인트라넷용 키 복구 정책 및 시스템 설계

Key Recovery Policy and System Design for Intranet

임 신 영, 이병 천*, 함 호 상, 박 상 봉

한국전자통신연구원
정보통신대학원*

요 약

인터넷 전자상거래가 가속화 되면서 기업간 인터넷을 이용한 전자상거래가 증가하고 있다. Business-To-Business 유형의 전자상거래는 인터넷 EDI 또는 글로벌 비즈니스 개념이 도입되어 관련 기술의 연구개발이 활발히 진행중이며 상용화된 서비스가 일부 제공되고 있다. 기업간 전자상거래 시 기업 내부 인력이 외부 즉, 거래 대상 기업 또는 경쟁 관계의 기업에 자사의 영업 및 기업 비밀을 제공하는 것은 명백한 범법 행위이다. 또한 인트라넷 내부 즉, 기업 내부망에 연동된 시스템을 사용하는 직원들이 정해진 근무시간에 다른 용도로 시스템 및 전산망 자원을 사용한다면 이 또한 회사 내부적으로 규제 대상이 되어야 한다. 특히, 일과외 시간에 공적 또는 사적인 용도 외에 사용자와는 전혀 관련 없는 전자우편 주소로 암호화된 문서를 송수신하였다면 기업 책임자는 기업의 시스템 및 전산망 자원을 업무 및 개인 용도 외적으로 사용한 의심스러운 행위에 대하여 확인할 권한이 있다고 본다. 본 논문은 기업간 전자상거래 수행 과정에서 기업 내부망 즉, 인트라넷에서 적용될 수 있는 보안 정책 중 키 복구 메커니즘이 적용될 수 있는 부분을 중심으로 새로운 키 복구 정책, 시나리오, 시스템 구성 및 키 복구 프로토콜을 제안한다.

1. 서 론

키 복구 및 키 위임 기술은 키 관리 기술의 일부분으로 존재하였으며, 암호학적으로 이론 체계가 정립되어가고 있으며, 현재 응용 부분에 그 적용을 두고 많은 찬반 논란이 있다 [9,10]. 특히, 미국에서 단계적으로 수행한 Clipper Project는 4단계 과제까지 수행되면서 현실적인 적용에 있어 실질적인 접근 방법으로 Key Recovery Alliance(KRA)가 결성되

어, 이 연합체의 기술 및 정책 의견이 수렴된 키 복구 관련 보안 시스템이 선보일 예정이다[5]. 사용자가 소유한 개인키 자체를 제 3 자에게 위탁하여 특정 조건이 만족될 경우, 키를 획득할 수 있는 키 위탁(Key Escrow)의 개념과 달리 키 복구(Key Recovery)는 사용자가 데이터의 암호화 시 생성한 세션키에 대하여 특정 조건이 만족될 경우, 특정 세션키로 암호화한 데이터만을 선별적으로 복구하는 개념이다.

참고로 미국이 수행하였던 Clipper project(1993-1996)의 경우, 1단계 과제(1993.4)의 Skipjack 알고리즘 및 Clipper 칩의 제시, 2단계 과제(1995.8)의 Commercial Key Escrow를 도입하여 64 비트 이하의 key escrow 장비의 수출 규제 해지, 3단계 과제(1996.5)의 공개키 방식의 키 관리 기반을 도입하여 이에 키 위임 체계의 개발 제시 등은 키 위임 개념이 기술적으로 적용되었으나 4단계 과제(1996.10)는 업계의 자발적인 참여를 유도하여 업계 자체적으로 키 위임 체계 개발을 촉구하고 있으며 현재 키 위임 및 키 복구 전반에 대한 현실적인 대안들을 검토하고 있다[6].

미국의 사례 외에 상용화된 키 위임 및 키 복구 서비스에 대한 사례분석을 통하여 인트라넷에서 적용 가능한 키 복구 체계를 도출하였다[1,2,3,4,7,8]. 본 논문에서는 인터넷 전자상거래를 수행하는 임의의 기업에서 운영하는 인트라넷 내부에 적용할 새로운 키 복구 정책 및 프로토콜을 제시한다.

2. 인트라넷의 특성

인트라넷(Intranet)은 기업 내부망으로 정의할 수 있으며, 인트라넷의 주요 구성요소는 미들웨어 기반의 Groupware 서비스들이다. 이 중에는 전자우편, 전자게시판, 전자결재, 디렉토리 정보 서비스 및 기업의 영업 행위 과정에서 요구되는 인사, 회계, 자재, 제조 및 영업망 관리에 대한 정보 서비스가 포함된다.

