+ 허종오 · 한국 CISSP협회 연구분과 이사, 전자계산기기술사


# 비즈니스 연속 계획과 운영 보안 도메인

지난 호에서는 암호학과 응용프로그램 보안 도메인에 대한 요점정리와 연습문제를 통해 CISSP가 되기 위해서 필요한 기본 지식과 응용 지식을 학습하였다. 이번 호에서는 CISSP의 10개 도메인 중에서 지금까지 학습한 관리적, 물리적, 기술적 지식들을 현장. 즉, 실무에서 어떻게 활용할 수 있는지를 종합적으로 정리한 비즈니스 연속 계획 도메인과 운영 보안 도메인에 대해서 알아보고자 한다.

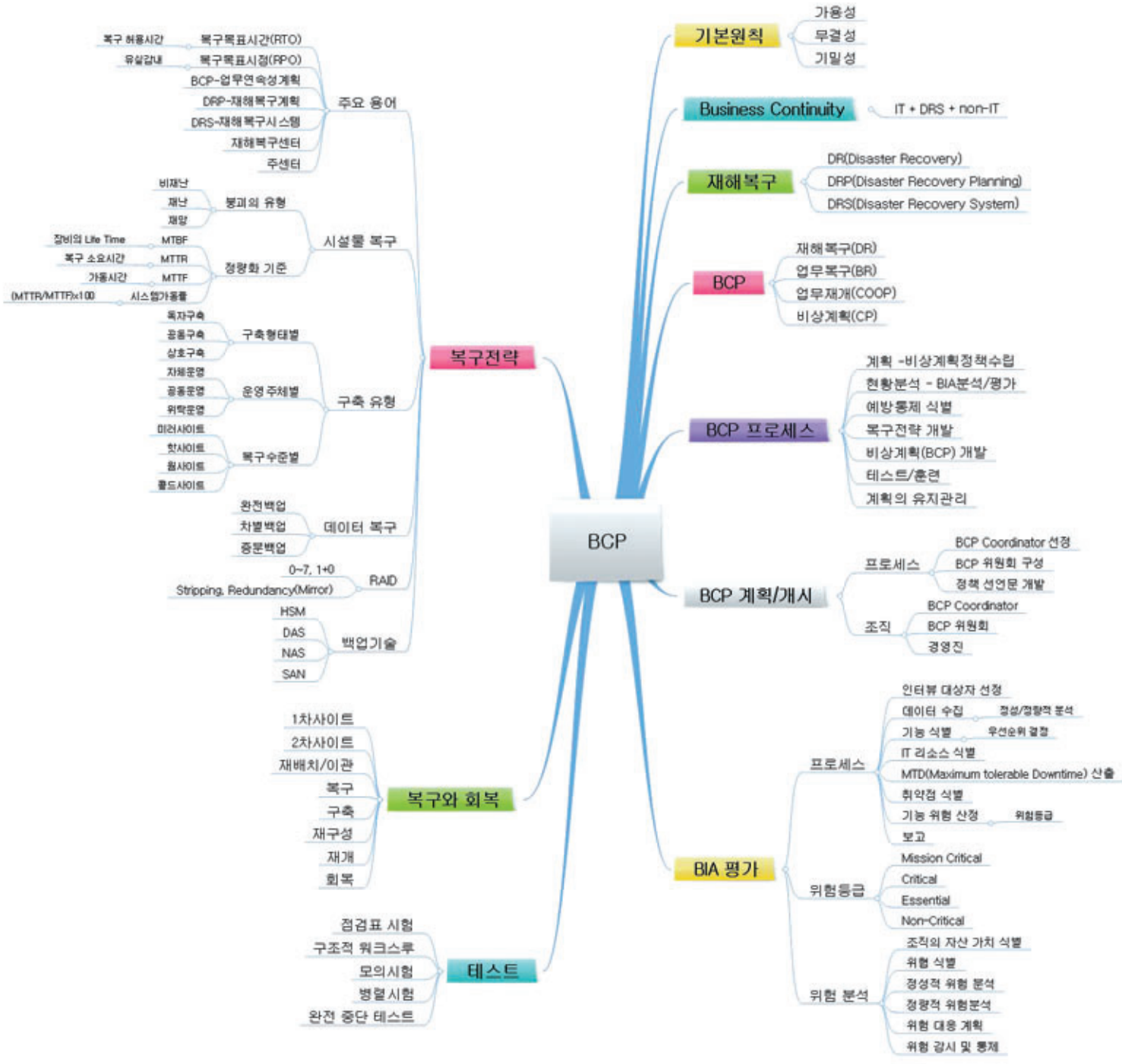
## 1. 비즈니스 연속 계획(Business Continuity Pan) 요점정리

