Business Content Security: Present Issues and Future Outlook for Its Employment

SHIMAZU Hideo

Abstract

In daily business work site, a huge amount of electronic documents are produced, stored in server computers or personal computers, and distributed. These documents contain a large number of highly confidential information. Unfortunately, these documents are not managed safely enough so that the risk of a possible leakage of confidential information has been tending to increase. This paper introduces 'Content security' which has the architecture of "an electronic document protects itself by itself." By introducing the concept of content security, the information protection architecture designed to prevent information leakage of electronic documents will be enhanced.

Keywords

electronic document, information leakage, Content security, digital rights management

1. Introduction

The day to day business environment processes a huge number of electronic documents that are stored in server and personal computers as well as being circulated. These documents contain a large amount of highly confidential information, like for example, spreadsheet data files that contain price lists of pre-marketed products, word processor files containing personal affairs information, PR presentation files that are not yet in the public domain and emails containing confidential information such as tie-up agreements with other companies, etc. Because such data and files are not always managed with optimum safety, it results as a consequence in an increased risk of confidential information leakages.

This paper introduces a content security that features "an electronic document protects itself by itself" concept. By introducing content security, the protection ability against information leakage of electronic documents will be enhanced.

2. Three-tier Information Security Model

The evolution of information security can be explained in three stages as described in **Fig. 1**. The first stage was the so-called 'Zone security.' A security wall surrounded entire company systems and strictly controlled the gates of the wall so that the data and machines inside the wall were supposedly all safe. The representative architecture for this kind of security system is a firewall. In those days, desktop PCs were the main

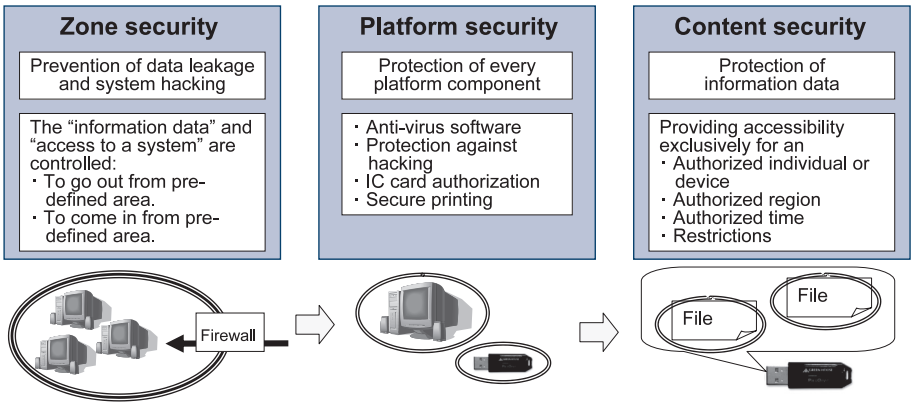

Fig. 1 The three security stages of protection domains.

stream in the business field and it hardly happened that PCs were taken out or brought in from outside companies. Therefore, architectures such as zone security were considered to be safe enough to protect the prevailing environment of information security.

As time passed, laptop PCs became the main stream in the market at the same time as a widespread and accelerated use of emailing and USB memories occurred. Zone security was no longer able to ensure satisfactory information security. Subsequently, various security systems have been introduced into the market that secure information security by protecting individual hardware including PC servers, network devices, USB memories, etc. For example, a personal firewall was mounted onto PCs, entire hard disks were encrypted, and anti-virus software was installed for file systems. Additionally, exclusive software was installed for the mail client software to check whether any spyware was contained in the transmitted data. The entire PC system was protected like a fortress by installing various countermeasure devices. At the same time, USB memories were protected by fingerprinting or password authentication devices and such USB memories were marketed one after another. This was the second stage of the information security evolution and the concept became known as 'Platform security.'

However, the accidents and troubles of information security could not be eliminated although much these security devices were installed. One of the reasons why this security architecture failed was the difficulty of achieving a complete implementation of security protection for the entire hardware component. Recently, commoditization and versatility of hardware devices have been greatly accelerated and many varieties of hardware devices are widely spread in the market so that it is almost impossible to carry out security protection countermeasures for the entire hardware arsenal of a company. Even if a single hardware component device avoids the security countermeasures, vital information may be leaked from it.

Information security could be strengthened if more security systems or more different types of security systems are installed at gateways in the zone or check points of the hardware. However, the more check points that are installed, the more complicated the management of information systems becomes. Moreover, such complicated system management could degrade the performance of the information systems. Even if more check points are installed, it follows that there are still chances of information leakage risks from the intervals between the check points. In support of this environment, the concept of "an electronic document that protects itself by itself" architecture has evolved. An information security technique based on this concept is that of 'Content security.'

By observing the changes in information security methods, it is shown that targets to be protected have focused on smaller and smaller units; from a whole information system inside a firewall at Zone security, to individual hardware devices at Platform security, then into each individual electronic documents stored in hardware devices at Content security.

3. Issues Involving the Usage and Security Management of Electronic Documents inside a Company

This section examines the issues of security management by observing how electronic documents are processed inside a company.

