Consideration for Information Security Issues in Geospatial Information Services of Local Governments

*by Makoto Hanashima**

Abstract

Geographic Information System (GIS) is one of the important elements of the IT infrastructure of local governments. In recent years, in the consequence of development of Web-based GIS technology, the definition of GIS has been changing to “Geospatial Information Service”. For a local government, the geospatial information service is becoming an important IT system in the field of information service or in the field of information disclosure for its residents. Since all of the governmental geospatial information is public property, it should not only be utilized but be protected. However, there is no standard or guideline for the information security regarding the geospatial information service in Japan. Therefore, a study from the stance of IT security is required in order to secure the geospatial information service and to protect the geospatial information as public property. ISO/IEC TR 13335 GMITS that is one of ISO standards for the IT security management is a useful framework for discussing regarding IT security policy of an information service.

This paper aims to consider regarding IT security requirements for the geospatial information service and analyze the specific threats to them according to the framework of GMITS. Based on the threat analysis, a set of safeguards for the baseline security of the geospatial information service is selected. In addition, technical issues of the safeguards to clarify the feasibility of them are discussed.

Introduction

Geographic information system (GIS) is one of the important factors that constitute social IT infrastructure today. Furthermore, the system that carries out interoperability of the geospatial information data through the Internet is becoming feasible. In this situation, GIS has been changed to the terminology meaning geospatial information service.

GIS in local governments is the main application field of GIS. Introduction of GIS in Japanese local governments shows rapid progress ignited by the Kobe earthquake in 1995. According to a survey in 2004 by the National Spatial Data Infrastructure Promoting Association (NSDIPA), the introductory rate of GIS in the all-prefectures agency is 100%. Moreover, in 40% of the cities, towns and villages, GIS introduction has been completed.

The main purpose of GIS in local governments is management of geospatial information in regard of administration and decision support. In addition, utilization of GIS for information disclosure and the public information service has become important year by year. Since the distribution of the geospatial information service can contribute to the improvement of the welfare of residents, it is a desirable usage of public resource.

On the other hand, standardization of the specification of Web Map Service (WMS) has been carried out by Open Geospatial Consortium (OGC) Inc., and the technical infrastructure of geospatial information service has been developed year by year. Not only the service of conventional “End to End” but also the service chaining by combining two or more geospatial information services are becoming possible. It is expected that the circumstances of the geospatial information service in local governments also change a lot by such technology. In some local governments, the operation of “wide-area integrated GIS” which has multi-service interoperability of geospatial information has already started.

In such condition while a user’s convenience and the quality of service improve greatly, the possibility of information security problem also increases. The service that a local government provides must not threaten the residents’ safety. In order to prevent illegal usage of the geospatial information that is public property, the countermeasure based on suitable information security is indispensable. However, in Japan, those countermeasures are being entrusted to each local government.

Therefore, in consideration of the circumstances of geospatial information services of local governments, to discuss those requirements for the information security systematically is required

The meaning and the purpose of research

In order to make the information service on the Internet secure, many technologies and standards already exist and are used in various fields. Thus, it is possible to secure the geospatial information service by technology theoretically.

All the same, the question I have to consider here is whether or not to discuss about the information security of geospatial information service.

Generally, in order to implement suitable IT security management, it is necessary to define clearly IT security requirement peculiar to the system or field. Even if it is using the same Web-based system technology, a security requirement is not the same in a medical information system and in GIS. It will be very natural to set up a suitable and logical security requirement in consideration of the characteristics of each IT system. Nevertheless, I think that such discussion has not been fully held in the field of geospatial information service.

Probably, there may be an opinion that the discussion about the IT security requirements should be held at the process of system design of an actual system. Such opinion will be reasonable if it is from the stance focused on implementation. It will not matter if sufficient security in that approach is ensured. However, since such bottom-up approach is not necessarily systematic, in many cases, there is a risk of the defect of security requirements. Therefore, I need the systematic and logical discussion regarding the requirements for an information security of geospatial information service.

As a framework for discussing such issues, there are the information security related standards and guidelines of ISO. I think the most appropriate standard is ISO/IEC TR 13335 Guidelines for the Management of IT Security (GMITS). GMITS provides a systematic framework for IT security management. Being based on the concept of GMITS, we would like to clarify the meaning of discussing IT security of geospatial information service.

"The Part 4" of GMITS has described the selection process of the safeguard of IT system for threats. According to the description of that part, when setting up the security level in an IT system, there are two approaches.

