The Journal of Korean
Institute of CALS/EC
Vol. 4, No. 3, Dec. 1999

기업 정보체계의 키 복구 기술*

임신영**, 강상승**, 하영국**, 함호상**, 박상봉**

Key Recovery Technology for Enterprise Information Infrastructure(EII)

Shin-Young Lim, Sang-Seung Kang, Young-Guk Ha,
Ho-Sang Ham, Sang-Bong Park

Abstract

As Electronic Commerce is getting larger, the volume of Internet-based commerce by enterprise is also getting larger. This phenomenon applies to Internet EDI, Global Internet Business, and CALS information services. In this paper, a new type of cryptographic key recovery mechanism satisfying requirements of business environment is proposed. It is also applied to enterprise information infrastructure for managing employees' task related to handling official properties of electronic enterprise documents exchange. This technology needs to be complied to information management policy of a certain enterprise environment because behavior of cryptographic key recovery can cause interruption of the employees' privacy. However, the cryptographic key recovery mechanism is able to applied to any kind of information service, the application areas of key recovery technology must be seriously considered as not disturbing user's privacy. It will depend on the policy of enterprise information management of a specific company.

Keyword *: Key Recovery, Enterprise information infrastructure*

---

* 본 논문은 정보통신부가 지원한 "CALS 요소기술 개발" 과제의 연구 결과임.

** 한국전자통신연구원 전자상거래연구부

1. 서론

인터넷 기반의 기업 정보 시스템은 암호 기술을 제공함으로써 사용자에게 안전한 기업 정보 사용자 환경을 제공할 수 있다. 그러나 기업의 자산인 기업 정보가 기업 종사자의 부주의 또는 고의로 인한 외부 유출이 암호 기술을 오용하여 발생된다면 기업 정보 관리 차원에서 심각한 관리상의 문제를 발생시킬 수 있다. 이를 통제하기 위한 기술적 대안으로 키 복구 기술이 제시되고 있으며, 이 기술은 키 관리 기술의 일부로서 현재 기반 기술의 적용을 두고 많은 찬반 논란이 있다[9,10]. 특히, 미국에서 단계적으로 수행한 Clipper Project는 4단계 과제까지 수행되면서 기술의 적용에 있어 구체적인 대안으로 전문 기술 업체로 구성된 Key Recovery Alliance(KRA)가 결성되어, 이 연합체의 기술 및 정책 의견이 수렴된 키 복구 시스템의 최소 요구사항이 제시된바 있다[5]. 키 복구 기술은 크게 2가지 유형으로 대별될 수 있다. 그 중 하나는 사용자가 소유한 개인키 자체를 제 3 자에게 위탁하여 특정 상황이 발생되는 경우, 사용자의 개인키를 법 집행 기관(예 : 수사기관)이 제 3 자로부터 획득할 수 있는 키 위탁(Key Escrow) 방식이고, 다른 하나는 키 캡슐화(Key Encapsulation) 방식으로 전자문서 송신자가 자신의 데이터를 암호화하기 위하여 생성한 세션키를 복구하는 것으로 선별적인 암호 메시지 복구를 캡슐화된 세션키의 개별적인 복구 기술로 처리하는 방식이다. 이 키 캡슐화 방식의 특징은 사용자가 개별적으로 세션키를 제3의 기관에 위탁하지 않아도 캡슐화된 세션키를 복구할 수 있는 기술적 방법을 제공할 수 있어야 한다.

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 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 캡슐화 전반에 대한 현실적인 대안들을 검토하고 있다[6].

본 논문의 구성은 미국의 사례 외에 상용화된 키 위임 및 키 캡슐화 방식에 대한 사례분석을 제시하고, 키 캡슐화를 기반으로 새롭게 제안한 키 복구 모델의 특성과 장점을 소개한다[1,2,3,4,7,8]. 그리고 새롭게 제안한 키 캡슐화 방식을 기업 정보 체계에 적용한 결과인 기업 정보 체계를 위한 키 복구 시스템을 인터넷 전자상거래를 수행하는 임의의 기업 내부에서 운영하는 인트라넷 범위에서 사용 가능한 키 복구 정책 및 시스템 설계로 제시한다.

2. 키 복구 기술

정보화 사회는 "정보의 접근 가능성"이라는 긍정적인 측면과 정보의 노출로 인한 "정보의 침해가능성"이라는 부정적인 측면에 대한 문제 해결이 요구되고 있다. 이러

