

# Embedded Web Server RX 操作手順書



## 使用条件

本書のすべて、または一部を許可なく複製することは禁じられています。

本書に含まれる情報は、性能改善のため、予告なく変更される場合があります。

本書に使用している製品の画面などは、使用するプリントシステムによって、本書と異なる場合があります。

本書で説明されている操作は、Windows 7 の印刷環境での操作を例としていま す。操作方法は Microsoft Windows 10, Windows 8.1、Windows 8、Windows Vista、 Windows XP、Windows Server 2012、Windows Server 2008、Windows Server 2003 環境でも基本的に同じです。

ここに記載された情報には関係なく、本製品の使用に伴って生じたいかなる問 題にも、当社は責任を負いません。

## 商標について

Microsoft Windows は、米国またはその他の国における Microsoft Corporation の商 標です。KPDL は、Kyocera Corporation の商標です。PCL は、Hewlett-Packard Company の商標です。Google および Google Cloud Print<sup>™</sup> は Google Inc. の商標ま たは登録商標です。

⑦ および QISO は、理想科学工業株式会社の登録商標または商標です。

本書で使用されているその他のブランド名および製品名はすべて、それを所有 する各企業の登録商標または商標です。

# 目次

1 はじめに	1
動作環境	1
エンベデッドサーバーへのアクセス	1
2 エンベデッドサーバーのホームページ	2
ログイン	2
トップバー	3
ナビゲーションメニュー	4
各種状態	5
3 ログインについて	6
ログインの認証方式	6
4 文書ボックス	7
ジョブボックス設定	7
5 デバイス設定	8
用紙 / 給紙 / 出力	8
節電 / タイマー	9
日付 / 時刻 1	10
システム	11
6 機能設定 1	3
共通 / ジョブ初期値	13
プリンター	14
メール	16
7 ネットワーク設定2	20
基本	20
TCP/IP	21
プロトコル	28
8 セキュリティー設定 3	12
デバイスセキュリティー	32
ネットワークセキュリティー	34
証明書	36
9 管理設定	8

部門管理	38
認証	40
通知 / レポート	41
履歴設定	42
SNMP	42
リセット	44

10	トラブルシューテ	ィング	•	45
10	トラブルシューテ	ィング	•	45

トラブルシューティング45
---------------

## 1 はじめに

Embedded Web Server RX (Remote eXtension)、以下エンベデッドサーバーは、プリント システムに組み込まれた Web サーバーです。プリントシステムの状況や設定内容の 確認、セキュリティー関連の設定、ネットワーク印刷、電子メールの送信などが可能 です。

エンベデッドサーバーによって、管理者は用紙やトナーの使用状況や、装着されたオ プション機能を確認することができます。エンベデッドサーバーは、デバイス設定の 構成、ジョブの監視、文書ボックスおよびアドレス帳を管理し、本体操作パネル同様 に設定が可能です。

## 動作環境

エンベデッドサーバーは次の環境で動作します。使用する前に確認してください。

### プロトコル

- TCP/IP プロトコルが PC にインストールされている。
- プリントシステムに IP アドレスが設定されている。

#### Web ブラウザー

- Microsoft Internet Explorer 8.0 以降 (Microsoft Internet Explorer は Microsoft Windows XP/Vista/7/8/8.1/10 および Microsoft Windows Server 2003/2008/2012 で動作します。)
- Mozilla Firefox 14.0 以降
- Safari 5.0 以降(Safari は Apple Mac OS X 10.4 以降で動作します。)
- Google Chrome 21.0 以降

## エンベデッドサーバーへのアクセス

ブラウザーのアドレス欄に、プリントシステムのホスト名、または IP アドレスを入 カしてエンターキーを押します。IP アドレスは、ネットワーク管理者から入手してく ださい。ここでは、Microsoft Internet Explorer を使用した場合を例として説明します。

- 1. ブラウザーを開きます。
- プリントシステムのホスト名、または IP アドレスを入力します。ホスト名を使用する 場合は、あらかじめ DNS サーバーを設定する必要があります。 (例:https://192.168.10.1)

「この Web サイトのセキュリティ証明書には問題があります」の画面が表示された場合、証明書の設定をしてください。詳細は、36ページの証明書を参照してください。または、証明書を設定しないでこのまま続行することもできます。

エンベデッドサーバーのホームページが表示されます。

ホームページのログイン欄にユーザー名とパスワードを入力します。初回ログイン時 はユーザー名、パスワードとも、Admin と入力すると、すべてのページにアクセスで きます。これは工場出荷時に設定されているものです。 2 エンベデッドサーバーのホーム ページ

エンベデッドサーバーのホームページでは、左列のナビゲーションメニューによって 各カテゴリーごとに設定値の確認や変更ができる他、右列ではナビゲーションメ ニューの選択状況に応じて、現在のユーザーや消耗品の情報などが表示されます。

		स न म	デル名:LP4040DN スト名:NM1062E8 駅:
<u> 赤ーム</u>	日本語	▼ 自動更新	最終更新: 2015/10/21 15:50:25
管理者ログイン	デバイス状況	1570	
	テルイス	√次 ● 準備中	ਾਟੱਤ.
ロヴイン	♂ 状況表示	<sup>©</sup>	中です。
デバイス情報	用紙	_	
ジョブ状況 >	給紙元 サイズ カセット1 A4	種類     容量       ●     普通紙     500	状况 30 %
	手差しトレイ A4-R	] 普通紙 100	用紙なし
	トナー		
	色     状況       ブラック	66%	
	────────────────────────────────────		

## ログイン

エンベデッドサーバーのすべてのページにアクセスするには、ユーザー名とパスワードを入力し、ログインする事が必要です。管理者権限を持つユーザでログインすると、文書ボックスやアドレス帳管理、デバイス設定などを含め、ナビゲーションメニュー上の全ページの操作が可能です。

					モ: ホ) 場)	デル名:LP4040DN スト名:NM1062E8 所:	
▲ ▲		日本語	•	■ 自動更新	_	最終更新: 2015/10/21 15:39:44	C
Section Admin		デバイス状況				_	
በሻፖንት		デバイス		状況	準備中"	ेंचे.	
		<b>状况表示</b>		۲	スリーフ。中	ਾਟਾਰ.	
三子デバイス情報	>	用紙				_	
ジョブ状況	>	給紙元 サイズ	種	類 容量 新紙 500		状況	
全主文書ボックス	>	チ差しトレイ A4-R		é通紙 100			
デバイス設定	>			_	_	r	_
機能設定	>	トナー 色 状況	-	-	-	_	-
ネットワーク設定	>	ブラック		66%			
1000000000000000000000000000000000000	>	廃棄トナー 正常					
管理設定	>						

エンベデッドサーバーへのアクセスに関しては、ネットワーク認証または部門管理の いずれかを使用して、ユーザーを選別することができます。詳細については、6ペー ジのログインについてを参照してください。

## トップバー

ホームページ最上部のトップバーでは、次の操作が可能です。

[ホーム]

他のページにも表示されるこの[ホーム]をクリックすると、簡単にホームページ (トップ画面)に戻ることができます。

#### [ 言語 ]

エンベデッドサーバーは、複数の言語による UI をサポートしています。言語を変 更するには、言語ドロップダウンリストをクリックし、適切な言語を選択します。 本機の操作パネルで使用されている言語と異なる言語を選択してエンベデッドサー バーを表示すると、一部の文字が正しく表示されない場合があります。

#### [自動更新]

エンベデッドサーバー画面を定期的に自動更新させるには、[自動更新]をチェック しておきます。

### 🧕 [ 更新 ]

バーの右端の丸い矢印アイコンをクリックすると、エンベデッドサーバー画面を随 時更新することができます。

### ナビゲーションメニュー

ホームページ左列のナビゲーションメニューには、各種機能にアクセスできるページ を表示させるバーがまとめられています。各バーをクリックする事により、次に説明 する各機能ごとのページへジャンプします。

[自分の情報]

[自分の情報]は、本機のユーザー認証がオンであり、エンベデッドサーバーに管理 者権限や一般ユーザー権限でログインした場合に表示されます。このページには ユーザーの設定に応じて、各種設定がまとめられています。閲覧できる範囲は、 ユーザーまたはグループの権限範囲に依存します。たとえば、ユーザーが文書ボッ クスを作成した場合、[自分の情報]内の文書ボックスを操作することが可能です。

[デバイス情報]

プリントシステム全体の各種情報が表示されます。[デバイス情報]をクリックする と、次のサブメニューが下に表示されます。 [構成]

機種情報(基本、識別情報、性能)、オプション機器の有無、ソフトウェアバー ジョン、およびネットワーク情報が表示されます。

[カウンター]

印刷ページ数、読み込みページ数が表示されます。[種類]ドロップダウンリスト で、表示させる印刷ページ数の種類を限定することができます。

[Embedded Web Server RX について]

バージョン情報、サポートされているブラウザーが表示されます。

[ジョブ状況]

印刷や送信ジョブ、保存ジョブ、予約ジョブ、およびジョブ履歴を含むすべてのデ バイスのジョブ情報が表示されます。[ジョブ状況]をクリックすると、次のサブメ ニューが下に表示されます。ユーザー権限によって、表示される項目が異なりま す。

[印刷ジョブ状況]

各ジョブ種類ごとに状況を表示します。表示画面を更新するには、[更新]をクリック します。表示されているジョブの処理を中止するには、[ジョブ中止]をクリックしま す。各ジョブ履歴の詳細を確認するには、そのジョブの[番号]または[ジョブ名]を クリックしてください。

[印刷ジョブ履歴]

各ジョブ種類ごとにジョブの履歴を表示します。履歴の一覧を更新するには、トッ プバー右端の[更新]をクリックします。各ジョブ履歴の詳細を確認するには、そ のジョブの[番号]または[ジョブ名]をクリックしてください。

[文書ボックス]

文書ボックスの追加や削除、または文書ボックス内の文書の削除など行います。[文 書ボックス]下には[ジョブボックス設定]があります。詳細については7ページの文 書ボックスを参照してください。

[デバイス設定]

本機の詳細設定を行います。[デバイス設定]下には[用紙/給紙/出力]、[[節電/ タイマー]、[日付/時刻]、[システム]があります。詳細については8ページのデ バイス設定を参照してください。

[機能設定]

機能の詳細設定を行います。[機能設定]下には[共通/ジョブ初期値]、[プリン ター]、[メール]、があります。詳細については13ページの機能設定を参照してく ださい。

[ネットワーク設定]

ネットワークの詳細設定を行います。[ネットワーク設定]下には[基本]、[TCP/ IP]、[プロトコル]があります。詳細については 20 ページのネットワーク設定を参 照してください。

[セキュリティー設定]

セキュリティーの詳細設定を行います。[セキュリティー設定]下には[デバイスセ キュリティー]、[ネットワークセキュリティー]、[証明書]があります。詳細につ いては 32ページのセキュリティー設定を参照してください。

[管理設定]

管理の詳細設定を行います。[管理設定]下には[部門管理]、[認証]、[通知/レ ポート]、[履歴設定]、[SNMP]、[リセット]、[リモートサービス]があります。詳 細については 38 ページの**管理設定**を参照してください。

#### 各種状態

ホームページは、右列にデバイス状況やユーザー状況、消耗品などの状態が表示され ます。プリントシステムの現在の設定を一覧で確認することができます。

[デバイス状況]

プリンターの動作状態を表示します。

[用紙]

給紙元ごとの用紙のサイズや種類、容量や残量を表示します。

[トナー]

トナー残量を表示します。また、廃棄トナーの状態を表示します。

## 3 ログインについて

このセクションでは、管理者がドメインおよびローカルユーザーを管理する方法について説明します。管理者は認証機能によって、ユーザーによるエンベデッドサーバーへのアクセス制限やパスワード設定などを実行できます。

### ログインの認証方式

管理者は、次に述べる2つの方法から認証方式を選択して、ユーザーごとに設定する ことができます。

ネットワーク認証を使用する場合は、ユーザー管理を有効にすることが必要です。

#### ネットワーク認証

ネットワーク認証を行うには、プリントシステムが、Windows ドメインネットワークの管理下にあることが前提条件です。[ユーザー名]と[パスワード]を入力し、ドロップダウンリストからログインするドメインを選択してください。

