정보자산 위험분석보고서

|  |  |  |  |
| --- | --- | --- | --- |
| **확**  **인** | **담당자** | **보안팀장** | **정보보호최고책임자** |
|  |  |  |

**개정이력**

|  |  |  |  |
| --- | --- | --- | --- |
| **개정번호** | **개정내용** | **담당자** | **시행일자** |
| 1.0 | 정보자산 위험분석보고서 | Team1 | 2015.10.02 |

**목차**

[I. 개요 7](#_Toc364793213)

[1. 목적 7](#_Toc364793214)

[2. 수행내용 7](#_Toc364793215)

[3. 평가기준 7](#_Toc364793216)

[3.1. 자산평가 7](#_Toc364793217)

[3.2. 우려사항 평가 8](#_Toc364793218)

[4. 수행절차 8](#_Toc364793219)

[5. 수행방법 9](#_Toc364793220)

[6. 문서검토 및 인터뷰 내용 9](#_Toc364793221)

[6.1. 문서검토 9](#_Toc364793222)

[6.2. 인터뷰 대상 및 내용 10](#_Toc364793223)

[7. 세부 수행 일정 12](#_Toc364793224)

[7.1. 수행 일정 12](#_Toc364793225)

[II. 위험분석 방법론 13](#_Toc364793226)

[1. 위험분석 방법 정의 13](#_Toc364793227)

[1.1. 접근방식에 따른 위험분석 방법 13](#_Toc364793228)

[1.2. 계량화 여부에 따른 위험분석 방법 14](#_Toc364793229)

[1.3. 위험분석 방법 선정 15](#_Toc364793230)

[III. 위험분석 결과 16](#_Toc364793231)

[1. 위험분석 절차 16](#_Toc364793232)

[2. 정보자산 분석 16](#_Toc364793233)

[2.1. 자산분석 개요 16](#_Toc364793234)

[2.2. 자산 식별 17](#_Toc364793235)

[2.3. 정보자산 그룹화 18](#_Toc364793236)

[2.4. 자산가치(중요도) 평가 20](#_Toc364793237)

[2.5. 자산평가 결과 22](#_Toc364793238)

[3. 우려사항 평가 24](#_Toc364793239)

[3.1. 우려사항 식별 25](#_Toc364793240)

[3.2. 발생가능성 평가 37](#_Toc364793241)

[3.3. 영향도 평가 38](#_Toc364793242)

[3.4. 법률준거성 평가 39](#_Toc364793243)

[3.5. 우려사항 평가 결과 39](#_Toc364793244)

[4. 위험분석 40](#_Toc364793245)

[4.1. 위험분석 개요 40](#_Toc364793246)

[4.2. 위험분석 방법 41](#_Toc364793247)

[4.3. 위험 수용 기준 설정 41](#_Toc364793248)

[4.4. 위험분석 결과 42](#_Toc364793249)

[IV. 보호대책 수립 45](#_Toc364793250)

[1. 보호대책 수립 전략 45](#_Toc364793251)

[2. 보호대책 선정 45](#_Toc364793252)

[3. 위험대응 전략 45](#_Toc364793253)

[4. 위험처리 계획 46](#_Toc364793254)

[V. 별첨 49](#_Toc364793255)

[1. 인터뷰 담당자 목록 49](#_Toc364793256)

[2. 위험분석 상세내역 50](#_Toc364793257)

**표목차**

[[표 3‑1] 자산중요도 테이블 8](#_Toc364793258)

[[표 3‑2] 우려사항 평가값 테이블(Concern Value Table) 8](#_Toc364793259)

[[표 4‑1] 위험분석 수행절차 8](#_Toc364793260)

[[표 5‑1] 위험분석 수행방법 9](#_Toc364793261)

[[표 7‑1] 위험분석 수행일정 12](#_Toc364793262)

[[표 1‑1] 접근방식에 따른 위험분석 방법 13](#_Toc364793263)

[[표 2‑1] 자산유형 및 식별방법 18](#_Toc364793264)

[[표 2‑2] 정보자산 그룹화 19](#_Toc364793265)

[[표 2‑3] 기밀성 평가기준 21](#_Toc364793266)

[[표 2‑4] 무결성 평가기준 21](#_Toc364793267)

[[표 2‑5] 가용성 평가기준 21](#_Toc364793268)

[[표 2‑6] 자산평가결과 22](#_Toc364793269)

[[표 2‑7] 자산그룹 분포 23](#_Toc364793270)

[[표 2‑8] 자산가치(중요도) 분포 24](#_Toc364793271)

[[표 3‑1] 관리적 우려사항 25](#_Toc364793272)

[[표 3‑2] 물리적 우려사항 26](#_Toc364793273)

[[표 3‑3] 기술적 우려사항 26](#_Toc364793274)

[[표 3‑4] 법적 우려사항 37](#_Toc364793275)

[[표 3‑5] 발생가능성 평가기준 38](#_Toc364793276)

[[표 3‑6] 영향도 평가기준 38](#_Toc364793277)

[[표 3‑7] 우려사항 평가값(Concern Value) 분포 39](#_Toc364793278)

[[표 4‑1] 위험분석 모델과 방법론 41](#_Toc364793279)

[[표 4‑2] 위험 등급 기준 41](#_Toc364793280)

[[표 4‑3] 위험도 분포 42](#_Toc364793281)

[[표 4‑4] 자산범주별 위험도 분포 43](#_Toc364793282)

[[표 4‑1] 위험처리계획 46](#_Toc364793283)

**그림목차**

[[그림 2‑1] 자산그룹 분포 23](#_Toc364793284)

[[그림 2‑2] 자산가치(중요도) 분포 24](#_Toc364793285)

[[그림 3‑1] 우려사항평가 분포 40](#_Toc364793286)

[[그림 4‑1] 위험도 분포 43](#_Toc364793287)

[[그림 4‑2] 자산범주별 위험도 분포 44](#_Toc364793288)

# 개요

## 목적

본 위험분석은 소프트웨어특성화대학원 과제관리시스템 내의 A, B, C 서비스에 대한 유·무형 자산에 대해 정보보호 현황, 요구사항, 가치 등을 분명하게 파악하고 이미 존재하고 있거나 발생 가능한 위협과 취약점에 대한 우려사항을 도출하여 효과적인 정보보호대책을 수립하는데 기반이 되게 하기 위함이다.

정보보호관리를 수행하는 가장 큰 목적은 조직 내 자산을 보호하기 위함이다. 정보보호관리의 일반적인 모델은 우선적으로 보안정책에 대한 현황을 파악한 후에 보안정책을 근거로 하여 위험 분석을 실시함으로써 조직이 보호해야 할 자산, 위협 및 취약점과 그로 인해 발생할 수 있는 피해 발생가능성, 피해 영향도 등을 식별하고 이에 대한 대응책을 제시한다.

