

KOREAN SECURITY BRIEFING REPORT

SECON & eGISEC 2023 is Asia's only Integrated Security Exhibition, celebrating its 22nd anniversary this year. This report is to help better understanding of Korean Security Market for visitors and exhibitors of SECON & eGISEC 2023.

Learn more about Security by visiting SECON & eGISEC 2023 in KINTEX, 29(Wed)~31(Fri) March 2023.

1. Korean Security Market Outlook

Under COVID-19 pandemic, Korean security companies have found their own breakthroughs by targeting non-face-to-face · non-contact solutions, COVID-19 preventive measures, and activation of telecommuting.

SECON & eGISEC's official media <Boannews> and <Security World> conducted "2022/2023 Security Market Survey" at the end of 2022. According to this survey, Korean industry is very positive about the market growth rate.

1-1. 2021~2024 Korean Security Market Volume

The volume of the Korean security market, combining both physical and cyber security in 2022, was \$5 billion. This was a 9% rise from \$4.7 billion in 2021.

The volume of the Korean cybersecurity market in 2022 was \$1.8 billion, up 11.2% from \$1.6 billion in 2021. It is expected to reach \$1.9 billion in 2023, up 5.8% from 2022, and \$2 billion in 2024, up 4.4% from 2023.

The volume of the Korean physical security market in 2022 was \$3.3 billion, up 7.8% from \$3 billion in 2021. In 2023, it is expected to be \$3.4 billion, up 4.3% from 2022, and \$3.6 billion in 2024, up 3.5% from 2023.

1-2. 2023 Security Budget by Korean Ministry of Science and ICT

Among "2023 government budget" of Korean Ministry of Science and ICT, budget related to information security and security itself was set at \$20 million. Training of information security professionals (preparing measures to train 100,000 talented cybersecurity professionals) was the largest at \$12 million. Information security system evaluation and certification base strengthening project (\$1.6 million), digital convergence security base expansion project (\$3 million for development of digital safety leading model, \$3 million for commercialization of quantum technology) were newly reflected in the budget.

2. Physical Security Market in Korea

Korean physical security market faced a new phase as various systems and products for safety received attention due to the enforcement of the Serious Disaster Punishment Act and the Itaewon disaster.

The continued advancement of artificial intelligence(A.I.) leads to convergence with various areas, and smart cities, where all security fields are applied, are expanding not only in large cities but also in small and medium-sized cities.

CCTV, which represents video surveillance products, is gradually evolving from a simple monitoring tool to an intelligent and autonomous situation recognition method, and is expanding its scope by converging with information security to protect video data.

2-1. 2022~2024 Korean Physical Security Market Volume

Looking at Korean physical security market in detail, the CCTV video surveillance sector achieved \$1 billion (34.1% share) in 2022. It is expected to reach \$1.1 billion (33.31% share) in 2023 and \$1.2 billion (33.74% share) in 2024. Integrated security services, smart cities, and alarm monitoring achieved \$1.5 billion (45.09% share) in 2022. It is expected to reach \$1.58 billion (45.37% share) in 2023 and \$1.6 billion (44.1% share) in 2024. The access control, biometric, and counter-terrorism sectors achieved \$690 million (20.81% share) in 2022. It is expected to reach \$730 million (21.32% share) in 2023 and \$800 million (22.16% share) in 2024.

2-2. Up-to-date Policies Regarding Korean Physical Security

1) The 1st Basic Plan for Data Industry Promotion (2023~2025)

"The 1st Basic Plan for Data Industry Promotion" is a legal plan established by Korean government to promote production · transactions of data every three years and to create a foundation for the data industry under Article 4 of "Act on the promotion of data industry and the activation of data use." Furthermore, it plans to create a national database that conveniently finds and utilizes data by establishing a "ONE Window" (2023, ISP) and "National Standardization Map" that allows anyone to easily search private · public data and access to information of valuation · quality certification.

2) AI Generalization · Industry Advancement Plan by Korean MSIT (2023)

Korean MSIT(Ministry of Science and ICT) plans to push forward the top 10 A.I.(Artificial Intelligence) projects, starting with an investment of about \$540 million in 2023, in order to spread AI to the entire country and generate practical results in the AI industry.

In the private sector, it will create large-scale AI demand such as "support for AI care robots for the elderly living alone," "introduction of AI robots and telephone counselling rooms for small business owners," and "application of medical AI in public hospitals."

