ACCESS MANAGEMENT SYSTEM

アドミニストレーターガイド

USRMA-1534-07 2023-03 ja

もくじ

はじめに 2

本書について 3
商標について 7
著作権について 8
免責事項 9

ご使用の前に 11

おもな機能 12
ユーザー認証方式と管理されるユーザーについて 17
使用制限のしくみについて 19
ベースロールとカスタムロールについて 20
デバイス管理権限について 23
デバイス機能の使用制限 26
Access Management System の構成 34
Access Management System の管理者について 35
必要な動作環境 37

Access Management System をセットアップする 39

ローカルデバイス認証方式で運用する場合のセットアップの流れ 40
サーバー認証方式で運用する場合のセットアップの流れ 42
デバイスとネットワーク環境の準備 44
User Authentication にログインする 47
デバイスの環境設定を行う 48
User Authentication の場合 49
ロールを管理する 62
User Authentication の場合 63

クライアントコンピューターをセットアップする 75

クライアントコンピューターをセットアップする流れ 76

ローカルデバイス認証方式での運用例 78

ローカルデバイス認証方式での運用例について 79
操作の流れ 81
デバイスとネットワーク環境を準備する 84
デバイスの環境設定を行う 85
カスタムロールを作成する 94
ロールをエクスポートする 98
ローカルユーザーを登録し、ロールを指定する 99
ユーザー情報をエクスポートする 103
ロールとユーザー情報をインポートする 104

部門別 ID 管理機能を起動する 107
タッチパネルディスプレーでログイン方式と使用制限を確認する 113
クライアントコンピューターをセットアップする 119
クライアントコンピューターで印刷制限を確認する 122

Access Management System の運用を中止する 126
Access Management System の運用を中止する流れ 127

困ったときには 129
メッセージ一覧 130
トラブルシューティング 138
終了コード一覧 139

付録 141
Access Management System 運用上のセキュリティーについて 142
アクセス制御用の鍵ペアを更新する 143
その他の注意事項 145

はじめに

はじめに 2
本書について 3
商標について 7
著作権について 8
免責事項 9

はじめに

このたびはキヤノン製品をお買い上げいただき、誠にありがとうございます。本製品の機能を十分にご理解いただき、より効果的にご利用いただくために、ご使用前にこの取扱説明書をよくお読みください。また、お読みいただきました後も大切に保管してください。

本書について

- 動作環境(P. 3)
- マークについて(P. 3)
- ボタンの表記について(P. 4)
- 画面について(P. 4)
- 略称について(P. 5)
- 用語について(P. 5)
- キーまたはボタン名称について(P. 5)

動作環境

このマニュアルは、次の Web ブラウザーで動作します。Web ブラウザーのスクリプト機能と Cookie を有効にして、使用してください。

Windows

- Internet Explorer 9 以降
- Microsoft Edge
- Firefox 38 以降
- Firefox ESR 38 以降
- Chrome 45 以降 *

macOS

- Safari 8 以降
- Firefox 38 以降
- Chrome 45 以降 *

Linux

- Firefox 38 以降

iOS

- Safari (iOS 6.0 以降) *

Android

- Chrome 45 以降 *

* インターネット上のマニュアル閲覧時のみ

マークについて

本書では、操作上必ず守っていただきたい事項や操作の説明に、下記のマークを付けています。

重要

操作上、必ず守っていただきたい重要事項や制限事項が書かれています。誤った操作によるトラブルや故障、物的損害を防ぐために、必ずお読みください。

メモ

操作の参考となることや補足説明が書かれています。お読みになることをおすすめします。

ボタンの表記について

本書では、デバイス上のキーやコンピューター画面上のボタンを次のように表記します。

- デバイスのタッチパネルディスプレー上のボタン：[ボタン名称]

  例：［ログイン］
  ［次へ］

- デバイス上の操作パネルのキー：＜キーアイコン＞＋（キー名称）

  例：　（スタート）
  ⓪～⑨（テンキー）

- コンピューター画面上のボタン/メニューコマンド：[ボタン/メニューコマンドの名称]

  例：［ログイン］
  ［OK］

メモ

- 本書では、Windows の操作手順は［設定］/［スタート］メニューとコントロールパネルの表示が、インストール直後のカスタマイズされていない状態であることを前提に記載しています。

画面について

本書で使われているコンピューター操作画面は、お使いの環境によって表示が異なる場合があります。

操作時に選択/クリックするボタンの場所は、（丸）で囲んで表しています。また、操作を行うボタンが複数表示されている場合は、それらをすべて囲んでいます。

3.

[ロール管理]をクリックします。

操作対象

略称について

本書に記載されている名称は、下記の略称を使用しています。

Microsoft Windows Server 2008 operating system 日本語版：	Windows Server 2008
Microsoft Windows Server 2008 R2 operating system 日本語版：	Windows Server 2008 R2
Microsoft Windows Server 2012 operating system 日本語版：	Windows Server 2012
Microsoft Windows Server 2012 R2 operating system 日本語版：	Windows Server 2012 R2
Microsoft Windows Server 2016 operating system 日本語版：	Windows Server 2016
Microsoft Windows Vista operating system:	Windows Vista
Microsoft Windows 7 operating system 日本語版：	Windows 7
Microsoft Windows 8.1 operating system 日本語版：	Windows 8.1
Microsoft Windows 10 operating system 日本語版：	Windows 10
Microsoft Windows operating system：	Windows
Microsoft Windows Internet Explorer：	Internet Explorer
Canon Access Management System：	AMS
Canon ACCESS MANAGEMENT SYSTEM Printer Driver Add-in：	AMS Printer Driver Add-in

用語について

- 本書の中で、「デバイス」とは、キヤノン製の複合機（MFP）を指します。
- 本書の中で、「Active Directory 認証」とは、「サーバー認証(Active Directory)」を指します。
- 本書の中で、Windows Server 2008（x64）と Windows Server 2008（x86）を表す場合は、「Windows Server 2008」と表記します。
- 本書の中で、Windows Server 2012 と Windows Server 2012 R2 の両方を表す場合は、「Windows Server 2012」と表記します。
- 本書の中で、Windows Server 2008/Windows Server 2008 R2/Windows Server 2012 のすべてを表す場合は、「Windows サーバー OS」と表記します。
- 本書の中で、Windows Vista/Windows 7/Windows 8.1/Windows 10 のすべてを表す場合は、「Windows クライアント OS」と表記します。

キーまたはボタン名称について

お使いの機種よっては、本書に記載しているキーまたはボタン名称と異なっていたり、操作パネル上のキーがタッチパネルディスプレー上のボタンに変更されている場合があります。

お使いの機種のキーまたはボタン名称は、本書では以下のように記載されています。

お使いの機種のキーまたはボタン名称	**本書で使用しているキーまたはボタン名称**
 、メインメニュー、ホーム	メインメニュー
 、カスタムメニュー	カスタムメニュー*
 、 	 （状況確認/中止）

お使いの機種のキーまたはボタン名称	**本書で使用しているキーまたはボタン名称**
、、	（設定/登録）
	（認証）

*お使いの機種によっては、カスタムメニューのボタンがホーム画面に表示されます。

商標について

「MEAP」は、キヤノンの複合機ならびにプリンターに搭載された「アプリケーションプラットフォーム」についてのキヤノン株式会社の商標です。

Windows、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または商標です。

その他、本書中の社名や商品名は、各社の登録商標または商標です。

著作権について

免責事項

本書の内容は予告なく変更することがありますのでご了承ください。

キヤノン株式会社は、ここに定める場合を除き、市場性、商品性、特定使用目的の適合性、または特許権の非侵害性に対する保証を含め、明示的または暗示的にかかわらず本書に関していかなる種類の保証を負うものではありません。キヤノン株式会社は、直接的、間接的、または結果的に生じたいかなる自然の損害、あるいは本書をご利用になったことにより生じたいかなる損害または費用についても、責任を負うものではありません。

ご使用の前に

ご使用の前に 11
おもな機能 12
ユーザー認証方式と管理されるユーザーについて 17
使用制限のしくみについて 19
ベースロールとカスタムロールについて 20
デバイス管理権限について 23
デバイス機能の使用制限 26
Access Management System の構成 34
Access Management System の管理者について 35
必要な動作環境 37

ご使用の前に

Access Management System の概要や必要な動作環境などについて説明します。

おもな機能

Access Management System は、デバイスの使用制限を管理するためのシステムです。以下のような機能をユーザーごとに制限します。

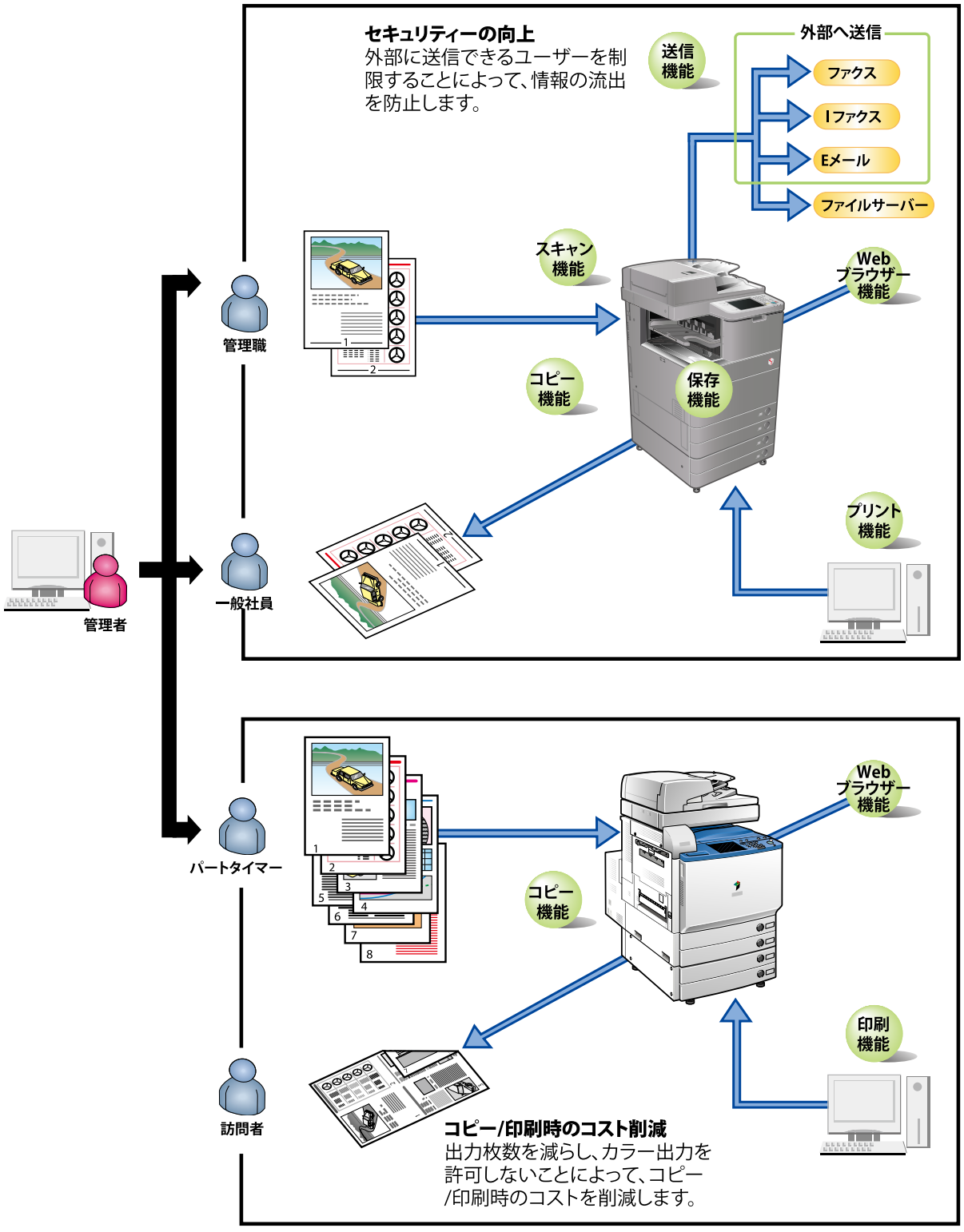
機能名	制限項目
プリント機能	カラープリント、片面プリント、ページレイアウトプリント、ボックスへの保存
保存機能	ボックス文書のカラープリント、ボックス文書の片面プリント、ボックス文書のページレイアウトプリント、メモリーメディアへの保存、スキャン文書のメモリーメディアへの保存、メモリーメディア文書のプリント
コピー機能	カラーコピー、片面コピー、ページレイアウトコピー
スキャン機能	カラースキャン
送信機能/ネットワークへの保存	E メール送信、E メール送信（「自分へ送信」機能の利用）、I ファクス送信、ファクス送信、ファイルサーバーへの送信、「マイフォルダー」送信機能の利用、宛先指定方法、送信ファイルの形式、ネットワーク保存先の登録

メモ

- お使いの機種によっては、対応していない制限項目があります。

Access Management System を利用することで、以下のような効果を上げることができます。

- 外部への情報流出の防止
  コピー、送信、ボックスなどの機能や、デバイスの[設定/登録]画面で使用できる操作をユーザーごとに制限することによって、外部への情報の流出を防止します。
- コストの抑止
  カラー出力、片面出力、ページレイアウト出力など、コピー/プリントに関わる機能をユーザーごとに制限することによって、デバイスの使用にかかるコストを抑えることができます。



ユーザー認証から使用制限までの流れ

Access Management System のセットアップが完了すると、タッチパネルディスプレーからデバイスを操作したり、コンピューターから印刷をするときに、ユーザー認証が必要になります。

タッチパネルディスプレーからデバイスを操作する場合<デバイス認証>

デバイス認証で使用する場合は、Access Management System のセットアップが完了すると、タッチパネルディスプレーにログイン画面が表示されます。

ユーザー名とパスワードを入力して[ログイン]を押すと、ユーザー認証が行われ、そのユーザーが使用できる機能だけがタッチパネルディスプレー上で操作可能になります。

未登録ユーザーがデバイスを使用するときには、ユーザー名やパスワードを入力しないで[Guest ログイン]を押すと、使用制限されていない機能だけがタッチパネルディスプレー上で操作可能になります。

デバイスの[設定/登録]画面からの操作も制限できるため、デバイスの設定変更を行うことができるユーザーを限定することができます。

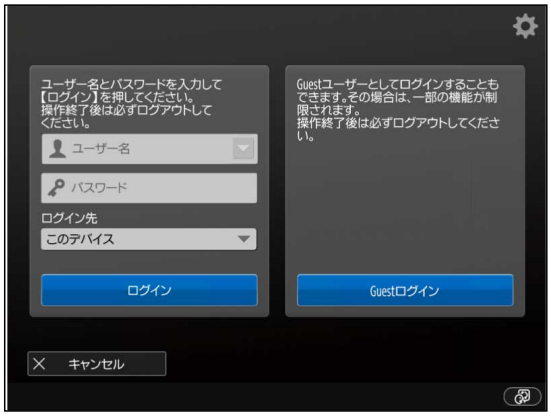
重要

- Access Management System を有効にご利用いただくために、デバイスを使い終わったら、必ず、（認証）またはタッチパネルディスプレー上の ログアウト （ログアウト）を押してログアウトしてください。

タッチパネルディスプレーからデバイスを操作する場合＜機能別認証＞

機能別認証で使用する場合は、Access Management System のセットアップが完了すると、タッチパネルディスプレーに[メインメニュー]画面が表示されます。

認証が設定されている機能のボタンを押すと、ログイン画面が表示されます。



ユーザー名とパスワードを入力して[ログイン]を押すと、ユーザー認証が行われ、そのユーザーに使用権限がある場合にのみ、タッチパネルディスプレー上に詳細な設定を行うための画面が表示されます。

メモ

- 未登録ユーザーに使用権限がある場合、[Guest ログイン]ボタンが表示されます。未登録ユーザーの利用権限は、ゲストロール([GuestUser])の設定値に従います。

デバイスの[設定/登録]画面からの操作も制限できるため、デバイスの設定変更を行うことができるユーザーを限定することができます。

重要

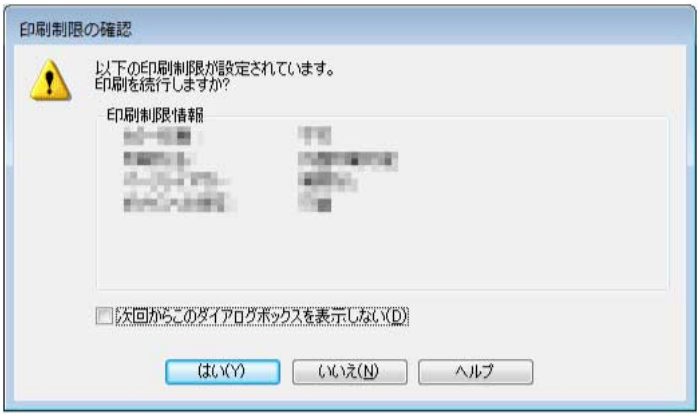
- Access Management System を有効にご利用いただくために、デバイスを使い終わったら、必ず、ID（認証）またはタッチパネルディスプレー上の ログアウト （ログアウト）を押してログアウトしてください。

コンピューターから印刷する場合

コンピューターからの印刷を制限する場合は、Access Management System のセットアップ後、デバイスを使用するすべてのクライアントコンピューターのセットアップ（プリンタードライバーの AMS 機能の有効化とユーザー情報の設定）が必要です。

クライアントコンピューターのセットアップが完了すると、ユーザーがコンピューターから印刷する際に、[認証のパスワード確認]ダイアログボックスが表示されるようになります。

パスワードを入力して[OK]をクリックすると、ユーザー認証が行われ、印刷時の機能が制限されます。

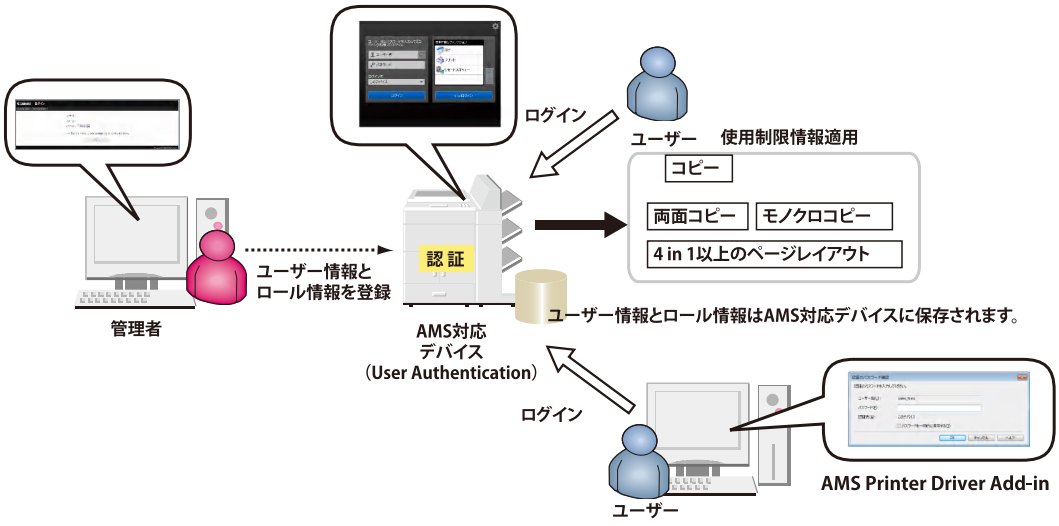


ユーザー認証方式と管理されるユーザーについて

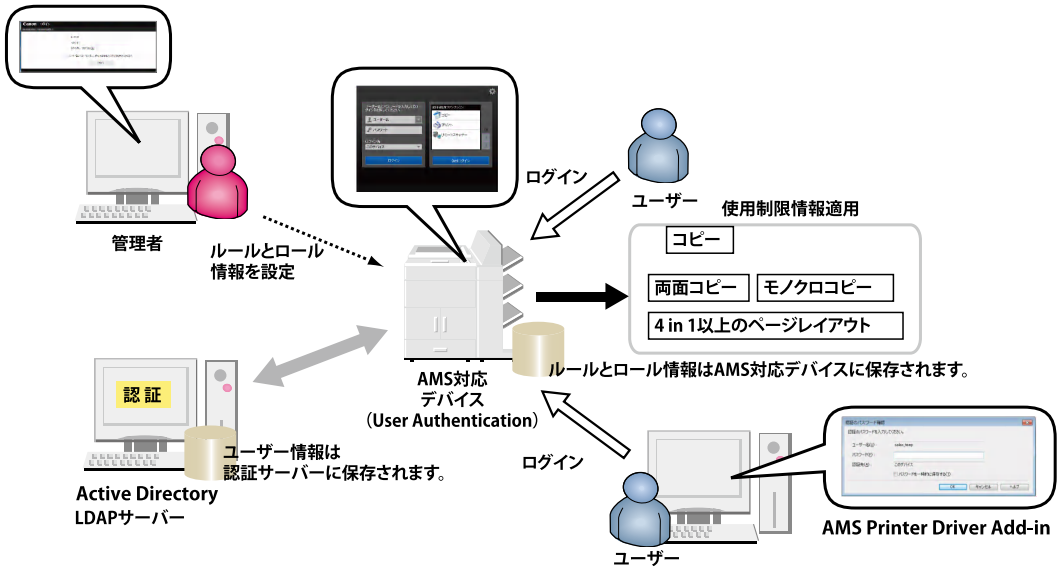
Access Management System で管理するデバイスで使用できるユーザー認証方式には、以下の種類があり、管理されるユーザーの種類が異なります。

ユーザー認証方式	説明
ローカルデバイス認証	ユーザー情報の管理やユーザーの認証をデバイス上で行います。ユーザーがユーザー名とパスワードを入力すると、デバイスに登録されているローカルユーザー情報に基づいてユーザー認証が行われます。
ローカルデバイス認証+Active Directory 認証、または、ローカルデバイス認証+LDAP 認証	Active Directory 認証とローカルデバイス認証、または、LDAP 認証とローカルデバイス認証の、サーバー認証/ローカルデバイス認証の両方に対応したユーザー認証方式です。たとえば、社員などの認証サーバーに登録されているユーザーを Active Directory 認証/LDAP 認証で管理し、外部スタッフなどの一時的なユーザーをローカルデバイス認証で管理します。 ネットワーク障害など、何らかの原因で認証サーバーにアクセスできなくなった場合でも、ローカルデバイス認証でデバイスを使用することができるので、Access Management System では、この方式による運用をおすすめします。 LDAP 認証は、LDAP サーバーに登録されているユーザー情報を使用してユーザー認証を行います。

ローカルデバイス認証方式



Active Directory 認証方式/LDAP 認証方式



メモ

- ローカルデバイス認証+Active Directory 認証、または、ローカルデバイス認証+LDAP 認証の場合は、ログインしたユーザーの種類によって認証先が異なります。

使用制限のしくみについて

Access Management System では、デバイスの使用制限情報を「ロール」と呼ばれる単位で管理します。ロールには、デバイスに搭載されている各機能の使用を許可する/許可しないなどを設定することができます。

ローカルデバイス認証方式で運用する場合は、Web ブラウザー経由の User Authentication を使用して、デバイスごとに、各ユーザーに個別に適用するロールを設定します。

サーバー認証方式で運用する場合には、ロールとユーザーの関連付け情報を作成します。

ベースロールとカスタムロールについて

デバイスの使用制限情報を設定するロールには、「ベースロール」と「カスタムロール」があります。

「ベースロール」とは、Access Management System に用意されているロールで、あらかじめ使用制限情報（デバイス管理権限とデバイス機能の使用制限）が設定されています。

「カスタムロール」とは、ベースロールを元にして独自に作成するロールです。オフィス環境に応じて、デバイス機能の使用制限情報を自由に設定することができます。デバイスの管理権限は、[元にするベースロール]の設定によって決まりますが、キヤノン複合機では、[デバイス管理制限]の設定が優先されます。

「カスタムロール（管理者）」は、[Administrator]を元にしたカスタムロールで、キヤノン複合機の管理がしやすいように、[デバイス管理制限]があらかじめ設定されています。

ベースロールとカスタムロール（管理者）には、以下の種類があります。デバイス機能の使用制限とデバイス管理権限の概要は、以下のとおりです。

重要

- デバイス管理権限には、リモート UI から操作する権限と、デバイスの操作パネルから操作する権限がありますが、AMS を使用しているデバイスでは、リモート UI から操作するデバイス管理権限は、[Administrator]/[DeviceAdmin]/[NetworkAdmin]ロール（または、これらと同一の使用制限を設定したカスタムロール）を割り当てられているユーザーにのみ与えられています。以下では、デバイスの操作パネルから操作する場合のデバイス管理権限について、説明します。
- ベースロールとカスタムロール（管理者）は、デバイス機能の使用制限情報とデバイス管理権限の編集を行えません。また、アプリケーション制限やボタン制限も設定できません。
- [GuestUser]ロールは、デバイス機能の使用制限情報の編集と、アプリケーション制限やボタン制限の設定を行えます。ただし、デバイス管理権限の編集は行えません。

メモ

- デバイスアプリケーションとは、デバイスに搭載されている機能ではなく、インストールすることによって使用できるようになった機能（MEAP アプリケーションなど）を指しています。

ロール名	デバイス機能の使用制限	デバイス管理権限
[Administrator]	すべての機能を使用できます。	[設定/登録]画面で、以下のキーを使用できません。 ● 重連コピーのリモートデバイス登録（ファンクション設定） ● 新規宛先の制限（ファンクション設定） ● 送信時に機器署名を必ずつける（ファンクション設定） ● アドレス帳の暗証番号（宛先設定）
[PowerUser]	すべての機能を使用できます。	[設定/登録]画面で、AMS を使用しない場合の制限に加えて、以下のキーを使用できません。 ● 重連コピーのリモートデバイス登録（ファンクション設定） ● 新規宛先の制限（ファンクション設定） ● 送信時に機器署名を必ずつける（ファンクション設定） ● アドレス帳の暗証番号（宛先設定） ● 送信レポート出力（ファンクション設定） ● 証明書設定の鍵削除（管理設定）

