指紋認証を用いた情報通過制御に関する一考察

5N－2

藤原 豊　大塚 浩昭　岡部 恵一　河田 悦生
NTT 情報通信研究所
e-mail: {yutaka,ohtsuka,okabe,kawada}@dsa.isl.ntt.co.jp

1. はじめに

ネットワーク化の進展に伴い目的・安全性等異なるドメインの接続要求が増大している．しかし，無条件な接続はネットワーク全体としてのセキュリティが確保できなくなるため，ファイアウォール等ドメインのゲートウェイ(関門)となる場所での通過制御が重要な問題となっている．

本稿では，指紋情報をクライアント及びゲートウェイで統合的に活用することによる安全性が高く効率的な情報通過制御方式について考察する．

2. 指紋認証

バイオメトリクス(指紋・虹彩等)によるユーザ認証[1]には，知識による認証(パスワード等)，持ち物による認証(カード等)に比べて，忘れない・紛失しない・盗まれないという特徴がある．指紋照合は，他バイオメトリクスと比べて，精度が高く，最近，低価格化が実現されつつあり，パソコンでの認証に適している．本稿では指紋認証を用いたアクセス制御について考える．

3. 指紋認証を用いたアクセス制御方法

クライアント，サーバ，それらの間にゲートウェイが存在する構成を考えたときに，指紋認証を用いた，サーバに対するアクセス制御方法は大別して以下の 3 種類があると考える．

(1)クライアント側で指紋認証

例えば，IC カードに 指紋情報，認証情報(パスワード等)を格納しておき，クライアント端末で指紋照合を行い合格した場合に，認証情報をサーバに送信する方式である．照合のための指紋情報・サーバに送信する認証情報を IC カード等で保持するためネットワークから隔離されていること，サーバに指紋情報を渡す必要がないこと等の特徴がある．

(2)サーバ側で認証

Web サーバ等に用いられているものが研究開発されている[1]．サーバに指紋情報を格納し，クライアント端末から指紋情報を送信し，サーバにて指紋照合を行う方式である．サーバ毎に指紋認証をカスタマイズできる．指紋認証できるように，サーバを改造する必要がある．

(3)ゲートウェイで認証

ネットワークのゲートウェイとなる場所に指紋を登録しておき，クライアント端末からゲートウェイに指紋情報を送信し，ゲートウェイにて指紋照合を行う方式である．指紋照合に合格した場合に，サーバに対するアクセスを許可する．

本稿では，指紋照合できるように個別にサーバを改造する必要がなく，サーバに対するアクセス制御を行うことができ，指紋の管理，通過制御を一括して行えるゲートウェイでの指紋認証を行う方法について述べる．

4. 指紋認証を用いたゲートウェイでのアクセス制御

ゲートウェイでの指紋認証システムを考える上で，実用性を考慮し，市販のファイアウォール製品に改造なしに指紋認証システムを組み込むことが重要である．その際，ネットワーク上を流れる指紋情報を保護し，ファイアウォールで指紋認証を利用できる必要がある．

4.1 指紋情報の保護

指紋情報を悪意の第三者に盗み見された場合，当人になりすまされサーバにアクセスを許してしまうことになる．そればかりか，指紋は，生涯不変のものであるため一度当人と当人の指紋情報の組が悪意の第三者にわたってしまった場合，一生悪用されつづけてしまうことになる．このようなことから，指紋情報を悪意の第三者から保護することが必要になる．

悪意の第三者から指紋情報を保護する手段として暗号化が必要である．また，暗号化していても暗号化鍵が

A study on access control system using fingerprint authentication
Yutaka FUJIWARA, Hiroaki OHTSUKA,
Keiichi OKABE, Etsuo KAWADA
NTT Information and Communication Systems Labs.

