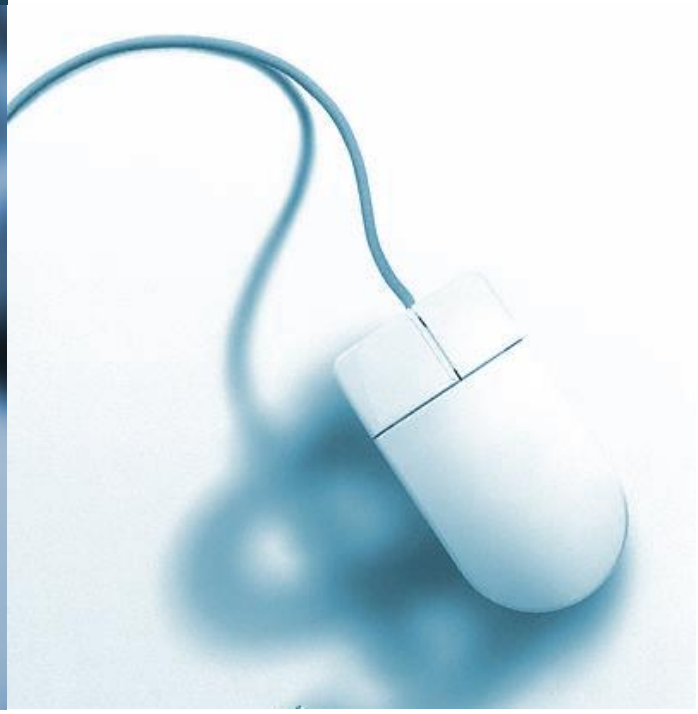
기업보안관리의 중요성과 대응방안



신 현 구

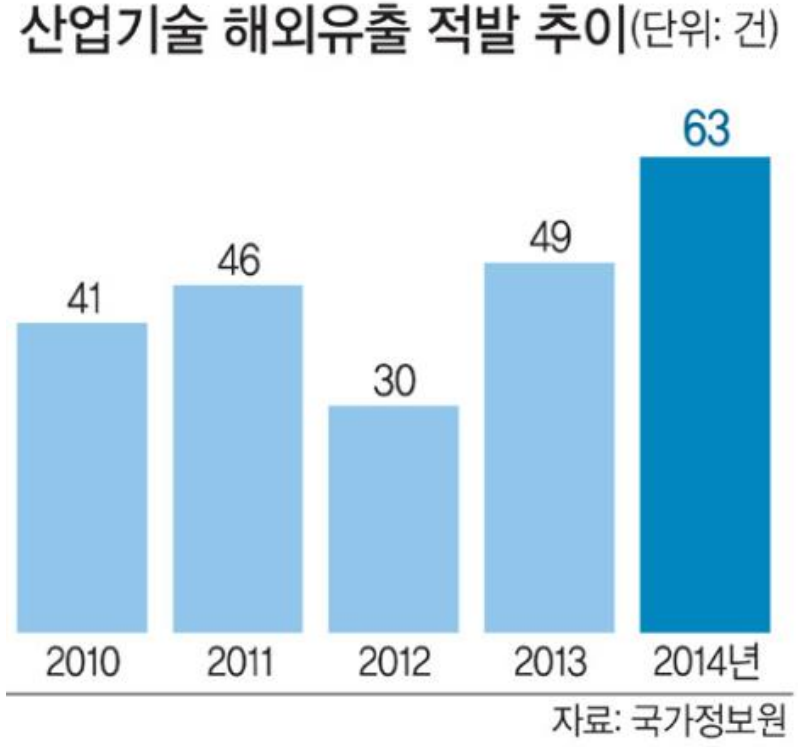
Contents

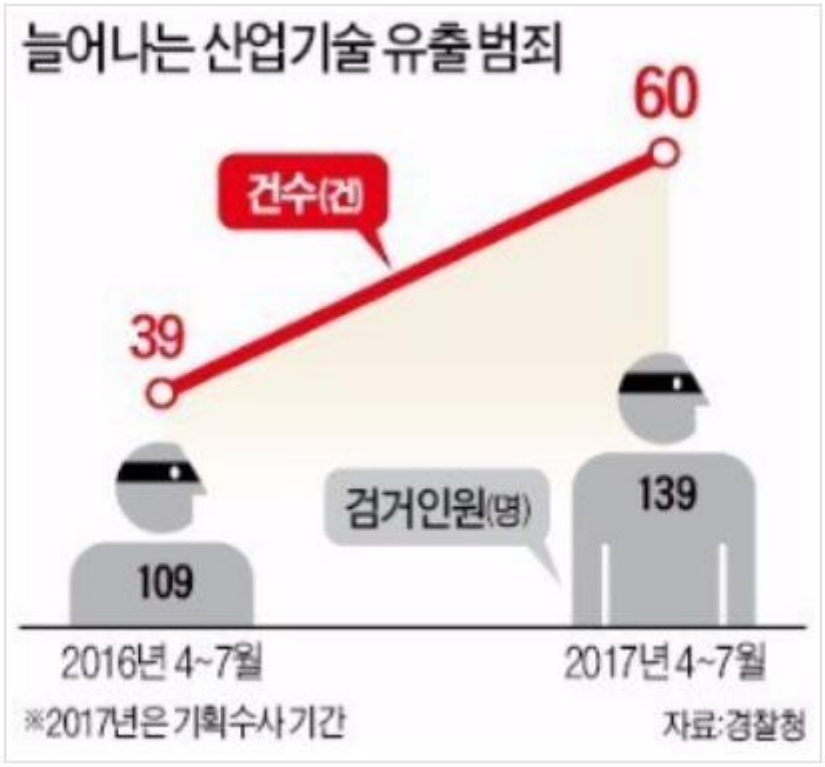
기업비밀 보호 동향과 산업스파이의 필연성

산업스파이와 전면전 선포 (서울신문, 보안뉴스)

대검찰청 중앙수사부 민간합동회의	• 삼성전자, 현대·기아차, LG, 두산, 하이닉스, SK, KT, 한화 등 대기업 참가 • 기술유출 예방과 관련 범죄 대응방법 토론, 회사별 산업보안 실태 파악 • 대검찰청 첨단범죄수사과, 일선청 첨담범죄수사부/특수부
경찰청 외사국, 산업기술유출수사대 발족	• 전문 수사경력 보유자 및 디지털 포렌식 증거분석 전문가 구성 • 불공정기업 수사 및 실질적 제재 강화, 기술유출 예방 및 피해기업 규제 • 산업기술 유출사건 검거실적 : 2004~2011, 국내유출(231) / 해외유출(86)

산업스파이 사건 현황 (해외 기술유출 사건)





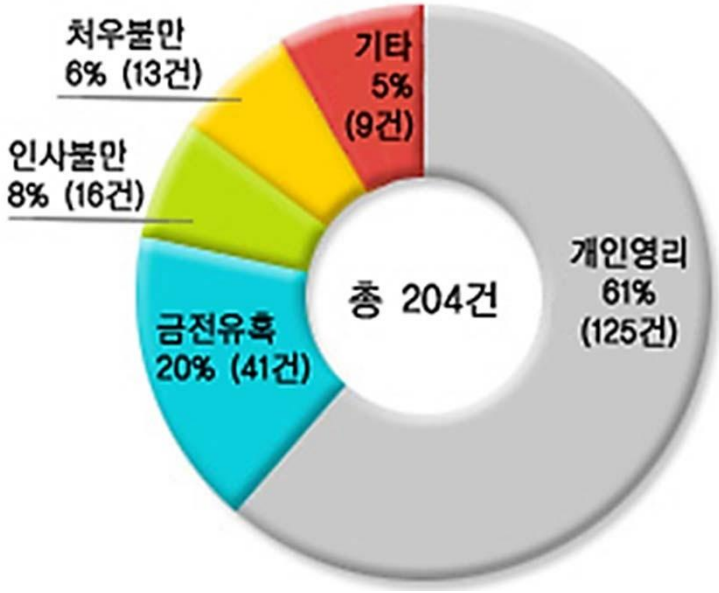
산업스파이 사건 현황 (유형별 분석)

기술유출 주체

- 전직직원, 현직직원, 협력업체를 통한 기술유출 → 92%

기술유출 동기

- 개인영리, 금전 유혹으로 인한 기술유출 → 81%



출처 : 산업기밀보호센터

산업스파이의 필연성

고급 정보(기술)를 소유하는 방법 3가지

하나	자체 개발하거나 인력양성하여 취득하는 방법
둘	정당한 대가를 주고 매입하는 방법
셋	?

→ 가장 쉽다 ! 가장 빠르다 ! 가장 경제적이다 !

기업비밀 유출사건 발생 원인

1 무한경쟁 시대의 기업의 과제

> 총성 없는 기술전쟁
>
> **가장 효과적인 연구개발 투자**는 타인이 개발한 영업비밀을 훔치는 것
>
> 지적재산권 보호 전문가 Yvonne M. Kisiel

경쟁력 확보를 위한 기업의 대응

고급 기술(정보)의 적시 개발·활용	+	기술(정보) 보호(보안)

기업비밀 유출 범죄 처리 현황

자료:대검찰청

연도	건수 (건)	인원 (명)	검찰 처리 내역 (명)					
			구속 구공판	불구속 구공판	구약식	기소 유예	공소권 없 음	혐의 없음
2011년	439	942	15 (1.6%)	125 (13.3%)	47 (5.0%)	82 (8.7%)	25 (2.7%)	648 (68.8%)
2012년	448	1,063	19 (1.8%)	147 (13.8%)	22 (2.1%)	63 (5.9%)	5 (0.5%)	807 (75.9%)
2013년	459	1,156	15 (1.3%)	116 (10.0%)	40 (3.5%)	65 (5.6%)	19 (1.6%)	901 (77.9%)
2014년	412	972	22 (2.3%)	116 (11.9%)	18 (1.9%)	33 (3.4%)	16 (1.6%)	767 (78.9%)
2015년	467	1,129	23 (2.0%)	161 (14.3%)	43 (3.8%)	23 (2.0%)	22 (1.9%)	857 (75.9%)
2016년	528	1,125	12 (1.1%)	149 (13.2%)	31 (2.7%)	40 (3.5%)	15 (1.3%)	**878 (78.0%)**

"정보유출은 순식간에, 법에 호소하면 최소6개월에서 5년 소요"

기업비밀 유출사건 발생 원인 (보안 불감증)

2 보안에 대한 두 가지 부정적인 생각

[구멍뚫린 기술 한국] 下·기술유출 방지 시스템 구축 시급

2007-05-24 17:39:38

세계 각국의 산업기술 보호 법제도

구분	법률명
미국	경제스파이법, EAR 특허법
독일	대외무역관리법, 부정경쟁방지법 외국환 및 외국무역법
일본	부정경쟁방지법, 외국환 및 외국무역법
한국	부정경쟁방지법, 대외무역법 산업기술유출방지법

자료:인하대 법대 김병일 교수 보고서

산업스파이가 국가의 운명을 좌우할 핵심기술 유출을 무차별적으로 빼내 가는 구멍 뚫린 '기술 한국호'를 구할 비책은 없을까.

