（4）次世代移動通信システムのセキュリティ技術

本研究所では，次世代移動通信システムのセキュリティ技術として，ネットワークレイヤセキュリティとアプリケーションレイヤセキュリティの2つの分野に重点を置いて検討を進めている．

クリスティアン シェーファー　フー ワン
Christian Schaefer　Hu Wang
アナン プラサド　トーマス ヴァルター　ペーター ショー
Anand Prasad　Thomas Walter　Peter Schoo

1. まえがき

近年，情報技術（IT：Information Technology）セキュリティの重要性が高まってきている．その最も大きな要因は，インターネットとWebベース技術の利用の増大であろう．これは，移動通信システムにも当てはまり，適切なセキュリティ対策の必要性が増大している．移動通信事業者におけるセキュリティ技術に関する研究は，以下の背景をかんがみると，今後一層重要となる．

⑴移動通信システムの普及に伴い，ユーザはそれが自身の生活にどのような影響と効果をもたらし得るかに期待を寄せる．そして，移動通信システムに求める「信頼」の度合いも変化していく．

⑵セキュリティに関するユーザ意識が高まるに伴い，通信事業者のビジネスモデルにおけるセキュリティの重要性が高まる．セキュリティは，製品品質や通信事業者の競争力の一要素としてより明確に認識され，高いセキュリティの提供は，市場における優位性を強め，ビジネスの成功をもたらす可能性がある．

⑶今日の通信システムは，移動通信ネットワークも含めて，公共インフラを構成する主たる要素となっている．エネルギー，金融，および医療など，多くは通信インフラに依存している．したがって，安全，かつ正確でサービス断のない移動通信システムの運用が移動通信事業者に求められる．

これらの背景と，ドコモがサービスとネットワークの両方を提供している現状を踏まえ，当研究所では，将来の移動通信システムのセキュリティに関する研究を進めている．

セキュリティとは，システムやそれを構成する製品の各所に見受けられる，安全の度合いをいう．セキュリティレベルは，「特に損害は予想されないので，防御は必要ない」から「大規模な損害をもたらし，ビジネスを停止させるおそれがあるため，最高レベルのセキュリティを採用する必要がある」まで，多岐にわたる．すべてのITアプリケーションやシステムに適応できる，唯一のセキュリティの解決策は存在せず，セキュリティの要求条件も個別にならざるを得ない．また，これらのセキュリティの解決策は，必要なセキュリティレベルとリスクをどの程度負えるかによって決められるものなので，システム設計および開発の段階で同時に検討される必要がある．さらに，セキュリティ機能の実装は既存の標準方式や製品をベースに行われることが多いため，その意味でもシステム統合の作業といえる．

次に，セキュリティの特性をさらに詳しくみると，以下の5つのセキュリティサービスに区別できる．これらは，セキュリティ確保やリスク軽減のため，標準化仕様の中にも見られる一般的な要素[1]である．

- 認証：システムエンティティが要求するアイデンティティ（ID），またはシステムエンティティに要求されるIDを確認するプロセス
- 承認：エンティティに与えられている，リソースへのアクセス許可
- 秘匿（秘守性）：権限のない個人，エンティティ，またはプロセスに対し，情報が利用されたり，開示されないようにする特性
- 改ざん防止：情報の正確さと整合性
- 否認防止：操作や通信への関与に対する虚偽の拒否に対しての保障

現在，ドコモはサービスとネットワークの両方を提供している．当研究所としても，ネットワークレイヤセキュリティとアプリケーションレイヤセキュリティの2つの分野（プロジェクト）についての研究を推進している．

ネットワークレイヤセキュリティは，プロトコル，インタフェースおよび情報の交換形式を網羅しており，これらは安全な情報伝送，基本機能とデータ形式および信頼性の高い通信をサポートするインフラ構成要素とアクセスプロトコルに関するものである．異種アクセス技術を含むネットワークインフラへのこれらセキュリティ要素技術の適応は，我々の参加する欧州研究プロジェクトの中でも進められている．2章では，この研究プロジェクトにおける，ネットワークレイヤセキュリティの検討対象と取り組む課題について述べる．

アプリケーションレイヤセキュリティは，例えば，プライベートLAN（Local Area Network）や企業システム間の安全な通信やアクセス，フェデレーション（federation，連

