# 公開を前提とした情報のグループによる所有

3F－4

森川 郁也　浅野 正一郎
東京大学工学部　学術情報センター研究開発部

## 1 はじめに

今日の情報ネットワークはあらゆる点でヘテロ（異質混合）であり、プロトコルなどの異質性を下層で吸収して上位層では等質に扱えるような構築がされている。しかしサービス、とくにセキュリティに対するポリシーの異質性は吸収しきれない問題である。このようなヘテロなネットワークにおいて、ユーザグループやメーリングリストといった、物理的・社会的な枠組に捕らわれない、横のつながりをもった論理的なグループが現れている。

本稿ではこのような論理的なグループが共有する情報に対するアクセスを独自のポリシーに基づいて制御しつつ公開する方式について提案・検討する。

以下の議論では、ユーザ／サービス提供者、個人／グループ、あるいは人間／機械などの区別を問わず、情報ネットワークの参加者をエンティティと呼ぶことにする。またネットワーク全体にわたって信頼しうる秘密通信・認証系として、RSA などの公開鍵暗号系[1]を仮定する。

## 2 公開を前提とした情報の所有

ある情報を公開して閲覧者に見せた場合、それが電子化された情報であれば、閲覧者がその情報を複製・保存し、さらに他人へ二次配布することは容易であり、これらを防ぐことは事実上不可能であると思われる。

そこで本稿では、複製の配布を防ぐのではなく、信頼したい情報は情報提供者から直接得るべきである、という立場をとる。たとえばある情報が公開されていることを、（ときにおおまかな）内容も含めて間接的に知ったエンティティが内容を確認するためには、その情報を提供者から直接得ればよい、という立場である。

この立場によれば、公開情報を所有するということは何らかの裏付けの下で正当に公開できるということであり、ディジタル署名[1]と組み合わせることでより強力な裏付けが可能である。さらにこの実現には情報を知りたい者が情報提供者から直接情報を得る仕組みが必要であり、従来のマスコミュニケーションを中心とした情報伝達では情報を知りたい者と提供者の間に第三者が介在せざるを得なかったが、情報ネットワークの普及によってより直接的な情報入手が可能となっている。

## 3 公開情報のグループ所有モデル

公開情報をグループで所有する一手法の、とくに公開に関する部分について提案・検討する。情報は万人に公開されても良いが、ここでは所有者グループ（$G_O$）によって定められた閲覧者グループ（$G_V$）にのみ公開されるものとする。これらのグループは物理的に近いエンティティ同士のみならずネットワークに広く散らばった論理的なグループをも想定している。また所有・公開する情報は検索を必要とするような大規模なものではなく、広報のような比較的小規模で単純な構造のものを想定している。

**所有者グループ $G_O$** 公開情報の本来の所有者であり、情報を誰に公開するかの判断、情報の改変などの権利をもつ。メンバには $G_O$ の閲覧鍵（暗号化・復号共通の秘密鍵）として $K_O$ が知らされる。

**閲覧者グループ $G_V$** 公開情報の閲覧を $G_O$ に認められたエンティティのグループであり、閲覧によって得た情報を無闇に配布したりしないよう $G_O$ によって一応の承認を受けたエンティティの集合である。メンバには $G_V$ 用の閲覧鍵として $K_V$ が知らされる。

**グループサーバ $S$** $G_O$ の運用するサーバであり、公開情報へのアクセスの制御などを司る。$S$ の実際の運用は $G_O$ のメンバの一人が代表して行なってもよいし、グループ外のエンティティに運用を依頼してもよい。$S$ は与えられたメンバリスト（$G_O$ と $G_V$ のもの）に従って情報の入出力をするのが主な役目で、暗号化や復号は行なわない。

### 3.1 情報の登録

所有者グループ $G_O$ はディジタル署名を施した公開情報 $P$ をランダムに生成した鍵 $K_R$ で暗号化し、暗号

---

Group ownership of information assumed to be open to the public
Ikuya MORIKAWA[1], Shoichiro ASANO[2]
[1]Faculty of Engineering, The University of Tokyo
[2]Research & Development Department, National Center for Science Information Systems

化情報 $C = E_{K_R}(P)$ をグループサーバ $S$に登録する。さらに $K_R$を、$G_O$の閲覧鍵 $K_O$および $G_V$の閲覧鍵 $K_V$で暗号化し、$K_{OR} = E_{K_O}(K_R)$ および $K_{VR} = E_{K_V}(K_R)$ を $S$に登録する。なお $K_O$や $K_V$自体は $G_O$が生成してグループ内で保持するもので、$S$には知らされない。

