Engineered Resilient Systems

About me.

현병욱 Byungwook Hyeon

- 소속 : 보안IDC운영팀 매니지드서비스유닛 (인턴)
- 이력 :

2009. 03 - 2012. 02 : 창동고등학교 졸업
2015. 02 - 2019. 02 : 청주대학교 컴퓨터정보공학과 학사 (중퇴)
2016. 01 - 2017. 10 : 705특공연대 3지역대 특공병, 병장 만기 전역
2019. 03 - 2021. 08 : 한양대학교 ERICA 소프트웨어학부 학사 (편입, 졸업예정)
2019. 04 - 2019. 04 : (주)마켓디자이너스(튜터링) 컨설팅 참여
2019. 03 - 2019. 06 : (주)대양엔바이오 박종운 대표 인터뷰 및 기업진단
2019. 09 - 2020. 06 : 클라우드 네이티브 컴퓨팅 플랫폼 개발 With KTds Architecture CoE팀
2020. 01 - 2020. 12 : NKInfinite 고등부 수학 강사
2020. 09 - 2020. 12 : 호텔정보시스템(PMS) 개발 프로젝트, Agora
2020. 10 - 2020. 12 : 대한민국 증권 시장에서 거래되는 주식에 대한 R기반 리스크 측도 및 평균 수익률 분석 프로젝트
2020. 11 - 2020. 12 : 콜옵션 소유자와 발행자 각각의 거래일에 대한 R기반 현금 흐름 및 만기 수익 분석 프로젝트
2021. 01 - 2021. 03 : 2020 가비아 동계 인턴십 SE부문, 매니지드서비스유닛 인턴
2021. 02 - : 가상 창업 프로세스 기반 ‘우리동네 이야기 - 우동’ 프로젝트 PM, CoreSW 부문장

Table of Contents

Preface

Resilience 프로젝트는 IDC의 기초이자 핵심인 resilience를 이해함으로써 업무 적응도 향상과 IDC 목적성을 확고히 하고자 보안IDC운영팀 Ryan 이사님의 제안으로 시작되었습니다. 이를 위해 Resilience, Dyanamic resilience 정의와 더불어 Resilience for IDC를 통해 IDC의 미래를 예측하는데 의의를 두고 있습니다.

이 교본은 전적으로 가비아IDC에 중점을 두고 작성된 것임을 참고해주시길 바라며, 조금이나마 가비아의 미래에 도움이 되길 바랍니다.

저자. 현병욱

Chapter 1.
Resilience Definition

Resilience

“Resilience”를 Cambridge Dictionary에서는 다음과 같이 정의한다.

- The quality of being able to return quickly to a previous good condition after problems.
- The ability of a substance to return to its usual shape after being bent, stretched, or pressed.

