公衆無線LAN　WEBログイン(Cookie)　IEEE 802.1X

Technology Reports

公衆無線LANサービスにおける利便性の向上

ドコモの公衆無線LANサービスを利用するためには，これまで接続ソフトを利用したログイン操作や，WEB画面でのID／パスワード入力をその都度行う必要があった．そこで，公衆無線LANサービスを簡単に利用できるように接続手順の簡素化を行い利便性の向上を図った．

ユビキタスサービス部　小林 篤史 †1　佐藤 秀和 †2
平澤 洋介　平田 謙司

1. まえがき

公衆無線LANサービスとは，IEEE（Institute of Electrical and Electronics Engineers）802.11a/b/g[*1]対応機器（パソコン・スマートフォン・PDA・ゲーム機など）を利用した，駅・空港・カフェ・ファストフード店などで最大54Mbit/sの高速大容量インターネットアクセスが可能となるサービスである（**表1**）．ドコモの公衆無線LANサービスは，2008年9月時点約6,500アクセスポイント（以下，AP）で利用可能で，月額・日額など多様な料金プラン（moperaU＋U「公衆無線LANコース」，Mzone（月額），Mzone（日額））が選択可能である．

公衆無線LANサービスの利用にあたっては，ユーザセキュリティの観点から，2つの認証を行っている（**図1**）．

⑴AP認証

不正利用を防ぐためにAPと携帯端末間で実施する認証であり，事業者識別のためにSSID（Service Set IDentifier）[*2]を利用している．さらに，セキュリティ対策として，APと携帯端末間の無線区間通信を暗号化している．

暗号化方式として，全ユーザが共通の暗号化キーを利用する固定WEP（Wired Equivalent Privacy）[*3]方式と，ユーザごとに暗号化キーを生成しかつ定期的に暗号化キーを更新できる高セキュリティのIEEE 802.1X[*4]認証方式の2方式を提供している．

⑵ユーザ認証

利用者を特定するためにブラウザにID／パスワードを投入して認証を行う．そのため，ユーザがインターネット接続を行うには，AP認証でAPを通過し，次にWEBログイン画面でID／パスワードの入力を行ってユーザ認証を完了する必要がある．スマートフォンなどでは，ユーザ認証のための，毎回のID／パスワード入力操作が難しくログインが完了するまで時間がかかっていた．

そこで，2008年7月1日よりドコモの公衆無線LANサービスエリアでは，ユーザの利便性向上を目的として，2つの機能を提供している．

①自動ログイン機能

高セキュリティのIEEE 802.1X対応携帯端末で，エリア内で無線接続すると自動的にユ

表1　IEEE 802.11a/b/g/の比較

	周波数帯	最大通信速度	変調方式
IEEE 802.11b	2.4GHz	11Mbit/s	DSSS
IEEE 802.11g	2.4GHz	54Mbit/s	OFDM
IEEE 802.11a	5.2GHz	54Mbit/s	OFDM（CCK）

CCK（Complementary Code Keying）：相補型符号変調
DSSS（Direct Sequence Spread Spectrum）：直接スペクトラム拡散方式
OFDM（Orthogonal Frequency Division Multiplexing）：直交周波数分割多重

†1　現在，コアネットワーク部
†2　現在，フロンティアサービス部

＊1　**IEEE 802.11a/b/g**：IEEEで規定された無線LAN規格．それぞれ5.2GHz帯／2.4GHz帯の周波数を利用し，通信速度最大54Mbit/sをサポートする．
＊2　**SSID**：無線LANでのアクセスポイントの識別子．
＊3　**WEP**：IEEE 802.11で規定されている，携帯端末／APに共通の暗号化キーを用いる暗号化技術．