In the technology sector, AI semiconductor technologies such as next-generation AI (2022-2026, \$2,800 million) that overcome current AI limitations as deep machine learning and lack of reliability, AI development (2023-2027, \$34 million), and NPU, Pim, and advanced packaging (2023, \$50 million in 2023) will be secured.

3) Plan to Provide Statistical Register by Statistics Korea (2023)

The Statistics Korea plans to provide a "statistical register" that links administrative data and statistical data so that it can be used in fusion with various data. It plans to focus on developing "comprehensive pension statistics" that link public · private pension data, analysing household debt status and characteristics through public · private cooperation, and developing "SGIS" that visualizes natural disasters and various statistical information on the map.

2-3. Korean Physical Security Trends

1) AI Upgrades to Deep Learning

"Intelligent" is a modifier for computers, automation, and applications, including CCTV, when artificial intelligence (AI) technology is applied. "Deep Learning" is a technology that classifies a lot of data, binds the same set together, identifies the relationship between the top and bottom, and allows computers to think and learn like humans. Korean security industry, which has been actively introduced and advanced artificial intelligence since a few years ago, is evolving from intelligent to deep learning and is mounting · developing various technologies. Gimpo Airport's parking area for the disabled operates a real-time crackdown system for illegal parking. Tongyeong City operates a CCTV suicide prevention system that applies AI deep learning techniques. Based on AI deep learning technology, it detects suicide risk behavior in advance by learning and analyzing lean-behavior among characteristics of suicide behavior. The Inhyeon Market Merchants Association in Seoul conducted an AI camera demonstration project to recognize fire using edge computers and deep learning for a year. The Busan Yacht Stadium and Geoje Botanical Garden in Gyeongsangnam-do completed a demonstration test of the "Integrated Platform for Safety Management-based on AI" at the end of 2022. The platform is equipped with parking specialties, abnormal behavior detection, road situation control, and marine facility management.

2) Density Monitoring, Leading Intelligent CCTV and Video Analysis

On 29th, October 2022, 158 people were killed and 197 injured as a large crowd gathered to enjoy the Halloween festival in Itaewon-dong, Yongsan-gu, Seoul. After the 10·29 disaster, the Ministry of the Interior and Safety held a joint meeting of public-private to establish a system for preventing and managing crowd-intensive accidents based on ICT (information and communication technology). At the meeting, measures to establish an "On-site Crowd Management system" using location signal data (moving population) from base-station, public transportation data from transportation institutions, and CCTV footage from local governments were discussed. It also discussed ways to apply them to on-sites through the revision of the Disaster Safety Act and R&D of CCTV and drone images for public safety. It is to establish and operate a system that can monitor density and prevent accidents by utilizing "People Counting" and "Group" functions of intelligent CCTV and intelligent video analysis solutions that have been mainly used for life safety and crime prevention before.

3) Access · Attendance Control Security Market

In Korea, "52-hour workweek", which took effect in July 2018, limited workers' extended working hours per week to a maximum of 12 hours. The 52-hour workweek has also been applied to workplaces with more than five employees and less than 50 employees since July 2021. Even if labor-management agree or workers want to, employers will face up to two years in prison or fines of up to \$15,000 if they exceed 52 hours of working hours a week. As absenteeism management function becomes more important due to the activation of telecommuting and flexible work system after COVID-19, physical security companies such as access control and biometric, integrated security service companies, groupware companies, ERP companies, and cloud-based service start-ups are fiercely competing. For user convenience, the industry not only combines biometric authentication such as face, fingerprint, and iris, but also provides various authentication methods including mobile employee ID. In addition, ERP, groupware solutions, and mobile devices are combined for effective attendance management in a telecommuting environment, and a solution that automatically shuts down the PC according to the user's leave of work time has been released.

4) Smart Agriculture Promotion, Must be Based on Security and Safety

On 8th, November 2022, Korean Ministry of Agriculture, Food and Rural Affairs announced that a bill to enact a law on fostering and supporting smart agriculture passed a state council of South Korea. The Ministry announced that it will develop and commercialize artificial intelligence (AI) prediction, AI greenhouse management, greenhouse robots, IoT for livestock, and VRT by 2027. As such, smart agriculture may be in a dangerous situation in the event of errors or hacking because various convergence · complex of high-tech technologies is used. In fact, in May 2021, JBS, which accounts for 20% of the U.S. meat supply, was attacked by ransomware, and this temporarily paralyzed the meat supply chain. According to foreign media in May 2022, about \$5 million worth of tractors were stolen by Russian soldiers from Agrotek-Invest (an agency of Russian-occupied agricultural machinery manufacturer John Deere) and all of them were remotely inoperable.

