「산업기술보호지침」 제43조(산업보안 안내서)에 따라 마련한 ‘산업보안 안내서’을 다음과 같이 제정·공지합니다.

산업보안 안내서

제정 2021년 4월 15일

제1장 산업기술 유출·침해 예방 및 보호 조치

제1절 관리적·인적 보안 관리

1. 보안정책과 보안계획

(1) 보안정책이란?

① 보안(관리)책임자가 보안 관련 사항에 대해 어떻게 운영하고 관리할 것인가를 하는 방향과 범위를 정하는 것이다. 그리고 중요한 목적은 보안을 실행하는 임직원 등에게 그 내용을 알리는 것이며 경영진의 승인은 필수이다. 아이 따라서 현장에서 사용자 또는 관리자 등 임직원이 각종 보안위험 요소들로부터 안전하게 자산을 보호하기 위해서 반드시 준수해야 할 원칙과 필수 사항을 설정하고 공지하는 것이다.

② 보안정책 수립은 단순히 보안관련 사항을 정하는 것이 아니라 보안사고에 대한 대책과 보안역량 향상을 위해서 구체적으로 어떻게 할 것인가 하는 주요 사항이 포함되어야 하며 보안정책 수립에 있어서 다음과 같은 중요성이 확보되어야 한다.

- 최소한의 투자로 최대의 보안 효과 유발
- 기술보호 등 보안 준수에 대한 진실성과 가시성 확보
- 최고 경영진의 지원과 신뢰를 기반
- 보안감사 기준 제시 및 책임회피 방지
- 현재와 미래의 변화에 대처하는 기준 제시

③ 조직의 보안 현황을 기초로 보안정책의 범위 및 책임과 이행 방향 등 보안정책 수립 시에는 사전에 아래와 같은 사항이 필요·충분하게 담보되어야 한다.

- 보안정책 설계를 위한 최고경영진 포함 보안책임자 승인
- 최고 경영진에게 보안정책의 필요성과 개념 인지
- 보안정책을 누가·어떻게 담당할 것인가에 대한 책임 명확화
- 사전 보안실태 취약점 점검 및 위험 분석 및 수준 평가

(2) 보안계획 수립

① 보안취약점 및 보호수준 분석

- 기업 등에서 보안사고의 발생 위험성이 높을수록 보안에 대한 중요성은 높아진다. 그러므로 기술 등 자산의 중요도를 평가하여 유출 또는 침해의 위험성을 분석한다. 또한 기술정보에 접속하는 임직원에 대한 보안관리 수준과 유출의 위험성도 분석한다.
- 임직원의 보안의식 수준 측정과 함께 보안취약점 분석은 다음 사항을 고려하여 평가한다.

> ※ 보안취약점 및 보안수준 분석 항목 (예시)
>
> · 보안규정과 세부지침 유무
> · 전담조직과 책임자 및 담당자 유무 및 업무 능력
> · 물리적인 보안시설, 보안장비 등의 구축 유무
> · 정보보안 시스템 등 도입 여부
> · 임직원의 보안의식 제고 활동과 참여도 등

② 연간 보안계획 수립

보안업무도 다른 직무와 같이 계획성 있는 추진을 위해서는 보안정책 수립만으로는 부족하고 조직의 보안역량 제고를 위한 구체적인 연간 보안계획이 필수적하다. 다음은 연간계획 수립 시 고려할 사항이다.

- 보안취약점 점검 결과 분석과 이러한 취약점에 대한 대책
- 연간 주요 사업이나 신규 사업에 대한 보안상 현안과 개선 대책
- 전년도 보안감사 또는 보안업무 심사분석 및 보안진단 시 제기된 문제점에 대한 개선 대책
- 보안교육 및 유출·침해 예방활동 등 보안관리에 관한 사항
- 기타 보안역량 개선을 위한 세부 계획 등을 포함

2. 보안조직 구성 및 역할

(1) 보안(관리)책임자 및 보안실무(전담)조직 구성·운영

① 보안조직은 기술보호 등 보안대상과 범위 등을 고려하여 전담조직 또는 겸임조직(Task force 등)으로 구성한다. 다만, 보안 활동의 독립성 보장 근거와 보안정책 이행 및 보안직무 전문성 확보를 위하여 총무 등 유사·관련부서와 분리한 보안조직 구성이 필요하다.

② 겸임조직으로 구성하더라도 보안직무에 대한 공식적인 지정 등의 인사절차가 필요하며, 보안직무에 대한 독립적인 평가를 통한 독립적 보안업무 환경 구축이 필요하다.

③ 보안조직에서는 보안정책 심의사항이나 규정의 제·개정 등의 활동은 관련 위원회를 구성하여 운영할 수 있다.

④ 산업기술 관련 각 부서의 장을 보안(관리)책임자로 지정하여 각 부서의 산업기술 보호 및 유출예방 활동업무를 수행한다.

⑤ 산업기술보호를 위해 보안조직에서 가장 필요한 역할은 현재 시행하는 산업기술보호 수준을 파악하는 것이다. 산업기술의 보호 수준의 파악은 미흡한 보안 분야를 도출하고 이에 대한 적절한 보호조치를 취하고 있는지 확인하고 보고하는 것이다.

(2) 산업기술보호 전담관리체제 구성

① 최고경영진 산하에 국가핵심기술 또는 산업기술보호를 위한 보안(관리)책임자를 지정한다.

② 국가핵심기술 또는 산업기술보호 관련 보안전담인력(담당자)이 2인 이상이 가능할 경우 각 부서(분야)별로 보안전담인력(담당자)을 지정한다.

③ 기관의 규모에 따라 산업기술보호의 필요성이 높은 경우(예시: 국가핵심기술 분야, 이직·전직이 잦은 업계, 기술경쟁이 심한 분야 등)에는 산업기술(국가핵심기술) 관리책임자 소속 하에 별도의 전담조직을 구성하고 운영한다.

3. 보안규정 수립 및 제·개정

(1) 보안규정 수립 방향

① 임직원이 보안활동을 일관성 있게 준수하기 위하여 다음 사항을 반영하여 항목, 방법, 주기 및 통제 등을 구체적으로 정한 보안규정을 수립한다.

- 규정된 세부사항은 관련 근거가 제시되도록 하고 그 내용을 구체적으로 작성
- 임직원이 준수해야 하는 보안 관련 법적 요구사항을 분석하고 반영

- 보안정책에서 정해 놓은 보안활동 주기, 수준, 방법 등 일관성 유지
- 보안규정은 상위조직 또는 관련기관 정책과의 연계성을 분석하여 내용상 상호 부합여부를 확인하고 적정성을 유지
- 필요한 경우 분야별 지침, 절차서 또는 매뉴얼을 별도로 마련

② 보안규정은 가능한 한 규격화된 단일규정으로 모든 보안관리 사항을 포함하고 임직원이 자의적인 해석이나 변칙적으로 시행할 수 없도록 명확하게 표현하고 구체적으로 규정한다.

③ 보안규정은 경영진(대표 또는 이사회 등)에 의해 승인된 보안규정으로 존재하여야 하며, 보안(관리)책임자 및 보안전담인력(담당자)을 비롯한 모든 임직원이 인지하도록 한다.

④ 보안규정 또는 지침 등 보안정책은 연1회 이상 검토하고 개정을 하는 경우에는 경영진에 보고·승인 이후 모든 임직원에게 공지한다.

⑤ 다음과 같은 경우를 포함하여 주기적으로 보안정책 타당성을 검토하여 보안규정을 개정한다.

- 내부·외부감사 결과/중대한 보안사고 발생/관련 법령 제·개정/새로운 보안 위협 또는 취약점 발견
- 보안환경의 중대한 변화, 사업 환경의 변화(예: 신규사업 확대) 및 정보통신 환경 또는 정부정책의 변화 등

⑥ 보안규정에 관련 법률 및 사업 등을 고려한 보안사고 등급을 수립하고 댓가성·의도성·재발가능성을 고려한 징계기준을 마련한다.

⑦ 보안규정 제·개정에 따른 전반적인 내용은 사전에 사내 또는 외부 법무 전문가 등의 검토가 필요하다. 이는 사내 규정임에도 관련 법령에 저촉되거나 위반하는 내용으로 정해 질 경우에는 향후 해당 규정의 효력이 발휘될 수 없는 경우가 있을 수 있기 때문에 이에

대비하여 보안규정을 제·개정 과정에서 법무 전문가 등의 검토는 이를 예방할 수 있기 때문이다.

(2) 보안규정 수립 검토

① 목적: 임직원 등이 참여하거나 관여하는 기술자산의 보안유지 및 효율적인 보안 활동을 도모하기 위함이다.

② 정의: 산업기술보호 등을 위한 보안규정의 용어를 정의한다.

③ 적용대상·범위: 보안규정의 적용에 따른 접근권한 등 대상과 범위를 정한다.

④ 보안조직: 기술자산 등의 보안관리를 효과적으로 수행하고 운영하기 위해 보안조직을 구성에 대한 내용을 정한다.

⑤ 분류기준: 기술자산의 중요도 및 위험도에 따라 보호·관리하는 기술자산의 등급을 설정한다. 대상기관의 장은 기관 내에서 생성된 문서·자료 등 기술 자산에 대하여 최소 3가지 등급 이상으로 분류할 수 있도록 분류기준을 정립한다. 다만 분류기준은 관련 법령 등에서 정하는 분류 기준과 방법을 반영할 수 있다

⑥ 자산분류 절차: 위 기준에 따라 생산된 기술자산을 구분하고 분류 및 확정하기 위한 절차를 정한다.

⑦ 기술자산의 중요도 및 위험도 평가 및 변경: 대상기관에 따라 기술자산의 중요도 및 위험도가 변경될 수 있으므로 주기적으로 평가하고 그에 따라 그 등급을 조정한다.

⑧ 기술자산의 중요도 및 위험도에 따른 조치: 기술자산의 등급에 따른 보안조치 항목과 내용을 규정한다.

⑨ 보안 위반 시 조치: 기술자산을 운영・관리・사용하는 자, 접근권한이 있는 자 및 제한된 자 등은 보안을 위하여 최선을 다하여야 하며, 이를 위반 시 관련 법규 또는 내부 징계관련 규정을 마련한다.

⑩ 보안사고 발생 시 처리: 기술자산 유출 등 보안사고가 발생한 경우 사고일시·장소, 사고자 인적사항, 사고내용 및 처리 절차, 후속조치 등을 정한다.

※ 보안규정 제・개정 참고사항(예시)

- 보안규정 제정 목적, 적용 범위, 용어 정의 등 총칙에 관한 사항
- 보안업무 및 역할의 분담 등 보안운영체계
- 보안업무 수행기구 및 관리감독제도와 절차에 관한 사항
- 보안교육, 보안 조치, 임용 및 퇴임시의 비밀유지 계약, 퇴직자 관리 등 인적보안에 관한 사항
- 비밀의 등급 구분, 취급 및 취급 인가, 수발, 보관, 활용, 파기 등 비밀의 보안조치에 관한 사항
- 임직원 및 외부인의 출입통제, 보호구역의 설정 및 보안관리 대책과 주야간 경비대책 등 시설보호에 관한 사항
- 기업 등의 기능이나 생산품, 취급업무 등을 고려하여 보안상 중요한 관리대상의 보안 관리에 관한 사항
- 협력업체와의 거래 등 관련업체의 보안 관리에 관한 사항
- 전산장비실, 정보통신처리 및 저장장치, 네트워크설비 등 정보통신 관련 기술적 보안에 관한 사항
- 보안사고 및 보안 위규자의 처리에 관한 사항
- 컴퓨터 외 모바일 기기, 노트북 등 다양한 기기 출현 등에 따른 기타 정보통신・전산기기 등의 보안에 관한 사항

4. 자산 분류 및 통제

(1) 산업기술보호를 위한 자산 구분

① 정보 자산: 금융정보, 마케팅정보, 업무관련 정보, 조직정보, 개인정보, DB 등 기관이 보유 관리하고 있는 모든 종류의 정보 (예: 문서파일, 데이터파일, 데이터베이스내의 데이터 등)

② 문서 자산: 정책/지침, 업무관련 문서, 인사기록, 보고서 등 기관이 보유 관리하고 있는 모든 문서 또는 자료 (예: 보고서, 계약서, 매뉴얼, 각종 대장 등)

③ 소프트웨어 자산: 운영 프로그램, 어플리케이션 프로그램, 통신 프로그램 등 정보시스템을 활용하여 생산, 저장 및 운용 프로그램

④ 물리적 자산: 서버 등 정보 시스템, 설비 등 기관의 업무에 활용되는 하드웨어, 방범 및 방재 시설 및 전력 설비 등의 자산

⑤ 인력 자산: 임직원, 퇴직(예정)자, 제3자(협력업체 임직원, 컨설턴트 등), 아웃소싱 직원 등 대상기관이 소속・관리하는 모든 인력

⑥ 대외기관 제공서비스: 클라우드 정보 서비스, 통신 서비스 등 대외기관으로부터 제공받는 서비스

(2) 자산의 보안등급 분류

① 자산의 보안등급 분류라 함은 자산의 가치와 중요성에 따라 등급을 결정하는 것으로, 기업 내 모든 문서・데이터 등을 포함함 자산에 대한 보안 등급 기준을 정하고, 등급에 따라서 비밀의 보관, 수발, 취급인가자 등 관리방법을 달리 하여야 하기 때문에 적정한 보안등급 분류가 자산을 보호하는 관건이라고 할 수 있다. 일반적으로 기관의 보안환경에 맞게 수립하여 운영한다.

② 보안등급 분류 및 책임

- 등급분류 권한은 결재권을 가진 부서장 또는 관리책임자에게 있다.
- 고의·실수로 자산 일부의 등급을 분류하지 않거나 잘못하여 분류하는 경우에 대한 책임은 결재권을 가진 해당 부서(팀)장에게 있다.
- 보안문서 분류는 최초로 문서를 생산한 작성(기안)자가 분류한다.

③ 보안등급 재분류

- 자산의 보안등급 재분류는 규정에 따라 비밀의 효력을 변경, 파기하거나 보존기간 자체를 합리적으로 변경하는 것을 말한다. 보존기간 변경 등도 해당 자산의 비밀효력의 변경을 가져오는 의미에서 볼 때 재분류라 할 수 있다.

(3) 분류된 자산의 보안 통제

① 보안등급에 따라서해 분류된 자산의 보안관리 및 통제를 위하여 다음 사항을 포함하여 추진한다.

- 자산별 관리책임자를 지정하거나 보안관리 전담부서 및 전담자를 선임하여 관리한다.
- 분류에 따른 주요 자산(출력자료, 전자문서, 전산정보 및 데이터 등)에는 접근권한을 설정한다.
- 보유하고 있는 자산에 대한 평가 및 보안등급 분류는 주기적으로 시행하고, 각각에 등급(극비, 비밀, 대외비 등)을 표시한다.
- 주요 자산의 신규 도입, 폐기, 재고 전환 등의 자산 변동사항을 파악하고 관리하여야 한다.

② 산업기술 보안관리 및 통제가 효과적으로 이루어지기 위해서는 내부에서 보안관리 조직 및 체계운영을 규정화할 필요가 있다. 따라서 비정기적으로 운영하기 보다는 보안규정으로 일원화된 보안관리 조직 및 운영시스템 하에 체계적으로 자산의 보안관리책임 여부,

접근 통제 및 자산관리 현황 파악·관리 등이 이루어지도록 하는 것이 바람직하다.

③ 산업기술보호를 위한 보안통제 및 관리를 전담하는 전담조직과 관리책임자 및 전담인력 등 책임자를 지정하고 역할과 직무범위를 규정화 한다.

5. 문서 보안

(1) 문서 등 보안관리 일반

① 생산되는 문서 등에 대한 생성/보관/파기에 대한 보안관리 방안을 수립한다.

※ 문서보안 관리 방안 (예시)

- 보관 불필요 및 보존 기한 만료 문서 파기
- 타인 작성 문서, 업무 무관 문서, 이전 부서 문서 등 본인이 책임 질 수 없는 문서 보관 금지
- 타 기과 내부문서, 정부기관 내부 문서 등 출처 및 보유 목적을 오해 받을 수 있는 문서 보관 금지 등

② 파일로 문서 또는 자료를 정보저장 시스템에 보관할 경우 암호화는 필수이며 외부에 의한 침해 위협이 높은 PC(인터넷 사용 가능)등에는 시스템 접속 및 문서관련 정보의 저장을 제한한다.

- 정보시스템 운영자/개발자 등 협력업체 직원 등의 철수/변경 시 보유 접속정보 점검 또는 회수
- 별도의 접속통제 솔루션을 활용하는 경우 파일 저장 금지 원칙 등 보안방안이 임직원에게 충분히 공지될 수 있도록 조치

(2) 문서 생산 및 비밀등급 표시

① 비밀의 표시는 분류된 문서에 대한 비밀등급을 외견상 식별할 수 있도록 표시하는 것을 말하며, 등급표시, 사본번호, 관리번호, 페이지와 보존기간 등 여러 가지 표시를 함으로써 취급인가자에게는 비밀임을 알려서 취급에 신중을 기하게 한다. 또한 비인가자에게는 경고하여 접근을 방지하려는 데 목적이 있다. 정보시스템에 저장된 전산문서를 다수 사용하고 있음에 따라 정보문서를 형태에 따른 비밀등급 부여는 기관별 정보보안 체계에 따라 차별화하여 관리할 수 있다.

② 비밀등급 표시

비밀등급의 표시는 그 비밀의 중요도에 따라 극비, 비밀, 대외비의 3단계 또는 회사의 사정에 따라 3단계 내외로 등급을 분류하고 비밀관리 방법과 취급절차 등에 차별화하여 관리한다.

- (문서 및 전산 데이터 등) 모든 보안문서 등에는 아래와 같이 등급을 문서의 우측 상단에 표시한다.

[표] 비밀등급 표시 (예시1)

극비	비밀	대외비
TOP SECRET	SECRET	RESTRICTED

[표] 비밀등급 표시 (예시1)

극비	비밀	대외비
TOP SECRET AAAA-0910-001	SECRET AAAA-0910-001	RESTRICTED AAAA-0910-001

- (필름 및 사진) 1매로 된 필름은 비밀표지가 되어 있는 봉투나 이에 준하는 용기에 넣어 보관한다, 연결되어 있는 필름은 처음과 끝에 해당 비밀등급을 삽입하고 봉투에 준하는 용기에 넣어 보관한다. 인화된 사진은 매표면 상하단 및 이면중앙에 적절한 크기의 비밀등

급을 표시하고 봉투나 이에 준하는 용기에 넣어 보관한다.
- (녹취록 또는 녹화물) 비밀을 녹음할 때에는 처음과 끝에 그 비밀등급과 허가되지 아니한 자에게 전달 또는 누설하는 때에는 관계법규에 의거 처벌한다는 경고 문구를 포함하여 녹음하고 봉투나 이에 준하는 용기에 넣어 보관한다.

③ 보존기간 표시

- 보존기간의 예고: 비밀문서 등을 생산하는 부서에서는 비밀등급을 분류할 때 파기예고 일자를 정할 수 있다. 기관마다 차이가 있지만, 보안문서는 예고일, 보존기간 등의 기준을 설정할 수 있다. 비밀을 접수한 부서에서 더 이상 비밀을 보관할 필요가 없을 경우에는 발송부서에 반송하거나 발송부서와의 협의 하에 예고문을 변경 또는 파기할 수 있다.
- 보존기간 상충: 보존기간을 정하는 경우 법규 또는 사내 보안규정에서 정하는 기준과 보안문서의 보존기간이 서로 상충된다면 관련 법규에 의한 보존기간을 따를 수 있다.
- 보존기간 이후 처리: 보존기간이 만료된 문서는 재분류 또는 파기한다.

(3) 비밀문서의 보관 및 관리

① 비밀문서의 보관

- 비밀문서를 생산하거나 수발한 이후에는 유출의 위험성이 없는 곳에 보관하고 필요시 열람 및 대출, 복제 등 다양하게 활용하고 그 용도가 종료되면 파기한다.
- 비밀문서의 보관은 비밀을 보호하는데 있어서 가장 중요한 수단중의 하나로, 화재, 도난 또는 파괴로부터 보호하고 비인가자의 접근을 방지할 수 있는 적절한 시설과 보관 장소에 보관하여야 한다.
- 시건장치도 관리책임자와 전담인력이 가능한 내·외부 열쇠를 분리

보관하고 카드리더기, 지문인식기, 홍채인식기, CCTV와 같은 보안설비를 사용하여 권한이 부여된 이용자만 접근할 수 있도록 한다. 또한, 보안문서에 RFID 칩을 내장하여 접근자가 사용한 문서의 기록을 남기고 불법적인 유출을 방지하기도 한다.
- 이러한 보안설비는 비용 투자가 많이 들고, 접근 및 이용이 번거로울 수 있으므로 비밀문서의 규모, 보안성 등을 종합적으로 고려하여 차별화하여 운영할 수 있다.

② 비밀문서 기록 유지

- 보안관리 의무가 있는 비밀문서의 양이 많거나, 문서관리의 편의성 및 정확성을 위하여 비밀관리기록부를 전산처리하여 관리할 수 있다. 중소기업에서는 비밀문서 자체가 소량이어서 비밀관리기록에 소홀하기 쉬우나 쟁송이 있는 경우 영업비밀로 인정받기 위하여 비밀관리 및 유지노력을 한 근거의 제시도 곤란한 경우가 있을 수 있으므로 비밀관리기록부는 필수적이다.
- 비밀관리기록부는 비밀문서 등의 작성・접수・발송・분류(재분류)・이송・이관 및 인계인수 등 일체의 사항을 관리하는 대장이다.
- 비밀대장은 수발사항이 명확히 기록되어야 하며, 특히 발송된 사본은 근거를 표시하여야 한다.

(4) 비밀문서 등의 파기

파기 예고일이 도래하면 재분류를 실시하고 그 용도를 다한 보안문서는 완전한 파기를 실시하여 보안상 의미 없는 관리업무의 과부하를 방지한다. (일반적으로 연1회 주기적으로 문서 파기 실시)

① 파기 시기(예시)

- 파기 예고일이 도래 하였을 때에는 업무상 계속 참조할 필요가 있는 경우 재분류 실시하여 파기일자를 연장할 수 있다.

- 파기 예고일 이전이라도 정기적인 점검(예시, 통상 년2회)을 통하여 보안문서 재분류하여 파기가 결정된 경우 파기할 수 있다.
- 생산된 보안문서가 등급분류시의 중요도에 비해 현저히 저하 되어서 현 시점에서 가치가 없거나 하는 경우 파기할 수 있다.
- 생산된 보안문서가 외부 유출되거나, 유사 기술이나 비밀이 타사에 의해 공개되어 가치가 현저히 저하된 경우 또는 기술관련 비밀이 특허로 등록되어 외부에 공개된 경우에는 파기할 수 있다.

② 파기 방법(예시)

- 일반문서의 파기는 문서 세단기를 이용하여 세절하여야 하며, 일반도면이나 코팅도면의 경우 소각 또는 대형 세단기를 이용하여 세절한다(예시: 문서 세단기 사용이 불가한 경우 A4용지 기준으로 16절 이상 분해하여 파기한다.
- USB, 외장하드와 같은 대용량 저장매체의 경우, 여러 차례의 포맷 또는 영구삭제 프로그램을 이용하여 복원이 불가하도록 삭제한다. 그러나, 최근에는 복구 기술의 발달로 인해 단순한 삭제프로그램을 이용한 파기는 100% 안전하다고 장담하기 어려우며, 이를 위해 용접기 등을 이용한 완전 소각 및 용해를 통하여 원상복구 불가능하도록 파쇄 하는 것이 안전할 수 있다.

(5) 전산문서 등의 자산 관리 및 통제

① 기관에서 기술문서 등의 문서자산은 출력물 형태 보다는 정보화되어 전산문서(File 포함) 형태로 빈번하고 많이 사용하고 있으며 대부분 시스템상으로 전산문서의 생성・열람・편집・삭제 이력을 전산관리하고 있다.

② 따라서 필요한 경우에는 출력물 형태의 자산관리대장 외에 시스템에서 전산 문서 이력관리를 실시하여 장기간 또는 정확한 보관이 가능하게 할 수 있다. 시스템에 의한 자산관리・통제는 건별 문구

추가나 수정 및 이력관리가 가능한 형태로의 자산관리가 가능하다.

6. 임직원 보안

(1) 임직원 보안 일반

① 재직 중인 임직원 보안은 기관의 비밀보호 책임과 의무가 있는 주체이며 또한 대부분의 기술유출 방지 및 예방을 위한 통제 대상이기도 하다. 임직원 보안을 보다 체계적으로 하려면 보안전담조직을 구성하고 보안부서 등에서 현장 실정에 맞는 보안시스템을 구축하며 임직원들의 보안의식 고취를 위한 교육 프로그램을 개발하고 운영하여야 한다.

② 임직원은 기관 내 비밀과 관련된 업무를 하거나 접근할 가능성이 상존하고, 기술상, 경영상 정보를 많이 취급하거나 취득하기 때문에 비밀 취급 여부에 관계없이 모든 임직들에게 보안서약서 또는 비밀유지서약서를 징구하여야 한다. 서약서 내용은 간략히 다음과 같다.

- 취득한 정보를 제3자에게 누설 금지
- 보안규정 및 지침 등을 반드시 준수
- 재직 중 취득한 정보를 퇴직 이후 본인 또는 제3자의 이익을 위해 이용 제한
- 재직 중 취득 한 정보는 업무 목적 외에 다른 목적으로 사용 금지
- 비밀유지서약 위반 시 민·형사상 책임을 지고 회사 손실 시에는 배상 원칙 준수
- 서약인 업무와 관련된 내용을 기술한 자료 첨부(필요시)

③ 귀중한 자산의 보호하기 위한 목적으로 임직원을 대상으로 비밀유지 서약을 시행하고 있으며, 비밀유지서약서는 영업비밀 침해 등 사고 시에 중요한 단서로서 활용될 수 있으므로 비밀취급 여부에 관계없이 모든 임직원에게 징구하는 것을 원칙으로 한다.

※ 임직원 보안 일반(예시)

- 모든 임직원에게 보안준수 관련 서약(비밀유지서약서 등)을 작성시키고, 작성한 서약(비밀유지서약서 등)을 보관・관리한다.
- 기관 내 제3자(협력업체, 아웃소싱업체, 외부전문가, 외국인 종업원 등)에 대한 보안규정을 안내하고 제발절차를 이행도록 하며 이를 체계적으로 관리한다.
- 채용(예정)인력의 직무경력 조사 및 보유 전문자격 등을 확인한다.
- 가능한(필요한) 경우, 대상인력(외국인력)에 대한 독립적인 신원확인 등(여권 혹은 유사한 서류 및 입국심사서류 등)을 실시한다.
- 기관에서 근무한 경험이 있는 자문인력(컨설팅, 연구 자문 등)에 대해서 가능한 범위 내에서 보안관리를 실시한다.

(2) 신입인력 채용 보안

① 채용과정에서 입사지원서, 자기소개서 등 서류심사, 인・적성검사, 개별면접・합동면접・주제발표 등의 다양한 심사 및 면접방법을 통해 인성적인 결함여부를 파악・검증하고 확인한다.

② 신입인력 입사 이전 고려사항(예시)

- 입사 지원서류를 통한 성장배경 및 주변 환경여건 확인
- 면접을 통한 태도, 애사심, 성실성 및 도덕성 등을 검증
- 인적성 검사를 통한 사회성, 대인관계 및 인격적 적합성 파악
- 전공, 전문성 및 학업 성취도 평가, 해당・관련분야 참여도 확인
- 인적성 프로그램 활용 및 필요 시 주요 사실 관련 여부 조사

③ 신입인력 채용 후 고려사항

- 고용계약서 및 보안서약서 작성 및 징구(보안서약서는 ‘산업기술보호지침’ 별표 참조)

- 기본적인 보안교육 실시
- 부서배치 후 체계적으로 지켜야 할 의무사항 포함 보안내용 재교육

④ 입사 후 업무수행 시 보안 위반으로 인한 피해가 없도록 아래 사항을 참고하여 보안교육을 실시한다.

- 보안 관련 법률의 이해, 최근 보안사고 사례, 사내 보안규정, 규정을 위반하는 경우 법적·제도적 책임 및 징계 양정 기준 등
- 신입 입사자 대상 연 1회 이상 보안교육 시행(집합, 온라인, 전달교육 등)하고, 보안서약서 서명 및 담당 부서에 제출

⑤ 보안서약서 제출 의무는 신규인력 채용 절차에서 기본적인 사항으로 보안(인사)부서에서 또는 소속(관리)부서에서 징구한다.

※ 보안서약서는 일반적으로 아래 사항을 반영하여 구성(예시)
• 징구시기/대상/방법/보관방법/보관기간 및 추가 징구 등의 필요 조건은 보안규정 등에 명기 • 최초 업무 수행 시, 매년 1회 정기 징구 또한 철저한 보안이 요구되는 중요 프로젝트/업무 투입 시 징구 • 법적 분쟁 발생 시 법률적 책임에 대한 증거자료로 사용할 수 있도록 찾기 쉽게 보관

(3) 경력인력 채용 보안

① 기관에 있어 우수인재 확보를 위해 불가피하게 경력사원을 채용하는 경우가 많지만 보안관리 관점에서는 신규인력 채용보다 더욱 고려해야 할 조건이 많다. 일부사례지만 경쟁업체에서 의도적으로 위장취업을 시켜 기술 자료를 유출하거나 개인의 이익만을 내세워 일정기간만 근무할 목적으로 취업하는 등 경력인원 채용은 당초의 채용 목적 외 피해를 입는 사례가 일부 발생하고 있기 때문이다.

② 경쟁업체에서 근무한 경력자가 영업비밀 및 경업금지약정 등을 준수해야 할 기간이 경과하지 않은 시점에 채용하여 관련 법규에 의거 법률적으로 문제가 유발되어 이직이 성립되지 않는 경우도 있다. 따라서 이전 근무처에서 영업비밀을 취급하고 퇴직 시 이전 직장의 영업비밀에 대한 유지 의무 계약서 또는 퇴직 시 비밀유지의무 조항을 작성하였는지 여부를 확인할 필요가 있다.

