科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　１８　日現在

機関番号：　１５１０１
研究種目：　若手研究(B)
研究期間：　2011～2013
課題番号：　２３７０００９８

研究課題名（和文）クラウドコンピューティング基盤を利用したユーザ指向の情報保護方式の研究

研究課題名（英文）User oriented information protection framework based on cloud computing Environment

研究代表者
高橋　健一（TAKAHASHI, Kenichi）

鳥取大学・工学（系）研究科（研究院）・准教授

研究者番号：３０３９９６７０

交付決定額（研究期間全体）：（直接経費）　　3,200,000円、（間接経費）　　960,000円

研究成果の概要（和文）：様々なサービスがインターネット上で提供されている。これらのサービスの一部はユーザに名前や住所、ID/パスワードなどの提供を求め、それらの情報と引き換えにサービスを提供する。一方で情報漏洩事件やフィッシングによる被害が頻発している。これらの原因の一つとして、情報利用に対する決定権がユーザにないことが挙げられる。そこで、サービス提供者だけでなく、ユーザ側でも情報の利用（保護）方法を決定可能な仕組みを研究する。これによって、ユーザ自身が安全だと思う方法でフィッシング等の脅威に対する対策を講じることができ、ユーザはそれぞれのサービスを同様に安心できるものとして利用できるようになる。

研究成果の概要（英文）：Some of Internet services request us to provide our personal information. When we use their services, we have to provide our personal information even if we cannot trust their service providers. This may cause the abuse of their personal information. Therefore, we propose a framework that prevents service providers from abusing users' personal information. In our framework, a user selects a method to use his/her information, and compels the service provider to use the method. Since personal information is used through the method selected by the user, the user is able to prevent the service provider from the abuse of his/her personal information. Thus, the user can relief to provide his/her personal information to the service provider. We have some problems to be solved for the realization of our framework. In this paper, we have to discuss a way to install a method selected by a user into a program a service provider has.

研究分野：　計算機システム・ネットワーク

科研費の分科・細目：　ネットワークセキュリティ技術

キーワード：　プライバシ

１．研究開始当初の背景

オンラインショッピングやオンラインバンキング等のインターネット上のサービスを利用するときに、ユーザは自分の個人情報、名前や住所、ID/パスワードなどの提供が求められる。しかし、一方で情報漏洩事件やフィッシングによる被害が頻発している。

これらの問題を解決するために様々な暗号アルゴリズムやプロトコル、また、その応用として SSH や電子証明書、PKI などの技術が研究されてきた。しかし、こららの研究では盗聴や成りすましなどの悪意のある第 3 者からの脅威に対抗することが主で、当事者（情報提供先：サービス提供者）による脅威への対抗策にはならない。このため、内部者からの脅威に対する問題は、近年重要な問題として取り上げられつつあり、そのことを議論されている。しかし、内部の攻撃者からの攻撃をどのように防ぐかが主目的であり、実施している内部脅威対策を情報の提供元（ユーザ）に知らせる方法については余り検討されていない。

そこで、情報利用に対する決定権をユーザにも持たせることによって、それぞれのユーザで安全・安心だと思う方法を選択可能な仕組みを研究する。これによって、ユーザ自身が安全だと思う方法でフィッシング等の脅威に対する対策を講じることができ、ユーザはそれぞれのサービスを同様に安心できるものとして利用できるようになる。

２．研究の目的

情報利用に対する決定権をユーザにも持たせることによって、それぞれのユーザで安全・安心だと思う情報利用（保護）方法を選択可能な仕組みを研究する。提案手法の概要と実現に向けての課題を図１に示す。