날로 지능화·대형화되는 산업스파이를 기업 스스로가 물리적으로 차단하기는 쉽지 않다. 사정이 이런데도 기업들의 핵심기술 보유 전현직 직원에 대한 보안 관리와 인사 시스템은 초보적인 수준이다.

파이낸셜뉴스
글로벌 시대의 새로운 시각 First-Class경제신문

- 보안관리를 할 만한 가치가 있는 첨단기술 등의 정보가 없다?
  → 기술수준이나 가치를 미국이나 일본 등 기술 선진국과만 비교하면서 발생하는 오해
- 지금까지 별일 없었으므로 생산에 도움이 되지 않는 일을 할 필요가 없다?
  → 보안의 필요성을 인식하지 못한 결과

기업비밀 유출사건 발생 원인 (저장기기 다양화)

3 영업비밀 유출 가능성의 증가

- 소형·대용량 저장기기 등 유출수단의 첨단화·다양화, 인터넷 등 정보의 유통·전달 네트워크 발전

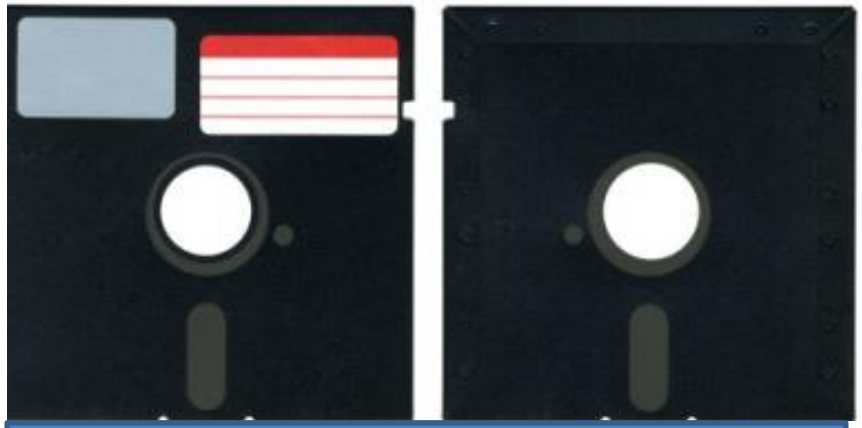



참고 (저장용량의 변천)

1956년 5MB(메가바이트) 저장매체
당시가격 12만 달러 (약 한화 1억5천만원)

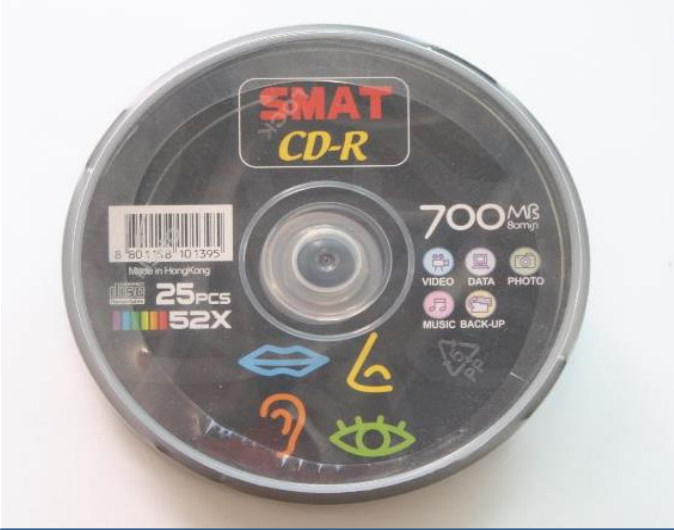
대비

참고 (저장용량의 변천)



1976년 5.25inch 디스켓 (용량1.2MB)

1982년 3.2inch플로피디스켓 (용량1.44MB)



1988년 CD-R, 1997년 CD-RW(용량700MB)

참고 (저장용량의 변천)

usb1.1 ->12Mbps (low speed) ->초창기속도

usb2.0 ->480Mbps(pull speed)

(2GB 4GB 8GB 16GB 32GB 64GB) 1.1보다 40배 빠름)

usb3.0 ->5Gbps (super speed)

(8GB 16GB 32GB 64GB 128GB 256GB) 2.0보다 10배빠름)

USB(32GB)

3.2 inch 디스켓대비 240,000배

SD 카드(400GB)

USB(2TB)

외장하드(1~3TB)

3.2 inch 디스켓대비 7,500,000배(1Tb0B)

핵심 인력관리의 중요성(보안부서장의 하소연)

- 우리회사 기밀? 유출 확신한다. 심각한 수준이다.
- 중역회의 자료가 밖에서 돌아다닌다.
- 경쟁사가 내부 임직원보다 (우리회사 정보를)먼저 안다.
- CEO는 성장에만 관심있다.
- 보안 중요성? 다 안다. 그러면서도 유출 후에나 후회한다.
- 귀동냥 정보가 많다.
- 출입이 자유롭다.
- 시급한 것(간부들 인식제고, 경영진 마인드 없다. (상무4, 수석부사장2, 부사장3, 사장님부터~~)
- 승인원이면 100% OPEN 된다고 봐야한다.
- 매월 협력업체 품질회의 개최(생산량, 공정도) 모두 다 안다.
- 경영자의 마인드가 회사 보안 수준이다.

기업비밀 유출 사례 (퇴사자)

사례 1 A사 퇴사자(임직원) 핵심기술 자료 유출

1 고위 임원 및 관리직 으로 재직하면서 중요 자료 입수

2 신규 사업을 추진하는 경쟁사로 전직

3 주요 정보를 회사에 반납하지 않고 USB 외장하드 등에 담아 퇴사

4 경쟁사에서 대규모 입찰 준비 등 사업 실행 착수

- 형사 대상자 6명에 대한 가압류 신청(손해배상청구권)
- 전직금지가처분 신청 **전원에 대해 퇴사 후 3년간 전직금지결정**

기업비밀 유출 사례 (내부직원)

사례 2 경쟁사로 퇴사한 후 친분관계 악용, 내부직원을 통한 기술유출

1 인사 불만을 이유로 퇴사 후 경쟁사로 이직, 전 직장 임직원에 대한 부당 유인

2 전 직장의 기술로 동일 제품 생산 / 판매, 제품 결함에 대한 Know-How 부족

3 친분관계 악용, 전 직장 내부직원들 회유 / 협박

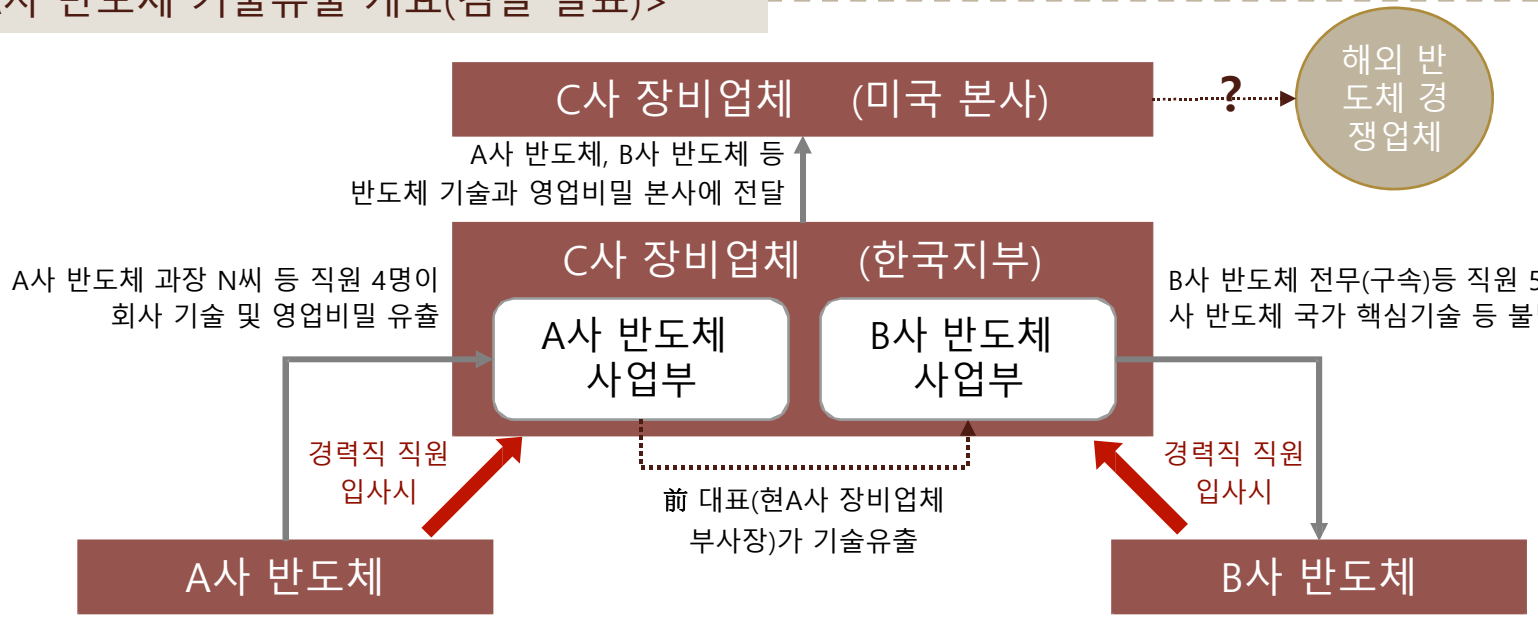
4 전 직장의 최신 기술자료 및 영업자료 유출, 전 직장 고객사 상대 제품 판매

