[초청강연]

학 술 발 표 2

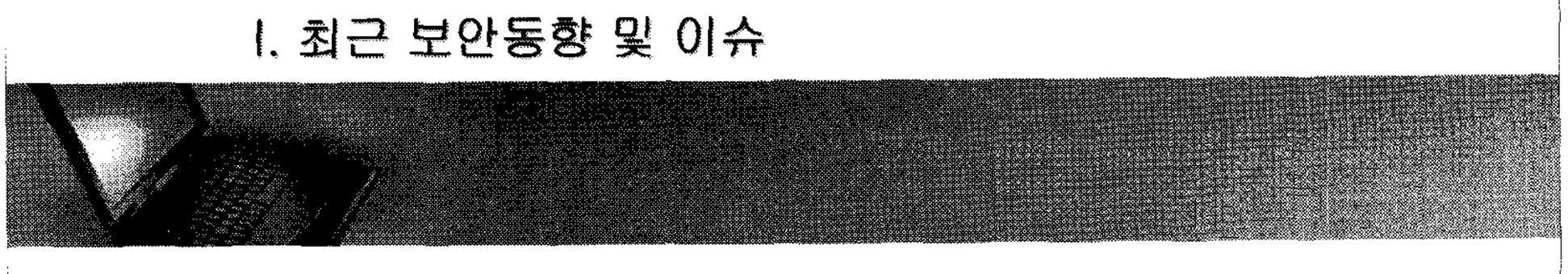
내부 정보유출 방지

- 인포섹(주) 전략컨설팅사업본부 수석 김선태 -

정보유출방지 전략 및 체계

2008. 07

목 차



I. 최근 보안동향 및 이슈

1. 최근 보안 이슈의 변화
2. 보안사고 동향
3. 정보유출의 원인과 배경
4. 정보유출 방지의 필요성

1. 최근 보안 이슈의 변화

최근 IT 기술의 발전에 따라 사회의 패러다임이 정보 위험사회(Risk Society)로 변화됨에 따라 보안위협의 변화에 맞는 보안대응의 변화가 필요함

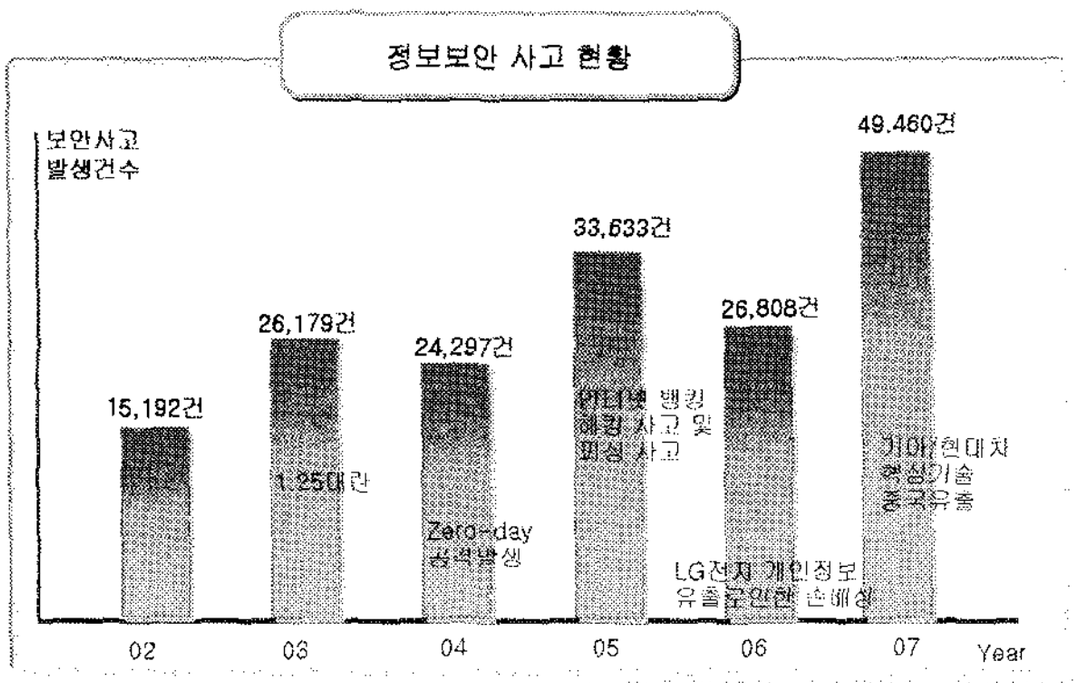
	과거	미래
변화	• IT Infra 중심의 보안위협 • - 서버, 네트워크, PC 등 • 단순 자기 과시형 공격 위협	• 특정정보에 대한 위협(개인정보, 기술정보 등) • - New Technology(Web 2.0, Mobile, VoIP, UCC etc) • 금전적/상업적 목적 추구
	• Compliance 요구 • - 기본적 규정(정보통신망법 등)으로 제재	• 전문화된 규정으로 Compliance 요구 강화 • - 개인정보보호법, 산업기술유출방지법, SOX 등
대응	• **이원화**: 기술적(IT) 보안, 인적/물리적 보안 • IT **인프라** 중심의 대응	• **일원화** 관리: 기술적(IT)/인적/물리적 보안 • **IT 서비스**, 특정정보 중점대응(개인정보/기술정보 등)
	• **선 서비스 개시 후** 보안 대책 수립	• **선 보안 검토 후** 서비스 개시

향후 Security 전망

- 사이버 침입 위협(해킹, 바이러스)의 지속적 증가
- 정보 위험사회(Risk Society)로 변화
  → 기업의 법적/윤리적/사회적 책임 증가(내부정보 유출방지, 개인정보 보호)

2. 보안사고 동향

정보화 사회의 역기능인 보안사고는 계속 증가하는 추세이며, 개인정보 및 중요기밀 정보의 유출을 통한 금전적, 경제적 피해가 증가하여 제도적 규제가 강화되는 등 기업의 윤리적/사회적 책임이 증가되고 있음



연도	중요 사고내용
'03	▪1.25 인터넷 대란 ▪MS Blaster웜 발생
'04	▪Zero-Day 공격 최초 발생
'05	▪인터넷 뱅킹 해킹, 공공사기(피싱) 첫등장 ▪SK컴즈, 넥스 : 서버해킹 웜 배포
'06	▪LG전자 입사지원자 개인 정보 유출사고 ▪삼성전자 휴대폰 기술유출 사고 발생 ▪중국발 웹 해킹 지속 증가(악성코드 진화)
'07	▪국민은행 고객정보유출로 인한 배상 ▪기아/현대차 핵심기술 중국유출

시사점

- 해킹사고는 지속적 증가추세이며 DDoS, 악성코드 등 새로운 공격유형으로 진화
- 고객정보, 내부정보의 유출사고로 인한 직간접 기업손실 발생 증가

