연구보안

산업체 정보보호 실태조사

1) 정보보호 인식

2) 정보보호 기반 및 환경

3) 침해사고 예방

4) 침해사고 대응

5) 주요 서비스별 정보보호

KISMI 한국정보보호경영연구소
Korea Information Security Management Institute

1) 정보보호 인식

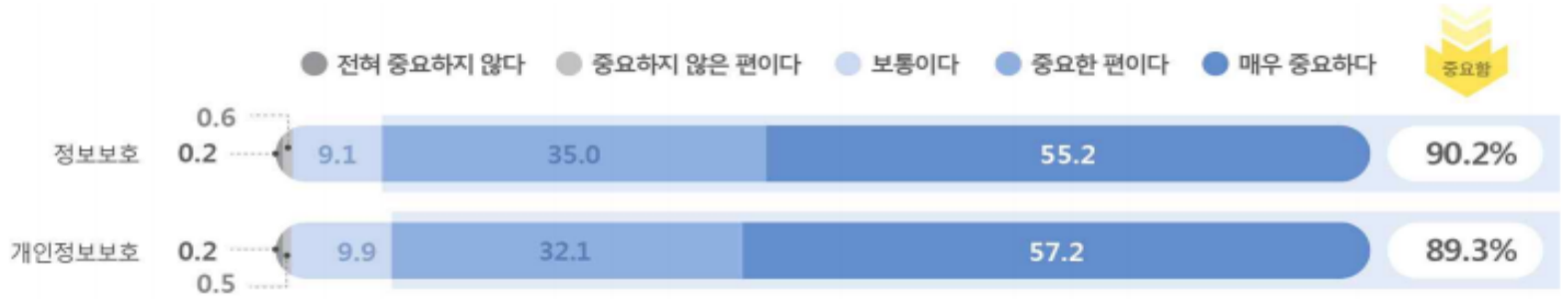
정보보호 중요성 인식 90.2%, 개인정보보호 중요성 인식 89.3%

▶ 네트워크에 연결된 컴퓨터 보유 사업체의 대부분이 정보보호 및 개인정보보호가 중요하다고 응답함

- '정보보호가 중요하다'고 인식하는 비율은 90.2%로 나타남
- '개인정보보호가 중요하다'고 인식하는 비율은 89.3%로 나타남

그림 1 - 1 정보보호 및 개인정보보호 중요성 인식률

(중요한 편이다 + 매우 중요하다, 단위 : %)



2) 정보보호 기반 및 환경

1. 정보보호(개인정보보호) 정책

사업체의 16.0%는 '정보보호 또는 개인정보보호' 정책 수립

- 사업체의 16.0%는 정보보호 또는 개인정보보호 정책을 수립하는 것으로 조사되었고, 전년(15.2%) 대비 0.8%p 증가함
- 규모별로 '종사자수 250인 이상(90.9%)' 사업체의 정책 수립률이 가장 높게 나타남 또한, '종사자수 10-49인(47.2%, 9.8%p↑)'과 '종사자수 50-249인(78.2%, 9.9%p↑)'에서 정책 수립률이 전년 대비 증가함

그림 1 - 2 정보보호(개인정보보호) 정책 수립률

(단위 : %)

2. 정보보호(개인정보보호) 조직

'정보보호 또는 개인정보보호' 조직 보유 5.5%, 전년 대비 4.4%p 감소

- 공식적인 정보보호 또는 개인정보보호 조직을 보유한 사업체의 비율은 5.5%로, 전년(9.9%) 대비 4.4%p 감소함
- 사업체의 정보보호(개인정보보호) 조직 보유율은 종사자 규모 전층에서 전년 대비 감소함

그림 1 - 4 정보보호(개인정보보호) 조직 보유율

(단위 : %)

2) 정보보호 기반 및 환경

3. 정보보호(개인정보보호) 교육

사업체의 28.0%는 '정보보호 또는 개인정보보호' 교육 실시

- 2017년 1년 간 임직원 대상으로 정보보호 또는 개인정보보호 교육을 실시한 비율은 28.0%로 전년(30.4%) 대비 2.4%p 감소함
- 규모별로 '종사자수 250인 이상(97.0%)' 사업체의 교육 실시율이 가장 높게 나타남 또한, '종사자수 10-49인(75.0%, 8.9%p↑)'과 '종사자수 250인 이상(97.0%, 6.1%p↑)'에서 교육 실시율이 전년 대비 증가함

그림 1 - 6 정보보호(개인정보보호) 교육 실시율

(단위 : %)

