Paradigm of Information Security as Interdisciplinary Comprehensive Science

Dr. Shigeo TSUJII
President
Institute of Information Security

Table of Contents

1. Introduction: Freedom, Equality & Security as Keywords

Freedom, equality & security – these 3 words seem to summarize the **ideal of the IT society.**

According to **Hegel, a German philosopher, "History is the process of broadening freedom."** It is certain that the law of history as defined by Hegel applies to the present day in spite of the historical and geographical distances lying between the great philosopher and us, as the stage where we human beings can freely act has been expanded from, what we call

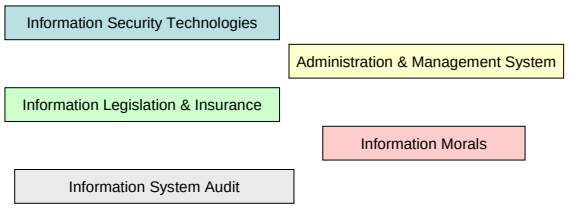
Real Space ⇨ Real × Cyber Space

Society should be designed to help people to enjoy the increased freedom brought by IT on an equal basis. This seems to be the universal ideal of the new age.

We can establish the ideal society only by finding solutions for such difficult problems as how we can improve usability and efficiency and, at the same time, enhance security, and how we can ensure national, social and public security on one hand, and protect privacy and restrict surveillance, or monitoring, over people on the other.

The solutions are often incompatible with one another.

The solutions need comprehensive measures with coordination among social system:



Information security is a hyper interdisciplinary comprehensive science.

My definition of Information security :

"The dynamic process for establishing an integrated social infrastructure; without infringing freedom broadened by IT and with closer linkage and coordination among technologies, administration and management techniques, legal and social systems and information morals;
in order to attain simultaneously efficiency, enhanced security, protected privacy and minimized surveillance over people."

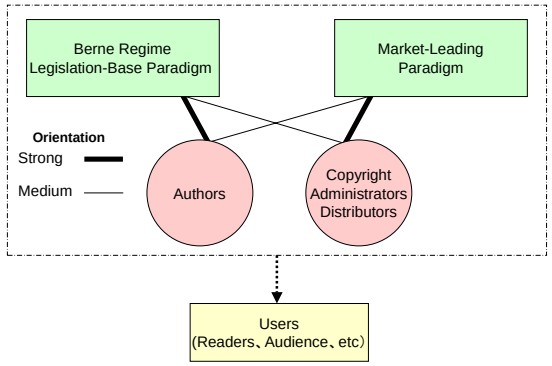
Purpose of the presentation is to consider

How the paradigm of information security as an interdisciplinary comprehensive science should be established.

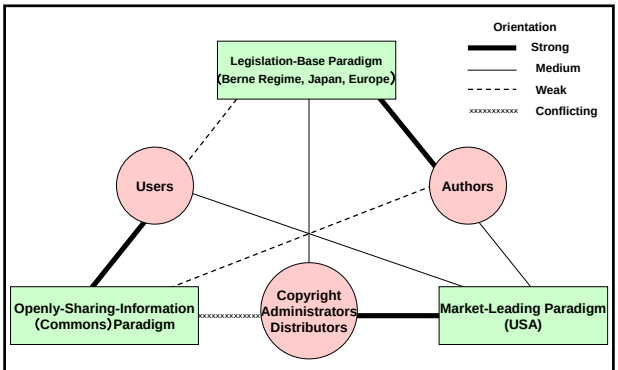
2. Contradictory Identity of Digital and Analog: Developing Fusion and Continuum of Social Structures

Digital technology breaks down barriers between industries, organizations, regions and space-time such as:

Producers vs Consumers	**Authors vs Readers**
Broadcasts vs Communications	**Public vs Private**
Inside vs Outside Companies	**Work vs Leisure**
Office vs Homes	**Business Organizations vs Individuals**
Assailants vs Victims	**Politicians vs Citizens**
Nations vs Nations	**Natural Science vs Liberal Arts & Social Studies**



Industrial Society Age



Correlation among 3 Paradigms（Berne Regime、Market-Leading、Openly-Sharing-Information）and Parties Concerned (Author, Copyright Management Distributor, User)

Computers and networks have formed **cyberspace**, a new world that human beings have stepped into for the first time. In the new world, they have acquired **greater freedom** but, at the same time, been faced with **unprecedented troubles in security, privacy protection** and the like.

