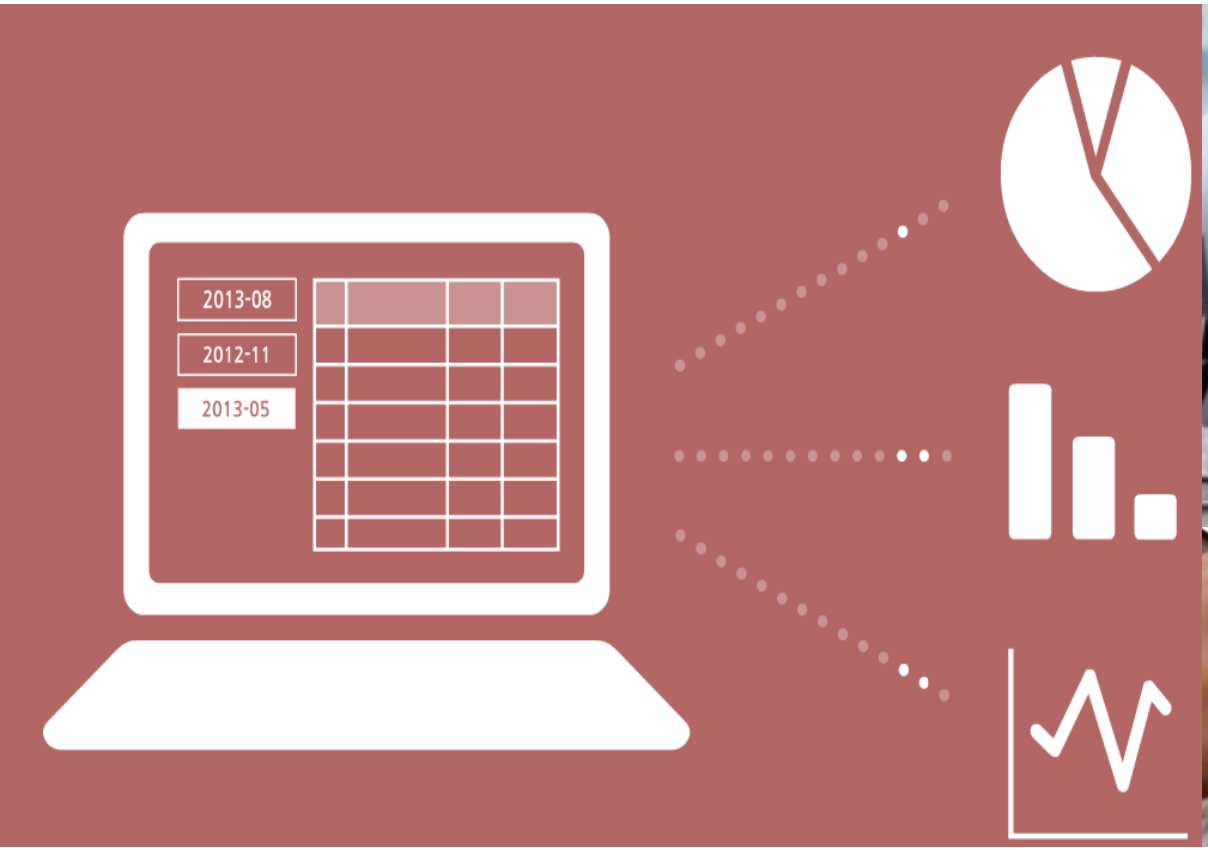
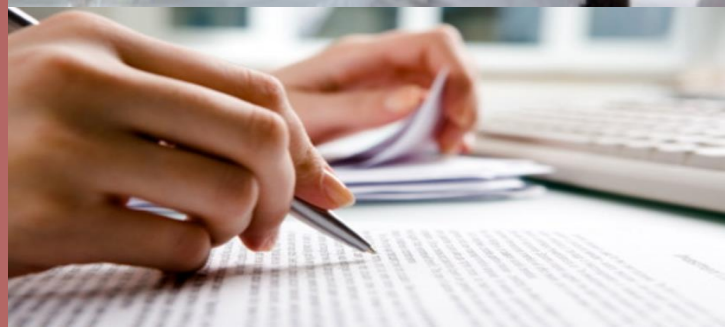