管理者権限でログインした場合は、ナビゲーションメニューには、[自分の情報], [デバイス情報],[ジョブ状況],[文書ボックス][デバイス設定],[機能設定],[ ネットワーク設定],[セキュリティー設定]、および[管理設定]が表示されます。

ー般ユーザーアカウントでログインした場合は、文書ボックスの追加や削除は行えず、[デバイス設定]、[機能設定]、[ネットワーク設定]、[セキュリティー設定]、および[管理設定]は表示されません。

ユーザーをネットワーク認証する方法については、40ページの認証を参照してください。

#### 部門管理による認証

認証設定が[オフ]で、部門管理が[オン]に設定されている場合は、部門 ID 入力 欄の上に[部門ログイン]および[管理者ログイン]が表示されます。部門管理 ID を[部門 ID]に入力し、[ログイン]をクリックします。

参考:管理者権限ユーザーでログインする場合は、[管理者ログイン]をクリックして ください。ユーザー名 とパスワードを入力し、[ログイン]をクリックします。

部門管理 ID を使用してアクセスすると、ナビゲーションメニューには、[自分の情報],[デバイス情報],[ジョブ状況]、および[文書ボックス]が表示されます。

## 4 文書ボックス

このページは、管理者権限や一般ユーザー権限でアクセスした場合に表示されます。 文書ボックスの新規追加や削除、また文書ボックス内の文書の削除を行います。一般 ユーザーアカウントの場合、文書の追加や削除は実行できません。

文書ボックスには、[ジョブボックス設定]があります。

ー般ユーザーアカウントを持つユーザーであっても、自身が作成した文書ボックス内 の文書を削除することは可能です。

## ジョブボックス設定

このセクションでは、ジョブボックス内のクイックコピージョブ保持数の設定と一時 保存文書の自動消去について説明します。印刷後に文書を保持するか、削除するかの 設定を選択することも可能です。

- ナビゲーションメニューの[文書ボックス]をクリックし、下に表示される[ジョブボックス設定]をクリックします。[ジョブボックス設定]ページが開きます。
- 2. [クイックコピージョブ保持数]の数値を入力します。0~300まで選択できます。
- 3. [再コピージョブ保持数]の数値を入力します。0~50まで選択できます。
- **4.** 一時保存文書の印刷後に自動的に消去するには、[一時保存文書の自動消去]のドロッ プダウンリストより、[1時間]、[4時間]、[1日]および[1週間]を選択します。 一時保存文書の印刷後に自動的に消去しないときには、[オフ]にします。
- 5. [設定]ボタンをクリックします。

## 5 デバイス設定

このページは、ネットワーク認証がオンの場合には、管理者権限でログイン(アクセス)した際に表示されます。

必要に応じて次の設定をしてください。詳細は下記を参照してください。

- 用紙 / 給紙 / 出力
- 原稿設定
- 節電 / タイマー
- 日付/時刻
- ・ システム

## 用紙 / 給紙 / 出力

このセクションでは各給紙力セットと手差しトレイにセットされている用紙のサイズ、種類、グループの設定、排紙先の設定および各種の詳細設定を行います。

#### カセット設定

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[用紙/給紙/ 出力]をクリックします。[用紙/給紙/出力設定]ページが開きます。
- 2. 各給紙カセットにセットする用紙種類を設定します。
- 3. [設定]ボタンをクリックします。

#### 手差しトレイ設定

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[用紙/給紙/ 出力]をクリックします。[用紙/給紙/出力設定]ページが開きます。
- 2. 手差しトレイにセットする用紙サイズと用紙種類を設定します。
- 3. [設定]ボタンをクリックします。

#### 排紙先設定

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[用紙/給紙/ 出力]をクリックします。[用紙/給紙/出力設定]ページが開きます。
- 2. 排紙先のトレイを設定します。
- 3. [設定]ボタンをクリックします。

### その他の設定

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[用紙/給紙/ 出力]をクリックします。[用紙/給紙/出力設定]ページが開きます。
- **2.** 次の設定ができます。

[優先給紙元]

優先して給紙するカセット、手差しトレイを選択できます。

[特定用紙種類の動作設定]

印刷方向に合わせるもしくは速度優先を選択できます。

**3.** [設定]ボタンをクリックします。

#### 用紙詳細設定

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[用紙/給紙/ 出力]をクリックします。[用紙/給紙/出力設定]ページが開きます。
- [用紙詳細設定]の[設定/登録]ボタンをクリックします。[用紙詳細設定]ページが開き ます。

次の設定ができます。

[カスタム用紙サイズ設定]

カスタム1(~4)の用紙サイズを指定できます。設定する場合はオンを選択し、[サイズ入力(X)]と[サイズ入力(Y)]の値を入力してください。

[用紙種類の設定]

各用紙の重さを設定できます。カスタム設定の場合、用紙の重さ、両面印刷の有 無、名前を設定できます。

3. [設定]ボタンをクリックします。

#### 節電/タイマー

このセクションでは節電モードおよびタイマーの詳細設定を行います。

#### 節電設定

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[節電/タイマー]をクリックします。[節電/タイマー設定]ページが開きます。
- 2. 次の設定ができます。
  - [スリープレベル]

[復帰優先]または[節電優先]から選びます。どちらを選んだ場合でも、操作パネル上のキーを押すか、本機が印刷ジョブを検知すると自動的に復帰し印刷を行います。

[復帰優先]は、[節電優先]よりもスリープモードから早く復帰します。

[節電優先]は、[復帰優先]よりもさらに消費電力を抑えた状態で、機能ごとにス リープモードを働かせるかを設定できます。また、スリープモードから使用可能な 状態へ復帰できる時間も[復帰優先]よりも遅くなります。

機種によっては、節電優先状態にエンベデッドウェブサーバー上に[スリープ中] ページが表示されます。この[スリープ中]画面の[起動]をクリックすることで も、スリープから復帰させることが可能です。

[スリープ条件]

節電優先モードを選択した場合は、インターフェイスまたはデバイス右側の[オン] のラジオボタンをクリックして、節電優先モードを適用したいインターフェイスま たはデバイスを選択します。特定のインターフェイスまたはデバイスに対して、節 電優先モードを適用したくない場合は、[オフ]をクリックしてください。たとえ ば、ネットワークからの印刷ジョブに対しては自動的にスリープ状態を解除し、印 刷を実行するには、[ネットワーク接続時]の右側の[オフ]のラジオボタンをク リックしておきます。

[スリープ時間]

本機が自動的にスリープ状態になるまでに時間を、1~240分の間で設定できます。

[電源オフ時間]

本機の電源が切れるまでの時間を、1時間~1週間の間で設定できます。

[電源オフ条件]

インターフェイスまたはデバイス右側の[オン]のラジオボタンをクリックして、 電源オフモードを適用したいインターフェイスまたはデバイスを選択します。特定 のインターフェイスまたはデバイスに対して、電源オフモードを適用したくない場 合は、[オフ]をクリックしてください。

3. [設定]ボタンをクリックします。

#### タイマー設定

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[節電/タイマー]をクリックします。[節電/タイマー設定]ページが開きます。
- 2. 次の設定ができます。

[オートパネルリセット]

自動的にパネルをリセットする設定をします。[オン]にすると、[パネルリセット時間]が表示され、パネルをリセットする時間を5~495秒の間で設定できます。

3. [設定]ボタンをクリックします。

### 日付/時刻

このセクションでは日付および時刻の詳細設定を行います。

#### 日付/時刻設定

 ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[日付/時刻] をクリックします。[日付/時刻設定]ページが開きます。

以下が表示されます。

[現在の時刻]

現在設定されている時刻を表示します。

[標準時(UTC/GMT)]

現在設定されているグリニッジ標準時を表示します。

2. 状況に応じて、次の設定ができます。

[日時], [年], [月], [日], [時刻], [日付形式], [時差]の各設定を選択してく ださい。

3. [設定]ボタンをクリックします。

#### 同期

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[日付/時刻] をクリックします。[日付/時刻設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

ネットワーク上の時刻サーバーを利用して時刻を取得し、定期的に正確な時刻が設定 できます。時刻サーバーのホスト名または IP アドレスを入力した後、[同期]ボタン をクリックします。

ホスト名を使用する場合は、あらかじめ DNS サーバーを設定する必要があります。

時刻は、各種レポートを本機からのメールとして送信するのに必要です。レポート メールの設定を行っている場合は、時刻を正しく設定することをお勧めします。

3. [設定]ボタンをクリックします。

## システム

このセクションではシステムの詳細設定を行います。

\*:このマークが付いている設定を変更した場合、デバイスまたはネットワークの再 起動が必要です。再起動は[リセット]のページで行ってください。

#### デバイス情報

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[システム] をクリックします。[システム設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

[ホスト名]、[固定資産番号]、[場所]の情報を入力してください。

ホスト名を使用する場合は、あらかじめ DNS サーバーを設定する必要があります。

3. [設定]ボタンをクリックします。

#### 基本

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[システム] をクリックします。[システム設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。
  - [言語選択]

使用言語を選択してください。

[RAM ディスクモード]

RAM ディスクの使用の有無を設定します。

[RAM ディスクサイズ]

RAM ディスクの容量を設定します。

[USB キーボードの種類]

該当するタイプを選択してください。

[A4/Letter の共通仕様]

A4 サイズと Letter サイズの用紙を、共通サイズとみなして給紙可能とします。[オン]にすると、例えば A4 サイズを指定して印刷を行う場合、A4 用紙がなくても、 Letter 用紙があれば Letter 用紙で印刷を行います。[オフ]の場合、同じく A4 サイズを指定して印刷を行う場合、A4 用紙がなければ用紙切れ表示を行い、印刷は行いません。

3. [設定]ボタンをクリックします。

#### エラー設定

- ナビゲーションメニューの[デバイス設定]をクリックし、下に表示される[システム] をクリックします。[システム設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

[手差し紙なし表示]

手差しトレイの紙が無くなった場合、表示の有無を選択します。

[エラー後自動継続]

エラー発生後に自動継続の有無を選択します。[オン]にした場合、自動継続時間を 5~495秒の数値で選択できます。

[トナー残量少の通知レベル]

トナー残量が少なくなった場合、通知の有無を選択します。[オン]にした場合、トナー残量を5~100の数値で選択できます。

3. [設定]ボタンをクリックします。

## 6 機能設定

このページは、ネットワーク認証がオンの場合には、管理者権限でログイン(アクセス)した際に表示されます。必要に応じて次の設定をしてください。詳細は下記を参照してください。

- 共通 / ジョブ初期値
- ・ プリンター
- ・ メール

## 共通/ジョブ初期値

このセクションでは共通設定、ジョブ初期値設定、スキャン初期値設定、出力初期値設定、コピー初期値設定、ファイル初期値設定など各種の詳細設定を行います。

#### 共通 / ジョブ初期値設定

- ナビゲーションメニューの[機能設定]をクリックし、下に表示される[共通/ジョブ初期値]をクリックします。[共通/ジョブ初期値設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

[文書名]

ジョブで使用する初期値の文書名を入力してください。

[付加情報]

日時、ジョブ番号などが選択できます。

3. [設定]ボタンをクリックします。

#### 出力初期値設定

- ナビゲーションメニューの[機能設定]をクリックし、下に表示される[共通/ジョブ初 期値]をクリックします。[共通/ジョブ初期値設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

[[JPEG/TIFF 印刷方法]

USB メモリから、JPEG ファイルを印刷するときの画像サイズを設定します。[用紙 サイズに合わせる]、[画像解像度のまま]、[印刷解像度に合わせる]から選択しま す。

[XPS 印刷サイズ調整]

XPS データを印刷するときの印刷サイズを指定します。[オン]に設定すると、用 紙サイズに合うようデータを調整して印刷し、[オフ]に設定すると、元のサイズの まま印刷します。

3. [設定]ボタンをクリックします。

## プリンター

このセクションではプリンターの詳細設定を行います。

\*:このマークが付いている設定を変更した場合、デバイスまたはネットワークの再 起動が必要です。再起動は[リセット]のページで行ってください。

#### 基本

- ナビゲーションメニューの[機能設定]をクリックし、下に表示される[プリンター]を クリックします。[プリンター設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

[エミュレーション]

エミュレーションを設定します。

[代替エミュレーション]

エミュレーションモードで [KPDL(自動)]を選択すると、印刷するデータに応じて KPDL ともう1つのエミュレーションモード(代替エミュレーション)を自動的 に切り替えることができます。[代替エミュレーション]は、オプションの Emulation Option を装着しているときに表示されます。