인트라넷 사용자는 기업 내부의 인력 구조에 따른 등급별 사용 권한이 부여되며, 각 등급별 사용자의 사용 권한은 회사 내부에서 정한 규정에 따라 인트라넷에서 제공되는 서비스를 사용할 수 있다.

일반적으로 인트라넷은 보안 방화벽이 구축되어 Incoming 패킷은 필터링 규약에 따라 관리되는 반면 Outgoing 패킷은 자유롭게 외부 정보 자원을 접근할 수 있도록 설정할 수 있다.

3. 전자상거래 환경에서의 인트라넷 관리 정책

본 논문은 인터넷 전자상거래를 수행하는 임의의 기업에서 운영하는 인트라넷을 대상으

로 하며, 인트라넷 측면에서 인트라넷을 운영하고 관리하기 위한 전반적인 정책을 우선적으로 고려하여 키 복구 정책을 도출하여야 할 것으로 보인다[11]

인트라넷의 전자상거래와 관련된 관리 정책은 일반적으로 논의되는 보안 위협에 대한 대응 방안이 포함되어 다음과 같은 범위에서 고려할 수 있으며, 기업 내부 특성을 고려하여 추가 또는 삭제되는 부분이 있을 수 있다.

- o 인트라넷 사용 목적
- o 인트라넷 관리 방침
- o 인트라넷 자원별 관리
  - 시스템, 전산망, 물리적 공간, 인적 자원
- o 인트라넷 자산 관리
  - 정보 자산 등급 분류 기준
  - 자산 분석(가치 기준)
  - 등급별 사용자 접근 범위
- o 인트라넷 관리자 업무 범위 및 권한
  - 자원 관리, 상황 처리 및 보고 절차
- o 인트라넷의 위협 분석 및 위험 평가
  - 취약성 분석, 보안 공격에 대한 분석, 영향 분석
- o 인트라넷 서비스 관리
  - Groupware 기반 서비스
  - 기업 영업 관련 서비스
  - 서비스 사용 현황 관리
- o 인적 자원 교육
- o 인트라넷 수요 및 공급 관리
  - 기업 방침에 따른 인트라넷 규모 및 서비스 관리
- o 인트라넷 전반 감사

4. 인트라넷에서의 키 복구 정책

키 복구 정책을 설정하기에 앞서 인트라넷의 환경을 다음과 같이 설정할 필요가 있다. 기업간 전자상거래 시 각 기업의 사용자들은 해당되는 거래 기간 또는 과정에 참여하는 사용자 등급별 공개키 인증서를 인증기관(CA)에서 발급받아 이를 근거로 전자상거래 업무를 수행하며, 동시에 인트라넷 환경의 기업 내 업무에도 사용할 수 있다. 한편 인트라넷 기업 내 업무용으로 별도의 공개키 인증서를 설정하여 사용할 수 도 있다.

사용자들은 자신에게 부여된 기업 내 업무를 수행하면서 필요에 따라 인트라넷에서 제공되는 공개키 암호 및 전자서명 기술을 전자우편, 전자게시판, 전자결재, 인사, 회계, 자재,

제조 및 영업망 관리 관련 작업 시 사용한다. 본 설정에는 인트라넷 내부에서 외부로 전자우편을 송수신할 수 있으며, 송수신하는 내용은 각 사용자의 작업 내용 또는 인트라넷에서 관리하는 정보 등이 될 수 있다. 사용자는 인트라넷 사용 규정에 정한대로 사안이 민감한 업무에 대하여 암호 기술을 사용한다.

사용자가 외부망에서 인트라넷 내부로 접근하기 위한 접근자 신원 확인은 일반적으로 One-Time password 기반 확인과 인트라넷 내부의 사용자 암호/공개키 인증서 기반 신분확인 절차를 거친 후 접근할 수 있다고 가정한다.

위와 같은 인트라넷 환경에서의 키 복구 정책은 키의 관리, 키 복구 목적, 키 복구 요청, 키 복구 결과 처리 및 키 복구 결과의 법적 효력에 대하여 다음과 같이 도출될 수 있다.

o 사용자의 키 쌍 생성 후 (서명용 및 암호용) 개인키의 관리는 사용자 자신이 담당한다.

o 사용자의 개인키는 여타의 이유에도 - 키 복구 포함 - 위임하지 않는다.

o 키 복구 대상은 사용자의 암호화된 문서의 복구를 위한 세션키 복구로 제한한다.

본 논문에서 선택한 키 복구 메카니즘은 Key Encapsulation 방식이며 이 방식의 장점은 다음과 같다.

