# 税理士業務のための
# ITリスク管理術

作・東海税理士会　情報システム委員会　イラスト・水島みき

# 目　次

# 第１章　若手税理士の事件簿

そう、俺はITを駆使して最先端システムを使いこなす若手税理士･･･と、勝手に思い込んでいた。そして事件は起きた。

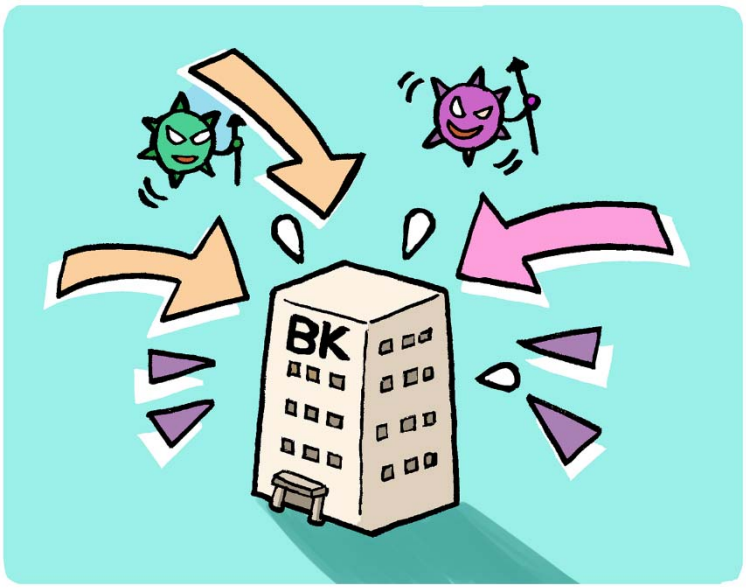
1 年前、平成〇〇年 3 月 14 日午前 11 時過ぎ。
確定申告の山場を過ぎて、若干落ち着きはじめた事務所で携帯電話が鳴った。

「ABC 銀行です。先生、今どちらにいらっしゃいますか？」
少しあわてた様子の担当者。

「事務所で申告の最終確認中ですよ。」
「先生、今日の 10 時 40 分頃ネットバンクを使ってらっしゃいましたか？」

「いや、今日は一度もログインしていませんが･･･」

「では、他にログインできる人はいらっしゃいますか？」
「もう一人居るには居るけど、今日はずっと外だし･･･、聞いてはみますが･･･」




「何かありましたか？」

「実は、先生のネットバンクに不正アクセスらしき形跡がありまして、今現在、当行で先生のネットバンクを停止しています。急ぎの振込みがあれば窓口まで･･･」

「ん？どういうこと？不正アクセス？」
「不正アクセスらしきって何？」

「先程、先生のネットバンクに何者かがログインした後、振込み指示の最後にワンタイムパス（銀行から渡されている乱数表）を入力するところで、不正入力が頻発してシステムが停止しました。その後も頻繁にアクセスしている形跡があります。」

「その他にも異常アクセスされている口座が当行の他にもありまして･･･」

「近隣の金融機関との連携で不正アクセスがあった場合は連絡を取り合うのですが、他行でも確認されているそうです！」

「事情は分かったけど、結論から言うと･･･俺の口座は大丈夫だったわけ？」

「ワンタイムパスが無ければ不正送金されていましたが、取り敢えず最後の最後で止まりましたので実害はないです。」

この電話の後、しばらく現実のことと認識するまでに時間がかかる俺。

そして、数日後。

「あれから当行で検討の結果、警察へ事件捜査の依頼をすることになりましたので、先生にも協力して頂くことになりますので宜しくお願いします。」

自分のログインID等がなぜ漏れた？もしくは盗まれたのか疑問だったので、当然この展開は自分にとっては有りがたい。

そして地元警察から連絡。
「地元警察のIT犯罪担当ですが、他にも同地域の金融機関で不正アクセス事案が有りますので、県警のサイバー犯罪対策課が伺います。よろしいでしょうか？」

（なにか大事になってきた！？）

「わかりました。ぜひお願いします。」

電話を切って、すぐ、今度は県警から入電。
「今から、伺いたいのですがどうですか？」

「大丈夫です、お待ちしております。」

電話を切って 1 時間後。県警 3 人組がやってきた。警視、警部、鑑識。
話もそこそこに鑑識が事務所 PC をいじりだす。

「いつもネットバンクをする PC はどれですか？」
「アクセスはどの PC でもできるか？」
「触るのは誰か？」
「ID の管理はどうなっているか？」等々
警視の質問に答えながら鑑識が事務所の PC を操作しているのを覗き込む。

すると、鑑識の手が止まった。


「警視、出ました。ほぼ間違いなくこの PC から ID 他が盗まれています！」

あっ　ソレ俺の PC。

マジかー！
何が起きたんだー！？

「え？どういうことですか？」
やっと我に返って鑑識に聞いてみる。

「この PC は『ウイルスに感染』しています！このフォルダーの中にある･･･云々カンヌン･･･。と、いうわけで、絶対ではないが、ほぼこの PC が流出元で間違いないでしょう。」

鑑識さん、ありがとうございました（泣）

高校から PC をかじり始めてはや 20 年。いろんなトラブルに巻き込まれてきたけど、その分トラブルには強いと思いこんでいた。ネット社会もいち早く乗りこなしてスマートに税理士業を展開していくはずだったのに･･･
ウイルス対策ソフトの過信か、PC への知識不足か。本業ではないところで足元をすくわれた感じだ。

鑑識の現場作業が終わると、今度は警視さんの事情聴取が始まった。
自分の事務所なのにお客さん側に座って質問攻めにあう。
何だろう、この違和感。被害者なのに責められている感じ。

事情聴取の内容はそれほど覚えてないが、終盤で先程の鑑識さんが一言。

「ところで、なぜこのシステムの旧バージョンが入っているの？」
「流出はウイルス感染によるものだけれども、そもそもウイルスに感染したのはこの旧バージョンの『セキュリティーホール』からの感染が濃厚なんだけど。」

