ISSN: 2586-6036
JWMAP website: http://accesson.kr/jwmap
doi: http://dx.doi.org/10.13106/jwmap.2026.vol9.no1.105

Strengthening Data Center Resilience via Technical, Operational, and Institutional Policy Incentives*

Young-Ju LEE[1], Won-Mo GAL[2]

1. First Author Student, Department of Medical IT, Eulji University, Korea,
Email: damyan@g.eulji.ac.kr
2. Corresponding Author Professor, Department of Environmental Health & Safety, Eulji University, Korea,
Email: wongal@eulji.ac.kr

Received: February 05, 2026. Revised: February 24, 2026. Accepted: February 28, 2026.

Abstract

This study analyzes the structural vulnerabilities of South Korea's data center disaster response systems following repeated large-scale fires at the SK C&C Pangyo center and the Daejeon National Computing and Information Agency. The primary purpose is to propose multi-faceted improvement strategies across technical, operational, and institutional dimensions to ensure the continuity of essential national services. Utilizing a comparative case analysis methodology, the research identifies centralized infrastructure and formalistic disaster recovery operations as primary failure factors. The principal results advocate for technical advancements, including an Active-Active based continuous service framework and Battery Monitoring System (BMS) cycles shortened to under 10 seconds to enhance physical safety. Operationally, it suggests mandating automated failover response systems and regular real-world simulation drills assuming worst-case scenarios like total center destruction. Institutionally, the study proposes mandating remote backups through Service Level Agreement (SLA) standards and introduces a market-oriented policy incentive system that grants preferential points for government-led projects to encourage voluntary investment. These measures aim to shift disaster recovery from a mere regulatory compliance cost into a strategic investment that strengthens organizational digital competitiveness. Ultimately, establishing administrative compensation frameworks and prioritizing budget allocation for tiered disaster recovery implementation will secure national digital resilience and create a sustainable, proactive crisis management framework.

Keywords : Data Center, Disaster Recovery (DR), Resilience, Active-Active System, Policy Incentives

JEL Classification Code: L86, H54, O38

1. Introduction

As modern society transitions into a knowledge and information-based era, data has established itself as a primary resource for creating value in social development. The explosive increase in data has heightened the need for stable storage and processing. Combined with the adoption of cloud computing, this has led to the emergence of Data Centers (DCs) as core infrastructure. As they

ensure the continuity of nationwide services like administration and finance, their stable operation is now an essential element of social infrastructure. Despite this significance, the 2022 Pangyo Data Center fire and the fire at the National Computing and Information Agency (NCIA) in 2025—occurring just three years later—clearly exposed the formalistic limitations and the lack of practical resilience in South Korea's Disaster Recovery (DR) systems. Particularly in the public sector, most systems lack established DR frameworks, posing a persistent risk of paralyzing core national functions.

Consequently, this study aims to conduct a multi-faceted analysis of the causes behind recurring large-scale disasters from technical, operational, and institutional perspectives. In particular, it proposes a differential implementation strategy based on system importance tiers to overcome the realistic constraints of immense construction costs. Furthermore, it suggests effective measures to strengthen resilience by shifting away from regulation-heavy policies and introducing policy incentives, such as granting preferential points for participation in government-led projects. The ultimate objective of this research is to move beyond simply minimizing service interruptions during disasters and to establish a virtuous cycle of crisis management framework that induces voluntary investment.

2. Case Analysis

2.1. Case Analysis of Domestic Data Center Fires

2.1.1. 2022 SK C&C Pangyo Data Center Fire

On October 15, 2022, a fire broke out at the SK C&C Pangyo Data Center in Seongnam, Gyeonggi-do, leading to the temporary suspension of various services hosted at the facility. In the case of Kakao Corp., major services were paralyzed, and it took approximately 127 hours for all services to be fully restored. This service interruption transcended a mere corporate failure, causing significant social repercussions on a national disaster level, with 105,116 damage claims reported.

