第 18 部

インターネットにおける広域無線網の利用実験

第 1 章

WRW 報告 - 移動体環境のセキュリティ

1.1 はじめに

携帯情報端末の普及や セルラホーン (携帯電話)，PHS，広域無線ネットワークの整備・普及により，移動環境下でのインタネットへのアクセスもより手軽になってきた．WIDE プロジェクトでも，従来から MUC，WRW，phone-shell，OS などの研究ワーキンググループにより， 移動体環境でのインターネットアクセス技術と，それに関連する技術について研究を行ってきた．

この章では，そのうち移動体環境のセキュリティ問題について，フォーカスを当てて検討する．

1.2 具体的脅威

移動体環境におけるセキュリティ上の脅威について，ITU-R の M.1078 勧告の分類を元に，具体的にする．

- 端末の盗難による不正利用

  当然ながら携帯機器は持ち歩きが用意なため，オフィスに設置された機器にくらべて，盗難や紛失の可能性が非常に高い．従って，機器が第 3 者の手に渡ったときも，機器の不正利用を防止する機構が必要となってくる．

  不正利用のケースとして，携帯機器そのものの機能，特に蓄積された情報を不正利用されるケースと，ネットワークを不正利用されるケースが考えられる．PDA のような高機能の携帯機器の場合は前者のほうが，携帯電話のような通信機能に特化した携帯機器では後者のほうが脅威となる．

- クローンの作成

  携帯機器の複製をつくりネットワークを不正に利用するものである．海外では，クローン電話の被害が多いことは，承知の通り．

- なりすまし

  機器内部のアドレス設定を不正に変更したり，ROM を交換するなどの方法により，自アドレス情報を偽り，別の機器になりすまして不正にネットワークを利用する．

- ハイジャック

  通信中の呼を横取りして，不正に通信を乗っ取る不正を ハイジャックと呼ぶ．なりすましの防止のため，通信路の確立時に通信相手を認証したとしても，その後の通信でハイジャックが可能なら，なりすましされてしまう．

  通常の専用線・LAN 等をベースにしたインターネットでも，ハイジャックの危険にさらされているが，携帯機器の通信手段である無線通信では，さらにその可能性が高い．

- ユーザ ID の不正入手

  携帯機器の ID や，ユーザの ID を盗聴することで不正入手し，なりすましなどの不正利用を行なう．

- ユーザ位置の不正入手

  広域の無線通信システムでは，ふつうサービスエリアをセルと呼ばれる小さなエリアに分割している．移動機器はその時点で属するエリアの局と通信することで，電波送信出力の省出力化，電波帯域の効率的な利用を行なうことができる．このようなシステムでは，セルに関連する情報により移動機器の大まかな位置を，知ることができる．

  このような情報，または，電波の発信源を調べる方法により，携帯機器のこの位置情報を，そのユーザに知られずに入手する危険がある．その結果，すなわちユーザの移動経路を知ることができてしまい，プライバシー，その他の問題を発生させる．

- ユーザ通信の盗聴

  無線通信では，第 3 者による盗聴の可能性が非常に高くなる．そのため，実際のシステムでは，スクランブルやメッセージの暗号化などの対策を行なっているが，暗号鍵を不正入手することができれば，暗号を解読することが可能になってしまう．鍵を入手する方法としては，鍵交換のための通信を盗聴したり，装置を分解したり管理用のコマンドを用いるなどの手段がとられる．

- ユーザ通信内容の改ざん

  流れている情報を第 3 者が不正に変更 (すなわち改ざん) できる危険性は，前述の盗聴と同じである．

- ユーザ位置情報の改ざん，ユーザサービス・プロファイルの改ざん

これらの制御情報を発信者が改ざんすることで，特定のサービスの不正利用等を行なうことができる．

- 加入者システムへの不正侵入

  ネットワーク側から，携帯機器への不正侵入である．携帯機器が高機能であれば，インターネット上の計算機と同様の脅威を及ぼすことになる．

- 料金支払い拒否

  不正なプロトコル，制御情報の改ざんなどで，料金の支払いを拒否する．いわゆる，ただかけである．情報の流出や改ざんではないが，通信システムへの脅威となる．

- 局内システム，網制御機構への侵入

  途中経路上の局内装置に不正にアクセスし情報を不正アクセスしたり，網管理の機構を不正に利用して運用を妨害するなどの脅威.

