금융보안 프레임워크 사례 연구

2017년 10월

금융위원회

고선영, 김효신

국외훈련개요

1. 훈련국 : 미국

2. 훈련기관명 : 금융정보공유분석센터(FS-ISAC*)
씨티은행(Citi Bank)
아마존웹서비스(AWS**)

* Financial Service Information Sharing and Analysis Center

** Amazon Web Services

3. 훈련분야 : 금융전산보안

4. 훈련기간 : 2017. 8. 20. ~ 2017. 9. 3.

훈련기관개요

1. 금융정보공유분석센터(FS-ISAC)

기관명	Financial Service Information Sharing and Analysis Center
주 소	12020 Sunrise Valley Dr Suite 230, Reston, VA 20191, USA
전화번호	1-877-612-2622
홈페이지	www.fsisac.com
기 능	○ FS-ISAC은 1998년 대통령령(Directive) 63에 의거하여 1999년에 설립되어, 금융회사, 보안 회사, 정부 등 공공 및 민간에서의 금융 관련 물리적·사이버보안 위협에 대한 정보공유 및 분석 역할 수행

2. 씨티은행(Citi Bank) CSFC

기관명	Citi Bank Cyber Security Fusion Center
주 소	283 King George Road, Building E, Warren, NJ, USA
전화번호	1-908-563-4916
홈페이지	www.citigroup.com
기 능	○ CITI CSFC는 2014년 9월에 설립되어, 씨티은행 전체의 사이버 공격 관련 예방, 감지, 대응, 복구 등을 수행
조 직	Citi's CSFC (13개 팀)

3. 아마존웹서비스(AWS)

기관명	Amazon Web Services
주 소	7 W 34th St, New York, NY 10001, USA
전화번호	1-206-266-2992
홈페이지	www.amazon.com
기 능	○ 2006년부터 아마존의 자체 기술플랫폼을 사용해 개발사 고객들에게 웹서비스를 제공하기 시작 ○ 아마존웹서비스(AWS)는 클라우드 인프라스트럭처 플랫폼으로 190개국 대기업, 정부기관, 스타트업 등과 제휴 ○ 현재 컴퓨팅, 스토리지, 네트워킹, 데이터베이스, 분석, 사물인터넷(IoT), 인공지능(AI), 보안 등 90여 개 서비스 제공
조 직	Amazon Web Services New York Branch

목 차

(요약)

미국은 경제 및 정부의 운영에 필수적인 통신, 에너지, 은행·금융, 교통 분야 등의 중요 인프라에 대한 물리적·사이버 기반 공격에 대응하기 위해 1998년 대통령지침 63(Presidential Decision Directive/ NSC-63)을 발효하고 민·관의 협력을 통해 중요 인프라의 취약점을 보완하기 위한 노력을 기울여 왔다.

미국 대통령지침 63, Annex A에서는 ISAC(Information Sharing and Analysis Center, 정보공유·분석센터)의 역할을 규정하고 있으며, ISAC은 중요 인프라에 대한 물리적·사이버 침해를 효과적으로 예방, 탐지, 복구하기 위해 위협, 취약점, 침해요인, 대응 방안 관련 정보를 수집·분석하고 관련 기관들에게 정보를 제공하는 업무를 수행하게 된다.

이에 근거하여 1999년에 미국 금융분야 ISAC(Financial Services – ISAC)이 설립되었으며, FS-ISAC은 금융회사, 보안 회사, 정부 기관, 법집행 기관 등과 협력하여 침해위협 정보를 신속하고 지속적으로 수집·분석하고 중요 정보를 7,000여 개의 관계 기관과 공유하고 있다.

제 1장에서는 미국 FS-ISAC 및 주요 협력 기관인 FSR(Financial Service Roundtable)의 역할, 운용, 모의 훈련 시행 등의 운영 현황을 살펴본다.

제 2장에서는 FS-ISAC에서 제공하는 교육 프로그램인 'Cyber Intelligence Tradecraft Training'의 주요 내용과 실습 과정을 소개함으로써 사이버 침해위협 정보의 분석과 관련된 이론과 실제 적용 사례를 소개한다.

제 3장에서는 글로벌 금융서비스 그룹인 미국 씨티은행의 자체적인 금융전산 보안 운영 사례를 통해, 민간 영역에서 어떻게 사이버 침해위협에 대응하여 정보들을 수집하고 분석, 공유, 대응하는지 현황을 파

악하고, 최근 사이버 범죄의 변화 양상과 이에 따른 사이버 보안 관리 발전 방향을 논의한다.

제 4장에서는 클라우드 서비스 관련 업계 선두 기업인 AWS(Amazon Web Services)의 사례를 소개함으로써, 금융권에서도 수요가 증가하고 있는 클라우드컴퓨팅의 특징, 장점 등을 이해하고 현재 제공되고 있는 주요 서비스의 동향 및 보안, 규제 이슈 등을 점검한다.

결국 미국 금융보안 프레임워크는 민·관의 유기적인 연계뿐만 아니라 민간에서의 철저한 자율보안 노력에 기반하고 있다고 할 수 있다. 1999년 설립된 FS-ISAC의 경우 최근들어 금융회사의 자율 보안에 대한 니즈 증가와 정보공유의 효과, 기관 상호간의 신뢰가 증대되면서 빠른 속도로 성장하고 있다. 미국 FS-ISAC은 정보공유·분석업무 외에도 Cyber Intelligence 전문가 양성, 사이버 침해사고 모의훈련, 글로벌 기관과 제휴 등을 통해 금융보안을 위한 다양한 업무를 수행하고 있다.

글로벌 금융 그룹은 씨티은행은 금융전산에 소요되는 '비용(Money)' 보다는 사람들이 씨티은행을 어떻게 생각하는지, 즉 'People's View'라는 관점에서 금융보안이 핵심적인 요소라고 판단하고 있다. 이에 따라 자체적으로 인력, 기술, 프로세스를 구축하여 자국내 씨티은행뿐만 아니라 전 세계 씨티은행 금융보안과 관련된 이슈들을 수집·분석하고 있으며, 빠르게 진화하는 사이버 리스크에 신속히 대응하기 위해 지속적인 노력을 기울이고 있다.

아마존웹서비스에서는 클라우드컴퓨팅 서비스를 통해 소규모 이용기업들이 시스템 운용 비용을 절감할 뿐만 아니라, 보안을 강화하고, 각국의 규제 이슈를 충족시킬 수 있도록 통합적인 서비스를 구현하고 있다. 현재 AWS, Google 등의 대형 클라우드컴퓨팅 서비스 제공 업체 외에는 아직 클라우드컴퓨팅 서비스의 신뢰성과 보안 수준에 대한 의문점은 있을 수 있으나, 향후 4차 산업혁명의 영향으로 각 산업 분야

에 소규모 ICT 기업들의 진출이 가속화 될 것이라 예상되면서 클라우드컴퓨팅에 대한 수요는 지속적으로 증가할 것이라 예상된다.

마지막으로, 국제적인 사이버 위협이 증가함에 따라 글로벌 관계 기관들간 사이버 인텔리전스 결과 및 이상금융거래(FDS) 정보의 공유에 대한 니즈는 지속적으로 증가될 것으로 보인다. 자국내 금융보안 프레임워크를 강화하는 노력을 계속 기울이는 한편 각국간 정보 공유를 증진시킬 수 있는 방안에 대한 연구가 필요할 것이다.

제 1장. 미국의 금융보안 제도 및 사이버 위협 대응

미국은 경제 및 정부의 운영에 필수적인 통신, 에너지, 은행·금융, 교통 분야 등의 중요 인프라에 대한 물리적·사이버 기반 공격에 대응하기 위해 1998년 대통령지침 63(Presidential Decision Directive/ NSC-63)을 발효하고 민·관의 협력을 통해 중요 인프라의 취약점을 보완하기 위한 노력을 기울여 왔다.

미국 대통령지침 63, Annex A에서는 ISAC(Information Sharing and Analysis Center, 정보공유·분석센터)의 역할을 규정하고 있으며, ISAC은 중요 인프라에 대한 물리적·사이버 침해를 효과적으로 예방, 탐지, 복구하기 위해 위협, 취약점, 침해요인, 대응 방안 관련 정보를 수집·분석하고 관련 기관들에게 정보를 제공하는 업무를 수행하게 된다.

이에 근거하여 1999년에 미국 금융분야 ISAC(Financial Services – ISAC)이 설립되었으며, FS-ISAC은 금융회사, 보안 회사, 정부 기관, 법집행 기관 등과 협력하여 침해위협 정보를 신속하고 지속적으로 수집·분석하고 중요 정보를 7,000여 개의 관계 기관과 공유하고 있다.

제 1장에서는 미국 FS-ISAC 및 주요 협력 기관인 FSR(Financial Service Roundtable)의 역할, 운용, 모의 훈련 시행 등의 운영 현황을 살펴보고, 제 2장에서는 FS-ISAC에서 제공하는 교육 프로그램인 'Cyber Intelligence Tradecraft Training'의 주요 내용과 실습 과정을 소개함으로써 사이버 침해위협 정보의 분석과 관련된 이론과 실제 적용 사례를 소개한다.

Ⅰ. 미국 금융정보공유분석센터(FS-ISAC)

1. 미국 FS-ISAC 회원 및 협조 기관

2017년 8월말 기준, 미국 FS-ISAC은 전 세계 38개국 7,000여개 금융회사, 보안 회사, 정부 기관, 다른 산업 분야의 ISAC 등과 회원 계약 또는 기관간 협약 등을 통해 사이버 위협 관련 정보를 공유·분석 하고 있다.

<미국 FS-ISAC 글로벌 회원 현황>

지 역	협력 기관
Canada	- 48개 회원(은행, 보험회사, 증권, 신용카드 등) - TD 은행은 FS-ISAC 이사회 참여
UK and Ireland	- 52개 회원
Rest of EMEA	- 54개 회원 - ING는 FS-ISAC 이사회 참여
Asia Pacific	- 53개 회원 - 싱가포르 MAS와 분석팀을 운영할 계획(2017년중) - Standard Charter에서 FS-ISAC 이사회 참여

2. 주요 업무

미국 FS-ISAC은 위협정보의 수집, 공유·분석뿐만 아니라, 예·경보 발령, 모의 훈련, 금융 분야 위기상황 관리, 회의체 운영 등 침해사고의 위험을 감소시키기 위한 활동 전반을 지원하고 있다.

<미국 FS-ISAC 주요 업무 현황>

주요 업무	내용
위협정보 수집, 공유·분석 (Security Operation Center* 운영) * Verisign 위탁 운영	1) 정보 수집 사이버·물리적 위협, 취약점, 침해사고, 해결책, 대응 방안 등 수집 2) 정보 분석 수집한 정보에 대해 정보분석팀(연중무휴, 24시간 운영)에서 기술적 타당성, 문제 발생 범위, 위험도 등을 분석, 분석 결과에 따른 공유 여부 결정 3) 정보 공유 이메일, SMS, FAX 전송 또는 웹사이트 게시

예·경보발령	금융 분야의 사이버·물리적 보안위협 경고 수준을 5단계(Low, Guarded, Elevated, High, Severe)로 분류하여 FS-ISAC 웹사이트에 게시
모의훈련(Cyber Attack Against Payment Processes)	참가기관의 위험관리절차 평가, 대응능력 점검 등을 위한 모의 훈련
금융분야 위기상황 관리	사이버·물리적 위기상황 발생 시 회원, 정부, 유관기관 등을 대상으로 비상소집하여 현재 상태를 파악하고 대응 방안에 대해 논의 (전화 회의)
회의체 운영	최신 위협정보와 관심 이슈 관련 협의를 위한 회의체를 운영
기타	1) 워크샵, 세미나 개최 2) 교육 3) 설문 조사 4) 헬프데스크

Ⅱ. Financial Services Roundtable(FSR)/BITS

1. 개 요

Financial Services Roundtable(FSR)은 민간 금융서비스 정책 정보 제공 기관으로, 은행, 보험, 자산관리, 카드 등 금융부문 전반에 관련된 제도개선 및 정부 정책방향 등을 제언하고 있다.

BITS는 FSR의 기술 정책 부서로서 (1) 사이버보안 및 금융사기 감소, (2) 규제 및 리스크 환경 조사, (3) 규제 이슈 제언, (4) 기술 프로그램의 효율성 및 효과 증진, (5) 신규 기술 구축 등의 사안을 다룬다.

2. BITS 구성

BITS는 금융회사 등의 고위경영진(C-Suite: CEO, CIO, CISO 등)으로 구성되어 있으며, 공동 협력을 위해 회원사 포럼 등을 제공하고 있다.

<BITS Leadership('17.8)>

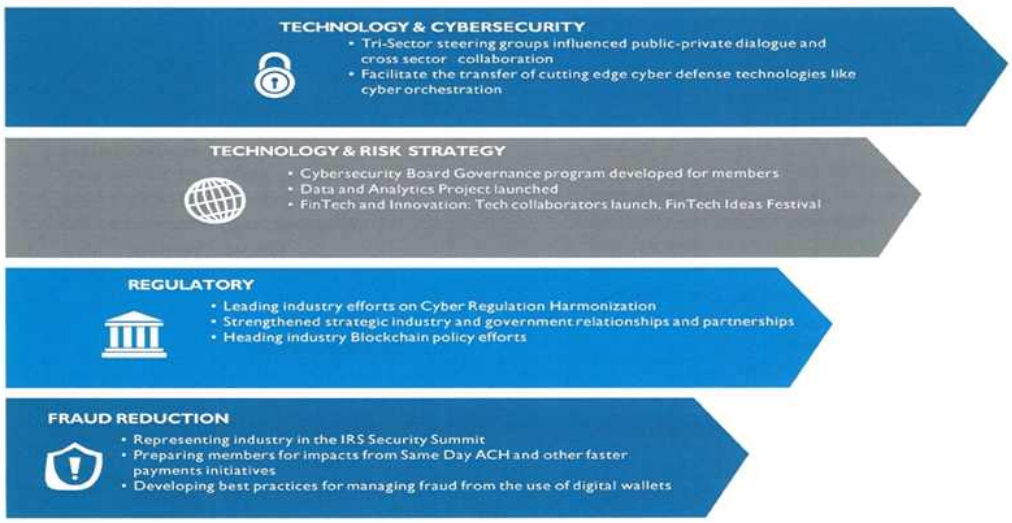
조 직	구 성
BITS COMMITTEE (CEO Only)	Chairman : Bill Rogers, SunTrust Banks Beth E. Mooney, KeyCorp Greg Carmichael, Fifth Third Bank Kelly S. King, BB&T Corporation 외 5인
BITS EXECUTIVE BOARD	Chairman : Anil Cheriyan, SunTrust Banks Amy G. Brady KeyCorp Aravind Immaneni, Fifth Third Bank Barbara Duck, BB&T Corporation 외 10인

3. 주요 업무

BITS의 주요 업무는 다음과 같다.

(1) 고위 공직자 및 산업 전문가 등을 대상으로 주요 정책 이슈 브리핑, (2) 민간 및 공공 부문의 주요 정책 결정자를 대상으로 한 이슈별 포럼 개최, (3) 다른 협회, 정부 기관, 회원사들과 협조하여 보안 시스템 개선, (4) 보안, 벤더 운영, 사업유지 요건 등에 관련된 규제기관과 연계, (5) 회원사들이 신규 기술 및 관련 정책·규제들의 영향을 예측하고 대응할 수 있도록 지원 등

< BITS/FSR 전략 >



Ⅲ. 참고 : 한국 금융정보공유분석센터

우리나라는 은행, 보험사 등의 금융 기반시설 보호를 위한 금융ISAC과 주요정보통신기반시설의 보호를 위한 정보통신 ISAC 등을 운영하고 있다.

금융보안원은 「정보통신기반보호법」 제16조(정보공유ㆍ분석센터)에 따라 금융ISAC을 운영하고 있으며 주요 정보통신기반시설 보호를 위한 정보공유ㆍ분석조직을 수행 중이다. 금융보안원은 또한 「전자금융감독규정」 제37조에 의한 침해사고대응기관이기도 하다.

<정보통신기반보호법 제16조>

① 금융, 통신 분야별 정보통신기반시설을 보호하기 위하여 다음 각 호의 업무를 수행하는 자는 정보공유, 분석센터를 구축 운영할 수 있다.
1. 취약점 및 침해요인과 그 대응방안에 관한 정보 제공
2. 침해사고가 발생하는 경우 실시간 경보, 분석체계 운영

④ 정부는 제1항 각 호의 업무를 수행하는 정보공유, 분석센터의 구축을 장려하고 그에 대한 기술적 지원을 할 수 있다.

<전자금융감독규정 제37조>

① 침해사고에 대응하기 위한 침해사고대응기관은 다음 각 호의 자로 한다.
1. 금융보안원

② 침해사고대응기관은 다음 각 호의 업무를 수행한다.
1. 침해사고에 관한 정보의 수집, 전파를 위한 정보공유체계의 구축
2. 침해사고의 예보, 경보 발령내용의 전파
3. 침해사고의 원인분석과 신속한 대응 및 피해 확산방지를 위해 필요한 조치

<금융보안원 주요 업무[1]>

조 직	구 성
금융부문 통합보안관제	· 금융부문 통합보안관제센터 운영 · 금융정보공유·분석센터 운영
침해사고 대응	· 침해사고 원인분석 및 대응 · 악성코드 정보 수집·분석 및 대응 · 침해사고 대응훈련 · 디도스공격 비상대응센터 운영
이상금융거래정보 공유시스템(FISS)	· 이상금융거래 탐지시스템(FDS)으로부터 탐지된 이상금융거래정보를 신속 공유
취약점 분석·평가	· 전자금융거래법 제21조의3, 정보통신기반보호법 제9조에 의거하여 취약점 관련 정보보호 대책 수립
금융권 자율보안체계 구축	· 금융권 자율보안체계 확립 지원
보안성 검토	· 금융회사 등의 신규 전자금융서비스에 대한 관리적, 물리적, 기술적 보안대책 검토 지원
개인정보 비식별조치 지원	· 금융분야 개인정보 비식별조치 지원 전문기관 지정
정보보호 관리체계 인증	· 정보통신망이용촉진 및 정보보호 등에 관한 법률 제47조에 따라 정보보호 관리체계(ISMS) 인증업무 수행

Ⅳ. 시사점 및 정책 제안

1. 시사점

미국 FS-ISAC은 빠른 속도로 성장하고 있으며 협력 기관이 2103년 4,400여개에서 2017년 6,000여개로 증가하였다. 이는 금융회사의 자율

1) 금융보안원, https://www.fsec.or.kr

적인 위협정보 공유에 대한 니즈와 기존 가입 기관의 정보공유 사례에 대한 효과 및 기관간 신뢰가 축적되면서 빠르게 회원가입 및 협력 기관이 증가하고 있기 때문인 것으로 보인다.

또한 정보 수사기관에서만 정보수집 및 분석이 필요한 것은 아니며, 금융회사 자체적으로도 자체적인 사이버보안을 위해 정보를 수집하고 분석하는 일련의 활동이 필요함을 알 수 있다.

2. 정책 제안

국제적인 사이버 위협이 증가함에 따라 글로벌 관계 기관들간 사이버 인텔리전스 결과 및 이상금융거래(FDS) 정보의 공유에 대한 니즈는 지속적으로 증가할 것으로 보인다. 사이버 인텔리전스 및 FDS 정보 공유를 위한 프로토콜 개발 및 실시간 공유 시스템을 구축할 수 있는 방안에 대한 고려가 필요한 것으로 보인다.

제 2장. 금융보안 교육 프로그램
: Cyber Intelligence Tradecraft Training

Ⅰ. 개 요

미국 FS-ISAC에서 사이버 인텔리전스(Cyber Intelligence) 전문가를 양성하기 위해 제공하는 정보수집 기법 및 분석 방법에 대한 교육과정이다. 공개되어 제공되고 있는 다양한 도구들을 이용하여 필요한 정보(Information)을 수집하고 분석에 적절한 방법론을 선택하여 단순한 정보 수집 이상의 인텔리전스(Intelligence)를 창출하는 것이 목표이다. 동 과정은 이론뿐만 아니라 팀 프로젝트인 케이스 스터디를 통한 실습 과정을 포함한다.

Ⅱ. 정보수집 및 분석 과정

1. 과정의 목표

사이버 인텔리전스 정보수집 및 분석 과정은 사이버 인텔리전스 정보수집 기법에 대해 배우고 이를 분석하는 다양한 기법들을 적용하여 인텔리전스를 구성하는 방법에 대해 학습한다.

특히, 사이버 인텔리전스를 위한 구조화 분석기법을 적용하여 정보분석관[2]이 입수한 불완전하고 애매모호한 기만적인 첩보들을 단계적으로 처리할 수 있는 절차에 대해 학습한다. 이러한 구조화 분석은 분석관이 생각하는 사고의 프로세스를 시스템적이고 투명한 방법으로 표현함으로써 다른 사람들과 쉽게 공유하고 궁극적으로 공동작업을 수월하게 하는 분석방법이다.

구조화 분석은 분석관들의 판단기초인 분석틀을 견고하게 만들어 주

2) 정보 분석 업무를 수행하는 전문가

는 데 유용하다. 구조화 분석기법은 분석적 문제를 여러 개의 구성부분으로 나누고 각각의 구성부분을 단계적으로 해결해 나가는 방법으로서 분석관이 다루어야하는 불확실하고 많은 양의 데이터를 체계적으로 조직화한다. 이러한 분석과정의 투명성을 통해 조직내부 또는 기관내부의 업무협조에 필수적인 효율적인 의사소통을 가능하게 한다.

