情 報 保 護 學 會 誌
第21卷 第1號, 2011. 2

미국의 연방정보보안관리법에 대한 연구

이 동 범*, 고 웅**, 곽 진***

요 약

IT 진화의 다른 면으로는 정보 보안 위협의 심각화와 개별 위험 증가도 잠재하고 있어 이에 대응하는 정보 보안 정책도 나날이 변화가 요구된다. 이에 따라 미국에서는 연방정보보안관리법을 제정하여 연방정부의 운영 및 자산에 대한 정보 보안 통제항목의 효율성을 강화하기 위한 총괄적인 프레임워크를 제공한다. 또한 연방정부 및 정보 시스템 보호를 위한 최소 통제 및 유지 방안 개발을 제공한다. 따라서 본 고에서는 미국의 연방정보보안관리법의 각 단계별 보안 활동을 분석하고자 한다.

Ⅰ. 서 론

정보기술(IT)은 발전을 계속하고 있으며, 차세대 네트워크, 클라우드 등 새로운 기술이나 서비스가 잇달아 만들어져서 실용화되고 있다. 기술의 변화는 업무 과정을 혁신하고 경영의 구조를 바꾸고 새로운 사업 기회와 시장을 지속적으로 만들어내고 있다. 이러한 기술 혁신은 기존의 시장 구조나 산업 구조에 대한 상당한 변화를 초래하고 사회 경제 구조의 변화를 촉진시킬 가능성이 있다.

한편 IT 진화의 다른 면으로는 정보 보안 위협의 심각화와 개별 위험 증가도 잠재하고 있어 이에 대응하는 정보 보안 기술도 나날이 변화가 요구된다.

경제에서 차지하는 IT 비중의 증가는 정부 및 기업 위험 관리의 정보 보안 중요성을 높이고 있다. 정보 시스템을 막는 보안이 아니라 정보유출방지나 컴플라이언스를 자각한 비즈니스 프로세스 관리, 내부 통제 관리를 고려한 거버넌스의 확립, 예상치 못한 사태에 대비할 수 있는 비즈니스 연속성 관리에 이르기까지 다양한 과제에 대해서 정부 및 기업이 대치해야 한다.

미국에서는 이러한 문제를 해결하기 위해 네트워크화된 국가기반 환경을 보호하고 민간인을 비롯해 국가안보 관련 기관과 법집행 기관 전체의 정보보호 노력을 조정하고자 연방정보보안관리법(FISMA : Federal Information Security Management Act)을 전자정부법(E-Government Act of 2002) 제 3편으로 제정하였다.

연방정보보안관리법은 각 연방기관의 문서 개발을 필요로 하며, 유관기관, 계약자, 또는 공급원을 포함하는 기관 통제와 자산을 지원하는 정보 및 정보 시스템을 위한 정보 보안을 제공하기 위해서 기관 전체에 대한 정보 보안 프로그램을 실시한다. 정보 보안 프로그램은 다음과 같은 내용을 포함한다.

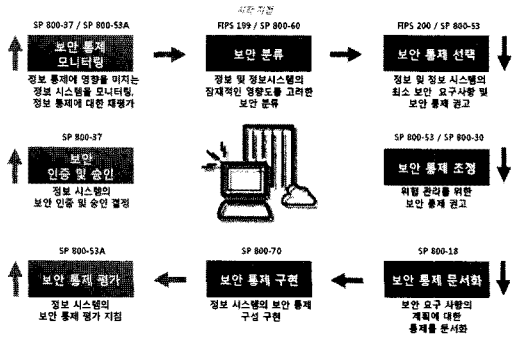
- □ 기관의 운영과 자산을 지원하는 정보 및 정보 시스템의 비인가 접근, 사용, 노출, 중단, 변경, 파괴의 결과에 대한 손실 정도를 포함하는 위험의 지속적인 평가
- □ 위험 평가를 기반으로 하는 정책과 절차는 비용-효과적인 정보 보안 위험을 허용 등급까지 감소시키고, 정보 보안은 각 기관의 정보 시스템의 생명 주기를 통하여 처리되는 것을 보증
- □ 네트워크, 시설, 정보 시스템 또는 정보 시스템의 그룹에 대한 적합한 정보 보안을 제공하기 위한 하위 계획
- □ 위험을 감소하기 위해 계획된 기관의 정책과 절차에 따라 활동 및 책임과 관련된 정보 보안 위험을 인원들에게 알리는 보안 인식 훈련
- □ 정보 보안 정책의 유효성, 절차, 운영 및 보안 통

* 순천향대학교 정보보호학과 정보보호응용및보증연구실 (dblee@sch.ac.kr)
** 순천향대학교 정보보호학과 정보보호응용및보증연구실 (wgo@sch.ac.kr)
*** 순천향대학교 정보보호학과 (jkwak@sch.ac.kr)

제의 주기적인 테스트와 평가는 위험의 의존도가 빈번하게 일어날 때 실시

- □ 제출된 정보 보안 정책, 절차, 기관 운행상의 결함은 계획, 구현, 평가 및 문서화에 대한 프로세스에서 개선 조치를 취함
- □ 보안 사고의 발견, 보고 및 대응하기 위한 절차
- □ 기관의 운영과 자산을 지원하는 정보 시스템에 대한 운영의 연속성을 보증하는 계획과 절차

FISMA는 1995년 문서감축법(Paperwork Reduction Act)과 1996년 정보기술개혁법(Information Technology Management Reform Act)의 비용-효과적인 보안에 대한 위험 기반 정책을 명백히 강조한다. 지원 및 입법을 강화하고 OMB 회람 A-130, 연방기관 자동화 정보 자원의 보안(Security of Federal Automated Information Resources)은 연방기관 내의 집행 기관을 요구한다.



〔그림 1〕 미 연방기관의 정보 보안 프레임워크

Ⅱ. 보안 분류

FIPS 199(연방기관의 정보 및 정보 시스템들의 보안 분류를 위한 표준)는 정보 및 정보 시스템을 분류하는 표준을 개발하는 첫 번째 임무를 나타낸다. FIPS 199는 정보 및 정보 시스템들에 대한 보안 분류 표준에 따라 공통의 프레임워크와 보안 표준에 대한 기준을 제공한다[1].

- □ 정보 보안의 중재자 역할을 포함하여, 정보 보안 프로그램의 효과적인 관리와 감독을 위해 민간, 국가 보안, 긴급 대응, 자치 보안과 법 집행 조직을 통한 노력이 필요
- □ 예산 관리국(OMB)과 의회의 효과적인 정보 보안 정책, 절차, 실행의 정당성과 유효성에 대한 정확한 보고를 위해 존재

2.1 정보 및 정보 시스템의 분류

FIPS 199는 정보 및 정보 시스템 보안 분류를 규정한다. 보안 분류는 조직에 주어진 임무를 수행하고, 자산을 보호하며, 법적인 책임을 이행함으로서 일상 기능 유지 및 인원의 보호를 위해 필요한 정보 및 정보 시스템을 위협하는 어떤 사건이 발생한 경우의 조직에 대한 잠재적 영향에 기반을 둔다. 보안 분류는 조직의 위험에 대한 평가를 할 때, 취약점과 위협 정보를 함께 사용한다.

2.1.1 보안 목적

FISMA는 정보 및 정보 시스템의 보안 목적들을 다음 3가지로 정의한다.

- □ 기밀성 : 「개인 프라이버시와 소유 정보를 보호하는 방법을 포함하여 정보 접근이나 게시에 대한 제한을 설정한다.」(전자정부법) 기밀성의 손실은 정보의 비인가 게시를 의미
- □ 무결성 : 「부적절한 정보 변조나 파기로부터 보호하고 부인방지와 인증에 대한 정보를 보증하는 것을 포함한다.」(전자정부법) 무결성의 손실은 정보의 비인가 변조나 파기를 의미
- □ 가용성 : 「신뢰할 수 있는 정보의 접근과 이용할 수 있는 것을 보증한다.」(전자정부법) 가용성의 손실은 정보 및 정보 시스템의 접근과 사용을 방해하는 것을 의미

2.1.2 조직과 인원에 대한 잠재적 영향

FIPS 199는 정보 및 정보 시스템에 대한 보안 침해(기밀성, 무결성, 가용성 손실)가 미칠 수 있는 조직 및 인원에 대한 잠재적 영향(potential impact)을 3개의 등급으로 정의하고 있다.

