EPSON
EXCEED YOUR VISION

システム管理者ガイド

CMP0317-00 JA

目次

商標 4

マニュアルの見方 5

マークの意味 5
マニュアル記載の前提 5
OS表記 5
マニュアルのご注意 6

はじめに 7

マニュアルの構成 7
マニュアルで使用する用語 7
用語 7
ネットワーク環境の例 9
プリンター接続のタイプ 12

プリンターの設定と管理 14

プリンター設定、管理の流れ 14
プリンターのネットワーク接続 15
印刷機能設定 15
メールサーバー設定 15
セキュリティー設定 15
運用・管理 16

ネットワーク接続編 17

ネットワーク接続の前に 17
接続設定情報の収集 17
IPアドレスの割り当て 18
DNSサーバー、プロキシサーバーについて 18
操作パネルでネットワークに接続する 18
IPアドレスを設定する 19
LANに接続する 20

機能設定編 23

設定に使うソフトウェア 23
Web Config（デバイスのウェブページ） 23
印刷機能を使う 24
サーバークライアント型接続での印刷設定 25
ピアツーピア型接続での印刷設定 28
メールサーバーを設定する 29
メールサーバー設定項目 30
メールサーバーとの接続を確認する 31
システムの詳細を設定する 33
操作パネルの動作を設定する 33
無操作時の省電力設定をする 34
タイムサーバーと日付/時刻を同期する 34
AirPrint設定 35
Epson Connectサービスを使う 35

本体のセキュリティー編 36

本体のセキュリティー機能の紹介 36
管理者パスワードの設定 36
操作パネルから管理者パスワードを変更する 37
Web Configから管理者パスワードを変更する 37
パネル操作を制限する 38
管理者ロックを有効にする 38
設定メニューの管理者ロック項目 38
外部インターフェイスを無効にする 39

運用・管理編 41

管理者としてプリンターにログオンする 41
Web Configで管理者としてログオンする 41
プリンターの情報を確認する 41
操作パネルから情報を確認する 41
Web Configから情報を確認する 42
イベント発生時にメール通知を受け取る 42
メール通知の概要 42
メール通知を設定する 42
ファームウェアのアップデート 44
Web Configでファームウェアをアップデートする 44
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 44
設定のバックアップ 45
設定をエクスポートする 45
設定をインポートする 45

トラブルを解決する 47

トラブルを解決するための糸口 47
プリンターの状態を確認する 47
エラーメッセージを確認する 47
ネットワーク接続診断レポートを印刷する 48
通信状態を確認する 54
接続テストをする 56
設定の初期化 57
トラブル事例 58
Web Configにアクセスできない 58
プリンター共有時のトラブル 60
共有サーバーの動作が重い 60
プリントサーバーのプリンター設定がクライアントコンピューターに反映されない 60

付録 61

ネットワーク関連のソフトウェア 61
Epson Device Admin 61
EpsonNet Config 61
EpsonNet Print（Windowsのみ） 62
EpsonNet SetupManager 63
操作パネルを使って無線LANに接続する（WPS） 63
プッシュボタンで自動設定する（AOSS/WPS） 63
PINコードで設定する（WPS） 64
Wi-Fi Direct（シンプルAP）接続を使う 64
Wi-Fi Direct（シンプルAP）の設定を変更する ...65
接続方法を変更する 66
有線LANから無線LANへの接続変更 66
無線LANから有線LANへの接続変更 67
プリンターが使用するポート 68

エンタープライズセキュリティー設定編 69

セキュリティー設定と防止できる脅威 70
セキュリティー機能の設定 70
プリンターとのSSL/TLS通信 71
使用できる電子証明書 71
CA署名証明書の取得とインポート 71
CA署名証明書を削除する 74
相手サーバー検証用CA証明書を設定する 75
利用するプロトコルを制御する 76
プロトコルを制御する 76
有効・無効が設定可能なプロトコル 77
プロトコルの設定項目 77
IPsec/IPフィルタリングで暗号化通信する 80
IPsec/IPフィルタリングの概要 80
基本ポリシーを設定する 80
個別ポリシーを設定する 84
IPsec/IPフィルタリングの設定例 90
IPsec/IPフィルタリングで使用する証明書を設定する 91
IEEE802.1X環境にプリンターを接続する 91
IEEE802.1Xを設定する 91
IEEE802.1Xで使用する証明書を設定する 93
プリンターのIEEE802.1X状態表示 93
トラブルを解決する 94
セキュリティー設定の初期化 94
セキュア環境への接続時のトラブル 95
電子証明書使用時のトラブル 97

商標

- EPSONおよびEXCEED YOUR VISIONはセイコーエプソン株式会社の登録商標です。
- Chrome、Chrome OS、AndroidはGoogle Inc.の商標です。
- Microsoft、Windows、Windows Serverは、米国Microsoft Corporationの米国およびその他の国における登録商標です。
- Apple、Mac、macOS、OS X、Bonjour、ColorSync、Safari、AirPrint、iPad、iPhone、iPod touch、iTunesは米国およびその他の国で登録されたApple Inc.の商標です。“iPhone”の商標は日本国内においてアイホン株式会社のライセンスに基づき使用されています。
- 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　この内容を無視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。この内容を無視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Windows Server 2012 R2の表示画面を使用しています。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 10」「Windows 8.1」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® 10 operating system 日本語版
- Microsoft® Windows® 8.1 operating system 日本語版

Mac OS

本書では、「macOS Big Sur」「macOS Catalina」「macOS Mojave」「macOS High Sierra」「macOS Sierra」「OS X El Capitan」「OS X Yosemite」「OS X Mavericks」「OS X Mountain Lion」「Mac OS X v10.7.x」「Mac OS X v10.6.8」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、お気付きの点があり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、不適当に使用されたり、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。

© 2021 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『ユーザーズガイド』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ー編

管理者パスワードの設定などプリンター本体に設定する、基本的なセキュリティー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ー設定編

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ー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サーバーによるプリンター共有）

プリンターをWindows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ー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）、EpsonNet SetupManager（エプソンネット セットアップマネージャー）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。

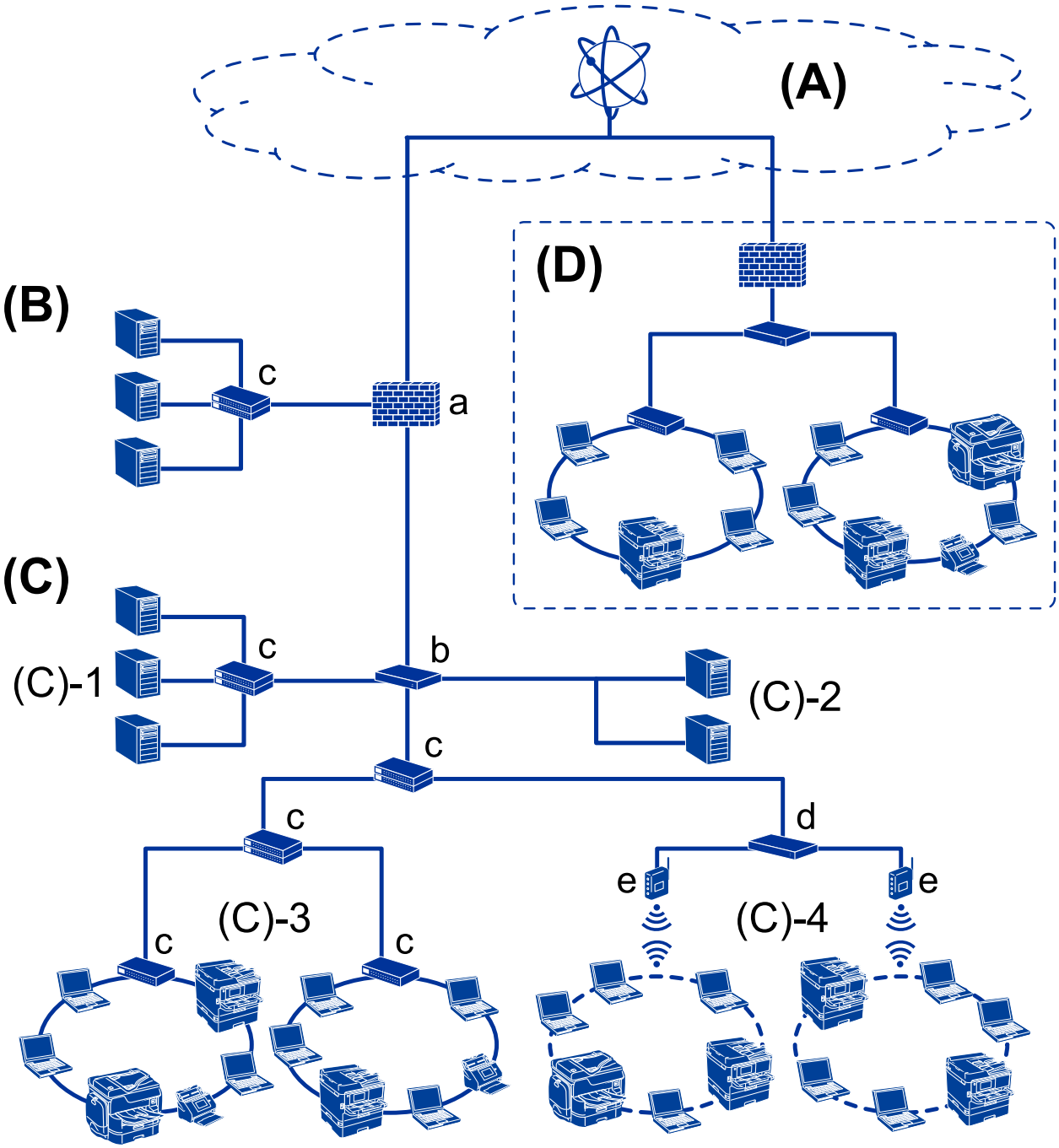
Unicode (UTF-8)