## 수행내용

* 기간 : 2015.09.20 ~ 2015.12.13
* 내용 : 소프트웨어특성화대학원 과제관리시스템의 주요 정보에 대한 위험분석 및 보호대책 수립
* 진단방법 : 개팀 인터뷰 및 문서 검토, 증적자료 검토, 현장 실사

## 평가기준

자산에 대한 중요도를 평가하고 소프트웨어특성화대학원 과제관리시스템의 성격에 따라 취약점에 따른 위협의 발생 가능성과 영향도를 통합적으로 나타낼 수 있는 위험 시나리오를 분석하여 우려사항을 도출하고 우려사항에 대한 발생가능성과 영향도를 평가하여 우려사항 평가값(Concern Value)를 도출한다.

자산에 중요도와 우려사항을 평가하여 위험도를 구하는 평가방식은 아래와 같다.

* 위험도 = 자산 중요도 + 우려사항 평가값(Concern Value)

### 자산평가

자산평가는 C(기밀성), I(무결성), A(가용성)에 대한 각 3점 척도로 평가를 하고 각각의 평가점수를 합산하여 점수를 구한다. 합산 점수에 따라서 자산의 중요도를 1~5점으로 구분하여 평가한다.

[표 ‑] 자산중요도 테이블

| **자산평가** | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **자산평가합계** | 9 | 8 | 7 | 6 | 5 | 4 | 3 | |
| **자산중요도** | 5 | 4 | 3 | | 2 | | | 1 |

### 우려사항 평가

자산에 대해서 위험 시나리오를 분석하여 우려사항을 도출하고 이에 대한 발생가능성과 영향도에 가중치 3배한 값과 법률준거성을 합산하여 우려사항 평가값(Concern Value)을 산정한다.

[표 ‑] 우려사항 평가값 테이블(Concern Value Table)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **발생가능성** | | **법률**  **준거성** | **영향도** | | | | |
| **VH**  **(Very High)** | **H**  **(High)** | **M**  **(Medium)** | **L**  **(Low)** | **VL**  **(Very Low)** |
| **5** | **4** | **3** | **2** | **1** |
| **VH**  **(Very High)** | **5** | **0/3** | 20/23 | 17/20 | 14/17 | 11/14 | 8/11 |
| **H**  **(High)** | **4** | **0/3** | 19/22 | 16/19 | 13/16 | 10/13 | 7/10 |
| **M**  **(Medium)** | **3** | **0/3** | 18/21 | 15/18 | 12/15 | 9/12 | 6/9 |
| **L**  **(Low)** | **2** | **0/3** | 17/20 | 14/17 | 11/14 | 8/11 | 5/8 |
| **VL**  **(Very Low)** | **1** | **0/3** | 16/19 | 13/16 | 10/13 | 7/10 | 4/7 |

## 수행절차

위험분석은 다음과 같은 절차에 의해서 진행된다.

[표 ‑] 위험분석 수행절차

| **단계** | **내용** |
| --- | --- |
| 대상선정 | * 업무, 조직, 위치, 자산 및 기술적 특성에 따른 ISMS 범위에 근거한 위험분석 범위 선정 |
| 현황분석 | * 정보보호관리체계인 KISA ISMS 통제항목 현황검토 * 정보보호관리체계 구현 수준을 위한 담당자 인터뷰 및 현황 분석 * 개인정보보호법, 정보통신망법 등 관련 법률준수에 대한 현황 분석 |
| 자산분석 | * 정보자산 현황 및 사용 용도 파악 * 담당자 자산평가 시트 작성 * 담당자 자산평가 작성결과 검토 |
| 위협·취약점분석  (우려사항 분석) | * 정보자산에 존재하는 위협과 취약점(우려사항) 검토 * 소프트웨어특성화대학원 과제관리시스템 건물 및 IDC의 물리적 시설 검토 * 기존 정보보호 정책에 대한 물리적 관리적 위협 및 취약점 검토 |
| 위험분석 | * 관리적, 물리적, 기술적, 법적 위험분석 |
| 보고서 작성 | * 정보자산 보호 위험분석 보고서 작성 |
| 보호대책 도출 | * 위험처리계획에 따른 보호대책 수립 |

## 수행방법

[표 ‑] 위험분석 수행방법

|  |  |
| --- | --- |
| **단계** | **내용** |
| 인터뷰 | * 보안관련 문서의 규정 및 지침사항과 현재 운영중인 보안관리 상의 현황 및 문제점을 파악하기 위한 인터뷰 실시 |
| 문서검토 | * 관련 문서를 검토하여 및 KISA ISMS의 통제내용 반영여부 확인 * 최근 기술적 취약점 진단결과 검토 |
| 현장실사 | * 문서검토와 인터뷰 과정에서 파악된 사실에 대해 통제사항 및 이행상태를 실제 방문 및 확인을 통해 검증 * 소프트웨어특성화대학원 과제관리시스템의 주요시설(전산센터, 방재실 등)에 대한 물리적 보안현황 검토 |

## 문서검토 및 인터뷰 내용

### 문서검토

| **구분** | | **문서명** | **비고** |
| --- | --- | --- | --- |
| **규정** | | 정보보안관리규정 | 규정 |
| **정보보호**  **관리체계** | **보안정책** | INT\_P00\_정보보호 및 IT보안정책서 | 1종 |
| **보안지침** | INT\_P02\_정보보호정책관리지침  INT\_P03\_아웃소싱보안관리지침  INT\_P04\_자산분류 및 위험관리지침  INT\_P05\_인력보안지침  INT\_P06\_물리적보안지침  INT\_P07\_개발 및 배포 보안관리지침  INT\_P08\_시스템 운영관리지침  INT\_P09\_암호관리지침  INT\_P10\_접근통제지침  INT\_P11\_전산운영 관리지침  INT\_P12\_문서관리지침  INT\_P13\_보안사고대응지침  INT\_P14\_법률준수에 관한 지침  INT\_P15\_보안감사지침  INT\_P16\_사업연속성 관리지침  INT\_P17\_개인PC보안관리지침  INT\_P18\_네트워크정보보호지침  INT\_P19\_데이터베이스정보보호지침  INT\_P20\_개인정보보호지침  INT\_P21\_영상정보처리보호지침 | 20종 |

### 인터뷰 대상 및 내용

| **날짜** | **담당부서** | **담당자** | **내용** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 세부 수행 일정

### 수행 일정

[표 ‑] 위험분석 수행일정

| **세부수행내역** | **내역** | **일정** | **비고** |
| --- | --- | --- | --- |
| 대상 및 일정 협의 | 진단 대상과 일정 상세 협의 | O/O~O/O |  |
| 현황분석 | 관리체계 현황분석, 인터뷰자료 작성 | O/O~O/O |  |
| 자산분석 | 자산조사 및 자산평가 | O/O~O/O |  |
| 위협·취약점(우려사항) 분석 | 위협, 취약점(우려사항) 분석  : 기술부문/관리부문(인터뷰) | O/O~O/O |  |
| 위험분석 | 위험분석 | O/O~O/O |  |
| 보고서 | 위험분석 보고서 작성 | O/O~O/O |  |

# 위험분석 방법론

## 위험분석 방법 정의

위험분석 및 평가 방법론은 과학적이고 정형적(structured)인 과정으로 위험을 알아내고 측정하려는 노력을 정리한 것이며, 방법론 자체는 전 세계적으로 수백 여 가지가 존재한다. 실제로 분석 및 평가를 수행하고자 할 경우, 대상 조직 및 특징, 요구사항, 수행 기간 등에 따라 다양한 방법론이 활용될 수 있으며, 앞의 여러 상황 및 환경을 고려하여 가장 적절한 방법을 선택하는 것이 중요하다.