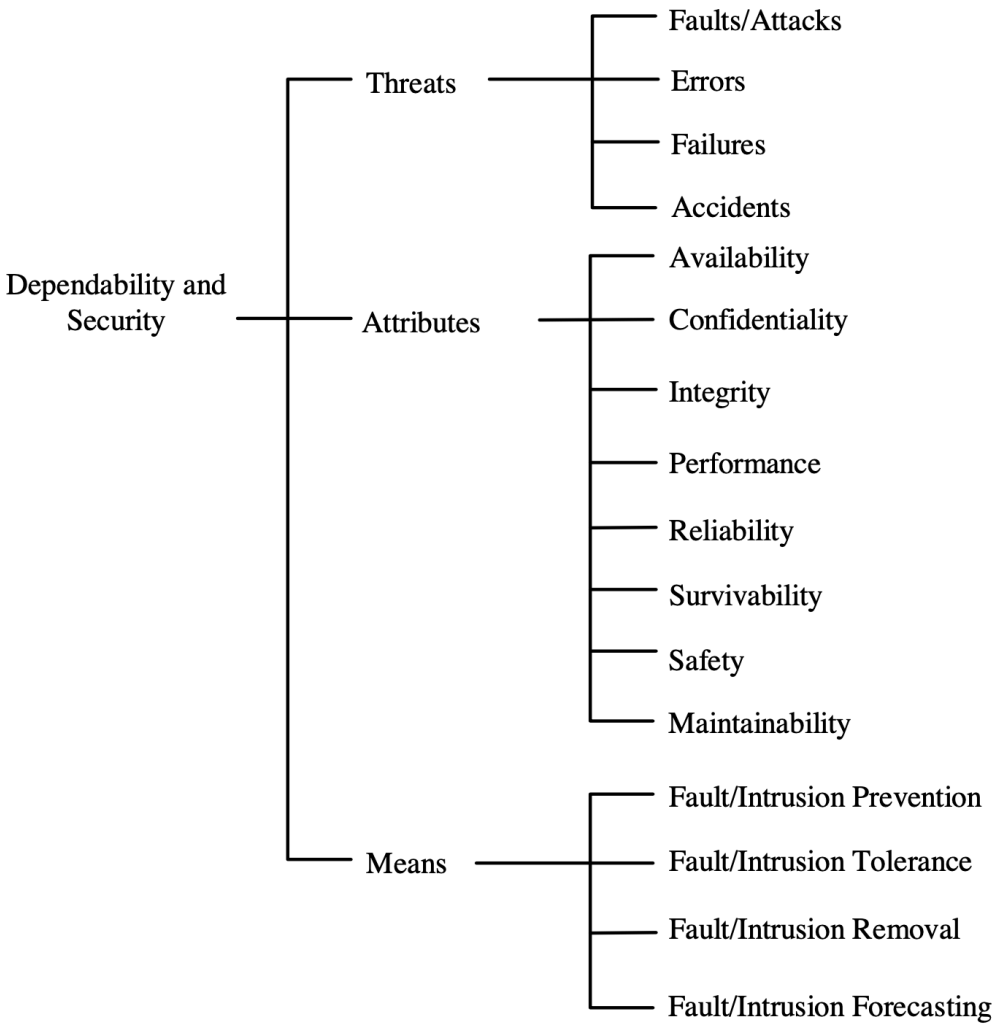
즉, 사람이나 사물이 외부의 개입(혹은 충격)으로인해 기존과 다른 상태에 도달했을 때 원래의 상태로 되돌아올 수 있는 능력이다. 다음 그림을 참고하면 이해하기 더 쉬울 것이다.

< 도미노 : 외부 개입 / 사람 : Resilience >

Network Resilience

이전 페이지에서 확인했듯이 resilience는 외부의 충격이나 개입으로인해 기존의 안정적인 상태에서 변화가 발생했을때 원래의 상태로 되돌아오는 능력, 즉 회복할 수 있는 능력을 의미한다. 그렇다면 resilience를 컴퓨터 환경에 적용한다면 어떻게 설명할 수 있을까?

본론에 들어가기에 앞서 컴퓨터 환경에서 발생할 수 있는 위협을 간략하게 정리한 다음 그림을 통해 전반적인 로드맵을 그려보길 추천한다.



첫 번째로 “Network Resilience”에 대해서 알아보자. “Network Resilience”를 Wikipedia에서는 다음과 같이 정의하고 있다.

- In computer networking, resilience is the ability to “provide and maintain an acceptable level of service in the face of faults and challenges to normal operation.”

즉, 장애나 문제로부터 서비스가 정상 운영될 수 있도록 유지하는 능력을 의미한다.

사전적 정의가 아닌 서비스 중심적으로 분석하게되면 “Network Resilience”는 서비스 운영 체계에 있어서 가장 핵심인 “사용자(고객) 중심”이라고 정의할 수 있다. 서비스의 연결성은 서비스 제공자가 운영하는 서비스를 사용자(고객)가 1차적으로 평가할 수 있기 때문이다. 예를들어 서버의 config 값이 잘못 설정되어 있는 소프트웨어 문

제나, 통신을 관장하는 서버나 스위치 단의 문제와 같은 하드웨어 문제로 인해 서비스 운영에 network 장애가 발생해서 고객이 서비스를 이용하는데 불편함을 경험하게된다면 이는 서비스 제공자의 수익 감소와 직결되는 중대한 문제가 될 것이다. 이로 인해서 통신 네트워크가 인프라 운영의 핵심 기본 구성 요소가 되면서 network resilience의 중요성은 지속적으로 증가하고 있다.