③ 경력 채용 전 고려사항(예시)

- 이력서, 자기 소개서를 면밀히 검토 확인
- 전직 회사에 대한 영업비밀 취급여부 서면 확인
- 이전 직장에서의 퇴직 동기 등 조사
- 위장 취업, 단기간 개인 목적의 취업 등의 가능성을 면접에서 검증
- 인적성 검사를 통한 인격적 결함 유무 판단
- 가능하면 범죄사실 및 개인 파산 등 법률적 문제가 없는 지 조사

④ 경력인력 채용 후 고려사항

- 고용계약서 및 비밀유지의무 보안서약서 작성
- 보안의식 제고 포함 기본적인 보안교육 실시
- 부서 배치 후 체계적으로 지켜야 할 보안내용 재교육

⑤ 경력인력 채용 후 인원관리

- 이전 근무처의 불만을 동일하게 현재 근무처에서도 불만 표출여부 또는 가능성 조사
- 가능한 경우 일정기간 핵심기술 취급 관련업무 자제 또는 접근 권한부여 제한
- 일정기간 경과 후 근무부서에서 적응하지 못하는 경우 관리 필요
- 외국인 종업원은 영문 및 한글 보안서약서를 동시에 징구 필요

(4) 퇴직(예정)인력 보안

① 퇴직(예정)인력은 조직 내 중요한 기술 또는 영업비밀 등을 숙지하고 있으며, 기관과의 갈등으로 퇴직하는 경우 기관에 대한 나쁜 감정으로 인한 영업비밀 등의 누설 가능성과 기관의 이미지에 좋지 않은 영향을 미칠 수 있다. 퇴직자가 재직 중에 지득한 영업비밀 등을 퇴직 후에 사용하거나 공개 또는 누설하지 아니하고 특히 산업기술 관련 창업이나 경쟁관계에 있는 기관 등에 일정기간 취업하지 않을 것을 서약하는 경업금지약정서를 징구한다. 만일 이 서약을 준수하지 않아 현재 소속기관에 손해를 끼치게 될 경우에는 관련 법률 등에 따라 책임을 지겠다는 내용을 포함한다.

② 퇴직에 의한 기술유출 등의 보안사고가 발생할 경우 대응은 사실상 법적 조치에 의존하는 수밖에 없다. 따라서 어려움이 많고 유출 증거를 입증하기도 쉽지 않을 뿐만 아니라 은닉하는 경우가 대부분이므로 퇴직 이전에 보안관리를 철저히 하는 것이 최선의 방법이다. 퇴직 의사를 표명하거나 퇴직 준비를 하고 있는 동태가 파악되면 가능하다면 6개월에서 1년 전 기간 동안의 자료 출력이나 다운로드 현황을 파악하고 더 나아가서 직무상 관련자료 송수신의 이력을 조사할 필요가 있다. 퇴직인력의 비밀유지서약서는 ‘산업기술보호지침’ [별표] 서식을 참고한다.

③ 퇴직인력 보안조치 및 관리는 다음의 내용을 참고한다.

- 기관의 기밀 누설 금지 등의 내용이 포함된 비밀유지서약서를 징구(재직 중 취득한 기술정보 및 경영정보 포함 영업비밀에 대한 비밀유지 준수 서약)
- 개인PC 및 업무관련 자료를 반납하도록 하고, 주요 반출물품에 대한 통제 실시
- 사내 시스템 및 회사 메일 계정을 퇴사 시 즉시 삭제
- 퇴사 전(前) 해당 부서장 또는 팀장(임원의 경우, 상위자)이 퇴직자 면담조서 확인을 통해 퇴직절차 진행
- 퇴직예정인력의 사내 정보 접속 및 전송 관련 로그를 점검하여 정보유출 가능성 여부 등을 확인

④ 퇴직 후 경쟁사에 취업 시 취업제한 등 법적처리(예시)

- 경쟁사 재취업 제한을 위한 필요충분한 근거가 있어야 한다(퇴사 후 x년간 동종업계 취업을 금하는 경업금지서약서 등).
- 관련 법규 등에 의거 기존 퇴직자가 경쟁사에 재취업하여서는 아니 되는 내용을 경쟁기업에 통보할 수 있으나, 개인정보보호법 위반이나 경쟁기업의 영업비밀 침해의 역효과가 발생할 수 있다. 따라서 기술유출 및 영업비밀 침해에 대한 상당한 의심 및 입증이 가능한 경우 해당분야 전문가 자문 하에 진행하는 것이 바람직하다.
- 또한 퇴직자가 이직 후 경쟁기업에서 하고 있는 업무 내용이 기관이 보유한 기술 또는 영업비밀에 해당되어 침해 받고 있다는 사실을 증명할 자료를 수집 및 확보가 필요하다.

(5) 외국인력 보안

① (외국인력 보안관리 특성과 강화 필요성) 외국인 인력이 국내에서 연구개발 및 기술·제조 및 생산 등의 분야에서 고용 등의 방법으로 근무하는 경우에는 중요한 기술정보 또는 결과물 등이 유출될 가능성을 배제할 수 없다. 따라서 외국인을 채용하여 산업기술 분야 등에 근무하게 하는 경우 외국인력에 대한 신원확인과 함께 근무에 따른 철저한 보안관리를 하여야 한다.

- 다만, 국내에서 근무하는 외국인력에 대한 보안관리는 별도의 보안규정 마련과 이를 위반 시에는 제재할 수 있으나 외국인력의 국적 등에 의해 경우에 따라서 국내 법규의 우선 적용이 불가하고 해당 국가의 법령 적용이 우선 될 수 있음에 유의한다.

② (채용 및 고용계약 보안관리) 채용 대상 외국인력의 인적사항 확인, 검증하고 외국인력 대상 별도의 보안관리 대책 수립 및 운영 방안을 고용계약과 병행하여 확정한 후 고용과 동시에 보안교육을 실시한다.

- 외국인력 채용 검토를 위한 신원과 경력을 공식적으로 검증할 자료의 제출을 요청하고 필요한 경우에는 공증을 실시한다.
- 근무에 따른 기술보호 등 보안의무(국내 관련 법령 준수 의무 부과 등)에 대해 보안교육을 실시하고 숙지하도록 한다.
- 고용계약서상에 기관의 보안규정 준수 의무 및 기술보호의무(국내 기술보호법령 준수 등) 부과 등을 명시하고 보안규정을 준수한다는 내용이 포함된 비밀유지서약서(국문・영문)를 징구한다.
- 사전 승인절차에 의하여 해당 근무지역 이외 출입을 제한하도록 조치하고 이에 따른 출입증(사원증)을 발급한다.

※ 외국인력 채용 시 비밀유지서약서 포함사항(예시)

- 근무 중 직무상 연구개발 등 취급한 기술・정보는 기관에 귀속
- 계약기간 및 종료 후에도 일정기간 비밀유지의무 명기
- 문서・자료 반출 시 사전 승인과 노트북, 정보통신망 등 이용 시 자료유출 위험에 대한 사용제한 또는 검색 및 통제 가능 명기
- 업무상 접근한계와 구역의 출입제한 및 비밀보호 의무 부여 명기
- 계약만료 시 업무상 개발한 자료, 반환의무와 기술자료 유출 여부 검색 가능 조건 명기 등

③ (직무 수행 중 보안관리) 외국인력이 국가핵심기술 분야에 근무하도록 하는 것은 꼭 필요한 최소한의 범위에서 참여하도록 하는 것이 바람직하다. 국가핵심기술 분야에 참여하는 경우에는 산업기술보호법(제10조) 및 관련 규정에 따라 국가핵심기술 보호를 위한 의무조치 부과하는 별도의 비밀유지서약서를 징구한다.

- 외국인력에 대한 직무 수행 중 보안관리(예시)는 다음과 같다.

- 정기적으로 보안교육을 실시하고 임직원 참여 보안예방활동에 적극 참여하도록 조치
- 근무 중 담당 직무와 관련이 없는 보호구역 등의 지정된 근무 장소 외 출입통제 대책 수립 및 조치
- 정보통신망 접근 권한 통제 및 감독 방안 수립 및 관리
- 부서장/담당임원의 통제(승인・경유)하에 E-mail, FAX 등 이용
- 노트북 및 저장장치 반출・입시 기술보호총괄책임자 및 기술보호 부서책임자 승인
- 해당 근무부서에 대해 주기적・불시적인 보안점검 실시 등
- 외국인력이 근무 중 직무상 해외로 출・입국에 따른 전후 보안교육 실시 및 서약서 징구

- 직무상 관련이 없는 기술자료 등을 무단으로 복사하거나 외장하드 등 정보저장장치 등에 저장하는 것을 사전에 차단한다.
- 사전에 승인되지 않은 야근을 많이 하거나 또는 잦은 휴일 근무가 발생되지 하지 않도록 사전 검토하고 관리한다.

④ (퇴직 및 고용계약 종료 시 보안관리) 외국인력이 고용계약 등의 종료에 따라 퇴직할 경우 해당직무분야의 기술정보 또는 성과물이 국외로 유출될 가능성을 배제할 수 없다. 따라서 외국인의 퇴직에 따른 기술유출 등의 위험을 최소화할 수 있는 보안 대책이 필요하다.

- 외국인력이 계약기간 만료에 따라 직무 수행 중에 취득한 기술 등 기밀내용이 누설되지 않도록 PC 등 하드웨어 및 보유 기술자료, 성과물 및 연구노트 등을 모두 회수한다.
- 대상기관은 퇴직 등에 따른 근무기간 동안 외국인력이 직무 수행 중에 취득하거나 인지한 기술정보 등에 대한 보안의무를 고지한다. 또한 퇴직 이후에 근무기간 취득하거나 지득한 기술정보 등의 비밀유지 의무를 부과하기 위하여 이를 위반 시 제재사항 등이 명시된 비밀유지서약서(영문・국문)를 징구한다.

- 산업기술보호법에 따라 국가핵심기술 등을 취급하는 국내 대상기관은 국내에서 근무하거나 고용계약 만료 예정인 외국인력이 국가핵심기술 등을 유출 또는 침해행위를 하거나 이와 같은 행위가 발생될 우려가 있을 경우에는 산업통상자원부장관 및 정보수사기관에 신고하고 즉시 조사 및 조치를 요청한다.

⑤ (임시 출입 외국인력 보안관리) 직무 특성상 외국인 기술고문, 컨설팅・자문 형태의 고용 등과 같은 방식에 의한 외국인의 기술지원 활동 등이 빈번해짐에 따라 이에 따른 기술정보 누설・유출 등의 보안 문제가 야기될 가능성이 있다. 이 경우 대상 외국인력에 대한 충분한 정보를 확보하고 채용 및 계약을 추진해야 기술정보 등의 유출 등을 예방할 수 있다. 특히 고용계약 등에 있어 다음 사항을 유의한다.

- 계약 시에는 비밀유지서약서를 포함하고 공증을 실시한다.
- 업무에 참여하는 해당 임직원은 비밀유지서약서를 징구한다.
- 용역 완료 후에도 계약기간 공유한 기술정보 등에 대한 비밀유지서약서를 징구하고, 외부에 기술정보 누설・유출 시 책임 부과 및 이에 대한 제재사항을 명기한다.
- 분쟁 가능성이 있는 용역 또는 자문 등에 의한 결과물에 대한 소유권도 고용계약서 또는 비밀유지계약서에 명기한다.

(6) 임직원 출입증 및 출장 보안

① 입직원 등 출입증 관리

- 재직 중인 임직원과 외부 방문객 간의 식별과 출입지역에 대한 제한 등의 차별화를 위해 최근 Bar code, RFID card, Smart card를 적용한 사원증이 많이 보급되고 있다. 하지만 신분증에는 사진을 부착하여 본인 여부를 확인할 수 있어야 하고, 쉽게 위변조가 되지 않도록 하여야 하며 유지관리 비용 절약을 위해 쉽게 훼손되지 않

도록 하는 것이 중요하다
- 신분증을 대여하거나 타인의 신분증을 패용하는 행위를 금지한다.

② 글로벌 시대에 해외 출장은 빈번하고 보편화된 업무의 일부로 출장 시에 노트북이나 USB 등 저장매체를 휴대하는 경우가 대부분이다. 해외출장 시 고려해야 할 보안수칙으로 아래와 같은 주의사항이 있으며 출장 전에 교육을 실시하거나 출장대상자에게 공지 또는 안내한다.

- 출발 전 방문국가에 관한 정보를 숙지한다.
- 여행사, 호텔 등에 출장과 관련된 정보 노출을 최소화 한다.
- 꼭 필요한 경우가 아니면 회사 로고가 들어간 복장을 피할 것
- 출장 중에는 업무와 관계없는 사람에게 현안 사항, 직책, 경력, 담당업무 등 관련정보를 언급하지 않는다.
- 대중교통, 공공장소에서는 업무상 비밀 또는 민감한 정보에 대해 이야기하지 않는다.
- 민감한 정보를 전송할 때에는 팩스, 전화 등의 사용을 자제한다.
- 호텔 객실 내에 보안문서, 노트북 등을 두고 외출하지 않는다.

③ 만일, 출장 중 보안사고가 발생할 경우 본인 스스로 취해야 할 행동요령에 대해서 기관의 관련규정 또는 지침 등을 충분히 숙지하는 것이 바람직하다.

7. 협력업체 등 외부인력 보안

(1) 외부인력 등 보안 일반

① 외부인력은 기관 등의 임직원이 아니면서 협력업체, 용역업체 등 업무 관련으로 기관을 방문하는 공무출입자와 업무와 직접 관련이 없이 개인적인 일로 방문하는 일일방문자 등을 외부인력으로 구분할 수 있다.

② 공무출입자는 설계・제조・생산 협력업체와 납품업체, 운송업체, 시설과 설비의 유지보수업체 등 각종 용역업체 인력과 상주하고 있는 미화원, 식당 종업원, 매점, 사내 사설기관 관리자 등 용역인력이 있다. 이들 공무출입자에게도 필요에 따라 주기적으로 보안교육을 실시하여야 한다. 다만 현실적으로 어려운 점을 감안하여 선택적으로 용역업체 관리자나 책임자에게 정기적으로 보안교육을 실시하고 교육 후에는 비밀유지서약서를 징구한다.

③ 업무적이거나 개인적으로 출입하는 일회성 방문의 경우에는 보안교육을 실시하기 어렵기 때문에 출입시에 보안관련 준수사항에 서명토록 하거나 보안서약 내용을 공지하여 인지하도록 한 후에 출입하도록 한다. 일일방문객 등 임시 출입자도 사무실 등에 출입제한구역들 출입할 때는 출입증을 교부하고 직원과 동행하도록 조치한다.

(2) 협력업체 등 상시출입자 보안관리

① 공무출입자는 임직원이 아니면서 원부자재 납품과 제품의 판매・유통업체, A/S업체, 운송업체 등 기관의 업무수행 또는 개발・생산・영업활동을 하는데 필요에 의하여 상시 출입하는 자이다. 기관 고문역, 자문역, 고문변호사, 세무사, 회계사, 노무사 등 전문가 그룹과 기관 건축물의 건설, 연구개발 용역업체의 임직원, 경비・청소, 각종 기계정비, 환경정화 등의 용역업체 관계자로서 기관의의 허락하에 상시 출입하는 인력을 포함한다.

② 이들은 기술 또는 영업비밀의 누설, 유출, 침해 등의 가능성이 분야에 있는 인력으로 가능한 비밀유지서약서를 징구토록 하는 등의 보안관리에 필요한 조치를 한다.

③ 용역・업무위탁 협력업체 등과 비밀유지계약을 체결한다. 그리고 기관의 일정한 업무를 수행하는 용역 위탁 시에는 용역계약과 동시에 비밀유지서약서를 징구한 후 업무를 수행하게 한다.

- 용역업체에 업무수행중 기업비밀의 대상과 범위를 정한다.
- 비밀유지 의무기간을 정한다.
- 용역업무 수행 중 비밀을 생산하는 경우 귀속문제를 명확히 한다.
- 용역업체의 비밀침해의 책임 여부를 명확히 한다.
- 비밀을 취급 또는 관리하는 자를 지정한다.

④ 협력업체 출입자와 개인별로 비밀유지서약서를 징구할 수 있다.

- 연구개발 등 중요 사업・과제를 공동을 추진하는 용역업체와 전반적인 비밀유지 계약은 물론이고 출입하는 용역업체 임직원에 대한 비밀유지 서약을 용역업체가 직접 서약서를 징구하여 제출하도록 한다. 이미 설명한 바와 같이 경쟁업체는 이러한 경우를 이용하거나 위장하여 기관의 중요 기술정보를 수집할 수 있기 때문이다.

⑤ 기타 제한구역 등 상시출입자의 경우도 출입이 가능한 구역 또는 시설에만 출입토록 한다. 기능하면 상시출입자의 출입증은 매일 회수하여 관리한다. 위조, 변조, 분실 등에 의한 사고를 방지하기 위하여 출입증은 회수하여 보관하는 것이 바람직하다. 용역업체의 출입자 신분으로 위장하여 보안 사고가 발생될 수 있기 때문이다.

※ 외부자(기관)와 업무 용역(위탁)계약 관련 보안 검토사항(예시)

- 보안관련 법률 준수/보안서약서 제출(비밀유지, 보안책임 등)
- 직원 대상 주기적인 보안교육 수행/업무수행 관련 지득한 정보・기술 유출 방지 및 비밀 준수
- 내부 네트워크(업무망) 연결 등에 따른 인터넷접속 통제, 무선・정보통신망 사용 통제 등 보안 조치
- 근무 공간 물리적 보호조치(장비 및 매체 반출입, 출입통제 등)
- 외부 직원 PC 등에 대한 보안관리 (백신설치, 안전한 패스워드 설정 및 주기적 변경, 화면보호기 설정 등)
- 제공 받은 계정에 대한 공유 금지 및 권한 외 접근 시도 차단

- 근무계약 해지 시 제공 자산의 반납, 계정 삭제, 정보 파기, 출입증반납, 비밀유지서약서 징구
- 업무 담당자 변경 시 적절한 보안 조치 및 교육 실시
- 보안사항 위반 시 처벌, 손해배상 책임, 보안사고 발생에 따른 보고 의무 부과 등
- 외부자와 보안관련 계약 시 비밀유지계약이나 보안관련 조항을 포함하여 계약하도록 사전 준비

(3) 방문자 등 임시출입자 보안 관리

① 기관에 임시 출입하는 자는 업무적으로 방문하거나 임직원과 사적인 일로 방문하는 등 일시적으로 방문하는 자로서 중요자산 등 비밀이 많은 기관은 내부출입을 제한하는 방법으로 일반구역에 면회실 또는 회의실을 이용하거나 출입통제지역에 접견실을 정하여 그 장소에만 출입할 수 있도록 한다.

② 임시출입자가 사무실 등 제한구역 출입이 필요한 경우에는 사전에 예약하게 하여 신분확인과 방문목적, 면담 및 만나고자 하는 임직원과의 관계 등을 조사하여 출입자관리 대장(서식)에 기록하고 방문자에게 출입증을 패용케 하는 것이 일반적인 방법이다.

③ 이 때 유의하여야 할 것은 방문자의 신분증이 아닌 명함이나 구두로 신분을 확인하는 것은 신분을 위장할 수 있으므로 주민등록증 등의 신분증으로 확인하여야 한다.

④ 또한 단체로 오는 시찰단, 관계기관의 공무로 방문하는 경우에는 사전에 관계기관의 방문 목적, 방문자 인적사항을 정상적인 절차를 통하여 접수 받아야 하고 접수한 후에는 그 단체에 사실 여부를 확인할 필요가 있다. 산업시찰단이나 관계기관의 방문은 개별적으로 신분 확인과 조사에 어려움이 있고, 현장에서 정서상, 관례상 할 수 없는 경우가 빈발할 수 있기 때문이다. 기관의 연구개발구역 등 주요 시설과 영업비밀 등의 취급을 많이 하는 근무구역은 보안구역으로 설정하여 외부인은 물론 관계직원 이외에는 출입을 제한한다.

⑤ 특히 단체관광, 외국인 등의 시찰 코스는 사전에 이러한 중요시설을 피하고 코스를 지정하여 안내를 하여야 한다. 만일에 대비하여 일시적인 출입자도 주요 산업기술 등에 관한 상담을 하거나 중요시설을 불가피하게 업무적으로 관람시킬 때에는 사전에 보안서약서를 징구할 수 있다.

(4) 방문객 노트북 및 저장매체 관리

① 방문객 물품 보안 일반

- 기술유출 방지를 위해 방문객들이 휴대하고 있는 노트북이나 USB, 외장하드 등을 반입, 반출 시 검색을 철저히 해야 한다. 기관마다 검색 방법이 다르지만 대체로 X-Ray, 금속탐지기, 노트북 반출입 검색 프로그램, 저장내용 Format 시스템 등을 이용한 방문객 출입 시 검색은 필수적이다. 다만 방문객이 많고 적음에 따라 검색 방법도 차별화하여 적용할 수 있기 때문에 기관의 실정에 적합한 방법을 선택할 수 있다.
- 검색을 실시할 때 주의사항은 기관을 방문한 인력에 대해 절차와 충분히 양해를 구한 상태에서 검색을 하여야 한다. 노트북이나 정보저장매체의 내용을 열람할 경우에는 개인정보보호에 위반되지 않도록 해야 하며, 방문객 등의 사전 동의 없이 임의로 실시하는 경우에는 민·형사상 책임이 발생할 수 있으므로 반드시 방문한 외부인력의 동의하에 실시한다. 반입이 불필요한 물품은 별도의 보관장소에 보관한다.

② 반입 검색(예시)

- 방문객 사전 예약 시 노트북 및 정보저장장치 반입 유무를 확인

- 사전에 등록되지 않은 경우에는 반입을 금지
- 입문 시 반입 목적 등의 사유를 기록
- 부득이한 경우 보안스티커를 사용하여 봉인
- 노트북 등의 저장 상태를 확인
- 사전 신고 또는 검색없이 반입되지 않도록 철저히 확인

③ 반출 검색(예시)

- 입문 후 저장된 내용에 대해서는 담당자의 내용확인을 거친 후 사유서를 첨부
- 노트북 등 정보저장장치 반출 시에도 검색을 통해서 확인
- 불법적으로 저장된 내용이 있는 지 여부를 확인
- 반입 시 봉인된 보안스티커 탈착 유무를 확인
- 저장된 내용에 대해서는 일정기간 동안 기록관리

8. 산업기술보호 교육

(1) 기술보호 교육 운영 및 관리

① 기술보호 교육은 보안에 대한 인식개선 및 교육대상자들이 반드시 알아야 할 보안규정이나 지침 내용을 주기적으로 숙지시키기 위하여 필요하다. 기술보호교육 대상은 모든 임직원 대상으로 실시한다.

- 교육대상은 업무별, 직급별, 조직단위별로 분리하고, 교육 빈도와 시기, 교육시간을 적절하게 조정하는 것이 바람직
- 보안규정을 비롯하여 사내외에서 발생한 보안사고 사례, 보안의무 위반 시 벌칙 등을 포함하여 실시
- 전체적으로 2시간 내외 분량으로 쉽게 접할 수 있도록 분야별로 동영상을 포함한 내용으로 편집하는 것이 바람직
- 교육 내용은 기업에서 가장 필요로 하는 부문에 집중하고, 보안의식 제고를 위한 내용은 누락하지 않되, 지나치게 길지 않도록 배려

② 최근 글로벌 코로나19 위기로 인하여 집합(집체)교육이 불가한 경우에는 비대면 방식의 온라인 교육 또는 메일 전달 후 숙지하는 등의 쌍방향 교육으로 기술보호 교육을 진행할 수 있다.

③ 교육자료 작성 시 고려사항(예시)

- 기술보호 인식을 향상시키기 위한 계획이 잘 되어 있는가.
- 보안교육의 효과를 평가하는 절차나 방법이 있는가.
- 법적(혹은 조직 내 규정) 조치에 따른 요구사항이 반영되어 있는가.
- 현재 적용되는 규정에 위반 사항은 없는가.
- 피교육자가 쉽게 이해할 수 있도록 준비하고 콘텐츠는 적절한가.
- 교육 내용이 최근 자료로 반영되어 있는가.
- 교육 대상자 별로 보안교재가 구성되어 있는가.

④ 교육 후 사후관리

- 교육 후 설문지를 통하여 교육 이해도를 점검한다.
- 보안교육 효과를 평가, 미흡한 점은 개선과 차후 교육에 반영한다.
- 개선 요구사항에 대해서는 적극적으로 검토하고 공지하도록 한다.
- 일정한 기간이 경과한 후 교육 결과에 대한 효과를 모니터링 한다.

(2) 임직원 대상 교육

① 임직원들의 업무와 역할, 상황에 맞춰 보안교육 내용과 교육 시점, 주기를 정하여 반복적으로 실시한다.

- 신규 입사자 및 경력입사자
- 관리자와 현장근무자 또는 비서직 근무자
- 보안책임자 및 핵심기술 취급 전문인력
- 해외 출장자 및 장기 파견자

(5) 기업 내 상주 또는 장기 계약 근무자

- 상주 용역업체 기술 엔지니어 및 용역업체 대표자
- 상주 용역업체 가운데 장기근무 근로자 등
- 중요 업무 파견 근로자
- 외국인 파견 근로자 등

(3) 자체교육 및 외부교육

산업기술 유출방지 및 보호를 위하여 교육을 실시하며 교육 시기, 대상, 내용에 따라 자체교육과 외부교육을 구분하여 실시한다.

① 기술보호교육은 아래와 같이 실시한다.

- 입사자 교육, 구성원 년 1회 보안교육 실행(Biz. 환경에 따라 횟수 조정 가능): 교육 방법은 집합 교육/온라인 교육/전달 교육 등 다양한 방법 활용이 가능하다.
- 정기 보안교육 이외에 특별한 상황이 발생할 경우 추가적인 보안교육을 수행: 관련 법률 및 제도, 정책 및 절차 개정, 보안사고 발생, 업무 환경의 중대한 변화가 발생하는 경우 등

② 자체교육

- 자체보안교육은 입사 시부터 퇴사 시까지 지속적으로 이루어져야 하는 매우 중요한 기술유출 방지 수단이다. 이러한 자체교육의 시행으로 인해 산업기술의 유출 및 침해 가능성을 낮출 수 있고, 햐후 보안사고에도 법적 증거로도 활용될 수 있다.
- 다만 외부교육은 자체교육 여건이 마련되지 않거나 자체교육만으로 교육목적의 달성이 어렵다고 판단될 경우에는 외부기관을 이용하여 위탁교육을 실시할 수 있다.

[표] 자체교육의 경우(예시)

구 분	내 용
시 기	ㅇ 정기교육 - 신규 채용 시 직원교육 - 산업기술 총괄책임자의 판단 하에 계획하여 실시 ㅇ 수시교육 - 연말, 연초 등 분위기가 어수선할 때 - 신규 기술거래를 시작할 때 - 외부에서 매수 등의 징후가 포착되었을 때 - 기술유출 방지에 관한 지침의 제·개정 시
대 상	ㅇ 모든 임직원(파견・상시근로자 및 외국인 포함)
내 용	- 산업기술 보호 세부규정 - 산업기술 보호 관련 법률(위반 시 처벌규정 포함) - 산업기술 보호 서약서 작성요구의 이유 및 내용 설명 - 생활보안 행동준칙(기관별 작성) - 기타 경영진의 판단 하에 교육하여야 할 내용들

③ 외부교육

- 시기와 대상은 자체교육의 경우와 유사하며 대상에 따라 산업기술보호협회 등 전문기관 교육과정에 참여하여 교육을 받도록 한다.
- 집체교육: 처음과 교육의 효과를 극대화하기 위해 특정한 장소에서 사례 중심적으로 실시하는 교육
- 사이버 교육: 반복적인 교육 또는 정례화가 가능한 교육
- 특별교육: 보안사고 또는 특별한 경우 특정인을 대상으로 실시
- 보안교육을 실시한 후에는 일자, 보안교육 내용, 참석자 서명 등을 작성하여 보관한다. 향후 보안교육 결과물은 법적인 증빙자료로 활용될 수 있으며, 또한 보안역량 제고를 위한 노력과 책임성에 대해서도 중요하다.

9. 예방적 보안 활동

(1) 보안점검

① 보안업무 수행상태의 적정여부, 보안규정이나 연간 보안업무 추진 계획, 각종 보안관계 지침이나 지시사항의 이행상태를 확인하고 현장의 보안관리상의 취약점 유무를 찾아내 이에 대한 자체적인 보안점검 추진 방알을 수립한다.

② 보안점검 방법 및 절차는 다음과 같다.

- 평가지에 의한 대상별(부서, 팀) 또는 목적별로 평가한다.
- 주간/야간으로 구분하여 정기적으로 또는 불시에 실시한다.
- 보안부서는 보안점검 결과 보고하고 시정 조치를 수검 부서에 요구한다.
- 각 팀(부서)은 시정 조치 확인 및 결과를 보안부서에 제출한다.
- 보안점검 일정은 가능하면 사전 예고없이 실시하여 평상 시 보안상태를 점검토록 한다.
- 다만, 점검방법에 있어서 최근 코로나 19로 인하여 방문점검이 불가하여 현장 방문이 불가한 경우에는 비대면 방식을 온라인 점검 또는 부서 내 보안담당자 통한 점검을 실시 할 수 있다.
- 보안규정, 지침의 인지상태 및 이행여부 등을 보안점검 대상으로 할 수 있다.

③ 보안점검 사항은 다음과 같다(예시).

- 간단히 시정조치가 가능한 보안관련 사항
- 보안규정 및 지침 등을 지속적으로 위반한 사실 또는 중대한 위반사실이 발견된 경우
- 정보자산에 대한 분류 및 관리 상태가 정상적이지 못한 경우
- 보안의 날 행사를 타당한 사유 없이 1개월 이상 미 시행한 경우

- 보안교육에 참석하지 아니하고 교육에 관련된 내용이 팀에서 이행되지 않는 경우
- 이전 보안점검 지적 사항에 대해 시정조치 노력이 없는 경우

④ 보안점검 결과보고서는 다음의 내용을 포함한다.

- 보안 위반사항 위주로 작성하고 개선과 재발방지 내용을 포함한다.
- 목적, 수검부서, 감사범위, 일시 등 확인된 위반사항 및 근거규정이 포함되어야 한다.
- 지적사항에 대해서는 충분한 근거와 시정조치 내용을 제시한다.

⑤ 보안점검 사후관리는 다음과 같다.

- 수검부서장은 보안점검 시 지적 사항을 조사하고 원인을 파악하며 시정 및 재발방지를 위한 세부 계획을 수립하고 이행토록 한다.
- 관련규정에 의해 보안위반자는 보안(관리)책임자(경영진 등)에게 보고하고 인사 또는 징계위원회에 회부하여 처리한다.
- 핵심기술을 취급하는 임직원에 대한 보안점검은 별도의 점검 계획을 수립하고 점검방법 등을 차별화 하여 추진할 수 있다.