- **형사 대상자에 대한 가압류 신청(손해배상청구권)**
- **내부 공모자 벌금형 선고**
- **시장 잠탈로 인한 기업의 경쟁력 약화 / 핵심인력 부당 유인**

기업비밀 유출 사례 (협력업체)

사례 3 납품 시 입수한 고객사의 정보를 고객사의 경쟁사에 누설

<A사 반도체 기술유출 개요(검찰 발표)>

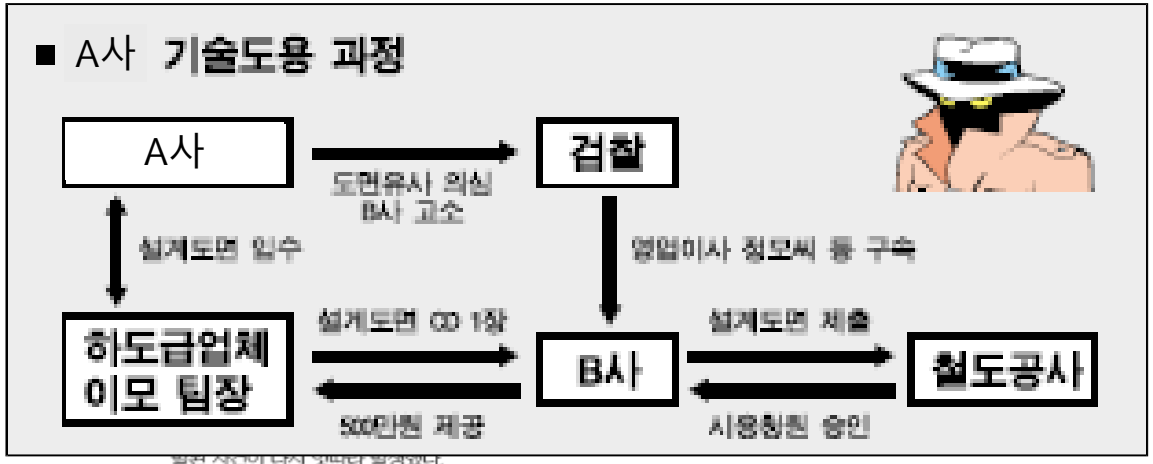


- **장비 납품(C사) 과정에서 A사 영업비밀 취득, A사의 경쟁사인 B사에 누설**
- **C사 前 대표 구속기소, A사 및 B사 직원 기소(총 15명 기소)**

외부업체와의 거래 시 또는 경력직 직원 입사 시 타사 영업비밀 내부반입 금지

기업비밀 유출 사례 (경쟁사)

사례 4 하도급 업체를 통한 전동차 설계 도면 유출 사건(2005)



검찰에 따르면 정씨는 지난해 12월 한국철도공사 전동차 시용창원 승인을 받기 위해 다른 직장에서 함께 근무했던 로템 하도급업체 이모(31·구속) 팀장에게 500만원을 주기로 하고 전동차 차체, 대차 부분 설계도면을 담은 CD 1장을 넘겨 받아 전동차설계도면 제작에 사용한 혐의를 받고 있다.

을 빼돌린 혐의로 O사 대표 오모(44)씨 등 2명도 불구속 기소했다.

검찰에 따르면 오씨는 지난 2004년 10월께 I사 국내영업팀장으로 근무하던 김모(35·불구속)씨에게 함께 근무할 것을 제의하면서 영업비밀을 빼돌릴 것을 지시, 대외비인 경영상 영업비밀을 e메일이나 CD로 넘겨받은 혐의를 받고 있다.

/이병관기자 comeon@sed.co.kr

- 경쟁사가 협력업체에게 금품을 제공, 영업비밀을 입수하여 제품 개발에 도용한 사안
- 검찰, 3명 구속 기소 등 총 8명 재판 회부
- 전원 유죄 확정
- 협력업체로 제공되는 자료가 경쟁사로 유출 될 수 있음에 유의

산업스파이 사건 특징

- 유출자 = 내부자
- 유출자 = 전현직 임직원
- 유출자 = 핵심임직원
- 유출자 = 불평불만자

- 유출 시 정보기기 활용
- 막대한 분량 유출
- 유출 흔적 발견 곤란
- 단독 소행이 드물다

출처 : 산업기밀보호센터

기업비밀유출
사고 대응 수행 전략

기업비밀 유출 방법

- 경쟁사 스카웃
- 공동 연구
- 촬 영
- 도 청
- 컴퓨터 침입
- 위장 침투
- 해 킹
- 매수
- 복사 및 절취
- 저장 장치
- 위장 합작
- 문서 유출
- 제3자 이용
- 미인계 활용

기업비밀 유출 시 적용 법률

	부정경쟁방지 및 영업비밀보호에 관한 법률
보호 대상	영업비밀(기술상 + 경영상 정보)
적용 범위	기업에 국한
보호 대상	기술상 정보+경영상 정보
보호 요건	**① 비공지성 ② 경제적 유용성 ③ 비밀관리성**
처벌 조항	비친고죄 / 미수.예비.음모 처벌

- 해외유출시 징역 10년(국내유출시 5년)
- 처벌대상 확대(누구든지)
- 행위 확대(예비, 음모, 미수 포함)
- 기본 0.5~1.5년, 가중 1~2년
- 법정형 상향(이득의 2~10배)

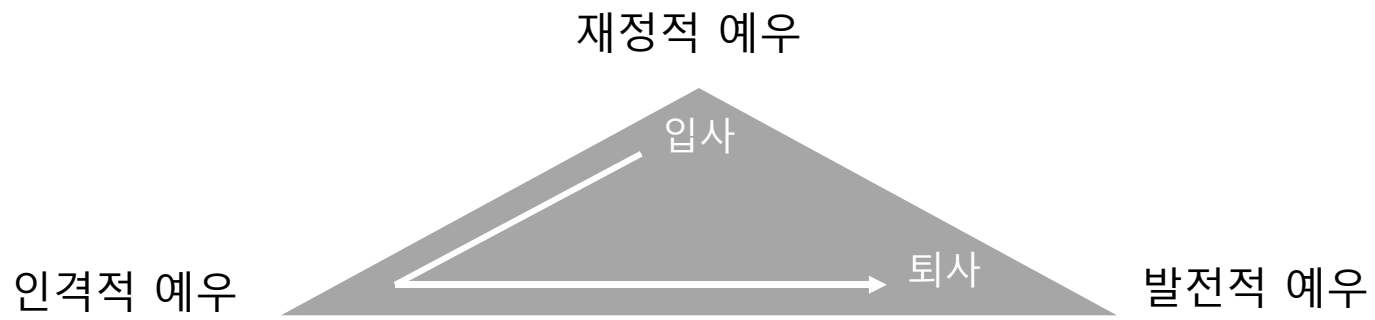
보호 요건

① 비공지성 ② 경제적 유용성 ③ '비밀관리성'이란?

대분류	소분류	내용
표시 고지	✓ 영업비밀 표시	• 영업비밀에 '기밀' 등 기재
	✓ 영업비밀 등급 분류	• 영업비밀을 일반 정보와 구분 • 영업비밀을 등급별로 관리
	✓ 보안교육	• 직원 대상 보안교육 실시
	✓ 영업비밀 고지	• 영업비밀 여부 및 범위를 고지 • 비밀유지의무 고지
계약	✓ 직원 대상 서약서 등 징구	• 입사, 퇴사 시 직원들에게 비밀유지서약서 등 징구
	✓ 거래업체와 비밀유지계약 체결	• 거래 전에 비밀유지계약 체결
행정 조치	✓ 보안규정 시행	• 사내 보안 관련 규정을 제정하여 시행
	✓ 보안담당자 지정	• 영업비밀 및 회사 보안을 전담하는 인력 지정
	✓ 영업비밀 열람/접근 제한	• 영업비밀에 대한 접근 권한을 구별하여 부여 • 영업비밀 열람, 사용 등 내역 기록
출입 제한	✓ 보안장치 설치 운영	• CCTV 카메라, 카드리더기 등 설치 운영
	✓ 개발실/보관실 분리 및 출입 제한	• 영업비밀을 생산하는 개발실 별도 운영하고 출입 통제 • 영업비밀을 보관하는 보관실을 별도 운영하고 출입 통제
	✓ 출입 시 보안 검사	• 회사나 통제구역 출입 시 소지품, IT기기 등 수색, 검사
IT 보안	✓ 영업비밀 복사/전송 제한	• 이동형 저장매체를 통한 복사 제한 • 이메일로 파일 첨부 통제
	✓ 컴퓨터/네트워크 암호 설정	• 컴퓨터 로그인 암호 설정 • 네트워크 접속 암호 설정
	✓ 보안프로그램 및 파일 암호화	• 컴퓨터 정보보호를 위한 프로그램 설치 운영 • 영업비밀 파일을 암호화하여 보관
기타 요소	✓ 기타	• 파쇄기 설치 • 퇴사 시 이메일 삭제 및 퇴사 시 하드디스크 포맷 • 규정 있으나 미시행 그 외 비밀관리성 판단요소

핵심인재 Retention (이직 조기경보시스템 구축)

- **전직직원, 현직직원, 협력업체를 통한 기술유출 → 92%**
- **CEO 의 보안에 대한 관심 최고조**



핵심인력의 직업관

순위	입사 이유	몰입 이유	퇴사 이유
1	복리후생 수준	최고경영자의 관심	상사와의 갈등
2	경쟁력 있는 급여	도전적인 직무	일과 삶의 불균형
3	일과 삶의 균형	의사결정 자율권	급여 불만

(출처: A사 내부 조사)

기업의 잠재적 리스크

보안 최대 위협 요소는 시스템 결함 아닌 '사람'

1029개 기업 보안 담당자 조사
직원 교육·프로세스 확립 우선

보안에 있어서 최대 위협 요소가 시스템 결함이 아닌 '사람'에 있다고 인식하는 보안 담당자가 늘어난다. 새로운 보안 솔루션을 도입하는 것보다 직원 인식 제고와 프로세스 확립이 필요하다는 분석이다.

