Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.2, Apr. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.2.439

데이터센터 물리 보안 수준 향상을 위한 물리보안 위협 분할도(PS-TBS)개발 연구*

배 춘 석,† 고 승 철‡
수원대학교

On Physical Security Threat Breakdown Structure for Data Center Physical Security Level Up*

Chun-sock Bae,† Sung-cheol Goh‡
The University Of Suwon

요 약

ICBMA(IoT, Cloud, Big Data, Mobile, AI)로 대변되는 정보기술의 발전은 데이터의 급증과 이를 수용하기 위한 데이터센터의 수적, 양적 증가로 이어지고 있다. 이에 데이터센터를 사회 중요 기반시설로 인식하고, 테러 공격 대응 등 안전성 확보를 위해서는 사전에 물리보안 위협의 식별이 매우 중요하다. 본 논문에서는 위협의 식별과 분류를 쉽게 처리할 목적으로 물리보안 위협 분할도(PS-TBS)를 개발하고, 전문가 설문조사를 통하여 개발 된 물리보안 위협 분할도의 타당성과 효용성을 검증한다. 또한 위협 분할도의 항목에 대해 상세 정의를 통해 실무 활용을 통한 물리보안 수준 향상에 기여하고자 한다.

ABSTRACT

The development of information technology represented by ICBMA (IoT, Cloud, Big Data, Mobile, AI), is leading to a surge in data and a numerical and quantitative increase in data centers to accommodate it. As the data center is recognized as a social infrastructure, It is very important to identify physical security threats in advance in order to secure safety, such as responding to a terrorist attack. In this paper, we develop physical security threat breakdown structure (PS-TBS) for easy identification and classification of threats, and verify the feasibility and effectiveness of the PS-TBS through expert questionnaires. In addition, we intend to contribute to the improvement of physical security level by practical use in detailed definition on items of PS-TBS.

Keywords: Threat Breakdown Structure, Data Center Security, Physical Security

I. 서 론

1.1 연구의 배경 및 목적

ICBMA(IoT, Cloud, Big data, Mobile, AI)의 영향으로 전 세계적으로 뿐만 아니라 국내에서도 데이터센터의 규모 확대 및 개수가 급증 하고 있으며, 더불어 관련 안전성 확보도 더욱 중요해지고 있다.

2018년 11월 발생한 국내 대형 통신사의 화재는 인근 5개구의 인터넷, 휴대전화 통신을 마비시키고 인명피해까지 발생하는 초유의 사태를 불러왔고 복구

Received(12. 27. 2018), Modified(03. 11. 2019), Accepted(03. 12. 2019)
* 이 논문은 과학기술정보통신부의 재원으로 과학기술일자리진흥원의 청년TLO육성사업의 지원에 의해 작성되었습니다.
† 주저자, csbae01@suwon.ac.kr
‡ 교신저자, goh5703@suwon.ac.kr(Corresponding author)

에 장기간이 소요 될 것으로 알려지면서 데이터센터 분야에도 물리보안의 중요성과 경각심을 일깨우고 있다.

국내에서는 이미 집적정보통신시설보호지침 등을 통해 데이터센터 설비 및 운영요건 등을 제시하고 있지만 그것만으로 안전성 확보가 가능할 지에 대해서는 확신이 어려운 상황이다. 데이터센터의 안전을 저해하는 위협요소가 정의되어 있지 않아 어떤 위협들이 존재하고 있으며, 이에 대해 어떻게 대응해야 하는지를 쉽게 알 수 없기 때문이다.

본 논문에서는 이러한 문제점을 해결할 목적으로, 물리보안 위협들을 분류하고 이를 기반으로 데이터센터 물리보안 위협 분할도를 개발한다. 또한 전문가 설문조사를 통해 물리보안 위협분할도의 타당성과 효용성을 검증하고, 위협 분류 항목의 세부 내용을 상세하게 정의한다. 이로서 더욱 향상된 데이터센터 물리보안 위험평가와 물리적 보안 위협분석을 기반으로 한 안전한 데이터센터 설계 효과가 기대된다.

1.2 연구의 범위 및 방법, 선행 연구조사

본 연구의 범위는 데이터센터의 물리보안과 관련된 위협분류체계로 하였다. 접근방법으로 기존의 사례분석, 물리보안 위협 분류 체계 도출과 검증, 그리고 목표로 하는 물리보안 위협 분할도 제시 등 단계별 접근을 수행하고자 한다.

