4E-5

ポリシ交渉によるユーザの同意に基づいた属性情報流通制御

畠山　誠,　五味　秀仁,　細野　繁,　藤田　悟
日本電気株式会社　インターネットシステム研究所
{m-hatake@ax, gomi@az, s-hosono@bu, fujita@cd}.jp.nec.com

１．　序論

属性情報をサービス提供プロバイダ間で流通するために、様々な技術仕様[1][2]が策定されている。これらの技術を利用することによって、プロバイダは、ユーザの属性情報をユーザからだけでなく、他のプロバイダからも取得できる。

本稿では、プロバイダ同士がプライバシポリシを交換し、プロバイダ間を流通させる属性情報とその情報の取り扱いを効率的に決定するためのポリ交渉プロトコルを提案する。単純にプライバシポリシを提示しあうだけでは、ポリシ交渉が収束しない可能性がある。そこで、プロバイダはユーザやプロバイダが規定したプライバシポリシに従いながら、少ない通信回数で流通させる属性情報とその取り扱いを決定する。

２．　プライバシポリシに基づいた属性流通

ユーザとプロバイダはあらかじめ、流通させる属性、利用目的、管理方法をプライバシポリシとして規定する。プライバシポリシは、ユーザが規定する「ユーザポリシ」(U_Policy)、属性情報を取得するプロバイダ(Attribute Receiver: **AR**)が受信する目的を規定する「受信ポリシ」(R_Policy)、属性情報を送信するプロバイダ(Attribute Sender: **AS**)が属性情報を送信する条件を規定する「送信ポリシ」(S_Policy)の 3 種類に分類した。

ユーザは、内容の異なる複数のポリシを規定しないものとする AS も同様に 1 つの S_Policy に全ての条件を規定する。しかし、AR は複数の R_Policy を規定できる。AR は属性を必要とする状況に応じて、様々な目的や条件で属性を取得することが考えられる。取得する状況が異なれば受信ポリシも異なるため、AR は複数の R_Policy を管理する。

AS が AR に属性情報を送信するためには、AR の受信ポリシが、

$$R\_Policy \subseteq (S\_Policy \cap U\_Policy) \cdots \quad (1)$$

を満たしていることを、AS が確認する。(1)を満たす場合にのみ、AS は AR に属性を送信する。しかし、AS は AR に送信できる属性を必ず持っているとは限らない。例えば、

$$S\_Policy \cap U\_Policy = \phi \quad \cdots \quad (2)$$

となる場合は、AS は AR に属性を送付しない。

AR は、AS に送付する R_Policy を変更することによって、属性を取得できるようになることがある。つまり、AR が送付した R_Policy が(1)を満たさなかった場合、AR は R_Policy を変更して再度属性を要求することができる。AR が R_Policy を変更するためには、R_Policy が最低限満たすべき条件(Requirement)を規定しておく必要がある。Requirement が規定されていれば、それを満たす範囲で AR は R_Policy を変更できる。例えば、AR は、

$$Requirement \supseteq R1\_Policy \quad \cdots \quad (3)$$

を満たす R1_Policy に従って属性を要求する。AR が、このポリシで属性を取得できない場合は、

$$Requirement \supseteq R2\_Policy \quad \cdots \quad (4)$$

を満たす R2_Policy に従って、AS に属性を要求することができる。

しかし、AR が R_Policy を変更すると、AR が(1)を満たす R_Policy を発見するまで、AS と AR の間で多くの通信が発生することが考えられる。そこで、属性情報を流通するポリシを効率的に決定するためのポリシプロトコルを提案する。

３．　ポリシ交渉プロトコル

プロバイダ間で属性情報を送受信する際に、AR と AS が互いにプライバシポリシを提示しあい、3 種類のプライバシポリシを照合することで、送受信する属性とその取り扱いを動的に決定する(図 1)。本稿のポリシ交渉では、プロバイダ同士が互いに信用していることを前提とする。

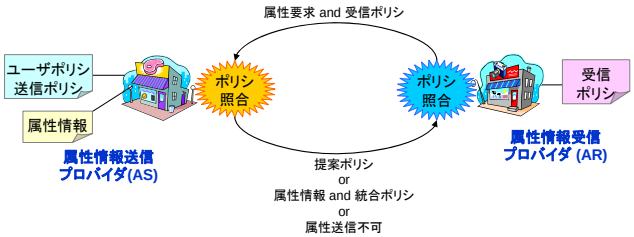

図 1 ポリシ交渉の概要

ここで、AS は U_Policy と S_Policy と属性情報を管理し、AR は R_Policy と Requirement を管理しているものとする。R_Policy は(3)や(4)を満たす形式で表現される。また本稿ではポリシの流通のみを扱い、属性要求のメッセージは扱わない。

"Attribute Exchange based on Privacy Policy Negotiation with User's Consent"
Makoto Hatakeyama, Hidehito Gomi, Shigeru Hosono and Satoru Fujita
NEC Internet Systems Research Laboratories