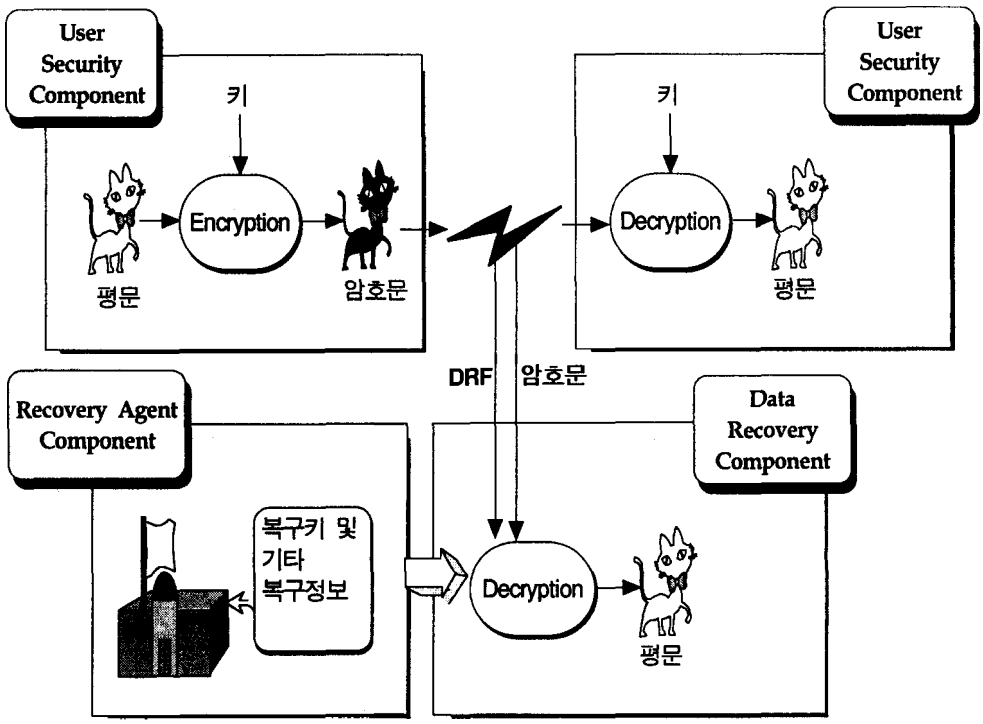
한 정보 보호 방법에는 물리적인 방법, 논리적인 방법 등이 있으나, 현실적으로 정보에 대한 직접적인 보호는 암호키를 이용한 암호 기술에 의존하고 있다. 암호키를 이용한 방법은, 암호키를 분실하거나 암호키가 손상되었을 때에 암호화된 데이터를 사용하지 못하게 된다. 그러므로, 키 분실 또는 손상으로 인하여 암호화된 데이터를 사용하지 못하게 되었을 때에는 키 복구 기술을 사용하여 데이터를 복구할 수 있다.

일반적으로 키 복구 시스템이란 사전에 약속된 특정한 조건하에서 암호화된 암호문을 정당한 권한에 의하여만 복호화가 가능한 시스템을 말한다. 여기서 특정한 조건이란 다음과 같다.

- 사용자(수신자)가 암호문을 복호화 할 수 있는 키를 분실하였을 때
- 사용자(송신자)가 속한 기관에서 감사가 요구될 때
- 정부 또한 법집행 기관의 감사가 요구할 때

즉, 키 복구란 암호 시스템에서 키를 가지고 암호문을 복호하는 정상적인 절차 외에 다른 방법 또는 정보 시스템 관리 정책에서 정한 비상 상황 및 유사시에 암호문을 복호할 수 있는 방법이다.

키 복구 시스템은 사용자 보안 요소(User Security Component : USC)와 복구 기관 요소(Recovery Agent Component : RAC), 데



<그림 1> 키 복구 시스템의 일반적인 구성 요소

이터 복구 요소(Data Recovery Component : DRC)로 구성된다. 키 복구 시스템의 일반적인 구성은 <그림 1>과 같다.

미국의 경우, 클리퍼 정책이 발표된 후 IBM을 비롯한 미국 내의 기업이 KRA(Key Recovery Alliance)를 결성해서 강력한 암호 제품 사용의 촉진을 위해 상업적인 용도로 수행하는 키 복구 기술의 상호 호환성, 키 복구 제품과 키 복구를 지원하지 않는 제품 사이의 상호운용 등의 문제 해결과 구현, 실행에 관한 해결책을 찾기 위한 활동을 펴고 있다.

현재 각국에서는 키 복구에 관한 정부와 사용자의 논란이 진행중이다. 키 복구 방식을 국가차원에서 도입하는 문제는 국가 보안 유지의 필요성과 사용자의 프라이버시 보호에 대한 욕구가 서로 상충되는 부분이 있기 때문에 향후 국가차원에서 균형 잡힌 정보 관리 체계 도출이 요구된다. 대체적으로 키 복구 유형은 키 위탁 방식과 키 캡슐화 방식이 있다<표 1>.

키 위탁 방식은 키 자체를 위탁하는 것으로서 사용자가 거부감을 가지고 있으며, 보관 기관의 신뢰도 수준, 서비스 사용 제한의 문제 등이 있으며, 키 캡슐화 방식은 사용자 정보에 키 복구 필드를 이용하여 복구하는 것으로 키 복구 필드의 인증 및 조작 방지 대책의 문제가 있다.

키 위탁 방식

키 위탁 방식은 사용자의 개인키 전부 또는 일부를 신뢰할 수 있는 제 3자(Trusted Third Party)에게 위탁하는 방식으로 유사시에 키를 확실하게 얻을 수 있다는 장점이 있다. 이 방식은 유사시에 키를 확실하게 얻을 수 있다는 장점이 있는 반면에, 키를 위탁하는 제 3자의 신뢰도에 많은 영향을 받는다. 또한 이러한 키 위탁 방식에서 위탁하는 키는 대부분 한시적으로 사용되는 세션키(session key)가 아니라 사용자의 개인키와 같이 오랜 주기 동안 사용되는 키가 되므로 신뢰도가 낮은 기관에서 키를 관리하는 경우에는 많은 문제점이 발생할 수 있다. 미국의 클리퍼 칩의 경우 초기에 정부 기관을 위탁기관으로 선정했으나, 사용자들의 강력한 반발로 위탁기관을 민간 부문으로 이전하기도 했었다.