One is the approach based on a "detailed risk analysis." A detailed risk analysis estimates risks based on detailed evaluation of the information property that is a target for protection, the threat evaluation to the information assets, and vulnerability evaluation of IT system. Therefore, it is possible to select the safeguard optimized to the target IT system. On the other hand, since this approach needs high-level technical knowledge and a great effort, it requires many resources. Thus, it is suitable for the system that needs an advanced information security. Oppositely, depending on the type of system, it may become surplus specification.

Another process is "baseline approach". Baseline approach selects a safeguard (baseline safeguard) so that the minimum-security level (baseline security) decided for each type of IT system may be satisfied. Because this approach can be implemented in minimum time and effort for a risk analysis or for selection of safeguards, for a system that does not need a high security level, its cost benefit is far good. Instead, this approach depends on the adequacy of baseline security. When the standard baseline security already verified in a system of the same kind does not exist, it cannot be implemented.

Actually, the peculiar baseline security guideline is already specified by a certain kind of application fields (medical service, financial information system, etc.). The application in such fields can implement a minimum safeguard without a detailed risk analysis. However, as far as I know, in Japan, such a guideline regarding geospatial information service of local governments does not exist.

The fact that there is no guideline of baseline security suggests that there can be three cases in the approach of IT security of geospatial information service of local governments.

Those cases are as follows

(1) It is based on the detailed risk analysis.

(2) It is based on informal approach.

(3) It is based on the baseline safeguard of other information service.

Since (1) requires high costs as I mentioned previously, it is difficult to carry out in a standard local government. Therefore, it is thought that (2) or (3) will mainly be chosen. In that case, following problems may arise by choosing these approaches.

a. When the interoperability of geospatial information service is carried out, complicated processing is required because of the differences in the security implementation between services.

b. Redundant investments to the security countermeasures that may not be so effective will continue in many local governments.

c. Some specific risks of geospatial information service may remain without consideration.

In order to prevent these problems, a systematic and logical discussion will be required regarding baseline security for geospatial information service. If the specific requirements for the information security of geospatial information service become clear, the guideline that contains these requirements in baseline security can be proposed. Even if there is no specific security requirement, certain criteria about baseline security should be shown.

From the above reasons, this research aims at contributing to the making of a practical guideline by discussing the baseline security of the geospatial information service in a local government, and proposing the prototype.

The workflow of research

In this research, the framework of GMITS is referred to, in order to discuss the baseline security of geospatial information service. Fig. 1 shows the relation between the framework of the security management of GMITS and this research.

As shown figure 1, the target of this research is a proposal of a baseline security guideline for the geospatial information service with consideration for the institutional restrictions of a local government and the actual condition of business environment in Japan. For that purpose, not only GMITS but also other standards may be applied. The reason for referring to these standards is to provide the systematic conceptual framework, but not to create the proposal based on a specific standard. (Of course, there is a possibility of designing a proposal based on the standard because of discussion.) Now, let us explain the workflow of our research.

A. Discussion of IT security policy regarding the geospatial information service

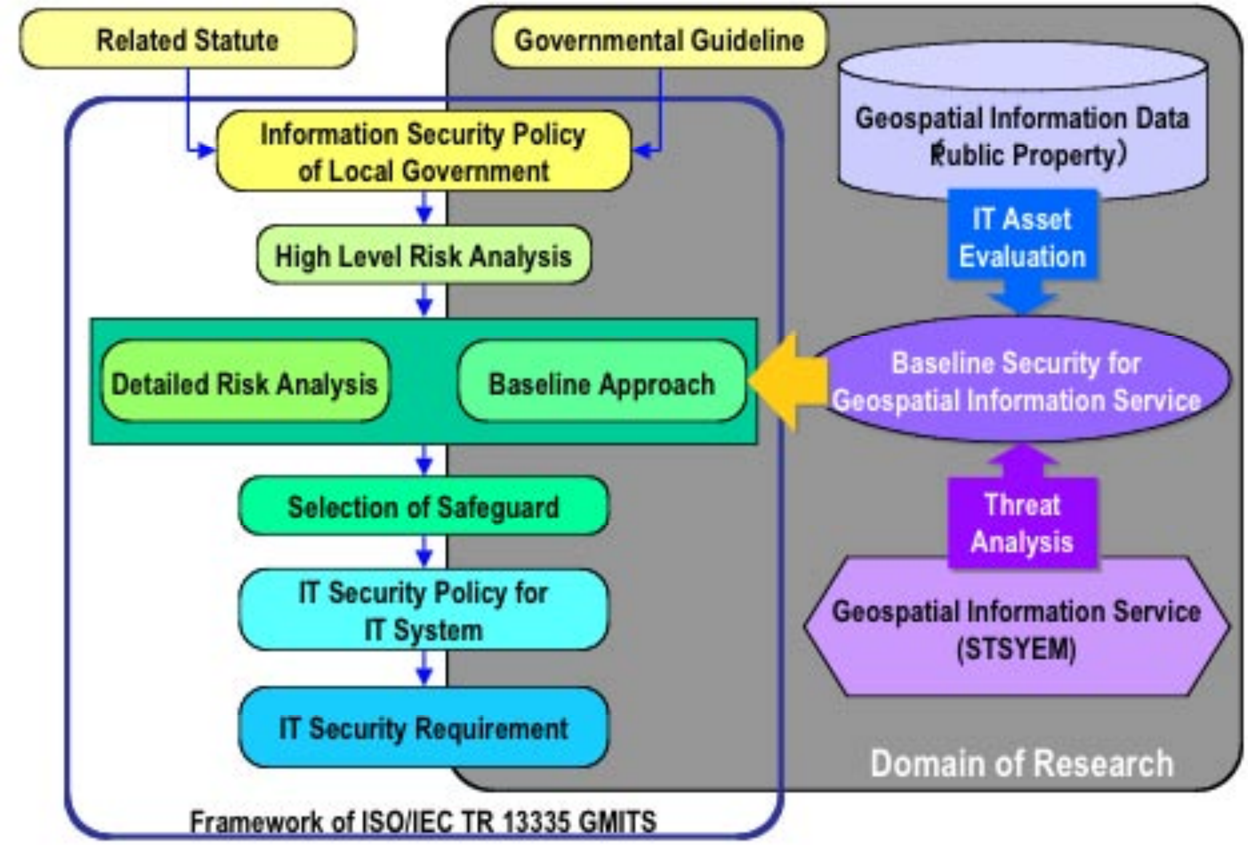
There are two levels of the security policy in IT security management.

