様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 １８ 日現在

機関番号：３２６４１
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５１０２３３

研究課題名（和文）クラウド環境下での動的原本性認証とアイデンティティの認証連携の高度化の研究

研究課題名（英文）On the study of identity authentication system with dynamic certified originality content on the cloud

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

交付決定額（研究期間全体）：（直接経費）　　4,200,000円

研究成果の概要（和文）：クラウド環境下における安全・安心な情報環境を確保するために動的原本性認証とアイデンティ ティの認証基盤を同時に連携する事によりクラウド上でも安全な環境を確保する研究を行った。デジタルコンテンツに対してばかりでなく認証情報に対しても第三者による原本性の証明を 確保するため従来静的で固定的であった時刻認証を、クラウド環境下での情報の動きにダイナミ ックに追従する動的な時刻認証の研究を行い、アイデンティティ基盤と連携する新しい視点での 研究を実施した。

研究成果の概要（英文）：In an electronic environment or digital society built on computers, recordkeeping relates inevitably to the time that is ticked away by the clocks embedded in the computers. Time is thus the infrastructure of this information society. The scope of discussion here focuses on some specific industries and applications for time-stamping technologies. We focused mainly on time-authentication (time-stamp). This study will be further refined step by step as their validity is verified in actual use. Our study proved the effectiveness of the New Authentication Extension Technology and Proxing Assurance between OpenID and Time Stamp to combine different social infrastructures to create new Secure services between Public Sector and Private Sector(Citizen). Though there are still issues to cope with outside of the realm of technology including accountability of each participants and the level of the service, we expect this service to be soon available in the real world.

研究分野：情報科学、情報社会学

キーワード：時刻認証　アイデンティティ　分散システム　クラウド　原本性の証明　拡張プロトコル

１．研究開始当初の背景

（1）クラウド利用の急速な普及やクラウドを利用した Social Media によるコミュニケーションや電子商取引の変容など情報環境が急速に変化するとともにモバイルデバイス、タブレット端末等のリアルタイム OS を利用した新たなインターネット利用の時代に突入した。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、国民のデータやプライバシーへの意識が向上しつつある。こうした中で、 個人情報保護法や e–文書法などデジタル・ネットワーク対応の法律が全面的に施行され、個人 の情報保護やコンテンツの原本性の保証の必要性が一層高まっている。

（2）その様な変容の内クラウド利用の急速な進展によりセキュリティやデジタルコンテンツの原本性の証明・存在の証明等を安全安心の視点から高度化する必要が出てきた。この様な背景から契約書や公文書ばかりでなく SOX 法のようなデジタル取引やコンテンツ全般およびコミュニケーションに対する原本性や存在証明を実施する必要に迫られてきた。特に、クラウドを対象とした研究はほとんど存在しなかった。情報社会の実現のためには、 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とデジタル情報の信頼性 と第三者による原本性の証明が不可欠である。

２．研究の目的

⑴ クラウド環境下における安全・安心な情報環境を確保するために動的原本性認証とアイデンティ ティの認証基盤を同時に連携する事によりクラウド上でも安全な環境を確保する研究を行う。また、デジタルコンテンツに対してばかりでなく認証情報に対しても第三者による原本性の証明を 確保するため従来静的で固定的であった時刻認証を、クラウド環境下での情報の動きにダイナミ ックに追従する動的な時刻認証の研究を行い、アイデンティティ基盤と連携する新しい視点での 研究を実施する。これらの研究によりクラウド環境下でも安全・安心な情報環境の創出を実現し、 動的時刻認証によりコンテンツとアイデンティティ認証を同時に実行する研究を行った。

⑵ 情報漏洩や情報のトラブル事件では、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。
⑴ 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。
⑵ 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。 ⑶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。 従来のアイデンティティマネジメントの基本は、3A
⑴認証(Authentication)...利用者をユニークに特定するための情報。 ⑵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)。 ⑶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。しかし、SocialMedia や クラウドの普及などに伴い上記 3A に加えて、「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、⑷「管理・運用(Administration)」⑸「監査・追跡(Audit)」も含めた 5A を研究対象と考えた。

３．研究の方法

（1）本研究の基盤となる下記の 4 つの主要要素について初めに研究を実施した。 I.動的時刻認証データ基盤研究 II.クラウド環境下での分散型認証基盤におけるアイデンティティ情報への時刻認証研究 III.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 クラウド環境下での Social Media における授業や実証実験により蓄積された認証情報を OpenID 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デジタルコンテンツの原本性の動的追跡性に関する研究を行った。
IV.OpenID ベース上の認証情報の分散協調環境 (クラウド)における拡張プロトコルの研究 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した。複数のネットワークとインターネットを介した 6 台の PC と 6 台のハードディスクを設定した。その他認証サーバー2 台（時刻認証と時刻設定）を利用した擬似認証局を設定した。それぞれの機器は、すべて物理的に異なるネットワーク上に設置した。さらに、予備のクラウドとして 3 台の PC およびストレージを用意した。インターネット上からのアクセス実験では、2 台の