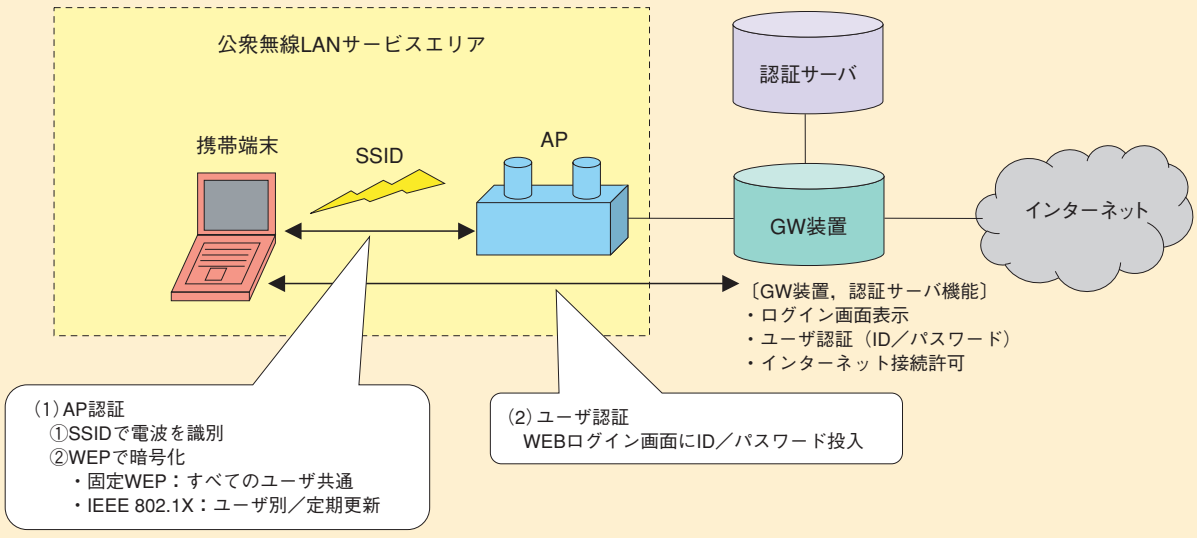

図1　公衆無線LANサービス接続方式概要

ーザ認証を実施する．

②かんたんログイン機能

IEEE 802.1Xに対応していない携帯端末で，ユーザ認証に使用したID／パスワードを一定期間ブラウザ内へ保持し，2回目以降のユーザ認証操作を簡易にする．

本稿では，自動ログインおよびかんたんログイン機能について解説する．

2. 自動ログイン機能

2.1 機能説明

これまで，クライアントソフトなどでWEBログインをワンクリックで行うことはできたが，本機能によりクライアントソフトをインストールしていなくても，IEEE 802.1Xで無線接続が完了するとユーザ認証が同時に実施されインターネット接続を行えるようになる．IEEE 802.1Xを利用した自動ログイン機能を**図2**に示す．

(1)従来の機能

ユーザは無線LANエリアで携帯端末を起動すると，携帯端末はIEEE 802.1X認証を通してAPへ接続しようとする（Step 1：AP認証①）．APは携帯端末からの要求により認証サーバと通信を行い，携帯端末認証を行う（Step 1：②）．携帯端末はIPアドレスを取得する（Step 1：③）．ユーザはWEBログイン画面でID／パスワードを投入しログインを実施（Step 2：ユーザ認証①）．GW（Gateway）装置はID／パスワード認証を実施し，認証されればインターネット接続を許可する（Step 2：②）．アプリケーション通信が可能になる（Step 3：インターネット接続）．

(2)今回新たに提供した機能

ユーザが無線LANエリアでの携帯端末を起動し，IPアドレスを取得するまでは，従来と同様である（Step 1：AP認証，ユーザ認証①～③）．AP認証で利用したID／パスワードで，GW装置はユーザ認証を行い，携帯端末に対してインターネット接続を許可する（Step 1：AP認証，ユーザ認証④）．アプリケーション通信が可能になる（Step 2：インターネット接続）．

本機能によりユーザは，ドコモの公衆無線LANサービスエリアに入って携帯端末の電源を入れるだけで，インターネットに接続することができる．

＊4 **IEEE 802.1X**：IEEEで策定されている無線LANにおけるユーザ認証の規格．ドコモでは認証方式としてEAP-TTLS（＊5参照）/PEAP（＊8参照）を提供している．APの実装により一定期間で再認証の実施および無線区間（携帯端末－AP間）の暗号化キーを更新しセキュリティを高めている．