- 누구에게도 개인키를 노출하지 않게 된다.
- 개인키 노출의 약점이 없으며, 공격 가능지점이 전무하다.
- 키 복구정보(KRI)의 생성시 제3자와의 통신이 불필요하므로 성능 측면에서 우수하며 높은 확장성이 제공된다.
- 키를 보관해야 하는 기반구조가 불필요하게 된다.
- 키 복구 동작이 사용자들에게 투명하게 된다.

o 키 복구 요청은 사용자가 송신 시 지정한 수신인과 인트라넷 최고 책임자가 할 수 있다.

o 키 복구 요청자 중 인트라넷 최고 책임자는 다음의 각 항에 해당하는 경우에 한하여 키 복구 요청을 할 수 있다.

- 기업내의 실무자 즉, 암호화된 전자문서의 소유자(수신인을 포함한 원 소유자-송신자-)의 유고로 인한 기업 내 고유 업무 처리 추진 시
- 인트라넷 관리자로부터 관리자의 일상 업무 중 인트라넷 사용 현황에 대한 감시 업무를 수행하는 과정에서 다음의 사항에 해당되는 건으로 최고 책임자에게 보고, 최고 책임자는 키 복구 상황이라고 판단될 경우, 인트라넷 관리자에게 키 복구 업무를 수행하도록 지시한다.

* 내부 사용자가 정상적인 업무 시간외에 거래 대상 기업 또는 경쟁 관계의 기업에 암호화된 문서를 전자우편으로 송수신한 경우
* 한밤중에 사용자와는 전혀 관련 없는 전자우편 주소로 암호화된 문서를 송수신하는 경우
* 인트라넷 사용자가 기업의 영업 및 기업 비밀 정보에 해당하는 정보를 암호 처리하여 외부로 유출하려는 의심스러운 징후를 발견한 경우

o 키 복구 후 선별적으로 암호화된 전자문서의 내용 열람은 키 복구 요청자(송신자가 지정한 수신인 및 인트라넷 최고 책임자)만이 할 수 있다.

o 키 복구 결과에 대한 내용의 법적 효력은 전자서명 특성 상 전자문서 원소유자의 소유자 신분 확인이 가능하므로 전자문서와 전자문서의 소유자간의 관계를 규정 지을 수 있으며, 이 관계 입증을 통한 법적 효력 획득이 가능하다고 본다.

5. 키 복구 시나리오

위의 키 복구 정책에 따른 키 복구시나리오는 키 복구 환경 설정 즉, 초기화, 메시지 생성 및 송신, 수신 메시지 정상 처리, 수신자 복구 요청 및 KRC 복구 요청으로 구분하여 논한다.

o 키 복구 환경 설정(초기화)

키 복구를 수행하는 엔티티는 두 가지 형태로 하나는 KRC(Key Recovery Center)이며 다른 하나는 KRA(Key Recovery Agent)이다. KRC는 키 복구를 주관하는 역할을 수행하며, KRA는 KRC의 키 복구 작업의 일부를 지원하는 역할을 수행한다. 통상 KRC는 단일 엔티티로 존재하며 KRA는 복수의 엔티티로 존재한다.

본 논문에서는 인트라넷 사용자의 공개키 인증서 등록을 수행하는 인증기관이 하나의 KRC와 두개의 KRA를 설정하여 키 복구를 수행하는 것으로 설정한다. 설정된 KRC와 KRA가 키 복구 업무를 수행하려면 인트라넷 내부 또는 외부의 인증기관에 공개키 인증서를 등록 한다.

인증기관은 사용자의 공개키 인증서 등록 시 키 복구 정보(KRI : Key Recovery Information)를 사용자의 공개키 인증서에 첨부한다. 사용자는 키 복구를 위하여 별도의 오퍼레이션은 하지 않는다.

인트라넷 관리자는 도메인 사용자들에게 키 복구 서비스 적용에 대한 키 복구 서비스 약관을 사용자가 인트라넷을 사용하기에 앞서 이에 대한 승인을 득한 후 인트라넷 서비스를 허용한다.

o 메시지 생성 및 송신

사용자는 전자우편 서비스를 이용하여 송신할 메시지를 생성하고 이를 수신자에게 송신한다. 이 과정에서 다음의 작업을 수행한다.

