재해복구(disaster recovery)

1. 업무영향분석(BIA, business impact analysis)

- BIA는 비지니스 진행 도중에 업무가 중단되었을 때 **미치는 영향에 대한 분석**이다.
- BIA는 발생 가능한 **모든 재해**를 고려하여 잠재적인 손실을 추정하고 재난을 분류한다.
- BIA는 정성적, 정량적, 기능적 분석을 실시한다.
- BIA는 분류된 재난에 대해 우선순위를 부여하고 실행 가능한 대안을 개발해야 한다.

BIA 주요 활동	• 인터뷰 및 문서로부터 데이터 수집한다. • 비지니스 기능, 행위, 처리를 문서화한다. • 기능별로 중요도 수준, 우선순위를 결정한다. • 기능별로 분류 도표와 중요도 수준, 우선순위 결정한다. • 핵심 프로세스에 필요한 자원을 식별한다. • 조직의 필요성에 의거하여 시스템의 중요성을 식별한다. • **최대허용중단시간**(MTD)을 산정한다.

// 최대허용중단시간(MTD, Maximum Tolerable Downtime) – 한계복구시간

- 핵심 프로세스가 중단된 채로 회사가 견딜 수 있는 최장시간이다.
- 조직이 업무처리 중단으로 인한 영향을 감내할 수 있는 시간이다.

2. 재해복구계획(DRP, disaster recovery plan)

재해복구계획은 천재지변, 해킹 등 각종 재난·재해로 인해 데이터센터 등 기업의 IT 인프라에 장애가 발생하여 기능을 수행하지 못하게 되었을 때, 이를 대체하거나 복구하여 원래 기능이 수행될 수 있도록 조치하는 시스템이다.

3. 업무연속성계획(BCP)

- BCP는 재해가 발생했을 때, **사업(business) 연속성**을 유지하려는 방법을 정의한 문서이다.
- BCP는 재해에도 정상적인 업무가 가능하도록 데이터 백업 및 복구뿐만 아니라
- BCP는 고객 서비스 지속성 보장, 핵심 업무 기능을 지속하는 환경 조성을 목적으로 한다.
- BCP 개발을 위해서는 기업이 운영하는 시스템 파악이 선행되어야 한다.

- BCP 개발을 위해서는 **업무영향분석(BIA, business impact analysis)**이 **선행**되어야 한다.
- BCP는 장애에 대한 예방을 통한 중단 없는 서비스를 제공하기 위한 체계이다.
- BCP는 사업의 연속성을 유지하기 위한 업무지속성 계획과 절차이다.
- BCP는 재난 발생 후에 경영 유지·복구 방법을 명시해야 한다.
- BCP는 비상시에 프로세스의 운영 재개에 필요한 조치를 정의한다.

// BCP 접근 4단계 방법론

단계 1. 프로젝트 범위 설정 및 기획
단계 2. 업무영향분석(BIA)
단계 3. 업무연속성계획(BCP)
단계 4. 계획 승인 및 실행

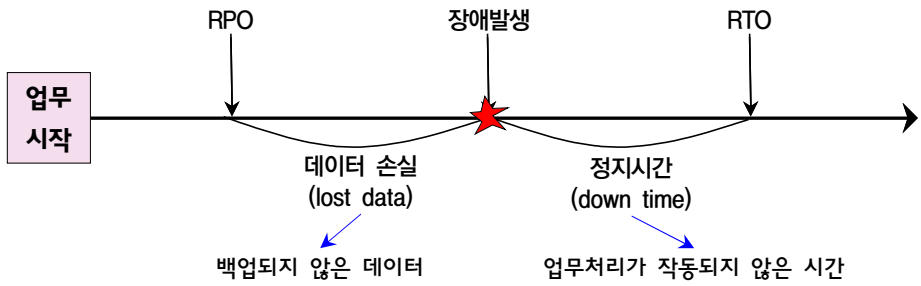
// DRP와 BCP 비교

DRP	DRP는 재해의 인해 **핵심 정보시스템 또는 데이터가 중단되는 것**에 대항하기 위해 명확하고 상세히 기술된 계획을 개발하는 것에 초점을 둔다.
BCP	BCP는 재해로 인해 **사업활동 또는 프로세스가 중단되는 것**에 대항하기 위해 명확하고 상세히 기술된 계획을 개발하는 것에 초점을 둔다.

