出所不明のパケット流通を防止するセキュアな情報通信ネットワーク

Secure Network Preventing Distribution of Unknown Packets

加藤　岳久　　**清水　歩**

■KATO Takehisa　■SHIMIZU Ayumu

インターネットを利用したシステムやサービスの増加とともに，ハッカーやクラッカーによるサーバへの攻撃が増加している。特に，サービスを妨害する攻撃は，サービス提供者にとって深刻な問題となっている。この研究では，防御が困難なサービス妨害攻撃であるDoS（Denial of Service）攻撃，DDoS（Distributed DoS）攻撃，更には踏み台といった攻撃からネットワークを守り，安定したサービス提供を図るシステムの構築を目的とする。具体的には，守るべきネットワークは，事前に利用者環境（外部）のネットワークからのアクセスに関するセキュリティポリシーを，外部ネットワークに提示する。そして，そのセキュリティポリシーに従った利用者の認証や機器の認証を行い，ポリシーに適合しないパケットを外部ネットワークから受け取らないことで，守るべきネットワークの安全性を確保する。

Attacks on servers by crackers have recently become more frequent with the growth in systems and services using the Internet. In particular, denial of service attacks pose a serious problem for a service provider.

Toshiba has proposed and developed a system that provides highly available services based on preventing denial of service attacks, distributed denial of service attacks, and connection laundering. Specifically, the network to be protected notifies the security policy to the network of the user environment. User and device authentication then follow in accordance with the security policy. Consequently, the network to be protected is secured by not receiving packets that do not conform with the security policy notified to external networks.

1　まえがき

インターネットの急速な広がりと相まって，オープンな通信ネットワークを介して重要なデータをやり取りする，EDI（Electronic Data Interchange），申請，調達といったシステムの利用者が増加している。

一方，ハッカーやクラッカーらによるホームページ改ざんや，個人情報の漏えい，コンピュータウィルス，SPAMメール（受信者の意図に関係なく届く広告などの電子メール），DDoS攻撃などが問題となっている。

政府は，“e-Japan戦略[1]”，“e-Japan重点計画[2]”を打ち出し，“e-Japan2002プログラム[3]”により，重点的かつ戦略的にIT（情報技術）施策をいっそう積極的に実施していくこととし，世界最先端のIT国家実現を目指している。

整備が進められている電子政府ネットワークは，霞ヶ関WAN（Wide Area Network）やLGWAN（Local Government WAN）という閉域ネットワークにより構成されている。電子政府は，サービスを国民や企業へ提供するために，オープンネットワークであるインターネットと接続することを想定している[4]。ここで，電子政府ネットワークとインターネットとの接続点におけるセキュリティ確保が，ネットワークセキュリティ上の重要な課題となる。

セキュリティ上脆弱（ぜいじゃく）な接続点があると，そこから電子政府や電子自治体内部への侵入やサービスの妨害を受ける可能性がある。

2　ポリシーベースによるアクセス制御

東芝は，接続点のセキュリティを，ネットワーク利用者である各自治体が個別に運用・管理しないスキームを検討した。

図1に示すように，電子政府ネットワークとインターネットとの間に中間ネットワークを設置し，中間ネットワーク内で電子政府サービスを受けるためのポリシーを共有し管理することで，各自治体におけるセキュリティレベルを統一する。このスキームでは，インターネットから中間ネットワークへ接続する際に，電子政府ネットワークに流通してよいパケットかをポリシーに基づいて判定することで，電子政府ネットワーク内に不正なパケットが流通せず，電子政府サービスを安全に保つことができる[5],[6]。

図1のとおり，提案する方式は中間ネットワークをゲートウェイ（以下，GWと略記）で構成し，あらかじめ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

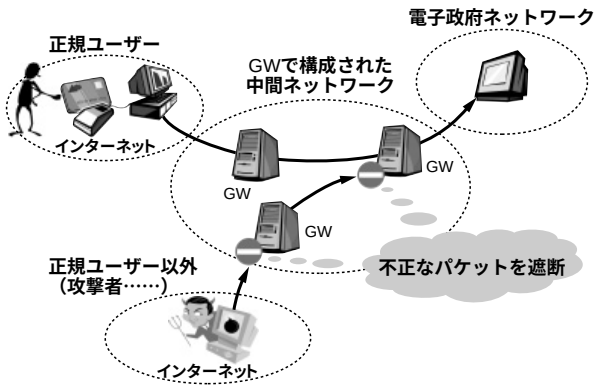

図1. 中間ネットワークを導入したセキュアなネットワーク ― 中間ネットワークの導入により，パケットの真正性を確保し，出所不明なパケットの流通を防止する。

Secure network utilizing intermediate gateway network

GW間で交換する。すなわち，GW間でやり取り可能なパケットに関するポリシーを交換することで，そのポリシーに適合したパケットのみを中間ネットワーク（以下，PAG（Policy-based Authentication Gateway）.net と呼ぶ）の入口で検査し通過させる。この結果，電子政府ネットワークは正しいパケットのみを受け入れることができる。これにより，外部から電子政府ネットワークへ流通するパケットの信頼性を高めることができる。

