

無線 LAN が実現する社会

法学部政治経済学科 4 年 9920449 番

山本 彩

目次

1章 無線 LAN とは

1-1 LAN とは

- ・ LAN とは
- ・ 定義

1-2 無線 LAN とは

- ・ 有線 LAN から無線 LAN へ
- ・ 無線 LAN とは
- ・ 導入のメリット・デメリット

二章 無線 LAN の技術的側面

2-1 ISM バンド

2-2 スペクトラム拡散方式

2-3 伝送方式

2-4 セキュリティ

- ・ ESS-ID
- ・ MAC フィルタリング
- ・ WEP による暗号化

3章 Bluetooth

3-1 概要

- ・ Bluetooth とは
- ・ SGI

3-2 Bluetooth の特長

3-3 背景と目的

四章 Bluetooth の技術的側面

5-1 情報伝達のメカニズム

5-2 通信相手を見つけるしくみ

5-3 セキュリティ

5-4 待機モードと電力制御

5-5 互換性の保証

五章 Bluetooth の利用法

5-1 利用法

- ・ 既存のモバイル端末に対して Bluetooth を搭載する
- ・ 電子機器で既に使用されている接続を Bluetooth に置き換える
- ・ 今まで接続技術を利用していない電子機器に Bluetooth を採用する

5-2 Bluetooth のかかえる課題

六章 まとめ

要旨

1970年代には一般の人にとって遠い存在だったコンピュータは、今では一般家庭にも普及し身近な存在となっている。コンピュータは今後、様々な形をとって生活に浸透していくと思われる。超高齢社会にむけてコンピュータを意識せず使うためのネットワークとして、無線 LAN を中心に据えて考えていく。そのなかでも特に Bluetooth がノーマライゼーション社会の実現の補助的存在としてどのような役割を果たしていくのか、一般的な無線 LAN と比較しつつ検討する。

1章では LAN 全体の概要を検討する。LAN とは何か、無線 LAN とは何かについて述べる。無線 LAN の種類も比較しつつ述べる。2章では無線 LAN の技術的な側面を説明する。後々検討していく Bluetooth も無線 LAN 技術を基にしているが、Bluetooth の特長でもあるその他の技術に関しては後の章でより詳しく検討する。3章は、Bluetooth が開発された目的、背景や概要について述べ、4章では、Bluetooth 独自の技術について述べる。5章は、Bluetooth の具体的な利用法に関する構想と Bluetooth の抱えている課題を挙げ、6章では高齢社会がくるにあたり無線 LAN、とくに Bluetooth がその特徴を活かすことで得られる利便性について検討する。日本では超高齢社会を目前にして、高齢者が1人であっても、豊かで活力ある生活を送るための対策を必要とされている。便利なコンピュータやネットワークシステムの利用は、高齢者が自立的な生活を送るために有用である。

1章 無線 LAN とは

1章では LAN とはどのようなものを簡潔に検討する。LAN には有線 LAN と無線 LAN の2種類がある。本論では無線 LAN が中心だが、有線 LAN と比較することで無線 LAN の特徴を述べる。

LAN とは

LAN とは Local Area Network (ローカルエリアネットワーク) の頭文字をとった略語である。ローカル、つまり、1つのオフィス内やフロア内、家庭などのような比較的小さな範囲でのネットワークを LAN という。LAN は、ローカルエリアにおいて、ホストコンピュータやデータ端末、コンピュータなどを一定以上の通信速度でパケット化されたデータを高速に送受信する伝送路を指す。LAN が開発された目的として、接続された装置間で自由に、かつ容易にデータ通信を実現することがあった。

現在、LAN では Ethernet という通信方式の規格を主流として使用している。Ethernet により通信速度や通信に使用するケーブル、データのやりとりの方式が定められていて、現在国内外で使用されているものの多くはこの規格に準拠してい

る。

LAN の標準化を推進する組織の 1 つ、IEEE (Institute of Electrical Electronics Engineers : 米国電気電子技術者協会) では LAN を以下のように定義している。

「多くの独立した装置が、適度なデータ伝送速度の物理的伝送路を通じて、適当な距離内で直接通信可能なデータ通信システム」

つまり LAN とは「周辺機器が、10 ~ 100Mbps (一般的には 10BASE-T や 100BASE-TX を利用しているが 1Gbps の転送速度をもつ LAN もある) の伝送速度の有線または無線媒体を通じて、地理的に限られた範囲内で直接通信可能なデータ通信システム」である。

LAN を導入することによりデータ、周辺機器、アプリケーションソフトの共有、分散処理、電子メールのやりとり、他ネットワークとのやり取りが実現する。それにより業務ロス、経費、人件費の削減、グループウェア、イントラネットの実現、ネットワークにおける受発注が自動化するなどのメリットがある。企業では、経済性の工場、生産性の向上、対顧客サービスの工場、マーケットやシェアの拡大などのメリットがある。

LAN とよく比較される WAN (Wide Area Network) という言葉がある。LAN よりも広い範囲でのネットワークで LAN 同士を繋いだネットワークを指すこともある。

1-1 無線 LAN とは

・有線 LAN から無線 LAN へ

LAN を構築する場合、伝送媒体として同軸ケーブル、ツイストペアケーブル、光ファイバケーブルなどのケーブルを端末ごとに接続する必要がある。ケーブルは技術の発展とともに進化しているが、配線スペースをとること、大規模な敷設の場合大きなコストになること、オフィスでは配置換えで机を動かした際もケーブルの再敷設といった手間と時間がかかること、家庭内ではケーブルの敷設が困難などの問題点がある。

この問題を克服するために登場したのが無線 LAN である。通常の LAN が物理的伝送媒体を使用するのに対して、無線 LAN では電波や赤外線などを用いてデータを伝送する。無線 LAN は IEEE802.11 によって標準化が進められている。では、無線 LAN とはどのようなものだろうか。

・無線 LAN とは

有線ケーブルなどを使わずに電波や光 (赤外線やレーザー) などの無線で通信を行う LAN をさす。アクセス・ポイントという小型の無線装置から数十メートルの範囲で、無線 LAN カードの付いたパソコンを利用して高速にネット接続することが

できる。現在発売されている無線 LAN の製品のほとんどは、IEEE802.11b か IEEE802.11a のどちらかの規格に対応している。

無線 LAN には、媒体として電波、赤外線を使用するものがある。

電波方式は 2 章で詳しく述べる ISM バンド (2.4GHz 帯) という電波免許不要な周波数帯の電波を使用し、IEEE802.11-1997 でも採用された MAC 層、物理層が無線 LAN 専用の方式で、1Mbps ~ 2Mbps 程度の転送スピードが主流になっている。なお、本論では電波方式を主に取り扱う。

赤外線方式は IrDA(Infrared Data Association) と呼ばれ、従来のイーサネット等で結ばれたネットワークの一部を赤外線に置き換えたものである。一般的な方式は 10M イーサネットの先にメディア変換アダプタ (リピーター) をつなぎ、光無線 HUB と通信する方式である。赤外線方式は赤外線の直射光か反射光が届く範囲出ししか使用できないため、設置場所に制約がある。伝送距離は 10m 以下だが、通信している相手が目に見えることと、赤外線が一方向性という特徴をもつこともあり、セキュリティに強いといわれている。また転送スピードが速い (16Mbps) ため条件さえ満たせば有線 LAN 同等の通信が可能という長所がある。さらに電波を使わないため、病院、医療機関で電波の影響を避けたい場所等に最適である。

無線 LAN 導入のメリット・デメリット

無線 LAN を導入すると、有線 LAN で言われているメリットを無線 LAN でもさらに得ることができる。

(1) モバイル性を最大限に発揮できる。無線 LAN は見通しの良いスペースであれば、実質的に 60m の距離があっても通信が可能である。家庭や小規模の事務所の中であれば、自由に移動しながらデータ通信ができ、ノートパソコンの存在価値は大いに高くなる。(2) ケーブルのトラブルを回避できる。有線 LAN では起こり得るケーブルの断線、アダプタからの脱落、接続先の誤り、ケーブル極性の取り違いなどは、無線 LAN では、基本的には発生しない。有線 LAN では設置するためには大掛かりな配線工事が必要だが、無線 LAN では、比較的短期間、低コストでネットワークの構築が可能となる。(3) インターネット接続を共有できる。ブロードバンド時代が到来し、パソコンをブロードバンドルータに複数代接続し、インターネット接続を共有することができる。しかし、ダイヤルアップルータに全てのパソコンをケーブル接続するのは見栄えも良くない上に機動性もない。ダイヤルアップルータとパソコンに無線 LAN アダプタを装着すれば、一人ひとりがそれぞれの部屋から同時にアクセスすることが可能となる。そのほかにもデータ、ドライブ、プリンタなどが共有できる。

