ICTの今後とセキュリティ

鹿児島大学
大学院理工学研究科　教授
学長補佐（情報担当）
学術情報基盤センター長
NPO鹿児島インファーメーション理事長
森邦彦

内容

1. ICTとは
2. インターネットの生い立ち
3. ICT産業の動向
4. ICTと情報セキュリティ
5. 今後のICTは？

1. ICTとは

ICT(Information and Communication Technology)は「情報通信技術」の略であり、IT(Information Technology)とほぼ同義の意味を持つが、コンピューター関連の技術をIT、コンピューター技術の活用に着目する場合をICTと、区別して用いる場合もある。国際的にICTが定着していることなどから、日本でも近年ICTがITに代わる言葉として広まりつつある。

by **知恵蔵2015**から抜粋

コミュニケーション

- コミュニケーション（交流）は、複数の人間や動物などが、感情、意思、情報などを、受け取りあうこと、あるいは伝えあうこと。
- コミュニケーションによって伝えられる情報の種類は、感情、意思、思考、知識など、様々
- 伝えるための媒体としては、言葉、表情、ジェスチャー、鳴き声、分泌物質（フェロモン等）など
- コミュニケーションのない社会はない。
  コミュニケーションは社会の根幹を形成する概念

情報の共有・伝達・保存手段

昔

- ボディーコミュニケーション（非言語・五感すべて）
- 絵画の発達：画像による情報伝達•保存（非言語・視覚）
- 言葉（言語）の発明：声による直接的情報伝達•保存（聴覚）
- 文字（記号）の発明：文書・手紙による情報伝達•保存（視覚）
- 印刷技術の発明：マスコミュニケーションの黎明
- 電話の発明：声による遠隔情報伝達（聴覚）
- ラジオの発明（聴覚）

今

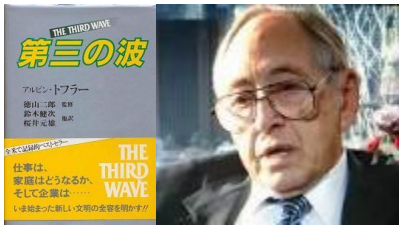
- カメラの発明：画像（映像）による詳細情報伝達•保存（視覚）
- テレビの発明（視覚・聴覚）

圧倒的な情報量と速度の差

- コンピュータの発明とネットワークの発明

ICT・ビッグデータ・IoTの時代

アルビントフラーの第３の波



- 1980年出版
- 第一の波:農耕の開始

  約15000年ほど前から農耕を開始したことにより、それ以前の狩猟採集社会の文化を置換した。
- 第二の波：産業革命

  18世紀から19世紀にかけて起こった工業化により、それまでの農耕社会から産業社会へと移り変わる。
- 第三の波：脱産業社会（脱工業化社会）

  トフラーは1950年代末にはこれを言いはじめ、多くの国が第二の波から第三の波に乗り換えつつあるとした。彼は、それを説明する造語をたくさん作り、他の人々が発明した情報化時代、情報化社会、情報革命のような造語にも言及した。

  by Wikipedia

2. インターネットの生い立ち

- 電子計算機の登場
- 宇宙開発とコンピュータ
- コンピュータと通信の融合
- インターネットの歴史

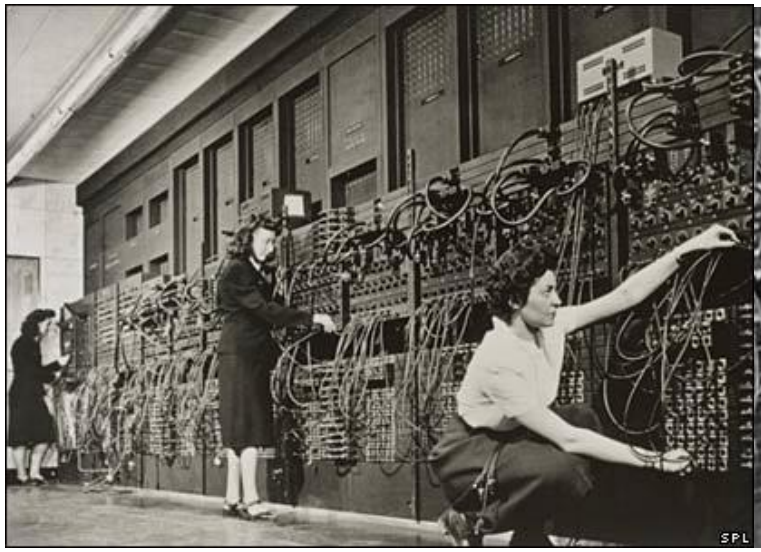
ENIAC

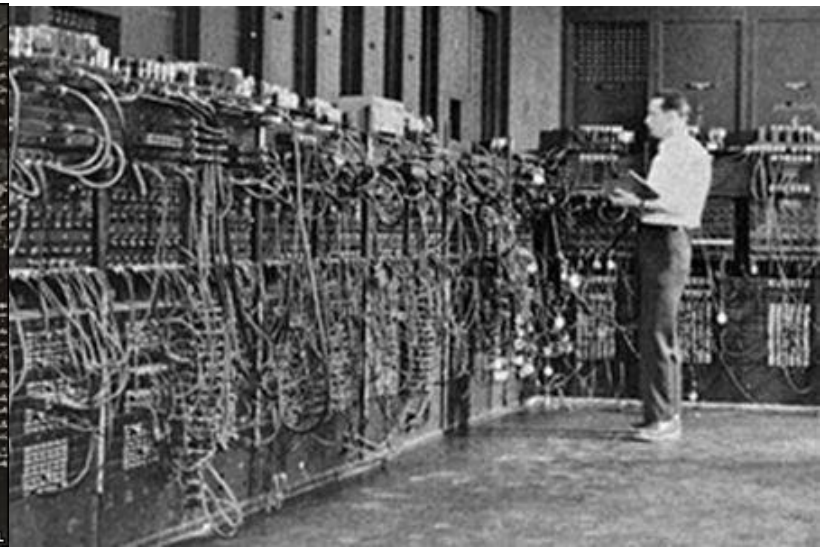
Electronic Numerical Integrator and Computer、「電子式数値積分・計算機」

1946年2月14日にペンシルベニア大学で初めて公開され、1955年10月2日まで使用

重量30トン、幅24m×奥行き0.9m×高さ2.5m

真空管18,000本、消費電力150kw



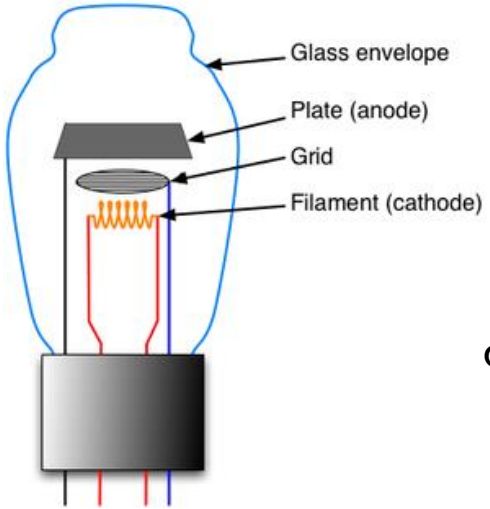


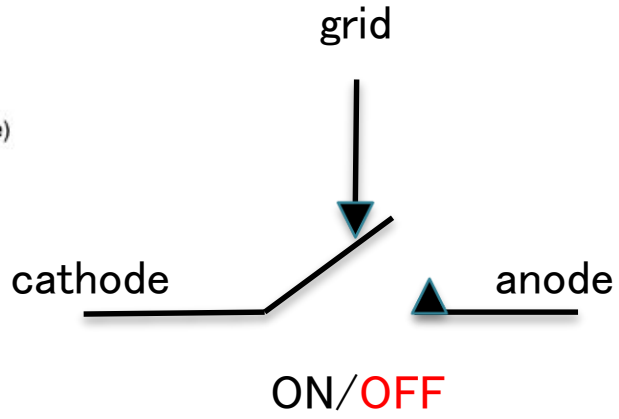
ENIAC

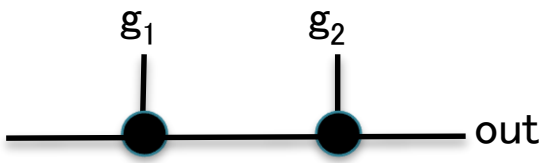
- 1943年に連合軍は北アフリカに上陸した。そこには、今まで砲兵が見たことのない地形が展開されていた。軍は急遽弾道表をほとんど全面的に修正しなくてはならなくなった。軍の要求は計算器（*電気機械式計算機）の処理能力を上回り、弾道表の作成はますます間に合わなくなってきた。この緊急事態が電子式ディジタル・コンピュータの開発を急がせる決定的なきっかけとなった。
- コンピュータ開発を推進する原動力は陸軍の弾道学上のニーズにあったが、ENIACの開発は第二次世界大戦(1939-1945)終結までに完了しなかった。

by UNISYSグループの歴史

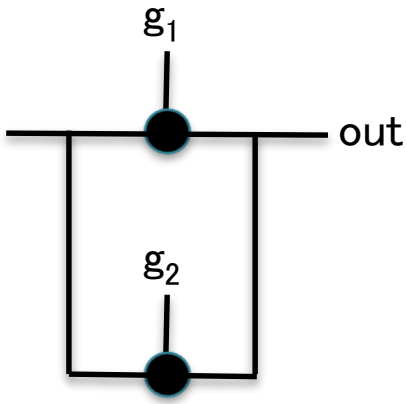
真空管





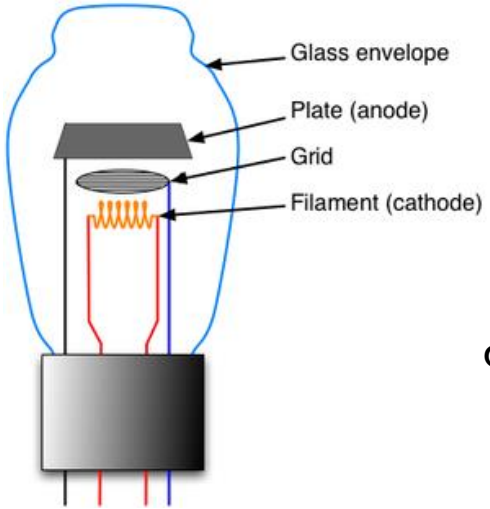


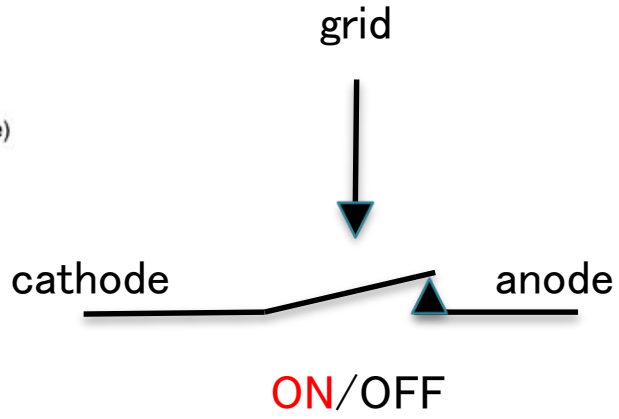
AND		
g_1	g_2	out
OFF	OFF	OFF
OFF	ON	OFF
ON	OFF	OFF
ON	ON	ON

