

システム管理者ガイド

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の定義 7

準備編 9

スキャナーの設定と管理の流れ 9

ネットワーク環境の例 10

スキャナー接続設定例の紹介 10

ネットワーク接続の準備 11

接続情報の収集 11

スキャナー仕様 12

使用するポート番号 12

IPアドレスの割り当てタイプ 12

DNSサーバー、プロキシサーバーについて 12

ネットワーク接続設定方法の紹介 12

接続編 14

ネットワークに接続する 14

操作パネルでネットワークに接続する 14

インストーラーを使ってネットワークに接続する 18

機能設定編 20

設定に使うソフトウェア 20

Web Config（デバイスのウェブページ） 20

スキャン機能を使う 22

コンピューターからスキャンするには 22

操作パネルを使ってスキャンするには 24

システムの詳細を設定する 26

操作パネルでシステム設定する 26

Web Configでシステム設定する 27

基本のセキュリティ編 30

基本のセキュリティ機能の紹介 30

管理者パスワードの設定 30

操作パネルから管理者パスワードを設定する 31

Web Configから管理者パスワードを設定する 31

管理者パスワードでロックされる項目 32

利用するプロトコルを制御する 33

有効・無効が設定可能なプロトコル 34

プロトコルの設定項目 35

運用・管理編 38

デバイスの情報を確認する 38

デバイスの管理（Epson Device Admin） 38

イベント発生時にメール通知を受け取る 39

メール通知の概要 39

メール通知を設定する 39

メールサーバーを設定する 40

メールサーバーとの接続を確認する 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

Epson Firmware Updaterを使ってファームウェアをアップデートする 44

設定をバックアップする 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情報 47

サーバーやネットワーク機器のログの確認 47

設定の初期化 47

操作パネルからネットワーク設定を初期の状態に戻す 47

デバイスとコンピューターの接続を確認する 47

コンピューターとの接続をPingで確認する - Windows	47
コンピューターとの接続をPingで確認する - Mac OS	49
ソフトウェア使用時のトラブル	50
Web Configにアクセスできない	50
EpsonNet Configで製品名やIPアドレスが表 示されない	51

付録53

ネットワーク関連のソフトウェア	53
Epson Device Admin	53
EpsonNet Config	53
EpsonNet SetupManager	54
EpsonNet ConfigでIPアドレスを設定する	54
一括でIPアドレスを設定する	54
IPアドレスを個別に設定する	57
スキャナーが使用するポート	58
操作パネルの管理者用設定メニュー	59

エンタープライズセキュリティー設定 編61

セキュリティー設定と防止できる脅威	61
セキュリティー機能の設定	62
スキャナーとのSSL/TLS通信	62
使用できる電子証明書	62
CA署名証明書の取得とインポート	63
CA署名証明書を削除する	66
自己署名証明書を更新する	67
相手サーバー検証用CA証明書を設定する	68
IPsec/IPフィルタリングで暗号化通信する	70
IPsec/IPフィルタリングの概要	70
基本ポリシーを設定する	71
個別ポリシーを設定する	74
IPsec/IPフィルタリングの設定例	80
IPsec/IPフィルタリングで使用する証明書を 設定する	81
SNMPv3プロトコルを利用する	82
SNMPv3の概要	82
SNMPv3を設定する	82
IEEE802.1X環境にスキャナーを接続する	84
IEEE802.1Xを設定する	84
IEEE802.1Xで使用する証明書を設定する	86
トラブルを解決する	87
セキュリティー設定の初期化	87

セキュア環境への接続時のトラブル	88
電子証明書使用時のトラブル	90

商標

- Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- 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、Windows Vista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 OS、OS X、AirMac、Bonjour、Safariは米国およびその他の国で登録されたApple Inc.の商標です。AirPrint は、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

- プリンタードライバーとEpson Scan 2（スキャナードライバー）の画面はWindows 10またはOS X El Capitanでの画面を使用しています。表示内容は機種や状況によって異なります。
- イラストは一例です。機種によって多少異なりますが、操作方法はほぼ同じです。
- 画面の設定項目は、機種や設定状況によって異なります。

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」「Windows 8」「Windows 7」「Windows Vista」「Windows XP」「Windows Server 2016」「Windows Server 2012 R2」「Windows Server 2012」「Windows Server 2008 R2」「Windows Server 2008」「Windows Server 2003 R2」「Windows Server 2003」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
- Microsoft® Windows® 8 operating system 日本語版
- Microsoft® Windows® 7 operating system 日本語版
- Microsoft® Windows Vista® operating system 日本語版
- Microsoft® Windows® XP operating system 日本語版

- Microsoft® Windows® XP Professional x64 Edition operating system 日本語版
- Microsoft® Windows Server® 2016 operating system 日本語版
- Microsoft® Windows Server® 2012 R2 operating system 日本語版
- Microsoft® Windows Server® 2012 operating system 日本語版
- Microsoft® Windows Server® 2008 R2 operating system 日本語版
- Microsoft® Windows Server® 2008 operating system 日本語版
- Microsoft® Windows Server® 2003 R2 operating system 日本語版
- Microsoft® Windows Server® 2003 operating system 日本語版

Mac OS

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「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、お気づ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。

©Seiko Epson Corporation 2019.

はじめに

マニュアルの構成

本書はデバイス管理者向けに、ネットワーク接続や、デバイスをユーザーが使用できるまでの設定をする方法を記載しています。

ユーザーが操作する機能は『ユーザーズガイド』をご覧ください。

準備編

デバイス管理者が行うことやデバイスの設定、管理をするためのソフトウェアを説明しています。

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。デバイスが使用するポートやDNS、プロキシサーバーの情報など接続環境も説明しています。

機能設定編

デバイスの各機能を使用するための、始めに設定する項目の説明しています。

基本のセキュリティー編

管理者パスワードの設定やプロトコルの制御など、基本的なセキュリティー設定を説明しています。

運用・管理編

デバイス使用開始後の情報確認やメンテナンスの方法などを説明しています。

トラブルを解決する

設定の初期化とネットワークで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

CA証明書、SSL/TLS通信、IPsec/IPフィルタリングなど、デバイスのセキュリティーを強化するための設定方法を説明しています。

なお、ここで説明している機能はデバイスによっては対応していない場合があります。

マニュアルで使用する用語の定義

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する設置や、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場合があります。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。

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。

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。

ブッシュスキャン

デバイスのパネル操作を起点としたスキャンの総称です。

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。

SP*	!	"	#	\$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
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。

準備編

この章では、システム管理者の役割や設定前の準備などを紹介しています。

スキャナーの設定と管理の流れ

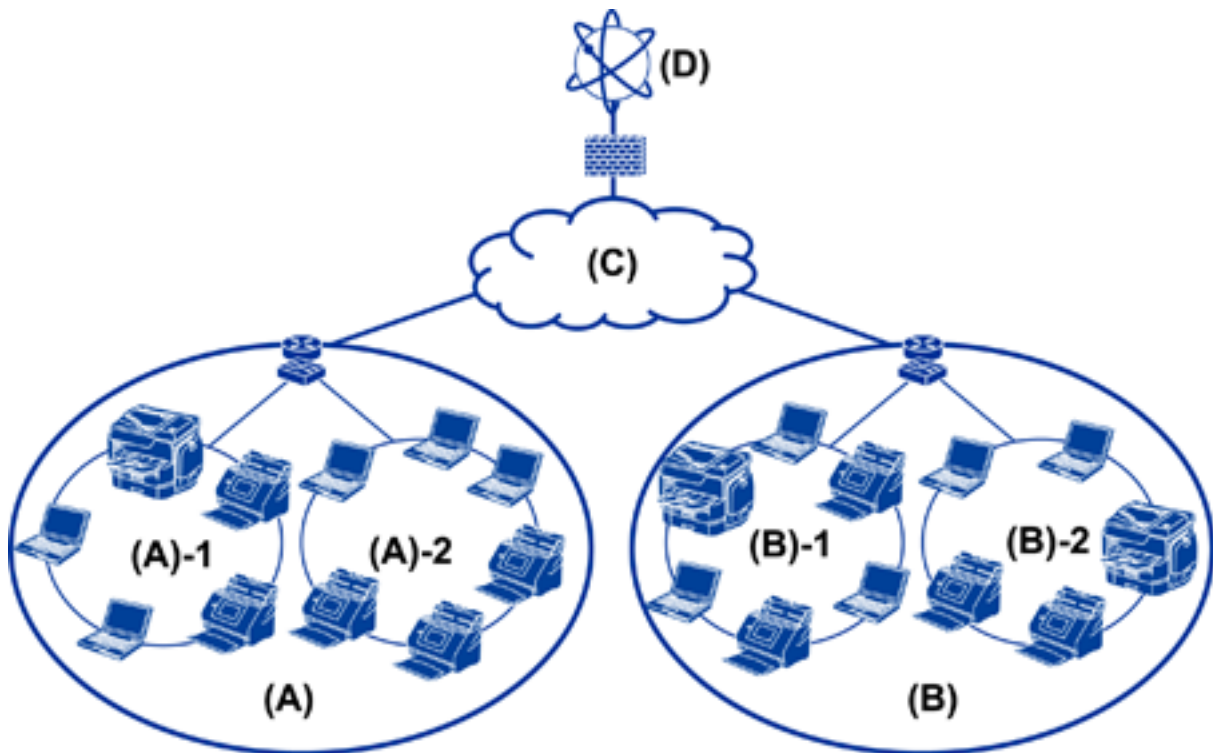
システム管理者はユーザーがスキャナーを使用できるように、ネットワークへの接続、初期設定、メンテナンスなどをします。

1. 準備する
 - 接続設定情報の収集
 - 接続形態の決定
2. 接続する
 - スキャナーの操作パネルを使ったネットワーク接続
3. 機能を設定する
 - スキャナードライバーの設定
 - その他の詳細設定
4. セキュリティー設定をする
 - 管理者設定
 - SSL/TLS
 - プロトコル制御
 - 高度なセキュリティー設定（オプション）
5. 運用、管理する
 - 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

- ➡ [「準備編」 9ページ](#)
- ➡ [「接続編」 14ページ](#)
- ➡ [「機能設定編」 20ページ](#)
- ➡ [「基本のセキュリティー編」 30ページ](#)
- ➡ [「運用・管理編」 38ページ](#)

ネットワーク環境の例



- (A) : オフィス1
- (A) -1 : LAN1
 - (A) -2 : LAN2
- (B) : オフィス2
- (B) -1 : LAN1
 - (B) -2 : LAN2
- (C) : WAN
- (D) : インターネット

スキャナー接続設定例の紹介

スキャナーの使用方法によって、主に2つの接続タイプがあります。どちらもコンピューターのあるネットワークに、ハブを介してスキャナーを接続します。

- サーバークライアント型接続（Windowsサーバーを使ったスキャナー、ジョブ管理）
- ピアツーピア型接続（クライアントコンピューターによる直接接続）

関連情報

- ➡ [「サーバークライアント型接続」11ページ](#)
- ➡ [「ピアツーピア型接続設定」11ページ](#)

サーバクライアント型接続

サーバーにインストールしたDocument Capture Pro Serverでスキャナーやジョブを一元管理します。主に複数のスキャナーを使って、大量の原稿を一定の形式でスキャンするような業務に向いています。

関連情報

➡ [「マニュアルで使用する用語の定義」7ページ](#)

ピアツーピア型接続設定

クライアントコンピューターにインストールされたEpson Scan 2などのスキャナードライバーから、個々のスキャナーを使用します。Document Capture Pro (Document Capture)をクライアントコンピューターにインストールすると、クライアントコンピューターにある個々のスキャンジョブを実行できます。

関連情報

➡ [「マニュアルで使用する用語の定義」7ページ](#)

