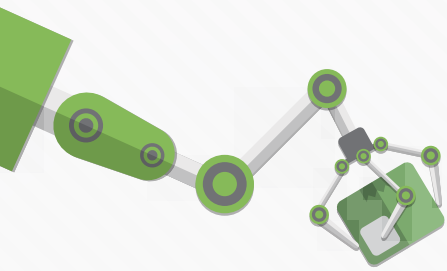
스마트공장
중요정보 유출방지 가이드

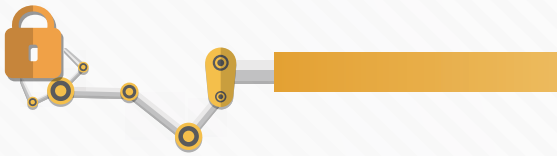
2017. 3

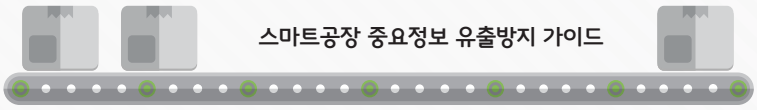
KISA 한국인터넷진흥원

스마트공장 중요정보 유출방지 가이드

CONTENTS







스마트공장 중요정보 유출방지 가이드

PART I 개요

1. 배경 및 목적
2. 범위 및 구성
3. 스마트공장 중요정보 유출 위협

Part Ⅰ

개요

1 배경 및 목적

세계는 지금 제조업 분야의 재도약을 위해 제4차 산업혁명, 제조업 혁신 3.0 등을 추진하고 있으며, 이에 대한 일환으로 스마트공장 구현에 박차를 가하고 있다. 스마트공장은 기존 제조업 생산 전 과정에 첨단 ICT 기술을 융합한 지능형 자율 생산 공장이라고 할 수 있다. 즉, 인공지능과 빅데이터 등을 활용하여 고객이 원하는 제품을 분석하여 고객 맞춤형 제품을 기획 · 설계하고, IoT, 자동화 로봇 등을 통해 최적화된 공정으로 제품을 자동 생산하며, 실시간으로 제품의 수 · 발주를 통제하는 공장시스템을 예로 들 수 있다.

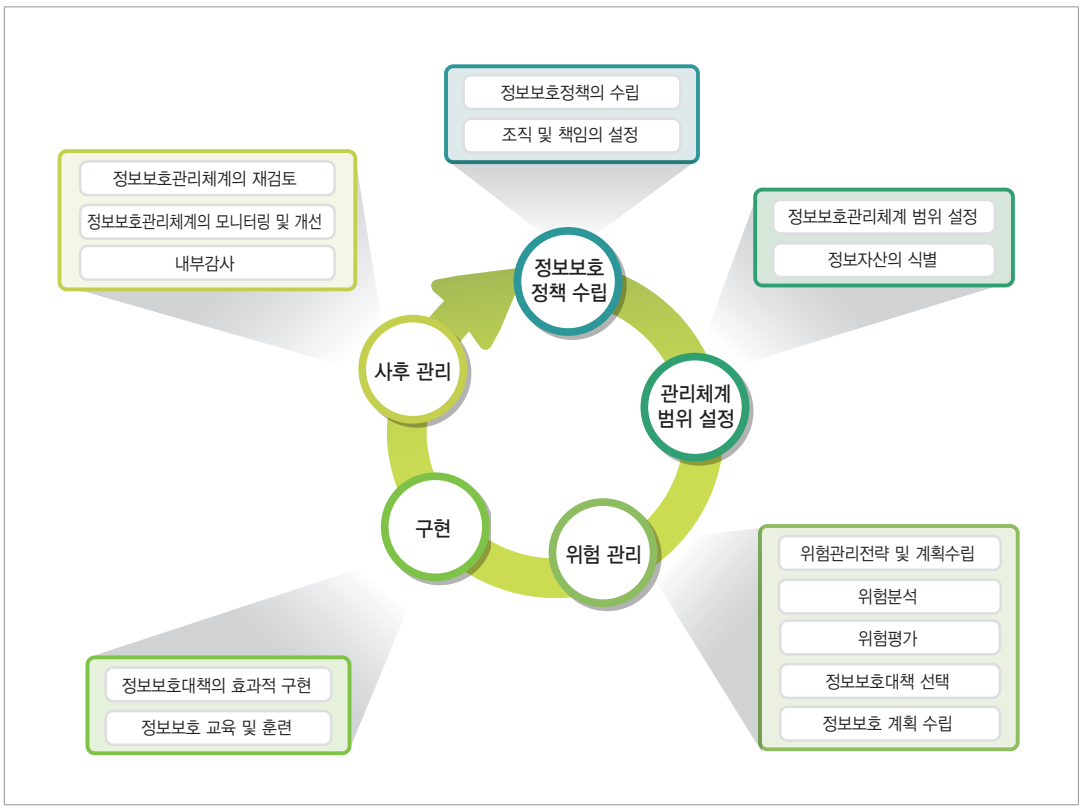
그림 Ⅰ-1 • 스마트공장 주요 특징

※ 출처 : 스마트공장 추진단, http://www.smart-factory.kr

스마트공장의 공장 제어시스템이 인간의 도움 없이 자율적으로 구동 · 유지되기 위해서는 기계 스스로 분석하고 제품을 설계하는 것은 물론, 생산 제어, 품질 · 공정 관리까지도 정확하게 수행할 수 있어야만 한다. 따라서 첨단 ICT 기술을 접목하는 과정에 공정 노하우, 제품 설계도, 영업기밀, 고객 요구 사항 분석 자료, 연구개발 성과물 등의 기업 중요정보가 반드시 활용 될 수밖에 없다.

그러나 스마트공장에서 기업의 중요정보를 활용하기에 앞서, ICT 기술 도입 시 발생할 수 있는 보안위협에 대해 먼저 충분히 인지해야 하며, 스마트공장의 특성에 맞추어 중요정보 유출 방지를 위한 방안을 마련해야 한다. 특히, ICT 기술 도입의 목적이 공장제어 자동화나 공장운영 상황에 따른 실시간 진단 및 처리 자동화 등을 통한 생산성 향상에 있으므로 공장제어시스템에 대한 원격 제어나 모니터링, 외부 네트워크와의 연결 등은 필수적일 수밖에 없다. 그러므로 이로 인해 발생하는 새로운 보안위협이 기업의 중요정보 유출로 이어지지 않도록 철저한 대비가 필요하다.

그림 Ⅰ-2 • **중요정보 보호 관리과정**



※ 출처 : ISMS 인증제도 소개자료, KISA

또한 세계 경제는 치열한 정보 경쟁 양상으로 발전하여 시시각각 경쟁 기업의 중요정보를 노리는 산업스파이의 활동과 내부자의 포섭이 빈번하게 이루어지고 있다. 기존에는 기업의 중요정보가 R&D센터, 경영센터 등에서 주로 보관 · 활용되어 왔지만, 스마트공장의 경우, 제품 생산 全과정에 걸쳐 중요정보가 저장 · 보관 · 활용되기 때문에 중요정보를 체계적으로 관리하는 것이 무엇보다 중요해졌다. 이때 중요정보를 제대로 통제하지 못하거나, 실시간 모니터링을 통해 중요정보의 부정사용 또는 불법유출 징후를 포착하지 못한다면 악의적인 내부자나 산업스파이에 의해 손쉽게 중요정보가 유출될 수 있다.

실제로 포스코경영연구원이 발간한 '다시 시작하는 인더스트리4.0'에 따르면, 독일전자산업협회(VDE) 회원사들이 가장 우려하는 것은 경쟁사에 자신의 중요정보가 노출되는 일이었다. 또한 사이버 공격으로 스마트공장의 주요 시스템이 파괴되거나 중단되면, 공장의 생산 및 서비스 연속성도 중단되어 기업의 평판 하락, 금전적인 손실 등이 발생하게 된다.

그러므로, 스마트공장에서도 중요정보를 적절히 보호하기 위한 정책을 수립하고, 중요정보의 생명주기에 따른 보안 위협과 취약성 분석 및 그로 인한 영향을 평가하여 적절한 중요정보 보호 관리체계를 수립하고 지속적으로 관리할 필요성이 제기되는 바이다

따라서 본 가이드는 스마트공장에서 발생할 수 있는 보안위협 분석을 통해 중요정보 유출 방지를 위한 관리체계 수립 · 운영 및 보안감사에 필요한 세부사항을 제시하고자 한다.

2 범위 및 구성

2.1 가이드의 범위

민관합동 스마트공장 추진단의 정의에 따르면 스마트공장을 IT 기술 활용 정도 및 역량에 수준에 따라 4단계 – 기초, 중간1, 중간2, 고도화 – 로 구분하고 있다. 이 중, 고도화 단계의 스마트공장은 전 세계적으로도 아직 구현된 사례가 없는 것으로 파악됨에 따라, 본 가이드에서는 현재 구축되어 있는 기초 단계에서부터 중간2 단계의 스마트공장에 대해서만 다루고자 한다.

표 Ⅰ-1 • 스마트 공장 수준별 구축 형태

단계	자동화	공장운영	비즈니스	가이드 범위
고도화	제어자동화 및 디지털식별이 결합된 IoT형 자동화	CPS, IoT, 빅데이터를 이용한 자가진단과 제어능력을 갖춘 지능형 생산	가치사슬 연계를 통한 실시간 고객 맞춤 서비스	×
중간2	설비 제어 자동화	실시간 의사 결정 및 설비 직접 제어	시장과 고객 요구에 능동적으로 대응한 실시간 의사결정 및 통제	○
중간1	설비로부터 실시간 데이터 수집	설비로부터 집계된 실적 중심의 공장 운영 분석	정보경영에 기반, 공장운영 등 실시간 정보 교류	
기초	바코드 RFID를 기초적 물류정보 수집 수준	공정물류 중심의 실적관리 수준	Lot-Tracking을 통한 품질 이력 관리	

※ 출처 : 스마트공장 추진단, http://www.smart-factory.kr

2.2 가이드의 구성

본 가이드는 크게 두 부분으로 구성되어 있다. 'Part Ⅰ'에서는 가이드의 개발 배경과 범위, 스마트공장의 정의와 중요정보 유출 위협에 대해 소개하며, 'Part Ⅱ'에서는 스마트공장 내 중요정보 유출 방지를 위한 10대 보안 요구사항과 관리체계 수립방안을 스마트공장의 특성 및 중요정보 생명주기를 고려하여 제시한다.

구체적으로 'Part Ⅱ'의 1장에서는 중요정보를 관리하는 전담 정보보호 조직을 구성하고, 보안규정을 통해 책임과 권한을 부여하는 등 전반적인 조직 정책을 수립하는 방법에 대하여 설명한다. 2장에서는 협력사 직원, 해외지사, 임직원, 퇴직자 등 중요정보에 접근 가능한 인력의 인적 보안관리 방안에 대해 설명한다.

3~9장에서는 스마트공장의 제품생산 전 과정에 걸쳐 존재하는 중요정보 생명주기를 식별-생성-접근-활용-보관-제공-파기의 총 7단계로 나누고, 각 단계별로 우선적으로 고려해야 하는 보안 요구사항에 대해 설명한다. 이어서 10장에서는 정기적 위험분석과 보안 취약점 점검, 그리고 발견된 문제점에 대한 보완조치 여부를 주기적으로 감사하는 보안감사에 대하여 소개 한다.

보안감사는 기존에 수립된 중요정보 관리체계의 적정성을 평가하고 보완하기 위한 단계로 전체 중요정보 관리체계의 영향을 주는 중요한 과정이라고 할 수 있다. 또한 중요정보 유출사고 발생 시에는 사고의 원인과 과정을 추적하기 위한 디지털 증거 확보로 활용 될 수 있다. 조직의 관점에서는 사고의 원인과 과정을 정확히 알아내야만 적절한 해결방안과 보안수준을 향상 시킬 수 있기 때문에 10장과 부록을 통해 보안감사 수행 절차와 데이터 수집 시 고려사항, 보안감사 도구 등을 구체적으로 소개 한다.

중요정보 유출 방지의 핵심이 체계화된 중요정보 관리체계를 구축하고 운영하는 것이기 때문에, 본 가이드에서 제시하는 바를 참고하여 스마트공장 중요정보 유출 위험에 효과적으로 대비할 수 있도록 생명주기 각 단계별 특성에 맞는 통제 방안을 수립 · 적용하고 정기적으로 보안감사를 통해 보완해 나가야 할 것이다.

3 스마트공장 중요정보 유출 위협

3.1 스마트공장 내 중요정보란?

스마트공장 내 중요정보에 대한 구체적인 정의나 범위는 각 공장별 특성(산업 분야, 주요 생산품 등)에 따라 다르게 정의될 수 있다. 다만, 국내 관련 법률 등에서는 산업에서의 중요정보에 대한 개념 및 정의를 아래와 같이 제시하고 있다.

표 Ⅰ-2 • **국내법 상 산업보안 관련 중요정보 개념 및 정의**

용어	정의
영업비밀	공공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서, 합리적인 노력에 의하여 비밀로 유지된, 생산방법, 판매방법, 그 밖에 영업활동에 유용한 기술상 또는 경영상의 정보
산업기술	제품 또는 용역의 개발 · 생산 · 보급 및 사용에 필요한 제반 방법 내지 기술상 정보
국가핵심기술	국내외 시장에서 차지하는 기술적 · 경제적 가치가 높거나 관련 산업의 성장잠재력이 높아 해외로 유출될 경우 국가의 안전보장 및 국민경제 발전에 중대한 악영향이 우려되는 산업기술

※ 관련법령 : 산업기술의 유출 방지 및 보호에 관한 법률 (https://http://www.law.go.kr/),
부정경쟁방지 및 영업비밀 보호에 관한 법률 (https://http://www.law.go.kr/)

관계 법령에서는 기업의 중요정보를 특정하지 않고 경쟁력 확보와 이윤추구를 위해 필요한 기술–경영 정보 등 넓은 범위로 정의하고 있다. 그럼으로 스마트공장의 경우에도, 아래 중요정보 유형 예시를 참고하여 공장의 특성에 맞게 '중요정보'를 정의할 수 있다.

단, '중요정보'라고 정의한 내용(정보의 종류 및 범위 등)은 차후 중요정보의 식별과 이에 대한 세부적 보안규

칙 설정, 관리체계 수립 등을 위한 기준이 될 수 있으므로 기업별로 자사 스마트공장의 특성을 충분히 고려하여 정의해야 한다.

그림 I -3 • 스마트공장의 중요정보 유형 예시

3.2 스마트공장 내 중요정보 유출 위협

스마트공장 구현의 핵심은 제품의 전 생산과정을 ICT 기술과 접목시켜 진화된 형태의 공장을 구축하는 것이다. 하지만 ICT 기술과의 접목으로 인해 기존 공장 환경에서는 발생하지 않았던 새로운 보안위협이 발생할 수 있게 되었다. 예를 들어, 기존에 수동으로 제어하던 공장 내 시스템의 경우 업무 담당자의 악의적 정보 유출 외에는 별다른 보안위협이 존재하지 않는다. 그러나 ICT기술을 접목하여 무선 기기를 이용해 공장 내 시스템을 원격제어나 모니터링을 하는 경우, 무선통신의 보안 취약점을 악용한 중요정보 유출 위협이 새로이 발생하게 된다.

(그림I-4)에서는 이와 같이 ICT기술이 접목된 스마트공장에서 발생 가능한 중요정보 유출 시나리오와 각 시나리오별로 어떤 보안위협이 존재하는지를 소개한다.

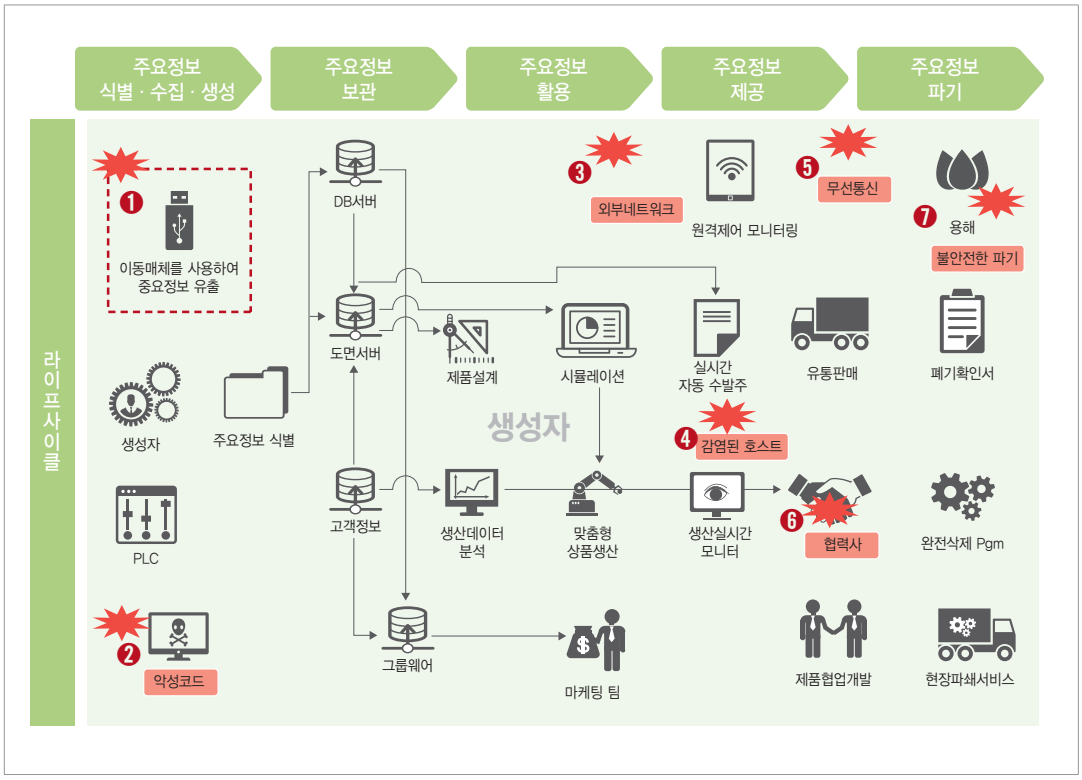
1) 이동형 저장매체에 대한 통제 시스템 및 중요정보 접근제어 시스템 등이 구축되지 않아 공장 제어시스템에 USB 등 외부매체를 직접 연결하여 중요정보 유출

2) 안티 바이러스 솔루션이 구축되지 않았거나 시스템 내 패치관리가 제대로 되지 않아 보안위협에 취약한 산업 장비의 악성코드 감염 및 이를 통한 중요정보 유출

3) 외부 네트워크와 분리된 폐쇄망을 주로 사용하던 공장 제어시스템이 스마트공장化 되면서 증가된 외부 네트워크를 통해 중요정보 유출

4) 외부에서 스마트공장을 원격 제어하거나 모니터링 할 수 있는 호스트 장비를 악용하여 중요정보 유출

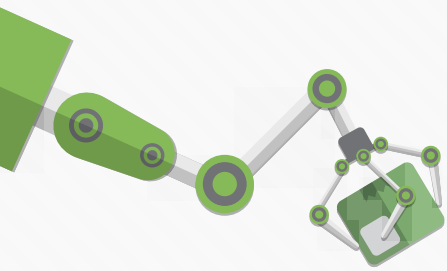
그림 Ⅰ-4 • 스마트공장 중요정보 생명주기별 중요정보 유출 위협 시나리오

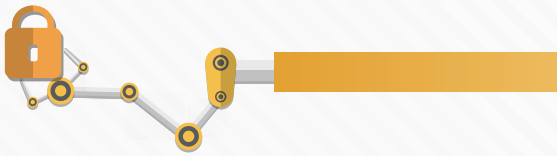


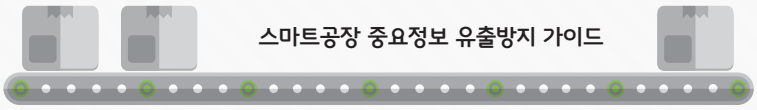
5) 스마트공장에서 사용되는 무선통신 보안약점을 악용한 스니핑 공격 등을 통해 중요정보 유출

6) 중요정보에 접근 가능한 협력업체 직원이나 악의적인 내부자에 의한 중요정보 유출

7) 매각 · 폐기된 자산과 출력물을 영구 삭제 솔루션 및 디가우저(Degausser) 등을 통해 완전히 삭제하고 파기하지 않아 남아있는 정보가 복구되어 중요정보 유출







스마트공장 중요정보 유출방지 가이드

PART Ⅱ 스마트공장 중요정보 유출 방지 가이드

1. 전담 정보보안 조직을 구성하고 책임과 권한을 부여한다
2. 중요정보 유출 방지를 위한 인적 보안관리 방안을 강화시킨다
3. 중요정보를 식별하여 등급을 부여하고 관리 · 통제한다
4. 중요정보의 생성단계부터 유출 방지 방안을 적용하여 통제한다
5. 중요정보 접근 시 권한 기반의 체계적 통제 방안을 적용한다
6. 중요정보 활용 시 악성코드 감염 및 전파 방지를 위한 대책을 마련하고 보안관제를 실시한다
7. 중요정보 보관 정책을 마련하고 통제한다
8. 중요정보 외부 제공 시 유출 방지 방안을 마련하고 통제한다
9. 중요정보 파기절차 및 방법을 마련하고 통제한다
10. 중요정보 유출 방지를 위해 정보시스템에 대한 취약점 점검 및 정기적인 보안감사을 실시한다

Part Ⅱ

스마트공장 중요정보 유출방지 가이드

다음은 스마트공장 내 중요정보 유출 방지를 위한 관리적 · 기술적 · 물리적 고려사항과 스마트공장의 특성 및 중요정보 생명주기에 따른 관리체계 수립 방안에 대한 10가지 가이드를 소개한다.