// BCP와 DRP 공통점

- 어떤 조직에서든 **대외비**로 관리한다.(보안 정책과 프로그램의 일부가 되어야 한다)
- 위험회피가 아니라 **위험수용**이다.
- 목적은 조직의 **가용성** 확보이다.
- 일부 예방적 기능이 있으나 **교정통제**로 분류된다.

4. 복구목표시점(RPO)과 복구목표시간(RTO)



◈ **복구목표시점(RPO, Recovery Point Objective) – 데이터 관점**

- RPO는 어느 시점에 **백업**할 것인지?를 결정하는 지표이다.**(백업시점)**
- RPO는 재해 발생으로 중단된 서비스에 대해 수용 가능한 데이터 손실과 연관된다.
- RPO는 수용 가능한 데이터 손실의 양을 결정하는데 효과적이다.**(손실되어도 무방)**
- 모든 데이터의 완벽한 복구는 현실적으로 어렵다.

◈ **복구목표시간(RTO, Recovery Time Objective) – 업무 관점**

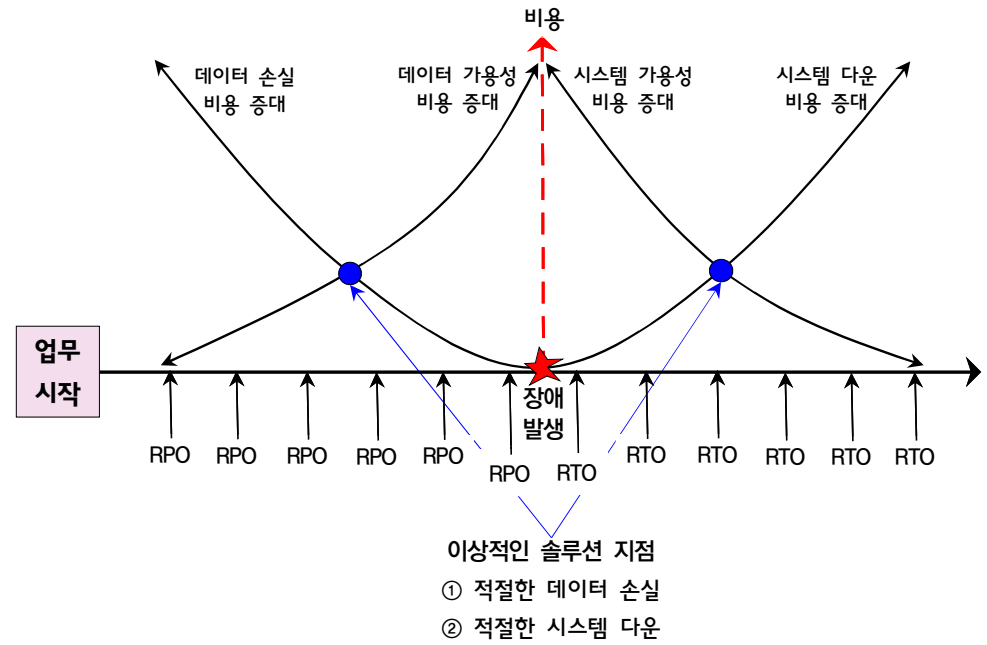
- 간단히 말하면, 복구목표시간(RTO)은 **복구하는데 걸리는 시간**이다.**(업무 관점)**
- RTO는 재해 발생 이후에 원 상태로 복구하는데 소요되는 시간이다.
- RTO는 서비스가 중단되었을 때, 서비스 복구까지 걸리는 최대 허용시간이다.
- RTO는 조직의 핵심 업무를 정상화시키기 위한 목표시간이다.
- RTO는 정성적/정량적 평가를 통해 산정한다.

// 예 : 메일을 이용하여 업무처리를 하는 경우

- 메일 데이터 손실 발생 : RPO와 관련
- 메일 서버 고장 발생 : RTO와 관련

4 http://cafe.daum.net/pass365(홍재연)

// 복구목표시점(RPO)과 복구목표시간(RTO) 비교



• RTO는 정보시스템 구축비용에 **반비례**한다.
• RTO는 재해 발생 손실에 **비례**한다.

• RPO와 RTO는 기업 상황에 맞도록 설정, 준비, 대비해야 한다.
↓예를 들면
• 금융 기관 : RPO = RTO ≒ 0
• 메일을 이용한 업무처리 : RPO = RTO ≒ 10분~1시간

• RTO=**0**인 재해복구시스템은 **주센터**와 **재해복구센터**의 데이터 전송방식을 **동기복제**방식으로 구성해야 한다.

