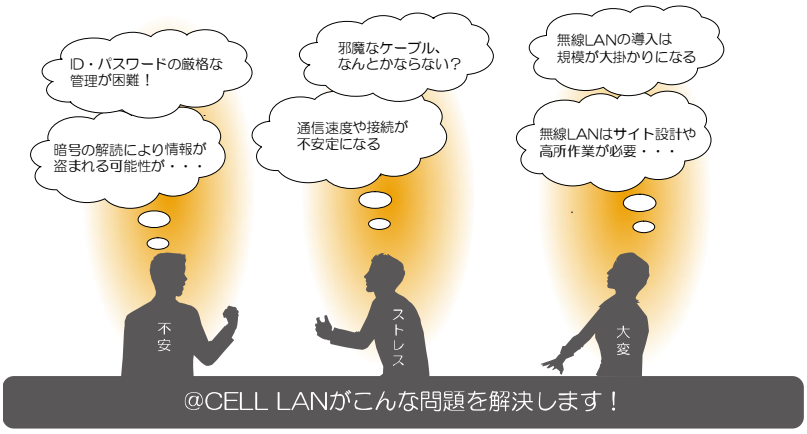
@CELL　LAN で実現する

セキュア LAN 構築術

利便性とセキュリティを両立
ISMS 適合を目指す LAN 環境



平成 21 年 7 月 1 日

株式会社セルクロス

目　次

1. セキュリティ関連の事件

情報漏えい事件が多発しています。下の表は、2008 年の 8 月の前半に報道された事件の一覧です。たったこれだけの期間であるにもかかわらず、その多さには「またか？」の次元を越えて、「このままで、日本は本当に大丈夫なのだろうか？」という不安さえ感じてしまいます。「自分たちだけは大丈夫」という楽観主義も、もはや通用しません。そんな社会に私たちは、生きています。

2008年8月19日	教員の規則違反による情報持出し後、個人PCから情報が流出 －詫間電波工業高等専門学校（香川）
2008年8月18日	イベント当選メールのシステム不具合による誤送信で個人情報流出 － TNX
2008年8月14日	委託先のSEが持ち出した個人情報9558件がWinny流出 － 新潟県総合生活協同組合
2008年8月13日	絵本のポータルWebサイトから不正アクセスにより顧客情報が漏洩？ 絵本ナビ
2008年8月11日	4月に発生した治験関連情報記録したPCの盗難被害を公表 － 東京CRO
2008年8月09日	店舗への不正侵入で顧客情報が盗難 － 山形三菱自動車販売
2008年8月06日	作業ミスによりネット上から学生の個人情報が閲覧可能に － 大阪商業大
2008年8月02日	職員の帰宅途中の買い物時にバイクからUSBメモリなど盗まれる －ワッセ森のひろば保育園（仙台）
2008年8月08日	営業担当者からの休暇案内メールの誤送信で個人情報が流出 － パナソニックシステムソリューションズ
2008年8月08日	研修医が無許可でUSBメモリ使用、個人情報を紛失 － 多摩南部地域病院
2008年8月08日	滋賀県の地域情報を発信するメルマガで誤配信 －アドレスが流出
2008年8月08日	生徒の成績含む未許可のUSBメモリを紛失 － 神奈川県立高校
2008年8月07日	顧客への案内メール誤送信、アドレスが流出 － 松下電工インフォメーションシステムズ
2008年8月06日	アウトドア用品サイト「ナチュラム」に不正アクセス － 最大65万件の個人情報が流出
2008年8月06日	介護施設の入所者情報がWinny流出 － 尼崎医療生協
2008年8月05日	口座情報を記録したマイクロフィッシュ紛失 － JAみなみ信州
2008年8月05日	医療機関の患者情報含むUSBメモリ、院内で見つかる － 都立病院
2008年8月05日	顧客情報を保存したノートPCを電車内で盗まれる －アイレップ
2008年8月04日	サイト運営者の氏名やサイト情報などが一部閲覧可能に －アドウェイズ
2008年8月01日	従業員の自宅最寄り駅でノートPCが鞄ごと盗難被害 － ジェック

NPO ネットワークセキュリティ協会（JNSA）が発表した報告によると、2007 年度だけでも漏えい人数は、3050 万人を超え、金銭的な賠償に換算すると、2 兆 2700 億円を超え、一件当たりの被害額も 28 億円になると試算しています。まさに、経営の根幹を揺るがす問題ともなりかねない状況です。