え？そうなの？

「バージョンアップしなくても業務に支障がなかったので、そのまま使ってました･･･。」
俄かに警視の顔が引きつる。

ついでの質問でワンタイムパスの仕組みも確認される･･･
「ワンタイムパスはメールで届くやつかな？それとも専用機器かな？」

「いえ、この紙です」
名刺サイズの紙を出す。

「え？紙？」

「紙ですが、何か･･･」

警視
「これは乱数表であって、ワンタイムパスなどではない！」

「金融機関にもセキュリティ強化を徹底させないと！」

こんな感じで県警の対応が終わると、最後は感染PCを本部で解析にかけるため没収されてしまった･･･

･･･それから、約 1 年後･･･

県警担当者から久しぶりの入電で、ことの顛末が知らされた。

まず、犯人は海外から国内のセキュリティが甘い PC を探し出し、そこを経由して遠隔操作でウイルス拡散、ネットバンク情報収集を行っていたらしい。
その標的となった PC は某県在住のおじいちゃんの Windows XP（セキュリティソフト未設定）。
おじいちゃんがネット環境で何をしていたか定かではないが、県警の捜査でもう PC は触らないと言っていたという･･･。

これは、東海税理士会会員の実話に基づくフィクションです。

PC セキュリティを怠った場合、自分自身の被害のみならず、図らずも関与先にもご迷惑をかけることになり得ます。
マイナンバー管理も加わったこの時期ですので、今一度、PC セキュリティだけでなく事務所の危機管理体制を見直してみてはいかがでしょうか。

第 1 章で自分のパソコンがウィルスに感染して大変な目にあった若手税理士。
実はセキュリティ対策をしっかりしていればウィルス感染は防げた可能性があります。
そんな若手税理士の体験を他人事だと思っている皆さん

## こんな勘違いしていませんか？

### 【その 1】うちはパソコンをインターネットに繋いでいないから安全だ ➡ NO！

インターネットに繋いで常にセキュリティのアップデートを行うため、インターネットに繋いでいないとそのアップデートができません。

顧問先の会社から USB で仕訳データをもらってきて、事務所のパソコンに取り込んだら一緒にウィルスも取り込んでしまった事例がたびたびあります。

さらに、ウィルスに感染したパソコンから仕訳データを USB で取り出して、顧問先のパソコンに取り込んだら顧問先のパソコンもウィルスに感染させてしまう可能性もあります。

### 【その 2】うちはパソコンの管理をすべて業者に任せているから安全だ ➡ NO!

各ベンダーの保守契約がされているパソコン以外は保守対象外になっており、知らぬ間にウィルスに感染していることがあります。

### 【その 3】うちはパソコンでメールやインターネットはやっていないから安全だ ➡ NO!

現在は FAX 等の複合機や電話がインターネットにつながっていることがあります。
さらに、FAX の内容が複合機の中に保存されていることもあり、それを知らずに複合機を処分したら機密情報を外部に流出させてしまう危険があります。

## 情報システムのセキュリティ対策は自分で行うことが大切です！！

また、マイナンバーの施行により、事務所での安全管理措置が求められています。
組織的安全管理措置　人的安全管理措置　物理的安全管理措置　技術的安全管理措置があり、この中でも情報システムのセキュリティ対策は、物理的安全管理措置と技術的安全管理措置に役立ちます。それらを税理士自身や職員にも徹底させることで人的安全管理措置にもつながります。

第 2 章・第 3 章では自分でできるセキュリティ対策をご紹介します。

# 第 2 章　お金をかけずにできるセキュリティ対策

## 1. こんな時にも　サインインパスワードの設定

所長　　「西川さん、浮かない顔をしているけど何かあったのか？」

スタッフ（西川）　「昨日訪問したお客様のところへノートパソコンを忘れてきてしまって。今から取りに伺うのですが、パソコンの中には他のお客様の資料も入っているので不安で。」