2.2 提供機能における改善点

⑴IEEE 802.1Xの2方式提供による接続不可の解消

自動ログインを提供するにあたりこれまでに提供してきたIEEE 802.1XのEAP-TTLS（Tunneled Transport Layer Security）[*5]方式（以下，TTLS）に加え，Windows XP®[*6]，Windows Vista®[*7]で標準搭載されているPEAP（Protected EAP）[*8]方式（以下，PEAP）に対応することで，ユーザはクライアントソフトをインストールしなくても，携帯端末に設定するだけで自動ログインを利用可能とした．IEEE 802.1X方式（EAP-TTLS/PEAP）の2方式を提供することとなるが，特定条件下にて接続できない携帯端末（PEAP認証時のフェーズ1 IDにanonymous[*9]が付与される携帯端末）が存在することが判明した．

・問題点

ドコモが提供しているクライアントソフトのTTLS認証時ではフェーズ1 IDにanonymousを付与しており，PEAP認証時はフェーズ1 IDにanonymousを付与しないと想定していた．しかし，携帯端末からのPEAP認証時のフェーズ1 IDにanonymousが付与される場合があり，その時，認証サーバはユ

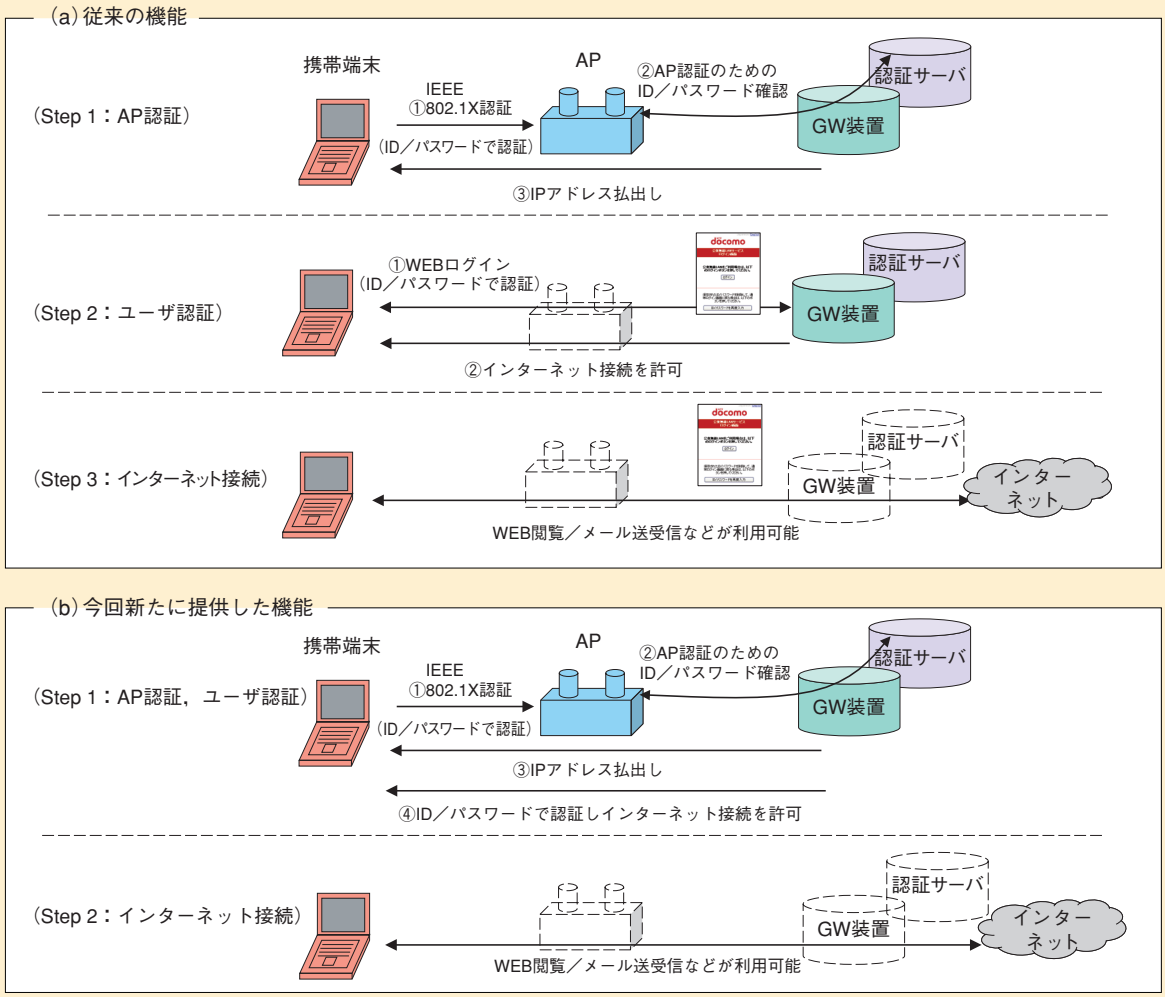

図2　IEEE 802.1X 認証を利用した自動ログイン機能

＊5 **EAP-TTLS**：EAP-TTLSは，携帯端末側へIDとパスワードを設定する方式．