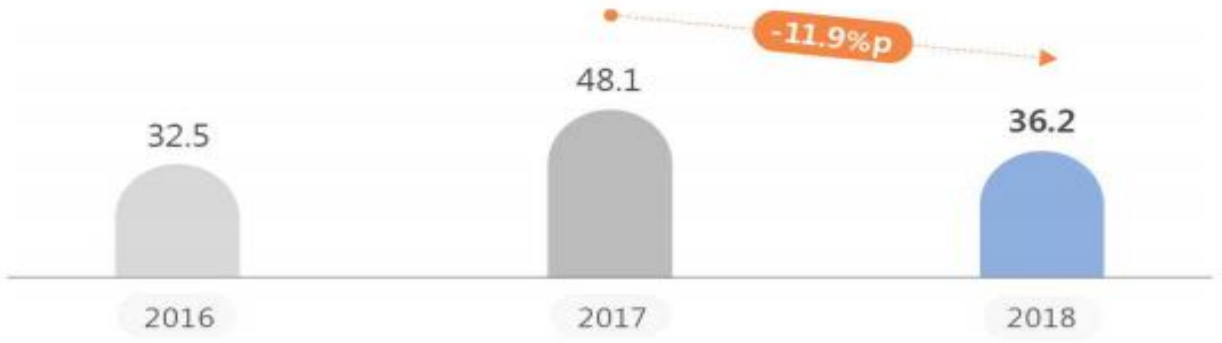
4. 정보보호(개인정보보호) 예산

'정보보호 또는 개인정보보호' 예산 편성 36.2%, 전년 대비 11.9%p 감소

- 2017년 1년 간 사업체의 36.2%는 IT 예산 중 정보보호 또는 개인정보보호 예산을 편성함
- IT 예산 중 정보보호 또는 개인정보보호 예산이 차지하는 비중은 '1% 미만(25.2%)'이 가장 높았으나, 전년(36.8%) 대비 11.6%p 감소함

그림 1 - 8 정보보호(개인정보보호) 예산 편성률

(단위 : %)



3) 침해사고 예방

가. 정보보호관리_시스템 및 네트워크 보안점검

사업체의 90.0%는 '시스템 및 네트워크 보안점검' 실시

- '시스템 및 네트워크에 대한 보안점검' 실시율은 90.0%로 전년(64.7%) 대비 25.3%p 증가함
  - 특히, 비정기적으로 보안점검을 실시하는 사업체는 67.1%로, 전년(42.3%) 대비 24.8%p 증가한 것으로 나타남
- 유형별로는 'PC의 취약점' 점검률이 99.0%로 가장 높고, 다음으로 '물리보안(55.4%)', '서버 운영체제(OS)(50.7%)' 등의 순으로 조사됨

그림 1 - 14 시스템 및 네트워크 보안점검 실시율

(단위 : %)

3) 침해사고 예방

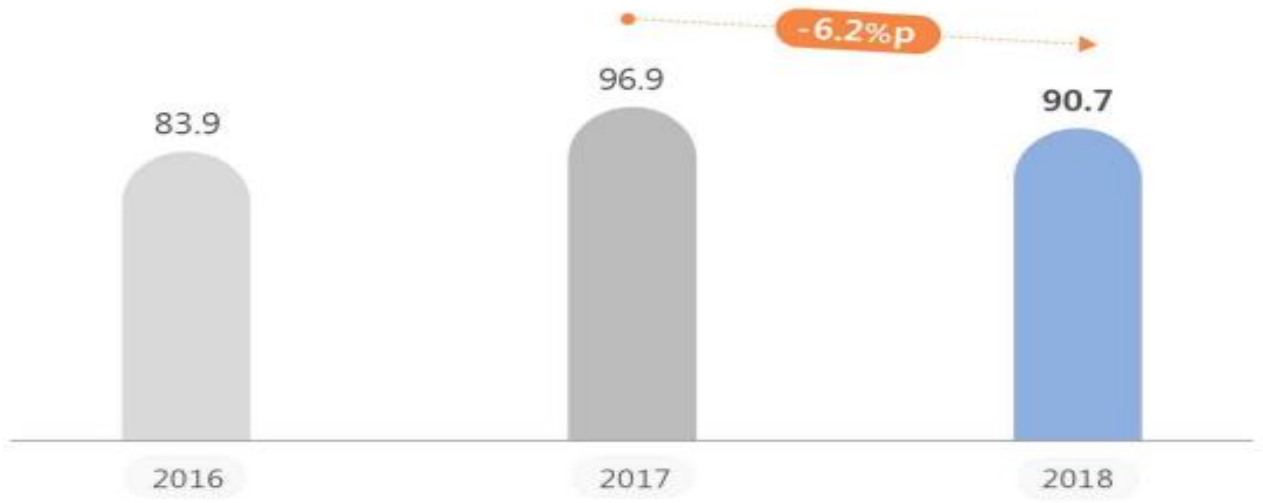
나. 보안패치 적용

'보안패치' 적용 90.7%, 전년 대비 6.2%p 감소

- 사업체의 90.7%는 PC나 서버에 보안패치를 적용하는 것으로 조사되었고, 전년(96.9%) 대비 6.2%p 감소함
- 보안패치 유형별로는 '정보보호 시스템'에 적용하는 비율이 97.3%로 가장 높았고, 다음으로 '내부에서 이용하는 서버(95.5%)' 등의 순으로 조사됨