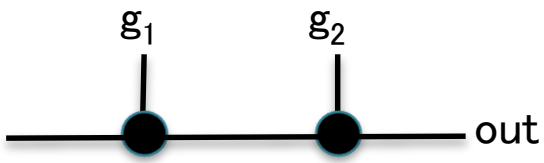


OR		
g_1	g_2	out
OFF	OFF	OFF
OFF	ON	ON
ON	OFF	ON
ON	ON	ON

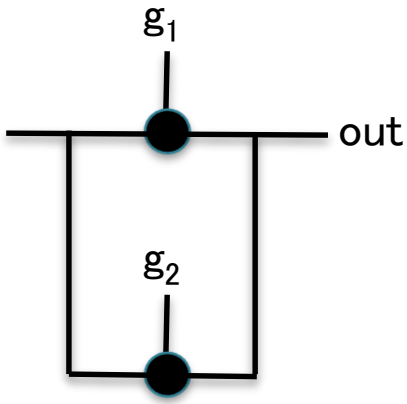
真空管







AND		
g_1	g_2	out
OFF	OFF	OFF
OFF	ON	OFF
ON	OFF	OFF
ON	ON	ON



OR		
g_1	g_2	out
OFF	OFF	OFF
OFF	ON	ON
ON	OFF	ON
ON	ON	ON

宇宙開発競争とコンピュータ

- ＡＲＰＡの誕生（スプートニックパニック）

  1957年10月（ソ連）スプートニック打ち上げ

  1957年11月（ソ連）生命維持装置付きスプートニック２号打ち上げ、ライカという犬を搭乗

スプートニク2号は大気圏再突入が不可能な設計だったため、1958年4月14日、大気圏再突入の際に崩壊した。ライカは打ち上げから10日後に薬入りの餌を与えられて安楽死させられた、とされていたが、実際にはストレスなどにより打ち上げ４日後に死亡。

by Wikipedia

宇宙開発競争とコンピュータ

- ＡＲＰＡの誕生（スプートニックパニック）

  1957年10月（ソ連）スプートニック打ち上げ

  1957年11月（ソ連）生命維持装置付きスプートニック２号打ち上げ、ライカという犬を搭乗

  →ソ連がロケットに核爆弾を取り付け、地球上のあらゆる場所を攻撃できることを意味する。

- 1957年12月（米国）宇宙に関する研究開発の一元化を図るため国防総省の傘下に高等研究計画局（Advanced Research Projects Agency ARPA）設置
- 1958年10月（米国）民間による宇宙開発を強力に推進するために、米国航空宇宙局（National Aeronautics and Space Administration NASA）を発足

コンピュータと通信の融合

- ARPAの発足

  宇宙開発競争を背景にして1957年12月（米国）宇宙に関する研究開発の一元化を図るため国防総省の傘下に高等研究計画局（Advanced Research Projects Agency ARPA）設置

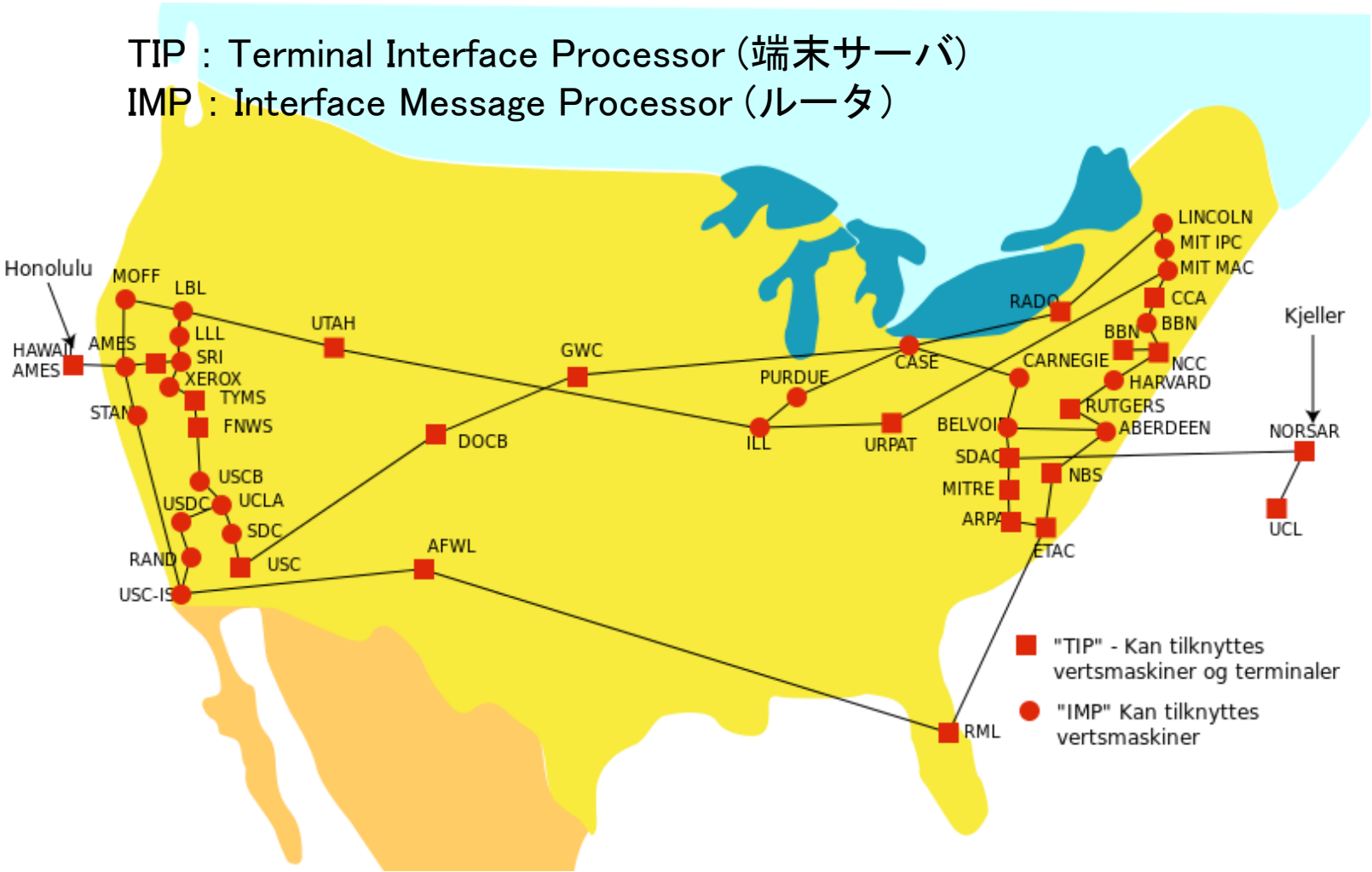
- 1967 ARPANET計画誕生

  世界で初めて運用されたパケット通信ネットワークであり、今日の世界的なインターネットの起源である。アメリカ国防総省の高等研究計画局（ARPA、後にDARPA）が資金を提供し、いくつかの大学と研究機関でプロジェクトが行われた。

  by Wikipedia

1974年時点のARPANETの構成

TIP：Terminal Interface Processor（端末サーバ）
IMP：Interface Message Processor（ルータ）



最初のルータ: IMP

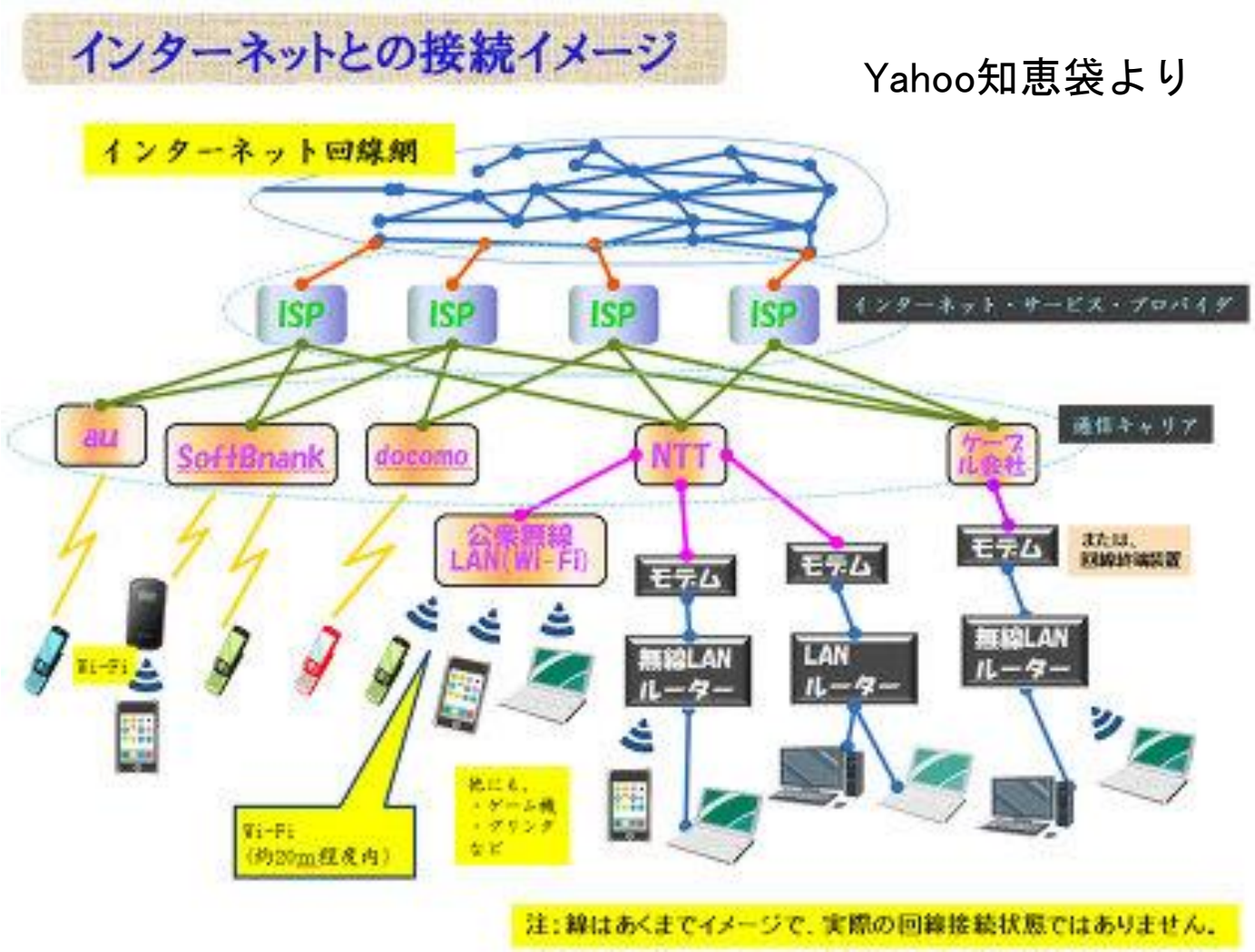
- Interface Message Processor

  ARPANETにおいてパケットのスイッチング処理を行う装置。現在のインターネットにおけるルーターの前身に当たる。

IMP1号機とレナード・クラインロック教授(UCLA)

