムを選択します。 [セキュリティプロトコル] が [ESP] のときに選択できます。
AH	認証アルゴリズム	AHで利用する認証アルゴリズムを選択します。 [セキュリティプロトコル] が [AH] のときに選択できます。

関連情報

- ➡ [「個別ポリシーを設定する」 68ページ](#)
- ➡ [「ローカルアドレス（プリンター）とリモートアドレス（ホスト）の組み合わせ」 73ページ](#)
- ➡ [「個別ポリシーのサービス名一覧」 73ページ](#)

ローカルアドレス（プリンター）とリモートアドレス（ホスト）の組み合わせ


		ローカルアドレス（プリンター）の設定値		
		IPv4	IPv6*2	使用可能な全てのアドレス*3
リモートアドレス（ホスト）の設定値	IPv4*1	○	×	○
	IPv6*1*2	×	○	○
	空白	○	○	○

*1 : [通信処理] で [IPsecの使用] を選択した場合、範囲指定はできません。

*2 : [通信処理] で [IPsecの使用] を選択した場合リンクローカルアドレス（fe80::）は選択できますが、個別ポリシーは無効になります。

*3 : IPv6リンクローカルアドレスは除きます。

個別ポリシーのサービス名一覧

 非対応のサービスは表示されますが、選択できません。

サービス名	プロトコルタイプ	ローカルポート番号	リモートポート番号	制御できる機能
全て	-	-	-	全てのサービス
ENPC	UDP	3289	任意	Epson Device Adminなどのアプリケーションソフト、プリンタードライバー（通信ドライバー）からのプリンター探索
SNMP	UDP	161	任意	Epson Device Adminなどのアプリケーションソフト、プリンタードライバー（通信ドライバー）からのプリンターMIB情報の取得と設定
LPR	TCP	515	任意	LPRデータの転送
RAW (Port9100)	TCP	9100	任意	RAWデータの転送
IPP/IPPS	TCP	631	任意	IPP/IPPS印刷のデータ転送
WSD	TCP	任意	5357	WSDの制御
WS-Discovery	UDP	3702	任意	WSDのプリンター探索
FTP データ (ローカル)	TCP	20	任意	FTPサーバー（FTP印刷のデータ転送）
FTP 制御 (ローカル)	TCP	21	任意	FTPサーバー（FTP印刷の制御）

サービス名	プロトコルタイプ	ローカルポート番号	リモートポート番号	制御できる機能
HTTP (ローカル)	TCP	80	任意	HTTP(S)サーバー (Web ConfigやWSDのデータ転送)
HTTPS (ローカル)	TCP	443	任意	
HTTP (リモート)	TCP	任意	80	HTTP(S)クライアント (ファームウェアアップデートやルート証明書の更新)
HTTPS (リモート)	TCP	任意	443	

IPsec/IPフィルタリングの設定例

IPsecで保護されたパケットだけを受け付ける

個別ポリシーを設定しない場合は、基本ポリシーだけが使われます。

〔基本ポリシー〕：

- 〔IPsec/IPフィルタリング〕：〔有効〕
- 〔通信処理〕：〔IPsecの使用〕
- 〔認証方式〕：〔事前共有キー〕
- 〔事前共有キー〕：1～127文字以内の任意文字

〔個別ポリシー〕：設定しない

印刷データとプリンター設定を受け付ける

指定したサービスからの印刷データとプリンター設定の通信を受け付ける場合の例です。

〔基本ポリシー〕：

- 〔IPsec/IPフィルタリング〕：〔有効〕
- 〔通信処理〕：〔通信を遮断〕

〔個別ポリシー〕：

- 〔この個別ポリシーを有効にする〕：チェックを入れる
- 〔通信処理〕：〔通信を通過〕
- 〔リモートアドレス (ホスト)〕：印刷クライアントのIPアドレス
- 〔ポート指定方法〕：〔サービス名〕
- 〔サービス名〕：〔ENPC〕、〔SNMP〕、〔HTTP (ローカル)〕、〔HTTPS (ローカル)〕、〔RAW (Port9100)〕にチェックを入れる

