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。

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、認可、アカウンティング（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。

- 機能情報の確認 （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の制約事項 （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 （9 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

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、英字の大文字小文字、数字、特殊文字（「!」、「@」、「#」、「$」、「%」、「^」、「&」、「*」、「(」、「)」）を任意に組み合わせたパスワードの作成が許可されています。

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。

パスワードの有効期限ポリシー

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。再試行の回数は、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 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： `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。
ステップ 4	**aaa common-criteria policy** *policy-name* 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** *number* 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** *number* 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** *number* 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** *number* 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** *number* 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.
==========================================================================
```

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

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

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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

RFC

RFC	Title
RFC 2865	*Remote Authentication Dial-in User Service*（リモート認証ダイヤルイン ユーザ サービス）
RFC 3576	『*Dynamic Authorization Extensions to RADIUS*』

シスコのテクニカル サポート

説明	Link
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。 お使いの製品のセキュリティ情報や技術情報を入手するために、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。 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。	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 15.0(2)SE Cisco IOS 15.2(1)E	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。 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**、**show aaa common-criteria policy**