スマートフォン、3 台のタブレット端末のより異なる場所からのアクセス実験を実施した。

（2）(1) の基盤システムの元に次の様な研究を実施した
I.クラウド環境下での原本性の証明に関する検証研究
II.認証情報の長期保存性の研究
III.クラウド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研究
IV.クラウド環境下におけるセキュリティサービス基盤としての総合化研究
Ｖ.さらにこれらの研究成果の利用が見込まれる現代社会の変容による人間行動への影響について研究を実施し特に消費行動に与える影響について詳しく研究を実施した。

４．研究成果

（1）本研究の基盤となる下記の 4 つの主要要素 I.動的時刻認証データ基盤研究 II.クラウド環境下での分散型認証基盤におけるアイデンティティ情報への時刻認証研究 III.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 IV.OpenID ベース上の認証情報の分散協調環(クラウド)における拡張プロトコルの研究
についてクラウド環境下での有効性を検証した。

(2) クラウド環境下での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った。 1 標準時との時刻同期管理、2 タイムスタンプ局内の時刻精度、3 タイムスタンプサーバ の時刻精度、4 時刻のトレーサビリティの検証を実施した。

(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った。

(4) クラウド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研究
分散環境であるクラウド上でのアイデンティティーをキーとした協調ワークへの応用研究を実施し有効に機能することを実証した。また、共有コンテンツにおいて知財形成を容易にするため論文作成をクラウド上で原本性と時刻管理をして本研究の拡張プロトコル方式が有効に機能することを実証した。
拡張プロトコルとしてオープン ID CX(コントラクト エクスチェンジ)を改造した。
AM：Access Manager、SP：Service Provider
(実験では認証局が兼務)
1. SP は AM の XRDS から､Template を探す。
2. SP は AM から Proposal Template の取得
3. SP は Proposal Template に変数記入→Proposal
4. SP は Proposal に署名→署名入り Proposal
5. SP は署名入り Proposal を AM へ送信
6. AM は、要求内容をユーザーに見せ、提供可否を確認
7. OK ならば、AM は Proposal に署名→Contract
8. AM は Contract を保存するとともに、SP へ返送
9. SP は Contract に基づき、データを取得したりして、User にサービスを提供

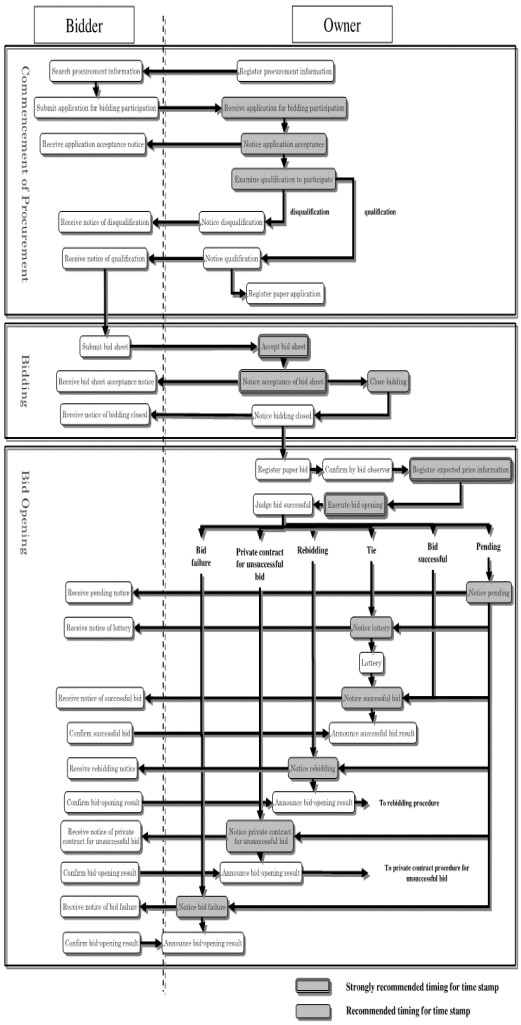

図 時刻認証 フロー

(5)　クラウド環境下におけるセキュリティサービス基盤としての総合化研究
それまでの研究に引き続き、次の 4 つの機能を総合化する研究を行った。
1)アイデンティティ管 理 クラウド環境下での認証上の拡張プロトコル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 OpenID と XAVML(eXtensible Access Control Markup Language)によるアクセス制御の研究
3)動的時刻認証の研究
4)クラウド環境下での総合的な電子認証と原本性の証明の連携 電子証明書と XKMS(XML K ey Management Specification)による検証を考慮した電子認証機能の研究を実施した。

