2025학년도 1학기 문헌연구보고서

안전한 클라우드 스토리지 서비스(Cloud Storage Service) 사용 방법 제안
- 이용자 차원에서

이름	서웅진
전공	경영학부 경영학전공
학번	20192663

안전한 클라우드 스토리지 서비스(Cloud Storage Service) 사용 방법 제안
- 이용자 차원에서

목차

본 보고서에서는 클라우드 컴퓨팅(Cloud Computing)[1] 자체의 고질적인 보안 취약성과, 클라우드 서비스(Cloud Service)[2] 운영 중 발생하는 보안 문제를 다룬다. 용어의 통일성과 독자의 가독성을 고려하여, 이들을 포괄하여 '클라우드 서비스'로 통칭한다.

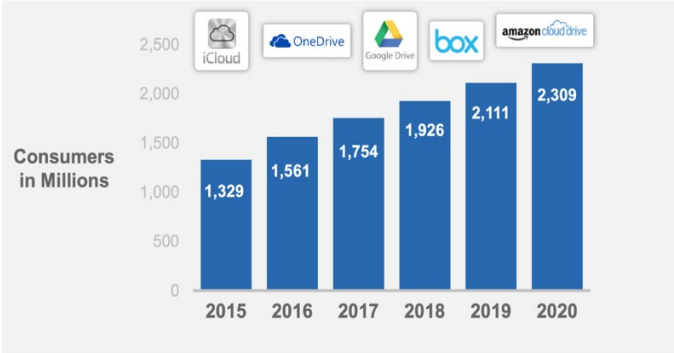
1) 이용자 입장에서, 인터넷(Internet)을 기반으로 서버(Server), DB(Database), 애플리케이션(Application) 등 다양한 IT(Information Technology) 자원을 필요에 따라 제공받아 사용하는 컴퓨팅(Computing) 기술 또는 개념이다.

2) 클라우드 컴퓨팅을 바탕으로 이용자에게 실제로 제공되는 서비스(Service)이다. 이용자는 로컬(Local) 장비에 직접 소프트웨어(SW)를 설치하거나 자원을 저장하지 않고, 인터넷을 통해 원격 서버에 접근하여 이들을 활용할 수 있다. 일반적으로 IaaS(Infra as a Service), PaaS(Platform as a Service), SaaS(Software as a Service)의 세 가지 형태로, 이용자가 제어할 수 있는 IT자원의 범위와 권한 수준에 따라 구분된다.

Ⅰ. 서론

2000년대 초, 정보화 시대로 접어들어 인터넷과 네트워크(Network)가 크게 발전 및 확산되면서, 확장된 IT 인프라(Infrastructure)가 요구되고 인터넷 서비스에 대한 수요가 높아졌다. 이와 함께, 이용자가 IT 자원들을 효율적으로 제공받을 수 있는 클라우드 서비스가 대두되었다. 그 덕에 이 서비스를 이용하는 기업의 경우, IT 인프라에 대한 관리 부담을 줄이면서 자사의 핵심 사업에 집중하면서 비용 효율성을 극대화할 수 있게 되었다. **Cisco**[3] Global Cloud Index 보고서에 따르면, 2020년에는, 클라우드 데이터 센터(Cloud Data Center)에서 처리되는 Installed Workload[4]의 수가 약 4억 개로 예상되며, 이는 전체 데이터 센터(Data Center)에서 Installed Workload를 처리하는 비중의 약 92%의 점유율을 차지하는 수치이다(Thomas Barnett Jr.·Arielle Sumits·Shruti Jain·Usha Andra·Taru Khurana, 2016. 11.:15).

또한, 정보화 시대의 핵심인 데이터(Data)[5]를 효과적이고 안전하게 관리할 수 있는 저장소에 대한 필요도 생겨났다. 그 대안으로, 이용자에게 용이한 데이터 백업(Data Backup) 기능을 제공하며, 이용자 접근성 및 네트워크 간 확장성이 높은 클라우드 스토리지 서비스(Cloud Storage Service)[6]가 해결책으로써 널리 활용되고 있다(이세원·홍아름·황준석, 2015:1~36). 실제로 <표1>을 통해 확인할 수 있듯이, 2020년 클라우드 스토리지 서비스의 이용자 수는 약 23억명으로 추산된다.



