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)

5H－06

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

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

1 はじめに

情報セキュリティ対策推進会議において，電子政府の情報セキュリティ確保のためのアクションプランが発表された．アクションプランでは，電子政府の情報セキュリティ確保を前倒しして実施し，総合的な安全性，信頼性の確保を行っていくとしている[1]．

情報セキュリティ確保において，昨今問題となっている 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策が必要である．

この様な攻撃への対策として，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ことで，攻撃を回避する方法が考えられる．そのためのネットワークと，認証方法について検討する．

2 電子政府ネットワーク

中央省庁ネットワークである霞ヶ関 WAN は，霞ヶ関 WAN 運用センターが設置され，各機関 LAN を専用回線で接続した網である．自治体ネットワークである LGWAN は，総合行政ネットワーク運用センターが設置され，各機関の広域 WAN を閉域 IP 網により接続したものである．

本研究で想定するネットワークを図 1 に示す．図 1 のごとく，霞ヶ関 WAN と LGWAN とが，ゲートウェイ(GW_G)で接続されているものとする．

オープンなネットワークである Internet も，霞ヶ関 WAN や LGWAN と GW により接続されているものとする．従って，Internet 網にも同様のゲートウェイ(GW_C)を設置し，Internet と政府ネットワークとが結ばれているものとする．

この霞ヶ関 WAN や LGWAN の様なクローズドネットワークと，Internet の様なオープンネットワークとを接続する場合，DoS，DDoS および踏み台攻撃への対策，並びにネットワークの安全性，信頼性を確保するには，政府ネットワークの部分に，不正なパケットが流通しない様な仕組みが必要となる．

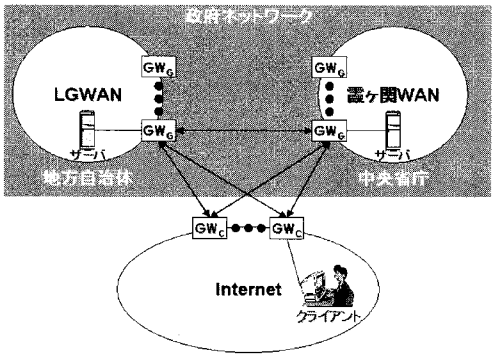

図 1. 想定するネットワーク

従来，VPN(Virtual Private Network)を用いて各ノードを結び，不正なパケットを排除することで，ノード内ネットワークを安全に保つことが図られてきた．

VPN を用いて電子政府に向けたセキュアなネットワークを構築する場合，様々なサービスに応じてセキュリティの設定を変える必要があるため運用が複雑となり，それがホールとなる可能性がある．

3 ポリシー交換を導入したセキュアなネットワーク[2]

クライアントは Internet 網に GW_C を通して接続されているとし，サーバは LGWAN 内もしくは霞ヶ関 WAN 内に設置され，GW_G を通して行政サービスを行うものとする．

この様な GW 間でのセキュリティ情報の交換として，暗号アルゴリズムや鍵の交換が行われることが多い．

例えば IPSec では，まず通信相手との間で SA(Security Association)と呼ぶコネクションを確立する．これは，IPSec では暗号アルゴリズムや認証アルゴリズムを規定していないため，通信間で使用するアルゴリズムなどの情報を保持するために用いられる[3]．

SA は，通信トラフィック毎に確立される．トラフィック情報，暗号アルゴリズム，認証アルゴリズムなど，セキュリティ情報からなるものである．このため，IPSec 通信を行うゲートウェイ(以下，GW)は，SA を確立した後に，SA 情報に基づき IPSec による通信処理を行う．

SA を構成するパラメータとして，

The Secure Network for Preventing the Outflow Unknown Packets (1)

Takehisa KATO†, Haruhiko YAMAGISHI††,
Tatsuro IKEDA†, Nobuyuki OHGISHI†††,
Yo FUJISAWA†††, Toshiyuki FUJIHIRA†††,
Toshiaki SAISHO†

†TOSHIBA Co., SI Technology Center, 3-22, kata-machi, Fuchu-shi, Tokyo, JAPAN

††TOSHIBA IT-Solutions Co., 1-18-2, Issei Bld., Akebono-cho, Tachikawa-shi, JAPAN