3. Cyber Security Market in Korea

3-1. 2022~2024 Korean Cyber Security Market Volume

In detail, the Korean information security product market (network security, system security, content/information leakage prevention security, etc.) reached \$1.3 billion in 2022, and is expected to reach \$1.4 billion in 2023, and \$1.5 billion in 2024. The volume of the information security service market (security consulting, security control, maintenance services, etc.) was \$440 million in 2022, and is expected to reach \$470 million in 2023, and \$489 million in 2024.

3-2. Up-to-date Policies Regarding Korean Cyber Security

1) Cyber Security, Sales Increase by \$15.349 billion Within 5 Years

In response to cyber threats that are expanding and becoming intelligent, Korean government has set a plan to increase cybersecurity sales to \$15 billion until 2027 by strengthening technology · talented people competitiveness and expanding organic cooperation between the private, government, and military. Specifically, through the 'cultivation of 100,000 talented cybersecurity professionals', the number of information security specialization schools, which is currently only three in the country, will be increased to 10 by 2026, and the number of convergence security academies will be increased from 8 in 2022 to 12 by 2026. Along with the "Cyber Talpiot" that links military cybersecurity work with job opening, the cyber reserve system will also be introduced for the systematic operation of cyber military reserve personnel.

As a national strategic industry, it will develop four major defense technologies from 2022, such as suppressing, protecting, detecting, and responding to cyberattacks, and promote the creation of cybersecurity funds to revitalize M&A and support corporate growth.

2) Secure Trust by Advancement of Blockchain and Digital Authentication

In Korea, new authentication technologies such as blockchain (DID) and biometric authentication (FIDO) will be developed within the next five years, and all identification will be converted to digital authentication. Interworking between digital certificates will also be promoted from this year so that they can be used by all institutions such as administration and finance with one certificate. Details of the 'digital wallet' evaluation · certification system that stores electronic certificates and digital certifications will be specified.

3) Deregulations on Information Security Area

In Korea, regulations regarding information security such as cloud security and information security product certification have been greatly eased from December 2022. In the field of information

security, evaluation standards related to cloud security certification will be improved and eased, and CC certification will also simplify evaluation and certification procedures when evaluating CC. The integrated product certification system will also introduce a pre-certification system along with the fast-track system to support the rapid release of innovative products. Regulations on video information will also be eased from the current resolution of 4m to less than 1.5m by expanding public disclosure.

3-3. Korean Cyber Security Trends

1) Ransomware, Developing into an Industry

One of the factors that led to explosive growth of ransomware in the past is the discovery of a tactic called "double threat." After encrypting and disabling data, they demand money, and if victims want to give up data, they threaten to disclose it to the world. Currently, ransomware organizations that have made huge profits from double threat strategies have reached the point of developing ransomware crime into an industry. A business model called Ransomware or RaaS has been established, and operators have also created negotiation portals that can safely negotiate with victims or customer support centers for customers on the dark web.

Experts predict that ransomware organizations will become more similar to corporate in the future. As large companies emerge one by one in the ransomware world, there can be ransomware specialized in certain industries or organizations that persistently target only certain companies.

2) Cloud Ecosystem, Possessing Threats in 2023

It is clear that cloud-related accidents will continue in 2023. The most common occurrence in the cloud ecosystem is accidents caused by configuration errors. Information that originally had to be accessed internally is exposed to the world due to incorrect cloud settings. Clouds are becoming increasingly complex like hybrid clouds (maintaining on-premise systems with cloud networks simultaneously) and multi-clouds (using multiple types of cloud services at the same time). As a result, the security features provided in this cloud may not work in the other cloud environments, and the same security features may need to be newly set for each cloud service. This leads to increase of mistakes and growth of attack surface. Third-party solutions are coming out that allow different clouds to be controlled through one interface, and these services are expected to be in the spotlight in 2023.