<표 1> 클라우드 스토리지 서비스 이용자 수

(Thomas Barnett Jr.·Arielle Sumits·Shruti Jain·Usha Andra·Taru Khurana, 2016. 11.:39)

---

3) 네트워크 산업을 선도하는 세계적인 IT 기업이다.

4) 본 단어의 정확한 의미를 정의하는 자료를 찾는데 어려움이 있어, ChatGPT의 답변으로 대신한다.
데이터센터 내에서 실제로 구동 중인 애플리케이션, 서비스, 가상머신, 컨테이너, 혹은 기타 컴퓨팅 작업 단위를 의미한다. 또한, 사내 ERP(Enterprise Resource Planning)와 같은 소규모 애플리케이션에 사용되는 Installed Workload는 3~10개 정도이며, 대형 포털(Portal)과 같은 대규모의 경우에는 수백 개 정도로 추정된다.
(ChatGPT 질문 글: "Data Center 개념에서 Installed Workload의 정의와, Installed Workload의 수량의 의미를 알기 쉽게 애플리케이션의 규모 별로 단일 애플리케이션에 사용되는 수량을 정리해서 알려줄래?")

5) 가공되지 않은 사실이나 수치이다. 지식의 발전 단계를 설명하는 DIKW 모델(Model)은, 데이터(Data)->정보(Information)->지식(Knowledge)->지혜(Wisdom)로 설명한다. 예를 들어, 데이터가 모여 정보를 구성한다. 정보화 시대로 접어들면서 정보와 함께 해당 모델의 기본단위인 데이터의 활용 및 관리가 중요해졌기에 본문에서는 '정보'가 아닌 '데이터'를 중심으로 서술하였다.

6) 이용자 제어 권한이 가장 낮은 SaaS의 한 종류로써, 데이터 저장소 서비스이다. 예로는, **Google Drive, Apple iCloud, Naver Cloud, Dropbox** 등이 있다.

그러나 이용자 수의 가파른 증가만큼 보안 사고의 위험성도 커진다. 보안 취약점과 같은 원인으로 인해 데이터 유출이 발생할 경우, 심각한 사태가 초래될 수 있다. 2012년, 약 6,800만 명의 이용자 정보가 유출된 **Dropbox** 보안 사고는 클라우드 보안의 중요성을 일깨운 대표적인 사례이다(Twingate Team, 2025. 5. 29.). 지금까지 클라우드 스토리지 서비스의 데이터 보안을 위해 클라우드 스토리지 서비스 회사에 대하여, 데이터 접근 제어 및 보안 키(Key) 관리 혹은 권한 관리 프로토콜(Protocol) 설계 혹은 아키텍처(Architecture) 설계와 관련하여 더 나은 방법을 제안하거나, 이용자의 사용 의도를 분석한 연구들은 있었다(신재복·김윤구·박우람·박찬익, 2013:303~309;민소연·이광형·진병욱, 2016:12~20;곽진·배원일·이은지, 2017:266~269;민경회·곽찬희·최한별·이희석, 2020:1~24). 하지만, 보안 사고로부터 보호받기 위해 이용자가 직접 행동할 수 있는 방법에 대한 연구는 없는 것으로 확인된다. 본 보고서는, 과거에 발생했던 보안 사고의 원인과 이에 대한 해결 수준을 중심으로 현재의 클라우드 스토리지 서비스의 보안 수준을 파악하여, 이용자가 보안 문제로부터 안전하게 서비스를 사용할 수 있는 방법들을 제안하고자 한다.

