様式 C-19

科学研究費補助金研究成果報告書

平成　21 年　3　月 31 日現在

研究種目：基盤研究（C）
研究期間：2007～2008
課題番号：19510176
研究課題名（和文）　アイデンティティ認証基盤における分散型原本性の証明システムの研究

研究課題名（英文）　On the Study of Certification System based on Identity Authentication Roaming with Time Authentication

研究代表者
大橋　正和　(Ohashi Masakazu)
中央大学　総合政策学部　教授
研究者番号：90160598

研究成果の概要：分散協調環境下における協調ワークおよび形成知財への原本性の検証を伴いながら分散環境下での認証を核とした協調ワークによる共同研究を中央大学と国内および米国の研究機関間で行った。研究成果をネットワーク上に動的に共有しながら公表論文等の作成を分散環境基盤上で協調した。その際ワーク証明・知財の原本性の証明をデータがインターネットのクラウド上で履歴管理を行い安全で動的な長期保存を想定して研究を実施した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	2,400,000	720,000	3,120,000
2008 年度	1,100,000	330,000	1,430,000
年度			
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：複合新領域
科研費の分科・細目：社会・安全システム科学、社会システム工学・安全システム
キーワード：認証ローミング、原本性証明、時刻認証、アイデンティティ基盤、分散認証、追跡性、長期保存、安全システム

１．研究開始当初の背景

近年、政府・自治体や企業において、IT の活用や文書の電子化が進む一方で、情報漏洩事件が相次いで社会問題化しており、国民のプライバシーへの意識が向上しつつある。こうした中で、2005 年 4 月 1 日からは個人情報保護法が全面的に施行され、個人情報保護の必要性が一層高まっている。電子政府・電子自治体の実現のためには、情報システムの高度なセキュリティを確保し、利用者の信頼を得ることが不可欠である。これら、情報漏洩事件では、ネットワークを通じた外部からの攻撃によるものに加えて、内部における不正アクセスや過失・事故による個人情報の流出が大きな問題となっている。そのため、単に機密情報を暗号化すれば解決する訳ではなく、あらかじめ定められた「誰に」「どの」情報へのアクセスを許可するのかを管理することが重要である。つまり、人（システム利用者）を適切に管理した上で、機密情報の適正な利用を管理することが必要であり、具体的には、大きく次の 3 点が課題となる。

