2C-2 テレワーク勤務環境での情報セキュリティ管理*

力武 健次　菊地 高広　永田 宏　浅見 徹†
（株）KDDI 研究所 高信頼 IP ネットワーク技術プロジェクト‡

1　はじめに

自宅などの事業所から離れた場所から通信回線を通して作業を行うテレワーク (telework) の従事者が増えている [1]。その理由としては、インターネットや携帯電話などの通信技術の普及と廉価化、そして会社までの片道通勤時間が 2 時間を越える遠距離通勤が一般化していることに代表される都市労働・居住環境の悪化、また育児や親族の介護などで自宅を離れることができない状況などさまざまなものが考えられる。

テレワークの普及に伴い、従来物理的な事業所内で閉じた環境を想定して行っていた、企業などの情報セキュリティ管理も、各勤務従事者が各自の勤務環境で行う必要が発生してきている。本論文では、テレワークを始めとした労働環境の変化に伴い発生している企業の情報セキュリティ管理の技術や手法、教育上の問題点について考察し、実際に取り得る対策の概要について述べる。

2　企業のセキュリティ・ポリシー

企業活動では、企業や従業員が個々に扱う情報のセキュリティ管理指針を統一して一貫性を持たせる必要がある。この管理指針を**セキュリティ・ポリシー**と呼ぶ。セキュリティ教育は、セキュリティ・ポリシーの理解徹底から始まる。テレワークの場合もこの要請は変わらない。この際、あまり複雑なポリシーでは、それ自身が紙などの形で外部に漏れる危険があるため、その内容は簡明に整理して作る必要がある。

セキュリティ・ポリシーの実施はまず機密の管理から始まる。企業活動には第三者に知られてはならない多くの**機密情報**がある。一例として、取引相手や顧客を特定できるプライバシーに関する情報、また未公開の業績や商品開発情報などがある。機密管理は企業の信用や他企業に対する優位を保つために欠かすことはできない。

一方、企業活動は機密に限らず、派生する多くの情報資産によって支えられる。従業員同士が交わす電子メールや、外部へ公開する決算報告書に至るまで、その内容は多種多様である。これらの中には、傍受されてもそのリスクは小さいものや、むしろ積極的に外部発信していくべきものもある。その意味で機密管理は、**機密でないものの管理**も含め、何がどの程度の機密であるのかの定義が重要となる。

情報の管理は、実際にはそれぞれに対してどのようにアクセスできるか、つまり**アクセス権**の問題に帰着する。アクセス権の実態は多様である。例えば文書情報について考えた場合、閲覧だけが可能なのか改訂する権限があるのか、廃棄する権限があるのかないのか、読む必要が誰にあるのか、等々の問題があり、実施方法は具体的に考える必要がある。同様に、情報の置き場所へのアクセス権管理も必要となる。具体例としては、紙の情報を保管する什器なら鍵の物理的管理であり、情報がコンピュータの中にあれば物理的管理同様ネットワークからのアクセス管理も必要となる。

---

* **Information Security Management under Teleworking Environment**

† Kenji RIKITAKE, Takahiro KIKUCHI, Hiroshi NAGATA, and Tohru ASAMI

‡ High Quality Internet Project, KDDI R&D Laboratories Inc. 2-1-15, Ohara, Kamifukuoka City, SAITAMA 356-8502 JAPAN

機密とアクセス権管理の 2 つの問題は、テレワーク従事者やその労働環境でも、他の事業所と同様に考えられなければならない。セキュリティ・ポリシーの実施では、細かい手順実施の技術面で**最も脆弱な部分が全体のセキュリティ・レベルを決めてしまう**。そのためテレワーク環境が脆弱であれば企業全体のセキュリティがそのレベルにまで落ちてしまう。この意味で、商品開発や財務管理など、高度な機密保持を要求される仕事は、テレワークには向かない。一方、公開論文執筆など、扱う情報の機密性とそのリスクが低い仕事は、テレワークにより適している。

3　テレワーク環境固有の問題

テレワークでのセキュリティ・ポリシーの維持には、テレワーク環境固有のセキュリティ問題を解決する必要がある。ここではテレワークの主な形態の一つである自宅からの**在宅勤務**での問題と、**機器管理**の問題、そして**機密情報の保持と消去**の問題の 3 つに分けて考察する。

3.1　在宅勤務のセキュリティ管理

在宅勤務のセキュリティ管理は、**住宅は主に居住のために使うように作られている**ことを念頭に置いて考える必要がある。以下に具体的事例のいくつかを取り上げる。実際には他にも多くの問題が発生するため個別に対処する必要がある。

建物と部屋の安全性　出入口の施錠、外部の窓やバルコニーなどからの侵入防止など物理的な安全確保が必要なのは言うまでもない。しかしその前に、部屋の中で仕事をする十分な空間が確保できるかどうかを考える必要がある。仕事専用の部屋が確保できれば問題はないが、ノートパソコンを居間で使うなど空間が狭いと、作業効率の低下などのリスクとなる可能性がある。