3. 정보유출의 원인과 배경

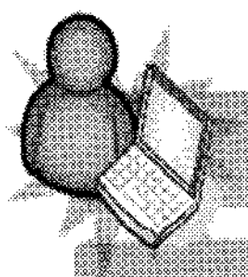
정보유출의 특징은 인적 통제의 한계, 기술적/환경적 변화, 정보의 특성에 따른 완전방지의 어려움 등 기존 정보보호와 차이점이 있음. 따라서 정보유출 방지를 위한 투자와 노력, 그리고 적극적 대응이 필요함

정보유출의 원인

- **인간의 본능과 기업의 이익의 충돌로 인한 괴리가 발생**
- **정보의 특성상 형체가 없으며, 유출 및 침해는 용이하지만 발견은 어려움**
- **과학기술의 발달과 보호의 한계로 인해 냉전시대의 정보기술이 산업스파이 장비로 활용**
- **OA기기의 적극적 활용 및 인터넷의 보편화로 인해 정보접근경로가 다양해짐**

정보유출로 인한 산업적 피해

- **독일의 경우 산업스파이로 인해 매년 5만명의 실직자가 발생(독일정보부장)**
- **우리나라 관계기관에서 추정한 기술유출 피해는 지난 2003년 이전 6년간 약 22조원으로 예상**
- **하이테크업체의 경우 매출액의 0.1% 직접손실과 간접비용을 포함하여 0.4%의 피해 발생(미국 전자협회)**



발생횟수는 적으나, 발생시 미치는 영향은 가장 크다

위험요소가 구체적이며 명확하지만, 통제는 어렵다

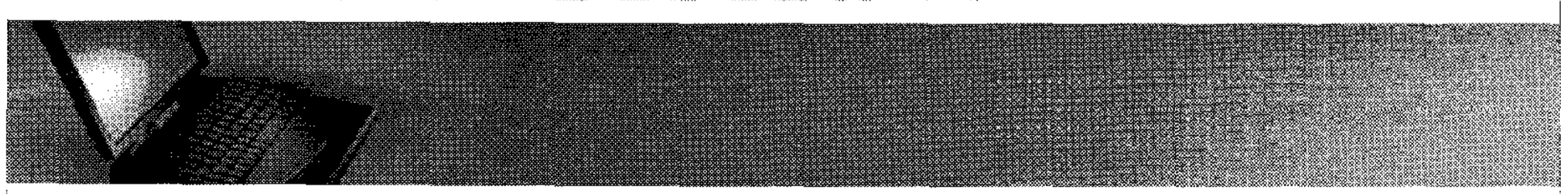
업무환경 전산화로 인한 대용량의 정보유출이 가능하다

정보의 처리, 복사, 전송 등의 정보유통의 편리성 증대로 인한 다양한 유출경로가 존재한다

실제 유출사고가 발생할 지라도 인지가 어렵다

어떠한 경우이든 정보유출의 원인은 사람의 문제이다

II. 내부정보유출 관련 법률 및 사례



1. 내부정보유출 관련 법률 및 피해규모
2. 내부정보유출 관련 처벌 규정
3. 내부정보유출에 의한 피해 사례 및 특징
4. 산업기술 유출방지 체제

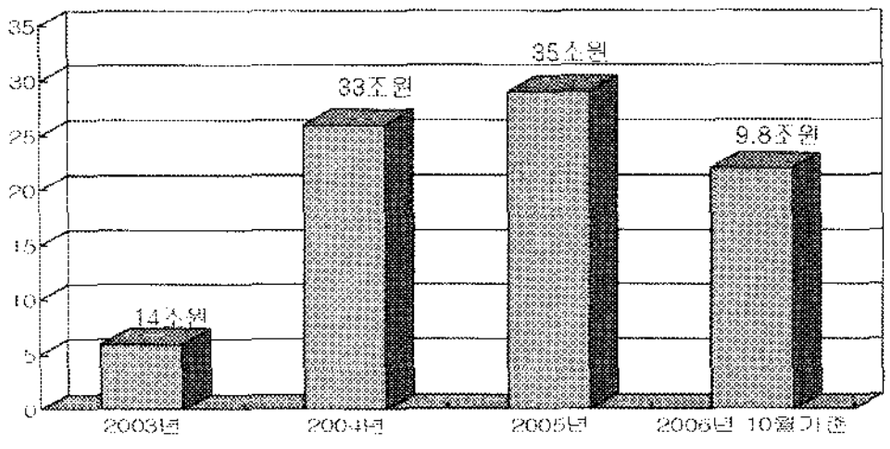
1. 내부정보유출 관련 법률 및 피해규모

최근 인터넷과 IT기술이 발전함에 따라 정보 유출의 방법도 다양해 지고 있으며, 대부분전/현직 임직원에 의한 내부정보 유출로 이로 인한 경제적 피해규모도 기하 급수적으로 증가하고 있습니다.

■ 부정경쟁 방지법 및 영업 비밀 보호법

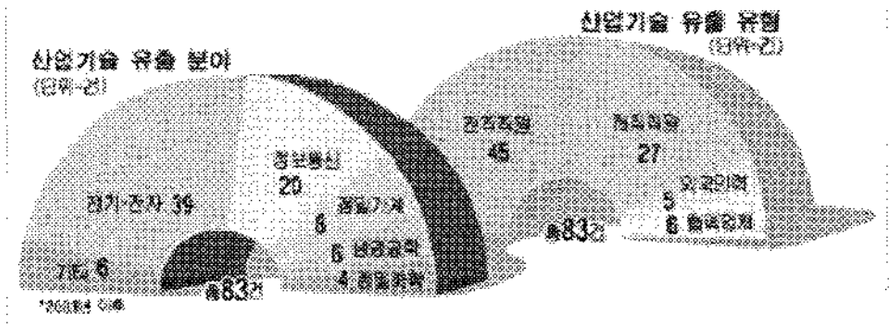
구분		한국	미국	일본
		영업비밀보호법	경제스파이법	부정경쟁방지법
보호 대상		기업의 비밀 (Know-How포함)	기술 또는 영업상 모든 정보	기술 또는 영업상 정보
법정형	국내	• 7년 이하 징역 또는 재산상 이득의 2배 이상	• 개인: 15년 이하의 징역 또는 50만불 이하 벌금 • 법인:1천만불 이하벌금	• 개인: 3년 이하의 징역 또는 3만엔 이하의 벌금
	국외	•5년 이하의 징역 또는 재산상 이득액의 2배 이상 10배 이하	• 개인:10년 이하의 징역 또는 50만불 이하벌금 • 법인:500만불 이하 벌금	• 법인: 3억엔 이하 벌금

■ 경제적 피해 규모(국내)



※ 출처: 한국산업보안연구소 (2006.10)

■ 피해 유형별 분류(국내)



※ 출처: 국가정보원(2006)

■ 산업 기술유출 방지법

- 산업기술유출방지법통과(4월 28일 시행)
- 현행법상 영업기밀유출방지법 외 처벌 조항 강화 (형량 7년 이하 7억 이하의 형사처벌)
- 임직원의 비밀 누설에 의한 처벌 조항 신설(형량5년 이하)