비즈니스 연속계획(이하 BCP) 도메인은 기업의 비즈니스 연속성을 보장하기 위한 계획, 절차와 함께 사용되는 기술적인 측면까지를 학습하는 과목이다. 이 도메인을 통해 기업은 재난, 재해로부터 시스템이 피해를 입을 경우 긴급 조치로 최소한의 기업 업무 가용성을 보장하기 위한 활동을 실시하며, 단계적으로 정상적으로 복구하기 위한 업무의 순서를 정하고, 운영하는 절차로 학습하게 된다.
BCP 도메인에서 학습해야 할 요점들은 다음 Domain Map을 통해 한 눈에 알 수 있다.

### 1-1. 비즈니스 연속성 계획(Business Continuity Planning)의 정의

기업의 업무 및 시스템의 연속성과 가용성을 확보하기 위해 기업에 대한 다양한 위험의 평가, 이러한 위험이 발생하는 경우 조직이 미치는 영향을 최소화하기 위한 정책 및 복구 프로세스로 구성된 계획서이다.

[그림 1] BCP의 Domain Map



### 1-2. 재해 복구 계획(Disaster Recovery Planning)의 정의

재해 발생 시 더 많은 피해를 줄이고 중요 시스템을 유지하기 위해 재난 발생 동안, 그리고 재난 사건 발생 즉시 실행되어야 할 조치사항으로 모두의 안전을 보장하며, 필수 구성 요소를 온라인 상태로 되돌리는 활동을 정리한 계획서이다.

(1) 재해 발생 원인

| 원인 | 종류 |
|---|---|
| 자연재해 | 천재지변, 홍수, 지진, 낙뢰, 태풍, 토네이도 등 |
| 사고 | 전원공급 중단, 통신 단절, 화재, 도난, 메일 침입, 바이러스, 교통사고, 화학적 오염 문제 등 |
| 물리적 충돌 | 테러, 시민 노동 운동, 사회 불안 요소 등 |
| 내부재해 | 파업, 근무 태만, 농성 등 |

(2) 재해 복구 계획과 재해 복구 시스템

| 종류 | 설명 |
|---|---|
| 재해 복구<br>(DR, Disaster Recovery) | 재해로 인하여 중단된 정보기술 서비스를 재개하는 것 |
| 재해 복구 계획<br>(DRP, Disaster Recovery Planning) | 정보기술 서비스 기반에 대하여 재해가 발생하는 경우를 대비하여,<br>이의 빠른 복구를 통해 업무에 대한 영향을 최소화하기 위한 제반 계획 |
| 재해 복구 시스템<br>(DRS, Disaster Recovery System) | 재해 복구 계획의 원활한 수행을 지원하기 위하여 평상 시에 확보하여 두는<br>인적 · 물적 자원 및 이들에 대한 지속적인 관리체계가 통합된 것 |

