Network Security and e-government

Dr. Suguru Yamaguchi

Nara Institute of Science and Technology

Who am I?

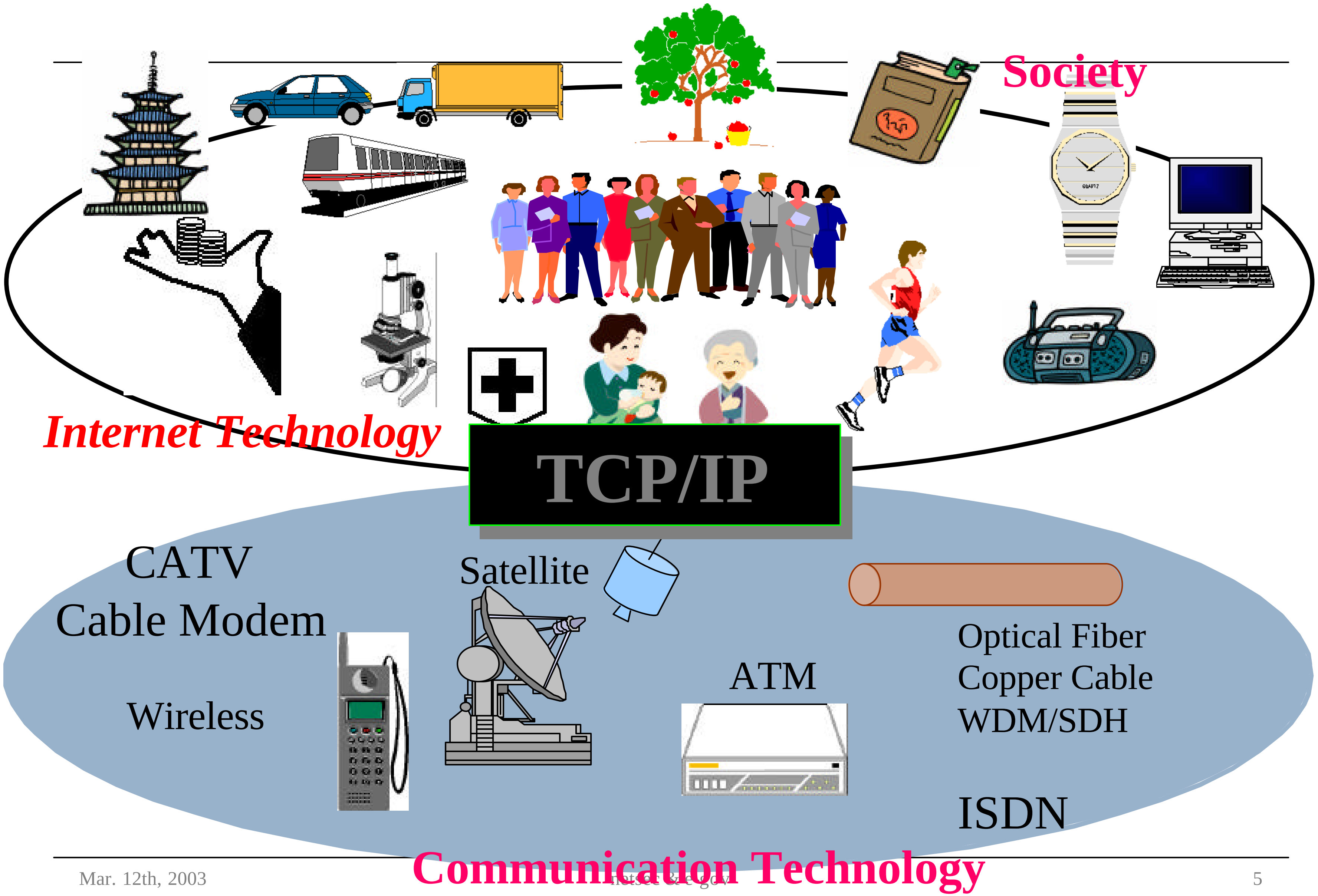
- Professor in graduate school of information science, Nara Institute of Science and Technology.
- Chairman of JPCERT/CC, which is CSIRT established in 1995 in Japan covering whole the nation as its constituency.
- Member of review board for JP government's E-government initiative called "e-Japan" project.

Agenda

- What should we do for protecting our infrastructure called "Internet"?
- Going “*e* way” even in government, benefits and risks
- Our case study in JP government
- Regional activities for internet security in AP region

