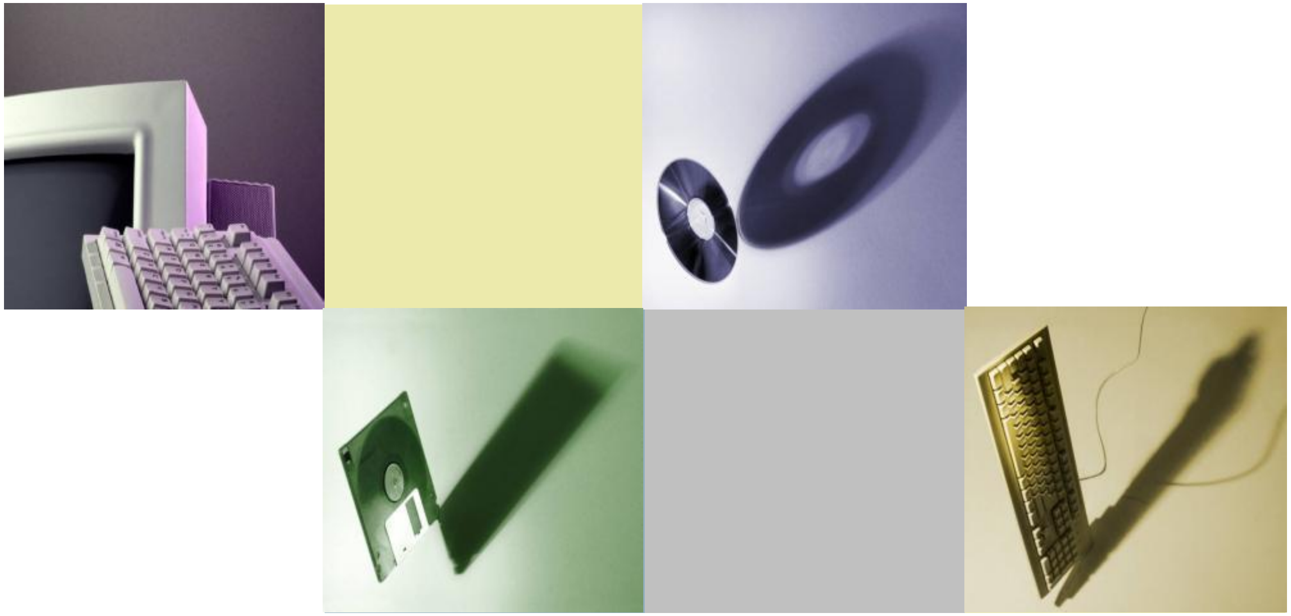
The Sample Policies for Information Security Measure for Universities

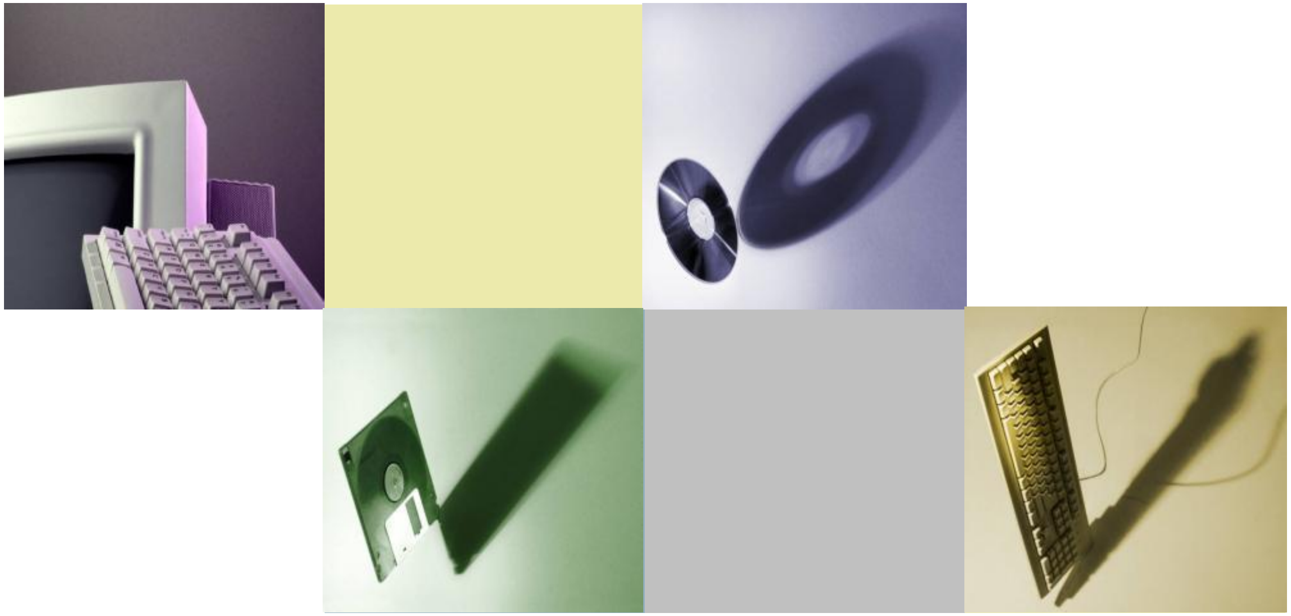


Tohoku University Hideaki Sone

Agenda

- **Activities and Information Security Measure in universities**
  - Activities of Universities, Variety of information, Security incidents, Requests
- **Sample policies for information security measures**
  - Background, WG Activities, Structure, Contents
- **Structure of the Sample Policies**
  - Character, Assumption, System of the sample policies
- **Usage of the sample policies in university**
  - Application, Example
- **Measures for information security education in universities**
  - Education material, Three Choice Tutorial

Activities and Information Security Measure in universities



Activities of Universities

【Members】

- Executive officers, personnel (office / technical / assistant), professors, temporary worker, contract worker
- Students (undergraduate, graduate, researcher) ←member?/ customer?
- TA/RA ←student? / personnel?
- Researchers (normal / visiting / contract / int’l / - - -) ←rights / responsibilities

