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　孔一
（鳥取大学大学院　工学研究科　情報エレクトロニクス専攻）

Policies for Program Conversion to Protect User's Information

Kuniaki Kuto, Kenichi Takahashi, Takao Kawamura and kazunori Sugahara (Tottori University)

1.　はじめに

現在，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，サービス提供者が個人情報の提供を要求する．しかし，ユーザは一旦渡した情報をどのように利用されているか確かめることができない．この結果，ユーザはサービス提供者に疑問を感じても，情報を渡しサービスを利用するか，情報を渡さずにサービスを利用しないかの選択肢しかない．そのため，ユーザの個人情報の処理方法を指定可能な仕組みが必要となる．ユーザの個人情報はサービス提供者が持つプログラムで処理される．そこで，サービス提供者の持つプログラムをユーザが指定した個人情報の処理方法に従って変換する仕組み(プログラム変換モデル)を提供する．これにより，ユーザ自身が個人情報の処理方法を指定することができる．そのため，サービス提供者による不正利用に対抗でき，安心してサービスを利用することができる．

2.　プログラム変換モデル

プログラム変換モデルでは，サービス提供者が持つプログラムをユーザが指定した処理方法に変換する．しかし，プログラム変換するためには，サービス提供者の持つプログラムがどのような処理をどのように行うか知る必要がある．そこで，サービス提供者のプログラムの処理方法を定義するために利用ポリシを導入する．ユーザはプログラムと利用ポリシを得ることでそのプログラムがユーザのどのような個人情報を，どのように処理するか知ることができる．また，ユーザは安心だと思う処理方法を選択し，プログラムを変換する必要がある．そこで，ユーザが安全だと思う処理方法を定義するための保護ポリシを導入する．ユーザは保護ポリシを選ぶことで，自分が安全だと思う処理方法を指定することができる．図 1 にプログラム変換モデルを示す．

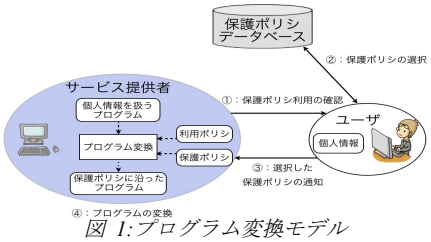

図 1:プログラム変換モデル

本モデルでは，ユーザはサービスを受ける際に保護ポリシデータベースにアクセスし，自分が安全だと思う保護ポリシを選択する．これをサービス提供者に送り，サービス提供者に保護ポリシの従ったプログラムの変換することを求める．サービス提供者は，保護ポリシ，利用ポリシによって，個人情報を扱うプログラムを保護ポリシを反映したプログラムに変換する．サービス提供者が変換されたプログラムを利用することでユーザが指定した処理方法で個人情報が処理され，安心してサービスを利用することができる．本稿では，このことを実現するためのステップとして保護ポリシと利用ポリシの定義のついて検討する．

3.　保護ポリシ

保護ポリシには利用者が安全だと思う処理方法が定義され，その定義に沿ってプログラムを変換する．図 2 に保護ポリシを示す．

```
〈EXPLANATION〉 説明
〈INFORMATION〉 information
〈OPERATION〉 operation
〈PROGRAMCONVERSIONRULE〉〈NAME〉
```

図 2:保護ポリシ

保護ポリシを選択するためにはどんな情報に対してどのような処理をするか知る必要がある．そのため，利用者に対する説明文を〈*EXPLANATION*〉に示す．これは自然言語で記述され，利用者はこれを見ることで内容を知ることができる．保護ポリシが変換対象とする情報情報は〈*INFORMATION*
〉で，変換対象となる操作は〈*OPERATION*〉で定義される．これらを読込むことで，変換対象となる情報や操作がわかる．また，プログラムの変換方法はプログラム変換ルールとして〈*PROGRAMCONVERSIONRULE*〉で定義される．サービス提供者のプログラムは，プログラム変換ルールに沿って変換される．プログラム変換ルールを表１に示す．

表 1:プログラム変換ルール

ルール名	ルールの説明
データ変換ルール	データを変換するルール
送受信制御ルール	変換前/後のデータの送受信を制御するルール
操作変換ルール	操作を変換するルール

ユーザが個人情報(データ)を守るためには，データを保護可能な形に変換することが必要となる．そのため，データを変換するためのデータ変換ルールが必要である．また，ネットワークサービスでの利用を考えると変換前/後のデータが送受信される．そのため，変換前/後のデータの送受信を制御する必要がある．さらに，データ変換前と後で同様の操作を適用できないことが考えられ，変換後のデータに対応する操作を定義する必要がある．これらのルールによってプログラムを変換する．

4. 利用ポリシ

利用ポリシにはプログラムがどのような処理をどのように行うか定義される．図３に利用ポリシを示す．

```
〈INFORMATION〉 value
〈SEND〉 method
〈RECEIVE〉 method
```

図 3:利用ポリシ

利用者は保護ポリシにより守りたい情報・操作を指定することができる．しかし，守りたい情報がプログラム中のどの変数で利用されているかわからない．そのため，情報がどの変数で利用されているかを〈*INFORMATION*〉で定義する．これにより，利用者が守りたい情報がプログラム中のどの変数に格納されているかがわかる．また，守りたい情報がどのような方法で送受信されるかを知る必要がある．そのため，送受信メソッドを定義する．送信メソッドを〈*SEND*〉に定義し，受信メソッドを〈*RECEIVE*〉で定義する．これにより，送受信メソッド名がわかり，情報の送受信制御が可能となる．

5. ポリシの適用方法の検討

変換プログラムは保護ポリシと利用ポリシを読込むことでサービス提供者の持つプログラムにユーザが安全だと思う処理方法を適用する．サービス提供者のプログラムを読込み，変数名などの情報を検索して，プログラムにプログラム変換ルールを適用する．このことを実現するために，まず，保護ポリシと利用ポリシの〈*INFORMATION*〉を読込み利用者が守りたい情報がプログラム中のどの変数に格納されているかを特定できる．ここで特定された変数に対してデータ変換ルールを適用する．同様に，〈*OPERATION*〉に示された操作に対して操作変換ルールを適用する．また，利用ポリシに定義された〈*SEND*〉と〈*RECEIVE*〉の情報をもとに送受信制御ルールを適用する．保護ポリシに定義されたすべてのプログラム変換ルールを適用することでユーザが安心だと思う処理方法が反映されたプログラムを生成できる．

6. おわりに

本研究は，プログラム変換モデルを実現する課題の一つであるプログラムの変換を実現するために，保護ポリシと利用ポリシを定義した．また，プログラム変換に必要なルールをプログラム変換ルールとして検討した．今後の課題としてプログラム変換ルールとプログラムの変換方法を実現することが挙げられる．

謝辞

本研究は科学研究費補助金（23700098）の支援を受けて行なった．

文　献

(1) NPO 日本ネットワークセキュリティ協会，2009 年情報セキュリティインシデントに関する庁舎報告書，http://www.jnsa.org/result/incident/2009.html