(6)　さらにこれらの研究成果の利用が見込まれる現代社会の変容による人間行動への影響について中央大学政策文化総合研究所、情報社会学会での研究プロジェクトにおいて連携して研究を実施した。特に本研究における成果の活用が見込まれる電子商取引や電子調達等の消費行動に与える影響について詳しく研究を実施した。
2012 年 12 月 3,4 日 Finland において INFORTE セミナーとして ”Contingency Management based on ICT ”を大橋、堀、Prof,Suomi（University of Turku）で企画・実施した。このセミナーでは、東日本大震災等を事例として本研究のテーマであるデータの安全性や保存性について大橋が講演した。また、福島原発事故における関連報告と避難地域の知識の継承に関する研究報告を行った。本研究を必要とする背景や周辺研究領域の研究も実施した。

情報社会の実現のためには、 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とデジタル情報の信頼性 と第三者による原本性の証明が不可欠である。これら、情報漏洩や情報のトラブル事件では、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、アイデンティティマネジメント基盤が必要となる。 従来のアイデンティティマネジメントの基本は、3A
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。しかし、SocialMedia やクラウドの普及などに伴い上記 3A に加えて、「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、
4)「管理・運用(Adminis tration)」
5)「監査・追跡(Audit)」も含めた 5A を研究対象と考え,この 5A の考え方に 基づき、複数サイトにまたがるクラウドなどの分 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。
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 サービス技術等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。
本研究では、動的時刻認証の研究を、分散型認証の拡張機能として研究し、原本性の研究とアイ デンティティ認証を同時に実現することによりクラウド環境下でも安 心 安 全 な環境を実現し 5A を実現した。
本研究では、急速に普及しつつあるクラウド環境下でのデジタルコンテンツを分 散 型 認証シス テムである OpenID や SAML 上に拡張プロトコルとして電子署名を施したコンテンツをアイデンティティ認証と同時にネットワーク上を経由してクラウド上 に 展 開することを可能とした。さらに、拡張機能を用いて動的時刻認証を同時に搭載しアイデンティティ認証が実施された時点で動的に時刻認証が施 される研究を行った。これにより、クラウド上に展開される暗号化されたデジタルコンテンツが、アイデンティティの 5A と結合されると同時にそのコンテン

ツが利用もしくは変更されると同時に時刻認証により動的に原本性と存在の証明が可能となる。このことは、クラウド環境下でも安心・安全な環境が確保され電子政府やビジネスでの利用が可能になることに意義があると考える。

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　5　件）

1. Koji Okudaa, Masakazu Ohashi
On the Studies of Recovery and Reconstruction of Fisheries Hit by the Great East Japan Earthquake, *Procedia Technology 5 (2012) pp. 208 – 214, Elsevier*

2. Noriko Kurataa,, Masakazu Ohashi, Mayumi Hori
Reconstructive Platform for Local Communities Damaged by Nuclear Disaster: A Proposal
Procedia Technology 5 (2012) pp.215 – 223, Elsevier

3. Huang Wen Cheng, Duan HajJiao, Fan Yingchen, Liu Chunli, Chen Tai- Wei, Mayumi Hori
中国と台湾の働き方の一考察
白鴎大学大学院経営研究(2013) Vol.13、p.13-41,

4. Masakazu Ohashi, Mayumi Hori
On the Study of Certified Originality for Digital Alteration Problem
-Technology Developments of the Time Authentication-
the Internatioanl Journal of Cyber Warfare and Terrorism, Issue1, Vol.3, pp15-28,IGI Global, 201310

5. **桐谷恵介、大橋正和**
要件定義における信頼マネジメントの必要性についてー日米比較による日本のシステム開発の特殊性からの考察–、情報社会学会誌、Vol.9,N o2, P.13-19, 201411

〔学会発表〕（計　16　件）

1. Kamei, S., M. Ohashi and M. Hori
Social Impact Information as the Cause for the Formation of Ties in Enterprises
Proceeding of 2015 48th Hawaii International Conference on System Sciences, IEEE Computer Society, pp.2786-2793.　20150109

2. **桐谷恵介、大橋正和**
分散協調体制での IT システム構築の効率化についてーテレワーク形式での要件定義における信頼マネジメントのモデル化の研究–、第 16 回日本テレワーク学会研究発表大会予稿集、p.4-9, 20140706

3. Yuto Shiratori, Masakazu Ohashi, Mayumi Hori and Yushi Okajima
Study on Collaborative Business and Educational Model with 3 Dimensional data for People with Disabilities - 3D Data Acquisition and Object Reconstruction through Crowdsourcing-, Proceeding of Ed-Media2014, p.1451-1465, 20140625