2. 두 가지 사고 유형

사이버 인텔리전스를 위한 분석 과정에서의 사고는 크게 직관적 사고와 분석적 사고를 예를 들 수 있다. 직관적 사고는 신속하고 효율적이고 때때로 무의식적이다. 이것은 분석관 스스로의 활용 가능한 지식, 과거의 경험 그리고 특정한 환경에서 사람이나 사물이 어떻게 움직이는가에 대한 장기간에 걸쳐 형성된 심리적 유형 등에 기초하여 자연스럽게 도출된다. 이는 노력을 적게 들이고 신속하고 효율적으로 판단하여 문제를 해결할 수 있게 해준다는 점에서 유용하다. 이것은 정확한 경우도 있을 수 있으나 직관적 사고는 잘못된 분석의 원인이 되는 인지적 편향(Cognitive Biases)이나 다른 직관적 오류(Intuitive Mistakes)를 초래할 수 있다.

반면 분석적 사고는 시간이 필요하고 의도적이고 의식적인 추론이다. 이것은 실증적이고 양적인 분석방법은 물론이고 비판적 사고(Critical Thinking), 구조화 분석기법과 같은 모든 정보분석의 유형을 포함한다.

동 교육과정에서는 인지적 편향과 직관적 오류가 발생할 수 있는 직관적 사고를 통한 정보분석을 지양하고, 분석적 사고의 여러 정보분석의 유형 중 구조화 분석기법을 학습할 수 있도록 한다.

3. 편향 다루기

직관적 사고의 활동을 통해 형성되고 표현된다고 생각되는 인지적

편향에는 다양한 형태가 존재한다. 편향의 잠재적 원인에는 전형적인 분석적 사고방식을 갖게 하는 직업의 경험, 훈련이나 교육, 가정교육 환경, 개인의 성격, 특정한 의사결정에 있어서의 개인적 영향력 등이 포함된다.

개인적 이기심에서 기인하는 편향을 제외하면 대부분의 편향은 사려 깊은 추론의 결과가 아니라 신속하고 무의식적이며 직관적인 사고의 결과이다. 직관적 사고는 보통은 타당하지만 불충분한 지식이나 미래 상황의 불확실성은 물론 다양한 편향에 의해 수시로 영향을 받게 된다. 구조화 분석기법은 직관적 사고에 있어 필연적으로 나타나는 분석적 편향을 확인하고, 극복하는 데 도움이 되는 분석적 사고의 한 유형이다.

다양한 구조화 분석기법들을 일반적인 직관적 함정은 물론이고 특정한 인지적 편향을 피할 수 있도록 하는 장점이 있다.

4. 구조화 분석기법의 역할

분석관이 주의해야 할 점은 구조화 분석기법은 편향을 없애는 기법이지 직관적 판단을 대체하는 것이 아니다. 구조화 분석기법의 역할은 분석관이 생각하여야 할 광범위한 선택사항을 확인함으로써 직관적 판단에 의문을 제기하는 것이다. 예를 들면 핵심가정 점검(Key Assumptions Check)은 기존 가정들 이외에 추가적인 가정들을 확인하고 이를 고려하도록 요구하는 것이다. 경쟁가설분석(Analysis of Competing Hypotheses)은 일치하는 가설보다는 반박하는 가설을 중심으로 대안적 가설을 확인하도록 요구하고 증거를 보다 체계적이고 분석하도록 요구하는 것이다.

항상 올바른 결론을 얻을 수 있는 방법은 없지만 구조화 분석기법은 오류의 빈도와 정보를 줄일 수 있다. 분석기법은 분석관이 확인된 인지적 한계를 완화하고 알려진 분석적 편향을 회피하며, 의문을 제기하

지 않은 심리상태 또는 사고방식과 관련된 문제점을 분명하게 직시할 수 있도록 도와준다. 분석기법은 분석관으로 하여금 분석적 문제에 대해 보다 철저하게 생각하게 하고 선입견이나 가정을 당연한 것으로 받아들이지 않고 의식적으로 검토하거나 검증하도록 한다.

구조화 분석기법에 대한 가장 일반적인 비판은 “활용할 수 있는 시간이 없다”는 것이다. 많은 정보분석관들의 경험에 의하면 이러한 비판은 타당하지 않다. 많은 기법들은 거의 시간이 필요하지 않다. 새로운 것을 배우는 데는 시간이 필요하지만 일단 배우고 나면 구조화 분석기법은 분석 시간을 절약하게 해준다. 특히 이것은 어떤 프로젝트가 새로 시작되거나 어떻게 진행해야 하는지 전체적인 모습을 구상하지 못할 경우에 개별 분석관들이 보다 효율적으로 분석을 하 수 있게 해준다. 구조화 분석기법은 증거자료의 수집과 해석에 도움을 주는 것은 물론 의사소통을 향상시켜 팀 활동을 도와준다. 결국 구조화 분석기법은 합리적 근거가 뒷받침되는 결론을 내릴 수 있기 때문에 다른 방법에 의해 도출된 결론보다 분명하고 받아들이기 쉽다. 이것은 상급자와 검토자의 재검토를 용이하게 하고 협조과정을 단축시켜 시간을 절약하게 해준다.

분석방법은 중요하지만 방법만으로는 분석의 정확성과 가치를 담보하기에 불충분하다. 분석방법은 실질적인 전문지식과 결합되어야 하고 호기심과 풍부한 상상력이 있어야 한다. 이것은 개인의 환경보다는 조직 환경에 의해 지원되고 동기가 부여될 필요가 있다.

5. 구조화 분석기법의 역사

구조화 분석기법(Structured Analytic Techniques)이라는 단어는 미국에서 2005년부터 사용되었다. 처음에는 대안분석(Alternative Analysis)이라고 명명되어 1980년대부터 사용되었다. 대안분석은 선택 가능한 복수의 설명이나 가설을 평가하고 타 문화에 대해 이해하고 다른 나라의 관점에서 사건을 분석하는 것을 뜻하였다.

CIA[3]에서 2000년에 정보분석의 효율성을 높이기 위해 셔먼켄트 정보분석학교(Sherman Kent School for Intelligence Analysis)가 설립되었을 때 당시 분석국 부국장인 존 맥라글린에 의해 분석기법을 조합하여 활용하는 방법을 발전시켰다. 이후 켄트학교는 2004년 그 동안 터득한 지식을 바탕으로 훈련교범을 개정하였으며, 서로 다른 10개 정보의 분석기법을 하나로 묶고 진단기법(Diagnostic Techniques), 반박기법(Contrarian Techniques), 추론기법(Imagination Techniques)의 세 개의 분류로 정리하여 "구조화 분석기법"이라고 명명하였다. 이후 2005년 6월 훈련교범 개정이 정식으로 승인되면서 공식 용어가 되었다.

Ⅲ. 적절한 분석기법 선택

앞서 인지적 편향과 직관적 오류를 줄이기 위해 구조화 분석기법을 사이버 인텔리전스에 적용한다고 기술하였다. 다음은 분석관이 흔히 직면할 가능성이 있는 12가지의 가장 흔한 직관적 함정이다.

<직관적 실수>

1. 첩보부재 무시	7. 패턴추정
2. 최초입수 첩보 편향	8. 최초 인상 의지
3. 학습교훈 강요	9. 증거 거부
4. 충분한 상상력 결여	10. 소표본 확대 해석
5. 하찮은 변화 기대	11. 불일치 증거 무시
6. 과거 경험 계획	12. 단순 해결 추정

분석관은 특히 다음의 5가지 함정에 빠지기 쉽다. (1) 다양한 가설들 또는 설명들을 검토하는데 실패, (2) 일치하지 않는 증거 무시, (3) 선행 가설을 지지하지 않는 증거 거부, (4) 불충분한 상상력 또는 핵심 증거를 획득하기 위한 대안적 가설들의 부족 그리고 (5) 과거 경험을

3) 중앙정보국(Central Intelligence Agency, CIA)

부적절하게 기획하는 것이다.

1. 핵심기법

다양한 분석기법의 기능과 그 분석기법이 어떠한 분석상황에 적합한지 알아보도록 한다.

1) 구조화 브레인스토밍(Structured Brainstorming)

이 방법은 널리 사용하는 방법으로 분석 프로젝트 초기에 특정분야를 잘 하는 전문가 집단으로부터 관련 정보를 이끌어 내거나 통찰력을 얻기 위해 사용하는 집단 아이디어 발굴 기법이다. 구조화 브레인스토밍을 통해 일련의 리스트를 작성하는 것이 목표이다. 정보분석에 있어서 관련 변수, 추동요인, 가설, 핵심 행위자, 이해관계자, 확보 가능한 증거, 정보출처, 잠재적 해결책, 잠재적 결과 또는 시나리오, 특정 상황에 대한 적의 예상반응과 같은 것들의 전체 리스트 작성이다. 이 외에도 명목집단기법(Nominal Group Technique)이 있다.

2) 교차영향력 매트릭스(Cross-Impact Matrix)

구조화 브레인스토밍을 통해 리스트를 작성하였다면 다음 작업은 교차영향력 매트릭스를 만들어 변수들 간의 관계, 추동요인들 간의 관계, 주요 행위자들 간의 관계에 대하여 논의하고 그 관계를 시각화할 수 있다. 이 과정에서 팀원들은 변수들에 대해 알게 되고 그 변수들이 어떻게 상관관계를 가지는지에 대한 공통된 지식을 쌓을 수 있다.

3) 핵심가정 점검(Key Assumptions Check)

보편적으로 많이 사용되는 기법으로 분석관들로 하여금 자신들의 분석에 전제가 되는 가장 중요한 가정들을 명확하게 나열하여 질문하는 것이다. 현재 사건에 대한 설명이든 미래 전개상황에 대한 예측이든

이런 작업들은 불완전하고 모호하며 잠재적으로 기만적일 수 있는 증거들의 해석을 통해 이루어지는 것이다. 그 간극을 채우기 위해서 분석관들은 보통 정치세력들 간의 상대적 힘, 다른 국가의 의도나 능력, 특정 국가에서 수행하는 정부의 일처리 방식, 주요 첩보출처의 신빙성, 같은 주제에 대한 과거 분석사례의 타당성, 활동이 일어나고 있는 전체 맥락에 있어서의 관련된 변화 유무 등에 대하여 가정들을 만들어 검토한다.

4) 지표(Indicators)

관찰이 되거나 잠재적으로 관찰이 가능한 행위 및 사건들로서 시간이 변하면서 변화를 탐지하거나 변화가 평가될 수 있어야 한다.

5) 경쟁가설분석(Analysis of Competing Hypotheses)

가장 가능성이 있는 하나의 가설을 사용하기보다 그럴듯한 가설들 모두를 가지고 시작하는 것이다. 분석관은 관련 정보 각각의 항목을 가지고 한 번에 하나씩 가설들과 일치하는지 불일치하는지를 판단하게 된다. 이 생각은 그것들을 확인하는데 있기보다 부정하는데 있다. 가장 가능성이 있는 가설은 그것을 지지하는 정보가 가장 많은 가설이라기보다는 그것을 반박할 수 있는 정보가 가장 적은 가설이 되는 것이다.

6) 사전부검 분석(Pre-Mortem Analysis) 및 구조화 자기비판(Structured Self-Critique)

이 두 가지 분석기법은 미래지향적 분석 작업을 함께 수행해온 소규모 분석 팀에서 효과적으로 자신들의 결론에 대한 정확성을 높일 수 있도록 한다. 사전부검(사전 실패가정) 분석은 일종의 재구조화 형식을 사용하게 해준다. 즉 전혀 다른 관점에서 질문과 문제를 재구성하여 그것을 다른 관점에서 보거나 다른 해답이 도출되도록 하는 것이다.

7) 발생가정 분석(What if? Analysis)

이 방법은 분석관이 발생가정 분석을 실행할 때에는 예상하지 못했던 사건이 발생했다고 상상을 하고 사후평가(Hindsight)를 통해 어떻게 해서 그것이 일어났으며 잠재적인 결과가 어떻게 될 것인가를 분석하는 것이다. “만약에 ~한다면”이라는 발생가정 분석은 정책결정자들이 혹시 잘못 결정할지도 모르는 개연성에 대하여 미리 경계할 수 있는 좋은 방법이 될 수 있다.

2. 하나의 프로젝트와 복수의 분석기법

통상 프로젝트에 하나의 분석기법만을 적용하지는 않는다. 아이디어 발굴, 아이디어 평가, 가정 찾아내기, 결론 도출, 이전에 도출된 결론에 도전하기 등 여러 가지 서로 다른 기법들이 다양하게 사용될 수 있다.

또한, 복수의 분석기법들은 분석 결론의 정확성을 점검하고 신뢰도를 제고하는데 사용될 수 있다. 연구조사 결과 매우 다른 방법을 통해 나온 예측결과와 전혀 다른 정보출처로부터 입수된 예측결과를 함께 통합하여 판단할 때 분석의 예측 정확성이 훨씬 더 향상된다.

3. 분석기법 선택의 일반적 실수

분석의 영향에 가장 큰 부분은 적절한 분석기법을 선택하였는지 여부이다. 분석기법의 선택이 중요함에도 불구하고 분석관들은 최적의 분석기법을 선정하는데 매우 혼동하는 경향이 있다. 특히 분석관들은 다음과 같은 요익에 영향을 받기 쉽다.

1) 대학 및 대학원 시절 학습법 사용 : 분석관들은 대학이나 대학원에서 배운 분석수단을 최선의 방법으로 생각하고 무턱대고 사용하려는 성향이 있다.

2) 습관화된 기법 사용 : 분석관들은 이미 알고 있는 것이나 쉽게 이용할 수 있는 것이라면 무엇이든 우선적으로 사용하려고 하는 경향이 있다.

3) 편의적 분석기법 사용 : 분석관들은 정보문제를 제기하는데 있어서 정말로 필요한 증거를 찾아 나서기 보다는 쉽게 입수할 수 있는 증거를 찾아서 그 증거에 부합되는 기법을 사용하려는 경향이 있다.

4) 시간제약 : 분석관들은 시간이 많이 소요되는 분석기법들을 피하려고 하는 경향이 있다.

Ⅳ. 분해와 시각화(Decomposition and Visualization)

분석관들이 정보분석을 할 때 직면하는 가장 어려운 점 중의 하나는 많은 첩보를 그들 머릿속에서 동시다발적으로 고려하는데 한계가 있다는 점이다. 예를 들어 우선 장점에 초점을 맞추어 본 후 단점을 고려하거나, 또는 어떤 결정을 우선적으로 선호했다가 다시 다른 결정을 선호하는 등 분석관의 생각이 흔들릴 수 있다. 이 뿐만 아니라 많은 변수들이 상호 작용하는 정보 문제에 대해 생각할 때 모든 변수들에 대한 동시 고려는 어려운 사항이다. 인간 사고의 한계로 인해 어떠한 도움 없이 오류가 없는 분석을 하는 것은 매우 어려운 일이다. 그래서 분해와 시각화에 대해 학습을 하고 다루는 문제나 이슈를 구성하고 있는 가 부분들을 분리하여 고려할 수 있도록 나누는 것이다. 시각화는 다양한 부분들이 어떻게 상호작용하는지에 대한 조직화된 방법이다.

1. 시작 체크리스트(Getting Started Checklist), AIMS(Audience, Issue, Message, Storyline), 고객 체크리스트(Customer Checklist), 이슈 재정의(Issue Redefinition)

분석관들이 새로운 프로젝트를 개념화하고 착수함에 있어 혼합하여 사용할 수 있는 기법이다. 이러한 분석 기법을 통해 분석관들은 프로젝트를 올바른 방향으로 시작할 수 있고 도중 방향 변경을 피할 수 있어 많은 시간을 절약할 수 있다.

2. 연대표(Chronologies)와 타임라인(Timelines)

사건이나 활동에 관한 자료를 체계적으로 정리하기 위해 사용하는 기법이다. 연대표는 관련 사건의 시점이나 순서를 이해하거나 주요 사건과 사건들 사이의 시간적 공백을 알아보는 것이 중요할 때 사용할 수 있다.

3. 분류(Sorting)

새로운 통찰력을 필요로 할 때 자료들을 체계화하기 위한 기본적인 기법이다. 이것은 엑셀 같은 컴퓨터 프로그램을 이용하여 비교를 위해 첩보 요소들을 몇 개의 카테고리들 또는 하위 카테고리들로 나눌 수 있을 때 효과적이다. 이것은 특히 초기에 자료 수집과 가설수립 과정에서 효과적이다.

4. 순위부여(Ranking), 점수부여(Scoring), 우선순위 결정(Prioritizing)

순위부여(Ranking), 점수부여(Scoring), 우선순위 결정(Prioritizing)은 향후 순위투표(Ranked Voting), 쌍대비교(Paired Comparison), 가중서열화(Weighted Ranking)라는 세 가지 다른 순위부여 기법들에 기초를 제공해 준다. 또한 구조화 브레인스토밍과 같은 아이디어 기법과 순위부여 기법을 결합시키는 것은 분석관들이 새로운 프로젝트를 시작하거나 기관 내 또는 외부 기관과 협력을 위해 효과적인 방법을 제시한다.

5. 매트릭스(Matrices)

비교와 분석을 용이하게 하기 위한 방식으로 자료를 분류하고 조직화하기 위한 포괄적인 분석 도구이다. 매트릭스는 두 종류의 변수들 사이의 관계 또는 한 종류의 변수들 사이의 상호관계를 분석하는데 이용된다. 매트릭스는 분석될 문제가 무엇이든 간에 필요한 만큼의 칸(Cell)을 가진 형태로 구성된다.

6. 벤 분석(Venn Analysis)

주장들에 대한 논리 탐구를 위해 시각적으로 표현하는 기법이다. 벤 다이어그램은 수학에서 집합론을 가르칠 때 흔히 이용된다. 또한 벤 분석은 단순히 분석적 주장들 사이의 일련의 관계를 보여주기 위해서나 추론의 결점을 파악하기 위해서 또는 자료 누락을 확인하기 위해서도 사용될 수 있다.

Ⅴ. 아이디어 창출(Idea Generation)

새로운 아이디어 그리고 기존의 아이디어들을 새로운 방법으로 결합시키는 것은 효과적인 분석을 위한 필수적인 요소이다. 아이디어 창출과 관련된 구조화 기법들은 특히 프로젝트의 초기 단계에서 아이디어들을 끌어내거나 창출하려는 목적을 위한 것이다.

어떤 의미에서 모든 구조화 분석기법들은 협력적인 집단과정 속에서 이용될 때 모든 아이디어 창출기법이라고 할 수 있다. 구조화된 과정은 팀 또는 집단 구성원들 간에 서로 다른 관점이나 추정들을 밝혀냄으로써 학습 의욕과 새로운 아이디어를 불러일으킨다. 아이디어 창출 기법은 많은 인지 편향, 특히 집단사고(Groupthink), 미성숙 종결(Premature Closure) 그리고 분석관이 어려운 문제에 대해 빠르고 쉽게 답변을 제공하고자 할 때 그 문제를 지속적으로 평가해 나가는 동안 정확성 부족 현상을 나타난다는 이른바 정신적 산탄총(Mental Shotgun) 현상을 방지하는데 효과적이다. 아이디어 창출 기법은 어떤

사건이 실제로 일어날 가능성보다 실현 가능성을 더 높게 추정하는 경향을 점검하거나 초기에는 중요하다고 생각하였으나 더 이상 확인할 수 있는 정보가 없는 경우에 계속 관심을 갖고 확인하기 위해 사용할 수 있다. 새로운 아이디어를 창출하거나 여러 갈래의 아이디어들을 종합하고자 할 때 집단이나 팀으로 구조화 분석기법을 사용하는 것이 개인 혼자서 하는 것보다 더 효과적이다.

1. 구조화 브레인스토밍(Structured Brainstorming)

이 기법은 단순히 동료 집단이 어떤 문제에 대해 둘러 앉아 이야기하는 것이 아니라 특정한 규칙과 절차를 따르는 하나의 집단 과정이다. 이것은 프로젝트 초기에 적절한 변수들의 목록, 추동 요인들, 다양한 모든 가설들, 핵심 행위자나 이해 관계자들, 이용 가능한 증거나 정보 출처, 어떤 문제에 대한 가능한 해결책, 또는 가능성 있는 결과나 시나리오를 확인하기 위해 사용된다. 이 기법은 거의 훈련을 필요로 하지 않으며, 미국 정보공동체에서 가장 자주 사용되는 구조화 기법의 하나이다. 이 기법은 분석관들이 자신들의 브레인스토밍 결과를 기록하고 저장할 수 있는 위키(Wiki)와 같은 수단을 병행하여 사용할 때 가장 효과적이다. 또한 참여자들은 직접 모여 브레인스토밍하는 경우에도 절차가 끝난 후 위키를 통해 그 브레인스토밍 결과를 개선하거나 추가 의견을 제시할 수 있다.

2. 온라인 브레인스토밍(Virtual Brainstorming)

참가자들이 지리적으로 서로 다른 위치에 있을 때 구조화 브레인스토밍을 진행하는 방법이다. 대면 접속이 없는 점은 불리한 점으로 작용할 수도 있지만 유리한 점으로 작용할 수도 있다. 장거리 브레인스토밍은 분석관들이 대면 형식의 브레인스토밍에서 느낄 수 있는 일종의 압박을 완화시키는데 도움이 될 수 있다. 또한 이러한 방법은 생산성을 증가시킬 수 있는데 왜냐하면 참가자들이 자신의 아이디어를 생각하는 동안 다른 사람의 아이디어를 신속하게 읽어야 한다거나 자신

의 말할 순서를 기다릴 필요 없이 편리한 시간에 위키를 통해 자신의 의견을 올릴 수 있기 때문이다. 문서, 그림, 사진, 비디오 등을 올릴 수 있고 참가자들이 각자 컴퓨터 화면을 통해 아이디어를 공유할 수 있는 동 위키 형식은 분석관들이 브레인스토밍 아이디어를 기록하고 계속 지켜본 다음 이에 대한 의견을 말할 수 있게 해준다.