合）を形成可能とする安全なデバイス連携やデータセキュリティなど，アプリケーションに固有の解決策を含む．また，電子文書署名（署名／検証）など，データやリソースを保護するためにアプリケーションで可能な手段も検討対象である．移動端末がフェデレーションを構成する際のセキュリティは，新たな検討分野であり，本研究所が提案を行っている．これにより，移動環境において，安全なフェデレーションを構築することが容易となる．これらについて，3章で述べる．

2. 次世代ネットワークレイヤセキュリティ

国際電気通信連合・無線通信部門（ITU-R：International Telecommunication Union-Radiocommunication sector）[2]は，次世代（第3世代以降）移動通信に必要な開発要求を定めたビジョンドキュメントを発行した．このビジョンには，「いつでも・どこでも最適な接続」という考え方が盛り込まれている．主な特徴は，①2010年頃までに50～100Mbit/sを目指した新しいエアインタフェースの提供（4G無線アクセスの特徴），②既存のシステム間，および①の新しいエアインタフェースとの統合である．

今後の移動通信ネットワークは，既存の無線アクセス方式，有線アクセス方式および新無線アクセス方式などを，コアネットワークに統合し，異種ネットワークをサポートすることが命題である．この場合のセキュリティにおける命題は，アクセス技術またはネットワーク技術に関係なく同じ（望むべき一定の）セキュリティレベルを達成することである．

次世代ネットワーク実現のためには，ユーザの支持も無視できない．ユーザの支持を得るためには，技術に依存しないサービス提供およびセキュリティ提供などが挙げられ，ユーザプライバシーの尊重や使いやすいサービスを考慮する必要がある．また，無線アクセスが本来持つ特徴（有線と異なり不特定多数のアクセスが可能なことなど）からも，セキュリティは重要な要素であり，無線技術の可能性を最大限に活かすには，セキュリティの十分な検討が必要である．

次世代システムにおいては，インターネット技術を利用したパケットベースのネットワーク技術へ向かう動きがある．このネットワーク技術における脆弱性とリスクは良く知られており，技術変化も著しいが，パケットネットワーク技術自体がこれらの問題を引き起こしているわけではない．むしろ，管理の及ばない広範囲なネットワークとアプリケーションの使用，および制御できない任意の多くのユーザなどがリスクを高める原因となっている．このような脆弱なパケットベースのネットワーク環境において，セキュリティの品質と価格（コスト）のバランスの取れた解を見つけることは非常に困難である．

この分野において，当研究所では，リスク分析の手法，インフラの保護，および異種アクセスネットワークのマルチプレーヤー環境におけるセキュリティの検討を行っている．次世代移動体通信ネットワークのセキュリティの検討を進めるにあたり，シナリオベースのセキュリティ検討プロジェクトではまず，ネットワークとそれに適応される技術の組合せを理解し（2.1節），その後，セキュリティ問題の把握（2.2節）を行っている．

2.1 無線ネットワーク技術の組合せ

各種無線システム技術の可能な組合せは，図1に示す関係図で表される[3]．この図において，青の矢印は，技術的には組合せが可能だが，現在の市場または周波数の問題により実現できていない組合せを示す．また，緑の矢印および2つの無線ネットワーク技術間に引かれた線は，可能な組合せを示す．さらに，技術や地理的な利用可否などの観点から技術の組合せを描く事も可能である[3]．

2.2 セキュリティ問題と課題

(1) 信頼性（トラスト）管理

主要なセキュリティ問題の1つとして信頼性が挙げられる．これは，ユーザが，そのシステムがどの程度正しく動作するかを信頼できる度合を意味し，我々の日常生活における信頼関係とほぼ同じものといえる．

移動通信システムでも同様に，信頼の構築は基本的なステップであり，安全な通信やビジネスにも影響する．ユーザは通信事業者をある程度信頼しなくてはならないし，同じく通信事業者はユーザを信頼する必要がある．また，ユーザが現在加入している通信事業者の所有していない別のネットワークに移動するとき，これら2つのネットワーク間に信頼関係が必要になる．

(2) 認証と鍵管理

認証メカニズムは，異種ネットワーク間のセキュリティ技術やポリシーにより異なる．このため，ドメイン間ハンドオーバでは，移動端末がいかにサービスに影響を与えず迅速にこの違いに適応できるかが課題となる．同様に，セキュリティに用いる鍵の管理方法はネットワークやシステムにより異なるため，移動端末の移動性が高い環境において，鍵管理をいかに的確に行うかが課題である．

