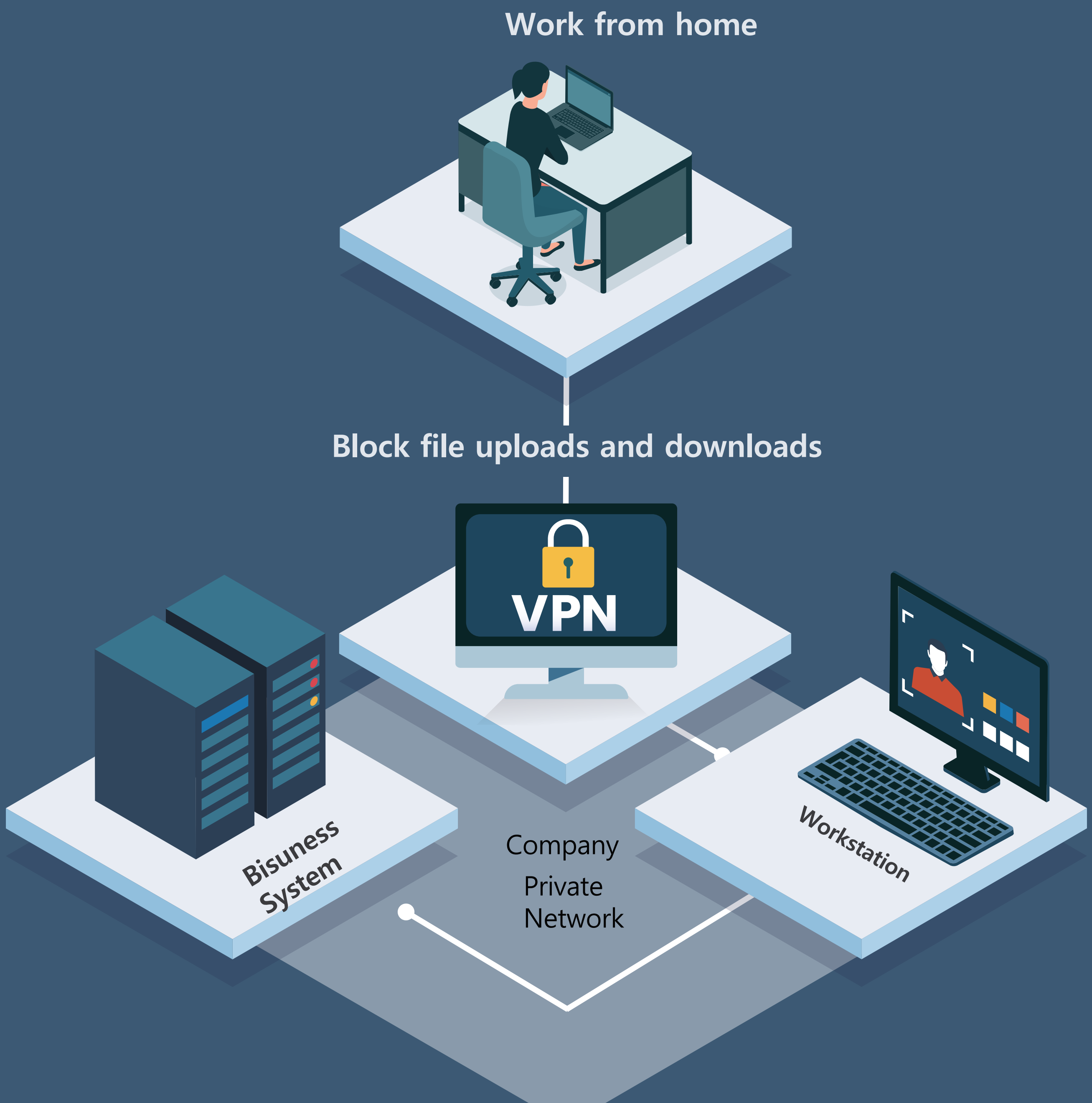
Solution for optimizing working from home

Real Time Desktop



01 Work at home environment requirements

- **Concerns about working from home**
  (Many check items required when configuring a telecommuting environment)

Security

Physical control of external
terminals Malware infection /
network infringement threat
of remote access of reso