4. Noriko KURATA , Masakazu OHASHI
Study on the Experience of Major Earthquakes and Decision-making for Risk Determination□-How the Previous Experience of Major Earthquakes Influenced Decision-Making by Local Residents in Regards to Nuclear Power Plants-、
Collected Papers Transformation of human behavior under the influence of The Infosocionomics Society、 Vol.1, pp.17-28, 20140305

5. Noriko Kurata, Yuko Kurata, Mayumi Hori, Masakazu Ohashi and Sumiko Kurata
A Preliminary Study on Succession of Health Care Information in Japan
Hawaii International Conference on Education、20140107

6. Mayumi Hori, Xuerui Chen, Masakazu Ohashi
On the Study of the Adaptive Collaborative Work with New Working Format for Work Life Balanced Society
Second International Conference on Virtual and Networked Organizations□Emergent Technologies and Tools, 20131120

7. Ling-Yu Liang, Mayumi HORI, Masakazu OHASHI
On the Study of Consumer Generated Media related with Inbound Marketing
Second International Conference on Virtual and Networked Organizations□Emergent Technologies and Tools, 20131120

8. M. Hori and Ohashi, M.
ON THE STUDY OF CERTIFIED ORIGINALITY OF E-PROCUREMENT
-BUSINESS DEVELOPMENTS OF THE TIME AUTHENTICATION-
Proceeding of THE 9TH INTERNATIONAL CONFERENCE ON

KNOWLEDGE-BASED ECONOMY AND GLOBAL MANAGEMENT, STUST Press, p.79-91, 20131107

9. 大橋正和
総括講演「情報社会と人間行動の変容 －Generation Y と Social Media－」（日中の消費行動の変容もふまえて）、Workshop 情報社会と人間行動の変容 －Generation Y と Social Media－、New York、中央大学政策文化総合研究所、情報社会学会 20130206

10. Masakazu Ohashi, Reima Suomi and Mayumi Hori
"Contingency Management based on ICT" Finland Inforte **セミナー（集中講演）、**Department of Computer Science and Information Systems 、 University of Jyväskylä and University of Turku 2012 **年** 12 **月** 3, 4 **日**

11, Masakazu Ohashi
Recent Perspectives of the Infosoionomics Society based on Information and Communication Technology -Japanese Governmental Large Scale Substantiative Experiments IN Last 10 Years -
Proceeding of THE 8TH INTERNATIONAL CONFERENCE ON KNOWLEDGE-BASED ECONOMY AND GLOBAL MANAGEMENT , p.55-80, 20121031

12. Mayumi Hori
Contingency Management Based on Flexible Working Format,
The 8th International Conference on Knowledge- based Economy and Global Management, 20121031

13. Kurata, N., Kurata, Y. &Ohashi, M.
Possibilities of Local Identity Platform: The Role of ICT to Pass Down Local Culture.
Proceedings of World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 20121011

14. 大橋正和
安心･安全な社会へのＩＣＴ技術
内閣府マイナンバーシンポジウム 大分 20120826
15. 大橋正和
安心･安全な社会へのＩＣＴ技術
内閣府マイナンバーシンポジウム 佐賀 20120609
16, 大橋正和
安心・安全な社会へのＩＣＴ技術
内閣府マイナンバーシンポジウム 長崎 20120608

〔図書〕（計 6 件）

1. 大橋正和
第1章 情報社会の消費の理論的考察 p.1-23
2. 大橋正和、高橋宏幸
第2章 情報社会における消費行動の変容 －デジタル化とインターネットの影響について p.25-58
3. 堀眞由美
第3章 現代社会の変容と女性消費者の動向 p.59-84
大橋正和**編著 現代社会の変容による人間行動の変化について－消費行動の変容を中心として,中央大学出版部 201503 p.216**

4. 大橋正和
第 2 章 情報社会とソーシャルデザイン －先駆者との対話を通じた情報社会での知識や社会の考え方、p.35-79
5. 堀眞由美
第4章 情報社会時代の働き方 女性労働の現状と課題から見る今後の働き方、p.127-145
公文俊平、大橋正和 **編著、情報社会のソーシャルデザイン－－情報社会学概説Ⅱ、NTT 出版、201412 p258**

6. Masakazu Ohashi, Nat Sakimura , Mituo Fujimoto, Mayumi Hori and Noriko Kurata
Technical Perspective of Authentication Policy Extension for the Adaptive Social Services and e-Health Care Management
Chapter 37 pp.719-726
Handbook of Research on ICTs for Healthcare and Social Services: Developments and Applications
Edited by Isabel Maria Miranda & Maria Manuela Cruz-Cunha , pp.978
IGI Global 201308

〔産業財産権〕
○出願状況（計 0 件）：

○取得状況（計 0 件）

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

(2)研究分担者
堀 眞由美 （Mayumi Hori）
白鴎大学 経営学部 教授
研究者番号： 9025903