様式 C-19

科学研究費補助金研究成果報告書

平成２１年６月２０日現在

研究種目：若手研究（B）
研究期間：2006～2008
課題番号：18700076
研究課題名（和文）
信頼可能なプログラムによる個人情報の保護実現に向けた研究
研究課題名（英文）
Research on Personal Information Protection based on Trusted Program
研究代表者
高橋　健一（Ken-ichi Takahashi）
財団法人九州先端科学技術研究所・情報セキュリティ研究室・研究員
研究者番号：　30399670

研究成果の概要：
本研究では、サービス提供者ではなく、ユーザが情報を利用するためのプログラムを生成することでサービス提供者による情報利用に制限を与え、情報を保護するための仕組みを示す。本枠組みの基本的な考え方は、情報の所有者であるユーザも、サービス提供者による情報の利用方法を指定し、責任を持てるべきだということである。すなわち、サービス提供者だけが（サービス提供者の責任において）ユーザの情報の利用方法を決定する現在のインターネットサービスのような仕組みではなく、ユーザもサービス提供者による情報利用方法を決定する。このことで、ユーザの情報利用におけるサービス提供者の責任を軽減し、かつ、ユーザが自分自身で情報保護対策を講じることが可能になる。このことを実現するためにはユーザが情報の利用方法を定義し、その利用方法に沿ってサービス提供者に情報を利用してもらうための仕組みが必要である。そこで、サービス提供者が持つユーザの情報を利用するためのプログラムを、ユーザが書き換えることで、サービス提供者によるユーザの情報利用を制御するための仕組みを検討した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,300,452	0	1,300,452
2007 年度	1,100,812	0	1,100,812
2008 年度	1,101,541	330,000	1,431,541
総　計	3,502,805	330,000	3,832,805

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：セキュアネットワーク

１．研究開始当初の背景

近年、ネットワーク基盤の広がりによってユビキタス環境が現実のものとなりつつある。ユビキタス環境では、ユーザの通信端末がさまざまな場所に存在する機器と通信し、ユーザの活動を補助するようになると考える。このことを実現するためには個人情報の利用が必要であり、このときに個人情報を保護するための仕組みが必要になる。例えば、インターネットでの物品購入時、その代金支払いのためにクレジットカード番号の入力が求められる。しかし、クレジットカード情報は個人情報であり、ユーザは購入代金支払い以外の目的で利用されることを望まない。このため、ユーザが許可する目的以外（購入代金の支払い）で、個人情報が利用されるのを防ぐための仕組みが必要になる。

２．研究の目的

個人情報を処理するための信頼可能なプログラムをユーザが準備することで、個人情報を保護するための仕組みを検討する。本提

案では、個人情報の提供が求められると、ユーザは個人情報を処理するためのプログラムを生成し、それをサービス提供者に送信する。そして、そのプログラムで個人情報を処理することをサービス提供者に依頼し、個人情報を送信する。サービス提供者はユーザから送られてきたプログラムによって個人情報を利用する。このように、個人情報を処理するためのプログラムをユーザが準備することで、サービス提供者による個人情報の利用を制限し、ユーザが許可する目的外に個人情報が利用されることを防ぐ。

３．研究の方法

本研究ではサービス提供者ではなく、ユーザが情報を利用するためのプログラムを生成することで、サービス提供者による情報利用に制限を与えるための枠組みを提案する。このことを実現するためには、1）プログラムの生成方法や 2）サービス提供者によるプログラムの改変防止、3）サービス提供者によるプログラムの動作検証などの課題が存在する。本研究では主に 1、2 の課題に取り組み、具体化することを試みた。

４．研究成果

（１）基本的な枠組みの提案

サービス提供者はユーザの情報（ID/パスワードや年齢など）を確認し、その情報に応じたサービスをユーザに提供する。このとき、サービス提供者はユーザの情報を確認するという要求を持ち、そのことを実現するためのプログラム（*original program*）を持つ。Original program はユーザ側で実行される *client program* とサービス提供者側で実行される *service program* から構成される。client program は主にユーザの情報を（必要であれば加工し）サービス提供者に対して送信する。