3. 명목집단기법(Nominal Group Technique, NGT)

구조화 브레인스토밍과 많은 부분 같은 기능을 수행하지만 아주 다른 접근법을 사용한다. 이것은 집단의 상관이나 거침없이 말하는 경향이 있는 구성원이 브레인스토밍 미팅을 주도하거나 또는 부하 직원들이 말하기를 꺼려하거나 그 미팅에서의 토론이 너무 과열될 우려가 있을 때 선호되는 기법이다. 이 기법은 모든 참가자들이 모든 아이디어를 다 내놓았다고 느낄 때까지 회람방식(Round-Robin Fashion)으로 참가자들이 한 번에 하나씩 아이디어들을 제시하도록 함으로써 동등한 참여를 권장한다.

4. 스타버스팅(Starbursting)

답변보다는 질문의 발굴에 초점을 맞춘 브레인스토밍의 한 형태이다. 조사 프로젝트의 매개변수들을 설정하기 위해 스타버스팅을 이용하여 답변이 필요한 질문을 찾아낸다. 질문들이 누가 무엇을, 언제 어디에서 왜라는 의문사로 시작한다. 조사 주제에 대해 가능한 많은 질문들을 발굴하기 위해 이러한 의문사로 직하는 질문들을 차례대로 브레인스토밍한다.

5. 교차영향력 매트릭스(Cross-Impact Matrix)

특정 분석 프로젝트에 관련된 변수들의 목록을 찾아내는 모든 형태의 브레인스토밍 실행이 끝난 다음에 이용할 수 있는 기법이다. 브레인스토밍의 실행 결과들을 매트릭스에 기입한다. 이 매트릭스는 각각

의 변수들이 특정 문제의 맥락에서 관련되어 있는 다른 변수들에게 얼마나 영향을 미치는가를 체계적으로 검토하는 집단토론을 이끌어 나가기 위해 이용될 수 있다. 가끔은 집단 토론을 통해 추가적 공동작업의 기초를 제공하는 소중한 학습 경험을 얻을 수 있다. 교차영향력 토론의 결과들은 지속적인 참조를 위해 위키 형태로 유지될 수 있다.

6. 형태 분석(Morphological Analysis)

이용 가능한 자료가 거의 없고 기습 가능성들이 중요한 의미가 있는 복잡하고 수량화할 수 없는 문제들을 다루는데 유용하다. 이 기법은 다차원적이고 매우 복잡하며 보통은 수량화할 수 없는 문제 공간(Problem Space)에서 모든 가능한 관계들을 체계적으로 찾아내고 검토하기 위한 일반적인 방법이다. 이것은 복잡한 상황에서 일어날 수 있는 다수의 결과들을 발굴하여 분석관들이 이전에 상상하지 못했거나 최소한 고려하지 않았던 방식으로 어떤 사건들이 발생할 가능성을 줄임으로써 기습을 방지하는데 도움이 된다. 이 방법을 이용하기 전에 훈련과 연습이 필요하며 형태적인 분석의 경험이 있는 진행자가 필요할 수도 있다.

7. 사분면 분할(Quadrant Crunching)

다수의 대안적 결과들을 체계적으로 발굴하기 위한 출발점으로서 핵심 가정들과 정 반대의 가정들을 활용하는 형태적 분석을 적용한 것이다. 이 기법은 두 가지 버전이 개발되었는데 기습을 피하기 위한 전통적 사분면 분할(Classic Quadrant Crunching)과 일련의 포괄적인 미래의 가능한 대안들을 밝혀내기 위한 예측적 사분면 분할(Foresight Quadrant Crunching)이다. 예를 들어 분석관은 테러리스트가 상수도를 공격할 수 있는 많은 다양한 방식들을 찾아내기 위해 전통적 사분면 분할을 사용할 수 있을 것이다.

사분면 분할은 분석관들로 하여금 다양하고 폭넓은 관점으로부터 이

슈를 다시 생각하게 하고, 또한 가설들의 기저를 이루는 모든 가정들에 대해 체계적으로 의문을 제기하도록 강력히 촉구한다. 이 기법은 이용 가능한 정보가 거의 없는 모호한 상황에서 활용할 수 있는 가장 유용한 방법이다.

Ⅵ. 시나리오와 지표(Scenarios and Indicators)

분석관이나 의사결정자가 복잡하고 계속 변화하는 불확실한 상황 속에서 미래를 예측하는 것은 쉽지 않다. 어떤 사건은 본질적으로 낮은 예측 가능성을 지닌다. 분석관이 할 수 있는 최선의 일은 미래의 결과를 결정하는 추동요인들을 확인하고 이들이 상호작용을 하여 미래를 형성할 때 이것들을 관찰하는 것이다. 시나리오는 이러한 작업을 수행하기 위한 중요한 수단이다. 시나리오는 어떻게 미래가 전개될지에 대해 그럴듯하게 꾸며진 스토리이다. 대안적 미래가 명확히 제시될 때 의사결정자는 이러한 미래를 마음속으로 그려보면서 “이러한 미래에 준비하기 위해 지금 무엇을 해야 하는가?”라는 스스로 자문하게 된다.

하나의 결과만을 추측하고 예측하는 것은 전형적으로 고위정책 관리자, 의사결정자, 기타 정보수요자에게 폐를 끼친다. 예를 들어 가장 가능성이 있는 것, 가장 가능성이 없는 것, 그리고 가장 위험한 것처럼 여러 가지 시나리오를 수립하는 것은 상황이 어떻게 전개되더라도 영향을 미칠 핵심 추동력과 요인에 대해 집중할 수 있도록 도와준다. 분석관이 가정을 점검하고 고충격・저확률 시나리오가 실제로 실현될 경우 유용한 경고 메시지를 발하기 위해 시나리오를 활용할 수 있다.

견실하게 시나리오 분석을 실시하는 것은 집단사고와 같이 잘 알려진 인지적 편향을 극복하기 위한 강력한 도구가 될 수 있다. 첫째, 시나리오 분석기법은 매우 광점위한 분야에 있어 탁월한 분석관으로 구성되는 다양한 팀을 필요로 한다. 둘째, 핵심 추동요인들을 밝히고 이들의 조합을 활용하여 다수의 대안적 경로들을 발굴하는 과정은 분석

관이 만약 오직 직관과 자신의 전문지식에만 의존한다면 결코 생각할 수 없는 미래에 대한 다양한 생각을 가능하게 해 줄 것이다.

지표(Indicators) 또는 이정표(Signposts)를 확인하고 모니터하는 것은 미래에 전개될 어떤 상황에 대해 조기경보를 제공할 수 있으나 이러한 초기 징후에 명확하게 나타나지 않는다. 지표는 오직 그 지표가 확인되는 구체적인 시나리오의 맥락에서 있어서만 의미를 갖는다. 시나리오와 관련 지표를 사전에 확인하는 것은 의미 있는 변화가 초기 징후를 인식하도록 마음을 준비시킬 수 있다. 지표는 분석의 초기 단계에서 분석관의 실제적 사고과정을 사로잡는데 활용될 수 있는 객관적이고 미리 설정된 리스트들을 수립하기 때문에 사후평가 편향(Hindsight Bias)을 극복하는데 특별히 유용하다. 이와 유사하게 만약 분석관이 나타날 것으로 생각했던 지표들이 실제로 나타나지 않았다면 이러한 지표들은 분석관이 어떤 상황이 전개되는 것이 불가피하다고 생각했던 인지적 편향을 경감시킬 수 있게 된다.

변화는 때때로 분석관이 이를 알아차리지 못하게 점진적으로 일어나거나 분석관은 변화가 너무 명확해서 무시할 수 없을 때까지 그 변화가 근본적으로 중요하지 않는 것으로 합리화한다. 일단 분석관이 한 이슈에 대해 어떤 입장을 취하게 되면 그들은 일반적으로 새로운 증거에 반응하며 그들의 판단을 변화시키는 속도가 늦어진다. 어떤 행동이나 사건이 중요하고 그들의 마음을 변화시킬 수 있는 것인지를 사전에 구체적으로 기록해 둔다면 분석관은 이러한 합리화 현상을 피할 수 있을 것이다.

시나리오의 또 다른 장점은 복합적인 아이디어들을 전달하기 위한 효율적인 메커니즘을 제공하는 것이다. 시나리오는 복합적인 아이디어들을 간략하게 표현하고 있다. 이러한 표현은 생각할 수 있는 모든 것들의 목록을 제공해주고 다른 분석관 및 의사결정자들과 의사소통을 할 수 있는 자료를 제공해준다.

1. 시나리오 분석(Scenarios Analysis)

하나의 상황이 전개될 수 있는 다양한 방법을 확인한다. 이러한 분석 유형은 의사결정자들에게 일어나는 모든 기회를 활용하고 미래에 있을지 모르는 모든 위험을 회피하기 위해 계획하는 데 도움을 준다. 단순 시나리오(Simple Scenarios)는 한 명의 개인 분석관 또는 소그룹의 분석관들이 시나리오들을 수립하기 위한 빠르고 쉬운 방법이다. 그것은 현재의 분석 방향에서 시작하여 다른 대안들을 탐색한다. 타당성 원추(Cone of Plausibility)는 소그룹 전문가 집단의 작업에 적합한 데 핵심 추동요인들을 정의하고 기본 시나리오를 설정한 다음 그럴듯한 대안 시나리오와 예측 불가능 상황을 검토하기 위해 추동요인에 수정을 가하는 방법으로 진행한다. 대안 미래분석(Alternative Futures Analysis)은 일단의 전문가들 및 때로는 의사결정자들과 훈련된 진행자들을 활용하는 좀 더 체계적이고 창의적인 절차이다. 복수 시나리오 수립(Multiple Scenarios Generation)은 조금 더 복잡하기는 하지만 대안 미래분석보다 더 많은 시나리오를 다룰 수 있다. 이것은 진행자를 필요로 하는데 이 기법의 활용은 사건이 가능성이 있다고 여겨지지 않는 방향으로 전개해 나갈 위험성이 크게 경감시킬 수 있다. 다섯 번째 기법인 예측적 사분면 분할은 복수 시나리오 수립과 핵심가정 점검 기법의 변형이다.

2. 지표(Indicators)

어떤 미래 사건의 조기경보를 제공하거나 관찰되는 것을 검증하기 위해 활용되는 전통적인 기법이다. 지표들은 여러 가능한 시나리오에서 어느 것이 전개되고 있는지를 확인하기 위해 시나리오들과 종종 짝을 이룬다. 그들은 정치적 불안정과 같은 바람직하지 않는 조건 또는 경제개혁과 같은 바람직한 조건을 향한 변화를 측정하는데도 활용된다. 시간 흐름에 따른 변화를 감시, 탐지 또는 평가하기 위해 특정 상황을 추적할 필요가 있을 때 지표들을 활용한다. 지표 리스트는 수집 노력을 안내하고 모든 이해 당사자들에게 관련 첩보를 보내기 위한 토

대가 된다. 그것은 나타나는 사건들을 추적하기 위한 기록 시스템의 토대로 작용할 수도 있다.

3. 지표 검증(Indicators Validation)

분석관들이 지표의 타당성을 평가하도록 도와주는 과정이다. 지표는 그것이 오직 한 시나리오 또는 한 가설의 가능성을 명확하게 가리키고 다른 것들은 가능성이 없음을 제시할 때 가장 타당하다. 지표들은 매우 빈번히 여러 다른 결과들 또는 다른 가설들과 일치할 수 있기 때문에 제한된 가치를 지닌다.

Ⅶ. 가설 수립과 검증(Hypothesis Generation and Testing)

정보, 법 집행 그리고 경제 분야에서 수행되는 분석은 과학의 정확성과 예측 가능함을 결코 달성할 수 없는데 왜냐하면 분석관들이 가지고 작업해야 하는 첩보는 일반적으로 불완전하고 애매모호하며 기만 가능성이 있기 때문이다. 그러나 분석과정은 과학의 교훈들을 통해 개선될 수 있도록 과학적 추론의 원리들을 적용할 수 있다.

과학적인 과정은 관찰, 분류, 가설들을 세우고 이러한 가설들을 검증하는 것을 포함한다. 가설 수립과 검증은 구조화 분석의 핵심 기능이다. 과거에 대한 가능한 설명 또는 미래에 대한 판단은 증거의 수집과 제시에 의해 검증될 필요가 있는 가설인 것이다. 가설수립과 관련된 기법들을 통해 다른 유사한 기법들은 분석관들에게 주제를 위해 새롭고 대안적 설명을 상상할 수 있게 해준다. 복수 가설들을 수립하는 과정은 여러 인지적 편향(Cognitive Biases)에 대한 대안이 될 수 있다. 그것은 분석관들에게 대안적 설명을 수립하도록 자극함으로써 닻내림 효과(Anchoring Effect)를 경감시키고 분석관들에게 새로운 아이디어와 다양한 순열(Multiple Permutations)을 경험하게 함으로써 확증 편향(Confirmation Bias)의 영향을 감소시키며 성급한 결론(Premature

Closure)에 이르는 것을 피하도록 도와준다.

이러한 대안적 설명들은 이용 가능한 증거와 대조하여 검증될 필요가 있다. 가설 검증 기법은 분석관들에게 자료의 질에 민감해지도록 자극하고 가설과 일치할 뿐 아니라 일치하지 않을 수 있는 첩보들을 찾게 한다. 모든 증거들을 체계적으로 검토함으로써 좀 더 생생하거나 가장 익숙한 시나리오들에 가장 많은 관심을 집중하려는 인지적 편향을 경감시킬 수 있다.

가설 수립과 검증은 기술로서 그 치밀함이 저절로 실현되는 것은 아니다. 그것은 중대한 이해관계가 걸린 상황 처리에 활용하기 위해 배울 수 있는 추론의 형태이다. 저절로 실현된다는 것은 직관적인 판단을 위해 우리의 기존 지식과 경험에 의지하는 것을 말한다. 이것은 우리가 매일 생활하는 대부분의 환경에서 대부분의 시간 동안 이루어지는 효과적인 접근방법이다. 그러나 정보분석에 있어서 이것은 충분하지 않다. 왜냐하면 정보 이슈들은 일반적으로 매우 복잡하고 실수의 위험과 비용이 너무 크기 때문이다. 그리고 상황은 종종 특이할 때가 있으며 그래서 과거의 지식과 경험에 의해 이루어지는 직관적인 판단은 틀리기 쉽다.

사람이 복잡한 선택에 직면하게 될 때 관행에 따라 직관적 판단에 의존하게 되는 현상을 노벨상 수상자 허버트 사이먼은 만족화 행동원리라는 용어로 설명하였다. 이것은 가장 바람직하거나 최선의 답을 찾기 위해 다양한 선택방안을 평가하는 것과는 구분되며 적합한 것으로 보이는 첫 번째 답에 만족한다는 것을 의미한다. 만족자는 모든 가정을 좀 더 폭넓게 보기 보다는 첫 번째 답을 지지하는 정보만을 구할지 모른다.

복합적인 이슈에 대한 좋은 분석은 일련의 대안 가설들과 함께 시작해야 한다. 또한 숙련된 분석관들은 과학자들이 사용하는 대안 가설에 대한 검증 도구를 사용한다. 가설은 가설에 부합하는 증거만을 인용하

여서는 결코 분명하게 증명될 수 없는데 왜냐하면 동일한 증거가 종종 하나 또는 그 이상의 다른 가설과도 일치할 수 있기 때문이다. 과학은 종종 가설들을 반박하거나 부당성을 증명함으로써 진행된다. 반박될 수 없는 가설은 그것을 지지하는 많은 증거를 가지는 것으로 보이는 가설로서 중요하게 받아들여져야 한다. 가설과 일치하지 않는 것으로 보이는 단순한 증거는 그 가설을 거부하기 위한 충분한 토대가 될 수도 있다. 가장 지지할 수 있는 가설은 그것에 반하는 증거가 가장 적은 경우가 많다. 분석관들은 귀추법(Abduction)으로 알려진 추론 형식을 활용하여 가설들을 검증하는데 이는 잘 알려진 두 가지 추론 형식인 연력법과 귀납법과는 다르다. 귀추법 추론은 일련의 사실들과 함께 시작한다. 이러한 사실들이 참이라고 할 때 사실들을 가장 잘 설명할 수 있는 가설들을 수립한다. 가장 지지할 수 있는 가설은 사실들을 가장 잘 설명하는 가설이다. 정보분석에 내재된 불확실성으로 인해 가설을 결정적으로 입증하거나 반박할 수 있는 것은 예외적인 경우에 속한다.

이 장은 특별히 가설수립을 위해 활용할 수 있는 세 가지 기법들을 설명한다. 다른 장들도 가설수립을 위해 활용할 수 있는 기법들을 포함하나 다양한 다른 목적들을 지닌다. 이들은 벤(Venn) 분석, 구조화 브레인스토밍, 명목집단 기법, 사분면 분할, 시나리오 분석, 델파이 기법 그리고 의사결정나무를 포함한다.

이 장은 가설검증을 위한 네 가지 기법들을 논의한다. 이들 중 하나는 경쟁가설분석(ACH)으로서 특별히 정보분석에서 활용하기 위해 리차즈 휴어가 개발하였다. 그것은 칼 포퍼의 과학 이론을 정보분석에 적용한 것이다. 포퍼는 20세기의 가장 영향력 있는 과학철학자 중의 한 사람이다. 그는 과학적 추론은 다양한 가설과 함께 시작되어야 하고 반박할 수 없는 가설들은 잠정적으로 받아들여야 하지만 반박을 통해 가설들을 제거하는 방법으로 추론을 전개해야 한다는 입장으로 잘 알려져 있다.

1. 가설수립(Hypothesis Generation)

단순 가설(Simple Hypotheses), 복수 가설 수립(Multiple Hypotheses Generator), 사분면 가설수립(Quadrant Hypothesis Generation) 등 세 가지 기법을 포함한다. 단순 가설은 사용하기 가장 쉬운 것이나 항상 최선의 선택은 아니다. 수립 가능한 모든 가설을 확인하기 위해 복수 가설수립 도구를 사용한다. 사분면 가설수립은 결과가 단 두 개의 추동요인들에 의해 결정될 가능성이 있을 때 일련의 가설들을 확인하기 위해 활용된다. 후자의 두 기법은 일련의 상호 배타적이고 포괄적이며 상세한(Mutually Exclusive Collectively Exhaustive, MECE) 가설들을 확인하는데 특히 유용하다.

2. 진단적 추론(Diagnostic Reasoning)

가설 검증을 중요한 새로운 첩보의 평가에 활용한다. 새로운 첩보는 그 첩보 자체의 그럴듯한 맥락에서 평가되어야 하고 분석관이 구축해 놓은 관념적 모형(Mental Model)의 맥락에서 평가되어서는 안 된다. 진단적 추론의 활용은 기습의 위험을 줄이는데 그것은 분석관이 적어도 대안 결론들을 어느 정도 감안할 것을 보장하기 때문이다. 진단적 추론은 단일의 증거항목을 평가하기 위해 활용된다는 점에서 경쟁가설분석과 다르다. 반면에 경쟁가설분석은 다양한 증거와 좀 더 복합적인 분석과정을 포함한 전체적인 이슈를 다룬다.

3. 경쟁가설분석(Analysis of Competing Hypotheses: ACH)

포퍼의 과학철학을 정보분석 분야에 적용한 것이다. 합리적으로 성립 가능한 모든 가설들을 확인하고 반박하려는 요구는 분석관에게 대부분의 분석 상황에 내재된 많은 불확실성을 인식하게 한다. 경쟁가설분석은 분석관에게 그 불확실성을 줄이기 위한 경로를 확인하기 위해 연관된 첩보를 분류하고 관리하도록 도와준다.

4. 논점 도표화

단일한 가설을 엄격하게 논리 검증하는데 활용할 수 있는 방법이다. 논점과 증거를 구조화한 시각적 표현은 분석 판단을 평가하기 쉽게 한다. 논점 도표화는 경쟁가설분석에 대한 논리적인 추구 방식이다. 단일의 가설을 위해 그리고 이에 반하는 논점의 구체적 표현이며 한편 경쟁가설분석은 다양한 가설들의 좀 더 일반적인 분석이다. 경쟁가설분석에 의해 선호된 가설에 대한 논점 도표화의 적절한 적용은 양 분석의 결과에 신뢰를 증가시킬 것이다.

5. 기만탐지

외국 정보기관, 경제적 경쟁상대 또는 다른 적대적인 기관에 의한 기만 가능성은 분석관이 고려해야만 하는 가설의 특별한 유형이기 때문에 이 장에서 논의된다. 기만 가능성은 경쟁가설분석에서 하나의 가설로서 포함될 수 있다. 기만탐지 기법을 통해 확인된 첩보는 경쟁가설분석 매트릭스에서 관련된 첩보로 입력될 수 있다.

Ⅷ. 인과관계의 평가(Assessment of Cause and Effect)

과거에 발생한 일을 설명하고 미래의 일을 예측하는 것은 기본적으로 인과관계의 연결고리를 잘 이해하는데 있다. 그러나 정보분석에서 다루는 변수들이나 상관관계는 대부분 학술연구에 공통된 실증적 분석이나 이론개발과 같은 것이 아니기 때문에 이해한다는 것이 어렵다.

분석관이 할 수 있는 최선의 것은 잘 알고 판단을 하는 것인데 그러한 판단은 분석관의 주관적인 전문지식과 추론능력에 달려 있기 때문에 여러 가지 인지적 함정과 추론의 오류에 빠질 위험성이 있다. 정보실패를 초래하는 가장 흔한 원인 중의 하나는 거울이미지(Mirror Image)인데 이것은 마치 다른 나라의 지도자들도 우리 자신과 유사한

상황에서는 똑같이 행동할 것이라고 무의식적인 가정을 하는 것이다. 정보실패를 초래하는 또 하나의 원인은 어떤 사람, 조직 또는 정부의 행위가 마치 전적으로 그 행위자의 성격에서 기인하는 것으로 판단하고 상황적 요인의 영향을 과소평가하는 경향이 있다. 이와 반대로 사람들은 자신의 행동에 대해서는 거의 전적으로 자신이 처한 상황에 의해 결정되었다고 생각하는 경향이 있다. 이러한 심리현상을 "기본적 귀인 오류"라고 한다.