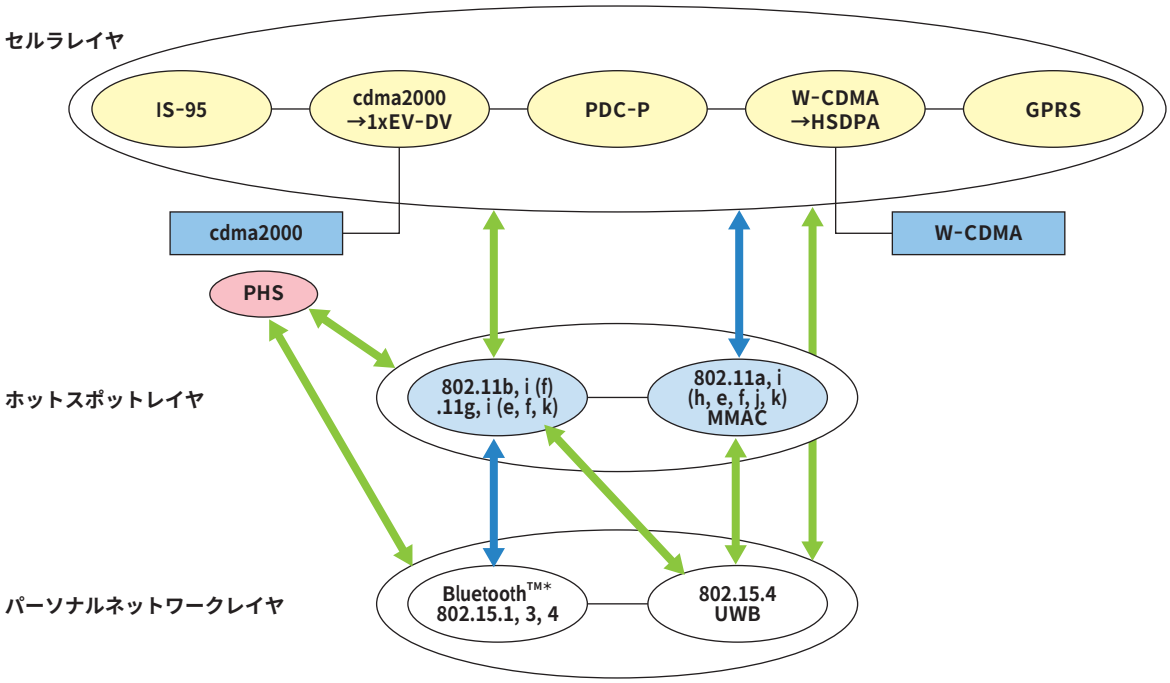

図1　ネットワーク技術の可能な組合せ

(3) サービスレベルアグリーメント

一般に，端末がネットワーク間を移動する場合には，サービスレベル契約（SLA：Service Level Agreement）の確保が重要となる．これは，以下の2つのセキュリティ問題に関連する．①ユーザに保証するセキュリティレベルに関する合意も含まれるため，SLAはハンドオーバによる影響を受けるべきではない，②移動先ネットワークでのSLAの交渉時に，不正侵入者から影響を受ける事が起こらないよう，配慮する必要がある．

(4) 安全なアタッチとデタッチ

移動端末とネットワークの安全なアタッチ・デタッチは重要な課題である．通常，初めてネットワークに接続する場合は，ネットワークと移動端末間で重要な情報が交換される．IP（Internet Protocol）ネットワークにおけるセキュリティ問題の1つとしてDHCP（Dynamic Host Configuration Protocol）が挙げられる．DHCPの使用は，偽造DHCPサーバによる攻撃や，不正な設定情報などの脅威を生む可能性がある．

(5) 課金

ビジネスおよびサービス提供の面から課金も重要な項目である．通信の途中で，異なるネットワーク間のハンドオーバが発生しても，課金記録の完全性や整合性をどのようにして維持するか，否認防止（例えば，顧客がサービスを使用したにもかかわらず，使用しなかったと虚偽の主張ができないような措置など）をどのようにして実現するかといった課題が挙げられる．

