Status of Remote Work Implementation and Security Considerations in Financial Institutions

Joo, Kwangsuk (https://blog.joomoney.net)

v The Financial Services Commission (FSC) has allowed remote work to ensure business continuity for financial institutions during the COVID-19 situation.

v Financial institutions are implementing enhanced security measures to prevent data leaks and other cyber incidents while conducting remote work.

v It is anticipated that remote work will continue even after the COVID-19 pandemic, necessitating ongoing interest and investment to maintain secure environments.

Preventing Cyber Incidents and Allowing Remote Work in Financial Institutions

The FSC allowed financial institutions to adopt remote work in response to the COVID-19 pandemic.

- (~2019) Remote work was not permitted due to physical network separation regulations for preventing cyber incidents.

< Examples of Major Cyber Incidents in Financial Institutions >

Type	Year	Affected Institution	Impact
System Destruction	2011	NH NongHyup Bank	Network paralysis and data deletion
Personal Data Leak	2012 ~2013	KB Card, NH Card, Lotte Card	Over 100 million records leaked
System Paralysis	2013	NH NongHyup Bank, Shinhan Bank	Network paralysis

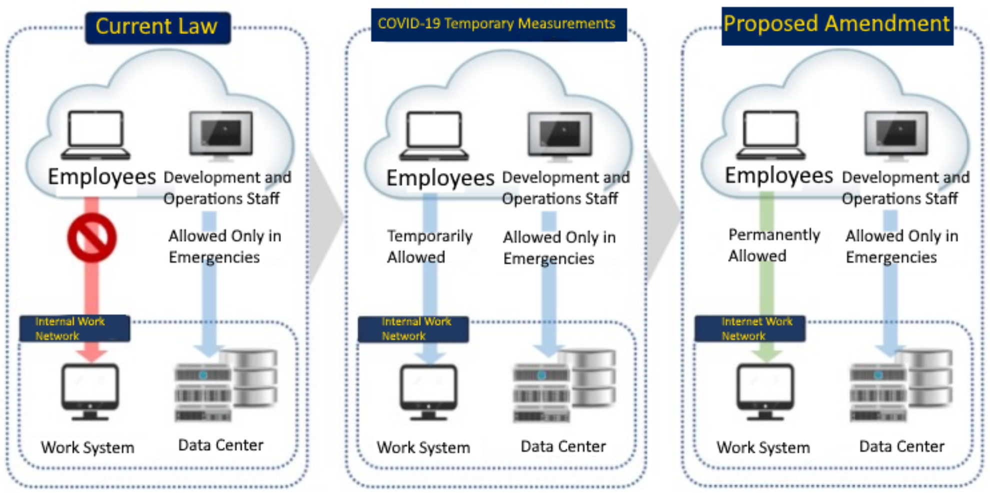
- (2020) Remote work permitted to ensure business continuity during the COVID-19 pandemic

☐ February 2020: FSC permitted remote work for financial employees in response to COVID-19.

☐ May 2020: Revision of National Intelligence Service’s basic security guidelines allowed public institution employees to work remotely.

☐ October 2020: Planned revision of the Enforcement Regulations on Electronic Financial Supervision to allow permanent remote work. (TO BE)

<재택근무 관련 망분리 제도 개선사항>



※ Source : Finanial Supervisory Service(FSS)

Active Implementation of Remote Work in Financial Institutions Amid the Pandemic

Policy Financial Institutions Implementing Remote Work in Line with Non-Face-to-Face Government Policies

- Policy financial institutions such as the Korea Housing Finance Corporation (HF), KDB Industrial Bank, Export-Import Bank, Korea Credit Guarantee Fund, Asset Management Corporation, and Industrial Bank of Korea have taken unprecedented steps to implement extensive remote work.

- HF has applied the same remote work measures for both its headquarters and branches and launched a non-face-to-face application service for housing pensions.

- KDB Industrial Bank is operating a remote work security system in collaboration with the National Intelligence Service and the Financial Services Commission.

- Korea Credit Guarantee Fund stated, “With the expansion of remote work, employees now commute with their work PCs.”