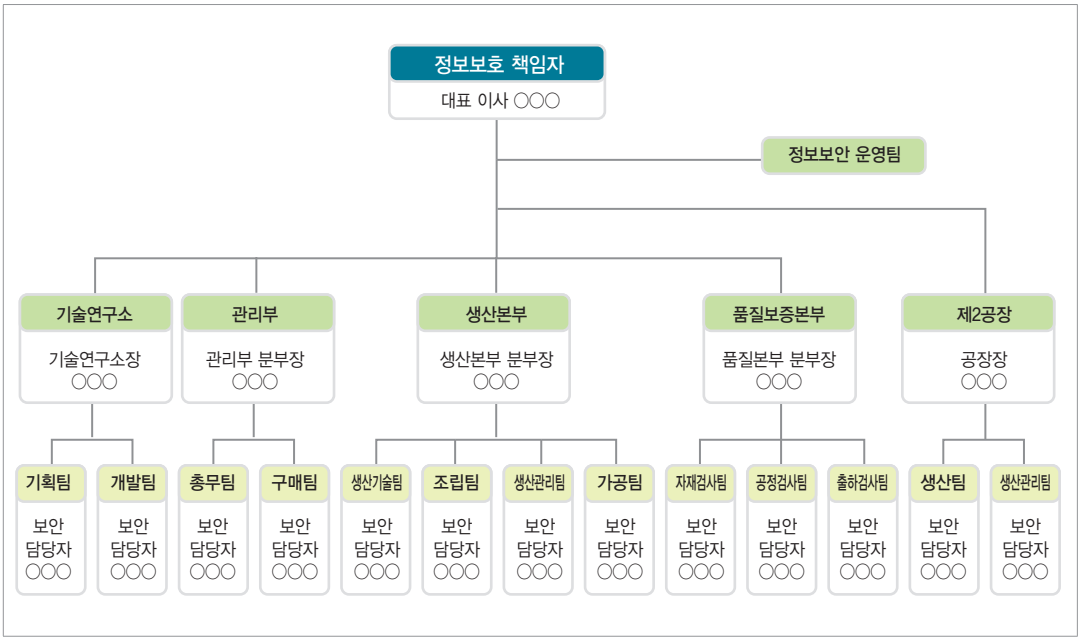
1 전담 정보보안 조직을 구성하고 책임과 역할을 부여한다

스마트공장에서 중요정보 보호 정책을 체계적으로 운영하기 위해서는 우선 중요정보를 관리하는 전담 정보보호 조직을 구성하여야 한다. 전담 정보보호 조직은 보안규정을 통해 책임과 권한을 명확히 부여하고 중요정보 보호 정책을 비롯한 전반적인 조직 정책을 수립해야 한다.

1.1 중요정보 보호를 위한 조직 운영

스마트공장을 구축한 기업의 최고경영자(CEO)는 조직의 규모 및 통제해야 할 정보의 중요도에 따라 필요인력, 예산 등을 확보하고, 중요정보를 체계적으로 보호하기 위한 실무조직을 구성해야 한다. 중요정보 보호를 위한 실무조직은 별도의 전담조직으로 구성하는 것이 바람직하며, 실무조직의 구성원을 임명할 경우 정보보호 전문성을 고려하도록 한다. 스마트공장 기업의 규모(크기 및 인력), 관리구조 등의 여건과 환경으로 인해 전담조직 구성이 어려운 경우, 겸임조직으로 구성할 수 있으나 이러한 경우에도 해당 조직에 대한 공식적인 선언이나 지정이 필요하다.

그림Ⅱ-1 • 정보보호 조직 구성 및 책임할당 예



스마트공장에서 생성되는 제품의 설계도, 특허 기술 등 중요정보를 보호하기 위한 실무조직은 정보보호 최고책임자와 그의 임무를 위임받아 업무를 수행하는 관리자, 조직에서 실무를 담당하는 부서별 중요정보 보호 담당자 등으로 구성될 수 있다. 더불어 기업의 중요정보 보호 전반에 걸친 사항들을 검토하고 결정할 수 있도록 정보보호위원회를 두도록 권고한다.

기업은 중요정보 보호 업무를 효율적으로 총괄 · 관리할 수 있도록 정보보호 최고 책임자를 임원급에서 지정하여야 한다. 그리고 인사발령 등의 공식적인 지정 절차를 거쳐 중요정보 보호에 대한 책임과 역할을 명확히 수행할 수 있도록 하는 것이 바람직하다. 다음은 정보보호 최고 책임자가 총괄하여 관리해야 할 업무 영역에 대한 예이다.

표 Ⅱ-1 • 정보보호 최고 책임자의 업무 영역 예

- 중요정보 보호 정책 및 정책시행 문서(지침/절차/매뉴얼 등)의 수립, 관리
- 중요정보 보호를 위한 조직 구성, 담당자별 명확한 책임과 권한 부여
- 중요정보 보호 관리체계 수립 및 운영
- 중요정보의 식별 및 보안등급 부여
- 임직원 대상 중요정보 보호 교육
- 그 밖의 법 · 제도에서 정한 중요정보(산업기밀 정보 등) 보호조치 이행 등

또한, 기업은 정보보호 최고 책임자의 관리 업무를 실무적으로 이행할 수 있도록 중요정보 관리자와 중요정보 보호 담당자의 책임과 역할을 구체적으로 정의하여야 하며 이를 직무기술서 등의 형태로 문서화하는 것이 중요하다. 또한 조직 내 KPI((Key Performance Indicator : 핵심성과지표), MBO(Management By Objectives : 목표관리), 인사평가와 같은 평가체계 내에 중요정보 보호 활동의 책임과 역할을 평가할 수 있는 항목을 포함하여 주기적으로 정보보호 최고 책임자와 정보보호 관련 담당자의 활동을 평가하도록 하여야 한다.

1.1.1 전담 정보보호 조직의 독립성 확보

전담 정보보호 조직이 중요정보를 체계적으로 보호하기 위해서는 전담조직의 독립성 확보가 중요하다. 다른 부서에 영향을 받지 않도록 현업업무와 직무상으로 분리하고 정보보호 최고 책임자나 이사회 등으로부터 직접적인 지시를 받아야 한다. 또한 보안 감사업무를 수행할 경우 필요한 모든 자료를 청구할 수 있는 권한 및 감사 결과 시 나타난 문제점에 대한 경영진의 공식적인 의견 제출과 시정을 요구할 수 있는 권한이 부여되어야 한다. 나아가 감사 결과를 이사회 등 최고 의결 기관에 직접 보고함으로써 보안감사의 의무를 완수할 수 있게 지원해야 한다.

1.1.2 조직 구성원의 정보보호의 책임과 역할 부여

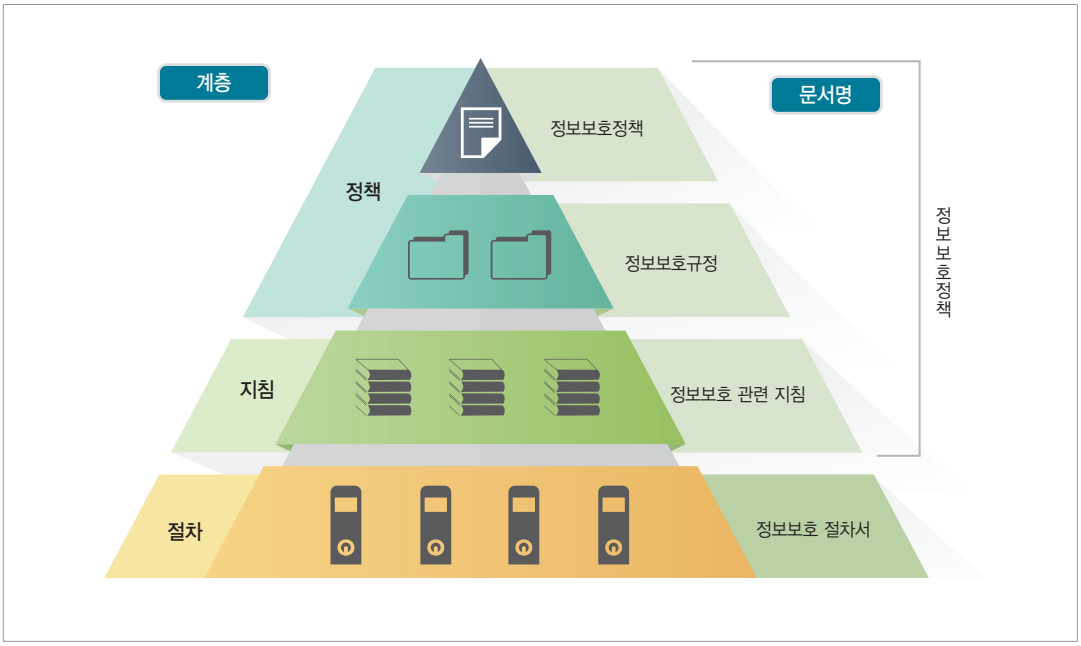
중요정보 보호를 위해서는 조직 구성원을 대상으로 직급과 담당 업무에 따른 역할과 책임을 명확히 정의하고 문서화해야 한다. 기술적으로도 권한이 있는 자만이 중요정보에 접근할 수 있도록 권한관리 및 접근통제 기능을 구현해야 한다. 특히, 접근통제 시스템에 보안토큰이나 스마트카드 등을 추가로 활용하면 보다 높은 보안성을 확보할 수 있다.

1.2 중요정보 보호 정책 수립 및 범위 설정

1.2.1. 중요정보 보호 정책 수립

스마트공장을 구축한 기업은 중요정보를 보호하기 위해 일관된 정보보호 정책을 가지고 있어야 한다. 최상위 단계로 정보보호 활동을 규정하는 정보보호 정책을 제정하고, 상위 단계의 정책을 세부적으로 시행할 수 있도록 규정, 지침, 절차 등으로 구분하여 제정할 수 있다.

그림Ⅱ-2 • 정보보호 정책 수립 단계



중요정보에 대한 정보보호 정책은 최고경영자(CEO)의 승인을 받아, 모든 임직원 및 관련자에게 배포되어야 하며 관련자는 해당 정책을 이해하고 있어야 한다.

중요정보에 대한 정보보호 정책 수립 시에는 정보보호 활동의 목적, 방향, 범위, 책임 및 각종 보호 조치방안 등 스마트공장에서 수행되는 모든 정보보호 활동을 포함해야 한다. 또한 스마트공장 구축 기업이 준수해야하는 정보보호 관련 법적 요구사항을 분석하여 정책에 반영해야 한다.

정책의 제 · 개정 시에는 이해관계자의 검토(협의 및 조정 등)를 통해 스마트공장 내에서 실제 수행하고 있는 중요정보 보호 활동이 정책 내용에 반영될 수 있도록 하여야 한다. 이해관계자는 상위정책과 정책시행 문서의 시행주체가 되는 부서 및 담당자(정보보호부서, 정보시스템 운영 및 개발 부서, 현업부서)를 의미한다. 또한, 중요정보 보호 관련 사안에 대한 실무적인 검토, 이행방안 업무를 수행하는 정보보호 실무협의회를 운영하고 있는 경우 이 조직을 통해 검토할 수도 있다.

정보보호 정책 및 정책시행 문서는 다음과 같은 상황이 발생한 경우를 포함하여 주기적으로 타당성 검토를 거쳐야 하며, 필요한 경우 제 · 개정 절차를 통해 해당 검토결과가 문서에 반영되어야 한다.

표 Ⅱ-2 • 정보보호 정책 및 정책시행 문서의 제·개정 필요 상황 예

- 내부감사 수행 결과
- 개인정보 및 정보보호 관련 법령 제 · 개정
- 중대한 침해사고 및 정보유출 사고 발생
- 새로운 위협 또는 취약점 발견
- 정보보호 환경의 중대한 변화
- 조직 사업 환경의 변화 (예 : 신규 공장 건립 및 확장)
- 정보시스템 환경의 중대한 변화 (예 : 차세대 시스템 구축)

1.2.2. 중요정보 보호 관리체계

스마트공장에서 생산되는 중요정보 보호를 위한 관리체계는 정보보호 정책 수립, 관리체계 범위설정, 위험관리, 구현, 사후관리 단계로 구성되며 각 단계별로 필요한 조치사항은 다음과 같다.

정보보호 정책 수립

정보보호 정책 수립 단계에서는 조직 전반에 걸쳐 적용되는 정보보호 정책을 수립하고 정보보호를 수행하기 위한 조직 내 각 부문의 책임을 설정한다.

관리체계 범위 설정

정보보호 관리체계의 범위를 설정하고 범위 내 정보자산을 식별하여 범위를 명확히 한다.

위험관리

정보자산에 적절한 위험관리 전략과 계획을 수립한다. 이에 따라 위험 요소들을 분석하고 위험도를 평가하여 대응이 필요한 위험에 대해 우선순위를 결정한다.

구현

위험관리 단계에서 수립된 정보보호 계획에 따라 정보보호대책을 효과적으로 구현하고 필요한 교육과 훈련을 진행한다.

사후관리

체계를 운영하는 과정에서 상시적인 모니터링을 수행하고 정기 내부감사를 통해 정책 준수사항을 확인한다. 이러한 결과에 기초하여 중요정보 보호 관리체계를 재검토하고 관리체계를 지속 개선한다.

2 중요정보 유출 방지를 위한 인적 보안관리 방안을 강화시킨다

중요정보 유출 사고는 외부의 해킹이나 악성코드를 통한 유출보다는 내부 직원 및 협력업체 직원을 통해 발생하는 것이 대부분이다. 실제로 국정원 산업기밀보호센터의 해외 기술유출 사건 자료를 분석한 결과, 전 · 현직 직원에 의한 기술 유출이 80%를 차지하고 있으며, 협력업체에 의한 기술유출도 7%를 차지하고 있다. 특히, 내부 직원이나 협력업체 직원의 경우, 중요정보가 가지고 있는 가치를 잘 알고 있고, 해당 정보에 대한 접근권한을 가지고 있는 경우가 많으므로 보다 손쉽게 정보 유출이 가능해진다. 그러므로 내부 직원 및 협력업체 등을 대상으로 보안의식을 함양시키고 인적보안을 강화하는 것은 매우 중요한 일이다. 그리고 무엇보다도 내부 임직원이라 하더라도 중요정보에 대한 접근은 매우 엄격히 제한해야 한다.

표 Ⅰ-3 • 2010년~2014년도 해외유출 적발 시행주체별 현황

전직직원	현직직원	협력업체	투자업체	기타	계
52.8%	27.1%	7.0%	0.4%	12.7%	100%

※ 출처: 산업기밀보호센터, http://service4.nis.go.kr

2.1 외부 협력직원 및 해외지사 인력 관리

외부 협력사에 업무를 위탁하는 경우에는 정보시스템, 네트워크, 인력 및 사무환경 등을 관리 · 통제하기 위한 보안 요구사항을 계약서상에 명시해야 하고 요구사항을 서비스수준협약(SLA: Service Level Agreement)에 반영해야 한다.

외부 위탁 계약서에 포함되어야 하는 보안 요구사항으로는 법적 요구상의 충족, 책임감 있는 보안관리, 정보자산의 비밀성과 무결성을 유지할 수 있는 대책, 일반 정보의 접근제한 및 오남용 방지 등이 있다. 또한 외부 위탁업체 직원은 외부자 보안정책을 포함한 정보보호 관련 규정을 준수할 것을 약속해야 하며, 비밀 유지를 위한

보안서약서를 함께 제출해야 한다. 이와 같은 계약서는 신청기관과 위탁업체의 책임자가 승인한 공식적인 계약서로써 관리되어야 한다.

표 Ⅱ-4 • 외부 위탁 계약서 작성 방안

- 외부 위탁 계약 시 관련된 보안 요구사항을 사전에 분석한다.
- 외부 위탁 계약 시 정보시스템, 네트워크 인력 및 사무환경 등을 관리 통제하기 위한 보안 요구사항을 계약서상에 명시한다.
- 보안 요구사항은 서비스수준협약에 반영하여, 이를 위반할 시 처벌을 가하거나 손해배상을 청구할 수 있음을 조항의 내용으로 명시한다.

해외에 R&D센터 등 연구시설을 설립하여, 신기술, 연구개발 등이 이루어지는 경우 중요정보 유출에 더욱 주의를 기울이고, 핵심기술을 블랙박스화 하여 현지인들의 모방을 방지하도록 해야 한다. 산업 분야마다 차이가 있을 수 있지만, 핵심 부품은 분해 및 재제작을 어렵게 하여 역 엔지니어링(reverse engineering)을 원천적으로 차단하는 방법이 있으며, 전체적인 제조 프로세스에서 중요정보가 유출되는 것을 방지하기 위해 현지 연구원에게는 단위별 프로세스만 알 수 있도록 업무를 제한적으로 공개하는 등의 방법 활용할 수 있다. 그 외에도 다음과 같은 방법을 통해 중요정보 유출을 방지해야 한다.

표 Ⅱ-5 • 해외지사의 인력관리 방안

- 해외에 진출한 국내 기업의 근로자가 대부분 현지인이더라도 핵심기술 및 시설의 보안담당은 한국인이 맡는다.
- 연구센터 내 전담 관리 조직을 두어 보유 기술을 체계적으로 관리한다.
- 외국인 연구원에 대해 별도 보안조치를 적용한다(영문 보안서약서 작성, 출입지역 제한, 반출 · 반입 물품제한, 특이동향 관리 등)

2.2 중요정보에 대한 정보보호 의식 강화 교육

최고경영자는 스마트공장 환경과 상황을 고려하여 중요정보 유출 방지와 관련한 교육부서와 담당자를 지정해야 하며, 교육 횟수 및 내용에 관해서도 내부 관리 지침을 마련하여야 한다. 정보보호 교육과 관련된 전문 교육은 외부 전문가나 전문기관을 통하여 실시할 수도 있다. 다음은 정보보호 의식 강화를 위한 내부 직원이나 협력사를 대상으로 실시하고 있는 교육활동의 예이다.

표 Ⅱ-6 • 정보보호 의식 강화 교육 프로그램 예

- 입사 시 중요정보 보호 관련 교육
- 임직원 중요정보 유출 방지 교육
- 신입사원, 경력사원 입사 시 6개월 이내 집체 교육
- 전 직원 대상 중요정보 보호 교육 및 홍보(1년 2회 이상)
- 협력사 직원에 대한 중요정보 유출 방지 관련 교육

중요정보에 대한 정보보호 의식 강화를 위한 교육내용으로는 다음 사항을 포함할 필요가 있다.

표 Ⅱ-7 • 정보보호 의식 강화 교육 내용 예

- 스마트공장 중요정보 보호의 필요성
- 중요정보 유출 위험의 구분 및 인지
- 중요정보 보호를 위한 업무 분장
- 중요정보 유출 방지 관련 법규
- 공장 내 중요정보 유출 방지를 위한 정책 및 보호체계
- 중요정보 유출사고 발생 시 대응 절차 및 방법 등

스마트공장 정보보호 의식 강화 교육은 시행 환경에 따라 정보보안 책임자가 집합교육, 온라인 교육, 유인물 배포 등의 교육 방법 중 적절한 것을 선택하여 시행할 수 있다. 이때 정보보안 담당자는 교육에 앞서 전 직원을 대상으로 교육 실시 관련 내용을 사전에 공지해야 한다. 임직원들이 중요정보 보안에 대한 책임감을 가지고 사내 보안 규정을 숙지하여 정확하게 실천할 수 있도록 전 직원을 대상으로 중요정보 보호 의식 강화 교육을 정기적으로 실시하도록 한다.

표 Ⅱ-8 • 정보보호 의식 교육 방법

- **정기교육** : 정기교육은 내부규정에 명시된 사항을 준수하여 최소 연 1회 이상 시행해야 하며, 정해진 시점에 정기교육을 실시하되, 전 직원이 참여할 수 있도록 시기와 장소, 내용 등을 계획단계에서부터 고려해야 한다.
- **수시교육** : 신입 및 경력 직원이 입사한 경우나 보안규정이 개정 된 경우, 중요정보 유출 사고가 발생한 경우 등을 포함하여 CEO나 정보보호관리 책임자가 보안교육이 필요하다고 인정한 경우에는 해당자를 대상으로 수시로 교육을 실시할 수 있고, 이때 직원들의 교육 참여가 적극 독려되어야 한다.

중요정보에 대한 정보보호 교육은 모든 임직원이 참석하는 것을 원칙으로 하며, 부득이한 사유로 교육에 참석하지 못한 임직원은 차후에 별도 교육을 받거나, 유인물 배포 및 전자메일을 통해 해당 교육내용을 숙지할 수 있도록 조치해야 한다.

표 Ⅱ-9 • 각 대상별 교육 내용 및 주기 예시

대상	교육 내용	주기
중역 이상	경영자 보안 교육	1회/년
부장 ~ 사원	예방 보안 교육	10시간
부장 ~ 과장	심화 보안 교육	10시간
대리 ~ 사원	기초 보안 교육	10시간
신입 전입 사원	생활 보안 교육/가상훈련	2시간
보안 담당자	실무 보안 교육/가상훈련	4회/년
보안 실무	외부 특별 교육	4회/년
핵심기술 취급자	핵심기술보안교육/가상훈련	수시
고 위험군	특별 보안 교육/가상훈련	수시

2.3. 침해사고 유출 시나리오에 맞는 가상훈련

가상훈련은 상시 교육의 일환으로 실제 침해사고 유출 시나리오에 맞는 훈련을 실시한다. 모의 해킹과 동일하게 화이트박스, 블랙박스와 같이 정보 유출 인지 유무에 따라 나뉘어 수행하도록 한다.

화이트박스 훈련

화이트박스 훈련은 고위험군 또는 훈련 대상자에게 가상훈련에 대한 시나리오를 미리 말해주고 실제로 하나하나 내부 유출의 가능성을 막는 방식으로 진행한다. 가상훈련 진행 후 보안 담당자와 훈련 대상자의 피드백을 공유함으로써 정책 적용 · 발전에 도움을 주도록 한다.

블랙박스 훈련

블랙박스 훈련은 단순 기술적인 정보 유출의 위협뿐만 아니라, 사회 공학적인 기법을 섞어 실제 외부 유혹에 대해 어떻게 대처하는지, 기술적으로 보안을 잘 수행하고 있는지 등을 훈련하는 방식으로 진행한다. 해당 테스트는 실제 정보 유출 시나리오와 거의 동일하게 사전 공지 없이 진행되므로, 훈련의 결과가 나쁠 경우 직원 평가에 감점 요인으로 책정하여, 항시 직원들이 정보유출에 대한 경각심을 가질 수 있도록 한다.

2.4 중요정보 접근이 가능한 인력의 책임성 강화 방안 마련(비밀유지서약)

중요정보 유출사고가 감소되지 않는 주된 이유는 중요정보 보호에 대한 임직원들의 보안의식과 책임감이 결여되어 있기 때문이다. 국정원 산업기밀보호센터의 기술 유출 적발 조사에 따르면, 78%가 금전적인 유혹이나 개인 영리를 목적으로 중요정보를 유출한 것으로 보고되었다. 그러므로 기업에서는 임직원의 입사 시부터 퇴직까지 전 기간에 걸쳐 중요정보 보호의 중요성을 각인시키고, 책임성 강화를 위한 방안을 시행해야 한다.