그림 1 - 16 보안패치 적용률

(자동 + 수동 + 문제 발생 시에만 업데이트, 단위 : %)



3) 침해사고 예방

다. 시스템 로그 및 데이터 백업 실시

'시스템 로그 또는 데이터 백업' 실시 49.8%

- 사업체의 49.8%는 시스템 로그 또는 중요 데이터를 백업하는 것으로 나타났고, 전년(52.5%) 대비 2.7%p 감소함
- 유형별로 '시스템 로그 백업' 실시율은 30.5%, '중요 데이터 백업'은 47.3%로 나타남
  - '중요데이터' 백업률은 2016년 35.5%, 2017년 46.8%, 2018년 47.3%로 증가 추세임

그림 1 - 18 백업 실시율

(단위 : %)

4) 침해사고 대응

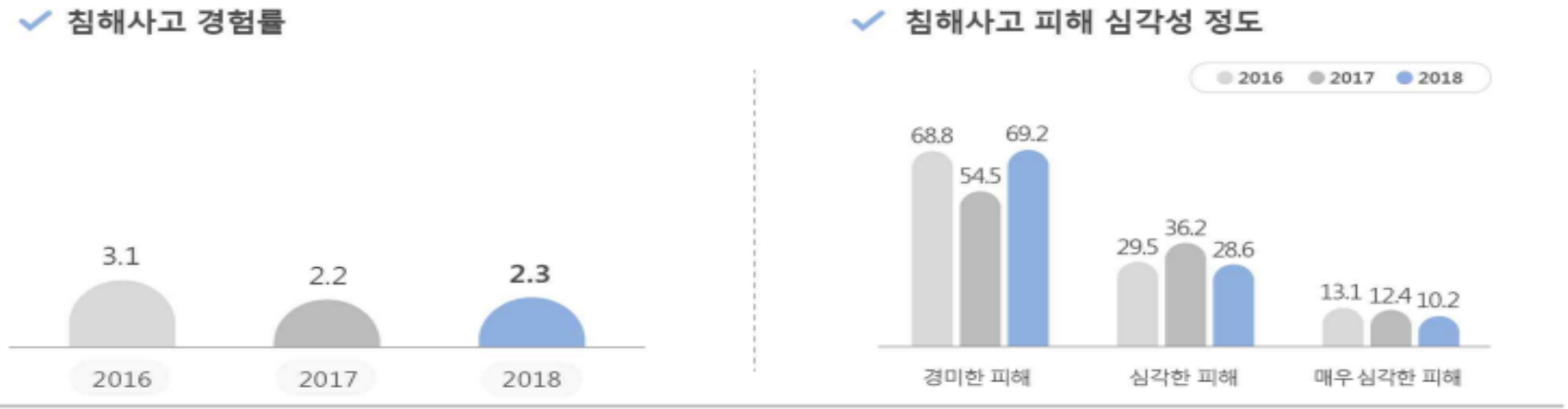
1. 침해사고 경험

사업체의 2.3%가 침해사고 경험

- 2017년 1년 간 사업체의 2.3%는 해킹, 악성코드, DDoS, 랜섬웨어 등 침해사고를 경험함
  - 침해사고는 '경미한 피해(69.2%)'가 가장 많았음
- 침해사고 경험 유형으로는 '랜섬웨어'가 56.3%로 가장 많았고, 다음으로 '악성코드(컴퓨터 바이러스, 웜, 트로이잔 등)에 의한 공격(47.7%)', '애드웨어/스파이웨어 감염(12.1%)' 등의 순임

그림 1 - 20 침해사고 경험 및 피해 심각성 정도

(단위 : %)



2. 침해사고 대응

침해사고 대응활동 수행 17.4%, 전년 대비 8.5%p 감소

- 사업체의 17.4%는 침해사고에 대응하기 위한 활동을 수행하는 것으로 조사되었고, 수행률은 전년(25.9%) 대비 8.5%p 감소함
- 대응활동 유형으로는 '침해사고 발생 또는 발생 징후 인지 시 대처를 위한 긴급연락체계 구축'이 10.9%로 가장 많았고, 다음으로 '침해사고 대응 계획 수립(7.8%)', '침해사고대응팀(CERT) 구축 및 운영(5.1%)' 등의 순으로 나타남