# 함께하는 연구보안 추진전략

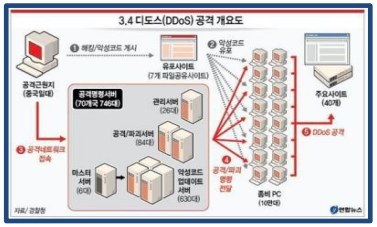
중앙대학교 산업보안학과
장 항 배 교수
(hbchang@cau.ac.kr)

# 최신 보안사고 현황

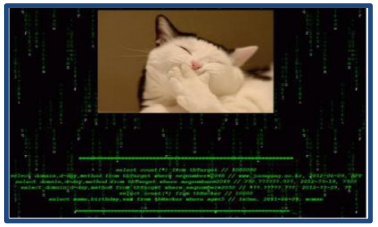
## 외부 사이버 공격


농협 전산망 해킹
(2011년)


네이트 개인정보 유출
(2011년)



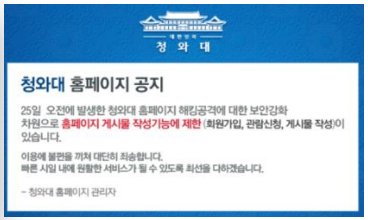

3·4 DDoS 공격
(2011년)



중앙일보 홈페이지 해킹
(2012년)


KT, 개인정보 유출
(2012년)


3.20 전산대란
(2013년)



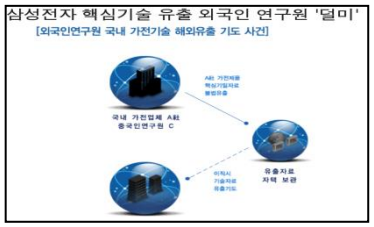

6.25 사이버테러
(2013년)


통신 3사 개인정보 유출
(2013년)


국토부 개인정보 유출
(2014년)

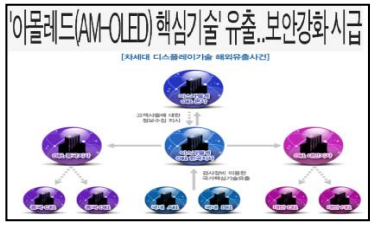
# 최신 보안사고 현황

## 내부 정보유출 사고



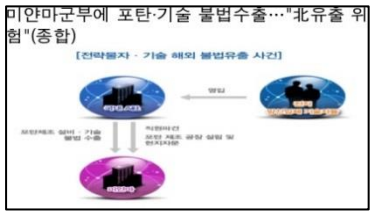

삼성전자 핵심기술 유출 (2011년)


태양전지 핵심기술 유출 (2012년)

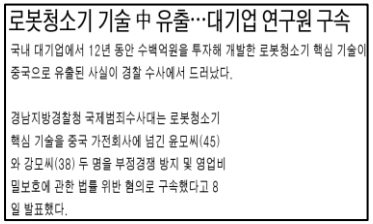



삼성 OLED핵심기술 유출 (2012년)


국방부 내부정보 유출 (2013년)




군 기술문서 유출 (2013년)




로봇청소기 핵심기술 유출 (2014년)


카드 3사 개인정보 유출 (2014년)


한수원 원전도면 유출 (2014년)


방위사업청 사업기밀 유출 (2015년)