2.4.1. 중요정보 보호를 강제할 수 있는 취업규칙 조항 개정

스마트공장 구축 기업은 업무, 시스템 관리 운용 등을 하면서 생산되는 설계도면, 생산 정보 등 중요정보가 내부자를 통해 외부에 유출되지 않도록 취업규칙 내에 중요정보 보호를 강제하는 조항을 넣을 수 있다. 즉, 취업규칙에 중요정보 유지의무, 경업금지의무, 중요정보의 창출 및 귀속에 관한 규정, 위반 시 조치 등을 포함시킬 수 있으며 이는 일반적 의미에서의 '보안유지서약서'와 함께 종업원 채용 시 정보보호 책임성을 부과할 수 있는 기본적인 장치로써 기능한다.

2.4.2. 인력관리 단계별 보안서약서 징구

취업규칙에 기초한 중요정보 보호 의무는 포괄적 · 일반적인 의무규정에 머무르고, 직원에게 공개된 정보 가운데 어떤 것이 보호 대상인지 불명확한 경우도 있다. 그래서 기업에서는 중요정보와 관련된 임직원들의 의무 규정을 명확화하기 위해 비밀유지 대상과 비밀보안 관리 및 부수의무, 예외 규정, 비밀보호 기간, 비밀보호 의무 위반 시 조치 사항 등을 포함한 중요정보 보호 서약서를 추가적으로 작성하도록 할 수 있다. 특히, 중요정보와 관련된 프로젝트에 투입되거나 퇴사 시에는 다음의 추가 고려사항을 참고하여 중요정보 보호를 위한 서약서를 작성하도록 해야 한다.

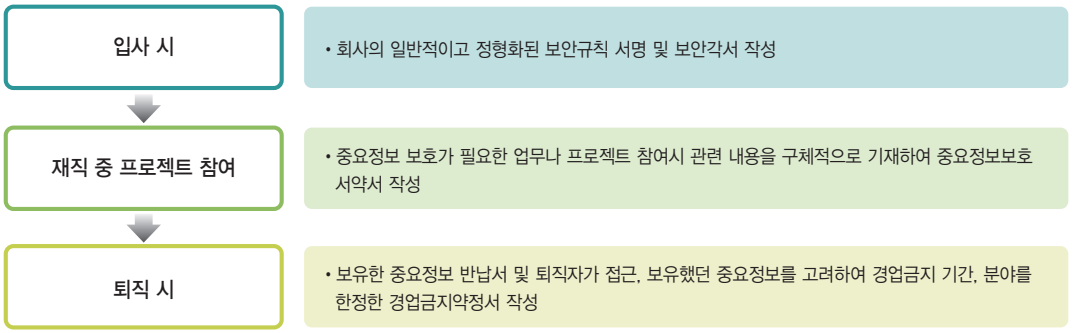
프로젝트 참여 등 재직기간 중요정보 보호 관련 서약서 작성

임직원이 재직 중 중요정보와 관련된 프로젝트에 참여하였다면, 앞서 설명한 서약서 상에 포함되어야할 내용 외에도 참여한 프로젝트 명, 프로젝트 기간, 프로젝트 수행 산출물과 중요정보 등을 포함한 중요정보 보호 서약서를 작성하도록 한다.

퇴직 시 중요정보 보호 관련 서약서 작성 시 고려사항

중요정보 보호를 위해 임직원의 퇴직 시에는 퇴직 후에도 중요정보 보호 의무를 유지해야할 책임이 있다는 내용을 퇴직 서약서에 포함시키고, 재직 기간 중 참여한 프로젝트, 업무 등을 통해 접근한 정보 중 중요정보 보호의무 대상의 범위를 명시하도록 한다. 특히, 퇴직자가 보유하였던 중요정보 및 자산의 내용은 가능한

구체적으로 기재하고, 보안규정에 따라 자료에 식별 코드나 문서 번호가 부여된 경우 관련 사항도 함께 기재하여 퇴직 전까지 반납서와 함께 반납하도록 한다. 관리 부서에는 제출된 내용에 누락이 없는지를 해당 직원의 퇴직 전까지 확인해야 한다.



경업금지약정서 작성 시 고려사항

경업금지약정이란 근로자가 퇴직 후 경쟁관계에 있는 업체에 취업하거나 스스로 경쟁업체를 설립, 운영하는 등의 경쟁행위를 하지 않을 것을 주 내용으로 하는 약정을 말한다. 그러므로 경업금지서약서 작성이 필요할 시에는 업종 · 분야와 경업금지 기간을 구체적으로 명시토록 한다. 다만, 경업금지 기간은 업종, 제품의 라이프 사이클, 특허출원 상황 등을 통합적으로 고려하여 결정해야 한다. 향후, 중요정보 유출 및 경쟁업종 금지 기간 중 경쟁업체로 이직할 경우, 관련법규에 의해 처벌받는다는 사실을 고지하고 퇴직 서약서에도 위와 같은 내용을 명기한다.

표 Ⅱ-10 • 실효성 있는 경업금지약정 체결을 위한 고려사항

- 중요정보 접근 가능성 있었던 자에게 중요정보 보호 의무를 부과해야 한다.
- 경업금지의 기간이나 지역적 범위, 직종은 지나치게 포괄적이지 않고 합리적인 수준에서 정하여 약정서에 기재해야 한다.
- 경업금지약정은 퇴사하는 근로자의 특성에 맞는 내용으로 개별적으로 체결하는 것이 바람직하다.
- 근로자에게 경업금지 의무를 부담하는 것에 상응하는 대가를 지급하는 것이 바람직하다.
- 근로자의 생계 등 이익을 보호하는 조치를 함께 취하는 것이 바람직하다.

3 중요정보를 식별하여 등급을 부여하고 관리 · 통제한다

중요정보 유출 방지를 위해서는 무엇보다 특허기술 및 제품 설계도 등 보호해야 할 정보자산을 식별하고 정보의 중요도에 따라 보안등급을 통제하는 것이 기본 요소라고 할 수 있다. 이를 위해 다음에서는 중요정보의 식별 및 목록관리, 보안등급 부여 방안 및 등급별 통제 방법에 대해 소개한다.

3.1 중요정보의 식별 및 목록 관리

유출될 경우 기업 이미지 하락 또는 경제적 손실을 발생시킬 수 있는 중요정보의 경우, 정보 생성 단계부터 식별하여 관리하여야 한다. 중요정보 보호 책임자는 새로운 정보가 생성될 때 해당 정보가 중요정보인지 여부를 판단할 수 있도록 '중요정보 식별 기준'을 마련하여 현업 부서에 제공하여야 한다.

현업 부서는 '중요정보 식별기준'에 따라 ①새로운 정보 생성 시 중요정보 여부를 판단하고, ②중요정보로 식별된 경우 '중요정보 목록'을 작성하여 부서장 승인을 받은 후 ③중요정보 관리 부서로 통보하여야 한다. 만약, 이를 이행하지 않을 경우 제재할 수 있는 근거를 마련하여 중요정보 관리 및 통제에 대한 책임성을 확립하도록 한다. 중요정보 목록의 통제방안은 다음을 포함할 수 있도록 한다.

표 Ⅱ-11 • 중요정보 목록에 대한 통제방안

- 중요정보 목록의 접근 통제(제한적 접근권한 부여)
- 중요정보 목록의 열람 이력 관리 및 보관
- 중요정보 목록 접근권한이 있는 직원의 관리
- 중요정보 목록의 변경 이력 관리
- 중요정보 목록 접근자 단말기(PC 등)에 대한 보안 점검 등

이때 중요정보의 목록을 출력물, 파일 등 여러 형태와 다양한 버전으로 관리하는 것은 보안 통제를 어렵게 하는 주된 요인이므로 목록 관리의 효율성, 비밀성, 무결성, 가용성 등을 확보하기 위해 전산화하여 관리할 필요가 있다. 중요정보 목록에는 다음과 같은 내용들이 포함될 수 있다.

표 Ⅱ-12 • 중요정보 목록

- 정보명(분류/내용) 및 정보의 형태
- 관리부서 및 관리책임자
- 정보의 생성 및 수정일시, 보존기간
- 정보의 보안등급 등

3.2 중요정보의 보안등급 부여

스마트공장에서 생성 · 관리되는 정보는 제품 설계도, 영업정보, 공장 운영현황, 각종 제어 정보 등 그 종류와 특징이 매우 다양할 뿐만 아니라, 해당 정보가 유출되었을 때 발생할 수 있는 유 · 무형의 피해 규모나 파급력 등도 매우 다양하다. 그러므로 이러한 정보들에 대해 동일한 기준의 보호조치를 취하는 것은 부적절한 관리 조치이며, 나아가 관리 노력 및 비용 등의 낭비로 이어질 수 있다. 뿐만 아니라 정작 철저히 보호해야할 핵심 정보에 대해서는 제대로 된 보호조치가 이뤄지지 않을 수도 있다. 그러므로 정보 유출 시 발생할 수 있는 유 · 무형의 피해(기업 이미지 하락, 경제적 손실) 규모나 파급력 등을 종합적으로 고려하여 중요정보별 보안등급을 부여하고 각 등급에 따른 보호조치를 차별화하여 관리할 필요가 있다.

중요정보의 보안등급은 조직에서 정한 중요도 평가기준에 따라 아래 예시와 같이 정할 수 있다.

표 Ⅱ-13 • 중요정보 보안등급의 구분 예

중요정보 보안등급	평가점수(합계)	설명
1급(비밀정보)	7점 이상	회사 내에서 알 필요가 있는 일부에게 제공되는 민감 정보 (예 : 고객 비밀정보, 개발S/W 소스코드, 제품 설계서, 회계 및 경영정보 등)
2급(대외비정보)	4~6점	회사직원 모두에게 공개되는 대외비 정보 (예 : 견적서, 제안서, 거래처 목록 등)
3급(일반정보)	3점 이하	외부에 공개되어도 되는 정보 (예 : 회사 소개자료, 제품 설명자료 등)

표 Ⅱ-14 • 보안등급의 평가기준 예

평가구분	보안등급 평가 요소	평가 수준
기업 이미지	– 중요정보가 유출(또는 훼손)되는 경우 기업의 이미지가 회복하기 어려울 정도로 추락할 수 있는 경우	상(3)
	– 중요정보가 유출(또는 훼손)되는 경우 기업의 이미지가 상당히 하락할 수 있는 경우	중(2)
	– 중요정보가 유출(또는 훼손)되어도 관계없거나, 기업 이미지에 미치는 영향이 경미한 경우	하(1)
경제적 손실	– 중요정보가 유출(또는 훼손)되는 경우 막대한 경제적 손실이 발생할 수 있는 경우	상(3)
	– 중요정보가 유출(또는 훼손)되는 경우 상당한 경제적 손실이 발생할 수 있는 경우	중(2)
	– 중요정보가 유출(또는 훼손)되어도 관계없거나 손실이 경미한 경우	하(1)
공장 운영	– 중요정보가 유출(또는 훼손)되는 경우 공장운영에 중대한 장애를 유발하거나 막대한 금전적 손실을 입히는 경우	상(3)
	– 중요정보가 유출(또는 훼손)되는 경우 공장운영에 상당한 장애를 유발하거나 상당한 금전적 손실을 입히는 경우	중(2)
	– 중요정보가 유출(또는 훼손)되어도 관계없거나 공장운영에 경미한 장애를 유발 또는 금전적 손실이 경미한 경우	하(1)

3.3 중요정보의 보안등급별 통제

보안등급별 통제항목은 중요정보 통제를 위한 인력, 예산 등 기업의 현황과 함께 다음의 내용을 고려하여 기업 특성에 맞추어 마련 후 적용할 수 있다.

표 Ⅱ-15 • 중요정보 보안등급별 통제항목 고려사항

- 중요정보의 권한은 업무의 필요한 최소 권한 부여 원칙을 적용
- 업무와 무관한 중요정보에 대한 접근을 차단
- 모든 중요정보에 대한 접근권한은 정보 소유자 또는 권한을 위임 받은 관리자에 의해 부여
- 1급 내지 2급의 중요정보는 부서장의 사전 승인 없이 외부 유출 및 공개 차단
- 중요정보에 대한 열람 제한
- 중요정보의 반입 및 반출 통제
- 중요정보 생성 및 보관 장소의 통제
- 중요정보 유출 방지를 위한 기술적 보호조치의 적용
- 중요정보 열람, 수정 등 로그 기록
- 모든 중요정보는 년 1회 주기적으로 보안등급을 평가

4 중요정보의 생성단계부터 유출 방지 방안을 적용하여 통제한다

중요정보 유출을 막기 위해서는 정보 생성단계부터 적절한 통제를 수행하는 것이 중요하다. 특히 중요정보의 생성 장소에는 시제품 정보, 제품 연구결과물, 설계도면 등 기업의 핵심 정보가 많이 있는 만큼 정보 생성자, 생성환경, 생성장소 등에 대한 통제 정책을 구체화하여 적용해야 한다.

4.1 중요정보 생성자에 대한 통제

'2016년 스마트공장 현황 및 정보보호 실태조사' 결과 중요정보 유출사고는 대부분 내부직원 및 협력사직원 등 사람에 의해 발생하는 것으로 파악되었고 잠재적 위협 요소와 관련해서도 '내부직원에 의한 중요정보 유출'을 주요 위협 요소로 꼽은 것으로 조사되었다. 중요정보가 정보 생성자를 통해 유출되는 것을 막기 위해서는 보안서약서 징구나 보안교육 등을 통한 직원의 윤리의식 제고뿐만 아니라 기술적으로 중요정보 접근을 통제하는 방안도 필요하다.

중요정보 생성자에 대한 기술적 통제방법으로는 개인 PC에 어떠한 중요정보도 저장하지 않고 제품 설계도면 작성 등의 업무 수행이 가능한 '데스크탑 가상화(VDI : Virtual Desktop Infrastructure)', 중요정보에 대해 사용자 권한과 보안정책을 설정해 보안성을 높이고 전자문서 유통에 대한 사후 감사를 지원하는 '디지털 저작권 관리(DRM : Digital Rights Management)', 그리고 직원의 고의나 실수로 인한 중요정보의 외부 유출을 방지하는 '데이터 유출 방지(DLP : Data Loss Prevention)' 솔루션 도입 등을 들 수 있다.

다음은 중요정보 생성자의 정보유출을 방지할 수 있는 솔루션인 VDI, DRM, DLP에 개념 및 주요기능에 대한 설명이다.

표 Ⅱ-16 • 주요 정보유출 방지 솔루션

- **데스크탑 가상화(VDI)** : 중앙에서 가상화로 동작하는 서버의 자원을 활용해 사용자별로 가상의 데스크탑 환경과 데이터 저장 공간을 제공하는 솔루션. 개인PC에는 데이터가 저장되지 않기 때문에 개인PC가 악성 프로그램에 감염되더라도 정보유출 위협으로부터 안전하며 중요정보가 중앙 서버에서 저장 · 관리되므로 데이터 관리 및 정보유출의 실시간 모니터링이 가능
- **디지털 저작권 관리(DRM)** : 내부정보 유출 방지 솔루션의 한 종류로 디지털 문서의 암호화를 통한 불법복제 방지, 문서의 열람 · 편집 · 저장 · 출력 등 사용자별 권한 통제, 중요정보의 인쇄 권한 및 출력 횟수 통제 등의 다양한 중요정보 유출 방지 기능 제공
- **데이터 유출 방지(DLP)** : DRM 및 PC보안 제품과 다르게 중요정보 생성자 및 접근권한이 있는 직원도 보안대상에 포함시켜 내부정보 흐름을 통제하여 중요정보의 불법 유출을 차단 · 방지할 수 있는 솔루션. 정보 유출 방지 · 감시, 인쇄 모니터링, 워터마크, 네트워크 통신포트 제어, 특정 사이트 접속 차단 등의 다양한 보안 기능을 제공

4.2 중요정보 생성 환경에 대한 통제

USB 등 이동형 저장매체의 통제

USB 등 이동형 저장매체는 크기가 작으면서도 충분히 많은 양의 데이터를 손쉽게 옮길 수 있어 중요정보를 불법적으로 저장하여 외부로 반출하기에 용이하다. 따라서 중요정보 생성에 사용되는 PC는 이동형 저장매체 사용을 원천 차단해야 하며, 필요 시 보안기능이 포함된 저장매체를 정해진 통제 절차에 따라 사용해야 한다.

표 Ⅱ-17 • 이동형 저장매체에 대한 통제 방안 예

- 이동형 저장매체의 반 · 출입 시 사전승인을 위한 절차를 수립하고 이를 효율적으로 관리하기 위한 관리대장과 폐기 절차도 세부적으로 마련한다.
- 이동형 저장매체를 도입하기 이전에 사전 보안성 검토 절차를 마련한다.
- 도입이 허가된 이동형 저장매체의 사용을 통제 · 관리하기 위한 규정과 지침을 마련하고 정보보호 관리자의 감독 하에 이행한다.
- 도입이 허가된 이동형 저장매체의 수량 및 보관 상태를 주기적으로 점검하고, 반출 · 입을 통제한다.
- 사용자 인증, 데이터 암호화 등의 보안기능이 제공되는 보안 USB를 사용한다.

표 Ⅱ-18 • 보안 USB의 보안기능 고려사항

규정 사항	세부 기능
사용자 식별인증	– PC 또는 노트북에 매체를 삽입하면 보안 S/W가 자동으로 작동 – 보안 S/W는 강제 종료하거나 삭제할 수 없음 – 취급자 식별 및 인증은 공인인증서 또는 ID/PW 방식으로 이루어짐 – 사용자 인증 후 매체 접근 가능
지정데이터 암복호화	– KCDSA(Korean Certificate-based Digital Signature Algorithm) 등의 암호화 표준 준수
지정된 자료의 임의복제 방지	– 사용자 인증 및 매체 인증 없이 매체에 접근 불가 – USB내의 비밀문서를 매체 내에 암호화
분실 시 데이터 보호를 위한 삭제	– 지정된 횟수 이상 패스워드 잘못 입력 시 USB내 파일 완전 삭제
기타	– 보안 USB 메모리에 대한 사용횟수, 사용기간, 사용가능 PC에 대한 설정 기능 – USB 사용 시 접속한 PC 및 네트워크 정보를 개인 E-Mail과 서버로 전송하여 분실, 도난 시 추적할 수 있는 정보 제공 기능

※ 출처 : 국정원, USB 메모리 등 보조기억매체 보안관리지침

스마트기기의 통제

중요정보가 생성되는 환경에서는 개인용 스마트기기 사용을 제한해야 한다. 다만, 업무상 불가피하게 필요한 경우 모바일 기기 관리(MDM : Mobile Device Management) 솔루션을 비롯하여, 바이러스 및 악성코드 탐지 · 차단 등의 보안 솔루션이 설치된 스마트기기를 사용해야 한다. 또한 사전에 등록된 스마트기기만 접근을 허용해야 하며, 가상사설망(VPN : Virtual Private Network) 등을 통해 암호화 통신을 해야 한다.

허용하지 않는 네트워크 차단

인터넷을 통한 중요정보 유출 및 악성코드 감염을 예방하기 위해서는 업무상 불필요한 인터넷 사이트를 차단해야할 뿐만 아니라 웹메일, P2P, 메신저, 웹하드, FTP, TELNET, 공유폴터 등 정보 유출의 수단으로 사용될 수 있는 네트워크 서비스를 모두 차단해야 한다. 또한, 정보 생성자의 PC에 무선네트워크 장치(USB 타입 동글 등) 등도 차단해야 한다.

4.3 중요정보 생성 장소에 대한 접근통제

중요정보가 생성되는 장소에 대한 물리적 통제방안을 마련하여 적용해야 한다. 비인가자의 출입을 통제할 수 있도록 업무형태, 환경 요소 등을 고려하여 다양한 출입통제 시스템을 구축 · 운영해야 한다.

수행업무에 따른 출입가능 구역의 설정 및 통제

일반 사무실과 달리 제품 설계도 등 기업의 핵심 정보를 생성하는 연구개발(R&D) 센터, 중요정보 저장 시스템 등 기업의 각종 정보시스템이 운영되는 전산실 등은 높은 등급의 보안구역으로 지정하여 내부 직원이라도 자유롭게 출입할 수 없도록 엄격한 출입통제 정책을 마련하여 적용해야 한다.

다음과 같이 보안등급에 따라 '공용구역', '접견구역', '제한구역', '통제구역'으로 구분할 수 있으며, 중요정보 생성장소는 통제구역으로 지정하여 관리해야 한다.

표 Ⅱ-19 • 보안등급에 따른 장소 구분 예

- **공용구역** : 보안상 차별화된 통제가 필요하지 않은 지역으로 임직원이나 외부인 등 모든 사람에게 공개된 구역
- **접견구역** : 임직원이나 출입이 허가된 정기 방문자나 임시 방문자에 한하여 출입이 가능한 구역
- **제한구역** : 보안상 비인가자의 접근을 방지하기 위하여 사전에 보안책임자로부터 허가를 받은 자만이 출입 가능한 구역
- **통제구역** : 중요정보의 생성 등 보안상 극히 중요한 장소로써 업무관련자 및 사전에 보안총괄책임자로부터 허가를 받은 자만이 출입 가능하고, 허가 받은 외부방문객 출입 시에도 직원의 동행이 반드시 필요한 구역

통제구역은 적절한 개폐장치를 설치하고 출입자를 식별하여 기록할 수 있는 장치를 두거나 이를 수행할 수 있는 인력을 배치하여야 한다. 다음의 장소들이 주로 주요 통제구역으로 구분될 수 있다.

표 Ⅱ-20 • 주요 통제구역 예

- 연구개발 센터
- 제품 설계실
- 외부협력사 개발실
- 전산기계실
- 주요 설비가 설치되어 있는 장소나 공간
- 데이터 보관실
- 기타 정보기록매체 보관 장소 등 통제가 요구되는 장소

중요정보 생성장소 출입기록의 보관

중요정보 생성장소 등 통제구역에 대한 출입기록은 출입자의 신원과 방문 목적, 방문 일시 등을 포함해야하며, 이 기록은 출입관리대장으로 관리되어야 한다. 통제구역 출입관리대장 이외에도 CCTV 녹화기록, 개폐장치의 로그기록 등이 보조 기록으로 활용될 수 있으며, 해당 기록은 일정기간 보관되어야 한다.

통제구역의 출입자 관리

중요정보 생성장소 등 통제구역에서 시행하는 규제수단은 법적 허용한도 내에서 세밀하고 철저하게 수행되어야 한다. 특히, 협력사 등 외부인 방문 시 외부인임을 식별 할 수 있도록 임시 방문증을 착용하게 하고, 담당자가 반드시 동행하여야 하며, 방문객의 출입이력을 꼼꼼히 관리대장에 기록하여야 한다.