(1) 情報システムを利用する全てのアイデンティティを漏れなく統合的に管理すること。

(2) 厳密な本人認証と、許可された必要な範

囲内に限られた情報アクセス制御を行うこと。
(3)誰がどの情報アクセスをいつ行ったのかをきちんと記録すること。
このような課題を解決し、安全・安心に運用するためには、アイデンティティを統合的に管理するアイデンティティマネジメント基盤が必要となる。
アイデンティティの 5A
(1)認証（Authentication）…利用者をユニークに特定するための情報。
(2)認可（Authorization）…利用者に与えられる権限情報（情報へのアクセス・操作許可)。
(3)属性（Attribute）)…利用者の個人属性（所属、役職など)。
すなわち、「どんな属性（Attribute）を持つ」「認証済みの誰それに（Authentication)」「どの情報へのアクセスを許可する（Authorization)」ということである。更に上記に加えて、こうした「アイデンティティ」を適切に運用、およびセキュリティ上の問題がないことを保証・説明するため、本研究では、「管理（Administration)」「監査（Audit)」も含めた 5A を研究対象と考える。
この 5A の考え方に基づき、複数サイトにまたがる分散システムをシームレスに利用するため、1 サイトにおいてログインした認証情報および利用者の属性情報、アクセス許可情報を、インターネットドメインをまたいで他のサイトでも適切に伝達および交換し持ちまわることが必要である。加えて、不要な情報を意図しない相手に公開しないために、あるサイトには A という情報のみを公開し、別のサイトには B という情報のみを公開したい、というような部分的な公開・非公開ポリシーを設定し、利用者が明示的な同意・承諾を管理できるオプトインの仕組みも必要となる。
また、場合によっては、プライバシー保護への要求から、利用者の個人情報を特定することができないが、同じ利用者から一貫して同じ情報を利用できるようにするといった匿名型の認証が期待されることもある。このような、多様な認証要件を満たすには、連携型アイデンティティマネジメントの考え方が不可欠となる。これら、より高度なアイデンティティマネジメント基盤は、Web サービス技術を利活用し相互連携したシステムの将来像実現を支える１つの技術基盤として、重要な役割を果たすと言える。
大橋が H17-18　情報通信研究機構　委託研究　「異なるＣＡ間の認証ローミング技術に関する研究開
発」によりアイデンティティ情報を受け渡すことなく異なる認証局間で認証情報を安全にローミングする技術を開発し全体の研究指導とビジネスモデルおよび実証実験を担当した。
これらの技術開発により、Web サービス向けシングルサインオン（SSO）仕様「SecurityAssertion Markup Language（SAML）2.0」を拡張した異なる認証局間での新たな技術を開発しアイデンティティ基盤の認証情報を安全にローミングする基礎研究を行った。
一方、H15-16　科学研究費　基盤研究（C）「デジタルコンテンツにおける原本性証明のための認証技術の研究」（代表：大橋正和）によりマルチメディアコンテンツにおける原本性の証明を時刻認証によって行う方法の研究と実証実験を行った。

２．研究の目的
本研究では、これらの研究成果をふまえて組織間や認証局間およびインターネットのような分散環境下におけるアイデンティティ基盤を想定しそれらの基盤上での認証情報の授受におけるアイデンティティ情報と異なる認証局での認証情報の管理と追跡性についての原本性の証明を時刻認証を用いて行う方法を研究する。また、これらの研究により認証情報の時刻認証による原本性の長期保存に関する研究を行う事を目的とする。本研究により、従来の電子署名のみの本人認証機能しかなく短期間しか認証できない認証基盤から、多様性を持ったアイデンティティ基盤の５Ａの相互間の認証を安心・安全に行う方法を分散型認証技術と時刻認証による原本性の証明によりインターネットのような分散協調環境下での新たな認証基盤の確立を可能とする研究を行う。

３．研究の方法
平成 19 年度
（１）認証ローミング・データ基盤研究
・認証データの存在情報の提供技術
　実際に利用者が、過去のデータや他の利用者が保持するデータを利用するためには、データの存在情報やデータ概要を知ることが必要である。そのために、データ生成時に作成されるメタデータもしくはディレクトリ情報を、複数の利用者が共有的に利用できることを念頭に、これらの情報提供手法を検討・実証的に研究する。
・分散型認証データの検索・抽出データの表示手法
　ある目的に従って検索・抽出される認証データは、効果的に利用者に提示・表示されることが重要である。そのデータが保持するメタデータやディレクトリ情報による実現手法を研究する。
・分散型認証データの活用ノウハウの蓄積手法
　利用者の認証データ検索やデータ活用の

