보안 문서의 보안 수준 변환을 위한 기법 연구

A Study of Security Level Conversion Scheme for Security Documents

조도은*, 여상수**

Do-Eun Cho*, Sang-Soo Yeo**

요 약

현재의 정보화 사회에서는 정보의 가치는 매우 높아졌으며, 정보를 획득, 관리, 사용하는 것에 대한 많은 연구 개발이 이루어지고 있다. 특정 기업(또는 기관)에서는 기업 내의 정보가 담긴 문서들의 보안 레벨을 엄격하게 규정하고 이에 대한 보안을 철저히 지키고 있다. 본 논문에서는, 상위 보안 레벨의 보안 문서를 하위 보안 레벨로 변환할 경우를 위해, 효과적으로 문서를 검열하고 특정 보안 키워드를 일반적인 단어로 변경하는데 필요한 요소 기술에 대해 소개한다.

Abstract

The value of information becomes very high, a large number of research works has been made for acquiring, managing, and using information. In a specific company (or organization), they are classifying company data documents with managed security levels, and they are securing their secured documents. In this paper, we introduce essential technologies enabling to inspect documents securely and to change specific keywords to normal words, in case that a higher security level document should be converted to a lower security level document.

Key words : security, database , word search, inspect

I. 서 론

정보화 사회에서는 정보가 가치를 가지고, 정보의 획득이 재화의 획득과 동일한 수준의 가치를 지니게 된다. 이러한 정보화 사회에서는 기업의 가치 또한 기업이 소유하고 있는 배타적인 정보에 의해서 평가되어 질 수 있으며, 실제로 기업 내의 비밀 정보들의 유출은 기업의 존폐와도 직결될 수 있는 매우 큰 문제로 인식되고 있다[1].

예전부터 많은 산업 스파이들이 경쟁사에서 중요 정보를 획득하여 자사의 입지를 굳건히 해 왔으며, 이는 특정 국가에서 이루어지지 않고 국경을 초월한 산업 정보 스파이들의 활동으로 인해 더욱 심화되고 있는 상황으로 보여진다. 따라서 기업은 데이터의 보호 및 안전한 접근을 위한 시스템을 갖추어야 한다[2]. 기업의 핵심정보 보호를 위하여 사용자를 분류하고 등급화 하여야 하며, 데이터의 중요도에 따라 사용자 접근을 제어하고 접근 권한에 따른 제어를 통

* 목원대학교 공학교육혁신센터(Innovation Center for Engineering Education, Mokwon University)
** 목원대학교 컴퓨터공학부(Division of Computer Engineering, Mokwon University)
· 제1저자 (First Author) : 조도은 · 교신저자 (Corresponding Author) : 여상수
· 투고일자 : 2011년 4월 12일
· 심사(수정)일자 : 2011년 4월 12일 (수정일자 : 2011년 6월 8일)
· 게재일자 : 2011년 6월 30일

해 기업의 핵심정보를 보호 할 수 있는 보안 솔루션이 필요하다. 이로 인해서, 각 기업들은 기업의 정보 자산을 효과적으로 관리할 필요성을 매우 실감하고, 여러 가지 보안 솔루션을 도입하고 있다. 이러한 보안 솔루션의 기본은 문서 보안 및 접근 제어가 된다. 더욱 깊이 들어가게 되면 특정 문서에는 보안 레벨 및 접근 가능자(가능 보안 그룹)들에 대한 정보가 입력되어 있으며, 이를 기반으로 이 문서를 열람 또는 변경할 수 있는 사람들이 정해지게 된다. 이러한 솔루션은 매우 다양하며, 동일한 솔루션을 적용하는 기업일지라도 이에 대한 적용 방식은 매우 다양하다고 할 수 있다.

본 논문에서는 특정 기업에서 보안 문서의 보안 수준을 변환할 경우 효과적으로 문서를 검열하고, 특정 보안 키워드를 일반적인 단어로 변경하는 자동화된 보안 수준 변환 기법과 요소기술을 소개하고자 한다.

이를 위해서는 기업 내에 문서 보안 레벨이 존재하며, 특정 문서 보안 솔루션이 존재하는 경우를 가정한다. 또한 이러한 가정 하에서 상위 보안 레벨의 문서가 하위 보안 레벨의 문서로 변경되어야 하는 경우가 있다는 것을 가정한다. 예를 들자면, 그림 1에 설명된 것과 같이 기업 내부 개발팀의 특정 상품 개발 보고서를 기업 홍보실에 보내고자 할 때, 기업의 핵심 기술 및 민감한 정보들을 검열하여 이들을 민감하지 않은 일반적인 정보로 대체하는 것이 필요할 것이다.