所長　　「そうか。サインインパスワードは設定してあるのか？」

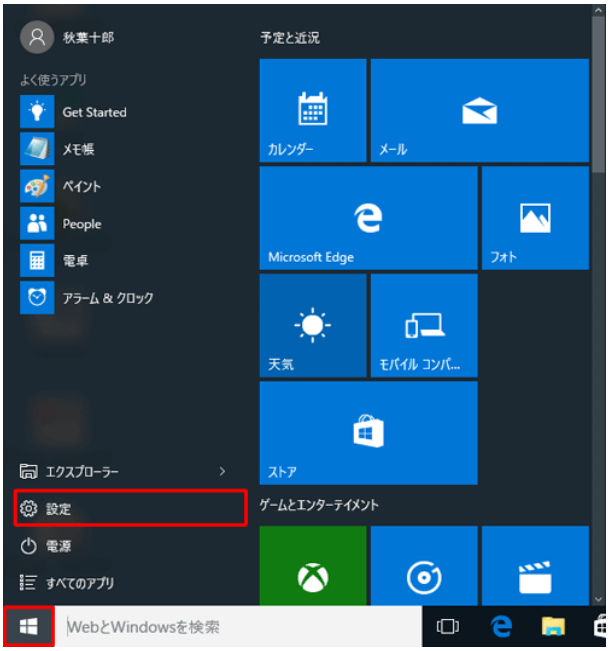
スタッフ　「それが・・・。 設定方法がわからなくて設定していないのです。」

所長　　「設定方法を教えるから、帰ってきたら設定しなさい。今回は、お客様のところだから大丈夫だと思うが、悪用されると大変だ。」

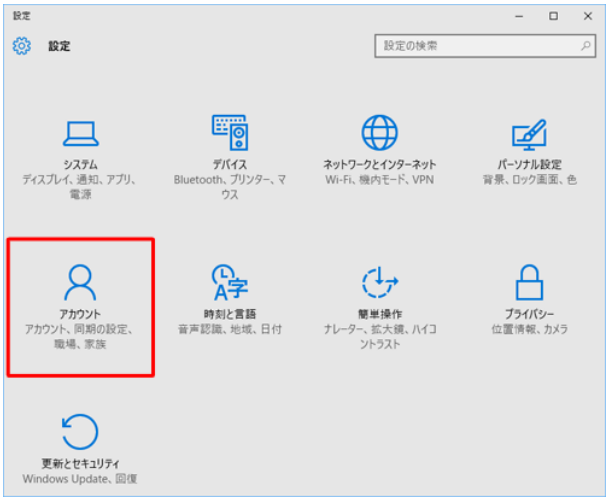
スタッフ　「すみません。急いで取りに行ってきます。」

## サインインパスワードの設定

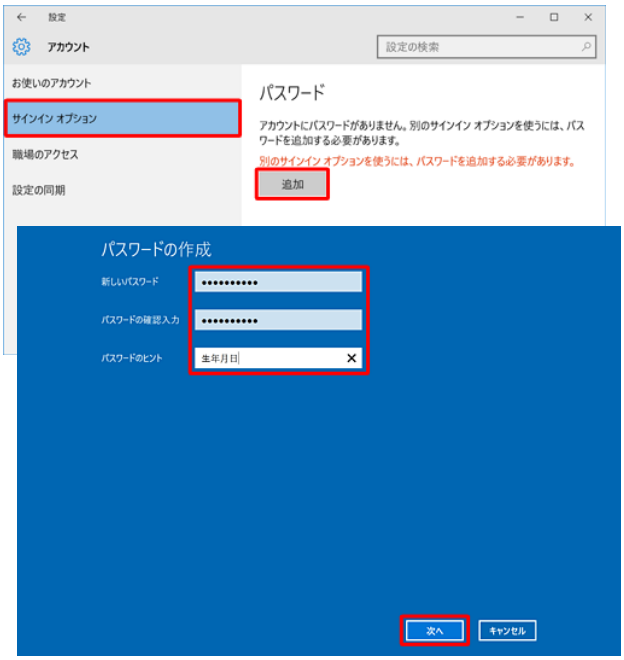
Windows では、アカウントのユーザーごとにパスワードを設定することができます。
パスワードを設定すると、パソコンにサインインするときパスワードの入力が必要になります。
自分のユーザーアカウントにパスワードを設定しておくことで、第三者によるデータの閲覧を防ぐことができ、長時間席を離れるときにも有効です。
特にノートパソコンやタブレットパソコンの場合には紛失に備えてセキュリティを強化できます。
Windows 10 でユーザーアカウントのパスワードを設定する際の操作手順を説明します。




1.「スタート」→「設定」の順にクリックします。




2.「設定」が表示されます。
　アカウント」をクリックします。



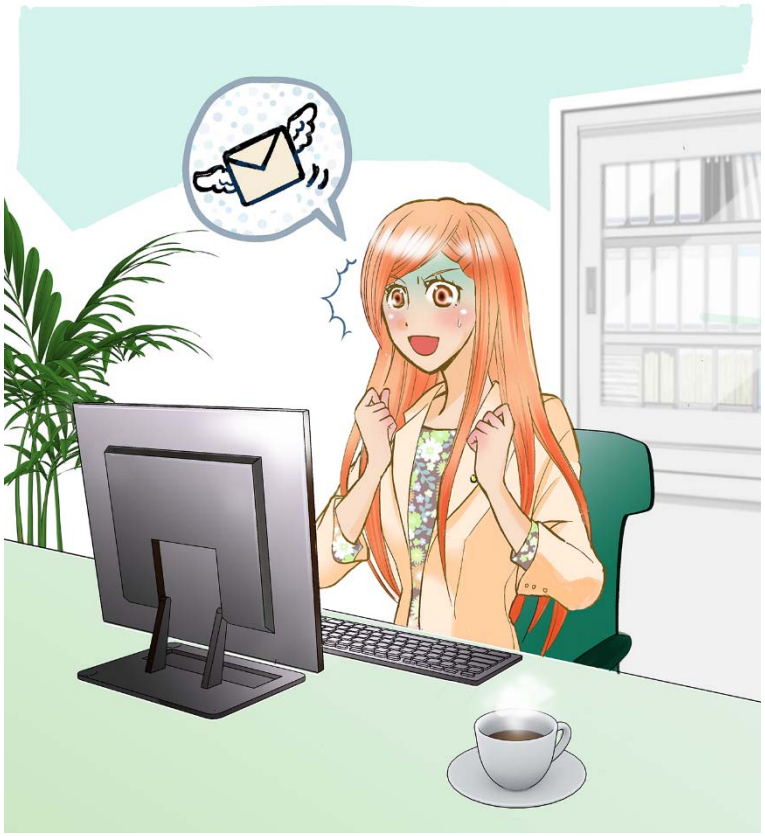

3.「サインインオプション」をクリックし、「パスワード」欄の「追加」をクリックします。

4. パスワードの作成」が表示されます。
　「新しいパスワード」「パスワードの確認入力」ボックスに設定したいパスワードを入力し、「パスワードのヒント」ボックスに、パスワードを忘れたときに備えてヒントを入力して、「次へ」をクリックします。

5.「完了」をクリックします。 以上で操作完了です。

次回サインインする際に、「パスワード」ボックスが表示されることを確認してください。

## 2. メールの誤送信を防ぐ



所長　　「西川さん、焦っているけど　どうした？」

スタッフ　「お客様から頼まれた試算表をメール送信しようと思ったのですが、ファイルを添付するのを忘れて
（西川）　　送ってしまったので、お詫びと併せてもう一回送らないといけないのです。」

所長　　「メールは送ってしまってから誤りに気付くことがあるな。うちの事務所では、送信前に一旦「送信トレイ」に保存されるように設定してチェックを増やすようにしよう。」