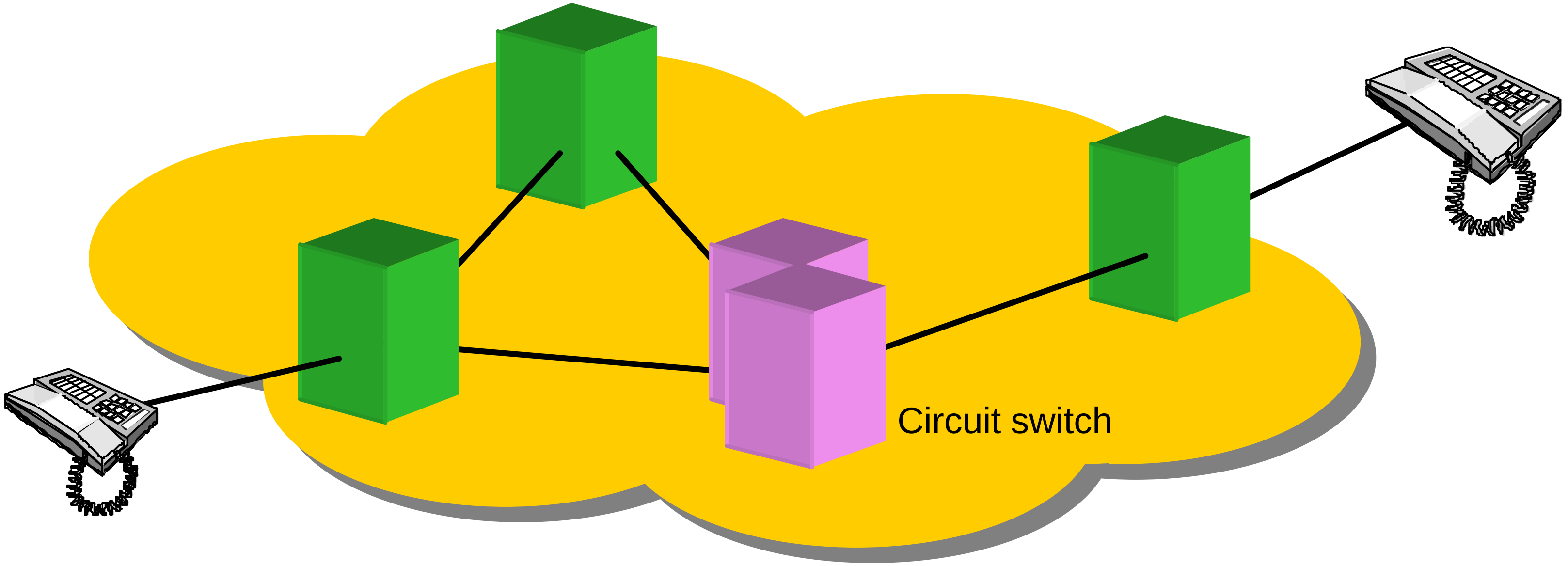
Internet and its current challenges

Internet: Global and Ubiquitous Infrastructure for Communication



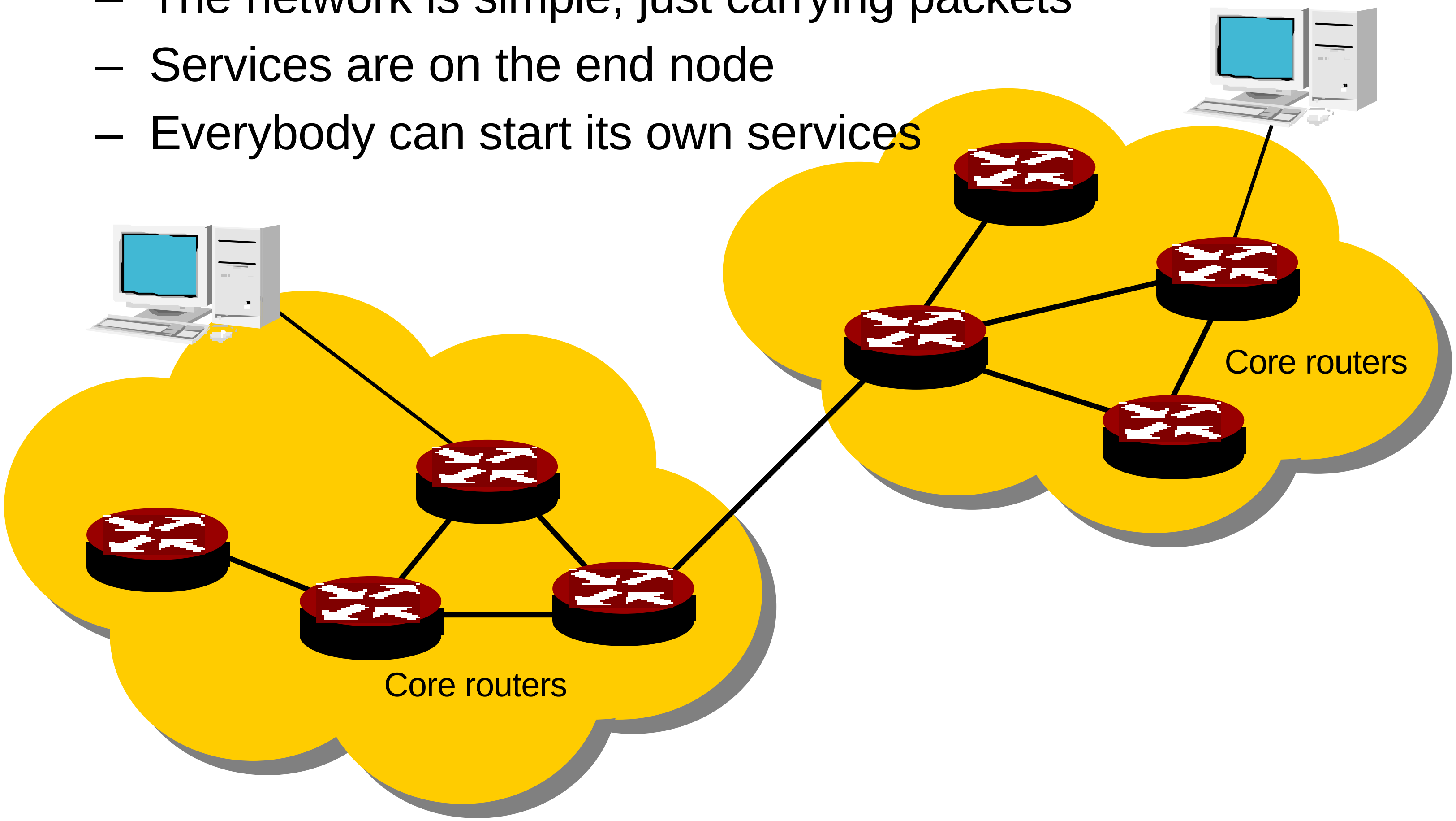
PSTN: services are defined by network

- Network as service infrastructure
  - End node (terminal) is simple & cheap
  - Services are provided by the network
    - Large investment is required, because there is no “small start”.
    - Only the network operators (telephone companies) have control on which services are provided.

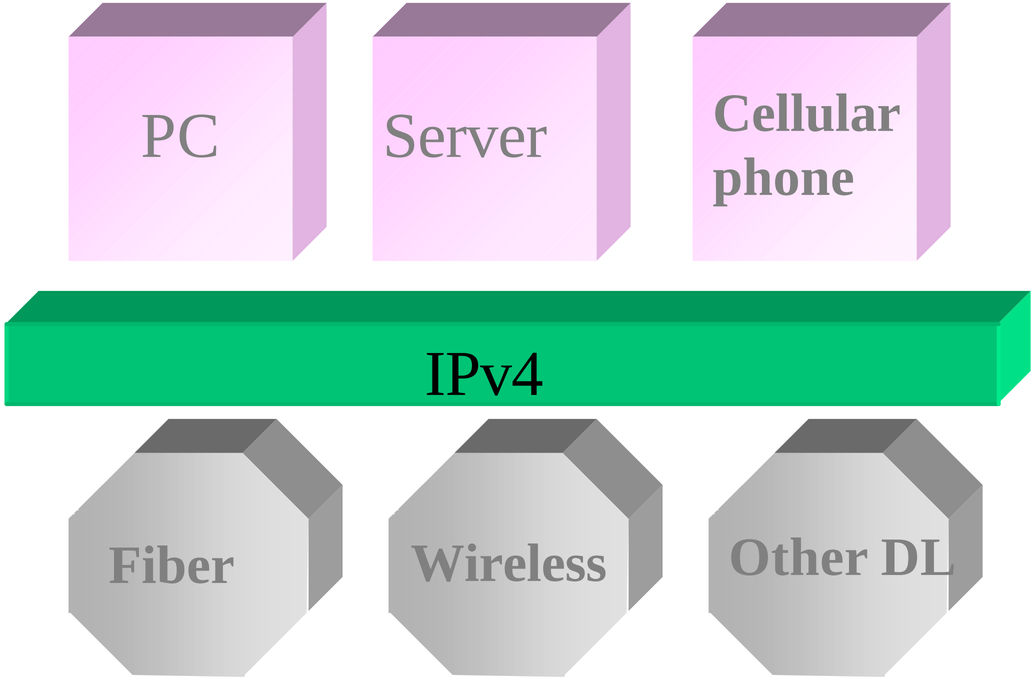


Internet: services are defined by end node

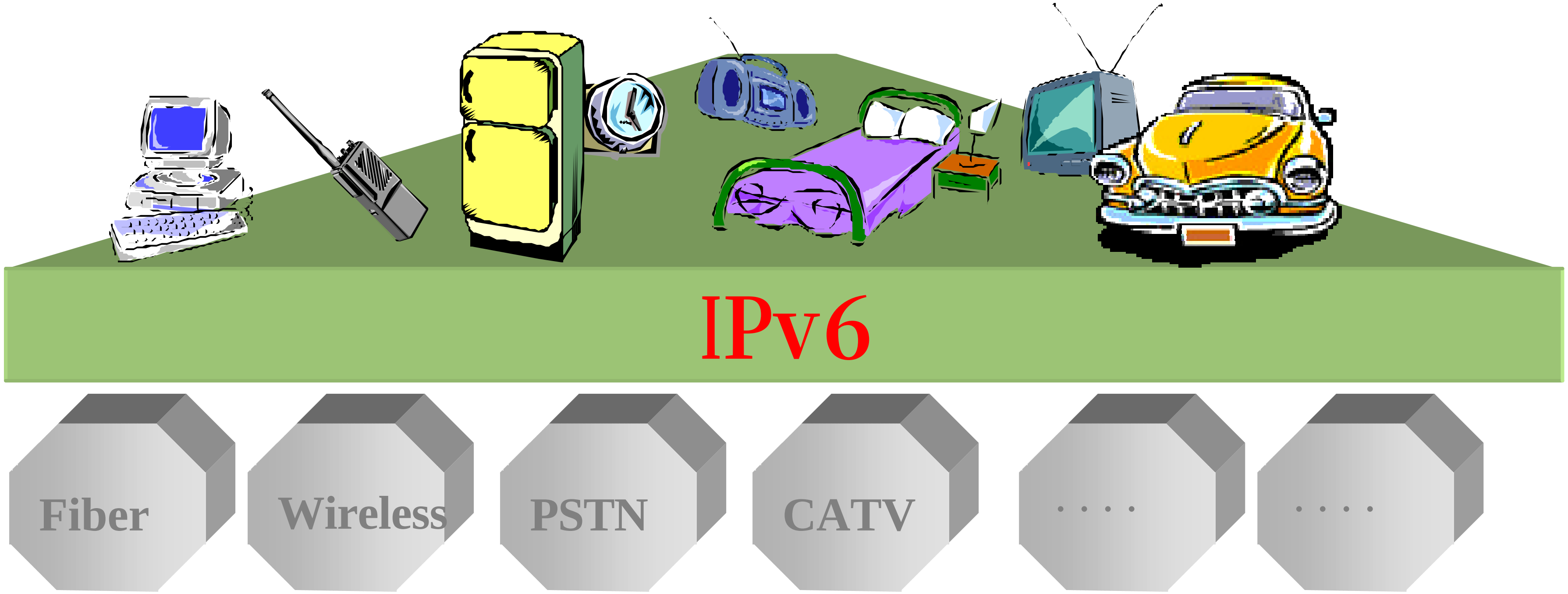
- End-to-End model
  - The network is simple, just carrying packets
  - Services are on the end node
  - Everybody can start its own services



Internet in “Today”



Internet for everything



Business on the Internet

- Many businesses rely on communication infrastructure
  - At beginning, banking and money transfer infrastructure
  - Some of current existing functions are implemented on the Internet
    - CALS/EDI
    - Online banking, trading, procurement, ….
- Large firms, small businesses and individuals are now using the Internet for their business
  - Internet is an universal digital/computer communication infrastructure
  - E-mail and WWW are vital

Challenges fore more deployment

- Coverage
  - Equal access
- Security
  - The Internet is now carrying actual “goods”
  - Protecting our money is highly required, similar to the actual world.
- Social System
  - Harmonize with current existing social systems
    - Law, “de facto” commerce procedures, ….
    - Provide a method to resolve civil cases even digital infrastructure is used.

E-Government

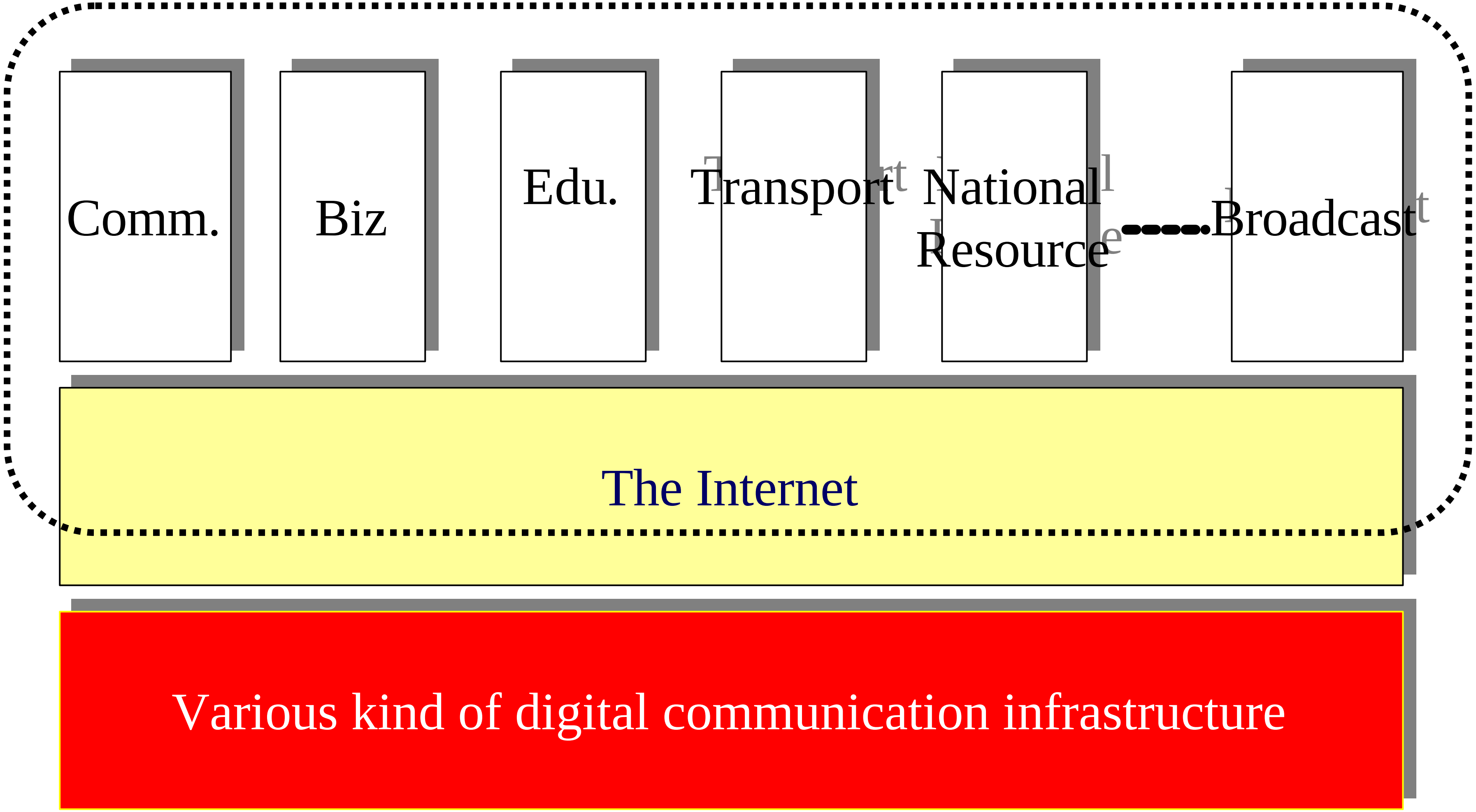
What is e-government? (1)

