Advances in Computer Science and Engineering
Volume 3, Number 3, 2009, Pages 219-242

A SURVEY ON THE STATE OF INFORMATION SECURITY AT LOCAL GOVERNMENTS IN JAPAN

DAVAR PISHVA*, **NAOSHI KITAMURA and SEIJI TSUGAWA**

*Ritsumeikan Asia Pacific University
1-1 Jumonjibaru, Beppu City
Oita 874-8577, Japan
e-mail: dpishva@apu.ac.jp

Hyogo Prefectural Government
5-10-1 Shimoyamate St.
Kobe City, Hyogo 650-8567, Japan
e-mail: Naoshi_Kitamura@pref.hyogo.jp
Seiichi.tsugawa@itu.int

Abstract

This paper describes the current state of information security at local governments in Japan. It explains existing information security policy management frameworks and the difficulties in implementing them, especially at small local government offices. It clearly identifies potential department level security threats. The paper also shows why it is essential to prepare local government personnel, who are in charge of the system, to understand their system and manage them effectively rather than rely on the services of outsourcing companies. The Hyogo Prefectural Government, which has been playing a leading role in providing measures for safety and security of Japanese society since the Great Hanshin Awaji Earthquake, is used as a good representative model, and the practicality of the new framework is justified by detailed security risk analyses of the physical systems and surveys. By showing existence of information risks at the Hyogo Prefectural Government, which takes information security issues more seriously than other local governments in Japan, concludes that information security risks exist equally in all local governments.

Keywords and phrases: security policy, security management, security assessment.

Received July 27, 2009

I. Introduction

Today's business activities depend highly on information systems and every enterprise has its own information for its business. In an industrialized country like Japan, most enterprises use information technology to establish their management governance. This helps them to improve their efficiency and cost performance. As it is called *IT governance*, information systems have significant impact on the operations. Information assets have thus become valuable commodities for business and information systems are the key factors to ensure the growths of enterprises. Hence, it is essential to control the design process, development cycle and effective utilization of information systems.

Local governments, like any other enterprise, have to manage their information which is also valuable for their business. Being in the business of public service, local governments handle large amounts of sensitive information about their citizens, organizations, corporations, and numerous other institutions. The information types are varied and include, but are not limited to, resident registration, health welfare, national pension, taxation, environmental pollution, and topography.

As information and its value continue to increase, so does the management complexity, vulnerability and attractiveness to malicious attacks. Security threats can come in the form of unauthorized accesses, computer viruses, or cyber attacks. The threats can also come from various sources; some of them may be insiders and the rest outsiders. Some of them may be deliberate and others accidental. At any rate, enterprises are subject to information security threats.

Security threats exploit vulnerabilities of an information system in order to compromise it. A system may be vulnerable because of an un-patched program, existence of an irrelevant user account, or utilization of an easily guessable password. Furthermore, due to the complexity of an information system, it is actually very difficult to develop one without any vulnerability. As long a system is up and running, vulnerabilities can emerge. Exploiting information system vulnerabilities can result in information leakage, functional failure, or denial of service. When such things happen in reality, they can jeopardize the enterprise and may cause huge financial or credibility losses.

II. State of Information Security in Japan

Japan has historically been a peaceful country, and it is a well known fact that the Japanese think they can have water and peace for free [2]. They are less conscious of security and do not fully realize the importance of information security until they get involved in a security incident. Furthermore, because of the nature of Japanese laws, there have been only a few cases in which large penalties were imposed for causing information security breach incidents. As such, the Japanese tend to have a less security conscious mind setting than people of other countries. According to an IBM survey in 2006, only 15% of Japanese companies are confident of confronting cybercrime, while on the average, 58% of foreign companies around the world are ready to handle such situations [14].

(A) Information security incidents

This section briefly examines the trends of information security incidents in Japan.

Figure 1 shows reported number of virus from 1990 to 2005 [16]. As can be observed, the number of incidents has been remarkably increased since 2004, due to the spread of many variants of Netsky and Mytob.

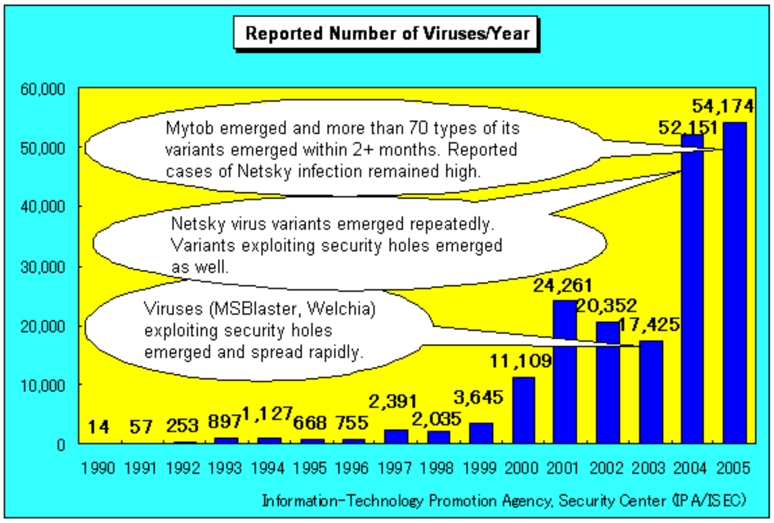

Figure 1. Spread of computer virus in Japan (Source: IPA/ISEC, 2006).

Figure 2 shows the number of cases of reported unauthorized computer access from 1997 to 2005 [17]. As can be observed, the number of cases per year exceeded 400 in the last 5 years.

