様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年５月２１日現在

機関番号：１１３０１
研究種目：若手研究（Ｂ）
研究期間：2010～2011
課題番号：22700064
研究課題名（和文）多様なセキュリティレベルを包括するユーザ・サイト認証法に関する基礎的研究
研究課題名（英文）A Study on user and site authentication including various security level
研究代表者
北形　元（KITAGATA GEN）
東北大学・電気通信研究所・准教授
研究者番号：20344731

研究成果の概要（和文）：
本研究課題では，申請者の先行研究であるユニバーサルな３次元仮想空間だけではなく，既存のWebサービスを含め，異なるレベルのセキュリティ要求に対し，統合的なユーザ，及びサイト認証を行うための基礎的な技術を開発した．具体的には，ユーザの同一性のみを明らかにする場合，ユーザの所属組織のみを明らかにする場合，年齢や国籍等ユーザの個人的な特徴のみを明らかにする場合，また氏名や住所などまで明らかにする場合など，セキュリティレベルを明確に分類し，それぞれに適した認証方式を自動的に選択・利用可能とする技術の基礎を実現した．

研究成果の概要（英文）：
In this research, including not only universal 3D virtual space but also existing web services, basic technology about integrated user and site authentication method is developed. For instance, various security level such as only identity of users, only organization of users, age and nationality of users, names and address of users. As a result, various security level is categorized, and basic technology to select and enable suitable authentication method is proposed.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	2,400,000	720,000	3,120,000
２０１１年度	800,000	240,000	1,040,000
年度			
年度			
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：サービス構築基盤技術，ユーザ認証，シングルサインオン

１．研究開始当初の背景

Web サービスにおいて，認証技術は，フィッシングのようなサイトのなりすまし，およびユーザのなりすましやスパム行為を防止する極めて重要な技術となっている．サイトのなりすまし防止においては，PKI(Public Key Infrastructure)が一般に広く普及しているが，高いセキュリティを提供する代わりに，管理コストが非常に高く，ショッピングサイトやインターネットオークション，イン

ターネットバンキングなど，金銭取引が発生し高いセキュリティを要求される場面では効果的だが，個人レベルのサイトでの導入は費用対効果が低く，適切ではない．一方で，ユーザの認証においては，極めて高いセキュリティレベルを要求される場合は，電話や郵送などの手段によりユーザの本人確認を行う場合もあるが，一般的には E-mail を信頼の基準としているケースが多く，この場合，登録申請者に E-mail により確認用の一時的なキーを送付し，これをサイトに入力させることにより，正しい E-mail アドレスかどうかを確認するのが一般的である．従来，この E-mail による本人確認はサイト毎に行われており，ユーザに関する氏名や住所などの個人情報は，それぞれの Web サービスを提供する組織が管理することが一般的であった．これに対し近年，ユーザの認証を個々の Web サービスから分離し，１回の認証により，複数のサービスを利用可能とする技術が注目されている．最も大きな注目を集めている技術として，OpenID が挙げられる．OpenID は，2005 年に米 Six Apart 社の Brad Fitzpatrick により考案された，サイト間にまたがるシングルサインオン(SSO)技術である．しかしながら，OpenID は，ユーザの同一性を保証する技術であり，セキュリティレベルは低い．すなわち，OpenID の所有者が，どのような組織に所属し，どのような人物であるのかは分らない．そのため，金銭取引が発生するような高いセキュリティレベルを要求するサイトへの利用は難しい．また，OpenID では個人情報が OpenID 発行サイトに登録される集中管理型の仕組みであり，ユーザ数に対するスケーラビリティが低いという問題があり，また，OpenID 発行サイト毎に，管理される個人情報の種類が異なるため，各 OpenID 発行サイト内に閉じたサービスとなる．