A high-level IT security policy is for the whole organization, and the security policy of individual IT system is created based on it.

In this research, the security policy of the geospatial information service is discussed as one of the individual IT security policies, assuming that overall IT security policy of the local government is already created.

Based on the governmental guideline, I interpret the security issues regarding the distribution of the geospatial information, and extract the security requirement of an IT

figure 1


Related Statute
Governmental Guideline
Information Security Policy of Local Government
High Level Risk Analysis
Detailed Risk Analysis
Baseline Approach
Selection of Safeguard
IT Security Policy for IT System
IT Security Requirement
Framework of ISO/IEC TR 13335 GMITS
Geospatial Information Data (Public Property)
IT Asset Evaluation
Baseline Security for Geospatial Information Service
Threat Analysis
Geospatial Information Service (STSYEM)
Domain of Research

system.

B. Outline risk analysis

GMITS recommends evaluating the importance and influence of an IT system, before considering a detailed safeguard. (See Fig. 2) That process is called "Outline risk analysis". When the result of "Outline risk analysis" indicates that the requirements of IT security are high, a detailed risk analysis needs to be implemented. (For example, a national-defense information system, the system regarding high-energy waste, etc.) In that case, I do not need to discuss about that kind of system, since the IT security is implemented depending on the specification of the system.

On the other hand, when the result of "Outline risk analysis" shows that it is not necessary to implement detailed risk analysis, an appropriate baseline approach should be considered. Therefore, the process of "Outline risk analysis" should be clarified. The plan of this research is to build up a simple evaluation model of "Outline risk analysis" based on a minimum risk assessment for the geospatial information service in local governments.

C. Making of a safeguard catalog

The requirements for selecting the safeguard to risks of IT security become clear according to Process B.

By cataloguing systematically the safeguard that suits the requirements, it becomes easy to define IT security requirements.