또한 상대방이 한 행동의 결과는 그들이 고의적으로 의도한 것으로 단정하는 경향이 있는데 그것이 상대방의 단순한 실수, 사고, 의도하지 않은 결과, 우연의 일치 또는 작은 원인에서 비롯되어 큰 사고로 발전했다는 것과 같은 사실은 인정하지 않으려고 한다. 분석관들은 종종 단 하나의 원인만 있을 것으로 생각하여 얼핏 보기에 충분히 개연성이 있는 중요한 요인이 발견되면 더 이상 새로운 조사나 추적을 하지 않고 예단해 버리는 경향이 있다. 인과관계에 대한 인식은 사람들이 관심을 갖는 방향에 다라 결정되는 부분도 있어서 결과적으로 쉽게 구할 수 있거나 사람의 눈길을 끄는 특징이 있거나 새로 입수된 생생한 첩보다 그렇지 않은 것보다 더욱 인과관계가 긴밀하다고 생각되는 경향이 있다.

사람들은 또한 논리적 추론과정에서도 공통적인 실수를 범하는 경향이 있다. 두 개가 동시에 발생하거나 또는 어떤 것에 이어 곧바로 다른 것이 발생하면 사람들은 그 둘이 상관성이 있다고 단정하는 것이다. 이 때 우리는 어떤 것이 다른 것의 원인이라고 가정하게 되는데 상관관계를 인과관계로 간주해서는 안 된다. 제3의 다른 요인이 그 둘의 직접적인 원인 될 수도 있기 때문이다.

인과관계에 대한 판단을 할 때 개입되는 이와 같은 인지적 오류의 위험성을 경감시킬 수 있는 쉬운 방법은 없다. 왜냐하면 분석관들은 보통 인과관계 확신에 필요한 정확한 정보가 부족하기 때문이다. 더구나 정보분석의 대상이 되는 복잡한 사건들은 그 자체로 하나의 요인이

아닌 여러 요인들이 복합적으로 상호작용하여 발생하는 경우가 많다.

상기 분석기법들을 적절하게 활용하면 여러 가지 공통된 인지적 제한 요인들을 감소시키고 분석관들의 올바른 분석 가능성을 증대시켜줄 것이다. 다음 항목은 정보분석관들이 현재 발생한 사건의 원인을 분석하려고 하거나 미래에 발생할 사태에 대한 예측을 시도하려고 할 때 활용할 수 있는 핵심전략에 대하여 상세하게 설명한다.

1) 상황적 논리(Situational Logic)

잘 알려진 사실과 특정한 시점이나 장소에서 작용하는 기본적인 요소들에 대한 이해를 기초로 전문적 판단을 하는 것이다. 분석관이 불완전하고 애매모호하며 기만 가능성까지 있는 첩보를 기초로 분석을 할 때에는 관심 국가의 의도, 능력, 업무의 정상적 작동을 가정하고 전문적 판단을 내리는 것이 일반적이다.

2) 역사적 상황과의 비교(Comparison with Historical Situations)

특정 상황과 관련된 사실을 잘 이해한 다음 이러한 이해를 바탕으로 과거 자신의 개인적 경험이나 역사적 사건에 비추어 유사한 상황에서 발생했던 과거사례를 결합하는 것이다. 이 전략은 유추법(Analogies)을 사용하는 것이다.

3) 이론의 적용(Applying Theory)

동일한 현상이 나타나는 여러 사례들을 체계적으로 연구한 결과를 근거로 판단하는 것을 말한다. 실증적 연구조사에 기초한 이론이나 모델은 특정한 유형의 사건이 언제, 어떻게 발생하는지를 설명하는데 사용된다. 많은 경우 학문적 모델들은 너무 일반화되어서 독특한 성격을 가지고 있는 대부분의 정보문제에 적용하기 어렵다. 그러나 관련 변수들을 확인하고 이러한 변수들이 특정한 결과를 초래할 수 있는 다양한

결합방법을 찾아내는 개념적 모델(Conceptual Model)의 경우에는 일반적인 유형의 문제에 대한 수집과 분석을 안내할 수 있는 견본(Template)으로서의 역할을 할 수 있다. 외생변수 통합사고(Outside-In Thinking)는 이와 같은 방법으로 현재의 사건을 설명하고 미래를 예측하는데 사용될 수 있다.

1. 핵심가정 점검 (Key Assumptions Check)

중요한 분석기법으로서 가장 많이 사용되는 기법의 하나이다. 분석적 판단은 항상 증거와 그 증거가 어떻게 해석되는지에 영향을 미치는 가정 또는 예상의 조합에 기초한다. 핵심가정 점검은 분석관들의 사고를 안내하는 가정 즉 관념적 모형(Mental Model)을 명확하게 하고 그것을 의심해 보고자 하는 체계적인 노력이다.

2. 구조화 유추(Structured Analogies)

유추를 통해 추론과정에 분석적 치밀함을 증대시키는 방법이다. 이 기법을 적용하려면 분석관이 관심문제와 가장 유사한 환경을 가진 하나의 문제를 선택하기 전에 유추를 적용할 수 있는 여러 개의 잠재적 사례들을 체계적으로 비교하는 것이 필요하다. 사람들이 어떤 결정을 내리거나 미래를 예측할 때 유추한 사례들은 과거 유사한 상황에서 발생한 것에 대한 정보를 포함하고 있기 때문에 유추를 통해 설명하는 것은 자연스럽게 보인다. 사람들은 패턴을 인식하기 되면 의식적으로 과거의 경험에서 성공적이었던 행동은 취하고 실패했던 행동은 피하려고 하는 경향이 있다. 그러나 분석관들은 어떤 문제에 대해 판단을 할 때 자신의 과거에 가졌던 생각을 지지하는 첫 번째 유추에 집착하는 강한 경향이 있는데 이를 극복해 나갈 필요가 있다.

3. 역할 연기(Role Playing)

실제 사건이나 또는 최근에 발생하여 관계자들이 대응할 필요가 있

는 사건에 대해 새로이 전개될 가상적인 사태의 진전을 다루는 것이다. 이러한 형태의 역할연기 기법은 대부분의 군사게임(Military Gaming)과는 달리, 거의 사전 준비 없이 하루 또는 이틀에 수행할 수 있다. 아주 간단한 역할연기 실행만으로도 현재의 복잡한 상황이 향후 어떻게 진전될지에 대해 창의적이고 체계적인 생각을 촉진시킬 수 있다. 역할연기기법은 또한 동일한 문제를 다루고 있으면서도 같은 공간에서 의견을 나눌 수 없었던 서로 다른 공간의 분석관들이 자신들의 관점을 제기하고 토의할 수 있는 효과적인 방법이기도 하다. 중요한 결정을 해야 하는데 시간은 없을 때 분석관들과 정책결정자들이 한자리에 모여 역동적으로 문제해결에 나설 수 있게 도와준다.

4. 레드 햇 분석 (Red Hat Analysis)

다른 사람들이 바라보는 것처럼 위협과 기회를 인식하고자 할 때 효율적인 방법이다. 정보 분석관들은 자주 외국의 지도자, 조직, 기관, 국가의 행위를 예측하고자 하는 경우가 있다. 이 경우 분석관들은 다른 사람들도 그들과 같은 방식으로 세상을 생각하고 인식할 것이라고 하는 거울 이미지(Mirror Imaging)라는 일반적인 오류를 피할 필요가 있다. 다만 레드 햇 분석은 해당 국가나 관련된 사람들에 대해 의미 있는 문화적 이해를 하지 않기 때문에 이용가치가 제한된다.

5. 외생변수 통합사고(Outside-in Thinking)

특별한 관심이슈에 영향을 미칠 수 있는 모든 요인들에 대하여 분석관의 사고 폭을 넓혀준다. 이 기법은 분석관으로 하여금 자신들의 전문영역을 넘어서지만 분석주제에 영향을 미칠 수 있는 광범위한 사회적, 조직적, 경제적, 환경적, 기술적, 정치적, 법적 그리고 글로벌한 요인이나 트렌드에 대해 보다 폭넓게 사고할 것을 요구한다.

Ⅸ. 이의 분석(Challenge Analysis)

이의 분석은 반박분석(Contrarian Analysis), 대안분석(Alternative Analysis), 경쟁분석(Competitive Analysis), 레드 팀 분석(Red Team Analysis) 그리고 악마의 변론(Devil's Advocacy)이라고 불리는 일련의 분석기법들을 모두 포함하는 것이다. 이 분석기법들의 공통점은 확립된 관념적 모형(Mental Model)이나 합의된 분석결과(Analytic Consensus)에 도전하게 함으로써 분석하고 검토한 결과를 보다 폭넓게 설명하거나 평가할 수 있도록 하는 점이다. 동일한 활동이 이처럼 다양한 이름으로 불리어 왔다는 것은 이 기법들이 어떻게 그리고 왜 사용되어 왔고 이것을 통해 무엇을 얻을 수 있는지에 대해 개념적 다양성이 있다는 것을 의미한다.

미국 정보공동체에서 합의된 판단(Consensus Judgement)이나 오랜 기간 확립된 관념적 모형(Long-Established Mental Model)에 대해 의문을 제기하는데 실패하는 것이 대부분의 심각한 정보실패의 한결같은 모습이라고 널리 인식되어 있다. 진주만사건 이래 거의 모든 미국의 정보실패 사례에 대해 사후부검분석(Postmortem Analysis)을 한 결과, 정보실패를 초래하는 핵심요인은 분석적인 관념적 모형(Analytic Mental Model)이라는 것을 확인하였다. 상황이 변화하였으나 과거의 경험에 기초한 분석관의 관념적 모형은 변화를 따라가지 못하거나 변화가 일으키는 파문을 파악하지 못하였다.

분석실패에 대한 이러한 기록은 "전문성의 모순"에 대한 논의를 불러왔다. 전문가들이 변화의 실체와 의미를 인식하는데 가장 늦을 수 있다. 예를 들면 중동 전문가들은 아랍의 봄을 예측하지 못했고 소련의 전문가들은 소련의 붕괴를 예측하지 못했으며 독일 전문가들은 독일의 재통일 움직임을 가장 늦게 받아들였다. 한국전쟁을 돌이켜 보면 중국 전문가들은 중국이 참전할 때까지도 참전하지 않을 것이라고 하였다.

분석관의 관념적 모형은 분석관이 특정 국가나 특정 분야에서 정상적으로 일이 진행되는지 여부를 판단하게 해주는 여과장치로 간주할 수 있다. 이것은 종종 분석관에게 무의식적으로 무엇을 찾아야 하고 무엇이 중요하며 자신이 보고 있는 것을 어떻게 해석해야 하는지에 대해 알려준다. 교육과 경험을 통해 형성된 관념적 모형은 하나의 필수적인 기능을 수행한다. 이것은 분석관이 현재 진행 중인 사건을 평가하거나 장차 발생할 사건을 예측하는 것과 같이 매일 수행하는 업무를 합리적이고 직관적으로 처리할 수 있게 해준다.

수년에 걸쳐 정확한 평가를 제공하였던 관념적 모형은 변화에 대해 대응이 늦어질 수 있다는 문제가 있다. 내용이 조금씩 변화하는 정보들이 시간을 두고 입수되게 되면 쉽게 기존의 관념적 모형에 융합되게 되는데 이렇게 되면 일정한 시간에 걸쳐 진행된 변화의 의미를 파악하기 어렵게 된다. 미래를 과거의 연장선으로 보려는 것은 인간의 본성이다. 커다란 흐름이나 사건은 천천히 진전되어 나가는 것이 일반적이기 때문에 훈련된 정보분석관이 아니면 미래를 예측하기 어려울 수도 있다. 그러나 우리의 일상생활이 항상 이런 식으로 이루어지는 것은 아니다. 가장 심각한 정보실패는 역사가 급변하여 방향을 바꿀 때 이러한 역사적 불연속성을 예측하지 못한 것이다. 2010년 미국 금융위기를 예측하지 못한 경제전문가들에게도 똑같이 말할 수 있다.

세상을 다른 관점에서 점검할 수 있는 상상력이 발휘될 수 없다면 이러한 놀라운 사건들을 예측하는 것은 어려운 일이다. 분석관으로 하여금 종전과는 다른 관점에서 사건을 평가하도록 하는 것인데 다른 말로 하면 다른 관념적 모형으로 사건을 평가하도록 하는 것이다.

또한 전통적인 지혜에 지속적으로 도전하여야 할 또 다른 논리적 이유가 있다. 전 CIA 국장이었던 마이클 헤이든은 “우리의 업무는 본질적으로 불문명하고 때로는 의도적으로 숨겨진 주제들을 다루는 것이다. 우리가 업무를 원활하게 수행하여 실제로 정책결정자에게 통찰력을 주고 흐름을 알려주고 이슈에 대해 분명한 모습을 제공했다고 하더

라도 우리의 판단에 대해 확실하다고 주장할 수는 없다"고 하였다. 헤이든 국장은 또한 10년 중에 7번을 맞히는 정도가 현실적인 기대치가 될 것이라고 하였다.

헤이든 국장이 말한 10번 중에 7번이라는 평가는 정보보고서에서 사용되는 가능성에 대한 언어적 표현을 살펴보아도 알 수 있다. "가능성 있음"은 정보평가나 예측에 있어서 가능성을 표현하는 가장 일반적인 언어적 표현이다. 불행하게도 "가능성 있음"을 포함하는 가능성을 표현하는 다양한 언어적 표현들이 수치로 전환될 경우 몇 퍼센트가 될 것인지에 대해서는 정보공동체 아원의 합의가 없다. 논의의 편의를 위해 여기에서는 셔먼 켄트의 정의에 따라 "가능성 있음"을 "75%에서 플러스 또는 마이너스 12%"를 의미하는 것으로 보기로 한다. 이것은 "가능성 있음"이라고 기술된 분석적 판단이 대략 그 시점에서 75%의 정확도를 가진 것으로 예상된다는 것이고 그러므로 25% 정보는 틀릴 수 있다는 것이다.

따라서 논리적으로 보면 정보분석관들이 "가능성 있음"이라고 기술하는 네 번의 판단 중에 한 번은 틀릴 수 있다는 것을 의미한다. 이런 측면이 바로 이의 분석(Challenge Analysis)이 성취할 수 있는 범위를 보여주고 있다. 이의 분석은 옳다고 확신하는 지배적인 견해에 대해 의문을 제기하는 역할만 하는 것이 아니다. 비록 이의 분석이 최초의 가능성 판단을 확신한다고 하더라도 나머지 25%의 확률에 대해 더 잘 이해하기 위해 노력해야 한다. 어떤 상황에서 전혀 다른 평가나 결과가 발생할 수 있고 그 평가나 결과는 무엇일까? 사건이 대안적인 방향으로 진행되고 있다는 것을 보여주는 증거에는 어떤 것이 있고 이러한 증거는 어떻게 나타날 것인가? 갈등관리에 있어서 이러한 확률에 대해 이해하는 것은 대립되는 의견을 둘러싸고 비생산적인 갈등이 발생할 가능성을 감소시켜 준다. 네 번 중의 한 번은 틀릴 가능성이 있다는 것을 인식하는 분석관은 나머지 25%를 설명할 수 있는 대안적인 평가들에 대해 최소한 개방적인 생각을 가져야 한다.

1) 자기비판(Self-Critique)

분석관으로 하여금 자신의 사고에 도전하도록 도와주는 기법에는 사전부검 분석(Premortem Analysis)과 구조화 자기비판(Structured Self-Critique)이 있다. 이 기법들은 다른 의견의 표출을 억누르고 순응하거나 합의하도록 압박하는 분석 팀 또는 그룹 내의 압력에 대항할 수 있게 해준다. 비즈니스 세계에서 활용되는 사전부검 분석을 발굴하여 보다 광범위한 정보분석 과정에 적용하였다.

2) 다른 사람에 대한 비판(Critique of Others)

분석관들은 발생가정 분석(What if? Analysis)이나 고충격·저확률 분석(High Impact·Low Probability Analysis)을 이용하여 대안적인 설명이나 결과를 제시함으로써 전통적 견해에 대해 적절한 의문을 제기할 수 있다.

3) 다른 사람에 의한 비판(Critique by Others) :

다른 사람에 의한 비판을 이끌어내는 데에는 몇 가지 기법이 이용될 수 있다. 그 중에서 "악마의 변론"(Devil's Advocacy)이 가장 잘 알려진 기법이다. "레드 팀"(Red Team)이라는 용어는 적의 관점에서 분석하는 임무를 부여받은 그룹을 표현하기 위한 것이다. "델파이 기법"(Delphi Method)이란 외부전문가 토론자로부터 의견을 도출하기 위한 구조화 과정이다.

1. 사전부검 분석(Premortem Analysis)

사전부검(사전 실패가정) 분석은 잠재적 실패요인을 확인하고 분석함으로써 실패가 발생하기 이전에 분석실패의 위험성을 감소시켜 준다. 분석관 스스로 몇 년의 경과한 미래를 상상해 본다. 분석관은 갑자기 자신이 한 분석이나 예측 또는 전략기획이 잘못되었다는 사실을 확실

한 출처를 통하여 알게 되었다. 그리고 무슨 일이 발생하면 잘못될 수 있는지 상상해 보는 것이다. 미래의 시점에서 이미 발생한 어떤 일을 설명하는 것이 장차 발생할 일을 예측하는 것보다 훨씬 쉽기 때문에 이러한 기법을 실행하면 예견할 수 없었던 문제를 확인하는데 도움이 된다.

2. 구조화 자기비판(Structured Self-Critique)

구조화 자기비판은 소규모의 팀이나 그룹이 자신들이 실시한 분석의 약점을 확인하기 위한 절차이다. 모든 팀원들이나 집단의 구성원들은 가상의 검은 모자(Hypothetical Black Hat)를 쓰고 자신들의 분석결과에 대해 지지자의 입장보다는 비판자의 입장이 된다. 이러한 반대편의 관점에서 출처의 불확실성, 사용된 분석절차, 중요한 가정, 증거의 진단성(Diagnosticity), 특이한 증거, 첩보 괴리(Information Gap), 사건과 관련된 광범위한 환경의 변화, 대안적 의사결정 모델, 문화적 전문지식의 활용 가능성, 기만 가능성이 있는 지표 등에 대해 질문을 한다. 이러한 의문사항들을 점검하면서 팀원들은 자신들의 판단에 대해 전반적인 신뢰도를 재평가한다.

3. 발생가정 분석(What If? Analysis)

발생가정 분석은 당시에는 발생할 것 같지 않지만 발생할 가능성이 있거나 실제로 이미 발생하기 시작한 사건에 대해 정책결정자에게 경고를 할 수 있는 중요한 기법이다. 이것은 정책결정자들의 판단이 틀릴 수도 있다는 가능성을 깨우치게 하는데 적절한 방법이다. 발생가정 분석은 시나리오 분석(Scenarios Analysis)과 유사한 기능을 수행하는데 중요한 변화의 초기 징후들을 인지할 수 있는 마음의 준비를 하도록 하고 만일의 사태가 발생하기 이전에 의사결정자가 대비책을 마련할 수 있도록 해 준다. 분석관은 어떤 사건이 발생하였다고 상상하고 어떻게 전개될 것인가를 검토한다.

4. 고충격・저활률 분석(High Impact・Low Probability Analysis)

고충격・저활률 분석은 분석관과 의사결정자로 하여금 발생할 가능성이 낮은 사건에 대해서 민감하게 대응하게 하고 실제로 사건이 발생할 경우 위험에 대비하거나 기회를 활용할 수 있는 방법을 강구하도록 하는 방법이다. 분석관들은 사건이 발생했다고 가정하고 어떻게 해서 사건이 발생할 수 있었으며 그 파급영향이 어떻게 될 것인지를 파악해야 한다.

5. 악마의 변론(Devil's Advocacy)

악마의 변론은 권한 있는 책임자로부터 악마의 변론가로 지명된 사람이 기존의 분석적 판단, 계획, 의사결정에 대해 비판적으로 최선의 방안을 만들어내는 기법이다.

6. 레드 팀 분석(Red Team Analysis)

특정 이슈와 관련하여 적이나 경쟁자가 어떻게 생각할지에 대해 판단한 전통적 견해에 도전하기 위해 필요한 문화적 요소를 포함한 다양한 분석기법을 망라하여 관리되고 추진되는 일종의 프로젝트이다.

7. 델파이 기법(Delphi Method)

델파이 기법은 지리적으로 흩어져 있는 전문가 패널로부터 전자적 수단을 통해 아이디어, 판단, 전망 등을 획득하기 위한 절차이다. 이것은 전문가의 판단이 도움이 되는 어떠한 주제에 대해서도 활용할 수 있는 오랜 시간에 걸쳐 검증된 유연한 절차이다. 이것은 어떤 조사결과를 재확인하는 방법으로도 사용할 수 있다. 만약 서로 다른 분석기법을 사용하는 다른 분석관들로부터 동일한 분석결과가 도출되었다고 한다면 이것은 그 결론에 대한 신뢰도를 크게 증가시키는 근거가 된다. 만약 두 개의 결론이 서로 일치하지 않는다고 한다면 이것은 새로

운 연구를 시작하게 되는 가치 있는 정보가 될 것이다.

X. 갈등관리(Conflict Management)

이견분석은 반대의견을 확인하고 대립하게 되는 일이 빈번하게 일어난다. 결국 그것이 이견분석의 목적이다. 그러나 이것은 두 가지 중요한 의문을 제기한다. 첫 번째는 이러한 대립이 적들 사이의 싸움이 아니라 학습경험이 될 수 있도록 어떻게 관리할 것인가 하는 것이다. 두 번째는 불확실성이 높은 주제를 분석하는 과정에서 어떤 의견이 틀렸다거나 두 의견 모두 보고서에 담을 가치가 있다고 할 경우에 이것을 어떻게 결정할 수 있느냐 하는 것이다.

