資料5－2

次世代の情報セキュリティ政策に関する研究会資料

近い将来の情報セキュリティ

～第四世代移動通信とユビキタスの視点から～

2008年3月06日

（株）NTTドコモ

はじめに

- 目的
  - 近い将来（現在から5年後程度）のセキュリティ問題の議論における話題として、
    - 第四世代移動通信
    - ユビキタスアプリケーション

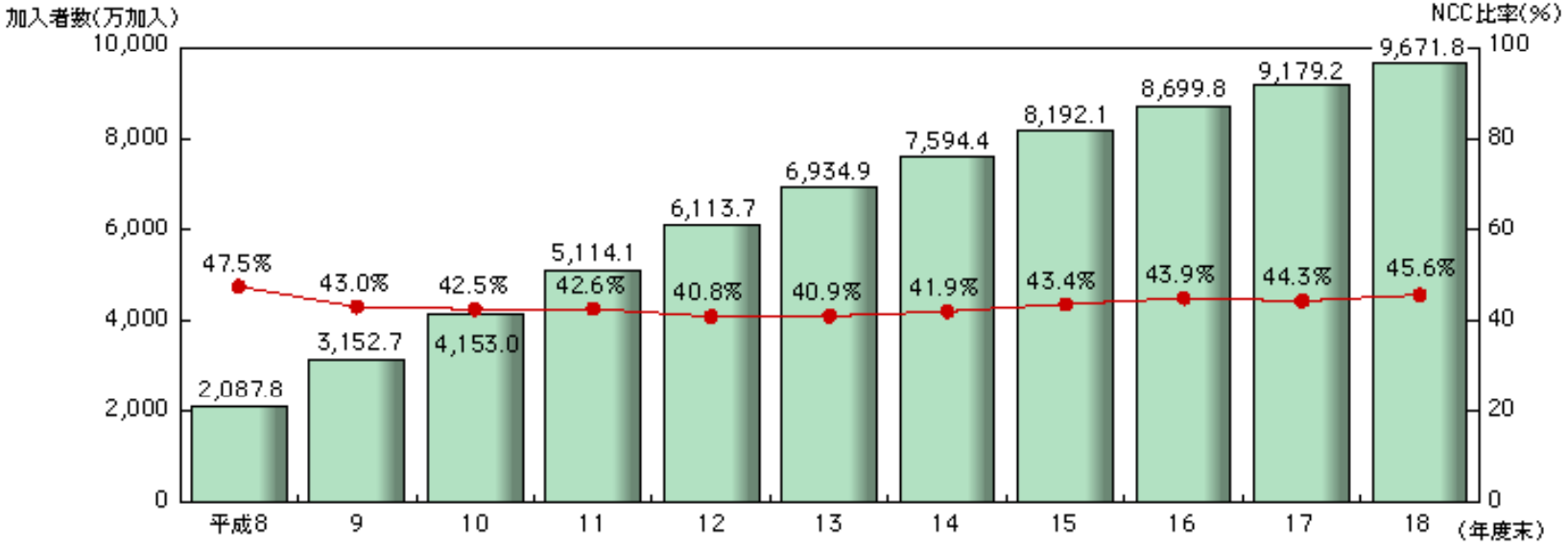
    なる2つの視点から、質的な変化として想定される脅威のトレンドを考察する。

    また、質的に新しくは無いものの、今後、
    - 量的な変化

    として想定される脅威のトレンドについても、併せて考察する。

移動通信の概況

- 平成18年度末における携帯電話の契約数は9,672万件（対前年度比5.4%増）
- 純増数は493万件（対前年度比2.7%増）となっており、6年ぶりに増加



加入者数	2,087.8	3,152.7	4,153.0	5,114.1	6,113.7	6,934.9	7,594.4	8,192.1	8,699.8	9,179.2	9,671.8
純増数	1,067.4	1,064.9	1,000.3	961.0	999.6	821.2	659.6	597.7	507.7	479.4	492.6
NCC比率	47.5%	43.0%	42.5%	42.6%	40.8%	40.9%	41.9%	43.4%	43.9%	44.3%	45.6%

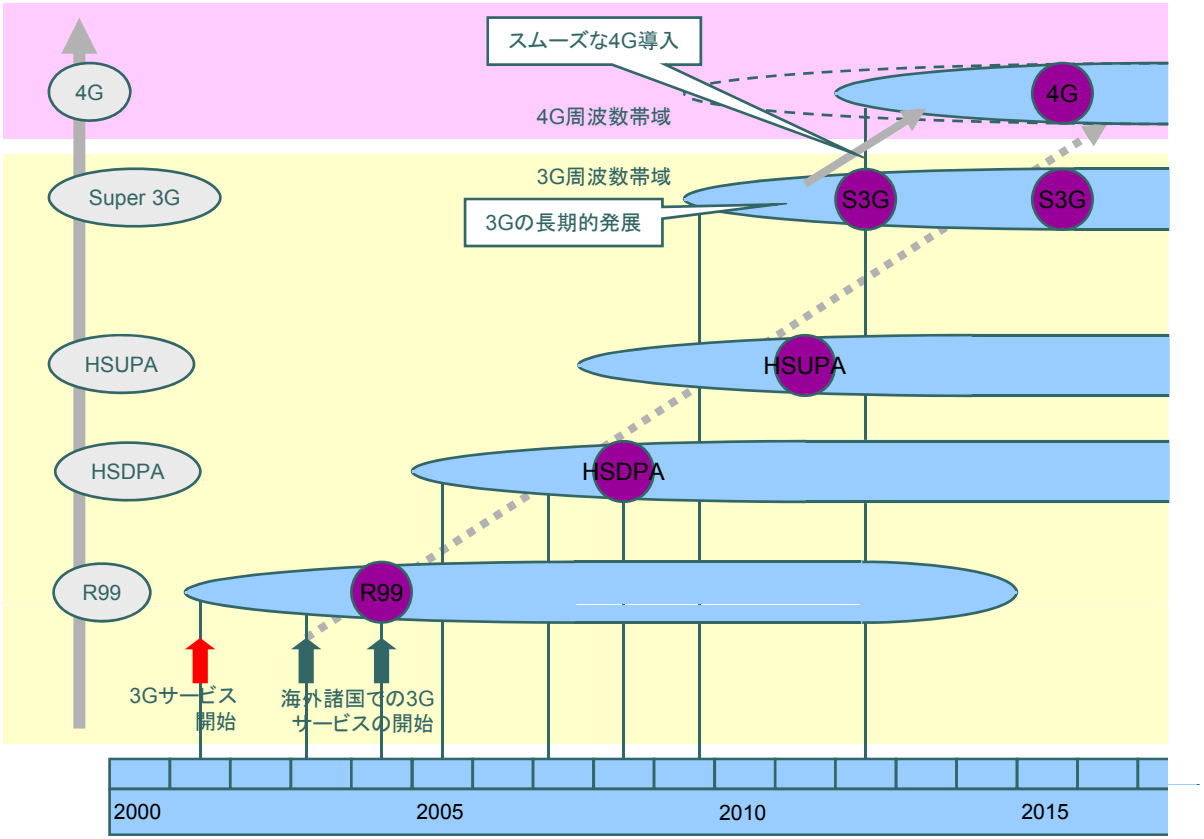
※　過去の数値については、データを精査した結果を踏まえ修正している

社団法人電気通信事業者協会資料により作成

平成19年度版情報通信白書より引用

第四世代移動通信へのシナリオ

- 移動通信の普及に伴い、生活基盤としての役割拡大が期待される
  - 高速通信
  - 低料金
  - サービスエリアの充実
  - サービスの多様性・使いやすさ
- 4Gは、2010年以降の導入を目指し、屋外伝送実験
- Super 3G を介して、4Gへスムーズに導入