물론, Network Resilience를 구성하는데 있어서 network 독립적으로 운영 및 관리가 필요한 것은 아니다. 이후에 언급하게 될 Security, System과 연계된 체계가 확립되야 Network Resilience를 구성할 수 있는 것이다. Network를 먼저 언급한 이유는 사용자 입장에서 1차적(가시적)으로 불편을 겪을 수 있는 부분이 network 장애이기 때문이다. 이와 관련해서는 이 장의 마지막에 다시 언급하도록 한다.

Security Resilience

“Security Resilience”를 Wikipedia에서는 “Cyber Resilience”로 다음과 같이 정의하고 있다.

- Cyber resilience refers to an entity’s ability continuously deliver the intended outcome, despite adverse cyber events.

즉, TCP ACK Flooding과 같은 Dos 계열이나 이와 유사한 외부 개입이나 충격이 발생하더라도 서비스나 시스템이 정상 운영될 수 있도록 유지하는 능력을 의미한다.

Security resilience를 조금 더 쉽게 이해하기 위해서 담벼락을 예로 들어보자. Security에서의 resilience는 농장에서 외부인이나 야생동물의 유입을 차단하기 위해 담벼락을 세우는 것과 같다. 담벼락을 세운다고해서 외부로부터의 유입을 100% 차단시킬 수 있다는 보장은 없다. 하지만 외부로부터의 유입이 발생한다고해서 농장의 기능이 멈추는 것도 아니다. 농장 주인이 침입자를 조기에 발견하여 조치한다면 농장에 어떠한 피해도 발생하지 않을 것이다. 또한, 침입자를 조기에 발견하지 못했다 하더라도 침입자의 규모, 목적, 특징 등의 요인에 따라 농장의 피해 정도가 달라질 것이다.

위에서 예시로 들었던 농장 사례를 서비스 중심적으로 분석하게되면 “Security Resilience”는 서비스 운영 체계에 있어서 “서비스 운용자(제공사) 중심”이라고 정의할 수 있다. Security resilience는 network resilience와 다르게 고객의 입장에서 인지하기 쉽지 않다. 보안상의 이슈가 발생했다 하더라도 critical한 수준의 문제가 아니라면 서비스 사용에 있어서 가시적으로 나타나지 않기 때문이다. 이러한 이유로 security resilience는 서비스 운용자 입장에서 고객의 개인 정보와 서비스의 안정화를 목표로 하는 것을 핵심 목표로 갖는 것이다.

System Resilience

“System Resilience”를 Wikipedia에서는 “Robustness”로 다음과 같이 정의하고 있다.

- In computer science, robustness is the ability of a computer system to cope with error during execution and cope with erroneous input.

해당 내용을 이해하기 위해서는 “System”의 정의를 먼저 이해할 필요가 있다. System은 흔히 컴퓨터 동작에 필요한 내부 system으로 정의 되기도 한다. 하지만, 이는 일부분으로 묘사된 것일 뿐이지 실제로는 서비스 운용을 목적으로 조직화된 모든 요소들의 집합체이다. 시스템의 대표적인 요소로는 하드웨어, 운영체제, 소프트웨어, 프로그램, 파일 등이 있다.

System의 정의를 이해했다면 Wikipedia에서 정의한 “Robustness”를 이해하기 수월할 것이다. System resilience는 서비스 운용에 필요한 system에 영향을 미칠 수 있는 장애로부터 견딜 수 있는 능력이다. 이를 서비스 중심적으로 분석하게되면 system resilience는 앞서서 배운 사용자(고객) 중심인 network resilience와 서비스 운용자(제공자) 중심인 security resilience의 통합이라고 생각하면 된다. Network resilience를 설명하면서 network resilience를 구성하는데 있어서 network 독립적으로 운영 및 관리가 필요한 것이 아니라는 말을 남긴적이 있다. 이와 연관된 것이 바로 system resilience이다. 앞서 말한 바와 같이 system resilience는 서비스 운용을 위한 공통의 목적으로 조직화된 모든 요소들의 집합이다. 따라서 network, security 또한 system resilience에 영향을 줄 수 있는 요소이다.

