内蔵 Web サーバー — セキュリティ

管理者ガイド

CS310, CS410, CS510, CX310, CX410, CX510, M1140, M1145, M3150, M3150dn, M5155, M5163, M5170, XM1140, XM1145, XM3150, XM5163, XM5170, XM7155, XM7163, XM7170, XC2132, MS310, MS410, MS510, MS61x, MS81x, MX310, MX410, MX51x, MX61x, MX71x, MX81x

2013 年 10 月

www.lexmark.com

目次

このガイドの対象となるセキュリティデバイス

製品定義に基づいてサポートされるセキュリティレベルは 2 種類です。使用可能な全機能の一覧については、5 ページの「認証と権限」を参照してください。

簡易セキュリティデバイス

CS310n/dn、CS410n/dn、CS410dtn、CX310n/dn、M1140、M1145、M3150dn、M5163dn、MS310d/dn、MS410d/dn、MS510dn、MS610dn、MS610dtn、MS810n/dn、MS810dtn、MS811n/dn、MS811dtn、MS812dn、MS812dtn、MX310dn

詳細セキュリティデバイス

CS510de、CS510dte、CX410de、CX410e/dte、CX510de、CX510dhe/dthe、M3150、M5155、M5163、M5170、XM1140、XM1145、XM3150、XM5163、XM5170、XM7155、XM7163、XM7170、XC2132、MS610de、MS610dte、MS810de、MS812de、MX410de、MX510de、MX511de、MX511dhe、MX511dte、MX610de、MX611de、MX611dhe、MX611dte、MX710de、MX710dhe、MX711de、MX711dhe/dthe、MX810de、MX810dfe、MX810dme、MX810dte、MX810dtfe、MX810dtme、MX810dxe、MX810dxfe、MX810dxme、MX811de、MX811dfe、MX811dme、MX811dte、MX811dtfe、MX811dtme、MX811dxe、MX811dxfe、MX811dxme、MX812de、MX812dfe、MX812dme、MX812dte、MX812dtfe、MX812dtme、MX812dxe、MX812dxfe、MX812dxme

内蔵 Web サーバーのセキュリティ機能を使用する

Lexmark 内蔵 Web サーバーは進化を遂げ、現在の変化の多い環境において、出力したドキュメントを安全な機密性の高い方法で保管できます。認証やグループ権限などの従来の方法では、管理者が内蔵 Web サーバーセキュリティテンプレートを使用し、機密ドキュメントを作成、保存、および送信するデバイスへのアクセスを制御できます。セキュリティテンプレートは Lexmark が開発した革新的なツールです。管理者はこのテンプレートを使用して、安全で柔軟なプロファイルを作成することで、重要なプリンタ機能や出力を、適切な認証資格情報を持つユーザーに制限できます。ソフト構成機能を単独で使用するか、共通アクセスカードなどの物理セキュリティと併用すると、プリンタがドキュメントセキュリティチェーンの弱点ではなくなります。

基本事項を理解する

内蔵 Web サーバーによってプリンタを保護するには、1 つ以上のコンポーネントを組み合わせ、プリンタを使用できるユーザーおよびユーザーがアクセスできる機能を定義します。認証、権限、グループなどのコンポーネントがあります。

プリンタのセキュリティを設定する前に、ユーザーとユーザーが実行する必要がある操作を特定する計画を作成します。次のような項目を考慮する必要があります。

- プリンタの場所と権限のあるユーザーがその領域にアクセスするかどうか
- プリンタに送信または保存される機密ドキュメント
- 組織の情報セキュリティポリシー。

認証と権限

認証は、システムが安全にユーザーを識別する方式です。

権限は、システムで認証されたユーザーが使用できる機能を指定します。許可された機能群は、「アクセス権」とも呼ばれます。

製品定義に基づいてサポートされるセキュリティレベルは 2 種類です。最も簡易的なレベルのセキュリティは、内部デバイス認証および権限方式だけをサポートしています。より詳細レベルのセキュリティでは、外部と内部の認証、権限、管理用の追加制限能力、機能、およびソリューションアクセスが許可されています。詳細セキュリティは、追加のソリューションをインストールできるデバイスでサポートされています。

簡易セキュリティでは、「パネル暗証番号保護」を使用して、プリンタコントロールパネルへのユーザーアクセスを制限し、「Web ページパスワード保護」を使用して、デバイスへの管理者アクセスを制限します。詳細については、10 ページの「パネル暗証の保護で 暗証番号 を作成する」および9 ページの「Web ページパスワードの保護でパスワードを作成する」を参照してください。

詳細レベルセキュリティのデバイスでは、指定した他の認証および権限の他に、暗証番号およびパスワード制限がサポートされています。このドキュメントでは、詳細セキュリティデバイスを中心に説明します。

✓ = サポート対象
X = サポート対象外

機能	簡易セキュリティデバイス	詳細セキュリティデバイス
パネル 暗証番号 保護	✓	X
暗証番号保護	X	✓

√ = サポート対象 X = サポート対象外		
機能	簡易セキュリティデバイス	詳細セキュリティデバイス
Web ページパスワード保護	√	X
パスワード保護	X	√
内部アカウント（ユーザー名およびユーザー名/パスワード）	X	√
グループ（内部）	X	√
LDAP	X	√
LDAP+GSSAPI	X	√
Kerberos 5	X	√
Active Directory	X	√
制限されたアクセス制御	√	X
アクセス制御（完全）	X	√
セキュリティテンプレート	X	√
基本セキュリティ設定	X	√

内蔵 Web サーバーは、次の 1 つ以上を使用して認証および権限を処理します。ビルディングブロックとも呼ばれます。

- 暗証番号 またはパネル 暗証番号 保護
- パスワードまたは Web ページパスワード保護
- 内部アカウント
- LDAP
- LDAP+GSSAPI
- Kerberos 5（LDAP+GSSAPI と合わせた場合にだけ使用）
- Active Directory

一部のプリンタモデルで低レベルセキュリティを実施するには、暗証番号とパスワード、またはパネル 暗証番号保護と Web ページパスワード保護を使用できます。これによって、プリンタまたは特定のプリンタ機能へのアクセスを、正しいコードを知っているユーザーに制限できます。このタイプのセキュリティは、プリンタがロビーや他の公共のビジネスエリアにあり、パスワードまたは暗証番号を知っている従業員だけがプリンタを使用できるようにする場合に適切なことがあります。正しいパスワードまたは 暗証番号 を入力する全員が同じ権限を取得し、ユーザーを個別に識別できないため、パスワードと暗証番号の安全性は、ユーザーを識別するか、識別して権限付与する必要がある他のビルディングブロックよりも低いと考えられます。

メモ: デフォルト設定には、認証または権限ビルディングブロックは含まれていません。つまり、全員が内蔵 Web サーバーに無制限にアクセスできます。

グループ

管理者は、内部アカウントまたは LDAP/LDAP+GSSAPI ビルディングブロックについて、最大 32 グループを使用するように指定できます。内蔵 Web サーバーセキュリティの目的では、グループを使用し、類似した機能へのアクセス権が必要なユーザーのグループを指定します。たとえば、会社 A では、倉庫の従業員はカラー印刷する必要がありませんが、営業およびマーケティングの従業員は毎日カラー印刷が必要です。このシナリオでは、「倉庫」グループと「営業およびマーケティング」グループを作成する必要があります。

アクセス制御

デフォルトでは、すべてのデバイスメニュー、設定、および機能のセキュリティが有効になっていません。アクセス制御（一部のデバイスでの別名「機能アクセス制御」）は、特定のメニューと機能へのアクセスを管理し、全体として機能を無効にするために使用されます。アクセス制御は、パスワード、暗証番号、またはセキュリティテンプレートによって設定できます。制御可能な機能数は、デバイスのタイプによって異なります。ただし、一部の MFP では、40 以上の個別メニューと機能を保護できます。

メモ: 個別のアクセス制御の一覧と説明については、42 ページの「付録 D：アクセス制御」を参照してください。

セキュリティテンプレート

一部のシナリオでは、共通デバイス機能への 暗証番号 保護アクセスなどの限定的なセキュリティだけが要求されます。別のシナリオでは、より強力なセキュリティとロールに基づく制限が求められます。個別のビルディングブロック、グループ、およびアクセス制御では、複雑なセキュリティ環境の要件を満たさない場合があります。印刷、コピー、Fax などの共通機能群へのアクセスが必要な異なるグループのユーザーに対応するために、管理者は、すべてのユーザーに必要な機能が割り当てられ、他の機能は権限のあるユーザーにだけ制限されるように、これらのコンポーネントを組み合わせることができなければなりません。

セキュリティテンプレートは、ビルディングブロックまたは 1 つ以上のグループと組み合わせられた特定のビルディングブロックを使用して作成されたプロファイルです。ビルディングブロックの組み合わせ方法によって、作成されるセキュリティのタイプが決まります。

ビルディングブロック	セキュリティのタイプ
内部アカウント	認証のみ
内部アカウントとグループ	認証と権限
Kerberos 5	認証のみ
LDAP	認証のみ
LDAP とグループ	認証と権限
LDAP+GSSAPI	認証のみ
LDAP+GSSAPI とグループ	認証と権限
パスワード	権限のみ
暗証番号	権限のみ

各デバイスは最大 140 のセキュリティテンプレートをサポートでき、管理者が各アクセス制御の特定のプロファイルを作成できます。

基本セキュリティセットアップでアクセスを制限する

基本セキュリティセットアップを使用すると、内蔵 Web サーバーのセキュリティセットアップとプリンタコントロールパネルの構成設定メニューへのアクセスが制限されます。簡易内部デバイスセキュリティ認証方式を定義できます。

メモ:

- プリンタ機種によりこの機能が無いものもあります。
- デフォルト設定には、認証または権限ビルディングブロックは含まれていません。つまり、全員が内蔵 Web サーバーに無制限にアクセスできます。

基本セキュリティセットアップを適用する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [認証タイプ]ドロップダウンリストから、次のいずれかを選択します。
   - **暗証番号**—暗証番号を入力します。各暗証番号の桁数は 4 ～ 16 桁でなければなりません。
   - **パスワード**—パスワード名を入力します。各パスワードには、128 文字以下の UTF-8 文字で、一意の名前を入力します。
   - **ユーザー ID とパスワード**—一意のユーザー ID を入力し、パスワードの名前を入力します。各パスワードには、128 文字以下の UTF-8 文字で、一意の名前を入力します。

3 **[基本セキュリティセットアップの適用]**をクリックします。

   メモ: この設定を適用すると、前の設定が上書きされる場合があります。

新しい設定が送信されます。次回、[セキュリティセットアップ]にアクセスするときに、適切な認証情報を入力するように要求されます。

基本セキュリティセットアップを変更または削除する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 適切な認証情報を入力し、[セキュリティセットアップ]へのアクセス権を取得します。

3 [基本セキュリティセットアップの変更と削除]で、新しい認証情報を入力します。

4 **[基本セキュリティセットアップの変更]**をクリックして、新しい認証情報を入力し、[セキュリティセットアップ]へのアクセス権を取得します。あるいは、**[基本セキュリティセットアップの削除]**をクリックし、すべての認証要件を削除します。

ビルディングブロックを編集

詳細セキュリティセットアップのパスワードを作成する

メモ:

- プリンタ機種によりこの機能が無いものもあります。
- 内蔵 Web サーバーは、各対応デバイスに、合計 250 個のユーザーレベルおよび管理者レベルパスワードを保存できます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [詳細セキュリティセットアップ]の下で**[パスワード]**をクリックします。

3 [パスワードを管理]の下で**[パスワードを追加]**をクリックします。

4 [設定名]ボックスでパスワード名を入力します。

メモ: 各パスワードには、128 文字以下の UTF-8 文字で、一意の名前を入力します(例:「Copy Lockout Password」)。

5 該当するボックスにパスワードを入力し、パスワードを再入力して確認します。

6 パスワードが管理者パスワードとして使用される場合は、**[管理者パスワード]**を選択します。

メモ: 管理者レベルのパスワードは標準のパスワードよりも優先されます。機能または設定は標準のパスワードで保護されている場合、管理者レベルのパスワードにもアクセス権が付与されます。

7 **[送信]**をクリックします。

メモ:

- パスワードを編集するには、リストからパスワードを選択し、設定を変更します。
- パスワードを削除するには、リストからパスワードを選択し、**[エントリの削除]**をクリックします。**[削除のリスト]**をクリックすると、選択状況に関係なく、リストのすべてのパスワードが削除されます。

Web ページパスワードの保護でパスワードを作成する

メモ:

- 低レベルセキュリティのプリンタでだけ使用できます。
- 内蔵 Web サーバーは、各対応デバイスに、合計 250 個のユーザーレベルおよび管理者レベルパスワードを保存できます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[Web ページパスワードの保護]**をクリックします。

2 [基本セキュリティ設定:ユーザーパスワードの作成]で、該当するボックスにパスワードを入力し、パスワードを再入力して確認します。

3 [基本セキュリティ設定:管理者パスワードの作成]で、該当するボックスにパスワードを入力し、パスワードを再入力して確認します。

メモ: 管理者レベルのパスワードは標準のパスワードよりも優先されます。機能または設定は標準のパスワードで保護されている場合、管理者レベルのパスワードにもアクセス権が付与されます。

4 **[変更]**をクリックします。

メモ: パスワードを編集するには、パスワードを変更し、**[変更]**をクリックします。パスワードを削除するには、**[エントリの削除]**をクリックします。

詳細セキュリティセットアップの 暗証番号 を作成する

メモ: プリンタ機種によりこの機能が無いものもあります。

一般的に、個人 ID 番号(暗証番号)が使用され、特定のデバイスメニューまたはデバイス自体へのアクセスが制御されます。また、暗証番号 を使用して、ドキュメント出力へのアクセスも制御できます。この場合、保留中の印刷、コピー、または Fax ジョブを取得するために、正しい 暗証番号 を入力する必要があります。内蔵 Web サーバーは、合計 250 個のユーザーレベルおよび管理者レベルの 暗証番号 を保存できます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [詳細セキュリティセットアップ]の下で**[暗証番号]** > **[暗証番号 を追加]**をクリックします。