이와 같은 경우는 물론 상품 개발팀 쪽의 특정 직원에 의해서 수작업으로 이루어질 수도 있을 것이지만, 자동화를 통한 안전성 및 작업 능률 향상을 하는 것이 결국은 기업의 정보 관리 체계 유지에 더욱 도움이 될 것이다.

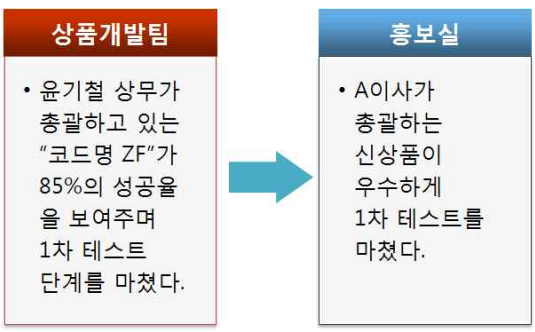

그림 1. 문서의 보안 레벨을 변경하는 경우의 예
Fig. 1. Example of security level change of a document

이러한 자동화된 문서 검열 및 보안 레벨의 변경은 정보 보안 키워드가 입력되어 있는 데이터베이스(키워드 DB, DB-K)와의 연동을 통해서 이루어지며, 이에 대한 자세한 설정은 보안 레벨 변경 규칙이 저장된 데이터베이스(규칙 DB, DB-R)의 통제를 받으며 이루어진다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로서 자동화된 문서 검열, 보안에 필요한 기술 및 환경에 관해 설명하고, 3장에서는 본 논문에서 제안하는 자동화된 문서 검열 및 보안 레벨 변경 기법에 필요한 요소기술들에 대해 기술한다. 4장에서는 3장에서 제시한 기법의 구현시 고려사항에 대하여 설명하고, 끝으로 5장에서는 결론과 향후 연구 계획에 대하여 언급한다.

Ⅱ. 관련 연구

2-1 XML 기반의 문서 관리

자동화된 문서 관리를 위해서는 문서의 형식이 정형화되어 있으며, 자동으로 판독 및 처리가 가능한 것이 매우 중요하다. 일반적인 문서 편집 소프트웨어에 의해 작성된 문서는 보안 관점에서 쉽게 판독 및 처리되기가 힘들기 때문에, 대부분의 경우 일정한 템플릿을 가지는 문서 형식을 만들고 이를 이용하게 된다. 그 가운데서 가장 효과적이며 범용적이라고 볼 수 있는 것이 XML(Extensible Markup Language)기반 문서이다[3].

XML은 DTD(Document Type Definition)를 통하여 문서의 구조를 정의하고, 정의된 구조에 따라서 문서를 작성해야 유효한 문서가 된다. 유효한 XML문서를 작성하기 위해서는 DTD구조를 정확히 이해하고, 시작 태그와 끝 태그를 반드시 기술하여야 하는 등의 정형화된 규칙에 따라야 한다[4]. 이러한 XML을 기반으로 한 문서의 효과적인 관리에 대한 연구가 활발하게 진행 중이다. 세그먼트 기반의 XML 문서 필터링과 NFA 표현을 사용한 문서 중심적 XML의 키워드 기반 필터링 기법이 그 대표적인 예라고 할 수 있다.

세그먼트 기반의 XML 문서 필터링 기법[5]은 가지형 패턴들에서 공유 가능한 세그먼트를 판별한 후 중복된 세그먼트 중 하나만 색인하여 시스템에 적용하여 필터링 과정에서 중복된 처리를 없앨 수 있다.가지형 패턴의 사용자 프로파일에서 세그먼트를 추출하여 해시 기반의 세그먼트 테이블에 저장하고 유지한다. 이 세그먼트는 사용자 프로파일을 터스 시퀀스 형태로 표현하는데 이용되고, 효율적인 필터링을 위한 콤팩트 시퀀스 인덱스에도 사용된다.

그림 2는 XML 문서가 순서를 가진 레이블된 트리로 표현된 것을 나타낸 것이다. 트리에 있는 각각의 노드는 XML 문서의 엘리먼트나 값(value)에 해당한다.

