テレワークにおける モビリティとセキュリティのバランスのあり方

三井　靖博　　作間　哲夫
千村　保文

インターネットの登場と携帯電話の進化により，人々の生活や仕事の仕方は大きく変化した。インターネットに常時接続できることで、電子メールなどコミュニケーション手段が広がり、世界中の情報にもアクセスが可能となった。さらに、携帯電話を介したインターネットへのアクセスが廉価に提供されたことにより、インターネットはいつでも・どこでも利用可能になってきた。この変化は、NGN*1)（次世代ネットワーク）の登場で、さらに加速するだろう。アクセスできる情報はテキストだけでなく、音声や映像などマルチメディア化されつつある。そして、日本あるいは世界中で高速、広帯域なネットワークアクセスができることにより、ワークスタイルも変わってくる。自宅や外出先でも安心・安全に仕事ができる「テレワーク*2)」が広がるだろう。

しかし、テレワークを便利で快適に、かつ安心・安全に使うためには、モビリティとセキュリティの適切なバランスが重要である。本稿では、NGN時代のテレワークにおけるモビリティとセキュリティのバランスに関する課題を示し、OKIが提唱するソリューションのコンセプトを解説する。

テレワークに必要なネットワーク環境

テレワークには自宅で行う在宅勤務だけでなくサテライトオフィスなどの施設を利用する施設利用勤務、いつでもどこでも仕事ができるモバイルワークなどがある。それぞれの形態で利用できるネットワーク環境は有線LAN、無線LAN、移動体通信網、さらにもうすぐサービスが始まるWiMAXなど多種多様である。在宅勤務者であっても外出してモバイルワークを行い、かつその逆もある。テレワークを行うテレワーカにとってネットワークの種類にかかわらず手軽に安心・安全に利用できるネットワーク環境が望まれる。

NGN時代のモビリティとは

NGNは、高速・広帯域、かつ高信頼、ハイセキュアなネットワークである。地理的に場所が移動しない固定端末だけでなく、携帯電話のような移動端末も収容できるシームレスなネットワークである。NGNは、いつでも・どこでも安心・安全にネットワークを介して生活、仕事ができるユビキタス社会の実現を目指している。NGNの時代には、多様なサービスをさまざまな場所で使えるようになるであろう。このことを移動性、モビリティのあるサービスと呼ぶ。

ITU-T（国際電気通信連盟、電気通信標準化部会）ではY.2001（NGN概要）勧告において、汎用的なモビリティを以下のように定義している。

「ユーザーや端末などの場所やアクセス手段が変わった場合に、環境の変化にかかわらずサービスにアクセスできる能力。サービスの有効性の程度は、アクセスネットワーク能力、ユーザーのホームネットワークと訪問先のネットワークの間のサービスレベルの契約などのいくつかの要因に依存する。」

補足すると、モビリティには以下の3パターンがある。

(a) 端末・モビリティ
(b) パーソナル・モビリティ
(c) サービス・モビリティ

(a) の端末・モビリティは、利用者が端末を持って移動して、同じサービスを使うケースである。アクセスするネットワーク事業者が変わったりすることもある。また、(b) のパーソナル・モビリティは、端末を持って移動するのではなく、利用者のみが移動し、移動先で別の端末にログインして、同じサービスを使うケースである。(c) のサービス・モビリティは、利用者が移動し、使っていた端末から別の端末にサービスを移行するケースである。たとえば、携帯端末を使ったテレビ電話で仕事の話をしながら家に帰宅し、そのまま家のIPTVに相手の映像を映すようなケースである。ちなみに、いずれのケースのモビリティでも、サービスを無中断で継続するか否かは、特定していない（サービス内容により異なる）。

NGN時代には、ネットワークサービスが多様化し、自宅や出張先でさまざまなサービスがシームレスに利用できるようになるだろう。

＊1）Next Generation Network。NGNは、従来の電話網が持つ信頼性・安定性を確保しながら、IPネットワークの柔軟性・経済性を備えた、次世代の情報通信ネットワーク。
＊2）情報通信手段を活用して行う、場所や時間に制約されない働き方。

