Ongoing Innovation

■ CASE STUDY ■

Open House Group Co., Ltd.

Connecting to a development environment with Zero Trust Access Achieving a secure and convenient environment as an alternative to VDI

Open House Group Co., Ltd., a comprehensive real estate company, has integrated IIJ Safous ZTA into the workplace for external development partners to whom the Information Systems Department outsources development projects. Previously, those in charge of configuring the VPN and VDI environment were responsible for doing so every time, creating a burden. Besides requiring the installation of client software, VDI had poor performance. Open House Group was able to overcome this difficulty by utilizing IIJ Safous ZTA's secure remote access and flexible access control capabilities. The performance of the work environment improved, and the number of man-hours required to set up the environment also decreased dramatically.

Challenges before the migration

A highly convenient and secure work environment was essential

— What is your company's goal in developing business?

Mr. Kosei Arai, Open House Group Co., Ltd.: Open House Group Co., Ltd. changed its trade name from its predecessor, Open House Co., Ltd. and made a new start as a holding company in January 2022. The operating companies within the group mainly operate in urban areas such as Kanto, Nagoya, Kansai, Fukuoka, and are launching businesses such as newly built detached houses sales, real estate management, condominium business, and real estate investment, providing "valuable real estate" with a customer-first approach.

Mr. Kosei Arai

Section Chief, Infrastructure Section
Infrastructure Group, Information Systems Department
Open House Group Co., Ltd.

We are also actively encouraging M&A to drive further expansion. Along with this, the number of employees and locations continues to grow. To achieve synergies as quickly as possible, we are integrating group networks while preserving security.

— Are the Group's security measures based on zero trust?

Mr. Arai: We believe that zero trust security is essential because our sales teams frequently use internal systems and the cloud while out of the office.

However, putting focus on security should not come at the expense of convenience. We collaborate closely with key people in business departments to listen to their needs and discuss solutions to ensure security while maintaining convenience, achieving balanced zero trust security.

— I heard that the business environment for external development partners was run on virtual desktop infrastructure (VDI), is this also because the balance of security and convenience was considered?

Mr. Hayato Masuzawa, Open House Group Co., Ltd.: We provided VDI as a work environment because our external development partners frequently work remotely from outside the office. Since we primarily create systems and applications internally, we rely on external development partners for development support and operational testing. With VDI, no data remains on the terminal side, lowering the risk of information leakage.

The VDI environment sets privileges for each user and limits the systems they can access. Furthermore, a firewall limited communication to certain ports.

Mr. Hayato Masuzawa

Infrastructure Section
Infrastructure Group, Information Systems Department
Open House Group Co., Ltd.

— On the other hand, it appears that there were some challenges with the VDI environment.

Mr. Masuzawa: This approach required downloading VDI client software, installing it on a PC, and accessing it using that client software. It was time-consuming and we also had performance concerns. Some also mentioned "not being able to start work immediately" and having a "lengthy response wait time."

Mr. Arai: Preparing in advance was equally challenging. When we outsource work to external development partners, we provide them with a VPN and VDI environment for remote access. However, each time we do so, we must also set up a VPN for each person and open a firewall port.

Although access is restricted based on privileges, it is difficult to monitor everything. The risk of being able to access internal systems and data that are unrelated to business operations could not be dismissed. Continuing to use the system in its current state was problematic from both a security and governance standpoint.

Why Open House Group chose IIJ Safous ZTA

Realized a work atmosphere in accordance with zero trust policies with Safous

— IIJ Safous ZTA was introduced to resolve the issue. What do you like about it?

Mr. Arai: In principle, we handle the infrastructure and security components internally. However, IIJ helps with network building and operation at each of our locations, as well as implementing certain IT policies. When we inquired about a secure remote access environment for international locations, we received a suggestion from IIJ about Safous ZTA.

Safous can be used by simply installing a device called App Gateway behind the firewall. In concept, users connect to Safous POP via the Internet using a web browser

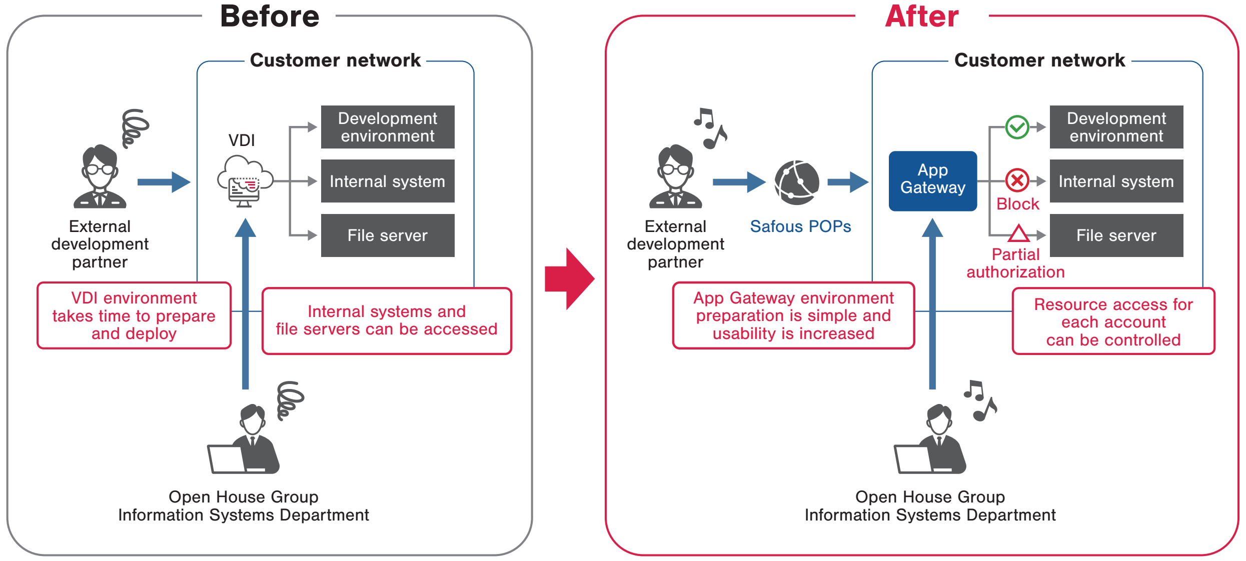
■ User profile ■

Open House Group Co., Ltd.

