

はかる 計・測・量 (8)

情報セキュリティをはかる

菅 沼 賢 一 三機工業(株)

キーワード：情報セキュリティ(Information Security)

1. 情報セキュリティの重要性と最近の動向

1.1 IT化が進む社会

1990年代になると急速に各企業のIT化が進み、ここ数年ではブロードバンド(ADSL, FTTHなど)の低価格化なども後押しして一般家庭でも普及が進んでいる。E mailなどはビジネスにおいて不可欠になり、メールを見ることができない環境にいると不安にさえなるほどである。インターネットなどは、一般家庭では調べ物や、遊び情報、買い物、画像や動画の閲覧が増え、企業では他社のリサーチ、世間動向などの調査、自社サイトの構築、公共物件の入札などインターネットを取り巻くビジネスが盛んとなっている。

また、住基ネットでの公的文書の入手、公共施設の予約なども行えるようになっていくなど、IT化が今後の暮らしの前提になっていく風潮となっている。

1.2 情報セキュリティとは

情報セキュリティと聞くと一般的にファイアウォールを設置したり、ウイルス対策ソフトを入れたりすることだという回答が返ってくる。実はそれだけにとどまらず、それに伴うそれぞれの環境に対するセキュリティも範ちゅうに入ってくる。それは外部からの脅威から情報資産・資源を保護することすべてを表す。一言で表現をすれば「情報を守る」ことになり、そのなかには次の三つの内容が含まれている。

- 1) 機密性：情報の内容を漏洩しないように機密を保つこと。情報により機密レベルが変わる。
- 2) 完全性：その情報が完全なものであること。すなわち、その情報が改ざんや隠匿されていないかを保障する。
- 3) 可用性：必要なときに、必要な人が、必要な情報を取り出せること。

1.3 セキュリティを考慮する相手

(1) 外部からの攻撃

外部から送られてくるメールによるウイルスの蔓延や、ハッカーによるネットワークの不正侵入などもこれにあたる。

ウイルスにはウイルス対策ソフトを導入することによりある程度の防御はできるが、新しいウイルスに対しては有

効ではなかったり、ウイルスパターンと呼ばれるウイルス情報ファイルを更新していなければ効果はない。

ハッカーによる不正侵入については、ファイアウォールと呼ばれる悪意を持った侵入を防ぐ機器やソフトを使い防御を行うことができる。

ただし、これらに対しては完全に防げるものではなく、攻撃者と防御者のいたちごっことなっているため、100%の精度を保つことはできない。そのため数種類の防御策をたてたり、ソフトウェアのアップデートを随時行い極力最新の状態にすることが必要となっている。

(2) 内部からの漏洩

企業にとっては、外部攻撃よりも影響が高いのはこの内部からの漏洩といわれている。情報漏洩のパターンには数種類あるが、代表的なものは「内部関係者によるデータの持出し」と「データ管理者の知識・意識レベルの低さによる盗難」が挙げられる。内部関係者のデータの持出しは某大手コンビニエンスストアのクレジットカード会員情報が流出した事件があった。これは2003年6月頃に管理・運営している外注会社のコンピュータから会員情報56万件が抜き取られ、名簿業者に売られていた事件で、不審な手紙が送られてきたという会員からの連絡を受け調査し発覚したものである。原因はいまだはっきりしていないものの外部委託に頼りすぎていること、ポリシーを徹底できていなかったことも大きく起因していると思われる。

データ管理者の知識・意識レベルの低さによる盗難は、インターネット上での情報発信や情報収集(アンケート・懸賞など)が少ない予算で効率的にマーケティングや顧客情報が収集できることから活発になってきている半面、比較的簡単に顧客情報が集まるため、情報セキュリティに対する認識の甘さから情報が流出している事例がある。実際には、昨年ごろから大手パソコン販売サイトや、某エステ会社のサイトにおいて、インターネット上で外部から見る事ができる場所に顧客情報があり、それを見つけたユーザーがその情報を抜き取り、ファイル交換ソフトなどで不特定多数に配布してしまった事件があった。