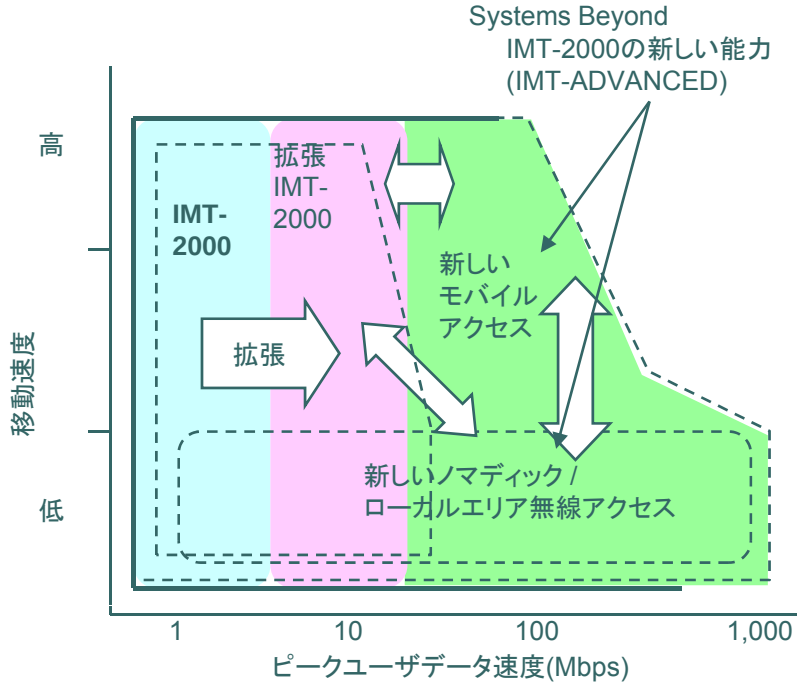


近い将来の情報セキュリティ

1. 第四世代移動通信の視点から
2. ユビキタスアプリケーションの視点から
3. 量的変化の視点から

第4世代移動通信の概要

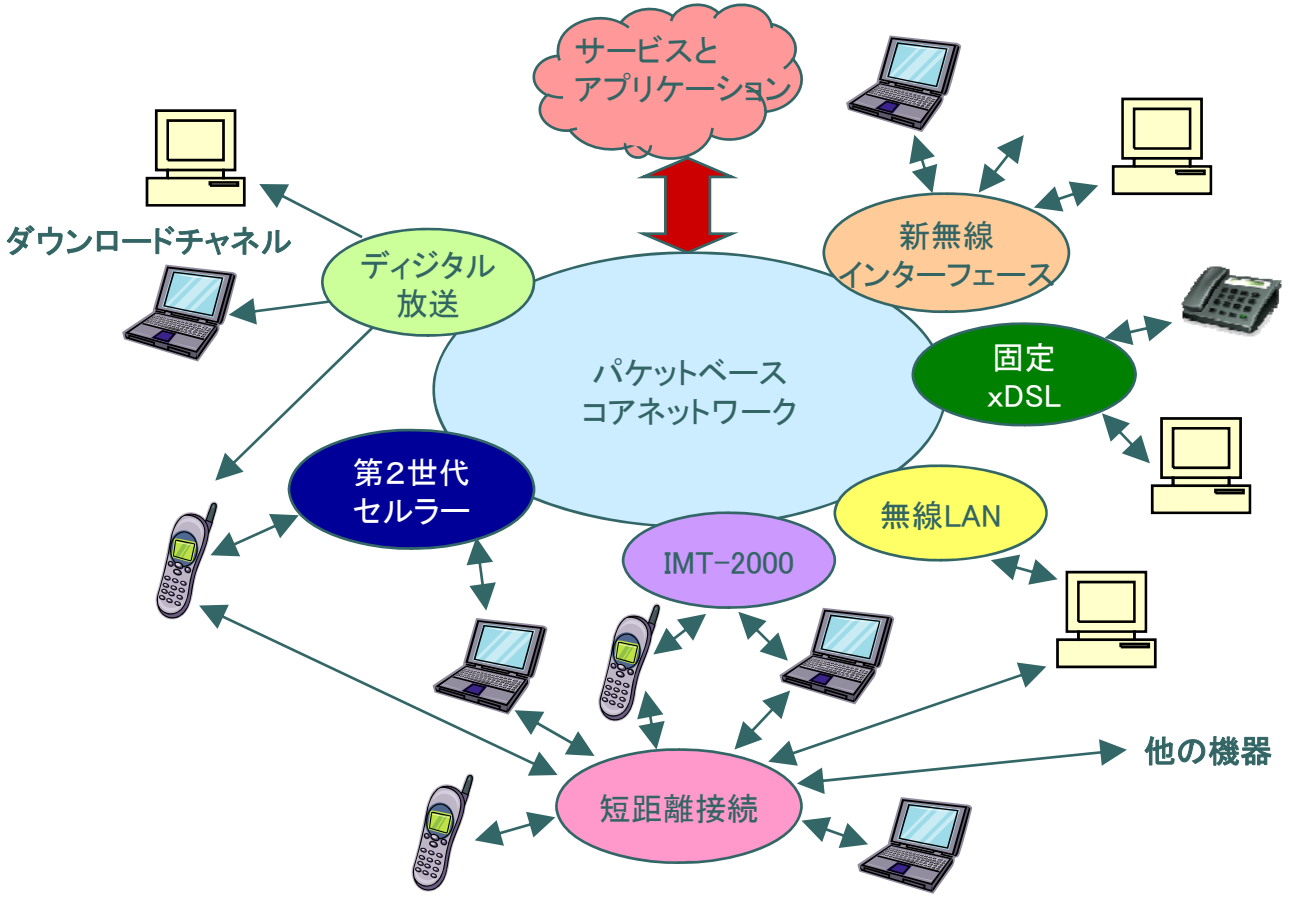
- 2000年のITU World Radio Conferenceから4Gの検討が始まる
  - Systems beyond IMT-2000
- 4GはIMT-ADVANCED
  - 新しいモバイルアクセス
  - 新しいノマディックアクセス 等
- 高速移動で100Mbps、低速移動で1Gbps



Recommendation ITU-R M.1645, Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000 より

各種ネットワークの融合

- 各種無線アクセスを収容
  - 第2世代セルラー
  - IMT-2000
  - 無線LAN
  - デジタル放送
  - 新無線インタフェース
- 固定系のアクセスも収容
  - PSTN（Public Switched Telephone Network）
  - ISDN（Integrated Services Digital Network）
  - x-DSL（x Digital Subscriber Line）
  - FTTH（Fiber To The Home）



Recommendation ITU-R M.1645, Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000 より

想定される脅威

- 端末の脅威
  - 端末のオープン化に伴う不正アプリケーション混入の脅威
- ネットワークの脅威
  - 正当なユーザになりすましての不正利用（不正なサービス享受）
  - 正当なユーザの通信データ／制御メッセージの盗聴（通信内容の奪取）
  - 正当なユーザの通信データ／制御メッセージの改ざん
  - 正当なユーザの利用状況の盗聴（通信事実の奪取）
- ユーザの脅威
  - 接続先ネットワークからの攻撃（マルウェア送信／不正接続 等）
- （脅威ではないが）利便性からの要求
  - 複数のIDの使い分けや、接続の都度認証するのは煩雑

脅威への対策

脅威	対策
端末の脅威 端末のオープン化に伴う不正アプリケーション混入の脅威	**PCにおける対策技術**の適用
ネットワークの脅威 ・正当なユーザになりすましての不正利用（不正なサービス享受） ・正当なユーザの通信データ／制御メッセージの盗聴（通信内容の奪取） ・正当なユーザの通信データ／制御メッセージの改ざん ・正当なユーザの利用状況の盗聴（通信事実の奪取）	相互認証、秘匿、インテグリティチェック、識別子機密 など、従来技術を強化しつつ対応
ユーザの脅威 接続先ネットワークからの攻撃（マルウェア送信／不正接続 等）	ゲートウェイにおける**境界セキュリティ**適用
（脅威ではないが）利便性からの要求 複数のIDの使い分けや、接続の都度認証するのは煩雑	**認証連携スキーム**の導入

端末プラットホームの脅威と対策 ～ PCに学ぶ ～

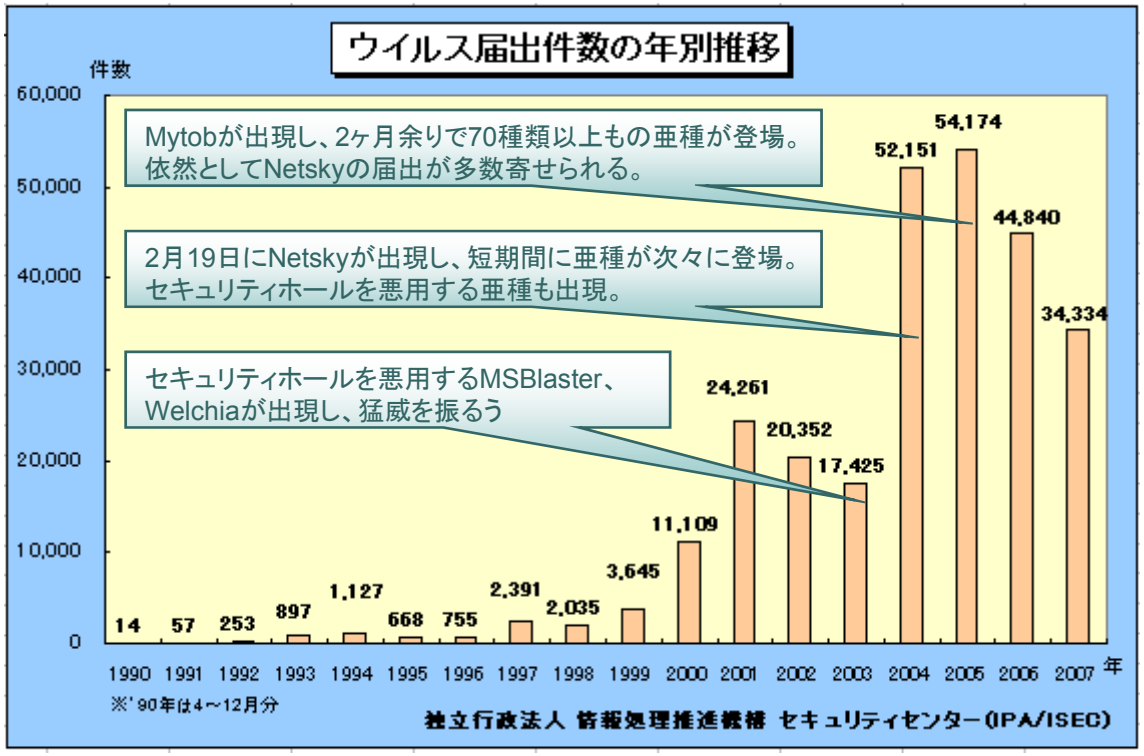
プラットホーム	概要説明	オープン化*の動向	オープン化した場合の主な脅威	脅威に対する対策
Mobile Oriented Applications Platform (Linux) (MOAP(L))	LinuxOSを上のFOMA向けの携帯電話基盤ソフトウェア	未定	・マルウェアの混入 ・データ改竄/破壊/漏洩 ・コンテンツの不正コピー	・アンチウィルス ・アクセス制御 ・ユーザ/権限 認証 ・アプリケーションの認証
Mobile Oriented Applications Platform (Symbian) (MOAP(S))	SymbianOS上のFOMA向けの携帯電話基盤ソフトウェア			
Windows Mobile	Windows Mobile OSを利用した携帯電話基盤ソフトウェア	既にオープン化済み		

