オフィスの節電と在宅勤務における事業継続・情報セキュリティ対策ガイドブック

在宅勤務における情報セキュリティ対策検討ワーキンググループ 編著

特定非営利活動法人
日本ネットワークセキュリティ協会

2012年7月13日　第2版

目　次

まえがき

現在、日本国内の多くの地域において、節電の必要性が叫ばれています。2011年3月に発生した東日本大震災で多くの発電所が被災した結果、2011年の春から夏にかけ、東北及び関東地域で節電への要請がなされました。一方、2012年の夏は国内のほとんどの原子力発電所が停止する中、関西と九州を中心とした地域で節電への協力が求められています。オフィスにおける作業の多くが電力の使用を前提としたものである現在、節電に積極的に協力しようとすると、業務遂行に何らかの影響が及ぶことは避けられません。また、全国的に電力の供給余力が逼迫している中、急激に電力需要が増大した場合、地域によっては停電が発生する可能性も出てきました。突然の停電は業務遂行の支障になるだけでなく、オフィス内のICT機器の故障の原因ともなりかねないため、事業継続の上での大きなリスクとなります。

こうした状況の中、震災直後の首都圏の鉄道において節電のため運行本数の削減などが実施されたことをきっかけとして、企業の中で在宅勤務を活用しようとする動きが出てきました。自宅で作業する従業員分のオフィスの消費電力を減らすことで、企業として節電に協力できるとともに、地域全体での消費電力の削減も実現できます。ただし在宅勤務は、これまでオフィスで行っていた業務をそのまま自宅へ持っていけば成立するものではありません。自宅で作業を行うことによるリスクへの対策を実施するとともに、オフィスとの間に安全なコミュニケーション手段を用意する必要があります。こうした対策を短期のうちに準備することは、情報セキュリティに関する知識が必要となることもあって、一般の企業には困難です。ゆえに、2011年の夏には十分な対策が講じられないまま、見切り発車的に在宅勤務が実施されてしまう恐れがありました。

そこで、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）では復興支援活動の一環として、有志により「在宅勤務における情報セキュリティ対策検討ワーキンググループ」を結成し、2011年7月に「オフィスの節電対策のための在宅勤務の情報セキュリティ対策ガイドブック」第1版を公表しました。これは、会員企業のメンバーの在宅勤務における情報セキュリティ対策に関する知見を集約したものです。短期での検討であったこともあり、網羅的な内容にはなりませんでしたが、多少なりとも在宅勤務を検討中の企業のお役に立てたものと自負しております。今回の第2版の作成にあたっては、現在の企業のニーズを踏まえ、在宅勤務だけでなく、停電が懸念されたり、節電が必要な状況下での事業継続対策に関する内容を追記しました。

本ガイドブックを参考にしていただくことで、皆様が企業における事業の継続、社会全体での節電の実現を通じて、より災害や脅威に強く、かつ働きやすい事業環境を築かれますことを願ってやみません。

第1章　停電や節電に備えるには

オフィスの停電対策や節電への協力が必要となるとき、企業では事業継続や情報セキュリティ対策をどのように考えればよいのか、その概要について説明します。

1.1　オフィスの停電に備える

1.1.1　停電が起きるとどうなるか

オフィスにおいて停電の可能性が懸念される場合、企業は以下の3種類の影響について検討する必要があります。

①　ICT 機器の動作に必要な電力が提供されなくなる

現在のオフィスワークでは、何らかの形でICT機器を利用しながら業務を遂行している場合がほとんどです。当然ながら停電になると、これらの機器への電源供給が行われなくなります。ノートPCなど、バッテリーを装備しているものは停電が発生しても一定の間は動作させることができますが、長期にわたる停電が発生するような場合には不十分です。また、ノートPCが動作していても、ルータやスイッチなどのネットワーク機器への電源供給が行われないことで、社内・社外とのネットワークによる接続ができなくなるので、停電前と同じように業務を続けられるわけではありません。

②　照明や空調など、オフィスの機能維持に必要な電力が提供されなくなる

これも当然のことですが、停電になれば照明や空調が利用できなくなります。現在のオフィスはこうした設備を前提に設計されているため、窓の数も少なく、夏季であれば気温の上昇で実質的に業務を行うことは難しい場合が多いでしょう。

③　突然停電になることで、ICT 機器が故障する

これは①②と異なり、停電が発生する瞬間の影響に関するものです。家電製品の場合は電源が突然切れても問題がないものが多いのですが、ICT機器の中には、突然に電源供給が途絶えることが故障の原因となるものが数多くあります。したがって、後述（第4章）する無停電電源装置を導入するなどの対策を講じていない場合、停電の発生はこうしたICT機器の故障の原因となることがあります。

さらにデリケートなICT機器の場合は、停電だけでなく、電力需要の急激な変化に伴う瞬間的（0.1秒以内）の停電や電圧の降下（これらはまとめて「瞬時電圧降下」や「瞬断」「瞬停」などと呼ばれます）によっても停止したり、故障してしまう場合があります。こ

うした瞬間的な電圧の変動は電力会社の供給余力が小さくなることで、いっそう発生しやすくなると考えられます。

1.1.2　停電と情報セキュリティ対策

上述のような影響を避けるため、企業は次のような対策を講じる必要があります。

(1) 突然の停電や電圧低下によるシステムやデータのダメージを防ぐ

上述のように、停電や電圧低下はICT機器の故障の原因となり、業務継続の支障となるため、電力供給の著しい逼迫や停電が懸念される場合には、何らかの対策を講じることが必要になります。もっとも一般的な対策は無停電電源装置（UPS）の導入であり、本ガイドブックの第4章で解説しています。

(2) 停電の間に事業を継続する

事業の内容によっては、停電だからといってわずかの間も業務を中断することが許されないものもあるかと思います。また、計画停電の場合、ビジネスアワーを中心に計画されることが多いことから、この時間帯に2～3時間程度まったく業務を行わないのは事業機会の喪失になると考える経営者の方も多いと思います。

事業継続の方法としては以下の2種類があり、両者の対策は全く異なるものとなります。詳細は本ガイドブックの第4章で説明します。

- **停電していない拠点に事業の主要機能を移す：** 担当者や資源を停電の影響のない拠点に移して事業を継続します。これには在宅勤務も含まれます。
- **停電の拠点で事業を継続する：** 事業を継続するのに必要な電力を自ら必要な電力を確保します。大容量のバッテリーを装備した上で、必要に応じて自家発電設備を設けます。

(3) 停電の間のセキュリティを確保する

まず考慮すべきは停電時に防犯システムが停止することで、物理的に危険な状態が発生しうることです。具体的にはICカードやバイオメトリクスなどで来訪者の認証を行っているドアが、停電時に開放状態になってしまうことなどが挙げられます。また、監視カメラや接近センサなども停電時は機能しなくなります。

ICTの関連でも同様の影響がありますが、停電によって保護すべき情報そのものにアクセス不能となる場合は、ネットワーク経由での不正アクセスを心配する必要はありません。上述の物理的な対策の喪失による、ICTシステムそのものの盗難などに警戒すべきです。

停電が予想される間、在宅勤務をはじめとして通常と異なる形態で事業を継続する場合、情報セキュリティに関するリスクも通常とは異なる形で発生しますので、事業継続計画の策定時にあわせて検討する必要があります。

1.2 節電に協力する

1.2.1 節電のタイプ

「オフィスにおける節電」と一口に言っても、電力供給の深刻性や行政機関からの要請の有無によって、やり方は変わってきます。節電の度合いが大きくなるほど、業務への影響も大きくなるため、そのバランスをどのようにとるかが経営面での大きな課題となります。

① 停電を防止するために必要最小限の電力でしのぐ

政府や自治体、電力会社からの緊急の節電要請が行われた場合に相当します。電力需要家における節電が行われない場合、停電になる恐れがあるためできるだけの協力を行うことが求められます。この場合は、オフィスでは以下のような取り組みを行うことが考えられます。

- 節電要請が解除されるまで、コピー機、プリンタ等の消費電力の大きな機器のすべてまたは一部の電源を切り、そうした機器を利用する必要がある業務を一時中断する。
- ノートPCのACアダプタを外し、バッテリーで動作させる（ただし、節電要請の時間帯の間、ずっとバッテリー稼働で動作可能な機器のみ）。
- 必要最小限以外の照明を消す。
- 空調設定温度を可能な範囲で上げる。もしくは空調機能を切って送風のみにしたり、空調そのものを停止する。

上記の対策は、どうしても実施できない部署・業務を除き、対象地域のすべての事業所において実施することが求められます。いずれの取り組みも一日中継続できるものではありません（不要な照明を消すなど、持続可能な対策は後述の④に相当するものです）。このレベルでの協力を行う場合は、その影響としての一時的な業務効率の低下を考慮に入れる必要があります。

② 節電目標値を達成する

企業として節電の目標値（節電を行わない場合と比較して15%削減など）を定め、

その実現のための対策を講じるものです。電力需要の逼迫が懸念される場合、行政機関や電力会社がこうした節電の目安となる目標値を「ご協力のお願い」として提示することが一般的です。企業はこれに対して、自社の事業に最も影響の少ない方法で協力することになります。

③ 企業の CSR として消費電力を削減する

②の目標値にとどまらず、より大規模に消費電力を減らし、それを公表することはCSR活動のひとつとしてとらえることもできます。必ずしも電力需要のピークに事業を継続しなくてもよい業務が存在する場合などは、思い切って一時的に中断し、担当者に研修や自宅待機をしてもらうなどの対策が考えられます。

④ 無理をせずにオフィスワークの消費電力を減らす

オフィスに設置しているPC等を利用していない時にモニタ電源を切ったり、スリープモードやシステムスタンバイの自動設定時間を短くするなどの対策を施すことで、無理せずオフィスワークの消費電力を減らすことが期待できます。PCのソフトウェアベンダの中には、クライアントPC向けに自動的にPCの消費電力を削減するプログラムを無償で配布しているところもあります[1]。こうしたプログラムを用いることで、PCに関して最大30%程度の消費電力削減効果が期待できます[2]。

また、サーバにおいても、オフィスに置かれているファイルサーバ等（モニターが付属しているもの）では、スクリーンセーバーの無効化やモニタの電源を切ることで、最大20%程度の電力削減を期待することができます。

⑤ ピーク時間の消費電力を減らす

電気は作り置きができないため、節電（突発的な停電を防ぐ意味も含む）の効果を高めるためには「ピーク時」に極力電気を使わないようにすることが重要です。その観点から言えば、ノートPCのようにバッテリーが使えるのであれば、ピーク時にはバッテリーで動作させるようにします。ただし、あらかじめバッテリーで3時間程度は動作することを確認してある機器に限ります。1時間程度でバッテリーが尽きてしまうような場合は、充電でかえって多くの電力を消費してしまう結果になってしまいます。

また、タブレット端末は充電時でも15W程度（ACアダプタを外せば0W）の電力しか使用しないので、Webブラウザでの調査や、電子メールを見る程度の作業であれば、タブレットとの併用も効果があるでしょう。

---

[1] 日本マイクロソフト社による Windows PC 自動節電プログラム(Microsoft Fix it 50666)を用いた場合。http://support.microsoft.com/kb/2545427/ja

[2] Windows Server の節電情報。http://technet.microsoft.com/ja-jp/windowsserver/hh282845

コラム　節電は誰のため？

2011 年の春から夏にかけて、東北と関東の企業は、政府と電力会社からの要請のもと、各社ともかなり思い切った節電を行いました。その結果起きたことは何か？ それは電気料金の大幅な節約です。オフィスの一部閉鎖やエレベータの停止など、お客様への迷惑にもなるためなかなかこれまで行いにくかったことも、政府からの要請ということで実施に踏み切ったところ、思いのほか効果があったと感じている企業が多いようです。

一方で、節電を通じて事業機会を失った企業も多数あり、節電しなければならない状況が早急に解決することが望ましいのは言うまでもありませんが、電力料金が上昇傾向にある中、節電対策の検討は企業にとって重要な課題であるといえるでしょう。

1.2.2　節電の方法に応じたセキュリティ対策

節電に協力することにより、これまでとは異なる情報セキュリティ対策が必要となる場合があります。節電に便乗した犯罪や攻撃が行われる可能性もあるため、あらかじめ十分にリスクを検討しておくことが重要です。

(1) 業務のやり方を見直す場合

見直しの内容に応じて、以下の対策を行うことを検討してください。

① 在宅勤務

自宅などの職場外で業務を行おうとする場合、オフィスにおける情報セキュリティ対策とは相当に異なる対策が必要になります。本ガイドブックの第3章を参照してください。

② オフィスの一部閉鎖

特定のフロアを閉鎖したり、オフィスの一部を使わないようにすることで節電する場合、その影響で情報セキュリティ対策のための機器（IDSやIPSなどのネットワーク監視機器、防犯カメラ等）が停止することのないように確認する必要があります。また、窓を開放する場合は侵入や盗撮などがおこなわれないかの確認が必要です。

(2) 業務のやり方はそのままで節電する場合

(1)と比較して、特別な対策が必要なケースは少なくなります。

① 節電機器へのリプレース

最新の機種へのリプレースの場合、一般的には情報セキュリティ対策が容易になる

場合が多いと考えられます。とはいえ、最新のOSであっても導入した直後の状態では多数の脆弱性が存在しているため、OSやアプリケーションについて最新のアップデートを適用した上で利用することを忘れないでください。

②　業務上支障の無い範囲での電気製品のスイッチオフ

基本的には、ICT機器の電源を切っている間は攻撃されることはありませんので、情報セキュリティ面での影響は小さいと考えられます。ただし、監視が必要なモニターの電源を切ってしまうことで異常の発見が遅れたり、社内の情報セキュリティ対策に関する事情に詳しくない人が知らずに監視機器の電源を切ってしまうことのないよう、必要に応じて「電源を切らないでください」などの掲示を行う必要があるかもしれません。

コラム　海外のクラウドへの移行は節電に貢献するか？

結論から言えば、日本国内にあった自前のサーバを廃止して、海外に設置されたクラウドサービスに移行するほうが一般的には節電になります。ただし、インターネットの仕組みの関係で、サーバのある地点からクラウドサービスまで、データをやりとりする中継地点ごとの中継機器（ルータ等）の消費電力は、移行前より増えてしまいます。したがって、日本全体で見ると、サーバ分の消費電力が丸々不要になるわけではありません。シビアな処理速度が要求される用途の場合はクラウドサービスとの間の通信時間が増えた分だけ処理に余計な時間がかかるようになり、それを待つ時間だけオフィスの電力を無駄遣いしてしまうようなこともあり得るので、万能の解決策ではありません。

一方、自社で負担する電気料金という観点からすると、クラウド化はその削減につながりますので、電気料金が極端に高くなるようなことがあれば、その対策としてクラウド化を進める選択肢はあり得ます。ただし日本中の企業が海外のクラウドサービスに移行するようなことにあれば、ISP が設備増強を強いられることで、接続料金の値上げが行われるかもしれません。

第2章　事業継続手段としての在宅勤務

2.1　在宅勤務とは

2.1.1　在宅勤務とその類似概念

本ガイドブックでは、在宅勤務を**「企業の従業員等[3]が、本来職場で行うべき業務を主として自宅で遂行すること」**という意味で扱います。在宅勤務に類似する概念としては、下表のものがあります。

表 1　在宅勤務の類似概念

テレワーク	職場との通信の利用を前提とした勤務形態を指します。テレワークには自宅以外（サテライトオフィス等）での業務遂行が含まれる一方、通信を使わない形での在宅勤務は含まれません。企業によっては「在宅勤務」という呼び方をせず、「テレワークの推奨」という表現を用いることもあります。情報セキュリティ対策に関しては、在宅勤務と同じ意味で扱っても特に問題はありません。
SOHO	Small Office/Home Office の略語です。これらのオフィスでは、情報資産の管理拠点が自宅もしくはそれに近い環境となります。自宅等で勤務することに関しては在宅勤務との違いはありませんが、はじめから情報資産を自宅等で管理することが前提となっている点が異なるため、今回の説明対象には含めません。

2.1.2　在宅勤務の利点と欠点

在宅勤務の利点と欠点をまとめると、おおよそ次ページの表のようになります（在宅勤務の方法によっては回避できる欠点は省いています）。表にもあるように、情報セキュリティに関するリスクは、オフィスと従業員の自宅との間での通信もしくは情報の移送が必然的に発生することで、情報漏えいの生ずる機会が増える分、高くなることは避けられません。そこで、こうしたリスクをいかにして抑えるかが、在宅勤務の成功の鍵となります。

[3] 本ガイドブックでは、主に企業での参照を想定して「従業員」と表記していますが、行政機関等での導入の場合は職員等に適宜読み替えてください。また、場所によっては従業員のほか経営者等も対象に含んでいる場合があります。

表 2　在宅勤務の利点と欠点

対象	利点	欠点
従業員	・通勤が不要 ・家族と過ごせる時間が長い ・柔軟な業務遂行が可能	・勤務に関する On と Off の区別をつけにくい ・職場の設備（コピー機等）を利用できない
企業	・事業継続性が高まる ・従業員のモチベーション向上が可能	・上司の目が届かない（成果評価では無関係） ・オフィスと従業員の自宅との間で通信もしくは情報の移送が発生し、その経路及び自宅における情報漏えいの可能性が高まる

このほか、財団法人日本テレワーク協会では、テレワークの効果として次表のような項目を挙げています[4]。在宅勤務やテレワークの実施は、単に事業継続や節電のための対策としてではなく、企業の価値を高める手段として、検討すべき価値のあるものであるといえるでしょう。

表 3　テレワークの効果

環境や社会問題に対するテレワークの効果	・都市問題の緩和（通勤人口の削減、交通渋滞の緩和等） ・地域活性化（UJI ターンの増加、地方での就業者増） ・雇用創出と新規産業の創出（障がい者、高齢者、育児中女性の就業機会増） ・地球環境負荷の軽減（通勤抑制による CO_2 削減） ・社会構造の改革（ワークライフバランス指向に対応できる働き方の実現）
就業者にとっての期待効果	・仕事の生産性、効率性の向上（業務を遂行するのに最適な場所を選択可能） ・通勤の肉体的・精神的負担の減少（自由時間増大、家庭内コミュニケーションの良好化）
経営者にとってのテレワークに対する期待、効果	・業務効率・生産性の向上（従業員の疲労・ストレス軽減、付加価値の高い創造的な働き方へのシフト） ・組織変革と経営スピード化の契機（権限の委譲、水平分散組織化） ・人材の確保と新しいナレッジの獲得（自らの人材教育の実践） ・オフィスコストの削減（ファシリティコストの削減） ・災害時の危機分散（物理的移動が困難時の業務遂行が可能）

[4] 詳細は社団法人日本テレワーク協会の Web サイトで紹介されています。 http://www.japan-telework.or.jp/

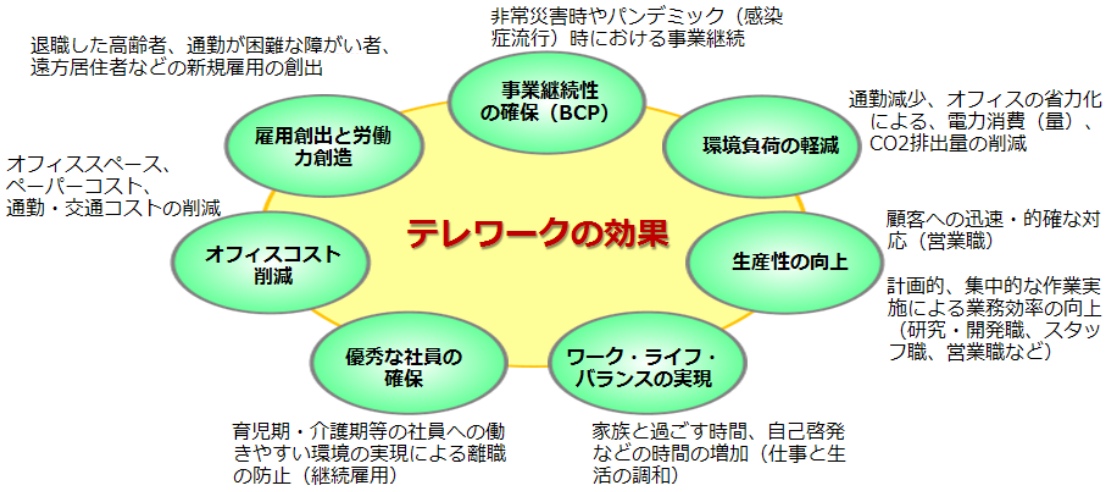

図 1　テレワーク実施による効果

コラム　日本におけるテレワーク普及の歴史

日本における在宅勤務の普及のいきさつとして、テレワークの歴史を簡単に紹介します。日本では 1980 年代初頭にテレワークの導入が始まりました。「在宅勤務」「在宅ワーク」「テレコミューティング」などとも呼ばれ、女性の社会進出が活発化する中、妊娠や育児期間等においても、在宅等で電話やファクシミリを活用して行える働き方として注目を集めるようになりました。

その後のバブル経済による地価高騰により、企業では都心部のオフィスにかかるコストが無視できないものとなったことで、郊外にオフィスを置き、近郊の従業員が通うサテライトオフィスが登場するなど、一部の企業において現在のテレワークに相当する制度の導入が試みられるようになりました。だだし、さまざまなテレワーク施設が開設されたものの、従業員によっては本社とサテライトオフィスの両方を利用することになるなど、コスト削減に大きく貢献しなかったこと、またバブル経済崩壊の影響もあって、90 年代に入るとテレワークの普及は一時停滞します。テレワークの本質が「働き方の変革」であるだけに、行政、企業、個人（社員）のすべてにおいて、さまざまな課題をひとつずつ解決する必要があったのですが、多くの企業においてテレワークは実験的な形にとどまったまま収束していきました。

しかしながら 90 年代後半になると、IT の発達により PC が一般に普及し、インターネットによる情報通信ネットワークが急速に発展しました。また、携帯電話の普及とあいまって、テレワークは再び脚光を浴び、そして、ブロードバンド回線を利用したインターネットを通じた働き方へと変化し、携帯電話やノート PC を利用し、決められた場所以外でも業務をおこなうモバイルワークがテレワークの新たな主流となりました。2000 年代に入ると、少子高齢社会での労働力確保や、「ワーク・ライフ・バランス」の実現のために、政府主導でテレワークが積極的に推進されるようになり、現在に至っています。

2.1.3 「これまでの在宅勤務」との目的の違いがもたらす影響

これまで、わが国の民間企業における在宅勤務制度は主として「自宅で育児や介護をしながら仕事がしたい」という従業員側の希望がまずあって、それを可能な範囲でかなえようという意図のもとで整備されてきました。このため、自宅で勤務をすることで生じる情報セキュリティ上のリスクについて、どのようなリスクがあり、どう対策すれば減らせるかを十分に検討した上で、在宅勤務にあたっての様々な条件を定め、それを承諾した従業者にのみ認めるという形で運用されてきました。従業員も、自宅での業務を実現するために積極的な協力や工夫を行ってきたのです。

一方、節電や停電対策を目的として在宅勤務を行おうとする場合、従業者が希望しているとは限らず、どちらかといえば企業側の都合で導入することが多いと考えられます。この結果、消極的に在宅勤務を行うことになる従業員が多数発生することになりますが、こうした従業員であっても、著しい不便を感じさせず、かつ情報漏えいなどの事故を生じさせることがないような在宅勤務方法を考える必要があります。このように、在宅勤務の目的が変わることで、その情報セキュリティ対策にも異なる観点が求められることを認識しなければなりません。

コラム　これまで国内で在宅勤務が普及しなかった理由

日本国内で計画的な『在宅勤務』が普及していない理由には、いくつかの要素が考えられます。技術面や制度面の障害などがある中で、日本独特の評価制度が及ぼしている影響が大きいのではないでしょうか。今でもまだ遅くまで残業しているほうが働いていることをアピールできる、といった考え方や受け取り方が残っているのが実情です。そのような状況では、いかに働いている姿を上司に見せるかが大きなポイントになります。こうした懸念の解消には、在宅勤務者を考慮した評価制度の導入が欠かせません。

気付かれにくい課題としては、在宅勤務で発生する通信費や光熱費は本来企業等で負担すべきものであるため、それをどう扱うかが挙げられます。通信費は月額固定のケースも多いのですが、電力・ガス等の光熱費は使用量に応じた課金が普通のため、相当額の在宅勤務手当を支給するなどの対応が望まれます。

なお、総務省の平成 22 年度通信利用動向調査によれば、企業がテレワークを導入しない理由として、以下の理由が挙げられています。

「テレワークに適した仕事がないから」（69.8%）
「情報漏洩が心配だから」（25.5%）
「業務の進行が難しいから」（20.5%）
「導入するメリットがよくわからないから」（20.3%）
「社内のコミュニケーションに支障があるから」（16.1%）
「顧客等外部対応に支障があるから」（12.5%）

2.1.4　最新の在宅勤務の動向

東日本大震災以降の在宅勤務をはじめとするテレワークの状況について、インターネット上で公表されている事例を紹介します。

(1) 実態調査

震災以降の実態調査結果として、以下の2例が挙げられます。

①　「東日本大震災後と柔軟なワークスタイル」に関する調査（ＮＴＴデータ経営研究所）[5]

東日本大震災後の2011年6月に、被災地を除いた全国の企業従業員約1000名を対象に実施したものです。テレワークを実施している企業は全体の2割に及び、震災後徐々に増加していることが示されています。また、半数以上の回答者が、テレワークなどの柔軟なワークスタイルの必要性を感じています。

②　平成２３年度テレワーク人口実態調査（国土交通省）[6]

毎年実施されている調査ですが、平成23年度におけるテレワーカーの比率ならびに人数は、それまで3年間の横ばい状態から大幅に増加していることが示されています。具体的には、就業している人のうち、職場以外で1週間あたり8時間以上ICTを用いて業務を行うと回答した人が全体の19.7%（前年比3ポイント増）となったほか、自宅で1分以上テレワークを行った経験がある人も490万人（前年比170万人増）となっています。こうした原因として、震災を契機としたテレワーク導入の進展、新たなICTツールの普及などが挙げられています。

(2) テレワークの導入事例

本ガイドブックにおける在宅勤務の導入事例は第6章で紹介しています。

①　日本マイクロソフト社のテレワーク導入事例（ITmedia）[7]

日本マイクロソフト社における、在宅勤務に限らない、モバイルワークの実践例の紹介記事です。新たな働き方と製品・サービスの活用についての最新動向が示されています。

[5] http://www.keieiken.co.jp/aboutus/newsrelease/110705/index.html
[6] http://www.mlit.go.jp/report/press/toshi02_hh_000019.html
[7] http://www.itmedia.co.jp/enterprise/articles/1205/14/news011.html

2.2 在宅勤務の導入に関する論点

2.2.1 論点Ⅰ： 在宅勤務を指示すべきかどうか

前述したように、在宅勤務における情報セキュリティ上のリスクは、方法によって程度はありますが、オフィスでの勤務と比較すれば高くなります。また、業務内容によっては効率の低下も懸念されます。そこで、従業員に在宅勤務を指示すべきかどうかは、代替案との比較において相対的に妥当かどうか、許容し得るかどうかがその判断の基準となります。

オフィスでの電力消費を抑制するための手段としては、実現可能性の有無は別として、在宅勤務以外にも以下のような方法が想定されます。

- 夏季休業日の増加
- 営業時間の短縮
- 節電の必要ない地域での業務遂行
- 電力消費の少ない機器への置き換え
- 自家発電の実施

これらの方法と比較して、業務効率の低下と情報セキュリティ上のリスクを勘案してもなお、業務を遂行する価値が高いと判断される場合は、在宅勤務が選択肢となるものと考えられます。もっとも、業務効率と情報セキュリティ上のリスクは次の「どのような作業をしてもらうか」によっても変わってくるので、論点ⅠとⅡは並行して検討する必要があるでしょう。

2.2.2 論点Ⅱ： 在宅勤務でどのような作業をしてもらうか

在宅勤務でどのような作業をするかによって、情報セキュリティ上のリスクは大きく変わってきます。下表に情報セキュリティにおける機密性を例に、リスクの大きさに応じた作業の種類をまとめましたので参考にしてください。

表 4　機密性に関する作業上のリスク

機密性リスク	主な作業
小	・公開情報の収集 ・社内／社外研修の受講（ｅラーニング教材等） ・公開用パンフレット等の作成
中	・個人情報・機密情報を含まない業務資料の作成・編集・分析 ・個人情報・機密情報を扱わない社内ミーティング ・決裁ワークフローの申請・承認
大	・個人情報・機密情報を含む業務資料の作成・編集・分析 ・顧客との打合せ、問い合わせ対応（顧客が了承している場合を除く） ・契約で守秘義務を課された情報の取り扱い