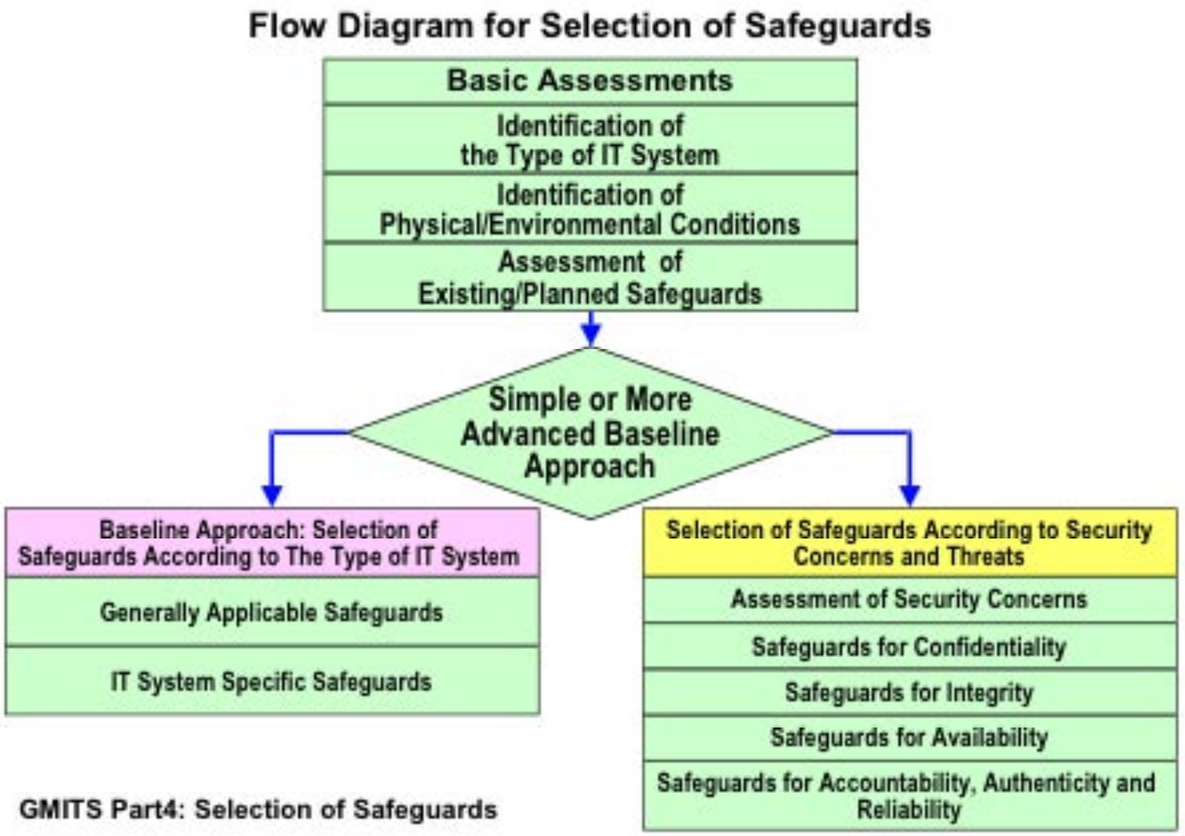
D. Making of a baseline security model for geospatial information service

On the basis of the safeguard catalog, a set of the safeguards is selected to construct a baseline security model for the geospatial information service. The baseline security model is defined in order to fill the security requirements of the geospatial information service.

E. Proposal of a baseline security guideline prototype

The last step of the research is to propose a baseline

figure 2


Flow Diagram for Selection of Safeguards
Basic Assessments
Identification of the Type of IT System
Identification of Physical/Environmental Conditions
Assessment of Existing/Planned Safeguards
Simple or More Advanced Baseline Approach
Baseline Approach: Selection of Safeguards According to The Type of IT System
Generally Applicable Safeguards
IT System Specific Safeguards
Selection of Safeguards According to Security Concerns and Threats
Assessment of Security Concerns
Safeguards for Confidentiality
Safeguards for Integrity
Safeguards for Availability
Safeguards for Accountability, Authenticity and Reliability
GMITS Part4: Selection of Safeguards

security guideline for local governments.

This paper shows the result of the discussion regarding the above-mentioned A and B. From now on, the research in this paper will be developed further and it is necessary to make it more practical. Future research is due to show the prototype of a guideline.

The security policy regarding geospatial information service

At present, there is no ordinance that refers concretely to the security policy of geospatial information service in Japan. The only document, "the Guideline regarding Distribution of Governmental Geographic Information", has been released by the "Related Ministry Liaison Conference for GIS" in 2003. This guideline is a de facto guideline of the geospatial information service by the public institution in Japan.

The most important point of this guideline is recognizing that the properties of geospatial information are different from those of other administration information. It also points out that the guideline is necessary in order to promote the distribution and disclosure of geospatial information. The main points of the guideline are summarized as follows.

(1) Governmental geospatial information is public property which all the people can enjoy conveniently. Therefore, it should not only be used inside an institution, but be positively provided for people.

(2) Although geospatial information is one of the administration information, smooth distribution may be unable to be promoted only by being based on the existing government ordinance, because of the specific properties of geospatial information. Those specific properties are as follows.

a. Since most of geospatial information is created by association of the work of various authors, the provider cannot avoid various rights management in regard of copyright.

b. In the case of almost all administration information, governmental duty is achieved by the disclosure of information, but for geospatial information it is important that a user can reproduce or process it after its distribution.

(3) Therefore, the guideline regarding information service based on the properties of geospatial information is necessary.