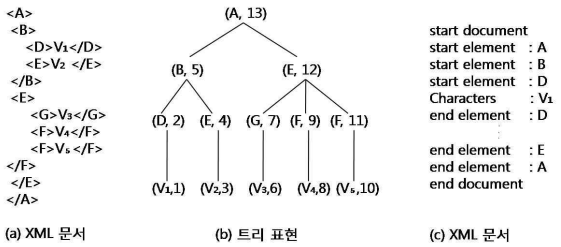

그림 2. 시퀀스 샘플 XML 문서[5]
Fig. 2. XML document of the sequence sample[5]

NFA 표현을 사용한 문서 중심적 XML의 키워드 기반 필터링 기법[6]은 확장된 XPath 명세와 그것을 표준 질의어로 사용하는 문서-중심적 XML 필터링 기법인 Pfilter를 제안한다. Pfilter는 값-기반 술어에서 피연산자의 공통 앞부분 문자를 공유하여 값-기반 술어의 처리 성능을 향상시킨다. 그림 3은 값-기반 술어 NFA의 조각을 나타내며, 그림 4는 값-기반 술어 NFA를 해시 테이블 기반으로 구현한 모습을 나타낸 것이다. 각 해시 테이블에 할당된 숫자는 상태번호를 나타내며 굵은 사각형은 승인 상태를 의미한다.

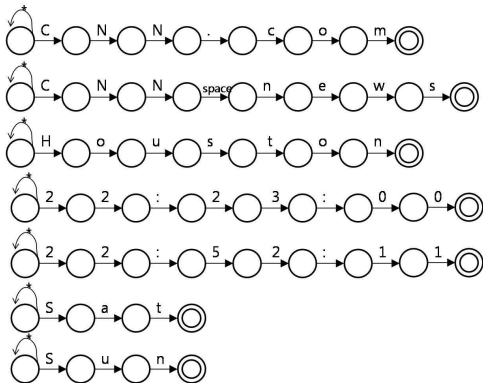

그림 3. 값-기반 술어 NFA 조각[6]
Fig. 3. Value-based predicate NFA fragments[6]

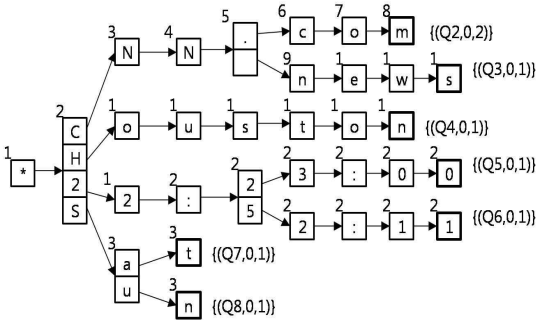

그림 4. 값-기반 술어 NFA의 해시-기반 구현[6]
Fig. 4. Hash-based implementation of value-based predicate NFA[6]

2-2 보안 키워드 기반의 데이터베이스

문서의 보안 수준 변환시에는 문서의 보안 레벨과 각 문서에 속한 단어들의 보안 레벨을 참고하여 최종적으로 변환해야 할 대상 단어들을 선택하는 것이 중요하다. 이를 위해서 변경 대상에 해당하는 단어인지 아닌지에 대한 정보가 필요하다. XML 기반 문서 내에서 보안 점검이 필요한 단어들은 특정 데이터베이스(DB-K)에서 검색이 이루어져야 하며, 검색 결과에 따라서 변경 작업이 수행되어야 한다. 이를 위해서는 기존의 키워드 기반의 DB 연구 결과들이 활용되어야 한다. 관련 연구로는 문맥 광고를 위한 온톨로지 기반 키워드 관리 시스템이 있다[7].

① 온톨로지

온톨로지는 '어떤 관심 분야를 개념화하기 위해 명시적으로 정형화한 명세'를 의미한다. 즉, 각 사물에서 공통점을 찾아내고 이를 하나의 집합 또는 범주로 나타내기 위해 의미, 지식의 쓰임새 등을 분명하고 자세하게 설명하는 것을 말한다.