ロール名	デバイス機能の使用制限	デバイス管理権限
[GeneralUser]	アドレス帳/宛先表の利用と宛先ドメインの指定を除く、すべての機能を使用できます。	[設定/登録]画面で、AMS を使用しない場合の制限に加えて、以下のキーを使用できません。 ● 重連コピーのリモートデバイス登録（ファンクション設定） ● 新規宛先の制限（ファンクション設定） ● 送信時に機器署名を必ずつける（ファンクション設定） ● 宛先設定 ● 送信レポート出力（ファンクション設定） ● 証明書設定の鍵削除（管理設定）
[LimitedUser]	コピー機能とプリント機能のみを使用できますが、カラー出力、片面出力、ページレイアウト、ボックスへの保存に制限があります。 スキャン機能、保存（ボックス文書の出力）機能、送信機能は使用できません。	[設定/登録]画面で、使用できるキーはありません。
[GuestUser] （ゲストロール）	コピー機能を使用できますが、カラー出力、片面出力、ページレイアウト、ボックスへの保存に制限があります。 スキャン機能、保存（ボックス文書の出力）機能、送信機能、プリント機能は使用できません。 アプリケーションの使用制限を設定できます。機種によって、メインメニュー上の各ボタンの使用制限も設定できます。	[設定/登録]画面で、使用できるキーはありません。
[NetworkAdmin] （カスタムロール（管理者））	すべての機能を使用できます。	[設定/登録]画面で、AMS を使用しない場合の制限に加えて、以下のキーを使用できません。 ● 重連コピーのリモートデバイス登録（ファンクション設定） ● 新規宛先の制限（ファンクション設定） ● 送信時に機器署名を必ずつける（ファンクション設定） ● アドレス帳の暗証番号（宛先設定）
[DeviceAdmin] （カスタムロール（管理者））	すべての機能を使用できます。	[設定/登録]画面で、AMS を使用しない場合の制限に加えて、以下のキーを使用できません。 ● 重連コピーのリモートデバイス登録（ファンクション設定） ● 新規宛先の制限（ファンクション設定） ● 送信時に機器署名を必ずつける（ファンクション設定） ● アドレス帳の暗証番号（宛先設定）

重要

- AMS を使用しない場合でもログインアプリケーションとして User Authentication を使用すると、一般ユーザー（[Administrator]/[DeviceAdmin]/[NetworkAdmin]以外のロールを設定されているユーザー）は、[設定/登録]画面の使用が制限されます。また、管理者ユーザーであっても、デバイス管理権限（[DeviceAdmin]/[NetworkAdmin]）に応じて、[設定/登録]画面の使用が制限されます。AMS を使用する場合は、AMS を使用しない場合の制限に加えて、さらに、上記の制限が加わります。

メモ

- お使いの機種によっては、対応していない制限項目があります。

デバイス管理権限について

Access Management System を運用しているデバイスでは、ユーザーに関連付けられたロールに従って、デバイスの管理に関する以下の画面の表示や操作が制限されます。

- [状況確認/中止]画面
- [設定/登録]画面

重要

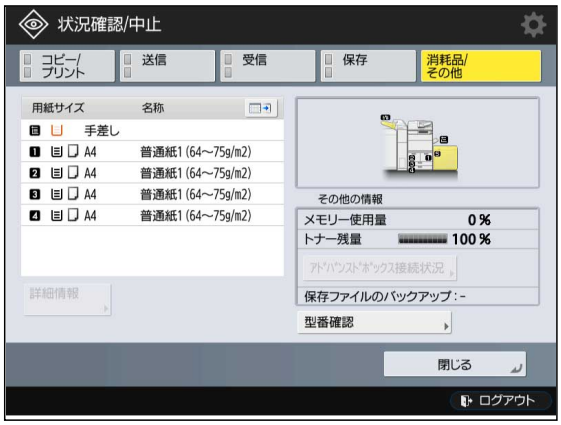
- AMS を使用しているデバイスでは、リモート UI から操作するデバイス管理権限は、[Administrator]/[DeviceAdmin]/[NetworkAdmin]ロール（または、これらと同一の使用制限を設定したカスタムロール）を割り当てられているユーザーにのみ与えられています。以下では、デバイスの操作パネルから操作する場合のデバイス管理権限について、説明します。

[状況確認/中止]画面の制限

デバイスで（状況確認/中止）を押すと、[状況確認/中止]画面が表示されます。Access Management System を運用している場合、デバイスにログインするまでは、[状況確認/中止]画面でデバイスの状況は表示できますが、コピーや送受信の状況などは表示できません。

メモ

- [状況確認/中止]画面の詳細は、デバイスに付属の取扱説明書を参照してください。



デバイス管理権限があるユーザー（[Administrator]ロールを関連付けられたユーザー、および、[DeviceAdmin]や[NetworkAdmin]も含めて[Administrator]を元に作成したカスタムロールを関連付けられたユーザー）がログインした場合は、ジョブの状況や履歴を表示/操作できるようになります。

デバイス管理権限がないユーザーがログインした場合は、ログインしたユーザー自身のジョブの状況や履歴は表示/操作できますが、他のユーザーのジョブについては、以下のように制限されます。

[状況確認/中止]画面				デバイス管理権限があるユーザー	デバイス管理権限がないユーザー
[コピー/プリント]	[ジョブ状況]	[プリント]	[優先プリント]	使用可	使用不可
			[詳細情報]		

[状況確認/中止]画面				デバイス管理権限があるユーザー	デバイス管理権限がないユーザー
			[中止]		
			[セキュアプリント]		
			ジョブ名	表示	「***」と表示
		[コピー]	[詳細情報]	使用可	使用不可
			[中止]		
[送信]		[送信]	[詳細情報]	使用可	使用不可
			[中止]		
			ジョブの宛先	表示	「***」と表示
		[ファクス]	[詳細情報]	使用可	使用不可
			[中止]		
			ジョブの宛先	表示	「***」と表示
[受信]		[転送]	[詳細情報]	使用可	使用不可
			[I ファクス受信確認]		
		[ファクス]	[詳細情報]		
			[中止]		
[保存]		-	[詳細情報]	使用可	使用不可
			[中止]		
			保存先	表示	「***」と表示
それ以外のキー				使用可	使用可
それ以外の表示				表示	表示

[設定/登録]の制限

AMS を有効にすると、以下の[設定/登録]の項目は利用できなくなります。設定項目は表示されません。

重要

- AMS を有効にすると、[新規宛先の制限]と[アドレス帳の暗証番号]の設定が無効になります。AMS を無効に変更しても、[新規宛先の制限]と[アドレス帳の暗証番号]は自動で元の設定には戻りません。再度設定が必要となります。

[設定/登録]画面			
[ファンクション設定]	[コピー]	[重連コピーのリモートデバイス登録]	
	[送信]	[共通設定]	[新規宛先の制限]*1
			有効期限切れ証明書使用時の送信を許可

[設定/登録]画面			
			[送信時に機器署名を必ずつける][*2]
			[E メール送信を「自分へ送信」に限定][*4]
			[ファイル送信を「マイフォルダー」に限定][*4]
	[ファイル保存/利用]	[メモリーメディア設定]	
[宛先設定]	[アドレス帳の暗証番号][*3]		

*1 ロール内の制限項目[新規宛先への送信]でユーザーごとに制限できます。
*2 ロール内の制限項目[送信時の機器署名]でユーザーごとに制限できます。
*3 アドレス帳の利用は、ロール内の制限項目[アドレス帳の利用/ネットワーク保存先の登録]でユーザーごとに制限できます。
*4 機種によっては、この項目は表示されません。

重要

- [設定/登録]画面で機能が制限されている場合、その機能に関連したショートカットは使用できません。
- ロール内の制限項目[スキャン]で、スキャン機能の使用が制限されている場合は、[ファンクション設定]→[共通]→[印刷動作]→[合成のフォーム登録]を使用できません。
- ロール内の制限項目[アドレス帳の利用/ネットワーク保存先の登録]で、アドレス帳の利用が[利用不可]に設定されている場合は、[宛先設定]→[宛先表リスト]/[宛先の登録]/[宛先表の名称登録]/[ワンタッチ登録]/[アドレス帳のデフォルト表示の変更]を使用できません。
  [閲覧のみ可能]に設定されている場合は、[宛先設定]→[宛先の登録]/[宛先表の名称登録]/[ワンタッチ登録]/[アドレス帳のデフォルト表示の変更]を使用できません。

デバイス機能の使用制限

ベースロールには、デバイス機能の使用制限が、以下のように設定されています。カスタムロールでは、以下の各項目の設定を変更することができます。

[機能カテゴリー制限](P. 26)
[機能カテゴリー制限の詳細](P. 27)
[アプリケーション制限](P. 32)
[ボタン制限](P. 33)

重要

- ゲストロール（[GuestUser]）は、デバイスの使用制限の設定値を変更することができます。カスタムロール（管理者）（[DeviceAdmin]/[NetworkAdmin]）は、デバイスの使用制限の設定値を変更できません。

[機能カテゴリー制限]

デバイス機能の使用制限を、カテゴリーごとに設定します。

重要

- ここでの設定よりも、[アプリケーション制限]の設定が優先されます。

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
プリント機能	許可する	○	○	○	○	○
	許可しない					
保存機能(ボックス/ホールド/メモリーメディア)	許可する	○	○	○		
	許可しない				○	○
コピー機能	許可する	○	○	○	○	○
	許可しない					
送信機能/ネットワークへの保存	許可する	○	○	○		
	許可しない				○	○
ウェブブラウザー機能	許可する	○	○	○		

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
	許可しない				○	○
ユーティリティー機能	許可する	○	○	○		
	許可しない				○	○
その他の機能	許可する	○	○	○		
	許可しない				○	○

[機能カテゴリー制限の詳細]

[機能カテゴリー制限]と[アプリケーション制限]で[許可する]に設定されているか、未設定のデバイス機能について、使用制限を詳細に設定します。

メモ

- お使いの機種によっては、対応していない制限項目があります。

プリント機能

コンピューターからの文書の出力制限（出力先：プリント、ボックス）を設定します。

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
プリント	許可する	○	○	○	○	○
	許可しない					
カラープリント	カラープリント可能	○	○	○		
	モノクロプリントのみ可能				○	○
プリント方法	片面プリント可能	○	○	○		
	両面プリントのみ可能				○	○
ページレイアウト	制限なし	○	○	○		
	1 in 1 不可					
	1～2 in 1 不可				○	○
ボックスへの保存	許可する	○	○	○		

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
	許可しない				○	○

重要

- 機種によって、ボックスへの保存機能を使用するにはファームウェアのバージョンアップが必要です。お使いのデバイスでファームウェアのバージョンアップが必要かどうかについては、担当サービスにお問い合わせください。

保存機能(ボックス/メモリーメディア)

ボックス文書の出力制限（出力先：プリント）を設定します。

重要

- この項目で制限できるのは、MEAP アプリケーションによるボックス文書の出力のみです。MEAP アプリケーション以外の機能を使ったボックス文書の出力は制限できません。たとえば、USB メモリをデバイスに接続して USB メモリ内の文書をプリントする操作は、AMS では制限できません。

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
プリント	許可する	○	○	○		
	許可しない				○	○
カラープリント	制限なし	○	○	○		
	フルカラープリント不可					
	フルカラー/2 色カラープリント不可					
	モノクロプリントのみ可能				○	○
プリント方法	片面プリント可能	○	○	○		
	両面プリントのみ可能				○	○
ページレイアウト	制限なし	○	○	○		
	1 in 1 不可					
	1～2 in 1 不可				○	○

保存機能（メモリーメディア）

メモリーメディアへの文書の入出力制限を設定します。

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
メモリーメディア	許可する	○	○	○		
	許可しない				○	○
スキャン	許可する	○	○	○		
	許可しない				○	○
プリント	許可する	○	○	○		
	許可しない				○	○

コピー機能

スキャン文書の出力制限（出力先：プリント）を設定します。

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
カラーコピー	制限なし	○	○	○		
	フルカラーコピー不可					
	フルカラー/2 色カラーコピー不可					
	モノクロコピーのみ可能				○	○
コピー方法	片面コピー可能	○	○	○		
	両面コピーのみ可能				○	○
ページレイアウト	制限なし	○	○	○		
	1 in 1 不可					
	1〜2 in 1 不可				○	○

スキャン機能

スキャン機能の使用制限を設定します。

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
スキャン	許可する	○	○	○		
	許可しない				○	○
カラースキャン	許可する	○	○	○		

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
	許可しない				○	○

送信機能/ネットワークへの保存

スキャン文書やボックス文書の出力制限（出力先：外部送信）などを設定します。ファイルサーバーやネットワークストレージへの保存にも適用します。

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
E メール送信	許可する	○	○	○		
	許可しない				○	○
E メール送信（「自分へ送信」機能の利用）	許可する	○	○	○		
	許可しない				○	○
I ファクス送信	許可する	○	○	○		
	許可しない				○	○
ファクス送信	許可する	○	○	○		
	許可しない				○	○
FTP 送信	許可する	○	○	○		
	許可しない				○	○
Windows（SMB）送信	許可する	○	○	○		
	許可しない				○	○
「マイフォルダー」送信機能の利用	スキャン文書やボックス文書の出力制限（出力先：マイフォルダー）を設定します。					
	許可する	○	○	○		

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
	許可しない				○	○
WebDAV 送信	許可する	○	○	○		
	許可しない				○	○
ボックス送信	スキャン文書の出力制限（出力先：ボックス）を設定します。					
	許可する	○	○	○		
	許可しない				○	○
宛先ドメインの指定	許可する	○	○			
	許可しない			○	○	○
アドレス帳の利用/ネットワーク保存先の登録	ネットワークストレージの登録/編集/削除にも適用されます。 User Authentication が搭載されている機種では、リモート UI で提供されるアドレス帳（宛先表の管理機能）の使用制限にも適用されます。					
	制限なし	○	○			
	利用不可				○	○
	閲覧のみ可能			○		
個人宛先表の利用	個人宛先表の使用制限を設定します。					
	許可する	○	○			
	許可しない			○	○	○
新規宛先への送信	許可する	○	○	○		
	許可しない				○	○
送信時の機器署名	PDF 送信時の機器署名の使用制限を設定します。					

制限項目		[Administrator] [DeviceAdmin] [NetworkAdmin]	[PowerUser]	[GeneralUser]	[LimitedUser]	[GuestUser]
	付加する				○	○
	付加しない	○	○	○		
送信するファイル形式	機器署名を付加できないファイル形式の送信の使用制限を設定します。					
	制限なし	○	○	○		
	制限する				○	○

[アプリケーション制限]

AMS では、機能ごと（[機能カテゴリー制限]と[機能カテゴリー制限の詳細]）の使用制限のほかに、アプリケーションごとの使用制限（[アプリケーション制限]）を設定することができます。

[アプリケーション制限]が設定されている場合は、その設定値に従って使用制限されますが、未設定の場合は、そのアプリケーションが所属する[機能カテゴリー制限]と[機能カテゴリー制限の詳細]の設定値に従って使用制限されます。いずれの機能カテゴリーにも所属していないアプリケーションは、[機能カテゴリー制限]の[その他の機能]の設定値に従って使用制限されます。

基本アプリケーションは、それぞれ、以下の機能カテゴリーに所属しています。

基本アプリケーション	カテゴリー
ウェブブラウザー	[ウェブブラウザー機能]カテゴリー
コピー	[コピー機能]カテゴリー
スキャンして送信/ファクス	[送信機能/ネットワークへの保存]カテゴリー
プリント/セキュアプリント	[プリント機能]カテゴリー
ホールド	[保存機能（ボックス/ホールド/メモリーメディア）]カテゴリー
モバイルプリント	[プリント機能]カテゴリー
保存ファイルの利用	[保存機能（ボックス/ホールド/メモリーメディア）]カテゴリー

重要

- [機能カテゴリー制限]での設定よりも、[アプリケーション制限] の設定が優先されます。
- ベースロールとカスタムロール（管理者）には、アプリケーション制限を設定できないので、すべてのアプリケーションについて、そのアプリケーションが所属する[機能カテゴリー制限]と[機能カテゴリー制限の詳細]の設定値に従って使用制限されます。

[ボタン制限]

User Authentication が搭載されている機種では、メインメニューやカスタムメニュー上のボタンに、使用制限を設定することができます。

ただし、ボタンにはアプリケーションにより提供される機能の一部が登録されているので、［アプリケーション制限］で［許可しない］に設定されている機能は、［ボタン制限］で使用を制限していなくても、使用できません。

基本アプリケーションにより提供される以下のボタンについて、使用制限を設定できます。

ボタン/アプレット名	アプリケーション名
コピー	コピー
ファクス	スキャンして送信
スキャンして送信	スキャンして送信
スキャンして保存	保存ファイルの利用
保存ファイルの利用	保存ファイルの利用
受信トレイ	保存ファイルの利用
セキュアプリント	セキュアプリント
ウェブブラウザー	ウェブブラウザー
リモートスキャナー	リモートスキャナー

重要

- ベースロールとカスタムロール（管理者）には、ボタン制限を設定できないので、すべてのボタンについて、そのボタンが所属するアプリケーションが所属する［機能カテゴリー制限］と［機能カテゴリー制限の詳細］の設定値に従って使用制限されます。

Access Management System の構成

Access Management System は、以下のソフトウェアで構成されます。

ソフトウェア	説明
User Authentication	AMS 対応のログインアプリケーションで、デバイス上で動作します。ロール情報を保持して、各ユーザーに関連付けられているロールに従って、デバイスの使用制限を実行します。また、ユーザー認証方式を選択可能なログインサービスを提供します。ローカルデバイス認証方式の場合は、ユーザー情報も保持して、ユーザー認証も行います。
ACCESS MANAGEMENT SYSTEM Printer Driver Add-in（AMS Printer Driver Add-in）	User Authentication から取得したロール情報に従って、コンピューターからの印刷を制限するための Add-in ソフトウェアです。AMS Printer Driver Add-in を有効化するには、あらかじめコンピューターに対応プリンタードライバーがインストールされている必要があります。

重要

- 以下のいずれかの条件を満たす場合は、AMS Printer Driver Add-in を有効化しなくても、ユーザーのカラー印刷、片面印刷、ボックスへの保存を制限することができます。

条件 1

- ローカルデバイス認証を使用している*1
- クライアントコンピューターで以下のいずれかのプリンタードライバーを使用している

  Canon LIPS4 Printer Driver V21.50 以降

  Canon LIPSLX Printer Driver V21.50 以降

  Canon LIPSLX V4 Printer Driver V5.10 以降
- デバイスで[ユーザー認証していないリモートジョブ]の制限が ON に設定されている
- プリンタードライバーで[ユーザー認証の設定]が設定されている

*1 サーバー認証を使用している場合は、ユーザーの印刷を制限するために AMS Printer Driver Add-in を有効化する必要があります。

条件 2

- デバイス認証または機能別認証を利用して、[プリント]にユーザー認証が設定されている
- [設定/登録]→[ファンクション設定]→[プリント]→[強制留め置き]が ON に設定されている

- サーバー認証を使用している場合は、ユーザーの印刷を制限するために AMS Printer Driver Add-in を有効化する必要があります。
- ユーザーがコンピューターから印刷する際のページレイアウトを制限する場合は、AMS Printer Driver Add-in を有効化する必要があります。
- [ユーザー認証していないリモートジョブ]の制限については、「**リモートジョブの使用制限を設定する (P. 57)**」を参照してください。
- プリンタードライバーについては、プリンタードライバーの取扱説明書を参照してください。

Access Management System の管理者について

Access Management System の運用には、以下の権限を持った管理者が必要です。必要な権限を与えることによって、1 人の管理者で運用することもできます。

ローカルデバイス認証方式で運用する場合(P. 35)
LDAP 認証方式で運用する場合(P. 35)
Active Directory 認証方式で運用する場合(P. 36)

ローカルデバイス認証方式で運用する場合

管理者の種類	役割	必要な権限
デバイスの管理者	● Access Management System の構成の決定 ● 使用制限の対象デバイスの管理 - 日付/時刻の設定 - ネットワークの設定 - システム管理部門 ID の登録 - User Authentication の起動 ● 使用制限の管理者ユーザーの選定	SMS（Service Management Service）にログインできる ただし、AMS の運用開始後は、[Administrator]ロールが関連付けられていることが必要です。
使用制限の管理者	● デバイスの環境設定 ● セキュリティーの設定 ● ユーザーの管理 ● ロールの管理 ● ロールとユーザーの関連付け	● [Administrator]ロールが関連付けられている
クライアントコンピューターの管理者	● クライアントコンピューターへのプリンタードライバーのインストールや更新 ● クライアントコンピューターにインストールしたプリンタードライバーで AMS 機能の有効化	クライアントコンピューターで使用している Windows の Administrator 権限

LDAP 認証方式で運用する場合

管理者の種類	役割	必要な権限
デバイスの管理者	● Access Management System の構成の決定 ● 使用制限の対象デバイスの管理 - 日付/時刻の設定 - ネットワークの設定 - システム管理部門 ID の登録 - User Authentication の起動 ● 使用制限の管理者ユーザーの選定	SMS（Service Management Service）にログインできる ただし、AMS の運用開始後は[Administrator]ロールが関連付けられていることが必要です。
使用制限の管理者	● デバイスの環境設定（デフォルトロールの設定） ● セキュリティーの設定 ● ユーザーの管理 ● ゲストロールの管理	● [Administrator]ロールが関連付けられている

管理者の種類	役割	必要な権限
クライアントコンピューターの管理者	• クライアントコンピューターへのプリンタードライバーのインストールや更新 • クライアントコンピューターにインストールしたプリンタードライバーで AMS 機能の有効化	• クライアントコンピューターで使用している Windows の Administrator 権限

Active Directory 認証方式で運用する場合

管理者の種類	役割	必要な権限
デバイスの管理者	• Access Management System の構成の決定 • 使用制限の対象デバイスの管理 - 日付/時刻の設定 - ネットワークの設定 - システム管理部門 ID の登録 - User Authentication の起動 • 使用制限の管理者ユーザーの選定	SMS（Service Management Service）にログインできる ただし、AMS の運用開始後は、[Administrator]ロールが関連付けられていることが必要です。
社内ネットワークの管理者	• DNS サーバーの設定 • ドメイン間の信頼関係の設定 • Active Directory への使用制限の管理者ユーザーグループの作成/ユーザーの追加	• DNS サーバーの管理者権限（マルチドメイン使用時） • Active Directory の管理者権限
使用制限の管理者	• デバイスの環境設定 • セキュリティーの設定 • ユーザーの管理 • ロールの管理 • ロールとユーザーの関連付け	• [Administrator]ロールを関連付けられている • Active Directory の管理者権限
クライアントコンピューターの管理者	• クライアントコンピューターへのプリンタードライバーのインストールや更新 • クライアントコンピューターにインストールしたプリンタードライバーで AMS 機能の有効化	クライアントコンピューターで使用している Windows の Administrator 権限

必要な動作環境

ここでは Access Management System の動作環境について説明します。

対応デバイス(P. 37)
クライアントコンピューター（AMS Printer Driver Add-in ）(P. 37)

対応デバイス

Access Management System は、User Authentication が起動していて、AMS のライセンス登録が完了しており、さらに、AMS が有効に設定されているデバイス（AMS 対応デバイス）で使用できます。

クライアントコンピューター（AMS Printer Driver Add-in ）

ユーザーのコンピューターからの印刷機能を制限するには、AMS 対応デバイスのプリンタードライバーに AMS Printer Driver Add-in を有効化することが必要です。クライアントコンピューター（印刷を行うコンピューター）の動作環境は、以下のとおりです。

対応プリンタードライバー

次のいずれかのプリンタードライバーを、あらかじめコンピューターにインストールしておくことが必要です。

- Generic Plus LIPS4 Printer Driver Ver.2.30 以降
- Generic Plus PS3 Printer Driver Ver.2.30 以降
- Generic Plus LIPSLX Printer Driver Ver.2.30 以降

対応 OS

プリンタードライバーの対応 OS については、プリンタードライバーの取扱説明書を参照してください。

共存可能な Add-in

- Canon imageWARE Trust Stamp Add-in
- Canon 暗号化セキュアプリント Driver Add-in for Client PC
- Canon imageWARE Secure Audit Manager Printer Driver Add-in
- Canon imageWARE Enterprise Management Console アカウント集計管理 Driver Add-in

重要

- プリンタードライバーのセキュアプリント機能または暗号化セキュアプリント Driver Add-in for Client PC が印刷時に表示するダイアログボックスでは、ユーザー名を指定できません（Windows の Administrator 権限を持つユーザーでコンピューターにログオンしている場合、ユーザー名を指定できますが無視されます）。[AMS]ページの[現在設定されているユーザー名]に表示されているユーザー名で、印刷が実行されます。

Access Management System をセットアップする

Access Management System をセットアップする 39
ローカルデバイス認証方式で運用する場合のセットアップの流れ 40
サーバー認証方式で運用する場合のセットアップの流れ 42
デバイスとネットワーク環境の準備 44
User Authentication にログインする 47
デバイスの環境設定を行う 48
User Authentication の場合 49
ロールを管理する 62
User Authentication の場合 63

Access Management System をセットアップする

ここでは、使用制限の対象となるデバイスの準備や各種ソフトウェアのインストール方法など、Access Management System のセットアップについて説明します。

ローカルデバイス認証方式で運用する場合のセットアップの流れ

ここでは、Access Management System をローカルデバイス認証方式で運用する場合のセットアップの流れを説明します。

重要

- システム構成やユーザー認証方式によって、必要な手順が異なります。サーバー認証方式で運用する場合は、「**サーバー認証方式で運用する場合のセットアップの流れ(P. 42)**」を参照してください。

1. デバイスとネットワーク環境の準備(P. 44)

Access Management System で運用するすべてのデバイスについて、ネットワーク環境や日時などを設定し、システム管理部門 ID を登録します。

2. AMS を有効にする

Access Management System で運用するすべてデバイス上で、AMS を有効にします。

詳細は、デバイスに付属の取扱説明書を参照してください。

3. User Authentication を起動する

すべての AMS 対応デバイスで、User Authentication を起動します。

詳細は、デバイスに付属の取扱説明書を参照してください。

4. セキュリティーを設定する

パスワードやロックアウトのポリシーなど、セキュリティーに関する設定を行います。

詳細は、デバイスに付属の取扱説明書を参照してください。

5. デバイスの環境設定を行う(P. 48)