では、次にデメリットだが、無線 LAN では有線 LAN とは異なり、特定の周波数帯域を利用するため、以下のようなデメリットがある。

(1) 電波が届きにくい所では通信が安定しない。有線 LAN はケーブルを使ってデータをやりとりするため安定した通信速度を保つ。対して無線 LAN は電波の届きにくいところでは通信速度が安定しない。そのため、常に電波状態が安定しているところを探して通信しなければならない。(2) セキュリティ対策が必要。無線 LAN 機器から発せられる電波は、見通しの良い所では 100 m 近くも電波が飛ぶ。電波の多方向性という特性上、相手の故意、故意でないに関わらず盗聴される危険性が極めて高い。そのため暗号化などで盗聴されないよう様々なセキュリティ対策の必要がある。盗聴対策だけではなく、OS やルータなどにもセキュリティ設定を施すなどの対策も必要である。これらは有線 LAN でも同じだが、無線 LAN ではより強化する必要がある。なお、セキュリティ技術に関しては後の章で詳しく述べる。(3) 隣り合うチャンネルでは電波干渉が起こる。無線 LAN が使用する ISM バンドでは、チャンネルは全部で 14 あるが、隣接する番号のチャンネルは周波数帯域が重なる。そのため、同じ場所で通信すると 2 つのチャンネルが干渉しあい混信する。同じ場所で無線 LAN を設定する場合にはチャンネルが干渉し合わないよう、できるだけ離れたチャンネル番号を設定する必要がある。(4) 無線 LAN は有線 LAN に比べると通信速度が遅い。基幹系の有線 LAN では実験段階では 10Gbps の通信速度も確認されている。無線 LAN も「光無線 LAN」が新たに誕生し、100Mbps、300Mbps と標準規格のネットワークを利用できるようになったが、今後格差が広がるものと考えられる。

有線 LAN と無線 LAN の違いを比較すると以下の表になる。

	有線 LAN	無線 LAN
標準規格	IEEE 802	IEEE 802.11b
伝送媒体	ケーブル	電波、赤外線等
通信プロトコル	TCP/IP, NetBUEI, IPS/SPX	TCP/IP, NetBUEI, IPS/SPX
伝送距離	100m (ハブまでの距離)	60m前後 (屋外見通し良) 30m前後 (屋内)
通信速度	最大 100Mbps	最大 11Mbps
通信品質	安定	電波状態により変化
Windows/Mac の混在	可能	可能
無線/有線間の相互通信	可能	可能
一台あたりのコスト	3000円程度	1万 5000円程度

(表 1)

2 章 無線 LAN の技術的側面

2 章からは、電波方式を採用する無線 LAN について述べていく。この章では無線 LAN に関する技術について述べる。

2-1 ISM バンド

無線 LAN は、その形態によって使用できる周波数帯域が限定されている。ISM バンド (Industrial, Scientific and Medical Band) は、産業科学医療用バンドとも呼ばれ、電子レンジや LSI 製造装置などの産業用装置や科学用装置、あるいは医療メスなどの医療機器での仕様が定められている周波数帯でもある。(図 1)

IEEE802.11 の無線 LAN などで使用されている周波数帯は、900MHz 帯、2.4GHz 帯、5.7GHz 帯の周波数帯域で、実現できる伝送速度は数 Mbps ~ 数十 Mbps である。無線 LAN 用の周波数として、1992 年 12 月の電波法に基づく無線設備規則などの郵政省令の公布・施行に伴い整備された。また、1999 年 12 月には、米国等との周波数の共通化を図るため、第 2 世代無線 LAN システム用に通信帯域幅の拡大 (26MHz → 83.5MHz) などの規制緩和が行なわれた。2.4 GHz 帯では雨・雪の影響はほとんどなく、降雨による減衰は無視できる。また、雷の影響については、避雷器により装置破壊を回避する。また、人体への影響を考慮すると、PHS と同じ小電力システムのため、基本的に人体への影響は無い。医療機器の影響は医療機器への影響は無視できるが、レーザメスやハイパーサーミア等の医療用 ISM 機器からの干渉の影響は受ける。通信チャンネルの切替え等により対処可能である。



(図 1)

無線 LAN では、他の機器からの電波干渉を回避するため、スペクトル拡散という技術を使用する。現在の無線 LAN 機器は、スペクトラム拡散(SS: Spread Spectrum)技術が導入されたことにより、通信がより安全に、高速に行えるように

なった。スペクトラム拡散は、符号分割多元接続 (CDMA: Code Division Multiple Access) を実現するための技術であり、情報信号を信号の持つ周波数帯域よりもはるかに広げて伝送する通信方式である。スペクトラム拡散には、信号に疑似雑音信号(PN: Pseudo noise)を掛け合わせて信号を拡散する直接拡散方式 (DSSS: Direct Sequence Spread Spectrum)と、キャリアの周波数を広い範囲で変化させる周波数ホッピング方式 (FHSS: Frequency Hopping Spread Spectrum)の 2 種類がある。

2-2 スペクトラム拡散方式

スペクトラム拡散方式とは、周波数、時間、コード体系、その他をベースに、利用可能な周波数帯域を分割する技術である。送信メッセージはパケットに分けられ、分割された周波数帯域に拡散して伝送される。拡散された信号は普通に聞くとホワイトノイズと変わらない。これを受信側は同じルールを使って再構築しなければならない。ルールが分からない限り第三者が信号を解読することは不可能なため傍受しにくい通信方法と言われている。このスペクトラム分散には DSSS と FHSS という 2 種類がある。

DSSS 方式 (直接拡散方式) は BPSK(Binary Phase Shift Keying) という位相変調した後 PN コードと呼ばれる特殊な拡散符号を掛け算することで、周波数スペクトラムを広帯域に拡散して送信する方式である。Bluetooth が採用する周波数分割スペクトラム拡散 (周波数ホッピング) 方式は周波数帯をいくつかのチャンネルに分割する。メッセージのパケットが選択されたチャンネル上を転送されると、電波は次のパケットを転送する別のチャンネルを選択する。(新しい周波数へのホッピング) このプロセスが繰り返され、メッセージは利用可能な周波数帯に拡散して転送される仕組みである。スペクトラム拡散を利用する技術は、周波数ホッピングのパターンを確立する手法をそれぞれ独自に定義している。メッセージの受信側はホッピング・パターンを認識し、正しいチャンネルでパケットを受け取り、メッセージを組み立てなくてはならない。このプロセスは周波数ホッピング・スペクトラム拡散 (FHSS) と呼ばれる。

FHSS は単一の周波数による通信と比較すると複雑だが、それを上回るメリットがある。まず、全ての無線が周波数を高速かつ無作為、または擬似的無作為にホップするため、RF 干渉が減少する。特定の周波数帯を利用するデバイスが全て FHSS を採用していれば、同一周波数上の伝送が衝突して起こる干渉は、それぞれの無線が単一のチャンネルを長時間利用した場合に比べて少なくなる。たとえ衝突が発生しても、パケットが一つ失われるだけであり、そのパケットも直ちに別の周波数で再転送されるため、通信に及ぼす影響は小さい。次に、FHSS ではメッセージの全てのパケットを受信して再構築できるのは、周波数のホッピング・パターンを知っている受信機だけであるため、一定のレベルのセキュリティを保障できる。スペクト

ラムのホッピング・パターンは様々な方法で決定されるので、未知のパターンを推測、追跡することは難しい。

DSSS と FHSS の特徴

- ・ FHSS は DSSS よりノイズに強い
- ・ FHSS は DSSS より消費電力が少ない
- ・ FHSS は拡張性に優れている
- ・ FHSS は電波干渉に強い
- ・ FHSS は設定チャンネル数が多い
- ・ DSSS は FHSS よりカバーエリアが広い
- ・ DSSS は FHSS よりスループットが高い
- ・ DSSS は通信速度が速い

2-3 伝送方式

IEEE802.11 では、データリンク層の下位副層である MAC に、無線 LAN のアクセス制御方式として CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance : 衝突回避型搬送波感知多重アクセス方式) を使用している。

対する Ethernet による有線 LAN の場合、CSMA/CD (Carrier Sense Multiple Access with Collision Detection : 衝突検出型搬送波検知多重方式) を用いる。有線 LAN と無線 LAN の伝送方式の比較をする。

