

과정명	
07차시	보안 위험 관리

<1> 위험 관리 계획 수립하기

[1] 위험 관리 계획 수립을 위한 자료 수집

(1) 위험 관리의 정의

1) 정보 보호에서 위험이란?

- '주어진 위협 원천이 특정한 잠재적 취약점(Vulnerability)을 이용할 가능성과 그로 인한 악성 사건이 조직에 미칠 수 있는 영향의 함수이다'라고 정의하고 있음

2) 위험이란?

- 원하지 않는 사건의 발생원이 되는 것이 위협(Threats)이며, 위협이 자산의 특정 속성에 영향을 미침으로서 자산에 대한 손실이 발생한다. 이에 따라 위험은 자산(Assets)과 위협, 취약점의 함수로 정의됨

3) 위험 관리란?

- 조직의 자산에 대한 위험을 감수할 수 있는 수준으로 유지하기 위하여 자산에 대한 위험을 분석하고 이러한 위험으로부터 자산을 보호하기 위해 비용 대비 효과적인 보호 대책을 마련하는 일련의 과정을 말함. 즉, 외부의 위협이 내부의 취약성을 이용하여 보유한 각종 자산에 피해를 입힐 수 있는 잠재적인 가능성이라 할 수 있음

(2) 위험의 구성 요소

1) 자산

- 조직이 보호하여야 할 대상으로서 정보, 하드웨어, 소프트웨어, 시설 등을 말함
- 자산의 유형에 따라 위협과의 관련 인력, 기업 이미지 등의 무형 자산을 포함하기도 함
- 자산의 유형에 따라 위협과의 관계, 즉 취약점이 분류될 수 있으므로 이런 측면에서 자산을 식별하고 분류하여 파악하는 것이 위험을 평가하는데 매우 중요함

2) 위협

- 위협은 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원이나 행위자로 정의됨
- 일반적으로 위협 원천에 따라, 크게 자연재해나 장비 고장 등의 환경적 요인에 의한 것과 인간에 의한 것으로 나눌 수 있고, 인간에 의한 위협은 다시 의도적인 위협과 우연한 위협으로 나눌 수 있음
- 위협에 관련하여 파악해야 할 속성은 발생 가능성으로 연간 발생 횟수 또는 발생 정도로 표현됨. 그러나 위협이 발생했다고 해서 반드시 피해자가 발생하는 것은 아니고 자산이 그 위협에 취약한지 그리고 그 취약점을 보호할 대책이 있는지에 따라 결과는 달라짐

3) 취약성

- 자산의 잠재적 속성으로서 위협의 이용 대상이 되는 것으로 정의되나, 때로 정보 보호 대책의 미비로 정의되기도 함
- 자산에 취약성이 없다면 위협이 발생해도 손실이 나타나지 않는다는 점에서 취약성은 자산과 위협 사이의 관계를 맺어 주는 특성으로 파악할 수 있음
- 자산과 위협 간에 어느 정도의 관계가 있는지, 즉 특정 위협이 발생할 때 특정 자산에 자산의 가치와 관련하여 어느 정도의 피해가 발생할 지를 취약점, 노출정도 또는 효과라는 값으로 나타냄

4) 정보 보호 대책

- 정보보호대책이란 위험에 대응하여 자산을 보호하기 위한 관리적, 물리적, 기술적 대책으로 정의됨

- 보호 대책을 선택할 때는 조직의 환경과 문화에 맞는 것을 선택하는 것이 중요
- 그 비용을 산정할 때는 구축비용뿐만 아니라 운영에 따른 관리비용을 반드시 고려해야 함