IDC Resilience

“IDC Resilience”는 Wikipedia에서 직접적으로 정의하고 있지 않지만, 한마디로 “Fault Tolerant System”이라고 할 수 있다. IDC의 정의 자체가 서버 컴퓨터를 한 장소에 모아 안정적으로 1년 365일 중단없는 서비스 관리 목적의 인터넷 데이터 센터인만큼, downtime 발생이 최소화되어야 한다. 이 과정이 바로 IDC Resilience이다. 이를 위해 IDC에서는 *HA와 *DR의 구축 및 zenius와 같은 통합 관리 모니터링 플랫폼을 통해 보안 관제 및 모니터링 지원으로 resilience 달성을 꾀하고있다.

이론상으로 보면 HA 구축으로 99.999%의 가용성인 “Five Nines” 달성으로 연간 downtime을 5분 26초 이하로 유지할 수 있다. 그럼에도 모든 서버에 five nines를 적용시키는데는 한계가 있다. 바로 ‘비용’ 때문이다. 이로 인해서 관련 업계에서는 안정적이고 효율적인 인프라를 구축하는 방법은 아주 간단하다고 말한다. 바로 ‘돈’만 있으면 되기 때문이다. 이러한 이유로 서버를 운영하는 기업들은 한정적인 자원 속에서 최고의 효율을 낼 수 있는 인프라 환경을 모색한다.

* HA : High Availability * DR : Disaster Recovery

사실 모든 서버가 five nines를 필요로 하지는 않는다. 산업 분야, 기업 규모, 기업 수익구조에 부합하는 인프라를 구축하면 된다. 이를 위해 가비아에서는 '매니지드 서비스'를 통해 컨설팅 서비스를 제공하고 있다. 컨설팅을 통해 고객 비즈니스에 최적화된 인프라 구축 및 점검을 받을 수 있다.

Dynamic Resilience

"Dynamic Resilience"를 이해하기 위해서는 "Dynamic"의 정의를 먼저 이해할 필요가 있다. "Dynamic"을 Cambridge Dictionary에서 다음과 같이 정의하고있다.

- Continuously changing or developing
- Relating to forces that produce movement

즉, 특정 상황에서 사람이나 물건의 움직임을 촉진시키는 힘에의해 지속적인 변화가 발생하는 경우를 의미한다.

이를 통해 "Dynamic Resilience"를 "외부 개입이나 충격으로부터 현 상태를 유지하기 위한 선제적인 혹은 지속적인 조치"라고 정의할 수 있다. 외부 개입에 의해 변경된 상태로부터 기존의 상태로 되돌아 오는 Resilience의 성질과 dynamic의 지속성에 의해 "선제 조치"의 의미가 포함된 것이다.

Dynamic Resilience의 대표적인 선제 조치 방안은 '휴먼 에러 방지'이다. 휴먼 에러 방지의 대표주자인 'Fat-Finger Error'를 예로 들어보자. Fat-finger error의 원인은 크게 2가지 측면으로 나뉜다. 바로 '인적 측면'과 '시스템 측면'이다. 인적 측면은 단어 그대로 사람으로 인해서 발생하는 에러를 의미한다. 이는 책임자의 의무 태만, 근무자의 도덕적 해이에 의해서 발생하게 된다. 이러한 에러는 IDC 근무자가 가장 기피해야 할 에러이지만, 생각보다 빈번히 발생하는 에러로 뽑힌다. 어떻게 보면 너무나도 간단히 방지할 수 있는 에러인데, 도대체 왜 인적 측면의 에러가 수시로 발생하는 것일까? 바로 근무자의 '책임감 부족' 때문이다. 즉, 고객사의 서버를 자신의 것이 아닌 타인의 것으로 가볍게 여기기 때문이다.