2.1.2. Limitations of the Disaster Recovery System at the Time

Although Kakao had distributed its data across three or more data centers, recovery still exceeded five days. According to a press release by the Ministry of Science and ICT, many of Kakao's core functions were concentrated in the Pangyo center, causing widespread impact. First, while data was redundant, system operation functions were not, and redundancy for major infrastructure was limited to within the Pangyo center. Furthermore, operation and management tools essential for disaster response lacked sufficient redundancy across centers. The absence of properly established automation and monitoring systems meant that automatic failover to other data centers was difficult, leading to delays as manual measures had to be taken during the actual accident.

2.1.3. 2025 Daejeon National Computing and Information Agency (NCIA) Fire

On September 26, 2025, a fire occurred at the NCIA in Daejeon. This incident paralyzed 709 government administrative network systems, including 96 government electronic services such as Government24, the e-People portal, mobile IDs, and postal services. The government declared a "Serious" crisis alert level. As of November 11, 36 days after the incident, the recovery rate stood at 92%.

2.1.4. Limitations of the Disaster Recovery System at the Time

This case clearly highlighted the limitations of the disaster recovery systems for government administrative information systems. According to the Board of Audit and Inspection, as of 2022, 1,428 business systems from 51 agencies were located at the Daejeon headquarters, but 92.6% of these systems lacked a disaster recovery (DR) system. Consequently, the capacity to recover was extremely limited in the event of total data loss at the Daejeon facility.

2.2. Implications through Comparison of Domestic Cases

An examination of domestic cases reveals that insufficient data center dualization caused serious setbacks in data and system recovery. Both the 2022 SK C&C Pangyo fire and the 2025 NCIA fire resulted in long-term service interruptions due to the lack of redundancy and the limitations of current disaster recovery frameworks. Despite previous government claims of a system capable of recovery within three hours using real-time backups, long-term service outages repeated in 2025. As seen in the Kakao incident, concentrating services in a single region without sufficient DR systems prevents rapid service resumption through other data centers. These cases demonstrate that service continuity and disaster recovery frameworks are not merely technical choices but essential tasks for maintaining national continuity and social trust.

3. Problems in Domestic Data Center Disaster Response

The 2022 SK C&C Pangyo data center fire and the 2025 National Computing and Information Agency (NCIA) Daejeon center fire clearly revealed structural vulnerabilities in South Korea's data center disaster response systems. These incidents were not merely limited to technical flaws or operational errors but demonstrated that institutional deficiencies could lead to recurring disasters. Consequently, there is an urgent need to strengthen practical resilience to minimize service interruptions and enable rapid recovery. This recognition highlights the necessity for both domestic corporations and government agencies to fundamentally re-examine and actively improve their disaster recovery systems.

3.1. Technical Problems

The fundamental cause in domestic data centers is a structural problem where core infrastructure and systems essential for service continuity are excessively concentrated in a single data center.

3.1.1. Centralized Structure and Incomplete Redundancy Design

Both SK C&C and the NCIA showed limitations in recovering services quickly using resources from other regions because their core systems were concentrated in specific physical spaces. The SK C&C case is a representative failure where system redundancy was misunderstood as being achieved through data backup alone. Due to the lack of a geographically dispersed redundancy system, protection from physical disasters was insufficient, and the Single Point of Failure (SPOF) problem, which paralyzes the entire center, remained unresolved.

3.1.2. Vulnerability of Data Backup Systems

These cases confirmed structural vulnerabilities where backup data was lost simultaneously with the original data. During the NCIA fire, a worst-case scenario occurred where both original and backup data were lost at once as servers and Uninterruptible Power Supplies (UPS) were damaged simultaneously. This illustrates the essential risk that if physical and geographical separation is not properly implemented, the purpose of backup data itself can vanish.

3.1.3. Early-Stage Operation of Redundancy Systems

Although the NCIA operated disaster recovery centers in Gwangju and Daegu, the implementation of a multi-regional simultaneous operation system between the main and DR centers was at an early stage. As a result, the DR centers could not quickly replace the functions of the main center and were limited to merely storing data.

3.2. Operational Problems

Even with robust infrastructure, disaster response is bound to fail if the capacity to operate it effectively is lacking.