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

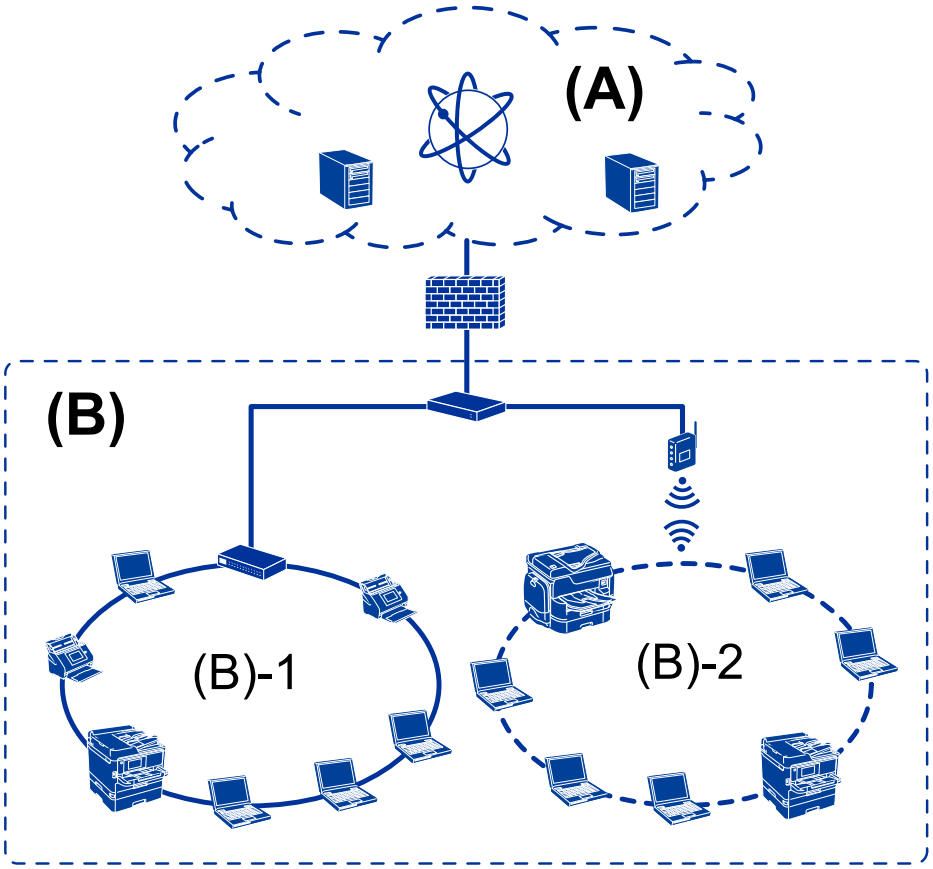
（C）：トラストゾーン（イントラネット）
ファイアウォールやUTM（総合脅威管理）で守られた信頼性のあるネットワークです。

- （C）-1：イントラネット内サーバー
  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ー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、セキュリティーを強化できます。
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：

Windowsサーバー上に、クライアントコンピューターの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ー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」7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ー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：

プリンタードライバーをコンピューターにインストールします。
EpsonNet SetupManagerを使うと、プリンター設定を含んだドライバーのパッケージを配布できます。

特徴：

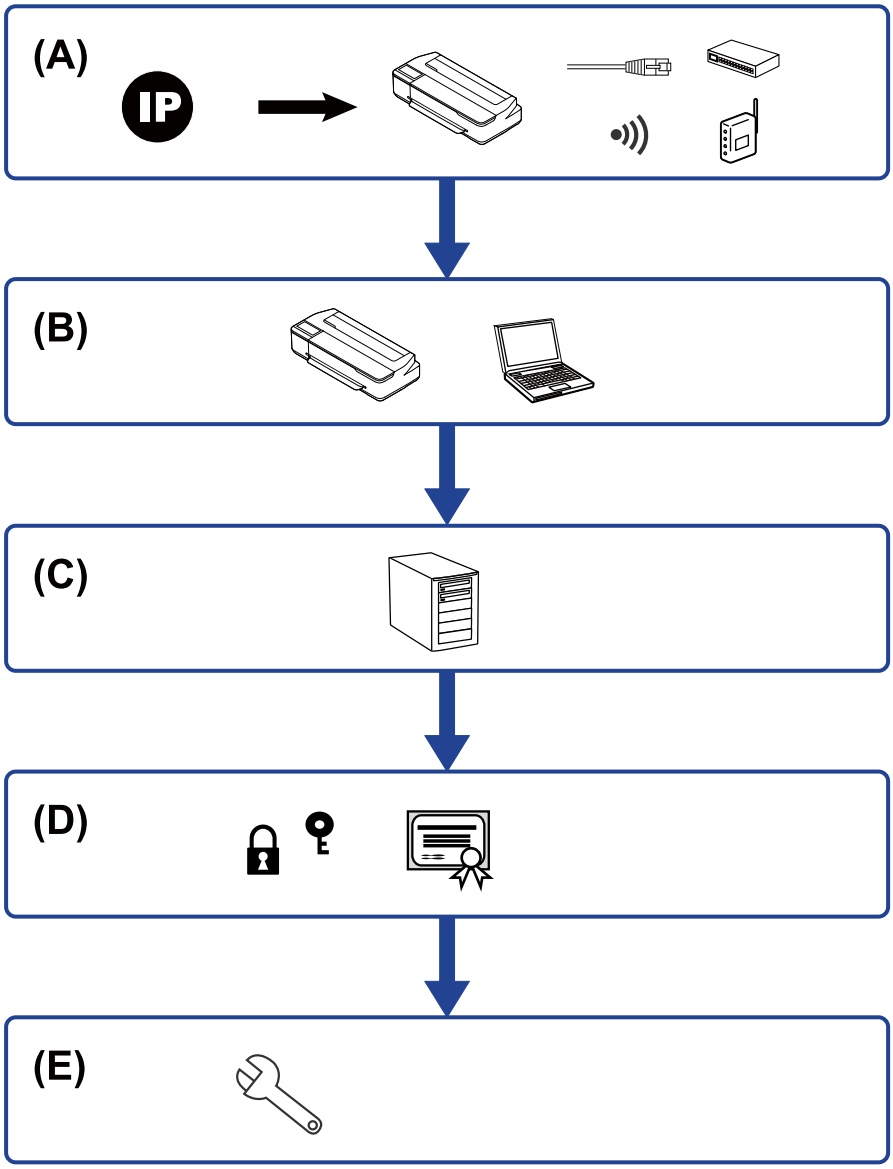
- プリンターに直接印刷データを送るので、印刷開始までに時間がかかりません。
- プリンターが稼働していれば印刷できます。

関連情報

➡ 「用語」7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	セキュリティー設定
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（LANケーブル接続、Wi-Fi設定）

関連情報

➡ 「ネットワーク接続編」17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」24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」29ページ

セキュリティー設定

- 管理者パスワード設定
- 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」36ページ
➡ 「エンタープライズセキュリティー設定編」69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」41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
デバイス接続方法	• 有線LAN • 無線LAN （Wi-Fi）	プリンターをネットワークに接続する方法を決定します。 有線LANは、LANスイッチ（ハブ）に接続します。 無線LANはアクセスポイントのSSIDに接続します。
LAN接続情報	• IPアドレス • サブネットマスク • デフォルトゲートウェイ	プリンターに割り当てるIPアドレスを決定します。 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。
無線LAN接続情報	• SSID • パスワード	プリンターを接続するアクセスポイントのSSID（ネットワークの名称）、パスワードです。 MACアドレスフィルタリング設定がされている場合は、プリンターを登録できるように事前にMACアドレスの登録をしておいてください。 対応している規格はユーザーズガイドをご覧ください。
DNSサーバー情報	• 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	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。 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。
プロキシサーバー情報	• プロキシサーバー名	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。 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。 • Epson Connectサービス • ファームウェア更新
ポート番号情報	• 開放するポート番号	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。 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。

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が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機能で割り当てる場合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『ユーザーズガイド』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［設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

3. ［ネットワーク設定］ - ［ネットワーク詳細設定］ - ［TCP/IP］の順に選択します。

4. ［手動］を選択します。

   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］を選択してください。［IPアドレス］、［サブネットマスク］、［デフォルトゲートウェイ］が自動設定され、IPアドレスの設定は終了です。

5. 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。

6. 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。

   設定が終了すると［ネットワーク詳細設定］画面に戻ります。

   参考 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、設定を続けることができません。入力した値に間違いがないか確認してください。

DNSサーバーを設定する

IPアドレスの設定に引き続き、必要に応じてDNSサーバーを設定します。

1. ホーム画面で［設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。
   IPアドレスの設定に続いて設定するときは、［ネットワーク詳細設定］画面が表示されています。手順3に進んでください。

2. ［ネットワーク設定］ - ［ネットワーク詳細設定］の順に選択します。

3. ［DNSサーバー］を選択します。

4. ［自動］または［手動］を選択します。

   IPアドレスを［自動］にした場合はDNSサーバー設定で［自動］、［手動］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］を選択して、次の手順に進みDNSサーバーのアドレスを入力してください。
   ［自動］を選択した場合は、DNSサーバーの設定は終了です。