*: ユーザが自由にOSレベルのアプリケーションを追加できること

PCにおける対策技術を適用して対処

境界セキュリティ ～ インターネットに学ぶ～ 〔1/4〕

- ウィルス届出件数の年別推移
  - コンピュータウィルス被害の届出は、ここ3年ほど減少傾向にあるものの、高い水準（平均100件/日程度）にある



コンピュータウイルスに関する届出について，独立行政法人 情報処理推進機構 セキュリティセンター(IPA/ISEC) より

境界セキュリティ ～ インターネットに学ぶ～ 〔2/4〕

- インターネット定点観測での不明なアクセス
  - インターネット定点観測(TALOT2)によると、2008年1月の期待しない（一方的な）アクセスの総数は、10観測点で244,657件
  - 1観測点で1日あたり227の発信元から789件のアクセスが
  - 1月の期待しない（一方的な）アクセスは昨年12月よりも若干ながら増加
  - 全体的なアクセスの件数は、定常化

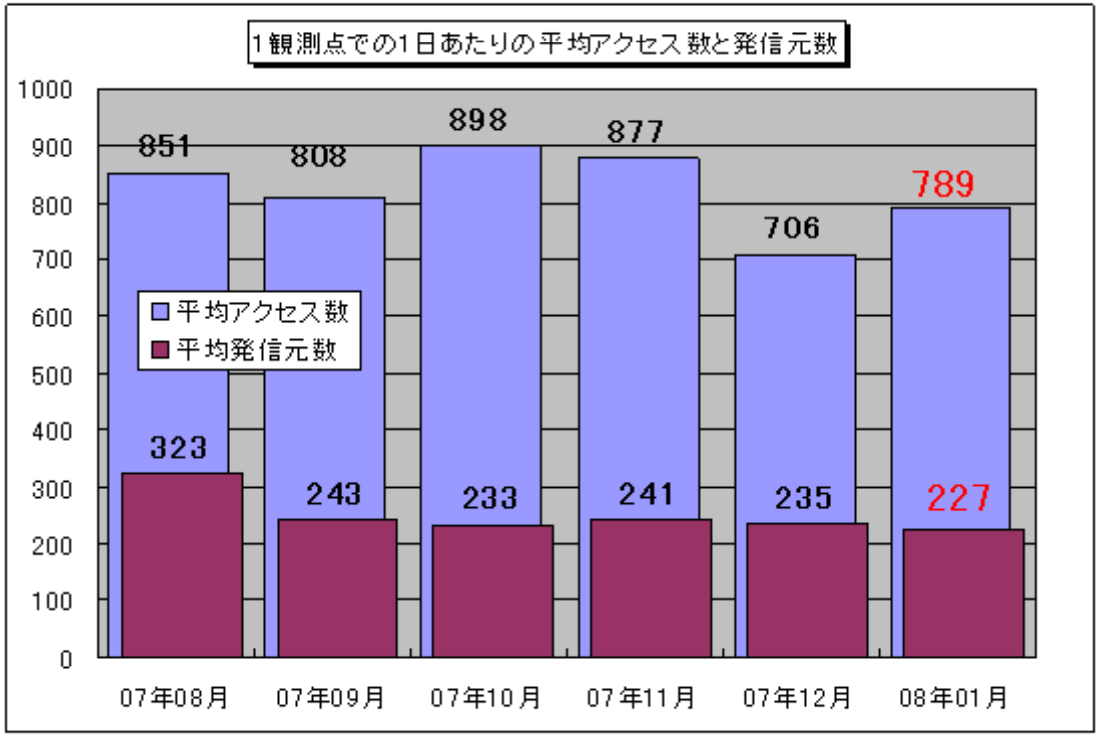


図 5-1: 1観測点での1日あたりの期待しない(一方的な)アクセス数および発信元数

コンピュータウイルス・不正アクセスの届出状況について, 独立行政法人 情報処理推進機構, セキュリティセンター(IPA/ISEC) より

境界セキュリティ ～ インターネットに学ぶ ～ 〔3/4〕

- 脅威
  - サービス停止／妨害
    - ホームページに潜む脆弱性をついた攻撃やサービス不能攻撃(DOS)により、ネットワーク帯域の圧迫やサーバのCPU負荷を増大させることでサイトが提供するサービス機能を麻痺させる攻撃。
  - 盗聴
    - 伝送途中でデータを除き見る攻撃。
  - 不正侵入
    - パスワード管理の不備やセキュリティホールへの対策不備を狙って、サーバの利用者(管理者)権限を奪取して不正にシステムにアクセスする攻撃。
  - なりすまし
    - 不正な利用者権限を用いて、例えばその利用者を騙ってサービスを享受したり、情報送信を行ったりする攻撃。
  - 改竄／破壊
    - 情報を不正に変更してしまう攻撃。
  - 踏み台
    - サーバに侵入し、そこをインターネット上に攻撃を仕掛ける拠点とする攻撃。

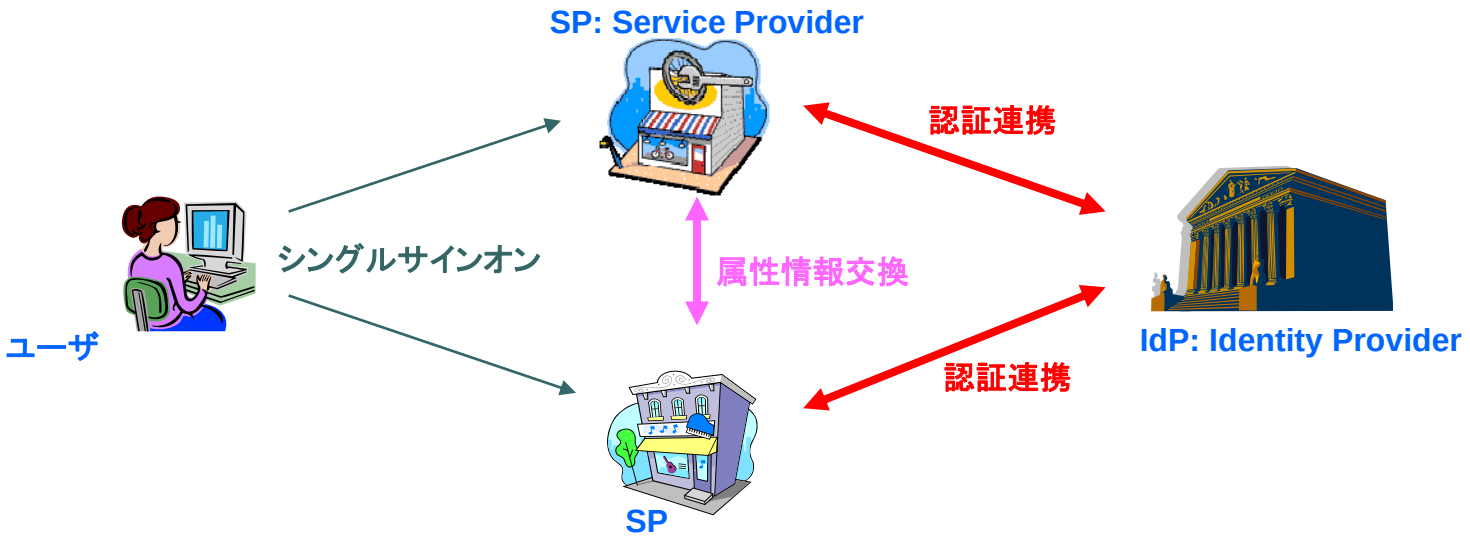
境界セキュリティ ～ インターネットに学ぶ ～ 〔4/4〕

- 境界セキュリティにおける対策分野は大きく4つに分類できる
- 守る対象分野によってセキュリティ対策の方法が異なる
- インターネット技術の利用にはスケーラビリティへの考慮が必要

対象分野	セキュリティ対策	備考
セキュア接続	・ファイアウォール ・IDS／IPS	―
リモートアクセス	・ユーザ認証（／相互認証） ・トンネリング（IPSec，SSL等）	・セキュア接続への対処と一体で提供される構成もある
メールゲートウェイ	・アンチウィルス ・アンチスパム ・メール監査	・メールサーバ自身へのセキュリティ対策も重要
Webゲートウェイ	・Webウィルスチェック ・URLフィルタリング ・Webアクセス監査	・インバウンドのみならず、アウトバウンドへのセキュリティ対策も必要

認証連携の例 ～ インターネットに学ぶ ～

- SAML / Liberty 概要
  - アイデンティティ管理に関係するエンティティ
    - ユーザ
    - アイデンティティプロバイダ（IdP）
    - サービスプロバイダ（SP）
  - アイデンティティ管理に関する仕様
    - 認証連携（SAML[1)], Liberty ID-FF[2)]）
    - 属性情報交換（Liberty ID-WSF[3)], ID-SIS[4)]）