すべての AMS 対応デバイスの環境設定を行います。

- **ユーザー認証方式を設定する(P. 49)**
- **登録ユーザーのデフォルトロールを設定する(P. 49)**
- **ロールの関連付け(P. 51)**
- **ログイン方式を設定する(P. 51)**
- **未登録ユーザーのログインを許可する(P. 51)**
- **ログイン画面に表示されるユーザーのログイン履歴数を設定する(P. 52)**

- **プリンタードライバーによるユーザー認証情報の保持を許可する(P. 53)**
- **AMS Printer Driver Add-in を使用しないドライバーからの印刷を禁止する(P. 54)**
- **リモートジョブの使用制限を設定する(P. 57)**
- **リモートスキャン/重連コピーの使用制限を設定する(P. 59)**
- **転送時の機器署名を設定する(P. 59)**
- **IPP 印刷を設定する(P. 60)**

6. ロールを管理する(P. 62)

必要に応じて、カスタムロールを作成/編集し、ゲストロールを編集します。ロールは、インポート/エクスポートできるので、複数台のデバイス上で利用できます。

- **カスタムロールを作成する(P. 63)**
- **カスタムロールを編集する(P. 67)**
- **[GuestUser]ロール（ゲストロール）を編集する(P. 68)**
- **カスタムロールを削除する(P. 69)**
- **ロールをインポートする(P. 70)**
- **ロールをエクスポートする(P. 72)**

7. ユーザーを管理する

デバイスを使用するユーザーを登録/編集します。ユーザー情報には適用するロール名も登録します。ロール名を登録しない場合、そのユーザーには、デバイスの環境設定の[デフォルトロール]で設定したロールが適用されます。ユーザー情報は、インポート/エクスポートできるので、複数台のデバイス上で利用できます。

詳細は、デバイスに付属の取扱説明書を参照してください。

ローカルデバイス認証方式で運用する場合の注意事項

ここでは、Access Management System をローカルデバイス認証方式で運用する際の注意事項について説明します。

部門別 ID 管理機能との併用について

部門別 ID 管理機能を併用する場合は、Access Management System のセットアップ（上記の操作）をすべて完了してから、部門別 ID 管理機能を起動し、部門 ID を登録してください。部門別 ID 管理機能の詳細は、デバイスに付属の取扱説明書を参照してください。

部門別 ID 管理機能を併用する場合は、ユーザー情報に登録した[部門 ID]および[パスワード]と、部門別 ID 管理情報に登録した[部門 ID]および[暗証番号]が一致している必要があります。機器情報配信などによって、部門別 ID 管理情報が変更された場合は、ユーザー情報もあわせて変更してください。

コンピューターからの印刷の制限について

コンピューターからの印刷を制限するには、上記の操作が完了した後、コンピューターにインストールされているプリンタードライバーで AMS 機能を有効化する必要があります。詳細は、プリンタードライバーの取扱説明書を参照してください。

サーバー認証方式で運用する場合のセットアップの流れ

ここでは、Access Management System をサーバー認証方式で運用する場合のセットアップの流れを説明します。

重要

- サーバー認証方式で運用する場合は、サーバーで管理されているユーザー情報を利用するので、ローカルデバイス認証方式でのユーザー管理に関する操作は不要です。
- システム構成やユーザー認証方式によって、必要な手順が異なります。ローカルデバイス認証方式で運用する場合は、「**ローカルデバイス認証方式で運用する場合のセットアップの流れ(P. 40)**」を参照してください。

1. デバイスとネットワーク環境の準備(P. 44)

Access Management System で運用するすべてのデバイスについて、ネットワーク環境や日時などを設定し、システム管理部門 ID を登録します。

2. AMS を有効にする

Access Management System で運用するすべてデバイス上で、AMS を有効にします。

詳細は、デバイスに付属の取扱説明書を参照してください。

3. User Authentication を起動する

すべての AMS 対応デバイスで、User Authentication を起動します。

詳細は、デバイスに付属の取扱説明書を参照してください。

4. セキュリティーを設定する

パスワードやロックアウトのポリシーなど、セキュリティーに関する設定を行います。

詳細は、デバイスに付属の取扱説明書を参照してください。

5. デバイスの環境設定を行う(P. 48)

すべての AMS 対応デバイスの環境設定を行います。

- **ユーザー認証方式を設定する(P. 49)**
- **登録ユーザーのデフォルトロールを設定する(P. 49)**
- **ロールの関連付け(P. 51)**
- **ログイン方式を設定する(P. 51)**
- **未登録ユーザーのログインを許可する(P. 51)**
- **ログイン画面に表示されるユーザーのログイン履歴数を設定する(P. 52)**

- **プリンタードライバーによるユーザー認証情報の保持を許可する(P. 53)**
- **AMS Printer Driver Add-in を使用しないドライバーからの印刷を禁止する(P. 54)**
- **リモートジョブの使用制限を設定する(P. 57)**
- **リモートスキャン/重連コピーの使用制限を設定する(P. 59)**
- **転送時の機器署名を設定する(P. 59)**
- **IPP 印刷を設定する(P. 60)**

6. ロールを管理する(P. 62)

必要に応じて、カスタムロールを作成/編集し、ゲストロールを編集します。ロールは、インポート/エクスポートできるので、複数台のデバイス上で利用できます。

- **カスタムロールを作成する(P. 63)**
- **カスタムロールを編集する(P. 67)**
- **[GuestUser]ロール（ゲストロール）を編集する(P. 68)**
- **カスタムロールを削除する(P. 69)**
- **ロールをインポートする(P. 70)**
- **ロールをエクスポートする(P. 72)**

サーバー認証方式で運用する場合の注意事項

ここでは、Access Management System をサーバー認証方式で運用する際の注意事項について説明します。

ローカルデバイス認証とサーバー認証を併用する場合のセットアップの流れについて

Access Management System では、ネットワーク障害など何らかの原因でサーバーにアクセスできなくなった場合に備えて、ローカルデバイス認証との併用をおすすめしています。ローカルデバイス認証とサーバー認証を併用する場合は、「**ローカルデバイス認証方式で運用する場合のセットアップの流れ(P. 40)**」の Step1～7 に従って操作した後、「**サーバー認証方式で運用する場合のセットアップの流れ(P. 42)**」の Step5 を行ってください。

ローカルデバイス認証とサーバー認証を併用する環境を構築した場合、ローカルユーザー情報を作成しないでローカルデバイス認証方式でデバイスを使用すると、すべてのユーザーが未登録ユーザー（[GuestUser]）としてデバイスを使用することになります。

重要

- User Authentication のサーバー認証方式を利用する場合は、部門別 ID 管理機能と併用できません。

コンピューターからの印刷の制限について

コンピューターからの印刷を制限するには、上記の操作が完了した後、コンピューターにインストールされているプリンタードライバーで AMS 機能を有効化する必要があります。詳細は、プリンタードライバーの取扱説明書を参照してください。

デバイスとネットワーク環境の準備

ここでは、使用制限の対象となるデバイスとネットワーク環境の設定について説明します。

- **日付/時刻を設定する(P. 44)**
- **ネットワークの設定をする(P. 44)**
- **Web ブラウザーからデバイスにアクセスできるようにする(P. 45)**
- **システム管理部門 ID を登録する(P. 45)**
- **LDAP サーバーを設定する(P. 45)**
- **DNS サーバーを設定する(P. 45)**
- **ドメインの信頼関係を設定する(P. 46)**

日付/時刻を設定する

Access Management System では、システムを構成するすべての機器（デバイス、クライアントコンピューター、サーバーコンピュータなど）の日付と時刻が合っていることが必要です。

[設定/登録]画面にある[環境設定]の[タイマー/電力設定]の[日付/時刻設定]で、日付と時刻を正しく設定します。

詳細は、デバイスに付属の取扱説明書を参照してください。

ネットワークの設定をする

Access Management System を導入するには、ネットワークからデバイスにアクセスできるように設定しておく必要があります。

[設定/登録]画面にある[環境設定]の[ネットワーク]で、各項目を設定します。

詳細は、デバイスに付属の取扱説明書を参照してください。

重要

- デバイスがすでにネットワーク上で運用されている場合（コンピューターからの印刷や送信機能が使用できている場合）は、この操作は不要です。

DNS サーバーを登録する

デバイスをドメイン環境で利用するには、使用する DNS サーバーをデバイスに登録する必要があります。

[設定/登録]画面にある[環境設定]の[ネットワーク]で設定します。

詳細は、デバイスに付属の取扱説明書を参照してください。

重要

- デバイスがすでにドメイン環境で運用されている場合は、この操作は不要です。

Web ブラウザーからデバイスにアクセスできるようにする

Access Management System を導入するには、Web ブラウザーからデバイスにアクセスできるように設定しておく必要があります。

詳細は、デバイスに付属の取扱説明書を参照してください。

重要

- プロキシサーバー経由では接続できません。プロキシサーバーをお使いの場合は、Web ブラウザーのプロキシサーバーの設定で、[例外]（プロキシを使用しないアドレス）にデバイスの IP アドレスを追加してください。（設定はネットワーク環境によって異なりますので、社内ネットワークの管理者に相談してください）。
- Web ブラウザーで、クッキー（Cookie）、JavaScript、JavaApplet を利用できるように設定していない場合は、この機能を使用できません。
- Web ブラウザーから文字を入力するときは、デバイスのタッチパネルディスプレーから入力できる文字を使用してください。それ以外の文字を使用すると、デバイスで正常に表示/認識されないことがあります。

システム管理部門 ID を登録する

Access Management System で適切に使用制限を行うには、システム管理部門 ID を登録しておく必要があります。

[設定/登録]画面にある[管理設定]の[ユーザー管理]の[システム管理者情報の設定]で設定します。

詳細は、デバイスに付属の取扱説明書を参照してください。

重要

- システム管理部門 ID とシステム管理暗証番号を知らなくても、[Administrator]/[DeviceAdmin]/[NetworkAdmin]の権限に応じたシステム管理設定を行うことができます。

LDAP サーバーを設定する

LDAP サーバー認証方式を利用する場合は、LDAP サーバーの情報を、User Authentication に設定します。詳細は、デバイスに付属の取扱説明書を参照してください。

DNS サーバーを設定する

デバイスをマルチドメイン環境で使用するために、以下のように、DNS サーバーを設定します。設定方法の詳細は、お使いの DNS サーバーの取扱説明書を参照してください。

- 認証先の Active Directory の DNS ドメイン名の名前解決が行える（ドメインコントローラーの IP アドレスを取得できる）
- DNS が SRV レコードをサポートしている

Active Directory 側で LDAP ポートのポート番号を変更している場合には、さらに、以下の設定が必要です。

- Active Directory の LDAP サービスの情報が SRV レコードとして以下のように登録されている
  - サービス：「_ldap」
  - プロトコル：「_tcp」
  - ポート番号：Active Directory ドメイン（ゾーン）の LDAP サービスが実際に使用しているポート番号

- このサービスを提供しているホスト：Active Directory ドメイン（ゾーン）の LDAP サービスを実際に提供しているドメインコントローラのホスト名

重要

- デバイスがすでにマルチドメイン環境で運用されている場合は、この操作は不要です。

ドメインの信頼関係を設定する

Access Management System では、ユーザーが所属しているドメインと信頼関係にあるドメインに所属するデバイスの使用制限も実行することができます。

Access Management System を Active Directory 認証方式で運用する場合に、ユーザーの所属ドメインとデバイスの所属ドメインが異なる場合は、ドメイン間に双方向の信頼関係を設定する必要があります。

重要

- Access Management System を Active Directory 認証以外のユーザー認証方式で運用する場合は、この操作は不要です。
- Active Directory の階層構造により発生する信頼関係では、ユーザーが所属しているドメインと異なるドメインに所属するデバイスの使用制限は実行できません。直接の信頼関係を設定してください。

User Authentication にログインする

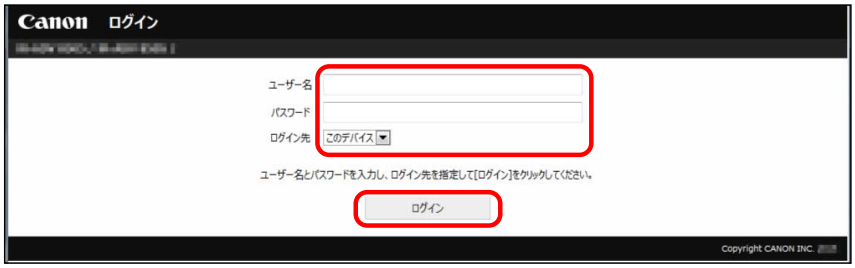
ロール管理やユーザー管理、デバイスの環境設定を行う際には、User Authentication にログインします。

1 Web ブラウザーを起動し、以下の URL を入力します。

http://< デバイスの IP アドレスまたはホスト名>

[ログイン]ページが表示されます。

2 [Administrator]ロールが関連付けられているユーザーのユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]をクリックします。



メモ

- お使いの機種が二要素認証を有効にしている場合は、[ログイン]をクリックしたあとにワンタイムパスワードを入力します。詳細は、デバイスに付属の取扱説明書を参照してください。

3 操作が終了したら、[ログアウト]をクリックします。

デバイスの環境設定を行う

ここでは、Access Management System を運用する場合のデバイスの環境設定について説明します。

User Authentication の場合(P. 49)

重要

- デバイスの環境設定は、[Administrator]ロールを関連付けられているユーザーのみが行えます。（[DeviceAdmin]や[NetworkAdmin]も含めて[Administrator]を元に作成したカスタムロールを関連付けられたユーザーは、デバイスの環境設定を行えません。）
- 使用するユーザー認証方式によって、設定すべき項目が異なります。詳細は、「**ローカルデバイス認証方式で運用する場合のセットアップの流れ(P. 40)**」または「**サーバー認証方式で運用する場合のセットアップの流れ(P. 42)**」を参照してください。

User Authentication の場合

ここでは、User Authentication で、デバイスの環境設定を行う方法について説明します。

- **ユーザー認証方式を設定する(P. 49)**
- **登録ユーザーのデフォルトロールを設定する(P. 49)**
- **ロールの関連付け(P. 51)**
- **ログイン方式を設定する(P. 51)**
- **未登録ユーザーのログインを許可する(P. 51)**
- **ログイン画面に表示されるユーザーのログイン履歴数を設定する(P. 52)**
- **プリンタードライバーによるユーザー認証情報の保持を許可する(P. 53)**
- **AMS Printer Driver Add-in を使用しないドライバーからの印刷を禁止する(P. 54)**
- **リモートジョブの使用制限を設定する(P. 57)**
- **リモートスキャン/重連コピーの使用制限を設定する(P. 59)**
- **転送時の機器署名を設定する(P. 59)**
- **IPP 印刷を設定する(P. 60)**

ユーザー認証方式を設定する

ユーザー認証方式を設定してください。詳細は、デバイスに付属の取扱説明書を参照してください。

登録ユーザーのデフォルトロールを設定する

ローカルデバイス認証方式を利用する場合に、ロールが関連付けられていないユーザー（ユーザー情報にロール名が書き込まれていないユーザー）がデバイスにログインした場合に適用されるロールを、ベースロールから選択します。

各ベースロールの使用制限については、「**ベースロールとカスタムロールについて(P. 20)**」を参照してください。

重要

- ベースロールにはアプリケーションの使用制限やボタンの使用制限を設定できないため、[デフォルトロールの設定]で指定したロールが適用されるユーザーには、アプリケーションごとやボタンごとの使用を制限できません。アプリケーションやボタンの使用を制限したいユーザーには、適切なカスタムロールを作成し、関連付ける必要があります。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[基本設定]をクリックします。

3 [編集]をクリックします。

4 [デフォルトロールの設定]の[ユーザー登録時のデフォルトロール]で、ロールを選択し、[更新]をクリックします。

ローカルデバイス認証方式を利用する場合は、ユーザー情報にロール名が書き込まれていないユーザーに、ここで選択されたロールが適用されます。

サーバー認証方式を利用する場合は、サーバーに登録されているユーザー情報に基づいて認証されたすべてのユーザーのうち、ロールの関連付けの条件に一致しないユーザーに、ここで選択されたロールが適用されます。

重要

- [デフォルトロールの設定]の設定は、デバイスの再起動後に有効になります。再起動の方法については、デバイスに付属の取扱説明書を参照してください。

ロールの関連付け

サーバー認証方式を利用する場合は、[ロールの関連付け]でサーバー認証のユーザーに適用するロールを設定してください。詳細は、デバイスに付属の取扱説明書を参照してください。

ログイン方式を設定する

ユーザー認証のためのログイン画面を表示するタイミングを設定します。ログイン方式には、「デバイス認証」と「機能別認証」の 2 種類があります。詳細は、デバイスに付属の取扱説明書を参照してください。

重要

- 機能別認証を選択する場合は、登録ユーザーに適用する使用制限が未登録ユーザーの使用制限（ゲストロール）よりも厳しくならないように、カスタムロールの作成/編集時やゲストロールの編集時に、特に注意してください。登録ユーザーに適用する使用制限が未登録ユーザーの使用制限よりも厳しい場合、ログイン前よりもログイン後の方が使用できる機能が少なくなってしまうので、適切にユーザー管理ができなくなる可能性があります。

未登録ユーザーのログインを許可する

ユーザー情報が登録されていないユーザーのデバイスへのログインを許可するかどうかを設定します。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

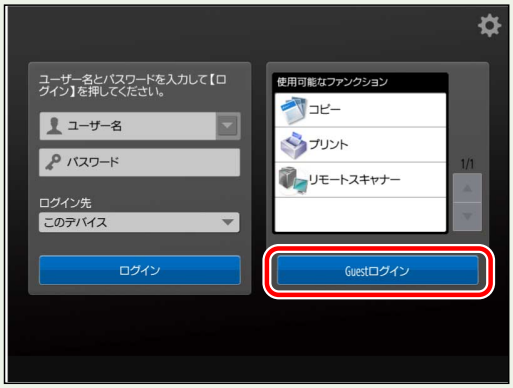
2 [設定/登録]→[ユーザー管理]→[認証管理]→[操作パネルの設定]をクリックします。

3 [編集]をクリックします。

4 [未登録ユーザーのログイン]の[Guest User としてログインを許可する]にチェックマークを付けて、[更新]をクリックします。

メモ

- [GuestUser]ロール（ゲストロール）は、編集できます。詳細は、「**[GuestUser]ロール（ゲストロール）を編集する(P. 68)**」を参照してください。
- ログイン方式としてデバイス認証を選択している場合に、[Guest User としてログインを許可する]にチェックマークを付けると、デバイスのタッチパネルディスプレーには、以下のようなログイン画面が表示されます。未登録ユーザーがログインするときは、ユーザー名とパスワードを入力しないで、[Guest ログイン]を押します。未登録ユーザーが使用できる機能は、[GuestUser]ロールの使用制限情報に従います。



ログイン画面に表示されるユーザーのログイン履歴数を設定する

ログイン時にタッチパネルディスプレーに表示されるユーザーのログイン履歴の数を設定します。履歴が残るように設定しておくと、ログイン時にユーザー名を履歴から選択できるので、入力の手間を省くことができます。

メモ

- 詳細は、デバイスに付属の取扱説明書を参照してください。

プリンタードライバーによるユーザー認証情報の保持を許可する

AMS Printer Driver Add-in 上でユーザーが入力したパスワードを保持することを許可するかどうかを設定します。パスワードを保持すると、AMS Printer Driver Add-in で初回認証以降はパスワードの入力が不要になります。

重要

- ユーザー認証情報の保持を許可しない場合は、AMS Printer Driver Add-in の[認証に使うユーザー名/パスワードの設定]ダイアログボックスで、[パスワードを保存し、印刷時に認証情報を確認しない]チェックボックスが無効になり、パスワードを保存できません。

メモ

- AMS Printer Driver Add-in を使用しない場合は、この項目を設定する必要はありません。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[基本設定]をクリックします。

3 [編集]をクリックします。

4 [プリンタードライバーの制御]の[ユーザー認証情報を保持する]にチェックマークを付けて、[更新]をクリックします。

重要

- [プリンタードライバーの制御]の設定は、デバイスの再起動後に有効になります。再起動の方法については、デバイスに付属の取扱説明書を参照してください。

AMS Printer Driver Add-in を使用しないドライバーからの印刷を禁止する

印刷制限に対応していないジョブの印刷を禁止するかどうかを設定します。

重要

- この項目の設定により制限されるジョブには、リモート UI からのダイレクトプリントも含まれます。この項目にチェックマークを付けた場合は、リモート UI で提供されているダイレクトプリント機能も利用できません。
- AMS Printer Driver Add-in が有効化されていないコンピューターや、不明なユーザーでログオンしたコンピューターからの印刷を制限したい場合は、印刷制限に対応していないジョブの印刷を禁止してください。

メモ

- AMS Printer Driver Add-in を使用しない場合は、この項目を設定する必要はありません。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[基本設定]をクリックします。

3 [編集]をクリックします。

4 [利用を制限する機能]の[AMS Printer Driver Add-in を使用しないドライバーからのプリント]にチェックマークを付けて、[更新]をクリックします。

重要

- [利用を制限する機能]の設定は、デバイスの再起動後に有効になります。再起動の方法については、デバイスに付属の取扱説明書を参照してください。(デバイスの再起動後、タッチパネルディスプレーに初期化完了画面が表示されたら、画面の指示に従って、もう一度、デバイスの電源を入れなおします。)

メモ

- [AMS Printer Driver Add-in を使用しないドライバーからのプリント]にチェックマークを付けた場合、AMS Printer Driver Add-in を有効化したプリンタードライバーから印刷の際に、セキュリティーチェックを自動的に行います。不正が見つかった場合には印刷がキャンセルされます。

リモートジョブの使用制限を設定する

ユーザー認証していないリモートジョブの使用制限を設定します。

重要

- ローカルデバイス認証を使用時、AMS Printer Driver Add-in を有効化せずにユーザーの印刷を制限する場合は、[ユーザー認証していないリモートジョブ]の制限を ON にしてください。詳細は、「**Access Management System の構成(P. 34)**」を参照してください。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[基本設定]をクリックします。

3 [編集]をクリックします。

4 [利用を制限する機能]の[ユーザー認証していないリモートジョブ]にチェックマークを付けて、[更新]をクリックします。

重要

- [利用を制限する機能]の設定は、デバイスの再起動後に有効になります。再起動の方法については、デバイスに付属の取扱説明書を参照してください。(デバイスの再起動後、タッチパネルディスプレーに初期化完了画面が表示されたら、画面の指示に従って、もう一度、デバイスの電源を入れなおします。)

リモートスキャン/重連コピーの使用制限を設定する

リモートスキャン/重連コピーの使用制限を設定します。

重要

- 使用制限が行われている AMS 対応デバイスは、重連コピーの送信元として使用することはできません。

メモ

- 詳細は、デバイスに付属の取扱説明書を参照してください。
- 重連コピー機能に対応していないデバイスでは、[重連コピー]は表示されません。

転送時の機器署名を設定する

デバイスからファイルを転送するときに、そのファイルに機器署名を付加するかどうかを設定します。

メモ

- 転送時の機器署名とは、オプションの機器署名 PDF 拡張キットにより転送するファイルに機器署名を付加する機能です。詳細は、デバイスに付属の取扱説明書を参照してください。(オプションがない場合に本設定を行っても、機能を利用できません。)

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[基本設定]をクリックします。

3 [編集]をクリックします。

4 [セキュリティー設定]の[転送時に機器署名を付加する]にチェックマークを付けて、[更新]をクリックします。

重要

- [セキュリティー設定]の設定は、デバイスの再起動後に有効になります。再起動の方法については、デバイスに付属の取扱説明書を参照してください。

IPP 印刷を設定する

IPP 印刷するときに、認証を使用するかどうかを設定します。

IPP 印刷時に認証を使用すると、ロールにしたがってユーザーの印刷(AirPrint を含む)を制限できます。

1 User Authentication にログインします。

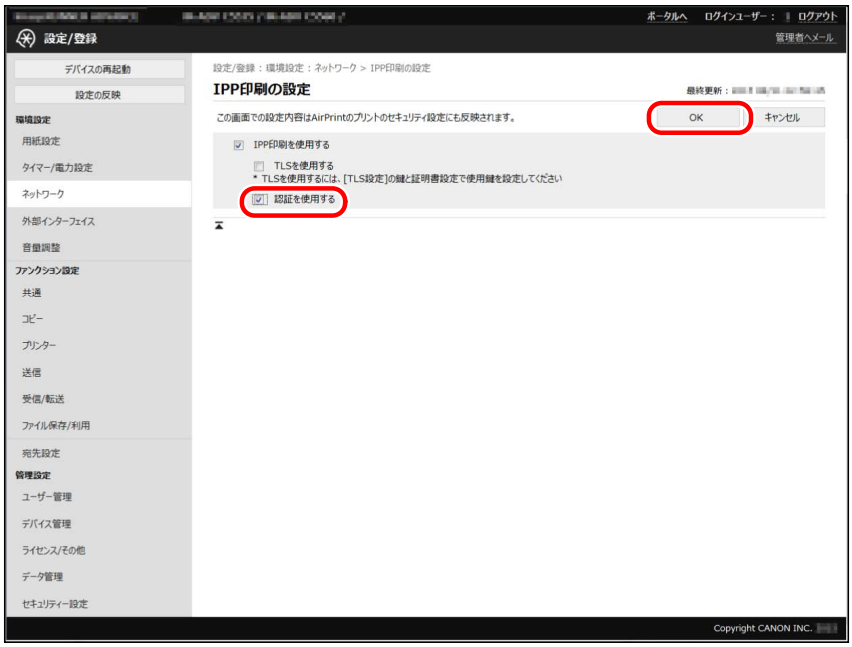
詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ネットワーク]→[IPP 印刷の設定]をクリックします。

3 [認証を使用する]にチェックマークを付けて、[OK]をクリックします。

メモ

- IPP 印刷を使用する設定になっている場合に、[認証を使用する]を設定できます。



ロールを管理する

ユーザーに関連付ける使用制限をロールとして登録/編集します。また、ロールを一括してインポート/エクスポートすることもできます。

ロールには、ベースロールとカスタムロールがあります。詳細は、「**ベースロールとカスタムロールについて(P. 20)**」を参照してください。

User Authentication の場合(P. 63)