# 최신 보안사고 현황

## 내부 정보유출 사고




# 중요정보 유출원인

## 중요정보 유출사고 원인(사회경제적 원인)

o 경제규모의 확대: 경제규모가 커지면서, 산업범죄의 규모 또한 증가하고 있음

o 기술의 향상: 기술이나 기밀 등에 대한 상품성이 높아짐

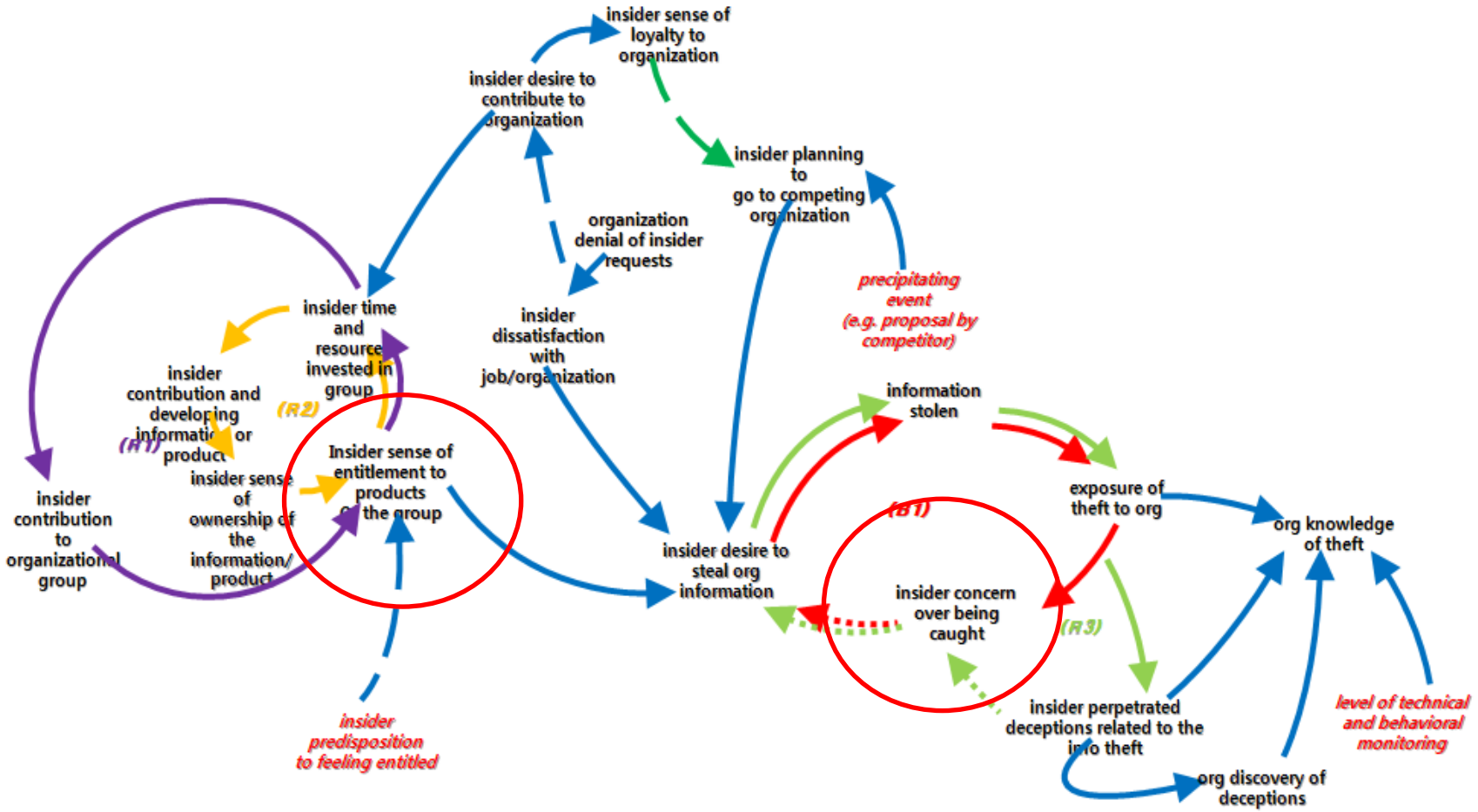
## 중요정보 유출사고 원인(범죄학적 원인)

o 억제적 요인: 잡힐 가능성 < 산업범죄를 저지르면서 생기는 이득 → 합리적 선택을 수행

o 발달적 요인: 각종 이유를 들어 자기의 잘못된 행위를 중화(합리화)시켜 도덕, 양심 등 범죄를 억제하는 기제들을 무력화하기 때문에 범죄행위가 용이해짐 ("회사는 이익을 많이 내고 있는데도 월급을 적게 받고 있으니까, 나는 당연히 일부를 가질 자격이 있다") → 사회적 중화(neutralization) 이론