- □ 잠재적 영향도가 '하(Low)'인 경우
  : 기밀성, 무결성, 가용성의 손실이 조직의 운영,

조직의 자산, 인원에게 한정적인 악영향을 미칠 것으로 예상된다. 즉, 조직의 주요 기능을 수행할 수 있으나, 기능의 효과적인 측면에서는 감소하고 조직의 자산 및 재정적인 부분에 경미한 손실과 인원에게 경미한 피해를 초래

□ 잠재적 영향도가 '중(Moderate)'인 경우

: 기밀성, 무결성, 가용성의 손실이 조직의 운영, 조직의 자산, 인원에게 중대한 악영향을 미칠 것으로 예상된다. 즉, 조직의 주요 기능은 수행할 수 있으나, 기능의 효과성은 상당히 감소되었거나, 조직 자산에 심각한 손상을 미쳤거나, 인원의 생명에는 영향을 미치지는 않으나 상당한 피해를 초래

□ 잠재적 영향도가 '상(High)'인 경우

: 기밀성, 무결성, 가용성의 손실이 조직의 운영, 조직의 자산, 인원에게 치명적인 악영향을 미칠 것으로 예상된다. 즉, 조직의 주요 기능을 수행할 수 없으며, 기능의 효과성은 상당히 감소되었거나, 조직 자산에 심각한 손상을 미쳤거나, 인원의 생명에 영향을 미치거나 심각한 부상을 당하는 경우에 해당

2.2 정보 및 정보 시스템의 잠재적인 보안 영향 등급 분류

정보 및 정보 시스템 유형을 잠재적인 보안 영향 등급을 기준으로 분류하기 위한 지침인 SP 800-60(정보 및 정보 시스템의 유형과 보안 분류의 적용 지침)은 FIPS 199 수행을 용이하게 하기 위한 보조적인 지침이다. 이 지침은 2권으로 나누어져 있다. 제 1권에서는 정보 유형의 식별 및 보안 분류의 지침을 나타낸다. 제 2권에서는 영향 할당의 사례나 보안 분류의 근거에 의거한 부록으로 구성되어 있다[2][3].

2.2.1 영향 등급의 정의와 보안 분류

각 조직은 잠재적 정보의 영향도를 각자의 운영 환경의 틀 안에서 검토하고 검토 결과에 따라 영향도를 사용하거나 수정한다. 정보의 영향도는 조직의 운영 환경에 따라 정의한다. 어떠한 조직의 운영 환경에서는 영향이 낮은 정보 유형일지라도 다른 조직의 운영 환경에서는 높은 영향도를 가질 수 있다.

〔표 1〕 잠재적 영향 등급 정의

등급	정의	영향
상	기밀성, 무결성, 가용성의 손실이 조직의 운영·자산·인원에게 치명적인 악영향을 미칠 것으로 예상	조직의 주요 기능을 수행할 수 없으며, 기능의 효과성은 상당히 감소되었거나, 조직 자산에 심각한 손상을 미쳤거나, 인원의 생명에 영향을 미치거나 심각한 부상을 당하는 경우
중	기밀성, 무결성, 가용성의 손실이 조직의 운영·자산·인원에게 중대한 악영향을 미칠 것으로 예상	조직의 주요 기능은 수행 할 수 있으나, 기능의 효과성은 상당히 감소되었거나, 조직 자산에 심각한 손상을 미쳤거나, 인원의 생명에는 영향을 미치지 않으나 상당한 피해를 초래한 경우
하	기밀성, 무결성, 가용성의 손실이 조직의 운영·자산·인원에게 한정적인 악영향을 미칠 것으로 예상	조직의 주요 기능을 수행 할 수 있으나, 기능의 효과적인 측면에서는 감소하고 조직의 자산 및 재정적인 부분에 경미한 손실과 인원에게 경미한 피해를 초래한 경우

일반적으로 정보 시스템은 많은 정보 유형을 취급한다. 이러한 정보 유형은 모두 같은 영향도를 가지는 것은 아니다. 손실된 정보 유형의 경우에는 다른 정보 유형들보다 시스템의 기능이나 연방기관의 임무를 크게 위협 할 수도 있다. 시스템 영향도는 시스템 임무와 기능뿐만 아니라 구성요소와 정보 유형을 모두 통합해서 평가를 실시해야 한다.

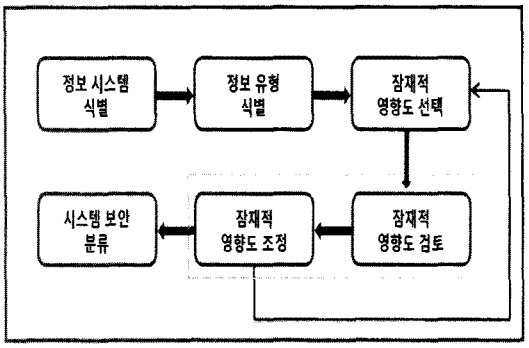
조직 및 개인의 잠재적 영향도는 [표 1]과 같이 '상', '중', '하' 3가지 등급으로 다음과 같이 정의한다.

2.2.2 정보 유형과 보안 관리 대책 및 영향 등급의 적용

정보 유형과 정보 시스템의 보안 통제 및 영향 등급에 적용하는 단계적인 방법론을 제공한다. 보안 등급 할당은 FIPS 199에 근거한다. [그림 2]는 보안 분류 과정을 보여주고, 보안 분류가 어떻게 보안 통제의 선택 과정을 충족시키는지 그 방법을 보여준다. 본 과정은 정보 시스템마다 실행된다.

□ 정보 시스템 식별 : 정보 시스템에는 일반 지원 시스템, 주요 응용 시스템, 로컬 시스템, 특수한 용도에 사용되는 시스템 등이 있다. 연방기관은 보안 분류를 실시하기 위한 목적으로 자체적으로 시스템 식별에 관한 정책을 개발한다.

□ 정보 유형 식별 : 사용자는 시스템별로 입력, 저



〔그림 2〕 보안 분류 과정

장, 처리, 출력되는 모든 정보 유형을 식별한다.

- □ 잠재적 영향도 선택 : 사용자가 식별한 정보 유형별로 잠재적 영향도를 선택한다.
- □ 잠재적 영향도 검토 및 조정 : 사용자가 검토할 시스템에 관련된 조직, 환경, 임무, 이용 및 접속에 근거하여 사용자의 정보 유형에 대해서 권고되고 있는 잠재적 영향도의 적절성을 검토한다. 잠재적 영향도를 검토 후 필요에 따라 영향도를 조정한다.
- □ 시스템 보안 분류 : 다음으로 검토할 시스템에 관련된 기밀성, 무결성, 가용성의 영향도를 결정한다. 정보 유형의 영향도는 각 시스템에 의해 처리된 모든 정보를 통합하여 검토한다.

보안 분류 과정이 완료되면 결과물에서 획득한 기밀성, 무결성, 가용성 영향도를 결정하고, 시스템의 위험 평가 및 보안 대책 선택에 이용할 수 있다.

Ⅲ. 보안 통제 선택

FIPS 200(연방기관의 정보 및 정보 시스템들의 보안 분류를 위한 표준)은 연방기관의 정보 및 정보시스템에 대한 최소 보안 요구사항과 그것을 만족하기 위해 필요한 보안 통제를 위험에 따라 선택하는 과정을 나타낸다. FIPS 200은 정보 보안을 위해 시스템에 요구되는 최소 보안 통제를 위한 시스템 등급 설정 기준을 제공하고, 연방기관 내에 안전한 정보 시스템을 개발하여 도입 및 운영을 촉진시키는데 목적이 있다. 또한 최소 보안 요구사항에 적절한 정보 시스템에 대한 보안 통제를 선택하고 반복 가능한 접근방법을 제공한다[4].

SP 800-53(연방기관 정보 시스템에 대한 권고된 보안 통제)의 목적은 연방기관의 집행기관을 지원하는 정보 시스템에 대한 보안 통제를 올바르게 선택하기 위한 지침을 제공한다. 이 지침은 연방기관의 정보를 처리, 저장, 전송, 수신하는 정보 시스템의 모든 구성요소에 적용되면 연방기관의 정보 시스템을 다음의 방법에 따라 안전하게 하기 위해서 개발되었다[5].

- □ 정보 시스템의 보안 통제 선택 및 설정은 일관성 있게 비교 가능하고 반복적인 접근을 쉽게 한다.
- □ FIPS 199에 따라 분류된 정보 시스템에 대한 최소한의 보안 통제 권고를 나타낸다.
- □ 조직의 정보 보안에 대한 현재의 요구를 충족시킬 뿐 아니라, 향후 요구사항과 기술의 변화에 따라 변화하는 요구를 충족하기 위해 안정성과 유연성을 갖춘 보안 통제 목록을 제공한다.
- □ 보안 통제의 유효성을 판단하기 위한 평가 방법 및 절차 개발 기반을 구축한다.

3.1 최소 보안 요구사항

최소 보안 요구사항은 연방기관 정보 시스템의 기밀성, 무결성, 가용성을 보호하며 시스템에 의해 처리되고 저장되는 정보에 관한 17가지의 보안 관련 분야를 모두 포함하고 있다. 이러한 분야에는 연방기관의 정보 및 정보 시스템 관리, 운영, 기술 측면을 포함하고 정보보안 프로그램 범위에서 균형이 잡힌 상태임을 나타낸다. 정책 및 절차는 정보 보안 프로그램을 연방기관 전체에 효과적으로 도입하여 연방기관의 정보 및 정보 시스템을 보호하기 위해서 도입된 보안 통제의 성공을 위해 중요한 역할을 하고 있다. 따라서 조직은 FIPS 200에 포함되어 있는 최소 보안 요구사항을 통제하기 위해 문서화된 정책과 절차를 작성하고 배포하여 효과적으로 도입할 수 있도록 해야 한다.