2 내부정보유출 관련 법률 및 처벌

2.1 부정경쟁방지 및 영업비밀 보호에 관한 법률

❑ 영업 비밀

영업비밀(Trade Secret)이란 공연히 알려져 있지 아니하고, 독립된 경제적 가치를 가지는 것으로서 상당한 노력에 의하여 비밀로 유지된 생산방법 · 판매방법 기타 영업 활동에 유용한 기술상 또는 경영상의 정보를 의미함 (부정경쟁 및 영업 비밀보호에 관한 법률 제 2조 제 2호)

❑ 영업 비밀의 종류

구분	기술상의 정보내용	경영상의 정보내용
주요내용	• 시설 및 제품의 설계도 • 물품의 생산 / 제조방법 • 물질의 배합방법 • 연구개발 보고서 및 데이터	• 전략 및 중요 계획 • 관리정보 • 고객 명부 • 매뉴얼 등 중요자료

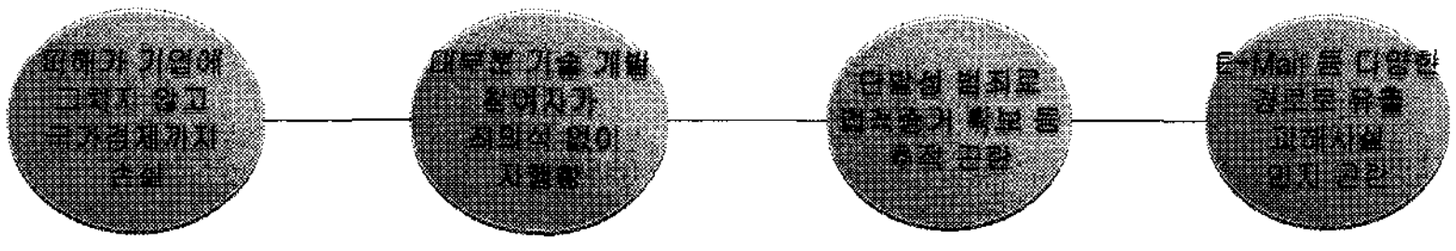
❑ 영업 비밀 침해 행위에 대한 구제 수단

구분	내용
침해행위	▶ 국내 : 영업비밀을 취득 사용하거나 제 3자에게 누설하는 행위 ▶ 국외 : 외국에서 사용하거나, 외국에서 사용될 것임을 알고 제 3자에게 누설하는 행위
처벌형량	▶ 국내 : 5년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하의 벌금 ▶ 국외 : 7년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하의 벌금

2.2 산업기밀 유출 방지법

❑ 산업기술의 부정한 유출을 방지하고 산업기술을 보호함으로써 국내 산업의 경쟁력을 강화하고 국가의 안전보장과 국민경제의 발전에 이바지함을 목적으로 제정됨 (2007년 4월 28일부터 효력이 발생됨)

2.3 내부 정보 유출에 의한 피해 특징 및 사례



사례	유출 경로	내용	기타
택지지구 개발 정보 유출 (2007.1)	내부 직원에 의한 정보 유출(중요 정보에 대한 접근 절차상 허점)	중요 정보에 대한 접근이 용이한 절차상 허점을 이용, 관련 직원이 개발 정보를 유출하여 부당이득을 취한 정보 유출 사건	핵심정보에 대한 등급별 분류 및 등급별 접근제한 필요
국내 H사의 자동차 핵심 기술 유출시도(2005.10)	외부 저장매체(CD-RW)를 이용	H사의 협력업체 직원이 자동차 핵심 기술을 CD-RW를 이용하여 CD에 저장, 중국으로 유출을 시도하다 적발	외부 저장매체사용 시 승인절차 필요(USB, 프린터 사용 등)
이통사의 고객정보 유출 (2004)	DB정보 유출	2004년 국내에서 발생한 대표적인 불법 내부정보 유출 사례로 현직 이동통신사 간부가 자사의 고객정보 600여만 명의 개인정보를 불법으로 유출해, 수억 원을 받고 매매한 사건	DB 감사 및 모니터링 필요
핵무기 관련 정보 유출 (2004)	이 메일을 통한 정보 유출	2004년 미국 ' 미 핵 연구소 이메일을 통한 정보 누출' 사건이 여러 차례 전송된 사실이 드러났고, 조사 결과 핵무기 시설에 관한 비밀정보가 이메일 시스템을 통해 외부로 전송된 사건 발생	이 메일 및 웹 메일 모니터링 필요

4.1 산업기술 유출방지 체계 - 관리시스템(사례)

산업 기술 유출 예방을 위해서는 최고경영층의 지시에 따라 조직 및 제도를 개선하고 기밀 관리 시스템을 도입하여 각종 기밀자료에 대한 접근 차단과 내부 기밀 문서의 외부 유출 방지를 위한 대책을 수립하고 보안 관리 감독 체계를 강화하여 비밀 유지계약 수립과 정기 보안 관리 교육을 강화해야 한다.

산업 기술 유출 예방

산업기밀 관리체계(관리시스템)

조직 및 제도	기밀 관리 시스템	보안감독체계
* 보안관리 규정 마련 * 보안담당부서 설치 * 보안담당자 지정 * 정기보안점검 * 정기 보안감사	* 카드키 설치 (예 : 연구실, 실험실 등) * 정보보안시스템 구축 (예 : 침입차단시스템, 침입탐지시스템 등) * 문서관리시스템 (예 : 보안등급부여 등) * DRM(디지털저작권관리) 솔루션 도입 * 문서세단기 * 패스워드 및 이동식 디스크관리 (예 : USB, 메모리스틱)	* 입사시 비밀엄수 서약작성 * 퇴사시 비밀유지 및 겸업금지 각서 * 거래업체 비밀유지계약 * 정기 보안관리 교육 * 연구노트, 일지 작성 * 방문자 출입통제

※ 출처: 한국산업기술진흥협회(2006.8)

4.2 내부 위험 방지대책(해외 권고안)

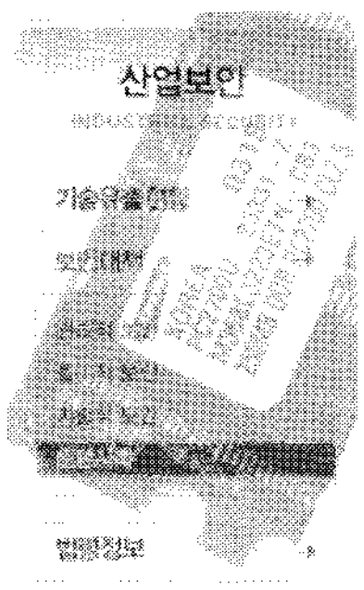
「월 스트리트저널(The Wall Street journal)」誌 「내부로부터의 위협」 題下 (06년 1월)