Especially since the terrorist attacks on New York in September 2001, there have been fruitless discussions continued on **the choice, or the well balance between freedom/privacy of individuals and security of society**. The arguments on what is the well balance often fall into **ideological confrontations**.

To achieve simultaneously protected privacy, improved security, expanded freedom and minimized possibility of excessive surveillance society,

Solution should be in comprehensive measures of close coordination among:
Technologies, Administration & Management Methods, System Audit, Laws and Information Ethics as in the figure below.

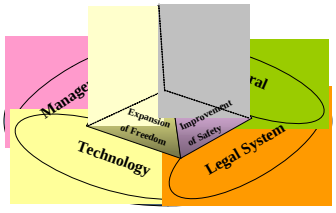


Figure 1. Concept of Information Security

3. Constructing the Ring of Information Security

Usual definition of Information Security:
The protection of information assets against various threats and attacks on their security;
preserving normal functions and conditions in terms of confidentiality, integrity, and availability;
enhancing information systems and the reliability of information so that users can use information systems in peace of mind.

3 components of information security since 1970s :

Confidentiality
Integrity
Availability

These concepts are formally defined in Table 1.

Table 1. Confidentiality, integrity, and availability

Confidentiality	Only specific people with permission to access particular information can access it.
Integrity	Information and its associated processing methods are authentic and complete.
Availability	The ability of authorized users to access information and related assets reliably whenever necessary is preserved.

Do these **3 elements** together constitute a **complete definition of information security?**

If one considers the importance of electronic certification, one has to say that this is an **insufficient definition.**

It is essential that it be possible to verify the identities of both the parties involved.

If it proves impossible to confirm a person's identity with absolute certainty, e-society will collapse completely.

It must be possible to **carry out electronic certification reliably using identification of individuals and digital signatures** to avoid malicious deception and accidental error in the invisible cyber-world.

Certification or provability is the **4th information security element** in addition to confidentiality, integrity, and availability.

The concept of provability includes the notion that a transaction leaves behind a record of the time at which it took place as proof.

The definition of **integrity** given in Table 1 is somewhat abstract.

It is also possible to frame a definition of integrity that also includes **reliable certification and verification.**

20 years ago **integrity** was understood to mean "**non-altered data**."

Now the definition is expanded to **encompass the concepts of certification and verification.**

- This kind of information security cannot be protected with **technology** alone.
- **Management** and **administration** within organizations must be carried out reliably.
- High **ethical standards** must be applied there.
- **Information ethics** are important.
- **Legal system** to deal with information crime must be put in place.

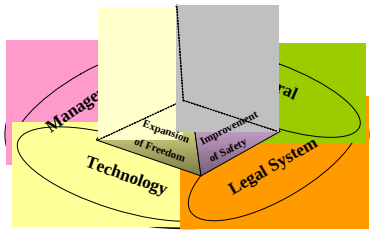


Figure 1. Concept of Information Security

Ultimately, to achieve information security, these 4 elements —**technology**, **management** and **administration**, the **legal system**, and **ethics**—must be interlocked with one another to construct a ring of strength.

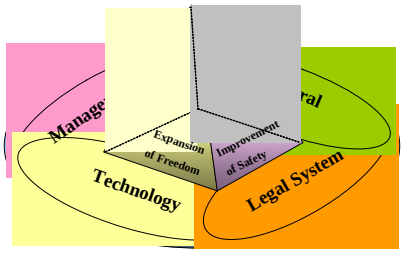


Figure 1. Concept of Information Security

(1) Technology

includes technologies for

- encryption,
- identification of an individual using bio-information,
- protection of copyright using electronic **watermarks** and the like,
- counter-measures to **combat viruses**,
- **firewall**,
- network security such as **intrusion detection systems** (**IDSs**).