[給紙指定動作]

印刷時に指定したサイズや種類の用紙が給紙元にない場合、どのように給紙処理を 行うかを指定します。[自動]の場合、指定した給紙元に指定の用紙がない場合、自 動的に他の給紙元を検索して指定と一致する用紙をさがします。[固定]の場合、指 定した給紙元に指定の用紙がない場合でも、他の給紙元の検索は行いません。

[改ページ待ち時間]

待ち時間を 5-495 秒の間で、5 秒単位で指定します。待ち時間の間にデータが受信 されない場合に、改ページが行われます。初期設定値は 30 秒です。

[ジョブ名]

ジョブ番号、ジョブ名など選択できます。

[ユーザー名]

ユーザー名の有無を選択できます。

[ワイドA4]

ワイド A4 サイズの印刷有無を選択できます。

[自動力セット切り替え]

自動力セット切り替えの有無を選択できます。

**3.** [設定]ボタンをクリックします。

#### Google Cloud Print 設定

 ナビゲーションメニューの[機能設定]をクリックし、下に表示される[プリンター]を クリックします。[プリンター設定]ページが開きます。

- **2.** [Google Cloud Print 設定]の[設定/登録]ボタンをクリックします。[Google Cloud Print 設定]ページが表示されます。
- 3. [基本]の設定をします。次の設定をしてください。
  - 1. プリンター名:デバイス名が表示されます。必要に応じて変更できます。
- **4.** [Google Cloud Print] の設定をします。次の設定をしてください。
  - 1. [登録]ボタンをクリックします。
  - 2. [URL] に表示されている URL をクリックします。Google Cloud Print のサインイン画面が表示されます。
  - 3. アカウント情報(Gmail アドレスとパスワード)を入力し、サインインを行います。
  - 4. [OK] ボタンをクリックします。デバイスが登録されます。
- 5. 必要に応じて、[Privet ( クラウドデバイスローカル検出のプロトコルと API)] の設定を します。
  - 1. ローカル検出:[オン]に設定すると、ローカルネットワークに接続されたデバ イスを検出します。
  - 2. ローカル印刷: [オン] に設定すると、クラウドサーバーを介さずに、ローカル ネットワークに接続されたデバイスから印刷します。
- **6.** [設定]ボタンをクリックします。

#### ページ制御設定

- ナビゲーションメニューの[機能設定]をクリックし、下に表示される[プリンター]を クリックします。[プリンター設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

[両面]

印刷モードを[片面]、[両面長辺とじ]、[両面短辺とじ]から選択できます。

[部数]

印刷部数を入力します。

[印刷の向き]

印刷方向を[たて]または[よこ]から選択できます。

- [改行(LF)動作]
  - 改行(LF)と復帰(CR)の設定を行います。
- [復帰(CR)動作]
  - 改行(LF)と復帰(CR)の設定を行います。
- [印刷範囲の補正(たて)]
  - 印刷範囲(たて)を-76.0~+76.0mmの範囲で補正します。
- [印刷範囲の補正(よこ)]
  - 印刷範囲(よこ)を-76.0~+76.0 mmの範囲で補正します。

3. [設定]ボタンをクリックします。

#### 印刷品質設定

- ナビゲーションメニューの[機能設定]をクリックし、下に表示される[プリンター]を クリックします。[プリンター設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

[[KIR]

9600 dpi 相当(600dpi×15 階調)×600 dpi のなめらかな印刷を実現する、スムージン グ機能の[オン]または[オフ]を行います。初期設定は[オフ]です。

[エコプリント]

トナー使用量を抑えて印刷コストを低減する、エコプリント機能の[オン]または[オフ]を行います。初期設定は[オフ]です。

[解像度]

解像度を選択します。初期設定は [Fast1200] です。

3. [設定]ボタンをクリックします。

#### アプリフィルター

アプリフィルターの設定を行います。アプリフィルターは、受信した印刷データを指 定したコードで変換して印刷する機能です。

[USB]、[パラレルインターフェイス]、[ロジカルプリンター1(~4)]

[オン]を選択すると、USB、パラレルインターフェイスまたはロジカルプリンター 1 (~4) からの印刷データに対してアプリフィルターが設定され、EUC から Shift-JIS へ変換されます。

また、次の設定ができます。

[開始文字列]

変換処理を行う対象テキストの、最初の文字列を指定します。入力可能な文字数 は、半角で15文字です。

[終了文字列]

変換処理を行う対象テキストの最後の文字列を指定します。初期設定は\fです。入 力可能な文字数は、半角で15文字です。

#### メール

このセクションではメールの詳細設定を行います。

#### SMTP

- ナビゲーションメニューの[機能設定]をクリックし、下に表示される[メール]をク リックします。[メール設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

[SMTP プロトコル]

SMTP の接続有無が表示されます。設定は [ プロトコル設定 ] ページの [SMTP (メール送信) ] で行ってください。

[SMTP サーバー名]

SMTP サーバーの名前または IP アドレスを入力します。サーバー名を入力する場合 は、DNS サーバーを設定する必要があります。DNS サーバーの設定は、[TCP/IP 設 定]ページで行います。

[SMTP ポート番号]

SMTP が使用するポート番号を入力します(初期設定は 25)。SMTP over SSL 接続でのデフォルトポート番号は 465 です。

[SMTP サーバーのタイムアウト]

SMTP サーバーへの接続がタイムアウトするまでの時間を、秒単位で指定します。

[認証]

SMTP 認証を行うかどうか、また [POP before SMTP] を認証方式として使用するかを 設定します。[オン]または [POP before SMTP] を選択した場合、[使用するユー ザー]をドロップダウンリストから選択できます。

[SMTP セキュリティー]

SMTP セキュリティーが有効なときは、設定した項目名を表示します。[SSL/TLS] または [STARTTLS] が選択されている場合に有効です。設定は [ プロトコル ] ペー ジで行ってください。

[POP before SMTP のタイムアウト]

POP3 サーバーへの接続がタイムアウトするまでの時間を、秒単位で指定します。[認 証]で [POP before SMTP] を選択した場合に設定できます。

[接続確認]

本ページで設定した内容が正しいかどうかをテストします。[テスト]ボタンを押す と、SMTP サーバーへ接続を試みます。

[ドメイン制限]

ドメイン制限の有無を設定できます。[ドメインリスト]ボタンを押して設定してく ださい。許可、または拒否する宛先のドメイン名を入力します。メールアドレスも 指定できます。

[設定]ボタンをクリックします。

#### POP3

- ナビゲーションメニューの[機能設定]をクリックし、下に表示される[メール]をク リックします。[メール設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。

[POP3 プロトコル]

POP3 の接続有無が表示されます。設定は[プロトコル設定]ページの[POP3 (メール 受信)]で行ってください。リモート印刷が[禁止する]に設定されている場合、 メール印刷はできません。[プリンター設定]ページで設定してください。 [着信チェック間隔]

着信メールの有無を確認するために、POP3 サーバーに接続する間隔を分単位で設定します。間隔を3から60分単位で指定してください。初期設定値は15分です。

[直ちに実行]

[受信]ボタンをクリックすると、直ちに POP3 サーバーに接続し、着信メールの有 無をチェックします。また、リモート印刷が[許可する]に設定されているとき、着 信メールがある場合は、受信メールを印刷します。

[ドメイン制限]

ドメイン制限の有無を設定できます。[ドメインリスト]ボタンを押して設定してく ださい。許可、または拒否する宛先のドメイン名を入力します。メールアドレスも 指定できます。

[POP3 ユーザー設定]

[設定/登録]ボタンをクリックして、次のユーザー設定をしてください。ユーザー 1~3まで設定できます。

- 1. ユーザー設定1 (~3):ユーザーを有効、または無効に設定します。
- 2. メールアドレス:メールアドレスを入力します。
- 3. POP3 サーバー名: POP3 サーバーのホスト名、または IP アドレスを入力します。 ホスト名を使用する場合は、あらかじめ DNS サーバーを設定する必要がありま す。
- POP3 ポート番号: POP3 が使用するポート番号を入力します(初期設定は110)。
   POP3 over SSL 接続でのデフォルトポート番号は 995 です。
- 5. POP3 サーバーのタイムアウト: POP3 サーバーへの接続がタイムアウトするまで の時間を、秒単位で指定します。
- 6. ログインユーザー名: POP3 アカウントのログインユーザー名を入力します。
- 7. ログインパスワード: POP3 アカウントのログインパスワードを入力します。
- APOP の使用: APOP を有効または無効に設定します。APOP は POP3 サーバーとの通信中に、ログインパスワードを暗号化するために使用される暗号化メカニズムです。[オフ]の場合、ログインパスワードは、プレーン ASCII テキストを使用して送信されます。[オン]の場合、ログインパスワードは、暗号化されて送信されるため読み取ることができません。
   APOP を使用するには、POP3 サーバーが APOP をサポートし、設定が有効であることが必要です。
- 9. POP3 セキュリティー: POP3 セキュリティーを有効または無効にするかを設定し ます。[SSL/TLS] または [STARTTLS] が選択されている場合に有効です。設定は [プロトコル設定]ページで行ってください。POP3 セキュリティーを使用する場 合、サーバー設定に合わせて POP3 ポート番号の変更が必要になる場合がありま す。SSL/TLS では 465、STARTTLS の場合は 25 または 587 が一般に使用される ポートです。
- 10. 接続確認:設定した内容が正しいかどうかをテストします。[テスト]ボタンを 押して、POP3 サーバーへ接続を試みます。
- 11.サーバーからのメールを削除する:受信後に、POP3 サーバー上のメールを削除 する設定を行います。[オン]に設定すると、サーバー上のメールは受信後削除 されます。[オフ]に設定すると、受信後もメールは削除されません。
- 12. メール送信のサイズ制限:メールの受信可能な最大サイズを、キロバイトで入力 します。送信サイズ制限を無効にするには、0を設定します。
- 13. カバーページ:メールの受信後、添付ファイルとともにメール本文の印刷を行うか を設定します。[オン]に設定すると、添付ファイルとメールの本文が印刷されま す。添付ファイルが存在しない場合は、メール本文のみが印刷されます。[オフ] に設定すると、添付ファイルのみ印刷されます。添付ファイルが存在しない場合、 印刷は行われません。

3. [設定]ボタンをクリックします。

#### メール送信設定

- ナビゲーションメニューの [機能設定]をクリックし、下に表示される [メール]をクリックします。[メール設定]ページが開きます。
- 2. 状況に応じて、次の設定ができます。
  - [メール送信のサイズ制限]

送信可能なメールの最大サイズをキロバイトで入力します。SMTP サーバーで送信 メールのサイズを制限している場合は、サイズを入力してください。メールのサイ ズが入力した値よりも大きい場合、エラーを表示し、メールは送信されません。 SMTP サーバーで送信メールのサイズを制限していない場合は、0を入力してくだ さい。

[差出人アドレス]

本機が送信するメールの、差出人のアドレスを表示します。

[署名]

メール本文の最後に挿入される署名を表示します。

[機能初期值]

機能の初期値の変更は[共通/ジョブ初期値設定]ページで行ってください。

3. [設定]ボタンをクリックします。

## 7 ネットワーク設定

このページは、ネットワーク認証がオンの場合には、管理者権限でログイン(アクセス)した際に表示されます。

必要に応じて次の設定をしてください。詳細は下記を参照してください。

- 基本
- TCP/IP
- プロトコル

## 基本

このセクションではネットワークの基本設定を行います。

- ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[基本] をクリックします。[基本]ページが開きます。
- [ホスト名]に現在の接続状況が表示されます。設定は[システム設定]ページで行って ください。
- [LAN インターフェイス]ドロップダウンリストから、[自動]、[10BASE-Half]、 [10BASE-Full]、[100BASE-Half]、[100BASE-Full] または[1000BASE-T]を選択します。
- 4. [クライアント証明書]に現在の状況が表示されます。設定する場合、[設定/登録]ボタンをクリックします。[証明書設定]ページが開くので、該当する証明書を選択してください。証明書自身をクリックすると、内容が表示されます。

[設定]ボタンをクリックすると確定します。

デバイス証明書の設定は、[セキュリティー設定]の[証明書]ページで行ってください。

5. プロキシ — を設定する場合は、[プロキシ —] を[オン]にして、必要に応じて、次の設定をします。

[プロキシーサーバー (HTTP)]