3.2.1. Absence of Automated Disaster Response Systems

There was a critical lack of systems to automatically switch services to data centers in other regions during a disaster. In the SK C&C case, even the automatic failover system was installed only in the Pangyo center where the fire occurred, which was a fatal design error subordinating the DR automation system to a single point of failure.

3.2.2. Insufficient Redundancy of Core Operation and Management Tools

Essential operational management and collaboration tools for rapid response were also concentrated in the single center affected by the disaster. This revealed a lack of resilience in the recovery process itself, as even the 'control tower' responsible for directing recovery was directly impacted.

3.2.3. Limited Functionality of Disaster Recovery Systems

The NCIA's DR system was designed to perform only minimal functions like storage or data backup during normal times, showing clear limits in providing continuous service during total system failures. This is a chronic operational issue where DR systems remain formalistic plans for regulatory compliance rather than practical capabilities for service continuity.

3.3. Institutional Problems

3.3.1. Legal Blind Spots in Digital Disaster Management

Past regulations were centered on telecommunications business operators, meaning value-added service providers like Kakao and data centers were effectively excluded from legal disaster management obligations. This legal vacuum was belatedly addressed through the 2023 amendment of the "Three Digital Safety Acts" after the Pangyo fire caused national confusion.

3.3.2. Formalistic Construction and Operation of Disaster Recovery Systems (DRS)

Even the public sector, which requires the highest level of stability, neglected its disaster preparedness duties. As of the end of 2022, 92.6% of all business systems managed by the NCIA did not have a DRS, exposing core national information systems to serious risks of service interruption.

3.3.3. Limitations in Recovery Levels and Oversight

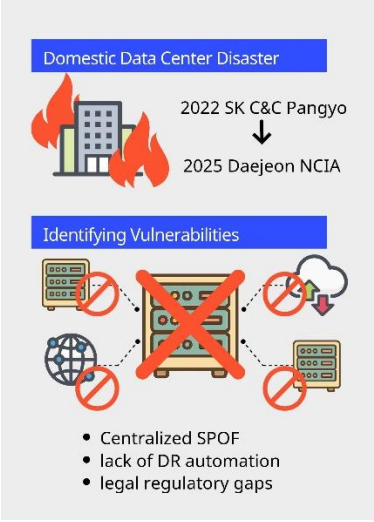
Even where DRS was established, most remained at the 'Warm Site' or 'Cold Site' level, requiring significant time for recovery, rather than the 'Hot Site' level for immediate resumption. Furthermore, Cloud Security Assurance Program (CSAP) certifications often ended up as mere "paper certifications," as they failed to properly inspect the actual redundancy of core equipment between main and DR centers.

3.3.4. Inefficiency in Administrative and Budgetary Management Systems

Provisions mandating data backup to remote locations, such as DR centers, were not included in the SLA (Service Level Agreement) standards for public sector cloud conversion projects. Consequently, 86.8% of agencies involved in the 2021 cloud conversion projects neglected serious risks by backing up data only within the main center.

3.3.5. Limitations of Reactive Policy Improvements

South Korea's digital disaster response system faces multi-layered institutional problems: legal blind spots, formalistic DRS operation, and administrative/budgetary inefficiencies. The biggest issue is that institutional improvements remain reactive "post-hoc" measures (closing the stable door after the horse has bolted) that only occur after experiencing large-scale disasters.



Note: NCIA: National Computing and Information Agency, SPOF: Single point of failure

Figure 1: Analysis of Major Fire Incidents

4. Improvement Measures for Domestic Data Centers

To overcome the structural vulnerabilities of domestic data centers and ensure the continuity of national services, organic improvements across technical, operational, and institutional dimensions are required. It is essential to establish effective design plans to prevent recurring disasters and provide the necessary policy support to implement them.

4.1. Technical Aspect: Advancing Physical Safety and Resilience

Designing to protect infrastructure from physical disasters and increase system resilience must take precedence.