有線 LAN の CSMA/CD では、データを送信する端末は、他の端末が送信しているか否かを確認するために、データ送信前に搬送波検知 (Carrier Sense) を行う。他の端末がデータを送信していなかった場合にデータ送信を開始するが、このデータは線を共有している (Multiple Access) すべての端末に送られてしまう。パケットを受け取った全ての端末は、フレームヘッダ内のあて先アドレスを確認し、アドレスが違う場合にはフレームを破棄する。もし、送信時に他の端末が同時に送信を開始した場合、伝送路でデータの衝突 (Collision) が発生する。衝突を検知した端末は送信を中止し、一定の時間待った後にデータを再送するという手続きをふむ。この機能を衝突検出 (Collision Detection) という。この伝送方式により、複数の端末で伝送路を共有することが可能となっている。

無線 LAN の CSMA/CA は、IEEE802.3 の CSMA/CD によく似た方式だが、衝突の検出が出来ないため、送信前に送信中の端末がないかを確認し、(Carrier Sense) さらに自分宛に送信されたパケットがないか確認する (Multiple Access)。衝突の可能性がない場合においてデータを送信する。もし、衝突が起こった場合には、送信待機 (Collision Avoidance) となる。次に再送するにはランダムに割り当てられた時間待機し、送信を開始する。衝突が起きた場合に、エラー回復を行えないため、上層位で再送を行う仕組みをとっている。

CSMA/CA は CSMA/CD との親和性を重視した方法で、有線 LAN との併用が可能となっている。

2-4 セキュリティ

無線通信の性質上、無関係の第三者の元に通信（電波）が到達することは阻止できないので、何のセキュリティ対策も施していない無線 LAN を運用していると、以下の 2 つの問題が発生することになる。一つめは、外部から無線 LAN に不正侵入される危険性がある。物理的にケーブルを接続しない限り通信ができない有線 LAN と異なり、無線 LAN では電波による交信が可能な範囲なら、屋外からでも接続できる。そのため、オフィスや家庭の外から勝手に無線 LAN に接続し、LAN 上のコンピュータに不正侵入を試みられる危険性が生じる。場合によっては、外部からワームなどによるアタックを受ける事態も考えられる。二つめは通信内容が第三者に漏洩する危険性が考えられる。無線 LAN のクライアントから放射される電波を傍受する、あるいは無線 LAN に接続して通信内容をモニターする、といった方法で、無線 LAN を介してやりとりされている内容が第三者に漏えいする危険性がある。

こうした事態に対処するため、次のようなセキュリティ対策が用意されている。

- ・ ESS-ID の設定により、ESS-ID を知らないユーザの接続を阻止する
- ・ アクセス・ポイントに MAC アドレスを登録し、登録したもの以外の接続を拒否する（特定の MAC アドレスの接続を明示的に拒否できるものもある）
- ・ 無線を通じてやりとりされる内容を暗号化し、傍受されても内容が分からないようにする（WEP 暗号化）

ESS-ID

ESS-ID（Enhanced Service Set ID）とは、IEEE802.11 で固定した相手先との接続を実現するための、識別データである。アクセス・ポイントが認証するフレーズをあらかじめ登録しておく方式で、無線 LAN を構築するためには最低限の設定である。使用者の負担は大きくなるが、フレーズを定期的に変えることでセキュリティレベルを高めることができる。

ESS-ID が一致している端末同士が無線 LAN 通信できるというシステムなので、無線通信を行いたい端末同士が同じ ESS-ID を設定することにより、セキュリティが確保される。

MAC アドレスフィルタリング

MAC アドレス（Media Access Control Address）は各ネットワークカード（NIC：Network Interface Card と呼ばれることもある）ごとに割り当てられる固有のアドレスで、世界中でただ 1 つの物理アドレスといえる。アクセス・ポイント（AP）に端末の MAC アドレスを登録し、登録していない端末からの通信についてはフィルタリングをする機能が、ほとんどの製品に備わっている。

イーサネットの MAC アドレスは 48bit (6bytes) であり、このうち先頭の 3bytes には、IEEE が管理しているネットワーク機器のベンダコード (メーカーを一意に識別できるコード) が割り当てられ、残り 3bytes には、ネットワークベンダが自社製品にそれぞれ固有の番号を割り当てる。このためある製品に割り当てられた MAC アドレスは、世界にただ 1 つしかなく、同じ MAC アドレスを持つ製品は存在しないことが保証されている。これを AP に登録しておけば、登録していない端末が AP を利用して外部のネットワークにアクセスするのを防ぐことができるようになる。

無線 LAN の機器は、すべての固有の MAC アドレスを持っているので、これを利用して特定の MAC アドレスを持つ聞き以外の無線接続を受け付けないように設定をおこなう。ただし、この機能は不正に AP へ侵入することを防ぐだけで、第三者の傍受 (パケットの受信) を防ぐことは出来ない。アクセス可能な MAC アドレスを設定することで、クライアントを制限し、許可を受けたクライアントからの通信しか受け取れないように制限する。

WEP

WEP (Wire Equivalent Privacy) とは直訳すると「有線ネットワークと同等のプライバシー機能」であり、IEEE802.11b や IEEE802.11a 無線 LAN で使用される暗号化仕様の総称である。実際にデータを暗号化するにはアメリカ RSA Security 社が開発した共有鍵暗号「RC4」と組み合わせて WEP は構成されている。WEP はデータリンク層で暗号化を行うため上位プロトコルに関係なく暗号化される。

WEP を使用するには、ユーザが暗号化の「キー (鍵)」となる ASCII 文字列を決めて、それをクライアントとアクセス・ポイントの双方に設定する必要がある。この ASCII 文字列は、長さが 5bytes の場合と 13bytes の場合があり、後者の方が「キー長」が長くなることから、秘匿性が向上する。実際に暗号化を行うには、この ASCII 文字列を 16 進数に変換したうえで、さらに 24bit の長さを持つ「IV (Initialization Vector、初期化ベクタ)」を組み合わせて、64bit、あるいは 128bit 長とした値を使う。なお、このとき 16 進数に付加される IV の値は、WEP を用いて通信する相手側にも送信される。

WEP が使用している RC4 は、「キー」の内容がランダムであることを前提にして、「キー」から乱数列を作成し、それと「明文」を XOR 演算した結果を「暗号文」として取り扱うストリーム暗号である。生成された「暗号文」に、暗号化の際に用いたのと同じ「キー」を使ってもう一度 XOR 演算すると、元の「明文」が取り出されるという原理を利用している。

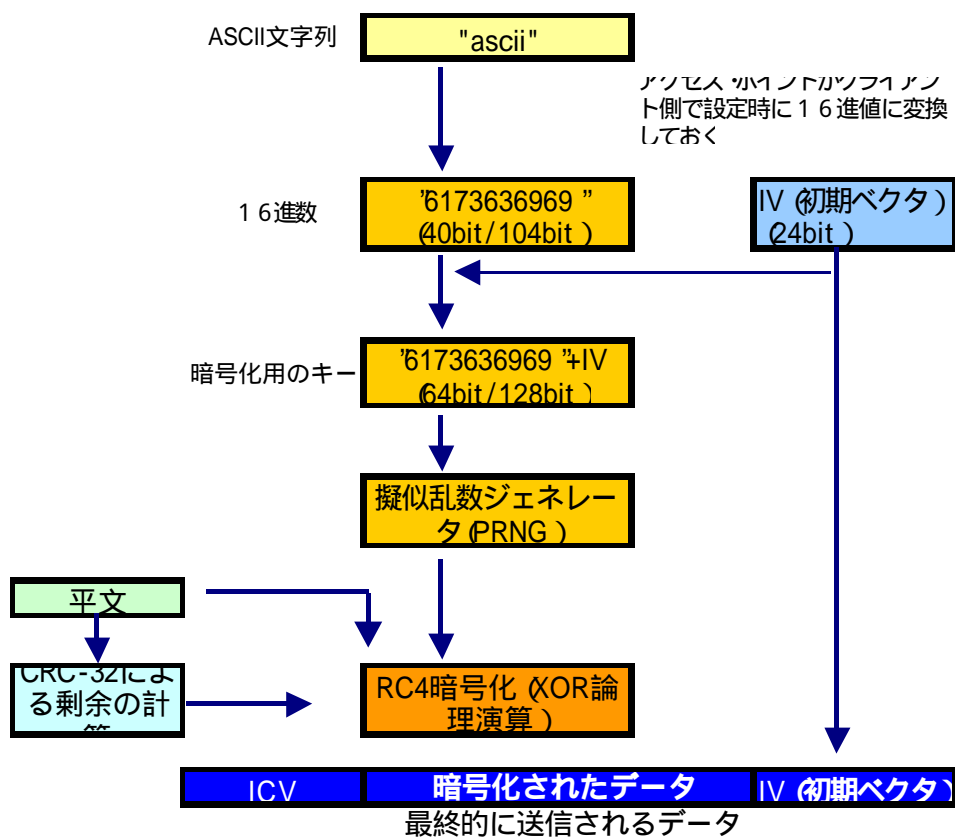
WEP の場合、ASCII 文字列から生成される 16 進値と IV を組み合わせて生成された「キー」を「擬似乱数ジェネレータ (PRNG: Pseudo-Random Number Generator)」に通して、そこから出力される乱数と、LAN でやりとりされるネットワーク・フレー