내부자에 의한 기업 보안 위협 방지책

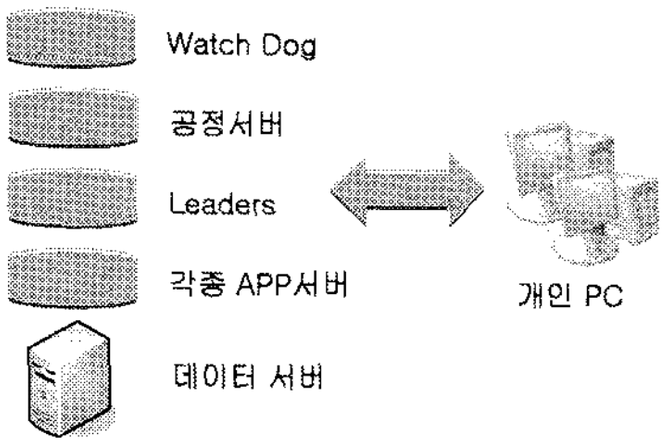
- **위협 요인 파악** ※ 잠재 위협 목록 파악 및 영향 분석, 피해 정도 계량화, 기술적 방법 또는 '비밀 유지 협약서' 등 최소한 법적 조치 마련
- **직원 신상파악** ※ 보안 부서 등 비밀 업무를 취급하는 부서의 근무자 채용 시 신원 배경 확인
- **보안 교육 실시** ※ 보안에 관한 자신의 역할과 책임을 이해 시키고, 보안 규정을 수용하고 따를 수 있도록 설득시킴
- **등급별 자료 분류** ※ 비밀분류 시스템을 갖춰 각 단계별 접근등급과 통제 수준 설정 (ex. Confidential, Secret, Top Secret –美 정부-)
- **중요자료 암호화** ※ 정보 중요도에 따라 분류한 후 합리적 기준에 따라 일반 사용자의 접근권한 제한 모든 정보에 접근 할 수 있는 시스템 관리자에 대한 특별 관리책 마련
- **네트워크 감시** ※ 외부 인터넷 망으로 나가는 e-mail이나 쪽지, 메시지 등을 감시 할 수 있는 소프트웨어 설치 또는 개인용 컴퓨터에서 실행되는 프로그램을 확인하여 특정 문서에 접근/유출행위를 통제 함

※ 출처: The Wall Street Journal (2006.1)

산업 기술이 발달함과 동시에 산업보안의 중요성과 위협 정도가 높아지고 있는 반면 산업 보안을 구체적으로 실현하기 위한 기술 유출 방지 대책 현실은 여전히 미숙한 상태임 이를 개선하고자 개선전에 개인 PC에서 중요 DB및 데이터서버에 접속하는 방법을 개선하여 Data Document Application을 이용한 접속을 통해 접근 제한을 구성함

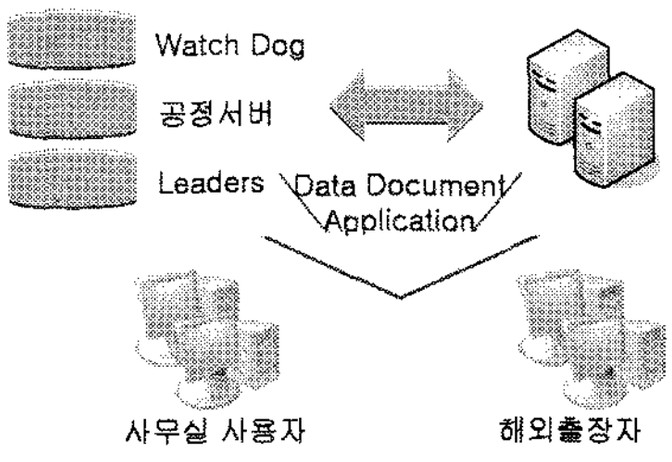


AS-IS



※ 데이터 및 문서 개인 PC에 보관 가능
※ 어플리케이션을 개인 PC에서 직접 구동

TO-BE

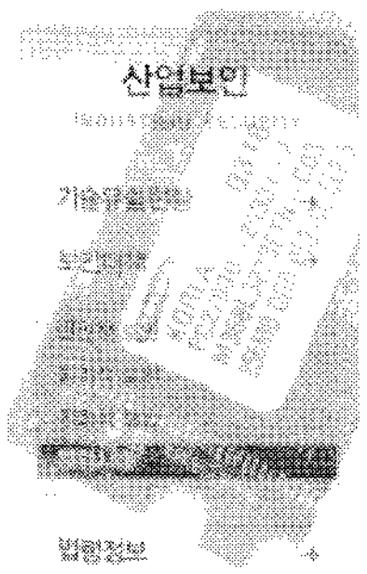


※ 모든 직원들은 데이터를 중앙의 서버에 보관
※ 어플리케이션 자체를 중앙의 서버에서 구동
※ 실제 데이터는 중앙서버에서 처리
※ 사용자에게는 화면 값 만을 전송
※ 사용자에 의한 클립보드, 하드디스크, 기타 저장장치를 이용한 자료 외부반출 제한

※ 출처: 국가정보원(NIS) 산업기술 정보센터

4. 산업기술 유출방지 사례 - 관리적 대책

보안규정을 마련하여 보안 절차 표준화를 구성하여, 회사 전반적인 보안업무 총괄 기준을 산업보안 관리 규정으로 삼고 회사 출입관리, 물품 반출입 규칙, 자료 유출방지 관리 절차, 전산 보안사항 표준화 등을 구성하고, 보안 점검 및 순찰을 강화하고, 보안 실무 지침서와 보안수첩 등의 보안책자를 발행하여 보안의 중요성을 교육한다.