② 키워드 추출

키워드 추출은 먼저 시스템이 XML 문서를 수집하여 XPath에 태그를 제거하고, 형태 분석기에서 형태 분석을 하여 명사를 추출해 낸다. 그 다음에 클러스터링을 통해 문서를 분류하거나 레벨에 따라 묶는다. 또한 데이터베이스에서 키워드를 추출하기 위해 TF*IDF 알고리즘을 사용한다. threshold값을 1.5로 하여 TF*IDF의 가중치가 적은 단어는 일차적으로 걸러낸다. 가중치가 높은 키워드만을 대상으로 Apriori 알고리즘을 사용해 키워드 사이의 관계를 추출해 낸다. 온톨로지를 구축할 때 사용한 OWL언어는 Subject-Predicate-Object의 구조를 가지므로 두 단어 사이의 관계만 필요하다. 이때 지지도는 0.05이상 신뢰도는 0.5이상인 frequent set을 대상으로 연관 키워드를 추출한다. 이렇게 추출한 연관 키워드는 다시 보안 담당자에 의해 보안 수준별로 연관성을 갖게 되고, 데이터베이스에 저장될 때에는 키워드끼리 연관성에 각 키워드별로 보안수준이 적용되어 사용된다.

③ XML 문서 검색

XML은 추상화된 정보 표현의 기본 단위가 문서가 아니라 엘리먼트(element)이다. 엘리먼트는 문서의 구조를 논리적으로 정의하는 DTD에 의해 알려질 수 있으므로 문서의 내용에 기반을 둔 검색 방법 이외에 문서 구조에 의한 검색을 지원 한다. DTD는 문서 내에 있는 요소들 간의 구조 정보로 XML 문서를 검색할 때에 문서 전체가 아닌 부분 항목들로 처리함으로써 사용자 질의에서 원하는 특정 영역에 바로 접근할 수 있는 구조 기반 정보 검색을 가능하게 한다. 그러나 구조화된 DTD 정보를 활용하기 위해서는 구조화된 자연어 질의를 이용해야 한다. 즉, 구조화된 DTD 정보를 활용할 수 없는 유형의 질의는 의미가 없기 때문에 DTD 정보를 활용해서 XML 문서를 검색할 수 있는 구조화된 자연어 질의를 사용한다.

III. 요소 기술들

3-1 문서 보안 키워드 DB(DB-K)의 구축 운영

보안 문서 내에서 특정 단어가 보안 레벨 변경시, 검열의 대상에 속하는지에 대한 판단은 특정 데이터베이스의 구축 및 운영을 통해서 가능하다. 그림 5는 자동화된 문서 검열 및 보안 레벨 변경시 연동되는 데이터베이스(키워드 DB, 규칙 DB)의 구성을 나타낸 것이다.

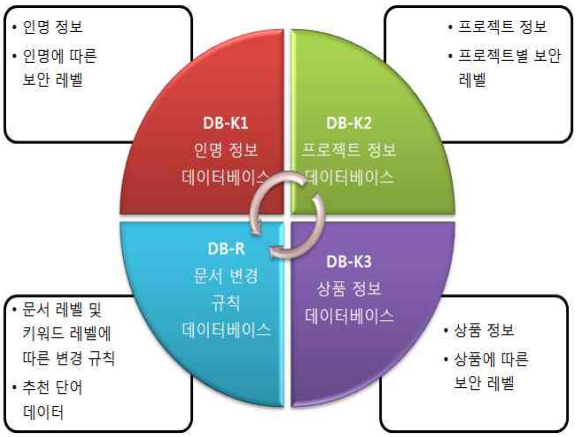

그림 5. DB-K 및 DB-R의 구성
Fig. 5. Configuration of DB-K and DB-R

각 보안 수준에 따른 단어의 삭제 및 변경은 주어를 변경하는 것을 원칙으로 하며, 이러한 삭제/변경 대상의 단어들은 시스템에서 설정된 키워드 데이터베이스(DB-K)들에 저장되어 있다. 그림 5에서 볼 수 있듯이 키워드 데이터베이스는 인명정보, 프로젝트 정보, 상품정보 등이 중요한 보안 키워드들과 이에 대한 보안 레벨들이 저장되어 있는 데이터베이스 이다. 보안 문서 내에 변경/삭제 대상인 키워드가 발견되었을 때에 이를 변경하는 방법은 앞서 언급한 것과 동일한 규칙을 적용할 수 있지만, 추가적으로 예외 규칙 등을 적용하기 위해서는 규칙들을 저장해두는 문서 변경 규칙 데이터베이스(DB-R)를 구축하는 것도 가능하다. 또한 변경을 위한 최종 승인은 최상위 보안 담당자의 확인을 거치도록 하는 것이 안전하다고 할 수 있다.