重要

- ロールの管理は、[Administrator]ロールを関連付けられているユーザーのみが行えます。([DeviceAdmin]や[NetworkAdmin]も含めて[Administrator]を元に作成したカスタムロールを関連付けられたユーザーは、ロールの管理を行えません。)
- 使用するユーザー認証方式によって、必要な作業が異なります。詳細は、「**ローカルデバイス認証方式で運用する場合のセットアップの流れ(P. 40)**」または「**サーバー認証方式で運用する場合のセットアップの流れ(P. 42)**」を参照してください。

User Authentication の場合

ここでは、User Authentication で、ロールを管理する方法について説明します。

- **カスタムロールを作成する(P. 63)**
- **カスタムロールを編集する(P. 67)**
- **[GuestUser]ロール（ゲストロール）を編集する(P. 68)**
- **カスタムロールを削除する(P. 69)**
- **ロールをインポートする(P. 70)**
- **ロールをエクスポートする(P. 72)**

カスタムロールを作成する

カスタムロールとは、ユーザー定義ロールのことで、ベースロールをもとに使用制限情報を追加/編集して、作成します。

また、作成したカスタムロールを編集することもできます。詳細は、「**カスタムロールを編集する(P. 67)**」を参照してください。

重要

- 登録できるロール数は最大 100 件までです。（ベースロールおよびカスタムロール（管理者）を含みます。）
- 旧バージョンの Access Management System でデバイスに登録したカスタムロールを、本バージョンでも利用できます。
- お使いのデバイスが対応していない機能については、User Authentication からは制限値を設定/確認できませんが、デバイス内では、すべての制限項目についての制限値を保持しています。（このため、コンピューターからの印刷の際に、モノクロ複合機を指定している場合でも、[カラー印刷]の制限値として[可能]と表示される場合があります。）
- カスタムロールには、未登録ユーザーの使用制限（ゲストロール）よりも厳しい使用制限を設定しないでください。登録ユーザーに適用する使用制限が未登録ユーザーの使用制限よりも厳しいと、ログイン前や[Guest ログイン]よりもログイン後の方が使用できる機能が少なくなってしまうので、適切にユーザー管理ができなくなる可能性があります。

メモ

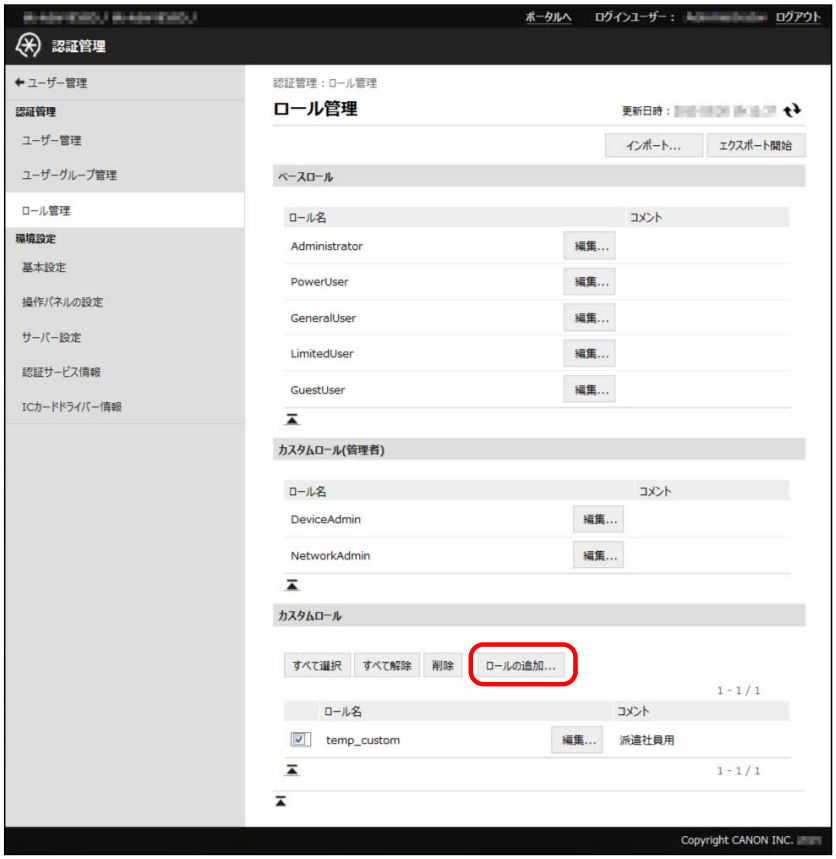
- カスタムロールを作成したら、バックアップのためエクスポートしておくことをおすすめします。また、エクスポートしたロールを他のデバイスにインポートすることで、作成したカスタムロールを複数のデバイスに登録できます。詳細は、「**ロールをインポートする(P. 70)**」、「**ロールをエクスポートする(P. 72)**」を参照してください。
- ユーザーへのロールの関連付けは、ユーザー管理画面から行います。デバイスに付属の取扱説明書を参照してください。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[ロール管理]をクリックします。

3 **[カスタムロール]の[ロールの追加]をクリックします。**



4 **必要な項目を設定し、[追加]をクリックします。**

新規のロールが登録されます。

入力する項目の内容、設定条件などは、以下のとおりです。

項目	設定内容	設定条件
[ロール名]	ロール名を設定します。	1 ～ 32 文字までの半角英数字および-（ハイフン）、_（アンダーバー）。すでに登録しているロール名は登録できません。 ベースロールやカスタムロール（管理者）と同じ名前や、類似する名前は付けられません。
[コメント]	ロールの説明を設定します。	0 ～ 50 文字までの任意の文字列
[元にするベースロール]	元にするベースロールを設定します。	[GuestUser]は設定できません。 ここで設定したベースロールにより、デバイスの管理権限が決まります。 [Administrator]が設定されている場合のみ、デバイス管理権限があります。
[デバイス管理制限]	デバイス管理権限をカテゴリーごとに設定します。 [すべての設定]： [制限なし]に設定されている場合は、[デバイス設定]と[ネットワーク設定]の設定値に関わらず、すべてのデバイス管理権限が制限されません。（デバイス管理権限について、[Administrator]ロールと同等の権限があります。） [制限する]に設定されている場合は、[デバイス設定]と[ネットワーク設定]の設定値に従って、デバイス管理権限が制限されます。（[デバイス設定]と[ネットワーク設定]の両方が[制限なし]に設定されても、デバイス管理権限について、[Administrator]ロールと同等の権限はありません。） [ネットワーク設定]： ネットワーク設定カテゴリーに属するデバイス管理権限について、[制限なし]/[利用不可]を設定します。 [デバイス設定]： デバイス設定カテゴリーに属するデバイス管理権限について、[制限なし]/[利用不可]を設定します。	[元にするベースロール]に[Administrator]が設定されている場合のみ、設定できます。
[機能カテゴリー制限]	機能カテゴリーごとに使用制限を設定します。	-
[機能カテゴリー制限の詳細]	詳細機能ごとに使用制限を設定します。	-
[アプリケーション制限]	デバイスアプリケーションの使用制限を設定します。	[機能カテゴリー制限]で[許可しない]に設定されていても、[アプリケーション制限]で[許可する]に設定したアプリケーションは、使用できます。
[ボタン制限]	メインメニューやカスタムメニューに表示されるボタンの使用制限を設定します。	[アプリケーション制限]で[許可しない]に設定されている機能は、[ボタン制限]で使用を制限していなくても、使用できません。

デバイス管理権限の詳細は「**デバイス管理権限について(P. 23)**」、使用制限項目の詳細は「**デバイス機能の使用制限(P. 26)**」参照してください。

メモ

- User Authentication のバージョンによっては、表示される項目が多少異なります。
- デバイスアプリケーションとは、デバイスに搭載されている機能ではなく、インストールすることによって使用できるようになった機能（MEAP アプリケーションなど）を指しています。

カスタムロールを編集する

登録されているカスタムロールを編集します。

重要

- ベースロールとカスタムロール（管理者）は[コメント]のみ編集できます。[GuestUser]ロールは、制限情報も編集できます。詳細は、「**[GuestUser]ロール（ゲストロール）を編集する(P. 68)**」を参照してください。
- カスタムロールのロール名を変更するには、一度ロールを削除し、新規にロールを登録しなおす必要があります。
- [元にするベースロール]を変更する（デバイス管理権限を変更する）には、一度ロールを削除し、新規にロールを登録しなおす必要があります。([元にするベースロール]を変更したい場合は、ロールをエクスポートし、テキストエディターで編集することもできます。ただし、制御文字を編集しないように、ご注意ください。)
- 変更したロール情報は、次回のログイン時から有効になります。ログイン中のユーザーには反映されません。
- カスタムロールには、未登録ユーザーの使用制限（ゲストロール）よりも厳しい使用制限を設定しないでください。登録ユーザーに適用する使用制限が未登録ユーザーの使用制限よりも厳しいと、ログイン前や[Guest ログイン]よりもログイン後の方が使用できる機能が少なくなってしまうので、適切にユーザー管理ができなくなる可能性があります。

メモ

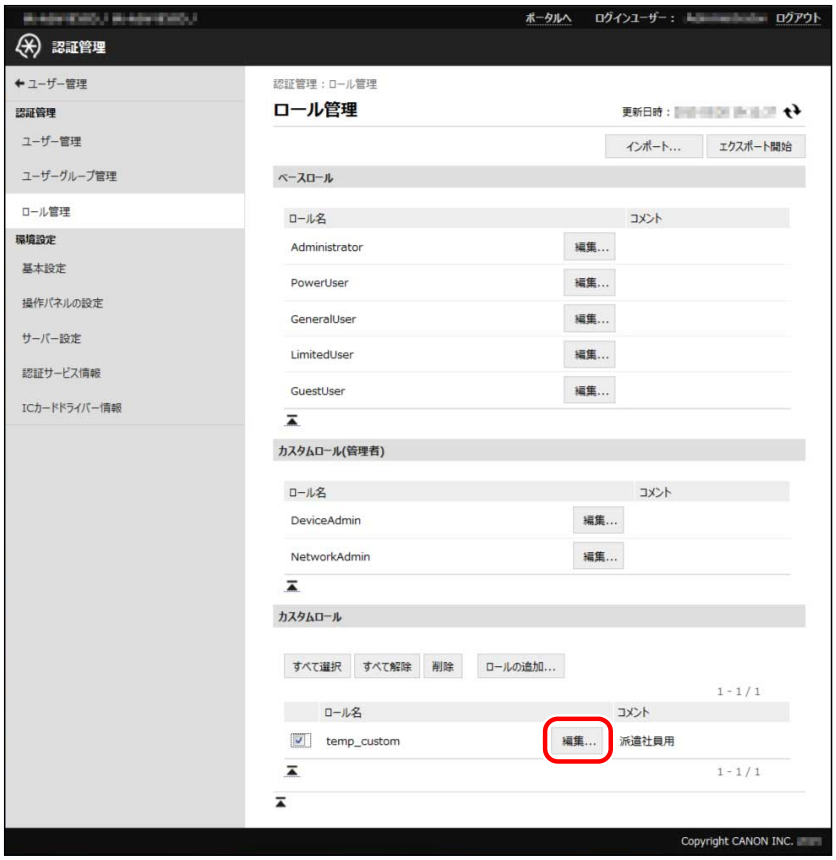
- カスタムロールを編集したら、バックアップのためエクスポートしておくことをおすすめします。詳細は、「**ロールをエクスポートする(P. 72)**」を参照してください。
- ユーザーへのロールの関連付けは、ユーザー管理画面から行います。詳細は、デバイスに付属の取扱説明書を参照してください。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[ロール管理]をクリックします。

3 編集するロールの[編集]をクリックします。



4 必要に応じて各項目を編集し、[更新]をクリックします。

ロール情報が変更されます。

重要

- [元にするベースロール]に[Administrator]が設定されていない場合は、[デバイス管理制限]を設定できません。

[GuestUser]ロール（ゲストロール）を編集する

未登録ユーザーのためのロールを編集します。

重要

- 変更したロール情報は、次回ログイン時から有効になります。ログイン中のユーザーには反映されません。
- ゲストロールには、他のベースロールやカスタムロールよりも厳しい使用制限を設定してください。未登録ユーザーの使用制限よりも登録ユーザーに適用する使用制限が厳しいと、ログイン前や[Guest ログイン]よりもログイン後の方が使用できる機能が少なくなってしまうので、適切にユーザー管理ができなくなる可能性があります。

メモ

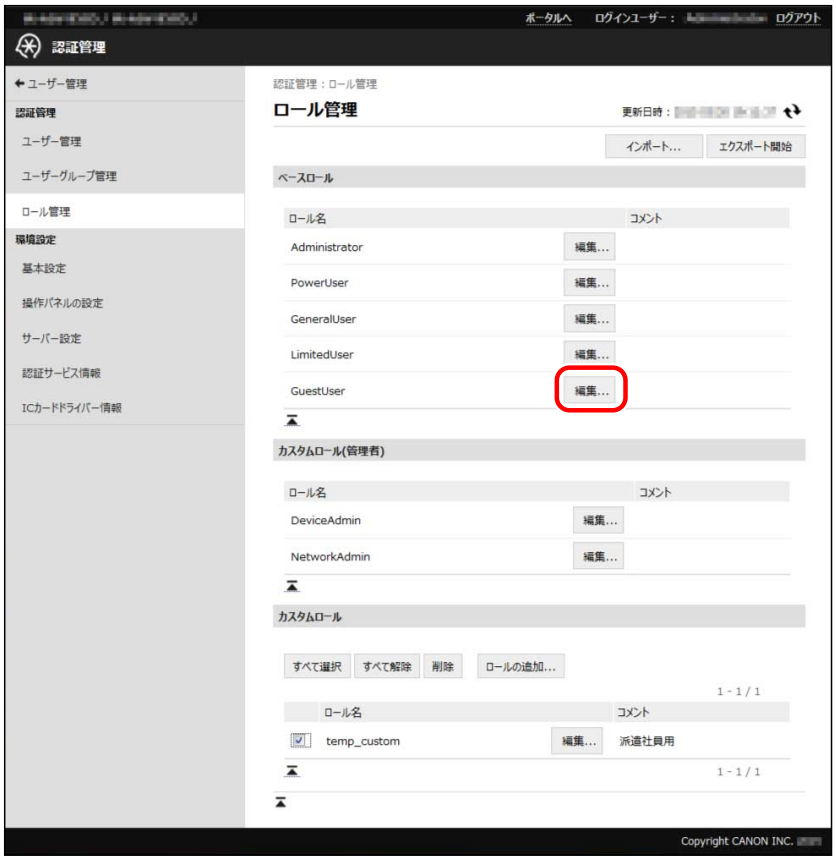
- [GuestUser]ロールを編集したら、バックアップのためエクスポートしておくことをおすすめします。詳細は、「**ロールをエクスポートする(P. 72)**」を参照してください。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[ロール管理]をクリックします。

3 [ベースロール]で[GuestUser]の[編集]をクリックします。



4 必要に応じて各項目を編集し、[更新]をクリックします。

ロール情報が変更されます。

カスタムロールを削除する

登録されているカスタムロールを削除します。

重要

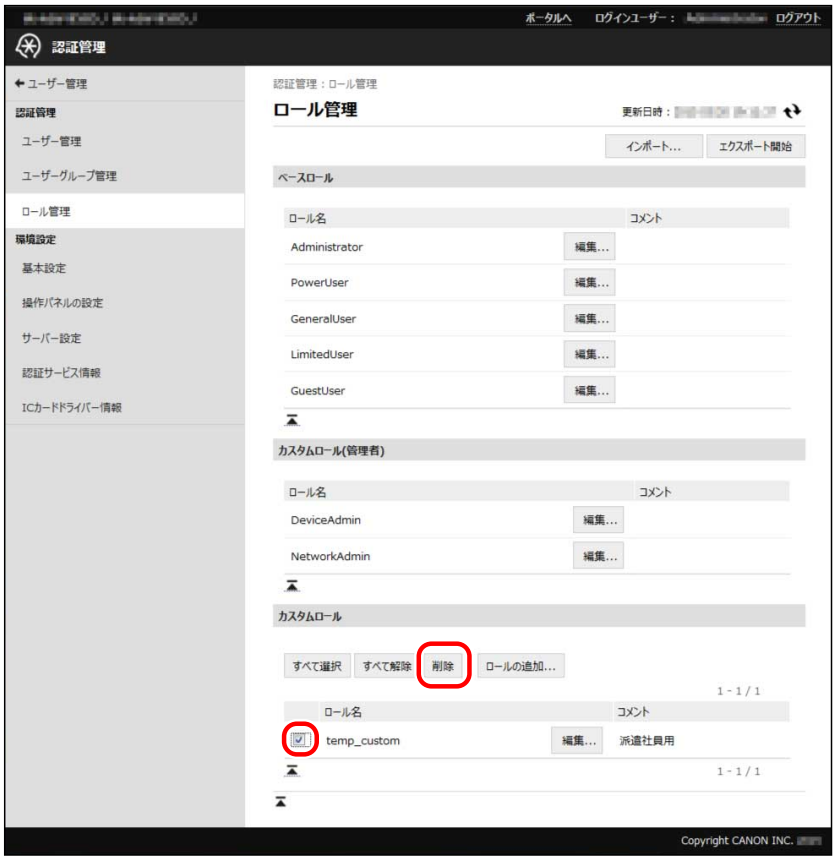
- ベースロールおよびカスタムロール（管理者）は削除できません。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 **[設定/登録]→[ユーザー管理]→[認証管理]→[ロール管理]をクリックします。**

3 **[カスタムロール]で削除するロールの先頭にチェックマークを付けたあと、[削除]をクリックします。**



ロールが削除されます。

メモ

- すべてのカスタムロールを選択するには、[すべて選択]をクリックします。

ロールをインポートする

他のデバイスなどに登録されていたロールをファイルから読み込んで登録できます。

重要

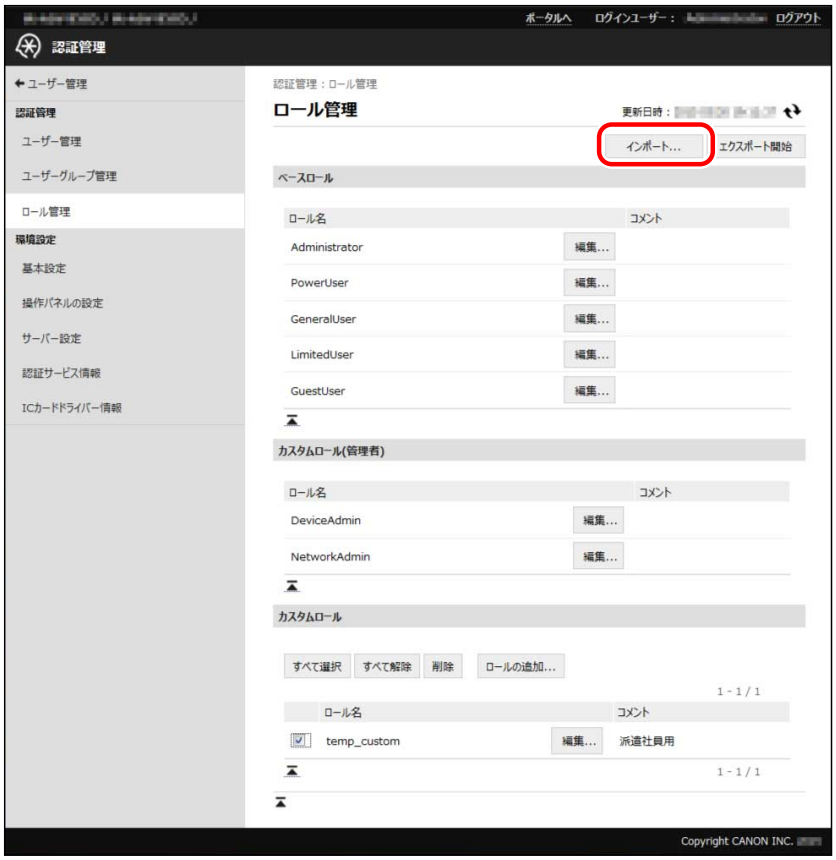
- インポートしたロールと同じロール名がすでに登録されていた場合は、インポートしたロール情報で上書きされます。ただし、ゲストロール以外のベースロールおよびカスタムロール（管理者）は、コメントのみが上書きされます。
- [デバイス管理制限]の設定が不正な場合（[すべての設定]で[制限なし]に設定されているのに[デバイス設定]や[ネットワーク設定]で[利用不可]に設定されている場合）は、不正なロール情報とみなして、インポートしません。
- インポートファイルに含まれていないロールがデバイスに登録されていた場合、そのロールを消去せずに、インポートファイル内のロールを追加で登録します。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[ロール管理]をクリックします。

3 [インポート]をクリックします。



4 [参照]をクリックしてインポート用のファイルを選択します。

5 [インポート開始]をクリックします。

ロールがインポートされます。

メモ

- ロールのインポートに失敗した場合は、ロールバック処理が行われ、インポート実行前の状態に戻ります。

ロールをエクスポートする

デバイスに登録されているロールをファイルに保存することができます。登録されているロールを別のデバイスで使用するときや、バックアップするときなどに利用します。

メモ

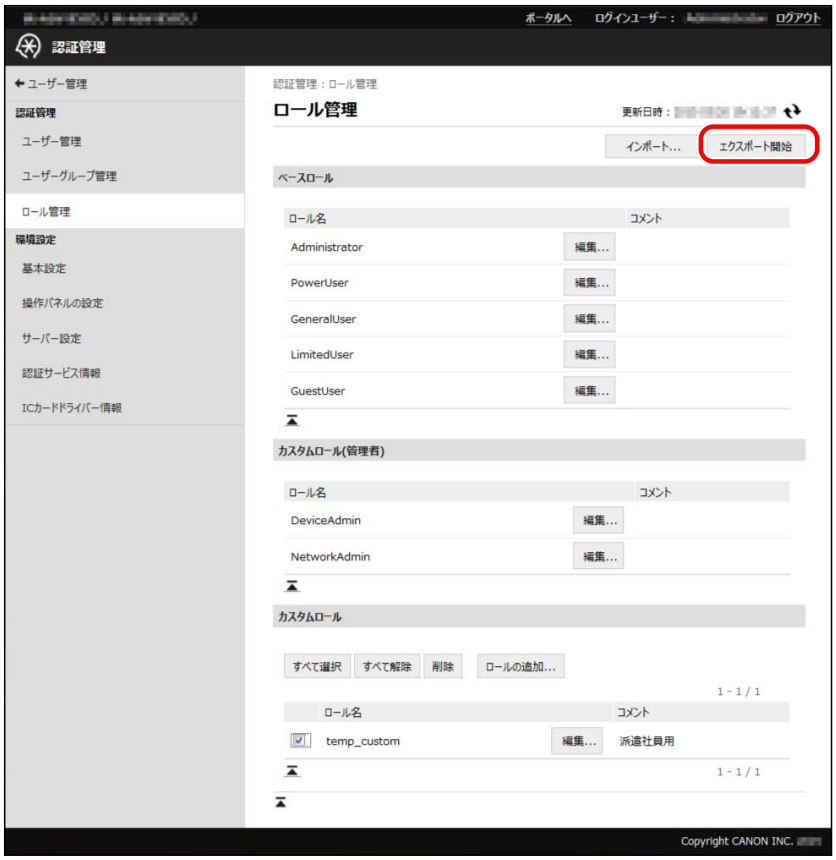
- ファイルの拡張子は「xml」、ファイル名の初期値は「roleData.xml」です。
- エクスポートしたファイルをテキストエディターで編集することもできます。ロール名を変更したい場合などには便利です。ただし、制御文字を編集しないように、ご注意ください。

1 User Authentication にログインします。

詳細は、「**User Authentication にログインする(P. 47)**」を参照してください。

2 [設定/登録]→[ユーザー管理]→[認証管理]→[ロール管理]をクリックします。

3 [エクスポート開始]をクリックします。



4 画面の指示に従って、ファイルの保存場所を指定します。

ファイルのダウンロードが開始されます。

クライアントコンピューターをセットアップする

クライアントコンピューターをセットアップする 75
クライアントコンピューターをセットアップする流れ 76

クライアントコンピューターをセットアップする

ここでは、AMS Printer Driver Add-in の有効化など、クライアントコンピューターのセットアップ方法について説明します。

クライアントコンピューターをセットアップする流れ

ここでは、AMS Printer Driver Add-in の有効化など、クライアントコンピューターのセットアップの流れについて説明します。

1. AMS Printer Driver Add-in を有効にする

Access Management System で、コンピューターからの印刷を制限するには、コンピューターにインストールされているプリンタードライバーで、AMS Printer Driver Add-in を有効にする必要があります。
詳細は、プリンタードライバーの取扱説明書を参照してください。

2. AMS の認証に使用するユーザー情報を設定する

AMS を使用してコンピューターから印刷するユーザーの情報を設定します。
詳細は、プリンタードライバーの取扱説明書を参照してください。

ローカルデバイス認証方式での運用例

ローカルデバイス認証方式での運用例 78
- ローカルデバイス認証方式での運用例について 79
- 操作の流れ 81
- デバイスとネットワーク環境を準備する 84
- デバイスの環境設定を行う 85
- カスタムロールを作成する 94
- ロールをエクスポートする 98
- ローカルユーザーを登録し、ロールを指定する 99
- ユーザー情報をエクスポートする 103
- ロールとユーザー情報をインポートする 104
- 部門別 ID 管理機能を起動する 107
- タッチパネルディスプレーでログイン方式と使用制限を確認する 113
- クライアントコンピューターをセットアップする 119
- クライアントコンピューターで印刷制限を確認する 122

ローカルデバイス認証方式での運用例

ここでは、ローカルデバイス認証方式で運用する Access Management System を新規に導入する際の手順について、例を挙げて説明します。

ローカルデバイス認証方式での運用例について

ここで説明する運用例では、システム管理部のスタッフが、デバイスの管理者と使用制限の管理者を兼任して、営業部に所属する課長_A、正社員_B、派遣社員_C の 3 名で構成されるグループのデバイスの使用制限を設定します。