Ⅱ. 클라우드 스토리지 서비스(Cloud Storage Service) 보안 사고 원인

1. 클라우드 스토리지 서비스 회사 차원의 원인

(1) 상존하는 해킹(Hacking) 위험과 보안 취약점

2024년 **Dropbox Sign**[7] 보안 사고에서 모든 이용자의 이름과 이메일 주소(Email Address), 일부 이용자의 전화번호 및 해시된(Hashed) [8] 비밀번호와 OAuth[9]와 같이 민감한 보안 정보가 유출되었다. **Dropbox Sign** 자동화 시스템 구성 도구에 대한 접근(access to a **Dropbox Sign** automated system configuration tool)을 얻은 해커(Hacker)가 백엔드(Backend)[10]에 접근한 것이다(Patrick Spencer, 2024. 5. 3.). 정확한 해킹 경로는 알려지지 않았고, 이를 찾지 못한 사례는 비단 이 사건에 한정되지 않는다. 2020년에 발생한 **EMA**(European Medicines Agency) 해킹 사건, 2019년에 발생한 미국의 금융회사 **Capital One** 보안 사고 또한 이에 대해 정확히 알려지지 않았다. 이를 정확히 규명하지는 못하는 이유는 정교해지는 해킹 수법과 같은 해커 차원의 것과, 보안을 기업의 핵심 요소로 인식하지 못하여 불충분한 투자가 이루어지는 기업 문화와 같은 회사 차원의 것 등이 있다(John Leyden, 2024. 11. 12.). 그러므로, 해킹을 막기 위한 근본적인 문제를 해결하지 못한다면 해킹 위험과 보안 취약점은 상존할 것이다.

---

7) **Dropbox**의 자회사이자 전자 서명 서비스이다.

8) 해시는, 데이터 유출 시 피해를 막기 위해 해시 함수를 이용해서 중요 데이터를 변형하는 것을 의미한다.

9) 공개된 권한 허용(Open Authorization)의 준 말이며, 제 3자 애플리케이션에 대한 사용자 정보를 알지 않고도, 특정 리소스(Resource)에 제한된 접근 권한을 받을 수 있도록 도와주는 인증 표준 프로토콜이다. 예를 들어, **ChatGPT** 로그인(Log-in) 창에서, '**Google** 계정으로 계속'을 통해 **ChatGPT** 서비스를 사용할 수 있는 것이다.

10) 웹이나 앱 개발에서 구분된 영역 중 하나이다. UI(User Interface)와 같이 이용자와 직접적으로 상호작용하는 영역을 프론트엔드(Front-End), DB 및 서버와 같이 사용자가 볼 수 없는 곳에서 서비스 운영을 돕는 백엔드로 나뉜다.

(2) 서비스 책임자의 낮은 수준의 보안 인식: 자격 증명 재사용

서론에서 언급한 2012년 **Dropbox** 보안 사고는 같은 년도에 발생한 **LinkedIn** 해킹 사건과 밀접한 관련이 있다(David Mosyan, 2023. 8. 1.). 해킹 피해를 당한 **Dropbox**의 한 직원이 회사 계정의 비밀번호를 **LinkedIn** 비밀번호와 동일하게 사용하고 있었고, 이를 통해 해커는 해당 직원의 회사 계정에 저장되어 있던 이용자들의 개인 정보에 접근하였다(Twingate Team, 2025. 5. 29.). 이 사례는 서비스 책임자의 낮은 수준의 보안 인식이 어떻게 보안 사고로 이어지는지를 단적으로 보여준다.

2. 이용자 차원의 원인

(1) 이용자가 쉽게 속을 수 있는 피싱(Phishing)[11]