The phrase "information security" contains strong overtones of **protection**.

Encryption is the core technology in information security.

Is encryption **only a technology for protection**?

In fact, encryption is a **driving force behind computerization** and an **engine of revolutionary change in society**.

Example: e-money

e-money is a currency in which technology such as digital signature technology (based on **public-key encryption**) is used to attach value to information to represent an amount of money.

The banknotes in use today derive their monetary value from the use of advanced printing technology and paper quality.

However, in the cyber-world, it is impossible to produce a currency where value is accorded based on material attributes.

E-money will come into being as follows:
using public-key encryption, only currency issuers, such as the Bank of Japan, will be able to use their secret private keys (which are kept secret) to perform a mathematical operation to attach a digital signature to information representing an amount of money.

E-money is in the vanguard of e-society and it is said that in the future it will bring about a seismic shift in the international economy.

It is only with the advent of encryption that it has become possible to implement the e-economy system (of which e-money forms a part), e-government systems (both at the national and local levels) and e-medical record systems.

In light of this, it might be argued that **to regard encryption as simply a technology of protection is to seriously belittle it**.

This type of information security, which incorporates encryption technology, is much more than a framework for "protection" and can be seen as a firm foundation for construction of society.

2 mainstays of Security technologies**:**

Cryptography & **Secure Computer Networks**

Cryptography
has formed a **magnificent and elegant** system.

Since 2000, there have been great changes of safety assessment and standardization of cryptograms in Japan, the United States and Europe.

In 1997, the National Institute of Standards and Technology (NIST), a U.S. federal agency, held a contest open to all citizens of the world with a view to attracting ideas for AES, Advanced Encryptions Standard, as a successor of DES, which had been widely used all over the world for 20 years but is almost outdated.

In 2001, Rigindael, designed by Belgian researchers, was adopted as a standard encryption of the federal government.

In Japan, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPMHAPT総務省), Ministry of Economy, Trade and Industry (METI経済産業省) and their affiliate organizations formed CRYPTREC, Cryptography Research & Evaluation Committee, who devoted strenuous efforts for 3 years and, in March 2002, completed a list of 29 methods of common and public key cryptography, hash function and pseudorandom numbers applicable to e-governments.

In the European Union, NESSIE, New European Scheme for Signature, Integration and Encryption, has chosen 12 types of excellent cryptography, including MISTY, invented by Mitsubishi Electric, Camellia by NTT and Mitsubishi, and PSEC-KEM by NTT. This fact proves that Japanese researchers have reached the highest level in the technology.

Technology of Secure Computer Networks

In Japan, there has not been brisk activity seen in studies for operating systems and other software partly because the fields were not favorable for researchers to publish the results of studies in papers and partly because the fields were dominated by Microsoft.

In such circumstances, however, there are signs of change emerging as open source software, such as Linux, becomes more common. Indeed, such movements are desirable. The trend, though, will not automatically or directly lead to improvement of security. Rather, there are concerns that a growing number of local versions might result in deterioration of security. Quick and aggressive research is required to develop "**secure OS**," "**secure programming**" and other techniques.

In addition, interdependent network systems, working in the most efficient mode, connected together and highly integrated, have potential vulnerabilities because defects of a component might produce negative effects on a wider part of the system.

Therefore, there is also a requirement for complete analysis and detection of the vulnerabilities and demand for immediate development of a systematic and dynamic database of the weaknesses.

(2) Management and Administration

How can information security be preserved in organizations such as companies and local governments?

Firstly, it is essential
- to clarify **information assets** to be protected,
- analyze to determine the **potential threats** to these assets,
- and formulate a **security policy**.

This policy will be a set of rules determined at senior management level, and based on the organization's management principles.

Secondly, it is necessary to adapt the international standards laid down by bodies such as the ISO (International Organization for Standardization), or the established national standards based on these standards, to the business or organization, and determine practical criteria and guidelines.