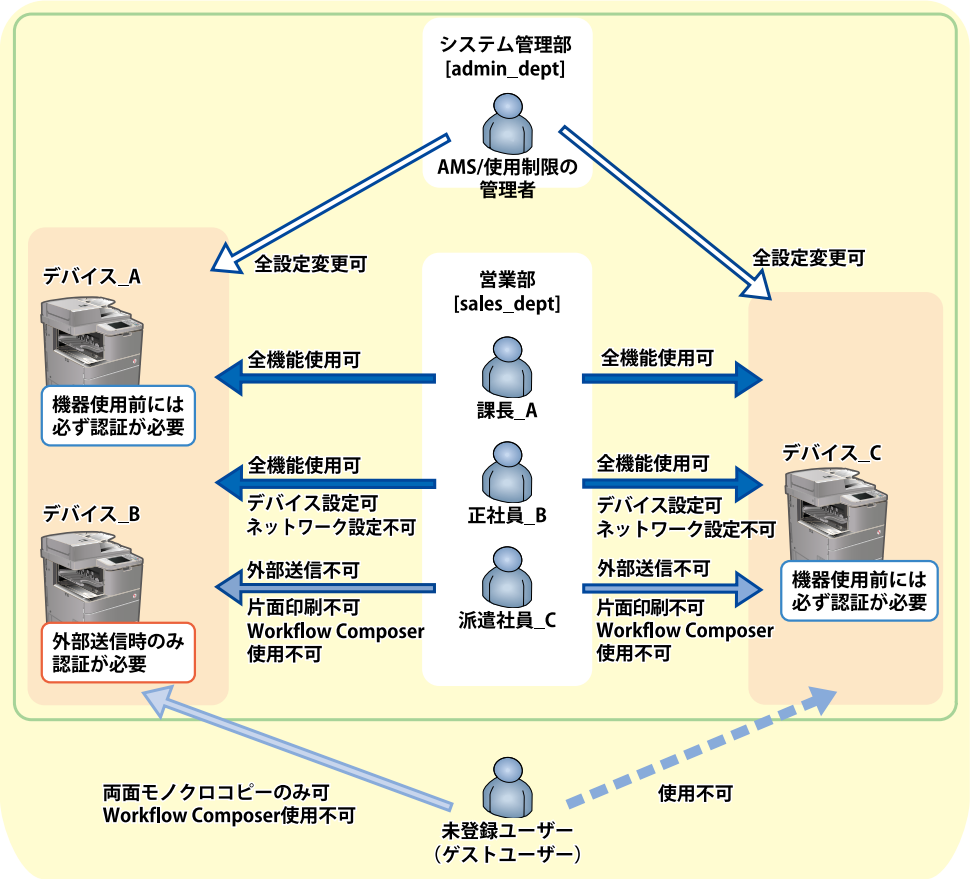
使用するデバイスは、デバイス_A、デバイス_B、デバイス_C の 3 台で、3 台のデバイスは同じ機種です。また、すべてが部門別 ID 管理機能との併用が可能な機種で、オプションの Workflow Composer が追加、開始されています。3 台のデバイスの管理は、デバイスの管理者であるシステム管理部のスタッフが行います。

デバイス_A とデバイス_C をデバイス認証で、デバイス_B を機能別認証で運用します。また、デバイス_A とデバイス_B には未登録ユーザーの使用を許可しますが、デバイス_C には未登録ユーザーの使用を禁止します。

登録ユーザーがデバイスにログインすると、役職に応じた使用制限が適用されます。

ユーザー登録されていないユーザーがデバイス_A を使用する際には、Guest ユーザーとしてログインします。デバイス_B を使用する際には、ログインのための操作は不要です。デバイス_C は使用できません。

部門 ID は、グループ単位（部署単位）で割り当てられていることを前提とします。



運用例で使用するユーザーとロールについて

この運用例では、以下のユーザーに対して、デバイスの使用制限を設定します。

スタッフ	ユーザー名/パスワード	関連付けるロール
営業部 [sales_dept] （部門 ID：3333333/暗証番号：0000003）		

スタッフ	ユーザー名/パスワード	関連付けるロール	
課長_A	[sales_manager] / [m_password]	[PowerUser]	すべてのデバイス機能を使用可。 [設定/登録]画面については、一部の機能を除き、使用不可。
正社員_B	[sales_regular] / [r_password]	[DeviceAdmin]	すべてのデバイス機能を使用可。 [設定/登録]画面については、ネットワーク管理機能を使用不可。
派遣社員_C	[sales_temp] / [t_password]	[temp_custom] （カスタムロール）	コンピューターからの片面印刷と、送信機能が使用不可。 [設定/登録]画面については、一部の機能を除き、使用不可。 Workflow Composer 使用不可。
システム管理部 [admin_dept] （システム管理部門 ID：1111111/システム管理暗証番号：0000001） （部門 ID：2222222/暗証番号：0000002）			
AMS/使用制限の管理者	[IT_management]/ [admin_password]	[Administrator]	すべてのデバイス機能を使用可。 [設定/登録]画面についても、すべての機能を使用可。
上記以外のユーザー	なし	[GuestUser]	両面モノクロコピーのみ使用可。 Workflow Composer 使用不可。

操作の流れ

ここでは、操作の流れを説明します。詳細な操作手順については、各ページを参照してください。

1. デバイスとネットワーク環境を準備する(P. 84)

Access Management System で運用するすべてのデバイスについて、ネットワーク環境や日時などを設定し、システム管理部門 ID を登録します。

2. AMS を有効にする

Access Management System で運用するすべてのデバイス上で、AMS を有効にします。

詳細は、デバイスに付属の取扱説明書を参照してください。

3. User Authentication を起動する

すべての AMS 対応デバイスで、User Authentication を起動します。

詳細は、デバイスに付属の取扱説明書を参照してください。

4. デバイスの環境設定を行う(P. 85)

すべての AMS 対応デバイスに、ユーザー認証方式やログイン方式、未登録ユーザーの使用可否などを設定した後、再起動します。この運用例では、デバイス_A とデバイス_C をデバイス認証に設定し、デバイス_B を機能別認証に設定します。また、デバイス_A とデバイス_B には未登録ユーザーの使用を許可し、デバイス_C には未登録ユーザーの使用を禁止します。

5. カスタムロールを作成する(P. 94)

この運用例では、デバイス_A 上で、[GeneralUser]ロールをもとにして、派遣社員用の[temp_custom]ロールを作成します。また、[GuestUser]ロールの内容も確認しておきます。

6. ロールをエクスポートする(P. 98)

この運用例では、デバイス_A 上のロール（[temp_custom]ロールだけでなくベースロールを含むすべてのロール）をエクスポートします。

7. ローカルユーザーを登録し、ロールを指定する(P. 99)

デバイス_A 上で、ユーザー情報を作成します。この運用例では、営業部とシステム管理部のスタッフのローカルユーザーアカウントを作成します。また、ユーザー情報には、各ローカルユーザーに適用するロール名も登録します。

重要

- 部門別 ID 管理機能を使用する場合は、各ユーザーのユーザー情報に部門 ID を設定してください。

8. ユーザー情報をエクスポートする(P. 103)

デバイス_A 上で作成したユーザー情報をエクスポートします。

9. ロールとユーザー情報をインポートする(P. 104)

すべての AMS 対応デバイスに、ロールとユーザー情報をインポートします。この運用例では、デバイス_B とデバイス_C にロールとユーザー情報をインポートします。

10. 部門別 ID 管理機能を起動する(P. 107)

部門別 ID 管理機能を起動します。この運用例では、デバイス_A、デバイス_B、デバイス_C に営業部とシステム管理部の部門 ID を登録します。

重要

- 部門別 ID 管理機能を起動する前に、各ユーザーのユーザー情報に部門 ID が設定されていることを確認してください。部門別 ID 管理機能を起動すると、ユーザー情報に部門 ID が登録されていないユーザーは、ログインできません。

11. タッチパネルディスプレーでログイン方式と使用制限を確認する(P. 113)

この運用例では、デバイス_A とデバイス_C がデバイス認証に、デバイス_B が機能別認証に、それぞれ設定されていることを確認します。また、各ユーザーでデバイスにログインし、指定した使用制限が適用されていることを確認します。

12. クライアントコンピューターをセットアップする(P. 119)

すべてのユーザーのコンピューターで AMS 機能対応のプリンタードライバーをインストールします。AMS 機能を有効化して、各々のユーザー情報を設定します。

13. クライアントコンピューターで印刷制限を確認する(P. 122)

クライアントコンピューターで、指定した印刷制限が適用されていることを確認します。

デバイスとネットワーク環境を準備する

この運用例では、新規に導入した 3 台のデバイスについて、デバイスとネットワーク環境の準備を行います。その後、システム管理部門 ID を設定して、システム管理部のスタッフ以外のユーザーがデバイスの設定を変更できないように設定します。

日付/時刻の設定をする(P. 84)
ネットワークの設定をする(P. 84)
Web ブラウザーからデバイスにアクセスできるようにする(P. 84)
システム管理部門 ID を登録する(P. 84)

日付/時刻の設定をする

すべてのデバイスについて、日付と時刻を正しく設定します。詳細は、デバイスに付属の取扱説明書を参照してください。

ネットワークの設定をする

すべてのデバイスについて、ネットワークの設定をします。詳細は、デバイスに付属の取扱説明書を参照してください。

Web ブラウザーからデバイスにアクセスできるようにする

すべてのデバイスについて、Web ブラウザーからデバイスにアクセスするための設定を行います。詳細は、「**Web ブラウザーからデバイスにアクセスできるようにする(P. 45)**」を参照してください。

システム管理部門 ID を登録する

すべてのデバイスにシステム管理部門 ID を登録して、システム管理者以外のユーザーがデバイスの設定を変更できないようにします。

この運用例では、システム管理部のスタッフをシステム管理者として登録します。各デバイスで、システム管理者の情報を以下のように設定してください。

詳細は、デバイスに付属の取扱説明書を参照してください。

[システム管理部門 ID]	1111111
[システム管理暗証番号]	0000001
[システム管理者名]	IT_management

デバイスの環境設定を行う

この運用例では、デバイス_A とデバイス_C をデバイス認証に、デバイス_B を機能別認証に設定します。また、デバイス_A とデバイス_B に未登録ユーザーの使用を許可し、デバイス_C には未登録ユーザーの使用を禁止します。

環境設定を行う(P. 85)

環境設定を行う

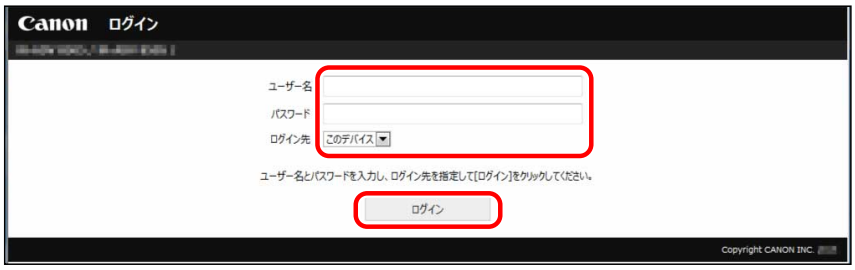
デバイス_A とデバイス_B とデバイス_C の環境設定を行います。セキュリティーの設定を行うことができます。この運用例では、デバイス_A とデバイス_B でセキュリティーの設定も行います。

1 Web ブラウザーを起動し、以下の URL を入力します。

http://<デバイスの IP アドレスまたはホスト名>

[ログイン]ページが表示されます。

2 [Administrator]ロールを関連付けられているユーザーのユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]をクリックします。



3 [設定/登録]→[ユーザー管理]→[認証管理]→[ユーザー管理]をクリックします。

4 [ユーザーの追加]をクリックします。

5 使用制限の管理者ユーザーのユーザー情報を登録し、[追加]をクリックします。

この運用例では、システム管理部のスタッフが、デバイスの管理者と使用制限の管理者を兼任しているので、「**デバイスとネットワーク環境を準備する(P. 84)**」でシステム管理者として登録したアカウントを、使用制限の管理者として登録します。

[ユーザー名]	IT_management
[パスワード]	admin_password
[設定するロール]	[Administrator]
[部門 ID]	2222222
[暗証番号]	0000002

メモ

- 使用制限の管理者（[Administrator]ロールを関連付けられたユーザー）にすべてのデバイス管理権限が与えられているため、必ずしも使用制限の管理者がシステム管理者（システム管理部門 ID を知っているユーザー）である必要はありません。

6 [ログアウト]をクリックします。

7 Web ブラウザーを起動し、以下の URL を入力します。

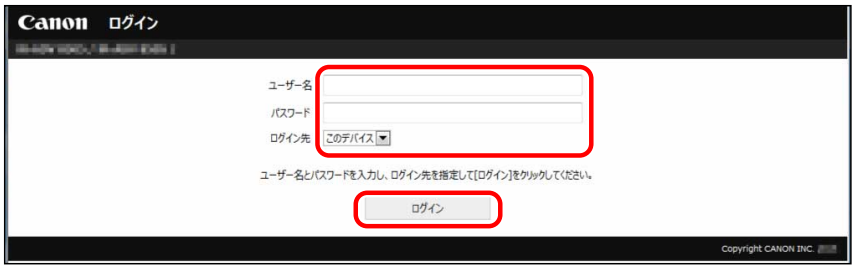
http://<デバイスの IP アドレスまたはホスト名>

[ログイン]ページが表示されます。

8 使用制限の管理者ユーザーのユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]をクリックします。

この運用例では、以下のように入力します。

[ユーザー名]	IT_management
[パスワード]	admin_password
[ログイン先]	[このデバイス]



9 **[設定/登録]→[セキュリティー設定]→[認証/パスワード設定]をクリックします。**

10 **[パスワード設定]の[編集]をクリックします。**

11 **[ユーザー認証のパスワード設定]で、パスワードのポリシーを設定します。**

- **[パスワードの最小文字数を設定する]にチェックマークを付けます。**
- **[最小文字数]ドロップダウンリストから[4]を選択します。**
- **[パスワードの有効期間を設定する]にチェックマークを付けます。**
- **[有効期間]に[30]と入力します。**
- **[OK]をクリックします。**

メモ

- 詳細は、デバイスに付属の取扱説明書を参照してください。

12 [環境設定]を設定します。

メモ

- 詳細は、「**デバイスの環境設定を行う(P. 48)**」、または、デバイスに付属の取扱説明書を参照してください。

[基本設定]

❑ **[設定/登録]→[ユーザー管理]→[認証管理]→[基本設定]をクリックします。**

❑ **[編集]をクリックします。**

❑ **必要な項目を設定して、[更新]をクリックします。**

[操作パネルの設定]

❑ **[設定/登録]→[ユーザー管理]→[認証管理]→[操作パネルの設定]をクリックします。**

❑ **[編集]をクリックします。**

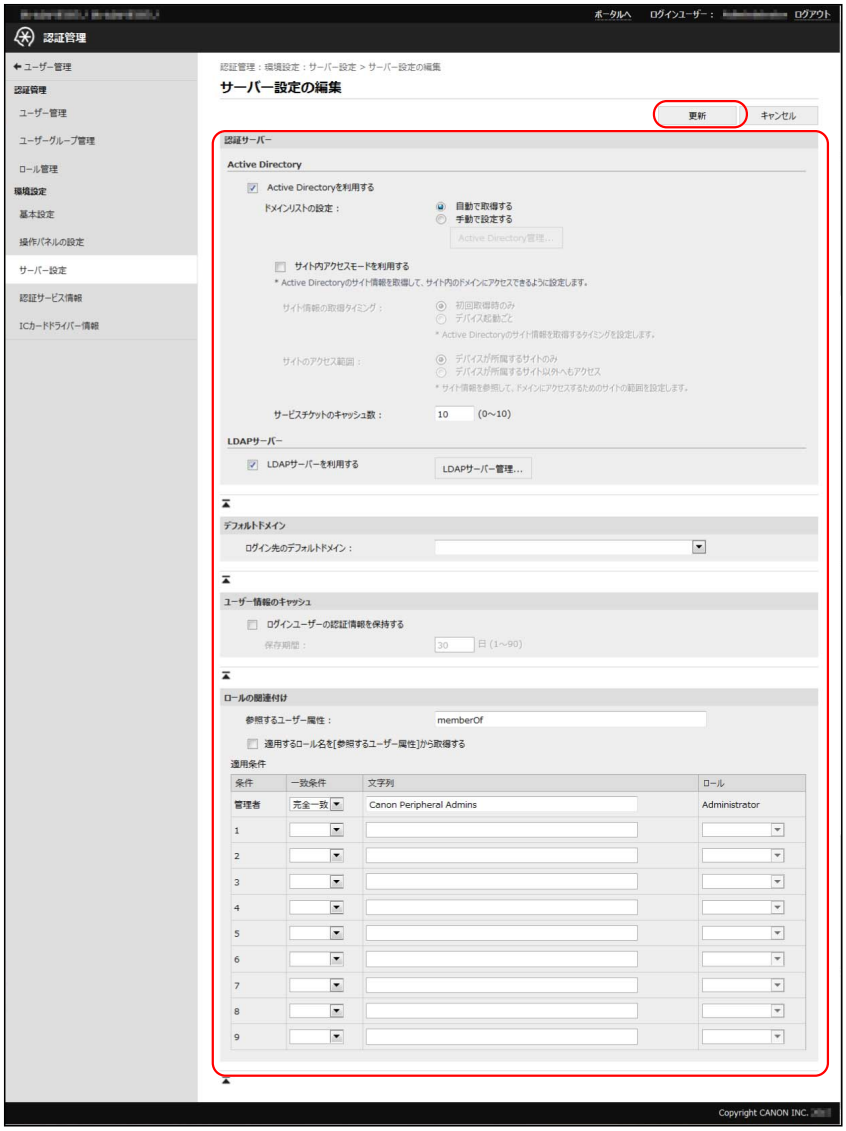
❑ **必要な項目を設定して、[更新]をクリックします。**

[サーバー設定]

❑ **[設定/登録]→[ユーザー管理]→[認証管理]→[サーバー設定]をクリックします。**

❑ **[編集]をクリックします。**

❑ **必要な項目を設定して、[更新]をクリックします。**



この運用例では、以下のように設定します。

デバイス_A

☞[基本設定]

[利用する認証機能]	[キーボード認証]
[ユーザー登録時のデフォルトロール]	[LimitedUser]
[利用を制限する機能]	[AMS Printer Driver Add-in を使用しないドライバーからのプリント]
	[ユーザー認証していないリモートジョブ]
[プリンタードライバーの制御]	[ユーザー認証情報を保持する]

☞[操作パネルの設定]

[ログイン画面の表示]	[デバイスでの操作開始時にログイン画面を表示する]
[未登録ユーザーのログイン]	[Guest User としてログインを許可する]

☞[サーバー設定]

[Active Directory の利用]	[利用しない]

[LDAP サーバーの利用]	[利用しない]

デバイス_B

☞ [基本設定]

[利用する認証機能]	[キーボード認証]
[ユーザー登録時のデフォルトロール]	[LimitedUser]
[利用を制限する機能]	[AMS Printer Driver Add-in を使用しないドライバーからのプリント]
	[ユーザー認証していないリモートジョブ]
[プリンタードライバーの制御]	[ユーザー認証情報を保持する]

☞ [操作パネルの設定]

[ログイン画面の表示]	[認証が必要な機能を選択時にログイン画面を表示する]
[認証する機能の選択]	[スキャンして送信]
	[Workflow Composer]
	[設定/登録]

☞ [サーバー設定]

[Active Directory の利用]	[利用しない]
[LDAP サーバーの利用]	[利用しない]

デバイス_C

☞ [基本設定]

[利用する認証機能]	[キーボード認証]
[ユーザー登録時のデフォルトロール]	[LimitedUser]
[利用を制限する機能]	[AMS Printer Driver Add-in を使用しないドライバーからのプリント]
	[ユーザー認証していないリモートジョブ]
[プリンタードライバーの制御]	[ユーザー認証情報を保持する]

☞ [操作パネルの設定]

[ログイン画面の表示]	[デバイスでの操作開始時にログイン画面を表示する]
[未登録ユーザーのログイン]	チェックマークをつけない

☞ [サーバー設定]

[Active Directory の利用]	[利用しない]
[LDAP サーバーの利用]	[利用しない]

13 [ログアウト]をクリックします。

14 デバイスを再起動します。

重要

- ここでの設定は、デバイスの再起動後に有効になります。再起動の方法については、デバイスに付属の取扱説明書を参照してください。

カスタムロールを作成する

Access Management System を運用する場合のカスタムロールを作成します。

また、適切にユーザー管理が行われるように、[GuestUser]ロールの内容を確認/編集しておきます。

カスタムロールを作成する(P. 94)
登録されている[GuestUser]ロールを編集する(P. 97)

カスタムロールを作成する

この運用例では、デバイス_A 上で、[GeneralUser]ロールをもとにして、派遣社員用ロール[temp_custom]を作成します。

1 Web ブラウザーを起動し、以下の URL を入力します。

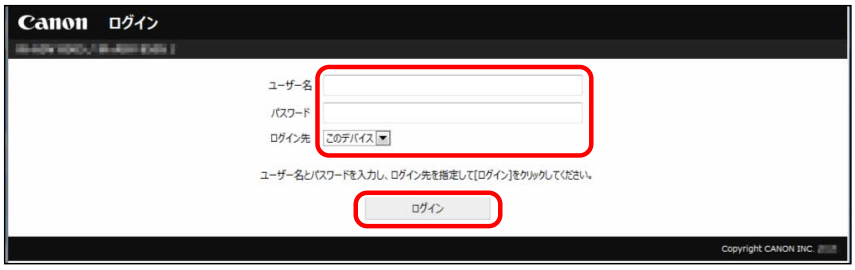
http://<デバイスの IP アドレスまたはホスト名>

[ログイン]ページが表示されます。

2 使用制限の管理者ユーザーのユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]をクリックします。

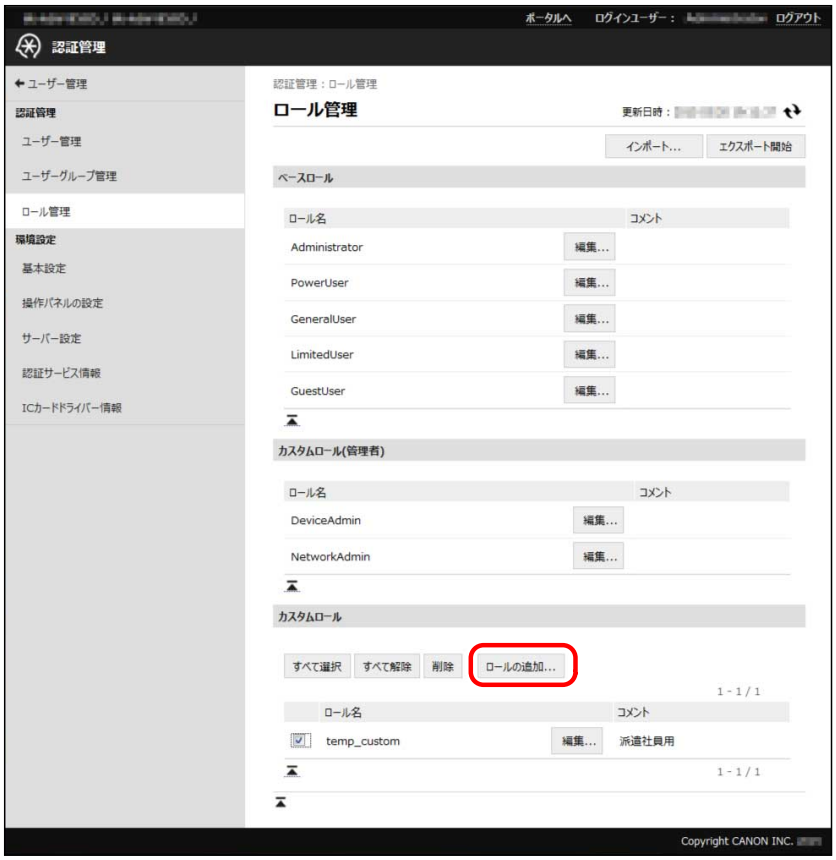
この運用例では、以下のように入力します。

[ユーザー名]	IT_management
[パスワード]	admin_password
[ログイン先]	[このデバイス]



3 [設定/登録]→[ユーザー管理]→[認証管理]→[ロール管理]をクリックします。

4 [ロールの追加]をクリックします。



5 必要な項目を編集して、[追加]をクリックします。

この運用例では、以下のように設定します。

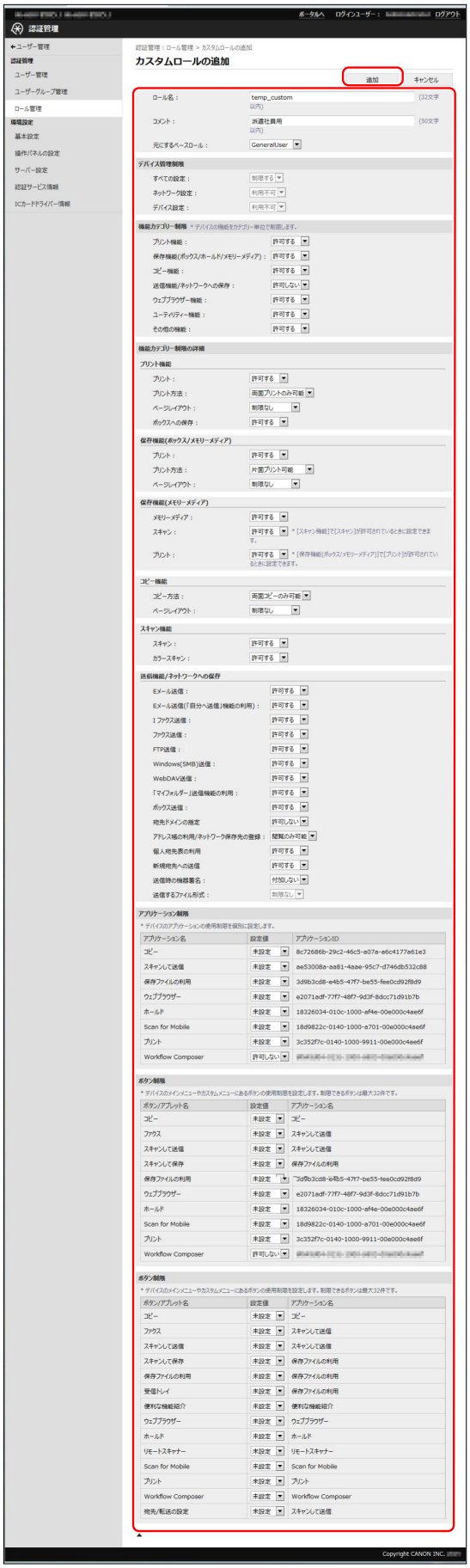
[ロール名]	temp_custom
[コメント]	派遣社員用
[元にするベースロール]	[GeneralUser]
[機能カテゴリー制限]の [送信機能/ネットワークへの保存]	[許可しない]
[機能カテゴリー制限の詳細]の [プリント機能]の [プリント方法]	[両面プリントのみ可能]
[機能カテゴリー制限の詳細]の [コピー機能]の[コピー方法]	[両面コピーのみ可能]
[アプリケーション制限]の [Workflow Composer]	[許可しない]