このような現実を受けて、各種法律の整備が進むと共に、ISMS に加え、P マークの取得、PCI DSS（Payment Card Industry Data Security Standard）への対応を進める企業が増えてきました。

しかし、その一方で企業の生産性や社員の利便性が、損なわれるようであれば、本末転倒なことです。

2.　LAN 構築にかかわる課題

「情報資産」は、企業活動の根幹であり、その保全を避けて通ることはできません。この「情報資産」の多くは、情報システム上で管理、運用されています。ですから、情報システムについてのセキュリティ対策は、「情報資産」の保全と不可分といえます。

しかし、情報システムのセキュリティ対策に完璧を求めることは不可能です。いくら管理を徹底しても人的ミスを避けることはできないし、悪意の第三者による攻撃は、日々進化する技術に支えられ、ますます巧妙なものとなっています。万が一の事件や事故を避けることは、現実的には不可能といえるでしょう。

ならば、コストをかけて徹底したセキュリティ対策を行えばいいかというと、それも現実的ではありません。仮にそれができたとしても、その経済的負担は膨大なものとなり、利便性が損なわれ、業務の生産性が著しく阻害されることを覚悟しなければならなりません。これでは、生産性を追求し利益を生み出さなければならないという企業目的に反することになります。

このような現実に対処しなければならない多くの企業にとって、ISMS（情報セキュリティ・マネージメント・システム）は、「情報資産」を保全するための国際標準（ガイドライン）として広く受け入れられています。

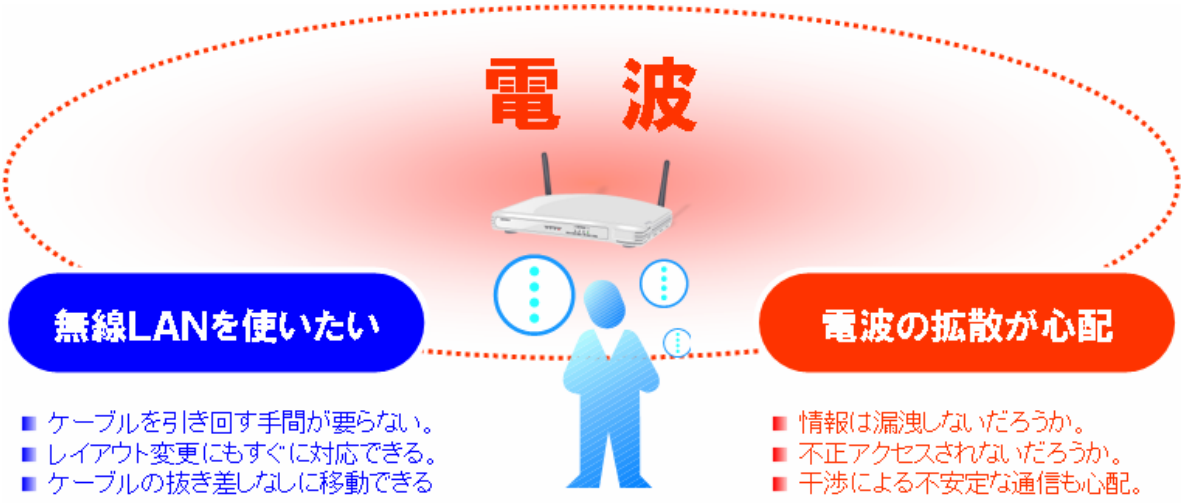
2009 年 2 月 9 日現在、この ISMS の適合認定を取得した国内企業は、3055 社を数えるまでになり、その数は今後も増加する傾向にあります。

ISMS の適合認定を取得した企業、あるいは、取得を目指す企業にとって、LAN 環境の構築は、頭を悩ますことのひとつです。

セキュリティを考えれば、外部からの不正アクセスや漏えいなどを心配しなくてもいい有線 LAN が選択肢となります。しかし、ケーブルを引き回す煩わしさや、乱雑に放置される LAN ケーブルによって、オフィスの美観を損ねるなどの難点もあります。

ならば、無線 LAN という方法もあります。有線 LAN の課題を解決すると共に、会議室や他部署へ移動、フリーアドレス・オフィスでの使用においても、ケーブルやコネクターの存在や数などを気にすることなく使えます。そのため、利便性は高く、オフィス・ワークの生産性を上げることにも役立ちます。また、設置やレイアウト変更にかかる手間や経費を節減できることなどもメリットもあります。