3 [設定名]ボックスで 暗証番号 設定名を入力します。

メモ: 各 暗証番号 は、128 文字以下の UTF-8 文字で、一意の名前を入力します(例:「Copy Lockout 暗証番号」)。

4 該当するボックスに 暗証番号 を入力し、暗証番号 を再入力して確認します。

デフォルトの 暗証番号 の長さを変更するには:

a **[設定]** > **[セキュリティ]** > **[その他のセキュリティセットアップ]**をクリックします。

b [最小暗証番号]フィールドに数字を入力し、**[送信]**をクリックします。

5 暗証番号 が管理者 暗証番号 として使用される場合は、**[管理者 暗証番号]**をクリックします。

メモ: 特定の管理者 暗証番号 によってアクティビティが保護されている場合は、その 暗証番号 だけがアクセス権を付与します。

6 **[送信]**をクリックします。

パネル暗証の保護で 暗証番号 を作成する

メモ: 低レベルセキュリティの一部のプリンタのみこの機能があります。

一般的に、個人 ID 番号(暗証番号)が使用され、特定のデバイスメニューまたはデバイス自体へのアクセスが制御されます。また、暗証番号を使用して、ドキュメント出力へのアクセスも制御できます。この場合、保留中の印刷、コピー、または Fax ジョブを取得するために、正しい 暗証番号 を入力する必要があります。内蔵 Web サーバーは、合計 250 個のユーザーレベルおよび管理者レベルの暗証番号を保存できます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[パネル暗証の保護]**をクリックします。

2 [基本セキュリティ設定:ユーザー 暗証番号 の作成]で、該当するボックスに 暗証番号を入力し、暗証番号を再入力して確認します。

3 [基本セキュリティ設定:管理者暗証番号の作成]で、該当するボックスに 暗証番号を入力し、暗証番号を再入力して確認します。

メモ: 各暗証番号は、128 文字以下の UTF-8 文字で、一意の名前を入力します(例:「Copy Lockout 暗証番号」)。

4 **[変更]**をクリックします。

メモ:

- アクセス制御が[ユーザー暗証番号]に設定されていると、プリンタの管理者暗証番号 でアクセス制御できます。
- この手順を完了した後にかぎり、ユーザー暗証番号または管理者暗証番号をプリンタの機能に割り当てることができます。

内部アカウントを設定する

メモ: プリンタ機種によりこの機能が無いものもあります。

内蔵 Web サーバー管理者は、サポート対象のデバイスごとに 1 つの内部アカウントビルディングブロックを設定できます。各内部アカウントビルディングブロックには、最大 250 個のユーザーアカウントと 32 個のユーザーグループを含めることができます。

内部アカウントビルディングブロックを単独でセキュリティテンプレートで使用し、認証レベルのセキュリティを実施できます。あるいは、1 つ以上のグループとともに使用し、認証と権限の両方を実施できます。

ユーザーグループを定義する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [詳細セキュリティセットアップ]の下で**[内部アカウント]** > **[内部アカウントに使用するグループをセットアップ]**をクリックします。

3 グループ名を入力します。

メモ: グループ名は、128 文字以下の UTF-8 文字で入力します。

4 **[追加]**をクリックします。

5 手順 3 ～ 4 を繰り返し、その他のユーザーグループを追加します。

メモ: グループを作成するときには、まず、すべてのユーザーのリストを作成します。次に、すべてのユーザーが必要なデバイス機能と、特定のユーザーだけが必要な機能を決定します。セキュリティテンプレートと統合されると、各グループはロールを実行します。ユーザーを複数のグループまたはロールに割り当て、すべての必要な機能へのアクセス権を付与できます。

ユーザーアカウントを作成する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [詳細セキュリティセットアップ]の下で**[内部アカウント]** > **[内部アカウントを追加]**をクリックします。

3 各アカウントに必要な情報を指定します。

- **アカウント名**—ユーザーのアカウント名を入力します(例:「Jack Smith」)。164 文字以下の UTF-8 文字で入力します。
- **ユーザー ID**—アカウントの ID を入力します(例:「jsmith」)。128 文字以下の UTF-8 文字で入力します。
- **パスワード**—8 ～ 128 文字のパスワードを入力します。
- **パスワード再入力**—前のフィールドに入力したパスワードを再入力します。
- **E メールアドレス**—ユーザーのメールアドレスを入力します(例:「jsmith@company.com」)。
- **グループ**—アカウントが属するグループを選択します。**Ctrl** キーを押すと、アカウントの複数のグループを選択できます。

4 **[送信]**をクリックすると、新しいアカウントが保存されます。**[キャンセル]**をクリックすると、新しいアカウントを保存せずに、[内部アカウントの管理]メニューに戻ります。

内部アカウントの設定を指定する

内部アカウント設定は、新しい内部アカウントの作成時に管理者が送信する情報と、認証時にユーザーが送信する情報を定義します。

- **カスタムビルディングブロック名**—このビルディングブロックの一意の名前を入力します。
- **E メールアドレスが必要**—このボックスをオンにすると、新しい内部アカウントの作成時に、E メールアドレスが必須フィールドになります。
- **ユーザー資格証明書が必要**—[**ユーザー ID**]または[**ユーザー ID とパスワード**]を選択し、認証時にユーザーが送信する必要がある情報を指定します。

プリンタを Active Directory ドメインに接続する

メモ:

- プリンタ機種によりこの機能が無いものもあります。
- 必ず HTTPS を使用し、プリンタをドメインに接続させる際に使用された認証資格情報を保護してください。
- HTTPS を選択しない場合は、Active Directory を設定できません。

1 Web ブラウザを開き、プリンタの IP アドレスまたはホスト名を入力します。

メモ: プリンタの IP アドレスまたはホスト名に関連付けられた警告メッセージが表示されます。続行するには、[**このサイトの閲覧を続行する(推奨されません)**]をクリックします。

2 内蔵 Web サーバーで次の操作を実行します。

[**設定**] > [**セキュリティ**] > [**セキュリティセットアップ**] > [**Active Directory**] > [**Active Directory ドメインに接続**]

3 各アカウントに必要な情報を指定します。

- **ドメイン名**--参加するドメインの名前を入力します。ドメイン名は大文字で入力することをお勧めします。
- **ユーザー ID**--ネットワーク管理者、またはコンピュータをネットワークに追加する権限を持つユーザーのユーザー名を入力します。
- **パスワード**--ネットワーク管理者、またはドメインに接続する権限を持つユーザーのパスワードを入力します。

  メモ: パスワードは大文字と小文字が区別されますが、これらのパスワードはデバイスによってキャッシュに保存されません。
- **組織単位**--組織単位名を入力します(任意)。

  メモ: これは必須フィールドではないため、省略可能です。

4 [**送信**]をクリックします。

メモ:

- [**送信**]ボタンをクリックすると、画面が点滅し、クリック音が聞こえる場合があります。
- 設定が失敗した場合は、大きい赤色の **X** マークが表示されます。また、ドメイン参加エラーの原因を示すメッセージも表示されます。

5 エラーがない場合は、設定が完了です。[**セキュリティテンプレートを管理**]をクリックすると、Active Directory 情報を使用して、セキュリティセットアップを完了できます。

メモ: LDAP+GSSAPI ビルディングブロックの確認や小規模な修正を行う場合は、[**セキュリティセットアップに戻る**]をクリックし、下に示される手順に従います。

確認および変更を開始するには、次の手順を実行します。

a [詳細セキュリティセットアップ]の下で**[Kerberos 5]**をクリックします。

b **[ファイルの表示]**をクリックし、Active Directory 設定を使用して作成された Kerberos 構成ファイルを開きます。

c ファイルを確認し、ブラウザの戻るボタンをクリックして、確認プロセスを続行します。

メモ: Kerberos 構成ファイルを編集またはコピーして、古いデバイスで使用しないでください。KDC サーバーアフィニティサービスで問題が発生する原因になるおそれがあります。古いデバイスは、KDC サーバーアフィニティサービスに関連付けられた特殊なマッピングを認識しません。

d **[セキュリティセットアップに戻る]**をクリックし、**[LDAP+GSSAPI]**をクリックします。

e [LDAP+GSSAPI 設定]の下で、Active Directory 設定プロセスによって作成されたビルディングブロックを検索し、クリックします。

メモ: デフォルトでは、ビルディングブロックはレルム名になります。また、[サーバーアドレス]フィールドには、ドメインコントローラ名が入力されます。

f 環境に応じて、次のようなビルディングブロックの一部を変更します。

- **サーバーポート**--LDAP の標準ポートは 389 です。別の共通ポートは 3268 ですが、Active Directory のグローバルカタログサーバー専用です。該当する場合は、ポートを 3268 に変更し、問い合わせ処理を高速化します。
- **検索ベース**--検索を開始するディレクトリツリーの場所をデバイスに指示します。識別名として指定されます。少なくとも、ディレクトリのルート(「dc=company,dc=com」など)を指定することをお勧めします。
- **Kerberos サービスチケットを使用する**--別名 SPNEGO という詳細設定です。ユーザーがコンピュータにログインしたときにユーザーが持っているセッションチケットが使用されます。この設定を選択しないことをお勧めします。
- **Active Directory デバイス資格証明書を使用**--Active Directory で作成されたサービスアカウントを使用する必要があるため、通常はこのボックスをオンにする必要があります。既存のサービスアカウントを使用するか、ユーザー認証資格情報(詳細設定)を使用するために、この設定を使用しない場合は、このボックスをオフにします。

g 必要に応じて、ページの右側のスクロールバーを使用し、次のフィールドにスクロールします。

- **グループ検索ベース**--特定のグループの検索を開始するディレクトリツリーの場所をデバイスに指示します。ユーザーまたはグループに基づく権限が必要でない場合は、このフィールドを入力する必要はありません。
- **グループの短い名前**--ユーザー定義フィールドであり、グループの名前を作成し、グループ ID に関連付けることができます。
- **グループ ID**--検索し、認証されたユーザーが権限のあるグループのメンバーであるかどうかを確認する必要があるコンテナまたは組織単位をデバイスに指示します。

h 変更した場合は、ページの右側のスクロールバーを使用して、ページの下にスクロールし、**[変更]**をクリックします。

LDAP を使用する

メモ: プリンタ機種によりこの機能が無いものもあります。

LDAP(ライトウェイトディレクトリアクセスプロトコル)は標準に基づいたプラットフォーム横断型の拡張可能なプロトコルです。TCP/IP レイヤーの上で直接動作し、特に組織的な情報ディレクトリに保存された情報にアクセスするために使用されます。LDAP の強みの 1 つは、特別な統合なしで、多数のさまざまな種類のデータベースと連携できる点です。このため、他の認証方式よりも柔軟です。

メモ:

- サポートされているデバイスには、最大 5 個の一意の LDAP 設定を保存できます。各設定には一意の名前が必要です。
- 管理者は最大 32 個のユーザー定義グループを作成し、各固有の LDAP 構成に適用できます。
- 外部サーバーに頼るあらゆる形態の認証と同様に、停電によってプリンタが認証サーバーと通信できない場合には、ユーザーは保護されたデバイス機能にアクセスできません。
- 不正アクセスを防止するために、プリンタコントロールパネルで**[ログアウト]**を選択し、各セッションを安全に終了することをお勧めします。

新しい LDAP 設定を追加するには

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [詳細セキュリティセットアップ]の下で**[LDAP]**をクリックします。

3 **[LDAP 設定を追加]**をクリックします。

[LDAP サーバー設定]ダイアログには 4 つの部分があります。

一般情報

- **セットアップ名**—セキュリティテンプレートの作成時には、この名前を使用して、各特定の LDAP サーバー設定が識別されます。
- **サーバーアドレス**—認証が実行される LDAP サーバーの IP アドレスまたはホスト名を入力します。
- **サーバーポート**—内蔵 Web サーバーは、このポートを使用して、LDAP サーバーと通信します。デフォルトの LDAP ポートは 389 です。
- **SSL/TLS を使用**—ドロップダウンメニューから、**[なし]**、**[SSL/TLS]**(Secure Sockets Layer/Transport Layer Security)、または**[TLS]**を選択します。
- **ユーザー ID 属性**—`cn`(共通名)、`uid`、`userid`、または**ユーザー定義**を入力します。
- **メール属性**—48 文字以下で、一意の電子メールアドレスを入力します。デフォルト値は「mail」です。
- **フルモード属性**—48 文字以下で入力します。デフォルト値は「cn」です。
- **検索ベース**—ユーザーアカウントがある LDAP サーバーのノードです。複数の検索ベースは、カンマで区切って入力できます。

  メモ: 検索ベースには、カンマで区切られた複数の属性があります。たとえば、cn(共通名)、ou(組織単位)、o(組織)、c(国)、dc(ドメイン)などがあります。
- **検索タイムアウト**—プリンタの機種に応じて、5 ～ 30 秒または 5 ～ 300 秒の値を入力します。
- **ユーザー入力が必要**—**[ユーザー ID とパスワード]**または**[ユーザー ID]**を選択し、LDAP ビルディングブロックによって保護されている機能へのアクセスを試行するときに、ユーザーが入力する必要がある認証資格情報を指定します。**[ユーザー ID とパスワード]**がデフォルト設定です。

デバイス認証資格情報

- **Active Directory デバイス資格証明書を使用**—選択すると、ユーザー認証資格情報とグループ指定を、他のネットワークサービスに対応する既存のネットワークから取得できます。
- **匿名 LDAP バインド**—選択すると、内蔵 Web サーバーが LDAP サーバーと匿名でバインドされ、[識別名]と[MFP パスワード]フィールドが使用できなくなります。
- **識別名**—プリントサーバーの識別名を入力します。
- **MFP パスワード**—プリントサーバーのパスワードを入力します。

特定のオブジェクトクラスを検索する

- **person**—選択すると、「個人」オブジェクトクラスも検索されます。
- **カスタムオブジェクトクラス**—選択すると、このカスタム検索オブジェクトクラスも検索されます。管理者は最大 3 つのカスタム検索オブジェクトクラスを定義できます（任意）。

LDAP グループ名

- 管理者は、LDAP サーバーに保存されている 32 個の名前付きグループを関連付けることができます。[グループ検索ベース]リストの下で、グループの ID を入力します。**[グループの短い名前]**と**[グループ ID]**の両方を指定する必要があります。
- セキュリティテンプレートを作成すると、管理者はこの設定からグループを選択し、デバイス機能へのアクセスを制御できます。

4 **[送信]**をクリックして変更を保存するか、**[キャンセル]**をクリックして前の値に戻ります。

既存の LDAP 設定を編集するには

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [詳細セキュリティセットアップ]の下で**[LDAP]**をクリックします。