重要

- この運用例では、デバイス_A に Workflow Composer がインストールされているので、[アプリケーション制限]に[Workflow Composer]が表示され、使用制限を設定できます。

メモ

- 詳細は、「**ロールを管理する(P. 62)**」を参照してください。



[temp_custom]ロールが登録されます。

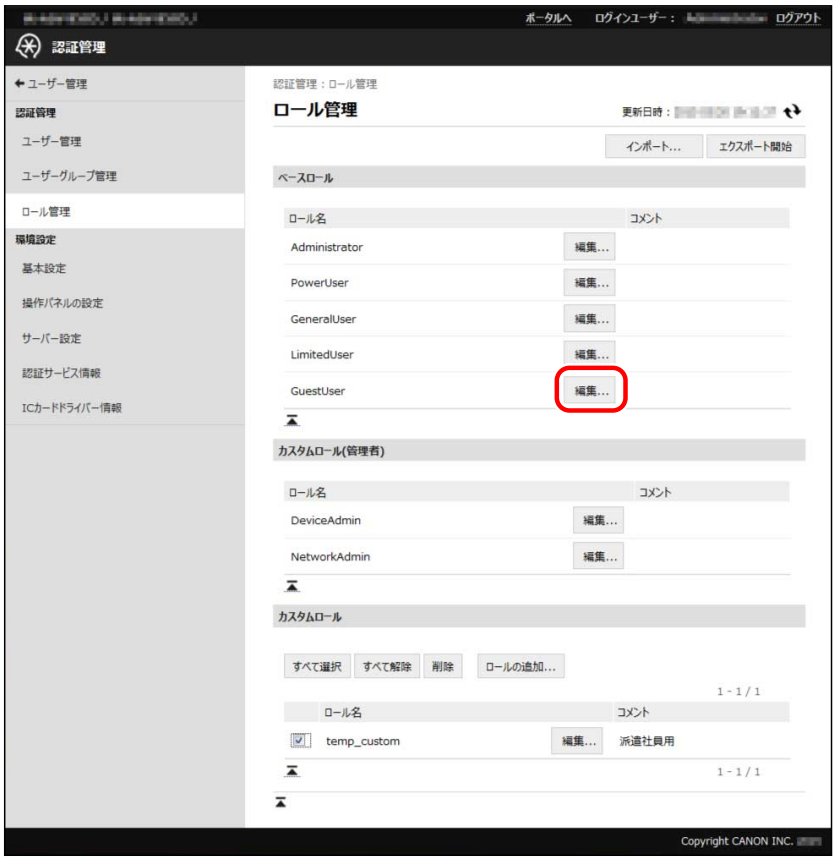
登録されている[GuestUser]ロールを編集する

デバイス_A に登録されている[GuestUser]ロールに設定されている使用制限の内容を確認し、アプリケーション制限を設定します。

重要

- 未登録ユーザー（[GuestUser]）の使用制限よりも登録ユーザーに適用する使用制限が厳しいと、ログイン前よりもログイン後の方が使用できる機能が少なくなってしまうので、適切にユーザー管理できなくなる可能性があります。

1 [ベースロール]で[GuestUser]の[編集]をクリックします。



2 使用制限の内容を確認します。

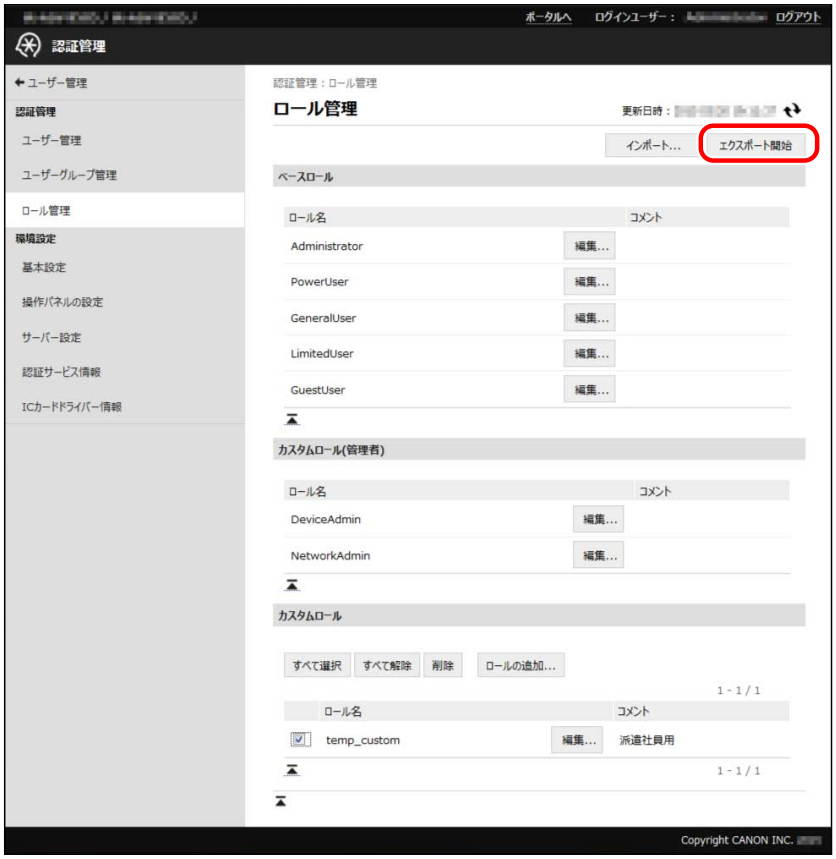
この運用例では、[GuestUser]ロールの設定内容が変更されていないことを確認します。設定値の詳細は、「**デバイス機能の使用制限(P. 26)**」を参照してください。

3 [アプリケーション制限]で、[スキャンして送信]、[Workflow Composer]を[許可しない]に設定して、[更新]をクリックします。

ロールをエクスポートする

この運用例では、デバイス_A 上のロールをエクスポートします。エクスポートでは、カスタムロールだけでなくすべてのロールを一括でファイルに保存します。

1 [ロール管理]ページで、[エクスポート開始]をクリックします。



2 画面の指示に従って、ファイルの保存場所を指定します。

ファイルのダウンロードが開始されます。

メモ

- ファイルの拡張子は「xml」、ファイル名の初期値は「roleData.xml」です。

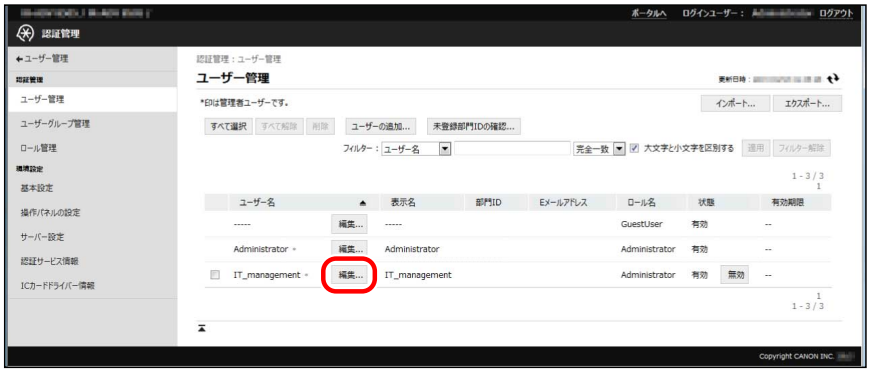
3 [ログアウト]をクリックします。

ローカルユーザーを登録し、ロールを指定する

この運用例では、デバイス_A に、営業部のスタッフ（課長_A、正社員_B、派遣社員_C）をローカルユーザーとして登録し、役職に応じたロールを指定します。

1 [設定/登録]→[ユーザー管理]→[認証管理]→[ユーザー管理]をクリックします。

2 使用制限の管理者の[編集]をクリックします。

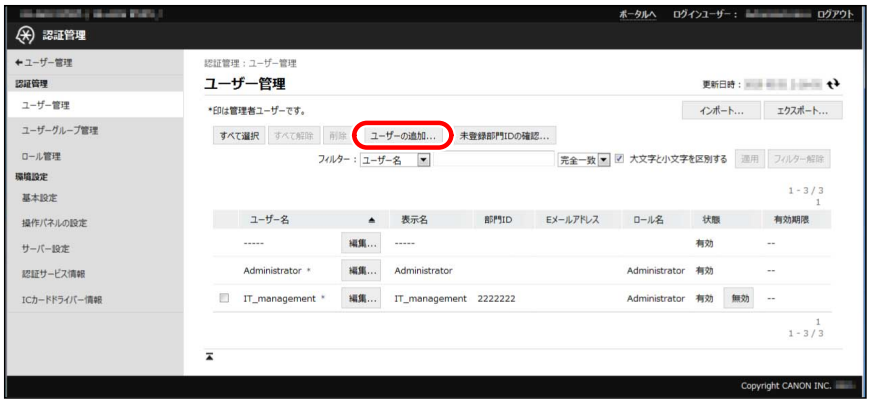


3 必要な項目を設定し、[更新]をクリックします。

この運用例では、以下のように設定します。

[部門 ID]	2222222
[暗証番号]	0000002

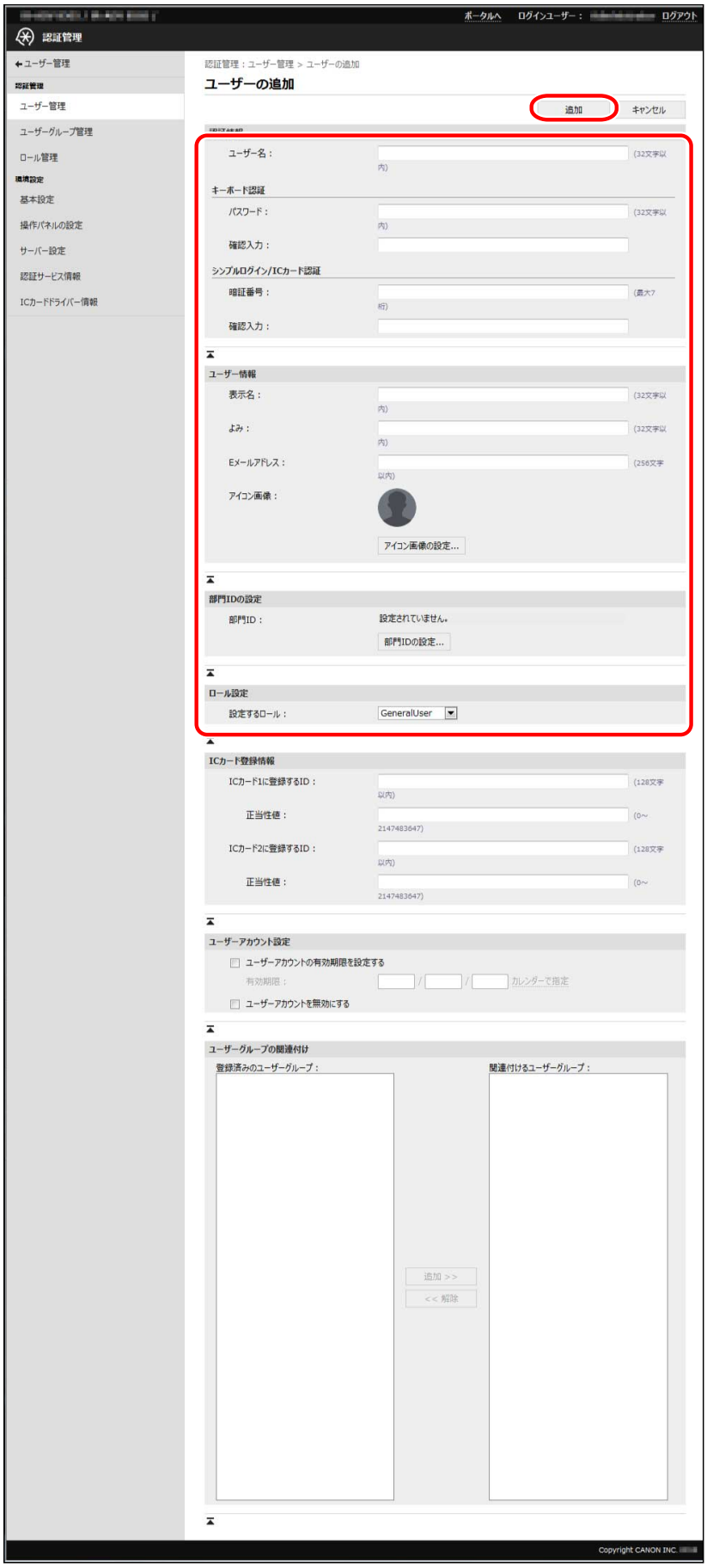
4 [ユーザーの追加]をクリックします。



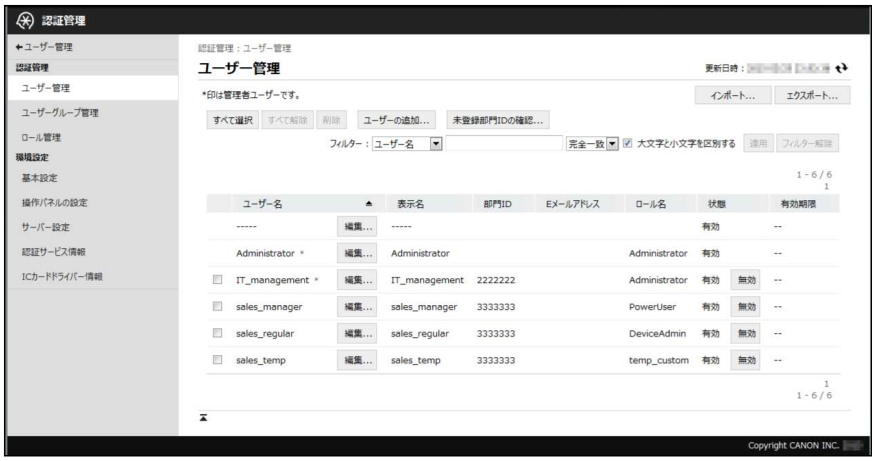
5 必要な項目を設定し、[追加]をクリックします。

この運用例では、以下のように設定します。

ローカルユーザー	設定項目	設定内容
課長_A	[ユーザー名]	sales_manager
	[パスワード]	m_password
	[部門 ID]	3333333
	[暗証番号]	0000003
	[設定するロール]	[PowerUser]
正社員_B	[ユーザー名]	sales_regular
	[パスワード]	r_password
	[部門 ID]	3333333
	[暗証番号]	0000003
	[設定するロール]	[DeviceAdmin]
派遣社員_C	[ユーザー名]	sales_temp
	[パスワード]	t_password
	[部門 ID]	3333333
	[暗証番号]	0000003
	[設定するロール]	[temp_custom]



ユーザー情報が登録されます。



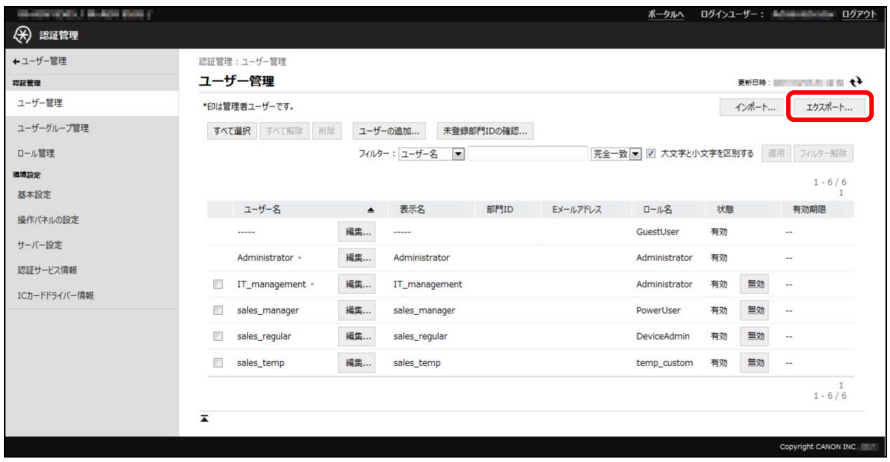
メモ

- 使用制限の管理者以外のユーザーも、自分のパスワードを変更することができます。これによって、セキュリティーを高めることができます。使用制限の管理者ユーザーは、他のユーザーにパスワードの変更ができることをお知らせください。変更方法については、デバイスに付属の取扱説明書を参照してください。

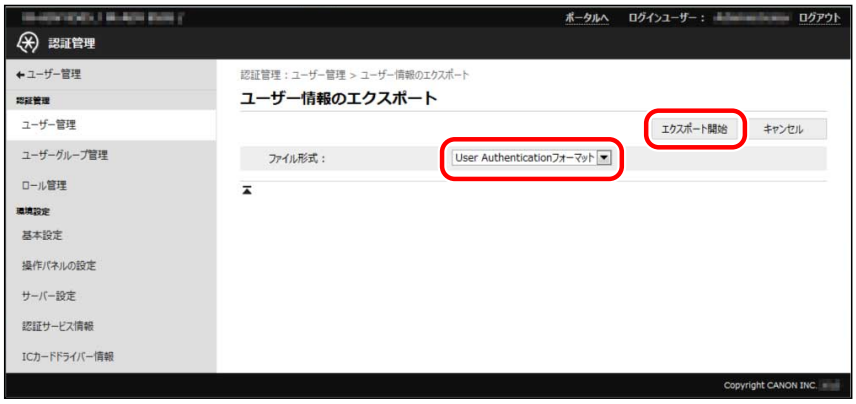
ユーザー情報をエクスポートする

この運用例では、デバイス_A 上のユーザー情報をエクスポートします。ユーザー情報は、各ユーザーに適用するロールが指定された状態で、エクスポートされます。

1 [ユーザー管理]ページで、[エクスポート]をクリックします。



2 [User Authentication フォーマット]が選択されていることを確認し、[エクスポート開始]をクリックします。



3 画面の指示に従って、ファイルの保存場所を指定します。

ファイルのダウンロードが開始されます。

メモ

- ファイルの拡張子は「csv」、ファイル名の初期値は「userData.csv」です。

4 [ログアウト]をクリックします。

ロールとユーザー情報をインポートする

この運用例では、デバイス_A からエクスポートしたロールとユーザー情報を、デバイス_B とデバイス_C にインポートします。

ロールとユーザー情報をインポートする(P. 104)

ロールとユーザー情報をインポートする

デバイス_B とデバイス_C に、ロールとユーザー情報をインポートします。手順 1 〜12 を、デバイス_B とデバイス_C で、それぞれ行います。

1 Web ブラウザーを起動し、以下の URL を入力します。

http://<デバイスの IP アドレスまたはホスト名>

[ログイン]ページが表示されます。

2 使用制限の管理者ユーザーのユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]をクリックします。

この運用例では、以下のように入力します。

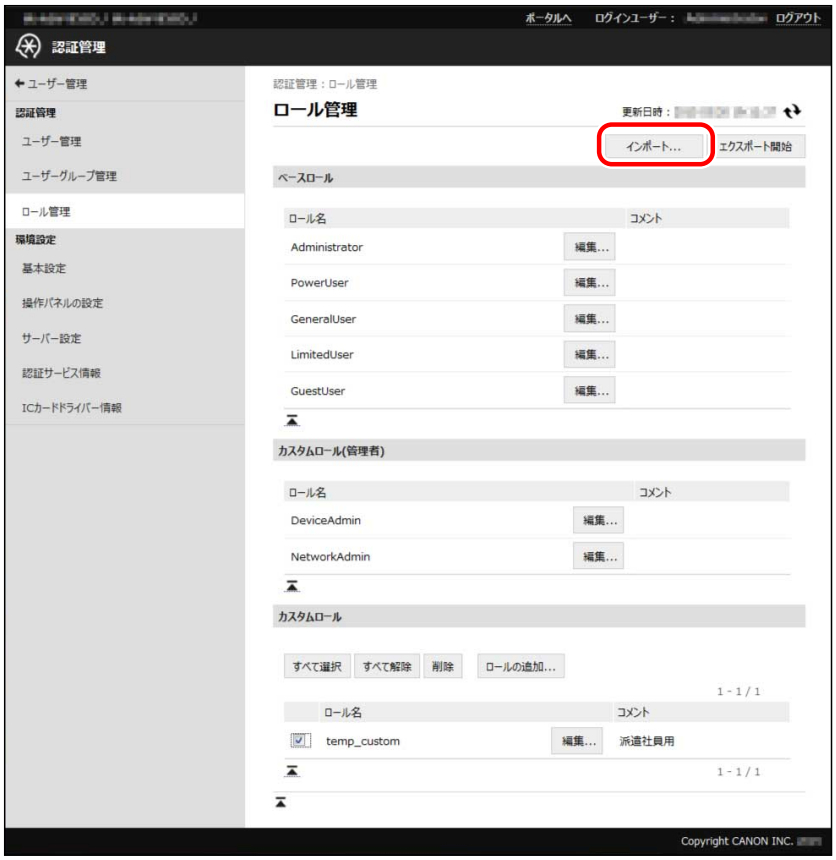
[ユーザー名]	IT_management
[パスワード]	admin_password
[ログイン先]	[このデバイス]

3 [設定/登録]→[ユーザー管理]→[認証管理]→[ロール管理]をクリックします。

重要

- インポートしたロールと同じロール名がすでに登録されていた場合は、インポートしたロール情報で上書きされます。

4 [インポート]をクリックします。

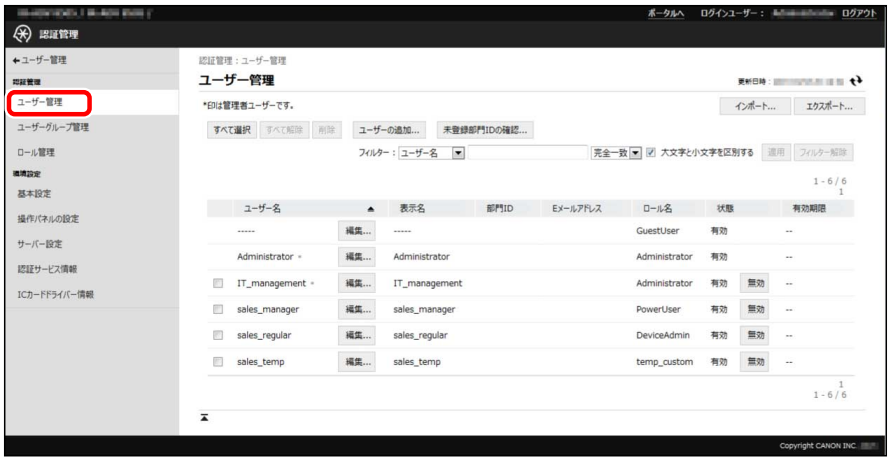


5 [参照]をクリックしてインポート用のファイルを選択します。

6 [インポート開始]をクリックします。

ロールがインポートされます。

7 [ユーザー管理]をクリックします。



重要

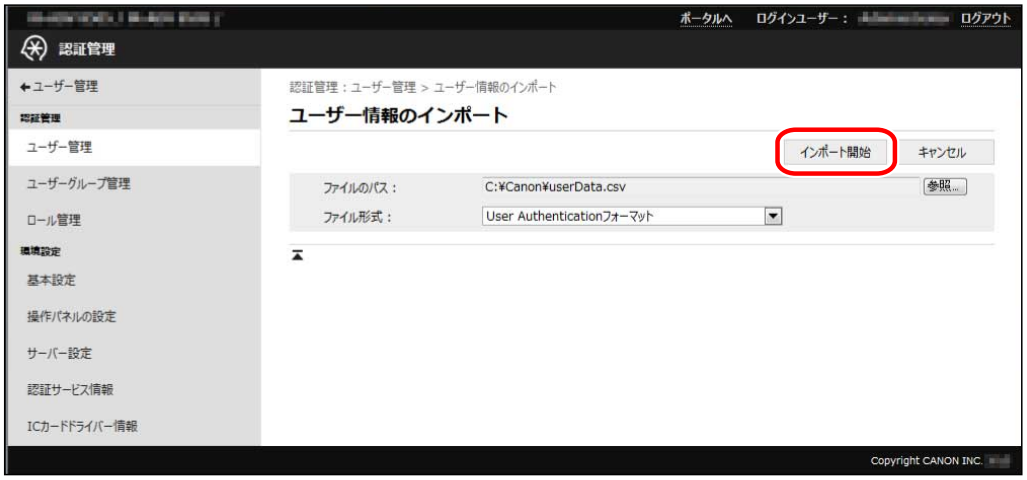
- インポートしたユーザーと同じユーザー名がすでに登録されていた場合は、インポートしたユーザー情報で上書きされます。

8 **[インポート]をクリックします。**

9 **[参照]をクリックしてインポート用のファイルを選択します。**

10 **[ファイル形式]で、[User Authentication フォーマット]を選択します。**

11 **[インポート開始]をクリックします。**



ユーザー情報がインポートされます。

12 **[ログアウト]をクリックします。**

部門別 ID 管理機能を起動する

部門別 ID 管理機能を起動します。この運用例では、3 台のデバイスに営業部とシステム管理部の部門 ID を登録します。

部門別 ID 管理機能を起動する(P. 107)

重要

- 部門別 ID 管理機能を起動する前に、各ユーザーのユーザー情報に部門 ID が設定されていることを確認してください。部門別 ID 管理機能を起動すると、ユーザー情報に部門 ID が登録されていないユーザーは、ログインできません。