2.2.3　論点Ⅲ：情報資産の持ち出しを認めるかどうか

業務の効率性とセキュリティリスクのバランスを保ちつつ、節電対策や災害対策の一環として効果的な在宅勤務の導入を実現するためには、原点に立ち返り、そもそも「持ち出し」とはどういうことなのかをしっかりと考える必要があります。

- 「持ち出す」物には何があるのか
- どこまでを「持ち出し」と定義するのか
- 「持ち出す」ことに伴うセキュリティのリスクにはどのようなものがあるか
- 「持ち出し」を伴う在宅勤務と「持ち出さない」在宅勤務のそれぞれの利点と欠点

こうしたことを組織として適切に把握し分析した上で、在宅勤務の導入及び「持ち出し」を認めるかどうかを判断する必要があります。

(1)「持ち出す」物には何があるのか

組織の「情報資産」と一概に言っても、業務で利用するPCや、USBメモリ等の電子可搬媒体等の物理的な資産もあれば、紙の文書や電子情報など様々な形態があります。では、「持ち出す」とは何を持ち出すことなのでしょうか。

(2) どこまでを「持ち出し」と定義するのか

顧客情報や経営情報など組織の情報を何も保存していないPCやUSBメモリを自宅に持ち帰るのも「持ち出し」でしょうか。それとも、紙の文書や電子情報を保存した業務に利用できる状態のPCを自宅に持ち帰った場合が「持ち出し」でしょうか。

- ネットワーク越しの社内ファイルサーバへのアクセスは「持ち出し」？

- 個人所有のPCから業務のWebメールを利用するのは「持ち出し」？
- データのローカルへのダウンロードを行わない業務システムのリモートアクセスは「持ち出し」？

「持ち出し」の定義はそれぞれの組織で考えるべきことですが、本ガイドブックでは、

「会社の情報を保存した機器・媒体を、物理的に職場外に持ち出すこと」

および

「会社の情報をネットワーク経由で、物理的に職場外にある機器・媒体の中に保存すること」

を指すこととします。本ガイドブック第3章では随所で「持ち出し」という言葉を用いていますが、上記の意味で使っていますのでご注意ください。

(3)「持ち出す」ことに伴うセキュリティのリスク

何を「持ち出し」とするのかはそれぞれの組織の判断にもよりますが、適切な判断を下すためには、それぞれのリスクを考慮することが必要です。

例えば何も情報を格納していないPCを自宅に持ち帰ったとします。このPCからは、社内LANにつながない限り何の情報を得ることもできません。せいぜいWeb閲覧ができる程度です。この場合のリスクとは何でしょうか。

- ハードウェアの紛失（物理資産に対する金銭的損失）程度
- 情報を格納していないPCや媒体の紛失（可用性の損失）はさほど大きな問題ではない

このPCを使って社内のネットワークにアクセスして業務をするとしても、PCのローカル上にデータを保存しなければ、漏えいや改ざんのリスクはさほど大きくありません。そして、ネットワーク越しで情報資産を利用させる場合には、組織がそのインフラを提供するなど、組織側でこうしたリスクを把握及びコントロールすることが比較的容易です。

これに対して、紙文書の「持ち出し」や、PCや電子可搬媒体に電子データとして会社の情報を保存した状態での「持ち出し」では、漏えいや改ざんがリスクの中心です。

- 盗難・紛失
- 盗み見

ひとたび自宅への「持ち出し」を許可してしまえば、組織の管理が及ばないところで組織の情報資産が扱われることになります。これは利用者自身の管理責任が大きくなるということです。

社内に保存されたままの情報を在宅勤務で利用するリスクの種類と、実際に物理的に持ち出して利用するリスクの種類は異なります。当然、リスクが異なれば必要となる対策も異なります。組織の立場からすれば、管理しやすい、すなわち「持ち出し」をしないで行う在宅勤務を選びたくなるでしょう。

しかし、それだけの理由で「持ち出す」か「持ち出さない」かを決定してしまうと、本来の在宅勤務導入の目的である業務効率の向上や節電対策、災害対策の対応を果たせているのかという疑問も生じます。

リスクだけではなく、利点と欠点を併せて考えなければなりません。

(4)「持ち出し」ての在宅勤務の利点と欠点

情報を紙や電子情報の形で物理的に職場外に保存して持ち出す方法には、以下の利点と欠点があります。

表 5　情報を物理的に持ち出して行う在宅勤務の利点・欠点

利点	欠点
・ VPN[8]等の特別な仕組みを構築したり、自社のインターネット接続回線を増強する必要がなく、費用をかけずに早期に導入可能 ・ オフィスの停電等の事態が発生した際でも、持ち出した情報で業務遂行が可能	・ 情報資産の漏えいや改ざんの危険性が高まる ・ 情報資産の正確な状態把握が困難（複製や副産物生成が行われるおそれ） ・ 持ち出す情報資産の管理に必要な管理工数が増大する

こうした分析を行った上で、組織の在宅勤務導入の目的や在宅勤務で扱う情報資産の性質に応じて、「持ち出し」を認めるべきかどうか判断する必要があります。

(5) 結局「持ち出し」を認めるべきか、認めないべきか

持ち出しを認める場合の要因

- 金銭的な問題（中小規模で情報システムに係る予算が潤沢でない場合）
- 節電対応などで導入に緊急性がある
- 事業業務内容の特性から例外的な対応を求められることが多い

[8] Virtual Private Network の略。公衆回線をあたかも専用回線であるかのように利用できるサービスで、データは認証や暗号化により保護されるため、盗聴などの危険性を下げることができます。詳細は本ガイドブック 3.2.3 を参照してください。

- ネットワーク等のインフラの容量性能に制限がある

持ち出しを認めない場合の要因

- 漏えい改ざんによる損失が大きい（個人情報の大量漏えい、多額の商取引にかかわる、等）
- 長期的な管理負荷の軽減も考慮して、シンクライアントや仮想デスクトップを選択したほうが経済的である

(6) 対策の選択も「持ち出し」の有無に応じて考慮する必要がある

情報を持ち出さない場合にとくに考慮すべき対策

- シンクライアント、リモートアクセス等手法の選択
- どこからアクセスを許可するか（例：自宅のみ、職場外のどこでも可）
- 災害等の有事においても信頼できるデータセンター／通信事業者の選定
- 通信経路の技術的安全性（機密性、可用性）
- 情報に対するユーザのアクセス権限管理
- IDパスワード、セキュリティトークン等の認証情報機器の安全管理
- 監視システム／サービスによる不正アクセス攻撃の検知

情報を持ち出す場合にとくに考慮すべき対策

- 持ち出してよい情報の分類、持出管理
- どこへの持ち出しを許可するか（例：自宅のみ、職場外のどこでも可）
- 情報持ち出しに関するルール、手続きの策定（紛失時の危機管理策を含む）
- 情報を持ち出す機器媒体の安全管理（紛失盗難対策）
- 在宅勤務を行うPCのセキュリティ対策（ウイルス対策、脆弱性対策等）
- 情報のコピーの制限、業務終了時の消去
- 上記対策についての在宅勤務者に対する周知教育
- 利用者のルール順守状況のモニタリング

2.2.4　論点Ⅳ：在宅勤務の方法として、どのような手段を認めるか

上述の論点Ⅰ～Ⅲの判断を行った時点で、在宅勤務として認める方法が決まってしまう場合も多いかもしれませんが、職場と自宅の間の移送方法や暗号化等の対策について検討する必要があります。詳細は本ガイドブックの第3章を参考にしてください。

コラム　自宅でも仕事がはかどるなら苦労はない？

今まで述べてきたように、現在想定されているようなオフィスの節電や停電対策のための在宅勤務となると、従業員が必ずしも望んで在宅での業務遂行を選択しているのではないこともあって、これまでと同じような成果が期待できるとは限りません。

従業員に在宅勤務を指示するにあたっては、以下のような点に留意する必要があるでしょう。

① 自宅での自己管理

職場と異なり従業員各自が業務遂行を自己管理する必要があります。特に本来はくつろぎの場である家庭において、業務時間をどのように確保するかが課題といえるでしょう。そうした意味で、オフィスとの電話連絡やテレビ会議等は、ある決まった時間に必ず業務の内容を考えることになるため、時間管理の支援手段として効果的です。もっとも、組織によっては全従業員で自宅作業ということもあるでしょうから、その場合は自宅同士で行うか、別の方法を考える必要があります。

② 在宅勤務の効率に関する個人差

『性格的に在宅勤務が不向きな方』がおられる可能性もあります。以下のような条件にあてはまる方は要注意です。

- ☑ **誰かと話をしないと不安**
  自信がないままに作業をすることになるので、生産性が上がらないかもしれません。
- ☑ **仕事はいつも締切間際にやる**
  自宅では時間管理がいっそう難しくなります。こうした性格が災いして職場で残業をしがちな人は、自宅では徹夜をすることにもなりかねません。
- ☑ **凝り性である**
  終業時間などの区切りがないので、際限なく仕事を続けてしまいがちです。一方で、良いものを作ろうと思うほどかえって手がつかなかったりもします。
- ☑ **現実逃避に走りやすい**
  自宅には会社とは比べものにならないほど誘惑が多いといえます。

2.3 在宅勤務の実施にあたって理解しておくべきこと

2.3.1 就業規則・ルール作り

在宅勤務を行うにあたり、就業規則や運用ルールが在宅勤務に対応しているか総務部門にて確認しておくとよいでしょう。在宅勤務の形態（就業場所）や期間（週何日や恒久的な施策か一時的な施策か）などにより、運用でカバーできるケースも多いと思われます。本ガイドブックでは情報セキュリティに焦点を置いているため、勤務時間の管理や人事評価などは、「THE Telework GUIDEBOOK　企業のためのテレワーク導入・運用ガイドブック（改訂版）」[9]などを参考にして下さい。

2.3.2 職場の情報資産を守る責任を負うということ

企業において「情報」は、事業を通じて収益を生むための一種の「経営資源」です。情報がもつ価値にもとづく「情報資産」という言葉も、浸透して久しくなっています。また業務を行う際には、個人情報、営業秘密、知的財産権や契約により秘密保持を義務づけられた情報など、安全管理が法的に求められる情報を取り扱うことも多くなっています。人的セキュリティ対策として秘密保持（非開示）に関する契約書等により「情報資産」の取り扱いに注意する事を誓約するとともに、技術的セキュリティ対策により情報漏えいを起こりにくくすることが重要です。なお、秘密保持（非開示）に関する契約は、「情報資産（顧客情報、営業機密情報、人事情報など）の特定」「得喪時の報告」「退職時の返還」「退職後の秘密保持」「損害賠償」等について、網羅すると良いでしょう。

職場を離れて自宅などの環境で業務を行うためには、必然的に職場の外で情報を取り扱わなければなりません。PCやUSBメモリ等の機器・媒体に情報を入れて持ち出す場合もあれば、職場外から社内のサーバにリモートアクセスして情報を利用する場合もありますが、会社の目の届かないところで情報を取り扱うという意味では同じです。

通常の勤務形態では情報の取扱いは職場内で行われますが、これがひとたび職場の外に持ち出されると様々なリスクに晒されることになります。たとえば、情報を持ち出した機器・媒体が移動中の紛失や盗難にあうリスク、セキュリティの不十分な自宅のPCに情報を保存した結果としてウイルス等により情報流出するリスク、職場外からのリモートアクセスのID・パスワードを他者に盗まれて不正アクセスされるリスクなどが挙げられます。これらのリスクはいずれも、セキュリティが管理された職場内のPCで業務を行う限りは生じない、在宅勤務特有のリスクです。JNSAの調査[10]によれば2010年に

[9] 日本テレワーク協会 2009 年 2 月発行（国土交通省・総務省・厚生労働省・経済産業省編集）
http://www.mlit.go.jp/crd/daisei/telework/

[10] NPO 日本ネットワークセキュリティ協会（JNSA）「情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」2010 年度版（2011 年 7 月 1 日公開） http://www.jnsa.org/result/incident/2010.html

発生した個人情報漏えいインシデントのうち、「紛失・置き忘れ」および「不正な情報持ち出し」によるものは284件（全体の17%）にのぼり、漏えいした個人情報の人数は55万人に達します。またJNSAの別の調査[11]では、就業者を対象としたアンケートで業務データが入ったPCを紛失した（または紛失しそうになった）経験のある人は全体の10.6%にのぼりました。そうした紛失・盗難の場所の内訳を見ると、ほぼ3分の2が移動中・出先・自宅などの職場の外での発生ケースとなっています。あえて乱暴な計算をするなら、従業員100人の会社で在宅勤務のためのPCを全従業員に配付した場合、そうしたPCのうち6～7台程度は職場外でPCの紛失・盗難にあう可能性があるということです。会社の管理の行き届かない場所で勤務するということは、業務で使用する資産を安全に取り扱う責任が、業務を行う個人により重く負わされるということです。

在宅勤務を導入するにあたっては、セキュリティのリスクが会社にとってのリスクであると同時に従業員個人にとっても重要事となることを、十分に周知・教育して、セキュリティ意識を涵養する必要があります。また、いかなる厳重な注意をもってもヒューマンエラーや不正を撲滅することは不可能であることを認識し、技術的なセキュリティ対策により安全性を高めることも極めて重要です。

2.3.3　家庭への配慮

(1) 家族への配慮

在宅勤務を始める際には、同居している家族、頻繁に出入りする親族と話し合いを行い、在宅勤務への理解を求めることが重要です。

在宅勤務は、オフィスにいる時よりも作業をしている姿が見えない分、企業から明確な成果を求められることが多く、そのために業務に集中する時間とスペースが必要であることを伝え、家族で話し合うことが望まれます。どうしても家族が自宅にいると、つい家事の手伝いを求められてしまうこともあります。そのため、業務中は出来る限り接近することを遠慮してもらうよう、業務時間を決めて家族に示すことが有効です。業務時間を決めた以上、自分でもこの時間を守るようにして、メリハリをつけて業務を遂行しましょう。

会社と締結した誓約書がある場合には、それを家族に見せて、セキュリティへの理解を求めることも有効です。

また、業務用PCは、家族用とは異なる機器とし、家族に触らせないように徹底しましょう。特に子どもが触ることで予期せぬ事態が発生するため、パスワードロックは必須です。

[11] NPO 日本ネットワークセキュリティ協会（JNSA）「情報セキュリティインシデントに関する調査報告書～発生確率編～」（2011 年 4 月 1 日公開） http://www.jnsa.org/result/incident/2010_probability.html

(2) スペースの確保（自分で行う対策）

在宅勤務者が自宅で配慮しなければならないことは、業務スペース及び保管スペースの確保です。施錠できる個室があればベストですが、リビング等の家族が出入りする部屋で業務を行う場合は、棚やカーテンで仕切るなどして、出来る限り独立したスペースを作りましょう。

また、書類やPCの保管用として、鍵の付いた棚も確保することが望まれます。子どもによるいたずらを予防するだけでなく、不用意に普通ごみとして処理されてしまうリスクもあります。出来る限り子どもや家族の手が届かない場所に保管しましょう。また、盗難対策として、外出時の戸締りも気をつけるようにしてください。

個室でない場合は、業務の会話を家族に聞かせないよう、なるべく電子メールを使いましょう。業務はできるだけペーパーレスにし、メモなどは散乱しやすいので、ノートなど散乱せずに綴じることのできる用紙を使いましょう。

(3) 在宅勤務のルールの共有（家族にお願いする対策）

家族に事情を理解してもらうため、家庭内での在宅勤務のルールを決めて文書化し、家族全員で共有することを推奨します。例えば以下のようなルールが考えられます。

- 業務の時間を決めて、その時間はできる限り話しかけない
  （一方で、業務時間を際限なく延長することもしない）
- 仕事で利用するPCや記録媒体は勝手に触らない
  （家族が自由に使えるPCや媒体を別に確保する）
- 仕事の紙は触らない。勝手に捨てない
- 電話をしているときは、静かにする
- 外出時の防犯は家族全員で気をつけること
- 仕事用の電話には勝手に出ない（騒音にならないようマナーモード等を活用）

2.4　在宅勤務による情報セキュリティインシデントへの対策方法

在宅勤務中に情報セキュリティインシデントが生じることを想定し、企業においてあらかじめ対策しておくべきこと、及びインシデントが起きてしまったときに実施すべき事項について説明します。

2.4.1　あらかじめ対策しておくべきこと

企業は在宅勤務を許可するに先立って、以下の事項について実施しておくべきです。とくに、在宅勤務を大規模に開始した後で情報セキュリティインシデントが生じた場合、主要なスタッフがそれぞれの自宅にいるような状況では迅速な対応が不可能となりますので、事前の準備はきわめて重要です。

(1) 在宅勤務に対応したルール、手続等の整備

従業員が在宅勤務を行う場合に、どのように行えばよいのかを判断するよりどころとなるようなルール、手続き等を整備します。具体的には以下のような文書を整備することが想定されます。

- 在宅勤務で行ってよいこと、禁止事項等を定めた規定等の整備
- 企業所有のICT機器を職場外に持ち出す際の手続、マニュアル等の策定
- 自己所有の機器を企業内ネットワークに接続する[12]際の手続、マニュアル等の策定
- 事故発生時のインシデント対応マニュアルの策定

(2) 連絡とサポートの体制整備と連絡手段の提供

在宅勤務となる役員・従業員との連絡の方法を定めるとともに、緊急時の連絡手段を準備します。連絡手段は緊急時専用である必要はなく、むしろ日頃から使い慣れている手段のほうが役に立ちます。ただし、緊急時にも利用可能であることをあらかじめ訓練等を通じて確認しておく必要があります。上述のように、緊急事態が発生した際に、対策における主要な役割を担うべき人が在宅勤務をしている可能性を考慮することが重要です。また、こうした連絡手段の整備と同時に、在宅における業務遂行を支援するためのサポート体制を整備することも考慮すべきです。

(3) 従業員の教育

在宅勤務の対象者だけでなく、オフィスで勤務する従業員に対しても、在宅勤務が

[12] 類似の概念に BYOD(Bring Your Own Device: 自己所有機器の職場への持ち込み)があります。ここに示す自己所有機器の自宅での利用と対策に関して一部共通性があるので、BYOD 対策を参考にすることができます。

行われている環境下での緊急時対応のあり方について、十分な教育を行っておく必要があります。従業員に周知すべき事項の例を以下に示します。

① 在宅勤務だから黙っていればわからないと考えてはいけない！

② 事故の事実内容をできるだけ正確に把握する。ただしあまり時間をかけずに報告に必要な最低限の情報を記録する。

③ ②の内容を会社のルールに定められた担当へ報告する。緊急事態であることを考えると電話連絡をした後で、メール報告とするのが良い。いずれにしても複数の連絡先の把握、複数の連絡手段の確保が重要。

④ 紛失や盗難の場合には、最寄りの警察や関係機関（駅など）に可能な限り速やかに連絡する。

⑤ 会社のルールに定められた担当と相談しながら、事故の影響範囲等を詳細に調査する。場合によっては出社して対応を行う必要がある。

(4) 事故発生時の訓練の実施

在宅勤務環境で緊急事態が発生した場合の対策について、(1)で策定した手続のもとで実際に行動できるかどうかを、あらかじめ訓練を通じて確認しておくことが重要です。緊急事態の際に、マニュアルなしに的確な行動が取れるのはフィクションの中のヒーローだけであって、普通の人間は経験や訓練したことのない行動をとっさにとることはできません。この場合の緊急事態は、在宅勤務における情報漏えい事故等に限らず、在宅勤務をしている経営陣の判断が必要となる事態など、多くのシナリオについて訓練の対象とすることが望ましいでしょう。

2.4.2 事故が発生した場合に実施すべき事項

前述の対策をあらかじめ準備した上で、事故が発生した場合には次のような対処を行うことが求められます。

(1) 対策のポイント

以下の観点から対策を実施します。

- 事態の正確な把握：在宅勤務実施時には、オフィスで事態を把握するために行動できる従業員の数が限定される可能性があります。こうした状況で効率よく事態の把握を行うためには、日頃から訓練を重ねておくことが重要です。
- 事故拡大の防止：事故の原因が新型のマルウェアなどである場合、放置しておくと被害が拡大する恐れがあります。場合によっては、すべての従業員に一時

的に業務を中止させるなどの決断も必要となります。

- 的確な情報発信：事故の影響を受ける顧客、関係者、従業員等それぞれに対して、タイムリーな情報発信を行うことで、風評やデマを抑止することが必要です。これもあらかじめ緊急時の情報発信について準備をしておかないと難しいものです。

(2) 情報漏えい時の対応ポイント

在宅勤務の場合に限ったものではありませんが、企業として対策を検討するにあたっては、独立行政法人情報処理推進機構が発行している「情報漏えい発生時の対応ポイント集」[13]が参考になります。

コラム「在宅」以外の社外での業務

在宅勤務を許可すると、実際には従業員が職場にも自宅にもいない場合、つまり外出先でもやり方によっては業務が可能になります。ただし、外出先では自宅とは別のリスクがあるため、以下に示す場面の例に応じて注意する必要があります。

① ホテルの客室内等（他者との空間の共有がなく、機器も共用しない場合）

部外者が立ち入ることのないホテルの客室は、情報漏えい等のリスクが比較的小さい環境といえます。ホテル従業員等が入室することによるリスクはあるものの、家族が脅威となり得る自宅よりも、状況によってはむしろ安全かもしれません。ただし、ホテルが提供するインターネット接続（有線 LAN、無線 LAN とも）を利用する場合は注意してください。他の宿泊者等が通信を傍受できてしまう環境になっていることも多いので、外部に漏れては困る内容をやりとりするのは危険です。こうした通信が必要な場合は、VPN による接続を利用するのが適切です。VPN が利用できない場合は、客室内にいてもあえて自前のモバイル通信を利用するほうが安全な場合が多いでしょう。

② 交通機関、喫茶店等（他者と空間を共有する場合）

上述したホテルでの対策に加え、外部からの視線に関する対策が必要になります。プライバシーフィルターなどが販売されているのでこれを利用することが対策になりますが、真後ろからの視線は防げないため、機密性の高い情報を閲覧・編集する場合の対策としては不十分であると考えてください。また、離席の際には盗難の恐れがあります。

③ ネットカフェ、公共の端末等（他者と機器を共用する場合）

職場から提供されたり、自分で所有している機器以外の機器を利用して業務をすることは避けてください。たとえ VPN 接続を利用する場合でも、キーボードの打鍵履歴などが密かに記録されている可能性があります。こうした機器を通じてパスワード等の認証情報が漏洩することは、組織全体の脅威となる恐れがあります。

[13]情報漏えい発生時の対応ポイント集, 2012 年 3 月第2版発行, 独立行政法人情報処理推進機構(IPA). http://www.ipa.go.jp/security/awareness/johorouei/

第3章　在宅勤務の方法

3.1 「持ち出さないで」行う在宅勤務

3.1.1 リモート作業環境を使う

(1) 自宅で仕事をするには？

仕事をするにはデータ（情報）とアプリケーションが必要です。会社にある業務用PCには、必要なアプリケーションがインストールされ、データにアクセスができ仕事が行えます。在宅勤務（外部での業務遂行含む）を行う場合、自宅環境にアプリケーションとデータをどのように準備するか考えなくてはいけません。アプリケーションはWeb化が進んだり、個人所有のPCに対するインストールがライセンス的に認められたりするなど、事前に準備できる環境が整いつつありますが、緊急時にはすぐに配布や準備ができないかもしれません。また、データはまさに情報資産であり、業務を行うためとはいえ、保護されていない状態で外部に持ち出すことはたいへん危険です。とくに個人所有のPCなどに機密情報を保存することは情報漏えいやセキュリティインシデントのリスクが飛躍的に高まってしまいます。これまで危険性が高いため、データの持ち出しは許可されなかったはずですが、緊急事態とはいえ、何の対策もなく持ち出しを許可する、またはセキュリティポリシーを緩和するなどの対策を実行すると、そこが弱点（脆弱性）となり、情報漏えい事件が発生してしまうかもしれません。

(2) 自宅で仕事をする方法

これまでのセキュリティポリシーとセキュリティレベルを維持しながら、安全に効率よく在宅勤務を実施する方法はないでしょうか？　ひとつは、これまでにも行われていたような持ち出すPCやデータを適切に保護する方法です。具体的には以下のような対策があります。

- 情報を分類し、業務に必要なデータだけ持ち出す。個人情報など重要度が高いデータは持ち出さない。
- 持ち出しするデータを暗号化する、またはハードディスクを丸ごと暗号化する。
- 接続するデバイスを制限する（会社支給PCのみ。個人所有PCは接続させない、など）。
- USBメモリなどの外部デバイスを制限する。
- セキュリティパッチやウイルス対策ソフトを最新版に維持する。

- P2Pソフトなど危険性が高いソフトウェアはインストールしない。
- 紛失や盗難に気を付ける。

これらの対策を行うためには、情報の分類をしたり、データ暗号化ソフトの導入、ウイルス対策ソフトやセキュリティパッチを最新版に維持するシステムなどを構築する必要があります。また、利用者側がデータを保存したPCやUSBメモリなどを紛失や盗難にあわないように常に意識して利用する必要もあります。このような人に依存する運用は、利用者向け教育やリテラシー向上なども必要で、システム導入や情報資産の分類作業なども必要になることを考えると、この夏すぐに対策を始めるには時間がなく、間に合わないかもしれません。

もう1つの方法は、「情報を持ち出さずに仕事をする」ということです。これまで、重要な情報を持ち出すためにはどう保護するか、そこにアクセスするデバイスや持ち出しPCをどう管理するか、という視点で対策が進められてきましたが、それらを厳密に管理していくことは莫大なコストと時間がかかります。

重要な情報と重要でない情報の分類も、ユーザのスキルに依存してしまい、うまくできないかもしれません。そこで、情報を持たずに仕事ができれば、情報の持ち出し方法や保護方法、重要な情報かどうかの分類などを考える必要がありません。

情報を持ち出さずに仕事をする方法としては、シンクライアントがあります。シンクライアントであれば、情報を持ち出さないため、情報の分類などの作業を減らし、利用者向け教育なども最小限でよく、すぐに対策を始めることができます。シンクライアントには以下のような特徴があります。

表 6　シンクライアント利用の利点・欠点

利点	欠点
・ 情報を持ち出さないため、情報漏えいの危険が少なく、環境や場所を選ばずに安全に仕事ができる ・ 情報資産の分類を意識しなくて良い ・ 部分的な導入（スモールスタート）が可能で、低コストで準備できる ・ 拡張性があり、大規模展開も可能	・ ネットワークが必要で、ネットワークがなければ何もできない ・ 細かな描画（CAD やデザインなど）が必要な業務には向かない（対応可能な製品もある） ・ 実用的に使うには、通信環境の増強などのコストが必要となる場合がある

こうした特徴から、この夏、節電対策のための在宅勤務を実現する方法として、導入が容易で、情報を持ち出さずに安全に仕事ができるシンクライアントが、その有力な解決策の1つであるといえるでしょう。

(3) 情報を持ち出さずに仕事をする　～シンクライアントの技術的背景～

シンクライアントを実現するには以下のような方法があります。

- デスクトップに接続する
- アプリケーションに接続する

「デスクトップに接続する」方法とは、そのPCを遠隔操作する方法です。あたかもそのPCの前に座っているように、デスクトップが表示され、すべてのアプリケーションやデータが使用できます。使用方法も通常のPCと変わらないため、別途教育なども必要ありません。リモートデスクトップ接続を許可するだけで実現できるため、すぐに開始することができます。

①　リモートデスクトップ

ア）　仮想 PC 方式:

VMwareや、Xen による仮想化されたサーバ環境で構築された複数の仮想マシンをネットワーク経由でユーザが利用できる仕組みです。1つの仮想マシン毎にOSやアプリケーションがインストールされていることで、独立したユーザ環境毎の個別情報の保管やカスタマイズなど、柔軟な対応が可能です。また、仮想マシンとして独立していることで、同じバージョンに対応したアプリケーションはほとんど稼動します。ユーザ毎に仮想マシンのOSとアプリケーションが起動することで、仮想化されたサーバのハードディスクやメモリのリソースを多く必要としますので、同ハードウェアスペックにおけるSBC(サーバーベースドコンピューティング)と比べ、ユーザ集約率は低くなる傾向にあります。また、仮想マシン毎に個々のOSとアプリケーションのライセンスが必要になります。クライアントPC側には、VMware仮想化環境ではVMware View 、XenServerによる仮想化環境にはXenDesktopの専用クライアントソフトウェアを導入して利用します。自社開発した独自アプリケーションを利用する環境や、クライアント環境を自由に利用できることを求められるソフトウェア開発環境などに適しています。「アプリケーションに接続する」方法とは、専用のシステムを用意して、アプリケーションだけ外部から利用する方法です。アプリケーション単位で使用させるかどうかを決めるため、より細かな制御ができますが、専用サーバの構築やアプリケーションの動作テストなどが必要なので、この夏の対策には時間的に間に合わないかもしれません。