In the field of information security the following international standards are well-known:

ISO/IEC 15408
ISO/IEC 17799

ISO 15408 is laid down as a provision standard for when organizations **purchase IT products** such as computers or IC cards.
This standard effectively started life in the **mid-1980s** as a **computer procurement standard** established by the US Department of Defense.
Subsequently, starting around 1990, extended standards were determined for general government and civilian use in various **European countries, such as Germany and UK**.

These standards were combined into today's ISO 15408.
ISO 15408 consists of **functional requirements** and **assurance requirements**.

- Functional requirements define the required functions of an IT product.
- Assurance requirements define the degree of reliability to which the **product's purported functions** are guaranteed when the product is implemented.

Functions are divided into 11 categories as shown in Table 2. These categories are then further subdivided.

Table 2 . ISO 15408 Security function Categories

1. Security auditing
2. Communications/denial prevention
3. Use of encryption
4. Protection of user data
5. Identification and verification
6. Security management
7. Privacy
8. Security function protection
9. Availability and resource management
10. Access control
11. High levels of authenticity and reliability

Regrettably, it is often said that the history of ISO15408 began in Japan in 1997. In fact, in the early 1990s, I served as the chair on the Security Subcommittee to the Open Environment Consolidation Committee established by the Ministry of International Trade and Industry (as it was then known通産省), and carried out a detailed investigation of computer security evaluation standards in the US and Europe.

In Japan, however, awareness of information security was low (users particularly were indifferent to it).
In addition, there existed a tacit perception that these types of standard were unnecessary since the manufacture of advanced products was Japan's forte, and since manufacturers' after-sales services was also of high quality.

There was also strong sentiment that the higher product costs and increases in time-to-market resulting from compliance with these standards would be serious drawbacks.

In addition, because of insufficient understanding of Internationally recognised or global standards, there was little stimulus in Japan for debate regarding computer security evaluation standards, and discussion stagnated until about 1997 when popularization of internet started.

- ISO 15408 is a procurement standard for organizations buying IT products.

- ISO 17799 is the standard that defines management measures for the use of IT products, information systems and the like which have already been purchased.
  - This ISO standard has been adapted from Part 1 of the UK standard BS 7799 (consisting of a Part 1 and a Part 2).
  - It is divided into 10 different management fields (Table 3) .
  - In Japan the ISMS (Information Security Management System) has been established in conformity with these standards.

Table 3. ISO 17799 information security management fields

1. Security policy
2. Security organization
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and application management
7. System development and maintenance
8. Access control
9. Business continuity planning
10. Compliance

Japan has the world's largest number of organizations that have been certified in accordance with ISMS. There are, however, concerns that, even though certified, they have not effectively conducted the PDCA (Plan-Do-Check-Act) cycle. It is also said that ISMS might lay such heavy burdens that small companies cannot bear them. The way of applying ISMS to small firms should be considered.

ISMS is not designed to quantify risk or determine risk levels. For the purpose of managing risk, it is also important to define what type of risk management should be conducted and at what level it should be carried out.

(3) Legal System

In order to get society to make use of technology, it is necessary to make adjustments to the legal system.

For example: electronic signature law
"Law Concerning Electronic Signatures and Certification Services" effective in April 2001 has enabled people to use digital signatures that use public-key encryption to conduct e-business transactions and e-government activities (both national and local) in peace of mind.

Several laws relating to information security are shown in Table 4.

Table 4. Examples of laws relating to information security

Laws concerning information security	Date of Enactment/ Effective Date
Law Concerning the Protection of Personal Information	2003/5/30 2003/5/30
Law for the Protection of Computer Processed Data Held by Administrative Organs	2003/5/30
Law to Amend Sections of the Criminal Law	2002/12/5 2002/12/25
Law to Amend Sections of Commercial Law	2001/11/28 2002/4/1
Electronic Consumer Contract and Electronic Consent Notification Law	2001/6/29 2002/12/25
Law Concerning Electronic Signatures and Certification Services	2000/5/31 2001/4/1
Copyright Law (revised)	2002/8/19
Commercial Registration Law (revised)	2002/12/13
Notary Public Law (revised)	2002/7/31
Law on Enforcement of the Civil Code (revised)	2002/7/31
Law on Monitoring of Communications for Investigation of Crime revised)	2001/12/12
Basic Resident Register Law (revised)	2002/12/13
Unauthorized Computer Access Law	1999/8/13 2000/2/13