주센터	• 현재 사용 중인 전산 인프라를 운영하는 전산센터이다. • 주 전산센터, 주 사이트라고도 함
재해복구센터	• 재해에 대비하여 업무연속성을 보장할 수 있도록 원격지에 구축한 전산센터이다. • 원격지센터 또는 백업센터라고도 한다.

5. 재해복구시스템

- 정보통신부 자료 참조

재해복구시스템은 복구 수준에 따라 **미러/핫/웜/콜드** 사이트로 구분한다.

미러사이트(mirror site)	주센터와 재해복구센터는 같은 수준으로 구축, **동시에 실시간 서비스**
↓	
핫사이트(hot site)	주센터와 재해복구센터는 같은 수준으로 구축, 재해복구센터는 **대기** 상태
↓	
웜사이트(warm site)	재해복구센터에는 **중요성이 높은 정보기술자원**만 보유
↓	
콜드사이트(cold site)	재해복구센터에는 **데이터**만 보관

① 미러사이트(mirror site)

- 미러사이트는 주센터와 같은 수준의 정보기술자원을 원격지에 구축해 둔다.
- 주센터와 재해복구센터 모두 액티브 상태(active-active)로 **실시간 동시 서비스**를 하는 방식
- 미러사이트의 이론적인 복구목표시간(RTO)과 복구목표시점(RPO)은 0이다.
- 초기투자 및 유지보수에 높은 비용이 필요하다.
- 데이터 갱신 빈도가 높지 않은 시스템에 적용 가능하다.
- 갱신 빈도가 높은 시스템에 적용하면, 양 사이트에 높은 부하 초래, 실용적이지 않다.
- 갱신 빈도가 높은 시스템은 핫사이트 구축이 일반적이다.

② 핫사이트(hot site)

- 주센터와 같은 수준의 자원을 대기상태(standby)로 원격지 사이트에 보유(active-standby)
- 동기 또는 비동기 방식의 실시간 미러링을 통해 데이터를 최신의 상태 유지(up-to-date)
- 주센터 재해시 재해복구센터의 정보시스템을 **액티브로 전환하여 서비스**하는 방식이다.
- 핫사이트는 RPO≒0을 지향한다.
- 핫사이트의 RTO는 수시간(약 4시간이내)이다.
- 데이터 실시간 미러링을 이용한 핫사이트를 미러사이트라고도 한다.
- 초기투자 및 유지보수에 높은 비용이 필요하다.
- 일반적으로, 데이터 갱신 빈도가 높은 시스템에 적용한다.

③ 웜사이트(warm site)

- 재해복구센터에 주센터와 같은 수준의 정보기술자원을 보유하는 대신(핫사이트와 유사),
- **중요성이 높은 정보기술자원**만 부분적으로 재해복구센터에 보유하는 방식이다.
- 웜사이트는 실시간 미러링을 수행하지 않으며,
- 웜사이트의 데이터 백업 주기는 수시간~1일정도이다.(핫사이트에 비해 다소 길다)
- 웜사이트의 RPO는 수시간~1일, RTO는 수일~수주이다.
- 웜사이트는 구축 및 유지비용은 핫사이트에 비해 저렴하다.
- 웜사이트는 초기 복구수준이 완전하지 않으며, 완전 복구까지는 다소 시일이 소요된다.

④ 콜드사이트(cold site)

- 콜드사이트는 원격지에 **데이터만 보관**한다.
- 콜드사이트는 서비스를 위한 자원은 확보하지 않거나 최소한으로 확보하고 있다.
- 콜드사이트는 재해가 발생하면 보간 데이터를 토대로 자원을 조달하여 복구를 개시한다.
- 콜드사이트의 RTO는 수주~수개월이다.(복구시간이 오래 걸림)
- 콜드사이트의 RPO는 수일~수주이다.(복구를 시작하는 시간이 오래 걸림)
- 콜드사이트는 주센터의 데이터를 주기적으로 원격지에 백업된다.(수일~수주, RPO와 같음)
- 콜드사이트는 구축 및 유지비용은 가장 적지만 복구소요시간이 매우 길고, 신뢰성이 낮다.