ネットワーク接続の準備

接続情報の収集

ネットワーク接続にはIPアドレスやゲートウェイアドレスなどが必要です。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	有線LAN接続にはカテゴリ5e以上の STP (Shielded Twisted Pair) ケーブルを使用してください。
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	IPアドレスをルーターのDHCP機能で自動設定する場合は、この情報の収集は不要です。
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	IPアドレスに固定IPアドレスを使う場合は、DNSサーバーを設定してください。 DHCP機能による自動割り当てをしている場合は、DNSサーバーを自動取得できない場合に設定してください。
プロキシサーバー情報	- プロキシサーバー名 - 使用するポート番号	インターネット接続にプロキシサーバーを利用していて、Epson Connectサービスやファームウェアの自動更新機能などを利用する場合は設定してください。

スキャナー仕様

スキャナーが対応している規格や接続モードなどの仕様は『ユーザーズガイド』をご覧ください。

使用するポート番号

スキャナーが使用するポート番号の情報は「付録」をご覧ください。

関連情報

➡ [「スキャナーが使用するポート」58ページ](#)

IPアドレスの割り当てタイプ

スキャナーのIPアドレス割り当てには以下のタイプがあります。

固定IPアドレス：

あらかじめ決めた固有のIPアドレスをスキャナーに割り当てます。

スキャナーやルーターの電源を切ってもIPアドレスは変更されないので、IPアドレスによる管理ができます。

多数のスキャナーを管理する大規模オフィスや学校などのネットワークにお勧めします。

DHCP機能による自動割り当て：

スキャナーを接続し、DHCP機能を提供しているルーターなどの機器と正常に通信できれば、正しいIPアドレスが自動で割り当てられます。

IPアドレスが変わると都合が悪いデバイスには、IPアドレスを予約して同じ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

インターネット接続するサービスを利用するときは、DNSサーバーを設定してください。設定しないと名前の解決ができないため、アクセス先をIPアドレスで指定する必要があります。

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口に配置され、コンピューターやスキャナ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。相手サーバーからはプロキシサーバーとだけ通信しているように見えています。よって、スキャナ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、セキュリティの向上が期待できます。

また、プロキシサーバーは通信の内容を見ることができるので、フィルタリング機能で特定のURLへのアクセスを禁止できます。

ネットワーク接続設定方法の紹介

スキャナーのIP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のネットワーク接続は、以下のような方法で設定します。

操作パネルを使う：

スキャナーの操作パネルを使って個別に設定します。スキャナーの接続設定をしてからネットワークに接続します。

インストーラーを使う：

インストーラーを使用すると、スキャナーのネットワーク設定やクライアントコンピュータの設定を自動でできます。インストーラーの指示に従っていくと設定できるので、ネットワークに関する深い知識がなくても接続できます。

ツールを使う：

システム管理者のコンピュータからツールを使って設定します。スキャナーを探索して設定することや、設定用SYLKファイルを作成して一括で設定できます。大量のスキャナーを設定できますが、設定前にLANケーブルで物理的に接続する必要があります。設定用の有線LANを構築できる場合にお勧めの方法です。

関連情報

- ➡ [「操作パネルでネットワークに接続する」 14ページ](#)
- ➡ [「インストーラーを使ってネットワークに接続する」 18ページ](#)
- ➡ [「EpsonNet ConfigでIPアドレスを設定する」 54ページ](#)

接続編

この章では、スキャナーをネットワークに接続するための環境や手順について説明しています。

ネットワークに接続する

操作パネルでネットワークに接続する

スキャナーの操作パネルを使って、スキャナ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

IP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。

1. スキャナーの電源を入れます。
2. スキャナーの操作パネルを左にフリックして【設定】をタップします。

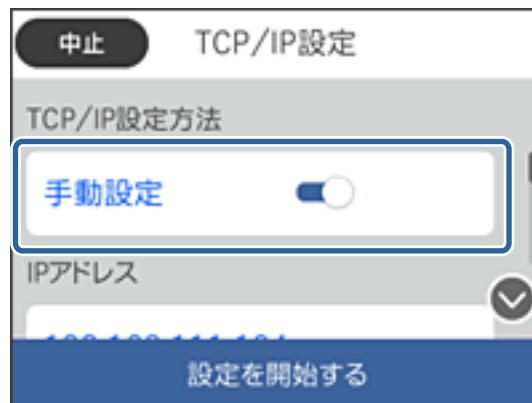


3. 【ネットワーク設定】 - 【設定を変更する】の順にタップします。
項目が表示されないときは、画面を上フリックしてください。

4. [TCP/IP] をタップします。



5. [TCP/IP設定方法] をタップして [手動設定] にします。



参考 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。その場合は、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] をタップし、表示されたキーパッドでIPアドレスを入力して [OK] をタップします。



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。

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. 【DNSサーバー】の【プライマリーDNS】をタップし、表示されたキーボードでプライマリーにするDNSサーバーのIPアドレスを入力して、【OK】をタップします。

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. 同様に【セカンダリーDNS】をタップし、表示されたキーボードでセカンダリーにするDNSサーバーのIPアドレスを入力して、【OK】をタップします。

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。

11. 設定完了画面が表示されたら【閉じる】をタップします。

【閉じる】をタップしなくても、一定時間を経過すると自動で画面が変わります。

有線LANで接続する

LANケーブルでネットワークに接続してから接続を確認します。

1. スキャナーとハブ（L2スイッチ）をLANケーブルで接続します。

ホーム画面のアイコンが  に変わります。

2. ホーム画面の  をタップします。



3. 画面を上フリックして、接続状態やIPアドレスなどが正しいか確認します。



プロキシサーバーを設定する

操作パネルからの設定はできません。Web Configを使用して設定します。

1. Web Configで【ネットワーク設定】 - 【基本】を選択します。
2. 【プロキシサーバー設定】で【使用する】を選択します。
3. 【プロキシサーバー】をIPv4アドレス形式、またはFQDN形式で指定して、【プロキシサーバーポート番号】にポート番号を入力します。
認証が必要なプロキシサーバーの場合、【プロキシサーバー認証ユーザー名】と【プロキシサーバー認証パスワード】を入力します。

4. 「次へ」 ボタンをクリックします。

The screenshot shows the Epson Web Config interface. On the left is a navigation menu with options like '管理者ログオフ', '情報確認', '製品情報', 'ネットワーク情報', 'パネルのスナップショット', 'メンテナンス情報', 'ハードウェア情報', 'スキャナー設定', 'ネットワーク設定', '無線LAN', 'ネットワーク基本', 'メールサーバー', 'ネットワークのセキュリティ設定', '利用サービス', 'システム設定', '設定のエクスポート/インポート', '管理者設定', '基本設定', 'DNS/プロキシ', 'ファームウェアアップデート', 'ルート証明書更新', and '製品情報'. The main area displays various settings for DNS, proxy, and IPv6. A blue box highlights the '次へ' (Next) button at the bottom of the main settings area.

5. 設定内容を確認して「設定変更」をクリックします。

関連情報

➔ 「Web Configの起動」 21ページ

インストーラーを使ってネットワークに接続する

スキャナーとコンピューターを接続設定するにはインストーラーを使うと便利です。インストーラーは以下のいずれかの方法で起動できます。

- ウェブサイトから設定
以下のウェブサイトアクセスして、製品名を入力します。[セットアップ]に進んで、作業を開始します。
<http://epson.sn>
- ソフトウェアディスクで設定（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、画面の指示に従って操作します。

接続方法を選択する

インストーラーの画面の指示に従って操作し、以下の画面が表示されたらコンピューターとスキャナーの接続方法を選択します。

- Windows

接続方法を選択して「次へ」をクリックします。



- Mac OS

接続方法を選択します。



この後は、画面の指示に従って操作します。必要なソフトウェアもインストールされます。

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はスキャナーの設定確認や変更がウェブブラウザ上でできるアプリケーションソフトです。Web Configを使用するには、あらかじめスキャナーにIPアドレスを設定しておく必要があります。

参考 スキャナ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。

以下の設定ページがあります。

- [基本設定]
スキャナーの基本機能の設定ができます。



- [詳細設定]
スキャナーの詳細設定ができます。主に管理者が使用するページです。

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、スキャナーの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。なお、HTTPSアクセス時にスキャナ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。

- HTTPSアクセス
IPv4 : `https://スキャナーのIPアドレス`
IPv6 : `https://[スキャナーのIPアドレス]`
- HTTPアクセス
IPv4 : `http://スキャナーのIPアドレス`
IPv6 : `http://[スキャナーのIPアドレス]`

参考

- 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]/`
- DNSにスキャナー名を登録すると、IPアドレスの代わりにスキャナー名が使用できます。

関連情報

- ➔ [「スキャナーとのSSL/TLS通信」 62ページ](#)
- ➔ [「使用できる電子証明書」 62ページ](#)

スキャン機能を使う

スキャナーの使い方に合わせて、以下のソフトウェアのインストールや設定をしてください。

- コンピューターからのスキャン
 - Web Configでネットワークスキャンサービスの有効を確認（工場出荷時は有効）
 - コンピューターへEpson Scan 2をインストールしてIPアドレスを設定
 - ジョブを使用してスキャンする場合はDocument Capture Pro／Document Captureのインストールとジョブ設定
- 操作パネルからのスキャン
 - Document Capture ProまたはDocument Capture Pro Serverを使用する場合：
Document Capture ProまたはDocument Capture Pro Serverのインストール
Document Capture ProまたはDocument Capture Pro Serverの設定（サーバーモード、クライアントモード）
 - WSDプロトコルを使用する場合：
Web Configまたは操作パネルでWSDの有効を確認（工場出荷時は有効）
デバイスの追加設定（Windowsコンピューター）

コンピューターからスキャンするには

コンピューターからネットワークを経由したスキャンをするには、ソフトウェアをインストールして、ネットワークスキャンサービスの有効を確認してください。

関連情報

- ➔ [「インストールするソフトウェア」 22ページ](#)
- ➔ [「ネットワークスキャンを有効にする」 23ページ](#)

インストールするソフトウェア

- Epson Scan 2
スキャナードライバーです。コンピューターからスキャンする場合、クライアントコンピューターそれぞれにインストールします。Document Capture Pro/Document Captureがコンピューターにインストールされている場合、本体のボタンに割り当てられたジョブを実行できます。
EpsonNet SetupManagerを使うと、パッケージで配布できます。

- Document Capture Pro (Windows) / Document Capture (Mac OS)
クライアントコンピューターへインストールします。ネットワーク上のDocument Capture Pro / Document Captureがインストールしてあるコンピューターに登録されたジョブを、コンピューターやスキャナーの操作パネルから呼び出して実行できます。
ネットワーク上のコンピューターからいつでもスキャンができます。スキャンするにはEpson Scan 2が必要です。

関連情報

➔ [「EpsonNet SetupManager」 54ページ](#)

Epson Scan 2にスキャナーのIPアドレスを設定する

スキャナーのIPアドレスを指定してネットワークでスキャナーを使用できるようにします。

1. [スタート] - [すべてのプログラム] - [EPSON] - [Epson Scan 2] から [Epson Scan 2 Utility] を起動します。
既に他のスキャナーが登録されている場合は、手順2に進みます。
登録されていない場合は、手順4へ進みます。
2. [スキャナー] の▼をクリックします。
3. [設定] をクリックします。
4. [編集を許可] をクリックして、[追加] をクリックします。
5. [機種] からスキャナーの機種名を選択します。
6. [ネットワークを検索] の [アドレス] から使用するスキャナーのIPアドレスを選択します。



