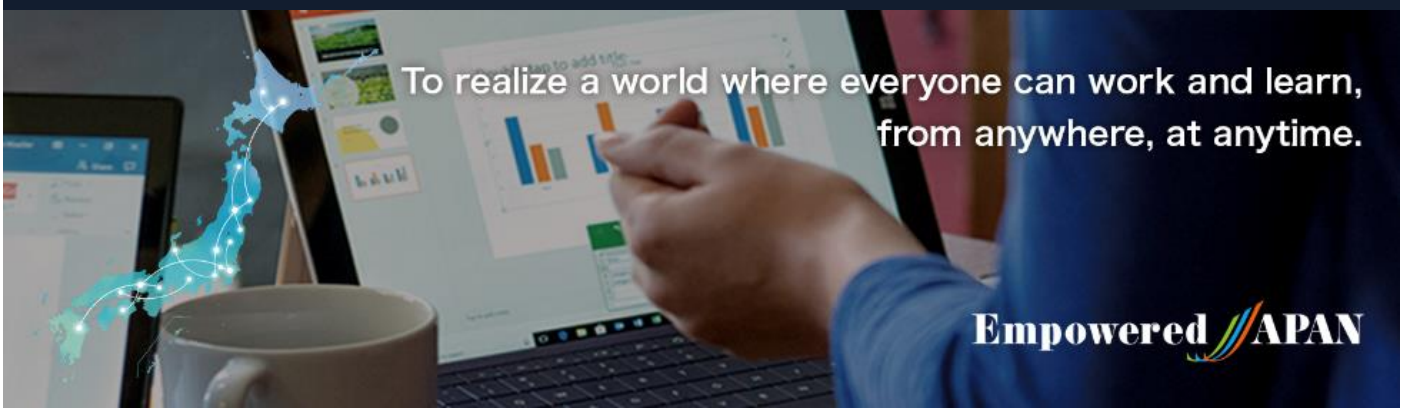
Empowered JAPAN Webinar Report



Empowered JAPAN Executive Steering Committee was established in 2018, “To realize a world where everyone can work and learn, from anywhere, at anytime.” To promote the true value of workstyle innovation including telework, the committee has been coordinating symposiums in both Tokyo and regional cities. And in collaboration with various local governments, Microsoft, and partners, the committee has been serving as an advisor to provide telework training for both corporate and individuals. In response to the spread of infection of corona virus (COVID-19) and the government announcement on February 25, 2020, which included the request to citizens to telework, the steering committee made the decision to launch a series of free webinars starting from March 17, 2020, to provide practical information for individuals and organizations across the nation, to telework and/or practice online education.

Category：IT tools and environment

Date：March, 31, 2020

Speaker：Makoto Yoshida
Trend Micro Incorporated
Enterprise Solutions Department,
Business Marketing Headquarters
Senior Manager

Starting with a major domestic SI, has been active as a product manager of high-end Unix servers and as a product expert working with foreign-affiliated vendors to spread system infrastructure throughout Japan; for example, providing OEM provision of mid-range storage for corporations.
For more than 10 years since joining Trend Micro Incorporated, has worked as a product manager in the field of gateway security. Was also involved in launching cloud-based security in addition to on-premise security.

Getting Started with Telework
～The Concerning First Step of Security～

One of the obstructions to promote teleworking is security. Many people are concerned about information leakage when it comes to remotely working from home or a cafe, etc. and hesitate to fully adopt teleworking.

What are the points for companies which are considering adopting teleworking and safely carry out work operation? Mr. Atsushi Yoshida, Senior Manager, Business Marketing Department, Trend Micro Inc. explained the vital points. Mr. Yoshida has years of experience as an IT infrastructure product expert and is enthusiastically working to promote and enlighten security measures.

"There are three major external security risks in teleworking: unauthorized access, theft/lost/peeping, and malware (virus) infection. Management must address measures against these risks." (Mr. Yoshida)

First, the fundamental principle to prevent unauthorized external access is thorough management of ID and password. "Some people stick a note with a password on their computer in case they forget, but this is the same as leaving your house key in front of the door. Also, try to complicate a password by combining numbers and letters." (Mr. Yoshida)

Mr. Yoshida pointed out that securing with an ID and password is not enough to protect security information from intruders who attempt unauthorized access using various means. He also suggested using multi-factor authentication that requires additional security information such as knowledge (password, date of birth, etc.), possession (smartphone type, etc.), and biological (fingerprint, etc.) for external access. "For example, entering date of birth (knowledge information) after a password is just multi-step authentication using only knowledge information, and not multi-factor. In order to strengthen security, multi-factor authentication by entering a security code, which is sent to the user's smartphone after entering a password, is essential for teleworking." (Mr. Yoshida)

Next, what are the points of measures against malware viruses? Malware viruses usually come through USB sticks, websites, and emails. In a vicious case, not only does the user's device become locked instantly and will not be able to work, but also faces the risk of important information being stolen.

The first step to prevent viruses is to keep the OS, apps, and browsers up to date, and install anti-malware software. "We recommend setting your device to automatically install updates when the latest version is released." (Mr. Yoshida)

For additional measures against virus infection, it is necessary to only supply a USB that supports antivirus within the company, prohibit the installation of apps unrelated to work, and list cloud services that can be used and types of data that can be stored in the cloud.

According to Mr. Yoshida, the worst thing about a virus attack through a website is a "drive-by download." This refers to an attack aiming for the vulnerabilities of legitimate websites, and malicious programs are unintentionally downloaded while the user is browsing. Of course, there are measures against this type of attack. Combining both the filter function that selects websites by category and reputation function that selects websites by evaluating the risk level helps you achieve a work environment where only safe and appropriate websites can be viewed.

In addition, over 90% of intrusion methods used by attackers is emails (based on a survey in 2019 by Trend Micro Inc.). Thus, implementing advanced security such as sandbox technology as a countermeasure at the company side and having preventive knowledge against spoofed emails at the teleworker side are crucial. "Nowadays, Japanese sentences in spoofed emails have improved and it is harder to identify whether they are legitimate or illegitimate. The user must always be on the alert and check the email address of the sender by placing the cursor over, etc." (Mr. Yoshida)

Finally, here is some advice on how to prevent theft, loss, and peeping. "When devices are used outside of the company, the HDD (hard disk) should be encrypted in case of loss or theft. To prevent peeping, use a privacy screen protector," said Mr. Yoshida. Also, turn on the Audit Log setting which allows you to trace the device in the event of an accident.

In order for the rules to be effective as described above and provided by management, it is essential for the teleworkers to comply.

When working from home, some teleworkers may use a Wi-Fi (router). In that case, "be sure to change the ID and password from the default settings for increased security." (Mr. Yoshida) When connecting to the network outside of home, teleworkers must use a mobile router provided by the company, and if it is not available, choose public Wi-Fi with high reliability. It is also important to display behavior models on the teleworker side, such as disabling the automated connection to Internet and avoid sending confidential information when outside. If you want to know more about security measures that change daily, we recommend the website iS702 which has a collection of the latest information.

"Rule, people, and technology are the elements that determine security. If these three elements mesh with each other like cogwheels, a stronger and safer environment can be realized," said Mr. Yoshida. How fast these cogwheels spin is up to understanding and participation of management.