(6) 合法的通信傍受と匿名性

通信事業者のネットワークにおける合法的通信傍受（lawful interception）が，該当国の国内法制として規定されている場合がある．公共通信目的に使用される場合には，セキュリティ方式がこの要求条件を満たす必要がある．

匿名性（ユーザIDの保護）とロケーションプライバシーの保護は，一般的な要求条件となってきた．オペレータの許可なしに，ユーザIDや位置情報が第3者に公開されてはならない．また，安全なアクセス接続が確立された後でも，部外者が信号データを記録して，ユーザIDなどの情報を引き出せるようなことは防止されなければならない．

(7) ネットワークリソース

IPレイヤは，レイヤ2とともに大きなヘッダを必要とし，多くの無線帯域を消費する．オーバヘッドの問題を軽減するために，IPヘッダの圧縮技術が用いられている．しかし，現在のヘッダ圧縮技術はセキュリティ対策が十分でなく，場合によってはヘッダコンプレッサの弱点をついて，サービス否認などを引き起こす可能性もある．

また，セキュリティ（例えばIPSec（Internet Protocol Security））やモビリティ（例えばMobile IP（Mobile Internet Protocol））に利用されるプロトコルのほとんどは，方式上のメッセージ交換のために，無線帯域とバッ

＊　Bluetooth：Bluetoothは，米国Bluetooth SIG, Inc.の登録商標．

テリ，すなわち，ネットワークと移動端末のリソースを消費する．特にユーザが頻繁に移動する場合，交換されるメッセージ量が非常に多くなり，セキュリティ要求条件に加えてリソースの要求条件を考慮する必要が生じる．

(8) インフラセキュリティ

通信事業者のインフラセキュリティも重要な問題であり，安全なプロトコルの設計とは分けて，取り扱われるべき問題である．インフラセキュリティとは，ネットワーク，ルータやサーバなどのネットワークノードおよびネットワークで利用可能な，あらゆる情報のセキュリティを意味し，これらのネットワークノードへの攻撃はネットワーク全体をクラッシュさせる可能性すらある．ネットワークノードの安全な管理とソフトウェアのタイムリーなアップグレードは，インフラセキュリティの大きな課題である．

3. 次世代アプリケーションレイヤセキュリティ

新しいアプリケーションが次々生まれ，移動端末の多様性が増していく事を踏まえると，アプリケーションレイヤセキュリティの検討においては，ユーザモビリティのサポートが，今後一層重要になる．以下3.1節では，ビジネスにおけるユーザモビリティを考慮したアプリケーションレイヤセキュリティの一例を取り上げ，要求条件と取り組むべき課題を抽出する．3.2節では，フェデレーションとセキュリティモジュールの概念を紹介し，さらに我々の貢献として移動環境におけるフェデレーションの構築手法を紹介する．3.3節では移動通信事業者が今後取り組むべき課題をまとめる．

3.1 モチベーションと適用例

例として，得意先情報や個人のスケジュールを管理するために携帯情報端末（PDA：Personal Digital Assistant）を使用している出張中の営業マンを考える（図2）．

この営業マンは，得意先や予定表の情報を更新するため，移動端末を介して企業ネットワークに接続する．彼は，企業の販売データベースから最新の販売数量を取得するために，自分の端末でデータを受信する必要があり，また，データ処理を簡単にするために，販売数量を含むスプレッドシートを自分のノートPCや公衆端末に転送する必要がある．

上述のシナリオを安全な環境で実現するためには，主に以下のセキュリティ（要求条件）を満たすことが必要となる．

- クライアントとサーバの相互認証，および複数のクライアントにおける企業データの共有
- 企業のリソースを使用するユーザとそこで使用されるアプリケーションの承認
- データの秘匿性と完全性，通信イベントとトランザクションの否認防止