ムの内容を XOR 演算している。その結果と、「キー」を生成するために使用した IV の値を、電波に乗せて相手に送信している。

このとき、通信開始時の認証手段として、「CHAP (Challenge Handshake Authentication Protocol) 認証」を使用し、お互いが使用している「キー」が同じであるかどうかを確認している。CHAP 認証とはチャレンジ&レスポンス認証といい、お互いが持っている「パスワード」や「キー」などのデータを、平文のまま通信路に流すことなく、それらが同一であるかどうかを相互に確認する認証方法の1つで、PPP 通信などでも使用されている。システムにログインや、リソースにアクセスするためには、パスワードやキーとなる文字列を相手に送信して認証してもらう必要があるが (WEP 暗号化の場合は、お互いの持つ「キー」が同一かどうかを確認し、そうでなければ通信を行わないようになっている)、このときに重要なデータを平文のまま送信してしまえば、第三者にデータが漏えいする可能性がある。そこで認証サーバ側では「チャレンジ値」というランダムな値を送信し、受信したクライアント側ではその値を自分の持つキーで暗号化して、その結果をサーバ側に返信する。サーバ側でも、同様に送信したチャレンジ値を自分の持つキーで暗号化して、それを受信した暗号化の結果と比較するか、もしくは自分のキーで復号化して、送信した値と同じかどうかを調べる。もし同一であれば、両者の持つキーは一致しているとみなされ、認証の成功をクライアント側に返す。また、送信されるデータの整合性チェックのため、送信時には「IA (Integrity Algorithm、一貫性アルゴリズム)」によって CRC-32 の値が計算される。この値のことを「ICV (Integrity Check Value、一貫性検査値)」といい、IV や、暗号化されたデータと共に送信され、受信側でエラー検出に利用される。

WEP による暗号化のプロセス

ASCII 文字列を 16 進数値に変換して IV (Initialization Vector、初期化ベクタ) と混合し、暗号化のキーとする。ここでは例として“ascii”という文字列をキーにしている。これを基にして IV と混合して擬似乱数列を発生させ、元の平文データ (ネットワーク・フレームのデータ) と XOR 演算して暗号化を行う。送信フレームには、暗号化されたデータのほかに検査用の ICV 値 ICV (Integrity Check Value、一貫性検査値) と IV 値も含まれる。受信側では、IV から同様に擬似乱数列を生成し、暗号化されたデータと XOR 演算して元の平文データと ICV を取り出す。



(図 2)

WEP による暗号化の手順

一方受信側では、自分が保持している 40bit のキー文字列と、暗号化されたデータと共に受信した IV の内容を同様に擬似乱数ジェネレータに入力し、生成された乱数と受信したデータを XOR 演算することで元のデータ (平文データと ICV) を取り出している。こうした動作原理から、WEP 暗号化の安全性は、ユーザがキーとして設定する ASCII 文字列の内容に大きく依存している。

3 章 Bluetooth

無線 LAN は日常生活からかけ離れた存在ではない。ラジオやテレビなどはもっとも身近な無線通信である。他にも携帯、コードレスフォン、テレビのリモコン、車庫のゲート、自動車の自動ロックなども無線通信を利用している。これらは生活を大変便利にした。

近年、新しい無線技術として Bluetooth という言葉をよく耳にする。Bluetooth を搭載した携帯電話やパソコンが注目されているが、既存の無線と Bluetooth では、何が違うのだろうか。Bluetooth が実現する新しい技術や社会にはどのようなことが考えられるのか、検討する。

3-1 概要

Bluetooth とは

Bluetooth とは、プロモータと呼ばれる創立メンバー（エリクソン・ノキア・IBM・インテル・東芝）が結成した業界団体 Bluetooth SIG(Special Interest Group) によって策定された短距離無線通信規格の総称である。Bluetooth の特徴を挙げていくと、(1)近距離無線通信である：コンピュータや通信デバイスの多くは近距離のデジタル通信技術で結ばれているが、多くがケーブルを利用して行なわれている。ケーブルを接続するためのコネクタ類は大きさやピンの数が異なるなど、形状はさまざまであり、ケーブル接続はやっかいなものとなっている。Bluetooth 技術を利用すれば、これらのデバイスはケーブルを用いることなく、単一の無線インターフェイス上で電波を介してデータをやり取りできる。Bluetooth は近距離用（通常 10m 以下）に設計されている。この範囲を、LAN や WAN に対して PAN(Personal Area Network) と呼ぶ。近距離に通信を限定することで消費電力が抑えられ、かつ、部品や開発のコスト化が図られる。これにより、部品や設計の単純な構造が可能となった。それにより、さらなるコスト削減や小型化に寄与することになり、バッテリー駆動が一般的な小型のポータブル・デバイスなどに最適である。(2)柔軟なネットワークの構築：5 章で詳しく述べるが、Bluetooth では一対一接続以外にも簡易ネットワークを構築できる。これはピコネットとよばれ、一つの島を形成しているような形になる。ピコネット間についても柔軟に移動可能なため、分散協調といったより発展性のある応用が考えられる。(3)音声とデータ通信：Bluetooth 技術では音声とデータを同様に扱うことが見込まれている。音声はデジタル形式で転送および格納されるのが一般的である。携帯電話などの音声アプリケーションは、情報へのアクセスやブラウジングにも利用されている。コンピュータは音声認識で音声による制御が可能となっている。無線通信技術の中には、音声以外に伝送できないものや、データトラフィックしか処理できないものがある。しかし、Bluetooth

は音声とデータの双方に対応し、どちらのタイプのコンテンツでもやり取り可能で、これら二つの世界を統合する画期的な技術である。(4)オープン仕様：4-2 で詳細を述べるが、Bluetooth SIG は設立当初から Bluetooth の広い普及のためにオープン仕様になっている。5) 世界中どこでも使える：電気通信産業は、政府の定める規制に適合しなければならず、規格も国によって異なる。無線通信についても無線周波数帯の利用は厳密な出力制限が課せられた免許制になっているのが一般的である。その中に無線周波数帯には免許なしでも利用できるバンドがある。ISM バンドである。Bluetooth が世界中で免許が不要な ISM 帯を利用することによって、Bluetooth 無線通信を搭載したデバイスは世界中どこでもだれでも自由に利用することが可能となっている。

Bluetooth SIG

前述した Bluetooth SIG だが、1998 年、携帯電話の業界をリードするエリクソンとノキア、パソコン業界の中でも特にノートパソコンをリードする IBM と東芝、そしてパソコン用プロセッサの業界をリードするインテルの 5 社から結成されている。Bluetooth SIG は、ワイヤレス接続技術である Bluetooth の技術開発を行い、その普及促進および管理などを行う企業・団体のグループである。SIG では法人という形態をとらずに運営が行なわれているため、運営に関わる資金や労力は、Bluetooth SIG を設立した 5 社がそれぞれ負担することになっている。

このように技術開発・普及促進・技術管理・財政的な面で Bluetooth SIG の活動を支援していく中心的役割を担う企業をプロモータという。Bluetooth SIG の設立当時 5 社だったのが、現在ではモトローラ・ルーセント・3Com・マイクロソフトが加わり 9 社で Bluetooth SIG を運営している。

Bluetooth SIG は Bluetooth をグローバル標準にすることを掲げている。そのために最も必要とされる制度的な方針は、技術仕様をオープンに取り扱うことである。これまで様々な業界や企業が接続技術を開発してきたが、労力と時間と費用を費やして開発した技術を無償でオープンにするという考えはなかった。しかし、業界間の差なくグローバルな展開を目標とする Bluetooth SIG にとっては技術仕様を無償でオープンにすることは不可欠な方針といえる。