5 중요정보 접근 시 권한기반의 체계적 통제 방안을 적용한다

중요정보 열람, 활용 등을 위한 접근 시 비인가자는 접근할 수 없도록 중요정보 접근통제 정책을 마련해야 한다. 중요정보 접근 시 접근자의 권한을 확인하여 내부 임직원이더라도 업무와 관련된 자만 접근이 가능하도록 통제할 수 있는 기술적 장치를 마련해야 한다. 또한 중요정보의 조회, 열람 및 복사 등 중요정보에 발생하는 이벤트에 대해서는 모두 전산화하여 이력을 관리해야 하며, 중요정보에 대한 모니터링을 통해

유출사고를 방지해야 한다.

5.1 중요정보 접근자의 권한을 확인하여 통제할 수 있는 기술적 장치 마련

제품 설계도, 특허정보 등 중요정보 열람 · 활용 등을 위한 접근 시 비인가자가 접근할 수 없도록 중요정보 접근통제 정책을 마련하여 적용해야 한다.

중요정보 접근에 대한 권한기반의 기술적 · 관리적 통제 방안

표 Ⅱ-21 • 중요정보 접근에 통제 고려사항

- 접근 통제 영역 및 범위, 규칙, 방법 등을 모두 포함하는 총괄적인 접근 통제 정책 수립
- 공식적인 사용자 등록 및 해지 절차 수립
- 중요정보에 접근하는 사용자의 계정 생성 및 변경 시, 접근 통제 정책에 따라 업무상 필요한 최소한의 권한만을 부여
- 중요정보는 안전한 암호 알고리즘을 사용하여 암호화하여 저장
- 서버/DB접근제어 솔루션을 활용하여 중요정보에 대한 접근이력 및 변경내역을 수집 · 관리
- 사용자 계정 등록/삭제(비활성화) 및 접근권한 등록/변경/삭제 권한이 특정 사람에게 집중되지 않도록 권한을 분산
- 관리자 및 특수 권한은 최소한의 인원에게만 책임자 승인 절차를 거쳐 권한을 부여하고, 관리자 및 특수 권한을 식별하여 별도 목록으로 관리
- 외부자에게 부여하는 계정은 한시적으로 부여하고 사용이 끝난 후에는 즉시 삭제 또는 정지 조치
- 중요정보에 대한 접근을 관리하기 위해 사용자의 계정 이용 현황(장기간 미사용 등) 및 인사 변동사항(퇴직 및 휴직, 직무변경, 부서변경) 등을 고려하여 접근권한 부여의 적정성 여부를 정기적으로 점검
- 중요정보에 대한 접근은 사용자 인증, 로그인 횟수 제한 등 안전한 사용자 인증 절차에 의해 통제되어야 하며, 필요 시 강화된 인증방식을 적용
  ※ 다수 로그인 실패 시 잠금 정책 구현과 2 factor 인증 방식 권장
- 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자의 사용은 제한하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 하에 사용
- 외부 위협요인 등을 고려하여 패스워드 복잡도 가중, 초기 패스워드 변경, 패스워드 변경주기 설정 강화 등을 포함한 패스워드 관리 절차를 수립 · 이행
- 패스워드 관리 책임을 사용자에게 주지시켜야 하며, 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리

5.2 중요정보 접근 및 활용에 대한 이력 관리 및 모니터링 방안

중요정보 접근 및 활용에 대한 이력 관리 방안

중요정보에 대한 접근 및 활용 내역은 전산화하여 관리해야 하며, 해당 내역은 일정기간 보관하도록 한다. 중요정보에 대한 이력에는 다음의 내용들이 포함될 수 있다.

표 Ⅱ-22 • 이력 관리 항목 예

- 중요정보 항목
- 열람 및 활용 구분
- 접근자 소속 부서 및 성명
- 접근일시, 접근기간
- 로그인 성공 / 실패에 대한 로그
- 활용내역
- 아이디 등 계정정보
- 기타 중요정보 유출사고 발생 시 감사에 관한 정보

모든 중요정보는 분리된 안전한 네트워크에 저장 · 관리할 수 있도록 하고, 네트워크를 통해 접근하는 모든 데이터에 대해 접근이력을 관리할 수 있는 체계를 구축해야 한다. 또한 중요정보 관련 모든 이력을 기록해야 하며 기록 내용은 일정기간 별도 저장매체에 백업 보관해야 한다. 이때 백업DB는 위변조 및 삭제가 불가능한 WORM(Write Once Read Many) 저장매체에 저장해야 한다.

중요정보 접근 이력 모니터링

기업의 모든 중요정보에 대한 비인가자 접근 및 인가자의 중요정보 접근 · 활용 시 관련 이력에 대한 로그를 기록하여 정기적으로 모니터링 해야 한다. 기업의 핵심 중요정보의 경우 비정상적인 접근을 탐지 · 차단할 수 있는 지능화된 관제시스템을 도입 · 운영해야 정보 유출 사고를 방지할 수 있다. 중요정보에 대한 모니터링을 위한 체계 구축 · 운영 시 다음 사항을 참고할 수 있다.

표 Ⅱ-23 • 중요정보 모니터링 체계 구축·운영 고려사항

- 중요정보의 종류, 관리 현황, 사용 현황 등을 가시적으로 파악할 수 있는 모니터링 시스템(대시보드) 구축
- 중요정보를 활용하는 어플리케이션 및 직원에 대한 정보를 실시간 파악하고 이상 징후 발생 시 알람, SMS, 이메일 등으로 관리자에게 통보하는 기능 포함
- 중요정보의 비정상 접근 및 유출 징후를 모니터링 할 수 있는 빅데이터를 활용한 실시간 모니터링 시스템(real-time monitoring) 구축
- 지능형 정보유출 시도에 대비하기 위해 비정상적인 접속이나 활동 등을 정확하게 인지하여 다양한 정보유출 시도 패턴과 새로운 유출 시도 형태를 즉각적이고 신속하게 탐지해내는 지능형 모니터링 체계 구축
- 비정상 행위 탐지를 위해 기존 규칙기반 이상 징후 탐지기술 외에 추가적으로 행위 프로파일링 기반의 이상 징후 탐지분석 기술 도입

6 중요정보 활용 시 악성코드 감염 및 전파 방지를 위한 대책을 마련하고 보안관제를 실시한다

스마트공장의 업무네트워크나 ICS네트워크의 악성코드 감염에 따른 중요정보 유출 및 제어망 감염을 방지하기 위해서는 네트워크 분리, 안티바이러스 시스템 운영, 시스템 패치 등의 대책이 필요하다. 또한, 악성코드가 유입되더라도 조기에 이를 탐지하여 격리 · 처리할 수 있는 관제 체계를 구축할 필요가 있다.

6.1 스마트공장의 적절한 네트워크 분리 방안

'스마트공장 현황 및 정보보호 실태조사(2016, KISA)' 결과, 중소형 공장의 경우 중요정보가 유통되는 연구개발 부서의 네트워크와 일반 업무네트워크, 공장 제어를 위한 ICS네트워크 간에 명확히 분리되지 않은 것으로 파악되었다. 망 분리가 안 되어 있을 경우 업무 네트워크에 유입된 악성코드가 ICS네트워크나 중요정보가 유통되는 네트워크로 전파될 수 있어 공장 가동에 심각한 장애를 일으킬 수 있을 뿐만 아니라 기업의 중요정보 등이 쉽게 유출될 수 있다. 이러한 피해를 예방하기 위해 네트워크 분리 시 다음의 방안을 고려해야 한다.

표 Ⅱ-24 • 네트워크 분리 시 고려사항

- 방화벽과 라우터의 구성 기준을 수립 및 실행
- 스마트공장 내의 정보 흐름을 보여주는 최신 네트워크 다이어그램 문서화
- 인터넷 연결과 DMZ(demilitarized zone), 내부 네트워크 영역 사이의 방화벽 요건 확인
- 네트워크 구성 요소를 관리하기 위한 그룹, 해당 역할 및 책임에 관한 설명 확인
- 사용이 허가된 모든 서비스, 프로토콜, 포트를 문서화하고 특히 안전하지 않은 프로토콜이 사용되는 경우 사용이 허가된 사유를 포함
- 방화벽 및 라우터 정책을 최소 반기 단위로 검토하여 부적절한 정책은 삭제
- 인바운드, 아웃바운드 트래픽에서 정보 접근에 필요한 트래픽을 식별하고, 불필요한 트래픽 접근을 제한
- 방화벽, 라우터의 구성을 검토하여 차단(Deny) 또는 허용(Permit) 설정 후에 전체차단(Deny All)을 사용하여 다른 모든 인바운드 및 아웃바운드 트래픽 차단
- 모든 무선 네트워크와 스마트공장 망 사이에 경계 방화벽을 설치하여 승인된 무선 트래픽만 허용
- 변조된 소스 IP 주소를 감지하여 네트워크에 침입하지 못하도록 위조 방지기술 적용
- 스마트공장 내부 망에서 인터넷으로 인증되지 않은 아웃바운드 트래픽은 비 허용
- 사설 IP(Private IP) 주소와 라우팅 정보를 허가되지 않은 제3자에게 공개하지 않음
- 직원이 소유하는 모든 모바일 장치의 네트워크 접근 통제
- 안전하지 않은 서비스, 프로토콜, 포트에 대하여 사용 허가 시 문서화된 이력으로 관리
- 방산기업 또는 방산협력기업의 경우, IT보안인증사무국에서 부여하는 CC인증이 적용된 보안솔루션을 사용 (단, 인증기간을 확인하여 만료된 제품의 경우 재인증 또는 솔루션 교체 요망)

6.2 안티바이러스 소프트웨어를 이용한 악성코드 유입 방지 방안

네크워크 망 분리, 방화벽 및 침입방지시스템(IPS) 등 네트워크 보안 장비만으로는 악성코드의 내부 유입을 완벽히 차단하기 어려운 것이 현실이다. 따라서 스마트공장 내부 네트워크로 유입되는 악성코드를 차단 및 탐지할 수 있도록 내부 네트워크에 연결되는 모든 서버 및 업무용 PC 등에 안티바이러스 소프트웨어를 설치해야 하며, 다음과 같이 운영할 수 있다.

표 Ⅱ-25 • 기업 내 안티바이러스 소프트웨어 운영 방식

- 회사에서 지정한 안티바이러스 소프트웨어의 설치
- 바이러스 탐지규칙(시그니처 파일)의 정기적인 업데이트 및 최신 상태 유지
- 안티바이러스 소프트웨어는 실시간 감시 체계로 운영하고 정기적으로 정밀 검사를 진행
- 안티바이러스 소프트웨어 미설치 단말의 네트워크 접속 차단
- 악성코드로부터 시스템을 보호하기 위한 보안 정책 및 운영 절차를 문서화

6.3 안전한 정보시스템 패치 방안

시스템에 취약성이 존재할 경우 악성코드 공격 시 영향을 받을 확률이 매우 높아진다.

'스마트공장 현황 및 정보보호 실태조사(2016, KISA)' 결과에 따르면 절반 이상의 공장 제어시스템이 주기적으로 보안업데이트를 진행하지 못하는 것으로 나타났다. 패치를 주기적으로 하지 못하는 이유에 대해서는 제어장비가 1년 365일 24시간 쉼 없이 가동되는 경우가 많아 패치 할 시간이 없다는 것과, 패치로 인한 오작동이나 시스템다운 등을 우려하여 패치를 하지 못하고 있다고 응답하였다. 또한, 공장 내 장비들이 대부분 오래전 도입된 것들로 Window XP, Windows Server 2003 등 공식적인 유지보수 지원이 종료된 운영체제를 사용하는 시스템이 많은 것으로 조사되어 패치 관리의 중요성이 더욱 커지고 있다. 많은 제어장비를 효율적이고 일괄적으로 패치하고 관리하기 위해서는 스마트공장 내부 네트워크상에 패치관리시스템(PMS: Patch Management System)을 구축하여 운영할 필요가 있다. 특히, PMS는 외부네트워크와 분리된 환경에서 다량의 장비를 일괄적으로 패치하기 때문에 서비스 단절을 최소화할 수 있다. 또한, 패치 적용 계획을 세워 패치 전에 해당 시스템의 안전성 테스트 등을 미리 거치면, 문제가 발생할 시 패치 적용 이전 상태로 되돌릴 수 있는 '롤-백(roll-back)' 등을 통해 안전하게 패치를 통제 · 관리 할 수 있다.

표 Ⅱ-26 • 안전한 보안패치를 위한 고려 사항

- 보안 취약성을 확인하고 새로 발견된 보안 취약성에 위험 순위(예: High, Medium, Low)를 할당
- 공급자가 제공하는 보안 패치를 설치하며, 심각한(Critical) 패치는 일정 우선으로 적용
- 보안 패치 변경 시, 시스템에 미치는 영향을 문서화
- 권한을 가진 직원의 문서화된 승인
- 패치 적용 시의 보안 기능 테스트
- 패치 적용 중 문제 발생 시 복원 절차 수립
- 패치 관리 시스템(PMS)에 의한 자동화된 패치 설치로 기업 전체 시스템에 일관된 보안 패치 적용
- PC 별 패치 상태 파악 및 패치 미설치 시 네트워크 차단하여 설치 유도
- 최근 브라우저와 플래시 플러그인 등의 신규 취약점이 다수 발견되고 있어 취약한 버전을 사용하는지 확인하여 적절한 보안 패치 적용
- 특정 취약한 브라우저 버전을 강제화하는 정책이 있을 경우 기술적 영향을 검토하여 정책 변경

6.4 악성코드가 유입될 수 있는 경로 분석 및 대응

악성코드가 유입될 수 있는 경로로는 사내 메일을 이용한 피싱(phishing), 특정 대상(개인, 조직, 기관 등)을 목표로 한 스피어 피싱*(spear phishing), 웹하드, 클라우드 서비스, 업무 비관련 사이트, 이동매체, 무선 인증 설정의 취약성을 악용한 비인가 접근, 랜섬웨어 감염 등이 있으며, 많은 유형이 계속해서 생겨나고 있는 만큼 악성코드가 유입될 수 있는 다양한 경로를 충분히 분석하여 대응해야 한다.

* 스피어 피싱 : 불특정 다수가 아닌 특정 기관이나 기업의 내부직원을 대상으로 집중적으로 공격하는 행위

표 Ⅱ-27 • 악성코드 유입 방지 방안

- 외부 이메일 서비스의 사용 금지
- 이메일 보안 솔루션 도입(예: PGP, S/MIME, IMAPS, SPF)을 통한 상호 송수신 자간 인증, 메일 내용 암호화 및 무결성 검사
- 이메일 첨부 파일 악성코드 검사
- 서버 및 PC의 USB포트 읽기/쓰기 차단
- 웹 하드 사용 금지
- 사내 파일 서버에 개인용 음악, 영화, 출처가 불문명한 프로그램 등 콘텐츠 배포 금지
- 클라우드 서비스 접속 금지
- 업무 비관련 사이트의 접속 차단
- 업무용으로 허가된 휴대형 접근 매체가 아닐 경우 사용 금지
- 허가되지 않은 무선 액세스 장비의 반입 및 사용 금지
- 정품 소프트웨어의 사용
- 네트워크를 세분화하여 악성코드 (랜섬웨어 등)의 확산을 모니터링
- 악성코드 유포 주소(IP)를 관문 방화벽에서 접속 차단
- 중요 데이터는 정기적으로 오프라인 백업 권고
- 빅데이터 기반 네트워크 모니터링 시스템 구축 · 운영

또한 최근 빈번하게 나타나고 있는 문제로 APT(Advanced Persistent Threat) 공격이 있는데, 악성코드가 내부 관리자 PC에 설치되어 장기간에 걸쳐 조직 내부 특권적 지위 및 권한을 가진 PC를 해킹하는 것이다. 이때 해킹을 통해 중요정보에 접근할 수 있고, 임계치를 초과하지 않는 한도 내에서 장기간에 걸쳐 방대한 정보를 계속해서 유출할 가능성도 있다. 정작 내부자는 오랜 기간에 걸쳐 이루어지는 이러한 해킹에 대해 감지조차 하지 못한다는 점에서 위험성을 더욱 크게 느낄 수 있다. 따라서 APT공격을 예방 · 탐지할 필요가 있는 스마트공장 환경에서는 빅데이터 기반의 정보 유출 탐지 기술의 도입도 적극 검토해야 한다.

7 중요정보 보관 정책을 마련하고 통제한다

스마트공장의 중요정보 유출 방지를 위해서는 중요정보에 대한 보관 정책을 마련하여 접근, 열람, 변조 등을 통제해야 한다. 또한 정책에 따라 일정 등급 이상의 문서는 필히 암호화 하여 보관 하도록 하여 중요정보 유출시 피해를 최소화 하여야 한다.

중요정보 보관 정책은 다음의 내용을 포함하여 수립할 수 있다.

표 Ⅱ-28 • 중요정보 보관정책 고려사항

- 업무기능 별(ex. 생산, R&D, 재무, 회계 등) , 등급 별(ex. 비밀, 대외비, 일반) 중요정보의 분류 체계를 수립
- 문서의 보관 위치 지정 (ex. 전자 문서 시스템에 보관하거나 출력물의 경우 상단 또는 좌측을 철하여 캐비닛에 보관)
- 문서의 보존 기간 명시 및 보존 기간 변경 시 책임자 승인을 득하도록 명시
- 완결된 문서는 시건장치가 되는 문서보관함(ex. 파일, 캐비닛)에 보관
- 보존 문서는 문서 보존실에 보존, 보존 문서 관리부서의 책임 하에 관리 · 운영
- 문서 보존실은 출입 통제 구역으로 지정, 출입에 대한 승인 절차 마련
- 이중 도어 설치 및 필요 시 경비원 확인 하에 한 명씩 출입 허용
- 보존 문서 관리 대장 비치 및 운영

7.1 중요정보는 암호화하여 보관한다.

스마트공장의 제품 도면, 청사진, 공정 제어용 설정 값, 생산자 정보 및 고객 정보, 내부 보고서, 전략 문건 등 유출시 피해가 클 것으로 예상되는 중요정보의 경우 높은 보안등급을 부여하고 보관 시 암호화 하여야 한다. 다음은 중요정보 암호화 시 고려해야 할 사항이다.

표 Ⅱ-29 • 중요정보 암호화 고려사항

- 저장된 중요정보를 평문으로 읽을 수 없도록 해시 값으로 변환하여 암호화
- 안전한 암호 알고리즘을 사용해야 하며, 암호화 키는 안전하게 보호될 수 있도록 암호화 키 관리에 대한 절차를 규정하고 문서화
- 중요정보 암호화에 사용되는 암호화 키에 대한 접근은 최소한의 관리자와 장소로 제한
- 중요정보 암호화 키에 대한 보호를 위해 키 자체를 암호화 하여 관리할 수 있는데, 이때 사용되는 마스터 키의 경우, 암호화 키와는 별도로 접근 통제를 받는 저장소에서 안전하게 관리
- 사용 기간이 만료된 암호화 키에 대해서는 변경을 의무화
- 암호화 키의 유출 등이 의심되는 경우, 해당 키를 폐기 또는 교체(변경)
- 평문 형태의 암호화 키를 하드웨어 장치에 저장하거나 스마트공장과 연계된 다른 기관에 배포할 시에는 비밀분산(Secret Sharing)* 기법 등 적용 가능
  * 암호화 키 정보를 수학적 연산을 통해 여러 개의 정보로 분할하고, 이 중 일부 정보의 결합만으로도 원본 암호화 키를 재구성할 수 있도록 함으로써원본 키의 노출 없이도 암호화 가능하도록 하는 기법
- 암호화 키에 대한 관리자를 지정하고 관리 책무를 부여
- 암호화 키는 한국인터넷진흥원, 미국 국립표준기술연구소(NIST) 등에서 권장하는 안전한 알고리즘을 사용 권고
- 화면이나 프린트 용지 등에 일부 자리만 출력하여 전체 내용을 확인하지 않아도 업무 처리가 가능한 경우, 문자 자르기(Truncation) 등을 적용

상기 제시한 방법 외에 안전한 암호화 알고리즘을 선택은 매우 중요하다. 다음은 NIST에서 사용을 허용 혹은 금지하고 있는 암호화 알고리즘이다.

표 Ⅱ-30 • NIST, 암호 알고리즘 유형별 금지·허용 대조표

알고리즘 유형	사용 목적	금지	허용
비대칭키 암호화	키 교환, 기밀성, 인증	RSA-1024	RSA-2048
대칭키 암호화	기밀성	RC4, DES, 2TDEA	3TDEA, AES, SEED, ARIA
일방향 암호화 해시	무결성	MD5, SHA-1	SHA-2, SHA-3
메시지 인증 코드	무결성, 인증	HMAC-MD5, HMAC-SHA1	HMAC-SHA-2

※ 출처 : NIST SP800-57(Recommendation for Key Management) 정리

중요정보 저장 시 암호화를 적용하기 위한 방안으로는 DB 암호화, 디스크 암호화, 파일 암호화 등의 방법이 있다.

표 Ⅱ-31 • 중요정보 암호화 적용 방안

- **DB 암호화** : DB에 데이터 저장 시 암호화를 하고, 엄격한 암호 키 관리를 통해 데이터를 보호하는 방법이다. 암호화된 데이터가 해킹으로 인해 유출되거나 권한 없는 자가 DB를 열람하더라도 키 없이는 복호화할 수 없어 내용 파악을 할 수 없도록 하는 것이 DB 암호화의 목적이다. 따라서, 암호 키 접근을 강화하고, 소수의 인가자에 의한 접근만 허용하도록 하는 것이 DB 암호화에서 매우 중요하다.
- **디스크 암호화 방안** : 디스크의 저장 장치의 논리 볼륨을 통째로 암호화하여 타인의 접근을 원천적으로 차단하는 보안 기술이다. 이를 이용하면 외장 디스크인 USB 메모리나 외장 하드 디스크는 물론 운영 체제가 설치된 하드 디스크의 시스템 볼륨까지도 암호화할 수 있다. 디스크 암호화에 적용된 논리적 접근 통제는 로컬 사용자 계정 로그인과는 별도로 적용되어야 한다.
- **파일 암호화 방안** : 파일에 암호화를 적용시키는 것으로, 파일 이동 시에도 계속해서 해당 파일을 보호하고 적절한 권한이 있는 사용자만 내용을 복호화 하여 확인할 수 있다.