< Examples of Remote Work Implementation in Policy Financial Institutions >

Institution	Implementation Examples
Korea Housing Finance Corporation	Secured dedicated equipment for all employees and implemented rotating remote work; launched a non-face-to-face application service for housing pensions
KDB Industrial Bank	Strengthened remote work security systems in consultation with the National Intelligence Service and the Financial Services Commission
Export-Import Bank	Increased remote work PCs and equipment from 180 to 410 units
Korea Credit Guarantee Fund	Innovated work systems for remote work; reduced density in the workplace
Asset Management Corporation	Implemented remote work for 30% of metropolitan area employees and introduced flexible work arrangements, including staggered working hours for all staff
Industrial Bank of Korea	Implemented rotating remote work for branch employees in addition to headquarters staff

※ Source : Financial News

Expanding Remote Work to Include Not Only Headquarters but Also Branches and Call Centers

- Financial institutions are actively implementing remote work to protect employees and ensure the continuity of operations during the COVID-19 situation

- Some banks have introduced remote work for call centers, focusing on consultations that do not require handling personal information

- The Industrial Bank of Korea, which has many corporate clients, also implemented remote work at its branches, primarily for completing mandatory legal training

< Remote Work Status in the Financial Sector Following the Strengthening of Social Distancing >

Category	Institution	Implementation Method
Banking	Hana Bank	Implemented remote and split work for two weeks starting August 19.
	KB Kookmin Bank	20% of headquarters staff working remotely, 15% working in split shifts
	Shinhan Bank	Mandated a 15% remote work rate for employees
	Woori Bank	Rotational remote work for 1–2 employees per department at headquarters
	Industrial Bank of Korea	One-third of headquarters staff and one-fifth of branch staff working remotely
Insurance	Hanwha Life	Half of the employees working remotely
	Samsung Life, Shinhan Life	Implemented split shifts
	Major non-life insurers initiated remote work (Samsung Fire & Marine, Hyundai Marine & Fire, DB Insurance, Meritz Fire & Marine Insurance, etc.)	
Card Companies	BC Card	Employees working remotely on a rotational basis, with half working remotely at a time
	KB Kookmin Card	All employees working remotely for two days each

※ Source : Money Today

Security Environment Required for Financial Institutions to Implement Remote Work

Four Core Information Security Technologies to Prevent Hacking or Data Breaches

1. Virtual Private Network (VPN)

□ Establishes a virtual dedicated line connecting homes to the internal network of financial institutions.

□ Blocks internet access, creating a dedicated connection to the internal network, reducing risks of remote control by hackers, data tampering, and leakage of communication content

2. Virtual Desktop Infrastructure (VDI)

□ Prevents file export and malware infection through the use of virtual desktops

□ Data processing is performed on a virtual PC within the financial institution's internal network, while the home PC functions only as an input/output device for keyboard, mouse, and display

□ Ensures safety from data leaks or infections as no data is stored or transferred on the home PC

3. Document Encryption (DRM)

□ Ensures that even if document files are leaked, they cannot be accessed externally

□ Encrypts documents so that their content remains unreadable unless connected to the server

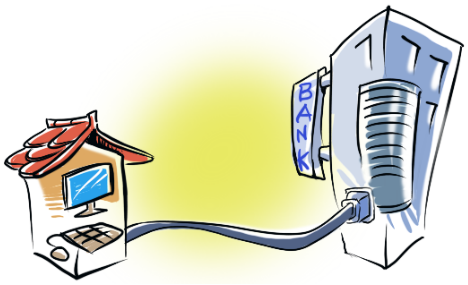
4. Two-Factor Authentication

□ Blocks unauthorized access by implementing enhanced authentication systems alongside ID/password login systems

□ The most widely used two-factor authentication system is OTP (One-Time Password), which verifies ownership by requiring a single-use password

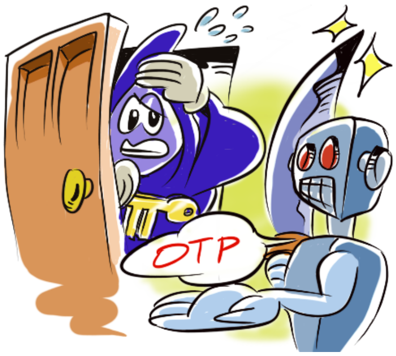
1. VPN: Virtual Private Network

2. VDI: Virtual Desktop Infrastructure



3. DRM: Document Encryption

4. Two-Factor Authentication: OTP, etc



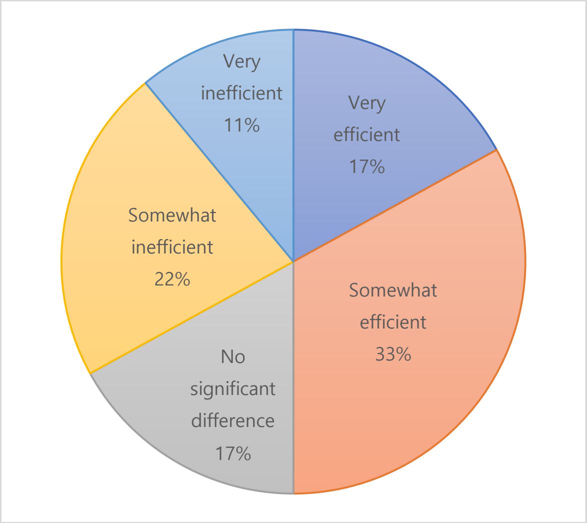
Remote Work Becomes a Routine Work Format