5. プライマリーDNSの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。

6. 同様にセカンダリーDNSサーバーを設定します。

   セカンダリーDNSサーバーがない場合は、“0.0.0.0”に設定してください。
   設定が終了すると［ネットワーク詳細設定］画面に戻ります。

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
- Epson Connectサービスやファームウェアの更新など、プリンターが直接インターネットに接続する機能を使用する

1. ホーム画面で［設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。
   IPアドレスの設定に続いて設定するときは、［ネットワーク詳細設定］画面が表示されています。手順3に進んでください。

2. ［ネットワーク設定］ - ［ネットワーク詳細設定］の順に選択します。

3. ［プロキシサーバー］を選択します。

4. ［使用する］を選択します。

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。

6. プロキシサーバーのポート番号を入力します。

   設定が終了すると［ネットワーク詳細設定］画面に戻ります。

LANに接続する

プリンターを有線LANまたは無線LANに接続します。

関連情報

➡ 「有線LANに接続する」20ページ
➡ 「無線LAN（Wi-Fi）に接続する」21ページ

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［設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

3. ［ネットワーク設定］ - ［接続診断］の順に選択します。

   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。

4. ▽ボタンを押して終了します。

   OKボタンを押す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。

関連情報

➡ 「有線LANから無線LANへの接続変更」66ページ

無線LAN（Wi-Fi）に接続する

アクセスポイントに接続するための情報をプリンターの操作パネルから手動で設定する方法です。手動で設定するには、アクセスポイントのSSIDとパスワードの情報が必要です。

参考 アクセスポイント（無線LANルーター）がWPSやAOSSに対応していると、SSIDやパスワードを使わずにプッシュボタンやPINコードで無線LAN接続設定できます。

1. ホーム画面で［無線LAN設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

2. ［無線LANルーターとつなぐ(推奨)］を選択します。

3. OKボタンを押して、次の画面に進みます。

4. ［無線LANルーターを検索］を選択します。

5. 接続する無線LANルーター（アクセスポイント）の SSID をプリンターの操作パネルから選択し、 OK ボタンを押します。

   参考
   - プリンターの操作パネルに接続したいSSIDが表示されないときは、［再検索する］を選択して一覧を更新してください。それでも表示されないときは、 ［その他のSSID］を選択してSSIDを直接入力してください。
   - SSIDがわからない場合は無線LANルーターのラベルに書かれていないかを確認してください。無線LANルーター（アクセスポイント）をメーカー設定値のまま利用している場合は、ラベルに書かれているSSIDを使用します。

6. パスワードを入力します。

   設定が終了したら、ネットワーク接続診断レポートを印刷するかどうかを選択します。

   参考
   - パスワードは大文字と小文字を区別して入力してください。
   - SSIDがわからない場合は無線LANルーター（アクセスポイント）本体のラベルなどに情報がないか確認してください。無線LANルーター（アクセスポイント）をメーカー設定値のまま利用している場合は、ラベルに書かれているSSIDを使用します。情報が見つからない場合は、無線LANルーター（アクセスポイント）のマニュアルをご覧ください。

7. 接続が完了したら、OKボタンを押します。

参考 接続に失敗した場合は用紙をセットし、OKボタンを押してネットワーク接続診断レポートを印刷します。

関連情報

- 「ネットワーク接続診断レポートの見方と対処方法」49ページ
- 「操作パネルを使って無線LANに接続する（WPS）」63ページ
- 「無線LANから有線LANへの接続変更」67ページ

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ー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ーを起動して、プリンターのIPアドレスを入力します。ブラウザーの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ー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 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、管理者パスワードの初期値は製造番号（シリアルナンバー）です。プリンター本体のラベルに記載されている製造番号（シリアルナンバー）をご確認ください。
不正アクセスを防止するため、速やかに初期パスワードを変更することをお勧めします。

関連情報

- 「プリンターとのSSL/TLS通信」71ページ
- 「使用できる電子証明書」71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対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。
ここではWindows Server 2012 R2を代表例として説明します。

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。

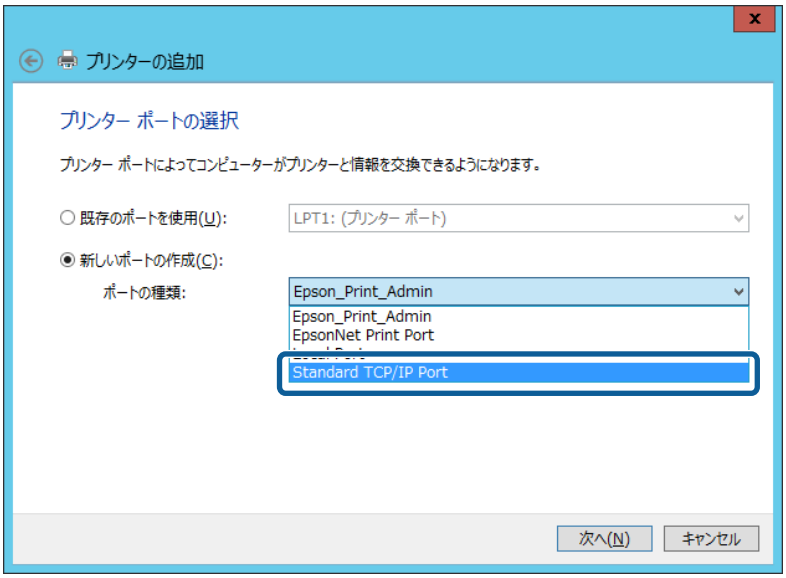
2. **プリンターを追加します。**

   ［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。**

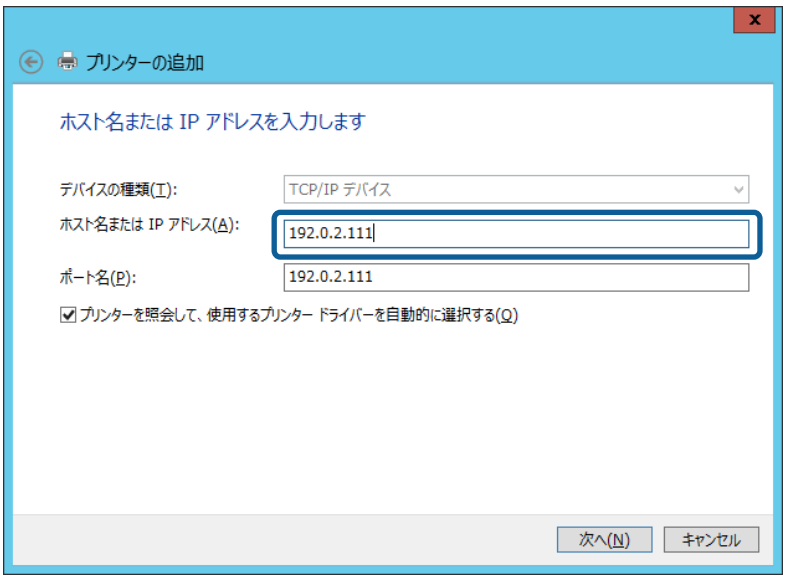


5. ［ホスト名またはIP アドレス］（または［プリンター名またはIP アドレス］）にプリンター名、またはプリンターのIP アドレスを入力して、［次へ］をクリックします。

   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を設定します。

   - プリンタードライバー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。
   - プリンタードライバーがインストールされていない場合
     ［ディスク使用］をクリックして、プリンターに付属のソフトウェアディスクをセットします。［参照］をクリックして、ディスクドライブのプリンタードライバーが格納されているフォルダーを指定します。正しいフォルダーを指定してください。OS環境により指定するフォルダーが異なります。
     32bit版Windows：WINX86
     64bit版Windows：WINX64

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）」27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ーで［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。

参考 プリンター共有時のトラブル

- 「共有サーバーの動作が重い」60ページ
- 「プリントサーバーのプリンター設定がクライアントコンピューターに反映されない」60ページ

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ーとクライアントコンピューター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ーで［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ーのWindowsバージョン（プロセッサータイプ）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」28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. プリント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）」27ページ
➡ 「追加ドライバーをインストールする（Windowsのみ）」27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をインストールします。

関連情報

➡ 「プリンタードライバーを設定する」28ページ

プリンター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でプリンタードライバーをインストールすることをお勧めします。エプソンのウェブサイトまたはソフトウェアディスクからインストーラーを起動します。

参考 たくさんのクライアントコンピューターからプリンターを使用する場合は、EpsonNet SetupManagerを使ってドライバーをパッケージして配布すると、インストール作業を大幅に軽減できます。

1. インストーラーを起動します。

   - ウェブサイトから起動する
     以下のウェブサイトにアクセスして、製品名を入力します。［セットアップ］に進み、ソフトウェアをダウンロードして起動します。
     http://epson.sn
   - ソフトウェアディスクから起動する（製品にソフトウェアディスクが同梱されていて、それを使用できる場合のみ）
     ソフトウェアディスクをコンピューターにセットします。

2. 接続方法を選択して、［次へ］をクリックします。

参考 ［ソフトウェアの変更と再接続方法を選択してください］画面が表示されたら、［プリンターの再セットアップ（無線LANルーターが替わった場合など）］を選択して［次へ］をクリックしてください。

3. この後は、画面の指示に従って操作します。

関連情報

➡ 「EpsonNet SetupManager」63ページ

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。

関連情報

- 「メールサーバーとの接続を確認する」31ページ
- 「メールサーバー設定項目」30ページ
- 「Web Configの起動」24ページ
- 「Web Configで管理者としてログオンする」41ページ

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	［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。 ［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。	
認証用パスワード	［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。 ［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。	
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。	

項目	設定値と説明	
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。
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。	