기출문제 분석

1. BCP(business continuity planning)에 대한 설명으로 옳지 않은 것은? [2021년 지방 9급]

① BCP는 사업의 연속성을 유지하기 위한 업무지속성 계획과 절차이다.
② BCP는 비상시에 프로세스의 운영 재개에 필요한 조치를 정의한다.
③ BIA는 조직의 필요성에 의거하여 시스템의 중요성을 식별한다.
④ DRP(disaster recovery plan)는 최대허용중단시간(maximum tolerable downtime)을 산정한다.

♤ **업무영향분석(BIA) / 업무연속성계획(BCP) / 재해복구계획(DRP, disaster recovery plan)**

- DRP(disaster recovery plan)는 **최대허용중단시간**(maximum tolerable downtime)을 산정한다.**(×)**
  → 최대허용중단시간은 **업무영향분석**(BIA)에서 산정한다.

// 최대허용중단시간(MTD, Maximum Tolerable Downtime) – 한계복구시간
- 핵심 프로세스가 중단된 채로 회사가 견딜 수 있는 최장시간이다.
- 조직이 업무처리 중단으로 인한 영향을 감내할 수 있는 시간이다.

정답 : ④

2. 업무연속성(BCP)에 대한 설명으로 옳지 않은 것은? [2019년 국가 9급]

① 업무연속성은 장애에 대한 예방을 통한 중단 없는 서비스 체계와 재난 발생 후에 경영 유지·복구 방법을 명시해야 한다.
② 재해복구시스템의 백업센터 중 미러사이트(mirror site)는 백업센터 중 가장 짧은 시간 안에 시스템을 복구한다.
③ 콜드사이트(cold site)는 주전산센터의 장비와 동일한 장비를 구비한 백업사이트이다.
④ 재난복구서비스인 웜사이트(warm site)는 구축 및 유지비용이 콜드사이트(cold site)에 비해서 높다.

♤ **업무연속성(BCP)**

- 콜드사이트(cold site)는 주전산센터의 장비와 동일한 장비를 구비한 백업사이트이다.(×)
  → 콜드사이트는 원격지에 **데이터만 보관**한다.
- 콜드사이트는 서비스를 위한 자원은 확보하지 않거나 최소한으로 확보하고 있다.
- 콜드사이트는 재해가 발생하면 보간 데이터를 토대로 자원을 조달하여 복구를 개시한다.

정답 : ③

3. IT 재해복구체계 수립 시, 업무영향분석(BIA: business impact analysis) 과정에서 고려하는 항목이 아닌 것은? [2019년 국가 7급]

① MTD(Maximum Tolerable Downtime)
② MTU(Maximum Transfer Unit)
③ RTO(Recovery Time Objective)
④ RPO(Recovery Point Objective)

♤ **IT 재해복구체계 수립 시, 업무영향분석(BIA)**

- 업무영향분석(BIA)은 재해가 발생했을 때, 복구최소대상인 단위업무를 정의하고, 단위업무의 복구우선순위와 복구목표시간, 복구목표시점 정의를 통해 업무복구에 필요한 자원을 산정하는 과정이다.
- 업무영향분석(BIA)을 이해하기 위해서는 기본적으로 다음 개념을 이해해야 한다.
- RTO / RPO / MTD / MTPD

◈ **복구목표시점(RPO, Recovery Point Objective) – 데이터 관점**
- RPO는 어느 시점에 **백업**할 것인지?를 결정하는 지표이다.**(백업시점)**
- RPO는 재해 발생으로 중단된 서비스에 대해 수용 가능한 데이터 손실과 연관된다.
- RPO는 수용 가능한 데이터 손실의 양을 결정하는데 효과적이다.**(손실되어도 무방)**
- 모든 데이터의 완벽한 복구는 현실적으로 어렵다.

◈ **복구목표시간(RTO, Recovery Time Objective) – 업무 관점**
- 간단히 말하면, 복구목표시간(RTO)은 **복구하는데 걸리는 시간**이다.**(업무 관점)**
- RTO는 재해 발생 이후에 원 상태로 복구하는데 소요되는 시간이다.
- RTO는 서비스가 중단되었을 때, 서비스 복구까지 걸리는 최대 허용시간이다.
- RTO는 조직의 핵심 업무를 정상화시키기 위한 목표시간이다.
- RTO는 정성적/정량적 평가를 통해 산정한다.