プロキシーサーバー (HTTP) のホスト名、または IP アドレスを入力します。ホス ト名を使用する場合は、あらかじめ DNS サーバーを設定する必要があります。

[ポート番号]

プロキシーサーバー(HTTP)のポート番号を入力します。

[すべてのプロトコルでこのプロキシーを使用する]

すべてのプロトコルで同じプロキシーを使用する場合は、[オン]を選択します。

[プロキシーサーバー(HTTPS)]

プロキシーサーバー (HTTPS) のホスト名、または IP アドレスを入力します。ホス ト名を使用する場合は、あらかじめ DNS サーバーを設定する必要があります。

[ポート番号]

プロキシーサーバー (HTTPS) のポート番号を入力します。

[プロキシーを使用しないドメイン]

プロキシーを使用しないドメインのアドレスを入力します。複数ある場合は、アドレスとアドレスの間にはセミコロン ";"を使用してください。

6. [設定]ボタンをクリックします。

#### **TCP/IP**

このセクションでは、TCP/IPの詳細設定を行います。

\*:このマークが付いている設定を変更した場合、デバイスまたはネットワークの再 起動が必要です。再起動は[リセット]のページで行ってください。

- ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[TCP/ IP]をクリックします。[TCP/IP 設定]ページが開きます。
- 2. 必要に応じて、次の設定をします。

[TCP/IP]

設定する場合、[オン]を選択してください。[オン]を選択すると、下記の[IPv4 設定]、[IPv6 設定]、[IP フィルター(IPv4)]、[IP フィルター(IPv6)]、[ロジカ ルプリンター]および[IPSec 設定]が表示されます。

[ダイナミック DNS]

DNS サーバーによって割り当てられている IP アドレスが変更された場合に、ダイ ナミック DNS を使用して、自動的に割り当て直すかどうかを指定します。設定す る場合、[オン]を選択してください。

3. [設定]ボタンをクリックします。

#### IPv4 設定

- ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[TCP/ IP]をクリックします。[TCP/IP 設定]ページが開きます。
- 2. 必要に応じて、次の設定をします。

[DHCP/BOOTP]

DHCP または BOOTP を使って、IP アドレスの自動取得を行うかどうかを指定します。

[Auto-IP]

[オン]にすると、DHCP サーバーがない場合、またはプリントシステムのDHCP 設定がオフの場合も、他の機器と重複しない IP アドレスが自動的に割り当てられます。割り当て可能な IP アドレス範囲は、Auto-IP 用にあらかじめ予約されている 169.254.0.0 - 169.254.255.255 です。DHCP サーバーによって、すでに IP アドレスを取得している場合は割り当てを行いません。

[IP アドレス]

[DHCP/BOOTP]が[オフ]の場合、システムのネットワーク設定の一部として、静的 IPv4 アドレスを入力できます。[DHCP/BOOTP]が[オン]の場合、動的 IPv4 アド

レスがデバイスに割り当てられている場合にはグレーアウトしています。IPv4 アドレスのフォーマットは、ピリオドで区切られた数字です。

例:192.168.110.171

[サブネットマスク]

サブネットマスクを指定します。[DHCP/BOOTP]が[オン]の場合、動的 IPv4 アド レスがデバイスに割り当てられている場合にはグレーアウトしています。

[デフォルトゲートウェイ]

デフォルトゲートウェイの IP アドレスを指定します。[DHCP/BOOTP] が[オン]の 場合、動的 IPv4 アドレスがデバイスに割り当てられている場合にはグレーアウトし ています。

[ドメイン名]

本機が所属するドメイン名を指定します。ホストプリンター名は含みません(例: abcde.com)。[DHCP/BOOTP]が[オン]の場合、動的 IPv4 アドレスがデバイスに割 り当てられている場合にはグレーアウトしています。

[DNS サーバー(プライマリー、セカンダリー)]

プライマリーおよびセカンダリー DNS (ドメインネームシステム) サーバーの IP アドレスを設定します。[DHCP/BOOTP] が [オン]の場合、[DHCP サーバーから DNS サーバーを使用]または [次の DNS サーバーを使用]を選択できます。[次の DNS サーバーを使用]を選択した場合、DNS サーバーの IP アドレスをプライマ リーとセカンダリーに入力できます。

[WINS サーバー(プライマリー、セカンダリー)]

プライマリーおよびセカンダリー WINS サーバーの IP アドレスを指定します。 [DHCP/BOOTP] が[オン]の場合、[DHCP サーバーから WINS サーバーを使用]ま たは[次の WINS サーバーを使用]を選択できます。[次の WINS サーバーを使用] を選択した場合、WINS サーバーの IP アドレスをプライマリーとセカンダリーに入 力できます。

#### IPv6 設定

- ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[TCP/ IP]をクリックします。[TCP/IP 設定]ページが開きます。
- 2. 必要に応じて、次の設定をします。

[IPv6]

IPv6 プロトコルを有効にするかどうかを設定します。使用する場合は、[オン]に します。

[IP アドレス]

システムのネットワーク設定の一部として、静的 IPv6 アドレスを入力できます。本 機に IPv6 のアドレスを割り当てます。IPv6 アドレスのフォーマットは、 2001:db8:3c4d:15::1a2c:1a1f のように、コロンで区切られた数字です。

[プレフィックス長]

IPv6 のプレフィックス長を入力します。0-128 の 10 進数で入力します。

[RA (Stateless)]

DHCP サーバーを使わずに、RA によって IPv6 アドレスを設定する場合に[オン] にします。この機能は、プリントシステムが接続されているネットワークに、RA ステートレスルーターが必要です。

[デフォルトゲートウェイ]

デフォルトゲートウェイの IPv6 アドレスを指定します。

[DHCPv6 (Stateful) ]

IPv6のIPアドレスを自動取得するかどうかを選択します。[RA (Stateless)]が[オン]の場合は、RA (ルーター設定)の自動設定の状態に従い、DHCPv6によるIPアドレスとサーバー情報の取得を行います。この機能は、プリントシステムが接続されているネットワークに、DHCPv6 ルーターが必要です。

[ドメイン名]

本機が所属するドメイン名を指定します。

[DNS サーバー(プライマリー、セカンダリー)]

プライマリーおよびセカンダリー DNS (ドメインネームシステム) サーバーの IP アドレスを指定します。[DHCPv6 (Stateful)]が[オン]の場合、[DHCP サーバーか ら DNS サーバーを使用]または[次の DNS サーバーを使用]を選択できます。[次 の DNS サーバーを使用]を選択した場合、DNS サーバーの IP アドレスをプライマ リーとセカンダリーに入力できます。

#### Bonjour 設定

- ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[TCP/ IP]をクリックします。[TCP/IP 設定]ページが開きます。
- 2. 必要に応じて、次の設定をします。

[Bonjour]

[オン]または[オフ]を選択します。

[Bonjour 名]

[Bonjour] が [オン] の場合、Bonjour 名が表示されます。必要に応じて変更すること もできます。

#### IPフィルター(IPv4)

IP フィルターの設定を行います。IP フィルターとは、本機へのアクセスを IP アドレ スやプロトコルによって制限する機能です。

許可するホストの IP アドレス、またはネットワークアドレスを指定します。IP フィルターの設定を行わない場合は、すべてのホストからのアクセスを許可します。

- ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[TCP/ IP]をクリックします。[TCP/IP 設定]ページが開きます。
- 2. [設定/登録]ボタンをクリックします。[IP フィルター(IPv4)]ページが開きます。必要 に応じて、次の設定をします。

[IPアドレス (IPv4)]

アクセスを許可する IP アドレス、またはワークアドレスを指定します。

[サブネットマスク]

許可するサブネットマスクを指定します。エントリーがない場合は、すべてのアク セスは許可されます。

ネットワークへのアクセスを許可するには、ネットワークの IPv4 アドレス、および サブネットマスクを入力します。例:ネットワーク 192 上のすべてのホストにアク セスを許可するには、IP アドレスに 192.0.0.0、サブネットマスクに 255.0.0.0 と入力 します。サブネットマスクは、空欄でもかまいません。

サブネットマスクが空欄の場合は、255.255.255.255 と入力した時と同様です。

[プロトコル]

許可するプロトコルを指定します。選択できるプロトコルは、次のとおりです。

- LPD
- FTP
- IPP
- ThinPrint
- HTTP
- Raw
- SNMP
- IPP over SSL
- HTTPS

参考 : ThinPrint は、オプションの ThinPrint Option が起動している場合に表示されます。

3. [設定]ボタンをクリックします。

IPフィルター (IPv6)

IP フィルターの設定を行います。IP フィルターとは、本機へのアクセスを IP アドレ スやプロトコルによって制限する機能です。

許可するホストの IP アドレス、またはネットワークアドレスを指定します。IP フィルターの設定を行わない場合は、すべてのホストからのアクセスを許可します。

- ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[TCP/ IP]をクリックします。[TCP/IP 設定]ページが開きます。
- 2. [設定/登録]ボタンをクリックします。[IP フィルター(IPv6)]ページが開きます。必要 に応じて、次の設定をします。

[IPアドレス (IPv6)]

許可する IP アドレスを指定します。エントリーがない場合は、すべてのアクセスは 許可されます。指定できるアドレスの数は、プレフィックス長の設定と IPv6 ネット ワークアドレスに依存します。IPv6 アドレスのフィルタリング: プレフィックス長 と希望する IPv6 アドレスを入力してください。

[プレフィックス長]

IPv6 のプレフィックス長を入力します。0-128 の 10 進数で入力します。

[プロトコル]

許可するプロトコルを指定します。選択できるプロトコルは、次のとおりです。

- LPD
- FTP
- IPP
- ThinPrint
- HTTP
- RawSNMP
- IPP over SSL
- HTTPS

## 参考: ThinPrint は、オプションの ThinPrint Option が起動している場合に表示されます。

3. [設定]ボタンをクリックします。

#### ロジカルプリンター

ロジカルプリンターの設定を行います。プリントデータを ASCII から PostScript へ変換したり、ジョブデータの先頭や終端に文字列(命令)を追加または置き換える仮想 プリンターとして、本機を使用することができます。ロジカルプリンターは4台まで 設定可能です。

ロジカルプリンターは、FTP、LPR、IPP、IPPS、SMB (NetBEUI)、Raw のいずれか のプロトコルで使用します。印刷時にポートが指定されていない場合、ロジカルプリ ンタ1(LP1)ポート9100が自動的に使用されます。

- ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[TCP/ IP]をクリックします。[TCP/IP 設定]ページが開きます。
- 2. [設定/登録]ボタンをクリックします。[ロジカルプリンター]ページが開きます。必要 に応じて、次の設定をします。

[TCP/IP ポート番号]

TCP の RAW ポート番号(9100 など)と同様に、ロジカルプリンターにポート番号 を指定します。指定されたロジカルプリンターに応じて、指定の RAW ポートに入 力されたデータが変換されます。指定済のポート(例えば FTP や LPD)と同じポー ト番号を指定した場合は、ポートの指定は無効です。

[双方向印刷]

TCP/IP ポートに印刷する際、双方向印刷を[オン]または[オフ]に設定できます。 双方向印刷を[オフ]にすると、送信データは廃棄されます。

PostScript や PJL コマンドによる印刷の場合、プリンターから受信したデータをクラ イアントに返すためには、双方向印刷を[オン]にする必要があります。

[ジョブのはじめ]

出力ポート(lp ポート)に直接出力する前に、プリンターに送信する文字列を指定 します。文字列指定は、印刷データを送出する前に制御コードを送信する事が必要 な場合に行います。

[ジョブの終わり]

出力ポート(lp ポート)に直接出力する前に、プリンターに送信する文字列を指定 します。文字列指定は、印刷データが送出された後に制御コードを送信する事が必 要な場合に行います。 3. [設定]ボタンをクリックします。

#### IPSec 設定

 ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[TCP/ IP]をクリックします。[TCP/IP 設定]ページが開きます。

IPSec プロトコルで通信を行う場合に、アクセスの制限を設定できます。

IPSec プロトコルを有効にするかどうかを設定します。使用する場合は、[オン]にします。使用しない場合は、[オフ]を選択します。

2. 必要に応じて、次の設定をします。

[有効期限チェック]

有効にすると、通信時にサーバー証明書の有効期限を確認します。有効期限が切れ ている場合は、通信が失敗します。有効に設定されていない場合は、有効期限の チェックを行いません。