또한 위탁방식을 사용할 경우 제 3자의

<표 1> 키 복구 방식

키 복구 방식		주요 특징
위탁	Escrow	사용자의 개인키의 전부 또는 일부를 하나 또는 그 이상의 신뢰기관에게 위탁하는 방식
	TTP(Third-Trusted Party)	신뢰할 수 있는 기관을 키 분배 센터로 지정하여 이 기관에서 암호학적 세션키를 생성, 사용자에게 분배하는 방식
	상업적 키 백업	신뢰 기관을 이용한 또 다른 방식으로 주로 내부 신뢰기관을 이용하여 사용자의 비밀키 사본을 저장
Encapsulation		키 복구 필드를 생성, 사용자 정보에 부가하는 방식으로 사용자의 개인키 정보는 포함하지 않으며, DRF(Data Recovery Field)가 부가된 해당 데이터만을 복구

신뢰도뿐만 아니라 사용자들이 위탁한 키의 안전한 보관과 관리 문제, 키가 법률 기관에 의해 합법적인 도청 목적으로 공개되었을 경우에 키의 사용기간의 제한 등이 중점적인 문제로 등장한다. 부가적으로는 키를 사용자가 생성해서 위탁할 것인지, 위탁 기관이 생성한 후에 사용자에게 알려줄 것인지 등에 관한 문제도 있다.

위탁 방식에서는 키 위탁 기관의 신뢰도를 높이고 키 정보가 집중됨으로써 보안 공격목표가 되는 것을 막기 위해서 비밀 분산 방식(Secret Sharing Scheme)을 사용하여 위탁된 키를 여러 기관에 분산시키는 방식 등이 사용되고 있다. 이 방식을 사용하는 경우, 복구 필드와 같은 부가 정보가 없으므로 현재 사용되는 기존의 모든 프로토콜에 별도의 수정 없이 적용할 수 있다. 따라서, 키 복구를 지원하지 않는 제품과의 상호 작용에도 별다른 문제점이 없어서 쉽게 적용이 가능하다는 장점이 있다.

전자상거래 및 인터넷을 통한 정보의 송수신 과정에서 사용자 정보의 보호 요구가 확대됨에 따라 암호 응용도 증가되고 있다. 이 중 키 복구 기술의 필요성이 증대되고있으며, 그 시장성이 무한하다고 할 수 있다. 따라서, 세계 각국에서는 기관이나 회사, 정부가 키 복구 제품[표 2]을 생산하기 위해 많은 노력을 투자하고 있다.

키 복구 방식의 다른 사례로 Trusted Third Party 모델이 있으며, 이 모델이 적용된 사례는 Yaksha system이 대표적이다. 이는 사용자가 Trusted Third Party(즉, 키 분배 센터)로부터 자신의 암호 키를 공급받아 사용하다 사용자의 암호 키를 분실 또는 복구가 필요할 경우, Trusted Third Party에게 키 복구를 요청하는 모델이다. 이 모델의 암호학적인 문제는 Trusted Third Party의 안전성에 있다.

다른 키 복구 방식으로 Commercial key backup 모델이 있다. 이는 데이터를 암호화할 때 사용자(송신자)가 자신의 암호용 개인키를 키 복구 기관에 전송하여 두고, 사용자가 키 복구를 요청하게 되면 키 복구 시스템은 사용자의 암호용 개인키를 제공하는 방식이다. 이러한 각각의 모델은 개인키 또는 특정 세션키에 대하여 신뢰할만한 기관 즉, 보안 시스템에 암호 키를 위탁하는 모델을 근간으로 하며, 이러한 키 위탁 방식에 근거한 모델들의 근본적인 암호학적 문제는 암호 키의 관리 측면에 있다.

본 논문에서 새롭게 제시하는 캡슐화 방식의 키 복구 시스템은 이러한 키 위탁 방식의 단점을 보완한 모델이며, 안전한 키 복구 오퍼레이션을 위하여 실질적인 암호 키의 복구를 이중 구조로 처리하였다.

3. 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.