Let me say that laws might be classified into **rules designed**
- **<u>to develop social infrastructure</u>** and
- **<u>to prevent injustices</u>.**

The Law Concerning Electronic Signatures and Certification Services (aggressors)

The Unauthorized Computer Access Law (defenders)

For either type of law, what is crucial to knowledge-driven society is that the legal system, conventionally focusing on corporeal things, should be transformed to be applicable universally to corporeal things and intangible (information) assets.

The growing cyberworld is eroding a ethnic characteristic of the Japanese people, which is the emotion of unity that has been formed and preserved in village communities. Through this erosion, conventional society, based on inner morals, is unavoidably broken down and transformed into a contract society. In such a society, so-called computer forensics will become familiar to people.

As information security is fundamental to social development, its performance as an economic system and a social scheme should be examined. For instance, the insurance system should be operated at premium rates calculated through the most exact possible risk analysis and cost assessment. As insurance services are provided through commercial enterprises, they should not be completely relied on as a final safety net. The system, however, should be correctly positioned in social infrastructures designed for information security.

It is reported that, seen from the viewpoint of managers of private companies and chiefs of local governments, one of the problems of information security is an unclear relation between investment and its effects. If a quantitative method for measuring the relation is invented, it may be useful to attract investment to the security system. Even if investment is not attracted, however, the managers and chiefs should recognize information security as infrastructure for management.

(4) Ethics

Although we speak constantly of ethics, there is an element of doubt about whether ethics can exert any influence in advancing information security. However, this is mankind's first attempt at constructing the cyberworld; and in the course of this process, the rapid rise of values and morals relating to information will become a great unseen force in advancing information security.

Central and local e-governments and private companies can primarily rely on technologies developed to prevent unauthorized access to confidential information.

In order to prevent information leaks, in contrast, they have to depend mainly on the conscience and morals people have regarding information. Information leakages cannot be prevented only by reliance on ethics, of course.

The governments and companies must combine technologies, administration and management methods, legal systems and information ethics for information security.

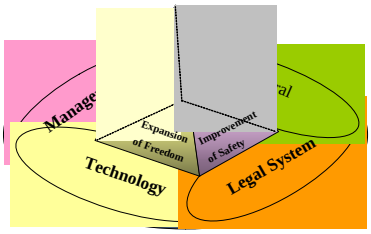


Figure 1. Concept of Information Security

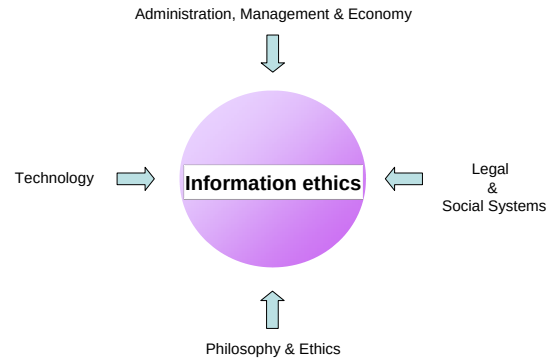


Figure 2. Interdisciplinary Features of Information Ethics

It is true that ethics has been a noble realm of philosophy since **ancient Greece**. There is also, however, the historical fact that ethics has been developing **under the influence of natural sciences and technologies**. On the gate of the Academy established by **Plato** there is believed to have been a tablet saying, “Let none ignorant of geometry enter here.”

Immanuel Kant's idea of categorical imperatives, moral laws to be obeyed without condition, seems to owe a lot to Newtonian physics. He was also a physicist and wrote about astronomy. Now that the cyberworld, a new world, is being explored, efforts should be made to construct new ethics.