関連情報

➡ 「メールサーバーを設定する」29ページ

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」24ページ
➡ 「Web Configで管理者としてログオンする」41ページ
➡ 「メールサーバー接続確認結果」32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。 • 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。 • 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
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。 • 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。 • 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。

メッセージ	原因
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。
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」31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。

   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：［設定］ - ［プリンターの基本設定］ - ［言語選択/Language］
   - パネルロック ：［設定］ - ［セキュリティー設定］ - ［管理者設定］ - ［管理者ロック］
3. ［設定］をクリックします。

関連情報

➡ 「Web Configの起動」24ページ
➡ 「Web Configで管理者としてログオンする」41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. ［節電移行時間］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。

   参考 プリンターの操作パネルからも設定できます。
   ［設定］ - ［プリンターの基本設定］ - ［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。

   参考 プリンターの操作パネルからも設定できます。
   ［設定］ - ［プリンターの基本設定］ - ［自動電源オフ設定］
4. ［設定］をクリックします。

関連情報

➡ 「Web Configの起動」24ページ
➡ 「Web Configで管理者としてログオンする」41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。

参考 ［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」24ページ
➡ 「Web Configで管理者としてログオンする」41ページ

AirPrint設定

印刷をAirPrintで行うための設定をします。
Web Configで［ネットワーク］タブ - ［AirPrint設定］を選択します。

項目	説明
Bonjourサービス名	BonjourのサービスをASCII (0x20-0x7E)で表せる41文字以内で入力します。
ロケーション	プリンターの設定場所など任意のロケーション情報を、UTF-8で表せる127バイト以内の文字列で入力します。
位置情報 緯度、経度 (WGS84)	プリンターの位置情報を入力します。入力は任意です。 WGS-84測地系の値を使用し、緯度と経度を「,」で区切ります。 緯度は-90～+90、経度は-180～+180の範囲で入力できます。また、小数点以下は6位まで入力でき、+は省略できます。
最優先プロトコル	優先するプロトコルを、IPPとPort9100から選択します。
Wide-Area Bonjour	Wide-Area Bonjourを使用するかどうか設定します。使用する場合、セグメントを越えた検索ができるように、プリンターがDNSサーバーに登録されている必要があります。
AirPrintを有効にする	IPP、Bonjour、AirPrintが有効になり、IPPはセキュア通信のみになります。

Epson Connectサービスを使う

インターネットを利用したEpson Connect（エプソン コネクト）サービスを使うと、コンピューターやスマートデバイスからいつでもどこからでも印刷できます。
インターネットを利用したサービスは以下の通りです。

メールプリント	Epson iPrintリモートプリント	リモートプリントドライバー
✓	✓	✓

詳しくはEpson Connectのポータルサイトをご覧ください。
https://www.epsonconnect.com/

本体のセキュリティー編

この章では、デバイス本体のセキュリティー設定について説明しています。

本体のセキュリティー機能の紹介

エプソンデバイスのセキュリティー機能を紹介します。

機能名	どんな機能か	何を設定するのか	何を防止できるのか
管理者パスワードの設定	ネットワークやUSBの接続設定など、システムに関わる設定をロックし、管理者以外は変更ができないようにします。	システム管理者がデバイスにパスワードを設定します。 Web Config、操作パネルのどちらからも変更ができます。	デバイスに保持されているIDやパスワード、ネットワーク設定などの情報が不正に参照または変更されるのを防ぎます。また、ネットワーク環境やセキュリティーポリシー、またはそれらに類する情報の漏えいなど、広範囲のセキュリティーリスクにつながる危険性を低減します。
外部インターフェイス設定	デバイスへ接続するインターフェイスを制御できます。	コンピューターとのUSB接続の有効、無効を設定します。	ネットワークを経由しない印刷を禁止することで、デバイスの不正使用を防止できます。

関連情報

- 「Web Configの概要」23ページ
- 「EpsonNet Config」61ページ
- 「管理者パスワードの設定」36ページ
- 「外部インターフェイスを無効にする」39ページ

管理者パスワードの設定

管理者パスワードを設定すると、プリンターのユーザーがシステム管理に関する設定を変更することを防ぎます。管理者パスワードはWeb Config、操作パネル、ソフトウェア（Epson Device Admin）のいずれからも変更ができます。ツールの操作方法についてはそれぞれのマニュアルをご覧ください。

!重要 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、管理者パスワードの初期値は製造番号（シリアルナンバー）です。プリンター本体のラベルに記載されている製造番号（シリアルナンバー）をご確認ください。
不正アクセスを防止するため、速やかに初期パスワードを変更することをお勧めします。

関連情報

- 「操作パネルから管理者パスワードを変更する」37ページ

➡ 「Web Configから管理者パスワードを変更する」37ページ
➡ 「Epson Device Admin」61ページ

操作パネルから管理者パスワードを変更する

プリンターの操作パネルから管理者パスワードを変更します。

1. プリンターの操作パネルで［設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

2. ［セキュリティー設定］ - ［管理者設定］の順に選択します。

3. ［管理者パスワード］ - ［変更］の順に選択します。

4. 現在のパスワードを入力します。

5. 新しいパスワードを入力します。

6. パスワードを再入力します。

参考 ［管理者パスワード］画面で［購入時の設定に戻す］を選択し、管理者パスワードを入力すると、管理者パスワードを初期パスワードに戻すことができます。

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［本体セキュリティー］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」24ページ
➡ 「Web Configで管理者としてログオンする」41ページ

パネル操作を制限する

管理者パスワードを設定してパネルの管理者ロックを有効にすると、プリンターのシステム設定に関する項目をユーザーが変更できないようにロックできます。
ロックされた機能を操作するには管理者パスワードが必要です。

管理者ロックを有効にする

パスワード設定したプリンターの管理者ロック を有効にします。

操作パネルを使って管理者ロックを有効にする

1. プリンターの操作パネルで［設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

2. ［セキュリティー設定］ - ［管理者設定］の順に選択します。

3. ［管理者ロック］ - ［オン］の順に選択します。

4. 確認画面でOKボタンを押します。

5. ［設定］ - ［ネットワーク設定］を選択し、パスワード入力を求められるか確認してください。

Web Configを使って管理者ロックを有効にする

1. Web Configで［ログオン］をクリックします。

2. ユーザー名（設定している場合）とパスワードを入力して［確認］をクリックします。

3. ［デバイス管理］タブ - ［パネル］を選択します。

4. ［パネルロック］から［オン］を選択します。

5. ［設定］をクリックします。

6. プリンターの操作パネルで［設定］ - ［ネットワーク設定］を選択し、パスワード入力を求められるか確認してください。

設定メニューの管理者ロック項目

管理者ロックによって操作パネルの［設定］メニュー内でパネルロックされる項目一覧です。

設定 メニュー		パネルロック
プリンター状態		×
用紙設定		×
プリンターのお手入れ		×
プリンターの基本設定		×
	給紙装置設定	×
	音の設定	×
	自動電源オフ設定	○
	日付/時刻設定	○
	言語選択/Language	○
	キーボード	×
	スリープ移行時間設定	○
	コンピューターのUSB接続	○
	長さ単位	×
	ハガキセット間違い通知	×
ネットワーク設定		○
Epson Connect設定		○
ネットワークステータスシートの印刷		×
印刷ページ数の確認		×
診断レポート		×
セキュリティー設定		○
初期設定に戻す		○

○＝ロックされます。
×＝ロックされません。

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： ［設定］ - ［プリンターの基本設定］ - ［コンピューターのUSB接続］

1. Web Configで［本体セキュリティー］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」24ページ
➡ 「Web Configで管理者としてログオンする」41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。
操作パネルでロックされている項目を操作するには、パスワードを入力します。

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。

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
  ［設定］ - ［プリンター状態］ - ［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。
- ネットワーク情報
  ［設定］ - ［ネットワーク設定］ - ［ステータスシート印刷］
  ［設定］ - ［ネットワークステータスシートの印刷］
  ネットワークステータスシートを印刷して、ネットワーク接続状態などの確認ができます。

- ネットワーク接続診断レポート
  ［設定］ - ［ネットワーク設定］ - ［接続診断］
  ［設定］ - ［診断レポート］ - ［ネットワーク］
  プリンターのネットワーク接続状況を診断し、レポートの印刷ができます。

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
  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。
- 使用状況
  初回印刷日、印刷面数、言語別印刷数などを確認できます。
- 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。

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」29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。

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」24ページ
- ➡ 「Web Configで管理者としてログオンする」41ページ
- ➡ 「メールサーバーを設定する」29ページ

メール通知の設定項目

項目	設定値と説明
インク残量限界値以下	インク残量が限界値以下になった場合に通知します。
インク残量少	インク残量が限界値に近づいた場合に通知します。
メンテナンスボックス空き容量なし	メンテナンスボックスがいっぱいになった場合に通知します。
メンテナンスボックス空き容量少	メンテナンスボックスがいっぱいになる手前で通知します。
管理者パスワード変更	管理者パスワードが変更された場合に通知します。
用紙なし	印刷指定の給紙装置で用紙なしエラーが発生した場合に通知します。
用紙残量少	印刷指定の給紙装置で用紙がなくなる手前で通知します。
印刷停止（※）	紙詰まり、用紙サイズ/用紙種類の不一致などで、印刷が停止したときに通知します。
プリンターエラー	プリンターエラーが発生した場合に通知します。
無線LAN故障	無線LANインターフェイスにエラーが発生した場合に通知します。
印刷ジョブ終了（※2）	プルダウンメニューで設定した数の印刷ジョブが終了するたびにメールを送信します。