２．研究の目的

本研究課題では，申請者の先行研究であるユニバーサルな３次元仮想空間だけではなく，既存の Web サービスを含め，異なるレベルのセキュリティ要求に対し，統合的なユーザ，及びサイト認証を行うための基礎的な技術を開発する．具体的には，ユーザの同一性のみを明らかにする場合，ユーザの所属組織のみを明らかにする場合，年齢や国籍等ユーザの個人的な特徴のみを明らかにする場合，また氏名や住所などまで明らかにする場合など，セキュリティレベルを明確に分類し，それぞれに適した認証方式を自動的に選択・利用可能とする技術の基礎を開発する．さらに，ユーザがどのレベルまでの個人情報をサイトに通知するかどうかを判断する基準として，サイトがどの組織に運用されているのか，あるいは誰に運用されているのかなど，サイトが要求するセキュリティレベルに応じ，サイトに対しても明確にレベル分けされたサイト運用者情報を要求する仕組みを実現する．すなわち，ユーザに関する個人情報とサイトに関する運用者情報間のネゴシエーションを行い，両者の要求を満足する必要最小限の個人情報，および運用者情報を自動的に選択する基礎的なフレームワークを設計・開発し，評価システムにより，提案技術の有用性を評価する．

３．研究の方法

本研究では，包括型マルチレベル認証の基本アーキテクチャを確立し，包括型マルチレベル認証ミドルウェアの基本設計，包括型マルチレベル認証ミドルウェアの試作，評価用プロトタイプシステムの設計・実装，評価実験，および総合評価を行い，多様なセキュリティレベルを包括するユーザ・サイト認証法の基礎を確立する．具体的には，以下の(A)～(F)の項目について研究を推進する．

(A) 既存関連技術の調査・分析
- 既存のサイト間ユーザ認証技術の調査・分析
- 既存の Web サービスにおけるセキュリティ要求に関する調査・分析
- 解決すべき技術課題の明確化

(B) セキュリティレベルのモデル化
- (A)の分析結果に基づくセキュリティ要求のモデル化
- ユーザの個人情報，およびサイトの運用者情報のモデル化
- セキュリティレベルのモデル化

(C) 包括型マルチレベル認証の基本アーキテクチャの確立
- (B)でモデル化したセキュリティレベルに基づき，ユーザとサイト間におけるセキュリティレベルのネゴシエーション方式の検討
- セキュリティレベルのネゴシエーションのためのコンポーネントの検討
- 包括型マルチレベル認証の基本アーキテクチャの確立

(D) 包括型マルチレベル認証ミドルウェアの開発
- (C)で確立した基本アーキテクチャに基づく，包括型マルチレベル認証 API の基本設計
- 包括型マルチレベル認証ミドルウェアの基本設計
- 包括型マルチレベル認証ミドルウェアの詳細設計と試作

(E) 評価用プロトタイプシステムの設計・実装と評価実験
- 包括型マルチレベル認証ミドルウェアを用いた評価用サービスの設計

・ 上記サービスを実現する評価用プロトタイプシステムの実装
・ 評価用プロトタイプシステムを用いた評価実験

(F) 総合評価（平成２３年度後半）
・ (E)の評価実験の結果を通じ，(A)～(E)全体の総合評価を行う．

４．研究成果

(1) S-P サービス基盤の提案

包括型マルチレベル認証を実現する基盤として，S-P(Socio-familiar Personalized)サービス基盤を提案する．S-P サービス基盤で扱う個人情報を以下に示す．

静的な個人情報：氏名，性別，住所，年齢，趣味嗜好など

動的な個人情報：食事の履歴，その日に摂取可能なカロリー・栄養素，医薬品の服用履歴など

初めて利用する場所でも，あたかもいつも利用しているように個人化されたサービスを実現するためには，上述の個人情報を様々なサービスから共通して利用可能とする必要がある．そこで，サービス基盤を下記の 4 つから構成する．