スタッフ　「この設定にすれば、送信前にチェックを 1 回増やせますね。」

所長　　「それと、添付ファイルは重要な情報があることが多いから、添付ファイルにはパスワードを設定して万が一誤送信しても情報が漏洩しないようにしよう。」

スタッフ　「はい。これで安心ですね。」

## 電子メールの誤送信による情報漏洩を防ぐ

電子メールの誤送信による主な情報漏えい事故は、以下に示す事例が多いようです。

① 宛先間違いにより発生する事故

② 一斉送信メールの送信方法の誤りによるメールアドレス漏えい事故

①の事故については、電子メール利用者の不注意が原因である場合が多いようですが、②の事故は電子メールの扱いに関する不慣れが原因となる場合が多いようです。

どちらの場合も、電子メールの宛先に関する問題であり、利用者が注意すれば防げる問題です。

これらのミスを防ぐためには、以下の対策が効果的です。

a. 電子メール送信前に、宛先や内容、添付ファイル有無の再確認を行う

b. TO、CC および BCC の使い方を理解する

C. 添付ファイルを暗号化する

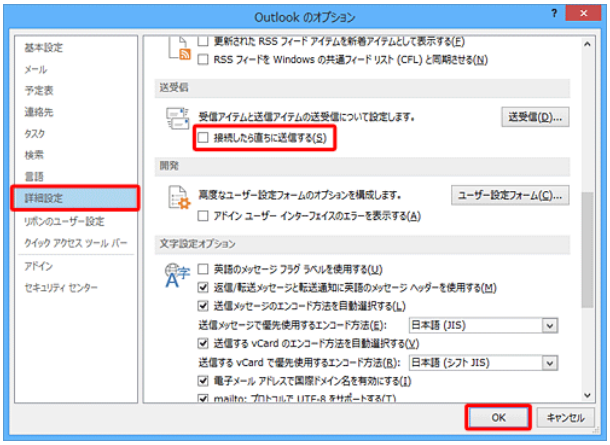
### a. 電子メール送信前に、宛先や内容、添付ファイル有無の再確認をする

電子メールを作成し、メール作成画面で送信ボタンをクリックすると、即送信されるのが一般的な（初期）設定です。送信ボタンをクリックする前に、宛先の再確認をすることが必要ですが、仮に送信ボタンをクリックしてもすぐに送信されない設定に変えることで、宛先等の再確認にさらなるチャンスが生まれます。

ここでは Outlook 2013 で作成したメールについて送信ボタンをクリックしてもすぐに送信されず、一旦「送信トレイ」に保存する際の操作手順を説明します。


1. リボンから「ファイル」タブをクリックします。


2. 「オプション」をクリックします。




3. 「Outlook のオプション」が表示されます。
「詳細設定」をクリックし、「送受信」欄の「接続したら直ちに送信する」のチェックを外して、「OK」をクリックします。 以上で操作完了です。

「送信トレイ」に保存されたメールを送信する場合は、リボンから「送受信」タブをクリックし、「送受信」グループの「すべて送信」をクリックします。

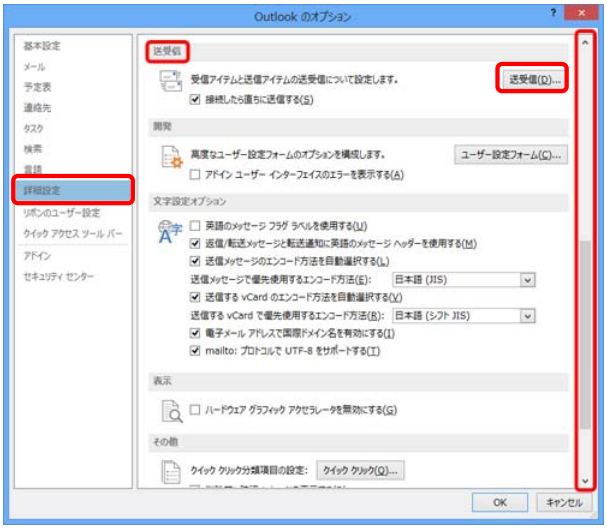
＜補足＞

メールの送受信を自動的に行う設定になっている場合は、「送信トレイ」に保存されたメールも設定時間が経過すると、自動的に送信されますので注意が必要です。

「送信トレイ」のメールが自動的に送信されないように、メールの送受信方法を手動に設定する場合は、以下の操作を行ってください。

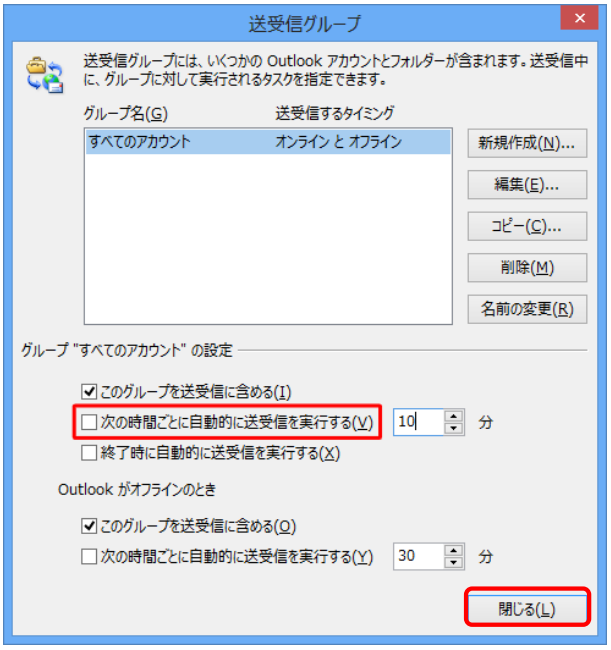

1. リボンから「ファイル」タブをクリックします。


2. 「オプション」をクリックします。




3. 「Outlook のオプション」が表示されます。

「詳細設定」をクリックし、画面右側のスクロールバーを移動して、「送受信」欄が表示されるまで画面をスクロールし「送受信」をクリックします。




4. 「送受信グループ」が表示されます。

「グループ"すべてのアカウント"の設定」欄の「次の時間ごとに自動的に送受信を実行する」のチェックを外して、「閉じる」をクリックします。 以上で操作完了です。

### b. TO、CC および BCC の使い方

電子メールをする時に、「TO」や「CC」、「BCC」の機能があります。これを理解しないまま使っていると、知らず知らずのうちにメールアドレス漏えい事故を起こしている可能性があります。 ここで一度「TO」「CC」と「BCC」の使い方を確認してみましょう。

**「TO」とは**

メールを送りたい相手（主送信先）のメールアドレスを入力します。カンマで区切って複数のメールアドレスを入れることもできます。

**「CC」とは**

カーボン・コピーの略です。基本的には、複数の人にメールを送る時に入力します。主送信先（TO)に対して副送信先がいる場合は CC にメールアドレスを記入します。

・CC に入力した相手には、TO に送るメールと同じメールが配信されます。

・CC に入力したメールアドレスはメールを受け取った人も参照できます。

ビジネスで使う場合、「TO（宛先）の人に送ったので参考までに見てくださいね」という送信者の意図を表すことができます。

事務所などで、同僚 A に対して会議の連絡をメールで送りたい時は、宛先（TO）には同僚 A のメールアドレスを入力します。と同時に、A に対してメールで連絡したことを上司 B にも知っておいてもらいたい場合は、「CC」欄に上司 B のメールアドレスを指定します。すると同僚 A にも上司 B にも、全く同じメールが届きます。