3 リストから設定をクリックします。

4 [LDAP 構成設定]ダイアログで必要な変更を行います。

5 **[変更]**をクリックして変更を保存するか、**[キャンセル]**をクリックして前の値に戻ります。

既存の LDAP 設定を削除するには

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [詳細セキュリティセットアップ]の下で**[LDAP]**をクリックします。

3 リストから設定を選択します。

4 **[エントリを削除]**をクリックしてプロファイルを削除するか、**[キャンセル]**をクリックして前の値に戻ります。

メモ:

- **[リストを削除]**をクリックすると、リストのすべての LDAP 設定が削除されます。
- LDAP ビルディングブロックがセキュリティテンプレートの一部として使用されている場合は、削除できません。

既存の LDAP 設定を検証するには

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [詳細セキュリティセットアップ]の下で**[LDAP]**をクリックします。

3 テストする設定の横の**[LDAP 認証設定のテスト]**をクリックします。

LDAP+GSSAPI を使用する

メモ: プリンタ機種によりこの機能が無いものもあります。

管理者によっては、簡易 LDAP 認証ではなく、送信が常に保護されている Generic Security Services Application Programming Interface (GSSAPI) を使用して、LDAP サーバーで認証することがあります。ユーザーは LADP サーバーで直接認証するのではなく、まず、Kerberos で認証し、Kerberos チケットを取得します。次に、このチケットが、GSSAPI プロトコル経由で LDAP サーバーに送信され、アクセスを確認します。一般的に、LDAP+GSSAPI は、Active Directory を実行するネットワークで使用されます。

メモ:

- LDAP+GSSAPI では、Kerberos 5 も設定する必要があります。
- サポートされているデバイスには、最大 5 個の一意の LDAP+GSSAPI 設定を保存できます。各設定には一意の名前が必要です。
- 外部サーバーに頼るあらゆる形態の認証と同様に、停電によってプリンタが認証サーバーと通信できない場合には、ユーザーは保護されたデバイス機能にアクセスできません。
- 不正アクセスを防止するために、プリンタコントロールパネルで**[ログアウト]**を選択し、各セッションを安全に終了することをお勧めします。

新しい LDAP+GSSAPI 設定を追加するには

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティ設定]**をクリックします。

2 [詳細セキュリティ設定]の下で**[LDAP+GSSAPI]**をクリックします。

3 **[LDAP+GSSAPI 設定を追加]**をクリックします。設定ダイアログには 4 つの部分があります。

一般情報

- **セットアップ名**—セキュリティテンプレートの作成時には、この名前を使用して、各特定の LDAP+GSSAPI サーバー設定が識別されます。
- **サーバーアドレス**—認証が実行される LDAP サーバーの IP アドレスまたはホスト名を入力します。
- **サーバーポート**—内蔵 Web サーバーが LDAP サーバーと通信するときに使用するポートです。デフォルトの LDAP ポートは 389 です。
- **SSL/TLS を使用**—ドロップダウンメニューから、**[なし]**、**[SSL/TLS]**(Secure Sockets Layer/Transport Layer Security)、または**[TLS]**を選択します。
- **ユーザー ID 属性**—`cn`(共通名)、`uid`、`userid`、または**ユーザー定義**を入力します。
- **メール属性**—48 文字以下で、一意の電子メールアドレスを入力します。デフォルト値は「mail」です。
- **フルモード属性**—48 文字以下で入力します。
- **検索ベース**—ユーザーアカウントがある LDAP サーバーのノードです。複数の検索ベースは、カンマで区切って入力できます。

  メモ: 検索ベースには、カンマで区切られた複数の属性があります。たとえば、cn(共通名)、ou(組織単位)、o(組織)、c(国)、dc(ドメイン)などがあります。
- **検索タイムアウト**—プリンタの機種に応じて、5 ～ 30 秒または 5 ～ 300 秒の値を入力します。
- **Kerberos サービスチケットを使用する**—選択した場合、Kerberos チケットが、GSSAPI プロトコル経由で LDAP サーバーに送信され、アクセスを取得します。

デバイス認証資格情報

- **Active Directory デバイス資格証明書を使用**—選択すると、ユーザー認証資格情報とグループ指定を、他のネットワークサービスに対応する既存のネットワークから取得できます。
- **MFP Kerberos ユーザー名**—プリントサーバーの識別名を入力します。
- **MFP パスワード**—プリントサーバーの Kerberos パスワードを入力します。

特定のオブジェクトクラスを検索する

- **person**—選択すると、「個人」オブジェクトクラスも検索されます。
- **カスタムオブジェクトクラス**—選択すると、このカスタム検索オブジェクトクラスも検索されます。管理者は最大 3 つのカスタム検索オブジェクトクラスを定義できます（任意）。

LDAP グループ名

- 管理者は、LDAP サーバーに保存されている 32 個の名前付きグループを関連付けることができます。[グループ検索ベース]リストの下で、グループの ID を入力します。**[グループの短い名前]**と**[グループ ID]**の両方を指定する必要があります。
- セキュリティテンプレートを作成すると、管理者はこの設定からグループを選択し、デバイス機能へのアクセスを制御できます。

4 **[送信]**をクリックして変更を保存するか、**[キャンセル]**をクリックして前の値に戻ります。

既存の LDAP+GSSAPI 設定を編集するには

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティ設定]**をクリックします。

2 [詳細セキュリティ設定]の下で**[LDAP+GSSAPI]**をクリックします。

3 リストから設定を選択します。

4 [LDAP 構成設定]ダイアログで必要な変更を行います。

5 **[変更]**をクリックして変更を保存するか、**[キャンセル]**をクリックして前の値に戻ります。

既存の LDAP+GSSAPI 設定を削除するには

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティ設定]**をクリックします。

2 [詳細セキュリティ設定]の下で**[LDAP+GSSAPI]**をクリックします。

3 リストから設定を選択します。

4 **[エントリを削除]**をクリックしてプロファイルを削除するか、**[キャンセル]**をクリックして前の値に戻ります。

メモ:

- **[リストを削除]**をクリックすると、リストのすべての LDAP+GSSAPI 設定が削除されます。
- LDAP+GSSAPI ビルディングブロックがセキュリティテンプレートの一部として使用されている場合は、削除できません。

LDAP+GSSAPI で使用するために Kerberos 5 を設定する

メモ: プリンタ機種によりこの機能が無いものもあります。

Kerberos 5 はユーザー認証目的で単独で使用できますが、多くの場合、LDAP+GSSAPI ビルディングブロックと合わせて使用されます。サポート対象のデバイスに保存できる Kerberos 構成ファイル（krb5.conf）は 1 つだけですが、krb5.conf ファイルは複数のレルムと Kerberos ドメインコントローラ（KDC）に適用できます。管理者は、さまざまなタイプの認証要求が Kerberos サーバーで受信される可能性があることを想定し、このようなすべての要求を処理できるように krb5.conf ファイルを設定する必要があります。

メモ:

- 使用される krb5.conf ファイルは 1 つだけであるため、簡易 Kerberos ファイルのアップロードまたは再送信を行うと、構成ファイルが上書きされます。

- krb5.conf ファイルにはデフォルトレルムを指定できます。ただし、構成ファイルでレルムが指定されていない場合は、指定された最初のレルムが認証用のデフォルトレルムとして使用されます。
- 外部サーバーに頼るあらゆる形態の認証と同様に、停電によってプリンタが認証サーバーと通信できない場合には、ユーザーは保護されたデバイス機能にアクセスできません。
- 不正アクセスを防止するために、プリンタコントロールパネルで**[ログアウト]**を選択し、各セッションを安全に終了することをお勧めします。

簡易 Kerberos 構成ファイルを作成する

1 内蔵 Web サーバーで、**[設定]** >**[セキュリティ]** >**[セキュリティ設定]**をクリックします。

2 [詳細セキュリティ設定]の下で**[Kerberos 5]**をクリックします。

3 [KDC アドレス]フィールドに、KDC(鍵配布センター)のアドレスまたはホスト名を入力します。

4 [KDC ポート]フィールドに、Kerberos サーバーで使用されるポートの番号(1 ～ 88)を入力します。

5 [レルム]フィールドに、Kerberos サーバーで使用されるレルム(またはドメイン)を入力します。

6 **[送信]**をクリックすると、この情報が krb5.conf ファイルとして選択したデバイスに保存されます。**[フォームのリセット]**をクリックすると、フィールドがリセットされ、再開されます。

Kerberos 構成ファイルをアップロードする

1 内蔵 Web サーバー(EWS)で、**[設定]** > **[セキュリティ]** > **[セキュリティ設定]**をクリックします。

2 [詳細セキュリティ設定]の下で**[Kerberos 5]**をクリックします。

3 **[参照]**をクリックし、krb5.conf ファイルをクリックします。

4 **[送信]**をクリックし、krb5.conf ファイルを選択したデバイスにアップロードします。

内蔵 Web サーバーは krb5.conf ファイルを自動的にテストし、機能していることを検証します。

メモ:

- **[フォームのリセット]**をクリックし、フィールドをリセットし、新しい構成ファイルを検索します。
- **[ファイルの削除]**をクリックし、Kerberos 構成ファイルを選択したデバイスから削除します。
- **[ファイルの表示]**をクリックし、選択したデバイスの Kerberos 構成ファイルを表示します。
- **[設定のテスト]**をクリックし、選択したデバイスの Kerberos 構成ファイルが機能していることを検証します。

日時を設定する

Kerberos サーバーでは、鍵要求で最近のタイムスタンプ(通常は 300 秒以内)が必要なため、プリンタ時刻が同期しているか、KDC システム時刻とほとんど一致している必要があります。プリンタ時刻設定は手動で更新するか、ネットワークタイムプロトコル(NTP)を使用するように設定し、信頼できる時計(通常は Kerberos サーバーで使用される時計)と自動的に同期できます。

1 内蔵 Web サーバーで、**[設定]** >**[セキュリティ]** >**[日付と時間を設定]**をクリックします。

2 設定を手動で管理するには、正しい日時を **YYYY-MM-DD HH:MM** 形式で入力し、ドロップダウンメニューからタイムゾーンを選択します。

メモ:

- 手動設定を入力すると、NTP の使用が自動的に無効になります。
- [タイムゾーン]リストから**[(UTC+ユーザー)カスタム]**を選択した場合、[カスタムタイムゾーン設定]の下でその他の設定を構成する必要があります。

3 地域で夏時間(DST)が採用されている場合、**[DST を自動的に適用]**チェックボックスをオンにします。

4 非標準のタイムゾーンまたは代替 DST カレンダーが適用されない地域の場合は、必要に応じて[カスタムタイムゾーン設定]を調整します。

5 日時を手動で管理せずに、NTP サーバーと同期するには、**[NTP の有効化]**チェックボックスをオンにし、NTP サーバーの IP アドレスまたはホスト名を入力します。

6 NTP サーバーが認証を要求する場合は、[認証]メニューから指定した方法を選択し、**[MD5 鍵のインストール]**リンクまたは**[自動鍵 IFF パラメータのインストール]**リンクをクリックし、一致する NTP 認証を含むファイルを参照します。

7 **[送信]**をクリックして変更を保存するか、**[フォームのリセット]**をクリックしてデフォルト設定を復元します。

CA Cert モニタを設定する

メモ: プリンタ機種によりこの機能が無いものもあります。

Active Directory 環境に参加すると、CA(認証機関)証明書の自動更新が必要です。Cert モニタが有効な場合、この機能が実行されます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[証明書管理]** > **[CA Cert モニタ設定]**をクリックします。

2 [CA 監視を有効にする]チェックボックスをオンにします。

3 デバイスが新しい CA 証明書を確認するスケジュール時刻を選択し、繰り返し間隔を選択します。

4 **[送信]**をクリックして、変更を保存します。

CA 証明書をただちにダウンロードする

メモ: プリンタ機種によりこの機能が無いものもあります。

Active Directory 登録プロセスでは、ドメインコントローラの証明機関(CA)証明書チェーンを自動的にダウンロードします。ただし、これは即時実行されません。CA 証明書の自動ダウンロードのデフォルト設定は、デバイスで指定されたタイムゾーンの午前 12:00 です。

CA 証明書をただちにダウンロードする

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[証明書管理]** > **[CA 証明書監視設定]**をクリックします。

2 [CA モニタを有効化]チェックボックスをオンにします。

3 [ただちに取得する]チェックボックスをオンにし、デバイス管理者がスケジュール済みの時間を無効にし、CA 証明書チェーンをただちにインストールできるようにします。

4 **[送信]**をクリックします。

メモ: Web ページが更新され、[証明書管理]ページに戻ります。

5 **[証明機関管理]**をクリックし、CA 証明書チェーンが正しくダウンロードされたことを確認します。

メモ: CA 証明書をより広範囲に確認する場合は、[証明機関共通名]セクションの下に表示される CA 証明書名をクリックします。

アクセスを保護する

バックアップパスワードを作成する

メモ: プリンタ機種によりこの機能が無いものもあります。

バックアップパスワードを使用すると、割り当てられたセキュリティのタイプに関係なく、内蔵 Web サーバー管理者がセキュリティメニューにアクセスできます。また、ネットワーク通信の問題がある場合や認証サーバーで障害が発生した場合など、他のセキュリティ方法が使用できない場合にも有効です。

メモ: 一部の企業では、セキュリティポリシーによって、バックアップパスワードなどの「バックドア」方法の使用が禁止されています。ポリシーを侵害する可能性のあるセキュリティ方式を展開する前に、企業のポリシーを確認してください。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [追加セキュリティセットアップ]の下で**[バックアップパスワード]**をクリックします。

3 **[バックアップパスワードを使用]**チェックボックスをオンにし、パスワードを入力して再入力します。

4 **[送信]**をクリックします。

ログイン制限を設定する

メモ: プリンタ機種によりこの機能が無いものもあります。

ほとんどの企業では、ワークステーションやサーバーなどの情報資産に対するログイン制限が設定されています。内蔵 Web サーバー管理者は、プリンタのログイン制限が企業のセキュリティポリシーに準拠していることも確認してください。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[その他のセキュリティ設定]** > **[ログイン制限]**をクリックします。