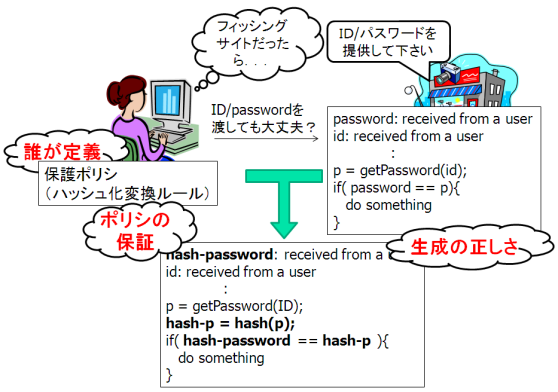

図１．実現に向けての課題

一般的にサービス提供者はユーザの情報を利用するためのプログラムを持つ。一方でユーザは情報の利用方法を定義した保護ポリシを持つ。ユーザは、サービス提供者が持つプログラムを保護ポリシに従って変換することで、保護ポリシに定義された情報保護方法を埋め込んだプログラム（Customized Program）を生成する。サービス提供者が Customized Program でユーザの情報を利用することで、サービス提供者による情報利用を制限し、ユーザは自分が指定した方法で自分の情報を守ることができる。しかし、本提案手法を実現するには、課題 1) 保護ポリシを誰が定義するのかといった問題や課題 2) 保護ポリシの保証に関する問題、課題 3) Customized Program 生成の正しさ検証に関する問題を解決する必要がある（図１）。そこで、本研究ではクラウドコンピューティング基盤を利用することで、これらの問題解決を図る。

３．研究の方法

本提案手法の実現に向けて、クラウドサービス（Security as a Service）としてルールレポジトリとプログラム変換代行サービスの 2 つを導入し、上記の課題を解決することを試みる。

ルールレポジトリには情報を守るための方法が保護ポリシとして保存されている。プログラム変換代行サービスは、保護ポリシに従ってプログラムを変換するサービスを提供する。

サービス提供者は自分が信頼できるプログラム変換代行サービスを指定する。サービス提供者から情報を提供を求められた場合、ユーザは自分が信頼できる情報利用（保護）方法を記した保護ポリシをルールレポジトリから選択する。プログラム変換代行サービスは、ユーザが選択した保護ポリシに従って定義された情報利用方法を埋め込んだプログラム（Customized Program）を生成する。ここで、ユーザは Customized Program を検証することで、保護ポリシに定義された情報利用方法が正しく埋め込まれていることを確認する。一方、サービス提供者は電子署名により、Customized Program が指定したプログラム変換代行サービスによって正しく生成されたものであることを確認する（課題３）。このことで、サービス提供者を信頼できなくても、また、クラウドサービスを信頼できなくても、ルールレポジトリのルールだけに信頼を置くことでユーザの情報を守ることが可能になる。

また、ルールレポジトリは誰でもアクセス可能なサービスとして公開されており、保存されている保護ポリシはテキストベースの情報として定義されている。保護ポリシはテキストベースの情報であるため、誰でもルールレポジトリから保護ポリシをダウンロードし検証することができる。このため、十分に利用実績のある保護ポリシはユーザの情報を守るための方法として十分に信頼できる、

保証されたものとして考えることができる（課題２）。また、保護ポリシは企業や個人等のボランティアによって登録される。例えば、クレジットカード会社がクレジットカード番号を保護するための保護ポリシを登録し、その利用をユーザに勧める。このことでユーザ個人で保護ポリシを定義しなくても、ルールレポジトリ中から自分が安心・安全だと思う方法（保護ポリシ）を選ぶことできるようになる（課題１）。

本研究では、上記枠組みの具体化、および、ルールレポジトリとプログラム変換代行サービスの詳細化に取り組むことで、ユーザ自身が安心・安全だと思う方法で情報保護対策を講じることが可能な枠組みを実現する。

４．研究成果

平成２３年度は保護ポリシを保存するためのルールレポジトリと保護ポリシに従ってプログラムを変換するためのプログラム変換代行サービスの２つについて検討した。ルールレポジトリに関する検討としては、保護ポリシの生成方法や生成者、管理方法、保護ポリシの保証の問題について検討すると共に問題点を明らかにした。ルールレポジトリの管理者がユーザとサービス提供者の両者から信頼される必要があるといった問題が最も大きな問題であり、その解決方法について検討した。プログラム変換代行サービスに関しては、プログラム変換サービスが動作する場所の検討や、変換されたプログラムを検証する方法についての検討を行った。また、ルールレポジトリとプログラム変換代行サービスを導入したシステム全体としての動作の流れについて検討を行うと共に、ＰＣ上にそれらの試作実装を行い、動作の確認を行った（図２）。