⑥ 보안 위반자 처리

- 보안위반자는 보안규정에 의거 기관의 보안(관리)책임자에게 보고 후 징계위원회에 상정하여 처리한다(예시: 보안사고 발생의 직접적인 원인을 제공한 자, 보안사고 발생을 인지하였음에도 소정의 조치를 취하지 않은 자, 정기 또는 수시 보안점검 결과 보안규정을 위반한 자 또는 고의 또는 과실로 비밀 누설 또는 반출과 같은 유사한 행위로 회사에 손해를 끼친 자 등)
- 만약, 직간접적으로 기관에 미치는 영향이 매우 크다고 판단될 경우에는 산업기술보호법 등의 관련 법률에 의거 법적처리를 검토할 수 있다.

(2) 보안사고 예방 활동

① 보안사고 예방활동 방향

- 산업기술 침해를 예방하기 위해 다양한 정책과 규정 운영, 유출 및 침해방지 시스템 도입, 교육 등의 추진과 아울러 가장 중요한 것은 임직원의 보안의식 저변 확대 및 고취를 위한 보안활동으로서 정기적이고 일상적인 보안 홍보 및 캠페인 활동이 중요한 방법이라고 할 수 있다.

② 대상 및 방법

- 매년 1회 이상 임직원 대상으로 포스터, 표어 공모전을 실시하여 보안의식을 고취하고 당선작은 포상하고 업무 공간 곳곳의 장소에 게시하여 홍보한다.
- 주기적으로 출입문 주변에 게시물 또는 플래카드를 설치하여 보안 중요성을 강조한다.
- 매월 보안의 날을 지정하여 방문객을 대상으로 캠페인을 실시하면 효과적이다.
- 보안 사고를 예방하는 차원에서 보안 뉴스레터를 제작, 배포하여 평소 보안에 대한 관심을 유발하도록 하는 방법도 추진한다.

③ 보안예방활동에 있어서 유의사항은 다음과 같다(예시).

- 예방활동 내용은 신선하고 새로운 의미를 부여하도록 초점을 둔다.
- 가능한 한 모든 임직원들의 참여 의식을 높이도록 고려한다.
- 홍보 내용은 강제성 보다는 부담 없이 전달하도록 간결하면서도 강한 매용 및 메시지를 담는다.
- 다른 기관의 내용 보다는 기관의 실정에 부합하는 내용으로 준비하여 공감대를 형성하도록 한다.

- 보안 마스코트나 심벌을 제정하여 활용하는 것도 효과적이다.

④ 보안 뉴스레터 발송 및 신고센터(Call center) 운영

- 정기적 또는 비정기적으로 보안 관련 소식지를 만들어 전 임직원에게 배포하여 읽어보게 함으로써 임직원 입장에서 보안관련 이벤트를 손쉽게 접하도록 할 수 있다.
- 월 1회 등 정기적으로 개정된 보안제도나 보안관련 뉴스 등을 소식지로 만들어 사내 임직원은 물론 협력업체에게도 배포하기도 한다.
- 임직원이 보안을 생활화하고 보안에 대한 의식 제고를 위해 기술유출 신고센터를 상시 24시간 체제로 운영하는 것이 바람직하다. 임직원 등에 의한 기술유출 징후가 있거나 유출사고 즉시 신고할 수 있도록 절차가 충분히 공지 되어야 하며 신고자의 신분에 대해서는 반드시 철저하게 비밀을 보장하고 포상제도로 신고제도가 활성화되도록 해야 한다.

⑤ 사고예방 모니터링

- 기술유출 침해를 예방하기 위해 임직원이 규정되어진 규정 또는 지침을 준수하는 지 여부를 오프라인과 온라인을 통해 법률적으로 허용된 범위에서 모니터링을 해야 할 필요가 있다. 이를 위해서는 정기・수시점검, 보안 감사 등의 형태로 점검하면서 모니터링을 한다. 점검 결과를 인사에 반영하여 승진이나 별도 포상 형태로 직원들에게 동기유발을 유도하면 긍정적인 요인으로 작용될 수 있다.
- 평소 보안규정 준수에 불만이 있는 임직원에 대해서는 면담제도를 통해 불만요소를 해소시키거나 업무전환을 유도해 보안 사고를 가능한 방지하도록 한다. 그리고 보안점검 및 감사를 통해 보안규정을 위반한 직원 또는 사업장에 대해서는 경고 또는 사규에 따라 징계를 함으로써 보안활동 및 제도를 정착시켜 나갈 필요가 있다.

제2절 물리적 보안 관리

1. 보호구역 개념과 통제 원칙

(1) 보호구역 지정 및 물리적 보안 활동

① 주요 사무구역, 연구개발 및 설계구역, 주요 설비 및 장치 설치구역 또는 지역 등을 외부인력 및 업무상 관련이 없는 내부인력에 대한 출입 제한이 가능한 구역으로 지정한다. 출입통제구역은 제한지역, 제한구역, 통제구역으로 업무성격에 따라 구분하여 출입통제 및 기술자료 등 자산의 반출입을 통제한다.

② 물리적 보안 활동을 일관성 있게 수행하기 위해서는 방법, 주기 등을 구체적으로 정한 보안지침, 매뉴얼 등을 수립하여야 하고 필요한 경우 통제영역별로 지침, 절차를 별도로 마련한다.

- 물리적 보안활동 관련 제시 가능한 근거 규정을 빠짐없이 마련
- 보안정책에서 규정하고 있는 물리적 보안 활동의 주기, 수준, 방법 등은 일관성 있게 유지
- 시설 내 보호 대상의 중요도에 따라 보안 통제관리 구역을 정의

③ 보호구역 지정에 따라 물리보안 시설의 설치 및 보안 인력의 배치 등 물리보안 통제 기준을 수립한다.

- 각 보안 활동의 수행주체별 책임과 역할을 정의하며, 최고 경영진의 승인 필요
- 제정된 정책은 임직원 및 각 담당자에게 언제든지 확인이 가능한 형태로 공지

④ 물리보안 시설은 보안사고의 예방 뿐 아니라, 사내 무단침입, 자산 훼손, 비인가 반출, 차량 돌진 등 보안사고가 발생할 경우, 즉각적

인 조치를 통해 인력 및 자산을 보호한다.

⑤ 보안사고 상황 발생 시 각 물리보안 시설 및 인력을 활용하여 통제 활동을 수행하며, 시설별 개별 통제 이외 유기적인 통제 활동 실행을 위하여 사고 대응 절차를 아래 사항을 고려하여 수립한다.

- 출입인가자, 비인가자 출입, 차량 통제, 물품 반출입 등 일상적인 보안 통제 상황에 대한 대응
- 차량 돌진, 비인가 침입, 물리보안 시설 훼손, 자산 및 정보 유출 시도 등 비상 상황에 대한 대응
- 총무/인사/보안 직원 등 유관 부서의 상황별 역할 및 보고 체계 등

(2) 보호구역별 보안 조치

① 제한지역(일반구역)

- 주요 정보에 대한 보안의식이 약해지기 쉬우므로 보안사고 발생 할 가능성이 있다.
- 외부인과 내부인을 구별하기 위해 구분된 사원증을 패용한다.
- 자리이탈 시 화면보호기 설정, 책상 정리, 주요 문서 및 자료 등은 시건장치가 있는 문서함 또는 자료함 등에 보관한다.

[표] 보호시스템 구분(예시1)

보호 시스템 구분	보호 내용	사용 가능 시스템(예시)
출입 통제 시스템	시설 출입 인원 및 차량기록관리	지문인식시스템. 카드출입시스템, 차량 출입시스템
화상 감시 시스템	인원 및 차량 출입 모니터링	CCTV 및 차량 출입 시스템
방범 시스템	화재 및 동작 감지를 통하여불법 침입을 방지	화재감지기, 동작감지기, 침입감지기

② 제한구역

- 허가받은 인력만이 출입하도록 하며, 외부인의 출입은 통제한다.
- 주요 설비의 훼손・파괴・오작동 등 문제에 대한 주의가 필요하다.

[표] 보호시스템 구분(예시2)

보호시스템 구분	보호 내용	사용 가능 시스템(예시)
출입 통제 시스템	시설 출입 인원 및 차량기록관리	지문인식시스템. 카드출입시스템, 차량 출입시스템, 차량 블랙박스 등 영상촬영 방지 장치
자료반출입 시스템	내부 자료의 반출입 모니터링	X-ray 검색기, 모바일 통제 시스템, 저장매체 반출입 모니터링 시스템
화상감시 시스템	인원, 차량 출입 모니터링	CCTV, 차량 출입 시스템
방범 시스템	화재 및 동작 감지를 통하여불법 침입을 방지	화재감지기, 동작감지기, 침입감지기

③ 통제구역

- 통제구역은 주요 기술에 대한 개발 및 연구가 이루어지고 중요한 기술정보를 보관・저장하고 있으므로 철저한 보안대책을 적용한다.
- 사전 출입이 허가된 근무자 이외 모든 인력의 출입을 금지한다.
- 외부인 및 그 외 임직원도 반드시 사전승인을 받은 후에 출입한다.

[표] 보호시스템 구분(예시3)

보호시스템 구분	보호 내용	사용 가능 시스템(예시)
출입 통제 시스템	시설 출입 인원 및 차량기록관리	지문인식시스템. 카드출입시스템, 차량

		출입시스템(차량 번호 인식, 역방향 진입 금지), 차량 블랙박스등 영상촬영 방지 장치
자료반출입 시스템	내부 자료의 반출입 모니터링	X-ray 검색기, 모바일 통제 시스템, 저장매체 반출입 모니터링 시스템
화상 감시 시스템	인원, 차량 출입 모니터링	CCTV, 차량 출입 시스템
방범 시스템	화재 및 동작 감지를 통하여불법 침입을 방지	화재감지기, 동작감지기, 침입감지기
도감청 방지 및 전자파 차단 시스템	도감청을 방지하며, 전자파를 이용한 자료 유출 방지와 전자파 공격으로부터 내부 전자설비를 보호	도감청 방지 시스템 무선랜 방화벽 EMP 차단 시스템

(3) 보호구역의 접근 권한 관리

① 산업기술 등을 보호하기 위하여 해당 기술과 관련 없는 인력이 기술자료 열람 등의 접근 또는 접속을 제한하며, 보유하고 있는 시설의 부안 분류에 따라 접근 권한에 차등을 주어 관리한다.

② 보유시설에 대한 접근권한 차등 부여는 임직원의 담당 직급 또는 직무에 따른 책임의 정도에 비례하여 하는 방식이 주로 이용된다. 또한 산업기술을 보유한 대상기관에서 중요기술을 보관하고 있는 구역에 대해서는 외부인은 물론, 경우에 따라서 내부인 중에서도 권한이 있는 일부만 들어갈 수 있도록 조치한다. 또한 보호구역에서 시행하는 규제수단은 법적 허용범위 내에서 세밀하고 철저하게 관리할 수 있다.

③ 접근제한 및 접근권한의 제한은 아래와 같은 방법이 있다.

- 근무분야와 직책에 의해 설정(추후 담당 직원이 교체되는 경우에도 대응 가능하다는 장점이 있음)
- 출입 또는 접근이 허용된 임직원에 대해서도 필요한 경우 비밀유지 서약을 통해 산업기술 공개 시 사전 허가 취득 등의 의무 부과
- RFID Tag gate, ID 카드, 차량 번호판 인식 시스템 등을 통해 출입하는 인원 및 차량의 접근을 통제하는 출입통제 시스템을 구축
- 정보유출 방지용 X-ray, 문형 금속탐지기 등을 통해 장비, 특히 전산장비 등의 반·출입을 통제하는 반·출입 관리시스템을 구축
- 인원 및 차량 등의 출입여부의 확인을 위한 화상감시 시스템을 구축하고 인원 및 차량의 출입이 빈번한 곳에는 CCTV를 설치

2. 보호구역에 대한 물리적 보안 통제

(1) 물리적 출입통제 기기

① 보호구역을 설정하고 허가된 인력만이 출입이 가능한 출입통제시스템을 설치・운영한다.

② 물리적 출입통제를 위한 CCTV 시스템 설치 및 운용: CCTV는 감시뿐만 아니라 기록 장치의 기능도 함께 보유하고 있다. CCTV를 운영할 때에는 운영 목적을 파악한 후 적정한 시스템으로 구성하여 CCTV를 운영해야 하며, 흑백과 컬러용 가운데 용도・비용・효과를 살펴보고 설치한다.

③ 도청탐지기는 주변 소리의 전파를 통해 탐지하는 것이다.

④ 파장 탐지기는 정해진 구역으로 파장을 송출한 뒤 수신기로 반사되는 파장을 조사하는 것으로, 극초단파, 초음파, 저주파 등이 있다.

⑤ 근접 탐지 시스템은 전기장을 발생시켜 감시하다가 침입자의 접근에 의해 전기장의 전하량이 변경되면 경보를 울린다. 파장 탐지기

처럼 방이나 일정 구역 전체를 탐지하는 것이 아니라 특정 보호대상(미술품, 금고 등) 주위만을 정확히 탐지하기 위해 사용한다. 광전・광도 측정 시스템은 광선 즉, 가시광선, 적외선 등을 발사하여 장애물을 만드는 것이다.

⑥ 적외선 탐지기는 정해진 구역으로 적외선을 송출한 뒤 수신기로 반사되는 적외선을 조사하는 것을 말한다.

(2) 보호구역의 물리적 보안 운영

① 사무실 및 설비 구역 또한 물리적 보호 방안이 필요하며, 데이터센터나 전산실은 조직의 중요한 자료, 데이터 및 시스템을 보관되는 장소로 조직 내의 가장 핵심적이고 출입통제시스템 완비된 안전한 구역에 위치해야 한다.

② 시설에 대한 점검항목은 벽, 창문, 천장, 바닥, 출입문, 방화등급 등이 있다. 일반적으로 데이터센터에서는 창문이 허용되지 않는다. 필요한 경우에만 고정방식의 창을 불투명하게 설치한다. 출입문은 벽과 같은 정도의 방화등급이며 외부에서 강압적으로 진입을 방지한다. 비상시 용이하게 탈출 가능해야 하며, 자동으로 열리는 기능이 있어야 한다.

③ 정보처리시설은 출입이 허용되지 않은 자들의 접근으로부터 보호될 수 있도록 배치해야 한다. 그리고, 정보처리 시설이 눈에 잘 뛰지 않게 하는 것이 좋으며, 시설 주변에 경고나 주의 메시지를 통해 중요한 시설임을 표시해야 한다.

④ 전원 및 공조 시설의 장애가 발생한 경우에도 정보시스템이 안전하게 보호될 수 있도록 해야 한다. 이 외에 케이블 보호 시설은 전원을 공급하는 전력선과 데이터를 전송하는 통신선은 손상이나 도청으로부터 보호해야 한다. 정보처리시설은 가용성과 무결성을 지속

적으로 보장할 수 있도록 주기적으로 유지보수를 한다. 외부로 반출된 정보시스템 장비는 사용과정에서 발생할 수 있는 위험에 대한 적절한 대책을 수립하고 적용해야 한다. 데이터 저장장비 및 저장매체를 반입 및 반출하기 위한 안전한 승인 절차를 마련한다.

(3) 외부 및 환경 위협 대응 보안

① 시설 자체에 대한 보안만큼 외부 및 환경 위협에 대한 보안도 중요하다. 자연재해 및 인재로 인한 피해를 대비할 수 있는 물리적 보안 방안을 수립하고 적용해야 한다. 외부 및 환경 위협의 종류로는 장애, 재해, 사고 등이 있다.

② 장애는 외부 및 환경 위협의 종류로 가장 먼저 건물·설비, 시스템, 네트워크 소프트웨어에 생긴 장애인 경우와 정보시스템 서비스 중지가 감내할 수 있는 시간을 초과한 경우이다. 재해는 자연재해와 산업재해가 있으며 자연재해로는 홍수, 태풍, 지진 등이 있고, 산업재해로는 화재, 폭발, 단수 등이 있다. 그리고 보안사고는 내부로부터의 유출사고, 외부 위협에 의한 침해사고와 해킹, 바이러스 웜, 서비스 거부 공격 등이 있다.

(4) 물리적 보안대책 및 통제

① 특별한 보호가 필요한 시설이나 장비를 권한이 없는 자가 물리적으로 접근을 차단하고 각종 물리적, 환경적 재난으로 보호하기 위해서는 보안구역을 정의하고 이에 따른 대책의 수립과 이행이 필요하다. 물리적 보호구역은 필요한 보안등급에 따라 정의되고, 각각에 대한 보안조치와 절차가 수립되어 있는지 점검해야 한다. 또한 각 보호구역 내의 중요한 장비, 문서, 매체를 반출입하기 위한 적절한 절차가 있는지 여부와 출입이 허가되지 않은 인력의 출입 경로가 보호구역을 지나가지 않도록 배치되어 있는지 살펴본다.

② 물리적 접근통제는 보호구역을 출입하는 자를 감시·통제하고 권한이 없는 자의 출입을 방지하기 위해 수립되어야 하는 보안절차이다. 물리적 통제가 부족하거나 보안 환경의 변화에 대한 대응이 부족한 경우 관련 자산이 위협에 노출될 수 있다. 물리적 접근 통제에 대한 자체 점검을 하기 위해서는 각 보호구역에 대해 규정 등에서 명시된 대로 물리적 접근 통제가 수행되고 있는지, 각 보호구역에 대한 접근통제 수행 내역을 주기적으로 점검하고 확인한다.

③ 정보저장장치를 폐기하는 경우에는 이를 물리적으로 파기하여야 하며 일반 데이터나 정품 소프트웨어는 폐기하기 전에 매체에 기록된 내용이 완전히 삭제되어 복구가 불가능한지 점검해야 한다. 이러한 점검이 부족한 경우 자산의 폐기 시 허가되지 않은 데이터의 노출이 발생할 수 있다. 장비의 안전한 폐기 및 재사용에 대한 자체점검을 하기 위해서는 장비파기 시 일반적인 정보를 담고 있는 매체를 식별하여 이를 물리적으로 파기하도록 하는 폐기 정책 및 절차가 있는지 확인한다.

④ 또한 중요한 정보를 담고 있는 장비의 재사용 시에는 저장 매체의 기록된 내용을 완전히 삭제하여 복구가 불가능한지 확인하고 사용하는지, 일반 데이터나 정품 소프트웨어는 장비내의 매체가 폐기되기 전에 저장된 정보가 완전히 삭제되고, 이에 대한 확인 및 점검이 수행되고 있는지 확인한다.

[표] 물리적 보안 자체점검 항목(예시)

• 별도의 보안이 필요한 시설과 장비를 보호하기 위한 보호구역을 정의 하고 이에 따른 보안대책을 수립하고 있는가?
• 물리적 보호구역이 필요한 보안등급에 따라 정의되고 각각에 대한 보안조치와 절차가 수립되어 있는가?
• 보호구역 내 중요한 장비, 문서, 전자정보통신 매체를 반출입하기 위한 적절한 절차가 있는가?
• 일반인의 출입경로가 보안지역을 지나가도록 배치되어 있는가?

- 각 보호구역에 대한 보안정책에 명시된 대로 물리적 접근 통제가 수행되고 있는가?
- 각 보호구역에 대한 접근통제 수행내역을 주기적으로 검토하고 있는가?
- 장비 파기 시 일반 정보를 담고 있는 매체를 식별하여 이를 물리적으로 파기하도록 하는 폐기 정책 및 절차가 있는가?
- 중요한 정보를 저장하고 있는 장비의 재사용시에는 정보저장매체에 저장된 내용을 완전히 삭제하여 복구가 불가능한지 확인하고 사용하는가?
- 일반 데이터나 정품 소프트웨어는 장비 내의 매체가 폐기되기 전에 저장된 정보가 완전히 삭제되고 이를 확인, 점검하는가?

3. 시설보안

(1) 시설보안의 개념

① 기관 등에서 보유하거나 임대하여 관리하는 모든 시설과 설비, 물자의 도난 및 각종 위해 행위로부터 보호하는 모든 유형, 무형의 조치를 의미하며, 사용하고 있는 시설을 어떻게 보호하느냐 하는 문제이다.

② 보안상의 가치는 그 시설 또는 장비의 경제적 가치뿐만이 아니고 정보적 가치, 안전사고의 위험성, 시설파괴 시 기업에게 미치는 영향이나 복구 시 소요되는 시간이나 비용 등을 종합적으로 검토한 가치를 말한다.

(2) 시설보안 활동 시 고려사항

① 외곽 경계에 대한 접근통제 및 관리

② 사업장 정문 외 출입구에 대한 탐지 시스템 구축 및 운영

③ 사업장 건물 출입구 검색시스템 및 잠금 시스템 운영

④ 주요 핵심 시설물 또는 설지에 대한 제한구역 및 보호구역 구별

⑤ 데이터 센터, 중앙통제실, 전산실 및 중요 시설물 접근 통제

⑥ 화재 예방, 탐지 및 통제 시스템 구축 운영

⑦ 정전에 대한 무정전 전원공급 시설 구축 운영

⑧ 중요 시설 출입 인가자에 대한 식별관리시스템 적용

(3) 보호구역 설정 및 관리

① 제한구역은 명확하게 지정하고 직원들이 인식할 수 있도록 조치

② 시스템 시설과 구역 물리적 안전조치 및 출입허가자 외 출입통제

③ 외부 연결 통로는 허가 없이 접근할 수 없도록 보안조치 구축

④ 사전 출입 인가 없이 카메라, 스마트폰 등 레코딩 장비 반입 금지

⑥ 통제구역 출입 권한에 대해서는 주기적으로 갱신 반영

⑦ 중요 시설들은 일반인 접근이 용이하지 않은 위치를 고려

⑧ 제한구역 출입 이력관리 가능토록 제한구역 내 관리시스템 등 구축

(4) 보호구역 구분

① 보호구역을 설정하는 데는 국가핵심기술 등 비밀을 취급, 보관하는 등 순수한 보안상의 중요성과 고가의 자산보관이나 대형 안전사고의 위험성 등 보안관리가 필요한 시설이면 무엇이나 보호구역으로 설정할 수 있다. 또 보호구역은 일시적 또는 일정 기간만 한시적으로 설정할 수도 있다.

[표] 보호구역 구분(예시)

구분	내용
제한지역 (일반구역)	비밀, 중요 기술시설 등의 보호를 위하여 일반인의 출입에 감시가 요구되는 지역 : 감시가 요구되는 시설물 내부와 외부의 경계선으로 외부인 출입의 접점 공간(출입통제 없이 접근 가능, 방문객 접견장소를 포함)
제한구역	제한지역에 포함되는 구역으로 비밀 또는 중요 기술시설 등에 대한 출입 비인가자의 접근을 차단하기 위해 그 출입에 허가가 요구되는 지역 : 비인가 외부인의 출입은 제한, 구성원 출입은 가능한 공간(사무실 등)
통제구역	비인가자의 출입이 금지되는 보안상 매우 중요한 지역 : 시설 내 중요한 구역으로 허가지 외 모든 출입자 통제 요구 구역(예시, 전산실, 연구실, 사이버통제센터, 방제센터 등)

(5) 주요 시설 물리적 보안

① 관제센터(Control Tower)

- 출입이 비인가자의 접근으로부터 보호될 수 있는 장소에 배치한다.
- 임직원의 시야에 잘 띄지 않는 곳에 배치하는 것이 좋다.

- 시설 주변에 경고나 주의 메시지로 중요시설임을 표시한다.
- 전력장애 및 공조시설 장애발생 시에도 안전하게 작동되어야 한다
- 전원을 공급하는 전력선과 데이터를 전송하는 통신선은 손상이나 도청으로부터 안전이 담보되어야 한다.
- 가용성과 무결성의 지속적인 보장이 되도록 유지하여야 한다.
- 장비·저장 매체 반출입 시 안전한 승인 절차가 마련되어야 한다.

② 데이터센터(Data Center)

- 외부로부터 안전성을 확보하여야 한다.
- 구조적으로 지진, 폭발, 화재, 홍수, 테러 등으로부터 안전성이 확보되어야 한다.
- 외부인이 쉽게 접근하지 못하도록 제한구역임을 표시하여야 한다.
- 인가된 자의 출입기록도 보관 유지하여야 한다.
- 비상연락장치 및 비상구, 물리적 접근통제 및 시건장치가 필수이다.

(6) CCTV 시스템

① 사람 눈을 대신하여 원격지의 상황을 영상으로 보고 확인하는 장치가 Closed Circuit Television 이라는 CCTV이다. CCTV 시스템의 기본 구성은 피사체를 촬영해서 전기적 신호로 변환하는 촬상부, 전기적 신호를 원거리로 전송하기 위한 전송부, 전송된 영상신호를 재생하고 표현하는 수상부로 구성되어 있고 대규모 시스템은 각종 제어와 화상 처리하는 부분이 별도로 구성된다.

② CCTV 주요 구성품

- 카메라, 녹화장치, 모니터: 가장 기본적인 CCTV 구성
- 매트릭스: 카메라에 입력된 영상을 관리자가 원하는 모니터에 출력
- 기타: 케이블(동축/광), 조이스틱 (매트릭스 운영)

③ CCTV 카메라 종류 및 특성

- CCD 카메라: Lens로 입사된 광 신호를 CCD(고체촬상소자)에서 전기신호로 바꾸고 Analog 신호를 Digital 신호로 변환하여 DSP에서 화상신호처리를 통해 Video신호를 출력, Monitoring이 가능하도록 하는 카메라
- 저조도 카메라: 조도가 낮은(약 10-3 Lux 이하)장소에서도 볼 수 있는 카메라
- 데이/나이트 카메라: 카메라가 지원하는 조도 이하로 낮아지면 영상이 흑백으로 전환
- 적외선 카메라: 카메라 렌즈 주위에 적외선 IR이 있어 물체에 반사되는 적외선을 영상처리 하는 카메라로, 카메라가 지원하는 조도 이하로 작아지면 적외선 IR이 작동하며 흑백으로 화면 제공
- 열영상 카메라: 물체의 표면 온도에 따라 방출 적외선이 변하는 원리를 이용하여 물체 온도를 계산하여 열화상으로 나타내는 시스템으로 주야간 보안감시, 해상감시, 산불 및 화재감시 용도로 사용

④ 카메라 형태에 따른 종류 및 특성

- 고정형 카메라: 고정하여 한곳만 영상을 보여주는 카메라
- 스피드돔 카메라: 상하좌우, 줌(Zoom)을 지원하며 보고자 하는 곳을 좌우 360도, 상하 180도 움직이며 볼 수 있는 둥근 돔형의 커버 부착 일체형 카메라
- 팬틸트 줌 카메라: 줌일체형 카메라에 팬틸트 기능(카메라의 상하좌우 조절 기능)이 추가되어 있는 일체형카메라로 넓은 지역을 감시하고 사각지대를 최소화 시킬 수 있는 카메라
- 옴니스캔 돔 카메라: 주변 인테리어와 조화를 이룰 수 있도록 설계. 제작된 돔 형태의 장치로 인테리어를 중시하는 고급건물과 보안을 중시하는 중요 건물에 주로 사용되며, 카메라 하우징과 팬/틸트 기능을 동시에 수행 가능
- 네트워크 카메라: 화상압축 기술에 네트워크기술(인터넷)을 접목시킨 신개념의 카메라로서 CCD 카메라를 내장한 고성능의 엠비디드 시스템을 기본으로, 영상을 디지털화하여 압축하고 네트워크로 그 데이터를 보내 인터넷을 통해 세계 어느 곳에서나 실시간으로 그 영상을 복원하여 볼 수 있게 하는 웹 기반 디지털 카메라

⑤ 카메라 선정 시 주의사항

- 우선 컬러 및 흑백여부, 룩스(Lux), 화소, 해상도 등의 적합성과 역광의 영향 유무 및 햇빛의 영향 등을 고려하여 선택한다. 감도는 대개 룩스(Lux)로 표시한다. 수치가 적을수록 감도는 좋으나 대부분은 사용 목적에 맞추어 선택하는 것이 바람직하다.
- 보통 흑백카메라의 경우 0.2Lux이하, 칼라카메라는 1lux이하의 제품을 쓰고 있다. 화소의 경우는 보통 흑백카메라는 27만화, 컬러 카메라의 경우 41만 화소에 제품을 많이 쓰고 있다. 따라서 카메라, 렌즈, 모니터, 비디오 전송 방법 등을 최적으로 선정해야만 유저들의 기대에 부응하는 탁월한 화상을 얻을 수 있다.

⑥ 카메라 설치 시 고려사항

- 설치 목적, 위치 선정(실내·외 및 주변환경), 카메라형태(Dome /Box), 감시 구역(고정/회전형), Cost, 사용시간(주야간 겸용, 적외선카메라), A/S성 등을 고려
- 실내: 입/출 인원 감시 범위가 용이한 위치에 설치
- 실외: 건물외부 보안 사각지역 및 위험물 장소 고려하여 설치
- 주간 카메라 위치 선정 시 역광을 피하도록 할 것, 불가피한 경우 Sun-shade를 부착하도록 조치
- 야간 카메라 위치 선정 시 주변 가로등이나 발광원을 고려
- 평지에 설치되는 카메라 Pole은 반드시 피뢰침을 설치하고 접지는 필수적으로 조치
- 이동하는 물체에 대한 녹화를 고려할 경우 카메라와 녹화장치의 성능을 고려

- 진동이 있는 지역은 가급적 피하고 불가피한 경우 방진장치를 겸비하여야 설치
- 고압전류 인근 지역은 전파장애를 일으킬 경우 Filter를 부착
- 개인정보보호에 관한 법률: 관련 전문가 등의 의견을 수렴한 후 설치가 가능하고, 설치 목적 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추어서는 아니 되며 녹음기능은 불가능

[표] 보안선을 기준으로 CCTV 설치 기준을 수립(예시)

구분	영상감시 범위(예시, 아래 구역의 출입구 및 이동 동선)
보안제1선 (제한지역)	- 시설물 진입하는 최초 경계선으로 외부인 출입이 빈번한 저층부(1~4층) 및 지하층 - 빌딩1층 외부, 주차장 입/출구, 주차장(지상/지하), 지하 출입문, 저층부 출입문 - 안내데스크, 공용 엘리베이터, 엘리베이터 홀, 접견실, 복도, 비상계단
보안제2선 (제한구역)	- 사무공간(연구실, 사무실, 임원실, 비서실) , 층별 방화문, 복도, 층간 엘리베이터 홀
보안제3선 (통제구역)	- 주요 회의실, 보안상황실, 정보전산실, 데이터센터, 문서(자료) 보관실 및 기타 중요시설

4. 인력 출입 통제

(1) 출입통제 필요성 및 통제 방향

① 물리적 보안의 중요한 요인은 임직원이나 방문객 등 인력에 대한 출입통제이다. 출입이 가능한 구역과 통제구역에 대해 권한과 통제 시스템을 설정, 운영하여 내외부에 의한 보안 위협요인으로부터 보호할 필요가 있다.

② 출입자를 효과적으로 통제하기 위해서는 시설과 구역에 대한 설계 단계에서 부터 고려한다.