- Online services for public administration
  - Businesses go online. Why doesn’t the Government go online?
  - Use computer & network in the process between public and privates
    - Ex. JP government case
    - Approx. 2000 procedures are existing between public/private interaction (notification, permissions, ….)
    - Remove “by document, with actual stuff, at office” principal
    - By 2005, 1360 procedures will be online.

What is e-government? (2)

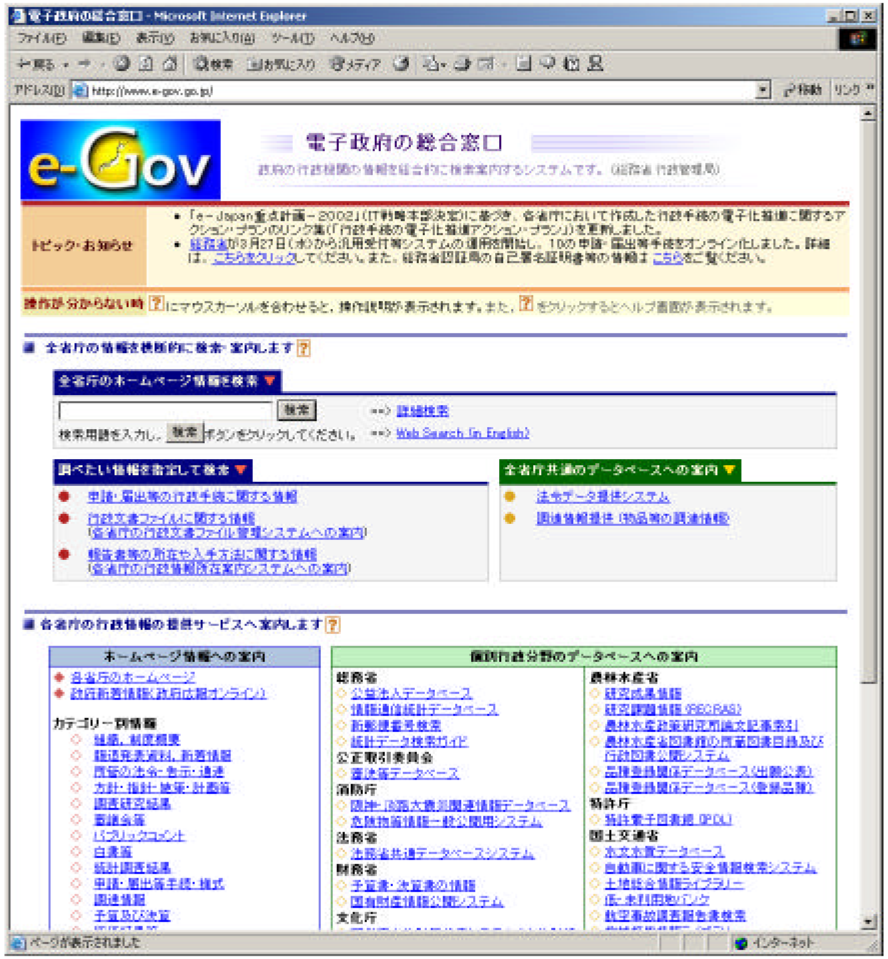
- Steps forward to “Business Process Restructuring”
  - High performance government
  - Interaction between national and regional
    - Delegates the actual process to regional administration body
    - Ex. Issuing passport, drivers’ license, car registration, …
  - Making communication infrastructure for various kind of “public services” by both national and regional administration body

E-government in 2005 (JP)



http://www.e-gov.go.jp/

- E-gov portal site
  - One stop service
  - Single window service
  - “online”


電子政府の総合窓口 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り メディア
アドレス(D) http://www.e-gov.go.jp/
移動 リンク
e-Gov

電子政府の総合窓口

政府の行政機関の情報を総合的に検索案内するシステムです。（総務省 行政管理局）

トピック・お知らせ

- 「e－Japan重点計画－2002」（IT戦略本部決定）に基づき、各省庁において作成した行政手続の電子化推進に関するアクション・プランのリンク集（「行政手続の電子化推進アクション・プラン」）を更新しました。
- 総務省が3月27日（水）から汎用受付等システムの運用を開始し、10の申請・届出等手続をオンライン化しました。詳細は、こちらをクリックしてください。また、総務省認証局の自己署名証明書等の情報はこちらをご覧ください。

操作が分からない時 ? にマウスカーソルを合わせると、操作説明が表示されます。また、? をクリックするとヘルプ画面が表示されます。

■ 全省庁の情報を横断的に検索・案内します ?

全省庁のホームページ情報を検索

[検索] ==> 詳細検索

検索用語を入力し、[検索]ボタンをクリックしてください。 ==> Web Search (in English)

調べたい情報を指定して検索

- 申請・届出等の行政手続に関する情報
- 行政文書ファイルに関する情報（各省庁の行政文書ファイル管理システムへの案内）
- 報告書等の所在や入手方法に関する情報（各省庁の行政情報所在案内システムへの案内）

全省庁共通のデータベースへの案内

- 法令データ提供システム
- 調達情報提供（物品等の調達情報）

■ 各省庁の行政情報の提供サービスへ案内します ?

ホームページ情報への案内

- 各省庁のホームページ
- 政府新着情報（政府広報オンライン）

カテゴリー別情報

- 組織、制度概要
- 報道発表資料、新着情報
- 所管の法令・告示・通達
- 方針・指針・施策・計画等
- 調査研究結果
- 審議会等
- パブリックコメント
- 白書等
- 統計調査結果
- 申請・届出等手続・様式
- 調達情報
- 予算及び決算