28일 인포메이션위크는 1029개 기업 보안 담당자를 대상으로 실시한 '2013 전략 보안 서베이' 결과에서 '효과적 보안 정책 수립'이 필요하다는 응답이 지난해 대비 가장 큰 폭으로 증가했다고 보도했다.

충분하지 못한 보안 예산이나 시스템 복잡성이 가장 큰 위협일 거라는 예상은 빗나갔다. 보고서에

2013 전략 보안 서베이 주요 결과

※( )안은 지난해 대비 증감률

자료:인포메이션위크

따르면 시스템 접근을 효과적으로 관리하고 적절한 정책을 수립하는 게 중요하다는 응답(33%)이 여러 항목 중 가장 큰 폭(11%)으로 증가했다. 2011년부터 사람에 대한 보안 우려가 지속적으로 늘어난다는 설명이다. 본인 비밀번호와 계정을 제대로 관리하고 절차를 밟아 시스템에 접근하도록 하는 직원 교육과 보안 인식 제고가 필요하다는 분석이다.

모바일 장비와 클라우드 환경 확산에 따른 시스템 복잡성 증가가 보안 위협이라는 응답은 여전히 가장 많은 비중(38%)을 차지했지만 지난해(52%)보다 14%나 떨어졌다. 데이터 증가가 위협이라는 응답 역시 19% 감소했다.

보고서는 보안 인식 제고 없이 무턱대고 솔루션만 도입한다고 해서 보안이 강해지지 않는다고 충고했다. 주기적인 보안 교육과 프로세스 확립이 우선시돼야 한다는 얘기다. 직원 개개인의 문제점을 파고들어 기업 정보에 접근하는 '소셜 엔지니어링 어택'이 증가하는 것도 보안 인식을 강화해야 하는 이유다.

보고서는 "보안을 강화하기 위해 솔루션 도입을 늘리는 경향이 많지만 절차를 확립하고 교육을 늘리는 게 더 중요하다"며 "소셜 미디어와 BYOD 환경이 확산될수록 교육의 필요성은 더 커진다"고 말했다.

안호천기자 hcan@etnews.com

보안솔루션 구축 + 소수 보안 전문가 영입 = 정보보호 끝???

보안사고 및 현업 점검 사례

- 퇴직자 관리 프로세스는 수립되어 있다?
- 내부정보 유출 방지를 위한 보안솔루션은 (DRM/DLP) 구축되어 있다?
- 협력업체/외주업체로부터 보안서약서는 받는다?
- 유출 기법이 진화되고 있다?
- 정책상 내부망과 외부망을 분리는 한다?
- 정책상 공유폴더 사용을 금지는 한다?
- 주기적으로 보안점검은 한다?

개 선 사 항

- 퇴직자 사용 HDD에 대한 증거확보
- 취약성 및 우회기법에 대한 점검과 피드백 (zip, txt, pdf / 확장자 변조, 서버 포트 통한 유출)
- 실질적인 점검 및 통제 프로세스
- 자체 전문인력 배양, 취약성 점검 및 피드백
- 외부 반출입 통제의 실효성
- 현업의 업무 공유 방법에 대한 점검과 피드백
- 모니터링 대상의 사전 분류 및 자동화 기법 개발

유출/퇴직 전 이상행동 유형

- **근무태도의 변화**
  - 상사와 격한 논쟁 혹은 높은 충성심에서 부정적인 태도
  - 평상시 안가던 타부서 사무실의 빈번한 출입
  - 타사 면접을 위해 휴가 사용
  - 타 업무에 대한 질문 / 조사의 빈번함
  - 연구활동보다 성과물 확보에 집착
  - 특별한 사유없이 일과후, 공휴일에 혼자 남아 있는 사람
- **행동의 변화**
  - 주변정리, 외부 통화를 숨기는 행동
  - 평상시와 다르게 동료의 접촉을 피하거나 최근 정서 변화가 심한 경우
  - 고위관리자나 핵심기술자 등과 친교에 관심높은 연수생
- **주요부서에 근무하다가 이유없이 갑자기 사직을 원하는 경우**
- **업무와 관련없는 서버, DB에 자주 접근하는 사람**
- **자신의 상황을 대변할 '대리인'을 만듦**
  - 이직자는 회사의 누구에게나 반드시 알림

퇴직시 점검포인트

- 퇴직자와 관련성 없는 정보 보유 / 정보의 외부 유출흔적
- 정보의 의도적 삭제 / 외부의 특정 세력과 교신
- 기타 부정, 준법위험 관련 증거의 존재
- 위장 취업의 경우 실제 이직할 직장과 가까운 곳에 부동산을 검색한 흔적
- 퇴사를 앞두고 외장 하드 모델을 검색한 흔적
- 평상시와 다르게 외부 메일을 자주 사용한 흔적

퇴직시 점검포인트

- **컴퓨터에 자신의 업무영역을 훨씬 벗어나는 방대한 자료를 축적**
  - 소프트웨어 개발부서에서 하드웨어 설계도 및 소스를 모으는 행위
- **졸업증명서, 주민등본 등을 인터넷으로 발급**
- **보안시스템 해제 방법 등 다양한 방법에 대한 인터넷 검색**
- **퇴직자의 보안유지 교육 후 서명**
- **동의서 체결 / 포렌식 인터뷰**

기업의 대응 전략 (퇴직자)

퇴직자의 정보 보관

- 퇴직자의 업무용 PC의 HDD 보관 관리
- 퇴직자의 정보 보관

- **퇴직자의 비위사실이 추가 발견되는 시점은 3개월에서 1년6개월 이후인 경우가많음**
- **핵심기술 및 경영상 중요 정보가 유출되었어도 증거부족으로 법적 대응이 어려움**

임직원 채용 시 점검 항목 예시

타사의 영업비밀 보유 여부 확인 및 개인 장비 포렌식 조사

전 직장 퇴직 시 각종 서약서 서명 여부 확인

- 전직금지 / 경업금지조항 및 기간 / 보상금 / 비밀유지서약 / 검색동의서 등

입사 예정자 인터뷰 및 지원서 검토

- 전 직장에서 디지털기기 반환여부 / 퇴직의사 표명시기 / ID반납 / 직무정지일

인터뷰 및 교육 실시

영업비밀 반입금지 경고와 즉각적인 업무 투입 자제

각종 서약서/동의서 체결

임직원 대상 보안의식 함양 교육 훈련

- **주기적인 임직원 교육훈련**

신규채용, 직무재배치임직원 영업비밀관리 교육

영업비밀 침해사례 인지 시 적기 보고의무 교육

영업비밀보호에 필요한 관리적, 물리적, 시스템적 보안방안 교육

새로운 영업비밀관리 프로그램 도입 및 변화관리 교육

각종 동의 양식 시행

- 겸업금지 / 경업금지 서약서
- 보안서약서
  - 무단복제, 제3자 제공, 누설, 비승인정보 및 저장매체 사용(mini SD등) 금지
- 정보검색 동의서
  - 이메일, SMS포함

- 경쟁사 영업비밀 반입금지 각서
- 퇴직시 정보자산 반납
- 비밀유지 서약서 (주요정보, 영업비밀 등)
  - 입사자용 / 재직자용 / 퇴직자용 / 협력업체용
  - 전산매체 사용자용 (노트북, USB, DVD, Remote Access, 정보접근)

입퇴사 시 유출, 유입

임직원 퇴사 시

자사 영업비밀 유출

전/현직 직원에 의한 영업비밀 유출
제3자에 의한 영업비밀 유출

- 기술, 투자비용 상실
- 침해품 저가공략/시장잠식
- 경영상 취약점/전략 노출

경력 채용 시

타사 영업비밀 부정유입

경력직 직원 통한 유입
부주의한 외부정보 수집/ 저장

- 수사, 구속, 압수수색, 처벌
- 손해배상책임
- 회사 책임, 이미지 실추

수행 전략 마련

- CEO 가 알고 싶은 것은… 유출사고가 났다는 사실을 알려고 하는 것이 아니다.
- 유출사고 사실만 부각시키지 말고, 어떻게 대응할 것인가?

민사상/형사상 조치의 전후 판단

- 형사 조치를 먼저 하는 것이 바람직

형사의 경우, 의뢰 기관 및 방식 선정

- 진정? 고소?
- 수사기관

지원팀 강화

- IT팀 이외 엔지니어팀 강화 투입
- TFT에 전념할 수 있도록 업무량 조정

상대방 동향은 지속적 파악

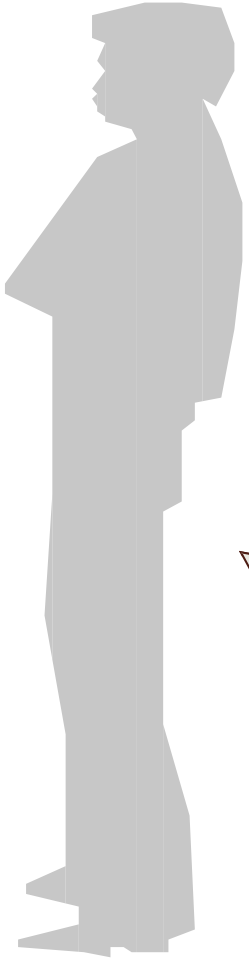
- 노출되지 않는 범위 내에서 지속적 동향 파악

기술유출 관련 통상적 변명 (수사단계)

- 영업비밀이 아니다.
  - 공개된 내용이다. 기
  - 술적 가치가 없다.

