

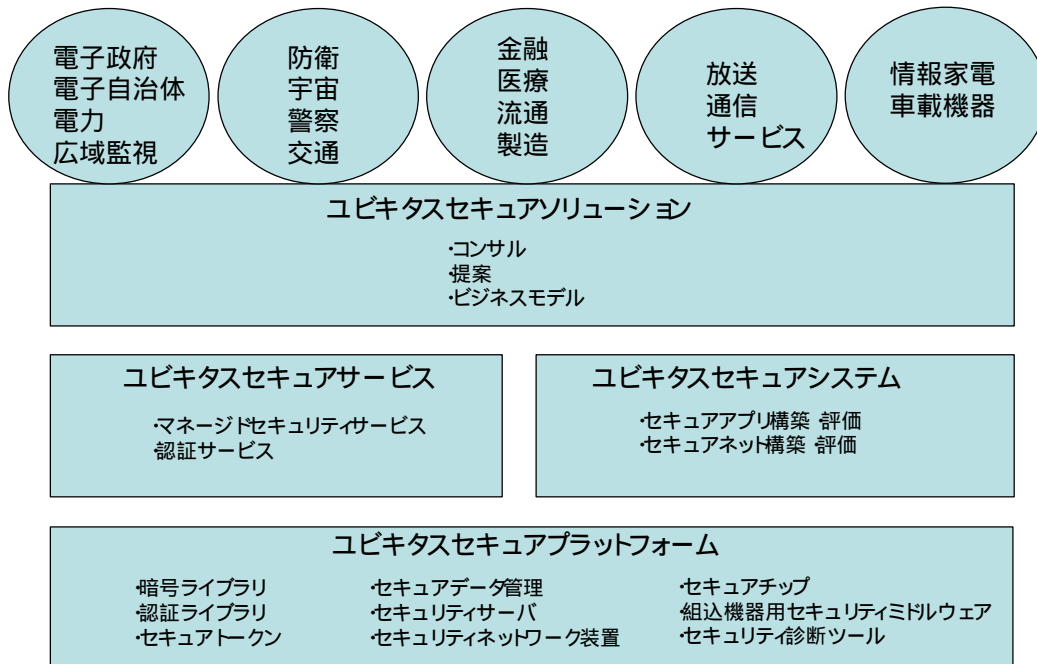
# ユビキタスセキュアソリューション

## 要旨

あらゆるものがネットワークに接続され、いつでも、どこでものユビキタスネットワーク社会が現実のものとなりつつある。ネットワーク化の進展により利便性が飛躍的に高まる一方で、セキュリティ上の課題が存在する。例えば、やりとりされる電子データは盗聴や改ざんの危険性がある。また、ネットワークの向こうにいる相手が、本当に自分の通信したい相手かどうか分からない。さらに、すべてのものがネットワークに接続されているがために、不正アクセスがあらゆるところで起こる可能性がある。こうしたセキュリティ上の不安に対して、これまでの技術的課題に加えてユビキタス環境で考慮すべき課題を解決する

必要がある。

“ユビキタスセキュアソリューション”では、世界トップレベルの当社の暗号技術を核とする“ユビキタスセキュアプラットフォーム”と、安全で安心なシステム構築とサービスを実現する“ユビキタスセキュアシステム”、“ユビキタスセキュアサービス”を提供する。“ユビキタスセキュアソリューション”により、電子政府や電子自治体、交通、防衛、宇宙、金融、などの社会重要インフラをより安全で強固なものとし、明るいセキュアネットワーク社会の進展に貢献する。



## ユビキタスセキュアソリューション

ユビキタスセキュアソリューションは、ユビキタスプラットフォームを利用して構築されるユビキタスセキュアシステム、ユビキタスセキュアサービスからなり、電子政府や電子自治体、防衛、宇宙、金融、医療といった重要社会インフラに対して安心と安全を提供する。

## 1. まえがき

インターネットの進展と、ネットワークのブロードバンド化、さらには携帯電話に見られるような、携帯情報端末の小型化や高度化、車載機器の高度化、情報家電のネットワーク化などにより、ユビキタスネットワーク社会が生まれてきている。さらに、無線タグを利用した流通管理やセンサーを利用した位置情報サービスなど、どこにでもコンピュータがあり、それらがネットワークにつながりいろいろな利便性を享受できる社会となってきた。こうしたユビキタスネットワーク社会は、利便性を大きくもたらす反面、なりすましや、不正アクセス、盗聴といった不安も存在する。このような不安を解決し、安全で安心なネットワーク社会を実現するためには、セキュリティが非常に重要となることはいうまでもない。

