G-36

多要素認証における自由な要素管理を可能にする認証システム

Multi-factor authentication system enables flexible factor management for network services

木村美里[1]，○ 木村美幸[1]，　木原雅巳[2]
Misato Kimura[1]，　*Miyuki Kimura[1]，　Masami Kihara[2]

Multi-factor authentication is being added to a number of different procedures. One of the most well-known examples is the ATM in banks; they require pin numbers and finger prints. Since new technologies for authentication are being developed, flexible utilization of various combinations of those methods is required to improve authentication strength. This paper proposes a multi-factor authentication system that can flexibly manage the key factors, and describes a system design to achieve independent and shared authentication servers.

1. はじめに

近年クラウドコンピューティングや SaaS(Software as a Service)の普及に伴い，サービスを利用する際に認証が必要なネットワークサービスが増加している．認証にはユーザ ID とパスワードを組み合わせて実装する ID/パスワード認証が多く用いられている．資産や個人情報のように，さらに確実に管理されるべきコンテンツを取り扱うサービスにおいては，ID/パスワード認証単体を実装するような単一認証ではなく，複数の認証を組み合わせるシステムが増加している．本論文では，複数の認証方式を組み合わせて使用する多要素認証システムにおいて，認証方式の追加や削除を自由に行うことができる，認証方式管理機能をもつ独立した共通認証サーバの設計法について述べる．

2. 多要素認証

近年 ID/パスワードなどの不正利用が増加していることから，銀行の ATM のように認証方式を複数にして利用者特定の信頼度を上げるサービスが増えている．しかし，従来の複数要素を利用するサービスにおいては，提供される認証の組み合わせは固定である．

これに対して，認証要素数を変えることで認証信頼度を変化させることができれば，利用料などでコンテンツ利用方法を管理できない場合でも，利用者に提供するコンテンツの品質によって，適切な信頼度をもつ認証方式を実現することができる．たとえばコンテンツの品質やコンテンツの利用範囲などを自由に管理することができる．

現在，実現可能な認証方式としては，ID/パスワード認証・マトリクス認証・携帯電話認証・メールチャネル認証・伝送遅延認証・位置情報認証・機器認証・IP アドレス認証などを挙げることができる．本論文では，このような複数の認証要素を自由に増減できる多要素認証システムを提案する．

3. 共通認証サーバの必要性

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を管理している．2.で述べたように，新しい認証方式が考えられ，複数の認証方式を使用すれば，認証の信頼度は向上するが，システム全体の改造となるので新しい認証方式を導入するには課題が多い．

認証に関するこのような問題を解決する方法として，本論文では，複数のネットワークサービスで共通に使用することができる共通認証サーバを提案する．認証方式をネットワークサービス本体から切り離してシステム設計ができれば，サービス内容の変化にともなう認証方式の変更にも柔軟に対応することができる。

4. 共通認証システムの必須要素

共通認証サーバに必要な機能は以下の 3 点である．

・異なる認証方式を使用するネットワークサービスに対応できること
・多要素の認証方式に対応すること
・新しい認証方式に対応できるように，認証方式の追加が可能であること

共通認証サーバに必要な要素には，

・認証方式情報
・ネットワークサービス情報
・ユーザ認証情報
・サーバ間で共通するセッション情報

などがある．

さらに，ネットワークサービスとの認証方式を含むユーザ情報の受け渡し機能，利用者の初期設定

１：日大理工・学部・子情　２：日大理工・教員・子情

機能などを共通認証サーバに追加することができる．これにより，ネットワークサービス本体は，最小限のユーザ情報だけを管理し，その他のユーザ管理をすべて共通認証サーバに依頼することが可能となる．

5. 認証方式の管理

認証サーバでは様々な認証方式を搭載し，その認証を組み合わせてネットワークサービスに提供する．

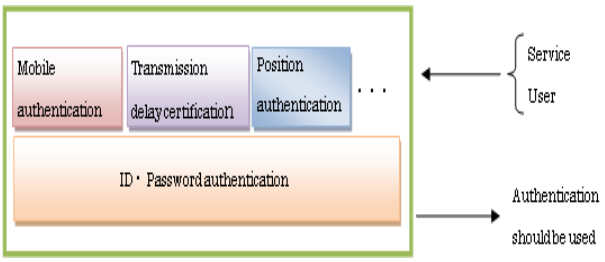

Figure 1. Authentication configuration

ネットワークサービスとそのユーザ情報を，サービスの初期登録時に認証管理情報として保存することによって，ユーザアクセスごとの認証要求に確実に対応する．ユーザ情報には，必要な認証の種類と，認証データが格納される．