# 중요정보 유출원인

## Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition(CERT, 2009)



# 중요정보 유출원인

## 중요정보 유출사고 원인(상황적 원인)

o 일상 활동(Routine Activity)이론 = 동기 부여된 범죄자 + 적당한 대상(매력 정도↑)
+ 능력 있는 보호자 부재(보호 정도↓) → 범죄기회 발생

o 범죄피해 확률 = 근접성(proximity) × 노출(exposure)
→ 중요정보 접근가능 용이성 ↑ + 중요정보 접근통제 수준 ↓

# 중요정보 취약점 조사

## 관리적 취약점 1

**내부자 위협 대응책에 대한 명확한 문서화**

**핵심부품/중요정보 유출 정책/규정/지침/절차 등이 미흡**

- 보안 관련 정책/규정/절차 등에 인가된 내부자에 의한 정보유출 방지를 위한 내용들이 미흡하거나 없음
- 응용 시스템 운영자 등 특수권한 보유자들이 준수해야 하는 정보유출 방지를 위한 구체적인 지침이 없음

**직무분리 및 최소 권한 부여 원칙 준수**

**기 제공된 접근권한 정책 및 기능 무시**

- 응용 시스템에서는 접근권한을 세분화 하여 접근제어를 할 수 있는 기능이 있지만, 사용하고 있지 않음(세분화된 권한관리 기능이 없는 시스템도 존재)
- 편의상 필요이상의 접근권한을 부여하여 사용하고 있어 정보유출 가능성이 높음

**전사적 위험평가를 주기적으로 수행**

**중요정보에 대한 조사 및 등급 분류 미흡**

- 어느 곳에서 어떤 종류의 핵심부품/중요정보 생성/유통/관리되는지 파악하지 못함
- 다양한 종류의 핵심부품/중요정보 정보가 민감도에 따라 분류, 관리 되지 않고 있음

**전 직원 대상 주기적 인식제고/훈련 수행**

**내부자 정보유출 방지에 대한 부정적 인식**

- 인가된 내부자에 의한 정보유출은 심각한 문제로 인식하지 못하고 있음
- 인가된 내부자에 의한 정보유출 사고는 미연에 방지할 수 없는 문제라고 대부분 인식

# 중요정보 취약점 조사

## 기술적 취약점

**의심스러운 행위에 대한 모니터링 및 대응**

### 응용 시스템의 정보유출 기능 미흡

- 응용 시스템 상에 내부자에 의한 정보유출 및 오남용 방지를 위한 기능이 없거나 미흡

### 다양한 정보유통 경로 상의 정보유출 통제 미흡

- USB 등 휴대용 저장매체를 통한 정보유통이 통제되고 있지 않음
- 메일이나 P2P 등으로 핵심부품/핵심정보를 발송할 경우 이를 감시할 수 없음

**직원들의 시스템 사용에 대한 로그 감시 및 대응**

### 대량 추출된 핵심부품/중요정보 파일의 보안관리 미흡

- 중요정보를 엑셀로 변환하여 업무활용 후 해당 파일을 삭제하지 않음
- 중요정보를 포함하고 있는 문서 초안 또는 완성 본이 담당자 PC에 남아있음
- PC에 저장된 핵심부품/중요정보를 포함한 파일들이 실수 또는 고의로 유출될 가능성이 높음

### 보안 시스템 우회 경로 존재

- 타 부서 및 기업과의 정보 공유를 위해 보안시스템의 일부 기능(영역복사 가능 등)을 사용하지 않고 있음
- 협업업체가 다른 제조사의 보안 시스템을 사용하는 경우 보안기능을 해제하여 송부

# 중요정보 취약점 조사

## 기술적 + 관리적 취약점

**강력한 사용자 인증 및 계정관리 정책과 절차 준수**

### 업무 편의를 위한 ID 및 비밀번호 공유

- 업무 편의상 ID 및 비밀번호를 공유하여 사용하고 있음
- 외부 업체에 제공된 사용자 ID와 패스워드를 외부 업체 직원들이 공유하여 사용
- 공유 ID에 의한 사고 발생시 책임 추적 성 확보 어려움 상태