【Activities】

- Education（for students）
- Research（together with students）
- Administration
- （Medical）

Varieties of information handled in universities

【Relationship with activities】

- Education：　Registration/score, course materials/coursework, e-learning
- Research：　paper draft, data, technology/equipment, publication
- Administration：　Personnel, finance, …, press release

【Request for information security】

- Information systems
- Confidential information（examination, paper/patent draft, management）
- Social responsibility
- Request about personal information protection, security export control, …
- Academic freedom
- Education about information security

Security incidents in universities

【Reports from others on the internet】

- Unauthorized access （scan attack, spam email）
- Virus （online/offline）
- Copyright infringement
    - Thoughtlessness, less-education

【Network failure】

- Backbone, external connection （route, abnormal traffic）

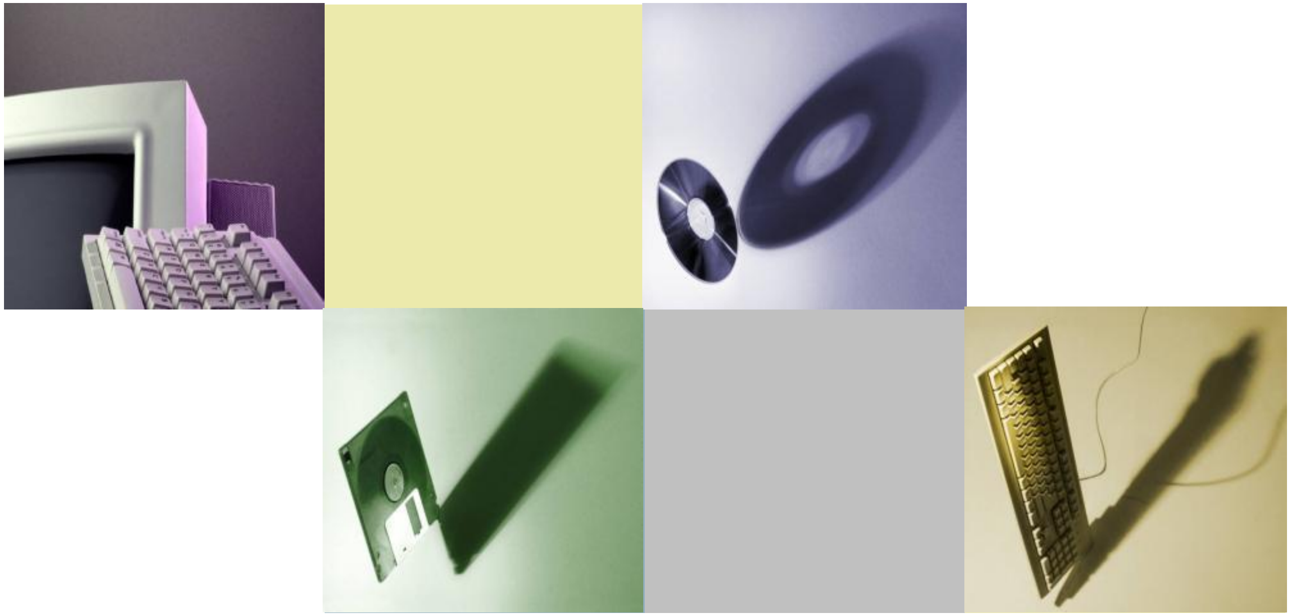
【Incidents on information control】

- Software license control
- Information leakage

Requests on efforts of universities

- **Establishment of information security policy**
- **Information security incident countermeasures**
  - Unauthorized access of/from internet
  - Countermeasure against information leakage
  - Prevention measure, user education, self-check
- **Reference to the uniform criterion for government agency**
  - Although the criterion does not cover universities, it is a useful reference for information systems to promote increase of its information security level
- **Establishment of system for information security**
  - essential requirement for national universities

Sample policies for information security measures



Background of establishment of information security policy of universities

【BG】

- Urgent need for increase of information security level

- Policy, rules and regulations, educational materials

- Wide range of expert knowledge on relationship to education and research activities, management, etc.

- The uniform criterion for government agency, Private Information Protection Law, corporated national universities, increasing security level

【Request】 **Sample policies to be used as templates**

Expert group from universities and engineers institute

Activities to establish sample policies for universities

- **2002-2003**
  - University computer centers and NII “Research meeting for security policy of university”
    - “Vision on information security policy of university”（March, 2002）
  - IEICE “Network management guideline study working group”
    - “Network management guideline for higher education institute”（April, 2003）
  - Increasing request for specific and effective sample policies
- **Establishment of sample policies by NII and IEICE（since 2006）**
  - Response to new requests
    - “The uniform criterion for government agency”（December, 2005）
    - Standard and effective policies
  - “Working Group for Information Security Policy for National Universities and Institutions “
    - Sub groups：
      - General field and structure, Network operation, Authentication operation, Clerical use, Users, Education and ethics
    - Supports：
      - National corporative computer centers, Informatization promotion association of national universities
      - MEXT, NISC (National Information Security Center)
    - Joint activity with IEICE “Network management guideline study WG”
      - Establishment of sample policies and interpretation, and publishment

