安心･安全な携帯電話の実現を目指して

小山　法孝　　三井　靖博

携帯電話の普及率が頭打ちとなり，市場では機能の充実，多様なサービスの提供に軸足が移りつつある。近年の携帯端末の機能充実とブロードバンド無線の発達によるモバイル環境の充実は，「いつでもどこでも，利用者の望む形で情報・サービスが提供され，快適な社会生活が実現する」，いわゆるユビキタス社会の到来が近いことを実感させる。企業においても，これらのインフラを最大限に活用し，企業活動に必要な情報，サービスを携帯端末で扱うなど，スピードと効率化による利益の最大化を目指す方向へ進んでいる。しかし，この流れは携帯電話による重要情報の扱いを増加させ，予想していなかった新たなセキュリティ事故を招く可能性を増大させることにもなっている。

本稿では，ユビキタス社会における最も重要な情報通信機器である携帯電話をターゲットとし，コンテキストアウェア技術を応用したユビキタスセキュリティ技術についてその概念とシステム構成を解説する。

携帯電話のセキュリティ脅威と現状対策

携帯電話の利用拡大に伴い，私的利用および業務利用の双方においてセキュリティ脅威が増しており，それらに対する対策がなされている。

具体的な脅威，対策としては，第一に，携帯電話の紛失とそれに伴う携帯電話内の電子価値（電子マネー，電子チケットまたは電子コンテンツなど）の紛失への対策としてストラップ（首から提げる）が利用されている。第二に，携帯電話内に保持された顧客情報や機密情報などの漏洩に対しては，特定の電話からダイヤルすることによる機能ロックやインターネットを利用した携帯電話内データ遠隔消去などのサービスが提供されている。第三に，携帯電話の不適切な利用（他者に見聞きされやすい場所での利用など）に対しては，現時点で，具体的対策は存在していない。

第二の脅威（携帯電話内の情報漏洩）に対する対策には遠隔ロック以外にもいくつか類似サービスが提供されているので，**表1**に示す。

表1　携帯電話のセキュリティサービス

機　能	具体的な実現方法の例
携帯電話紛失時の遠隔機能ロック	利用者があらかじめ登録した電話から、登録した方法で複数回ダイヤルして機能をロック
携帯電話紛失時の遠隔データ消去	利用者からの連絡により管理者が遠隔操作し消去
データ自動消去	保存期間を予め設定したり、一定時間アクセスが無いデータの自動消去
	アプリケーションと連動し各作業終了時に関連データ消去
遠隔データマネージメント	携帯とサーバ間でデータ同期や、サーバへのデータバックアップ
	遠隔からデータ同期、転送、消去
	利用者が専用ウェブサイトにアクセスし，データ消去指示

コンテキストアウェア技術とは

一般的に，ある対象のコンテキストとはその対象を取り巻く状況を意味する。具体的には，位置，時刻，温度／加速度などの物理状況，その対象が特定のサービスを利用中か否か，など非常に広範囲のものが含まれる。個々のコンテキストを組み合わせて，複合的なコンテキストを形成することもできる。たとえば，周囲音，振動，加速度を組み合わせて電車内にいるというコンテキストを推測できる。さらに，コンテキストは，現在の状況に限るものではなく，過去／現在／未来の状況およびその組み合わせとして考えることもできる。

次に，コンテキストアウェア技術とは，コンテキストに応じて最適なサービスを提供するための技術を意味する。例としては，現在の時刻と利用者の位置に即して最も効果的な広告を提供することなどが考えられる。さまざまな状況でコンピューティング環境を利用できるユビキタス社会では，状況に応じたサービス提供に対するニーズが高く，コンテキストアウェア技術はまさに時代にマッチしたものであるということができる。

コンテキストアウェア技術の研究は1980年代後半から行われているが，盛んになったのは最近の数年であり，欧米を中心に国内外の大学，研究機関，大企業で行われている。現時点では，ほとんどの研究は，コンテキストに