＊6 **Windows XP®**：米国Microsoft Corp.の登録商標．

＊7 **Windows Vista®**：米国Microsoft Corp.の登録商標．

＊8 **PEAP**：PEAPは米マイクロソフト社が開発した規格でEAP-TTLSと同様に携帯端末へIDとパスワードを設定する方式．Windows XP，Windows Vistaに標準搭載されている．

＊9 **anonymous**：ユーザIDを通知しない場合に用いる匿名のID．

ーザがTTLS認証を要求していると判断する．その後，携帯端末は，TTLS-Start通知を受けると，認証サーバに対してPEAP認証要求を通知する．しかし，認証サーバはTTLSと確定済のため，方式不一致とし接続不可となる事象を確認した（**図3**(a)）．

・解決策と改善

フェーズ1 IDでの方式確定を廃止し，認証サーバからの最初の通知を一律PEAP-Startとし，応答と異なる認証要求であっても認証サーバは適切に応答することで解決した．携帯端末がTTLS認証を要求する場合，認証サーバからはPEAP-Startが通知されるが，携帯端末はTTLS認証要求を通知する．応答と異なる認証要求であるが，認証サーバはTTLS-Startを応答し，認証が継続される（図3(b)）．

(2)二重ログイン制御実施とWEB画面への表示

公衆無線LANサービスでは，同一のID／パスワードを利用して複数の携帯端末で利用可能なことから，同一のIDの利用では，同時に複数携帯端末が利用できないように二重ログインを不可としている．しかし，AP認証（IEEE 802.1X）に関

