少人数スタッフ施設のための
「情報セキュリティ」最初の一歩

2012 年 4 月

＜参考・引用＞　IPA　「５分で出来る自社チェックシート」
http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-shindan-s.pdf

◆目次

はじめに
第 1 回　保管について
第 2 回　持ち出しについて
第 3 回　廃棄について　その 1
第 4 回　廃棄について　その 2
第 5 回　事務所について　その 1
第 6 回　事務所について　その 2
第 7 回　事務所について　その 3
第 8 回　パソコンについて　その 1
第 9 回　パソコンについて　その 2
第 10 回　パソコンについて　その 3
第 11 回　パソコンについて　その 4
第 12 回　パスワードについて　その 1
第 13 回　パスワードについて　その 2
第 14 回　パスワードについて　その 3
第 15 回　ウィルス対策について　その 1
第 16 回　ウィルス対策について　その 2
第 17 回　メールについて　その 1
第 18 回　メールについて　その 2
第 19 回　メールについて　その 3
第 20 回　バックアップについて
第 21 回　従業者について　その 1
第 22 回　従業者について　その 2
第 23 回　取引先について
第 24 回　事故対応について
第 25 回　ルールについて

2012 年 2 月～4 月まで、スタッフブログに連載したものに加筆・修正して編集したものです。

◆　はじめに

　このままで大丈夫かなぁ？と思いつつ、取り組むきっかけが見つからないまま、日々の多忙さに埋もれていく・・・かもしれないのがパソコン周りの安全対策ではないでしょうか？

　というわけで、保育園や作業所など、スタッフの人数が少ない施設を想定して、それでも取り組まなければならない「情報セキュリティ（安全対策）」を、全２５ポイントについてご紹介していきます。

　すぐに取り組めるものもあれば、毎日こつこつとすることもあります。

　また、専門のベンダー（サービス提供会社）と相談しなければならないこともあります。

　ブログを読んでいただいた後、すぐに起こしてもらうアクションも一緒にご紹介しますので、これを機会に、皆様の職場の情報セキュリティについて点検をしてみてください。

　なお、２５のポイントについては、情報処理推進機構（IPA）が作成した

　「５分で出来る自社チェックシート」

　http://www.ipa.go.jp/security/fy20/reports/sme-guide/documents/sme-shindan-s.pdf

をもとにしています。先を急ぐ方は、こちらをご利用ください。

　お役に立てれば幸いです。

◆第１回　保管について

　まずは、チェックから。

　外出時、離席時に重要情報を机の上に放置せず、鍵付き書庫または指定の場所に保管し施錠するなど、重要情報がみだりに扱われないようにしていますか？

　これはもう、整理整頓、躾のレベルのお話ですが、情報セキュリティの基本中の基本に間違いありません。やりっぱ、なげっぱ、すてっぱ・・・は職場文化として出来るだけ排除するようにしましょう。

　出来るだけ、スタッフが着席していないときのデスクには、書類をはじめモノを置かないようにしてみてください。

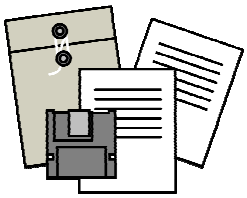
　各担当のデスクに立てかけてあるファイルなども、一度置き場所について、その場所で本当に大丈夫かどうか検討してみることもお勧めです。

　出来るだけ書類置き場はキャビネットにまとめて、必要に応じてキャビネットから持ち出すという方法の方が、無用のトラブルを回避することができると思われます。

　ともあれ、結構、デスク周りの整理整頓状況というのは、人から見られているものです。

　地味な対策ですが、まずはここからスタートしましょう！

◆第２回　持ち出しについて



まずは、チェックから。

重要情報を社外へ持ち出す時はパスワードロックをかけ、盗難・紛失対策をしていますか？

そもそも、何をもって重要情報とするか？が決まっていないと、ロックをかけるかけないの判断がつきませんねぇ。

まずは紙、パソコン問わずファイルを作るときから、情報のランク付けをするのも方法のひとつです。

取り急ぎ、持ち出しについては、個人情報であれば、パスワードロックをかけ、盗られたり、なくしたりしないよう、たとえ盗られたりなくしたりしても、容易にその情報が見られないようにするなどの対策をしてください。