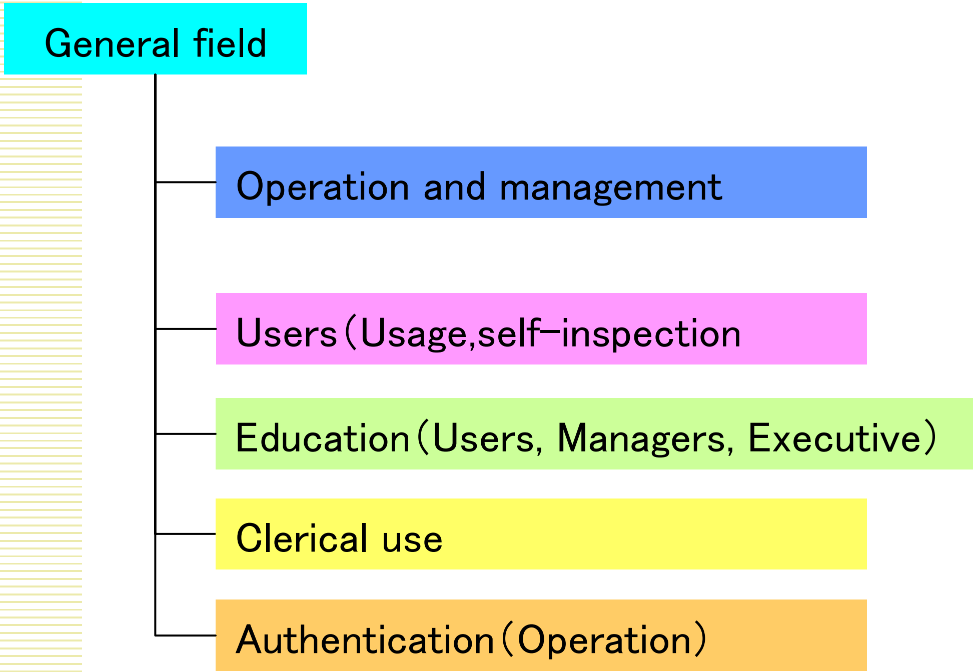
Sample policies referring the government criterion

	Uniform criterion for government agency (NISC)	Network management guideline for higher education institute (IEICE)
Target	Ministries Government officers	Universities, colleges Professors, students,
Information systems	Management by system section Internal use Web site (Official site only)	Independent operation by departments and labs System for research/experiment Web site (many local sites, Web BBS, Blogs)
	Easy to control	Balance between security control and academic freedom Education

Activity to establish the sample policies

◆Agenda and structure

- □Establishment of rules and manuals, referring comments and questions
- □Public comments request (August 2007)
- □Publication of “The Sample Policies for Information Security Measure for Institutions of Higher Education”（October 2007）
- □Lectures at seminars and workshops to spread the results