CC 機能の注意点は、メールを受け取った相手には、送信先のアドレスが全て見えること。「TO」や「CC」で複数の相手に一斉にメールを送る場合、お互いにメールアドレスがわかっても問題ない関係なのか確認が必要です。お互いのメールアドレスが表示されてしまうので、場合によっては個人情報（メールアドレス）の漏えいになりかねません。取引先とメールをやり取りする時は十分に注意しましょう。

**「BCC」とは**

ブラインド・カーボン・コピーの略です。CC と同じく複数の人にメールを送る時に入力します。

・BCC に入力した相手には、TO に送るメールと同じメールが配信されます。

・BCC に入力したメールアドレスはメールを受け取った人からは参照できません。

BCC メールは、「面識がない人たちに一斉にメールを送る時」に使います。

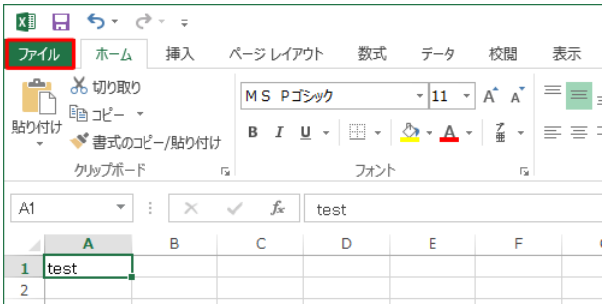
「TO」 に送信者自身のメールアドレスを入力して、「BCC」 に複数のアドレスを入力すれば、受け取った人たちは「BCC」に入力したメールアドレスは一切見ることができません。

「BCC」は、取引先（「TO」）に送ったメールを、自分の上司（「BCC」）にも見てもらいたい場合や、お互い面識のない人たちに一斉にメールを送りたい時に便利です。

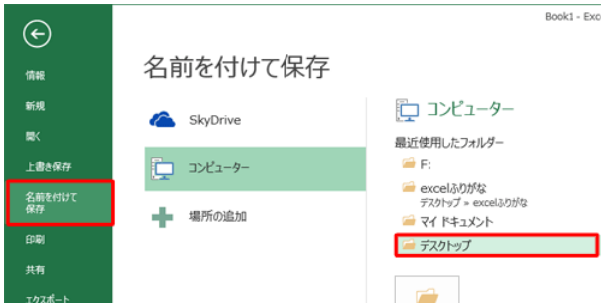
### C. 添付ファイルを暗号化する

電子メールで重要なファイルを送信する際、ファイルにパスワードを設定し暗号化するのが効果的です。これは、万が一ファイルが第三者に渡ってしまっても、閲覧できないようにするためです。ここでは、ビジネスで電子メールに添付することが多い Excel ファイルと PDF ファイルについてパスワードの設定方法を説明します。

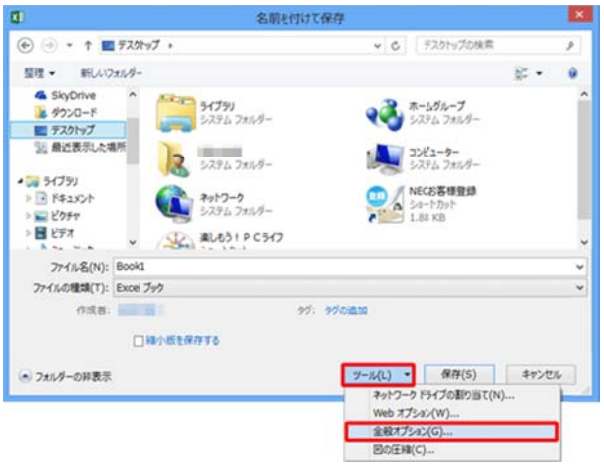
## Excel2013 の場合



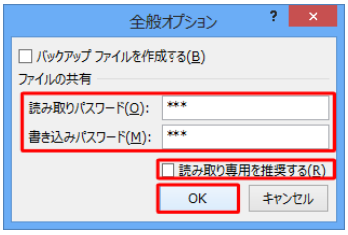

1. パスワードを設定するファイルを開き、リボンから「ファイル」タブをクリックします。




2. 「名前を付けて保存」をクリックし、保存先をクリックします。
   ここでは例として、保存先として「デスクトップ」をクリックします。

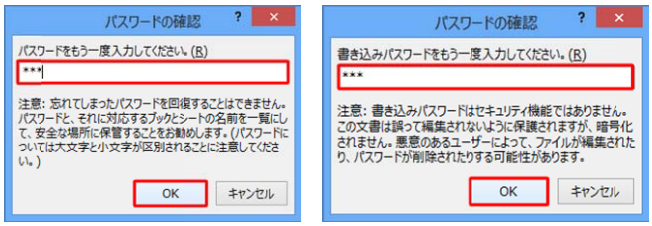



3. 「名前を付けて保存」が表示されます。
   画面下部の「ツール」をクリックして、表示される一覧の「全般オプション」をクリックします。




4. 「全般オプション」が表示されます。
   「ファイルの共有」欄の「読み取りパスワード」ボックスと「書き込みパスワード」ボックスに任意のパスワードを入力して、「OK」をクリックします。
   ・読み取りパスワード ： ファイルを開く際のパスワードです。
   ・書き込みパスワード ： ファイルを編集する際のパスワードです。
   ※読み取りパスワードと書き込みパスワードは個別にパスワードを設定することもできます。