※ 출처: 국가정보원(NIS)
산업기술 정보센터

보안규정

❑ 보안 절차 표준화

※ **산업보안 관리규정**
회사 전반적인 보안업무에 관한 총괄 기준

※ **출입자 관리 규칙**
회사 출입보안에 관한 전반적인 절차

※ **물품 반출입 규칙**
회사 내/외부의 반출입 절차

※ **자료 유출 방지 관리 기준**
회사 중요 자료에 대한 보안관리 절차

※ **전산 보안 관리 규칙**
전산 보안에 관한 사항 표준화

보안점검

❑ 보안 점검 및 순찰

※ **정기점검 : 매월 보안의 날 야간 보안 점검**

※ **비정기 점검 : 불시 보안 점검 실시**

※ **주요점검 내용**
책상 위 서류방치, 휴지통에 서류 원형 방치상태
비밀자료 보관상태, 개인 PC보안상태
사무실 및 보관함 시건 상태

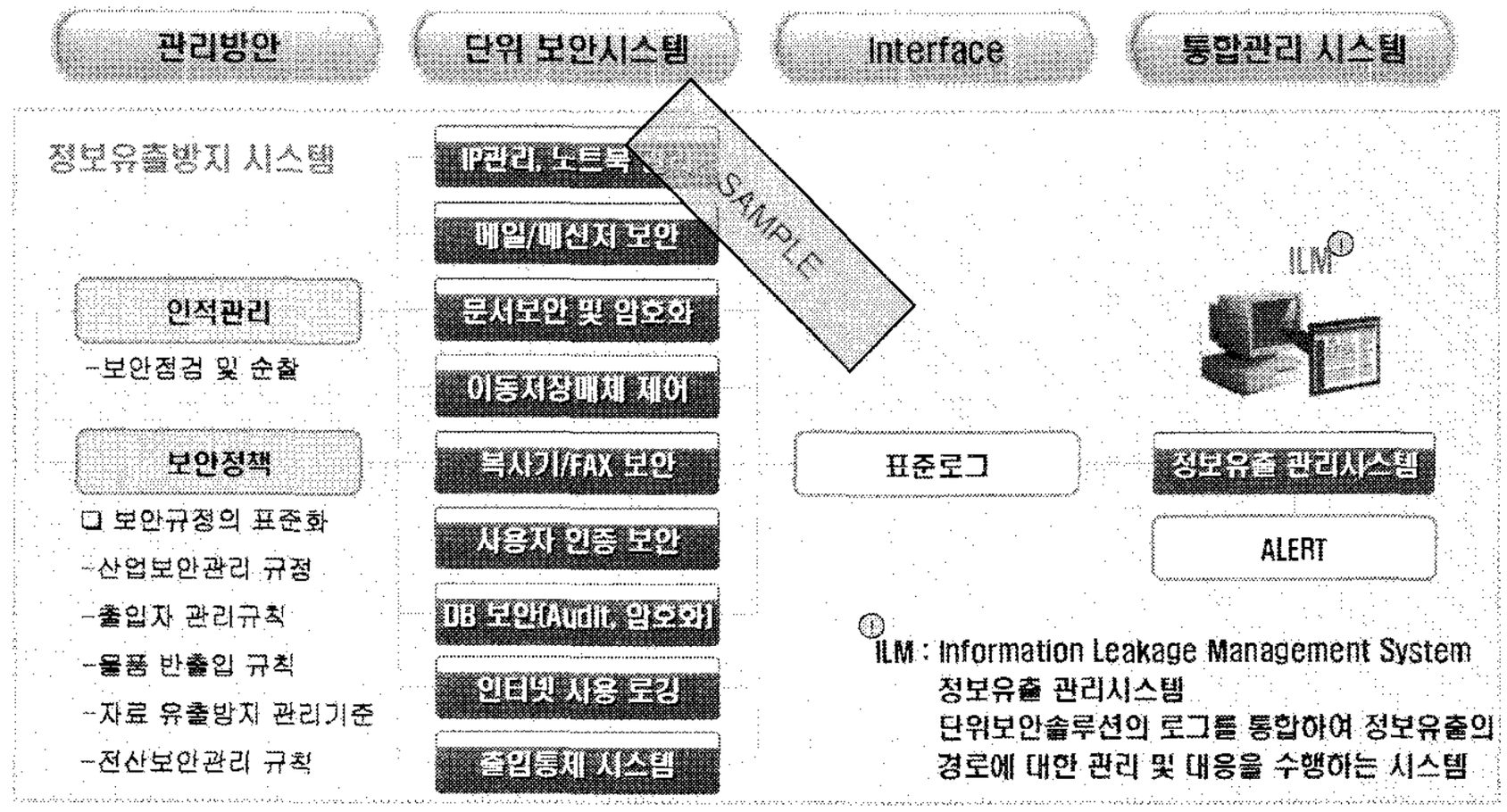
※ **조치사항**

보안스티커 부착경고 ⇨ 전사공지 ⇨ **출문시 보안요원 확인**

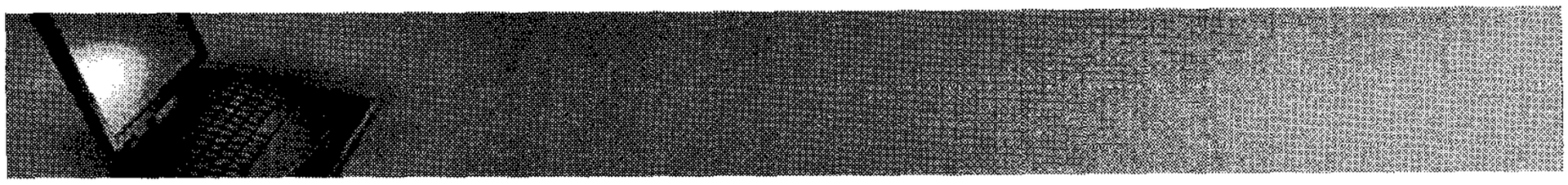
※ **보안책자 발행**
1. 보안실무 지침서　　2. 보안수첩

4. 산업기술 유출방지 사례 - 통합관리시스템

정보유출방지 시스템은 다양한 보안솔루션이 적용될 것입니다. 따라서 이러한 솔루션이 제공하는 정보를 통하여 종합적인 정보의 유출 관리 및 대응이 가능한 통합관리 시스템이 필요합니다.



3. 내부정보 유출방지 체계수립



3.1 정보유출방지의 특징

3.2 내부정보유출방지 체계

해커 등으로부터 기인하는 외부의 위협과는 달리 내부정보 유출은 다음과 같은 특성을 지니고 있으며, 이러한 특성을 고려하여 4단계 정보유출방지 전략을 토대로 수립합니다.

기업내부 정보유출 특성

발생횟수는 적으나, 발생시 미치는 영향은 가장 크다

위험요소가 구체적이며 명확하여도, 통제는 어렵다

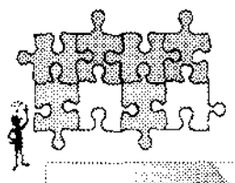
업무환경 전산화로 인한 대용량의 정보 유출이 가능하다

정보의 처리, 복사, 전송 등의 정보유통의 편리성 증대로 인한 다양한 유출경로가 존재한다

실제 유출사고가 발생할 지라도 인지가 어렵다

어떠한 경우이든 정보유출의 원인은 사람의 문제이다

특성고려



정보유출방지 전략

1 단계 업무를 파악하라 !
(보호방안의 현실화 및 구체화)

2 단계 보호할 대상을 명확히 하라 !
(대상의 구체화)

3 단계 사람이 우선이다 !
(임직원 변화관리, 업무변화 최소화)

4 단계 예방, 추적뿐 아니라 예측가능 하여야 한다 !
(유출에 대한 관리 및 대응)

3.2 내부정보유출방지 체계 - 수립절차

내부정보 유출대응 체계 진단을 통해 내부 중요 정보의 유출 경로와 발생 가능성에 대한 수준진단을 수행하고, 사고 예방 및 모니터링을 위한 기술적/관리적/물리적 관점의 대책방안을 수립합니다.

I. 환경 및 현황분석	II. 시나리오 정의 및 위험도 평가	III. 개선 및 통제방안 수립	IV. 정보유출방지체계 구축운영
• IT및 기업환경 조사 • 보안환경 파악 • 내부정보유출 대응체계 현황 파악	• On-Line 내부정보 유출 점검 및 평가 • Off-Line 내부정보 유출 점검 및 평가 • 주요 위협 시나리오 선정 • 내부정보 유출대응 수준 평가	• 위험 대응을 위한 개선방안 도출 • 즉시 및 단/중기 이행과제 선정 (솔루션 포함) • 이행계획 권고안 작성	

3.2 내부정보유출방지 체계 - 내부정보 등급 분류

정보유출방지의 대상이 되는 보호대상, 즉 중요정보를 정의하고 그에 대한 분류를 함으로써 비용대비 효과적인 정보유출방지 시스템 설계의 토대를 마련합니다.