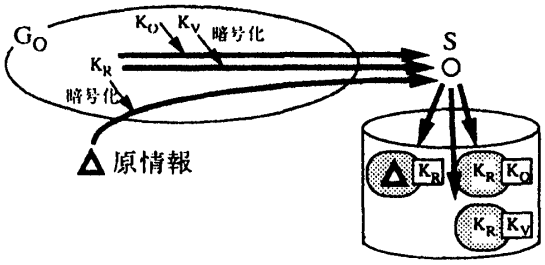


図 1: 公開情報の登録

### 3.2 情報の閲覧

サーバ $S$が閲覧の要求を受けた場合、あらかじめ与えられたメンバリストによって相手が $G_O$あるいは $G_V$のメンバであることを確認する。

$G_O$のメンバからの要求ならば、$S$は $K_{OR}$および $C$を送信する。所有者メンバは $K_{OR}$を復号して $K_R$を得、これを用いて $C$より $P$を復号する。

$G_V$のメンバからの要求ならば、$S$は $K_{VR}$および $C$を送信する。閲覧者メンバは $K_{VR}$を復号して $K_R$を得、これを用いて $C$より $P$を復号する。

### 3.3 新規閲覧者の登録

新たに閲覧を希望する者、すなわち $G_V$に加入したいエンティティが現れた場合には以下のようにする。

新たに閲覧を希望する者 $X$の要求を受けたサーバ $S$はまずその旨を $G_O$のメンバに広報する。メンバは（多数決をとる、新規閲覧者の受け入れを判断するサブグループに委ねる、などの所定の合意方法で）受け入れを採決し、その結果を $S$に伝える（$S$が裁定役を行なってもよい）。さらに $G_O$は $K_V$を $X$の公開鍵で暗号化して $S$に預けておく（$K_{XV}$とする）。

$X$を受け入れるならば、$S$は $G_V$のメンバリストに $X$を追加し、$K_{XV}$ を $X$に送る。$X$は $K_{XV}$を自分の秘密鍵で復号し $K_V$を得る。これで $X$は $G_V$に登録されたこととなる。

### 3.4 検討事項

上述の方式の特徴として、所有者グループが独自のグループローカルな判断基準（ポリシー）で閲覧者グループのメンバを登録できる点が挙げられる。

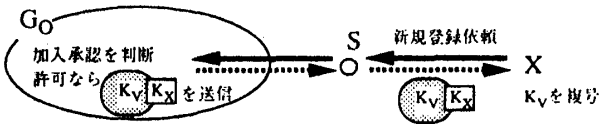


図 2: 新規閲覧者の登録

またサーバ $S$には原情報 $P$やその暗号化に用いられる鍵 $K_R$、$K_O$、$K_V$が知られないため、$S$の運営を所有者でも閲覧者でもない第三者に依頼することも可能である。

情報 $P$へのアクセス制御は、メンバリストによる確認と暗号化によって二重に行なわれている。通信の盗聴やなりすましによってメンバリストの確認をパスしても、情報を復号することはできない。公開鍵暗号系によって秘密通信を行なえば一層の安全が確保できる。

もちろん情報を復号できないということは、閲覧者グループ $G_V$のメンバが $K_V$を漏出しないという前提に基づいているが、その危険を最小限にするために所有者グループ $G_O$による $G_V$のメンバのチェックが行なわれるのであり、また漏出が露見すれば $K_V$および $K_R$を変更し原情報 $P$および $K_R$ を暗号化しなおすことで、それ以降の原情報の漏出を防ぐことができる。メンバの脱退についても同様の操作で実現できる。鍵の再配布の手間を省くため、$K_R$は所有者グループと閲覧者グループで異なる二つの鍵（$K_O$と $K_V$）で暗号化されている。

## 4 むすび

本稿では論理的なグループにも適合する公開情報のグループ所有について、とくにその公開の運用法を検討した。本方式の特徴としては、グループサーバに情報が漏れないため第三者に運営を依頼できること、所有者グループ独自の判断基準によって閲覧者グループのメンバを登録することが可能であること、などが挙げられる。

所有者グループ内での合意のとり方、所有者グループのメンバの変化、情報の改変のような他のグループ活動、およびスケーラビリティなどについてのさらなる検討が今後の課題である。

## 参考文献

[1] R. L. Rivest, A. Shamir, and L. Adleman : "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", CACM Vol. 21 No. 2 (Feb. 1978)

[2] 大田, 清水 : "暗号を用いた共有情報参照制御方式の検討", 信学技報 OFS93-31 (Jan.1994)