学生向けポータルサイトにおける個人認証システムの構築
Construction of a personal authentication system on the Student Portal

嶋田　理博
Michihiro Shimada

要旨

奈良学園大学保健医療学部ポータルサイト上で、学生個人ごとのコンテンツやサービスを提供するため、個人認証システムを構築した。構築したシステムは、パスワードの平文を扱わずに認証を行えるダイジェスト認証と、パスワードのオンライン自動発行機能から構成されている。システムは約２年間稼働しており、その間にのべ約400名のユーザが利用し、約1,000個のパスワードを発行した。

キーワード：学生ポータルサイト　パスワード　ダイジェスト認証

Ⅰ．はじめに

筆者は、奈良学園大学保健医療学部において、2014年の開設年度に保健医療学部ポータルサイト（以下単に「ポータルサイト」という）を立ち上げ、以来、運営・管理を行っている。ポータルサイトは、主に学生向けのウェブサイトである。教員・事務局からの講義資料や連絡、教材や文献へのリンク、教員のメールアドレスや研究室、オフィスアワーの一覧など、学修や学生生活に必要な情報を一箇所で入手できるよう集約し、学生へ利便性を提供している（図１）。

図１　保健医療学部ポータルサイト

ポータルサイトには、講義資料のように多数の学生へ共通に提供するコンテンツが多いが、看護技術セルフトレーニングのベッド予約、看護技術チェックの評価履歴、臨地実習時の看護技術経験録・自己評価の記録・閲覧など、学生個人ごとのコンテンツで、個人認証が必要とされるコンテンツもある。そのため、2016年度に、ポータルサイト上で個人認証を行うシステム（以下単に「本システム」という）を構築することとした。

本論文では、本システムの技術的解説と、利用実態の報告を行う。

Ⅱ．システムの構成

1. 認証の方法

本システムでは、ユーザは、ユーザ名（学籍番号）とパスワードを用いて、ポータルサイトにログインし、ポータルサイト内の個人別コンテンツにアクセスする。認証方式は、パスワードの盗聴や改竄を防ぐため、パスワードそのものは通信せず、ハッシュ値で認証を行うダイジェスト認証[1][2]を用いている。

ダイジェスト認証は、下記①～⑤の手順で行う（図２）。

① ユーザがポータルサイト内の認証が必要なページにアクセスする。

② サーバが「ノンス文字列」を生成し、「レルム文字列」とともにクライアントに送る。「ノンス文字列」は認証のつど生成される使い捨てのランダムな文字列である。盗聴者からのリプレイ攻撃を防ぐためのセッショントークンとして使われる。また、「レルム文字列」は、クライアントのパスワードダイアログに表示される文字列である。

③ クライアントに「ユーザ名」「パスワード」の入力を促すダイアログと「レルム文字列」が表示される。

④ ユーザが「ユーザ名」「パスワード」を入力すると、サーバが生成したものとは別の「ノンス文字列」をクライアントも生成し、「ユーザ名」「パスワード」「レルム文字列」「ノンス文字列」（サーバで生成したものと、クライアントで生成したものの２つ）を元にした文字列のMD5ハッシュ値[3]と「ノンス文字列」をサーバに送信する。

⑤ サーバ上のデータベースには「ユーザ名」「パスワード」「レルム文字列」を元にした文字列のMD5ハッシュ値を保存している。サーバは、クライアントから送信されてきた「ノンス文字列」とデータベースに保存されているMD5ハッシュ値とを用いて計算したMD5ハッシュ値、同じくクライアントから送信されてきた「ユーザ名」「パスワード」「レルム文字列」「ノンス文字列」を元にした文字列のMD5ハッシュ値とを比較する。一致すれば認証成功で、個人ごとのコンテンツページへ遷移し、一致しなければ認証失敗で、認証失敗メッセージを表示するページへ遷移する。

