本資料について

本資料は下記論文を基にして作成されたものです．文書の内容の正確さは保障できないため，正確な知識を求める方は原文を参照してください．

齋藤孝道　梅澤健太郎　奥乃博
プライバシーを重視するアクセス制御方式の一方式
電子情報通信学会論文誌 D-I Vol.J84-D-I No.11
pp.1553-1562 2001年11月

プライバシーを重視するアクセス制御システムの一方式

渡邊研究室
00J120　保母雅敏

はじめに

- 認証と権限管理(アクセス制御)は区別されないことがある
  - UNIXにおけるアクセス制御(ユーザ名･パスワード)
  - PKIX(PKI with X.509)における認証(IDによる権限管理)　etc.
- アクセス制御に“認証”という過程が含まれる
  - 「誰がどのようなサービスを利用したか」が知られてしまう
- アクセス制御において、利用者を知る必要がない場面
  - ネットワークを利用したサービスを享受する際のプライバシー問題
- 認証をせずアクセス制御だけを行う方法
  - SPKI(Simple PKI)の枠組みを利用した方式

公開鍵を用いたアクセス制御

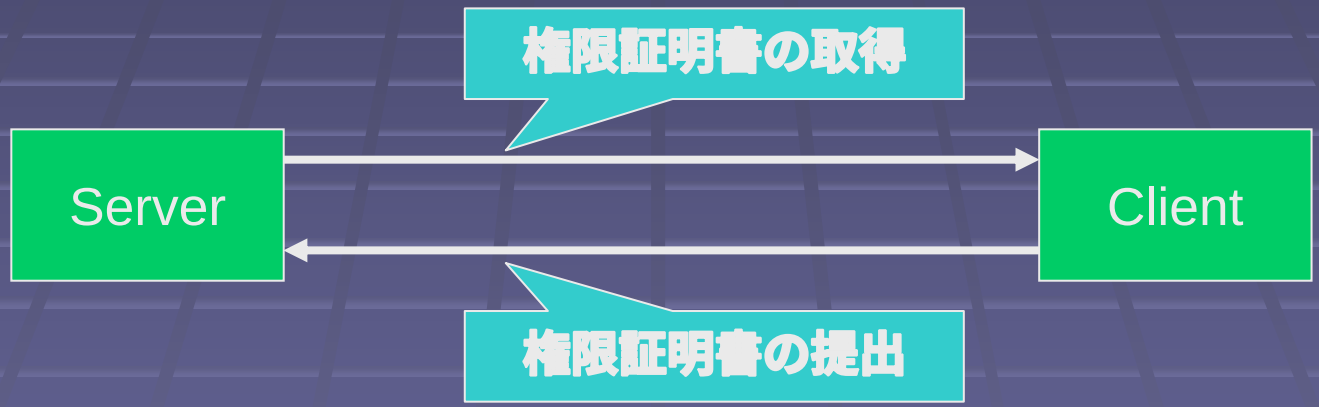
- “ID情報” “公開鍵” “権限” に基づいている
- ID証明書(ID情報・公開鍵)
  - ID情報と公開鍵の組を発行者が電子署名したもの
  - 発行者の信頼に応じて、公開鍵がある主体の物であると信頼できる
- 権限証明書(公開鍵・権限)
  - 公開鍵と権限の組を発行者が電子署名したもの
  - サーバによって発行され、最終的にサーバに戻ってくる
- 属性証明書(権限・ID情報)
  - 権限とID情報の組を発行者が電子署名したもの
  - ACL(Access Control List)として知られている

SPKIの特徴

- 権限証明書を用いたアクセス制御
- プライバシーの確保
  - ID情報を含まないため、証明書からID情報を推測する事が出来ない
- 効率的で簡潔な枠組み
  - 証明書のやりとりが閉じているため、第三者機関などの基盤が不要
- 権限委譲の容易性
  - 権限をID情報に直接関連させていないため、当事者間での証明書の委譲が可能
- 特定サービスへの非依存性
- 自己証明可能な証明書
  - 第三者を介さずに、証明書の正当性を確認することが可能