Apply process

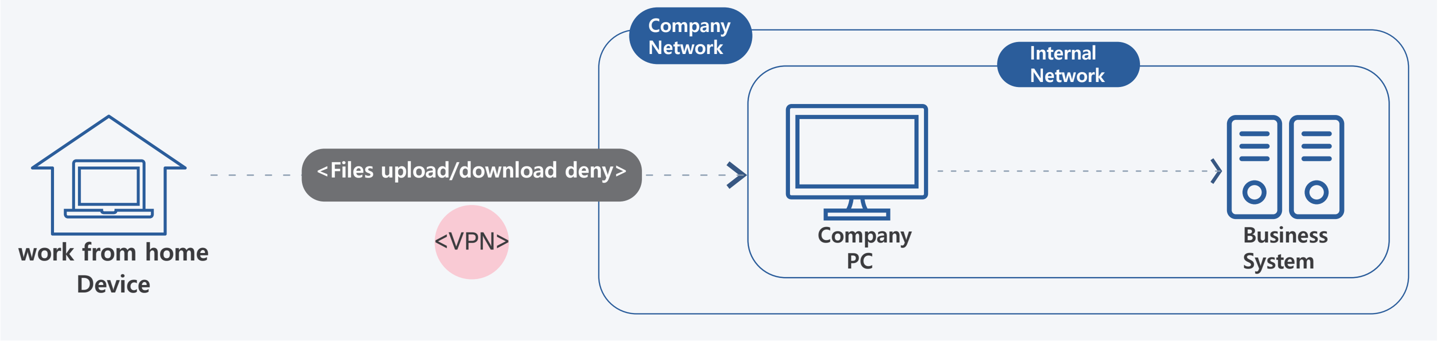
Environmental configuration time
Understand the essential requirements
Budget execution / maintenance,
management, and tonicity

Usage performance

Performance of business equipment
Limited setting for each group that
minimizes discomfort in the company /
home environment

- **FSI(FINANCIAL SECURITY INSTITUTE) Types of telecommuting**
  http://www.fsec.or.kr/fseceng/index.do

1. Outer staff working from home –
   Applies only to all corporate business terminals, so it depends on the location and does not apply.
2. System Developer working from home -
   If the computer room information system is directly connected and opened, remote contact cannot be permitted.
3. Important terminal remote access–
   mportant terminals are prohibited from being carried out to the outside, and cannot work from home by contacting an external device via the Internet



<Example of FSI Remote Desktop program permission method>

• Remote Acess security compliance of FSI

Amendments

01 Allowing employees to work from home at any time through remote contact by clearly stating the exceptions to network separation

02 Build and clarify step-by-step security so that you can build and operate a telecommuting infrastructure at the same level of security as the department business network.