**퇴사시 응용 시스템 접근권한 차단**

### 정보 접근 권한 변경관리 미흡

- 접근권한 변 경시 수동 또는 지연 처리로 인한 휴면, 미 삭제, 미 변경 계정 존재
- 퇴사 직원 계정을 이용한 사고 발생시 책임 추적 성 확보 어려움

**시스템 관리자 및 특수권한 소유자에 대한 각별한 주의**

### 직무분리 및 최소권한 부여 원칙 준수 취약

- 응용 시스템 관리와 보안관리를 1명이 수행
- 응용 시스템(데이터베이스) 관리자 등 IT 담당자에게 과도한 접근권한 부여
- 응용 시스템 또는 DB 관리 목적의 PC가 인터넷에 상시 접속되어 있어 민감한 정보의 다량 유출 가능성이 높음

### 외주 용역업체의 보안 관리 미흡

- 부분적인 응용 시스템의 관리는 외주 용역업체에 전적으로 의존하고 있음
- 외주 용역업체 직원에 의한 정보 접근 등의 이력관리가 이루어지지 않고 있음
- 외주 용역업체 직원에 의한 사고 발생시 책임 추적 성 확보가 매우 어려움

# 중요정보 취약점 분석

## 중요정보 취약점 분석결과

### 중요정보 취약점 조사결과

- 내부자 정보유출 방지에 대한 부정적 인식
- 중요정보 유출 정책/규정/지침/절차 미흡
- 업무 편의를 위한 ID 및 비밀번호 공유
- 직무분리 및 최소권한 부여 원칙 준수 취약
- 외주 용역업체의 보안 관리 미흡
- 정보 접근 권한 변경관리 미흡

### 중요정보 유출사고 근본원인

- 내부자에 의한 문제를 과소평가, 의도적 무시
- 의심스러우면 쓰지 말고 썼거든 믿으라는 유교문화

- 보안보다 편리성, 신속성을 우선시
- 겉으로 보이는 성과 위주 업무 수행

- 합리적, 논리적, 체계적 보안 의사 결정 구조 취약
- 조직의 저항을 최소화하면서 문제를 해결하려는 경향

- 형식적인 인식제고/훈련/교육 실시
- 인식제고 위주의 교육만 실시

- 보안을 기술적 대책으로만 해결하려는 경향

# 공공기관 보안의식 조사결과 시사점

개념적으로 인지하고 조직의 보안수준

**구성원들의 조직 보안수준에 대한 “공감대(공유)” 형성 필요**

실제적 측정된 조직의 보안수준

**기관장 보안(계획수립, 업무지원 등) 추진 의지 및 활동 수준**

기관장 보안담당자 일반직원

**기관장의 가시적인 보안 활동 필요**

# 공공기관 보안의식 조사결과 시사점

**보안 정책 및 규정 준수 수준**

**신규(변경) 보안 정책 및 규정에 따른 기존업무 변화 수용성**

기관장 일반직원 보안담당자

**아직도 일반직원은 “보안”은 불편한 것으로 받아들여지고 있으며,**

**이에 대한 의식제고 노력(캠페인, 개인 업무평가 반영, 세분화된 보상/처벌 규정 등) 없이**

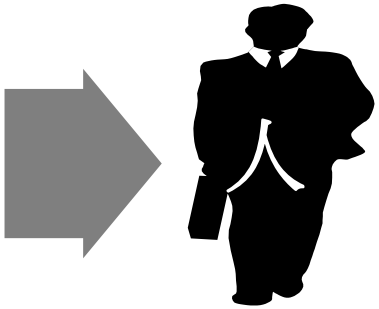
**보안지식이 실제 보안행위로 옮겨지기 어려울 것으로 예상됨**

# 공공기관 보안의식 조사결과 시사점

## 조직 보안수준

## 구성원 보안의식





**(사례) "주기적인 평가를 통해 관련 지식을 획득"**

o 평가(test)를 통과하여야 정보시스템에 접근가능
o 평가를 통과하면 개인보안 인증서를 발급
(시작 점수(point) 부여)
o 개인보안 인증서는 주기적으로 발급하여야 함
o 보안에 위반하는 행위를 했을 경우 점수 차감
o 일정수준 이하로 점수가 하락했을 경우 재 평가

