高品質インターネット　1－6
（2001. 11. 21）

Security Issues on Home Teleworking over Internet

Kenji Rikitake, Takahiro Kikuchi, Hiroshi Nagata, Tatsuaki Hamai
and Tohru Asami

High Quality Internet Project, KDDI R&D Laboratories Inc.
2-1-15 Ohara, Kamifukuoka City, Saitama 356-8502 JAPAN / phone: +81 492 78 7303
email: kenji@kddilabs.jp

Teleworking from home has become a major alternative workstyle for skilled workers such as software engineers and content creators. Recent deployment of inexpensive access methods to Internet such as ADSL (Asynchronous Digital Subscriber Link) and Cable TV has given sufficient bandwidth for home-based teleworkers to perform most of their tasks from home. On the other hand, Internet has become a very hostile environment for unprotected devices, and home equipments are now major victims of security attacks. In this paper, we first analyze the fundamental Internet security requirements of integrating home teleworking systems into a corporate network. We also address some of the notable technical, social and policy issues specific to teleworking over Internet, and propose solutions to these issues for integrating teleworkers from home as a viable corporate unit of workforce.

Keywords: Internet, Security, Teleworking

インターネットを通じた
在宅テレワークでのセキュリティ問題

力武 健次　菊地 高広　永田 宏　濱井 龍明　浅見 徹

株式会社 KDDI 研究所 高信頼 IP ネットワーク技術プロジェクト
〒356-8502 埼玉県上福岡市大原 2-1-15 Tel: 0492-78-7303
email: kenji@kddilabs.jp

在宅テレワーク (遠隔勤務) はソフトウェア技術者やコンテンツ制作者など技能労働者にとって有力な勤務形態の一つとなった。近年 ADSL(非対称デジタル加入者網) やケーブルテレビなどインターネットへの安価なアクセス手段の普及により、在宅テレワーク勤務者は大部分の業務を家から行うのに十分な帯域を得られるようになった。しかしその一方で、インターネットは無防備な装置にとって非常に危険な環境となり、家庭の機器はセキュリティ攻撃の主な被害者となっている。本論文では、まず在宅テレワーク用の情報システムを企業ネットワークへ統合するための基本的なインターネットセキュリティ上の要請について分析する。また、インターネット上でのテレワークに関するいくつかの技術的、社会的そして制度的な問題について論じるとともに、これらの問題の解決策を示し、在宅テレワーク従事者を企業にとって有力な労働力として統合するための方策を提案する。

キーワード: インターネット、セキュリティ、テレワーク

1 Introduction

Performing business tasks using Internet for exchanging information between home and office has become popular, as the cost of Internet connectivity rapidly decreases. In this paper we call this kind of home-based working style as *home teleworking*. We also define the word *teleworking* to meet the following conditions [10]:

1. Teleworking means performing business tasks as well as non-teleworking workers, including but not limited to, writing documents, developing software or hardware, managing Internet systems of remote sites, etc.;
2. Teleworking employees can decide where to work by themselves, under agreement with the employer if not self-employed;
3. Teleworking hours are considered as the standard working hours and treated the same as the non-teleworkers (if the working hours are not restricted, this condition is not applicable).

Working from home [14] is a common workstyle, especially in the United States of America or Canada where the majority of workforce is self-employed. And recently in Japan, even though the majority of workforce is organizational employees, more and more people choose home teleworking instead of commuting to the office, by the following social and practical reasons:

- The average hours of bidirectional commuting per day continuously increase as more people concentrate to the urban area. In Tokyo and vicinity, spending *four hours per each day for commuting* is considered *not exceptional*. Many people feel this unacceptable and choose teleworking as an alternative.
- Taking care of elderly people, children, and family members with disabilities requires staying home. Many employers do not want to lose skilled employees just because of this requirement, and start to offer teleworking as a way to keep them employed.
- The economic resession since 1990s forces people to become self-employed. Recent fall of Internet connectivity cost lowers the barrier of starting up business by home teleworking.
- As the economic environment rapidly changes, organizations and corporations should be able to follow up and change themselves by dynamically reorganizing internal and external workforces. Higa [1] defines an organization meets this requirement as *agile, aggressive, and autonomous (AAA)*, and he claims teleworking is a critical tool to create an AAA organization.