General field

Operation and management

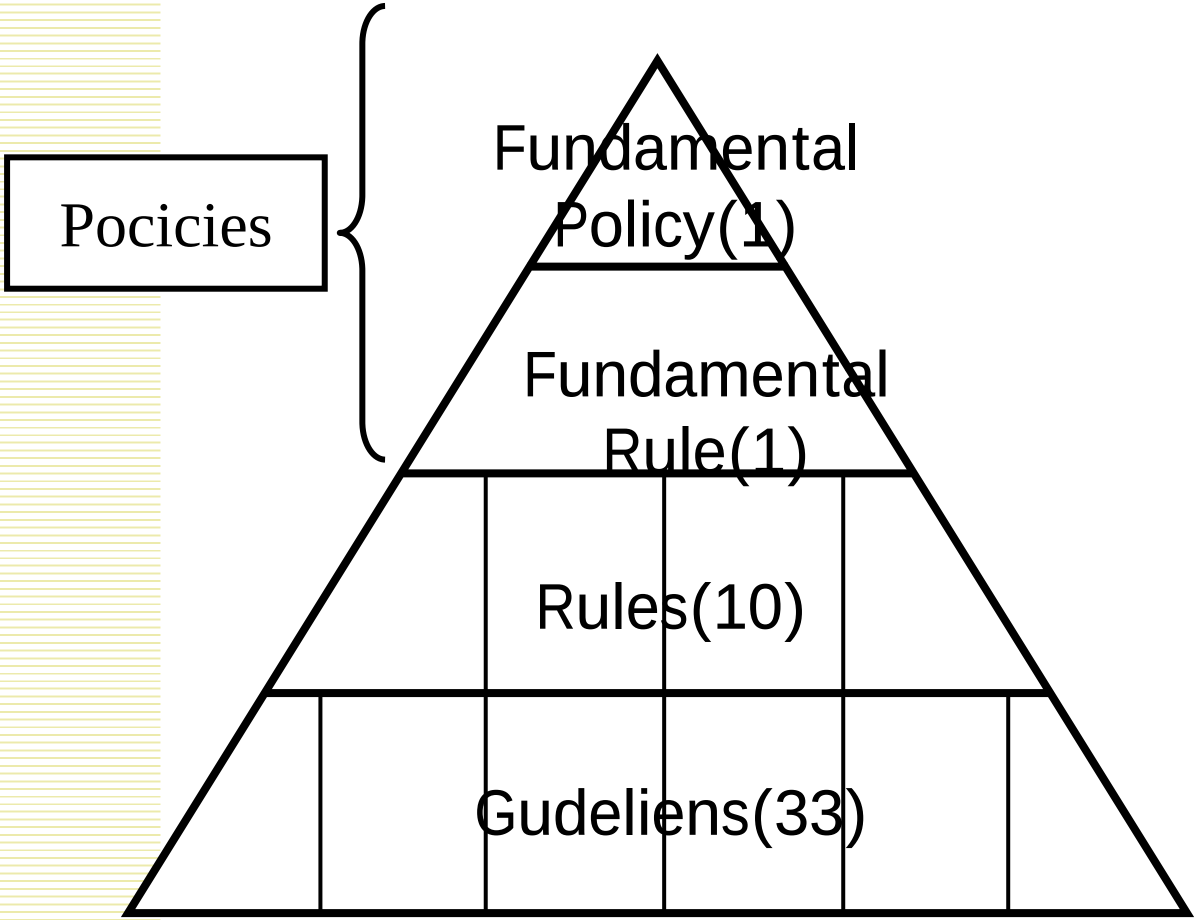
Users（Usage,self−inspection

Education（Users, Managers, Executive）

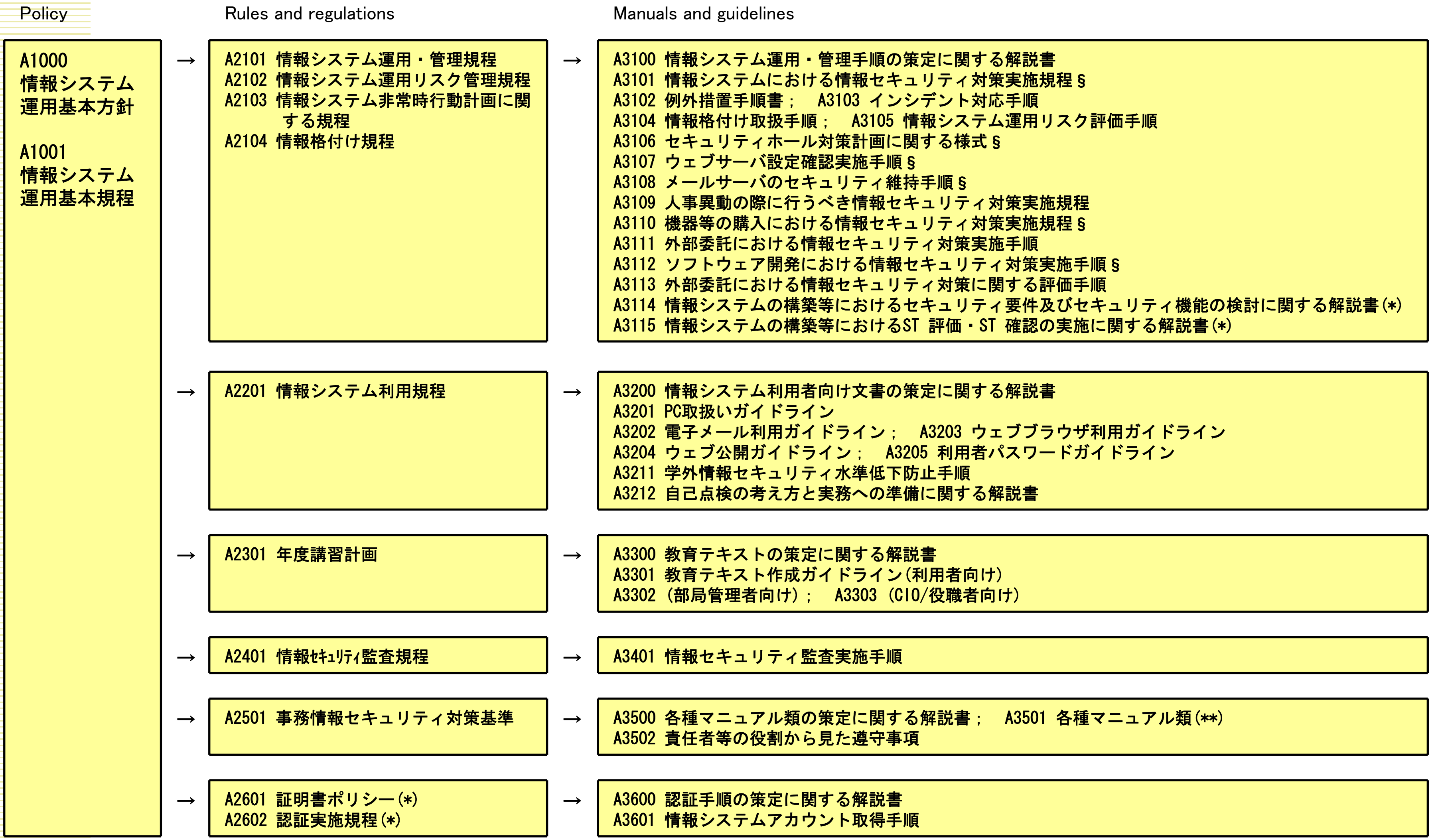
Clerical use

Authentication（Operation）

System of the sample policies



Structure of the sample policies



Policy

A1000
情報システム
運用基本方針

A1001
情報システム
運用基本規程

Rules and regulations

→ A2101 情報システム運用・管理規程
A2102 情報システム運用リスク管理規程
A2103 情報システム非常時行動計画に関する規程
A2104 情報格付け規程

→ A2201 情報システム利用規程

→ A2301 年度講習計画

→ A2401 情報ｾｷｭﾘﾃｨ監査規程

→ A2501 事務情報セキュリティ対策基準

→ A2601 証明書ポリシー(*)
A2602 認証実施規程(*)

Manuals and guidelines

→ A3100 情報システム運用・管理手順の策定に関する解説書
A3101 情報システムにおける情報セキュリティ対策実施規程§
A3102 例外措置手順書； A3103 インシデント対応手順
A3104 情報格付け取扱手順； A3105 情報システム運用リスク評価手順
A3106 セキュリティホール対策計画に関する様式§
A3107 ウェブサーバ設定確認実施手順§
A3108 メールサーバのセキュリティ維持手順§
A3109 人事異動の際に行うべき情報セキュリティ対策実施規程
A3110 機器等の購入における情報セキュリティ対策実施規程§
A3111 外部委託における情報セキュリティ対策実施手順
A3112 ソフトウェア開発における情報セキュリティ対策実施手順§
A3113 外部委託における情報セキュリティ対策に関する評価手順
A3114 情報システムの構築等におけるセキュリティ要件及びセキュリティ機能の検討に関する解説書(*)
A3115 情報システムの構築等におけるST 評価・ST 確認の実施に関する解説書(*)

→ A3200 情報システム利用者向け文書の策定に関する解説書
A3201 PC取扱いガイドライン
A3202 電子メール利用ガイドライン； A3203 ウェブブラウザ利用ガイドライン
A3204 ウェブ公開ガイドライン； A3205 利用者パスワードガイドライン
A3211 学外情報セキュリティ水準低下防止手順
A3212 自己点検の考え方と実務への準備に関する解説書

→ A3300 教育テキストの策定に関する解説書
A3301 教育テキスト作成ガイドライン(利用者向け)
A3302 (部局管理者向け)； A3303 (CIO/役職者向け)