- 세션키로 원문(평문)에 대한 암호문 생성(A)
- 원문에 대하여 송신자의 서명용 개인키로 서명 생성(B)
- 세션키를 수신자의 암호용 공개키로 전자봉투 생성(C)
- 공개키 인증서 확장 필드에 정의된 키 복구 정보(KRI)를 이용하여 하며 세션키를 KRA 엔티티 수 만큼 부분 세션키를 생성(D)

o 수신 메시지 정상 처리

수신자는 위의 A, B, C와 자신의 암호용 개인키 및 송신자의 서명용 공개키를 이용하여 송신한 원문에 대한 무결성 확인과 메시지 내용 및 송신자 신분 인증을 수행한 후 메시지 원문에 대하여 작업한다. 이 과정에서 D 정보를 사용하지 않는다.

o 수신자 복구 요청

수신자가 자신의 암호용 개인키의 분실 등 수신자가 수신 메시지 정상 처리를 할 수 없게되면 수신자는 수신된 메시지에 대한 복구를 KRC에 요청한다. 이 과정에서 사용자는 D의 내용 중 KRC 정보 등을 이용한다.

o KRC 복구 요청

복구 정책 중 키 복구 요청에 따라 인트라넷 최고 책임자는 KRC에게 키 복구를 요청할 수 있다.

o 복구 절차

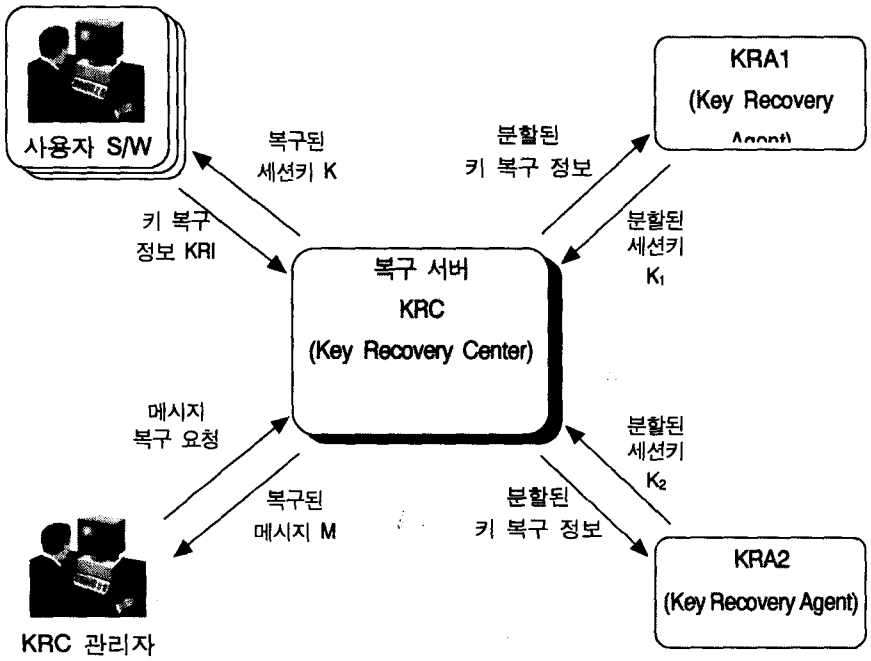
KRC는 사용자(수신자) 및 KRC 관리자로부터 복구 작업 요청이 수신되면 요청에 대한 신분 확인 과정을 거친 후 KRA 엔티티들에게 암호화된 부분 세션키를 보내어 복호화하도록 요청한다. KRC는 KRA로부터 부분 세션키 복호화 결과를 수신하면 부분 세션키를 조합하여 세션키를 복구한다. 복구한 세션키는 사용자(수신자) 또는 KRC 관리자에게 송신되어 암호문을 처리할 수 있도록 한다.

6. 키 복구 프로토콜

키 복구에 대한 기본 프로토콜의 구성은 전체 시스템의 구조상 구성 요소, 단계별 프로토콜 세 및 기본적인 프로토콜 데이터 단위(PDU : Protocol Data Unit)에 대하여 논한다. 특히, PDU 부분은 설정 시 고려 사항을 중심으로 논한다. 수신 메시지 정상 처리의 프로토콜 명세는 일반 암호 송수신 프로토콜 명세와 동일하여 본 논문에서 생략한다.

6.1. 키 복구 시스템의 구성

아래 <그림 1>은 키 복구 시스템 구성도로 시스템을 구성하는 요소는 5가지로 이 중 전자 문서 송수신 부분은 생략하였다.



<그림 1> 키 복구 시스템 구성도

▶ **사용자 S/W** : 사용자가 수신된 전자문서를 복구할 수 없을 때, 복구 서버(KRC)에게 전자문서 복구를 요청한다.