その一方でこのメリットを生み出す電波を利用した通信が、そのままセキュリティ上のリスクに結びつくという懸念を払拭できません。というのも、無線 LAN 機器から発される電波は、窓や壁を突き抜けて屋外へ簡単に漏れてしまうため、社内情報の漏えいや社内ネットワークへの不正アクセスの危険性が有線 LAN に比べて高いと考えられているからです。そのため、無線 LAN の高い利便性を認めながらも導入に踏み切れない企業も少なくありません。



無線 LAN の「利便性」と有線 LAN の「セキュリティ」を同時に享受したい。この対立する課題を同時に解決できる新たな選択肢が求められています。

3.　ISMS の規定するリスク

LAN を構築する場合、どのようなセキュリティ・リスクを排除しなければならないのか？　ISMS の規定するリスクという観点で考えてみることにしましょう。

ISMS では、リスクを以下のように評価しています。

リスクの評価＝情報資産の価値×脅威の評価×脆弱性の評価

「情報資産」とは、企業活動を行うために必要な情報のことです。「脅威」とは、企業活動に損失や損害をもたらすセキュリティ事故の潜在的原因です。「脆弱性」とは、この「脅威」を誘引する弱点やセキュリティ・ホールです。

例えば、「情報資産」とは、

- 個人情報
- 人事情報
- 設計情報

などで、その重要度に応じて、その価値が規定されます。

また、「脅威」とは、

- 不正なユーザーによるネットワークへのアクセス
- 盗聴
- 通信への侵入

などです。

この「脅威」を誘引するものが、「脆弱性」です。

- 外部からアクセスされやすいネットワーク環境
- アクセスコントロールの欠如
- 不適切なパスワード

などとなります。

ISMS では、まず、管理すべき対象となる「情報資産」を規定します。そして、その「情報資産」に対する「脅威」と「脆弱性」を事前に把握し、そこから生じるリスクが、組織の活動にどの程度の影響を及ぼすかを評価すると共に、これらリスクが企業の経営に悪影響を与えないようにすることや企業価値を毀損しないよう、対策を求めています。

リスクを規定する 3 つの要因の内、まずは、「脅威」と「脆弱性」について、詳しく見ていくことにしましょう。

まず 「脅威」とは、「情報資産」を毀損し、企業活動や組織に重大な損害を与える要因です。これを ISMS では、以下の 3 つに区分しています。

脅威の分類		
人為的脅威		環境的脅威
意図的脅威 Deliberate	偶発的脅威 Accidental	環境的脅威 Environmental

「意図的脅威」とは、盗難や不正アクセスなどの悪意に基づく行為によって生じる脅威を意味しています。また、「偶発的脅威」とは、停電や火災などを指し、「環境的脅威」とは、地震や静電気による磁気データの破壊などを意味しています。

LAN の利用に当たっては、上記のうち、「人為的脅威」である「意図的脅威」と「偶発的脅威」への対策が、必要となります。これら「脅威」と「脆弱性」との関係を示したものが、以下の表です。

脆弱性の分類	脆弱性の例	関連する脅威の例
環境、施設	ドア、窓などの物理的保護の欠如	盗難
	不安定な電源供給設備	停電、誤動作
	災害を受けやすい立地条件	洪水、地震など
ハードウェア	温度変化に影響を受けやすい	故障、誤動作
	記憶媒体のメンテナンス不足	故障、情報漏えい
ソフトウェア	仕様書の不備	ソフトウェア障害、誤作動
	アクセスコントロールの欠如	なりすまし、改ざん、情報漏えい
	不適切なパスワード管理	不正アクセス、改ざん、情報漏えい
	監査証跡（ログ管理）の欠如	不正アクセス
	バックアップコピーの欠如	復旧不能
	文書化の欠如	オペレーティングミス
通信	保護されていない通信経路	盗聴、不正ユーザーによるアクセス、通信への不正な侵入
	ケーブル接続の欠陥	通信傍受、通信不能
	非暗号化	情報漏えい
文章	保管不備	盗難、紛失
	コピーに関する教育の不徹底	盗難、情報漏えい
人事	要因の欠如	ミス、不満によるいやがらせ
	清掃スタッフなどに対する監督不在	盗難、システム破壊
	不十分なセキュリティ訓練	オペレーションミス、復旧遅延
	セキュリティ意識の欠如	情報漏えい、システム破壊
そのほか	予算不足	さまざまな脅威
	不適切な保守サービスの利用	故障時に復旧不能
	納入情報の保管不備	信用の失墜