<표 2> 키 복구 제품 비교

Product	User Security component (USC)					Key Escrow Component (KEC)					Data Recovery Component (DRC)	
	APP	Enc Alg	Keys	DIF	Imp	Role	Type	Esc Keys	Split	Service	Keys Req	Per
AT&T Crypto Backup	f,c	Ur	pub	pub	S		C	master	1,k/n	dec K	S	K
Banker SecureKEES	c	U	priv	pub,k	H		C	user	k/n	rel KU	S/R	S/R
Bell Atlantic Yaksa	c,f	U	priv	na		KMI	C	session	1	rel K		K
Blaze File Crypto	f	U	none	na	H		C	dir	1	dec file	S	K
Clipper Chip(EES)	c	C	priv	priv	H		G	prod	2/2	rel KU/exp	S	S
Cylink Key Escrow	c,f	U	priv	pub,k		PKI	C	user	1,k/n	rel KU	S/R	S/R
Desmedt Traceable	c	U	priv	pub,k				user			R	R
Fortezza Card	c,f	C	priv	pub	H		C	user	1	rel KU	R	R
Fortress KISS	c	U	priv	pub,k	H	PKI	G	master	2/2	dec KU	S/R	S/R
Kilian/Leighton F-safe	c	U	priv	pub,k				user	k/n	rel KU		
Leiberchi TB-Clipper	c	C	priv	priv	H/c		G	prod	2/2	rel KU/tb	S	S
Leighton/Micali		U	priv	na				prod		rel KU/K	S/R	S/R
Lenstra/Winkler/Yaobi	c	U	priv	pub		PKI		user	k/n	rel KUV/tb	S/R	S/R
Lotus Notes Int'l	c	U	pub	pub	S		G	master		dec partial K	S	K
Micali Fair Crypto	c	U	priv	pub,k		PKI		user	k/n	rel KU/tb	R	R
Micali "Partial Escrow								partial				
Micali/Sidney Esc.		U	priv	priv				user	t/u/n	rel KU		
National CAKE	f,c	U	pub	pub	H		C	master	1	dec K	S	S
Nechvantal Public-Key	c		pub	pub				prod	n/n	rel KU	S	S
Nortel Entrust	c,f	Ur	priv	pub,k	H,S	PKI	C	user	1	rel KU	S/R	S/R
PC Sec. Stoplock KE	c,f	Ur	priv		S	KMI	C	system				
Royal Holloway TTPs	c	U	priv	priv,k		PKI	C	user		rel KU	S/R	S/R
RSA Secure	f	Ur	pub	pub	S		C	master	k/n	dec K	S	K
Shamir Partial Escrow			priv					partial		rel		
TECSEC VEIL	f	U	priv	priv,k	S	KMI	C	system	n/n	rel K	S/R	K
TESS w Key Escrow	c	U	priv	na	H	PKI	C	user	any	rel KU	S/R	S/R
ThresholdDecryption	c	U	priv	pub				user	k/n	th-dec K	S?	S?
TIS Comm Key Esc.	f,c	U	pub	pub			C	master	1	dec K	S	K
TIS Software Clipper	c	U	pub	pub	S			prod	2/2	rel KU	S	S

<표 3> 표 2의 기호 설명

▶ User Security Component(USC)
· App=application
c=communication; f=files and other stored objects
· Enc Alg = data encryption algorithm
C=classi-field; U = unclassified; Ur = proprietary unclassified
· Keys =stored keys used with key escrow 기능
priv = private keys and optionally public keys
pub = public key only
· DRF = encryption keys used to compute Data Recovery Field
priv = private keys(and, optionally, public keys)
pub = public keys
k = DRF also used with key establishment/distribution
na = not applicable
· Imp = Implementation
H = some special hardware required
H/c = hardware with a clock
S = software with optional hardware

▶ Data Recovery Component (DRC)
· Keys Req = keys required for decrypting data
S = keys associated with the sender or the sender's USC
R = keys associated with the receiver or the receiver's USC
S/R = keys associated with either sender or receiver
· Per = frequency with which DRC must Interact with KEC to get keys
K = once per session/file key
S = once per sender
R = once per receiver
▶ Key Escrow Component (KEC)
· Role = Integration of key escrow into key management Infrastructure
KMI = Integrated with key management Infrastructure
PKI = component of public key Infrastructure administered by certificate authorities
· Type = type of System
C = keys held by commercial or private sector escrow agents
G = keys held by government
· Esc Keys = keys stored in escrow
dir = file encryption key used with entire directory
master = escrow agent master key
partial = part of user or application key
prod = product unique key
session = session key
system = keys managed by system
user = user key
· Split = splitting of keys with escrow agents
n/n = n out of n needed for decryption
k/n = k out of n needed using threshold techniques
t/u/n = allows t to conpire and compromise key and n-u to withhold
· Service = service provided to DRC
dec K = decrypt data encryption key K
rel K = release K from escrow
thd-dec K = use threshold decryption
dec KU = decrypt user or product key
rel KU = release KU from escrow
rel KUV = release keys used by pair of users U and V
tb = time-bounded keys released
exp = keys released with expiration date

4. 전자상거래 환경에서의 기업정보망 관리 정책

본 논문은 인터넷 전자상거래를 수행하는 임의의 기업에서 운영하는 인트라넷을 대상으로 새롭게 제안하는 키 복구 시스템을 적용하였으며, 인트라넷 측면에서 인트라넷을 운영하고 관리하기 위한 전반적인 정책을 우선적으로 고려하여 키 복구 정책을 도출하였다[11].

전자상거래와 관련된 인트라넷의 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

5. 기업정보망의 키 복구 정책

키 복구 정책을 설정하기에 앞서 기업정보망 즉, 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 발급 받아 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. 공개키 인증서란 공개키 암호 기술을 사용하기 위하여 필요한 인증서이다. 공개키 암호 기술을 사용하는 방식은 사용자들은 각기 키쌍 즉, 공개키와 개인키를 생성하고 이 중 공개키를 신뢰할 만한 인증 기관에 등록한다. 그러면 제 3자가 사용자의 공개된 공개키 인증서 내의 사용자 공개키를 이용하여 암호문을 생성하고 이를 사용자에게 보내면 사용자는 공개키에 대한 개인키를 대입함으로써 암호문을 해독할 수 있는 기술이 바로 공개키 암호 기술이다.