또한, 중요정보의 송 · 수신시에는 메시지 암호화를 적용할 수 있으며, 중요정보 암호화에 사용되는 암호화 키 등의 안전한 관리를 위해서는 HSM 등을 이용할 수 있다.

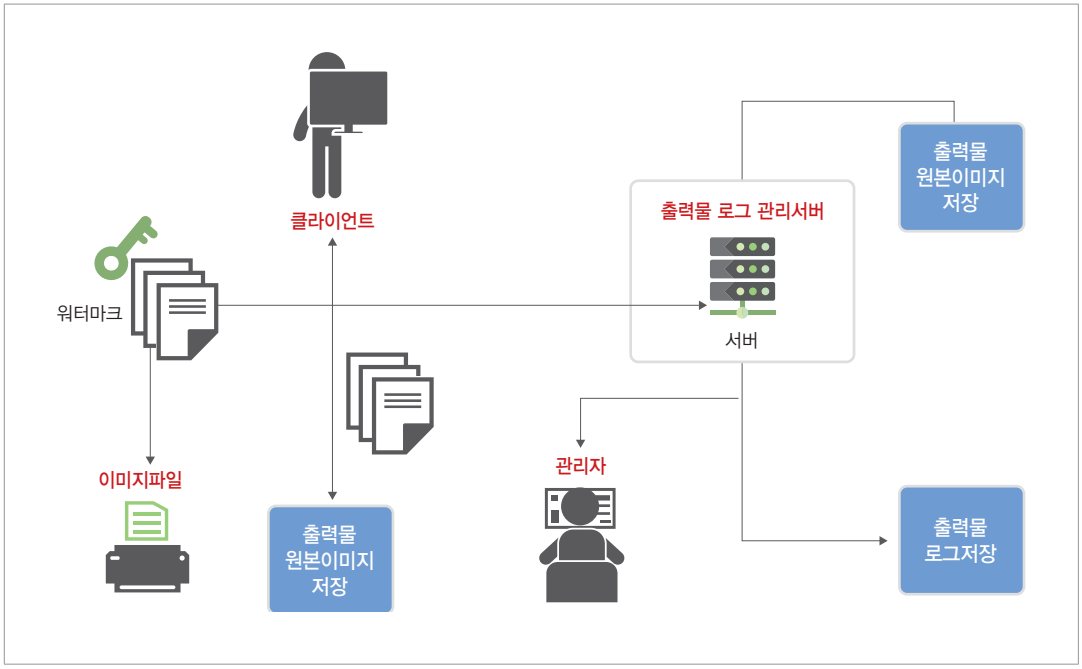
표 Ⅱ-32 • 송수신 메시지 암호화 및 암호키 관리 방안

- **메시지암호화** : 중요파일 등의 정보가 네트워크를 경유하여 다른 서버나 기관의 저장소로 안전하게 전달되어야 하는 경우 기밀성을 강화하기 위해 중요정보를 선별하여 암호화하는 것이 메시지 암호화이다. 정보를 송수신할 서버와 클라이언트는 상호 인증을 수행하여 송수신 대상이 맞음을 검증해야 한다. 이 과정 중 메시지를 암호화 하는 데 사용될 암호화 키도 안전하게 교환된다.
- **HSM (Hardware Security Module)** : 스마트공장의 중요정보를 저장해야 할 경우 암호화에 사용된 키를 안전하게 보호하기 위한 방법으로 하드웨어 보호를 적용하여 격리하는 방법이다. 즉, 암호화 키를 HSM(Hardware Security Module)에 저장하고 복호화 연산 수행 시 HSM 내에서 수행하는 것인데, 이를 통해 저장된 중요정보는 비 인가된 내부자 또는 해커가 해독할 수 없다.

7.2 중요정보 출력 시 접근인력 기록 및 통제방안

중요정보를 복사, 인쇄, 스캔하거나, FAX 등을 사용 할 시에는 이력 저장 및 모니터링을 할 수 있어야 한다. ID 카드 인증 등을 통해 인증 받은 사람만 이용 가능하도록 하여 열람과 출력 등을 통제하고 출력한 내역은 서버에 기록을 남기도록 한다. 스마트공자 내에 내부 문서 관리 시스템이 있는 경우, 이러한 시스템과 연동하여 높은 등급의 중요정보는 부서장의 승인을 받고 출력이 가능하도록 하여야 한다.

그림 Ⅱ-3 • 출력물 관리 구성도



중요정보의 출력 및 인쇄 등의 과정에서 불법적 유출의 위협을 줄이기 위해서는 다음과 같은 기법들을 활용할 수 있다.

표 Ⅱ-33 • 중요정보 유출 방지를 위한 보안기법 예

- **워터마킹기술** : 출력 · 복사물에 해당 기관의 명칭 및 로고, 일련번호, 출력기기 고유번호, 출력자 성명, 출력 시간 등을 표시하여 원본 출처 및 정보를 추적 할 수 있도록 한다.
- **보안용지** : 특수 센서가 내장된 보안용지로써, 출력 및 외부 유출 시 센서에 의해서 감지되어 경보가 울린다.
- **보안 게이트** : 보안용지의 특정 센서에 반응하는 게이트로써 승인되지 않은 보안용지의 무단 반출 시 경보가 발생하거나, 출입 게이트 개폐 통제를 통해서 외부로 나갈 수 없게 만드는 시스템이다.
- **보안 프린터** : 프린터, 복사, 팩스와 같이 종이로 출력되는 모든 인쇄물에 대해서 일반 용지와 보안용지를 구분한다. 일반용지 사용 시 출력물 내용이 보이지 않거나, 상급관리자에게 자동으로 알림이 가게 되고, 서버에 출력 명령 IP 및 시간/ 내용에 대한 사항들이 기록되어, 출력 후에도 추적 관리가 가능하다.

8 중요정보 외부 제공 시 유출 방지 방안을 마련하고 통제한다

폐쇄 망에서 동작하도록 설계된 공장 시스템의 경우 시스템 인증이나 네트워크 보안을 고려하지 않고 물리적 접근통제만 구현 된 경우가 있다. 이러한 경우, 스마트공장 환경으로의 확장 과정에서 생산효율화를 이유로 내부 공장 시스템이 기업 네트워크 등 외부와 연결되면 상대적으로 보안위협에 취약한 공장 내부 시스템을 통해 중요정보가 외부로 쉽게 유출될 수 있으므로 주의해야 한다.

8.1 기업 업무네트워크와 ICS 네트워크 구조

일반적으로 기업 업무 네트워크에서는 인터넷 접속, E-mail 등의 사용이 가능하지만 공장 내부 시스템인 ICS(Industrial Control System) 네트워크에서는 허용되지 않는다. 그러므로 기업 업무 네트워크의 보안위협이 ICS 네트워크에 영향을 미치지 않도록 업무 네트워크와 ICS네트워크를 분리하여 구성할 것을 권고한다. 다만, 스마트공장의 경우 생산효율성 등을 이유로 두 네트워크 간에 연결이 요구되는 경우가 종종 발생할 수 있으며, 이러한 연결은 매우 중요한 보안 위협이 될 수 있다. 그러므로 ICS네트워크와 기업 업무 네트워크 간에 연결이 필요한 경우, 다음과 같은 방안을 고려할 수 있다.

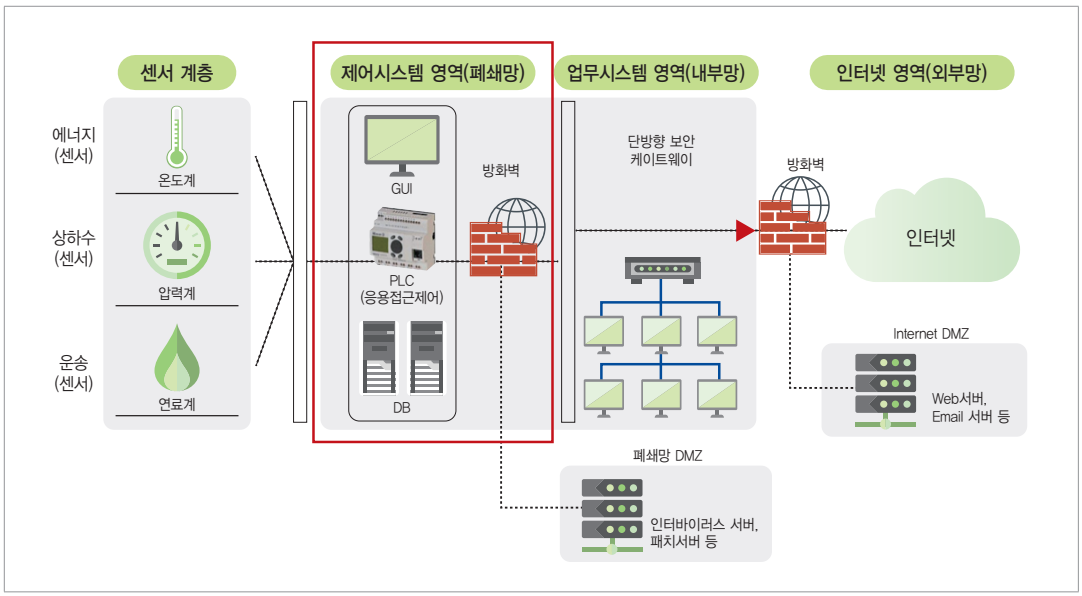
표 Ⅱ-34 • ICS 망과 기업 네트워크 연결 시 고려사항

- 네트워크가 연결되어야 하는 경우, 최소한의 (가능하다면 단일의) 연결만을 허용하고, 반드시 문서화한다.
- ICS 네트워크 및 장치에 대한 물리적인 접근을 통제한다.
- ICS 데이터 스토리지 및 통신에 대해 암호화 또는 암호화 해시함수와 같은 보안 기법을 적용한다.
- 실현 가능한 신뢰성 및 보안성을 갖춘 네트워크 프로토콜 및 서비스를 사용한다.
- ICS에 설치되기 전에, 실제 시스템 운영 조건과 유사한 환경의 테스트 시스템에서 모든 패치를 테스트를 한 후, 보안 패치를 신속하게 적용한다.
- ICS 장비뿐만 아니라 네트워크 장비, 보안 장비, 스토리지 장비 등에 탑재된 펌웨어 또는 소프트웨어에 보안 취약점이 있을 경우에도 테스트 시스템에 필드 조건과 유사한 환경에서 패치 테스트를 한 후에 보안 패치를 적용한다.
- 작업을 수행하기 위해 필요한 ICS 사용자 권한을 최소한으로 제한한다.
  (ex. 최소한의 권한을 지닌 각 역할에 기반한 접근통제)
- ICS 네트워크와 기업 네트워크의 사용자들을 위한 인증 메커니즘, 자격증명을 별도로 구분하여 사용 한다. (ex. ICS 네트워크 계정은 기업 네트워크 사용자 계정을 사용해서는 안 됨)
- ICS의 중요 영역에 대해 감사 추적 및 모니터링을 수행한다.
- ICS망과 회사 내부망의 연결은 일반적으로 허용하지 않지만 만약 연결이 필요할 경우 방화벽과 DMZ를 통해서 연결하고 단방향 통신을 적용하여 내부망에서 ICS망으로 접근하지 못하도록 권고한다.

- 외부 연결에 대해서는 특정 통신을 위해 요구되는 포트만 열고, 최소한의 접근만 허용하도록 한다.
- 방화벽 및 라우터 정책을 주기적으로 검토하여 부적절한 정책을 삭제한다.
- 방화벽, 라우터의 구성을 검토하여 허가된 트래픽 설정 후 Deny All을 사용하여 다른 모든 인바운드 및 아웃바운드 트래픽을 차단한다.
- 사용 허가된 모든 서비스, 프로토콜, 포트에 대하여 허가된 이유를 문서화한다.
- 네트워크 구성 요소를 관리하기 위한 그룹, 역할, 책임에 대한 내용을 문서화 한다.
- Private IP 주소와 라우팅 정보를 허가되지 않은 제3자에게 공개하지 않는다.
- 위 · 변조된 소스 IP 주소를 감지하여 네트워크에 침입하지 못하도록 한다.
- 센서 등을 활용하기 위하여 무선 네트워크를 연결해야 하는 경우 사용단말 환경 및 네트워크에 연결되는 시스템 등을 확인하여 보안위험을 미리 평가하고 대책을 마련한 후 연결한다.
- 직원이 소유하는 모든 모바일 장치에 접근통제 또는 개인 방화벽 소프트웨어를 설치한다.
- 중요정보를 망간 이동시에는 망간 자료 전송 시스템(일반향 자료 전송)을 경유하고 반드시 결정권자의 승인을 받도록 한다.
- 방산기업 또는 방산협력기업의 경우, IT보안인증사무국에서 부여하는 CC인증이 적용된 보안솔루션을 사용해야 한다.

추가적으로 기업의 업무 네트워크와 ICS네트워크 간에 직접적인 통신 연결을 하지 않고 중간에 DMZ 영역을 구축하도록 하고, DMZ 영역에는 패치관리시스템(PMS, Patch Management System), 안티바이러스 서버 등을 위치시켜 패치관리나 안티바이러스 관리를 수행하도록 하는 방안도 있다.

그림 Ⅱ-4 • 산업제어시스템 네트워크 구성도



또한 외부에서 업무 등의 목적으로 접근을 해야 하는 경우가 있다면 구간 암호화 방식 VPN(Virtual Private Network)을 이용하여야 한다. VPN이란 공중 네트워크를 사설 네트워크처럼 사용할 수 있도록 인증과 데이터 암호화를 이용해 보안을 강화한 기술로, 전용선으로 연결되어 있지 않은 외부 연계 기관과 가상으로 전용선을 구현하게 해주는 기능이다.

9 중요정보 파기절차 및 방법을 마련하고 통제한다

스마트공장 내 중요정보를 삭제하거나 파기할 경우 추후 복구나 재활용이 가능하지 않도록 완전히 삭제하고 파기해야 한다. 이동형 저장매체, 출력물, PC, 서버 등을 매각하거나 폐기할 때 중요정보가 불완전하게 파기된 채로 외부인의 손에 들어가게 되면 중요정보가 손쉽게 복구되어 유출될 수 있다. 따라서 중요정보 삭제 및 파기에 대해 세부 규정과 절차를 마련하여 이를 준수하도록 한다.

9.1 중요정보 파기 절차

중요정보 보존 시 명시된 기한에 따라 파기 예고일이 도래하였을 때 중요정보의 파기를 결정한다. 단, 업무상 계속 참조할 필요가 있는 중요정보는 파기 시기가 도래한 경우라도 재분류하여 파기 일을 연장해야 한다.

표 Ⅱ-35 • **중요정보 파기 절차**

- 파기 예고일이 도래한 중요정보는 도래 시점에 파기를 검토한다.
- 파기가 결정된 중요정보는 9.2 중요정보 안전한 파기 방법에서 소개하는 파기 방법을 참고하여 담당자가 파기 한다.
- 파기가 완료된 중요정보에 대해서 중요정보관리 기록부에 파기여부를 체크하여 현황(파기 주체, 일시, 파기 파일명 혹은 매체명 등)을 관리한다.

9.2 중요정보 안전한 파기 방법

이동형 저장 매체, PC · 서버 · 노트북 · 업무용 휴대전화/카메라/캠코더 등 전산장비를 매각하거나 폐기 할 경우 저장된 데이터가 복구 불가능하도록 초기화하거나 완전파괴 처리해야 하고, 인쇄 출력물 등의 자료는 식별 불가능하도록 물리적으로 파기 하여야 한다.

다음에서는 중요정보를 안전하게 파기하기 위한 다양한 방법을 소개한다.

표 Ⅱ-36 • 중요정보 파기 방법

- **전문 폐기업체 활용** : 전문 폐기업체에 파기를 의뢰할 수 있으며, 파기 과정에는 반드시 담당자가 참관하여 삭제절차 · 방법 준수 여부 등을 확인 · 감독 하여야 한다.
- **전용 소거장비(디가우저 등) 이용** : 저장매체에 역자기장을 이용해 매체의 자화값을 "0"으로 만들어 저장자료의 복원이 불가능하게 만드는 것으로 반드시 저장매체의 자기력보다 큰 자기력을 보유한 장비를 사용해야 한다.
- **완전포맷** : 저장매체 전체의 자료저장 위치에 새로운 자료(0 또는 1)를 중복하여 저장하는 것으로 중요정보를 처리한 시스템은 완전포맷 3회 이상으로 저장자료를 삭제해야 한다.
- **완전파괴(소각 · 파쇄 · 용해)** : 파쇄조각 크기가 0.25mm 이하가 되도록 물리적으로 파괴하는 것을 말하며, 종이류 문서(출력물, 도면 등)은 세단기를 이용하여 파쇄하거나 소각하여 문서 복구가 불가능하도록 조치할 수 있다.
- **중요정보 파기절차 확인** : 빅데이터 및 클라우드 시스템의 경우 데이터의 분산 저장 처리로 인해 기존의 폐기 기술로는 완벽하게 처리 확인이 어려우므로 서비스 제공자가 객관적인 데이터 폐기에 대한 모니터링 시스템과 논리적인 완전한 폐기 프로세스를 제공하는지 여부를 확인한다.

10 중요정보 유출 방지를 위해 정보시스템에 대한 취약점 점검 및 정기적인 보안감사를 실시한다

스마트공장의 중요정보 유출방지를 위해서는 중요정보가 보관되어 있는 정보시스템 및 중요정보를 생산 · 활용하는 임직원의 PC, 네트워크 등에 대한 정기적인 취약점 점검을 통한 보완 조치를 실시해야 하며, 중요정보 관리체계의 효과적인 운영 및 임직원 준수 여부를 점검하기 위해 정기적으로 보안감사를 실시해야 한다.

10.1 정기적인 취약점 점검 및 모의해킹 수행

중요정보를 보관하고 있는 시스템이 취약점에 노출되어 있는지 확인하기 위해 매년 1회 이상 또는 시스템의 신규 · 변경이 발생한 경우 취약점 점검과 모의해킹을 수행해야 한다. 이를 통해 발견된 취약점은 위험도 평가를 통해 우선순위에 따라 보완 조치해야 한다. 취약점 점검 및 모의해킹은 〈표 Ⅱ-37〉을 참고할 수 있다.

표 Ⅱ-37 • 취약점 점검 및 모의해킹 수행 방안

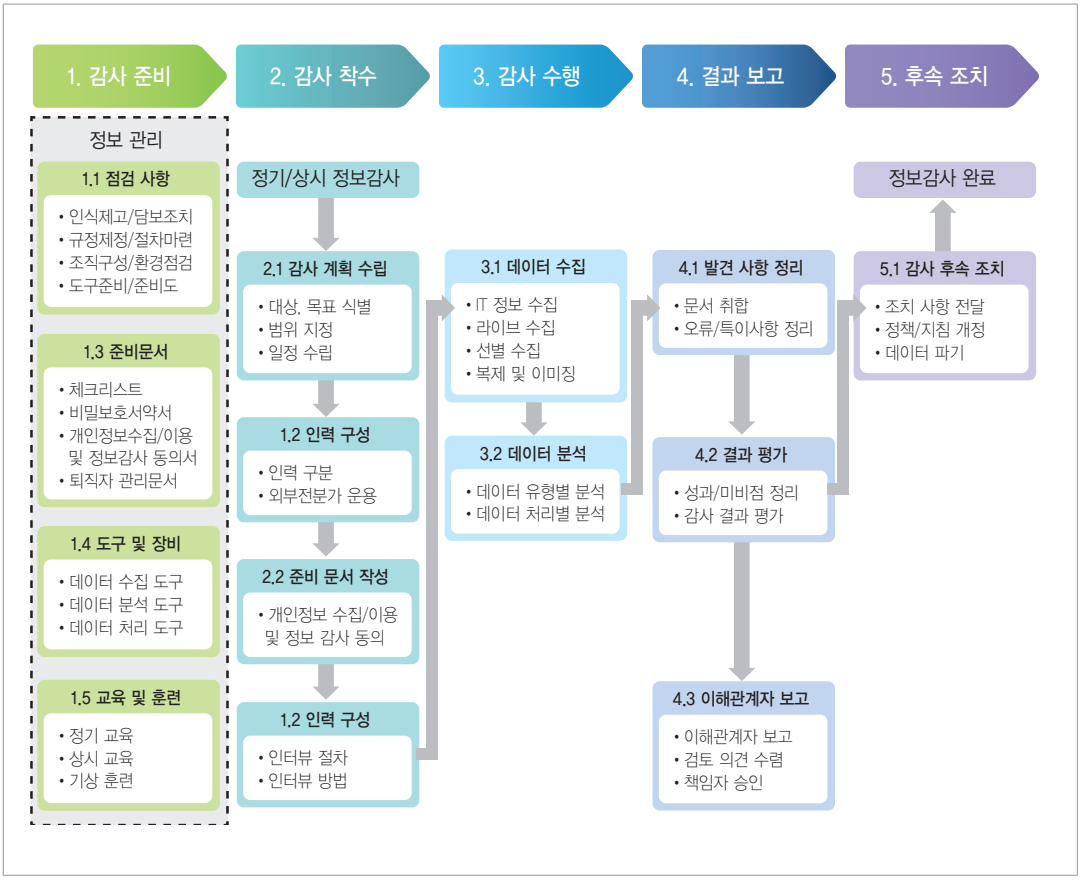
- 취약점 점검 정책과 절차에는 취약점 점검 대상 (서버, 네트워크 장비 등), 점검 주기, 점검 담당자 및 책임자 지정, 취약점 점검 절차 및 방법이 포함된다.
- 시스템 중요도에 따라 주기적으로 취약점 점검을 실시하고 결과보고서를 작성한다.
- 취약점 점검 시, 라우터, 스위치 등 네트워크 장비 구성 및 설정 취약점, 서버 OS의 보안 설정 취약점, 방화벽 등 정보보호시스템 취약점, 어플리케이션 취약점, 웹 취약점, 모바일 앱 취약점, IoT 기기 및 근거리 무선 네트워크 취약점을 대상으로 한다.
- 취약점 점검 결과 보고서에는 이력관리가 될 수 있도록 점검 일시, 점검 대상, 점검 방법, 점검 내용 및 결과, 발견 사항, 조치 사항을 포함한다.
- 회사의 규모 및 보유하고 있는 정보의 중요도에 따라 모의해킹 수행 여부를 결정한다.
- 취약점 점검 결과에서 발견된 취약점별로 대응방안 및 조치 결과를 문서화하여 조치 결과서를 작성하고, 스마트공장 책임자에게 보고한다.
- 불가피하게 조치할 수 없는 취약점의 경우 사유를 명확하게 파악하여 책임자에게 보고하고, 대응 방안을 모색한다.