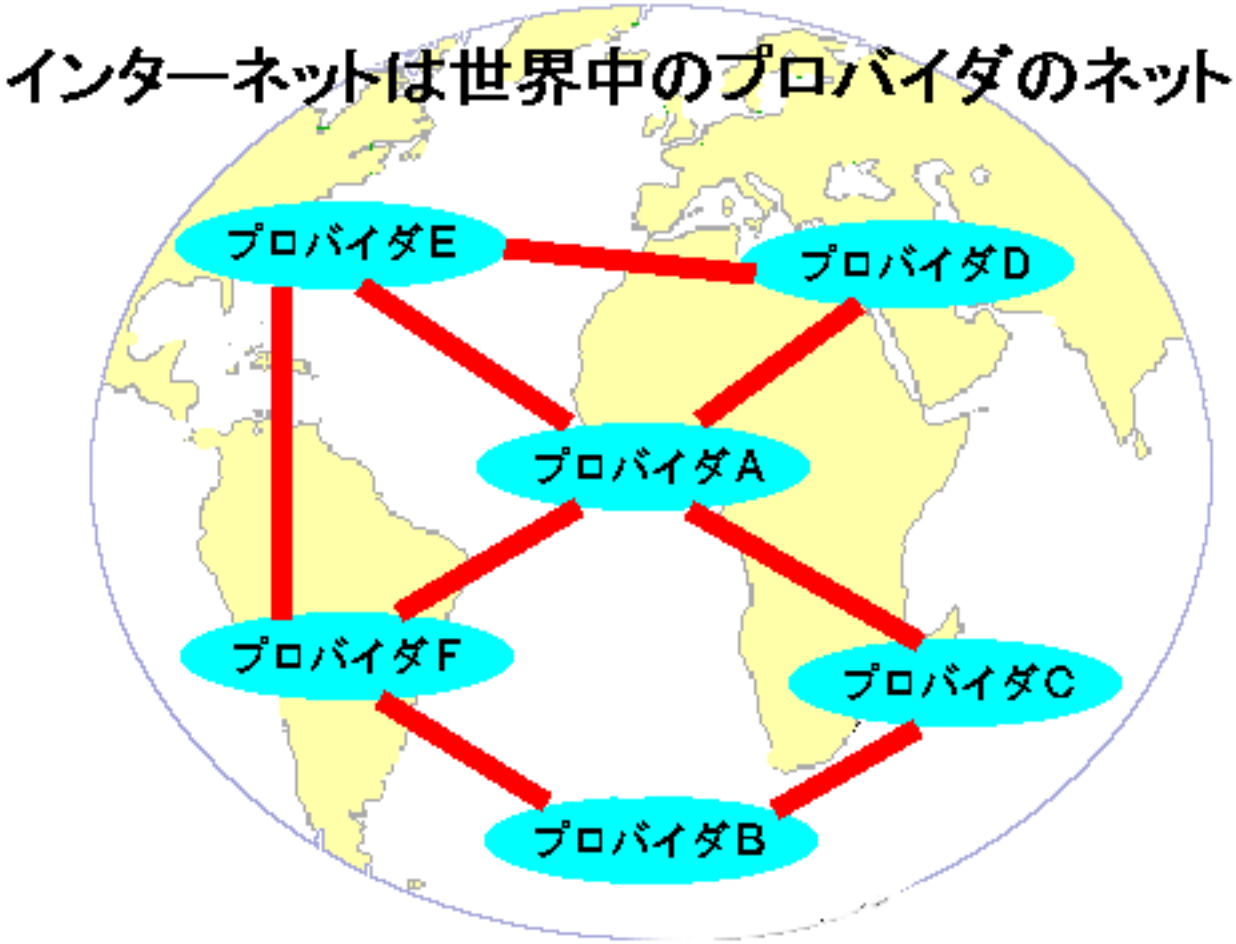
by Wikipedia

インターネットの概念



Yahoo知恵袋より

インターネットの概念



http://komakusa.net/internet/internet1.htmlより

インターネットの歴史

- 1942 ABC（アナタソフ、ベリー）　;　1946　ENIAC（モークリー、エッカート）
- 1967 ARPANET計画誕生

  米国防総省高等研究計画局(ARPA; Advanced Research Projects Agency)の資金提供により、世界初のパケット通信ネットワークであるARPANET(Advanced Research Projects Agency Network)の研究プロジェクトが発足。
- 1969 ARPANET開始(4ノード)

  現在のインターネットの起源とも言えるARPANET (Advanced Research Projects Agency Network)が、カリフォルニア大学ロサンゼルス校(UCLA)、カリフォルニア大学サンタバーバラ校(UCSB)、ユタ大学、スタンフォード研究所(SRI; Stanford Research Institute)の4拠点をIMP (Interface Message Processor)を用いて接続する形で運用が開始されました。
- 1972 ARPAがDARPAへと改称

  国防高等研究計画局(DARPA; Defense Advanced Research Projects Agency)へと変更。
- 1972　ARPANETのNATO域への拡大(イギリス、ノルウェー)
- 1980　イーサネット規格公開

インターネットの歴史

- 1981 CSNET(Computer Science Research Network)運用開始
  予算や認可制限のためにARPANETに直接接続できない学究機関にネットワークを提供
- 1983　ARPANETでTCP/IPが標準プロトコルとして採用
- 1983　DNSに関する一連のRFCが発表
- 1985 初のコンピュータウイルス(Brain)誕生
- 1987 学術情報ネットワーク運用開始
  後にSINET (Science Information NETwork)へと発展
- 1989 ネットワークアドレス調整委員会がIPアドレスの割り当てを開始
  1992年6月にJNICに引き継ぐ、JNICは1993年にJPNIC（一般社団法人）に改組
- 1993 HTMLバージョン1.0が公開される
- 1993 郵政省がインターネットの商用利用を許可

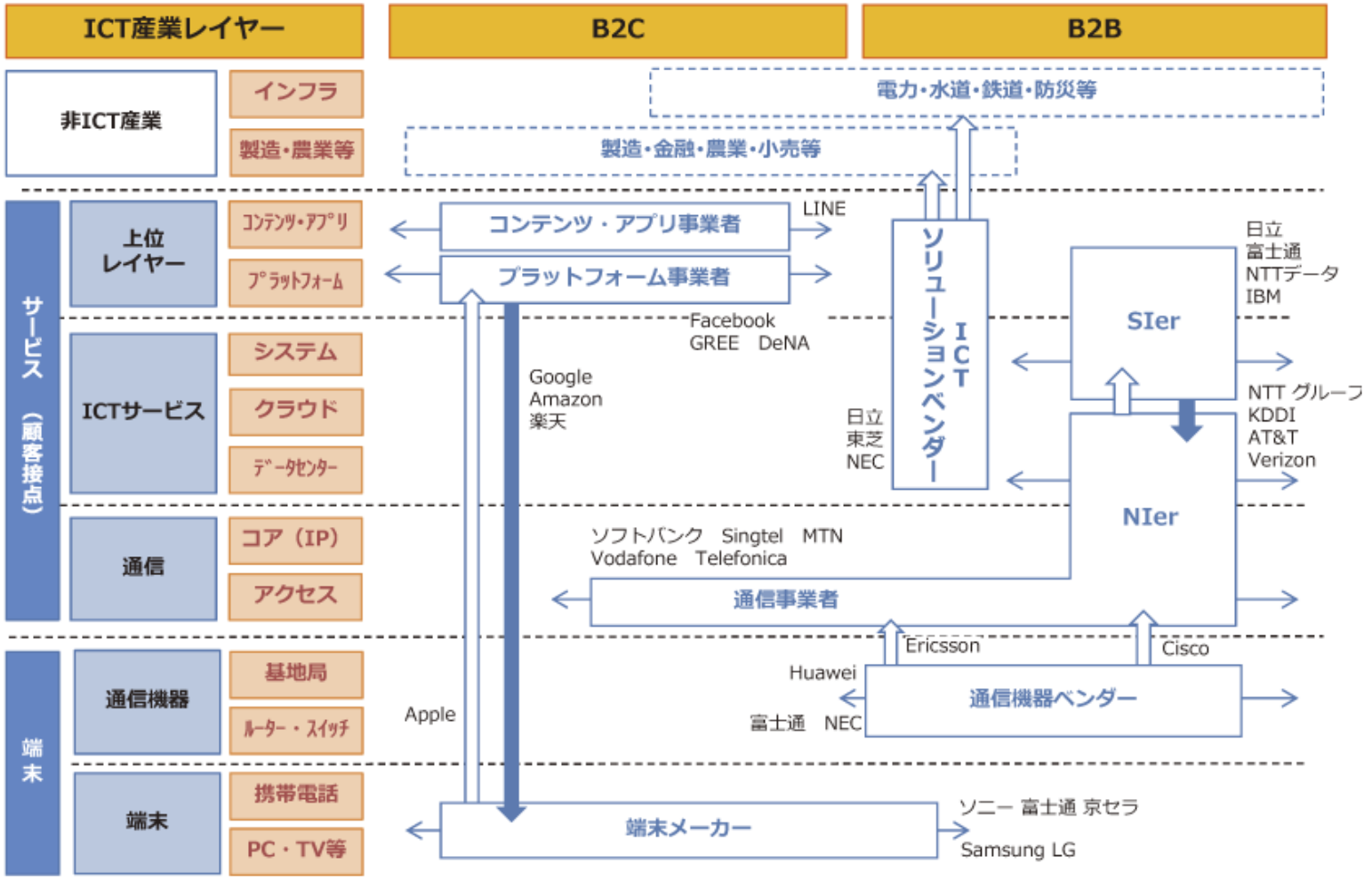
旧郵政省により日本におけるインターネットの商用利用が許可され、ISP事業などの実施が可能になりました。

- 1994 W3C(World Wide Web Consortium)設立
- 1995　IPv6仕様（RFC1884)決定

3. ICT産業の動向

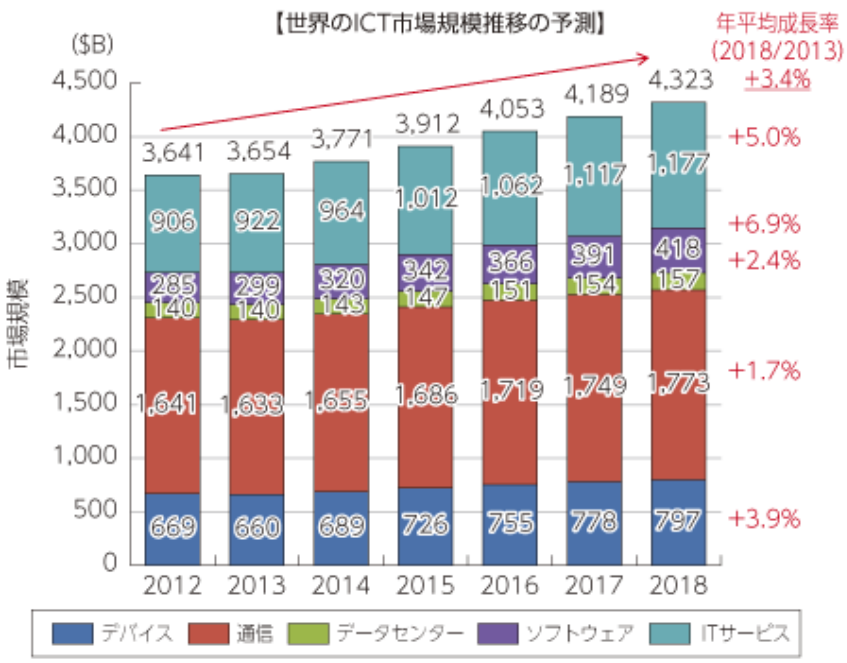
- ICT産業のレイヤーおよび事業者
- グローバルICT市場の予測と成長率
- ICT産業の業種別割合と成長率
- 各国のICT
- ICTサービスレイヤー：クラウドの浸透