* 접근방식에 따른 위험분석
* 정량적 접근법(Quantitative Approach)
* 정성적 접근법(Descriptive Approach)
* 계량화 여부에 다른 위험분석
* 기준선 접근법(Baseline Approach)
* 전문가적 접근법(Risk Analysis Approach)
* Informal Approach
* Detailed Approach
* Combined Approach

### 접근방식에 따른 위험분석 방법

위험분석 및 평가 방법은 접근방식에 따라 다음과 같이 크게 정량적인 기법과 정성적인 기법으로 나눌 수 있다.

[표 ‑] 접근방식에 따른 위험분석 방법

| **구분** | **정량적 기법** | **정성적 기법** |
| --- | --- | --- |
| 특징 | 손실 크기를 화폐 단위로 측정이 가능할 때 사용함  과거자료 접근법, 수학공식 접근법, 확률분포 추정법 | 손실 크기를 측정할 수 없어서 위험을 구간 및 기술변수(예: H:3, M:2, L:1)로 표현함  분석자의 경험 및 지식에 기초한 위험분석 방법  델파이법, 시나리오법, 순위결정법 |
| 장점 | 정량화된 자료의 사용으로 비용-효과 분석 및 예산 계획이 용이함  수리적 방법의 사용으로 계산이 논리적임  보다 객관적인 정보를 얻음 | 정량화하기 어려운 정보의 평가에 용이함  용어의 이해가 쉬움  분석의 소요시간 짧음 |
| 단점 | 정확한 정량화 수치를 구하기가 어려움  수리 계산에 많은 시간과 노력이 필요함 | 주관적 판단의 남용 여지가 있음  비용-효과 분석이 어려움 |

### 계량화 여부에 따른 위험분석 방법

위험분석 및 평가 대상 조직의 보안요구사항, 가용자원(전문인력, 기간, 예산 등), 규모 등을 고려하여 적절한 접근방식을 선택하는 것이 필요하다. 일반적으로 기준선 접근법(Baseline Approach), 전문가 판단법(Informal Approach), 상세위험 접근법(Detailed Risk Approach), 복합적 접근법(Combined Approach) 우려사항 접근법(Concern Approach)중 선택적으로 적용한다.

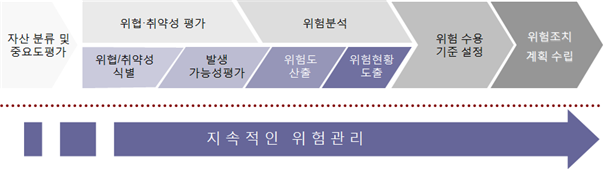
| **구분** | **특징** |
| --- | --- |
| 기준선접근법 | 모든 시스템에 대하여 보호의 기본수준을 정하고 이를 달성하기 위하여 일련의 보호대책을 선택  시간과 비용이 많이 들지 않고 모든 조직에서 기본적으로 필요한 보호대책 선택 가능  조직의 특성을 고려하지 않았기 때문에, 조직 내에 부서별로 적정 보안 수준보다도 높게 혹은 낮게 보안통제 적용 |
| 전문가판단법 | 정형화된 방법을 사용하지 않고 전문가의 지식과 경험에 따라서 위험을 분석  작은 조직에서 비용 효과적  구조화된 접근 방법이 없기 때문에, 위험을 제대로 평가하기 어렵고 보호대책의 선택 및 소요비용을 합리적으로 도출하기 어려우며 계속적으로 반복되는 보안관리의 보안감사 및 사후관리가 제한 |
| 상세위험접근법 | 자산의 가치를 측정하고 자산에 대한 위협의 정도와 취약점을 분석하여 위험의 정도를 결정  조직 내에 적절한 보안수준 마련 가능  전문적인 지식과 시간과 노력이 많이 소요 |
| 복합적접근법 | 먼저 조직활동에 필수적인 높은 위험의 시스템을 식별하고 이러한 시스템에 대해서는 ‘상세위험 접근법’을, 그렇지 않은 시스템에는 ‘기준선 접근법’ 등 다른 방법을 사용  보안전략을 빠르게 구축할 수 있고, 상대적으로 시간과 노력을 효율적으로 활용 가능  두 가지 방법의 적용대상을 명확하게 설정하지 못함으로써 자원의 낭비 발생 가능 |
| 우려사항접근법 | 조직의 성격에 따라 위협과 취약점을 구분하지 않고 하나로 나타내어 위험도를 도출할 수 있는데 이를 ‘우려사항’이라고 정의하고 우려되는 정도를 나타내는 우려도(Concern Value) 값을 평가  자산의 가치가 낮으면 대책이 없음에도 ‘취약점이 낮다’고 평가를 하거나 자산의 가치가 높으면 대책이 존재함에도 ‘취약점이 높다’라고 평가하는 오류를 제거하는 데 효과적  파악된 취약점을 이용할 위협을 분석하여 우려사항을 도출하고 각 자산에 대하여 이 우려사항을 평가하는 방식 |

### 위험분석 방법 선정

위에서 언급한 위험분석 방법의 정의와 접근방식에 따른 위험분석 방법 및 계량화 위험분석 방법 등을 고려하여 위험분석 방법으로 ‘우려사항 접근법(Concern Approach)’을 적용하였다. 우려사항 접근법은 자산의 가치를 측정하고 자산에 대한 위협의 정도와 취약점을 통합적으로 파악한 우려사항(Concern)에 대한 분석을 통하여 위험도를 결정한다.

# 위험분석 결과

## 위험분석 절차

정보보호 측면의 위험분석 절차는 자산분석, 위협·취약점 분석, 위험분석, 위험 수용기준 설정, 위험조치의 보호대책 수립 절차로 진행되며, 다음의 그림과 같다.

자산분석은 소프트웨어특성화대학원 과제관리시스템 정보자산 상세 현황을 파악하여 그룹화하고, 그룹화된 정보자산그룹을 기밀성, 무결성, 가용성 측면에서 가치를 평가한다. 위험분석은 소프트웨어특성화대학원 과제관리시스템의 정보자산에서 발생될 수 있는 다양한 위협과 위협이 미치는 영향도를 통합한 우려사항를 작성하여 각 우려사항에 대하여 발생가능성과 영향도를 평가한다. 취약점분석은 정보보호 관리체계 보안점검 결과 및 기존 시스템 취약점 점검 결과를 참조하여 분석한다. 정보자산의 가치, 위협도, 취약점에 대한 우려사항 수준을 고려하여 위험도를 분석하고, 위험에 대한 보호대책을 수립하는 단계로 진행한다. 상세 수행 방법 및 결과는 각 단계별로 기술한다.