[制限]

IPSec プロトコル以外のパケットに対するデフォルトのポリシーを選択します。ルールに設定したホスト、もしくは、ネットワーク以外とも通信を行う場合は、[許可] を選択します。上記のルールに設定したホスト、もしくはネットワークのみと通信 を行う場合は、[禁止]を選択します。[許可]設定時、IPSec ルール設定で指定され たネットワーク以外からの通信も受け付けます。[禁止]設定時、IPSec ルール設定 で指定されたネットワーク以外からの通信も受け付けません。

[ルート証明]

証明書が有効かどうかを表示します。[ルート証明書1サブジェクト]~[ルート証明書5サブジェクト]まで5項目が表示されます。証明書の設定は[証明書]ページで行ってください。

[IPSec  $\mathcal{W} - \mathcal{W}$ ]

IPSec プロトコルで通信を行う場合に、使用するルールが有効かどうかを表示しま す。[ルール 1] ~ [ルール 10] まで 10 項目が表示されます。設定する場合、[設定 / 登録]ボタンをクリックして [IPSec ルール 1 (~ 10) 設定]ページで、次の設定を 行ってください。

1. [ポリシー]

[ルール]: IPSec 通信でのルールを使用するかどうか選択します。 [鍵管理方式]:ルールで使用する鍵の方式を[IKEv1]、[IKEv2]または[手動]を 選択してください。 [カプセル化モード]:[トランスポート]は、あらかじめ暗号化したデータをカ プセル化し、IP ヘッダをつけて送信します。送信ホスト、受信ホストが共に IPSec に対応している場合は最もシンプルな設定になります。[トンネル]は、途 中に用意されたゲートウェイを利用します。送信ホストから発信された IP パ ケットをゲートウェイが受け取り、IP パケット全体を暗号化して IPSec でカプセ ル化して新たな IP ヘッダをつけて送信します。

IPSec プロトコル通信で、ルールを使用するかどうか選択します。

 [IP アドレス]
 [IP バージョン]:接続先の IP バージョンを選択します。[IPv4] または [IPv6] を選択します。
 [IP アドレス (IPv4)]: IPSec で接続するホスト、もしくはネットワークの IPv4 アドレスを入力してください。IPSec を適用する範囲を限定する場合は、確実に IP アドレスを指定してください。設定が空欄の場合は、すべての IPv4 アドレス を対象として扱います。

[サブネットマスク]:[IP バージョン]に[IPv4]を選択した場合、IPSec で接続するホスト、またはネットワークのサブネットマスクを入力してください。設定が空欄の場合は、ホストアドレスとして扱います。

[IP アドレス(IPv6)]: IPSec で接続するホスト、もしくはネットワークの IPv6 アドレスを入力してください。IPSec を適用する範囲を限定する場合は、確実に IP アドレスを指定してください。設定が空欄の場合は、すべての IPv6 アドレス を対象として扱います。

[プレフィックス長]:[IP バージョン]に[IPv6]を選択した場合は、IPSec で接続 するホスト、またはネットワークのプレフィックス長を入力してください。設定 が空欄の場合は、ホストアドレスとして扱います。

[リモートピアアドレス]:[カプセル化モード]で[トンネル]を選んだ場合、リ モートコントロールする IP アドレスを指定します。

3. [認証]:[鍵管理方式]で[IKEv1]を選んだ場合、ローカル側の認証を設定します。 共有キーとなる文字列を設定して通信を行う場合は、[認証方式]から[事前共有 キー]を選択し、下のテキストボックスに事前共有キーとなる文字列を入力します。 CA発行のデバイス証明書や、ルート証明書を使用する場合は、[証明書]を選択し てください。[証明書]を選択した場合、デバイス証明書の有無が表示されます。設 定する場合は、[設定/登録]ボタンをクリックして証明書を選択してください。デ バイス証明書の設定は、[セキュリティー設定]の[証明書]ページで行ってください。 い。

[鍵管理方式]で[IKEv2]を選んだ場合、ローカル側とリモート側の認証を設定しま す。ローカル側では、[認証方式]、[ローカル ID タイプ]、[ローカル ID]、[デバ イス証明書]をそれぞれ設定してください。[リモート側]では、[認証方式]、[リ モート ID タイプ]、[リモート ID]、[事前共有キー]をそれぞれ設定してください。

4. [ 鍵交換(IKE phase1)]: IKE phase1 では、接続相手との間に ISAKMP SA を生成し、安全な通信を確立します。接続先に合わせて、次の項目を設定してください。

[モード]:[認証]の[鍵管理方式]で[IKEv1]を選んだ場合に設定できます。 [Main Mode]は、接続先と交換される情報量が多くなりますが、ID を保護できま す。[Aggressive Mode]は、[Main Mode]より接続先と交換される情報量は少なく てすみますが、ID の保護や、パラメーターのネゴシエーションの範囲に制限があ ります。[Aggressive Mode]を選択し、さらに[認証方式]に[事前共有]キーを 選択した場合は、ルール設定のIP アドレスの指定には、ホストアドレスのみ設 定できます。

[Hash]:Hash アルゴリズムを選択します。

[暗号化]:暗号化アルゴリズムを選択します。

[Diffie-Hellman グループ]: Diffi-Hellman 鍵共有アルゴリズムによって、保護されていないネットワークにある2つのホスト間において、安全に秘密鍵を共有することができます。使用するDiffie-Hellman グループを選択します。

- [有効期間(時間)]: ISAKMP SA の有効期間を、秒単位で設定します。
- 5. [データ保護(IKE phase2)]

IKE phase2 では、IKE phase1 によって確立された SA を使用して、AH や ESP など の IPSec SA を確立します。接続先に合わせて、次の項目を設定してください。 [プロトコル]:プロトコルを、[ESP] または [AH] から選択します。[ESP] はパ ケット内容のプライバシーと完全性が守られます。次の項目で、Hash と暗号化ア ルゴリズムを選択します。[AH] は、暗号化チェックサムによってパケット内容 の完全性が保護されます。[AH] を選択すると、AES-GCM-128/192/256 は使用で きません。次項目で、Hash アルゴリズムを選択します。

[Hash]: Hash アルゴリズムを選択します。[暗号化]で AES-GCM-128/192/256の いずれかを選択した場合、Hash にも同ビットの AES-GCM-128/192/256 または AES-GMAC-128/192/256 を選択する必要があります。

[暗号化]:暗号化アルゴリズムを選択します。([プロトコル]で[ESP]選択時の み。)[Hash]でAES-GCM-128/192/256を選択した場合、暗号化にも同ビットの AES-GCMを選択する必要があります。また、[Hash]でAES-GMAC-128/192/256 を選択した場合、暗号化は同ビットのaes-gcmを選択する必要があります。暗号 化アルゴリズムを選択しない場合は、暗号化を行わずに認証を行います。 [PFS]:[PFS]を[オン]にすることにより、ある鍵が解読されてもその解読され た鍵から後に生成された鍵を解読できないようにします。これにより安全性が高 まりますが、鍵の生成プロセスが増えます。 Diffie-Hellman グループ:[PFS]を[オン]にした場合、使用する Diffie-Hellman グ ループを選択します。 [有効期間測定]:[時刻]または[時間&データサイズ]を選択してください。 [有効期間(時間)]:IPSec SA の有効期間を、秒単位で設定します。 [有効期間(データサイズ)]:有効期間測定で[時間およびデータサイズ]を選 択した場合に設定できます。IPSec SA の有効期間中のデータサイズを、KB単位 で設定します。 [拡張シーケンス番号]:IPSec でシーケンス番号の拡張(64 ビット化)をするか どうか設定します。設定する場合、[オン]を選択してください。

6. [手動鍵設定]:[鍵管理方式]で[手動]を選んだ場合、[プロトコル]、[Hash]、[暗 号化]、[SPIフォーマット]、[インバウンド SPI]、[アウトバウンド SPI]、[鍵 フォーマット]、[インバウンド認証鍵]、[アウトバウンド認証鍵]、[インバウンド 暗号鍵]、[アウトバウンド 暗号鍵]、をそれぞれ設定してください。

[設定]ボタンをクリックして確定してください。

3. [設定]ボタンをクリックします。

## プロトコル

このセクションでは、通信手順または通信規約であるプロトコルの詳細設定を行います。

\*:このマークが付いている設定を変更した場合、デバイスまたはネットワークの再起動が必要です。再起動は[リセット]のページで行ってください。

- ナビゲーションメニューの[ネットワーク設定]をクリックし、下に表示される[プロト コル]をクリックします。[プロトコル設定]ページが開きます。
- 2. 必要に応じて、次の設定をします。

[印刷プロトコル]

印刷時のプロトコルを設定します。次の設定をしてください。

 [NetBEUI]: NetBEUI プロトコルを使用して、ピアツーピア環境での印刷が可能 です。この場合、本機は Windows のマイネットワークに登録されます。NetBEUI は SMB プロトコルの転送に使用される、NetBIOS プロトコルを拡張したもので す。

NetBEUI プロトコルを有効または無効に設定します。NetBEUI が[オン]の場合は、NetBIOS (NMB)による名前解決が利用できます。

[ワークグループ]: ワークグループは、"Windows Network Neighborhood" の [ ネットワーク全体 ] に表示されるワークグループを表します。

- [説明]:本機の説明を入力します。(この欄は、空欄でもかまいません。)
- 2. [LPD]:LPD プロトコルは、テキストファイルや PostScript ファイルの印刷を想 定した印刷システムです。LPD プロトコルを有効にするには[オン]に設定しま す。
- 3. [FTP (受信)]: FTP は、ネットワークでファイルの転送を行うための通信プロトコルです。FTP プロトコルで受信を有効にするには[オン]に設定します。
- [IPP]: IPP は、インターネットなどの TCP/IP ネットワークを通じて印刷データの送受信や印刷機器の制御を行うプロトコルです。IPP プロトコルを有効にするには[オン]に設定します。[ポート番号]は1~32767の間で入力してください。通常は631です。(例:http://(IP アドレス):631/printers/lp1)

- [IPP over SSL]: IPP プロトコルでの通信で、証明書を付加することができます。 IPP over SSL を有効にするには[オン]に設定します。この設定を使用する場合 は、[ネットワークセキュリティー設定]ページで SSL の設定を[オン]にしてく ださい。[ポート番号]は1~32767の間で入力してください。通常は443です。 [IPP over SSL 証明書]の状況が表示されます。設定する場合は、[設定/登録]ボ タンをクリックし、デバイス証明書を選択してください。[設定]ボタンをクリッ クすると、設定が確定されます。 デバイス証明書の設定は[セキュリティー設定]の[証明書]ページで行ってくだ さい。この証明書は IPP over SSL と HTTPS、共通で使用されます。
- 6. [IPP 認証]: IPP 認証を[オン]に設定すると、印刷時にユーザー認証を行い、第 三者による不正使用を防止できます。この設定を使用する場合は、[管理設定] の[認証設定]ページで認証の設定を[ネットワーク認証]にしてください。[IPP 認証]の[オン]を選択し、[デフォルトユーザー名]を入力してください。
- [RAW]: RAW プロトコルは、LPR とは異なる手順で印刷する方法です。一般に ポート番号として 9100 を使い、SNMP や MIB などを使ってプリンタを制御しま す。RAW プロトコルを有効にするには [オン]に設定します。
- [WSD 印刷]: WSD は Windows Vista において新たなネットワーク接続を実現す るプロトコルであり、複合機やプリンタデバイスの検知(インストール)やデー タ送受信がより容易に使用できます。WSD プロトコルを有効にするには[オン] に設定します。
- [POP3 (メール受信)]: POP3 は、電子メールを取得するための標準プロトコルです。POP3 プロトコルは、POP3 電子メール クライアントと電子メールが保存されているサーバーの間の接続を制御します。POP3 プロトコルでメール受信を有効にするには [オン]に設定します。詳細設定は [機能設定]の[メール設定]ページで行ってください。リモート印刷が禁止の場合、メール印刷はできませんので [プリンター設定]ページで許可してください。

[POP3 セキュリティー(ユーザー1(~3))]の方式をドロップダウンリストの[オフ]、[STARTTLS]または[SSL/TLS]より選択してください。この設定を使用する場合は、[ネットワークセキュリティー設定]ページでSSLの設定をオンにしてください。

[送信プロトコル]