分散認証基盤(U-PIMM:User-owned Personal Information Management Mechanism)：後述するサービスインタフェース，個人情報サーバ，およびサービス提供サーバ間で公開鍵を分散管理し，PKI 等の集中型の公開鍵基盤を使用せずに，安全な通信路を提供する．

サービスインタフェース：レストラン内のメニュー端末や，バス停など，利用者がサービスを利用する際に用いるインタフェース．

サービス提供サーバ：メニュー提案システムや，バスのアナウンスシステム等，サービスを提供するサーバであり，どのようなサービスを提供するのかを示すサービス情報，および，どのような個人情報を得られると，どのようなパーソナライズが行えるのかを示す，個人情報利用知識を保持する．

個人情報サーバ：上述の個人情報を格納するサーバである．また，どのようなサービスに対して，どのような個人情報を提供してよいかという，個人情報開示知識を保持する．本サーバは，自宅に設置されるホームサーバ等，ネットワークに常時接続し，信頼できるサーバを想定する．サービス提供サーバからフィードバックされるサービス利用履歴に基づき，動的に個人情報を更新する．

(2)個人情報の要求・開示手順

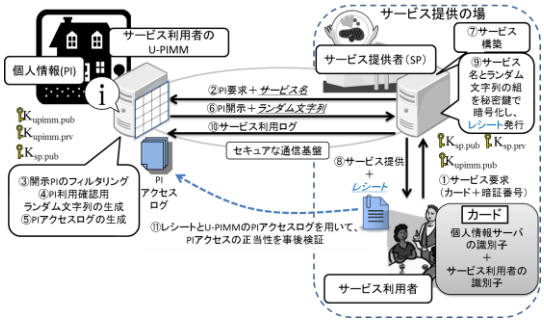

図 1 に個人情報(Personal Information:PI)の要求・開示手順を示す．ユーザが S-P サービス利用する際には，以下のような手順で個人情報を要求・開示し，サービスの個人化のために利活用する．

① ID によるログイン

ユーザは，RFID のカードを用い，ログインし，サービス要求を行う

② 利用知識に基づき，サービスに必要な個人情報を要求

サービス提供者はサービスに必要な個人情報をユーザの個人情報サーバに要求する

③ 開示知識に基づいた PI 解決

個人情報サーバ(U-PIMM)は，サービス提供者からの個人情報要求と開示知識を元に，開示する個人情報を決定する

④ 開示知識などを元に必要最低限の個人情報を開示

サービス提供者に対して，サービスに必要な最低限の個人情報を提示する

⑤ サービス処理

個人情報サーバから取得した個人情報を元に，サービスを処理する

⑥ サービス結果通知

サービスの内容・結果をユーザに通知する

個人情報の要求や開示に関して，サービス提供者は個人情報をいかに要求するか，ユーザは個人情報をいかに開示するか，各々ポリシー持っている．本手順によって，両者の個人情報の扱いに関するポリシーを考慮した上での個人情報の取り扱えるため，高度なサービスの個人化やサービスの連携が可能になる．

(3) 実験と考察

上述の構成要素のプロトタイプを Java 言語を用いて実装した．なお，個人情報，個人情報利用知識，および個人情報開示知識は，RDF データベースを用いた二項関係のルールとして記述し，開示可能な個人情報を導出する機能を，Allegro Common Lisp で実装した．また，サービス例として，レストランのメニュー推薦システムと薬局における医薬

品の購入補助システムを実装した．サービス利用時の個人情報サーバとサービス提供者サーバ間の通信は公開鍵暗号方式で暗号化した上で，ネゴシエーションを行う．

S-P サービスの有効性を示すため，実装したシステムを用いて，動作検証を行った．ユーザがサービスインタフェースを介して薬局の医薬品購入補助システムを利用すると，サービス提供サーバが個人情報サーバへ個人情報を要求した．個人情報サーバは，個人情報開示知識とサービス情報，及び要求された個人情報を吟味し，サービス提供サーバが提供するサービスに必要な，年齢やアレルギーや持病，既往歴などの情報を含む健康情報などの必要最小限の個人情報をサービス提供サーバに与えた．その結果，提案した S-P サービス基盤が有効に機能し，年齢や飲み合わせを考慮した医薬品が提示された．以上から，個人情報を動的に利用しながら，複数サービスで連携して高度なサービスの個人化が可能になった事が確認できた．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計３件）