## 정보자산 분석

정보자산들이 전자적인 침해행위를 받아 연속적인 업무수행을 할 수 없는 상황이 된다면 소프트웨어특성화대학원 과제관리시스템 업무의 피해 뿐만 아니라 관련 소프트웨어특성화대학원 과제관리시스템 자산 및 관련 업체들에게 피해가 확대되고 규모도 증가하게 된다. 따라서 소프트웨어특성화대학원 과제관리시스템의 주요 정보자산들을 파악하고 각각의 업무를 수행하는데 어느 정도의 가치를 내포하고 있는지를 파악한다.

### 자산분석 개요

자산분석은 소프트웨어특성화대학원 과제관리시스템 내에 존재하는 정보자산을 식별하여 그룹화하고, 해당 정보자산그룹이 가지고 있는 중요도를 산정하여 가치를 평가하는 작업이며, 이러한 정보자산 분석을 바탕으로 위협 및 취약점에 대해서 통합적인 우려사항의 분석을 수행하며, 추후 보호대책 수립의 기초 자료로 활용된다.

정보자산 분석은 다음과 같이 3단계로 수행된다.

* 1단계: 자산 식별
* 2단계: 자산 그룹화
* 3단계: 자산 가치(중요도) 평가

자산 식별 단계에서는 위험분석 및 평가의 범위 내 정보자산의 효과적인 분류가 가능하도록 범주를 설정하여 해당 범주 내에 포함되는 모든 자산에 대한 목록을 확보하여 자산을 식별한다. 자산 그룹화 단계에서는 식별된 자산목록 상에서 자산의 유사한 특성을 고려하여 그룹화 하였다. 자산 가치 평가 단계에서는 그룹화된 자산에 대하여 해당 자산의 소유자 혹은 주관부서에 의해 기밀성, 무결성, 가용성 측면에서 자산의 가치를 평가하는 작업을 수행한다.

### 자산 식별

위험분석 및 평가의 수행 대상인 자산은 기본적으로 정보, 정보시스템, 정보시스템 관련 자산의 범주로 파악될 수 있다.

정보는 주로 업무상 이용하게 되는 응용프로그램 상에 존재하는 데이터와 파일서버 혹은 PC 등에 파일 형태로 존재하는 전자문서, 그리고 하드카피 형태로 별도 보관이 필요한 종이문서의 유형이 있을 수 있다.

정보시스템은 업무 처리를 위한 서버, 네트워크, PC 등의 장비인 H/W와 해당 H/W 상에 설치된 OS, DBMS, 상용 소프트웨어, 별도 개발된 응용프로그램 등의 S/W 유형으로 파악 가능하다. 정보시스템 관련 자산은 정보시스템이 위치한 전산실 혹은 사무실 등의 물리적 공간과 여기에 설치된 각종 설비, 그리고 이러한 정보시스템을 운영 및 개발하기 위해 필요한 인적자원을 포함한다. 일정한 형태를 가지고 있지 않은 정보는 그 속성상 여러 부서별로 산재되어 있고 일원화되어 관리되기 힘들어 직접적인 파악이 불가능한 성격을 갖는다. 따라서, 데이터, 전자문서, 종이문서 파악을 위해 해당 정보 자산의 소유부서 혹은 주관부서를 통하여 자산 식별을 수행하였다.

정보시스템 관련 자산 중 인적자원, 물리적 공간으로 구분할 수 있으며 이를 별도로 분류하고 위험분석이 수행될 수 있도록 자산을 분류하였다.

결론적으로, 자산 범위 내에 포함되는 개별 자산 유형에 대한 식별은 아래와 같이 이루어졌다.

[표 ‑] 자산유형 및 식별방법

|  |  |
| --- | --- |
| **자산유형** | **자산식별방법** |
| Information | 문서파일, 데이터파일, 데이터베이스 내의 데이터 등 |
|
|
| Service | 건물, 사무실, 데이터센터 등 물리적 시설 전력공급, 환기시설, 방재시설 등 정보시스템 운영을 지원하기 위한 시설 |
|
| Documents | 종이로된 정보로 보고서, 계약서, 매뉴얼, 각종대장 등 |
|
| Software | 패키지 소프트웨어, 시스템 소프트웨어, 응용 프로그램 등 |
|
| Physical | 서버(공용 자원을 갖고 여러 사용자에게 서비스를 제공하는 컴퓨터 시스템),  네트워크 장비(네트워크 장비, 통신 회선 등),  정보보호시스템(해당 부서 내 정보자산의 분류 및 식별),  개인용 사무기기(PC, 노트북, 스마트폰 등) 등 |
| People | 소유자, 관리자, 사용자, 운영자, 개발자 등 정보시스템 관리 인력 |
|

### 정보자산 그룹화

다양한 유형의 여러 자산들을 모두 개별적으로 가치 평가를 하거나 위험 분석을 수행하는 것은 상당히 비효율적이고 추후 위험 분석 결과에 대한 신빙성에 혼란을 야기시키는 원인이 된다. 따라서 보다 효율적인 자산 가치 평가 및 위험 분석 수행을 위해 다음 사항을 고려하여 자산을 그룹화 하였다.

* 동일하거나 유사한 서비스를 위한 자산
* 중요도, 위치, 소유자가 동일하여 위협 및 취약점에 따른 위험이 동일한 경우
* 동일한 부서에 의해 관리되고 있는 경우

다음은 이러한 기준에 따라 각 유형의 자산을 그룹화한 결과이다.

[표 ‑] 정보자산 그룹화

|  |  |  |
| --- | --- | --- |
| **자산유형** | **코드** | **자산** |
| Information | A01 | 문서관리서버 |
| A02 | 그룹웨어 |
| A03 | 업무지원 |
| Service | A01 | 사내 |
| A02 | 사외 |
| Documents | A01 | 정보보안규정 |
| A02 | 시스템운영 및 관리 |
| Software | A01 | 시스템소프트웨어 |
| A02 | 사내소프트웨어 |
| Physical | A01 | 게임공통 |
| A02 | 공통 |
| A03 | 웹게임군 |
| A04 | 퍼블리싱 |
| A05 | 보안장비 |
| A06 | 네트워크 |
| A07 | 전사 |
| A08 | 업무용장비 |
| A09 | 매체 |
| People | A01 | 서비스 운영 및 관리 |
| A02 | 아웃소싱 |

### 자산가치(중요도) 평가

1. C, I, A 평가

파악된 자산 가치는 기밀성(Confidentiality) 측면에서 시스템에서 저장/처리/제공되는 정보가 유출되었을 경우 조직 및 사업에 미치는 영향을 평가하고, 무결성(Integrity) 측면에서 시스템에서 저장/처리/제공되는 정보가 무단 변조되는 경우 조직 및 사업에 미치는 영향을 평가하고, 가용성(Availibility) 측면에서 시스템이 장애 및 침해사고 등으로 인해 일정 시간 가동이 중단될 경우 조직 및 사업에 미치는 영향을 평가한다. C, I, A 평가는 영향 정도에 따라 1~3점을 부여하며, 평가 기준은 다음과 같다.