新しい認証方式が可能になった場合には，ネットワーク側から，ユーザ情報の更新を受けることで，新しい認証方式が利用可能になる．ユーザへの認証方法の変更通知も，共通認証サーバが代行できる．

6. 共通認証システムの構成

6.1 サーバ間の連携

共通認証サーバでは，利用する認証方式の種類と数が，ネットワークサービスごとに異なる．認証方式によっては，サーバ自体が異なる．提案する共通認証システムでは，伝送遅延認証サーバ，位置認証サーバなどが別サーバで運用されるため，これらのサーバと連携をとる必要がある．

サーバ間連携では、ユーザを次の認証へ導くために，セッションデータを共有する必要があり，セッションハンドラをデータベースによって共通管理し，サーバ間で受け渡す仕組みを導入する．この仕組みは，複数のサービスからなる複合型サービス提供にも必須となる．

ユーザの共通認証サーバ，その他認証サーバ，コンテンツサーバ間のスムーズな移動を実現するために，セッションハンドラと同様に，ユーザ情報，クッキーやセッション・ユーザ認証に関する情報が含まれるリクエストを共通管理することも必要である．提案システムではユーザテーブル，リクエストテーブルを作成し，サービス間で共有する仕組みを採用する．このテーブルには，共通認証サーバを利用する場合，認証終了後，サービス側が要求する URI にリダイレクトにより自動的にユーザを誘導するための情報も必要となる．

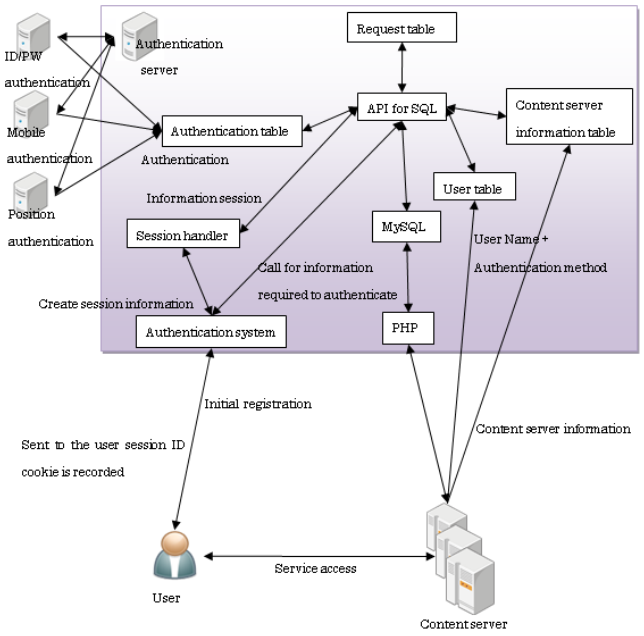

Figure 2. Common authentication system configuration

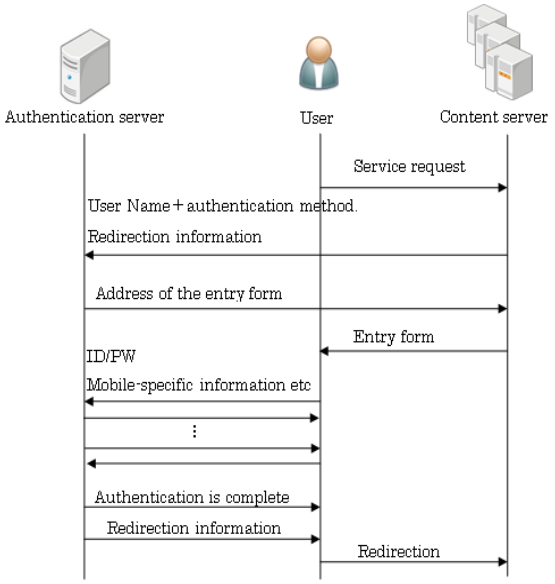

Figure 3. Exchange during authentication

7. まとめ

今回，複数の認証を組み合わせて利用することができる共通認証サーバを提案した．本論文で提案したシステムは，現時点では提案段階であり，これからシステムの構築を行っていく予定である．

参考文献

[1] 山田，他，情報処理学会研究報告，2010