イ）　SBC(サーバーベースドコンピューティング):

複数のクライアントPCがサーバ上でアプリケーションを共有して使用するもので、一般的にはマイクロソフト社のWindows Server(NT4.0以降)で提供されているターミナルサービスの仕組みを利用します。クライアントPCからは、キーボードやマウスの操作情報がサーバに送られ、その結果の画面イメージのみクライアントPCに転送されます。サーバ上でアプリケーション共有される仕組みのため、一部稼動しない場合を想定し

た事前検証の必要性や、アプリケーションの予期せぬ停止により複数ユーザに影響が出るなど運用面の考慮が必要です。ハードウェアのリソースやライセンス種別により、コストの最適化が図りやすい特性を持っています。SBCの代表的な製品であるCitrix社の XenApp もWindows Server 上のアプリケーション共有サービスを提供し、クライアントはマイクロソフトWindows に限らず、Mac、LinuxなどのOSでも利用可能で、スマートフォンなど新しいデバイスまで利用範囲は拡張されています。オフィスアプリケーションやブラウザベースのWebアプリケーションを使用する提携業務などを行うユーザ環境に適しています。

上記のような方法を使ってシンクライアントを準備すれば、情報を持たずに仕事ができるようになります。ただし、シンクライアントは以下のような様々な課題があり、これまで導入できないケースがありました。

- 専用のサーバやシステムを構築し運用する必要がある
- アプリケーションが動かないなどの相性問題がある
- 広帯域のネットワークを確保する必要がある（特にモバイル環境）
- 接続する側とされる側の両方のシステムを準備するためコストが高くなる

現在は、これらの課題を解決する新しい技術が出てきており、シンクライアントの導入が実現しやすくなっています。具体的には以下のような技術です。

- PCを仮想環境に構築する「デスクトップ仮想化」
- 個人所有のPCから安全にデスクトップに接続できる「USB型シンクライアント」
- 自宅やモバイル環境におけるネットワーク帯域の増加

これらの技術を利用すると、従来からの課題をクリアしてシンクライアントを早く、低コストで準備することができます。

(4) シンクライアント環境の準備

シンクライアント環境があれば、職場でも職場外でも、いつでも、どこからでも、同じデスクトップが表示されます。デスクトップにあるアイコンはもちろん、ハードディスクに保存されている情報も、どこから、どんなデバイスを使って接続しても、まったく同じです。また、情報はデスクトップ上にあり、一切持ち出されないため、何も意識する必要なく安全で効率よく仕事ができます。

このシンクライアント環境を構築するためには何を準備すればよいでしょうか？具体的には以下の3つを準備します。

- 接続するデスクトップ環境（仮想デスクトップや自席PCなど）

- VPN接続環境（IPSecやSSL-VPNなど）
- 接続元環境（シンクライアント専用端末やUSB型シンクライアント、スマートフォンやタブレットデバイスなど）

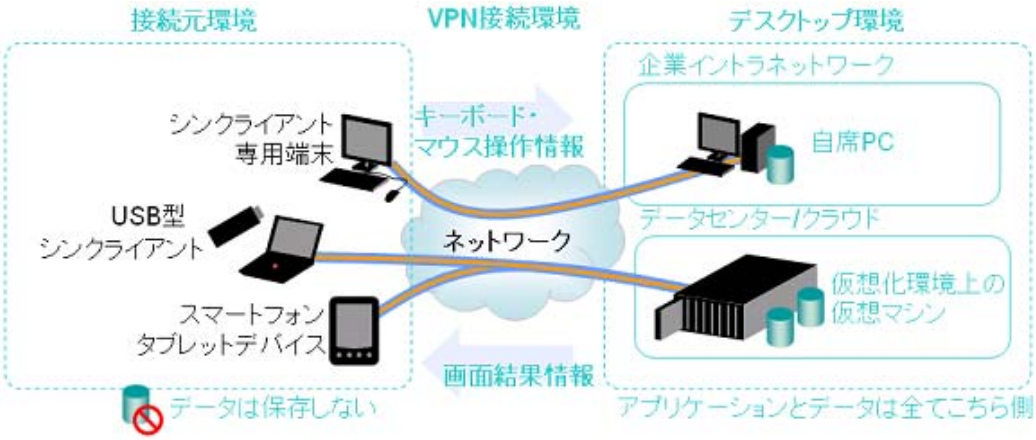

図 2　VPN 接続環境

① デスクトップ環境

アプリケーションがインストールされ、データが保存されるデスクトップを準備します。これらは物理的に移動されることなく、自宅からリモートデスクトップ接続を利用して動作させます。デスクトップ環境は仮想化環境でも物理PC（自席PC）でもどちらでもかまいません。

② VPN 接続環境

自宅から社内ネットワークに接続するために、VPN（Virtual Private Network）接続環境を準備します。VPNはインターネットなどの不特定多数が利用する回線の中に、あたかも自前の専用線のように安全に通信できる接続関係を構築するサービスのことで、IPSec[14]やSSL-VPNなど様々な種類があります。

③ 接続元環境

自宅の個人所有PCから直接接続することには、データのコピーやウイルスの侵入など、様々なリスクが伴います。シンクライアント専用端末やUSB型シンクライアントなどを利用して、データを持ち出せない、ウイルス感染や侵入などもしない端末を選定します。また、スマートフォンやタブレットデバイスなどを利用することもできます。

【参考】シンクライアント環境 最小構成例

USBシンクライアント(またはタブレットデバイス）を利用した自席PCにリモートデスクト

[14] インターネットで暗号化した通信を行うための規格です。詳細は 3.2.3(2)を参照してください。

ップ接続する環境の紹介。USB型シンクライアントとVPNシステムだけで導入できます。（VPNシステムをお持ちであればUSB型シンクライアントのみで良い）

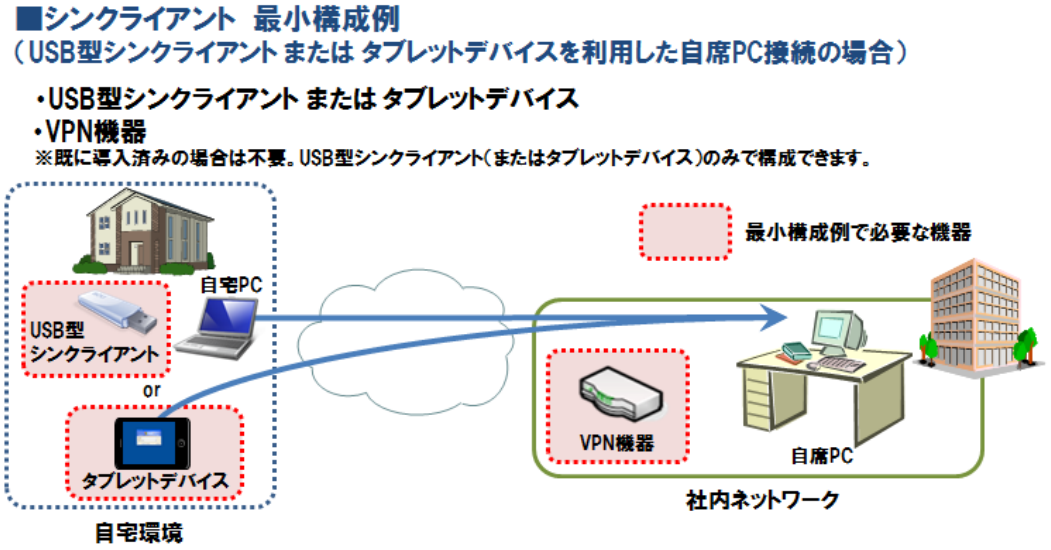

図 3　シンクライアントの構成例

(5) 普段から利用するシステムにする

震災および電力不足への対策として、在宅勤務や職場外での業務を認める動きが出ています。ただし、こうした対策のためだけに利用するシステムでは費用対効果が望めません。また、緊急時だけ利用するシステムは、その利用方法やアカウント情報、パスワードなどがすぐに分からず結局使えない、というケースがよくあります。そこで、この在宅勤務や職場外での業務（リモートアクセス）環境を普段から使い、効率よく業務ができる新しいワークスタイルを創出することが重要です。何かしらの緊急事態に、在宅勤務を命じても、いつもの延長線上で普段通りに仕事ができる環境を整備しておけば、機会損失なども最低限にとどめることができます。在宅勤務を行う環境は、事業継続性という観点からも重要なポイントと言えます。最後に、繰り返しになりますが、この夏在宅勤務を始めることは節電対策などを考えると極めて重要です。シンクライアントであれば、限られた時間の中でも、安全で効率的な在宅勤務環境を整備できます。ただ、そのためだけのシステムにするのではなく、これをきっかけにして新しいワークスタイルを創出し、生産性の向上やさらなるメリットの追求を行い、事業継続性の確保と企業の活性化や飛躍を実現できるようにしていくことが、在宅勤務を成功させるカギだと思います。

3.1.2　情報セキュリティ上の問題の少ない作業のみを在宅で行う

3.1.1項では情報漏えい対策を行いつつ、在宅勤務を行う方法に触れてきましたが、ここでは逆に、情報漏えいが生じても問題の少ない作業のみで在宅勤務を行う可能性について検討します。

「漏えいが生じても問題が全くない作業」とはどのような作業でしょうか？　社会一般に公開されている情報（公開情報）のみを用いる作業はこれに該当するでしょう。ただし、内容的には機密性が全くなくても、それが公開を前提としていない文書に記載されている場合、その文書の漏えいは問題となります。たとえば、自社の名前が入った社内打ち合わせ用メモのデータが漏れた場合、自社の管理体制はどうなっていたのか等、組織の信用面での被害が生ずるのは間違いありません。同様に、自組織宛の電子メールが漏えいする場合も同様です。したがって、漏えいしても問題が全くない作業というのは相当に限定されると考える必要があります。

(1) 研修・自己啓発

自宅でeラーニングを受講したり、書籍や雑誌を用いて自習する場合について検討します。

①　情報セキュリティ上のリスク

市販されている書籍や雑誌（紙媒体・デジタルコンテンツとも）を読んで学習するだけであれば、情報漏えい等の問題はほとんどありません。厳密に言えば、ある企業の従業員があるジャンルの書籍を読んでいることが明らかになることで、その企業の新規展開方針が外部に漏えいする可能性はあります。ただし、そこまでリスクを考慮するのであれば、外部の検索エンジンに入力するキーワードについても慎重にカモフラージュする必要があるはずで、そうした対策をとっていない限り気にする必要はないでしょう。

自宅での商用eラーニングサービスの受講、ストリーミングによるセミナーの視聴等も情報漏えいという面では問題の少ない作業といえます。ただし、こうしたサービスを利用する際には認証を行う必要があるものが大半です。企業が費用を負担し、企業から認証用のアカウントを提供されている場合は、その認証情報（ユーザID、パスワード）が漏えいすることのないように配慮する必要があります。

勤務先のサーバに接続してのeラーニングサービスの受講や教材の参照等については、接続することがシステムの情報セキュリティ上の脆弱性を生じさせないようにする必要があるため、内容的に問題はなくても一定のセキュリティ対策が欠かせません。

②　在宅勤務での運用方法

以下のような運用方法が考えられます。PCが必要な場合は、従業員が自宅で所

有しているものを利用することを前提とします。ただし認証情報の管理の必要上、最低限の情報セキュリティ対策（パスワードの使い回し禁止、フィッシングに関する基礎知識の啓発）を行うことが求められます。

- 週1日程度の研修日を設け、自宅からeラーニングサービスを受講してもらう
- あらかじめ課題を与え、その課題に対する解答の作成は自宅で行うことを認める

(2) 情報収集

検索エンジンやオンライン辞典、データベースを使うことで、業務に必要な情報を収集し、とりまとめる場合について検討します。

① 情報セキュリティ上のリスク

各種の検索エンジンや、無料で利用できるデータベースで情報収集を行うこと自体のリスクはほとんどないといえます。検索エンジンのサービス提供者は、どのようなキーワードがどの頻度で入力されているかを、そのドメイン属性とともに分析（データマイニング）しているため、事業内容によっては安易に利用することが望ましくない場合があります。むしろ、自宅から検索することで企業ドメインとの関連が見えにくくなる点で、自宅から検索するほうが望ましいとさえいえるかもしれません。

一方、情報収集の結果については注意が必要です。検索されたページのハードコピーを印刷していくだけ、といった作業であれば問題はありませんが、結果を整理して資料にまとめるのであれば、その資料は公開情報のみをベースにしていたとしても、企業の事業に役立てる形でまとめられている以上、管理すべき情報であるといえます。したがって、その資料を作成・保管するPC等の機器の情報セキュリティ対策を適切に行う必要があります。

自宅で商用データベースを用いた情報収集を行う場合は、その認証情報（ユーザID、パスワード）が漏えいすることのないように配慮する必要があります。

② 在宅勤務での運用方法

在宅での情報収集に関しては、以下のような運用方法が考えられます。資料作成等を含めた作業を行う場合は、リモート作業環境やVPN接続においてのみ許可することが望ましいのですが、従業員は自宅のPCのインターネット接続で直接検索した方が速い場合はそちらを利用しがちなので、そうした点にも配慮が必要です。

- 在宅勤務での情報収集を認めるが、行って良い作業を検索、ダウンロード、閲覧、印刷、要点のまとめ等に限定する
- 情報収集結果をとりまとめた資料を作成する場合は、業務内容や自社名が類

推されないように配慮することを求める

(3) 論文作成・学会活動等

自宅で対外公表を前提とした論文等を執筆する場合について検討します。

① 情報セキュリティ上のリスク

公表を前提とした論文の執筆作業自体による情報セキュリティ上のリスクは、一般的には小さいといえます。ただし、最先端の研究等で競合他社と一刻を争って提出する必要があるような場合などは、内容の機密保持対策が求められます。

一方、本格的な論文等の場合は長期にわたって執筆することになりますが、ハードディスクの故障をはじめとする機器のトラブルによるデータの消失については、オフィスのようにバックアップ環境を完備していることは自宅では考えにくく、在宅勤務者の自己責任で対策を講じる必要があります。

論文の査読等、自宅で他者の情報を扱うことも考えられます。査読論文は自社の情報資産ではないため、直接の管理対象にはなりませんが、情報漏えいの事故が発生した場合の影響が自社に及ぶ可能性があるため、対象者に必要な対策を講じるよう指導することが必要かもしれません。

② 在宅勤務での運用方法

在宅での論文作成等に関しては、以下のような運用方法が考えられます。在宅勤務としてではなく、時間外での作業ということであれば、すでに容認している企業も多いかもしれません。必要に応じて、ミラーリングやバックアップの方法についての啓発を行うことも考えられます。

- 業務の一環として行っている学会活動のうち、論文執筆等の作業に関しては在宅勤務の形で勤務時間内の作業を認める
- 論文査読等を含む学会活動を在宅勤務で行うことを許可するにあたって、自己の責任で情報セキュリティ対策を講じることに関する誓約書の提出を求める

3.2 「持ち出して」行う在宅勤務

3.2.1 職場の機器を持ち出して仕事する

(1) PC のセキュリティ対策

情報漏えい防止の観点からも、業務への個人PCの利用を制限している企業が多いため、リモートアクセスは企業貸与のPCを経由して行われることがほとんどです。しかし、ただちに在宅勤務が必要な場合などでは、在宅勤務用の貸与PCの確保が困難などの理由から、個人PCの利用が認められる可能性が高まります。会社支給PCにおいてはある程度の対策が徹底されていることが想定されますが、個人所有PCに関しては、対策されていない、という以前に、対策されているかどうかもわからない、という状況であることがそもそもの問題となります。

① 個人 PC の潜在リスク

個人の資産であるため、利用するソフトウェアの制限やウイルス対策、脆弱性対策を強要することができません。したがって、それぞれの対策状況に関しては、個人によってばらつきが大きいと考えられます。セキュリティ的な観点からは、最低ラインを想定することが好ましいことから、個人所有PCと会社支給PCの混在する在宅勤務環境においては、ウイルス対策も脆弱性対策もなされていないことを想定した対策を講じる必要があります。

② 利用するソフトウェアの制限

会社支給のPCであれば、利用するソフトウェアを制限することは可能ですが、個人のPCに対して利用するソフトウェアを制限することは難しいでしょう。会社の運用では、システム管理者等によってPCに対する管理者権限が設定され、その管理者権限がないと、利用ソフトウェアをインストールできないといった管理や制限を行うことで、不要な通信や脆弱性を低減しているのが一般的です。一方、個人のPCに対して新たに管理者権限を設定することも、インストールされているソフトウェアを正確に管理することも現実的に困難です。このため、管理者としては、未知のソフトウェアがインストールされているPCで業務が行われるという危険性があること、また利用者は不適切なソフトウェアがインストールされていることによって、自らのPCから業務情報が漏えいする危険性があることを認識することが重要です。これらの危険性を下げるためには、利用者と管理者の各々が対策する必要があります。例えば、利用者は各自で不適切なソフトウェアをインストールしていないかを確認すること、管理者は教育などを通じて注意喚起を行うことが必要になります。

③ ウイルス対策について

「パターンファイルが最新でない」「ウイルス対策ソフトが会社管理のものでない」「そもそもウイルス対策ソフトがインストールされていない」という、ウイルス対策ソフトにまつわる問題は、そもそもウイルス対策を対策ソフトにのみ依存しているから発生する問題です。ウイルス対策ソフトやパターンファイルに依存しない検出方法を行うことで、個々のPCのウイルス対策状況から独立した対策をとることが可能になります。

昨今のウイルスの持つ特徴である、「インターネット上のサーバへ向けた特殊な通信」を逆手にとり、通信をモニタリングし、ウイルスの発するパターンを見つけることで、感染端末の発見と特定が可能になります。この方法は、パターンに依存しないため、パターンファイルが最新でない、といった問題を切り離すことができます。さらに、亜種などのいわゆる「ゼロデイ」に関しても、通信をベースに検出が可能であることから、パターンの間に合わない、いわゆる「未知ウイルス」の検出の可能性も秘めています。

④ 脆弱性対策について

脆弱性は、それ単体では無害であるとも言えます。しかし、脆弱性を攻撃するコードにより、悪用されたときにその影響が最悪な形で発揮されることになるのです。つまり、仮に脆弱性が残っていたとしても、それを悪用されないような対策を施すことで、ある程度のリスク回避が実現できるのです。

VPN上の端末を発端とする、社内ネットワークへ向けた脆弱性攻撃拡大を防御するためには、VPNセグメントと社内ネットワークの間に脆弱性攻撃コードを検出する仕掛けをしておく対策が有効です。脆弱性を悪用する攻撃を検出し、その通信を遮断することにより、社内ネットワークに存在するかかもしれない脆弱性を持った端末への攻撃や、大規模感染を防止することができます。

(2) PC の健全性の維持確認

通常、社内で利用しているPCは、ウイルス対策やパッチ管理のツールなどで、セキュリティレベルの維持管理を行っていますが、この機器を職場外に持ち出して利用する場合、社内ネットワークに常時接続されているわけではないため、ウイルス対策の更新が正しく行われていない、クライアントファイアウォールや、侵入防止システム(IPS)[15]などの機能が正しく動作していないなど、そのままブロードバンドネットワークに接続するには問題のある状態になっている可能性があります。導入したセキュリティ対策の機能が正しく動作していることを、クライアント側で自動的に監査し、必要に応じて修正を行い、最低限のセキュリティレベルを維持する仕組みを導入することで、より安全に仕事が行えるようになります。また、VPNなどで社内ネットワークに接続させる場合における、最低限のセキュリティレベルを整えることで、ウイルスワームなどの脅威が

[15] Intrusion Detection System の略。不正なアクセスを検知すると接続を遮断する機能をもったシステムのこと。

VPNを経由し、社内ネットワークに広がる可能性を低減することができます。

最低限のセキュリティレベルとして、下記のポイント考慮することを推奨します。

① ウイルス対策について

オフラインでの利用期間や週末などを考慮し、ある程度の期間を許容することで、大きく利便性を損なうことなくセキュリティレベルを維持できます。期間は、業務の利用方法などを考慮する必要がありますが、2～3日程度の期間が適切です。また、更新されているかだけではなく、リアルタイムのスキャン機能が有効になっているか等、ウイルス対策製品が正しく動作していることを確認することもポイントとなります。

② クライアントファイアウォール、IPS について

ウイルス対策機能と同様に、クライアントファイアウォール機能、IPS（侵入防止システム）の機能についても、確認を行うことが必要となります。特に外部のネットワークに接続する場合、ゲートウェイにネットワークレベルのファイアウォールが導入されていないため、PCに対し直接攻撃が仕掛けられる場合もあります。上記の機能が正しく更新、機能されていることで、PCがネットワークに接続され、ウイルス対策が更新されるまでの間のセキュリティを担保することができます。

③ パッチの適用（脆弱性対策）について

ネットワーク経由の攻撃や、ドライブバイダウンロードなどのWebからの攻撃を適切に防ぐためには、パッチの適用が必要となります。資産管理ツールや、パッチ適用ツールを用いて、パッチの管理適用を行っているケースが多いと考えますが、その場合においても、必ず適用されていないといけないパッチについては、確認し強制的に適用する仕組みを用意することが望ましいです。

④ ネットワークの接続制御

導入したセキュリティ機能が適切に機能していないなどの問題があった場合には、ネットワーク接続についての制御を考慮する必要があります。問題を抱えた状態のまま、インターネットへのブロードバンド接続を行わせることはリスクを伴うため、クライアント側で接続を制御できることがより望ましい対策といえます。また、ネットワークへの接続が拒否された場合に、ユーザが確認するべき点や、連絡先などを事前に周知徹底しておくことも、在宅勤務中の利便性を維持するためにも重要になります。

⑤ データの暗号化

日常業務で利用する会社のPCには業務に必要なデータやお客様情報、メールアドレス等の多くの個人情報や機密情報が保存されていることでしょう。特にノートPCにお

いては職場外へ持ち出して利用しているケースも多く、PCの盗難/紛失による情報漏えいリスクに常にさらされています。万が一の盗難/紛失に対し、貴重なデータは暗号化し、第三者への情報漏えいを防ぐ対策の実施が望まれます。HDD内データの暗号化対策には主にファイル暗号とHDD暗号の2つの対策が挙げられます。

ア）　ファイル暗号化

機密データをファイル単位で暗号化します。主に特定のフォルダに保存したデータが暗号化の対象となります。そのため機密データの暗号化の有無は利用者に運用に委ねられます。機密データが暗号化されているかどうかは利用者任せとなってしまうため、その点を留意した運用が必要になります。

イ）　HDD 暗号化

HDD暗号はハードディスク(HDD)[16]全体を暗号化します。OS起動前にパスワードによる認証が成功すると、暗号鍵がメモリ上に読み込まれて、その暗号鍵を通してHDD内のデータがバックグランドで読み書きされます。HDD暗号のメリットはHDD内の全てのデータが暗号化されるため、利用者は”データを暗号する”ということを意識することなく、HDD内のデータが全て暗号化される点にあると言えるでしょう。PC操作を得意としない利用者とっても非常に利便性が高く、管理者視点からみても、どのユーザが利用してもデータが必ず暗号化されるため、HDD内のデータを必ず暗号化させることが可能になります。

(3) デバイス制御、私物 USB メモリの利用制御

USBメモリでデータを持ち出す際は、盗難/紛失に備え必ず暗号化してデータを書込むことが望ましいです。しかし、私物の暗号機能付USBメモリならよいということではありません。暗号化されたデータを取り出すためのパスワードも、私物であれば、簡単なパスワードが設定されていることも十分想定されます。紛失/盗難からの情報漏えいのリスクを軽減するために、会社のセキュリティポリシーにそったパスワード設定と暗号機能を備えた会社支給のUSBメモリのみ利用許可する運用が望まれます。

この項では、職場の機器を持ち出して仕事をするために会社支給のUSBメモリのみ利用可能にするデバイス制御機能と、他のセキュリティ対策を組み合わせる方法を紹介します。

①　特定 USB メモリ以外の利用制限

システム管理者が指定したUSBメモリだけに利用許可するソフトウェアやシステムがあります。これらを利用することで、他のデバイスを制限するだけではなく、誤って私物のUSBメモリへの書き出すことを未然に防ぐことが可能です。

[16] ハードディスクに限らず、SSD(Solid State Drive:フラッシュメモリを用いた記録装置)でも同じです。

②　データを持ち出す際の管理

USBメモリを利用してデータを持ち出す際の管理として、操作ログを取得するソフトウェアやシステムがあります。これらを利用することで、持ち出したファイル名の特定や持ち出したユーザーの特定が可能となり、不用意な持ち出しを検出することが可能です。また、万が一、紛失した際にも、誰がどのファイルをどのような状態（暗号化されていたか？）で紛失したのかを特定することが可能です。

③　重要データの PC ローカル保存禁止

重要データの持ち出しについては、作成・編集するファイルをPCに保存することが一般的ですが、PCに保存された重要ファイルはコントロールできなくなるため、持ち出し厳禁という対策になる場合もあります。現在、USBメモリ内の重要ファイルに対してPCローカルへの保存を禁止するシステムもあり、重要ファイルを不用意にPCへ保存することを防ぐことが可能となります。

また、これらのシステムには、個人情報漏えい対策として、個人情報が含まれるファイルを探索する機能や、隔離する機能もあり、これらを併用することも可能です。

④　申請・承認に基づく USB メモリへの書き出し

上記の3つ（特定USBメモリ制限、持ち出し管理、ローカル保存禁止）を組合せ、持ち出し申請と承認を管理するシステムがあります。このシステムを利用することで、持ち出しファイルと申請ユーザ及び、承認者が何時から何時まで持ち出しを許可したのか？を管理することが可能となります。

(4) 業務用スマートデバイスの活用

現在、USBメモリ以外のデバイス（フラッシュメモリカード、オーディオプレーヤー等）を記録媒体として利用することも可能であり、スマートフォンやタブレット等を利用することや、PCや他のサービスと連携することも考えられます。スマートフォンやタブレットは、USBメモリとは異なり、デバイス自らが通信機能や管理機能があります。例えば、インベントリ収集やアプリケーション起動制御、及びネットワーク接続制御などの機能があり、安全に利用できる環境が整っています。

スマートフォンの安全な利用に関する管理やセキュリティ対策は、JNSAの調査研究部会　スマートフォン活用セキュリティポリシーガイドライン策定WGが発行したスマートフォン活用セキュリティガイドライン（β版）[17]に詳しく記載されていますので、参照してください。

[17]「スマートフォン活用セキュリティガイドラインβ版」 http://www.jnsa.org/result/2010/smap_guideline_Beta.pdf

3.2.2　自宅の機器で仕事する

(1) 情報をどうやって移送するか

在宅勤務者に情報(データ)を送付する方法として、物理媒体を使用して送付する方法とオンラインで情報を送付する方法があります。本項では、物理媒体を使用して送付する際のセキュリティについて説明します。通常、データを物理的に搬送する場合、媒体としてCD/DVD、USBメモリまたは印刷物(紙)が想定されます。媒体の紛失盗難対策が重要ですので、媒体自体での対策、搬送方法での対策を紹介します。

①　物理媒体のセキュリティ対策

■ CD/DVD

CD/DVD自体にセキュリティ機能はありませんので、データをコピーする際にパスワードを付けるなどして、他者に見られないようにします。

■ USBメモリ

セキュリティUSBメモリであれば、パスワードや生体認証(指紋)付のものがありますので、紛失盗難対策には適しています。また、コピー制御機能(USBメモリ内のファイルをPC等へコピーさせない)付のもの(多くは専用ソフトウェア)もあります。USBメモリから情報が外に出ないので安心です。

■ 印刷物(紙)

「透かし印刷」により肉眼では認識しづらい方法で印刷物に「印」を付け、複写すると見えなくしたり、複写物であることを判定することはできますが、オリジナルを見えなくする技術はありません。

②　データの物理的な搬送

物理的な搬送においては、まず梱包方法に注意します。搬送中に袋が破れて、媒体を紛失した事例も報告されています。次に搬送方法ですが、自身で持ち運ぶ際は、自分で責任を負うしかありませんが業者に委託する場合はサービスの違いを理解して選ぶようにします。

サービスの違いに注意すべき点

- 信書(日報等報告書や契約書等)を送れるかどうか
- 受領印をもらえるかどうか

先方のポストへ投函するだけのサービスの場合、確実に相手が受け取った証明ができません。多くの場合、伝票番号から追跡が可能です。なお、受領印をもらえない

サービスであっても投函までの追跡ができるサービスもあります。

ア）　損害賠償の有無および金額

損害賠償があるからといってセキュリティが高い訳ではありませんし、事業者の紛失破損が多いわけでもありませんが、送付物の価値に見合った損害賠償が受けられるか確認しておくと良いでしょう。