③ 내부적으로는 임직원이 부담을 가지지지 않고 업무 수행을 할 수 있어야 하고 외부인에게는 자연스럽게 방문기관에 대하여 호감을 갖도록 할 수 있는 반면에 출입은 엄격하게 통제할 수 있도록 시설의 구조부터 적절하여야 구성해야 하기 때문이다.

④ 출입통제도 일률적으로 어떠한 방법과 절차가 제일 좋다고 제시할 수는 없으나 시설의 기능과 규모, 임직원과 출입하는 외부인력의 규모, 시설의 구조, 출입자 통제의 필요성 등을 종합적으로 검토하여 결정하여야 하는데, 가능하면 필요한 보안장비 또는 시설을 설치하여 정책과 규정에 충실한 통제를 하는 것이 효과적이다.

(2) 임직원 출입통제

일반적으로 사원증 제도가 있으나 엄격한 출입통제를 필요로 하는 곳은 업무에 따라 각각 출입허가지역을 분류하여 다르게 운영한다.

(3) 임직원 등 보호구역의 출입관리

① 출입이 허가된 임직원 이외에 부득이하게 통제구역을 출입하여야 하는 인력에 대해서는 허가된 자에 한하여 출입하게 하고 출입자 명부를 비치하여 기록을 유지・관리한다.

② 출입허가를 받은 방문자는 보호구역내에서 어떠한 경우에라도 담당 책임자의 통제 또는 승인을 득하도록 하고 이를 위반 시 강제 퇴실 또는 퇴장 조치한다.

③ 외부에 지정된 보호구역에는 울타리, 출입구 설치, 경보장치, CCTV 설치 및 적외선 감지기, 열・충격・전파 등 각종 감지 장치 등을

규모에 맞게 설치・운영한다.

④ CCTV 시스템은 관련 법률에 근거하여 최대 30일 까지 녹화 기록이 유지될 수 있도록 설치 운영한다.

(4) 외부인 출입통제

① 외부인 방문시 가급적 방문 예약제를 실시한다.

② 외부인과 직원을 구분하기 위하여 방문자 출입증 제도를 운영한다.

③ 휴대품 확인 및 저장매체, 전산장비, 촬영매체 반입은 사전에 허거된 경우에만 허용한다.

④ 가능한 외부 면회실은 이용하며, 출입 통제시 외부인에게 과도한 불편을 주어 거부감을 주지 않도록 주의한다.

5. 물품 반출입 통제

(1) 물품의 반출입 정책

① 물품의 무단 반출이 발생하지 않도록 책임(담당)자를 지정한다.

② 물품 반출의 경우, 무상・유상・재반출입 업무 프로세스에 의거 실시한다.

③ 재반입의 경우, 반드시 재반입 현황을 관리해야 하며 반입 기일이 경과한 경우 반출처에 문의 및 회수한다.

④ 외부에서 제공된 물품의 경우, List-up 관리하며 업무 종료 시 자체 폐기 또는 반납 처리한다.

(2) 물품 보관 유지관리 및 폐기 처리

① 보관 물품의 현황을 확인・관리한다(생산량/사외 제공 수량/사내 보관 수량 등).

② 중요 물품의 경우, 외부인 접근이 불가능한 구역에 보관한다.

③ 물품 폐기 시, 반드시 형태를 알아 볼 수 없도록 폐기한다.

④ 폐기 현황을 관리한다(품명/폐기 수량/폐기일/폐기 인원 등)

⑤ 폐기 시 반드시 2인 이상 인력이 참석하여 폐기한다.

(3) 저장매체 반출입 통제

① 간단한 정보저장매체로 중요한 기술자료나 데이터 등을 짧은 시간에 다운로드 가능하므로 각별한 반출입 절차를 통하여 통제한다(예시, 입문 시에 저장매체의 용량을 기록하고 출문 시 비교).

② 사전 반입이 허가되지 않은 저장매체는 수거하여 임시 보관하거나 또는 정보저장이 불가하도록 보안스티커 부착 등으로 통제한다.

③ 저장장치가 내재된 스마트폰 등 휴대폰의 경우 실시간으로 수/발신이 가능하므로 보안스티커 부착 등으로 통제한다.

④ 중요 핵심 또는 보호구역 출입 시 저장매체를 휴대하지 않도록 하는 등의 보안조치를 실시하다.

⑤ 출문시에 저장매체의 파일 용량의 증가 여부를 확인하고 담당부서의 관리자의 승인 여부를 확인한다.

(4) 사진 촬영 통제

① 사진 한 장으로 중요한 시설·장치의 구조와 재원 모두 파악 가능하므로 주의한다.

② 휴대폰 등에 의하여 통제구역에서 사진 촬영 후 실시간으로 전송이 가능하므로 통제한다.

③ 사진 촬영 허가는 보안책임자 또는 시설물 책임자의 사전 보안성 검토를 받아야 한다.

④ 기관 홍보용 기사, 방송 촬영의 경우에도 사전 협의된 구역만 촬영토록 하고 관계 직원이 동행하도록 한다.

⑤ 시설물 외부 촬영을 허가 받은 경우 식별 완장, 모자 또는 별도의 허가 표시를 할 수 있도록 한다.

⑥ 무단으로 촬영하거나 촬영된 장비 발견 시 사후대책 강구하여 재발방지에 중점을 둔다.

⑦ 무단으로 촬영 발견 시 직원들에게 사전 교육을 통해 신고하도록 공지한다.

⑧ 노트북, 테블릿 PC 등의 일체형 카메라에 대해서도 사전 승인을 득하지 아니한 촬영을 금지한다.

(5) X-Ray 검색시스템

① 출입자 가방이나 노트북 등 휴대하는 물품에 대해 X-Ray 투시기를 통과토록 하여 검색한다. 주로 카메라, 저장매체, 유해물질, 폭발물,

기타 비밀자료 저장이 가능한 매체 등을 검색한다.

② X-Ray 검색은 입문 시 및 출문 시 모두 검색한다.

③ 소량의 서류는 검색이 아니되므로 육안 검사도 병행한다.

(6) 물품 및 휴대형 금속탐지기

① 출입자가 지니거나 다른 방법으로 은닉한 것을 검색하는 시스템이다.

② 출입문에 금속탐지기를 설치할 공간이 없거나 간편하게 검색하기 위해 사용하는 휴대형 금속탐지기를 사용한다.

6. 출입통제시스템(Access Control System)

(1) 출입통제시스템 개요

① 중요 재산이나 시설물 보호 수단으로 물리적 환경이나 건물 유형, 이용형태에 따라 출입이 허가된 인력에 대해서만 출입을 허용하는 시스템이다. 허가를 위한 개인 식별 방법은 카드(ID, 자기)와 같은 물리적 확인방법과 비밀번호, ID와 같이 본인만의 정보로 증명하는 지식적 고유정보 그리고 얼굴, 지문, 홍채, 망막, 음성과 같이 본인의 육체적 속성에 의한 생체식별정보로 개인을 식별한다.

② 이러한 개인 식별로 등록된 인력을 구분하는 출입통제시스템은 단순히 출입통제만 하는 것 외에도 근태관리, 식당관리, 도서자료관리, 순찰관리, CCTV 시스템 등과 연계하여 사용한다.

③ 출입통제시스템의 표준 설정 및 운영관리 절차는 다음과 같이 이행한다.

- 출입통제시스템의 관리자를 지정
- 출입 Data를 기록하고 일정 기간 보존(최소 1년 이상 보관 및 보존 기한 만료 기록은 가급적 삭제)
- 관리자 권한의 행위 및 시설 조작, 임의 Open 등 이상 징후의 로그를 기록하고, 일정기간 보관 및 백업
- 통제 시스템은 가능한 인사 DB와 연동하고, 계정 발급 최소화 (1인 1계정), 계정별로 접근권한을 설정(모니터링을 위한 공용 계정은 가능하나, 관리자 권한은 1인 1계정 필수)
- 제조사 기본 계정은 삭제 또는 PW를 변경하여 사용하고, 사용자 비밀번호는 복잡도, 변경 주기를 준수
- 출입 통제 시스템/설비는 폐쇄망으로 구축(외부 및 구성원 PC 등에서 NW을 통한 접근 방화벽 차단)
- 출입 통제 설비의 원격 Open, 소방연동 (Fail-Safe), 시간대 別 통제 정책 등 기능적 요구사항을 적용
- 개인/ 그룹/ 출입문/ 일자/ 시간 별로 출입기록을 확인가능 해야 함
- 출입통제설비 현황 모니터링을 위한 全 출입문 Visual Map을 제공
- 모든 출입문의 개폐 상태 모니터링 및 출입문의 강제 개방, 장시간 개방, 분실카드 Tagging, Tampering 공격 탐지 제공
- 출입통제 시스템 구축 설비는 전산실 등 비인가자의 출입이 엄격히 통제되는 환경에 위치

④ 출입통제시스템의 설치 기준에 따라 아래와 같이 설치한다.

- 보안선 정의에 따른 제한/통제구역에 Card Reader 시스템 설치
- 물리보안시설 설치지침에 따른 표준 규격 채용 및 설정 이행((소방 연동 Fail-Safe), 독립전원, 퇴실버튼 조작차단(문틀과 이격), EM Lock 내부설치 등).

(2) 출입 게이트 시스템

건물 로비나 출입구의 보안이 필요한 곳에 효과적인 접근 제어를 제공

하는 동시에 유연성 있는 출입 통제를 하는 시스템이다.

① 턴 스타일 게이트(Turn Stile Gate)

- 기존출입통제시스템과 연동되어 사용 가능
- 환경에 대한 최신 출입통제 수단으로 효과적인 방호벽을 형성
- 연속적인 인가자 구분과 인가자 뒤에 따라오는 비인가자를 감지하여 경보를 발생

② 스피드 게이트(Speed Gate)

- 다수인의 출입을 단시간 내에 처리 가능하며 비인가자 출입은 철저히 제한
- 출입통제시스템과 연계가능하며 Lobby의 출입통제용으로 사용
- 각종 탐지장비(문형 검색대, 출입통제 시스템, X-Lay 투시기 등)와 함께 운용이 가능

③ Flap Gate

- 측면에 설치된 센서로 사용자를 감지
- FLAP으로 출입통로를 개폐하는 형태로 통로개방, 통로 폐쇄의 두 가지 모드로 사용 가능
- 짧은 시간에 많은 사용자의 통과가 가능분당 최대 60명)
- FLAP은 안정성 재고로 100%우레탄으로 제작되었으며 내구성이 강한 제품으로 잔고장이 없고 정기적인 먼지 청소와 기름 공급으로 안정적인 동작 및 수명을 유지

④ Security Gate(security booth)

- 기물 파괴나 절도, 산업 스파이 등의 위험에 노출되기 쉬운 지역을 위한 고도의 통제장치로 출입 시 한명씩 출입하는 시스템

- 두 단계의 승인 절차를 통한 완벽한 보안 유지(첫 번째 문이 승인 신호가 나면 열리고, 사용자가 들어가면 닫히며 두 번째 문이 2단계 승인에 의해 열리면 최종 입실)
- Booth 내부에 입실한 사람은 승인이 거절되면 입실했던 Door가 Open되면서 출입이 거절.

(3) 카드 출입 시스템

① 기본적인 기능인 출입통제 기능으로 개인에게 할당된 ID카드 등록(성명, 사번 등의 개인정보), 삭제와 카드별 통제 등급 설정(허용지역, 허용시간, 유효기간)이 있다. 그리고 제어기능으로 원격지에서 통제지역의 출입문 개폐 제어와 엘리베이터, 차량통제, Bar Gate 등을 제어하며 아울러 감시기능으로는 강제로 통제지역의 출입문을 개폐하면 경보를 발생하고 통제지역의 출입문이 닫히지 않고 계속 열려 있는 상태를 감시하거나 시스템 기기간의 통신이 단선되는 것을 감시한다.

② ID 번호가 입력된 카드를 카드리더에 삽입 또는 근접하였을 때 시스템에 입력된 카드는 시스템 동작이 되어 Bar Gate를 구동시켜 출입을 할 수 있도록 하는 장치로서 형식 및 방식에 따라 여러 종류가 있다.

(4) 생체인식 시스템

개인마다 특징이 다른 신체 일부를 인식하는 장치로서 아래와 같은 종류가 있다.

① 지문인식: 손가락 지문은 땀샘이 융기되어 일정한 흐름을 형성한 것으로 지문에 있는 산모양의 곡선을 분석해 점이나 끊어지는 부분 등의 특징을 식별한다.

② 얼굴인식: 얼굴 전체적인 구성요소나 표정을 여섯 개의 감정 표현으로 분류하는 방식 또는 알고리즘을 이용한 자연스러운 얼굴 동작을 추출하여 데이터화 하는 방식 등이 있다.

(5) 차량 출입통제 가이드라인

① 기업의 중요 시설, 기간 통신시설 및 인원에 대한 외부 위협으로부터 예방을 위해 입문차량 내부의 위험물 탑재 여부를 확인한다.

② 물품과 자재 등 자산을 보호하기 위하여 반출물자와 수량을 확인하고 반출증의 정당한 발급과 물자의 유출을 검사하여 통제한다.

③ 차량통제는 사무실 건물과 사업장, 연구소 등 건물 용도와 주차장의 위치, 구조 등을 고려하여 통제 여부, 방법, 절차 등을 강구한다.

④ 차량 출입로 및 주차장에 감시 시스템 운영하여 재산상 피해 발생 시 사후에 조치한다.

⑤ 차량 출입관리 이력은 최소 1년 기간 동안 기록하여 보관 한다

⑥ 사내 출입이 허가된 차량이지만 사전 출문허가 없이 임의로 출문할 수 없도록 통제 시스템 구축한다.

⑦ 외부차량 출입 시에는 블랙박스 카메라의 덮개를 사용하도록 하여, 내부 시설에 대한 촬영을 금지한다.

⑧ 차량 출입관리는 탑승자 및 탑재물에 대한 통제가 동시에 이루어져야 하며, 아래 내용을 포함하는 차량 출입통제시설 설치 기준 및 통제 프로세스를 수립한다.

- 차량 출입통제를 위한 보안요원의 배치 기준

- 차량 출입통제시설의 설치 위치 및 기능 요건
- 차량 입/출차 시 통제 프로세스(차량・탑승자・탑재물 등)
- 차량 돌진에 대비한 시설(바리게이트, 과속방지턱 등) 구축 확보

(6) 차량 출입 통제시스템

① 출입통제 시스템 일종으로 카드 또는 무선주파수를 인식하여 바게이트(Bar Gate)를 동작시키는 형태로 콘트롤러(무선수신기 또는 RF Reader), Bar Gate, Loop Coil로 구성되며 기본적으로 차량의 진입을 제한하기 위해 진입 차량에 RF카드 또는 무선송신기를 발급하여 주차 지역에 정기적으로 출입이 가능한 차량만을 통과시키는 시스템으로 인식 거리에 의해 근거리 방식과 원거리 방식으로 구분된다.

- (근거리 방식(Passive Type)) 일반적으로 125KHz의 저주파수대를 이용한 Passive Type으로 카드 내부에 배터리 없이 반영구적으로 사용 할 수 있으나, 인식거리가 10Cm ~ 60Cm 정도로 한정되어 있어 승용차 위주의 정적인 입・출차 환경의 주차장에 유효하게 사용할 수 있다.

- (원거리 방식(Active Type)) 단거리 RF 시스템은 운전자가 차창을 내리고 Card Reader에 근접 시켜야 하기 때문에 번거롭고 정차 후 조작해야 하는 정체성 등의 문제점이 있었으나, 원거리 타입은 Card내부에 배터리가 내장되어 3m~10m 까지 인식할 수 있어 이러한 문제를 해결한 시스템으로 실용화가 되고 있다. 단번에 많은 정기고객이나 직원 등의 입・출차가 빈번하게 발생되는 대학교, 공공기관 등 대형 주차장에 주로 적용되고 있다.

② (차량번호판 인식) RF카드를 사용하지 않고 IP Mega Fixel 카메라를 적용하여 차량 출입시 진입하는 차량의 화상 및 차량번호를 인식하여 사전에 출입이 허용된 차량은 Data 저장과 동시에 차단기가 개방되며 통제관리 한다.

③ (대테러 차량 보안시스템) 중요 보호지역이나 산업시설지역에 강제로 진입하려는 차량을 차단하는 바리케이트로서 유압 또는 공압에 의해 바리케이트가 상승・하강하며 차량 충돌 후에도 정상적인 동작이 가능한 최첨단 차량진입 차단 시스템이다. 이와 같이 비인가 차량의 진입을 차단하는 시스템으로는 Road Blocker, Tire Killer 및 Bollard 등이 있으며, 이들 장비의 분류는 차량의 통행방법이나 미관을 고려하여 적재적소에 최적의 시스템을 구축하여 운영한다.

제3절 기술적 보안 관리

1. 정보 보안 개요

(1) 정보보안 개념

① 정보자산의 정의: 보유하고 있는 정보 자체는 물론, 그 정보를 생산하거나 보관 또는 전송하는 장치 및 시설물 또는 시스템에 전자적으로 담고 있는 전자문서・자료, 전자도면, 전자노트, 영상매체, 정보전산 데이터 및 시스템 관련 기록 등과 전자적으로 생성된 경영상의 정보 등을 포함하는 자산이다.

② 정보보안 목적: 정보를 불법적인 유출, 침해, 조작, 노출, 변조 및 파괴 등의 행위로부터 안전하게 보호하기 위해 위험 요인을 파악하고, 예방 대책 및 대응 조치를 수립・시행하는데 목적이 있다.

③ 정보보안의 목표: 정보의 생성, 처리, 전송, 출력 등 정보 순환의 모든 과정에서 정보의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability), 책임추적성(Accountability), 인증성(Authentication), 신뢰성(Reliability)를 확보하는 것이다.

④ 정보자산 구분 및 책임: 정보자산을 유형별로 물리적 자산, 정보 자

산, 소프트웨어 자산, 통신 자산 등으로 분류할 수 있으며 자산에 대한 소유자, 관리자, 사용자를 선정하고 명확한 책임을 부여한다.

⑤ 정보의 가치평가: 자산에 대해 손실·피해 발생 시 조직의 피해정도를 추정할 수 있도록 소유권을 명확하게 하고 그 정보에 대한 가치에 따른 중요도를 사전에 평가한다. 이 가치평가 기준에 의거 정보자산의 보안등급을 부여하고 자원에 대한 소유권에 대해서도 정보 생성자, 정보 관리자, 위탁 관리자, 개인 아이디어, 특허권, 저작원 등 지식재산권의 종류를 구분하여 관리한다.

(2) 정보자산 위험관리

위험관리란 불확실한 사건에 대한 위협을 식별, 통제, 최소화하도록 분석하고 유지 관리하는 전반적인 절차이다.

① 위험 요인 식별: 위험 요인은 침입, 파괴, 유출, 복사, 위조/변조 등으로 구분되어 지고, 이 요인들에 대해 정보 자산에 영향을 끼치는 위협과 취약성을 식별하고 분류하여 지속적으로 확인 점검이 필요하다.

② 위험분석 및 평가: 어떤 방법으로 위험요인을 분석하고 점검하며, 분석 평가할 것인지 기준이 정립되어 있어야 하며 이를 위해 체크리스트를 만들어 활용하는 것이 유용하다. 한편, 위험요인으로는 부정 수단, 스파이 활동, 파괴 행위 사고, 임직원의 실수, 시스템 고장, 자연적 재해, 해킹 등이 있다.

③ 정보자산 보안 위험의 종류

- Buffer over-flow: 저장된 위치에 많은 데이터를 저장시켜 버퍼를 넘치게 하는 행위
- 논리 폭탄: 활성화 전에는 실행되지 않다가 활성화 시점이 되면 작

동하는 바이러스
- 복제 코드: 기존 프로그램에 붙어 원래의 프로그램 정보를 추출하는 프로그램
- Sniffing: 모든 네트워크 트래픽을 감시하기 위해 네트워크 인터페이스에 붙거나, 디스크로 부터 데이터의 흐름을 감시하기 위해 디스크 인터페이스에 붙여 이동 데이터를 감시하는 프로그램
- Sniff: “냄새를 맡다.“, “킁킁거리다“ 라는 사전적인 뜻으로 네트워크 상에 지나다니는 패킷들을 캡처하여 그 안에 있는 내용을 들여다보는 기술을 말한다. 이런 스니핑을 할 수 있도록 도와주는 도구를 “스니퍼(Sniffer)“ 라고 한다. 스니핑의 종류로는다음과 같다.
  - 다른 이의 대화를 엿듣는 것
  - 도청(Eavesdropping)
  - 전화선이나 UTP(Unshielded Twisted Pair)에 태핑(Tapping)을 해서 전기적 신호를 분석해 정보를 찾아내는 것
  - 전기적 신호를 템페스트(Tempest) 장비를 이용해 분석하는 것

- Spoofing: 인가되지 않은 사람이나 프로그램이 허가 받은 것처럼 위장하여 시스템에 접근하는 행위를 말하며 네트워크에서 스푸핑 대상은 MAC 주소, IP주소, 포트 등 네트워크 통신과 관련된 모든 것이 될 수 있고, 스푸핑은 속임을 이용한 공격을 총칭한다.
- Troijan Horse: 정상적인 기능을 하는 프로그램으로 가장하여 프로그램 내에 숨어서 의도하지 않은 기능을 수행하는 프로그램으로 자기의 흔적을 남기지 않아 발견이 어렵다.
- Virus: 자신 스스로 복사해서 다른 프로그램에 감염시키는 프로그램
- Worm: 시스템에서 시스템으로 프로그램을 퍼트리기 위해 네트웍크 결함을 이용하는 바이러스이다.
- Ransomware(랜섬웨어) : 몸값을 뜻하는 Ransom과 악성 코드를 뜻하는 Malware의 합성어이며, 사용자의 동의 없이 컴퓨터에 설치하고 무단으로 사용자의 파일을 모두 암호화 시켜 인질로 잡고 금전을 요구하는 악성 프로그램을 말한다.
- 보호구역에서는 정보통신 네트워크상에서 발생하는 해킹공격 및 외

부침입(스니핑(Sniffing), 스푸핑(Spoofing), DoS, DDoS)공격 등과 같은 다양한 위협으로부터 정보자산 보안을 위해 통신네트워크를 보호하여야 한다. 전화, 인터넷, 팩스 등은 항상 외부로부터 도청당할 위험에 놓여 있다. 특히, E-mail에 관해서는 외부발송 E-Mail 크기를 일정규모 이하로 제한하고, 이를 초과할 경우에는 해당 부서장의 승인을 받도록 한다.

(3) PC, 서버 등 정보시스템 보안

① 사무실에서의 컴퓨터는 없어서는 안 될 업무 수단이자 도구인 반면 컴퓨터에 저장된 비밀이 그만큼 쉽게 유출되거나 도난당할 위험에 놓여있다. 특히 최근 정보통신기술과 해킹기술의 발달은 타인의 컴퓨터에 더욱 용이하게 접근할 수 있게 하여, 일순간의 부주의로 오랜 시간 연구·개발한 성과물이 쉽게 멸실되거나 도난당할 수 있다.

② 비밀이 저장된 컴퓨터에 대해서는 접근을 최소화함과 동시에 반드시 패스워드를 사용해야만 접근할 수 있도록 하고, 수시로 패스워드를 변경하여 담당자 외에는 접근이 불가능 하도록 한다.

③ 연구개발·기술설계부서 및 비밀이 저장되어 있는 컴퓨터들은 가능하면 외부 통신망에 연결하지 말고 사용하고 만약 통신망에 연결하여 사용 시에는 비인가자 무단침입 방지를 위해 침입차단 시스템(방화벽)을 설치·운영하여 산업기술 등이 해킹당하지 않도록 주의를 기울여야 한다. 부득이하게 정보통신 관리를 위한 외부 인력을 사용할 경우에는 비밀유지서약서를 징구한다.

④ 패스워드는 충분한 길이로 생성: 문자, 숫자, 특수문자를 조합하여 패스워드를 생성, 정기적으로 패스워드를 변경하고, 사전에서 찾을 수 있는 단어나 이를 조합한 패스워드는 사용을 금지하며 그리고 키보드 자판에 나열된 형태 등을 사용하지 않는다.

(4) 네트워크 및 무선통신 보안

① 안전한 무선 네트워크 환경을 만들기 위해서는 무선 네트워크 보안 정책을 먼저 수립한다.

② 다음은 기본적으로 무선 네트워크에서 무선통신기술에 의해 수행해야하는 보안 설정 사항이다.

- SSID(Service Set Identifier, 서비스 셋 식별자) 설정을 통한 접속 제한
- 폐쇄시스템 운영(SSID 숨김 기능)
- MAC 주소 인증
- WEP(Wired Equivalency Privacy) 인증
- EAP(Extensible Authentication Protocol) 인증
- AP 장비 물리적 접근 차단
- 무선 네트워크 단말기의 관리 강화
- AP 장비의 전파 출력 조정
- 암호화키 길이 증가

(5) 인터넷 보안

① (로그인 시) 웹 브라우저를 이용한 로그인 시에는 보안 접속을 선택하여 보안모드로 접속해야 하며 공동으로 사용하는 컴퓨터에서 아이디 저장은 금지하고, 사용 후에는 반드시 로그아웃을 실시한다.

② (프로그램 설치 시) 웹 사이트에서 제공하는 ActiveX 프로그램은 신뢰할 수 있는 사이트에서만 받아서 설치한다.

③ (인증서 사용 시) 공인 인증서는 USB와 같은 이동식 장치에 저장해서 중요정보를 안전하게 관리하고 보관은 시건장치가 마련된 캐비넷이나 금고 등에 보관한다.

④ (패스워드 관리 시) 인터넷 웹 사이트에서 사용하는 패스워드는 정기적으로 변경해야 하며 어려운 패스워드를 사용해야 하며, 모든 사이트에 동일하게 사용하는 것은 바람직하지 못하다.

⑤ (인터넷 사이트 관리자 페이지) 인터넷에 열려있는 사이트의 관리자용 페이지에 대한 접속 시 관리자 계정은 쉽게 추측가능하지 않은 계정을 사용해야 한다. 비밀번호는 비밀번호 규칙에 의하여 사용하고 오류횟수를 반드시 지정하여 일정횟수(3회) 오류 발생 시 계정을 차단하고 추후 변경하여 사용하도록 한다. 또한 관리자 페이지 접속 시 ID/PW 이외에 OTP나 2 Factor(문자, SNS 등) 인증을 추가사용하고 접속자 IP와 Mac 주소 등을 지정하여 (예: admin, 기업명 등) 비인가자의 접속을 차단한다. 일정시간 미사용시에는 자동으로 세션 타임아웃을 적용하여 접속을 종료한다.

(6) 보안장비

① 방화벽(Firewall): 방화벽(침입 차단 시스템)은 내부 네트워크의 시스템들을 외부의 불법적인 접근으로부터 보호하기 위해 네트워크 진입점에 설치한 소프트웨어나 하드웨어를 총칭한다.

- 방화벽의 기능
  - 접근 제어(Access Control) 즉, 패킷 필터링 기능으로 가장 기본적이고 중요한 기능으로 내부로 통과시킬 접근과 그렇지 않은 접근을 결정하여 허용과 차단을 수행
  - 다양한 기능(NAT, 프록시, 로깅, 감사추적, 식별, 증, 데이터 암호화, 무결성 관리 등)을 제공

- 방화벽의 종류는 패킷 필터링(Packet Filtering) 방화벽, 어플리케이션 레벨(Application Level) 방화벽, 하이브리드(Hybrid) 방화벽, 서킷 레벨(Circuit Level) 방화벽 및 스테이트풀 인스펙션(Stateful Inspection) 방화벽 등이 있다.

② 침입 탐지 시스템(Intrusion Detection System, IDS): 방화벽이 효과적인 차단에 실패하였을 경우 피해를 최소화 하고, 네트워크 관리자 부재 시에도 적절히 대응할 수 있는 보안 솔루션이다.

③ 가상사설망(Virtual Private Network, VPN)은 인터넷과 같은 공중망을 이용하여 마치 사설망을 사용하듯 네트워크를 안전하게 연결하기 위한 가상의 통신터널을 만들어 데이터를 암호화하여 전송하는 네트워크이다.

④ 통합위협관리 시스템(UTM): 방화벽, 침입 탐지 및 방지 시스템, 가상 전용 네트워크,웹 컨텐츠 필터링, 안티스팸 소프트웨어 등을 포함하는 여러 개의 보안 도구를 이용한 관리 시스템이다. 다양한 보안 솔루션을 하나의 장비에서 통합 관리 할 수 있는 장점이 있으나, 각 기능에 대한 라이선스와 설정을 정확히 설정하지 않으면 장점들을 충분히 이용할 수 없는 단점도 있다.

(7) 보안 솔루션 종류 및 특징

① DRM (Digital Rights Management): 컨텐츠의 자유로운 복제는 허용하되 불법 사용은 철저히 막는 것이 DRM의 목적이다.

② DLP (Data Loss Prevention): DLP는 정보유출방지 솔루션으로 이메일, 메신저 등 기업 내 다양한 정보유출 경로와 매체를 감시·통제하며, 인가된 사용자의 고의적인 불법 행위에 의해 외부로 중요 정보가 새나가는 것을 추적하는 솔루션이다.

③ NAC (Network Access Control): 사용자 단말(PC, 노트북 등)의 네트워크에 접근 시도 시 사용자가 정당한 사용자인지, 사용자 단말은 사전에 정의해놓은 보안정책을 준수했는지 여부를 검사해 네트워크 접속을 통제하는 통합 보안관리 솔루션이다.

⑤ 무선방화벽 (WIPS): WIPS는 무선침입방지시스템, 무선방화벽, 웹스, 무선네트워크보안솔루션이라고 다양하게 부른다. 무선 네트워크 환경에서는 유선 네트워크와는 달리, 눈에 보이지 않는 전파를 탐지하고 제어해야 하기 때문에 유선 방화벽과 몇 가지 큰 차이점이 있다. 스마트폰을 이용한 테더링 기능도 제어하므로 테더링으로 인한 해킹이나 자료유출도 WIPS에서 탐지할 수 있다. WIPS 장비는 단독으로 구성되지 않으며, 중앙에 WIPS 관리서버가 1대 설치되고, 15~30m 거리마다 센서(지점장비)장비를 설치한다. 센서장비는 범위가 넓을수록 장애물이 없는 천정이나 높은 곳에 설치되는 것이 일반적이다. 무선 네트워크는 장애물이 없으면 회사나 건물 밖에서도 수신 할 수 있으므로 반드시 설치할 장소의 가장 끝부분에 설치하는 것이 좋다.