GW間で交換される情報として，次が考えられる。

⑴　サービス内容
⑵　使用可能な暗号アルゴリズムの種類
⑶　使用するセキュア通信プロトコル
⑷　サービスが使用可能な認証方式
⑸　サービスを許可する認証デバイス種別

ポリシーは，XML（eXtensible Markup Language）により記述され，ポリシーの生成者によるXML署名により正当性が保証される。GW間で交換されるポリシーの例を**図2**に示す。

PAG.netでは，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[7]を適用した。

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，個人に固有な生体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，本人確認を行う環境について共通的に評価を実施し，環境が正しいことを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，次の3点を前提とした。

⑴　利用者の識別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GWで確認しパケットを送出する。

```
<?xml version="1.0" encoding="Shift_JIS"?>
<node>
  <サービス service="戸籍請求" comment="">
    <アドレス item="URL" value="157.49.1.1" comment=""/>
    <ポート番号 item="PortNo" value="70" comment=""/>
    <ターゲット item="利用者認証" comment="">
      <セキュリティレベル item="セキュリティレベル" value="高" comment="セキュリティレベル">
        <property item="高" value="指紋" comment="高レベルの設定"/>
          <property item="指紋" value="光学式" comment=""/>
      </セキュリティレベル>
    </ターゲット>
    <ターゲット item="通信方法" comment="">
      <セキュリティレベル item="セキュリティレベル" value="中" comment="">
        <property item="中" value="限定なし" comment="中"/>
      </セキュリティレベル>
    </ターゲット>
    <ターゲット item="機器認証" comment="">
      <セキュリティレベル SecurityLevel="セキュリティレベル" value="低" comment="">
        <property item="低" value="しない" comment=""/>
      </セキュリティレベル>
    </ターゲット>
  </サービス>
</node>
```

図2. セキュリティ ポリシー情報の例 ― 電子政府ネットワークで提供されるサービスへのアクセスやデータのやり取りに必要なポリシーが記述される。

Example of security policy data

⑵　クライアント，利用者認証デバイス，個人情報デバイスには，Public CA（Certification Authority）が発行した公開鍵証明書を組み込む。
⑶　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，電子署名の生成や検証が可能であり，かつ署名鍵などの秘密情報は耐タンパメモリに格納されており，外部に漏えいすることはない。

3　PAG.netを用いた試作システム

PAG.netの動作や安全性を評価するため，最小構成の試作システムを構築した。試作したシステムの全体構成を**図3**に示す。

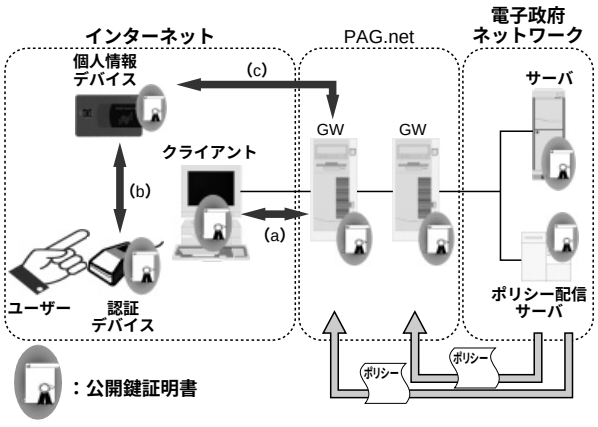

図3. 試作システムの全体構成 ― 電子政府ネットワークのサービスごとに設定されるポリシーをPAG.net内のGWに配信する。配信されたポリシーに基づいて，利用者の環境や利用者の正当性を検証する。

Configuration of prototype system

PAG.netでは，サービス提供側からサービスを受けるために必要なセキュリティに関するポリシーデータをPAG.net内GWへ配信する。

PAG.net内のいずれかのGWは，利用者からサービスの要求を受け取ると，利用者の環境から出力されるパケットの出所を明らかにするため，ポリシーデータに基づき利用者側の認証を行う。