Bluetooth SIG のアダプタになるには、アダプタに関する同意書に調印すれば比較的簡単にメンバーになれる。(その際に費用はかからず、その後も年会費などの費用の義務も負わない。財政的な支援はすべてプロモータによってまかなわれる。) アダプタに関する同意書の概要には「Bluetooth 技術企画の中に、アダプタとなる企業・団体の側で所有する知的財産権が存在する場合には、それを利用する権利を Bluetooth SIG の全メンバーに対して無償で提供する」とある。現在までに Bluetooth の技術開発に際して数々の知的財産が生み出されているが、これによ

って Bluetooth の技術規格に準拠した製品の開発や製造を行う権利が無償で得られる仕組みになっている。さらに、製品が Bluetooth の技術規格に準拠しているかを試験し、この試験に合格した製品に対しては Bluetooth ロゴが発行される。ロゴが製品に明示されることで初めて他の Bluetooth 製品との相互接続を保障することとなる。製品やサービスに Bluetooth ロゴを与える一方、ユーザに対しては、“Bluetooth” というブランドを与えて統一的なワイヤレス環境の構築を目指すべく、通信業界とパソコン業界を統合した一つの世界基準技術に向けて進めつつある。このブランドについては、ブランド価値として「簡便性」、「機密性」、「自由度」、「多様性」、「信頼性」という5つのキーワードがある。Bluetooth のブランド目的は、ワイヤレス接続を通じて「簡便」ではあるが、「機密性」と「信頼性」を確保した通信ソリューションを創造する「自由度」をすべての人々に与えることである。この「多様性」は機動性を高めるとともに、双方向通信を行うために人々やそれらの危機に対して、革新的な通信方法を提供するものである。

3-2 .Bluetooth 開発の背景と目的

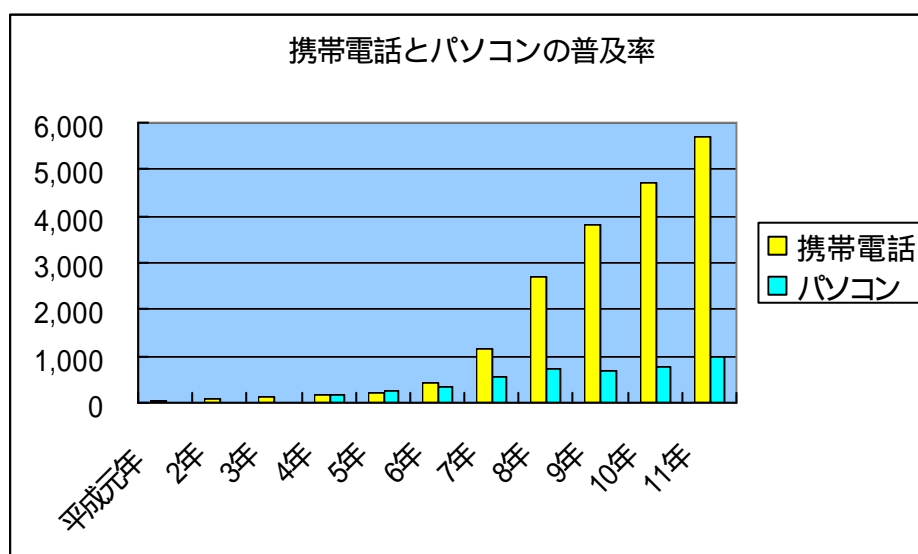
Bluetooth はもともとあらゆるモバイル端末同士をワイヤレス接続することを目的として開発された技術である。ここでのモバイル端末には、コンシューマ製品から業務用端末までいろいろなものが考えられる。携帯電話とパソコンを代表する企業がプロモータに名を連ねていることからわかるように、本来、Bluetooth の技術開発を行う際に最初に対象としてきた端末は携帯電話とノートパソコンである。しかし、Bluetooth 技術仕様はオープンであるという Bluetooth SIG の運営方針のもとに、誰もが Bluetooth 技術仕様を閲覧でき、Bluetooth 技術を搭載した製品やサービスの開発をおこなうことができる。そのためモバイル端末の枠は、携帯電話やノートパソコンとその周辺機器にとどまらず、全ての電子機器を意味している。現在、Bluetooth を搭載してもモバイル端末としての特徴を損なわないようにしなくてはならない。つまり、Bluetooth を搭載したために端末の外形が大きくなったり、重くなったりしては意味がない。また Bluetooth が消費する電力がモバイル端末本体よりも大きくならないようにする必要がある。

Bluetooth は 1999 年の技術仕様公開から急速に参加企業数を増やしている。通信業界に限らず様々な業界において注目されている。

まず携帯電話は、昨今では幅広い年齢層で利用されている。携帯電話本体の値段も安価でインターネットに接続できる等、様々な機能が追加されており、もはや手放すことの出来ない存在となっている。次にパソコンは、業務用に利用されていたものが、現在では一人に一台のパソコンを持つようになった。さらにそれぞれのパソコンがネットワークで接続され、データなどを共有するのが当たり前となった。

インターネットにアクセスするためにはパソコンが必需品であったが、現在ではインターネット接続機能を搭載したワープロやテレビなどが市場に現れた。1995年から96年にかけてプライベートでもインターネットにアクセスする人口が増え始めた。一般ユーザー向けのインターネット・サービス・プロバイダ業者が急速に増え始めた時期でもある。インターネットの利用は携帯電話が普及し始めた時期と重なって著しく増加した。(図3参照)

この時期は、同時にノートパソコンの出荷台数が伸びた時期でもある。携帯電話を用いたモバイルデータ通信が本格的に市場導入し始めたこともあり、携帯電話とパソコンを繋いでインターネットにアクセスするようになった。これが、Bluetoothが様々な業界から注目されるようになった要因の一つと考えられる。さらに重要なことはモバイル端末が普及するためには、それぞれが機能やアプリケーションを向上させていく必要があるが、そのニーズにこたえたのがBluetoothである。つまり、これらの普及したモバイル端末自体に大きな付加価値を与えてくれるのが、Bluetoothというモバイル端末に特化したワイヤレス接続技術である。Bluetoothの適用できる範囲が単にモバイル端末間にとどまらず固定装置にも拡張でき、これら最も潤っている市場セグメントとの接点が見出され、Bluetoothは更に注目されるようになった。



平成13年通信白書参照 (図3)

3-3、Bluetoothの規格

モバイル機器間での使用

Bluetoothの開発、標準化により、携帯電話などのモバイル機器からインターネット接続が可能になった。携帯電話やPDAなどのモバイル機器にBluetoothを実装するためには、Bluetooth自体をさらに小型化かつ軽量化する必要があった。さらに価格や消費電力を抑える必要があった。そこで、Bluetoothは送信距離と電

力に応じて3つのタイプが用意された。対応する機器によって、どのタイプを使用するのかを選択することが出来るようになっている。出力が大きくなればなるほど、本体が大きくなるという特徴がある。

また、モバイル機器で使用するためには、使用するLSIなどの半導体を小さくする必要があった。Bluetoothを構成するLSIは、当初3チップ構成だったが、その後2チップ構成になり、最近では1チップ構成のLSIで実現することができるように変化した。

- **Power Class 1**

- 最大出力 100mW

- 見通距離 100m

- **Power Class 2**

- 最大出力 2.5mW

- 見通距離 20m

- **Power Class 3**

- 最大出力 1mW

- 見通距離 10m

4章 Bluetooth の技術的側面

Bluetooth は今までの無線の規格から大きく脱したものではない。二章で述べた技術は Bluetooth の技術としても使用されている。ここでは無線 LAN にはない Bluetooth 独自の技術を検討する。

4-1 ピコネット

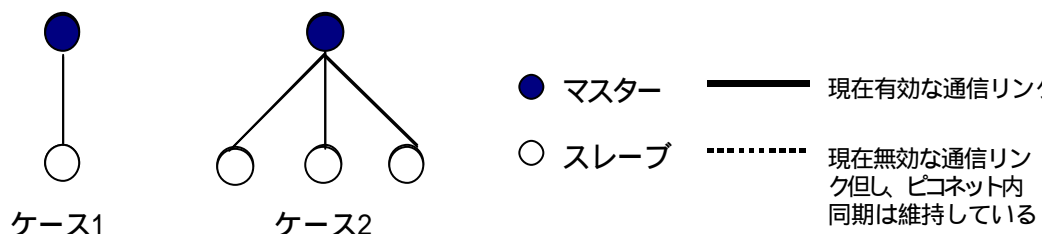
Bluetooth には、それぞれの機器に特別な設定をすることなく、お互いを近づけるだけで接続（アドホック接続）できるという特徴がある。この時に形成される通信ネットワークを、Bluetooth では「ピコネット」と呼び、同一ピコネット内に属する Bluetooth 端末は、周波数軸と時間軸において同期している状態にある。

