情報セキュリティのための IP ネットワーク利用制御

Control of Using IP Networks for Information Security

佐藤　直†　　岡田 康義†
Naoshi Sato　　Yasuyoshi Okada

1. まえがき

IP ネットワークのセキュリティ維持を目的に，IP ネットワークのセキュリティ評価基準，あるいはセキュリティ証明書やネット免許に関する議論が高まっている[1]-[4]．これらの規則や制度が導入されると，これまでのような自由なネット利用ができなくなると想像されることから反対する声も大きいが，機密情報漏洩や詐欺事件が後を絶たない現状を考慮すると，セキュリティの点からネットワーク利用に一定の制限を加え健全化することが喫緊の課題であると考えられる．本稿では上記認識のもとに，セキュアな IP ネットワークを取り戻すためのシステム構築方針を提言し，さらに同ネットワークシステムにおける利用制御技術について課題を考察する．

2. セキュアな IP ネットワーク

周知のように，インターネットは電話網のようにネットワーク全体を統合的に管理・制御する機構を持たないのが特徴である．この特徴はネットワークとしての拡張性と利用の自由度を飛躍的に高めたが，他方で悪意ある利用も促進する結果となった．悪意ある利用の結果の代表例として，迷惑メールトラヒックのネットワーク寡占が取り沙汰されることが多い．迷惑メール対策の一つとして，利用者（送信元）認証を行う OP25B(Outbound Port 25 Blocking)が推奨されており，迷惑メール削減に大きな効果があることが知られている[5]．この事例は，セキュアな IP ネットワークの有り様として，ネットワークの入り口で利用者を認証すべきことを示している．筆者らはさらに利用者自身や利用端末のセキュリティをチェック（検証）して利用を制御する IP ネットワークシステムを提案した[6],[7]．同システムの構成イメージを図 1 に示す．図 1 は通信事業者が構築する管理された公衆用ネットワークシステムであると仮定する．同システムは，利用者情報を伝達する転送系とセキュリティの点から通信接続やパケット転送を管理・制御する系の 2 層構造を成している．また，同図では，利用者（クライアント）がサーバにアクセスし情報提供サービスを受ける例を示している．

この例において，IP ネットワークは利用者のセキュリティに関する証明書を発行・管理する機能を有する．さらに，呼制御機能や転送制御機能は，従来の機能の他に，上記のような証明書類を基に利用者の IP ネットワーク利用資格をゲートウェイで検証し，通信接続やパケット転送を制御する．

3. 利用制御の要点と課題

セキュア IP ネットワークシステムによる利用制御の要点と課題を考察する．すなわち，セキュリティ証明，およびセキュリティ維持のための呼制御・転送制御を検討する．なお，利用者端末やネットワーク等は相互認証され，やりとりされる情報も全て暗号化されることを前提とする．以後，この暗号化・認証機能に関する記述を省略する．

3.1 セキュリティの証明

(1)検疫機能

ネットワークセキュリティは多様であるため，普遍的な評価方法を定め，セキュリティを確保することは難しい．しかし，近年，LAN 接続を対象に PC のセキュリティ対策ソフト更新状況を調べる検疫技術の進歩が著しい[8]．この検疫機能を公衆用ネットワークのオプションサービスと位置づけ，後述するセキュリティ証明書に検疫結果

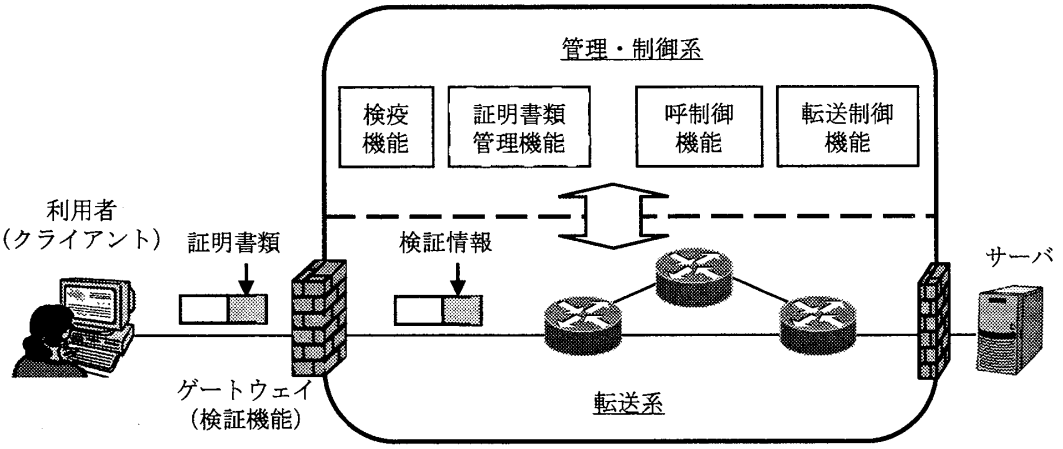

図 1　セキュアIPネットワークシステムの構成イメージ

† 情報セキュリティ大学院大学

（例．最新パッチがあたっている／いない），または最後の更新日付を IP ネットワーク側の署名付きで記載する．

(2)証明書類管理機能

交通運輸制度あるいは健康医療制度からの類推として種々のセキュリティ証明書を適用する．交通運輸制度からは，自動車免許や海外渡航ビザに相当する，ネット免許やアクセス査証（通行証）を定めて利用条件を証明する．また，健康医療制度からは，診療録や健康診断報告書に相当するセキュリティカルテを定めて，必要に応じて閲覧できるようにする．これらの証明書類は階層構造を有するデータベースに保存され，台帳サービスとして提供することが想定される．証明書類のコード化体系や保存ルールを確立する必要がある．