個人情報のほか、会議資料や予算･決算資料なども重要情報です。

仕事で使っている情報を持って外に出るときのルールは、たとえば「持ち出し５ヶ条」など作って、掲示したり、持ち出す人に読んでもらってから出かけさせるなどなどいかがでしょうか？

この持ち出しという行為は、結構お気楽に考えている人が多いのが現実です。

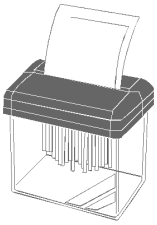
多くが仕事熱心で、勤務時間内に仕事が終わらないから、自宅でやろう・・・という動機で。

けれど、紛失した場合は、大変な責任が問われることを承知しておいてもらいましょう。

「持ち出し５ヶ条」（例）

１．利用者の氏名が記載されている情報は、外に持ち出さないこと
２．どうしても持ち出す場合には、必ず上長の承認を得ることとし、無断で持ち出さないこと
３．.持ち出した情報が電子データの場合は、絶対にパスワードを設定し、記録媒体は肌身離さず携行すること
４．持ち出した情報が紙の場合、中味の見えない封筒に入れ、肌身離さず携行すること
５．第三者の目に入る場所で情報を見ないこと

◆第３回　廃棄について　その１



まずは、チェックから。

重要な書類やＣＤなどを廃棄する場合は、シュレッダーで裁断するなどのように、重要情報が読めなくなるような処分をしていますか？

書類の裏の白紙がもったいないからと、そのままメモ用紙やお絵かき用として流用すると、思わぬところから情報漏えいとなる場合があります。

実際にあったお話ですが、お役所から高齢者リストが流出したケースでは、担当部署が廃棄リストとして保管していたものを、隣の保育課が管轄の公立保育園の園児のお絵かき用の紙として回し、保護者がびっくり！というケースもありました。

せめて、個人名がわかるところは切り抜くくらいの配慮は必要です。

ちなみに、マジックなどで塗りつぶしても、データは見え見えなので意味がありません。

ゴミ箱に捨てる前に、情報は意味不明、判読不可能の状態にすることを癖にしてしまいましょう。

◆第４回　廃棄について　その２

まずは、チェックから。

重要情報の入ったパソコン・記憶媒体を廃棄する場合は、消去ソフトを利用したり、業者に消去を依頼するなどのように、電子データが読めなくなるような処理をしていますか？

そうなんです、パソコンはそのまま捨ててはいけません。

せめて、ハードディスクだけでも取り出しておきましょう。

マウスをクリックして削除・・・という作業だけでは、データは「削除するデータ」という印をつけられただけで、確かに存在したままなのです。

現在、電子機器を廃棄するには、所定の手続きや免許のある業者さんでなければできませんので、機器の廃棄そのものには大変気を使われると思いますが、中味のデータまで責任を持ってくれるわけではありません。

リース契約をしているパソコンなどについては、リース会社と、リース期限を迎えたパソコン内のデータの消去についてはどのような扱いになるか確認をしておきましょう。

◆第５回　事務所について　その１

まずは、チェックから。

　事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？

　事務所に入ったら、見知らぬ人が・・・お客様だと思って挨拶だけしたけれど、何者？と思うシーンってありますよね。
　お客様には、確かにお客様だとわかるゲストバッチなど付けてもらうようにしましょう。
　誰かが知っていると思ったら、結局誰も知らなかった・・・なんてことにならないように、目に見える対策が必要です。
　また、事務所内に外部の人だけ残してしまうなどというのも気をつけてあげましょう。
　残された方は、あらぬ疑いを持たれたらどうしようと、大変落ち着かないものです。
（以前、代表社印をデスクに出しっぱなしにして出かけてしまった社長さんがいました。残された身は、代表社印から目をはずすことが出来ず、ひたすら固まっておりました）

◆第６回　事務所について　その２

まずはチェックから。

　ノートパソコン利用者は、退社時に、机の上のノートパソコンを引き出しに片付けるなどのように、盗難防止対策をしていますか？

　事務所からパソコンが盗まれたことで、被害者なのに個人情報を漏えいしてしまったとして加害者になってしまうケースがあとを絶ちません。
　こんな残念な目に遭わないように、デスクに置いたノートパソコンは、仕事を終えて帰宅されるときには、必ず引き出しなど、出来たら鍵のかかる所定の場所に片付けるようにしてみてください。
　とにかく、フリーで出しっぱなしはいけません。
　ノートパソコンそのものならば代用もききますが、中に入っている情報は、一度外にでてしまったらもう、回収不能と心得ましょう。