(1) Attribute Management of Electronic Documents

Various attributes are allocated to electronic documents and it is essential to check if these are being correctly assigned. Who and what type of authentication should be permitted to execute what kind of operation (referring data, editing data, printing, duplication, etc.). Also their date validity should be checked. However, it is difficult to manage all of these items manually. It is essential to establish a mechanism to manage and inspect such attributes automatically by computers.

(2) Ownership Management of Electronic Documents

An employee who creates an electronic document will be its owner at that time. However, if the electronic document contains details relating to a department or a specific project, it should belong to that department or project and the attribute of the electronic document should be provided according to the rules decided by the department or project and not by an individual who creates the document. For example, when a specification sheet of non-marketed products is created, it should be circulated inside the related project team and should not be disclosed to other project teams or departments, even if they are established within the same company.

(3) The Management of Electronic Documents Other than Those in File Format

Among the electronic documents in systems installed inside a company, database records and email texts are just as important as the file format data. If any of the records from the database are used to create spreadsheets or text files, the risk of information leakage will increase because none of the security protection countermeasures are provided for the created files. Therefore, an effective electronic documents information security protection methodology is required in order to avoid such a risk.

When considering email transmission, information leakage occurs when an email containing confidential information is dispatched to unpredicted email receivers and the email details are read by the wrong person(s). To prevent this happening, it is necessary to encrypt the email text temporarily in order to protect it from information leakage.

4. Content Security Architectures

The issues in security management described in Section 3 can be solved by 1) identifying the attribute and affiliation of electronic documents, and 2) introducing a suitable content security architecture that functions such that the electronic document is enabled to protect itself. The architecture of the content security has three features; content rights management, attribute management and distribution management.

(1) Content Rights Management

The basic mechanism for performing content rights management is that used by the DRM (Digital Rights Management). The DRM mechanism was developed and has been spreading in the market as a system that deals with paid internet content such as video and music files that carry a small charge. This system can also be employed to perform the internal electronic documents management of a company.

DRM architecture is illustrated in **Fig. 2**. When a new electronic document is created, the creator applies the registration of the license to the DRM server. This license pre-defines; method of use, distribution rights and attribute information. When the registration is applied, the DRM server encrypts the electronic document together with the attribute information.

This encryption process is called encapsulation. Once the data is encapsulated, its distribution is allowed to be carried out freely. A user who wants to use an encrypted electronic document applies a user license to the DRM server. When the DRM server authenticates the user's right of use, the license ticket defines several attributions and restrictions in distribution such as the number of times it is available for use, permission to copy or not, etc. Users can only decrypt electronic documents under these conditions. The license ticket is protected from being copied in order to avoid its being used by someone without an authorization to use the electronic document. For some electronic documents, a license ticket is not allowed to be distributed. In such a case a user has to apply the user license to the DRM server every time he/she wants to use it.

By managing electronic documents using DRM architecture, the encapsulated files cannot be decrypted without acquiring authentication or a user license ticket from the DRM server. This constraint also applies at a location where leaked information is received. Therefore, even if any information is leaked, the content of the encapsulated file will not be deciphered.

(2) Content Attribute Management

The various rules are regulated by a department or a project

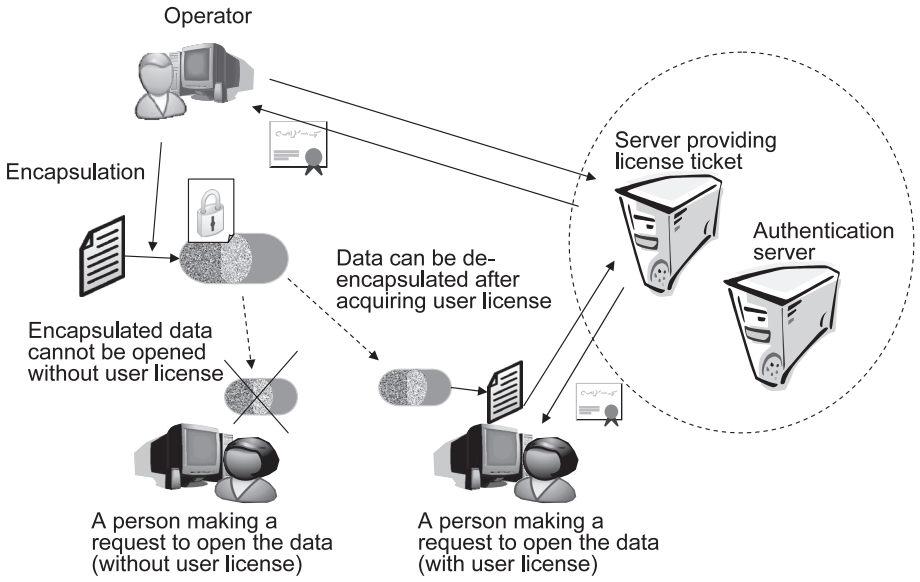

Fig. 2 Architecture of DRM (Digital Rights Management).

team and the rules are provided to the electronic documents as attributes. Attributes details are; 1) a list of the department or project team members and the rights and restrictions of individuals in operating electronic documents such as editing permitted/prohibited and duplicating permitted/prohibited, 2) a list of hardware devices including PCs, common file servers, etc. to be operated by the department or the project, and 3) allocation management that decides which devices should store the electronic documents. The functions to control these attributes details are essential for the DRM management to manage highly confidential electronic documents with the highest levels of security.