4.1.1. Ensuring Physical Safety and Power Continuity

To prevent lithium-ion battery fires, the measurement cycle of the Battery Monitoring System (BMS) should be shortened to 10 seconds or less, and the installation of other electrical equipment within battery rooms should be prohibited to block fire spread paths. Additionally, a power bypass system capable of remote power control or bypass supply during disasters should be established to minimize service interruptions caused by power outages.

4.1.2. Active-Active Based Continuous Service Framework

The "Single Point of Failure" (SPOF) problem, where an entire service stops if a specific center is paralyzed, must be fundamentally resolved. To achieve this, an Active-Active system—where multiple regions operate simultaneously—should be built for core applications and management tools, ensuring immediate service continuity without additional transition time during a disaster.

4.2. Operational Aspect: Strengthening Control Automation and Practical Verification Systems

Advanced operational management processes must support technical infrastructure to ensure it functions in real-world scenarios.

4.2.1. Disability Response Automation and Monitoring

Automation elements, such as Global Server Load Balancing (GSLB), should be applied to enable immediate service switching upon failure. Furthermore, professional monitoring solutions like APM (Application Performance Management) and DPM (Database Performance Management) should be introduced to constant monitor for signs of failure.

4.2.2. Practical Simulation Drills for Worst-Case Scenarios

Redundancy tests must be mandated before system launch to verify the practical suitability of the designed recovery framework. Regular simulation drills assuming worst-case scenarios, such as the destruction of a data center, should be conducted to master response capabilities within the Recovery Time Objective (RTO) and enhance the effectiveness of manuals.

4.3. Institutional Aspect: Eliminating Legal Blind Spots and Substantiating Management Supervision

Institutional improvements are needed to strengthen legal responsibility for digital disaster management and abolish formalistic operations.

4.3.1. Expanding Disaster Management Obligations and Strengthening Certification

Disaster management obligations based on the "Three Digital Safety Acts" must be strictly applied to large-scale data centers and value-added telecommunications service providers. Additionally, Cloud Security Assurance Program (CSAP) evaluations should shift from document-centered certification to on-site inspections to verify the actual redundancy of core equipment between the main and DR centers.

4.3.2. Revising SLA Standards

Standard Service Level Agreements (SLA) for public sector cloud conversion must include mandatory provisions for remote backup and recovery systems to improve the current risky structure concentrated on backups within a single center.

4.4. Policy Incentives: Introducing Incentive Systems for Voluntary Participation

To ensure the effectiveness of the digital disaster response system, policy reward mechanisms must be established to induce proactive investment from both private and public sectors.

4.4.1. Market-Oriented Incentives for the Private Sector

Visible benefits should be provided to providers who voluntarily build Active-Active systems exceeding legal requirements or demonstrate excellent performance in government-led drills. A key proposal is to grant preferential points in technical evaluations when selecting contractors for government informatics or nationwide cloud conversion projects based on their level of DR advancement. This will encourage companies to view DR systems as a means of securing competitiveness through contribution to national infrastructure rather than a mere expense.

4.4.2. Administrative Incentives to Promote Public Sector DR Implementation

Incentives are needed to lower administrative and budgetary barriers for government agencies, given that 92.6% currently lack DR systems.

• Budget and Evaluation Linkage: Priority budget allocation should be given to projects including DR centers or Active-Active implementation, and "Digital Service Continuity Rate" should be reflected as a performance indicator in government agency evaluations.

• Strategic Tiered Approach: Since building Active-Active systems for all systems is cost-inefficient, they should be applied preferentially to Tier 1 and 2 core services based on system impact.

• Public Cloud Certification Benefits: Agencies moving to private clouds that establish remote backup systems should receive benefits such as simplified CSAP procedures or extended certification validity to ease administrative burdens.

These multi-faceted incentive systems will help break the practice of "minimum compliance" and serve as a driving force to quickly secure national digital resilience and a sustainable crisis management framework.