特定のIPアドレスからの通信のみ受け付ける

管理者など特定のコンピューターからの通信のみを受け付ける場合の例です。

〔基本ポリシー〕：

- 〔IPsec/IPフィルタリング〕：〔有効〕
- 〔通信処理〕：〔通信を遮断〕

〔個別ポリシー〕：

- 〔この個別ポリシーを有効にする〕：チェックを入れる
- 〔通信処理〕：〔通信を通過〕
- 〔リモートアドレス（ホスト）〕：管理者用クライアントのIPアドレス

参考 ポリシーの設定に関わらず、プリンターの検索や設定を行うためのプロトコルは使用できます。

IPsec/IPフィルタリングで使用する証明書を設定する

IPsec/IPフィルタリングで使用するクライアント証明書を設定します。設定すると、IPsec/IPフィルタリングの認証方式で証明書を使用できるようになります。なお、相手サーバー検証用の証明書を設定する場合は、〔相手サーバー検証用CA証明書〕で行います。

1. Web Configで〔ネットワークセキュリティ〕タブ - 〔IPsec/IPフィルタリング〕 - 〔クライアント証明書〕を選択します。
2. 〔クライアント証明書〕画面で証明書をインポートします。

CA局が発行した証明書をインポートしている場合は、証明書をコピーしてIPsec/IPフィルタリングで使用できます。コピーする場合は、〔コピー元〕からどの証明書を使うか選択して〔コピー〕をクリックしてください。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)
- ➡ [「CA署名証明書を取得する」 55ページ](#)

IEEE802.1X環境にプリンターを接続する

IEEE802.1Xを設定する

プリンターにIEEE802.1Xを設定すると、RADIUSサーバーと認証機能を持ったLANスイッチやアクセスポイントに接続されたネットワークで使用できます。

1. Web Configで〔ネットワークセキュリティ〕タブ - 〔IEEE802.1X〕 - 〔基本〕を選択します。
2. 各項目を設定します。

3. 〔次へ〕をクリックします。

確認画面が表示されます。

4. 〔設定〕をクリックします。

設定がプリンターに反映されます。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)
- ➡ [「IEEE802.1Xの設定項目」 76ページ](#)
- ➡ [「IEEE802.1Xを設定したのにつながらない」 81ページ](#)

IEEE802.1Xの設定項目

項目	設定値と説明	
IEEE802.1X (有線LAN)	[IEEE802.1X] - [基本] 画面で設定した値をIEEE802.1X (有線LAN) に対して有効または無効にするかを選択します。	
認証方式	プリンターとRADIUSサーバーとの認証方式を設定します。	
	EAP-TLS	CA署名証明書を取得してインポートする必要があります。
	PEAP-TLS	
	EAP-TTLS	パスワードを設定する必要があります。
	PEAP/MSCHAPv2	
ユーザーID	RADIUSサーバーの認証に使うIDを設定します。 ASCII (0x20～0x7E) で表せる1バイト文字で1～128文字以内で入力します。	
パスワード	プリンターを認証するためのパスワードを設定します。 ASCII (0x20～0x7E) で表せる1バイト文字で1～128文字以内で入力します。WindowsベースのプリントサーバーをRADIUSサーバーとして使用する場合は、最大127文字になります。	
パスワード確認入力	確認のため、入力したパスワードをもう一度入力します。	
サーバーID	特定のRADIUSサーバーで認証したいときに使用します。設定した文字列が、RADIUSサーバーから送信されるサーバー証明書のsubjectフィールドまたはsubjectAltNameフィールドに含まれているかを検証します。 ASCII (0x20～0x7E) で表せる1バイト文字で0～128文字以内で入力します。	
証明書の検証 (有線LAN)	相手サーバー証明書の検証を設定します。認証方式に関わらず設定ができます。[相手サーバー検証用CA証明書] 画面で証明書をインポートします。	
Anonymous名	[認証方式] が [PEAP-TLS] 、 [EAP-TTLS] 、 [PEAP/MSCHAPv2] の場合、PEAP認証のフェーズ1において、ユーザーIDの代わりに匿名を使用したいときに設定します。 ASCII (0x20～0x7E) で表せる1バイト文字で0～128文字以内で入力します。	
暗号強度	以下のいずれかを選択します。	
	高い	AES256/3DES
	標準	AES256/3DES/AES128/RC4

関連情報

- ➡ [「IEEE802.1Xを設定する」 75ページ](#)

IEEE802.1Xで使用する証明書を設定する

IEEE802.1Xで使用するクライアント証明書を設定します。設定すると、IEEE802.1Xの認証方式で[EAP-TLS]と[PEAP-TLS]が使用できるようになります。なお、相手サーバー検証用の証明書を設定する場合は、[相手サーバー検証用CA証明書]で行います。

1. Web Configで[ネットワークセキュリティ] タブ - [IEEE802.1X] - [クライアント証明書] を選択します。
2. [クライアント証明書] に使用する電子証明書を設定します。

CA局が発行した証明書をインポートしている場合は、証明書をコピーしてIEEE802.1Xで使用できます。コピーする場合は、[コピー元] からどの証明書をを使うか選択して[コピー] をクリックしてください。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)
- ➡ [「CA署名証明書の取得とインポート」 55ページ](#)