1. 기밀성평가 기준

[표 ‑] 기밀성 평가기준

| **등급** | **등급내용** | **설 명** |
| --- | --- | --- |
| **High** | 3 | 조직 내부에서도 특별히 허가를 받은 사람들만이 볼 수 있어야 하며, 조직 외부에 공개되는 경우 개인 프라이버시나 조직의 사업 진행에 치명적인 피해를 줄 수 있는 수준 |
| **Medium** | 2 | 조직 내부에서는 공개될 수 있으나 조직 외부에 공개되는 경우 개인 프라이버시나 조직의 사업 진행에 상당한 문제를 발생시킬 수 있는 수준 |
| **Low** | 1 | 조직 외부에 공개되는 경우 개인 프라이버시나 조직의 사업 진행에 미치는 영향이 미미한 수준 |

1. 무결성 평가기준

[표 ‑] 무결성 평가기준

| **등급** | **등급내용** | **설 명** |
| --- | --- | --- |
| **High** | 3 | 정보가 변경되거나 손상되는 경우 업무에 상당한 영향을 끼침 |
| **Medium** | 2 | 정보가 변경되거나 손상되는 경우 업무에 영향을 끼침 |
| **Low** | 1 | 정보가 변경되거나 손상되는 경우 업무에 주는 영향이 미미함 |

1. 가용성 평가기준

[표 ‑] 가용성 평가기준

| **등급** | **등급내용** | **설 명** |
| --- | --- | --- |
| **High** | 3 | 매일 95% 이상의 가동을 필요로 하는 시스템 및 네트워크와 기타 정보로 중단되는 경우 조직의 운영과 사업 진행에 치명적인 피해를 줄 수 있는 수준 |
| **Medium** | 2 | 표준 가동(업무)시간 동안 가동을 필요로 하는 시스템 및 네트워크와 기타 정보로 중단되는 경우 조직의 운영과 사업 진행에 상당한 문제를 발생시킬 수 있는 수준 |
| **Low** | 1 | 표준 가동(업무)시간에 비례하여 50%이상의 가동을 필요로 하는 시스템 및 네트워크와 기타 정보로 중단되는 경우 조직의 운영과 사업 진행에 미치는 영향이 미미한 수준 |

1. 자산의 가치(중요도) 평가

자산의 가치평가는 자산 그룹별 기밀성, 무결성, 가용성의 합계 값을 기준으로 평가한다. 자산의 가치(중요도)는 자산 그룹별 C(기밀성), I(무결성), A(가용성)의 합산 점수에 따라 1점에서 5점으로 평가한다.

|  |
| --- |
| **자산가치(중요도) = 기밀성 + 무결성 + 가용성 => 1점~5점** |

자산의 가치평가는 자산 그룹별 기밀성, 무결성, 가용성의 합계 값을 기준으로 평가한다.

[표 ‑] 자산평가결과

|  |  |  |
| --- | --- | --- |
| **자산평가합계**  **(C+I+A)** | **자산가치**  **(중요도)** | **설명** |
| 9점 | 5 | 해당 자산이 피해를 입으면 매우 심각한 손실이나 해당 업무가 어려워질 수도 있음 |
| 8점 | 4 | 해당 자산이 피해를 입으면 심각한 손실이나 해당 업무에 부정적인 영향을 미침 |
| 7점 ∼ 6점 | 3 | 해당 자산이 피해를 입으면 업무적, 재무적으로 손실이 발생되기 시작 함 |
| 5점 ∼ 4점 | 2 | 해당 자산이 피해를 입으면 해당 영역 또는 해당 서비스에 작은 영향 발생 |
| 3점 | 1 | 해당 자산에 피해가 발생해도 업무적, 재무적으로 거의 영향이 없음 |

### 자산평가 결과

#### 자산그룹의 분포현황

자산은 6개의 대분류, 15개의 중분류, 85개의 소분류, 476개의 자산그룹으로 분류할 수 있다. 그중 Physical 자산 57.4%, Information 자산26.1%로 소프트웨어특성화대학원 과제관리시스템 자산의 대부분을 차지한다.

[표 ‑] 자산그룹 분포

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **대분류** | **중분류** | **소분류** | **자산그룹** | **비율** |
| Information | 2 | 34 | 124 | 26.1% |
| Service | 1 | 1 | 1 | 0.2% |
| Documents | 1 | 7 | 18 | 3.8% |
| Software | 1 | 8 | 14 | 2.9% |
| Physical | 8 | 19 | 273 | 57.4% |
| People | 2 | 16 | 46 | 9.7% |
| **합계** | 15 | 85 | 476 | 100.0% |

[그림 ‑] 자산그룹 분포

#### 자산가치(중요도)의 분포현황

소프트웨어특성화대학원 과제관리시스템의 자산은 대그룹 6개 항목에 1점~5점으로 다양하게 분포하고 있다. 특히 가장 중요한 4∼5점 자산은 21.8%의 비율을 차지하고 있다.

[표 ‑] 자산가치(중요도) 분포

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **자산가치 (중요도)** | **Information** | **Service** | **Documents** | **Software** | **Physical** | **People** | **비율** |
| 5 | 8 | 1 | 1 | 4 | 11 | 46 | 14.9% |
| 4 | 28 | 0 | 0 | 0 | 5 | 0 | 6.9% |
| 3 | 51 | 0 | 2 | 6 | 24 | 0 | 17.4% |
| 2 | 34 | 0 | 12 | 1 | 232 | 0 | 58.6% |
| 1 | 3 | 0 | 3 | 3 | 1 | 0 | 2.1% |
| 합계 | 124 | 1 | 18 | 14 | 273 | 46 | 100.0% |

[그림 ‑] 자산가치(중요도) 분포

## 우려사항 평가

자산에 대해서 위험이 발생하게 되는 취약점에 대해서 위험 시나리오를 분석하여 우려사항이 발생할 수 있는 가능성과 그 발생으로부터 소프트웨어특성화대학원 과제관리시스템에 피해가 발생되는 영향도를 고려하여 평가한다.

### 우려사항 식별

조직 내에 존재하는 취약점을 적절히 식별하기 위하여 관리 및 운영 전반의 포괄적인 부분에 해당하는 관리적, 물리적 평가기준을 반영하였으며, 자산에 대한 기술적 취약점을 같이 고려하였다. 관리적, 물리적 평가기준은 아래 관리적 우려사항, 물리적 우려사항에서, 기술적 평가기준은 기술적 우려사항에서 확인할 수 있다.