03 Target : Financial industry staff / Call center, etc.

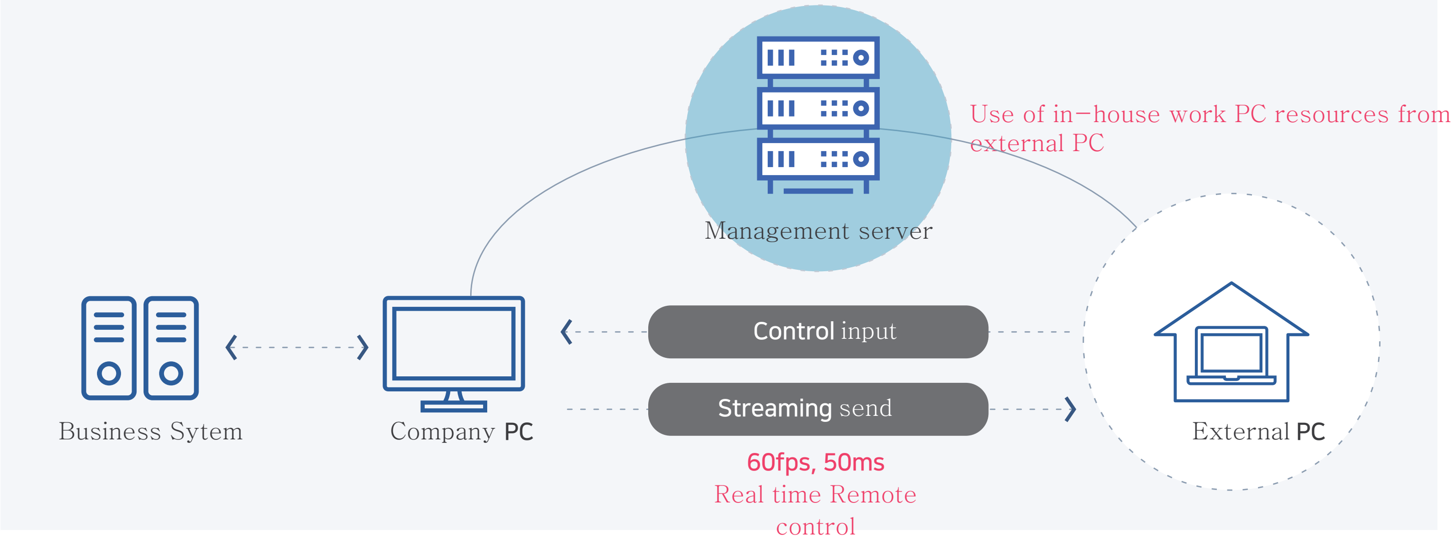
Remote Acess security checklist

Allow connections only with minimal IP and port	Allow external terminals to access only internal systems required for business
Save remote access logs	Save remote access user information/date/ access system information logs
Blocking unauthorized IP access	Restrict unauthorized IP so that only external terminals registered (approved) in advance access
Multi–Factorauthentication	2–Factor authentication for remote access
Authentication failed/ blocked more than a certain number of times	Block access when authentication fails more than a certain number of times –> Identity verification
Connection valid time setting	Blocking the connection if there is no business processing for a certain period of time (e.g.: 15 minutes) after remote access

02 Real Time Desktop Function introduction

Real Time Desktop Diagram

In the form of streaming the internal PC screen to the external PC screen as it is by transmitting only input/command from the external PC to the internal PC, the company working environment is provided as it is when working from home.



Real Time Desktop – Key Message

Security

- Documents cannot be taken out of the office by working from home
- In-house security policy can be applied to work from home as it is

Convenience

- Minimizes the user's sense of disparity due to security by providing the existing desktop environment as it is
- Managed by simple "agent" installation

Economics

- Reduced introduction cost as existing PCs can be used as they are without the need to purchase additional software and hardware
- Available as a perpetual license

Easy to manage

- Easy local user and policy control by providing "manager portal" for administrators
- Security watermark, screen capture prevention, forgery and alteration impossible function can be set

The fastest telecommuting solution (check product performance video)

High-performance engine video without delay even when using 3D games remotely

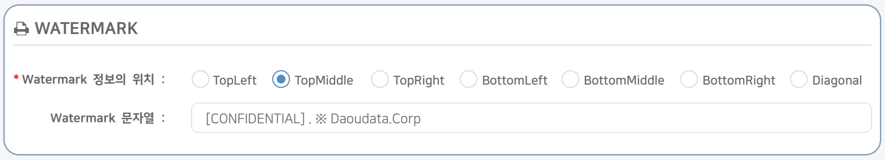
Even between different internet lines CAD remote use video without feeling of foreignness

03

Main function

Watermark

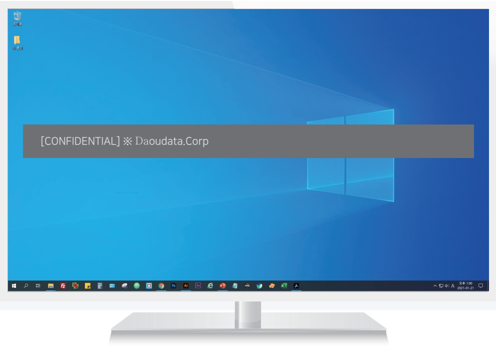
Provides a watermark function and basically displays it on confidential documents and materials inside the company.