ピコネットは、最大 8 台までの Bluetooth 対応機器を接続することができ、1 台の「マスター」と、最大 7 台までの「スレーブ」が存在している。

マスターとは、コンピュータネットワークのクライアント・サーバにおけるサーバに相当する端末で、ホッピングする周波数やタイミングを決めている他、ネットワークのトラフィックや状態を管理する役目を持つ。また、最大 8 台までの Bluetooth 対応機器を接続できるとあるが、実際には 9 台以上の機器がある場合においても、9 台目以降はパークモードという待ちの状態で存在することができるようになっており、マスターとの同期だけは行なわれるようになっている。

このように、1 台のマスターに対して複数のスレーブが接続される状態を、マルチポイント接続と呼ぶ。マスターは接続のために使われる ID 情報をもっており、これを利用することでセキュリティの確保も可能となっている。一方、スレーブはクライアントに相当する端末で、マスターの制御を受けながら通信する。

マスターとスレーブはその役割が固定されておらず、いつでもその役割を交代することが可能である。たとえ、マスターが最初にネットワークから抜けた場合でも、別の機器がマスターとなりピコネットはそのまま形成され続けることができる。



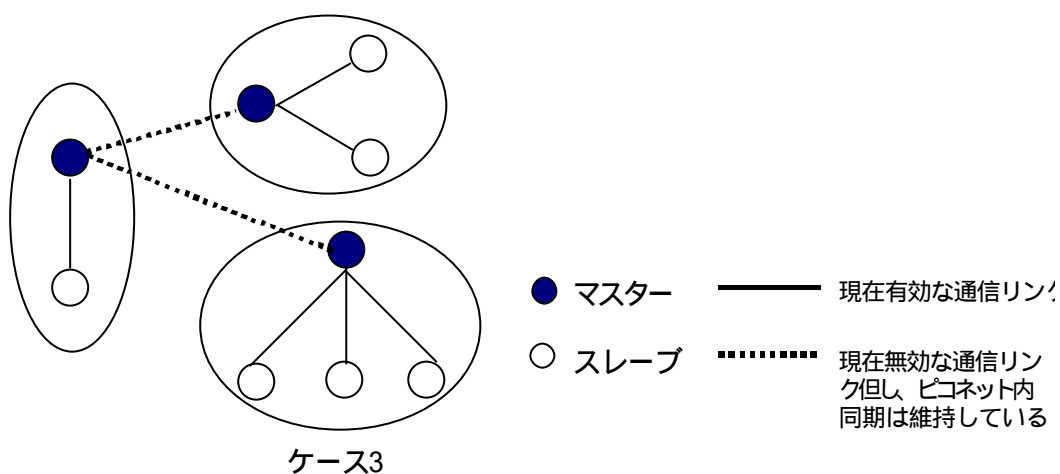
(構成例 1)

最もシンプルなトポロジー構成はケース 1 のマスターとスレーブが一つずつ存在する一対一の通信である。これに対してケース 2 では、マスターに対して複数のス

レーブが接続されている例である。ここでは 3 つのスレーブが 1 つのマスターと通信している。

構成例 2 は構成例 1 を拡張したものである。ケース 3 には、3 つの独立したピコネットが存在している。これらが独立して存在するというのは、それぞれが個別に周波数軸と時間軸の同期を確保している状態にあるということである。

また、この例ではそれぞれのピコネット同士はマスターまたはスレーブを介して接続されている。このようなピコネットが相互接続された無線ネットワークを「スカッターネット (Scatter net)」と呼ぶ。



(構成例 2)

ピコネット内の機器は PIN コード (Personal Identification Number Code) と呼ばれる暗証番号によって接続の認証を行っている。通信可能エリアに Bluetooth 機器を置いただけで、機器同士が勝手に通信がおこなうわけではない。Bluetooth で構成されたピコネットに参加する場合には、認証が必要であるが、2-2 で述べたチャレンジ・レスポンス方式が採用されている。

4-2 待機モードと電力制御

・ インクワイアリとページング

Bluetooth では、マスターがスレーブに BD_ADDR とクロックの値を伝達し、タイムスロットと周波数ホッピングパターンを同期させてはじめて、案たいしたピコネット内での通信が可能となる。この BD_ADDR とマスター・クロックの伝達の手順として、インクワイアリ (問い合わせ) とページング (呼び出し) という手順が定められている。

インクワイアリ手順は、通信範囲内にどのような Bluetooth 機器が存在するのかをマスターが知らない場合に実施する手順で、マスター機器が同報パケットを連続的に送信し、それを受信したスレーブ機器が自機に関する情報を返送すること

により実行される。

一方、ページング手順は、マスターが通信範囲内に特定の機器が存在していることを知っており、特定の機器をピコネットに参加させる場合に実行する手順である。ページング手順では、マスター機器から特定スレーブ機器向けの packets を連続的に送信し、対象となったスレーブ機器がそれに応答することにより実行される。

Bluetooth のベースバンドプロトコルでは、装置の基本的な状態として、通信を行っておらず、接続要求待ちの状態であるスタンバイ状態と、ピコネットに参加して実際に情報伝送を行う状態であるコネクション状態を定めている。コネクション状態で実際に通信を行うモードはアクティブモードと呼ばれるが、それ以外にも低消費電力モードとして「パークモード」「ホールドモード」「スニフモード」の3種類がある。Bluetooth 端末はこれら各モードにおいて最低限の送受信処理のみを行い、それ以外ではピコネット内同期を維持するために必要な内部処理しか行わない。これによって各モードにある Bluetooth 端末は電力の消費を低減させることができる。

パークモード

Bluetooth の通信では、通信を開始する際にはピコネットの構成のため、インクワイアリやページング手順の実施が必要である。しかし、中断した通信を再開するたびにインクワイアリやページングを実施することは無駄となりうる。そこで、通信は行わないがピコネットに参加するための必要な同期情報は保持した状態としてパークモードを規定することによって、インクワイアリやページングの処理を行わず、休眠状態から速やかに通信を再開することを可能としている。

ホールドモード

ホールドモードでは、機器間で一定時間通信を休止するというネゴシエーションを行うことにより、消費電力を低く抑えつつ、通信可能状態へ速やかに移行可能な休止状態をとることを可能としている。

スニフモード

「スニフモード」は、スレーブ特有の低消費電力モードである。各 Bluetooth 機器は、コネクション状態では互いの送信を監視している必要があるが、スニフモードでは、一定の間隔をおいてのみしか送信を行わないという規定を設けることにより、休止中の監視を不要とし、送信監視に必要な電力消費を低減している。

4-3 セキュリティ

Bluetooth では、無線媒体を使用している以上、信号が放射状に広がっていくことは避けられない。このような状況の中で誤接続と盗聴防止の観点から Bluetooth におけるセキュリティは大変重要な機能である。Bluetooth セキュリティの概念には大別して、「認証 (Authentication)」と「暗号化 (Encryption)」の2つが存在

する。

認証とは自分と特定の相手との間で接続を許可判断することであり、暗号化とは自分が通信中のデータを第三者に盗聴されないように保護することをいう。これら認証と暗号化は独立的に処理されるものであり、機能的には直接関連はない。Bluetooth セキュリティは、「リンクキー (Link Key)」という概念で管理されてリ
ティを管理するパラメータのことである。つまり、あるマスターとそのピコネット
に属するスレーブの2 端末間でこのパラメータが共通に設定されていなければ通
信をすることができない。当然、このリンクキーは第三者には開示されてはなら
ない。

Bluetooth では4 種類のリンクキーがあり、用途と目的に応じて使い分けをする。
それら4 種類とは、「初期化キー (Initialization Key)」「単体キー (Unit Key)」、
「複合キー (Combination Key)」「マスターキー (Master Key)」である。

リンクキーはBluetooth 端末間で定められるセキュリティのパラメータだが、実
際にそれが Bluetooth セキュリティとして果たす役割は以下の3 つがある。