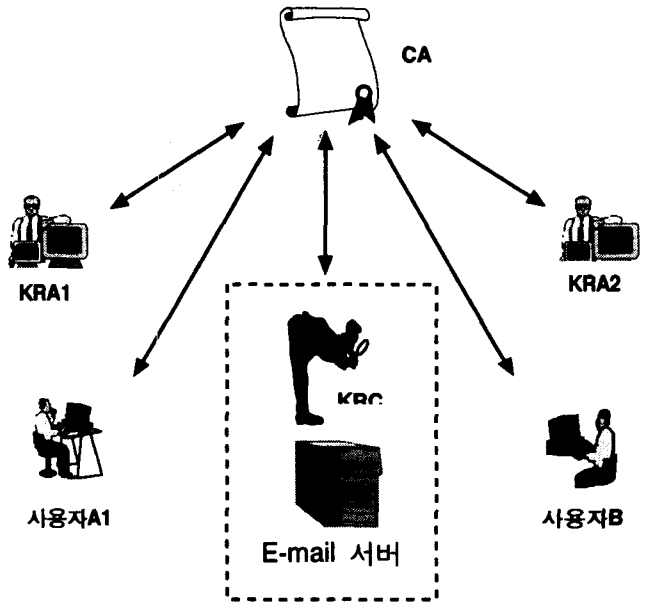
▶ **키 복구 서버(KRC) 관리자** : 인트라넷 관리자로 기업 내에서 설정한 인트라넷 관리 정책 및 복구 정책에 따른 업무를 수행한다. 또한 법 집행 기관의 법무 수행에 관련된 정당한 요구나 법적인 권한 집행에 의하여 메시지를 복구할 때, 기업 책임자는 KRC 관리자에게 키 복구 업무에 대한 지시를 내린다.

▶ **키 복구 서버(KRC)** : 사용자 S/W(수신자)나 KRC 관리자의 요구에 의해 KRI를 분할하여 KRA1, KRA2에게 암호화된 부분 세션키 복구(복호화) 요청을 하여 이를 사용자 EH는 KRC

관리자에게 전송하며, KRC는 부분 세션키를 조합하여 암호화된 메시지 복구를 수행한다. (이 과정에서 사용자 인증과 메시지 획득을 위해 인증기관과 전자문서 송수신 서버와 접속한다.)

▶ **복구 대행자(KRA)** : 키 복구 서버의 요청으로 암호화된 부분 세션키 복구를 지원하는 역할을 수행한다.(본 논문에서는 2개의 키 복구 대행자를 설정하였다.)

6.2. 키 복구 환경 설정(초기화) 프로토콜



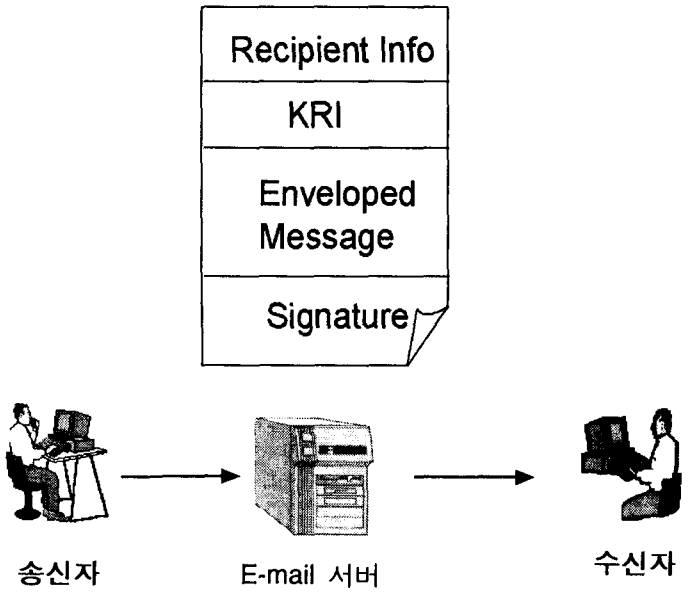
<그림 2> 복구 시스템 초기화

① 전자우편(E-mail) 서버, KRC, KRA1, KRA2는 CA로부터 공개키 인증서를 Off-line 형식으로 획득한다.

② CA는 복구정책에서 설정된 KRC, KRA1, KRA2를 키 복구 서버군으로 설정 후 이들의 공개키 인증서들을 자신의 시스템내에 설치한다.

③ 사용자 A, 사용자 B는 CA에 공개키 인증서 발급 요청하며, 이때 CA는 사용자 공개키 인증서를 생성하는 과정에서 KRC, KRA1, KRA2의 정보를 공개키 인증서 확장 필드에 입력하여 발급한다.

