September 29, 2026 National Assembly Budget Office NABO Focus Vol. 177

nabo Focus

Effectiveness of Personal Information Breach-Related Fiscal Programs and Improvement Tasks

Industry Budget Analysis Division Analyst Kim Ji-su

Background

▪ **In the first half of 2026, 432 personal information breach reports[1] were filed, nearly matching the annual total of 447 in 2025. A series of large-scale breaches at major operators handling citizens' personal information has heightened the need to assess the effectiveness of personal information protection programs.**

- Large-scale breaches affected companies providing services closely tied to daily life, including TVING (39.54 million accounts), Coupang (37.56 million people), and Duo (430,000 people).[2]

※ Breach reports: ('21) 163 → ('25) 447 → (H1 '26) 432

▪ **The Personal Information Protection Commission's major program expenditures increased by KRW 20.25 billion (58.3%), from KRW 34.72 billion in 2022 to KRW 54.97 billion in 2026. The government's 2027 budget proposal allocates KRW 80.1 billion, an increase of KRW 25.13 billion (45.7%).**

- Major programs include "Strengthening Personal Information Protection," which establishes a foundation for protection through policymaking, education, and certification, and "Response to Personal Information Issues," which enhances investigative capacity through breach investigations and the operation of a digital forensics lab.
- R&D programs, such as "Development of Technologies for Trust-Based AI Personal Information Protection and Utilization (R&D)," are also underway, with KRW 18.16 billion allocated in the 2027 budget proposal.

[Table 1] Major Personal Information Protection Programs (2022–2027)

(Unit: KRW million, %)

Category	2022	2023	2024	2025	2026	2027 (Proposal)	Change rate (vs. '26)
Major program budget	34,719	42,721	49,364	48,995	54,967	80,095[1]	45.7
(1031) Strengthening Personal Information Protection	8,925	9,231	9,639	9,693	8,478	8,792	3.7
(2034) Response to Personal Information Issues	8,044	11,139	9,832	10,887	10,815	14,454	33.6

Note: 1) The 2027 figure includes the Public Interest Reporting Encouragement Fund program (Ministry of Planning and Budget).

1. The 2022–2026 figures represent current budget amounts, while the 2027 figure represents the government's budget proposal. All figures are based on the 2027 budget classification.

Source: Personal Information Protection Commission

1) Personal Information Protection Commission press release (July 16, 2026), "Achieving Prevention-Centered Personal Information Protection That Supports AI Innovation and Promotes Citizens' Rights"

2) Duo and Coupang figures are based on the Commission's sanction decisions dated April 22 and June 10, 2026, respectively; the TVING figure reflects the breach scale confirmed in June 2026.

▪ **This paper examines the operational performance of related fiscal programs and identifies areas for improvement to assess whether increased fiscal inputs in response to surging breach incidents have improved incident investigation performance and breach prevention.**

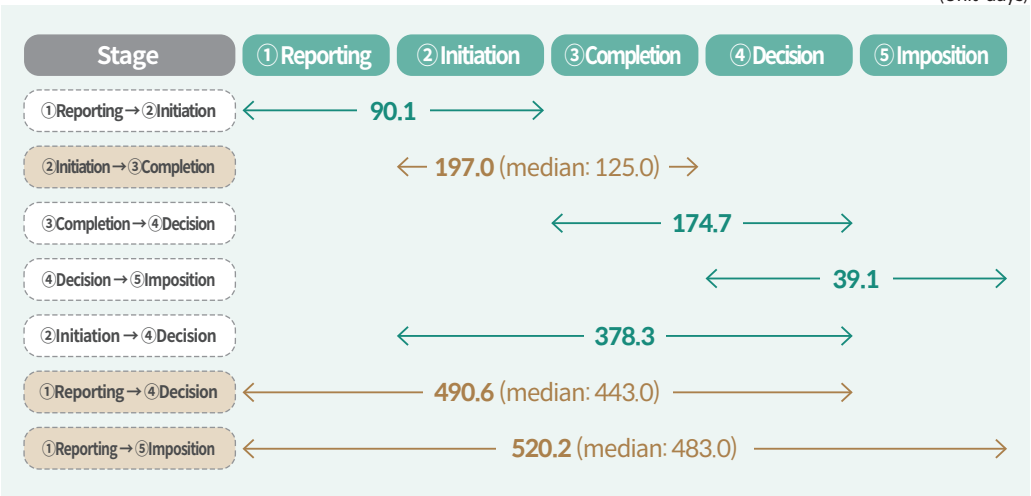
Problem ①
: Prolonged Incident Investigations

▪ **Incident investigations have been prolonged, averaging 490.6 days from breach reporting to decision.**[3)]

- Cases with identifiable processing dates were analyzed among approximately 700 cases with published decisions from November 2020 to April 2026.
- On average, reporting → investigation initiation took 90.1 days, initiation → completion 197.0 days, and completion → decision (disposition) 174.7 days. Reporting to decision averaged 490.6 days, and reporting to imposition of fines and penalty surcharges averaged 520.2 days.