†††TOSHIBA Information Systems Co., 2-1, Nisshin-cho, Kawasaki-ku, Kawasaki-shi, Kanagawa, JAPAN

- 通信を行う2点間の識別子
- セキュリティプロトコルの種類
- 暗号アルゴリズム，および暗号鍵

などがある．

この様に，GW 間で交換されるセキュリティ情報は暗号アルゴリズムなどで，利用者認証に関わる情報は含まれない．このため，送信元 GW から送信されるパケットが，どの様な機器で，どの様な認証が行われたか，に関する情報がない．

そこで，GW 間で交換する情報として，各サービスに対する暗号化に関する情報に加え，認証に関する情報を提示することとする．こうすることで，送信元 GW から出力されるパケットに利用者認証に関する情報を加えられ，パケットの信頼性を高められる．

GW 間で交換される情報として，

- サービス
- 使用可能な暗号アルゴリズムの種類
- 使用するセキュア通信プロトコル
- サービスが使用可能な認証方式
- サービスを許可する認証デバイス種別

など，が考えられる．

例えば，図1においてGWCが設置された場合，もしくはGWCからの接続要求があった場合に，サービスを提供するGWGからポリシー情報が提示され，GWCは応答として使用可能な暗号アルゴリズムや使用する認証方式や認証デバイス情報を返す．

これにより，サービス提供側である GWG では，GWC から送信されるパケットについて，サービスを提供するために必要な認証が行われていることが保証される．逆に，保証が確認できないパケットについては，GWG の内部に流入することはない．

また GWC は GWG から提示されたポリシー条件に合わない暗号化や認証が行われていないパケットを出力しないため，政府ネットワークに不正なパケットが流入することを防止することが可能となる．

4　本人確認保証フレームワーク[4]の導入

GW間でアクセスに関する条件(ポリシー)を交換することにより，その条件に合わないパケットは送出しない，もしくは受信しないネットワークの認証について考える．

クライアントからのパケットが不正なものではないことを確認するために，本人確認保証フレームワークの適用を検討した．

本人確認保証フレームワークは，ネットワーク上で本人と認証するために，個人に固有な情報を用いたバイオメトリクス認証を用いる．そして，複数のバイオメトリクス装置を用いることを想定し，本人確認を行った環境などを共通的に評価，および保証して利用する基盤である．

本人確認保証フレームワークを導入するにあたり，下記設定を前提とした認証プロトコルを設計した[5]．

- 利用者認証にはバイオメトリクスを用い，かつ，その認証に用いた環境を相互に確認しパケットを送出する．
- クライアントと GWC，個人情報デバイスと GW，および個人情報デバイスと利用者認証デバイスとの間で，それぞれ ISO/IEC 9798 Entity Authentication(JIS X 5056)をベースとした認証を行う．また，サーバとGWGとの間でも，ISO/IEC 9798 Entity Authentication(JIS X 5056)をベースとした機器認証を行う．
- クライアントや利用者認証デバイス，個人情報デバイスは Public CA(Certification Authority)，例えば，LGWAN における各都道府県に設置されている NOC CA(Network Operation Center CA)が発行した公開鍵証明書が組み込まれているものとする．
- クライアント，GW，利用者認証デバイス，個人情報デバイスは，電子署名の生成／検証が可能であり，かつ署名鍵などの秘密情報は耐タンパーメモリに格納されており，外部に漏洩することはない．

5　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と認証方法について提案した．

提案するネットワーク，および認証は，DoS，DDoS，踏み台といった攻撃を防止する有効な手段と考えられる．

今後は，電子政府サービスへの適用を検討する．

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] “電子政府の情報セキュリティ確保のためのアクションプラン”，情報セキュリティ対策推進会議，2001/10

[2] 池田，加藤，他；“パケットの信頼性を高める認証プロトコル”，SCIS2002 予稿集，2002/1

[3] "Security Architecture for the Internet Protocol", http://www.ietf.org/rfc/rfc2401.txt

[4] 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

[5] 山岸，加藤，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(2)”，第 64 回情報処理全国大会論文集