그림 1 - 22 침해사고 대응활동 수행률

(단위 : %)

5) 주요 서비스별 정보보호

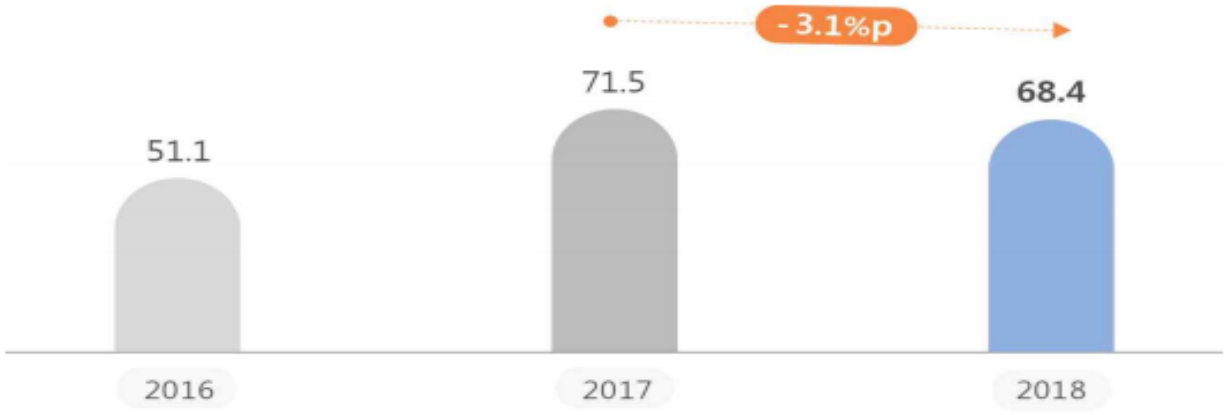
1. 무선랜

무선랜 구축 및 운영 68.4%, 전년 대비 3.1%p 감소

- 사업체의 68.4%는 사내 무선랜(Wi-Fi)을 구축하여 운영하고 있는 것으로 조사되었고, 전년(71.5%) 대비 3.1%p 감소함
- 사업체의 31.5%는 '무선공유기를 통한 악성코드 감염'을 가장 우려하는 것으로 나타났고, 다음으로 '무선공유기의 DDosS 등 공격도구로 악용(30.5%)'되는 것을 우려함

그림 1 - 30 무선랜 구축 및 운영률

(단위 : %)



5) 주요 서비스별 정보보호

2. 클라우드

'클라우드 서비스' 이용 7.4%, 향후 도입 또는 유지 계획 8.1%

▶ 사업체의 7.4%는 클라우드 서비스를 이용하는 것으로 조사되었고, 전년(6.6%) 대비 0.8%p 증가함
- 클라우드 서비스를 향후 도입 또는 유지할 계획은 8.1%로 전년(6.7%) 대비 1.4%p 증가함

▶ 사업체의 56.2%는 '데이터 위탁저장에 따른 정보유출'을 가장 우려하는 것으로 나타났고, 다음으로 '자원 공유·집중화로 서비스 장애시 대규모 피해 발생(54.9%)'을 우려함

그림 1 - 32 클라우드 서비스 이용 및 향후 도입(유지) 계획

(단위 : %)

✓ 클라우드 서비스 이용률

✓ 클라우드 서비스 향후 도입(유지) 계획

3. 사물인터넷(IoT)

'사물인터넷(IoT) 제품·서비스' 이용 9.1%, 전년 대비 4.2%p 증가

- 사물인터넷 제품 및 서비스 이용률은 9.1%로 전년(4.9%) 대비 4.2%p 증가함
  - 사업체의 10.9%는 사물인터넷 제품 및 서비스를 향후 도입 또는 유지할 계획으로 조사되었고, 전년(5.5%) 대비 5.4%p 증가함
- 사업체의 44.3%는 '정보유출'을 가장 우려하는 것으로 나타났고, 다음으로 '해킹 및 악성코드 감염(42.7%)', '무선신호교란 및 장애(40.4%)' 등의 순임

그림 1 - 34 사물인터넷(IoT) 제품·서비스 이용 및 향후 도입(유지) 계획

(단위 : %)