なお，現状，検疫は，端末の健全性のチェックが主であり，端末を操作する利用者自身（人間）の攻撃性（悪意性）はチェックされない．レピュテーションシステム[9]など，利用者の攻撃性を測定評価し管理する仕組みの導入も今後の課題となる．また，証明書の内容はセンシティブであるため，利用者の開示制御権や犯罪捜査時の閲覧権も事前にルール化しておく必要がある．

3.2 呼制御と転送制御

(1)呼制御機能

図１で，IP ネットワークやあて先端末（サーバ）のセキュリティポリシー（アクセス許可方針）は呼制御機能により上述のデータベースに予め登録されるものとする．利用者は接続要求時，セキュリティ証明書を含む IP パケットを利用者側ゲートウェイに提示し，上記のセキュリティポリシーに適合するか否かの検証を受ける．同ゲートウェイが接続可と判断した場合，IP パケットに検証情報を付してネットワーク内に転送する．この検証情報はネットワーク内に保存するとともに利用者にも通知する．この利用者とネットワークのやりとりも検討課題となる．

なお，セキュリティポリシーは私的あるいは公共的な観点から設定する．現状，セキュリティポリシーは企業や個人が個々に設定しているが，インフラとしてのセキュリティを維持するには，社会的コンセンサスの基に，最低限守るべき事項を規定して，セキュリティの証明や各種制御に反映する必要がある．

(2)転送制御機能

ネット免許のような資格を設定した場合，利用制御として，図１のゲートウェイで，資格不適合パケットを全て廃棄するのが一般的であろう．しかし，このような一律的な措置は著しく利便性を損なう恐れがある．そこで他の利用制御として，資格不適合であっても利用を許可するが，ネットワーク内でパケット転送を差別化する方法を提案する．すなわち，経路制御，品質制御，輻輳制御等，パケット転送に関わる制御において，上述の検証情報を基に差別化を行う．通常，経路制御では，ルータのホップ数等を尺度として，最短経路を選択するが，セキュリティが確保されていない場合，最短経路に比べより長い経路を設定する．品質制御では，セキュリティレベルを加味して帯域の確保や転送の優先順位を決定する．輻輳制御では，セキュリティレベルが低い程，より早期に，またはより厳しく送信を抑制する．

なお，主情報のみならず，監視・管理プロトコルの利用（例．ping）においても，検証情報により差別化すれば不正アクセスの減少が期待できる．

4．考察

(1)実現性：本提案は自律分散を基調としたネットワークではなく，十分な管理・制御能力を持つネットワーク（例．NGN）で実現可能であろう．

(2)効果：セキュリティ証明書類や検証情報はセキュリティ上の問題が起きないことを保証するものではない（例．ゼロディ攻撃には対処できない）．しかし，セキュリティ被害の多くは既知のセキュリティ対策の未実施に起因すること，およびセキュリティポリシーの統一化が図られることから，セキュリティが改善すると考えられる．

(3)コスト負担：本提案によれば，セキュリティ対策コストはネットワーク側が増し利用者側が減る．セキュリティ対策をネットワーク側で集中して行うことで，効率化され，トータルコストが削減できることを考慮して，コストの負担割合を定める必要がある．

(4)法制度：本提案は電気通信事業法が規定する「通信の秘密」や「公平性」と関わる．セキュリティ維持の観点から，これらの規定のあり方を再検討する必要がある．

5．むすび

安心して利用できる IP ネットワークを実現するためのシステム構成技術と課題を検討した．ネットワークセキュリティに関わる諸機関・諸兄の活発な検討を期待する．

最後に，討論いただいた本学研究室ゼミ生に感謝する．

文　献

[1]Draft Rec. X.805sna:Network security assessment/ guidelines based on ITU-T Recommendation X.805, Q5/17(2007.8)

[2]磯原隆将，石田千枝，北田夕子，竹森敬祐，笹瀬巌：検疫結果を保証するセキュリティ保証基盤，情処論 Vol.47, No.2, pp.434-445(2006.2)

[3]安田浩：ユビキタス社会におけるセキュリティ技術,CEATEC2005(2005.10)

[4]WIRED VISION: Desperate Botnet Battlers Call for an Internet Driver's License(2007.6)

[5]総務省報道資料：特定電子メール等による電子メールの送受信上の支障の防止に資する技術の研究開発及び電子メールに係る役務を提供する電気通信事業者によるその導入の状況(2007.11)

[6]佐藤直：検証ベース IP ネットワークの提案，2006 年信学総大 B-7-120(2006.3)

[7]佐藤直，岡田康義：情報セキュリティレベルに応じたネットワーク利用資格制度導入の提言，2007 年日本社会情報学会合同研究大会論文集，pp.160～163(2007.9)

[8]横山恵一，田中英彦：イントラネットにおける IPv6 検疫ネットワークシステムの提案，CSS2005，1A-1(2005.10)

[9]T.Sakai,K.Terada,T.Araragi: Robust Online Reputation Mechanism by Stochastic Approximation. Adaptive Agents and Multi-Agent Systems II,LNAI 3394, pp.230-244, Springer-Verlag(2005.2)