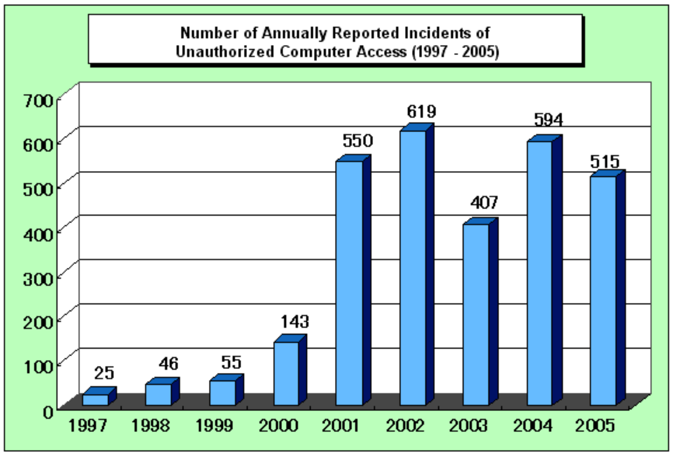

Figure 2. Unauthorized computer access in Japan (Source: IPA/ISEC, 2006).

Table I shows the numbers of reported security incidents and affected victims from 2002 to 2005 [25, 26]. As can be observed, the total number in 2005 is about 18 times that of 2003. Such a tremendous increase is due to full enforcement of Personal Information Protection Act (PIPA) which came into effect in 2004. This indicates that prior to the PIPA, only very few security incidents were publicized. There are of course many more cases of information leakage that occur through anonymous P2P file sharing applications such as Winny and Share [4].

Table I. Information leak disclosure in Japan (Source: NPO JNSA, 2006)

Year	2002	2003	2004	2005
Total number of organization reporting	63	57	366	1,032
Number of victims	418,716	1,554,592	10,435,061	8,814,735
Average number of victims per incident	7,613	30,482	31,057	8,922

(B) Information security audit

Information security audit or assessment is essential for improving and managing information security risks. The implementation cycle is usually called 'PDCA', which stands for plan - do - check - act. An enterprise makes a security policy, adopts a security measures and monitors its operation. These activities must also be evaluated for possible improvement.

In Japan, the security audit system was established by the Ministry of Economy Trade and Industry (METI) in April 2003. A total of 510 companies have registered for the system as of 2005 [34]. Information security audits are still at its infancy state in Japan, but the National Government is trying to facilitate its adoption.

(C) Commonly used standards

ISO/IEC17799 is a globally used standard that has been developed based on the UK's BS7799. The most commonly used information security standard in Japan, however, is the Information Security Management System (ISMS) which is based on BS7799-2. Although ISO/IEC17799 does not have a certificate mechanism, both ISMS and BS7799 do. Acquisition of an ISMS or BS7799 certificate demonstrates that an organization can manage information security at a certain required level. As of July 2006, there were a total of 1681 ISMS certified companies in Japan [15]. As shown in Figure 3, the number has steadily increased since the inception of ISMS in April 2002. Given the formation of the new global standard, ISO/IEC27001, it is projected that many companies would gradually shift toward this standard.

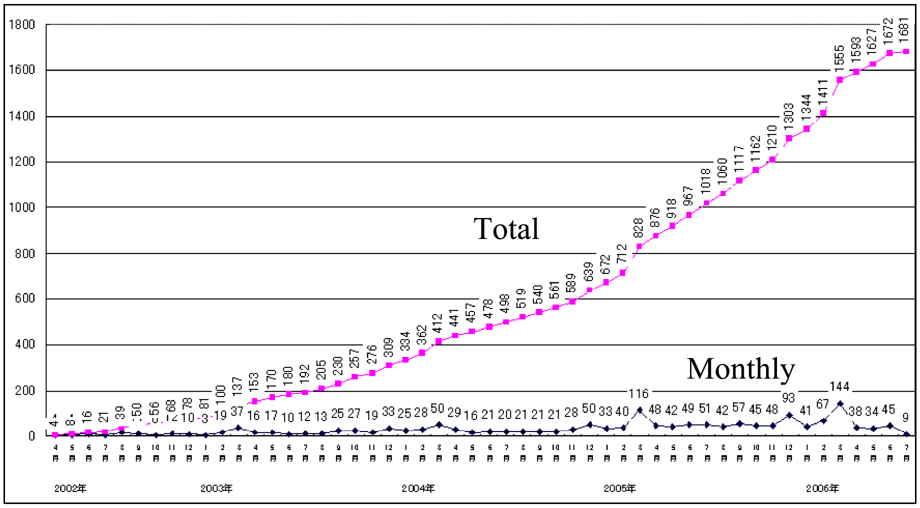

Figure 3. Number of ISMS certified companies (Source: JIPDEC, 2006).

III. Information Management at Local Governments

This section briefly examines the nature of information systems in local governments, their peculiarities, available resources, existing security management framework and associated problems.

(A) Characteristics of the information system

In Japanese local government offices, information are usually kept at the level of the department or division that needs the information for regular operations. Such information, however, are acquired by government authorities in accordance to the guidelines of pertinent laws and regulations. They are kept confidential and online-connection to other information systems for the purpose of data exchange is strictly governed by the personal information protection ordinance of the local government. This, however, leads to information overlap and inconsistency (e.g., a person's name, address, etc., may be stored at several departments). Each department also tends to develop its own information system for managing its business. As such, many functionally similar information systems are developed and operated in parallel and independent of each other across the departments.

(B) Resource allocation for information management

While information systems play an important role, most local governments have paid less attention to efficient management in comparison to private organizations. This is because of the organizational nature and management philosophy of the local governments which creates numerous constraints to train skilled IT personnel.

First of all, preference is given to train people competent in general affairs who can handle numerous tasks in the local government than to train people in a rapidly changing, growth unpredictable field like information technology. Furthermore, for numerous administrative reasons, local government personnel are not allowed to stay in a specific department for a long period of time. They are usually rotated geographically and/or departmentally every couple of years and are expected to efficiently function in their new locations. Consequently, those in charge of information technology are regular employees trained in general affairs that perform system administrators' tasks on their available time. Hence, fewer budgets get also allocated toward training competent leaders in information technology. With the exception of a few departments such as accounting and personnel, local government personnel have little know-how about in-house information system development, management, or maintenance. They mostly rely on the services of outside vendors.

