Revisions of the Cloud Security Assurance Program (CSAP)

Control Strategy Officer Noh Min-cheol

The Ministry of Science and ICT announced partial amendments to cloud security assurance (CSAP[1]), a certification required for private companies to provide cloud services to the public sector on January 31, and it is currently in effect. This revision was made 7 years after the 「Criteria for Cloud Computing Service Information Protection」 had been announced in April 2016.

The main content of this amendment is to divide the cloud security assurance system in the public sector into high, middle, and low levels according to system importance, and to have a different security regulation for each level. In particular, the revision relaxes the security regulation for the 'low' level by allowing logical network separation in addition to physical network separation.

Moreover, as it is expected that the government/public agency information system cloud conversion project to be carried out by 2025 will begin with a relatively less sensitive task, i.e. the 'low' level, some of the domestic and overseas cloud service providers (CSP[2]) reacted with joy while others with disappointment. It is said that the decision was made to revitalize the overall cloud market and innovate public services by opening up the public domain where security deregulation is limited, but concerns are raised that domestic CSPs, which are relatively less competitive than their overseas counterparts, may be pushed out of the competition.

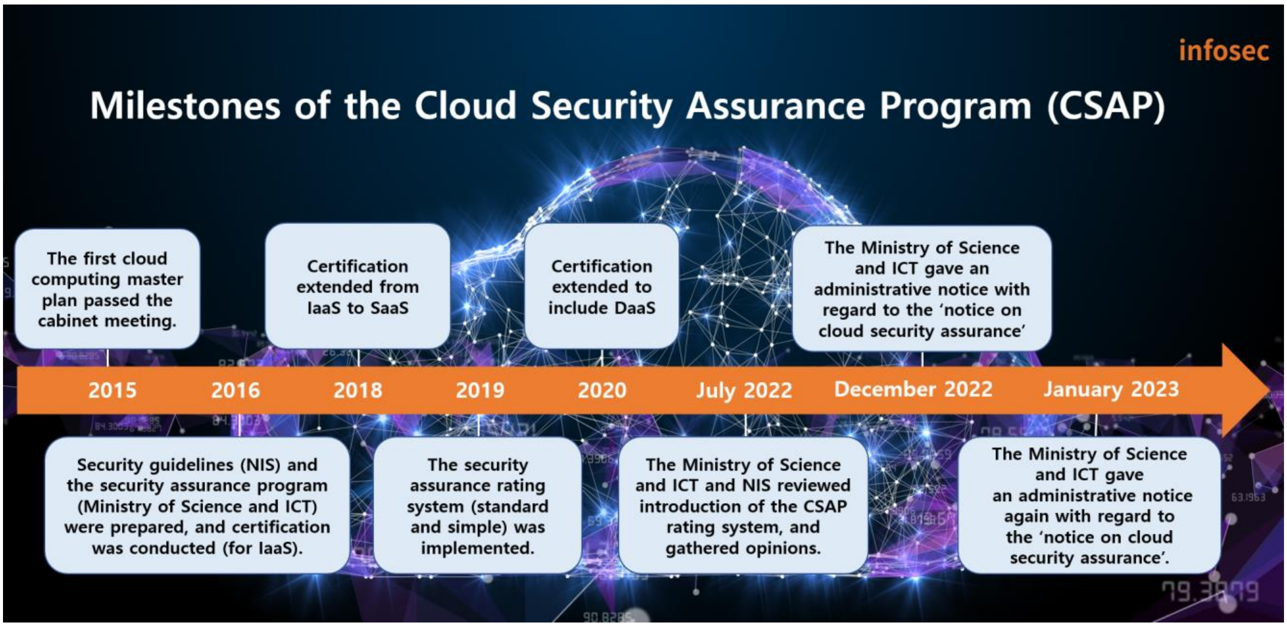
In this headline, we will review the background of the revision of the Cloud Security Assurance Program, the situation of domestic/overseas cloud service providers (CSPs), and the contents of administrative/physical/technical safeguards changed by this revision.