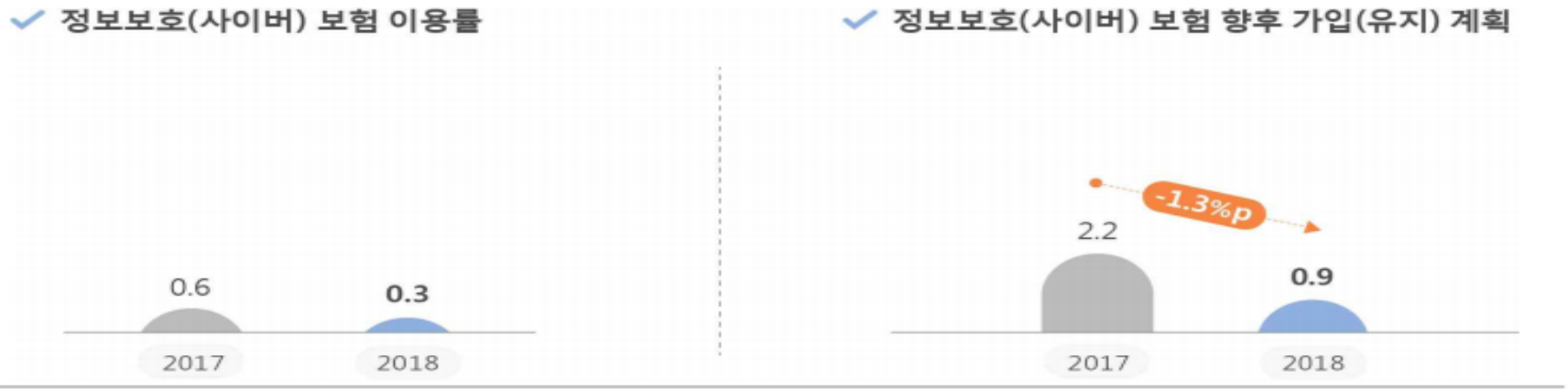
4. 정보보호(사이버) 보험

'정보보호(사이버) 보험' 이용 0.3%, 향후 가입 또는 유지 계획 0.9%

- 정보보호(사이버) 보험 이용률은 0.3%로 전년(0.6%)과 비슷한 수준임
  - 사업체의 0.9%는 정보보호(사이버) 보험을 향후 도입 또는 유지할 계획으로 조사되었고, 전년(2.2%) 대비 1.3%p 감소함
- 정보보호(사이버) 보험 가입 시, '개인정보 유출 사고 발생 시 배상 비용(70.9%)'이 가장 보장받고 싶은 사항으로 조사되었고, 다음으로 '개인정보 유출 사고 발생 시 대응 비용(조사, 통지, 법률자문)(70.1%)' 등의 순으로 높게 나타남

그림 1 - 36 정보보호(사이버) 보험 이용 및 향후 가입(유지) 계획

(단위 : %)



연구보안

산업기술 비밀 유출과 보호

1) 산업기술보호 법률 및 대응방안

2) 연구보안 행동 수칙

3) 연구스파이 색출 요령

KISMI 한국정보보호경영연구소
Korea Information Security Management Institute

1) 산업기술보호 법률 및 대응방안

산업기술유출관련 처벌조항

산업기술유출방지 및 보호에 관한 법률위반 제 36조(벌칙)

산업기술을 외국에서 사용하거나 사용되게 할 목적 으로 제14조 각 호의 어느 하나에 해당하는 행위를 한 자 ⇒ 10년 징역 또는 10억원 벌금

제14조 각호의 어느 하나에 해당하는 행위를 한 자 ⇒ 5년 이하의 징역 또는 5억원 이하 벌금

제 37조(예비 · 음모) 제36조 1항의 죄를 범할 목적으로 예비 또는 음모한 자 ⇒ 3년 이하의 징역 또는 3천만원 이하의 벌금

부정경쟁방지 및 영업비밀보호법 위반

부정한 이익을 얻거나 기업에 손해를 입힐 목적으로 그 기업에 유용한 영업비밀을 취득 · 사용 또는 제3자에게 누설 한 자 ⇒ 10년 이하의 징역 또는 그 재산상 이득액의 2배 이상 10배 이하에 상당하는 벌금

형법 제356조 (업무상의 배임)