The Internet systems for teleworking, however, are still premature for business, especially regarding the security issues. Several models of teleworking application have been proposed among the teleworking research communities [11] [6], but very few of them have emphasized the importance of integrating security policies and technologies into the telecommuting environments. Recently home networks have been targets of malicious attacks since the always-on connectivities such as ADSL and Cable TV have been gaining popularity among home network users. Those networks are considered notably vulnerable to many known network attacks [3]. Connecting home networks without implementing adequate precautional security measures to an organizational network results in adding vulnerabilities to the entire working environment of the organization.

Since April 2001, we connect the home network of one of the authors Rikitake, in Toyonaka City, Osaka, Japan as a home teleworking branch of our corporate computing environment [7]. We also connect our Kyoto Branch office as an office teleworking branch [8]. The two branches are connected to our corporate headquarter network in Kamifukuoka City, Saitama, Japan. We needed to establish these teleworking systems to reduce document-processing overhead between Toyonaka/Kyoto and Kamifukuoka, and to perform a field test of teleworking to evaluate how it affects to the productivity and quality of work results.

In this paper, we first analyze some aspects of security requirement for home telecommuting regarding to our experience. We also review the results of the technical experiments performed at Rikitake's home teleworking environment, and address the issues on reinforcing security of home networks and the teleworking systems.

2 Organizational Security Policies and Teleworking

Each organization has its own security policies and procedures to consistently handle sensitive information such as personal records or trade secrets. Every member of the organization should know and act as the security policy directs. The teleworkers are no exception. They need to be aware of teleworking-specific issues, as well as the general security enforcement procedures, to avoid imposing vulnerabilities to the entire organizational structure. Teleworking systems should maintain adequate security compliance. Otherwise, the systems may become the weakest points of failure on security incidents. Teleworkers involving in an organizational work should be well-educated to comply with the security standard [9].

The organizational security policies include the computer security issues. The core issues have two major parts: how to handle the accessibility of information, and defining who has or does not have the rights to access. Sensitive information may exist in anywhere in any form; a piece of paper, a flash-memory card, a floppy disk, a CD-R disc, or in a hard disk. The accessibility to the information inside these media should be well-defined in the organizational security policies.

Teleworkers usually work outside the organizational facilities. Access to the information which should not be placed outside the organizational facilities has to be minimized to the teleworkers to prevent the information leakage. Business tasks which handle sensitive information such as the corporate finance management or product development are generally not suitable for teleworking unless precise security control is performed. On the other hand, the tasks which are less restrictive such as writing a non-classified research paper fit well with teleworking.

3 Information Security on Home Teleworking Environment

Maintaining secure working environment for home teleworking is a critical issue to maintain the integrity of the organizational security. In this section we describe the specific security issues of home teleworking: managing the facility and computer equipments, and maintaining confidentiality of sensitive information.

One of the important issues which should not be forgotten is that the primary purpose of home is *to live*, and *not* to work. Some of the home-specific security issues which need to be reviewed follow:

- Teleworkers have to take care of their business equipments by themselves. Home teleworkers should guard their business equipments from unwanted access by the other family members or other kind of incidents. For example, Ethernet cables should be protected from physical stress by attaching them to the walls of the room or covering them under the carpets.
- The physical security of the house should be well-tightened to minimize the risk of theft, arson, or any other criminal activities. The working space for teleworking should be secured as well. A dedicated room for teleworking is strongly recommended. A notebook computer and a table are not necessarily sufficient if a teleworker need to protect his or her working environment, let alone concentrate on working with their tasks.
- The housing facility often lacks ability to supply adequate power of electricity or to provide wiring for Internet connectivity. The equipments for teleworking should be able to run safely for 24 hours a day. Each home teleworker should assess the resources he or she needs to stably perform the working tasks. Computers, routers and other always-on equipments should be kept in a cool place to prevent overheating. An uninterruptible power supply (UPS) is critical to prevent the equipments from unexpected power surge or outage.