同居者のリスク　配偶者など同居者が競合関係にある会社に勤務している場合は、機密の漏れが起こりかねない。公務員等別途守秘義務が課される場合もある。また、幼児や老人などが同居している場合、事故で機器が壊されるなどの可能性も考えておかねばならない。特に、家族で FAX など通信機器を共用している場合は、機密の漏れに注意する必要がある。

通信機器事故の防止　自宅でテレワークに使う回線の物理的な安全は、従事者自らが確保する義務がある。具体的には、イーサネットなど配線の保護や、作業用パソコンなどの過熱防止、無停電電源による停電対策などが必要となる。

機密廃棄手段の確保　業務上やり取りされた書類は、シュレッダーで裁断するなどで可能な限り機密を守って廃棄する必要がある [*1]。また、CD-R やフロッピーディスクなどの記録媒体は、廃棄の際は初期化などコンピュータによる内容消去だけでなく、ハサミによる裁断などで**物理的に解読不能にする**必要がある。ハードディスクなどの媒体も、コントローラ基板等を破壊して**再利用不能にして廃棄する。**

3.2　テレワーク機器のセキュリティ管理

テレワークの場合、従事者が使う機器のセキュリティ管理は、その機器を通じて企業全体の情報が漏れる可能性を考えると、他の事業所の機器と同程度以上に厳しく行う必要がある。テレワークの場合は特に、ノートパソコンなど**可搬性の高い機器を使うことが多い**ため、その点に留意して対応する必要がある。具体的な管理指針の例としては、以下のものが挙げられる。

機器の可用性確保　テレワークに使う機器は、海外出張時など代替機を確保することが困難な状況下で使われることが多い。機器の信頼性は一般の業務用機器と同様以上に高いものが要求される。また、仮に機器が故障した場合は、入手が容易な市販の機器でキーボードなどの構成部品を代用できるよう、システムの設計段階で考慮しておく必要がある。

機器の盗難防止　コンピュータはそれ自身に資産価値があるため、盗まれる可能性がある。また、業

[*1] 本稿執筆時現在（2001 年 7 月）、1 万円程度で A4 版コピー紙数枚を同時裁断できる機器が入手できる。

務に使われる機器は、内部に他機器へのアクセス管理情報や機密情報が含まれていた場合、産業スパイ行為に利用される恐れがある。基本的に盗まれないように注意することは言うまでもないが、電源投入時の起動パスワード等で簡単に悪意の第三者が機密情報を取得できないようにしておくことも重要である。

情報媒体の盗難防止　情報機器だけでなく、情報を記録した媒体の保全や盗難防止策も立てておく必要がある。最近はスマートカードなど小型大容量の媒体が普及しているため、情報を盗むのはますます容易になっている。また、ハードディスクなどの固定媒体も盗難に遭う可能性は CD-R などと同様と考えなければならない。

3.3　機密情報の保持と消去

従来の企業内ネットワークは**社内外接続部で不正情報やアクセスの試みを遮断する囲い込み方式**が主であったが、テレワークの場合は一般公衆回線を使うため、この囲い込み方式のモデルでは十分な安全は確保できない [2]。**個々の機器の不正アクセスに対する対攻撃性を強化して機密防衛に努める**必要がある（図 1）。具体例としては、以下の方法が挙げられる。

機器毎のファイアウォール使用　囲い込みの手段が使えない以上、不正パケットによる DoS (Denial-of-Service) 攻撃やポートスキャンなどには、各機器で対応する必要がある。具体的には、OS カーネルのフィルタリング機能を使い、不正なパケットの送受信を防ぐのが望ましい [*2]。

認証情報の暗号化　利用者認証の際、暗号化していないパスワードをネットワーク上で使えば、即傍受されて他者へのなりすましに使われる。これを防ぐには、使い捨てパスワード [*3]やチャレンジ＝レスポンス型認証 [*4]で最低限認証用情報は暗号化

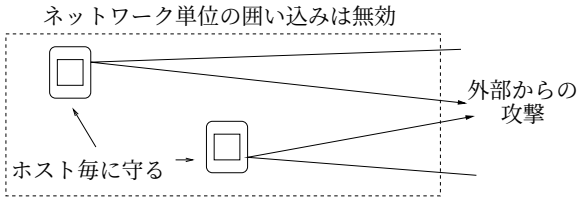

図 1: 囲い込みからホスト毎の個別防衛へ

すべきである。バイオメトリック認証との併用も効果的であろう。

通信路の暗号化　公開鍵を使ったトランスポート層での暗号化 [*5]や、暗号による実質的な専用線接続技術 (VPN) [*6]は通信内容傍受防止のために積極的に使うべきである。この場合手元の秘密鍵は暗号化して保存する必要がある [*7]。また、公開鍵の証明書自身の出自は利用のたびに検査し、疑いのあるものは使用してはならない。