(4) The basic policy regarding the distribution of geospatial information that the government owns is defined as follows.

a. In principle, the government shall not set a restriction in usage of geospatial information that is distributed freely through the Internet as much as possible.

b. From a viewpoint of ensuring governmental accountability, whereabouts, distribution propriety, distribution process, distribution conditions, etc. shall be indicated on the Internet.

c. The government shall make sure that geospatial information may not correspond to the nondisclosure information defined by "Freedom of Information Act" of Japan as much as possible.

Furthermore, in 2004, the liaison conference released the "collection of Q&A" as the guide of actual operation. The handling of the copyright of governmental geospatial information and the interpretation of the government regarding the issues for actual operation are described in this "Q&A." In addition, this guideline describes, "Although judgment regarding geospatial information is fundamentally entrusted to a local government, it is possible to provide geographic information according to the distribution guideline."

When a local government considers its distribution of geospatial information, these two documents are considered to become a source of a basic security policy. Therefore, I will be able to extract the security policy requirements for geospatial information service of a local government from this guideline. The requirements are as follows.

A. Protection of geospatial information regarding privacy.

B. Ensuring confidentiality of nondisclosure geospatial information.

C. Ensuring integrity and authenticity of geospatial information.

D. Management of the access privilege of geospatial information.

E. Prevention from violation of the copyright of geospatial information.

F. Maintenance of accountability of local government for geospatial information.

G. Ensuring availability of geospatial information service.

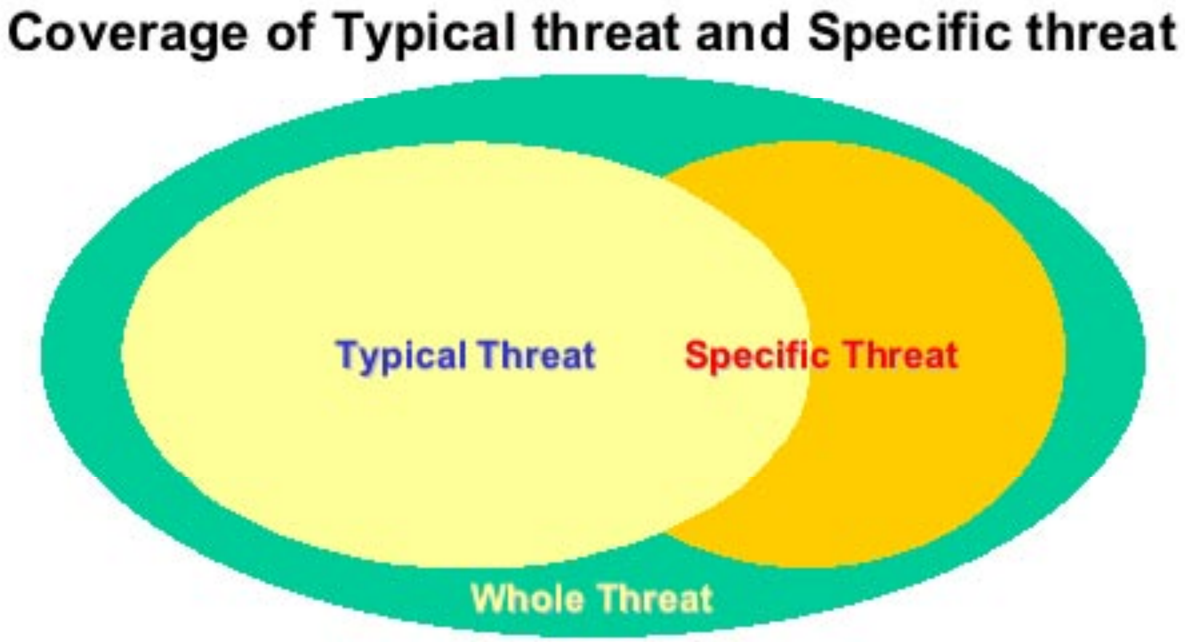
Threats and damages over geospatial information service

Next, I would like to consider the threats over these requirements, and the damage caused by them.

First, threats are divided into two classifications. One is “Typical Threat” that is enumerated in GMITS Part 3 Annex C “List of Possible Threat Types”. Another one is “Specific Threat” that is peculiar to the geospatial information service. “Typical Threat” and “Specific Threat” are not independent of each other. There is an intersection area as shown in Fig. 3.

In order to clarify actual risks, some “Typical Threat” should be redefined as “Specific Threat”. Based on our consideration about “Specific Threat” regarding GIS of local governments, I have enumerated them as follows.

figure 3



A. Protection of geospatial information regarding privacy

This requirement is endangered by leakage, theft, failure, loss, tampering, forgery, etc. of privacy information. The possible damages in this case are as follows.

a. Risk of infringing on individual (corporate) security and profits arises.

b. The legal liability based on a related statute is prosecuted.

c. The evaluation to administration falls.

d. The promotion of utilization of service is obstructed.