실제로 가비아 SE로 근무하면서 인적 측면 에러를 목격한 경험이 있다. 폴더를 삭제하는 과정에서 잘못된 경로의 명령어를 입력하여 고객사의 root 디렉토리가 삭제된 경우였다. 이는 전적으로 근무자의 책임감 부족으로 인해 발생한 경우이다. 이러한 사례는 시스템 수준에서 방지하기가 쉽지 않다. 즉, 근무자 수준에서 방지하는 방법이 최선이라는 말인 것이다. 이를 방지하기 위해서 근무자는 다음과 같은 생각을 항상 품고 있어야 할 것이다.

첫 번째, "고객의 서버는 타인의 것이 아닌 내 자신의 것이다."

- 인간은 본디 이기적인 측면을 갖고 태어난다. 남의 것이 피해보는 것은 지나칠 수 있지만 자신의 것이 피해보는 것은 지나치지 않는다는 것이다. 당장 자신의 사무실 주변에 존재하는 비품들을 둘러봐라. 볼펜, 전화, 책상, 냉장고 등만 봐도 관리는 커녕 먼지가 수북히 쌓여 있을 것이다. 내 물건이 아닌 회사의 물건이라고 여겨왔기 때문이다. 지금까지 사소하게 여겨왔던 물건이겠지만, 사소한 물건조차 관리하지 못하면서 고객사의 서버를 제대로 관리할 수 있을 것인가에 대해서 고민해볼 필요가 있다.

두 번째, “사람은 완벽하지 않다.”
- 인간은 완벽한 존재가 아니다. 이를 인간 스스로 인지하고 창조해낸 것이 바로 ‘컴퓨터’이다. 인간은 컴퓨터처럼 정해진 명령어에만 따라서 동작하는 대상이 아니다. 정해진 상황에 맞춰서 사고하는 능력에 따라서 행동하는 존재이다. 따라서 자신이 하는 행동에 지속적으로 의심하는 습관을 들여야 한다. 물론, 자신의 능력과 행동에 자신감을 가지지 말라는 것이 아니다. 단지, 명령어를 입력하거나 구상하는 단계에 있어서 이중, 삼중으로 검토할 필요가 있다는 것이다.

시스템 측면의 에러는 관리 시스템 미비로 인해 발생하는 에러이다. 모니터링 인프라 미비, 운영 시스템의 불안정성 등의 이유로 발생하는 것이다. 이를 듣고 혹자는 이러한 생각을 가질 수 있다. “휴먼 에러의 한가지 측면이라면서 시스템의 불안정성으로 인해 발생하는 에러라면 휴먼 에러가 아닌거 아닌가?”. 하지만 이는 전적으로 잘못된 생각이다. 컴퓨터에 구성되는 시스템은 컴퓨터 스스로 구축하는 것이 아니라 사람의 선택에 따라서 구축되는 것이기 때문이다. 따라서 자연적으로 발생되는 시스템의 문제가 아닌 방지 차원에서의 문제는 전적으로 사람으로 인해 발생하는 에러인 것이다.

시스템 측면의 에러를 방지하는 방법은 크게 어렵지 않다. 모니터링 체계에 감지된 내역에 대한 즉각적인 공유와 해당 내역에 대한 이중, 삼중 크로스 체크가 체계가 확립되면 되기 때문이다. 쉽게 말해, 시스템에 대한 전적인 신뢰가 아닌 여러 사람들이 보유하고있는 지식의 공유가 이루어지면 되는 것이다.

장비 스스로 발생하게되는 대부분의 물리적인 혹은 소프트웨어로 인한 장애는 critical하지 않다. 일반적으로 단기간 내에 처리가 가능하기 때문이다. 하지만 사람으로부터 발생된 에러는 고객에게 critical한 피해를 줄 수 있고, 이로 인해서 고객과 체결된 SLA에 치명적인 결과를 가져올 수 있다. 이로 인해서 IDC 근무자들에게 교육하는 핵심이 ‘휴먼 에러 방지’인 것이다.