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。

Web Configでファームウェアをアップデートする

プリンターがインターネットに接続できると、Web Configからファームウェアをアップデートできます。

1. Web Configで［デバイス管理］タブ - ［ファームウェアアップデート］を選択します。
2. ［確認開始］をクリックします。

   ファームウェアの確認が始まり、更新されたファームウェアがあるとファームの情報が表示されます。
3. ［開始］をクリックし、画面の案内に従って操作します。

参考 Epson Device Adminを使ってもファームウェアをアップデートできます。デバイス一覧でファームウェアの情報が確認ができます。この方法は、複数のデバイスのファームウェアをアップデートするのに便利です。詳細はEpson Device Adminのマニュアルやヘルプをご覧ください。

関連情報

- 「Web Configの起動」24ページ
- 「Web Configで管理者としてログオンする」41ページ
- 「Epson Device Admin」61ページ

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

コンピューター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にアクセスして、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ーと、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」24ページ
- 「Web Configで管理者としてログオンする」41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。

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ドライバーの画面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。
- ネットワーク接続診断レポート
  ネットワークとプリンターの状況を診断して、結果がレポートされます。
  プリンター側から判別できるエラーを見つけることができます。
- 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」42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。

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。詳しくはマニュアルをご覧ください。 エラーコード：XXXXX	• **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ときは、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。	• **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。	• **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ー］ - ［ルート証明書更新］
Recovery Mode	• **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。

ネットワーク接続診断レポートを印刷する

プリンターと無線LANルーター（アクセスポイント）の接続状態を確認するために、ネットワーク接続診断レポートを印刷します。

1. 印刷用紙をセットします。
2. ホーム画面で［設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。
3. ［診断レポート］ - ［ネットワーク］の順に選択します。

   診断が始まります。
4. OKボタンを押します。

5. 画面の指示に従って、ネットワーク接続診断レポートを印刷します。

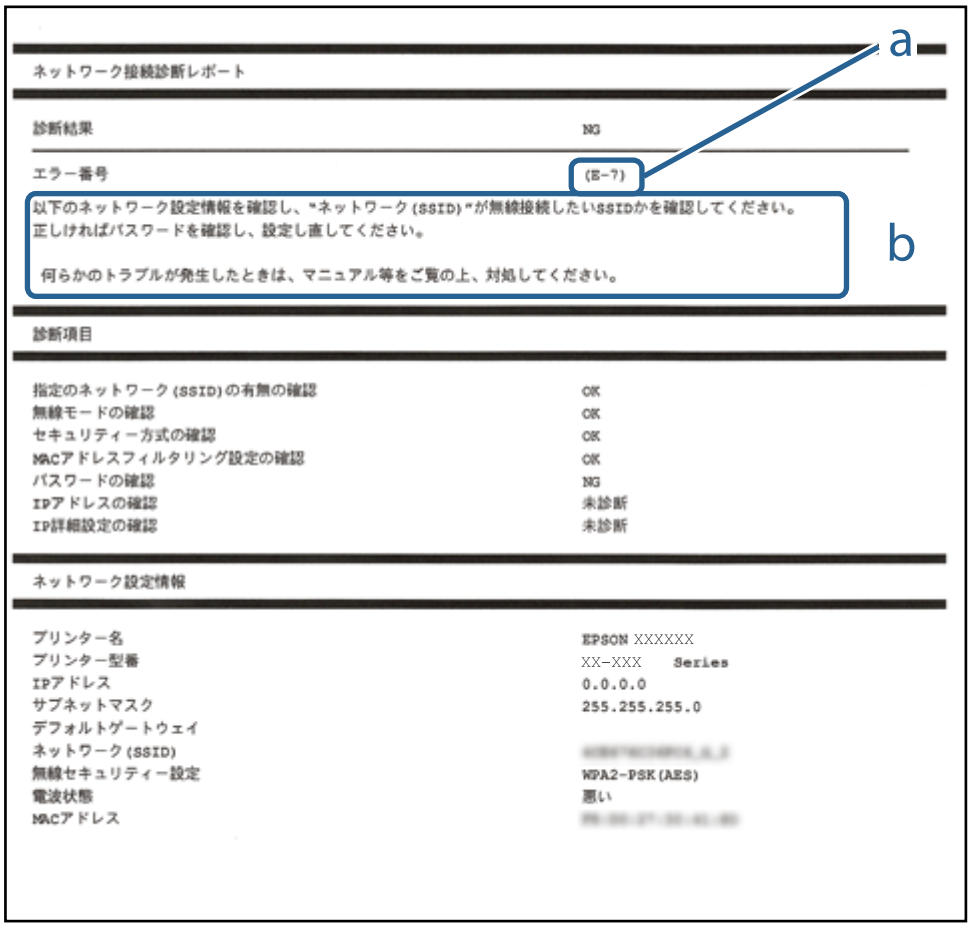
エラーがある場合はネットワーク接続診断レポートの内容を確認して対処してください。

関連情報

➡ 「ネットワーク接続診断レポートの見方と対処方法」49ページ

ネットワーク接続診断レポートの見方と対処方法

ネットワーク接続診断レポートのメッセージとエラー番号を確認して対処してください。



a. エラー番号
b. ネットワーク環境に関するメッセージ

E-1

対処方法：

- LAN ケーブルが、プリンターやハブなどのネットワーク機器にしっかり差し込まれているか確認してください。
- ハブなどのネットワーク機器の電源が入っているか確認してください。

- プリンターを無線LAN（Wi-Fi）で使用したい場合は、プリンターの無線LANが有効になっていないため、無線LAN接続設定をやり直してください。

E-2, E-3, E-7

対処方法：

- 無線LANルーターの電源が入っているか確認してください。
- コンピューターやその他の機器が無線LANルーターと正常に通信できているか確認してください。
- 無線LANルーターの電源を切ります。10秒くらい待ってから、電源を入れてください。
- プリンターと無線LANルーターは近くに置き、間にある障害物は取り除いてください。
- SSIDを直接入力したときは、入力したSSIDが正しいかを確認してください。SSIDはネットワーク接続診断レポートの［ネットワーク設定情報］で確認できます。
- 1つの無線LANルーターに複数のSSIDが存在する場合、表示されたSSIDから選択してください。SSIDが非対応の周波数を使用していると、SSIDは表示されません。
- プッシュボタンを使った自動設定をする場合は、お使いの無線LANルーターがWPSに対応しているか確認してください。WPSに対応していないときは、プッシュボタンを使った自動設定はできません。
- SSIDにASCII文字（半角英数字、記号）以外の文字列が使われていないか確認してください。プリンターは、ASCII文字以外の文字列が含まれたSSIDは表示できません。
- 無線LANルーターに接続する場合は、SSIDとパスワードを事前に確認してください。無線LANルーターをメーカー設定値のまま使用している場合は、ラベルなどに書かれているSSIDとパスワードが設定されています。SSIDとパスワードがわからない場合は無線LANルーターを設定した人に確認するか、無線LANルーターのマニュアルをご覧ください。
- スマートデバイスなどのテザリング機能で生成したSSIDに接続したい場合は、スマートデバイスのマニュアルなどでSSIDとパスワードを確認してください。
- 無線LAN（Wi-Fi）で突然接続できなくなった場合は、以下を確認してください。どれかに当てはまる場合は、以下のウェブサイトでインストーラーをダウンロードして、ネットワーク設定をやり直してください。
  http://epson.sn-［セットアップ］
  - お使いのネットワーク環境に、新たに別のスマートデバイスからプッシュボタン自動設定（AOSS／WPS）で設定したか
  - この無線LAN（Wi-Fi）ネットワークは、プッシュボタン自動設定以外の方法で設定されたか
  - 株式会社バッファロー製の無線LANルーターで、プッシュボタンで設定（AOSS）できるタイプを使っているか

E-5

対処方法：

無線LANルーターが以下のいずれかのセキュリティー方式になっているかを確認してください。なっていない場合は、以下のセキュリティー方式を使用するよう無線LANルーターの設定を変更し、プリンターのネットワーク設定をし直してください。

- WEP-64 bit (40 bit)
- WEP-128 bit (104 bit)
- WPA PSK (TKIP/AES)*

- WPA2 PSK (TKIP/AES)*
- WPA (TKIP/AES)
- WPA2 (TKIP/AES)
- WPA3-SAE (AES)
- WPA2/WPA3-Enterprise

* WPA PSKはWPA Personal、WPA2 PSKはWPA2 Personalとも呼ばれます。

E-6

対処方法：

- MACアドレスフィルタリングが無効になっていることを確認してください。有効の場合は、プリンターのMACアドレスを登録して、フィルタリングされないようにしてください。詳しくは無線LANルーターのマニュアルをご覧ください。プリンターのMACアドレスはネットワーク接続診断レポートの［ネットワーク設定情報］で確認できます。
- 無線LANルーターのWEPセキュリティー方式でShared認証が有効になっている場合は、認証キーおよびインデックスが正しいことを確認してください。
- 無線LANルーターに設定されている同時接続可能な機器数が、接続するネットワーク機器の台数より少ない場合は、接続できる数を増やしてください。設定方法は、無線LANルーターのマニュアルをご覧ください。

E-8

対処方法：

- プリンターの TCP/IP 設定を［自動］にしているときは、無線LANルーターのDHCPを有効にしてください。
- プリンターの TCP/IP 設定を［手動］にしているときは、手動で設定したIPアドレスが有効範囲外（0.0.0.0 など）のため、無効になっています。有効なIPアドレスをプリンターの操作パネルから設定してください。