3.2 보안 통제 권고

3.2.1 보안 통제의 구성과 구조

보안 통제는 구성과 구조가 명확하게 정의되고 있다. 보안 통제는 통제 선택 및 설정, 두 과정에서도 쉽게 사용할 수 있도록 클래스와 패밀리에 따라 구분된다. 보안

〔표 2〕 보안 통제의 클래스, 패밀리 및 식별자

식별자	패밀리	클래스
AC	접근 통제	기술
AT	의식향상 및 훈련	운영
AU	감사와 책임 추적성	기술
CA	인증, 승인, 보안 평가	관리
CM	구성 관리	운영
CP	비상 대응 계획	운영
IA	식별 및 인증	기술
IR	사고 대응	운영
MA	유지 보수	운영
MP	기록매체 보호	운영
PE	물리적 및 환경적인 보호	운영
PL	계획	관리
PS	인적 보안	운영
RA	위험 평가	관리
SA	시스템 및 서비스 조달	관리
SC	시스템 및 통신 보호	기술
SI	시스템 및 정보 무결성	운영

통제에는 3가지의 일반적인 클래스(관리, 운영, 기술) 및 17개의 패밀리가 있다. 각 패밀리는 패밀리 고유의 보안 기능과 관련이 있는 보안 통제가 포함되어 있다. 또한 각 패밀리는 패밀리를 고유하게 식별하기 위한 식별자(2자)를 할당하고 있다. [표 2]는 보안 통제 목록의 클래스와 패밀리의 대응과 각 패밀리의 식별자를 나타낸다.

각 통제를 고유하게 식별하기 위해 패밀리 식별자에 숫자 식별자(통제가 패밀리 중 몇 번째 통제인지 나타내는 값)를 추가하고 있다. 예를 들어, CP-9는 비상 대응 계획 패밀리 중 9번째 통제이다.

3.2.2 보안 통제 기준

조직은 법률, 대통령령, 지시, 정책이나 규정(ex : FISMA, OMB 회람 A-130 부록 III)이 결정하는 보안 요구사항을 준수한 보안 통제의 채택을 요구하고 있다. 조직의 과제는 적절한 보안 통제를 선택하기 위한 것이다. 적절한 보안 통제는 도입 후 그 유효성이 입증되어야 하며, 비용-효과가 높은 방법으로 보안 요구사항을 충족해야 한다. 조직에 특정한 보안 요구사항을 충족하는 보안 통제를 제대로 선택하는 것은 중요한 작업이다.

3.2.3 공통 보안 통제

조직 전체의 정보 보안 프로그램을 파악하여 조직의 1개 이상의 정보 시스템에 적용할 수 있는 공통 보안 통제를 파악하는데 도움이 된다. 공통 보안 통제는 조직 전체의 정보 시스템, 특정 장소의 정보 시스템 그룹, 여러 운영 거점에 배치된 공통 정보 시스템, 서브시스템 또는 애플리케이션에 적용될 수 있다. 공통 보안 통제는 다음과 같은 특징을 갖는다.

- □ 공통 보안 통제를 개발, 도입, 평가의 책임을 조직의 책임자 또는 부서에 할당할 수 있다.
- □ 공통 보안 통제의 평가 결과는 통제가 적용되는 정보 시스템의 보안 인증 및 승인 과정의 증명으로 사용할 수 있다.

3.2.4 외부 환경의 보안 통제

조직에서 중요한 임무와 기능을 수행하기 위해 외부 서비스 제공자가 제공하는 정보 시스템의 서비스에 의존하는 경우가 많아지고 있다. 외부 서비스 제공자와의 관계는 다양한 형태로 구성된다.

조직의 업무와 자산, 인원에 대한 위험을 수용할 수 있는 등급에 대한 보증이나 신뢰는 승인 책임자가 외부 서비스 제공자를 얼마나 신용하고 있는지 여부에 따라 달려있다. 경우에 따라 서비스를 보호하기 위한 보안 통제의 선택뿐 아니라, 이러한 통제의 유효성을 입증하는 증거의 제출에 대해 승인 책임자가 외부 서비스 제공자를 얼마나 직접 관리할 수 있을지에 근거하기도 한다. 외부 서비스 제공자를 관리할 수 있는 방법은 일반적으로 계약 및 서비스 레벨 보증서(SLA)의 조건에 의해 결정된다.

3.2.5 보안 통제 보증

보증은 정보 시스템에 도입된 보안 통제의 유효성을 보증하는 것이고, 신뢰의 근거가 된다. 보증은 다음과 같은 여러 가지 방법으로 얻을 수 있다.

- □ 보안 통제의 개발자나 도입자가 통제를 설계, 개발 및 구현 기술과 기법의 일환으로 실행하는 작업
- □ 통제가 얼마나 제대로 구현되고 있는지, 예상대로

운영되고 있는지, 시스템의 보안 요구 사항에 대한 적합성의 입장에서 원하는 결과를 어느 정도 생산하고 있는지에 대한 테스트 및 평가 과정에서 보안 통제의 평가자가 취하는 행동

3.2.6 수정 및 확장

통제 목록에 나열되는 보안 통제는 정보 시스템의 최신 보호 수단 및 대책으로 현재 실시되고 있는 것이다. 보안 통제는 다음과 같은 요소를 반영하기 위하여 정기적으로 재검토되고 개정된다.

- □ 통제를 사용함으로써 얻은 경험
- □ 조직의 보안 요구사항의 변경
- □ 새로운 위협과 공격 방법의 출현
- □ 추가로 사용할 수 있는 보안 기술

3.3. 과정

3.3.1 초기 기준의 선택과 조정

정보 시스템에 대한 종합적인 영향도가 명확해지면, 영향도 '하', '중', '상' 기준 통제 중에서 보안 통제의 초기 설정을 선택할 수 있다. 조직은 이 지침에서 설명한 조건에 따라 기준 보안 통제를 자유롭게 조정할 수 있다. 조정 활동에는 다음과 같은 것들이 포함된다.

- □ 기준 통제의 초기 설정에 적합한 스코핑 지침(scoping guidance)을 적용
- □ 필요한 경우, 추가적인 보안 통제를 지정
- □ 보안 통제에 대한 매개 변수를 지정할 수 있는 경우에는 조직이 정한 매개변수를 지정

3.3.2 조정된 기준에 추가

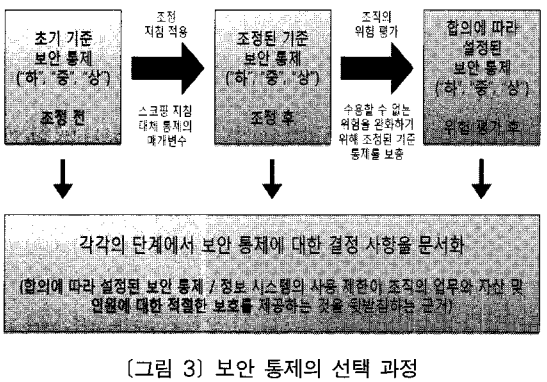
조정된 보안 기준 통제는 정보 시스템에 적절한 보안 통제를 찾기 위한 기점 또는 시작점으로 봐야 한다. 조정된 기준 통제는 조직이 조직의 업무와 자산을 보호하기 위해 필요한 정보 보안상의 선관주의의무(Due Diligence)를 결정할 때 사용한다. 또한 이러한 통제는 조직의 업무와 자산, 인원에 대한 위험을 충분히 완화할 수 있어야 한다.

대부분의 경우, 정보 시스템의 특정 위협과 취약성을 해결하거나 관련 법률, 대통령령, 지시, 정책, 표준, 규제의 요구사항을 충족하기 위해서는 추가적인 보안 통제나 통제 강화 방안이 필요하다. 보안 통제의 선택 과정에서 위험 평가와 조정된 기준의 보안 통제는 조직의 업무와 자산, 인원을 적절히 보호하기 위해 필요한 보안 통제가 위험을 충분히 줄일 수 있는 등급여부를 판단하는 중요한 입력 정보가 된다. 조직은 보안 통제의 강화 또는 조정된 통제에 대한 보충을 용이하게 하기 위해 보안 통제 목록을 최대한 활용하는 것이 권고된다.

경우에 따라서는 조직에서 자신이 사용하는 정보기술이 매우 높은 수준이지만, 현재 실시중인 통제는 조직의 중요하고 필수적인 임무를 적절하게 보호할 수 없다는 것을 알게 된다. 즉, 조직이 임무 위험을 완화하기 위한 보안 통제를 적용할 수 없다는 것이다. 이런 경우에는 대체 전략을 사용하여 조직의 임무에 방해되지 않도록 해야 한다. 여기서 대체 전략은 적극적인 정보 기술 이용에 의한 임무 위험에 대처하기 위한 전략이다. 정보 시스템의 사용에 대한 제한은 다음과 같은 경우에 위험을 완화하기 위한 대안으로 사용할 수 있다.

- □ 기술 및 자원상의 제약으로 인해 보안 통제를 도입할 수 없는 경우
- □ 확인된 위협원에 대한 통제가 충분한 효과를 기대할 수 없는 경우

[그림 3]은 보안 통제의 선택 과정을 나타낸다. 이 중에는 초기 기준 통제에 대한 조정 및 조직의 위험 평가에 근거하여 수정한 기준 보안 통제가 포함되어 있다.



〔그림 3〕 보안 통제의 선택 과정

Ⅳ. 보안 통제 조정

SP 800-30(정보 기술 시스템을 위한 위험 관리 지침)은 IT 시스템에서 식별된 위험 평가 및 완화를 정의하며 실무상의 지침을 포함하고 효과적인 위험 관리 프로그램 구축을 위한 기초 방안을 제공한다. 궁극적으로 추구하는 목표는 IT와 관련된 임무에 대한 위험을 조직이 적절하게 관리할 수 있도록 지원하는 것이다. 또한 SP 800-30은 높은 보안 통제를 선택하기 위한 정보도 제공한다. 이러한 통제는 위험을 완화하고, 업무에 관련된 정보와 이러한 정보를 처리, 저장, 전달하는 IT 시스템을 적절하게 보호할 수 있다. 조직은 SP 800-30에서 제안하는 포괄적인 과정과 절차를 확장하거나 생략하여 각각의 환경에 맞는 IT 관련 임무에 대한 위험을 관리할 수 있다[6].

