비즈니스 연속성 측면에서 바라본 성공적인 재해복구(DR)시스템 구축 방안

더 이상 선택이 아닌 필수가 되어버린 기업의 재해복구(DR)시스템 구축

'정부 24' 서비스까지 중단…공공기관 민원서류 발급 올스톱

카카오, 데이터센터 화재로 서비스 중단… 카뱅까지 영향

2023 년 상반기 전자금융사고 197 건…디도스 공격부터 하드웨어 노후화까지

2023 년 11 월 8 일, 금융감독원은 「금융기관 IT 부문 안정성 강화 가이드라인」을 발표하였다. 이는 최근 전산사고가 빈번하게 발생하는 것을 방지하고, 실제 비상 상황이 발생할 시 신속하게 서비스를 복구하기 위함이다. 또한 금융당국은 전산사고로 서비스가 3 시간 이상 중단될 경우 현장점검에 즉각 착수하며 기본적인 IT 내부통제 사항들을 소홀히 하여 전산사고가 발생하면 엄중 조치에 나설 방침이다.

DR(Disaster Recovery) 시스템란 무엇일까? 기업은 왜 DR 구축 및 가동에 어려움을 겪는 것일까?

DR 시스템이란 전산센터에 발생한 재해로 정보시스템의 운영이 중단되어 업무 및 서비스에 마비가 발생하였을 때, 즉각적인 업무 및 서비스 재개를 위해 중단된 정보시스템을 정상적으로 회복시키기 위한 추가적으로 마련된 IT 운영 인프라(시설) 및 IT 정보자원(H/W, S/W, N/W, 보안 등)을 포함하고 이와 관련된 이중화 복제기술들을 의미한다.

기업들은 DR 시스템 구축을 위해 대개 외부 컨설팅 업체에 자문을 구하기도 하며, 네트워크 구축, 스토리지/서버 이중화, 통신 회선 사용에 관한 비용 투자 등 많은 시설적·비용적 투자가 이루어져야 한다. 이로 인해, 기업들은 사실상 구축에 대한 필요성을 인지하고 있음에도 불구하고, DR 시스템을 신규 구축하거나, 기존 시스템의 미비점 개선 또는 유지보수를 위한 투자진행 등의 결정을 내리기에는 다양한 어려움이 존재한다.

또한, 재난·재해가 발생하기 이전에는 DR 시스템이 비상 상황에서 정상적으로 가동되는지 확인할 수 있는 이상적인 방안이 없다는 것도 DR 시스템을 보유하고 있는 기업들의 고민 중 하나이다. 정기적으로 DR 시스템 가동에 대한 모의훈련을 진행하기는 하지만, 이러한 훈련들도 사실상 부분적 또는 한정적 범위로 이루어지는 경우가 많으며 수시로 변동되는 정보 자산의 변화로 전체적인 재해복구 전환 훈련은 현실적으로 어려운 부분이 많다. 또한 이러한 상황 중에 재난이 발생하여 재해복구 시스템 가동이 필요한 경우 다양한 문제점이 발생할 수 있다.

뿐만 아니라, 우리나라는 비용/관리적인 측면상 대부분의 주데이터센터와 재해복구(DR)센터 간 지리적 위치가 멀지 않아, 비상시 동일 재해권에 속해 DR 시스템이 정상적으로 작동하지 않을 가능성도 배제하지 못한다.

실제 DR 시스템 가동 사례로는 어떤 것들이 있을까?