(3) 위험 관리의 목적

1) 손실 발생 전 관리의 목적

1. 경제적 목적의 위험 관리

- 가장 최소의 비용이 소요되는 경제적인 위험 관리 방법을 선택하여 위험에 의한 손해 발생에 대처하는 것

2. 불안 감소 목적의 위험 관리

- 위험 관리를 통하여 위험의 존재로 인한 불안을 제거하거나 최소화하는 목적도 존재

3. 의무 규정 충족 목적의 위험 관리

- 기업은 외부 기관에 의한 의무 규정을 충족시켜야 하는데, 위험 관리는 이러한 의무 규정을 충족시키기 위한 목적을 가지고 있음

2) 손실 발생 후 관리의 목적

1. 생존 목적의 위험 관리

- 손실 발생 후 위험 관리의 목적 중 가장 중요한 것으로 손실에도 불구하고 가계나 기업이 존재하도록 하는 것을 의미함

2. 활동 계속 목적의 위험 관리

- 막대한 손해 발생에도 불구하고 활동을 계속할 수 있도록 하는 것으로, 기업의 경우 영업 활동을 지속하도록 관리하는 것을 의미함

3. 안정 수입 목적의 위험 관리

- 기업의 경우 영업 활동이 지속되어야만 수입의 안정도 도모될 수 있다는 것

4. 성장 계속 목적의 위험 관리

- 기업이 계속적으로 성장할 수 있도록 관리하는 것

5. 사회 책임 목적의 위험 관리

- 손해가 발생한 경우 기업은 그 손해가 사회에 끼치는 영향을 최소화할 수 있도록 위험을 관리하는 것

(4) 위험 관리의 과정

1) 위험 분석 범위 선정

- 업무, 조직, 위치, 자산 및 기술적 특성에 따라 관리체제 범위에 근거한 위험 분석 범위를 선정

2) 위험 분석 방법 정의

- 효율적인 위험 분석 수행을 위하여 계량화 여부에 따른 정량적 혹은 정성적 방법을 선택
- 접근 방법에 따라 기준선 접근법, 상세 위험 접근법, 복합적 접근법들을 선택

3) 자산 식별 및 평가

- 조직의 업무와 연관된 정보와 정보시스템을 포함하는 정보 자산을 식별
- 해당 자산의 기밀성, 무결성, 가용성이 상실되었을 때의 결과가 조직에 미칠 수 있는 영향을 고려하여 가치를 평가

4) 위험 분석

- 자산에 대한 위협의 시기별 및 발생 가능성 정도를 인터뷰 또는 실사를 통하여 측정

5) 취약점 분석

- 식별된 위협에 대하여 자산이 어느 정도 취약한가를 인터뷰 또는 실사를 통하여 판명
- 정보와 같이 위협과 취약점의 구분이 어려운 경우 우려 사항으로 구분하여 분석하는 경우도 있음

6) 위험 평가(위험도 산정)

- 식별된 자산, 위협 및 취약점을 기준으로 위험도를 산출하고 기존의 보호대책을 파악한

- 식별된 자산별 위협, 취약점 및 위험도를 정리하여 위험을 평가
- 7) 정보 보호 대책의 선정
- 위험 평가 결과를 토대로 해당 위험도를 수용 가능한 보증의 정도까지 낮추기 위한 보호대책을 선정

[2] 위험 관리 계획 수립

(1) 위험 관리 범위 설정

- 기업의 목표 및 정책, 법적 요구 사항 등을 고려하여 조직, 역할, 책임, 주요 과정을 포함한 위험 관리 전략 및 계획을 수립하고, 기업에 적합한 위험 관리 방법을 선택하여 문서화해야 함

1) 위험 관리 조직, 일정, 방법의 명시

- 조직의 정보 보호 정책에 따라 조직의 목표, 법적 요구 사항 등을 고려하여 위험 관리를 수행할 조직을 지정하고, 관련된 각 조직의 역할과 책임, 기본적인 절차 등을 문서화 해야 함

2) 위험 관리 수행 주기

- 위험 분석·평가는 1~2년 단위로 정기적으로 수행하는 것을 권고하고 있음

3) 위험 관리 방법의 재검토

- 기존의 위험 분석·평가 방법이 현재에도 적절한지를 검토하고 수행

(2) 위험 관리 범위의 중요성

- 정의한 내용에 따라 향후 실시하는 정보 보호 관리 체계 구축에 영향을 끼치게 됨. 정보 자산의 규명 및 위험 관리, 그리고 관리 방안의 적용이나 운영 관리 등 적용 대상의 정보 보호 수준을 유지하는 활동 전반에 영향을 주게 됨