履歴・ログといった活用に係わる情報を蓄積することにより以降の認証データ利用の効率化を図ることが可能となる。これらの活用ノウハウにかかわる情報の生成・蓄積の手法を研究する。
（２）アイデンティティ基盤における時刻認証研究
下記のような項目について認証情報の原本性の検証を行う。
(a) 時刻ソース (b) 精度(c) 精度の証明 (d) タイムスタンプポリシー(e) タイムスタンプのデータ形式 (f) 発行者情報 (g) 要求者情報(h) シリアル番号(i) 順序性 (j) 元データの表現(k) 非改ざん（完全性）を保証する情報(l) ハッシュアルゴリズム、署名アルゴリズム、鍵長(m) 署名鍵(n) 証明書、失効情報(o) 有効期間(p) 危殆化への対応(q) 転送プロトコル (r) 再送攻撃への対処
（３）インターネット上の分散型認証における追跡性の対応研究
中央大学総合政策学部の授業や実証実験により蓄積された認証情報を SAML2.0 ベースの認証に対応する方式に変換してインターネット上の分散環境で原本性の追跡性に関する研究を行う。
（４）SAML2.0 ベース上の認証情報の分散協調環境における基盤研究
分担者間のインターネットによる分散協調環境を利用して本研究を遂行するに当たって生成されるアイデンティティ情報および認証データに対応できるようにネットワーク環境を整備する。
平成 20 年度
（１）セキュリティサービス基盤としての総合化研究
平成 19 年度の研究に引き続き、次の 4 つの機能を総合化する研究を行う。
①アイデンティティ管理
異なる CA 間の認証ローミングによるシングルサインオン機能の研究
②アクセス・コントロール
SAML と XAVML（ eXtensible Access Control Markup Language）によるアクセス制御の研究
③タイムスタンプ（時刻認証）
平成 19 年度に行う研究の成果を TSP（Time Stamp Protocol）RFC3161 を適用した TCP ベースでのサーバアクセス機能の研究
④電子認証
電子証明書と XKMS(XML Key Management Specification)による検証を考慮した電子認証機能
（２）原本性の証明に関する検証研究
認証情報に関する原本性の証明のための時刻認証に関するタイムソースの管理・トレーサビリティに関する検証を行うとともに追跡性に関する時刻認証の精度に関する検証を行う。
① 標準時との時刻同期管理
タイムスタンプ局の使用するタイムスタンプシステムの時刻は、UTC と時刻同期していることを検証する。
② タイムスタンプ局内の時刻精度
タイムスタンプ局内で稼動する全システムの時刻の精度は、UTC に対して３秒以内を維持することを検証する。
③ タイムスタンプサーバの時刻精度
タイムスタンプ局の使用するタイムスタンプサーバの時刻精度は、UTC に対して３秒以内を維持することを検証する。
④ 時刻のトレーサビリティ
標準時配信認証局、もしくは標準時配信国家機関がタイムスタンプ局に対して行った時刻監査の記録を保持することにより、タイムスタンプ局がタイムスタンプに使用した時刻の UTC に対するトレーサビリティを保持していることを検証する。
（３） 認証情報の長期保存性の研究
分散環境下での異なる認証局間での認証情報を時刻認証による追跡性の研究を行うことによりそれらの情報の長期保存性に関して認証情報の証明期間を考慮した一定期間毎のラッピングによる再度の時刻認証に関する方法について検証する。これにより現データを分散環境下に分散した状態で認証情報のみをラッピングすることにより長期に亘る原本性の証明が可能になる研究を行う。
（４）分散協調環境下における協調ワークおよび形成知財への時刻認証研究の確立
上記検証を伴いながら分散環境下での認証を核とした協調ワークにより共同研究を行い成果を共有しながら研究成果報告書を分散環境下での知財の原本性の証明を行いながら作成する。
平成 19 年～20 年度
分散環境下でのアイデンティティ基盤をインターネットを利用した仮想空間(クラウド)上に構築しワーク証明などの応用研究を行う。

４．研究成果
従来のように組織内の構成員だけを対象範囲としたネットワーク活用だけでなく、オープンな社会ネットワークにおいて、たとえば自治体が住民と共にその企画作業や業務処理を行っていく様な事例でも、オープンな社会ネットワークを活用した分散環境下でのワーク基盤構築は重要である。しかしながらその構築において、セキュリティの基盤とマネジメントについて考慮したものでなければ効果的に安心した活用ができない。
業務ごとにセキュリティポリシーを明確にし、どういうレベルのセキュリティをかけるかを情報資産ごとに管理・設定し、関係者