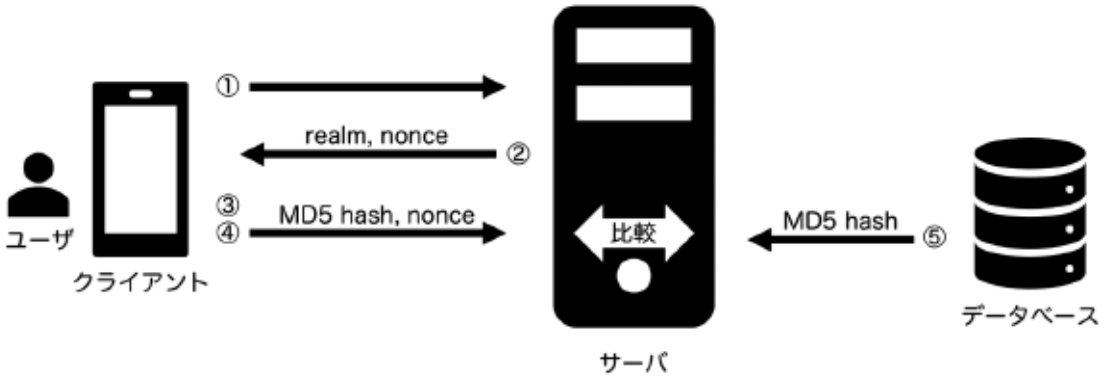

図２　ダイジェスト認証におけるクライアント⇔サーバ間の通信

以上の手順により、「パスワード」そのものをデータベース内に保存したり、送信したりすることなく認証することが可能である。

2. パスワードの発行

認証に用いるパスワードは、学内のPCログインやメール送受信などに使用しているActiveDirectoryのアカウントと連動することも可能であるが、本システム独自のアカウント、パスワードにより個人認証を行っている。理由は、ActiveDirectoryのアカウントと連動させると、システムの構築・管理が大がかりになってしまうことと、後述するように、ユーザがパスワードを忘れた場合に容易に再発行できるようにするため、そして、非常勤講師や卒業生など大学のアカウントを持たないユーザに、将来サービスを提供する可能性を考えてのことである。

ユーザ名は学籍番号で在学中変わることはないが、パスワードは任意のタイミングでオンラインで発行（再発行）できるようにしている。ユーザはパスワードを忘れてしまうことがしばしばあるが、パスワードを忘れても、管理者に負担をかけずに再発行対応ができるようにするためである。

オンラインでのパスワード発行は、下記①～③の手順で行う。

① ユーザが、パスワード発行ページにユーザ名（学籍番号）を入力し、パスワード発行をシステムに依頼する。
② サーバからユーザのメールアドレス宛に、パスワード発行リクエストのアドレスが送られる。
③ ②の時刻から指定制限時間以内に、ユーザがそのアドレスにアクセスすると、ユーザのメールアドレス宛に発行（再発行）されたパスワードが送られる。

最初のリクエストでパスワードを発行せず、ユーザのメールアドレス宛にパスワード発行リクエストのアドレスを送る、という手順を踏んでいるのは、①のユーザ名（学籍番号）入力が、他人でもできてしまうため、不正な発行を防ぐためである。指定制限時間を設けているのは、過去のメールに記載のアドレスに誤ってアクセスしてしまい、パスワードを再発行してしまうことを防止するためである。

パスワード発行リクエストおよびパスワード本体は、下記Ａ～Ｅのデータにより構成し、改竄チェックおよびエラーチェックを行い、生成している。実際に送受信に使う際には、データはBase64[4][5]によりエンコードし、6bitのデータを英数字１文字として表現している。括弧内の数字がその文字数である。Base64の本来の仕様では、エンコードした文字列の文字数が４の倍数でない場合、４の倍数になるように末尾にイコール（=）を追加して文字数を調整するが、本システムではそのような文字数の調整は行っていない。

Ａ）リクエスト時刻（UNIXタイムスタンプ） … 30bit（５文字）
Ｂ）ユーザ名（学籍番号） … 24bit（４文字）
Ｃ）Ａ+Ｂ+「ソルト文字列」のMD5ハッシュ値 … 128bit（通信しない）
Ｄ）Ｃの１bit目～60bit目 … 60bit（10文字）
Ｅ）Ｃの61bit目～108bit目 … 48bit（８文字）

「ソルト文字列」は、MD5ハッシュ値を計算する文字列に付加する適当な文字列である。付加することにより、MD5ハッシュ値から元の文字列を解読したり、リクエストを改竄したりすることが難しくなる。「ソルト文字列」は、管理者が定め秘匿しておく。