部門別 ID 管理機能を起動する

デバイスで、部門別 ID 管理機能を起動します。

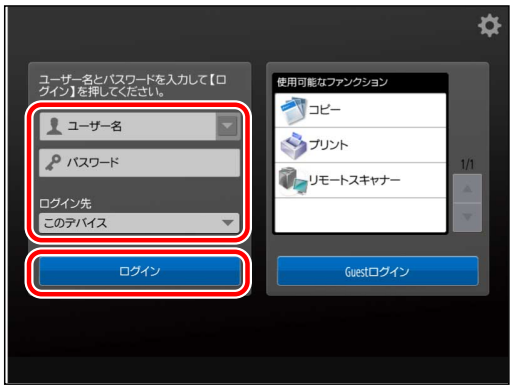
デバイス_A とデバイス_C で部門別 ID 管理機能を起動する

手順 1 ～9 を、デバイス_A とデバイス_C で、それぞれ行います。

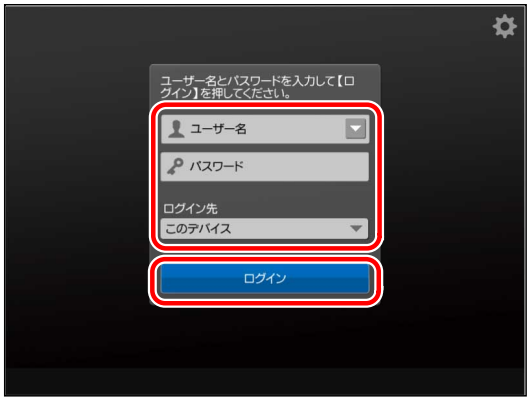
1 使用制限の管理者ユーザーのユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]を押します。

[ユーザー名]	IT_management
[パスワード]	admin_password
[ログイン先]	[このデバイス]

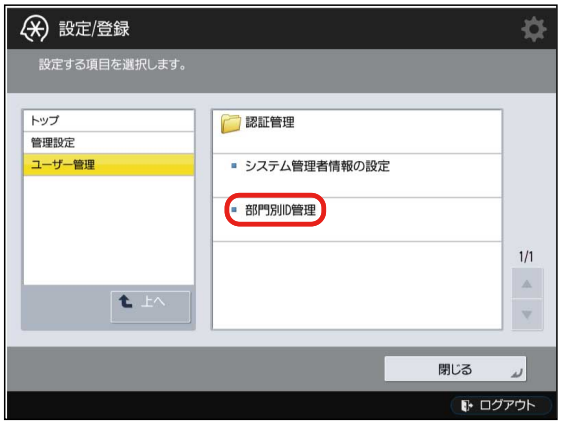
デバイス_A の場合



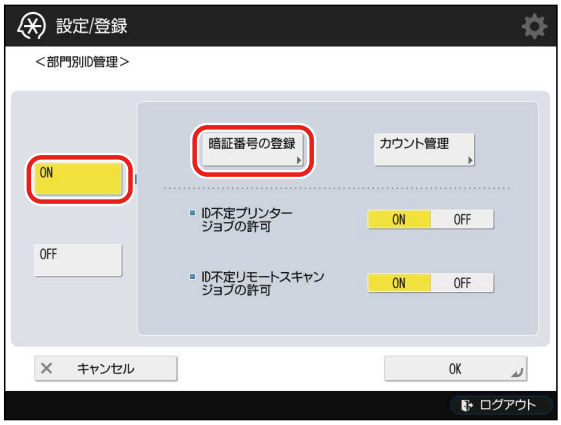
デバイス_C の場合



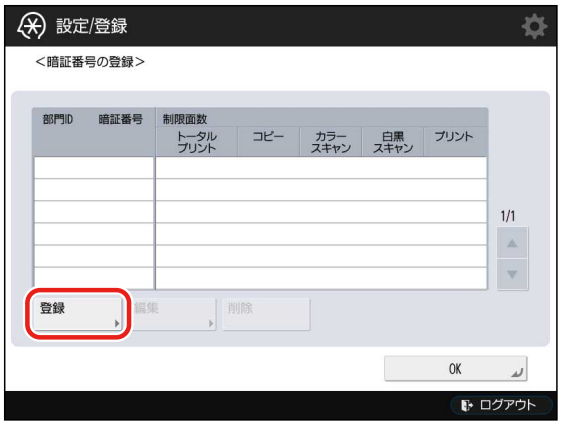
2 （設定/登録）→[管理設定]→[ユーザー管理]→[部門別 ID 管理]を押します。



3 [ON]→[暗証番号の登録]を押します。



4 [登録]を押します。



5 **[部門 ID]を押して、営業部の部門 ID「3333333」を入力します。**

6 **[暗証番号]を押して、[暗証番号]と[確認入力]に「0000003」と入力し、[OK]を押します。**

7 **[OK]を押します。**

8 **手順 4～7 と同様の手順で、システム管理部の部門 ID を登録します。**

[部門 ID]	2222222
[暗証番号]	0000002

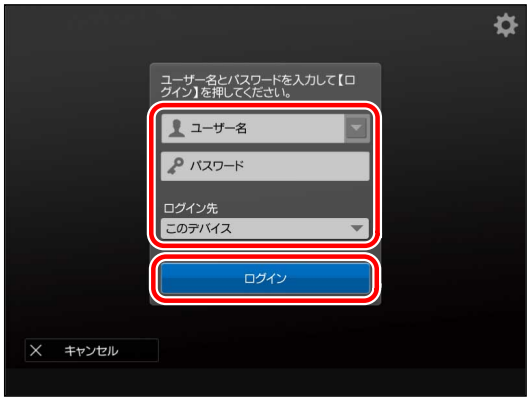
9 **メインメニューまで戻ります。**

デバイス_B で部門別 ID 管理機能を起動する

1 **（設定/登録）を押します。**

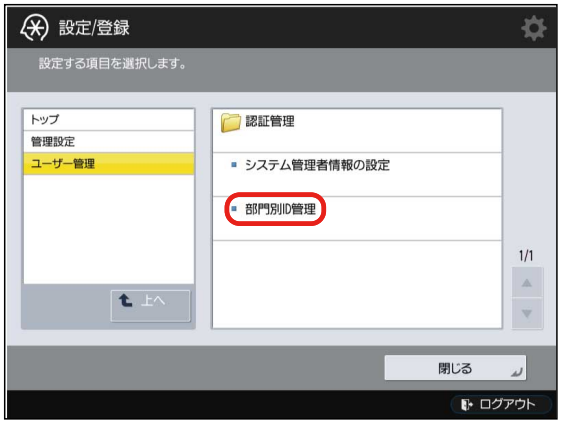
2 **使用制限の管理者ユーザーのユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、 [ログイン]を押します。**

[ユーザー名]	IT_management
[パスワード]	admin_password
[ログイン先]	[このデバイス]

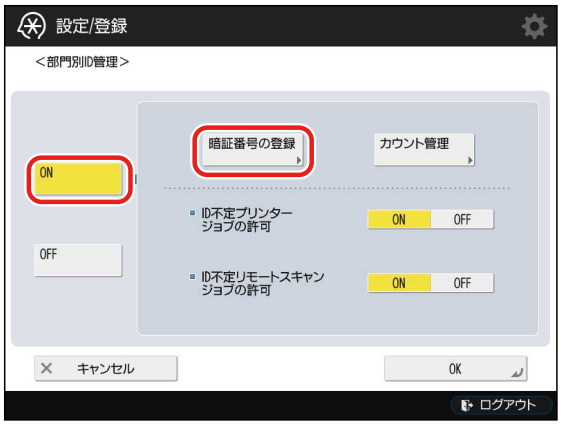


3 **[機器設定]を押します。**

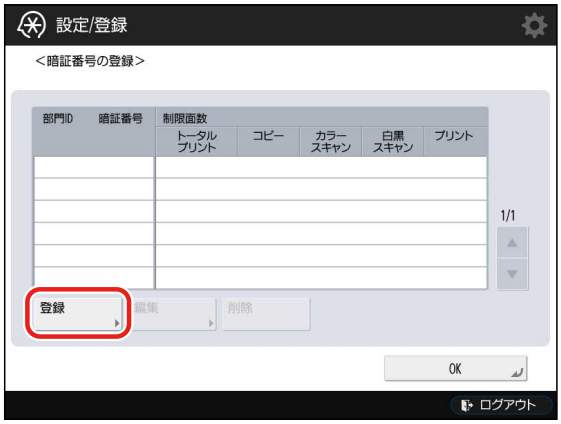
4 **[管理設定]→[ユーザー管理]→[部門別 ID 管理]を押します。**



5 **[ON]→[暗証番号の登録]を押します。**



6 [登録]を押します。



7 [部門 ID]を押して、営業部の部門 ID「3333333」を入力します。

8 [暗証番号]を押して、[暗証番号]と[確認入力]に「0000003」と入力し、[OK]を押します。

9 **[OK]を押します。**

10 **手順 6～9 と同様の手順で、システム管理部の部門 ID を登録します。**

[部門 ID]	2222222
[暗証番号]	0000002

11 **メインメニューまで戻ります。**

タッチパネルディスプレーでログイン方式と使用制限を確認する

この運用例では、デバイス_A には、[Guest ログイン]が表示されているログイン画面が、デバイス_B には、すべての機能ボタンが表示されているメインメニューが、デバイス_C には、[Guest ログイン]が表示されていないログイン画面が、それぞれ表示されていることを確認します。また、各ユーザー名でデバイスにログインして、デバイス機能の使用制限とデバイス管理権限が正しく設定されていることを確認します。

デバイス_A とデバイス_C で確認する(P. 113)
デバイス_B で確認する(P. 115)

デバイス_A とデバイス_C で確認する

手順 1 ～12 を、デバイス_A とデバイス_C で、それぞれ行います。

1 タッチパネルディスプレーに、以下の画面が表示されていることを確認します。

デバイス_A の場合

デバイス_C の場合

2 [ユーザー名]と[パスワード]に、[sales_temp]のユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]を押します。

[ユーザー名]	sales_temp

[パスワード]	t_password
[ログイン先]	[このデバイス]

3 [スキャンして送信]と[Workflow Composer]を操作できないことを確認します。

4 （設定/登録）を押します。

5 [ファンクション設定]→[送信]→[レポート出力]を操作できないことを確認します。

画面の詳細は、デバイスに付属の取扱説明書を参照してください。

6 （認証）を押して、AMS 対応デバイスからログアウトします。

7 [ユーザー名]と[パスワード]に、[sales_regular]のユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]を押します。

[ユーザー名]	sales_regular
[パスワード]	r_password
[ログイン先]	[このデバイス]

8 [スキャンして送信]と[Workflow Composer]を操作できることを確認します。

9 **（設定/登録）を押します。**

10 **[ファンクション設定]→[送信]→[レポート出力]を操作できることを確認します。**

画面の詳細は、デバイスに付属の取扱説明書を参照してください。

11 **（認証）を押して、AMS 対応デバイスからログアウトします。**

12 **他のユーザーでログインして、デバイス機能の使用制限とデバイスの管理権限が正しく設定されていることを確認します。**

この運用例では、ログインするユーザーによって、以下のように表示されます。

デバイス_A の場合

ユーザー名	パスワード	[スキャンして送信]と[Workflow Composer]	[ファンクション設定]→[送信]→[レポート出力]
sales_manager	m_password	操作可	操作可
sales_regular	r_password	操作可	操作可
sales_temp	t_password	操作不可	操作不可
IT_management	admin_password	操作可	操作可
ゲストユーザー	-	操作不可	操作不可

デバイス_C の場合

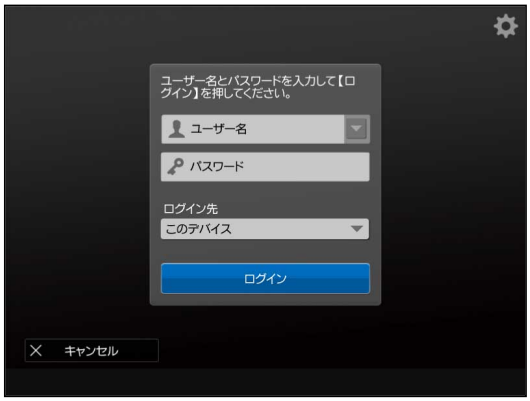
ユーザー名	パスワード	[スキャンして送信]と[Workflow Composer]	[ファンクション設定]→[送信]→[レポート出力]
sales_manager	m_password	操作可	操作可
sales_regular	r_password	操作可	操作可
sales_temp	t_password	操作不可	操作不可
IT_management	admin_password	操作可	操作可

デバイス_B で確認する

1 **タッチパネルディスプレーに、以下の画面が表示されていることを確認します。**

2 **[スキャンして送信]を押します。**

3 **ログイン画面が表示されることを確認します。**



4 **[ユーザー名]と[パスワード]に、[sales_temp]のユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]を押します。**

[ユーザー名]	sales_temp
[パスワード]	t_password
[ログイン先]	[このデバイス]

5 **[スキャンして送信]を操作できないことを確認します。**

同様に、[Workflow Composer]を操作できないことを確認します。

6 **（設定/登録）→[ログイン]を押します。**

ログイン画面が表示されます。

7 **[ユーザー名]と[パスワード]に、[sales_temp]のユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]を押します。**

[ユーザー名]	sales_temp
[パスワード]	t_password

[ログイン先]	[このデバイス]

8 [ファンクション設定]→[送信]→[レポート出力]を操作できないことを確認します。

画面の詳細は、デバイスに付属の取扱説明書を参照してください。

9 （認証）を押して、AMS 対応デバイスからログアウトします。

10 [スキャンして送信]を押します。

ログイン画面が表示されます。

11 [ユーザー名]と[パスワード]に、[sales_regular]のユーザー名とパスワードを入力し、[ログイン先]で[このデバイス]を選択して、[ログイン]を押します。

[ユーザー名]	sales_regular
[パスワード]	r_password
[ログイン先]	[このデバイス]

12 [スキャンして送信]画面に移行することを確認します。

同様に、[Workflow Composer]画面に移行することを確認します。

13 （設定/登録）を押します。

14 [ファンクション設定]→[送信]→[レポート出力]を操作できることを確認します。

画面の詳細は、デバイスに付属の取扱説明書を参照してください。

15 （認証）を押して、AMS 対応デバイスからログアウトします。

16 他のユーザーでログインして、デバイス機能の使用制限とデバイスの管理権限が正しく設定されていることを確認します。

この運用例では、ログインするユーザーによって、以下のように表示されます。

ユーザー名	パスワード	[スキャンして送信]と[Workflow Composer]	[ファンクション設定]→[送信]→[レポート出力]
sales_manager	m_password	操作可	操作可
sales_regular	r_password	操作可	操作可
sales_temp	t_password	操作不可	操作不可
IT_management	admin_password	操作可	操作可

クライアントコンピューターをセットアップする

Access Management System で、コンピューターからの印刷を制限するには、コンピューターにインストールされているプリンタードライバーで AMS 機能を有効にして、ユーザー情報を設定する必要があります。

AMS Printer Driver Add-in を有効化する(P. 119)
AMS Printer Driver Add-in にユーザー情報を設定する(P. 120)
他のクライアントコンピューターをセットアップする(P. 121)

この運用例では、3 台のデバイスを使用しますが、デバイス_A とデバイス_B とデバイス_C は同じ機種なので、1 つのプリンタードライバーを使用します。

1 つの[AMS]ページ上で設定すれば、ログオン中のコンピューターから使用するすべての AMS Printer Driver Add-in に適用されます。したがってユーザー情報の設定も 1 回の操作で完了します。

重要

- プリンタードライバーによっては、AMS Printer Driver Add-In が組み込まれていません。最新のプリンタードライバーお使いください。
- 共有プリンター環境で使用する場合は、プリントサーバー上のプリンタードライバーで AMS 機能を有効化してください。
- システムを構成するすべての機器（デバイス、クライアントコンピューター、サーバーコンピューターなど）の日付/時刻が合っていないと、印刷に時間がかかったり、印刷できなかったりすることがあります。デバイスの設定方法については、デバイスに付属の取扱説明書を参照してください。

AMS Printer Driver Add-in を有効化する

1 Windows の Administrator 権限を持つユーザーでコンピューターにログオンします。

2 Windows 8.1/Server 2012 を使用している場合は、デスクトップへ移動します。

3 起動しているアプリケーションをすべて終了します。

4 デバイス_A とデバイス_B とデバイス_C が使用するプリンタードライバーの最新版をインストールします。

メモ

- 最新のプリンタードライバーは、キヤノンの Web サイトからダウンロードできます。
- プリンタードライバーが「Standard TCP/IP ポート」でインストールされていない場合は、「Standard TCP/IP ポート」で更新することをお勧めします。

5 **デバイス_A とデバイス_B とデバイス_C のプリンターアイコンを追加します。**

詳細は、お使いの Windows の取扱説明書を参照してください。

6 **追加したプリンターで AMS 機能を有効化します。**

詳細は、プリンタードライバーの取扱説明書を参照してください。

AMS Printer Driver Add-in にユーザー情報を設定する

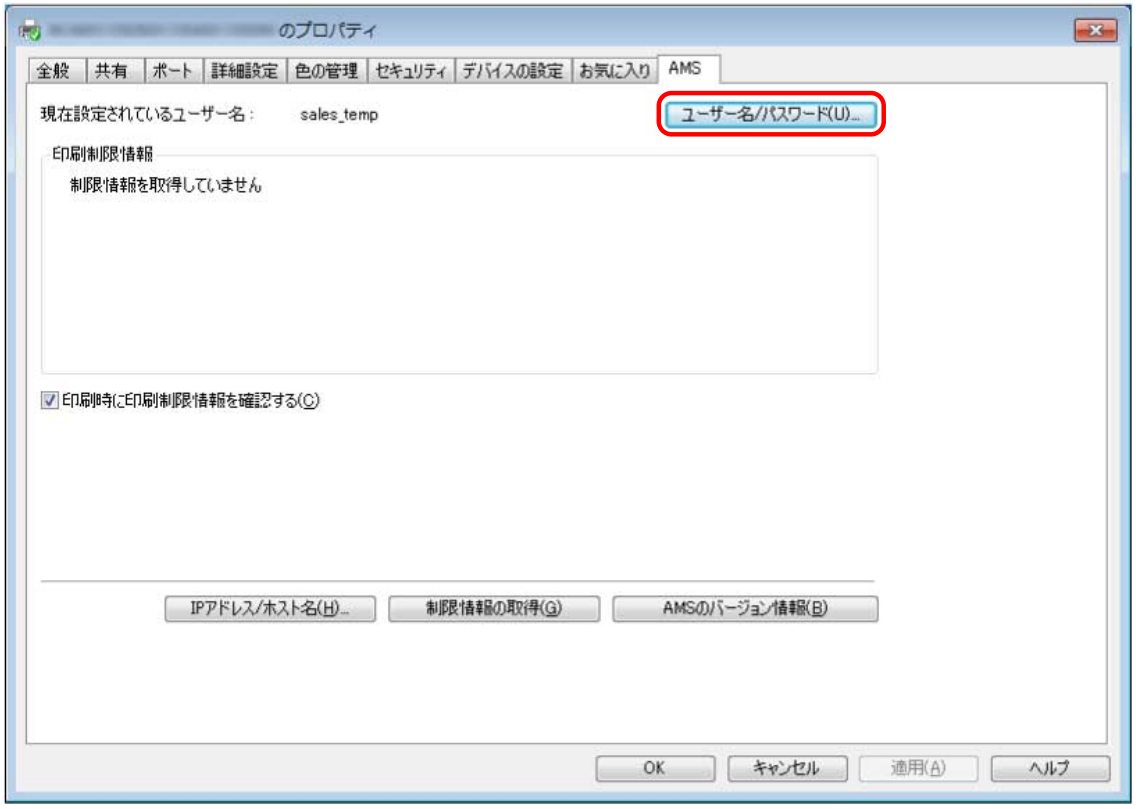
1 **AMS Printer Driver Add-in を有効化したコンピューターにログオンします。**

2 **Windows 8.1/Server 2012 を使用している場合は、デスクトップへ移動します。**

3 **デバイス_A のアイコンを右クリックし、[プロパティ]を選択します。**

4 **[AMS]タブをクリックします。**

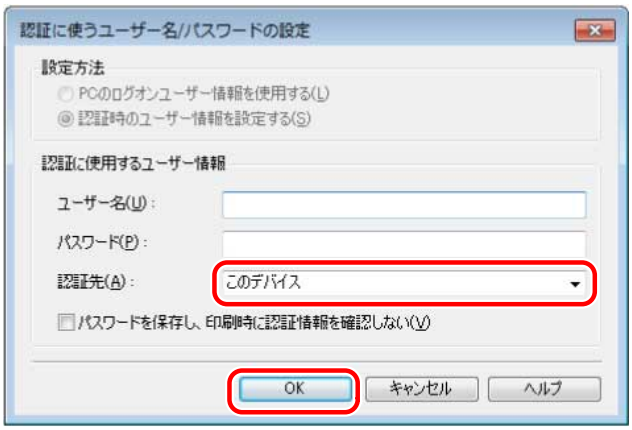
5 **[ユーザー名/パスワード]をクリックします。**



[認証に使うユーザー名/パスワードの設定]ダイアログボックスが表示されます。

6 [認証先]で[このデバイス]が選択されていることを確認し、[ユーザー名]と[パスワード]に[sales_temp]のユーザー名とパスワードを入力したあと、[OK]をクリックします。

[ユーザー名]：sales_temp
[パスワード]：t_password



メモ

- この運用例では、デバイスの環境設定の[プリンタードライバーの制御]で[ユーザー認証情報を保持する]にチェックマークを付けたので、[パスワードを保存し、印刷時に認証情報を確認しない]チェックボックスが有効になっています。

7 [印刷時に印刷制限情報を確認する]にチェックマークを付けます。

8 [OK]をクリックして、ダイアログボックスを閉じます。

他のクライアントコンピューターをセットアップする

「AMS Printer Driver Add-in を有効化する(P. 119)」と**「AMS Printer Driver Add-in にユーザー情報を設定する(P. 120)」**の手順に従って、すべてのユーザーのクライアントコンピューターをセットアップします。

クライアントコンピューターで印刷制限を確認する

設定した印刷制限情報が正しく適用されていることを、クライアントコンピューター上で確認します。

メモ

- AMS Printer Driver Add-in の詳細については、プリンタードライバーの取扱説明書を参照してください。

1 AMS Printer Driver Add-in に[sales_temp]のユーザー名とパスワードを設定したコンピューターにログオンします。

2 任意のアプリケーションから、片面印刷を実行します。

[認証のパスワード確認]ダイアログボックスが表示されます。

メモ

- この運用例では、AMS Printer Driver Add-in にユーザー情報を設定した際に、[パスワードを保存し、印刷時に認証情報を確認しない]にチェックマークを付けていないので、[認証のパスワード確認]ダイアログボックスが表示されます。

3 パスワードを入力して、[OK]をクリックします。

[パスワード]：t_password

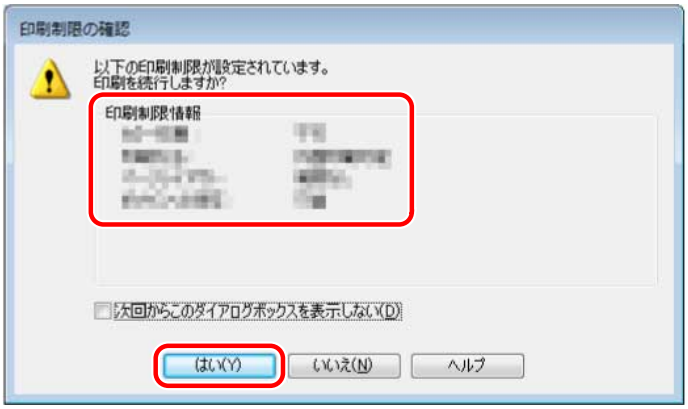
[印刷制限の確認]ダイアログボックスが表示されます。

メモ

- この運用例では、AMS Printer Driver Add-in にユーザー情報を設定した際に、[印刷時に印刷制限情報を確認する]にチェックマークを付けたので、[印刷制限の確認]ダイアログボックスが表示されます。
- Windows 8.1/Server 2012 で Windows ストアアプリから印刷する場合、印刷のたびにパスワードを入力するように設定していると、「印刷するには入力が必要です。デスクトップへ移動します。」というメッセージが表示されます。このときは、デスクトップへ移動し、表示されているダイアログボックスに従って入力してください。
  メッセージは一定時間で消えますが、デスクトップへ移動してダイアログボックスに従った操作を完了するまでは、印刷が開始されません。ご注意ください。

- [パスワードを一時的に保存する]にチェックマークを付けると、次回から、パスワードを入力せずに印刷できるようになります。

4 印刷制限情報を確認して、[はい]をクリックします。



印刷が実行されます。

メモ

- Windows 8.1/Server 2012 で Windows ストアアプリから印刷する場合、印刷のたびに印刷制限情報を確認するように設定していると、「印刷するには入力が必要です。デスクトップへ移動します。」というメッセージが表示されます。このときは、デスクトップへ移動し、表示されているダイアログボックスに従って操作してください。
  メッセージは一定時間で消えますが、デスクトップへ移動してダイアログボックスに従った操作を完了するまでは、印刷が開始されません。ご注意ください。
- [次回からこのダイアログボックスを表示しない]にチェックマークを付けると、次回から、この画面を表示せずに印刷できるようになります。

5 印刷対象が両面で印刷されたことを確認します。

6 他のユーザー名とパスワードを設定したコンピューターにログインして、印刷制限が正しく設定されていることを確認します。

この運用例では、ユーザーによって各デバイスを使用するときの印刷制限が異なります。

ユーザー名	パスワード	[カラー印刷]	[印刷方法]	[ページレイアウト]	[ボックスへの保存]
sales_manager	m_password	可能	片面印刷 可能	制限なし	可能
sales_regular	r_password	可能	片面印刷 可能	制限なし	可能
sales_temp	t_password	不可	両面印刷のみ	制限なし	可能
IT_management	admin_password	可能	片面印刷 可能	制限なし	可能
ゲストユーザー	ゲストユーザーはコンピューターから印刷できません。				