SPKIにおけるアクセス制御

- ID情報を知らせずに所有者の権限を保証する方法

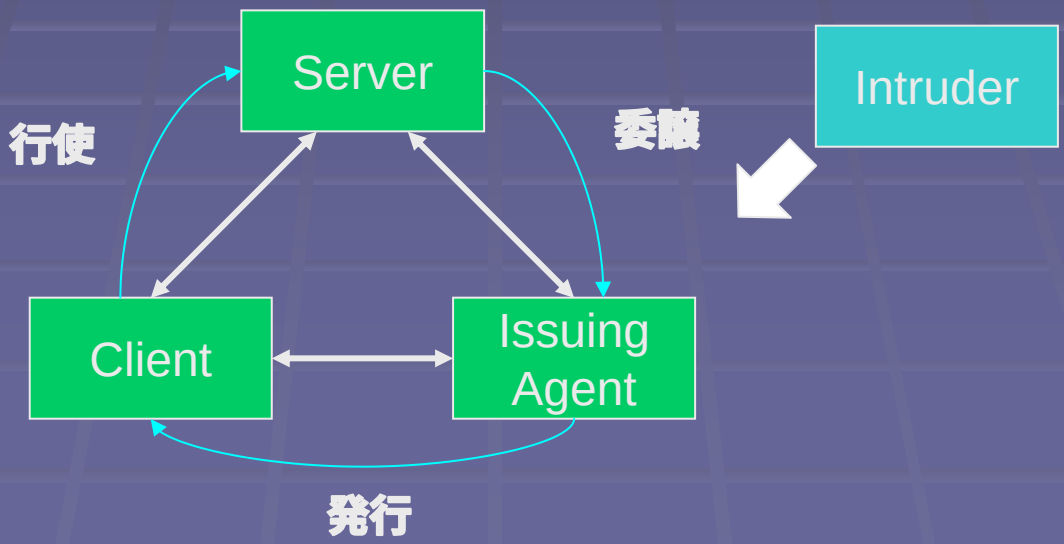


匿名のアクセスは許可するが、
利用者は選別したいという矛盾した要求

→SPKIでは選別方法が提示されていない

システムの仕様

- ID情報を含まない権限証明書の利用
- 権限の発行(認証)と行使(権限管理)の分離
  →“匿名アクセス”と“利用者の選別”を解決
- 信頼できる第三者の導入
  - 利用者を区別し、どのような権限証明書を発行したかを保管
  - サーバは独自の名前空間を持たなくても良い



