出所不明パケットの流出を防止するセキュアなネットワークの研究開発(2)

5H−07 山岸 晴彦†, 加藤 岳久††, 池田 竜朗††, 大岸 伸之†††, 藤澤 要†††, 藤平 俊行†††, 才所 敏明††

†東芝ITソリューション(株), ††(株)東芝 SI技術開発センター, †††東芝情報システム(株)

1 はじめに

電子政府の情報セキュリティ対策において，DoS(Denial of Service：サービス不能攻撃)や，DDoS(Distributed DoS：分散型DoS)，踏み台攻撃に対する対応が必要である．

攻撃の対策として，電子政府ネットワーク内に不正なパケットを流通させない方法が考えられる．その一つとして，ノード間でセキュリティポリシーを交換し，そのポリシーに従った認証を行うセキュアネットワークを提案した[1]．

本稿では，提案したセキュアネットワークにおける認証プロトコルの詳細，および有効性を確認するための検証システムについて述べる．

2 提案ネットワークの認証プロトコル

提案するセキュアネットワークにおいて，使用する認証プロトコルを検討した．本認証プロトコルでは，本人確認フレームワーク[2]が導入されていることを前提とした．

認証は，サービスを受ける利用者に対する認証と，その認証を行う機器に対する認証と，に大別される．そこで，以下の3つの認証を行うこととした．

- クライアントとゲートウェイとの認証
  (端末機器認証)
- 個人情報デバイスと利用者認証デバイスとの認証
  (デバイス間認証)
- 個人情報デバイスとゲートウェイとの認証
  (利用者認証)

以下では，各プロトコルについて述べる．なお，プロトコルにおける応答は，エンティティの電子署名である．

2.1 クライアントとゲートウェイとの認証

クライアントとゲートウェイ(GW)との認証は，図1の手順で行われる．

1) クライアント(Client)からGWへ認証要求として，クライアント証明書($Cert_{client}$)を送る．
2) GWは受信したクライアント証明書の正当性検証を行い，乱数($Rand_{GW}$)を生成してGW証明書($Cert_{GW}$)と共に送信する．
3) クライアントはGW証明書の正当性検証を行い，クライアント応答($Response_{client}$)を生成する．そして，乱数($Rand_{client}$)を生成し，クライアント応答と共にGWへ送信する．
4) GWはクライアント応答の検証を行い，GW応答を生成し送信する．クライアントは，GW応答を検証する．

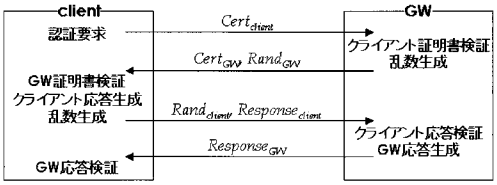

図1. クライアントとGWとの認証プロトコル

2.2 個人情報デバイスと利用者認証デバイスとの認証

利用者を確認するための個人情報デバイス(ICC_{user})と本人を確認するための利用者認証デバイス(BID：Biometrics Identify Device)間の認証プロトコルを図2に示す．ここで，個人情報デバイスは，署名生成／検証可能なICカードを想定する．

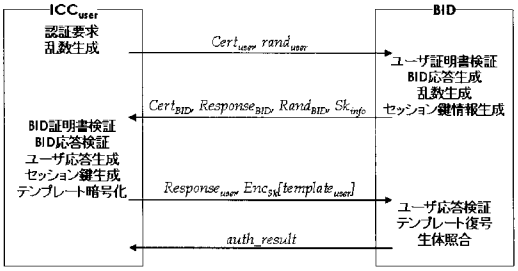

図2. 個人情報デバイスとBIDとの認証プロトコル

1) 個人情報デバイス(ICC_{user})から，ユーザ証明書($Cert_{user}$)とユーザ乱数($Rand_{user}$)とを送信する．
2) BIDはユーザ証明書を検証し，BID応答($Response_{BID}$)を生成する．さらに乱数($Rand_{BID}$)を生成し，暗号化通信を行うためのセッション鍵生成情報(Sk_{info})を生成する．そして，認証デバイス証明書($Cert_{BID}$)，BID応答，乱数，セッション鍵情報を送信

The Secure Network for Preventing the Outflow Unknown Packets (2)
Haruhiko YAMAGISHI†, Takehisa Kato††,
Tatsuro IKEDA††, Nobuyuki OHGISHI†††,
Yo FUJISAWA†††, Toshiyuki FUJIHIRA†††,
Toshiaki SAISHO††

†TOSHIBA IT-Solutions Co., 1-18-2, Issei Bld., Akebono-cho, Tachikawa-shi, JAPAN
††TOSHIBA Co., SI Technology Center, 3-22, kata-machi, Fuchu-shi, Tokyo, JAPAN
†††TOSHIBA Information Systems Co., 2-1, Nisshin-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa, JAPAN

する.