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 제안한 키 복구 메카니즘은 키 캡슐화 방식을 근간으로 하며, 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 감시업무를 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 경쟁관계의 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

- ㅇ 키 복구 후 선별적으로 암호화된 전자문서의 내용 열람은 키 복구 요청자(송신자가 지정한 수신인 및 인트라넷 최고책임자)만이 할 수 있다.
- ㅇ 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.

6. 키 복구 시나리오

위의 키 복구 정책에 따른 키 복구 시나리오는 키 복구 환경 설정 즉, 초기화, 메시지 생성 및 송신, 수신 메시지 정상 처리, 수신자/KRC(Key Recovery Center) 복구 요청 및 복구 처리로 구분하여 논한다.

ㅇ 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 복구 작업을 관리하는 역할을 수행하며, KRA는 KRC의 키 복구 작업의 일부를 실질적으로 수행한다. 통상 KRC는 단일 엔티티로 존재하며 KRA는 복수의 엔티티로 존재하는 것으로 설정한다.

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

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.

ㅇ 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 세션키를 KRA 엔티티 수 만큼 부분 세션키를 생성(D)
- 생성된 부분 세션키는 KRI에 명시된

KRA 암호용 공개키로 암호화된 후 역시 KRI에 명시된 KRC의 암호용 공개키로 이중 암호화한다(E).

- 송신자는 A, B, C, E 정보를 수신자에게 전송한다.

○ 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 정보 E를 사용하지 않는다.

○ 수신자 복구 요청

수신자가 자신의 암호용 개인키의 분실로 인하여 수신자가 수신 메시지 정상 처리를 할 수 없게되거나 송신자가 인트라넷 관리 규정을 위반하여 인트라넷 관리자의 임부 중 하나인 키 복구 작업을 위하여 송신자의 메시지에 대한 복구를 KRC에 요청한다. 이 과정에서 사용자 또는 인트라넷 관리자는 E의 내용을 사용하여 KRC에게 키 복구 요청 메시지를 전송한다.

○ KRC 복구 요청

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

○ 복구 처리

KRC는 사용자(수신자) 및 인트라넷 관리자 즉, KRC 관리자로부터 복구 작업 요청이 수신되면 요청에 대한 신분 확인 과정을 거친 후 KRA 엔터티들에게 암호화된 부분 세션키를 보내어 복호화 하도록 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.

7. 키 복구 프로토콜

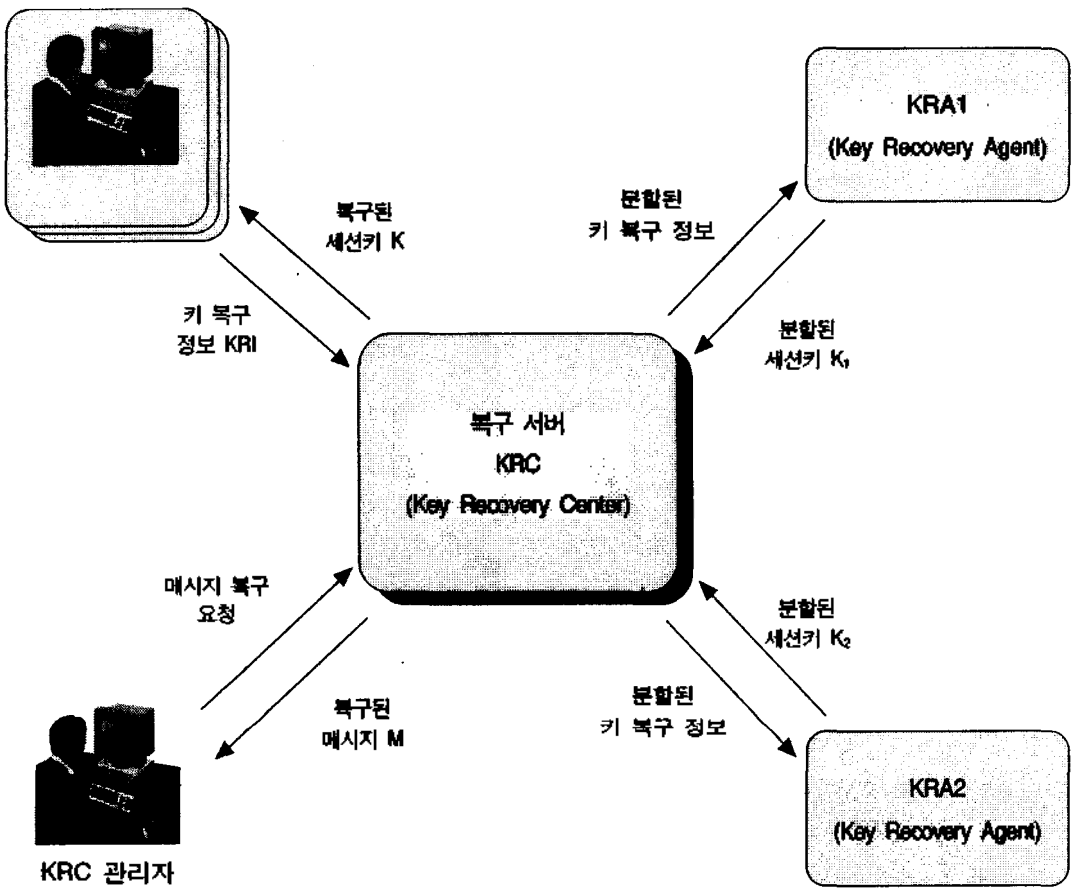
제안한 키 복구 방식에 대한 기본 프로토콜은 전체 시스템의 구조상 구성 요소, 단계별 프로토콜 및 기본적인 프로토콜 데이터 단위(PDU : Protocol Data Unit)로 구분하여 논한다. 특히, PDU 부분은 설정 시 고려 사항을 중심으로 논한다. 수신 메시지 정상 처리의 프로토콜 명세는 일반 암호 송수신 프로토콜 명세와 동일하여 본 논문에서 생략한다.