### 1-3. BCP(Business Continuity Planning) 수립 절차

| 원인 | 종류 |
|---|---|
| 비상 계획<br>정책 수립 | – BCP를 개발하는데 필요한 지침을 제공<br>– 업무 수행에 필요한 역할에 권한을 위임하는 정책 작성<br>– 범위/목표/역할의 정의, 법률과 규정의 요구사항과 통합<br>– 경영진은 정책을 승인하고 지원<br>· 정책의 포함 요소 : 책임과 역할, 범위, 훈련 요구사항, 훈련 일정, 유지관리 일정, 백업 |
| BIA 평가 | – 중요한 기능과 시스템, 리소스의 식별<br>– 리소스에 대한 MTD 계산<br>– 중단 영향과 허용 가능한 정지 시간 기반으로 복구 우선순위 개발<br>– 위험과 취약점을 식별하고 위험을 계산<br>– 백업 솔루션을 식별 |
| 예방통제<br>식별 | – 경제적인 방법으로 조직의 위험 수준을 줄일 수 있는 통제와 대책을 식별 및 구현<br>– 대책의 이행, 대책의 유지관리<br>– 예방통제는 비상계획에 문서화되고 관련된 인력은 언제, 어떻게 그 대책을 사용해야할지 훈련 필요 관련 대책은 항상 효과적 이도록 유지<br>· Preventive control : UPS, Generator, Fire suppression system, 화재 감지장치, 누수 감지, 내화금고, 재해마스터 시스템,<br>shutdown switch, 백업, 암호화 등 |
| 복구전략<br>개발 | – 시스템과 중대한 기능을 빠르게 온라인으로 복구되는 것을 보증하기 위한 방법 개발<br>– 복구 방법의 정의, 시스템 아키텍처와 통합<br>– 복구전략은 IT운영을 및 연관된 서비스의 중지를 빠르고 효과적으로 회복하기 위한 방법을 제시<br>· 백업 방법 : electronic vaulting, mirrored disks(RAID), Offsite backup facility<br>· 대체 사이트 : long-term effects<br>· 구현 방법 : Cold, warm, hot, mobile, mirror site |

| 원인 | 종류 |
|---|---|
| 비상 계획 개발 | – 재해 시 무능력한 상태에서조직의 비즈니스 기능을 유지 할 수 있는 절차와 지침 작성<br>– 절차, 복구 솔루션, 임무와 역할, 비상대응<br>– 비즈니스 과정, 시설물, 공급과 기술, 데이터 등 |
| 테스트, 훈련 | – 계획을 테스트, 계획의 개선, 직원교육<br>– BCP 부족한 부분을 식별하기 위해 테스트하고 예정된 업무를 준비할 수 있도록 훈련<br>– 테스트 목표의 개발, 성공요소의 개발, 계획에 포함, 인력의 훈련 |
| 계획의 유지관리 | – 변경 통제 프로세스에 통합<br>– 책임 부여/할당/계획 업데이트<br>– 계획의 검토 및 업데이트, 내외부 조직의 조화, 대책의 분배, 변경의 문서화 |

### 1-4. 비즈니스 영향 분석(Business Impact Analysis) 프로세스

BCP를 수립하는 절차 중에서 가장 중요한 프로세스로 비즈니스 영향 분석이 있다. 비즈니스 영향 분석을 하는 이유는 재해가 발생하여 시스템이 멈출 경우에 어떤 비즈니스에 얼마만큼의 영향을 미치는지 알아내는 것을 목적으로 한다.

| 단계 | 설명 |
|---|---|
| 대상자 선정 | – 데이터 수집을 위해 인터뷰할 대상 선정 |
| 데이터 수집 | – 데이터 수집 기술을 생성<br>· 조사, 설문, 정성적/정량적 분석 |
| 기능 식별 | – 기업의 핵심 비즈니스기능 식별<br>· 우선순위 결정 |
| 리소스 식별 | – 비즈니스 기능별 IT 리소스 식별 |
| MTD(Maximum Tolerable Downtime) 산출 | – 재해 중단 시 리소스 없이 업무 지속가능 시간 산출<br>· 비 필수 30일<br>· 보통(Normal) 7일<br>· 중요(Important) 72시간<br>· 긴급(Urgent) 24시간<br>· 중대(Critical) 수 분에서 수 시간<br>– 기업의 업무 기능과 자산은 모두 위 영역 중 하나로 분류<br>– 유지 보수 업체와 SLA 체결이나 백업 솔루션 도입 시 사용 |
| 취약점 식별 | – 핵심 비즈니스 기능의 취약점과 위협 식별<br>· 재해 발생가능성<br>· 인위적, 자연적 또는 기술적 위협 식별 |
| 기능 위험 산정 | – 개별적 비즈니스 기능에 대한 위험 산정 |
| 보고 | – 모든 사항을 문서화 하고 경영진에게 제출 |

### 1-5. 재해 복구 시스템 복구 수준별 유형

재해 복구 시스템을 구성함에 있어 업무의 중요성, 업무 영향도를 평가하여 다음과 같이 복구 수준을 정한다.