パスワード発行リクエストのアドレスには、上記Ａ+Ｂ+Ｄの文字列を含める。この文字列により、以下の３つのチェックが可能となる。

・リクエストが改竄されていないかどうかのチェック

・リクエストが指定制限時間内かどうかのチェック

・ユーザ名（学籍番号）が有効で、そのユーザが在籍しているかどうかのチェック

以上３つのチェックで問題がないことを確認したら、上記Ｅの文字列をパスワードとして確定する。Ｅの文字列には時刻の情報が関係しているので、同じユーザであっても、発行するたびにパスワードは異なるものとなる。サーバはユーザのメールアドレス宛に、Ｅの文字列を確定したパスワードとして送るとともに、「ユーザ名」とＥの文字列のMD5ハッシュ値をデータベースに記録する。パスワード本体はデータベースには記録しない。

Ⅲ．利用の実態

本システムが稼働を開始した2016年８月から2018年６月までの23ヶ月間の、月別、学年別のパスワード発行数（再発行含む）の推移を表１に示す。なお、学部一期生が2014年入学なので、2016年度の４年生はいない。また、５年生以上は４年生に含めて数えている。

表１　月別、学年別のパスワード発行数の推移

年	月	１年生	２年生	３年生	４年生	合計
2016	8	2	5	69		76
	9	1	1	10		12
	10	78	1	2		81
	11	25	0	5		30
	12	2	0	1		3
2017	1	4	0	0		4
	2	0	1	0		1
	3	0	0	3		3
2017	4	1	20	0	10	31
	5	0	6	1	0	7
	6	0	18	0	1	19
	7	2	0	0	0	2
	8	0	3	122	17	142
	9	0	0	1	0	1
	10	102	0	1	0	103
	11	18	1	0	1	20
	12	6	0	1	0	7
2018	1	1	0	1	0	2
	2	0	0	79	19	98
	3	0	0	3	0	3
2018	4	102	3	0	1	106
	5	76	26	5	5	112
	6	12	77	0	13	102

パスワードののべ発行総数（再発行含む）は965である。これは、学生１人あたり、年間1.6回パスワードを発行していることに相当する。

表１からは、パスワードの発行が特定の時期に集中していることが分かる。これは、演習科目や実習科目で、ポータルサイト内の個人パスワードが必要なコンテンツへのアクセスが必要となり始める時期と関係している。2016年と2017年の10月に、１年生の個人パスワード発行が多いのは、「基礎看護技術演習Ⅰ」のセルフトレーニングのベッド予約、および、技術チェック閲覧に必要となるためである。2018年度から、当該科目の開講期が前期となったため、2018年は１年生の個人パスワード発行は４月に多くなっている。また、2016年と2017年の８月に、３年生の個人パスワード発行が多いのは、各看護学領域別臨地実習で看護技術経験録・自己評価の記録・閲覧に必要となるためである。2018年２月も３年生の個人パスワード発行が多いのは、学期末に看護技術経験録・自己評価をまとめて記録する学生が多かったためと思われる。

Ⅳ. まとめ

ポータルサイトにおける個人認証システムは約２年間問題なく稼働しており、その間に約1,000のパスワードを発行・管理することできた。ユーザ数数百名程度の小規模なウェブサイトで、ユーザ個人ごとのコンテンツやサービスを提供する目的に相応しいシステムであると言える。

今後は、このシステムを拡張し、学生だけでなく、教職員も個人認証ができるようなシステムとし、教職員がポータルサイトに「お知らせ」を掲示したり、担当科目の教材をアップロードする際に、本認証システムを利用するなど、システムの応用と利活用を図ってゆきたい。

参考文献

［１］Franks, J., *et al.* 1997, “An Extension to HTTP : Digest Access Authentication”, RFC 2069.
［２］Franks, J., *et al.* 1999, “HTTP Authentication : Basic and Digest Access Authentication”, RFC 2617.
［３］Rivest, R. 1992, “The MD5 Message-Digest Algorithm”, RFC 1321.
［４］Josefsson, S.(Ed.) 2003, “The Base16, Base32, and Base64 Data Encodings”, RFC 3548.
［５］Josefsson, S. 2006, “The Base16, Base32, and Base64 Data Encodings”, RFC 4648.