1. (성공사례) 미국 9.11 테러로 인한 모건스탠리 DR 시스템 가동

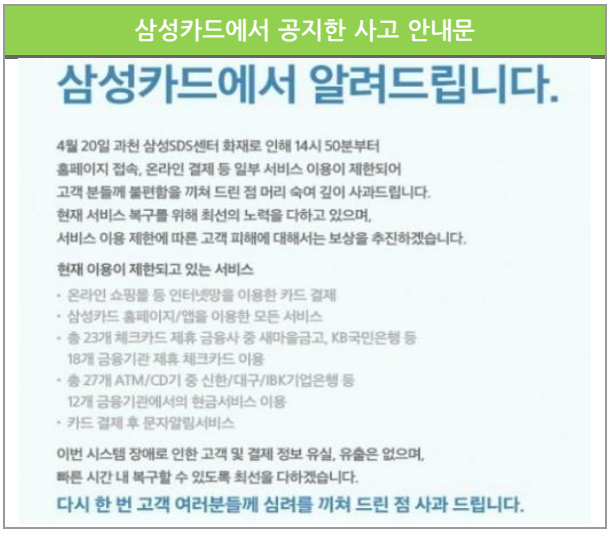
대표적인 성공 사례로는 성공적인 BCM 체계 구축 및 운영으로 유명한 케이스인 '모건스탠리' 사례이다. 모건스탠리는 2001 년 미국 9.11 테러라는 대위기 속에서, 기 구축한 BCP 와 이와 연계된 DR 시스템을 성공적으로 이행 및 가동하였다.

모건스탠리 임직원은 사고 당시 혼란스러운 상황 속에도 불구하고 대피 매뉴얼에 따라 계획을 이행하였으며, DR 시스템 가동 담당 임직원은 백업 센터로 이동하여 데이터를 성공적으로 복원, 72 시간만에 업무를 정상적으로 재개하였다.

2. (실패사례) 삼성 SDS 과천 전산센터 화재로 인한 삼성카드 업무 중단

대표적인 재해복구 실패 사례로는 삼성카드가 있다. 2014 년 발생한 삼성 SDS 과천 데이터센터 화재 사고로 해당 데이터센터를 사용하고 있었던 삼성 금융 계열사들의 IT 시스템 운영 및 일부 업무에 피해가 발생하게 되었다. 이에 삼성화재, 삼성증권 등 다른 계열사들은 발빠르게 업무를 정상화하였으나, 유일하게 삼성카드의 경우 온라인 결제서비스가 전면 중단되며 사고 발생 후 일주일까지 온라인 쇼핑몰 결제 시스템 다운으로 소비자에 서비스를 제공하지 못하였다.

삼성카드에서 공지한 사고 안내문


삼성카드에서 알려드립니다.

4월 20일 과천 삼성SDS센터 화재로 인해 14시 50분부터
홈페이지 접속, 온라인 결제 등 일부 서비스 이용이 제한되어
고객 분들께 불편함을 끼쳐 드린 점 머리 숙여 깊이 사과드립니다.
현재 서비스 복구를 위해 최선의 노력을 다하고 있으며,
서비스 이용 제한에 따른 고객 피해에 대해서는 보상을 추진하겠습니다.

현재 이용이 제한되고 있는 서비스

- 온라인 쇼핑몰 등 인터넷망을 이용한 카드 결제
- 삼성카드 홈페이지/앱을 이용한 모든 서비스
- 총 23개 체크카드 제휴 금융사 중 새마을금고, KB국민은행 등 18개 금융기관 제휴 체크카드 이용
- 총 27개 ATM/CD기 중 신한/대구/IBK기업은행 등 12개 금융기관에서의 현금서비스 이용
- 카드 결제 후 문자알림서비스

이번 시스템 장애로 인한 고객 및 결제 정보 유실, 유출은 없으며,
빠른 시간 내 복구할 수 있도록 최선을 다하겠습니다.
다시 한 번 고객 여러분들께 심려를 끼쳐 드린 점 사과 드립니다.

"당시 신한카드의 경우, 전산시스템 재해 시 10 분 이내에 승인 시스템이 복구되어 지도록 구축되어 있었다."

금융권은 금융감독원의 규제 하에 DR 시스템 구축에 대한 기준이 마련되어 있었으며, 특히나 실시간 결제시스템이 필수적인 카드 업계의 경우, IT 시스템 사고에 대비하여 지역을 두 곳 이상으로 분산하고 별도의 재해복구 시스템으로 IT 시스템을 운영하는 것이 일반적이기 때문에 삼성카드의 결제서비스 장애는 당시 사회적으로 상당한 화제로 소비자 및 업계의 많은 이슈를 야기하였다.