Head office:
2-7-2 Marunouchi, Chiyoda-ku, Tokyo
Founded: September 1997
Capital: JPY 20,131,480,000

Open House Group Co., Ltd. is a holding corporation that handles the operations of its subsidiary enterprises, including Open House. Open House engages in real estate sales and brokerage business, newly built detached house sales business, and condominium development businesses, etc. Among these, the newly built detached house sales business is the company's core business. The company provides total support for home construction in prime areas, from land purchase to planning, design, and construction.
https://openhouse-group.co.jp/en/

System overview


Before
Customer network
VDI
Development environment
Internal system
File server
External development partner
VDI environment takes time to prepare and deploy
Internal systems and file servers can be accessed
Open House Group Information Systems Department
After
Customer network
Safous POPs
App Gateway
Development environment
Internal system
File server
Block
Partial authorization
External development partner
App Gateway environment preparation is simple and usability is increased
Resource access for each account can be controlled
Open House Group Information Systems Department

and a TLS tunnel is established to give secure private access to their own environment. Multi-factor authentication and fine-grained access restrictions allow for secure access to internal resources. Access logs and PC operation history can also be saved.

This led us to think that we could create a secure alternative to the VDI environment for external development partners in line with our zero trust security policy, which had previously been an issue.

— Did your company propose the idea of employing it as an alternative to a VDI environment?

Mr. Arai: Yes, that is correct. We use Zscaler as one of our zero trust security solutions, but our prior VDI environment could not interface with Zscaler due to technical limitations. This was also one of the reasons why I was concerned about security.

In that sense, by integrating IIJ Safous ZTA with Zscaler, the system can operate within a zero trust security policy. Furthermore, it is simple to set up and easy for users to use. I felt there was no better option than to adopt this integration.

Mr. Masuzawa: We did the testing across three months, beginning in July 2023.

— What points did you concentrate on throughout your testing?

Mr. Masuzawa: We primarily built and tested App Gateway on our side. Tests included usability, performance, and multi-factor authentication functionality. In addition to ID/password authentication, multi-factor authentication can include SMS, QR code, and other methods. During the tests, IIJ provided support such as changing the user timeout interval access during use.

As a result of our testing, we believed it could be used as a VDI and officially launched it in October 2023.

What IIJ Safous ZTA achieved

Improved security performance and usability, decreased time needed for environment preparation

— Fine-grained access restrictions are essential for security. What kind of policy does IIJ Safous ZTA operate under?

Mr. Arai: There are controls at the user, protocol, and application levels in line with our objectives, creating an environment in which external development partners could only access authorized resources. Access to systems unrelated to operations performed by external development partners is prohibited and file servers are restricted, allowing only limited access to certain resources.

— What benefits have you experienced?

Mr. Masuzawa: We have replaced VDI with Safous as the remote access environment for external development partners. Until we did that, creating a VDI environment was a massive burden. We had to open ports on the firewall and establish a VPN for the VDI environment and access line. After that, we also had to test the system to make sure it was operating correctly.

It used to take around half a day to prepare the VDI for use. Now accounts can be created by setting up an App Gateway server and linking users. The work can be done in less than an hour.

Not only has the workload been greatly reduced, but the work environment can now be deployed in a short period of time, allowing external development partners to begin work immediately.

Mr. Arai: **I also like that Safous can be used without making any changes to the existing systems. We can continue to operate without changing zero trust security settings and policies, including SASE.**

Access logs and PC operation history are both saved, so even if a security issue arises due to internal fraud or carelessness, an audit trail is always available. Having a system like this in place will also improve the effectiveness of discouraging internal misconduct.

— What are the reactions of users who are now using IIJ Safous ZTA?

Mr. Masuzawa: We received positive feedback because it's smooth and easy to work with. There is no need to install client software like before and it can be viewed using a web browser. People also like that it doesn't take a lot of effort to set up.

Mr. Arai: Previously, even if we provided a VDI, there would be problems such as not being able to access it. However, since the introduction of Safous, there have been no reports of problems from users. Both performance and stability have increased.

— Please tell us about your future plans.

Mr. Arai: Our current challenges include network optimization and the advancement of zero trust security in conjunction with organizational integration at all of our locations.

Security precautions are in place not only to protect our company, but also to safeguard sensitive customer information. IIJ offers a wide range of network services and has advanced technical skills. We look forward to receiving more helpful suggestions and support for network efficiency and zero trust security advancements.

What we offer

■ **IIJ Safous ZTA**

[Inquiries]
Internet Initiative, Inc.
TEL: +81-3-5205-4466 E-mail: info@iij.ad.jp Website: https://www.iij.ad.jp/en/

• This article is based on an interview given in April 2024. The data, organization names, titles, etc. in the article were correct as of the date of the interview.
• Company names and service names are registered trademarks or trademarks of their respective companies.

Internet Initiative Japan