“Specific Threat” which causes such damages includes:

(1) Exposure of the privacy information by a connected referencability (A vulnerability that is able to guess the nondisclosure information in a certain database by indirect reference of the information in other databases.)

(2) Tampering and forgery of data

(3) Illegal copy of data

B. Ensuring the confidentiality of nondisclosure geospatial information

This requirement is endangered by leakage, theft, failure, tampering and forgery of nondisclosure information. The possible damages in this case are as follows.

a. The threat on the security by leakage of a social infrastructure or national-defense-related nondisclosure information is caused.

b. The threat to safety of residents is caused.

“Specific Threat” which causes such damages includes:

(1) Exposure of the nondisclosure information by a connected referencability

(2) Tampering and forgery of data

(3) Illegal copy of data

(4) Data error

C. Ensuring integrity and authenticity of geospatial information
This requirement is endangered by forgery, tampering and defect of geospatial information. The possible damages in this case are as follows.

a. There is a possibility that all of the services using the geospatial information will be influenced by the defect of information.

b. There is a risk that tampered digital map or geospatial information is abused as an official document.

c. Trouble or crime by the tampered geospatial information is caused.

d. The reliance on geospatial information falls.

«Specific Threat» which causes such damages includes:

(1) Tampering and forgery of data

(2) Illegal copy of data

(3) Data error

(4) Masquerading of a source

D. Management of the access privilege of geospatial information
This requirement is endangered by fraudulent procurement or setting error of the access privilege of geospatial information. The possible damages in this case are as follows.

a. The serious threat over the security of entire information system is caused.

b. The services that use geospatial information are disturbed.

c. The reliance on geospatial information service falls.

«Specific Threat» which causes such damages includes:

(1) Setting error of an access privilege

(2) The attack by unauthorized service

(3) The attack to Web application

E. Prevention from violation of the copyright of geospatial information
This requirement is endangered by violation or masquerade of copyright of geospatial information. The possible damages in this case are as follows.

a. Risk of infringing on the profits of an author or a user is caused.

b. The legal liability relevant to protection of copyright is prosecuted.

«Specific Threat» which causes such damages includes:

(1) Setting error of an access privilege

(2) Masquerading of an author or a source

(3) Tampering and forgery of data

(4) Illegal copy and distribution of data

F. Maintenance of accountability of local governments for geospatial information
This requirement is endangered by failure, disturbance, and loss and tampering of audit information. The possible damages in this case are as follows.

a. Risk of overlooking an information crime and the illegal use of information is caused.

b. Possibility that spoils the accountability of administration is caused.

c. The legal liability regarding business administration of local government is prosecuted.

«Specific Threat» which causes such damages includes:

(1) Tampering and deletion of an audit log

(2) Data error

(3) Setting error of an access privilege

(4) Tampering and forgery of data

(5) Illegal copy and distribution of data

G. Ensuring the availability of geospatial information service
This requirement is endangered by failure of system,

hardware, network, etc. The possible damages in this case are as follows.

a. It interferes with the correspondence in the time of disaster and emergency.

b. It becomes impossible to maintain the business continuity of a local government.

c. It has a bad influence on the service of other local governments.

d. The reliance on geospatial information service falls.

«Specific Threat» which causes such damage includes:

(1) Failure of interoperability between systems

(2) The attack by unauthorized service

(3) The attack to Web application

(4) Tampering and forgery of data

(5) Data error

6. "Specific Threat" to geospatial information service
Since «Typical Threat» has been described by GMITS, let us explain regarding «Specific Threat» concretely here.

(1) Tampering and forgery of data

It is difficult to distinguish the tampered geospatial information data. For example, when the polygon data of a land partition is changed or a non-existing block is forged, the first people that see the map are unable to detect the tampering with the geospatial data. The geospatial information data of a local government can be used as an official document, if the criterion is satisfied. Therefore, the general user will not suspect the authenticity of the map. When a tampered map data is provided from the GIS service of a local government, a very dangerous situation may be caused.

(2) Illegal copy and distribution of data

Although geospatial information data is public property, it cannot be necessarily reproduced unconditionally. Copyright is generated even if the geospatial information has been made by public institutions. Since the utilization conditions of geospatial data are sure to be specified by the government, all the reproductions that do not follow the conditions are illegal copies. When one map image is the result of editing a set of geospatial data, copyright exists for all the data. Therefore, in such reproduction of a map image, it is necessary to obtain agreement of all the copyright holders. If a large amount of the illegal copy that disregarded the utilization conditions is distributed, there is a possibility to cause the trouble of copyright infringement.