6.3. 메시지 생성 및 송신 프로토콜



<그림 3> 메시지 생성 및 송신

① 메시지 원문을 압축한다. ⇒ Z

② 임의의 세션키를 생성한다. ⇒ K (DES 키)

③ 메시지를 세션키(K)로 암호화한다. ⇒ $C = E_K(Z)$

④ 수신자 정보를 생성한다.(수신자의 암호용 공개키로 세션키 암호화) ⇒ $RI = E_{pkr}(K)$

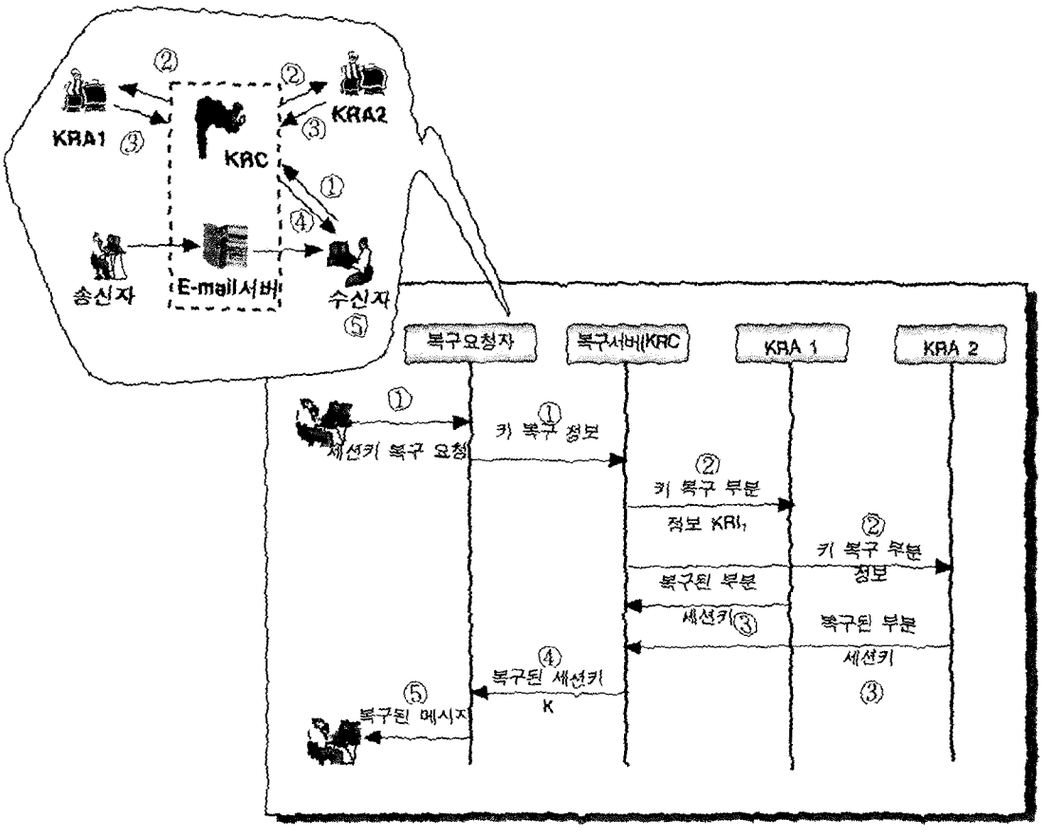
⑤ 송신자 정보를 생성한다.(송신자의 서명용 개인키로 원문에 대하여 서명) ⇛
SI = $S_{sks}(H(M))$, (메시지 원문의 해쉬 값에 대한 서명문)

⑥ 키 복구 정보를 생성한다.(KRI) - 자신의 공개키 인증서에 등재된 복구기관
i) 세션키를 KRA의 숫자만큼의 부분 세션키로 나눈다. ⇛ K = K1⊕K2
ii) 부분 세션키들을 KRA의 공개키로 암호화하여 KRI를 생성한다.

⑦ 수신자 정보, 암호문, 송신자 정보, 전자 문서 복구 정보, 자신의 서명용 공개키 인증서 및 암호용 공개키 인증서를 전자우편(E-Mail) 서비스를 통하여 송신한다.

⑧ 전자우편(E-Mail) 서버는 메시지가 적절한 KRI를 포함하지 않은 경우 송신을 제한할 수 있다.