1.3　対策

セルラ，PHS，MCA とった，実際の通信システムでは，このような脅威に対して，多種多様の対策を行なっている．暗号化による通信の機密保護，鍵交換プロトコルの工夫による鍵漏洩防止，IC カードのような特別な鍵管理機構による ID の保全などである．公開鍵を用いたより安全な機密保護機構も検討されている．

ここでは無線ネットワークをインターネットのサブネットワークとしてとらえ，携帯機器をインターネットアクセスターミナルとして用いたときのセキュリティ上の問題と対策の方向について検討しよう.

- エンドエンドでの認証と暗号化

  無線システムでは，通信経路 (すなわち無線区間) での通信内容の盗聴や，改ざん，なりすましの可能性が高い．そのため，その区間の暗号化などによる機密保護や認証の機構が必要であることはすでに述べた.

  インターネットは，管理組織の異なる複数のネットワークを経由して，相手と通信することが普通である．そのため特定のネットワークやリンクのみを暗号化しても，全体でそれほどセキュリティ脅威が改善されない．無線区間の暗号化は確かに，盗聴やなりすましの有効な手段であるが，一方で，携帯機器から通信対象のシステムまでを通してみると，(危険な部分ではあるが) 一部のリンクの暗号化を行なったにすぎない.

  インターネットでは，PEM や PGP といったセキュリティ強化版のメイルのように，メイルの発信者がメッセージを暗号化し，

受信者が復号化する，いわゆるエンド-エンドでの機密保護策がとられることがある．これによって，ネットワーク上では平文にならずに，すべて暗号文のまま通信されるため，盗聴の危険のあるリンクや他組織の管理するネットワークを経由しても，安全は確保される．

従って，無線を用いた携帯環境でも，無線区間の暗号化は，端末 ID や制御情報の保護，正常運用の妨害といった無線システムとしてのセキュリティ保全のためのものと位置付け，ユーザの認証やメッセージの保護は，エンド-エンドでの対策を行なうことでより確実な対策が可能となる．

- 紛失や盗難の問題

  我々の想定している携帯機器は，ノート PC のような可搬型のコンピュータや PDA といった，高度な機能をもち，情報を蓄積しているものである．このため，紛失や盗難のときの第 3 者による，機器やネットワークの不正利用，情報の不正アクセスは深刻な問題である．

  携帯電話のような専用のハードウエアでは，(十分とは言えないが) 機器の内容を保護する幾つかの機構が用意されている．さらに，紛失や盗難が発生しても，その端末の機能をシステムとして無効にすることができる．しかし，通常のパーソナルコンピュータベースに作られた携帯機器では，ソフトウエア面，ハードウエア面からのセキュリティ対策は，必ずしも十分ではない．たとえば，リセット等の方法でソフトウエアによるプロテクションを外したり，内蔵のハードディスクやフラッシュメモリなどの記憶メディアを取り外し，別の装置に接続し内容をアクセスするといったことは，比較的容易に行なうことができる．

  したがって，高機能の携帯機器では，内蔵の記録メディアのアクセスを容易にできないような，ハードウエア上の機構を用意するほかに，記録の暗号化や，不正アクセス時の内容の自己破壊機構，遠隔による内容破壊の機構を用意する必要があろう．特に，通信に用いる，鍵やパスワード，ID 等の情報は，複数の施策を行なう必要がある．

  蓄積しているデータを紛失することによる損害も大きな問題となる．システム側と携帯機器側で情報を重複してもったり，不要な情報は携帯機器側では，極力保持しないという対策も重要となる．そのために，システムと携帯機器との間で，適切なポリシのもと情報を共有するための分散ファイルのような，情報管理機構が必要となってくる．

1.4 まとめ

移動体環境下でのセキュリティ保全対策は，通信の機密・なりすましについていえば，従来からインターネット上で利用されている，

- エンド-エンドでの暗号化による機密保護，認証

を唯一の方法として，積極的に利用すべきである．

一方，携帯機器の大きな特徴である可搬性による紛失や盗難による第 3 者の不正アクセスの脅威は， 移動体環境独特のものであり，そのために，

- 携帯機器のタンパプルーフなどハードウエア上の対策
- 機器内の蓄積データの暗号化等による保護策
- 特に機器内に保存した鍵や ID，パスワード等の保護策
- データの分散配置によるデータ紛失時のダメージの軽減策

が必要となってくる．今後，具体的な対策，方式について，具体的に検討を進めて行きたい．