10.2 정보시스템에 대한 정기적인 보안감사 수행

스마트공장 내 중요정보가 보관 · 활용되고 있는 정보시스템 및 네트워크 등에 대한 보안감사를 정기적으로 수행하여 중요정보 관리정책 및 지침에 맞게 정보가 생성 · 관리(활용, 보관, 파기 등) · 감독 · 보호되는지 확인해야 한다. 이를 준수하지 않거나 관리가 미흡한 부분이 발견되었을 경우, 즉시 개선하여 중요정보 유출 위협을 사전에 차단해야 한다.

보안감사는 감사인의 능력에 따라 감사 수준이 달라지지 않아야 하므로 체크리스트 등을 활용할 수 있으며, 〈그림 Ⅱ-5〉와 같이 "감사준비→감사착수→감사수행→결과보고→ 후속조치" 절차에 따라 수행된다.

그림 Ⅱ-5 • 보안감사 절차



10.2.1 보안감사 준비

보안감사 준비 단계는 조직에서 보안감사를 위한 환경을 마련하고 있는지 확인하는 단계로, 보안감사 및 점검 활동에 대한 규정 · 지침의 유무와 해당 규정 · 지침의 적합성을 검토하고, 보안감사를 위한 사전 준비사항이 마련될 수 있도록 하는 단계이다. 이는 조직을 대상으로 한 보안감사 수행이 가능한지, 즉 조직의 제반 환경이 보안감사 수행을 불가능하도록 하는 요소가 없는지를 확인하는 과정이라고 할 수 있다.

1) 보안감사 사전 준비사항

성공적인 보안감사가 이루어질 수 있게 조직에서는 사전에 보안감사를 위한 환경을 마련해야 한다. 보안감사의 정당성을 확보하기 위한 규정을 제정하고, 조직의 구성원이 보안감사가 필요하다고 인식할 수 있는 환경을 만들어야 한다. 보안감사가 적절히 이루어질 수 있도록 〈표 Ⅱ-38〉 같은 항목을 사전에 준비해야 한다.

표 Ⅱ-38 • 보안감사 사전 준비사항

구분	내용
보안감사 필요성 인식제고	보안감사를 통하여 준수해야할 법이나 규정의 위반에 대비하고, 법위반에 따른 불이익으로부터 개인과 조직을 보호하기 위하여 보안감사가 필요함을 임직원에게 인식
보안감사 정당성 확보 조치	보안감사의 대상이 되는 정보나 구성원과의 사이에서 법적 분쟁이 발생하지 않도록 보안감사의 절차적 정당성을 확보
보안감사 신뢰성 담보 조치	보안감사의 신뢰성 · 실효성 확보를 위해서는 무엇보다 보안감사를 정상적으로 수행할 수 있는 '진실한 정보' 혹은 '진정한 정보'가 지속적으로 추적 · 관리되고 보관될 수 있는 환경을 마련
보안감사 독립성 담보 조치	보안감사는 다른 부서에 영향을 받지 않을 만큼 충분히 독립적이어야 함
보안감사 규정 제정	보안감사가 효율적으로 이루어지고 조직 내부에서 명확히 실시될 수 있도록 규범적 근거를 마련
보안감사 절차 마련	보안감사의 기본 절차를 마련하고 감사 목적에 따라 세부적인 절차를 마련해두어야 하며, 감사 결과가 감사인의 역량에 따라 좌우되는 것을 최소화하기 위해 절차는 가능한 세분화할 필요
보안감사 조직 구성	보안감사를 실시하는 조직의 독립성과 중립성을 확보하는 것이 중요하며, 감사인의 역할과 권한을 명확히 해야 함
보안감사 준비도 점검	보안감사 준비도란 "조사비용은 최소로 하고 디지털 증거의 활용 가능성을 최대로 하기 위한 조직의 준비 능력"으로, 사고 발생 시 사고의 원인과 과정을 빠르고 정확하게 추적하기 위한 준비부터 단계별 대응 방법까지 모두 포괄 ※ "부록 1. 보안감사 준비 시 점검사항" 참고

2) 보안감사 준비문서

감사팀은 보안감사를 수행하는 중에 직면하는 여러 상황에 맞춰 적법한 감사를 수행하기 위하여 여러 가지 동의서 및 필요 서류들을 준비해야 한다. 다음 〈표 Ⅱ-39〉은 보안감사 준비 과정에서 필요한 문서들의 예이다.

표 Ⅱ-39 • 보안감사 준비 과정에서 필요한 문서

구분	내용
보안감사 근거문서	보안감사 시 전산자산 및 개인 업무 데이터에 대한 회사의 열람이 가능함을 증명하기 위한 근거문서
보안감사 체크리스트	보안감사 목적에 맞게 사전 점검 사항을 체크리스트 형태로 목록화 필요
비밀보호서약서	감사팀이 감사 중 획득하는 개인정보 또는 비밀에 대해 비밀을 유지할 것을 동의하는 서약서로 감사 수행 전 감사팀 전원에게 서명을 받아두어야 함
개인정보 수집 및 이용 동의서	감사 수행 도중에 감사팀이 획득 할 수 있는 개인정보가 포함된 문서 등의 취급 및 감사에 개인정보를 활용하는 행위에 대하여 감사 대상자가 동의하는 것을 증명하는 동의서를 사전에 받아야 함
보안감사 동의서	감사 대상자에게 받아야 하는 동의서로, 감사가 진행되는 동안 감사팀의 통제와 요구에 즉시 응하겠다는 내용 등을 포함
퇴직자 관리 문서	비밀유지 서약을 한 직원의 퇴직 시 필요한 문서로, 해당 직원이 기존 비밀유지를 서약한 사항에 대해 이를 유지 · 이행할 것을 촉구하는 내용을 포함

3) 보안감사 도구 및 장비

보안감사의 대상은 대부분이 디지털 데이터로 구성된다. 보안감사의 대상을 세분화한 후 각 대상 분석에 적합한 도구나 솔루션을 사전에 준비해야 한다. 보안감사인은 준비한 도구와 솔루션을 다양한 환경에서 테스트하여 분석 대상의 정보를 오류 없이 적절히 표현해주는지 확인해야 한다. 보안감사 관련 도구는 "부록3. 보안감사 도구 소개"를 참고할 수 있다.

4) 교육 및 훈련

내부자에 대한 교육은 입사 후 퇴직 전까지 지속적인 정보 유출 방지 교육을 실시해야 한다. 이론만 교육하는 것은 직원들의 흥미와 집중도가 떨어지고, 실제 기밀 유출에 대한 인지도가 낮기 때문에 이론과 가상훈련 등의 실무를 겸해야 효과적이다. 교육과 훈련에 관한 자세한 내용은 Part II의 '2장. 중요정보 유출 방지를 위한 인적 보안관리 방안을 강화시킨다.' 부분을 참고할 수 있다.

5) 보안감사인의 사전 점검사항

보안감사가 효과적으로 이루어지기 위해서 보안감사인은 사전에 점검항목을 확인하여야 한다. "부록 1. 보안감사 준비 점검사항 – 보안감사 준비 단계의 보안감사인의 사전 점검항목" 에서는 감사 준비 단계에서 보안감사인이 점검해야 할 항목들을 소개한다.

10.2.2 보안감사 착수

감사 준비단계의 점검 결과가 적정한 경우 보안감사 착수 단계를 수행한다. 보안감사 착수 단계는 감사 목표, 대상 및 범위를 식별하고, 일정을 수립하는데 그 목적이 있다. 보안감사인은 정보 감사의 목표를 식별하고, 해당 목표에 따른 감사 수행 범위와 일정을 설정한다. 감사 목표의 식별은 이어지는 절차들에 대한 의사 결정의 기준이 되는 중요한 절차이며, 감사 범위 역시 감사 목표에 따라서 구체적으로 설정될 필요가 있다.

1) 감사 계획 수립

보안감사인은 감사의 목표를 식별하고, 해당 목표에 따른 감사 수행 범위와 일정을 설정한다. 감사 준비에서 결과보고에 이르는 세부 일정 계획을 수립하고, 각각의 단계를 수행하기 위한 자원, 단계별 산출물 등을 확인하여야 한다. 감사 계획은 〈표 II-40〉 감사 계획서 작성 시 고려사항을 참고하여 디지털 포렌식 기술을 활용하여 무결성, 신뢰성, 정당성 등에 오류 없이 진행할 수 있도록 수립하고 문서화해야 한다.

표 Ⅱ-40 • 감사 계획서 작성 시 고려사항

구분	내용
보안감사 계획서에 포함되는 기본항목	감사계획서는 감사목적, 기간, 범위, 장소, 일정, 결과처리 등을 포함하며, 경영진의 승인을 받아야 함
위험평가 결과 반영	감사계획 수립 시에는 반드시 위험평가를 실시해야 하고 이를 통해 식별된 감사 대상 및 목표를 감사계획에 반영
보안감사 기법	감사기본항목과 위험평가를 기초로 감사대상이 식별 되면 감사대상에 적합한 감사기법을 선택 ※ "부록 2. 감사 착수 고려사항의 감사 대상별 적용 가능한 보안감사 기법" 참고

2) 감사인력 구성

감사 인력은 서로 소통이 가능하고, 각 인원별로 주어진 감사 수행 업무가 명확해야 한다. 또한 기업의 규모에 따라 감사팀이 감사해야 할 범위, 요점 등이 달라지기 때문에 기업의 규모를 고려하여 인력을 구성해야 한다. 감사 인력은 크게 인터뷰, 수집, 분석, 검토 인력으로 나눌 수 있다.

감사 투명성을 보장하기 위해 상황에 따라 외부전문가로 구성된 감사 인력을 운영할 필요가 있다. 외부전문가는 변호사, 회계사 등 전문자격을 갖춘 사람과 실무 경험이 많은 IT 전문가 등으로 구성할 수 있다.

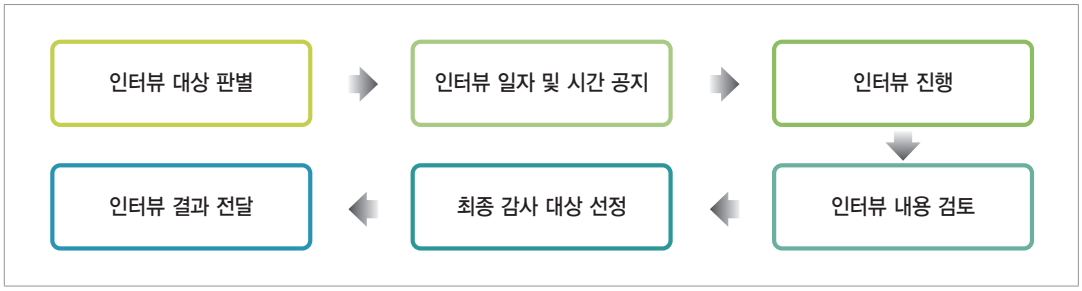
3) 준비 문서 작성

감사 수행 전 감사 대상자에게 정보 제공 및 감사 협조 동의서 등 준비 문서를 받아 추후 법적으로도 문제가 없도록 해야 한다. 보안감사에 필요한 준비 문서로는 개인정보 수집 및 이용 동의서, 보안감사 동의서 등이 있다.

4) 대상자 인터뷰

인터뷰란 감사 수행 전 감사 대상을 보다 명확히 선정하고, 감사 시 데이터 수집 및 분석 범위를 선정하는데 도움을 받기 위해 수행하는 단계이다. 인터뷰 시 감사의 목적과 형식, 범위 등을 명확히 고지할 필요가 있다. 인터뷰만으로는 원하는 결과를 도출하기 쉽지 않기 때문에, 감사 과정에서 확보한 전산 로그 및 정보보안 로그 등을 분석한 데이터를 기반으로 인터뷰 내용을 검증할 필요가 있다. 일반적으로 인터뷰는 아래 〈그림 Ⅱ-6〉과 같은 절차를 가진다.

그림 Ⅱ-6 • 대상자 인터뷰 절차



10.2.3 보안감사 수행

보안감사 수행 단계는 식별된 감사의 목표 및 범위 등 감사계획에 따라 실질적인 감사를 수행하는 단계로 관련 근거를 확보하는 「데이터 수집」 단계와 수집된 데이터를 감사 목적에 맞춰 분석하는 「데이터 분석」 단계로 나눌 수 있다.

1) 데이터 수집

보안감사를 위한 데이터를 수집 · 생성하는 '감사 데이터 수집' 절차로써, '일반 수집' 방식과 '정밀 수집' 방식으로 구분할 수 있다.

가) 일반수집 방식

일반 수집 방식은 매체의 할당 데이터 중 일부 데이터를 감사 데이터 항목으로 선별적으로 확보하는 방식으로, 비교적 단시간 내 확보 가능하다는 특징이 있으며 시스템 로그 등의 비활성 데이터를 위주로 한다. 데이터 수집 방식 별 고려사항은 "부록 4. 데이터 유형별 수집 방법 및 고려사항 소개"을 참고할 수 있다.

표 Ⅱ-41 • 일반 수집 방식 종류

구분	내용
IT 정보 수집	감사에 유용하게 활용할 수 있는 IT 정보로는 AV 로그, 방화벽 로그, IDS/IPS 로그, 메일서버 로그, DRM 로그, DLP 로그 등
라이브 데이터 수집	시스템 전원이 켜져 있는 상태에서 데이터를 수집하는 방법으로, 구동중인 시스템 상태를 반영하는 정보(프로세스 정보, 네트워크 정보, 열린 파일 목록, 현재 로그온 사용자 정보 등)를 포함하며, 라이브 데이터는 활성 데이터, 비활성 데이터, 물리메모리로 나눌 수 있다

나) 정밀수집 방식

정밀 수집 방식은 물리적 데이터를 수집하는 방법으로 매체 이미지 생성 · 복제를 통해 할당 데이터, 시그니처 등 확보 가능한 데이터 항목을 최대한 확보하는 방식이다. 이미지 생성 또는 복제를 통해 원본을 보존하기 때문에 상대적으로 복잡한 절차와 많은 시간이 소요된다는 특징을 가진다.

일반수집의 경우 논리적인 데이터만 수집 하는데, 논리적인 데이터 만으로는 슬랙 영역을 조사하거나 삭제된 데이터를 복구할 수 없다. 또한, 논리적인 데이터 수집은 데이터 자체보다는 사용 흔적 수집에 초점을 맞추기 때문에 데이터 자체를 살펴보기 위해서는 물리적인 데이터 전체를 수집하는 정밀수집 방식을 적용해야 한다. 정밀수집 방식의 대표적인 방법으로 복제와 이미징이 있다.

표 Ⅱ-42 • 정밀 수집 방식 종류

구분	내용
복제	복제란 원본 저장장치의 모든 섹터를 사본 저장장치에 그대로 복제하는 것을 의미하며, 복제된 사본은 원본과 동일하기 때문에 원본의 모든 작업을 재현 가능
이미징	이미징이란 저장장치 원본의 모든 섹터를 파일 형태로 만드는 것을 의미하며, 이미징 역시 복제와 동일하게 원본의 모든 데이터가 복사되기 때문에 삭제된 파일의 복구가 가능

2) 데이터 분석

감사 목적에 맞게 데이터를 수집하였다면 수집한 데이터를 바탕으로 데이터 분석을 진행한다. 데이터 분석 시에는 〈표 Ⅱ-43〉의 사항들을 고려해야 한다.

표 Ⅱ-43 • 데이터 분석 시 고려사항

고려사항	설명
분석 절차 마련	– 단일 데이터가 아닌 수많은 데이터의 흔적을 연관하여 분석해야하기 때문에 분석에 경험이 많더라도 일부 데이터를 누락하거나 한쪽에 치우친 분석을 할 수 있음 – 따라서 분석 결과의 객관성을 유지시키기 위해 분석 데이터 별로 기본 분석 절차를 마련해야 함
분석 결과에 대해 상호 검토	– 감사의 기본은 주관적인 판단을 제외하고 객관적인 분석 필요 – 주관적인 판단을 최소화하기 위해 분석은 항상 2인 이상이 수행하고 결과는 상호 검토와 재현을 통해 오류를 최소화
수집 데이터 양, 감사 일정의 맞는 분석시스템 성능	– 분석 시스템의 성능에 따라 분석 결과가 1~2일 안에 나올 수도 있고 일주일 이상 소요될 수 있음 – 따라서 조직의 감사 목적에 따라 수집 데이터를 분류한 후 고성능의 작업이 필요한 경우에는 별도의 전용 시스템을 통해 분석 수행

가) 데이터 유형별 분석

데이터 분석은 크게 개별 분석과 통합 분석으로 나눌 수 있다. 데이터 수집 단계에서 일반 수집 방식으로 수집된 데이터는 개별 분석으로 진행하고, 정밀 수집방식으로 수집된 데이터는 통합 분석으로 진행된다.

표 Ⅱ-44 • 데이터 유형별 분석 구분

구분	설명
개별 분석	개별 분석은 복제나 이미징을 이용해 전체 데이터가 수집된 경우가 아닌 감사 목적에 필요한 개별 데이터가 수집된 경우에 수행
통합 분석	통합 분석은 복제나 이미징을 이용해 저장장치 전체가 수집된 경우에 수행하며, 개별 분석보다는 일반적인 형태로 대부분의 통합 분석 도구는 복제된 저장장치나 이미지 형태를 입력받을 수 있음

나) 데이터 처리별 분석

데이터 처리에 방법에 따라 데이터 분석은 크게 데이터 인덱싱, 데이터 탐색, 데이터 복구 등으로 구분할 수 있다.

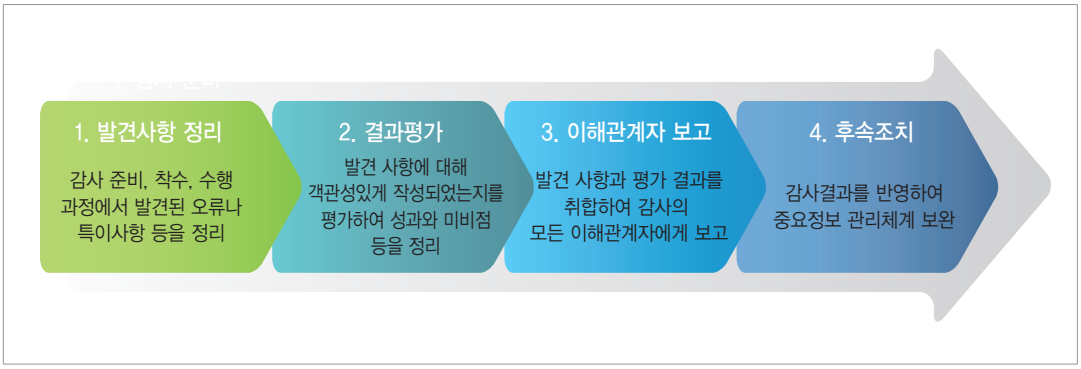
표 Ⅱ-45 • 데이터 처리 방법별 구분

구분	설명
데이터 인덱싱	파일명이나 파일내용을 검색하여 진행할 때 주로 사용하는 방식
데이터 탐색	데이터 탐색은 구조 탐색을 비롯해 은닉된 데이터 탐색과 암호화, 인코딩, 압축 등 변환이 필요한 데이터 처리도 포함하여 진행 ※ 데이터 탐색에 많이 사용되는 분석 도구는 부록3. 보안감사 도구항목 참고
데이터 복구	데이터 분석 관점에서는 악의적 또는 임의적으로 데이터가 삭제되는 경우를 대비하여 가능한 최대로 복구를 진행한 후에 분석을 수행 ※ 데이터 복구와 관련된 도구는 부록3. 보안감사 도구 항목 참고

10.2.4 감사결과 보고 및 후속 조치

감사 준비, 착수, 수행이 완료되면 각 과정의 결과를 취합하여 평가를 수행한 후 감사 결과를 보고한다. 감사팀은 감사활동 내용과 이와 관련된 증적자료 등을 기록한 감사조사서를 작성하고 정보누설 또는 분실되지 않도록 안전하게 보관해야 한다. 또한 감사과정에서 발견된 중요정보관리체계의 미비점을 개선할 수 있도록 보안감사인은 조직의 정책 · 지침 개정 등을 지원해줘야 한다.

그림 Ⅱ-7 • 감사결과 보고절차



1) 발견 사항 정리

감사 준비, 착수, 수행 과정에서 작성된 결과 문서를 취합하고 과정 중에 나타난 오류나 특이사항 등을 정리한다.

2) 결과 평가

정리된 발견 사항에 대해 절차대로 잘 진행이 되었는지 각 결과가 객관성 있게 작성되었는지를 평가하여 성과와 미비점 등을 정리한다. 분석뿐만 아니라 평가도 객관성 있게 진행되려면 감사 목적에 따라 평가의 각 항목을 미리 문서화하고 평가 기준이나 방법을 마련해두어야 한다.

3) 이해관계자 보고

발견 사항과 평가 결과를 모두 취합하여 감사의 모든 이해관계자에게 보고를 수행한다. 보고서를 통해 문서화 된 감사 결과에 대해서는 이해관계자들의 검토 의견이 수렴되어야 하며, 이에 대하여 적절한 책임자의 승인이 이루어져야 한다. 특히, 이해관계자들이 다음의 '후속 조치' 단계에서 수행될 수 있는 활동들을 충분히 고려하고 의사 결정한 결과가 감사팀에게 전달될 수 있도록 해야 한다.

4) 감사결과의 후속조치

수감기관은 감사 결과에 대한 이해관계자의 검토 및 의견을 반영하여 후속조치를 수행하고 보안감사인은 감사 결과에 따른 사후 조치를 포함해 후속 조치를 지원해야 한다. 후속조치로는 감사 대상 조직에 대한 '중요정보 관리체계 개선 지원' 활동을 들 수 있다. 감사 결과 확인되는 중요정보 관리체계 정책 · 지침의 개선점을 구체적으로 식별하고 개선할 수 있도록 보안감사인의 전문성을 바탕으로 해당 활동을 지원하여야 한다.