このように，PAG.netでは以下の二つの大きな特長がある。

⑴　ポリシーデータの配信　　ポリシー配信サーバは，サービスごとに図2のポリシーデータを作成し，PAG.net内GWに配信する。ポリシーが変更された場合は，そのデータを配信し上書きする。

⑵　利用者側の認証　　利用者側は，三つの認証を行う。

ⓐ　クライアント端末とGWとの間で，相互に正当性を検証する。

ⓑ　個人情報デバイスと認証デバイスとの間で，相互に正当性を検証する。

ⓒ　個人情報デバイスとGWとの間で，相互に正当性を検証する。

上記の認証，及びサーバとGWとの間は，共に国際標準ISO/IEC9798認証（Entity Authentication（JIS X 5056））をベースとした認証を行う（ISO：国際標準化機構，IEC：国際電気標準会議）。

これらの準備が完了し，クライアント端末から出力されるパケットが，ポリシーに記述された条件を満足していることをGWで確認できると，利用者はサービスを受けることができる。

試作システムでは，PAG.net内のセキュア通信プロトコルとして，IPsec（IP security protocol）[8]を採用した。これによるメリットは次の2点である。

⑴　サービス側が上位層で，どのようなセキュア通信プロトコルであっても，PAG.net内のセキュア通信が影響を受けることがない。

⑵　サービス側のアプリケーションに依存することがない。

4　ポリシー配信方法に関する検討

PAG.netでは，サービスを提供するポリシーデータを共有し管理することで，様々なサービスに対するセキュリティレベルを統一することができる。ここで，PAG.net内へポリシーデータを，効率良く配信することが重要となる。

そこで，PAG.net内へのセキュリティポリシーデータを配信する方法として，以下の四つの方式について検討を実施した。

各方式の構成を**図4**に示す。

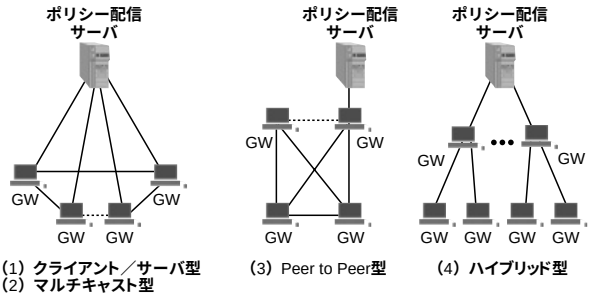

図4．ポリシー配信方式― 4種類の方式について検証した。
Policy distribution methods

⑴　クライアント／サーバ型ポリシー配信　　GWの1台1台がポリシー配信サーバに対して，ポリシーデータを要求し，ポリシーデータを受信する。

⑵　マルチキャスト型ポリシー配信　　ポリシー配信サーバから，PAG.net内の全GWにポリシーデータを配信する。

⑶　Peer to Peer型ポリシー配信　　ポリシー配信サーバから1台のGWに配信すると，自律的にGWがポリシーデータを配信する。

⑷　ハイブリッド型ポリシー配信　　Peer to Peer型とマルチキャスト型を合わせた方式で，特定のGWにはマルチキャストで，以降はPeer to Peer型で配信する。

Peer to Peer型ポリシー配信を行う場合に，ポリシーデータの配信効率がどの程度であるか，シミュレーションした結果を**図5**に示す。図5は，一つの新しいデータを，任意の一つのPeerに渡したとき，データ交換回数を横軸に，Peerの何%が新しいデータを保有できるかを縦軸に計算したものである。

図5から，クライアント（PAG.net内のGW）が1,000万台で

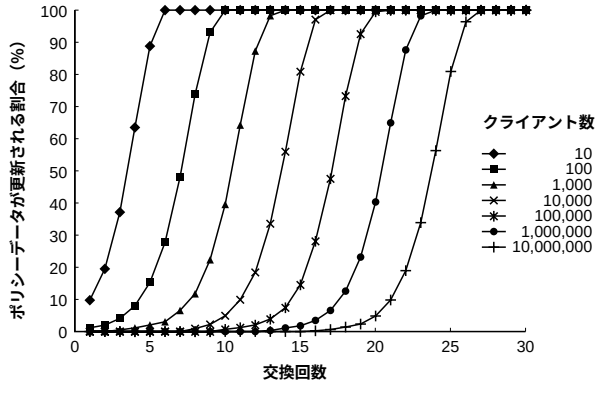

図5．Peer to Peer型データ配信の効率― Peer to Peer型配信の場合，ポリシーデータの配信効率についてシミュレーションした。
Efficiency of peer-to-peer type policy data distribution