**구성원 보안인식** + **구성원 보안지식** + **구성원 보안행위**

**산업보안 중요성에 대한 가시적인 인식제고 노력 필요**

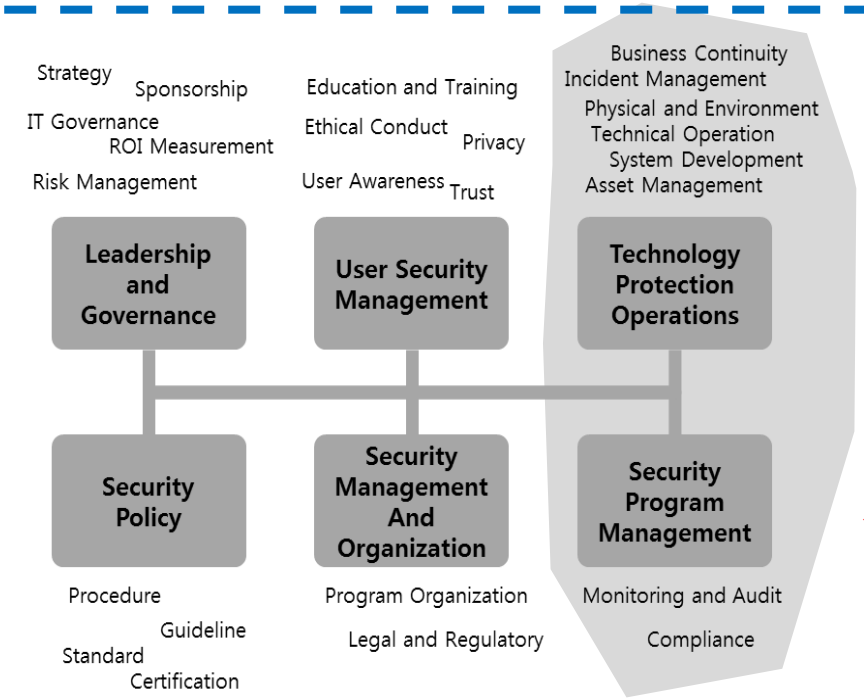
**일반직원, 보안담당자 대상의 전문지식 교육**

**알고 있는 보안지식에 대한 실제적인 훈련 및 점검 필요**

# 미래 산업보안 추진방향

## 미래 지능형 환경과 보안전략 설계방향

비 생물적 요소
(환경)




생물적 요소
(도구)

조직 내·외부의 보안위협 대응에 있어서도
**기술과학(공학)과 사회과학의 균형 感 있는 보안설계 중요**

# 연구보안 중요성

## 연구환경 변화

| (과거 연구환경) | | (현재 연구환경) |
|---|---|---|
| 폐쇄형 연구 | 글로벌화 → | 개방형 연구 |
| 무역보호주의 | 기술개발 가속화 → | 기술보호주의 |
| 문서화(종이) | IT 기기 활용(융합) → | 전자 파일화 |
| 단독연구 | 연구 대형화(협업) → | 공동연구 |