2 適切なログイン制限を入力します。
- **ログインエラー**—ユーザーがロックアウトされる前にログイン失敗できる上限回数を指定します。
- **エラー時間枠**—ユーザーがロックアウトされるまでの時間を指定します
- **ロックアウト時間**—ロックアウト時間を指定します。
- **パネルログインタイムアウト**—自動ログオフの前に、ユーザーがログインできる時間を指定します。
- **リモートログインタイムアウト**—自動ログオフの前に、ユーザーがリモートログインできる時間を指定します。

3 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてデフォルト設定を復元します。

セキュリティテンプレートを使用して機能アクセスを制御する

メモ: プリンタ機種によりこの機能が無いものもあります。

各アクセス制御または機能アクセス制御は、セキュリティを要求しない（デフォルト）ように設定するか、その機能のドロップダウンメニューで使用可能なビルディングブロック選択項目のいずれかを使用するように設定できます。各アクセス制御に割り当てられるセキュリティ方式は 1 つだけです。

手順 1:ビルディングブロックを作成する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 [詳細セキュリティセットアップ]の下の手順 1 から、環境に該当するビルディングブロック(またはブロック)をクリックして設定します。

特定のタイプのビルディングブロックの設定の詳細については、8 ページの「ビルディングブロックを編集」の該当セクションを参照してください。

手順 2:セキュリティテンプレートを作成する

1 つまたは 2 のビルディングブロックを最大 128 文字の一意の名前と組み合わせ、セキュリティテンプレートを作成できます。各デバイスは最大 140 個のセキュリティテンプレートをサポートできます。セキュリティテンプレートの名前は一意でなければなりませんが、ビルディングブロックとセキュリティテンプレートを同じ名前にすることはできます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 手順 2 から、[詳細セキュリティセットアップ]の下で**[セキュリティテンプレート]**をクリックします。

3 [セキュリティテンプレートの管理]の下で**[セキュリティテンプレートの追加]**をクリックします。

4 [セキュリティテンプレート名]フィールドで、128 文字以下の一意の名前を入力します。「Administrator_Only」や「Common_Functions_Template」などのわかりやすい名前を指定すると便利です。

5 [認証設定]リストから、ユーザーの認証方式を選択します。

メモ: [認証設定]リストには、デバイスで設定された認証ビルディングブロックが入力されます。

6 権限を使用するには、**[権限の追加]**をクリックしてから、[権限設定]リストでビルディングブロックをクリックします。

メモ: [権限設定]リストには、デバイスで使用可能な権限ビルディングブロックが入力されます。

7 グループを使用するには、**[グループの変更]**をクリックし、セキュリティテンプレートに含める 1 つ以上のグループをクリックします。

メモ: **Ctrl** キーを押すと、複数のグループを選択できます。

8 **[テンプレートの保存]**をクリックします。

メモ:

- 特定のビルディングブロック(パスワードと PIN など)は、個別の権限をサポートしません。
- 個別のユーザーが認証されない簡易権限レベルのセキュリティでは、管理者がパスワードまたは PIN だけをセキュリティテンプレートに割り当て、特定のデバイス機能へのアクセスを制御します。パスワードまたは PIN で制御された機能にアクセスするには、正しいコードを入力する必要があります。

手順 3:セキュリティテンプレートをアクセス制御に割り当てる

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 手順 3 から、[詳細セキュリティセットアップ]の下で**[アクセス制御]**をクリックします。

3 機能名の横にあるドロップダウンメニューから、保護する機能ごとに、セキュリティテンプレートを選択します。

4 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてすべての変更をキャンセルします。

セキュリティテンプレートで制御された機能にアクセスするには、適切な認証資格情報を入力する必要があります。

メモ:

- 不正アクセスを防止するために、プリンタコントロールパネルで**[ログアウト]**を選択し、各セッションを安全に終了することをお勧めします。

- 個別のアクセス制御の一覧と説明については、42 ページの「付録 D:アクセス制御」を参照してください。

既存のセキュリティテンプレートを編集または削除する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 手順 2 から、[詳細セキュリティセットアップ]の下で**[セキュリティテンプレート]**をクリックします。

3 リストからセキュリティテンプレートを選択します。

4 必要に応じてフィールドを編集します。

5 **[変更]**をクリックして、変更を保存します。

メモ:

- **[キャンセル]**をクリックすると、前の設定値が保持されます。
- **[エントリを削除]**をクリックすると、選択したセキュリティテンプレートが削除されます。
- [セキュリティテンプレートの管理]画面で**[リストを削除]**をクリックすると、デバイスのすべてのセキュリティテンプレートが削除されます。
- 未使用のセキュリティテンプレートだけを削除できます。ただし、使用中のセキュリティテンプレートを編集することはできます。

証明書とその他の設定を管理する

メモ: プリンタ機種によりこの機能が無いものもあります。

[証明書管理]メニューは、SSL、PSec、および 802.1X 接続の証明書を利用するようにプリンタを設定できます。また、MFP は SSL 認証とアドレス帳検索で、LDA の証明書を使用します。

デバイスを構成する手順には、次の作業があります。

- CA(認証機関)の証明書をデバイスに読み込む
- デバイスの証明書を作成するか、デバイスのデフォルトの証明書を使用する
- デバイスの証明書データを使用して、CA が署名した証明書を作成する
- CA が署名した証明書をデバイスに読み込む

メモ: このプロセスを大幅に簡素化するには、新しい自動証明書登録アプリケーションを使用します。これは、Active Directory 登録の使用中に実行できます。このアプリケーションの使用方法の詳細については、41 ページの「付録 C:自動証明書登録アプリケーション」を参照してください。

証明機関の証明書をデバイスにインストールする

メモ: この機能は、ネットワークプリンタまたはプリントサーバーに接続されたプリンタでだけ使用できます。

プリンタがネットワーク上の他のシステムの認証資格情報を信頼して確認できるように、証明機関(CA)が必要です。CA 証明書がない場合、プリンタには、安全な接続を確立しようとしているシステムによって提供された証明書を信頼するかどうかを判断する手段がありません。

使用される CA の証明書ファイル(.pem 形式)から始めます。このファイルを作成する方法の例については、41 ページの「付録 A:CA ファイルの作成」を参照してください。

1 Web ブラウザを開き、プリンタの IP アドレスまたはホスト名を入力します。

2 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[証明書管理]** > **[証明機関管理]**をクリックします。

メモ:

- このウィンドウでは、デバイス管理者が新しい CA 証明書の要求を開始し、すべての CA 証明書を削除し、以前にインストールされた CA 証明書を表示できます。インストールされた CA 証明書の詳細を表示したり、特定の CA 証明書を削除したりするには、[証明機関共通名]見出しの下に一覧表示される証明書共通名リンクをクリックします。
- 新しい、特別な構成が行われていないデバイスの場合、このページにはインストール済みの CA 証明書は表示されません。

3 **[新規]**をクリックすると、[証明機関インストール]画面が表示されます。

4 **[参照]**をクリックし、.pem 形式の証明機関ファイルを選択して、**[送信]**を選択します。これで、CA 証明書のインストール処理が完了です。

デバイスの証明書情報を設定する

メモ: プリンタ機種によりこの機能が無いものもあります。

プリンタには自己生成証明書があります。一部の処理(802.1x、IPSec など)では、プリンタ証明書を、認証機関が署名した証明書にアップグレードする必要があります。

プリンタには証明書署名要求があり、表示またはダウンロードできます。これによって、プリンタの署名付き証明書を取得するプロセスが大幅に容易になります。

1 Web ブラウザを開き、プリンタの IP アドレスまたはホスト名を入力します。

2 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[証明書管理]** > **[証明書標準設定を設定]**をクリックします。

メモ: [証明書標準設定を設定]メニューでは、組織の証明書要件に適合した内容の情報で、デバイスの未構成の情報を更新できます。

3 組織に適合するすべてのフィールドを更新したら、**[送信]**をクリックします。詳細については、25 ページの「証明書のデフォルトを設定する」 を参照してください。

メモ: Web ページが更新され、[証明書管理]ページに戻ります。

4 **[デバイス証明書管理]**リンクをクリックします。

メモ:

- このウィンドウでは、デバイス管理者が新しいデバイス証明書の要求を開始し、すべてのデバイス証明書を削除し、以前にインストールされたデバイス証明書を表示できます。インストールされたデバイス証明書の詳細を表示したり、特定のデバイス証明書を削除したりするには、[フレンドリ名]見出しの下に一覧表示される証明書共通名リンクをクリックします。
- 新しい、特別な構成が行われていないデバイスの場合、このページにはデフォルトの自己署名証明書が表示されます。

5 目的のデバイス証明書のリンクを選択し、証明書署名要求情報を取得します。

メモ:

- デフォルトの証明書リンクを使用すると、手順 2 または他の名前の証明書で作成されたデフォルト証明書を使用できます。証明書情報が表示されます。
- 他の証明書を作成するには**[新規]**を選択します。[証明書生成パラメータ]ページが開きます。詳細については、24 ページの「新しい証明書を作成する」 を参照してください。

6 **[署名要求をダウンロード]**をクリックし、.csr ファイルを保存して、メモ帳などのテキストエディタで開きます。

メモ: ファイルデータは標準形式で表示され、アプリケーションウィンドウには base-64 表示が含まれます。情報をハイライト表示してコピーします。後から貼り付け操作で使用します。

7 現在の内蔵 Web サーバーページを開いたままにして、新しい Web ブラウザで認証機関の Web サイトを開きます。

8 認証機関で定義されている CA 証明書要求プロセスに従います。サンプル要求は、41 ページの「付録 B:CA が署名したデバイス証明書の作成」を参照してください。

メモ: このプロセスを実行すると、新しい CA 署名付きデバイス証明書ファイル(.pem 形式)が作成されます。このファイルは次の手順で必要なため、コンピュータに保存します。

9 内蔵 Web サーバーから、「デフォルト」の[デバイス証明書管理]ページに戻り、**[署名済み証明書をインストール]**をクリックします。

10 **[参照]**をクリックし、手順 8 で作成された CA 署名付きデバイス証明書ファイルを選択します。

11 **[送信]**をクリックします。

メモ: これで、署名されたプリンタ証明書の作成とインストールが完了です。SSL または IPSec 接続のネゴシエートを使用するときに、相手のシステムに対して有効な証明書を提供できるようになります。

新しい証明書を作成する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[証明書管理]**をクリックします。

2 **[デバイス証明書管理]** > **[新規]**をクリックします。

3 該当するフィールドに値を入力します。

- **フレンドリ名**—証明書の名前を入力します(最大 64 文字)。
- **共通名**—デバイスの名前を入力します(最大 128 文字)。

  メモ: このフィールドを空白にすると、デバイスのホスト名が使用されます。
- **組織名**—証明書を発行する会社または組織の名前を入力します(最大 128 文字)。
- **部署名**—証明書を発行する会社または組織内の単位の名前を入力します(最大 128 文字)。
- **国/地域**—証明書を発行する会社または組織が所在する国または地域を入力します(最大 2 文字)。
- **都道府県**—証明書を発行する会社または組織が所在する都道府県名を入力します(最大 128 文字)。
- **市区町村**—証明書を発行する会社または組織が所在する市区町村名を入力します(最大 128 文字)。
- **主題代替名**—RFC 2459 に準拠した代替名とプレフィックスを入力します。たとえば、`IP:1.2.3.4` の形式で IP アドレスを入力するか、`DNS:ldap.company.com` の形式で DNS アドレスを入力します。このフィールドを空白にすると、IPv4 アドレスが使用されます(最大 128 文字)。

4 **[新しい証明書を生成]**をクリックします。

証明書を表示、ダウンロード、および削除する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[証明書管理]** > **[デバイス証明書管理]**をクリックします。

2 リストから証明書を選択します。

証明書の詳細は、[デバイス証明書管理]ウィンドウに表示されます。

3 次のいずれかをクリックします。
- **削除**—以前に保存された証明書を削除します。
- **ファイルにダウンロード**—.pem ファイルとして証明書をダウンロードまたは保存します。
- **署名要求をダウンロード**—.csr ファイルとして署名要求をダウンロードまたは保存します。
- **署名済み証明書をインストール**—以前に署名された証明書をアップロードします。

証明書のデフォルトを設定する

管理者は、サポート対象のデバイスに対して生成された証明書のデフォルト値を設定できます。ここで入力する値は、このフィールドが画面上で空白の場合でも、[証明書管理]タスクで生成されるすべての証明書で表示されます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[証明書管理]** > **[証明書標準設定を設定]**をクリックします。

2 該当するフィールドに値を入力します。
- **共通名**—デバイスの名前を入力します(最大 128 文字)。

  メモ: このフィールドを空白にすると、デバイスのドメイン名が使用されます。
- **組織名**—証明書を発行する会社または組織の名前を入力します。
- **部署名**—証明書を発行する会社または組織内の単位の名前を入力します。
- **国/地域**—証明書を発行する会社または組織が所在する国または地域を入力します(最大 2 文字)。
- **都道府県**—証明書を発行する会社または組織が所在する都道府県名を入力します。
- **市区町村**—証明書を発行する会社または組織が所在する市区町村名を入力します。
- **主題代替名**—RFC 2459 に準拠した代替名とプレフィックスを入力します。たとえば、`IP:1.2.3.4` の形式で IP アドレスを入力するか、`DNS:ldap.company.com` の形式で DNS アドレスを入力します。このフィールドを空白にすると、IPv4 アドレスが使用されます。

  メモ: 明記されていない場合は、すべてのフィールドに最大 128 文字入力できます。

3 **[送信]**をクリックします。

コンフィデンシャル印刷を設定する

機密情報や重要情報を印刷するユーザーは、コンフィデンシャル印刷オプションを選択できます。このオプションを使用すると、印刷ジョブが PIN で保護されるため、プリンタコントロールパネルで PIN を入力するまで、印刷ジョブが印刷キューに留まります。