をクリックして  をクリックすると一覧が更新されます。スキャナーのIPアドレスが見つからない場合は、[アドレスを入力] を選択してIPアドレスを入力します。

7. [追加] をクリックします。
8. [OK] をクリックします。

ネットワークスキャンを有効にする

クライアントコンピューターからネットワークでスキャンをするにはネットワークスキャンサービスを設定します。工場出荷時には有効に設定されています。

1. Web Configで [利用サービス] - [ネットワークスキャン] を選択します。
2. [EPSON Scan] の [スキャン機能を有効にする] が選択されていることを確認します。

選択されている場合はここで終了です。Web Configを閉じます。

選択されていない場合は、選択して次の手順に進みます。

3. [次へ] をクリックします。

4. [設定] をクリックします。

ネットワークが再起動して、設定が有効になります。

関連情報

➡ [「Web Configの起動」 21ページ](#)

操作パネルを使ってスキャンするには

スキャナーの操作パネルを使ったスキャン to フォルダー機能やスキャン to メール機能、メールやフォルダーなどへのスキャン結果の転送は、コンピューターからジョブを実行して行います。

スキャン結果を転送する場合は、Document Capture Pro ServerやDocument Capture Proでジョブを設定してください。

設定内容の詳細やジョブの設定方法は、Document Capture Pro Server、Document Capture Proのヘルプ、マニュアルをご覧ください。

関連情報

➡ [「Document Capture Pro Server/Document Capture Proを設定する」 24ページ](#)

➡ [「サーバーやフォルダーの設定」 25ページ](#)

コンピューターにインストールするソフトウェア

- Document Capture Pro Server

Document Capture Proのサーバー版です。Windowsサーバーへインストールします。複数のデバイスやジョブをサーバーで一元管理できます。複数のスキャナーから同時にスキャンジョブを実行できます。

Document Capture Pro Serverの認証版を使用すると、ユーザーや所属に結びつけたジョブ管理やスキャン履歴の閲覧などができます。

Document Capture Pro Serverの詳細はエプソンの問い合わせ窓口にお問い合わせください。

- Document Capture Pro (Windows) / Document Capture (Mac OS)

コンピューターからスキャンする場合と同様にコンピューターに登録されたスキャンジョブをスキャナーの操作パネルから呼び出して実行できます。複数のスキャナーからコンピューターのジョブを同時に実行することはできません。

Document Capture Pro Server/Document Capture Proを設定する

スキャナーの操作パネルからスキャン機能を使用するための設定をします。

1. Web Configで[利用サービス] - [Document Capture Pro] を選択します。

2. [動作モード] を選択します。

- サーバーモード：

Document Capture Pro Serverを使用する場合に選択します。

- クライアントモード：
コンピュータを特定せずに、ネットワーク内の各クライアントコンピュータにインストールされている Document Capture Pro (Document Capture) のジョブを選択して実行する場合に設定します。

3. 選択したモードに応じて以下を設定します。

- サーバーモード：
[サーバーアドレス] に Document Capture Pro Server をインストールしているサーバーを指定します。
IPv4、IPv6、ホスト名、FQDN のいずれかの形式で 2～252 文字以内で指定します。FQDN 形式では US-ASCII 文字の数字とアルファベット、ハイフン（先頭と末尾以外）が使用できます。
- クライアントモード：
Document Capture Pro (Document Capture) からスキャナーのグループを指定して使用する場合は [グループ設定] を指定します。

4. [設定変更] をクリックします。

関連情報

➡ [「Web Configの起動」 21ページ](#)

サーバーやフォルダーの設定

Document Capture Pro、Document Capture Pro Server は、スキャンしたデータを一旦サーバーやクライアントコンピュータに保存し、転送機能を使ってスキャン to フォルダー機能やスキャン to メール機能などを実行します。Document Capture Pro、Document Capture Pro Server がインストールしてあるコンピュータからコンピュータやクラウドサービスへ転送するための権限や情報が必要です。

以下を参考に使用する機能の情報を準備してください。

これらの機能は Document Capture Pro や Document Capture Pro Server で設定します。設定内容の詳細は、Document Capture Pro Server、Document Capture Pro のヘルプ、マニュアルをご覧ください。

機能名	設定	必要なもの
スキャン to フォルダー機能 (SMB)	保存フォルダーの作成と共有設定	保存フォルダーを作成するコンピュータへの管理者権限ユーザーアカウント
	スキャン to フォルダー (SMB) の宛先	保存フォルダーがあるコンピュータへログオンするためのユーザー名、パスワード、保存フォルダーへの書き込みの権利
スキャン to フォルダー機能 (FTP)	FTPサーバーログオン設定	保存先FTPサーバーへのログオン情報、保存フォルダーへの書き込みの権利
スキャン to メール機能	メールサーバーの設定	メールサーバーの設定情報
スキャン to Document Capture Pro 機能 (Document Capture Pro Server を使用する場合)	各種クラウドサービスへのログオン設定	インターネット接続環境 各種クラウドサービスへのアカウント登録

WSDスキャンを使う (Windows)

コンピュータが Windows Vista 以降の場合、WSDスキャンを使用できます。

WSDプロトコルが使用できるとスキャナーの操作パネルに「コンピューター(WSD)」が表示されます。

1. Web Configで「利用サービス」 - 「プロトコル」を選択します。
2. 「WSD設定」で「WSDを有効にする」にチェックが入っていることを確認します。
入っている場合はここで終了し、Web Configを閉じます。
入っていない場合はチェックを入れ、次の手順に進みます。
3. 「次へ」をクリックします。
4. 設定内容を確認して「設定変更」をクリックします。

システムの詳細を設定する

操作パネルでシステム設定する

画面の明るさを設定

画面の明るさを設定します。

1. 操作パネルのホーム画面で「設定」をタップします。
2. 「共通設定」 - 「画面の明るさ設定」の順にタップします。
3.  または  をタップして明るさを調整します。
1から9まで調整できます。
4. 「OK」をタップします。

音の設定をする

パネル操作音やエラー音の設定をします。

1. 操作パネルのホーム画面で「設定」をタップします。
2. 「共通設定」 - 「音の設定」の順にタップします。
3. 必要に応じて以下の項目を設定します。
 - 操作音
操作パネルの操作音の音量を設定します。

- エラー音
エラー音の音量を設定します。

4. [OK] をタップします。

関連情報

➡ [「Web Configの起動」 21ページ](#)

原稿の重送検知を設定する

スキャンする原稿の重送を検知し、重送した場合にスキャンを停止する機能の設定をします。
封筒やステッカーを貼り付けた紙など重送と判断される原稿をスキャンする場合は、オフに設定してください。

参考 Web ConfigまたはEpson Scan 2からも設定できます。

1. 操作パネルのホーム画面で[設定] をタップします。
2. [外部スキャン設定] - [超音波重送検知] の順にタップします。
3. [超音波重送検知] をタップして、オン・オフを切り替えます。
4. [閉じる] をタップします。

低速モードを設定する

伝票のような薄い原稿をスキャンする場合は、紙詰まりしないように低速でスキャンするように設定します。

1. 操作パネルのホーム画面で[設定] をタップします。
2. [外部スキャン設定] - [低速モード] の順にタップします。
3. [低速モード] をタップして、オン・オフを切り替えます。
4. [閉じる] をタップします。

Web Configでシステム設定する

無操作時の省電力設定をする

スキャナー無操作時の省電力設定をします。使用する環境に合わせて時間を設定してください。

参考 スキャナーの操作パネルからも設定できます。

1. Web Configで[システム設定] - [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。
3. 【自動電源オフ時間】に電源が切れるまでの時間を設定します。
4. 【設定】をクリックします。

関連情報

➡ [「Web Configの起動」 21ページ](#)

操作パネルの動作を設定する

スキャナ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【システム設定】 - 【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行う場合に管理者パスワードの入力を求められます。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】にすると利用者制限の利用者、またはシステム管理者としてログオンしている状態で、設定した時間内に操作パネルの操作をしなかった場合に、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。
3. 【設定】をクリックします。

関連情報

➡ [「Web Configの起動」 21ページ](#)

外部インターフェイスの制限を設定する

コンピューターからのUSB 接続を制限できます。ネットワーク経由以外のスキャンを制限する場合に設定します。

1. Web Configで【システム設定】 - 【外部インターフェイス】を選択します。
2. 【有効】または【無効】を選択します。
制限する場合は【無効】を選択します。
3. 【設定】をクリックします。

タイムサーバーと日付/時刻を同期する

CA証明書を使っている場合は連携すると時間に関するトラブルを防げます。

印刷枚数で課金されるシステムでプリンターを使用している場合は、システムが時間を管理しているので、タイムサーバーと連携する必要はありません。

1. Web Configで【システム設定】 - 【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】で【使用する】を選択します。
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10,800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」 21ページ](#)

基本のセキュリティ編

この章では、特別な環境を必要としない基本のセキュリティ設定について説明しています。

基本のセキュリティ機能の紹介

特別な環境を必要としない基本のセキュリティ設定を説明します。

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
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て管理者以外の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、Epson Device Admin、EpsonNet Configのどこからでも設定や変更ができます。	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リスクにつながる危険性を低減します。
プロトコルの制御	デバイス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逐次して、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。

関連情報

- ➔ [「Web Configの概要」 20ページ](#)
- ➔ [「EpsonNet Config」 53ページ](#)
- ➔ [「Epson Device Admin」 53ページ](#)
- ➔ [「管理者パスワードの設定」 30ページ](#)
- ➔ [「利用するプロトコルを制御する」 33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、管理者以外がシステム管理に関する設定を変更できなくなります。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、EpsonNet Config）のいずれからでも設定、変更ができます。ツールの操作方法はそれぞれのマニュアルをご覧ください。

関連情報

- ➔ [「操作パネルから管理者パスワードを設定する」 31ページ](#)
- ➔ [「Web Configから管理者パスワードを設定する」 31ページ](#)
- ➔ [「EpsonNet Config」 53ページ](#)

➡ [「Epson Device Admin」 53ページ](#)

操作パネルから管理者パスワードを設定する

スキャナーの操作パネルから管理者パスワードを設定をします。

1. スキャナーの操作パネルで【設定】をタップします。
2. 【管理者用設定】 - 【管理者設定】の順にタップします。
項目が表示されないときは、画面を上フリックして項目を表示してください。
3. 【管理者パスワード】 - 【新規設定】の順にタップします。
4. 任意のパスワードを入力して、【OK】をタップします。
5. パスワードを再入力して、【OK】をタップします。
6. 確認画面で【OK】をタップします。
管理者設定画面に戻ります
7. 【管理者ロック】をタップして、確認画面で【OK】をタップします。
管理者ロックが【オン】になり、ロックされたメニュー項目を操作しようとするとき管理者パスワードの入力を求められるようになります。

- 参考**
- 【設定】 - 【共通設定】 - 【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初期画面に戻ります。
 - 管理者パスワードは、【管理者パスワード】から【変更】、【設定クリア】を選択して、管理者パスワードを入力すると変更や削除ができます。

Web Configから管理者パスワードを設定する

Web Configを使って管理者パスワードを設定します。

1. Web Configで【管理者設定】 - 【管理者認証情報変更】を選択します。

2. 「新しいパスワード」と「新しいパスワードの確認」に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。

パスワードを変更するには、現在のパスワードを入力します。

3. 「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「管理者ログオン」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削除するには、「管理者設定」 - 「管理者認証情報削除」をクリックして管理者パスワードを入力します。

関連情報

➔ [「Web Configの起動」 21ページ](#)

管理者パスワードでロックされる項目

システム管理者はデバイスにおける全機能の設定や、変更の権限を持っています。
また、デバイスに管理者パスワードを設定すると、デバイス管理に関わる項目を変更できないようにロックできます。
システム管理者が制御できる項目は以下の通りです。