あっても，25回の交換で96％以上，30回で100％の配信効率が得られることがわかった。

PAG.net内のGWが1万台である場合に，5分につき1回ポリシーデータを交換したと仮定しても，およそ75分ですべてのGWに新たなポリシーデータが行き渡る。

表1は，ポリシーデータの配信に必要な項目について，四つの方式を比較検討した結果である。表中の ○，△，× は，3段階評価で各方式の相対評価を行った。

表1．ポリシー配信方式の比較結果
Results of comparison of policy distribution methods

方　式	スピード	負荷分散	可用性	確実性	仕組み	運用性
クライアント／サーバ型	×	×	×	○	単純	○
マルチキャスト型	○	○	△	×	普通	×
Peer to Peer型	△	○	○	○	普通	△
ハイブリッド型	○	△	×	△	複雑	△

○←優－△－劣→×

この検討では，ポリシーデータ配信のみについて検証したものであり，ポリシーデータの真正性検証，GW間の認証は含んでいない。

ポリシーデータの配信だけに着目すると，PAG.net内のGW数が少なければ，クライアント／サーバ型ポリシー配信が良い。GW数が増加して数万台規模になれば，Peer to Peer型ポリシー配信が良い。

しかし，ポリシーデータの真正性検証やGW間の認証といったオーバヘッドを考慮すると，単純にGW数だけで配信方式を決定することはできない。

今後は，PAG.net内のGW数とポリシー配信の頻度なども考慮し，検討した方式を適応的に組み合わせた効率の良い配信方式を検討していく。

5　あとがき

守るべきネットワークへの攻撃を防止するため，出所が不明なパケットを流通させないことで，ネットワークを防御する構成と認証方法について提案した。

提案方式は，互いのネットワークへアクセスするためのセキュリティポリシーを交換し，相手のネットワークからパケットが出力される時点で，受け入れられるか判断する。このため，自ネットワークへは出所が明らかなパケットのみが到達するため，不特定多数からのアクセスによるDoS攻撃，DDoS攻撃，踏み台攻撃といった，防御が困難な攻撃を防止するのに有効と考えられる。

この方式は，電子政府ネットワークの保護を目的に研究・開発を進めている。しかし，電子政府ネットワークだけでなく，例えば企業間電子商取引，特定ユーザー向けの企業サービス（コンテンツ流通など）への展開も視野に入れた検討を行い，実験システムを構築して動作検証や安全性の評価も進めていく。

謝　辞

この論文は，通信・放送機構が実施する2001年度及び2002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。

文　献

⑴ IT戦略本部．e-Japan戦略．＜http://www.kantei.go.jp/jp/it/network/dai1/pdfs/s5_2.pdf＞，（参照2003-4-2）．
⑵ IT戦略本部．e-Japan重点計画．＜http://www.kantei.go.jp/jp/it/network/dai3/3siryou40.html＞，（参照2003-4-2）．
⑶ IT戦略本部．e-Japan2002プログラム．＜http://www.kantei.go.jp/jp/it/network/dai5/5siryou2.html＞，（参照2003-4-2）．
⑷ 自治大臣官房情報政策室．総合行政ネットワーク構築に関する調査研究最終報告書，2001-3．＜http://www.soumu.go.jp/kokusai/pdf/report.pdf＞，（参照2003-4-2）．
⑸ 池田竜朗，ほか．“ パケットの信頼性を高める認証プロトコル ”．SCIS2002予稿集，2002-01，電子情報通信学会情報セキュリティ研究専門委員会，p.543－547.
⑹ 加藤岳久，ほか．“ 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），（2） ”．第64回情報処理学会全国大会講演論文集（3），2002-3-12，p.415－418.
⑺ 池田竜朗，ほか．“ 本人確認保証フレームワーク（BRAIN）の研究 ”．CSS2001論文集，情報処理学会．p.121－126.
⑻ S. Kent ; R. Atkinson. "Security Architecture for the Internet Protocol". ＜http://www.ietf.org/rfc/rfc2401.txt＞，（参照2003-5-30）．

加藤　岳久　KATO Takehisa
e-ソリューション社 SI技術開発センター SI技術担当主務。課金決済，プライバシー保護，ネットワークセキュリティの研究・開発に従事。電子情報通信学会，情報処理学会会員。
Systems Integration Technology Center

清水　　歩　SHIMIZU Ayumu, D.Eng.
e-ソリューション社 SI技術開発センター SI技術担当，工博。ネットワークの研究・開発に従事。日本地熱学会会員。
Systems Integration Technology Center