- □ 조직의 정보를 저장, 처리, 전송하는 IT 시스템을 보다 효율적으로 보호
- □ 경영진이 충분한 정보를 바탕으로 위험 관리에 대해 적절한 판단을 내리고, IT 예산의 일부가 되는 위험 관리에 대한 지출을 효율성 있게 수행
- □ 위험 관리 실시의 결과로 작성되는 문서에 근거해 경영진이 IT 시스템에 대해서 승인을 실시할 수 있도록 지원

4.1 위험 관리

4.1.1 위험 관리의 중요성

위험 관리는 IT 관리자가 그 운영과 보호 수단의 경제적 비용의 균형을 잡으면서 조직의 임무를 지원하는 IT 시스템과 데이터를 보호함으로써 임무 수행 능력을 향상시키는 것을 수행하는 과정이다.

조직의 대표는 조직의 임무 달성에 필요한 능력을 확보해야 한다. 이러한 임무의 책임자는 실제로 위협에 직면할 경우, 임무 수행에 필요한 지원 등급을 제공하기 위해서 IT 시스템을 제공해야 하는 보안 능력을 확인할 필요가 있다. 다수의 조직은 IT 보안에 대한 예산 책정에 어려움을 가지고 있다. 따라서 IT 보안에 대한 지출은 다른 경영 판단과 마찬가지로 철저하게 검토해야 한다. 효율적으로 체계화된 위험 관리 방법론을 효과적으로 사용하는 경우, 임무 수행에 필수적인 보안 능력을 제공하기 때문에 경영진이 효율적인 통제를 확인하는데 도움이 된다.

4.1.2 개발 생명 주기 위험 관리의 통합

조직이 IT 시스템에 위험 관리 과정을 도입하는 주된 이유는 조직에 부정적인 영향도의 최소화 및 의사 결정을 위한 확실한 근거를 제공하는데 있다. 효과적인 위험 관리는 개발 생명 주기에 통합해야 한다. IT 시스템의 개발 생명 주기는 5단계로 다음과 같다. 공개 단계, 개발/구매 단계, 구현 단계, 운영/유지 보수 단계, 폐기 단계이다. 경우에 따라서는 1개의 IT 시스템이 여러 단계에 있을 수 있다. 그러나 위험 관리의 방법론은 평가가 실시되는 개발 생명 주기의 어느 단계에서나 마찬가지이다. 위험 관리는 개발 생명 주기의 주요 단계에서 실

〔표 3〕 개발 생명 주기 위험 관리의 통합

개발 생명 주기 단계	특징	위험 관리 활동의 지원
1단계 공개	IT 시스템에 대한 요구를 나타내고 IT 시스템의 목적과 적용 범위를 문서화	확인된 위험의 보안 요구사항 및 운영시 보안 대책을 포함하는 시스템 요구사항을 만드는데 이용
2단계 개발/구매	IT 시스템을 설계, 구매, 프로그램 개발 또는 구축	확인된 위험은 시스템 개발의 구조와 설계 교환에 연결하는 IT 시스템 보안 분석에 이용
3단계 구현	시스템의 보안 기능을 구성, 유효화, 시험, 검증	위험 관리 과정은 해당 요구사항과 그 모델화된 운영 환경에서 시스템 도입에 관한 평가를 지원. 확인된 위험에 대한 판단은 시스템 운영 전에 결정
4단계 운영/유지 보수	하드웨어와 소프트웨어를 추가하거나, 조직 과정, 정책, 절차의 변화에 따라 시스템은 계속적으로 변경	정기적인 시스템의 재승인에 대해서, IT 시스템의 운영, 제공 환경의 큰 변화가 있는 경우에는 반드시 위험 관리 활동을 실시
5단계 폐기	정보, 하드웨어, 소프트웨어의 폐기가 이루어질 수 있다. 그 중에는 정보의 이동, 보관, 폐기, 파괴, 하드웨어와 소프트웨어의 무해화가 포함	하드웨어와 소프트웨어가 적절히 폐기되고 잔여 데이터가 제대로 처리되고 시스템 이동을 안전하고 조직적인 방법으로 이루어질 수 있도록 하기 위해 폐기 또는 교체 예정 시스템 구성 요소에 대한 위험 관리 활동을 수행

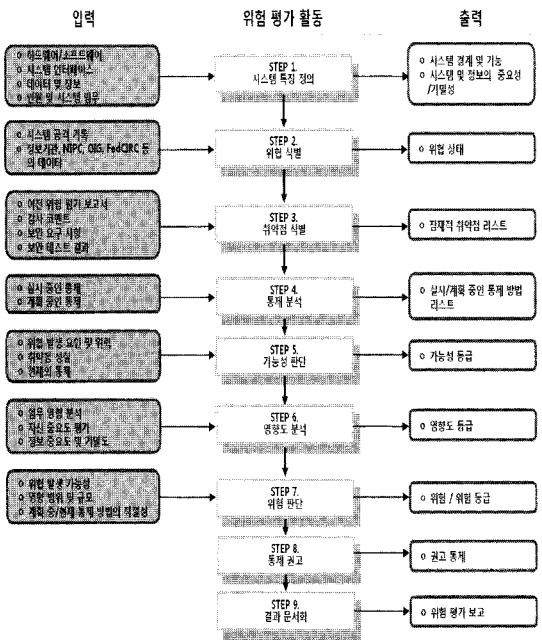
행할 수 있는 반복적인 과정이다. [표 3]은 각 개발 생명 주기 단계의 특징과 각 단계를 지원하기 위한 위험 관리의 실시 방법에 대해서 나타낸다.

4.2. 위험 평가

위험 평가는 위험 관리 방법의 첫 번째 과정이다. 조직은 위험 평가를 이용하여 개발 생명 주기 전체를 포함한 IT 시스템의 잠재적 위협 및 위험의 규모를 판단한다. 이 과정에서 출력은 위험 완화 과정에서 위험을 감소 또는 제거하기 위한 적절한 관리 방법을 식별하는데 효과적이다.

위험이 발생할 가능성을 판단하기 위해서 잠재적 취약성과 IT 시스템에 도입된 통제와 함께 IT 시스템에 대한 위협 분석이 필요하다. 임무에 대한 잠재적 영향의 정도가 영향도를 좌우하고 영향을 받는 IT 자산과 자원의 상대적 가치를 결정한다.

2, 3, 4, 6단계는 1단계를 완료 후에 병행하여 실행할 수 있다. [그림 4]는 각 단계에서 정보의 입력과 출력을 보여준다.



〔그림 4〕 위험 평가

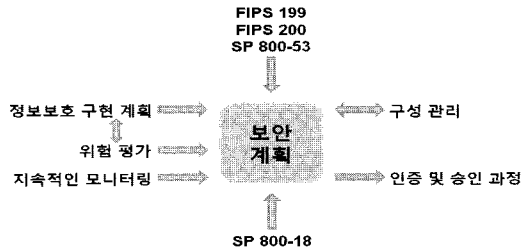
Ⅴ. 보안 통제 문서화

SP 800-18(연방기관 시스템을 위한 보안 계획 개발 지침)은 FIPS 199에 기술된 정보 시스템의 분류 요구사항과 SP 800-53 및 FIPS 200에 기술된 특정 시스템에 필요한 최소 보안 통제를 이용하여 선택된 보안 통제를 SP 800-30을 통해 조정한 후, 이를 시스템 기반의 보안 계획으로 문서화하기 위한 지침을 제공하기 위해 작성되었다[7].

5.1. 시스템 보안 계획에 대한 책임

연방기관은 시스템 보안 계획 과정에 대한 정책을 만들어야 한다. 시스템 보안 계획은 지속적으로 업데이트 되는 문서이고, 보안 통제를 실시하기 위한 정기적인 재검토, 수정, 정보 보안 구현 계획을 필요로 한다. 계획을 검토하고 계획을 최신 상태로 유지하고 계획한 보안 통제를 확인하는 방법에 대한 요점을 정리하는 절차를 마련해야 한다. 또한 시스템에 대한 보안 인증 및 승인 과정을 진행하기 전에 시스템 보안 계획의 개발 및 검토를 이행하는 과정이 요구사항에 포함되어야 한다.

보안 인증 및 승인 과정에서 시스템 보안 계획의 분석, 업데이트, 수용을 실시한다. 인증자는 시스템 보안 계획에 기술된 보안 통제가 정보 시스템에 지정된 FIPS 199 보안 분류를 준수하는지 확인하고 시스템 보안 계획, 위험 평가 또는 동등한 문서의 위협 및 취약성의 식별과 초기 위험 판정이 식별되고 문서화가 되고 있는지 확인한다. 보안 인증 결과는 위험의 재평가, 복구 활동을 추적하는데 필요한 정보 보안 구현 계획 작성, 시스템 보안 계획의 업데이트에 사용되고 나아가서 승인 책임자가 보안 승인 결정을 내릴 때 사실에 근거한 자료를 제공한다.