(3) 위험 분석 접근 방법론

1) 위험 평가 전략

1. 기본 통제 접근법

- 베이스라인 접근법은 모든 시스템에 대하여 표준화된 보안 대책의 세트를 체크리스트 형태로 제공
- 체크리스트에 있는 보안 대책이 현재 구현되어 있는지를 판단하여 없는 것을 구현하는 방식을 취함

장점	- 분석의 비용과 시간 절약 용이함
단점	<ul style="list-style-type: none"> - 과보호 또는 부족한 보호가 될 가능성이 있음 - 조직에 적합한 체크리스트가 존재하는 경우가 아니라면 위험 분석을 하지 않는 것과 유사한 상태가 될 수 있음 - 조직의 자산 변동이나 새로운 위협, 취약성의 발생 또는 위험 발생률의 변화 등 보안 환경의 변화를 적절하게 반영하지 못함 - 담당자로 하여금 보안 상태 자체보다 체크리스트를 통해 나타나는 점수에 집착하게 함으로써 보안 요구사항에 따른 우선순위보다는 구현 용이성에 따라 정보보호 대책을 구현하게 되는 경향이 나타날 수 있음

2. 비정형 접근법

- 구조적인 방법론에 기반하지 않고 경험자의 지식을 사용하여 위험 분석을 수행하는 것
- 상세 위험 분석보다 빠르고 비용이 덜 듦
- 특정 위험 분석 모델과 기법을 선정하여 수행하지 않고 수행자의 경험에 따라 중요 위험 중심으로 분석

장점	- 상세 위험분석보다 빠르고 비용이 적게 듦
단점	- 작은 규모의 조직에는 적합할 수 있으나 새롭게 나타나거나 수행자의 경험 분야가 적은 위험 영역을 놓칠 가능성이 있음

	- 논리적이고 검증된 방법론이 아닌 검토자의 개인적 경험에 지나치게 의존하므로 사업 분야 및 보안에 전문성이 높은 인력이 참여하여 수행하지 않으면 실패할 위험이 있음
--	--

3. 상세 위험 분석

- 잘 정립된 모델에 기초하여 자산 분석, 위험 분석, 취약성 분석의 각 단계를 수행하여 위험을 평가하는 것
- 방법론에 따라서는 취약성 분석과 별도로 설치된 정보 보호 대책 분석을 수행하기도 함

장점	- 조직의 자산 및 보안 요구 사항을 구체적으로 분석하여 가장 적절한 대책을 수립할 수 있으며, 자산, 위험, 취약성의 목록이 작성, 검토되었으므로 이후 변경이 발생하였을 때 해당 변경에 관련된 사항만을 추가, 조정, 삭제함으로써 보안 환경의 변화에 적절히 대처할 수 있음
단점	- 분석에 시간과 노력이 많이 소요됨 - 채택한 위험분석 방법론을 잘 이해해야 하므로 비정형 접근법과 마찬가지로 고급의 인적 자원이 필요함

4. 복합 접근법

- 고위험 영역을 식별하여 상세 위험 분석을 수행하고 다른 영역은 베이스라인 접근법을 사용하는 방식

장점	- 비용과 자원을 효과적으로 사용할 수 있으며, 고위험 영역을 빠르게 식별하고 적절하게 처리할 수 있음
단점	- 고위험 영역이 잘못 식별되었을 경우 위험 분석 비용이 낭비되거나, 부적절하게 대응할 수 있음

2) 위험 평가 방법

1. 정량적 접근법

- 정량적 접근법은 손실 및 위험의 크기를 금액으로 나타내고, 위험을 손실액과 같은 숫자로 표현
- 주로 미국에서 사용하고 있는 방식으로 연산 예산 손실액을 계산하기 위하여 관련된 모든 값들을 정량화시켜 표현

장점	-비용·가치 분석이 수행될 수 있음 - 예산 계획에 활용할 수 있으며, 평가된 값이 의미하는 바가 분명하다는 점에서 유용함
단점	- 분석에 필요한 시간이나 노력의 비용이 커짐 - 분석을 통한 값이 실제 자산의 가치를 정확히 반영할 수 없음

