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**

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では，サービス提供者が個人情報の提出を要求する．しかし，ユーザは一旦渡した情報をどのように利用されるかを確かめることができない．また，情報漏洩事件(1)や不正利用なども多発している．そのため，ユーザはサービス提供者に個人情報を渡すことに不安を感じる．そこで，利用者の個人情報をサービス提供者が悪用することから守る仕組みを提案する．サービス提供者の悪用を防ぐためには利用者が個人情報の処理を制御する必要がある．本モデルでは利用者に個人情報の処理方法の処理方法を選択させ，サービス提供者にその処理方法を強制する．利用者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．そのため，本モデルでは利用者に選択された処理方法をサービス提供者が持つプログラムに反映する．サービス提供者は利用者が選択した処理方法が反映されたプログラムを通して個人情報を処理する．個人情報は利用者が選択した処理方法に従って処理されるため，利用者はサービス提供者による個人情報の悪用を妨げることができる．その結果，利用者は安心して自身の個人情報をサービス提供者に提供できる．

本稿では，本システムを実現するための最初のステップとして，利用者が選択した処理方法を反映するためにプログラムを変換する方法を検討する．

2　個人情報保護モデル

個人情報保護モデルでは，サービス提供者がもつプログラムにユーザが指定した処理方法を反映する．このことを実現するためには，サービス提供者が持つプログラムとユーザが指定した処理方法を反映するための情報が必要となる．そこで，利用ポリシと保護ポリシを定義する．

利用ポリシ

プログラムを変換するためには，サービス提供者が持つプログラムがどのような処理をどのように行うかを知る必要がある．そこで，サービス提供者のプログラムの処理方法を利用ポリシとして定義する．利用ポリシはサービス提供者がユーザに要求する個人情報ごとに準備され，ユーザは利用ポリシを得ることで，そのプログラムが個人情報をどのように処理するかを知ることができる．

保護ポリシ

提案モデルにおいて，ユーザが安心だと思う処理方法を選択し，その処理方法をサービス提供者が持つプログラムに反映する．そこで，処理方法の説明とその反映方法を保護ポリシとして定義する．処理方法の説明によってユーザは自分が安心できる処理方法（保護ポリシ）を選択でき，反映方法に従って，その処理方法をサービス提供者のプログラムに反映できる．

プログラム変換は変換モジュールによって行われる．変換モジュールではサービス提供者のプログラムを保護ポリシと利用ポリシに従って変換することで，ユーザが指定した処理方法を反映したプログラムを生成する．また，予め定義された複数の保護ポリシを管理するための保護ポリシデータベースを定義する．ユーザは保護ポリシデータベースの中から，自分が安心だと考える個人情報の処理方法に対応する保護ポリシを選択し利用することができる．図1にプログラム変換モデルの概要を示す．

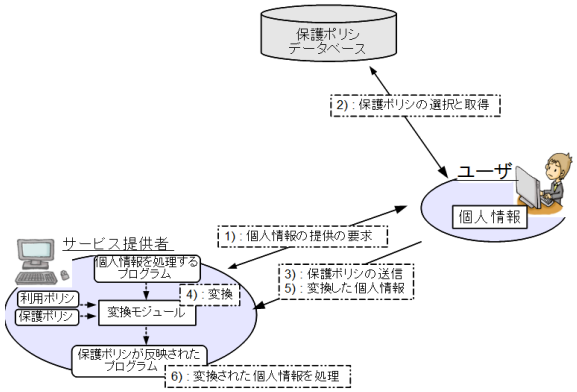

図 1　個人情報保護モデル．

1　ユーザはサービス提供者が信頼できず，個人情報を与えることに不安を感じる．そこで，ユーザは自分で処理方法を決定したいことをサービス提供者に伝え，処理方法を決定するために利用ポリシが必要であることを伝える．このため，サービス提供者は利用ポリシをユーザに送信する．

2　ユーザは利用ポリシにより，個人情報を処理するプログラムでどのような個人情報がどのように処理されているかを知ることができる．そこで，ユーザは保護ポリシデータベースにアクセスし，利用ポリシに定義された処理方法に合致する保護ポリシの一覧を得る．ユ

*　鳥取大学　工学部　知能情報工学科
**　鳥取大学　工学研究科　情報エレクトロニクス専攻

ーザはその中から最も安心できる処理方法が定義された保護ポリシを選択・取得する.

3 ユーザは選択した保護ポリシをサービス提供者に送信する.