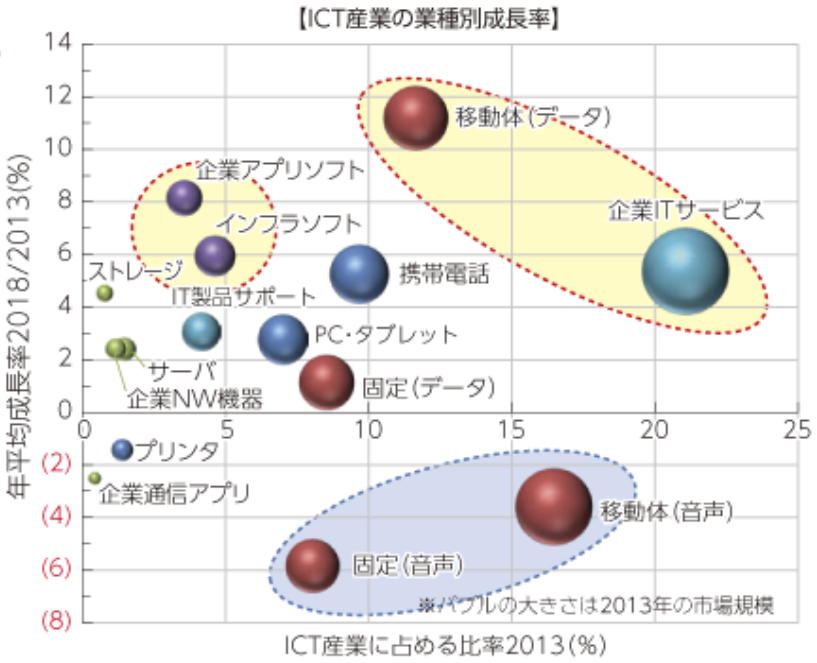
ICT産業のレイヤーおよび事業者



2014年版　情報通信白書　（総務省）

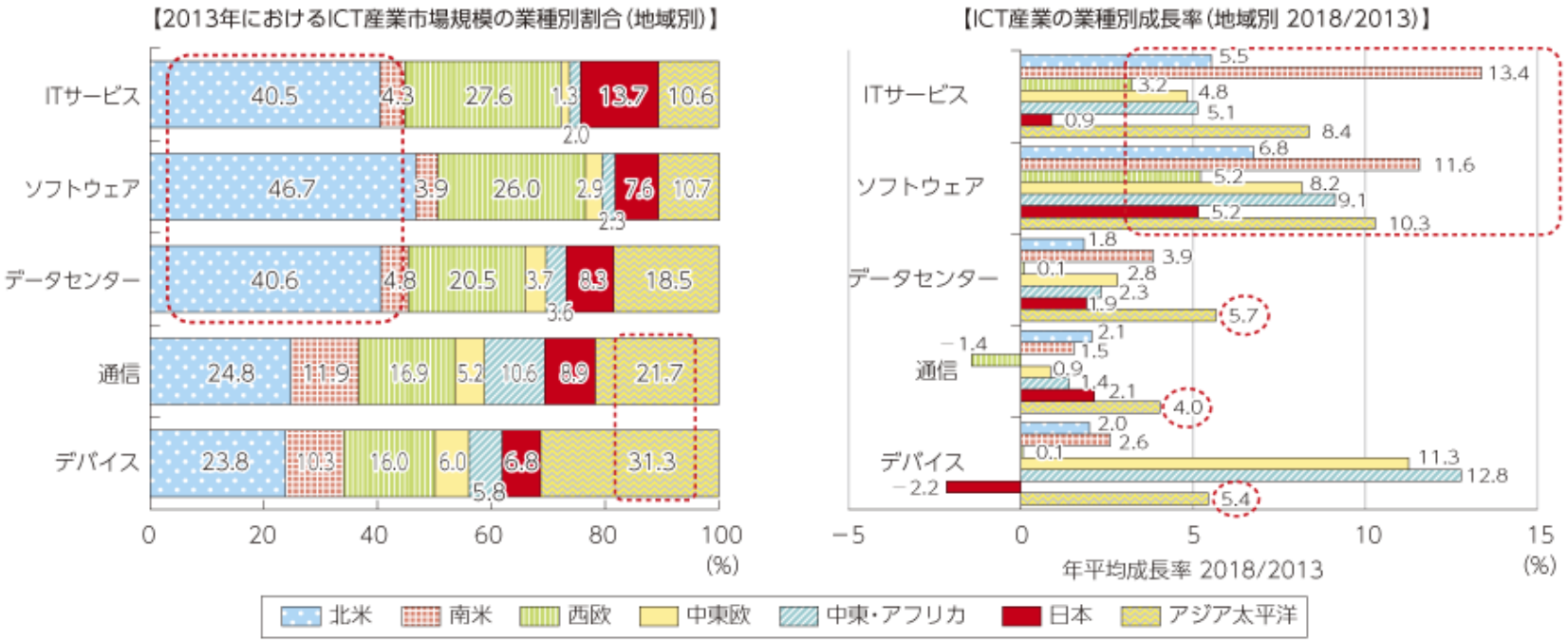
グローバルICT市場の予測と成長率





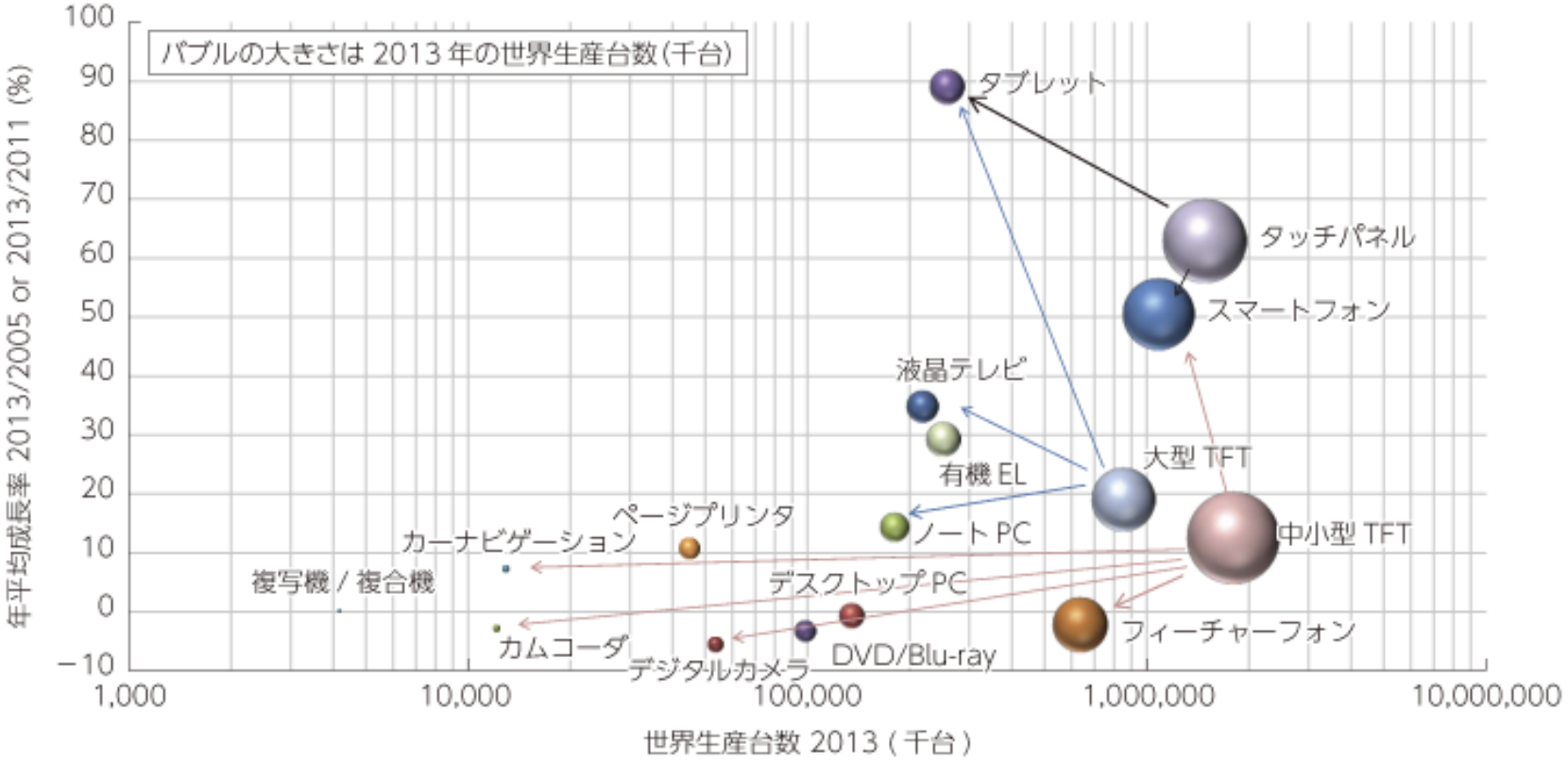
2014年版　情報通信白書　（総務省）

ICT産業の業種別(地域別)割合と成長率



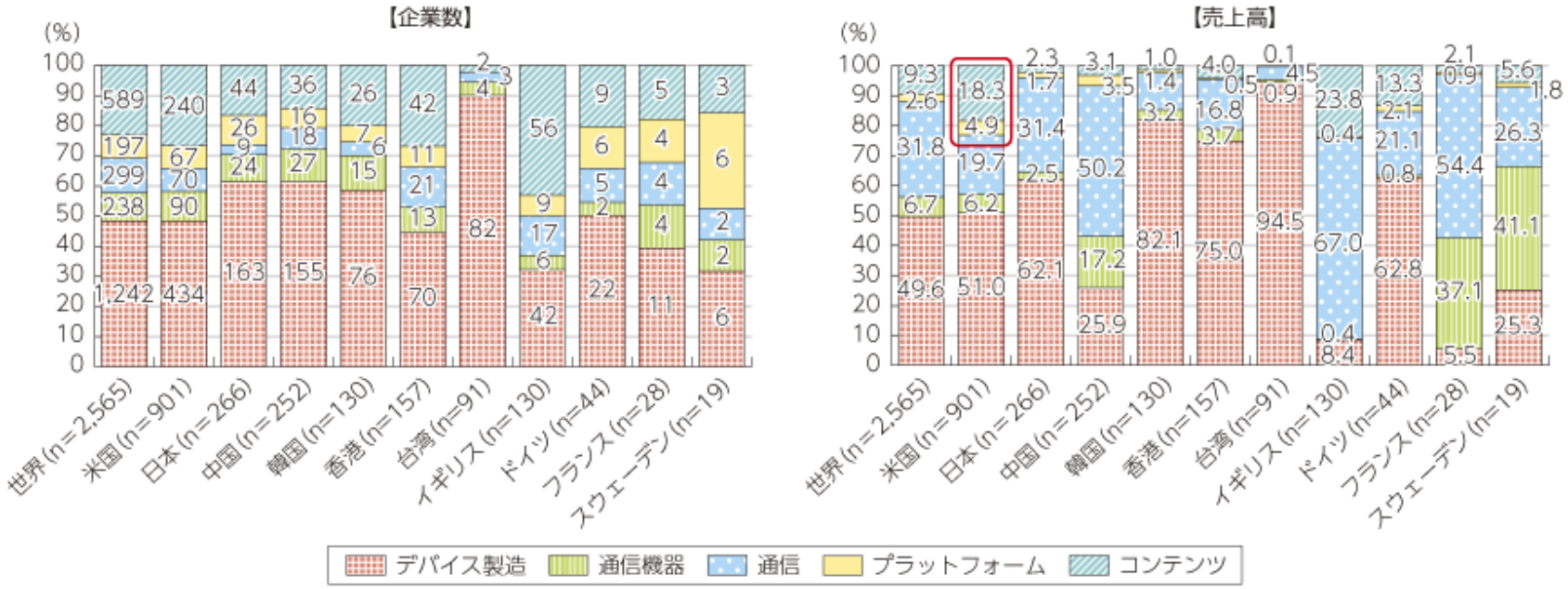
2014年版　情報通信白書　（総務省）

世界における端末及びパネル等の生産台数



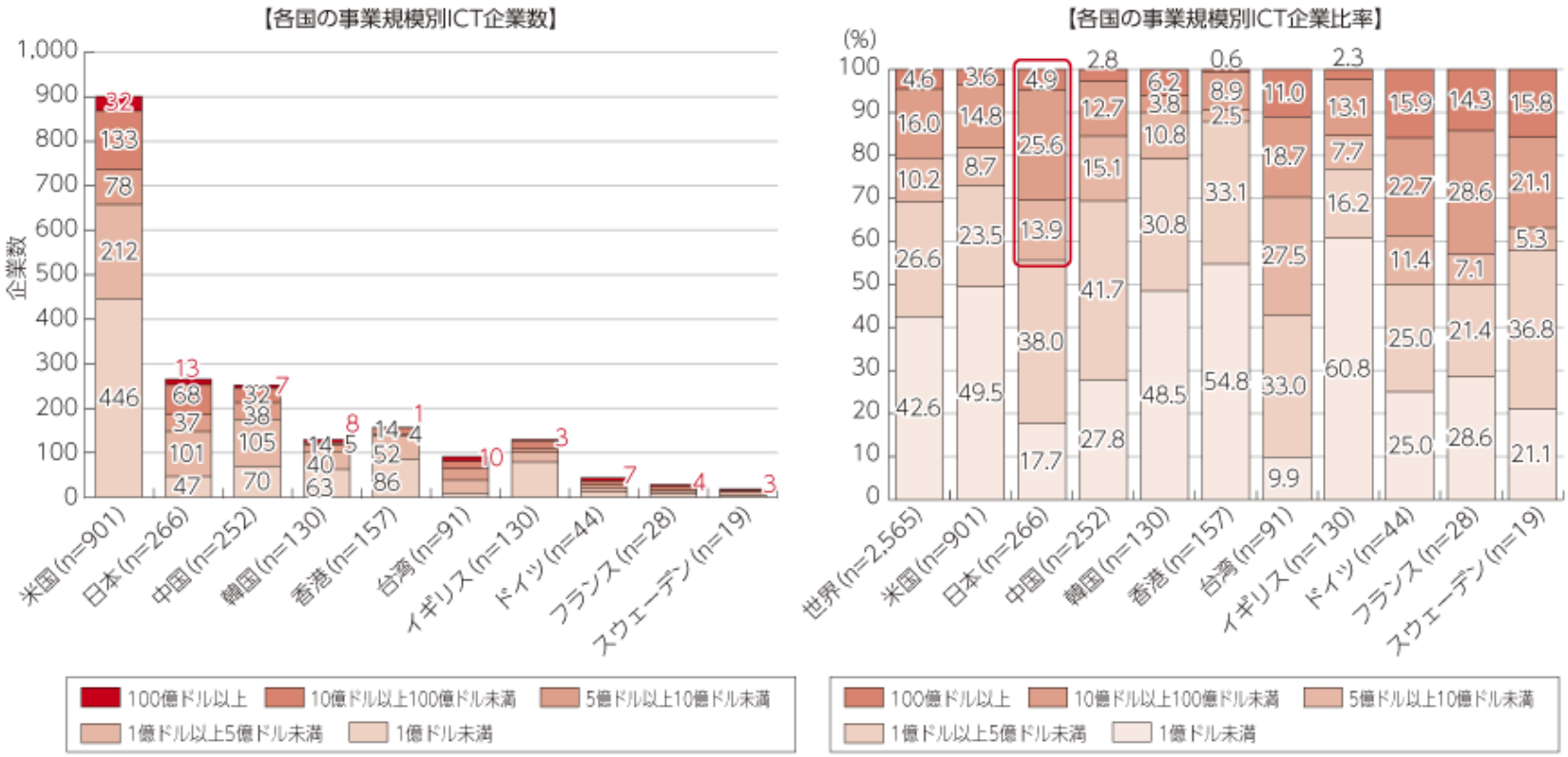
2014年版　情報通信白書　（総務省）

各国のICT企業数と売上高の比率



2014年版　情報通信白書　（総務省）

各国の事業規模別ICT企業数と比率



2014年版　情報通信白書　（総務省）

各国における売上上位１０企業

売上高100億ドル以上の上位１０企業

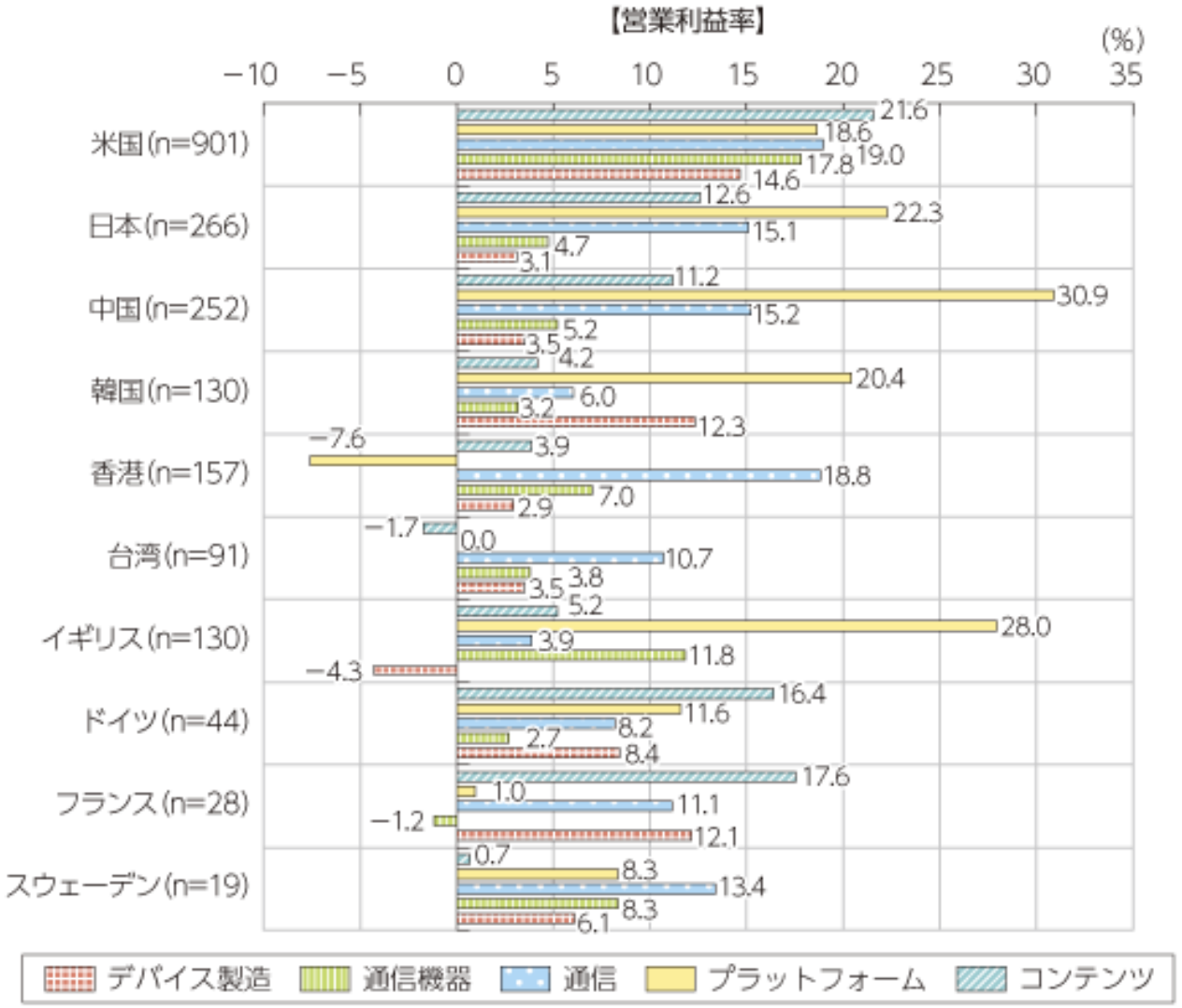
【主要国における売上高100億ドル以上の上位10位企業（2013年または最新年）】

米国	日本	中国	韓国	香港	台湾	イギリス	ドイツ	フランス	スウェーデン
Apple	NTT	China Mobile(注)	Samsung	Lenovo	Hon Hai	Vodafone	BASF	Alcatel-Lucent	Ericsson
GE	パナソニック	China Telecom	LG Electronics		Compal Electronics	BT	Siemens	Orange	AB Electrolux
AT&T	ソニー	China Unicom(注)	LG Display		Wistron	Liberty Global	DT	Vivendi	TeliaSonera
Verizon	東芝	Great Wall Technology	KT Corp		TSMC		SAP	Bouygues S.A.	
HP	NTTドコモ	ZTE	SK Telecom		Innolux		Bertelsmann		
Microsoft	KDDI	Huawei	SK Hynix		Asustek		Fresenius Medical Care		
Comcast	三菱電機	TCL	LS		Acer		BSH		
Google	ソフトバンク		LG Uplus		Inventec				
Intel	NEC				AU Optronics				
Cisco	シャープ				WPG				