これらの情報は、不当な金額請求や不可解なダイレクトメールを送付することに利用され、実際に金銭的な被害を受ける場合が少なくない。そればかりか精神的な打撃など

表-1 電磁波の種類と利用例

	種 類	周 波 数	波 長	利 用 例
放 射 線 (電離放射線)	ガンマ線(γ線) エックス線(X線)		1/10 000 000 mm 1/100 000 mm	医 療 材料検査 X線写真
光(太陽光)	紫 外 線 可 視 光 線 赤 外 線 遠 赤 外 線		1/10 000 mm 1/100 mm 1/10 mm	殺 菌 灯 光 学 機 器 赤外線ヒータ
電 波 (非電離放射線)	マイクロ波 サブミリ波 ミリ波(EHF) センチ波(SHF) 極超短波(UHF) 超短波(VHF) 短波(HF) 中波(MF) 長波(LF) 超長波(VLF)	30~300 GHz 3~30 GHz 300~3 GHz 30~300 MHz 3~30 MHz 300~3 MHz 30~300 kHz 3~30 kHz	1 mm 1 cm 10 cm 1 m 10 m 100 m 1 km 10 km 100 km	光通信システム レーダー 電子レンジ, 携帯電話 警察・消防通信 FM放送, テレビ放送 アマチュア無線 AM放送 船舶・航空機用通信 電磁調理器
電 磁 界	超低周波(ELF)	50~60 Hz	6 000 km	送電線 家庭電化製品

により、被害者の社会生活にまで影響を及ぼしかねない問題となる。もちろん、流出させてしまった企業にとっても信用問題となり、会社存続事態危ぶまれる例もでてきている。

(3) 災害などによる事故

地震・洪水などによる天災や、火の不始末などの失火でのデータ紛失をさしているが、これらの対策もセキュリティの一つとなる。一般的には、バックアップ媒体や筐体を距離的に離れた場所に設置したり、専門の保管会社に委託するなどの対策をとる。

2. 情報社会における脅威

2.1 電磁波における脅威

(1) 電磁波とは

電磁波とは電気と磁気が相互に作用して発生するエネルギーの波のことで、大きくは放射線、太陽光線、電波、電磁界の四つに分けることができる。放射されて進む一つの波の長さ(距離)を波長といい、1秒間に繰り返される波の数を周波数という(表-1)。

電磁波の中で、太陽光線より波長の短いものを放射線といい、ガンマ線やエックス線がそれに該当する。また、太陽光線より波長の長いものを電波といい、波長の長さに応じて極超短波、短波、中波、長波などと分類される。家庭用電源に使われる周波数は50 Hz、もしくは60 Hzだが、100 Hz以下の超低周波は空中を伝わらないため、いわゆる電波とは区別され、電磁界と呼ばれている。

(2) 電磁波の影響

よく“電磁波が体に何らかの影響を及ぼす”として話題に

なるが、正確にいえばすべての電磁波を問題にしているのではなく、送電線や一般の電化製品から放射される極低周波の交流電流から発生する磁界と、携帯電話や電子レンジなどから放射される極超短波(300 MHz~3 GHz)が問題となっている。

もちろん、周波数の非常に高い放射線を大量に浴びてしまうと、そのエネルギーの大きさからDNAなどの遺伝子を傷つけてしまう可能性があるし、太陽光線の紫外線も大量に浴びると肌が黒くなり、次第に皮膚を痛め、やがて皮膚がんになるという報告もされている。以前から携帯電話の電磁波(電波)が人体に及ぼす影響について長らく議論が行われてきたが、現在利用されている周波数では“脳腫瘍の原因にならない”との発表が総務省よりなされた。

(3) 電磁波の新しい脅威

電磁波は人体に与える影響以外にも盗聴や攻撃などが取りざたされている。そもそもこの技術は数年前に米国国防省が開発したものがベースとなっており、国家機密レベルであったため機器としては非常に高価なものだったが、最近ではある程度の知識を持った技術者であれば、簡易なものであれば個人レベルでの制作も可能になってきたともいわれている。さらにOSの脆弱性や、物理的な盗難などに対する意識が高まったため、新たに電磁波が脅威を与える手段として利用され始めたという背景もある。この脅威の具体例としては、電磁波を離れた場所で傍受する“電磁波盗聴”や、情報機器を狙った“電磁波攻撃”がある。電磁波盗聴は、情報機器がVCCI規制値を守っていても、極弱い情報を含む電磁波を発して、ケーブルがアンテナの役目をして外部に漏洩している。その電波を特殊な装置を使

い傍受，再生し盗み出している。また，電磁波攻撃とは建物内や極近隣に侵入し，特殊な装置を使い電磁波を発生，侵入させ情報機器を誤動作させることをさす。一見電磁波攻撃は被害が少ないように思えるが，数分に一度 PC が再起動するなどをおこせば十分業務に支障を与えることが可能である。