1 内蔵 Web サーバーで、**[設定]** >**[セキュリティ]** >**[コンフィデンシャル印刷設定]**をクリックします。

2 次のオプションを入力します。

使用	目的
無効暗証番号許容回数 オフ 2 ～ 10	無効な暗証番号(PIN)を入力できる最大回数を制限します。 **メモ:** • このメニュー項目は、正常に動作するフォーマット済みのハードディスクがプリンタに実装されているときのみ表示されます。 • 0 を入力すると、ユーザーは間違った PIN を何度でも入力できます。 • 2 ～ 10 の値を入力し、ロックアウトされるまでにユーザーが間違った PIN を入力できる回数を指定します。 • この上限回数に達すると、該当するユーザー名と暗証番号(PIN)に対する印刷ジョブが削除されます。
コンフィデンシャル印刷ジョブの有効期限 オフ 1 時間 4 時間 24 時間 1 週間	コンフィデンシャル印刷ジョブがプリンタに保存される期間を制限します。 **メモ:** • コンフィデンシャル印刷ジョブがプリンタのメモリまたはハードディスクにあるときに有効期限の設定が変更された場合、それらの印刷ジョブの有効期限は新しい設定値に変更されません。 • プリンタの電源がオフになると、プリンタのメモリにあったコンフィデンシャル印刷ジョブはすべて削除されます。
ジョブ期限切れの繰り返し オフ 1 時間 4 時間 24 時間 1 週間	印刷ジョブがプリンタに保存される期間を制限します。
ジョブ期限切れの確認 オフ 1 時間 4 時間 24 時間 1 週間	ベリファイ(確認)が必要な印刷ジョブがプリンタに保存される期間を制限します。
予約印刷ジョブの有効期限 オフ 1 時間 4 時間 24 時間 1 週間	後で印刷する予約印刷ジョブがプリンタに保存される期間を制限します。
メモ: 工場出荷時は[オフ]に設定されています。	

3 **[送信]**をクリックして変更を保存するか、**[フォームのリセット]**をクリックしてデフォルト設定を復元します。

USB デバイスを有効/無効にする

メモ: プリンタ機種によりこの機能が無いものもあります。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[USB デバイスをスケジュール]**をクリックします。

2 [デバイスの無効化]メニューで選択すると、USB デバイスまたはフラッシュドライブからだけ印刷が無効になります。

メモ: すべてのスケジュール済みの「無効」アクションは、この設定の影響を受けません。

3 **[送信]**をクリックします。

4 特定の日数または特定の時間に、USB デバイスの使用を有効または無効にします。スケジュールを作成するには、次の手順を実行します。

a [アクション]メニューで、**[有効化]**または**[無効化]**を選択し、指定した時刻に発生するアクションを指定します。

b [時間]メニューで、選択したアクションが開始される時間を選択します(例:午前 6:00 に開始するには「06:00」)。

c [曜日]メニューで、スケジュールが実行される曜日を選択します(例:「平日(月～金)」)。

d **[追加]**をクリックし、アクションをスケジュールに保存します。

メモ:

- デフォルトでは、USB デバイスの使用が有効です。
- USB デバイスの使用を再度有効にする場合には、各「無効」スケジュールエントリの「有効」スケジュールエントリも作成する必要があります。

一時データファイルをハードディスクから消去する

特定のデバイスでは、管理者が[一時データファイルの消去]を使用して、残っている機密資料をデバイスから削除し、メモリ領域を解放できます。この設定では、ランダムデータパターンを使用し、ハードドライブに保存され、削除設定されたファイルを安全に上書きします。簡易ワイプの場合、シングルパスで上書きできます。セキュリティを強化する場合は、マルチパスを使用できます。マルチパスワイプは、米国国防省の 5220.22-M 規格に準拠しており、ハードディスクからデータを確実に消去することができます。

メモ: すべてのプリンタにハードディスクが搭載されているわけではありません。メインの[セキュリティ]メニューに[一時データファイルの消去]が表示されない場合は、デバイスでサポートされていません。

1 内蔵 Web サーバーで、**[設定]** >**[セキュリティ]** >**[一時データファイルの消去]**をクリックします。

メモ: 設定できるワイプモードは**[自動]**だけです。

2 次の設定を変更します。

- **シングルパス**– プリンタのハードディスクを繰り返しビットパターンのシングルパスで上書きします。これは工場出荷時の設定です。
- **マルチパス** – プリンタをランダムなビットパターンで複数回上書きしてから、検証パスを実行します。セキュアな上書きは、米国国防省の 5220.22M 規格に準拠しており、ハードディスクからデータを確実に消去することができます。機密性の高い情報は、この方法で消去する必要があります。

3 **[送信]**をクリックして、変更を保存します。

セキュリティ監査ログ設定を構成する

メモ: プリンタ機種によりこの機能が無いものもあります。

セキュリティ監査ログを使用すると、管理者は、ユーザー権限失敗、管理者認証の成功、デバイスへの Kerberos ファイルのアップロードなど、デバイスのセキュリティ関連イベントを監視できます。デフォルトでは、セキュリティログはデバイスに保存されますが、ネットワーク syslog サーバーに送信し、処理または保存できます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティ監査ログ]**をクリックします。

2 **[監査を有効化]**を選択すると、セキュリティ監査ロギング（syslog）が有効になります。

3 リモート Syslog サーバーの IP アドレスまたはホスト名を入力し、**[リモート Syslog 有効化]** チェックボックスをオンにして、ログイベントをネットワーク syslog サーバーに送信します。

メモ: [リモート Syslog 有効化] チェックボックスは、IP アドレスまたはホスト名が入力されるまで使用できません。

4 宛先サーバーで使用されるリモート Syslog ポート番号を入力します。デフォルト値は 514 です。

5 [リモート Syslog 方式]メニューから、次のいずれかを選択します。
- 標準 UDP—低優先度の転送プロトコルを使用して、ログメッセージとイベントを送信します。
- Stunnel—宛先サーバーに実装されている場合。

6 [リモート Syslog 機能]メニューで、宛先サーバーでログインするためのイベントの機能コードを選択します。デバイスから送信されるすべてのイベントは、同じ機能コードでタグ付けされるため、ネットワーク監視または侵入検出ソフトウェアでソートおよびフィルタリングできます。

メモ: 手順 4 ～ 6 は、リモート Syslog が有効な場合にだけ適用されます。

7 [ログ記録するイベントの重要度]メニューで、メッセージとイベントを記録するための優先度レベル条件（0 ～ 7）を選択します。

メモ: 最高重要度が 0、最低重要度が 7 です。選択した重要度レベル以上が記録されます。たとえば、**[レベル 4 - 警告]**が選択されると、重要度レベル 0 ～ 4 が記録されます。

8 **[ログ記録されていないイベントをリモート Syslog に書き込む]**を選択すると、重要度に関係なく、すべてのイベントがリモートサーバーに送信されます。

9 [管理者の E メールアドレス]フィールドに、特定のログイベントを管理者に自動的に通知するための 1 つ以上の E メールアドレス（カンマ区切り）を入力し、次のオプションを選択します。
- **E メール ログ消去アラート**—**[ログの削除]**ボタンをクリックすると表示されます。
- **E メール ログ ラップ アラート**—ログが満杯になり、最も古いエントリの上書きが開始されると表示されます。
- **ログフル時の動作**—次の 2 つのオプションのドロップリストです。
  - 最も古いエントリに上書き
  - ログを E メール送信し、全エントリを削除
- **E メール % フルアラート**—ログ保存領域が特定の容量の割合に達すると表示されます。
- **% フルアラートレベル（1 ～ 99%）**—アラートがトリガーされる前のログの満杯度を設定します。
- **E メール ログ エクスポート アラート**—ログファイルをエクスポートすると表示されます。
- **E メール ログ設定変更アラート**—ログ設定を変更すると表示されます。
- **ログ行終了**—ログファイルの各行の末尾の終了方法を設定します。ドロップダウンメニューから行末尾オプションを選択します。
- **エクスポートにデジタル署名**—エクスポートされた各ログファイルにデジタル署名を追加します。

メモ: E メールアラートを使用するには、**[送信]**をクリックして変更を保存し、**[E メールサーバーをセットアップ]**リンクに従って、SMTP 設定を構成します。

10 **[送信]**をクリックして変更を保存するか、**[フォームのリセット]**をクリックしてデフォルト設定を復元します。

E メールサーバー設定

1 [セキュリティ監査ログ]メイン画面で、**[E メールサーバーをセットアップ]**をクリックします。

2 [SMTP 設定]で、電子メールの送信でデバイスが使用する、プライマリ SMTP ゲートウェイの IP アドレスまたはホスト名を入力します。

3 宛先サーバーのプライマリ SMTP ゲートウェイポート番号を入力します。デフォルト値は 25 です。

4 セカンダリまたはバックアップ SMTP サーバーを使用している場合は、サーバーの IP アドレス/ホスト名と SMTP ポートを入力します。

5 SMTP タイムアウトには、タイムアウトする前に、デバイスが SMTP サーバーからの応答を待機する秒数(5 ～ 30 秒)を入力します。デフォルト値は 30 秒です。

6 失敗またはバウンスされたメッセージの場合に、プリンタから送信されるメッセージへの応答を受信するには、[返信アドレス]を入力します。

7 [SSL/TLS の使用]リストで、**[無効]**、**[交渉]**、または**[必須]**を選択し、暗号化されたリンクで E メールが送信されるかどうかを指定します。

8 SMTP でユーザー認証資格情報が必要な場合、[SMTP サーバー認証]リストから認証方式を選択します。デフォルト設定は、[認証不要]です。

9 [デバイスから送信される E メール]リストで、認証なしの場合は**[なし]**、認証が必要な場合は**[デバイス SMTP 証明書を使用]**を選択します。

10 [ユーザーから送信される E メール]リストで、認証なしの場合は**[なし]**、認証が必要な場合は**[デバイス SMTP 証明書を使用]**を選択します。

11 E メールを送信するためにデバイスが認証資格情報を提供する必要がある場合、[デバイス認証資格情報]の下で、ネットワークに該当する情報を入力します。

12 **[送信]**をクリックして変更を保存するか、**[フォームのリセット]**をクリックしてデフォルト設定を復元します。

セキュリティ監査ログを表示または削除する

- 現在の syslog のテキストファイルを表示または保存するには、**[ログのエクスポート]**をクリックします。
- 現在の syslog を削除するには、**[ログの削除]**をクリックします。

内蔵 Web サーバーを使用してワイヤレスネットワークにプリンタを接続する

カスタマイズを開始する前に、以下の点を確認してください。

- プリンタが一時的にイーサネットネットワークに接続されている。
- ワイヤレスネットワークアダプタがプリンタに取り付けられ、正しく動作している。詳細については、ワイヤレスネットワークアダプタに付属の説明書を参照してください。

1 Web ブラウザを開き、アドレスフィールドにプリンタの IP アドレスを入力します。

メモ:

- [ネットワーク/ポート]メニューの[TCP/IP]セクションでプリンタの IP アドレスを確認します。IP アドレスは、123.123.123.123 のようなピリオドで区切られた 4 つの数字の並びで表されます。

- プロキシサーバーを使用している場合は、Web ページを正しく読み込むために、プロキシサーバーを一時的に無効にしてください。

2 **[設定]** > **[ネットワーク/ポート]** > **[ワイヤレス]**の順にクリックします。

3 アクセスポイント(無線ルーター)の設定と一致するように設定を変更します。

メモ: 正しい SSID が入力されていることを確認してください。

4 **[送信]**をクリックします。

5 プリンタの電源を切り、イーサネットケーブルを取り外します。5 秒以上待ってから、再び電源を入れます。

6 プリンタがネットワークに接続されているかどうかを確認するには、ネットワーク設定ページを印刷します。「ネットワークカード [X]」セクションで、ステータスが「接続中」であるかどうかを確認します。

詳細については、『ユーザーズガイド』の「プリンタのセットアップを確認する」を参照してください。

802.1X 認証を設定する

メモ: プリンタ機種によりこの機能が無いものもあります。

一般的にはワイヤレスデバイスと接続に関連付けられますが、802.1X 認証は有線環境とワイヤレス環境の両方をサポートします。デバイスのワイヤレスが有効な場合、802.1X はワイヤレスメニューに表示されます。

次のネットワーク認証メカニズムは、802.1X プロトコルネゴシエーションに含めることができます。

- EAP-MD5
- EAP-TLS
- 次の方式の EAP-TTLS:
  - CHAP
  - MSCHAP
  - MSCHAPv2
  - PAP
- EAP_MSCHAPV2
- PEAP
- LEAP

EAP Type	MFP またはプリンタで必要
EAP-MD5	デバイスのログイン名とパスワード
EAP-TLS	デバイスのログイン名とパスワード、CA 証明書、署名付きのデバイス証明書
EAP-TTLS	デバイスのログイン名とパスワード、CA 証明書
PEAP (TLS)	デバイスのログイン名とパスワード、CA 証明書、署名付きのデバイス証明書
LEAP	デバイスのログイン名とパスワード

メモ: 802.1X プロセスに参加するすべてのデバイスが同じ EAP 認証タイプをサポートしていることを確認することが重要です。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[802.1x]**をクリックします。

2 [802.1x 認証]の下で次の手順を実行します。

a **[有効]**チェックボックスをオンにし、802.1X 認証を有効にします。

b 認証サーバーにログインするためにプリンタが使用するログイン名とパスワードを入力します。

c 認証サーバーでセキュリティ証明書の確認を要求するには、**[サーバー証明書の確認]**チェックボックスをオンにします。

メモ:

- デジタル証明書を使用して、認証サーバーへの安全な接続を確立する場合は、802.1X 認証設定を変更する前に、プリンタで設定する必要があります。デジタル証明書の設定の詳細については、22 ページの「証明書とその他の設定を管理する」を参照してください。
- TLS(Transport Layer Security)、PEAP(Protected Extensible Authentication Protocol)、および TTLS(Tunneled Transport Security Layer)では、サーバー証明書の確認が必須です。

d **[イベントログを有効化]**チェックボックスをオンにすると、802.1X 認証関連アクティビティが記録されます。

警告！破損の恐れあり: フラッシュ部品の摩耗を低減するには、必要なときにだけこの機能を使用します。

e [802.1X デバイス証明書]リストから、使用するデジタル証明書を選択します。1 つの証明書だけがインストールされている場合、**[デフォルト]**だけがリストに表示されます。

3 [使用可能な認証メカニズム]の下で、該当するプロトコルの横のチェックボックスをオンにし、プリンタが認識する認証プロトコルを選択します。

4 [TTLS 認証方式]リストから、認証サーバーとプリンタ間で作成された安全なトンネル経由で許可する認証方式を選択します。

5 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてデフォルト設定を復元します。

メモ: アスタリスク(*)が付いた設定を変更すると、プリントサーバーがリセットされます。

SNMP を設定する

SNMP(簡易ネットワーク管理プロトコル)は、ネットワークに接続されたデバイスで管理者の注意が必要な条件があるかどうかを監視するために、ネットワーク管理システムで使用されます。内蔵 Web サーバーでは、管理者は、SNMP バージョン 1 ～ 3 の設定を構成できます。