次に以下の節では，上記要求条件を満たし，モバイルデバイスのグループ間と企業ネットワーク間における安全な通信環境を確立するための手法を述べる．

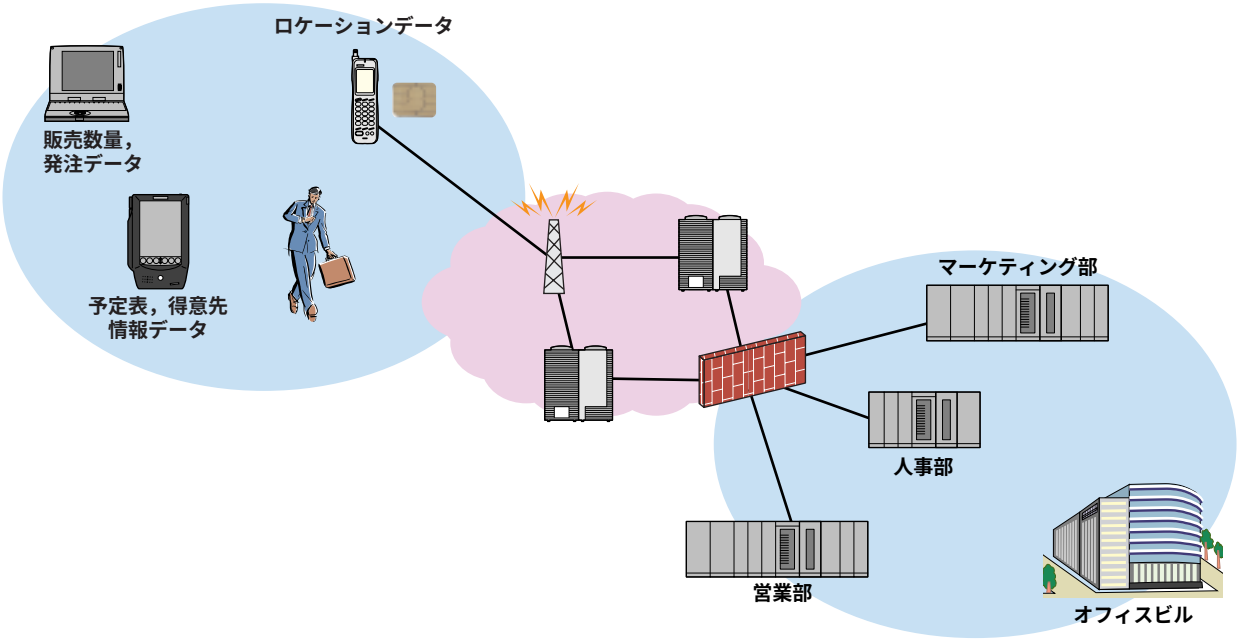

図2　営業マンを例としたフェデレーション構成のイメージ

3.2 フェデレーションデバイスセキュリティ

企業と従業員（B2E）間でのビジネスアプリケーションに重点を置くセキュリティ技術の検討が（前述で示したような例を中心に），第5次欧州研究計画[4]のWiTness（Wireless Trust for mobile business）プロジェクトにおいて行われている．ここでは，安全なモバイルビジネスアプリケーションを実現するために，フェデレーションとセキュリティモジュールという2つの基本概念が用いられている．

(1) フェデレーション

フェデレーションの定義は，デバイス群が協業（コラボレーション）ネットワークを形成するという概念であり（上記の例では，移動端末とノートPCの連携），また各ネットワークノードの役割は端末能力と信頼性に基づいて（事前に，またはアドホック的に）決められる．各デバイスは，例えば，秘密鍵と公開鍵のペア，公開鍵証明書と信頼性証明書といったセキュリティ証明書を格納している．

したがって，フェデレーションは，オーナーの異なる通信機器間における連携関係であるといえる．また，フェデレーションは，信頼できるプラットフォームの概念を，単一エンティティから分散された環境へ拡張したものである．

(2) セキュリティモジュール

セキュリティモジュールは，ユーザの機密データ（ユーザの秘密鍵など）を保持し，セキュリティ関連の機能（ディジタル署名，秘密鍵による暗号化など）を実行する．ここで留意すべき点は，すべての秘密鍵などの秘密データは企業ネットワーク内で生成され，モジュールの初期化中に格納されることである．よって，セキュリティモジュールは，フェデレーション内で唯一信頼できる要素といえる．セキュリティモジュールは耐タンパハードウェア（不正改造できないよう，安全に設計されたハードウェア）上に実装されており，一例として，スマートカードが挙げられる．

フェデレーションを組むモバイルデバイスが，（モジュール内にある）秘密データへアクセスしたり，セキュリティ操作の実行を要求する場合には，常にセキュリティモジュールへのアクセスが行われる．したがって，セキュリティモジュールのないフェデレーションは，企業ネットワークに信頼されず，特定の操作やリソースへのアクセスが企業ネットワークによって許可されないことも起こり得る．