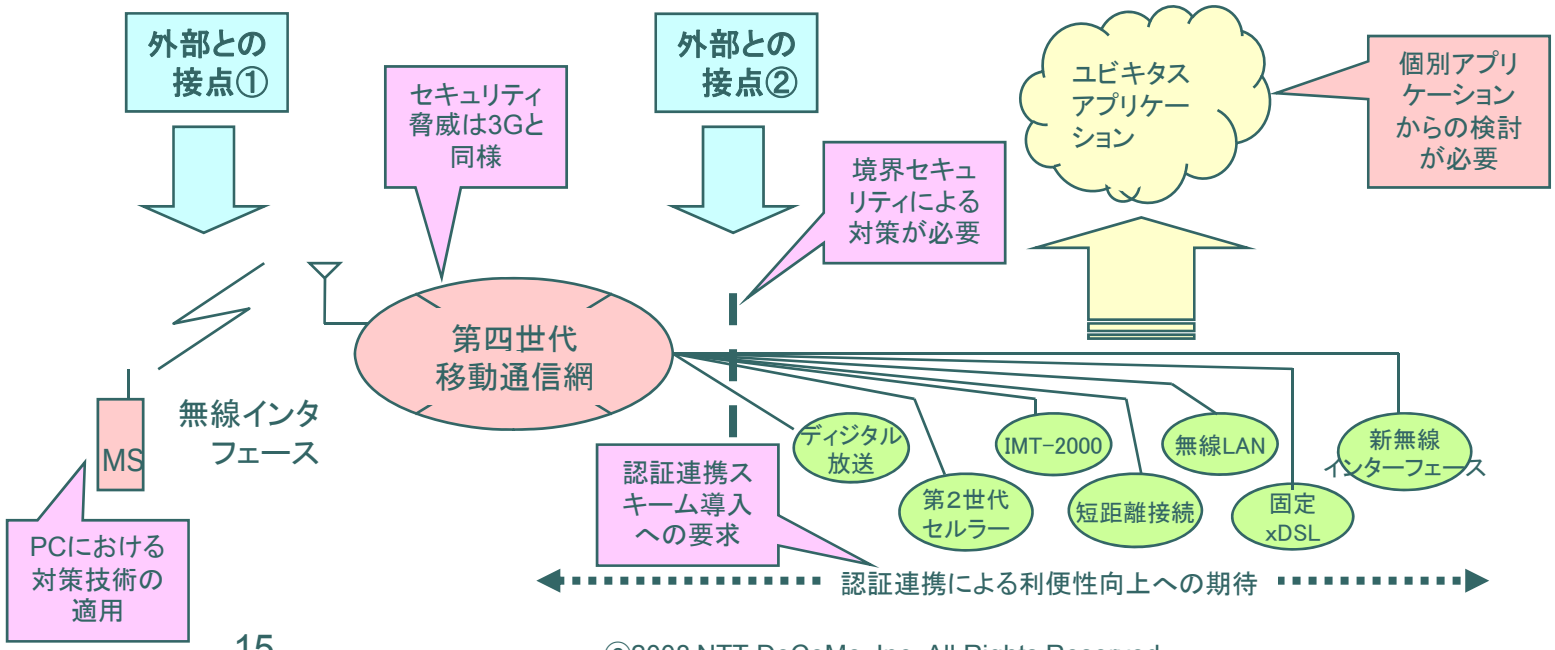


（1）SAML (Security Assertion Markup Language) : シングルサインオンと認証連携のフレームワーク
（2）ID-FF (Liberty Identity Federation Framework) : シングルサインオンと認証連携のフレームワーク
（3）ID-WSF (Liberty Identity Web Services Framework) : 個人属性情報交換のためのWebサービス基盤
（4）ID-SIS (Services Interface Specifications) : ID-WSFと各種サービスとのインターフェース仕様

Liberty Alliance Day 2007 資料, “SAML / Libertyを利用したアイデンティティ連携” より引用

第四世代移動通信のセキュリティ – まとめ

- 4Gネットワークの特徴
  - 高速データ伝送
    - → セキュリティ脅威は3Gと同様（外部との接点①を含む）
    - → 端末プラットフォームのオープン化に伴う脅威
      - → PCにおける対策技術の適用
  - 各種ネットワークの融合
    - → 新たな脅威発生の可能性（外部との接点②）
      - → 他網接続ポイントでの阻止 → 境界セキュリティ
    - → 認証連携スキーム導入への要求
- ユビキタスアプリケーションの展開
  - アプリケーションに依存する脅威発生の可能性
    - → 個別アプリケーションからの検討が必要

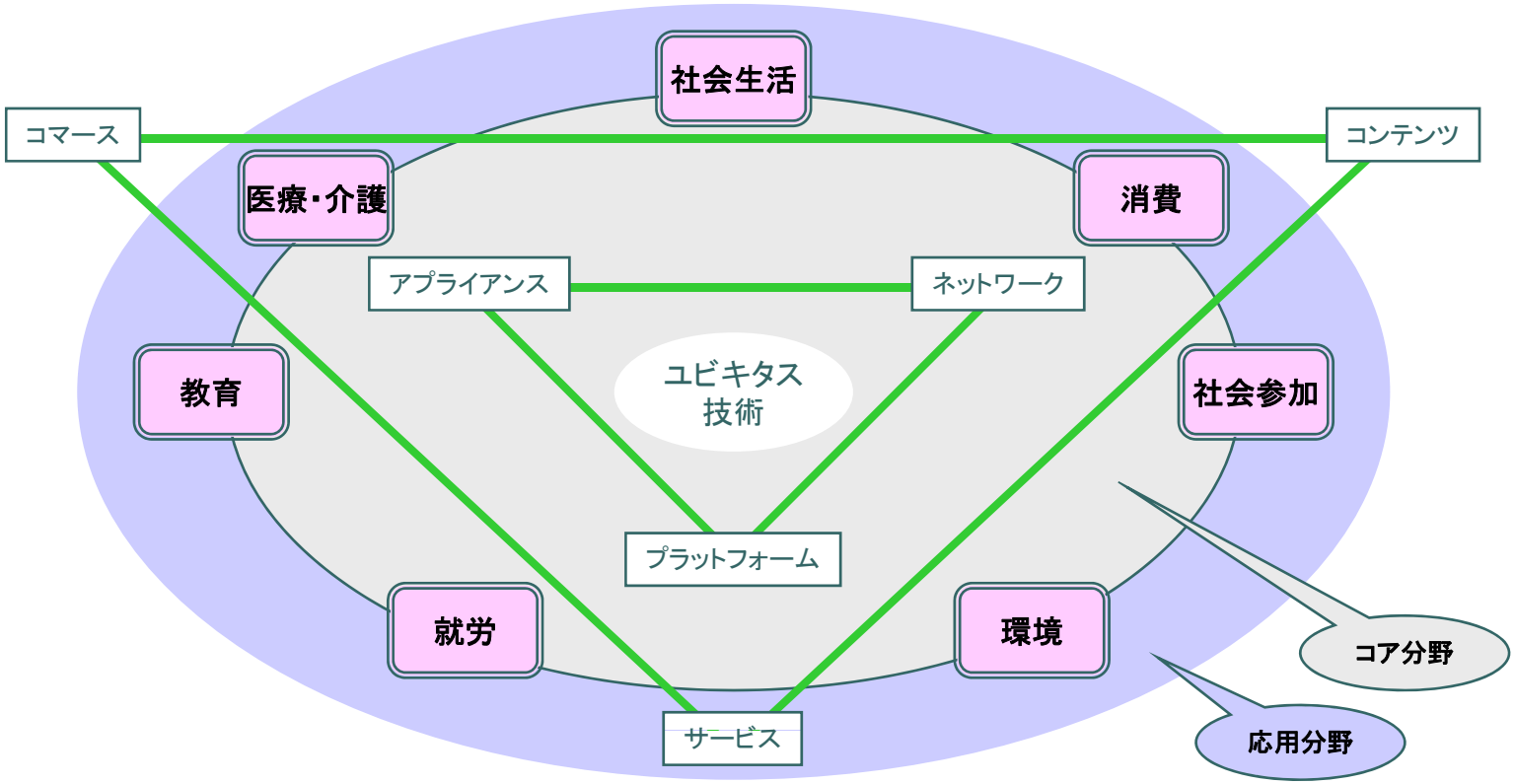


近い将来の情報セキュリティ

1. 第四世代移動通信の視点から
2. ユビキタスアプリケーションの視点から
3. 量的変化の視点から

ユビキタス技術の応用分野

- ユビキタスアプリケーションは以下の7分野に大別できる
  - 社会生活
  - 社会参加
  - 就労
  - 医療・介護
  - 消費
  - 環境
  - 教育