Researchers, teachers and other citizens should recognize in common that the day has come when barriers should be withdrawn between social-cultural studies and natural sciences.

In addition, research conducted from the economic viewpoint seems useful for ethics. Researchers should, for instance, consider how much local governments could save from administration costs if they improved the awareness of the officers and employees.

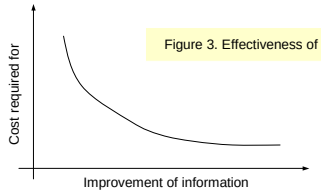


Figure 3. Effectiveness of information Ethics

Different people have different recognition of the phrase, “protection of private information” because there is a diversity of understanding on how information should be protected.
Studies should be conducted, in consideration of personal interests, on the relation between economic benefits to be produced with the use of personal information and expense burden to be imposed for preserving the information.

It is unpredictable now, however, how the sense of privacy will be changed as life-spheres of people are altered and expanded from village communities through urban societies to the ubiquitous society.

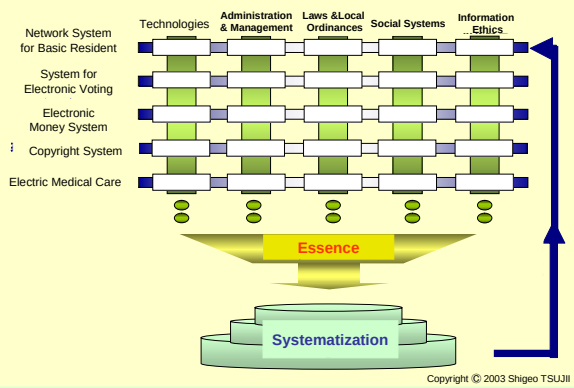
As described above, information security is a typical **interdisciplinary science**, or a **combination of the humanities, social sciences and natural sciences**. However, combining 3 disciplines is easier said than done. Mere amalgamation of 3 bears no fruit. They should be combined so that they will be **integrated and sublated (aufheben).** Substantial combinations can only be made by piling up detailed studies of actual social systems.

Examples of actual systems for information security:
- Network System for Basic Resident Register
- Electronic voting system
- Electronic money
- Electric medical care

The systems should be formed through a meticulous and firm combination of technologies, management skills, administration and control techniques, legal and social schemes, and information ethics so that societies will come as close as possible to an ideal state, where efficiency and usability, security, and protection of private information, which are almost incompatible, stand together.

Through such a dynamic process of combination, the system of information security as an interdisciplinary comprehensive science will be established (Figure 5).

Figure 4. For Construction of Comprehensive Information



Take electronic voting systems for example. The system is based on homomorphic public key encryption, which enables votes to be counted, leaving what each voter has written, for or against a policy, for example, encrypted.

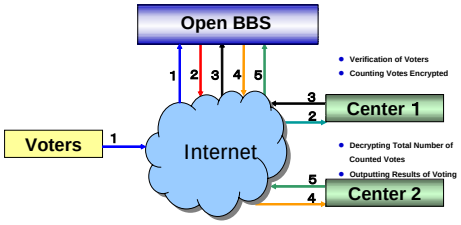


Figure 5. Electronic Voting System

As the ballots are counted only to figure out the total number of polls for and against the policy, privacy of each voter is protected, with correct counting secured. The system is also designed to examine

- whether a voter casts a duplicate vote,
- whether a voter writes 2 on a ballot when he or she is required to write 0 or 1 according to a rule,
- whether a ballot-counting center is duly working to count votes, though no third party can see what the voter writes, 0 or 1 in this case.

This is enabled by means of ZKIP, Zero Knowledge Interactive Proof, an encryption protocol which could be called mathematical magic.