(C) Factors aiding information security risks

There are some peculiarities in the source and nature of information security risks at local governments. Despite the fact that local government offices have personnel from as few as 100 people to as many as 170,000, the expected information security risk management level is the same from all of the offices. The decentralized nature of information makes them more vulnerable. They are also more attractive to the attackers because any damage can create large impacts. The information are also easily available to unskilled personnel, part time employees, and outside vendors. Furthermore, because of the bureaucratic nature of the local governments, it takes a long time to act on and properly handle an information security breach incident.

(D) Information security management framework

The most commonly used information security management guideline among local governments is that issued by Ministry of Internal Affairs and Communications (MIC) in December 2003 [20]. It is based on ISMS and provides a specific list for security management, a procedure for information security audit, general methods for technical evaluation, and self-check lists. Although local governments conduct information security management based on this standard, following all of the guidelines becomes cumbersome and impractical in most cases. As such, the guidelines must be customized and an essential minimum set needs to be uniformly implemented throughout all local government offices, as these handle information of similar value.

(E) Outlook of information governance

More and more local governments have established their own information security policy. During the past three years, the coverage has increased from 30.2% to 96.3%, as indicated in Figure 4 [21]. Currently 100% of the 47 Prefectural offices and 96.2% of the 2,418 Municipalities have established their own information security policies. The driving force behind such a rapid growth can be attributed to the MIC guidelines and to the legislation of pertinent laws and regulations such as PIPA.

Figure 5 shows the level of security measures that local governments take for numerous procedures. As can be observed, the implementation rate is quite high for items like: ‘Check the entrance and exit of server rooms’, ‘Backup the power supply’, ‘Backup data’ and ‘Store access logs’, and low for ‘Encrypt important information assets’ and ‘Encrypt information on the in-house LAN’. Note also that large differences (over 40%) exist between Prefectures and Municipalities in the items of ‘Erase data upon retirement’ (prefectures: 83.0%, municipalities: 36.6%) and ‘Security education for employees’ (prefectures: 95.7%, municipalities: 51.5%). These are attributable to the differences in organizational scales.

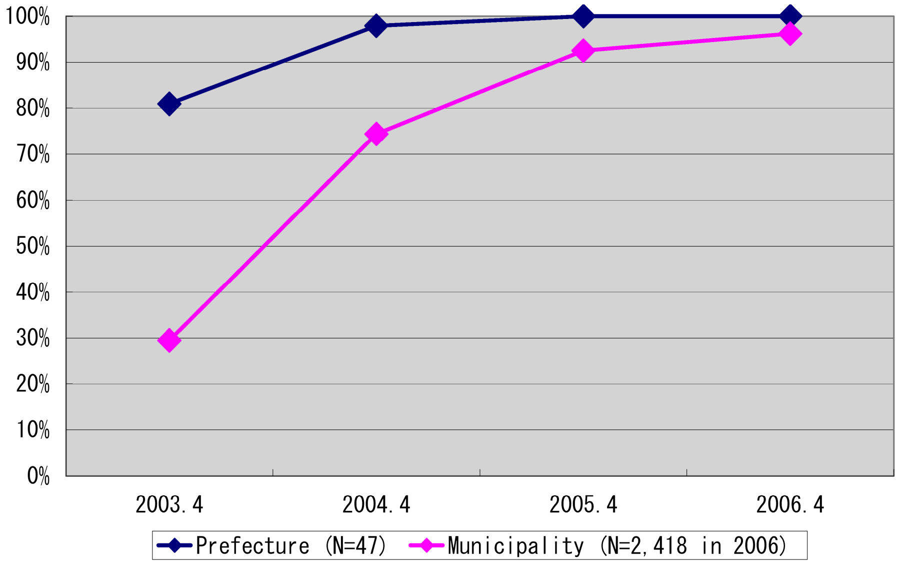

Figure 4. Establishment of information security policies (Source: MIC, 2005).

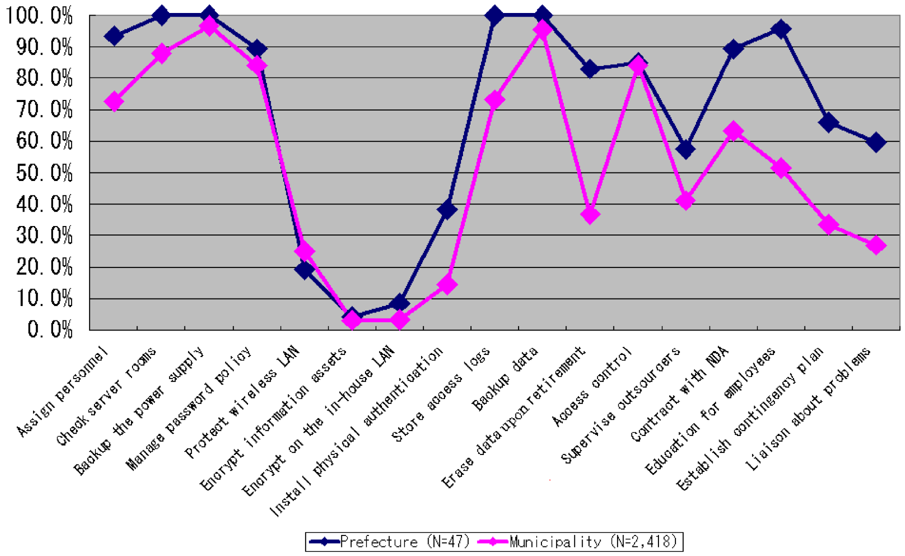

Figure 5. State of information security measures (Source: MIC, 2005).

Table II shows the state of information security audit system in the respective offices. As expected, more Prefectural offices than Municipalities have or plan to acquire a security audit system.