(3) Content Distribution Management

Once an electronic document is encapsulated and managed with the DRM system, even in the context of how the document is distributed, it cannot be decoded into an ordinary file unless the person attempting to do so has a legitimate right. This means that there is no distribution management necessary at all inside the infrastructure of the same DRM architecture. However, it is difficult to utilize the benefits of this DRM architecture when an electronic document is expected to be distributed to other types of DRM infrastructures. In the case that an electronic document is distributed to different types of DRM infrastructures, the encapsulated electronic document file must be de-encapsulated temporarily in order to unlock the security protection. It will then have to be protected by the security method that is adopted at the side of the DRM architecture where the file is transmitted before it is distributed on the receiver's side infrastructure. The convenience of operating a distribution management system is a very important factor in promoting the diffusion of the DRM architecture among companies.

5. Content Security Examples

This section introduces case studies to explain the functions of the DRM architecture. The content rights management is explained by introducing a case in which Microsoft Windows Rights Management Services (RMS) is employed. The content attribution management is described by using as an example, the InfoCage/File Series, which is NEC's information leakage protection software.

(1) Rights Management with RMS

RMS is the information protection middleware running on Windows Server 2003, which provides the basic configuration for DRM. It is necessary to install an RMS server for license management and an Active Directory server for user ID management. A user can encapsulate data files created in Microsoft Office 2003 even while working on a file, because Microsoft Office 2003 collaborates with the RMS server directly.

When a user tries to read a file encrypted with RMS, the application software on which the user is working links to the RMS server directly. The RMS server automatically confirms the user license authentication of the encapsulated file in order to allow the user to start working on the file. Therefore, a user can work on electronic documents without being aware that the file is encrypted with RMS.

(2) Attribution Management with the InfoCage/File Series

The InfoCage File series enables encapsulation of any type of file. However, it does not incorporate application software that links directly to a DRM server, as in the cooperative relationship between Microsoft Office 2003 and RMS. The features of the InfoCage File series are automatic patrol in specified file folders and integrated management functions based on the defined security policies.

With RMS, a person creating a file has to encrypt it every time that it is created. This means that someone creating a file must always be sure to encrypt the file, however, this procedure might sometimes be forgotten. On the other hand, with the InfoCage File series, if a user designates specific file folders, an agent program of the InfoCage File series patrols these file folders regularly and encrypts the files automatically when it finds any files that are not encrypted. **(Fig.3)** This results in a decrease in the risk of information leakage happening due to a user's carelessness in not encrypting a

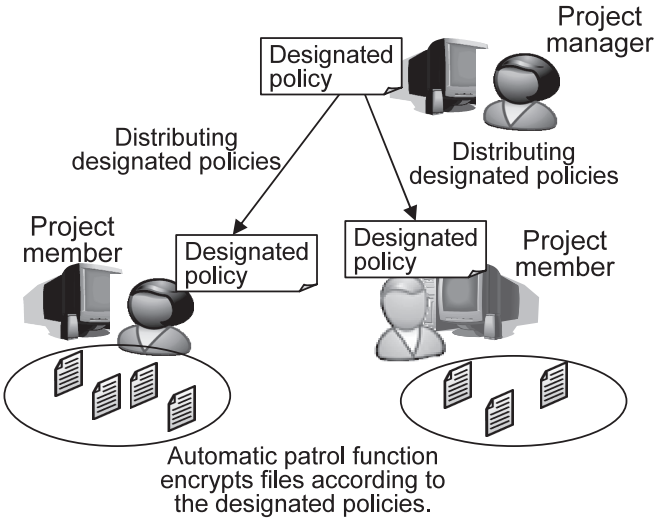

Fig. 3 InfoCage File series.

file. For example, when a user creates a spreadsheet data file by using a part of the database and stores it in a folder that the agent program patrols, the agent program automatically encrypts the files even if a user forgets to encrypt them. Designated policies such as the automatic patrol function and automatic file encapsulation, etc. can be defined for each department or project. These policies are distributed to the members automatically so that unified management inside the department or the project is easily available.

6. Conclusion – Future Development –

This paper introduces the need for content security and its architecture. Content security offers an effective countermeasure against information leakage. However, the products that are currently available on the market are not capable of performing all of the functions required to provide a fully effective content security environment. One of the issues to be resolved in the future is the need for an optimum distribution method to enable the transmission of electronic documents between companies that employ different authentication systems or DRM architectures. We are expecting to be able to market products that are capable of achieving effective content security during the course of our work on the resolution of such issues.

---

*The corporate and product names mentioned in this paper are trademarks or registered trademarks of their respective owners.

Author's Profile

SHIMAZU Hideo
General Manager,
System Technologies Laboratory,
NEC System Technologies, Ltd.