注）便宜上中国に分類

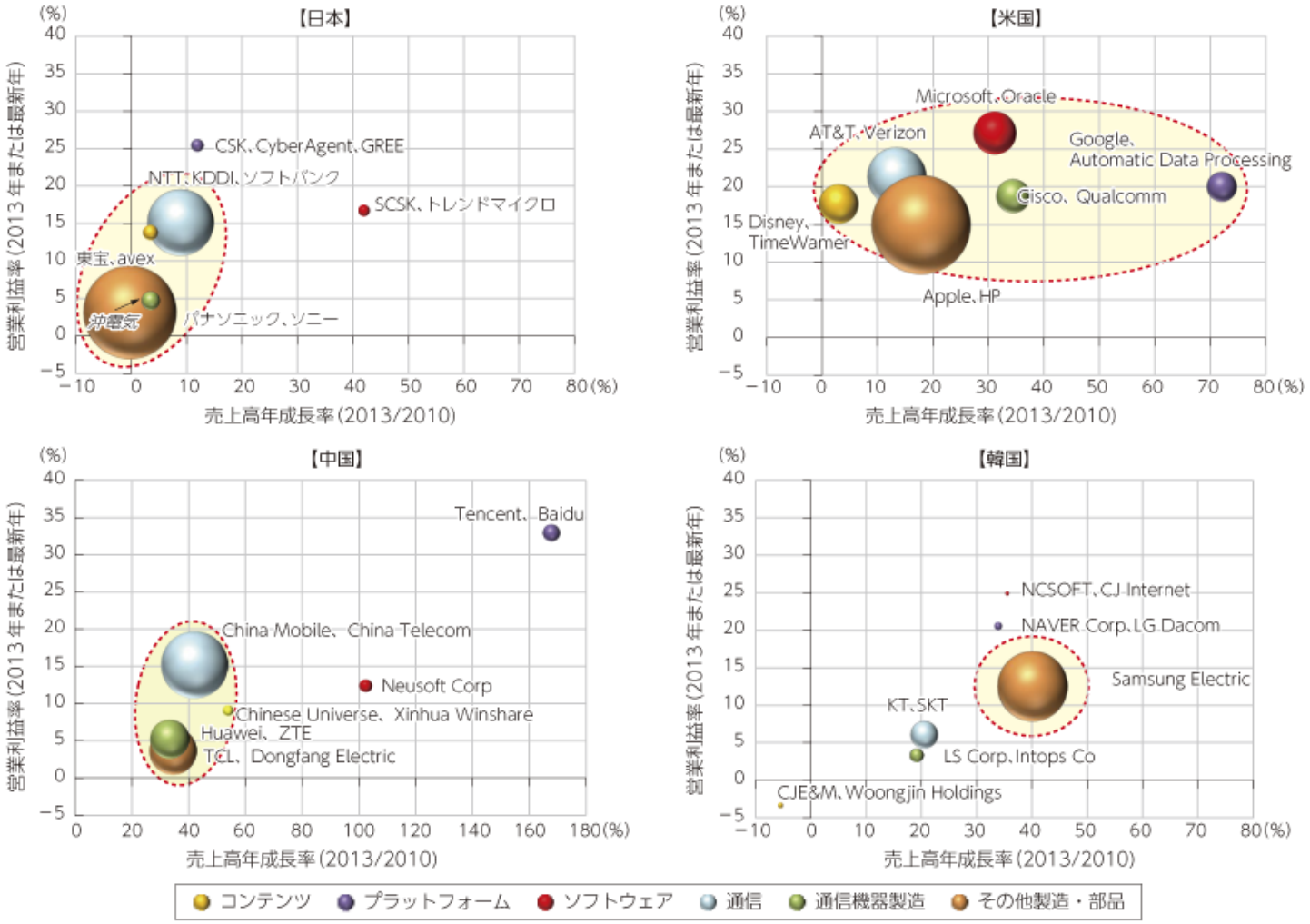
2014年版　情報通信白書　（総務省）

各国の産業レイヤー別利益率



2014年版　情報通信白書　（総務省）

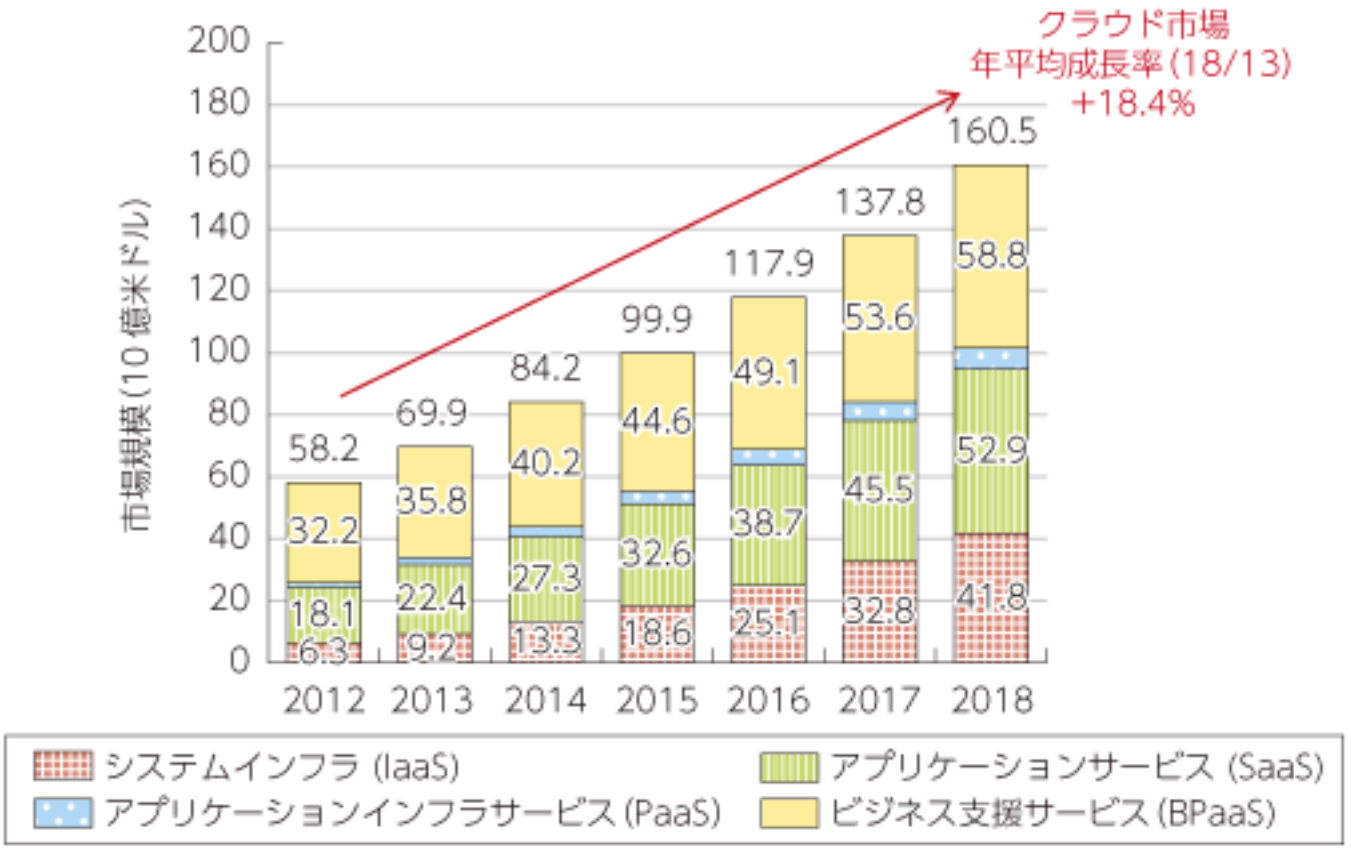
各国の業種別利益率と成長率



※バブルの大きさは売上高（2013年または最新年）
※バブルは当該業種全体の売上高を示し、企業名は該当バブル内で売上高が大きい主な企業の例示である。

2014年版　情報通信白書　（総務省）

ICTサービスレイヤー：クラウドの浸透



2014年版　情報通信白書　（総務省）

クラウドサービス

- IaaS(Infrastructure as a Service)

インターネットを利用したコンピュータの利用形態である。IaaSでは、コンピュータシステムを構築および稼動させるための基盤（仮想マシンやネットワークなどのインフラ）そのものを、インターネット経由のサービスとして提供する。Amazon EC2

- SaaS(Software as a Service)

必要な機能を必要な分だけサービスとして利用できるようにしたソフトウェア（主にアプリケーションソフトウェア）もしくはその提供形態のこと。一般にはインターネット経由で必要な機能を利用する仕組みで、シングルシステム・マルチテナント方式になっているものを指す。Google Apps

- PaaS(Platform as a Service)

アプリケーションソフトが稼動するためのハードウェアやOSなどのプラットフォーム一式を、インターネット上のサービスとして提供する形態のことを指します。

- BPaaS(Business Process as a Service)

ビジネス・プロセス・アズ・ア・サービス（BPaaS）とは、比較的新しいコンセプトであり、ビジネス・プロセス・マネジメント（BPM）に、SaaS・IaaS・PaaSといったクラウドサービスの形態を組み合わせたものである。BPMでは営業、生産、販売、サポートなど個々の企業活動を一連のプロセスとして捉え、企業の戦略や目標を実現するために最適なプロセスを設計し、実際の業務に適用する。

4. ICTと情報セキュリティ

- 初期の頃は善意のユーザーのみを想定しており、悪意のある第三者が介在することは想定していない。
- 1967年に始まったARPANET（パケット通信ネットワーク）は利用する人の大半は研究者であり、悪意のある人はいないし、利用する人も技術に精通した人達であった。
- 現在では幼児から高齢者、良い人から悪い人、ICTに詳しい人から無関心な人、様々な人達が色々な利用の仕方。
- 同じ端末でも人によっては、まったく違う利用の仕方
- セキュリティを考えたときに的を絞ることが難しい

情報インシデント

- 情報の漏洩

  ICTは情報を効率良く編集・伝達・公開するためのもの、あるいはそのような思想で設計されている。

- 情報の改ざん

  ICTは情報を効率良く編集・伝達・公開するためのもの、初期の頃は悪意の第三者がいる想定にはない。

- 情報アクセスの中断・停止

  インターネットは元々特定の箇所がアクセス不可になっても全体として動作するような設計。特定の箇所がアクセス不可になることを前提としている。

- 情報システムの乗っ取り・踏み台

ベネッセ個人情報流出事件

- 2014年7月9日（発覚）
- この事件は、流出した顧客情報が最大で2070万件に及ぶ大規模なもの。流出した情報は、進研ゼミなどといったサービスの顧客の情報であり、子供や保護者の氏名、住所、電話番号、性別、生年月日など。ベネッセ側は、社内調査により、データベースの顧客情報が外部に持ち出されたことから流出したと説明。これはベネッセの顧客に、ベネッセのみに登録した個人情報を使った、別の通信教育を行う会社からのダイレクトメールが届くようになり、ベネッセから個人情報が漏洩しているのではないかという問い合わせの急増により発覚した。

by Wikipedia

ベネッセ個人情報流出事件

- 充電のためにスマートフォンを接続したところ、スマートフォンがストレージデバイスとして認識され、データ移行が可能になってしまった点が犯行への決定打となった。しかし、もちろんベネッセ側も情報漏えい対策を何もしていなかったわけではない。24時間体制のセキュリティ監視、書き込み禁止のデバイス制御 環境、担当者の私物検査や持ち込み制限といった施策を行っていた。
- ベネッセの対策のどこに落ち度があったのか。辻伸弘氏は次の2点に絞られると述べた。
  - ✓ スマートフォンを持ち込ませてしまったこと
  - ✓ PTP（Picture Transfer Protocol）／MTP（Media Transfer Protocol）制御の不備
- 抜粋 http://www.itmedia.co.jp/enterprise/articles/1411/18/news044.html

媒体別情報漏洩

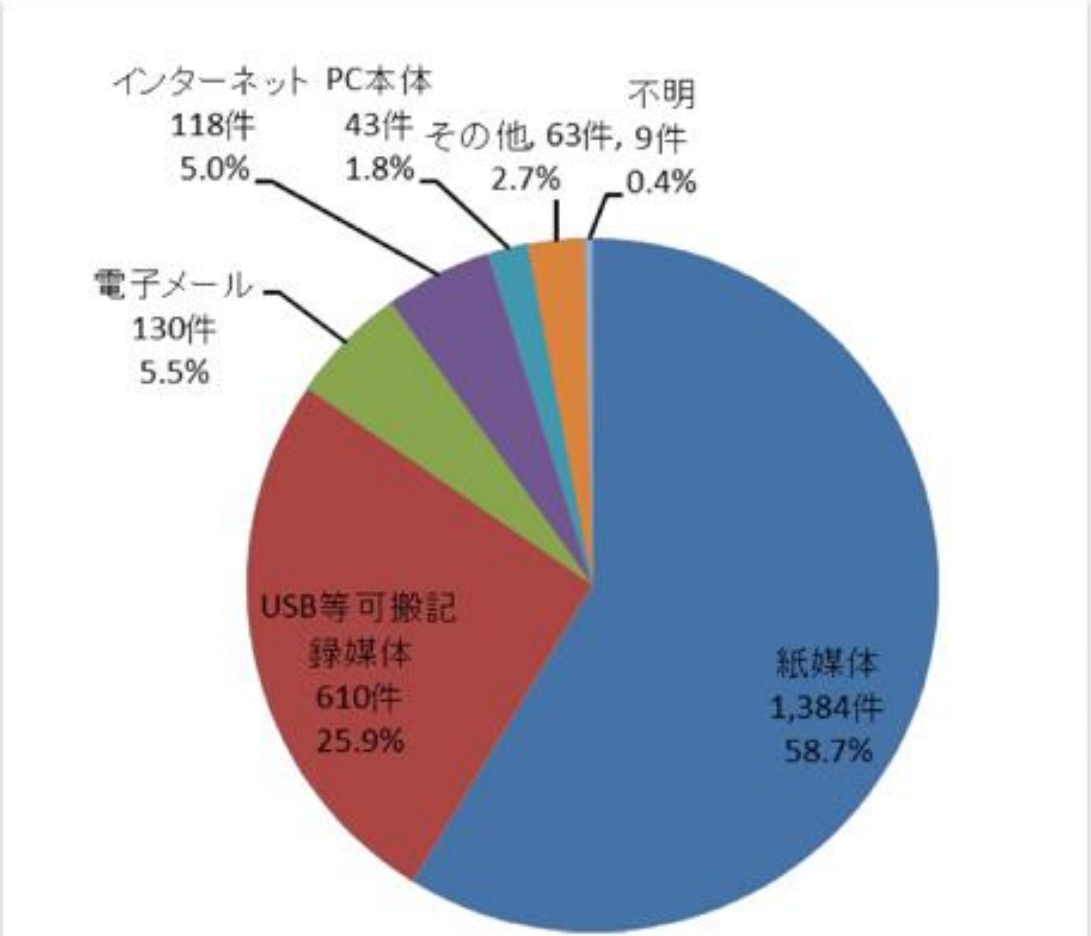


図 3-16：漏えい媒体・経路（件数）

JNSA「2012年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」

年金機構情報流出事件

- 2015年6月
- 今回の情報漏えいは、「標的型メール」と呼ばれる添付ファイル付きのメールがきっかけとなった。一般に公開されている年金機構のアドレス宛てに5月8日に届いたメールがそれで、「厚生年金基金制度の見直しについて（試案）に関する意見」というタイトルで、LZH方式の圧縮ファイルが添付されていた。
- この添付ファイルを開くと、WordやPDFのアイコンが付いたファイルが現れる。一見すると普通の文書ファイルに見え、ダブルクリックすれば実際に文書が表示される。しかし、これらは本当は実行形式のプログラムであり、表示される文書は“おとり”なのだ。ファイルを開いたパソコンは即座にウイルスに感染してしまうが、開いた当人はウイルス感染に気づかないままでいた可能性が高い。