→ A3401 情報セキュリティ監査実施手順

→ A3500 各種マニュアル類の策定に関する解説書； A3501 各種マニュアル類(**)
A3502 責任者等の役割から見た遵守事項

→ A3600 認証手順の策定に関する解説書
A3601 情報システムアカウント取得手順

§は策定手引書
(*) 外部文書の参照のみ,
(**) 各大学にて策定することを想定

Content of the sample policies

（Total 45，586p）	Policy A10xx（12p）	Rules/Regulations A2xxx（200p）	Manuals/Guidelines A3xxx（374p）
General x0xx	2，12p		
Management x1xx		4，　47p	16，186p
Usage x2xx		1，　　8p	8，　95p
Education x3xx		1，　　5p	4，　38p
Audit x4xx		1，　　4p	1，　24p
Clerical use x5xx		1，134p	2，　24p
Authentication x6xx		2，　　2p	2，　　7p

9，　76p

Publication of the sample policies

- **Publication on the Internet**
  - http://www.nii.ac.jp/csi/sp/
  - 31 October, 2007
  - Also link from http://www.ieice.org/jpn/h191031.html
- **″The Sample Policies for Information Security Measure for Institutions of Higher Education”**
  - PDF file, text file
  - FAQ and news
- **Result of request for public comments (August, 2007)**
- **Other materials**
  - Old versions
  - “Vision on information security policy of university” （March, 2002）

Working Group for Promoting Information Security Policy in Institutions of Higher Education

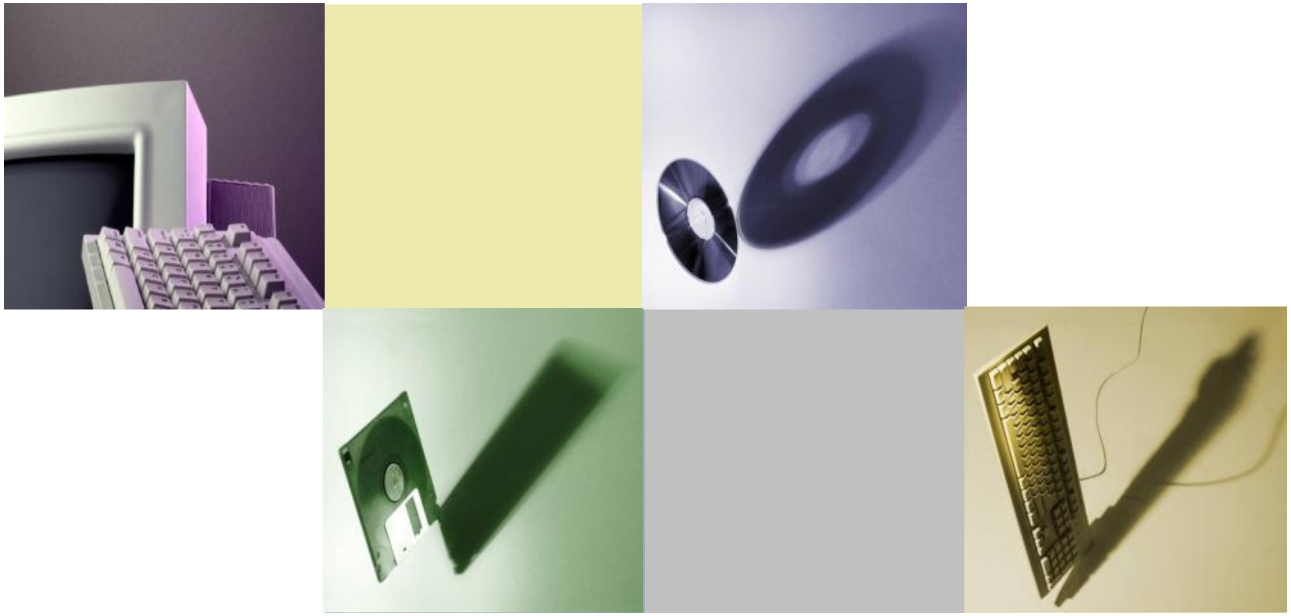
- **Promotion of information security policy to universities**
  - Development of promotional materials for use of the sample policies
    - Development of educational materials
    - Information on usage of the sample policies
    - Support for study at each university
    - Lectures

- **Response to questions/requests on the sample policies**

- **Preparation for further revision**
  - Survey on changing circumstances and new requests
    - Revision of the governmental criterion, progress of technology/services

- **Since December, 2007**

Structure of the Sample Policies



Character of the sample policies

- Established as sample policies for universities
  - Standard and effective information security policies
  - To be customized at each university/institute

- Reference to the government criterion
  - Especially, on clerical information systems