6.4.수신자 복구 요청 프로토콜



<그림 4> 수신자 복구 요청

수신자가 정상적으로 암호문을 해독할 수 없는 상황인 경우,

① 사용자가 KRC에게 세션키 복구를 요청한다.(KRI)

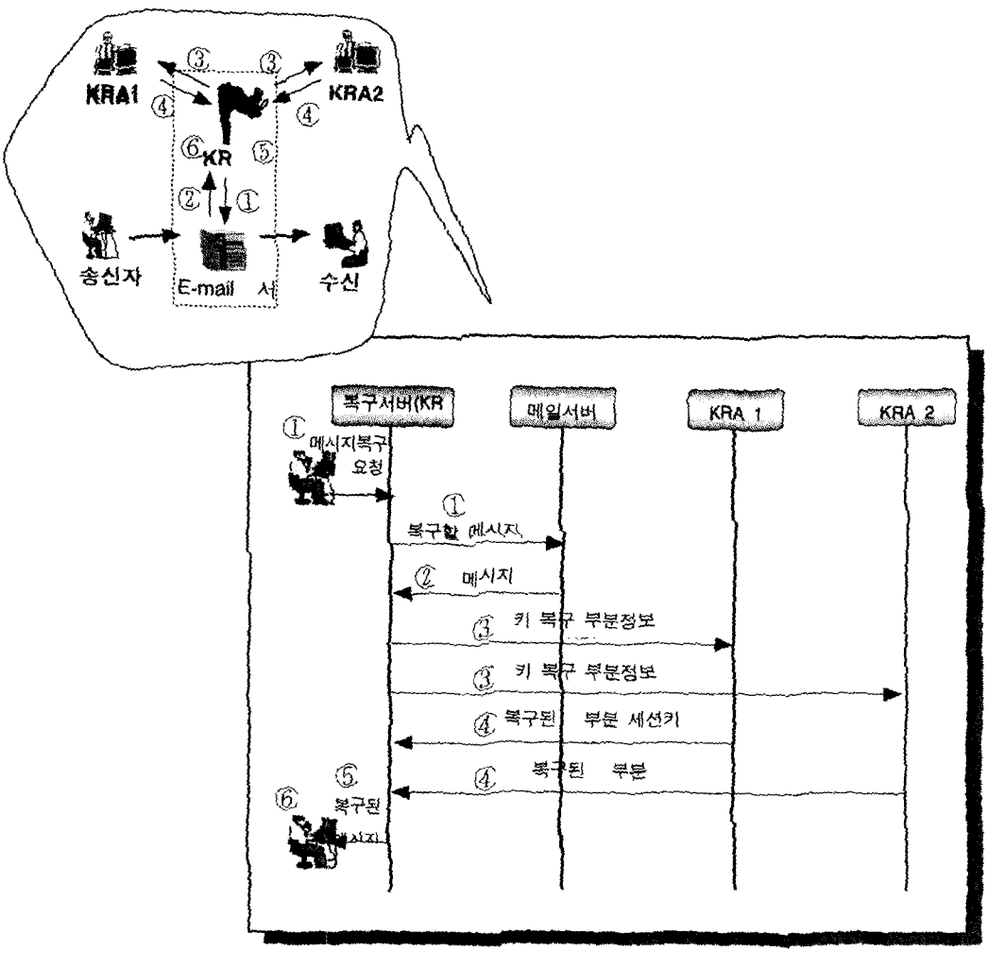
② KRC는 KRI로부터 각 KRA들에 부분 세션키 복구를 요청한다.

③ KRA는 요청 확인 후 부분 세션키를 복구하여 응답한다.

④ KRC는 세션키 K를 복구하여 사용자에게 제공한다.

⑤ 사용자는 세션키 K를 이용하여 메시지 M을 제공한다.

6.5. KRC 복구 요청 프로토콜



<그림 5> KRC 복구 요청

인트라넷 키 복구 정책에 따라 인트라넷 관리자는 KRC에게 특정 송신자의 암호화된 전자문서 내용을 확보하기 위하여 다음의 과정을 수행한다.

① KRC는 복구할 메시지인 송신자의 특정 메시지를 전자우편(E-Mail) 서버에 요청한다.

② 전자우편(E-Mail) 서버는 KRC를 인증 후 요청한 메시지를 KRC로 송신한다.

③ KRC는 메시지에서 KRI 획득 후 각 KRA들에 암호화된 부분 세션키 복호화를 요청한다.

④ KRA는 요청 확인 후 암호화된 부분 세션키를 복호화하여 KRC에 응답한다.

⑤ KRC는 부분 세션키로부터 세션키 K를 복구한다.

⑥ KRC는 K를 이용하여 메시지 M을 복구하여 기업 책임자에게 암호 송신한다.