イ）　専用 BOX

紛失しては困る重要なデータであれば、高セキュリティな専用BOXサービスもあります。

これらのサービスは事業者により異なりますので、送付する情報の価値とサービスの内容配送コストを考慮して送付方法を決定するようにします。

(2) 自宅の個人所有 PC における情報セキュリティ対策

ここでは、個人所有のPCを対象に情報セキュリティ対策を説明します。個人所有のスマートフォン・タブレットの業務利用（BYOD：Bring Your Own Deviceと呼びます）においてもセキュリティ対策の考え方は同じですが、まだまだ発展途上であり、OSも日々アップデートしています。セキュリティ対策ソフトもPCとは機能が違うものもありますので、個人が使用するスマートフォン・タブレットのOSとバージョン、セキュリティ対策ソフト等を申告してもらい、最善のセキュリティ対策が施されているか確認し、使用を許可するのか、あるいは業務を限定し社内ネットワークへ接続させないなどリスクを低減できるように、検討すべきです。

① PC のセキュリティ対策

自宅の個人所有PCのセキュリティ対策としては、主にウイルス対策ソフトの導入と適切な設定、及びセキュリティパッチの適用等が挙げられます。これらの対策は、3.2.1項の「PCの健全性の維持・確認」と同様になりますので、詳しくは3.2.1項をご参照ください。

② ソフトウェアの起動制限

自宅の個人所有PCに対して、利用できるソフトウェアを会社が制限することは難しいですが、利用者が意図しないソフトウェアの起動を制限することは検討できると思われます。例えば、P2P(ファイル交換)ソフトなどを介した情報漏えい事件は数多く存在しますが、これらのソフトウェアの起動を制限するソリューションも存在します。

上記で示したウイルス対策ソフトと併用することで、さらにセキュリティを高めることが可能です。

③ 機密文書隔離対策

機密文書の管理として、持ち出し申請と承認を管理し、機密文書のファイル自体を隔離するシステムがあります。このシステムを利用することで、持ち出しファイルと申請ユーザ及び、承認者を管理することが可能となります。

④ VPN 接続中にクライアントに残されたデータを保存させないことで情報漏えいを防止

災害発生時には、たまたま会社支給PCや許可PCを持ち歩いていればそれを自宅に持ち帰りそれを使用して仕事をする、ということも可能ですが、オフィスにPCを置いたまま避難し、そのまま帰宅せざるを得なかった場合など、自宅の個人所有PCからのアクセスを認める必要が出てくるケースもあります。

自宅からリモートアクセスを認めた場合のリスクとして、次のような問題があります。

ア）　端末のセキュリティ

自宅の個人所有PCに適切なセキュリティ対策が十分になされているかどうかは一切不明な上に、Winnyに代表されるP2Pソフトや各種のウイルスに感染している可能性があります。

イ）　ネットワーク

会社のインフラにリモートアクセスして接続してしまうことによるさまざまなリスクがあります。たとえば、ウイルス（ワーム）の感染やインフラへの攻撃、企業ネットワークとインターネットに同時にアクセスできることで企業内情報がWebメール等を通じて漏えいするリスクなどです。

ウ）　ファイル（情報漏えい）

社内にある機密情報を個人所有のPCにコピーできてしまうことによる、情報漏えいのリスクがあります。

SSL-VPN製品において、エンドポイントセキュリティ機能、SSL-VPNトンネルの設定、そしてSSL-VPNセッション終了時にはローカルに保存したファイルやキャッシュをすべて削除する機能等を併用することでセキュリティと利便性とコストのバランスの取れたセキュアリモートアクセスソリューションを実現することが可能です。

まず、端末のセキュリティについてですが、ログオン画面を出す"前"にPC端末にウイルス対策製品やデスクトップファイアウォールが動作しているかの確認、ウイルス定義ファイル(ウイルスパターン情報)が十分に新しいかの確認をして、その検査をパスしないとログオン画面にすら到達できないようにできます。ここでログオン"前"にチェックすることが重要な理由として、仮にキーボードの入力内容を盗み取るキーロガーなどのマ

ルウェア(悪意あるソフトウェア)が動作している場合、ログオン後にそれをチェックしていては手遅れになるからです。

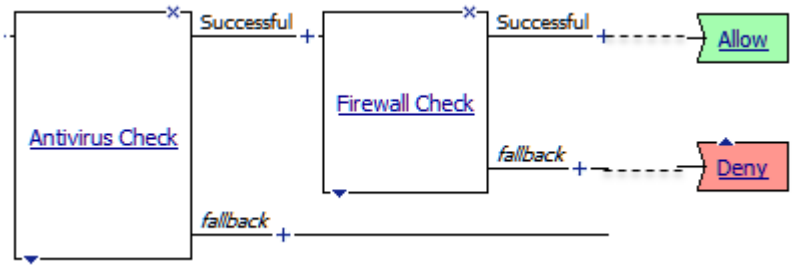

図 4　ウイルス対策製品とデスクトップファイアウォールの動作チェック

次に、SSL-VPNトンネル接続中はリモート拠点からもイントラネット経由からもインターネットへはアクセスできなくする必要があります。

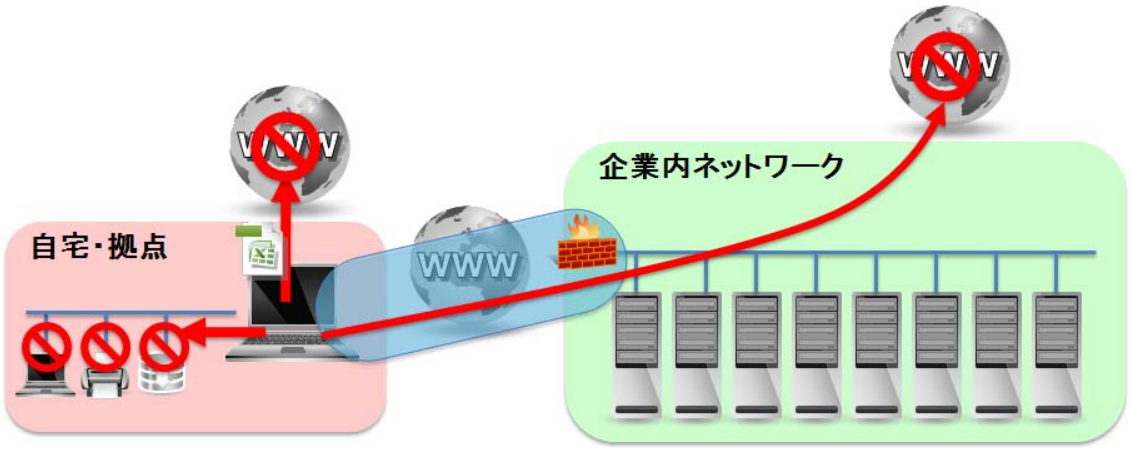

図 5　インターネットへのアクセス制限

そして社内ファイルサーバなどを利用していったんPC上にファイルを保存しても、それを端末に残さないようにしたり、印刷やUSBメモリへのコピーをさせないようにするなどの対策が必要になります。

こうした機能を利用しながら適切なSSL-VPNトンネル設定、エンドポイントセキュリティ機能を併用することで、シンクライアントほどではありませんが、セキュリティレベルを安価にある程度高めることが可能になります。

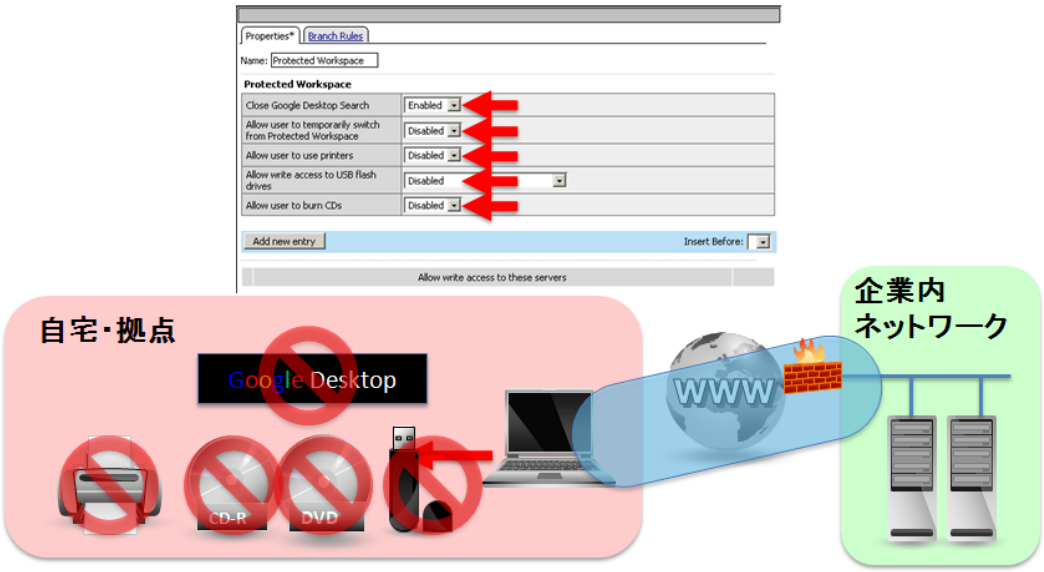

図 6　各種記録媒体や端末への保存制限

(3) モバイル機器の情報セキュリティ対策

電車内や喫茶店などで、PCを操作しているビジネスマンをよく見かけます。ノートPCの性能向上、街中でのネットワーク環境の向上により、オフィスの環境をそのまま職場外で利用できるため、こうした環境で業務遂行をしたくなるのも当然でしょう。しかしモバイル機器には、情報漏えいや社内ネットワークへのアクセスなど、セキュリティ上解決すべき課題も多くあります。

モバイル機器の最大のリスクは紛失盗難による情報漏えいです。電車内に鞄ごと置忘れたり、ひったくりや車上荒し、空き巣などで生じます。JNSAが集計している情報セキュリティインシデントに関する調査でも、紛失置忘れ、盗難ともこれまで毎年100件以上報告されてきました。自宅での盗難対策としては、盗難防止ワイヤーで固定したり鍵のかかる場所に保管するなどの方法が考えられるものの、盗難・紛失による事故を前提とした対策を取ることも重要です。対策としては、PCを盗まれても、第三者がディスク内の情報を解読できないようにすることや、PCには機密情報を保管しないようにすることなどが挙げられます。

以下では、紛失、置忘れ、盗難、ネットワーク侵入等、モバイル機器（モバイルPC、携帯電話、スマートフォン）における各種のリスクに備えるための必要なセキュリティ対策について説明します。

①　HDD（もしくはファイル）の暗号化

電源OFF時に、HDDを別のコンピュータで解析することを防止するために、HDD暗号化ツールを使用します。HDD全体を暗号化するとファイル名も見えないため、安全性が高まります。また、操作上は何も意識をしないので、暗号化し忘れることはありま

せん。一部のPCでは、TPM（Trusted Platform Module）と呼ばれるセキュリティチップを搭載し、HDDから物理的に切り離して暗号鍵をTPMに保存することで、PCの紛失盗難時にも、HDD内の暗号化ファイルの復号化をほぼ不可能にすることができます。

② パスワードの設定

HDDを暗号化していても、OSにログオンした状態では、ファイルの中身が見えてしまいます。また、HDD暗号化をしていない場合は、パスワードにより保護します。

③ パワーオンパスワード（BIOS パスワード）の設定

PCの起動時に認証を行います。

④ ログオンユーザのパスワードの設定

OSログオン時やスタンバイの復帰時に認証を行います。一部のノートPCやUSBメモリには指紋認証デバイスを搭載したものもあり、パスワードと併用して生体認証を用いることもできる。また、携帯やスマートフォンでは、パスワードの文字数が少ないため頻繁に変更するなどの工夫も必要です。

⑤ ネットワークからの防御

PCをインターネットに接続して使う場合、ネットワークからの防御も考慮しなくてはなりません。OSにはさまざまな機能がありますが、使わない機能や、インターネットとは無関係の機能もあります。これらの機能が知らない間にウイルスに感染する、侵入されるといった行為の原因となる場合も多く、対策が必要です。

ア） OS の弱点を修正する

OSの脆弱性を修正したプログラム（Service Packを含む）を適用し、最新の状態を保つ。

イ） セキュリティ対策ソフトウェアを導入する

パーソナルファイアウォールソフトを導入する。ウイルス対策ソフトを導入する。URLフィルタソフトやスパイウェア駆除ツールを導入する[18]。

⑥ キャリアのサービス

携帯やスマートフォンでは、キャリアがセキュリティサービスを提供しています。

[18] 会社支給の PC であれば、これらは設定されていることが一般的です。ただし、社内では自動的に最新の状態に更新される設定であっても、ウイルス対策ソフトの「パターンファイル」の更新サーバが社内にあり、VPN で接続しないと更新されない場合もあるので注意する必要があります。

ア）　遠隔データ消去機能

紛失盗難時に、遠隔操作により「アドレス帳の削除」や「端末を初期化」するサービスです。

イ）　オンラインバックアップ

アドレス帳など、キャリアにバックアップし、万一の紛失の際、どんな情報が漏えいしたか確認できます。

(4) 無線 LAN の情報セキュリティ対策

無線LANの情報セキュリティ対策については、親機の設定と、子機の設定が挙げられます。正しく設定を行わない場合には、以下の脅威（危険）があります。

- 通信内容を傍受され、見られてしまう。
- 不正に家庭内のネットワークに侵入される。または、迷惑メール等の踏み台になってしまう。

通信内容を見られてしまうことを防ぐ為には、親機と子機を正しく設定する必要があります。また、ネットワークに侵入される、踏み台になってしまうことを防ぐには、主に親機の設定を確実にする必要があります。

以下にて、具体的な設定・確認項目について説明します。

①　子機の設定・確認

子機については、少なくとも以下のような設定、確認が必要でしょう。

- 意図した通信先（親機）に接続しているか？を確認するためにSSIDをチェックする。
- 意図した通信手段（暗号方式の設定）になっているかを確認する。

意図した通信先に接続しているか？を確認せずに、無線LANを利用すると、自動的にセキュアでない通信手段によって接続する可能性があり、通信内容を傍受されてしまう危険性があります。

また、意図した通信手段（暗号方式の設定）になっているかを確認せずに、無線LANを利用すると、上記と同様に、通信内容を傍受されてしまう危険性があります。では、選択すべきでない暗号方式の設定は、どのような方式なのかについては、親機の設定方法で説明します。

②　親機の設定・確認

親機については、少なくとも以下のような設定、確認が必要でしょう。

- 暗号化方式の設定
- SSIDの設定
- MACアドレスフィルタリング

暗号方式については、以下のような種類があり、現状では、WEPは強度が不十分であり、選択すべきではないとされています。

表 7　無線 LAN の暗号化方式の比較

方式名称	推奨など
WEP	選択すべきでない。他の設定に切り替える。
WPA（TKIP）	WEP の代替として利用されている方式。
WPA2（AES）	市販されている主な製品の中で最も推奨されている設定。

SSIDは、各無線LANメーカーによって、すでに設定されて状態で販売されています。このSSIDは、他人の子機からも確認できるため、無線LAN（親機）の存在を知らせることにもなります。そのため、「ステルス機能」を有効にすることで、周辺機器に発信するビーコン信号を停止し、他の子機に親機の存在を見えなくすることもできます。また、意図していない周辺機器や他人の子機に対して親機を応答させないために、MACアドレスによるフィルタリング設定も可能です。

これらの設定以外にも、現在では、様々な機能があります。例えば、現在販売されている無線LAN製品では、「特定の暗号方式に限定する機能」もあり、この設定を有効にすることで、弱い暗号方式にレベルダウンすることを防ぐことができます。さらに、上記の設定を自動的に一括で設定できる「AOSS」等もあります。また、親機に「通信ログ」設定機能や、通信（プロトコル）や接続しないサイト等を制御する機能もあるので、これらを組み合わせて、よりセキュアな無線LAN環境を構築することを推奨します。

なお、無線LANは、購入したまま（出荷時状態）でも利用できますが、SSIDによって製造メーカーがわかること、特定された製造メーカーによっては、親機の設定用の初期IDや初期パスワードなどが調べることでわかってしまう可能性もあります。そのため、少なくとも、SSIDと暗号方式を設定する必要があります。また、踏み台にならないためには、少なくとも親機において通信ログを確認する必要があります。

すでに上記に関する設定方法や確認方法は、各種の情報が公開されていますので、詳しくは、下記のサイトを参考に設定や確認を実施してください。

- 一般利用者のための情報セキュリティ対策-実践編　安全な無線LANの利用（総務省）
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_enduser/ippan06.htm
- 無線LANのセキュリティに関する注意（IPA：情報処理推進機構）
  http://www.ipa.go.jp/security/ciadr/wirelesslan.html
- 無線LANのセキュリティに関するガイドライン（改訂版）（JEITA：電子情報技術産業協会）
  http://it.jeita.or.jp/perinfo/committee/pc/wirelessLAN2/

3.2.3　職場外でのネットワーク接続

(1) 物理的な接続形態

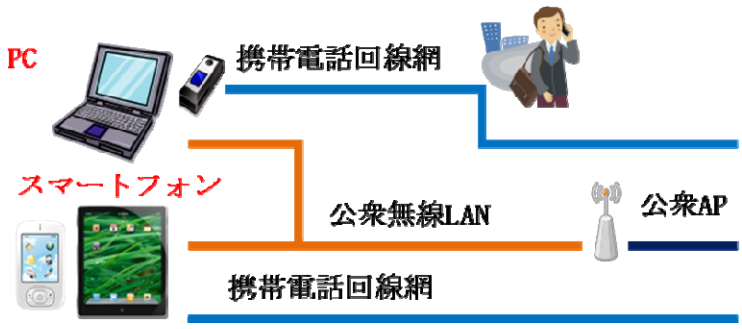

図 7　職場外での接続形態

職場外で、PCやスマートフォン・タブレットを使用する場合の接続形態には2種類あります。PCの場合、データ通信カード等を用いて携帯電話回線網（3G/4G/WiMAX）に接続する方法と、公衆無線LANに接続する方法です。

駅や飲食店など、街中のさまざまなところにアクセスポイント（AP）と呼ばれる公衆無線LANを利用できるエリアが広がっています。公衆無線LANのアクセスポイントの中には、認証無しで接続できるアクセスポイント（鍵マークの付いていないアクセスポイントで「野良WiFi」などと呼ばれます）も多くあります。これらの通信は暗号化されていないため、通信の内容が傍受される可能性があります。認証・暗号化されていないアクセスポイント、所有者不明のアクセスポイントへの接続は避け、契約している公衆無線LANサービス以外への接続はしないようにすべきです。

一方で、暗号化設定がなされているアクセスポイントを利用する場合も、「アクセスポイントのなりすまし」による攻撃が行われる可能性があります。攻撃者は正しいアクセスポイントと同じSSIDとパスワードを設定した偽アクセスポイントを設置し、利用者が誤って接続するのを待ちます。そしてその偽アクセスポイントを通じてやりとりされる情報を傍受するのです。こうした攻撃に対処するには、VPN接続を用いて通信内容を暗号化するのが有効です。

なお、携帯電話回線網（3G/4G/WiMAX）は、携帯事業者が提供しているため、通信が傍受されることはありません。VPNを使えない状況で業務に関わる情報のやりとりを行う必要がある場合、WiFi接続を「使わない」設定にして、こうした携帯電話回線網での接続を行うことを心がけるべきです。

(2) VPN サービス

代表的な接続方式ごとに、以下に特徴を説明します。

① L2TP/IPSec

IPSecはIP通信のデータを暗号化して送信元のIPアドレスの真正性(詐称されていないこと)と、送られるデータの内容の真正性(改ざんされていないこと)を保証する仕組みで、RFC 2401～2412、RFC 2451などで規定されているIPの拡張プロトコルです。

もともとIPアドレスが固定されて動的に変わることのない環境で使われることを前提にしていたため、通信装置同士の認証機能はあるものの、リモート接続するユーザに対する認証を行う仕組みはありませんでした。

そこで、RFC3193で標準化されたL2TP+IPSecによる仕組みでIPSecとユーザ認証の両方を行えるようにした仕組みが近年では一般的であり、さまざまなルータ機器だけでなく、Windows ServerやMac OS X ServerなどもL2TP/IPSecによるVPNの仕組みは標準で備えています。また後述しますSSL-VPNのようにPPPフレームのカプセル化によるオーバーヘッドもないため、スループットの面ではいったん接続さえできてしまえば高速に通信できるというメリットがあります。

その一方でIPSecはその通信のために4500/UDP、500/UDPといったポートで接続可能である必要があるため、たとえば端末がケーブルテレビなどのインターネット接続やホテル、出向先のオフィスなどの環境およびセキュリティポリシー(インターネットアクセスはHTTPプロキシ経由でないと認められていないなど)によってこれらのポートが開いていない場合に、接続できないこともあります。

② SSL-VPN

SSL-VPNというと、HTTPSを使うことからリバースプロキシの一種だと言われることもよくあります。実際のところSSL-VPN装置ではリバースプロキシの形でHTTPSコンテンツをインターネット側に提供する形の機能もあるものも多くありますが、リバースプロキシに関しては後述のWebアプリケーション/SSOの部分で紹介いたします。

SSL-VPNトンネルは、L2TP/IPSecによるリモートアクセスと同じように、企業ネットワーク外、たとえば自宅やインターネットカフェ、出張出向先などの拠点から安全に企業ネットワークに接続し、端末が社内にいるのと全く同じように利用できるような環境を提供します。これによりオフィスの外にいても、社内のファイルサーバへのファイル共有、メールやカレンダー、業務アプリケーションなどをそのまま利用可能になります。

そのときに使用するプロトコルがHTTPSなので、HTTPプロキシ経由でも接続が可能であること、HTTPSでインターネットにアクセス可能であれば利用できることからL2TP/IPsecによるリモートアクセスに比べて接続可能な機会が格段に多くなるのが特徴です。

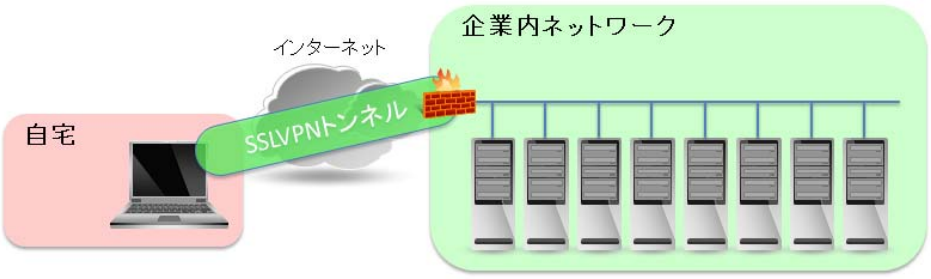

図 8　SSL-VPN の概念図

一方、SSL-VPNでは、PPPフレームをHTTPSの中にカプセル化して通信を行うため、L2TP/IPSecに比べるとスループット(通信速度)の面では劣ると言われてきました。ただし、リモート接続環境においてはむしろ接続環境自体がボトルネックになることが多いこと、さらにプロセッサの劇的な性能向上や後に触れるDTLSが利用できるものも出てきたことで、最近ではスループットが問題になることはほとんどなくなっています。

SSL-VPN接続時の具体的なイメージは次ページのようになります。接続元のPCの実際のIPアドレスとは別に仮想VPNアドレスを払い出し、その仮想VPNアドレスからの通信とすることが可能です（NATをかけることも可能です）。社内からのアクセスとは区別することができるほか、個人または端末毎に異なる仮想VPNアドレスを割り当てることもできるため、いつ、誰がどこからアクセスしているのかをきちんと記録して監査証跡を取るというような運用がなされているケースが一般的です。

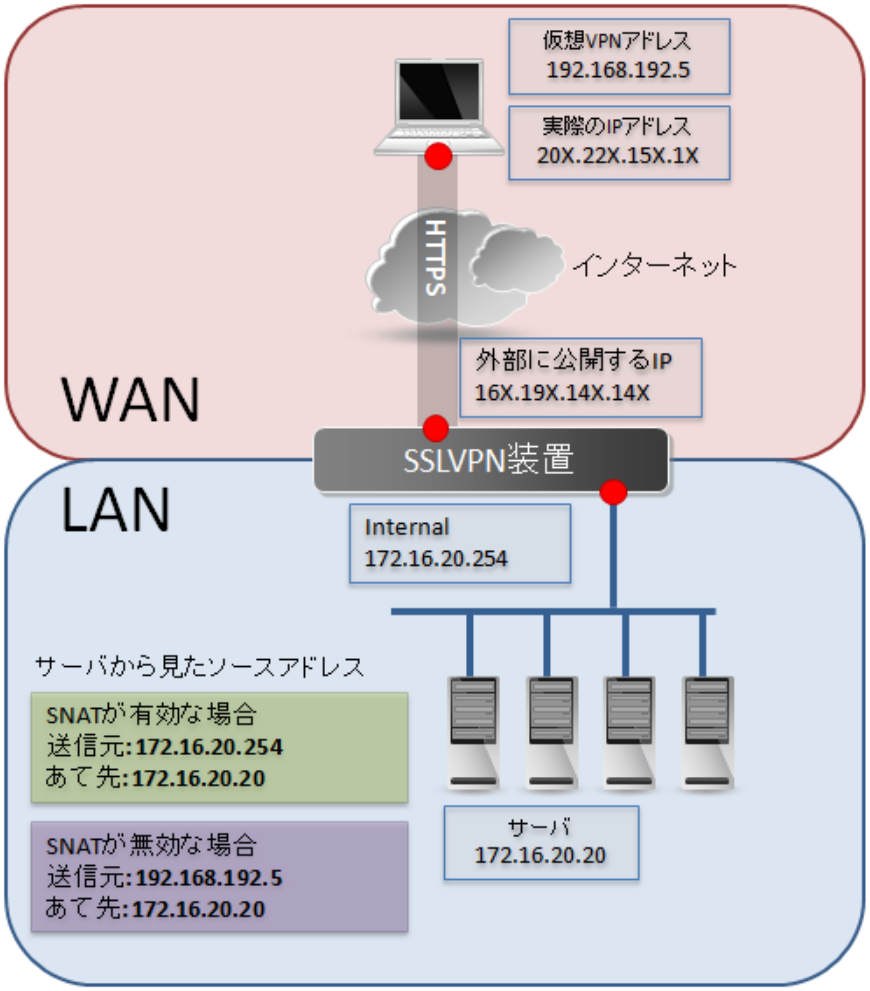

図 9　SSL-VPN 装置による接続の概念図

(3) 遠隔情報同期サービス（ActiveSync の例）

ActiveSyncは主にiPhoneやAndroid、Windows Mobile/Windows Phoneなどの携帯情報端末で、電子メール、カレンダー(予定表)、タスクリスト、連絡先、メモなどの情報を同期することができます。実態はHTTP/HTTPSプロトコルを使用していますので、3GネットワークやWifiなどインターネット接続可能な端末であれば、どこでも社内リソースに参照が可能な環境を提供できます。同様のソリューションとしてBlackBerry端末もBlackBerry Enterprise Service(ブラックベリーエンタープライズサービス)が挙げられます。

ActiveSyncでは、通常ActiveDirectoryのIDとパスワードを使用して認証することになりますので、私物のiPhoneなどでも設定してしまえば簡単に利用できてしまう問題もあります。またExchange Server(IIS)をインターネットから直接アクセスできる環境に置く必要があるため、セキュリティ上の懸念もあります。

こうした課題を解決するために、SSL-VPN製品や高機能な負荷分散装置(アプリケ

ーションデリバリーコントローラー)の中には、ActiveSync用のリバースプロキシとして動作する機能をもつものもあり、「Windowsをインターネットに直接さらさなくて済む」「クライアント証明書による認証やデバイス認証機能の追加」「ActiveSyncに特化したウェブアプリケーションファイアウォール(WAF)機能を提供することによりDoS/DDoS(大量アクセス)攻撃、BruteForce(パスワード総当たり)攻撃から保護」などのセキュリティおよび運用上のメリットを提供できる製品もあります。