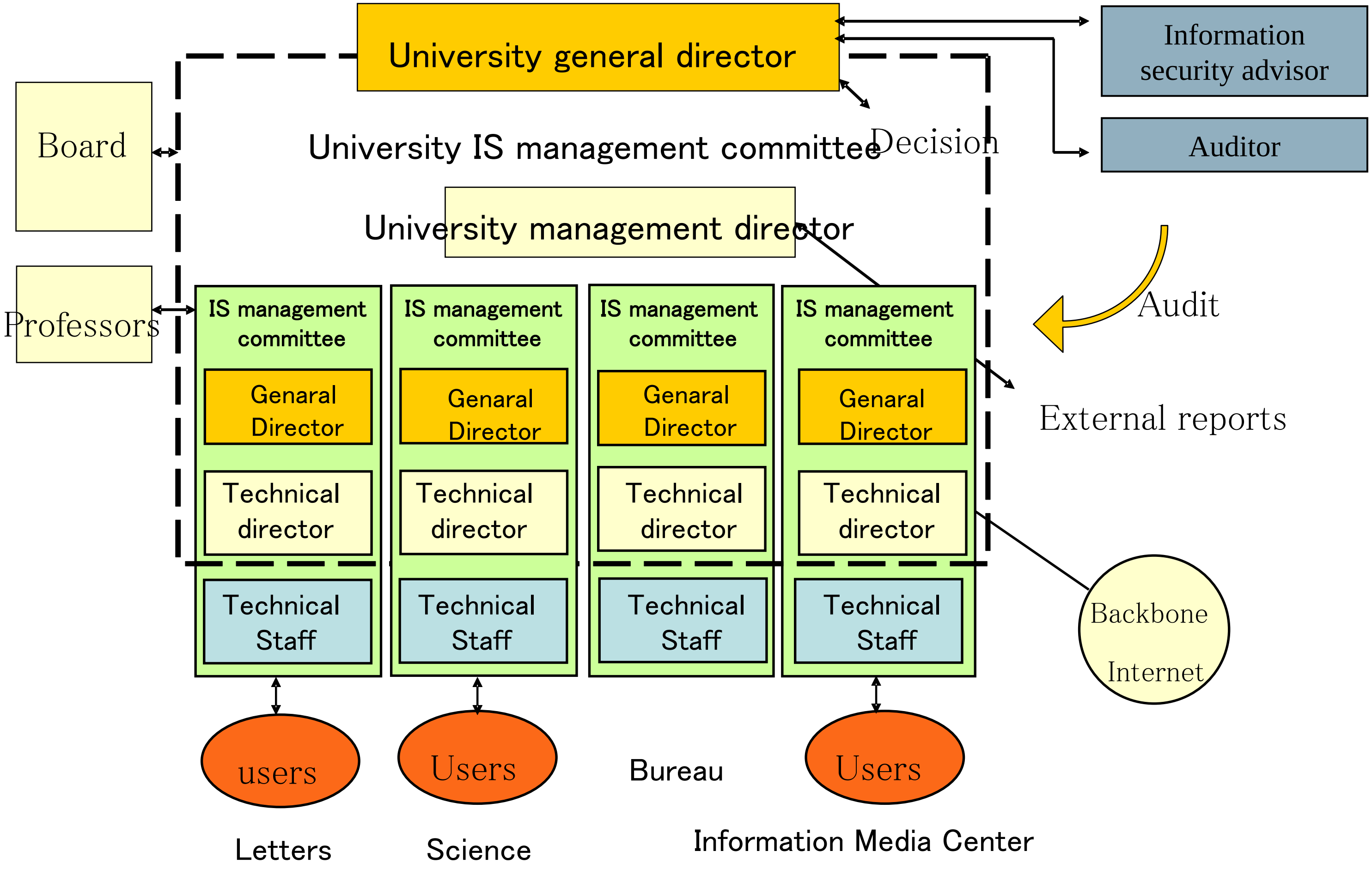
- Reference to other standards and orders
  - ISO, and other information security standres

Assumption in the sample policies

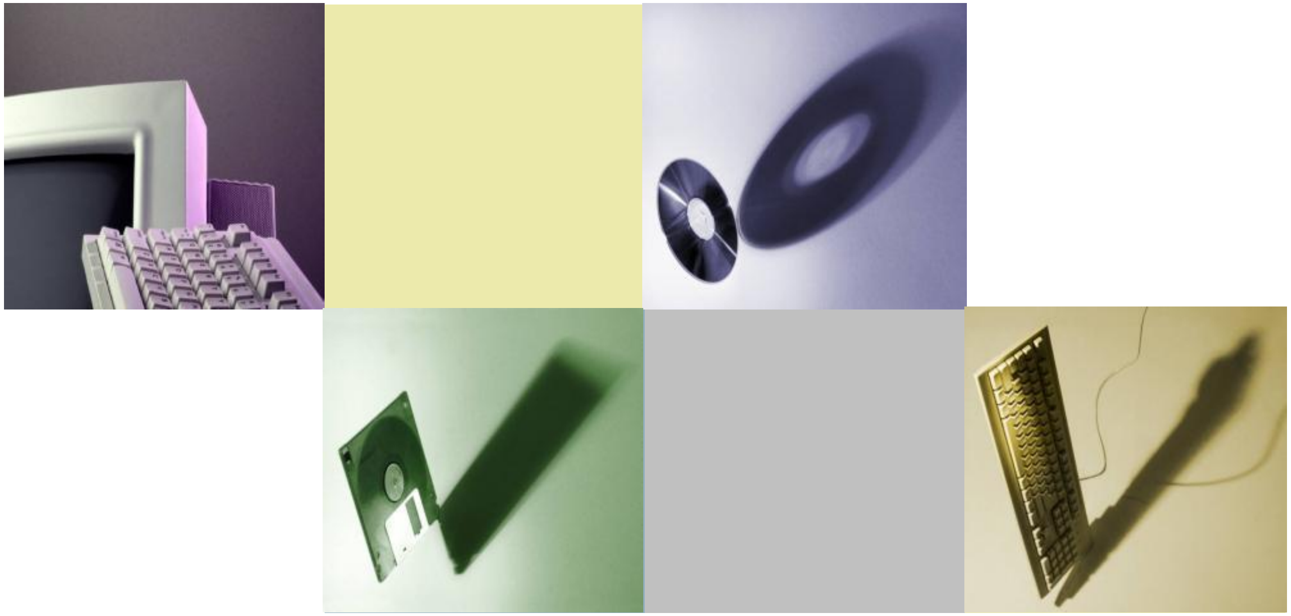
- **A hypothetical “A University”**
  - Two Faculties of Letters and Science
  - 1,000 students（250 each grade）
  - Information Media Center
    - Campus network and information systems
  - One of vice-president is posted as CIO (and CISO)

- **Effective reference for each university**
  - Reference to the government criterion to the extent possible
  - Also reference to “Network management guideline study working group” (2003) to consider conditions in universities
  - Extension to information systems to include information asset security

Information system management structure in "A University"