보안 문서는 각각의 보안 레벨을 가지고 있지만,

각 보안 문서 내에서도 보안 레벨이 중요하지 않은 단어와 보안 레벨이 높은 단어들로 구분될 수 있다. 예를 들자면, “조사”들은 보안 레벨 변경 검열 대상에서 제외될 수 있는 것이다. 그림 6은 문서의 보안 레벨 변경시 문서 안에 각기 다른 보안 수준의 단어가 존재하는 경우의 예를 보여주며, 이러한 경우 단어의 보안레벨은 문서의 최하위 보안 수준에 따른다.

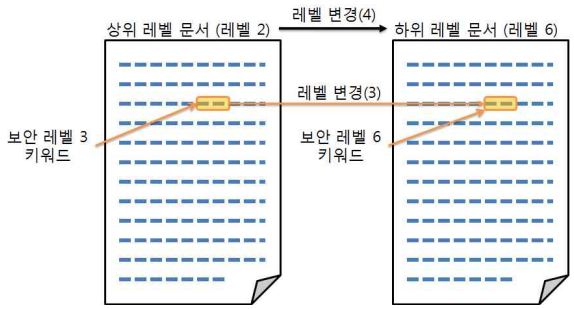

그림 6. 문서 보안 레벨 변경의 예
Fig. 6. Example of security level change of a document

3-2 규칙 DB(DB-R)의 구축 운영

여러 가지 상황에 따라 적용되어야 하는 규칙이 상이할 수 있으므로, 이에 대한 규칙 데이터베이스가 따로 운영되어야 한다. 규칙 구분의 중요한 요소는 1) 문서의 보안 레벨, 2)문서에 포함된 키워드의 보안 레벨, 3)최종 변경된 문서가 가지게 되는 보안 레벨 등이다. 이 3가지의 요소에 따라서 키워드를 a)변경, b)삭제할지를 정하게 되며, 경우에 따라서 키워드가 포함된 문장에 대해서 c)문장 변경, d)문장 삭제가 이루어질 수도 있다.

3-3 정형 문서의 보안 레벨 변경 프로세스

정형 문서의 보안 레벨 변경은 앞서 언급한 DB-K와 DB-R과의 연동을 통해서 이루어진다. 자세한 변환 작업은 그림 7에 설명되어 있다. 1)문서 자동 변환에 관련된 인수(현재문서 보안레벨, 최종문서 보안레벨, 기타 추가 인수)가 입력되고, 2)변경대상에 해당하는 키워드 선정을 위한 DB 연동과 규칙 구분 요소 파악, 3)키워드 매칭, 규칙 적용을 통해 변환작업이 이루어진 후, 4)최종적인 승인 과정이 뒤따르게 된다.

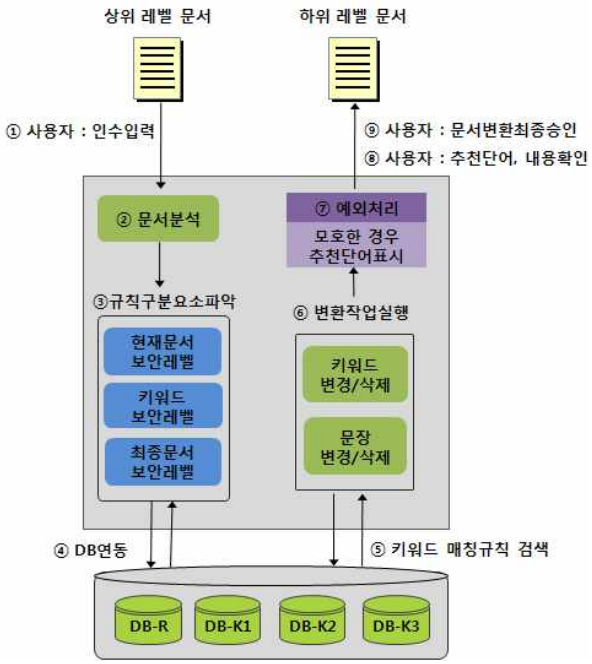

그림 7. 문서 보안 레벨 변경 주요 프로세스
Fig. 7. Main processes of the document's security level change

다음 표1~표5는 임의로 작성된 보안 문서의 예를 들어, 자동화된 검사 및 변경을 위해 고안된 XML 문서로 변환하는 전략에 대한 예를 보여주는 것이다. 이와 관련된 DTD와 원문, 변환된 XML 문서 등에 대한 설명이 예시되어 있다.