감사 계획에 따라 수행한 감사 범위 외 추가 혹은 별도로 수행할 필요성이 있다고 판단되는 경우 추가 분석

및 조사를 지원할 수 있다. 추가 조사는 네트워크(Network), 모바일(Mobile) 등 다양한 환경을 대상으로 수행될 수 있다. '법적 대응 지원' 역시 후속 조치 중 하나에 해당하며, 법정 제출을 위한 별도의 보고서 작성 및 법정 증언이 이에 해당한다. 각 활동에서 요구되는 전문성 등을 고려하여 조직 내 법무부서 혹은 외부의 전문가와 함께 수행할 필요가 있다

스마트공장 중요정보 유출방지 가이드

부록

부록 1

보안감사 준비 시 점검사항

1.1. 보안감사 준비도 – 체크리스트

점검 항목	예	아니오
• 프리패치 서비스가 활성화되어 있나요?		
• 파일시스템 트랜잭션 로그 크기가 512MB 이상으로 설정되어 있나요?		
• 파일시스템 변경 로그가 4GB 이상으로 설정되어 있나요?		
• 파일시스템 접근 시간이 갱신되도록 설정되어 있나요?		
• 로컬 방화벽에 로그가 남도록 설정되어 있나요?		
• 로컬 방화벽 로그 크기가 20MB 이상으로 설정되어 있나요?		
• 볼륨 섀도 복사본 크기가 볼륨 용량의 10% 이상으로 설정되어 있나요?		
• 이벤트 로그 서비스가 활성화되어 있나요?		
• 이벤트 로그 설정의 계정 관리 감사가 설정되어 있나요?		
• 이벤트 로그 설정의 계정 로그온 이벤트 감사가 설정되어 있나요?		
• 이벤트 로그 설정의 권한 사용 감사가 설정되어 있나요?		
• 이벤트 로그 설정의 로그온 이벤트 감사가 설정되어 있나요?		
• 이벤트 로그 설정의 시스템 이벤트 감사가 설정되어 있나요?		
• 주요 이벤트 로그 크기가 4GB 이상으로 설정되어 있나요?		
– 응용프로그램(Application) 이벤트 로그		
– 보안(Security) 이벤트 로그		
– 시스템(System) 이벤트 로그		

점검 항목	예	아니오
• 추가 이벤트 로그 크기가 100MB 이상으로 설정되어 있나요?		
– Microsoft–Windows–Application–Experience		
– Microsoft–Windows–DriverFrameworks–UserMode		
– Microsoft–Windows–NetworkProfile		
– Microsoft–Windows–OfflineFiles		
– Microsoft–Windows–TerminalServices–LocalSessionManager		
– Microsoft–Windows–TerminalServices–RemoteConnectionManager		
– Microsoft–Windows–WER–Diagnostics		
– Microsoft–Windows–Windows Defender		
– Microsoft–Windows–WLAN–AutoConfig		
• 주요 이벤트 로그의 백업이 설정되어 있나요?		
– 응용프로그램(Application) 이벤트 로그		
– 보안(Security) 이벤트 로그		
– 시스템(System) 이벤트 로그		
• 추가 이벤트 로그 크기의 백업이 설정되어 있나요?		
– Microsoft–Windows–Application–Experience		
– Microsoft–Windows–DriverFrameworks–UserMode		
– Microsoft–Windows–NetworkProfile		
– Microsoft–Windows–OfflineFiles		
– Microsoft–Windows–TerminalServices–LocalSessionManager		
– Microsoft–Windows–TerminalServices–RemoteConnectionManager		
– Microsoft–Windows–WER–Diagnostics		
– Microsoft–Windows–Windows Defender		
– Microsoft–Windows–WLAN–AutoConfig		

1.2 보안감사 준비도 – 설정방법

프리패치 활성화 설정

점검 항목	프리패치 활성화 여부
점검 목적	프리패치 설정을 강화하여 프로그램의 실행 흔적을 추적
점검 이유	클라이언트는 기본 활성화되어 있으나 수정된 운영체제에서는 비활성화되어 있는 경우가 있으므로, 반드시 확인함. 또한, 서버 제품군이나 SSD를 사용하는 시스템에서는 자동 비활성화 되므로 강제로 활성화되도록 설정할 필요가 있음
점검 환경	온라인 혹은 오프라인
점검 방법	• 온라인 점검 – 레지스트리 키: KEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩Sessi on Manager₩Memory Management₩PrefetchParameters – 레지스트리 값: EnablePrefetcher (REG_DWORD) • 오프라인 점검 – 레지스트리 키: KEY_LOCAL_MACHINE₩SYSTEM₩ControlSet00(#)₩Control₩Session Manager₩Memory Management₩PrefetchParameters – 레지스트리 값: EnablePrefetcher (REG_DWORD)
설정 방법	• Enable Prefetcher 값 설정 – 0x00: 비활성화 – 0x01: 응용프로그램 프리패칭 활성화 – 0x02: 부트 프리패칭 활성화 – 0x03: 응용프로그램과 부트 프리패칭 활성화 (권장)

파일시스템 트랜잭션 로그 크기 설정

점검 항목	NTFS 파일시스템 트랜잭션 로그($LogFile) 크기
점검 목적	파일시스템 트랜잭션 로그 크기를 증가시켜 시스템에서 일어난 트랜잭션 정보를 추적
점검 이유	NTFS 파일시스템 트랜잭션 로그는 파일시스템 상의 트랜잭션 정보를 저장하는 로그임. 트랜잭션 로그를 관리하는 이유는 CHKDSK와 같이 파일시스템 상에서 트랜잭션 오류가 발생했을 때 롤백시키기 위한 용도임. 이 트랜잭션 로그를 활용하면 파일시스템에서 일어났던 상세한 트랜잭션 정보를 알 수 있지만, 기본 크기가 64MB로 설정되어 있어 2~3시간 내에 빠른 대응이 되지 않으면 활용가치가 낮을 수 밖에 없음. 따라서, 해당 로그의 크기를 증가시켜 활용가치를 높여줄 필요가 있음
점검 환경	온라인

점검 방법	• 온라인 점검 – 커맨드 명령 $〉 chkdsk /L
설정 방법	• 로그 크기 설정 (기본 KB) – 커맨드 명령 $〉 chkdsk /F /L:〈size〉 (512MB 이상 권장) 예) $〉 chkdsk /F /L:524288

파일시스템 변경 로그 크기 설정

점검 항목	NTFS 파일시스템 변경 로그($UsnJrnl) 크기
점검 목적	파일시스템 변경 로그 크기를 증가시켜 시스템에서 일어난 다양한 파일의 변경 상태를 추적
점검 이유	NTFS 파일시스템 변경 로그는 파일에 변경이 일어날 때마다 변경의 상태를 기록하는 로그임. 파일시스템 행위 중 파일 접근을 제외하고 대부분은 파일의 상태를 변경시키기 때문에 변경 로그는 시스템 및 사용자의 흔적을 추적하는데 매우 중요한 로그임. 변경 로그는 트랜잭션 로그에 비해 크기가 커 보통 1주일 가량의 변경 정보를 알 수 있지만 장기간 추적을 원한다면 그 크기를 더 증가시켜줄 필요가 있음
점검 환경	온라인
점검 방법	• 온라인 점검 – 커맨드 명령: $UsnJrnl $〉 fsutil usn queryjournal 〈Volume〉 예) $〉 fsutil usn queryjournal c:
설정 방법	• 로그 크기 설정 – 커맨드 명령: $UsnJrnl $〉 fsutil usn createjournal m=〈MaxSize〉 a=〈AllocationDelta〉 〈Volume〉 (4GB 권장) 예) $〉 fsutil usn createjournal m=4294967296 a=4194304 c:

파일시스템 접근시간 갱신 설정

점검 항목	NTFS 파일시스템 접근 시간 갱신 활성화 여부
점검 목적	파일시스템 시간정보를 갱신하도록 설정하여 시스템 및 사용자 흔적을 좀 더 원활히 추적
점검 이유	윈도우의 기본 파일시스템으로 널리 사용되는 NTFS는 Vista 이후부터 접근시간이 갱신되지 않도록 기본 설정되어 있음. 접근 시간은 사용자 행위나 악성코드 행위를 추적할 때 유용하게 활용될 수 있으므로 이를 활성화할 필요가 있음

점검 환경	온라인 혹은 오프라인
점검 방법	• 온라인 점검 – 레지스트리 키: HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Control₩FileSystem – 레지스트리 값: NtfsDisableLastAccessUpdate (REG_DWORD) • 오프라인 점검 – 레지스트리 키: HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet00(#)₩Control₩FileSystem – 레지스트리 값: NtfsDisableLastAccessUpdate (REG_DWORD)
설정 방법	• NtfsDisableLastAccessUpdate 값 설정 – 0x00: 갱신함 (권장) – 0x01: 갱신 안함

로컬 방화벽 로그 크기 설정

점검 항목	로컬 방화벽 로그 크기
점검 목적	로컬 방화벽 로그 크기를 증가시켜 장기간 흔적을 추적
점검 이유	로컬 방화벽 로그는 기본적으로 4MB의 크기를 가지므로 장기간의 이벤트 추적을 위해서 로그 크기를 늘려줄 필요가 있음
점검 환경	온라인 혹은 오프라인
점검 방법	• 온라인 점검 – [제어판] ➡ [Windows 방화벽] ➡ [고급설정] ➡ [동작] ➡ [속성] ➡ 각 탭 [로깅] – 레지스트리 키: HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩Shar edAccess₩Parameters₩FirewallPolicy₩〈Profile〉₩Logging – 레지스트리 값: LogFileSize (REG_DWORD) • 오프라인 점검 – 레지스트리 키: HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet00(#)₩services₩Share dAccess₩Parameters₩FirewallPolicy₩〈Profile〉₩Logging – 레지스트리 값: LogFileSize (REG_DWORD)
설정 방법	• LogFileSize 값 설정 (기본 KB) – 0x5000 (20480) (20MB 이상 권장)

로컬 방화벽 로그 활성화 설정

점검 항목	로컬 방화벽 로그 활성화 여부
점검 목적	로컬 방화벽 로깅을 설정하여 내부망에서 이루어지는 비정상 접속을 추적
점검 이유	로컬 방화벽은 내부망에서 이루어지는 비정상 접속에 대한 기본적인 방어를 수행해주지만 로깅이 설정되어 있지 않아 연결 이력을 추적하기 어려우므로 로깅 설정을 강화시켜줄 필요가 있음
점검 환경	온라인 혹은 오프라인
점검 방법	• 온라인 점검 – [제어판] ➡ [Windows 방화벽] ➡ [고급설정] ➡ [동작] ➡ [속성] ➡ 각 탭 [로깅] – 레지스트리 키: HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩SharedAccess₩Parameters₩FirewallPolicy₩〈Profile〉₩Logging – 레지스트리 값: LogDroppedPackets, LogSuccessfulConnections (REG_DWORD) • 오프라인 점검 – 레지스트리 키: HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet00(#)₩services₩SharedAccess₩Parameters₩FirewallPolicy₩〈Profile〉₩Logging – 레지스트리 값: LogDroppedPackets, LogSuccessfulConnections (REG_DWORD)
설정 방법	• LogDroppedPackets, LogSuccessfulConnections 값 설정 – 0x00: 로깅 비활성화 – 0x01: 로깅 활성화 (권장)

볼륨 섀도 복사본 크기 설정

점검 항목	볼륨 섀도 복사본 크기
점검 목적	볼륨 섀도 복사본 크기를 늘려 백업된 이전 상태를 추적
점검 이유	시스템 설정 및 이전 파일이 백업된 볼륨 섀도 복사본을 이용하면 과거 상태의 흔적을 추적할 수 있음. 하지만 복사본 할당 크기가 작을 경우 추적 가능한 기간이 짧으므로 복사본 할당 크기를 늘려줄 필요가 있음
점검 환경	온라인
점검 방법	• 온라인 점검 – [제어판] ➡ [시스템] ➡ [고급 시스템 설정] ➡ [시스템 보호] 탭 ➡ 볼륨 선택, [구성] – 커맨드명령 $〉 vssadmin list shadowstorage /for=〈volume〉 예) $〉 vssadmin list shadowstorage /for=c:

설정 방법	• 복사본 크기 설정 – 커맨드명령 $〉 vssadmin resize shadowstorage /for=〈volume〉 /on=〈storevolume〉 /maxsize=〈size〉 예) $〉 vssadmin resize shadowstorage /for=c: /on=c: /maxsize=15gb

이벤트 로그 활성화 설정

점검 항목	이벤트 로그 활성화
점검 목적	이벤트 로그 활성화를 통해 시스템 및 사용자 이벤트 추적
점검 이유	이벤트 로그가 흔적을 추적하는데 많은 도움을 주고 있지만 다양한 원인에 의해 비활성 화될 수 있으므로 서비스의 활성화 여부를 모니터링 할 필요가 있음
점검 환경	온라인 혹은 오프라인
점검 방법	• 온라인 점검 – [제어판] ➡ [관리 도구] ➡ [서비스] ➡ Windows Event Log 서비스 상태 – 레지스트리 키: HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩eventlog – 레지스트리 값: Start (REG_DWORD) • 오프라인 점검 – 레지스트리 키: HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet00(#)₩services₩eventlog – 레지스트리 값: Start (REG_DWORD)
설정 방법	• Start 값 설정 – 0x02: 자동 (권장) – 0x03: 수동 – 0x04: 사용 안함

이벤트 로그 로깅 항목 설정

점검 항목	이벤트 로그 항목 설정
점검 목적	이벤트 로그의 로깅 항목을 설정하여 보다 상세한 시스템 및 사용자 이벤트 추적
점검 이유	윈도우 환경에서 이벤트 로그는 기본 활성화되지만 기본 로깅 되는 항목 이외에 상세 항목을 대부분 설정하지 않은 기본 상태로 운용을 함. 보다 상세한 추적을 위해서는 기본 설정이 아닌 세부적인 로깅 항목 설정이 필요함

점검 환경	온라인 혹은 오프라인
점검 방법	• 온라인 점검 – [제어판] ➡ [관리 도구] ➡ [로컬 보안 정책] ➡ [로컬 정책] ➡ [감사 정책] – 레지스트리 키: HKEY_LOCAL_MACHINE₩SECURITY₩Policy₩PolAdtEv – 레지스트리 값: (기본값) • 오프라인 점검 – 레지스트리 키: HKEY_LOCAL_MACHINE₩SECURITY₩Policy₩PolAdtEv – 레지스트리 값: (기본값)
설정 방법	• 이벤트 로그 설정 항목 – 계정 관리 감사 – 성공, 실패 (권장) – 계정 로그온 이벤트 감사 – 성공, 실패 (권장) – 권한 사용 감사 – 성공, 실패 (권장) – 로그온 이벤트 감사 – 성공, 실패 (권장) – 시스템 이벤트 감사 – 성공, 실패 (권장)

이벤트 로그 크기 설정

점검 항목	이벤트 로그 크기 설정
점검 목적	이벤트 로그 크기를 증가시켜 효율적인 시스템 및 사용자 이벤트 추적
점검 이유	이벤트 로그가 흔적을 추적하는데 많은 도움을 주고 있지만, 기본 크기가 작아 단기간의 로그만 추적이 가능하므로 크기를 늘려줄 필요가 있음
점검 환경	온라인 혹은 오프라인
점검 방법	• 온라인 점검 – 레지스트리 키 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩eventlog₩〈Log〉 HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩WINEVT₩Channels₩〈Log〉 – 레지스트리 값: MaxSize (REG_DWORD) • 오프라인 점검 – 레지스트리 키 HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet00(#)₩services₩eventlog₩〈Log〉 HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩WINEVT₩Channels₩〈Log〉 – 레지스트리 값: MaxSize (REG_DWORD)

설정 방법	• 이벤트 로그 크기 설정 – 주요 이벤트 4GB 이상 설정 Application, System, Security – 추가 추적용 이벤트 로그 100MB 이상 설정 Microsoft–Windows–Application–Experience Microsoft–Windows–DriverFrameworks–UserMode Microsoft–Windows–NetworkProfile Microsoft–Windows–OfflineFiles Microsoft–Windows–TerminalServices–LocalSessionManager Microsoft–Windows–TerminalServices–RemoteConnectionManager Microsoft–Windows–WER–Diagnostics Microsoft–Windows–Windows Defender Microsoft–Windows–WLAN–AutoConfig

이벤트 로그 백업 설정

점검 항목	이벤트 로그 백업 여부
점검 목적	이벤트 로그 백업을 통해 장기간의 시스템 및 사용자 이벤트 추적
점검 이유	이벤트 로그가 흔적을 추적하는데 많은 도움을 주고 있지만 설정된 크기가 꽉 찰 경우 이전 이벤트를 삭제하고 기록하기 때문에 과거 기록을 추적하는데 어려움이 있을 수 있으므로 이벤트 로그 백업을 설정할 필요가 있음
점검 환경	온라인 혹은 오프라인
점검 방법	• 온라인 점검 – 레지스트리 키 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩services₩eventlog₩〈Log〉 HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩WINEVT₩Channels₩〈Log〉 – 레지스트리 값: AutoBackupLogFiles (REG_DWORD) • 오프라인 점검 – 레지스트리 키 HKEY_LOCAL_MACHINE₩SYSTEM₩ControlSet00(#)₩services₩eventlog₩〈Log〉 HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩WINEVT₩Channels₩〈Log〉 – 레지스트리 값: AutoBackupLogFiles (REG_DWORD)
설정 방법	• AutoBackLogFiles 값 설정 – 0x00: 백업 안함 – 0X01: 자동 백업

1.3. 보안감사 준비 단계에서 보안감사인의 사전 점검항목 (예시)

보안감사인의 사전 점검항목
• 정보자산 식별 방법 마련 및 정기적 갱신 여부
• 정보자산 관리 기준 규정 마련 및 정기적 갱신 여부
• 정보시스템 및 정보자산 목록
• 소프트웨어 목록 관리
• 보안감사 관련 사항의 규정 및 승인
• 보안감사 데이터 수집/분석 절차와 관련 도구 및 솔루션 마련 여부
• 임직원(계약직 포함) 및 외주 인력에 대한 보안감사 수행 관련 동의 방법
• 입 · 퇴사자 처리 및 임직원 부서 이동에 따른 프로세스 마련 여부
• 보안감사 목적별 모니터링 방안 마련 여부
• 조직의 보안 정책을 중앙에서 배포/관리하는 시스템 적용 여부
• 보안감사 이벤트 식별 방안 마련 여부
• 데이터 분류 및 중앙화를 통한 관리 여부
• 데이터 유출 방지(DLP) 및 매체 제어(DC) 솔루션 도입 여부
• 문서 암호화 솔루션(DRM) 도입 여부
• 데이터 파기 정책 수립 여부
• 보안감사 사후 데이터 처리 방안 마련 여부
• 중장기 감사계획
• 위험평가보고서
• 조직에서 준수해야 하는 외부 기준(법령, 계약조건 등)
• 감사 제약사항(감사 일정, 감사 장소, 감사 비용)
• 재감사가 필요한 경우 이에 대한 결정권한을 가진 책임자의 승인

부록 2

보안감사 착수 시 고려사항

2.1. 감사 대상별 적용 가능한 보안감사 기법 (예시)

감사기법	정의	주요 감사 대상	설명	비고
면담조사 (인터뷰)	중요정보관리체계 또는 보호대책의 구축 및 운영 현황의 적절성을 평가하기 위해 관련자들에게 질문을 통해 답을 얻는 감사기법	인터뷰 대상자, 인터뷰 대상 조직 등	• 서면질의 • 필요한 경우 외부 위탁업무를 처리하는 외부직원 대상 인터뷰 포함 • 질문에 대한 답변 일관성 확보 • 여러 담당자 및 관리자에게 중복질문을 통해 답변의 신뢰성 확보 • 다른 감사기법을 통해 조사한 결과와 대조하여 일관성 확인	
문서검토	중요정보관리체계 또는 보호대책의 구축 및 운영 현황의 적절성을 평가하기 위해 정보보호 정책서 및 시행문서, 운영기록 등을 확인하는 감사기법	검토 대상 문서(정책서, 시행문서, 운영기록), 시스템 등	• 직무분리 규정, 정보보호 관련 역할정의, 정보보호 정책 및 운영지침, 각종 신청서, 관리대장, 시스템 환경설정, 시스템 감사로그 등 • 객관성 확보에는 좋지만 시스템을 조작하는 경우 신중하여야 함 • 여러 문서를 종합적으로 검토하고 인터뷰 조사결과와 병행하여 진행	문서목록 운영기록
현장조사 (현장방문)	중요정보관리체계 또는 보호대책의 구축 및 운영 현황의 적절성을 평가하기 위해 감사인력이 직접 현장을 방문하여 눈으로 확인하는 감사기법	현장조사 대상 시스템, 환경 등	• 시스템 운영자가 운영관리 지침에 따라 시스템을 실제 운영하고 있는지 감사자가 직접 확인하여 타당성 여부를 판단 • 감사인력이 눈으로 직접 확인 • 기술적 보호대책에 대해 현장조사가 가능 • 수감기관에서 의도적으로 보여주지 않는 부분에 대해서는 확인 불가 • 운영기록을 모두 확인하는 것이 불가능	보호대책이 실제로 운영되고 있는 환경, 상황, 활동을 확인
재 실시	정보보호 대책 운영 현황의 적절성을 판단하기 위해 감사인력이 보호대책을 직접 운영하여 확인하는 감사 기법	재조사 대상 시스템 등	• 감사인력이 직접 조작하여 확인 • 감사인력이 직접 검증한 부분에 대해서만 확인 • 우연히 직접 검증한 분야에만 문제가 없었을 가능성이 있음 • 모든 보호대책을 직접 검증할 수 없음	

부록 3

보안감사 도구 소개

물리 메모리 수집 도구

명칭	인터페이스	라이선스
Memorize	CLI	무료
FD(FastDump) Pro	CLI	상용
DumpIt	CLI	상용
Winen	CLI	상용
FTK Imager	GUI	무료

운영체제 점유 파일 수집 도구

명칭	인터페이스	라이선스
forecopy	CLI	무료
RawCopy	CLI	무료

쓰기방지장치

명칭	인터페이스	라이선스
Tableau Forensic Bridge	하드웨어 장치	상용
Forensic Dock Series	하드웨어 장치	상용

복제 · 이미징 장비

명칭	인터페이스	라이선스
TD3	하드웨어 장비	상용
TD2u	하드웨어 장비	상용
Falcon	하드웨어 장비	상용
Image MASSter Solo-4	하드웨어 장비	상용

데이터 인덱싱 도구

명칭	인터페이스	라이선스
Intella	GUI	상용
Nuix	GUI	상용
Splunk	GUI	상용
ELK	GUI	무료

데이터 탐색 도구

명칭	인터페이스	라이선스
EnCase Forensic	GUI	상용
FTK	GUI	상용
X-Ways Forensics	GUI	상용
Argos, DFAS	GUI	상용

데이터 복구 도구

명칭	인터페이스	라이선스
Recover My Files	GUI	상용
R-Studio	GUI	상용
Stellar Pheonix Windows Data Recovery	GUI	상용
FINALDATA	GUI	상용

부록 4

데이터 유형별 수집 방법 및 고려사항

IT 정보 수집

IT정보 수집은 조직 내에 설치된 다양한 솔루션 및 장비의 로그를 수집하여 보안감사에 활용하는 방법이다. 해당 정보는 IT 부서의 협조를 통해 사전에 확보해야 한다. IT 정보 수집 시 아래와 같은 사항을 고려해야 한다.