3) Smartphones, Hackers' Main Target in 2023

The security threat targeting smartphones used by the entire nation is expected to intensify in 2023. As an IT powerhouse, Korea has developed a 'mobile driver' license that can be installed on smartphones. The Ministry of the Interior and Safety cooperated with administrations of supreme court of Korea and started an electronic certificate service for 22 types of family registration certificates, including family relationship certificates, in November last year. Also, the ministry added 11 types of real estate and corporate registration certificates frequently issued and used by the public. In line with this, the attackers began to distribute malicious apps disguised as self-authentication apps and mobile ID apps. Attackers are also succeeding in high-level infringement attacks by combining stolen credentials and social engineering techniques.

4) Metaverse, Future Industry on the Rise

Metaverse is a combination of "Meta," which means transcendence and virtuality, and "Universe," which means space. Metaverse refers to a three-dimensional platform that can communicate, work, and do cultural, economic activities like the real world in the virtual world. McKinsey & Company, a consulting firm, predicted that the 2030 metaverse market will grow to up to \$5 trillion in a report titled "Value Creation in the metaverse." Interest in metaverse is also actively progressing in Korea. The Seoul Metropolitan Government announced the Metaverse Seoul Platform Ethics Guide through the Seoul Digital Foundation, and BNK Busan Bank began operating the MetaB Busan Bank, which implemented the virtual headquarters in the Metaverse Platform Zepp (ZEP). As Korea is active in the introduction and construction of metaverse, the security threat to metaverse in virtual space is also increasing and upgrading. According to the Korea Internet & Security Agency, △ non-replaceable token (NFT) theft linked to metaverse △ avatar sexual assaults △ concerns over sexual exploitation of children and adolescents through metaverse △ threats of theft and imitation of avatar and account information were selected as infringement accidents related to metaverse.

5) PhaaS, Phishing Attack as a Service

In March 2022, 'Microsoft Office 365', a subscription-type office software, was found to have been abused in the form of PhaaS. When you open an email sent from a European architectural consulting firm, a login page for Microsoft Office 365 appears. If you look at the information on the fake bait page, you can see the "open a ticket" link, and if you click this link, you will be connected to a malicious site. To learn about PhaaS, which was abused in this case, you first need to know about Phishing. Phishing is a combination of private data and fishing, and is a cyber-attack derived from fishing users' financial information and passwords. Such phishing is now further expanding its scope to "PhaaS: Phishing as a Service"(similar way to "SaaS: Software as a Service") which provides a separate "subscription service" for only the parts that subscribers want. Typical ways to block phishing attacks include maintaining software patches and updates, activating backups, and blocking websites known as the epicenter of phishing attacks.

6) Stolen Signature Key at "NHN PAYCO" and "MS"

In Korea, two cases of stealing signature keys, undiscovered until late in December 2022, shook the security industry at the end of the year. The first incident caused a stir after it was revealed that the app signature key of NHN's simple payment service "PAYCO" was leaked on 5th, December, 2022. Another incident was the theft of Microsoft's digital signature. Attackers who stole Microsoft's official digital signatures used them to authenticate malicious drivers, and malicious drivers that were not caught on the surveillance network of security solutions were found to be mobilized for various cyber-attacks. Even if it is malicious code or illegal software, you will pass the security check safely, and the victim will not receive any warning. For this reason, hackers are expected to move intensely to obtain official signature keys in 2023. Therefore, defending companies will no longer simply rely on normal file and normal program approved from the company's internal security system and will consistently monitor. This will lead to interests in 'Zero Trust' and strengthening authentication security.

3-4. 2023 Top 10 Keywords in Cyber Security Industry

2023 Top 10 Keywords in Cyber Security Industry

No.	Top 10 keywords	Definition	contents
1	Artificial Intelligence and Machine Learning	Artificial Intelligence (AI) is a branch of computer science that deals with the creation of intelligent machines that can perform tasks which require human intelligence, such as speech recognition or experiential learning. Machine learning (ML) represents a subfield of AI that trains machines to learn automatically from existing data.	<p>"Increased use of AI and machine learning"</p> <p>Artificial Intelligence (AI) and machine learning (ML) are becoming increasingly popular in the cybersecurity industry for their ability to detect and prevent cyberattacks more effectively than traditional security solutions. As cyber threats become more complex, AI and ML are expected to play an important role in protecting organizations from these threats.</p>
2	Cloud Security	Cloud security refers to a set of policies, technologies, and controls designed to protect cloud-based system, data, and infrastructure from unauthorized access, theft, or damage. Ensuring that data stored in the cloud is secure and compliant with industry and regulatory standards is Cloud security's key mission.	<p>"Increasing adoption of cloud-based security solutions"</p> <p>As more and more organizations accumulate data to the cloud, the need for cloud-based security solutions that can protect critical data and applications in the cloud is increasing.</p>
3	Internet of Things Security	Internet of Things (IoT) security is an action taken to protect IoT devices, systems, and networks from cyber threats and attacks. IoT security includes ensuring confidentiality, integrity, and availability of data transmitted and processed by IoT devices, as well as ensuring that the devices themselves are safe and cannot be compromised by attackers.	<p>"Security based on design"</p> <p>Many organizations are now designing IoT (Internet of Things) devices from a proactive perspective with security in mind from the beginning rather than attempting to add security features later.</p>