〔그림 5〕 정보보안 계획 수립을 위한 입력/출력물

여기서 언급하는 역할과 책임은 연방기관의 다양한 임무와 조직 구조를 근거로 하는 경우 보안 계획 관련 역할에 대한 명명 규칙이나 연방기관 직원에 대한 책임을 할당하는 방법(ex : 1개의 역할을 여러 명의 담당자

에게 할당하거나 여러 개의 역할을 1명의 담당자에게 할당 등)이 다른 경우가 있다.

Ⅵ. 보안 통제 구현

SP 800-70(IT 제품을 위한 보안 구성 점검표 프로그램 - 점검표 사용자와 개발자를 위한 지침)은 IT 제품의 보안 구성 점검표의 사용자와 개발자를 대상으로 하고 있다. 점검표의 사용자에 대해서는 보안 구성 점검표와 그 이점을 설명하고, NIST 점검표 프로그램을 사용해서 점검표를 검색 및 취득하는 방법을 설명한다. 개발자에 대해서는 NIST 점검표 프로그램 참여 정책, 절차, 일반적인 요구사항을 설명한다[8].

6.1 NIST 보안 구성 점검표 프로그램

이 부분에서는 NIST 점검표 프로그램을 설명한다. 첫째로, 점검표의 내용을 설명하고, 점검표를 작성하는 빈도가 높은 IT 제품군의 예를 보여준다. 다음으로 보안 설정 점검표를 통해 얻은 이점을 설명한다. 또한 NIST 점검표 프로그램의 목표와 이점도 제공한다. 점검표의 사용자와 개발자 절차 및 운영 환경에 대한 종류의 개요와 구성 점검표 사용과 관련된 FISMA 관련 지침 요약을 보여준다.

6.1.1 보안 구성 점검표 정의

보안 구성 점검표는 기본적으로 운영 환경에 맞추어 IT 제품을 구성하기 위한 지침이나 절차를 기재한 문서이다. 점검표는 IT 개발 업체, 컨소시엄, 학계, 업계, 연방기관, 기타 정부 기관, 기타 공공 및 민간 부분에 의해 개발된다. 점검표에는 다음의 요소가 포함된다.

- □ 다양한 보안 구성을 자동적으로 구성하는 구성파일
- □ 점검표 사용자에게 IT 제품을 수동으로 구성하는 방법 설명
- □ 장치를 안전하게 설치 및 구성하기 위해 권고되는 방법 설명
- □ 감사, 인증 메커니즘 및 경계 보안 등의 사항에 관한 지침을 기재한 정책 문서

보안 점검표의 대상이 되는 장치 및 소프트웨어의 일부 유형은 다음과 같다.

- □ 범용 운영 시스템
- □ 일반적인 데스크탑 응용 프로그램
- □ 라우터와 같은 기반구조(ex : 라우터, 방화벽, VPN, IDS 등)
- □ 응용 프로그램 서버(ex : DNS, DHCP, SMTP, FTP 등)
- □ 모바일 장치, 스캐너, 프린터, 복사기, 팩스 복합기 등

6.2. NIST 점검표 프로그램

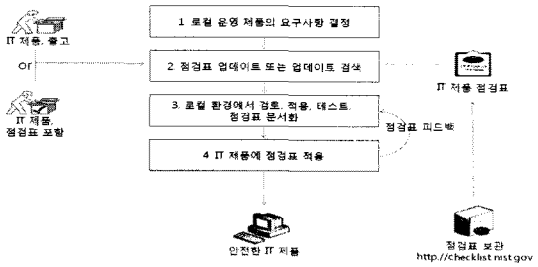
NIST 프로그램은 점검표를 체계적이고 간편하게 사용할 수 있으며, NIST 프로그램의 목표는 다음과 같다.

- □ 개발자가 NIST 점검표를 제출하기 위한 프레임워크를 제공함으로써 점검표의 개발 및 공유를 촉진
- □ 동일한 환경에 접속된 다양한 종류의 시스템을 보호하기 위한 일관된 접근법을 제공함으로써 개발자를 지원
- □ 점검표의 검토, 업데이트, 유지 보수에 대한 관리 과정을 제공

6.3. 점검표 사용

가정 사용자에서부터 대규모 조직의 시스템 관리자에 이르는 모든 점검표 사용자에게도 각각 고유한 요구사항이 있지만, 여기에서 설명하는 과정은 대부분의 경우에 해당된다. 이 부분에서는 로컬 환경의 위협과 위험, 위협이 발생한 경우의 영향도에 대한 초기 분석을 실시하기 위한 지침이 포함된다. 다음은 NIST 점검표 보고서에서 점검표를 선택하고, 구매하는 과정을 설명하며 점검표의 분석, 조정, 신청 절차를 권고한다.

[그림 6]에는 점검표를 사용하는 일반적인 프로세스를 보여준다. 1단계에서 점검표를 사용하는 사용자는 로컬 요구 사항 및 보안 요구 사항 또는 보안 정책을 분석하고 적절한 운영 환경 모델을 확인한다. 그 다음 사용자는 필요한 상황에 적합한 IT 제품을 선택한다. 2단계에서 사용자는 IT 제품과 선택한 운영 환경에 일치하는 점검표를 보고서에서 참조한다. 사용자들은 함께 제공되는 문서 및 도구와 함께 점검표를 다운로드한다. 3단계에서 사용자는 다운로드한 점검표 확인 및 테스트



〔그림 6〕 점검표 사용자의 프로세스

를 거쳐, 필요한 경우 로컬 정책 및 기능에 대해 점검표를 사용자 정의한다. 점검표에 대한 의견은 보고서를 통해 NIST와 개발자에게 전달할 수 있다. 4단계에서 사용자는 점검표 신청에 실패하고, 점검표의 신청에 의해 예기치 않은 문제가 발생 할 경우 영향을 받을 우려가 있는 정보를 백업하여 점검표를 실제 운영 시스템에 적용하기 위한 준비를 실시한다. 마지막으로 점검표를 실제 운영 시스템에 적용한다.

Ⅶ. 보안 통제 평가

SP 800-53A(연방기관 정보 시스템의 보안 통제 평가 지침)는 연방기관의 효력 있는 정보 시스템 보안 통제 평가를 위해 포괄적인 절차 제시 및 보안 평가 계획을 수립한 지침이다. 지침은 SP 800-53의 보안 시스템 정의 및 연방 정보 보안 시스템을 위한 보안 통제 권고가 적용되며, 기관에 의해 추가적인 보안통제가 개발되기도 한다. 연방기관은 정보 시스템의 보다 높은 보안성을 위해 지침을 개발하였다[9].

- □ 일관성, 우수성, 지속적인 법적 효력이 있는 보안 통제의 평가
- □ 효율적 보안 통제를 통합 규정하여 예산 낭비 방지
- □ 정보 시스템의 운영에서 우려되는 위험성에 대한 인식 및 이해도 기여
- □ 보다 완전하고 신뢰성 있는 정보가 필요한 기관에 보안 인가 결정과 정보 공유 및 FISMA 준수 제공

7.1 기준

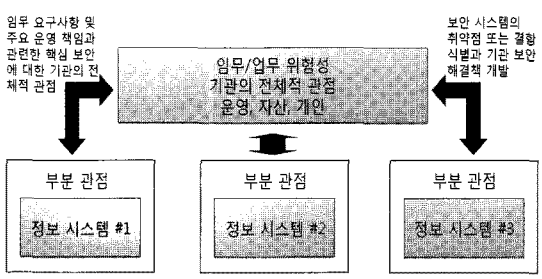
7.1.1 시스템 개발 생명 주기 내의 평가

정보 보안 평가는 신청 받은 정보 시스템에 사용된 보안 통제의 효율성, 신뢰성, 보증을 위해 시스템 개발 생명 주기의 다양한 단계를 실행한다. SP 800-53A는 시스템 개발 생명 주기에 정보 보안 평가 활동을 지원하기 위해서, 평가의 포괄적인 절차를 제공한다. 또한, 정보 보안 평가는 시스템이 사용되는 운영 환경에서 보안 통제를 보증하는데 도움이 되도록 생명 주기의 운영 및 유지 보수 단계 사이에 정보 시스템 소유자, 정보 보안 담당자, 승인 책임자, 회계 감사원 및 일반 감사관에 의해 수행된다. 정보 보안 평가 보증은 생명 주기의 마지막에 수행된다.

7.1.2 정보 보안 통제 평가를 위한 전략

기관은 정보 보안 평가를 실시하기 위한 전략 개발을 장려하며, 보다 효율적인 비용과 일관성 있는 평가를 촉진한다. 평가 전략은 정보 보안 분류 과정, 보안 통제 선택 과정 및 공통 보안 통제 식별의 체계적인 검증에 의한 위험 관리 프레임워크 초기 단계를 모든 정보 시스템에 적용시킨다. 기관은 최대한 공통 통제를 사용하도록 한다.

- □ 정보 시스템 평가 결과 검토 후 임무/업무 관련의 활동 사항 결정에 참고하며 기관의 정보 시스템에서 체계적인 위험에 대한 영향도 평가 및 조직을 지원하는 정보 시스템의 영향도 수준의 기능 정보 제공
- □ 기관의 전체적인 정보 시스템 체계의 약점 및 결함 검증 제공
- □ 전체 기관의 정보 보안 문제 해결 방안 제공
- □ 전체 정보 보안 문제의 효율적 해결 비용을 위하여 위협, 취약점 및 전략에 관한 자료 보관



〔그림 7〕 정보 시스템 평가와 임무/업무에 대한 위험성

[그림 7]은 독자적인 정보 시스템의 평가 및 임무/업무 위험성의 전체적 결정과 수용 사이의 관계를 설명한다.