업무상의 임무에 위배하여 제355조의 죄를 범한 자 ⇒ 10년 이하의 징역 또는 3천만원 이하의 벌금

1) 산업기술보호 법률 및 대응방안

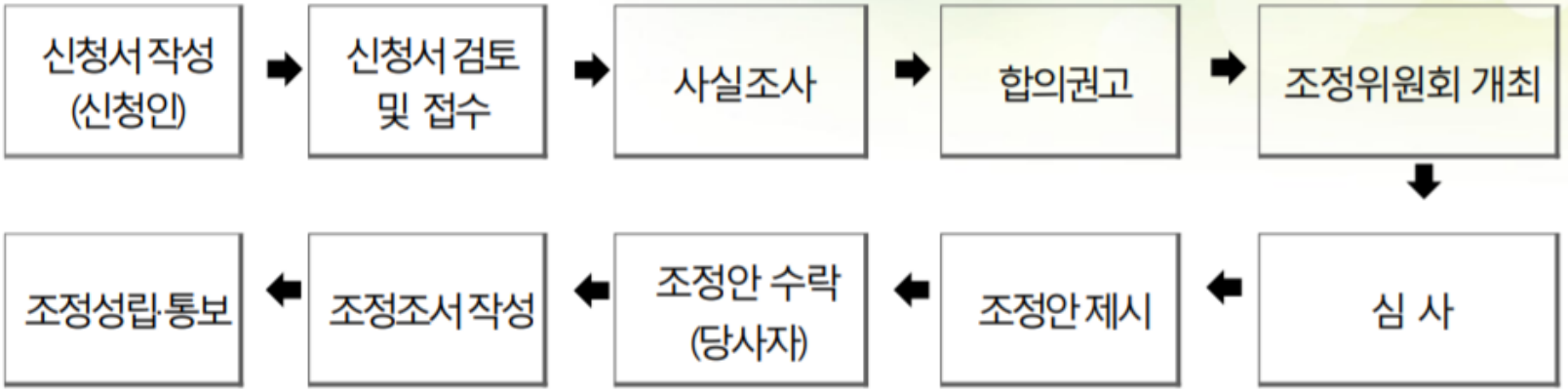
산업기술분쟁조정위원회

산업기술분쟁조정제도란

산업기술의 유출 등*에 대한 당사자(기업·연구기관·대학·개인 등)간의 분쟁 사건을 신속하게 조정하고 해결하기 위한 제도

* 산업기술의 침해행위, 부당한 기술탈취, 기술자료의 유출 등에 관한 분쟁

조정절차(3개월 소요)



상담 및 접수 : 한국산업기술보호협회 분쟁조정위원회 사무국

02-3489-7012 / hjsmagic@kaits.or.kr

1) 산업기술보호 법률 및 대응방안

. 산업기술보호협회 업무(법률 제16조 4항)

- 산업기술보호를 위한 정책 개발 및 협력
- 산업기술의 유출 관련 정보 전파
- 산업기술의 유출방지를 위한 상담 · 홍보 · 교육 · 실태조사
- 국내외 산업기술보호 관련 자료 수집 · 분석 및 발간
- 산업기술 보안에 대한 자문 지원
- 산업기술분쟁조정위원회의 업무지원
- 그 밖의 산업통상자원부 위탁 사업 및 협회 정관이 정한 사업

2) 연구보안 행동수칙

1 신분증 관리

- 신분증은 출근시부터 규정된 위치에 패용한다.
- 신분증은 신분증명과 출입허용을 나타내는 증표이므로 관리에 주의 한다.
- 신분증은 어떠한 경우에도 타인에게 대여하거나 양도해서는 안된다.
- 신분증 분실 시, 비인가자의 출입을 예방하기 위해 즉시 총무인사팀에 신고한다.

Use of ID Badges

- ID badges must be worn as the way shown on left.
- ID badges, showing an employee's identification and authorization of entry, must be taken a good care of.
- ID badges cannot be lent or borrowed in any case.
- At the loss of ID badges, immediate report to the General Affairs and Personnel Team is required to prevent an unauthorized person's entry to the property.

2 출 · 퇴근 시 정보보안

- 빈손으로 출근, 빈손으로 퇴근을 원칙으로 한다.
- 미인가 정보저장매체(PC, 외장형HDD, USB, CD/DVD)의 무단 반 · 출입을 삼간다.
- 퇴근시나 자리를 비울 때는 책상 위에 방치되는 자료가 없도록 하고, 중요문서나 정보저장매체는 캐비넷 등에 보관한다.

Information Security When Arriving and Leaving Work

- Do not bring things in or take them out when arriving and leaving work.
- Do not bring in or take out unauthorized information carriers such as PC, external HDD, USB, CD/DVD.
- Do not keep important documents or information carriers on desk unattended, and surely keep them in a cabinet when leaving the office.

2) 연구보안 행동수칙

3 외부 방문객 출입 보안

- 외부 방문객의 사내 출입 시 반드시 사전예약 후 방문토록 한다.
- 외부인원 사내 출입 시 반드시 방문증을 패용토록 하고, 안내자가 동행한다.
- 내방객의 사무실 출입을 최대한 제한하고, 면회실 등 지정된 장소를 이용하도록 한다.