(1) 미러 사이트(Mirror Site)

– 주 센터와 동일한 수준의 정보 기술 자원을 원격지에 구축해두고, 주 센터와 재해 복구센터 모두 액티브 상태로 실시간에 동시 서비스를 하는 방식

– 재해 발생 시 복구까지의 소요시간(RTO)은 즉시(이론적으로는 0)

– 초기 투자 및 유지 보수에 높은 비용이 소요
– 웹 어플리케이션 서비스 등 데이터의 업데이트의 빈도가 높지 않은 시스템에 적용 가능

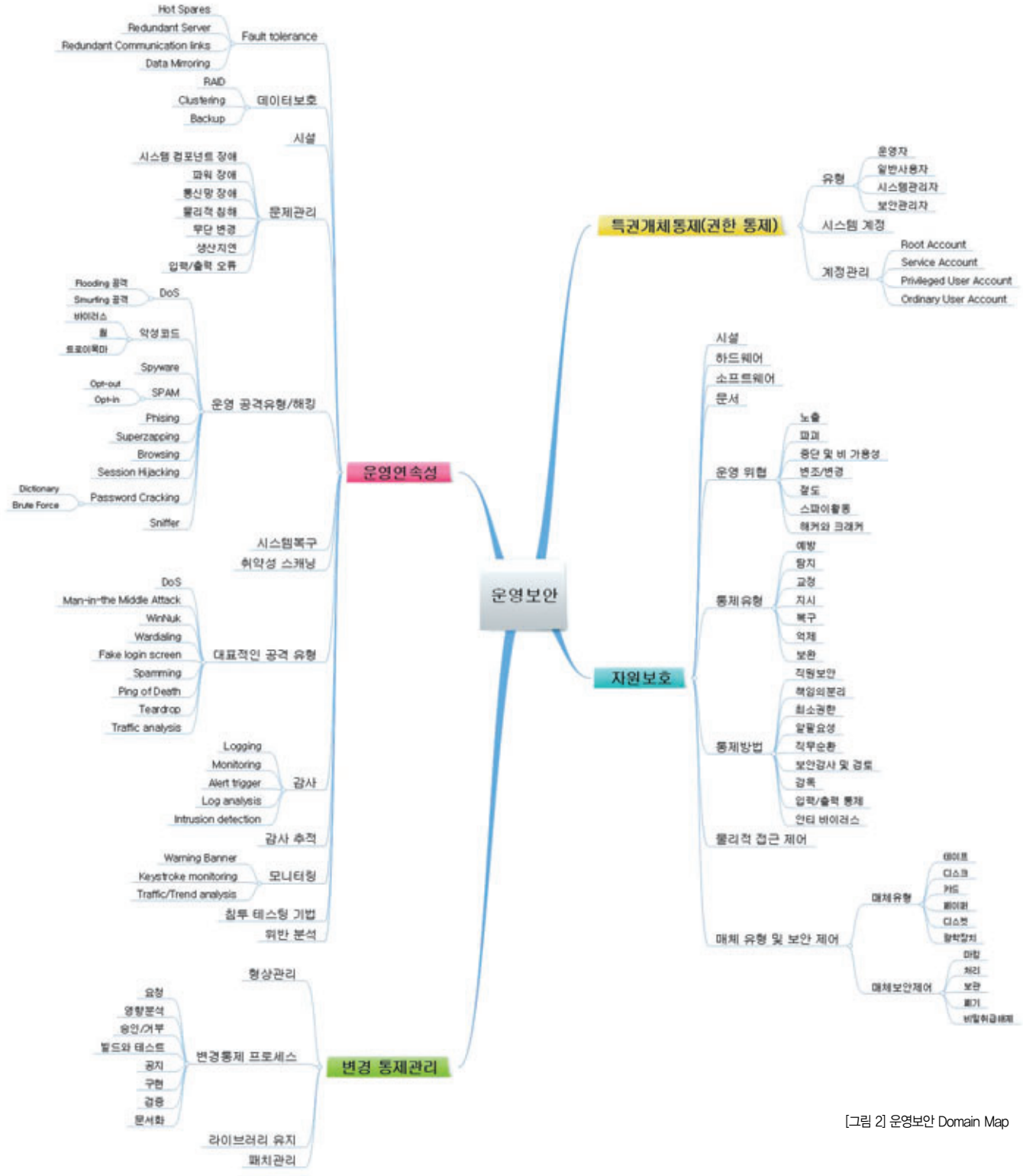
(2) 핫 사이트(Hot Site)
– 주 센터와 동일한 수준의 정보 기술 자원을 대기 상태(Standard)로 사이트에 보유하면서, 동기적 또는 비동기적 방식으로 실시간 미러링(Mirroring)을 통하여 데이터를 최신으로 유지
– 주 센터 재해 시 재해 복구 센터의 정보 시스템을 액티브로 전환하여 서비스하는 방식
– 재해 발생 시 복구까지의 RTO은 수 시간(약 4시간 이내)
– 초기 투자 및 유지 보수에 높은 비용 소요
– 데이터베이스 어플리케이션 등 데이터의 업데이트 빈도가 높은 시스템의 경우 사용