予想される脅威

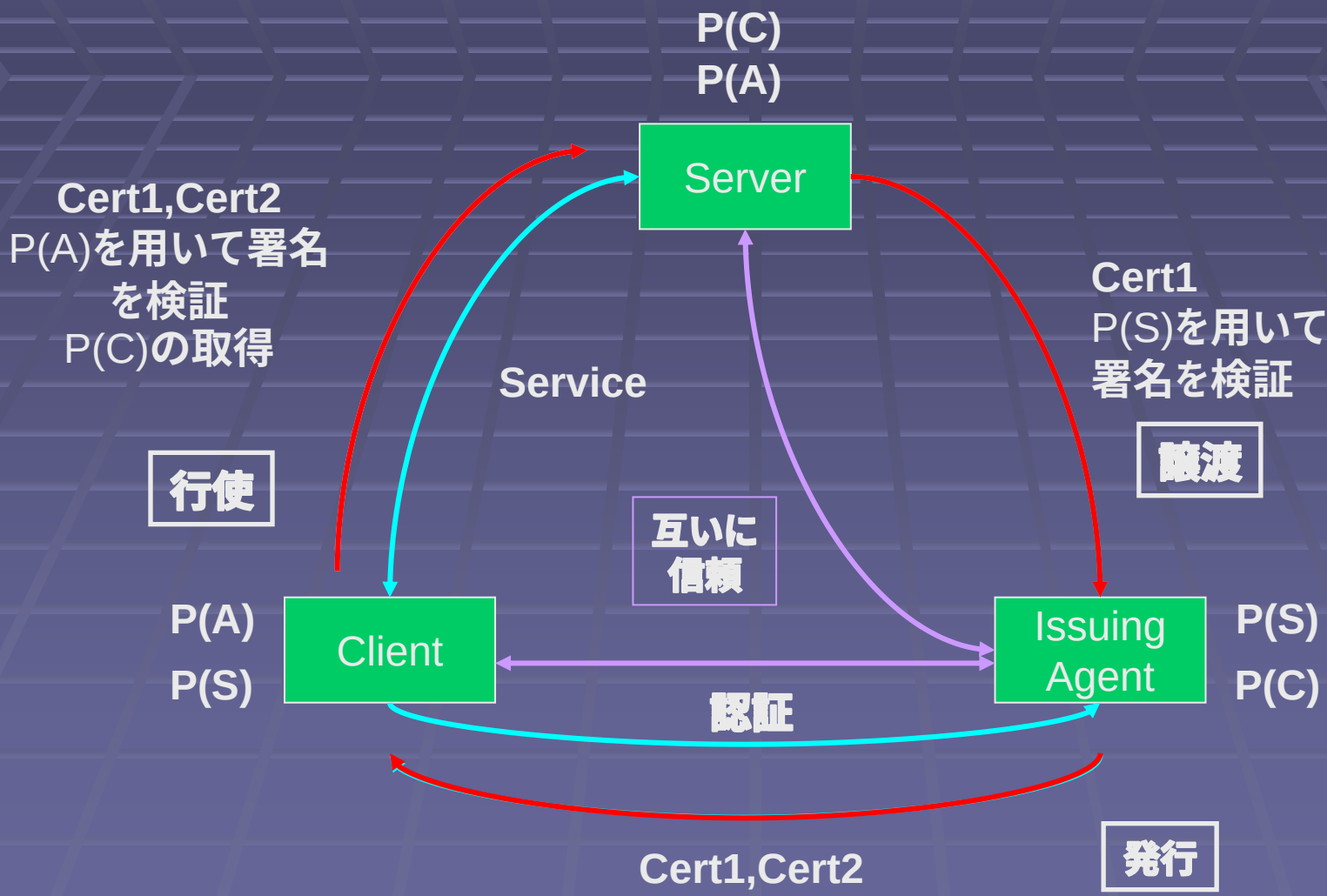
- **傍受**(Interception)
  - 侵入者が通信を傍受すること
- **改竄**(Modification)
  - 侵入者が通報を奪い取り、書き換えて正常な通報のように送信すること
- **捏造**(Fabrication)
  - 侵入者が不正な効果を生むために生成した情報を送信すること
- **なりすまし**(Masquerade)
  - 侵入者が異なった正当な主体である振りをすること
- **サービス拒否**(Denial of Service)
  - 侵入者がシステム資源を使用できない状態にすること

- DoS**攻撃を防ぐのは難しい**

システムを構成する主体

- Server
  - Clientに対してサービスを提供する主体
  - 2枚の権限証明書(Cert1,Cert2)をClientから受け取り、対応するサービスを提供する
  - IAに対して権限証明書(Cert1)を発行する
- Issuing Agent
  - Serverから権限証明書(Cert1)を受け取り、Clientに対応した権限証明書(Cert2)を発行する主体
  - ACL等のポリシーを保持し、ユーザIDと公開鍵及び権限の対応を用いて提供するサービスを決定する
  - 認証し特定したClientに対して権限証明書(Cert1,Cert2)を委譲する
- Client
  - IAから委譲された権限証明書(Cert1,Cert2)をServerに提示してサービスを享受する主体
  - 予め自己のユーザIDをIAに登録する

システムの概要


P(C)
P(A)
Server
Cert1,Cert2
P(A)を用いて署名を検証
P(C)の取得
Service
Cert1
P(S)を用いて署名を検証
行使
譲渡
互いに信頼
P(A)
P(S)
Client
Issuing Agent
P(S)
P(C)
認証
発行
Cert1,Cert2
P(A)を用いて署名を検証
Serverの公開鍵P(S)を取得

委譲

- ServerがIAに対し「権限証明書(Cert2)を発行する権限」をCert1を用いて譲渡する
  - Cert1 =
    <P(S),P(A),(委譲の可否),(権限の上限),(有効期限)>
    を秘密鍵S(S)で署名したもの