4 Keeping sensitive information safe at home

Information in the house is not necessarily safe even when only one person lives there; let alone if many family members live together inside. Teleworkers should deliberately act to protect sensitive information, not only that of working partners but also their own private one. Some of the home-specific issues of preventing revelation of sensitive information which need to be reviewed before tele-

working at home follow:

- Individuals living with the teleworker(s) can be a source of security risk, especially when they work for the competing organizations. Sometimes they are legally prohibited to perform work-related activities at home. Sharing telecommunication equipments may become a path of leakage for sensitive information. A facsimile message can be seen by one of them before it is reached to the specified teleworker.
- Computers shared between family members without proper access right control means making path of unwanted information leakage. If a teleworker uses a shared machine, sensitive information should never be stored in the shareable file systems inside. Keeping sensitive information under per-user software protection, such as UNIX file permission system, should be a minimum requirement; storing such information to a removable medium is strongly recommended. Even an email (electronic mail) message often contains sensitive information, so never let the other family members read the teleworker's mail messages, and vice versa.
- Unused media such as old hard disks or CD-R/RWs should be immediately erased or destroyed once if they are no longer necessary. Software formatting is mandatory if reusing those media for other purposes. If they are not reusable or broken, *physically destroying the media into pieces* is the *only* effective way to prevent unwanted disclosure of the information by a third party.

5 Administrative Issues of Secure Teleworking

Teleworking through Internet requires taking care of many security precautions and preventive measures against potential adversaries, since the information passing through the networks are easy to be wiretapped and be forged for impersonation and various attacks. Since the most of business workers have little awareness of Internet security details, education of the hostility of Internet to them and how to defend themselves from malicious attacks are critical issues for secure teleworking.

One of the good examples about how little ordinary workers care about Internet security is explained in a Wired News article [13]. The article reports that many of the dismissed former dot-com company employees take the formerly-corporate computers to their home, and connect them to the home networks *with no extra security protection added.* Most of these machines are configured to operate in a corporate network protected by skilled system administrators with corporate-strength firewalls and other security measures, so they are prone to become victims of known security attacks.

The *Nimda Worm* [5] and *Code Red Worm* [4], which have effectively spreaded themselves to the Microsoft Windows operating system machines throughout the world by using many known possible measures to infect other machines, have also victimized many home computers and turned them into the worm senders to the Internet. Most of the users, however, could not find out what the problem was, let alone correct the problem by themselves. The Wired News article [13] reports that Kerry Rondell, one of the ordinary users referred in the article who had been given a corporate machine as a severance pay, only felt that her machine was just *acting funny* when it was attacked by the virus, and that she could only take her machine to a computer repair shop since *she didn't know what to do*. Each organization who hires teleworkers should form an incident response team to support the victims like Rondell and other users.

To defend against the current security threats, we propose at least two major security tools should be mandatorily installed into the machines which are connected to home networks: *anti-virus software* and *per-host firewall*. Anti-virus software is critical to keep the system integrity by detecting the existence of computer viruses or other malicious activities within the system. Per-host firewall is a set of filtering software on the various network protocol layers to prevent accepting harmful, unwanted and hazardous contents.

Anti-virus software has already gained enough popularity among the ordinary users, but the idea of *installing and activating firewalls to each client and every server*, is still little known to the ordinary users and system administrators. Obviously, installing these tools does not solve the whole

problems; each user should promptly maintain the tools with the latest patches and other upgrade information. Developing a plug-and-play package to install these tools for organizational users is required to raise the organizational network security awareness and strength.