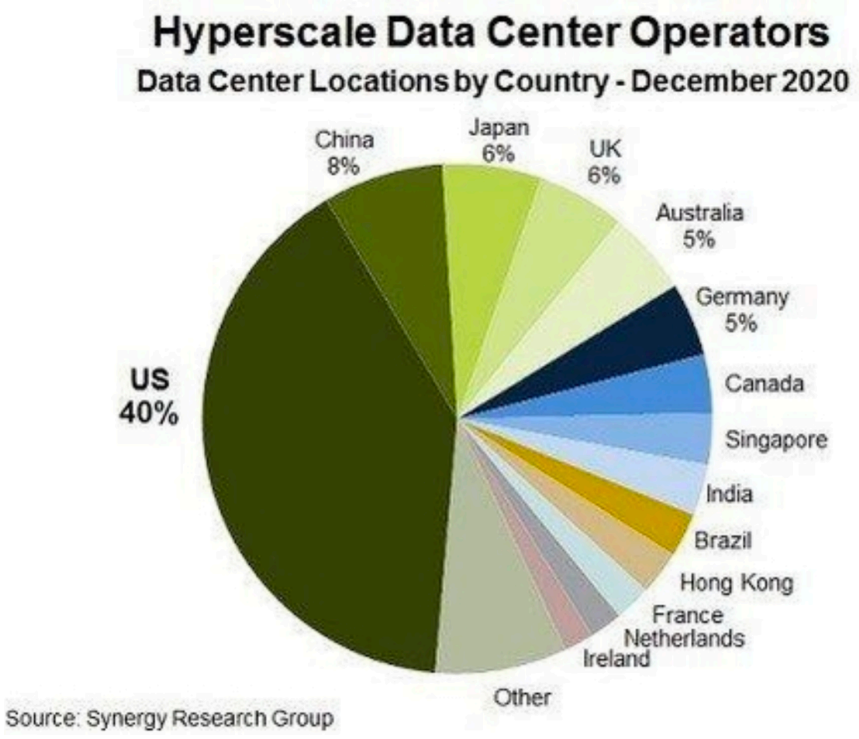
* RTO : Recovery Time Objective

Chapter 2.
Resilience for IDC

이번 장에서는 “Resilience for IDC”를 사업적으로 분석해보고자 한다. Network, Security, System를 제외한 Resilience for IDC에 대해서만 다루는 이유는 이들 모두가 독립적인 것이 아니라 서로 관계를 맺고 있으며, IDC는 network, security, system의 종합체로 전체를 아우를 수 있기 때문이다. 이번 장을 통해 Resilience for IDC에 대한 정의와 적용 방안에 대해 이해하고 IDC의 미래를 예측해볼 수 있기를 바란다.

이전 장에서 언급했듯이, resilience는 외부에서 가해지는 힘이나 충격으로부터 원 상태로 복원하는 능력을 의미한다. 그렇다면, 가비아IDC를 기준으로 외부에서 가해지는 힘이나 충격에는 어떤 것이 있을까?

본론에 들어가기에 앞서 전세계 데이터센터 동향에 대해서 파악해보도록 하자.



전세계 데이터센터는 2021년 2월 기준 미국 39%, 중국 10%, 일본 6%, 기타 45%의 비중을 갖고 있으며, 세부적으로는 미국 2,653개, 영국 451개, 독일 442개, 캐나다 279개, 네덜란드 274개, 호주 272개, 프랑스 248개, 일본 199개의 분포를 나타내고 있다. 그 중에서 주목해야 할 부분은 한국이다. 한국은 아직까지는 데이터센터 산업에 있어서 이렇다 할 영향력을 미치지 못하고 있다. 하지만, 한국은 현재 세계 5위의 데이터 생산국으로, 이는 가공 대상의 수많은 데이터를 보유하고는 있지만, 이를 보관할 데이터센터는 부족하다는 의미를 갖는다. 이를 수많은 기업들이 인지하고 한국으로의 데이터센터 진출에 나서고 있다. 대표적으로 AWS, Azure, Oracle, Naver, Kakao 등이 있다. AWS는 클라우드에서 기밀 데이터 호스팅 인증을 받은 몇 안되는 회사중에 하나이다. 이를 통해 AWS는 'AWS Secret Region' 운용을 통해 미 정부 대상으로 'GovCloud Region'을 제공하는 등 공공 인프라 클라우드 구축에 열을 올리고 있다. 이러한 AWS는 한국 진출 취소를 번복하고 현재는 Seoul region을 구축하여 데이터 센터를 운영중에 있다. 또한, Oracle은 서울, 춘천에 데이터센터를 개소하여 'Business Consistency'와 'Immediate Disaster Recovery' 체계를 구축하고 있다. 이 외에도 IBM, MS 등의 글로벌 산업군 리드 기업들의 적극적인 한국행이 단행되고 있다. 이러한 흐름에 발맞춰 한국 기업들도 데이터센터 구축에 대규모 투자를 단행하고 있다는 것이다. 네이버는 춘천 데이터센터와 더불어 2023년까지 세종에 하이퍼스케일 규모의 데이터센터 '각 세종' 건립을 추진중에 있으며, 카카오 또한 안산시 한양대 캠퍼스에 하이퍼스케일 규모의 IDC 건립을 추진중에 있다.