[1] It is a system that enables certification authorities to evaluate and certify whether the services provided by cloud service providers comply with the information protection standards in accordance with Subparagraph 2 of Article 23 of the 『Act On The Development Of Cloud Computing And Protection Of Its Users』, and supports users so that users can safely use cloud service.

[2] A Cloud Service Provider (CSP) means a company that provides public cloud infrastructure and platform services. A CSP builds its own data center, provides multiple virtualized physical servers, and supports everything necessary for server operation, such as network, storage and power. Representative examples are Amazon's 'AWS', Microsoft's 'Azure' and Google's 'GCP'. Domestic companies include NAVER Cloud, NHN Cloud and KT Cloud.

* Source: Korea Internet & Security Agency (KISA) website

1. Background and progress of Cloud Security Assurance Program (CSAP) revision



Milestones of the Cloud Security Assurance Program (CSAP)

2015: The first cloud computing master plan passed the cabinet meeting.

2016: Security guidelines (NIS) and the security assurance program (Ministry of Science and ICT) were prepared, and certification was conducted (for IaaS).

2018: Certification extended from IaaS to SaaS

2019: The security assurance rating system (standard and simple) was implemented.

2020: Certification extended to include DaaS

July 2022: The Ministry of Science and ICT and NIS reviewed introduction of the CSAP rating system, and gathered opinions.

December 2022: The Ministry of Science and ICT gave an administrative notice with regard to the 'notice on cloud security assurance'

January 2023: The Ministry of Science and ICT gave an administrative notice again with regard to the 'notice on cloud security assurance'.

* Source: The reprocessed image from an Electronic Times article (https://www.etnews.com/20230130000194)

In the meantime, overseas CSPs such as Amazon Web Service (AWS), Microsoft (MS), and Google Cloud have been steadily requesting deregulation of the Cloud Security Assurance Program (CSAP) to enter the Korean market. After US President Joe Biden visited Korea in May 2022, it was reported that the American Chamber of Commerce in Korea sent an official letter to the Ministry of Science and ICT about the Cloud Security Assurance Program (CSAP) and permission of logical network separation. Later, as the National Intelligence Service gathered opinions on the Cloud Security Assurance Program (CSAP) deregulation from domestic CSPs, details of the deregulation began to be announced.

In June 2022, the Ministry of Science and ICT held a meeting on 'Measures for Supporting Growth of Domestic SW Companies and Overseas Expansion for a Qualitative Leap in the SW Industry' and issued instructions for mitigation and revision of the Cloud Security Assurance Program (CSAP) and announced a plan to mitigate the security assurance system within the third quarter. In July, the Ministry of Science and ICT announced a plan to subdivide security assurance into high, middle, and low levels, and in August, it formalized security assurance program levels and differential application of the mitigation measures.

In November 2022, the Ministry of Science and ICT held a briefing session on the cloud security assurance revision plan, and provided information on the certification evaluation method regarding which companies complained about a burden in the existing security assurance process along with major changes according to the announced revision of the cloud security assurance evaluation agency designation plan, the certification evaluation fee imposition and support plan, etc.

During this process, there was an attempt to hold a meeting with domestic CSPs in relation to security assurance, but most of the companies did not attend the meeting. Rather, domestic CSPs criticized the Government's revision of the Cloud Security Assurance Program as "going against the global trend" during the parliamentary inspection of government offices, and demanded improvement of the system.

Later in December 2022, the Ministry of Science and ICT issued an administrative notice on the partial amendments to the 「Notice on cloud security assurance notice on cloud security assurance」 on January 18, 2023, and finally on January 31, 2023, the ministry partially revised and announced the 「Notice on cloud security assurance」 (Ministry of Science and ICT Notice No. 2023-3).

The Ministry of Science and ICT said the reason for the revisions was "to determine matters necessary for the introduction of a cloud security assurance grading system that classifies the systems of national agencies into 3 levels to revitalize the use of private cloud in the public sector and applies differentiated security assurance standards to different levels.

2. Details of the revisions of the Cloud Security Assurance Program (CSAP)

The major revisions announced on January 31, 2023 are divided into three major categories.