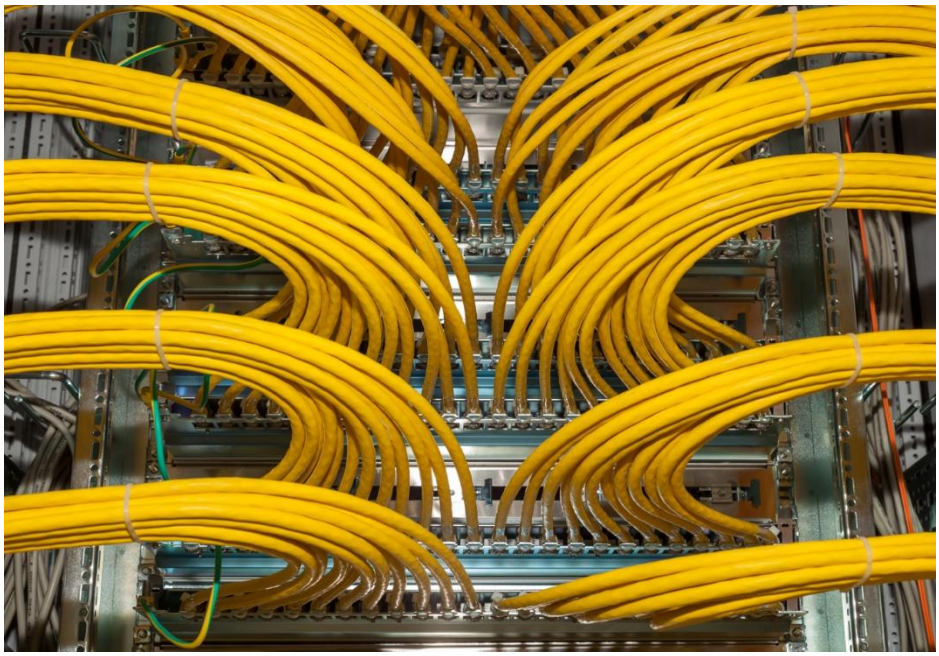
삼성카드는 왜 재해복구시스템은 성공적으로 가동하지 못하였을까?

① **비용적 측면의 부담**
- 대대적인 시스템 개편에 따른 비용 문제 부담
- 서비스 도입 기간 대비 적은 유지보수 횟수(비용 문제)

② **시스템 우선 순위 설정 미흡**
- 시스템 間 중요도/의존도 파악 미흡으로 인한, 결제서비스에 대한 DRS 가동 실패 (당시 수원 DR 센터가 있었음에도 결제서비스에 대한 재해복구시스템은 부재하였음)

그렇다면, 제대로 된 DR 시스템을 구축하려면 어떠한 사항들이 고려되어야 할까?

1. 재해복구(DR)시스템의 **RTO** 기산 시점을 명확하게 설정할 것
2. 재해복구(DR)시스템 가동기준에 대한 기준을 명확하게 설정할 것
3. 재해복구계획(DRP)에 대한 유지관리를 통해 자료의 최신화를 보장할 것
4. 시스템 **RTO** 산정 시 비즈니스(업무) 관점의 **RTO** 를 반드시 고려할 것
5. 정보자산 도입~폐기의 전체 **Life Cycle** 관점에서 재해복구시스템을 고려할 것



1. 재해복구(DR)시스템의 RTO 기산 시점을 명확하게 설정할 것

RTO(Recovery Time Objective)란 '복구목표시간'으로 시스템 또는 업무에 장애가 발생하여 중단될 경우, 목표로 하는 재가동 시점까지의 시간을 말한다. 예를 들어, A 라는 업무가 6 시간 이상 중단되어 회사에 심각한 영향을 미칠 경우, 회사는 A 와 관련된 업무 시스템이 중단되는 상황을 가정하여 '6 시간'이내로 복구하는 목표 시간을 설정하면 된다. (RTO 설정 시 전사 시스템에 대한 중요도를 상호 비교 고려하여, 각 시스템의 '최대중단허용기간(MTPD)[1]' 내 차등적으로 RTO 를 설정하면 된다.)

[1] MTPD(Maximum Tolerable Period of Disruption)란?

해당 서비스의 중단을 회사에서 허용할 수 있는 최대 기간을 말한다.