[표 ‑] 관리적 우려사항

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 정보보호정책 | TMMGT-001 | 정보보호정책의 준수가 미흡하여 정보보안 사고가 발생할 수 있다. |

[표 ‑] 물리적 우려사항

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 물리적보안 | TMPHY-001 | 장비의 배치가 계획적으로 이루어지지 않아 허가되지 않은 자의 접근으로 인한 실수나 의도적인 고장, 허가되지 않은 사용, 도난이 발생할 수 있고 환기 문제, 소규모 화재나 누수의 영향이 발생할 수 있다. |

[표 ‑] 기술적 우려사항

* 서버(리눅스)

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 계정관리설정 | TMSSL-001 | root 이외의 UID/GID가 0인 사용자가 존재함으로 인해 공격자가 시스템 관리자 권한을 획득할 수 있다. |

* 서버(FreeBSD)

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 계정 관리 설정 | TMSSB-001 | root 이외의 UID/GID가 0인 사용자가 존재함으로 인해 공격자가 시스템 관리자 권한을 획득할 수 있다. |

* 서버(윈도우)

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 계정관리 설정 | TMSSW-001 | Administrator 계정의 이름을 변경하지 않음으로 인해 공격자가 Administrator 계정을 통하여 시스템 관리자 권한을 획득할 수 있다. |

* 웹 서버

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 입력 값 검증부재 | TMG-001 | XSS(Cross Site Scripting) 취약점으로 공격자가 타 사용자(관리자)의 인증정보를 획득할 수 있다. |

* DB(Oracle)

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 계정 보안관리 | TMDOR-001 | Default 계정/패스워드를 사용함으로 인해 공격자가 알려진 정보를 이용하여 데이터베이스에 쉽게 접근할 수 있다. |

* DB(MySql)

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 계정 및 패스워드 관리 | TMDMY-001 | 불필요한 계정이 존재하여 공격자가 계정의 취약점을 통해 권한 획득이 가능하다. |

* Web/Was(Apache)

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 서버 보안 설정 | TMWEA-001 | 불필요한 계정이 존재하여 공격자가 계정의 취약점을 통해 권한을 획득할 수 있다. |

* Web/Was(Tomcat)

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 감사 및 로깅 | TMWAT-002 | 로그 기록 설정이 부적절하여 시스템에 발생하는 합법, 비합법적인 활동들을 추적할 수 없다. |
| 환경설정 | TMWAT-003 | 원격 SHUTDOWN 포트가 기본포트(8005)으로 설정되어 있어 공격자에 의해 shutdown 될 수 있다. |

* Web/Was(IIS)

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 감사 및 로깅 | TMWAI-001 | 로그 관리가 부적절하여 발생하는 합법, 비합법적인 활동들을 추적할 수 없다. |

* 네트워크

| **영역** | **코드** | **우려사항** |
| --- | --- | --- |
| 계정 관리 | TMNWK-001 | 장비 포트 접속 패스워드 설정이 되어있지 않아 비인가된 사용자가 접속할 수 있다. |

[표 ‑] 법적 우려사항

|  |  |  |
| --- | --- | --- |
| **영역** | **코드** | **우려사항** |
| 법률준수 | TMCPL-001 | 데이터의 기본 접근통제 및 기록기능 등을 우회할 수 있는 특수 기능이 허가나 기록을 남기지 않고 사용될 수 있다. |

### 발생가능성 평가

우려사항의 발생 빈도를 조사하여 우려사항이 발생할 수 있는 가능성을 파악하였다. 우려사항의 발생 주기를 1 년을 기준으로 표현할 경우 연간손실 예측이 용이하다. 그러나 어떤 우려사항은 하루에도 여러 번 발생할 수 있고, 어떤 우려사항은 수년간에 걸쳐 전혀 발생하지 않을 수도 있다. 즉, 발생 빈도 추정에 과거의 통계와 경험이 가장 신뢰할 수 있는 근거가 되지만 실제 정확한 빈도를 파악하는 것이 쉽지 않은 작업이므로, 조직 내의 과거 유관 자료 혹은 담당자들의 소견에 따라 평균적인 우려사항 발생가능성을 조사하여 반영하였다.

우려사항 발생가능성은 다음의 기준에 따라 분류하여 등급을 결정하였다.

[표 ‑] 발생가능성 평가기준

| **등급** | **점수** | **발생 가능성** | **과거 발생을 참조하는 경우** |
| --- | --- | --- | --- |
| VH  (Very High) | 5 | 가능성이 매우 높음(80% 이상의 확률) | 평균적으로 1개월에 한번 혹은 그 이상의 빈도로 이벤트가 발생함 |
| H  (High) | 4 | 가능성 높음(60% 이상의 확률) | 평균적으로 3개월에 한번 정도의 빈도로 이벤트가 발생함 |
| M  (Medium) | 3 | 가능성 존재함(40% 정도의 확률) | 평균적으로 6개월에 한번 정도의 빈도로 이벤트가 발생함 |
| L  (Low) | 2 | 가능성 어느 정도 있음(20% 정도의 확률) | 평균적으로 1년에 한번 정도의 빈도로 이벤트가 발생함 |
| VL  (Very Low) | 1 | 가능성 거의 없음(확률 거의 없음) | 평균적으로 3년에 한번 혹은 그 이하의 빈도로 이벤트가 발생함 |

### 영향도 평가

우려사항의 발생에 따른 영향도를 평가하였다. 어떤 우려사항은 자주 발생하지만 소프트웨어특성화대학원 과제관리시스템에 손실을 주지 않을 수 있는 반면, 다른 우려사항은 자주 발생하지 않더라도 한번 발생하면 치명적 손실을 줄 수 있기 때문이다.

[표 ‑] 영향도 평가기준

| **등급** | **점수** | **재정적손실** | **영업권손실** | **사업경쟁력** | **사업운영** |
| --- | --- | --- | --- | --- | --- |
| VH  (Very High) | 5 | 1억원 이상 | 고객 및 광범위한 이미지 손실 | 심각한 영향 | 전업무에 막대한 영향 |
| H  (High) | 4 | 1억원~5천만원 | 전사 이미지 손실 | 중대한 영향 | 유관부서 업무에 많은 영향 |
| M  (Medium) | 3 | 5천만원~1천만원 | 내부 이미지 손실 | 보통의 영향 | 유관부서 업무에 영향 |
| L  (Low) | 2 | 1천만원~1백만원 | 팀 내부 이미지 손실 | 약간의 영향 | 해당업무에 영향 |
| VL  (Very Low) | 1 | 1백만원 이하 | 손실 거의 없음 | 거의 영향 없음 | 업무에 거의 영향 없음 |

### 법률준거성 평가

개인정보보호법 또는 정보통신망법의 준수여부에 대하여 위험 시나리오(우려사항)의 법률준거성을 평가하였다. 법률준거성 점수는 0점 또는 3점을 부여한다. 법률준거성에 해당하는 경우 3점 그렇지 않은 경우는 0점으로 한다.