出展：ユビキタスネットワーキングフォーラム

概要とアプリケーション例

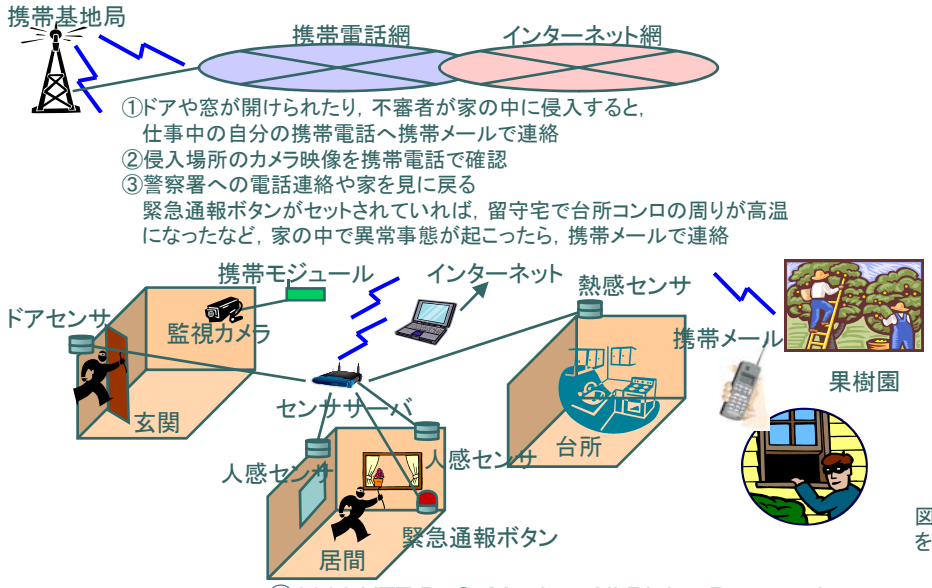
分　　野	概 要 と ア プ リ ケ ー シ ョ ン 例
社会生活	どこにいても適切な情報獲得が可能になり、各人の生活活動の中でより適切な行動選択が可能となる。 ・ICタグによる薬剤や食品の品質期限管理　・ホームネットワークによる家電制御／自宅遠隔監視 ・近傍ネットワーク危険検知による交通事故防止　・子どもや老人の所在確認／迷子アラーム ・任意の端末からの行政サービス享受　など
消費	「必要な時に場所を選ばす、適正な価格で安心して」消費活動を行うことが可能になる。 ・認証PFによる高額商品の安全な発注／決済　・ICカード等によるチケットレス入場／乗車／通行 ・ICタグによるレジでの支払い行為の省略　・街中広告からのWeb連携注文／コンテンツ閲覧 ・あらゆる場所でのブロードバンドコンテンツ閲覧　・TV番組と連携したWeb閲覧／商品情報獲得　など
社会参加	公共空間の設備や提供される情報により、全ての人にとって同等の社会参加が可能になる。 ・センサネットワークによる視聴覚／高齢者バリアフリー　・街中での多言語対応翻訳ナビゲーション ・ICチップによる身体条件対応型トイレ、エスカレータ　・携帯端末での情報交換／出会い創出　など
環境	人的移動の削減や物流の効率化によって、エネルギー消費の削減や地球環境の負荷軽減に貢献する。 ・テレワークによる移動の減少　・ICチップによる効率的物流 ・気象データ収集への乗用車のICチップ等の利用　・位置情報NW活用最適誘導による交通量抑制 など
就労	自分のライフスタイルに合わせて労働環境を選ぶことが可能になる。 ・任意のディスプレイがマイ端末に変身する　・端末やNWに最適な配信でコンテンツを利用できる ・映像/音声/業務データ等が併用できる遠隔会議　・移動中における一番近いプリンタからの印刷 ・会議場での携帯端末連携型情報交換相手通知　・P2PでのDB更新や免疫プログラムの流通　など
教育	現在の教育水準に存在する各種制約が解消され、誰もが最高水準の教育を受けることが可能になる。 ・遠隔講義と文字認識による高画質板書配信　・教材シームレス配信とNW対応型電子ブック流通 ・映像やメモを共有したグループ野外体験学習　・エージェント巡回による研究情報等の収集蓄積管理 ・3Dマルチアングル映像での演劇・舞台等鑑賞　・3D高臨場感／高精細データによる共同研究　など
医療・介護	予防的側面からの効果により、医療を受ける機会を減少させ、医療費の削減効果が得られる。 ・生体情報監視による疾病予防／早期発見／緊急通報　・高精細映像による簡易受診/相談/応急処置 ・ICカードによる受診履歴や既往症/副作用情報確認　・DNA認証による意識不明者身元確認　など

ユビキタスネットワーク戦略（ユビキタスネットワーキングフォーラム編）を参考に作成

（1）社会生活

- どこにいても適切な情報獲得が可能になり、各人の生活活動の中でより適切な行動選択が可能となる。

アプリケーション例	脅威	対策（例）
ICタグによる薬剤や食品の品質期限管理	ICタグ追跡（居場所の暴露、個人の特定）	タグ情報のワンタイム化
	プライバシー問題（所有物の暴露）	タグ情報の暗号化
ホームネットワークによる家電制御／自宅遠隔監視	不正アクセス／侵入	ファイアウォール／IPS
	マルウェア攻撃	マルウェアチェック
近傍ネットワーク危険検知による交通事故防止	近傍ネットワークの切断／遅延	低遅延／高信頼ネットワーク
子どもや老人の所在確認／迷子アラーム	タグ外し	タグの隠蔽／埋込み
	圏外（水没含む）	エリアの充実
任意の端末からの行政サービス享受　など	なりすまし	相互認証
	個人情報漏洩（キーロガー等）	ワンタームパスワード
		暗号化キーボード
		PCの初期状態自動復帰

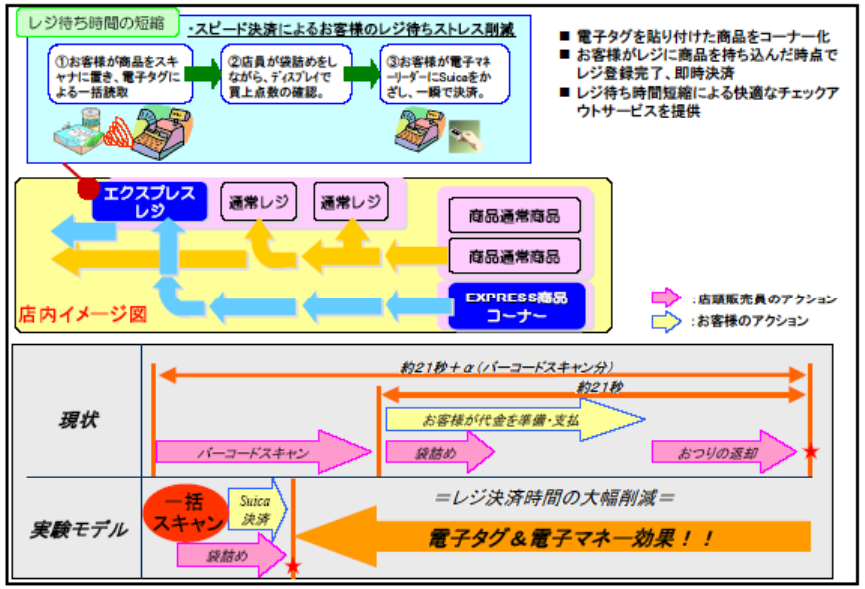


図は“センサネットワーク”，阪田史郎編著
を参考に一部修正

（2）消費

- 「必要な時に場所を選ばす、適正な価格で安心して」消費活動を行うことが可能になる。

アプリケーション例	脅威	対策（例）
認証PFによる高額商品の安全な発注／決済	なりすまし	相互認証
	発注／予約／決済情報の改竄／盗聴	暗号化
		改竄検知
ICカード等によるチケットレス入場／乗車／通行	電子チケットの複製／偽造／改竄	複製防止
		電子署名
ICタグによるレジでの支払い行為の省略	ICタグ追跡（居場所の暴露、個人の特定）	タグ情報のワンタイム化
	プライバシー問題（所有物の暴露）	タグ情報の暗号化
街中広告からのWeb連携注文／コンテンツ閲覧	広告／看板フィッシング	URL署名検証
あらゆる場所でのブロードバンドコンテンツ閲覧	コンテンツの不正コピー	コピープロテクト
	コンテンツの視聴条件侵害	視聴権管理／強制
TV番組と連携したWeb閲覧／商品情報獲得　など	不正アクセス／侵入	ファイアウォール／IPS
	マルウェア攻撃	マルウェアチェック



図は経済産業省：『日本版フューチャーストア・プロジェクト』について（H17.11.08）より

（3）社会参加

- 「公共空間の設備や提供される情報により、全ての人にとって同等の社会参加が可能になる。

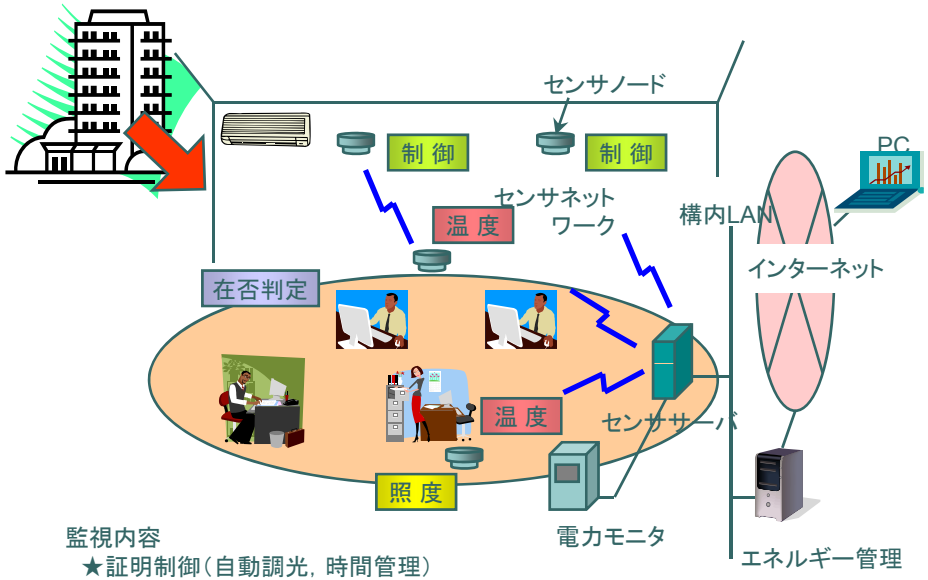
アプリケーション例	脅威	対策（例）
センサネットワークによる視聴覚／高齢者バリアフリー	タグ偽造／改竄	タグの認証
	偽装誘導／詐欺	相手認証
街中での多言語対応翻訳ナビゲーション	なりすまし	
	ICタグ追跡（居場所の暴露、個人の特定）	タグ情報のワンタイム化
ICチップによる身体条件対応型トイレ、エスカレータ	プライバシー問題（身体条件等の暴露）	タグ情報の暗号化
携帯端末での情報交換／出会い創出　など	コンテンツの不正コピー	コピープロテクト
	コンテンツの視聴条件侵害	視聴権管理／強制
	意図しない出会い	属性認証

