例外処理を考慮した情報コンセント管理方式

Management of Information Outlet System with Exception Handling

田島 浩一, 西村 浩二, 岸場 清悟, 相原 玲二
Kouichi Tashima Kouji Nishimura Seigo Kishiba Reiji Aibara
広島大学 情報メディア教育研究センター
Information Media Center Hiroshima University
〒739-8511 広島県東広島市鏡山 1-4-2
Kagamiyama 1-4-2, Higashihiroshima, Hiroshima, 739-8511 JAPAN

概要

ネットワーク利用の制限や利用の記録保存のために認証機能の付いた情報コンセントが広く利用されているが, 一般的に認証の際に利用されているブラウザや専用ソフトによる認証方法ではプリンタやブロードバンドルータ, IP 電話器などの機器は, それらによる認証に対応できない場合がある. 情報コンセントの導入時にその問題の解決としてはじめから特定ホストに対して定常的に通信を許可するように設定し利用を開始することで導入時の対応可能であるが, 後々そのような機器の追加や変更等その都度情報コンセントの管理者により設定の変更が必要となる. そこで本提案では, キャンパス内での運用に支障の出ないような方法で, これらの情報コンセント管理における例外処理を考慮するため MAC アドレスの登録による情報コンセントの管理方式を提案する.

キーワード: 情報コンセント, ユーザ認証, DHCP, アクセス制御

1 はじめに

持ち込んだ PC の一時的な利用や不特定者の利用する固定端末などからのネットワーク利用の制限や利用の記録保持のために, 認証機能の付いた情報コンセント (文献[1]〜[3]のような例) が広く利用されており, ここでは利用者が直接機器を操作しユーザ名/パスワードによる認証で利用可能となる方式が用いられている. この仕組みを利用し, 組織内 LAN の奥深くを含む全体をこのような認証付き情報コンセントの配下に置き, 組織内のセキュリティ向上を図る事が次に考えられるが, ブラウザからの入力や CGI 実行などによる認証では, プリンタやブロードバンドルータなどブラウザを持たない機器では認証が困難であり, 導入時にこれらの機器は認証不要とするような設定を行う例外的な処置が必要となる (**例外処理-1** とする). この認証不要の機能が利用できる場合に, 利用者によっては一度認証する事で一定期間は再度認証しなくても使い続けたいという要望 (**例外処理-2** とする) が考えられ, 例えば, 厳密に入退室の管理された部屋で特定の利用者のみ利用する場合において, その例外設定がセキュリティレベルを下げるとは判断できない場合も考えられる. 我々の組織でも我々の開発してきた PortGuard システム[4] やその

製品版を運用してきた際に，これらの要望や例外の設定が必要である事は経験済みであり，自組織の広い範囲に導入して運用する場合を考え，これらの例外処理の負荷を軽くして運用する一つとして MAC アドレスの登録を行い運用する方法について提案し，その構成および考察について報告する.

2 管理方式

2.1 管理方針および機能の概要

例外処理-1 の認証できない機器のネットワーク利用には，事前に情報コンセントの設定で問題なく利用できるように穴を開ける方法がよく用いられ，通常利用とは異なり利用開始と終了のログを残せない利用となる.　穴を開ける際に，安全に重きをおいて考えると情報コンセントを管理する管理者が操作し設定を管理する傾向が強く負担になるが，逆に誰でも自由に穴を開ける事はそもそも推奨される利用ではない.
ここで，穴を開けた先である認証不要とする機器にはそもそも所有者があり，その所有者が機器をネットワークに接続した状態で，この機器を指定して自分の責任で穴を開けるのであれば，十分責任の取れる穴の開け方になると考え，その機器を所有者を登録しておき穴の開け閉めはその所有者に限定して例外処理-1 の利用を可能とする方針とした.　図 1に，通常の認証を経て利用する場合に登録操作も可能とするように変更した認証ページの画面を示す.
ここでは，認証ページに，ID の入力以外に端末の MAC アドレスを登録するためのフィールドを追加しており，認証時の ID で例外処理-1 扱いの機器を以下のフォームで登録する.