(3) 웜 사이트(Warm Site)
– 핫 사이트와 유사하나 재해 복구 센터에 주 센터와 동일한 수준의 정보 기술 자원을 보유하는 대신 중요성이 높은 정보 기술 자원만 부분적으로 재해 복구 센터에 보유하는 방식
– 실시간 미러링을 수행하기 않으며 데이터의 백업 주기가 수 시간에서 1일 정도로 핫사이트에 비해 다소 김(RTO가 수 일~수 주)

(4) 콜드 사이트(Cold Site)
– 데이터만 원격지에 보관하고 서비스를 위한 정보 자원은 확보하지 않거나 장소 등 최소한으로만 확보하고 있다가 재해 시에 데이터를 근간으로 필요한 정보 자원을 조달하여 복구하는 방식
– 주 센터의 데이터는 주기적(수 일~수 주)으로 원격지에 백업
– 구축과 유지보수 비용이 가장 저렴하나 복구 소요시간이 매우 길고 복구의 신뢰성이 낮음

지금까지 BCP에 대해서 살펴보았다. BCP는 주요 업무 복구 절차를 설명하는 것이 주를 이루고 있다. 따라서, 관리자가 갖추어야 할 필수 업무 절차이므로, 최근 시험의 추세인 관리자 위주의 시험에 맞게 출제 빈도가 높아지고 있다. 또한, 실제 상황에 어떻게 처리할 것인지 묻는 문제가 많이 출제되므로, 학습 시에 실제 상황을 함께 연상하는 학습이 필요하다.

| 분야 | Key Factor | 출제 비중 |
|---|---|---|
| BCP | – 비즈니스 리소스 식별과 가치 할당 이해<br>– 비즈니스 영향 분석과 가능한 손실 예측기법 학습<br>– 단위 운선순위와 위기관리 이해<br>– 계획 개발, 실행 그리고 관리유지 방법 이해 | 보통 |




[그림 2] 운영보안 Domain Map

## 2. 운영 보안(Operation Security) 요점정리

운영 보안은 실제 기업의 시스템, 네트워크, 어플리케이션, 환경이 안전하고 보호되어 실행하도록 유지하기 위한 모든 활동을 학습하는 도메인이다. 따라서, 운영 보안은 BCP와 같이 지금까지 배운 각종 관리적, 기술적, 물리적 보안 대책들이 총망라된 도메인이다.