そのため，これらの脅威に対するため新情報セキュリティ技術研究会は各省庁などが進める情報セキュリティ政策を踏まえ，2003年6月に「電磁波セキュリティガイドライン」のドラフトを作成し，同研究会のサイトで発表している。新情報セキュリティ技術研究会は，2001年9月発足した国内41社が参加している民間団体で情報セキュリティ確保のニーズが高まるのを受けて，電磁波セキュリティの必要性を訴えこのガイドラインの完成を目指している。

今回ドラフトが発表された「電磁波セキュリティガイドライン」では，必要な測定方法や建築工事設計基準などについてまとめられ，2003年度中には漏洩電磁波の基準値など具体的な項目のまとめを進めて完成をする予定となっている。

(4) 電磁波の測定単位

電磁波を測定する場合の単位は，電磁波の種類(低周波か高周波か)によって違ってくる。それは周波数の違いにより電磁波の性質が違ってくるので，一つの単位で比較することができないからである。低周波の場合は一つの波(波長)が大きいので電場と磁場を分けて測定するため磁場(ガウス or テスラ)と電場という単位で表し，高周波の場合は電場と磁場が一体化しているので電力密度という単位で表す。

a 磁場の単位(低周波)

ガウスというのは磁束密度の国際単位で，1平方センチメートルあたりの磁力線の数をさす。1997年10月1日から磁束密度の国際単位はガウスからテスラに変更された。ちなみに地球上では平均50マイクロテスラの磁場があって，極地(北極や南極)に近づくほど高くなっている。N極とS極は動かないので静磁場という。

$$1 \text{ G (ガウス)} = 0.1 \text{ mT (ミリテスラ)}$$

$$1 \text{ 万 G (ガウス)} = 1 \text{ T (テスラ)}$$

b 電場の単位(低周波)

電場の強さを表す単位は「キロボルト/メートル [kV/m]」や「ボルト/センチメートル [V/cm]」を用いる。低周波の電磁波問題は磁場のガウスが基準となることが多いが，電場の人体への影響も懸念されている。

$$1 \text{ kV/m} = 10 \text{ V/cm}$$

c 電力密度の単位(マイクロ波)

携帯電話や電子レンジで利用されるマイクロ波の単位に

ついては，電場と磁場が絡み合った状態ででてきている。1平方センチメートルの面積に何ミリワットの熱量が通過したかで考える。これは電磁波の伝わる方向に対して垂直な単位断面積あたりの通過電力(単位:[mW/cm²]など)となる。

(5) SAR

SAR(Specific Absorption Rate)は，電波の平均エネルギー量を表す比吸収率のことで，電波が人間の健康に影響を及ぼさないよう，科学的根拠に基づいて定められた技術基準である。この基準値は周波数単位に定められていて，2002年には携帯電話などの発する電波について新たに制度が法制化された。この値は「電磁界にさらされたことによって任意の生体組織10グラムが任意の6分間に吸収したエネルギーを10グラムで除し，さらに6分で除して得た値」と規定されている。日本国内では国際非電離放射線防護委員会(ICNIRP)のガイドラインにそって許容値は2W/kgとなっていて，米国で許容値は1.6W/kgとなっているなど各国で足並みはそろっていない。しかし，日本国内で発売されている携帯電話は0.3~0.7W/kgと許容値を大幅に下回っているため問題とはならない。

国際ガイドラインによると人体への影響は，携帯電話の数十万台に相当する，138kW/kg相当の電波を2時間から3時間，眼球に浴びた場合に白内障を生ずると報告されている。

(6) 電磁波の測定機器

機器には幾つもの種類があり，測定する対象の周波数や出力により使い分けている。磁力には方向性があるため機器のセンサの数により精度が変わり，センサ数が多いほど精度が高くなる。

- 1) ガウスメータ：主に高圧線，配電線，変電所，家電製品などの磁場を計測するための機器。
- 2) フィールドメータ：電子レンジや携帯電話などマイクロ波の電力密度を計測するための機器。
- 3) マイクロアラート：携帯電話の基地局などの電力密度を計測するための機器で，マイクロワット単位での計測を行う場合に使用する。