このとき、情報の所有者であるユーザもサービス提供者による情報の利用方法に責任を持ち、決定できるようになるためには、ユーザが自分が持つ情報の利用方法を定義し、その定義に従ってサービス提供者に情報を利用してもらう必要がある。我々はこのことを実現するために *usage policy* と *protection policy* を定義した。Usage policy は、サービス提供者がサービス提供のためにどの情報をどのように利用する必要があるか、また original program 中のどこでその情報を利用するかを定義する。ユーザは usage policy を見ることで、自分が提供する情報が（サービス提供者によって）original program の中でどのように利用されるかを知ることができる。Protection policy はユーザがどのような情報への操作を許可するかを定義する。また、protection policy はプログラム変換ルールを持ち、プログラム変換ルールに従って original program を書き換えることで、ユーザは自分が期待する情報保護対策を講じたプログラム（*trusted program*）を生成する（図１）。サービス提供者に trusted program を利用させることで、サービス提供者によるユーザの情報利用を制御し、ユーザが安全だと思う方法で情報を守ることができる。

図 1. Trusted Program の生成

ユーザはサービスを利用するとき、そのサービスの提供者から original program と usage policy を受け取る。ユーザはユーザの情報利用を制限するための trusted program を original program から protection policy のプログラム変換ルールに従って生成し、サービス提供者にその trusted program でユーザの情報を利用することを要求する。サービス提供者が trusted program によってユーザの情報を利用することで、サービス提供者の情報利用方法が制限され、ユーザは情報を保護することができる。

（２）Trusted Program の生成

Trusted Program はプログラム変換ルールに従って生成する。プログラム変換ルールはサービス提供者による情報利用を制限し保護することが目的である。このため、プログラム変換ルールは、Original Program 中のユーザの情報を利用する操作を、ユーザが安全だと思う方法に変換できる必要がある。このことを実現するためには、どのような操作をユーザが定義した操作に置き換えたいのか，ユーザが定義した操作ではどのような値が必要になるか，それらの値の送信が許可されているか，置き換えられた操作を開始するのは誰かを定義する必要がある。また、第 3 者の介在操作や複数操作の atomicity 等を定義できる必要がある。そこで図２のプログラム変換ルールを定義した。

例えば、サービス提供者が会員確認のためにパスワードを要求する場合、パスワードの等価性を確認するための操作（equal）だけが、パスワードへの操作方法として利用できればよい。このため、サービス提供者はログインのためにパスワードを利用することが必要で、パスワードへの操作方法として equal という操作が必要であること、Original Program 中で equal 操作を実現するために必要な部分を Usage Policy で宣言する。一方、ユーザはパスワードを守るために

```
<program-conversion-rule name = name >
  <exe-side>          = <nickname> // "user", "service provider" or other entity name
  <operation-rule>    = <function> -> <function>[*{<operator><function>}]
  <operator>          = "||" | "&&" | "xor" | etc …
  <value-rule>        = <value> “from” <values> “by” <function> “at” <nickname>
  <value-attribute>   = <value> “(dis)allowed” [“to” <nickname> [*{via <nickname>}]]
  <function-rule>     = <function><real-function>
  <help>              = <nickname><address>[<third-party-rule>]
<third-party-rule>    =  operation of third party | program-conversion-rule-name>
<atomicity>           = *<program-conversion-rule-name>
  <roll-back>         = <program-conversion-rule-name>
```

図２．プログラム変換ルール

会員確認のためだけのパスワード利用を許可すること、パスワードの等価性を確認する操作を許可すること、および、プログラム変換ルールによってパスワードの等価性確認がどのように実現される必要があるかを Protection Policy で宣言する。このとき、パスワードの等価性の確認にユーザがハッシュパスワードを使う方法を安全だと考える場合、ユーザがそのためのプログラム変換ルールを定義する。このことでハッシュパスワードを利用したプログラムを動的に生成することができる（図３）。

```
// do something
id = receive("ID");
pass = receive("password");
y = findPassFor(id);
equal(pass, y) ? login success : return;
// do something
```

変換

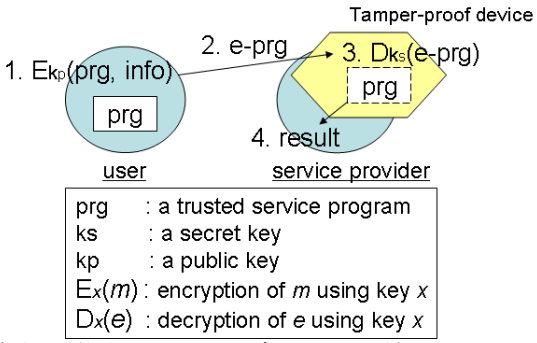
```
// do something
id = receive("ID");
r = receive("r");
hash-password = receive("password");
y = findPassFor(id);
hash-y = hash(y, r);
equal(hash-password, hash-y) ?
                  login sucess : return;
// do something
```