SNMP バージョン 1、2c

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[SNMP]**をクリックします。

2 [SNMP バージョン 1、2c]の下で、**[有効]**を選択します。

3 SNMP 変数を設定できるようにするには、**[SNMP セットを許可]**を選択します。

4 SNMP コミュニティ ID で使用される名前を入力します。デフォルトのコミュニティ名は「public」です。

5 デバイスドライバと他の印刷アプリケーションの自動インストールを支援するには、**[プリンタポートモニタ MIB を有効化]**(プリンタポート監視 MIB)を選択します。

6 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてデフォルト値を復元します。

SNMP バージョン 3

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[SNMP]**をクリックします。

2 [SNMP バージョン 3]の下で、**[有効]**を選択します。

3 リモートインストール、構成変更、およびデバイス監視を許可するには、[SNMPPv3 読み書きユーザー]フィールドにユーザー名を、[SNMPPv3 読み書きパスワード]フィールドにパスワードを入力します。

4 デバイス監視だけを許可するには、[SNMPPv3 読み取り専用ユーザー]フィールドにユーザー名を、[SNMPPv3 読み取り専用パスワード]フィールドにパスワードを入力します。

5 [SNMPv3 最低認証レベル]リストで、**[認証なし、プライバシーなし]**、**[認証あり、プライバシーなし]**、または**[認証あり、プライバシーあり]**を選択します。

6 [SNMPv3 認証ハッシュ]リストで、**[MD5]**または**[SHA1]**を選択します。

7 [SNMPv3 プライバシーアルゴリズム]リストで、**[DES]**、**[AES-128]**、**[AES-192]**、または**[AES-256]**を選択します。

8 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてデフォルト値を復元します。

SNMP トラップを設定する

SNMP バージョン 1, 2c または SNMP バージョン 3 を設定した後は、SNMP「トラップ」またはアラートメッセージをトリガーするイベントを指定することで、ネットワーク管理システムに送信されるアラートをさらにカスタマイズできます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[SNMP]**をクリックします。

2 **[SNMP トラップの設定]**をクリックします。

3 [IP アドレス]リストで、空白の IP アドレスエントリ（**0.0.0.0** と表示）のいずれかをクリックします。

4 [トラップ宛先]で、ネットワーク管理サーバーまたは監視ステーションの IP アドレスを入力し、アラートを生成する各条件の横にあるチェックボックスをクリックします。

5 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてすべてのフィールドをクリアします。

TCP/IP ポートアクセス設定を構成する

メモ: プリンタ機種によりこの機能が無いものもあります。

デバイスの異なる TCP/IP ポートで、アクセスを設定できます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[TCP/IP ポートへのアクセス]**をクリックします。

メモ: TCP/IP ポートのリストが表示されます。デフォルトでは、TCP 10000 (Telnet) を除くすべてのポートが有効です。

2 TCP/IP ポートのチェックボックスをクリックし、アクセス設定を変更します。

3 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてデフォルト設定を復元します。

IPsec 設定を構成する

メモ: プリンタ機種によりこの機能が無いものもあります。

1 内蔵 Web サーバーで、**[設定]** > **[ネットワーク/ポート]** > **[IPSec]**をクリックします。

2 [IPSec]メニューページで、次の設定を構成します。

設定	説明
IPSec 有効 オン オフ	プリンタの IP セキュリティ設定を有効または無効にします。 **メモ**: 工場出荷時は[オン]に設定されています。
* これは工場出荷時の設定です。	

設定	説明
接続 事前共有鍵で認証された接続 ホスト 1 ホスト 2 ホスト 3 ホスト 4 ホスト 5 ホスト 6 ホスト 7 ホスト 8 ホスト 9 ホスト 10 証明書で認証された接続 ホスト 1 ホスト 2 ホスト 3 ホスト 4 ホスト 5	プリンタの認証済みの接続を設定します。 • ホスト 1 ～ 10 については、次の設定を構成できます。 – **アドレス**—最大 45 バイトの文字を入力できます。 – **キー**—最大 256 バイトの文字を入力できます。 • ホスト 1 ～ 5 については、次の設定を構成できます。 – **アドレス[/サブネット]**—最大 59 バイトの文字を入力できます。
設定 DH グループ 暗号化 認証 証明書確認 ピア証明書の確認 オン* オフ デバイス証明書を選択	プリンタの暗号化と認証方式を指定するには、各設定のオプションを選択します。
* これは工場出荷時の設定です。	

3 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてデフォルト値を復元します。

セキュリティリセット設定を有効にする

メモ: プリンタ機種によりこの機能が無いものもあります。

セキュリティリセット設定は、マザーボードにあるハードウェア設定です。管理者は内蔵 Web サーバーを使用して、この設定を使用する効果を指定します。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[その他のセキュリティ設定]**を選択します。

2 [セキュリティリセット設定]リストから、次のいずれかを選択します。
- **効果なし**—すべてのセキュリティメニューへのアクセスが削除されるため、注意して使用する必要があります。
- **アクセス制御 = 「セキュリティなし」**—機能アクセス制御からだけセキュリティが削除されます。
- **出荷時のセキュリティ標準設定をリセット**—すべてのセキュリティ設定がデフォルト値に復元されます。

3 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてデフォルト設定を復元します。

警告！破損の恐れあり: **[効果なし]**を選択し、パスワード(または他の該当する認証資格情報)をなくした場合は、セキュリティメニューにアクセスできません。デバイスの RIP カード(マザーボード)を交換し、セキュリティメニューへのアクセス権を再取得するには、サービスコールが必要です。

ハードディスクとその他のメモリの保護

揮発性に関する記述

本機には、さまざまなタイプのメモリが搭載されています。各メモリには、デバイスやネットワークの設定、内蔵ソリューションから取得した情報、ユーザーのデータを保存できます。各メモリのタイプ、および各メモリに保存されているデータのタイプは以下のとおりです。

- **揮発性メモリ** – 本機には、単純な印刷・コピージョブ時にユーザーのデータを一時的にバッファに格納する標準的なランダムアクセスメモリ(RAM)を使用しています。
- **不揮発性メモリ** – 本機には、EEPROM および NAND(フラッシュメモリ)の 2 つの形態の不揮発性メモリが使用されています。両タイプ共、オペレーティングシステムやデバイスの設定、ネットワーク情報、スキャナやブックマークの設定、内蔵ソリューションの保存に使用されます。
- **ハードディスクメモリ** – 一部のデバイスには、ハードディスクドライブが搭載されています。プリンタのハードディスクは、各デバイス固有の機能に対応するように設計されており、印刷に関係のないデータの長期間の保存には使用できません。このハードディスクは、ユーザーが情報を抽出したり、フォルダを作成したり、ディスク/ネットワークファイル共有を作成したり、クライアントデバイスから情報を直接 FTP するための機能は備えていません。これにより、複雑なスキャン、印刷、および Fax ジョブでバッファに保存されたユーザーデータ、用紙データ、フォントデータを保持できます。

次のように、お使いのプリンタに搭載されている記憶装置の内容を消去した方がよい状況がいくつかあります。

- プリンタの稼働を中止する
- プリンタのハードドライブを交換する
- プリンタを別の部門または場所に移動する
- 外部の業者によりプリンタが修理される
- プリンタが修理のために社外に搬送される

ハードドライブの廃棄

メモ: すべてのプリンタにハードディスクが搭載されているわけではありません。

高セキュリティ環境では、プリンタまたはそのハードディスクが社外に搬出された際にプリンタハードディスクに保存されている機密データに不正にアクセスされることがないように、さらなる措置を講じることが必要になります。ほとんどのデータは、電子的に消去できますが、プリンタまたはハードディスクを廃棄する前に次の措置のうち 1 つ以上を行ってください。

- **消磁** – 磁場を使用してハードドライブをフラッシュし、保存されているデータを消去します。
- **破砕** – ハードディスクを物理的に圧縮して構成部品を破壊し、読み取りを不可能にします。
- **裁断** – ハードディスクが小さな金属片になるまで物理的に切断します。

メモ: 大部分のデータは電子的に消去できますが、すべてのデータの完全な消去を保証する唯一の方法は、各記憶装置を完全に破壊することです。

揮発性メモリを消去する

プリンタに搭載されている揮発性メモリ（RAM）で情報を保持するには、電源供給が必要です。プリンタの電源を切るだけで、バッファに格納されているデータを消去できます。

不揮発性メモリを消去する

取り付けられたメモリデバイスのタイプとデバイスで保存されたデータのタイプに応じて、不揮発性メモリに保存されたデータを消去するには、複数の方法があります。

- **個別の設定**—プリンタコントロールパネルまたはプリンタの内蔵 Web サーバーを使用して、個別のプリンタ設定を消去できます。詳細については、『ユーザーガイド』を参照してください。
- **デバイスとネットワーク設定**—プリンタの［構成設定］メニューを使用し、NVRAM をリセットすると、デバイスとネットワーク設定を消去し、出荷時設定を復元できます。
- **セキュリティ設定**—出荷時設定を復元するかセキュリティ設定を消去するには、内蔵 Web サーバーのセキュリティリセット設定の動作を選択し、マザーボードのハードウェア設定を移動します。
- **Fax データ**—プリンタにハードディスクがない場合や Fax ストレージとして NAND を選択した場合、Fax 設定とデータを消去するには、プリンタの［構成設定］メニューを使用して NVRAM をリセットします。

  メモ: プリンタのハードディスクが Fax ストレージとしてパーティション分割されていない場合は、パーティションを再フォーマットして、Fax データと設定を消去する必要があります。
- **内蔵ソリューション**—内蔵ソリューションに関連付けられた情報と設定を消去するには、ソリューションをアンインストールするか、プリンタの［構成設定］メニューを使用して出荷時設定を復元します。

データ完全消去を設定する

メモ:

- このメニューは、基本または詳細セキュリティがデバイスで有効で、「リモートのセキュリティメニュー」アクセス制御が有効な場合にだけ表示されます。
- デバイスに保存されたすべての設定、アプリケーション、および保留中のジョブまたは Fax データを選択してクリアしたり、ハードディスクのすべての内容を消去したりできます。データのクリアとハードディスクの消去の両方を選択した場合、ネットワーク設定を含め、デバイスが最初の工場出荷時設定に復元されます。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[工場集荷状態に復元]** > **[データ完全消去]**をクリックします。

  警告！破損の恐れあり: プリンタの電源を切らないでください。

2 すべての設定、アプリケーション、およびジョブデータをクリアする場合は、**[プリンタのメモリを消去]**チェックボックスをオンにします。

3 ハードディスクのすべての内容を消去する場合は、**[ハードディスクを消去]**チェックボックスをオンにし、次のいずれかを選択します。
  - **1回のパス消去**— プリンタのハードディスクの内容を繰り返しビットパターンのシングルパスで上書きします。
  - **複数回パス消去**— プリンタのハードディスクの内容をランダムなビットパターンで複数回上書きしてから、検証パスを実行します。セキュアな消去は、米国国防省の 5220.22-M 規格に準拠しており、ハードディスクからデータを確実に消去することができます。機密性の高い情報は、この方法で消去する必要があります。

  メモ:

  - この設定にアクセスするには、まず、セキュリティテンプレートで適用されたセキュリティ FAC（機能アクセス制御）を満たす必要があります。
  - 工場出荷時は［1 回のパス消去］に設定されています。

4 確認チェックボックスをオンにすると、[開始]ボタンが有効になります。

5 **[開始]**をクリックします。

プリンタハードディスクメモリを完全に消去する

メモ:

- すべてのプリンタにハードディスクが搭載されているわけではありません。
- [構成設定]メニューへのアクセスは、**[構成設定]**メニュー機能アクセス制御によって、制限または無効にできます。詳細については、42 ページの「付録 D:アクセス制御」を参照してください。

プリンタのメニューの[Configuring Disk Wiping]を使用すると、削除対象としてチェックを付けたファイルを確実に上書きすることにより、スキャン、印刷、コピー、FAX の各ジョブによって残された機密情報を削除することができます。

内蔵 Web サーバーを使用した、ハードディスクメモリに保存された残りのジョブ情報の消去については、27 ページの「一時データファイルをハードディスクから消去する」を参照してください。

プリンタコントロールパネルを使用する

1 電源スイッチでプリンタの電源を切ってください。

2 デバイスの電源を入れながら、キーパッドの **2** キーと **6** キーを同時に押します。[構成設定]メニューで起動するまでには、約 1 分かかります。

MFP が準備完了状態になると、コピーや FAX などの通常のホーム画面のアイコンの代わりにタッチスクリーンに機能一覧が表示されます。

3 進行状況バーの画面が表示されたら、ボタンを放します。プリンタで電源投入リセットが実行され、[構成設定]メニューが表示されます。

4 **[ディスクをワイプ]**をタッチしてから、次のいずれかのオプションをタッチします。
- **[ディスクをワイプ(高速)]** – シングルパスでディスクをすべてゼロで上書きします。
- **[ディスクをワイプ(セキュア)]** – ディスクをランダムなビットパターンで複数回上書きしてから、検証パスを実行します。セキュアな上書きは、米国国防省の 5220.22-M 規格に準拠しており、ハードディスクからデータを確実に消去することができます。機密性の高い情報は、この方法で消去する必要があります。

5 ディスクの消去を開始するには、**[はい]**を押します。

メモ:

- ステータスバーにはディスクワイプタスクの進行状況が表示されます。
- ディスクのワイプには、数分から 1 時間以上かかります。この間は、プリンタを他の処理に使用できません。

6 **[戻る]** > **[設定メニューを閉じる]**を押します。

プリンタで電源投入時リセットが実行され、通常の動作モードに戻ります。

プリンタハードディスクの暗号化を設定する

ハードディスクの暗号化を有効にすると、プリンタまたはハードディスクの盗難の際に機密データの喪失を防ぐことができます。

メモ: すべてのプリンタにハードディスクが搭載されているわけではありません。

内蔵 Web サーバーを使用する

1 Web ブラウザを開き、アドレスフィールドにプリンタの IP アドレスを入力します。

メモ:

- プリンタのホーム画面でプリンタの IP アドレスを確認します。IP アドレスは、123.123.123.123 のように、ピリオドで区切られた 4 つの数字の組み合わせとして表示されます。
- プロキシサーバーを使用している場合は、一時的に無効にし、Web ページを正しく読み込んでください。

2 **[設定]** > **[セキュリティ]** > **[ディスク暗号化]**をクリックします。

メモ: フォーマット済みの正常なプリンタハードディスクが搭載されている場合にのみ、[セキュリティ]メニューに[ディスク暗号化]が表示されます。

3 [ディスク暗号化]メニューから、次のいずれかを選択します。

- **無効化**—ディスク暗号化を無効にします。
- **有効化**—ディスク暗号化を有効にします。

メモ:

- 工場出荷時は[無効化]に設定されています。
- この設定を変更すると、プリンタで電源オンリセットが発生します。

警告！破損の恐れあり: ディスク暗号化設定を変更すると、ハードディスクの内容が消去されます。

4 ディスクの消去と暗号化を続行するには、**[送信]**をクリックします。

メモ: 暗号化には約 2 分かかります。

警告！破損の恐れあり: 暗号化処理中はプリンタの電源を切らないでください。

5 **[更新]**をクリックすると、内蔵 Web サーバーに戻ります。

プリンタコントロールパネルを使用する

1 プリンタの電源を切ります。

2 プリンタの電源を入れながら、**2** および **6** を長押しします。進行状況バーの画面が表示されたら、ボタンを放します。

プリンタで電源投入シーケンスが実行され、[構成設定]メニューが表示されます。プリンタが完全に起動すると、タッチスクリーンに機能一覧が表示されます。

3 **[ディスク暗号化]** > **[有効化]**をタッチします。

4 ディスクの暗号化を続行するには、**[はい]**を押します。

メモ:

- 暗号化処理中はプリンタの電源を切らないでください。データの損失につながることがあります。
- 暗号化には約 2 分かかります。

- ステータスバーにはディスクワイプタスクの進行状況が表示されます。ディスクが暗号化されると、プリンタは、[有効化/無効化]画面に戻ります。

5 **[戻る]** > **[設定メニューを閉じる]**を押します。

プリンタで電源投入時リセットが実行され、通常の動作モードに戻ります。

シナリオ

シナリオ：公共の場所のプリンタ

プリンタがロビーなどの公共の場所にある場合に、一般のユーザーがプリンタを使用できないようにするには、パスワードまたは 暗証番号 によって簡易的にデバイスを保護できます。管理者は、許可されたデバイスユーザー全員に同じパスワードまたは 暗証番号 を割り当てます。あるいは、個別のコードを割り当てて、個別の機能を保護します。重要な点は、パスワードまたは 暗証番号 を知っている全員が、そのコードで保護されたすべての機能にアクセスできるということです。

手順 1：パスワードまたは 暗証番号 を作成する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 ［詳細セキュリティセットアップ］の下で**[暗証番号]**または**[パスワード]**をクリックし、設定します。

一部のプリンタモデルでは、パネル 暗証番号 保護と Web ページパスワード保護によって、暗証番号 とパスワードを設定できます。詳細については、10 ページの「パネル暗証の保護で 暗証番号 を作成する」および 9 ページの「Web ページパスワードの保護でパスワードを作成する」を参照してください。

3 **[送信]**をクリックして、変更を保存します。

暗証番号 またはパスワードの設定の詳細については、8 ページの「ビルディングブロックを編集」の該当セクションを参照してください。

手順 2：セキュリティテンプレートを作成する

メモ: プリンタ機種によりこの機能が無いものもあります。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 ［詳細セキュリティセットアップ］の下で**[セキュリティテンプレート]**をクリックします。

3 ［セキュリティテンプレートの管理］の下で**[セキュリティテンプレートを追加]**をクリックします。

4 ［セキュリティテンプレート名］フィールドで、128 文字以下の一意の名前を入力します。「Administrator_Only」や「Common_Functions_Template」などのわかりやすい名前を指定すると便利です。

5 ［認証セットアップ］メニューリストで、手順 1 で作成した 暗証番号 またはパスワードを選択します。

6 **[テンプレートの保存]**をクリックします。

手順 3：セキュリティテンプレートをアクセス制御に割り当てる

メモ: プリンタ機種によりこの機能が無いものもあります。

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 ［詳細セキュリティセットアップ］の下で**[アクセス制御]**をクリックします。

3 必要に応じて、**[すべて展開]**または特定のフォルダをクリックし、使用可能な機能の一覧を表示します。

4 保護する各機能の横のドロップダウンメニューから、手順 2 で作成されたセキュリティテンプレートを選択します。

5 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてすべての変更をキャンセルします。

このセキュリティテンプレートで制御された機能にアクセスするには、適切な 暗証番号 またはパスワードを入力する必要があります。

シナリオ：スタンドアロンまたは小規模オフィス

メモ: プリンタ機種によりこの機能が無いものもあります。

プリンタがネットワークに接続されていないか、認証サーバーを使用してユーザーアクセス権をデバイスに付与していない場合は、認証または権限付与のために、内部アカウントを内蔵 Web サーバー内に作成して保存できます。

手順 1：個別のユーザーアカウントを設定する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 ［詳細セキュリティセットアップ］の下で**[内部アカウント]**をクリックし、設定します。

個別のユーザーアカウントの設定の詳細については、11 ページの「内部アカウントを設定する」を参照してください。

手順 2：セキュリティテンプレートを作成する

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 ［詳細セキュリティセットアップ］の下で**[セキュリティテンプレート]**をクリックします。

3 ［セキュリティテンプレートの管理］の下で**[セキュリティテンプレートを追加]**をクリックします。

4 ［セキュリティテンプレート名］フィールドで、128 文字以下の一意の名前を入力します。「Administrator_Only」や「Common_Functions_Template」などのわかりやすい名前を指定すると便利です。

5 ［認証セットアップ］メニューから、ユーザーの認証方式を選択します。このリストには、デバイスで設定された認証ビルディングブロックが入力されます。

6 権限を使用するには、**[承認を追加]**をクリックしてから、［承認セットアップ］メニューでビルディングブロックを選択します。このリストには、デバイスで使用可能な権限ビルディングブロックが入力されます。

メモ: 特定のビルディングブロック（パスワードと暗証番号など）は、個別の権限をサポートしません。

7 グループを使用するには、**[グループの変更]**をクリックし、セキュリティテンプレートに含める 1 つ以上のグループを選択します。**Ctrl** キーを押すと、複数のグループを選択できます。

8 **[テンプレートの保存]**をクリックします。

手順 3：セキュリティテンプレートをアクセス制御に割り当てる

1 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。

2 ［詳細セキュリティセットアップ］の下で**[アクセス制御]**をクリックします。

3 必要に応じて、**[すべて展開]**または特定のフォルダをクリックし、使用可能な機能の一覧を表示します。

4 機能名の横にあるドロップダウンメニューから、保護する機能ごとに、セキュリティテンプレートを選択します。

5 **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてすべての変更をキャンセルします。

セキュリティテンプレートで制御された機能にアクセスするには、適切な認証資格情報を入力する必要があります。

シナリオ：Active Directory を実行するネットワーク

メモ: プリンタ機種によりこの機能が無いものもあります。

Active Directory を実行するネットワークでは、管理者は、内蔵 Web サーバーの LDAP+GSSAPI 機能を使用し、既にネットワークに展開された認証および権限サービスを利用できます。ユーザー認証資格情報とグループ指定は既存のネットワークから取得できるため、プリンタへのアクセスが他のネットワークサービスと同様にシームレスになります。

Active Directory と統合するように内蔵 Web サーバーを構成する前に、次の点を理解しておく必要があります。

- ドメイン名
- ユーザー ID（ドメイン）
- パスワード（ユーザー ID）

詳細については、12 ページの「プリンタを Active Directory ドメインに接続する」を参照してください。

セキュリティテンプレートを作成する

1. 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。
2. ［詳細セキュリティセットアップ］の下で**[セキュリティテンプレート]**をクリックします。
3. ［セキュリティテンプレートの管理］の下で**[セキュリティテンプレートを追加]**をクリックします。
4. ［セキュリティテンプレート名］フィールドで、128 文字以下の一意の名前を入力します。「Administrator_Only」や「Common_Functions_Template」などのわかりやすい名前を指定すると便利です。
5. ［認証セットアップ］リストから、認証クライアントアプリケーションまたはビルディングブロック設定に割り当てられた名前を選択します。
6. **[承認を追加]**をクリックし、認証クライアントアプリケーションまたはビルディングブロック設定に割り当てられた名前を選択します。
7. グループを使用するには、**[グループを変更]**をクリックし、［Active Directory グループ名］リストから 1 つ以上のグループを選択します。**Ctrl** キーを押すと、複数のグループを選択できます。
8. **[テンプレートの保存]**をクリックします。

セキュリティテンプレートをアクセス制御に割り当てる

1. 内蔵 Web サーバーで、**[設定]** > **[セキュリティ]** > **[セキュリティセットアップ]**をクリックします。
2. ［詳細セキュリティセットアップ］の下で**[アクセス制御]**をクリックします。
3. 機能名の横にあるドロップダウンメニューから、保護する機能ごとに、新しく作成されたセキュリティテンプレートを選択します。
4. **[送信]**をクリックして変更を保存するか、**[フォームをリセット]**をクリックしてすべての変更をキャンセルします。

   セキュリティテンプレートで制御された機能にアクセスするには、適切な認証資格情報を入力する必要があります。

付録

付録 A:CA ファイルの作成

メモ: この認証機関の CA ファイルの生成例では、Windows 認証機関サーバーを使用することを想定しています。

1 ブラウザウィンドウで CA を参照します。URL には http//<CA のアドレス>/CertSrv を使用してください。**CA のアドレス**は、CA サーバーの IP アドレスまたはホスト名です。

メモ: CA の Web ページが開く前に、Windows ログインウィンドウがポップアップ表示され、CA の Web ページにアクセスできることを確認するためにユーザー認証資格情報が要求される場合があります。

2 **[CA 証明書、証明書チェーン、または CRL のダウンロード]**をクリックします。

3 **[Base 64 エンコード]**をクリックし、**[CA 証明書のダウンロード]**をクリックします。

メモ: DER エンコーディングはサポートされません。

4 証明書をファイルに保存します。ファイル名は任意ですが、拡張子は「.pem」でなければなりません。

付録 B:CA が署名したデバイス証明書の作成

メモ: この認証機関の CA ファイルの生成例では、Windows 認証機関サーバーを使用することを想定しています。

1 ブラウザウィンドウで CA を参照します。URL には http//<CA のアドレス>/CertSrv を使用してください。**CA のアドレス**は、CA サーバーの IP アドレスまたはホスト名です。

2 **[証明書の要求]**をクリックします。

3 **[詳細証明書要求]**をクリックします。

4 **[Base 64 エンコードを使用して証明書要求を送信]**をクリックします。

5 デバイスからコピーされた情報(.csr プロンプト)を[保存された要求]フィールドに貼り付け、Web サーバータイプの証明書テンプレートを選択します。

6 **[送信]**をクリックします。

メモ: サーバーで要求が処理されるには少し時間がかかります。その後にダイアログウィンドウが表示されます。

7 **[Base 64 エンコード]**を選択し、**[証明書のダウンロード]**をクリックします。

メモ: DER エンコーディングはサポートされません。

8 証明書をファイルに保存します。ファイル名は任意ですが、拡張子は「.pem」でなければなりません。

付録 C:自動証明書登録アプリケーション

このアプリケーションをインストールすると、デバイス証明書署名要求が自動的に作成され、署名要求が承認のために認証機関(CA)に送信されます。次に、CA 署名付きデバイス証明書が取得され、インストールされます。以前の手動プロセスは、必要な初期設定が少ない簡易プロセスに置き換わります。

このアプリケーションが機能するには、デバイスが Active Directory 環境に参加し、証明書登録 Web サービス(サーバーロール)アプリケーションが顧客のネットワークにインストールされている必要があります。

メモ: 次の使用手順の例では、証明書登録 Web サービスが Windows 2008 R2 サーバーにインストールされているという前提です。

1 Web ブラウザを開き、アドレスフィールドにプリンタの IP アドレスまたはホスト名を入力します。

2 内蔵 Web サーバーで、**[設定]** >**[セキュリティ]** >**[証明書管理]** >**[デバイス証明書管理]**をクリックします。

3 **[詳細管理]**をクリックして、自動証明書登録アプリケーションを使用し、**[新しい証明書の要求]**をクリックします。

メモ: 10 ～ 15 秒間画面が更新される場合があります。このときに、デバイスはサーバー上の証明書登録 Web サービスに接続し、デバイスが使用できる証明書テンプレートを取り込んでいます。

4 [デバイス証明書管理] >[詳細] >[テンプレート]ページで、次のテンプレートオプションから、証明書の要求時に使用するオプションを選択します。

- **IPSec**—IPSec ネゴシエーションで使用されるデバイス証明書をインストールする場合。
- **Web サーバー**—SSL 経由での EWS や LDAP など、SSL/TLS 接続を保護する場合。
- **RAS および IAS サーバー**—802.1X ネゴシエーションで使用されるデバイス証明書をインストールする場合。

5 **[証明書の要求]**をクリックします。この画面で、このデバイスの証明書をカスタマイズします。

メモ: 最初にテンプレート詳細を確認する場合は、**[証明書の要求]**ではなく、**[表示]**をクリックします。

6 [証明書の要求]Web ページから設定を修正します。この操作は必要な場合にだけ行ってください。

メモ:

- データが入力されたフィールドと選択されたチェックボックスが、CA から取得されたテンプレートのデフォルトです。選択すると変更できますが、一般的に、デフォルトテンプレートは CA 管理者による適切な設定で構成されています。一部の設定を変更すると、要求が拒否される場合があります。
- [件名の折りたたみ/展開]フィールドリンクを使用して、証明書を作成または生成するために使用されるデバイス情報を変更します。これには、[証明書管理]の下の[証明書のデフォルトの設定]リンクと同じ情報が含まれます。

7 [送信]をクリックすると、証明書署名要求(CSR)が CA に送信されます。

メモ: 10 ～ 15 秒間画面が更新される場合があります。このときに、デバイスは証明書登録 Web サービスに接続し、CA 署名付き証明書の生成を要求しています。