2.2 通信による脅威

(1) パケットとは

コンピュータ通信において，送信先のアドレスなどの制御情報を付加されたデータの小さなまとまりのことをいい，データをパケットに分割して送受信する通信方式をパケット通信と呼ぶ。データを多数のパケットに分割して送受信することにより，ある2地点間の通信に途中の回線が占有されることがなくなり，通信回線を効率よく利用することができる。また，柔軟に経路選択が行えるため，一部に障害がでて他の回線で代替できるという利点もある。

(2) 通信を利用した脅威

通信を利用した脅威は、あまり知識がなくてもインターネット上からどこからでもできるレベルのものから、高度なものまでさまざまな種類がある。

a メールボム

大容量のメールを送りつけたり、CCで大量のメールを送りつけるなどで相手のネットワークの負荷を高めたり、メールサーバをパンクさせたりする行為。この対策としてプロバイダや企業のメールサーバ上でメール受信の容量制限や、同一相手からの受信制限が行われている。

b DOS攻撃

ネットワークを通じて相手のコンピュータやルータなどに不正なデータを送信したり、ネットワーク負荷を高くしてダウンさせる攻撃。また、最近では分散DOS攻撃が増えている。これは世界中で流行したブラスタウイルスが有名な例で、ウイルス(不正なパケットを出すプログラム)をコンピュータに忍び込ませて、そのコンピュータの利用者も気づかないまま内部のネットワークに攻撃を仕掛けるものである。

c パケットスニффリング

ネットワークを流れるパケットを盗聴し、そこからIDやパスワードを拾い出すことをいう。“パケット盗聴”とも呼ばれ、パスワード以外にもメールの盗聴などが行われることもある。多くのネットワークでは管理の必要から、管理者はネットワーク内のパケットを自由にみるようになるようになっていて、悪意を持った人物が管理者権限を手に入れた場合、ネットワーク内部から外部へアクセスしている人物のパケットを盗聴し、さまざまな情報を知ることが可能である。また、ネットワークによっては管理者でなくとも盗聴が可能な場合があり、注意が必要となる。

パケットスニッフリングへの対抗手段は、通信経路の暗号化や定期的なパスワード変更が一般的で、インターネットなどの開かれたネットワークでは、どこで誰がパケットを盗み見ているかわからないため、暗号化できないTelnetやFTPなどのアプリケーションは使用すべきでないといわれている。

(3) 通信の脅威に対する防御策

一般的にはウイルス対策ソフトの導入やファイアウォールなどの設置などが挙げられるが、これらはすでに起きた脅威に対する防御策のため、新しいものに対する効力はなくそれだけでは完全とはならない。また、ウイルスだけではなくメールボム的なものであればサーバの利用HDD領域の監視や、随時パケットの監視などを行わなければならない。

社内のシステム部門における運用では、コスト面や人的負担が大きい一括してアウトソーシングするなど対応

する企業が増えている。

(4) 新たな通信の脅威

企業内で無線LAN設備が増え始めるとともに、電波を盗聴したり不正にアクセスをするなどの脅威が取りざたされている。これは電磁波の脅威と似通った印象を受けますが、電磁波の盗聴などよりも比較的安価で容易に行えるためより注意が必要ともいえる。

無線LANは“IEEE 802.11a”、“IEEE 802.11b”といった国際規格に準拠してつくられている場合がほとんどで、この規格が一致していればメーカーを問わず通信ができる。一見便利なようだが、この基準に準拠した無線LANカードを持っていればどこへ行っても通信できることになる。もちろん、これらのセキュリティを保つ方法が幾つかあるが実施されていないケースも目立っている。しかも無線LANを導入する企業や一般ユーザーは、配線などがわからない、配線をシンプルにしたいなどの理由から無線LANを導入する場合があるため、セキュリティ意識が低い場合が見受けられる。逆にセキュリティに配慮できるほどのユーザーは無線LANの導入を見送る傾向にあるのが現状である。しかし、手軽に接続できるためその利便性から駅や喫茶店などでよく見かけるホットスポットの場所が増えている。しかし、そういった場所ではあまり問題となっていないのは携帯プロバイダや店舗の受付からユーザーIDとパスワードを取得する方法が多く利用されているのと、元来見ず知らずの人がアクセスすることを前提としているためユーザーの情報セキュリティに対する意識も高いことが考えられる。