WATERMARK

* Watermark 정보의 위치 : ○ TopLeft ● TopMiddle ○ TopRight ○ BottomLeft ○ BottomMiddle ○ BottomRight ○ Diagonal

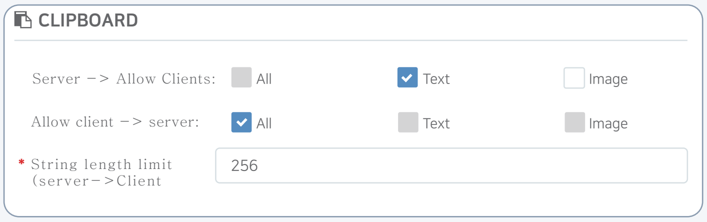
Watermark 문자열 : [CONFIDENTIAL] . ※ Daoudata.Corp



[CONFIDENTIAL] ※ Daoudata.Corp

Clipboard control

Clipboard prevention function is provided, and server ↔ client allow/block
Policy can be set to control the file copy "extension" by analyzing the data size and type in detail

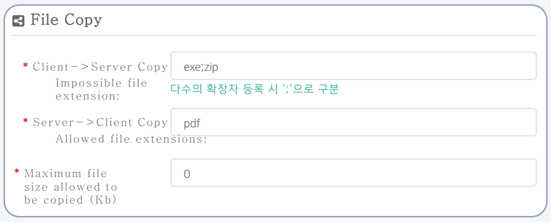


CLIPBOARD

Server −> Allow Clients: □ All ☑ Text □ Image

Allow client −> server: ☑ All □ Text □ Image

* String length limit (server−>Client: 256



File Copy

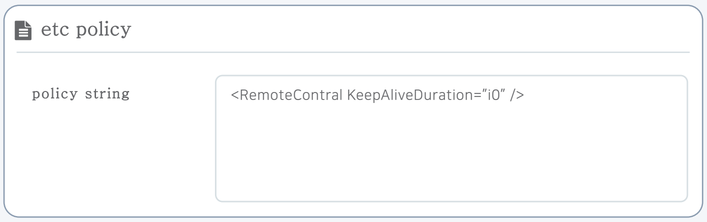
* Client−>Server Copy Impossible file extension: exe;zip
다수의 확장자 등록 시 ';'으로 구분

* Server−>Client Copy Allowed file extensions: pdf

* Maximum file size allowed to be copied (Kb): 0

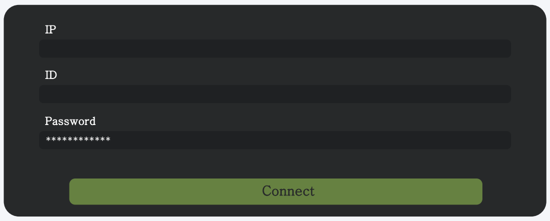
Session validity limit

Session validity limit time can be set due to the absence of home workers, etc.
*If you do not enter a specific time (5 minutes/10 minutes) with "Keepalive" setting, the session is out