### 우려사항 평가 결과

산정된 발생가능성, 영향도, 법률준거성을 기반으로 위험시나리오(우려사항)을 평가한다. 위험 시나리오(우려사항)에 대한 우려사항의 값(Concern Value)은 발생가능성, 영향도 **x3(**가중치), 법률준거성 가중치(0 또는 3)를 합산하여 평가한다.

|  |
| --- |
| **우려사항 평가값(Concern Value) = 발생가능성 + 영향도 x 3 + 법률준거성(0 또는 3)** |

[표 ‑] 우려사항 평가값(Concern Value) 분포

| **Concern Value** | **Information** | **Service** | **Documents** | **Software** | **Physical** | **People** | **합계** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **2** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **3** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **4** | 0 | 0 | 0 | 0 | 4 | 0 | 4 |
| **5** | 0 | 0 | 0 | 0 | 3 | 0 | 3 |
| **6** | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **7** | 0 | 0 | 15 | 0 | 0 | 0 | 15 |
| **8** | 127 | 1 | 0 | 14 | 285 | 0 | 427 |
| **9** | 1 | 0 | 0 | 0 | 1 | 92 | 94 |
| **10** | 104 | 1 | 3 | 0 | 313 | 0 | 421 |
| **11** | 73 | 1 | 0 | 0 | 321 | 0 | 395 |
| **12** | 4 | 0 | 0 | 0 | 216 | 0 | 220 |
| **13** | 37 | 0 | 19 | 0 | 420 | 0 | 476 |
| **14** | 132 | 1 | 0 | 14 | 1488 | 0 | 1635 |
| **15** | 2 | 1 | 0 | 0 | 590 | 0 | 593 |
| **16** | 0 | 0 | 0 | 0 | 1558 | 0 | 1558 |
| **17** | 4 | 0 | 0 | 0 | 216 | 0 | 220 |
| **18** | 6 | 0 | 0 | 0 | 3339 | 0 | 3345 |
| **19** | 0 | 0 | 0 | 0 | 1557 | 0 | 1557 |
| **20** | 0 | 0 | 0 | 0 | 939 | 0 | 939 |
| **21** | 0 | 0 | 0 | 0 | 12 | 0 | 12 |
| **22** | 0 | 0 | 0 | 0 | 6 | 0 | 6 |
| **23** | 0 | 0 | 0 | 0 | 3 | 0 | 3 |
| 합계 | 490 | 5 | 37 | 28 | 11271 | 92 | 11923 |

[그림 ‑] 우려사항평가 분포

## 위험분석

### 위험분석 개요

정보자산의 취약점에 대해서 우려사항 평가를 통하여 자산에 발생 가능한 위험수준을 파악하고 이에 대한 보안통제를 적용함으로써 자산의 위험수준을 감소시키는 위험관리체계의 수립을 수행한다.

위험도란 취약점을 이용하여 위협이 발생하고 그로 인하여 자산이 손상을 입게 될 잠재적인 가능성을 말한다. 일반적으로 위험 분석 시 위험도 산정에 있어서 위협 및 취약점은 그 구분이 모호한 경우가 많아 여러 위험분석 방법론들에서도 서로 상이한 위협과 취약점의 처리순서를 보이고 있다. 아래와 같이 자산(A), 위협(T), 취약점(V) 및 위험(R)에 대해 자산기반의 위험분석 방법이 존재하기도 하며, 위협과 취약점간의 애매성을 배제하기 위해 한가지만을 선택하고 있는 경우도 존재한다.

[표 ‑] 위험분석 모델과 방법론

| **위험분석모델** | **위험분석방법론** |
| --- | --- |
| AVR 모델 : 자산→취약점→위험(위협 없음) | ISO/IEC TR 13335-3부 |
| AVTR 모델 : 자산→취약점→위협→위험 | BDSS, HWAK |
| ATVR 모델 : 자산→위협→취약점→위험 | FIFP-65, FIPS-191, CRAMM, BDSS, 팬타, PRAM, CISSP, OCTAVE |
| ATR 모델 : 자산→위협→위험(취약점 없음) | CSE |
| TVR 모델 : 위협→취약점→위험 (자산 없음) | SP-800-30, SSE-CMM, GAO1, GAO3, 에너지성-SRAG |
| TR 모델 : 위협→위험 (자산과 취약점 없음) | 법무성-SRAG |
| 자료 없음 | ISO/IEC TR 13335-1부, BS-7799, Open Framework |

여기서는 보다 체계적인 위험분석을 위하여 위협과 취약점을 통합하여 파악하는 방법을 선택하였다. 즉, 자산에 대한 가치를 평가하고, 자산과 연관된 취약점을 식별, 자산에 따른 취약점을 체계적으로 분석하여 우려사항에 대한 세부위험을 규명하고, 이러한 위험이 발생된 경우 자산에 영향을 미칠 것으로 예상되는 피해 정도를 고려하여 위험분석을 수행한다.

### 위험분석 방법

#### 위험도 평가방법

위험분석은 자산 평가, 우려사항 평가의 결과를 합한 위험도를 위험등급 5단계(매우 높음, 높음, 중간, 낮음, 매우 낮음)로 평가한다. 위험도의 결과는 해당자산에 취약점이 존재할 때 의미를 지니며, 위험도에 따라 정보보호대책과 우선순위를 정한다. 위험도 산정 방법은 다음과 같다.

|  |
| --- |
| **위험도 = 자산가치(중요도) + 우려사항 평가값(Concern Value)** |

### 위험 수용 기준 설정

위험분석을 통하여 도출된 위험도에 따라 아래의 표 기준으로 등급을 산정하고 등급에 따른 위험 수용 여부를 설정한다.

[표 ‑] 위험 등급 기준

| **위험등급** | **위험도** | **수용여부** | **내용** |
| --- | --- | --- | --- |
| 1등급 | 25~28 | 관리해야 할 위험 | 정보의 유출, 변조, 파괴, 서비스 중지로 업무수행 및 기업이미지에 매우 심각한 위험  정보보호관련 법률에 대한 준거성에 영향을 줄 수 있는 위험 |
| 2등급 | 20~24 | 관리해야 할 위험 | 정보의 유출, 변조, 파괴, 서비스 중지로 업무수행과 기업이미지에 심각한 위험 |
| 3등급 | 16~19 | 관리해야 할 위험 | 업무수행에 중대한 영향은 발생하지 않으나 관리적 조치가 필요한 상태 |
| 4등급 | 11~15 | 허용 가능한 위험 | 업무수행에 위험이 발생하나 심각한 영향이 아니며 빠른 시간 내에 복구 가능 |
| 5등급 | 5~10 | 허용 가능한 위험 | 위험이 거의 발생하지 않거나 발생 시에도 업무에 미치는 영향이 미비함 |

### 위험분석 결과

위험분석은 소프트웨어특성화대학원 과제관리시스템의 모든 정보자산을 대상으로 잠재적인 보안위협, 보안취약점이 무엇이며, 소프트웨어특성화대학원 과제관리시스템 내 보안취약점에 따른 우려사항이 어느 정도의 수준을 가지고 있는지 평가하고 이에 대해 위험도를 평가한다.

#### 위험 등급별 분포

각 자산가치 등급과 취약점에 따른 우려사항 수준을 평가한 결과를 토대로 위험도를 산정한 결과 1등급부터 3등급의 위험도를 갖는 위험 요인은 전체 위험(Risk) 중 80% 이상을 차지하고 있다.