2014년 **iCloud** 유명인 사진 유출 사건은 특정 유명인들의 **iCloud**에 저장되어 있던 사진이 유출된 일이다(Edwin Chan·Christina Farr, 2014. 9. 4.). 피싱 범죄자인 Ryan Collins의 소행으로 추측되며, 2016년 3월 그는 1년 6개월 징역을 선고받았다. 그의 피싱 방식은 **Apple 및 Google**을 사칭하여 이용자들에게 ID(Identifier)와 비밀번호를 요구하는 이메일(Email)을 보낸 것이다(U.S. Attorney's Office, Central District of California, 2016. 10. 27.). 또 다른 사례로는 주로 학생이나 교직원에게 공유 작업이 빈번하게 이루어지는 **Google Docs**를 사칭하는 이메일을 보내, **Google** 로그인 창과 유사한 홈페이지로 유인한 후 그들의 자격증명을 훔치는 피싱 범죄가 존재한다(Montclair State University, 2025. 2. 27.). 그러므로, 서비스의 보안을 책임지는 회사뿐만 아니라 이용자 또한 보안 사고의 표적이 될 수 있음을 인지해야 한다.

(2) 민감한 데이터(Data)의 부적절한 공유 범위 설정

2017년 3월부터 2023년 11월까지, 일본에 본사를 둔 게임(Game) 개발 기업 **Ateam**이 **Google Drive**에 보관하는 일부 개인 정보를 공유 범위 제한 없이 링크(Link)를 가진 모두가 열람할 수 있게 설정하였다. 이로 인해, 이용자의 정보를 포함한 1,369건의 회사 개인 정보가 유출되었다(Ateam Holdings, 2023. 12. 20.). 또한, 영국의 사이버(Cyber) 보안 기업인 **Metomic**의 2023년 **Google** 스캐너(Scanner)[12] 보고서에 따르면, 약 650만 개의 스캔된 **Google Drive** 파일(File)의 34.2%(약 210만 개)가 회사 도메인(Business) 외부의 이메일 주소와 공유되어 있으며, 0.5%(약 3만 개)가 링크를 가진 모두가 열람할 수 있도록 설정되어 있다고 밝혔다(Metomic, 2025. 3. 20.). 2017년 기준 **Google Drive** 파일의 개수가 2조개로 추산되며(Matthew Humphries, 2017. 5. 8.), 이를 미루어 보았을 때 단순 계산으로, 100 억개의 파일[13]이 링크를 가진 모두가 열람할 수 있는 것으로 추정된다. 앞서 언급한 보안 사고와 링크가 오픈(Open)된 파일의 수는, 이용자가 데이터의 공유 범위 설정에 대하여 신중을 기할 필요가 있음을 시사한다.

---

11) 개인 데이터(private data)와 피싱(fishing)의 합성어이다. 이용자와 관련된 신뢰할 수 있는 기관을 사칭하여 이메일이나 전화를 통해, 이용자의 개인정보를 낚는다는 의미이다.

12) **Metomic**의 보안 진단 도구를 의미한다. 즉, **Google** 스캐너란 **Google** 서비스의 보안을 진단하는 도구를 의미한다.

13) 2조 * 0.5% = 100억.

Ⅲ. 현재의 클라우드 스토리지 서비스 보안 수준: 보안 취약점 대응 방식에 관하여

Ⅱ장에서 서비스 책임자의 낮은 수준의 보안 인식 및 보안 취약점과 같은 회사 차원의 원인과, 피싱 및 부적절한 데이터 공유 범위 설정과 같은 이용자 차원의 원인으로 인한 보안 사고가 존재하는 것을 확인했다. 보안 취약점을 제외한 3개의 원인은 기술적인 부분이 아닌, 인간 중심 대응 관점에서 바라보는 것이 적절할 것이다. 그러므로, 위 3가지 원인에 대해서는 Ⅳ장에서 서술하며, 이 장에서는 보안 취약점 대응 방식에 관한 현재의 클라우드 스토리지 서비스의 보안 수준에 대하여 살펴보고자 한다.