하버드 비즈니스 리뷰에 게재된 한 논문은 서로 다른 이해관계를 가진 조직 또는 조직단위 사이에는 불가피하게 때로는 바람직하다고 할 수 있는 갈등이 발생하게 되는데 이러한 갈등을 받아들이고 적극적으로 관리할 때 협력이 증진된다고 강조하고 있다.

의견 불일치를 다루는 가장 일반적인 절차는 의견일치를 강요하거나 차이점을 희석시키거나 미국 정보공동체처럼 평가보고서에 반대의견을 각주로 달게 하는 것이다. 그러나 정보분석 공동체들(Analytic Communities)이 끝가지 자신의 입장을 고수하다가 결국은 마지막 단계에서 억지로 조정당하는 것보다 분석의 초기단계에서 공동작업을 수용하여 의견 불일치를 효과적으로 다룰 수 있게 되는 것이 바람직할 것이다. 기관 내 또는 기관 간 협력을 위해 구조화 분석기법을 사용하는 장점 중의 하나는 이 기법들이 분석과정의 출발점에서 의견 차이를 확인할 수 있게 해 준다는 것이다. 이것은 관리자들이 관여하기 전에 실무 수준에서 서로의 의견 차이를 해소하지는 못하더라도 최소한 이해할 수 있는 시간을 제공한다.

서로 상반되는 정보평가나 예측평가를 어떻게 다룰 것인가 하는 문

제는 무엇을 성취할 수 있을 것인가 하는 기대에 따라 달라질 수 있다. 다른 어떤 분야보다도 정보 분석관은 전형적으로 불완전하고 애매모호하며 잠재적인 거짓증거들로 업무를 한다. 게다가 정보 분석관은 자신과 같은 문화권에서도 예측하기가 어려운 인간 행태(Human Behavior)를 이해하여야 한다는 점을 생각하면 정보분석이 가끔 틀렸다고 판명되는 것은 그리 놀라운 일이 아니다. 정보분석관은 기본적으로 불확실한 일을 다루기 때문에 그들이 불확실한 것도 어쩔 수 없다는 원칙을 수용하는 것은 서로 상충되는 의견을 적절하게 관리할 수 있는 장을 마련하는데 도움이 된다. 어떤 경우에는 하나의 입장이 반박되고 기각될 것이다. 또 다른 경우에는 보통은 그 중 하나가 다른 것보다 더 가능성이 높지만 두 개 이상의 입장이 합리적인 정보평가나 예측평가로 인정될 수 있을 것이다. 그러한 경우 각자의 입장이 선택 가능한 방안의 범위 내에 있다고 인정을 받게 된다면 갈등은 완화될 것이다.

"가능성 있음"이라고 기술된 정보평가나 예측평가는 네 번 중에 하나가 틀릴 가능성을 의미한다고 하였다. 분석관들의 상반된 의견 때문에 이러한 표현을 사용하게 되었다면 이것은 적절한 조치가 필요하다는 것을 암시하는 것이다. 만약 어떤 정보분석이 엄밀한 기준에 따라 진행되었으나 여전히 반대의견이 남아있다고 하면 이것은 적절한 조치가 필요하다는 것을 암시하는 것이다. 만약 어떤 정보분석이 엄밀한 기준에 따라 진행되었으나 여전히 반대의견이 남아있다고 하면 정책결정자에게 불확실성을 최소화하거나 은폐한 보고서를 제출하기 보다는 오히려 불확실성 자체를 직접 다룬 보고서를 제출하는 것이 도움이 될 것이다. 불확실성이 커지면 거질수록 가장 가능성 높은 정보평가 또는 예측평가가 포함되어 있고 하나 이상의 대안적 방안이 제시되어 있는 보고서를 기초로 불확실성을 해결하기 위한 노력을 하는 것이 더욱 적절하기 때문이다. 불확실성의 정도를 평가할 때 고려해야 할 요인들은 다음과 같다.

1) 미래상황에 대한 예측평가가 일반적으로 과거나 현재사건에 대한

정보평가보다 더 불확실하다.

2) 정답이 없는 미스터리가 정답이 존재하여 찾을 수 있는 퍼즐보다 훨씬 불확실하다.

3) 만들어진 가정들이 많을수록 불확실성도 커진다. 의도와 능력에 대한 가정들은 그것들이 변화하였든 변화하지 않았든 중요하다.

4) 인간의 행태나 정책결정에 대한 분석은 기술적 자료의 분석보다 훨씬 더 불확실하다.

5) 복잡한 역학관계가 작동하는 시스템이 단순한 시스템보다 더 불확실하다. 시스템의 변수와 이해관계자가 많을수록 무슨 일이 발생할지 예측하는 것이 어려워진다.

만약 대안적 정보평가 또는 예측평가를 기초로 토론을 진행하여 의사결정하기로 정하였다면 다음과 같은 사항을 작성하도록 한다.

1) 하나의 보고서에 상충되는 의견을 비교 분석하여 제시

2) 대안 시나리오 분석

3) 발생가정 분석 또는 고충격・저확률 분석

4) “두 번째 의견”(Second Opinion)이라고 명시된 보고서

1. 대립적 공동작업(Adversarial Collaboration)

대립적 공동작업은 의견이 상충되는 집단들이 어떻게 서로 협력하여 차이점을 해소하고 의견이 다른 이유를 이해하며 그 차이점을 설명하는 보고서를 공동으로 작성할 것인가에 대해 합의하는 절차이다.

2. 구조화 토론(Structured Debate)

구조화 토론은 특정한 이슈에 대해 상충되는 관점을 가진 집단들이 “동료 배심원”(Jury of Peers), 선임분석관 또는 고위관리자들 앞에서 진행하는 기획된 토론이다. 첫 단계에서 양측은 각자 자신의 입장에 대한 최선의 변론서를 작성하여 다른 상대방에서 전달한다. 다음 단계에서는 자신들의 주장을 옹호하기보다는 상대방의 주장을 반박하는데 집중하여 구두 토론을 벌인다. 그 목적은 서로의 주장을 이해할 수 있도록 설명하고 서로 비교하는 것이다. 만약 어떤 측의 주장도 서로 반박하기 어렵다고 한다면 양측의 주장 모두 보고서에 반영할만한 가치가 있다는 것을 의미할 것이다.

Ⅺ. 효과적인 Intelligence 보고서 작성 원칙

상기의 과정을 통해 수집·분석한 자료들을 정책결정자들에게 효과적으로 보고하기 위해서는 다음과 같은 보고서 작성 원칙을 준수할 것을 권장한다.

1) 원칙 1 : 주요 사항을 두괄식으로 작성한다.

2) 원칙 2 : 근거를 제시한다.

3) 원칙 3 : 능동태를 사용한다.

4) 원칙 4 : 짧고 쉬운(명확한) 단어를 사용한다.

5) 원칙 5 : 짧은 문장으로 쓴다.

6) 원칙 6 : 정확하고, 신뢰할 수 있고, 완결되게 작성한다.

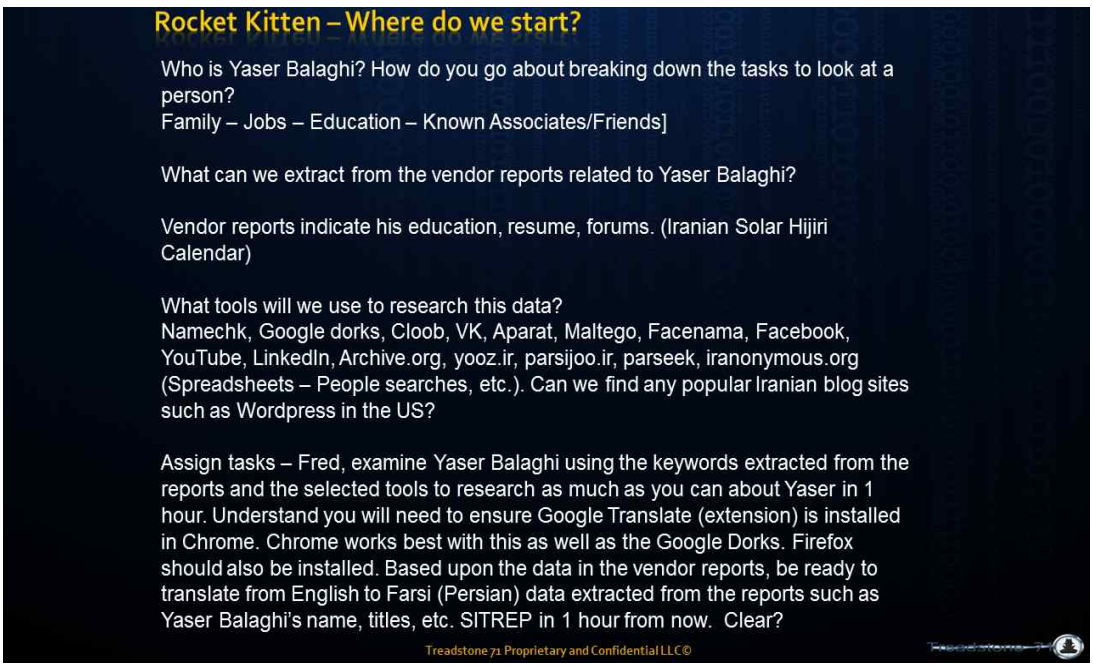
Ⅻ. Case Study : Rocket Kitten Group 사례

2014년 초부터 이란에 기반한 해커 그룹이 특정 개인을 타겟으로 malware infection 등을 통해 활동해 왔다. 이 사이버 스파이 그룹은 'Rocket Kitten'이라 불리고 있다.

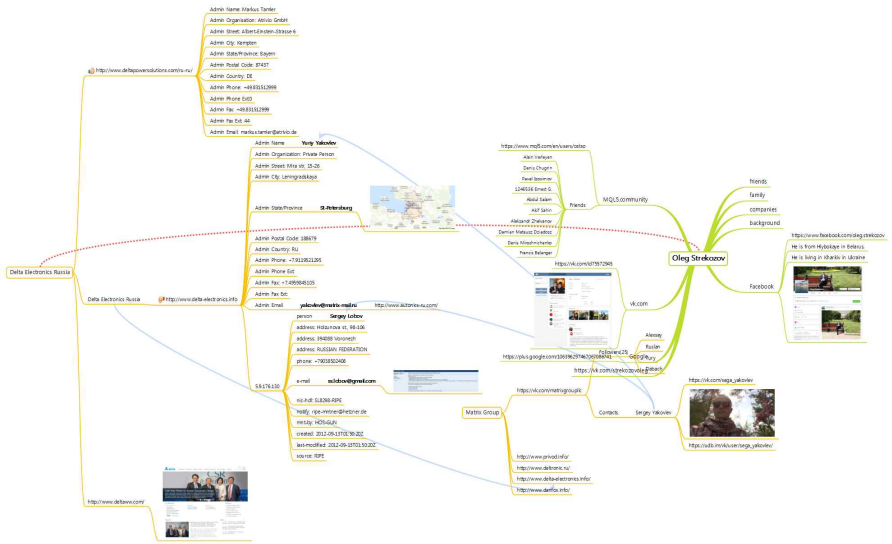
Rocket Kitten이 금융회사 A의 사이버 보안에 위협이 될지 여부를 판단하여 보고하기 위해, 팀별로 Rocket Kitten 및 배후 인물이라 추정되는 Yaser Balaghi 등에 대해 주요기관 보고서, 페이스북 등 SNS, 인터넷 자료 등을 검색하고, Rocket Kitten의 활동 목적에 대한 가설을 세워 검증함으로써 사이버 보안 분석 보고서를 작성한다.

분석 툴 : vendor reports, Namchk, Google dorks, Cloob, Maltego, Facenama, Facebook, YouTube, Linkedln, Archive.org, yooz.ir, parseek, iranonymous.org 등

<케이스 스터디 실습 과제>



< Brainstorming >



<가설 수립 및 검증을 위한 Collection Plan 작성 예시>

F2 | Specific Information Requirement

Priority Intelligence Requirement - Priority Level (1-5 with 1 being the highest)	Priority Intelligence Requirement	Type	Observable	Specific Information Requirement	Detection Point	Strategic	Operational	Tactical	Technical
1	Provide a list of adversaries and their capabilities for DDoS'ing our environment	Standing order One time Urgent	Unusually slow network performance (opening files or accessing websites)	How long with the attack go on for? Will our customers be impacted by the slowness?	Website logs - Firewall	Impact to the business, strategy development, non-technical, geo-political aspects, trends and patterns	Adversary identification, motives, adversary centers of gravity, impending or under attack status	TTPs	Indicators of Compromise
			Unavailability of a particular website	When will the website be back online?	IPS detection of the attack				
			Inability to access any website	Are the adversaries asking for anything in return for stopping the attack?	Routers and Switches with ACL capability				
			Dramatic increase in the amount of spam you receive in your account	Are the adversaries trying to phish us and send other malware via email?	Application front end hardware packet analysis				

Internal Sources	Open Sources	Vendor Sources
Define log files, aggregators, SIEMS, HUNT/Detect, Big Data, Business Units. Orchestration - validate sensor viability, monitoring functionality. Ensure awareness of technology maintenance, upgrades, change/release management.	Existing sources - New Sources - Passive - Darknet - Non-English language, Persona usage	Assess your vendors for credibility and reliability. Analyze vendors for type of data

Intelligence Components

Priority Intelligence Requirement -	Priority

Priority Intel Req (PIR) / Collection Plan / Sheet1

제 3장. 씨티은행 CSFC(Cyber Security Fusion Center)

Ⅰ. 개 요

□ 글로벌 금융서비스 그룹인 미국 씨티은행의 금융전산 보안 운영 사례를 통해 민간 영역에서 사이버 침해위협에 대응하여 어떻게 정보들을 수집하고 분석, 공유, 대응하는지 현황을 파악하고자 함

□ 또한, 최근 사이버 범죄의 변화 양상과 이에 따른 사이버 보안 관리 발전 방향도 점검

Ⅱ. 사이버 보안[4)]

1. 사이버 보안 관련 중요사항

□ 사이버 공격의 빈도, 스피드, 효과는 계속 증가하고 있음

□ Bad Actors : 사이버 범죄자, 민족 국가, 사이버 테러리스트, 핵티비스트를 포함. 그러나 내부 위협에 대해서도 신경써야 함. APT는 대부분 민족 국가이며, 일부 범죄자들은 유사한 특성을 보임

□ 사이버 시큐리티 단의 방어전략 : 강력한 예방 요소를 가져야 함, 단 어떤 기관/회사도 예방 전략만으로 100% 성공적일 수는 없음. 감지 능력과 대응 능력이 동일하게 critical함

□ 위협과 싸우기 위해 필요한 것들 : 인적 자원, 프로세스, 기술

---

4) Elizabeth Petrie 외 2인, “From Cybercrime to Espionage: What Treasurers Need to Know About the Cyber Threat Landscape”, Citi’s Treasury and Finance Conference 2017,
https://www.citievents.com/metron/(medialibrary)/97f16f50-fbf4-437c-8789-ecfb511248d7/meetings/17ada0d1-f144-4b6d-b427-8f41e38b054b/documents/1515.pdf

□ 시큐리티는 진화해야 하고 신규 사이버 리스크에 적응해야 함

□ 정보를 공유하는 파트너쉽을 구축하고 그 안에서 협력하는 것이 end-to-end 시큐리티를 유지하는 핵심임

2. 사이버 공격의 비즈니스 영향도

□ $ 2조 : 2019년까지 글로벌 사이버 범죄에 따른 비용 발생 추정치

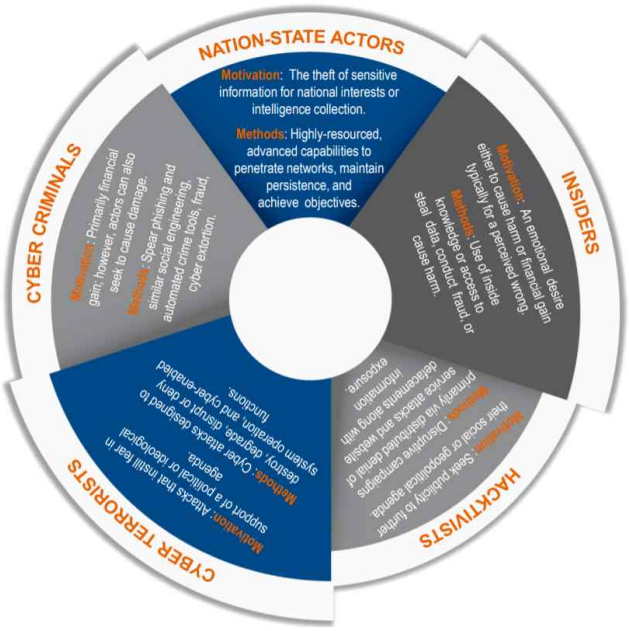
□ $ 4천억 : 2015년 지적 재산의 도난에 따른 연간 추정 손실

□ $ 3600만 : 2015년 기업들의 사이버 범죄에 따른 비용

- 미국 $ 1,540만, 독일 750Germany $ 750만
- 일본 $ 680만, 영국 $ 630만

3. 사이버 범죄자 유형

□ 사이버 범죄자, 민족국가 활동가, 사이버 테러리스트, 핵티비스트, 내부자 등



4. 금융분야 APT(Advanced Persistent Threat)의 동기 변화

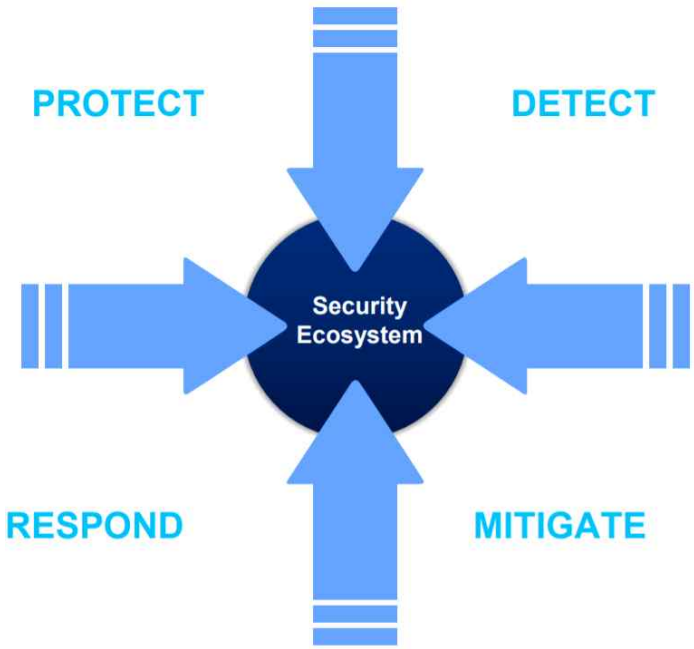
□ 금전 탈취 → 데이터 파괴 → 고객 신뢰 파탄 [1]

□ 1회성으로 끝날 수도 있는 금전 탈취에서 비즈니스에 장기간 치명적 타격을 미치는 고객 신뢰 파탄으로 동기가 변화함

□ 이에 따라, 더 신중하고 체계적이고 지속적인 대응 필요

5. 공격자보다 앞서가기

□ 보호, 감지, 대응, 완화 과정의 지속적 수행 및 생태계 내 내재화 필요



6. 리스크 노출 방지를 위한 체크리스트

□ 취약점과 리스크 평가

- 크리티컬한 프로세스와 데이터를 관리하는 3rd 파티 시스템에 대한 취약점/리스크 평가는 빈번하게 수행, 검토되어야 함

- 리스크 레벨에 따라 내부 뿐 아니라 외부 평가도 진행 필요

- 식별된 갭 들은 개선/수정 및 추적되어야 함

□ 고 위험 정보/기능에 대한 보호

- 지적 재산, 개인정보, 거래 정보 등 리스크가 큰 정보/기능은 보호되어야 함

- 중요 데이터들이 공격자 들의 손에 들어갔을 경우에 비즈니스에 미치는 금전적·평판상 영향 고려 필요

□ 직원의 주의 의무(Employee Due Diligence)

- 시스템과 데이터에 접근하는 3rd 파티 직원에 대해, 개인적 배경 체크, 스태프 순환, 트레이닝, 권한 부여(entitlements), 접근 검토, 강제적/의무적/필수적 결근/부재 시행 등과 같은 엄격한 절차 구축이 필요함

□ 안전한 통신 연결

- 방화벽, 암호화 및 데이터/시스템 보호용 기타 메커니즘 등을 이용한 3rd 파티와의 안전한 통신 연결 필요

- 통신상의 보안에 대한 최소 기준은 최고 경영진 선까지 합의되어야 하고 취약점 평가 시에 포함되어 검증되어야 함

□ 직무 분리

- 고위험(리스크) 활동에 대해서는 직무 분리 체계 구축 필요

- 정책/절차, 패스워드 관리와 이에 대한 감사에 의해 뒷받침되어야 함

□ 시스템 접근 제한

- 고 위험 시스템이 동일 네트워크상의 어디에서 접근 가능해 지고 타 시스템/데이터와 혼합되는지에 대해 고려되어야 함

□ 이슈 관리 계획 및 대응 프로세스

- 이슈 관리 계획 및 대응 프로세스는 모든 데이터/시스템의 위반이나 불법사항의 경우에 행해지고 테스트되어야 함

- 대응 프로세스의 요소에까지 합의를 이루는 것이 중요함

□ 물리적 사이트의 시큐리티 검토

- 메인센터나 백업센터에 대한 최소 기준이 합의되어야 함

□ 개인정보 보유 정책

- 데이터 보유, 저장 및 개인정보보호와 관련된 정책이 수립되고 시행 중이어야 함

- 개인정보 보유 정책은 합의되어야 하고, 어떤 정보가 어디에 얼마나 보관될지에 대해 명확하게 제시되어야 함

7. 사이버 보안 관련 기타 참고사항

□ FS-ISAC : 현재 4천여개의 은행과 정보를 공유 중

□ 대응의 속도가 매우 중요함

- 공격자의 공격 속도는 급격히 가속화 되는 경향이 있음

□ 최근 인터넷을 통해 해킹 대행, 해킹 도구 구매가 용이해짐

- (예) Dark Web
  - · 이메일, SNS 계정 탈취 : $129
  - · 회사 이메일 계정 탈취 : $500
  - · 트로이안 제공 : $5~10
  - · DDoS : 1시간 $5~10, 1일 $30~55
  - · Exploit kit 구매 : Adobe $5000, iOS와 MS Windows용도 구매 가능