etc policy

policy string <RemoteContral KeepAliveDuration="i0" />



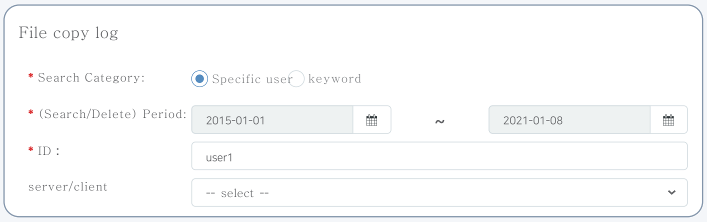
IP

ID

Password: ************

File copy log

Viewing server ↔ user−to−user file copy log by period



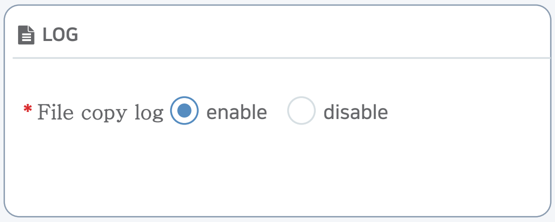
File copy log

* Search Category: ● Specific user ○ keyword

* (Search/Delete) Period: 2015-01-01 ~ 2021-01-08

* ID : user1

server/client: -- select --

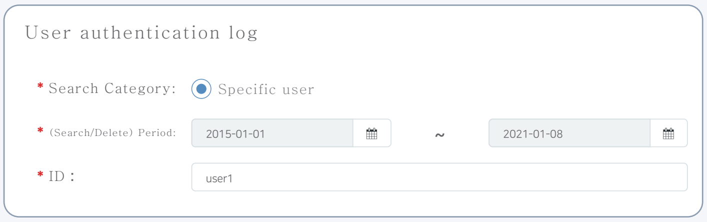


LOG

* File copy log ● enable ○ disable

User authentication log

User login access log results (connection/failure) can be checked by period

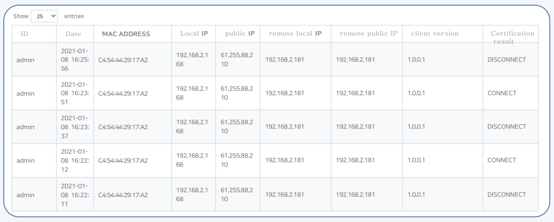


User authentication log

* Search Category: ● Specific user

* (Search/Delete) Period: 2015-01-01 ~ 2021-01-08

* ID : user1



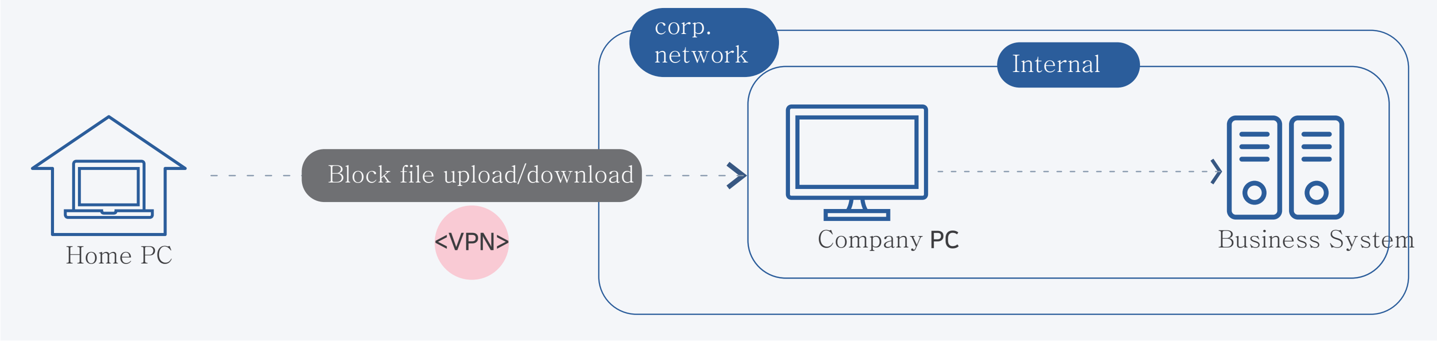
Show 25 entries

ID	Date	MAC ADDRESS	Local IP	public IP	remote local IP	remote public IP	client version	Certification result
admin	2021-01-08 16:25:56	C4:54:44:29:17:A2	192.168.2.168	61.255.88.210	192.168.2.181	192.168.2.181	1.0.0.1	DISCONNECT
admin	2021-01-08 16:23:51	C4:54:44:29:17:A2	192.168.2.168	61.255.88.210	192.168.2.181	192.168.2.181	1.0.0.1	CONNECT
admin	2021-01-08 16:23:37	C4:54:44:29:17:A2	192.168.2.168	61.255.88.210	192.168.2.181	192.168.2.181	1.0.0.1	DISCONNECT
admin	2021-01-08 16:22:12	C4:54:44:29:17:A2	192.168.2.168	61.255.88.210	192.168.2.181	192.168.2.181	1.0.0.1	CONNECT
admin	2021-01-08 16:22:11	C4:54:44:29:17:A2	192.168.2.168	61.255.88.210	192.168.2.181	192.168.2.181	1.0.0.1	DISCONNECT