6 Secure Communication Tools for Teleworking

One of the important issues to protect teleworking network links from wiretapping is using an encryption method between the teleworker's system and the organizational servers. Many tools as follows are available and widely in use:

- SSH (secure shell) [12] is suitable for UNIX and Windows users who mostly develop software or perform administation on shared servers.
- SSL (Secure Socket Layer) works best with existing Web-based transactional systems, such as form-input application database.
- VPN (Virtual Private Network) with IPsec, which incorporates authentication and encryption into Internet Protocol layer, works very well to secure the links with the least modification of the application software and systems.
- To communicate across unprotected multiple servers, an end-to-end application-level encryption method such as PGP (Pretty Good Privacy) for email is most effective, since it only requires the end-to-end user exchange of the public keys, and prevent the intermediate servers to wiretap the transmitted contents.

Incorporating these tools for daily teleworking activities is critical to keep the communication link secure and reliable. Combining multiple methods is effective to avoid being attacked due to unprecedented vulnerabilities.

7 Our showcase of a secure teleworking system

We have made and use two teleworking branches for performing our daily business tasks. One of the branches, Rikitake's home network, is a showcase of how a home Internet system can be designed as a secure network system, while providing adequate usability for necessary services to the business activities.

A brief diagram of Rikitake's home network is shown in Figure 1. The network connects to two different ISPs (Internet Service Providers). The ISP A, which provides an ADSL connectivity of 512kbps uplink and minimum-512kbps downlink mentioned in Figure 1, assigns a dynamic single global address. On the other hand, the ISP B which serves a 128kbps leased line connectivity assigns a fixed block of netmask /28 (equivalent to 14 hosts).

To efficiently utilize the available ISP links, we have developed a notification system between the two hosts of different default routes [7], to announce the address given by the ISP A (ADSL ISP) with a DNS (Domain Name System) server on the ISP B (Fixed Link ISP), so that we can use ISP A as an Internet server with a fixed host name. Host X invokes the DNS database update program on Host Y using SSH when the address given from the ISP A is changed. Host Y immediately reflect the change so the DNS entry for Host X is always consistent.

Incoming traffics from the ISP A and B are filtered and inspected by the Host X, Router to ISP B, and each host including Host Y and the Terminal hosts. The Host X and Y run FreeBSD 4.4-STABLE to provide the functionalities for necessary services. Host X handles the traffic to ISP A, and the Host Y handles the traffic to ISP B. We mainly use the ISP A for outgoing Web and streaming access which consumes a lot of bandwidth, while we maintain DNS server traffic, mail exchange, VPN connections, and remote terminal access directed to the ISP B for stable and reliable communication.

Various kinds of teleworking tasks are well-managed by Rikitake's home network system. A list of some of the tasks follows:

- Using VPNs in either thorough an SSH tunnel or an IPsec tunnel, Web-based form processing of our corporate database systems is handled with no difficulty. We handle many kind of tasks by the Web-based corporate system, including but not limited to, business trip expense application, traffic expense report, application of purchase and the approval, project management workflow control, application of external publishing research papers and the