3.1 ポリシ照合

3.1.1 AS 側のポリシ照合

AS は、AR から送信ポリシ R1_Policy が送られてくることによって、ポリシ照合処理を開始する。

AS は最初に、AR から送られてきた R1_Policy が(1)を満たしているか判断する。満たしている場合には、AS は AR に属性情報と「統合ポリシ」(I_Policy)を送付する。この I_Policy は、

$$I\_Policy = R1\_Policy \quad \cdots (5)$$

$$I\_Policy \subseteq (S\_Policy \cap U\_Policy) \cdots (6)$$

と定義する。R1_Policy は AR が規定したポリシであるが、I_Policy は S_Policy と U_Policy に従っていることが確認されたポリシである。I_Policy を属性情報と共に送付するのは、属性情報の取り扱いを確認するためである。

R1_Policy が(1)を満たしていない場合には、AS は属性情報を送信せずに、属性情報流通を実現するための手がかりを与える。AS が「属性情報送信不可」という情報のみを送信すると、AR は再度属性を要求する可能性があり、通信回数が多くなる。

AS は手がかりとして、AR に対して、AR が取得可能な属性要素を規定する「提案ポリシ」(P_Policy)を送付する。P_Policy は以下の条件を満たす。

$$P\_Policy = (S\_Policy \cap U\_Policy)_{for\_AR} \quad \cdots \quad (7)$$

ここで、$(S\_Policy \cap U\_Policy)_{for\_AR}$ とは、S_Policy ∩ U_Policy のポリシ集合の中で、AR が取得できる属性に関するポリシの集合である。

もし、P_Policy が空集合の場合は、AS は AR に送付できる属性を持っていないことになる。この場合は、AS は AR に「送付可能な属性なし」というメッセージを送信する。

3.1.2 AR 側のポリシ照合

AR は、AS から P_Policy を取得した場合、ポリシ照合を開始する。

最初に AR は、AR 自身が取得可能な属性情報とその取り扱いに関するポリシを決定する。

$$(S\_Policy \cap U\_Policy \cap R\_Policy) \supseteq R2\_Policy \cdots (8)$$

(8)を満たす R2_Policy が空集合である場合は、AR が取得できる属性情報は存在しないことになる。この場合は、ポリシ交渉を中止する。

(8)を満たす R2_Policy が存在する場合は、AR は再度このポリシに従って AS に属性情報を要求する。ここで要求する属性は(8)を満たしているので、(1)も満たしている。

3.2 ポリシ交渉におけるメッセージフロー

ポリシ交渉は、以下のメッセージの流れになる。

A) 属性要求送付

AR は AS に対し、属性要求と R1_Policy を送付する。

B) 応答メッセージ送付

AS は AR にポリシ照合の結果を送付する。結果には、「属性情報 + I_Policy」「P_Policy」「送付可能な属性なし」という 3 種類ある。

C) 属性要求送付

AR は、AS に再度属性要求と(8)を満たす R2_Policy を送付する。

D) 属性送付

AS は AR に、「属性情報 + I_Policy」を送付する。

C)のポリシは(8)を満たすため、必ず属性が送られることになる。

4. 考察

本稿のポリシ交渉を用いると、ユーザの同意に基づいた属性情報の 2 次流通ができる。AR が AS(AS1 とする)から属性情報を取得すると AR は属性情報を管理するため AS(AS2 とする)として振舞うことができる。AS2 が取得した属性を 2 次流通するときには、AS2 が管理するユーザポリシ(U´_Policy)を、

$$U´\_Policy = I\_Policy \subseteq (S\_Policy \cap U\_Policy) \cdots (9)$$

と定義する。I_Policy は、AS2 が AS1 から取得したものであり、U_Policy の部分集合となっている。そこで、I_Policy をユーザが規定したユーザポリシとみなす。さらに、AS2 は AS2 自身が設定した送信ポリシ(S´_Policy)を利用して再度ポリシ交渉ができる。このとき、AS2 が R´_Policy というポリシを受け取ったとき、

$$R´\_Policy \subseteq (S´\_Policy \cap U´\_Policy) \cdots (10)$$

を満たす場合に、AS2 は属性情報を送信できる。

本ポリシ交渉ではプロバイダ同士が信用していることを前提としたため、ポリシを開示できた。そのため、AS は属性流通の手がかりとして(7)のポリシを送信した。AR は(7)を利用すると、確実に属性を取得できる受信ポリシを決定することができた。つまり AS と AR 間で 2 往復の通信で属性流通が完了した。しかし、プロバイダ間の信用を前提としない場合、AS は手がかりを送付しないため AR は何度も属性要求を送付する可能性がある。

5. 結論

本稿では、プライバシを考慮した属性情報流通を効率化するためのポリシ交渉プロトコルを提案した。このプロトコルを利用することによって、ユーザのポリシに基づいて、少ない通信回数で属性情報を流通できることを確認した。

参考文献

[1] Liberty Alliance Project, “Liberty ID-WSF Web Services Framework Overview”, Version 1.1, November 2003. http://www.projectliberty.org/

[2] Dick Hardt and Isabel Walcott,“The Sxip Network Overview”, Version 1.0.4, September 2004. https://sxip.org/