図２．ユーザインタフェース（保護ポリシ選択時）

平成２４年度は前年度に検討結果を踏まえ、１）システムの流れを具体化し試験的に実装してみると共に、２）保護ポリシによるプログラムの書き換え方法の具体化を行った。

システムの流れの具体化としては、ユーザ側の動作を Google Chrome のアドオンにより、サービス提供者とルールレポジトリの動作をサーブレットと JSP により実装した。実装したシステムをウェブ上に公開されている、個人情報の入力を要求するページに適用することでシステムの動作の確認を行った。

また、保護ポリシによるプログラムの書き換え方法の具体化に関しては、利用ポリシ・保護ポリシの詳細化を行うと共に書き換え手順の具体化を行った。プログラムの書き換えは、構文解析ツールである ASTParser を利用し、書き換えるプログラムを構造化する。構造化したプログラムに対して、ポリシの適用箇所を特定し、特定された部分をポリシに従って置き換える。置き換えられたものをプログラムとして再構成することで実現する（図３）。

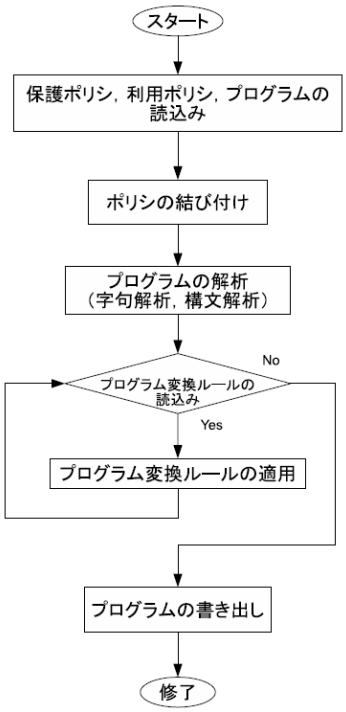

図３．プログラム変換の流れ

平成２５年度は保護ポリシによるプログラム書き換えの実装、および評価を行った。評価としては、保護ポリシを 7 個と変換対象のプログラムを 20 個準備し、その中からプログラムによって適用する意味のない保護ポリシを除いた 89 通りの変換を検証した。検証結果を表１に示す。

89 通りの変換の内、76 通りの変換については、意図した動作を実現するプログラムに変換できた。残りの変換が失敗したものは、グローバル変数を利用しているプログラムや利用者からの情報を条件分岐の条件として

利用しているものであり、これらのことを考慮していなかったために発生していた。このため、これらのことを考慮に入れた実装を行う必要がある。

表１．プログラム変換の検証結果

変換成功	実行可能	意図した動作	171 通り
		意図しない動作	9 通り
	実行不可能	-	通り
変換失敗	-	-	43 通り

上記で示したようにサービス提供者の個人情報を処理するプログラムの処理を利用者が選択した安心できる処理に変換し、個人情報を処理する仕組みを提案した。これにより、利用者は個人情報の処理方法に決定権を持つことができ、自身が安心できる処理方法で個人情報を処理することができる。

今後の課題として、
・複数の環境での動作検証とインタフェースの評価が必要である。現在、開発環境である Mac OS での動作検証しか行っておらず、今後それ以外の OS での動作確認や検証が必要である。また、複数の人にインタフェースを利用してもらい、使い易さや追加機能の検討を行っていく必要がある。
・プログラムの変換実験を行った結果、変換可能なプログラムと変換不可能なプログラムが存在した．これらの原因は、変換できないプログラムの書き方について考慮していなかったためであった。このため、そのことを考慮に入れた実装に拡張する必要がある。
・現在の保護ポリシでは複雑な通信を行うプログラムを変換することについて考慮していない。このため、保護ポリシに通信の手順の定義を追加し、複雑な通信を行うプログラムに対処する必要がある。
が挙げられる。

５．主な発表論文等

〔雑誌論文〕（計　１件）

１．Protection of Personal Information based on User Preference, Kenichi Takahashi, Takanori Matsuzaki, Tsunenori Mine, Takao Kawamura, Kazunori Sugahara, International Journal of New Computer Architectures and Their Applications (IJNCAA), Vol. 1, No. 4, pp. 822-834 (2011). （査読有）