送信時のプロトコルを設定します。次の設定をしてください。

 [SMTP (メール送信)]: SMTP とは簡易メール転送プロトコルのことで、電子 メールを転送するプロトコルです。SMTP プロトコルでメール送信を有効にする には[オン]に設定します。詳細設定は、[機能設定]の[メール設定]ページで 行ってください。
 [SMTP セキュリティー]の方式をドロップダウンリストの[STARTTLS]、[SSL/ TLS]または[オフ]より選択してください。この設定を使用する場合は、[ネッ

トワークセキュリティー ] ページで SSL の設定を [ オン ] にしてください。

[その他プロトコル]

その他のネットワークプロトコルを設定します。次の設定をしてください。

- [SNMPv1/v2c]: SNMP プロトコルは、ネットワーク内の管理情報の通信に使用されます。用紙切れなどのエラーが発生した場合、本機は自動的にトラップの生成を行い、指定されたトラップ受信者にエラーメッセージを送信します。SNMPv1/v2c プロトコルを有効にするには[オン]に設定します。詳細設定は、[管理設定]の[SNMP 設定]ページで行ってください。
- [SNMPv3]: SNMP プロトコルは、ネットワーク内の管理情報の通信に使用され ます。SNMPv3 プロトコルを有効にするには[オン]に設定します。詳細設定は、 [管理設定]の[SNMP 設定]ページで行ってください。
- 3. [HTTP]:HTTP プロトコルは、WWW サーバーとブラウザの間で、ウェブページ のデータを送受信する際のプロトコルです。HTTP プロトコルを有効にするには [オン]に設定します。

- [HTTPS]: HTTPS プロトコルは、SSL や TLS で暗号化するプロトコルです。Web サーバーとWeb ブラウザの間の通信が暗号化されていることを意味します。 HTTPS プロトコルを有効にするには[オン]に設定します。この設定を使用する 場合は、[ネットワークセキュリティー設定]ページでSSLの設定を[オン]にし てください。[HTTPS 証明書]で証明書の状況が表示されます。設定する場合は、 [設定/登録]ボタンをクリックし、デバイス証明書を選択してください。[設定] ボタンをクリックすると、設定が確定されます。 デバイス証明書の設定は、[セキュリティー設定]の[証明書]ページで行ってく ださい。この証明書はIPP over SSL と HTTPS 共通で使用されます。
- 5. [Enhanced WSD]: Enhanced WSD は、ネットワークに接続したさまざまなデバイ スを簡単につないで利用するための手続きを規定します。Enhanced WSD プロト コルを有効にするには [オン]に設定します。
- [Enhanced WSD (SSL)]: Enhanced WSD (SSL)は、Enhanced WSD で SSL を使用したセキュリティープロトコルであり、暗号化、認証、完全性(改竄防止)を提供します。Enhanced WSD (SSL)プロトコルを有効にするには[オン]に設定します。この設定を使用する場合は、[ネットワークセキュリティー設定]ページでSSL の設定を[オン]にしてください。[Enhanced WSD over SSL 証明書]で証明書の状況が表示されます。設定する場合は、[設定/登録]ボタンをクリックし、デバイス証明書を選択してください。[設定]ボタンをクリックすると、設定が確定されます。

デバイス証明書の設定は、[セキュリティー設定]の[証明書]ページで行ってく ださい。

7. [LDAP]:LDAPサーバー上のアドレス帳を外部のアドレス帳として参照し、メール アドレスを宛先に指定することが出来ます。LDAPプロトコルを有効にするには[オン]に設定します。外部アドレス帳の詳細設定は、[アドレス帳管理]の[外部アドレス帳設定]ページで行ってください。また、認証の詳細設定は、[管理設定]の[認証]で行ってください。

[LDAP セキュリティー]の方式を、[ネットワーク認証]のドロップダウンリストで [STARTTLS]、[SSL/TLS]または[オフ]、より選択してください。この設定を使用す る場合は、[セキュリティー設定]の[ネットワークセキュリティー]ページで SSL の設定を[オン]にしてください。

 [IEEE802.1x]: IEEE802.1x のセキュリティープロトコルにより、クライアント証明書に基づいて安全なネットワークヘログインできます。IEEE802.1x プロトコルを有効にするには[オン]に設定します。 IEEE802.1x を設定する場合、[設定/登録]ボタンをクリックします。 [IEEE802.1x 設定]ページで状況が表示されます。次の設定をしてください。

IEEE802.1x

[有効な暗号方式]:暗号方式をドロップダウンリストの[EAP-TLS]、[EAP-TTLS]、[EAP-FAST]または[PEAP(AP-MS-CHAPv2)]より選択してください。 [トンネル内認証プロトコル]:[有効な暗号方式]で、[EAP-TTLS]を指定した場 合に設定します。認証方式をドロップダウンリストの[MSCHAPV2]、 [MSCHAP]、[CHAP]または[PAP]より選択してください。 [ログインユーザー名]:アクセスするユーザー名を入力します。IEEE802.1x ク

[パスワード]:[有効な暗号方式]で、[EAP-TTLS]、[EAP-FAST]または

[PEAP(AP-MS-CHAPv2)] を指定した場合に設定します。パスワードを入力してください。

[一般名]:暗号方式で、[EAP-TTLS]、[EAP-FAST] または [PEAP(AP-MS-CHAPv2)]を指定した場合に設定します。サーバーの確認が必要な場合、サーバーの証明書の一般名を指定します。

[一般名の一致法則]:暗号方式で、[EAP-TTLS]、[EAP-FAST]または [PEAP(AP-MS-CHAPv2)]を指定した場合に設定します。サーバー証明書の確認を行う際、[一般名] で指定した名称とサーバー証明書内の一般名を比較します。このときに、[完全一致] が必要か、または[部分一致]で良いかを選択します。

[有効期限チェック]:[オン]にすると、通信時にサーバー証明書の有効期限を 確認します。有効期限が切れている場合は、通信が失敗します。有効に設定され ていない場合は、有効期限のチェックを行いません。 [IEEE802.1x クライアント証明書]:[IEEE802.1x クライアント証明書]で証明書 の状況が表示されます。設定する場合は、[設定/登録]ボタンをクリックし、デ バイス証明書を選択してください。[設定]ボタンをクリックすると、設定が確 定されます。デバイス証明書の設定は、[セキュリティー設定]の[証明書]ペー ジで行ってください。

証明書の状態

[ルート証明書1(~5)]、[IEEE802.1x クライアント証明書]:証明書の状況が 一覧表示されます。ルート証明書の設定は、[セキュリティー設定]の[証明書] ページで行ってください。

- 9. [LLTD]: LLTD は、ネットワーク構成を検出し、サービス品質の診断を行うプロトコルです。LLTD プロトコルを有効にするには [オン] に設定します。
- 3. [設定]ボタンをクリックします。

## 8 セキュリティー設定

このページは、管理者権限でログイン(アクセス)した際に表示されます。 必要に応じて次の設定をしてください。詳細は下記を参照してください。

- デバイスセキュリティー
- 送信セキュリティー
- ネットワークセキュリティー
- 証明書

## デバイスセキュリティー

このセクションではデバイスのセキュリティー設定を行います。

#### インターフェイスブロック

インターフェイスごとにアクセスをブロック(制限)できます。

- ナビゲーションメニューの[セキュリティー設定]をクリックし、下に表示される[デバ イスセキュリティー]をクリックします。[デバイスセキュリティー設定]ページが開 きます。
- 2. 必要に応じて、次の設定をします。

[ネットワーク]

ネットワークインターフェイスからのアクセスは、制限できません。プロトコルご とにアクセスを制限することが可能です。詳細は、[ネットワーク設定]の[プロト コル設定]ページを参照してください。

[USB デバイス]

USB ポートに接続するデバイス機器をブロックする場合、[ブロックする]を選択 します。

[USB ホスト]

USB ホスト機器をブロックする場合、[ブロックする]を選択します。

[USBストレージ]

USB ポートに接続する記憶装置をブロックする場合、[ブロックする]を選択します。

[パラレルインターフェイス]

パラレルインターフェイスをブロックする場合、[ブロックする]を選択します。

[オプションインターフェイス]

オプションインターフェイスをブロックする場合、[ブロックする]を選択します。

3. [設定]ボタンをクリックします。

#### 操作パネルロック

操作パネルからのアクセスを制限します。

- ナビゲーションメニューの[セキュリティー設定]をクリックし、下に表示される[デバ イスセキュリティー]をクリックします。[デバイスセキュリティー設定]ページが開 きます。
- [操作パネルロック]で、ドロップダウンリストの[オン]、[部分ロック1]、[部分ロック 2]、[部分ロック3]または[オン(一部)]、[オフ]を選択します。

#### 参考:機種によって表示が異なります。

必要に応じて、次の設定をします。

[オン]

入出力、ジョブの実行および用紙に関連する設定が禁止されます。部分的に制限 する場合、下記の[部分ロック1(~3)]を使用してください。

[部分ロック1]

ネットワーク設定、システム設定、文書ボックス設定などの入出力に関連する設 定が禁止されます。(例:アドレス帳およびボックスの登録/編集)

[部分ロック2]

[部分ロック1]の制限に加え、パネル設定、プリンター設定などのジョブの実行 に関連する設定が禁止されます。(例:ストップキーの使用、ジョブのキャンセ ル)

[部分ロック3]

[部分ロック2]の制限に加え、用紙に関連する設定が禁止されます。(例:カ セット設定、手差しトレイ設定)

[オフ]

すべてのキーが使用できます。

3. [設定]ボタンをクリックします。

#### 状況 / 履歴の表示

ジョブ状況およびジョブ履歴が制限できます。

- ナビゲーションメニューの[セキュリティー設定]をクリックし、下に表示される[デバ イスセキュリティー]をクリックします。[デバイスセキュリティー設定]ページが開 きます。
- 2. 必要に応じて、次の設定をします。

[ジョブ状況の詳細の表示]

ジョブの進行状況(詳細)の制限が可能です。[表示しない]を選択時には、管理者 権限でログインしたユーザーのみジョブ状況を表示します。[すべて表示]を選択時 には、ログインユーザーの権限に関わらずすべてのジョブ状況を表示します。[自 分のジョブのみ]を選択時には、自身のジョブ状況のみを表示します。

[ジョブ履歴の表示]

ジョブの履歴の制限が可能です。[表示しない]を選択時には、管理者権限でログインしたユーザーのみジョブ履歴を表示します。[すべて表示]を選択時には、ログインユーザーの権限に関わらずすべてのジョブ履歴を表示します。[自分のジョブのみ]を選択時には、自身のジョブ履歴のみを表示します。

3. [設定]ボタンをクリックします。

### ネットワークセキュリティー

このセクションでは、ネットワークのセキュリティー設定を行います。

\*:このマークが付いている設定を変更した場合、デバイスまたはネットワークの再 起動が必要です。再起動は[リセット]のページで行ってください。

#### ネットワークセキュリティー設定

- ナビゲーションメニューの[セキュリティー設定]をクリックし、下に表示される[ネットワークセキュリティー]をクリックします。[ネットワークセキュリティー設定] ページが開きます。
- 2. 必要に応じて、次の設定をします。

[SSL]

SSL プロトコルは、暗号機能を使用して、PC と本体間の通信を暗号化することが できます。設定する場合、[オン]にしてください。[オフ]にすると、SSL 通信が 無効になります。

[サーバー機能時の設定]

サーバー側のセキュリティー設定をします。次の設定をしてください。

- 1. [TLS バージョン]: TLS プロトコルは、情報を暗号化して送受信するプロトコル の一つです。使用するバージョンを [SSL3.0/TLS1.0]、[TLS1.1] および [TLS1.2] から選択してください。(複数選択が可能です。)
- [有効な暗号方式]:使用する暗号アルゴリズムを、[ARCFOUR]、[DES]、 [3DES]、[AES] および [AES-GCM] から選択してください。(複数選択が可能で す。)
- 3. [Hash]: Hash アルゴリズムを、[SHA1] および [SHA2(256/384)] から選択してくだ さい。(複数選択が可能です。)
- 4. [HTTP セキュリティー]:HTTP 使用時のセキュリティーレベルを指定します。
  [セキュア(HTTPS)]:HTTP プロトコルでのすべての通信を暗号化します。
  https://で始まる URL のみがアクセス可能です。http://で始まる URL が指定された場合、自動的に https://へリダイレクトされます。
  [非セキュア(HTTPSとHTTP)]:HTTP プロトコルでの暗号通信と、非暗号通信の両方をアクセス可能にします。https://とhttp://いずれの URL でもアクセスできます。前者の場合は暗号通信、後者は通常通信となります。
- 5. [IPP セキュリティー]: IPP 使用時のセキュリティーレベルを指定します。 [セキュア(IPPS)]: HTTP プロトコルでのすべての通信を暗号化します。 [非セキュア(IPPS と IPP)]: IPP プロトコルでの暗号通信と、非暗号通信の両方 をアクセス可能にします。
- [クライアント機能時の設定]