A. Establishment of a grading system for the existing cloud security assurance (revision of Article 14)

− Establishing the grounds for implementation of a grading system (high, medium and low level) that applies differentiated security assurance standards according to the information protection level of cloud computing service

B. Disclosing detailed inspection items according to security assurance types and levels (revision of Article 15)

− Establishing the grounds for disclosing detailed inspection items within the security assurance standards according to cloud security assurance types and levels

C. Revision of security measures according to cloud security assurance levels (schedules 1, 2, 3, 4 and 7)

− Revising cloud computing service safeguards used by national agencies, e.g. administrative, physical and technical

Examining the revised Cloud Security Assurance Program (CSAP),

First, according to Article 14 of the 「Notice on cloud security assurance」 (security assurance types and levels), cloud security assurance are divided into 4 types and 3 levels.

The types of security assurance are as follows:

〈Table 1〉 Security assurance type

Classification	Security assurance type
IaaS certification	Certification of services that provide servers, storage devices and networks
SaaS certification	Certification of services that provide software like application programs
PaaS certification	Certification of services that provide the environment for development, distribution, operation and management of software like application programs
Other	Certification of services that combines two or more of the above three services certification

According to the above security assurance types, the security assurance levels are divided into high, medium, or low after revision from the existing IaaS, SaaS (standard level), SasS (simple level), and PaaS.

〈Table 2〉 Evaluation criteria by security level

Level	System level classification	Evaluation criteria
Low	Disclosed public data operation systems that do not include personal information	· Improvement: physical network separation → logical network separation - Relieving existing physical separation requirements between private and public sectors to allow SaaS (domestic software as a service) providers to enter the public market - However, the physical location of the cloud system and data is limited to Korea.
Medium	Systems that include or operate confidential business data	· Maintaining the current level - Allowing secure network access · Rational simplification - Integrating and abolishing existing types (IaaS, SaaS standard, SaaS simple) and deleting unnecessary items - Relaxing table separation criteria by institution
	Depending on the importance, administrative internal work systems can also be included.	
High	Administrative internal work operation systems that include sensitive information	· Reinforcing security

There are 82 systems that acquired cloud service security assurance between 2016 and February 2023, and can be used by government agencies: 9 IaaS, 22 SaaS standard, 48 simple SaaS, and 3 DaaS.

〈Table 3〉 Systems that acquired cloud service security assurance by year

Year	Total		2016	2017	2018	2019	2020	2021	2022	2023
Current status	82		1	3	2	8	8	23	26	11

For more information, visit the National Cyber Security Center[3] under the National Intelligence Service and the Korea Internet & Security Agency (KISA)[4].

[3] Basic Guidelines on National Information Security (as of January 31, 2023). https://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=InstructionGuide_main&nttId=18590&pageIndex=1

[4] Cloud security assurance certificate issuance by year. https://isms.kisa.or.kr/main/csap/issue/

Second, Article 15 (security assurance standard) classified Cloud Security Assurance Program (CSAP) items into 14 control items and 117 evaluation items. 14 control items and 106 evaluation items for administrative/physical/technical safeguards (schedules 1～3) are applied.

〈Table 4〉 Control items and evaluation items by administrative/physical/technical area

Classification	Control item	No of evaulation items	No of low grade applied
Administrative	Information protection policies and organizations	5	2
	Human security	11	2
	Asset management	10	3
	Service supply chain management	4	2
	Incident management	7	6
	Service continuity management	7	5
	Compliance	4	2
	Subtotal	48	22
Physical	Physical protective zone	5	2
	Protection of information processing facilities and equipment	6	-
	Subtotal	11	2
Technical	Security of virtualization	10	6
	Access control	9	9
	Network security	6	5
	Data protection and encryption	10	3
	System development and introduction security	12	6
	Subtotal	47	29
Total of 14 areas		106	53

In addition, if cloud computing services are provided to administrative and public agencies, the cloud computing service safeguards (schedule 4) used by government agencies, etc., apply 11 evaluation items in one area.