手元の情報の暗号化と不要情報の消去　重要な情報は、コンピュータ上では暗号化して保管すべきである。また、長期間手元に置いておくことがふさわしくない情報は、できるだけ速やかに消去すべきである。

これらの手順を徹底するには、コンピュータ技術に明るくない従事者でも作業できるように、 plug-and-play で使えるツールが必要であろう。

4　テレワーク従事者への教育内容

テレワークでは他の勤務形態以上に多くのセキュリティ上のリスクがある。これを避けるためには、テレワーク従事者がセキュリティ・ポリシーを常に理解し、実行するための**継続的なセキュリティ教育**が欠かせない。具体的には、全社共通の教育内容に加え、テレワーク固有の問題の教育が必要である。以下に教育内容の一例を述べる。

[*2] FreeBSD などの PC UNIX では基本仕様として用意されており、Windows 系 OS でも製品として数千円程度で購入することができる。

[*3] OPIE (One-Time Passwords in Everything) など。

[*4] PPP の CHAP 認証、POP3 の APOP 認証など。この方法は認証用の秘密を暗号化できないため、機器の盗難には対抗できない。

[*5] ssh (secure shell) や SSL (Secure Socket Layer) など。

[*6] Virtual Private Network の略。

[*7] ssh や SSL ではパスフレーズで保護できる。

機密内容の定義　自宅や出張先などのテレワーク環境下でも、業務上の機密の定義は他の事業所の場合と変わらず、全社のセキュリティ・ポリシーに従う。

機密廃棄の方法　テレワーク環境下でも、機密廃棄の方法は、シュレッダーや記録媒体の物理的破壊などの方法を取り、廃棄物からの情報の漏れを可能な限り防がなければならない。

業務通信の傍受防止　テレワークでは、本社など他の事業所間との通信によって業務を行うことが不可欠になる。この際、利便性から携帯電話のメールサービスや、アナログ方式のコードレス電話、無線 LAN [3] などがしばしば使われるが、これらの方式はどれも通信内容を第三者に自由に傍受されるため、可能な限り使用しないよう周知徹底する。

機器・家屋・部屋の安全確保　ノートパソコンなど機器の盗難や不正使用に対して防護策を講じておく。また、家屋や部屋の施錠、同居者への機密保護義務の周知徹底、その他事前の事故防止策実施などを行う。

事故発生時の即時報告　機器の盗難や機密情報の紛失など**セキュリティ事故が発生した疑いのある場合は、すぐに対応担当者へ報告し対策を行う**。事故対応の方法はセキュリティ・ポリシーの一部に組み込んで置く必要がある。業務内容に関する対応は各業務担当部署で行うが、最終的には全社の事故の全情報を掌握している部署 (総務部など) が必要となる。

継続的教育の義務化　セキュリティ・ポリシーに関する教育は、他の業務関連事項同様、企業の構成員全員に対して定期的かつ継続的に行われる必要がある。具体的には最低年 1 回の研修、また異動等職務内容に変化が生じた場合はその都度教育を行う。

5　まとめ

本論文では、企業の情報セキュリティ管理と、その管理指針であるセキュリティ・ポリシーをテレワーク環境の導入に際してどのように対応させるべきかについて、現実の技術的また教育上の問題点について考察し、対策の実例について概要を述べた。

テレワークは企業から見た場合、従業員個人の問題として捉えられがちであるが、セキュリティ管理の視点から考えた場合は、まさに各個人が各々独立した事業所であるかのように対応していく必要がある。個人情報の保護などに関して世論が敏感になっている現在、業務機密の管理は、各従業員のライフスタイルから通信回線の利用法まであらゆる側面から考えて行う必要がある。

今後、人材の流動化に伴い、企業活動は**集団としての会社**から**個人が各々の能力を発揮するチーム活動**へと移行していくだろう。その際のセキュリティ管理は、これらの活動をできるだけ妨害せずに、しかも簡便な方法で高い技術的水準を確保できるものへと変わっていく必要がある。本稿がその一助となれば幸いである。

謝辞

本稿執筆の際テレワーク環境の構築にご協力いただいた（株）KDDI 研究所 ネットワークエンジニアリンググループ 主査の堀田 孝男氏、また同研究所 京都分室の平井 由美子氏に感謝する。

参考文献

[1] 小豆川裕子、W. A. スピンクス: 企業テレワーク入門, 日経文庫 791, 日本経済新聞社 (1999).

[2] 斉藤 国博: SOHO に適したセキュリティ対策, 日経インターネットテクノロジー、第 45 号 (2001 年 4 月号), pp. 148-167, 日経 BP 社 (2001).

[3] W. A. Arbaugh, N. Shankar, and Y.C.J. Wan: Your 802.11 Wireless Network has No Clothes, March 30, 2001, `http://www.cs.umd.edu/~waa/wireless.pdf` (2001).