



コモンクライテリアに準拠したパスワードの強度と管理

コモンクライテリアに準拠したパスワードの強度と管理機能は、ユーザパスワードを指定するルール、保存、検索、提供のためのパスワードポリシーおよびセキュリティメカニズムを指定するために使用されます。

ローカルユーザについては、ユーザのプロファイルとパスワード情報が重要なパラメータとともにシスコデバイスに保存され、このプロファイルを使用して、ユーザのローカル認証が行われます。このユーザになり得るのは、管理者（ターミナルアクセス）またはネットワークユーザ（たとえば、ネットワークアクセスのために認証された PPP ユーザ）です。

リモートユーザについては、ユーザプロファイル情報がリモートサーバに保存されている場合、管理アクセスとネットワークアクセスの双方にサードパーティの認証、許可、およびアカウントリング（AAA）サーバを使って AAA サービスが提供される可能性があります。

- [コモンクライテリアに準拠したパスワードの強度と管理の制約事項（1 ページ）](#)
- [コモンクライテリアに準拠したパスワードの強度と管理に関する情報（2 ページ）](#)
- [コモンクライテリアに準拠したパスワードの強度と管理の設定方法（4 ページ）](#)
- [コモンクライテリアに準拠したパスワードの強度と管理の設定例（7 ページ）](#)
- [コモンクライテリアに準拠したパスワードの強度と管理に関するその他の参考資料（8 ページ）](#)
- [コモンクライテリアに準拠したパスワードの強度と管理の機能情報（8 ページ）](#)

コモンクライテリアに準拠したパスワードの強度と管理の制約事項

vtty を使用して同時にシステムにログインできるユーザは 4 人までです。

コモンクライテリアに準拠したパスワードの強度と管理に関する情報

次の各項では、パスワードの強度と管理について説明します。

パスワード構成ポリシー

パスワード構成ポリシーでは、パスワードを作成するために、英字の大文字小文字、数字、特殊文字（「!」、「@」、「#」、「\$」、「%」、「^」、「&」、「*」、「(」、「)」など）を自由に組み合わせて使用できます。

パスワード長ポリシー

パスワードの最小長と最大長は、管理者により柔軟に設定することが可能です。推奨されるパスワードの最小長は8文字です。管理者は、パスワードの最小長（1）も最大長（64）も指定できます。

パスワードのライフタイムポリシー

セキュリティ管理者は、パスワードのライフタイムを最大限にするための設定可能オプションを提供できます。ライフタイムパラメータが設定されていない場合、設定済みのパスワードは無限に有効です。最大ライフタイムは、設定可能な値を年、月、日、時間、分、および秒単位で入力することにより設定できます。ライフタイム設定は設定の一部であるためリロード後も有効ですが、パスワード作成時刻はシステムがリポートするたびに新しい時刻に更新されます。たとえば、パスワードに1ヵ月のライフタイムが設定されており、29日目にシステムがリポートした場合、そのパスワードはシステムリポート後1ヵ月間有効になります。

パスワード有効期限ポリシー

ユーザがログインを試みたときにこのユーザのパスワードクレデンシャルが期限切れになっていた場合、次の処理が行われます。

1. ユーザは、期限切れのパスワードの入力に成功した後、新しいパスワードを設定するように求められます。
2. ユーザが新しいパスワードを入力すると、パスワードセキュリティポリシーに照らしてそのパスワードが検証されます。
3. 新しいパスワードがパスワードセキュリティポリシーに適合していれば、認証、許可、およびアカウントिंग（AAA）データベースが更新され、ユーザは新しいパスワードで認証されます。

4. 新しいパスワードがパスワードセキュリティポリシーに適合していない場合、ユーザは再度パスワードの入力を求められます。再試行数は、AAAでは制限されていません。認証失敗の場合のパスワードプロンプトの再試行数は、それぞれのターミナルアクセスインタラクティブモジュールによって制御されます。たとえばTelnetでは、3回失敗するとセッションが終了します。

パスワードのライフタイムを設定されていないユーザがすでにログインしているときに、セキュリティ管理者がそのユーザのライフタイムを設定すると、ライフタイムがデータベースに設定されます。同じユーザが次回に認証されるときに、システムがパスワードの期限を確認します。パスワード期限がチェックされるのは認証フェーズの間のみです。

すでに認証済みかつシステムにログイン中のユーザのパスワードが期限切れになっても、何のアクションも起こりません。同じユーザが次に認証されるときに初めて、ユーザにパスワード変更が求められます。

パスワード変更ポリシー

新しいパスワードは、前のパスワードから4文字以上変更されている必要があります。パスワード変更のきっかけとなるシナリオとしては、次のようなものが考えられます。

- セキュリティ管理者がパスワードの変更を求める場合。
- ユーザがプロファイル使用による認証を試みたが、そのプロファイルのパスワードが期限切れになっている場合。

セキュリティ管理者がパスワードセキュリティポリシーを変更し、既存のプロファイルがそのパスワードセキュリティポリシールールに適合しなくなっても、ユーザがすでにシステムにログインしている場合には、何のアクションも起こりません。ユーザは、パスワードセキュリティ制限に適合しないプロファイルを使用して認証を試みたときに初めて、パスワードを変更するよう求められます。

ユーザがパスワードを変更すると、セキュリティ管理者によって古いプロファイルに設定されているライフタイムパラメータが、新しいパスワードのライフタイムパラメータとして引き継がれます。

dot1xなどの非インタラクティブクライアントでは、パスワードの期限が切れると、適切なエラーメッセージがクライアントに送られます。クライアントは、セキュリティ管理者に連絡してパスワードを更新する必要があります。