6.6. 프로토콜 데이터 단위(PDU)

키 복구 시스템의 프로토콜 데이터 단위 중 기본적으로 고려할 KRC 및 KRA의 PDU에 대하여 아래와 같이 정의할 수 있다. 그외에 공개키 인증서 확장 필드에 정의해야할 KRI(또는 Key Recovery Header) 및 전자우편 서버에서 송신 문서 확인 시 적절한 KRI로 송신하는 지의 여부를 판정하기 위한 정보를 PDU에 반영하는 것 등은 본 논문에서 생략한다.

KRC의 기본 PDU 명세

```
KRC-system-name
KRC-host-ip-address
KRC-certificate-serial-number
KRC-KRA-1-host-ip-address
KRA-1-certificate-serial-number
KRC-KRA-2-host-ip-address
KRA-2-certificate-serial-number
KRC-public-key-algorithm-id
KRC-digital-signature-algorithm-id
KRC-signature
KRC-Recovery-Handler
{
  KRC-RH-request-process-id
  KRC-RH-reason-code
```

```
    KRC-RH-Email-host-ip-address
    KRC-RH-requestor-information(KRC or Receiver)
      RH-Requestor-name
      RH-Requestor-certificate-serial-number
    KRC-RH-Session-Key-Information
      RH-public-key-algorithm-id
      RH-digital-signature-algorithm-id
    KRC-RH-signature
  }
```

KRA의 기본 PDU 명세

```
KRA-system-name
KRA-host-ip-address
KRA-certificate-serial-number
KRA-public-key-algorithm-id
KRA-digital-signature-algorithm-id
KRA-signature
KRA-Recovery-Handler
{
  KRA-RH-request-process-id
  KRA-RH-reason-code
  KRC-Request-Information
    RI-Requestor-name(KRC or Receiver)
    RI-Requestor-certificate-serial-number
  KRA-Splitted-Session-Key-Information
    SS-public-key-algorithm-id
    SS-digital-signature-algorithm-id
  KRA-RH-signature
}
```

7. 결 론

정보화 사회의 기업간 경제 행위 기반이 될 인터넷 전자상거래는 기업 입장에서 경쟁력 및 생산성 측면에서 획기적인 전기를 마련할 것으로 보인다. 한편 이러한 기반구조를 오용 또는 의도적으로 역기능 사고를 유발할 경우, 발생 가능한 피해는 기존 문서화된 사회에서의 피해정도에 비하여 심각성과 후유증이 크기 때문에 이러한 정보 서비스를 사용하고 관리하는 과정에서 안전장치의 설정(정책 수립)과 구축은 필수적이라고 본다.

본 논문에서 제시한 인터넷 전자상거래 과정에서 임의의 기업 내부망에서 적용될 수 있는 보안 정책 중 키 복구 기술에 해당되는 정책 도출과 키 복구 프로토콜은 미국의 Clipper project 및 상용 제품의 사례분석을 통하여 새롭게 제안하였다.

향후 이러한 제안에 대한 현실적인 내용을 도출하여 이를 대상으로 시험적으로 한시적인

기간동안 현업에서 사용해 봄으로써 현실적인 적용 여부를 분석할 필요가 있다고 본다.

참 고 문 헌

[1] Baker, et al, Cryptographic Key Management and Validation System, US Pat No. 5,812,666, Oct., 1995.

[2] Gradient Technologies' Implementing Key Recovery Strong Encryption for Worldwide Use, http://www.gradient.com/Products/Pc-dce/WhitePaper/Keyrecovery.html

[3] IBM KeyWorks(5648-A52), Key Recovery Service provider(5697-C86), http://www.ibm.com/Security/html/wp_keymgt.html

[4] Johnson, et al, Cryptographic Key Recovery System, US Pat No. 5,815,573, Apr., 1996.

[5] Key Recovery Alliance, http://www.kra.org

[6] Key Recovery Examples, http://csrc.nist.gov/krdp/exa.html

[7] Key Recovery Standard, http://csrc.nist.gov/

[8] The SecretAgent Key Recovery Mechanism, Information Security Corporation, http://www.infoseccorp.com/press/kr.html

[9] 송유진, 비밀분산방식의 새로운 구성법, 한국정보보호학회지, 제 7 권, 제 4 호, pp. 3-10, Dec., 1997.

[10] 이임영, 채승철, Key Recovery 시스템에 관한 고찰, 한국정보보호학회지, 제 7 권, 제 4 호, pp. 45-58, Dec., 1997.

[11] 임신영, 인터넷 관리자를 위한 보안 지침서, 1997.1.