本稿では、2章でユビキタスネットワークを概観し、3章では、ユビキタスネットワークにおけるセキュリティの課題を整理する。4章では、当社の考えるユビキタスセキュアソリューションについて述べ、5章でまとめと今後の課題を述べる。

## 2. ユビキタスネットワーク

ユビキタスネットワークをモデル化したものが図1である。

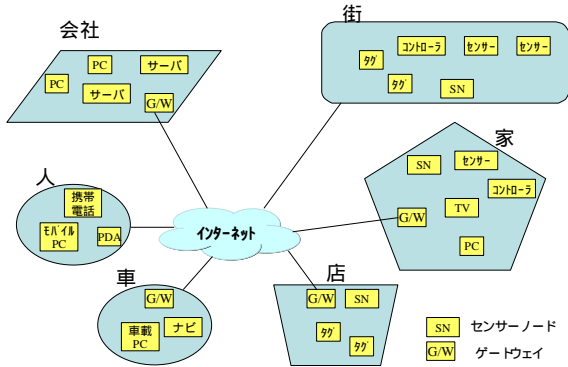


図1 ユビキタスネットワーク環境(一例)

オフィスや家庭でLANが構成され、ゲートウェイを介してインターネットに接続されている状況から、家庭やショップなどで、センサーやコントローラがいたるところに埋め込まれ、ネットワーク化されるようになる。そして、これまで計算機やネットワークが中心のシステムから、人を中心としたネットワークへと変化していく。ゲートウェイやセンサーノードは、IPアドレスによる接続である。しかしながら、センサーやコントローラ、無線タグは、独自のネットワークを構成することも考えられ、センサーノードが重要な役割を果たす。センサーノードと、タグ、センサー、コントローラ間は、IrDA (Infrared Direct

Access) やブルートゥース、DSRC (Dedicated Short Range Communication)、無線LANなど様々な通信方式を考慮する必要がある。

## 3. ユビキタスネットワークにおけるセキュリティの課題

2章で述べたユビキタスネットワークにおける主な脅威と対策を整理したものを図2に示す。

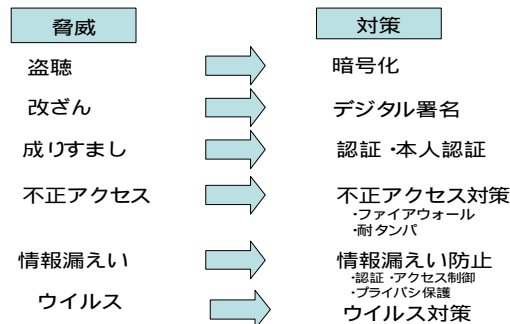


図2 脅威と対策

図2に示した表現は、一般的な情報セキュリティの脅威と対策であるが、ここでは、それぞれの対策に関連したユビキタスネットワーク環境での具体的な課題について述べる。

### (1) 暗号・認証

組込み機器への実装を考慮し、小型で高速なものが求められる。また、H/WやOSといったプラットフォームも多様化する。

### (2) 本人認証

本人認証は、IDとパスワードといった単純なものから、本人確認を重視した生体識別情報を利用した個人認証へと移行する。より確実な本人認証技術が必要となる。

### (3) 不正アクセス対策

携帯端末を介したアドホックネットワークにより、携帯端末を経由した不正アクセスや携帯端末自身への不正アクセスを防ぐためのコンパクトファイアウォール機能が必要となる。

端末やICカードに鍵情報など守るべきものが実装されるようになり、電力解析やタイミング解析などの攻撃からそれらを守るための耐タンバ技術が必要となる。

### (4) ウイルス対策

組込み機器等を考慮し、各種プラットフォームでのウイルス対策が必要となる。

### (5) 情報漏えい防止

いろいろな情報が集められるため、特に個人情報が漏洩する可能性があり、認証とアクセス制御により情報の漏えいを防止する必要がある。また、外部からの不正アクセスによる漏えいだけでなく、内部者による漏えいを防止する施策が重要となる。

### (6) リアルタイムセキュアプロトコル

セキュアネットワークという観点からは、IPsec

(Internet Protocol Security)やSSL(Secure Socket Layer)といったセキュアプロトコルのほかに、センサーノードとセンサーやコントローラ間のようにリアルタイム性が要求される通信でのセキュアプロトコルを開発する必要がある。

#### (7) プライバシ

位置情報や個人の購買の履歴など、あらゆるものが収集され分析されるようになると、プライバシーが侵害されることとなる。匿名性のあるサービスの実現や、収集情報の目的外使用への制限を加える仕組みなどが必要となる。