⑥ 보안 USB: 정보유출방지 등의 보안 기능을 갖춘 USB 메모리를 말한다. 보안 USB는 필수적으로 사용자 식별・인증, 지정데이터 암호화・복호화, 저장된 자료의 임의복제 방지, 분실 시 데이터 보호를 위한 삭제 등의 기능을 갖추고 있다.

⑥ 보안 솔루션 도입: 보안솔루션의 경우 장기적인 정책에 기반한 실질적인 보안 프로세스의 정착과 무엇보다 조직의 구성원들에 대한 보안 인식 강화가 중요하다.

2. 정보시스템 보안대책 일반

(1) 보호 시스템 분류 및 관리

최근 몇 년 동안 발생한 산업기술의 유출 및 피해 사례를 보면 바이러스 침입 및 해킹 등에 의한 경우가 적지 않음을 알 수 있다. 따라서 바이러스 침입과 해킹에 관한 대비를 더욱 철저하게 할 필요가 있다.

① 서버 보호, 응용시스템 보호, PC 보호, 네트워크 보호 등으로 보호 시스템을 분류하여 관리한다.

② 보호시스템을 분류하고 내부 조직의 역할 설정 및 책임자 구성 등에 따라 각 조직의 담당자를 지정한다.

③ 망분리 사용: 산업기술이나 영업비밀 등 중요 기술정보나 자료가 있는 서버, DB, 저장 매체 등은 해킹 등의 유출 위험을 감소하기 위하여 인터넷망과 분리되도록 네트워크 구성을 하여야 하며, 필요시에는 다른 업무망과도 분리된 영역으로 구성할 수 있다. 내부망(업무망)과 외부망(인터넷망)으로 망분리된 환경에서 서로의 망간에 자료를 안전하게 전송할 수 있게 지원하는 시스템이 망연계 시스템이다. 망연계 시스템은 정해진 보안 정책을 준수하면서 자료를 전송할 수 있게 한다. 여기에는 파일 전송 방식과 데이터를 전송하는 스트리밍 방식이 있다.

(2) 이메일, PC 등 사용자 측면 보안 대책

정보시스템을 운용하는 대상기관의 장은 보안대책을 강구해야 한다. 이메일 시스템, PC, 노트북 등 쉽게 접할 수 있는 정보시스템에 대한 보안대책은 다음 사항을 고려한다.

① 정보시스템의 관리자 계정은 쉽게 추측가능하지 않은 계정을 사용해야 한다. 비밀번호는 비밀번호 규칙에 의하여 사용하고 오류횟수를 반드시 지정하여 일정횟수(3회) 오류 발생시 계정을 차단하고 추후 변경하여 사용하도록 한다. 또한 관리자용 페이지 접속 시 ID/PW 이외에 OTP나 2 Factor(문자, SNS 등) 인증을 추가사용하고, 접속자 IP와 Mac 주소 등을 지정하여 (예 : admin, 기업명 등) 비인가자의 접속을 차단한다. 일정시간 미사용시에는 자동으로 세션 타임아웃을 적용하여 접속을 종료한다.

② 이메일에 대한 보안대책으로 다음 각 호의 조치를 취한다.

- 외부발송 이메일의 크기를 일정규모 이하로 제한하고 이를 초과할 경우에는 해당 부서장의 승인을 받는다.
- 파일 첨부 메일 수발신시 메일시스템에 해당 ID, IP address 및 파일 내용을 기록으로 남긴다.
- 이메일은 공용계정을 사용하지 않으며, 이메일 서버의 관리자 페이지에 대한 보안은 ①의 사항과 동일하게 적용한다.
- 이메일 계정은 사내 그룹웨어 계정이나 내부 시스템의 계정과 별도로 다르게 사용하여야 한다. 즉 이메일 계정을 통하여 내부 시스템 계정을 추측하거나 접속하지 못하도록 한다.
- 이메일은 상시 수·발신처를 확인하도록 하고, 발신처가 변경되었을 경우 유선으로 재확인하도록 하여 '피싱'을 예방해야 한다.
- 이메일 서버에서 보안 필터링과 보안 규칙을 적용하여 스팸이나 악성코드를 필터링 한다.

③ 개인PC의 보안대책으로 다음 각 호의 조치를 취한다.

- 화면보호기 대기시간은 5분 이내로 설정
- 라이센스 없는 불법 소프트웨어의 사용을 금지

④ 노트북(또는 태블릿)에 대한 보호대책으로 다음 각 호의 조치를 취한다.

- 인가되지 않은 개인용 노트북은 사용을 금지
- 노트북 하드디스크 내에 중요정보의 저장을 금지
- 노트북 외부 반출 시 이에 대한 부서장 승인 또는 보안관련 부서 담당자 확인 절차 후 반출

⑤ 컴퓨터에 대한 공통 보안대책으로 다음 각 호의 조치를 취한다.

- 패스워드 8자리 이상 영문·숫자·특수문자를 혼용해서 설정하고, 주기적으로 변경
- 3회 이상 접촉 실패 시 잠금 기능을 적용

⑥ 카메라, 카메라 폰 또는 스마트 폰에 대한 공통 보호대책으로 다음 각 호의 조치를 취한다.

- 기관 출입 전 카메라, 스마트 폰 소지를 엄격히 제한
- 기관 출입 시 소지하게 할 경우 카메라 기능 사용 및 타 저장 매체와 연결을 할 수 없도록 제한

⑦ 그 외 각 기관 건물 출입구에 24시간 검색대를 설치하여 보조기억매체, 카메라 등을 통한 정보유출을 방지한다.

(3) 업무 및 사무 환경에서의 보안대책

개인PC, 노트북, 프린터 및 스마트기기 등 접근 가능성이 높은 매체들은 주로 사무실이나 회의실 등의 일반구역에 많이 존재하며, 이러한 일반구역은 일반인들도 출입 승인을 받으면 충분히 출입할 수 있기 때문에 생각보다 산업기술의 유출 및 침해사례가 많다. 따라서 이와 같이 일상 업무에서 자주 활용되면서 소지 및 이동이 용이한 매체에 대해서는 더욱 강화된 정보시스템 보안대책이 필요하다.

① 정보시스템을 운용하는 대상기관의 장은 이메일, 개인PC, 노트북, 컴퓨터에 대한 보안대책으로 위 지침의 조치를 취한다.

② 카메라 또는 스마트폰 등에 대하여는 기관 출입 시부터 각각의 소지를 엄격하게 제한한다.

③ 근무 중 이석 시에는 화면보호기를 설정하고, 중요 자료 관련 문서

는 열람 후에는 반드시 시건 장치가 되어있는 캐비닛에 보관하도록 하며 그리고 프린터, 팩스 등은 되도록 사무실 안쪽에 배치하여 일반인들이 출입하면서 쉽게 볼 수 없도록 한다.

(4) 시스템 관리 측면 보안 대책

① “서버 보안”이라 함은 서버·DB 보호, 세션로깅, 서버 취약점 점검 서비스 등을 말한다.

② “응용시스템 보안”이라 함은 웹 방화벽, 웹 스캔, 사용자 인증, DRM(디지털 저작권 관리) 등을 말한다.

③ “PC 보안”이라 함은 통합 PC보안, 온라인 PC 보안, 출력물 보안, PC 자가진단, Anti-Spam, Anti-Phishing, PMS(패치관리 시스템) 등을 말한다.

④ “네트워크 보안”이라 함은 IPS(침입방지 시스템), 방화벽, NAC (네트워크 접근제어 시스템), IDS(침입탐지 시스템), VPN(가상 사설망), 무선랜 보호, IP관리, 바이러스 관리 등을 말한다.

3. PC 등의 보안

(1) 계정 및 암호관리

① 계정관리: 웜이나 바이러스 등에 감염되더라도 피해를 최소화할 수 있도록 일반사용자 계정과 관리자 계정을 분리하고, 사용자 계정에 따라 권한과 암호를 설정하여 로그인을 할 수 있도록 보안설정이 필요하다.

② 암호관리: 암호를 사용하지 않으면 사용자의 개인정보가 고의 또는 실수로 타인에게 유출될 수 있으므로 암호 설정은 반드시 필요하

며, 암호 설정 시에는 특수문자 등을 이용하여 타인이 추측할 수 없도록 설정하는 것이 필요하다.

③ 사용자가 PC 사용 시 준수해야 할 사항과 PC보안 정책을 수립한다.

- PW 설정, 스크린 세이버 등의 비인가 사용자의 오남용 방지 지침
- PC 반출 금지, 시건장치 등 분실 방지 지침
- 백신, 비인가 SW설치 금지 등 PC를 보호하기 위한 지침
- HDD 공유금지, 비인가 Site 접속금지 등 유출 방지를 위한 지침 등

④ PC보안 정책 이행을 위해 아래 사항을 적용한다.

- 사용자 PW 설정 (복잡도, 변경 주기, 오류 입력 時 임계값) 및 PW 변경 방법 홍보
- 스크린세이버 설정 (10분 이하) 및 해제 時 암호 입력 적용
- 백신 설치 및 백신 / 보안 패치 최신 유지
- HDD 공유 금지 및 정품 SW 사용 / 서비스 종료 된 SW 사용 금지
- 휴대용 저장치를 통한 바이러스 및 악성코드 자동 실행 방지(예시: 연결 時 바이러스 검사 실행, 자동 실행 기능 해제 및 숨김 파일 및 폴더 등이 표시되도록 PC 등 단말기 옵션 변경 등

(2) 개인 PC 보안 설정

① 공유폴더관리: 공유폴더는 네트워크를 통해 여러 사람이 사용할 수 있도록 제공되는 컴퓨터의 공동 자료저장 공간이므로, 임의의 사용자가 삭제 또는 위·변조 하지 못하도록 숨은 공유 폴더 제거 및 공유 폴더 권한 설정이 필요하다.

② 화면보호기 설정: 화면보호기는 모니터에서 작업 중인 내용을 감추는 기능과 타인의 직접적인 접근을 차단하는 기능을 하므로 일정시간 자리를 비울 경우 화면보호기 암호가 작동되도록 설정한다.

③ 웹브라우저 보안 설정: 웹브라우저의 보안설정이 (보통) 이하이면 사용자 동의 없이 스파이웨어 등이 설치되고, 이로 인해 악성프로그램으로 인한 해킹목표 및 해킹 경유지로도 사용될 우려가 높으므로 보안 수준 설정은 (보통) 이상 설정해야하며, 필요에 따라서는 <사용자 지정>을 설정한다.

④ 이메일 보안 설정: 자체 이메일 시스템, Outlook Express 등의 메일 프로그램을 사용하여 웜 혹은 스파이웨어에 감염된 메일을 열어볼 경우 바이러스, 악성코드 등으로 계정 및 암호, 신용정보 등이 유출될 위험이 크므로 이를 방지하기 위해 바이러스 방지 및 미리 보기 방지 기능 설정 필요하다.

⑤ 웹메일 보안 설정: 받은 편지에 대한 바이러스 검사를 자동으로 해주는 웹 메일 시스템을 사용 시 보안 접속 기능을 제공하는 경우 반드시 체크해야 한다.

⑥ 침입 차단 및 팝업 차단 기능 설정: PC는 인터넷에 연결되는 순간부터 해커들로부터 지속적으로 공격을 받게 되는데, 이렇게 공격자가 네트워크를 통해 내 PC로 접속하지 못하도록 하기 위해 윈도우즈에서 제공하는 침입차단 기능 설정이 필요하다.

⑦ 부팅 디스크 관리: 해킹, 바이러스, 웜 등에 의한 침해사고시 부팅이 안되어 자료손실을 초래 할 수 있으므로, 시스템 복구를 위해 별도의 부팅디스크 제작이 필요하다.

⑧ 무선랜 보안 설정: 무선랜 사용 시 해커가 무선랜 AP(Access Point)에 접속해 네트워크를 사용할 수 있고, 자신의 네트워크 패킷을 도청해 각종 계정, 암호, 신용정보 등 중요정보를 가로챌 수 있으므로 보안설정이 필요하다. WPA2 이상의 암호화 보안 설정을 해야 한다.

⑨ 문서암호 설정: 문서에 암호를 설정한 후 저장하면 저장 내용이 암호화되어 내용 유출을 막을 수 있으므로 중요 문서는 암호화한다.

(3) PC H/W 및 S/W 운영 보안관리

① 운영체제의 불필요한 서비스 제거: 윈도우즈를 설치하면 많은 양의 서비스가 설치되는데 일부 서비스는 거의 사용되지 않으면서 보안 취약점을 발생시킬 수 있으므로 이러한 서비스는 제거가 필요하다.

② 이벤트 및 로그관리: 불법적인 접근 시도나 침해사고가 발생하였을 때 증거자료나 추적을 위해서는 이벤트 및 로그를 남겨야 하며 이를 위해서는 이벤트 뷰어 및 감사정책 설정이 필요하다.

(4) 개인 PC 및 노트북 보안 프로그램

① 바이러스 백신 설치: 바이러스는 개인 PC에 저장된 중요 데이터나, 시스템을 손상시키고 백도어 등을 심어 신용정보 등을 유출시키는 등의 심각한 문제를 초래할 수 있으므로 PC를 안전하게 보호하기 위하여 최소한의 정보보호 제품인 백신은 기본적으로 설치한다.

② 스파이웨어 제거기: 스파이웨어란 타인의 컴퓨터에 잠입, 해킹 툴 등을 설치하여 사용자의 중요한 개인 정보를 유출해 내는 프로그램으로 사용자 비밀정보 유출 방지를 위해 스파이웨어 제거기를 사용한다.

③ 개인용 침입차단시스템: 개인 PC에 인터넷 등 외부에서 들어오는 트래픽들을 접근통제 규칙에 따라 허가하거나 거부하여 해킹 등의 공격을 차단하는 기본적인 정보보호 제품으로 개인 PC내의 프로그램, 데이터 등의 보호를 위해 필요하다.

④ 스팸메일 차단기: 개인 PC나 서버에 탑재되어 광고, 음란물 등을 포함하는 대량의 불필요한 스팸메일을 제거하는 개인용 정보보호 제품으로 스팸메일 처리로 인한 업무 생산성 저하, 스팸메일에 포함된 악성코드로 인한 정보유출 등을 방지하기 위하여 스팸메일 차단기를 설치한다.

⑤ 랜섬웨어는 몸값을 뜻하는 Ransom과 악성 코드를 뜻하는 Malware의 합성어이며 사용자의 동의 없이 컴퓨터에 설치하고 무단으로 사용자의 파일을 모두 암호화시켜 인질로 잡고 금전을 요구하는 악성 프로그램을 말한다. 이를 방지하기 위해서는 안티랜섬웨어 솔루션을 설치하고 인터넷에서 출처가 불명확한 파일을 다운로드하지 말아야 한다.

(5) PC 통합 보안관리

① 패치관리시스템

- 보안관리 정책: 개인별로 보안 패치를 함으로써 각 PC별 보안패치 수준이 달라 발생하는 지속적인 보안 사고를 최소화하기 위해 중앙집중식으로 기업의 모든 시스템(또는 단일 종류의 시스템)에 대하여 패치 및 사용할 수 있는 어플리케이션을 통제하고 관리할 수 있는 기능을 제공하는 패치 관리 시스템을 설치할 필요가 있다.

- 주요 기능: 보안 기본정책 및 운영이 가능, 지속적이고 자동적으로 패치 적용, 중앙에서 집중적으로 보안관리, 패치 관리를 위한 인터페이스 제공, 보안정책에 맞춰 권한 부여 및 관리 및 패치 적용 현황에 대한 TOP Level 그래픽 리포팅 제공 등이다.

② 통합보안시스템

- 보안관리 정책: 중소기업에서는 기업 내 수많은 직원용 PC에 대한

백신 설치 및 업데이트, 불법프로그램 사용 감시, 패치 설치 등을 개별적으로 관리할 경우 보안수준 차이 및 관리의 어려움으로 인한 취약점, 비용문제 등이 발생할 수 있으므로 비용 대비 효과적으로 일관된 보안관리를 위해 통합 보안 시스템 설치가 필요하다.

- 주요 기능: 불법 소프트웨어 관리, 일괄적인 소프트웨어 배포 및 복구, 기업 내 S/W 및 H/W 자산관리, 중앙 집중식 바이러스 관리 및 실질적으로 각 PC에 대한 보안정책 관리가 가능하다.

4 서버 보안

(1) 서버 보안 일반

① 업데이트 관리: 윈도우즈 및 Unix 계열의 서버는 정식 발매 이후에도 취약성 등이 종종 발견되어, 이로 인해 해커들에 의해 해킹 공격을 받아 서버에 내장된 중요 데이터 등이 손실되거나 손상될 수 있으므로 업데이트 기능을 이용하여 보안패치 등이 최신 버전을 유지할 수 있도록 지속적인 업데이트한다.

② 계정 및 암호관리: 관리자 이외에 다른 사용자가 불법적으로 서버에 접근을 시도하는 행위 등으로 부터 보호하기 위해 패스워드 길이 및 잘못된 로그온 시도 횟수 지정 등 암호 정책 및 계정 잠금 정책 설정이 필요하다.

③ 공유폴더 관리: 공유폴더는 네트워크를 통해 여러 사람이 사용할 수 있도록 제공되는 컴퓨터의 공동 자료저장 공간이므로, 임의의 사용자가 삭제 또는 위/변조 하지 못하도록 숨은 공유 폴더 제거 및 공유 폴더 권한을 설정한다.

④ 파일시스템 관리: 파일시스템은 사용자 및 운영체제 데이터가 저장되는 운영체제의 자료구조이므로, 불법적인 로컬 및 원격 사용자로

부터 손상, 삭제, 특정 명령어 실행 등의 사고를 방지하기 위해서는 파일시스템에서 제공하는 권한 설정 등의 보안기능을 설정한다.

(2) 서버 운영 옵션 보안관리

① 서버 접근 제어: 접근제어는 각 사용자들이 디렉토리나 파일 등 특정 시스템 개체에 접근 할 수 있는 권한을 의미하며 다수의 사용자가 접근하는 서버 시스템의 경우, 정당한 사용자가 서버에 접근을 시도하는지 등에 정책을 세워서 관리한다.

② 사용자 권한 설정: 사용자별로 네트워크 및 서버 접근에 대한 권한을 설정함으로써 비인가자의 불법적인 접근을 사전에 차단 및 자원의 효율적인 관리를 위해 사용자별 권한을 설정한다.

③ 불필요한 서비스 제거 관리: 운영체제를 설치하면 많은 수의 서비스들이 설치되는데 일부 서비스는 실제로 거의 사용되지 않으면서 보안 취약점을 발생시키고 성능 저하를 초래할 수 있으므로 불필요한 서비스는 제거한다(예시, 미사용 FTP, Telnet, 내부 파일서버용 NAS의 인터넷 접속, 기타 외부 인터넷 서비스 등).

④ TCP/IP 통합보안 설정: 서버에 접속하는 사용자, 해킹 및 바이러스 차단을 위해서는 보안제품 사용 외에도 서버에 탑재된 TCP/IP에 대한 필터링 등의 보안설정을 통해 차단할 수 있으므로 이에 대한 보안설정이 필요하다.

⑤ 보안 옵션 설정: 계정관리, 계정 로그온, 디렉토리 서비스 엑세스, 개체 엑세스, 사용권한, 프로세스 추적, 정책 변경 등 시스템 관리자는 옵션을 설정하여 관리한다.

(3) 시스템 및 프로그램 접근 통제

① 접근통제정책 수립: 시스템과 프로그램에 대한 책임있는 IT 부문전문가 또는 관리자에 의해 수립되어야 하고, 접근 제어 정책은 사용자 편리, 운영상 효과, 기술적 제한을 고려한 보안부문 책임자가 정책을 수립한다.

② 접근통제정책(사용자 접근관리)

- 정보시스템 접근 권한에 대한 업무 절차 수립 및 공식적 시행
- 업무가 변경되거나 퇴사한 경우 접근 권한 즉시 제거
- 주기적으로 시스템 사용자 계정관리를 검토하고 모니터링 실시
- 특수 권한 사용자 계정관리는 별도로 관리
- 시스템 오류 또는 운영체제 보완을 위한 정기적 점검 필수
- 사후 보안 사고를 대비하여 최소 기간 동안 기록관리

③ 시스템 관리자 접근관리

- 전산 시스템 담당 업무를 분산하여 접근할 수 있도록 상호 견제 관리체계 구축이 필요
- 로그 수정, 해체, 삭제에 대한 자동 백업 시스템 구축
- 컴퓨터 운영자나 보안관리자라도 열람 및 출력에 대한 기록을 삭제하지 못하도록 조치
- 규칙적이고 적절한 방법으로 시스템 로그 및 시스템 감사

④ 데이터 무결성 관리

- 데이터 베이스상에 있는 자료 값들이 정확하도록 보장하는 관리 작업이 필요
- 잘못된 갱신으로부터의 보호나 불법적인 조작에 대한 보호를 통한 정확성 유지
- 데이터베이스 시스템 내의 무결성 유지관리 제어시스템 운영

5. 네트워크 보안

(1) 네트워크 보안 위협

① 네트워크 보안 개요: 데이터 및 네트워크 링크의 가용성과 네트워크를 통해 전송되거나 처리되는 정보의 정확성 및 안전성, 일관성을 통한 정보의 무결성을 보장하는 데 목적이 있다. 또한 정보의 비밀성도 보장해야 한다.

② 네트워크 보안 패러다임의 변화: 정보통신망의 융합, 인터넷 기반망의 세분화, 유무선 통합지원 백본망, 유무선 네트워크의 초고속화, 무선통신의 발전 및 네트워크 노드의 지능화 등이다.

③ 차세대 네트워크 보안모델

- 이기종 보안 제품들간 상호연동을 위한 프로토콜 개발
- 시스템 보안기능과 네트워크 기능을 함께 갖춘 성능 보장형 프로토콜 개발
- 사용자 서비스 및 편의 제공, 인증의 간편화 구조이면서 안전한 보안모델 개발

※ 네트워크 보안 일반 (예시)

ㅇ 아래 내용이 포함된 도입절차를 수립하여 새로운 네트워크 장비 도입/변경 시 활용한다.
- 현재 NW 장비의 이용률, 사용량, 능력한계 분석, 추가 자원의 필요성 및 시기에 대한 예상
- 성능, 안전성, 신뢰성, 보안성, 법규 등을 포함한 NW장비의 기능적, 운영적 요구사항 파악
- 기존 장비 및 통제 솔루션과의 호환성, 상호 운영성, 기술표준에 따른 확장성 등 고려

ㅇ 계정/권한 관련하여 아래 내용을 포함하는 관리 정책을 수립한다.

- 1인 1계정 사용, 공유금지 (필요 時 별도 승인), 최소권한 부여
- 계정/권한 신청, 승인 절차 (R&R)
- 비밀번호 작성 및 변경 규칙 적용, 인사이동 시 권한 변경/말소 처리
- 권한 부여/변경기록 보관
- 주기적 이행 점검 등

ㅇ 아래 내용을 포함하는 내부Network 접근통제 관리 정책을 수립한다.
- 외부에서 내부망 접근통제를 위한 방법 및 정책 (인터넷, 관계사, 타사 등)
- 내부 망 사용 장비 (PC / 모바일 등)의 통제 방법 및 정책
- 접근 통제 허용 절차 등

(2) 네트워크 공격 방법

① 서비스 거부공격 (Denial of Service)

- DoS공격은 대량의 패킷을 이용하여 네트워크를 마비시키거나 특정 서비스의 수행을 방해 하는 공격으로 시스템의 한 프로세스가 자원을 모두 독점하여 다른 프로세스가 서비스를 제공하지 못하도록 하는 공격이다.
- 네트워크로 연결되어 있는 많은 수의 호스트들의 패킷을 범람시킬 수 있는 DOS(denial of service) 공격용 프로그램을 분산 설치하여 이들이 서로 통합된 형태로 공격 대상 시스템에 대해 시스템 마비를 일으키는 기법이다. DOS 공격은 공격할 시스템의 하드웨어나 소프트웨어 등을 무력하게 만들어 시스템이 정상적인 수행을 하는데 문제를 일으키는 모든 행위를 의미하며 매우 다양한 공격이 가능하고, 즉시 주목할 만한 결과를 얻을 수 있다. 공격 방법으로는 smurf, trinoo, SYN Flooding 등이 있다.

② 스니핑 (sniffing)

- 스니핑은 네트워크상에서 자신이 아닌 다른 상대방들의 패킷 교환

을 엿듣는 것을 의미하며 간단히 말하여 네트워크 트래픽을 도청(eavesdropping)하는 과정을 스니핑이라고 할 수 있다.
- TCP/IP 프로토콜을 이용한 통신에서는 통신매체를 통과하는 패킷들이 암호화가 되지 않은 상태이므로 이 패킷을 도청하여 메시지 내용을 볼 수 있다. 공격방법에는 Switch Jamming, ARP Redirect 공격, ARP Spoofing 공격 등이 있다.

③ 스푸핑 (spoofing)

- 스푸핑 공격은 IP주소, 하드웨어 주소(MAC address)등의 정보를 속임으로써 권한을 획득하고 중요 정보를 가로채고, 서비스 방해까지 행하는 공격으로써 다양한 원리를 이용하여 공격을 수행하는 기술이며, 예로써 리눅스의 rlogin 서비스는 서버에 클라이언트의 IP 및 계정을 등록하여 등록된 클라이언트만이 서버에 접속을 허용하는 서비스로써 공격자는 정상적인 클라이언트 패킷을 스니핑하여 IP 및 계정정보를 획득하고 계정생성과 IP변경을 통하여 서버에 비정상적인 접속을 시도한다. 스푸핑 방법에는 ARP 스푸핑, DNS (Domain Name Server) 스푸핑, 이메일 스푸핑 등이 있다.

④ 시스템 오류를 이용한 공격

- 지정된 메모리의 양보다 더 많은 양의 데이터를 쓰려고 할 때 발생하거나, 컴퓨터 프로그램을 실행시키는 과정과 컴퓨터가 프로그램을 실행시킬 때 메모리에서 일어나는 일 등을 자세하게 이해하고 있어야 공격방법을 이해할 수 있는 어려운 기술 중의 하나다.
- 공격 방법으로는 버퍼 오버플로우 공격, 스택 버퍼 오버플로우 공격, 힙(Heap) 오버플로우 공격 등이 있다.

⑤ 사회공학적 방법(Social Engineering)

- 사람을 속여서 민감한 정보를 유출하게 하는 방법으로 피싱

(Phishing)이 대표적이다.

(3) 네트워크 보안 관리

① 네트워크 보안정책 및 접근통제

- 네트워크에 접근 가능한 사용자를 구분하여 인가하고 관리
- 외부로 부터의 연결은 반드시 사용자 인증을 거치도록 조치
- 유관기관과 네트워크를 공유하는 경우 논리적으로 네트워크 분리
- 공유 네트워크나 외부 네트워크 사이에 연결이 존재하는 경우 라우팅을 설정
- 외부 해킹 시도에 대한 보호장치를 만들고 주기적으로 점검
- 시스템 관리자 및 유지 보수자에 대한 관리도 엄격하게 조치

② 네트워크 위협으로부터 보호방법

- 자료의 중요도에 따라 보안등급을 설정
- 가능한 네트워크 경로에 관한 이력관리 실시
- 데이터 전송 경로를 지정 관리
- 허가되지 않은 사용자의 접근을 통제
- 송/수신자간 신원 확인을 위한 경우 인증 확인.
- 전송 또는 비밀 데이터 전송 시 암호화하여 전송

③ 네트워크 대역 분리 및 망분리 사용

- 기업내부 네트워크 IP대역은 고정 IP를 사용하여 부여된 IP를 관리하고 부서별로 서로 동일 네트워크 대역을 사용하지 말아야 한다.
- 또한 기업내 상주하는 외부인, 협력사 직원들의 네트워크 구역도 별도로 설정하여 내부직원 네트워크 대역과 구분한다.
- 만일 협력사에 내부 네트워크 사용을 지원하게 될 경우에는 협력사 네트워크를 통하여 내부 내트워크 접속을 차단하고 필요시 보안정

책에 의거하여 서비스를 하게한다.
- 특히 기업에서 산업기술이나 영업비밀 등 중요 기술정보나 자료가 있는 서버, DB, 저장 매체 등은 해킹 등의 유출 위험을 감소하기 위하여 인터넷망과 분리되도록 네트워크 구성을 하여야 하며, 중요 부서나 연구부서 등도 인터넷망 접속을 차단하거나 망을 분리하여 사용하게 한다. 다만 인터넷망을 필요시에는 망연계 시스템을 통하여 자료를 전송하도록 한다.

(4) 네트워크 보안시스템

① 방화벽 (Firewall)

- 방화벽이란 외부로부터 내부망을 보호하기 위한 네트워크 구성요소 중의 하나로써 외부의 불법 침입으로부터 내부의 정보자산을 보호하고 외부로부터 유해 정보 유입을 차단하기 위한 정책과 이를 지원하는 H/W 및 S/W를 말한다.
- 외부망에 의한 내부망과 시스템을 보호하기 위하여 내부망으로 들어오는 모든 패킷을 검사하여 미리 허가된 패킷만 통과시키는 보안시스템이다.

② 방화벽의 기능

- 접근제어 : 정책에 의하여 허용/차단 결정하기 위한 검사
- 로깅 및 감사추적; 인증(Authentication); 스니핑 등의 공격에 대응하는 방법의 인증; 무결성 및 트래픽 암호화 및 트래픽 로그

③ 도구 및 방법

- TCP-Wrapper: 네트워크서비스에 관련된 트래픽을 제어하고 모니터링 할 수 있는 방화벽 Tool로써 임의의 호스트가 서비스를 요청해 오면 실제 데몬을 구동하기 이전에 접속을 허용한 시스템인지 아닌

지 여부를 확인하여 호스트명 및 서비스명을 로그에 남긴 후 허가된 시스템은 서비스를 제공하고 허가되지 않은 경우에 접속을 차단하는 도구이다.
- IPchain/ IPTable: 패킷필터링 방화벽으로 패킷이 어디서 왔는지 어디로 향하는지, 어떤 프로토콜을 이용하는지 등의 정보를 이용하여 패킷을'DROP'하거나 'ACCEPT'하는 방법으로 차단한다.

④ 방화벽 구축 시 고려사항

- 어떤 정보를 보호할 것인가
- 보호해야 할 정보들에 대한 위협 분석
- 정보의 중요성에 대한 분석
- 사용자 계정에 대한 정의
- 보호해야 할 정보에 사용 가능한 어플리케이션과 서비스 종류 분석
- 네트워크 장비 및 호스트 보호에 대한 비용 분석
- 해커 등과 같은 불법 침입자가 시스템 내부에 침입했을 경우 대응책 강구
- 네트워크 시스템에서 자동 점검 시스템 운영 및 주기적인 보안점검

(5) 침입탐지시스템(Intrusion Detection system)

① 침입탐지시스템의 구축 목적은 해킹 등의 불법 행위에 대한 실시간 탐지 및 차단과 침입차단시스템에서 허용한 패킷을 이용하는 해킹 공격의 방어 등이다. 침입탐지시스템은 대상 시스템(네트워크 세그먼트 탐지 영역)에 대한 인가되지 않은 행위와 비정상적인 행동을 탐지하고, 탐지된 불법 행위를 구별하여 실시간으로 침입을 차단하는 기능을 가진 보안시스템이다.