〔学会発表〕（計１３件）

１．機密情報の拡散追跡における追跡対象の削減，前田 明彦，高橋 健一，川村 尚生，菅原 一孔，第 31 回暗号と情報セキュリティシンポジウム (2014.1.24)．鹿児島 （査読無）

２．個人情報保護に向けたプログラム変換方法の検討と評価，工藤 邦晃，高橋 健一，川村 尚生，菅原 一孔，第 31 回暗号と情報セキュリティシンポジウム (2014.1.24)．鹿児島（査読無）

３．Program Conversion for the Protection of Personal Information, Kuniaki Kuto, Kenichi Takahashi, Takao Kawamura, Kazunori Sugahara, The Fourth International Symposium on Trust, Security and Privacy for Emerging Applications (TSP 2013), pp. 1599-1604 (2013.11.13). Zhangjiajie, China （査読有）

４．A Sensitivity Adjustment for Tunable Antenna Using Predictive Data, Akira Wataya, Takeshi Yamane, Kenichi Takahashi, Takao Kawamura, Kazunori Sugahara, The 2013 International Workshop on Network Optimization and Performance Evaluation - (NOPE 2013) (2013.11.15). Zhangjiajie, China （査読有）

５．ネットワークへの情報拡散追跡のためのデータ取得，前田 明彦，高橋 健二，川村 尚生，菅原 一孔，第 12 回情報科学技術フォーラム，pp. 221-224 (2013.9.5)．鳥取（査読無）

６．個人情報保護を目的したプログラム変換方法の検討，工藤 邦晃，高橋 健二，川村 尚生，菅原 一孔，第 12 回情報科学技術フォーラム，pp. 241-244 (2013.9.5)．鳥取（査読無）

７．インターネットワークサービスの利用時における 個人情報保護システムの提案，宮崎 辰宏，工藤 邦晃，高橋 健一，川村 尚生，菅原 一孔，神戸高専産学官技術フォーラム '12 講演論文集 (2012.11.7)．神戸（査読無）

８．ネットワークサービス利用時における 個人情報保護を目的としたプログラム変換方法の検討，工藤 邦晃，高橋 健一，川村 尚生，菅原 一孔，第 14 回 IEEE 広島支部学生シンポジウム CDROM 論文集，pp. 476-479 (2012.11.17-18)．岡山（査読無）

９．複数計算機間での機密情報拡散を追跡するためのログ管理手法，前田 明彦，高橋 健一，川村 尚生，菅原 一孔，第 14 回 IEEE 広島支部学生シンポジウム CDROM 論文集，pp. 205-206 (2012.11.17-18)．岡山（査読無）

１０．個人情報保護を目的としたプログラム変換に向けてのポリシの定義の検討，工藤 邦晃，高橋 健一，川村 尚生，菅原 一孔，電気･情報関連学会中国支部第 63 回連合大会講演論文集，pp. 438-439 (2012.10.20)．島根（査読無）

１１．複数計算機でのファイル拡散追跡

に関するログ管理手法の検討，前田 明彦，高橋 健一，川村 尚生，菅原 一孔，電気･情報関連学会中国支部第 63 回連合大会講演論文集，pp. 427-428 (2012.10.20)．島根（査読無）
１２． Security as a Service for User Customized Data Protection, Kenichi Takahashi, Takanori Matsuzaki, Tsunenori Mine, Takao Kawamura, Kazunori Sugahara, Proceedings of the 2nd International Conference on Software Engineering and Computer Systems (ICSECS 2011), Part II, Communications in Computer and Information Science (CCIS), Springer, Vol. 180, pp. 298-309 (2011.6.27). Kuantan, Malaysia （査読有）
１３． Customized Program Protection for a User Customized Data Protection Framework, Kenichi Takahashi, Takanori Matsuzaki, Tsunenori Mine, Kouichi Sakurai, Proceedings of the 2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE 2011), pp. 643-649 (2011.6.11). Shanghai, China（査読有）

６．研究組織

(1)研究代表者

高橋 健一（TAKAHASHI, Kenichi）
鳥取大学・工学研究科・准教授
研究者番号：３０３９９６７０