E-9

対処方法：

以下を確認してください。

- プリンターを利用する機器の電源が入っているか
- プリンターを利用する機器から、インターネットへのアクセスや同じネットワーク上の、他のコンピューター、ネットワーク機器にアクセスできるか

上記を確認してもプリンターと他のネットワーク機器が接続できない場合は、無線LANルーターの電源を切ります。10秒くらい待ってから、電源を入れてください。続いて、以下のウェブサイトでインストーラーをダウンロードして、ネットワーク設定をやり直してください。
http://epson.sn-［セットアップ］

E-10

対処方法：

以下を確認してください。

- ネットワーク上の他の機器の電源が入っているか
- プリンターのTCP/IP設定を［手動］にしているときは、ネットワークアドレス（IPアドレス、サブネットマスク、デフォルトゲートウェイ）が正しいか

ネットワークアドレスが間違っている場合は、設定し直してください。IPアドレス、サブネットマスク、デフォルトゲートウェイはネットワーク接続診断レポートの［ネットワーク設定情報］で確認できます。
DHCPを有効にしているときは、プリンターのTCP/IP設定を［自動］にしてください。IPアドレスを手動で設定したい場合は、ネットワーク接続診断レポートの［ネットワーク設定情報］でプリンターのIPアドレスを確認し、プリンターのネットワーク設定画面で手動を選択して、設定してください。サブネットマスクは「255.255.255.0」に設定してください。
それでもプリンターと他のネットワーク機器が接続できない場合は、無線LANルーターの電源を切ります。10秒くらい待ってから、電源を入れてください。

E-11

対処方法：

以下を確認してください。

- プリンターのTCP/IP設定を手動設定にしたときは、プリンターに設定されたデフォルトゲートウェイのアドレスが正しいか
- デフォルトゲートウェイに指定した機器の電源が入っているか

デフォルトゲートウェイのアドレスを正しく設定してください。プリンターのデフォルトゲートウェイのアドレスはネットワーク接続診断レポートの［ネットワーク設定情報］で確認できます。

E-12

対処方法：

以下を確認してください。

- ネットワーク上の他の機器の電源が入っているか
- 手動で設定したプリンターのネットワークアドレス（IPアドレス、サブネットマスク、デフォルトゲートウェイ）が正しいか
- 他の機器のネットワークアドレス（サブネットマスク、デフォルトゲートウェイ）が同一になっているか
- 他の機器のIPアドレスと重複していないか

上記を確認してもプリンターと他のネットワーク機器が接続できない場合は、以下の対処を試してみてください。

- 無線LANルーターの電源を切ります。10秒くらい待ってから、電源を入れます。
- インストーラーを使って、ネットワーク設定をやり直してください。インストーラーは以下のウェブサイトから起動できます。
  http://epson.sn-［セットアップ］

- セキュリティータイプ「WEP」は、無線LANルーターに複数のセキュリティーキーを登録できます。複数のキーが登録されているときは、最初（1番目）のインデックスのセキュリティーキーがプリンターに設定されているかを確認してください。

E-13

対処方法：

以下を確認してください。

- ネットワーク機器（無線LANルーター、ハブ、ルーターなど）の電源が入っているか
- プリンター以外のネットワーク機器が手動でTCP/IP設定されていないか。（他のネットワーク機器のTCP/IP設定が手動で、プリンターのTCP/IP設定のみ自動設定になっていると、プリンターだけが異なるネットワークになってしまう可能性があります。）

問題がないときは、以下をお試しください。

- 無線LANルーターの電源を切ります。10秒くらい待ってから、電源を入れます。
- プリンターと同じネットワーク上のコンピューターで、インストーラーを使ってネットワーク設定をし直してください。インストーラーは以下のウェブサイトから起動できます。
  http://epson.sn-［セットアップ］
- セキュリティータイプ「WEP」は、無線LANルーターに複数のセキュリティーキーを登録できます。複数のキーが登録されているときは、最初（1番目）のインデックスのセキュリティーキーがプリンターに設定されているかを確認してください。

ネットワーク環境に関するメッセージ

メッセージ	対処方法
*無線環境の改善が必要です。 無線LANルーターの電源を入れ直してください。 それでも解消しないときは無線LANルーターのマニュアルをご覧ください。	プリンターを無線LANルーターの近くに移動し、機器間にある障害物を取り除いてから無線LANルーターの電源を入れ直します。10秒くらい待ってから、電源を入れてください。それでも接続できない場合は、無線LANルーターのマニュアルをご覧ください。
*無線接続が可能な機器数の上限に達しています。 機器を追加したいときは、他の機器の接続を解除してください。	Wi-Fi Direct（シンプルAP）接続で同時接続できる無線機器が最大限接続されています。他のコンピューターやスマートデバイスを追加するには、プリンターを使用していないコンピューターやスマートデバイスの接続を解除するか他のネットワークに接続させてから追加してください。 同時接続できる無線機器の台数と接続されている台数は、プリンターの操作パネルまたはネットワークステータスシートで確認できます。
周囲にWi-Fi Directと重複するSSIDが存在します。 スマートデバイス(無線機器)をプリンターに接続できないときは、 Wi-Fi DirectのSSIDを変更してください。	プリンターの操作パネルからWi-Fi Direct設定の画面を表示し、設定を変更するメニューから接続名を変更してください。接続名はDIRECT-XX-の後に続く文字列を変更できます。半角22文字以内で入力します。

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［設定］を選択します。

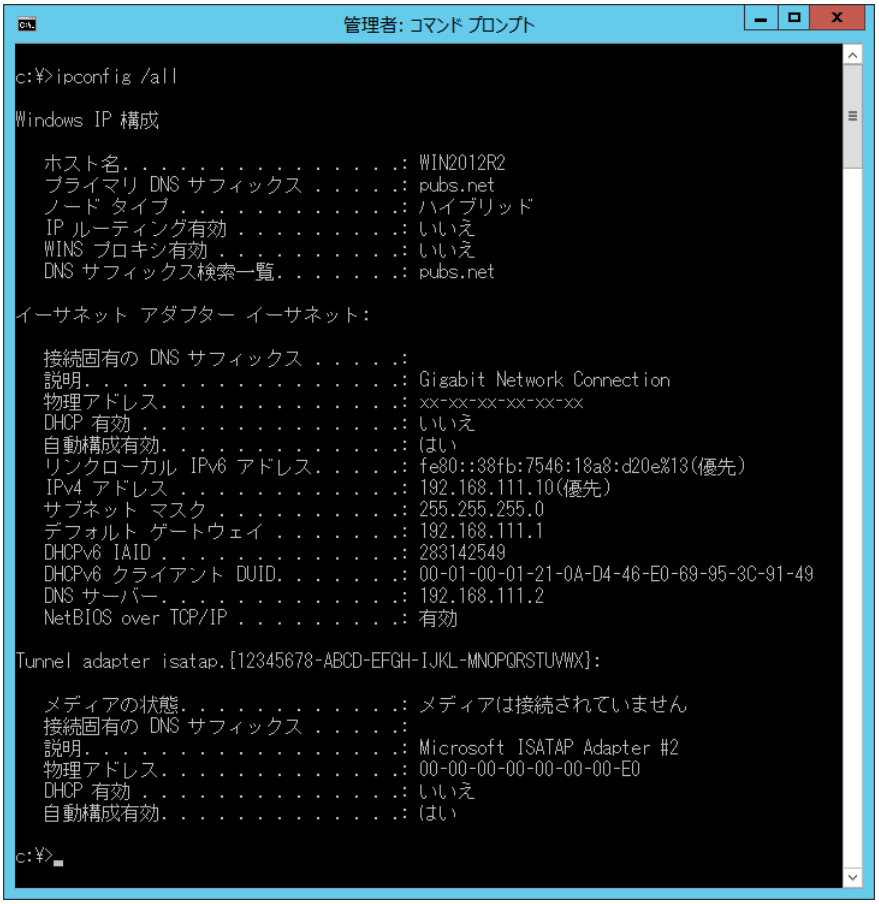
   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。
3. ［ネットワーク設定］ - ［ステータスシート印刷］の順に選択します。
4. OKボタンを押します。

   ネットワークステータスシートが印刷されます。

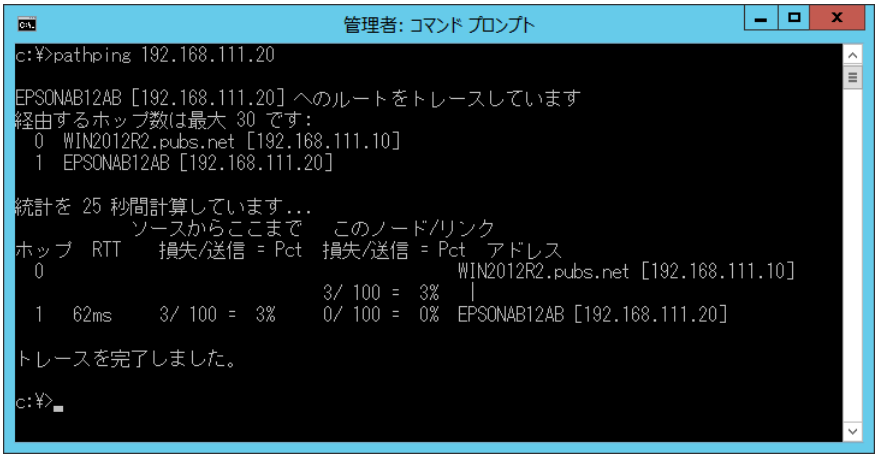
コンピューターのネットワークを確認する - Windows

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イ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：



- 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



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」31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