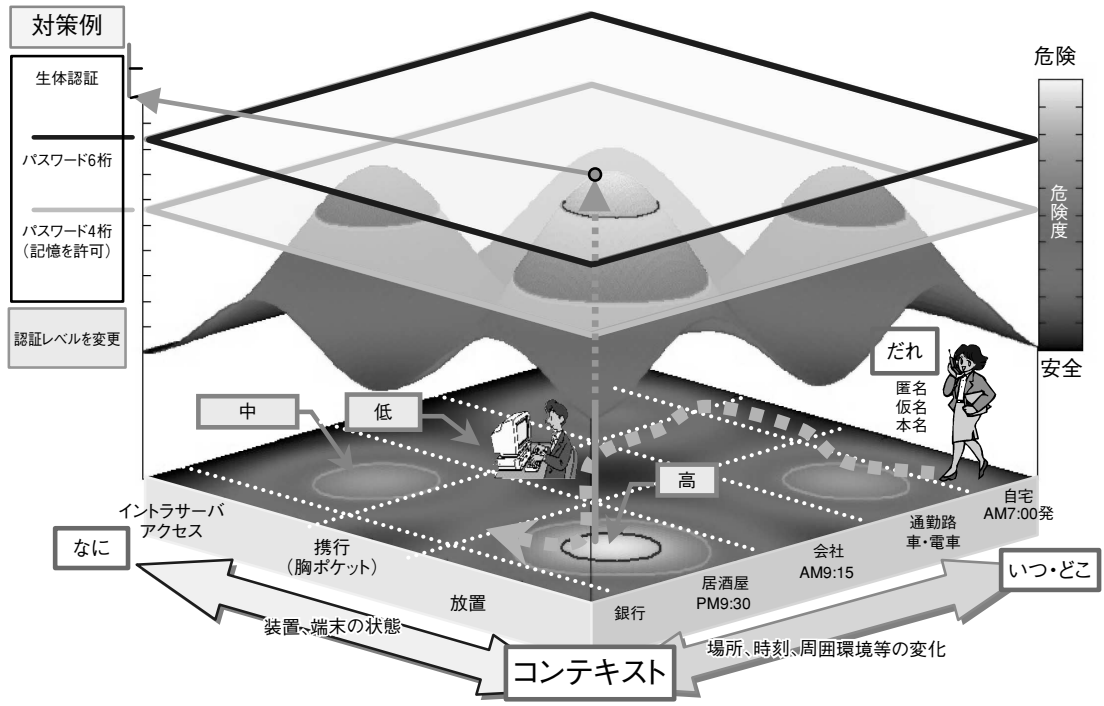

図1　ユビキタスセキュリティのイメージ

応じて利用者の利便性を向上させることを目的としたものである。

ユビキタスセキュリティとは

先に挙げた携帯電話のセキュリティ対策には次のような課題がある。

① 紛失対策が煩わしく業務効率が阻害される。
② 紛失に気がついてからでは遅く，また対処方法が複雑で時間がかかる（この間に事故が発生することも考えられる）。
③ 利用者の自覚頼りなのでうっかりミスは防ぎきれない。

そこで，筆者らはコンテキストアウェア技術を利用してこれらの課題を解決する技術の開発に取り組んでいる。具体的には，携帯電話内外の各種情報を利用して携帯電話の周囲の状況を検知し，脅威を認識して，自律的に予防・抑止を行ったり，サーバに通知したりするコンテキストアウェアなセキュリティ技術を開発しており，この技術を「ユビキタスセキュリティ技術」と呼んでいる。

図1に，ユビキタスセキュリティのイメージを示す。

本図は，携帯電話の状況を「場所，時刻，周囲環境等の変化」と「装置，端末の状態」の組み合わせで考えた場合に，利用者の行動に伴い危険度（右側縦軸）が変化することを示している。たとえば，利用者が携帯電話を，自宅や会社で身近に保持している時，または，胸ポケットなどに携行している時は安全であるが，通勤路，居酒屋，銀行などで放置されている場合には危険度が高いと考えられる。コンテキストアウェアなユビキタスセキュリティ技術では，この危険度の変化状況を自動的に認識し，その状況に応じた安全対策に自動的に切り替える（左側縦軸）。

次に，ユビキタスセキュリティを実現するために必要な機能について記述する。

ユビキタスセキュリティでは，携帯電話内外の各種情報からコンテキストを検知し，さらに自律的に脅威を認識する。まず，コンテキストの検知には，主に，携帯電話内蔵センサ，外部装置，または外部サービスを利用する。**表2**に，具体的にコンテキストを検知する方法の例を示す。