クライアント (PC) 側のセキュリティー設定をします。次の設定をしてください。

 [TLS バージョン]: TLS プロトコルは、情報を暗号化して送受信するプロトコル の一つです。使用するバージョンを [SSL3.0/TLS1.0]、[TLS1.1] および [TLS1.2] から選択してください。(複数選択が可能です。)

- [有効な暗号方式]:使用する暗号アルゴリズムを、[ARCFOUR]、[DES]、 [3DES]、[AES] および [AES-GCM] から選択してください。(複数選択が可能で す。)
- 3. [Hash]: Hash アルゴリズムを、[SHA1] および [SHA2(256/384)] から選択してくだ さい。(複数選択が可能です。)
- 複数選択した場合、いずれかの暗号方式で自動で接続します。 4. [証明書チェック]:[オン]に設定すると、通信時にサーバー証明書に設定され ている有効期限をチェックします。有効期限が切れている場合には、通信が失敗 します。有効期限のチェックを行わない場合は、[オフ]を設定します。

参考:SSLを[オン]にし、[HTTP セキュリティー]を[セキュア(HTTPS)]に 設定した場合、TWAIN ドライバーから文書ボックスへのアクセスができなくな ります。

3. [設定]ボタンをクリックします。

#### ネットワークアクセス設定

- ナビゲーションメニューの[セキュリティー設定]をクリックし、下に表示される[ネットワークセキュリティー]をクリックします。[ネットワークセキュリティー設定] ページが開きます。
- 2. 必要に応じて、次の設定をします。

[フィルタリング/ファイアウォール]

デバイスのネットワークアクセスを制御し、特定のネットワークアドレスのみ許可 をすることができます。詳細設定は、[ネットワーク設定]の[TCP/IP 設定]ページ にある[IP フィルター(IPV4)]または[IP フィルター(IPV6)]を参照してくださ い。

[SNMPv1/v2c]

SNMP のリードコミュニティー名とライトコミュニティー名は、SNMP 経由でのデ バイス情報取得と設定を制御するパスワードとして使用します。詳細は、[管理設 定]の[SNMP 設定]ページを参照してください。

[SNMPv3]

SNMPv3の通信設定は、SNMP 経由での認証 / 暗号化通信を制御するために使用します。詳細は、[管理設定]の[SNMP 設定]ページを参照してください。

[SSL]

SSL 通信を使用するためにはセキュアプロトコルの設定を行う必要があります。詳細は、[ネットワークセキュリティー設定]ページの[SSL]を参照してください。

[IEEE802.1x]

IEEE802.1x を使用するためには、IEEE802.1x の設定を行う必要があります。詳細 は、[ネットワーク設定]の[プロトコル設定]ページにある[IEEE802.1x 設定]を 参照してください。

[IPSec]

IPSec 通信を使用するためには、IPSec の設定を行う必要があります。詳細は、[ネットワーク設定]の[TCP/IP 設定]ページを参照してください。

3. [設定]ボタンをクリックします。

### 証明書

このセクションでは、証明書の詳細を確認、作成、更新することができます。これら の設定内容を変更した場合は、ネットワークまたは本体をリセット(再起動)する必 要があります。

\*:このマークが付いている設定を変更した場合、デバイスまたはネットワークの再 起動が必要です。再起動は[リセット]のページで行ってください。

#### デバイス証明書

- ナビゲーションメニューの[セキュリティー設定]をクリックし、下に表示される[証明 書]をクリックします。[証明書]ページが開きます。
- デバイス証明書が一覧表示され、次の確認ができます。[デバイス証明書 1]は、初期設定で自動的に発行されています。自動発行された証明書には、国別コードと一般名、および 10 年の有効期限が設定されています。

[状態]

証明書が有効かどうか表示します。

[サブジェクト]

国別コードと一般名が表示されます。

[有効期限]

証明書の有効期限を表示します。

[プロトコル]

使用するプロトコルの種類が表示されます。(HTTPS、IPP over SSL、Enhanced WSD (SSL)、IEEE802.1X、ThinPrint、DSM Scan、IPsecRuleX、その他プロトコル)

3. 必要に応じて、次の設定をします。

[デバイス証明書1(~5)]

初期設定の変更、新規作成の設定/登録、および削除ができます。

[デバイス証明書1(~5)]の[設定/登録]ボタンをクリックします。[デバイス 証明書1(~5)設定]ページが開き、現在の状況が表示されます。次の確認および 設定ができます。

- [状態]:証明書が有効かどうか表示します。
- 「有効期限」:証明書の有効期限を表示します。
- [証明書の詳細]: [表示]ボタンをクリックすると、証明書の詳細内容を見ることができます。
- [自己発行証明書を作成する]:[作成]ボタンをクリックすると、[証明書に必要 なデータの編集]ページが開きます。設定する情報を入力または設定してくださ い。[国コード]、[都道府県名]、[市町村名]、[組織名]、[部門名]、[一般名]、 [メールアドレス]、[標準時(UTC/GMT)]、[有効期限]、[鍵長]は自動的に表 示されます。[鍵長]は暗号の計算に用いる暗号鍵のデータ量のことで、[1024 bit] または [2048 bit]より選択してください。[設定]ボタンをクリックして、内容を 確定してください。
- [証明書を更新する]:[更新]ボタンをクリックすると、[有効期限設定]ページ が開きます。有効期限を入力してください。[標準時(UTC/GMT)]は自動的に表 示されます。[設定]ボタンをクリックして、内容を確定してください。

- [証明書の削除]:[削除]ボタンをクリックすると、証明書が表示されます。内容 を削除してください。
- [証明書をエクスポートする]:[エクスポート]ボタンをクリックすると、ファイ ルのダウンロード画面が表示されます。内容を保存してください。

[ルート証明書1(~5)]

新規で作成し、設定/登録、および削除ができます。

- [ルート証明書1(~5)]の[設定/登録]ボタンをクリックします。[ルート証明書1(~5)設定]ページが開き、現在の状況が表示されます。次の確認および設定ができます。
- [状態]:証明書が有効かどうか表示します。
- [有効期限]:証明書の有効期限を表示します。
- [証明書をインポート]:[インポート]ボタンをクリックすると、[ファイルのインポート]ページが開きます。[参照]ボタンをクリックしてインポートするファイルを選択してください。[設定]ボタンをクリックして、内容を確定してください。
- 2. [ルート証明書2(~5)]を削除するには、[ルート証明書2(~5)]の[削除] ボタンをクリックします。

参考:証明書は、個別に各プロトコルまたは各設定に割り当てることができます。 IPSec ルール証明書の設定は、[ネットワーク設定]の[TCP/IP]で行ってください。 その他のプロトコル証明書の設定は、[ネットワーク設定]の[プロトコル設定]ペー ジで行ってください。

## 9 管理設定

このページは、ネットワーク認証がオンの場合には、管理者権限でログイン(アクセス)した際に表示されます。

必要に応じて次の設定をしてください。詳細は下記を参照してください。

- 部門管理
- 認証
- 通知 / レポート
- 履歴設定
- SNMP
- リセットリモートサービス

#### 部門管理

このセクションでは部門管理の詳細設定を行います。

#### 設定/登録

部門管理を使用するためには、部門管理設定を設定する必要があります。

- ナビゲーションメニューの[管理設定]をクリックし、下に表示される[部門管理]をク リックします。[設定/登録]ページが開きます。
- [設定/登録]ボタンをクリックします。[部門管理設定]ページが開きます。必要に応じて、次の設定をします。

[部門管理]

部門管理機能を使用する場合する場合、[オン]を選択します。

[部門管理方式]

ネットワーク認証を介して部門管理をする場合、[ネットワーク]を選択します。

[動作設定]

次の設定をしてください。

- 1. 制限超過時設定:制限枚数に達したときの処理を、[即時禁止]、[次ジョブから 禁止]、[警告のみ]から選択します。
- 2. ID 不明ジョブ処理:部門コードが不明な(部門コードが送られてこない)ジョ ブが届いた場合の処理方法を[許可する]、[拒否する]から選択します。
- 手順2の[部門管理]で[オン]を選択した場合、[カウンター制限初期値]および[用紙サイズ別集計]が表示されます。
- **4.** [カウンター制限初期値]の設定をします。各カウンターの制限初期値を1~9999999の 範囲で入力してください。

3.

5. [設定]ボタンをクリックします。

#### ローカル部門管理リスト

このセクションでは、部門の追加、削除、および部門集計の設定を行います。

#### 部門追加

部門ごとまたは全部門の集計をするためには、部門を追加する必要があります。

- 1. [部門追加]アイコンをクリックします。[新規部門 詳細情報]ページが開きます。
- 2. [部門詳細情報]の設定をします。次の設定をしてください。

[部門 ID]

部門 ID を入力します。

- 3. [制限]の設定をします。
  - 1. 各機能の使用方法の制限を、[制限しない]、[カウンター制限]、[使用禁止]から選択します。
  - 2. 各機能の使用方法の制限値を1~9999999の範囲で入力します。
- 4. [設定]ボタンをクリックします。

#### 削除

- 部門 ID 左隣にあるチェックボックスをクリックします。複数選択する場合は、[すべ てチェック]アイコンをクリックします。
- 2. [削除]アイコンをクリックします。

カウンター

- **1.** 部門 ID 左隣にあるチェックボックスをクリックします。
- [カウンター]ボタンをクリックします。選択した部門の集計結果が表示されます。
- 3. 集計結果を確認します。
  - [印刷ページ数]

ドロップダウンリストより、目的に応じて[機能別印刷ページ数]、[レイアウト別 印刷ページ数]を選択します。

[カウンターリセット]

[リセット]ボタンをクリックして、カウンターをリセットします。

- **4.** [その他部門]ボタンまたは[全部門合計]ボタンをクリックして、上記手順と同様に集計結果を確認します。
  - [その他部門]

その他部門の集計結果を表示します。

[全部門合計]

全部門合計の集計結果を表示します。

認証

このセクションでは認証の詳細設定を行います。

#### 設定/登録

認証を使用するためには、認証設定を設定する必要があります。

- ナビゲーションメニューの[管理設定]をクリックし、下に表示される[認証]をクリッ クします。[設定/登録]ページが開きます。
- 2. [設定/登録]ボタンをクリックします。[認証設定]ページが開きます。必要に応じて、 次の設定をします。

[基本]

[認証]:ドロップダウンリストより[オフ]、または[ネットワーク認証]を選択します。

[動作設定]

ID 不明ジョブ処理として、[許可する]、[拒否する]から選択します。設定自体は [部門管理設定]ページで行います。

- 3. 手順2の[基本]で[ネットワーク認証]を選択した場合、次の設定をしてください。
  - ネットワーク認証サーバーを設定します。 ホスト名:ネットワーク認証サーバーのホスト名を入力してください。ホスト名 を使用する場合は、あらかじめ DNS サーバーを設定する必要があります。 ポート番号:ネットワーク認証サーバーのポート番号を入力してください。 サーバータイプ:ドロップダウンリストからサーバータイプを選択してください。 初期ドメイン:[ドメインリスト]ボタンをクリックして表示されるリストで、 ドメイン名を入力し、[設定]ボタンをクリックください。複数入力した場合は、 ドロップダウンリストから選択できるようになります。
     ネットワークユーザー設定をします。 ネットワークユーザー情報の取得:[オン]または[オフ]を選択してください。
     [サーバー設定]ボタンをクリックして、サーバー設定をします。
  - LDAP:[オン]になっていることを確認してください。[オフ]の場合、[ネット ワーク設定]の[プロトコル設定]ページで[オン]に設定してください。 LDAP サーバー名:LDAP サーバー名を入力してください。 LDAP ポート番号:LDAP ポート番号を入力してください。 検索のタイムアウト:秒単位で入力してください。 LDAP セキュリティー:[ネットワーク設定]の[プロトコル設定]ページで設定 してください。
  - 4. [ユーザー情報取得タグ]を設定します。[名前 1]、[名前 2]、[メールアドレス] を入力してください。
  - 5. [設定]ボタンをクリックしてください。
  - グループ認可を設定する場合、[オン]を選択し、[グループリスト]ボタンをク リックしてください。表示されるグループリストから認可対象のグループを選択 し、[設定]ボタンをクリックしてください。
- **4.** [動作設定]の設定をします。ID不明ジョブ処理として、[許可する]、[拒否する]から選択します。設定自体は、[管理設定]の[部門管理設定]ページで行います。
- 5. [設定]ボタンをクリックします。