7.1. 키 복구 시스템의 구성

<그림 2>는 키 복구 시스템 구성도로 시스템을 구성하는 요소는 5가지로 이 중 전자 문서 송수신 부분은 생략하였다.

▶ **사용자 S/W** : 사용자가 수신된 전자문서를 복구할 수 없을 때, 복구 서버(KRC)에게 전자 문서 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 관



<그림 2> 키 복구 시스템 구성도

련된 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.)

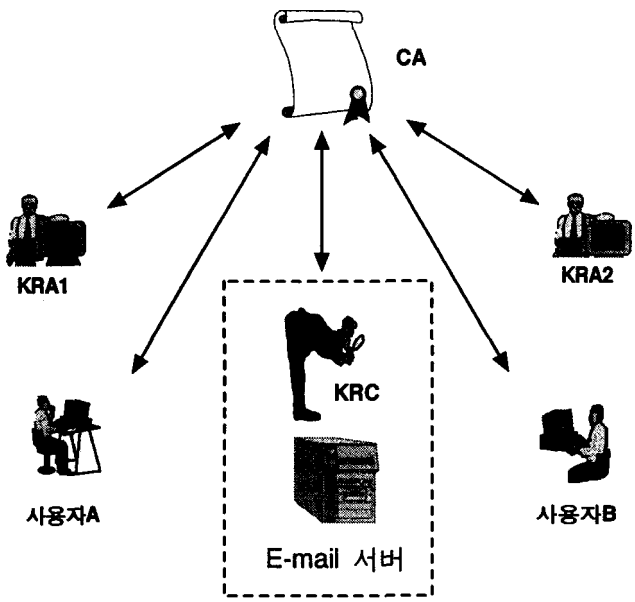
7.2. 키 복구 환경 설정(초기화) 프로토콜

<그림 3>은 복구 시스템 초기화에 관한 부분으로 초기화 과정에 수행하는 작업을 정의하였다.

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 인



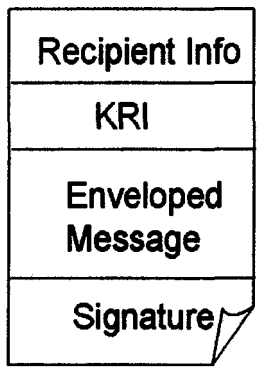
<그림 3> 복구 시스템 초기화

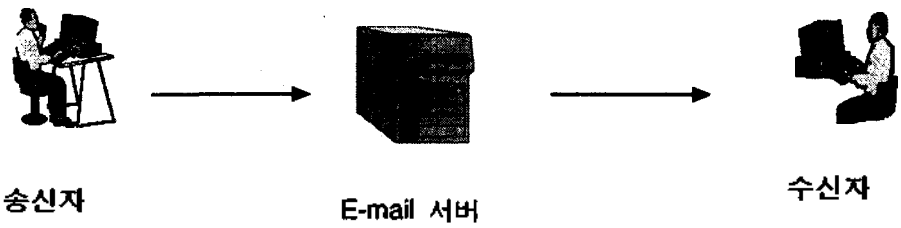
증서 발급 요청하며, 이때 CA는 사용자 공개키 인증서를 생성하는 과정에서 KRC, KRA1, KRA2의 정보를 공개키 인증서 확장 필드에 입력하여 발급한다.

7.3. 메시지 생성 및 송신 프로토콜

<그림 4>는 메시지 생성 및 송신 과정에서 작업 수행 참여 시스템에 관한 사항이다. 다음의 내용은 메시지 생성 및 송신 프로토콜에 관한 프로토콜 명세의 주요 내용이다.

① 메시지 원문을 압축한다. ⇒ Z
② 임의의 세션키를 생성한다. ⇒ K (DES 키)





<그림 4> 메시지 생성 및 송신 과정

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, 전자문서 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.

7.4. 수신자 복구 요청 프로토콜

<그림 5>는 수신자 측에서 복구 요청하는 경우, 관련 과정을 도식화한 것이다.