4	Quantum Computing and Cryptography	<p>Quantum computing is a type of computing that uses quantum bits or qubits instead of classical bits to perform calculations, and since quantum computers are based on the principle of quantum mechanics, certain types of calculations can be performed much faster than conventional computers. Quantum computing has the potential to revolutionize a wide range of industries, from new drug development to financial modeling, by enabling complex calculations that were currently impossible with conventional computers.</p>	<p>"Consolidate quantum safe encryption" As more and more organizations begin to adopt quantum computing technologies, the need to integrate quantum safe encryption into existing security systems to protect against potential quantum attacks is increasing.</p>
5	Zero-Trust Security Model	<p>Zero-trust security is a network and data security model that assumes all users, devices, and applications in the network are potential threats and that no one can be trusted by default. The zero-trust model is designed to overcome the limitations of existing security models that rely on boundary defenses to protect networks and data.</p>	<p>"Transition to proactive cybersecurity measures" Organizations are designing zero-trust-based organizational security modules from the underlying assumptions of organizational design, and are starting to shift their focus from reactive cybersecurity measures to more proactive measures such as threat tracking, penetration testing, and vulnerability assessment.</p>
6	Cyber Threat Intelligence	<p>Cyber Threat Intelligence (CTI) is an information system that collects potential cyber threats to protect organizations from cyberattacks. This includes gathering, analyzing, and sharing information about new cyber threats, such as malware, phishing campaigns, and other malicious activities.</p>	<p>"A greater emphasis on real-time threat intelligence" In the era of Advanced Persistent Threats (APT), the importance of having real-time threat intelligence to detect and respond to threats when they appear is increasing.</p>

7	Ransomware Defense and Recovery	Ransomware Defense and Recovery refers to a set of processes, technologies, and best practices that your organization uses to protect and recover from ransomware attacks. Ransomware is a type of malware that encrypts an organization's files or systems and requires ransom payments in exchange for decryption keys.	<p>"Use more backups"</p> <p>Regular and secure backups are an essential component of ransomware recovery, and organizations are increasingly implementing secure backup solutions to keep up-to-date copies of their data in the event of a ransomware attack.</p>
8	Supply Chain Security	Supply chain security is the process of protecting an organization's supply chain from potential cyber threats and other risks. A supply chain is a network related to the creation and delivery of products or services, which can include suppliers, manufacturers, distributors, and retailers.	<p>"Concerns about supply chain security"</p> <p>As organizations rely on third-party providers to outsource critical services within their organization, there is a growing concern about information leakage in supply chain security, and there is a growing need to review security partnerships with suppliers to build strong security systems.</p>
9	Data Privacy and Protection	Data privacy and protection refers to a set of policies, procedures and techniques used to protect personal data and to ensure that data is collected, used, and shared in a way that respects personal privacy rights. Personal data includes any information that can be used to identify individuals, such as names, address, email address, or social security numbers.	<p>"Increasing interest in privacy and compliance"</p> <p>As data privacy regulations increase at the government level, organizations are increasingly focused on protecting users' privacy and ensuring compliance with regulatory requirements.</p>
10	Identity and Access Management	ID and Access Management (IAM) refers to a set of policies, procedures, and technologies used to manage and control access to an organization's digital resources and to control who has access to which information resources, and when.	<p>"Emphasize ID and Access Management"</p> <p>As organizations continue to use more devices and applications, the importance of having a robust Access Management (IAM) system to control access to critical data and applications is growing.</p>

SECON & eGISEC 2023 Secretariat

Tel: +82-2-6715-5400

Fax: +82-2-432-5885

Email: global@seconexpo.com