Table II. State of information security audit (Source: MIC, 2005)

		Prefecture $(N = 47)$	Municipality $(N = 2,418)$
Have an audit system		26 (55.3%)	504 (20.8%)
	Internal audit	10 (38.5%)	344 (68.3%)
	External audit	12 (46.1%)	108 (21.4%)
	Internal and external	4 (15.4%)	52 (10.3%)
Plan an audit system		21 (44.7%)	1,231 (50.9%)
No plan for audit system		0 (0 %)	683 (28.2%)

(F) Information security enhancement efforts

Local governments also try to improve their information security but, there are issues which facilitate/complicate the process [19]. Usually the smaller offices are at a disadvantage. Nonetheless, information security management is still at the infancy stage and the steps of PDCA cycle have not yet matured. This is because, most local governments have just established their security policies and are beginning to implement them. Furthermore, MIC guidelines on risk analysis and security audit are not much utilized due to being quite general and envisioning hypothetical environments.

The levels of information security management at local governments are thus unsatisfactory, considering the huge amount of information being dealt with. Legal constraints and lack of direct incentives (with the exception of information and administration divisions) also adversely affect the process. A framework that local governments need for information security improvement is not a detailed list of procedures or guidelines, but handy methods that ordinary government personnel can implement on their own with some initial trainings.

IV. Hyogo Prefectural Government as a Study Model

We used the Hyogo Prefectural Government as a model for collecting first-hand data on how information security is handled. State of the actual information security system is compared with its perceived status, potential sources of discrepancies are identified, and recommendations on how to improve the actual state of information security at local governments are made.

The Hyogo Prefectural Government is a good representative model for local governments because it is one of the most active local governments that works on information security issues in Japan [8], [10], [33]. Hyogo Prefecture is also known as a miniature of Japan because it encompasses various characteristics of Japan. It contains a rich variety of communities ranging from large cities to rural villages, has isolated islands, diverse climatic and natural conditions [12], [13]. Among the 47 prefectures of Japan, it has the 11th biggest land area, 8th largest population, and has also 8th highest gross product.

It has also seriously embraced information security management since 2002 and its operations are that of a typical local government (culture, education, community corporation, disaster prevention, health, welfare, environment, industry, employment, agriculture, forestry, fisheries, public works, urban development and housing).

Therefore, identification of information security flaws in the prefecture's system and recommendations on how to make improvements can equally benefit other local governments in Japan.

(A) Overview of information management

Hyogo Prefecture has developed its own information security management framework since 2002. It has around 150 bases which include the head office, 10 district branches and sub-branches. Every department has developed its own information system. There are about 79 major departmental systems as of March 2006 [11]. A few of the systems, which serve as back offices, e.g., for personnel and accounting, are managed by somewhat skilled IT personnel, and managements of the rest are outsourced. These 79 information systems are categorized into the following 4 types: critical systems (11), departmental business systems (46), systems operated by mainframe (9), systems dedicated to delegated tasks from the national government (13).

(B) Information security audit

In order to monitor the state of information security, we conducted an annual assessment for department level information system from 2002 to 2005 [5-7, 9]. Here, we briefly examine the results of risk analysis for acceptable risk levels [35-38].

Figure 6 shows average gap value, (a ratio between a calculated risk level and an acceptable one), of administrative servers in relation to various types of risks. As can be observed, security risks have apparently improved steadily since 2002, and have become close to a minimum acceptable level (100%).

However, examination of the gap value for a particular risk, e.g., computer virus, shows that though a general tendency of improvement is seen with all server types, departmental business servers do not have acceptable risk levels (Figure 7).

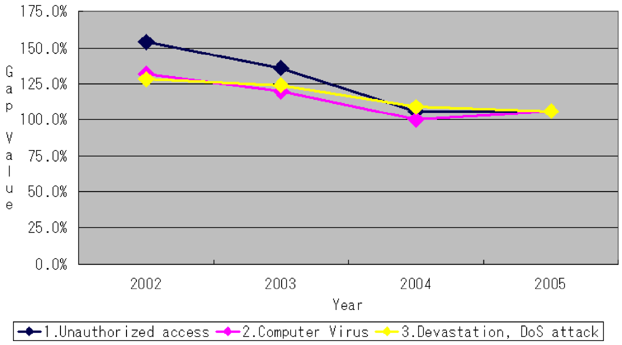

Figure 6. Average gap value for administrative servers.

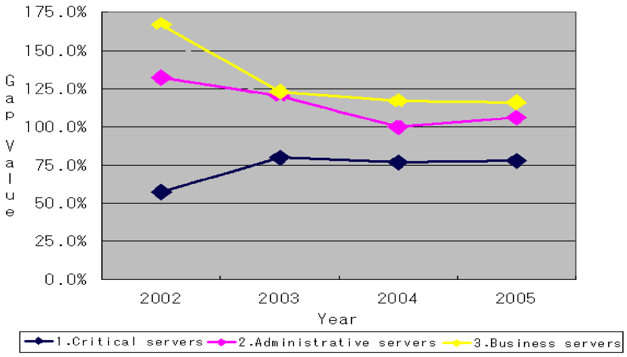

Figure 7. Average gap value for all servers.

The situation looks even worse, when the risk level is examined on a per server basis. Figure 8 shows per server based risk levels in 2003 and 2005 [6, 9]. Here, *N* indicates the number of servers, and its increase in every category is due to system reinforcement done during a two-year period. As can be observed, risk levels have improved for critical servers by around 33% and by 58% for administrative servers, while improvement of business servers has been a comparatively negligible amount of 3%.