アイテム	説明
スキャナーの設定	重送検知や低速モードの設定。

アイテム	説明
有線LAN接続設定	デバイス名やIPアドレスの変更、DNSサーバーやプロキシサーバーの設定など、ネットワーク接続に関する設定変更。
利用サービスの設定	通信プロトコルの制御や、ネットワークスキャン、Document Capture Proなどのサービスの設定。
メールサーバーの設定	デバイスが直接通信するメールサーバーの設定。
セキュリティ設定	SSL/TLS通信、IPsecやIPフィルタリング、IEEE802.1Xなどネットワークセキュリティに関する設定。
ルート証明書更新	Document Capture Pro Serverの認証やWeb Configからのファームウェアアップデートに必要なルート証明書の更新。
ファームウェアアップデート	デバイスのファームウェアの更新確認とアップデート。
時間、タイマー設定	スリープ移行時間、自動電源オフ、日付/時刻、無操作タイマーの時間など、タイマーに関する設定。
初期設定に戻す	スキャナーの設定を工場出荷時の状態にする設定。
管理者設定	管理者ロックや管理者パスワードの設定。
認証装置の設定	認証装置のID設定。認証装置対応の認証システムでスキャナーを使う場合に設定します。

利用するプロトコルを制御する

スキャンする場合、いろいろな経路やプロトコルからスキャンできます。また、不特定多数のコンピューターからネットワークスキャンが利用可能になります。たとえば、特定の経路やプロトコルのスキャンだけを許可できます。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スキャンなどのセキュリティリスクを軽減できます。

製品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【利用サービス】 - 【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。

設定がスキャナーに反映されます。

関連情報

- ➡ [「Web Configの起動」 21ページ](#)
- ➡ [「有効・無効が設定可能なプロトコル」 34ページ](#)
- ➡ [「プロトコルの設定項目」 35ページ](#)

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は機器の検索やスキャンなどに使われます。
SLP設定	SLP機能の有効・無効が設定できます。SLPはエプソンデバイスではEpson Scan 2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ポートからのスキャン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。
SNMPv1/v2c設定	SNMPv1/v2cの有効・無効を指定できます。エプソンデバイス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。エプソンデバイス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。

関連情報

- ➡ [「利用するプロトコルを制御する」 33ページ](#)
- ➡ [「プロトコルの設定項目」 35ページ](#)

プロトコルの設定項目

EPSON

[管理者ログオフ](#)
[情報確認](#)
[製品情報](#)
[ネットワーク情報](#)
[パネルのスナップショット](#)
[メンテナンス情報](#)
[ハードウェア情報](#)
[スキャナー設定](#)
[ネットワーク設定](#)
[ネットワークのセキュリティ設定](#)
[利用サービス](#)
[プロトコル](#)
[ネットワークスキャン](#)
[Document Capture Pro](#)
[システム設定](#)
[設定のエクスポート/インポート](#)
[管理者設定](#)
[基本設定](#)
[DNS/プロキシ](#)
[ファームウェアアップデート](#)
[ルート証明書更新](#)
[製品情報](#)

利用サービス>プロトコル

※各プロトコルのデバイス名、Bonjour名を変更するには、ネットワーク基本のデバイス名を変更してください。
各プロトコルのロケーションを変更するには、ネットワーク基本のロケーションを変更してください。

Bonjour設定

☒ Bonjourを使用する

Bonjour名:

EPSONXXXX.local

Bonjourサービス名:

EPSON XXXX.XXXXX

ロケーション:

SLP設定

☒ SLP機能を有効にする

WSD設定

☒ WSDを有効にする

スキャンタイムアウト (秒):

300

デバイス名:

EPSONXXXX

ロケーション:

LLTD設定

☒ LLTDを有効にする

デバイス名:

EPSONXXXX

LLMNR設定

☒ LLMNRを有効にする

アイテム	設定値と説明
Bonjour設定	
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サービス名を表示、設定できます。
ロケーション	Bonjourのロケーションが表示されます。
SLP設定	
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。Epson Scan 2やEpsonNet Configでのネットワーク探索に使われます。
WSD設定	
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。
スキャンタイムアウト (秒)	WSDスキャン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。

基本のセキュリティ編

アイテム	設定値と説明
ロケーション	WSDのロケーションが表示されます。
LLTD設定	
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	
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。
SNMPv1/v2c設定	
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。SNMPv3をサポートしているスキャナーのみ表示されます。
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	
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	SNMPv3.の暗号化アルゴリズムを選択します。
パスワード	SNMPv3.の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。

アイテム	設定値と説明
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。

関連情報

- ➡ [「利用するプロトコルを制御する」 33ページ](#)
- ➡ [「有効・無効が設定可能なプロトコル」 34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。

デバイスの情報を確認する

Web Configの【情報確認】から運用しているデバイスの、以下の情報を確認できます。

- 製品情報
言語、ステータス、クラウドサービス、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。
- 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。
- メンテナンス情報
利用開始日、スキャン枚数などを確認できます。
- ハードウェア情報
スキャナーのステータスを確認できます。

関連情報

➔ [「Web Configの起動」 21ページ](#)

デバイスの管理（Epson Device Admin）

Epson Device Adminを使うと多数のデバイスを管理、運用ができます。Epson Device Adminはルーターを越えた場所（別ネットワーク）にあるデバイスも管理ができます。主に以下の管理機能があります。機能や操作の詳細はEpson Device Adminのマニュアルやヘルプをご覧ください。

- デバイスの探索
ネットワークにあるデバイスを探索して一覧に登録できます。同じネットワークに接続されているエプソン製デバイスならば、IPアドレスが未設定でも発見できます。
また、ネットワークにあるコンピューターにUSBで接続されたデバイスも探索できます。コンピューターにはEpson Device USB Agent（エプソン デバイス USB エージェント）がインストールされている必要があります。
- デバイス設定
デバイスの詳細項目設定をテンプレートにして、デバイスに統一した設定値を適用できます。ネットワークに接続されていれば、IPアドレスが未設定のデバイスにIPアドレスを割り当てることができます。
- デバイスの監視
ネットワーク上のデバイスから定期的にデバイスの状態や詳細情報を収集できます。また、ネットワーク上のコンピューターにUSBで接続されたデバイスや、デバイスリストに登録した他社製のデバイスも監視できます。USB接続のデバイスを監視するには、コンピューターにEpson Device USB Agentがインストールされている必要があります。

- アラート管理
紙詰まり、消耗品交換など、デバイスが出すアラートを監視できます。また、事前に条件を設定するとアラートが発生したときに自動で管理者へメールで通知できます。
- レポート管理
デバイスや消耗品の使用状況、スキャン枚数などの情報を蓄積して定期的にレポートを作成できます。また、作成したレポートの保管やメールでの送信ができます。

関連情報

➡ [「Epson Device Admin」 53ページ](#)

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

メール通知とは、イベントが発生したときにメールを受け取る機能です。メールアドレスは5つまで登録でき、それぞれに受け取りたいイベントを設定できます。

この機能を使うには、メールサーバー設定をする必要があります。

関連情報

➡ [「メールサーバーを設定する」 40ページ](#)

メール通知を設定する

この機能を利用するにはメールサーバーの設定が必要です。

1. Web Configで【管理者設定】 - 【メール通知】を選択します。
2. メールを受け取る送信先のメールアドレスを入力します。
3. メール通知の言語を選択します。

4. 通知を受け取りたいイベントをチェックします。

EPSON

管理者ログオフ

情報確認

製品情報

ネットワーク情報

パネルのスナップショット

メンテナンス情報

ハードウェア情報

スキャナー設定

ネットワーク設定

ネットワークのセキュリティ設定

利用サービス

システム設定

設定のエクスポート/インポート

管理者設定

管理者認証情報変更

管理者認証情報削除

管理者名/連絡先

メール通知

基本設定

DNS/プロキシ

ファームウェアアップデート

ルート証明書更新

製品情報

管理者設定 > メール通知

メール通知を使用するには事前にメールサーバー設定を行ってください。

宛先設定

設定された宛先に、選択した言語のメールを送信します。

1:	admin@example.com	日本語
2:	administrator@example.com	日本語
3:		日本語
4:		日本語
5:		日本語

通知設定

チェックを付けた項目の状態のときにメールを送信します。

	1	2	3	4	5
管理者パスワード変更	☒	☒	☐	☐	☐
スキャナーエラー	☒	☐	☐	☐	☐

設定 購入時の設定に戻す

5. [設定] をクリックします。

関連情報

- ➡ 「Web Configの起動」 21ページ
- ➡ 「メールサーバーを設定する」 40ページ

メールサーバーを設定する

設定の前に以下を確認してください。

- スキャナーがネットワークに接続されていること
- コンピューターのメール設定時に使ったサーバー情報

- Web Configで【ネットワーク設定】 - 【メールサーバー】 - 【基本】を選択します。
- 各項目を設定します。
- 【設定】を選択します。
設定結果が表示されます。

関連情報

- ➡ 「Web Configの起動」 21ページ

➡ 「メールサーバー設定項目」 41 ページ

メールサーバー設定項目

アイテム	設定値と説明	
認証方式	スキャナ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	メールサーバーとの通信時に認証を行いません。
	SMTP認証	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	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ASCII (0x20-0x7E) で表せる0～255文字以内で入力します。	
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A-Z a-z 0-9 ! # \$ % & ' * + , - . / = ? ^ _ { } ~ @を使用し、0～20文字以内で入力します。	
送信元アドレス	送信元を示すメールアドレスを入力します。: () < > [] ; ¥ を除くASCII (0x20-0x7E) で表せる0～255文字以内で入力します。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、0～255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までの半角数字を入力します。	

アイテム	設定値と説明	
セキュア接続	メールサーバーのセキュア接続方式を指定します。	
	なし	【認証方式】で【POP before SMTP】を選択した場合は【なし】になります。
	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。
	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。
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。	
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A～Z a～z 0～9 . - を使用して0～255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。	
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、1～65535までの数字入力をします。	

関連情報

➡ [「メールサーバーを設定する」40ページ](#)

メールサーバーとの接続を確認する

1. Web Configで【ネットワーク設定】 - 【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」21ページ](#)

➡ [「メールサーバー接続確認結果」42ページ](#)

メールサーバー接続確認結果

メッセージ	説明
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。 - スキャナ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

メッセージ	説明
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。 ・ スキャナ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	スキャナ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	スキャナ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スキャナ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、スキャナーはSMTP認証を実行していません。

メッセージ	説明
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、スキャナーは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。
製品は処理動作中のためアクセスできません。	スキャナ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」 42ページ](#)

ファームウェアのアップデート

Web Configでファームウェアをアップデートする

Web Configからファームウェアをアップデートします。デバイスのインターネット接続が必要です。

1. Web Configで【基本設定】 - 【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」 21ページ](#)
 ➔ [「Epson Device Admin」 53ページ](#)

Epson Firmware Updaterを使って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。
<http://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デバイスを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。

設定をバックアップする

Web Configで設定項目をエクスポートすることで、設定項目を別のスキャナーにコピーできます。

設定をエクスポートする

スキャナーに設定されている個々の設定値をエクスポートします。

1. Web Configで【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。親のカテゴリを選択すると、子のカテゴリ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 スキャナーのIP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、スキャナ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」 21ページ](#)

設定をインポートする

Web Configの設定ファイルをスキャナーにインポートします。

！重要 スキャナー名や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アドレスを持つスキャナ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【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。

設定がスキャナーに反映されます。

関連情報

➡ [「Web Configの起動」 21ページ](#)