コラム　ActiveSync とパスワード変更時のアカウントロックの悲劇

企業において、ActiveSync を利用している端末と PC で同一の ActiveDirectory（AD）を使用しているケースは多いかと思います。その AD 上でユーザーアカウントのパスワードポリシーを「x 日毎に変更を強制」や「n 分以内に m 回パスワードを間違えたらアカウントをロックする」というように厳格に設定している場合があります。この厳格に設定したポリシーに従い、ユーザが PC でパスワードを変更した後、ActiveSync を利用しているスマートデバイス上で ActiveSync のパスワード変更をし忘れることがよくあります。ActiveSync のパスワード変更をし忘れることで、スマートフォン上に設定・保存されたままの古いパスワードで自動的に ActiveSync の同期失敗と再試行が短期間に行われてしまいます。その結果、当該アカウントがロックされ、PC もスマートデバイスも利用できないという事態が発生することがあります。結果として、情報システム部門への対応依頼が増え、対応工数が増えるという事態にもなりかねません。

このような事態を防ぐために、例えば米 F5 ネットワークス社の BIG-IP APM モジュールなどのアクセスポリシー制御機能を持つアプリケーションデリバリーコントローラーを間に設置して、AD の認証に一度失敗したユーザーは n 分間は再ログオンできないようにする、という設定を施し、AD への問い合わせ頻度を抑制することで、ユーザー側にパスワード変更を実施した為、同期に失敗しているということを認識させることが可能となり、ユーザにとって、予期しないアカウントロックの発生を未然に防ぐことができます。

(4) Web アプリケーションにおけるシングルサインオン(SSO)

メールやカレンダー、タスクリストやスケジュール、業務上の承認フローや勤怠管理、ファイルサーバなどの社内業務で使用されるさまざまなアプリケーションをWebアプリケーション化することで、今までさまざまなポートを開けたりそれぞれのプロトコルについてSSL対応したりするなどの構成上の複雑さを解決し、Webアプリケーションとして利用可能な環境を提供する方法も最近ではよく見られる形態です。

また、こうしたイントラネットでの利用だけではなく、いわゆるエクストラネットでの利用、たとえば製造業など、多くの部品サプライヤとの円滑なコミュニケーションを図り業務を推進する目的で受発注管理などの業務システムをWebアプリケーション化して、どこからでも利用可能にする仕組みを構築しているケースがあります。

このメリットとして、ブラウザのみでアクセス可能なため、端末を問わずに利用可能になるというものがあります。こうしたWebベースのアプリケーションが サイロ型でシステム毎に異なる認証方法・認証システムを用いている場合、その運用管理が複雑になり、システムの追加のたびに認証システムも含めて全てゼロから作り直していくという従来の方法を見直して、一つの大型の統合認証レイヤーを構築し、既存の認証基盤に基づいて認証・認可(アクセス権の制御)を行うという新しい方法でWebアプリケーションへのアクセスを一本化して、システムの単純化、運用機器点数の削減および運用にかかる手間を減らすことで大幅なコスト削減を実現するというダイナミック・サービス・モデルという考え方も最近では注目されてきています。

統合的に認証を束ねてシングルサインオンを実現する方法として、SAMLやOpenIDといった複数サイト間での信頼関係を結ぶ方法があり、今後普及するものと注目されています。一方で、既存のWebアプリケーションに対して少ない手間でシングルサインオンを実現する方法として、認証・認可のプロキシ、つまりアクセスポリシー管理製品を使用するという考え方が挙げられます。

高機能な負荷分散装置(アプリケーションデリバリーコントローラー)の中には、リバースプロキシとして動作しながら認証基盤との情報をやりとりし、また各 Webアプリケーションの認証方法(フォームにID/Passwordを入れるフォーム認証、HTTP Basic認証、NTLMv1/v2認証、特定のHTTPヘッダに認証情報を入れておく方法など)を吸収しながら、いったんリバースプロキシの認証を通れば各Webアプリケーションへの認証は全てシングルサインオン(SSO)で実現することのできる製品もあり、注目されてきています。

コラム　SSLVPN と UDP アプリケーションは相性が悪いこともあるって本当？

SSLVPN トンネルは、リモートアクセスコントローラーと拠点にある接続元との間のインターネットを利用する部分は HTTPS が利用され、PPP フレームがカプセル化されて HTTPS の中を通る仕組みで拠点間を接続し、イントラネットにいるのと同じような作業環境を提供する仕組みになっています。SSLVPN トンネル接続中は IP 到達可能な状態になるため、その上で動作する IP レベルのアプリケーションは TCP も UDP もどちらも利用可能です。

ネットワークの品質が十分に高ければほとんど問題になることはないのですが、リモート端末の存在する場所の電波状況が悪いなどの理由でパケットのロストと再送が発生するような環境で SSLVPN トンネルを張り、かつ VoIP や PCoIP などの UDP アプリケーションを利用している場合に、問題が起きることがあります。

端末とリモートアクセスコントローラーの間は SSLVPN の名の通り HTTPS での通信、つまり TCP なのでパケットのロストがあると再送されますが、その上で UDP アプリケーションを利用していると、UDP では不要なパケットの重複が発生し、その結果 SSLVPN トンネル自体が安定しなくなることがあるという問題が起きることがあります。

新しい SSLVPN 装置では、HTTPS に加えて DTLS※1 を利用することで、UDP を使用した SSLVPN トンネルを利用することができるものもあり、UDP アプリケーションを利用したときに高いパフォーマンスが出るだけでなく、安定したネットワークの利用が可能になると高く評価されています。

※1　DTLS は、RFC 4347 で策定され、OpenSSL でも実装されています。
　　TLS の UDP バージョンのようなものです。　http://tools.ietf.org/html/rfc4347

3.2.4　認証

(1) デバイスの認証

自宅にある私物のデバイスであっても、会社で支給されるデバイスであっても、デバイスを特定した上で許可されたデバイスのみ接続を許可するように設定することで、許可されていないデバイスによる第三者からのなりすまし試行、不正なアクセスを防ぐことができます。デバイスを特定する方法として、いくつかの方法と課題、ベストプラクティスについて紹介いたします。

① 証明書 (Windows PC、iPhone、Android 4.0)

クライアント証明書認証は強固なクライアント認証の方法の一つですが、証明書の配布と失効管理の面で運用負荷がかかります。たとえば配布面において、ファイルで証明書をメールやUSBメモリなどファイルで存在する形で配布してしまうとその証明書を複数の許可されていないデバイスにまで設定されてしまうなどのリスクが発生します。

また、FireFoxにクライアント証明書をインポートした場合、エクスポートも可能になるため、結局証明書が再利用されてしまうリスクが発生します。そこで、マシン証明書を使用するという方法も一つの強固な方法です。マシン証明書とは、使用する証明書自体はただの証明書なのでクライアント証明書と同様ですが、証明書が格納される領域がマシンストアとなるため、容易には取り出すことができなくなる利点があります。

また証明書の配付において、情報システム部でいったんPCを預かり、エクスポートできないような形でクライアント証明書をインストールして利用できるようにする、という運用がかかりますが、たとえば遠隔地や自宅にあるPCをアクセス許可したい場合に、物理的にPCを持ってくることができないため、現実的にはかなり厳しいものとなるでしょう。

このようなファイルの形でのクライアント証明書の代わりに、USBトークン(あるいはUSBドングル)と呼ばれる、USBデバイスをPCに装着したときにのみクライアント証明書として利用可能な製品もありますが、物理デバイスとなるため、最初から遠隔地にある人への配布が課題になることもあります。また、配布運用における負荷を低減することのできる製品もあり、たとえばインターネット経由でアクセスし、PCのブラウザ経由でワンクリックでマシン証明書をインストールしたり、iPhoneにワンクリックで証明書をインストールしたりできるだけではなく、管理者も容易に失効管理ができるような高度な証明書管理製品も出てきており、こうしたソリューションを支える強力な製品として活用されてきています。

コラム　システム管理者の視点でみる証明書失効管理の課題と解決策

多要素認証の仕組みを導入しているシステムにおいてはユーザーの退職・デバイス紛失などのタイミングでクライアント証明書を失効させるケースは頻繁にあるかと思われます。

クライアント証明書の失効管理には、CRL（Certificate Revocation List）、OCSP（Online Certificate Status Protocol）、CRLDP（CRL Distribution Points）等を用いる方法があります。多数のユーザーが利用するシステムにおいては、CRL 自体が巨大なデータになり、パフォーマンスが劣化し、最悪の場合、読み込みができなくなる事態が発生することがあります。また、OCSP, CRLDP を使用する場合、それらのサーバーがダウンしてしまうと、認証ができなくなり、システム利用に大きな影響を及ぼしてしまうことにつながります。OCSP, CRLDP のサーバーの冗長性を考慮すると、ハードウェア台数が増加し、システムの肥大化、運用・保守コストの増加を招くことになります。こういった課題があることから、証明書の失効管理の方法として既存の認証サーバーを利用する方式もあります。

例えば、米 F5 ネットワークス社の BIG-IP APM モジュールなどのアクセスポリシー制御機能を持つアプリケーションデリバリーコントローラーでは柔軟なアクセスポリシー制御を設定することが可能です。同製品において、クライアント証明書と RADIUS の ID とパスワードによる二要素認証をする場合に、ユーザーの RADIUS Attribute（RADIUS 属性情報）の中にクライアント証明書のシリアル番号も合わせて記録しておき、クライアント証明書のシリアル番号が該当ユーザーの RADIUS Attribute に含まれていることをもってクライアント証明書が有効であると判断し、アクセス許可をするという方法が採用されています。この方法では使用するプロトコルは異なりますが、セキュリティ上のロジックとしても CRL や OCSP と等価であること、冗長構成の考慮も認証サーバーについてのみ考えればよいこと、運用管理を認証サーバー側の操作で一元化できるメリットもあるこ

② **デバイス固有情報** (Windows PC、iPhone、Android)

デバイスを固定するために、ネットワークカードが持つ固有情報としてMACアドレスがあげられます。ただ、Windowsにおいてはドライバの設定レジストリの設定により簡単にMACアドレスの変更が可能になり、偽装も容易なためセキュリティ上ほとんど意味をなしません。そのため、Windows PCの場合は上記のマシン証明書を使用するか、そのほかの偽装困難なものとしてたとえばハードディスクのデバイスシリアル番号、マザーボードのデバイスシリアル番号などをキーにして許可されているデバイスかどうかを判断することが一つの強力なデバイス認証の方法です。

またiPhone、Androidといった端末には電話固有のIMEI番号という個体識別IDがあり、IMEI番号をキーにすることも可能です。ただ、電話ではないiPod touchやWifi版iPadではIMEI番号を持たないため、これらの場合はMACアドレスをキーにするのも一つの方法でしょう。

(2) 人の認証

システム利用における人の認証とは、本人認証を意味します。本人認証とは、ある人がアクセス対象に自分が確かに本人であることを証明することとなります。

本人認証の要素として、大きく分けて次の3つが利用されています。

- WHAT YOU KNOW（本人だけが知っていること）：パスワード、秘密の質問等
- WHAT YOU HAVE（本人だけが持っているもの）：ハードウェアトークン、証明書、ICカード等
- WHAT YOU ARE（本人であるという生体的特徴）：指紋、虹彩、静脈、声紋等

各要素にはそれぞれ特長があり、利用用途に応じて適切な要素が選択されています。それぞれの特長、問題点を見てみましょう。

① 固定パスワード

システム利用時の認証として最も基本的な手法です。複雑なパスワードの設定や定期変更ルールの徹底により、ある程度の強度を保つことは可能です。ただし、近年増えつつあるフィッシングや不正プログラム、従来からある盗聴・盗み見、パスワードの推測等の脅威に弱いため、社内における業務システムへのアクセス等、ある程度安全性が担保された用途で利用されることが多くなっています。

② ワンタイムパスワード

特定のルール(時刻ベース等)により生成されるランダムな値をパスワードとして利用する手法です。そのランダム性、有効期間の短さ等により、固定パスワードの弱点を克服した手法となります。ハードウェアトークン、ソフトウェアトークン等の生成器と組み合わせることで、「知っていること」と「持っているもの」の二要素認証を構成することができ、この構成で利用されることが増えています。巧妙に仕組まれたフィッシングやトークンの管理について注意が必要ですが、比較的安価に一定レベルの認証強化が可能です。

③ 生体認証(指紋、虹彩、静脈、声紋等)

本人のみが持つ生体的特徴を元に認証を行う手法です。認証強度は実装方法に依存しますが、その実装が堅固であるという前提に立てば、もっとも認証要素の複製が困難であると言えます。データセンターや研究所等、高レベルのセキュリティが要求される施設の物理セキュリティとしても利用されます。リモートアクセス用途では、高価なソリューションとなることが想定されますが、高レベルのセキュリティを必要とするシステムでは利用の検討対象となります。一点問題があるとすれば、万が一認証データが漏えいした場合、そのデータが生体的特徴という点から変更や再設定が不可能となり、

取り返しのつかない状態となるということがあげられます。

④ リスクベース認証

本人認証やデバイス認証を補完する機能として、近年利用されることが増えてきた手法です。ユーザ情報や端末の環境情報(ブラウザ情報、OS情報等)、アクセス元情報等の各種情報から、本人のアクセスと不正アクセスとの差異を検出する仕組みとなっています。ID/パスワード+トークン(証明書、生体認証)と、このリスクベース認証を組み合わせ、最悪の事態に備えてもう一段防御ラインを用意する形での利用が多くなっています。難点は通常の認証システムに加えリスクベース認証用のシステムを導入することになるため、高価なソリューションとなりがちであることです。ただし、現在は安価なサービス型で提供されているものもあり、認証強化の手法として広がりつつあります。

上記に紹介した認証方式を理解し、利用対象システムの用途、重要度、想定される脅威に応じた適切な組み合わせで認証レベルを設定することを推奨します。

コラム　パスワード認証だけで大丈夫？

最近の大規模な個人情報漏えい事件をはじめとして、セキュリティインシデントが多発しているように見えます。そのような一連のインシデントに絡んで、興味深い指摘がありました。

「某所の漏えいデータを解析した結果、約９割のアカウントが別のサービスで同一のパスワードを利用していたことがわかった。」

現在、巧妙化するフィッシング手法、増加する不正プログラム(malware)等を背景とし、ユーザ ID/パスワードの不正取得による成りすましの発生する可能性は非常に高まっています。また、クラウドサービスの利用や本ガイドブックのターゲットでもある在宅勤務、あるいはスマートデバイスの利用の広がりにより、インターネット上での ID/パスワードの利用機会はますます増えています。特定組織を標的としたフィッシングあるいはソーシャルエンジニアリングを駆使した攻撃により ID/パスワードが漏えいした場合は、攻撃者のモチベーションが明確(金銭目的、機密情報目的等)であるため、その攻撃の結果として発生する被害は非常に深刻なものとなります。このような状況で、パスワードの設定ルールや運用ルールだけで、パスワードの不正取得による成りすましを防ぐことができるでしょうか？

特定サービスにおいてセキュリティを強化していても、ID/パスワードの使いまわしが行われていた場合、他の事業者にて ID/パスワード漏えいが起きることで被害を受ける可能性もあります。「パスワード認証 is Dead」これが結論です。そろそろ前提条件の見直しが必要ではないでしょうか？ 「パスワードは漏えいするものである」これが新しい前提です。「パスワードをいかに守るか」だけでなく、漏れても影響の少ないように対策を考えたほうがよいのではないでしょうか。もちろん守るべきシステムの価値と対策にかける費用のバランスから、これまでどおりパスワードだけの認証を選択することもあるでしょう。しかし、少なくとも「パスワード＋もう１要素」の「多要素認証」を認証方式の常識、スタート地点として考えてみてはいかがでしょうか？ 追加する要素は、証明書、ワンタイムパスワード、ハードウェアトークン、生体認証等、強度・費用・管理工数面でさまざまな特徴を持つソリューションが存在します。重要なシステムへのアクセスであれば、認証時の各種情報から成りすましを検出する「リスクベース認証」を組み合わせるのもよいでしょう。インターネット上のサービスを組み合わせて利用する機会が増える中、認証方式の常識も変化を迫られている、一連のインシデントからそんなことを考えるのは職業ゆえに、でしょうか。

3.2.5　紙媒体を持ち出して仕事する

(1) 紙媒体のリスク

紙媒体を持ち出す際のリスクを考える前に、なぜ持ち出してしまうのか、その理由を考えてみましょう。

- データに比べて持ち出しやすい
- 閲覧するためのツールが不要
- 必要なものだけ選ぶのが比較的容易
- 他人に気付かれずにコッソリ持ち出せてしまう

いずれも紙媒体の可搬性があるゆえに発生する行為です。データをPCや持ち出し用の外部メディア(USBメモリなど)へコピーをすることなく、プリントアウトしたものをそのまま持ち出すことができますので、急いでいる時につい、というケースが多いのではないか思います。外出する直前にプリントアウトして、そのままプリンタから持って出るという行動パターンが結構多いのではないでしょうか。

上記の理由を踏まえてリスクを考えてみますと、紙媒体のもっとも大きなリスクは「情報漏えいにつながる何らかの行為を行った場合の追跡が出来ない」という一点につきるのではないかと思います。紙に印刷する前のデジタルデータであれば、システム的（技術的）な管理やコントロールが可能ですが、データを印刷した紙は、管理やコントロールができなくなり、追跡も難しくなります。たとえば、紛失や置き忘れ、盗難といった事故が起こった後に、その紙を追跡することができません。また、コピー機でのコピー、写真撮影、手による書き写しなど、複製を行った場合も、どこにその複製物が存在しているかを追跡することはできません。

プリント時に透かしを入れ、誰が紛失したのかを追跡可能にする方法や、地紋等を特殊なデータを付加して印刷し、印刷した紙をコピーやスキャンした際に、元のデータを見えなくする等の方法もありますが、これらはすべて抑止効果的に機能し、紛失による情報漏えいのリスク低減には寄与しないので、根本的な解決策はないと考えるべきです。

(2) 紙媒体の処分方法

機密文書の処分は、裁断・破砕・溶解処理などを行う専門業者があるので任せるのが安全です。ただし、文書の処理を委託する場合のコストを考える必要がありますので、すべての文書を委託するのではなく、文書の機密性によって処理方法を考えましょう。さらに、専門業者が安全管理を維持するための方策をとっているかを確認する

必要があるでしょう。たとえば、輸送や処理を他の業者に委託することなく、請け負った業者が処理までの行程を直接行っているか、廃棄証明書を発行しているか、などを委託する前に確認をするとよいかと思います。また、下段のコラムにもある通り、求められる機密性によっては、廃棄の方法によっては復元されてしまう場合もあるので、「その業者が、どのように廃棄するのか？」を事前に確認しておく必要もあります。

コラム　シュレッダーで裁断された紙からも情報漏洩する

戦時中は紙で情報のやりとりが行われていて、機密保持の目的から紙を短冊状に切って破棄するという方法がとられていました。しかし、手をかければ短冊状の紙を集めて並べ替えて元の文書を復元することが可能になり、より凝った裁断方法が選択されるようになってきました。最近では、裁断された紙を全てスキャナで取り込んでより効率よく復元するというサービスも現れてきており、シュレッダーで裁断するだけでは情報漏洩は防ぐことができなくなってきています。情報の重要度にもよりますが、本当に確実に破棄したい紙文書は、最終的には溶解・焼却などの手続きも必要になってくると言えるでしょう。

3.3 職場とのコミュニケーションの方法

第1章でも述べたように、在宅勤務を行うことでこれまでのオフィスにおける従業員の管理方法がそのまま適用できない場面が生じてきます。特に企業の管理者からみると、部下が見えない場所で業務を行うことに不安を感じることが予想されます。単に業務を円滑に行うためだけでなく、双方の心理的な距離を縮めるためにも、同僚間、在宅勤務者（会社にいる人と在宅勤務者）間で十分なコミュニケーションをとることが重要です。

Computerworldによるアンケート調査によると、東北地方太平洋沖地震の翌週に在宅勤務を実施した企業は、回答企業のうち約20%でした。在宅勤務時のコミュニケーションの方法としては、87.2%が電子メール、73.5%が携帯電話でコミュニケーションを図っています（下図参照）。今回は緊急の事情であり、暫定的な体制のもとで実施されたことによる影響もあると想定されますが、在宅勤務が急激に増加しない限り、日常的なコミュニケーションの延長である電子メール、携帯電話が依然として主流であるものと考えられます。

本章では、電子メール、携帯電話を中心に社内（職場）とのコミュニケーションをセキュリティに考慮しつつ、円滑に行う注意点について説明します。

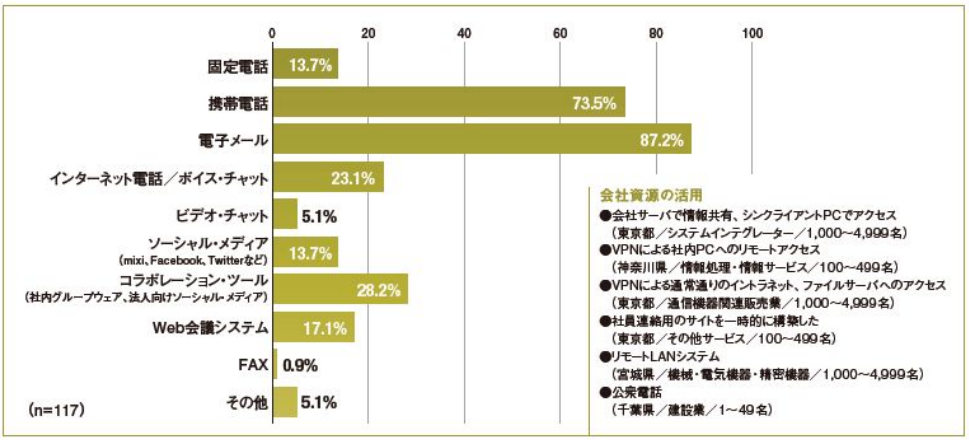

図 10　在宅勤務中、社員間のコミュニケーションに使用した通信手段
（東北地方太平洋沖地震の翌週に在宅勤務を行った 117 名による回答）

出典：非常時における企業の「テレワーク／在宅勤務」体制調査
Computerworld（http://www.computerworld.jp/topics/2011shinsai/192020.html）

3.3.1　テレビ会議とテレビ電話

在宅勤務は、オフィスワークと異なるため、社内や外部との連絡が疎遠になりがちです。そのため、社内や外部とのコミュニケーションツールが重要となりますが、現在は、様々なコミュニケーションツールが提供されているため、各々の特性を活かしたコミュニケーションツールを選択し、利用することが可能です。また、電話やテレビ会議等は、相手先と直接、会話や表情を確認できるため、在宅勤務時には、重要なコミュニケーションツールになります。

この節では、電話やテレビ会議等に代表される以下の5種類のコミュニケーションツールを紹介します。

- 固定電話／携帯電話
- ボイスチャット
- ビデオチャット
- テレビ（Web）会議システム
- IPテレフォニーシステム

上記の5種類のツールを実際に利用した方にも意見を聞き、在宅勤務時の運用を想定した利用方法や留意事項をまとめました。

(1) 共通した利点

はじめに、電話やテレビ会議等を利用し、リアルタイムに社内や外部とコミュニケーションすることによる利点を紹介します。

- リアルタイムにコミュニケーションが可能
- 表情や、言葉の間などから意思疎通が容易
- 在宅勤務での孤独感・疎外感の防止が可能
- 文字ベース（メール）コミュニケーションの補足説明に利用可能

上記の利点は、本項で紹介する5種類のコミュニケーションツールに共通した利点ですが、運用上の注意点や留意事項は、各々のツールによって異なるため、以下に個別で紹介します。コミュニケーションツールの選択にご活用ください。

①　固定電話／携帯電話

電話の利用については、既に固定電話か携帯電話があり、特別なソフトウェアやシステムを必要としないため、すぐに運用することが可能です。一方、通信費用やサービス料に関する処理手続きや、記録を残す場合に問題があります。

ア）　主な利用方法

社用携帯電話／個人の固定電話／携帯電話を使用したコミュニケーションです。1対1の通話に限られますが、個人所有機器にて容易に使用可能です。

イ）　利用上の留意事項

利用にあたっては、下表の内容に留意する必要があります。

表 8　固定電話／携帯電話の利用上の留意事項

コスト	・通話料がかかる ・通信費明細から会社に費用を請求する場合、請求処理のコストがかかる ・発信前に特定の番号を指定して会社払いとなるサービスを利用する場合、サービス料がかかる
記録・情報管理	・音声記録が残らないため、記録を残すものについては議事録が必要

②　ボイスチャット

ボイスチャットの利用については、電話利用に比べ、使用するデバイスとソフトウェア（システムを含む）を確保・配布する必要があります。また、使用するソフトウェアやシステムによっては、社内のポリシーとの調整が必要になり、サービスを受けるためのアカウント情報等のリスク管理面でも検討が必要になります。そのため、導入や運用の前に、これらを調整、検討することが重要になります。

ア）　主な利用方法

スピーカー・マイク／ヘッドセットを接続したPCに専用ソフトウェアをインストールし、インターネット上のサービスのアカウントを取得することにより、同じサービスを使用したPC同士の通話を可能とします。インターネット接続料金を別にすれば基本的に通信費用を考慮することなくコミュニケーションが可能です（使用するサービスによっては、相手先との通話については別途料金が必要となる場合があります）。

基本的には1対1の通話ですが、同じソフトウェア同士の通話では多人数での同時ボイスチャットが可能なものもあります。

イ）　利用上の留意事項

利用にあたっては、下表の内容に留意する必要があります。

表 9　ボイスチャットの利用上の留意事項

コスト	・使用デバイス(マイク・ヘッドセット)を配布する場合のコストがかかる ・通常の電話への通話には料金契約が必要
ポリシー・リスク	・使用するソフトウェアが社内ポリシーで禁止されている場合、社内ポリシーとの調整が必要 ・サービスのアカウント情報は各サービス会社管理となるため、自社でリスク管理ができない
記録・情報管理	・音声記録が残らないため、記録を残すものについては議事録が必要 ・ファイルをやりとりする機能があるものについては、データの送受に配慮が必要

③　ビデオチャット

ビデオチャットの利用については、ボイスチャットの使用デバイスにカメラの追加が必要になります。また、運用・機能面の留意事項として、システムやサービスによっては、コマ切れや音切れが発生し易いこと等が挙げられます。なお、導入・運用前に、調整、検討するべきポイントはボイスチャットとほぼ同様です。

ア）　主な利用方法

スピーカー・マイク／ヘッドセットに加え、カメラを接続したPCに専用ソフトウェアをインストールし、インターネット上のサービスのアカウントを取得することにより、同じサービスを使用したPC同士の動画通話を可能とします。音声に加え、互いの顔が確認できるという利点があります。インターネット接続料金を別にすれば基本的に通信費用を考慮することなくコミュニケーションが可能です（使用するサービスによっては他の電話網との通話については料金契約が必要となる場合があります）。

基本的には1対1の通話ですが、同じソフトウェア同士の通話では多人数でのビデオチャットが可能なものもあります（多人数のビデオチャットでは、利用料金がかかる場合があります）。

イ）　利用上の留意事項

利用にあたっては、下表の内容に留意する必要があります。

表 10　ビデオチャットの利用上の留意事項

コスト	・使用デバイス(カメラ・マイク・ヘッドセット)を配布する場合のコストがかかる ・通常の電話への通話、多人数でのビデオチャットの際には料金契約が必要
ポリシー・リスク	・使用するソフトウェアが社内ポリシーで禁止されている場合、社内ポリシーとの調整が必要 ・サービスのアカウント情報は各サービス会社管理となるため、自社でリスク管理ができない
記録・情報管理	・記録が残らないため、記録を残すものについては議事録が必要 ・ファイルをやりとりする機能があるものについては、データの送受に配慮が必要 ・音声だけの通話に比べ、通信容量が大きいためコマ切れや音切れが発生し易い

④ テレビ（Web）会議システム

テレビ(Web)会議システムは、ビデオチャットと同様の機材(使用デバイス)で利用できます。また、主なサービス形態として専用サーバを利用する場合と、クラウドサービスを利用する場合に分かれ、各々のサービス形態によってコスト面、リスク面が異なります。

ア） 主な利用方法

ビデオチャット同様、スピーカー・マイク／ヘッドセットに加え、カメラを接続したPCにテレビ会議用のソフトウェアをインストールし、テレビ会議システムのWebサイトにアクセスすることでテレビ会議に参加します。ホワイトボード機能、参加者のデスクトップ共有機能、録画機能などが利用でき、会議向けに設計されているという点で前述の個人向けのビデオチャットとは異なります。

また、サービス形態としては、クラウドサービスと専用サーバ利用の2つの形式があります。

イ） 利用上の留意事項

利用にあたっては、下表の内容に留意する必要があります。

表 11　テレビ（Web）会議システムの利用上の留意事項

コスト	・使用デバイス(カメラ・マイク・ヘッドセット)を配布する場合のコストがかかる ・【専用サーバ利用の場合】専用サーバ構築のコストがかかる ・【クラウドサービス利用の場合】サービス利用料のコストがかかる
ポリシー・リスク	・使用するソフトウェアが社内ポリシーで禁止されている場合、社内ポリシーとの調整が必要 ・【クラウドサービス利用の場合】サービスのアカウント情報はサービス会社管理となるため、自社でリスク管理ができない
記録・情報管理	・ファイルをやりとりする機能があるものについては、データの送受に配慮が必要 ・【専用サーバ利用の場合】ＳＳＬ-ＶＰＮ経由で使用する場合、コマ切れや音切れが発生し易い

