



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、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機能の設定例（7 ページ）](#)
- [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（9 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

- vty 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

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ブ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カ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ブートした場合、そのパスワードはシステムリブート後1ヵ月間有効になります。

月数を使用してライフタイムを設定すると、ポリシーは、指定された月の日数に関係なくライフタイムを30日に設定します。

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、AAAデータベースが更新され、ユーザーは新しいパスワードで認証されます。

- 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

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ープロファイルに適用するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa common-criteria policy *policy-name***
5. **char-changes *number***
6. **max-length *number***
7. **min-length *number***
8. **numeric-count *number***
9. **special-case *number***
10. **exit**
11. **username *username* common-criteria-policy *policy-name* password *password***
12. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	Device> enable	
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 をグローバルに有効にします。
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。

	コマンドまたはアクション	目的
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 username common-criteria-policy policy-name password password 例： Device(config)# username user1 common-criteria-policy policy1 password password1	(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。
ステップ 12	end 例： Device(config)# end	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、次の作業を実行します。

手順の概要

1. **enable**
2. **show aaa common-criteria policy name policy-name**
3. **show aaa common-criteria policy all**

手順の詳細

ステップ 1 enable

特権 EXEC モードをイネーブルにします。

例：

```
Device> enable
```

ステップ 2 show aaa common-criteria policy name policy-name

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。

例：

```
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.
```

ステップ3 show aaa common-criteria policy all

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。

例：

```
Device# show aaa common-criteria policy all
=====
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.
=====
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.
=====
```

トラブルシューティングのヒント

debug aaa common-criteria コマンドを使用して、AAA コモンクライテリアをトラブルシューティングします。

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機能の設定例

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
```

その他の参考資料

次の項で、RADIUS パケット オブ ディスコネクト機能に関する参考資料を紹介します。

関連資料

関連項目	マニュアルタイトル
AAA	『Cisco IOS XE Security Configuration Guide, Securing User Services, Release 2』の「Authentication, Authorization, and Accounting (AAA)」
セキュリティ コマンド	『Cisco IOS Security Command Reference』
CLI 設定	『Cisco IOS XE Configuration Fundamentals Configuration Guide, Release 2』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェアリリース、およびフィーチャセットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2865	『 <i>Remote Authentication Dial-in User Service</i> 』
RFC 3576	『 <i>Dynamic Authorization Extensions to RADIUS</i> 』

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	http://www.cisco.com/en/US/support/index.html

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 トレー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		<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機能は、ユーザーパスワードを指定するルールの保存、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。</p> <p>次のコマンドが導入または変更されました。aaa common-criteria policy、debug aaa common-criteria、およびshow aaa common-criteria policy。</p>

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。