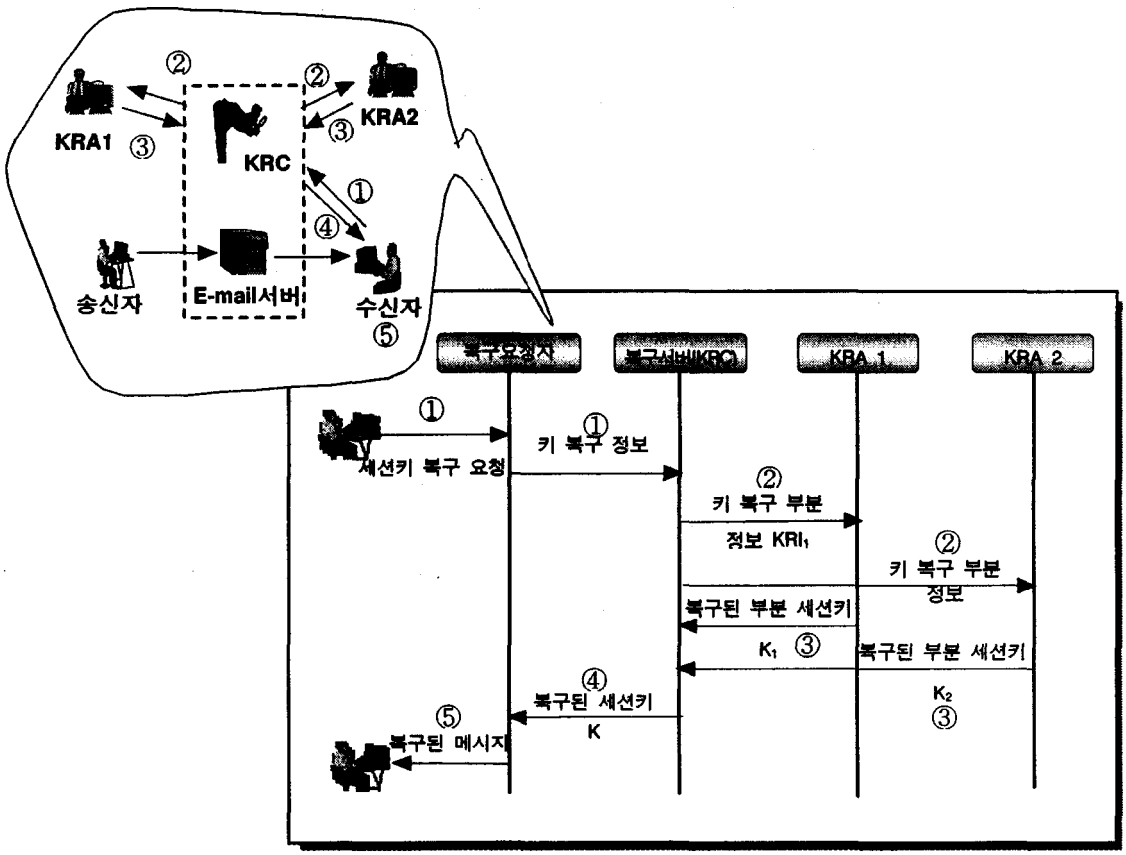
수신자가 정상적으로 암호문을 해독할 수 없는 상황인 경우,

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.

7.5. KRC 복구 요청 프로토콜

기업정보망 정보 관리 정책 중 키 복구 정책에 따라 인트라넷 관리자 즉, 기업정보망 관리자는 송신자의 특정 메시지를 전자우편(E-Mail) 서버에 요청한다.