ユーザ再認証ポリシー

ユーザがパスワードを変更すると、ユーザの再認証が行われます。

期限満了時にパスワードを変更すると、新しいパスワードに対してユーザ認証が行われます。このような場合、実際には、以前のクレデンシャルに基づいて認証が行われ、データベースで新しいパスワードが更新されます。



(注) ユーザがパスワードを変更できるのは、ログイン中かつ古いパスワードの期限が切れた後のみです。ただし、セキュリティ管理者はこのユーザのパスワードをいつでも変更できます。

フレームド（非インタラクティブ）セッションのサポート

dot1xなどのクライアントがローカルデータベースを使用して認証を行うときには、コモンクライテリアに準拠したパスワードの強度と管理機能が適用されます。ただし、パスワードの期限が切れると、クライアントによるパスワード変更はできなくなります。そのようなクライアントには適切なエラーメッセージが送られます。そのユーザは、セキュリティ管理者にパスワードの変更を要求する必要があります。

コモンクライテリアに準拠したパスワードの強度と管理の設定方法

次の各項では、パスワードの強度と管理の設定について説明します。

パスワードセキュリティポリシーの設定

パスワードセキュリティポリシーを作成し、そのポリシーを特定のユーザプロファイルに適用するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	aaa new-model 例： Device(config)# aaa new-model	AAA をグローバルにイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	aaa common-criteria policy <i>policy-name</i> 例： Device (config) # aaa common-criteria policy policy1	AAA セキュリティパスワードポリシーを作成し、コモンクライテリア設定ポリシー モードを開始します。
ステップ 5	char-changes <i>number</i> 例： Device (config-cc-policy) # char-changes 4	(任意) 古いパスワードから新規のパスワードへの変更文字数を指定します。
ステップ 6	max-length <i>number</i> 例： Device (config-cc-policy) # max-length 25	(任意) パスワードの最大長を指定します。
ステップ 7	min-length <i>number</i> 例： Device (config-cc-policy) # min-length 8	(任意) パスワードの最小長を指定します。
ステップ 8	numeric-count <i>number</i> 例： Device (config-cc-policy) # numeric-count 4	(任意) パスワード内の数字の数を指定します。
ステップ 9	special-case <i>number</i> 例： Device (config-cc-policy) # special-case 3	(任意) パスワード内の特殊文字の数を指定します。
ステップ 10	exit 例： Device (config-cc-policy) # exit	(任意) コモンクライテリア設定ポリシーモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 11	username <i>username</i> common-criteria-policy <i>policy-name</i> password <i>password</i>	(任意) ユーザプロファイルに特定のポリシーとパスワードを適用します。

	コマンドまたはアクション	目的
	例： <pre>Device(config)# username user1 common-criteria-policy policy1 password password1</pre>	(注) 単一の数字はパスワードとして使用できません。単一の数字でパスワードを設定しようとすると、次のコンソールメッセージが表示されます。 <pre>username user2 common-criteria-policy Hay_passwd_policy_2 password 3 % Incomplete command.</pre>
ステップ 12	end 例： <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。

コモンクライテリアポリシーの確認

すべてのコモンクライテリアセキュリティポリシーを確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： <pre>Device> enable</pre>	特権 EXEC モードをイネーブルにします。
ステップ 2	show aaa common-criteria policy name policy-name 例： <pre>Device# show aaa common-criteria policy name policy1 Policy name: policy1 Minimum length: 1 Maximum length: 64 Upper Count: 20 Lower Count: 20 Numeric Count: 5 Special Count: 2 Number of character changes 4 Valid forever. User tied to this policy will not expire.</pre>	特定のポリシーのパスワードセキュリティポリシー情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	<p>show aaa common-criteria policy all</p> <p>例 :</p> <pre>Device# show aaa common-criteria policy all</pre> <hr/> <pre>Policy name: policy1 Minimum length: 1 Maximum length: 64 Upper Count: 20 Lower Count: 20 Numeric Count: 5 Special Count: 2 Number of character changes 4 Valid forever. User tied to this policy will not expire.</pre> <hr/> <pre>Policy name: policy2 Minimum length: 1 Maximum length: 34 Upper Count: 10 Lower Count: 5 Numeric Count: 4 Special Count: 2 Number of character changes 2 Valid forever. User tied to this policy will not expire.</pre>	<p>設定されたすべてのポリシーのパスワードセキュリティポリシー情報を表示します。</p>

コモンクライテリアに準拠したパスワードの強度と管理の設定例

次の項では、コモンクライテリアに準拠したパスワードの強度と管理の設定例を示します。

例：コモンクライテリアに準拠したパスワードの強度と管理

次の例は、コモンクライテリアセキュリティポリシーを作成し、特定のポリシーをユーザプロファイルに適用する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa common-criteria policy policy1
Device(config-cc-policy)# char-changes 4
Device(config-cc-policy)# max-length 20
Device(config-cc-policy)# min-length 6
Device(config-cc-policy)# numeric-count 2
Device(config-cc-policy)# special-case 2
Device(config-cc-policy)# exit
Device(config)# username user1 common-criteria-policy policy1 password password1
Device(config)# end
```

コモンクライテリアに準拠したパスワードの強度と管理に関するその他の参考資料

RFC

RFC	タイトル
RFC 2865	<i>Remote Authentication Dial-in User Service</i> (リモート認証ダイヤルインユーザ サービス)
RFC 3576	『 <i>Dynamic Authorization Extensions to RADIUS</i> 』

コモンクライテリアに準拠したパスワードの強度と管理の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: コモンクライテリアに準拠したパスワードの強度と管理の機能情報

機能名	リリース	機能情報
コモンクライテリアに準拠したパスワードの強度と管理	Cisco IOS Release 15.2(7)E1	この機能が導入されました。