データベースにセキュリティのパラメータを登録する。

設定されたパラメータに基づいて認証判断をすること。

秘匿性を確保するための処理に必要な暗号鍵を生成すること。

初期化キー

初期化キーとは、初めて接続を試みる Bluetooth 端末で使用される秘密鍵である。
今までに一度も接続したことがない Bluetooth 端末同士が通信をする場合、それら
の間でリンクキーは、まだデータベースにパラメータ設定されていない状態になっ
ている。同様な状況として、過去に接続を行ったことがあっても何らかの理由でデ
ータベースにリンクキーがパラメータ設定されていない場合に通信開始プロセス
を保護するために初期化キーは使用される。セキュリティ管理のパラメータとして
役割を有するが、暫定的なリンクキーとして扱われるものであり、初期化キーその
ものはデータベースに記録されることはない。

単体キー

単体キーとはおよそ恒久的に用いるリンクキーであり、接続対象の端末とは無関
係に1 つしか存在しない。つまり、新しい接続対象の端末が現れるたびに初期化キ
ーの生成を行うが、既に単体キーが生成されている場合は、新たに単体キーを生成
せずに既にある単体キーを用いる。このため、データベースにパラメータ設定され
るリンクキーに自分の単体キーを用いた場合には、接続相手が複数であってもその
値は同一となるので、複数個のリンクキーを管理する必要がなくなる。

復号キー

復号キーもおよそ恒久的に用いるリンクキーだが、接続対象の端末が複数個ある
場合には、その接続相手の数だけ存在する。

マスタキー

マスタキーとは、同一ピコネット内のスレーブに対する同報通信パケットを亜 G 投下する暗号キーを生成するために用いるリンクキーである。道央通信に暗号化を適用するには、同一ピコネット内の全てのスレーブが同一のリンクキーを持つ必要がある。リンクキーが異なるとまったく違った暗号キーを生成してしまい、同報通信パケットの暗号化に使えないからである。

Bluetooth では、すべてのスレーブで共有されるこのリンクキーをマスタキーと呼び、同報通信パケットを暗号化するための暗号キーを生成するときの入力に用いる。ただし、マスタキーは暫定的なリンクキーで、その必要がなくなったときに破棄されて、もともとデータベースにパラメータ設定されているリンクキーが有効となる。このマスタキーの生成要求は、マスターからスレーブに対して通知される。

* Bluetooth での認証は 2-2 で紹介した CHAT 方式を使用している。

5章 Bluetooth の利用法

Bluetooth について検討してきたが、実際にはどのような利用が考えられているのだろうか。Bluetooth の特徴から考えられる利用法と、現在の業界の動向と Bluetooth がもたらしている課題を述べる。

5-1 Bluetooth の利用法

Bluetooth では、音声認識が一つの重要なキーワードである。身近なモバイル端末である携帯電話と Bluetooth の関係は切っても切り離せないものである。Bluetooth が搭載された携帯電話を中心にどのような利用が考えられるか例をあげる。なお、これらをより体系的に見る方法として以下の3つの視点から検討する。

既存のモバイル端末に対して Bluetooth を搭載する

電子機器で既に使用されている接続を Bluetooth に置き換える

今まで接続技術を利用していない電子機器に Bluetooth を採用する

既存のモバイル端末に対して Bluetooth を搭載する

Bluetooth が搭載された携帯電話

- ・ モバイル電子マネーの利用

携帯電話を利用して自動販売機で飲み物を購入できるほか、電車や地下鉄で Bluetooth 改札口ができれば、チケットレスで乗降車ができるようになり、混雑は回避される。Bluetooth は世界共通なので、海外でも利用できる。

- ・ インターコム

Bluetooth が搭載された携帯電話では、Bluetooth の電波が届く範囲での通信は無料となる。人が多い中で待ち合わせの相手を探す時や、メールアドレス・電話番号、画像などのデータを送る時などにも便利である。

- ・ 携帯電話の分離

携帯電話の共通の部分である通話の部分分離して使うことが考えられる。Bluetooth を搭載すると、ヘッドセットを耳にかけ、電話機の通信コアと無線でやりとりして、ハンズフリーで電話を受けたり、かけたりすることができる。通話部分が分離されることにより、画面の部分が大きくなった情報端末的な機器や、逆にコンパクトにしてウェアラブルにするなど、用途に応じて様々な形状のものが実現可能となる。

- ・ リモートコントロール

移動中の電子機器のコントロールはすべて携帯電話からできるようになる。ノートパソコンのファイルの検索や送信指定などが、その都度ノートパソコンを

立ち上げなくても携帯電話からリモートで行える。逆に、携帯電話で受信したメールやその添付ファイルも指定するだけで様々な電子機器に送信することが可能となる。

- GPS

緊急時に身に付けている電子時計などを押すと、かばんの中にある携帯電話に自動的に無線でつながり、携帯電話に搭載されている GPS の位置情報や携帯電話に登録済みの個人情報など、情報を加え、自動的に 110 番通報される電子機器で既に使用されている接続を Bluetooth に置き換える

- パソコンと周辺機器

マウスやキーボード、プリンタ、モデムなどの周辺機器とパソコン本体の接続も無線で可能となり、家中どこからでもインターネットや印刷が簡単にできる

- 会議や講義での利用

Bluetooth 搭載のプロジェクタがあれば、スクリーンに映し出した資料を同時に会議や講義に出席した全員のパソコンにも同じ画面を示すことができる。

今まで接続技術を利用していない電子機器に Bluetooth を採用する

- メッセージプッシュ、情報アクセス

空港のカウンタやホテルのロビー、デパート、美術館などの狭い空間内で、位置に依存した情報の配信やアクセスが可能である。人が多く集まるような場所にいる場合、メッセージプッシュによって道案内やガイド、サービスの案内などがあれば便利である。

- 電子ポスターと PDA

電子ポスターから PDA に情報をダウンロードできる。例えば、映画館ではプロモーションビデオをダウンロードし、面白そうであれば PDA で座席の予約をし、ゲートを通過して席に着くことができる。

- 複数プレーヤーで対戦ゲーム

ゲーム機に Bluetooth を搭載すると、近くにいる人と通信費をかけずに対戦ゲームで遊べるようになる。

- 名刺交換

Bluetooth 搭載の携帯電話や PDA に自分の名刺を登録しておくビジネスで相手と名刺交換ができる。

- ホームシステム

Bluetooth と携帯電話の融合によるテレビ、エアコン、風呂などの電子機器の制御に携帯電話が使えるようになる Bluetooth ホームシステムや、Bluetooth の音声認識機能を利用したドアロックの開閉システムが考えられている。声紋を登録して、個人を特定することでセキュリティを実装する。

5-2 Bluetooth のかかえる課題

既存のモバイル端末に対して Bluetooth を搭載する場合、大きさ、重さ、消費電力、さらには持ち歩くための機器本体の使い勝手などがモバイル端末として最適化されていなくてはならない。ほとんどのモバイル端末は小さく、軽く、消費電力が低く抑えられている。Bluetooth の搭載によってこれらの特徴が損なわれることがないように Bluetooth 本体を小さくし、消費電力を抑える開発が進められなくてはならない。電力供給については、物によっては腕時計のように太陽エネルギーや振動によって電力を貯蓄する技術が開発されると思われる。

Bluetooth は今まで接続技術を利用していない電子機器に Bluetooth を採用する。つまり、今までにないアプリケーションやサービスを創造する。従って、新たな発想と他の分野の技術開発やサービス提供を見据えて考えなくてはならない。

これは Bluetooth が単にケーブルなどの 1 対 1 接続機能の代替として位置付けられているのではなく、1 対多接続の機能、音声とデータの統合、または指向性の制限を受けないなど Bluetooth 特有の機能を備えていることから、その適用範囲が多岐に渡ることが考えられている。例えば、モバイル電子マネー、駐車場などの予約、電車の改札、ドアロックの開閉、ワイヤレスカフェ、メッセージプッシュ、情報アクセス、ワイヤレスホームシステムなどがある。特に、モバイル電子マネーは一見便利であるが無線という技術を使用する以上、より強力にセキュリティと認証を強化しなくてはならない。

6章 まとめ

本論では、無線 LAN が実現する社会というテーマで無線 LAN の可能性について検討してきた。有線 LAN は基幹で大規模な LAN を支え、終端になると無線 LAN でネットワークを形成する。Bluetooth はもっと身近な範囲な家電などを扱うものとして全く別の役割をもつものとして捉えている。