Usage of the sample policies in university



Application to policies of each university

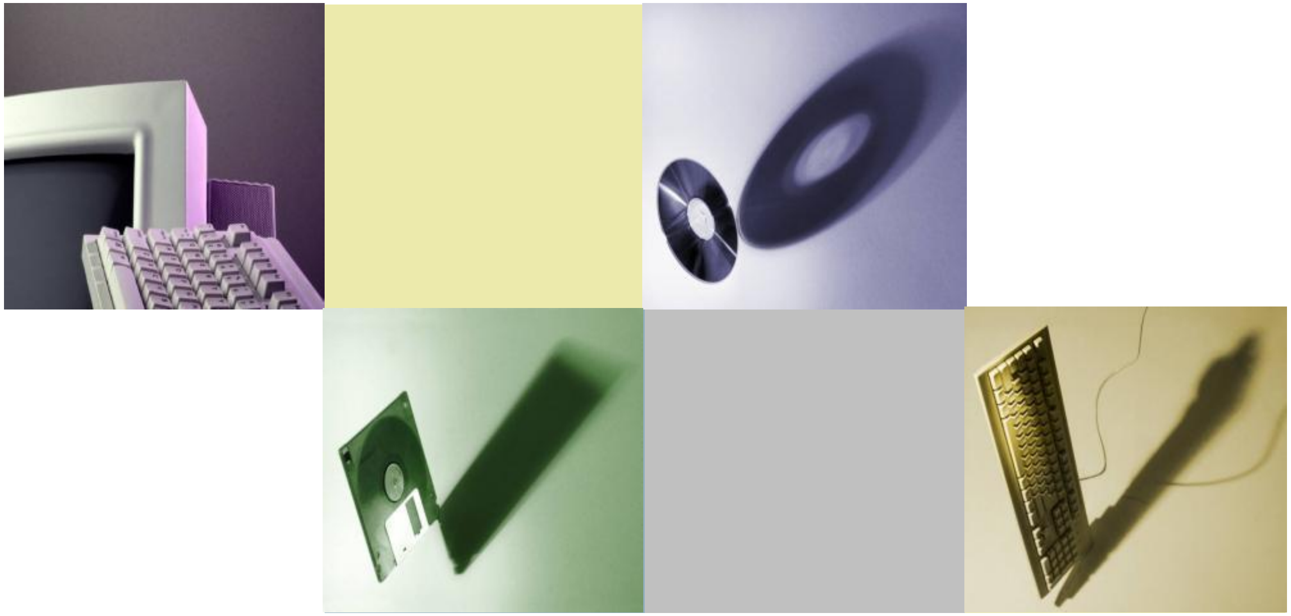
- **The sample policies were established for a virtual university**

- **Referring the sample, appropriate adjustment (alteration and change) is needed**
  - Selection of necessary rules, adjustment, and establishment by a commettee of the university
    - （Some universities made no changes… ）
  - Matching with the university’s management policy, systems, and existing rules and regulations
    - Network→Information systems→Total information security
    - Matching with document handling rules for “paper”

An example of application in a university

- **Range and policy of discussion**
  - Range → Same as the sample for clerical department; Depending on rating for research results, etc.
  - Is a measurement equipment an information system? → Rule a general criterion, and discuss at department committee for more details
  - Matching with document handling rules → Notice on matching of rating and handling; “Papers” are governed by existing rules.
- **Fundamental policy, rules and standards → Revision by referring the sample policies**
- **Rules and regulations for management → Retain consistency with existing rules**
- **User rules → Consistency with rules for existing systems**

Measures for information security education in universities



Enlightenment for students and members

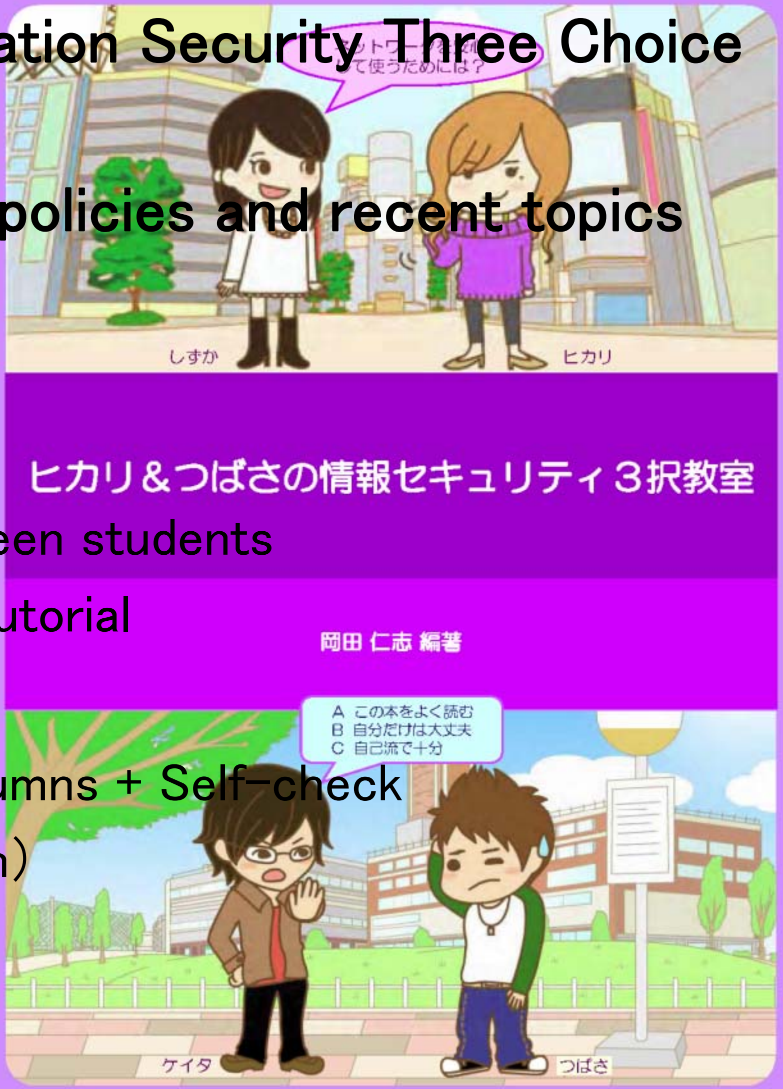
- **Education for fresh members**
  - Entrance guidance（Before class registration）
  - Class of information processing exercise（After some experience）
- **Education for staffs**
  - On recruitment
  - Periodical development, and evaluation?
- **Education materials for students and members**
  - Textbook for information processing exercise
  - Textbook for information security／ethics education

