3D－7

ディレクトリシステムに基づく認証処理のための INサービスデータ管理機能に関する一検討

山田秀昭　野村眞吾　中尾康二
国際電信電話株式会社　研究所

１．はじめに

インテリジェントネットワーク(IN)上で実現される通信サービスの多くは、ユーザの認証を必須としており、安全な認証処理の実現は IN における重要な検討課題の一つである。特に IN での実現が望まれているモビリティサービスでは、ユーザが複数の網を移動（ローミング）するため高度な認証処理を必要とする。IN でのユーザの認証方式としては、網内に閉じたユーザ認証のみでなく、遠隔網での認証も可能で、かつモビリティサービスを含めた各種通信サービスへの適用性の高い[3]、チャレンジ応答型認証方式（CR 認証方式)が、有力視されている。

本稿では、サービスデータ機能(SDF)を中心として、CR 認証方式を実現するための具体的な実現方式の検討を行う。

２．IN SDF モデルと CR 認証方式

（１）IN SDF の機能モデル

最新の IN 勧告である能力セット１(CS1)では、図１に示す SDF の機能モデルを規定している[1]。図１で、SDF data_manager（SD_M）はサービスデータへのアクセス機能を、Security manager (SC_M)は SCF のアクセス権の確認等のセキュリティ管理機能を提供する。格納管理されるデータは、サービスの実行に必要な Service data、認証に用いる Authentication data、さらにこれらのデータへのアクセス権管理の制御情報などの Operational data に分類される。また SDF へのアクセスプロトコル、及びデータ格納形態については、汎用的なデータベースアクセスプロトコルである X.500 ディレクトリを採用している。

（２）CR 認証方式

CR 認証方式では、乱数等の時変情報 (C)とこれを認証用の関数(fk)により処理した結果(R=fk(C))の組（C/R ペア）を用いて、C をユーザに発行して返される値が R であることを確認することで網がユーザを認証する。ここで fk は、網毎に異なる認証用秘密関数(f)をユーザ毎に異なる鍵(K)により動作させる関数である。認証の安全性を確保するためには、認証の度に C/R ペアを変える必要がある。

CR 認証方式を既に採用している GSM 等の移動体通信網（非 IN）では、ユーザがローミングしている間はローミング先の網（Visited 網）でユーザ認証を行う。Visited 網は、ユーザが契約している網（Home 網）から C/R ペアをあらかじめ複数獲得して格納しておき、ユーザ認証時にこれを使用することにより、Home 網にアクセスすることなく効率的なユーザ認証を実現する（VLR 方式）。この時 Visited 網では、認証で使用した C/R ペアの個数を管理し、不足した場合には Home 網から新たな C/R ペアを獲得する。

Home 網では、獲得要求に答えて C/R ペアを複数生成する必要があり、また R の生成に用いる鍵 K を厳重に格納／管理している。

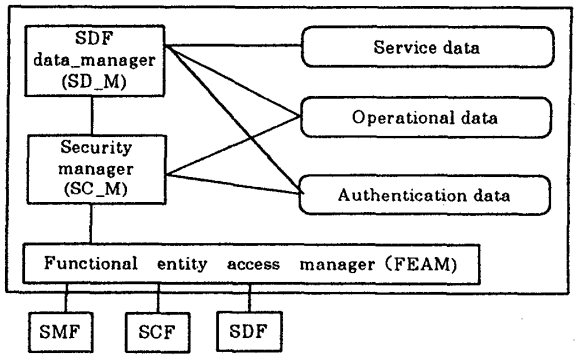

図１：SDF の機能モデル

３．IN における CR 認証方式の実現

３．１検討課題

IN において CR 認証方式を実現するためには、以下の課題を解決する必要がある。

（１）ディレクトリによる CR 認証方式の実現

IN においては、SDF のサービスデータへのアクセス制限を管理する機能として SC_M を定義し、その機能の整理が行われているが、未だ概念的なモデルとなっており、CR 認証方式に適用できる認証機能の実現性については明確となっていない。特に SDF アクセスプロトコルとして採用されたディレクトリを用いた、C/R ペアの格納管理機構など、CR 認証方式の実現性を検証しておく必要がある。

（２）鍵 K の管理における安全性

CR 認証方式では、鍵 K が露呈するとその鍵 K を持つユーザになりすますことが可能となり、認証の安全性が著しく損なわれる。現状の CR 認証方式では、Home 網において、ユーザ毎の多くの鍵 K が管理されており、これらすべてについて厳重なアクセス管理が必要となる。このため安全性の維持コストが高いだけでなく、露呈する可能性は否定できない。

A Study of IN SDF for User Authentication based on Directory system
Hideaki YAMADA, Shingo NOMURA, Kouji NAKAO
KDD R&D Laboratories