**연구환경변화에 따른**
**연구성과물 유출 가능성 증가!**

# 연구보안 중요성

## 연구보안 정의와 법령

**정부의 지원을 받아 국가연구개발사업을 수행하는 기관에서 연구내용 및 연구결과물이 외부로 유출되지 않도록 관리하는 제반 업무**

### 연구보안 관계법령

**[법] 산업기술의 유출방지 및 보호에 관한 법률**

**[시행령] 산업기술의 유출방지 및 보호에 관한 법률**

**[부령]국가 연구개발사업 공통보안관리규칙**

**[법] 과학기술기본법**

- 제 11조 제 5항 국가연구개발사업의 보안

**[대통령령] 국가연구개발사업의 관리 등에 관한 규정**

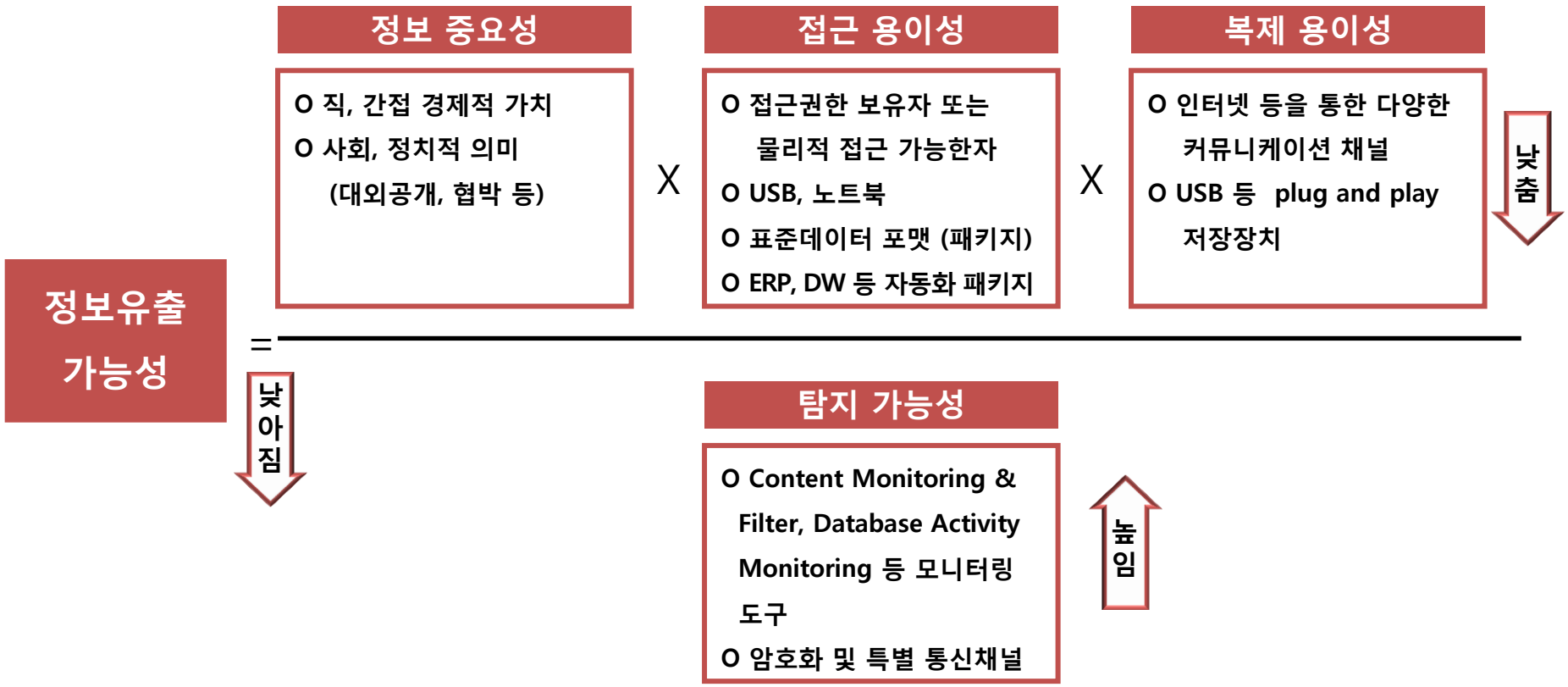
- 제 5장 국가연구개발사업의 보안 및 정보관리

# 연구보안 추진방향

## 연구성과 유출방지 추진전략


# 연구보안 추진방향

## 연구성과물 유출방지 관리모형



# 연구보안 관리체계

## 연구보안 추진체계

| 항목 | 내용 |
|---|---|
| 보안관리 심의회 구성 | O 보안관리심의회 구성과 운영에 관한 사항<br>O 보안관리심의회 위원장에서 중앙행정기관의 장 |
| 연구결과 보안등급화 | O 연구개발결과의 보안등급을 명시적으로 규정<br>O 연구개발 평가위원회에서 보안등급의 적절성을 검토한 후 변경 가능 |
| 보안실태 합동점검 | O 중앙행정기관의 장은 국가정보원장 등 관계기관 합동으로 실태점검<br>O 점검대상 및 시기, 내용 및 방법 등을 협의<br>O 개선명령을 받은 연구기관은 3개월 이내 관계기관 등에 보고 |
| 보안사고유형 설계 | O 보안사고의 유형을 구체화<br>O 정보의 유출, 누설, 분실, 도난<br>O 정보를 유통, 관리, 보존하는 시스템의 유출, 손괴, 파괴 등 |
| 해외유출 차단 | O 중요 연구정보의 국외유출을 방지하기 위한 사항[해외기술이전 시]<br>O 보안과제 관련하여 외국기관 방문 시 관계기관에 통보 |

# 연구보안 관리체계

## 연구보안 관리체계 구성

### 1. 보안관리체계

① 자체규정
② 보안심의회 운영
③ 보안책임자 지정
④ 보안교육
⑤ 외국기관과 공동연구 시 사전승인

### 2. 참여연구원 관리

① 보안서약서
② 퇴직예정자 관리
③ 방문자 관리