먼저, 클라우드 스토리지 서비스는 클라우드 서비스 중 하나인 점을 상기할 필요가 있다[14]. 클라우드 서비스 고유의 보안 특성을 알아보기 위해, 이 서비스가 존재하기 이전의 IT자원을 관리했던 방식을 함께 살펴보아야 한다. 과거 주된 방식은 온프레미스(On-Premise)[15] 혹은 데이터 센터 공간 대여 방식이었다. 이 2 가지 방식은 IT 자원을 이용자가 직접 관리하며, 물리적인 방식으로 구축된다는 공통점을 가진다. 이와 달리, 클라우드 서비스는 IT자원 관리 권한의 대부분이 서비스 회사에게 있으며, 가상화된 환경에서 서비스를 제공한다(Kacha, L.·Zitouni, A.,2018:1;Kacha, L.·Zitouni, A.,2018:3). 이와 같은 클라우드 서비스의 2가지 특징은 양날의 검이다. 이용자는 IT자원을 효율적으로 제공받아 관리하는 반면에, 가상화된 환경에서 존재할 수 있는 보안 위협으로부터 이용자의 예방 및 대응 가능성을 극도로 축소시킨다는 문제점을 야기한다. 예를 들어, 서비스 회사의 보안 취약점으로 인해 데이터가 유출되거나 소실된다고 하더라도, 데이터의 실소유주인 이용자는 회사의 조치에 기대야 하는 상황이 발생하게 된다. 그러므로 서비스 회사는 이용자가 보안 문제로부터 안전하다고 느낄 수 있도록, 정기적으로 보안에 대한 외부 검증을 받거나, 이용자의 IT 자원에 대한 관리 권한은 높이되 관리 부담은 최소화하는 등의 조치를 취해야 한다.

Ⅳ. 이용자 차원의 안전한 클라우드 스토리지 서비스 사용 방법

1. 높은 보안 인식 고취: 자격 증명 재사용/피싱/부적절한 데이터 공유 범위 설정에 관하여

서비스 책임자 뿐만 아니라, 이용자도 자격 증명 재사용을 주의해야 한다. 피해 규모가 작을 뿐 피해를 입을 가능성은 동일하게 존재하기 때문이다. 다음으로, 피싱을 완벽히 막을 뚜렷한 대안을 찾는 것은 어려울 것이라고 생각한다. 앞으로 수법은 더 교묘해질 것이기 때문이다(James Martin, 2025. 5. 22.). 따라서, 이메일 및 전화뿐만 아니라 실제 서비스를 제공하는 애플리케이션 등 경로와 상관없이 개인정보를 요구하는 일이 발생한다면, 일정한 시간을 두고 실제 서비스에서 제공하는 절차인지 여부를 먼저 확인해야 한다. 마지막으로, Ⅱ장에서 추정된 약 100 억 개의 파일이 링크가 오픈 되게 설정된 점은, 링크를 신뢰하는 계정에게 공유하였기에 이 방식이 신뢰 가능하다고 판단된 결과라고 생각한다[16]. 그러나, 이용자는 신뢰되지 않은 제3자가 누군가의 중요 데이터의 링크를 알아낼 수도 있다는 점(bomber bot, 2024. 4. 20.)을 유념하며, 파일 건별로 적절한 공유 범위 설정에 대한 검토가 필요하다.

14) 클라우드 스토리지 서비스의 보안은 곧 클라우드 서비스의 보안을 의미한다. 이 장에 한해, 2개의 단어를 혼용하지만 의미는 거의 동일하다.

15) IT자원을 가상화 된 서비스로 빌려주는 클라우드 서비스와 달리, 자체적으로 IT 자원을 구축하는 것을 의미한다.

16) 잘 사용되지 않는 일명 트래쉬(Trash) 파일의 존재도 이유에 포함될 것이다.

2. 중요 정보는 로컬(Local) 저장소 보관 혹은 백업(Backup)

앞서 언급한 보안 사고들과 현재의 클라우드 스토리지 서비스의 보안을 고려했을 때, 이 서비스에만 기대는 것은 위험한 생각이다. 양날의 검과 같은 이것의 보안 특성의 단점을 회피할 수 있는 가장 간단한 방법은, 물리적 손상만 피한다면 거의 안전하게 데이터를 보관할 수 있는 USB(Universal Serial Bus)와 같은 로컬 저장소를 이용하는 것이다. 특히 중요 정보를 보관하는 것을 권장하며, 활용도가 높은 것의 경우 클라우드 스토리지 서비스에 저장하되, 로컬 저장소에도 백업하는 것을 권한다.