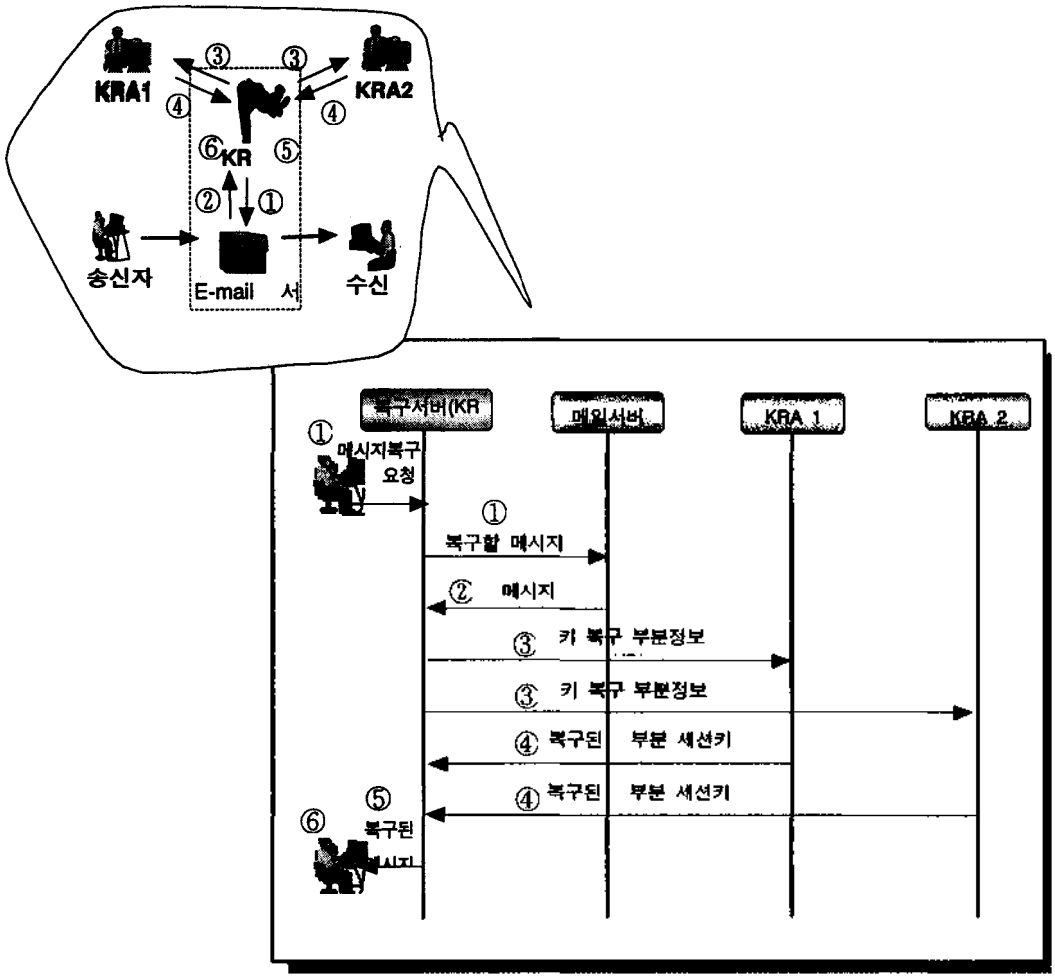
① KRC는 복구할 메시지인 송신자의 특정 메시지를 전자우편(E-Mail) 서버에 요청한다.
② 전자우편(E-Mail) 서버는 KRC를 인증 후 요청한 메시지를 KRC로 송신한다.
③ KRC는 메시지에서 KRI 획득 후 각 KRA들에 암호화된 부분 세션키 복호화를 요청한다.
④ KRA는 요청 확인 후 암호화된 부분 세션키를 복호화하여 KRC에 응답한다.
⑤ KRC는 부분 세션키로부터 세션키 K를 복구한다.
⑥ KRC는 K를 이용하여 메시지 M을 복구하여 기업 책임자에게 암호 송신한다.



<그림 5> 수신자 복구 요청 구조

7.6. 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.



<그림 6> KRC 복구 요청 구조

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
}
```

8. 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 정보 시스템 환경에서의 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 내부망, 즉, 인트라넷에 적용될 수 있는 정보 시스템 보안 정책 중 키 복구 기술에 해당되는 정책 도출을 하였다. 기존 키 복구 솔루션 및 방식을 검토하였으며, 존재하는 문제점을 개선한 키 캡슐화된 키 복구 메카니즘을 제시하였다. 도출된 보안 정책에 대하여 제안한 키 복구 메카니즘을 적용한 시스템으로 기업 정보체계에서의 키 복구 시스템을 본 논문에서 제시하였다. 본 논문에서 제시한 시스템에 대하여 향후 시스템의 성능 분석과 정보보호 차원의 안전성 등을 검증하는 연구가 요구된다.

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, 제7권, 제4호, pp. 45-58, Dec., 1997.
[11] 임신영, 인터넷 관리자를 위한 보안 지침서, 1997.1.

저자 소개

임신영 (e-mail) sylim@econos.etri.re.kr
1983 건국대학교 공업화학과 학사
1985 건국대학교 화학공학과 석사
1992 건국대학교 전자계산학과 석사
1997 고려대학교 컴퓨터과학과 박사수료
1987~1998 한국전자통신연구원 부설 시스템공학연구소 선임연구원
1998~현재 한국전자통신연구원 전자상거래연구부 선임연구원

강상승 (e-mail) sskang@econos.etri.re.kr
1997 경북대 전자공학과 학사
1999 경북대 전자공학과 석사
1999~현재 한국전자통신연구원 전자상거래연구부 연구원

하영국 (e-mail) ygha@econos.etri.re.kr
1993 건국대학교 전산학과 학사
1995 건국대학교 대학원 전산학과 석사
1995~1998 한국전자통신연구원 부설 시스템공학연구소 연구원
1998~현재 한국전자통신연구원 전자상거래연구부 연구원

함호상 (e-mail) hsham@etri.re.kr
1977 고려대학교 산업공학과 학사
1983 고려대학교 산업공학과 석사
1995 고려대학교 산업공학과 박사
1979~1981 새한자동차(주)
1982~1998 한국전자통신연구원 부설 시스템공학연구소 전자거래연구팀 팀장
1998~현재 한국전자통신연구원 전자상거래연구부 전자거래연구팀 팀장

박상봉 (e-mail) sbpark@etri.re.kr
1974 고려대학교 산업공학과 학사
1976 고려대학교 경영학 석사
1975~1981 한국과학기술연구소 전자계산부
1982~1993 한국과학기술원 시스템공학센터
1993~1996 한국과학기술원 시스템공학연구소
1996~1998 한국전자통신연구소 부설 시스템공학연구소
1998~현재 한국전자통신연구원 전자상거래연구부 부장