이러한 기업들의 대규모 투자를 보고 혹자는 이러한 생각을 하기도 한다. "데이터센터가 미래 먹거리구나!". 하지만 이는 산업군의 흐름을 제대로 읽지 못한 경우이다. 오늘날의 데이터센터는 단순히 데이터를 보관하는 이전의 데이터센터와 다르다. 2025년까지 클라우드와 따로 노는 데이터센터는 사라진다는 뉴타닉스 클라우드인덱스 보고서가 있다. 이 보고서에 따르면 국내 기업들은 클라우드 미지원 데이터센터를 처분하거나 클라우드 통합을 고려하고 있다는 내용이 포함되어있다. 이 사실을 통해 우리는 한 가지 사실을 알 수 있다. "클라우드와 데이터센터는 떼려야 뗄 수 없는 관계이다."

이정도면 가비아IDC 기준의 외부에서 가해지는 힘이나 충격에 대해서 어느정도 눈치챘으리라 생각된다. 그렇다. 바로, 선제적인 대규모 투자를 단행중인 기업들이다. 가비아는 과천 신규 사옥 설립 추진과 동시에 독자적인 데이터센터 건립을 추진중에 있다. 하지만 AWS, 네이버 등의 기업과 비교했을때 규모적인 측면에서 가비아는 확연히 뒤쳐지게된다. 그렇다면 가비아는 어떻게 해야 미래 데이터센터 산업군에서 살아남을 수 있을것인가. 저자는 그 해답으로 '계열사 분할'을 제안하고자 한다. 현재 가비아 연간 수익의 약 40% 이상이 IDC에서 발생하고있다. 이는 가비아 입장에서의 보안IDC운영팀은 수익구조에 있어서 지나치게 한 분야로 치중된 사업부이며, 보안IDC운영팀 입장에서는 독자 생존 가능한 수익구조를 갖는 사업부라는 의미를 내포하고있다. 여기서의 문제는 가비아는 미래먹거리로 클라우드를 채택하고 있다는 점이다. 물론, 이전에 언급했던 바와 같이 클라우드와 데이터센터는 떼려야 뗄 수 없는 관계를 갖고 있다. 하지만, 지나치게 한쪽으로 치우친 수익구조는 가비아의 클라우드 집중 투자에 제한된다. 즉, R&D와 더불어 인적자원 확보에도 비상이 걸린다는 말이다. 이러한 상황을 타개하기위해 가비아는 LG화학과 LG에너지솔루션처럼 보안IDC운영팀을 독자 법인으로하는 계열사 분할을 단행해야 한다. 계열사 분할을 통해 가비아가 얻게되는 이점은 다음과 같다.

첫 번째, 미래 먹거리 확보 경쟁력 확보가 가능하다.