図は厚生労働省，“障害者白書”（H18.06）より

（4）環境

- 人的移動の削減や物流の効率化によって、エネルギー消費の削減や地球環境の負荷軽減に貢献する。

アプリケーション例	脅威	対策（例）
テレワークによる移動の減少	不正アクセス／侵入	ファイアウォール／IPS
	マルウェア攻撃	マルウエアチェック
ICチップによる効率的物流	ICタグ追跡（居場所の暴露、個人の特定）	タグ情報のワンタイム化
	プライバシー問題（所有物の暴露）	タグ情報の暗号化
気象データ収集への乗用車のICチップ等の利用	タグ偽造／改竄	タグの認証
位置情報NW活用最適誘導による交通量抑制 など	偽装誘導／詐欺	相手認証



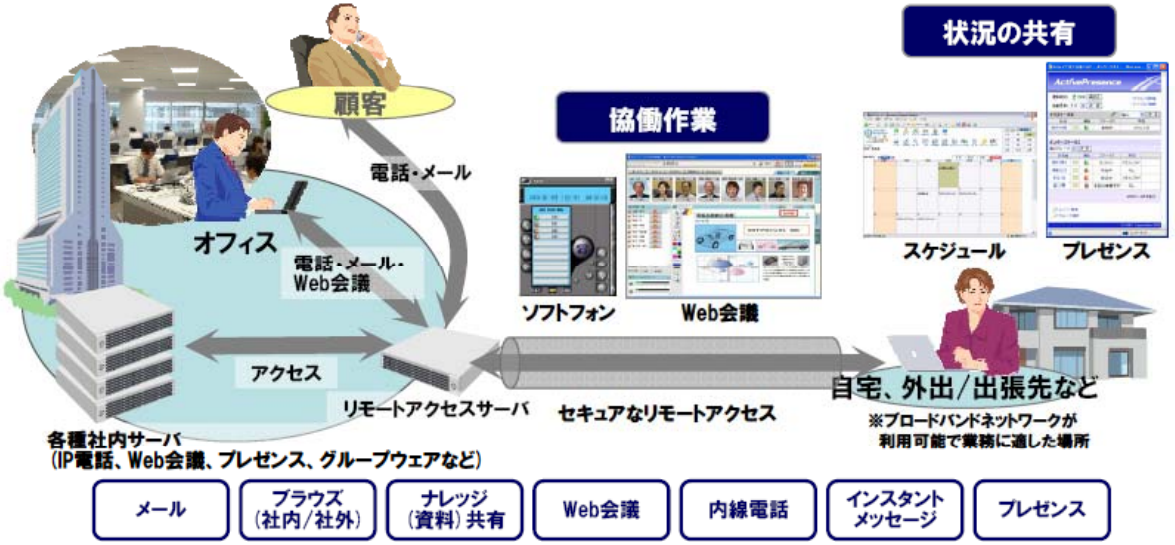
監視内容
★証明制御（自動調光，時間管理）
★空調制御（温湿度管理，塵埃，CO2）
★電力監視，エネルギー計測

図は“センサネットワーク”，阪田史郎編著を参考に一部修正

（5）就労

- 自分のライフスタイルに合わせて労働環境を選ぶことが可能になる。

アプリケーション例	脅威	対策（例）
任意のディスプレイがマイ端末に変身する	なりすまし	相互認証
端末やNWに最適な配信でコンテンツを利用できる	情報漏洩（キーロガー等）	ワンタイムパスワード
	コンテンツの不正コピー	暗号化キーボード
	コンテンツの利用条件侵害	PCの初期状態自動復帰
映像/音声/業務データ等が併用できる遠隔会議	データの改竄／盗聴	コピープロテクト
	不正アクセス／侵入	視聴権管理／強制
		改竄検知
移動中における一番近いプリンタからの印刷		暗号化
会議場での携帯端末連携型情報交換相手通知	意図しない出会い	ファイアウォール／IPS
	個人の追跡／特定	属性認証
P2PでのDB更新や免疫プログラムの流通　など	マルウェア攻撃	IDのワンタイム化
		マルウェアチェック



総務省：“u－Japanベストプラクティス2007事例集”より引用

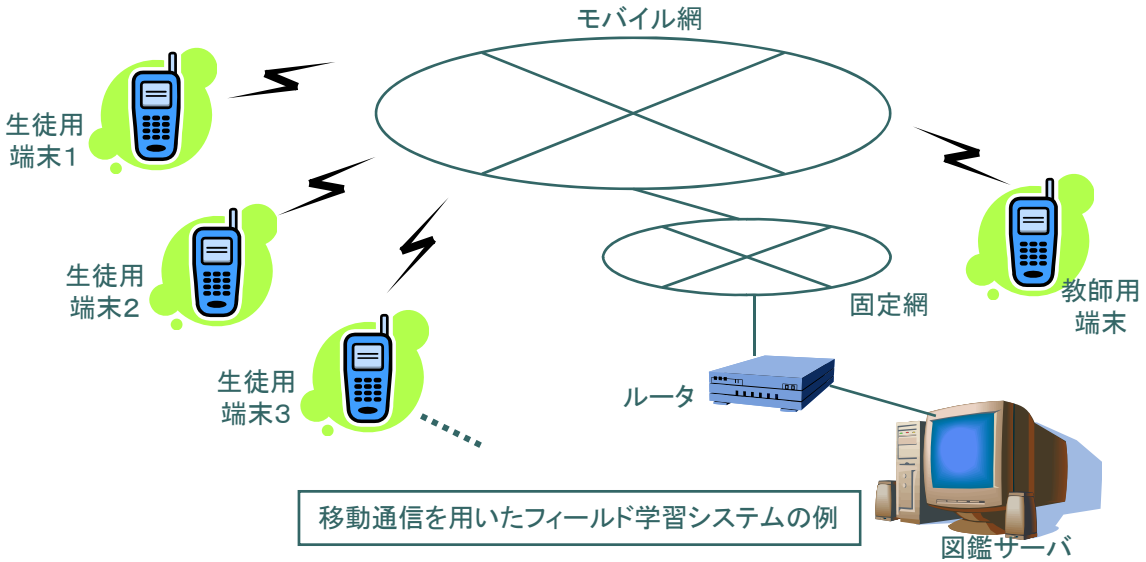
（6）教育

- 現在の教育水準に存在する各種制約が解消され、誰もが最高水準の教育を受けることが可能になる。

- **アプリケーション例**
  - 遠隔講義と文字認識による高画質板書配信
  - 教材シームレス配信とNW対応型電子ブック流通
  - 映像やメモを共有したグループ野外体験学習
  - エージェント巡回による研究情報等の収集蓄積管理
  - 3Dマルチアングル映像での演劇・舞台等鑑賞
  - 3D高臨場感／高精細データによる共同研究等

- **脅威**
  - データの改竄／盗聴
  - 不正アクセス／侵入
  - コンテンツの不正コピー
  - コンテンツの利用条件侵害
  - 意図しない出会い
  - 個人の追跡／特定
  - 偽装誘導／詐欺
  - なりすまし

- **対策（例）**
  - 改竄検知
  - 暗号化
  - ファイアウォール／IPS
  - コピープロテクト
  - 視聴権管理／強制
  - 属性認証
  - IDのワンタイム化
  - 署名
  - 属性認証
  - 相互認証



移動通信を用いたフィールド学習システムの例

（7）医療・介護

- 予防的側面からの効果により、医療を受ける機会を減少させ、医療費の削減効果が得られる。

アプリケーション例

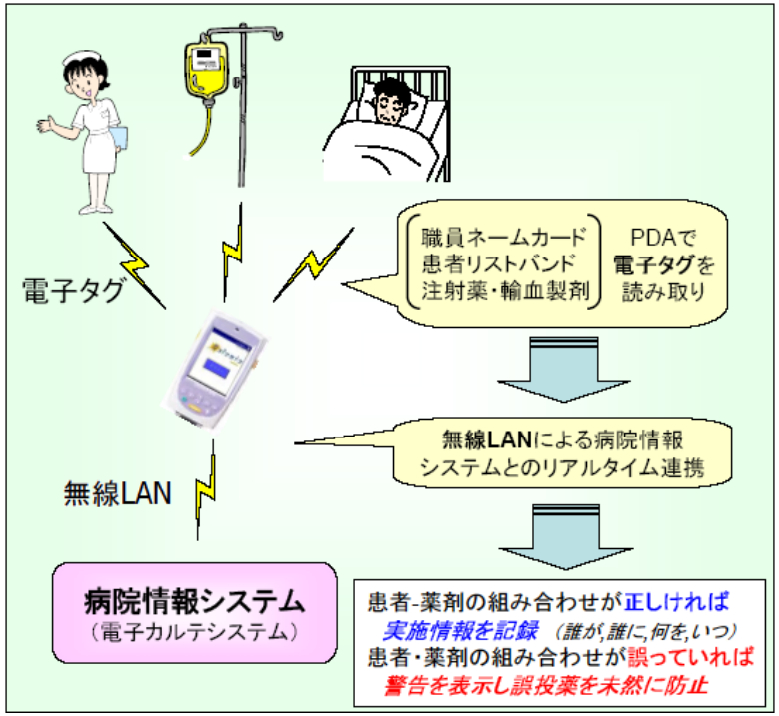
- 生体情報監視による疾病予防／早期発見／緊急通報
- 高精細映像による簡易受診/相談/応急処置
- ICカードによる受診履歴や既往症/副作用情報確認
- DNA認証による意識不明者身元確認　など