② 침입탐지의 목적

- 외부로 부터 공격뿐만 아니라 내부자의 IP 도용 해킹도 차단 가능

- 접속하는 IP에 상관없이 모든 Packets에 대해 검사하므로 침입 차단
- Hacking 발견 시 시스템 관리자에게 휴대폰, 전자메일 등으로 즉시 전송하므로 신속 대응 가능
- 탐지는 물론 침입 경로까지 파악 가능하므로 근본적인 차단 시스템 구축이 용이

③ 침입탐지 모델

- 침입탐지 모델은 입력의 타입이나 시스템의 상태, 특정 패턴 등의 요소를 규칙에 어긋날 때 인지하는 방법
- 정해진 모델과 일치할 경우를 침입으로 간주하는 방법
- 생성된 Profile을 주기적으로 관찰하여 비정상적인 행위를 추출하는 방법

(6) 가상사설망(VPN, Virtual Private Network)

① 기업 간 또는 기업과 사용자간 중요 기밀자료를 인터넷 등을 이용하여 교환 시 공격자에게 자료 누출, 변조 등의 침해사고가 발생할 수 있으므로 이를 방지하고 안전한 데이터 전송을 위해 인터넷망을 전용선처럼 사용할 수 있도록 특수통신체계와 암호화기법을 제공하는 서비스가 필요하며 VPN은 이를 지원한다.

② VPN 사용 시 장단점

- 적은 예산으로 광범위한 네트워크 구성 등 효율성 제공으로 경제적 이익 기대
- 가입자별 서비스 차별화를 할 수 있어 서비스의 질적 향상 도모
- 새로운 기술의 접목이 가능
- 전용선과 같은 수준의 신뢰성 확보 부족
- 사설망에 비해 완벽한 보안처리가 미흡

(7) 네트워크관리 시스템(NMS, Network Management System)

① 네트워크 관리시스템은 네트워크상의 장비들에 대한 중앙 감시 체계를 구축하여 트래픽을 모니터링하고 관련 정보를 수집, 분석, 저장하는 시스템으로 해킹 및 시스템 장애 등으로 인하여 시스템 및 네트워크 이상 발생 시 적시에 발견하고 대응하기 위해 필요하다. 주요 기능은 장애관리, 구성관리, 계정관리, 성능관리를 지원한다.

(8) 통합 보안관리 시스템(ESM, Enterprise Security Management)

① 보안을 강화하기 위하여 다양한 장비를 구축하여 왔으며 서로 다른 기종의 보안장비 및 솔루션을 구축 운영하는 경우에 관리의 효율성을 높이고, 보안 취약점을 최소화하며, 이기종간의 연동을 통해 전체 시스템의 통합 관리 중요성이 증대되고 있다. 이를 지원하기 위하여 통합 보안관리 시스템이 필요하고 통합 보안정책 수립 등으로 종합적이고 효율적인 대응 및 유지관리 용이성을 제공하고 있다. 주요기능은 관제기능, 운영관리 기능 등이 있다.

(9) 무선 네트워크 접속 통제

① 무선네트워크 시스템의 효율적인 보안 관리를 위하여 무선인터넷 관리자(이하 “관리자”라 한다)를 지정한다. 그리고 관리자는 자체적으로 보안성을 평가하여 보유 자료에 대해 접근권한을 차등 부여하고, 정보보호책임자는 관리자의 보안성 평가에 따른 등급에 따라 접근권한을 해당 사용자에게 부여한다.

② 무선네트워크의 효율적인 보안 관리를 위하여 무선 인터넷 관리자를 지정하고, 관리자는 보유 자료에 대해 접근권한을 차등 부여하고, 정보보호책임자는 관리자의 보안성 평가에 따라 접근권한을 사용자에게 부여함으로써 인가된 범위 이외의 자료접근을 통제한다.

③ 무선네트워크 시스템의 효율적인 보안 관리를 위하여 관리자를 지정 및 운영하고 관리자는 허가를 받지 않은 자가 무선네트워크 시스템 또는 업무용 PC 등을 무단으로 조작하여 전산자료를 훼손시키지 못하도록 아래와 같은 보안대책을 단말기 사용자에게 지원할 수 있다.

- 장비·자료·사용자별 비밀번호를 사용하고 주기적으로 변경하고 지문인식 등 생체인식 기술을 적용
- 5분 이상 PC 작업 중단 시 비밀번호가 적용된 화면보호 조치 실시
- PC용 최신백신, 침입차단 · 탐지 시스템 등을 운용하고 운영체제 및 응용프로그램의 최신 보안패치를 유지

6. 인터넷 보안

(1) 인터넷 보안 위협 요소

① 인터넷 보안 위협 요소

- 데이터 변조, 전송 메시지 변조와 위조 또는 네트워크상에서 도청, 네트워크 구조 정보 유출, 서버 정보 도난
- 사용자 서비스 거부, 시스템 및 디스크 메모리 오버 플로우
- 정당한 사용자를 사칭하거나 데이터 변조

② 인터넷을 통한 공격유형

- 취득한 정보의 변조, 재전송, 불법 수정, 불법적인 서비스 접근
- 신분위장: 타인이 권한자 행세를 하면서 적극적인 공격형태를 취함
- 재전송: 획득한 데이터를 다른 결과를 발생시키기 위해 재전송
- 메시지 변조: 수신자에게 전송되는 자료를 획득 변조하여 수신자에게 오인하도록 전송
- 메시지 송수신 부인: 개방형 통신망의 헛점을 이용하여 혼란 야기

- 불법적인 시스템 접근: 불법적으로 획득한 권한을 이용 시스템 내 자료 파괴 및 서비스 정보 이용

③ 인터넷 위협으로부터 보호

- 데이터와 정보의 비밀 유지를 위해 암호화 송수신 시스템 구축
- 메시지에 대한 서명과 인증 시스템 확보
- 접근 권리를 결정하거나 부여하기 위해 접근대상 정보 및 접근자의 자격 통제 및 다양한 방법으로 검증할 수 있는 인증 시스템 구축
- 네트워크/서버/호스트 침입차단 시스템 구축
- 보안사고 대비 로그온 관리나 감지시스템 구축
- 개인정보보호를 위한 별도의 서버 관리 및 엄격한 접근 통제
- 주기적인 모의 해킹 또는 시뮬레이션 점검

④ 인터넷 사이트에 대하여 수시 검색을 실시하여 인터넷상에 Open 되어 있는 홈페이지나 인터넷 사이트를 찾아서 보안 정책들이 적용되어 있는지 확인하고 미흡시에는 즉시 보안을 적용하여야 한다.

- 쇼단(https://www.shodan.io) 등을 이용하여 홈페이지, ERP, 그룹웨어, 이메일, FTP(파일전송 서비스) 등 인터넷에 외부로 열려있는 사이트를 확인한다.
- 임직원들의 명함이나 이메일 주소를 내부 시스템의 계정으로 사용하지 않도록 하여야 한다.
- 각종 서버 및 네트워크, 정보시스템에 대한 취약점을 점검한다.

(2) 웹 서버 보안

① 웹 서버의 취약점

- 공개용 또는 상용 웹서버의 구현상 문제로 인한 보안 취약점 존재
- 외부의 사용자에게 호스트의 정보를 보여주거나 사용자의 입력 정

보를 통해 임의의 명령 수행 등이 취약
- 웹서버 구성의 잘못으로 파일 접근권한 획득, 디렉토리 내용 리스팅, 심볼릭 링크 등이 취약
- 다른 서비스와 연계된 복합적인 문제점 노출 우려에 따른 웹 서버 보안대책 요구

② 웹 서버 보안대책

- 웹서버에서 불필요하게 제공되는 서비스를 삭제하여 문제 요인 제거하고, 일반 호스트의 서비스 삭제 등 최소한의 인터넷 서비스만 제공한다.
- 서비스 거부 공격에 대비하여 최신 버전의 보안 패치와 동시에 암호화, 인증기능을 강화한다.
- 정기적으로 백업을 하여 해킹이나 재난에 대비하고, 침입탐지 시스템에 침입시도가 있을 경우 경고기능 추가하며 웹 서버 관리는 콘솔에서 하고 원격 접근 시 해당 로그를 존치한다.
- 시스템의 취약점을 점검해 주는 보안도구 설치를 의무화한다.

(3) 인터넷 IP 프로토콜(Protocol)

① IPv4

- 현재 인터넷을 연결하고 있는 TCP/IP 버전4 프로토콜
- 주소의 크기는 32비트이고, 라우팅에 의한 경로 배정
- 인터넷 사용자의 급증에 따른 인터넷 주소의 부족
- 현재 발생하고 있는 보안적인 문제에 대한 대비가 취약

② IPv6

- IPv4의 기능적 호환성을 갖고 있으며, IPv4의 취약점인 주소 고갈문제를 해결한 버전(128비트)

- 고속망, 저속망에서도 효율적으로 정보 서비스 제공
- 미래의 새로운 옵션에 대응하기 위한 유동성 제공
- 송신측이 특별한 처리를 요구할 경우 특별한 트래픽에 속하는 패킷의 라벨링 즉, Flow Labeling 가능
- 데이터의 무결성 및 비밀성을 제공하는 인증과 Privacy 기능
- IPv4에 비해 네트워크 해석에 있어 융통성 있는 라우팅 제공

③ IPSec

- 암호화와 인증이라는 강력한 보안 서비스를 IP 패킷 단위로 제공하며 이 기술은 방화벽이나 VPN에 응용
- 차세대 인터넷 프로토콜인 IPv6에서는 IPSeC을 포함

(4) 각종 인터넷 보안 도구(Tool)

① 보안소켓계층(SSL : Secure Socket Layer)

- 사이버 공간에서 전달되는 정보의 안전한 거래를 보장하기 위해 인터넷 통신규약 프로토콜
- 주요 포털업체들이 개인정보 누출 방지를 위해 금융거래 온라인 결재 부문에 사용
- 세션 식별, 전자서명, 상호인증, 암호화 체계 구축

② 전송계층보안 (TLS : Transport Layer Security)

- 두 통신개체 사이에 안전한 연결을 설정하기 위해 Privacy와 신뢰성을 제공 및 상대방의 신원은 비대칭 암호화 기법을 사용하여 인증하므로 보안성 향상
- 공유 비밀정보의 협상은 안전하고 연결부 중간에서 비밀정보가 도청될 가능성 배제
- 신뢰성이 보장되고 공격자에 의해 통신 내용이 수정될 수 없으며,

이에 대한 시도를 감지 가능
- 전자서명, 데이터 암호화, 공개키 암호화 체계 구축

③ PGP (Pretty Good Privacy)

- PGP는 전자우편의 경우 다른 사용자에게 도달할 때까지 여러 호스트를 거치게 되며, 전송 도중에 얼마든지 도청, 변조될 가능성이 상존하는 문제가 있으므로 이를 해결하기 위한 개발된 보안기술이다.
- 전자우편 내용을 암호화하여 전송하므로 중간에서 도청한다고 해도 암호키가 없기 때문에 열람이 불가하다.
- PGP는 특정한 키가 있어야만 내용을 볼 수 있기 때문에 기밀성, 인증, 부인방지 등의 보안기능을 제공한다.
- 문제점: 사용자 A의 키라고 받은 공개키가 정말로 A의 공개키인지 확인하는 방법이 어렵다.
- 공개키 관리 : 플로피 디스크나 우편으로 직접 전달, e-mail송부 후 전화확인 또는 인증기관을 통해 전달한다.
- 문서에 디지털 서명이 부가되면 수신자가 문서를 받아보고 불법적인 변경 여부를 확인한다.

④ S/MIME (Secure / Multipurpose Internet Mail Extension)

- PGP의 보안 문제점을 보완한 전자우편 보안시스템
- 다수의 수신자를 위한 암호키, 서명된 데이터의 암호화
- S/MIME은 전자우편 송부 전에 반드시 전자서명, 암호화 또는 전자서명 + 암호화 선택을 하도록 구성
- 사용자가 S/MIME 보안 서비스를 받기 위해서는 공개키 인증서를 미리 발급을 의무화
- 수신자에게 안전하게 배달되었음을 알려주는 영수증을 제공

7. 무선통신 보안

(1) 무선통신 보안

① 무선 네트워크 보안 정책에 따라 아래 사항 확인하고 이행한다.

- 무선 네트워크 장비 접속 단말기 및 사용자 인증
- 무선 네트워크 접속 단말기에 대한 보안(백신 등)
- 무선 네트워크 장비(예: AP, Access Point) 보안 및 허용장비 리스트
- 무선 네트워크를 통하여 접근 할 수 있는 정보시스템 범위 또는 기능 정의
- 무선 네트워크 사용권한 신청/변경/삭제 절차, 사용자 식별 및 인증
- 무선 네트워크 서비스 거리 제한 (주파수 세기 조정), 정보송수신 시 무선망 암호화 기준(예시: WPA2)
- 전산실 등 통제구역 내 무선 네트워크 사용 제한 및 외부자용 무선 네트워크와 분리
- SSID(Service Set Identification) 브로드캐스팅 중지 및 추측 어려운 SSID 사용 등

② 아래 내용이 포함된 도입절차를 수립하여 데이터베이스 도입에 활용한다.

- 현재 시스템 자원의 이용률, 사용량, 능력한계 분석, 추가 솔루션의 필요성 및 시기에 대한 예상
- 성능, 안전성, 신뢰성, 보안성, 법규 등을 포함한 솔루션의 기능적, 운영상 요구사항
- 기존 시스템과의 호환성, 상호 운영성, 기술표준에 따른 확장성
- 해당 솔루션을 통한 보안사고 사례 및 알려진 취약점에 대한 조치 현황 등

③ 계정/권한 관련하여 아래 내용을 포함하는 관리 정책을 수립한다.

- 1인 1계정 사용, 공유금지 (필요 시 별도 승인), 최소권한 부여

- 계정/권한 신청, 승인 절차 (R&R)
- 비밀번호 작성 및 변경규칙 적용, 인사이동 시 권한변경/말소 처리
- 권한 부여/변경기록 보관
- 응용프로그램(웹 등)용으로 부여된 계정의 경우 사용자의 공용 사용 금지(별도 계정 부여)
- 주기적 이행 점검 등

④ 아래 내용을 포함하는 DB 접근 통제 정책을 수립한다.

- 접근 통제 대상 DB 정의
- 일반 사용자의 DB 직접 접근은 가급적 차단(일부 CS 방식 프로그램은 가능한 보안 대책 강구 필요)
- 서비스 목적 접근은 서버 IP와 서비스 Port 기반 허용하며, 외부 및 DMZ 서버의 직접 접근은 가급적 제한
- DBA등 관리자의 접근은 접속 가능한 Tool과 허용 인력, 접속 Port, IP 등을 한정(접근 통제 Tool 사용 등)
- 중요정보가 포함된 DB는 접속자에 따라 테이블 또는 컬럼 단위로 접근을 통제
- 상기 접근 허용을 위한 신청시스템 운영

⑤ 기획/분석 단계에서 일반적인 개발보안 요건 도출 및 영향 평가를 통한 보안 요건 도출을 실행한다.

- 사업의 정보보호 요구사항(예: 접근권한 정의 및 통제 원칙, 암호화 대상 선정 등)
- 정보보호 관련 기술적인 요구사항 등(예 : 인증, 암호화 등)
- 최초 계약 시 보안 요구 사항 및 분석 및 평가를 통한 보안 요건은 기능적/비기능적 보안 요구사항으로 관리함

⑥ 설계/개발 단계에서 Secure Coding을 적용하고, 운영자와 개발자의 직무를 가급적 분리한다(운영 시스템 접근통제 포함).

⑦ 테스트/운영 이관 단계에서 Infra 취약점 점검, 모의해킹, 소스코드 취약점 분석, 등을 수행하여 결함을 조치한다.

⑧ 계정/권한 관련하여 아래 내용을 포함하는 관리 정책을 수립한다.

- 1인 1계정 사용, 공유금지 (필요 時 별도 승인), 최소권한 부여
- 계정/권한 신청, 승인 절차 (R&R)
- 인사이동 시 즉시 권한 변경/말소 처리
- 권한 부여/변경기록 보관 및 주기적 이행 점검 등

⑨ Application 접근통제 관련하여 아래 내용을 포함하는 관리 정책을 수립한다.

- 사용자 권한 유형에 따른 접근 통제 강화 방식
- 사용자의 접근 환경에 따른 접근 허용 여부 (모바일 접근 or 외부 PC 접근 등)
- 접근 시 인증 방식 (ID/PW, OTP 등), 세션 처리 방식
- 접근 시 암호화 대상 및 암호화 방식
- 접근 통제에 대한 허용 및 예외처리 절차

(2) 무선 LAN 보안

① 보안설정이 되어 있지 않은 무선랜은 외부인으로부터 무선공유기를 무단으로 사용할 수 있고 해커가 접속하여 해킹이나 정보유출 등 다양한 보안사고를 유발할 수도 있다. 그 중 스마트폰 사용자는 무작위로 검색되는 무선 AP를 이용하는 사례가 늘고 있기 때문에 대상기관에서는 각별히 주의한다. 요즈음 사용하고 있는 스마트폰은 기존 PC에서 가지고 있던 위협과 모바일기기의 위협을 모두 포함하고 있으므로 무선랜 보안 설정은 필수적이다.

② 무선 LAN의 기술적 취약점

- 도청: 무선 AP에서 발송되는 전자파가 필요 이상으로 전달되는 것
- DoS(서비스거부): 무선 AP에 대량의 무선패킷을 전송하여 무력화하는 것
- 불법 AP: 공격자가 불법적으로 전송 데이터를 수집하는 것
- 비인가 접근: ID, MAC 주소 노출로 정보 취득 후 무력화 시키는 것

③ 무선 LAN 보안정책

- 기업은 무선 LAN 사용을 제한하고 특별한 경우 허가 후 암호 노출 방지 대책을 수립
- 비허가자 접근 탐지 및 차단 시스템을 구축
- 허가된 무선랜 암호는 주기적으로 변경하여 사용
- 사용자가 일정기간 미사용 시 자동접속 기능을 차단 및 설정
- 정책 위반 무선장비의 로깅을 차단
- 사용자 로그에 대한 수시 분석 실시
- 사용자가 일정기간 미사용 시 자동접속 기능을 차단 설정

④ 무선 LAN 암호화 기술

- WEP(Wired Equivalent Privacy): 대칭키 구조의 암호화 알고리즘 RC4 사용 및 RC4 알고리즘은 그대로 사용하면서 암호화 킷값을 주기적으로 변경 관리
- TKIP(Temporal Key Integrity Protocol): 기존 WEP 보안상 문제점을 개선 및 WEP이 갖고 있는 기본적인 취약점은 그대로 존재하므로 보안성이 미흡
- WPA(Wi-fi Protected Access): 별도 인증 서버가 있어서 서버에서 인증을 통과해야만 접속 가능 및 WPA에는 WPA2, WPA-PSK 등 여러가지 방식 존재

(3) 모바일 보안

스마트폰은 개인이 휴대가 간편하고 통제관리가 어려우며 저장 공간이 엄청난 관계로 기관에서 보안관리 측면에 가장 어려움이 많다. 더욱이 기업의 업무 편리성을 위해 제공되는 스마트폰은 개인 또는 공용으로 사용하기 때문에 각별한 주의가 필요하다.

① 스마트폰의 위험 요인

- 스마트폰 분실 및 도난에 따른 기업정보 유출
- WI-FI 해킹 및 사용자 부주의에 의한 도/감청
- 바이러스 감염 스마트폰과 회사 내 PC 연결을 통한 악성코드 전파
- GPS를 통한 위치 정보 노출
- 스마트폰에 설치된 기관 시스템 탈취로 인한 2차 보안사고 유발

② 기업용 스마트폰 보안대책

- 등록된 단말기만 업무시스템에 접속 허용
- 업무자료 유출방지를 위해 무선랜, 터더링, 화면캡처 금지
- 운영체제 무결성을 주기적으로 점검할 수 있도록 기업별 모바일관리시스템 MDM 시스템 설정 운영
- MDM 시스템은 분실 도난 시 저장자료 와 소프트웨어 원격삭제 보안대책 마련
- 비밀번호 주기적 변경 수행 및 인증코드 운영
- 비정상적인 접속 시 강제 세션 종료
- 모든 송수신 데이터 암호화 기능 부여
- 기업용 스마트폰 주기적인 모니터링으로 보안성 점검

8. 클라우드 보안

(1) 클라우드 특징

① 클라우드 사업자와 직접 상호작용하지 않고 사용기업(사용자)별로 제공하는 개별 관리화면을 통해 서비스를 이용할 수 있다.

② 모바일 기기 등의 디바이스를 통해서 서비스접속이 가능하다.

③ 사업자의 컴퓨팅 리소스를 여러 사용기업(사용자)이 공유하는 형태로 이용하며, 사용기업(사용자)는 자신이 사용하는 리소스의 정확한 위치를 알 수 없다.

④ 필요에 따라 필요한 만큼의 스케일 업(처리능력을 높이는 것)과 스케일 다운(처리능력을 낮추는 것)이 가능하다.

⑤ 이용한 만큼 요금이 부과되는 종량제 서비스이다.

⑥ 클라우드 서비스 관리 주체와 수준에 따라 서비스형 인프라 스트럭처(IaaS), 서비스형 플랫폼(PaaS), 서비스형 소프트웨어(SaaS)가 있다.

⑦ 클라우드 이용 모델에 따라 퍼블릭 클라우드, 프라이빗 클라우드, 커뮤니티 클라우드, 하이브리드 클라우드 등의 유형이 있다.

(2) 클라우드 보안대책

① 클라우드를 이용함으로 인해, 사용기업(사용자)은 자사가 보유한 정보의 관리와 처리를 클라우드 사업자에게 맡겨 운영하므로 보안 등의 리스크를 모두 통제할 수 없다는 문제가 발생할 수 있다.

② 클라우드 사용기업(사용자)은 사업자 및 이용자 측에 잠재된 보안 위험 요소를 확인하고 대응한다.

③ 사용기업(사용자)은 클라우드 사업자와 정보보호 및 개인정보보호

등에 대한 책임과 역할을 명확히 정의하고 이를 계약서나 SLA (Service Level Agreement) 등에 반영한다.

④ 클라우드 환경에서의 서비스 개발 및 배포 프로세스에 대한 개발 보안 정책을 수립하고 준수한다.

⑤ 클라우드 접속용 사용자 PC 등에서는 PC 보안 정책을 준수한다.

⑥ 클라우드 마스터 키 또는 특수 권한용 계정은 최고 관리자 이외에는 유출되지 않도록 한다.

⑦ 사용기업(사용자)의 PC 등에서 클라우드 서비스에 접속 시에는 VPN을 통하여 접속하여야 보안성을 강화할 수 있다.

⑧ IAM, OS 계정 등의 클라우드 계정관리 정책을 수립하고 준수하여야 한다. 미사용 계정은 비활성화 또는 삭제해야 한다. 또한 OTP 등의 이중인증을 사용하여 보안을 강화한다.

⑨ 클라우드에서 웹서비스를 이용하는 경우에는 웹방화벽 및 방화벽을 설치하여 운영한다.

⑩ 클라우드 서비스에서의 네트워크 보안 정책을 적용하여 업무의 중요도나 용도에 따라 프라이빗, 퍼블릭 등의 구역을 나누어서 보안을 적용한다.

⑪ 클라우드의 서버 및 DB에 대한 접속 및 작업은 로그를 저장하고 모니터링 할 수 있도록 한다.

⑫ 클라우드에서 서비스하기 위한 프로그램 Source Code는 설치하기 전에 소스코드의 취약점을 점검하여 보안 이슈가 없음을 확인한 후 제공한다. 특히 GitHub 등의 Open Source 등의 사용 시에는 반드시

소스코드 취약점의 유무를 확인하고 사용한다. 소스코드에는 절대로 클라우드 마스터 키 등의 중요 정보를 저장하지 않는다.

9 스마트 팩토리 보안

(1) 스마트 팩토리 특징

① 기업의 공장 설비들은 공정을 제어하고 운영하는 기반기술이 디지털화하고 인터넷에 연결되면서 제조공정의 인프라와 인력이 맞물린 사물인터넷(IoT)으로 변화하고 있지만, 사무환경보다 까다로운 산업현장의 보안성 확보 문제가 신기술을 활용하기 어려운 배경으로 작용하고 있다.

② 스마트 팩토리 핵심기술은 로봇, 3D프린터, 스마트센서, IoT, 빅데이터, 인공지능, 머신러닝, 디지털 트윈, 증강현실, 산업보안 등으로 구분되어 진다. 이 기술들은 물리영역, 네트워크영역, 데이터분석영역을 아우르는 전체 과정에 걸쳐 보안이 취약하면 생산 기반의 문제가 발생한다.

③ 스마트 팩토리에서 발생 가능한 보안사고 유형으로는 다음과 같다.

- 악성코드 유입
- 시스템 자체 취약성
- 무단 원격 접속
- 비인가 기기의 내부망 접속
- 직원의 실수
- 직원의 고의 프로그램 유출
- 비인가자의 자산 유출

④ 보안사고로 인한 피해는 공장이나 산업기반시설내 공정을 제어하는 PLC, 인버터, 서보드라이브, CNC, 분산제어시스템(DCS), 온도제어기, 유량제어기 등 공정 제어장치와 로봇, 디지털모터기동반같은 구동장치, 터치패널이나 HMI, SCADA같은 운전반, 이들을 연결하는 네트워크스위치와 데이터가 연결되는 산업데이터센터까지 위협 대상이 될 수 있다.

(2) 스마트 팩토리 보안대책

① 외부로부터의 바이러스 및 악성코드 유입은 제어 프로그램을 파괴한다.

- 제조업체는 보안관점에서 해당 시스템의 제어기와 네트워크 장치의 접근추적 기능 유무, 통신포트 잠금장치 유무를 파악한다.
- 보안패치를 적용하지 못해 시스템에 취약성이 존재하는 경우 바이러스 감염으로 설비 동작이 중단될 수 있다.
- 펌웨어 등을 최신으로 업데이트한다.
- 외부 침입자의 비인가 접근으로 데이터가 유출될 수도 있다.
- 제조업체는 해당 시스템의 보안패치 관리 기능, 제어기 공급업체별 보안패치 배포절차를 확인한다.

② 무단 원격접속, 비인가 기기의 내부 네트워크 접속으로 프로그램의 변경, 제어기 운전모드 변경, 프로그램 무단복제, 파괴 사고가 발생할 수 있다.

- 제조업체는 네트워크 스위치의 패킷조사 등 보안기능, 맥어드레스 인지 정확성 기능, 방화벽 설치여부, 접근제어 기능, 운전모드변경 추적기능을 파악한다.
- 디바이스들에 대한 초기 비밀번호를 재설정한다.
- 암호화된 통신 프로토콜을 이용한다.

③ 직원 실수나 고의, 또는 비인가자 네트워크 접속으로 제어프로그램 변경과 오작동, 바이러스 감염에 따른 시스템 중단 및 오작동, 산업

기밀 등 지적자산 유출 등이 벌어지거나 유도될 수 있다.

- 제조업체는 제어기의 패스워드 설정, 소스프로그램 보호 기능, 외부 접근에 대한 보호, 네트워크 접근제어 및 추적 기능, 프로그램 접근 제어 기능, 프로그램 수정 및 변경관리와 복구기능, 설정값 변경 추적기능, 중앙화 보안관리시스템 유무를 확인한다.

10. 모의 해킹

(1) 모의해킹 목적

① 해커의 입장에서 회사 내 보안의 취약성을 찾아내어 보안 문제점을 점검, 분석하고 대응방안을 제시한다.

② 해킹기술의 발달로 회사 내 전산시스템망의 안전성확보가 필요하며, 이를 위해 주기적인 실시가 필요하다.

③ 회사 내 전산시스템이나 각종 사용되고 있는 모든 프로그램의 무결성이 확보되었다고 보기 어려우므로 이를 예방하기 위한 보안시스템 역시 한계성이 존재하므로 모의해킹을 통한 시스템의 보완이 요구된다.

(2) 모의해킹 방법

① 정보시스템에 접근하는 방식을 두 가지로 구분할 수 있다. 하나는 네트워크 정보를 모르는 해커 입장에서 시도하는 외부망 접근 시도와 기본적인 네트워크 정보를 알고 수행하는 내부자 관점의 내부망 접근방식이다.

② 모의해킹의 수준과 해킹에 사용되는 Tool에 대한 범위를 정한다. 대부분의 해킹사고가 많이 발생하는 수준에서 점검을 실시하고 순차적으로 강화해 나가는 방법으로 추진하는 것이 바람직하다.

(3) 모의해킹 점검항목 및 절차

① 점검 Tool은 여러 기관에서 정의하고 있지만 회사 내 점검에는 ISS Internet Scanner 도구가 가장 보편적이다. 이 Tool은 침입탐지 패턴 데이터베이스를 이용하여 로컬, 원격 시스템 및 네트워크의 보안 취약점 점검을 수행하기 위한 스캐너이다

② 점검항목은 회사 내 실정에 따라 달리 하는 것이 좋으나 가장 많이 사용하는 항목이 SANS TOOL 20정도라고 보면 무리가 없다.

③ (모의해킹 절차) 점검대상 및 항목 선정/시스템 및 프로그램에 대한 정보수집 및 분석/모의해킹에 따른 위험성 사전 대비책 강구/대상 시스템 취약점 공격/침입에 대한 취약점 증거 확보/모의해킹에 대한 대응방안 보고서 정리

[표] 모의해킹 결과에 따른 개선조치 방안 (예시)

공격방법	차단방법	보안솔루션
특정 IP 및 Port 이용 공격	IP, Port 차단	Firewall
Worm, DoS	트래픽, 패턴분석	Network IP, Virus Wall
바이러스, 악성코드	파일, 프로세스 분석	Vachine, 서버보안
웹 애플리케이션 해킹	프로그램 취약점 수정	-

제2장 산업기술 유출·침해 대응 및 복구

제1절 산업기술 유출·침해 보안사고 대응 및 복구

1. 보안사고 확인 및 보고

(1) 보안사고 확인 및 보고・신고

① 내부 보고: 내부자에 의한 산업기술의 유출 등 보안사고를 발견한 경우, 사실관계를 확인한 후 보안규정 등 기관 내부의 보고체제에 따라 즉시 보고를 한다. 내부 보고 체계는 기관별로 절차적인 차이가 있을 수 있으나, 일반적으로 발견자, 그가 소속한 부서의 장, 그 부서가 속한 상급 부서장, 경영진(대표자 포함)의 순서이다.