①Gen Kitagata, Kazuto Sasai, Johan Sveholm, Norio Shiratori, and Tetsuo Kinoshita, ″ Agent-based Access Rights Delegation utilizing Social Relationships ,″ International Journal of Energy, Information and Communications, 査読有, Vol.2, No.4, pp.87-100, 2011 年 11 月.

②橋本 和夫, 北形 元, 高橋 秀幸, 武田 敦志, チャクラボルティ デバシシュ, 白鳥 則郎, ″ Socio-familiar Personalized Service の提案とその応用 ―次世代ユビキタスサービスを実現するネットワークソフトウェアへ向けて―,″ 電子情報通信学会論文誌, 査読有, Vol. J94-B ,No.4, pp.492-502, 2011 年 4 月 1 日. **（招待論文）**

③Kazuto Sasai, Johan Sveholm, Gen Kitagata, and Tetsuo Kinoshita,″ A Practical Design and Implementation of Active Information Resource based Network Management System ,″ International Journal of Energy, Information and Communications, 査読有 , Vol.2, No.4, pp.67-86, 2011 年 11 月.

〔学会発表〕（計６件）

①Kazuo Hashimoto, Gen Kitagata, Hideyuki Takahashi, Atushi Takeda, Debasish Chakraborty, Norio SHIRATORI, ″ Socio-familiar Personalized Service and its Application -Towards a New Network Software for Next Generation Ubiquitous Service-″, Proc. of the 10th International Symposium on Autonomous Decentralized Systems (ISADS2011), 2010 年 12 月 25 日,東京. **(Invited)**

②Gen Kitagata, Debasish Chakraborty, Satoshi Ogawa, Atushi Takeda, Kazuo Hashimoto and Norio Shiratori, ″Visitor Access Control Scheme utilizing Social Relationship in the RealWorld,″ Trust Management IV, IFIP Advances in Information and Communication Technology 2010 (IFIPTM2010), 査読有, Vol.321, 2010 年 6 月 16 日, 盛岡.

③北形 元, 半井 明大, 大澤 由憲, 今村 理, 武田 敦志, 橋本 和夫, 白鳥 則郎, ″Socio-familiar Personalized Service の概念に基づくメニュー推薦システム″,情報処理学会 第 18 回 マルチメディア通信と分散処理ワークショップ (DPSWS2010), 2010 年 10 月 27 日,宮崎. **（ベストデモンストレーション賞受賞）**

④北形 元, ″Socio-familiar Personalized サービスについての取り組み″,電子情報通信学会 第 12 回ネットワークソフトウェア研究会, 2011 年 3 月 23 日, 鹿児島県西之表市.

⑤ Kazuto Sasai, Gen Kitagata, Tetsuo Kinoshita, ″Complementary Interaction between Human-oriented Knowledge and Machine-oriented Information on AIR-NMS,″ Proc of the 2nd International Conference on Morphological Computation (ICMC2011), 査読有, pp.111-113 2011 年 9 月 13 日, Italy.

⑥Khamisi Kalegele, Johan Sveholm, Hideyuki Takahashi, Kazuto Sasai, Gen Kitagata, Tetsuo Kinoshita, ″On-demand Numerosity Reduction for Object Learning,″ Proc of the Workshop on Internet of Things and Service Platforms (IoTSP 2011), 査読有, 2011 年 12 月 6 日, 東京.

６．研究組織
(1)研究代表者
北形 元（KITAGATA GEN）
東北大学・電気通信研究所・准教授
研究者番号：20344731