メッセージダイジェスト

[Java]

```
/*
 * create : 2004/12/22
 * creator: yagi
 * version: 1.0
 * summary:
 *
 * history:
 *  1.0 新規作成
 */
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;

public class Security {
    /**
     * MessageDigest インスタンス
     */
    private static MessageDigest md = null;

    /**
     * 暗号化に使用するアルゴリズム
     */
    public static final String DIGEST_ALGORITHM = "SHA";

    /**
     * パスワードをハッシュ関数 ( 一方向要約関数 ) で、暗号化する
     * @param orginalPassword
     * @return
     * @throws NoSuchAlgorithmException
     */
    public static String getCryptPassWord(String orginalPassword) throws NoSuchAlgorithmException {

        byte[] digest = getDigest(orginalPassword.getBytes());

        StringBuffer sb = new StringBuffer();
        for(int i = 0; i < digest.length; i++) {
            sb.append(Integer.toHexString((digest[i] >> 4) & 0x0f));
            sb.append(Integer.toHexString( digest[i] & 0x0f));
        }
        return new String(sb);
    }

    /**
     * 暗号化前のパスワードと暗号化後のパスワードを比較する
     * @param orgPass
     * @param cryptPass
     * @return
     * @throws NoSuchAlgorithmException
     */
        public static boolean checkPassword(String orgPass, String cryptPass) throws
NoSuchAlgorithmException {
        return MessageDigest.isEqual(
            getCryptPassWord(orgPass).getBytes(),
            cryptPass.getBytes());
    }

    /**
     * 暗号化後のハッシュ値の桁数を取得する
     * @return
     * @throws NoSuchAlgorithmException
     */
    public static int getDigestLength() throws NoSuchAlgorithmException {
        return getMessageDigetst().getDigestLength();
    }

    /**
     * ダイジェストを取得する
     * @param val
     * @return
     * @throws NoSuchAlgorithmException
     */
    private static byte[] getDigest(byte[] val)
        throws NoSuchAlgorithmException {
```

```
        getMessageDigetst().update(val);
        byte[] digest = getMessageDigetst().digest();
        resetDigest();

        return digest;
    }

    /**
     * MessageDigest のインスタンスを取得
     * @return
     * @throws NoSuchAlgorithmException
     */
    private static MessageDigest getMessageDigetst() throws NoSuchAlgorithmException {
        if (md == null) {
            md = MessageDigest.getInstance(DIGEST_ALGORITHM);
        }
        return md;
    }

    /**
     * MessageDigest のインスタンスを初期化
     * @throws NoSuchAlgorithmException
     */
    private static void resetDigest() throws NoSuchAlgorithmException {
        getMessageDigetst().reset();
    }
}
```