〈Table 5〉 Public institutions' security requirement control items and evaluation items

Classification	Control item	No of evaulation items	No of low grade applied
Public institutions' security requirements	Administrative safeguards	4	4
	Physical safeguards	2	2
	Technical safeguards	5	5
	Subtotal	11	11

Detailed inspection items are disclosed on the Korea Internet & Security Agency website.

Lastly, evaluation items for administrative/physical/technical safeguards according to the cloud security assurance levels have been partially changed.

In particular, in relation to cloud computing service safeguards used by national agencies, there is the most controversy in the part where all of the high, middle, and low levels are applied to the physical location and area separation control items within the physical safeguards. To meet the physical location criteria for cloud systems, backup systems and data, and the management and operation personnel for them, the data center must be located in Korea, and CC certification must pass the Common Criteria supervised by the National Intelligence Service.

For network separation, the physical network separation, which used to be applied previously, is applied to the high and mediun levels, and only the lower levels are applied so that physical or logical network separation is possible for the cloud computing service areas for general users.

3. Situation of domestic/overseas CSPs following the revision of the Cloud Security Assurance Program (CSAP)

According to the Fair Trade Commission, overseas cloud services already accounted for more than 73% of the private market in 2021 (AWS 62.1%, and Azure 12%). If the cloud market is opened due to the revision of the security assurance program, it is predicted that the monopoly or oligopoly of foreign companies can be expanded to the public market. So the position of domestic CSPs (NAVER, KT, NHN) is very negative. Along with this, there are voices of concern that large-scale foreign companies will dominate the domestic market and data sovereignty will be seriously damaged.

Due to existing physical network separation requirements of security assurance, foreign CSPs were not allowed to enter the Korean market, but foreign companies' entry into the public sector is becoming more likely as the revision makes an exception for the "low" level and 61 items among the existing control items. Due to this, there is a concern that foreign companies may encroach on the public market as well. So it is requested that the high, middle, and low levels should be implemented at the same time.

On the other hand, unlike the domestic cloud service providers (CSP), the managed service providers (MSP)[5] are neutral. This is because it was found that foreign global CSP companies that have entered the domestic market actively utilize transactions through MSPs rather than direct transactions with customers in the domestic market. Therefore, as major domestic managed service providers, such as Megazone Cloud and Bespin Global, can get opportunities to expand their business through collaboration with Amazon and Google, they are in favor of it internally, whereas they seem to be very prudent externally. On the other hand, as SaaS-related companies, many of which are SMEs, are expecting more business opportunities if foreign CSP companies participate in the market, their expectations are running high.

[5] MSP (Managed Service Provider) is a cloud management service provider in charge of overall cloud business, from consulting for cloud introduction to conversion, construction, operation, and maintenance service. It applies effective service configuration plans according to various services provided by CSP and customer needs, and helps management so that the applied cloud infrastructure can be safely operated 24 hours a day, 365 days a year. Representative domestic MSPs include Bespin Global, Megazone Cloud, and GS Neotek.

4. Closing

So far, we have looked at the background of the security assurance program and the changes to come.

The Ministry of Science and ICT plans to prepare and implement separate standards for the high and medium levels after the announcement of the Cloud Security Assurance Program (CSAP). However, it is possible to apply for certification with regard to security assurance types and levels (IaaS, SaaS standard, SaaS simple, etc.) according to the previous notice until the implementation of the high and medium levels, and the existing SaaS simple certification can be recognized as equivalent to a lower level certification.

The Government expects that a private cloud market is formed in the public sector due to deregulation, and overall demands will expand, but CSP (cloud service providers), MSP (managed service providers), and software as a service (SaaS) have mixed views. In particular, opposition from domestic CSP companies is expected amid concerns that foreign CSPs that have already dominated the private market will dominate the public market as well, reducing the competitiveness of domestic cloud service providers. On the other hand, it is known that overseas CSPs are continuously requesting that the high and medium levels should be deregulated as well through the US government.

There are also concerns that public data sovereignty may be undermined. Although the physical storage location of the system and data for the cloud service is limited to Korea, there are concerns that data may be leaked abroad through the backup data system. We hope that the Government and CSP companies will do their best to coordinate their opinions so that data sovereignty can be secured and reliable and stable services can be provided.