a 電波の盗聴

無線LANの盗聴は、市販のアナライザソフトといわれるもので比較的簡単にできる。このソフトは無線LAN管理ソフトで本来はセキュリティ対策用に使用するものである。これはアンテナ付近でスキャンモード機能を開始するとアクセスポイントが見つかり、そこでやりとりをしているパケットが表示されるだけである。また、無線LANカードに指向性の高いアンテナをつけると、ビル間転送などで利用されるようなものであれば離れた所からの傍受も可能となる。ただし、WEPなどの暗号化をしていけば解読が難しくなる。パケットの暗号化には一般ユーザー向け商品に多く組み込んであるWEP64、WEP128などがあり、これはユーザーが決めたパスワードをパケットの中に組み入れる方式となる。しかし、簡単な暗号化だけだとインターネット上のフリーソフトなどでも解読できてしまうものもあるため、ビジネスユースでは多少不安が残る。ビジネスユースのWPAと呼ばれる暗号化を用いることが多く、認証サーバを利用するなどより高度な暗号化が行える。

表-2 不正アクセス行為の発生状況およびその特徴

	平成 12 年		平成 13 年		平成 14 年		平成 15 年 上半期
	通 年	法施行後 半年 [†]	通 年	上 半 期	通 年	上 半 期	
認知件数	106	35	1 253	959	329	94	114
海外からのアクセス	25	14	448	418	13	4	21
国内からのアクセス	73	20	258	165	286	71	83
アクセス元不明	8	1	547	376	30	19	10

注 [†] 不正アクセス行為の禁止などに関する法律(平成 11 年法律第 128 号。以下「不正アクセス禁止法」という。)の施行日である平成 12 年 2 月 13 日から平成 12 年 8 月 12 日までの間をいう。以下同じ。(平成 15 年 8 月 21 日付警察庁発表資料より)

b 不正なアクセス

無線 LAN のアクセスポイントに接続する場合のセキュリティとして、アンテナ側で MAC アドレス(機器固有番号)をアンテナ側に事前登録したり、ユーザー ID とパスワードを設定するなどがある。企業内の LAN に侵入されると盗聴と同じくパケットの監視などがより簡単に行えるだけでなく、共有フォルダをアクセスされる可能性もでてくる。

3. セキュリティに関連する法規・基準

セキュリティ関連の法規・基準は国内においては指針や規定などがすでに幾つか制定されていて、今後ますます強化されていく傾向にある。また、国際的にはセキュリティの ISO ともいわれ、ガイドラインである BS 7799/ISMS などがある。

3.1 国内における法規・基準

平成 7 年ごろから各省庁から情報システム関連の基準が公示されていて、代表的なものは次のとおりである。

“コンピュータウイルス対策基準”

(平成 7 年 7 月 7 日付通商産業省告示第 429 号)

“情報システム安全対策基準”

(平成 7 年 8 月 29 日付通商産業省告示第 518 号)

“コンピュータ不正アクセス対策基準”

(平成 8 年 8 月 8 日付通商産業省告示第 362 号)

“情報システム安全対策指針”

(平成 9 年 9 月 18 日付国家公安委員会告示第 9 号)

これらは急速な情報化の発展を受けて、国民生活の安全を確保し、情報社会における秩序を維持することを目的として設けた基準であるが、あくまで指針や基準であったため拘束力がない。しかし、2000 年にハッカー対策のための取組みとして、政府機関の防護技術の開発や監視・緊急対処体制の強化、民間重要分野などにおける防護強化の促進などが示され、ハッカーに対する根本的な対策を政府全体で推進することが合意された。それを受けて、情報セキュリティ関係省庁局長等会議において「ハッカー対策等

の基盤整備に係る行動計画」が策定された(表-2)。

3.2 国際社会における基準

(1) BS 7799 の概略

BS(英国規格協会)によって規定されている企業・団体向けの情報システムセキュリティ管理のガイドラインで、セキュリティシステムの運用管理に重点が置かれている点の特徴となっていて、情報資産に対し機密性、完全性、可用性の視点からリスク分析を行い、リスクに基づいて対策措置を設定することを述べている。これは、“BS 7799 1 情報セキュリティ管理実施基準”と“BS 7799 2 情報セキュリティ管理システム使用”からなっていて、BS 7799 1 が国際規格である“ISO/IEC 17799 情報技術 情報セキュリティ管理実施基準”になる。日本では ISO/IEC 17799 を国家規格として採用している。

(2) ISMS とは

ISMS とは「情報セキュリティマネジメントシステム」といい、2002 年、(財)日本情報処理開発協会(JIPDEC)を中心に正式運用が始まった。これは ISO/IEC 17799 などの国際基準を踏まえつつ、情報化社会において安全にかつ信頼性を確保するために第三者適合性評価制度として確立している。