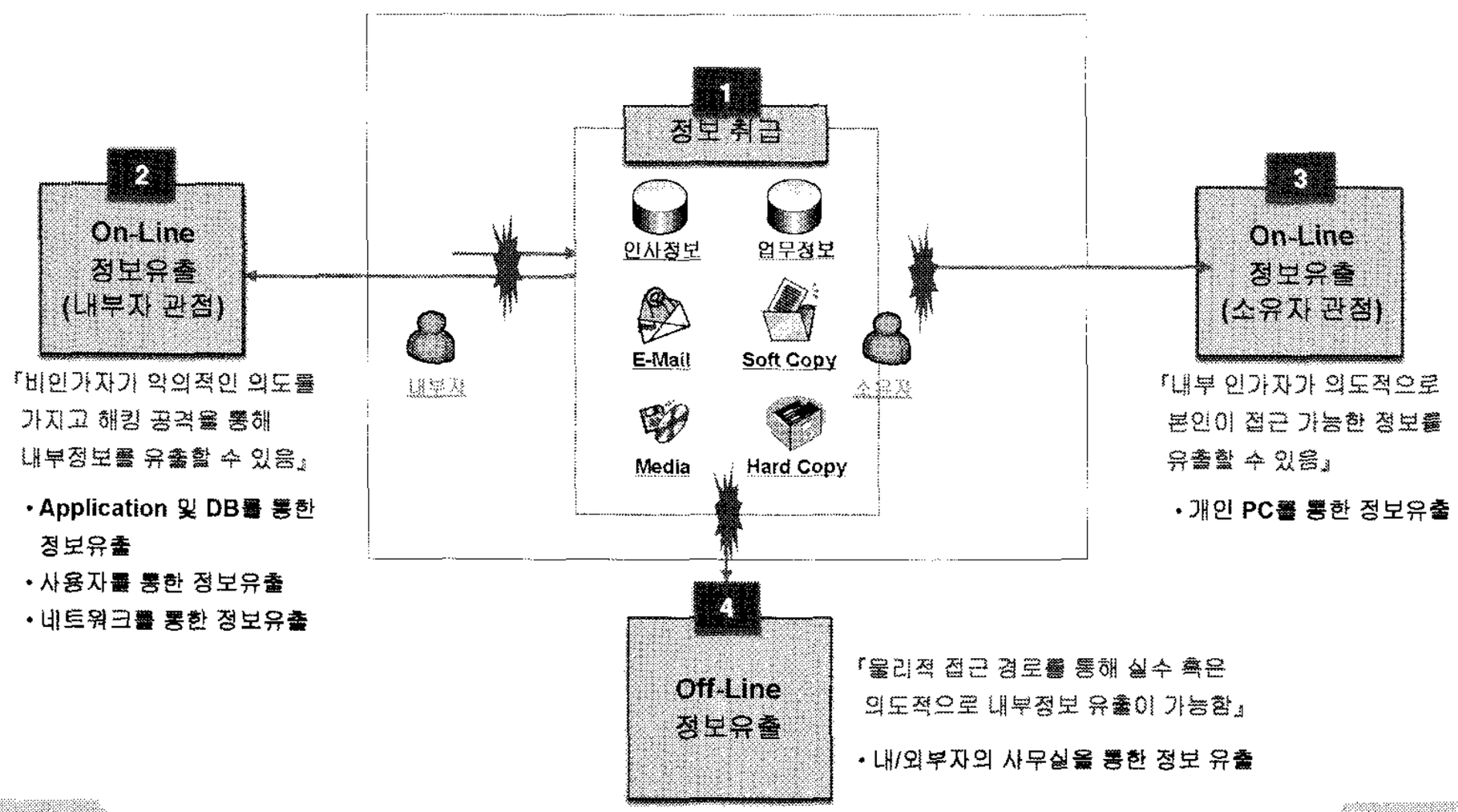
IT lifecycle 상에서 발생할 수 있는 위협요소와 "산업기술 유출 방지법", "부당경쟁 방지 및 영업비밀 보호법"을 고려하여 정보 등급체계를 정의하여 분류

① 정보 등급체계	등급 설명	예방 정보
Special Controls	생존의 위협	새로운 공정이나 제품의 비밀 공식이나 비법
Company Confidential	심각한 손실	제품의 공정, 고객 리스트가 기업의 가치를 좌우할 정도로 중요한 것
Private Confidential	규명할 수 있는 피해, 혹은 문제점의 발생원인	개인적인 데이터, 가격의 설정

① 미국 국방부가 국가 산업안전 프로그램 운영 지침의 분류 기준

3.2 내부정보유출방지 체계 - 진단 및 평가

정보유출 발생 경로 및 주체를 고려하여 다음의 4가지 영역에 대한 진단 및 평가를 수행합니다.



「비인가자가 악의적인 의도를 가지고 해킹 공격을 통해 내부정보를 유출할 수 있음」

- **Application 및 DB를 통한 정보유출**
- 사용자를 통한 정보유출
- 네트워크를 통한 정보유출

「내부 인가자가 의도적으로 본인이 접근 가능한 정보를 유출할 수 있음」

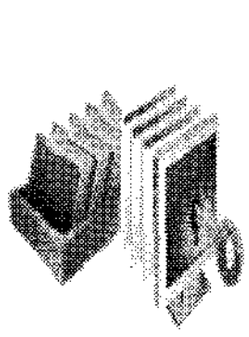
- 개인 **PC**를 통한 정보유출

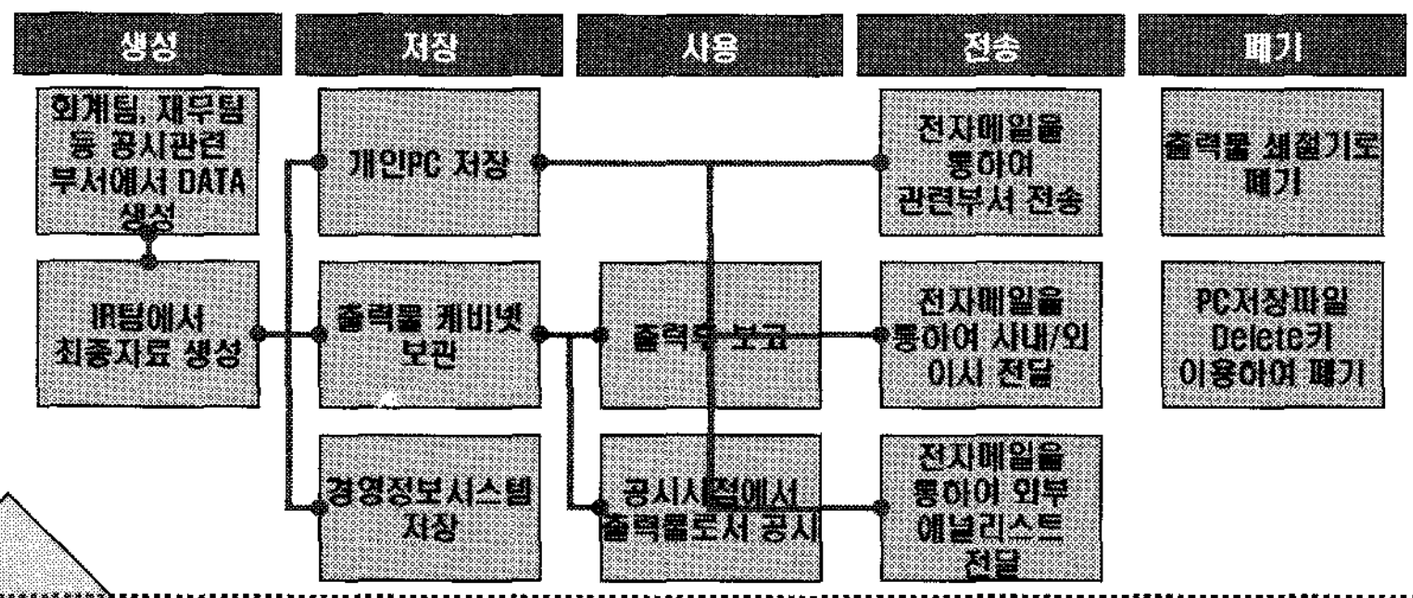
「물리적 접근 경로를 통해 실수 혹은 의도적으로 내부정보 유출이 가능함」

