セキュリティを再チェック

ウイルス対策ソフトだけで安心していませんか？

セキュリティと聞くと「ウイルス対策ソフトを使用しているから関係ないや」と言う方はいませんか？でも、本当にウイルス対策ソフトだけで安心できるのでしょうか？ウイルス対策ソフトをインストールしていてもウイルスに感染する事もありますし、ハッカーに攻撃を受ける事もあります。それにウイルス対策だけがセキュリティではありません。自社のセキュリティ対策を見つめ直し、春に新入社員を迎え入れるましょう。

せっかくのウイルス対策ソフトが・・・

ウイルス対策ソフトを導入していても、各機能を理解して、上手に設定していなければ本当のウイルス対策にはなりません。また、**ウイルス対策ソフトを導入していれば100％安心できるという考えは捨て**ておかなければいけません。
ウイルス対策ソフトの多くは、通常の「**ウイルス検索**」と「**リアルタイム検索**」の2つの検索機能を持っています。この2つは大きく役割が違います。リアルタイム検索はパソコンへのウイルスの侵入を常に監視して処理をします。ただ、初期設定では全てのファイルを監視しているわけではないようです。リアルタイム検索をすり抜けてウイルスが侵入してくる可能性も否定できないのです。**リアルタイム検索機能があるから通常のウイルス検索を実行しないのは間違った使い方なのです。**
リアルタイム検索機能をONにしておき、お昼休みや外出中など長時間パソコンを使用しないときに「ウイルス検索」を実行するようにして、ウイルス対策ソフトをフルに利用しましょう。

ウイルス対策ソフトをすり抜けるウイルス

バックナンバー（2005年9月）でもご紹介していますが、リアルタイム検索をすり抜けるものに**スパイウェア**が上げられます。最近のウイルス対策ソフトは**スパイウェア検索機能**もあり、ウイルス検索をすると、いくつかの**Cookie**（クッキー）をスパイウェアとして見つける事があります。Cookieはホームページを見るだけでパソコンの中に作成されるファイルで、ホームページの表示を助ける役目もしますが、悪用されればあなたのパソコンの中の情報が流出する恐れもあります。スパイウェアの駆除のためにも**「リアルタイム検索」と定期的な「ウイルス検索」の実行**が重要なのです。

これだけやれば大丈夫？

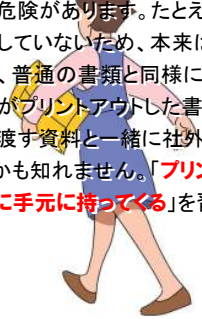
セキュリティ対策は、**複数の対策を組み合わせる**事が大事です。ウイルス対策ソフト、ブロードバンドルータ、パーソナルファイアウォールソフトなどを導入して、外部からの不正侵入に備えましょう。
また、**WindowsUpdate**や**OfficeUpdate**の実施で、**ソフトウェアの脆弱性を解消**する事も大切です。
ウイルス対策、不正侵入の対策に、
「これだけやれば大丈夫！」という事はないのです。
インターネットを利用している以上「ウイルスの脅威」「不正侵入の標的」は平等なのです。『自分（自社）だけは大丈夫！』ではないのです。

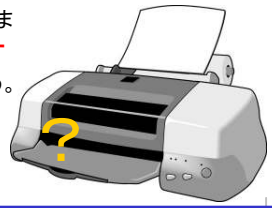
ウイルス対策だけがセキュリティじゃありません！

情報の流出はウイルスだけが原因ではありません。社内だからといって重要な書類を机の上に広げたままにしていませんか。いろんな事を想定して、社内のルールを作成しましょう。思わぬ「穴」が見つかるかも知れません。

プリントアウトした書類を、いつまでもプリンタに放置していませんか？

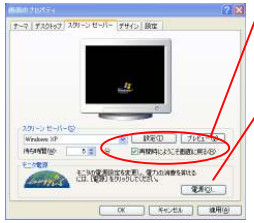
プリントアウトしたものの取り扱い（重要度）は出力した本人ならわかっていますが、そうでない人の手に渡った場合には、適切には扱われない危険があります。たとえ悪意のない人の手に渡っても、それに直接関係していないため、本来は廃棄の手順が決められた書類にもかかわらず、普通の書類と同様に処分してしまうかもしれません。また、別の社員がプリントアウトした書類も一緒になっているとは気付かず、取引先に渡す資料と一緒に社外に持ち出してしまうかも知れません。「**プリントアウトしたらすぐに手元に持ってくる**」を習慣付けましょう。





スクリーンセイバーはセキュリティのツールです。

顧客情報の画面を開いたまま、昼食や休憩、外出していませんか？
これもセキュリティ意識の欠けた行動です。席を離れる時はスクリーンセイバーを使いましょう。昔はモニタの「焼付け」を防止するツールでしたが、今は立派なセキュリティツールです。**スクリーンセイバーにはパスワードを設定**して使いましょう。



「再開時にようこそ画面にもどる」にチェック

「スタンバイ」機能をお使いの場合は、「電源」ボタンをクリックして「詳細設定」タブにある、**「スタンバイから回復するときパスワードの入力を求める」**にもチェックを付けましょう。
パスワードの設定は基本中の基本です。

もちろんパソコン起動時のログインのパスワードの設定は不可欠です。

「パスワード」設定は基本中の基本

パソコン起動時に、パスワードの入力をせずにログインしている方はいませんか。「自分しか使わないから・・・」「社員共用パソコンだから・・・」と、パスワードの設定をしていないのはとても危険です。外部からの侵入者にガラス張りの状態になっています。パスワードの設定はセキュリティの基本です。すぐに設定しましょう。

こんなパスワードじゃダメ！

1. ユーザIDと同じパスワード
2. 推測されやすいもの（人名、社名、password 等）
3. 短いもの（abc、123、777 等）

強いパスワードって？

難しく考える必要はありません。上の「ダメなパスワード」でなければ良いのです。

1. 記号を入れる。
2. 自分なりのルールで加工する。

これだけでパスワードは強くなります。たとえば、pass → p!a1s2s3 のようにします。passと、記号「！」と数字の123を合成します。
daido + #777 = d#a7i7d7o など人名・社名プラス短い数字でも強いパスワードはできます。覚えるのも簡単ではないでしょうか。

パスワードの管理

企業の場合、誰かが**一括してパスワードの管理**をする事が大事です。
個人が勝手にパスワードを設定していては、その社員が出張や休暇中、パソコン内のファイルにアクセスできなくなってしまいます。
また、「パスワードの強さ」もバラバラになってしまいます。
『パスワード管理者がパスワードを発行する』『パスワードを変更する場合はパスワード管理者の認証を得る』などの社内ルールを作り、パスワードを管理してください。

継続できるセキュリティ対策は

セキュリティ対策の徹底を継続するには、「**守りやすい**」事が大切です。「守りやすい」＝「安易なもの」ではありません。社内の誰もが、「**同じ判断を出来るもの**」という事です。そのルールを文書化して徹底する事でセキュリティ対策は継続されていくはずです。

開発室から

昨年の年末に、ついにテレビが見れる「ワンセグ携帯」電話を購入しました。以前使っていた携帯電話より薄くなって、画面は大きくなって、かなり気に入っています。でも。肝心のテレビは・・・。
見る機会がありません。仕事中に見る事は出来ないし、通勤のクルマには既にテレビがついているし、家では普通のテレビを見るし・・・。
皆さんはどんな時に携帯のテレビを見ていますか？