⑤ IP テレフォニーシステム

IPテレフォニーシステムの利用については、上記の4種類と比較すると、IP電話システムが必要になるという点が異なります。

ア）　主な利用方法

社内電話がソフトウェアによる通話が可能なIP電話システムで構築されている場合、在宅勤務においてもSSL－VPN等のリモートアクセスにより社内と同様の手段で内線通話や外線通話が可能です。

イ）　利用上の留意事項

利用にあたっては、下表の内容に留意する必要があります。

表 12　IP テレフォニーシステムの利用上の留意事項

コスト	・新規でＩＰ電話システムを構築する場合には膨大なコストがかかる
運用・性能面	・ＩＰ電話の仕組みとＳＳＬ－ＶＰＮの仕様が一般的に相性が良くないため、音声品質が悪い（製品によってはカバーできるものもある）。

3.3.2　電子メール

職場とのコミュニケーションの代表的手段といえるのが、すでにコミュニケーションインフラとなって久しい電子メールです。今夏に向けて、早期に在宅勤務の導入・運用を実施する場合、コミュニケーションツールを使い慣れていることが重要になります。そのため、在宅勤務時のコミュニケーションツールとしては、電子メールが利用される機会が最も多いものと考えられます。

電子メールによって得られる主な利点は、以下の3点になります。

- 時間に制約されない
- コミュニケーションとしての履歴が残る
- 同報メール、メーリングリストの活用により関係者と一斉にコミュニケーションが図れる

こうした電子メールについて、在宅勤務での利用方法を電子メールアドレスの選択から検討していきます。

(1) 電子メールアドレスの種類

在宅勤務で利用される電子メールアドレスとしては、以下の3種類が想定されます。

① 会社メールアドレス

会社で割り当てられているメールアドレスであり、ほとんどの場合は会社のドメイン名で付与されます。

② 個人メールアドレス

個人で契約しているISPのメールアドレス、あるはフリーメールアドレスです。

③ 携帯メールアドレス

携帯電話に割り振られたメールアドレスです。

(2) 電子メールアドレスの種類ごとの懸念事項

電子メールを利用するためには、セキュリティ的な配慮と、運用上の懸念事項があります。特に、上記の電子メールアドレス種類によっては、個別に懸念事項があるため、これらを踏まえて導入検討する必要があります。在宅勤務によっては、複数のメールアドレスを併用する場合も想定できますが、主な懸念事項は以下になります。

表 13　機密性に関する作業上のリスク

アドレスの種類	主な懸念事項
会社メールアドレス	在宅勤務で用いるPCで社内イントラへVPN接続可能であれば問題ありませんが、社内LANへアクセスできない場合、メールサーバから受信できる環境をどのように確保するかが課題となります。ただし、会社メールアドレスがクラウドサービスを利用している場合はこの限りではありません。
個人メールアドレス	個人アドレスを使用する場合、家族との共用アドレスは不可とするなどルールの徹底と、本人証明が必須になります。また、メール受信に POP で受信したり、Web メールの際に暗号化されていない HTTP である場合は、通信の盗聴が容易であるため避けるべきです。
携帯メールアドレス	携帯メールアドレスを使用する場合は、本人証明が必須となります。携帯電話の紛失による漏えいの可能性があるため、必要最小限の情報に限定し、個人情報やメールの削除等のルール化が必要になります。

(3) 電子メールのセキュリティ対策と留意事項

在宅勤務時における電子メールのセキュリティ対策は、一般的なセキュリティ対策と変わりありませんが、物理的及び通信路の安全が確保されていない環境で情報が取り扱われるということであり、一般的な勤務時よりも以下の点をより厳密に運用する必要があります。

また、電子メールに利用するシステム（メールクライアントソフト等）やPC（会社支給PCか個人所有PCか）によっても留意事項が異なります。主なセキュリティ対策及び留意事項は以下になります。

表 14　テレワークの効果

セキュリティ対策	・誤送信対策 ・盗聴対策（添付ファイルによるデータの送受では暗号化が必須） ・ログインアカウント／パスワード管理の徹底
留意事項	・自宅の個人所有 PC に受信メールが蓄積される ・会社のメールアドレスのみを利用可能とすると、ドメイン名判定によるメール誤送信対策が徹底しやすくなるため、業務用には会社メールアドレスのみを使用可能とすることが望ましい ・データの送受に関しては、顧客・社外関係者に対しては暗号化してメール。社内とのやりとりに際してはファイルサーバを使用などを検討することが望ましい ・電子メールのみでは説明不足による誤解等が発生しやすくなるため、不明点は電話等で確認することを習慣化する

(4) フィッシングメールや標的型攻撃メールへの対策

コミュニケーション手段として電子メールを活用する場合、フィッシングメール[19]や標的型攻撃メール[20]への対策を強化する必要があります。特に、在宅勤務においては、不審なメールに対して気軽に相談できる環境でなく、また、気の緩みも否めないため被害に遭遇する可能性が高くなると考えられます。

これらへの対策[21]としては以下のようなものがあります。これらの対策に加え、日ごろから他のコミュニケーション手段等も活用し、不審なメールに関する情報共有を密にすることも被害拡大防止には有効です。

① 添付ファイルやリンクに注意し不用意にアクセスしない

常日頃から、受信したメールに添付されているファイルやリンク(ショートリンクを含む)に対して注意する習慣付けるようにし、不用意にファイルを開いたり、リンク先にアクセスしないように心掛ける。

② パスワードで暗号化し添付ファイルを送信する

あらかじめ電子メール以外の方法でパスワードを共有しておき、そのパスワードで暗号化した添付ファイルを送信し、なりすましを検知できるようにします。

③ 電子署名を活用する

電子署名に対応したメールソフトウェアを活用することにより、誰が作成した文面であるのか検証することが可能になります。この電子署名の活用は、在宅勤務に限らず全社的なフィッシングメール対策としてあらかじめ導入を検討しておくことが重要です。

④ パスワードの共用は避ける

万一フィッシングにより、ポータルサイトやゲーム・銀行等のサイトのログイン情報が詐取された場合、業務で使用するサイト(グループウェア等)へ不正アクセスされる可能性があります。業務で使用するパスワードは、個人で利用するサイトとは別々のものに設定する(サービス事業者ごとに別々に設定することが望ましい)ようにします。

---

[19] 不正に第三者を騙り、本物そっくりの電子メール等を用いて個人情報を詐取しようとする電子メール。
[20] 情報詐取を目的として、特定の組織・担当者のみに送られる電子メール。
[21] フィッシング対策の詳細については、フィッシング対策協議会が「フィッシング対策ガイドライン」を発行しているのでご参照ください。 http://www.antiphishing.jp/report/pdf/antiphishing_guide.pdf

3.3.3　データの送受

個人情報や機密情報の有無に関わらず、在宅（職場外）勤務者とデータの送受を行う際には、セキュリティの確保が重要です。この節では、オンラインのデータ送受とセキュリティ上の解決策を説明します。

オンラインでデータの送受をする際の最大の注意点は、盗聴対策です。どのような方法であっても、送受の際にデータが他者に見られないようにする必要があります。また、ファイルをダウンロードするために必要となる認証情報（ユーザID、パスワード）が漏えいすると自社従業員に偽装してデータにアクセスすることが可能になるため、認証情報の管理も重要になります。さらに、社外のサービスを利用する場合には、自社でリスク管理ができないということも留意する必要があります。

なお、物理的なデータの送受については、3.2.2項をご参照ください。

(1) オンラインストレージ（グループウェア含む）

オンラインストレージとは、インターネット上でディスクスペースを貸出すサービスであり、複数のユーザと共有することが可能です。また、グループウェアの追加機能として、ファイル管理を提供するサービスもあります。オンラインストレージを利用する際には、ファイル保存期間、1ファイルの最大アップロード容量、全体の容量などを比較し、どのサービスを利用するかを検討することになります。

さらにセキュリティの観点から、以下の点も考慮する必要があります。

ア）　全社で同じサービスを利用する

部門ごとにバラバラにサービスを利用すると、インターネット上のあちこちにファイルが分散され管理が行き届かない可能性があります。

イ）　ログインパスワード

パスワード及びパスワードの管理には、不正アクセスを防止するため、十分な長さとランダムな文字列を設定する必要があります。また、パスワードの有効期間等は、全社統一ルールを決めることを推奨します。

ウ）　通信の暗号化

盗聴を防止するため、サービスへのログインおよびファイルの送受の際に、通信が暗号化されるSSL(HTTPS)を使用するサービスを選ぶことを推奨します。一方、何らかの理由で、これらのサービスを利用できない場合は、送受するファイル自体にパスワードを設定し、他者に情報を見られないようにする等の対策が必要となります。

② 電子メール

メールサーバの制限にもよりますが、数MB程度までのデータであれば電子メールが最も利用しやすいデータ送受の方法です。しかし、電子メールには盗聴、誤送信、なりすまし等の対策が必要になります。対策としては以下のものがあります。

- メールサーバでメールを暗号化する
- 添付ファイルを分離し添付ファイルをパスワード付ファイルに変換して送付する
- 添付ファイルを分離し添付ファイルのURLをメールの本文に挿入して送り、相手がメールサーバへログインしてダウンロードする

③ FTP サーバ

一般的にオンラインストレージサービスは、他社が提供する共用サービスです。一方、重要な情報を送受したい場合は、自社で管理するサービスでファイルの送受を行いたい場合もあり、この場合に利用されるのがFTPサーバです。PCにFTPクライアントソフトを導入して使用します。FTPの場合も、オンラインストレージサービスと同様に、パスワード管理と盗聴対策が必要です。盗聴対策には、通信が暗号化されるSFTP（SSH File Transfer Protocol）を利用する必要があります。

④ ファイルサーバ

会社支給のPCを利用し、VPNにて社内LANへアクセスできる場合は、ファイルサーバを使用してデータの送受を行う方法が、使い慣れた操作（社内にいるのと同じ感覚）で利用できるため、好ましいと言えます（ただし、社内LANへのアクセス制御には注意が必要です）。また、ファイルサーバで実施できるセキュリティ対策として、ファイルサーバでのアクセス制限、バックアップ、ログの記録等、多くの方法を選択できるメリットもあります。

第4章 オフィスにおける停電･節電対策

本章ではオフィス内での停電や節電に備えた事業継続対策、及び情報セキュリティ対策について紹介します。

4.1 停電時の対策

(1) 突然の停電や電圧低下によるシステムやデータのダメージを防ぐ

これまで、日本の商用電力品質はきわめて高く、工事など計画的な場合を除いて停電となる可能性があるのは、落雷の直撃を受けたり、近くの送電線に障害が発生したときなどのごく限られた場合でした。したがって、ほとんどのオフィスでは停電の発生を想定した対策を実施していません。第2章に示したように、いきなり電力供給が絶たれることでICT機器が故障する可能性があるため、停電の可能性がある場合はまずこの「停電の瞬間のダメージ」への対策を考える必要があります。

① 対策を考えなくてもよい機器

ノートPCは、外出先で不安定な電源を利用することを考慮して設計されており、外部電源からの供給が突然停止すると、直ちに内蔵バッテリーからの供給に切り替わるため、停電の瞬間のダメージへの対策を考える必要はありません。

また、照明や空調などの設備も、停電で故障することはありませんので、対策は行いません。

② 無停電電源装置（UPS）

停電によるダメージを防ぐため、もっとも一般的に利用される機器です。サーバ等のICT機器と電源の間に設置することで、停電から一定の間、停電前と同じように電力が供給されます。後述する自家発電機などの導入とは異なり、高額な投資を行わなくても対策が可能という点で優れています。ただし、以下の点に注意する必要があります。

ア） 「無停電」でいられるのは数分～最大 20 分程度

「無停電電源装置」という名前で誤解しやすいのですが、あくまでも一時しのぎの効果しかありません。停電後ただちに正しい終了操作を行い、電源供給が途絶えても問題のない状態にするまでの電源供給を行うための装置です。この終了操作を自動で行う機能をもち、ICT機器の側も適切に設定しておいた場合は、人が関与しないで済むのですが、そうでない場合は無停電電源装置が発する警報音を合図に、人手で停

止操作を行う必要があります。これを怠ると、無停電電源装置が入っていない状態と変わらない結果になります。

イ）　停電に数回対応させると、性能が低下することがある

無停電電源装置には蓄電池が内蔵されており、性能はその蓄電池に左右されます。2011年度の関東地区の計画停電が行われた地域において、停電に何度か（10回に満たない回数）対応させたことで、無停電電源装置の性能（この場合は電力を供給できる時間）が著しく低下した事例があるようです。ただし、消費電力がどのくらいのサーバをつないでいたか等、使い方によって性能低下の度合いも変わってくると考えられ、数回の停電で必ず性能低下が生ずるかどうかは何とも言えません。

なお、蓄電池は充放電を繰り返すことで必ず劣化します。300回程度繰り返すと電力供給時間はほとんどゼロになると考えられますが、これは蓄電池の化学的な特性によるものであるため避けられません。

ウ）　UPS自体も故障する

UPSも電子機器のひとつに過ぎませんので、時には故障します。UPSが故障すると、停電と同時に電源供給が中断してしまいます[22]。日常的に使うものではないので、故障しているかどうかがわかりにくいのが難点です。

UPSの故障による影響を避けるためには、UPSの多重化を行います。電源の多重化の場合、通常は電源を並列に配置しますが、UPSの場合は直列につないでも、どれか1台が正常に機能すれば目的を達成することができます。ただし多重化する場合、同一形式の製品で多重化することは避けてください。同一形式の場合、異なるメーカーや形式の機器と比較して、同時に故障する可能性が高くなるためです。

(2) 停電の間に事業を継続する

第1章でも述べたように、停電の間に事業を継続する方法には以下の2種類があり、対策は全く異なります。

①　停電していない拠点に事業の主要機能を移す

担当者や資源を停電の影響のない拠点に移して事業を継続します。これは計画停電の場合のように、あらかじめ停電が発生することがわかっている場合のみに有効な方法です。電力需要が逼迫した結果、想定外の停電が発生するような場合には効果がありません。

[22] 正確には、UPS の故障には停電でなくても電源供給が行われなくなるタイプの故障も存在しますが、これは容易に検知できるので、今回の検討からは除外します。

ア）　電力需要に余裕のある拠点で事業を継続する

海外に工場や営業拠点をもっている企業の場合、一時的にそちらに本社機能ももたせることが考えられます。国内では沖縄地方は以前から原子力発電に依存していないため、電力供給量には余裕があります。もっとも、2011年には関東･東北地区の電力需給が逼迫したために関西に本社機能や業務の中枢機能を移した企業は、2012年に関西地区での電力需要逼迫に苦しむことになりました。このように、一時的な対策にはなっても、持続的な対策とはなり得ない可能性があることを念頭に置く必要があります。

イ）　在宅勤務を行う

零細･SOHO企業などの場合、経営者や従業員の自宅などが停電の影響を受けない場合は、そちらに事業拠点を移すことも考えられます。ただし、自宅で十分な情報セキュリティ対策が行われていない環境に移すのは危険です。第3章に示した対策の導入を検討すべきです。

②　停電の拠点で事業を継続する

あくまで現在の拠点で事業を継続する場合の対策は、以下の通りです。

ア）　電源の確保

計画停電で想定されている2時間程度の停電に対処する手段として、次の方法があります。

■ ディーゼル発電機

停電対策として、病院など停電による業務停止が許されない施設で利用されています。ただし、利用にあたって以下の注意が必要です。

- 発電機の動作に伴い騒音や排煙が発生します。設置場所が自社の敷地外に隣接している場合、苦情のため夜間の運転ができないことがあります。
- 長時間の運転のためには多くの燃料が必要ですが、軽油で200リットル以上、A重油で400リットル以上を建物内や地上に保管する場合、少量危険物取扱所の扱いとなり、消防署への届け出が必要となります。この範囲内で計画停電等、数時間の停電に対処しようとすると、停電時に利用可能な電力はかなり絞り込む必要が生じます。
- 災害時のように長時間の停電に対処するには、上述のように多くの燃料の備蓄が必要となります。さらに、連続稼働すると発電機に障害が発生しやすくなります。こうしたトラブルによる停電を避けるためには、後述の蓄電池の併用、もしくは発電機の多重化等の対策が必要となり、多くのコストが必要となります。

■ **蓄電池**

大容量の蓄電池を拠点に設置する方法です。蓄電池への充電や放電は直流で行われるため、DC-ACコンバータを介して商用電力と同じ電圧の交流に変換します。騒音や燃料調達などの心配はありませんが、オフィスの必要電力を賄おうとすると、ディーゼル発電機より高価となります。東京電力管内で2011年4月に行われた計画停電のように2～3時間の停電を想定する場合、数百万～数千万の投資が必要になります。ただし、東日本大震災以降の電力需要の高まりの中、数十万円レベルの充電池が市場に出てきました。これは、PC1台と周辺機器等、必要な範囲のみへの数時間の電力供給を可能とするものであり、自社サーバの運用等、必要最小限の事業継続を考える場合には検討価値があります。

イ）　ネットワーク接続の確保

上述のように、電力の確保については自社の努力で何とかすることが可能ですが、インターネット等、ネットワークの接続確保については通信キャリア等における停電対策に依存せざるを得ません。各種サービスの停電時の確保見通しはおおむね以下のようになっています。

■ **光ファイバ、**ADSL**、専用線、加入電話回線**

通信キャリアの拠点には非常用電源が装備され、計画停電程度の時間であればサービスは継続されます。一方、利用者側の設備に必要な電源は商用電源を利用していることが多いので、何も対策していない場合、停電になると利用できなくなります。したがって、自らの拠点の設備への電力供給について、ア）に示した方法で確保することで通信の維持が可能となります。

■ **携帯電話、**3G **ネットワーク**

無線基地局には蓄電池が装備され、計画停電程度の時間であればサービスは継続されます。また、非常用発電機を備えた無線基地局も存在します。利用者側の機器、すなわち携帯電話や3Gモデム、モバイルルータ等はバッテリー動作が可能なものが多く、停電時も比較的電源の確保は容易と思われるので、計画停電においてはインターネット等との接続を維持できる可能性が高いと考えられます。ただし災害時等には通信が輻輳しやすいことに注意が必要です。この場合、通信できなくても電力は消費されてしまうため、つながらない場合は電源を切ってバッテリーを温存するなどの対策を考える必要があります。

■ **公衆無線** LAN（Wi-Fi **アクセスポイント**）

低コストで基地局を設置している場合が多いため、停電時はほとんどの基地局が機能停止となることが想定されます。したがって、計画停電時、災害時とも、利用できないと思って対策を講じる必要があります。

4.2 オフィスの ICT 機器の節電

(1) オフィスの ICT 機器節電のための可視化

今日、オフィスでは様々な業務でICT機器を運用しています。例えば、今やPCを使用するのはICT部門だけでなく、幅広い業種で部門に関わらずに従業員は日常的にPCを使用しています。ICT機器の利用は多くの業務と不可分に結びついており、同じ企業内であっても部門によって利用状況は異なります。そのため、業務内容に配慮して節電を実施しなければ、質の高いサービスの継続と十分な節電効果を両立させることはできません。部門やフロアごとに、きめ細かい節電を計画するために、オフィスのICT機器の電力使用を可視化することが必要です。

① 機器タイプの把握

ICT機器の種類によって節電へのアプローチは異なります。PCとサーバでは消費電力や使用状況は大きく異なります。どの部門でどんな種類のICT機器がどれだけ使用されているかを把握することで、きめ細かい節電ポリシーの作成や、節電効果の見積もりが可能となります。

② 物理的な設置場所の把握

オフィスが地理的に分散している場合は、どこにどれだけのICT機器が存在し、どの程度の電力使用量かを把握することで、地域別の節電計画を立てることが可能です。

また、同じオフィス内であっても、フロアごとにICT機器の設置状況を把握できれば、例えば、夏場にサーバやデスクトップPCが多いフロアと少ないフロアで空調の設定温度を変える等、オフィスのファシリティと組み合わせた対策も可能となります。

③ 時間軸での傾向の把握

電力需給の逼迫する時間帯と、オフィス内の電力使用が最大となる時間帯をずらす、いわゆるピークシフトの実施にあたっては、電力の使用状況を時間軸で把握することが必要です。

また、時間ごとの電力使用状況を精査することで、特定の部門では、定刻でICT機器の電源を強制的にオフにする等の思い切った施策が可能となるかもしれません。オフィスでいつ、どれだけ電力が使用されているかを把握することは、節電ポリシーの策定にあたり、ポリシーの対象範囲、効果と業務への影響度を見積もるために重要です。

(2) オフィスの ICT 機器節電のための計画策定

① 節電効果を得るための対策項目の検討

クライアントPC、サーバであれば、非使用時の電源オフに加えて、CPUのパフォーマンスダウン、モニターのこまめな電源オフや輝度の調整が挙げられます。Windows PCであれば、電源オプション機能の省電力設定も有効です。

② サービス継続を維持するための検討

多くの場合、節電効果と業務効率はトレードオフの関係にあります。節電のための施策が自社のサービスに対してどの程度の影響を与えるかを慎重に検討する必要があります。サービスレベルの維持に必須な機器については、節電の対象から除外する等の配慮が必要です。

③ 機器のリプレースの検討

比較的古い機器を使っている場合は、節電の手段として機器のリプレースが対策となり得ます。CPUやグラフィックカード、さらにはOSの電源管理の改善などによりパソコンは、数年前に比べ大幅に性能が向上し、電力効率も向上しています。24時間稼働のサーバであれば、消費電力の削減効果はさらに大きくなります。

表 15　パソコンの消費電力比較[23]

条件	消費電力	デスクトップ		ノート	
		WindowsXP	Windows7	WindowsXP	Windows7
アイドル時	平均(W)	102	52	36	16
アプリケーション使用時（※）	平均(W)	108	53	37	16
	最大(W)	154	67	53	33
	最小(W)	100	50	34	13

※Internet Explorer にて 20 秒毎にページ遷移させ 5 分間計測

(3) オフィスの ICT 機器節電のためのコントロール

① 節電ポリシーの実行

節電ポリシーを実行する際は、速やかかつ過不足なくポリシーが適用されることが重要です。節電ポリシーの徹底が不十分であれば、期待した節電効果を得ることはできません。ユーザーの自主性に任せた展開方法では、節電ポリシーの実施は不徹底

[23] 日本マイクロソフト社 Windows PC 消費電力検証結果レポートより抜粋
http://technet.microsoft.com/ja-jp/windows/hh146891

になりがちです。特に、ユーザー個々に利用しているPCについては、管理者によってリモートからポリシーを一括実行できる方法を工夫する必要があります。

また、節電効果を測定するために、ポリシー実行前と実行後の電力使用状況をそれぞれ把握しておかなければなりません。

②　節電ポリシーを強制するツールの導入

上記①の節電ポリシーを一括で実行するにはツールの導入も有効です。資産管理を行うソフトウェアや一部のアンチウイルスソフトウェア等では、節電ポリシーを強制する機能を提供しており、管理サーバから節電ポリシーを配信してPCの電源プランを一元で強制変更することが出来ます。また、変更後にレポート機能を使って表示することで、節電効果を把握することも可能です。

コラム　離席時にパソコンの電源を切る？

一般的に、トイレなどの離席時には、自宅であればＰＣはそのまま、会社であればスクリーンセーバを起動しＰＣをロックするのではないでしょうか？ＰＣはスクリーンセーバが動いている間も電力を使用します。それでは食事の際や、打合せなど長時間離席する場合はどうでしょうか？

ＰＣは電源が落ちているとほとんど電力を使用しません。しかし起動・停止時には、大きな電力を使用します。一時的に各種デバイスを停止するスリープ（スタンバイ）の機能は、停止時・復帰時にシャットダウンほど電力を使用しません。

表２の通り、例え数分程度の離席でも、１時間 45 分（WindowsXP デスクトップの場合）以内であればスリープを使用する方が省電力なのです。スリープによる停止およびスリープからの復帰にかかる時間は 30 秒程度ですから、離席時はスリープ機能を使用することをお勧めします。

表 16　スクリーンセーバ／スリープ／シャットダウン時の停止から復帰までの消費電力

	デスクトップ		ノート	
	WindowsXP	Windows7	WindowsXP	Windows7
スクリーンセーバ(※)使用時の消費電力(W)	103	53	32	16
シャットダウン＋起動時の使用電力(Ws)	7,501	3,289	2,659	1,582
待機電力(W)	2.31	0.64	0.81	0.38
スリープ＋スリープ復帰時の使用電力(Ws)	2,309	1,083	715	355
スリープ時待機電力(W)	3.14	1.00	1.64	0.56
スリープとアイドルの使用電力が等しくなる時間	23 秒	21 秒	24 秒	23 秒
シャットダウンとスリープの使用電力が等しくなる時間	約 105 分	約 100 分	約 40 分	約 110 分

※スクリーンセーバにはブランクを使用
日本マイクロソフト社 Windows PC 消費電力検証結果レポートより抜粋（「スリープとアイドルの使用電力が等しくなる時間」については JNSA にて算出）

③ 節電ポリシーの PDCA サイクル

節電ポリシーを実行したら、実行前と実行後で電力使用の状況を比較して、節電効果を測定･評価します。期待した節電効果が得られていない場合や、サービスの提供に想定以上の影響が発生した場合は、節電ポリシーを見直し、再度ポリシーを実行します。十分な節電効果が得られた場合でも、ICT機器の使用状況は組織体制の変更や業務内容の変化等に伴い時間と共に変化することが考えられるので、節電ポリシーの実行･評価･見直しのプロセスは定期的に繰り返す必要があります。

(4) オフィスの ICT 機器節電の継続性への考慮点

① ユーザーへの情報開示と啓蒙活動

節電ポリシーの内容によっては、ユーザーの利便性を制限する場合もあります。そのため、ユーザーの理解を得るためには、節電の必要性、社会的意義の啓蒙活動と共に、節電ポリシーの実施によって得られた節電効果のフィードバックを行うことも重要です。

節電の結果をユーザーと共有することは、ユーザーのモチベーションを維持し、節電意識の向上に有効です。

(5) オフィスの ICT 機器節電におけるセキュリティ対策の重要性

複数のICT機器に対して節電ポリシーを実施する場合、すべての機器を手作業でコントロールすることは非効率です。多くの場合、管理者がリモートからコントロールする方式になると考えられます。リモートでICT機器をコントロールできる環境では、十分なセキュリティ対策を講じる必要があります。リモートコントロール権限が悪意ある人間の手に渡れば、重要なシステムが停止されてしまう危険があります。

① コントロールに欠かせない特権 ID 管理

節電ポリシーの実行のため、ICT機器をリモートからコントロールする場合、リモートコントロール用の特権IDを不正使用され、重要なICT機器が停止される危険があります。オフィス内の誰でも全てのICT機器のコントロールができるような運用は避けるべきです。リモートコントロール用の特権IDは厳重に管理されなければなりません。

② ICT 機器のプラットフォームに必要なセキュリティ対策

ICT機器をリモートから一元操作する場合、コントロール用の管理サーバをセキュアに保たなければなりません。管理サーバが不正侵入された場合、オフィス内のICT機器全ての電源制御を奪われる可能性があります。管理サーバに対しては、サーバの

要塞化やファイアウォール等により適切なアクセス制御を施す必要があります。

また、管理サーバと管理対象端末の間の通信を盗聴されると、コントロール権限を持つ特権IDが漏えいしてしまう可能性があります。可能であれば、通信の暗号化も検討すべきです。ネットワークのアクセス制御も重要です、節電対象のICT機器について、不特定多数のコンピューターからの電力コントロールを受け付けるような設定は避けるべきです。

コラム　オフィスの節電効果ってどれぐらいあったのか？

＜ＩＴ企業Ａ社＞

本社ビルにおいて７月～９月の３か月間に、デスクトップＰＣのノートＰＣへの置き換え、空調温度の高めの設定、照明の間引き、ＬＥＤ照明の利用、フロアの一定期間不使用などのオフィス節電対策を実施しました。その結果、２０１１年度の電力使用量は対前年同期比約３６％の削減を達成し、電気料金も約２億円の削減となりました。また、社員の有給休暇の取得促進、総労働時間の短縮、在宅勤務制度利用者の大幅な増加といった副次的な効果も現れています。