데이터 센터 물리보안과 관련된 선행연구는 아직 많지 않은 편이다. 강현선(2015)은 효율적이고 안전한 데이터센터의 물리적 보안방안에 관한 연구에서 데이터센터 입지조건, 데이터센터 물리적 통제방안, 보안 설비 및 접근 통제방안, 데이터센터 통합관제시스템 등에 대해 논의하였다[1].

김기욱 외(2012)는 재해정보를 고려한 클라우드 데이터센터 입지선정에 관한 연구에서 자연재해, 인적재해, 지형조건을 입지선정의 중요한 고려사항으로 논의하였다[2].

이문구 외(2013)는 지능형지속위협에 대한 차세대 융합보안 프레임워크에 관한 연구에서 데이터센터의 물리보안 체계에 대한 큰 그림을 포함하여 전체 융합보안체계를 논의하였다[3].

배춘석(2017)은 데이터센터 물리보안요건 표준화 방안에 대한 연구에서 통신, 설비, 전력, 공조·소화 부문으로 나누어 물리보안 요건 표준안을 논의하였다[4].

기타 정상진 외(2015), 송길헌 외(2009) 등 데이터센터 관련 여러 선행 연구들은 에너지 절감에 중점을 두었으며 따라서 물리보안에는 한계가 있었다고 하겠다[5,6,7].

이처럼 선행 연구들에서는 부족한 데이터센터 물리보안위협에 대한 연구는 매우 중요하고도 시급하다.

II. 현행 데이터센터 물리보안 위협 분류 분석

2.1 정보보안 위협 분류 일반 현황 및 시사점

먼저 일반적인 정보보안 관점에서 보면, 대표적인 정보보안 위협에 대한 분류를 제시한 사례는 미국 국가 기술 표준원의 NIST SP 800-12에서 제시한 9개의 분류이다[8]. 이중에서 4번째 항목만이 물리보안과 연관성이 높은 항목이다.

NIST SP800-30에서 좀 더 구체적으로 제시한 위협의 분류는 4가지로 구분된다[9].

정보보호 분야 국제 표준인 ISO/IEC27005 (Infosec Risk Management)에서는 위험관리 측면에서 식별, 분석, 평가, 대응에 이르는 일련의 절차를 제시하고 있다[10,11]. 위험 식별의 세부 규격으로 위협 식별이 포함되어 있지만 다이어그램에서 명시적으로 표현 안 된 점은 그 중요성에 비추어 볼 때 아쉬움이 있다.

위협을 잘 분류하고 정의한 위협 모델링 사례로,

Table 1. NIST SP800-12 Common Threat Types

No	Classification	Comments
1	Errors and Omissions	Management Security
2	Fraud and Theft	
3	Employee Sabotage	
4	Loss of Physical and Infrastructure Support	Physical Security
5	Malicious Hackers	Technical Security
6	Industrial Espionage	Management Security
7	Malicious Code	Technical Security
8	Foreign Government Espionage	Management Security
9	Threats to Personal Privacy	

Table 2. NIST SP800-30 Common Threat-sources

No	Classification	Details
1	Adversarial	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources events
2	Accidental	Erroneous actions taken by individuals in the course of executing their everyday responsibilities
3	Structural	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters
4	Environmental	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization

OWASP(Open Web Application Security Project) Top 10 보고서는 위협의 식별이 얼마나 정보보호에 중요한지를 보여준다.

웹 응용 영역에서 위협요인들에 대한 분석을 통해서 보안위험 Top 10을 도출하여 발표하고 있으며, 이를 통해서 해당 보안 위험들에 대해 효과적인 대응이 이루어지도록 전 세계적으로 기여하고 있다[12].

비록 웹 응용에 한정되어 정의되어 있지만 OWASP의 위협모델링이 주는 시사점은 소프트웨어 개발수명 주기 상에서 다음과 같은 기대효과를 줄 수 있다는 것이다[12].