5. 「パスワードの確認」が表示されます。
   設定したパスワードを再度入力して、「OK」をクリックします。



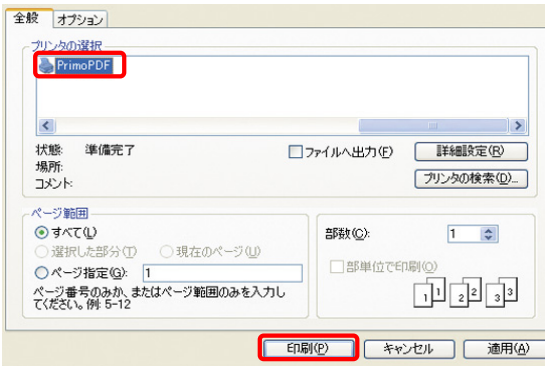

※書き込みパスワードはファイルの編集を制限する機能です。


6. 「ファイル名」ボックスにファイルの名前を入力して、「保存」をクリックします。 以上で操作完了です。

## PDF ファイル（PrimoPDF の場合）

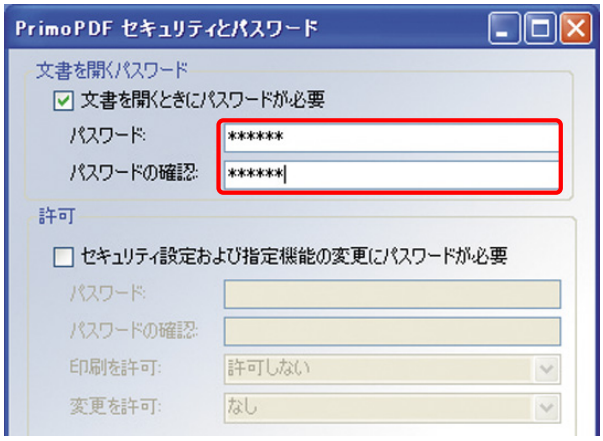
PDF ファイルの作成は Adobe 社の「Acrobat」というソフトが一般的ですが、今回は無料のソフトであるエクセルソフト社の「PrimoPDF」というソフトで操作手順を説明します。

1. 「PrimoPDF」がインストールされていない場合にはダウンロード、インストールを行います。
   ※インターネットで「PrimoPDF」と検索し、XLsoft Corporation の公式ホームページからダウンロードしてください。




2.PDF ファイルに変換したいデータを開き、「ファイル」→「印刷」を開くと、「PrimoPDF」というプリンタがあるので、選択して「印刷」ボタンをクリックします。


3. 「PDF のセキュリティ」の「変更」をクリックします。




4. 「文書を開くときにパスワードが必要」にチェックしてパスワードを設定し、「OK」をクリックします。


5. PDF ファイルの保存先を指定し、出力するファイル名を入力し、「PDF の作成」をクリックします。 以上で操作完了です。

暗号化した添付ファイルを送信した後に、相手先にパスワードを伝える際には安全のため電話や FAX などにし電子メール以外の方法で伝えるのが効果的です。

## 3.パスワードについて


所長　　「最近はパスワードを解読され情報が盗まれる事件が増えているようだが、西川さんのパスワードはどんなものかね？」

スタッフ（西川）　「『nishikawa1010』です！」

所長　　「それは苗字と何ですか？」

スタッフ　「誕生日です！！」

所長　　「ずいぶんとわかりやすいな。すぐに変えた方がいいな。」

スタッフ　「でも・・・ どのようなパスワードにしたらよいのかわからなくて・・。」

所長　　「よし！　一緒に考えよう。」

**パスワードの付け方と管理の仕方について**

外部からのサイバー攻撃によって、情報が盗まれてしまう場合があります。
これは決して、大手企業だけの話ではなく、私たちの管理している小規模のサイトや、ウェブサービス、SNS なども攻撃対象となっています。
「自分なんかが狙われるわけない。」と思っているのであれば要注意です。
サイバー攻撃のほとんどは、無差別で行われています。
サイバー攻撃の場合、コンピューターが自動的に数字やよくある名前、辞書に掲載されている単語を自動的に組み合わせたりして勝手にやっています。
推測しやすいパスワードを設定してしまうと、それだけすぐに解読されてしまうということです。

パスワードを付ける際には「複雑なパスワードにすることです。
ポイントとしては、
① 8 文字以上にする
② アルファベットの大文字と小文字を含める
③ ＠ などの記号を含める
という点を守ってください。
それを踏まえた上で、自分だけにわかるルールでパスワードを作っておくと良いでしょう。

例えば、
名前 2 文字＋家族の誕生日 4 桁＋氏名 2 文字＋携帯番号下 4 桁＋＠ といった感じで、パスワードのルールを決めます。
山田太郎、妻の誕生日7月 23 日、携帯番号 090―1234―5678 の場合、先ほどのルールでパスワードを作ると、
「Ta0723Ya5678＠」となります。
すると、他の人が見た場合はよくわからなくても、自分だけはルールを覚えていれば、思い出せるわけです。

サービスごとサービス名等のアルファベットをどこかに加えたりすることで異なるパスワードを作成することができます。

ルールを自分で決めて、パスワードを作ってみてください。
※上記のルールはそのまま使わないでください！

＜参考文献＞

・NEC パーソナル商品総合情報サイト　121ware　サービス＆サポート　Q&A

・独立行政法人　情報処理推進機構セキュリティセンター　電子メール利用時の危険対策のしおり

・BIGLOBE　エンジョイ！マガジン　メールの「CC」と「BCC」の使い方とマナー

・教えて君.net　パスワード付きの PDF を作成する方法を教えて。

・オクゴエ！　解読されにくい正しいパスワードの付け方と管理の仕方

# 第 3 章　ちょっとお金をかけてできるセキュリティ対策

## 1. 物理的なセキュリティ対策 「物理的安全管理措置」

税理士事務所はお客様の大切な個人情報を多数保管しています。その中でも最近はパソコンでほとんどの重要な情報を閲覧できる状態にあります。
事務所への訪問者が事務所内を見ることなく応接室に入れるようにすることが一番ですが、なかなかそこまでやるのは難しいです。
そこで次のような対策をとると良いでしょう。