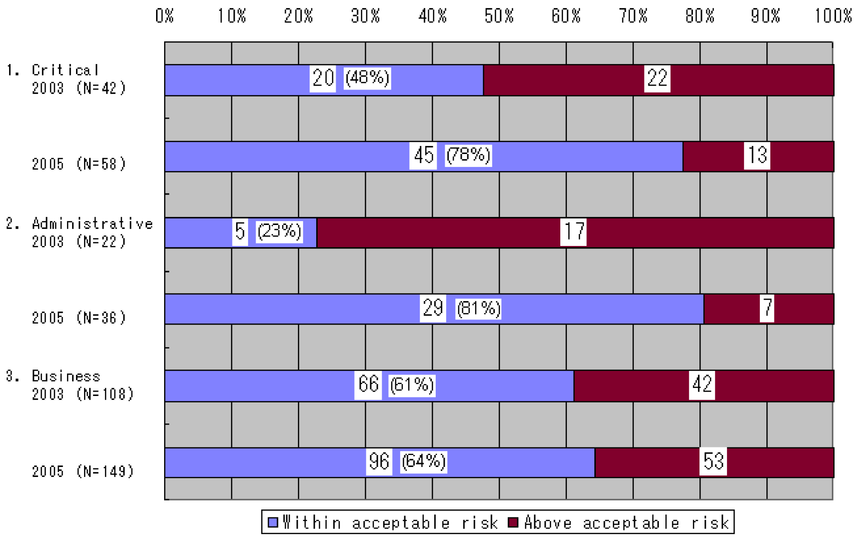

Figure 8. Server based average gap value.

This shows that although tremendous improvements have been made in regard to information security risks at critical and administrative servers, the same is not true for business servers, which are mostly managed by ordinary Prefectural employees. It further indicates that in Hyogo Prefecture, despite the existence of an information security management framework based on ISMS and MIC guidelines, security risks of business servers have not been properly handled. This made us wonder about what may have caused this phenomenon! Were security procedures actually implemented? Can the system administrators effectively manage the systems, etc.?

V. Examination of Security Measures

In order to investigate the above phenomenon, we re-examined the security measures at Hyogo Prefecture's head office by doing a detailed risk analysis on the physical systems and by conducting surveys. The investigation involved vulnerability assessment of databases and web servers and re-examination of security risks in terms of data protection. 23 out of a total of 79 systems were used in the process. 21 database servers on 14 systems and 48 web servers on 18 systems were assessed. Examination of security procedures was carried out by distributing survey questionnaires to system administrators of 17 systems.

(A) Vulnerability measurements

Vulnerability scanners were primarily used in our investigation since these enable us to readily examine a large number of servers in a relatively short period of time. For web systems, we used Nikto [23] and N-Stealth [27] and for database systems, we used AppDetective [1]. In addition, the following softwares were used to complement the evaluation process: nmap [24], Nessus [22], SQL Dict [32], SQL Auditing Tools [31], Oracle Auditing Tools (OAT) [28] and OSScanner [29]. Nmap and Nessus were used for verification of the operational states of services, and Nessus, SQL Dict, SQL Auditing Tools, OAT and OSScanner were employed to check the correctness of the vulnerability detection.

The following sections detail assessments of our measurements and the analysis of database servers. Presentation of similar results, which were also obtained for web servers, is omitted because of spatial constraints.

(B) Assessment results for database servers

Table III shows a summary of assessment results obtained for database servers in July 2006. As can be observed, 10 out of 13 Microsoft SQL servers, and all of 8 Oracle servers did not have the latest updates. Considering the fact that the latest updates for these software were available a year earlier (MS SQL server 2000 SP4 was released in May 2005 and Oracle 9.2.0.7.0 in August 2005), this indicates that the servers were not properly maintained.

Table III. General status of database servers (July 2006)

	Patched with the latest updates	Not patched with the latest updates	Total
Microsoft SQL server	3	10	13
Oracle	0	8	8
Total	3	18	21

Tables IV and V show scan results for potential risks facing 13 Microsoft SQL and 8 Oracle servers, respectively. They are categorized into seven types: denial of services, misconfigurations, password attacks, vulnerabilities, access control, application integrity, identification/password control, and OS integrity. The severity is ranked according to the 4 categories of high, middle, low and informational.

Table IV. Potential risks for MS SQL servers (July 2006)

	High	Middle	Low	Informational	Example
Denial of services	-	-	-	-	(None)
Misconfigurations	-	-	13	-	Low: Standard SQL Server authentication allowed
Password attacks	3	-	-	-	High: Blank password for system administrators acct.
Vulnerabilities	10	10	1	-	High: Named Pipe Hijacking
Access control	13	13	13	13	High: Agent jobs privilege escalation High: Permission on registry extended proc
Application integrity	10	12	13	-	High: MDX Query buffer overflow
Identification/ Password control	9	13	12	-	High: Password same as login name
OS integrity	-	-	13	-	Low: Registry extended proc not removed

Table V. Potential risks for Oracle servers (July 2006)

	High	Middle	Low	Informational	Example
Denial of services	-	-	6	-	Low: Malformed RPC request DOS
Misconfigurations	6	-	-	-	High: ADMIN_RESTRICTIONS flag not set
Password attacks	7	-	-	-	High: Default database password
Vulnerabilities	8	4	-	-	High: Database link buffer overflow
Access control	6	6	5	3	High: Create library privilege
Application integrity	6	6	5	-	High: BFILENAME buffer overflow
Identification/ Password control	6	-	-	4	High: Easily-guessed database password
OS integrity	-	-	-	-	(None)

First, let us observe the ‘Vulnerabilities’ and ‘Application integrity’ categories. We can see that 10 out of 13 MS SQL servers and almost all of the Oracle servers have ‘high’ risks. A typical cause could be failure to patch the systems with the latest updates, thus exposing them to computer virus exploitation.

Next, let us examine the ‘Denial of Services’, ‘Misconfigurations’ and ‘Access Control’ categories. All 13 MS SQL servers and 6 out of 8 Oracle servers have ‘high’ risks too. A typical cause could be improper access privilege management, which can expose system files to malicious alterations. Apparently, unnecessary privileges were given during installation of the systems and were left as they were since then.

Lastly, by observing the ‘Password attacks’ and ‘Identification/Password Control’ categories, we can see that 9 out of 13 MS SQL server and 7 out of 8 Oracle servers show ‘high’ risks as well. Typical causes were traced to usage of blank password for system administrator accounts (on 3 MS SQL servers) and utilization of default account settings (on 7 Oracle servers). Use of such easily guessable passwords on administrative accounts makes the system highly susceptible to unauthorized access.