LAN を使用する場合に当てはめて考えてみると、「脆弱性」に相当するものが「保護されていない通信経路」に当たります。つまり、有線 LAN のように、物理的に外部からアクセスできない場合や無線 LAN を使用する場合に、高度な暗号化を行うなどの適切な対策がとられなければ、「外部からアクセスされやすいネットワーク環境」が存在することになることになります。

この「脆弱性」に対応する「脅威」は、「盗聴」、「不正ユーザーによるアクセス」、「通信への不正侵入」などがそれに当たります。

また、仮に適切な対策が施されていたとしても、ユーザーの役割や権限に応じた「アクセス・コントロールの欠如」や「パスワードや暗号鍵の不適切管理」という「脆弱性」が存在すれば、「なりすまし」、「改ざん」、「情報漏えい」、「不正アクセス」などの「脅威」を高めることになります。

4. ISMS に適合した LAN 構築上の課題

ISMS では、「情報資産」を以下の 10 の区分に分けて、管理することを求めています。

	管理分野	管理内容
1	セキュリティ基本方針	情報セキュリティマネジメントの方針
2	組織のセキュリティ	情報セキュリティ推進に責任を持つ委員会の設置
3	資産の分類および管理	資産項目の作成や資産分類についての規定
4	人的セキュリティ	人的要因によるリスク軽減を目的に、責任、採用条件などを規定
5	物理的および環境的セキュリティ	入退室管理、施設や装置取り付けなどについて規定
6	通信および運用管理	情報処理システムの運用管理のセキュリティについて規定
7	アクセス制御	利用者の情報アクセス管理やネットワークアクセス制御について規定
8	システムの開発および保守	健全な開発・運用のため、システムへのセキュリティ要件、アプリケーションプログラムに対するセキュリティ要件、情報の秘匿・認証、暗号鍵の管理などについて規定
9	事業継続管理	事故、災害からの復旧・予防管理、事業継続管理について規定
10	適合性	知的所有権、プライバシー保護などの法的措置への準拠(適合性)を規定

LAN の導入については、「人的セキュリティ」、「物理的および環境的セキュリティ」、「通信および運用管理」、「アクセス制御」にかかわる管理が必要となります。

実際の利用シーンを考えてみましょう。

まず、有線 LAN の場合、資格の無い人間が許可なくオフィス内に侵入するといった「物理的および環境的セキュリティ」が、適切に運用されていれば、「外部からアクセスされやすいネットワーク環境」という「脆弱性」はなくなり、これに伴う「脅威」も生じることはありません。

これに対して、無線 LAN の利用は、「電波が外部に漏れる」という原理的な不安要素を抱えています。この課題に対処する手段が、暗号化通信です。

そのひとつである WEP 暗号のように、その解読方法が公知なものならばともかくとして、AES 暗号などの最新の技術であれば、この課題は、「完全」に解決できるという意見もあります。

しかし、WEP 暗号もかつてはそうであったように、ソフトウェア的な対策に「完全」はありません。LAN の管理者は、「暗号が破られる」可能性という不安を常に抱えていなければならないのです。

となると、その不安をなくすためには、暗号化というソフトウェア的な対策ではなく、有線 LAN のように物理的な対策をとるしか方法はないのでしょうか。

そうすると、今度は、無線 LAN の利便性を享受できず、オフィス･ワークの生産性向上に制約を設けることになります。
また、「電波」という不可視なものを使用するという、ある種漠然とした不安と相まって、採用に難色を示している企業も少なくありません。