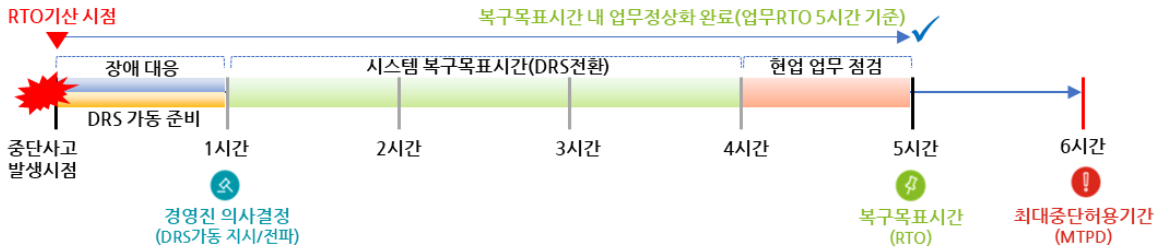
우선 설명을 위해 A 라는 업무는 RTO 가 5 시간이며 관련 업무시스템의 RTO 를 3 시간으로 설정하였다고 가정하였을 때, 기업은 반드시 RTO 의 시작 시점을 명확하게 고려하여야 할 필요가 있다. 그것은 바로 'RTO 의 기산시점' 이다. 대부분의 기업은 장애가 발생하였을 때 RTO 이내에 해당 시스템을 복구하겠다는 막연한 복구계획을 세우고 있다. 하지만 정작 대부분 IT 담당자는 RTO 이내에 해당 시스템 또는 업무를 복구하기 위한 세부 기준인 '출발점'을 설정하는 것을 간과한다. 이 부분은 현업 업무담당자와 IT 시스템 담당자와의 RTO 시작 시점의 인식차이에서 비롯된다.

즉, RTO 의 기산시점('출발점')은 하기와 같이 두가지 기준이 존재할 수 있다.

---

① 'RTO 기산 시점 = 시스템 또는 업무 중단 시점'

- 시스템이 중단된 시점부터 즉시 재해복구(DR) 준비를 시작하는 것을 의미한다.



---

② '기업의 C-Level 의 의사결정이 내려진 시점 = RTO 기산 시점'

- 기업의 경영진 또는 임원의 재난선포(지시 전파) 시점부터 재해복구(DR) 준비를 시작하는 것을 의미한다.

A 라는 업무의 복구에 소요되는 시간이 5 시간이라고 가정하였을 때, ①번 '시스템 또는 업무 중단 시점부터' 즉시 복구하는 경우, RTO 내 해당 시스템을 충분히 복구할 수 있다. 하지만, ②번 'RTO 기산 시점 = 기업의 C-Level 의 의사결정이 내려진 시점부터' 복구를 시작하는 경우, 경영진 의사결정에 소요된 1 시간 이후부터 재해복구(DR)시스템 가동 준비를 하여 업무 RTO 5 시간을 넘기고 서야 겨우 해당 시스템을 복구할 수 있게 된다.

현실적으로 기업은 경영진의 의사결정이 내려진 후에야 비로소 재해복구(DR) 시스템을 가동할 수 있는 경우가 많다. 재해복구(DR)시스템은 대게 막대한 비용이 투자되고, 기업의 사활이 걸려져 있는 상황에 가동되는 경우가 많기 때문에, 경영진의 의사결정이 없는

상황에서 판단에 따라 시스템을 즉각 가동시키기에는 복원에 대한 Risk 를 감당해야하는 부담감이 적지 않을 것이다. 따라서, 업무 RTO 를 설정할 때에는 RTO 기산시점을 명확화하고, 경영진의 의사결정에 필요한 일정 시간을 고려하여 시스템 RTO 를 설정할 필요가 있다.