### (1)訪問者にパソコンの画面を見せないようにする。

**① 事務所内の机のレイアウトを工夫する**
**② 事務所内や机にパーテーションを設置する**
**③ パソコンの画面に「のぞき見防止フィルター」を装着する**

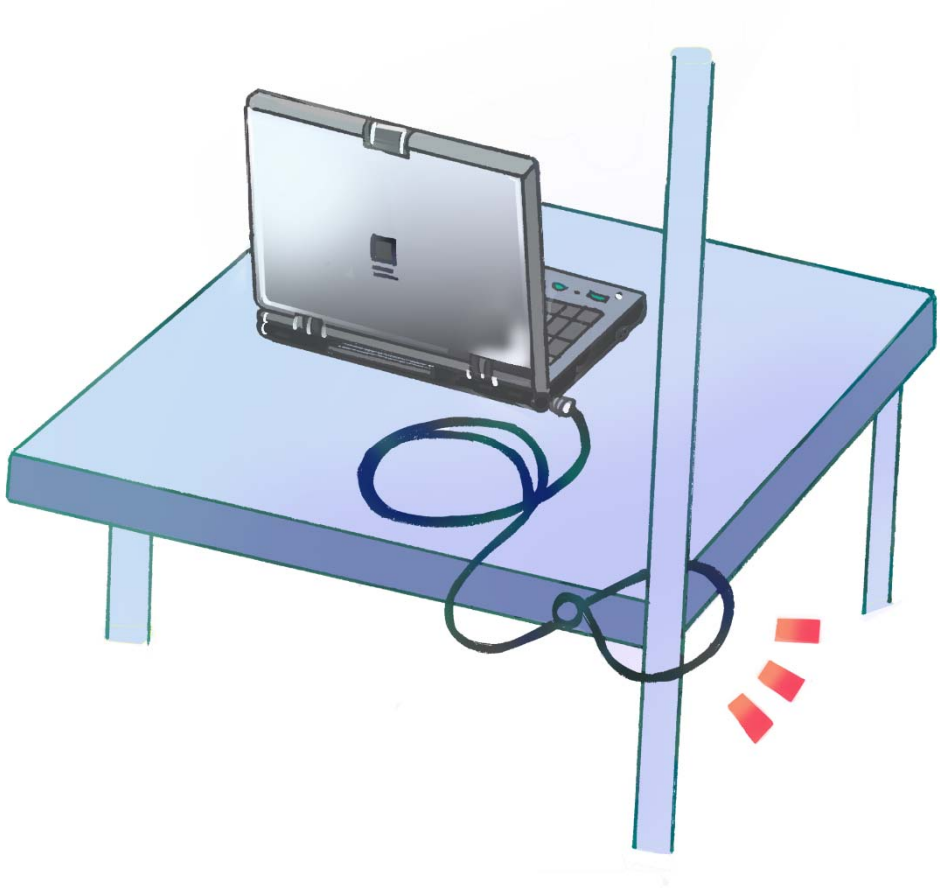
① 全員が入り口に向かって座るようなレイアウトにすることで画面が見えなくなります。
② パーテーションを設置して部屋を区切ってみるのも良いでしょう。机ごとにパーテーションを設置するのも効果的です。
③ のぞき見防止フィルターと言う商品が売られています。スマートフォンではメジャーな商品ですが、パソコンの画面用にも各種サイズで発売されています。

※のぞき見防止フィルター
価格：7,000 円～20,000 円（画面の大きさや、ブルーライト除去等の付属機能による）

## (2)ノートパソコンにはワイヤーロックをつける

　持ち運びに便利なノートパソコンを事務所内で使っている所も多いと思います。
持ち運びに便利ということは、他人が持ち出してしまう危険もあるということです。
自転車にもあるようにノートパソコンにもワイヤーロックが発売されています。

価格：2,000 円～6,000 円



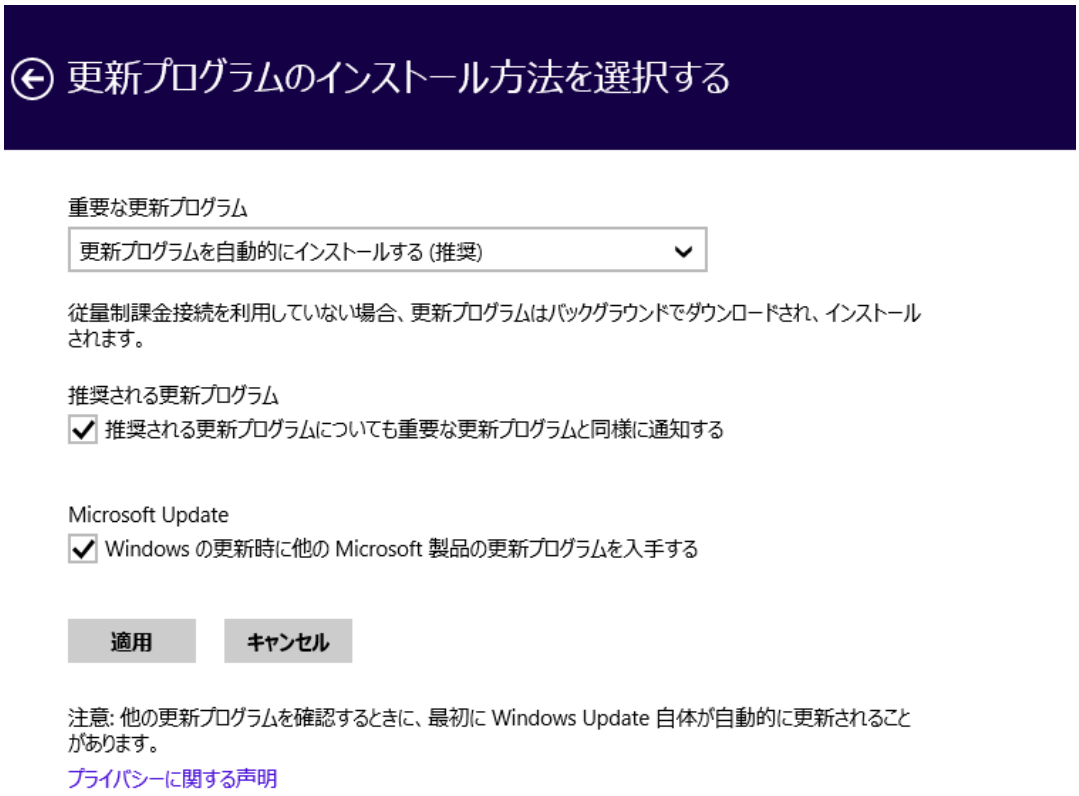
# 2. パソコンのセキュリティ対策 「技術的安全管理措置」

次にウィルス等からパソコンを守る方法をご紹介します。
(1)と(2)は必ずやるようにしましょう。

## (1)最低限やること　その 1

**【OS、Acrobat reader、Flash、Java 等の自動アップデートをオンにして、常に最新の状態にする】**

OS、アプリは常に脆弱性（脆弱性：プログラムの不具合や設計上のミスが原因となって発生したセキュリティ上の欠陥のこと）が発見され、それに対応する修正プログラムが作られています。基本的にこの修正プログラムは自動でアップデートされる設定になっていますが、まれに自動アップデートがオフになっていることがあるので、気を付けましょう。