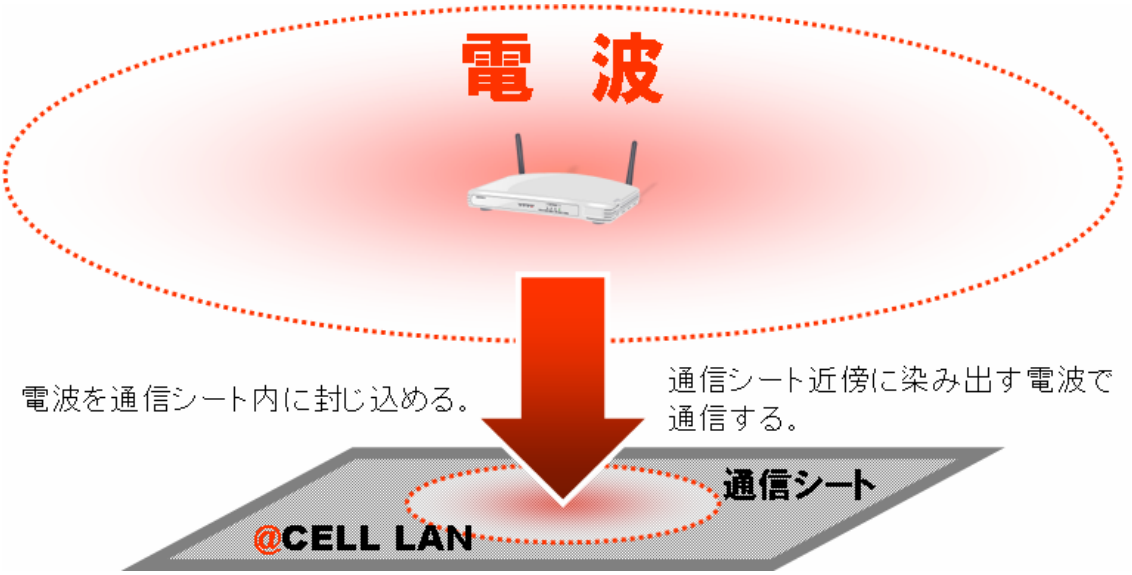
有線 LAN と無線 LAN という、二者択一の選択肢に依存する限り、この矛盾を永遠に解消することはできないのです。

5.　@CELL LAN（アットセル・ラン）とは

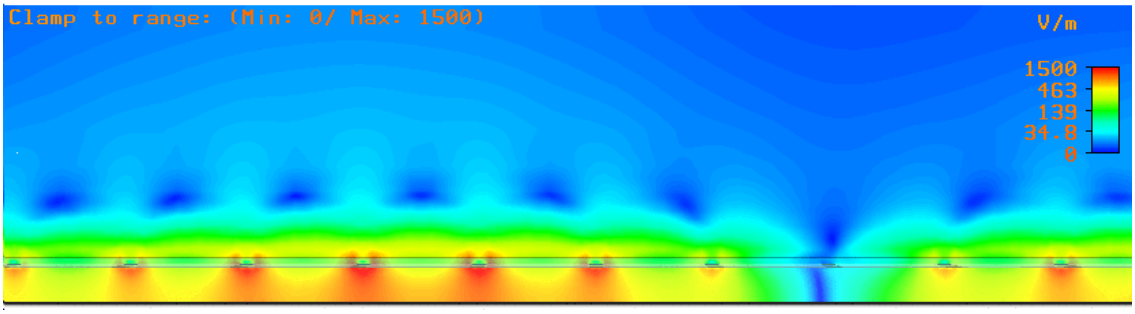
@CELL　LAN とは、このような矛盾を解消し、無線 LAN の持つ利便性と有線 LAN のような高度なセキュリティを同時に享受する手段として開発された新しい LAN システムです。

写真をご覧ください。@CELL LAN を実際に設置した様子を示したものです。

@CELL LAN は、デスクや会議テーブル上に置いた通信シート内に、無線 LAN の電波を封じ込めます。そこに無線 LAN 端末を置くとはじめて通信ができるようになるというものです。