- 위협의 문서화와 완화
- 안전한 설계 수립
- 보안과 개발간의 공감대 생성을 통한 협력
- 보안 요구를 시험하기 위한 보안 시험 케이스, 보안 시험 시나리오 식별
- 위협과 규제 요건의 식별 및 위험 평가
- 요구되는 통제 대책의 수립 및 도입
- 위험과 통제 대책, 사용성간의 균형
- 수용 가능한 위험에 기초한 불필요한 통제대책

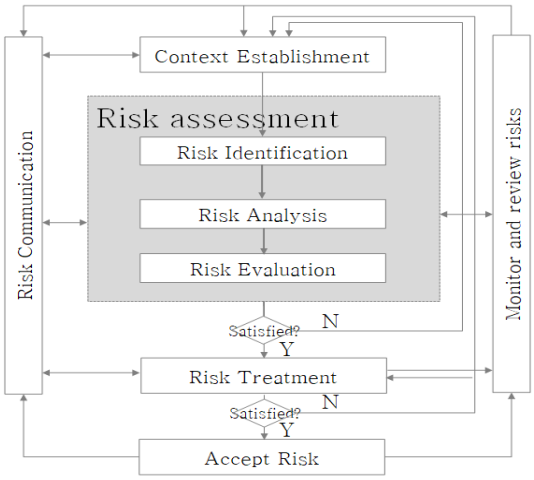

Fig. 1. ISO/IEC 27005 Infosec Risk Management Process Diagram

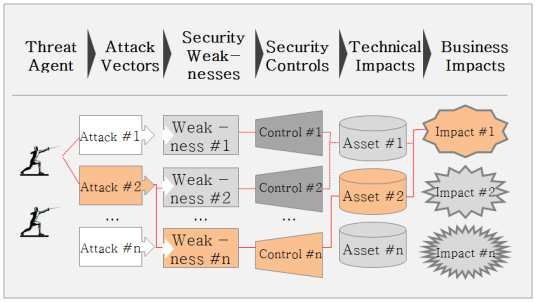

Fig. 2. OWASP Threat and Impact Model

식별

- 비즈니스 요구와 목표가 악의적인 행위자, 사고, 다른 영향 요소에 대응하여 적정하게 보호된다는 보장
- 자원에 대한 효과적인 투자

데이터센터 물리보안과 같은 영역에서도 위 기대효과들을 얻기 위해서는 위협에 대한 식별 및 분류가 매우 중요하다[13].

2.2 데이터센터 물리보안 위협 분류 현황 및 시사점

정보보호 일반에서 좀 더 영역을 좁혀 데이터센터 물리보안 위협 분류를 보면, 직접적인 분류체계를 확인하기가 어렵지만 민간 사업자들이 제품 마케팅 차원에서 발표한 내용들을 발견 할 수 있다.

데이터센터의 에너지관리 및 자동화 분야 글로벌

Table 3. Distributed Physical Threat

No	Classification	Description
1	Air temperature	Room, Rack, Equipment air temperature
2	Humidity	Room and rack related humidity at specific temperature
3	Liquid leaks	Water and coolant leaks
4	Human error and personal access	Unintentional abnormalities, unauthorized malicious data center intrusion
5	Smoke/Fire	Electrical or material fire
6	Hazardous airborne contaminants	Airborne chemicals(such as hydrogen from batteries) and particles(such as dust)

전문 기업인 슈나이더일렉트릭사는 백서를 통해 데이터센터와 관련된 분산된 물리위협으로 6가지를 제시하였다[14].

국내에서는 데이터센터 관련 안전 및 신뢰성 확보를 위해 전원중단, 수해사고, 화재사고, 시설보안사고 등 피해사례의 개선 차원에서 2002년도에 데이터센터 기반시설에 대한 물리적·기술적 보호조치 항목을 정의하였다[15].

이를 기반으로 '집적정보 통신시설 보호지침(과학기술정보통신부 고시)'이 수립되어 활용되고 있으나, 위협 측면의 접근보다는 피해에 대한 대응조치 관점에서만 정의되어 최근까지 이어진 데이터센터 물리보안 침해 사례에 비추어볼 때 실제적인 효과성 측면에서 한계가 있다[4, 16, 17, 18, 19, 20].