표 1. 보안레벨 3의 문서 예(원문)
Table 1. Example of the document with security level 3

발행처 : 상품개발팀(L2) 수신처 : 홍보팀(L6) 윤기철 상무(L2)가 총괄하고 있는 “코드명 ZF(L1)”가 85%의 성공률(L2)을 보여주며 1차 테스트 단계를 마쳤다.

표 2 문서변환 DTD의 예(per.dtd)
Table 2. DTD example for the document conversion(per.dtd)

```
<?xml version="1.0" encoding="utf-8"?>
<!-- 루트엘리먼트 -->
<!ELEMENT 보안열람문서 (문서정보*, 문서내용*)>
<!ELEMENT 문서정보 (발행처, 수신처, 열람자, 참조) >
<!ELEMENT 발행처 (기관*, 부서*) >
<!ELEMENT 기관 (#PCDATA) >
<!ELEMENT 부서 (#PCDATA) >
<!ELEMENT 수신처 (기관*, 부서*) >
<!ELEMENT 기관 (#PCDATA) >
<!ELEMENT 부서 (#PCDATA) >
<!ELEMENT 열람자 (누구*)>
<!ELEMENT 누구 (#PCDATA) >
<!ELEMENT 참조 (부서*, 누구*)>
<!ELEMENT 부서 (#PCDATA) >
<!ELEMENT 누구 (#PCDATA) >
<!ELEMENT 문서내용 (언제*, 어디서*, 누가*, 무엇을*,
어떻게*, 왜*) >
<!ELEMENT 언제 (#PCDATA) >
<!ELEMENT 어디서 (#PCDATA) >
<!ELEMENT 누가 (#PCDATA) >
<!ELEMENT 무엇을 (#PCDATA) >
<!ELEMENT 어떻게 (#PCDATA) >
<!ELEMENT 왜 (#PCDATA) >
```

표 3 보안 레벨 3의 XML 문서
Table 3. XML document of the security level 3

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE DOCU SYSTEM "per.dtd">
<보안열람문서>
<문서정보>
 <발행처>
   <부서> 상품개발팀</부서>
 </발행처>
 <수신처>
   <부서> 홍보팀</부서>
 </수신처>
</문서정보>
<문서내용>
 <어디서> 상품개발팀 </어디서>
 <누가> 윤기철 상무</누가>
 <무엇을> 코드명 ZF </무엇을>
 <어떻게> 85%의 성공율 </어떻게>
 <어떻게> 1차 테스트 마쳤다. </어떻게>
</문서내용>
</보안열람문서>
```

표 4 보안 레벨 6이 적용된 문서 XML
Table 4. Example of the applied xml document to security level 6

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE DOCU SYSTEM "per.dtd">
<보안열람문서>
<문서정보>
 <발행처>
   <부서> 상품개발팀</부서>
 </발행처>
 <수신처>
   <부서> 홍보팀</부서>
 </수신처>
</문서정보>
<문서내용>
 <어디서> 상품개발팀 </어디서>
 <누가> A이사</누가>
 <무엇을> 신상품 </무엇을>
 <어떻게> 우수하게 </어떻게>
 <어떻게> 1차 테스트 마쳤다. </어떻게>
</문서내용>
</보안열람문서>
```

표 5 보안레벨 6으로 변환된 문서 예
Table 5. Example of the converted document to security level 6

```
발행처 : 상품개발팀
수신처 : 홍보팀

A이사가 총괄하는 신상품이 우수하게 1차 테스트 단
계를 마쳤다.
```

IV. 구현시 고려 사항

4-1 XML 기반의 문서 보안 솔루션

기본적으로 본 논문에서 제안하는 문서 보안 수준 변환 기법은 정형화된 문서에 대한 자동 변환을 위한 것이므로, 문서의 정형성 확보를 위해서 XML 기반의 문서 보안 솔루션이 기반이 되어야 한다.

또한 “흔글(HWP)” 문서 편집 소프트웨어는 내부적으로 XML 인식 기능이 있다. 흔글 문서를 XML로 자동 변환할 수 있도록 정형화하면 본 기법을 사용 가능할 것으로 판단된다.