Web Configから無線LANを無効にする

Web Configから無線LAN（Wi-Fi）を無効にします。無線LAN（Wi-Fi）接続時に無線LANを無効にすると、無線接続が切断されます。

1. Web Configで［ネットワーク］タブ - ［無線LAN］の順に選択して、［無効にする］を選択します。
2. メッセージを確認して、［設定］を選択します。

Web ConfigからWi-Fi Direct（シンプルAP）を無効にする

Web ConfigからWi-Fi Direct（シンプルAP）を無効にします。

1. Web Configで［ネットワーク］タブ - ［Wi-Fi Direct］を選択します。
2. ［Wi-Fi Direct］を［無効］にします。
3. ［次へ］をクリックします。
4. メッセージを確認して、［設定］を選択します。

操作パネルから無線LANを無効にする

無線LAN（Wi-Fi）接続時に無線LANを無効にすると、無線接続が切断されます。

1. ホーム画面で［無線LAN設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。
2. ［無線LANルーターとつなぐ(推奨)］を選択します。
3. OKボタンを押して、次の画面に進みます。
4. ［その他］を選択します。
5. ［無線LAN を無効にする］を選択します。
6. メッセージを確認して、OKボタンを押します。

操作パネルからWi-Fi Direct（シンプルAP）接続を無効にする

参考 Wi-Fi Direct（シンプルAP）接続で複数のコンピューターやスマートデバイスがプリンターと接続されていた場合、Wi-Fi Direct（シンプルAP）接続を無効にすると、全ての接続が切断されます。特定の機器だけを切断したいときは、スマートデバイス側から接続を切断してください。

1. ホーム画面で［無線LAN設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

2. ［スマートデバイスと直接つなぐ］を選択します。

3. OKボタンを押して、次の画面に進みます。

4. OKボタンを押して、次の画面に進みます。

5. ▽ボタンを押して、設定変更に進みます。

6. ［無効設定］を選択します。

7. メッセージを確認して、OKボタンを押します。

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［設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

2. ［初期設定に戻す］ - ［ネットワーク設定］の順に選択します。

3. メッセージを確認して、OKボタンを押します。

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ブラウザーが 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ーで起動できます。ブラウザー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「セキュリティー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。

- 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」24ページ
➡ 「IPアドレスを設定する」19ページ

プリンター共有時のトラブル

共有サーバーの動作が重い

共有プリンターの動作が重いときは以下の手順で対処してください。

1. プリントサーバーのコンピューターで［コントロールパネル］ - ［デバイスとプリンター］を選択します。
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］ - ［全般］タブを選択し、［基本設定］を選択します。
3. プリンタードライバーの［ユーティリティー］タブで［通知の設定］を選択します。
4. ［共有プリンターをモニターさせる］にチェックを付けます。

プリントサーバーのプリンター設定がクライアントコンピューターに反映されない

以下の手順でクライアントコンピューターのドライバーを再インストールしてください。

1. プリントサーバーのコンピューターで［コントロールパネル］ - ［デバイスとプリンター］を選択します。
2. 共有するプリンタアイコンを右クリックし、［プリンターのプロパティ］ - ［詳細設定］タブを選択します。
3. ［標準の設定］ を選択し、プリンターの設定を行って［OK］をクリックします。
4. クライアントコンピューターから共有プリンターのプリンタードライバーを削除します。
5. クライアントコンピューターにプリンタードライバーを再インストールします。

参考
- クライアントコンピューターでプリンター設定を変更すると、プリントサーバーのプリンター設定（デフォルト設定など）がクライアントコンピューターに反映されなくなります。
- ［お気に入り］・［ユーザー定義サイズ］・［カスタムメディア設定］・［メニューの整理］など、一部の設定は、クライアントコンピューターに反映されません。これらの設定は、プリントサーバーのプリンタードライバーから設定ファイル（お気に入り設定など）を書き出し、クライアントコンピューターで読み込むことで反映できます。

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

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 Configの起動 - Mac OS

［移動］－［アプリケーション］－［Epson Software］－［EpsonNet］－［EpsonNet Config SE］から［EpsonNet Config］を選択します。

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。

EpsonNet SetupManager

ネットワークプリンターのドライバーやEPSONプリンターウィンドウ！3のインストールから印刷ポートの設定までを自動で実行するパッケージを作成するソフトウェアです。環境の異なるドライバーのパッケージを一括して作成できるため、ドライバーの配布やインストール、設定など管理者が行う環境構築作業を大幅に軽減できます。
詳細はエプソンのウェブサイトをご覧ください。

操作パネルを使って無線LANに接続する（WPS）

プリンターの操作パネルでWPS機能を使った無線LAN接続ができます。

関連情報

- 「プッシュボタンで自動設定する（AOSS/WPS）」63ページ
- 「PINコードで設定する（WPS）」64ページ

プッシュボタンで自動設定する（AOSS/WPS）

無線LANルーター（アクセスポイント）のプッシュボタンで無線LAN（Wi-Fi）を自動設定する方法です。以下の条件に当てはまる場合は、この方法で設定できます。

- 無線LANルーター（アクセスポイント）がAOSSやWPS（Wi-Fi Protected Setup）に対応している
- 既存の無線LAN（Wi-Fi）をプッシュボタンで設定している

1. ホーム画面で［無線LAN設定］を選択します。

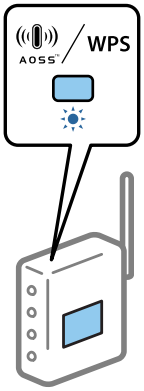
   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

2. ［無線LANルーターとつなぐ(推奨)］を選択します。

3. OKボタンを押して、次の画面に進みます。

4. ［プッシュボタンで設定(AOSS/WPS)］を選択します。

5. 無線LANルーター（アクセスポイント）のプッシュボタンをランプが点滅するまで押します。



プッシュボタンの位置がわからない、またはボタンが見当たらない場合は、無線LANルーター（アクセスポイント）のマニュアルをご覧ください。

6. プリンターの操作パネルの OKボタンを押します。この後は、画面の指示に従って操作します。

参考 接続に失敗した場合は無線LANルーター（アクセスポイント）を再起動し、無線LANルーター（アクセスポイント）とプリンターを近づけてから再度設定してください。それでも解決しないときは、ネットワーク接続診断レポートを印刷して対処方法を確認してください。

PINコードで設定する（WPS）

PINコードを使って無線LANルーター（アクセスポイント）に接続する方法です。無線LANルーター（アクセスポイント）がWPS（Wi-Fi Protected Setup）に対応している場合は、この方法で設定できます。PINコードを無線LANルーター（アクセスポイント）に入力するときに、コンピューターを使います。

1. ホーム画面で［無線LAN設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

2. ［無線LANルーターとつなぐ(推奨)］を選択します。

3. OKボタンを押して、次の画面に進みます。

4. ［その他］を選択します。

5. ［PINコード自動設定(WPS)］を選択します。

6. プリンターに表示されているPINコード（8桁の数字）を、2分以内にコンピューターから無線LANルーター（アクセスポイント）に入力します。

   参考 PINコードの入力方法は、無線LANルーター（アクセスポイント）のマニュアルをご覧ください。

7. プリンターの操作パネルでOKボタンを押します。

   設定完了のメッセージが表示されたら終了です。

   参考 接続に失敗した場合は無線LANルーター（アクセスポイント）を再起動し、無線LANルーター（アクセスポイント）とプリンターを近づけてから再度設定してください。それでも解決しないときは、ネットワーク接続診断レポートを印刷して対処方法を確認してください。

Wi-Fi Direct（シンプルAP）接続を使う

Wi-Fi Direct（シンプルAP）接続は、プリンターとデバイスを直接Wi-Fiで接続します。
プリンターが接続されているネットワークを経由しないので、ログオン権限のないネットワークに接続されたプリンターを一時的に使用するような場合にも使用できます。
Wi-Fi Direct（シンプルAP）接続でプリンターを接続する方法の詳細は『ユーザーズガイド』をご覧ください。

Wi-Fi Direct（シンプルAP）の設定を変更する

Wi-Fi Direct（シンプルAP）が有効なとき、接続名やパスワードなどのWi-Fi Direct設定を変更できます。

1. ホーム画面で［無線LAN設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

2. ［スマートデバイスと直接つなぐ］を選択します。

3. OKボタンを押して、次の画面に進みます。

4. OKボタンを押して、次の画面に進みます。

5. ▽ボタンを押して、設定変更に進みます。

6. 変更したいメニューを選択します。

   以下のメニューが選択できます。

   - ［接続名を変更する］
     プリンターに接続するWi-Fi Direct（シンプルAP）の接続名（SSID）を任意の値に変更します。接続名（SSID）に設定できるのは、操作パネルのソフトキーボードに表示されたASCII文字です。
     接続名（SSID）を変更すると接続しているデバイスは全て切断されます。接続名を変更した場合は、接続する機器から新しい接続名（SSID）で接続し直してください。
   - ［パスワードを変更する］
     プリンターに接続するWi-Fi Direct（シンプルAP）のパスワードを変更します。パスワードに設定できるのは、操作パネルのソフトキーボードに表示されたASCII文字です。
     パスワードを変更すると接続しているデバイスは全て切断されます。パスワードを変更した場合は、接続する機器から新しいパスワードで接続し直してください。
   - ［周波数帯を変更する］
     プリンターに接続するWi-Fi Direct（シンプルAP）の周波数帯を変更します。2.4GHzまたは5GHzに設定できます。
     周波数帯を変更すると接続しているデバイスは全て切断されます。再度接続してください。
     周波数帯を5GHzに設定した場合、5GHz非対応のデバイスからは再接続できなくなります。
   - ［無効設定］
     Wi-Fi Direct（シンプルAP）を無効にします。無効にすると接続しているデバイスは全て切断されます。
   - ［購入時の設定に戻す］
     Wi-Fi Direct（シンプルAP）設定の全てを購入時の設定に戻します。
     また、プリンターが保持しているスマートデバイスのWi-Fi Direct機能を使った接続情報の登録を削除します。