個別行政分野のデータベースへの案内

総務省
- 公益法人データベース
- 情報通信統計データベース
- 郵便番号検索
- 統計データ検索ガイド

公正取引委員会
- 審決等データベース

消防庁
- 阪神・淡路大震災関連情報データベース
- 危険物等情報一般公開用システム

法務省
- 法務省共通データベースシステム

財務省
- 予算書・決算書の情報
- 国有財産情報公開システム

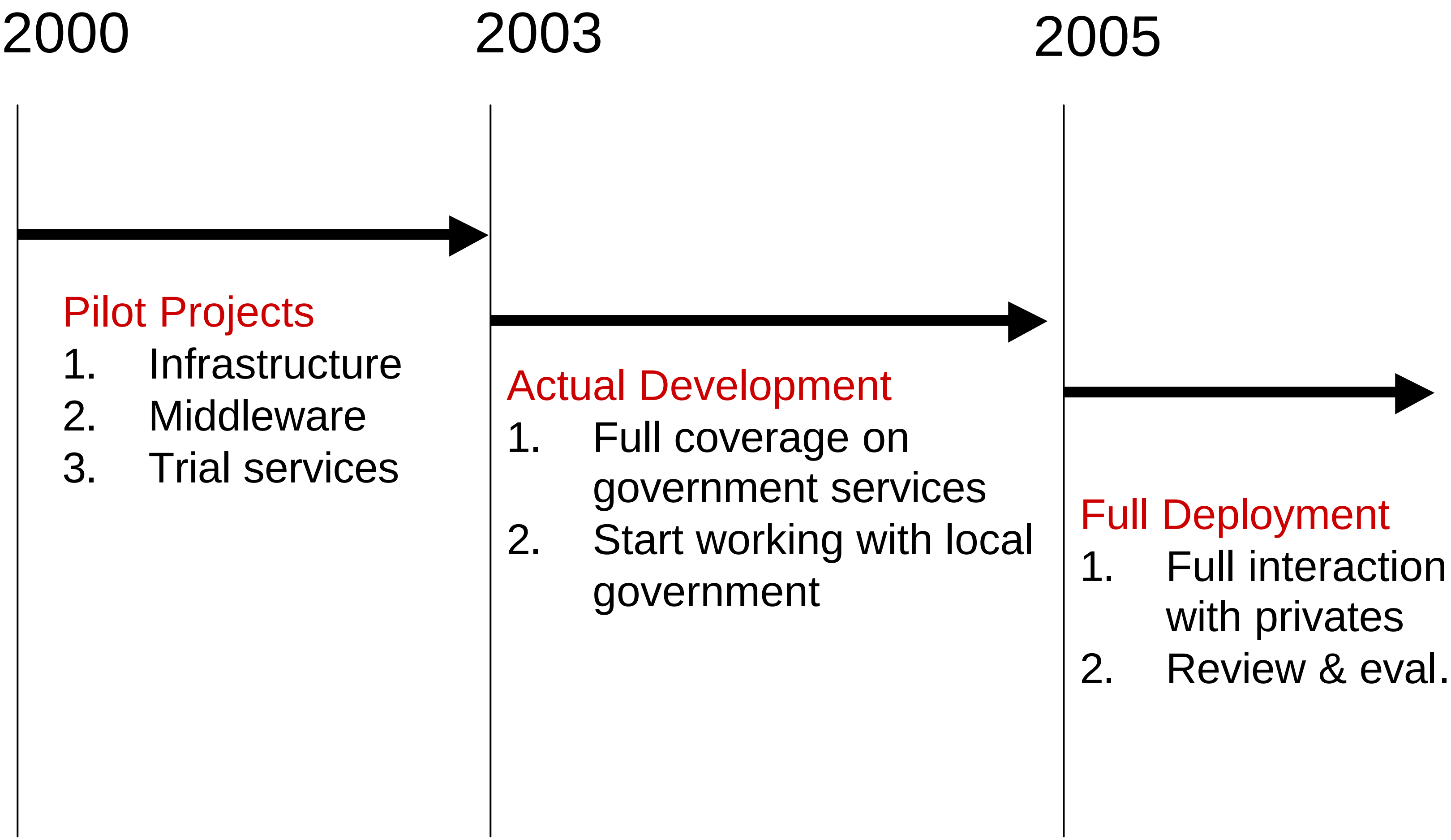
文化庁

農林水産省
- 研究成果情報
- 研究課題情報 (RECRAS)
- 農林水産政策研究所論文記事索引
- 農林水産省図書館の所蔵図書目録及び行政図書公開システム
- 品種登録関係データベース（出願公表）
- 品種登録関係データベース（登録品種）

特許庁
- 特許電子図書館 (IPDL)

国土交通省
- 水文水質データベース
- 自動車に関する安全情報検索システム
- 土地総合情報ライブラリー
- 低・未利用地バンク
- 航空事故調査報告書検索

Development Process



2000

2003

2005

Pilot Projects

1. Infrastructure
2. Middleware
3. Trial services

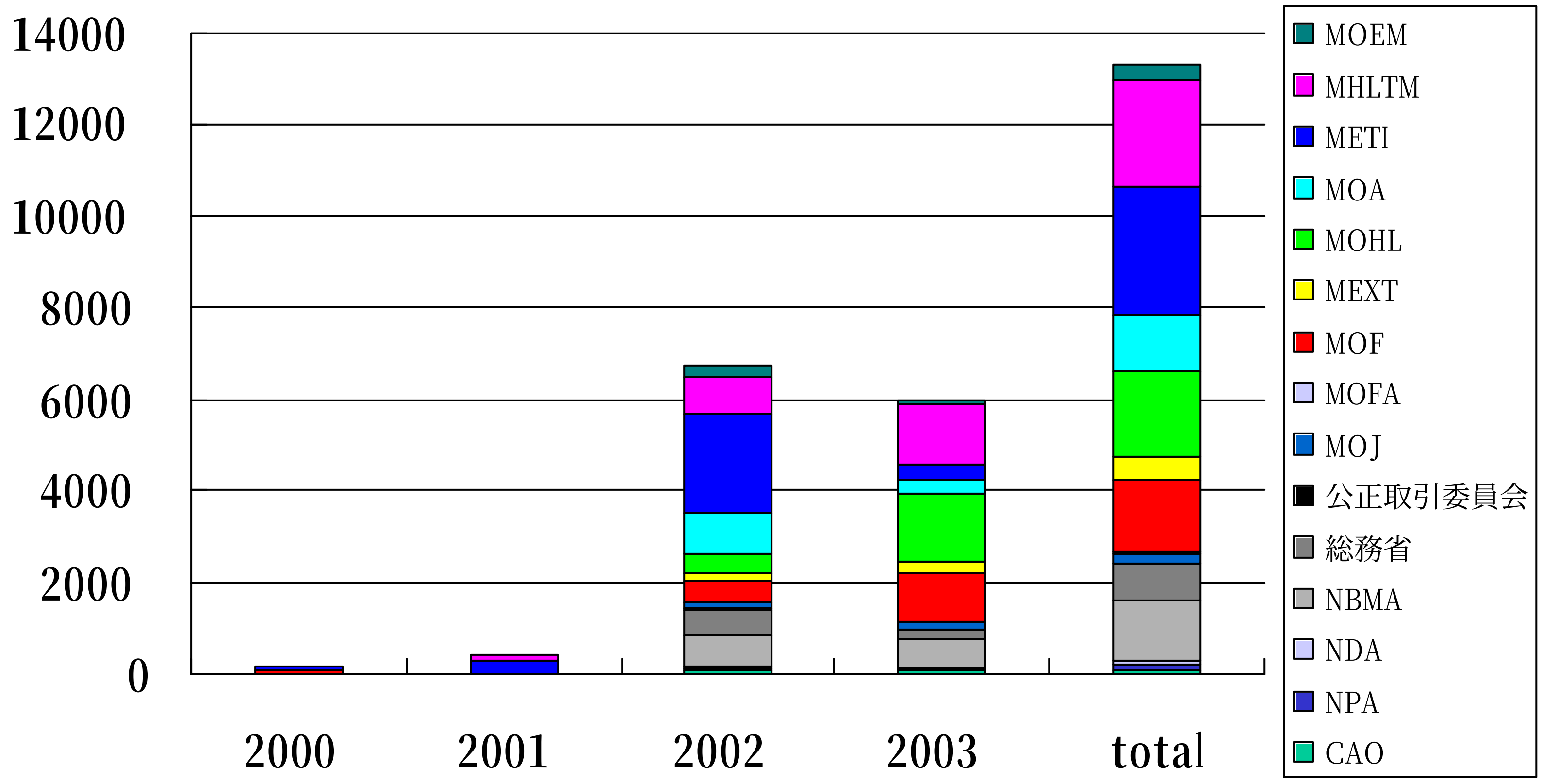
Actual Development

1. Full coverage on government services
2. Start working with local government

Full Deployment

1. Full interaction with privates
2. Review & eval.

E-government progress in JP gov.

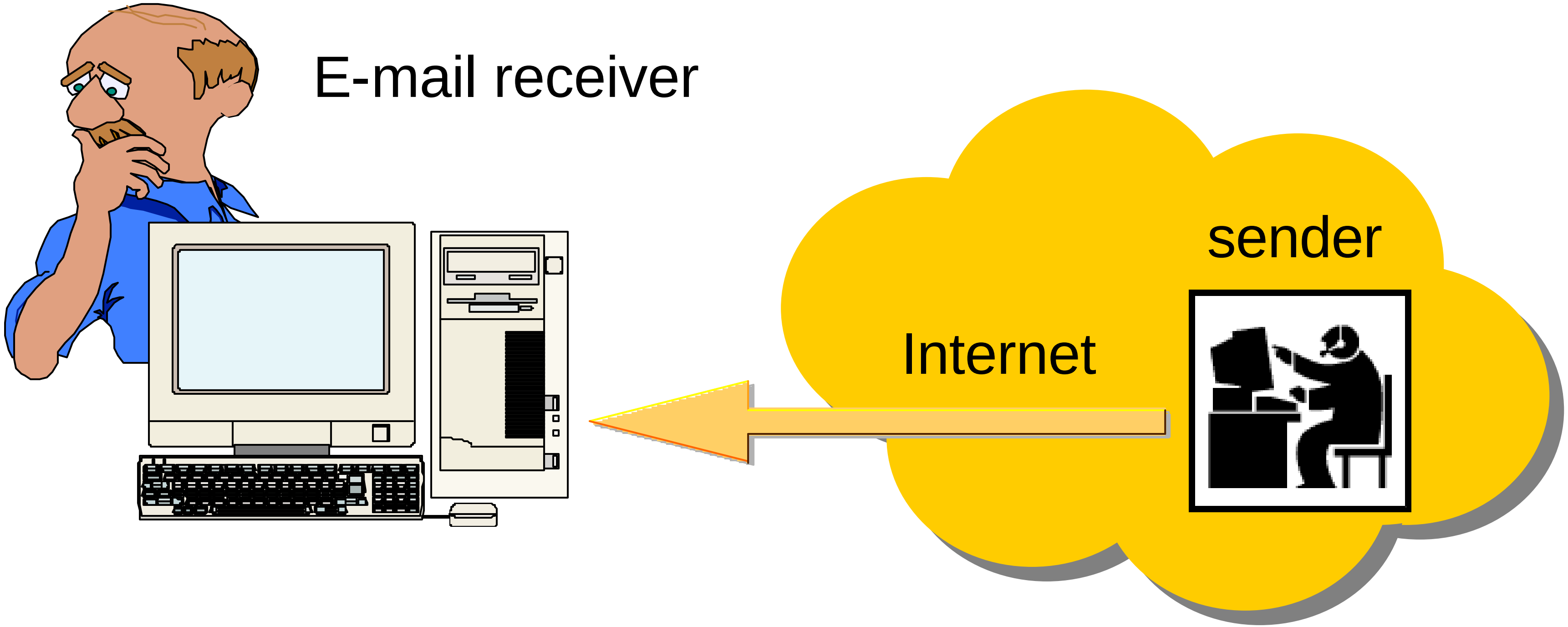


Components

- Infrastructure
  - Network for ministries and agencies in government
  - Cryptography & PKI
- Software / Middleware
  - Accelerating development of services
  - Common platform and common middleware
    - WWW and meta platform for “service description”
- Revision on regulations / laws / orders…
  - Digital signature and privacy management
  - Simplify procedures to fit them to online services
  - Payment for handling charges
  - ….