プリンターのIEEE802.1X状態表示

IEEE802.1Xの動作状態はネットワークステータスシートを印刷し、「IEEE802.1X」の項目で確認できます。ネットワークステータスシートの印刷方法はプリンターのマニュアルをご覧ください。

ステータス表示	IEEE802.1Xの動作状態
Disable	IEEE802.1X機能が無効になっています。
EAP Success	IEEE802.1X認証が成功し、ネットワークに接続されています。
Authenticating	IEEE802.1Xの認証中です。
Config Error	ユーザーIDが設定されていないため、認証に失敗しました。
Client Certificate Error	クライアント証明書の有効期限が切れているため、認証に失敗しました。
Timeout Error	RADIUSサーバーや認証ハブからの応答がないため、認証に失敗しました。
User ID Error	プリンターのユーザーIDまたは認証プロトコルに不備があるため、認証に失敗しました。
Server ID Error	サーバーの証明書に記載されているサーバーIDと通信しているサーバーIDが一致しないため、認証に失敗しました。
Server Certificate Error	サーバーの証明書に以下の不備があるため、認証に失敗しました。 <ul style="list-style-type: none"> • 証明書の有効期限切れ • 証明書のチェーンの異常

ステータス表示	IEEE802.1Xの動作状態
CA Certificate Error	<p>CA証明書に以下の不備があるため、認証に失敗しました。</p> <ul style="list-style-type: none"> • CA証明書の指定が間違っている • 正しいCA証明書がインポートされていない • CA証明書の有効期限切れ
EAP Failure	<p>プリンターの設定に以下の不備があるため、認証に失敗しました。</p> <ul style="list-style-type: none"> • クライアント証明書に何らかの不備がある（〔認証方式〕が〔EAP-TLS〕または〔PEAP-TLS〕の場合） • ユーザーIDまたはパスワードの間違い（〔認証方式〕が〔EAP-TTLS〕または〔PEAP/MSCHAPv2〕の場合）

トラブルを解決する

セキュリティ設定の初期化

IPsec/IPフィルタリングやIEEE802.1Xなど高度なセキュア環境を構築している場合、設定ミスや機器、サーバーのトラブルなどでデバイスと通信できなくなる可能性があります。この場合、セキュリティ機能を初期化してデバイスの設定をやり直したり、一時的に使用できるようにしたりします。

操作パネルからセキュリティ機能を無効にする

操作パネルを使ってIPsec/IPフィルタリングやIEEE802.1Xを無効に設定します。

1. Menu - [本体設定] - [ネットワーク設定] の順に選択します。
2. [詳細設定] を選択します。
3. 無効にしたい機能を選択します。
 - [IPsec/IPフィルタリングの無効化]
 - [IEEE802.1Xの無効化]
4. 確認画面で[設定開始] を選択します。
5. 設定完了のメッセージが表示されたら[閉じる] を選択します。
 [閉じる] を選択しなくても、一定時間を経過すると次の画面に進みます。

セキュア環境への接続時のトラブル

事前共有キーを忘れてしまった

事前共有キーを再設定する

Web Configの[ネットワークセキュリティ] タブ - [IPsec/IPフィルタリング] - [基本] - [基本ポリシー] または [個別ポリシー] の画面でキーを変更します。

事前共有キーを変更したら、相手先コンピュータの事前共有キーの設定もやり直してください。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)

IPsec通信ができない

プリンターまたはコンピュータがサポートしていないアルゴリズムを指定している

プリンターがサポートするアルゴリズムは以下の通りです。コンピュータの設定を確認してください。

セキュリティメソッド	アルゴリズム
IKE暗号化アルゴリズム	AES-CBC-128、AES-CBC-192、AES-CBC-256、AES-GCM-128*、AES-GCM-192*、AES-GCM-256*、3DES
IKE認証アルゴリズム	SHA-1、SHA-256、SHA-384、SHA-512、MD5
IKE鍵交換アルゴリズム	DH Group1、DH Group2、DH Group5、DH Group14、DH Group15、DH Group16、DH Group17、DH Group18、DH Group19、DH Group20、DH Group21、DH Group22、DH Group23、DH Group24、DH Group25、DH Group26、DH Group27*、DH Group28*、DH Group29*、DH Group30*
ESP暗号化アルゴリズム	AES-CBC-128、AES-CBC-192、AES-CBC-256、AES-GCM-128、AES-GCM-192、AES-GCM-256、3DES
ESP認証アルゴリズム	SHA-1、SHA-256、SHA-384、SHA-512、MD5
AH認証アルゴリズム	SHA-1、SHA-256、SHA-384、SHA-512、MD5