トラブルを解決する

トラブルを解決するための情報

本書に記載されていないスキャナーに関する情報は以下のマニュアルをご覧ください。

- ユーザーズガイド
スキャナーをコンピューターから使う方法やメンテナンス、トラブルの解決方法が記載されています。

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。

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購入時の設定に戻します。

1. ホーム画面で【設定】をタップします。
2. 【管理者用設定】 - 【初期設定に戻す】 - 【ネットワーク設定】の順にタップします。
3. メッセージを確認して、【はい】をタップします。
4. 設定完了のメッセージが表示されたら【閉じる】をタップします。
【閉じる】をタップしなくても、一定時間を経過すると次の画面に進みます。

デバイスとコンピューターの接続を確認する

コンピューターとの接続をPingで確認する - Windows

Pingを使ってコンピューターとスキャナーの通信ができていないか確認します。以下の手順で接続を確認してください。

1. 接続を確認したいスキャナーのIPアドレスを確認します。

Epson Scan 2を使って確認してください。

2. コンピューターのコマンドプロンプトを表示します。

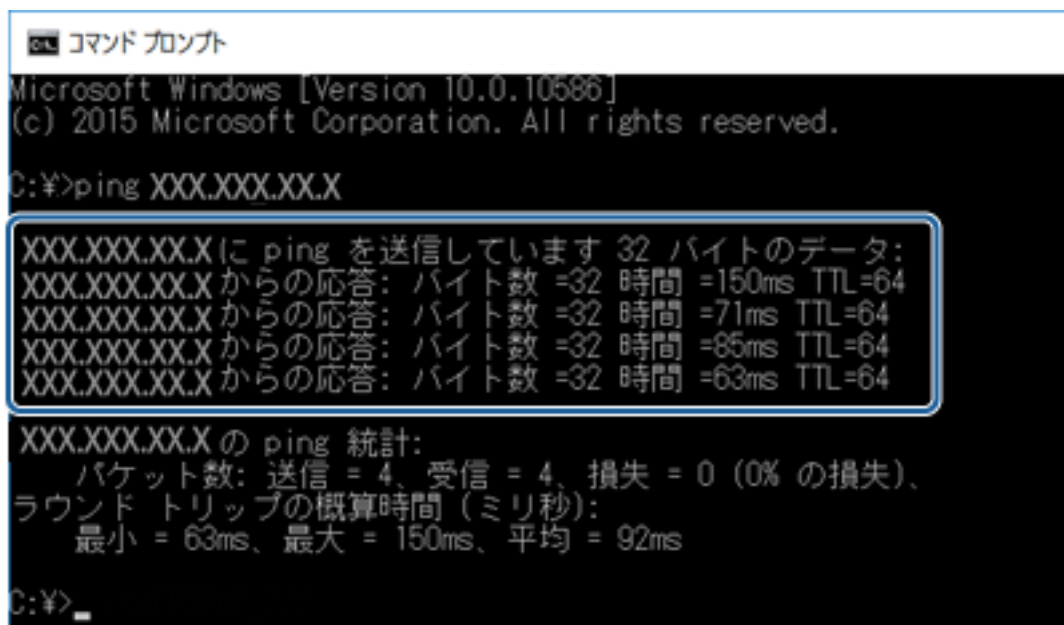
- Windows 10
スタートボタンを右クリックまたは長押しして、[コマンドプロンプト] を選択します。
- Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
アプリ画面を表示して、[コマンドプロンプト] を選択します。
- Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008以前
スタートボタンをクリックして [すべてのプログラム] または [プログラム] - [アクセサリ] - [コマンドプロンプト] の順に選択します。

3. 「ping xxx.xxx.xxx.xxx」と入力して、Enterキーを押します。

xxx.xxx.xxx.xxxにはスキャナーのIPアドレスを入れてください。

4. 通信状況を確認します。

スキャナ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。



```
コマンド プロンプト
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

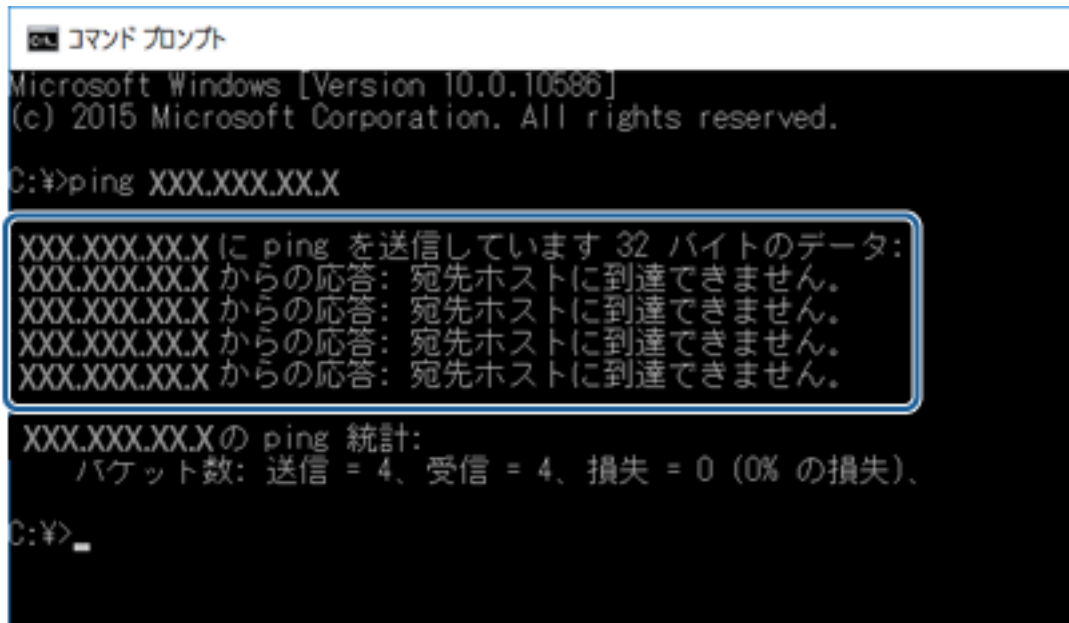
C:\>ping XXX.XXX.XX.X

XXX.XXX.XX.Xに ping を送信しています 32 バイトのデータ:
XXX.XXX.XX.X からの応答: バイト数 =32 時間 =150ms TTL=64
XXX.XXX.XX.X からの応答: バイト数 =32 時間 =71ms TTL=64
XXX.XXX.XX.X からの応答: バイト数 =32 時間 =85ms TTL=64
XXX.XXX.XX.X からの応答: バイト数 =32 時間 =63ms TTL=64

XXX.XXX.XX.X 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 = 63ms、最大 = 150ms、平均 = 92ms

C:\>
```

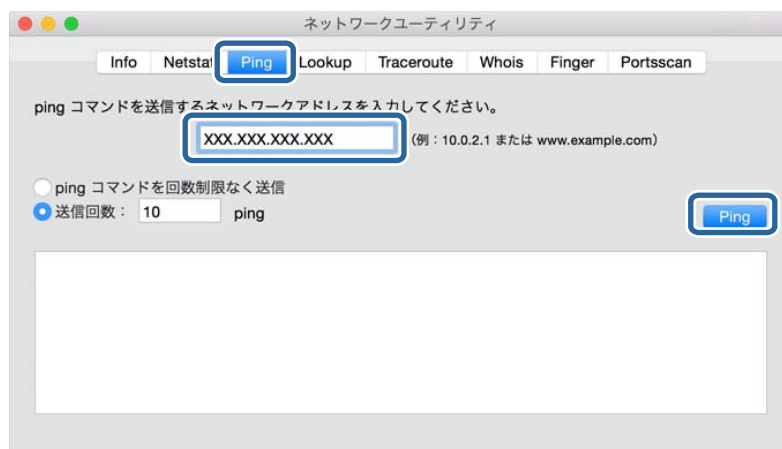

スキャナーとコンピューターが通信できていないと以下のように表示されます。



コンピューターとの接続をPingで確認する - Mac OS

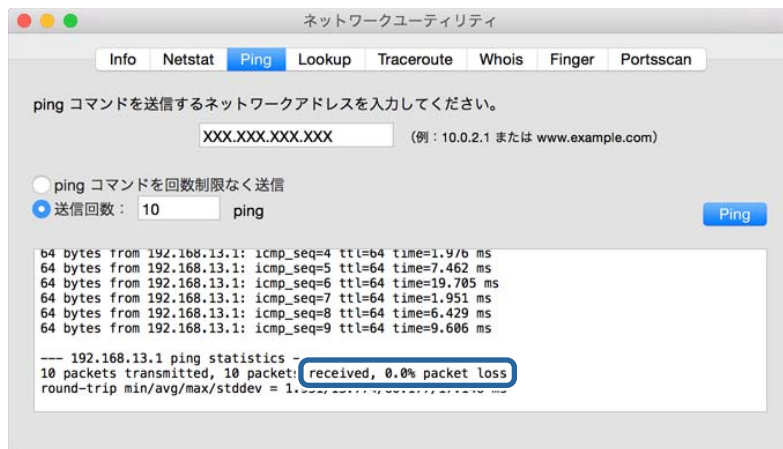
Pingを使ってコンピューターとスキャナーの通信ができていないか確認します。以下の手順で接続を確認してください。

1. 接続を確認したいスキャナーのIPアドレスを確認します。
Epson Scan 2を使って確認してください。
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。
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。

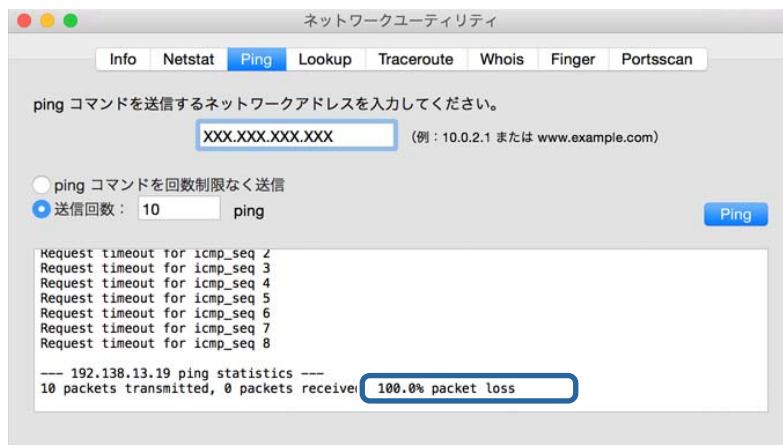


4. 通信状況を確認します。

スキャナ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。



スキャナ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。



ソフトウェア使用時のトラブル

Web Configにアクセスできない

スキャナーにIPアドレスを設定していますか？

スキャナーの操作パネルやEpson Device Admin、EpsonNet Configなどを使ってIPアドレスを設定してください。

SSL/TLSの暗号強度に対応するメッセージ暗号化に、Webブラウザーが対応していますか？

SSL/TLSの暗号強度に対応するメッセージ暗号化は以下の通りです。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のみ、Web Configを起動できます。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

Web ConfigにSSL通信 (https) で接続したときに「有効期限が切れている」と表示されましたか？

証明書の有効期限が切れていたら証明書を取得し直してください。証明書の有効期限内に表示されるときは、スキャナーの時刻が正しく設定されているか確認してください。

Web ConfigにSSL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....」と表示されましたか？

自己署名証明書またはCSRの作成時に「コモンネーム」で記述したアドレスとブラウザに入力したアドレスが一致していません。証明書を取得し直すか、スキャナー名を変更してください。

スキャナーをプロキシサーバー経由で使用していますか？

スキャナーでプロキシサーバーを使用する設定にしている場合、ブラウザのプロキシサーバーの設定が必要です。

- 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、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。
設定例：
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」 21ページ](#)
- ➡ [「IPアドレスを設定する」 14ページ](#)
- ➡ [「EpsonNet ConfigでIPアドレスを設定する」 54ページ](#)