1 章では、LAN に関して述べている。LAN とは限られた比較的狭い範囲でのネットワークで、ホストコンピュータやデータ端末、コンピュータなどを一定以上の通信速度でパケット化されたデータを高速に送受信する伝送路を指す。LAN は接続された装置間で自由に、かつ容易にデータ通信を実現することを目的に開発された。LAN を構築する場合、ケーブルを端末ごとに接続する必要がある。ケーブルは配線スペースをとること、配線工事などで費用と手間と時間がかかることから物理媒体を通さない無線 LAN が開発された。有線 LAN が同軸ケーブル、ツイストペアケーブル、光ファイバケーブルなどを使うのに対して、無線 LAN では大別して電波と赤外線を使用して通信を行う。有線 LAN に対して、無線 LAN のメリットとデメリットを検討する。メリットは(1)モバイル性を最大限に発揮できる(2)ケーブルのトラブルを回避できる。(3)インターネット接続を共有できる、などが挙げられる。デメリットとしては、(1)電波が届きにくい所では通信が安定しない。(2)セキュリティ対策が必要。(3)隣り合うチャンネルでは電波干渉が起こる。(4)伝送速度が有線 LAN に比べて10分の1程度である。などを挙げた。

2 章では無線 LAN の技術的側面を検討している。ISM バンド、スペクトラム拡散方式、伝送方式、セキュリティについて述べている。これらは、3 章以降で述べる Bluetooth でも使用されているものである。

3 章からは有線 LAN、無線 LAN の新しい形である Bluetooth に注目し、検討した。Bluetooth とは、携帯電話とパソコンを代表する 5 社によって結成された業界団体 Bluetooth SIG によって策定された短距離無線通信規格の総称である。Bluetooth と無線 LAN の違いは、Bluetooth が(1)PAN とよばれる範囲での近距離無線通信であること、低消費電力であること(2)柔軟なネットワークの構築が可能であること(3)音声とデータを同様に扱うことが見込まれていること(4)オープン仕様であること(5)世界中どこでも使える技術であることなどである。Bluetooth はもともとはあらゆるモバイル端末同士をワイヤレス接続することを目的として開発された技術であるが、Bluetooth 技術仕様はオープンであるため、誰もが Bluetooth 技術を搭載した製品やサービスの開発をおこなうことができる。そのためモバイル端末の枠は、全ての電子機器まで広がった。

4 章では、Bluetooth の技術的側面を扱っている。2 章 無線 LAN の技術的側

面で述べた技術を踏まえて、Bluetooth 独自の技術について検討している。Bluetooth は電波方式の無線 LAN で、ISM 電波帯域を使用している。Bluetooth の通信方式はスペクトラム拡散方式を使用している。スペクトラム拡散は拡散方式が 2 種類あるが、Bluetooth では周波数ホッピング方式を使用している。伝送方式は無線 LAN 一般が使用している CSMA/CA 方式を使用している。Bluetooth 独自の技術として、ピコネットという 1 対多の接続がある。また Bluetooth には電気消費を極力抑えるためのパークモード、ホールドモード、スニフモードという技術がある。Bluetooth でのセキュリティは認証と暗号化によって支えられている。認証はチャレンジ・レスポンス方式を取り入れ、リンクキーという 4 つのキーで暗号化する。

5 章では、既存のモバイル端末に対して Bluetooth を搭載する 電子機器で既に使用されている接続を Bluetooth に置き換える 今まで接続技術を利用していない電子機器に Bluetooth を採用する 以上の 3 つの視点から Bluetooth の利用法と未熟な Bluetooth 技術の課題点を検討した。

無線 LAN の利用と、新たな発展としての Bluetooth は、我々の生活をより豊かに便利にする。ローカルエリアとパーソナルエリアをカバーするため機器を設置し、無線 LAN と Bluetooth を使用していた。しかし、現在ではホットスポットとして、コーヒーショップ、ファーストフード、駅などで無線 LAN が使用できる場所が広がっている。逆に、今後電波が乱れ飛ぶ社会を想定してアイススポットという電波が全く届かない場所を設置する動きもある。アイススポットを作らない限り、携帯電話、無線 LAN をふくめた電波の影響を遮断できなくなる社会が実現しつつあるということである。我々が意識することなく浸透しつつあるネットワーク社会だが、無線 LAN、Bluetooth の利用はいたるところから情報を送受信することができる。Bluetooth は 10m という限られた範囲でのネットワークであるため、移動してもすぐに最新の情報を得ることができる。モバイル端末に対しての Bluetooth の利用とオープン仕様という特長は、様々な企業にとって新製品の開発のチャンスであり、使いやすい商品は消費者にとっても望ましいことである。

無線 LAN、特に Bluetooth について述べてきたが、ネットワーク全体で考えると、無線 LAN だけが今後発展するわけではない。1 章で無線 LAN のデメリットの 1 つにあげた通信速度の問題は、解決するまでに時間がかかるのは確かである。LAN というローカルなネットワークであっても、大きなデータを複数扱う基幹ネットワークは、伝送速度が速く、安定している有線 LAN である必要がある。中心にある大規模なネットワークから端末へと移り、基幹ネットワークと個人、家庭、オフィスを繋ぐのは無線 LAN である。LAN の中心ほどの伝送速度を必要としない末端では、無線 LAN が時間、費用、手間などの理由から利用される。無線 LAN の機器自体の値段も以前と比べて下がってきており、オフィスへの導入も進んでいる。無線 LAN は末端系として、

通信速度をあげるなどの技術革新を進めつつ発展していく。もっと身近なエリアでの使用や、持ち歩くことで常に新しい情報を得るための手段としては Bluetooth が便利である。Bluetooth は本論で紹介した通り、有線 LAN も、従来の無線 LAN にない新しい特性を獲得している。有線 LAN、無線 LAN、Bluetooth はそれぞれの特長を活かし、共存してネットワークを形成している。

Bluetooth の開発によって、有線 LAN と無線 LAN の共存体系にも新しい分野が進出することになった。Bluetooth の大きな特徴は、無線であること、音声もデータとして扱えること、低消費電力であること、ウェアラブルであることなどである。

その中でも、現在、IT 業界をはじめとする様々な業界は「ユビキタス」という概念に注目している。ユビキタスを実現するためのツールの 1 つとして Bluetooth も注目されている。ユビキタスとは、ラテン語で「いたるところに偏在する」という意味で、インターネットなどの情報ネットワークに、いつでも、どこからでも、どんなツールを使ってでも、コンピュータにアクセスできる環境を指す。1988年にマーク・ワイザーが提唱した概念で、正確には「ユビキタス・コンピューティング」である。それまで、対パソコンでしか使用することができなかったコンピュータやインターネットを、通勤途中でも、オフの海岸でも、どこにいても、どこからでも使用できることができるようにするのがユビキタスの概念である。

アクセスに使う端末は、パソコンや携帯電話に限らず、冷蔵庫や電子レンジといった家電製品、自動車、自動販売機等もインターネット接続され、ウェアラブル・コンピュータと呼ばれる身に付けるコンピュータも開発中である。自由度を高めるため、これらの情報端末間は無線 LAN や Bluetooth で接続される。

無線 LAN を使用したユビキタス社会の到来は、我々にとっても便利であるのと同時に、高齢者や障害をもつ人にとっても豊かな生活をもたらすものである。

高齢者の人口は増加し続け、2005 年には成人の 4 分の 1 が高齢者になる。高齢者は自立して生活をし、豊かな生活を楽しんでいきたいと考えている。Bluetooth の特徴の一つでもある音声認識技術があれば行動に制限のある高齢者や障害者でも音声のみで家電に命令をだすことができるようになる。外出先では行く先々の Bluetooth 端末から情報が発信され、バリアフリーの情報などを受け取り行動することができるだろう。視覚障害者にはヘッドセットから電話の受信、来客、交通信号の情報などが入手できる。

こういったユビキタス社会が到来には、従来の LAN だけでなく、無線 LAN と Bluetooth 技術が必要である。我々の生活がより豊かになるのと同時に、高齢者、障害者にとって自立的で活動的な豊かな生活を送ることができる社会が無線 LAN によって実現される。

参考文献

- 鈴木憲一 『ゼロからはじめる無線 LAN』 株式会社アスキー 2001 年
- 福田崇男 「無線 LAN のここが危ない」『日経 Internet solutions』日経 BP 社
2002 年 11 月号
- 小泉修 『図解でわかる LAN のすべて』 日本実業出版社 2001 年
- 宮津和弘 『ワイヤレス通信の新技术 Bluetooth ガイドブック』
日刊工業新聞社 2000 年
- ブレント・ミラー、チャトシツク・ビズネス・イノベーション 『Bluetooth テクノロジーへの招待』
ピアソン・エデュケーション 2002 年
- E-Trainer.jp 『よくわかる最新ユビキタスネットワークの基本と仕組み～次世代ネットワークによる「ユビキタス社会」とは?』 秀和システム
2002 年