*：IKEv2のみ対応

関連情報

- ➡ [「IPsec/IPフィルタリングで暗号化通信する」 64ページ](#)

突然通信ができなくなった

プリンターのIPアドレスが変更された、または使用できなくなった

個別ポリシーのローカルアドレスに登録されているIPアドレスが変更や使用できなくなった場合、IPsecでは通信できなくなります。プリンターの操作パネルでIPsecを無効にしてください。

Web Configの [ネットワークセキュリティ] タブー [IPsec/IPフィルタリング] - [基本] - [個別ポリシー] - [ローカルアドレス (プリンター)] に設定したIPアドレスが、DHCPのリース切れや再起動、IPv6アドレスの有効期限切れや再取得失敗によって見つからない可能性があります。

IPアドレスは、固定のIPアドレスを使用してください。

コンピューターのIPアドレスが変更された、または使用できなくなった

個別ポリシーのリモートアドレスに登録されているIPアドレスが変更や使用できなくなった場合、IPsecでは通信できなくなります。

プリンターの操作パネルでIPsecを無効にしてください。

Web Configの [ネットワークセキュリティ] タブー [IPsec/IPフィルタリング] - [基本] - [個別ポリシー] - [リモートアドレス (ホスト)] に設定したIPアドレスが、DHCPのリース切れや再起動、IPv6アドレスの有効期限切れや再取得失敗によって見つからない可能性があります。

IPアドレスは、固定のIPアドレスを使用してください。

関連情報

- ➡ [「Web Configの起動」 23ページ](#)
- ➡ [「Web Configで管理者としてログオンする」 35ページ](#)
- ➡ [「IPsec/IPフィルタリングで暗号化通信する」 64ページ](#)

セキュアIPP印刷のポートが作成できない

SSL/TLS通信のサーバー証明書に正しい証明書が指定されていない

正しい証明書が指定されていないとポート作成に失敗する場合があります。証明書が正しいか確認してください。

プリンターを使用するコンピューターにCA証明書がインポートされていない

コンピューターにCA証明書がインポートされていないと、ポート作成に失敗する場合があります。CA証明書がインポートされているか確認してください。

関連情報

- ➡ [「IPsec/IPフィルタリングで暗号化通信する」 64ページ](#)

IPsec/IPフィルタリング設定したのにつながらない

IPsec/IPフィルタリングの設定が間違っている

プリンターの操作パネルからIPsec/IPフィルタリングを無効にしてください。プリンターとコンピューターを接続して、IPsec/IPフィルタリングの設定をやり直してください。

関連情報

➡ [「IPsec/IPフィルタリングで暗号化通信する」 64ページ](#)

IEEE802.1Xを設定したのにつながらない

IEEE802.1Xの設定が間違っている

プリンターの操作パネルからIEEE802.1Xを無効にしてください。プリンターとコンピューターを接続して、IEEE802.1Xの設定をやり直してください。

関連情報

➡ [「IEEE802.1Xを設定する」 75ページ](#)

電子証明書使用時のトラブル

CA署名証明書のインポートができない

入手したCA署名証明書と作成したCSRの情報が一致していない

CA署名証明書とCSRは、同一の情報である必要があります。以下の点を確認してください。

- 同時に複数の機器でCSRを作成した場合、一致しない機器に証明書をインポートしようとしたか
情報を確認して、一致する機器にインポートしてください
- CA局にCSRを送付した後、プリンターに保存されているCSRを再生成したか
再生成したCSRでCA署名証明書を取得し直してください。

入手したCA署名証明書のファイル容量が5KBを超えている

5KBを超えるCA署名証明書は、インポートできません。

証明書をインポートする際のパスワードが正しくない

正しいパスワードを入力してください。パスワードを忘れた場合、証明書をインポートできません。CA署名証明書を取得し直してください。

関連情報

➡ [「CA署名証明書をインポートする」 56ページ](#)

自己署名証明書が更新できない

コモンネームが入力されていない

「コモンネーム」は必ず入力してください。

コモンネームに不正な文字が使用されている

IPv4、IPv6、ホスト名、FQDNのいずれかの形式をASCII (0x20-0x7E)で表せる1～128文字以内で指定します。

【コモンネーム】にカンマやスペースが使われている

カンマが入力されると【コモンネーム】はそこで分割されます。また、カンマの前後にスペースを入れるとエラーになります。

関連情報

➡ [「自己署名証明書を更新する」59ページ](#)