Security for Visits

- Visits must be pre-authorized.
- A visitor must wear a visitor's ID badge and be accompanied with an employee as a guide.
- A visitor can only visit least number of offices and sites that must be pre-arranged.

4 문서 보안

- 민감한 문서는 가급적 복사하지 않고 이면지로 사용하지 않는다.
- 비밀내용이 포함된 문서나 자료 또는 폐지 등은 반드시 세절하여 소각하며 단 한장이라도 함부로 버리지 않는다.
- 전출 또는 퇴직 시 보유하고 있는 모든 비밀문서는 반드시 반납한다.

Security for Documents

- Do not make copies of sensitive documents nor use them as scrap paper.
- Shred and burn classified documents when they become waste and do not simply throw any of them.
- Return all the classified documents as being transferred or retire.

2) 연구보안 행동수칙

5 업무비밀 보호의무 준수

- 업무를 수행함에 있어 취득하거나 알게되는 회사의 모든 정보를 사전 승낙 없이 제3자에게 공개 또는 누설, 제공하지 않아야 한다.
- 또한 이를 업무목적 이외의 부정한 목적으로 사용하지 않아야 한다. "너만 알고있어"식의 비밀누설을 엄금하고 작은 정보라도 경쟁사에 큰 도움이 될 수 있다는 것을 명심하여 보안을 생활화한다.
- 업무수행 관련 지식이나 노하우는 문서화 하여 지적재산으로 등록 후 활용한다. 사내 상주 외부인(외국 기술고문, 고용인, 컨설턴트, A/S업체)이 민감 정보를 요청할 때에는 반드시 공식절차를 거치도록 하며, 정보는 엄격히 선별하여 제공한다.
- 비밀유출의 주된 경로는 항상 내부에 있음을 명심한다.

Observance of Work Confidentiality

- Any information acquired at work should not be disclosed to the third party without pre - permission. Also, do not use the information for inappropriate purpose except for work.
- Disclosure like "it is between you and me"cannot be accepted. Keep it in mind that any bit of information can be a help to a competitor.
- Knowledge and know-how from the work should be documented and registered as IP. Contractors (including foreign researchers, contract-workers,consultants, A/S personnel) must be allowed limited access to important information. When they ask, information must be selectively offered.

6 원내 생활 보안

- 원내에서 무단 촬영을 금지한다
  출입이 금지된 통제구역은 철저히 '통제' 한다.
- 보안 취약부분 발견 시 반드시 보안 부서에 통보하여 조치한다.
- 보안사고는 은폐하지 말고 보안부서에 즉시 보고하여 대처한다.
- 주변에 누군가가 기밀을 탐지할 수 있음을 명심하고 보안상의 허점은 없는지 점검한다.

Security for Everyday-life at KIRAMS

- Unauthorized shooting and photo taking are not allowed. Access limited areas should be kept such.
- Security weakness identified must be reported to the security team.
- Security-related incidents should not be hidden, rather immediately reported to the security team.
- Check any possible security weak points since anyone can steal secrets.

2) 연구보안 행동수칙

7 컴퓨터 사용 보안

- PC부팅, 윈도우, 화면보호기 암호를 설정하고, 주기적으로 변경한다. 화면보호기는 항상 "10분 이내"로 설정.
- 공유 폴더를 사용할 경우 반드시 암호를 설정 하고, 사용은 최소 인원으로 설정.
- 바이러스 검색 및 예방 소프트웨어를 설치하고 초기 동작시에 작동토록 하며 항상 최신 버전을 유지하도록 자동 업데이트한다.
- 시스템을 사용하지 않을 때나 자리를 비울 때는 반드시 로그아웃 한다.
- 인터넷 브라우저 보안레벨은 사용업무에 따라 적정한 레벨로 사용.
- S/W는 항상 정품을 사용한다.
- 정보저장매체(PC/외장형HDD/USB/CD/DVD)는 반드시 승인된 것만 사용한다.

Security for PC

- Passwords must be installed and regularly changed for PC booting, windows, screensavers. Screensavers must be on when the computer is not in use for 10 minutes or less.
- Sharing folders must be used with passwords. Ensure that only the least number of people can share them.
- Virus check-up and preventive software must be activated from the start when a PC is on. Always update them to keep the latest version of them.
- Log out when PC is not in use or the user leaves the desk.
- Security level for internet browser should be designated according to work.
- Use only original software.
- Use only authorized information carriers (PC, external HDD, USB, CD, and DVD).

