Enterprise Data Loss Prevention System Having a Function of Coping with Civil Suits*

Youngsoo Kim, Namje Park**, and Dowon Hong

Summary. More and more enterprises and organizations are adopting Data Loss Prevention (DLP) systems to detect and prevent the unauthorized use and transmission of their confidential information. Usually, DLP systems identify, monitor, and protect data in use, data in motion, and data at rest through deep content inspection, contextual security analysis of transaction and with a centralized management framework. Electronic documents, e-mails or network logs that are produced within enterprise, can be included in enterprise's confidential information. On the other hand, as ESI is included in extent of evidence that become discovery's target in FRCP taken effect on December 1, 2006, enterprises been always vexing in several litigations are hurrying to adopt systematic ESI administration and confrontation system to prevent a lawsuit from losing owing to failure in duty of presenting related evidences and to maintain their confidences. This paper is about enterprise DLP system having a function of coping with civil suits. We loaded various functions needed at discovery process of civil suit to conventional enterprise DLP system. The proposed system can reduce enterprise's damage by coping spontaneously about enterprise's litigation dispute.

1 Introduction

More and more enterprises and organizations are adopting Data Loss Prevention (DLP) systems to detect and prevent the unauthorized use and transmission of their confidential information. Usually, DLP systems identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions),

Youngsoo Kim · Dowon Hong
Cryptography Research Team, Electronics & Telecommunications Research Institute
138 GaJeong-no, YuSeong-Gu, Daejeon, 305-700, Korea
e-mail: {blitzkrieg,dwhong}@etri.re.kr

Namje Park
Department of Computer Education, Teachers College, Jeju National University
61 Iljudong-ro, Jeju-si, Jeju-do, 690-781, Korea
e-mail: namjepark@jejunu.ac.kr

* This work was supported by the IT R&D program of MKE/KEIT[10035157, Development of Digital Forensic Technologies for Real-Time Analysis].

** Corresponding author.

R. Lee (Ed.): Computers, Networks, Systems, & Industrial Eng. 2011, SCI 365, pp. 201–208.
springerlink.com

and data at rest (e.g., data storage) through deep content inspection, contextual security analysis of transaction and with a centralized management framework[1]. Electronic documents, e-mails or network logs that are produced within enterprise, can be included in enterprise's confidential information.

On the other hand, as ESI (Electronically Stored Information) is included in extent of evidence that become discovery's target in FRCP taken effect on December 1, 2006, enterprises been always vexing in several litigations are hurrying to adopt systematic ESI administration and confrontation system to prevent a lawsuit from losing owing to failure in duty of presenting related evidences and to maintain their confidences[2].

FRCP (Federal Rules of Civil Procedure) has a procedure of asking an opposing part to open related evidences and information through discovery[3]. A litigant opens and collects information and evidences to clarify a point at issue of litigation, by legal method out of court in order to prepare trial. By asking each other to open an opposing party's evidences, documents, and witnesses, it can help litigants proceed this lawsuit under the same condition.

Litigants should open all evidences they have by themselves prior to trial and can request the other party or the third party to make public theirs at the same time[4]. The purpose of this requesting procedure for opening evidences is to make clear a point at issue of suit and secure all evidences which might be hidden purposely on trial, and there are a lot of cases that compromise is achieved prior to trial because each party knows about the other party's evidences in detail. Discovery is made in writing such as a written request, a written answer, or a written protest and all documents need a lawyer's signature. This process is fulfilled between litigants without a court's participation. However, if a dispute occurs which a litigant rejects requests of the other litigant, a court participates in it. If litigants make excessive or expensive discovery requests on purpose, a court can revoke them, conversely, they do not their duty of discovery in good faith, a court can imposes mandatory sanctions.

As ESI is included in extent of evidence that become discovery's target in FRCP taken effect on December 1, 2006, terminology named e-Discovery was appeared[5]. Enterprises been always vexing in several litigations are hurrying to adopt systematic ESI administration and confrontation system to prevent a lawsuit from losing owing to failure in duty of presenting related evidences and to maintain their confidences[6].

To satisfy this enterprise's necessity, some tools and solutions that can shorten litigation costs and time radically having various automated functions that is necessary in e-Discovery process are released. However, it can be very inefficient that enterprises which already have their own e-mail and documents management system or information protection solution additionally adopt these tools and solutions, the price increases greatly according to enterprise's scale.

In this paper, we propose an efficient system having a function of integrated security and a function of coping with civil procedure simultaneously that loads new functions needed at discovery process of civil suit to conventional enterprise DLP system.

It includes functions of information management, identification, preservation, collection, processing, analysis, review, production, and presentation of EDRM