- 유출의 고의가 없었다.

- 개인적 연구 목적이다



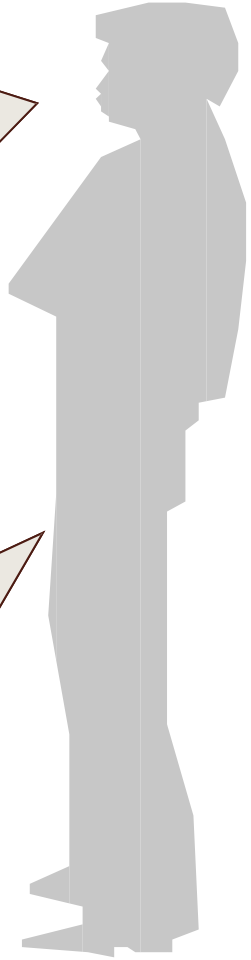
- 상대방 회사에 이용가치가 없다.
  - 개발방식이 달라 전혀 필요가 없다.

- 개인적 범행이다.
  - 회사는 관여하지 않았고, 전혀 몰랐다.
  - 개인적으로 사용했을 뿐 회사가 지시한 적 없다.
  - 검토했지만, 필요가 없어 사용하지 않았다.

기술유출 관련 통상적 변명 (공판단계)

- 피고인들의 퇴사와 관련한 사실관계
  - 회사가 사실상 제대로 대우하지 않아 각자 스스로 퇴사한 것이지 미리 상의하고 계획한 것이 아니다.

- 영업비밀 유출 관련
  - PC에 있는 유출흔적은 사실과 다르다. 백업 또는 백신 등



- 퇴사후 전직과 관련하여 입수한 사실관계
  - 퇴사후에 직장을 알아보다가 우연히 입사하게 된 것이지, 상대방 회사가 기술유출을 조장한 바 없다.

- 회사의 보안관리 – 물리적, 시스템적, 관리적
  - 보안지침, 보안서약서 – 서명한 바 없다. 내용도 모르고 서명했다.
  - 출입통제 – 허술했다. 영업
  - 비밀 관리 – 부실했다. 교육
  - 및 점검 – 거의 없었다.

비밀관리성 탄핵 (영업비밀 분류)

- 상당한 노력에 의하여 비밀로 유지되어야 한다.
- CEO 의 최우선 관심사는 영업비밀분류체계 및 자체 대응 역량 강화

As-Is

To-Be

기업의 보안관리 전략

- 보안 10대 수칙-

기업 대응 전략 (보안 10대 수칙)

수칙 1. 기술보호를 위한 관리규정을 갖추고 실시해야 합니다.

CASE

항목	내용
보안정책 수립	임직원 공지(또는 교육) 및 서명
보안전략 수립	보안규정 및 지침 수립 취약성 분석에 대한 대책 및 개선방안 도출 보안관리 세부 계획 수립
보안규정 운영	경영진에 의한 승인 및 임직원의 인식 강화 보안정책, 지침의 주기적인 검토와 개정 실시 보안교육, 비밀유지계약서, 퇴직자 관리사항 포함 내외부인의 출입통제 및 보호구역 설정 보안사고 및 보안 위규자 처리에 관한 규정 최소한의 통제로 최대의 효과 방안 마련

- **보안관리 세부규정을 운영하되 주기적으로 갱신하여야 한다.**
- **갱신은 경영진에 보고, 확인 후 임직원에게 그 사실을 공지하여야 한다.**

기업 대응 전략 (보안 10대 수칙)

CASE

산업 보안 방침

OOOO주식회사는 핵심인재 및 지적 재산은 물론 회사의 모든 유·무형 자산이 회사 경쟁력의 원천임을 인식, 산업보안 활동이 회사의 미래 뿐만 아니라 국익수호에도 기여함을 명심하여 자율 참여의 보안 문화를 확립함으로써 회사의 지속 가능한 발전을 추구한다.

1. 핵심기술 및 핵심인력을 포함한 유·무형 자산을 보호함으로써 핵심역량 강화 및 경쟁력 제고에 기여한다.
2. 산업보안에 관한 제반 법규를 준수함은 물론, 관련업체 및 협력업체의 영업비밀보호 노력에도 동참한다.
3. 지속적인 교육 및 홍보를 통해 임직원의 보안의식을 제고시켜 자율참여의 보안문화 확립에 적극 노력한다.
4. 산업보안 활동을 위한 전담조직 및 조직별 관련 인력을 두어 자율참여 기반의 체계적 보안시스템을 구축하고 지속적으로 관리, 개선한다.
5. 본 방침의 효율적 이행을 위해 필요시 객관적인 외부진단 등을 받아 회사의 산업보안 활동에 적극 활용한다.

201 년 월 일

0000주식회사 대표이사 0 0 0

기업 대응 전략 (보안 10대 수칙)

수칙 2. 보안관리를 위한 전담인력을 반드시 지정해야 합니다

CASE

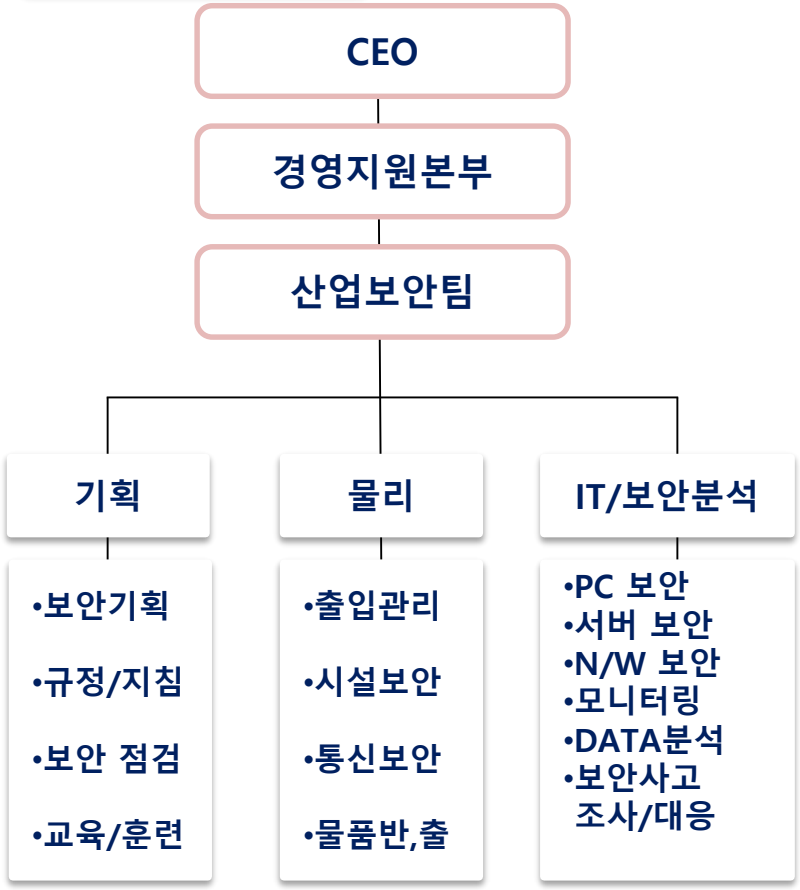
관리자 명	임 명	업 무 영 역
대 표	CEO	▪ 보안정책 (전담조직, 전문인력 확보, 예산투입, 관련기술 확보 등)
회사 보안책임자	CSO	▪ CEO를 보좌하여 회사 보안업무 총괄 ▪ 정보보안 분과위원 임무수행 (회사 보안관리위원장)
회사 보안담당관	보안팀장	▪ CSO를 보좌하여 임무 수행 ▪ 회사 보안업무수행에 관한 계획의 작성 및 시행에 대한 조정,감독 ▪ 보안규정,보안교재 작성 및 보안교육(부문보안담당관,부서보안책임자,신입사원)실시 ▪ 보안책임자, 통신 및 OA기기 관리책임자 운영체제 유지 ▪ 대상자 신원조사의뢰 및 회사 보안문서 소유현황 조사 ▪ 보안지도점검, 평가, 보안사고 조사 및 보안 위규자 징계건의, 보안협의회 운영 개최
회사 보안담당자	보안팀원	▪ 회사보안직위자 교육 및 세미나 주관 ▪ 보안규정 및 관련 매뉴얼 제 개정 ▪ 회사보안감사 수행 및 보고 ▪ 회사보안조직 및 제도 운영 ▪ 회사출입통제시스템 도입 및 운영 ▪ 보안관련 대 관청 업무 ▪ 정보유출 (산업스파이) 신고센터 운용

기업 대응 전략 (보안 10대 수칙)

수칙 2. 보안관리를 위한 전담인력을 반드시 지정해야 합니다

CASE

조직구성



부서개요 및 업무내용

주요업무 (대분류)	중분류	세부 업무내용
보안 기획	전략/제도 회의체 운영	1) 년간 보안전략/Master Plan 수립 2) 전사 회의체 운영/제도 개선 3) 보안 Issue 대응/지표관리 4) 표준 제.개정/교육개발/실적 관리 5) 對 그룹/CI 업무
물리 보안	시설 보안 상황실 운영	1) 보안 Infra 구축/운영 2) 상황실 및 보안근무인력 운영 3) 사업장 보안 Risk 개선 4) 전사(사업장) 점검/실적 및 위규율 관리 5) 대외기관 대응 업무
IT 보안	시스템 구축/운영	1) IT 보안정책 수립/시행 2) IT 보안 취약점 진단/개선 3) 현업 시스템 대상 보안성 검토 4) IT 보안시스템 운영

기업 대응 전략 (보안 10대 수칙)

수칙 2. 보안관리를 위한 전담인력을 반드시 지정해야 합니다

CASE

보안수준 향상을 위한 R&R 확립

부서/담당	주요 업무	상세 내용
법인장 (President)	주요 의사 결정	• 정보보안/개인정보보호 총괄 • 보안관련 주요 의사결정
정보보안 주관부서	개인정보보호 및 기업보안 총괄	• 정보보안 및 개인정보보호 기준 수립/ 교육/ 홍보/ 진단 • 각종 보안시스템 운영 및 관리 점검
부서장	보안 절차 승인	• 부서원 보안 프로세스 관련 승인
HR부서	인원보안	• 비밀유지서약서 접수 (신입/임직원/임시직/협력사) • 퇴직자 보안(퇴직 Checklist 확인)
총무부서	시설보안	• CCTV 카메라 관리, 출입권한관리, 문서 파쇄기 관리 등
IT부서	IT보안	• PC 반납 시 PC내 자료 안전한 삭제 • Network, DB, PC 보안관리(PW,화면보호기, 공유폴더 등) • 보안 프로그램 운영 (백신, 방화벽, 보안 프로그램 등)

기업 대응 전략 (보안 10대 수칙)

수칙 3. 전직원을 대상으로 정기적인 기술보호 교육을 실시해야 합니다.