(3) The attack by unauthorized service

Interoperability technology realizes cooperation of several Web services, but it also enables malicious Web service attacks to GIS without a user's awareness. A Web service hijacked by the attacker can be injected with tampered geospatial information data which can execute damages to the service.

(4) The attack to Web application

Usually, a geospatial information service is implemented as a Web application. Although various measures are taken about IT security of a Web application, it is not easy to build a Web application without vulnerability. When a Web application is attacked, it causes execution of malicious codes, hijack of a system, tampering of a Web site, and so on.

(5) Masquerading of the author or the source

On the utilization conditions of geospatial information, the designation of the copyright holders or the source is required in many cases. However, when there is no way of attesting the authenticity of the author, a malicious third party may misrepresent the author, and the user cannot know it. It is not necessarily authentic information just because the copyright notice is indicated. Therefore, it is possible that copyright notice is abused in order to camouflage the information tampered by the third party.

(6) Setting error of the access privilege

Generally, geospatial information consists of the data of many features. In order to manage nondisclosure information, it is necessary to set up the access privilege of each feature, and it is thought that very complicated management is performed. If the setup of an access privilege has an error, it causes leakage of nondisclosure information immediately and causes various security problems.

(7) Exposure of confidential information by a connected referencability

Although geospatial information itself is not confidential information, a certain kind of geospatial information may expose confidential information, when it is used combining other information. A safeguard cannot be implemented individually in each case, since it is very difficult to detect and prevent a connected referencability. If the exposure of nondisclosure information occurs, there is a risk that a legal liability is prosecuted.

(8) Data error

It is very difficult to discover the error of geospatial information. Although a geometric check, a numerical check of attribute information and so on by a computer are possible, there are many errors undetectable with those checks. For the service that an independent local government provides, its influence will stop in that region, but when interoperability of geospatial information is being performed, there is a risk that erroneous data is diffused in many services.

(9) Tampering and deleting audit log information

The audit information, such as audit log files is indispensable, because accountability is an important requirement for a local government. When such audit information is lost or is tampered, a serious threat over the safety of the whole IT security is caused. Moreover, since accountability of a local government is lost, there is a risk that a legal liability is prosecuted.

(10) Failure of interoperability between systems

When geospatial information service is operating based on the interoperability of Web services, a failure of one service will affect other services immediately. For example, if the service that provides the background map stops, others cannot continue their services. Therefore, such failure of interoperability between systems is a serious threat to geospatial information service.

The safeguards to «Specific Threat»

Following consideration above, I discuss what kind of safeguard is applicable to each «Specific Threat». The results of the discussion are shown as follows.

(1) Tampering and forgery of data

a. The access control to data

b. Authentication of the authenticity of the data based on digital signature

c. Tampering-proof data generation

(2) An illegal copy and distribution of data

a. Authentication of the authenticity of the data based on digital signature.

b. Authentication of the data provider by digital signature

(3) The attack by an unauthorized service

a. Mutual authentication by the security framework of a Web service

b. Mutual authentication in an application level

c. Reinforcement of the detection function of an unauthorized service

(4) The attack to a Web application

a. Reinforcement of robustness of a Web application

b. Reinforcement of attack detection function

c. Using rich client

(5) Masquerading of an author or a source

a. Authentication by digital signature of an author or a source

b. Using digital watermarking

(6) Setting error of an access privilege

a. Application of an access-control model

b. Using an access-control framework

(7) Exposure of the confidential information by a connected referencability.

a. The limitation of the resolution by metadata

(8) Data error

a. Early distribution of error information

b. Audit of the updating log of data

(9) Tampering and deletion of an audit log information

a. Reinforcement of a logging system

(10) The failure of Interoperability between systems

a. Implementation of the error-tracking function of a Web service

Summary of the safeguards

The above-mentioned list of safeguards includes those whose feasibility has not been examined. That is, they can be sorted into the following two categories.

A. The safeguards that can be implemented by existing technologies

(1) Implementation of WS-Security technology

Web service-related safeguards are almost feasible by applying the technology of WS-Security in which standardization is promoted by Organization for the Advancement of Structured Information Standards (OASIS).

(2) Application of a secure data transmission protocol

Regarding the data transmission of «End to End», it is secured by using Secure Sockets Layer (SSL). However, in the case of the data transmission over more than one service, other technique is required.

(3) Application of an access model

Based on access models, such as Role Based Access Control (RBAC) model, the access control that is able to ensure consistency of the whole system is feasible.