② 국가기관에 신고: 산업기술의 유출방지 및 보호에 관한 법률 제15조(산업기술의 침해신고 등)에 따라 국가핵심기술과 국가연구개발사업으로 개발한 산업기술을 보유한 대상기관의 장은 그 기술이 유출 또는 침해 행위가 발생할 우려가 있거나 유출 또는 침해된 때에는 산업통상자원부(기술안보과) 및 국가정보원(산업기밀보호센터)에 신고(「산업기술보호법」 시행규칙 제7호 서식 참조)하고 필요한 조사 및 조치를 요청한다.

③ 보고 및 신고단계에서의 내・외부 공개 주의: 신고단계에서는 자체조사가 진행되어야 하므로 내부에서도 극소수 인원만 인지하고 증거자료 확인 및 관련정보 수집과 보안사고에 따른 영향 최소화 등의 조치가 선행되어야 하므로 외부에 일체 누설되지 않도록 한다(기술유출상담: 산업보안정보도서관(www.is-portal.net) 참조).

(2) 보안사고 자체조사 및 응급조치

① 기술유출 사고 사실 등 자체 조사

- 산업기술의 유출사고가 있거나 또는 이를 의심할 만한 상황이 발생한 경우, 이를 발견한 임직원 또는 보안부서는 일차적으로 산업기술 침해가 있었다고 판단되는 제반 상황 또는 유출이 의심되는 내부 또는 외부요인 및 임직원 또는 부서 등을 파악한다. 또한 의심할 수 있는 임직원 및 소속부서의 과거 업무 내역 확인 또는 외부에 의한 경로 등 기술유출 경로 등을 자체적으로 조사한다.
- 임직원 또는 부서를 확인하면서 어떤 경로로 산업기술이 유출되었는지 현장 또는 가능성을 조사한다. 해당 분야 산업기술 취급 인력, 보안관리실태(관련 도면, 자료, 컴퓨터 파일, USB 등의 저장장치 등의 보안관리 현황) 및 해당 산업기술에 대한 최근 열람 내지 수정 현황 등을 파악한다.
- 산업기술이 유출되어 이를 사용한 것으로 의심되는 기업에 대하여 과거 계약 여부・실적 또는 계약을 위한 교섭현황 등 업무상 내역 등을 파악하여 유출하였을 것으로 의심되는 임직원 또는 부서를 특정하거나 한정하여야 한다.
- 조사결과 포함할 사항은 관련 당사자, 유출발생 일시, 유출된 산업기술 등의 내용 및 규모, 예상되는 유출경로, 이로 예상되는 재산상 피해예상 규모, 향후 대책에 대한 의견 등으로 구성할 수 있다.
- 산업기술의 유출 등이 있다고 의심할 만한 정황으로는 산업기술로 관리하면서 생산하던 제품과 동일하거나 유사한 제품이 유통되고 있는 경우가 있다. 유사한 제품이 유통되고 있다면 해당 제품을 역설계Reverse engineering) 등을 실시하여 산업기술이 사용되었는지를 검증할 수 있다.

② 기술유출 사고에 대한 응급조치

- 산업기술 유출 등의 경위를 확인한 결과, 이미 발생한 보안사고의 확산을 방지하거나 또는 앞으로 추가적인 유출피해가 계속 발생할 수 있다고 예상되는 경우에는 즉각적이고 가능한 보안조치를 취하여 추가적인 유출피해를 방지한다.
- 내부 임직원에 의한 산업기술의 유출 등의 피해가 있었으나 그것이 제3자에게 제공되기만 하였을 뿐이고 아직 그 제3자가 이를 다른 곳에 유출하거나 또는 이를 사용하지 않고 있다면, 즉시 내부 임직원 및 제3자로부터 관련되는 산업기술의 추가 유출을 금지시킴과

동시에 산업기술 정보가 보관된 문서, 지료, 파일 등을 즉시 회수하고 이를 삭제 또는 보존 등 조치한다.

③ 정보침해 사고 피해 범위 등의 조사

- 정보보안사고에 의한 침해된 기술정보의 피해 범위를 평가하기 위해 무엇이 손상되고 피해가 발생되었는지 식별한다. 만약 보안사고에 따른 정보시스템의 취약성이 완전히 해결되지 않으면 사고 재발 가능성이 높아진다. 만약 손상된 기술정보가 복구될 수 없으면 보안사고를 해결하고 복구하더라도 업무과정에서 오랜 기간 영향을 줄 것이다. 네트워크로 서로 연결된 컴퓨터 및 정보시스템 환경에서 하나의 시스템이 손상을 받으면 다른 시스템의 모든 기술정보에 피해를 입었는지 파악하기 위해 조사한다.

- 보안사고의 정의에 따라 그 범위를 식별하고 그 영향이 평가되어야 하는데 우선순위를 부여하여 효과적으로 대응하기 위해서 보안사고에 의한 기술정보의 침해 범위를 분석하는 것이 매우 중요하다. 보안사고의 범위와 영향을 분석하기 위해 사이트의 결합 형태에 따라 다음과 같은 기준을 근거하여 적절하게 분석한다.

※ 정보침해 등이 보안사고 분석 사항(예사)

- 다중 사이트 사건인가?
- 사이트에서 많은 컴퓨터가 이번 보안사고에 영향을 받았는가?
- 국가핵심기술 등의 민감한 기술정보와 포함되어 있는가?
- 사건 침투지점은 무엇인가? (네트워크, 무선통신, 로컬단말기 등)
- 보안사고의 잠재적인 손실은 무엇인가?
- 보안사고의 종결을 위한 추정시간은?
- 보안사고 처리를 위해 요구되는 자원은 무엇인가?
- 법률적인 준수 의무에 따른 이행 요건과 관련이 있는가?
- 본 보안사고에 대한 언론에서 관심이 있는가?

- 보안사고로 인한 손실과 그 영향의 분석은 상당한 시간이 소비될 수 있다. 그러나 사건의 본질을 간파하기 위해 침해가 발생하자마자 전체 시스템과 모든 구성요소에 의심을 가져야 한다. 시스템 소프트웨어는 가장 가능성이 있는 표적이고, 예비조치가 시스템의 감염에 의한 모든 변화를 탐지할 수 있는 열쇠이다. 공급자로부터 받은 원본이 있다면 모든 시스템 파일에 대한 분석이 이루어져야 하고, 불법적인 사건 처리에 관련된 모든 부분은 기록 및 보관되어야 한다.

④ 정보침해 사고 피해 확산방지 응급 조치

- 정보시스템을 통한 산업기술정보 등 침해 시 보안사고 범위의 확산을 저지하기 위한 첫 번째 단계는 산업기술이 저장된 정보시스템의 가동을 중단하는 것이다. 정보시스템의 속도와 연결성은 보안 사고를 증가시키고 있다. 자동화된 공격시스템은 정보시스템의 네트워크와 취약한 서버의 위치를 스캔할 수 있다. 또한 인력의 개입이 없이도 시스템을 관찰할 수 있다.

- 대규모로 서로 연결된 정보시스템에서 단지 하나의 시스템만 손상을 받는 경우는 드물다. 이러한 환경에서 보안사고가 발견되었을 때 이를 복구하기 위해서 보안사고의 증거를 수집하는 것은 손상된 시스템의 결정에 도움을 줄 수 있다. 시스템 로그, 소프트웨어 변경, 설정파일 등은 손상을 표시하는데 이용될 수 있다. 유사한 속성(예: 운영체계 버전)을 가진 시스템 또는 실행중인 동일서비스는 일반적인 취약점을 통해서 손상되기 쉽다.

- 그리고 처음 침투공격이 시작된 곳으로부터 공격받은 정보시스템을 분리시킴으로써 공격의 접근을 방어할 수 있다. 주로 침입차단시스템(firewall)을 설치하고 침투공격의 접근을 차단하여 외부 공격자가 네트워크를 통해서 더 이상 침투할 수 없도록 한다. 공격자가 정보시스템으로 들어오는 다른 경로를 발견할 수도 있으며, 내부에서도 공격이 시도될 수도 있다. 따라서 물리적인 정보시스템 접근은 정

해진 시스템을 통해서만 가능하도록 한다.

- 또한 정보시스템은 보관된 기술정보에 침투하는 공격상태로 위치하기 이전에 악성 프로세스를 중지시켜야 한다. 이 프로세스는 시스템에서 실행 중인 것처럼 보이도록 위장되기도 하며 보이지 않게 숨겨져 있기도 한다. 어떤 악성 코드는 시스템 시작 시에 자신의 위치를 복사할 수도 있다. 따라서 최신으로 업데이트된 엔진을 가진 프로그램(백신프로그램 등)을 사용하여 악성 코드를 제거한다.

- 아울러 정보시스템 접근 로그의 변경과 저장된 산업기술정보에 추가 피해를 주지 못하도록 모든 사용자의 접근 및 외부에서의 접근을 차단하고 보안책임(관리)자 등의 승인 하에 접속하도록 하여 로그 등에 대한 증거 자료를 별도로 확보한다.

※ 정보시스템 제어권의 회복(예시)

- 정보시스템 제어권의 회복은 정보시스템이 침투되어 파괴되기 이전 상태로 복구하여 기밀성이 유지되는 운영 상태로 되돌리는 것을 의미한다.
- 정보시스템이 피해를 입었을 경우, 비밀번호 정보도 피해를 입었을 가능성이 매우 높다. 따라서 모든 비밀번호를 변경하여야 한다. 만약 조직의 내부로부터 발생한 공격이라면 사고대응팀 이외의 사용자는 접근할 수 없도록 제한해야 한다.
- 정보시스템 침투에 이용된 특정 서비스를 중지하여 임직원의 사용을 제한시켜야 한다.

2. 증거 확보 및 대응 검토

(1) 보안사고 대응 증거 확보

① 기술유출 등의 보안사고에 관련된 현장 상황 및 컴퓨터 하드디스크 등 관련 물품 또는 전자기록 등을 사고 현장을 있는 그대로 보존하

고, 사진 또는 비디오 촬영, 유출자 진술서 내지 확인서 등을 통해 증거(향후에 필요한 경우 소송에 따른 법원 등 증거제출 가능)를 신속히 확보한다. 이는 향후 기술유출 등의 보안사고에 대한 형사적 및 민사적 법적 절차를 추진하기 위해 반드시 필요하기 때문이다.

② 이러한 일차적인 보안사고 증거를 확보함에 있어서는 그 증거의 신빙성, 객관성 및 확보일자를 담보할 수 있도록 그 주체, 일시, 장소, 증거확보 경위 등을 함께 포함시킬 필요가 있다. 그리고 사고행위자가 아닌 제3자로부터 진술서나 확인서를 받는 경우에도 해당 제3자의 서명, 날인을 함께 받는다.

③ 보안사고에 대한 증거가 확보되지 않은 상태에서 섣부른 법적 조치(가처분신청 , 민사소송, 형사소송 등)는 향후 소송이나 법적 조치 등에서 어려움을 있을 수 있으므로 필요한 증거가 확보되도록 신중을 기한다.

(2) 법적 조치 사전 검토

① 경쟁업체와 관련된 산업기술 유출 등의 보안사고가 발생한 결과 해당 산업기술이 회복하기 어려울 정도로 공개되었거나 또는 이로 인하여 막대한 기술적 및 재산상 피해가 예상되거나 발생하였음에도 상대방과 상호간의 협의를 통한 합의가 이루어 지지 못하는 경우 또는 협의에 의한 합의와 관계없이 소송 등 법적 조치를 우선 검토하거나 선제적으로 조치할 수 있다.

② 이러한 사전 검토 등에 따른 법적 조치는 형사고소, 민사소송 등이 있다. 산업기술의 사용을 금지시키거나 산업기술 침해로 입은 손해배상을 법적으로 청구하기 위해서는 원칙적으로 산업기술 침해금지 가처분, 산업기술 침해금지 소송, 손해배상 청구소송 등의 민사소송을 법원에 제기하여야 한다.

③ 소송을 제기하려면 해당하는 산업기술이 유출 또는 침해되었는지를 당연히 주장하고 입증하여야 한다. 재판과정은 공개하는 것이 원칙이므로 소송을 통하여 오히려 산업기술이 공개될 가능성도 있음에 주의 한다. 민·형사를 불문하고 재판은 공개되어야 함을 원칙으로 하고 있다. 일반적으로 산업기술이 공개될 우려가 있다는 것만으로는 재판의 비공개 사유가 된다고 보기는 어려울 수도 있다. 그럼에도 산업기술보호법에 근거 소송과정에서의 당사자 간 비밀을 유지하도록 법원이 명령할 수 있는 법률적 제도가 마련되어 있다.

④ 산업기술 유출 등에 관한 소송에서는 당사자의 신청에 따라 법원이 검토하여 비밀유지명령을 발할 수 있으므로, 필요한 경우 산업기술보호법에서 정하는 사유를 소명하여 해당 소송 과정에서의 상대 당사자에 의한 유출된 기술정보의 공개 등을 방지할 수 있다.

⑤ 산업기술보호법에 따르면 제3자가 재판기록을 열람할 가능성도 있다. 소송 당사자뿐만 아니라 이해관계를 소명한 자는 소송기록의 열람·복사를 신청할 수 있다. 따라서 소장이나 준비서면 등에 산업기술을 기재하게 되는 때에는 이러한 사정을 소명하여 법원으로 하여금 소송기록의 열람·복사를 신청할 수 있는 자를 당사자로 한정하도록 하는 조치를 취하는 것도 방법이다.

(3) 당사자 간의 합의 검토

① 비록 산업기술 유출 등 보안사고가 발생하기는 하였으나 다행히 공개되거나 확산되지 않았고 또한 상대방이 이를 직접적으로 사용하지도 않아 아직 대상기관에 직접적인 피해가 발생하지 않았으며, 그리고 산업기술 유출에 따른 보안사고가 언론 등을 통하여 외부적으로 알려지지도 않았다면, 소송 등 법적 조치를 통하여 이를 해결하기 보다는 가능한 경우에는 유출행위에 관련된 당해 기업 또는 인력과 합의를 통하여 해결할 수 있다.

② 소송 등 법적 조치를 취하는 경우에 비하여 상호 합의를 통하여 문

제를 해결하는 것은 경우에 따라서 이점이 있을 수 있다. 즉, 보안사고가 발생한 기업은 산업기술 유출 등 보안사고 피해가 언론을 통해 외부적으로 알려지는 것은 예상보다 큰 이미지 손상을 초래할 수 있다, 특히 보안사고가 외부로 알려진다면 납품계약의 체결 등 현실적으로 경영상의 불이익이 초래될 수도 있다. 따라서 기업 간에 발생된다면 문제를 상호간 합의로서 해결하는 방법 등 이러한 위험을 배제할 수 있다.

③ 경쟁업체에 대해 법적 조치를 취하여 문제를 해결하는 경우 많은 비용 및 시간이 소요될 수 있을 뿐만 아니라 상대방과 적대적 관계가 지속됨으로써 앞으로 연쇄적인 법적 대응이 발생할 수 있다. 경우에 따라서는 산업기술 유출에 대한 보안사고 해결을 협의하면서 평소 사업 진행 과정에서 상대방에게 요구 할 필요가 있었던 사항을 함께 합의조건에 포함시킴으로써 산업기술 유출사고 해결에 대한 반대급부로 요구조건을 관철시킬 수도 있다.

3. 상황 분석 및 대응 조치

(1) 사고대응팀 구성

① 보안사고에 따른 조치 등을 수행하는 사고대응팀은 산업기술 유출 등의 보안사고 재발 방지를 위해서 필요최소한의 인원으로 제한하여 구성하되 보안전문가, 법률전문가, 홍보담당자를 포함하고 업무 지휘는 보안(관리)책임자 또는 경영진에서 담당한다.

※ 사고대응팀 구성 시 고려사항(예시)

- 보안사고 조사자, IT보안 전문가 및 산업보안관리사 등 보안 분야별 전문가 확보
- 기술·정보책임자 또는 경영진 및 관련 법률 전문가 등 확보
- 기관 내부에 공범이 있거나 특별한 친분관계가 있는 경우 보안이 누설되는 경우가 있으므로 최소 인원으로 한정하여 진행

· 사고행위자가 증거를 인멸 등의 행위를 중단하는 것을 막기 위해 상황 파악을 최대한 비밀리에 진행 · 사고행위자가 특정(확정)되었을 경우 조사 인터뷰 진행 후 증거 수집 절차 진행 및 정보수사기관 협조 요청

② 보안사고 상황 분석 및 대응방안 검토

- 침해 또는 유출된 기술의 형태, 기술의 규모, 기술유출의 주체 및 유출 경로 등 보안사고에 대한 상황을 파악한다. 그리고 초동조치를 통해 보안사고에 대한 상황이 파악되면 적절한 대응방안을 검토한다.

※ 상황분석 대응 방안 검토(예시) · 자체적인 상호협의에 의한 해결 · 산업기술 침해행위에 대한 금지청구권 행사 · 산업기술의 침해 신고 및 소송 또는 법적인 절차 대응 등 · 기술유출 피해 보상 등을 위한 산업기술 분쟁조정의 신청

(2) 보안사고 대응 조치 및 복구

① 기술유출 등의 보안사고는 유출된 기술자료가 어떠한 종류의 자료 형태(종이문서, 전자파일)인지를 확인하는 등 기술유출에 따른 다음과 같은 보안사고에 대한 대응조치를 취한다.

- 유출 경로를 파악하여 유사사고가 재발하지 않도록 자료 저장 및 유통경로를 차단하거나 접근통제를 강화한다.
- 인력에 기인한 자료 유출이라면 유출자를 찾아내거나 주변 임직원에 의한 유사 사고가 발생하지 않도록 주의를 기울이고 사전에 유출을 방지할 수 있도록 모니터링 체계를 만든다.
- 유출된 자료의 회수가능한지 확인하고 최대한 회수할 수 있도록 조치하고 최종적으로 회수 불가능한 경우에는 수사기관에 의뢰하여

피해를 차단할 수 있도록 한다.
- 유출된 기술자료 등이 대상기관의 경영에 미치는 영향 여부를 파악하여, 피해 범위를 최소화 하도록 한다.
- 기술자료 유출 등의 보안사고가 발생되지 않도록 기술문서·정보자료에 대한 접근 여부를 재검토하여 임직원 개인의 직무 역할에 따른 접근 제한을 제도적으로 강화한다.

② 기술유출 보안사고의 경우, 유출된 자료로 인한 피해 정도와 예상 규모를 검토하여 산정하고 복구대책을 마련 및 대응 조직을 구성하여 복구계획을 수립, 추진한다.

- 유출된 자료의 파급 영향도가 기업 외부까지 연계되는 것이라면 관련 기관 및 기업에 침해사실을 전파하고 피해를 최소화 하도록 조치한다.
- 유출된 자료의 파급 영향도가 기업 내부에만 영향을 미치는 경우에는 피해 정도에 따라 유출된 자료의 회수 노력 및 무용지물이 되도록 무효화 방안을 수립하고 조치한다.
- 유출된 자료가 외부에서 유통되는 경로를 파악하고, 회수 조치방안을 수립한다.
- 유출 경로를 추적하기 위하여 출입통제 현황 및 자료 반출입 상태를 확인하여 미흡한 부분을 보완하고 모니터링 체계를 수립한다.
- CCTV 및 출입기록을 통하여 자료 유출 시 영상증거나 출입기록 등의 증적자료 확보가 되도록 수정 보완하고 모니터링 한다.
- 개인 물품의 반출입 상태 및 점검시의 미흡한 점을 수정 보완하도록 한다.
- 물리적 출입 권한을 강화하고 이력을 상시 확인하고 점검할 수 있도록 보안을 강화한다.

③ 정보침해 등에 의한 보안사고 복구는 원상태로 시스템을 되돌리고 사고로 인해 야기된 손상을 제거하여 가용성을 회복시키고 정확한 정보로 복원하는 과정이다. 손상된 시스템을 복구하는 것은 정상적

인 작동으로 되돌아가는 것을 의미한다.

④ 복구 우선순위의 설정에는, 대부분의 환경에서 가용성보다 정보의 정확성이 더 중요하게 간주되지만 어떤 환경에서는 정확성보다 가용성이 더 중요한 경우도 있다. 업무 요소에 따라 중요도의 순서가 결정되어야 한다. 사고 복구에서는 손실의 최소화가 중요하므로 빠른 탐지와 복구에 기초를 두어 사고의 규모를 제한해야 한다.

- 우선순위의 적절한 결정을 위해 사용할 수 없는 시스템과 보호되지 않을 때 이용될 수 있는 서비스의 위협에 대한 비용을 이해하고 있어야 한다. 업무 우선순위와 계약 및 법적 요건에 기초하여 시스템의 복구에 필요한 비용과 시간 요구사항을 파악한다.

⑤ 외부의 공격자 등에 의한 기술정보 침해 등 보안사고에 따른 정보시스템이나 서비스를 가능한 신속하게 복구하기 위한 비상복구 절차를 수립해야 하며 다음과 같은 사항을 포함한다.

- 시스템별 복구절차 및 방법
- 복구 범위 및 담당자
- 원인분석을 위한 증거자료 수집방법
- 시스템 및 네트워크에 대한 취약점 제거 등 사후관리
- 재발방지를 위한 방안 및 기타 복구에 필요한 사항

⑥ 정보시스템 관리자는 복구 우선순위에 의한 정보자원을 분류하는 논리적인 기구를 구축하고 이용한다. 이 기구에서는 가장 위급한 정보자원부터 우선 복구순위를 부여한다. 그리고 중요한 통신시스템이 홍수 또는 화재와 같은 재난으로부터 손실을 발생할 경우에 대비하여 재난복구계획을 준비하고 정기적으로 갱신 및 시험한다.

⑦ 정보보안대책의 실행에도 불구하고 정보보안사고가 발생하였다면 이 보안대책은 개선되어야 한다. 하나의 취약성이 제거되면 다른

유사한 취약성도 제거되어야 한다. 정보보안대책의 실행은 아직 보고되지 않은 유사한 취약성에 기초한 사고를 방지하는데 도움이 된다. 정보보안대책의 개선은 기존 보안대책의 변경이나 새로운 보안대책의 추가를 포함한다. 정보보안 개선대책은 기술적이거나 절차적인 개선이 될 수 있다.

⑧ 정보시스템의 취약성은 사고대응팀 또는 시스템 공급자의 보고에 의해 발견되고 제거되거나 관리될 수 있다. 대부분의 공격은 알려진 취약점을 이용하므로 모든 시스템은 충분히 신뢰할 수 있는 공급자로부터 최신의 패치를 받아서 적용하여야 한다. 침해·침투 등 보안취약성을 이용한 보안 사고를 당한 경우에는 해당 시스템의 보안취약성을 보고하고 재발방지를 위해 관리목록에 추가한다.

※ 정보시스템 취약성 관리 방법(예시)

- 패치 적용: 패치(patch)는 특정 취약성을 보완하기 위한 소프트웨어의 일부이다. 패치는 빠른 테스트와 적용을 위해 사용된다. 패치 적용은 매우 특정한 보안 이슈에 초점을 맞추고 있어서 다른 관련 취약성이나 관련 소프트웨어 시스템에 포함된 취약성을 처리하기는 어렵다.
- 서비스 보완: 취약성이 보완된 서비스는 취약성을 이용한 침투을 제거할 수 있다. 또한 서비스에 필요 없는 소프트웨어를 시스템에서 제거할 수도 있다.
- 절차 변경: 절차의 변경으로 취약성을 제거하는데 이용할 수 있다. 보안과 연관된 기술, 업무 상태, 법률 등을 검토하고 변경하는 것이 여기에 해당한다.

⑨ 모든 보안대책과 복구의 우선순위 설정은 보안사고로부터 얻은 정보를 기초로 재검토되어야 한다. 새로운 보안 취약성이 발견되거나 새로운 서비스가 추가되면 보안대책의 설정을 유지하기 위해 추가적인 보안절차의 검토가 필요한지 판단한다. 또한 예상치 못한 곳에 보안대책을 추가해야 할 필요성이 있는지 평가해야 한다.

4. 재발 방지 조치

(1) 보안사고 분석 및 대응 조치 문서화

① 보안사고 분석은 대응과정을 개선하는 데 필요하며, 다음과 같은 문제(예시)에 답변해야 한다.

※ 보안사고 분석 사항(예시)
· 정확하게 언제 무엇이 발생되었는가? · 임직원은 얼마나 잘 대응하였는가? · 임직원에게 필요한 정보는 무엇이었으며, 얼마나 신속하게 얻을 수 있었는가? · 다음 사건에는 어떤 것이 달라져야 하는가?

② 분석 과정에서는 보안사고에서 수집된 모든 정보와 이벤트를 발생 순서대로 정리해야 한다. 손해에 대한 예상비용 산정은 사고에 영향을 받은 모든 정보자원에 대해 판단해야 한다. 사고의 결과로 발생한 민형사상의 책임을 요구해야 할 수도 있기 때문이다.

③ 보안사고의 후속 처리과정에서 가장 중요한 사항은 사고처리를 기록하는 과정이다. 이러한 기록은 사고대응팀 등이 관리자와 같은 특정 대상에게 보고하는 보안사고의 문서화 과정라고 할 수 있다.

- 후속처리 보고서에 포함될 대부분의 정보는 시간대별 상황 문서로 이미 수집되어 있어야 한다(시간대별 상황 문서화).
- 기술적 요약서는 처리과정을 향상시키고 최선의 대응을 위한 기초가 된다. 이 문서는 조직 내에 있는 다른 기술적 그룹과 공유할 수도 있고, 조직 구성원의 보안인식을 향상시킬 수도 있다.
- 관리적 요약서는 사고의 범위와 크기, 영향을 이해하기 위해 필요한 내부적인 관점을 제공한다(관리적 요약 문서화).

- 보안사고는 사고를 관리하기 위해 준비된 절차를 테스트하는 기능도 한다. 사고가 수습될 때가 관리과정을 재검토하고 대책을 보완하는 시기이다(사고평가 과정 문서화).
- 위험 분석은 위험 식별과 위험 평가를 포함하기 때문에 어떤 요소가 손실에 많이 영향을 미치고 관리과정에서 중요한지 결정할 수 있도록 해준다. 이러한 추정은 손실이 발생되기 전까지는 검증이 어렵다. 따라서 추정이 현실적인지 검토한다(위험 분석) .
- 업무영향 분석은 보안사고가 조직에서 차지하는 재정적 영향을 판단하는 것이다. 예를 들어, 성수기의 제품 판매수익 등을 기초로 할 수 있다. 또한 정해진 복구 전략을 수행하는데 필요한 추정비용과 관련비용을 포함시킨다. 추정비용과 실제 손실비용을 비교하면 추후 업무영향을 예측하고 개선하는데 도움이 된다(업무영향 분석).

(2) 법적 대응 및 조치 검토

① 보안사고는 여러 가지 법률적 사항을 포함하고 있다. 보안사고를 처리하는 과정에서 초기에 조직의 법률 관련부서나 관계자에게 사실을 알리고 법적으로 파생될 문제를 고려해야 효율적인 사고처리가 될 수 있다.

② 법률 자문가는 향후 법적 조치에 필요한 문서의 형태를 제공할 수 있어야 한다. 법적 조치는 형사소송과 민사소송으로 구분된다. 형사소송의 경우에는 시스템을 사고이전으로 복구하는데 소요되는 시간과 노력이 손해배상을 산정하고, 벌칙을 판단하는 중요한 요소가 된다. 민사소송의 경우에는 손해를 배상받을 수 있도록 손해를 항목화 및 정량화시켜야 한다. 특정한 피해에 대해서는 법적 소송제기가 향후 유사한 사고를 예방하는데 효과적일 수 있다.

③ 보안사고에 사용된 방법이 일반에게 잘 알려져 있는 경우에는 소송제기가 효과가 있다. 법적 소송은 잠재적인 공격자가 유사 행위로 인해 다른 공격자가 이전에 발생한 소송사건에 대한 법률적 범위를

설정하는데도 도움이 된다. 하지만 대부분의 경우에 법적 소송은 시간, 인력, 비용 문제가 발생하므로 심사숙고해야 한다. 이러한 문제에 대한 이해를 돕기 위해 경영관리 시스템 관리자나 시스템 보안 관리자 및 해당·관련분야의 법률전문가 등과 협의한다.

5. 보안사고 대응 및 복구 훈련

① 사고의 대응 및 복구 계획은 보안사고 예방계획, 사고조치계획, 사고복구계획 등으로 구분한다. 훈련방법에 따른 결과를 토대로 사고의 대응 및 복구훈련을 수정하여 피해를 줄이는 것이 목적이다.

② 유출 및 침해 등 보안사고 예방계획에는 평소 산업기술의 유출 및 침해를 막기 위하여 지켜야할 사항들이 포함되어야 하며 모든 임·직원은 보안사고 예방계획이 잘 지켜질 수 있도록 각자 수시로 확인하도록 한다. 다음으로, 사고조치계획에는 산업기술이 유출 및 침해되었을 경우를 예상하여 부서 및 인력별로 조치해야 할 사항들을 미리 규정해 두고, 사고가 발생할 경우 해당 조치계획에 따라 신속히 대응함으로써 빠른 시간 내에 처리가 가능하도록 한다. 끝으로, 복구계획은 조치 중 복구와 관련된 내용을 미리 규정해 둠으로써 업무의 정상화를 위해 우선적으로 노력해야 할 사항들을 확인할 수 있도록 한다.

③ 사고의 대응 및 복구훈련은 산업기술의 유출방지 및 보호 세부규정을 보다 현실적으로 정하는데 도움을 주는 기능을 제공함과 동시에 차후 침해사고가 발생할 시에 시의적절하고 정확한 대응을 할 수 있도록 도와준다.

④ 보안사고 대응 및 복구는 훈련을 통해 피해를 최소화하도록 한다. 훈련방법에는 Table-top 훈련, Drill 훈련, Exercise 훈련 등이 있다.

- (Table-top 훈련) 대표자 포함 경영진만 참여하여 메시지 위주로 시

행하는 메시지 훈련이다. 부여된 메시지에 대한 조치를 구두 혹은 문서로 시행하며 조치에 따른 영향도 산정하여 메시지로 부여한다.
- (Drill 훈련) 메시지를 이용해 하는 점은 Table-top 훈련과 비슷하나 추가로 모형을 이용하는 것이 특징이다. “Drill”의 일반적인 의미는 연습과 동일한 개념으로 사용되기도 한다.
- (Exercise 훈련) 말 그대로 실제 행동으로 조치하는 훈련이다. 산업기술의 유출 및 침해상황을 최대한 생동감 있게 묘사하고 실제 행동으로 훈련한다.
- (보안사고 대응) 복구훈련을 마친 후에는 훈련의 결과를 토대로 사고의 대응 및 복구계획을 수정하여 가장 피해가 적도록 준비한다.