(3) フェデレーションの構築プロセス

前述の例を参考にすると，フェデレーションの確立には以下の3つのステップが必要となる．

①セキュリティモジュールと企業ネットワークが相互認証を行う

②セキュリティモジュールは，連合するモバイルデバイス群（例中のノートPCやPDA）を認証する

③モバイルデバイス群が，企業ネットワークと認証を行う

上記ステップ①は確立した手順（SSL（Secure Socket Layer）接続の確立など）に従って実行される．双方のエンティティには証明書が事前にインストールされており，それらが接続確立中に交換され，有効性の確認が行われる．また，それ以降の通信で使用されるセッション鍵は，セキュリティモジュールの公開鍵に暗号化し，セキュリティモジュールに送信される．ステップ②も上記とほぼ同様であり，認証後にセッション鍵は安全に転送される．

さらに，セキュリティモジュールはフェデレーションするモバイルデバイスを認証することに加え，これらのモバイルデバイスが使用する有効期限付のテンポラリ証明書というセキュリティトークンを生成し，転送する．これにより，モバイルデバイスがフェデレーションに含まれていることを企業ネットワークに示すことが可能になる．

ステップ③はステップ①と同様の手順で行われ，これにより企業ネットワークがモバイルデバイス間でセッション鍵の交換を行うことが可能となる．これら一連の手順を経て，上記の例では，安全で信頼できるフェデレーションがユーザ側にあるセキュリティモジュール，ノートPC，PDAなどと企業ネットワークの間で確立され，これらの安全なチャネルを通し，希望するビジネスタスクが実行されることになる．

3.3 移動通信事業者のアプリケーションセキュリティにおける挑戦

移動通信ネットワークは，ユーザがどこからでも企業アプリケーションへアクセスすることを可能とし，ビジネスの新たな活性化を促して来た．これは，モバイルビジネスアプリケーションが通信事業者にトラヒックの増加というメリットを生み，また，サービスプロバイダにも新しいビジネスの可能性を提供する．

(1) セキュリティと新しいビジネスとの関係

これまで述べたように，移動端末に組み込まれたスマートカードは2つの大きな役割を持つ．まず，移動通信事業者が端末を識別するのに使用するセキュリティトークン．次に，企業が個々の従業員を識別するのに使用するセキュリティトークンであり，企業と従業員間の安全

表1　コンピューティングおよび通信パラダイム

	過去	現在	将来	未来
アプリケーション	アプリケーション固有	クライアント・サーバ（Webブラウジングや Webサービスが中心）	クライアント・サーバ，Webブラウジング，Webサービス，P2P	ユビキタスモバイル端末と通信
端末	デスクトップシステム	デスクトップシステム，移動端末（PDA，携帯電話）	移動端末（PDA，携帯端末）フェデレーションを構成したモバイルデバイス群	
ネットワーク	イントラネット	イントラネット，VPN	イントラネット，VPN，インターネット，有線および無線ネットワーク	

なエンド・ツー・エンド（E2E：End to End）通信を可能とする．これは移動通信事業者がスマートカードへのアクセスをサードパーティ，すなわち企業に許可することになり，企業はアプリケーション固有のセキュリティデータ（鍵や証明書など）を格納・管理することが可能となる．したがって，移動通信事業者と企業間に密接な関係が確立されていくだろう．

このような手法は，最近提供されたドコモのクライアント認証サービス，FirstPass[5]上でも適用可能でありFOMA（Freedom Of Mobile multimedia Access）ユーザは，FOMAカード上に公開鍵証明書をダウンロードすることが可能となった．FirstPassでは，現在のところスマートカードが通信事業者の管理下にあるが，3.1節で紹介したWiTnessプロジェクトの中では，スマートカードへのアクセス権限を第3者へ委任することも可能である．将来，企業などのサードパーティが，このようなサービスに参加し，クライアント証明書を使って顧客の認証が可能となるかもしれない．

WiTnessプロジェクトではアプリケーションセキュリティサポートに関する枠組みを実装した，これにより通信事業者も，新たなアプリケーションを提供したり，補完的なビジネスモデルとしての統合モデルを提供することが可能となる．ここでいう「補完的」とは，このモデルがユーザ数の増大やトラヒック増加のみに依存するのではなく，付加価値サービスを提供することを意味している．