보안 통제 평가를 관리하는 것은 정보 시스템 관리자에게 공식적으로 부여된 주요 권한이며 반드시 평가 결정 권리를 갖고 있는 유관기관의 적극적인 참여를 필요로 한다.

7.1.3 평가 절차

평가 절차는 각각의 평가 방법, 평가 대상, 평가 목적으로 이루어진다. 평가 목적은 특정 보안 통제와 관련된 결정 보고서를 포함한다. 결정 보고서는 보안 통제 요구사항에 대한 평가 결과를 보증하기 위하여 SP 800-53 내용과 밀접한 관련이 있다. 평가 결과는 보안 통제의 전체 효율성을 결정하는데 도움이 되도록 사용된다.

평가 대상은 데이터 항목을 구체적으로 식별하며 명세서, 메커니즘, 활동 및 인원을 포함한다. 명세서는 정보 시스템의 평가 결과 문서이다(ex : 정책, 절차, 대책, 시스템 정보 보안 요구사항, 기능 설계, 구조상의 설계). 메커니즘은 구체적인 하드웨어, 소프트웨어 또는 정보 시스템 내에서 사용된 펌웨어의 예방 수단 및 대책이다. 활동은 인원과 관련된 정보 시스템을 지원하고 있는 구체적인 보안 관련 수행 또는 행동이다. 인원 또는 그룹은 위에 설명된 명세서, 메커니즘, 또는 활동을 적용하는 인원이다.

평가 방법은 평가자의 활동 및 검사, 면접, 테스트를 규정한다. 검사 방법은 평가 대상의 검토, 검사, 관찰, 연구 또는 분석이다. 평가 방법의 목적은 평가자의 업무를 돕는 것이며, 검사 방법의 목적은 평가자에게 목적 설명 또는 증명의 이해를 돕는 것이다. 테스트 방법은 현실에서 예상되는 행동과 비교하기 위해서 지정된 조건 하에 1개 이상의 평가 대상을 테스트하는 과정이다. 3개 평가 결과는 평가 결정에 반영되며 평가 절차 요구사항을 만족하게 된다.

각각의 정보 시스템 영향도는 SP 800-53에 정의된 최소 보증 요구사항을 갖고 있다. 보안 통제 개발자와 구현자는 보증 요구사항을 준수한다. 보증 요구사항에 근거하여, 보안 통제 개발자와 구현자는 요구되는 활동을 수행한다. 이 활동의 목적은 보안 통제의 정확한 수행과 정보 시스템의 의도적 운영을 위한 보안 요구사항 충족을 돕는 것이다. 평가자는 개발자 및 구현자에게 보안 통제 보증을 위해 정보를 제공 받을 수 있다.

7.2 과정

7.2.1 보안 통제 평가를 위한 준비

기관의 준비 활동은 평가담당자의 효율적인 보안 통제 평가 수행에 중요한 영향을 미친다. 준비 활동은 비용, 일정, 평가의 수행과 관련된 범위이다. 기관은 보안 통제 평가를 위한 다음 사항을 준비한다.

- ☐ 보증을 위한 보안 통제 평가 정책을 기관 내에 공지하여 이해를 돕는다.
- ☐ 통제 평가 단계의 사전 요구사항인 NIST의 위험관리 프레임워크를 갖춰야 하며, 관리 담당자를 지정해야 한다.
- ☐ 공통 통제에 따른 보안 통제 보증은 기관 실정에 적합하게 개발 및 실행되어야 한다.
- ☐ 보안 통제 평가의 목적과 적용범위를 설정한다.
- ☐ 중요한 보안 통제 평가가 위급하게 수행될 상황에 대비하여 기관 직원을 배치한다.
- ☐ 보안 통제 평가에 관계된 기관 직원 사이에 통신 연락망을 개설한다.
- ☐ 기관은 평가 관리의 효율성을 위해 보안 통제 평가 및 표준안에 준수한 평가 결정 시간 계획을 수립한다.
- ☐ 보안 통제 평가 실행을 책임질 독립적인 평가자/평가팀을 구성한다.
- ☐ 평가자/평가팀에게 관련 문서를 제공한다(정책, 절차, 계획, 명세서, 구조, 데이터, 관리자/운영자 매뉴얼, 정보 시스템 문서, 상호 협정 관계, 이전 평가 결과).
- ☐ 보안 통제 실행에 관한 부정확한 표현, 오해, 보안 통제 약점/결점을 최소화하기 위해서 기관과 평가자, 평가팀 사이의 절차를 마련한다.

7.2.2 정보 보안 평가 계획 개발

정보 보안 평가 계획은 보안 통제 평가 및 평가 방법의 로드맵이다. 보안 통제 평가의 최종 결과 및 출력이 정보 보안 평가 보고서가 된다. 정보 시스템 보증 문서는 정보 보안 승인 패키지의 3개 중요 문서 중 하나이다. 평가자는 정보 보안 평가 보고서에 근거하여 정보 시스템 및 기관 전체에 사용될 효율적인 보안 통제를

결정한다. 정보 보안 평가 보고서는 조직 운영, 기관 자산, 인원, 다른 기관 및 국가의 위험에 대한 승인 책임자의 결정에 있어서 중요한 요소이다.

다음은 기관 정보 시스템의 보안 통제 평가 시 고려할 사항에 대해 개발된 절차이다.

- □ 보안 통제 평가의 방법을 결정한다.
- □ 평가 목적/범위 및 보안 계획 구성요소에 기초하여 보안 통제/통제 기능을 결정한다.
- □ 보안 통제 및 통제 기능에 따른 평가 시 사용될 평가 절차를 선택한다.
- □ 정보 시스템의 영향도 수준을 위한 선택된 평가 절차 및 조직의 운영 환경을 맞게 조정한다.
- □ SP 800-53에 포함되지 않은 통제 보안 기능 제출 또는 SP 800-53A의 범위를 벗어난 보증이 필요한 경우를 대비한 평가 절차를 개발해야 한다.
- □ 확장된 평가 절차의 적용 전략을 개발해야 한다.
- □ 중복된 업무를 간소화한 효율적인 평가 절차와 평가 비용 절충 해결책을 수립한다.
- □ 평가 계획을 완료하면 승인을 받는다.

7.2.3 보안 통제 평가 수행

정보 보안 평가 계획이 기관에 승인된 후, 평가자 또는 평가팀은 이정표 및 일정에 따라서 계획을 실행한다. 평가 목적은 명시된 평가 방법을 선택된 평가 대상에 적용하고 각각의 평가 목적 관련 결정에 필요한 정보를 편집/생성을 완료하는 것이다. 평가자에 의해 실행된 평가 절차에 포함된 각각의 결정 보고서의 결과에 다음을 표시한다.

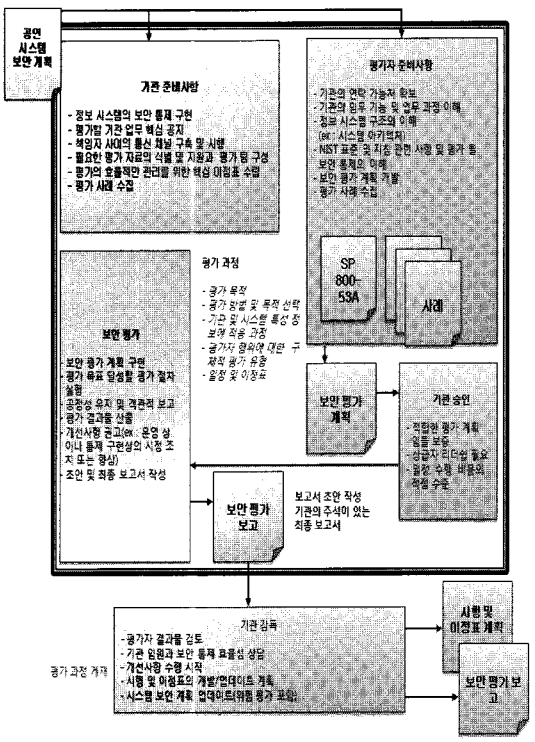
- □ 만족 : (S), 불만족 : (O)

만족된 평가 결과는 결정 보고서에 의해 작성된 보안 통제의 부분을 나타내며, 수집된 평가 정보가 통제 평가 결과 만족을 위한 평가 목적임을 나타낸다. 불만족한 평가 결과는 결정 보고서에 작성된 보안 통제 부분이 수집된 평가 정보가 통제의 운영 및 구현에 대해 기관이 추가로 작성해서 제출해야 할 잠재적인 예외 사항이 있음을 나타낸다. 불만족한 평가 결과는 평가 보고서에 이유를 명시하며, 평가자는 특정 결정에 필요한 충분한 정보가 없었음을 결정 보고서에 나타낸다.

7.2.4 정보 보안 평가 보고서 결과 분석

보안 통제 평가의 결과가 정보 보안 계획의 내용에 최종적으로 영향을 주고, 활동 및 이정표, 정보 시스템 소유자의 계획에 대한 평가자의 결과는 기관 임원의 검토 및 동의 하에 평가에서 식별된 약점과 결함을 정정하기 위한 절차를 결정한다. 만족 및 불만족을 표시하기 위한 평가 결과 보고서 양식은 기관 임원을 위해 약점과 결함의 명시에 대한 투명성 제공과 기관의 우선순위인 위험 완화를 위한 징계 및 구조를 조장한다.