◆第７回　事務所について　その３

まずはチェックから。

最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？

情報セキュリティのお話ではありますが、職場のセキュリティそのものを点検してみましょう。

最後に職場を出る人は、パソコンやポット、コピーなどの電源を切ったり、さまざまな点検事項があるはずです。

いつ、誰が、必要なチェックをしたかどうか、何時に帰ったのかなど記入表を用意します。

スタッフの人数が少ないと、お互いなあなあになったり、「当たり前」なために、何も記録に残らない傾向が強くなりますが、記録を残すことで意識を強めたり、何かあったときの証拠ともなることを考えておきましょう。

◆第８回　パソコンについて　その１

まずはチェックから。

Windows Update　を行うなどのように、常にソフトウェアを安全な状態にしていますか？

上の質問について、Windows Update　って何？　と思った方、またはなぜ、Windows Update が必要なのかよく知らないという方は、すぐにパソコン関係の取引があるベンダー（サービス事業者）に連絡をとって、直に説明を受けましょう。

これは、パソコンを利用したり、または管理する立場の方は「絶対」に必要な知識と対応だからです。

ここでいう　Windows Update　とは、マイクロソフト社が提供しているウィンドウズパソコンの不具合を修正するプログラムのことですが、パソコン内の情報を漏えいさせないためには、セキュリティホールと呼ばれる欠陥などを潰していく作業がどうしても必要となります。

これを怠るということは、バックの底に穴を開けたまま、硬貨を入れておくようなものです。

バッグの底をふさぐ努力は、バッグの持ち主の責任です。

実際に、どのようなタイミングで、どのような方法で行われるのかは、ベンダーに確認の上、常にソフトウェアを安全な状態にするために必要な対策は、専門家であるベンダーとよく相談して検討をしてください。

費用をかけなければ守れないものも当然でてきます。

◆第９回　パソコンについて　その２

まずはチェックから。

ファイル交換ソフトを入れないようにするなどのように、ファイルが流出する危険性が高いソフトウェアの使用を禁止していますか？

今回もやはり、「ファイル交換ソフトって何？」と思った方、聞いたことはあるけれど、実際何が問題なのか説明が出来ない方は、専門家と相談してみましょう。

ファイル交換ソフトは、Winny や Share といった名称のものが代表的なもので、インターネット上で不特定多数のコンピュータ間でファイル（データ）をやり取りできるソフトウェアのことをいいます。

便利な反面、自分でも気がつかないうちに、自分のデータが他人と共有されてしまう場合があります。

個人的な趣味でパソコンを使うわけではありませんから、原則、仕事で使うパソコンには導入を禁止することがほとんどです。

職場の管理者がそれと知らないうちに、職場のパソコンにインストールされているケースも耳にしますので、まずは今使用中のパソコンにファイル交換ソフトが入っていないかどうか、確認しておきましょう。

確認の方法がわからない場合は、ベンダーに相談を！

素人がすぐに対応できる問題ではありませんから、専門家を活用してください。

その次には、職場としてファイル交換ソフトの使用禁止を規定明文化し、パソコンを利用するスタッフに周知徹底させてください。

◆第 10 回　パソコンについて　その３

まずはチェックから。

社内外での個人パソコンの業務使用を許可制にするなどのように、業務で個人パソコンを使用することの是非を明確にしていますか？

パソコンを買う予算がないとか、個人で持っているパソコンの方が性能が高いとか、使い慣れているとか、そんな理由で個人パソコンが職場に持ち込まれることがありませんか？

融通性に富む少人数の職場では結構「あり」だったりします。（気持ち、すごくわかります）けれど、今日を限りに、それは「なし」にしましょう。

もし、どうしても個人パソコンを仕事に利用させるようであれば、それはそれで、しっかりとしたルール（責任の所在、対象業務の範囲、経費負担等）を決める必要があります。これはこれで、大変な作業です。