OKIが提案するテレワークスタイル

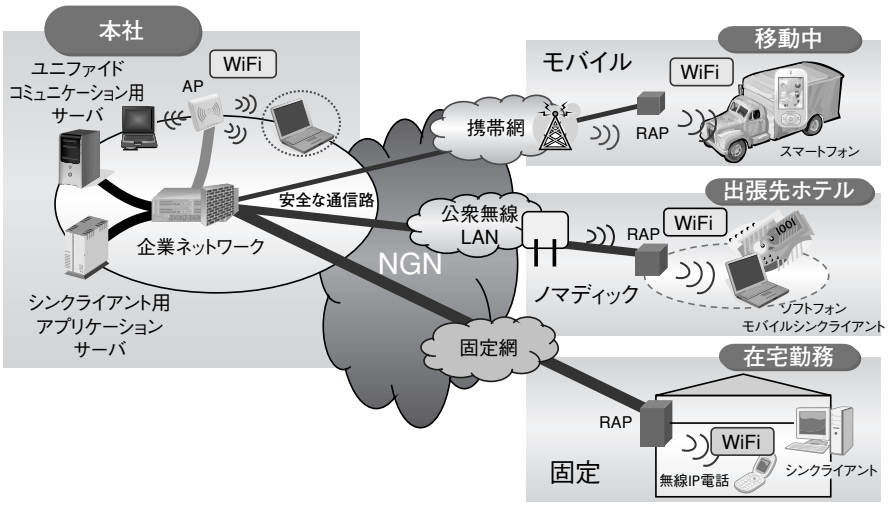

図1　テレワーク実施形態の分類

テレワークにおける課題

（1）テレワーク実施形態の整理

テレワークの実施形態から見たモビリティを大きく分類すると、固定実施、ノマディック実施、モバイル実施の3つの形態に分類できる（**図1**）。

それぞれの形態について、現状を整理する。

①固定実施

ネットワークは基本的に高速で定額利用が中心である。端末もディスクトップPCのような機能的にも制約の無いものを使うことが可能である。業務を社内と同等に行うための機能はそろっている。

しかし、私的利用PCをそのまま使用して、社内システム利用などのサービスを享受するためには、端末面でセキュリティ脅威が大きい。ネットワーク面でも家庭内およびインターネットなどの管理されていない、脅威の存在が予想されるネットワークを利用するため、そのままでは危険である。

②ノマディック実施

ネットワークは固定実施と同等レベルが使える可能性は高いが、行く先々で変化する。場所によってはモバイル実施と同等のネットワークを使う必要もある。端末は持ち運ぶために小型軽量なものが望まれ、機能的に固定実施の端末と比較すると若干劣る。

セキュリティ的には、変化するネットワーク環境、および端末が小型軽量であるがゆえの盗難や紛失の危険性の高まりにより、固定実施より高いセキュリティが必要である。

③モバイル実施

ネットワークは基本的に携帯網などの移動体通信網を利用する必要がある。端末はモバイル用の端末でなければ、常に持ち運ぶことなどできない。

セキュリティ的にはネットワーク面でも端末面でもノマディック実施よりさらに脅威は増加し、高いセキュリティが必要である。

ネットワーク環境向上や端末の進歩の恩恵を受けて、1990年代後半から2000年代前半には社内システムの自宅やホテルからのノマディックな利用や、移動中や必要時にいつでも可能なモバイル利用が流行りはじめた。しかし、その流行りは近年あっというまに影を潜め、今では「モバイルPCは危険なので持ち出し禁止」となっている企業も多い。結局のところ、モビリティだけが先に急激に拡大したため、もう一つの重要な要素であるセキュリティが追いついていかず、情報漏えいに対する脅威や事故に対する批判を恐れるあまり、モビリティを犠牲にしているのが実態である。

テレワーク白書2007でも、せっかくテレワークを導入したにもかかわらず、中断してしまった企業の中断理由のトップとしてセキュリティの問題が挙げられている[1)]。テレワークを禁止しておけば安全なのは確かだが、それ

では折角ICT（Information and Communication Technology、情報通信技術）の進歩から生み出されたモビリティの活用を放棄していることになり、テレワークを活かした企業活動の効率化をも放棄することになっている。

今後のNGNの展開や、更なる技術の進歩により、モビリティの構成要素であるネットワークや端末の更なる進歩が見込まれる。しかしそれを活用するためには、モビリティに見合ったセキュリティが必要となる。