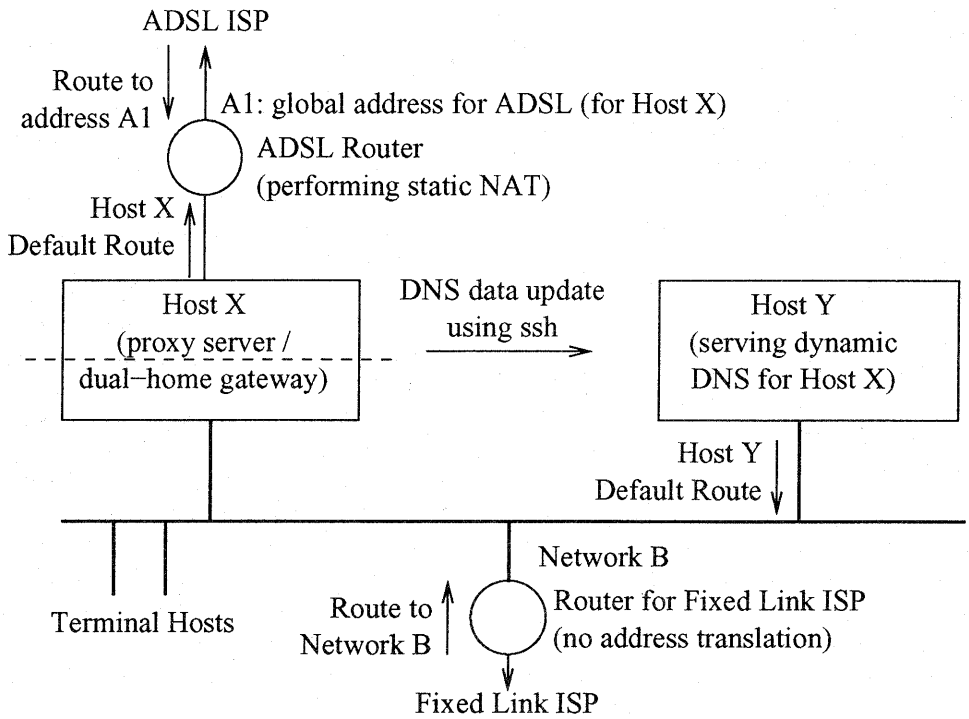

Fig. 1: Connectivity Diagram of Rikitake's Home Network

approval.

- Email is another critical application for exchanging messages and making decisions within and outside our project members. We provide some secure email servers for our daily business operation.
- We run a remote printing system to support a paper-based approval system, which enables a Windows client to directly print out documents to a printer in our headquarter office using BSD LPD (Line Printer Daemon, RFC1179) protocol over VPN tunnels. This eliminates most of the facsimile traffics inside our project.
- We have tested our home-made Internet Phone system called *MeeTwo* [*1], which supports a point-to-point voice and video communication between two Windows machines. We also evaluated Microsoft's NetMeeting, but we didn't choose it for the production use, because of the deficiency of echo-cancellation ability on the voice communication.

[*1] see `http://www.meetwo.net/` for the further details of MeeTwo.

8 Lessons Learned

In this section, we pick up some of the lessons learned during this production-level field test of home teleworking:

- The bandwidth and reliability of ADSL does not hamper the teleworking tasks. We have measured the bandwidth at Rikitake's house and our Kyoto branch. The uplink bandwidth of 512kbps is steadily available. At Rikitake's house, the maximum downlink bandwidth is 576kbps, probably because of the long distance from the ADSL ISP's DSLAM (Digital Subscriber Line Access Multiplexer) to the house [2]. At our Kyoto Branch office, however, 1.0~1.2Mbps downlink is steadily available. In either case, concerning the running cost of the ADSL services (a few thousand Japanese Yen per month), they are drastically cost-effective comparing to the previously-

available digital leased line links.

- Our Internet Phone system *MeeTwo* is originally designed for low-bandwidth environment such as for a dialup phone network modem link. We have experienced difficulties on the voice communication since the quality of the audio link is as worse as that of international phone lines. Increasing the bandwidth setting of the MeeTwo software did not change the audio setting; it only changed the video frame rate. This is not suitable for ordinary office workers to communication with voices over Internet. We have measured that the MeeTwo only uses about 6kbps for the audio link. Increasing the rate to 16~32kbps with a codec of smaller transmission delay and lower distortion may significantly enhance the usability of the application over ADSL or where an always-on Internet link of 64kbps or more. Microsoft's NetMeeting has similar deficiencies.
- Current IPsec VPN system relies on Cisco System's VPN Client and the VPN3000 Concentrator at our headquarter office. This means all VPN traffics have to be relayed through the Concentrator, and the system will not scale well when the number of teleworkers increase. An end-to-end VPN system is needed to solve this issue. Cisco's VPN Client has another issue that it only handles a single IP address for a machine. Developing a practical way to establish a VPN tunnel between two IP networks is critical for forming a cluster of networks which may dynamically change the internal subnet structure.

9 Conclusions

We have described the information security issues on home teleworking, focused to the Internet environment and the application of best current practices of security measures, such as firewalls, data filtering, and generic wiretap protection schemes on the Internet protocol suite. We have also explained our teleworking system examples, what we have achieved and what we have not, and the lessons learned from our field-test experience.