CASE

□ 목 적
- 기술보호의 필요성/중요성을 임직원들과 공유하고 보안 Mind 제고
- 기술보호 지침과 절차를 명확히 숙지하여 의도적 또는 무의식적인 정보의 유출을 미연에 방지

□ 종 류
- 대상에 따라 신입.경력/임원/보안 담당자/재직자 교육으로 분류
- 전 직원 (임원 제외)은 년 1회 온라인 보안교육 이수 必

구 분	교육 대상			
	신입/경력	임원	보안 담당자	재직자
주 기	- 발생 時	- 年 1회	- 半期 1회	- 집합 (년 1회) - 온라인 (년 1회)
강 사	- 보안부서장	- 외부 강사	- 보안부서장	- 보안부서장
내 용	- 보안정책/ Process	- 대내.외 보안 동향	- 주요 보안 Issue/동향	- 보안정책 및 Process - 보안 위규 사례 - 핵심 기술 유출 사고 사례

- 시기별(정기교육, 수시교육), 대상자별(전 임직원, 파견근로자, 외국인별)
- 내용 : 기술보호 규정 및 법률 / 서약서 작성 및 내용 / 생활보안 행동준칙 / 사내 보안시스템 구축
- 중요 핵심기술 취급자(사용자) 특별교육
- 보안의식 고취 외부전문가 특강(연 1회 이상)
- 보안사고 예방 우수자 선발 및 포상

기업 대응 전략 (보안 10대 수칙)

수칙 4. 전체 직원에게 비밀유지서약서, 핵심직원은 전직금지서약서를 체결해야 합니다.

CASE

□ 목　적

- 서약서 징구는 당사의 독립된 경제적 가치와 합리적인 노력에 의해 비밀로 유지된 생산 방법, 판매 방법, 영업 활동 및 기술상 또는 경영상의 유.무형 자산을 보호하기 위함

□ 대　상

- 全 임직원[OO사업장/OO사업장/서울사무소/OO사무소]
- 회사 신규 임용 및 채용자 [채용 時]
- 사내 상주 분사 자회사 및 용역, 촉탁, 계약자
- 사내 非상주 상시 출입자[건설, 개발, A/S, 어학 강사, 컨설턴트 等)
- 건설, 개발, 공사 等의 사유로 1주 이상 상주자

□ 종류 및 징구 시기

- (임직원) 입사자용　: 신규/경력/전배/채용 時
- (임직원) 재직자용　: 年 1회 (年初)
- (임직원) 퇴직자용　: 임·직원 퇴사 時
- 협력업체 사원용　: 당사 임직원과 동일
- 외부 방문객용　: 당사 방문 시 징구 정문 안내데스크에서 징구
- 프로젝트 참여자용 : 당사 주관 프로젝트 계약 체결 時　3

기업 대응 전략 (보안 10대 수칙)

수칙 5. 핵심기술 인력이 퇴직할 경우 철저한 사후관리를 해야 합니다.

CASE

항 목	내 용
채용인원 관리	● 신규·경력 : 보안서약서 징구 및 보안교육 실시, 일정기간 접근권한 제한
재직 임직원 관리	● 비밀유지서약서(매년), 보안교육(년 2회 이상), 보안점검 및 감사 (수시) ● 사원증 관리, 상벌제도 활성화, 예방 신고센터 운영
해외 출장자 관리	● 휴대용 기기 최소화(출장용 노트북 별도 운영, USB등 저장매체 암호화) ● 출장관련 정보 노출 금지, 회사 로고 복장 자제, 공공장소 업무상 대화 및 공용PC 사용 자제
비서의 보안 관리	● 일정 및 회의자료 등 보안 유지, 임원 출장 시 시건 확인
퇴직자 관리	● 보안서약서 징구, 퇴직자 보안교육 실시 ● 정보 유출 및 삭제 흔적 확인, 사용 HDD 보관(업무별 상의, 필요 시 동의서 작성)
외래인 및 협력사 관리	● 비밀보호서약서 징구, 보안교육 실시 ● 출입증 발급, 출입 구역 명시
방문객 차량 관리	● 운전자 및 차량 내부 검색, CCTV통한 출입이력 보관
방문객 노트북 및 저장매체 관리	● 반입 통제, 필요 시 보안스티커 부착, 반출 시 저장 상태 확인
외국인 관리	● 신원 및 경력 확인, 타사 근무 사항 확인, 비밀유지서약서 작성, 출입 구역 제한
해외업체와 기술제휴	● 비밀보호서약서 작성 (계약 시·용역 완료 후), 제공된 기술자료에 대한 반환 및 폐기 확인 ● 기술에 대한 소유권 명시, 기술유출 시 책임소재 조항 명시

기업 대응 전략 (보안 10대 수칙)

수칙 6. 중요 기술은 영업비밀로 분류하고 별도로 관리해야 합니다.

CASE

자산의 종류	내 용
문서자산	정책/지침, 업무관련 문서, 인사기록, 송장 등 기업이 보유하고 있는 출력 문서(보고서, 계약서, 매뉴얼, 각종 대장)
인적자산	내부직원, 퇴직자, 제3자(외주업체, 컨설턴트 등), 아웃소싱직원, 고객 등 기업에 속해있는 모든 인원
정보자산	금융정보, 영업정보, 업무정보, 조직정보, 개인정보, DB 등 기업이 보유, 관리하고 있는 모든 정보(문서파일, 데이터파일, 데이터베이스 내의 데이터 등)
물리적 자산	서버, 하드디스크 등 기업의 업무에 활용되는 하드웨어
S/W 자산	운영 프로그램, 어플리케이션 프로그램, 통신 프로그램 등 정보시스템에서 상용하는 프로그램
대외제공자산	정보서비스, 통신서비스, 전원, 수도, 사무실 등 대외기관으로부터 제공받는 서비스

- **기업이 보유한 자산에 대한 분류기준은 기업에서 결정하여 시행한다.**
- **등급 분류기준은 가급적 기업의 규모, 능력, 업종 등을 종합하여 결정한다.**
- **기준이 정해지면 부서장이 분류기준과 등급(3등급 이하)을 결정하여 이행하며, 이때 관리대장을 작성하여야 한다.**

기업 대응 전략 (보안 10대 수칙)

수칙 7. 중요 서류는 별도보관하고 접근, 복제, 반출은 철저히 관리해야 합니다

CASE

항 목	내 용
보안문서 정의	● 출력물, 상황판, 차트, 그림, 사진, 필름, HDD, CD, USB, CCTV 등
보안문서 생산	● 취급자 제한, 기안 및 배포 계획 수립, 최소 생산, 비밀내용 최소화 표기
보안문서 등급 분류	● 극비 / 비밀 / 대외비 구분 ● 보안문서에 대하여 등급표시, 사본번호, 관리번호, 페이지, 보존기간, 경고문 표시
보안문서의 수발 관리	● 접수 및 발송이력 관리대장 기록
보안문서의 보관 및 기록 관리	● 화재·도난·파괴로 부터 안전한 지역, 비 인가자 접근 제한 ● 시건 장치 및 출입대장 기록
보안문서 기록 유지	● 비밀관리·비밀열람 기록부 작성
비밀의 파기	● 일분문서 : 세단기 ● 전자문서 : 영구삭제 프로그램 및 물리적 파쇄

기업 대응 전략 (보안 10대 수칙)

수칙 8. 중요 설비, 장치가 설치된 곳은 통제구역으로 설정하고 관리해야 합니다.

CASE

□ 내방객의 사내 출입은 '내방객 출입 관리' 기준을 따르며, 당사 임직원과 동일한 보안관리규정을 적용

□ 사원증 사용
- 사내 상주는 하지 않으나, 주 3회 이상 출입하는 내방객 : 임시 사원증 발급/사용
- 非정기적 또는 1회성 내방객 : 출입 패찰 사용

□ 사내 출입
- 정문 면회실 및 회의실 사용을 권장 (不필요한 사내 출입 최대한 억제)
- 업무 목적상 반드시 사내로 출입해야 할 경우,
  당사 업무 담당자가 정문 안내 데스크에서 내방객을 인솔하여 목적지까지 동행
- 임시 사원증의 경우, 출입 가능지역은 최소화 (정문 Gate 및 해당 건물 입구)
- 출입 패찰을 패용한 내방객은 해당 표찰이 출입을 허용한 지역만 출입
  * 출입 패찰마다 색을 입혀 출입 가능한 지역을 표시
- 내방객은 출입 패찰을 눈에 잘 띄는 상의에 패용

□ 보안관리규정 未준수자에 대한 조치
- 보안 상.벌점 운영 지침에 의거, 벌점 누계 5점 또는 중대 보안 사고자의 경우 당사 출입 제한
- 당사 업무관련 담당자에게 벌점 부여

기업 대응 전략 (보안 10대 수칙)

수칙 8. 중요 설비, 장치가 설치된 곳은 통제구역으로 설정하고 관리해야 합니다.