Identity is required in many situation

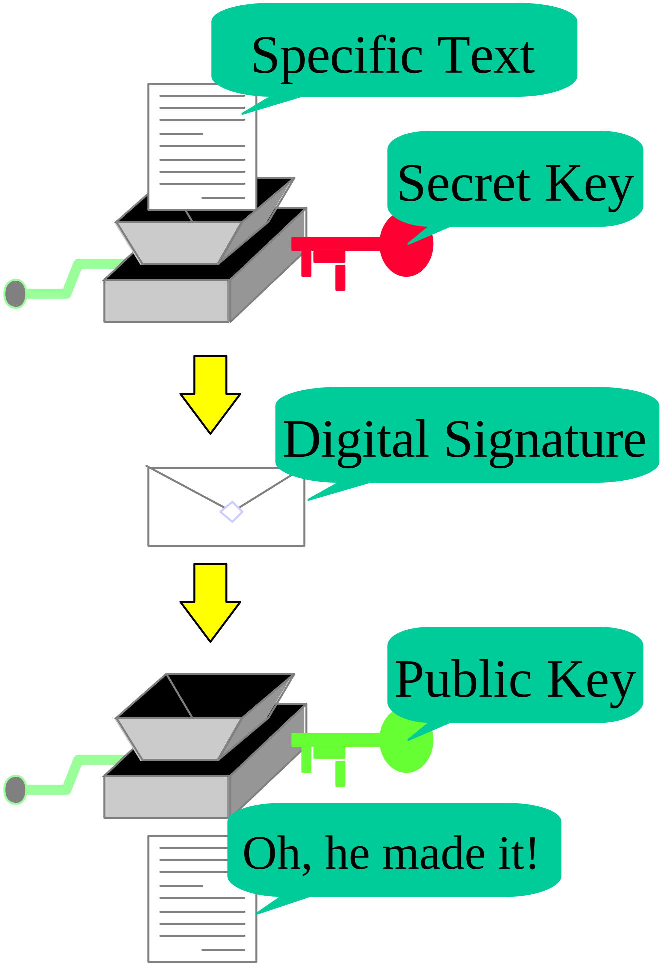
How can we know who really sent the e-mail?



What is PKI?

- Public-Key Infrastructure
  - Digital signature using asymmetric key (public key) cryptography mechanism
    - Originally developed by DH in 1974
  - Scalable / trustful public key management infrastructure is a key idea of PKI
    - Using “trusted third party” model to ensure the correctness of the certificates.
    - Not limited to the Internet services
  - Many Applications exist
    - Secure Web Access via SSL/TLS (https)
    - Encrypted/Signed E-mail (S/MIME)
    - Applet Verification (Java, Active-X, etc.)

Mechanism of Digital Signature



- Using public key cryptography
  - Public key is widely available
  - Secret key is kept secretly only at the holder
- Sending specific text which is also known by receiver
- If the encrypted text can be decrypted properly, then the sender is the person who has the public key!
- Digital Signature

What can PKI provide?

- Authentication
- Integrity
- Confidentiality

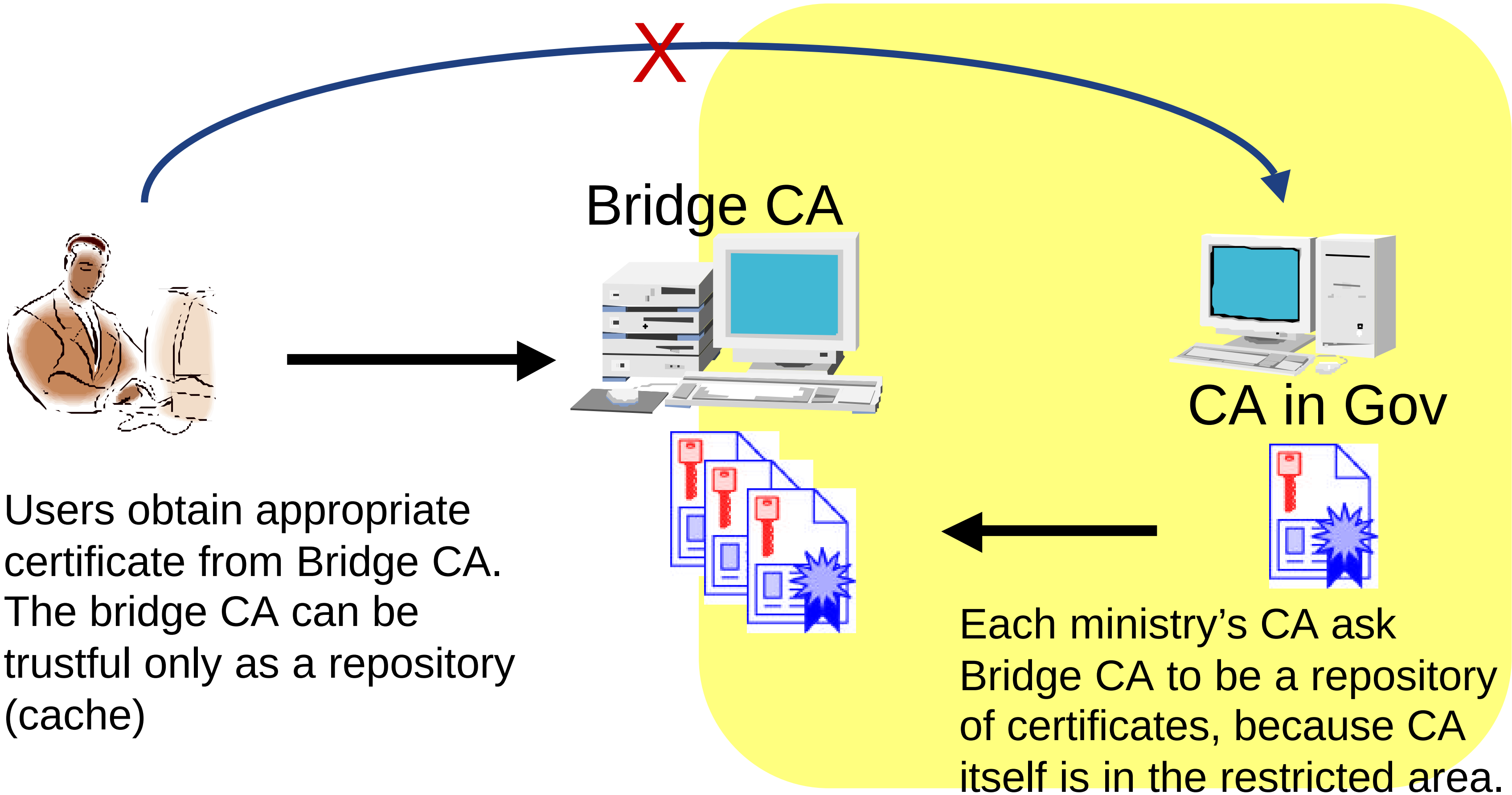
GPKI (1)

- Authentication and digital signature infrastructure which can work with e-government services
  - Government-PKI
  - Authentication platform inside the government to show identity of position (not person!)
    - Permissions are issued under the name of “minister” not “the person itself”
  - Workable with other PKI existing in private sectors
    - We are now using PKI applications and services
    - Bridging CA model
      - Single window to bridge government and private sectors

GPKI (2)

- Each ministry now operates its own CA
  - Certification Authority
  - Multiple CA are existing and they are completely isolated from others
- In private sector, multiple root CA are in operation
  - “forest”, not “tree”
- Mutual/Cross authentication is the matter
  - Several candidate
  - GPKI (jp) and FPKI (us) are now using Bridge-CA model to reduce complicated management factor (single window is a quite simple enough)

Bridge CA: single window to access CA’s



Users obtain appropriate certificate from Bridge CA. The bridge CA can be trustful only as a repository (cache)

Each ministry’s CA ask Bridge CA to be a repository of certificates, because CA itself is in the restricted area.

PKI in public

- Issue X.509 certificates for individuals and legitimate entities (firms, companies, …)
  - Digital signature using these certificates are effective and have to be handled as a real “signature”
  - Government set a new regulation in 2000
    - Digital signature regulation
    - Issuers’ requirement
    - Issuer registration procedures
  - Government does have a control of certificates for non-individual legitimate entities.
    - Because company registration have to be handled simultaneously.