メモ

- お使いの機種によっては、対応していない制限項目があります。

Access Management System の運用を中止する

Access Management System の運用を中止する 126
Access Management System の運用を中止する流れ 127

Access Management System の運用を中止する

ここでは、Access Management System の運用を中止する方法について説明します。

Access Management System の運用を中止する流れ

ここでは、Access Management System の運用を中止するための操作の流れについて説明します。

1. AMS を無効にする

Access Management System の運用を中止するすべてのデバイス上で、AMS を無効にします。

詳細は、デバイスに付属の取扱説明書を参照してください。

2. AMS Printer Driver Add-in を無効にする

クライアントコンピューターのプリンタードライバーで AMS Printer Driver Add-in を無効にします。
詳細は、プリンタードライバーの取扱説明書を参照してください。

困ったときには

困ったときには 129
メッセージ一覧 130
トラブルシューティング 138
終了コード一覧 139

困ったときには

ここでは、トラブルシューティングやエラーメッセージなどを記載しています。

メッセージ一覧

ここでは、Access Management System のセットアップ中や運用中に表示されるメッセージへの対処方法を説明します。

User Authentication(P. 130)
AMS Printer Driver Add-in(P. 130)

User Authentication

<application name> を開始するにあたり、他のアプリケーションとの動作に関して注意事項があります。

状況 1	このデバイスアプリケーションは、AMS に対応していないため、機能毎の詳細な使用制限が行えません。
対処	必要に応じて、ロール情報内の[アプリケーション制限]で使用制限を行ってください。

状況 2	アプリケーション一覧に表示されたデバイスアプリケーションは、AMS に対応していないため、機能毎の詳細な使用制限が行えません。
対処	必要に応じて、ロール情報内の[アプリケーション制限]で使用制限を行ってください。

AMS Printer Driver Add-in

AMS Printer Driver Add-in の操作

以下の設定が印刷制限に反しているため、印刷結果が設定と異なるか印刷ジョブがキャンセルされる可能性があります。
<コントロール名>

状況	ユーザーが設定した値が、制限情報で指定された印刷制限値を超えています。
対処	印刷制限値を確認してください。印刷ジョブがキャンセルされた場合には、制限値を超えない範囲で値を再設定して、もう一度印刷を行ってください。 印刷制限値を確認するには、プリンタープロパティダイアログボックスの[AMS]ページで、[制限情報の取得]ボタンをクリックしてください。

デバイスからの応答がないため、制限情報を取得できませんでした。
電源が入っていることを確認し、しばらくしてから取得しなおしてください。
それでも問題が解決しない場合は、管理者にお問い合わせください。

状況	何らかの原因でデバイスと通信できない状態です。ネットワーク設定、接続状況など通信環境に問題がある可能性があります。

対処	デバイスの電源が ON になっているか、LAN ケーブルなどが正しく接続されているかを確認し、しばらくしてから制限情報を取得しなおしてください。それでも取得できない場合は、AMS 管理者にお問い合わせください。

制限情報を取得できませんでした。

状況 1	ネットワーク設定、接続状況など通信環境に問題がある可能性があります。
対処	ネットワーク設定を確認してから制限情報を取得しなおしてください。それでも取得できない場合は、AMS 管理者にお問い合わせください。

状況 2	AMS が有効になっていません。
対処	AMS を有効に設定してください。詳細は、デバイスに付属の取扱説明書を参照してください。

印刷制限の内容が更新されました。
印刷しなおしてください。

状況	AMS のサーバーに設定されている印刷制限値が更新されています。
対処	印刷制限値を確認して、もう一度印刷を行ってください。 印刷制限値を確認するには、プリンタープロパティダイアログボックスの [AMS] ページで [制限情報の取得] ボタンをクリックしてください。

以下の設定が印刷制限に反しているため、印刷を中止します。
<コントロール名>

状況	プリンターの印刷設定で、制限情報で指定されている印刷制限と併用が不可能な項目が設定されています。
対処	印刷制限値を確認して、もう一度印刷を行ってください。 印刷制限値を確認するには、プリンタープロパティダイアログボックスの [AMS] ページで [制限情報の取得] ボタンをクリックしてください。

このデバイスに対する印刷権限がありません。
別のプリンターを選択してください。

状況	選択したデバイスで印刷する権限が与えられていません。
対処	使用制限の管理者からデバイスに対する印刷許可をもらうか、他のデバイスを選択して印刷してください。

[ボックスへの保存]が[不可]となっているため、[保存]モードを設定できません。
印刷を中止します。

状況	印刷設定の出力方法で[保存]が指定されています。印刷制限で[ボックスへの保存]が許可されていません。
対処	保存印刷の指定を解除してください。または、使用制限の管理者にお問い合わせください。

以下の設定が印刷制限に反しているため、印刷結果が設定と異なる可能性があります。

＜コントロール名＞

状況	ユーザーが設定した値が、制限情報で指定された印刷制限値を超えています。ただし、対応プリンターによっては併用不可設定の項目が印刷制限を越えた場合でも表示されません。
対処	印刷制限値を確認してください。 印刷制限値を確認するには、プリンタープロパティダイアログボックスの [AMS] ページで [制限情報の取得] ボタンをクリックしてください。

[ページレイアウト]が[1〜2 in 1 不可]となっているため、製本印刷ができません。
設定しなおしてください。

状況	ページレイアウト制限のため、製本印刷はできません。
対処	製本印刷の指定を解除してください。または、使用制限の管理者にお問い合わせください。

[ページレイアウト]が[1 in 1 不可]または、[1〜2 in 1 不可]となっているため、ポスター印刷ができません。
設定しなおしてください。

状況	ページレイアウト制限のため、ポスター印刷はできません。
対処	ポスター印刷の指定を解除してください。または、使用制限の管理者にお問い合わせください。

[印刷方法]が[両面印刷のみ]となっているため、ポスター印刷ができません。
設定しなおしてください。

状況	印刷制限のため、ポスター印刷はできません。
対処	ポスター印刷の指定を解除してください。または、使用制限の管理者にお問い合わせください。

[ボックスへの保存]が[不可]となっているため、[保存]モードを設定できません。
設定しなおしてください。

状況	印刷設定の出力方法で[保存]が指定されています。印刷制限で[ボックスへの保存]が許可されていません。。
対処	保存印刷の指定を解除してください。または、使用制限の管理者にお問い合わせください。

[ページレイアウト]が[1〜2 in 1 不可]となっているため、製本印刷ができません。
印刷を中止します。

状況	ページレイアウト制限のため、製本印刷はできません。
対処	製本印刷の指定を解除してください。または、使用制限の管理者にお問い合わせください。

[ページレイアウト]が[1 in 1 不可]または、[1〜2 in 1 不可]となっているため、ポスター印刷ができません。

印刷を中止します。

状況	ページレイアウト制限のため、ポスター印刷はできません。
対処	ポスター印刷の指定を解除してください。または、使用制限の管理者にお問い合わせください。

[印刷方法]が[両面印刷のみ]となっているため、ポスター印刷ができません。
印刷を中止します。

状況	印刷制限のため、ポスター印刷はできません。
対処	ポスター印刷の指定を解除してください。または、使用制限の管理者にお問い合わせください。

フォームファイルの作成、またはオーバーレイ印字はできません。
印刷を中止します。

状況	印刷設定で、オーバーレイ印字、またはフォームファイル作成が指定されています。オーバーレイ印字、およびフォームファイル作成は使用できません。
対処	オーバーレイ印字、またはフォームファイル作成の指定を解除してください。または、使用制限の管理者にお問い合わせください。

デバイスの IP アドレスまたはホスト名が取得できません。
管理者にお問い合わせください。

状況	デバイスの IP アドレスまたはホスト名が取得できませんでした。
対処	Windows の管理者権限を持つユーザーでコンピューターにログオンしている場合、[デバイスの IP アドレス/ホスト名の指定]ダイアログボックスでデバイスの IP アドレス/ホスト名を指定してください。設定できない場合は、AMS 管理者にお問い合わせください。

ネットワークの設定に問題があるため、制限情報を取得できません。
管理者にお問い合わせください。

状況	AMS Printer Driver Add-in に設定した IP アドレスやホスト名が誤っているか、ネットワーク設定に問題がある可能性があります。
対処	[デバイスの IP アドレス/ホスト名の指定]ダイアログボックスで IP アドレス/ホスト名の設定を確認し、ネットワーク設定を確認してから制限情報を取得しなおしてください。それでも取得できない場合は、AMS 管理者にお問い合わせください。

フォームファイルの作成、またはオーバーレイ印字はできません。
設定しなおしてください。

状況	印刷設定で、オーバーレイ印字、またはフォームファイル作成が指定されています。オーバーレイ印字、およびフォームファイル作成は使用できません。
対処	オーバーレイ印字、またはフォームファイル作成の指定を解除してください。または、使用制限の管理者にお問い合わせください。

ネットワークの設定に問題があるため、制限情報を取得できません。管理者にお問い合わせください。印刷を中止します。

状況	AMS Printer Driver Add-in に設定した IP アドレスやホスト名が誤っているか、ネットワーク設定に問題がある可能性があります。
対処	[デバイスの IP アドレス/ホスト名の指定]ダイアログボックスで IP アドレス/ホスト名の設定を確認し、ネットワーク設定を確認してから印刷しなおしてください。それでも印刷できない場合は、AMS 管理者にお問い合わせください。

デバイスからの応答がないため、制限情報を取得できませんでした。印刷を中止します。
電源が入っていることを確認し、しばらくしてから印刷しなおしてください。
それでも問題が解決しない場合は、管理者にお問い合わせください。

状況	何らかの原因でデバイスと通信できない状態です。ネットワーク設定、接続状況など通信環境に問題がある可能性があります。
対処	デバイスの電源が ON になっているか、LAN ケーブルなどが正しく接続されているかを確認し、しばらくしてから印刷しなおしてください。それでも印刷できない場合は、AMS 管理者にお問い合わせください。

[ページレイアウト]が[1 in 1 不可]または、[1〜2 in 1 不可]となっているため、くるみ製本印刷ができません。
設定しなおしてください。

状況	ページレイアウト制限のため、くるみ製本はできません。
対処	くるみ製本の指定を解除してください。または、使用制限の管理者にお問い合わせください。

[ページレイアウト]が[1 in 1 不可]または、[1〜2 in 1 不可]となっているため、くるみ製本印刷ができません。
印刷を中止します。

状況	ページレイアウト制限のため、くるみ製本はできません。
対処	くるみ製本の指定を解除してください。または、使用制限の管理者にお問い合わせください。

ユーザー情報を設定できませんでした。

状況	何らかの原因により、ユーザー情報を取得できませんでした。
対処	しばらくしてからユーザー情報を設定しなおしてください。設定できない場合は、AMS 管理者にお問い合わせください。

デバイスの IP アドレスまたはホスト名を取得できませんでした。

状況	デバイスの IP アドレスまたはホスト名を取得できませんでした。
対処	[デバイスの IP アドレス/ホスト名]テキストボックスに IP アドレスまたはホスト名を入力してください。

[ボックスへの保存]が[不可]となっているため、[ホールド]モードに設定できません。印刷を中止します。

状況	印刷設定の出力方法で[ホールド]が指定されています。印刷制限で[ボックスへの保存]が許可されていません。
対処	ホールドモードの指定を解除してください。または使用制限の管理者にお問い合わせください。

[ボックスへの保存]が[不可]となっているため、選択した出力方法を設定できません。印刷を中止します。

状況	印刷設定の出力方法で[保存]または[ホールド]が指定されています。印刷制限で[ボックスへの保存]が許可されていません。
対処	保存印刷またはホールドモードの指定を解除してください。または使用制限の管理者にお問い合わせください。

[ボックスへの保存]が[不可]となっているため、[ホールド]モードに設定できません。設定しなおしてください。

状況	印刷設定の出力方法で[ホールド]が指定されています。印刷制限で[ボックスへの保存]が許可されていません。
対処	ホールドモードの指定を解除してください。または使用制限の管理者にお問い合わせください。

[ボックスへの保存]が[不可]となっているため、選択した出力方法を設定できません。設定しなおしてください。

状況	印刷設定の出力方法で[保存]または[ホールド]が指定されています。印刷制限で[ボックスへの保存]が許可されていません。
対処	保存印刷またはホールドモードの指定を解除してください。または使用制限の管理者にお問い合わせください。

[デバイスの IP アドレス/ホスト名]が入力されていません。[デバイスの IP アドレス/ホスト名]を入力してください。

状況	[デバイスの IP アドレス/ホスト名]を入力せずに、[OK]がクリックされました。
対処	[デバイスの IP アドレス/ホスト名]を入力してから、[OK]をクリックしてください。

ネットワークの設定に問題があるため、ユーザー情報を設定できませんでした。管理者にお問い合わせください。

状況	AMS Printer Driver Add-in に設定した IP アドレスやホスト名が誤っているか、ネットワーク設定に問題がある可能性があります。
対処	[デバイスの IP アドレス/ホスト名の指定]ダイアログボックスで IP アドレス/ホスト名の設定を確認し、ネットワーク設定を確認してからユーザー情報を設定しなおしてください。それでも設定できない場合は、AMS 管理者にお問い合わせください。

デバイスからの応答がないため、ユーザー情報を設定できませんでした。

電源が入っていることを確認し、しばらくしてから設定しなおしてください。
それでも問題が解決しない場合は、管理者にお問い合わせください。

状況	何らかの原因でデバイスと通信できない状態です。ネットワーク設定、接続状況など通信環境に問題がある可能性があります。
対処	デバイスの電源が ON になっているか、LAN ケーブルなどが正しく接続されているかを確認し、しばらくしてからユーザー情報を設定しなおしてください。それでも設定できない場合は、AMS 管理者にお問い合わせください。

[認証先]に入力したドメイン名に使用できない文字が含まれています。確認してください。

状況	ローカルデバイス認証の場合、［認証先］で、［このデバイス］以外が選択されています。 Active Directory 認証の場合、［認証先］に入力したドメイン名に不正な文字が使用されています。
対処	ローカルデバイス認証の場合は、［認証先］では［このデバイス］を選択してください。Active Directory 認証の場合は、確認後、正しいドメイン名を入力しなおしてください。

設定したユーザー情報と取得した制限情報に含まれるユーザー情報が一致しません。
ユーザー情報を設定しなおしてください。
ドメイン認証の場合は、[認証先]に NetBIOS ドメイン名を入力してください。

状況	AMS Printer Driver Add-in で設定したユーザー情報と、取得した制限情報に設定されているユーザー情報が一致していません。
対処	[認証に使うユーザー名/パスワードの設定]ダイアログボックスで設定したユーザー情報を確認してください。 ローカルデバイス認証の場合は、［認証先］では［このデバイス］を選択してください。Active Directory 認証の場合は、［認証先］に NetBIOS ドメイン名を指定してください。

設定されているユーザー情報と取得した制限情報に含まれるユーザー情報が一致しません。
ユーザー情報を設定しなおしてください。

状況	AMS Printer Driver Add-in で設定したユーザー情報と、取得した制限情報に設定されているユーザー情報が一致していません。
対処	[認証に使うユーザー名/パスワードの設定]ダイアログボックスで設定したユーザー情報を確認してください。 ローカルデバイス認証の場合は、［認証先］では［このデバイス］を選択してください。Active Directory 認証の場合は、［認証先］に NetBIOS ドメイン名を指定してください。

設定されているユーザー情報と取得した制限情報に含まれるユーザー情報が一致しません。
印刷を中止します。

状況	AMS Printer Driver Add-in で設定したユーザー情報と、取得した制限情報に設定されているユーザー情報が一致していません。
対処	[認証に使うユーザー名/パスワードの設定]ダイアログボックスで設定したユーザー情報を確認してください。 ローカルデバイス認証の場合は、［認証先］では［このデバイス］を選択してください。Active Directory 認証の場合は、［認証先］に NetBIOS ドメイン名を指定してください。

アカウントがロックアウトされています。

しばらくしてから再度認証を行うか、管理者にお問い合わせください。

状況	[認証に使うユーザー名/パスワードの設定]ダイアログボックスからの認証に使用するユーザーアカウントがロックアウトされています。
対処	しばらくしてから再度認証を行ってください。認証できない場合は、使用制限の管理者にお問い合わせください。

アカウントがロックアウトされているため、制限情報を取得できませんでした。しばらくしてから取得しなおすか、管理者にお問い合わせください。

状況	制限情報を取得する際の認証に使用するユーザーアカウントがロックアウトされています。
対処	しばらくしてから再度認証を行ってください。制限情報を取得できない場合は、使用制限の管理者にお問い合わせください。

アカウントがロックアウトされているため、制限情報を取得できませんでした。印刷を中止します。しばらくしてから印刷しなおすか、管理者にお問い合わせください。

状況	印刷時の認証に使用するユーザーアカウントがロックアウトされています。
対処	しばらくしてからもう一度印刷を行ってください。印刷できない場合は、使用制限の管理者にお問い合わせください。

トラブルシューティング

ここでは、Access Management System の運用中にトラブルが生じた場合の対処方法について説明します。

[1〜2 in 1 不可]に設定されているユーザーが、ボックス文書を出力できない

原因	異なるページレイアウト設定の文書（たとえば、2 in 1 文書と 4 in 1 文書）を結合してボックスに保管すると、ページレイアウト設定がリセットされて 1 in 1 文書として保存されるため、[1〜2 in 1 不可]に設定されているユーザーは出力できません。
対処	ページレイアウト制限を適用されているユーザーが出力する可能性のある文書をボックスに保管する場合は、異なるページレイアウトの文書を結合しないでください。

終了コード一覧

ジョブや操作が正常に終了していない場合は、終了コードを確認し、表示されている終了コードに応じて、必要な処理を行ってください。終了コードは、[状況確認/中止]画面またはシステム状況画面のジョブ履歴の詳細情報画面で確認することができます。

メモ

- 「# 817」は、使用制限の対象となるデバイスに対して重連コピーを送信したデバイスで表示されます。
- 「# 866」は、コンピューターからジョブが送信されたデバイスで表示されます。

#817

状況	重連コピーの送信先となる AMS 対応デバイスで、重連コピーの受信が許可されていないため、ジョブがキャンセルされました。
対処	重連コピーの送信先となる AMS 対応デバイスで、重連コピーの受信を許可に設定してください。詳細は、デバイスに付属の取扱説明書を参照してください。AMS 対応デバイスで重連コピーを受信させない場合は、送信元のデバイスで重連コピープリンターの送信先としての登録を解除してください。

#866

状況	セキュリティー違反エラーのジョブを検知しました。
対処	ジョブの内容を確認してください。

付録

付録 141
Access Management System 運用上のセキュリティーについて 142
アクセス制御用の鍵ペアを更新する 143
その他の注意事項 145

付録

ここでは、セキュリティー上の注意事項などを記載しています。

Access Management System 運用上のセキュリティーについて

Access Management System は、外部への情報流出やコストの抑止などを目的に、デバイス機能の使用を制限するシステムです。

Access Management System の導入後、デバイス利用環境のセキュリティーを保つために、以下のセキュリティーポリシーを考慮して、運用されることをおすすめします。

ユーザーの管理

Active Directory を導入していない場合でも、ユーザーアカウントの管理を行ってください。たとえば、1 つのユーザーアカウントで複数のユーザーがデバイスにログインできるような運用は避けてください。デバイスとコンピューターへのログインユーザー名を同じにすることで、より厳密にユーザー管理を行うことができます。

コンピューターの管理者権限の管理

コンピューターの管理者権限の管理を行ってください。たとえば、Windows の管理者権限を持つユーザーでコンピューターにログオンして、AMS Printer Driver Add-in を無効化した場合は、Access Management System による印刷制限が行えなくなります。

ドメイン認証で運用している場合は、各ユーザーがコンピューターのログオン時に、ドメインにログインすることをおすすめします。

デバイスの管理

AMS 対応デバイス以外のデバイス（使用制限の対象外デバイス）については、独自に管理を行ってください。たとえば、AMS 対応デバイスでカラー出力や外部への送信機能を制限している場合でも、Access Management System で管理していないデバイスでこれらの機能を利用することが可能です。

Access Management System で管理していないデバイスは、管理者の近くに設置するなど、セキュリティーの管理を行うことをおすすめします。

アクセス制御用の鍵ペアを更新する

セキュリティーを向上させるため、必要に応じて鍵ペアは定期的に更新してください。ここでは、アクセス制御用の鍵ペアを更新する手順を説明します。

鍵ペアの更新後、すぐに印刷を実行する場合は、その前に、プリンタープロパティダイアログボックスの［AMS］ページの［制限情報の取得］をクリックして、印刷制限情報を取得してください。AMS Printer Driver Add-in が、鍵ペア更新前に取得された印刷制限情報を使用して印刷しようとすると、エラー終了します。2 度目以降の印刷が禁止されている文書などは、印刷できなくなりますので、ご注意ください。（鍵ペアの更新後、約 30 分を経過すると、自動的に印刷制限情報が取得されるので、正常に印刷できます。）

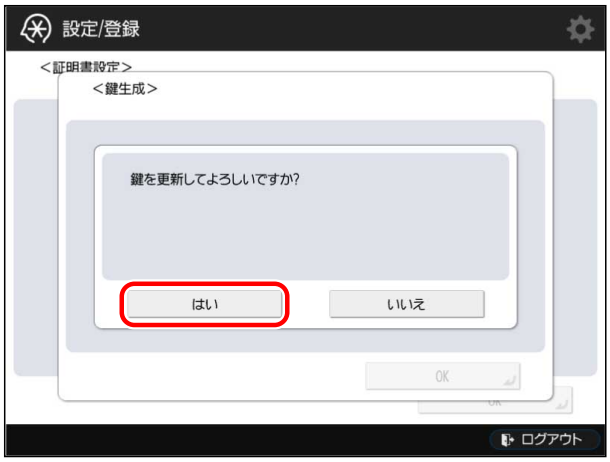
アクセス制御用の鍵ペアを更新する(P. 143)

アクセス制御用の鍵ペアを更新する

1 **（設定/登録）→[管理設定]→[デバイス管理]→[証明書設定]→[鍵生成]を押します。**

2 **[アクセス制御用の鍵生成/更新]を押します。**

3 **[はい]を押します。**



4 メインメニューまで戻ってからデバイスを再起動します。

鍵ペアが更新されます。

重要

- 鍵ペアは、デバイスの再起動後に更新されます。再起動の方法については、デバイスに付属の取扱説明書を参照してください。

その他の注意事項

ここでは、Access Management System を運用する上での注意事項について説明します。

部門別 ID 管理機能との併用について

User Authentication を Active Directory 認証方式や LDAP 認証方式で運用する場合は、部門別 ID 管理機能と併用できません。

部門別 ID 管理機能の詳細は、デバイスに付属の取扱説明書を参照してください。

ジョブのキャンセル

関連付けられたロールにかかわらず、使用制限が行われている AMS 対応デバイスから、以下の処理中にユーザーがログアウトした場合は、ジョブがキャンセルされます。

- スキャン実行中
- コピーのジョブ結合の続行確認中
- お試しコピーの続行確認中
- 送信文書のプレビュー中

リモート UI の制限

使用制限が行われている AMS 対応デバイスに、以下のユーザー以外がログインした場合は、[ポータルへ]、[状況確認/中止]以外のボタンをクリックすると、エラー画面が表示されます。

- [Administrator]/[DeviceAdmin]/[NetworkAdmin]ロールが関連付けられているユーザー
- 使用制限のすべての項目が制限されない設定のロールを関連付けられているユーザー

リモート UI のアドレス帳

User Authentication が搭載されている機種では、リモート UI で提供されるアドレス帳（宛先表の管理機能）の使用制限を設定することができます。
ロールの［アドレス帳の利用/ネットワーク保存先の登録］で設定します。

リモート UI のダイレクトプリント

User Authentication が搭載されている機種では、デバイスの環境設定で、リモート UI で提供されているダイレクトプリント機能（プリンタードライバーを介せずにプリントする機能）の使用制限を設定することができます。

デバイスの環境設定で、［利用を制限する機能］の［AMS Printer Driver Add-in を使用しないドライバーからのプリント］にチェックマークを付けた場合は、ダイレクトプリントを利用できません。

デバイスの環境設定で、［利用を制限する機能］の［AMS Printer Driver Add-in を使用しないドライバーからのプリント］にチェックマークを付けない場合は、ダイレクトプリントを利用できます。ただし、カラー印刷を制限するなどの詳細な使用制限を行うことができません。

重連コピー機能の制限

使用制限が行われている AMS 対応デバイスは、重連コピーの送信元として使用することはできません。重連コピーに関連するキーは、以下のように制限されます。

- コピー基本画面の[その他の機能]-[重連コピー]が表示されない
- [設定/登録]画面から設定する[重連コピーのリモートデバイス登録]が無効になる

[設定/登録]の制限

デバイスの[設定/登録]の一部の設定項目は、AMS が稼働しているデバイスでは制限がかかるため、表示されなくなります。詳細は、「**[設定/登録]の制限(P. 24)**」を参照してください。

[設定/登録]の[新規宛先の制限]の制限

AMS が稼働しているデバイスでは、[設定/登録]の[新規宛先の制限]は利用できません。設定は無効化されて、非表示となります。AMS を無効に変更しても、設定は自動で元の設定には戻りません。再度設定が必要となります。

AMS が稼働しているデバイスでは、類似の制限をロール内の制限項目[新規宛先への送信]でユーザーごとに設定できます。

[設定/登録]の[アドレス帳の暗証番号]の制限

AMS が稼働しているデバイスでは、[設定/登録]の[アドレス帳の暗証番号]は利用できません。暗証番号はクリアされて、非表示となります。AMS を無効に変更しても、暗証番号は自動で元の設定には戻りません。再度設定が必要となります。

AMS が稼働しているデバイスでは、アドレス帳に対する制限は、ロール内の制限項目[アドレス帳の利用/ネットワーク保存先の登録]でユーザーごとに設定できます。

オーバーレイ印字の制限

AMS が稼働しているデバイスでは、プリンタードライバ―からオーバーレイ印字、およびフォームファイル作成は使用できません。

ファクスの制限

AMS が稼働しているデバイスでは、ファクスのダイレクト送信、オンフックは使用できません。

This Font Software is licensed under the SIL Open Font License, Version 1.1.

This license is copied below, and is also available with a FAQ at: http://scripts.sil.org/OFL

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION
This license becomes null and void if any of the above conditions are not met.

DISCLAIMER
THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.