Home networking, not only limited to teleworking, is a core issue for deploying IPv6 devices throughout the real world. The issues explained in this paper is also entirely applicable to the IPv6 networks. We consider bandwidth and Internet reachability technology are no longer barriers to deploy home networks and teleworking. We rather need to solve the social issues of making frameworks to support home networks, and to develop usability-conscious application tools to get the most out of the ADSL and other *broadband* links.

Acknowledgements

We thank Yuko Fujita, Yumiko Hirai, Sachiko Hirota, Takao Hotta, Kazunori Matsumoto, Kazuo Hashimoto, Koji Nakao, and the other members of KDDI R&D Labotaroties Inc. for helping us to solve the management and technical issues on teleworking.

We would also like to thank Dr. Shin-ichi Nakagawa of Communications Research Laboratory, and Dr. Mieko Kimura of Takeda Research Institute of Life Science, for their continuous support to our High Quality Internet Project.

References

[1] Kunihiko Higa: *A Proposal for Telework-based Organizational Evolution*, Proceedings of the Third Japan Telework Society Conference, pp. 105–110 (June 2001).

[2] David Ginsburg, *Implementing ADSL*, Addison-Wesley, ISBN 0-201-65760-0 (1999).

[3] CERT/CC: *Continuing Threats to Home Users*, CERT Advisory CA-2001-20 (last revised: July 23, 2001). `http://www.cert.org/advisories/CA-2001-20.html`

[4] CERT/CC: *Continuing Threat of the "Code Red" Worm*, CERT Advisory CA-2001-23 (last revised: August 23, 2001). `http://www.cert.org/advisories/CA-2001-23.html`

[5] CERT/CC: *Nimda Worm*, CERT Advisory CA-2001-26 (last revised: September 25, 2001). `http://www.cert.org/advisories/CA-2001-26.html`

[6] Motonari Tanabu: *An Information Management System for Collaborators*, Proceedings of the Second Japan Telework Society Con-

ference, pp. 17–22 (June 2000).

[7] Kenji Rikitake, Takahiro Kikuchi, Hiroshi Nagata, Tatsuaki Hamai, and Tohru Asami: *Practical DNS Support for Dialup ADSL*, Proceedings of IPSJ 4th Computer Security Symposium (CSS2001) (October 2001).

[8] Kenji Rikitake, Takahiro Kikuchi, Hiroshi Nagata, Kazuo Hashimoto, and Tohru Asami: *Solving Management Issues of Inexpensive Internet-VPN Teleworking*, Human Interface Society HIS2001 Symposium Proceedings, pp. 593–596 (October 2001).

[9] Kenji Rikitake, Takahiro Kikuchi, Hiroshi Nagata, and Tohru Asami: *Information Security Management under Teleworking Environment*, IPSJ 63rd National Convention Proceedings Vol.3, pp. 625–628 (September 2001).

[10] Ikuo Shibata, W. A. Spinks, Yukio Tsutumi, Norimasa Yoshida, Daisuke Sahori, Kunio Noguchi, Kazuhisa Fukuda, Takahito Watanabe: *Observations on Telework Population Surveys (1) — Defining "telework" as a first step*, Proceedings of the Third Japan Telework Society Conference, pp. 37–42 (June 2001).

[11] Tsunehiko Sasaki, Tomoyuki Araki, and Fujio Yamamoto: *Information Management for Mobile Work using One-hand-PDA*, Proceedings of the Second Japan Telework Society Conference, pp. 13–16 (June 2000).

[12] Daniel J. Barrett, and Richard E. Silverman: *SSH, The Secure Shell: The Definitive Guide*, O'Reilly & Associates, ISBN 0-596-00011-1 (2001).

[13] Michelle Delio: *Beware That Company Box You Took*, Wired News, September 4, 2001, `http://www.wired.com/news/print/0,1294,46417,00.html`

[14] Paul and Sarah Edwards: *Working From Home: Everything You Need to Know About Living and Working Under the Same Roof (5th Edition)*, Jeremy P. Tarcher/Putnam, ISBN 0-87477-976-6 (1999).