(2) モビリティとセキュリティのバランス

前項の通り、テレワークとして企業の内外で、いつでも・どこでも仕事ができることはメリットがあることばかりではない。モビリティが高まると、ネットワーク環境としても端末としてもセキュリティ・リスクが高まる。そのため、多くの企業では、モバイルPCなどの端末を持ち出し禁止にしたり、端末に時間の掛かる多重認証やネットワークや端末性能を低減させるセキュリティソフトウェアなどのような“常に”重くて堅いセキュリティを導入したりする対策を採っている。しかし、このような対応は、折角のモビリティの利便性を制約することになる。そのため、利用者の権限や移動先での情報アクセスの目的、利用するアプリケーションに応じたバランスのとれたセキュリティ施策が重要となる。OKIは、このようなNGN時代のユビキタス社会に向けたセキュリティを「ユビキタスセキュリティ」と呼んでいる。

必要となるセキュリティは脅威の大きさや種類によって変化し、脅威は資産の価値や種類、置かれている状況などによって変化する。全ての脅威に対して対応でき、利用者に負担の無いセキュリティなど存在しない。融通の利かない堅いセキュリティは得てして利用者にとって手間がかかり利便性の低いものである。そのようなセキュリティを常に利用させるようなセキュリティ施策では、結局利用者が拒否したり利用者の負担になったりするため、期待していたセキュリティ効果や業務効率向上が実現できなくなることになる。

課題解決のアプローチ

(1) ユビキタスセキュリティのコンセプト

ユビキタスセキュリティとは、安心・安全にネットワークサービスを活用するためのセキュリティである。モビリティとセキュリティのバランスを取り、利用者の環境・状況に応じて、いつでも・どこでも、安心・安全なネットワークサービス機能を提供可能とする。

ユビキタスセキュリティを実現するために、OKIは以下の3つのUに始まる機能を提供する（**図2**）。

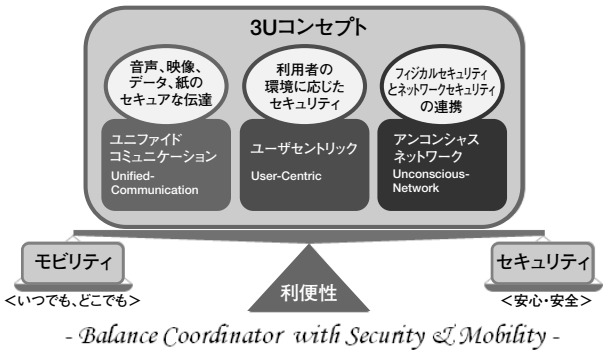

図2　ユビキタスセキュリティ

①ユーザーセントリック

いつでも・どこでも、安心・安全にサービスを利用できるようにするためには、利用者の環境に応じてサービスを提供するための、人に優しいセキュリティ機能が重要である。

②ユニファイドコミュニケーション

すべての情報は、音声、映像、データ、紙といったメディアとして伝達される。これらのマルチメディアはネットワークやアプリケーション上で統合され、さまざまなコミュニケーションを提供するユニファイドコミュニケーションを実現する。ユビキタス社会では、セキュアなユニファイドコミュニケーション機能が重要である。

③アンコンシャスネットワーク

利用者に優しく、かつ利便性に優れたサービスのためには、環境に埋め込まれ、さりげなく利用者の行動をモニタリングし、支援を行うネットワーク機能が重要である。

(2) ソリューション例

テレワークの課題解決において、ユビキタスセキュリティ・コンセプトの適用例を以下に示す。

①RAP（Remote Access Point）

テレワークにおいてテレワーカーが効率的に作業するためには企業ネットワークとの接続が必要となるが、その際にはセキュリティの高い通信路を確立する必要がある。

そのために「VPN（Virtual Private Network）」が基本的に使われ、その実現に広く利用される技術としてPPTP（Point to Point Tunneling Protocol）、L2TP / IPsec（Layer-2 Tunneling Protocol / IPsec）、IPsec、

SSL-VPN、SSH tunnelingなどがあるが、いずれもVPN確立時の認証と通信内容の暗号化が行われる。

利用するVPN選択にあたってはセキュリティ強度だけでなく、使用する端末や利用場所に応じたNAT（Network Address Translation）への対応、利用するアプリケーションの導入の容易さなどを、利用者が考慮する必要がある。