4-2 모호성 배제를 위한 변경 내용 추천 방식

자동 변환이 이루어지는 과정에서 중복된 규칙에 의해서 상호 상충되는 변환이 가능한 경우에는 이를 “모호한 경우”라고 보고, 모호한 경우에 대한 변경 가능한 하나 이상의 변경 내용을 최종 승인자에게 보여줌으로써 판단을 내릴 수 있도록 유도한다.

V. 결 론

기업은 핵심정보 보호를 위하여 여러 가지 보안 솔루션을 도입하고 있다. 이러한 보안 솔루션은 문서의 보안 및 접근 제어를 통해 이루어지며, 특정 문서에는 보안 레벨 및 접근 가능자들에 대한 정보가 입력되어 있어 이를 기반으로 문서의 열람 또는 변경할 수 있는 사람들이 정해지게 된다. 기업 내에서는 조직과의 효과적인 업무 달성을 위해, 종종 다른 보안 수준의 접근 가능자들 사이에 정보를 교환해야 할 필요가 생긴다. 본 논문에서는 이러한 경우 보안 문서의 자동화된 보안 수준 변환기법과 필요한 요소기술에 대하여 소개하였다. 이는 특정 기업에서 상위 보안 레벨의 보안 문서를 하위 보안 레벨로 변환할 경우, 효과적으로 문서를 검열하고 특정 보안 키워드를 일반적인 단어로 변경하는 기법이다. 이러한 작업은 특정 직원에 의하여 수작업으로 이루어 질수도 있을 것이지만, 자동화를 통하여 안전성 및 작업 능률 향상을 가져오며 기업의 정보 관리 체계 유지에도 도움이 될 수 있다. 본 연구는 현재 연구 개발 초기 단계에 있지만, 향후 구체적인 아키텍처의 설계와 실제적인 구현과정에 대한 주요한 기반 문서로서 활용될 수 있을 것으로 판단된다.

참 고 문 헌

[1] 송지훈, 이시진, 장항배, “내부정보유출 방지를 위한 데이터베이스 보안 솔루션 보안성 평가”, *한국정보기술학회논문지* 제7권, 제3호, pp. 179 ~ 187, 2009년 6월.

[2] J.H Kim, H.J Kim, “Design of Internal Information Leakage Detection System Considering the PrivacyViolation”, *ICTC2010 (International Conference on ICT Convergence 2010)*, 2010.

[3] M. M. Moro, S. Malaika, L. Lim, "Preserving XML Queries during Schema Evolution," *Proceedings of the 16th international conference on World Wide Web*, pp.1341-1342, May. 2007.

[4] Extensible Markup Language(XML) 1.0, available at http://www.w3.org/TR/REC- xml, 2004.

[5] 권준호, Praveen Rao, 문봉기, 이석호, “세그먼트 기반의 XML 문서 필터링”, *정보과학회논문지 : 데이터베이스*, 제35권, 제4호, pp. 368 ~ 378, 2008년 8월.

[6] 이경한, 박석, “NFA 표현을 사용한 문서-중심적 XML의 키워드 기반 필터링 기법”, *정보과학회논문지 : 데이터베이스*, 제33권, 제5호, pp. 437 ~ 452, 2006년 10월.

[7] 김경민, 이태상, 이원휘, 안동언, 정성종, 장영권, “문맥광고를 위한 온톨로지 기반 키워드 관리 시스템”, *한국인터넷정보학회 학술발표대회 논문집*, 제8권, 제1호, pp. 479 ~ 483, 2007년 6월.

조 도 은 (趙都恩)

2007년 2월 : 충북대학교 공학박사
2005년 3월~2006년 2월 : 충주대학교 강의전임강사
2007년 3월~2008년 2월 : 충북대학교 BK21충북정보화사업단 연구원
2008년 3월~현재 : 목원대학교 공학교육혁신센터 전임강사
관심분야 : 정보보호, USN정보보호, 유비쿼터스 보안 등

여 상 수 (呂相壽)

2005년 8월 : 중앙대학교 공학박사
2006년 3월~2007년 2월 : 단국대학교 강의전임강사
2007년 2월~2008년 1월 : 큐슈대학교 정보공학부 방문연구원
2008년 2월~2009년 2월 : (주)비티웍스 연구개발본부 부장
2009년 3월~현재 : 목원대학교 컴퓨터공학부 교수
관심분야 : 정보보호 기술 및 정책, 멀티미디어 시스템, 임베디드 시스템, 유비쿼터스 보안 등