- 미래 먹거리는 당연히 '클라우드 산업'이다. 특히, 가비아의 사업관과 일치하는 '공공클라우드 산업'은 가비아가 반드시 확보해야 할 산업군이다. 가비아는 공격적인 시장 확보가 아닌 안정적 확장 전략을 채택하고있다. 클라우드 산업의 큰 파이를 차지하는 기업 대상 클라우드는 경쟁이 치열하다. 물론, 공공 기관 클라우드 경쟁도 치열한건 마찬가지이지만, CSAP 등의 인증 체계가 경쟁 참여 필수 자격 요건인 만큼 시장 참여 문턱이 높다는 특징이 있다. 가비아는 이미 CSAP 인증을 받은 기업으로, 공공클라우드 분야에 있어서는 선두 그룹에 포함된다고 할 수 있다. 이를 무기로 보안IDC운영팀의 계열사 분할을 통해 가비아는 기존 IDC운영 경험을 토대로 클라우드 개발에 전념하여 공공클라우드 확보를 통한 안정적인 고정 수익 만들기에 전념할 수 있게 된다. 또한, 클라우드 운영에 필요한 데이터 센터를 타사가 아닌 자사 계열사의 IDC로 채택함으로써 대외적인 보안 신뢰도를 구축할 수 있다.

두 번째, 양방향 기업 규모 확장이 가능하다.

- 보안IDC운영팀은 고정 수익 창출과 더불어 안정적인 수익 확장 가능성이 보장된 사업부이다. 이를 활용하여 보안IDC운영팀 독자 법인 설립 과정에 가비아 자금을 투입하고 독자 법인 상장을 통해 보안IDC운영팀은 유동자산을 확보할 수 있으며, 가비아는 자본력 확장 및 기업 규모 확장을 달성할 수 있게 된다. 또한, 가비아 클라우드 데이터센터를 독자 법인과 계약함으로써 내부거래를 통한 양사의 동반 성장이 가능하게 된다.

세 번째, 경쟁력 확보가 가능하다.

- 가비아가 진출하고자 하는 공공클라우드는 보안에 대한 신뢰도가 가장 중요하다. 이러한 상황에서 가비아가 글로벌 기업들에 비해서 부족하다고 여겨지는 부분이 바로 신뢰적 측면이다. 대표적으로 AWS의 경우 이미 미국 정부 대상의 공공클라우드 운용 경험이 있는만큼, 공공클라우드 분야에 있어서의 신뢰도가 높다. 이와 반대로 가비아는 대규모 공공클라우드 운용 경험이 부족한 것이 사실이다. 저자는 이를 타개하기 위해 계열사 분할이 단행되어야 한다고 생각한다. 그 이유는 바로 '기술 패권' 때문이다. 이에 대한 대표적인 사례로 삼성전자를 예로들수있다. 삼성전자의 경우 5G장비 수주전에 돌입하여 미국의 통신사 버라이즌과 약 8조 상당의 5G 네트워크 장비, 솔루션 계약을 수주했지만, 이후에는 이렇다할 성과를 내지 못하고 있다. 그 이유는 각 국가의 정부단위의 기술 패권 확보 노력 때문이다. 미국이나 일본 등의 국가에서는 기술력 확보를 위해 자국 업체 밀어주기에 혈안이 되어있다. 일본의 경우 자국 업체의 장비, 솔루션을 도입할 경우 세금 감면 등의 혜택을 주는 등의 정책을 체택중에있다. 자국 기업의 규모 확장을 통한 기술 패권 확보를 위해서이다. 이러한 산업군 흐름을 한국도 피해가지는 못할 것이다. 아무리 자유시장 체계라 할지라도 자국 우선주위는 당연한 조치이기 때문이다. 이 과정에 있어서 가비아가 계열사 분할을 통해 특정 산업군 전문 기업 이미지 확보와 더불어 기술력 향상을 달성하게 된다면 국내 공공클라우드 분야에서 AWS, MS 등의 기업들과 경쟁할 수 있는 능력을 갖출 수 있으리라 확신한다.

한국데이터센터연합회에 따르면 한국은 2025년 아시아태평양지역 IDC 시장 2위로 부상할 것이라고 예측했다. 이러한 흐름에 발맞춰 가비아가 보안IDC운영팀의 독자 법인 설립을 목표로 계열사 분할을 단행한다면 안정적인 사업 확장과 더불어 경쟁력 확보를 달성할 수 있기를 바란다.