CASE

Ⅰ. 서울청사

2016. 2.24(일):시험지 및 답안지 탈취목적
- 외박 후 복귀하는 의경 뒤따라 진입

2016. 3. 6(일) 후문태그실패(신분증 분실신고)로 정문 집입(신분증 확인만으로 출입 가능)

2016. 3.24(목)
- 두번째 탈취한 신분증으로 정문 진입
- 신분증 도난신고로 스피드게이트 실패
- 지하주차장에서 신분증 제시 후 진입성공

2016.4.1(금):청사 재진입(확인차)

Ⅱ. 청사내 체력단련실

2016. 2.24(일) 라커룸에서 공무원 신분증 탈취

2016. 3. 6(일) 라커룸에서 공무원 신분증 탈취(2차)

Ⅲ. 16층 인사혁신처 복도

2016. 2.24(일) 채용관리과 잠입 실패(도어락)

2016.3.6(일) 사무실출입 암호 확인 후 진입 성공(답안지를 못 찾아 실패)

Ⅳ. 채용관리과 담당공무원 PC

3.24(목) 23:31-58 담당주무관 PC PW 접속 실패

3.26(토) PC접근 시험성적 및 합격자 명단 조작

공무원의 업무용 PC 보안 지침 : ⓐ부팅 단계 시모스(CMOS) 암호 ⓑ윈도우 운영체제 암호 ⓒ화면 보호기 암호 ⓓ중요 문서 암호 총 4중의 보안 암호설정의무

기업 대응 전략 (보안 10대 수칙)

수칙 9. 중요한 기술은 특허나 기술자료 임치로 보호해야 안전합니다.

임치제도란?
중소기업의 핵심 기술정보를 제3기관에 안전하게 보관하여 기술개발 및 보유 사실 입증(대중소기업상생협력촉진법 제24조의2 내지 제24조의5)

- 타 업체의 모방이 우려되어 특허출원을 하지 않는 기업
- 대기업 등 거래 기업으로부터 핵심 기술 제공을 요구받는 기업
- 영업단계에서 거래 기업에게 해당 기술에 대한 신뢰성을 보장받고 싶은 기업

《기술자료 임치제도》

☞ 중소기업은 핵심기술 정보를 제3의 신뢰성 있는 기관인 대·중소기업협력재단에 안전하게 보관하고 기술 유출이 발생하였을 경우 임치된 기술자료를 이용하여 해당 기술의 보유 사실을 입증할 수 있음. 또한 중소기업과 함께 기술자료 임치제도를 이용한 대기업 등 거래기업은 중소기업이 폐업, 파산 등을 한 경우 기술자료를 교부받아 지속적인 유지보수 및 안정적인 사용이 가능

☞ 임치의 대상은 생산방법, 설계도, 매뉴얼 등 기술상의 정보와 재무, 회계, 원가, 각종 보고서 등 경영정보를 포함

기업 대응 전략 (보안 10대 수칙)

수칙 9. 중요한 기술은 특허나 기술자료 임치로 보호해야 안전합니다.

- 중소기업은 핵심 기술정보를 제3의 신뢰성 있는 기관(대·중소기업협력재단)에 보관하여 기술유출을 예방하고, 기술유출 발생 시 임치물을 이용하여 기술개발 사실을 입증
- 대기업은 중소기업이 파산·폐업 등을 한 경우, 해당 임치물을 이용하여 지속적인 유지보수 및 기술의 사용이 가능하게 하는 제도

- 부당한 기술자료 제공요구 금지(제25조제1항 제12호)
- 기술자료 임치제도를 이용 시 개발사실에 대한 법적 추정력 부여

기술상 정보

생산제조방법
시설제품 설계도 및 매뉴얼
물질 배합 비율 성분표
연구개발보고서 및 관련 각종 데이터
SW소스코드데이터 및 디지털 콘텐츠

경영상 정보

기업의 운영 및 관리와 관련된 기밀서류
(재무, 회계, 인사, 마케팅, 노무, 생산)

기업의 매출과 관련된 기밀서류
(원가, 거래처, 각종 보고서 및 매뉴얼)

기업 대응 전략 (보안 10대 수칙)

수칙 10. 정보시스템에 대한 보안을 철저히 해야 합니다.

- 메일/메신저 파일첨부 전송
- CD/USB 파일 저장 반출
- 업무시스템 주요 정보 화면Dump
- 출력물 반출
- PC반출/외부작업 시 유출
- 시스템/DB/NW관리자 의 정보유출
- 승인되지 않은 무선 장비의 장착을 통한 정
- 타인 권한을 도용하여 정보 획득 후 유출
- 접근이 통제되지 않은 시스템 권한 획득.및
- 협력/하청업체에 재 배포 및 가공이 가능한 형태의
- 외부에서 내부 업무시스템 접속 후 정보의
- 승인되지 않은 접근을 통한 업무시스템/주요 정보의
- 악성코드 유포로 인한 업무시스템 장애 유
- 악성코드 유포로 인한 공정시스템 장애 유발
- 승인되지 않은 유/무선 네트워크 접근을 통한 내부정보 절취
- 협력업체에 제공되는 시스템의 오접속 유 또는 노출로 인한 정보의 유출
- 협력업체/하청업체 시스템에 대외비 정보의 등록으로 인한 정보유출
- 사외에서 임직원이 업무시스템 접속 시 전송구간에서의 인증정보의 도청/절취, 전송자료의 도청/절취
- 해킹을 통한 대외 서비스 시스템의 고객정보 및 주요정보의 절취
- 해킹을 통한 대외 서비스 시스템(홈페이지/B2C, B/B)의 조작 및 변경
- DDoS 공격을 통한 대외 서비스 시스템 및 N/W 장비의 서비스 중단
- 해킹 후 대외 서비스 시스템 및 업무 시스템을 악성코드 유포경로로 활용
- 해킹을 통한 내부망 / 공정망 침입 후 업무 시스템 / 공정 시스템 공격

너무 많다.

해야 할 것이 .

보안 USB / Device 통제	PC 보안
DLP (Data Loss Protection)	
출력물 보안 시스템	
PC DRM	
Anti-Virus	
SBC	
서버 접근제어	서버 보안
DB 접근제어 / 암호화	
Anti-Virus	
Session 로깅	
IP 관리 시스템	네트워크 보안
무선 보안시스템 (인증 / 차단)	
발신로깅 및 차단	
L2 보안 스위치	
Firewall	
NAC	
VPN	
SSL VPN	
DDoS 방어	
IDS / IPS	
Proxy	
웹 방화벽	App 보안
소스코드 보안	
SSO	
PKI	
Application 문서 DRM	
Application 도면 DRM	
보안 웹 하드	
화면 Dump 방지 – Web DRM	
취약점 분석 Tool	
OTP	
통합 시스템 모니터링/관제/위험관리	보안 관리
패치 관리 시스템	
전사적 계정관리 시스템	
통합 로그분석 시스템	

자료출처: 더존ISS 교육자료

기업 대응 전략 (벌점제 도입)

보안 위규 항목별 벌점 기준

CASE

구분	보 안 위 규 항 목	벌점
4급 보안 위규	. 사원증 未소지(2회), 추가위규시, 0.5점 추가 · 퇴근후 PC전원 미OFF · 사내에서 사원증 미패용 · 보안당직 미실시(중식시간) · 사원증 분실 · 내방객 관리 소홀(무단배회) · Key 방치(개인서랍, 문서함) · 대외비문서 세절기 미사용 · 대외비 문서/도면 방치(업무용 수첩 포함) · 핸드폰 스티커(렌즈, 메모리Port) 미부착 · PC 3대 패스워드 未설정 · 책상서랍 또는 문서함 미시건	1점
3급 보안 위반	· 불법 소프트웨어 사용 · 개인 저장매체 미신고 반입 (저장매체에 당사 자료가 없는경우) · 비업무성 자료의 사내 배포 · 보안스티커(카메라폰 포함) 고의 훼손 · 무단 공유폴더 생성 · 보안교육 무단 불참	2점

구분	보 안 위 규 항 목	벌점
3급 보안 위반	· 미등록 정보기기의 사용 (USB, PDA, 노트북, MP3, 외장 HDD 등) · 대외비 자료를 불필요한 수신자에게 송부 · 대외비 본문/첨부파일이 포함된 싱글메일 전송시 대외비 자료 대외비옵션 미설정 · 대외비 문서 또는 도면의 싱글게시 · 싱글로 대외비 문서/도면/공정데이터를 무단으로 사외 송부시 · 회의실 등 공용PC내 자료 방치	2점
2급 보안 위반	· 무단 사진 촬영 · 개인PC내 보안프로그램 무단 삭제 · 메일을 통한 대외비 자료 사외 송부 · 사원증 타인 대여 · 보안시설의 고의적 파손 · 저장매체에 대외비자료 저장 무단반출 (대외비문서, 공정데이터, 도면등 포함) · 대외비자료(출력물 등) 무단반출	3점
1급 보안 위반	· 저장매체 은닉後 무단 반출 (고의성, 대외비 자료 포함) · 대외비자료 은닉후 무단 반출(고의성)	5점

기업 대응 전략 (벌점제 도입)

CASE

순번	항목	Penalty
1	외부 Mail 미 승인 발송	15점 (상)
2	정보 저장 매체 무단 반·출입	
3	PC Plus 미 설치	
4	회사 생산제품(시료품 등)의 무단 반출	
5	비문관리 Process 위반	
6	사외 Network 무단 사용	
7	중요문서 방치	10점 (중)
8	비 인가 Network 장비 사용	
9	보안라벨 미 부착 및 훼손	
10	노트북/정보저장매체 방치	
11	보안검색 불응/업무 방해	
12	VPN ID 대여 및 무단도용	
13	보안서약서 미 제출	
14	개인정보저장매체 무단 반입	
15	Fax 발송 Process 미 준수	5점 (하)
16	ID카드 도용/대여	
17	PC 패스워드 설정기준 미 준수	
	취약 공유 폴더 사용	
18	방문객 관리 Process 미 준수	
19	환입 처리 기간 미 준수	
20	불법 Software 사용	