表2　コンテキスト検知方法の例

コンテキスト		検知方法
携帯が本人から離れた		本人が装着する別装置との距離
携帯使用中	誰かが手に持っている	静電容量、温度
	誰かが開いている	電気信号
	誰かが画面を見ている	カメラ画像、赤外線
	誰かが操作している	キー入力
	誰かが危険な操作をしている（例：パスワード探り）	操作パターン
危険度の高い場所（例：飲食店、電車内）		位置検知

このように検知したコンテキストおよびその組み合わせにより，携帯電話の脅威を認識することができる。たとえば，**表2**において，「携帯が本人から離れた」と「誰かが操作している」との組み合わせにより，本人以外の誰かが操作していることが検知でき，より確度の高い脅威を認識することができる。

携帯電話には，コンテキストおよびその組み合わせに応じて予防・抑止を実施するためのルールを保持する。コンテキストが発生，変化するごとにこのルールが参照され，ルールに応じてセキュリティ対策が実行される。

また，携帯電話で取得したコンテキストや事故情報を管理サーバに送信，蓄積し，後に解析，学習することにより，新たなルールの生成や既存ルールの改良を行い，逐次，ルールを最適化する。更新されたルールは，適時，管理サーバから携帯電話へ送信され，携帯電話内で更新される。このプロセスにより，将来，未知の新たな脅威に対しても防御を行えるようになるとともに，これまでのルールにも改良が重ねられていく。

図2に，ユビキタスセキュリティシステム概念を示す。

ユビキタスセキュリティシステムが機能することにより，以下の対策が自律的に実現できるようになる。

① 煩わしい対策なしに，簡単に携帯電話の紛失を抑止
② 紛失後，利用者が気づく前でも，携帯電話内情報の漏洩や携帯電話の悪用を抑止
③ 利用者の過失による携帯電話の不適切な利用を抑止

システム構成概要

図3に，本システムの構成を示す。

(1) 携帯電話の機能概要

携帯電話上ではコンテキスト管理ソフトが動作し，周辺装置と連携して，さまざまなコンテキストを検知，管理することができる。

- 内部センサを利用して，接触（タッチセンサ）や動き（加速度センサ）等を検知
- 外部センサとBluetooth等で無線通信することによる，さまざまな外部センサ値の取得または携帯電話との距離計測
- GPS等を利用した位置検知（外部サービス連携）
- センサNWと連携した各種状況モニタリング

(2) 管理サーバの機能概要

管理サーバは，主に，外部サービスとの連携，ルールの管理／送信のために利用する。

外部サービスとは，ASP（Application Service Provider）サービス等を意味し，たとえば，監視カメラによるモニターサービスが想定される。不審な映像を検知したというコンテキストを管理サーバで受け，携帯電話に提供することができる。

