G-17

多要素認証を用いた高機能サービスのためのサーバ構成法

The server configuration method using multi-element authentication for highly efficient service

○石濱洋輔[1]
Yosuke Ishihama

A standalone version common authentication system is developed in this research. The free design of a service system is enabled by making an authentication system independent, and a common authentication server realizes all change of the authentic method accompanying change of a service system of future service contents. As main functions, a multi-element controlling function, "Single Sigh on" function, an authentication level control facility...etc. are held. By doing so, strengthening of the security of the conventional authentication, improvement in usabiliity, and mitigation of a developer's burden are aimed at.

1.研究背景

2005 年頃からクラウドコンピューティングや SaaS(Software as a Service)が普及し，それに伴い認証の必要性が増加している．また，現在のネットワークサービスでは，個々のサービスが認証方式を含めてすべて管理している． 新しい認証方式や，複数認証を組み合わせて使用すれば，認証の信頼度は向上するが，システム全体の改造となるため新しい認証方式や，複数の認証方式の組み合わせを導入するには，サービス管理者に認証についての知識が必要であることや，認証システムを構成する技術が必要である．

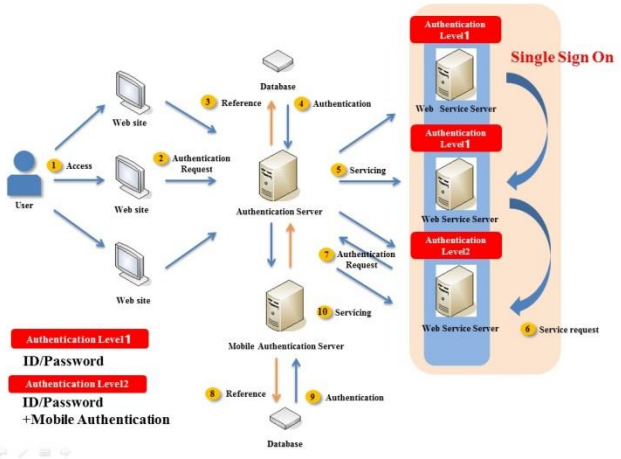

Figure1. Composition of a common authentication server

2. 研究目的

本研究では，多要素認証を用いた高機能サービスのための，認証方式の管理，円滑な認証をするためのサーバ構成法を用いた独立した共通認証サーバの提案，実現を目的とする．

3.サーバ構成法

サーバ構成の図を以下に示す．

本研究の共通認証システムは，多要素認証管理機能，Single Sign On 機能，レベル制御機能を保持している．

3.1.多要素認証管理

認証サーバでは様々な認証方式を管理し，その認証を組み合わせて Web サービスを提供する．

新しい認証方式を追加する場合は，認証サーバのデータベースへ新しい認証方式の URI を登録することで認証を受けられるようになる．

1：日大理工・学部・子情

3.2. Single Sign On

Single Sign On とは最初に 1 回認証に成功すれば,以降は利用するシステムが変わっても，利用が許可されているシステムであれば認証プロセスを経ることなくそのまま利用できる認証システムである．今回はその中でも，リバースプロキシ型 SSO システムを用いる．リバースプロキシ型とはすべての Web サーバへのアクセスを，認証サーバを兼ねたプロキシサーバに集約し，ユーザ認証を行う方式である．

クライアントがログインに成功すると，認証サーバは目的のサーバに代行アクセスする．

3.3.認証レベル制御機能

認証レベル制御機能とは SSO(Single Sign On)により認証レベルの違う Web サイトへアクセスした場合に制御を行う機能である．例えば，認証レベル 1 (ID/パスワード認証)の Web サービスに認証済みのクライアントから，認証レベル 2 (ID/パスワード認証＋携帯認証)の Web サービスへ SSO(Single Sign On)で移動する場合は，認証の差分である携帯認証をユーザに行ってもらうことでその Web サービスを受けることができる．一方，認証レベル 2 (ID/パスワード認証+携帯認証)の Web サービスに認証済みのクライアントはそれ以下の認証レベルの Web サービスを受けることができる。認証プロセスを以下に示す.

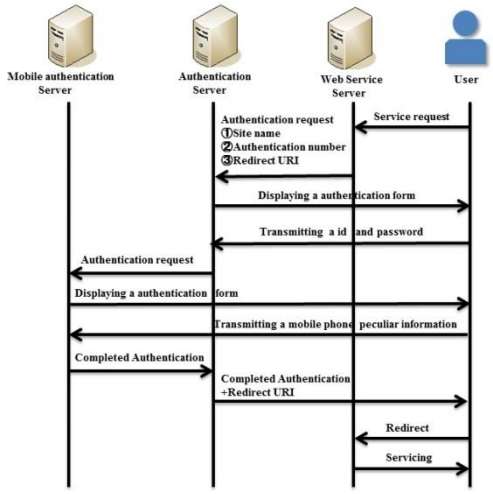

Figure2. Authentication process

(a)認証方式の決定

ユーザが Web サービスサーバにサービス要求し，ネットワークサービスサーバが，認証が必要だと判断すると，認証サーバへそのユーザが使用すべき認証方式コードを送信する．認証サーバはそのコードを用い，使用する認証に対応した情報を認証サーバ内のデータベースから取り出す.

(b)ユーザ認証

(a)のように認証方式が決定された後，認証サーバは使用する認証方式に対応した入力ドームのアドレスを Web サービスサーバに送り，Web サービスサーバはその URI にユーザを誘導する．ユーザが入力フォームでデータを入力し，認証サーバが生起の認証データと照合することで認証を完了する．

認証が完了すると，認証サーバはリダイレクト情報をユーザに送信する．ユーザはリダイレクト情報を基にリダイレクトすることで，要求したサービスを受けることができる．

5.結果

①ID/パスワードを 1 つにすることができるため，複数の ID/パスワードをメモ帳などに残すというようなセキュリティの面でのリスクがなくなり，厳格なパスワード管理が実現できる．

②Single Sign On 機能により，何度も識別情報を入力する必要がなく，システム利用での労力やストレスが軽減される．

③共通認証サーバが認証方式を管理するため，Web サービスサーバ管理者は認証に関する専門知識を必要としなくなり，負担を軽減できる．

6.参考文献

[1]よくわかる PHP の教科書, 303p, 2011 年 4 月 1 日発行