(C) Risk analysis for database servers

We performed risk analysis on the scanned data in order to determine acceptable risk levels. The analysis was done on three types of risks, i.e., (1) unauthorized access, (2) computer viruses, (3) devastation and DOS attacks. A numerical value from 4 to 1 was assigned to indicate the occurrence interval of such threats in the following order:

- 4 = Frequently.
- 3 = Occasionally.
- 2 = Accidentally.
- 1 = Rarely.

The following numerical values were also used to indicate the vulnerability levels of such threats:

- 4 = Administrative privilege permission.
- 3 = Data access permission.
- 2 = Avoidable through preventive operations.
- 1 = Can resist well-known security holes.

Table VI shows a summary of the result for database servers. Entries in the ‘Risk’ column were derived by simply multiplying threat and vulnerability values for the three risk types, and the ‘Gap Value’ is the ratio between the calculated and an acceptable (1st row) risk levels. Entries for unacceptable risk levels (gap value > 100%) are hatched to improve clarity of the results. (Entries in the 1st four columns are attributes of the systems.)

As can be observed, 10 out of 21 servers have unacceptable risk levels for unauthorized access, 18 out of 21 have unacceptable risk levels for computer virus, and 16 out of 21 have unacceptable risk levels against devastation and DOS Attack. The ‘Ave.’ column indicates that 20 out of 21 database servers, on the average, have unacceptable risk levels.

Table VI. Security risks of database servers (July 2006)

System	Server	DBMS	Network	Threat			Vulnerability			Risk				Gap Value (%)			
				1	2	3	1	2	3	Total	1	2	3	1	2	3	Ave.
Acceptable				3	4	2	2	2	2	18	6	8	4	100	100	100	100
#05	#01	MS SQL	Separated	2	3	2	3	3	3	21	6	9	6	100	113	150	121
	#02	MS SQL	Separated	2	3	2	3	3	3	21	6	9	6	100	113	150	121
	#03	Oracle	DMZ	3	4	2	1	3	2	19	3	12	4	50	150	100	100
#07		Oracle	Inhouse VPN	2	3	2	4	3	2	21	8	9	4	133	113	100	115
#08		MS SQL	Common LAN	3	4	2	4	3	3	30	12	12	6	200	150	150	167
#09		MS SQL	Common LAN	3	4	2	4	3	3	30	12	12	6	200	150	150	167
#11		Oracle	Inhouse VPN	2	3	2	4	3	2	21	8	9	4	133	113	100	115
#13		Oracle	Separated	2	3	2	4	3	3	23	8	9	6	133	113	150	132
#14		MS SQL	Common LAN	3	4	2	2	2	3	20	6	8	6	100	100	150	117
#15		MS SQL	Common LAN	3	4	2	2	4	4	30	6	16	8	100	200	200	167
#16	#01	Oracle	DMZ	3	4	2	4	4	3	34	12	16	6	200	200	150	183
	#02	Oracle	Separated	2	3	2	4	4	3	26	8	12	6	133	150	150	144
	#03	MS SQL	Separated	2	3	2	3	2	3	18	6	6	6	100	75	150	108
	#04	MS SQL	Separated	2	3	2	3	2	3	18	6	6	6	100	75	150	108
	#05	MS SQL	Separated	2	3	2	3	3	3	21	6	9	6	100	113	150	121
	#06	MS SQL	Separated	2	3	2	3	3	3	21	6	9	6	100	113	150	121
#18		Oracle	Separated	2	3	2	4	4	2	24	8	12	4	133	150	100	128
#19		Oracle	Common LAN	3	4	2	4	4	2	32	12	16	4	200	200	100	167
#20		MS SQL	Inhouse VPN	2	3	2	3	3	3	21	6	9	6	100	113	150	121
#21		MS SQL	Inhouse VPN	2	3	2	4	3	3	23	8	9	6	133	113	150	132
#23		MS SQL	Inhouse VPN	2	3	2	4	3	4	25	8	9	8	133	113	200	149
Average				2.3	3.3	2.0	3.3	3.1	2.9	23.8	7.7	10.4	5.7	128	130	143	133

(D) Survey of information security practices

In order to determine the potential causes of such high risks, we conducted a survey by interviewing department level system administrators. A total of 17 system administrators took part in answering numerous questions from the following domains:

1. The length of service as a system administrator.
2. Information security policies of the department.
3. Details of contracts with outsourcers.
4. Implementation of information security measures.
5. Security measures being taken in the department.
6. Knowledge of information security.

The results are summarized as follows:

1. The average length of service as a system administrator was 2 years, and 8 out of 17 had no system administrator experience when they assumed their posts.

2. Though most of the departments have information security policies, these have not been reviewed in the past three years. 6 out of 17 system administrators did not even know about the existence of information security policy in their departments!

3. Most of the less experienced system administrators did not understand the details of contracts, did not evaluate reports that were submitted to them by the outsourcers, and simply assumed that the outsourcers were responsible for all security issues and were doing their jobs well.

4. Most experienced system administrators, however, implemented information security measures.

5. Security measures were mostly limited to firewalls, virtual private network (VPN) and antivirus software. Most departments did not regularly store detailed access logs of their database management systems (DBMS).

6. The system administrators' understating was mostly limited to what they had learned through self-study, as they were not provided enough opportunity to undergo formal training. Most of the less technically inclined system administrators relied on instructions from experienced colleagues.

(E) Potential sources of discrepancies

Discrepancies between the perceived status of information security and its actual state per our evaluation at the Hyogo Prefectural Government can be attributed to the following constraints:

- Shortage of experienced and knowledgeable system administrators.
- Insufficient organizational support to train competent IT personnel.
- Assumption that mere existence of information security policy implies secured environment.
- Excessive dependency on outsourcers and inability to supervise and monitor their work.

Furthermore, the leading steps that the prefecture had taken for security measurement emphasized the following aspects:

- The emphasis was to protect the 'systems' and not the 'information' itself.
- Security threats and vulnerability measures were mostly taken against attack from outsiders, i.e., attack from insiders were not seriously considered.