管理サーバではルールを管理し，適時携帯電話へ送信する。

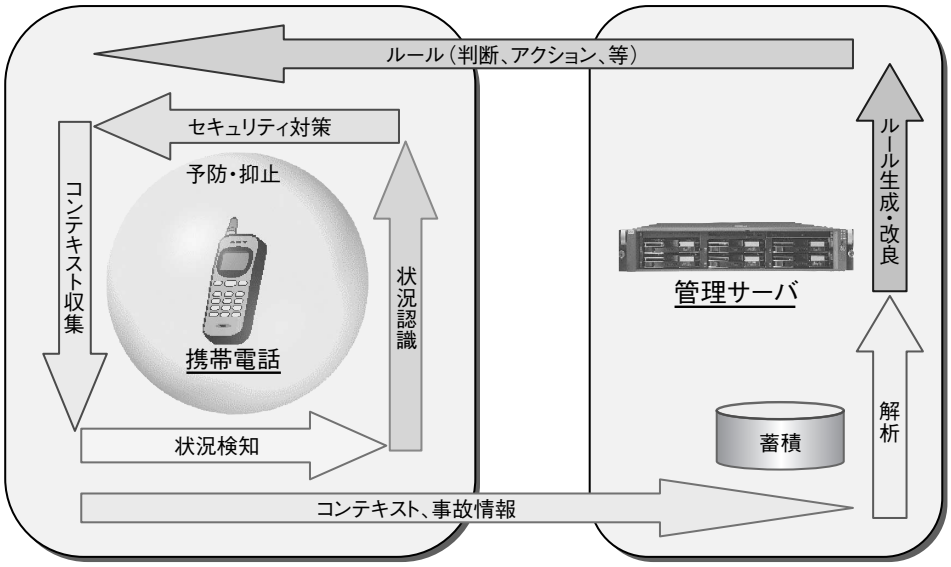

図2　ユビキタスセキュリティシステム

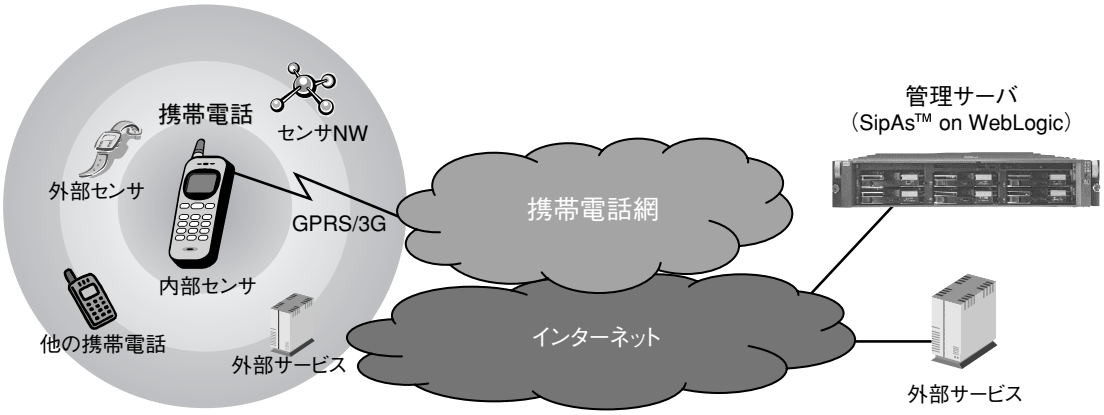

図3　システム構成

(3) ネットワークを介したコンテキスト共有

携帯電話，管理サーバ間は，携帯電話網およびインターネットを介して通信を行う。通信データは，ルールと各種コンテキストである。

携帯電話のコンテキストは他の携帯電話と共有することもできる。コンテキストを共有することにより，他の携帯電話のコンテキストを利用できるとともに，複数のコンテキストの組み合わせを利用することができる。コンテキスト共有機能は，インスタントメッセージ（IM）などで利用されるプレゼンス機能を自然に拡張したものと考えることもでき，将来的に，ユビキタスコンピューティング環境において広く利用できる可能性がある。

通信プロトコルには，リアルタイム性，双方向性を有し，国際標準の地位を確立しているSIP（Session Initiation Protocol）を使用する。SIPは，プレゼンス実装にも利用されており，コンテキスト共有にも親和性があるものと考える。管理サーバのプラットフォームとしては，沖電気が開発したSIP搭載アプリケーションサーバ「SipAs ™*1) on WebLogic*2)」を使用する。

ま と め

現在，重要情報を持ち歩く機会の多いビジネスマン向けに，紛失，情報漏洩，不適切な使用を自律的に抑止する安心・安全な携帯電話サービスを提供することを目標に開発を進めている。

具体的には，ユビキタスセキュリティ技術の有効性評価およびマーケティングのためのデモンストレーションシステムを構築中である。このシステムでは，**図2**に示した基本的な機能およびフローを実装する予定である。
将来的には，新たなセンサの追加や端末外のセンサの利用などのセンサの拡充，コンテキストや事故情報の解析およびルール生成や改良の自動化，を考えており，それによって，以下の目標を実現する予定である。

◆プロアクティブセキュリティ

一般に「問題が起きる前の対策コスト＜問題が起きた後の対策コスト」であり，脅威が発生する前の早い段階での予防が最も効果的である。過去の事故情報を基に，あらかじめコンテキスト認識結果から想定される脅威を予測し，自動的に相応のセキュリティ対策を実施する。

◆邪魔にならないユーザインタフェース

煩わしさのため使ってもらえない機能や狼少年的警告では意味がない。そのため，利便性，セキュリティ，およびプライバシー保護のすべての面で利用水準を満たすことが必要である。管理サーバにおいて，利用者からのフィードバックによる自動学習を行い，使い勝手の向上を図る。 ◆◆

●筆者紹介

小山法孝：Noritaka Koyama. 情報通信事業グループ インキュベーション本部 セキュリティソリューション開発部
三井靖博：Yasuhiro Mitsui. 情報通信事業グループ インキュベーション本部 セキュリティソリューション開発部

*1)SipAsは沖電気工業(株)の商標です。 *2)BEA WebLogicはBEA Systems, Inc.の登録商標です。