#### (8) 教育

管理者はもちろん、利用者も広くセキュリティの重要性について知る必要がある。そのため、対象者に応じたセキュリティ教育が必要になっている。

### 4. ユビキタスセキュアソリューション

ユビキタスセキュアソリューションは、電子政府や電子自治体、防衛、宇宙、金融、医療といった重要社会インフラに対して安心と安全を提供する。さらに、家庭や街、生活環境へと広がっていくユビキタスネットワーク環境のセキュリティ基盤を提供する。

そのために、3章で述べた課題を解決する技術要素を開発し、ユビキタスセキュアプラットフォームとして提供する。

さらに要旨の図に示すように、このユビキタスセキュアプラットフォームを利用して、ユビキタスセキュアシステムおよびユビキタスセキュアサービスを提供することによって、ユビキタスセキュアソリューションを実現する。

#### 4.1 ユビキタスセキュアプラットフォーム

ユビキタスセキュアプラットフォームは、暗号ライブラリ、セキュリティサーバといった、セキュアシステム構築およびセキュアサービスのための構成要素からなる。

以下に代表的な構成要素について述べる。

##### (1) 組込み向け暗号ライブラリ

MI<sup>STY</sup>(注)の技術を利用したKASUMIが、WCDMA(Wideband Code Division Multiple Access)の標準に採用されたことが示すように、当社は暗号アルゴリズムとその小型化、高速化実装に関しては世界トップレベルにある。各種の暗号アルゴリズム(乱数生成、共通鍵暗号、公開鍵暗号、ハッシュ関数)を組込みマイコン、Windows(注)、UNIX(注)等プラットフォーム上で提供する。

##### (2) 組込み向け認証ライブラリ

PKI(Public Key Infrastructure)を利用した認証システムは、多くの機能要素から構成されるが、必要な機能を選択的に組み合わせ可能とすることで、用途に応じたシ

ステムがコンパクトに実装可能である。組込み機器等はリソースに限りがあり、処理として負荷のかかる署名検証などをサーバ側で実行するためのプロトコルなどを実装する。

#### (3) セキュリティサーバ

組込み機器のセキュアライブラリとともにセキュアシステム構築に必須となるセキュリティサーバの代表的なものとして以下がある。

- (a) 認証サーバ：PKIに基づく各種認証書を発行する。
- (b) 署名検証サーバ：リソースに制限のある組込み機器上の署名検証処理との分担により署名の検証をおこなう。
- (c) タイムスタンプサーバ：電子データの生成時刻、更新時刻などの時刻を保証するためにタイムスタンプを発行する。
- (d) 統合認証サーバ：複数のサービスにそれぞれログインするのではなく一度のログインで複数のサービスを利用可能とする。
- (e) 公証サーバ：実際に電子データのやりとりが行われたことを、タイムスタンプなどを利用して証明する。

#### (4) セキュアデータ管理

主にサーバ側で、文書や監視情報ログなどのデータを蓄積・格納する場合の秘匿・アクセス管理・長期保存・情報漏洩防止・著作権管理などのセキュリティ機能を実現する。

#### (5) セキュリティネットワーク装置

ネットワークレベルのセキュリティを確保する不正アクセス監視装置やネットワーク暗号装置などがある。

#### (6) 組込み機器用セキュリティミドルウェア

組込み機器の遠隔保守・監視に必要な認証、アクセス制御、メッセージング、プログラムダウンロードなどの機能を実現する。

#### (7) 耐タンパセキュアボード

大量のセキュアトランザクションを処理するサーバにおいて、暗号処理の高速化および鍵等の秘密情報を物理的攻撃から守る耐タンパセキュアボードを利用する。

#### (8) セキュアトークン

ICカード、USB(Universal Serial Bus)トークンなどの鍵管理デバイス(他社製含む)と上記暗号・認証ライブラリとの連携機能を実現する。また、各種機器に搭載可能なセキュリティデバイス(鍵と暗号モジュールを耐タンパなハードウェアとして実現するもの)としても提供する。

### 4.2 ユビキタスセキュアシステム

ユビキタスセキュアプラットフォームを利用しシステム構築を実施する。ソリューション対応でいろいろなシステム構築が考えられる。セキュアネットワーク構築・評価技術、セキュアアプリケーション構築・評価技術が重要と

なる。

#### (1) セキュアネットワーク構築・評価技術

ファイアウォールの設定や不正アクセス監視装置の導入、あるいはVPN (Virtual Private Network) などネットワークセキュリティを考慮したネットワーク構築技術、およびネットワークのセキュリティを評価する技術を提供する。