脅威

- 圏外／輻輳
- なりすまし
- データの改竄／盗聴
- 個人情報漏洩（端末紛失等）

対策（例）

- エリア／設備の充実
- 相互認証
- 改竄検知
- 暗号化
- 端末ロック
- 端末内情報の遠隔削除



総務省："u－Japanベストプラクティス2007事例集" より引用

ユビキタスアプリケーションに特徴的な脅威 – まとめ

○ ユビキタスアプリケーションに特徴的な脅威は、「ICタグ」や「端末」、「ナビゲーション」など、リアル世界との接点に見られる。

- ICタグ
  - タグの追跡（居場所の暴露、個人の特定）
  - プライバシー問題（所有物、個人属性の暴露）
  - タグ偽造／改竄
  - タグ外し／外れ
- 通信
  - 不正アクセス／侵入
  - マルウェア攻撃
  - 近傍ネットワークの切断／遅延
  - 近傍ネットワークでの個人の追跡／特定
  - 圏外／輻輳
- サービス利用
  - なりすまし
  - 発注／予約／決済情報の改竄／盗聴
  - 利用権（チケット）の複製／偽造／改竄
- コンテンツ利用
  - コンテンツの不正コピー
  - コンテンツの視聴権条件侵害
- 端末
  - 共用端末からの情報漏洩（キーロガー等）
  - 端末の紛失／盗難による情報漏洩
- ナビゲーション
  - 偽装誘導／詐欺
  - 意図しない出会い