2. 정상적 접근법

- 손실 크기를 화폐가치로 측정할 수 없어 위험을 기술 변수로 표현하는 경우 주관적이며, 근거가 제공되지 않지만 시간, 노력, 비용이 적게 듦

장점	- 금액으로 평가하기 어려운 정보의 평가에 용이함 - 분석 시간이 상대적으로 짧고 이해가 쉬움 - 쉽게 위험 분석을 수행가능하며 위험의 우선순위를 파악이 용이함
단점	- 산정된 위험의 객관적 검증이 어려움 - 위험 분석을 수행하는 사람에 따라 결과가 달라질 수 있음(주관적) - 비용 효과적인 분석의 근거를 제공할 수 없음

<2> 위험 분석하기

[1] 정보보호 대상 자산 파악 및 평가

(1) 자산의 파악

- 보유한 중요 자산을 보호하는 것이 목적이기 때문에 자산의 파악과 평가가 필요

- 무엇을 먼저 보호하여야 할지 식별하기 위하여 자산 목록을 작성. 조직의 업무 특성에 따라 정보 자산 분류 기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리
- 정보 자산의 식별은 현재 보유중인 핵심 자산 및 서비스 중 보호해야 할 대상을 정의하는 것
- 새로 도입되는 자산은 개별적으로 식별하여 관리대상에 포함
- 조직 내에 자산 관리 시스템 등과 관체체계에서 요구하는 정보 자산 분류와 차이가 있을 경우 관리체계 구축 및 운영을 위해 추가로 관리가 필요하다. 관리체계 범위 내 주요 단말 운용 현황을 작성

(2) 자산 파악의 대상

- 자산을 파악할 때에 일반적으로 정보 자산과 관련 있는 모든 것을 대상이라고 할 수 있는데, 이에는 전자 정보, 문서, 소프트웨어, 시설, 하드웨어, 지원 설비, 인력 등이 있음
- 단 조직이 진행하고 있는 사업에 따라 중점으로 파악되고 관리되어야 할 자산의 유형은 다소 차이가 있을 수 있음

(3) 자산의 분류 및 등록

- 1) 유형 자산
 - 시스템 자산
 - 인력, 물리적 자산
- 2) 무형 자산
 - 데이터
 - 소프트웨어

(4) 자산 평가

- 향후 위험평가 등에 큰 영향을 미치게 되므로 자산 평가는 매우 신중하게 객관적으로 평가
- 정보 중심의 자산 가치 평가가 이루어져야 하며 자산 소유자뿐만 아니라 관리자, 책임자, 필요시 경영진 참여하에 평가하는 것이 가장 좋음
- 1) 자산 가치 평가 기준
 1. 식별된 자산에 대한 침해 사고가 발생한 경우
 - 기밀성, 무결성, 가용성으로 나눌 수 있음
 2. 비즈니스와 서비스에 영향을 주는 정도를 고려한 경우
 - 장애 복구를 위한 목표 시간, 침해 사고 발생 시 피해 규모, 위험 발생 가능성이 있음

[2] 자산에 대한 위협 식별 및 발생 가능성 평가

(1) 취약점이란?

- 위협이 발생하는 전제 조건으로, 자산이 가지고 있는 보안상의 결점 또는 취약한 속성

1) 취약점의 유형

1. 환경 및 시설
2. 하드웨어
3. 소프트웨어

2) 취약점 점검

1. 관리적 관점
 - 정보 보호 관리 체계 보안 통제에 근거하여 취약점을 점검하는 것
2. 기술적 관점
 - 서버, 네트워크, PC 보안 점검 등을 통하여 취약점을 점검하는 것
3. 물리적 관점

- 문서 검토, 체크리스트, 면담 등을 통하여 취약점을 점검하는 것

[3] 자산에 대하여 위험이 미치는 영향 평가

(1) 수용 가능한 목표 위험 수준의 결정

- 위험의 평가를 통하여 위험의 우선순위가 결정되었으므로 예산 규모나 사용 가능한 자원을 우선순위가 높은 위험부터 대응하는 것도 가능
- 목표 위험 수준보다 낮은 위험은 수용하고 그 이상의 위험에 대해서는 당장 대응하지는 못하더라도 이 목표 수준을 달성하기 위한 장기 계획을 수립하여 대응하는 것
- 목표를 가지고 위험을 관리하게 되면 장기적인 예산 계획을 세우고 어느 정도의 위험을 안고 사업을 진행하고 있으며 언제 목표 위험 수준에 도달할지를 확인할 수 있음. 위험을 완전히 없앨 수는 없으나 어느 정도의 위험이 어떤 분야에서 발생 가능한지를 알고 있는 것은 대단히 중요함