[표 ‑] 위험도 분포

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1등급** | **2등급** | **3등급** | **4등급** | **5등급** | **총합계** |
| **위험수** | **21** | **5942** | **3959** | **1709** | **292** | **11923** |
| **백분율** | **0.2%** | **49.8%** | **33.2%** | **14.3%** | **2.4%** | **100.0%** |

[그림 ‑] 위험도 분포

#### 자산 범주별 위험도 분포

다음은 자산범주별/등급별 위험도 분포이다.

[표 ‑] 자산범주별 위험도 분포

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **1등급** | **2등급** | **3등급** | **4등급** | **5등급** | **총합계** |
| Information | 0 | 10 | 132 | 310 | 38 | **490** |
| Service | 0 | 1 | 2 | 2 | 0 | **5** |
| Documents | 0 | 0 | 16 | 9 | 12 | **37** |
| Software | 0 | 0 | 11 | 13 | 4 | **28** |
| Physical | 21 | 5931 | 3798 | 1283 | 238 | **11271** |
| People | 0 | 0 | 0 | 92 | 0 | **92** |
| **위험수** | **21** | **5942** | **3959** | **1709** | **292** | **11923** |
| **백분율** | **0.2%** | **49.8%** | **33.2%** | **14.3%** | **2.4%** | **100.0%** |

[그림 ‑] 자산범주별 위험도 분포

# 보호대책 수립

보호대책은 보안 위험등급 중 고위험군에 해당하는 위험 및 자산을 도출하고 그 위험을 경감하기 위해 보호대책을 수립한다.

## 보호대책 수립 전략

도출된 모든 위험에 대한 보호대책 수립전략은 시간과 비용을 고려하여 비현실적이고, 비효율적인 위험은 제외하고 소프트웨어특성화대학원 과제관리시스템에서 필요로 하는 위험관리수준(DOA : Degree of Assurance, 이하 ‘DoA’)을 결정하여 DoA이상 되는 위험에 대해 보호대책을 수립함을 원칙으로 한다.

소프트웨어특성화대학원 과제관리시스템은 실무자 협의와 CISO의 최종 승인을 통해 수용 가능한 위험수준(DoA)을 위험등급 3으로 선정하였다. 위험등급 3(위험도 16)은 ISMS의 보안 목표를 충족시키고 비즈니스 수행에 무리를 주지 않는 위험관리 수준(DoA)이다.

DoA를 위험등급 3이상으로 선정한 이유는 모든 위험을 관리하기에는 시간적, 비용적 문제가 발생될 수 있으며, 3등급 이하의 위험은 업무수행에 위험이 발생하더라도 심각한 정도가 아니며 빠른 시간 내에 복구가 가능하고 신속히 대응할 수 있는 정도의 위험으로 해당 담당자의 지속적인 모니터링으로 조치가 가능하다고 판단되었기 때문이다.

## 보호대책 선정

보호대책 선정은 관리체계(IS) 위험과 기술분석(TA) 위험으로 나누어 고려되어야 한다. 관리체계 위험은 DoA 기준에 따라 보호대책을 선정하여도 위험에 대한 통제가 가능한 반면 기술분석 위험은 최소의 위험으로도 해킹의 피해가 발생할 수 있기 때문이다. 기술분석위험은 모두 조치함을 원칙으로 한다.

## 위험대응 전략

정보보호대책을 수립하기에 앞서 우선적으로 정보보호대책수립을 위한 위험별 대응전략을 결정해야 한다.

위험별 대응전략으로 위험분석 결과 3등급이상을 초과하는 위험에 대해서 위험수용, 위험감소, 위험회피, 위험전가를 선택한다.

* 위험 수용(acceptance)이란 현재의 위험을 받아들이고 잠재적 손실 비용을 감수하는 것을 말한다. 어떠한 대책을 도입하더라도 위험을 완전히 제거할 수는 없으므로, 일정 수준 이하의 위험은 감수하고 사업을 진행하는 것이다.
* 위험 감소(Risk reduction, mitigation)란 위험을 감소시킬 수 있는 대책을 채택하여 구현하는 것이다. 대책의 채택 시에는 이에 따른 비용이 소요되기 때문에 이 비용과 실제 감소되는 위험의 크기를 비교하는 비용효과 분석을 실시한다. 즉,

|  |
| --- |
| **정보보호대책의 효과 = 기존 ALE - 대책구현 후 ALE - 연간대책비용** |

으로서 양(+)의 효과를 갖는 정보보호대책을 선택한다.

* 위험 회피(Risk avoidance)는 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것이다. 위험의 발생가능성 및 영향도가 높아 직접적으로 보호대책을 수립할 수 없는 자산이나 여건의 한계로 해당업무 철수 또는 주변 자산들의 보호대책 수립과 같이 다른 대안을 모색함으로써 위험도을 떨어뜨릴 수 있다.
* 위험 전가(Risk transfer)란 보험이나 외주 등으로 잠재적 비용을 제3자에게 이전하거나 할당하는 것이다. 보호대책을 수립하기에는 많은 투자가 수반되는 경우 보호대책으로 보험 등을 가입함으로써 보안사고 발생에 의한 피해를 대체할 수 있다.

## 위험처리 계획

위험처리 계획은 “3. 위험대응 전략”에 따라 해당 자산의 주요위험에 대해 대응전략에 대한 대응방안을 마련한다. 발견된 위험은 관리, 물리, 기술로 분류하여 체계적으로 위험처리계획을 수립한다.

[표 ‑] 위험처리계획

| **부문** | **주요사항** | **대응전략** | **대응방안** | **수행시기** |
| --- | --- | --- | --- | --- |
| 관리 | 정보보호  정책 |  |  |  |
| 외부자보안 |  |  |  |
|  |  |  |
| 시스템 개발보안 |  |  |  |
| 감소 | **시험데이터 보안 강화**   * 실제 운영데이터의 사용 제한: 시험과정의 데이터는 운영데이터와 다르게 임의의 데이터를 생성하거나 가공하여 사용 | 중기 |
|  |  |  |
| 암호통제 |  |  |  |
|  |  |  |
| 접근통제 |  |  |  |
|  |  |  |
|  |  |  |
| 운영보안 |  |  |  |
| 침해사고관리 |  |  |  |
|  |  |  |
| IT재해복구 |  |  |  |
| 물리 | 물리적보안 |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 기술 | 보안취약점 개선 |  |  |  |

(수행시기 – 단기: 2015/12, 중기: 2016/6, 장기: 2016년 이내)

# 별첨

## 인터뷰 담당자 목록

| **담당부서** | **담당자** | **근무처 전화** | **전자메일** |
| --- | --- | --- | --- |
| 기획실 | 홍길동 | 000-000-0000 | gildong@tm.com |
| … | … | … | … |

## 위험분석 상세내역

위험분석 상세내역은 문서 “TM 정보자산 위험분석평가표.xlsx”에서 확인할 수 있다.