Ⅲ. 씨티은행 IT 개요

□ 서비스 제공 현황

- 약 2억의 고객, 160개 국가에 서비스 제공 중
- 물리적으로 98개 국가에서 서비스 제공
- 하루에 $4조 이동 (그 중 모바일 채널로 $2조 이동)

□ 글로벌 데이터 센터

- 약 20개의 데이터 센터 (한국 내 2개)
- 다른 데이터 센터로 DR 전환 가능

- 한국은 개인정보 등 법적인 문제로 2개 데이터 센터(서울, 부산)를 한국에 두고 있으나 메인센터와 DR간 거리가 너무 가깝다는 의견(싱가포르나 홍콩에 구축 희망)

□ 씨티은행 IT 관련 기타 참고사항

- DR RTO(Recovery Time Objective)
  - 업무별로 DR RTO 다름, 중요업무는 Active-Active 구조

- 블록체인 관련
  - 연구소에서 검토 중이나 특별한 적용 사례는 아직 없음

- 클라우드 관련
  - salesforce.com의 프라이빗 클라우드 SAAS 이용
  - 중요 업무를 퍼블릭 클라우드에 올릴 계획은 현재 없음

- 사이버 시큐리티 관련 직원 수
  - 뉴저지 CSFC에 60명 (전체 2000명 이상)

- PKI(Public Key Infrastructure), 인증서 : 인증과 서명에 일부 사용 (양자 컴퓨팅이 PKI 기술을 파괴할까 우려 중)

- ISO/IEC 27001[5] 인증 획득

Ⅳ. CSFC 개요

1. CSFC(Cyber Security Fusion Center) 개요

5) 국제 표준 정보보호 인증으로 정보보호 분야에서 가장 권위 있는 인증방식. 원래 영국표준(BS, British Standard)이던 BS7799이었으나 2005년 11월에 ISO 표준으로 승격됨. 인증 범위는 정보보호 정책, 통신·운영, 접근통제, 정보보호사고 대응 등 정보보호 관리 11개 영역 133개 항목에 대해 얼마나 잘 계획하고 구현하며, 점검하고, 개선하는가를 평가하고 이에 대해 인증을 수여함

□ 사이버 시큐리티 퓨전 센터로 2014년 9월에 설립

□ 13개팀으로 구성된 지능 주도(intelligence-led) 기관

□ 4,700개 고객사 보유

□ 씨티은행 전체의 사이버 공격 관련 예방, 감지, 대응, 복구 등 활동 통합

□ 공격을 예방하고 리스크를 감소시키고 경영진의 의사결정을 돕기 위해, 협업을 통해, 다양한 원천으로부터의 지능·정보를 융합

2. CSFC의 전략적 목표

□ 씨티, 고객, 주요 협력사들에 대한 사이버 공격을 예방하고 감지

□ 씨티의 취약점과 리스크 감소

□ 효과적/효율적 대응 노력을 통한 피해/공격 최소화

□ 배움을 실행으로 전환

3. 전 세계 CSFC 위치

□ 미국 뉴저지, 싱가포르, 헝가리 부다페스트

Ⅴ. CSFC 운영

1. CSFC 조직

※ 총 13개의 팀으로 구성됨 (a Team of Teams)

○ Cyber Intelligence Center
- 정보 수집 공유
○ Advanced Adversary Interdiction
○ Security Incident Management
- 고객에게 신속하게 상황을 전달해주는 역할
- 빠른 복구가 가장 중요함
○ Third Party Information Security Assessment
○ Global Intelligence & Analysis
○ Citi Security Investigative Services
○ Emergency Management
○ Vulnerability Assessment
○ SOC (Security Operation Center)
- 텍사스와 싱가포르에 위치
- 1달간 200억개 사고 발생
- 그 중 800~1000개가 진짜 이벤트임
- 그 중 100개 정도의 이벤트가 CSFC로 옴
○ GCB Fraud
○ CSFC Core Team 등

2. CSFC의 사이버 킬 체인 채택[6)]

□ 킬 체인(Kill Chain)

- 세계적인 군수업체 록히드마틴의 등록상표

- 적의 미사일을 실시간으로 탐지하고 공격으로 잇는 일련의 공격

6) 이대영 기자, "사이버 킬 체인(Cyber Kill Chain)", ITWorld 용어풀이, 2016.08.18., http://www.itworld.co.kr/news/100774#csidx86dfa417c2b750a9e255db2c835528f

형 방위 시스템을 일컫는 용어

- 1991년 걸프전에서 처음 등장하였으며, 이라크 군의 스커드 미사일을 방어하기 위한 선제 공격형 방어 전략

- 날아가는 미사일을 맞추는 것보다 발사하기 전의 미사일 시설을 먼저 타격한다는 것

- 탐지에서 교전까지 소요시간을 얼마나 단축하느냐가 중요

□ 사이버 킬 체인(Cyber Kill Chain) 개요

- APT(Advanced Persistent Threat)라고 불리는 지능형 위협 공격을 설명하는데 주로 사용되는 용어 중 하나

- 사이버 보안 세계에서는 뚫리지 않는 방패는 없다는 것이 정설이 됨(공격자가 충분한 시간과 자원을 갖고 꾸준히 공격한다면 뚫지 못할 시스템은 없으며, 이런 공격을 막아낼 수 있는 조직은 전무하다는 것)

- 따라서 100% 막겠다는 방어 전략은 불가능하며, 해킹 당했다는 가정 속에서 모든 조직의 보안 전략을 세우고 실행해야 함

- 이러한 전통적 보안 전략의 한계로 새로운 방어 전략 필요

- 이런 상황에서 제시된 전략 가운데 하나가 사이버 킬 체인임

- IT 보안 업계에서 공격자가 조직을 공격할 때 쓰는 방법을 7단계로 정의함

□ 사이버 킬 체인(Cyber Kill Chain) 7단계

- 정찰(Reconnaissance)
- 공격코드 제작(Weaponization)
- 전달(Delivery)
- 취약점 공격(Exploitation)
- 설치(Installation)
- 명령 및 제어(Command and Control)
- 목표시스템 장악(Actions on objectives)

□ 사이버 킬 체인 세부내용

- 공격자의 입장에서 사이버 공격 활동을 파악·분석해 공격단계별로 조직에 가해지는 위협 요소를 제거, 또는 완화함

- 록히드 마틴은 이를 침입 타격순환체계(Intrusion Kill Chain)라 칭하였으며, 이후 이 전략은 회사 인프라 보호 계획의 기초가 됨

- 록히트 마틴 백서 : "공격자의 위협 그 자체와 공격 의도, 역량, 원칙, 운영 패턴 등을 이해한다면 전통적인 취약점 중심의 프로세스와 시스템으로도 조직의 회복 탄력성을 확보할 수 있다"

□ 사이버 킬 체인 전략의 목적

- 공격자의 첨단 공격에 대응하고 조직의 회복 탄력성을 구축하기 위해 공격 구성요소를 파악하고, 공격자들의 지속적인 활동에 법적 책임을 지움으로써 공격의 성공 확률을 낮추는데 있음

□ 사이버 킬 전략의 한계에 따른 진화

- 최근 사이버 킬 체인 전략의 한계를 주장하는 보안 전문가가 존재 (보안 컨설턴트 신 말론, 블랙햇 컨퍼런스 2016)

- "사이버 킬 체인의 문제는 방화벽을 침입자에 대한 핵심 방어 수단으로 가정하고 있다는 점이다. 그러나 상황이 완전히 바뀌었다. 기업은 방화벽 내부에 대한 방어를 반드시 강화해야 한다“

- 이는 기존 사이버 킬 체인에 새로운 단계를 더 추가해야 한다는 것을 의미함 (말론의 제안은 전체적인 7 단계는 같지만 대신 그 앞에 ’내부’라는 말이 붙음)

- 이는 공격자가 이미 침입한 것을 가정한 상태에서 공격 단계를 분석한 것

- 보통 방어자가 내부 공격 코드 제작을 막는 것은 힘드나, 시스템과 애플리케이션을 더 단단하게 만들었다면 공격 코드 작성을 조금 더 어렵게 만들 수 있으며 네트워크에 가짜 기기를 추가해 작업을 더 어렵게 만드는 것도 가능함

- 킬 체인의 모든 단계에서 공격 시간을 늦추고 공격을 계속할 경우, 공격비용도 계속 늘어나게 하는 방어책을 마련한다는 것

□ CSFC의 사이버 킬 체인 채택 목표

- 공격자가 공격 체인의 각 단계들을 거칠 때 툴, 테크닉, 프로세스를 노출하여야만 한다는 점을 최대한 이용하는 것이 목표임 [1]

3. 지능 주도

□ 지능 주도(“intelligence-led”)가 장기 성공의 열쇠임

- Know your enemy, Know yourself
- 지능 주도가 단지 사실을 저장함을 의미하지 않음

- 사실을 얻고, 얻어진 사실들을 이용하여 스토리를 만드는 것
- 1개 인시던트를 위협의 끝으로 보는 것이 아니라, 위협의 시작으로 보는 것임

4. 정보 공유

□ 정보 공유(Information Sharing) 이슈 사항

- 미국 내 공유는 원활함

- 외국으로 공유는 원활하지 못함 (사유 : 법적·문화적 문제. 법적 책임 문제로 인한 변호사들의 기피 등)

- 유럽은 IP주소도 개인정보로 분류되어 있어서 공유가 어려움

- 현실적인 어려움에도 불구하고 더 많은 정보 공유를 원함

□ 정보 공유의 2 방향 : 기술적 방향, 전략적 방향

5. 기타 CSFC 운영현황

□ 매일 아침 9:30 quick standup 콜 수행

- 글로벌 센터들과 각종 정보 공유

□ 사이버 워 게임(Cyber War Game)

- 대응 훈련을 게임 형식으로 만들어서 수행

□ 퓨전을 위한 사무실 자리 배치

- 서로 다른 각종 팀의 구성원들을 섞어서 자리 배치
- 6개월간 같은 자리에 앉고 그 후 자리 이동

□ 사이버 어택을 10초마다 확인

□ CSFC 비디오 월(Video Wall) 운영

- 각종 정보 화면 실시간 제공

- 타 센터 사람들 동향도 화면 내 동영상으로 확인 (실제 위기상황 시 파악 가능)

- Fraud나 3rd 파티와 관련 내용도 업데이트 되며 수시 확인

- 주요 뉴스, SNS 확인 화면 포함
  ※ 정보 속도는 SNS, 인터넷 뉴스, 전통 뉴스 순으로 빠름

- Outage 앱을 통한 정전 현황 화면 포함

- 전세계 인터넷 사용량 정보 화면 포함 (akamai사 제공)

- 기술적 이슈 화면 포함 (나스닥에서 모아서 제공)

6. CSFC의 지향점

□ 'Money 보다 People's View가 더 중요함'

- 금전적 이득을 얼마나 올리나 보다 사람들이 씨티은행을 어떻게 생각하느냐가 훨씬 더 중요함

- 최근 맥킨지에서 윤리적인(ethical) 것에 더 집중할 것을 컨설팅함

Ⅵ. 시사점 및 고려사항

□ 금전적, 기술적 요소 외 필수 사항

- 보안은 기술 자체보다 리스크 관리 차원의 접근이 필요함
- 위협대응을 위해서는 기술 외 인력, 프로세스가 함께 필요함
- 보안은 수익, 예산, 비용 등 금전적 차원의 접근보다 고객과 자사의 자산을 보호하고, 고객으로부터의 신뢰와 평판을 유지하는 차원에서의 고려가 필요함
- 각종 공격자(위협 제공자)의 동기와 프로세스를 파악하는 것이 공격자의 기술을 파악하는 것 못지않게 중요함

□ 최근 사이버 범죄의 변화 양상

- 사이버 공격의 빈도, 스피드, 효과는 계속 증가하는 추세
- 어떤 기관/회사도 예방 전략만으로 100% 성공적일 수는 없으며, 감지 능력과 대응 능력이 동일하게 중요함
- 사이버 리스크가 빠르게 진화하고 새롭게 생겨나고 있음
- 최근 공격자의 동기가, 1회성 금전 탈취에서 비즈니스에 장기간 치명적 타격을 미치는 고객 신뢰 파탄으로 변화함

□ 보안 관리 발전 방향

- 리스크 관리 프로세스 내재화 차원의 접근 필요
- 정보 공유 파트너쉽 구축 및 협력이 보안 유지의 핵심임
- 보호, 감지, 대응, 완화 과정의 지속적 수행 및 내재화 필수
- 공격 속도의 급격한 가속화에 대비한 신속 대응 능력 필요

제 4장. 아마존 웹 서비스(AWS)

Ⅰ. 개 요

□ 최근 정보통신기술(ICT)활용 패러다임이 정보시스템을 자체적으로 구축하는 방식에서 클라우드컴퓨팅 서비스를 활용하는 방식으로 전환되는 중

※ 과학기술정보통신부는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제정(2015) 등을 통해 클라우드 산업 경쟁력 강화를 도모

□ 해외 금융권에서도 수익성 제고 및 서비스 경쟁력 향상 등을 목적으로 클라우드컴퓨팅 도입을 고려하는 금융회사가 증가하는 추세

□ 향후 금융과 ICT의 융합이 촉진되면서 클라우드컴퓨팅을 활용한 금융서비스에 대한 수요가 계속 증가할 것으로 예상되면서, 새로운 전자금융수단 등장에 따른 보안위협 및 서비스 동향 등을 파악하고자 함

Ⅱ. 클라우드 컴퓨팅

1. 클라우드 컴퓨팅 개념

□ 클라우드 컴퓨팅 개념[7]

- 서비스 플랫폼에서 컴퓨팅 파워, 데이터베이스 스토리지, 애플리케이션 및 기타 IT 리소스를 필요에 따라 인터넷을 통해 제공하고 사용한 만큼만 비용을 지불하는 것

7) Amazon AWS 홈페이지, “클라우드 컴퓨팅이란?” , https://aws.amazon.com/ko/what-is-cloud-computing/

□ 미국 NIST[8]가 정의한 클라우드 컴퓨팅 특징 5가지

- 온 디맨드 셀프 서비스
  - 소비자가 일방적으로 서버 타임, 네트워크 스토리지 등의 컴퓨팅 자원을 조달 가능
  - 서비스 제공자와의 실 접촉이나 상호작용 없이 자동 조달

- 광역 네트워크 접속
  - 모바일, PC, 워크스테이션 등 다양한 클라이언트 플랫폼에서 네트워크를 통해 서비스 접속 및 이용 가능

- 리소스 풀링
  - 여러 소비자를 지원하기 위해 서비스 제공자의 컴퓨팅 자원의 풀을 형성한 후, 소비자별 요구에 따라 다양한 물리적/가상적 자원을 동적으로 할당/재할당

- 신속한 탄력성(Rapid elasticity)
  - 자원의 탄력적 조달 및 해제
  - 고객 요구에 맞게 자원할당을 자동 확장/축소
  - 고객에게는 조달 가능 자원이 무제한인 것으로 보이고, 언제든지 얼마든지 할당 가능한 것으로 보임

- 서비스 측정성 (Measured service)
  - 자원 사용량의 측정, 제어, 레포팅 가능
  - 서비스 벤더와 고객 양측에 투명하게 사용량 정보 제공

2. 클라우드 컴퓨팅 혜택

□ 유연하고 비용이 저렴한 IT 리소스에 대한 빠른 액세스를 제공

8) National Institute of Standards and Technology, NIST

□ 하드웨어에 막대한 사전 투자를 하거나 하드웨어를 유지 관리하기 위해 많은 시간을 할애하지 않아도 됨

□ 새로운 아이디어를 실현하거나 IT 부서를 운영하는 데 필요한 컴퓨팅 리소스의 유형 및 크기를 정확하게 프로비저닝 가능

□ 필요한 만큼의 리소스에 즉시 액세스 가능

□ 사용한 만큼의 리소스에 대해서만 비용을 지불

3. 클라우드 컴퓨팅 작동 원리

□ 클라우드 컴퓨팅은 서버, 스토리지, 데이터베이스 및 광범위한 애플리케이션 서비스를 인터넷을 통해 간단하게 액세스할 수 있는 방법을 제공함

□ Amazon Web Services와 같은 클라우드 서비스 플랫폼은 이러한 애플리케이션 서비스에 필요한 네트워크 연결 하드웨어를 소유하고 이에 대한 유지 관리를 담당

□ 사용자는 웹 애플리케이션을 통해 필요한 것을 조달하여 사용

4. 클라우드 컴퓨팅 6가지 이점

□ 자본 비용을 가변 비용으로 대체

- 사전에 데이터 센터와 서버에 대규모의 투자를 하는 대신 컴퓨팅 리소스를 사용할 때만, 사용한 만큼의 리소스에 대해서만 비용 지불

□ 규모의 경제로 얻게 되는 이점

- 고객 자체 인프라보다 가변 비용이 낮음
- Amazon Web Services와 같은 공급자는 규모의 경제를 달성할 수 있어, 종량 과금제 요금이 더 낮아짐

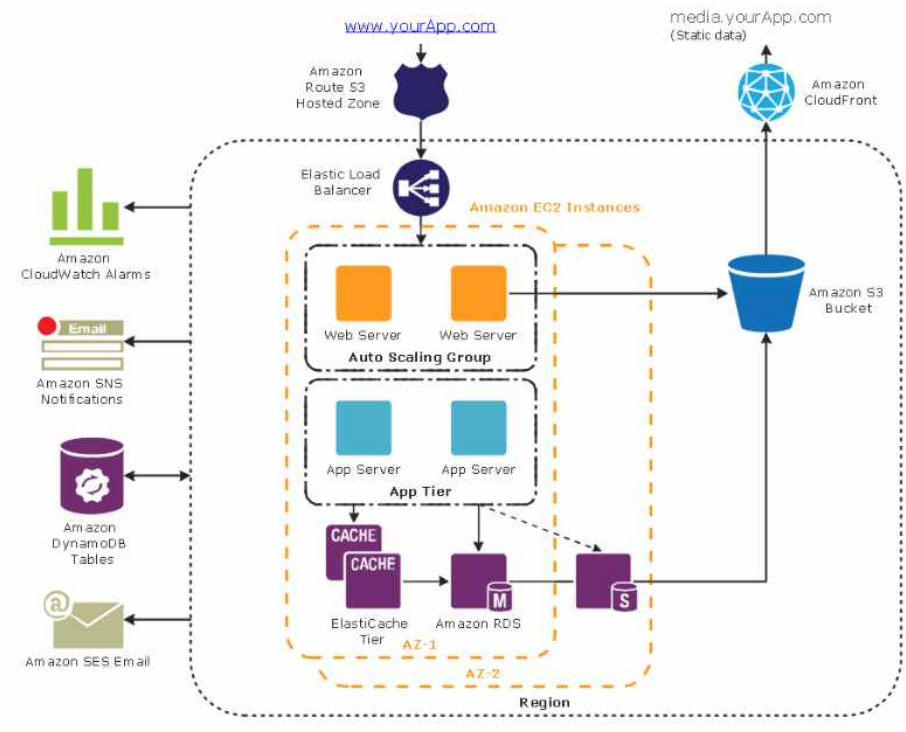
□ 용량 추정 불필요

- 필요한 인프라 용량을 추정할 필요가 없음

- 애플리케이션 배포 전에 용량을 결정하면 고가의 리소스를 구입하여 유휴 상태로 유지하게 되거나 한정된 용량으로 작업하게 되는 경우가 발생

- 클라우드 컴퓨팅 사용 시, 필요한 만큼의 리소스에 액세스하고 필요에 따라 몇분 만에 확장·축소할 수 있음

< AWS의 자동 용량 조절 방식 >



□ 속도 및 민첩성 개선

- 새로운 IT 리소스를 클릭 한 번으로 사용 가능

- 해당 리소스를 개발자에게 제공하기까지의 시간을 몇 주에서 단 몇 분으로 단축 가능

- 이에 따라 실험 및 개발에 드는 비용이 절감되고 시간이 단축되어 조직의 민첩성이 크게 향상됨

□ 데이터 센터 운영 및 유지 관리에 비용 투자 불필요

- 인프라가 아닌 비즈니스 차별화에 집중 가능

- 수많은 서버 등 인프라 관리가 불필요하여 고객에게 더욱 집중할 수 있음

□ 몇 분 만에 전 세계에 배포

- 클릭 몇 번으로 전 세계의 여러 리전에 애플리케이션을 손쉽게 배포할 수 있음

- 이는 최소 비용으로 고객 지연 시간은 줄이면서 더 나은 사용 환경을 간편하게 제공할 수 있음을 의미함

5. 클라우드 컴퓨팅 서비스 유형[9]

□ 서비스로서의 인프라 (IaaS: Infra as a Service)

9) Amazon AWS 홈페이지, “클라우드 컴퓨팅 유형”, https://aws.amazon.com/ko/types-of-cloud-computing/

- 시스템·네트워크 등 물리적 인프라를 서비스 형태로 제공

- 클라우드 IT의 기본 빌딩 블록을 포함

- 네트워킹 기능, 컴퓨터(가상 또는 전용 하드웨어) 및 데이터 스토리지 공간 등을 제공

- IT 리소스에 대해 가장 높은 수준의 유연성과 관리 제어를 제공

- 기존 IT 리소스와 가장 유사함

- AWS의 EC2, ELB, VPC 등이 대표적인 IaaS의 예임

□ 서비스로서의 플랫폼 (PaaS: Platform as a Service)