EpsonNet Configで製品名やIPアドレスが表示されない

Windowsセキュリティの重要な警告画面やファイアウォールソフトが表示した画面で、[ブロックする]、[キャンセル] や [遮断する] を選択しましたか？

[ブロックする]、[キャンセル] や [遮断する] を選択すると通信ができなくなるため、EpsonNet Config または EpsonNet Setupで製品名が表示されません。

通信を可能にするには、Windowsファイアウォールや市販のセキュリティソフトでEpsonNet Configを例外アプリケーションとして登録してください。それでも表示できないときは、市販のセキュリティソフトを終了してからEpsonNet Configを再度起動してください。

通信エラーのタイムアウトが短い設定になっていませんか？

EpsonNet Configの [ツール] - [オプション] - [タイムアウト] で、[通信エラー] とする時間を大きい値に変更してみてください。ただし、検索に時間がかかるためEpsonNet Configの動作は遅くなります。

関連情報

- ➡ [「EpsonNet Configの起動 - Windows」 54ページ](#)
- ➡ [「EpsonNet Configの起動 - Mac OS」 54ページ](#)

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、デバイスのネットワークへの導入、設定、管理ができるアプリケーションソフトです。デバイスのステータスや消耗品情報などの詳細情報を把握し、アラートを通知したり、使用状況をレポートしたりできます。デバイスの詳細項目設定をテンプレートにして、デバイスに統一した設定値を適用できます。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、IPアドレスのアサインや接続形態の変更などスキャナーのネットワーク設定ができるアプリケーションソフトです。Windows版はバッチファイルを使用して複数台のスキャナーを同時に設定できます。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 SetupManager

ネットワークスキャナーのドライバーのインストールや設定からDocument Capture Proのインストール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。

EpsonNet ConfigでIPアドレスを設定する

EpsonNet Configを使ってスキャナーのIPアドレスを設定できます。EpsonNet Configを使うと IPアドレスを設定していないスキャナーにLANケーブルで接続してからIPアドレスを割り当てられます。

一括でIPアドレスを設定する

一括設定するためのファイルを作成する

MAC アドレスと機種名をキーにして、IPアドレスを設定するための SYLKファイルを作成します。

1. 表計算ソフト（Microsoft Excel）またはテキストエディターを起動します。
2. 設定項目名として「Info_MACAddress」（MAC アドレス）と「Info_ModelName」（機種名）、
「TCPIP_IPAddress」（IP アドレス）を 1 行目に入力します。
設定項目は、以下の文字列通りに入力してください。大文字/小文字、全角/半角を識別するため、1文字でも異なると設定項目として認識されません。
以下の設定項目を入力することで、EpsonNet Configが各行に記載される情報の意味を判断します。

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. 各行に MACアドレスと機種名、設定したい IPアドレスを入力します。

Info_MACAddress	Info_ModelName	TCPIP_IPAddress
0000XXXX0001	ALC-XXXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXXX	192.168.100.104

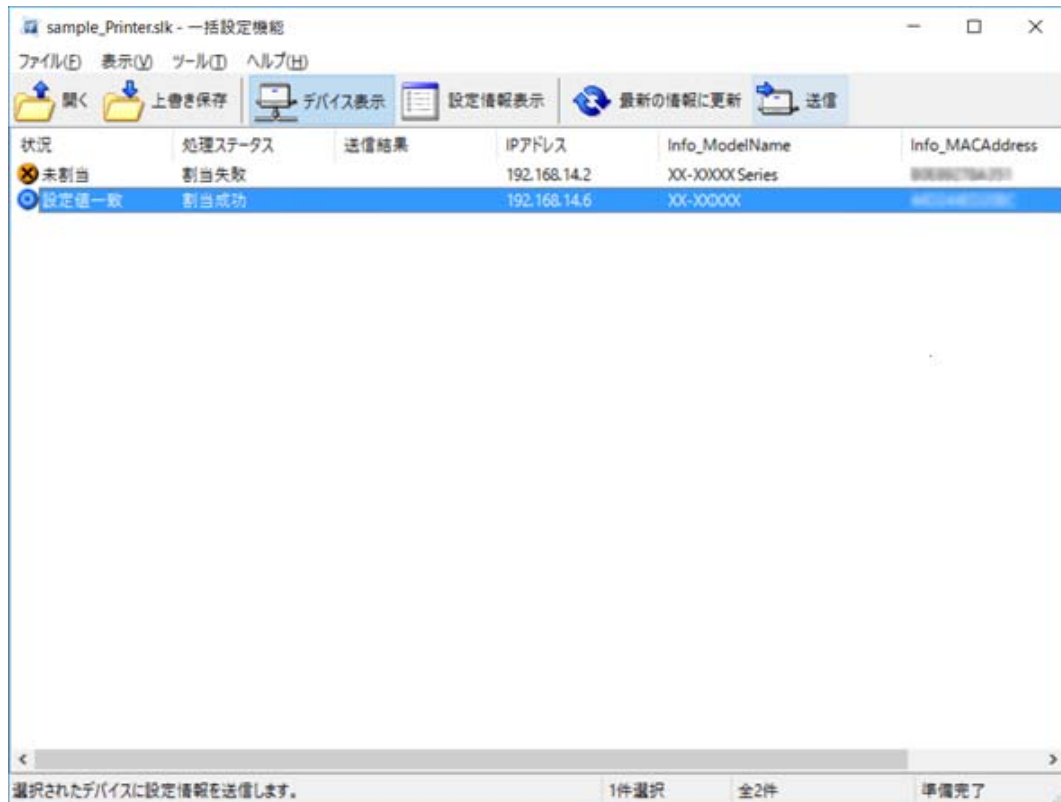
4. 任意の名称で SYLKファイル（拡張子 .slk）として保存します。

設定ファイルを適用して一括設定する

設定ファイル（SYLKファイル）に記載した IPアドレスを、一括してスキャナーに割り当てます。あらかじめ設定ファイルを作成しておきます。

1. LANケーブルで全てのデバイスをネットワークに接続します。
2. スキャナーの電源を入れます。
3. EpsonNet Configを起動します。
ネットワーク上のスキャナーが一覧表示されます。表示に時間がかかることがあります。
4. [ツール] - [一括設定] をクリックします。
5. [開く] をクリックします。
6. ファイル選択画面で、設定値を記述した SYLK ファイル（拡張子.slk）を選択してから、[開く] をクリックします。

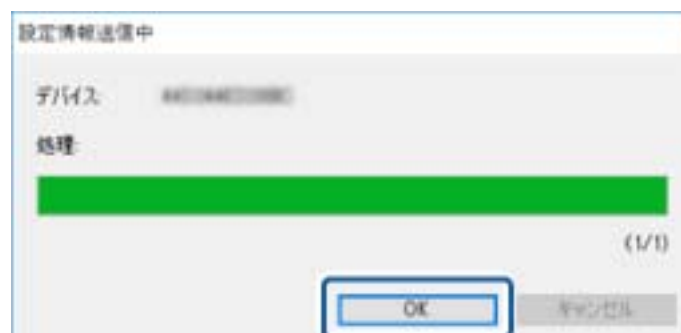
7. 【状況】の欄が【未割当】、【処理ステータス】が【割当成功】となっているデバイスの中から、一括設定するデバイスを選択します。
複数選択するときは、マウスでドラッグするか、CtrlキーまたはShiftキーを押したままクリックして選択します。



8. 【送信】をクリックします。
9. パスワード入力画面が表示されたときは、パスワードを入力して【OK】をクリックします。
設定が送信されます。

！重要 プログレスバーが終了するまではネットワークインターフェイスに情報が送られています。デバイスまたは無線アダプターの電源を切ったり、データをデバイスに送ったりしないでください。

10. 【設定情報送信中】画面で【OK】をクリックします。



11. 設定したデバイスの状況を確認します。

 や  が表示された デバイスは、設定ファイルの記載内容やデバイスが正常に再起動したか確認してください。

アイコンの 状態	状況	処理ステータス	説明
	設定完了	設定成功	正常に設定が完了しました。
	設定完了	復帰確認中	情報を送信すると設定を有効にするために各デバイスが再起動されます。再起動後正常に接続できるか確認しています。
	設定完了	復帰確認失敗	設定送信後にデバイスが確認できません。デバイスの電源が入っているか、正常に再起動したか確認してください。
	設定完了	探索中	設定ファイルに記載されているデバイスを探索中です。*
	設定完了	探索失敗	既に設定が完了したデバイスが確認できません。デバイスの電源が入っているか、正常に再起動したか確認してください。*

*：設定情報表示時のみ

関連情報

- ➔ [「EpsonNet Configの起動 - Windows」 54ページ](#)
- ➔ [「EpsonNet Configの起動 - Mac OS」 54ページ](#)

IPアドレスを個別に設定する

EpsonNet ConfigでスキャナーのIPアドレスを設定します。

1. スキャナーの電源を入れます。
2. LANケーブルでスキャナーをネットワークに接続します。
3. EpsonNet Configを起動します。
ネットワーク上のスキャナーが一覧表示されます。表示に時間がかかることがあります。
4. 設定するスキャナーをダブルクリックします。

 同じ製品名のスキャナーを複数台接続した場合は、MACアドレスで識別できます。

5. 左のメニューから【ネットワーク】 - 【TCP/IP】 - 【基本】 を選択します。

6. [IPアドレス]、[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。



参考 セキュアなネットワークにスキャナーを接続する場合は、固定アドレスを設定してください。

7. [送信] をクリックします。

設定情報の送信を確認する画面が表示されます。

8. [OK] をクリックします。

送信完了の画面が表示されます。

参考 「設定は正常に更新されました。」のメッセージが表示されるまではデバイスに情報を送っています。デバイスの電源を切ったり、データをデバイスに送ったりしないでください。

9. [OK] をクリックします。

関連情報

- ➔ [「EpsonNet Configの起動 - Windows」 54ページ](#)
- ➔ [「EpsonNet Configの起動 - Mac OS」 54ページ](#)

スキャナーが使用するポート

スキャナ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）	使用する	送信先（サーバー）	プロトコル	ポート番号
スキャナー	メール送信（メール通知）	SMTPサーバー	SMTP（TCP）	25
			SMTP SSL/TLS（TCP）	465
			SMTP STARTTLS（TCP）	587
	POP before SMTP接続（メール通知）	POPサーバー	POP3（TCP）	110
	WSDの制御	クライアントコンピューター	WSD（TCP）	5357
	Document Capture Proからのブッシュスキャン時のコンピューター探索	クライアントコンピューター	Network Push Scan Discovery	2968
クライアントコンピューター	Document Capture Proからのブッシュスキャン時のジョブ情報取得	クライアントコンピューター	Network Push Scan	2968
	EpsonNet Configなどのアプリケーションソフト、スキャナードライバーからのスキャナー探索	スキャナー	ENPC（UDP）	3289
	EpsonNet Configなどのアプリケーションソフト、スキャナードライバーからのスキャナーMIB情報の取得と設定	スキャナー	SNMP（UDP）	161
	WSDのスキャナー探索	スキャナー	WS-Discovery（UDP）	3702
	Document Capture Proからのスキャンデータの転送	スキャナー	Network Scan（TCP）	1865

操作パネルの管理者用設定メニュー

（ ）は初期値です。

〔設定〕 - 〔機器情報〕

スキャン枚数リセット			
------------	--	--	--

〔設定〕 - 〔外部スキャン設定〕

超音波重送検知			（オフ）
低速モード			（オフ）
設定クリア			

〔設定〕 - 〔共通設定〕

付録

画面の明るさ設定			(9)
音の設定	操作音		(中)
	エラー音		(中)
スリープ移行時間設定			(10分)
自動電源オフ設定			(設定しない)
日付/時刻設定	日付/時刻		
	日付設定		
	時差		
言語選択/Language			(日本語)
無操作タイムアウト			(オン) (3分)
コンピューターのUSB 接続			
設定クリア			