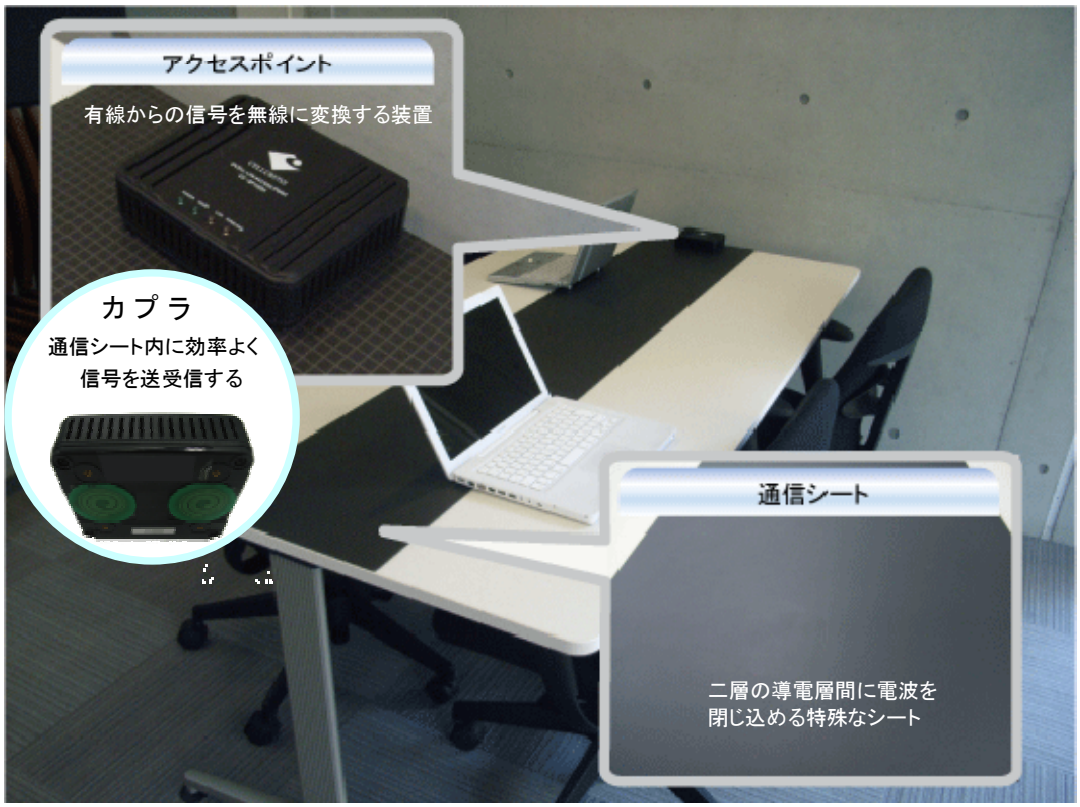


そのシートからは、微弱な電波が染み出しています。この電波は、エバネッセント波と言われるもので、シートから離れれば離れるほど急激に弱くなり、シート外からは受信できないように設計されています。無線 LAN 対応のノート PC であれば、シートの上に置いたときに、最も効率が良くなるように作られています。



このような仕組みにより、このシートに接触、またはそのごく近傍にいなければ通信できません。

図をご覧ください。@CELL LAN システムの構成を示したものです。



デスクや会議テーブル上に置く「通信シート」と既存の社内 LAN との通信の受け渡しを行う「アクセスポイント」の 2 つによって構成されています。アクセスポイントの底面には、シート内に電波を送り込むと共に無線 LAN 端末からの電波を吸い上げる「カプラ」が実装されています。

@CELL LAN で使用できるノートパソコンなどの端末については、特別なソフトウェアやハードウェアは必要ありません。一般的な無線 LAN 規格である 802.11g または a が使用できれば、何の問題もなく利用可能です。

また、オプションの「クライアント・アダプタ」を USB を介して端末に接続すると、電波は、この「クライアント・アダプタ」と通信シートの近傍数センチに限定され、ほぼ完全に電波の飛散を封じ込めることが可能となります。

以上のように、@CELL LAN を使えば、無線 LAN と同等の利便性と有線 LAN と同等のセキュリティを同時に手にすることができるのです。

このように、@CELL LAN は、ISMS 認証にも対応できる高いセキュリティ性能を備えています。加えて端末が、通信シートに接することが接続の条件になりますから、物理的に通信のエリアを限定できます。この特性から、電波の干渉や障害物などを予め調査して、機器の配置や数などを設計しなければならない「サイト・サーベイ」は必要ありません。

また、天井などにアクセスポイントやアンテナを据え付けるために、高所工事も不要になるなど、導入時やオフィス・レイアウト変更に伴う負担が、大幅に軽減されるといったメリットもあります。

他にも、どの通信シートから接続しているかを特定できますので、利用者の位置情報の取得による在席管理、特定エリアからのアクセス制限、利用者の位置と利用履歴を組み合わせたアクセス履歴管理など、高いセキュリティ性能と無線 LAN の利便性を享受しながら、通常の無線 LAN では実現不可能な、新たな付加価値をご提供します。

6.　@CELL LAN で変わるオフィス・ワーク

これまでご紹介してきた特性を活かすことで、@CELL LAN は、次のようなオフィス・シーンを演出します。

■ オフィス･デスクでの利用

通信シートをデスクに置く（デスク天板に通信シートを内蔵した製品も発売されています）。 無線 LAN 機能を持つノート PC をその上に載せるだけで、社内のネットワークにつながります。デスクの美観を損ねることはありません。また、移動にもコネクターの抜き差しは不要です。オフィス・レイアウトの変更に伴う配線工事も不要です。

また、複数テナントが入るビルにオフィスを構える場合は、他社への電波の漏えいも心配です。このようなリスクを回避しつつ、無線 LAN の持つ機動性を発揮することが可能です。