V. 결론

이 글의 목적은 클라우드 스토리지 서비스가 이것의 유용성 덕분에 쉽게 대중화되었지만, 데이터를 다루는 서비스이기에 운영과 이용에 있어 주의가 요구되는 몇 가지 지점들이 존재하고, 이에 대해 서비스를 제공하는 회사뿐만 아니라 이용자도 인지해야 할 필요성이 있다는 것이다. 이러한 점에서, 과거에 발생한 보안 사고의 원인들과 이들 중 기술적인 면에서 해결책을 강구해야 할 회사의 보안 취약점과 관련한 보안 수준을 고려하여, 이용자가 보안 사고로부터 안전하게 서비스를 사용할 수 있는 몇 가지 방법들을 제안하였다.

서비스 회사가 아닌 이용자 측면에서의 연구가 적은 이유는, 서비스 특성상 대부분의 관리 권한이 회사에 있기에 회사 측면에서 방법을 찾는 것이 효과적이기 때문으로 추측된다. 그러나 보안 사고 발생 시 피해자가 2명[17]이며, 각각의 피해자에게 방법을 찾을 수 있는 열쇠가 필요하다고 생각한다. 본 보고서는 이용자에게도 클라우드 스토리지 서비스의 보안에 대하여 생각해볼 거리를 남기며, 보안 사고에 대비하고, 보안 사고 발생 시에도 피해를 최소화할 수 있는 방법에 대한 열쇠를 쥐여주었다는 점에서 의의가 있다.

이용자들의 IT 관리에 대한 부담을 덜어주기 위해, 서비스의 관리 권한이 회사에 치중되어 있기에, 이러한 서비스의 특성은 앞으로도 지속될 것이라고 생각한다. 그러므로, 단지 기술적인 측면이 아닌 다각화된 시선에서 이용자가 서비스를 안전하게 이용할 수 있는 방법을 모색하는 연구가 진행되어, 클라우드 스토리지 서비스가 앞으로 안전하게 운영되고 사용되기를 바란다.

17) '2명'은 회사와 이용자를 의미하며, 2 부류 혹은 2그룹(Group)이란 말이 더 적절하다. 하지만 이 문맥에서는, 회사와 이용자가 이분법적으로 나뉘어 회사만 고민하는 것이 아닌 모두가 함께 해야 할 필요성이 있다는 판단 하에, 양자 간의 관계성을 높이기 위해 '2명'이라는 비유적 표현을 사용했다.

[참고문헌]