Table 4. Recent Data Center Incident Cases

Period	Institution	Content and impact
2010. 12	Citibank	Water flooding into computer room / Business stopping for 3 days
2011. 01	Macquarie Securities	Leakage from the broken air-conditioning system caused by cold wave /No business impact since it is after the close of the market
2012. 04	KaKaoTalk (LG CNS)	Power cut off the front panel/ Service Stop over 4 hours
2012. 05	KaKaoTalk (KINX)	Cut off communication line during sewage drilling construction / Service stopping over 1 hour
2012. 06	Port Authority (KLNet)	UPS and emergency generator inoperable in case of a momentary blackout caused by heavy rain / Service stop in major ports
2012. 07	CJ Group	Blackout / Service stop in major subsidiary's homepage
2013. 07	Korea Exchange	Blackout/Night-time transaction stop
2014. 04	Samsung SDS	Building Exterior Wall Fire / Service stop of Samsung Card and other customers
2014. 05	Nice Information Communication	Blackout / Payment operation stop over 2 hours
2015. 12	SK Broadband	UPS Failure / IPTV Service stop for 30 minutes
2017. 06	NHN Enter	Air conditioning system failure after damaged water pipes/ On-line shopping mall service stop for 16 hours
2018. 02	KT Kangnam center	Blackout / Many customers service stop for 6 hours

상기 언론에 보도된 물리보안 사고 외의 이슈발생은 훨씬 많은 상황이며 이를 개선하기 위해서는 대응조치만을 강조하는 방식에서 벗어나 원인에 해당하는 위협에 집중하여 이를 체계화 할 필요성이 매우 크다[21].

III. 목표 데이터센터 물리보안 위협 분류 도출 및 검증

3.1 데이터 센터 물리보안 위협 분류 접근 방식 정의

3.1.1 기존의 위협 분류 방식의 주요 이슈

기존의 위협 분류들을 보면 정보보안 전체를 포괄하여 구체성이 미흡하거나, 물리보안 관련된 제품이나 서비스를 판매하기 위한 특정업체의 의도 반영, 위험 모델링과의 비일관성, 새로 나타난 위협 유형을 미포함 하는 문제점이 있다.

Table 5. As-Is Threat Category Definition Issues

Issues	Description	Related
Too comprehensive	Information protection defined from a wide perspective, data center physical security details are not specific	NIST
Too narrow	Applicable only from the perspective of the respective product company for the purpose of promoting or selling the product/service	Schneider Electric
Inconsi-stent to risk modeling	Threats should be risk-assessmentable in conjunction with assets, protection value, and vulnerability in the data center, but cannot be mapped to relevance	All
Do not accept change	The emergence of new technologies and new threats as the environment changes are not reflected	All

3.1.2 개선된 새로운 위협 분류 접근 방식 정의

위에서 제기한 주요 이슈들을 좀 더 개선한 위협 분류는 범위 적합성, 객관성, 모형 일관성, 변화적응성을 축으로 아래와 같이 접근하였다.

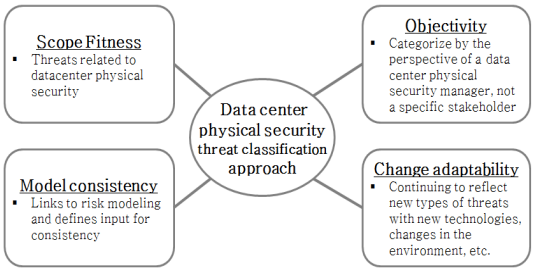

Fig. 3. Threat Categorization Approach

3.2 데이터센터 물리보안 위협 분류(안) 및 검증 결과

3.2.1 데이터센터 물리보안 위협 분류(안)

데이터센터 물리보안 위협과 관련한 참조 문헌들, 기존 연구 논문들, 실무 경험상의 지식 등을 기초로 새로운 위협분류 접근방식을 적용하여 아래와 같이 데이터센터 물리보안 위협 분할도(이하 "PS-TBS", Physical Security - Threat Breakdown Structure) 초안을 도출하였다.

물리보안 책임자의 관점으로 필요하다고 판단되는 위협요소를 모두 포괄 하고, 최신의 위협을 고려한 Trend 범주를 추가하고, 실제 침해의 직접 목표가 되는 자산범주를 포함하여 위험평가와의 일관성을 향상하도록 하였다. 도출된 결과는 위치, 통제가능성, 출처, 구성요소, 형태, 최신성의 6가지를 기초로 21개의 위협분류 항목을 정의하였다.