が使いやすい（可用性）を保ちながら、取り扱う情報や業務システムの機密性や完全性を守るセキュリティの仕組みが必要となるが実際にオープンな環境で業務毎にそのような仕組みを確立するのは困難である。

電子政府・電子自治体の実現のためには、情報システムの高度なセキュリティを確保し、利用者の信頼を得ることが不可欠である。情報の適正な利用を管理することが必要であり、具体的には、大きく次の 3 点が課題となる。

信頼性のあるネットワークを基盤とした安心・安全な情報社会を実現するためには、セキュリティ基盤、アイデンティティ基盤、サービス基盤の３つの基盤を確立する必要がある。特に、情報の適正な利用を図るためのアイデンティティ基盤とタイムスタンプが重要である。

・情報の適正な利用

(1) 情報システムを利用する全てのアイデンティティを漏れなく分散環境下で統合的に管理・運用すること（アイデンティティ基盤）

(2) 認証・許可・属性といった厳密な本人認証と、許可された必要な範囲内に限られた情報アクセス制御を行うこと（アイデンティティ基盤）

(3) 誰がどの情報アクセスをいつ行ったのかをきちんと記録し、内容も含めて第三者による原本性の証明が可能なこと（タイムスタンプ）

このような課題を解決し、かつ適正なコストで運用するためには、アイデンティティを統合的に管理するアイデンティティマネジメント基盤が必要となる。

・アイデンティティの５Ａ

従来からアイデンティティの３A ということが言われてきた。すなわち、「どんな属性（Attribute）を持つ」「認証済みの誰それに（Authentication）」「どの情報へのアクセスを許可する（Authorization）」ということである。

① 認証（Authentication）…利用者をユニークに特定するための情報

② 認可（Authorization）…利用者に与えられる権限情報（情報へのアクセス・操作許可）

③ 属性（Attribute））…利用者の個人属性（所属、役職など）

更に上記に加えて、こうした「アイデンティティ」を適切に運用、およびセキュリティ上の問題がないことを保証・説明するため、アイデンティティマネジメントにおいては「運用・管理（Administration）」「監査・追跡（Audit）」も含めた 5A を重視している。５A 間の相互運用性を５Ａ全てにおいて異なる認証主体間、サービス主体間で連携し、ワンストップサービスとそれに伴う認可・属性の交換、複数の認証主体にまたがる追跡・監査の実現が必要である。

④運営・管理（Administration)…アイデンティティの適切な運営・管理

⑤監査・追跡（Audit） …セキュリティ上の問題がないことを保証・説明する（監査・追跡）

相互運用性については、５Ａ全てにおいて異なる認証主体間、サービス主体間で連携し、ワンストップサービスとそれに伴う認可、属性の交換、複数の認証主体にまたがる追跡・監査の実現が必要である。このアイデンティティ基盤は、RFID などの広範な普及によって航空手荷物のように荷物にも人のアイデンティティを付与したり、ユビキタス環境では、物品（生産者証明等）にも数々の情報を付与するときにはアイデンティティ基盤が重要な役割を果たすことになる。

分散環境下での認証の仕組みとしては、認証情報を SAML を利用してリダイレクトする方法で行うのが一般的である。しかし、分散協調ワークのように複数の組織に属していてさらにモバイルワークのように場所も移動する場合、一人の人間が複数のプロジェクトに関わる場合のように複雑な要件を持っている。このような場合、単純なリダイレクトによる分散認証よりも第三者機関も含めた信頼できる認証局間での認証情報のローミングを利用した分散認証が重要になる。

従来の閉鎖系のシステムであればデジタルデータの存在も内部であり使う時刻も閉鎖系の中での閉じた時間で動いていれば充分であった。ネットワーク化された例でもデータベースのように分散されている同一システムと見なされるシステムであればシステム内の相対的な時刻を合わせればシステムは正常に機能していると見なされている。多様な人々や組織が利用するインターネットやｉＤＣ間でのデータ転送やアプリケーションの利用には従来の閉鎖系の仕組みや考え方は成り立たなくなってきている。