8 통신보안

- 패스워드는 영문, 숫자를 조합하여 8자리 이상 사용한다.
- 외부로 메시지(e-mail, FTP 등)를 전송할 때는 반드시 회사에서 지급한 계정만을 사용한다.
- 업무용 PC로 웹하드, P2P 등 파일공유 사이트 접속을 금지한다.
- 해킹의 우려가 있는 이메일이나 웹상에서 중요정보를 공유하지 않는다.
- 의심스러운 외부메일은 열람하지 않고 삭제하고, 자동보안 패치를 설정한다

Security for Communication

- Use 8-digit-or-more passwords composed of English alphabets and numbers.
- Use accounts only offered by the firm when a message (e-mail, FTP, etc.) is transmitted to the outside.
- Do not use the office PC to access file-sharing sites such as web-hard or P2P.
- Do not share e-mails or important information on the internet vulnerable to hacking.
- Do not read suspicious emails sent from outside source, delete them, and install an automatic security patch.

3) 연구스파이 색출 요령

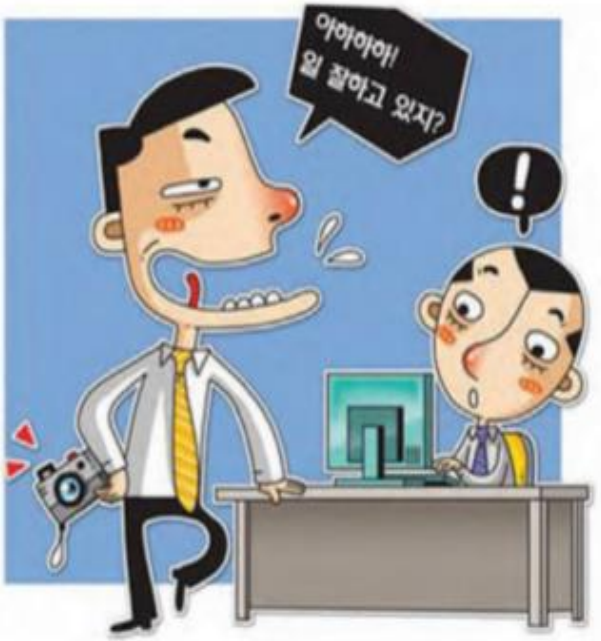
1 업무 시 산업스파이 색출 요령

① 본인의 업무와 관련 없는 다른 직원의 업무에 대해 묻는 사람

A person who asks for work information that is not related to his or her work

② 업무와 관계없는 영상장비를 사무실에 반입하는 사람

A person who brings a camera to office with no reason



3) 연구스파이 색출 요령

③ 본인의 업무와 관련 없는 부서와 사무실을 번번히 출입하는 사람

A person who often visits other offices and teams with no relation to his or her own work

④ 기관 기밀이 보관되어 있는 장소에 주어진 임무와 관계없이 접근을 시도하는 사람

A person who attempts to gain access to labs or offices with secrets kept with no clear relation to his or her work

3) 연구스파이 색출 요령

5 평상시와 다르게 동료와의 접촉을 회피하는 등 최근 정서변화가 심한 사람

A person who avoids contacts or often shows emotional ups-and-downs

6 주요업무에서 근무하다 이유 없이 갑자기 사직하는 사람

A person who suddenly quits from important work with no reason

3) 연구스파이 색출 요령

⑦ 업무를 빙자, 주요 기밀자료를 복사하고 개인적으로 보관하고 있는 사람

A person who personally copies and keeps confidential documents or materials on the pretext of work

⑧ 주어진 업무와 관련 없는 DB에 자주 접촉하는 사람

A person who often gains access to DB that is not related to his or her own work

3) 연구스파이 색출 요령

⑨ 동료가 없을 때 컴퓨터에 무단 접근하여 조작하는 사람

A person who uses the computer of a colleague with no pre-permission when the colleague is away from the PC

⑩ 특별한 사유없이 일과 후나 공휴일에 빈사무실에 혼자 남아 있는 사람

A person who stays alone in the office after working hours or during the weekends with no special reason

3) 연구스파이 색출 요령

⑪ 기술습득보다 고위관리자나 핵심기술자 등과의 친교에 관심이 높은 연수생

A student or trainee who is interested in making aquantance with high-ranking managers or Key researchers rather than in learning

⑫ 자기 주거지에 동료가 방문하는 것을 지나치게 기피하는 연구원

A researcher who never accepts any visits of other researchers to his or her residence

3) 연구스파이 색출 요령

⑬ 연구활동보다는 연구성과물 확보에 지나치게 집착하는 연구원

A student or trainee who is interested in making aquantance with high-ranking managers or Key researchers rather than in learning

⑭ 시찰, 견학을 하면서 지정된 방문코스 외에 다른 시설에 관심을 갖고 있는 방문객

A researcher who never accepts any visits of other researchers to his or her residence

감사합니다.

KISMI 한국정보보호경영연구소
Korea Information Security Management Institute