■ 会議室での利用

不特定の人数が集まる会議室。 ネットワークに接続できることは、常識です。しかし、機密性の高い情報がやり取りされることも多く、セキュリティには、大いに気を使います。しかし、LAN ケーブルが、会議テーブルの上に放置されている光景は、お客様も同席される会議室では、見苦しいものです。また、ケーブルの抜き差しによるコネクターの損傷も少なくありません。また、席を移動することもしばしばの会議で、有線 LAN は、不自由です。@CELL LAN は、このような会議室に接続の自由度と美観、セキュリティをすべて満足する最適なソリューションを提供いたします。

■ 応接室での利用

来客者にネット接続環境を提供する。 このような便宜の供与は、来客者の満足度を高め、自社の評価を高めることにもつながります。しかし、社内ネットワークを介したアクセスは、セキュリティ・リスクを高めることになります。そこで、応接室のような来客者を前提とするスペースでは、@CELL LAN を設置して、インターネット接続環境だけを提供することも可能です。

7.　@CELL LAN によるセキュリティ対策

@CELL LAN と無線 LAN の主な相違点として、電波の到達範囲の違いが挙げられます。
無線 LAN では広い範囲で安定した通信を広確保するために電波をより遠方へ飛ばす技術に注力してきた傾向がありましたが、逆に電波を遠方へ飛ばすことで、電波干渉による影響の増大やセキュリティ・リスクの増大など様々な問題も浮かび上がってきます。

@CELL LAN では、通信シートから離れた場所からは AP の電波が届かないために、ネットワークに接続することは不可能です。したがって、接続パスワードを知っていても外から接続することはできません。ネットワークに接続されて情報が盗まれるリスクはありません。
これに対し無線 LAN の場合は、接続パスワードを知っている悪意あるものが、電波が届くエリアからネットワークに接続して情報を盗むことが可能です。

@CELL LAN 専用のアダプタではなく、PC 内蔵の無線 LAN アダプタや通常の無線 LAN カード等を利用した場合、PC（内蔵の無線 LAN アダプタや無線 LAN カード等）から送信する電波は、遠くまで飛散するため傍受される可能性があります。そのため、暗号なしでは情報が漏えいするリスクがありますし、WEP による暗号化も暗号解読ツールで解読されて情報漏えいする可能性があります。
無線 LAN と比較して@CELL LAN は

・AP の送信電波は受信されないので暗号解読に必要な大量データを採取されにくい
・解読されても（外部から）ネットワーク接続が不可能である

などリスクは低くなりますがまだ安全ではありません。しかし暗号化に接続パスワードを盗まれても送信データの解読が不可能な AES を使った WPA/WPA2 を用いれば安全です。
無線 LAN の場合は、WAP/WPA2 を暗号化に使用しても、接続パスワードが盗まれる（あるいは見破られれば）ネットワークに接続され、例えばデータベースから大量の個人情報が盗まれる等の情報漏えいが発生する可能性があります。

安全であることを説明するためには、無線 LAN の場合は、接続パスワードの管理体制や認証サーバの必要に応じた厳格な更新等の管理を実施していることの証明が必要です。これに対し@CELL LAN の場合は、前述のことから安全であることを明快に説明することができます。

ネットワークにおける認証は、接続するべき正当な相手であるかを確認する手続きのことです。通常は「ネットワークに接続する端末」が正当であるかという確認を、「接続されるネットワーク機器」が行う手続きです。誰がどこから接続するか分からない状況、例えばインターネットを経由して接続したり、無線 LAN を使用して接続するような状況においては、認証は必須になります。
限られた場所からのみ接続が可能なネットワークの場合、「その場所に存在すること」が正当で

あることを他の方法によって保証される場合は、認証は必須ではありません。例えば、セキュリティコントロールされた部屋あるいはオフィスの内部では、入り口で既に正当な権利を持ったものであることが確認・保証されているので、内部にいる限りは再度認証する必要がない、といったケースがあります。

ネットワーク接続における認証は大きく分類して次のような手法があります。

・MAC アドレス等（機器固有のデータ）を用いる方法
・ID およびパスワード（知っている情報）を入力させる方法
・証明書（認証局が発行した証明書および秘密鍵データ）を用いる方法

機器固有のデータを用いる方法では、設定が面倒なことがありますが、以後は意識することなく利用できます。ただし、そのデータも詐称される危険性があります。
ID およびパスワードは、簡便な方法ですが、盗まれて用いられる可能性があり、その安全な管理の課題があります。
証明書を用いる手法は、より信頼できる方法ですが、仕掛けが大掛かりです。