3) 個人情報デバイスは, 受信したBID証明書, BID応答を検証し, ユーザ応答($Response_{user}$)を生成する. そしてセッション鍵を生成し, バイオメトリクス認証に用いるテンプレートを暗号化する. 図2中の$Enc_k[m]$は, メッセージmを鍵kで暗号化することを示す. そして, ユーザ応答と暗号化したテンプレートを送信する.

4) BIDは, ユーザ応答の検証を行い, 暗号化されたテンプレートを復号し, 利用者のバイオメトリクス認証を実行し認証結果(auth_result)を返す.

2.3 個人情報デバイスとゲートウェイとの認証

利用者を確認するための個人情報デバイスとGWとの認証プロトコルを図3に示す.

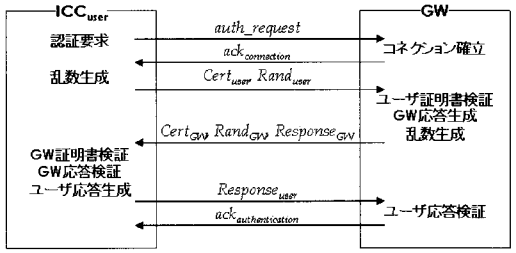

図3. 個人情報デバイスとGWとの認証プロトコル

1) 個人情報デバイス(ICC_{user})からGWへコネクション要求を出す. GWはコネクション要求を受け取ると, コネクションを確立し応答を返す.

2) 個人情報デバイスは, GWとのコネクションが確立したことを確認し, 乱数($Rand_{user}$)を生成してユーザ証明書($Cert_{user}$)と共に送信する.

3) GWはユーザ証明書の正当性検証を行い, GW応答($Response_{GW}$)を生成する. また, 乱数($Rand_{GW}$)を生成し, GW応答, GW証明書($Cert_{GW}$)と共に送信する.

4) 個人情報デバイスは, GW証明書の正当性検証を行い, GW応答の検証を行う. ユーザ応答($Response_{user}$)を生成し返す.

5) GWはユーザ応答の検証を行い, 認証が完了したことを個人情報デバイスに通知する.

3 システム構成

図4に, 検証システムの全体構成図を示す. 利用者ICカードは認証プロトコルにおける個人情報デバイス(ICCuser), クライアントICカードはクライアント(Client), 指紋照合装置は利用者認証デバイス(BID)にそれぞれ対応する. 証明書発行装置は, 本システムにおいて必要となる各種証明書の発行, およびそれらをICカードに格納するための装置として開発を行った.

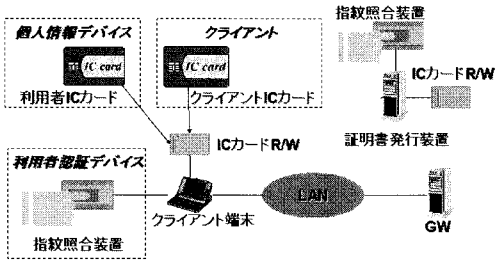

図4. システム全体構成図

図5にクライアントPC内のシステム構成を示す. 実装したエンティティは, エンティティ間の認証プロトコルを厳密に処理するため, それぞれ独立したプロセスとして実装を行った. また, プロセスとGW間の通信にはTCP/IPを, プロセス同士の通信にはOSが提供するプロセス間通信(メッセージ)を用いた.

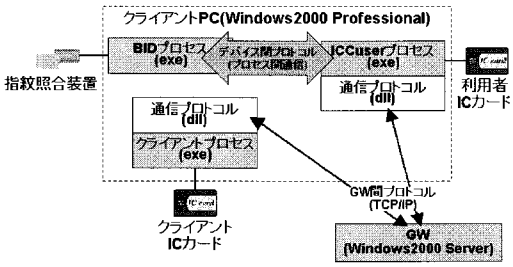

図5. クライアントPC内におけるシステム構成図

4 おわりに

電子政府ネットワークにおいて, 不正パケットを流通させないためのネットワークにおける認証プロトコルについて提案した.

今後は, 認証結果をパケットへのせ, 電子政府ネットワーク側のGWへ伝えるための手段, およびGWへの乗っ取りに対する対策を検討する必要がある.

謝辞

本発表は, 通信・放送機構が実施する平成13年度 高度通信・放送研究に係る委託研究「出所不明のパケット流出を許さないセキュアな情報通信ネットワークの研究開発」の委託を受け, 当社が研究開発しているシステムに関するものである. 関係者各位のご支援に感謝する.

参考文献

[1] 加藤, 山岸, 他; “出所不明パケットの流出を防止するセキュアなネットワークの研究開発(1)”, 第64回情報処理全国大会論文集

[2] 池田, 大岸, 他; “本人確認保証フレームワーク(BRAIN)の研究”, CSS2001論文集, p.121-126