[4] 자산에 대한 위험 발생 시 위험 평가

(1) 위험 평가

- 위험도 및 자산과 관련된 정보에 따라 자산을 그룹화하여 위험 평가를 실시. 위험 평가 시 이전에 실시한 자산 평가, 위험 평가, 취약성 평가 자료와 위험도 산정 기준 매트릭스를 이용 위험 평가는 다음 사항에 의거하여 시행함
- 1) 위험 평가를 위하여 각 업무별로 자산 분류 기준표에 따라 자산을 그룹화
 - 자산 분류에 따른 위험 평가 결과를 쉽게 파악하고 업무와 관련하여 자산들의 위험 수준의 정도를 보여 줌으로써 주요 업무에 대한 보호 대책 수립을 용이하게 함
- 2) 각 자산의 자산 가치 판단 기준을 명시하여 업무 수행 시 중요하게 요구되는 자산의 기능이 무엇인지를 파악할 수 있도록 함
 - 자산의 가치 또한 자산의 주요 기능이 조직에 미치는 영향의 정도로서 평가되어야 함
 - 위험 평가를 통한 자산의 보호 대책 수립 시 이러한 자산의 주요 기능을 보호하는 측면에서 시행되도록 함
- 3) 자산 가치, 위험 수준, 취약성 수준은 이전 태스크에서 평가한 자료를 사용
- 4) 위험도 산정 기준 매트릭스에 의거하여 자산 가치, 위험 수준, 취약성 수준에 따른 위험도를 평가
 - 위험도를 평가한 후에는 평가된 위험도와 위험도 산정 기준이 부합하는지 확인
- 5) 각 자산에 대한 위험도를 평가하고 평가 자산에 대한 위험도가 실제로 어떤 의미를 가지고 있으며 업무 수행에 어떤 위험을 초래할 수 있는지에 대한 평가 의견을 기재하여 담당자가 쉽게 자산에 대한 위험을 인식할 수 있도록 함

<3> 위험 분석 결과 조치하기

[1] 취약점 제거 및 위험 최소화를 위한 통제 방안 도출

(1) 위험 처리 전략

- 각 조직은 자기 조직의 위험에 대한 태도에 따라 서로 다른 처리 전략을 가질 수 있음

(2) 통제 사항 및 대책 선정

1) 통제 사항 선정

- 해당 통제 사항들은 각종의 실제적인 대책을 대부분 포함하고 있음
- 위험의 내용과 규모에 따라서는 제시된 통제 사항의 내용 중에서도 더 세부적이고 강력한 대책이 필요할 경우가 있음
- 통제 사항의 설명에는 구체적으로 제시되지 않은 대책을 강구 하여야 할 경우도 있음
- 선택된 통제 사항은 다른 기존 통제 사항과 함께 계획, 구현, 사후 관리의 관리 과정 요구

사항의 적용을 받아야 함

- 통제 선정 시에는 전략 선정 시 적용된 기술, 재정, 적용되는 법, 제도, 시간, 조직 문화 등 여러 가지 제약 조건이 여전히 고려되어야 함. 선택된 각 통제 사항은 비용·효과 분석을 통하여 정당화되어야 함. 즉, 통제의 구현과 유지에 들어가는 비용이 해당 위험의 감소량보다 적어야 함
- 정성적인 위험 분석을 수 행하였을 경우에는 통제의 비용을 구체적으로 정당화하기가 쉽지 않음