- Security assessments were mostly limited to OS and the network layers, i.e., application layer threats were not investigated.
- Security assessments of public web servers were limited to external-use and did not include internal-usage.

VI. Discussion

Based on the results of vulnerability assessments and the ways in which information security is implemented in Hyogo Prefecture; the following generalization can be drawn in regard to the state of information security in local governments in Japan:

(A) Narrow scope of coverage

It seems that institutionalized efforts toward implementing information security have focused on protecting the systems rather than the valuable information that are stored therein. The use of antivirus software, firewalls and separation of systems by means of multiprotocol label switching virtual private networks (MPLS-VPN) are popular but, little attention is given to internal abuses. Disgruntled employees could easily leak sensitive information of a department without getting noticed.

Database and web-application systems of Hyogo Prefecture, which hold valuable information of its clientele, were not secured. This is because web servers were not patched with the latest updates and were left vulnerable against known security holes. Existence of unnecessary default setting and use of easily guessable passwords on database systems made them vulnerable to internal abuses. Access control, logging, and auditing were implemented in only a few instances.

(B) Difficulties in policy implementation

There are a number of reasons that make implementation of information security policies difficult at local governments:

1. Overburdening of experienced and knowledgeable system administrators because of inadequate IT skills among end users and their supervisors.

2. Existence of technical communication gaps among system administrators, their supervisors and end users.

3. Inability to continue enforcement of existing information security procedures after a regular personnel reshuffling of the local governments.

4. Inability to review existing information security procedures and adopt them to current situation.

(C) Difficulties in technical supervision

Supervisors of the division chief level in each department are not keen about actual information security management. A common mentality is: because they cannot understand the technology, they would rather delegate such tasks to system administrators. Such an attitude indicates lack of responsibility since administration of the system is also a part of their work. In fact, the supervisors are one of the final signatories when it comes to approving a new departmental information security procedure or certifying its current state.

(D) Difficulties in performance evaluation

Even though information security is mostly outsourced, many system administrators are not capable of supervising and evaluating their work. As a matter of fact, many less technically inclined system administrators simply assume that outsourcers are performing their obligation as stipulated in their contracts. However, in many cases, outsourcers shortchange the departments because compliance to security procedures does not create extra profit.

VII. Proposal of a New Information Security Management Framework

The following two approaches are recommended in order to come up with a better information security management framework at local governments:

(A) Adoption of practical techniques

First of all, the job of system administrators should be recognized as a profession in itself and sufficient technical training should be provided in accordance to their important roles and responsibilities. Suitable system administrator training programs and virtual systems, on which they could safely practice techniques to overcome malicious users’ tactics, should be provided.

When highly-trained system administrators have to be rotated because of the personnel reshuffling policy of the local governments, they should be rotated in line with their job descriptions. This way, investments on their training will not be wasted; they can efficiently function in their new assignments and effectively contribute to information management goals of the local governments. This will also reduce heavy reliance on outsourcers, consequently, reducing substantial budget requirements. Furthermore, it is not even recommended to outsource security of local governments' information system, which contains huge amounts of sensitive information [3].

They should also be familiarized with both organizational and departmental information security objectives of the local governments. They should be provided with detailed but practically implementable department level information security procedures to enable them to protect valuable information of their departments. They should also be able to effectively supervise outsourcers, (when their services become absolutely necessary), in line with the organizational information security objectives.

Implementation of information security practices should begin from the moment a new system is installed. Since the systems are mostly installed by outsourcers, department level system administrators should ensure correct system configuration, appropriate access controls, and enforcement of strong passwords usage practices.

In implementing security practices, particular attention should also be given to application level risks. As was observed in the case of Hyogo Prefecture, simply securing the operating system and network layers is not enough.

Security practices should equally protect the information itself. Current practices are centered on protecting the computers against attacks from outsiders. There are no serious provisions for preventing information leakage via insiders and legitimate users. If such people abuse the system, then they can cause substantial damage and it would also be very difficult to trace the source due to inappropriate logs and audit practices.

Finally, supervisory groups should be created, at least at Prefectural levels, to enforce uniform adoption of well developed systems and practices, and to prevent parallel development of functionally similar type information system throughout the local government offices. Incentives for novel information system development, coordinated management, and preventive maintenance, which greatly enhance the smooth operation of offices, should also be provided.

(B) Refinement of procedures

Security procedures should be reviewed on a regular basis. Furthermore, the review should be carried out according to risk analysis in order to reflect the current situation. To avoid budgetary constraints, the review should be conducted at a low cost, and there are many readily available tools that allow a professionally trained system administrator to achieve such objectives.

A model of Request for Proposal (RFP) for security procedures and their implementations should be introduced. Without a model, it is difficult for system administrators to establish information security requirements from scratch, considering their busy schedules and time-constraints. Introduction of such a model could be as simple as exemplifying the names of some security specifications issued by some public/non-profit organization in Japan [18].

Consensus should also be built on an acceptable security risk level prior to the adoption of security measures. Administrative managers should be held accountable for the enforcement of the agreed-upon information security risk managements. The current practice of placing an administrative manager symbolically in charge of information security and having the job done by a system administrator should also be changed.

VIII. Conclusion

In this paper, we explored the possibility of improving the information security management in local governments in Japan. The study revealed that at present, an effective information security management framework does not exist in the local governments. It also showed that there are many factors that mitigate information security risks in local governments and the seriousness of some of these have not been fully considered.

In order to come up with a reliable recommendation on how to improve the situation, we used the Hyogo Prefectural Government as a good representative model, obtained first-hand vulnerability data from their physical systems, performed a detailed security risk analysis to assess the situation, and by conducting surveys on how information security practices are actually done, we were able to identify potential areas that need to be improved.

Existence of information risks at the Hyogo Prefectural Government, which takes information security issues more seriously than other local governments in Japan, indicates that information security risks exist equally in all local governments. Furthermore, the value of information is the same for people regardless of the scale of local governments.