2. 재해복구(DR)시스템 가동기준에 대한 기준을 명확하게 설정할 것

비상상황 발생 시, 기업이 가장 필요로 하는 것은 시기 적절한 의사결정일 것이다. 기업이 어떠한 상황에서 어떤 유형의 재난·재해를 맞닥뜨리게 될지는 사전에 알 수 있는 방법이 없다. 이러한 불확실성 때문에 기업은 늘 예상하지 못한 사건/사고에 직면하고 있으며, 내부 뿐만 아니라 외부 Risk 에 대해서도 직/간접적으로 모니터링해야 한다. 경영진 또한 이러한 상황에 대비하여 리스크 관리 체계를 마련하고 IT 관점에서는 재해복구체계에 투자하는 것이 중요하다.

기업이 IT 중대 장애 등의 비상상황 시, 신속하게 업무 또는 서비스를 복구하기 위해서는 반드시 재해복구시스템의 가동 기준을 사전에 정의하고 있어야 할 것이며, 누가, 언제, 어느 시점에서, 어떻게 상황을 전파하고 DR 시스템을 가동시킬 것인지 구체적으로 계획 및 문서화할 필요가 있다.

여기서 중요한 것은 기존의 장애대응 체계와 재해복구(DR)시스템 가동 기준을 명확히 이해하고 구분하여 정의되어야 한다는 것이다. 즉, 사고의 영향도 및 심각도를 고려하지 않고 기존의 장애등급 및 장애 처리 프로세스에 따라 장애를 처리하는 경우 적절한 재해복구(DR) 가동 시점을 놓칠 수 있다. 따라서 이벤트를 발견하고 초기에 확인한 실무자 입장의 장애 등급 판단과 위기 상황의 대응과 책임을 담당하는 관리자(의사결정권자)의 입장에서 영향도, 심각도, 중단 예상시간이 고려된 사고등급은 장애 등급과 다르게 판단될 수 있다는 것을 반드시 고려해야 한다.

[IT 상황전파 및 사고보고 보고기준 예시]

<table>
<tr><th rowspan="2">사고 등급</th><th colspan="2">Escalation</th><th rowspan="2">고려사항</th><th rowspan="2">DR 가동 여부</th></tr>
<tr><th>보고라인</th><th>시기</th></tr>
<tr><td>1 등급</td><td>• 당직자(OP) → IT 실무 담당자 & IT 센터장
• IT 센터장 → CIO & CEO</td><td rowspan="2">즉시 보고</td><td>• 신속한 상황전파 고려 보고 단계 최소화</td><td>즉시 가동</td></tr>
<tr><td>2 등급</td><td>• 당직자(OP) → IT 실무 담당자 → IT 센터장 → CIO</td><td>• 1 등급 상향 가능성 고려, 선제적 DR 가동 대기</td><td>필요시 가동
(부분적 가동)</td></tr>
<tr><td>3 등급</td><td>• 당직자(OP) → IT 실무 담당자 → IT 센터장</td><td>정기적 보고</td><td>• 1/2 등급으로 상황 변화를 대비, 상황 종료시까지 지속적 모니터링 실시</td><td>-</td></tr>
<tr><td>4 등급</td><td>• 당직자(OP) → IT 실무 담당자</td><td>정기적 보고</td><td>• 예방적/주기적 모니터링 시행</td><td>-</td></tr>
</table>

※ 1 등급의 경우 당직자(OP)가 외주 인력인 경우 "IT 실무 담당자"가 상황전파 실시

3. 재해복구계획(DRP[2])에 대한 유지관리를 통해 자료의 최신화를 보장할 것

기업이 재해복구(DR)체계에 대한 매뉴얼인 IT-BCP 및 DR 절차서 또는 지침 등을 보유하고 있다면, 문서관리 지침에 따른 주기적인 유지관리를 통해 매뉴얼 또는 지침 등의 최신화를 보장하여야 할 것이다.

뿐만 아니라, DR 가동 관련 유관부서에서는 DR 가동에 필요한 제 3 자(벤더사 및 협력사 등)에 대한 인력 Pool 및 비상연락망 등을 현행화하고 체계적으로 관리하여, 어느 상황에서나 필요한 경우 필요 인력에 연락을 취해 조치를 취할 수 있도록 대비하여야 할 것이다.

[2] DRP(Disaster Recovery Plan)란?

재해 발생 시 정해진 업무 복구 순서에 따라 정보시스템을 체계적으로 복구하도록 수립한 절차를 말한다.