2) 선택된 통제 사항의 대책 선정 절차

- 먼저 각 위험을 경영진이 결정한 수용 가능한 목표 위험 수준과 비교
- 위험도가 목표 위험 수준과 같거나 그 이하인 위험은 수용. 즉, 아무런 조치를 취하지 않음
- 목표 위험 수준보다 위험도가 높은 경우 이 위험을 목표 위험 수준까지 감소시킬 수 있는 대책이 있는지 알아봄. 대책의 구현 및 유지에 들어가는 비용과 감소 되는 위험을 비교하여 구현 비용을 감수할 가치가 있는지를 개략적으로 평가
- 대책 구현 비용이 적절하고 이 대책을 구현함으로써 위험이 목표 위험 수준 이하로 감소될 수 있다고 판단된다면 해당 대책을 선정함으로써 위험을 감소시킴
- 위험을 목표 수준까지 감소시킬 수 있는 대책이 기술적으로 존재하지 않거나 대책이 존재 하더라도 구현 및 유지 비용이 이로 인하여 감소되는 위험의 규모 이상이라고 판단되면 이 위험을 전가할 적절한 대상이 존재하는지 알아봄

[2] 통제 방안 적용 시 소요 비용 간의 비용 편익 분석 수행

(1) 비용 효과 분석

1) 위험 감소

- 위험 감소 전략은 고위험에 대하여 보안 대책을 적용하여 그 수치를 낮추는 방법으로, 크게 기술적인 통제와 관리적인 통제로 나눌 수 있음. 기술적인 통제는 시스템의 암호 정책 적용과 같은, 사용자의 의지와는 관계없이 시스템의 설정을 통하여 강제화 할 수 있는 경우를 말함
- 이와 같은 기술적인 통제는 반드시 지켜질 수밖에 없는 특성이 존재하는데, 이러한 통제를 적용하면 위험이 0으로 감소하는 경향이 있음
- 관리적인 통제는 보안 인식 제고를 통한 보안사고 위험 확률 감소와 정보 보호 관리 체계를 수립, 이행하여 일련의 보안 활동을 통하여 조직이 보안 활동을 함으로써 위험 수치를 낮추는 방법이 있으나 사람이 수행하는 일이기 때문에 반드시 지켜질 수밖에 없는 통제는 사실상 불가능. 그러므로 기술적 통제와는 달리 위험이 다소 감소하지만 0으로 감소하지는 않음

2) 위험 수용

- 위험 수용은 위험이 발생할 경우 손실에 대하여 감수하고 위험을 관리하는 방법
- 자산의 가치보다 훨씬 고비용의 투자를 할 경우 보안 대책 자체가 더 큰 손해
- 보호 대책의 비용이 손실 처리 비용보다 더 큰 경우 위험 수용이라는 전략을 택할 수 있음

3) 위험 회피

- 위험 회피 전략은 위험을 발생시키는 요인인 자체를 제거하여 위험을 피함
- 위험 회피 전략은 핵심 프로세스나 정보 자산이 아닌 경우에만 적용할 수 있는데 여기서 핵심 서비스인 오프라인 서비스를, 여러 가지 보안 위험 요소로 인하여 포기라는 회피 전략을 세우기는 어렵기 때문임

4) 위험 전가

- 위험 전가는 위험 발생 요소를 제3자에게 넘기는 방법
- 이런 경우 사고가 발생 시 비용이 보험사를 통하여 지급되기 때문에 위험 발생에 대한 처리 비용이 낮아짐
- 위험 전가는 전가 비용보다 손실 처리 비용이 더 클 경우 택할 수 있는 전략

[3] 위험 관리 수행 과정 문서화

(1) 문서화 과정

- 정보 보호 관리 체계 수립 및 운영의 근거는 정책, 지침, 절차 등을 수립하고, 문서화하여 관리되어야 함

1) 문서 요건

- 정보 보호 관리 체계와 관련된 문서는 기업의 모든 임직원 및 관련자들이 쉽게 이용할 수 있도록 해당 기업의 규모 및 운영 환경, 기능 등을 고려하여 문서화

2) 문서의 통제

- 작성된 문서는 문서의 발생 타당성 승인, 갱신, 배포, 폐기 등의 통제를 위한 절차를 수립해야 함

3) 문서화

- 정보 보호 관리 체계를 효과적이고 효율적으로 운영하기 위하여 운영 기록을 확인, 유지 보수, 보존, 폐기하는 문서화된 절차를 수립하고 유지·관리