@CELL LAN は、インターネット経由や無線 LAN と異なり、接続している人が見えて判りますので、「その場所にいること」自体によって認証が完了している場合は、基本的にはネットワークとしての認証は不要です。しかし、トータルのシステムとして認証の仕掛けがあり、それを用いる場合には、場所による認証とネットワーク認証の二重の確認が行われていることになり、より安全です。

暗号技術は、必要な人以外には内容が分からないようにして、データ通信あるいはデータ保存を行う技術です。最近は 2 つの鍵のペアで暗号化・複号化を行う特別な暗号技術を使って電子署名、証明書といった ICT（情報通信技術）社会に必要なインフラを実現する公開鍵暗号もあります。

・共通鍵暗号：1 つの鍵でデータや通信が第三者に分からないように暗号・復号する
・公開鍵暗号：公開鍵・秘密鍵のペア（2 つ）の異なる鍵を持ち、電子署名等に使用する

暗号技術に基づいた仕掛けが安全であることは、暗号解読に要する計算時間が膨大であるために、現実のコンピュータでは実質的に解読不能であることを安全性の拠り所としています。しかしながら暗号の研究により、特別な解読方法で現実的な解読時間で解読することができることが発見されて、ある暗号アルゴリズムが安全でなくなることも起こりえます。

現在の ICT 社会では、「安全な通信」や「個人や機器の特定」のために暗号技術が用いられており、その安全性を評価する公的機関 CRYPTREC があります。CRYPTREC では、推奨暗号をとして安全な暗号のリストを公開しています。

無線 LAN で使用されている暗号として次のものがあります。

・WEP：従来使用されてきた暗号。解読手法が発見されて現在は安全ではないとされている
・TKIP：WEP を用いて暗号鍵を定期的に変更するが、基本的に WEP と同等
・AES： 米国および日本の公的機関が現在安全として推奨する暗号

昨今メディアでも報道されているように、WEP は高速な解読方法が発見されて「安全ではない」とされています。 AES は暗号の安全性評価の公的機関で評価されて推奨されています。

@CELL LAN では、前述の「クライアント・アダプタ」の様な PC 側にも専用のアダプタを用いて電波飛散を抑えた場合は、原理的に暗号の必要はありません。PC 側に専用のアダプタを用いない場合は暗号化が必要であり、安全な AES の使用を推奨します。

8. まとめ

@CELL LAN（アットセル・ラン）は、無線 LAN の持つ利便性と有線 LAN のような高度なセキュリティを同時に享受する手段として開発された新しい LAN システムです。 無線 LAN の持つ「脆弱性」の根源である「電波によるアクセス」をオフィス・デスクあるいは、会議テーブルのごく近傍に限定し、それより外部からのアクセスを遮断することで、これを実現します。

簡単に言ってしまえば、ノート PC をデスクやテーブルに置いたときだけ（LAN ケーブルは必要ありません）、ネットワークにつながるのです。ですから、隣の部屋や外の廊下、屋外からネットワークへ侵入することは、有線 LAN 同様に物理的に不可能となります。

つまり、「保護されていない通信経路」が、外部からは物理的に遮断されることから、仮に悪意のあるものが、パスワードを知っていて、外部からアクセスしようとしても、アクセスポイントからの電波が届かない、つまり、「外部からアクセスされやすいネットワーク環境」という「脆弱性」が存在しません。このため、「通信への侵入」や「ネットワークへの不正アクセス」、「盗聴」といった「脅威」が排除されることになるのです。

@CELL LAN は、このように無線 LAN の持つ「脆弱性」を無くし、有線 LAN と同等のセキュアな LAN 環境を実現します。加えて、物理的な結線の無い無線 LAN 同様の「利便性」を享受することができるという、今までにないまったく新しい LAN 構築のソリューションなのです。

リスク・スコア表

脅威の評価		低			中			高		
脆弱性の評価		低	中	高	低	中	高	低	中	高
資産の価値	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

@CELL LAN では，物理的な脅威が存在しないため、脆弱性、脅威ともに低く評価されます

仮に暗号化等の対策がなされていても、物理的な経路が存在するため、人為的な脅威を完全に排除することはできません

十分な対策がとられない場合、脆弱性、脅威共に高く評価されます

情報セキュリティ対策に真摯に取り組まれている企業、さらには、ISMS の認定取得を目指されている企業の皆様にとっては、新たな選択肢を手に入れることができるのです。

以上