It is envisioned that local governments can greatly improve their information security management systems by investing in their qualified key personnel, reviewing their personnel shuffling policies, and dynamically adapting to practical and implementable security policies. Such practices will reduce reliance on the services of outsourcing companies, thus generating an associated budget surplus and resulting in good security policy practices. It is further hoped that the Hyogo Prefectural Government, by trying to improve their current state of information security management at the Prefectural level, will serve as an exemplary model for other local governments in Japan.

Acknowledgements

The authors would like to thank Dr. Keiji Takeda for his useful suggestions and valuable comments during the initial phase of this work. Special thanks are also due to Hyogo Institute of Information Education Foundation for partially supporting this work.

References

[1] AppDetective free version.
http://www.appsecinc.com/products/appdetective/

[2] Isaiah Ben-Dasan (Shichihei Yamamoto), The Japanese and the Jewish, 1970.

[3] CSI/FBI, CSI/FBI Computer crime and security survey, 2005, pp. 9-10.

[4] http://www.securitypark.co.uk/article.asp? Articleid = 25103 & CategoryID=1.
Antinny worm creates data havoc in Japan by infecting Winny Peer to Peer (P2P) File Sharing Program, Posted in Security News - IT and Computer Security - on 22/03/2006.

[5] Hyogo Prefectural Government, The report of internal information security audit, October 2002.

[6] Hyogo Prefectural Government, The report of external information security audit, October 2003.

[7] Hyogo Prefectural Government, The report of internal information security audit, October 2004.

[8] Hyogo Prefectural Government, The Second Promotion Strategy of Information Technology in Hyogo Prefecture, P.7, 2004, pp. 43-44.

[9] Hyogo Prefectural Government, The report of internal information security audit, October 2005.

[10] Hyogo Prefectural Government, Programs for the Second Promotion Strategy of Information Technology in Hyogo Prefecture in 2006, P.1, 2006, p. 24.

[11] Hyogo Prefectural Government, Enterprise Architecture of Information System in Hyogo Prefectural Government, March 2006.
http://web.pref.hyogo.jp/jichijo/ea17/index.htm

[12] Hyogo Prefectural Government, Hyogo Profile Hyogo Prefecture-A Japan in Miniature.
http://web.pref.hyogo.jp/english/main/htmls/miniature03.html

[13] Hyogo Prefecture, Wikipedia - the free encyclopedia.
http://en.wikipedia.org/wiki/Hyogo_Prefecture.

[14] IBM, Survey of company security against cybercrime, 2006.
http://www-06.ibm.com/jp/press/20060501001.html
http://www-03.ibm.com/press/us/en/pressrelease/19367.wss

[15] ISMS certificated companies in Japan.
http://www.isms.jipdec.jp/lst/ind/suii.html
http://www.iso27001certificates.com/.

[16] IT Security Center Information-technology Promotion Agency, Japan, Virus Report Status for 2005, January 27, 2006.

[17] IT Security Center Information-technology Promotion Agency, Japan, Unauthorized Computer Access Report Status for 2005, January 27, 2006.

[18] Japan Network Security Association, Security requires specification of RFP in Web system beta version, December 2005.
http://www.jnsa.org/active/2005/active2005_1_4a.html

[19] Local Government Measure of Security Support Forum, The issues that facilitate information security audit, March 2006.

[20] Ministry of Internal Affairs and Communications, Research report of the way of information security audit for local government, December 2003.

[21] Ministry of Internal Affairs and Communications, The outlook of information governance in local government, October 2005.

[22] Nessus Vulnerability Scanner.
http://www.nessus.org/.

[23] Nikto.
http://www.cirt.net/code/nikto.shtml

[24] nmap.
http://www.insecure.org/nmap/download.html.

[25] NPO Japan Network Security Association, 2004 Information Security Incident Survey Report ver1.1 - Information Disclosure: Projected Legal Reparations and Observations (Legal Reparations and Influence on Share Price), January 10, 2006.

[26] NPO Japan Network Security Association, 2005 Information Security Incident Survey Report ver1.0 - unsettled version, June 1, 2006.

[27] N-Stealth Free Version.
http://www.nstalker.com/eng/products/nstealth/

[28] Oracle Auditing Tools (OAT).
http://www.cqure.net/wp/?page_id=2.

[29] OSScanner.
http://www.cqure.net/wp/?page_id=3.

[30] D. Pishva, N. Kitamura, S. Tsugawa and K. Takeda, An initiative to improve the state of information security at local governments in Japan, 41th Annual IEEE International Carnahan Conferences on Security Technology, 2007, pp. 8-17.

[31] SQL Auditing Tools.
http://www.cqure.net/wp/?page_id=6.

[32] SQL Dict.
http://www.ntsecurity.nu/toolbox/sqldict/.

[33] The Hyogo Information Security Promotion Association, Hyogo Information Security Promotion Program, 2006, pp. 3-4.

[34] The registry of information security audit companies.
http://www.meti.go.jp/policy/netsecurity/iskansa/index.html.

[35] Seiji Tsugawa, A study on the construction of the risk management cycle for the information assets of the local government, The Journal of Japan Society of Information and Communication Research 22(2) (2004), 55-62.

[36] Seiji Tsugawa, An experimental study on the construction of the risk analysis model for the information security management of the local governments, Security Management No. 17, The Japan Society of Security Management, 2004.

[37] Seiji Tsugawa and Shoziro Kuroda, A study on the construction of the risk management cycle for the information assets of the local governments - In the experimental case of Hyogo Prefectural Government, The Journal of Japan Society of Information and Communication Research 22(2) (2004), 1-12.

[38] Seiji Tsugawa and Shoziro Kuroda, An experimental study on the construction of the risk analysis model for the information security management of the local governments - In the Experimental Case of the Information Security Audit of the Hyogo Prefectural Government, Japan Society of Security Management Magazine Vol. 17, 2004.