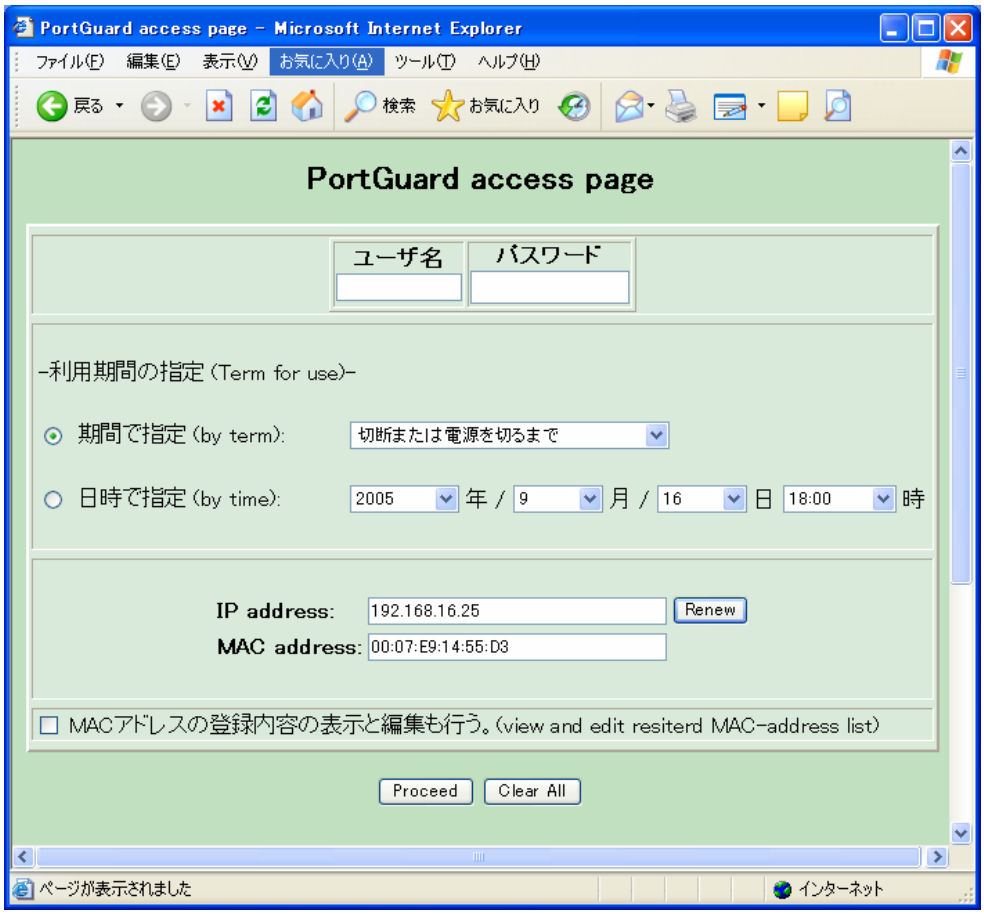

図 1 登録・認証画面

認証ページの構成は，我々の組織でのこれまでの運用方針で，通常の情報コンセント利用時には，切断または電源を切る事で利用を終了する方法を用いており，例外処理を行わない（これまでと同じ利用の）場合に，ユーザ名及びパスワードの ID を入力し送信するのみで，これまで同様に利用可能であるようにフォームのデフォルト状態を設定した．

利用期間を指定する場合には，ID 入力欄の次の欄の「利用期間の指定」を操作し指定する．この欄では，利用期間の指定を「切断または電源を切るまで」以外に，今日中，今週，今月，今年，解除指定するまで，の 6 個の選択肢と，利用終了日時を指定するインタフェースを用意した．次の欄には，期間の指定をする際に，利用者が IP/MAC アドレスを入力できるフォームを用意したが，これは，操作中の端末のアドレスの確認が可能できるようにすぐ横の [renew] ボタンによる取得とフォームを埋めて再表示する機能を用意した．

また，ブラウザを持たない機器の登録もこの画面から行い，「2．3 登録条件の指定」により更新や追加可能を確認した後に登録を受け付け，設定した機器が利用可能となる．次の欄には，登録内容の確認や編修を行いたい場合にのみチェックを入れて利用する．COOKIE 等端末を特定して認証情報を引き継ぐ方式をとらないため，登録内容の表示の認証もあわせて行うようにこの画面に用意した．編集画面では，リスト表示された登録をチェックボックスにチェックをいれて削除する機能と1 つを選択してその IP/MAC アドレスをフォームに埋めた状態で図 1の画面に戻る機能を用意した．