現在、情報セキュリティの問題として、前述にもあるとおり外部からの改ざん、攻撃や内部関係者による情報の漏洩などが存在しているので、それら個別の技術対策はそれぞれのレベルで実施されている。そこで ISMS は、個別問題ごとの技術対策のほかに組織のマネジメントとして、自らのリスク評価により必要なセキュリティレベルを決め、プランを持ちシステム運用をしていくことを目指すものである。

(3) ISMS のポイント

作成したポリシー(方針)をもとに、

1) Plan: 情報資産の特定をし、リスク分析、ポリシー策定、教育訓練の具体的計画、方針を策定する。

2) Do: Plan に基づいて対策の実施・運用

3) Check: 実施した結果の監査を行う(運用監査、シ

ステム監査・監視)

4) Act: 原因を踏まえて経営陣による効果的な対策をたてる

このサイクルを継続的に繰り返し、情報セキュリティレベルの向上を図る。そのため、一度取得して終わりというものではなく、継続的に行うことが必要となる。

(4) マネジメント枠組みの確立

ISMS はリスクマネジメントを行うために、適切なセキュリティ対策に必要な、資源配分を決定し、実施していくものである。そのための決定プロセスを規定する必要がある。それを“マネジメント枠組み”といい、枠組み作成を6段階で行う。

Step 1: 情報セキュリティポリシーを策定する

Step 2: その中で ISMS の適用範囲を定義する

Step 3: Step 1 に基づきリスクアセスメント(評価)を実施する

Step 4: マネジメント枠組みのもとで管理するリスクを決定する

Step 5: 最適なリスク評価に基づき、実施すべき管理策を選択する

Step 6: 適用宣言書を作成し、選択した管理策を公表する

“詳細管理策”として、セキュリティポリシー、セキュリティ組織、情報資産の分類および管理、人的セキュリティなどの項目がある。それらすべての管理策を実施する必要はなく、リスク評価や要求されるシステムの保証の度合いに基づいて選択し、実施できる。このことは企業にとって事業内容や予算に応じて管理策を決められ、より適切な情報セキュリティ管理を可能にする。ここで重要なのは管理策を策定することではなく、Step 6にあるように適用宣言書を作成し明確に公表することであり、リスク評価やリスクマネジメントのPDCAサイクルを回すなかで、さらに適切な管理策が見つかれば、追加・修正していくことが重要になってくる。

ISMSを実施している企業では、今までのような個々の技術対策ではなく人的、技術的、物理的といった面で包括的に情報セキュリティ管理が可能になり、さらに ISMS 認

証を取得することで顧客にも情報セキュリティに対する安全性をアピールでき、わざわざ安全性を説明しなくても信頼関係を向上することができるため、さらなるビジネスの拡大へつながることが考えられる。

4. 情報セキュリティの今後

現在は社会全体でセキュリティの意識が向上してはいるが、法律や企業内規約の整備が遅れているのが現状である。しかし、政府の e-japan 戦略が実現し IT 化が進むと、サイバーテロなどにより何らかの被害を受けたときに個人の生活だけではなく、国家の機能にも重大な支障が及ぶ事態となる。それを受けて、対策や指針なども積極的に打ち出す方向が示されており、数年前から行われている内閣官房情報セキュリティ対策推進室による情報セキュリティ対策推進会議の開催や、経済産業省から“情報セキュリティ総合戦略”が発表されるなど各政府機関は継続的に取り組んでいたり、大学や民間団体も積極的な活動をしている。しかし、民間企業や個人ユーザーまでに周知徹底されることができておらず、今後の課題となっている。これらを推し進めるには、まず提案をする役目である IT 関連ベンダをはじめとするインフラを提案、構築、施工をする立場に立つ企業の意識を向上させ、そこから裾野を広げることが重要となると考えられる。

参考文献

- 1) 総務省“電波利用ホームページ”電波防護指針
- 2) (社)電波産業会(ARIB)ホームページ
- 3) (財)日本情報処理開発協会ホームページ
- 4) 大久保貞利：“誰でもわかる電磁波問題”

(2003/11/26 原稿受理)



菅沼賢一 すがぬまけんいち

生年月日 昭和43年1月23日/最終学歴 東海大学/主な業績 社内システム構築・運用, 社内インフラ構築・運用