[設定] - [管理者用設定]

管理者設定	管理者パスワード	新規設定	
		変更	
		設定クリア	
	管理者ロック		(オフ)
	認証設定		(オフ)
WSD設定			(オフ)
購入時の設定に戻る			

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

ネットワークにデバイスを接続すると、離れた場所からアクセスして使用できます。また、デバイス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。

リスクを回避するため、エプソン製デバイス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
SSL/TLS通信	SSL/TLS通信でコンピューターとデバイスの通信経路を暗号化します。ブラウザ経由の通信の内容が保護されます。	CA局より取得したサーバー用のCA証明書をデバイスに設定します。	コンピューターからデバイスへの設定情報やデータ内容の漏えいが防げます。また、ファームウェアアップデートなど、デバイス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場合も保護されます。
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、セキュアでないスキャン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、デバイス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。	デバイスへの不正アクセス、通信データの傍受や改ざんを防止できます。
SNMPv3	ネットワークで接続されたデバイスの監視、制御するSNMPプロトコルにデータの整合性、暗号化、ユーザー認証などの機能が追加されています。	SNMPv3を有効にして、認証や暗号化の方法を設定します。	ネットワーク経由での設定変更や、状態監視での機密性が確保できます。
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デバイス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。	不正なデバイスへのアクセスや使用を防止できます。
IDカード認証	デバイスに接続した認証装置にIDカードをかざすと、登録された利用者がデバイスを使用できるようになります。デバイスや利用者別の履歴の取得、利用者や所属ごとに使用できるデバイス、機能の制限を設定できます。	デバイスに認証装置を接続して、認証システム内で利用者の情報を設定します。	デバイスの不正使用、なりすましを防止できます。

関連情報

- ➔ [「スキャナーとのSSL/TLS通信」 62ページ](#)
- ➔ [「IPsec/IPフィルタリングで暗号化通信する」 70ページ](#)
- ➔ [「SNMPv3プロトコルを利用する」 82ページ](#)
- ➔ [「IEEE802.1X環境にスキャナーを接続する」 84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。

スキャナーとのSSL/TLS通信

SSL/TLS (Secure Sockets Layer/Transport Layer Security) 通信でスキャナ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は、CA局に申請して発行してもらいます。信頼性のあるCA局の証明書を使用すると、データ通信の安全が確保できます。CA署名証明書は、取得した各セキュリティ機能だけでなく、他の機能でも使用できます。
- CA証明書
CA署名証明書のチェーンやチェーン内の証明書です。接続相手サーバーの検証に使用できます。相手サーバーの証明書を発行したCA局から入手します。
- 自己署名証明書
スキャナーが自ら発行し署名した証明書です。証明書としては信頼性がなく、なりすましは防げません。また、SSL通信をすると、ブラウザからセキュリティ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」 63ページ](#)
- ➔ [「CA署名証明書を削除する」 66ページ](#)
- ➔ [「自己署名証明書を更新する」 67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[ネットワークのセキュリティ設定]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. [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。

インポートされると完了メッセージが表示されます。

5. [ネットワークのセキュリティ設定] 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。



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、スキャナ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。

関連情報

- ➡ [「Web Configの起動」 21ページ](#)
- ➡ [「CSRの設定項目」 64ページ](#)
- ➡ [「CA署名証明書をインポートする」 64ページ](#)

CSRの設定項目

アイテム	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。 設定例： Web ConfigにアクセスするURL：https://10.152.12.225 コモンネーム：10.152.12.225
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。

関連情報

➡ [「CA署名証明書を取得する」63ページ](#)

CA署名証明書をインポートする

- ！重要**
- スキャナ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。
 - 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[ネットワークのセキュリティ設定]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。

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] : スキャナ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。



「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」 21ページ](#)
- ➡ [「CA署名証明書のインポート設定項目」 66ページ](#)

CA署名証明書のインポート設定項目

EPSON

管理者ログオフ

情報確認

製品情報

ネットワーク情報

パネルのスナップショット

メンテナンス情報

ハードウェア情報

スキャナー設定

ネットワーク設定

ネットワークのセキュリティ設定

SSL/TLS

基本

証明書

IPsec/IPフィルタリング

IEEE802.1X

相手サーバー検証用CA証明書

利用サービス

システム設定

設定のエクスポート/インポート

管理者設定

基本設定

DNS/プロキシ

ファームウェアアップデート

ルート証明書更新

製品情報

ネットワークのセキュリティ設定 > SSL/TLS > 証明書

サーバー証明書:

証明書 (PEM/DER)

Browse...

secret.pem

秘密鍵:

Browse...

secret.pem

パスワード:

CA証明書1:

Browse...

ca_certificate.pem

CA証明書2:

Browse...

ca_certificate.pem

※証明書をインポートするときは、HTTPSで暗号化して通信することをお勧めします。

設定

戻る

アイテム	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。
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	秘密鍵暗号化のため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」 64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、一度削除してしまう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 [ネットワークのセキュリティ設定] 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。

関連情報

➡ [\[Web Configの起動\] 21ページ](#)

自己署名証明書を更新する

HTTPSサーバー機能を搭載しているスキャナーは自己署名証明書の更新ができます。自己署名証明書を使用すると、Web Configの起動時に警告のメッセージが表示されます。

自己署名証明書は、CA署名証明書を取得しインポートするまでの期間中一時的に使用することをお勧めします。

1. Web Configで [ネットワークのセキュリティ設定] - [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。

スキャナーにアクセスするIPアドレスやFQDN名などの識別子を入力します。1～128文字以内で入力できます。

参考 識別名 (DN) はカンマで分割できます。

4. 証明書の有効期間を選択します。

EPSON

管理者ログアウト

情報確認

製品情報

ネットワーク情報

パネルのスナップショット

メンテナンス情報

ハードウェア情報

スキャナー設定

ネットワーク設定

ネットワークのセキュリティ設定

SSL/TLS

基本

証明書

IPsec/IPフィルタリング

IEEE802.1X

相手サーバー検証用CA証明書

利用サービス

システム設定

設定のエクスポート/インポート

管理者設定

基本設定

DNS/プロキシ

ファームウェアアップデート

ルート証明書更新

製品情報

ネットワークのセキュリティ設定 > SSL/TLS > 証明書

公開鍵長: RSA 2048bit - SHA-256

コモンネーム: EPSONXXXXXX.EPSONXXXXXX.local, 192.0.2.111

組織名: SEIKO EPSON CORP.

有効期間開始日時 (UTC): 2017-02-21 06:50:28 UTC

有効期間 (年): 10

次へ 戻る

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。

設定がスキャナーに反映されます。

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」 21ページ](#)

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証明書のインポート、表示、削除ができます。

相手サーバー検証用CA証明書をインポートする

1. Web Configで[ネットワークのセキュリティ設定] - [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。

関連情報

➡ [「Web Configの起動」 21ページ](#)

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「ネットワークのセキュリティ設定」 - 「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。

管理者ログオフ

情報確認

製品情報

ネットワーク情報

パネルのスナップショット

メンテナンス情報

ハードウェア情報

スキャナー設定

ネットワーク設定

ネットワークのセキュリティ設定

SSL/TLS

IPsec/IPフィルタリング

IEEE802.1X

相手サーバー検証用CA証明書

利用サービス

システム設定

設定のエクスポート/インポート

管理者設定

基本設定

DNS/ブロキシ

ファームウェアアップデート

ルート証明書更新

製品情報

ネットワークのセキュリティ設定 > 相手サーバー検証用CA証明書

証明書のインポートや削除をすぐに通信に反映するには[ネットワーク再起動]を押してください。
他の機能の設定や、本体の再起動でも、この設定が通信に反映されることがあります。

No.	Certificate Data	Action
1	Version: 3 (0x2) Serial Number:	削除
2		インポート
3		インポート
4		インポート
5		インポート
6		インポート
7		インポート
8		インポート
9		インポート
10		インポート

ネットワーク再起動

3. 確認のメッセージを確認して、削除します。

関連情報

➡ 「Web Configの起動」 21ページ

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搭載したスキャナーでは、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。フィルタリングのために基本ポリシーを設定します。基本ポリシーはスキャナ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。個別ポリシーは、スキャナ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スキャナ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。

参考 Windows Vista以降またはWindows Server 2008以降のWindowsは、IPsecに対応しています。

基本ポリシーを設定する

1. Web Configで「ネットワークのセキュリティ設定」 - 「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。
設定がスキャナーに反映されます。

関連情報

- ➡ 「Web Configの起動」 21ページ
- ➡ 「基本ポリシーの設定項目」 71ページ

基本ポリシーの設定項目

EPSON

管理者ログオフ

情報確認

製品情報

ネットワーク情報

パネルのスナップショット

メンテナンス情報

ハードウェア情報

スキャナー設定

ネットワーク設定

ネットワークのセキュリティ設定

SSL/TLS

IPsec/IPフィルタリング

基本

クライアント証明書

IEEE802.1X

相手サーバー検証用CA証明書

利用サービス

システム設定

設定のエクスポート/インポート

管理者設定

基本設定

DNS/プロキシ

ファームウェアアップデート

ルート証明書更新

製品情報

ネットワークのセキュリティ設定 > IPsec/IPフィルタリング > 基本

ポリシー適用の優先順位
個別ポリシー1 > 個別ポリシー2 > ... 個別ポリシー10 > デフォルトポリシー

基本ポリシー 1 2 3 4 5 6 7 8 9 10

IPsec/IPフィルタリング: ☒ 有効 ☐ 無効

デフォルトポリシー

通信処理: IPsecの使用

IKEバージョン: ☒ IKEv1 ☐ IKEv2

認証方式: 事前共有キー

事前共有キー:

事前共有キー確認入力:

カプセル化: トランスポートモード

リモートゲートウェイアドレス(トンネルモード):

セキュリティプロトコル: ESP

アルゴリズム設定

IKE

暗号化アルゴリズム: 任意

認証アルゴリズム: 任意

鍵交換アルゴリズム: 任意

ESP

アイテム	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。

エンタープライズセキュリティ設定編

アイテム	設定値と説明	
通信処理	IP通信の制御方法を設定します。	
	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 のバージョンをIKEv1とIKEv2から選択します。 スキャナ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。	
	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が設定できます。
	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。	
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、スキャナーを何のIDで認証させるか選択します。
	ID	IDの種類に合わせてスキャナーの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 (1 x 20～0x7E) 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 (0 x 20～0x7E) 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 (0 x 20～0x7E) 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。

アイテム	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の種類に合わせてスキャナーの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。	
	トランスポートモード	主に同じLAN内だけでスキャナーと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スキャナ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。	
	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		
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。

アイテム	設定値と説明	
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」71ページ](#)

個別ポリシーを設定する

1. Web Configで【ネットワークのセキュリティ設定】 - 【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。
設定がスキャナーに反映されます。

関連情報

➡ [「Web Configの起動」21ページ](#)
➡ [「個別ポリシーの設定項目」75ページ](#)

個別ポリシーの設定項目

EPSON

管理者ログオフ

情報確認

製品情報

ネットワーク情報

パネルのスナップショット

メンテナンス情報

ハードウェア情報

スキャナー設定

ネットワーク設定

ネットワークのセキュリティ設定

SSL/TLS

IPsec/IPフィルタリング

基本

クライアント証明書

IEEE802.1X

相手サーバー検証用CA証明書

利用サービス

システム設定

設定のエクスポート/インポート

管理者設定

基本設定

DNS/プロキシ

ファームウェアアップデート

ルート証明書更新

製品情報

ネットワークのセキュリティ設定 > IPsec/IPフィルタリング > 基本

ポリシー適用の優先順位
個別ポリシー1 > 個別ポリシー2 > ... 個別ポリシー10 > デフォルトポリシー

基本ポリシー 1 2 3 4 5 6 7 8 9 10

この個別ポリシーを有効にする

通信処理: IPsecの使用

ローカルアドレス (スキャナー): 使用可能な全てのアドレス

リモートアドレス (ホスト):