## 通知 / レポート

このセクションでは通知 / レポートの詳細設定を行います。

#### 通知 / レポート設定

- ナビゲーションメニューの[管理設定]をクリックし、下に表示される[通知/レポート] をクリックします。[通知/レポート設定]ページが開きます。
- 2. [メンテナンスレポート]の設定をします。

[製品 ID]

製品 ID を入力します。

[受取人アドレス]

メンテナンスレポートの受取人アドレスを入力します。アドレスとアドレスの間に はセミコロン ";" を使用してください。

[サブジェクト]

レポートの件名を入力します。

[メンテナンスレポート間隔]

ドロップダウンリストより[なし]、[月ごと]、[週ごと]、[日ごと]、[時間ごと] を選択します。

[月ごと]を選択した場合、送信する月をチェックし、[日]と[時刻]のドロップ ダウンリストから数値を選択します。

[週ごと]を選択した場合、[曜日]と[時刻]のドロップダウンリストから数値を 選択します。

[日ごと]を選択した場合、[時刻]のドロップダウンリストから数値を選択します。 [時間ごと]を選択した場合、[時間ごと]のドロップダウンリストから数値を選択 します。

[直ちに実行]

[送信]ボタンをクリックすると、メンテナンスレポートを受取人に送信します。

- 3. [イベントレポート/スケジュールレポート1 (~3)]の設定をします。
  - [受取人1(~3)のメールアドレス]

受取人1(~3)のメールアドレスを入力します。

[サブジェクト]

変数を使用して、レポートの件名を入力します。

[イベントレポート]

[イベントレポート項目]で、イベントレポートで知らせる項目を選択し、[イベントレポート間隔]で送信するレポートの間隔を入力します。

[スケジュールレポート]

[カウンターステータス]をチェックすると、カウンターレポートを添付します。

[スケジュールレポート間隔]

ドロップダウンリストより[なし]、[月ごと]、[週ごと]、[日ごと]、[時間ごと] を選択します。

[月ごと]を選択した場合、送信する月をチェックし、[日]と[時刻]のドロップ ダウンリストから数値を選択します。

[週ごと]を選択した場合、[曜日]と[時刻]のドロップダウンリストから数値を 選択します。

[日ごと]を選択した場合、[時刻]のドロップダウンリストから数値を選択します。 [時間ごと]を選択した場合、[時間ごと]のドロップダウンリストから数値を選択 します。

[直ちに実行]

[送信]ボタンをクリックすると、スケジュールレポートを受取人1~3に送信しま す。

4. [設定]ボタンをクリックします。

#### 履歴設定

このセクションでは履歴設定の詳細設定を行います

#### 履歴設定

- ナビゲーションメニューの[管理設定]をクリックし、下に表示される[履歴設定]をク リックします。[履歴設定]ページが開きます。
- 2. [ジョブ履歴]の設定をします。

[受取人アドレス]

レポートを受け取るメールアドレスを入力します。メールアドレスを複数入力する には、メールアドレスをセミコロン(;) で区切って入力します。

[件名]

ジョブ履歴の件名を入力します。

[自動送信]

ジョブ履歴の送信を設定します。[オン]または[オフ]を選択してください。

[履歴数]

送信時のジョブ履歴件数を、1から1500まで設定できます。

[個人情報]

ジョブ履歴に個人情報を含まるかどうかを設定します。[含める]または[含めない] を選択してください。

[直ちに実行]

[送信]ボタンをクリックすると、ジョブ履歴を受取人に送信します。

3. [設定]ボタンをクリックします。

#### **SNMP**

このセクションでは SNMP の詳細設定を行います。

\*:このマークが付いている設定を変更した場合、デバイスまたはネットワークの再 起動が必要です。再起動は[リセット]のページで行ってください。

#### SNMP 設定

- ナビゲーションメニューの[管理設定]をクリックし、下に表示される[SNMP]をクリックします。[SNMP 設定]ページが開きます。
- **2.** [SNMPv1/v2c]の設定をします。

[SNMPv1/v2c]

SNMP v1/v2c プロトコルを有効にするかどうかを設定します。[ネットワーク設定] の[プロトコル設定]ページで[オン]、[オフ]から選択します。

[リードコミュニティー名]

読取要求用のコミュニティー名を入力します。初期設定のリードコミュニティー名 は public です。設定変更後は、本体をリセットする必要があります。

[ライトコミュニティー名]

変更要求用のコミュニティー名を入力します。初期設定のリードコミュニティー名 は public です。設定変更後は、本体をリセットする必要があります。

[sysContact]

MIB-II sysContact オブジェクトです。通常はネットワーク管理者のメールアドレスです。

[sysName]

MIB-II sysName オブジェクトです。通常は本機のホスト名またはドメイン名です。

[sysLocation]

MIB-II sysLocation オブジェクトです。[デバイス設定]の[システム設定]ページに 設定されている情報が表示されます。表示を変更する場合は、[システム]をクリッ クします。

[HP Web Jetadmin 互換]

HP Web Jetadmin からのアクセスを可能にするかどうかを、[オン]または[オフ]で 設定します。設定変更後は、本体をリセットする必要があります。

[認証トラップ]

認証トラップを使用するかどうかを設定します。[オン]にすると、不正なコミュニ ティー名を使用した読取りや書込みが試みられたときに、SNMPトラップが生成さ れます。トラップは次項目で指定するトラップアドレスに送信されます。設定変更 後は、本体をリセットする必要があります。

[トラップ受信]

[設定/登録]ボタンをクリックすると、トラップ受信が設定されます。

3. [SNMPv3]の設定をします。設定変更後は、本体をリセットする必要があります。

[SNMPv3]

SNMPv3 プロトコルを使用するかどうかを設定します。[ネットワーク設定]の[プ ロトコル設定]ページにある[オン]、[オフ]から選択します。 [認証]

SNMP 通信を行なう際に、認証を行なうかどうかを設定します。

[Hash]

Hash アルゴリズムを [MD5] または [SHA1] から選択します。[認証]を[オン]にした場合に表示します。

[暗号通信]

SNMP 通信を行なう際に、通信の暗号化を行なうかどうかを設定します。[認証]を [オン]にした場合に表示します。

[暗号化]

暗号化アルゴリズムを [DES] または [AES] から選択します。[ 認証 ] を [ オン ] にした 場合に表示します。

[読み取りユーザー]

読み取り専用ユーザーの [ユーザー名]および [パスワード]を入力します。

[読み書きユーザー]

読み書きユーザーの [ユーザー名]および [パスワード]を入力します。

4. [設定]ボタンをクリックします。

#### リセット

このセクションではリセットの詳細設定を行います。

#### 再起動

- ナビゲーションメニューの[管理設定]をクリックし、下に表示される[リセット]をク リックします。[リセット]ページが開きます。
- **2.** 必要に応じて、デバイスまたはネットワークを再起動します。

[デバイスの再起動]

[デバイスの再起動]ボタンをクリックすると、デバイスが再起動します。

[ネットワークの再起動]

[ネットワークの再起動]ボタンをクリックすると、本体内部のネットワークイン ターフェイスカードが再起動します

#### 工場出荷時リセット

- ナビゲーションメニューの[管理設定]をクリックし、下に表示される[リセット]をク リックします。[リセット]ページが開きます。
- 2. 必要に応じて、[初期化]ボタンをクリックします。デバイスが工場出荷時の設定に戻ります。

10 トラブルシューティング

エンベデッドサーバーでトラブルが発生した場合は、次の表を参照して確認や処理を 行ってください。

## トラブルシューティング

不具合内容	確認事項	対処方法	参照
エンベデッドサー バーにアクセスで きない。	本機の電源は入っています か?	電源を入れてから待機状態に なるまで待ち、エンベデッド サーバーにアクセスしてくだ さい。	本体使用説明書
	ネットワークケーブルは適 切に接続されていますか?	ネットワークケーブルを正し く接続してください。	本体使用説明書
	ネットワークの設定は正し いですか?	操作パネルからネットワーク 設定を実行してください。正 しい設定については、ネット ワーク管理者にお問い合わせ ください。	-
	本機の IP アドレスは正しく 入力されていますか?	正しい IP アドレスを入力して ください。ネットワーク管理 者に本機の IP アドレスを問い 合わせてください。	-
	Web ブラウザーは正しく ネットワーク設定が行われ ていますか?	Web ブラウザーのネットワー ク設定をチェックしてくださ い。詳細は、Web ブラウザー のヘルプ機能を参照してくだ さい。	-
	管理者によって IP フィル ター機能が設定されていま すか?	IP フィルター設定に合ったア ドレスから、エンベデッド サーバーにアクセスしてくだ さい。	23 ページの IP フィルター (IPv4) 24 ページの IP フィルター (IPv6)
	セキュリティー設定 > ネッ トワークセキュリティー > サーバー機能時の設定の [HTTP セキュリティー] が、 [HTTP セキュア(HTTPS)] に設定されていますか?	HTTP セキュリティーがセキュ ア (HTTPS) に設定されてい る場合は、https://からはじま る URL を指定します。http:// ではエンベデッドサーバーに アクセスできません。	34 ページのネット ワークセキュリ ティー

不具合内容	確認事項	対処方法	参照
エンベデッドサー バーにアクセスで きない。	ブラウザーのバージョン は、エンベデッドサーバー で対応しているバージョン より新しいですか?	エンベデッドサーバーで対応 されているバージョンのブラ ウザーを使用してください。	1 ページの <b>動作</b> 環 境
エンベデッドサー バーの表示が文字 化けする。	ブラウザーのバージョン は、エンベデッドサーバー で対応しているバージョン より新しいですか?	エンベデッドサーバーで対応 されているバージョンのブラ ウザーを使用してください。	1 ページの <b>動作環</b> 境
	本体操作パネルの表示言語 と同じ言語を、エンベデッ ドサーバーで選択していま すか?	操作パネルの表示言語と同じ 言語を選択してください。	3ページのトップ バー
特定のページにア クセスできません。	アクセスレベルが [ ユー ザー ] に設定されていませ んか ?	アクセスレベルを[管理者]に 変更してください。	41 ページの通知 / レポート
設定動作ができま せん。	印刷またはスキャン動作中 ではありませんか?	動作が完了するまでお待ちく ださい。	-
設定が確定されま せん。	設定を行った後、[ 設定 ] をクリックしましたか ?	設定を行った後は、他のペー ジに移動したりエンベデッド サーバーを閉じる前に、かな らず[設定]をクリックして、 確定してください。	-
	再起動が必要な設定の場 合、[再起動]をクリック しましたか?	本体の再起動を行ってくださ い。設定が保存されます。	44 ページのリセッ ト
	エンベデッドサーバーと同 時に、本体の操作パネル上 でシステムメニューの操作 を行っていませんか?	システムメニューの操作が完 了してから、エンベデッド サーバーの操作を行ってくだ さい。	-
管理者パスワード を忘れてしまった。	-	サービス担当者までご連絡く ださい。	-
エラーや警告が表 示される。	本体操作パネル表示に、エ ラーや警告が表示されてい ますか?	プリントシステム付属の使用 説明書を参照して、表示され たメッセージに対応する対応 手順を実行してください。	本体使用説明書



## お問い合わせ先

本体・オブション製品に関しては お客様相談室 200.0120-534-881 受付時間(月~金 10:00~12:00,13:00~17:00 土・日・祝日・当社休業日を除く)

当社製プリンタドライバソフトアプリケーションの操作に関しては
 サポートセンター 2000,0120-229-330
 受付時間(月~金9:00~17:30 ±・日・祝日・当社休業日を除く)



〒108-8385 東京都港区芝5-34-7 田町センタービル 電話(03)5441-6666 ホームページ http://www.riso.co.jp/

2015.10 EWSRSJA00