図３．ハッシュパスワードを利用するための Trusted Program 生成例

（３）Trusted Program の保護

Trusted Program はサービス提供者によって実行され、このとき、サービス提供者が Trusted Program の内容を解析し改変することで不正に情報を得ることが考えられる。このことを防ぐために、耐タンパデバイスを利用する方法を検討した。

ここでは、サービス提供者が公開鍵暗号を



実行可能な耐タンパデバイスを持つことを仮定する。このとき、ユーザはサービス提供者が持つ耐タンパデバイスに向けて公開鍵で暗号化した Trusted Program を送信し、サービス提供者は耐タンパデバイス内で Trusted Program を実行する（図４）。このことで、Trusted Program の解析や改変を防止できる。

図４．耐タンパデバイス利用による Trusted Program の保護

（４）今後の課題

ユーザが trusted program を生成することで、サービス提供者による情報利用に制限を与え、ユーザの情報を守るための仕組みを示した。しかし、本方式を実現するためには、サービス提供者による trusted program の実行内容の確認が必要となる。Trusted program が original program で意図したことと異なる動作を実現するのであれば、サービス提供者にとってその trusted program を利用する意味がない。このため、trusted program が適切な protection policy によって original

program から生成されたものであると検証できることが必要となる。これは、サービス提供者が original program と protection policy から実際に trusted program が生成できることを確認することや、Proof-Carrying Code のようなプログラムの動作証明書を付加することで解決できるものであると考える。

５．主な発表論文等

〔雑誌論文〕（計１件）

① Ken'ichi Takahashi, Zhaoyu Liu, Kouichi Sakurai、Makoto Amamiya, A Framework for User Privacy Protection Using Trusted Program, International Journal of Security and Its Applications, Vol.1, No.2, pp.59-70, 2007, 査読有

〔学会発表〕（計９件）

① Kenichi Takahashi, Kouichi Sakurai, A Framework for the User-Oriented Personal Information Protection, The International Conference on Security & Management, pp.12-18, 2006, 査読有

② 高橋健一、Zhaoyu Liu、櫻井幸一、ユーザ主導で個人情報を守ることが可能なプログラム生成方法の検討、２００７年暗号と情報セキュリティシンポジウム、3D3-4（CD-ROM）, 2007, 査読無

③ Kenichi Takahashi, Zhaoyu Liu, Kouichi Sakurai, An Approach of Program Analysis Prevention for Information Protection, 2007 International Conference on Multimedia and Ubiquitous Engineering, pp.35-40, 2007, 査読有

④ Kenichi Takahashi, Zhaoyu Liu, Kouichi Sakurai, Makoto Amamiya, An Approach of Trusted Program Generation for User-Responsible Privacy、Ubiquitous Intelligence, LNCS4611, pp.1159-1170, 2007, 査読有

⑤ 藤井雅和, 高橋健一, 櫻井幸一, 16th USENIX Security Symposium, および The Third International Symposium on Information Assurance and Security 参加報告, Computer Security Symposium 2007, 1B-2（CD-ROM）, 2007, 査読無

⑥ 藤井雅和, 高橋健一, 堀良彰, 櫻井幸一, 第3者の助けを借りた不正侵入検知モデルの一考察, 2008 年暗号と情報セキュリティシンポジウム, 1C2-5（CD-ROM）, 2008, 査読無

⑦ 高橋健一, Zhaoyu Liu, 櫻井幸一, プログラム書き換えによる情報保護の検討、2008 年暗号と情報セキュリティシンポジウム, 1D2-2（CD-ROM）, 2008, 査読無.

⑧ 高橋健一, 境顕宏, 櫻井幸一, 個別アドレス割り当てによるメーリングリストへのスパムメール防止方法の提案と実装, Computer Security Symposium 2008, pp.791-796, 2008, 査読無

⑨ Kenichi Takahashi, Akihiro Sakai, Kouichi Sakurai, Invalidation of Mailing list Address to Block Spam Mails, The 2008 International Symposium on Modeling, Assembly and Management for Service Oriented Engineering, pp.841-846, 2008, 査読有

〔図書〕（計０件）
なし

〔産業財産権〕
○出願状況（計０件）
なし

○取得状況（計０件）
なし

〔その他〕
なし

６．研究組織
(1)研究代表者
高橋　健一(TAKAHASHI　KENICHI)
財団法人　九州先端科学技術研究所・情報セキュリティ研究室・研究員
研究者番号：３０３９９６７０

(2)研究分担者
なし

(3)連携研究者
なし