[資料 C] 安全なハッシュ方式 PBKDF2 を使おう

Open Source Solution Technology Corporation
HAMANO Tsukasa <info@osstech.co.jp>
オープンソースカンファレンス 2015 .Enterprise

1 概要

OpenLDAP はデフォルトでは SSHA(SALT 付き SHA1) でパスワードをハッシュ化します。クラウドコンピューティングや GPU の登場により、計算リソースがより安価になった現在、もはやこの方法は安全とは言えません。SHA2 であっても同様に総当り攻撃に対して脆弱です。

より安全で未来に順応する PBKDF2 を使いましょう。

2 PBKDF2 モジュールで利用可能なスキーマ

- {PBKDF2} - {PBKDF2-SHA1}の別名
- {PBKDF2-SHA1}
- {PBKDF2-SHA256}
- {PBKDF2-SHA512}

3 メッセージフォーマット

```
{PBKDF2}<Iteration>$<Adapted Base64 Salt>$<Adapted Base64 DK>
```

4 ハッシュの生成方法

```
$ /opt/osstech/sbin/slappasswd -o module-load=pw-pbkdf2.la -h {PBKDF2} -s secret
{PBKDF2}10000$MK6XC0/DMbzzlaAI5cdoJg$Hg/A7JcQJ0XrpiO54auaKh0a9zo
```

※この方法ではラウンド数が固定 (10000 回) です。

5 Python PassLib でハッシュを生成する

```
#!/usr/bin/env python

from passlib.hash import ldap_pbkdf2_sha1
print(ldap_pbkdf2_sha1.encrypt("secret", rounds=10000))
```

6 LDIF 例

```
dn: cn=test,dc=example,dc=com
objectClass: person
cn: test
sn: test
userPassword: {PBKDF2}10000$MK6XC0/DMbzzlaAI5cdoJg$Hg/A7JcQJ0XrpiO54auaKh0a9zo
```