抜粋 http://trendy.nikkeibp.co.jp/article/column/20150616/1065252/?rt=nocnt

年金機構情報流出事件

- 今回の日本年金機構からの情報漏えいは、Emdiviと呼ばれるウイルスによるものだったことが分かっている。
- 添付された圧縮ファイルをダブルクリックすると、2つのファイルが開かれる。1つがおとりファイルで、受信者が興味を引きそうな文章が開く。これにより、ファイルを開いた被害者は 怪しまずにそのまま放置してしまうのだ。この裏で、もう1つのファイル「RAT」＝遠隔操作ツールが実行される。これがEmdiviだ。
- Emdiviはブラウザーに登録されているパスワードとIDを抜き出すツールを起動する。これを実行すると、IE（インターネットエクスプローラ）、Chrome、Firefoxなどのブラウザーに登録されたユーザー名とパスワードの一覧を表示する。犯人はこのパスワードを使って、他のシステムへの侵入に使っていると思われる。

抜粋
http://trendy.nikkeibp.co.jp/article/column/20150616/1065252/?rt=nocnt

年金機構情報流出事件

- Emdiviはもう一つのメール関連のデータを盗み取るツールも起動する。被害組織の中で使われているメールアドレスや、メールサーバーのIPアドレス、被害端末で使われているメールサーバーへのログイン用IDやパスワードを盗むためのツールだ。
- これにより、メールの内容がすべて攻撃者に筒抜けになってしまう。情報漏れが起きるだけでなく、ここから標的型攻撃メールの宛先を増やすことにもつながる。また、添付ファイルを実際に使われたものに置き換える、といった攻撃のブラッシュアップも可能になるだろう。
- Windowsのログイン名やドメイン名（組織名）、パスワードを盗み取るツールも起動する。
- 他各種の情報抜き取りツールを起動する。

抜粋
http://trendy.nikkeibp.co.jp/article/column/20150616/1065252/?rt=nocnt

標的型攻撃

- ソーシャルエンジニアリングを悪用して標的のユーザに対して「標的型メール」を送る、あるいは待ち受けサイトにて、不正プログラムの実行や悪意あるWebサイトに誘導する方法。
- 企業・組織の内部サーバへ侵入する目的のために、まずは一般社員の端末を不正プログラムで感染させることで支配下に置き、内部ネットワークへの入り口とする。
- 内部ネットワークに侵入した攻撃者は、辞書攻撃やブルートフォース攻撃（総当たり攻撃）などで、サーバのDomain Admin権限を奪取する。

水飲み場型攻撃

- Webを使った標的型攻撃（2012年頃から）
- Webページを改ざんし、ねらった標的のみにウイルスを感染させるような“わな”を仕掛ける。
- 通常は、ソフトウエアの脆弱性を突くプログラムが仕込まれているので、Webページにアクセスするだけで、ウイルスに感染する恐れがある。JavaやInternet Explorer（IE）といった、広く使われているソフトウエアの脆弱性を悪用することが多い。
- 標的ユーザーにだけウイルスを配布
- ペネトレーション（脆弱性診断）などでは発見が困難

Advanced Persistent Threat (APT)

- 先進的な持続的脅威
- 標的型攻撃の一種に分類されるサイバー攻撃
- 「特定の組織に不正侵入し、時間や手段などを問わず目的達成に向け標的に特化して行う継続的な攻撃」（トレンドマイクロ）

Advanced Persistent Threat (APT): 招かれざる侵入者

長期間にわたってネットワーク内の情報を取得し、検出を回避する攻撃者の手口

1. 侵入
攻撃者はソーシャルエンジニアリングを利用して、脆弱なシステムや従業員に標的を絞ったマルウェアを送り、ネットワークに侵入します。

2. 検出
侵入した攻撃者は、検出されないように「身を潜めてゆっくりと(low and slow)」活動します。 その後、内部から企業のセキュリティ対策を解読し、戦術を組み立て、成功を収めるために複数のキルチェーン（攻撃プロセス）を並行して配置します。

3. 取得
攻撃者は保護されていないシステムにアクセスし、長期間にわたって情報を取得します。
また、マルウェアをインストールし、気づかれないようにデータを入手したり、業務を中断させます。

4. 転送
取得された情報は、さらなる悪用や詐欺行為などのため、攻撃者の本拠地に送信されます。

基本的なセキュリティ対策

- パソコンの基本的な管理

  パスワードロック（推測されにくいパスワード）

  ウイルス対策ソフトのインストール、最新のパターンファイル

  最新のOS・アプリであるか

- 情報の管理（持ち出し）

  不必要な持ち出しをしない（出来ないようにする）

  ファイルの暗号化、パスワード

  例）ベネッセ

- パソコンや記憶媒体の廃棄について

  完全な消去・廃棄（FormatだけではX）

- 管理者や経営者はインシデントが発生することを想定し、対策を検討しておく。

一般的な注意事項

- フィッシングサイトに注意
- 個人情報の書き込み
- 標的型攻撃の手口を知ろう
- SNSのマナーとリスク
- オンラインショッピングでの注意
- ネットオークションに注意
- 出会い系サイトに注意

フィッシングの被害を避けるために

- 明らかに必要のないメールは開かず削除

  最大の防御法は、スパムメール同様、送信者や件名から判断して明らかに必要のないメールは開かずに削除することです。

- メールの内容をよく確認した上で冷静に対応

  クレジットカード会社や金融機関が、クレジットカードの番号や暗証番号をホームページ上で入力するように求めるメールを送ってくることはまずありません。

- 迷惑メールやSNS上のリンクをむやみにクリックしない

  見知らぬ相手からのメールに記載されたリンクや、SNS上に投稿された怪しげな広告リンクのクリックなどは安易になわない。（PCの遠隔操作事件）

- 主業務PCとメールやブラウザをするPCを分ける

  非PC・Email系の通信手段(スマホでLINE/FaceBook)を考慮したほうが良い？

個人情報の書き込み

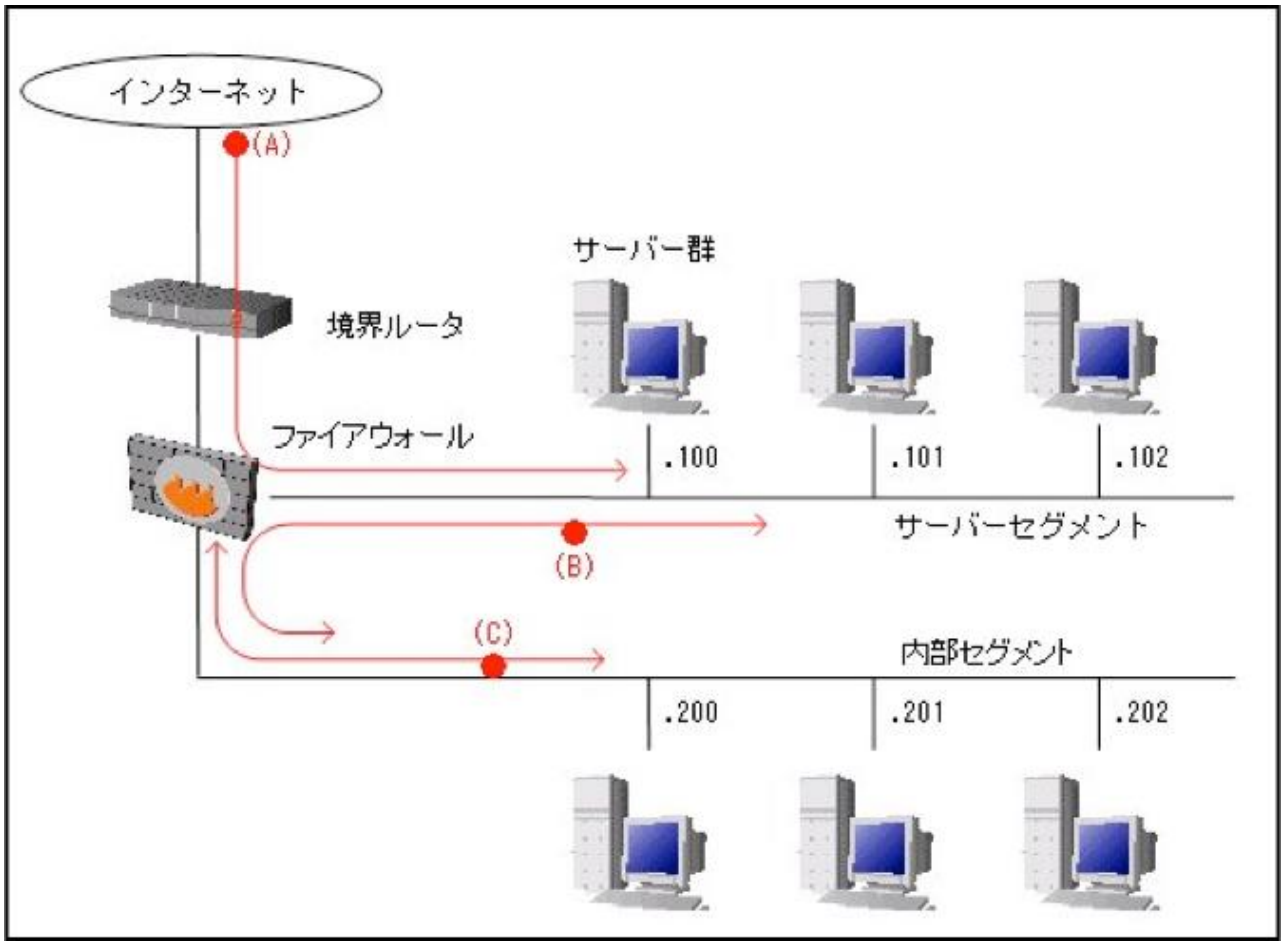
- 自分の不注意や知識不足で、軽い気持ちで怪しいWebサイト（SNS、掲示板、Twitter）に個人情報を記載し、個人情報を漏らしてしまう可能性も考えられます。
- 人肉検索の対象になる
- ソーシャルエンジニアリング（ソーシャルハッキング）の対象になる。

Social engineering : 社会工学
大規模な集団における、大衆の姿勢や社会的なふるまいの影響への働きかけを研究する学問。社会と個人の関係、サイバー空間と個人の関係に関する研究分野
人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する方法のこと。