### 2-1. 시스템 권한 관리

시스템에 대한 사용자의 역할과 책임을 명확하게 하기 위해 시스템에 대한 권한 개체를 관리한다. 권한은 운영자, 일반 사용자, 시스템 관리자, 보안 관리자로 구분된다.

| 유형 | 설명 |
|---|---|
| 운영자<br>(System Operators) | – 시스템의 실제 Operating을 담당<br>– 시스템 관리자보다는 낮지만 높은 레벨의 권한을 가짐<br>– 보안 정책을 우회 할 수 있음<br>– 일반적으로 메인 프레임 아키텍처환경에서 사용<br>· Implementing the initial program<br>· Monitoring execution of system<br>· Controlling job flow<br>· cf. Superzapping : 통제수단을 우회할 수 있는 관리자용 유틸리티 |
| 일반 사용자<br>(Ordinary Users) | – 운영자에 비해 권한이 제약됨<br>– 허락된 응용에만 접근 가능<br>– 일반적으로 C/S 아키텍처 환경에서 사용<br>– 최소 권한의 원칙 준수 |
| 시스템 관리자<br>(System Administrators) | – 시스템 관리자는 시스템 운영 및 유지보수를 총괄<br>– 각종 워크스테이션, 서버, 응용 시스템, 네트워크 장비 등에 대한 유지보수와 모니터링 이 주요 Task 활동<br>· 시스템의 Startup/Shutdown<br>· 사용자 등록/삭제<br>· 하드웨어 관리<br>· 디스크/데이터 마운팅 |
| 보안 관리자<br>(Security Administrators) | – 보안 시스템의 운영에 대한 관리. 감시 Role<br>· File Sensitivity Label<br>· System Security Characteristics<br>· User Clearance<br>· Passwords<br>· Account Characteristics<br>· Security Profile<br>· Audit Data Analysis and management |

### 2-2. 자원 보호(Resource Protection)

보호해야 할 운영 자원들이 다양한 형태로 존재한다.

(1) 시설(Facilities)

– IT 운영환경 유지를 위한 충분한 설비 필요
– 다양한 유틸리티와 시스템은 운영 지원과 지속적인 보호 필요
– 화재 탐지(detection)와 방재(suppression) 시설 필요
– 난방(Heating), 환기(ventilation), 에어컨 시설 등 적절한 온도 유지와 습도 제어를 위한 환경을 구성
– 신뢰성 있는 전력 공급과 분산 시스템 지원을 통해서만 충분한 가용성 보장 가능

(2) 하드웨어(Hardware)

– 시스템 하드웨어는 적정한 기밀성(confidentiality), 가용성(availability), 통합성(Integrity)을 위한 충분한 보안 측정 요구

– 보안 측정(Security Measure)은 최소 권한 원칙에 따름

· Access control for server and host system

· Printing Device Management

· Firewalls act as the network sentinel

· VPN(Virtual Private Network) devices encrypt network traffic

· Access Control for Routers and switches

· Network Cable Management(Periodically Inspection etc.)

· Wireless equipment Management(WEP, WAP encryption algorithm)

(3) 소프트웨어(Software)

– License Management

· Prevent SW license copyright infringement

· Prevent illegal duplication and distribution of licensed software

– Sensitive type 정보들은 password file로 관리

– Audit log review

(4) 문서(Documentation)

– 모든 문서는 시스템을 통해 목록화하여 관리 통제

– 내부 문서는 네트워크 설계, 취약성, 소유 방법, hard or soft copy에 대한 제어

– Hard or soft copy format에 대한 물리적, 논리적 제어 관리

이러한 자원들이 노출된 운영 위협은 다음과 같다.