완화 과정에서 선임 책임자 관여는 가장 중요하고 민감한 임무를 지원하는 정보 시스템의 위험 결함 제출 및 정정을 보증하기 위해서 필요하다. 결국 평가 결과 및 후속 조치 완화는 정보 시스템 소유자가 기관 관계자와 공동으로 위험 평가 및 보안 계획 업데이트 실행을 시작하게 된다. 따라서 승인 책임자에 의해 사용될 핵심 문서를 결정하는 정보 시스템의 보안 특성(업데이트된 위험 평가의 보안 계획, 보안 평가 보고, 실행 및



〔그림 8〕 보안 통제 평가 과정

일정 계획)은 보안 통제 평가의 결과를 반영하여 업데이트된다.

[그림 8]은 평가 이전, 평가 중, 평가 후 보안 통제 평가의 개요를 제공한다.

Ⅷ. 보안 인증 및 승인

SP 800-37(연방기관 정보 시스템의 보안 인증 및 승인 지침)의 목적은 연방기관의 운영 기관을 지원하고 있는 정보 시스템의 보안 인증 및 승인을 위한 지침을 제공한다. 지침은 연방기관 내에 보다 안전한 정보 시스템을 구축하는데 도움이 될 수 있도록 개발되었다[10].

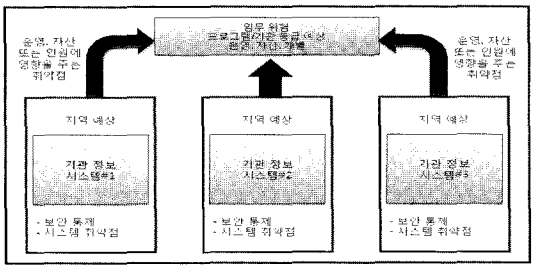
- □ 연방기관 정보 시스템의 보안 통제를 보다 일관성 있고, 비교가능하며, 반복할 수 있는 평가를 가능하게 한다.
- □ 정보 시스템의 운영으로 초래되는 기관 관련 임무의 위험에 대한 이해를 개선시킨다.
- □ 보안 승인에 관한 의사결정자에게 보다 완전하고, 신뢰할 수 있는 정보를 제공한다.

8.1 보안 인증 및 승인

보안 인증 및 승인은 매우 밀접히 관련되어 보이나, 실제로는 별개의 활동이다. 보안 승인은 정보 시스템의 기관 운영, 기관 자산, 인원 위험에 관한 수용 및 관리이다. 승인 책임자는 기관 운영, 자산, 인원, 임무, 업무에 필요한 위험의 수용에 대한 결정권을 가지며, 각 기관의 위험 수용 여부를 결정해야 한다.

보안 인증은 승인 책임자에게 정보 시스템 내의 운영이 적합한지 또는 그 운영이 현재 지속되고 있는지에 대한 신뢰성 있는 위험에 근거한 결정을 하기 위하여 필요한 중요한 정보를 직접적으로 제공한다. 이 정보는 통제의 정확한 운영을 위한 범위를 결정하기 위해 정보 시스템의 보안 통제 평가 및 시스템을 위한 보안 요구사항을 충족시키는 방법을 제공한다. 보안 인증은 기관에 필요한 폭 넓은 다양한 평가 방법(ex : 면접, 점검, 연구, 검사, 증명, 분석) 및 관련 평가 절차가 포함되어 있다.

보안 통제의 선택에 대한 결정은 정보 시스템의 보안 요구사항(보안 통제 선택, 승인 책임자, 상급기관 정보 보안 담당관에 의해 승인된 시스템 보안 계획)을 충족하는 시스템 개발 생명 주기의 개시 단계 사이에 해당



〔그림 9〕 정보 시스템의 취약성과 임무 위험

한다. 레거시 정보 시스템을 위한 시스템 보안 계획이 승인될 때, 보안 통제의 타당성 결정은 보안 인증 이전에 수행한다.

보안 인증은 기관 운영, 기관 자산, 인원에 관한 위험 결정을 포함하지 않는다. 각 프로그램 또는 각 기관의 위험 결정은 기술적인 초점, 보안 인증에 기인하여 정보 시스템의 시스템 등급 예상보다 기관의 전략적인 예상을 요구한다. 승인 책임자, 담당자에게 권한을 주는 것은 보안 통제 설정 후에 정보 시스템에 남아있는 알려진 취약성에 근거하여 위험 결정 임무를 수행하는 것이다. 이러한 위험 수용에 관한 최종 결정은 승인 책임자의 책임이다. 기관내 개별 조언이 필요할 때, 승인 책임자 또는 담당자는 인증 및 승인 과정의 어떤 단계에서도 정보 시스템의 보안에 관한 조언을 얻을 수 있다.

[그림 9]은 정보 시스템의 취약성 및 프로그램/기관 등급, 임무 위험 사이의 관계를 설명한다.

보안 승인은 진행 중인 위험 관리 과정의 동적인 부분이다. 정보 시스템은 시스템의 현재 보안 상태를 반영하고 있는 구체적인 시점에서 운영을 위해 인가된다. 정보 시스템(하드웨어, 펌웨어, 소프트웨어, 인원 포함)의 부득이한 변화와 이에 대한 잠재적 영향력을 가진 기관 운영, 기관 자산, 인원에게 정보 시스템의 원칙이 되는 보안 통제의 효율성을 모니터링이 가능하도록 구조적이고 숙련된 과정을 요구한다. 따라서 초기 보안 승인은 다음과 같은 내용을 지속적인 모니터링 과정으로 보충, 보완해야 한다.

- □ 정보 시스템의 변경 사항 추적
- □ 변경 사항이 보안에 미치는 영향도를 분석
- □ 보안 통제와 시스템 보안 계획의 적절한 수정
- □ 시스템 보안 상태 보고

성공적인 보안 인증 및 승인 과정의 완료는 기관 임

원에게 정보 시스템의 신뢰성 있는 보안 통제와 시스템이 고려해야 할 인가 과정의 위험기반 결정에 있어서, 정보 시스템의 결함에 대한 적절한 계획 및 예산 해결 방안을 제공한다.

8.2 과정

보안 인증 및 승인 과정은 4단계로 구성되어 있다.

- □ 개시 단계
- □ 보안 인증 단계
- □ 보안 승인 단계
- □ 지속적인 모니터링 단계

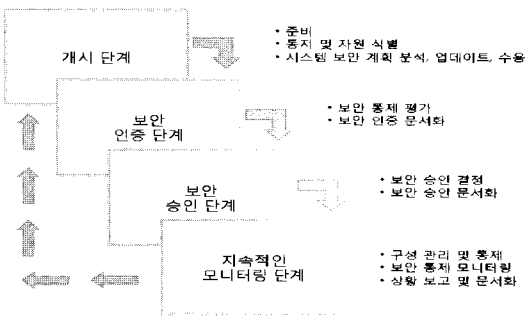
각 단계는 신뢰할 수 있는 인원이 수행하게 될 작업과 보조 작업의 정의가 명확하게 구성되어 있다. 보안 인증 및 승인 활동은 시스템 개발 제품 생명 주기에서 적절한 단계에 있는 정보 시스템에 적용될 수 있다. [그림 10]은 각 단계의 과정에서 관련 작업을 포함한 보안 인증 및 승인 과정에 대한 높은 수준의 관점을 제공한다.

8.2.1 개시 단계

개시 단계는 3가지 작업으로 구성된다.

- □ 준비
- □ 통지와 자원 식별
- □ 시스템 보안 계획 분석, 업데이트, 승인

이 단계의 목적은 인증자가 정보 시스템에서 보안 통제의 평가를 시작하기 전에, 시스템 보안 요구사항 문서



〔그림 10〕 보안 인증 및 승인 과정

를 포함하는 시스템 보안 계획의 내용에 승인 책임자와 상급기관 정보보안 담당관이 동의하고 있다는 것을 보증하는 것이다. 정보 시스템 소유자, 정보 소유자, 정보 시스템 보안 담당자, 인증자, 사용자 대리인 같은 주요 관계자와 함께 승인 책임자 및 정보 보안 담당관의 개시 단계 참여는 보안 인증 및 승인의 성공에 가장 중요하다. 개시 단계 동안에 필요한 정보의 중요한 부분은 정보 시스템 소유자에 의해 사전에 생성되어야 한다.

- □ 개시 위험 평가
- □ 시스템 보안 계획의 개발
- □ 사전 평가 지도(보안 테스트 및 평가, 확인 및 검증, 감사)

새로운 정보 시스템 또는 주요 업그레이드를 수행한 시스템을 위해, 이 정보는 일반적으로 시스템 요구사항이 수립되는 시스템 개발 생명 주기의 개시 단계 동안 생성된다. 일반적으로 레거시 시스템을 위해 시스템 개발 수명 주기의 운영과 유지 단계에서, 이 정보는 가장 최근의 시스템 보안 계획과 위험 평가로부터 얻게 된다. 대부분의 경우, 위험 평가와 시스템 보안 계획은 기관 임원들에 의해 사전 검토 및 승인된다. 보안 인증 및 승인 단계의 개시 단계는 완료된 시스템의 보안 계획과 위험 평가를 확인할 수 있는 검사점(check point)의 역할을 한다. 만약 정보 시스템 소유자가 위험 평가와 시스템 보안 계획을 완료하지 않았다면, 보안 인증 및 승인 과정의 진행 이전에 완료해야 한다.