  Ex. Cert1=<P(S),P(A),(TRUE),(file1,file2),(7/Jan/2000)>

- IAはP(S)を用いてCert1の正当性を検証し、受信確認をServerに返す

発行

- IAは権限証明書(Cert2)を発行し、Cert1と共にClientに譲渡する
  - Cert2 =
    <P(A),P(C),(委譲の可否),(権限の上限),(有効期限)>
    を秘密鍵S(A)で署名したもの
    ※権限の上限はCert1のものをこえてはならない

    Ex. Cert2=<P(A),P(C),(FALSE),(file2),(5/Dec/1999)>
- ClientはP(A)を用いてCert2の正当性を検証する
- P(S)を獲得することにより、Cert1の正当性を検証する

行使

- ServerはClientから提出された権限証明書を検証する
  - Cert1に含まれるP(S)がServer自身のものかどうか
  - Cert1の電子署名の検証
  - Cert1とCert2に含まれるP(A)を比較
  - Cert2の電子署名の検証
- 検証された2枚の権限証明書を簡略化する

  Ex. <P(S),P(C),(FALSE),(file2),(5/Dec/1999)>

- 作成された情報を元に、Clientにサービスを提供する
  - P(C)を用いて暗号通信を行う

提案方式の利点

- ID情報を利用しないアクセス制御
  - サーバにID情報を晒さないアクセス制御を可能にする
  - 個人情報漏洩を考慮したアクセス制御の一つの解決策
- 権限を持つサーバによって証明書が発行される
  - サービスを提供するサーバは、委譲する権限と証明書の管理を支配下における
  - 証明書は発行者に戻ってくるので、フォーマットの変更が容易
- サーバは独自の名前空間を持たず、信頼できる第三者の持つ名前空間を利用する
  - アクセスしてくる主体のIDを管理する必要がない
  - データベース管理負荷の軽減

匿名アクセスと管理

- サービスを提供する範囲
  - Issuing Agentの管理下にあるClientが対象
- アクセス制御
  - 権限証明書の発行と行使の分離により、制限のあるアクセス制御が可能
- Clientの匿名性
  - 権限証明書にはID情報は記載されないため、ID情報をServerに示すことなくアクセス可能
  - Clientの匿名性はIssuing Agentの方針に依存

提案方式の安全性

- 権限証明書の改竄
  - IAがClientを認証する際に発生
  - 電子署名により、改竄はServerによって容易に発見可能
- 証明書の不正入手
  - 通信傍受により、不正入手は可能
  - 提出されるCert2に含まれるP(C)に対するS(C)を所持しているのは正規のClientのみである
- 証明書の複製
  - 同一の証明書は、シリアル番号やClient用の公開鍵で発見可能
  - 複数回利用の際はClientを認証
- 証明書の再発行
  - IAより再発行を受ける
  - 失効した証明書をServerに通知

証明書の失効

- PKIXでは、CRL(Certificate Revocation List)またはOCSP(Online Certificate Status Protocol)によって証明書失効を確認
  - CRLはリストが膨大になり、確認するまでのタイムタグが大きい
  - OCSPは必要に応じてオンラインで確認するため、トラフィックに応じたインフラが必要
- SPKIでは、証明書がServerに戻ってくるため、Serverが証明書失効を自由に行える

まとめ

- プライバシーを重視した安全なアクセス制御方式を提案
- 権限行使にID情報は必要ないSPKIの枠組みを利用
- Issuing Agentの導入によって、証明書発行と行使を分離
  - プライバシーを重視し、適切なクライアントに適切なサービスを提供することが可能

おわり

証明書の簡略化

- 以下の条件の時、複数の証明書を簡略化することが可能

Cert1 = <T1,S1，D1,A1,V1>
Cert2 = <T2,S2，D2,A2,V2>　　のとき

S1 = T2　かつ　D1 = TRUE　ならば

<T1,S2，D2,AIntersect(A1,A2),VIntersect(V1,V2)>

AIntersect(A1,A2)：A1，A2の共通する権限
VIntersect(V1,V2)：V1,V2のうち先に期限切れとなる値