(2) アプリケーションセキュリティの今後の進化

近年，コンピューティングや通信環境は，ユーザやビジネスニーズによって表1に見られるような変化を遂げて来た．現在のアプリケーションセキュリティサポートに関する研究は，主にビジネスアプリケーションに重点を置いて，表1の「現在」とほとんどの「将来」の列をカバーしているといえるが，ピア・ツー・ピア（P2P：Peer to Peer）アプリケーションはまだあまり触れられていない．一方，「未来」のユビキタス環境においては，新たな課題が予想される．一例を挙げると，前述のシナリオでは，セキュリティは単一ドメインの管理下に置かれ，（すなわち，1つの企業がすべての要求条件を定義し）そのために必要なインフラを構築してきた．一方未来は，端末ベンダ，ユーザ，サービスプロバイダなどの，複数のドメインがセキュリティにかかわってくると思われる．この場合，セキュリティと信頼性を確立するためには，すべての関連パートナーと関係を持つ信頼できる第3者が必要となる．移動端末を提供し，ユーザやプロバイダのニーズを理解する移動通信事業者は，この信頼できる第3者となることも可能であり，今後その存在価値がさらに高まることが考えられる．

4. あとがき

本稿では，本研究室の2つの分野の研究内容を紹介した．2章では，ネットワークレイヤセキュリティについて述べ，今後，検討すべき無線ネットワーク技術の組合せの整理と取組みが必要な主たる問題の抽出を行った．次世代ネットワークの検討においては，安全なアクセス技術，ハンドオーバやモビリティにおけるセキュリティ技術が不可欠である事を確認した．今後の計画としては，セキュリティの評価手法や，安全なハンドオーバ方式の提案，また，異なる管理下にあるネットワーク間でのセキュリティなどへ検討対象を広げていきたい．一方，アプリケーションレイヤセキュリティにおいては，方式の実現のため重要な技術であるフェデレーションとセキュリティモジュール技術について述べるとともに，移動環境におけるフェデレーションの構築の手順を示した．今後は，この方式を発展させ，コンテキスト認識型の通信などにおける応用を試みたい．

文　献

[1] IETF Internet RFC 2828-Internet Security Glossary, May 2000.
[2] International Telecommunication Union Radio-communication sector, http://www.itu.int/ITU-R/.
[3] S. Rohr, B. Kpatcha, C. Eckert, A.R. Prasad, P. Schoo and H. Wang: “Feasible and Meaningful Combinations of Access and Network

Technologies for Future Mobile Communications, ” submitted for publication, WWRF #10[PS1], Oct. 27–28, 2003, New York, USA.

[4] WiTness consortium, Wireless Trust for mobile business, http://www.wireless-trust.org.

[5] N. Nakamura, H. Yamamoto and M. Onogawa: “ FirstPass Service Overview, ” NTT DoCoMo Technical Journal, Vol. 5, No. 3, pp. 4–10, Dec. 2003.

用 語 一 覧

cdma2000 ： code division multiple access2000
DHCP ： Dynamic Host Configuration Protocol
E2E ： End to End（エンド・ツー・エンド）
FOMA ： Freedom Of Mobile multimedia Access
GPRS ： General Packet Radio Service
HSDPA ： High-Speed Downlink Packet Access
IP ： Internet Protocol
IPSec ： Internet Protocol Security
IS-95 ： Interim Standard-95
IT ： Information Technology（情報技術）
ITU-R ： International Telecommunication Union-Radiocommunication sector（国際電気通信連合・無線通信部門）
LAN ： Local Area Network
MMAC ： Multimedia Mobile Access Communication systems
Mobile IP ： Mobile Internet Protocol
P2P ： Peer to Peer（ピア・ツー・ピア）
PDA ： Personal Digital Assistant（携帯情報端末）
PDC-P ： PDC mobile Packet data communication system（PDC移動パケット通信システム）
PHS ： Personal Handy-phone System
SLA ： Service Level Agreement（サービスレベル契約）
SSL ： Secure Socket Layer
UWB ： Ultra Wide Band
VPN ： Virtual Private Network（下りリンク高速パケットアクセス）
W-CDMA ： Wideband Code Division Multiple Access（広帯域符号分割多元接続方式）
WiTness ： Wireless Trust for mobile business