Table 6. Physical Security Threat Breakdown Structure Draft

Category(6)	Classification Item(21)
Location(2)	Internal, External
Controllability(2)	Controllable, Uncontrollable
Source(3)	Nature, Environment, Human
Asset(4)	Communication, Power, Location·Building, Air Conditioning·Fire Prevention
Attack Type(8)	Explosion, Collision, Damage, Combustion, Flooding, Vibration, Disturbance, Etc.
Trend(2)	Old, New

3.2.2 데이터센터 PS-TBS 검증결과

검증 방법은 다음과 같이 진행 하였다.

- 조사대상: 데이터센터 관련 업무 담당자 200여 명(실제 응답자 106명)
- 조사기간: 2018년 11월 25일 ~ 12월 10일(16일간)
- 조사방법: 설문조사 툴(구글 폼)사용
- 조사항목: 참여자 기본사항, 데이터센터 물리보안 위협과 위험의 인식 수준, PS-TBS 항목 적합성 정도, 활용 시 예상 기대 효과 조사

전문가들의 응답결과를 분석한 결과 PS-TBS 수립 필요성에 대한 확인, 항목들의 적정성 여부 판단, 활용 시 예상 기대효과가 높은 것으로 나타났다.

설문참여자들의 주요 업무는 데이터센터분야 82명 및 정보보호분야 58명(복수 응답) 등으로 데이터센터 물리보안 설문 목적에 부합하도록 구성되었다.

관련 업무 수행 경력은 7년 이상 66명으로 응답의 신뢰도 측면에서 충분하다고 판단하였다.

물리보안 위협과 위험에 대한 인식 조사결과 물리보안 위협요인 식별과 대응을 위해 데이터센터 PS-TBS의 필요성에 대해 높음 이상의 응답이

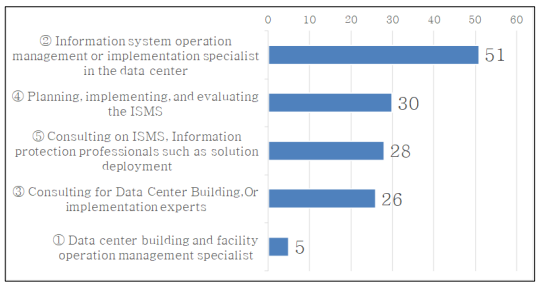

Fig. 4. Respondent Number on Role (Multiple selection allowed)

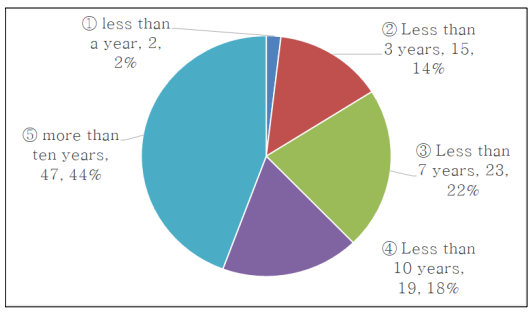

Fig. 5. Respondent Ratio of Experience

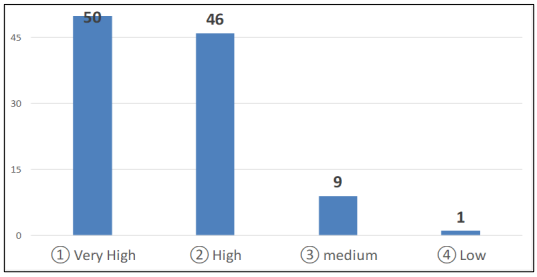

Fig. 6. Ratio of Respondent of Needs on Data Center PS-TBS

96(91%)명으로 본 연구의 필요성을 확인 하였다.

데이터센터 PS-TBS 항목에 대한 검증결과 적합 이상 응답한 수는 항목별 평균 74.2명(71%)로 나타났다. 적합 이상 응답비율이 51% 이상인 경우를 채택한 결과는 아래와 같으며 6개 범주 21개 항목이 모두 포함되었다.