電子自治体を例にとっても、県庁には、ＬＡＮ内のシステムと外部から接続されるＬＧＷＡＮ（総務省），住基ネット（総務省)、防災ネット（国土交通省)、インターネット、支所・出張所への専用線、市町村とのネットワークなど様々な仕組みが接続されているが、それぞれ別々のシステムとして閉鎖系的な考え方で運用されている。これからは、それらを総合的に考え有機的な結合をして動く開放系のシステムとしての考え方が重要である。

これほどデジタル化が進展したシステムでの共通の絶対基準とはなにかというとそれは時刻であり、特に絶対時刻（標準時刻）が基準である。さらに、デジタル化されたコンテンツ・データはバーチャルなため原本性の証明や組織・個人の認証が必要であり時刻認

証の仕組みが考えられている。時刻認証は、原本生の証明を第三者が客観的に証明する仕組みでありペーパーレスのデジタル時代には、このデジタルでの原本性確保が最重要課題である。この技術には、「改ざん防止」と「改ざん検出」の２つの機能がある。時刻認証は、原本性の保証として諸外国の電子署名法等で採用されている。時刻認証は認証された時刻以降改ざんされていないことを証明する仕組みである。
これらタイムビジネスの主要な２つの要素、標準時刻配信、時刻認証は、株式等の金融商品のネット上での取引や知財の原本生の証明など「なりすまし」、「改ざん」、「事後否認」などを防止する意味でも情報社会の基盤のなかで最も重要な仕組みであると考えられている。これなではデジタル社会はあり得ないし我々の通常の活動（アナログの世界）と連携させる唯一の絶対基準であると言っても過言ではない。
時刻認証については下記の項目について検討しアイデンティティ基盤の上に認証の仕組みを実装し分散協調ワークにおけるワークの証明（アクセスデータおよびログデータへの時刻認証）と成果についての原本性の証明を行う。
これらを考慮して下記４つの機能についてワーク認証のためネットワーク上に無線ＬＡＮを利用した模擬プラットフォームを構築し研究を行った。

(1) アイデンティティ管理　異なるCA間の認証ローミングによるシングルサインオン機能の研究
(2) アクセス・コントロール　SAMLとXAVML（eXtensible Access Control Markup Language）によるアクセス制御の研究
(3) タイムスタンプ（時刻認証）TSP（Time Stamp Protocol）RFC3161を適用したTCPベースでのサーバアクセス機能の研究
(4) 電子認証　電子証明書とXKMS(XML Key Management Specification)による検証を考慮した電子認証機能

対象としたのは、分散協調ワークにより発生するアクセス記録(ログデータ)、ワークで使用したコンテンツ（オフライン時も含む)、プロジェクト・マネジメント(役割分担等)、勤務(作業)日誌である。これらの記録を、ログとしてばかりでなくワーク認証データとし2008年3，4月に実証実験を行い有効性を検証した。

分散協調ワークをWebサービスの「サービス」の側面として捉え、現実世界の環境そのものがユーザに価値を提供するというユビキタスの観点からみたサービスと利用者を人的資源と考えてワークを証明・認証する研究を行った。ワークをサービスとして捉えるとそれらの基本的な性質は１．無形性、２．相互性、３．継続性、４．信頼性、として考え、ユーザに環境が合わせて使いやすくする仕組み（コンテキストアウェアネス）を実現するためにコンテキストマネジメントサービスの原本性の研究と、必要な要素に対してサービスを最適化するための情報を管理するシステムを研究した。これらの研究成果をふまえて人的資源を中心としたワーク情報を組織間や認証局間およびインターネットのような分散環境下における共有データを分散型のアイデンティティ基盤上に想定しそれらの基盤上でのワーク認証情報の授受におけるアイデンティティ情報と異なる認証局での認証情報の管理と追跡性についての原本性の証明を時刻認証を用いて行いネット上に分散したワークプレースを利用した認証情報とテレワークにおけるワークの証明を時刻認証の応用による研究を行った。今後は、本研究で行った技術システムの研究を分散協調環境下におけるプロジェクト・マネジメントシステムなどによるマネジメントシステムとの連携などへの応用研究に発展させたい。

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　４　件）

①Ohashi, M. and M.Hori
“Citizen-Centric e-Healthcare Management Based on Authentication Roaming between Different Certificate Authorities”、査読　有
総合政策研究、Vol.13、2008.03　pp.65-76.