登録の際に，IP アドレスや MAC アドレスの欄に接続していない機器や実際の設定と異なる指定をした場合には，リクエスト送信時に実行する CGI により IP アドレスから MAC アドレスの検索及び，MAC アドレスへの到達確認（ARP の確認）を行い確認しているため，登録できない．

2．2 例外処理の実装

PortGuard システムは端末の利用者がネットワークを利用する際に主に外部の認証サーバの認証経てネットワーク利用を提供するシステムであり，図 2に示す構成で動作し，アクセスを制御するゲートウェイ動作をする**コントローラ部**とそれらを管理する **PortGuard サーバ部**より成る．利用者はコントローラ部のいずれかより PortGuard サーバにアクセスし認証に成功するとコントローラ部のアクセス制御設定を開放しネットワークが利用できるという動作である．

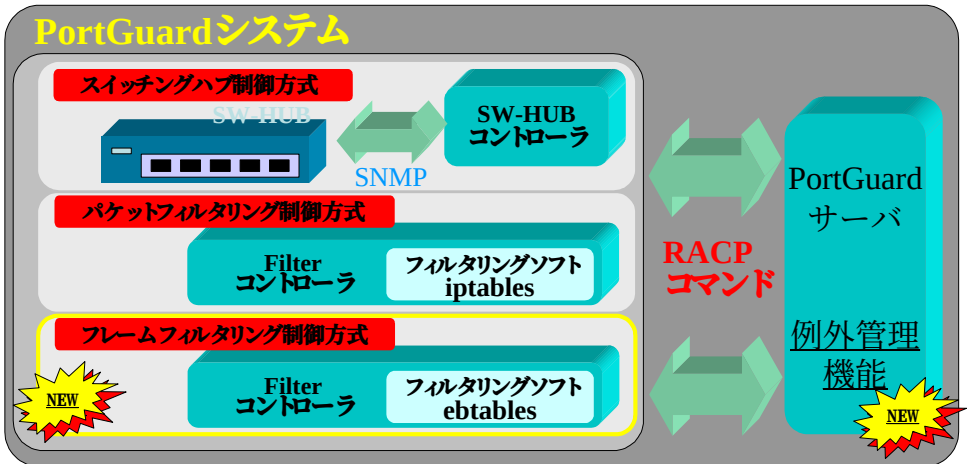

図 2 PortGuard システムの概要

本実装は, PortGuard システムに, 認証が不要とする設定および例外管理機能の追加を実装した. また, NAT やルータを超えると利用できないような Windows 共有等のブロードキャストドメイン内での利用を想定した利用形態に対応するため, イーサネットフレーム単位で Layer2 制御を行うコントローラ部を新たに追加した.

図 3にこの度の変更後の認証と利用開始までの図を示す. 認証ページの要求時に認証ページを CGI 実行後に生成するようにし, その CGI より認証の要不要を処理し, 認証不要の処理を行っている.

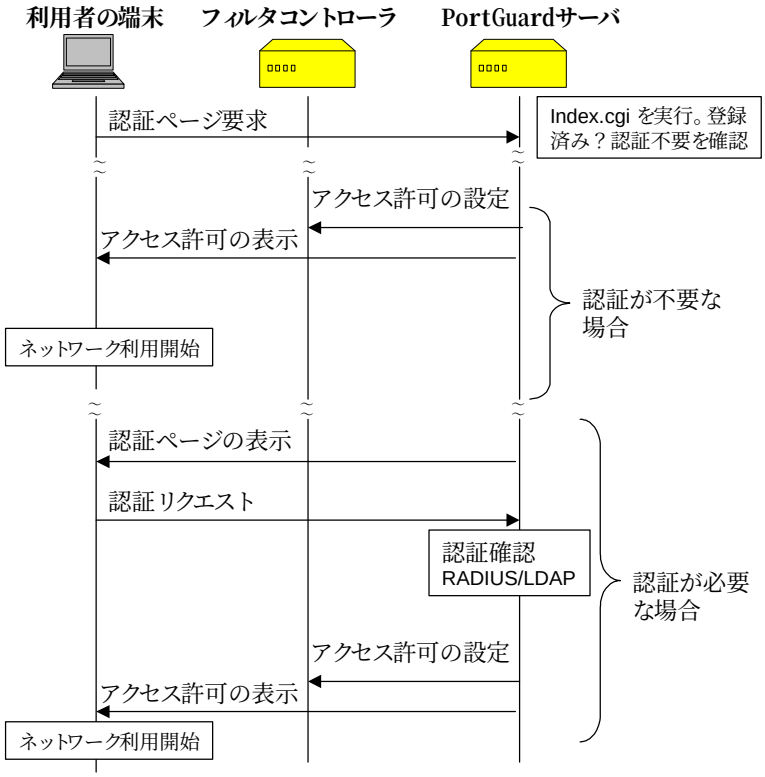

図 3 処理 操作)の手順

2. 3 登録条件の指定

現時点での変更処理の受付方針として以下のルールを検討中である.

