



パスワード暗号化



m:
<https://pandorafms.com/manual/!778/>
Permanent link:
https://pandorafms.com/manual/!778/ja/documentation/pandorafms/technical_annexes/08_password_encryption
2024/12/03 19:30





パスワード暗号化

[Pandora FMS ドキュメント一覧に戻る](#)

Pandora FMS はデータベース上のパスワードの暗号化に対応しています。

暗号化キーは、ユーザが用意するパスフレーズから生成され、(キーやパスフレーズも含め)データベースには保存されません。これにより、データベースのダンプからパスワードを再現することはできません。

ユーザがパスワードを設定すると、暗号化はユーザーに対して透過的に機能します。

ユーザが入力したパスワードが失われた場合、Pandora FMS データベースに保存されているパスワードを回復することはできません。安全な場所に保存するか、config.php および pandora_server.conf ファイルのバックアップを作成してください。

技術詳細

パスワードは、128bit の Rijndael cipher の ECB モードを使って暗号化しています。パスフレーズの MD5 から、最初に 256bit のキーが生成されます。

新規インストールの Pandora FMS での設定

キー暗号化を有効にするには、Pandora FMS サーバと Web コンソールの両方でパスワードを設定する必要があります。

暗号化の手順は次の通りです。

- コマンドセンター (メタコンソール) と ノード の両方でサーバを停止します。
- /etc/pandora/pandora_server.conf 内の encryption_passphrase および、ノード および コマンドセンター(メタコンソール) 双方の /var/www/html/pandora_console/include/config.php を更新します。

```
$config["encryption_passphrase"]="あなたの暗号化パスフレーズ";
```

- ノード および コマンドセンター(メタコンソール) 両方の暗号化スクリプトを起動します。

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

変更を加えてスクリプトを実行した後、Pandora FMS サーバを再起動する必要があります。

暗号化パスワードの変更

暗号化パスワードが漏洩した場合には、それを変更することができます。まず、データベースに保存されているパスワードを復号化する必要があります。

```
/usr/bin/pandora_encrypt_db -d /etc/pandora/pandora_server.conf
```

その後、暗号化パスワードを変更し（[新規インストールでの設定のセクション](#)で説明したように）、再度暗号化することができます。

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

7.0NG 739以降には、[安全な認証管理](#)が含まれています。この処理を正しく完了するには、次の章を参照してください。

認証情報管理:

暗号化されたデータベースがある場合、データを失うことなく資格情報管理を引き続き使用するには、`tcredential_store` テーブルを除くすべてのデータを復号化します。

そのためには、以下のコマンドを実行します。

```
/usr/bin/pandora_encrypt_db -d -c /etc/pandora/pandora_server.conf
```

暗号化が解除されます。

暗号化を解除したら、再度暗号化を行います。

```
/usr/bin/pandora_encrypt_db /etc/pandora/pandora_server.conf
```

初回の暗号化では、最後のコマンドを実行します。

暗号化パスワードの削除

Pandora FMS に保存されるすべてのパスワードを暗号化しておくことをお勧めします。

- コマンドセンター(メタコンソール) と ノード 双方のサーバを停止します。
- コマンドセンター(メタコンソール) と ノード の両方で復号化スクリプトを起動します。

```
/usr/bin/pandora_encrypt_db -d /etc/pandora/pandora_server.conf
```

- コマンドセンター (メタコンソール) と ノード の両方で、`/etc/pandora/pandora_server.conf` と `/var/www/html/pandora_console/include/config.php` の `encryption_passphrase` をコメントアウトします。

```
# $config["encryption_passphrase"]="your encryption passphrase";
```

変更を加えてスクリプトを実行した後は、Pandora FMS サーバを再起動することを忘れないでください。

[Pandora FMS ドキュメント一覧に戻る](#)