What we have to do

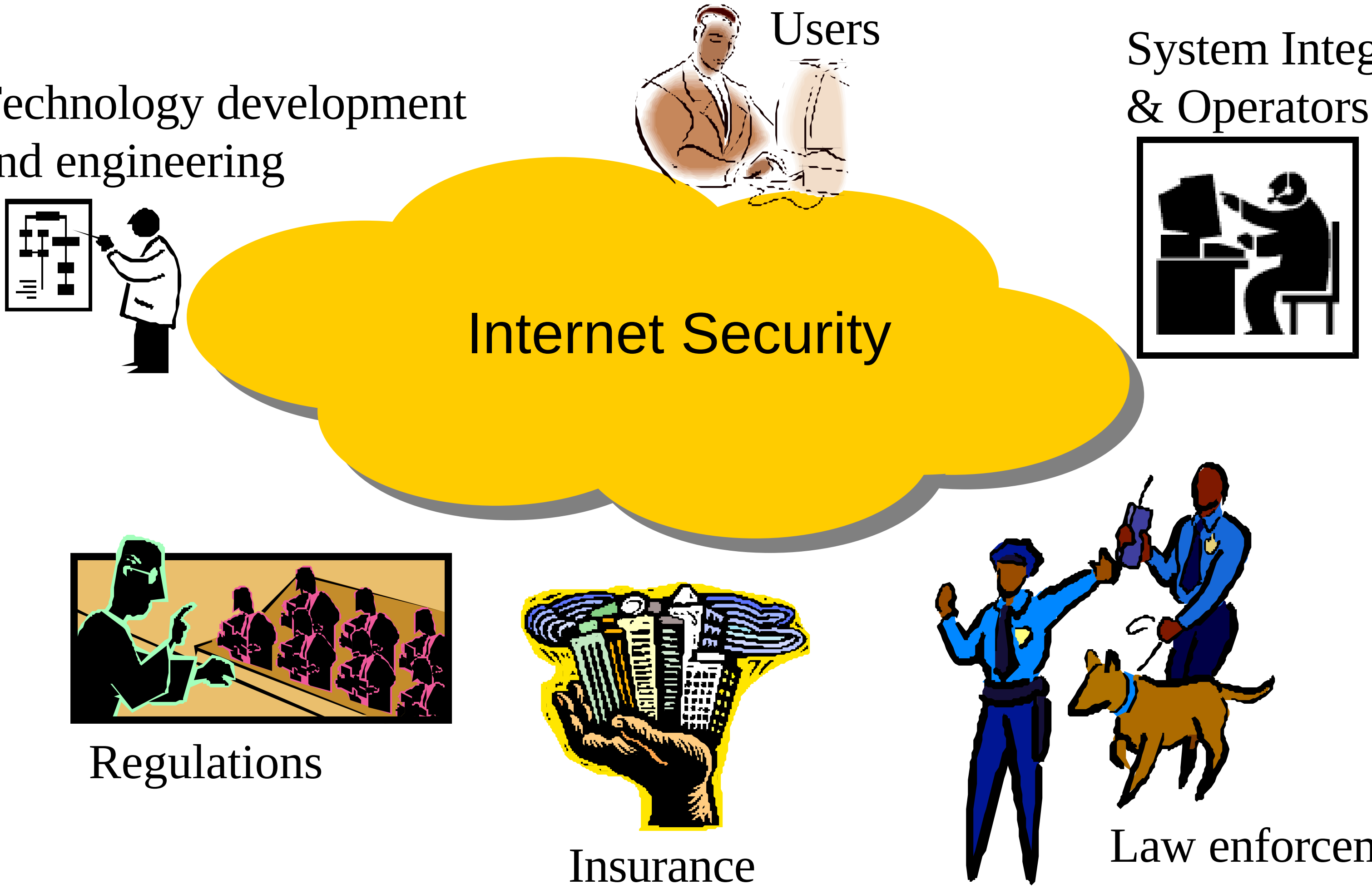
- System development
  - Actual system development in the government
  - Mainly resides on the Internet for providing its services to the public, but it surely work together with the current existing systems in private sectors.
- Change regulations
  - Review and change if needed.
  - Consistent policy on the work
- Evaluation
  - Objectives, review, ….

Vital component for e-Gov project

- Clearly defined objectives
  - If your government does not have any consensus on what we'll make and its objectives, your e-Government project will surely be failed.
- Evaluation mechanism
  - If your government does not have any mechanism to review and evaluate the project in public, your project will surely be failed.
- Professional human resources
  - If your government does not have any professional human resource on computer systems/communication/network involved to the e-Government design process, your project will never be launched properly and also never be accepted to the public.

Protect e-government platform called Internet

Who is involved?



Internet Security

Users

Technology development and engineering

System Integrators & Operators

Regulations

Insurance

Law enforcement

What government should do?

- Protect your infrastructure for e-government project
  - Network and computation resources in your government
  - Enrich your security management
  - Rules and orders for internals.

- Develop “culture of security”
  - Make social system to fit to e-way
  - Regulations, orders, guidelines, laws, policy, …..
  - Awareness and outreach
  - Equal access
  - Fund for technology development

Government actions

- Set policy on cryptography
- Funding for security technology research and development
- Deliver sustainable awareness program for public
- Introduce international standard: ISO15408 and 17799
- Human resource development for security management
- Force all the ministries and agencies to set their own security policy and security management procedures
- Set some regulations and laws for digital signature, stop illegal access, privacy, using government owned databases, …..
- Develop CSIRT team inside government and help CSIRT in public sector
- Set “Infrastructure protection program”
- …..

What is security management? (1)

- Documentation & Logging
  - Security Policy:
    - Develop a document on what should be protected and how we protect. This document should be simple enough to allow everyone understand.
  - Guidelines & Procedures:
    - Develop documents or manuals as emergency procedures, daily management, etc.
  - Review and evaluate these documents if we have any kind of incident
    - Revise if needed.

Security Policy and its Procedures

- Top level statement on the security management
  - “security policy”
  - Make things clear in terms of security management
    - What is your information assets?
    - What is your mission?
    - Who has the right to stop the services?
    - Who has the right to evaluate the systems?
    - Who has an active role of management of e-government components?
    - ….
  - According to the security policy, we have to develop several procedures as its breakdown
  - BPR (Business Process Restructuring)

What is security management? (2)

- Maintain measures to check if the procedure is executed as it was defined.
  - Audit
  - If any kind of problem was found, then you have to make improvement on management, procedures themselves, then resolve the problem.
    - Do not leave them without any resolution
    - Give appropriate power for entity who deliver the “audit”

What is security management? (3)

- Set rules for everyone in the group
  - Cover everyone, every entity. No exception!
    - Everybody are in the same boat…..
  - Integrity on rules is important
    - Awareness and comprehensive understandings
  - Guidelines and rules on various area
    - Procurement process
    - Software requirement
      - Source code, ISO15408, GPKI middleware, ….

What is security management? (4)

- Usability can not be sacrificed.
  - Digital platform is now a dependable infrastructure, therefore, its performance is the matter.
  - Security management may put more burden on users.
    - But, not acceptable if the burden causes drawbacks on performance
    - But, security management is required
  - Use “Money”
    - Investment
    - Introduce technology and engineering to achieve well designed security management platform, even they are not making usability sacrificed.
    - CISO (Chief information and Security Officer) is in charge of the design.
      - CISO should know the actual work environment
      - CISO should have well trained communication capability to make negotiations and arrangement with actual workers.
      - CISO should know technology also!
  - Each ministry has its own CISO
    - But, ultra high level office can work for this role?

What is security management? (5)

- Make involvement from many areas
  - Not limited to technology/engineering area
  - Financial management
  - HRM (Human Resource Management) and other RM
  - Regulations and Laws
  - Public Relations and Publicity activities
  - ….

What is security management? (6)

- Security management is done by professional works
  - Leading edge technologies
    - Fight against bad guys who have technologies
  - Update, renew, improvement, replace to more advanced tech.
  - Professional is highly required.

Alliance among CSIRTs in AP

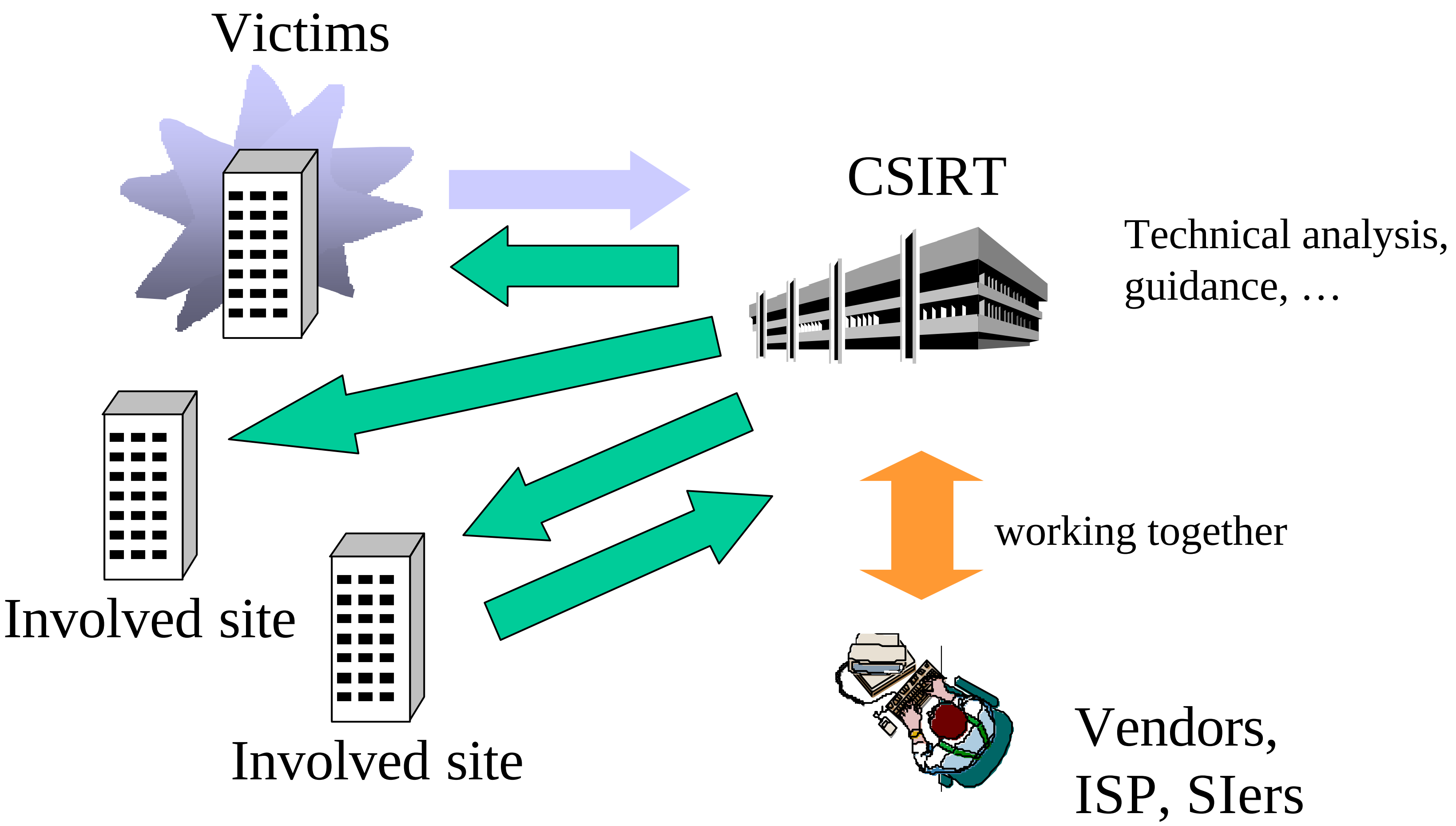
CSIRT

- Computer Security Incident Response Team
  - The concept was originally developed by U.S. during the incident called “Internet Worm” in 1988.
    - CERT/CC
  - There are several types of CSIRT existing.
    - Under government
    - NPO
    - Commercial services and Customer support
    - ….