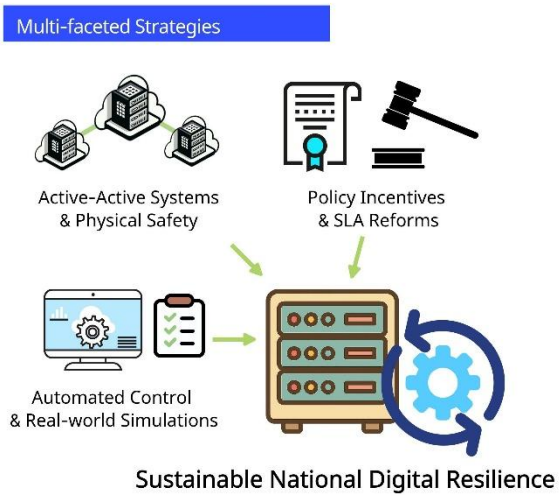


Figure 2: Multi-faceted Improvement Strategies

5. Conclusions

This study has emphasized that the stable operation of Data Centers (DCs), which have become core infrastructure in a knowledge and information-based

society, is an essential element for maintaining national functions and building social trust. Despite this importance, an in-depth analysis of the root causes of recurring large-scale disasters—such as the 2022 SK C&C Pangyo fire and the 2025 NCIA fire—revealed structural vulnerabilities, specifically the formalistic operation and lack of practical effectiveness in current Disaster Recovery (DR) systems.

The core conclusions derived from this research for strengthening data center resilience are as follows:

• Technical Advancement: To resolve the "Single Point of Failure" problem, recovery levels must be upgraded to an Active-Active based continuous service framework. Additionally, to prevent lithium-ion battery fires, BMS measurement cycles should be shortened to 10 seconds or less, and physical safety facilities must be strengthened to ensure infrastructure survival.

• Strengthening Operational Verification: Along with introducing specialized solutions for automated control, real-world simulation drills assuming worst-case scenarios, such as the total destruction of a data center, should be mandated to master practical response capabilities.

• Institutional Foundation and Eliminating Blind Spots: The scope of the "Three Digital Safety Acts" should be expanded to strengthen the responsibility of large-scale operators. Furthermore, remote backup provisions must be mandated as a legal obligation by including them in standard SLA (Service Level Agreement) templates for public cloud transitions.

• Introduction of Policy Incentives: Shifting away from regulation-heavy responses, a policy reward mechanism is needed, such as granting preferential points for government-led projects to private operators who voluntarily build Active-Active systems or demonstrate excellent drill performance. To improve the low DR adoption rate (92.6%) in the public sector, priority budget allocation and administrative incentives must be implemented in parallel.

This research is significant in that it structurally analyzed failure causes across technology, operation, and systems and provided basic data for future policy formulation by proposing practical policy incentives like the "preferential point system". However, the fact that Korea's digital disaster response remains a reactive "post-hoc" approach is a challenge that must be overcome in the future.

Future research should focus on assessing the empirical effects of the incentive systems and Active-Active frameworks proposed in this study. To transform expensive DR infrastructure from idle resources into active assets, further analysis is needed on technical feasibility and guidelines for utilizing these resources in normal times for AI model training, large-scale data analysis, or high-load test environments (Sandboxes). Such research on the "multi-faceted utilization of DR resources" will provide a practical basis for elevating the national crisis management framework by framing DR implementation as an investment that strengthens organizational digital competitiveness rather than a mere cost of regulatory compliance.

Acknowledgements

This research was supported by the Regional Innovation System & Education(RISE) program through the Gyeonggi RISE Center, funded by the Ministry of Education(MOE) and the Gyeonggi-do, Republic of Korea.(2025-RISE-09-A28)

References

Board of Audit and Inspection (BAI). (2025a, October 20). *Intelligent informatization project, Ministry of the Interior and Safety*. Retrieved January 20, 2025, from https://www.bai.go.kr/bai/result/organ/list

Board of Audit and Inspection (BAI). (2025b, October 20). *Intelligent informatization project, Ministry of Science and ICT*. Retrieved January 20, 2025, from https://www.bai.go.kr/bai/result/organ/list

Board of Audit and Inspection (BAI). (2025c, October 30). *Audit of the National Computing and Information Agency's intelligent informatization projects*. Retrieved January 20, 2025, from https://www.bai.go.kr/bai/result/organ/list

Byeon, S., & Cho, J. (2025, May 23). Strategies for Sustainable Operation of Data Centers: Technological and Institutional Approaches. *KIEAE Journal*.