④ 해외 출장 시 보안교육
⑤ 외국인 별도 보안조치

### 3. 연구결과의 관리

① 보안등급 표기
② 해외기술이전 관계법령 준수
③ 제3자 실시계약 금지


### 4. 연구시설관리

① 통신매체 반입 절차 마련
② 정보보관실 특별관리
③ 출입자 개인별 권한 부여

### 5. 정보통신망 관리

① 방화벽
② USB 등 인가 후 사용
③ 데이터 백업 시스템 구축
④ 정보 시스템 사용기록 보관
⑤ 외부와 내부 망 분리

# 연구보안 관리체계

## 연구보안 성공요인

| | |
|---|---|
| 생각을 바꿔라 | O 전통적인 보안업무가 주로 외부자의 침입에 대비한 시스템이나 네트워크 보안에 초점<br>O 과거와 같은 접근방법에서 벗어나야 함 |
| 기본에 충실해라 | O 핵심정보 보안을 위한 기본적 활동은 외부자 침입 뿐만 아니라 내부자 보안을 위해서도 필수<br>O 기 제공된 보안 기반체계만 잘 준수하여도, 상당 수준의 정보유출을 방지할 수 있을 것임 |
| 끈기 있게 추진해라 | O 핵심 정보 보안의 성과를 보려면 장기적인 노력이 필요함<br>O 내부자 정보유출 방지에 대한 노력의 성과를 보려면, 단기적인 성과를 목표로 추진하기 보다는 장기적인 관점에서 꾸준히 추진해야 함 |
| 높은 사람을 움직여라 | O 내부자 정보유출은 조직 내부 구성원과 업무 프로세스를 대상으로 하기 때문에, 내부에서의 많은 저항이 예상 됨<br>O 높은 사람의 솔선수범과 적극적 지원이 없으면 성공하기 어려움 |
| 수준 및 동향을 측정하라 | O 정기적 조사 및 측정을 통해 취약점을 발견하고, 지속적으로 개선해야 할 포인트를 찾아야 함 |
| 변화관리 기법을 도입해라 | O 변화노력을 성공시키려면 변화관리 기법(예: unfreezing-moving-freezing) 기법, 저항관리 기법, 효과적 커뮤니케이션 기법 등을 도입, 실천해야 함 |
| 외부의 전문인력을 적극 활용해라 | O 내부에서는 객관적인 시각에서 내부의 문제점을 정확히 파악하기 힘듦<br>O 외부 전문 인력을 통해 문제점을 파악하고 변화를 도모한다면, 업무 방식 변경에서 오는 내부 저항을 최소화시킬 수 있으며 또한 전문성을 도움 받을 수 있음 |

# 함께하는 연구보안 추진전략



## 경청해 주셔서 감사합니다!