CSIRT: its functions

- Provide response to incidents happen in its constituency
  - Mechanism to obtain reports from customers in its constituency
  - Preparation for its response
    - Technical support
    - Communication Switchboard
    - ……
  - Procedures

CSIRT: Coordination



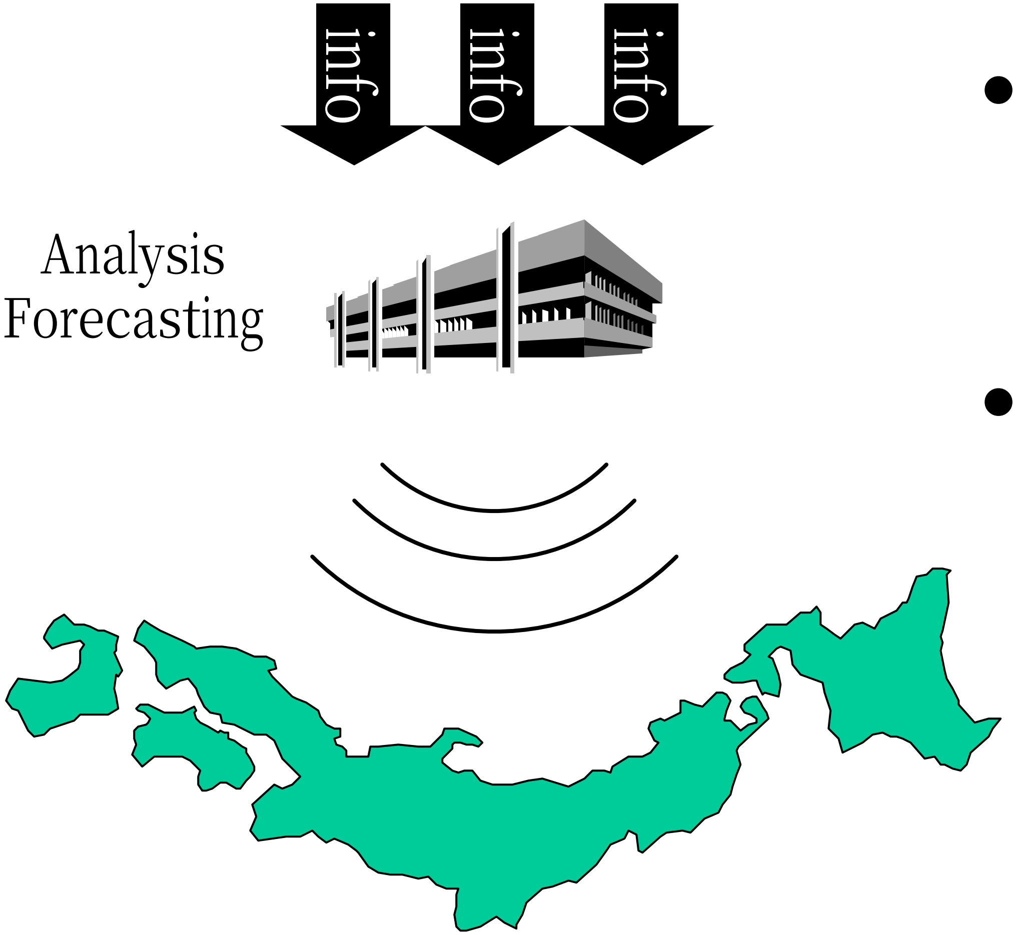
CSIRT: its functions

- Information clearing house
  - Develop measures to fix security holes, against computer viruses and worms.
    - Working with hardware/software vendors directly
  - CSIRT provides secure manner for distributing the information to the public
    - Ex. Vendor notes

CSIRT: its functions

- Observations
  - Observe security incidents and develop forecast.
    - Ex. Virus calendar
  - Warnings and Alerts
    - Public awareness on the risk we are facing

CSIRT: warnings & alerts



- Technical source for fixing security holes
  - Vendor notes
  - CERT/CC advisory
  - ….
- Warnings & Alerts
  - Quick fix on systems in its constituency

Alliance among CSIRT (1)

- There are many direct communication between CSIRT
  - Contact victims and involved sites via CSIRT
  - Sharing observations
  - Sharing technical information and vendor notes

Alliance among CSIRT (2)

- FIRST: Forum of Incident Response and Security Teams
  - CSIRT's global forum
  - http://www.first.org/
  - Membership
    - Basic infrastructure for communication among CSIRT; we can trust on communication with FIRST members.

Alliance among CSIRT (3)

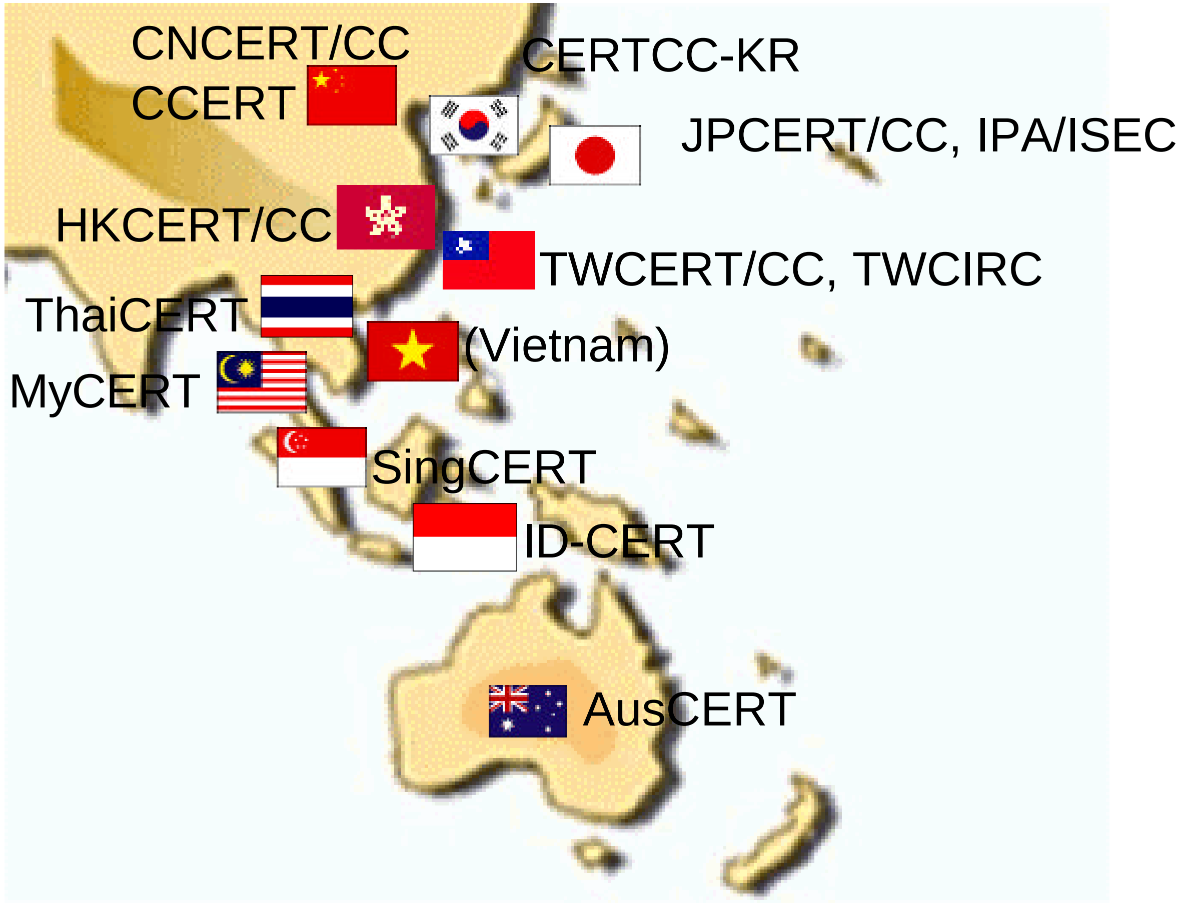
- Development of regional forum
  - Internet is a dependable infrastructure for regional economic activities.
  - More demand to work together with other CSIRT in region.
    - CERT-CC/KR and JPCERT/CC
    - AusCERT and SingCERT….

APCERT

- Asia Pacific Computer Emergency Response Teams
  - Regional forum of CSIRT in AP
  - 1st AGM was held on Feb. 25th 2003 in APSIRC2003
    - AusCERT (steering committee chair)
    - SC: AusCERT, JPCERT/CC, HKCERT, SingCERT, MyCERT, CERTCC-KR, CNCERT/CC
    - Secretariat: JPCERT/CC and CERTCC-KR

    - APSIRC (AP Security Incident Response Conference) is our annual conference.