- 내/외부자의 사무실을 통한 정보 유출

3.2 내부정보유출방지 체계 - 시나리오 정의 및 위험도 평가

중요정보를 단위정보로서 파악하는것이 아닌, 임직원의 업무속에서 파악하여야만 적합한 유출방지 시스템을 설계할 수 있습니다. 그에 대한 가장 효과적인 방법은 대상 정보의 Life Cycle을 파악하는 것입니다.

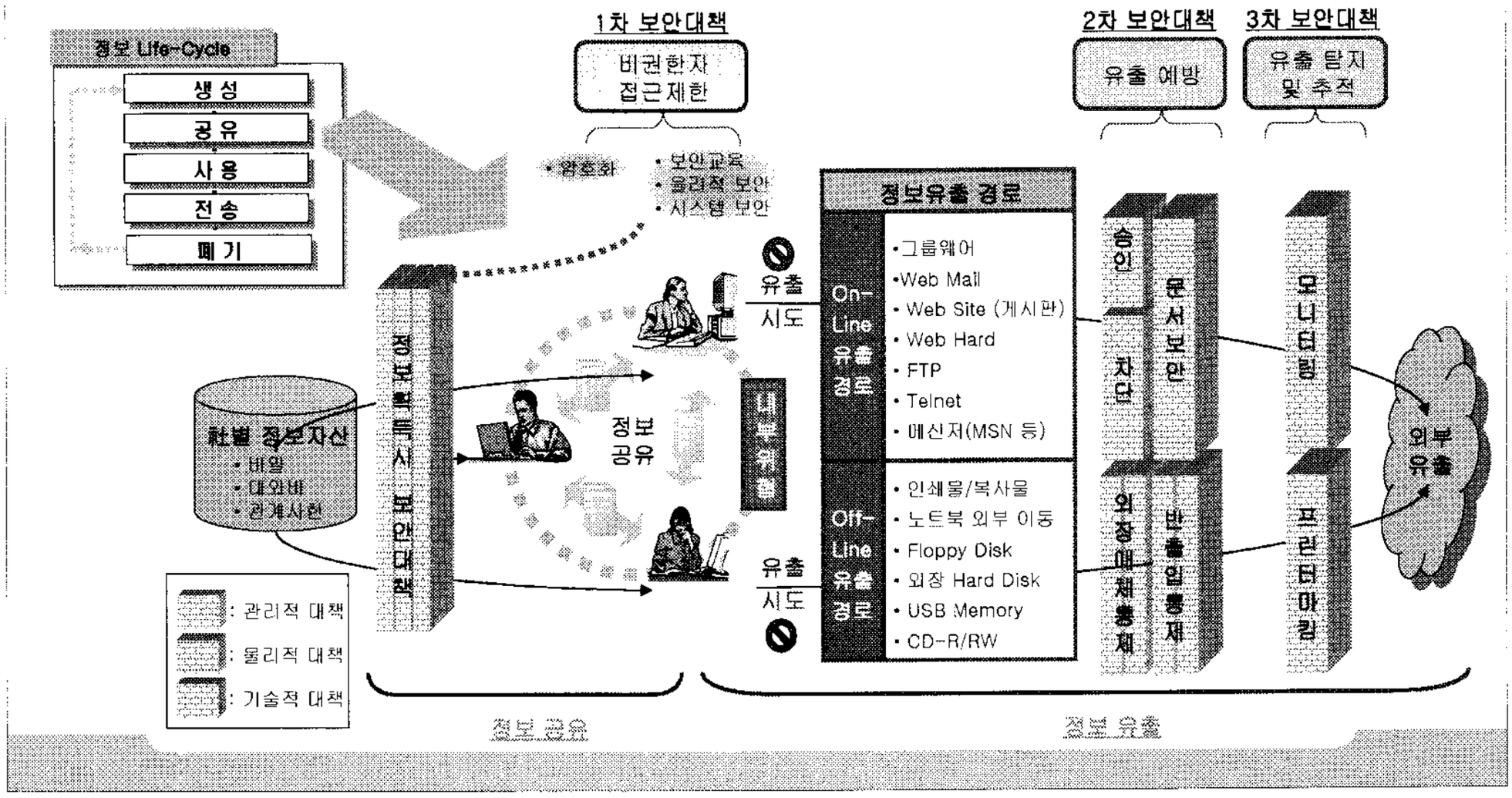




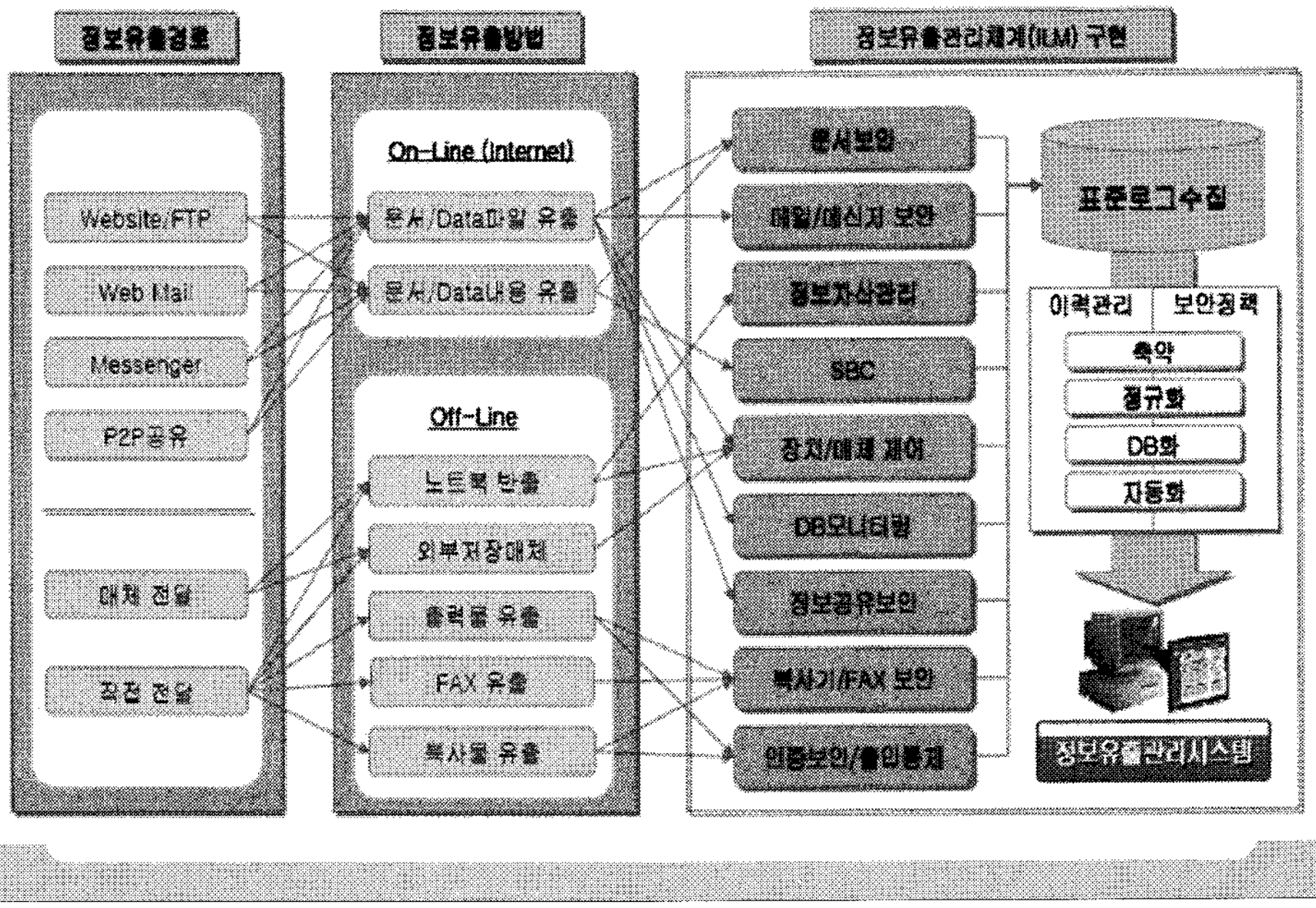
	유출 시나리오	정보의 중요도	발생가능성	발생시영향	위험도
저장	개인PC의 패스워드 미설정으로 허가되지 않은 접근에 의한 유출	Medium	Medium	High	Medium