7. 画面の案内に従って操作します。

参考 以下の設定項目は、Web Configの［ネットワーク］ タブ - ［Wi-Fi Direct］からも設定できます。

- Wi-Fi Direct（シンプルAP）を有効または無効にする
- ネットワーク名（SSID）を変更する
- パスワードを変更する
- 周波数帯を変更する
- Wi-Fi Direct（シンプルAP）の設定を初期の状態に戻す

接続方法を変更する

既存のネットワーク接続方法を変更します。ネットワークが正常に動いている状態で変更してください。
IPアドレス取得を手動設定にしている場合、接続変更するネットワークで同じIPアドレスが使えるか、ネットワーク管理者に確認してから操作を始めてください。

参考 無線LANを有効にすると、有線LANは無効になります。

関連情報

- 「有線LANから無線LANへの接続変更」66ページ
- 「無線LANから有線LANへの接続変更」67ページ

有線LANから無線LANへの接続変更

操作パネルで無線LAN接続に変更する

プリンターの操作パネルで有線LAN接続から無線LAN接続に変更します。変更方法は操作パネルを使った無線LAN接続設定と同じです。このマニュアル内の無線LAN接続設定の説明をご覧ください。

関連情報

- 「無線LAN（Wi-Fi）に接続する」21ページ

Web Configで無線LAN接続に変更する

Web Configを使って有線LANから無線LANに接続変更します。

1. Web Configで［ネットワーク］タブ - ［無線LAN］を選択します。
2. ［設定］をクリックします。
3. 表示されたSSIDの一覧から接続したいネットワーク（SSID）を選択して、パスワードを入力します。

   アクセスポイントの設定によってはSSID が表示されないことがあります。その場合は［SSID入力］を選択して、接続するSSIDを直接入力してください。
4. ［次へ］をクリックします。
5. 表示された内容を確認して［設定］をクリックします。
6. プリンターに接続されているLANケーブルを抜きます。

参考 Epson Device Adminを使用して接続変更することもできます。詳細はEpson Device Adminのマニュアルやヘルプをご覧ください。

関連情報

- 「Web Configの起動」24ページ
- 「Web Configで管理者としてログオンする」41ページ
- 「Epson Device Admin」61ページ

無線LANから有線LANへの接続変更

操作パネルで有線LAN接続に変更する

無線LAN（Wi-Fi）接続時に操作パネルから有線LAN接続に変更するには以下の手順で操作します。

1. プリンターとルーターをLANケーブルで接続します。
2. プリンターの操作パネルで無線LAN（Wi-Fi）を無効にします。

関連情報

- 「有線LANに接続する」20ページ
- 「操作パネルから無線LANを無効にする」57ページ

Web Configで有線LAN接続に変更する

Web Configを使って無線LAN接続から有線LAN接続に変更します。

1. Web Configで［ネットワーク］タブ - ［無線LAN］を選択します。
2. ［無効にする］をクリックします。
3. メッセージを確認して、［OK］を選択します。
4. 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。

参考 Epson Device Adminを使用して接続変更することもできます。詳細はEpson Device Adminのマニュアルやヘルプをご覧ください。

関連情報

- 「Web Configの起動」24ページ
- 「Web Configで管理者としてログオンする」41ページ
- 「Epson Device Admin」61ページ

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。

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
	Epson Connectを利用した機能の利用	Epson Connectサーバー	HTTPS	443
			XMPP	5222
	WSDの制御	クライアントコンピューター	WSD（TCP）	5357
クライアントコンピューター	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
	AirPrint（IPP/IPPS印刷）のデータの転送	プリンター	IPP/IPPS（TCP）	631
	WSDのプリンター探索	プリンター	WS-Discovery（UDP）	3702

エンタープライズセキュリティー設定編

この章では、高度なセキュリティー機能を説明しています。

セキュリティー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ー技術を搭載しています。
お客さまの情報環境での条件に合わせて、必要なセキュリティー設定をしてください。

機能名	どんな機能か	何を設定するのか	何を防止できるのか
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Epson Connect、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ー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	無線LAN や有線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

- 「プリンターとのSSL/TLS通信」71ページ
- 「利用するプロトコルを制御する」76ページ
- 「IPsec/IPフィルタリングで暗号化通信する」80ページ
- 「IEEE802.1X環境にプリンターを接続する」91ページ

セキュリティー機能の設定

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ー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、ブラウザーでIPアドレスを入力してWeb Configを起動して設定できます。セキュリティー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。

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ーが、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。
  セキュリティー設定をする際に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。
  ブラウザー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ー警告が出ることがあります。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」71ページ
- 「CA署名証明書を削除する」74ページ
- 「自己署名証明書を更新する」76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ー］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。

   参考 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ー］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	CSR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。

項目	設定値と説明
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。

関連情報

➡ 「CA署名証明書を取得する」71ページ

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ー］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ー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」24ページ
- 「Web Configで管理者としてログオンする」41ページ
- 「CA署名証明書のインポート設定項目」74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。
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」73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ー］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」24ページ
- 「Web Configで管理者としてログオンする」41ページ
- 「CSRの設定項目」72ページ
- 「CA署名証明書をインポートする」73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ー］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ー］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」24ページ
- 「Web Configで管理者としてログオンする」41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ー］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ー］ 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」24ページ
- 「Web Configで管理者としてログオンする」41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ー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ー］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。
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。
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。

項目	設定値と説明
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

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。
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。

項目	設定値と説明
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

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。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。
URL（Wi-Fi Direct）	Wi-Fi Directで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。

SNMPv1/v2c設定

項目	設定値と説明
SNMPv1/v2cを有効にする	チェックを入れるとSNMPv1/v2cを有効にします。
アクセス権限	SNMPv1/v2c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。

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。
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ー通信ができます。

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ー］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」24ページ
- 「Web Configで管理者としてログオンする」41ページ
- 「基本ポリシーの設定項目」81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。

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。

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。

- ［セキュリティープロトコル］
  ［通信処理］で［IPsecの使用］を選択した場合、IPsecのセキュリティー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。 ［セキュリティープロトコル］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。 ［セキュリティープロトコル］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。 ［セキュリティープロトコル］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」80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ー］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」24ページ
➡ 「Web Configで管理者としてログオンする」41ページ
➡ 「個別ポリシーの設定項目」85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のセキュリティー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のセキュリティー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のセキュリティー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のセキュリティー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。

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。

［セキュリティープロトコル］
［通信処理］で［IPsecの使用］を選択した場合、IPsecのセキュリティー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。 ［セキュリティープロトコル］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。 ［セキュリティープロトコル］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。 ［セキュリティープロトコル］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」84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」89ページ
➡ 「個別ポリシーのサービス名一覧」89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

参考 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、エプソンのプリンター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
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	

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 (リモート)	TCP	任意	80	HTTP(S)クライアント（Epson Connectの通信、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ー］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」24ページ
- 「Web Configで管理者としてログオンする」41ページ
- 「CA署名証明書を取得する」71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ー］タブ - ［IEEE802.1X］ - ［基本］を選択します。
2. 各項目を設定します。

   無線LANで使う場合は［無線LAN設定］をクリックしてSSIDを選択するか、入力してください。

   参考 ここでの設定値は有線LANと無線LANで共通に使えます。
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」24ページ

➡ 「Web Configで管理者としてログオンする」41ページ
➡ 「IEEE802.1Xの設定項目」92ページ
➡ 「IEEE802.1Xを設定したのにつながらない」97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。	
IEEE802.1X (無線LAN)	IEEE802.1X（無線LAN）の接続状態が表示されます。	
接続方法	現在のネットワーク接続方法が表示されます。	
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0～128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0～128文字以内で入力します。Windowsサーバーをを 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	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」91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ー］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」24ページ
- ➡ 「Web Configで管理者としてログオンする」41ページ
- ➡ 「CA署名証明書の取得とインポート」71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。 • 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	CA証明書に以下の不備があるため、認証に失敗しました。 • 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	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。 • 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

セキュリティー設定の初期化

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、セキュリティー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ー機能を無効にする

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. ホーム画面で［設定］を選択します。

   項目を選択するには、▲▼◀▶ボタンで動かして、OKボタンを押してください。

2. ［ネットワーク設定］ - ［ネットワーク詳細設定］の順に選択します。

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. メッセージを確認して、OKボタンを押します。

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ー］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ー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」24ページ
➡ 「Web Configで管理者としてログオンする」41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ー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。コンピューターの設定を確認してください。

セキュリティーメソッド	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」80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ー］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ー］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」24ページ
- 「Web Configで管理者としてログオンする」41ページ
- 「IPsec/IPフィルタリングで暗号化通信する」80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」80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」80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無線LANと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」91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」73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」76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」71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。	**原因：** プリンターに日付や時刻が設定されていません。 **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。
パスワードが正しくありません。	**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。 **対処：** 正しいパスワードを入力してください。
不正なファイルです。	**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。 **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。
	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。 **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。
	原因： 証明書に含まれるチェーンが不正です。 **対処：** 証明書の詳細はCA局のWebサイトをご覧ください。
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。	**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。 **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。
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。	**原因：** 証明書の有効期限が切れています。 **対処：** • 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：** • 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ました。 **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」71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」74ページ
➡ 「CA署名証明書をインポートする」73ページ