Table 7. Research Result on Threat Item Classification of Data Center PS-TBS Draft

No	Category & Classification Item(27)	responses above Suitable(%)	Adoption status
1	Location	76(72%)	O(Yes)
1-1	Location-Internal	81(76%)	O(Yes)
1-2	Location-External	74(70%)	O(Yes)
2	Controllability	79(75%)	O(Yes)
2-1	Controllability-Controllable	71(67%)	O(Yes)
2-2	Controllability-Uncontrollable	73(69%)	O(Yes)
3	Source	72(68%)	O(Yes)
3-1	Source-Nature	70(66%)	O(Yes)
3-2	Source-Environment	71(67%)	O(Yes)
3-3	Source-Human	73(69%)	O(Yes)
4	Asset	80(75%)	O(Yes)
4-1	Asset-Communication	76(72%)	O(Yes)
4-2	Asset-Power	79(75%)	O(Yes)
4-3	Asset-Location·Building	75(71%)	O(Yes)
4-4	Asset-Air Conditioning·Fire Prevention	79(75%)	O(Yes)
5	Attack Type	78(74%)	O(Yes)
5-1	Attack Type-Explosion	72(68%)	O(Yes)
5-2	Attack Type-Collision	74(70%)	O(Yes)

No	Category & Classification Item(27)	responses above Suitable(%)	Adoption status
5-3	Attack Type-Damage	68(64%)	O(Yes)
5-4	Attack Type-Combustion	73(69%)	O(Yes)
5-5	Attack Type-Flooding	77(73%)	O(Yes)
5-6	Attack Type-Vibration	75(71%)	O(Yes)
5-7	Attack Type-Disturbance	71(67%)	O(Yes)
5-8	Attack Type-Etc	68(64%)	O(Yes)
6	Trend	72(68%)	O(Yes)
6-1	Trend-Old	72(68%)	O(Yes)
6-2	Trend-New	75(71%)	O(Yes)

활용 시 예상되는 기대효과 항목에 대해서는 위협 식별 ~ 보호대책 운영 및 개선의 5단계 14항목에 대해서 각 높음 이상 응답 수 평균 83명(78%)으로 데이터센터 PS-TBS에 대한 높은 활용 효과를 기대할 수 있는 것으로 나타났다.

Table 8. Research Result on Expected Benefit of Data Center PS-TBS Draft

#	Phase	Activity	responses above High(%)
1	Identifying and analyzing threats	Identification of existing physical security threats	85(80%)
2		Identification of new physical security threats	77(73%)
3		Analysis of Physical Threats	87(85%)
4		Possible types of physical security attacks identification	85(80%)
5	Risk analysis	Affected data center assets identification	78(74%)
6		Exploitation of data center assets	80(75%)
7		Vulnerability analysis of data center assets	82(77%)
8	Risk assessment	Estimating the risk level of physical security in data center	84(79%)
9		Estimating the effects of physical security risks	85(80%)
10	Protection Measures	Derivation of data center physical protection requirements	85(80%)
11		Establishing protection measures against data center physical security threats	86(81%)
12	Operation and improvement of protective measures	Evaluation of existing physical protection measures	81(76%)
13		Improving existing physical protection measures	84(79%)
14		Monitoring and continuous improvement across the physical protection system	83(78%)

IV. 목표 물리보안 위협 분류 분석결과

4.1 제시하는 데이터센터 물리보안 위협 분류

전문가 설문결과를 바탕으로 확정된 데이터센터 PS-TBS는 아래와 같다.

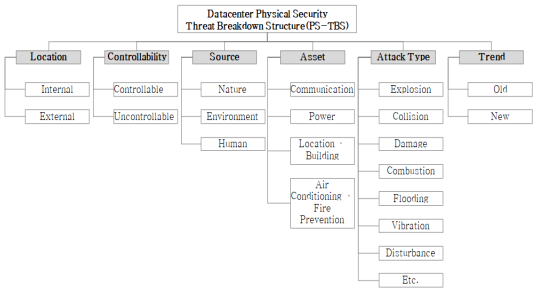

Fig. 7. Data Center Physical Security Threat Breakdown Structure Proposed

4.2 데이터센터 물리보안 위협 분류 세부 내용

제시된 데이터센터 PS-TBS를 세부적으로 정의하였으며 이를 통해 좀 더 상세하게 데이터센터 관련

위협들을 식별 및 분석할 수 있도록 하였다.