毎回同じでは，悪意の第三者が，暗号化したものを盗み見し，そのまま，照合機関に送信することにより，なりすまされてしまう(リプライ攻撃)．このため毎回異なる暗号化鍵で指紋情報を暗号化する必要がある．

指紋情報を送信する前に，指紋情報を暗号化するセッション鍵を生成し，公開鍵暗号方式を用いて，共有する．このやりとりを指紋情報送信のたびに行う．

4.2 ファイアウォールでの指紋認証

ファイアウォール製品は，ユーザ名・パスワードによる利用者認証ができるものとする．ファイアウォール製品にて外部認証装置に認証を依頼する機構としてRADIUS[2]が用いられている．RADIUS のパスワードフィールドに指紋情報を載せる方法が考えられる．しかし，現在の RADIUS の仕様上，サイズが十分でない．また，クライアント－指紋照合サーバ間で，毎回異なる暗号化鍵を交換し，指紋情報を暗号化する仕組みを RADIUS では提供できない．そこで，次の方法を考え試作した．

クライアント端末から，ユーザ名・指紋情報の組を受け取り，指紋認証を行い，認証に合格した場合，ファイアウォールにユーザ名・パスワードを送信する認証サーバと，クライアント端末で動作し，認証サーバからの要求に応じてユーザ名・指紋情報を送信する指紋取得デーモンが試作のポイントである．以下に処理の流れを示す．

(1)認証サーバ上に，ユーザ名，指紋情報，パスワードを登録しておく．ファイアウォール上に，認証サーバに登録したものと同じユーザ名，パスワードを登録しておく．

(2)クライアントは，サーバに接続要求をだす．

(3)ファイアウォールは，上記の要求を保留し，認証サーバにユーザ名とパスワードを要求する．

(4)認証サーバはクライアント上の指紋取得デーモンに指紋取得要求を出す．

(5)指紋取得デーモンはユーザにセンサに指を置くように要求する．ユーザはセンサに指を置く．

(6)指紋取得デーモンは，ユーザ名と指紋情報を認証サーバに送信する．指紋情報は毎回異なる鍵で暗号化する．

(7)認証サーバは登録されている指紋情報と照合する．OKの場合，対応するユーザ名，パスワードをファイアウォールに送信する．

(8)ファイアウォールは自身が持っているユーザ名パスワードで認証する．結果OKになり，保留していたクライアント端末からの要求をサーバに通す．

図1にシステムの構成を示す．認証サーバを DMZ 上に配置することにより，攻撃者にさらすことがない．直接，クライアントがサーバにアクセスできない．また，ファイアウォールはユーザ名・パスワードの受け入れ先を DMZ に限定することができる．

上記システムを試作しその方式の有効性を確認した．

5　まとめ

ゲートウェイ上で，指紋認証を用いて，アクセス制御を行う方法について考察，試作した．本稿のアクセス制御方式を用いれば，ファイアウォールが備えている機能を外部の認証サーバで設定した情報に基づきユーザ個々のアクセス制御を制御するため，ファイアウォールの運用と認証サーバの運用とを独立に行うことができる．より高いセキュリティが要求されるサーバに対してのアクセス制御は認証サーバに任せるなどして，セキュリティに対する要求レベルが異なるサーバ群を一台のファイアウォールで守ることができる．

今回は指紋認証を考えたが，本方式は他の手段(声紋・虹彩・その他新たな認証方法)でも適用可能である．

参考文献

[1]内田薫，服部浩明，“バイオメトリクスによるユーザ認証”，NEC 技報 Vol.51，pp.161-165，1998.

[2]Rigney, et. al.，“Remote Authentication Dial In User Service (RADIUS)”，RFC2138，1997.

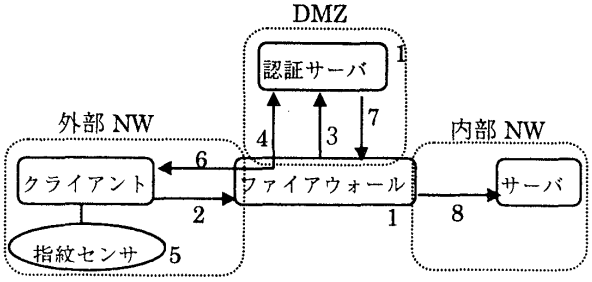

図１．システム構成