전송	허가되지 않은 이동 저장매체에 복사된 정보의 허가되지 않은 접근에 의한 유출	Medium	High	High	High

3.2 내부정보유출방지 체계 - 개선 및 통제방안 수립

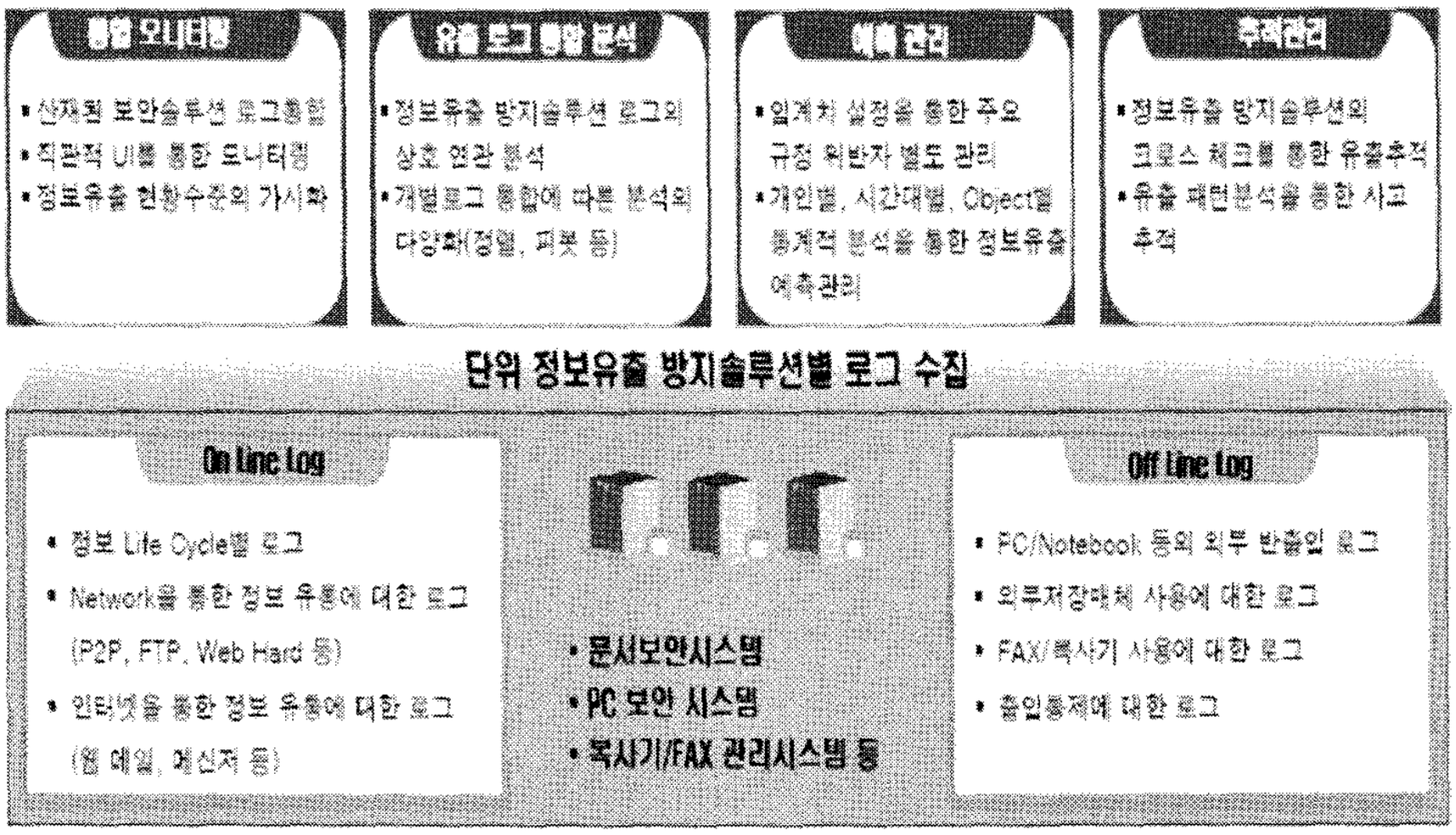
정보분류 기준 사외비 이상의 등급에 해당하는 내부 정보유출에 대응하기 위해서는 On-Line과 Off-Line 상에서의 내부정보 Life cycle 관점에서의 물리적, 관리적, 기술적 보안위협을 파악하여 보안대책을 수립하는 것이 효과적입니다.



3.2 내부정보유출방지 체계 - 정보유출관리 시스템



3.2 내부정보유출방지 체계 – 관리방안



Q & A