上記課題の解決アプローチとして、弊社ではアルバネットワークス社の自分の／自社のネットワークを持ち運ぶというRAPソリューションを提案する。バックボーンとして中間ネットワークの種別を意識せず、さまざまなネットワークが利用でき、VPN接続が可能であれば、社内のネットワークを持ち運んで、いつでも・どこでも業務のために社内と同じ装置がそのまま使える。その結果として、利用者の手間（端末の設定変更など）は軽減される上に、変更に伴うセキュリティ脅威が軽減される。

②シンクライアント*3) におけるマルチメディア利用

テレワークでは社外から企業情報を扱うため、端末面における脅威、たとえば盗難／紛失などにも考慮する必要がある。シンクライアントはデータ／アプリケーションを社内に置き、操作のためにのみ使用しデータを保持しないため、情報漏洩対策として有効である。

しかし、シンクライアントでユニファイドコミュニケーションを利用する場合には注意すべき点がある。たとえば、ソフトフォンはテレワークにおいて、社内とのコミュニケーションに重要な役割を果たすだけでなく、社外の取引先からの電話も社内にいるのと同様に対応できるため非常に有効だが、ソフトフォンは通話品質の確保のためにcodecによる音声圧縮とrtpによるネットワーク遅延／揺らぎ対策を行う。

シンクライアントではソフトフォンのプログラムが社内のサーバ上で動作するため、rtp / codecが処理された後でインターネットを経由してシンクライアントと送受されるため、通話品質が極端に悪化する。この問題を解決するためには、rtp / codec処理をシンクライアント上で実行するなどの対策が必要となる。

③コンテキストを利用したセキュリティ

携帯電話などのモバイル端末においては、PCで行われていた各種のセキュリティ対策が徐々に適用されるようになってきた。特に法人利用ではVPN、暗号化、端末管理、ウィルス対策、情報漏えい対策など、PCと同等レベルの対策が適用されてきている。さらにモビリティの観点から考えれば、本来はPCよりモバイル端末の脅威レベルの方が高い上、モバイル端末が扱う資産（データや資料など）もPCと同等になってきており、モバイル端末に対してPCと同等のセキュリティに加えて、モバイル端末ならではの対策も必要となると予想する。

そのためのアプローチとして、アンコンシャスネットワークのコンセプトに基づき、端末やネットワークのコンテキストを利用して、危険を察知し、リスクを低減するべく動作する仕組みを検討している。もちろんこの仕組みはモバイル端末のみならず、モビリティを活用したICTの利用全般において有益だと考えている。

今後の展望

テレワークは、NGNの普及、携帯端末の多様化と少子高齢化などの社会的要因により、ワークスタイルのひとつとして定着してゆくであろう。今後は、単にいつでも・どこでも仕事ができるだけでなく、利用する環境に応じたセキュリティを確保することが必要となる。本稿では、持ち運びする機器を中心に解説したが、今後は“情報”面から見たセキュリティ確保のためのサービス基盤の整備拡充がさらに重要である。

お わ り に

テレワークをより有益なものにするには、単に技術だけでは十分でない。テレワークに適した仕事の進め方や評価基準、さらに職場や家族などの周囲の理解と協力無しには実現しない。本稿を記載するにあたり、実際にテレワークを試行し、多くの意見をいただいた。今後も市場の声に素直に耳を傾けてゆきたい。 ◆◆

■参考文献

1)「テレワーク白書 2007」，社団法人 日本テレワーク協会，2007年

●筆者紹介

三井靖博：Yasuhiro Mitsui. セキュリティ・アンド・モビリティカンパニー 新規プロダクトチーム チームマネージャ
作間哲夫：Tetsuo Sakuma. セキュリティ・アンド・モビリティカンパニー 新規プロダクトチーム
千村保文：Yasubumi Chimura. セキュリティ・アンド・モビリティカンパニー VP

*3)ユーザーが使うクライアント （コンピュータ）端末に必要最小限の処理をさせ、ほとんどの処理をサーバ側に集中させたシステム（広義のシンクライアント）。または、そのようなシステムで使われる機能を絞り込んだクライアント端末（狭義のシンクライアント）。