Kakao. (2025, October 19). *Reasons for 2022 KakaoTalk service outage*. Retrieved January 20, 2025, from https://www.kakaocorp.com/page/detail/9902?lang=KOR

Kang, H. (2024). Research on Data Replication Method for Building an Enterprise Disaster Recovery System. *The Journal of the Convergence on Culture Technology, 10*(1), 411-417.

Kang, H. S. (2018). A Study on Information System and Disaster Recovery System for Business Continuity. *Journal of Security Engineering, 15*(5), 319-332.

Kang, K. H. (2020). *Blockchain siseutem-eul iyonghan geumyung-gigwan-ui hyoyuljeogin jaehaebokgusiseutem unyoungbangan* [Management strategies of effective disaster recovery system for financial institutions using the blockchain system] (Master's thesis, Kwangwoon University, Korea). Retrieved from https://www.riss.kr/link?id=T15685085

Kim, H., Lee, S., & Shin, I. (2013). BCP utilizing Disaster Recovery-System for the Protection of the Information System Design. *Journal of the Korea Society of Computer and Information, 18*(7), 93-100.

Kim, S. S. (2018). *Jaenane daebihan jibangjachidanche jeonjagirokmurui jaehaebokgusiseutem guchuk bangan: Onnarasiseutem, pyojungirokgwansiseutem jungsim* [A study on the construction of disaster recovery system for electronic records of local governments: Focusing on On-nara system and standard records management system] (Master's thesis, Joongbu University, Korea). Retrieved from http://www.riss.kr/link?id=T14780922

Korea Policy Briefing. (2025a, October 17). *Crisis alert for the fire at the National Computing and Information Agency*. Retrieved January 20, 2025, from https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000336

Korea Policy Briefing. (2025b, October 19). *Number of services at the National Computing and Information Agency*. Retrieved January 20, 2025, from https://www.mois.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000336&nttId=121257

Korea Policy Briefing. (2025c, October 19). *Ministry of the Interior and Safety's Disaster Recovery System recovery time*. Retrieved January 20, 2025, from https://www.korea.kr/news/policyNewsView.do?newsId=148907215

Korea Policy Briefing. (2025d, October 20). *Three Digital Safety Acts*. Retrieved January 20, 2025, from https://www.korea.kr/briefing/pressReleaseView.do?newsId=156577257

Korea Policy Briefing. (2025e, October 20). *Ministry of Science and ICT (MSIT) measures to strengthen digital service stability*. Retrieved January 20, 2025, from https://www.korea.kr/briefing/pressReleaseView.do?newsId=156560039

Korea Policy Briefing. (2025f, October 20). *Digital service failure investigation results*. Retrieved January 20, 2025, from https://www.korea.kr/briefing/pressReleaseView.do?newsId=156540807

Korea Policy Briefing. (2025g, October 30). *Announcement of digital service failure investigation results and corrective requests*. Retrieved January 20, 2025, from https://www.korea.kr/briefing/pressReleaseView.do?newsId=156540807

Korea Policy Briefing. (2025h, November 1). *Recovery status of National Computing and Information Agency information systems*. Retrieved January 20, 2025, from https://www.mois.go.kr/frt/bbs/type013/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000006&nttId=121213

Lim, S. M., & Lee, Y. J. (2004, May 21-22). A Study on Disaster Recovery Planning and Automation Support System Implementation in a Data Consolidation Center of Multi-organizations. *Proceedings of the Journal of the Korean Operations Research and Management Science Society*.

Lim, S. M., & Lee, Y. J. (2005). A Study on Models of Data Consolidation Center for Multi-Organization in Public Sector. *IE Interfaces, 18*(4), 418-430.

National Computing and Information Agency (NCIA). (2025, October 21). *Digital government service design, construction, and operation manual*. Retrieved January 20, 2025, from https://www.nirs.go.kr/