APCERT funding members



APCERT: its activities

- Encourage and help establishment CSIRTs in this region
  - Still many economies do not have its CSIRT function
- Develop infrastructure to share technical and incident information among full members
- Provide “awareness” program for all the members
- Develop stable contact point in each economy
- Lobbying

Note

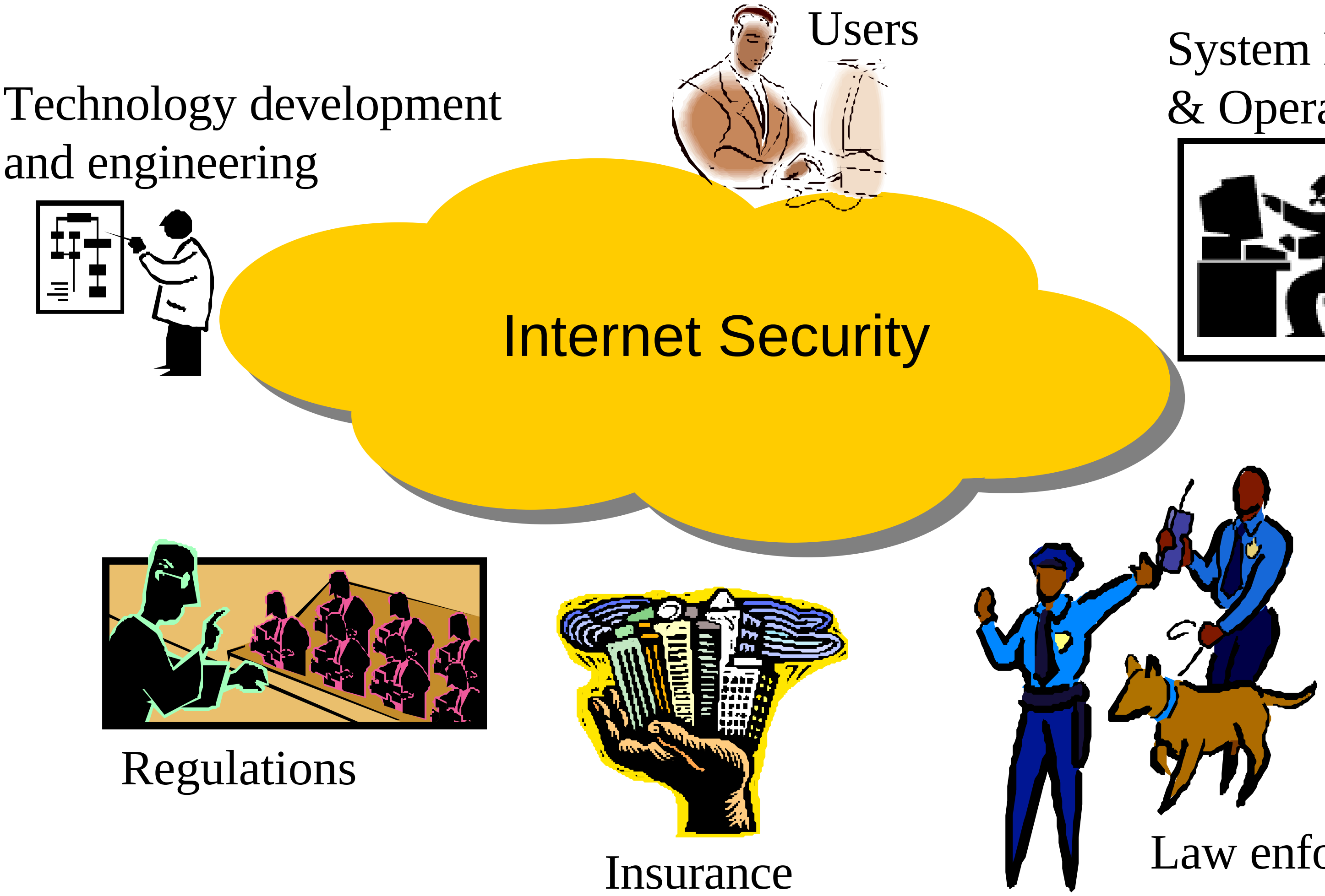
- Each full member does not represent its economy
  - multiple CSIRT in a single economy mutually complement
    - Ex. Japan
      - JPCERT/CC – generic last resort
      - NIRT – for government
      - IPA – nation wide, but mainly concentrated on viruses so far
      - IIJ-ST – ISP’s customer support
      - ….

Note

- We have to help “evolving process” of CSIRT
  - Initially, single CSIRT is formed.
  - Move to “federation” of CSIRT
    - ISP does have a important role to reduce security incident. They are in front line for internet users.
    - Government does have a responsibility to enrich its coverage in terms of security management: e-government.
    - HW/SW vendors does have liability on its product.

Demand from other community

Who is involved?



Internet Security

Users

Technology development and engineering

System Integrators & Operators

Regulations

Insurance

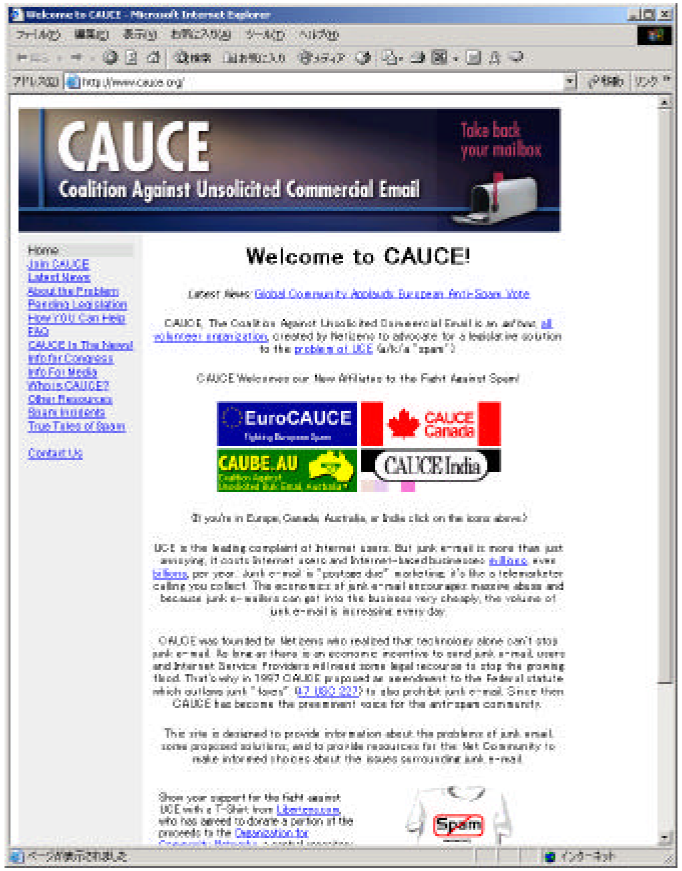
Law enforcement

Anti-SPAM

- a social DoS attack + DoS attack on infrastructure itself
  - a vehicle for transferring malicious code
  - Immoral/indecent contents considered harmful especially for young generations.
- Comprehensive approach includes engineering, new technology development, regulations, awareness are required

CAUCE & APCAUCE

- http://www.cauce.org/
- Anti-spam “awareness” program and community support.
- CAUCE a la Asia & Pacific will be formed soon.



Welcome to CAUCE!

Latest News: Global Community Applauds European Anti-Spam Vote

CAUCE, The Coalition Against Unsolicited Commercial Email is an ad hoc, all volunteer organization, created by Netizens to advocate for a legislative solution to the problem of UCE (a/k/a "spam")

CAUCE Welcomes our New Affiliates to the Fight Against Spam!

(If you're in Europe, Canada, Australia, or India click on the icons above.)

UCE is the leading complaint of Internet users. But junk e-mail is more than just annoying, it costs Internet users and Internet-based businesses millions, even billions, per year. Junk e-mail is "postage due" marketing; it's like a telemarketer calling you collect. The economics of junk e-mail encourages massive abuse and because junk e-mailers can get into the business very cheaply, the volume of junk e-mail is increasing every day.

CAUCE was founded by Netizens who realized that technology alone can't stop junk e-mail. As long as there is an economic incentive to send junk e-mail, users and Internet Service Providers will need some legal recourse to stop the growing flood. That's why in 1997 CAUCE proposed an amendment to the Federal statute which outlaws junk "faxes" (47 USC 227) to also prohibit junk e-mail. Since then CAUCE has become the preeminent voice for the anti-spam community.

This site is designed to provide information about the problems of junk email, some proposed solutions, and to provide resources for the Net Community to make informed choices about the issues surrounding junk e-mail.

Show your support for the fight against UCE with a T-Shirt from Libertees.com, who has agreed to donate a portion of the proceeds to the Organization for Community Networks, a central operating

Law Enforcement (1)

- Police and other law enforcement bodies have their own “working together” environment.
  - Based on international mutual anti-crime treaty
  - Asian Crime Investigation Research Institute
  - Ex. G8 group’s “Lyon group”, Interpole, …

Law Enforcement (2)

- Getting more working on various areas
  - Human resource development
    - Fundamental technologies, engineering and network operations
    - Crime-scene Investigation is surely their business, but cyber crime forensics is still in its evolving process, therefore, some CSIRT are working together with law enforcement entity.

Regional WG in inter-governmental coordination framework

- ASEAN’s e-security WG
- APEC/TEL e-security WG
- E-government initiatives in each economy
- ….

Other aspects

- Homeland security against cyber terrorism
- National infrastructure protection
- Standardization on secure operation of information and communication systems.
  - ISO17799 and others
  - Certification

Work Together

- Harmonization
- Concept of “Culture of Security” by OECD
- Players are different in each segment.
  - Gov, CSIRT, Law Enforcement, ….
- Encourage them to have conversations and corporation
  - Mutual trust, sharing information, ….