②Ohashi, M and M. Hori
User-Centric Social Design Technology: Demonstrative Experiment on Authentication Roaming between Different Certificate Authorities、査読　有
“Expanding the Knowledge Economy Issues, Application, Case Studies” Vol.4, pp.1394-1406, 2007.10.IOS Press

③Hori, M.
How flexible working format affects work-life balance:　The Contribution of telework to the quality of　life for working women in Japan, 査読　有、Proceedings of

International Women's Conference 2007, pp.80-84,Toowoomba, Australia, 2007

④Hori, M.
New Working Format Model: E work in Web2.0 Era Collaborative Telework as Knowledge Creation, 査読有
Proceedings of ETHICOMP ,pp249-254, Meiji University, Tokyo, Japan, 2007

〔学会発表〕(計 5 件)
①Ohashi, M. and M. Hori
"The System of the XML Web Services on the Adaptive Collaboration Platform"
ED-MEDIA 2009, 25.June 2009 発表決定
Hilton Hotel,Honolulu,Hawaii
②大橋正和・堀眞由美
分散型アイデンティティ基盤と時刻認証によるワーク証明の研究、
テレワーク学会、2008 年 6 月 29 日、沖縄県産業支援センター
③大橋正和、堀眞由美
シチズン・セントリックの考え方ー次世代における公共の概念ー、中央大学共同研究プロジェクト・情報社会学会研究会、2008.03.08 ,中央大学記念館
④大橋正和
社会の変容と ICT の最近(将来)の課題、学術振興会、第 171 研究会、2008.03.06、主婦会館

⑤大橋正和
データセンターが果たす役割について ーiDC の最新動向ー 、e-Port 推進協議会講演会、
2008.02.21、福岡、福岡国際ホール

〔図書〕(計 2 件)
①Ohashi, M. and M.Hori
"Technical Perspective for the e-Health Care Management of Adaptive Collaboration Based on Authentication Roaming between Different Certificate Authorities"
Chapter of *Handbook of Research on Developments in e-Health and Telemedicine: Technological and Social Perspectives*
edited by M. Manuela Cunha, Antonio Tavares and Ricardo Simoe
IGI Global, July 2009 発刊決定

②M. Hori and M. Ohashi,
Chapterp.14 "Knowledge Creation and Adaptive Collaboration Based on XML Web Services"、pp.292-305
"Knowledge and Technology Management Virtual Organizations: Issues, Trends, Opportunities ,and Solutions"
Edited by Dr.Goran D.Putnik & Dr.Maria Manuela Cunha ,
IDEA Group Publishing, 2007. p.368

〔その他〕

①大橋正和
「現代社会の変容と情報社会」、大学と生活、第 45 号(通巻 519 号)2007-9、独立行政法人日本学生支援機構、pp.7-14、2007.09.

②大橋正和
「シチズン・セントリックな考え方」 中央評論、No.260、pp.045-051、2007.07

６．研究組織
(1)研究代表者
大橋 正和 (Ohashi Masakazu)
中央大学 総合政策学部 教授
研究者番号:90160598
(2)研究分担者

(3)連携研究者
堀 眞由美 (Hori Mayumi)
白鴎大学 経営学部 教授
研究者番号:90259036

松野 良一 (Matsuno Ryoichi)
中央大学 総合政策学部 教授
研究者番号:10365885