- 곽진·배원일·이은지 (2017), 「클라우드 스토리지 보안을 위한 보안 아키텍처 설계 연구」, 『한국정보처리학회 학술대회논문집』 24(1), 한국정보처리학회, 266~269 쪽.
- 민경회·곽찬희·최한별·이희석 (2020), 「개인용 클라우드 서비스 사용 의도 연구 : 가치 비교를 중심으로」, 『경영정보학연구』 22(2), 한국경영정보학회, 1~24 쪽.
- 민소연·이광형·진병욱 (2016), 「클라우드 환경에서 안전한 스토리지 접근 제어를 위한 권한 관리 프로토콜 설계」, 『한국산학기술학회 논문지』 17(9), 한국산학기술학회, 12~20 쪽.
- 이세원·홍아름·황준석 (2015), 「클라우드 스토리지 서비스에 대한 개인 사용자의선호 요인 연구」, 『기술혁신연구』 23(1), 1~36 쪽.
- 신재복·김윤구·박우람·박찬익 (2013), 「모바일 클라우드 스토리지 서비스에서의 데이터 보안을 위한 데이터 접근 제어 및 보안 키 관리 기법」, 『대한임베디드공학회논문지』 8(6), 대한임베디드공학회, 303~309 쪽.
- bomber bot (2024. 4. 20.), *Google Dorking For Penetration Testers — A Practical Tutorial*, BOMBERBOT, https://www.bomberbot.com/penetration-testing/google-dorking-for-penetration-testers-a-practical-tutorial/?utm_source=chatgpt.com (2025. 6. 1.).
- David Mosyan (2023. 8. 1.), *How exactly hackers got into LinkedIn and Dropbox*, Medium, https://medium.com/%40dmosyan/how-exactly-hackers-got-into-linkedin-and-dropbox-f153e96f6abc (2025. 5. 30.).
- Edwin Chan·Christina Farr (2014. 9. 4.), *Apple says its systems not to blame for celebrity photo breach*, Reuters, https://www.reuters.com/article/lifestyle/apple-says-its-systems-not-to-blame-for-celebrity-photo-breach-idUSKBN0GX29C/?utm_source=chatgpt.com (2025. 5. 31.).
- James Martin (2025. 5. 22.), *7 AI Cybersecurity Trends For The 2025 Cybercrime Landscape*, Exploding Topics, https://explodingtopics.com/blog/ai-cybersecurity?utm_source=chatgpt.com (2025. 6. 1.).
- John Leyden (2024. 11. 12.), *'파악하기 어려워지는 보안 침해 원인'… 현직 전문가가 밝힌 이유 7 가지*, CIO, https://www.cio.com/article/3603010/점점-더-파악하기-어려운-보안-침해-원인---현.html (2025. 6. 4.).
- Kacha, L.·Zitouni, A. (2018), *An Overview on Data Security in Cloud Computing*, arXiv:1812.09053.
- Matthew Humphries (2017. 5. 8.), *Google Drive Passes 2 Trillion Files Stored*, PC MAG, https://uk.pcmag.com/onlinecloud-backup-services/89223/google-drive-passes-2-trillion-files-stored (2025. 5. 31.).
- Metomic (2025. 3. 20.), *Metomic finds 40% of Google Drive files contain sensitive information, putting organizations at risk of a data breach*, Metomic, https://www.metomic.io/resource-centre/metomic-finds-40-of-google-drive-files-contain-sensitive-information-putting-organizations-at-risk-of-a-data-breach (2025. 5. 31.).
- Montclair State University (2025. 2. 27.), *Sneaky Google Docs Phishing Scam on the Rise!,* Montclair State University, https://www.montclair.edu/phish-files/2025/02/27/sneaky-google-docs-phishing-scam/ (2025. 6. 4.).
- Patrick Spencer (2024. 5. 3.), *Mitigating the Risk of Software Supply Chain Attacks: Insights From the Dropbox Sign Breach*, Kiteworks, https://www.kiteworks.com/cybersecurity-risk-management/dropbox-sign-breach/?utm_source=chatgpt.com (2025. 5. 30.).
- Thomas Barnett Jr.·Arielle Sumits·Shruti Jain·Usha Andra·Taru Khurana (2016. 11.), *Cisco Global Cloud Index 2015–2020*, Cisco, https://www.cisco.com/c/dam/m/en_us/service-

provider/ciscoknowledgenetwork/files/622_11_15-16-Cisco_GCI_CKN_2015-2020_AMER_EMEAR_NOV2016.pdf (2025. 5. 20.).
- Twingate Team (2024. 5. 23), *What happened in the Dropbox data breach?*, Twingate, https://www.twingate.com/blog/tips/dropbox-data-breach (2025. 5. 29.).
- U.S. Attorney's Office, Central District of California (2016. 10. 27.), *Pennsylvania Man Sentenced Today to 18 Months in Federal Prison for Hacking Apple and Google E-Mail Accounts Belonging to More Than 100 People, Including Many Celebrities*, U.S. Department of Justice, https://www.justice.gov/usao-cdca/pr/pennsylvania-man-sentenced-today-18-months-federal-prison-hacking-apple-and-google-e?utm_source=chatgpt.com (2025. 5. 31.).
- Ateam Holdings (2023. 12. 20.), *お客様情報の外部流出の可能性に関するご報告とお詫び*, Ateam, https://www.a-tm.co.jp/news/44238/ (2025. 5. 31.).