CSRが作成できない

コモンネームが入力されていない

【コモンネーム】は必ず入力してください。

コモンネーム、組織名、部署名、市町村名、都道府県名に不正な文字が使用されている

IPv4、IPv6、ホスト名、FQDNのいずれかの形式をASCII (0x20-0x7E)で表せる文字で指定します。

コモンネームにカンマやスペースが使われている

カンマが入力されると【コモンネーム】はそこで分割されます。また、カンマの前後にスペースを入れるとエラーになります。

関連情報

➡ [「CA署名証明書を取得する」55ページ](#)

証明書に関する警告が表示された

メッセージ	原因と対処
サーバー証明書を指定してください。	原因： インポートするファイルが指定されていません。 対処： ファイルを選択してから【インポート】をクリックしてください。
CA証明書1の参照先を入力してください。	原因： CA証明書1が未入力で、CA証明書2が入力されています。 対処： 先にCA証明書1をインポートしてください。
以下の入力値が正しくありません。	原因： ファイルパスやパスワードに不正な文字が含まれています。 対処： 表示された項目に入力した文字が正しいか確認してください。

メッセージ	原因と対処
日付/時刻が設定されていません。	<p>原因： プリンターに日付や時刻が設定されていません。</p> <p>対処： Web ConfigやEpsonNet Configまたはプリンターの操作パネルから日付や時刻を設定してください。</p>
パスワードが正しくありません。	<p>原因： CA証明書に設定されているパスワードと入力したパスワードが一致しません。</p> <p>対処： 正しいパスワードを入力してください。</p>
不正なファイルです。	<p>原因： インポートしようとしたファイルがX509形式の証明書ではありません。</p> <p>対処： 信頼されたCA局から送付された証明書ファイルを選択しているか確認してください。</p>
	<p>原因： インポートできるファイルサイズを超えています。インポートできるファイルサイズは5KBです。</p> <p>対処： ファイルが正しい場合、証明書が破損していたり改ざんされていたりする可能性があります。</p>
	<p>原因： 証明書に含まれるチェーンが不正です。</p> <p>対処： 証明書の詳細はCA局のWebサイトをご覧ください。</p>
3つ以上のCA証明書が含まれたサーバー証明書は使用できません。	<p>原因： PKCS#12形式の証明書ファイルに3つ以上のCA証明書が含まれています。</p> <p>対処： PKCS#12形式から複数のPEM形式に変換して個別にインポートするか、2つ以下のCA証明書でPKCS#12形式ファイルを再作成してインポートしてください。</p>
有効期間外の証明書です。証明書の有効期間、またはプリンターの日付/時刻設定を確認してください。	<p>原因： 証明書の有効期限が切れています。</p> <p>対処：</p> <ul style="list-style-type: none"> 証明書の有効期限が切れている場合、新しい証明書をCA局から取得してインポートしてください。 証明書の有効期限が切れていない場合、プリンターの日付や時刻の設定が正しいか確認してください。

メッセージ	原因と対処
秘密鍵が必要な証明書ファイルです。	原因： 証明書と対になった秘密鍵がありません。 対処： <ul style="list-style-type: none"> • コンピューターで生成したCSRで取得したPEM/DER形式の証明書の場合、秘密鍵ファイルを指定してください。 • コンピューターで生成したCSRで取得したPKCS#12形式の証明書の場合、秘密鍵を含めたファイルを作成してください。
	原因： Web Configで生成したCSRで取得したPEM/DER形式の証明書を再度インポートしようとした。 対処： Web Configで生成したCSRで取得したPEM/DER形式の証明書は、一度しかインポートできません。
設定に失敗しました。	原因： プリンターとコンピューターの通信が遮断された、何らかの原因でファイルが読み取りできない、などの原因で正しく設定できませんでした。 対処： 指定しているファイルや通信状況を確認して、再度インポートしてください。

関連情報

➡ [「使用できる電子証明書」 54ページ](#)

CA署名証明書を誤って削除した

CA署名証明書をバックアップ保存したファイルがない

CA署名証明書をバックアップ保存したファイルがあれば、それを使って再度インポートしてください。
 Web Configで生成したCSRで取得した証明書は、一度削除してしまうと再インポートができません。CSRを再生成して証明書を取得し直してください。

関連情報

➡ [「CA署名証明書を削除する」 58ページ](#)

➡ [「CA署名証明書をインポートする」 56ページ](#)