＜ＩＴ企業Ｂ社＞

Ｂ社ではオフィス内の PC に対し、IT 機器の電力管理ソフトウェアを導入し、定刻以降電源オフ、モニターを５分以上使用していない場合自動的にスタンバイ状態にするという節電ポリシーを実施することで、オフィス内 IT 機器について最大で約 10%の節電効果を上げました。オフィスの IT 機器に対する電力管理により得られる節電効果は、IT 機器の種類・使用状況、実施する節電ポリシーによって変化します。

第5章　セキュリティ対策の参考情報

ここでは、在宅勤務に直接関係するものではありませんが、在宅勤務を導入するにあたって、あわせて整備・検討しておくと有効な情報セキュリティ対策について紹介します。

5.1　情報の格付け

(1) 情報の取り扱いと情報の格付けとの関係

情報を取り扱う際、情報セキュリティの確保を意識することは言うまでもありませんが、情報セキュリティを確保するには下表の3つの基本的な要件があります。

表 17　情報セキュリティの 3 要件

要件の種類	定義
機密性	情報にアクセスを許可されたものだけがその情報にアクセスできる状態を保つこと
完全性	情報が改ざんや消去されたりしない状態を保つこと
可用性	情報へのアクセスを許可されたものが、必要な時に中断することなく情報へアクセスできる状態を保つこと

情報セキュリティは、このような3つの要件を満たせるように対策を講じていくことが必要です。しかし、どのような情報にも高いレベルでこれらの要件を満たすような対策は、情報の取り扱い手順のプロセスを複雑化させ利便性を損なってしまったり、対策のための冗長なコストを掛けてしまったり、適切なセキュリティ対策とは言えません。適切なセキュリティ対策のために、管理している情報の特性から、これらの要件に対しどのくらいのレベルで管理すべきかの基準を明確にして、そのレベルに応じたセキュリティ対策を講じていく必要があります。そうすることで、従業員が情報を扱う際、その情報に必要なセキュリティレベルと必要なセキュリティ対策が理解できるようになるのです。このような情報に必要なセキュリティレベルの区分を明確にすることを「情報の格付け」といいます。情報の格付けでは、セキュリティ要件に合わせ、3つまたは2つの観点から行います。

①機密性の観点からの情報の格付け

②完全性の観点からの情報の格付け

③可用性の観点からの情報の格付け

基本は、上記①～③の3つの観点から格付けを行いますが、②③を一緒にして重要性の観点からの格付けにすることもあります。この場合は、機密性の観点と重要性の観点の2つの観点からの格付けとなります。在宅勤務でのICT環境は、社内でのICT環境と違ってくるため、社内とは違ったセキュリティ対策を検討しなければなりません。そのためには、情報の格付けとその格付けに従った在宅勤務でのセキュリティ対策を明確にしておく必要があるのです。

(2) 情報の格付けの考え方

このように、情報の格付けには幾つかの観点があります。それぞれの観点による考え方をまとめてみると下記のようになります。

① 機密性の観点からの情報の格付け

情報の格付けにおける最も重要な要素は情報の「機密度」です。これは情報セキュリティに求められる機密性の観点から、その情報のセキュリティ管理上必要な機密レベルを明確にするものです。一般的に「関係者外秘」や「社外秘」などと分けられているものです。対象の情報が、本来見る必要のない人たちに見られないように保護するための基準となります。ここでの考え方のポイントは、対象の情報が漏えいした場合の人や企業に対する影響の大きさをもとにレベル分けすることです。影響の大きさとは、人に関することでは権利や人命にかかわる影響度合い、企業に関することでは利益や経営、企業の信頼性にかかわる影響度合いなどに基づいて2～3段階のレベル分けをします。レベル分けしたら、レベル毎に「複製」、「配布」、「送信」、「授受」、「破棄」など、業務上のプロセスにおける制限事項を定義しておきます。

② 完全性の観点からの情報の格付け

情報に対して求められる完全性のレベルを明確にします。情報が改ざんや消去されることにより、業務に支障が出る情報について、その業務への支障の度合いにより、求められる完全性のレベルを明確にします。対象の情報が改ざんや破損のないように保持するための基準となります。ここでの考え方のポイントは、対象の情報が、改ざんや消去されることにより、業務および業務を通して関係する企業や人、サービスに及ぼす影響の大きさをもとにレベル分けします。影響の大きさとは、人に関することでは権利や人命にかかわる影響度合い、企業に関することでは利益や経営、企業の信頼性にかかわる影響度合い、サービスに関することではサービスの信頼性や継続性などに基づいて2～3段階のレベル分けをします。レベル分けしたら、レベル毎に「保存期間」、「保存場所」、「書換え」、「破棄」など、業務上のプロセスにおける制限事項を定義し

ておきます。

③　可用性の観点からの情報の格付け

情報に対して求められる可用性のレベルを明確にします。情報が利用できなくなることにより、業務に支障が出る情報について、その業務への支障の度合いにより、求められる可用性のレベルを明確にします。対象の情報が利用すべき時にいつでも利用できるように保持するための基準となります。ここでの考え方のポイントは、対象の情報が、利用不可能になることにより、業務および業務を通して関係する企業や人、サービスに及ぼす影響の大きさをもとにレベル分けします。影響の大きさとは、人に関することでは権利や人命にかかわる影響度合い、企業に関することでは利益や経営、企業の信頼性にかかわる影響度合い、サービスに関することではサービスの信頼性や継続性などを元にして2～3段階のレベル分けをします。レベル分けしたら、レベル毎に「保存場所」、「破損した場合の復旧許容時間」、「バックアップ」など、業務上のプロセスにおける制限事項を定義しておきます。

上記のように、完全性の観点と可用性の観点は、考慮すべき影響対象が業務に対する影響であって、大変近い観点と言えます。そのため、管理を簡略化するために、この2つを合わせて重要性の観点として格付けをする企業も多くあります。

情報の格付けのポイントは、情報の種類により、確保すべき機密性や重要性の観点が変わってくることです。個人情報などは、機密性が確保できず漏えいした際、個人のプライバシーに影響をおよぼしたり、重要性を確保できず改ざんされた際には個人の権利・利益に影響を及ぼしたりしてしまいます。更には、「個人情報の保護に関する法律」に対するコンプライアンスの観点からも、機密性や重要性の両面の確保が必要です。

一方、企業の公開情報などは、機密性は必要ありませんが、内容が改ざんや消去されることにより、誤った情報を発信し、消費者や取引先に対する信用を損なったり、または提供するサービスが提供できなくなり、サービスの継続性を脅かし、ひいては利用者に対するサービス品質を落とすことになってしまいます。

このように情報の種類により、確保すべき観点とそのレベルは変わってきますので、社内の情報格付けの基準を明確にして、情報毎に格付けをしておくことが必要です。そうすることで情報の利用者が、利用する情報に必要な機密性や重要性のレベルが分かるようになり、組織として均一な情報管理ができるようになるための基礎づくりにつながります。

(3) 一般的な企業の情報の格付けの例

企業における情報の格付けは、機密性と重要性（完全性、可用性）の2つの観点か

ら行うのが一般的です。特に在宅勤務では、機密性の観点を強く意識する必要があります。格付けの区分は、その情報に明示することになりますので、区分名（ラベル名）は分かりやすい付け方にすることが望ましいと言えます。下記に一般的な企業の一例を示しますので参考にしてください。

① 機密性の観点

表 18　機密性の観点からの格付けの例

レベル	ラベル名	定義
機密レベル３	「関係者外秘」	漏えいすることにより、社会、会社、個人に対し甚大な影響を及ぼす可能性がある情報で、特定の者のみがアクセスできる情報。
機密レベル２	「社外秘」	漏えいすることにより、社会、会社、個人に対し影響を及ぼす可能性がある情報で、従業員のみがアクセスできる情報。
機密レベル１	「一般」	漏えいすることによる影響はなく、上記「関係者外秘」および「社外秘」以外の情報。

② 重要性の観点

表 19　重要性の観点からの格付けの例

レベル	ラベル名	定義
重要レベル３	「最重要」	改ざん、消去されることにより、業務、社会、会社、個人に対して甚大な影響を及ぼす可能性がある情報。
重要レベル２	「重要」	改ざん、消去されることにより、業務、社会、会社、個人に対して影響を及ぼす可能性がある情報。
重要レベル１	「一般」	改ざん、消去されることによる影響はなく、上記「最重要」および「重要」以外の情報。

コラム　政府機関の場合

政府機関では、「政府機関の情報セキュリティ対策のための統一規範」（情報セキュリティ政策会議決定）という政府機関共通の情報セキュリティ対策に対する考え方の基本方針をまとめたものがあります。このなかで、政府機関が扱う情報に対して情報の格付けを行わなければならないことになっています。そして、情報毎に格付けの区分を明示することになっています。政府機関の場合、情報の格付けは、「機密性」、「完全性」、「可用性」の３つ観点から行うことになっていますので、少し複雑な管理になると言えます。

実際の基準の考え方については、「情報の格付け及び取扱制限に関する規程」策定手引書（内閣官房情報セキュリティセンター）の中にまとめられています（下記ＵＲＬ参照）。雛型形式でまとめられていますので、自社内の情報格付けの規程や基準書作成の参考にすると良いでしょう。ただし、政府機関を対象としている関係で、国家、行政、国民、企業に関する情報など多種多様な情報を扱うことを前提とした内容になっています。企業で参考にする場合には、自社内で扱う情報の種類や特性を加味して、自社に合う内容にカスタマイズすることが必要です。重要インフラ企業や政府組織との直接的な取引がある企業であれば、このフレームを意識した内容にすべきでしょう。そうでない企業は、「5.1⑶　一般的な企業の情報格付けの例」で示したような機密性と重要性の２つの観点から格付けを行うことで、日常の業務の中で必要以上に複雑化させることなく、定着しやすい基準にできるでしょう。

「情報の格付け及び取扱制限に関する規程」策定手引書（内閣官房情報セキュリティセンター：2011 年４月）
http://www.nisc.go.jp/active/general/pdf/dm3-01-101_manual.pdf

5.2 情報の持ち出し・持ち込み管理

5.2.1 情報の持ち出しの管理

今までの情報セキュリティ対策では、社内情報を職場外に持ち出すことは業務上限られた範囲であり、情報の持ち出しは厳しく管理される傾向がありました。しかし、在宅勤務を検討すると、今までの情報の持ち出し管理では、想定されていなかった事象もあり、業務効率上、色々と不具合が出てきます。在宅勤務を効果的にするためには、情報の持ち出し管理に関して再考し、在宅勤務を考慮した情報の持ち出しに関する管理体制やルールを明確にする必要があります。在宅勤務環境では、情報セキュリティ上の脅威が高まる上に、社内と同様のセキュリティレベルを維持するのが難しいという状況にあります。つまり、情報漏えい等の情報セキュリティリスクは確実に高くなります。このような状況を十分把握し、より堅実な管理を行うことが求められます。人的な管理に加え、システム的なセキュリティ対策を複合的に組み合わせ、セキュリティ対策を検討することが望まれます。主な対策案としては、下記事項のような事項があります。

(1) 人的な管理

- 情報の持ち出しに関するセキュリティ対策遵守の誓約書を提出させる(在宅勤務開始時)
- 情報の持ち出し時には、持ち出し媒体や情報の内容に関する申請をし、上長が承認の上、その記録を取る
- 持ち出した情報の管理状況に問題がないか日常的に報告(セルフチェックなど)させる

(2) システム的な対策

- 持ち出す情報は必ず暗号化する
- 自宅で利用しているPC内でも暗号化する
- 持ち出し先で利用するPCのセキュリティ対策は社内PCと同等以上にする(認証、ウイルス対策、バックアップ)
- 持ち出し先で利用するPCはリモートからデータ消去できるようなシステムを導入する
- リモートから社内環境にアクセスする場合、あらかじめ承認された情報(データ、ファイル)以外はアクセス出来ないよう制限する

- 在宅環境でのシステム動作ログを取得する

これらの方法以外に、在宅勤務のシステム面の仕組み自体にセキュリティ上のリスクを低減する方法を採用することも考えられます。例えば、クラウドコンピューティング環境やシンクライアントの利用により、在宅環境には情報が存在しない、残らない仕組みで運用することが一例としてあげられます。このような環境であれば、情報は、クラウド内で一元管理ができ、セキュリティもある程度のレベルを保つことが出来ます。在宅環境に情報が存在しなくなるため、在宅環境でのセキュリティレベルも、過度に意識する必要もなくなります。その他では、運用面の制限ですが、機密度や重要度の高い情報を利用する業務は在宅では行わない運用で在宅先でのリスク低減を図ることも有効な方法です。

このように、在宅勤務のシステム形態によっても、対策のポイントが変わってきますので、自社における在宅勤務のシステム形態に合わせたセキュリティ対策を検討するようにしましょう。但し、システム形態によらず、人的対策については、誓約書の提出など利用者のセキュリティ意識を高める対策を講じておくことは、変わらず重要な事項となります。

5.2.2　情報の持ち込みの管理

情報の持ち込み時、一番注意しなければならないことは、ウイルス等のマルウェアを持ち込んでしまうことです。これは、在宅勤務の環境でも同様です。特に注意しなければならないのは、在宅環境では、公私の区別をしっかり付けていないと、私用で持ち込んだ情報からウイルスに感染し、業務用の環境に被害を及ぼしてしまう可能性があります。在宅環境であっても、ウイルスに感染していないかの事前確認や不用意な情報の持ち込みを制限するなどの対策が必要です。主な対策案としては、下記事項のような事項があります。

(1) 人的な管理

- 情報の持ち込みに関するセキュリティ対策遵守の誓約書を提出させる(在宅勤務開始時)
- 情報の持ち込み時には、情報の提供元にウイルスチェック済みの確認を取る
- 不用意に情報を持ち込んでいないか日常的に報告(セルフチェックなど)させる
- 在宅での業務環境では、業務に関係ないサイトへのアクセスを禁止する
- 電子メールの添付ファイル等で情報を在宅環境に、もしくは在宅環境から職場環境にそれぞれ持ち込む場合には、事前に十分な注意を払う

(2) システム的な対策

- 在宅環境で、常に最新のウイルスチェックができるようにする
- 持ち出し先で利用するPCはリモートからデータ消去できるようなシステムを導入する
- 在宅環境でのシステム動作ログを取得する

5.3 従業員教育

5.3.1 情報セキュリティ教育

通常勤務の場合、事務所内で就労しており管理職や同僚がそばにいてルール等を守らせる環境がありました。しかしながら在宅勤務では、当然業務を行っている就労者は基本的に一人であり、マネージャーの管理や同僚の目が気にならなくなります。ここで重要になってくるのが個人の意識です。情報漏えい事故等を未然に防ぐためには、個人のモラルと意識の向上が非常に重要になってきます。

在宅勤務導入については、ルールの整備、ハードウェアやインフラの準備を行うことで充分な対策ができたと満足してしまいがちです。これと合わせてモラルと意識向上のための教育も充分に考慮し実施する必要があります。

5.3.2 在宅でもできる研修

教育の実施については、定期的な研修の提供と理解度の確認が重要です。しかしながら、在宅勤務者に対してそのたびに事務所に呼び研修を行うことは非効率でありコスト面でも簡単に導入できないことが考えられます。インターネット環境を利用したeラーニングの導入が効率的であり、安価な手段です。一般的にeラーニングでは、知識研修と理解度チェック等の試験を手軽に利用できます。集合研修のように同じ時刻に同じ場所へ就労者を集める必要がないことから、実施に関する敷居の低い研修手段であるといえます。また、震災による節電対策という観点からも、最近注目されています。

(1) eラーニングの種類

ア)　ビデオ配信

ビデオによるeラーニングの導入に関しては、これまで回線・帯域の問題で企業の情報システム部門等から躊躇する場合や却下される場合も多かったと思われます。しかしながら、在宅を基本とした導入であれば可能になるかもしれません。最近の傾向として、ブロードバンド回線や光回線の普及により、企業で利用するインターネットよりも家庭の環境のほうが高速になっている場合が増えています。

イ)　静止画

ビデオの作成に比べ、簡単に利用することができます。教育教材は、プレゼンテーション作成ソフトや文書作成ソフトを利用してインターネットに公開するHTMLやイメージ画像を作成することで代用できます。

(2) 理解度の計測について

eラーニングの仕組みでは、試験の実施が簡単に行えます。また、試験を行うことで研修に対する理解度を容易に把握することができます。

「想定例」
在宅勤務の導入と合わせて、在宅勤務者の情報セキュリティにおける最低限の理解を求めている。

- ✓　半年に１回の、静止画を利用したｅラーニングの実施を義務化
- ✓　理解度試験での、合格点クリアを義務化

上記２点をクリアしなかった場合、企業とのネットワーク接続を認めない。

5.4　セルフチェック

5.4.1　運用の定着とセルフチェック

セキュリティ対策は、通常の業務プロセスの中に組み込まれて実施されます。しかしながら、手間が増える、面倒であるなどの理由で、つい忘れてしまいがちになります。特に在宅勤務の対象になる出先や自宅などは、社内と違い、上長など周りの目が届かないため、意識も弱くなりがちです。在宅勤務での従業員のセキュリティ意識を高めるため、定期的な従業員教育のみでなく、日常的に意識させる仕組みが必要です。

その効果的な方法の一つがセルフチェックです。従業員が、在宅時に意識しなければならないセキュリティ対策項目をチェックリストにして、実行した結果を定期的にチェックさせ、提出させ、上長が運用状況を確認します。この一連の結果（本人のチェック、上長の確認）は、運用証跡として残しておきます。このように、在宅勤務でのセキュリティ対策を定着させるためには、従業員に対して日常的にセキュリティ対策を意識させるプロセスを運用し、従業員の意識を定着させる仕組みを導入することが必要です。

また、セルフチェックは利用者のみでなくシステムの管理者にも対策を定着させるため、同様な仕組みを準備すると良いでしょう。

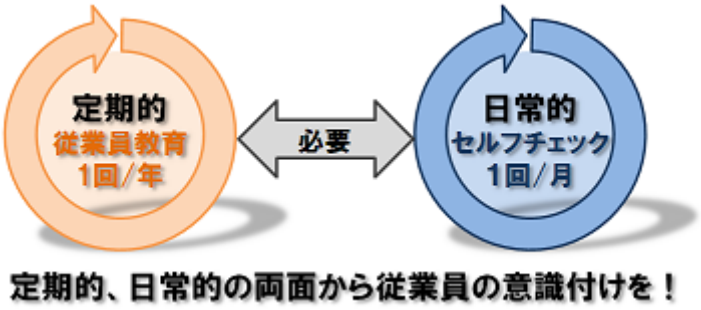

図 11　セルフチェックによる従業員の意識付け

5.4.2　セルフチェックの運用

セルフチェックを運用するには、先ずチェック項目を決めなければなりません。利用者が在宅時に行うべき重要なセキュリティ対策をチェックリストしてまとめます。チェック項目は多すぎても少なすぎても効果がでません。多すぎると形骸化しやすくなります。逆に少ないと頭に入り易いですが、対策の網羅性の面で支障があります。一般的な目安としては10項目前後くらいが適切なボリュームです。また、チェックリストは管理者向

けのものも準備しておきます。こちらについては、管理者の視点で重要なセキュリティ対策をまとめます。

　これらの準備が済んだら、従業員教育によりセルフチェックの目的とともにチェック項目の説明を行い、理解を深めます。チェックリストはEXCEL等で配布し、日々のチェック結果を上長に提出し、上長が確認するようにします。または、ポータルサイトなどにセルフチェックが出来るようなページを作成しておき、利用者のチェック結果と上長の確認状況をサーバで一括管理できるようにすると管理面では更に良いと言えます。これらのチェックは1回/月くらいの目安で、その月の状況をチェックするのが目安です。上長による確認結果の記録は監査時の証跡にもなりますので記録として保管しておきます。また、チェックリストは定期的に見直し、見直した結果は、チェックリストへ反映させるとともに、再教育により利用者への落とし込みを行います。このように、チェックリストの作成から、落とし込み、運用、見直し、のサイクルを回しながら継続運用し、セキュリティ対策の定着を図っていきます。

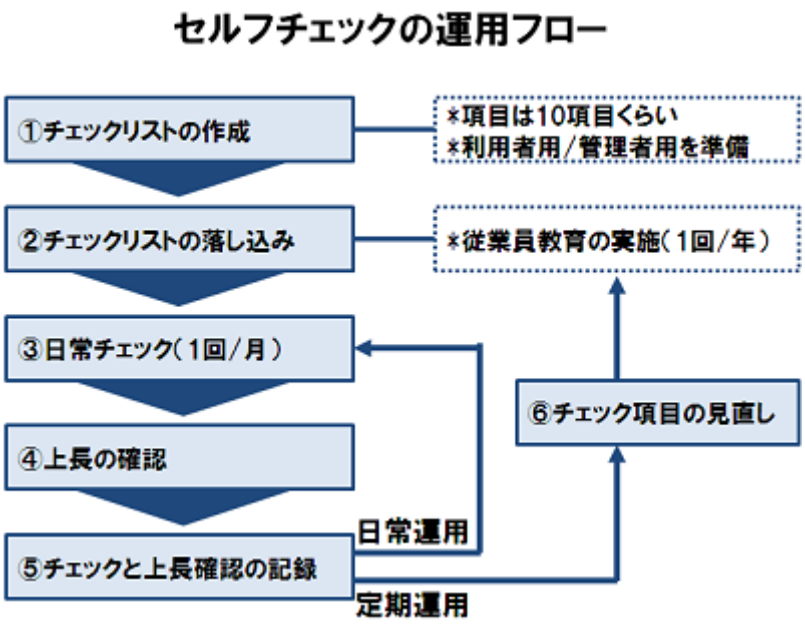

図 12　セルフチェックの運用フロー

第6章　在宅勤務と節電対策の事例

ここでは、実際に在宅勤務や節電対策を導入・実践している企業における事例を紹介します。

6.1　事例1：　株式会社 NTT データ

(1) 導入の経緯・目的

多様な人材の活用、社員満足度の向上、生産性の向上、労働時間の短縮など在宅勤務を通じて働き方の変革を実行することを目的としています。在宅勤務制度導入の検討にあたっては、導入を希望する社員がワーキンググループを作りボトムアップで検討を進め、トライアルの導入を通じて会社側と社員側で改革と改善を重ねて繰り上げた制度です。

(2) 対象業務・対象者

社員等で、自宅において業務を遂行することが可能な環境にあり、かつ、本人が希望し上司が承認する場合であれば職種、年齢、性別を問いません（ただし育成期間中の社員は除く）。在宅勤務に適した仕事として、「一人でできる仕事、計画的にできる仕事、集中力が要求される仕事、作業内容と結果が明確になる仕事、個人情報および厳秘資料を使用しない仕事」を推奨していますが、実際に以下のような業務で在宅勤務制度が利用されています。

- 全社員共通：　議事録、報告書等の作成・レビュー。インターネット、書籍による情報収集。電話、メールによる関係者との調整、問い合わせ対応。IBT研修の実施。電子決裁。就業管理。
- 営業：　企画書・提案書・見積書等の資料作成、修正。
- 開発：　開発作業進捗の管理。品質評価報告書・マニュアル等の執筆、レビュー。
- 研究：　論文執筆や校正。文献による下調べ。特許情報の調査。
- スタッフ：　関連法制度等のレポート作成。

(3) セキュリティ上の工夫点

在宅勤務にあたっては全社のセキュリティポリシーを遵守することが求められますが、在宅勤務に特化したセキュリティ対策の主なものとして下記の対策を実施しています。

- 個人情報および厳秘資料を使用する業務を禁止する
- 原則として会社から貸与されたシンクライアントを利用することとする（HDDの無いPCに限る）
- リモートアクセスの認証にはワンタイムパスワードを利用する
- 自宅での紙媒体の使用を禁止する
- 自宅のFAXを使用することを禁止する
- 自宅で無線LANを使用する際には通信経路の暗号化を必須とする
- 在宅勤務の作業場所には家族が近寄らないように工夫する
- 在宅勤務の申請時にセキュリティルールに関するチェックリストでルールを確認する

（4）利用状況について

①　在宅勤務の効果

在宅勤務制度の利用者および上司から以下のような効果が報告されています。

- 介護のために年休がなくなり退職を考えていたが、その問題が解消された
- 通勤に関する負担が少なくなり、仕事の効率が上がった
- 仕事の「見える化」が向上し、段取り良く仕事ができるようになった
- 静かな環境で仕事に集中できるようになった
- 在宅勤務中の成果について報告することで、上司とのコミュニケーション機会が増えた
- 家族とのコミュニケーションがとりやすくなり、家族からの評価も上がった

②　在宅勤務の課題

在宅勤務制度をさらに普及させるためには、以下のような課題があります。

- 一部の管理職やリーダーは自分が職場不在ではマネジメントが回らないと考えており、上位職の働き方変革やマネジメント方法に対する意識改革が必要
- 上司や同僚の理解が得にくいと考えている社員が多いため、職場単位で在宅勤務についての有効性に関する議論などを実施することが必要
- セキュリティを確保した上で適用可能な業務を拡大するためのITインフラの整備が必要

(5) 東日本大震災対応で変更したルールなど

昨年度は、東日本大震災および福島第一原子力発電所の事故に伴い、国の主導により電力総量規制対策が実施されました。当社もオフィス等における徹底した節電を実施するためのひとつの施策として、在宅勤務の積極的な活用を推奨しています。節電対応はビジネスを進めていくうえでは大変厳しいものですが、この機会を「働き方の変革」を進めていくための良いきっかけとして位置づけ、これまでの慣習や、常識、考え方にとらわれない柔軟な仕事の仕方を実現するべきだと考えています。

在宅勤務制度の積極的な活用を推進するために、現行制度を以下のとおり一時的に改正し制度緩和を実施しました。

- 従来認めていなかった入社間もない育成期間中の社員等も対象に含め全社員としました
- 私物PCの利用を可能としました(ただし、セキュリティ教育の受講、誓約書等の提出を求めました)
- 利用申請等運用上のルールを簡略化しました

(6) 昨年度の実施状況と今年度の計画

オフィス等における節電施策のひとつとして、首都圏の自社保有ビルを中心に夏期期間中に1週間連続してフロア単位にオフィスを不使用とする施策を実施しました。フロア不使用期間中は、有給休暇・夏季休暇の取得、共通オフィスの利用を推奨すると共に、在宅勤務の積極的な利用を推進しました。それと併せ、在宅勤務で必要となるリモートアクセスの同時アクセス数を増やすなどIT環境の充実も図りました。この結果、今まで在宅勤務利用にあまり積極的でなかった組織や管理職が自分の組織やチームでも在宅勤務を利用しようという動きが拡大しました。

今年度も引き続き、1週間連続したフロア不使用の施策を継続すると共に、働き方の変革として、在宅勤務を積極的に活用することを推進します。また、在宅勤務制度へのエントリーおよび利用時申請についてシステム化を図り、より簡便に制度を利用できるような環境を整備しました。ただし、昨年度実施した、私物PCの利用の一時的な制限緩和については、セキュリティ上の理由から今年度は緩和を実施しないことにしました。

6.2 事例2：株式会社シマンテック

(1) 導入の経緯・目的

2011年3月の東日本大震災の影響で電力需給の逼迫が予想されることから、東京本社において消費電力削減を推進するため、在宅勤務日を週2回設け、節電を推進することとなりました。元々在宅勤務が出来る環境がある程度整ってはおりましたが、制度化することによりフレキシブルかつ効率的に働く環境を実現することを目的としています。お客様、パートナー様に対しては、IT環境整えることによりビジネスの継続性を確保していきます。

(2) 対象業務・対象者

正社員と派遣社員及び契約社員の一部を対象としています。営業、システムエンジニア、開発、マーケティング等オフィスにリモートアクセスで仕事が可能な職種を対象としています。サポート業務、電話による営業等はインフラの関係からこれまで通りの社内勤務としています。

(3) セキュリティ上の工夫点

① 人事

全社のセキュリティポリシーの遵守徹底と、契約社員及び派遣社員の機密情報の取り扱いに関する取り交わしを見直しました。

② インフラ

ノートPC及びBlackBerry、iPhone/iPad等のモバイルデバイスを利用し、職場外から業務が行えるインフラを提供しています。セキュリティ対策としては以下を実現しています。

- モバイルデバイスの暗号化
- USBメモリ等のデバイス制御の実装
- 機密情報のブラウザからの書き込み/電子メールの送信の監視・防止の実装
- VPN接続による通信の暗号化
- VPN接続時のワンタイムパスワード認証（ワンタイムパスワードはBlackBerry等のデバイスで実現）
- 検疫システムによる安全なデバイスのみの接続