B. The safeguards that need further discussion

(1) Improvement in the robustness of a Web application

Since it is depending on the implementation of an individual service, the systematic process that defends the attack on Web applications has not been established yet.

The discussion regarding construction of a robust Web application system should cover not only the software skill but also the aspect of operation.

(2) Realization of the traceability of a Web service component

If the interoperability between Web services becomes complicated, it will be difficult to detect the failure of a Web component. The function to trace the Web service that is malfunctioning in a service chain and to perform suitable failure processing is necessary.

(3) Implementation of the digital signature and authentication protocol in the Open Geospacial Consortium (OGC)'s open architecture.

There is no description regarding security in the open architecture specification of OGC, such as Web Map Service. How to implement security requirements is depending on each application system. However, regarding a signature and authentication of geospatial data, I consider that it will be more suitable to build in the framework of GIS technology. Thus, more technological consideration is required about this issue.

As mentioned above, regarding the safeguard to «Specific Threat», a continuous discussion is necessary.

Conclusion

In this paper, I clarify meaning of discussing IT security of the geospatial information service in local governments at the first, and then specified the workflow of research.

Then, I consider regarding the framework of baseline security for geospatial information service of local governments, and suggest that the baseline approach of GIMITS was an appropriate framework.

Furthermore, based on the governmental guideline, I show the IT security requirements for geospatial information service of local governments, and discuss regarding the threat over those security requirements.

Finally, I enumerate the possible safeguards to «Specific Threat» of geospatial information service, and consider regarding their technical issues.

Although this paper is the first step in my research, I think that I can show the meaning and the importance of the baseline security of geospatial information service.

From now on, the following issues will be discussed in the research.

(1) A conceptual model for «Outline Risk Analysis»

(2) Revalidation of «Specific Threat»

(3) Verification of safeguards against «Specific Threat»

(4) Abstract specification of the baseline-safeguards for geospatial information

Since it is thought that the image of a specific system is required to progress the discussion, I am going to define the geospatial information service as a virtual workbench. Further consideration regarding the safeguards for «Specific Threat» of GIS will be carried out with the virtual workbench.

References

Belussi,A,et al. “An Authorization Model for Geographical Maps” In Proc. GIS’04. Nov. 12-13. 2004.

Downs,R & Lenhardt,C. “Privacy and Confidentiality Issues with Spatial Data” IASSIST 2003.

ISO. “Geographic information Web map server interface”

ISO/DIS 19128. 2004.

ISO. "ISO/IEC TR 13335 Guideline for the management of IT Security" JIS Handbook 2005: 74-415.

ISO. "ISO/IEC15408:2005 Common Criteria for Information Technology Security Evaluation Version 2.3" ISO. 2005.

IT Strategy Committee. "e-Japan StrategyII" Ministry of Internal Affairs and Communications (MIC). Japan. 2003. http://www.kantei.go.jp/jp/singi/it2/

Japan Standards Association. "JIS Handbook – Information Security 2005" Japan Standards Association. 2005

Joshi,J, et al. "Digital Government Security Infrastructure Design Challenges" IEEE Computer. 2001.

Ministry of Internal Affairs and Communications. "Manual for Implemetation and Operation of Integrated GIS" 2004.

NSDIPA. "Annual Survey of GIS in Local Governments" http://www.gisportal.jp/case/lo_case/h16.html

OASIS. "WSS SOAP Message Security (WS-Security 2004)" OASIS Open. 2004.

OASIS. "XACML Profile for Role Based Access Control (RBAC)" Committee Draft 01. OASIS Open. Feb. 2004.

OGC. " OpenGIS Reference Model" OGC 03-040. Open Geospatial Consortium Inc. 2003.

OGC. "OpenGIS Web Map Server Cookbook" OGC 03-050r1. Open Geospatial Consortium Inc. 2004.

Related Ministry Liaison Conference for GIS. "Q & A: The Guideline regarding Distribution of Governmental Geographic Information" 2004.

Related Ministry Liaison Conference for GIS. "The Guideline regarding Distribution of Governmental Geographic Information" 2003.

Taylor,K & Murty,J. "Implementing Role Based Access Control for Federated Information Systems on the Web" Australasian Information Security Workshop 2003 (AISW2003)

Watanabe, Kozo. "Practical guide for Integrated GIS in Local Government" Nikkan Kogyo Shimbun Inc. 2003.

* Makoto Hanashima is a Senior Researcher at the Institute for Areal Studies, Foundation (IAS), Tokyo and the Institute of Information Security (IISEC), Yokohama. Email: mhana@ias.or.jp. The paper was presented at the IASSIST 2006 conference in Ann Arbor, Michigan, USA in the session, «The Big Picture: GIS Data Challenges and Solutions».