Table 9. Description on Threat Item Classification of Data Center PS-TBS Proposed

No	Classification Item	Description
1	Location	Where threats occur
1-1	Location-Internal	Internal data center
1-2	Location-External	Out of data center
2	Controllability	whether there is the possibility of proactive control over the threat occurrence itself or when the threat occurred
2-1	Controllability-Controllable	Controllable(ex. intrusion, theft, vandalism, equipment breakdown, operational error, etc.)
2-2	Controllability-Uncontrollable	Uncontrollable(ex. Most natural disasters, such as wars, riots, political unrest, attacks by international terrorist organizations, etc.)
3	Source	the original starting point from which the threat originated
3-1	Source-Nature	Start with natural elements
3-2	Source-Environment	Start with environmental elements (ex. Chemical contamination of air in computer room)
3-3	Source-Human	Start with a person's action or omission
4	Asset	Critical components to be protected from the data center's own perspective (the assets protected by the information system are technical security targets)
4-1	Asset-Communication	Telecommunications-related facilities, equipment, and environment that connect the data center to the outside (ex. line operators, telecommunications ports, circuit station reception rooms, backbone equipment, telecommunication cables, etc.)
4-2	Asset-Power	Facilities, equipment, and environment for supplying power to the data center (ex. power service operators, power supply routes, power acquisition facilities, power cable, battery room, UPS, emergency generator, etc.)
4-3	Asset-Location·Building	Data center location, building information (ex. wall configuration, parking, building security system, access control and monitoring, server room doors, windows, offices, cargo pickup, etc.)
4-4	Asset-Air Conditioning·Fire Prevention	Building temperature-related air conditioning, water supply and drainage facilities, fuel storage tanks, fire and water leak detection and control facilities, etc.
5	Attack Type	A series of well-organized actions utilizing one or more security vulnerabilities that result in a physical security breach
5-1	Attack Type-Explosion	Explosion, gunpowder, gas explosion, dust explosion, etc. resulting in a series of fires.
5-2	Attack Type-Collision	Strong interaction due to relatively close contact with moving objects or particles (ex. car crashes, aircraft crashes, firing or dumping objects on the data center building, etc.)
5-3	Attack Type-Damage	Cause the target object to break or malfunction (ex. Breaks CCTVs for data center monitoring, damage to access control devices or equipment, damage to boundaries such as fences, etc.)
5-4	Attack	Make the target object burn

No	Classification Item	Description
	Type-Combustion	with light and heat (ex. Fire in the data center building, misfire, etc.)
5-5	Attack Type-Flooding	Parts of the data center or target equipment are submerged or drained (ex. floodwater of the data center, building leak, etc.)
5-6	Attack Type-Vibration	Repeatedly altering the position, orientation, and shape of the target object over time (ex. Vibration of data center buildings due to earthquake, equipment vibration inside computer room while moving)
5-7	Attack Type-Disturbance	Electromagnetic waves, strong noise, etc. to prevent normal operation and activities (ex. electronic attacks, EMP attacks, etc.)
5-8	Attack Type-Etc	Incoming and discharging animals such as rats and snakes, postal delivery of toxic substances, etc.
6	Trend	Threats based on technology advancements, new ideas
6-1	Trend-Old	Already Known Threats in the Market
6-2	Trend-New	New Technology and Idea-Based Threats (ex. drone, self-driving car, IoT-based device attack, etc.)

V. 결 론

데이터센터 수명주기 관점에서 각 단계별로 아래와 같이 PS-TBS를 활용한 효과적인 물리보안 활동 수행이 가능하다.

- 데이터센터 기획 단계: 위치, 유형 결정 시 참고
- 데이터센터 개념설계 단계: 설계 요건으로 명시할 물리보안 위협요인의 식별 및 선택
- 데이터센터 기본/실시 설계 단계: 물리보안 요건 반영, 시설 설계 안전성 국제인증(Uptime Tier - Design) 획득
- 데이터센터 시공 단계: 안전 설계 내용대로 시공, 시설 운영 안전성 국제인증(Uptime Tier - Facility) 획득
- 데이터센터 운영/유지보수 단계: 상시 위협 모니터링 및 신규 위협 식별에 참고

데이터센터 PS-TBS는 물리보안 측면에서 아래와 같이 안전성 향상에 기여할 수 있다.