なぜ個人パソコンの利用を制限するかは、職場による情報の管理の徹底が図れないからです。

徹底されない情報管理のもとでは、情報の安全など望むべくもありません。

◆第 11 回　パソコンについて　その 4

まずはチェックから。

退社時にパソコンの電源を落とすなどのように、他人に使われないようにしていますか？

節電が国民的努力として求められている昨今、パソコンの省電力はとても重要な課題です

・・・という面は確かにあるのですが、ここは情報のセキュリティのお話ですね。

他人に「どうぞ使ってください」とばかりの状態に置いてしまう、その神経の緩さが問題です。気をつけましょう。

◆第 12 回　パスワードについて　その 1

まずはチェックから。

パスワードは自分の名前を避けるなどのように、他人に推測されにくいものに設定していますか？

職員一人に一台のパソコンでない場合、パスワードは設定していなかったりされることが多いようですが、共有であってもパスワードは設定しておきましょう。

少なくとも第三者が容易にパソコンを使用することを防ぐ効果があります。

このパスワードも、職員の方の名前にしたり、施設の名称にするなどは避けて、よその人にはわからないけれど、内部の人は良く知っている～という連想ができるパスワードだといいですね。

◆第 13 回　パスワードについて　その 2

まずはチェックから。

パスワードを他人が見えるような場所に貼らないなどのように、他人にわからないように管理していますか？

当たり前のことですが、とても大事なことです。
最近ではもう、大丈夫かと思いますが、パスワードを決めたあと、なんのためらいも無く、付箋紙にパスワードを書いてパソコンに貼り付けた方に遭遇したことがあります。
最近のパスワードは最低でも６桁、厚労省のガイドラインでは８桁英数字混じりを推奨していますが、当時はたった４桁だったのにもかかわらず・・・気をつけましょう！

◆第 14 回　パスワードについて　その 3

まずはチェックから。

ログイン用のパスワードを定期的に変更するなどのように、他人に見破られにくくしていますか？

パスワードは一度設定したら定期的に変更するものなのです。
このような場合の「定期的」は常識では１ヶ月間ですね。
厳密に実施すると、２世代前（前の前）までと同じパスワードは使わないようにします。
配置転換や、退職者が出た場合などは、定期的であることにとらわれずに即、変更することをお勧めします。
ルーチンワークの中に、パスワードを変更する日を決めておいてもいいかもしれません。

◆第 15 回　ウィルス対策について　その 1

まずはチェックから。

パソコンにはウイルス対策ソフトを入れるなどのように、怪しい Web サイトや不審なメールを介したウイルスから、パソコンを守るための対策をおこなっていますか？

具体的にどんな対策をとっているか説明が出来るようであれば合格ですが、よくわからないなぁ・・・という場合は、やはり専門家（ベンダー）に協力してもらいましょう。
セキュリティレベルの設定は、最低→普通→高度とレベルがありますので、予算と相談

しながら決めておきましょう。
　ここはしっかり対策をとらないと、安全管理義務違反になる可能性がありますからしっかり！

◆第 16 回　ウィルス対策について　その 2

まずはチェックから。

　ウイルス対策ソフトのウイルス定義ファイルを自動更新するなどのように、常に最新のウイルス定義ファイルになるようにしていますか？

　定義ファイルって何？と思った方は、即、専門家（ベンダー）にご相談を！
　ウィルス定義ファイルとは、コンピュータウィルスを検出するためのデータベースファイルで、いわばウィルス一覧表のようなものです。
　この一覧表に載っているウィルスが入っていないかを確かめるわけですね。
　一覧表が常に最新になっていないと、新種のウィルスはスルーをして、皆さんのパソコンに入り込んでしまうので、一覧表が最新であることはとても大切なことなのです。

◆第 17 回　メールについて　その 1

まずはチェックから。

　電子メールを送る前に、目視にて送信先アドレスの確認をするなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？

　これは、ついうっかりやってしまうミスへの対策です。
　送る前にチェックする・・・を体に覚えさせることが必要ですね。
　一度失敗して、ひやっとした経験でもないと、つい手を抜いてしまいがちです。
　電子メールの使い方については、見よう見真似ではなく、一度しっかりとルールやお作法を確認しておきましょう。

◆第 18 回　メールについて　その 2

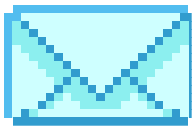
まずはチェックから。

　お互いのメールアドレスを知らない複数人にメールを送る場合は、Bcc 機能を活用するな

どのように、メールアドレスを誤って他人に伝えてしまわないようにしていますか？

Ｃｃ機能とＢｃｃ機能の違いや、その使い方については正しく理解していますか？
前回の送信前の目視同様、メールのルールやお作法を確認しておきましょう。
知らない間柄ではないだろうと、ご本人の了解を得ないままに、他人にメールアドレスを知られるようなことをしてしまうと、大きな信用問題になりかねません。
重々、気をつけましょう。
＊　Bcc　Blind　Carbon　Copy の略で、他の受信者にメールアドレスを伏せて送信する機能