従って、INでCR認証方式を使用する場合においては、鍵Kの安全かつ効率的な格納を実現していく必要がある。

3．2 CR認証方式の実現手法

CR認証方式に用いるC/Rペアはサービスの実行時に必要となるデータであり、INにおいてはSDFで管理することとなる。SDF機能モデルにおいては、C/Rペアは Authentication data に対応し、C/Rペアへのアクセス制限などの情報はOperational dataに対応する。一般に認証に関与する機能モジュールを限定することで認証の安全性が確保できることや、認証用に格納すべきデータの管理が必要であることから、SDFのSC_Mの機能としてC/Rペアの管理、獲得機能が実現できることが望ましい。以下では、ディレクトリを用いてこれらの機能が実現できることを示し、さらにCR認証方式の安全性の向上について検討する。

（1）ディレクトリによるCR認証方式の実現

C/Rペアの管理では、まずディレクトリでの格納形態を決定する必要がある。C/Rペアの格納形態としては、エントリ、属性、属性値の何れかに対応させることが必要である。C/Rペアをエントリに対応させた場合、C/Rペアの格納時に格納する個数分の格納操作（Add Entry）を発行する必要があり、操作が煩雑となる。属性値に対応づける場合は、最小アクセス単位が属性であるため、検索操作（Search）を行った後、検索されたC/Rペアの中から使用するC/Rペアを選択する必要があり、処理が複雑となる。これに対し、個々のC/Rペアを属性に対応づければ、C/Rペアの格納（Modify Entry の Add Atribute 操作）、検索がそれぞれ一回の操作で可能となるので、C/Rペアの格納方式には、この方式を採用する（図2）。なお、アクセス制御のためのOperational dataは、ディレクトリでそれと等価な属性であるOperational属性に対応させることでAuthentication dataへのアクセスをSC_Mのみに限定させることが可能である。

さらに、認証の度に異なるC/Rペアを使うため、使用したC/Rペアを削除する機能が必要となる。また、C/Rペアの不足時にHome網へC/Rペアの追加要求を行うために、有効なC/Rペアの個数を管理する必要がある。これらの機能は、サービスに依存しない共通的な処理であり、SDF内のSC_Mの機能として位置づけることができる。SC_Mの機能とすることで、サービス制御機能(SCF)からのアクセスはC/Rペアの入手要求のみに限定することが可能であり、C/Rペアの管理機能はSC_Mが一括して行うことで安全性の確保が容易となる。

以上により、ディレクトリを用いてCR認証に必要なデータの管理が可能である。

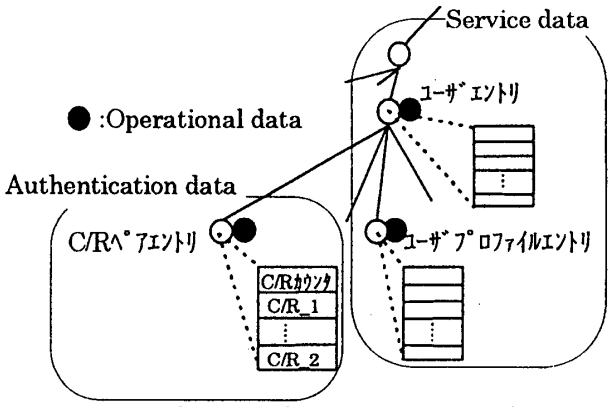

図2：データのディレクトリ格納形態

（2）鍵Kの管理における安全性

Home網ではユーザ毎に異なる大量の鍵Kを格納保管するため、その秘匿性維持が問題となる。そこで本稿では、図3に示すようにVisited網からの要求毎にユーザIDを用いて鍵Kを生成し、得られた鍵Kを用いてC/Rペアを生成する方式を提案する。C/Rペアの生成については実時間性に即した生成が可能であり、大量の鍵Kを格納する方式と比べ、本方式では鍵生成用の関数(g)と秘密関数fのみを保管すればよい。このため個々のユーザの鍵Kの厳重なアクセス管理が不要となるだけでなく、鍵Kの露呈によるCR認証方式の安全性の低下を防ぐことができる。

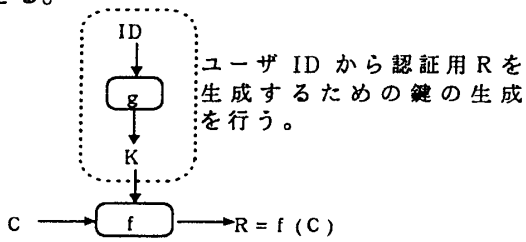

図3：C/Rペアの生成機構

4．まとめ：

本稿では、ディレクトリアクセスに基づくSDFを前提として、IN上でのCR認証方式の実現について検討した。その結果、CR認証方式を実現するために必要なSDF機能の提案を行い、ディレクトリにおける認証データの格納形態を提示した。これによりCR認証方式が、ユーザ認証を必要とするモビリティサービスに代表される多くのINサービスにて実現できる見通しを得た。

今後はこれらの検討に基づいたSDF機能の実装を行い、機構の有効性の検証を行う予定である。最後に、日頃ご指導を戴くKDD研究所浦野所長、福光次長、若原交換グループリーダに感謝致します。

参考文献：[1]ITU-T Q.121X シリーズ勧告 1995.
[2]ITU-T X.500 シリーズ勧告 1993.
[3]中尾康二、山田秀昭：“高度INのための認証方式の提案”、電子情報通信学会 1995.9