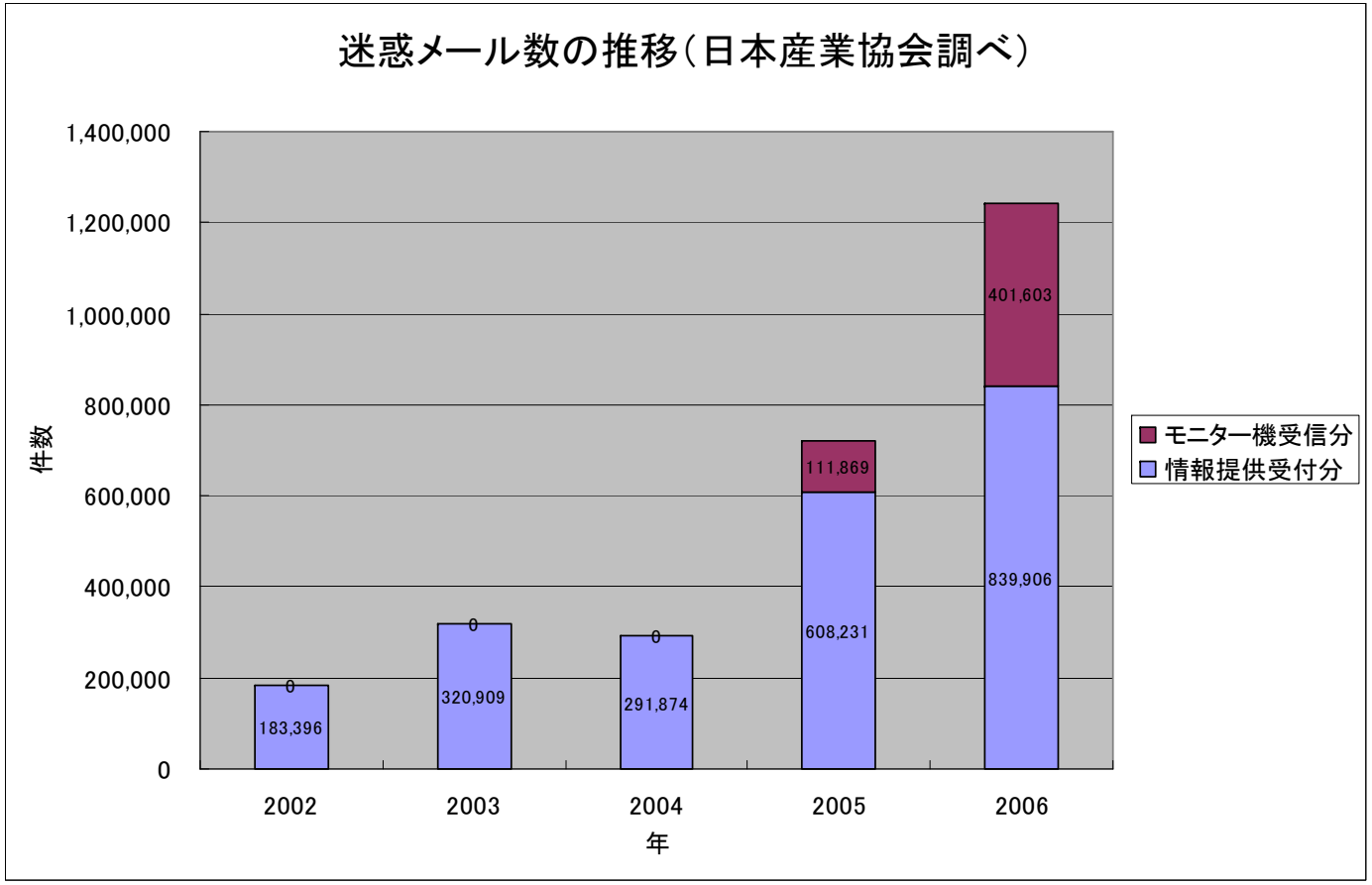
近い将来の情報セキュリティ

1. 第四世代移動通信の視点から
2. ユビキタスアプリケーションの視点から
3. 量的変化の視点から
   - 迷惑メールを例として

迷惑メール数の推移

- 迷惑メールはここ数年急激に増加している

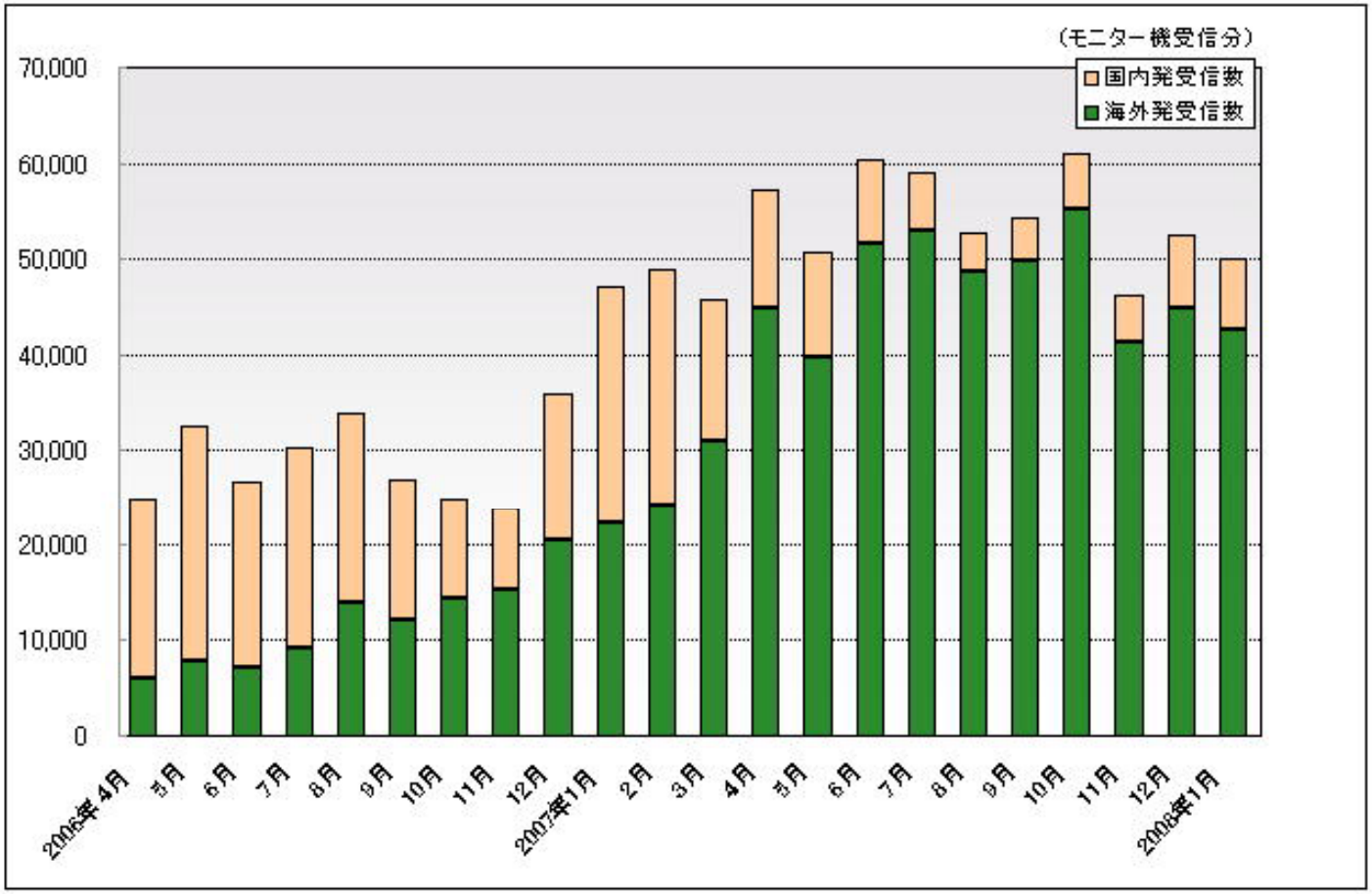
（日本産業協会調べ）



（財）日本産業協会 “迷惑メールの統計” より

国内・海外発メール受信数推移

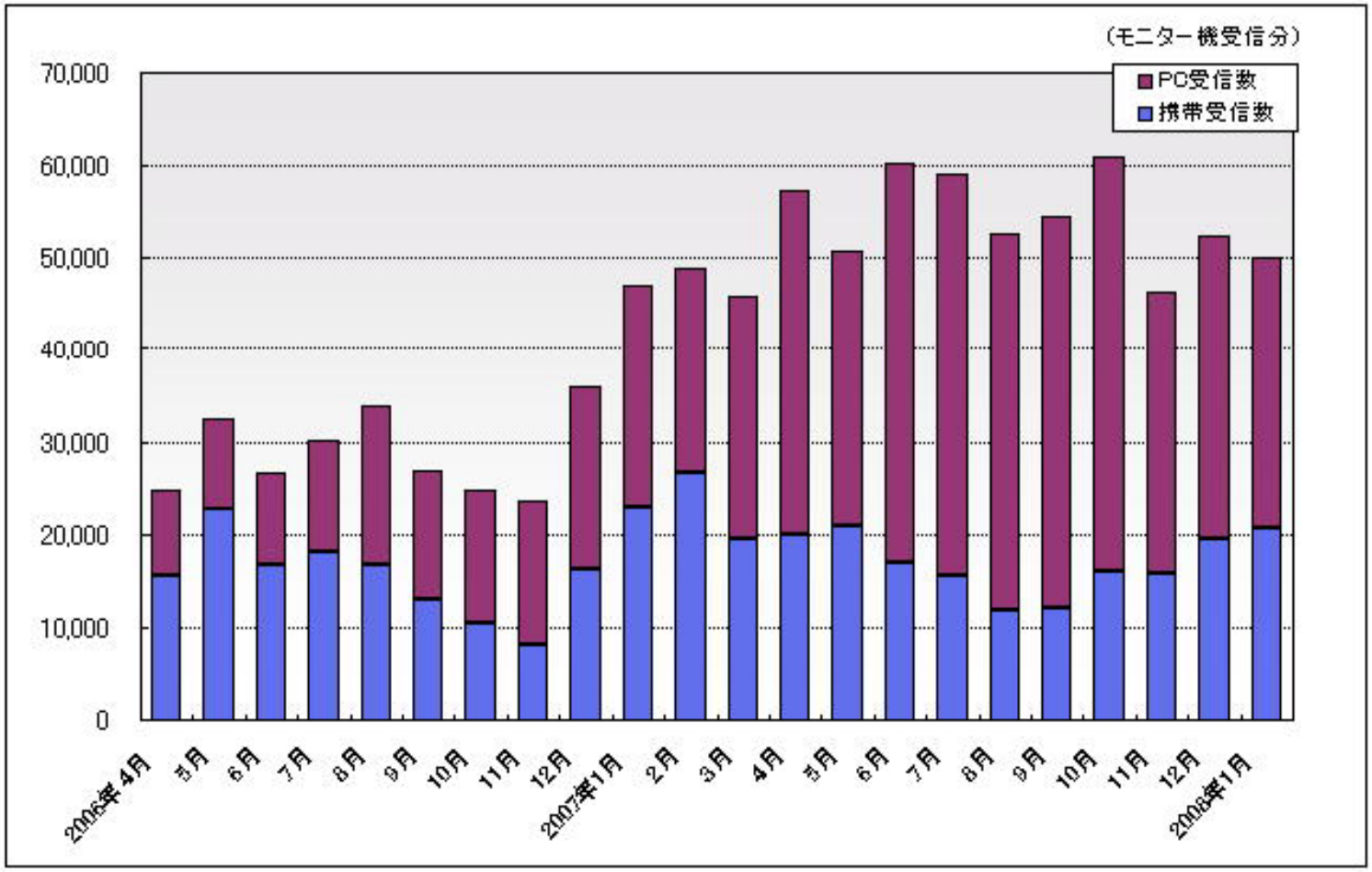
- 著しい増加傾向が見られる
- 海外発のものが圧倒的に多い



（財）日本産業協会 “迷惑メールの統計” より

媒体別受信数推移

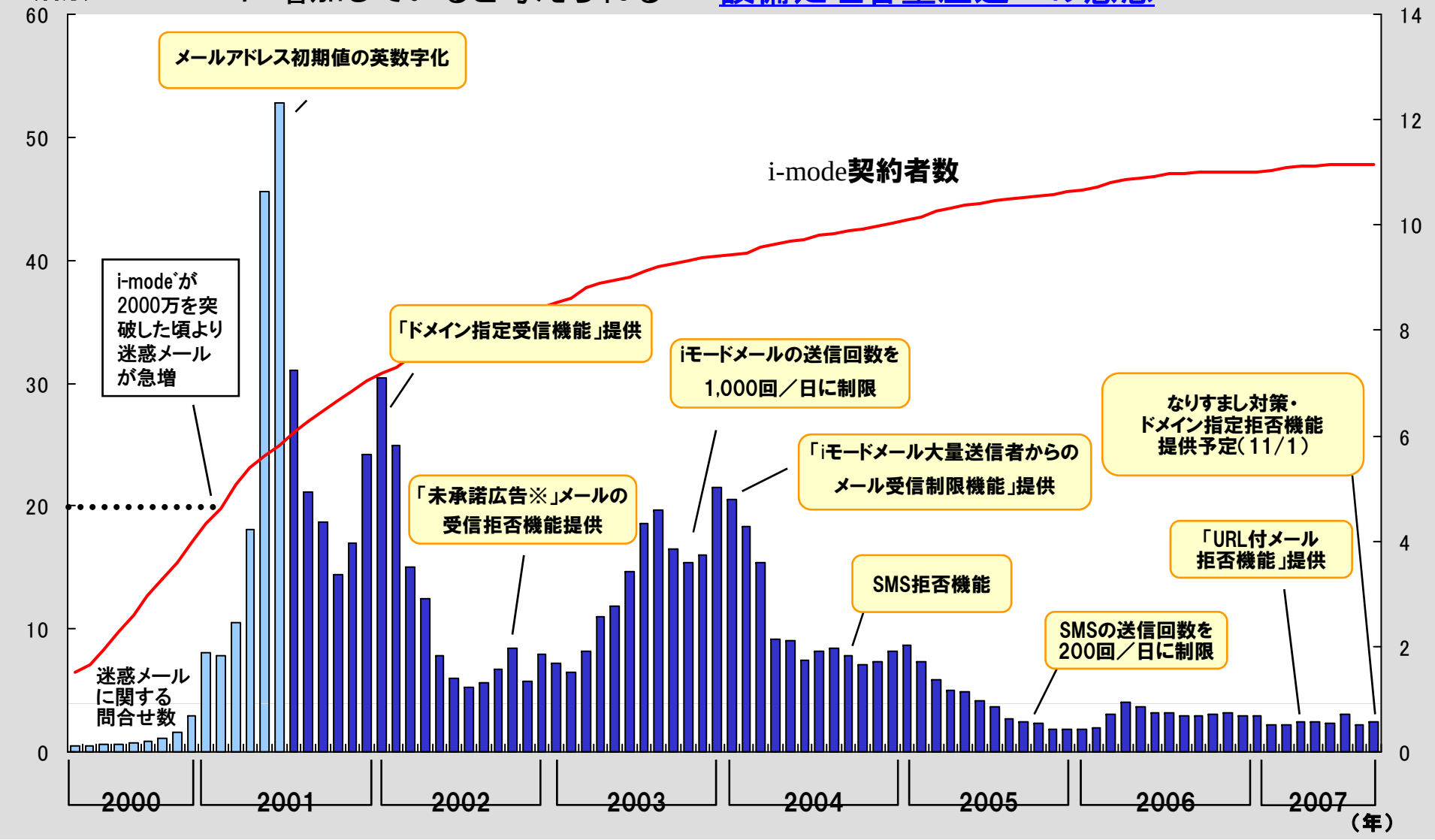
- 2006年後半以降、携帯とパソコンの受信数が逆転している
- 携帯受信数よりもパソコンの受信数の方が支配的



（財）日本産業協会 “迷惑メールの統計” より

迷惑メールへの各種対策（NTTドコモ）

- 迷惑メールへの遮断施策は、高い効果を上げている
- 迷惑メールの増加を鑑みるに、サーバにおけるブロック件数は確実に増加していると考えられる → 設備処理容量圧迫への懸念



迷惑メールの増加と対策 ― まとめ

- 傾向のまとめ
  - 迷惑メールに増加の傾向が見られる
    - 特にここ2～3年の増加が著しい
  - 最近の傾向として、海外からと見られる迷惑メールの比率が高い
  - 最近は、携帯電話よりもパソコンへの迷惑メールが支配的である
- 対策（案）
  - 設備の増強で対応しているのが一般的な状況
  - 技術的な対策とともに、国際的な連携策も有効と考えられる

おわりに

近い将来のセキュリティ問題のトレンドを3つの視点から考察した

- 第四世代移動通信網の視点から
  - コアネットワークに想定される基本的な脅威は第三世代および現在のPC環境に準ずる
  - 接続先ネットワークが多様化することによる脅威の増加が想定される
  - （脅威ではないが）認証機会の増大による利便性の低下が懸念される
- ユビキタスアプリケーションの視点から
  - ユビキタスアプリケーションに特徴的な脅威は、リアル世界との接点に見られる
    - ICタグに起因するプライバシー問題や信頼性などが懸念される
    - 端末を共用することや、携帯端末内への重要情報の蓄積量の増加に伴う情報漏洩リスクの増大が懸念される
    - ナビゲーションに関連する偽装や詐欺、意図しない出会いなどのリスクも増大が懸念される
- 量的変化の視点から
  - 迷惑メールは増加の一途を辿っており、設備処理容量の圧迫という脅威が懸念される