8.2.2 보안 인증 단계

보안 인증 단계는 2개의 작업으로 구성되어 있다.

- □ 보안 통제 평가
- □ 보안 인증 문서

이 단계의 목적은 정보 시스템의 보안 통제가 정확히 실행되고, 의도대로 운영될 수 있고, 시스템의 보안 요구사항을 충족하도록 요구된 결과를 만들어내는 범위를 결정한다. 이 단계는 보안 통제의 결함을 시정하고 정보 시스템의 알려진 취약성을 감소, 제거하기 위해서 계획된 특정한 행동을 처리한다. 이 단계를 성공적으로 완료하면 승인 책임자은 기관 운영, 기관 자산, 인원의 위험

을 결정하기 위해서 보안 인증으로부터 필요한 정보를 소유한다. 따라서 정보 시스템에 대한 적절한 보안 승인 결정을 판단할 수 있다.

8.2.3 보안 승인 단계

보안 승인 단계는 2개의 작업으로 이루어진다.

- □ 보안 승인 결정
- □ 보안 승인 문서

이 단계의 목적은 정보 시스템에 잘 알려진 취약성이 기관 업무, 기관 자산, 인원에게 위험이 수용 가능한 수준인지를 결정하는 것이다. 이 단계의 성공적 완성에 있어서, 정보 시스템 소유자의 목적은 다음과 같다.

- □ 정보 시스템 운영 인가
- □ 구체적인 기간 및 조건 하에 정보 시스템을 운영하기 위한 잠재적 인가
- □ 정보 시스템 운영 비인가

8.2.4 지속적인 모니터링 단계

지속적인 모니터링 단계는 3개의 작업으로 이루어진다.

- □ 구성 관리와 통제
- □ 보안 통제 모니터링
- □ 상태 보고와 문서화

이 단계의 목적은 시스템 보안 영향력에 변화가 일어날 때, 정보 시스템 보안 통제의 감시 및 모니터링을 제공하고, 공식적인 승인을 알린다. 이 단계의 활동은 정보 시스템 생명 주기를 통해 지속적으로 실행된다. 재승인은 정보 시스템에 구체적인 변화가 요구되거나 연방 기관 정책이 정보 시스템의 주기적인 재승인을 요구할 때 실시된다.

Ⅸ. 보안 통제 모니터링

9.1 정보 통제에 대한 재평가

평가자는 보다 비용-효과적인 평가를 위해서 기존의 보안 통제 평가 정보를 이용해야 한다. 평가의 재이용은 정보 시스템의 이전 승인된 평가에 기반을 두어 정보 보안 통제 유효성을 결정하는 증거로 고려된다. 평가 절차는 정보 보안 통제의 정확한 실행, 의도된 운영, 정보 시스템의 정보 보안 요구사항을 충족하는 결정을 위한 증거를 명시한다. 현재 평가에 이전 평가 결과의 재이용 및 결과 값을 고려할 때, 평가자는 다음을 결정해야 한다.

- □ 증거의 신뢰성
- □ 이전 분석의 타당성
- □ 현재 정보 시스템 운영 환경에 적용 가능성

이는 특정 상황에서, 완벽한 평가 목적을 제출하는 추가적인 평가 활동과 더불어 재이용을 고려하여 사전 평가 결과가 추가로 필요하게 된다.

9.2. 지속적인 모니터링

보안 인증 및 승인 프로세스의 중요한 측면은 정보 시스템에 대한 보안 통제의 지속적인 모니터링을 포함하는 승인 이후이다. 효과적이고 지속적인 모니터링 프로그램은 다음의 내용을 요구한다.

- □ 구성 관리와 구성 통제 프로세스
- □ 정보 시스템의 변경에 대한 보안 영향도 분석
- □ 정보 시스템에서 선택된 보안 통제의 평가와 적절한 기관 임원에게 보안 상태에 대한 보고

지속적인 모니터링의 결과는 규칙적으로 승인 책임자 및 상급기관 정보 보안 담당관에게 문서화되고 보고되어야 한다. 지속적인 모니터링 결과는 시스템 보안 계획 및 정보 보안 구현 계획을 위해 필요한 업데이트에 관하여 고려되어야 한다. 승인 책임자, 상급기관 정보 보안 담당관, 정보 시스템 소유자 및 인증자는 추후 보안 인증 및 승인 활동의 지침으로 이 계획을 사용할 수 있다. 정보 보안 구현 계획은 다음의 내용을 포함한다.

- □ 계획에 나열된 현재 미해결 항목에 있어서 진행을 보고한다.
- □ 보안 영향도 분석 또는 보안 통제 모니터링 동안에 발견된 정보 시스템의 취약성을 처리한다.
- □ 정보 시스템 소유자가 취약성을 처리하는 것에

대한 의도를 설명한다.

정보 시스템에 있어서 보안 통제의 모니터링은 시스템 개발 생명 주기를 통해 지속된다. 재승인은 시스템의 보안에 영향을 주는 정보 시스템에 중요한 변화가 있거나, 연방기관 정책에 따라 지정된 기간이 경과되었을 때 발생한다.

X. 결 론

본 고에서는 미국의 정보보안관리법에 대해서 분석하였다. 정보보안관리법은 연방정부의 운영 및 자산에 대한 정보 보안 통제항목의 효율성을 강화하기 위한 총괄적인 프레임워크 및 통제 방안을 제공한다. 또한 연방정부 및 정보 시스템 보호를 위한 최소 통제 및 유지 방안 개발을 제공하여 정보 보안 대책 추진을 위한 끊임없는 노력을 유지하고 있다.

향후 컴퓨팅 패러다임의 변화와 함께 클라우드 컴퓨팅, 임베디드 시스템, 차세대 네트워크 등의 키워드가 정보 보안 산업과 연계될 것으로 전망된다. 새로운 기술 동향을 고려하여 국내에서도 정부의 정보 보안 대책 향상에 기여하는 연구 개발과 투자 유치, 구조 변화 및 정보 보안 산업의 활성화에 입각한 정책 수립이 심도 있게 연구될 필요가 있다.

참고문헌

[1] NIST, "FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems", 2004.

[2] NIST, "Special Publication 800-60 Volume I Revision 1 : Guide for Mapping Types of Information and Information Systems to Security Categories", 2008.

[3] NIST, "Special Publication 800-60 Volume II Revision 1 : Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories", 2008.

[4] NIST, "FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems", 2006.

[5] NIST, "Special Publication 800-53 Revision 2 : Recommended Security Controls for Federal Information Systems", 2007.

[6] NIST, "Special Publication 800-30 : Risk Management Guide for Information Technology Systems", 2002.

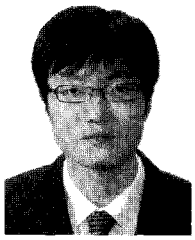
[7] NIST, "Special Publication 800-18 Revision 1 : Guide for Developing Security Plans for federal Information Systems", 2006

[8] NIST, "Special Publication 800-70 : Security Configuration Checklists Program for IT Products - Guidance for Checklists Users and Developers", 2005.

[9] NIST, "Special Publication 800-53A : Guide for Assessing the Security Controls in Federal Information Systems", 2008.

[10] NIST, "Special Publication 800-37 : Guide for the Security Certification and Accreditation of Federal Information Systems", 2004.

〈著者紹介〉

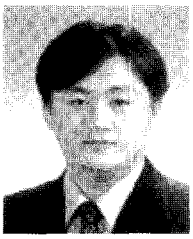


이 동 범 (Dongbum Lee)
학생회원

2008년 2월 : 순천향대학교 정보보호학과 학사 졸업
2010년 2월~2010년 2월 : 순천향대학교 정보보호학과 석사 졸업
2010년 3월~현재 : 순천향대학교 정보보호학과 박사과정
<관심분야> 정보보호, 보안성 평가, 전자여권 보안 등

고 웅 (Woong Go)
학생회원

2008년 2월: 순천향대학교 정보보호학과 학사 졸업
2008년 3월~2010년 2월: 순천향대학교 정보보호학과 석사 졸업
2010년 3월~현재 : 순천향대학교 정보보호학과 박사과정
<관심분야> 정보보호, 보안성 평가, 개인정보보호, 융합보안 등



곽 진 (Jin Kwak)
종신회원

1994~2006년 : 성균관대학교 전자공학과(공학사 공학석사, 공학박사)
2006~2006 : 일본 큐슈대학교 방문연구원
2006~2006 : 일본 큐슈시스템 정보기술연구소 특별연구원
2006~2007 : 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~2009 : 정보통신연구진흥원 집필위원
2009~2009 : 순천향대학교 공과대학 교학부장
현재 : 정보통신산업진흥원 기술평가위원, 디지털아이디관리포럼 기술평가위원, 한국정보통신기술협회 JTC/SC27 분과 기술위원, 한국정보통신기술협회 표준화 로드맵 기술표준기획 전담반 기술위원, 순천향대학교 정보보호학과 학과장, 순천향BIT 창업보육센터 소장, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국인터넷진흥원 미래융합IT서비스 보안연구회 스마트그리드 보안 분과 기술위원, 교육과학기술부 국가기술 수준 평가 전문위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원
<관심분야> 암호프로토콜, RFID 시스템 응용보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안 등