An example of education material for information security and ethics

- **Tohoku University “Computer network guideline for security and ethical conduct”　（13 pages, 1st ver. 1999）**
  - Precautions for security and ethical conduct, which must be followed by students and staffs when using the computer network.
  - １．Network community and rules
  - ２．The Basic Concept
    - The freedom of speech and academic freedom
    - Protecting the life, security and property of everyone
    - Respecting everyone ‘s privacy
    - Following the laws, rules and regulations
  - ３．Network Security
    - ID, password, unauthorized access/monitoring, protection, etc.
  - ４．Network Citizenship
  - ５．Cooperating with the net, Using more effectively

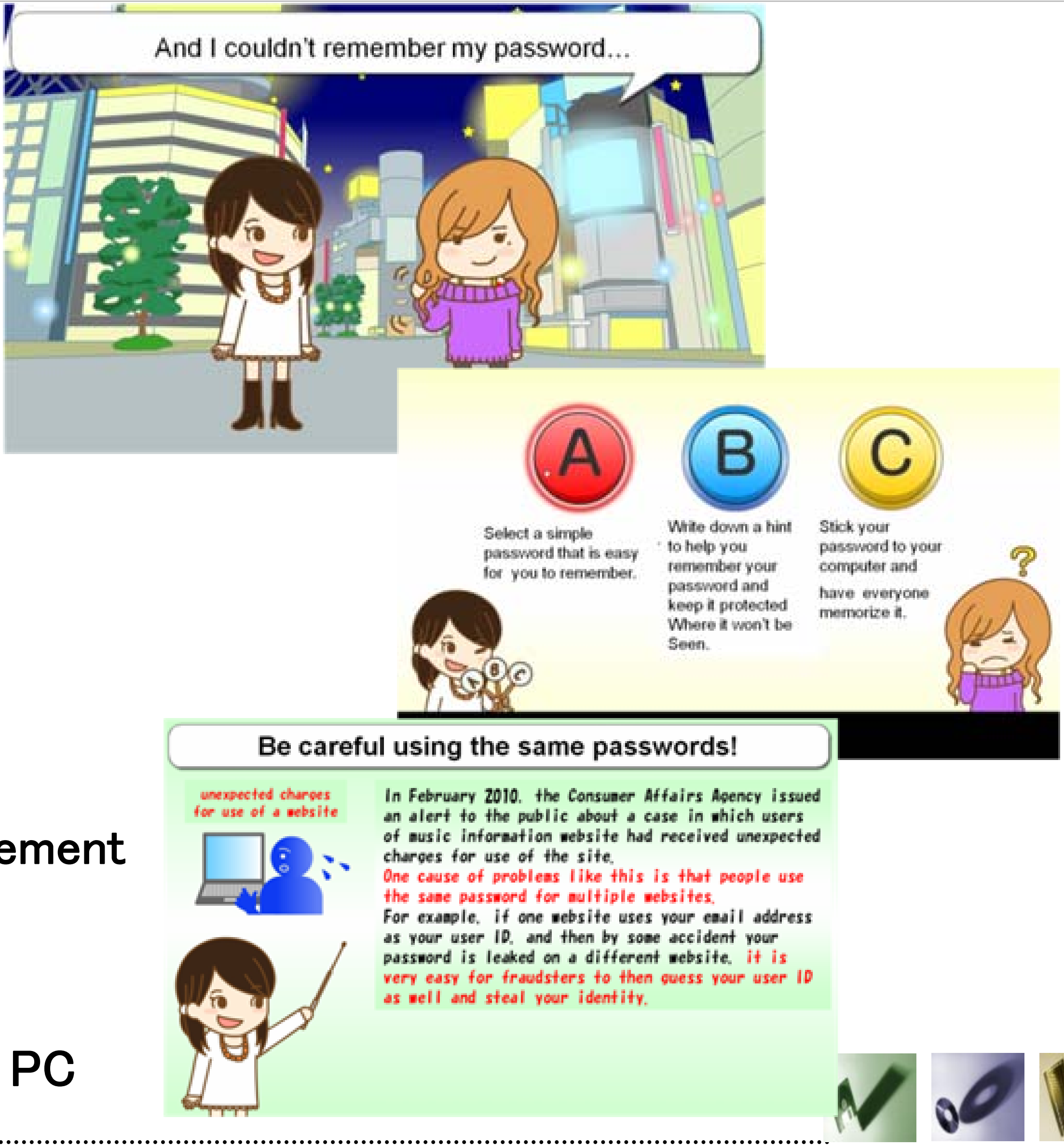
Development of material for information security education

- "Hikari & Tsubasa's Information Security Three Choice Tutorial"
- Fundamental of the sample policies and recent topics
  - Target on university students
  - 14 lessons
- Easy to self-learn
  - Anime of conversations between students
  - Three choice quiz + friendly tutorial
- Extension learning
  - Tutorial + Study points + Columns + Self-check
  - Textbook (4 pages description)



Three Choice Tutorial – Index

1. Virus
2. Phishing
3. Anonymous BBS
4. USB memory
5. SNS
6. Malware
7. Fraud bill
8. Copyright
9. Attached file
10. Wireless LAN
11. Password management
12. OS update
13. Net-shopping
14. Before dispose a PC



And I couldn't remember my password…

A
Select a simple password that is easy for you to remember.

B
Write down a hint to help you remember your password and keep it protected Where it won't be Seen.

C
Stick your password to your computer and have everyone memorize it.

Be careful using the same passwords!

unexpected charges for use of a website

In February 2010, the Consumer Affairs Agency issued an alert to the public about a case in which users of music information website had received unexpected charges for use of the site.
One cause of problems like this is that people use the same password for multiple websites.
For example, if one website uses your email address as your user ID, and then by some accident your password is leaked on a different website, it is very easy for fraudsters to then guess your user ID as well and steal your identity.