- SaaS를 플랫폼 개념으로 확대한 서비스[10)]
- 개발 플랫폼 자체를 서비스 형태로 제공한 것
  - (예) 웹 서비스를 개발하려면 장고, 루비 온 레일즈와 같은 소프트웨어를 설치하고, 코드를 개발한 뒤 깃(git) 등으로 코드 형상을 관리하며 테스트하고 배포하는 등의 모든 과정을 관리해야 함. 이는 경험 있는 개발자의 손길이 필요한 난이도가 높은 작업임. Paas는 이러한 일을 대신 해줌

- AWS의 엘라스틱 빈스톡(Elastic Beanstalk)이 Paas에 해당

- PaaS 사용 시, 기본 인프라(하드웨어와 OS)를 관리할 필요가 없어 애플리케이션 개발과 관리에 집중할 수 있음

- 리소스 구매, 용량 계획, 소프트웨어 유지 관리, 패치 등의 작업 불필요

10) 윤상배 외 1인, “아마존 웹 서비스를 이용한 글로벌 서비스 인프라 설계”, 2016.04.15., 위키북스

□ 서비스로서의 소프트웨어 (SaaS: Software as a Service)

- 일반 사용자가 Iaas를 사용하는 이유는 운영체제를 직접 제어하고 그 위에 S/W를 올려서 서비스하기 위해서임

- 소프트웨어와 운영체제를 일일이 설치하고 설정하는 대신 IaaS에 S/W까지 패키지로 묶어서 제공하는 서비스

- 사용자는 운영체제와 소프트웨어 설치와 같은 부분을 신경 쓸 필요가 없으며. 소프트웨어의 사용에만 신경쓰면 됨

- 사용자가 S/W를 설치하여 직접 SaaS를 만들 수 있음

- AWS는 사용자간 SaaS 거래를 위한 마켓 플레이스 제공

- 서비스 제공자에 의해 실행되고 관리되는 완전한 제품을 고객에게 제공

- 대부분의 경우 최종 사용자 애플리케이션을 지칭

- SaaS 이용 시, 서비스가 어떻게 유지 관리되는지 또는 기본 인프라가 어떻게 관리되는지 생각할 필요가 없음

- SaaS 예
  - 이메일 제품을 관리할 필요가 없고 이메일 서버의 HW 및 OS를 유지 관리할 필요가 없는 웹 기반 이메일
  - AWS RDS(데이터베이스), SQS(메시지 큐), 엘라스틱 캐시(캐시 서비스) 등

6. 클라우드 적용하기 좋은 사례

□ IT 서비스 처리량의 산정이 어려운 경우

- 이 경우, IT 인프라를 자체 구축한다면 과도한 투자 또는 리소스 부족의 가능성이 높음

- 클라우드 적용 후 실제 서비스 양 확인 후 동적으로 자원 할당 가능

□ 짧은 기간동안 인프라 필요 시

- 필요한 기간 동안만 클라우드 서비스 이용 가능

□ HPC(High Performance Computing) 필요시

- 각종 데이터 분석 등 고속/고성능 계산이 필요한 경우에도 클라우드가 적합할 수 있음

- 금융 관련 분야의 경우 각종 통계/분석 등

- 금융 규제 관련 분야에서 고성능 실시간 계산을 요하는 경우에도 적합

- GRID를 원할 때마다 늘리고 줄어들 수 있음

- 높은 대역폭, 저지연 네트워킹, 초고성능 컴퓨팅 가용성 및 성능 확보 가능

- 클라우드 이용시, 클라우드에서 추가적으로 제공하는 데이터 분석 등 툴도 함께 활용 가능함

□ 기타, 자원의 동적 확장성/탄력성이 필요한 경우

- 아마존 예제
  - · prime day 이벤트 시 평소의 10배로 접속 증가
  - · 해당 일에만 IT 리소스 추가 할당 후 불필요시 원복
  - · 이 경우 인프라 비용을 피크에 맞출 필요가 없음

※ AWS 측에서 언급한 클라우드 이용 효과
- 확장성(Scalability)로 인해 45% 비용 절감 가능
  (나스닥은 65% 절감)
- 데이터 양 만큼만 비용을 지불함으로써 30% 비용 절감

Ⅲ. AWS 개요

※ 아마존의 혁신에 대한 생각

1. AWS(Amazon Web Services) 개요[11)]

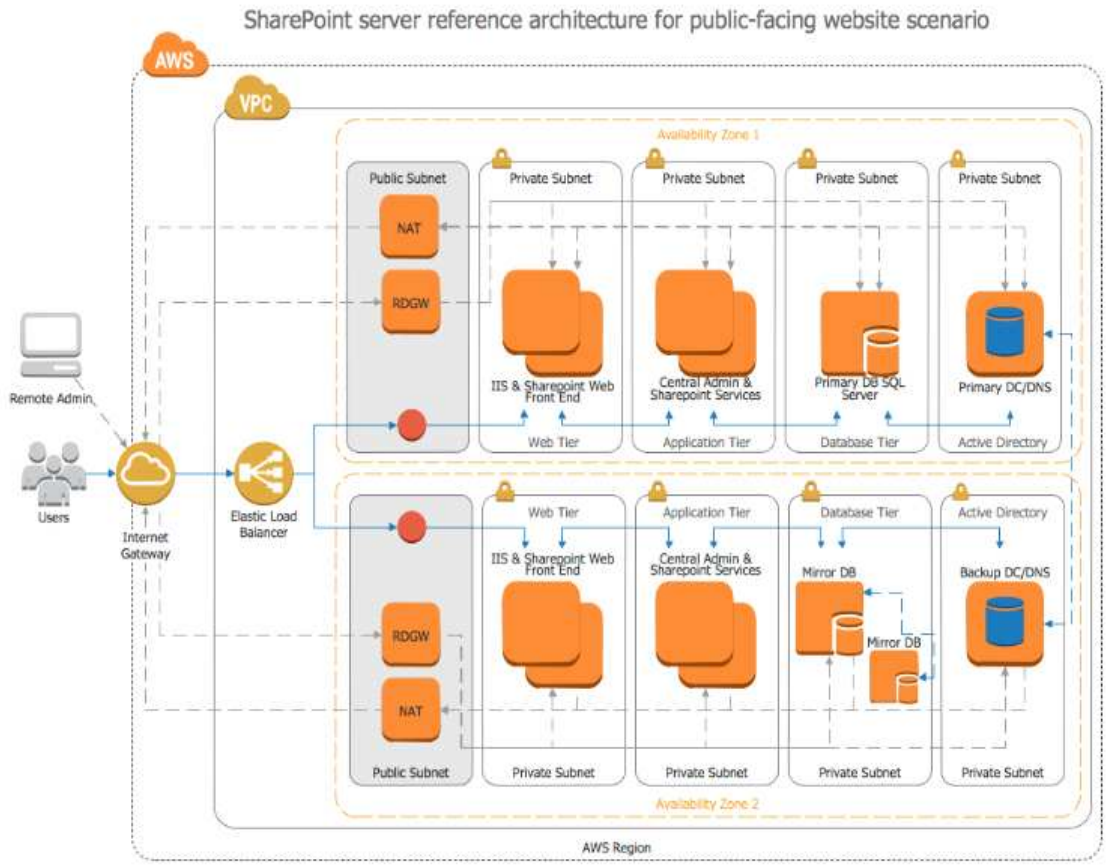
□ AWS는 amazon.com에서 제공하는 클라우드 서비스

□ 웹을 통해 이용할 수 있는 클라우드 컴퓨팅 플랫폼

□ 2004년 11월에 일반인에게 서비스를 공개

□ 2017년 8월말에는 93개의 서비스를 제공할 수 있도록 성장

< Amazon Web Services >



11) 타테오카 마모루 외 5인, "탄력적 개발로 이끄는 AWS 실천 기술", 2016.12.02., 제이펍

2. 사용자의 AWS 선호 이유

□ 많은 서비스

- 가상서버를 사용할 수 있는 컴퓨터 서비스(EC2) 이외에 DNS 서비스(Route53)와 CDN(Contenets Delivery Network) 서비스 등 많은 서비스를 제공

- 인프라와 패치 등의 관리를 AWS가 대신 해주는 관리 서비스(Management Service)도 존재

- DNS 서비스와 콘텐츠 전송 서비스는 종합 관리 서비스(Full Management Service)임

- 이러한 서비스 활용 시, 부하 분산을 통한 신뢰성 높은 시스템을 손쉽게 구축 및 운용할 수 있음

□ 유연한 리소스

- 리소스를 필요할 때 필요한 만큼 만들어서 사용 가능
- '필요한 만큼'이란, 서버 대수나 사양을 유연하게 만들고 조정할 수 있다는 뜻

- 예를 들어 쇼핑몰 운용 시, 이벤트 시행으로 평소보다 많은 사용자가 접속할 경우, 이벤트 기간에만 서버 리소스를 늘리고, 이벤트가 끝나면 리소스를 다시 줄일 수 있음

□ 종량 과금

- 사용한 만큼 비용을 지불하는 종량 과금 정책
- 필요할 때 사용한 만큼 내면 되므로 비용 효율 면에서 유리

3. AWS의 물리적 구성요소

□ 지역 (Region, 리전)

- AWS의 각 서비스가 제공되는 지역을 뜻함

- 예를 들어 서울(Seoul 지역)이나 미국 동부(US East 지역) 등 '16년 9월 기준 전 세계에는 13개 지역에 존재

- 지역에 따라 사용할 수 있는 서비스가 다르므로 사용하고 싶은 지역에서 서비스를 사용할 수 있는지 확인 필요

- 최신 서비스는 기본적으로 미국에서 사용할 수 있으며, 순차적으로 다른 지역에서도 사용할 수 있게 확대 됨

□ 가용 영역 (Availability Zone)

- 가용 영역은 독립된 데이터 센터라고 말할 수 있으며, 모든 지역에 반드시 두 개 이상의 가용 영역이 존재함

- 그 이유는 가용성을 위한 것으로, 하나의 가용 영역이 천재지변이나 장애에 의해 이용할 수 없는 상태가 되더라도 다른 가용 영역에서 시스템이 가동되도록 설계되어 있음

- 가용 영역 사이에는 고속 회선으로 연결되어 있음

□ 에지 로케이션 (Edge Location)

- 콘텐츠 전송 서비스인 CloudFront 및 DNS 서버 서비스인 Route53을 제공하는 장소를 말함

- ‘16년 9월 기준 전 세계에 60개의 에지 로케이션이 있으며, 한국에 2개, 일본에 3개가 존재

- CloudFront로 콘텐츠를 전송할 때 에지 로케이션이 사용자와 가까운 곳에 있으면 빠른 전송 속도 구현 가능

※ 2017년 8월말 현재, 16개 리전, 42개 가용 영역, 74개 에지 로케이션 존재

4. AWS 기타 특징

□ 자동 용량 조절 (Auto scaling)

- AWS에서 제공하는 서비스 중의 하나

- 소프트웨어에서 오토 스케일링은 일반적인 기능이나, 하드웨어는 물리적인 실체가 필요하고 사용량이 줄어들 때 회수하기가 어려워 오토 스케일링을 적용하기 쉽지 않음

- AWS는 기존에 하드웨어로 관리하던 로드 밸런서를 소프트웨어 형식으로 제공하여 오토 스케일링을 적용 가능

- 요청이 늘어나면 자동으로 로드 밸런서 인스턴스를 늘려서 늘어난 요청을 처리하고, 줄어들면 회수

- 사용자 관여 없이 자동으로 진행

※ Auto scaling은 수평적 확장임. 가상 머신 내 수직적 확장은 리부팅 등에 따른 서비스/기기의 중단이 발생할 수 있음

□ 감사(audit) 기능을 제공함

- CloudTail이라는 도구 사용시 모든 API 콜 로깅 가능

- 사용자만 접근 가능하며 AWS는 접근 불가능

□ AWS 이용시 기타 특징

- AWS에서 침해 대응 전문팀 운영 : AWS 이용시 침해대응, 운영, DDoS 대응 등에 대해 신경 쓸 필요 없음

- IoT, mobile, AI, 어낼러틱스, 보안 등 관련 93개 서비스

- DDoS 방지에 대해서 별도 비용 지불이 불필요함

Ⅳ. AWS 제공 서비스

1. AWS 주요 서비스 (보안 관련 제외)

□ EC2(Elastic Compute Cloud)

- 가상 서버를 필요할 때 필요한 만큼 자유롭게 생성·사용할 수 있고, 사용한 만큼만 비용을 지급하는 서비스로 가장 널리 사용

- 애플리케이션의 규모나 부하에 맞춰 사양을 높이거나 가상 서버 대수를 늘릴 수 있는 유연성을 가짐

- 예를 들어, 제공하는 웹서비스 이벤트 등으로 일시적인 접속자 수 증가가 예상된다면 피크일 때만 서버를 늘리고, 접속자 수가 줄어들면 서버를 줄일 수 있음

- AWS는 다양한 종류의 리눅스와 윈도 운영체제를 지원

- 가상 머신을 AWS의 독자 포맷인 AMI(Amzaon Machine Image) 형태로 저장 가능

- 타 사용자의 가상 서버 AMI를 마켓 플레이스에서 구매 가능

□ Route53

- SLA 100%의 웹 기반 DNS 서비스

- EC2와 같이 리전별로 제공되는 서비스가 아닌 전 세계에 설치되어 있는 에지 로케이션 기반으로 제공되는 서비스

- 전 세계 에지 로케이션 중에 가장 가까운 로케이션에서 응답을 주므로 빠르고 가용성이 높고 확장성이 뛰어남

- 다른 서비스와 마찬가지로 API로 DNS 설정 가능

- 기존 DNS 서버처럼 패치 등의 작업이 불필요함

□ VPC(Virtual Private Cloud)

- 논리적인 가상 네트워크를 구축할 수 있는 서비스

- 외부 네트워크에서 인터넷에 접속할 수 있는 DMZ 서브넷 및 인터넷에서는 접속할 수 없는 사설 서브넷 생성 가능

□ S3(Simple Stroage Service)[12)]

12) Amazon AWS 홈페이지, “Amazon S3”, https://aws.amazon.com/ko/s3/

- 아주 높은 내구성을 가진 웹 스토리지 서비스

- 웹 사이트에서 모바일 앱, 기업 애플리케이션, IoT 센서나 디바이스의 데이터에 이르기까지 어디서나 원하는 양의 데이터를 저장하고 검색할 수 있도록 구축된 객체 스토리지

- 99.999999999%의 내구성을 제공

- 쿼리 지원 기능을 가진 유일한 클라우드 스토리지 솔루션

- S3에 있는 데이터에 대해 즉시 강력한 분석 수행 가능

□ CloudFront[13)]

- 콘텐츠를 전 세계로 빠르게 전송할 수 있는 서비스 (CDN)

- 짧은 지연 시간과 빠른 전송 속도로 최종 사용자에게 데이터, 동영상, 애플리케이션 및 API를 안전하게 전송

- API, AWS Management Console, AWS CloudFormation, CLI 및 SDK와 같이 이미 익숙한 AWS 도구를 사용하여 몇 분 만에 CloudFront를 시작 가능

□ RDS(Relational Database Service)[14)]

- OS 및 패치 등의 관리가 필요 없는 RDB

13) Amazon AWS 홈페이지, “Amazon CloudFront”, https://aws.amazon.com/ko/cloudfront/

14) Amazon AWS 홈페이지, “Amazon Relational Database Service(RDS)”, https://aws.amazon.com/ko/rds/

- 클라우드에서 관계형 데이터베이스를 더욱 간편하게 설정, 운영 및 확장할 수 있음

- 하드웨어 프로비저닝, 데이터베이스 설정, 패치 및 백업과 같은 시간 소모적인 관리 작업을 자동화

- 여러 데이터베이스 인스턴스 유형(메모리, 성능 또는 I/O 최적화)으로 제공됨

- Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, Microsoft SQL Server의 6개 DB 엔진 중 선택 가능

- AWS Database Migration Service를 사용하여 기존 데이터베이스를 Amazon RDS로 손쉽게 마이그레이션 또는 복제할 수 있음

□ ELB(Elastic Load Balancing)[15)]

- 자동으로 스케일 인, 스케일 아웃이 가능한 고가용성을 가진 로드 밸런서 서비스

- 인입 트래픽을 Amazon EC2 인스턴스, 컨테이너, IP 주소와 같은 여러 대상에 자동으로 분산

- 단일 가용 영역 또는 여러 가용 영역에서 다양한 애플리케이션 부하를 처리 가능

- 세 가지 로드 밸런서 제공
  ① Application Load Balancer : Application Load Balancer는 HTTP 및 HTTPS 트래픽의 로드 밸런싱에 가장 적합하며,

15) Amazon AWS 홈페이지, “Elastic Load Balancing”, https://aws.amazon.com/ko/elasticloadbalancing/

마이크로서비스와 컨테이너 등 최신 애플리케이션 아키텍처 전달을 위한 고급 요청 라우팅 기능을 제공함. Layer 7에서 작동함

② Network Load Balancer : 극한의 성능이 요구되는 TCP 트래픽의 로드 밸런싱에 가장 적합함. Layer 4에서 작동하며, 초당 수백만 개의 요청을 처리하면서 극히 낮은 지연 시간을 유지할 수 있음. 갑작스러운 일시적 트래픽 패턴 처리에도 최적화되어 있음

③ Classic Load Balancer : 여러 Amazon EC2 인스턴스에서 기본적인 로드 밸런싱을 제공

□ CloudWatch[16)]

- 여러 서비스의 감시와 모니터링을 하는 서비스

- 지표를 수집 및 추적하고, 로그 파일을 수집 및 모니터링하며, 경보를 설정하고, AWS 리소스 변경에 자동으로 대응할 수 있음

- AWS 리소스뿐만 아니라 애플리케이션과 서비스에서 생성된 사용자 정의 지표 및 애플리케이션에서 생성된 모든 로그 파일을 모니터링할 수 있음

- 시스템 전반의 리소스 사용률, 애플리케이션 성능, 운영 상태를 파악할 수 있음

□ CloudTrail[17)]

---

16) Amazon AWS 홈페이지, “Amazon CloudWatch”, https://aws.amazon.com/ko/cloudwatch/?sc_channel=PS&sc_campaign=acquisition_KR&sc_publisher=google&sc_medium=english_cloudwatch_b&sc_content=cloudwatch_e&sc_detail=cloudwatch&sc_category=cloudwatch&sc_segment=161200533728&sc_matchtype=e&sc_country=KR&s_kwcid=AL!4422!3!161200533728!e!!g!!cloudwatch&ef_id=V7x5GwAABLjUTVuM:20170924115044:s

17) Amazon AWS 홈페이지, “AWS CloudTrail”,

- 사용자 활동 및 API 사용 추적

- AWS 계정의 거버넌스, 규정 준수, 운영 감사, 위험 감사가 가능한 서비스

- AWS 인프라에서 계정 활동과 관련된 작업을 기록하고 지속적으로 모니터링하며 보관할 수 있음

- AWS Management Console, AWS SDK, 명령줄 도구 및 기타 AWS 서비스를 통해 수행된 작업을 비롯하여 AWS 계정 활동의 이벤트 기록을 제공

- 이러한 이벤트 기록을 통해 보안 분석, 리소스 변경 추적, 문제 해결을 간소화할 수 있음

- 장점 : 규정 준수 간소화, 사용자 및 리소스 활동에 대한 가시성, 보안 분석 및 문제 해결, 보안 자동화

□ QuickSight

- 빅데이터를 위한 비지니스 인텔리전스 솔루션

- 비쥬얼라이제이션 기능 제공

□ Cloud Directory[18)]

---

https://aws.amazon.com/ko/cloudtrail/?sc_channel=PS&sc_campaign=acquisition_KR&sc_publisher=google&sc_medium=english_cloudtrail_b&sc_content=cloudtrail_e&sc_detail=aws%20cloudtrail&sc_category=cloudtrial&sc_segment=161191313896&sc_matchtype=e&sc_country=KR&s_kwcid=AL!4422!3!161191313896!e!!g!!aws%20cloudtrail&ef_id=V7x5GwAABLjUTVuM:20170924115832:s

18) Amazon AWS 홈페이지, “Amazon Cloud Directory” , https://aws.amazon.com/ko/cloud-directory/

- 다차원의 데이터 계층 구조를 구성할 수 있는 클라우드 네이티브 디렉터리

- Active Directory Lightweight Directory Services(AD LDS)와 LDAP 기반 디렉터리와 같은 기존 디렉터리 솔루션은 단일 계층 구조만 지원

- Cloud Directory는 다차원에 걸친 계층 구조로 이루어진 디렉터리를 생성할 수 있는 유연성을 제공

- 완전관리형 서비스인 Cloud Directory는 인프라 확장이나 서버 관리와 같은 시간 소모적이고 많은 비용이 드는 관리 작업을 없애 줌

- 스키마를 정의하고, 디렉터리를 생성한 다음, Cloud Directory API를 호출하여 디렉터리를 채우기만 하면 됨

□ Snowball[19)]

- 대용량 데이터를 전송하는 서비스

- 안전한 어플라이언스 기기를 사용하여 대용량 데이터를 송수신하는 페타바이트 규모의 데이터 전송 솔루션

- 고속 네트워크 비용, 오랜 전송 시간, 보안 문제 등 흔히 발생하는 대규모 데이터 전송과 관련된 문제를 해결 가능

- 데이터 전송을 위해 코드를 작성하거나 하드웨어를 구매할 필요

19) Amazon AWS 홈페이지, “AWS Snowball”, https://aws.amazon.com/ko/snowball/

가 없음

- Snowball 어플라이언스가 고객에게 자동으로 배송됨

- 클라이언트에서 파일을 암호화하여 고속으로 어플라이언스로 전송

- 이점 : 빠른 속도, 고도의 확장성, 변조 방지 및 보안(Trusted Platform Module(TPM), 256-비트 암호화 및 변조 방지 엔클로저를 사용), 간편성 및 호환성, 고속 인터넷 전송 대비 저렴한 비용(1/5 수준), 쉬운 데이터 검색