[Figure 1] **Average Duration of Personal Information Incident Investigations by Stage (Nov. 2020–Apr. 2026)**

(Unit: days)



Notes: 1. The analysis covers cases with identifiable dates for each stage among decisions published on the Personal Information Protection Commission's website from November 2020 to April 2026. Case counts may vary by stage.
2. Includes only investigations based on reports or tips, excluding planned investigations and preliminary inspections.
3. Stage durations are calculated from the dates of reporting, investigation initiation, investigation completion (or prior notification), decision (disposition), and imposition of fines and penalty surcharges.

Source: National Assembly Budget Office analysis based on the Commission's published decisions and press releases

- However, the Commission appears to have limited capacity to analyze delays and the causes of long-pending cases using stage-by-stage processing statistics and to systematically manage individual case statuses.

▪ **Although investment in investigation support has increased in response to rising breach reports, including additional investigators and a digital forensic lab, improvements in case processing and processing time appear limited.**

3) National Assembly Budget Office analysis based on the Commission's published decisions and press releases

[Table 2] **Breach Reports, Decisions, and Processing per Investigator (2021–2025)**

(Unit: cases, persons, days)

Category	2021	2022	2023	2024	2025
Breach reports received	163	167	318	307	447
Incident investigation decisions	264	162	272	318	360
Investigation personnel	30	34	37	37	38
Decisions per investigator	8.8	4.8	7.4	8.6	9.5
Avg. days, reporting → decision (disposition)	357.7	436.8	528.3	589.1	508.2

Notes: 1. Reports are counted by year of receipt and decisions by year of decision (disposition). Decisions include nonpublic items, self-initiated investigations, and cases transferred from other ministries, but exclude planned investigations and preliminary inspections.
2. Investigation personnel are year-end headcounts of staff directly conducting incident investigations; decisions per investigator = decisions ÷ investigation personnel.
3. Average days are based on NABO's own analysis of published decisions (see [Figure 1]), covering only cases with identifiable reporting and decision dates and excluding planned investigations and preliminary inspections.

Source: Recompiled by the National Assembly Budget Office based on materials submitted by the Commission

- Decisions per investigator increased only slightly, from 8.8 in 2021 to 9.5 in 2025.
- The average time from reporting to decision remained high: ('21) 357.7 → ('24) 589.1 → ('25) 508.2 days.
- Although the forensic lab was established in December 2025, dedicated staff were still being recruited as of September 2026, leaving the operational foundation for its full use in investigations inadequate.

▪ **Despite statutory time limits for investigation and case processing, substantial delays occur between reporting and investigation initiation, raising concerns about the timeliness of investigations and dispositions.**[4)]

- Of 310 cases with identifiable reporting and initiation dates, only 102 (32.9%) began within 14 days of reporting, while 58 (18.7%) took 180 days or longer to initiate.

▪ **Of 1,402 breach reports filed from 2021 to 2025, only 538 cases had decisions recorded during the same period, suggesting a growing backlog of undecided and ongoing cases.**

- Because the processing-period analysis covers only published decisions in completed cases, actual durations may be longer if long-pending undecided and ongoing cases are included.

4) Regulations on Investigations and Dispositions by the Personal Information Protection Commission
Article 5 (Preliminary Review, etc.)
② For reports under Article 4, etc., an investigator shall report to the relevant director general within 14 days of case assignment on whether to initiate an investigation. This period may be extended where unavoidable circumstances, such as fact verification, warrant an extension.
Article 7 (Investigation Period)
① The investigation commencement date shall be the date of the investigation initiation report under Article 6.
② An investigator shall complete the investigation results report under Article 15(1) within six months of commencement (12 months for complex cases requiring expertise). Where an extension is necessary due to unavoidable circumstances, the investigator shall specify the extension period and report it to the relevant director general.

Problem ②
: Inadequate Investigation and Response Systems

▪ **Operational negligence is the leading cause of breaches in the public sector, while hacking predominates in the private sector. However, investigation and prevention programs do not adequately address these differing risk factors.**

- In 2025, operational negligence accounted for the largest public-sector share at 53.1% (68 cases), while hacking accounted for 72.7% (232 cases) in the private sector.
  - Operational negligence includes procedural compliance failures, such as misaddressed recipients, access-permission errors, and publicly posting personal information. Hacking involves technical intrusion routes, including malware infection (ransomware and web shells) and exploitation of web vulnerabilities such as SQL injection.