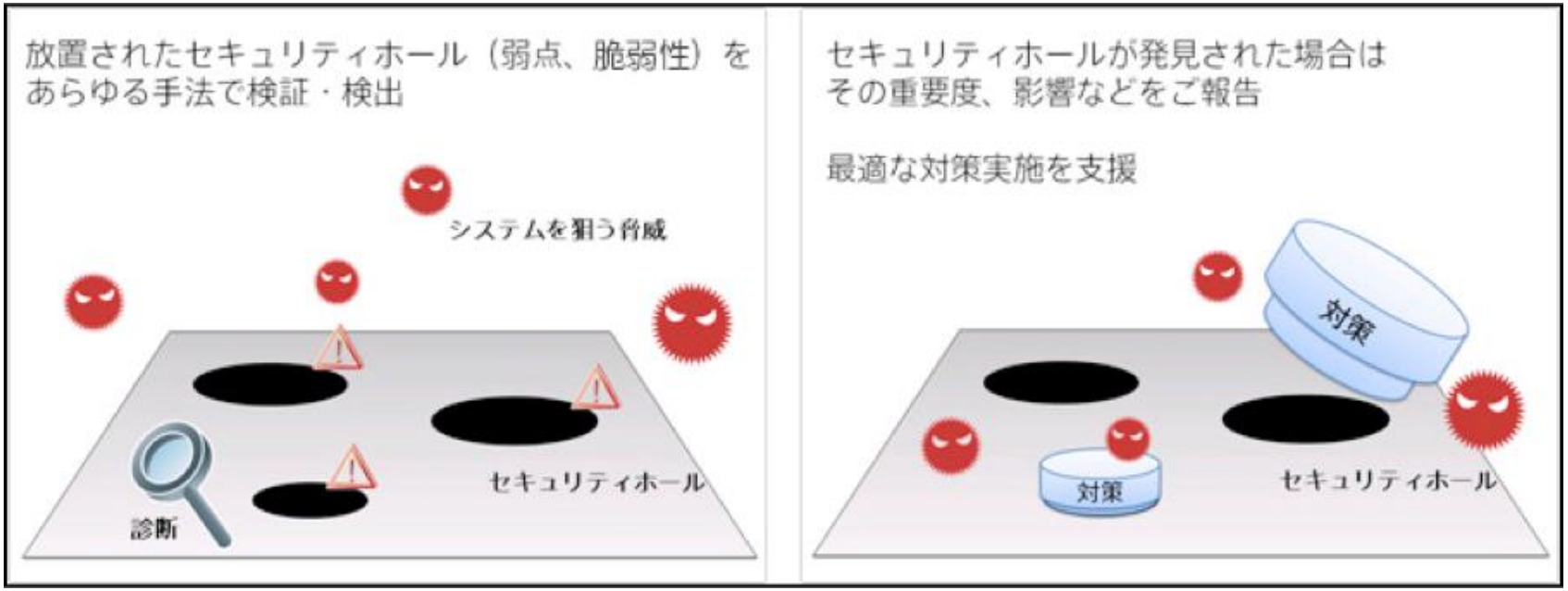
サーバーの脆弱性診断

- 対象となるシステムに存在するセキュリティホール（弱点、脆弱性）を発見・検出
- 結果に基づいてセキュリティホールを塞ぐことにより、侵入、改ざん、情報漏えいなどのインシデントによる被害を未然に防ぐことができる。

http://itpro.nikkeibp.co.jp/article/COLUMN/20060816/245784/



(A)攻撃者と同じ条件で検査できる。脆弱性が検出された場合は，緊急に対策する必要とする。ファイアウオールやIDS／IPSの効果も測定できる。
(B)各サーバーの脆弱性を詳しく検査できる。例えば，サーバー・セグメントを踏み台とした内部セグメントやデータベース・サーバーなどへの侵入の可否について検査することができる。
(C)内部セグメントのクライアントPCの脆弱性や，内部セグメントからサーバー・セグメントへのアクセス制御の効果（内部からの不正アクセスの可能性）について検査できる。



ロブラックボックス型

動作している対象システムに対し、実際に擬似的な侵入・攻撃を仕掛ける。
別名：ペネトレーションテスト（Penetration 貫通・挿入）

ロホワイトボックス型

システムの設計書、仕様書、設定情報、ソースコードなどをもとに、机上で診断。

ブラックボックス型

- Webアプリケーション脆弱性検査

  Webアプリケーションの脆弱性を検出することを主にしたツール。不正なHTTPリクエストを送信し擬似攻撃を行うことで、クロスサイトスクリプティングやSQLインジェクション等を見つけることができる。

- ネットワーク脆弱性検査

  ネットワークレイヤの脆弱性を見つけることを目的としたツール。サーバやネットワーク機器の設定不備やパッチ適用の不備による、バッファオーバーフロー等の脆弱性を見つけることができる。

ブラックボックス型

- Webアプリケーション脆弱性検査ツール

  リモート診断、ソースコード/設計仕様書等による診断

  - ✓ AppScan [IBM]
  - ✓ webinspect [Hewlett-Packard]
  - ✓ VEX -Vulnerability Explorer [ユービーセキュア]

- ネットワーク脆弱性検査ツール

  原則としてネットワーク層のリモート診断のみ

  - ✓ SecureScout [SecureScout]
  - ✓ QualysGuard [Qualys]
  - ✓ Nessus [Tenable Network Security]
  - ✓ Retina [eEye Digital Security]
  - ✓ Penetrator [Penetrator Vulnerability Scanner]
  - ✓ ISS Internet Scanner [IBM]
  - ✓ McAfee Vulnerability Manager [McAfee]

tenable network security

- HOME Edition は Free
  ただし検査対象はプライベートアドレスのみ
  商用使用は禁止
- Enterprise Edition は $2,190/年
- WindowsおよびMac OS X、各種Linux、FreeBSD、Solaris向けのバイナリパッケージが用意

NESSUS診断レポート

Summary

Critical	High	Medium	Low	Info	Total
1	0	2	2	23	28

Details

Severity	Plugin Id	Name
Critical (10.0)	33850	Unsupported Unix Operating System
Medium (4.3)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (4.3)	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10107	HTTP Server Type and Version
Info	10263	SMTP Server Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11219	Nessus SYN scanner

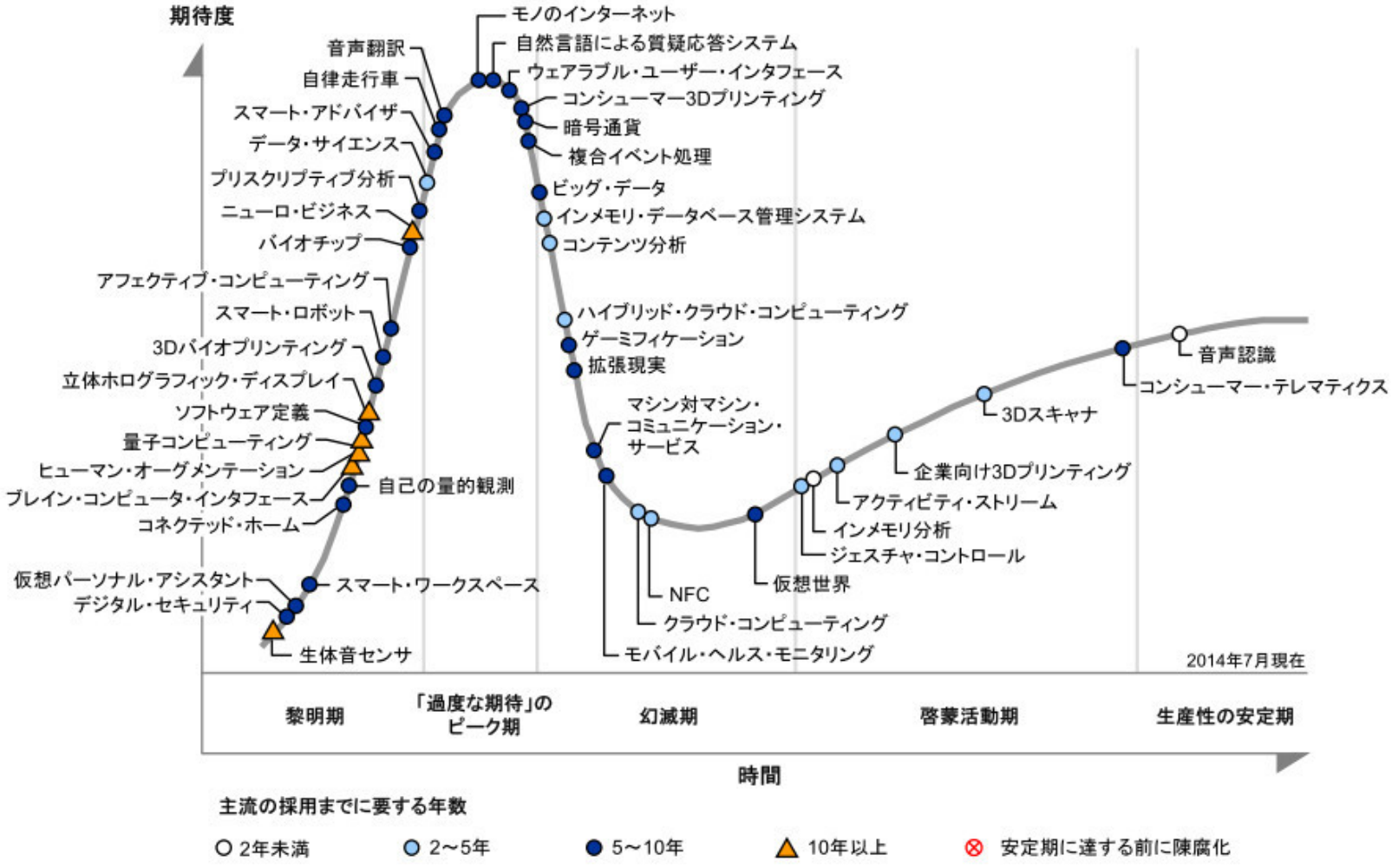
5. 今後のICTは？

- 米国ガートナー（調査会社）、「先進テクノロジー・ハイプサイクル（Emerging Technologies Hype Cycle）」2013年版リポート（2013年8月19日）

- 【ハイプ・サイクル】
- 新技術が登場し実際に普及するまでに、メディアやユーザーの期待が時間経過とともに、どう変化していくかを示したサイクル。

- **黎明期**：新技術への関心が高まる時期。新製品発表やその他のイベントが報道され、関心が高まる。
- **流行期**：期待が最も大きい時期。成功事例が出ることもあるが、多くは失敗に終わる。
- **幻滅期**：急速に関心が失われる時期。メディアはその話題や技術を取り上げなくなる。
- **回復期**：利点と適用方法が徐々に理解されるようになる時期。 メディアでその技術が取り上げられなくなる一方、いくつかの事業は「啓蒙の坂」を登りながら継続し、その利点と適用方法を理解するようになる。
- **安定期**：本格的な導入や採用が行われる時期。広範に宣伝され受け入れられるようになると、技術は「生産性の台地」に到達する。

ガートナー
「先進テクノロジのハイプ・サイクル：2014年」



近い将来

- ウェアラブルコンピュータとIoT

腕時計形のコンピュータや、PDA、小型コンピュータ、付随する通信装置やセンサ類（カメラやGPS受信装置など）

Google Glass, iWatch

http://www.apple.com/jp/shop/watch

http://ideahack.me/article/156

Internet of Things：IoT

- クラウド、ソーシャル、ビッグデータに続く重要トレンドとして「モノのインターネット」（Internet of Things：IoT）が注目を集めている。 IoTの概念そのものはそれほど難しいものではない。従来型のインターネットがコンピューターのネットワークであったのに対して、テクノロジーの進化により、今まではネットワークに接続されていなかった「モノ」がインターネットを介して情報をやり取りする能力を備えていくということだ。

by http://enterprisezine.jp/iti/detail/5741

- ユビキタスを技術面から捉えた概念
- 端末数の爆発　＞　IPv6は必要不可欠か？

ICTは今後どうなるか

- ICTの急速な発展・進化は、確かにアルビントフラーの予言したように、人間社会に劇的な変化をもたらしているようだ。
- しかしその劇的な変化は人間社会にとって、良いものなのか悪いものなのか？、どの方向に向かっているか？は誰も良く判っていない。
- まるでコックリさんのようにミスリードも可能であり、全体としては予測不可能

とはいいつつも、これだけは！

- ICT産業は世界的にも成長が見込まれる。
- 特にアジアは著しい経済成長が見込まれる。
- ICT産業は頭脳さえあれば成長が可能な分野。（中小企業でもビッグになれる可能性大）
- ICT産業は社会にとって重要なインフラであり続ける。
- IoTの本格普及を前にしてセキュリティ環境の整備は急務。