DRM 및 암호화 솔루션 고려

수집 대상 시스템이 암호화 솔루션을 사용하거나 DRM 관리 하에 있는 경우 감사 데이터를 원활히 수집할 수 없으므로 사전에 수집 대상 목록을 작성하여 솔루션으로 인한 제약이 없도록 준비해야 한다.

정보 선별화

일반적으로 조직에 관리되는 IT 정보는 종류도 다양하지만 각 종류별로 양도 매우 많다. 따라서 전체를 수집할 것인지 기간이나 식별자를 이용해 선별적으로 수집할 것인지에 대한 고려가 필요하다. 잘못된 판단으로 시간을 낭비하거나 불필요한 정보가 수집되지 않도록 담당자 인터뷰 시 충분한 질의를 통해 내용을 파악해야 한다. 정보 선별화는 감사인의 경험이 많이 요구되는 만큼 현장 대응 경력이 5년 이상인 감사인이 항상 포함되도록 인력을 구성해야 한다.

라이브 데이터

라이브 수집은 시스템 전원이 켜져 있는 상태에서 데이터를 수집하는 방법이다. 구동 중인 상태에서 데이터를 수집하기 때문에 데이터 수집 시 아래와 같은 사항을 고려해야 한다.

시스템 흔적 최소화

일반적인 라이브 데이터 수집 방식은 소프트웨어를 이용한 수집이다. 수집을 위해 소프트웨어를 실행하면 프로그램이 메모리에 로드되면서 수집 대상인 메모리를 변경시킬 수 있으므로 이 변경을 최소화하도록 구성해야 한다. 또한, 수집 데이터로 인해 수집 대상 시스템이 손상을 입을 수 있으므로 수집 데이터는 반드시 외장저장장치나 네트워크를 이용해 다른 시스템으로 전송하도록 구성해야 한다. 또한, 소프트웨어와 함께 로드되는 추가 라이브러리(.DLL, .SO 등)에 의한 변경을 최소화하기 위해 라이브러리는 보통 정적 컴파일을

수행한다.

수집 과정 로깅

사전에 테스트를 수행하더라도 수집 대상 환경은 워낙 다양하기 때문에 수집 로그를 남겨 정상적으로 수집이 되었는지를 검증할 수 있어야 한다. 가능하면 단순 로그 이외에 오류 발생 시 원인을 알 수 있도록 로그를 구성하는 것이 필요하다.

반복적인 테스트

수집 환경은 예측할 수 없기 때문에 테스트 환경에서 도출할 수 없는 문제가 발생할 수도 있다. 따라서 다양한 환경에서 반복적인 테스트를 수행하여 수집 과정에 대한 안정성을 높여야 한다.

신속한 수집

라이브 데이터는 수집 대상 시스템 상태를 가장 잘 알려줄 수 있는 데이터이지만 시스템 변경에 영향을 미칠 수 있기 때문에 최대한 안전한 방법으로 빠르게 수집해야 한다.

라이브 데이터 수집 순서

라이브 데이터는 활성 데이터, 비활성 데이터, 물리메모리로 구성되어 있다. 단일 스크립트에 모두 수집될 수 있도록 구성하는 경우 수집 순서를 고려하는 것이 바람직하다. 라이브 데이터 수집 순서는 프리패치→활성데이터→비활성데이터→네트워크 패킷순서 순서로 수집하는 것을 추천한다.

프리패치를 가장 먼저 수집하는 이유는 수집과정에서 시스템에 영향을 미칠 수 있기 때문이다. 라이브 데이터 수집에 사용되는 프로그램을 실행하면 기존 시스템의 프리패치 파일을 갱신할 수 있기 때문에 이를 가장 먼서 수집하고 이어서 활성 데이터와 비활성 데이터 순서대로 수집하다.

활성데이터 중 네트워크 연결 정보는 같은 망 내에서 사용자 식별을 위해 사용하게 되는 ARP 캐시처럼 자체 갱신 시간이 있기 때문에 휘발성이 매우 높은 정보라 볼 수 있다. 이와 같은 이유로 활성데이터 중에서는 네트워크 연결 정보를 가장 먼저 수집하고, 그 후 물리메모리 덤프를 진행한다. 물리메모리 덤프에 소요되는 시간은 라이브 데이터 중 가장 오래 걸리지만 명령어 기반 수집 방식의 단점을 보완할 수 있고 나중에 정밀 분석이 가능하기 때문에 가능하다면 수집 하도록 한다.

네트워크 패킷 정보는 현재 시스템 상태를 잘 보여주기는 하지만 목적에 따라 수집이 불필요할 수도 있기 때문에 가장 마지막에 수집하고 스크립트에 옵션을 주어 수집 여부를 선택할 수 있도록 구성하는 것이 바람직하다.

일반적인 라이브 데이터 수집 순서는 아래와 같다.

순서	구분	수집 항목
1	비활성	프리패치
2	활성	네트워크 정보
3	활성	물리메모리
4	활성	프로세스 정보
5	활성	사용자 로그온 정보
6	활성	시스템 정보
7	활성	네트워크 인터페이스 정보
8	활성	작업스케줄러, 클립보드, 자동실행 정보
9	비활성	MBR, VBR
10	비활성	파일시스템 메타데이터, 파일시스템 로그
11	비활성	레지스트리, 이벤트 로그
12	비활성	바로가기, 점프 목록
13	비활성	%SystemRoot% 하위 주요 파일
14	비활성	웹브라우저 아티팩트
15	활성	네트워크 패킷

시스템 스크립트 사용 시 고려사항

시스템 스크립트는 시스템 지원하는 기본명령어를 활용하여 수집하는 방법으로시스템 셸에서 지원하는 기본기능을 주로 활용하기 때문에 다른 언어의 스크립트에 비해 스크립트를 사용하기 위한 별도의 프로그램 설치 등이 없다는 점에서 시스템에 미치는 영향을 최소화할 수 있다. 일반적으로 윈도우는 배치 스크립트, 리눅스는 셸 스크립트를 많이 사용한다. 셸 프로그래밍이 가능하다면 수집 데이터를 하나씩 수집하는 것이 아닌 자동화하여 신속하게 수집할 수 있으며, 시스템 스크립트 사용은 아래 표와 같은 장 · 단점이 있다.

장점	단점
• 한 번에 쉽게 데이터 획득 가능 • 타 스크립트에 비해 최소한의 영향 • 저용량 스크립트 파일로 휴대성 편리 • 쉽게 배울 수 있는 언어	• 시스템 명령어만 사용가능 • 가공된 데이터 획득이 어려움 • 시스템에 영향을 끼침 • 작성자의 역량에 따라 수집 데이터가 달라짐

스크립트를 이용해 수집한 데이터는 시스템 명령에서 지원하는 데이터만 제한적으로 수집이 가능하기 때문에

데이터를 가공하는 과정에 제한이 있다. 따라서 다양한 도구로 분석하고 상호 검증하기 위해서는 데이터 수집 시 원본을 수집하는 것을 추천 하지만 원본 수집이 제약될 경우 최대한 많은 정보를 수집할 수 있게 스크립트를 구성하여 활용할 수 있다.

활성 데이터 수집

활성 데이터는 전원이 켜져 있는 상태에서만 메모리(RAM)에 유지되는 데이터로 직원의 데이터 유출, 시스템 가용성의 문제, 악성 코드에 의한 감염 등을 분석할 때 사용할 수 있는 데이터이다. 활성 데이터 수집은 다양한 시스템 명령을 스크립트를 이용해 자동화하여 수집하는 것이 일반적이다. 스크립트는 수집 대상 시스템에 최소한의 영향을 미치도록 별도의 설치가 필요하지 않는 시스템 스크립트를 주로 이용한다.

보안감사 분석 시 유용한 활성 데이터

활성데이터 수집 시 시스템에 영향을 최소화하여 수집해야 한다. 수집해야 하는 활성데이터의 종류와 양은 사건의 영향과 분석 목적에 따라 변경될 수 있으므로 조사를 통해 달성하고자 하는 목표를 사전에 명확히 설정할 필요가 있다. 보안감사 분석 시 유용하게 활용될 수 있는 활성 데이터는 아래 표와 같다.

데이터	설명
네트워크 정보	네트워크 연결, 네트워크 인터페이스, 라우팅 테이블, 연결된 세션, 열린 포트 등의 정보를 통해, 자산 유출 위협을 끼칠 수 있는 외부 서비스에 대한 분석에 도움을 줄 수 있음
프로세스 정보	구동 중인 프로세스의 이름, 커맨드라인, 소유자, 이미지 경로, 서명 여부, 설명, 메모리 점유율 등의 정보를 획득하여 구동 상의 문제, 악의적인 프로세스 여부를 확인
사용자 로그온 정보	시스템에 로컬이나 네트워크로 로그인한 사용자의 정보를 수집하여 비정상 로그인 여부를 확인
시스템 정보	시스템 기본 정보, 그룹 정책, 서비스 목록, 시작/종료 시간, 시스템 최근 활동 내역, 최근 검색 내역 등 기본 시스템의 정보를 확인하여 분석 대상에 대한 이해 및 분석 방향을 정할 수 있음
네트워크 인터페이스 정보	구동 모드, IP 주소, DNS 캐시, MAC 주소 등 네트워크 인터페이스 카드 정보를 수집하여 악의적인 설정 및 연결을 확인할 수 있음
패스워드 정보	시스템에 자동 저장될 수 있는 메일, 네트워크, 웹 브라우저, 무선 네트워크, RDP 등의 사용자 패스워드 정보를 획득하여 추후 분석에 활용할 수 있음
작업 스케줄러자동 실행 정보	시스템에서 지속적으로 동작하도록 구성할 수 있는 작업 스케줄러와 자동 실행 정보를 수집하여 지속성을 가진 프로그램을 파악할 수 있음
네트워크 패킷	수집 시점에 네트워크에 이상 징후가 있다고 판단되면 라이브한 네트워크 패킷을 수집하여 수집된 다른 흔적과 비교 분석하는 등 유용하게 활용할 수 있음

활성 데이터 수집에 사용되는 명령어

수집 대상의 명령어는 안전성을 담보할 수 없기 때문에 수집에 사용하는 명령어는 미리 준비하도록 한다. 분석 대상이 예측되는 경우 사전에 테스트를 통해 최적화해야 하고, 예측할 수 없는 경우 환경별로 구성된 수집 명령어 세트를 준비해야 한다. 활성 데이터 수집에 사용되는 일반적인 명령 및 옵션은 다음 표와 같다.

분류	명칭	상세설명 URL
네트워크 정보	arp –a	http://technet.microsoft.com/en-us/library/cc754761.aspx
	netstat –nao	http://technet.microsoft.com/en-us/library/ff961504.aspx
	route PRINT	http://technet.microsoft.com/en-us/library/ff961510.aspx
	cports /stext	http://www.nirsoft.net/utils/cports.html
	urlprotocolview /stext	http://www.nirsoft.net/utils/url_protocol_view.html
	net session/file/share	http://technet.microsoft.com/en-us/library/hh750729.aspx
	nbtstat –c	http://technet.microsoft.com/en-us/library/ff961511.aspx
	tcpvcon –a –c	http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx
프로세스 정보	pslist	http://technet.microsoft.com/en-us/sysinternals/bb896682.aspx
	cprocess	http://www.nirsoft.net/utils/cprocess.html
	tasklist –V	http://technet.microsoft.com/en-us/library/cc730909.aspx
	tlist (–c | –t | –s)	http://msdn.microsoft.com/en-us/library/windows/hardware/ff558901(v=vs.85).aspx
	listdlls	http://technet.microsoft.com/en-us/sysinternals/bb896656.aspx
	dllexp	http://www.nirsoft.net/utils/dll_export_viewer.html
	injecteddll	http://www.nirsoft.net/utils/injected_dll.html
	handle	http://technet.microsoft.com/en-us/sysinternals/bb896655.aspx
	openfilesview	http://www.nirsoft.net/utils/opened_files_view.html
사용자 로그온 정보	psloggedon	http://technet.microsoft.com/en-us/sysinternals/bb897545.aspx
	logonsessions	http://technet.microsoft.com/en-us/sysinternals/bb896769.aspx
	netusers /local /history	http://www.systemtools.com/cgi-bin/download.pl?NetUsers
	net user	http://technet.microsoft.com/en-us/library/cc771865.aspx

분류	명칭	상세설명 URL
시스템 정보	psinfo (-d | -s | -h)	http://technet.microsoft.com/en-us/sysinternals/bb897550.aspx
	wul	http://www.nirsoft.net/utils/wul.html
	gplist	http://ntsecurity.nu/toolbox/gplist/
	gpresult /Z	http://technet.microsoft.com/en-us/library/cc733160.aspx
	psservice	http://technet.microsoft.com/en-us/sysinternals/bb897542.aspx
네트워크 인터페이스 정보	promiscdetect	http://ntsecurity.nu/toolbox/promiscdetect/
	ipconfig /all	http://technet.microsoft.com/ko-kr/library/bb490921.aspx
	ipconfig /displaydns	http://technet.microsoft.com/ko-kr/library/bb490921.aspx
	getmac	http://technet.microsoft.com/en-us/library/bb490913.aspx
기타 정보	schtasks /query /fo list /V	http://technet.microsoft.com/en-us/library/bb490996.aspx
	autorunsc	http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx

휘발성 민감도(OOV, Order Of Volatility) 고려

휘발성 민감도란 휘발성의 정도를 나타내는 것으로 수집 데이터에 따라 민감도가 다양하다. 수집 데이터의 민감도보다 수집 과정에 대한 절차를 신속하게 하는 것이 더 중요하지만 수집 도구 구성에 무리가 없는 경우 휘발성 민감도를 고려하여 준비하는 것이 도움이 된다. 다음 표는 RFC와 NIST 표준에 정의된 휘발성 민감도로 번호가 작을수록 휘발성 민감도가 높다.

휘발성 민감도(OOV)

	RFC 3227	NIST SP 800-86
1	레지스터, 캐시	네트워크 연결 정보
2	라우팅 테이블, ARP 캐시	로그온 세션
3	프로세스 정보 커널 통계 정보	물리메모리
4	물리메모리	프로세스 정보
5	임시 파일시스템	열린 파일
6	저장장치	네트워크 설정 정보
7	원격 로그온과 모니터링 데이터	시스템 시간
8	물리적 설정, 네트워크 토폴로지	-
9	기타 저장장치	-

다양한 도구와 명령어 중복 실행

활성 데이터 수집은 명령어와 도구에 따라 출력이 다르기 때문에 가능한 전체 내용을 획득할 수 있도록 출력이 다양한 도구를 중복 실행해야 한다. 또한, 명령어의 방식에 따라 출력이 다르게 나타날 수도 있으므로 다양한 명령어와 옵션을 사용하여 중복 실행하여 데이터를 수집할 필요가 있다.

비활성 데이터 수집

비활성 데이터는 전원이 꺼진 상태에서도 유지되는 저장장치 데이터로 실제 분석에 가장 효과적으로 활용되는 데이터 이지만 최근 저장장치 용량의 증가로 저장장치를 수집하는 시간이 환경에 따라 상당히 오래 걸릴 수 있어 비활성 주요 데이터를 먼저 수집하여 정밀 분석 전에 분석 대상 및 전체적인 분석 방향을 계획하는 것이 좋다.

보안감사 분석 시 유용한 비활성 데이터

보안감사 분석 시 유용하게 활용될 수 있는 비활성 데이터는 다음 표와 같다.

보안감사 분석 시 유용한 비활성 데이터

데이터	설명
파일시스템 메타 데이터	저장장치에 존재하는 파일의 속성 정보를 가지는 파일 시스템 메타 데이터 수집을 통해, 파일의 생성/수정/접근/속성 변경 시간과 해당 파일의 속성(암호, 숨김 등)을 파악할 수 있음. 또한 파일 시스템 로그 데이터와 함께 사용하여 파일의 행위에 대한 더욱 더 자세한 정보를 제공해 줄 수 있음
파일시스템 로그	파일시스템 상에서 일어난 트랜잭션, 변경 내역을 관리하는 로그로 로그가 유지되는 시간 동안 매우 상세한 파일시스템 I/O 정보를 확인할 수 있음. 기본 로그의 용량 제한이 있지만 특정 시점의 시스템 상태를 가장 상세하게 볼 수 있는 정보로 감사에 유용하게 활용될 수 있음
레지스트리	윈도우 운영체제에서 사용하는 설정 데이터로, 시스템에 설치된 파일 및 프로그램, 기타 모든 설정 정보가 여기에 기록되어 있음. 설정뿐만 아니라 사용자의 행위 파악에 도움이 되는 저장장치 연결정보, 최근 열람 파일 및 문서, 최근 설치 애플리케이션 등 매우 다양한 정보를 통해 보안감사 분석 시 유용하게 활용할 수 있음
프리패치 파일	윈도우 운영체제에서 응용프로그램을 실행할 경우 초기 빠른 실행을 위해 생성, 관리하는 파일로 응용프로그램의 최근 실행 시간, 실행 횟수, 참조 파일 목록 등을 확인할 수 있음
이벤트 로그	윈도우 운영체제에서 일어나는 전반적인 이벤트를 모두 기록하고 있는 파일임. 해당 이벤트 로그는 시스템 정보 해당 파일의 분석을 통해 특정 시점의 PC에 행해진 이벤트를 정의 할 수 있으며, 다른 파일 분석 결과와 연계하여 보안감사 분석에 유용하게 사용할 수 있음
웹브라우저 로그	웹브라우저를 통해 접근한 웹 페이지, 메일 사이트, 방문 페이지 사본 등 웹 사이트 방문 이력 등을 통해 보안감사 분석에 사용할 수 있음
바로가기 파일	파일 실행 시 자동으로 생성되는 파일로 파일의 실행 이력과 바로가기 대상의 상세 정보를 획득할 수 있는 파일임. 최근 실행한 문서, 외장 저장 장치 사용 이력 등을 확인 가능하며, 신속한 수집 시 사용자 행위 파악에 유용하게 사용할 수 있음
휴지통 정보	단순 삭제를 수행할 경우 해당 파일에 대한 메타 정보와 데이터는 휴지통에서 확인할 수 있음. 감사 시나리오에 맞게 해당 데이터를 통해 분석에 활용할 수 있음
기타 로그 파일	기타 아이콘 캐시, 썸네일 캐시, 점프 목록, Local System 흔적, IIS 로그, Setupapi 로그, 작업 스케줄러 로그, 방화벽 로그 등 시스템에 설정 된 로그에 따라 수집 여부를 달리 할 수 있음. 해당 로그는 실제 행위 분석에 활용 가능하며 결과의 신뢰성에 도움이 되는 자료로 보안감사 시 활용할 수 있음

관리자 권한 사용

비활성 주요 데이터는 대부분 시스템에서 중요하게 사용되는 데이터이기 때문에 수집을 위해서는 반드시 관리자 권한이 요구된다. 따라서 반드시 관리자 권한을 사용해 수집될 수 있도록 구성할 필요가 있다.

수집 데이터 선별

비활성 데이터는 종류나 시스템 환경에 따라 수집 용량이 다양할 수 있다. 라이브 데이터 수집 후 이미징이나 복제가 이루어진다면 사전 분석에 활용할 수 있는 데이터만 선별해 수집하는 것이 바람직하다. 수집 데이터 선별은 현장의 상황을 고려하여 감사 목적에 맞게 현장 대응 인력이 판단하여 수집해야 한다.

운영체제 점유 파일 수집 방법

일부 비활성 데이터는 운영체제가 실행되는 동안 시스템이 점유하고 있기 때문에 API를 이용한 복사 방법으로 수집하는 것이 어렵다. 따라서 물리적인 방법으로 수집하는 등의 수집 방안이 고려되어야 한다.

※ 운영체제 점유 파일을 수집할 수 있는 도구는 "부록 3. 보안감사 도구 소개"를 참고

부록 5

참고문헌

[1] 사물인터넷(IoT)정보보호 로드맵 (미래창조과학부, 2014)

[2] IoT 공통 보안 원칙 (IoT보안얼라이언스, 2015)

[3] IoT 공통 보안 가이드 (IoT보안얼라이언스, 2016)

[4] SP 800-82 Revision 2 . Guide to Industrial Control Systems (ICS) Security (NIST, 2015)

[5] Guide to Increased Security in Industrial Information and Control Systems (MSB, 2014)

[6] 국가연구개발사업 보안관리 표준 매뉴얼(미래창조과학부, 2014)

[7] IT 외주인력 보안통제 안내서 (KISA, 2011)

[8] 정보의 안전한 저장과 관리를 위한 보조기억매체 이용 안내서 (KISA, 2010)

[9] 정보보호 조직 구성 및 운영 가이드 (TTA, 2012)

[10] 조직의 정보보호를 위한 자산 관리 지침 (TTA, 2010)

[11] 개인정보 처리단계별 기술적 보호조치 가이드라인 (행정안전부, 2009)

[12] 개인정보 위험도 분석 기준 및 해설서 (행정안전부, 2012)

[13] 인력관리 지원 가이드 (KAITS, 2015)

[14] 산업기밀보호센터(http://service4.nis.go.kr/)

[15] 민관합동 스마트공장 추진단 (http://www.smart-factory.kr/)

[16] 산업기술 보호 지침 및 매뉴얼 (KAITS, 2014)

[17] 중소기업 기술보호 매뉴얼 (대 · 중소기업협력재단, 2013)

[18] 정보감사 가이드라인 (KISA, 2014)

[19] SP 800-86: Guide to Integrating Forensic Techniques into Incident Response, August (NIST, 2006).

스마트공장 중요정보 유출방지 가이드

인 쇄 2017년 3월 인쇄
발 행 2017년 3월 발행

발행처 한국인터넷진흥원
발행인 백기승
주 소 05717 서울시 송파구 중대로 135(가락동 78) IT벤처타워
TEL. 405-5118 / FAX. 405-5119 / www.kisa.or.kr

제 작 호정씨앤피(02-2277-4718)