



パスワード、ログオン、およびロックアウトのポリシーの指定

Cisco Unity Connection では、認証規則を使用して、電話アクセスと Web ツール アクセスに対するパスワードポリシーとアカウントロックアウトポリシー、および Cisco Unity Connection ボイスメッセージにアクセスするすべてのユーザの Web ツール アクセスに対するログオンポリシーを決定します。

次の各項を参照してください。

- [認証規則を使用した、パスワード、ログオン、およびロックアウトに関するポリシーの指定 \(P.16-1\)](#)
- [認証規則の作成と修正、およびユーザへの規則の割り当て \(P.16-2\)](#)

認証規則を使用した、パスワード、ログオン、およびロックアウトに関するポリシーの指定

Cisco Unity Connection では、すべてのユーザアカウントのパスワードおよびロックアウトを認証規則によって制御します。認証規則を使用すると、Connection への電話でのユーザアクセス、および Cisco Unity Connection の管理と Cisco Personal Communications Assistant (PCA) へのユーザアクセスがセキュリティで保護されます。

認証規則では、たとえば次の項目を指定します。

- ログオン失敗の許容回数。この数を超えると、アカウントがロックされます。
- ロックされたアカウントがリセットされるまでの期間（分単位）。
- ロックされたアカウントのロック解除を、管理者による手動操作にするかどうか。
- 許容される最短のパスワードの長さ。
- パスワードの有効日数。

認証規則の作成と修正、およびユーザへの規則の割り当て

認証規則は、Connection の管理の [システム設定 (System Settings)] > [認証規則 (Authentication Rules)] ページで指定します。Connection には、次に示す、あらかじめ定義された認証規則が含まれています。

[ボイスメール認証規則 (推奨) (Recommended Voice Mail Authentication Rule)]	デフォルトでは、この規則が適用されるのは、Connection への電話でのユーザ アクセスを設定した各ユーザ アカウントおよびユーザ テンプレートの [パスワードの設定 (Password Settings)] ページにある、[ボイスメール (Voice Mail)] パスワードです。
[Web アプリケーション認証規則 (推奨) (Recommended Web Application Authentication Rule)]	デフォルトでは、この規則が適用されるのは、Cisco Unity Connection の管理または Cisco Personal Communications Assistant へのユーザ アクセスを設定した各ユーザ アカウントおよびユーザ テンプレートの [パスワードの設定 (Password Settings)] ページにある、[Web アプリケーション (Web Application)] パスワードです。

これらのデフォルト設定は変更可能であり、追加の認証規則をいくつでも作成できます。

ユーザ アカウントおよびテンプレートに関する、Connection へのユーザ アクセスを制御するための認証規則は、管理者が指定します。ユーザ アカウントまたはテンプレートの認証規則を指定するには、『Cisco Unity Connection ユーザの移動、追加、変更ガイド』の「ユーザ アカウントの設定によって制御される機能の設定」の章の「パスワード」の項を参照してください。このドキュメントは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。