2. AWS 주요 서비스 (보안/인증 관련)

□ IAM(Identity and Access Management)[20]

- 사용자와 사용자 권한을 관리하는 서비스

- 소스에 대한 액세스를 안전하게 통제할 수 있게 함

- AWS 사용자 및 그룹을 만들고 관리하며 AWS 리소스에 대한 액세스를 허용 및 거부할 수 있음

- IAM은 AWS 계정에서 추가 비용 없이 제공되는 기능

- AWS 리소스에 대한 세분화된 액세스 제어
  - 사용자가 AWS 서비스 API 및 특정 리소스에 대한 액세스를 제어할 수 있게 함
  - 원본 IP 주소, SSL 사용 여부 또는 멀티 팩터 인증 여부 등을 접근제어 조건에 추가 가능

20) Amazon AWS 홈페이지, “Identity and Access Management”, https://aws.amazon.com/ko/iam/

- 권한이 높은 사용자용 MFA (Multi-Factor Authentication)
  - MFA 사용 시, 사용자가 MFA 토큰 또는 MFA가 활성화된 모바일 디바이스를 실제 소유하고 있음을 증명해야 함

- 웹 자격 증명 공급자를 사용한 모바일 애플리케이션용 액세스 제어 관리 : 일정 기간 동안 특정 AWS 리소스에만 액세스할 수 있는 임시 보안 자격 증명을 요청해 모바일 및 브라우저 기반 애플리케이션이 안전하게 AWS 리소스에 접근하도록 할 수 있음

- 기능 : IAM은 역할과 권한 생성을 지원함
  - IAM 사용자 및 액세스 관리 : IAM에서 사용자를 생성하거나, 사용자에게 개별 보안 자격 증명(즉, 액세스 키, 암호, 멀티 팩터 인증 디바이스)을 할당하거나, AWS 서비스 및 리소스에 대한 액세스를 제공하도록 임시 보안 자격 증명을 요청할 수 있음. 사용자가 수행할 수 있는 작업을 제어하기 위해 권한을 관리할 수 있음
  - IAM 역할 및 해당 권한 관리 : IAM에서 역할을 생성하고 권한을 관리하여 역할을 맡는 엔터티 또는 AWS 서비스가 수행할 수 있는 작업을 제어할 수 있음. 또한, 역할을 맡을 수 있는 엔터티를 정의 가능. 서비스에 연결된 역할을 사용하여 사용자를 대신해 AWS 리소스를 생성하고 관리하는 AWS 서비스에 권한을 위임 가능
  - 연동 사용자 및 해당 권한 관리 : 자격 증명 연동을 사용하면 자격 증명별로 IAM 사용자를 생성하지 않고도 기업의 기존 자격 증명(사용자, 그룹 및 규칙)으로 AWS Management Console에 액세스하고, AWS API를 호출하며, 리소스에 액세스할 수 있음

□ Inspector[21)]

21) Amazon AWS 홈페이지, “Amazon Inspector”, https://aws.amazon.com/ko/inspector/

- AWS에 배포된 애플리케이션의 보안과 규정 준수를 개선하는 데 도움이 되는 자동화된 보안 평가 서비스

- 애플리케이션의 취약성 등을 자동으로 평가

□ Certificate Manager[22)]

- AWS 서비스에 사용할 SSL/TLS 인증서를 손쉽게 조달, 관리 및 배포할 수 있게 해주는 서비스

- 간편한 인증서 취득 지원
  - 키 페어 또는 CSR(Certificate Signing Request)을 생성하거나, CSR을 인증 기관에 제출하거나, 취득한 인증서를 업로드 및 설치할 필요가 없이, AWS Management Console에서 클릭 몇 번으로 AWS에서 신뢰할 수 있는 SSL/TLS 인증서를 요청할 수 있음

- 인증서 배포 처리 및 사용자가 웹 사이트 또는 애플리케이션에 대해 SSL/TLS를 활성화할 수 있도록 지원함

- 무료 서비스 : 인증서를 조달하는데 추가 비용이 들지 않음

- 관리형 인증서 갱신 지원
  - SSL/TLS 인증서의 갱신 프로세스를 관리하고 갱신된 인증서를 AWS 리소스에 배포하여 수동 프로세스로 인해 발생할 수 있는 오류를 방지함

- CloudTrail 로그를 검토하여 인증서의 사용을 감사 가능

---

22) Amazon AWS 홈페이지, “AWS Certificate Manager”, https://aws.amazon.com/ko/certificate-manager/

- 타사 인증기관(CA) 발급 인증서의 적용 기능 포함

□ CloudHSM[23)]

- AWS 클라우드상의 관리형 하드웨어 보안 모듈(HSM)

- AWS 클라우드에서 자체 암호화 키를 손쉽게 생성 및 사용할 수 있도록 지원하는 클라우드 기반 하드웨어 보안 모듈

- FIPS 140-2 레벨 3 인증 HSM을 사용

- 업계 표준에 기반한 개방형 HSM
  - CloudHSM은 PKCS#11, Java Cryptography Extensions(JCE) 및 Microsoft CryptoNG(CNG) 라이브러리와 같은 업계 표준 API를 지원
  - 키를 다른 상용 HSM으로 전송할 수 있어 AWS로부터 또는 AWS로 용이하게 키 마이그레이션

- 암호화 키에 대한 제어 유지
  - 사용자를 생성하고 HSM 정책을 설정할 수 있도록 안전한 채널을 통해 HSM에 대한 액세스를 제공함
  - CloudHSM을 통해 생성·사용하는 암호화 키는 고객이 지정한 HSM 사용자만 액세스 가능
  - AWS는 고객의 암호화 키에 접근 불가함

- 강력한 인증으로 키를 보호
  - 중요한 관리 및 키 관리 기능에 대해 Quorum 인증을 지원하고 고객이 제공한 토큰을 사용한 Multi-Factor

23) Amazon AWS 홈페이지, “AWS CloudHSM”, https://aws.amazon.com/ko/cloudhsm/

Authentication(MFA)을 지원

- 간편한 관리
  · 하드웨어 프로비저닝, 소프트웨어 패치, 고가용성, 백업 등의 관리 작업을 자동화한 완전관리형 서비스

□ Key Management Service(KMS)[24)]

- 데이터를 암호화할 때 사용하는 키를 손쉽게 생성 및 제어

- 하드웨어 보안 모듈(HSM)을 사용하여 키를 안전하게 보호

- 중앙 집중식 키 관리
  · 암호화 키를 중앙에서 관리 가능
  · 모든 키 사용에 대한 단일 보기를 제공
  · AWS Management Console, AWS SDK 또는 CLI를 사용하여 쉽게 키를 생성하고, 가져오고, 교체할 수 있을 뿐 아니라 사용 정책 정의 및 사용 감사도 가능

- AWS 서비스와의 통합
  · 여러 다른 AWS 서비스와 통합되어 사용자가 관리하는 키를 사용해 데이터를 손쉽게 암호화 가능

- 암호화와 키 관리를 프로그래밍 방식으로 애플리케이션에 통합하기 위한 SDK를 제공

- 내장된 감사 기능
  · AWS CloudTrail과 통합되어 KMS API 호출 로그를 제공
  · 키의 액세스와 관련된 세부 정보를 제공하여 규정 준수와 규제 요구 사항을 충족하도록 지원

24) Amazon AWS 홈페이지, “AWS Key Management Service(KMS)”, https://aws.amazon.com/ko/kms/

- 저렴한 비용
  - 계정의 기본 키 스토리지에 대한 요금이 없음
  - 추가 생성한 마스터 키와 키 사용에 대해서만 지불

- 암호화되지 않은 키는 메모리에서만 사용

□ Organizations[25)]

- 여러 AWS 계정을 정책 기반으로 중앙 관리

- 계정 그룹에 대한 정책 관리 및 계정 생성 자동화

- AWS 계정을 정책 기반으로 관리하는 기능을 제공

- 모든 AWS 고객이 추가 비용 없이 사용 가능한 서비스

- AWS 서비스에 대한 액세스 권한 제어
  - AWS 계정별 사용 가능 서비스를 중앙에서 제어하는 SCP(서비스 제어 정책) 생성 가능

□ Shield[26)]

- 웹 애플리케이션을 보호하는 디도스(DDoS) 보호 서비스

- AWS Shield에는 두 계층 존재
  - Shield Standard : 추가 비용 없이 Shield Standard에 의한 자동 보호 기능 제공. 네트워크 및 전송 계층 DDoS 공격으

25) Amazon AWS 홈페이지, “AWS Organizations”, https://aws.amazon.com/ko/organizations/

26) Amazon AWS 홈페이지, “AWS Shield”, https://aws.amazon.com/ko/shield/

로부터의 보호 수행

- Shield Advanced : Shield Standard가 제공하는 일반적 네트워크 및 전송 계층 보호 이외에, 정교한 대규모 DDoS 공격에 대한 추가 보호/완화, 실시간의 공격 가시성, WAF(웹 애플리케이션 방화벽)과의 통합 등을 제공

□ WAF[27)]

- 웹 애플리케이션 방화벽

- 웹 취약점 공격으로부터 웹 애플리케이션을 보호

- SQL 명령어 주입이나 크로스 사이트 스크립팅 등 일반적인 공격 패턴을 차단하는 사용자 지정 규칙과 특정 애플리케이션을 위해 설계된 규칙을 생성할 수 있음

- 웹 보안 규칙의 생성, 배포 및 유지보수를 자동화하는 데 사용할 수 있는 모든 기능을 갖춘 API가 포함되어 있음

□ Macie[28)]

- 머신 러닝을 사용하여 AWS에 저장된 민감한 데이터를 자동으로 검색, 분류 및 보호하는 보안 서비스

- 머신러닝으로 특이/이상 접근 판단

- 개인 식별 정보(PII) 또는 지적 재산과 같은 민감한 데이터를 인식하고, 이러한 데이터가 어떻게 액세스되고 이동되는지 파악할

27) Amazon AWS 홈페이지, “AWS WAF” , https://aws.amazon.com/ko/waf/

28) Amazon AWS 홈페이지, “Amazon Macie”, https://aws.amazon.com/ko/macie/

수 있는 대시보드 및 알림을 제공

- 비정상적인 데이터 액세스 활동을 지속적으로 모니터링하여 무단 액세스 또는 의도하지 않은 데이터 유출 위험이 감지될 경우 상세한 알림을 생성

- Amazon S3에 저장된 데이터를 보호할 수 있음

- 장점 : 우수한 데이터 가시성, 간단한 설정, 쉬운 관리, 머신 러닝을 통해 데이터 보안 자동화 등

3. AWS 보안 서비스 주요 특징

□ AWS 가상 머신

- Xen Hypervisor를 수정하여 개발

- 보안 강화를 위한 맵핑 서비스 등 추가 개발 (VM을 분리하기 위해)

□ AWS 가상 머신(EC2) 접속 방법

- 키 쌍을 사용한 SSH 접속
  - 키 쌍 생성 후 공개키는 AWS 쪽에 보관하며, 인스턴스를 생성할 때 사용
  - AWS EC2 서버에 접속 시, 클라이언트에서 개인키를 이용하여 SSH 접속 (ID에 대한 패스워드는 미입력 가능)

- 윈도우 인스턴스 접속
  - 접속 방법이 리모트 데스크톱이므로 SSH 대신 리모트 데스크톱 포트를 열어줘야 함. SSH 공개키 인증이 아닌 리모트

데스크톱의 비밀번호(관리자 비밀번호) 인증

□ Security Manager Agent

- 원하는 보안을 추가할 수 있다 함

- 모든 행위에(SDK, Storage, EC2, 웹서버, 커스터머의 콜마다) 인증(Authentication)을 요구함

□ 인증

- 금융기관 등 고객사의 몫
- AD, Trust Relationship, Temporary Token, Internal Signature 등 여러 방식 이용 가능
- 멀티 팩터(2-factor) 인증 가능
- ID/패스워드 또는 랩탑의 특정버튼 누르기 등 가능
- UBkey로 인증도 가능

□ PKI 관련

- 인증서 사용시 클라우드 사용 가능하게 할 수 있음

- 외부의 PKI를 integration 가능함

- 가능 범위가 SSL/TLS에 한정되는지는 명확하지 않음

□ 암호화 관련

- DBMS 암호화 가능, 암호화 해서 DB에 넣어야 함
- DB 전용 암호화 솔루션은 아닌 것으로 판단됨
- 기존 DB의 암호화 feature 이용 가능

- 디스크 볼륨 암호화 가능
- 클라우드 안과 밖에서 모두 암호화 가능
- 유비쿼터스 암호화(encryption)

□ AWS 획득 인증

- ISO 9001, SOC, ISO 27001, CSA 등 (20여개)

□ 기타 사항

- Managed Service 이용 가능
- LB, FW, IPS, IDS 등 Security Solution : AWS 자체 솔루션도 가지고 있음
- 1800 이상 보안 컨트롤

Ⅴ. AWS 및 클라우드 관련 동향

1. 미국 금융권 등 이용 동향

□ Capital One, FINRA, Pacific Life 등 금융 서비스 고객[29)]

- 크리티컬 워크로드를 AWS로 이전하고 고성능 컴퓨팅, 데이터 분석, 디지털 변혁, 보안 및 규정 준수, 재해 복구 등과 같은 영역에서 효율성을 실현하고 있음

※ 캐피탈 원 CIO : '클라우드에서 보안을 더 좋게 할 수 있다.'

□ Simple

29) Amazon AWS 홈페이지, "금융 서비스 클라우드 솔루션", https://aws.amazon.com/ko/financial-services/

- Banco Bilbao Vizcaya Argentaria(BBVA)의 자회사로 고객 지향의 클라우드 우선 온라인 은행

□ FINRA

- AWS에서 제공하는 도구를 사용해 매일 수십억 개의 시장 이벤트를 분석할 수 있게 되었음

- EVP & CIO : '클라우드가 셀프 호스팅보다 더 안전하다'

- FINRA[30]에서 AWS 이용 후, 안전성에 대한 문의는 별로 없고, 도입/적용 방법에 대한 문의가 많아졌다고 함

□ Pacific Life

- AWS 덕분에 운영업무보다 혁신에 더 많은 시간 할애 [27]

□ 34개 은행이 AWS 서비스 이용하며, 그중 50% 정도가 크리티컬한 데이터를 저장함

□ 에이온 (보험사)

- 10일 걸린 특정 계산 업무를, GPunit 이용시 10분으로 단축

□ AIG : 씨카드 계산, 부하테스트 등에 AWS 이용

□ DTCC(Depository Trust & Clearing Corporation)

- 세계 최대 금융거래정보저장소로, 클라우드 컴퓨팅 이용

30) financial Industry Regulatory Authority : 캐피탈 마켓 감시 감독 기관, 브록커 딜러 4,600 회사 등 관리 감독

□ 나스닥

- 2~3개 레거시 DW에 AWS Redshift(데이터 분석) 서비스 이용

□ 기타 미국 동향

- 헬스케어 등 민감정보도 AWS에 저장
- 정부/정보기관도 AWS 이용 추세
- 그리드 컴퓨팅, 대형 워크로드가 클라우드로 많이 옮겨 감
- 코어뱅킹 마이그레이션은 아직은 많지 않음

□ AWS 적용을 위한 교육

- GE : 3000명을 3년간 교육
- Capital One : 5천명을 2년간 교육

2. 미국 제도 법규 동향 (금융권 클라우드 적용 관련)

□ FFIEC[31] 핸드북

- Risk based, Result based (Technology based가 아님)
- 무엇을 고려하고 따라야만 하는지에 대한 얘기만 나옴
- 데이터센터 등에 대한 물리적 분리 관련 내용도 없음

□ Guidance from ICC

- 아웃소싱을 금지하지 않으며 그에 대한 기준 언급이 있음 (2013~19, Suggestion for Outsourcing)

31) 미국 연방금융기관 검사협의회(Federal Financial Institutions Examination Council, FFIEC)

□ 최근 클라우드 관련 인식

- 클라우드가 없이는 IDC 구축 비용이 너무 많이 든다는 것을 정부/기관 등도 동의하고 있다고 함 (대기업보다 중소기업)

※ AWS의 국내 금융 고객사로는 미래에셋자산운용을 제시

3. 싱가포르, 홍콩 동향

□ 싱가포르 DBS 은행

- 2018년까지 최소 50%의 워크로드를 AWS로 옮길 계획
- 고객의 보험을 클라우드 AI가 분석
- 청산, 결제, 증권을 블록체인에도 올림(블록체인이 아닌 기존 시스템과 병렬 운영)

□ 싱가포르 MAS (Monetary Authority of Singapore)

- “Innovation lab” 운영
- “Cloud Relevant Guildelines” 발표
  - 2013년에는 매우 엄격
  - 2016년 : guideline on outsourcing 만듦
    (2016년에 논리적 분리도 안전함을 인정)
- 은행간 데이터 공유를 금지하지 않음

□ 홍콩 금융권 동향

- 핀테크 규제 샌드박스 구성
- 대출, 결제에 블록체인 이용
- 정보보호 관련 법률 발표
- CPS 231 가이드라인 등에서 아웃소싱 관련 내용 포함

Ⅵ. 시사점 및 고려사항

1. 클라우드 관련 법규 이슈

□ 한국 등 국가에서 “data residency” 요구사항이 있음

- 시스템, 데이터 등의 자국 내 존재 요건

□ 법규 상 물리적 분리 요건이 존재할 경우 제약 발생

- 클라우드는 고객사 간 물리적 분리가 아닌 논리적 분리임

□ 민감 정보 보안 관련 법적 허용 여부

- AWS 등 클라우드 벤더사는 데이터 암호화 기능을 제공함

- 고객사에서 암호화 기능을 적용하지 않을 경우, 기술적/이론적으로 클라우드 벤더사가 접근 가능하다 함

- 단, AWS의 경우 관리적/정책적으로 절대 접근을 하지 않는다 함

- 기술적/이론적으로 금융사의 민감정보를 클라우드 벤더사가 접근 가능한 상황에서, 금융 핵심 서비스의 클라우드 이관에 대한 허용 여부가 이슈사항임

□ 클라우드 벤더간 이동성 (Reversablilty)

- ‘클라우드 벤더 이동이 쉬운가?’가 정부 관심사항 중 하나임

- 다양한 이관 사례가 존재한다 함 (AWS→타사, 타사→AWS)

- AWS는 법적/계약상 “Lock-in”이 없으며 옮겨가는 것까지 지원해 준다 함

- 페타 바이트 이동시 스노우 볼 지원 (전용 어플라이언스에 박싱, 쉽핑 후 송부)

  ※ 타 클라우드 벤더로 이동시, 업무 내 클라우드 API 이용 부분을 모두 수정하는 등 많은 공수가 필요할 것으로 보임

  ※ 법적/계약상의 “Lock-in”은 없으나, AWS API 등에 대한 고착화에 따른 “Lock-in”은 불가피할 것으로 판단됨

  ※ “Lock-in”의 주 원인은 클라우드 벤더간 API의 차이로 보이나, 현재 벤더간 API 표준화 움직임 등은 없으며, AWS도 관련 필요성을 느끼지 않고 있는 것으로 보임

2. 클라우드 보안/인증 관련 이슈

□ 금융 고객의 민감 정보 보호 방안

- 금융 고객사에서 암호화 기능을 적용하지 않을 경우, 기술적/이론적으로 클라우드 벤더사가 접근 가능함

- 이는 다수 금융기관이 중요업무를 클라우드로 이관하지 않는 주된 이유로 보임

- 클라우드 서비스 제공자 입장에서는, 클라우드 적용시 민감정보를 쉽고 성능저하 없이 보호할 수 있는 방안 제시가 필요할 것으로 판단됨 (고객 불편 없는 자동 암호화 방안 등)

3. 클라우드 도입 장벽과 AWS[32)]

□ 클라우드 도입 장벽

- 보안
- 규제
- 대상 워크로드
- 아키텍처, 구현
- 운영, 유지보수

□ 보안과 규제 준수 및 선도

- AWS는 기존의 보안과 규제에 적합하도록 서비스를 제공할 뿐 아니라 최근에 가시화와 통제, 감사에서 더 많은 혁신을 하고 있는 것으로 주장

- 가시화(Visibility)
  - 단지 원클릭으로 고객의 전체 인프라를 볼 수 있는 환경. 로깅 분석을 통한 통찰력 있는 분석 가능

- 관리 및 통제(Control)
  - 데이터가 저장되어 있는 위치와 권한에 따른 엄격한 관리. AWS와 고객의 책임 공유 모델 (Shared Responsibility Model) 수행 등

- 감사(Auditability)
  - 3rd 파티 검증 및 중요한 워크로드에 대한 인증 (Certification) 등

※ “자사의 경험에 의하면, 자체 데이터센터보다 AWS 클라우드

32) 정우진, “한국 금융권을 위한 aws cloud 도입 제언”, AWS Finance Seminar, https://www.slideshare.net/awskorea/cloud-adoption-strategy-for-fsis-63860548

의 보안이 더 강력하다고 생각됩니다." - Tom Soderstrom, CTO, NASA JPL

4. 보안 패러다임의 전환

□ 보안 패러다임의 전환 (레거시 데이터 센터 → AWS)

- 넓은 물리적 공간 → 좁은 물리적 공간
- 전체 소유 → 필요한 만큼만 소유 (Own just enough)
- 모든 것을 직접 구축 → 핵심 가치에 집중
- 직접 관리하는 서비스 → 플랫폼 서비스
- 정적 아키텍처 → 지속적 진화 아키텍처
- 집중되지 않은 관리 → API를 통한 중앙 집중 관리

□ API 기반의 보안 등 패러다임의 전환에 적응 필요