제2절 산업기술 유출·침해 구제 조치

1. 산업기술 유출 및 침해 신고

① 국가핵심기술 및 국가연구개발사업으로 개발한 산업기술을 보유한 기관은 산업기술 유출 또는 침해행위가 발생할 우려가 있거나 발생한 때에는 산업통상자원부와 및 정보수사기관에 신고한다.

② 산업기술의 유출 또는 침해신고를 하거나 이에 필요한 조치를 요청하고자 하는 경우에는 산업기술침해신고서(「산업기술보호법」 시행규칙 별지 제7호 서식 참조)를 산업통상자원부 및 정보수사기관에 제출한다.

③ 긴급히 산업기술의 유출 또는 침해신고를 하여야 하는 경우에는 구두 또는 정보통신망 등의 방법으로 이용하여 요청한 후 즉시 산업기술침해신고서를 산업통상자원부 및 정보수사기관에 제출한다.

④ 산업기술 보유 대상기관은 산업기술 침해행위가 발생할 우려가 있거나 발생한 사실을 반드시 신고해야 하는 의무가 있다.

2. 산업기술 유출·침해에 대한 법적 조치

(1) 산업기술 침해행위 금지 청구

① 산업기술보호법 제14조의2(산업기술 침해행위에 대한 금지청구권 등)는 국가핵심기술을 포함한 산업기술 침해행위를 하거나 하려는 자에 대하여 영업상의 이익이 침해되거나 침해될 우려가 있는 경우에는 법원에 그 행위의 금지 또는 예방을 청구할 수 있다. 다만 실무적으로는 금지청구와 예방청구는 엄격히 구분되고 있지는 않고 현실적으로 산업기술의 침해행위가 있지 않더라도 침해 우려가 있다면 금지 청구는 가능하다.

② 침해행위를 조성한 물건의 폐기, 침해행위에 제공된 설비의 제거, 부정취득·사용·공개 행위의 중지, 완성제품의 배포·판매 중지, 침해행위의 금지 또는 예방을 위하여 필요한 조치 등이다.

③ 산업기술 보유기관은 침해금지 예방청구권을 행사할 때에 침해행위를 조성한 물건의 폐기, 침해행위에 제공된 설비의 제거, 그 밖에 침해행위의 금지 또는 예방을 위하여 필요한 조치를 함께 청구할 수 있다. '침해행위를 조성한 물건'이란 침해행위에 필연적인 물건, 즉 그 물건의 존재 없이는 산업기술이 침해되지 아니하는 것과 같은 물건(예시, 제품의 제조 노하우인 경우는 설계도면, 기술사양서, 제조·생산 절차서, 원재료 사용 분석평가서 및 시방서 등)이라고 할 수 있다.

④ 대상기관의 장은 침해행위를 조성한 물건의 폐기, 침해행위에 제공된 설비의 제거, 그 밖에 침해행위의 금지 또는 예방을 위하여 필요한 조치를 함께 청구한다.

⑤ 침해행위자를 확인한 날부터 3년 이내 행사하지 아니하거나, 그 침해행위가 시작된 날부터 10년이 지나면 시효의 완성으로 예방·금지

청구권은 소멸되므로 대상기관의 장은 이를 유의한다.

(2) 손해배상 청구

① 고의 또는 과실에 의한 산업기술 침해행위로 산업기술 보유자의 영업상 이익을 침해하여 손해를 입힌 자는 그 손해를 배상할 책임을 진다. 손해배상청구는 산업기술 침해행위의 금지청구권과는 별도로 이미 침해된 부분에 대하여 금전을 통한 원상회복을 구하는 청구라고 할 수 있다.

② 원칙적으로 손해배상을 청구하기 위해서는 산업기술의 침해행위가 있고 손해의 발생이 있으며, 침해행위와 손해 발생 사이에 인과관계가 있다는 사실 및 손해발생액을 산업기술의 보유기관이 주장·입증하여야 한다.

③ 산업기술보호법은 법원이 재량으로 상당한 손해액을 인정할 수 있음을 규정하고 있다. 즉, 법원은 손해가 발생된 것은 인정되나 그 손해액을 입증하기 위하여 필요한 사실을 입증하는 것이 해당 사실의 성질상 극히 곤란한 경우에는 변론 취지와 증거조사의 결과에 기초하여 상당한 손해액을 인정할 수 있다.

④ 또한 산업기술 침해행위가 고의적인 것으로 인정되는 경우에는 법원은 산업기술보호법에 규정된 사항을 고려하여 손해인정 금액의 3배 범위 내에서 징벌적인 손해 배상액을 명령할 수 있다.

(3) 산업기술 침해 이유 경업금지 청구

① 산업기술 침해 관련 분쟁은 기업에서 산업기술을 취급한 임직원이 경쟁기업 등으로 전직(轉職)하거나, 스스로 경쟁 기업을 운영하는 경우(競業)에 그러한 행위의 금지를 청구하는 형태로 자주 일어난다. 그런데 경업금지 청구는 기업의 산업기술 보호와 근로자의 직업선택의 자유가 충돌하는 국면이라는 점에서 산업스파이에 의한

산업기술 침해와는 다른 문제가 발생한다고 볼 수 있다.

② 산업기술을 취급하던 임직원이 이를 경쟁기업에서 사용하는 것이 산업기술의 침해행위가 되기 위해서는 근로자에게 퇴직 후에도 그 정보를 비밀로 유지 할 의무가 있어야 한다. 퇴직 후에도 비밀을 유지한다는 내용의 명시적인 약정이 없는 경우에도, 판례는 인적 신뢰관계의 특성 등에 비추어 신의칙상 또는 묵시적으로 그러한 의무를 부담하기로 약정하였다고 보아야 할 경우에는 일정기간 비밀유지 의무가 인정된다는 태도이다.

(4) 경업금지약정 근거 전직금지 청구

① 산업기술을 전제로 하지 않고 임직원과의 사이에 체결한 경업금지 약정을 근거로 경쟁기업으로의 취업을 금지하는 내용의 청구를 하는 경우도 있다. 이 경우 법리적으로 산업기술의 침해 금지에 필요한 조치의 하나로서 사용자가 보유한 산업기술 정보를 보호하기 위하여 근로자의 직업선택의 자유를 제한한다는 측면에서 법리적으로 유사한 측면이 있고, 실제로 사용자가 근로자와의 관계에서 비밀유지 약정과 경업금지 약정을 동시에 체결하는 경우도 많다.

② 그러나 판례는 산업기술보호법이 아니라 경업금지약정을 근거로 경업금지를 청구하는 경우에는 그러한 약정의 효력은 합리성이 인정되는 범위'내에서만 인정하는 경향이 있다.

(5) 산업기술보호법에 따른 제도적 구제 수단

① 산업기술보호법 제14조(산업기술의 유출 및 침해행위 금지)은 국가핵심기술을 포함한 산업기술의 국내외 유출 및 침해행위를 형사적으로 처벌하는 규정을 두고 있다. 이러한 형사절차는 산업기술 보유자가 국가정보원, 경찰, 검찰 등 정보수사기관에게 조사, 고소 또는 고발을 제기함으로써 시작되는 것이 일반적이다.

② 산업기술보호법은 산업통상자원부장관 소속 하에 산업기술분쟁조정위원회(사무국은 산업기술보호협회에 설치)를 두고 당사자의 신청에 의해 산업기술의 유출과 관련한 분쟁을 조정하여 처리할 수 있도록 하고 있다. 분정조정의 처리는 산업기술분쟁조정위원회가 작성하여 제시한 조정안을 당사자들이 수락이 필요하다.

3. 산업기술 분쟁조정 신청 및 처리

① 산업기술보호법에 따른 산업기술 유출과 관련한 분쟁의 조정을 원하는 경우에는 신청취지와 원인을 기재한 조정신청서를 산업기술분쟁조정위원회(이하 “조정위원회”라 한다)에 제출하여 분쟁의 조정을 신청한다.

② 산업기술의 유출에 관한 다툼이 있을 경우, 법원이나 심판을 통해서 해결하는데 소요되는 비용과 시간 등의 문제를 절약할 수 있도록 산업통상자원부가 설치한 조정위원회에서 당사자를 분쟁해결절차에 직접 참가시켜 상호간의 합의를 유도해 내는 제도이다.

③ 대상기관의 장은 산업기술 유출과 관련한 분쟁의 조정을 원하는 경우에는 신청취지와 원인을 기재한 조정신청서를 조정위원회에 제출하여 분쟁조정을 신청한다.

- 신청대상: 산업기술의 유출, 침해 등에 관한 분쟁이다.
- 분생조정을 신청하는 경우, 조정위원회는 전담 조정부를 구성하여 상호간의 합의를 통한 분쟁해결을 유도할 수 있다.

4. 상호 협의에 의한 처리

① 산업기술이 유출만 되고 아직 공개 또는 사용되지 않은 상태라고 확인되면 이를 회수하고 공개하지 않는다는 각서를 받는 등 상호

협의를 통해 원만하게 해결할 수 있다.

② 산업기술 보유기관 등도 대외적인 이미지 손상을 받지 않고 침해자도 침해사실이 공개되지 않아 윤리적·도덕적으로 비난을 면할 수 있으며 상호 협의 하에 영업 비밀을 반환받아 계속 비밀로 유지할 수 있으므로 적극적으로 시도하여야 할 대응책이다. 이는 상호 협의 하에 원만하게 해결하는 것으로 바람직하다.

③ 산업보안 책임자(담당자) 및 경영진은 핵심기술이 유출만 되고 아직 공개 또는 사용되지 않은 상태라면 산업기술 및 영업비밀 유출자와 접속하여 사건 정황을 파악한다.

④ 사건 정황을 파악하고 유출된 산업기술 등이 향후 공개될 염려가 없다면 이를 회수하고 상호협의로 사고를 해결할 수 있다.

⑤ 보안책임자(담당자)는 향후 사고 재발 방지를 위하여 협의내용을 산업기술 및 영업비밀 유출에 관한 보고서를 작성하여 보고한다.

제3장 산업기술 계약 시 유출 방지 및 보호 조치

제1절 인수·합병 또는 합작투자 계약

1. 인수·합병 또는 합작투자 시 비밀유지 전략 수립

① 다른 기업과의 인수·합병 또는 합작투자 등으로 인해 중요한 산업기술의 유출이 빈번하게 발생한다.

② 특히 인수·합병의 경우 인수·합병 대상 기업에 대한 실사 등 인수·합병 대상자를 탐색하는 단계를 거치는 것이 통상적이고, 이 과정에서 인수·합병 대상 기업이 보유한 산업기술의 유출이 빈번하게 발생한다. 따라서 실사 전 단계에서 비밀유지계약을 별도로 체결하거나 의향서(LOI, Letter of intent)나 양해각서(MOU, Memorandum of understanding) 체결 시 비밀유지의무를 부과하는 조항을 두어 산업기술의 유출을 방지할 필요가 있다.

> ※ 의향서나 양해각서 내 비밀유지의무 부과 조항 (예시)
>
> - (제O조) 양 당사자는 양 당사자 사이 주고 받은 비밀 정보를 비밀로 유지하기 위하여 취급자로부터 비밀유지서약서를 징구하는 등 합리적인 관리를 하여야 한다.
> - (제O조) 양 당사자는 본 의향서(또는 양해각서)를 체결한 목적 외의 용도로 비밀 정보를 사용하지 않기로 한다.
> - (제O조) 양 당사자는 양 당사자 사이 주고받은 비밀 정보를 제3자 또는 관련 없는 직원에게 공개하거나 누설하여서는 아니 된다.

③ 인수·합병 대상 기업이 중요한 산업기술을 보유한 경우 다음과 같은 점을 고려하여 기술이전에 따른 피해 최소화 및 비밀유지 전략을 수립한다.

- 특별전략팀을 구성하는 등 전략 수립과 관련된 담당자를 선임하여 책임 소재를 명확히 한다.
- 상대방 기업 탐색 및 협상, MOU 체결, 실사 및 평가, 기술이전 계약 체결, 기술 이전 이후의 각 단계별로 산업기술 유출 방지와 유출 및 침해 발생 시 조치방법을 구체적으로 수립한다.
- 계약 당사자 및 근로자, 중개기관 등 기술이전과 관련된 모든 관련자들에 대한 비밀유지 의무를 부과하는 전략을 수립한다. 특히 비밀유지의무를 부과할 때 계약 당사자 뿐만 아니라 담당자 등 기술의 내용을 알 수 있는 근로자, 인수·합병 중개기관이 개입되어 있는 경우 중개기관에게도 비밀유지의무를 부과하여야 한다는 점에 유의하여야 한다.

2. 인수·합병 또는 합작투자 기업 보안체계 점검

① 인수·합병 또는 합작투자 등을 본격적으로 진행하기에 앞서 상대방 기업이 비밀유지 의무를 이행할 능력이 있는지 여부를 확인한다. 산업기술의 유출은 악의적으로 발생시키는 경우뿐 만 아니라, 산업기술의 보호역량이 부족하여 발생되는 경우도 있다. 따라서 상대방 기업의 비밀유지의사 및 비밀유지 능력 등 보안체계를 종합적으로 점검한다.

② 사전적으로 상대방 기업에서 산업기술이 유출된 적이 있는지 또는 상대방 기업이 다른 기업의 산업기술을 무단 사용하였거나 비밀유지 계약을 불이행한 사례가 있었는지 등을 검색한다.

③ 아래와 같은 사항을 고려하여 상대방 기업의 비밀유지의무 이행 능력이 있는지 여부를 평가한다.

- 보유 자산의 분류와 통제를 적절히 하고 있는가.
- 산업기술 보호에 적합한 보안규정이 마련되어 유지, 관리되고 이행되고 있는가.
- 산업기술을 보호할 수 있는 조직이 구성되어 있는가.
- 산업기술을 취급하는 기술 인력을 포함한 임직원에게 비밀유지의무를 부과하고, 보안관련 교육을 실시하고 있는가.
- 중요 산업기술을 보호하기 위한 침입 방지 대책은 적절한가.
- 정보시스템은 산업기술 보호에 맞게 설정되고 관리되고 있는가.
- 사고 발생 시 대응 및 복구 대책은 마련되어 있는가.

④ 상대방 기업의 보안체계 등 산업기술 유출 방지 및 보호 조치가 미흡한 경우 부족한 점과 보완사항을 상대방 기업에게 통보하여 일정 기간 내에 그에 맞는 조치를 취하도록 하고 사후에 보완이 이루어진 경우에만 상대방 기업과 계약을 체결한다.

3. 의향서(LOI) 및 양해각서(MOU) 작성

① 인수·합병 또는 합작투자 등에 관한 본 계약을 체결하기 이전에 상대방 기업과 의향서(LOI), 양해각서(MOU) 등을 작성하는 것이 보통이다. 본 계약 체결 전 산업기술이 상대방 기업으로 유출되거나 상대방 기업을 통해 유출되는 일이 없도록 한다.

② 의향서(LOI), 양해각서(MOU)는 법적인 구속력을 받지 않도록 작성되는 것이 통상이므로, 비밀유지의무에 관하여 상대방 기업에게 법적인 구속력을 받도록 하려면 이와 관련된 조항을 규정할 필요가 있다.

③ 의향서(LOI) 및 양해각서(MOU) 등에 다음의 내용을 포함시킬 필요가 있다.

- 실사를 위해 필요한 경우를 제외하고 상대방 기업에게 산업기술과 관련된 정보의 제공을 요구하지 않는다.
- 산업기술을 제공받았다고 하더라도 상대방 기업의 사전 서면 동의 없이 제3자에게 누설, 공개하거나 임의로 이용하지 않는다.
- 비밀유지의무 부과와 관련된 규정은 법적인 구속력을 갖는다.

※ 의향서나 양해각서 내 포함시켜야 하는 조항 (예시)

- (제O조) 양 당사자는 양 당사자 사이 주고 받은 비밀 정보를 비밀로 유지하기 위하여 취급자로부터 비밀유지서약서를 징구하는 등 합리적인 관리를 하여야 한다.
- (제O조) 양 당사자는 본 의향서(또는 양해각서)를 체결한 목적 외의 용도로 비밀 정보를 사용하지 않기로 하며, 위 목적 이상의 정보 제공을 요구하지 못한다.
- (제O조) 양 당사자는 양 당사자 사이 주고받은 비밀 정보를 제3자 또는 관련 없는 직원에게 공개하거나 누설하여서는 아니 된다.
- (제O조) 위의 제O조, 제O조는 법적 구속력을 갖는다.

4. 인수·합병 또는 합작투자 등에 관한 계약서 작성

① 계약서는 계약이 성립되었음을 증명하는 서류로서 사후적인 문제 발생 시 중요한 증거가 된다. 따라서 계약서에는 산업기술 유출에 대비하기 위한 조항을 반드시 포함한다.

② 본 계약서에 산업기술에 관한 자료의 보존방법, 접근 및 이용제한, 제3자에 대한 누설, 공개, 제공 등 금지에 관한 조항을 규정한다.

③ 근로자 등 개인이 산업기술 등을 유출한 경우 상대방 기업이 연대 책임을 질 수 있다는 문구를 명시한다.

※ 인수·합병 또는 합작투자 등에 관한 계약서 내 산업기술 유출방지를 위해 필요한 조항 (예시)

- (제O조) 양 당사자는 양 당사자 사이 주고 받은 비밀 정보를 비밀로 유지하기 위하여 취급자로부터 비밀유지서약서를 징구하고, 취급자 외의 자의 접근 및 이용을 제한하는 등 합리적인 관리를 하여야 한다.
- (제O조) 양 당사자는 본 의향서(또는 양해각서)를 체결한 목적 외의 용도로 비밀 정보를 사용하지 않기로 한다.
- (제O조) 양 당사자는 양 당사자 사이 주고받은 비밀 정보를 제3자 또는 관련 없는 직원에게 공개하거나 누설하여서는 아니 된다.
- (제O조) 양 당사자는 비밀정보를 취급하는 직원이 상대방 당사자의 산업기술 등을 유출한 경우 산업기술 등을 유출한 당사자는 산업기술 등을 유출 당한 당사자에게 발생한 손해에 대하여 직원과 연대하여 책임을 부담한다.

5. 인수·합병 또는 합작투자 후 존속기업의 보호조치

① 인수·합병 후 존속하는 회사 또는 합작투자로 신설된 회사는 산업기술의 보호를 위해 다음 각 호의 기술보호 조치를 한다.

- 산업기술에 대한 보호 등급의 부여와 보안관리 규정의 제정
- 산업기술 관리책임자와 보호구역의 지정
- 산업기술 보호구역의 통신시설과 통신수단에 대한 보안
- 산업기술 관련 정보의 처리 과정과 결과에 관한 자료의 보호
- 산업기술의 연구개발 인력에 대한 비밀유지의무 부과 및 보안교육 실시
- 산업기술의 유출 사고에 대한 대응체제 구축

② 인수·합병 후 존속하는 회사 또는 합작투자로 신설된 회사는 주기적으로 산업기술의 보호조치가 적절한지 평가하고 미비점을 보완한다.

제2절 기술 라이선스 계약

1. 기술 라이선스 계약 비밀유지 전략 수립

① 기술 라이선스 계약은 기술제공자가 상대방인 기술 도입자에게 특정기술에 대하여 실시권을 허락하는 기술대여형 계약으로서, 기업은 라이선스 계약을 통해 제품이나 기술을 독자적으로 개발하지 않고도 동일한 제품이나 기술을 획득할 수 있다. 이러한 라이선스 계약에서는 계약 전반에 걸쳐 기술 자체가 이전되어 버리는 결과가 발생할 수 있으므로, 산업기술의 유출에 유의한다.

② 이에 기술 라이선스 계약 체결 전, 산업기술 유출을 방지하기 위하여 다음의 내용을 고려한다.

- 기술 라이선스 계약의 체결 전에 산업기술의 유출이 우려되는 상황을 파악하여, 상대기업으로의 기술이전에 따른 영향 및 상대국의 지식재산권 보호 상황 등을 파악한다.
- 위의 내용을 통하여 파악한 사항을 고려하여 기술이전 여부를 결정한다.
- 기술이전하기로 결정한 경우 산업기술 이전에 따른 피해 최소화 및

비밀유지를 위한 전략을 구체적으로 수립한다.

2. 기술 라이선스 계약 기업의 보안체계 점검

① 라이선스 계약을 체결할 때 기술을 이전하기에 앞서 상대방 기업이 비밀유지의무를 이행할 능력이 있는지 여부를 확인하며 산업기술의 유출방지 및 보호를 위한 충분한 조치를 취하기 전까지 계약에 따라 기술을 이전하여서는 아니 된다.

② 라이선스 계약 시 산업기술의 유출은 어느 일방의 대상기관이 악의적으로 발생시키는 경우뿐 만 아니라, 산업기술의 보호 능력이 부족하여 발생되는 경우도 있기 때문에, 대상기관은 상대방 기업의 비밀유지 의사 및 비밀유지 능력을 철저히 평가해야 한다.

③ 라이선스 계약을 체결할 때 대상기관의 장은 사전적으로 상대방 기업에서 산업기술이 유출된 적이 있는지 또는 상대방 기업이 다른 기업의 산업기술을 무단 사용하였거나 비밀유지 계약을 불이행한 사례가 있었는지 등을 검색한다.

④ 대상기관의 장은 아래와 같은 사항을 고려하여 상대방 기업의 비밀유지의무 이행 능력이 있는지 여부를 평가한다.

- 보유 자산의 분류와 통제를 적절히 하고 있는가.
- 산업기술 보호에 적합한 세부규정이 마련되어 유지·관리 및 이행되고 있는가.
- 비밀유지의무를 부과하고 교육을 실시하는 등 산업기술 보호를 위한 인력관리는 철저한가.
- 중요 산업기술을 보호하기 위한 침입 방지 대책은 적절한가.
- 정보시스템은 산업기술 보호에 맞게 설정되고 관리되고 있는가.
- 사고 발생 시 대응 및 복구 대책은 마련되어 있는가.

⑤ 상대방 기업의 보안체계 등 산업기술 유출 방지 및 보호 조치가 미흡한 경우 대상기관의 장은 부족한 점과 보완사항을 상대방 기업에게 통보하여 일정 기간 내에 수정 조치하도록 하고, 보완이 이루어진 경우에만 상대방 기업과 산업기술 계약을 체결한다.

3. 기술 라이선스 계약서 작성

① 계약서는 계약이 성립되었음을 증명하는 서류로서, 사후적인 문제 발생 시 중요한 증거가 된다. 따라서 계약서에는 산업기술 유출에 대비하기 위한 조항뿐 만 아니라 문제 발생 시의 조치에 대한 조항 등도 포함한다.

② 기술 라이선스 계약서에 다음 각 호의 사항을 명시한다.

- 대상 기술 및 노하우의 범위, 대상지역 특정
- 기술이전을 위한 지도방법
- 서브 라이선스(재실시 허락) 금지
- 제3자에 대한 누설, 공개, 목적 외 이용 금지
- 계약 종료 후 비밀유지 및 관련 물품과 설비의 반환
- 개량기술 성과의 귀속(개량발명 범위, 보고, 권리귀속 형태 등)
- 비밀유지의무의 존속기간
- 계약의 유효기간,계약의 변경·해지·종료
- 계약 위반에 대한 벌칙
- 계약 위반으로 인하여 발생한 손해의 배상

제3절 기술 위・수탁 계약

1. 위·수탁 계약 비밀 유지 전략 수립

① 위・수탁 계약은 하청위탁자가 하청수탁자에게 특정기술을 제공하고 상대방에게 자기의 기관으로서 당해기술을 실시하게 하는 계약

으로서 하청 라이선스 계약이라고도 한다. 위·수탁 계약은 수탁자가 위탁자에 비하여 기술수준이 낮은 경우가 대부분이므로 위탁자의 기술지도가 필요하다. 따라서 기술수준이 낮은 수탁자의 입장에서는 생산공정, 제조설비, 기술지도 등 전 범위에 걸쳐 기술유출을 할 유인이 높으므로 전략적인 대응이 요구된다.

② 위·수탁 계약을 체결함으로써 중요한 산업기술이 수탁기업으로 유출될 우려가 있는 경우에는 설비의 이전이나 생산공정 관여 또는 기술지도 등 생산기술의 이전에 따른 피해 최소화 및 비밀유지를 위한 전략을 수립한다.

③ 다음의 내용에 유의하여 위·수탁 계약 비밀 유지 전략을 수립한다.

- 위·수탁 계약을 체결하는 경우 기술집약적 공정과 노동집약적 공정을 구분한다.
- 기술집약적 공정은 국내 혹은 지식재산권 보호가 가능한 국가에 두고 노동집약적 공정 해외에 두고 생산에 필요한 것만을 해외에 이전하는 내용이 계약서에 포함되어 있는지 검토한다.
- 위·수탁 계약과 관련된 생산기술의 이전에 따른 피해 최소화 및 비밀유지를 위한 전략을 수립한다.

2. 수탁기업의 보안체계 점검

① 위·수탁 계약에 따라 설비의 이전이나 생산공정 관여 또는 기술지도 등을 하기에 앞서 수탁기업이 비밀유지의무의 이행 능력이 있는지의 여부를 확인한다.

② 위·수탁 계약 시 산업기술의 유출은 수탁기관이 악의적으로 발생시키는 경우뿐만 아니라, 수탁기관의 산업기술 보호 능력이 부족하여 발생되는 경우도 있기 때문에, 수탁기업의 비밀유지 의사 및 비밀유지 능력을 종합적으로 평가한다.

- 라이선스 계약을 체결할 때 사전적으로 수탁기업에서 산업기술이 유출된 적이 있는지 또는 수탁기업이 다른 기업의 산업기술을 무단 사용하였거나 비밀유지 계약을 불이행한 사례가 있었는지 등을 조사한다.

- 아래와 같은 사항을 고려하여 수탁기업의 비밀유지의무 이행 능력이 있는지 여부를 평가한다.

※ 비밀유지의무 이행 능력 여부 Check lists (예시)

- 보유 자산의 분류와 통제를 적절히 하고 있는가?
- 산업기술 보호에 적합한 세부규정이 마련되어 유지, 관리되고 이행되고 있는가?
- 산업기술을 보호할 수 있는 조직이 구성되어 있는가?
- 산업기술을 취급하는 근로자들에게 비밀유지의무를 부과하고, 관련 교육을 실시하고 있는가?
- 중요 산업기술을 보호하기 위한 침입 방지 대책은 적절한가?
- 정보시스템은 산업기술 보호에 맞게 설정되고 관리되고 있는가?
- 사고 발생 시 대응 및 복구 대책은 마련되어 있는가?

③ 수탁기업의 보안체계 등 산업기술 유출 방지 및 보호 조치가 미흡한 경우 부족한 점과 보완사항을 상대방 기업에게 통보하여 일정 기간 내에 그에 맞는 조치를 취하도록 하고 사후에 보완이 이루어진 경우에만 수탁기업과 계약을 체결한다.

3. 위·수탁 계약서 작성

① 위·수탁업무 과정에서 위탁기관 또는 수탁기관의 산업기술이 유출될 가능성이 높다. 특히 위·수탁 기관간의 대등한 지위가 아닌 경우 기술탈취 등이 문제되는 경우가 자주 발생하게 된다. 따라서 부당한 방법을 통한 기술 탈취나 기술 유출 등을 사전에 방지하기 위

하여 위·수탁 계약서에 산업기술 유출이 문제될 수 있는 사항에 대해 다음의 내용을 참고하여 작성한다.

② 위·수탁 계약서에 다음 각 호 사항을 명시한다.

- 위탁 생산을 위한 지도방법
- 위탁 생산을 위해 제공되는 유형의 자료, 무형의 정보의 범위
- 위탁기업으로부터 제공받은 자료, 정보, 노하우의 비밀관리와 관련된 조항
- 수탁기업에서 위탁기업으로부터 제공받은 자료·정보·노하우를 취급하는 임직원에 대한 비밀유지의무 부과 및 교육과 관련된 조항
- 생산된 제품의 외부 판매 금지 조항
- 위탁기업으로부터 제공받은 자료·정보·노하우의 누설·공개·목적 이외 이용을 금지하는 조항
- 계약 종료 후 비밀유지 및 관련 물품과 설비의 반환
- 계약 종료 후 비밀유지의무 존속기간
- 위반행위에 대한 벌칙 조항
- 위반행위로 인하여 발생한 손해배상 조항
- 계약의 유효기간, 계약의 변경·해지·종료

4. 비밀유지 서약서(NDA, Non-disclosure agreement)

① 산업기술의 유출은 기업 차원에서 조직적으로 이루어지는 경우뿐만 아니라, 임직원 등 개인 차원에서 발생할 수 있다. 인수·합병 또는 합작투자 계약은 물론 기술 라이선스 계약, 위·수탁 계약을 체결하는 경우에는 상대방 기업과 계약서를 체결하는 것과는 별도로 해당 계약 체결을 주도하였거나 또는 주도하게 될 주요 임직원에 대하여 산업기술 보호에 관한 서약서를 징구하는 것이 필요하다.

② 이를 위해 계약에 참여하는 모든 임직원의 명단을 작성하여 산업기술을 인지하게 되는 인적 범위를 파악하고, 해당 임직원을 지속적으로 관리한다. 그리고 이들로부터 비밀유지서약서를 작성하여 제출하도록 한다. 참여자의 변경이 있는 경우 산업기술 계약 참여자 명단과 서약서를 체크하여 서약서를 징구하지 않은 자가 없는지 검토하고 아직 서약서를 작성하지 않은 자에게도 추가적으로 서약서를 징구한다.

③ 비밀유지서약서에는 다음의 내용이 필수적으로 포함한다.

- 서약서를 작성하는 임직원이 취급하는 기업의 비밀 정보 및 자료
- 비밀 정보 및 자료의 누설, 공개 및 목적외 이용 금지
- 비밀 정보 및 자료의 비밀관리
- 부서이동 등 비밀정 보 및 자료를 취급하지 않게 된 경우 비밀 정보 및 자료의 반환, 폐기, 삭제
- 비밀유지서약서 규정된 의무 위반 시 제재(징계, 손해배상 등)

※ 본 '산업보안 안내서'는 산업기술보호법 제8조(보호지침의 제정 등) 및 같은 법 시행령 제10조(보호지침의 제정)에 따른 "산업기술보호지침('21.1.15, 산업통상자원부장관 고시)" 제43조(산업보안 안내서)에 따라 산업통상자원부와 한국산업기술보호협회가 제정하여 마련된 자료임