- ウイルス対策／Firewall／IPSの実装
- のぞき見防止シートの装着

(4) 利用状況について

① 在宅勤務の効果

7月の実施に向けて、6月にリハーサルを行い、以下のようなフィードバックがありました。

- 通勤に関する時間を削減することで、業務への割り当て時間が増え効率が上がった
- 仕事に集中することができ、業務の効率が上がった
- 家族とのコミュニケーションや家族へのケアする時間が増え、家族全体の満足度が上がった

② 在宅勤務の課題

これから課題が増える可能性がありますが、現時点では以下のような課題が見えています。

- 社員の行動を上司が把握しづらいため、業務に支障が出る場面が予想される
- 社員のワークロードが分かりづらくなり、社員へのケア等を益々注意する必要がある
- 職種によっては業務の成果を明確化し、評価を定量的に実施する必要がある

(5) 東日本大震災対応で変更したルールなど

2011年7月から9月まで、週2日の在宅勤務日を設定しました。

(6) 昨年度の実施状況と今年度の計画

昨夏の節電対策として、東京本社における消費電力を削減する施策を実施しました。具体的には、7月1日から9月22日までの約2ヶ月半、火曜日および金曜日に限定して2フロア分の空調を停止し(一部のサーバールームを除きます。)、社員にも在宅勤務を奨励しました。また、この期間中は、通常勤務日でも空調・冷房の設定温度を28℃に変更、照明器具の照度を50%減光調整するなど、オフィスの省電力削減を目指しました。一方、この期間は社員に対し、会社の情報システムにVPN接続できるノートPCを貸与し、通常と同じ業務ができる環境を用意するほか、一部の社員にはBlackBerryやiPhoneなどの携帯情報端末を貸与し、業務を継続できるようにしました。

この結果、セキュリティ対策の施された安全なPC及びネットワーク環境での在宅勤務を実現することができ、社員の生産性向上にもつながりました。一方で、「週2日の在宅勤務奨励日は顧客との打ち合わせのための応接室確保が困難」、「社内の打ち合わせがしづらくなった」などの課題も見えました。

今年度も昨年度の経験や反省点を踏まえ、政府の施策に応じて必要な対策を検討・推進してまいります。

6.3 事例3：株式会社 NTTPC コミュニケーションズ

(1) 導入の経緯・目的

2011年3月の東日本大震災による電力供給能力不足を受けて、社会的責任が大きいNTTグループの1社として25%～30%の消費電力削減目標が即座に計画されました。オフィスでは会議室などの照明機器の運用、エレベータの運転など細かい部分で徹底的な節電対策を実行し、ビルのファシリティから電力消費量を可視化できる設備がある本社については、消費電力を社内ポータル上に表示して、社員の節電への意識向上にも盛んに取り組みました。

社内ITについても、帰宅時のPC電源オフの徹底周知等、取り組みを進めていたが、1500台近い業務用PCの電源管理を社員の意識向上のみに頼るのは限界があり、IT機器の電力消費量の可視化や電源管理を実現するソリューションを導入する必要があると考えました。

NTTPCコミュニケーションズでは、部門や業務によって様々なメーカーのPCやディスプレイ、プリンターを利用しています。詳細な節電計画を策定⇒実行⇒効果を得るためには、メーカーを問わず、様々なIT機器の消費電力を統合的にモニターする仕組みが必要でした。電源設備や各コンセントに物理センサーを設置するような設備投資を行うと、時間とお金が多くかかってしまいます。

そこでメーカーに依存せず、既存のIPネットワークを利用して消費電力を可視化できるソフトウェア・ソリューションであるJouleXという製品を検討しました。

(2) IT 消費電力管理 JouleX 適用イメージ

神田オフィスにJouleX Energy Managerを設置し、ネットワーク経由で新橋、神田、大阪の3拠点のIT機器の消費電力をモニター、コントロールしています。

① モニター対象デバイス

- 3拠点、1,550台のデバイス
- デスクトップPC(WindowsXP/VISTA/7)
- サーバ(Windows Server 2003/2008)
- モニターディスプレイ
- プリンター

②　コントロールポリシー

- 平日20時にメッセージを出力し30分以上応答がない場合に自動でシャットダウン、電源オフを実行
- モニターを5分以上使用していない場合、スタンバイモードに変更

(3) 導入の効果

ITのエネルギー管理を開始した2011年7月から2012年3月までの8ヶ月間での電力削減量は23.17MW/h、CO2排出量に換算すると13.9tを削減することができました。また、社内ポータルにJouleXでモニターした消費電力を表示することによる社員の節電意識の向上にも役立ったと感じています。今後もモニターした結果を元に既存の節電ポリシーのカスタマイズや新しい節電ポリシーの追加を行い、ユーザーへのサービスレベルを維持しながら節電効果の向上を図っていきたいと考えています。

(4) 将来の展望

オフィスのIT機器に対するエネルギー管理によって消費電力の削減がある程度効果があることがわかりました。そしてユーザーへのサービスを維持しながら節電のためのポリシー運用を実施していくことのノウハウを得ることができました。

このノウハウを活用し、より大きな電力を消費するデータセンターのサーバやネットワーク機器への提供拡大を検討していきたいと考えています。お客様へのサービス品質を下げることなく消費電力を削減できれば、お客様へ新しい価値を提供できるばかりか、社会や地域への貢献も実現できると考えています。

6.4　事例4：株式会社ラック

(1) 導入の経緯・目的

3.11の災害後、業務上で可能な範囲での節電を実施することになりました。節電に関しては様々な取り組みを実施しましたが、特に「定常的に電力を利用する」社内のサーバ環境及び試験環境に関して、移設などを伴う対策を実施し、これが奏功しました。

(2) 社内サーバ環境特有の検討点

節電を行うに際して最も問題になったのは、「節電した結果品質が大幅に劣化しては、サービス継続上問題が発生する」ことと、サーバのような「サービスを提供し続けることに意味があるサービスをどのように節電するか？」です。この問題の解決策は、それぞれの事情において様々に異なることと思いますが、本検討では、影響度や範囲の整理を行い、続いて実施していなかった対策の適用を検討しました。

①　影響の整理

サービス提供及びサービス継続の問題から主に、以下の2点の影響を考慮すべき状況にありました。

- 「試験環境の利用に制限が加わる」ことは「サービス品質の劣化」に直接影響することを意味する
- 「サーバの利用に制限が加わること」は、「業務効率」に直接影響する事を意味する

②　未実施であった対策

当社固有の状況として、以下に挙げる対策は実施されていました。

- 当社ではサービス提供のために、IDC(インターネットデータセンター)を利用している
- 既に業務効率の向上と情報保護のために、一部社員に対しリモートデスクトップを利用した仮想端末を割り当てている

(3) 節電対策と節電効果

この状況を利用し、節電対策を検討した結果、以下の方策を採ることで節電効果とコスト削減効果を生み出すことが見込まれました。

- 複数台のサーバの整理を実施し、仮想化した上でIDCに収容する

- 試験環境などのネットワーク機材などをIDCに移設し、遠隔から利用する

この対策は、まず出来るものから実施するという方針に基づき実施しました。その結果、「マシンルーム電気料金」及び「マシンルーム空調料金」に効果が現れました。

○ マシンルーム電気料金：約10%削減

○ マシンルーム空調料金：約18%削減

(4) 節電効果の主な理由

節電効果を生み出せた理由を以下に挙げます。

- オフィスに設置してある機器を減少させることによって、発熱が減少し、空調設備に掛かる負荷が下がり、電力消費量が減少する
- 機器をまとめることにより、「高消費電力・低性能」のサーバ機器多数から「低消費電力・高性能」の機器少数に集約できた、その結果、必要電力総量を大きく減らせる
- 一般的なオフィスビルにおいては、業務時間帯における空調料金とそれ以外の時間帯における空調料金には差がある。後者の料金は、利用料に合わせて追加で徴収される事になる場合が多いと考えられる。しかし、IDCにおいては24時間365日、固定額のため、この部分のコスト削減が可能になる
- (当社の場合)既にIDCを利用していたため、余分なコストが発生しなかった。また、既に契約済みの電力の内、利用されていなかった部分に収容できたため、追加コストが一切発生しなかった
- IDCを利用することによって、空調などのコストを大きく抑えることができた。

当社の例はIDCを既に利用しており初期費用がかからなかった部分など一般的とは言えない部分もありますが、上手にIDC等の外部業者を利用することで、コスト削減や電力消費を抑えることができると考えられます。

おわりに

本ガイドブックは、企業の節電対応策として在宅勤務の導入を検討されていたり、事業継続対策を考えておられる皆様を対象に、情報セキュリティの観点からこれだけは知っておくべきという考え方や対策方法についてのノウハウをまとめたものです。東日本大震災という未曽有の大災害をきっかけに、各企業・組織、個人がそれぞれ節電の意識を高めると共に、これまでの働き方を変えようという動きが拡大しています。そして、そのような変革をサポートする新しい技術やサービスが現れはじめています。それらを有効に活用する上でも、本ガイドブックが一助となれば幸いです。

今後、皆様が実践された経験等をフィードバックしていただき、本ガイドブックをより有用なものとすべく改善していきたいと考えています。ぜひご意見、ご質問等を下記までお寄せ下さい。

特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）事務局
E-Mail： sec@jnsa.org
（件名を「節電・在宅勤務ガイドブックについて」などとしていただけると幸いです）

ワーキンググループメンバーと執筆担当

＜2012 年度改訂版メンバー＞（氏名の五十音順・敬称略、◎＝リーダー）

	赤間　健一	トレンドマイクロ株式会社	
	稲場　未南	みずほ情報総研株式会社	（編集）
	小川　博久	みずほ情報総研株式会社	（1章、編集）
	金田　智史	株式会社シマンテック	（6章）
	許　　先明	株式会社ラック	（4章）
	津村　賢哉	株式会社ラック	（4章）
◎	冨田　高樹	みずほ情報総研株式会社	（1章、編集）
	西尾　秀一	株式会社エヌ・ティ・ティ・データ	（2章、6章）
	本多　規克	アルプスシステムインテグレーション株式会社	（1～3章）
	松橋　孝志	トレンドマイクロ株式会社	（4章）
	山田　一博	株式会社ラック	（4章）
	吉野　賢剛	F5 ネットワークスジャパン株式会社	（3章）

＜2011 年度版メンバー＞（所属は当時のもの）

赤間　健一	トレンドマイクロ株式会社
池永　章	株式会社シマンテック
市川　順之	伊藤忠テクノソリューションズ株式会社
稲場　未南	みずほ情報総研株式会社
小川　博久	みずほ情報総研株式会社
奥原　雅之	富士通株式会社
栂　　崇	日本アイ・ビー・エム システムズ・エンジニアリング株式会社
金子　以澄	日本 CA 株式会社
川辺　康史	株式会社メトロ
桐山　太一	株式会社アーク情報システム
小林　青己	ソフトバンク・テクノロジー株式会社
坂本　慶	サイバーソリューション株式会社
鈴木　英樹	株式会社 OSK
須永　知之	株式会社富士通ソーシアルサイエンスラボラトリ
仙田　健	株式会社富士通ソーシアルサイエンスラボラトリ
高橋　崇	株式会社インフォセック
田中　洋	株式会社インフォセック
手塚　信之	住商情報システム株式会社
徳田　敏文	日本アイ・ビー・エム株式会社
冨田　高樹	みずほ情報総研株式会社
友國　直樹	トレンドマイクロ株式会社
永田　牧子	株式会社富士通ソーシアルサイエンスラボラトリ
西尾　秀一	株式会社エヌ・ティ・ティ・データ

肥田　雄一朗	クオリティ株式会社
藤田　延也	F5 ネットワークスジャパン株式会社
別府　卓也	株式会社 OSK
本多　規克	アルプスシステムインテグレーション株式会社
松木　豪	株式会社アーク情報システム
松田　康宏	株式会社メトロ
宮崎　亮	株式会社 JMC
森　真梨子	伊藤忠テクノソリューションズ株式会社
山本　総夫	ソフトバンク・テクノロジー株式会社
油井　秀人	富士通エフ・アイ・ピー株式会社
横川　典子	トレンドマイクロ株式会社
吉野　賢剛	F5 ネットワークスジャパン株式会社
渡辺　仙吉	日本アイ・ビー・エム株式会社

付録1：在宅勤務で有用な製品・サービスの紹介

〇在宅勤務の際のデータ搬送を安全にするセキュリティ USB メモリ作成ソフト

「InterSafe SecureDevice」

SecureDevice は、汎用 USB メモリをセキュリティ USB メモリに変換するソフトウェアです。
セキュリティ USB メモリ内のデータは、USB メモリ内で編集・保存は出来ますが、自宅 PC へコピーすることは出来ません。簡単に安全な在宅勤務環境をご提供します。
また、オプションのセキュアポーターを使用することで、USB メモリ内のデータを暗号化し、メールやクラウド上で安全にやり取りすることが可能です。

【製品情報詳細】

http://www.alsi.co.jp/security/sd/

http://www.alsi.co.jp/security/issd_p/

◆お問い合わせ先◆

アルプス システム インテグレーション株式会社

営業統括部

E-Mail: ssg@alsi.co.jp

TEL：03-5499-1331

○モバイル PC 向け Web フィルタリングサービス「InterSafe CATS」

モバイル PC のフィルタリングが可能なクラウド型 Web フィルタリングサービス。

社内ネットワークに接続していない在宅勤務時の Web アクセス管理を実現します。

さらにファイル共有ソフトなどのプログラム起動制限も可能。Web 経由の情報漏えいや私的利用、ウイルスのダウンロードを防止します。

フィルタリングサービスとして唯一、「ASP・SaaS 安全・信頼性に係る情報開示認定制度」の認定を取得しています。

【製品情報詳細】

http://www.alsi.co.jp/security/iscats/

◆お問い合わせ先◆

アルプス システム インテグレーション株式会社

営業統括部

E-Mail: ssg@alsi.co.jp

TEL：03-5499-1331

○外部デバイス持出し管理ソフト「InterSafe ILP」

外部デバイスへの不正なデータ持出を制御します。持ち出す際は、ワークフローの申請・承認によって許可されたファイル・媒体のみ持出し可能です。また、コピーガード・ウイルス対策付きセキュリティ USB メモリが作成できるため、自宅の PC でも安全に作業できます。

仮想デスクトップ環境（VMWare View5.1）もサポートしますので、VDI 使用時のデバイスを制御できます。

【製品情報詳細】

http://www.alsi.co.jp/security/ilp/

◆お問い合わせ先◆

アルプス システム インテグレーション株式会社

営業統括部

E-Mail: ssg@alsi.co.jp

TEL：03-5499-1331

〇テレワークに最適なセキュリティソリューション「BizSMA(TM)」

テレワークで有効なスマートフォンやタブレット型端末といったスマートデバイス活用に必要となる、セキュリティ対策の検討、情報システムにおけるセキュリティ基盤整備、利用者教育などを提供するサービスです。

【ソリューションご紹介】
http://www.nttdata.co.jp/release/2011/061700.html

◆お問い合わせ先◆
株式会社 NTT データ
基盤システム事業本部　セキュリティビジネス推進室
TEL：050-5546-2301

〇在宅勤務に最適なリモートアクセスソリューション「BIG-IP Edge Gateway」

F5 ネットワークスの提供する「BIG-IP Edge Gateway」は、高いセキュリティとアプリケーションの高速化機能を備え、モバイルネットワーク環境やリモート拠点にて、ビジネスユーザに対して安全で快適なアプリケーション利用環境を、コスト効率良く提供します。

【ソリューションご紹介】
http://www.f5networks.co.jp/topics/edge/

◆お問い合わせ先◆
F5 ネットワークスジャパン株式会社　F5 First Contact
TEL：03-5114-3210
http://www.f5networks.co.jp/fc/
受付時間：平日　9:30～18:00

○どこでも仮想デスクトップを実現する「BIG-IP Access Policy Manager(APM)」

F5 ネットワークスの提供する「BIG-IP APM」は Web アプリケーションアクセスの利便性とセキュリティの向上を可能にするソリューションです。仮想アプライアンスでも提供している為、余ったサーバのリソースを有効に利用し、VMware 社や Citrix 社の仮想デスクトップ環境をスモールスタートで始めたい場合にも最適です。下記のソリューション紹介ページでは VMware 社の提供する仮想デスクトップ製品 VMware View との連携について、ご紹介しています。

【ソリューションご紹介】
http://www.f5networks.co.jp/topics/apm/

◆お問い合わせ先◆
F5 ネットワークスジャパン株式会社 F5 First Contact
TEL：03-5114-3210
http://www.f5networks.co.jp/fc/
受付時間：平日 9:30～18:00

○F5 コンサルティングサービス

大手金融業、製造業等での SSL-VPN 接続サービス等、ミッションクリティカルなシステムにおける豊富なコンサルティング実績に基づき、リモートアクセスにおける認証システム・端末環境に合わせた最適なセキュリティレベルとコストのバランスの取れたポリシーのコンサルティングを行い、失敗のない導入をお手伝い致します。例えば、単一のグローバル IP アドレスで ActiveSync, Outlook Web Access（OWA）,SSL-VPN のゲートウェイを統合した基盤をご提案することも可能です。

【サービスご紹介】
http://www.f5networks.co.jp/service/consulting/

◆お問い合わせ先◆
F5 ネットワークスジャパン株式会社 F5 First Contact
TEL：03-5114-3210
http://www.f5networks.co.jp/fc/
受付時間：平日 9:30～18:00

○PC の電源設定を管理する 「Altiris Client Management Suite」

企業が設定する節電目標に応じて、PC の電源設定(Windows の場合「電源オプション」の設定)を制御します。例えば、電源を接続した状態で離席した場合に、モニタを Off にするまでの時間やスタンバイ状態にするまでの時間を管理者がポリシーとして指定し、PC に対して強制的に制御をかけることができます。

【詳細情報】

http://www.symantec.com/ja/jp/client-management-suite

◆お問い合わせ先◆
株式会社 シマンテック
シマンテックセールスインフォメーションセンター（法人向け）
受付時間：10:00～12:00, 13:00～17:00（土、日、祝日、年末年始を除く）
Tel: 03-5229-1912

○ディスク全体暗号化「Symantec PGP Whole Disk Encryption」

在宅勤務を推進する上で重要となるノートパソコンの紛失・盗難による情報漏えい対策、その鍵となるのがハードディスクの暗号化です。Symantec PGP Whole Disk Encryption(PGP WDE)は OS の領域はもちろん一時領域を含むブートディスクをまるごと暗号化することにより情報を確実に保護します。スタンドアロンでの導入展開はもちろん、管理サーバーである PGP Universal Server と併用することにより、各ノートパソコンに対し企業ポリシーの適用、パスフレーズを忘れてしまった際の復旧など安全かつ柔軟な運用管理が実現できます。

【詳細情報】
http://www.symantec.com/ja/jp/business/whole-disk-encryption

◆お問い合わせ先◆
株式会社 シマンテック
シマンテックセールスインフォメーションセンター（法人向け）
受付時間：10:00～12:00, 13:00～17:00（土、日、祝日、年末年始を除く）
Tel: 03-5229-1912

〇持ち出しに対応したエンドポイントセキュリティ製品

「Symantec Endpoint Protection」

ノートパソコンなどを持ち出し、在宅勤務をするために、エンドポイントをしっかり保護できるセキュリティソフトウェアが必要です。Symantec Endpoint Protection は、持ち出されたパソコンをウイルスやワームから保護するために必要な、ウイルス対策、侵入防止（IPS）、デバイス制御を統合した製品です。社内ネットワークと社外ネットワークを認識し、接続されたネットワークに応じて、セキュリティ対策ポリシーを自動的に切り替えることで、持ち出されたノートパソコンを様々な脅威からしっかりと守ります。

【詳細情報】

http://www.symantec.com/ja/jp/business/endpoint-protection

◆お問い合わせ先◆

株式会社 シマンテック

シマンテックセールスインフォメーションセンター（法人向け）

受付時間：10:00～12:00, 13:00～17:00（土、日、祝日、年末年始を除く）

Tel: 03-5229-1912

〇スマートフォン、タブレットなどのモバイルデバイスを管理する

「Symantec Mobile Management」

在宅勤務やオフィス外勤務において活用されるスマートフォンやタブレットといったモバイルデバイスを、より安全かつ効率的に使えるようにポリシーで管理します。例えば、メールや VPN、Wifi などのスマートフォンの設定の自動化、パスワードの強制、リモートワイプ、Jailbreak の検出など情報を保護するための機能を提供します。

【詳細情報】

http://www.symantec.com/ja/jp/mobile-management

◆お問い合わせ先◆

株式会社 シマンテック

シマンテックセールスインフォメーションセンター（法人向け）

受付時間：10:00～12:00, 13:00～17:00（土、日、祝日、年末年始を除く）

Tel: 03-5229-1912

〇企業の節電対策をサポートする「Trend Micro Power Management オプション」

「Trend Micro Power Management オプション」は、ウイルスバスターコーポレートエディション導入環境に機能追加として導入することで、企業内にある PC の電源プランを節電ポリシーに準じた設定に強制変更すると共に、レポート機能によって節電効果を一元で把握することが出来ます。

【製品情報詳細】
http://jp.trendmicro.com/jp/products/enterprise/corp_pm/

◆お問い合わせ先◆
トレンドマイクロ株式会社
法人お問い合わせ窓口
Tel: 03-5334-3601

〇ワークスタイル変革ソリューション(在宅勤務支援)

弊社が提供する次世代のワークスタイルは、仮想デスクトップ、ユニファイドコラボレーションと急速に導入の進むスマートデバイスを組み合わせて、オフィスに縛られない働き方を実現するものです。お客様との時間、家族との時間を両立したいという弊社社員のワークライフバランスに向けた声を実現したノウハウをお客様にご提供致します。

【次世代ワークスタイルへの取り組み】
http://www.netone.co.jp/report/case/20120323-2.html

【ソリューションご紹介】
デスクトップ仮想化ソリューション
http://www.netone.co.jp/biz/solution/vdi.html
ユニファイドコミュニケーションソリューション
http://www.netone.co.jp/biz/solution/uc.html

◆お問い合わせ先◆
ネットワンシステムズ株式会社
http://www.netone.co.jp/contact.html

〇統合エネルギー管理システム「JouleX Energy Manager」

JouleX Energy Manager は、企業において今まで見えていなかった IT 機器の消費電力の可視化を実現します。デバイスを幅広くサポートし、種類やベンダの異なるデバイスを一括で管理可能です。

【製品情報詳細】

http://www.lac.co.jp/service/fasirity/joulex.html

◆お問い合わせ先◆

株式会社ラック　ブランドソリューション営業部

Tel: 03-6757-0100

E-Mail: sales@lac.co.jp

付録2：参考になる情報源

節電･BCP（事業継続）対策に向けたテレワークの活用（総務省）
http://www.soumu.go.jp/main_content/000119363.pdf

情報漏えい発生時の対応ポイント集（独立行政法人情報処理推進機構（IPA）、2012 年 3 月）
http://www.ipa.go.jp/security/awareness/johorouei/

SOHO 事業者における情報セキュリティ対策の調査研究報告書（財団法人マルチメディア振興センター、2005 年3月）
http://www.fmmc.or.jp/information/report/upfiles/46/045.pdf

テレワークの推進（総務省）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/

テレワーク（国土交通省）
http://http://www.mlit.go.jp/crd/daisei/telework/index.html

在宅ワークの適正な実施のために（厚生労働省）
http://www.mhlw.go.jp/seisakunitsuite/bunya/koyou_roudou/koyoukintou/zaitaku/index.html

情報通信機器を活用した在宅勤務の適切な導入及び実施のためのガイドライン（厚生労働省）
http://www.mhlw.go.jp/houdou/2004/03/h0305-1.html

社団法人日本テレワーク協会
http://www.japan-telework.or.jp/index.html

情報漏えい対策サイト「情報セキュリティ対策チェックシート」（セコム株式会社）
http://www.secomtrust.net/infomeasure/rouei/check.html

テレワークの有する可能性（みずほ情報総研株式会社によるコラム記事）
http://www.mizuho-ir.co.jp/publication/column/2012/0327.html
http://www.mizuho-ir.co.jp/publication/column/2012/0424.html
http://www.mizuho-ir.co.jp/publication/column/2012/0529.html
http://www.mizuho-ir.co.jp/publication/column/2012/0626.html

付録3：目的別チェックリスト

在宅勤務や節電対策等において考慮すべき事項を目的別に整理しました。皆様のところで事業継続計画・情報セキュリティ対策を立案する際にご活用ください。

① 在宅勤務Ⅰ（企業の ICT 機器を用いて業務を行う場合）

カテゴリ	チェック項目	条件・論点等	本書記載頁	チェック
在宅勤務に関する規定	就業規則等の見直し		P21	
	ICT機器の職場外持ち出し規定の整備		P24	
	情報資産の職場外持ち出し規定の整備	シンクライアントの場合は不要	P24	
在宅勤務する従業員	在宅勤務の実施に関する申請		P24	
	就業時間や職場との連絡方法に関する上司との合意形成		P21, P24	
	家族との調整	セキュリティ確保、勤務時間確保に関する協力	P22-23	
自宅等に設置するシンクライアント、タブレットデバイス等	必要数の調達	シンクライアントの実現方法には専用端末、USB型、タブレットデバイス利用など多くの方法がある	P30-32	
モバイルPC等	必要数の調達			
	ディスク暗号化	ハードディスク、SSD等の暗号化	P38-39 P45-46	
	外部書き出し規制	シンクライアントとしてPCを用いる場合、USBメモリやメモリカード、CD/DVDへの書き出しを規制する	P39-P40	
職場までのネットワーク	業務遂行可能な通信速度を有する回線の確保	企業が提供する無線接続、または従業員が契約するインターネット接続など（費用負担はどちらで行うか検討の必要有り）	P50-53	
	安全な接続方法の提供	VPNサービスなどによる通信経路上の暗号化	P51-53	
	無線LANのセキュリティ対策	WPA2による暗号化の設定が必要	P47-49	
在宅勤務者のサポート	マニュアルの作成		P24	
	教育の実施		P24-25	
	サポートサービスの提供		P24	
インシデント対応	情報漏えいの発生などを例とする訓練の実施		P25-26	

② 在宅勤務Ⅱ（従業員の私物を用いて業務を行う場合）

カテゴリ	チェック項目	条件・論点等	本書記載頁	チェック
在宅勤務に関する規定	就業規則等の見直し		P21	
	情報資産の職場外持ち出し規定の整備		P24	
在宅勤務する従業員	在宅勤務の実施に関する申請		P24	
	就業時間や職場との連絡方法に関する上司との合意形成		P21, P24	
	家族との調整	セキュリティ確保、勤務時間確保に関する協力	P22-23	
従業員の私物PC	業務で必要なアプリケーションのインストール	認証用アプリケーション、業務用アプリケーション、オフィスソフトウェア等	P41-44	
	セキュリティ設定、 セキュリティ強化		P42-44	
職場までのネットワーク	業務遂行可能な通信速度を有する回線の確保	企業が提供する無線接続、または従業員が契約するインターネット接続など（費用負担はどちらで行うか検討の必要有り）	P50	
	安全な接続方法の提供	VPNサービスなどによる通信経路上の暗号化	P51-53	
	無線LANのセキュリティ対策	WPA2による暗号化の設定が必要	P47-49	
在宅勤務者のサポート	マニュアルの作成		P24	
	教育の実施		P24-25	
	サポートサービスの提供		P24	
インシデント対応	情報漏えいの発生などを例とする訓練の実施		P25-26	

③ 停電対策（停電となる拠点での必要最小限の業務継続）

カテゴリ	チェック項目	条件・論点等	本書記載頁	チェック
停電によるICT機器の故障防止	無停電電源の設置	サーバ及びネットワーク機器用に準備	P75-76	
停電時の電源供給	必要機器の抽出			
	大容量蓄電池の準備		P77	
	ディーゼル発電機の準備		P76	
	燃料の確保		P76	

④ 節電対策（可能な限り通常の業務機能を維持しつつ節電目標を達成）

カテゴリ	チェック項目	条件・論点等	本書記載頁	チェック
電力需要の可視化	機器の種類・設置場所の把握		P79	
	時間軸での消費傾向の把握		P79-80	
節電ポリシーの実行	ツールによる監視・制御		P80-81	
	PDCAサイクルによる改善		P82	

オフィスの節電と在宅勤務における
事業継続・情報セキュリティ対策ガイドブック

2012 年 7 月 13 日　　第 2 版公開

特定非営利活動法人日本ネットワークセキュリティ協会（JNSA） 社会活動部会
在宅勤務における情報セキュリティ対策検討ワーキンググループ　編著

（お問い合わせ先）
特定非営利活動法人日本ネットワークセキュリティ協会（JNSA） 事務局
〒105-0003　東京都港区西新橋1－22－12　JC ビル3F
TEL：03-3519-6440　　FAX：03-3519-6441　　E-Mail：sec@jnsa.org