| 위협 | 설명 |
|---|---|
| 노출<br>(Disclosure) | – 권한이 없는 주체에게 정보가 공개되는 것<br>– 기존의 보안 모델인 DAC 환경에서취약성 발생<br>– 개인별 데이터를 Copy하여 운용하는 과정에서 발생 가능 |
| 파괴(Destruction) | – 시스템 데이터나 자원의 파괴는 악의적이거나, 고의가 아니지만 회복 할 수 없는 손상 결과 초래, 대부분 Man-made 재해 |
| 중단 및<br>비 가용성 | – Interruption and Non availability<br>– 장비, 서비스, 운영 프로시저들의 장애로 시스템의 중단<br>– DoS 공격이나 악성코드로 인한 운용 장애 |
| 변조/변경 | – Corruption and Modification<br>– 환경적인 요인이나 개별적인 행위에 대해 시스템이나 데이터가 손상<br>– 온도 변경이나 전력 문제로 인해 작성 데이터에 오류가 발생 가능 |
| 절도(Theft) | – 데이터나 장비가 내부자나 도둑으로부터 절도 당함 |
| 스파이 활동<br>(Espionage) | – 기업 정보에 대한 보안 취약은 기업 경쟁우위 확보에 치명적<br>– 정부 기관뿐만 아니라 비즈니스 환경에서도 발생 가능 |

| 위협 | 설명 |
|---|---|
| 해커와 크래커 | – Hackers and Crackers<br>– 악의적인 해커들은 재미나, 자기 테스트나 오픈 소스 해킹 툴을 이용하여 시스템 침입하여 백 도어 등을 설치하여 쉽게 접근 가능<br>– Cracker : 보안 요소들을 불능으로 만들어 즐거움이나 이익을 얻기 위해 시스템에 침입. 악의적인 해커 지칭 |
| 악성코드<br>(Malicious Code) | – 정보를 무단으로 수집하거나 시스템의 치명적인 손상을 미치는 모든 유형의 위협<br>– 일반적으로 Trojan horse, viruses, worms, spyware, logic bombs 등 |

### 2-3. 운영 연속성(Continuity of Operations)

운영 시스템들의 연속성을 보장하기 위해 필요한 대응책은 다음과 같다.

(1) Fault Tolerance

– 시스템의 결함 허용성을 보장하기 위해 각 item을 중복 구성하는 방법

– 일부 컴포넌트의 결함에도 운영 연속성을 보장

– FT 시스템은 장치 오류 시 즉시, 자동적으로 전환되어 운영 연속성을 보장

(2) 데이터 보호

– 조직의 중요한 요소인 데이터를 보호하기 위한 여러 방법이 존재

– Data Backup은 시점의 데이터 손실을 가져오지만 Data  Redundancy는 장애 시 데이터 손실 없이 가용성을 보장해 줌

· RAID(Redundancy array of inexpensive disks) : Data Redundancy의 대표적인 방법으로 RAID는 이중화 및 성능 향상을 위한 기술

· 클러스터링(Clustering) : 각 서버가 요청 서비스를 참여한다는 것을 제외하고, 이중화 서버와 유사한 결함 허용 기술

· 백업(Backup) : 드라이브에 문제나 재난, 소프트웨어 오류 등이 발생 시 데이터 복구를 위한 절차 수립/백업 대상, 백업 주기 및 백업 절차에 대한 계획 수립

지금까지 운영 보안에 대해서 알아보았다. 운영 보안은 출제 빈도는 약하지만, 관리적, 기술적, 물리적 통제 방법들이 접목된 도메인이므로, 다른 과목의 선행 학습이 중요하다.

| 분야 | Key Factor | 출제 비중 |
|---|---|---|
| 운영 보안 | – 직원과 직무 기능에 관련된 관리 책임 이해<br>– Antivirus, 교육, 감사, 리소스 보호 활동의 관리 개념<br>– 예방적, 탐지적, 교정적, 복구 통제 학습<br>– 표준 준수의 의무 개념 학습 | 보통 |

이번 호에는 BCP와 운영 보안 도메인을 살펴보았다. BCP는 최근에 출제 빈도가 높아지는 추세이며, 상황식 문제를 출제하여 난이도가 높은 편이다. 따라서, 실무 경험을 참고로 한 학습이 필요하다. 운영 보안은 다른 과목의 선행 학습을 통해 다양한 위협과 기술적 대응책에 대한 학습이 필요한 도메인이다.