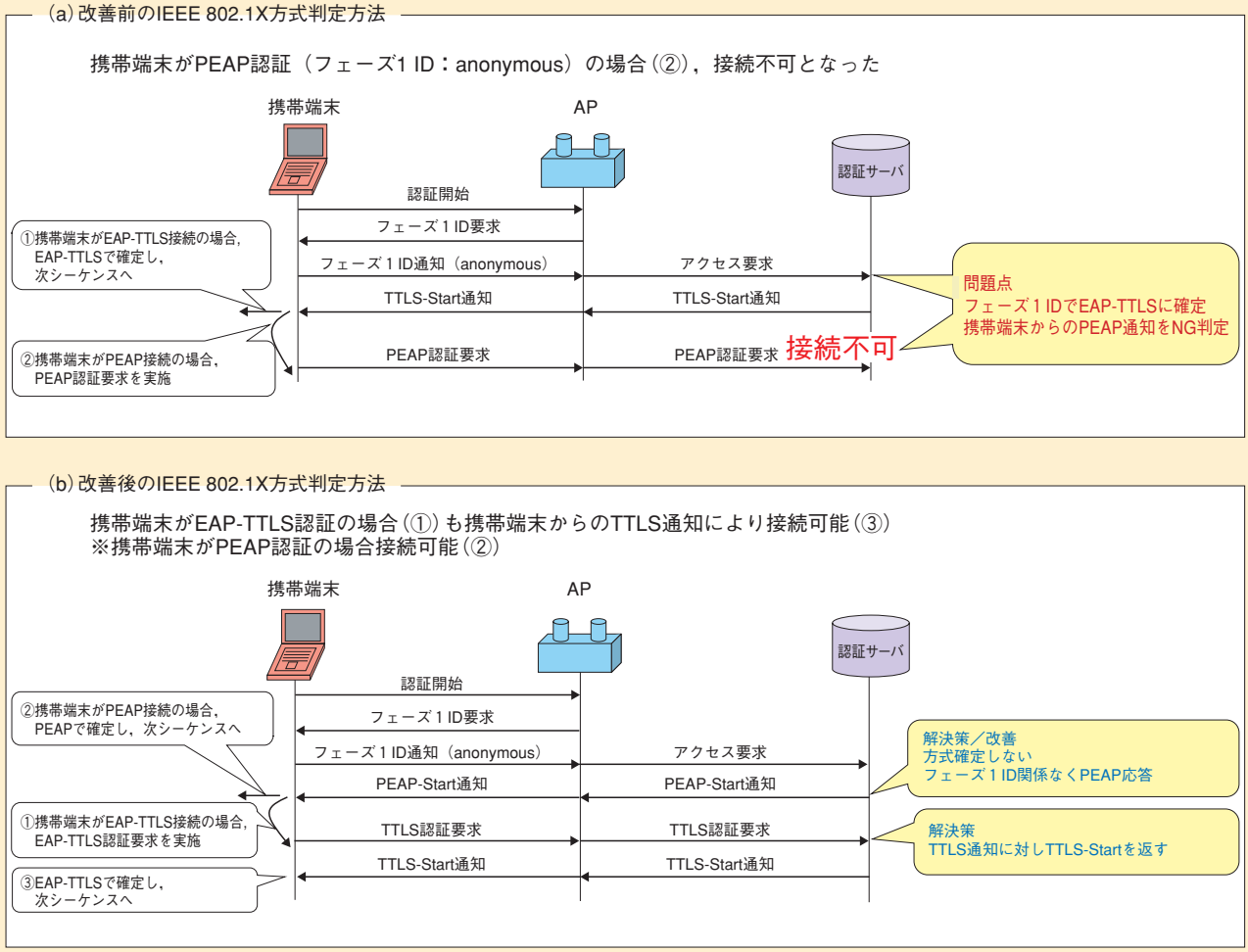

図3　IEEE 802.1X方式判定方法について

しては，定期的に再認証を実施するため，近くの公衆無線LANサービスエリアをまたいで利用する場合のようにAP間移動時の利用などを想定し，AP認証の二重ログイン（同一ユーザID／パスワードの利用）は許容とした．ただしユーザ認証については，複数の携帯端末での利用防止のため，二重ログイン不可はそのままとした．

しかし，特定の条件下にてユーザは無線が接続され，自動ログインをしているつもりが，インターネット接続ができない状態になっている場合が存在する（二重ログイン状態）．そこで，そのようなことがないように，自動ログイン時にログイン画面を表示せずに，最初のHTTP要求時に二重ログインエラー画面を表示してユーザにすでにID／パスワードが利用されていることを示すことで，ユーザは片方のログイン状態をログアウトするなどの対処ができるようにした．

⑶誤請求防止

ユーザは公衆無線LANサービスエリアに入り携帯端末の電源を入れるだけでインターネット接続が可能となる場合があるため，日額契約者やローミングイン利用のユーザ[*10]が意識せずに課金されることを防止するため，契約種別によって自動ログイン機能利用の可否を決定し，月額または定額のユーザのみ利用可能とした．