1) 機器の新規追加 新規 MAC アドレスの機器を接続した場合)

- o 個人利用の PC の場合, 登録者　利用者でありおよその場合, 登録者の権限でアクセス制御する.
- o 不特定者の利用する共同利用 PC の場合, その PC の管理者が登録するものとする. LAN カード交換時の再登録を考慮して, この PC の直接的なメンテナンスを行うものをこの PC の管理者とする.)

2) 登録済みの機器の変更 機器交換時には, 主に削除と追加の操作を行う)

- o 2. 1節の利用インタフェースより削除後に再度登録を行うなどの方法で変更する.

3) 機器の取り外し

- o 時の登録削除は, 登録者のみ可能

4) その他の制限

- o 登録ごとに登録者を記録するため, 同一者による総登録数の上限の設定を可能とする.

3 考察

o 固定設置されている共有端末の場合

この端末の登録者のみ例外処理- 1および 2が可能であるため, その他にあたる端末を利用するものは通常の利用のみ可能である.

o 持ち込み端末や個人所有の PC の場合

端末の MAC アドレスを利用者が登録する事で, この端末への例外処理-2 が可能であるが, 本人の責任で設定し利用することは問題とならないと考えている.　このような利用者であっても, 携帯型 IP 電話器のような機器を利用する可能性を考慮すると, 例外処理-1 でそれらを利用する事ができるようになる. 例外処理－ 1を使い, 他の人端末を認証せずに使わせる事が懸念されるが, これを禁止しても認証した端末自体を他の人に使わせるなど認証した人の責任で他の人が使う事は防ぐ事はできない. ここでは, 利用時の特に注意すべき点として利用方法などの説明での対策を図る.

o 登録時における注意点について

登録者のみ削除や設定変更が出来るシステムでは, 先に登録したほうが有効となるため, 未登録の機器を勝手に登録されるという懸念がある.　登録には認証が必要で記録が残る事や, 運用面で購入した機器を LAN 接続する際や, 情報コンセント配下に接続しなおす際には速やかに登録する事を推奨する事で設定の妨害はおよそ防げると考えている.

4 おわりに

本報告では, 認証付き情報コンセントの管理者への管理コストの低下をめざし, かつ利用者の利便性の向上する例外処理- 1と2を利用するための登録の手間の運用として MAC アドレスを登録制にし, 登録者に登録作業の要求と利便性の提供を行う方法による管理方法を提案した. 考察においても特に不正利用の元になる管理方式とは考えていないが, 継続的な運用によりその評価と検証を進めたい.

今後の課題として長時間利用していない場合の登録者への連絡や, 利用中に指定した期間が終了する際に切断予告の通知方法（作業中に気づくように端末側にポップアップで知らせる例えば RSS によるメッセージのような仕組み）等の利用について検討中である.

また, 本実装では PC 上に開発したソフト及びオープンソースのサーバソフトを利用してゲートウェイとして動作する実装としているが, 実際に 5 年程度の間, 1000Base で接続する多数の PC やネットワーク機器で広帯域なトラフィックを扱う事などを想定すると, ゲートウェイには動的にこまかなアクセス制御のできる高性能スイッチが候補に挙がり, そこにおいても本研究での機能や運用評価が生かされると考えている.

参考文献

[1] 石橋勇人, 坂本晃, 山井成良, 安倍広多, 松浦敏雄, 利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式」. 情報処理学会論文誌, Vol. 42, No. 1, pp. 79--88, 2001

[2] 渡辺義明, 渡辺健次, 江藤博文, 只木進一, 利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発」, 情報処理学会論文誌, Vol42, No. 12, pp. 2802-2809, 2001

[3] 西村 浩二, 秋成 秀紀, 野村 嘉洋, 相原 玲二, 遠隔機器制御プロトコルを用いた有線/無線 LAN 用情報コンセントシステム」, 情報処理学会論文誌, Vol. 43 No. 2, pp. 662-630, 2002

[4] PortGuard システム http://www. portguard. org/