다음 호에는 지금까지 학습한 8가지 도메인의 기반이 되는 법, 규제, 정책 도메인과 시설물 관리를 위한 물리적 도메인에 대해서 알아보고자 한다.

### 3. 연습 문제

간단한 문제를 통해서 이번 호에서 배운 도메인에 대한 이해능력을 키우자. 중요한 것은 실제 시험에서는 이보다 어려운 문제가 출제되나, 기본을 알면 충분히 풀 수 있는 문제이니, 문제를 풀고 이해하지 못하는 부분은 요점정리를 통해 재학습이 필요하다.

▣ BCP

1. 사업 연속성 계획(BCP)의 검토시점은 언제인가?
   ① 매년 1회　② 분기별 1회
   ③ 반기 1회　④ 필요할 때마다

2. 시스템의 가용성 계산 시 짧을수록 좋은 것은 어떤 것인가?
   ① MTBF　② MTTR
   ③ MTTF　④ MTAR

3. 디스크 백업에서 속도가 빠르고 패리티 체크가 되는 RAID 방식은 무엇인가?
   ① RAID 0　② RAID 1
   ③ RAID 5　④ RAID 6

4. 핫 사이트를구축하려 할 때 가장 적합한 위치는?
   ① 동일한 전력망 내에 있는 동일한 건물
   ② 서로 다른 전력망 내에 있는 동일한 건물
   ③ 동일한 전력망 내에 있는 멀리 떨어진 건물
   ④ 서로 다른 전력망 내에 있는 멀리 떨어진 건물

5. 경영진이 보안 관리자에게 비상대응절차(Emergency Procedure)에 대한 교육시행을 지시했다. 비상대응절차에 대한 적절한 설명은 무엇인가?
   ① 비상대응절차는 전 직원에게 구두상으로 전달되어야 한다.
   ② 누구라도 알아볼 수 있도록 명확하게 문서화되고 주기적으로 갱신되어야 한다.
   ③ 비상대응절차는 최고 경영진이 최초 작성 후 변경해서는 안 되는 정책이다.
   ④ 비상대응절차에는 회사 기밀이 포함되어 있어 관리자에게만 교육한다.

▣ 운영 보안

1. 백신에서 행동 기반으로 바이러스를 탐지할 때 좋은 방법은 무엇인가?
   ① 휴리스틱 탐지　② 시그니쳐 탐지
   ③ 폴리모픽 탐지　④ 추론 탐지

2. 시스템을 백업함에 있어서 월 단위로는 시스템 전체를 백업하고, 주 단위로는 전주에 비해 바뀐 내용만을, 일 단위로는 전날에 비해 바뀐 내용만을 백업한다. 이렇게 할 경우 주, 일 백업은 백업할 양이 많지 않아 시·공간적으로 모두 효율적이게 된다. 이렇게 백업을 작은 단위로 나누어서 하는 방법을 무엇이라고 하는가?
   ① 전체 백업　② 완전+증분
   ③ 완전+차등　④ 누적 백업

3. 서버는 SYN/ACK 응답을 보낸 클라이언트로부터 ACK가 올 때까지 기다리게 되고 서버는 ACK 메시지를 받지 못하게 되었다. 어떠한 공격을 받고 있는 것인가?
   ① Land Attack
   ② Smurf Attack
   ③ Syn Flooding Attack
   ④ Ping of Death Attack

4. 해커의 침입으로 시스템의 오류가 발생하여 경영진으로부터 복구를 지시 받았다. 시스템의 복구는 어떤 통제인가?
   ① 탐지 통제　② 교정 통제
   ③ 변경 통제　④ 예방 통제

5. 다음 중 동종의 기기(FAX)들 사이의 통신을 암호화하기 위해 가장 적절한 키는 무엇인가?
   ① 개인키　② 공유키
   ③ 공개키　④ 비밀키

정답 : ①, ②, ③, ④, ②, ①, ②, ③, ②, ②