B-6-82

ユーザとその居場所に応じたアクセス制御

Location Sensitive User Access Control

宗吉　隆行　　田中　英彦
Takayuki Muneyoshi　　Hidehiko Tanaka

情報セキュリティ大学院大学
Institute of Information Security

1. 背景

企業などのイントラネットでアクセス制御を行う際には，その主要なものとして，ファイアウォール（ＦＷ）と各ユーザが持つアクセス権が挙げられる．ＦＷは，一般には建物や部屋毎に設定されたセグメント間の通信を規定するものであることが多い．またユーザのアクセス権は情報サービス毎に設定される．筆者らは主に場所の要請で設定されているアクセス制御のポリシーにユーザのアクセス権を考慮した，アクセス制御マップについて提案した[1].

本稿ではイントラネットでアクセス制御マップを適用するシステムの構成について述べる．

2. 適用

ユーザのアクセス権に場所によるアクセス制御を考慮することによって，場所に依存しないユーザ権限の行使，ユーザ権限に依存しない利用場所でのアクセス制御等を実現することができる．

例えば会議室ではユーザの権限を優先させたり，休憩スペースではユーザに寄らずパブリックなスペースとしてのアクセス権を設定することが出来る．

3. システム概要

本システムは，場所とユーザに応じた通信制御を行う認証ゲートウェイ（ＡGW），認証処理と制御マップの配信を行う Access Controller（ＡＣ），及びアクセス制御マップを持つ Access Control Manager（ＡＣＭ） からなる（図１）．場所情報には認証ゲートウェイの証明書とそれに対応するＭＡＣアドレスの情報，部屋等の場所の名前などが含まれる．

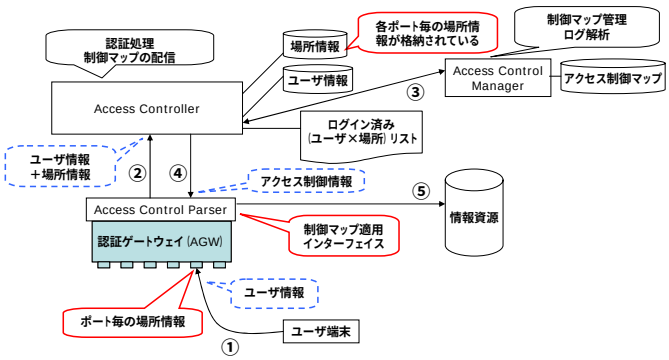

図１．システム概略図

ユーザが端末の利用を開始してから認証ゲートウェイの先にある情報資源へアクセスするまでの手順は以下の通りである．

①ユーザ情報の送出
　端末からユーザ情報を AGW に送信する
②AGW での認証
　ユーザ、場所、AGW を認証する．
　i) AGW，AC 双方の証明書を使用した SSL 通信を確立する
　ii) ユーザ情報と接続されたインターフェイスの MAC アドレスを AC に送信する
　iii) AC で認証処理を行う
　・証明書と送られた MAC アドレスの整合性をとる．
　・ログイン済み情報を参照し，ユーザが別の場所ですでにログイン済みかどうかを見る．
　・ユーザを認証する
　AGW の証明書は，機器単位で発行し，予めＡＣに登録しておく．
③AC は ACM に認証済みのユーザ，場所の情報を送り，適合するアクセス制御マップを取得する
④AGW は AC から受け取ったアクセス制御マップを特定ポート，特定 IP アドレスに適用する
⑤ユーザは AGW に適用された制御に従って情報資源へアクセスする．

場所の情報を認証ゲートウェイのＭＡＣアドレスとし，認証ゲートウェイに証明書を付けることで，ユーザからの場所のなりすましを防いでいる．複数の認証ゲートウェイにも対応する．また，無線ＬＡＮの利用については，悪意あるユーザによるなりすましを防ぎつつ場所の特定が出来れば可能であろうと考えられる．もしくは無線ＬＡＮという一つの場所としてアクセス制御を考えればよい．さらに，外部ネットワークからの接続についても同様に考えることで本システムに適用出来る．

4. まとめ

ユーザの認証時に場所の情報を認証情報に含めることで，ユーザが利用している場所に応じたアクセス制御が実現できる．現在，実装を行っており，完了次第，本方式の評価と拡張などを行う予定である．

参考文献

[1] 宗吉 隆行, 小柳 和子, 相場 信夫, “ユーザアクセス権と統合されたセグメント管理によるネットワークのユーザビリティの向上,” 信ソ大 , B-6-49, p.49, September 2005.