4. 시스템 RTO 산정 시 비즈니스 관점의 RTO 를 반드시 고려할 것

기업은 기업의 '비즈니스 연속성관리'와 'IT 연속성관리'를 별개가 아닌, 상호 연계하여 재난·재해에 대한 계획과 전략을 수립하여야 할 것이다.

예시로, B 은행이 비즈니스 관점의 BCM 체계 수립 시, 재난·재해에 상황 속에서도 3 시간 이내에 '이상금융거래 탐지' 업무를 수행해야 한다고 설정하였다면, 해당 업무를 수행하기 위한 필수자원을 식별할 때, 사용하는 IT System 을 함께 식별하여야 할 것이다.

또한, B 은행의 IT 연속성관리체계 점검을 통해, 해당 업무에 필요한 '이상금융거래 탐지시스템(FDS; Fraud Detection System)'에 대한 DR 시스템이 구축되어 있는지 확인하여야 할 것이며, 해당 시스템이 3 시간 이내에 복구될 수 있는지 여부를 확인하여 비즈니스 관점의 RTO 와 시스템 관점의 RTO 를 일치시켜야 할 것이다.

5. 정보자산 도입~폐기의 전체 Life Cycle 관점에서 재해복구시스템을 고려할 것

기업은 IT 시스템 설계 시, 초기 단계에서부터 해당 시스템의 기능을 세부적으로 분석하여 중요도를 측정해야 할 필요가 있다.

예를 들어 시스템 개발을 동반한 신규 업무가 발생하여 업무영향분석(BIA; Business impact Analysis)를 통해 해당 업무의 RTO 가 1 시간으로 중요도가 매우 높은 업무로 선정되었다면, 시스템 개발 이후 정보자산의 도입 시 재해복구 수준을 업무 RTO 를 고려하여 1 시간 이내에 복구할 수 있는 DR 시스템을 도입해야 한다.

대부분의 기업은 비즈니스 관점에서의 RTO 요구사항과는 별도로 IT 운영관점의 서비스 효율화로 인해 당장의 IT 인프라 운영관점의 편리성(백업, 소산, 인력, 예산 제약 등)에 따라 각 업무시스템의 재해복구시스템의 도입을 미루거나 추후 일괄적으로 도입 진행하는 경우가 대부분이다. 이는 재해 시 재해복구시스템의 실패 가능성을 높이는 대표적인 Risk 이며, 재해복구시스템의 성공 가능성을 높이기 위해서는 정보자산 도입 초반부터 재해복구시스템을 함께 설계되어야 하고 나아가 업무 부서의 요구 사항이 재해복구 시스템 관련 정보자산 도입과 연계 되어 정보자산 도입~폐기의 전체 Life Cycle 에 반영되어 운영되어야 한다. 최근에는 많은 기업들이 클라우드를 도입하면서 운영 인프라에 대한

관리를 조금 더 유연성 있게 할 수 있으므로 비즈니스 단의 업무 중요도에 맞춰서 재해복구시스템도 민첩하게 효율화 하여 관리가 가능할 것이다.

결론

DR 시스템 구축은 형식적인 구축·운영과 훈련에 그쳐 실제 적용하지 못하는 경우가 적지 않다. 따라서, 실제 재난 등의 위기 발생 시, 기업의 운영체계가 연속성을 갖지 못하는 상황이 초래될 가능성이 높다.

국내 금융업, 제조업 할 것 없이 DR 시스템의 구축이 필수적으로 요구되고 있는 오늘날, 효과적인 재난·재해 대응을 위하여 기업은 DR 시스템에 구축과 더불어 BCM 체계 구축에 대해 긍정적으로 검토해 보아야 한다. DR 시스템 및 BCM 체계를 기 구축하고 있는 기업의 경우, 실질적인 운용 효과 및 효율성을 위하여 전체 체계에 대한 대대적인 점검이 필요할 것으로 보인다.

[Reference]

- 금융기관 재해복구센터 구축 권고안, 금융감독원

- BCP 모범규준, 금융감독원

- (기사) 삼성 SDS-삼성카드, 수백억 피해보상 어떻게 될까?, 미디어펜, 2015.01.12