- 더욱 향상된 데이터센터 물리보안 위험평가
- 물리적 보안 위협 기반의 데이터센터 안전 설계
- 위협 모델링을 통한 물리보안 투자의 효과 향상
- 필요한 물리보안 대응책 수립 및 도입 의사결정
- 위협 기반으로 불필요한 통제대책 식별 가능
- 데이터센터 물리보안 위협의 문서화 및 공유
- 데이터센터 안전성에 대한 비즈니스 측면의 향상된 신뢰 제공 가능

References

[1] Hyun-sun Kang, "An efficient and secure physical security method of data center," Journal of Security Engineering, 12(6), pp. 609-620, Dec. 2015

[2] Ki-uk Kim and Chang-soo Kim, "A study on the construction and site selection of the cloud data center considering disaster information," Journal of Communications and Networks, 16(12), pp. 2575-2580, Jun. 2012

[3] Moon-goo Lee and Chun-sock Bae, "Next generation convergence security framework for advanced persistent threat," Journal of The Institute of Electronics Engineers of Korea, 50(9), pp. 2336-2343, Sep.2013

[4] Chun-sock Bae, "A study on data center physical security requirements standardization," M.E. Thesis, Konkuk university Graduate School of Information and telecommunications, Feb. 2017

[5] Sang-jin Jung and Jun-hwa Song,

"The trend of standardization on energy efficient and safe data center," TTA Journal, 158, pp.87-93, Mar. 2015

〔6〕 Jin-kyun Cho and Byung-seon Kim, "The cooling and air distribution systems for the optimal IT environment control in the (internet) data center," Architectural Institute of Korea, 24(2), pp. 313-320, Feb. 2008

〔7〕 Gil-heon Song and Taek-soo shin, "A study on the introduction of green IT based on the cases of implementing green internet data center," Information Systems Review, 11(2), pp. 147-167, Aug. 2009

〔8〕 Barbra Guttman and Edward Roback, "An introduction to computer security: the NIST handbook," NIST SP 800-12, Oct. 1995

〔9〕 Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk management guide for information technology systems," NIST SP 800-30, Jul. 2002

〔10〕 Everett Cath, "A risky business: ISO 31000 and 27005 unwrapped," Computer Fraud & Security, vol. 2011, no. 2, pp. 5~7, 2011

〔11〕 Adil Sayouti, Siham Benhadou, Hicham Medromi and Mohamed Ghazouani, "An integrated use of ISO27005, mehari and multi-agents system in order to design a comprehensive information security risk management tool," International journal of applied information systems, vol. 7, no. 2, pp. 10-15, 2014

〔12〕 OWASP Foundation, "OWASP top 10 - 2017 most critical web application security risks," OWASP Foundation, https://owasp.org, Jun. 2018

〔13〕 Elena Ramona Stroie and Alina Cristina Rusu, "Security risk management - approaches and methodology," Informatica Economica, vol. 15, no. 1, pp. 228-240, 2011

〔14〕 Christian Cowan and Chris Gaskins, Monitoring physical threats in the data center, Schneider Electric - Data Center Science Center, Dec. 2006

〔15〕 KISA, IDC safety・reliability appraisal item research, Technology support sponsorship project 02-01 result Report, Dec. 2002

〔16〕 "KaKao Talk service stop, because of IDC cable line cut down incident", Money Today News, May 25, 2012

〔17〕 "Failure experienced by 6 of 10 among data center operators in recent 1 year", ZDNet Korea News, Apr. 4, 2016

〔18〕 "SKbroadband, BTV service stopped by data center service failure", Newspim, Dec. 16, 2015

〔19〕 "NHN Entertainment, IT new business went down, because of data center service failure", Digital Times, Jun. 20, 2017

〔20〕 "KT, Connection to game and other service stopped by data center service failure", YTN News, Feb, 2, 2018

〔21〕 Do-young, Park, Server room and data center operation status research and improvement proposal in south korea, IDC Korea, Jun. 2016

〈저 자 소 개〉

배 춘 석 (Chun-sock Bae) 정회원
1993년 2월: 전남대학교 경영학과 학사
2017년 2월: 건국대학교 정보보안학과 석사
2018년 3월~현재: 수원대학교 컴퓨터학과 박사과정,
1993년 4월~현재: ㈜LG CNS 클라우드아키텍처팀 재직, 정보관리기술사(2008)
〈관심분야〉 정보보호, 데이터센터 구축 및 운영, 클라우드컴퓨팅

고 승 철 (Sung-cheol Goh) 종신회원
1981년 2월: 연세대학교 수학과 학사
1983년 2월: 연세대학교 수학과 석사
1992년 8월: 포항공과대학교 수학과 박사
2011년 9월~현재: 수원대학교 정보보호학과 교수
〈관심분야〉 정보보호, 국방사이버보안, 암호학, 클라우드컴퓨팅