◈ **한계복구시간(MTD, Maximum Tolerable Downtime)**
- 핵심 프로세스가 중단된 채로 회사가 견딜 수 있는 최장시간
- 조직이 업무처리 중단으로 인한 영향을 감내할 수 있는 시간

◈ **최대허용중단시간(MTPD. Maximum Tolerable Period of Disruption)**
- 회사의 특정 업무 중단 시 회사에서 허용할 수 있는 최대중단기간을 의미
- 업무 중단 발생 시 영향 추정을 위하여 단위업무별 MTPD를 산정한다.
- MTPD는 자사의 주요 재무요소를 적용 후 단위업무별로 산정한다.
- MTPD는 조직으로 하여금 수용 불가한 상태가 되기까지 소요되는 시간을 말한다.

◈ **최대전송단위(MTU, Maximum Transfer Unit)**
- MTU는 네트웍의 물리매체에서 최대로 보낼 수 있는 데이터그램 크기이다.(바이트)
- MTU는 업무영향분석(BIA)과 무관하다.

정답 : ②

4. 다음에서 설명하는 재해복구시스템의 복구 방식은? [2015년 국가 9급]

재해복구센터에 주 센터와 동일한 수준의 시스템을 대기상태로 두어,
동기적 또는 비동기적 방식으로 실시간 복제를 통하여 최신의 데이터 상태를 유지하고 있다가,
재해 시 재해복구센터의 시스템을 활성화 상태로 전환하여 복구하는 방식이다.

---

① 핫사이트(hot site)
② 미러사이트(mirror site)
③ 웜사이트(warm site)
④ 콜드사이트(cold site)

♤ **재해복구시스템 - 핫사이트(hot site)**

- 주센터와 같은 수준의 자원을 대기상태(standby)로 원격지 사이트에 보유(active-standby)
- 동기 또는 비동기 방식의 실시간 미러링을 통해 데이터를 최신의 상태 유지(up-to-date)
- 주센터 재해시 재해복구센터의 정보시스템을 **액티브로 전환하여 서비스**하는 방식이다.
- 핫사이트는 RPO≒0을 지향한다. 핫사이트의 RTO는 수시간(약 4시간이내)이다.

정답 : ①

5. 재해복구시스템의 복구 수준별 유형에 대한 설명으로 옳은 것은? [2017년 지방 9급]

① Warm site는 Mirror site에 비해 전체 데이터 복구소요시간이 빠르다.
② Cold site는 Mirror site에 비해 높은 구축비용이 필요하다.
③ Hot site는 Cold site에 비해 구축비용이 높고, 데이터의 업데이트가 많은 경우에 적합하다.
④ Mirror site는 Cold site에 비해 구축비용이 저렴하고, 복구에 긴 시간이 소요된다.

♤ **재해복구시스템**

---

① Warm site는 Mirror site에 비해 전체 데이터 복구소요시간이 빠르다.**(×)**
→ Mirror site의 이론적인 복구목표시간(RTO)과 복구목표시점(RPO)은 0이다.
② Cold site는 Mirror site에 비해 높은 구축비용이 필요하다.**(×)**
→ Cold site는 구축비용은 가장 저렴하지만 복구소요시간이 매우 길고, 신뢰성이 낮다.
④ Mirror site는 Cold site에 비해 구축비용이 저렴하고, 복구에 긴 시간이 소요된다.**(×)**
→ Cold site가 구축비용이 저렴하고, 복구에 긴 시간이 소요된다.

정답 : ③

6. 재해복구시스템의 복구 수준별 유형에 대한 설명으로 옳지 않은 것은? [2017년 국가 7급]

① Mirror Site－주센터와 동일한 수준의 정보기술자원(하드웨어, 소프트웨어, 기타 부대장비 등)을 원격지에 구축하여 모두 액티브 상태에서 실시간으로 동시에 서비스하는 방식

② Hot Site －주센터와 동일한 수준의 정보기술자원을 대기상태(standby)로 원격지에 구축하여 동기적 혹은 비동기적 미러링을 통해 데이터의 최신을 유지하고 있다가 주센터 재해 시 액티브로 전환하여 서비스하는 방식

③ Down Site－웹 애플리케이션 서비스 등 데이터의 업데이트 빈도가 높은 정보시스템을 액티브로 전환하여 서비스하는 방식

④ Cold Site－기계실, 전원시설, 통신설비, 공조시설, 온도조절시스템 등을 갖추어 놓고, 주센터 재해 시 정보기술자원을 설치하여 서비스하는 방식

♤ **재해복구시스템의 복구 수준별 유형**

• 재해복구시스템은 복구 수준에 따라 **미러/핫/웜/콜드** 사이트로 구분한다.

정답 : ③