⑷URLログアウト

これまでサービス終了を行うために，ログイン後にログアウトボタンを配置した画面を表示していたが，今回自動ログインを行うとログアウト画面が表示されなくなったため，ブラウザのアドレス欄にログアウト用URLを入れるだけでログアウトできるようにした．

⑸ログアウト時の注意喚起

自動ログイン時にユーザがログアウトしても無線接続は継続されており，IEEE 802.1Xの再認証が行われるため，ログアウト画面に無線接続を切断しない場合は，再度自動ログインしてしまう場合があることを注意喚起した．

3. かんたんログイン機能

3.1 機能説明

WEBログイン画面において30日間ID／パスワードを保存する機能を提供し，ワンクリックでのログインを可能とした（**図4**）．

⑴従来の機能

ユーザ認証を実施するためにログイン画面表示～ログイン動作を毎回行う必要があった．

・ログイン画面表示

ユーザは，WEBブラウザを立ち上げ，GW装置はインターネット接続可否を判定しWEBログイン画面をリダイレクト表示する．

・ログイン動作

ユーザはログイン画面にID／パスワードを投入しログインボタンを押下する．GW装置はID／パスワードを判定し，認証完了となればインターネット接続を許可する．

⑵今回新たに提供した機能

ユーザは，一度ID／パスワードを投入して保存すれば次回のログインからID／パスワードを投入せずにログインボタンを押下するだけでログイン可能とした（初回登録より30日間）．なお，携帯端末はCookie[*11]を保存可能でありCookie保存を有効に設定しておく必要がある．

・1回目のログイン画面表示とログイン動作

ユーザはこれまでと同様のログイン画面にID／パスワードを投入し，「ID／パスワードを保持する」にチェックしログインボタンを押下する．GW装置はID／パスワードを判定し，認証完了すればインターネット接続を許可するとともに携帯端末へCookieを送付する．携帯端末はCookieを保存する．

・2回目以降のログイン画面表示

GW装置はインターネット接続可否とCookie保存期間を判定して初回Cookie保存後30日以内であればかんたんログイン画面を表示する．Cookie保存後31日以降であれば通常のログイン画面を表示する．