4 サービス提供者は変換モジュールに個人情報を処理するプログラムと保護ポリシ, 利用ポリシを与えることで保護ポリシが反映されたプログラムを生成する.

5 ユーザは保護ポリシに従い, 守りたい個人情報を変換する. 変換した個人情報をサービス提供者に送信する.

6 サービス提供者は, ユーザから送られてきた個人情報を変換されたプログラムで処理する. その後, サービスをユーザに提供する.

これにより, ユーザは個人情報を安全だと思う処理方法でサービス提供者に処理してもらうことが可能となる.

3 プログラム変換方法

本システムでは, 利用者によって選択された個人情報の処理方法は利用者が選択した保護ポリシと利用ポリシに従ってプログラムに反映される. 反映はプログラム変換モジュールによって行われる. 変換プログラムの流れを図 2 に示す.

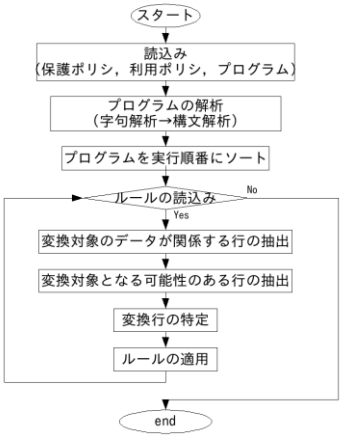

図 2 プログラム変換の流れ.

変換モジュールは保護ポリシ, 利用ポリシ, サービス提供者が個人情報を扱うプログラムを読み込む. 保護ポリシを読み込むことで, 変換対象となる情報, 操作, プログラムの変換方法(変換ルール)がわかる. また, 利用ポリシを読み込むことで, 保護ポリシが変換対象とする情報が個人情報を扱うプログラムでどの変数に格納されて処理させるかや, その情報の送受信方法を知ることができる. 利用ポリシで定義された変数を見ることでプログラム中のどの変数に守りたい情報が格納されているか知ることができる. 次に, どこでデータを変換すればいいか決定する必要がある. そこで, 反映箇所を特定するためにプログラムを解析する. 守りたい情報は利用ポリシに定義された変数に格納されている. このため, 字句解析により変数が関係する行を特定する. また, プログラム中で変数に格納されたデータは代入やメソッドに引数として渡すなどの処理が行われる. そのため, データの流れを追跡する. このことを実現するためには, 分析した字句を解析することで変数が何を示すか, また, 各行が何を示すかを意味付けする必要がある. そこで, 字句解析と構文解析を行う. これにより, 字句や文をプログラム上で意味付けできる. これらの解析を行うことでデータの流れを追跡する.

次に, プログラムをソートする. これにより, データの一流れが実際にどう行われているかを知ることができる. また, データの流れもわかるため, 変換後に正常に動作するかも確かめることができる. 他にも, 複数のクラスファイルからなるプログラムを 1 つのファイルにまとめることで, データの追跡がしやすくなる.

その後, ルールの適用箇所の候補を抽出する. ソートされたプログラムからデータが関係する行や格納される変数が関係している行をすべて抽出することで, 反映箇所の候補を抽出することができる. そこから, 変換対象となる可能性のある行を抽出する. そのため, 反映すると正常に動作しない行やデータが何らかの処理が行われた後の行などの変換しても意味のないところを削除する. 変換対象となる行が複数行ある場合は順番付けや絞り込みルールを定義し, 反映箇所を 1 つに絞り込む. 絞り込んだ行に変換ルールを反映することで変換プログラムを生成する.

上記の処理を保護ポリシに書かれたルールがすべて反映されるまで繰り返す. ルールをすべて反映することにより, 保護ポリシが反映されたプログラムを生成することができる. その後, 仮想上で生成されたプログラムをテスト実行させる. 正しく実行されれば, 変換を終了する. しかし, 実行されなかった場合は, 実行時のエラーに関わったルールの反映対象の箇所が複数存在するか調べて, 複数存在する場合は, 反映箇所を変えてルールを反映し, 再びテスト実行させる. すべてエラーの場合または複数存在しない場合は, 変換エラーを返す.

4 おわりに

本研究では, 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プログラム変換方法について検討をした. 今後の課題として, 保護ポリシと利用ポリシ, プログラム変換ルールの定義, 変換プログラムの実装があげられる.

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.

参考文献

(1) NPO 日本ネットワークセキュリティ協会, 2010 年情報セキュリティインシデントに関する調査報告書 http://www.jnsa.org/result/incident/2010.html

【プライバシー】【セキュリティ】【プログラム変換】【個人情報】