（更新プログラムのインストール方法を選択する画面）

なお、Microsoft のサポートが終了した WindowsXP 以前の OS や、サポートが終了した Office2003(Word2003・Excel2003・PowerPoint2003)以前の Office は使わないようにしましょう。

## (2)最低限やること　その 2

### 【ウィルス対策ソフトを入れる】

ウィルス対策ソフトは必ず入れましょう。

① 機能

・受信する電子メールや CD-R、USB メモリなど外部からコンピュータが受け取るデータにウィルスが含まれていないかチェックし、ウィルスに感染することを防ぎます。

・送信する電子メールなど、コンピュータの外部に出ていくデータにウィルスが含まれていないかをチェックします。
・コンピュータがウィルスに感染している場合には、ウィルスを隔離したり、場合によっては駆除します。

② 種類
多数のウィルス対策ソフトが販売されていますが、メジャーで売れ筋のソフトを入れた方が良いでしょう。有名なソフトをいくつか挙げると次のようになります。

トレンドマイクロ社　ウィルスバスター
シマンテック社　ノートンセキュリティ
Microsoft 社ディフェンダー
McAfee 社　マカフィー

価格：年間 7,000 円前後
パソコンショップの他、ネットで直接購入・ダウンロードできます。

③ 各会計ベンダーお勧めのソフト
メジャーなソフトであっても、会計ベンダーによって相性が悪いソフトがあり、ブロックがかかって使えないことがあります。
各ベンダーにお勧めのソフトを聞いてから導入すると良いでしょう。

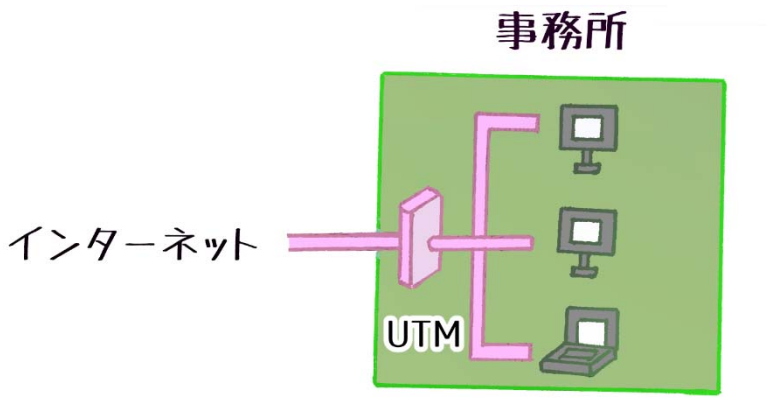
④ 注意点
・ウィルス対策ソフトは、パソコンに侵入したウィルスを駆除することはできますが、侵入自体を防ぐことができません。侵入を防ぐには次の UTM が有効です。

## (3)より完璧を目指したい場合

### 【UTM(統合脅威管理アプライアンス)を設置する】

ウィルス対策ソフトはウィルスのパソコンへの侵入自体を防ぐことができません。インターネットの入り口でウィルスの侵入を防ぐのが UTM（統合脅威管理アプライアンス）です。
複数の異なるセキュリティ機能を一つの機器に統合し、集中的にネットワーク管理（統合脅威管理）ができるようになります。
ウィルス対策ソフトではカバーできない脅威に対応できるほか、複数のパソコンがあり社内ネットワークを構築している事務所は UTM 導入のメリットがあります。

現状、ウィルス対策ソフトと UTM を導入すれば、完璧に近いセキュリティ対策が実現できます。




① UTM でできること

・業務外のホームページ閲覧防止、不正に改ざんされたサイトへの誘導の防止（ウェブフィルタリング）
・ホームページからダウンロードするファイルにスパイウェアなどのウィルスが混入していないかチェック（WEB アンチウィルス）
・スパムメール（迷惑メール）の受信を防止（アンチスパム）
・ウィルスに感染した USB からパソコンを守る
・悪意のあるソフトウェア（ワーム・トロイの木馬）からの防御
・コンピュータやネットワークと外部ネットワークの境界に設置し内外の通信を中継・監視（ファイアウォール）

② UTM のメーカーと価格

・DELL 社　SonicWALL
・フォーティーネット社　FortiGate
・サクサ㈱　SS3000
・NTT　BizBox

事務所の規模によって価格が異なる

中小規模 10 台前後の場合
UTM 本体＋5 年の保守料で、35 万円～65 万円

ベンダーで設置した場合はベンダーが保守を行う。

（例）

ミロクは　FortiGate　30D　 5 年保守料込で総額 300,000 円程度

ICS は　DELL 社製　FWⅧ（Dell　SonicWAAL　TZ105W）　5 年保守料込で総額 400,000 円程度

③ UTM のメリット・デメリット

＜メリット＞

・複数のパソコンを一括管理してウィルス等の対策ができる

・UTM のサポートセンターが常時監視してくれる。

・UTM の保守サポートに入っておけば UTM のアップデートは自動のため自分でのメンテナンスは不要

・顧問先に事務所の情報システムセキュリティの万全さをアピールでき信頼性の向上を図れる

＜デメリット＞

・セキュリティの強度の設定次第で、容量の大きいメールがはじかれてしまう事がある。
強度を落とすと逆に何でも受信してしまうことがある。

・UTM では端末のウィルス駆除ができない。
そのため UTM を導入してもウィルス対策ソフトは必要

## ※悪質な営業電話にご注意を！

マイナンバー施行による事務所のセキュリティ対策ということで、オーバースペックな高額 UTM を売りつける悪徳業者が出現しています！
数名～10 人程度の組織が多い税理士事務所は上記のように 35 万～65 万円程度で設置可能です。

＜参考文献＞

総務省　国民のための情報セキュリティサイト

税理士業務のためのＩＴリスク管理術

平成２９年３月発行

作　　東海税理士会　情報システム委員会
イラスト　水島みき
発行　　東海税理士会
〒450-0003
名古屋市中村区名駅南 2-14-19
住友生命名古屋ビル 22 階
ＴＥＬ　052-581-7508・ＦＡＸ　052-561-2866
http://www.tokaizei.or.jp