8 成功した場合は、[デバイス証明書管理]>[詳細]Web ページに戻り、新しい CA 署名付きデバイス証明書と指定された名前が証明書のリストに表示されます。失敗した場合は、エラーメッセージが表示されます。

メモ: テンプレートがサーバーで指定され、CA 管理者の承認が必要な場合は、保留中の証明書の個別の表が表示されます。また、証明書が一覧表示される[デバイス証明書管理]画面には、要求が管理者の承認待ちであることを示すメッセージが表示されます。証明書は、承認されるまで有効になりません。承認が付与されると、メッセージが消え、インストール済み証明書の表には証明書が表示されます。

新しい証明書に関連付けられた情報を表示するには、証明書名のリンクを選択できます。[更新]リンクを使用すると、現在の CA 証明書の有効期限(デフォルトは 2 年)が近づいたときに証明書を更新します。

有効期限が近づいている証明書を自動的に更新するように指定するには、[設定] >[アプリケーション] >[アプリケーション管理]Web ページの[構成設定]タブで、[証明書を自動的に更新する]チェックボックスをオンにし、[自動更新しきい値]設定で有効期限前の日数を指定してから、**[適用]**をクリックします。

付録 D:アクセス制御

メモ: デバイスタイプと取り付けられたオプションによっては、一部のアクセス制御(機能アクセス制御)がプリンタで使用できない場合があります。

管理メニュー

機能アクセス制御	説明
構成設定メニュー	設定メニューへのアクセスを保護します。
デバイスでショートカットを管理	プリンタコントロールパネルから、[設定]メニューの[ショートカットの管理]セクションへのアクセスを保護します。
リモートでショートカットを管理	内蔵 Web サーバーから、[設定]メニューの[ショートカットの管理]セクションへのアクセスを保護します。
デバイスのネットワーク/ポートメニュー	プリンタコントロールパネルから、[設定]メニューの[ネットワーク/ポート]セクションへのアクセスを保護します。
リモートのネットワーク/ポートメニュー	内蔵 Web サーバーから、[設定]メニューの[ネットワーク/ポート]セクションへのアクセスを保護します。
デバイスのオプションカード設定	プリンタコントロールパネルから、[設定]メニューの[オプションカード設定]セクションへのアクセスを制御します。設定オプションのあるオプションカードがデバイスに取り付けられている場合にだけ適用されます。
リモートでのオプションカード設定	内蔵 Web サーバーから、[設定]メニューの[オプションカード設定]セクションへのアクセスを制御します。設定オプションのあるオプションカードがデバイスに取り付けられている場合にだけ適用されます。
デバイスの用紙メニュー	プリンタコントロールパネルから、[用紙]メニューへのアクセスを保護します。
リモートの用紙メニュー	内蔵 Web サーバーから、[用紙]メニューへのアクセスを保護します。
デバイスのレポートメニュー	プリンタコントロールパネルから、[レポート]メニューへのアクセスを保護します。
リモートのレポートメニュー	内蔵 Web サーバーから、[レポート]メニューへのアクセスを保護します。
デバイスのセキュリティメニュー	プリンタコントロールパネルから、[セキュリティ]メニューへのアクセスを保護します。
リモートのセキュリティメニュー	内蔵 Web サーバーから、[セキュリティ]メニューへのアクセスを保護します。
デバイスのサービスエンジニアメニュー	プリンタコントロールパネルから、[サービスエンジニア]メニューへのアクセスを保護します。
リモートでのサービスエンジニアメニュー	内蔵 Web サーバーから、[サービスエンジニア]メニューへのアクセスを保護します。
デバイスの設定メニュー	プリンタコントロールパネルから、[設定]メニューの[一般設定]および[印刷設定]セクションへのアクセスを保護します。
リモートの設定メニュー	内蔵 Web サーバーから、[設定]メニューの[一般設定]および[印刷設定]セクションへのアクセスを保護します。

管理

機能アクセス制御	説明
ファームウェア更新	フラッシュドライブ以外の場所からファームウェアを更新する機能を制御します。この機能が保護されている場合、FTP や内蔵 Web サーバー経由で受信されたファームウェアファイルは、無視(フラッシュ)されます。
操作パネルロック	プリンタコントロールパネルのロック機能へのアクセスを保護します。有効な場合、適切な認証資格情報を持つユーザーがプリンタタッチスクリーンをロックおよびロック解除できます。ロック状態では、タッチスクリーンには、「デバイスのロック解除」アイコンだけが表示され、適切な認証資格情報が入力されるまでデバイスの操作を実行できません。ロック解除されると、ユーザーがデバイスからログアウトしても、タッチスクリーンがロック解除された状態になります。コントロールパネルのロックを有効にするには、「デバイスのロック」アイコンを選択してから、適切な認証資格情報を入力する必要があります。

機能アクセス制御	説明
PJL デバイス設定変更	無効にすると、受信印刷ジョブによって受信されたすべてのデバイス設定変更が無視されます。
リモート管理	MarkVision™ などのリモート管理ツールによって、プリンタ設定と機能へのアクセスを制御します。保護されている場合は、安全に保護された通信チャネル（正しく構成およびインストールされた MarkVision で提供されたチャネルなど）経由でしか、プリンタの構成設定を変更できません。
アプリ構成	すべてのインストール済みソリューションの構成へのアクセスを制御します。
Web インポート/エクスポート設定	内蔵 Web サーバーからプリンタ設定ファイル（UCF ファイル）をインポートおよびエクスポートできるかどうかを制御します。
構成ファイルのインポート/エクスポート	設定とセキュリティ構成ファイルをインポートおよびエクスポートできるかどうかを制御します。
インターネットプリンティングプロトコル（IPP）	IPP を使用できるかどうかを制御します。

機能アクセス

機能アクセス制御	説明
アドレス帳	[FAX にスキャン]および[E メールにスキャン]機能でアドレス帳検索を実行できるかどうかを制御します。
デバイスのジョブをキャンセル	プリンタコントロールパネルから、ジョブをキャンセルできるかどうかを制御します。
ホーム画面から言語を変更	プリンタコントロールパネルから、[言語を変更]機能へのアクセスを制御します。
カラードロップアウト	スキャンおよびコピー機能の[カラードロップアウト]機能を使用できるかどうかを制御します。
カラー印刷をコピー	カラーコピーを実行できるかどうかを制御します。権限のないユーザーの場合、コピージョブが白黒で印刷されます。
コピー機能	コピーを使用できるかどうかを制御します。
デバイスにブックマークを作成	プリンタコントロールパネルから、新しいブックマークを作成できるかどうかを制御します。
リモートでブックマークを作成	内蔵 Web サーバーの[設定]メニューの[ブックマーク設定]セクションから、新しいブックマークを作成できるかどうかを制御します。
プロファイルを作成	新しいプロファイルを作成できるかどうかを制御します。
E メール機能	E メールにスキャン機能へのアクセスを制御します。
FAX 機能	FAX にスキャン機能へのアクセスを制御します。
フラッシュドライブカラー印刷	フラッシュドライブからカラー印刷できるかどうかを制御します。権限のないユーザーの場合、印刷ジョブが白黒で印刷されます。
フラッシュメモリのアクセスを許可	フラッシュドライブへのアクセスを制御します。
フラッシュドライブプリント	フラッシュドライブから印刷できるかどうかを制御します。
フラッシュドライブスキャン	フラッシュドライブからドキュメントをスキャンできるかどうかを制御します。
FTP 機能	FTP にスキャン機能へのアクセスを制御します。
保持されたジョブにアクセス	保持されたジョブ機能へのアクセスを保護します。
PictBridge 印刷	一部のデバイスで、接続された PictBridge 対応デジタルカメラから印刷できるかどうかを制御します。 **メモ**: 選択したデバイスだけです。

機能アクセス制御	説明
保持された FAX をリリース	保持された FAX をリリース（印刷）できるかどうかを制御します。
プロファイルを使用	スキャンショートカット、ワークフロー、eSF アプリケーションなどのプロファイルへのアクセスを制御します。

デバイスアプリ

機能アクセス制御	説明
新しいアプリ	プリンタにインストールされた各アプリケーション固有のアクセス制御について、初期セキュリティプロファイルを制御します。
アプリ 1 ～ 10	アプリケーション 1 ～ 10 のアクセス制御は、インストール済みの eSF アプリケーションと LDSS によって作成されたプロファイルに割り当てることができます。各アプリケーションのアクセス制御は、アプリケーションまたはプロファイルの作成または設定時に割り当てられます。

メモ:

- インストールしたアプリケーションによっては、その他のアプリケーション固有のアクセス制御が、アプリケーション 1 ～ 10 の下に一覧表示される場合があります。インストール済みのアプリケーションで使用可能な場合は、これらの追加アクセス制御を使用します。その他のソリューション固有のアクセス制御がない場合は、番号 10 までのアクセス制御のいずれかを、保護するアプリケーションに割り当てます。
- 一部のアプリケーションはデフォルト構成としてプリンタに含まれ、機能アクセス制御選択項目として表示される場合があります。

通知

版通知

2013 年 10 月

この章に記載された内容は、これらの条項と地域法とに矛盾が生じる国では適用されないものとします。Lexmark International, Inc. は本ドキュメントを「現状有姿」で提供し、明示的または黙示的であるかを問わず、商品性および特定目的に対する適合性の黙示的保証を含み、これに限定されないその他すべての保証を否認します。一部の地域では特定の商取引での明示的または黙示的な保証に対する免責を許可していない場合があり、これらの地域ではお客様に対して本条項が適用されない場合があります。

本ドキュメントには、不正確な技術情報または誤植が含まれている場合があります。ここに記載された情報は定期的に変更され、今後のバージョンにはその変更が含まれます。記載された製品またはプログラムは、任意の時期に改良または変更が加えられる場合があります。

本ドキュメントで特定の製品、プログラム、またはサービスについて言及している場合でも、すべての国々でそれらが使用可能であることを黙示的に意味しているものではありません。特定の製品、プログラム、またはサービスについてのすべての記述は、それらの製品、プログラム、またはサービスのみを使用することを明示的または黙示的に示しているものではありません。既存の知的財産権を侵害しない、同等の機能を持つすべての製品、プログラム、またはサービスを代替して使用することができます。製造元が明示的に指定した以外の製品、プログラム、またはサービスと組み合わせた場合の動作の評価および検証は、ユーザーの責任において行ってください。

Lexmark テクニカルサポートについては、**http://support.lexmark.com** を参照してください。

消耗品とダウンロードについては、**http://www.lexmark.com** を参照してください。

商標

Lexmark およびダイヤモンドのデザインを組み合わせた Lexmark のロゴは、Lexmark International, Inc. の商標であり、アメリカ合衆国およびその他の国々で登録されています。

その他の商標は各所有者に帰属します。

GOVERNMENT END USERS

The Software Program and any related documentation are "Commercial Items," as that term is defined in 48 C.F.R. 2.101, "Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. 12.212 or 48 C.F.R. 227.7202, as applicable. Consistent with 48 C.F.R. 12.212 or 48 C.F.R. 227.7202-1 through 227.7207-4, as applicable, the Commercial Computer Software and Commercial Software Documentation are licensed to the U.S. Government end users (a) only as Commerical Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

GifEncoder

GifEncoder - writes out an image as a GIF. Transparency handling and variable bit size courtesy of Jack Palevich. Copyright (C) 1996 by Jef Poskanzer * <jef@acme.com>. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Visit the ACME Labs Java page for up-to-date versions of this and other fine Java utilities: http://www.acme.com/java/

ZXing 1.7

This project consists of contributions from several people, recognized here for convenience, in alphabetical order.

Agustín Delgado (Servinform S.A.), Aitor Almeida (University of Deusto), Alasdair Mackintosh (Google), Alexander Martin (Haase & Martin GmbH), Andreas Pillath, Andrew Walbran (Google), Andrey Sitnik, Androida.hu / http://www.androida.hu/, Antonio Manuel Benjumea (Servinform S.A.), Brian Brown (Google), Chang Hyun Park, Christian Brunschen (Google), crowdin.net, Daniel Switkin (Google), Dave MacLachlan (Google), David Phillip Oster (Google), David Albert (Bug Labs), David Olivier, Diego Pierotto, drejc83, Eduardo Castillejo (University of Deusto), Emanuele Aina, Eric Kobrin (Velocitude), Erik Barbara, Fred Lin (Anobiit), gcstang, Hannes Erven, hypest (Barcorama project), Isaac Potoczny-Jones, Jeff Breidenbach (Google), John Connolly (Bug Labs), Jonas Petersson (Prisjakt), Joseph Wain (Google), Juho Mikkonen, jwicks, Kevin O'Sullivan (SITA), Kevin Xue (NetDragon Websoft Inc., China), Lachezar Dobrev, Luiz Silva, Luka Finžgar, Marcelo, Mateusz Jędrasik, Matrix44, Matthew Schulkind (Google), Matt York (LifeMarks), Mohamad Fairol, Morgan Courbet, Nikolaos Ftylitakis, Pablo Orduña (University of Deusto), Paul Hackenberger, Ralf Kistner, Randy Shen (Acer), Rasmus Schrøder Sørensen, Richard Hřivňák, Romain Pechayre, Roman Nurik (Google), Ryan Alford, Sanford Squires, Sean Owen (Google), Shiyuan Guo / 郭世元, Simon Flannery (Ericsson), Steven Parkes, Suraj Supekar, Sven Klinkhamer, Thomas Gerbet, Vince Francis (LifeMarks), Wolfgang Jung, Yakov Okshtein (Google)

Apache License Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1 Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2 Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3 Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4 Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- **a** (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
- **b** (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
- **c** (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- **d** (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5 Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6 Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7 Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8 Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9 Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or

claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

セキュリティ関連用語集

アクセス制御	個別のデバイスメニュー、機能、および設定が、どのユーザーに対して使用可能かどうかを制御する設定。一部のデバイスでは、機能アクセス制御とも言われます。
セキュリティテンプレート	内蔵 Web サーバーで作成および保存されるプロファイルであり、デバイス機能を管理するために、アクセス制御とともに使用されます。
認証	ユーザーを安全に識別する方法。
権限	ユーザーが使用できる機能を指定する方法。
グループ	共通の特性を持つユーザーの集合。
ビルディングブロック	内蔵 Web サーバーで使用される認証および権限ツール。パスワード、PIN、内部アカウント、LDAP、LDAP+GSSAPI、Kerberos 5 があります。

索引

数値

A

B

C

D

E

F

G

H