・2回目以降のログイン動作

Cookie保存後30日以内の場合は，ユーザは「ログイン」ボタンを押下する．31日以降の場合は，1回目のログインと同様となる．

＊10 **ローミングイン利用のユーザ**：他事業者の契約者でドコモの公衆無線LANエリアで利用するユーザ．

＊11 **Cookie**：ユーザに関する情報やサイトへの訪問時間／回数などを携帯端末に保存し，ユーザの利便性を向上させる機能．

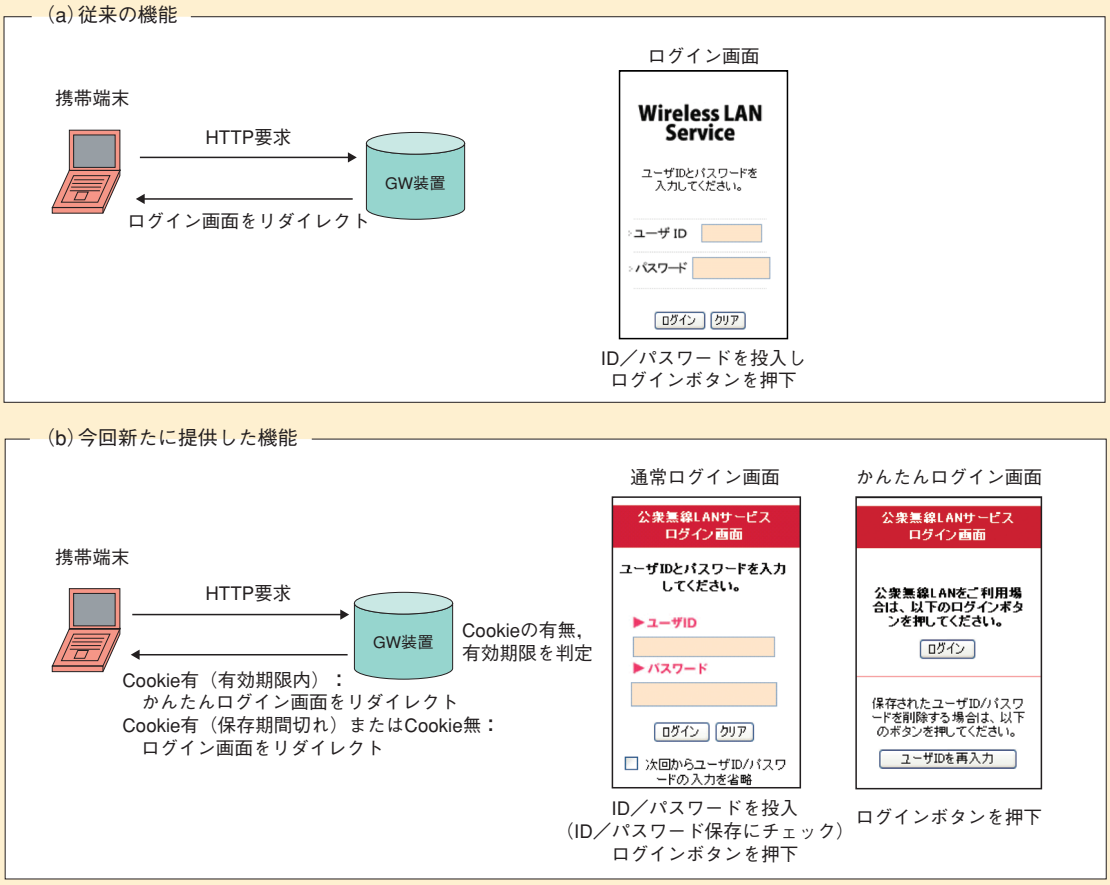

図4　WEBログイン機能の比較（かんたんログイン機能）

3.2 提供機能における改善点

ID／パスワード保存機能であるかんたんログイン提供において大きく3つの改善を行った．

(1)セキュリティ対策

①かんたんログイン画面でのID／パスワード非表示

ID／パスワード非表示にし，公衆の場所で利用する携帯端末のID／パスワードを周囲から見られないようにした．

②Cookie保存期間を設定

Cookieの有効期限を設けることで，万一Cookieが漏洩したとしても継続して利用できないようにし不正利用を防ぐようにした．また，利用状況などを考慮してCookie保存期間を柔軟に変更できるようにシステムを構築した．

(2)操作性の向上

ユーザがID／パスワード変更を実施した場合に，ログイン画面に「ユーザID／パスワードを再入力ボタン」をつけることで，ボタン1つで変更後のID／パスワードを投入できるようにした．ブラウザ内の設定でCookie削除を実施しなくても「ユーザID再入力」ボタンを押すだけでCookieを無効化しID／パスワードを投入可能なログイン画面を表示し新しいID／パスワードでログインできる．

(3)かんたんログイン設定状態を反映した画面表示

図4で示すように，状況によりかんたんログイン画面と通常のログイン画面の2つのログイン画面が表示される．ログイン画面がキャッシュされていると，Cookie保存期間中に通常ログイン画面が表示されるなど本来表示されるべきでない画面が表示さることがあり，まず，キャッシュを利用してはならないという意味のHTTPヘッダ（Cache-Control：no-cache）を送信して対処していた．しかし，特定のブラウザでは同一セッション内（ブラウザを終了させない場合）ではキャッシュが利用され，表示されるべきでない画面が表示されることがあった．よってHTTPヘッダ（Cache-Control：no-store）も送出するようWEB Server設定を追加することで，特定ブラウザ内の同一セッションでのキャッシュを防ぎ，想定どおりのログイン画面表示を可能とした．

4. あとがき

本稿では，公衆無線LANサービスをより簡単に利用するための2つの機能（自動ログイン・かんたんログイン）の方式について解説した．この機能とサービスエリアの充実により，従来以上にユーザへ利用しやすい環境を提供できたと考えている．今後もエリアの充実やさらなる機能拡充によりワイヤレスブロードバンドの発展に寄与していきたい．