ポート指定方法: ポート番号

サービス名:

☐ 全て

☐ ENPC

☐ SNMP

☐ LPR

☐ RAW (Port9100)

☐ IPP/PPS

☐ WSD

☐ WS-Discovery

☐ Network Scan

☐ Network Push Scan

☐ Network Push Scan Discovery

☐ FTP データ (ローカル)

☐ FTP 制御 (ローカル)

☐ FTP データ (リモート)

☐ FTP 制御 (リモート)

☐ CIFS (ローカル)

☐ CIFS (リモート)

☐ NetBIOS Name Service (ローカル)

☐ NetBIOS Datagram Service (ローカル)

☐ NetBIOS Session Service (ローカル)

☐ NetBIOS Name Service (リモート)

☐ NetBIOS Datagram Service (リモート)

☐ NetBIOS Session Service (リモート)

アイテム	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	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 (スキャナー)	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。スキャナーの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。	
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。	

エンタープライズセキュリティ設定編

アイテム	設定値と説明	
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。	
	全てのプロトコル	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] か [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。 設定例: 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] か [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。 設定例: 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 のバージョンをIKEv1とIKEv2から選択します。 スキャナ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。	
	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が設定できます。
	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。	

アイテム	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、スキャナーを何のIDで認証させるか選択します。
	ID	IDの種類に合わせてスキャナーの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が設定できます。
	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の種類に合わせてスキャナーの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が設定できます。
	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。

アイテム	設定値と説明	
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。	
	トランスポートモード	主に同じLAN内だけでスキャナーと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スキャナ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。	
	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		
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」 74ページ](#)
- ➡ [「ローカルアドレス（スキャナー）とリモートアドレス（ホスト）の組み合わせ」 79ページ](#)
- ➡ [「個別ポリシーのサービス名一覧」 79ページ](#)

ローカルアドレス（スキャナー）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（スキャナー）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	EpsonNet Configなどのアプリケーションソフト、スキャナードライバーからのスキャナー探索
SNMP	UDP	161	任意	EpsonNet Configなどのアプリケーションソフト、スキャナードライバーからのスキャナーMIB情報の取得と設定
WSD	TCP	任意	5357	WSDの制御
WS-Discovery	UDP	3702	任意	WSDのスキャナー探索
Network Scan	TCP	1865	任意	Document Capture Proからのスキャンデータの転送
Network Push Scan Discovery	UDP	2968	任意	スキャナーからのコンピューター探索
Network Push Scan	TCP	任意	2968	Document Capture Pro、Document Captureからのプッシュスキャン時のジョブ情報取得

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、基本ポリシーのみ使われます。

〔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

Epson Scan 2を使用したスキャンとスキャナー設定を受け付ける

指定したサービスからのスキャンデータとスキャナ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)〕：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〕、〔Network Scan〕、〔HTTP (ローカル)〕、〔HTTPS (ローカル)〕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、スキャナ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。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[ネットワークのセキュリティ設定] - [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てください。

IEEE802.1XまたはSSL/TLSで、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] 21ページ
- ➡ [CA署名証明書の取得とインポート] 63ページ

SNMPv3プロトコルを利用する

SNMPv3の概要

SNMPはネットワークに接続されたデバイスの情報を収集して監視や制御を行うためのプロトコルで、SNMPv3は管理セキュリティ機能が強化されたバージョンです。

SNMPv3 を使うと、対応する機器管理ツールとの状態監視や設定変更のSNMP通信（パケット）を認証・暗号化でき、盗聴やなりすまし、改ざんなどネットワークからのリスクからSNMP通信（パケット）を守ることができます。

SNMPv3を設定する

スキャナーがSNMPv3プロトコルに対応している場合、スキャナーへのアクセスを監視・制御できます。

1. Web Configで【利用サービス】 - 【プロトコル】 を選択します。
2. 【SNMPv3設定】 の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。
設定がスキャナーに反映されます。

関連情報

- ➡ [「Web Configの起動」 21ページ](#)
- ➡ [「SNMPv3の設定項目」 83ページ](#)

SNMPv3の設定項目

The screenshot shows the 'SNMPv3設定' (SNMPv3 Settings) page in the Epson management interface. The left sidebar contains a navigation menu with categories like '情報確認' (Information Confirmation), 'システム設定' (System Settings), and '基本設定' (Basic Settings). The main content area is divided into sections for 'SNMPv1/v2c設定' (SNMPv1/v2c Settings) and 'SNMPv3設定' (SNMPv3 Settings). In the 'SNMPv3設定' section, the 'SNMPv3を有効にする' (Enable SNMPv3) checkbox is checked. Below this, the 'ユーザー名' (Username) is set to 'admin'. The '認証設定' (Authentication Settings) section includes 'アルゴリズム' (Algorithm) set to 'MD5', and fields for 'パスワード' (Password) and 'パスワード確認入力' (Password Confirmation Input). The '暗号化設定' (Encryption Settings) section includes 'アルゴリズム' (Algorithm) set to 'DES', and fields for 'パスワード' (Password) and 'パスワード確認入力' (Password Confirmation Input). At the bottom, the 'コンテキスト名' (Context Name) is set to 'EPSON'. A '次へ' (Next) button is located at the bottom right of the settings area.

アイテム	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字以内で入力します。
認証設定	
アルゴリズム	認証用のアルゴリズムを選択します。
パスワード	ASCII (0x20-0x7E)で表せる8～32文字以内で入力します。
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	暗号化用のアルゴリズムを選択します。
パスワード	ASCII (0x20-0x7E)で表せる8～32文字以内で入力します。
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	1バイト文字を使って1～32字以内で入力します。

関連情報

➡ [「SNMPv3を設定する」 82ページ](#)

IEEE802.1X環境にスキャナーを接続する

IEEE802.1Xを設定する

IEEE802.1Xに対応しているスキャナーは、認証機能を持ったネットワーク（RADIUSサーバーと認証機能を持ったハブに接続されたネットワーク）環境に接続して使用できます。

1. Web Configで「ネットワークのセキュリティ設定」 - 「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。
設定がスキャナーに反映されます。

関連情報

- ➡ [「Web Configの起動」 21ページ](#)
- ➡ [「IEEE802.1Xの設定項目」 85ページ](#)
- ➡ [「IEEE802.1Xを設定したのにつながらない」 90ページ](#)

IEEE802.1Xの設定項目

EPSON

管理者ログオフ

情報確認

製品情報

ネットワーク情報

パネルのスナップショット

メンテナンス情報

ハードウェア情報

☑ スキャナー設定

☑ ネットワーク設定

☑ ネットワークのセキュリティ設定

☑ SSL/TLS

☑ IPsec/IPフィルタリング

☐ IEEE802.1X

基本

クライアント証明書

相手サーバー検証用CA証明書

☑ 利用サービス

☑ システム設定

☑ 設定のエクスポート/インポート

☑ 管理者設定

基本設定

DNS/プロキシ

ファームウェアアップデート

ルート証明書更新

製品情報

ネットワークのセキュリティ設定 > IEEE802.1X > 基本

IEEE802.1X (有線LAN) : ☒ 有効 ☐ 無効

認証方式 : EAP-TLS

ユーザーID :

パスワード :

パスワード確認入力 :

サーバーID :

証明書の検証 : ☒ 有効 ☐ 無効

Anonymous名 :

暗号強度 : 標準

次へ

アイテム	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	スキャナーと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	
	PEAP/MSCHAPv2	パスワードを設定する必要があります。
ユーザーID	RADIUSサーバーの認証に使うIDを設定します。 ASCII (1 x 20～0x7E) 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	スキャナーを認証するためのパスワードを設定します。 ASCII (1 x 20～0x7E) 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 (0 x 20～0x7E) で表せる1バイト文字で0～128文字以内で入力します。	

アイテム	設定値と説明	
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てください。	
Anonymous名	[認証方式] が [PEAP-TLS] または [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」 84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。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 [ネットワークのセキュリティー設定] - [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た場合はコピーできます。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」 21ページ](#)
- ➔ [「CA署名証明書の取得とインポート」 63ページ](#)

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. [設定] - [ネットワーク設定] の順にタップします。
2. [設定を変更する] をタップします。
3. 無効にしたい機能をタップします。
 - [IPsec/IPフィルタリング]
 - [IEEE802.1X]
4. 設定完了のメッセージが表示されたら [設定開始] をタップします。

Web Configからのセキュリティ機能の初期化

IEEE802.1Xの場合はデバイスがネットワーク上で認識できなくなる可能性があります。その場合はスキャナーの操作パネルから機能を無効にしてください。

IPsec/IPフィルタリングの場合、コンピューターからアクセスできれば無効に設定できます。

IPsec/IPフィルタリングを無効化する

1. Web Configで [ネットワークのセキュリティ設定] - [IPsec/IPフィルタリング] - [基本] を選択します。
2. [基本ポリシー] の [IPsec/IPフィルタリング] の [無効] を選択します。
3. [次へ] をクリックして、全てのグループポリシーの [この個別ポリシーを有効にする] のチェックを外します。
4. [設定] をクリックします。

関連情報

➡ [「Web Configの起動」 21ページ](#)

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

Web Configでキーを設定し直してください。

Web Configの [ネットワークのセキュリティ設定] - [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、相手先のコンピューターの事前共有キーも設定してください。

関連情報

➡ [「Web Configの起動」 21ページ](#)

IPsec通信ができない

コンピューターの設定でサポートしていないアルゴリズムを指定していませんか？

スキャナーがサポートするアルゴリズムは以下の通りです。

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」70ページ](#)

突然通信ができなくなった

スキャナーのIPアドレスが変更または使用不可になっていませんか？

スキャナーの操作パネルからIPsecを無効にしてください。

Web Configの [ネットワークのセキュリティ設定] - [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 (スキャナー)] 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アドレスが変更または使用不可になっていませんか？

スキャナーの操作パネルからIPsecを無効にしてください。

Web Configの [ネットワークのセキュリティ設定] - [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」21ページ](#)

➡ [「IPsec/IPフィルタリングで暗号化通信する」 70ページ](#)

IPsec/IPフィルタリング設定したのにつながらない

設定が間違っている可能性があります。

スキャナ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。スキャナ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」 70ページ](#)

IEEE802.1Xを設定したのにつながらない

設定が間違っている可能性があります。

スキャナーの操作パネルからIEEE802.1Xを無効にしてください。スキャナ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」 84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ますか？

CA署名証明書とCSRは、不一致の情報の場合インポートできません。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ていませんか？
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、スキャナーに保存されているCSRを再生成しましたか？
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を超えていませんか？

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は正しいですか？

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。

関連情報

➡ [「CA署名証明書をインポートする」 64ページ](#)

自己署名証明書が更新できない

コモンネームが未入力ではありませんか？

〔コモンネーム〕は必ず入力してください。

コモンネームに入力可能な文字以外（例：日本語）を入力していませんか？

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を使用していませんか？

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」67ページ](#)

CSRが作成できない

コモンネームが未入力ではありませんか？

〔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、都道府県名に入力可能な文字以外を入力していませんか？例えば日本語は使えません。

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を使用していませんか？

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」63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。

メッセージ	原因と対処
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のみ入力されています。 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。
日付/時刻が設定されていません。	原因： スキャナーに日付や時刻が設定されていません。 対処： Web ConfigやEpsonNet Config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、スキャナ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： スキャナ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」 62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ありますか？

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」 66ページ](#)

➡ [「CA署名証明書をインポートする」 64ページ](#)