✓ **취지**
보안의 생활화와 자율준수 문화 조성

✓ **조치 사항 (개인별)**
과거 3년간의 누적 점수

- 30점: 팀장 통보
- 50점: 본부장/사업부장 통보
- 70점: 징계위원회 회부

* **매월 Team Security Score 현황을 취합하여 임원들께 Report함.**

기업 대응 전략 (단계별 로드맵)

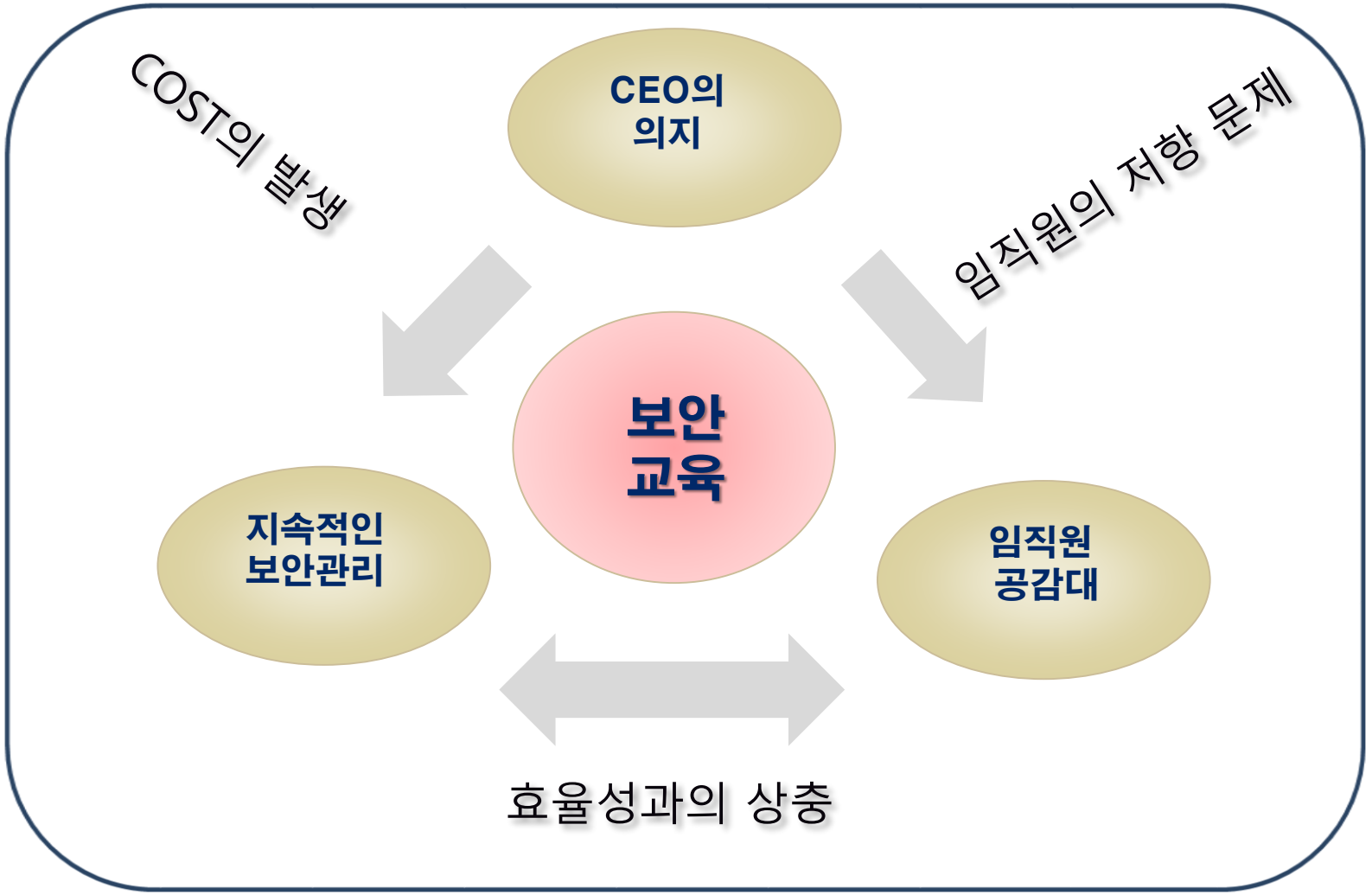
CASE

구분	구현 항목 / 단계	1단계 보안수준(C급)	2단계 보안수준(B급)	3단계 보안수준(A급)
법인형태	❑ 법인의 중요도에 따라 분류	❑ 일반법인(판매/SVC)	❑ 주요법인 (생산/제판, 대표,판매)	❑ 핵심법인 (연구소, 연구소가 있는 생산/제판)
보안조직	❑ 보안담당자/조직	❑ 보안 전담자(1명)	❑ 보안 전담자(2명)	❑ 보안 전담자(2명 ↑)
관리적 보안	❑ 보안규정/기준 ❑ 비밀유지서약서 ❑ 보안교육/홍보 ❑ 진단/점검, 비문관리 ❑ 사고 대응/조치 ❑ 인원보안(협력업체,퇴직자) ❑ 위험관리(RM)	❑ 규정 수립 ❑ 비밀유지서약서 수취 ❑ 보안교육/홍보 ❑ 자체 보안점검	❑ 기준 등 보안절차 수립 ❑ 전문가 양성 교육 ❑ 정기 보안진단 ❑ 사고대응체계 구축 ❑ 퇴직자 관리 ❑ 협력업체 관리 ❑ 비문관리	❑ 정책/제도 변화관리 ❑ 상시 Audit체계 ❑ 전문적 사고대응 ❑ 핵심인력 관리 ❑ ISMS 구축(위험관리)
물리적 보안	❑ 방문객/보호(통제)구역 관리 ❑ 감시(CCTV / DVR)관리 ❑ 출입통제시스템 ❑ 저장매체관리 ❑ 보안검색 장비 ❑ 폐문서 처리 (세절기) ❑ 도.감청탐색	❑ 방문객 관리 ❑ 보호(통제)구역 관리 ❑ 감시 장비(CCTV/DVR) ❑ 출입통제시스템 ❑ 저장매체 반출/입 관리 ❑ 폐문서 관리	❑ ID카드 발급 관리 ❑ 차량 출입관리(차량통제) ❑ 주차장, Layout 재정비 ❑ 면회실 별도 구축 ※ 면회실 : 외부인 사무실 출입 통제 ※ 물리적 보안 표준 Guide	❑ 보안검색 장비 - X-Ray, EAS 등 ❑ 통합 모니터링시스템 ※방문객, 사무실 출입, 저장매체 소 지, 저장매체 반출/입 등 ※ 물리적 보안 표준 Guide
기술적 보안	❑ Client PC(PC검) ❑ 인터넷접속관리 ❑ SP (Security Portal) ❑ 메일 모니터링, DRM ❑ 무선 랜 통제/서버 관리	❑ Client PC(PC 점검)	❑ SP(방문예약,저장매체 관리, ID카드 발급 등) ❑ 메일 모니터링	❑ 인터넷접속관리 - 메신저,P2P 등 ❑ 서버관리(도면, 소스 보관서버) ❑ DRM(업무 기간시스템) ❑ 무선LAN 통제/관리
	❑ 전사 공통시스템	❑ PC Plus, WWSCAN, FAX보안시스템, PC DRM, 통합 모니터링시스템 ※ 통합 모니터링시스템 : PC Plus, DRM, 메일, 메신저, FAX 수발/신 등		

기업 대응 전략 (요약)

- 등급분류 및 표시 ·고지의 원칙
- 최소인원 참가의 원칙
- 최적 보관의 원칙
- 기록 보존의 원칙
- 책임한계 명확화의 원칙
- 3내 (視內 · 手內 · 函內) 원칙
- 철저한 상의하달의 원칙(C-Level의 솔선수범)
- 공수래 공수거 원칙

기업 대응 전략 (보안교육의 중요성)

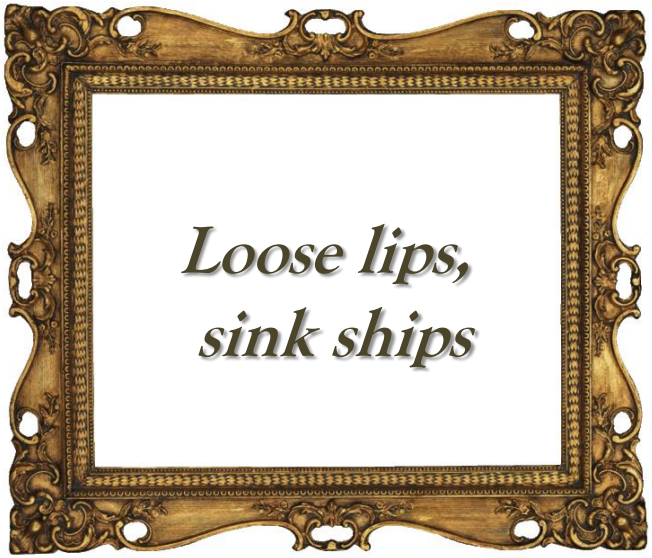


보안! 최대의 취약점은 사람!

『회사정보를 안전하게 보호하려면 첨단 보안시스템 도입보다 임직원 보안의식 제고 가 가장 중요하다』

-전설의 해커, 해커들의 우상 Kevin Mitnick


5' 0"
4' 6
4
사내보안의
첫 번째 책임은
사장님!



1977 Apple lobby

"**情報**가 열리면 **企業**은 무너집니다."

Q & A

감사합니다

[참고 자료 출처]
- ✓ 국가정보원 산업기밀보호센터
- ✓ 김앤장 법률사무소
- ✓ 대중소기업농어업협력재단 기술보호지침
- ✓ 산업스파이방어전략(김종길 저)
- ✓ 관리보안핸드북(신현구 외)

중부대학교 경찰경호학부
Security Mgt Ph.D 신현구
010-9072-9255 / 041-750-6749
peter7664@joongbu.ac.kr