[Table 3] **Personal Information Breach Reports by Cause and Sector (Public and Private)**

(Unit: cases, %)

Category	Public sector			Private sector		
	Cause	Cases	Share	Cause	Cases	Share
1	Operational negligence	68	53.1	Hacking	232	72.7
2	Hacking	44	34.4	Operational negligence	42	13.2
3	System error	6	4.7	System error	18	5.6
4	Unknown cause	5	3.9	Unknown cause	16	5
5	Intentional disclosure	5	3.9	Intentional disclosure	11	3.4

Source: Personal Information Protection Commission and Korea Internet & Security Agency, "Trends in Personal Information Breach Reports and Investigation and Disposition Cases in 2025"

- Accordingly, internal controls, access permissions, and processing procedures appear particularly important in the public sector, while intrusion routes and security vulnerabilities are more significant in the private sector.

Problem ③
: Inadequate Feedback of Investigation Results into Prevention

▪ **Breaches continue to recur at the same institutions, yet vulnerabilities identified through investigations and dispositions are not adequately incorporated into preventive mechanisms, limiting their effectiveness in preventing recurrence.**

- The analysis identified 47 institutions with two or more confirmed breaches (128 related cases), highlighting the need to assess whether their protection systems have improved.
  - Repeated incidents may result from previously identified vulnerabilities as well as other legal violations and administrative or technical weaknesses. Corrective individual violations alone may therefore be insufficient to improve an institution's overall protection system.
  - Incident investigations and dispositions, inspections of intensively managed public-sector systems[5], personal information protection level assessments[6], and (public-sector) ISMS-P certification and follow-up[7] operate separately. As a result, vulnerabilities identified and improvements achieved are not adequately reflected in the inspection criteria and assessment indicators of preventive mechanisms.

5) A system that designates public systems processing large-scale or sensitive personal information and intensively manages their safety measures, pursuant to Article 30-2 of the Enforcement Decree of the Personal Information Protection Act and Article 14(1) of the Standards for Measures to Ensure the Safety of Personal Information.

6) An annual assessment of public institutions' implementation of personal information protection policies and duties and compliance with statutory requirements, pursuant to Article 11-2 of the Personal Information Protection Act.

7) A certification system verifying that information security and personal information protection management systems meet established standards, pursuant to Article 32-2 of the Personal Information Protection Act and Article 47 of the Act on Promotion of Information and Communications Network Utilization and Information Protection.

Tasks for Improvement

▪ **Case management procedures and investigation support infrastructure need to be reorganized to accelerate incident investigation processing.**

- Given confirmed delays in initiating investigations after reporting, cases should be prioritized by breach scale, potential harm, and complexity. Processing times at each stage from reporting to decision, along with reasons for delays, should be monitored.
- Given the large number of cases without complete decisions (dispositions), processed and unprocessed reports should be tracked separately by year, and separate procedures should be established for long-pending cases, including confirming reasons for delays and establishing processing plans.
- Dedicated forensic lab staff and other operational resources should be secured, and case support results and analysis times monitored to ensure that these resources strengthen actual investigation capabilities.

▪ **Investigation and prevention programs need to be designed to address the distinct causes of incidents in the public and private sectors.**

- Given the high share of operational negligence in the public sector, checks of internal controls, access permissions, and processing procedures and monitoring of improvement measures should be strengthened, along with accountability measures such as linkage to institutional assessments.
- Given the high share of hacking in the private sector, technical investigation capabilities, including intrusion route analysis and digital forensics, should be strengthened. Major vulnerabilities identified through investigations should inform prevention and inspection programs.

▪ **A feedback system needs to be established to link investigation and disposition results to preventive mechanisms.**

- For institutions with large-scale or repeated breaches, responses should extend beyond corrective action for individual violations to comprehensively address the causes of recurrence and administrative and technical vulnerabilities, enabling institution-wide improvements to protection systems.
- Recurrent vulnerabilities identified through investigations should be accumulated and classified by type and reflected in the inspection criteria of preventive mechanisms, including public institution protection level assessments, ISMS-P certification management, and inspections of intensively managed systems.

☞ For details, see *Overall Analysis of the Settlement of Accounts for Fiscal Year 2025 III*, "Tasks for Improving the Response System for Personal Information Breaches and the Operation of Personal Information Protection Policies"

Publication Registration No. | **31-9700484-001731-14** ISSN | **2672-0280**
Published by | **National Assembly Budget Office** Publisher | **Chi Dong-ha, Chief of the National Assembly Budget Office**
Produced by | **Industry Budget Analysis Division, Budget Analysis Department** Contact | **+82-2-6788-4630**

National Assembly Budget Office