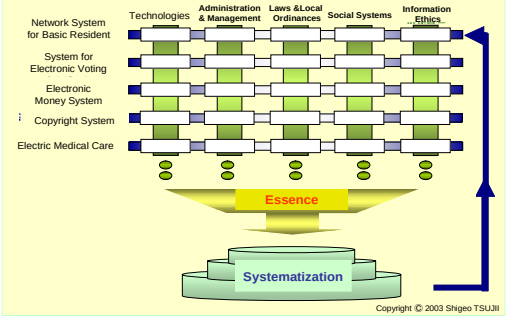
The system shown in Figure 5 is designed on condition that there is no collusion between counting and polling centers. If there is any chance of collusion, the centers can be divided to prevent such collusion. If, however, all the centers were to be engaged in collusion, almost all fraud would be ignored. In other words, no system could work properly if it were to be operated or managed only by those acting in bad faith. Such an assumption would make no sense though. When the Basic Residential Registers Network System was being planned, some opponents questioned closely whether it was absolutely secure, and some supporters insisted that it was perfectly protected.

Neither the questions nor insistences made sense, in fact. If no system should be operated without complete safety, all the transportation systems, including automobiles and airplanes, would be abolished.

Though transportation systems are used with an understanding of the risk level, electronic social systems seem unfamiliar and intangible. It is natural, therefore, that people may feel somehow anxious about the systems.

The anxieties could be reduced only by a close combination of technologies, administration and management techniques, legal systems and morals.

Figure 4. For Construction of Comprehensive Information



4. Human resource development for information security

Human resource development for information security is crucial to advanced IT countries. The author has divided human resources required for the field into 4 types.

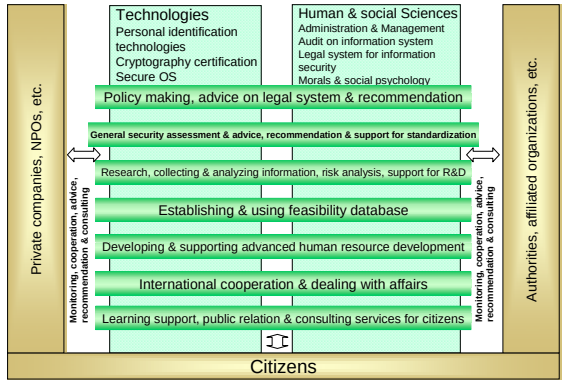
(1) Organization leaders who have enough knowledge and judgment about the whole range of information security to manage the organizations

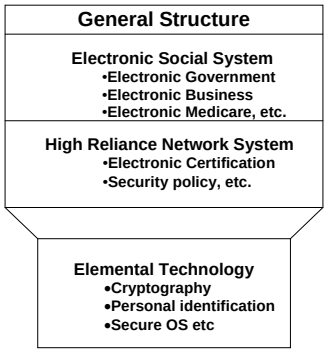
(2) System engineers who have deep knowledge of information security

(3) Experts of administration and management of ISMS and the like

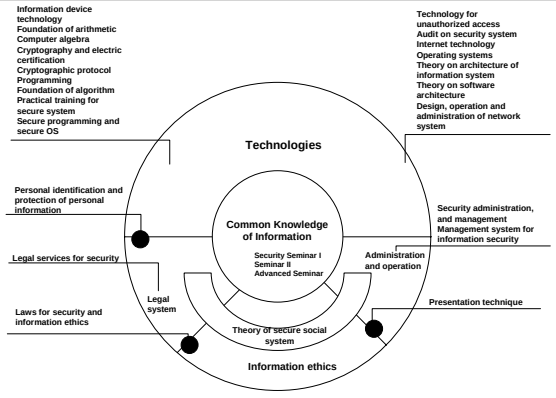
(4) Researchers of individual realms, such as cryptography, computer security technology and legal system

The number of experts, except cryptography researchers and engineers, working in Japan is much smaller than that of USA. It is reported that Japan needs more than 10,000 experts, though the number is not as large as in USA, to promote computerization at about 3,000 local governments.





Class Structure of Information Security Technology



Curriculum of Institute of Information Security

5. Conclusion

The Guidelines for the Security of Information Systems revised by OECD in August 2002 proposed that **participants in networks share a culture of security**. In my opinion this proposal is a timely remark since I define culture as "the **sum total of a given group's inherent values and behavior patterns**."