04

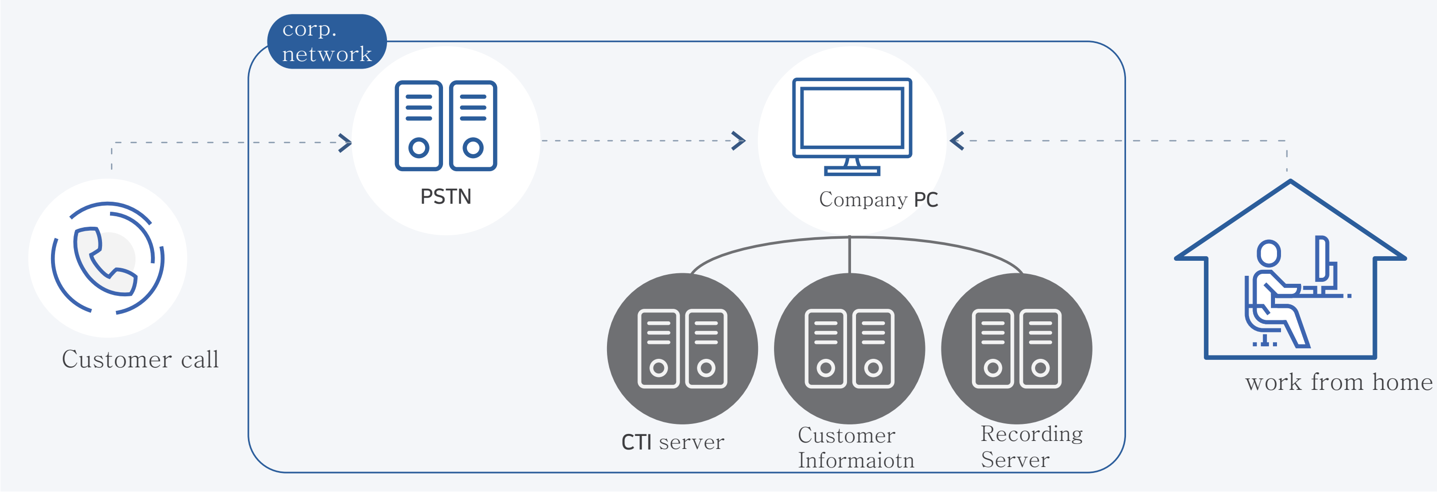
Case Study

- Financial company introduction scenario
  (indirect access to in–house PC)



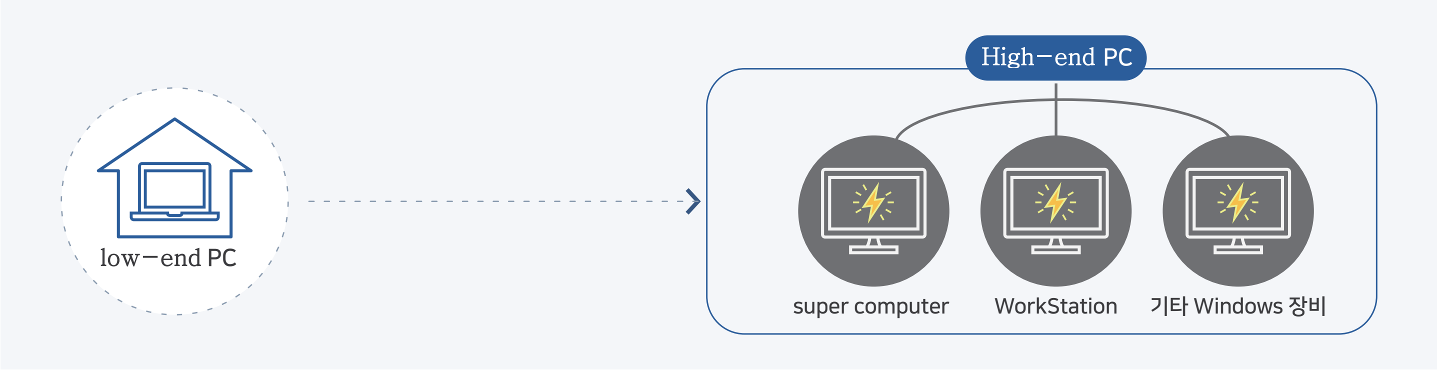
- In–house equipment/environment as it is
  (Call Center's telecommuting environment)

1. Without additional system construction, in–house call center system environment can be used as it is in a telecommuting environment
2. Data export control / prevention of information leakage when working from home by setting the watermark function



- Remote use of high–end PC

Remote access to high–end equipment (super computer / WorkStation / other Windows equipment) in the company even on a low–end PC working from home to use in–house PC resources as it is.



(주)다우데이타
주소 : 서울시 마포구 독막로311 재화스퀘어 11층
홈페이지 : http://members.daoudata.co.kr
대표번호 : 02 - 3410 - 5100