◆第 19 回　メールについて　その 3

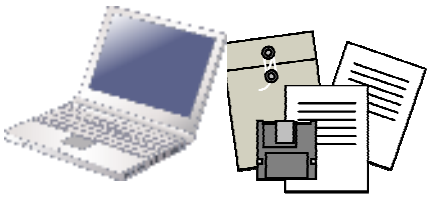


まずはチェックから。

重要情報をメールで送る場合は、暗号メールを使うか、重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？

メール本文に重要情報を記述するのは避けましょう。
ワード文書などにして、それをパスワード付きの添付ファイルにする方が安全です。
その場合のパスワードはメール本文に書くことはせずに、電話を使うなどして相手先本人に直接連絡する方法が一般的です。
パスワードをつけずに添付ファイルを送ってはいけません！

◆第 20 回　バックアップについて



まずはチェックから。

バックアップについて重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？

情報が何らかの理由で失われた場合、またはウィルス感染などで使用できなくなった場合に備える必要があります。
どのようなバックアップ対策が有効かは、専門家と相談して実施するのが早道です。
外部記憶装置にバックアップをとることが一番容易ではありますが、この場合、外部記憶装置（ハードディスクやフラッシュメモリなど）の管理もまた厳重に行う必要が生じます。
継続した運用が可能なように、「定期的」に行うためのルールも作る必要があります。
「１」のつく日はバックアップの日にするなど決めておくのも良いと思います。
（スーパーの安売り日みたいですけど・・・忘れないかもしれない）

◆第 21 回　従業者について　その 1

さて、今回からは、全体的なマネジメントがチェックの対象です。
ではまずはチェックから。

採用の際に守秘義務があることを知らせるなどのように、従業者に機密を守らせていますか？

当たり前のことを認識したり、実行したりするのが一番難しいものですね。
守秘義務については、誓約書を取り交わすなど、意識的な働きかけが必要です。

◆第 22 回　従業者について　その 2

まずはチェックから。

情報管理の大切さなどを定期的に説明するなどのように、従業者に意識付けを行っていますか？

ここでいう「定期的」とは月に一度・・・より少し緩めで、最低でも年に１回というあたりでしょうか？
個人情報保護のガイドラインなどでは、個人情報についての教育を少なくとも年に１回と規定しているので、これと合わせて説明会や勉強会を実施してもいいかもしれません。
こういうときに、ベンダーの担当営業などに手伝ってもらいましょう！

◆第 23 回　取引先について

まずはチェックから。

取引先について契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、取引先に機密を守ることを求めていますか？

すべての取引先を対象にしているわけではありませんが、個人情報や会計情報などを取り扱う取引先との契約には、かならず秘密保持の契約条項を入れる必要があります。
すでに契約書の取り交わしが済んでいるような場合は、業務契約書とは別に、秘密保持契約書などを取り交わすこともあります。

◆第 24 回　事故対応について

まずはチェックから。

　事故対応について重要情報の流出や紛失、盗難があった場合の対応手順書を作成するなどのように、事故が発生した場合に備えた準備をしていますか？

　事故は起きないに越したことはありませんが、事の大小に関わらず起きたときはもう、パニックになります。
　一度に対処しなければならない問題が押し寄せてくるものですから、誰に、何を、どうするといったことはあらかじめ決めておくことを絶対的に、お勧めします。

◆第 25 回　ルールについて

今回で最後のチェック。最後といえば、仕上げということです。
まずはチェックから。

　ルールについて情報セキュリティ対策（上記 1～24 など）を会社のルールにするなどのように、情報セキュリティ対策の内容を明確にしていますか？

　決めたことはルール化して、運用を継続していかなければなりません。
　すべての手順などは、誰でも参照できるように、またルールが形骸化していないかを点検できるように明文化します。
　今回ご紹介した１～２４のポイントを項目にして、決めたことを記述すればりっぱな「情報セキュリティ規定」が出来ます。ただし、本当に最初の一歩の規定なので、上手に育ててりっぱな規定にしてあげてください。

おわり