- Remote work is being recognized as effective and sustainable, supported by various surveys:

- According to a survey by MK Economy, 66.8% of respondents stated that remote work is "as efficient as or more efficient than before," with the main reason for increased efficiency being "reduced time wasted on commuting" (69.3%)

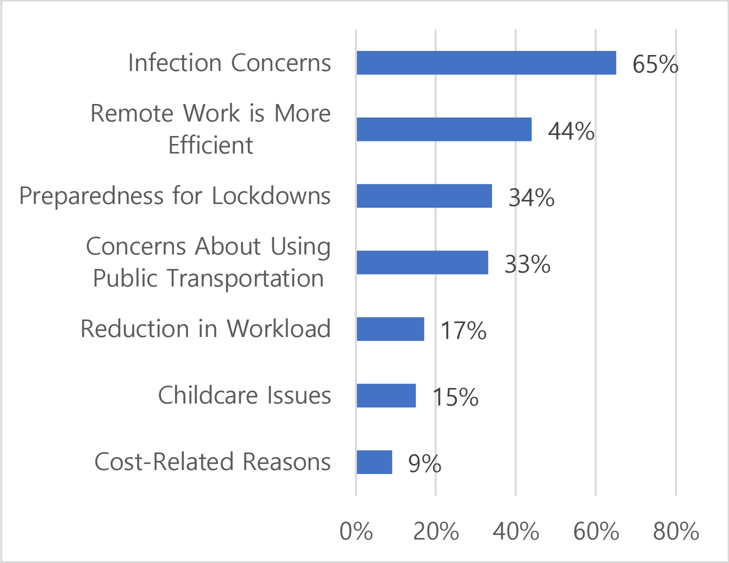
- A survey by the Institute of Directors (IoD) in the UK revealed that 74% of respondents plan to expand remote work. The main reasons companies are reducing office usage are "infection concerns" (65%) and "remote work being more effective" (44%)

< Efficiency of Remote Work >



※ Source : MK Economy

< Reasons for Reducing Office Usage >



※ Source : Institute of Directors (IoD), UK

Remote Work Becomes Routine and Must Be Operated Securely with Attention to Security

- To prevent cyber incidents, remote workers must adhere to security guidelines:

- Cyberattacks targeting remote workers could potentially breach the internal networks of institutions with segregated systems

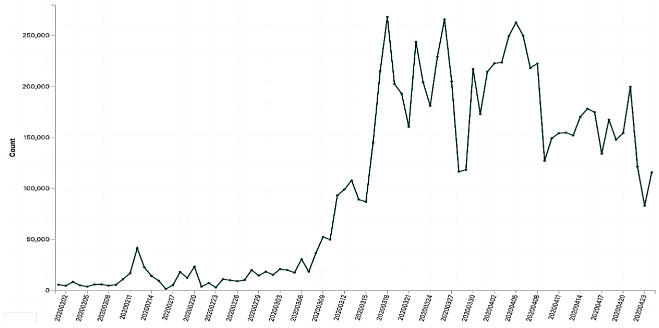
- The Korea Internet & Security Agency (KISA) has published “Six Essential Security Practices for Remote Work.”

- Companies reducing budgets due to COVID-19 must continue investing in security:

- The Financial Security Institute reported that "1% of COVID-19-related emails are suspected to be malicious," and threats of breaches are increasing

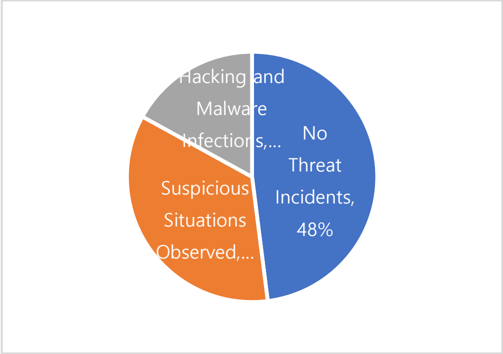
- Security measures, once limited to internal environments, must be expanded to external environments to ensure a safe remote work setup

< Increase in Spam Emails (February–April 2020) >



※ Source : RiskIQ

< Examples of Cyber Threats During Remote Work >



※ Source : Korea Internet & Security Agency (KISA)