#### (2) セキュアアプリケーション構築・評価技術

最近、Webアプリケーションの脆弱性を攻撃される場合が多くあり、アプリケーションそのものもセキュリティを考慮した設計、開発を実施する。また、開発物の脆弱性を評価する技術を提供する。

### 4.3 コビキタスセキュアサービス

ソリューション対応のサービスには、課金・決済サービスを始めとしていろいろなものが考えられるが、ここでは代表的なものとして、三菱電機情報ネットワーク株式会社 (MIND) が提供するマネージドセキュリティサービスと、ジャパンネット株式会社 (JapanNet) が提供する電子認証サービスについて述べる。

#### (1) マネージドセキュリティサービス

セキュリティは構築して完了ではなく、むしろ、スタートである。日々のセキュリティ監視、新たな脆弱性への対応、システム変更時のセキュリティチェックによって、セキュリティは維持される。MIND社は調査分析から、設計、導入、運用・監視及び評価というサイクルに対応したトータルなマネージドセキュリティサービスを提供している (図3)。米国 RedSiren Technologies 社 (旧 SRI コンサルティング社) との提携等で常に最新情報をサービスに反映し、24時間365日の統合管制センター (ICC: Integrated Control Center) をベースに絶え間ないサービスを提供している。なお、MINDではBS7799-2 (情報セキュリティ管理システム仕様 / 認証規格) の認証を取得し、情報セキュリティマネジメントシステムの確立・維持によって、信頼されるサービスを提供している。以下に代表的なサービスを紹介する。

##### (a) セキュリティ診断サービス

システムのセキュリティ状態を擬似攻撃によって診断する。三菱統合セキュリティ診断ツール (ISAT) を使用したクロスサイト・スクリプティングによる脆弱性チェックなど、Webアプリケーションまで踏み込んだ診断も行う。診断結果は検出した脆弱性の対策も提示している。

##### (b) セキュリティ教育・情報サービス

初心者から専門家までに対応した総合的な情報セキュリティのeラーニングサービス (InfoSecU) を用意している。また、日々公開されるセキュリティ情報を複

数の情報ソースからシステム管理者に代わって対象システム要件を踏まえて収集、分析し、その対処と合わせて提示している。

##### (c) 不正アクセス監視 / インシデントレスポンスサービス

もはや、ファイアウォールだけではセキュリティを維持できなくなっている。セキュリティホールへの攻撃を不正アクセス監視装置による24時間監視を行っている。万が一の緊急事態発生時には原因究明から対処までのインシデントレスポンスにも対応している。

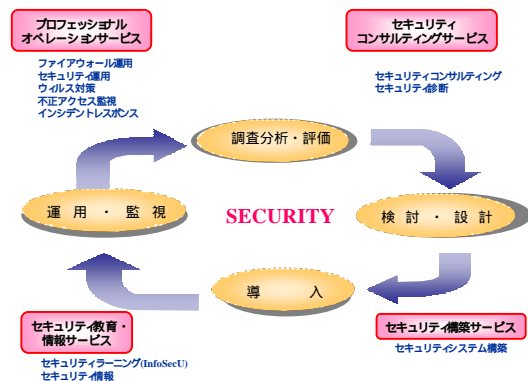


図3 MINDマネージドセキュリティサービス

#### (2) 電子認証サービス

JapanNetは、PKIに基づく証明書の発行サービスをはじめ電子認証システムの運営管理サービス (ハウジング、ホスティング) 等を提供している。証明書発行サービスについては、特定認証業務の公的認定を取得し、府省・自治体が実施する電子調達参加者向けの証明書発行も行なう。

### 5. むすび

セキュリティの製品やサービスを提供するにあたり、ISO15408 (セキュリティ評価基準) やBS7799-2の認証が重要となる。また、セキュリティは単に技術のみならず、法律・規制とも密接にからむため、社会の要請にあった仕組みとして提供していく必要がある。

コビキタスネットワーク社会におけるセキュリティ上の課題を整理し、我々の考えるコビキタスセキュアソリューションについて述べた。世界トップレベルにある暗号技術を核として、セキュアサービス、セキュアシステムを提供し、今後益々進展するコビキタスネットワーク社会に向けて、安全で安心なコビキタスセキュアソリューションを順次提供していく。

MISTYは、三菱電機の登録商標である。

Windowsは、米国 Microsoft Corp. の商標又は登録商標である。

UNIXは、米国 The Open Group Ltd. が独占的にライセンスしている登録商標である。