常時SSLに始まる情報セキュリティについて

RIK NETWORKS – リックネットワークス –
http://www.riknetworks.co.jp/

初めに

みなさんに質問です。

次のページにでてくる言葉を知っていますか？

初めに

1.検索エンジン

2.SEO

3.SSL

4.コンピュータウイルス

5.情報漏えい

6.フリーメール

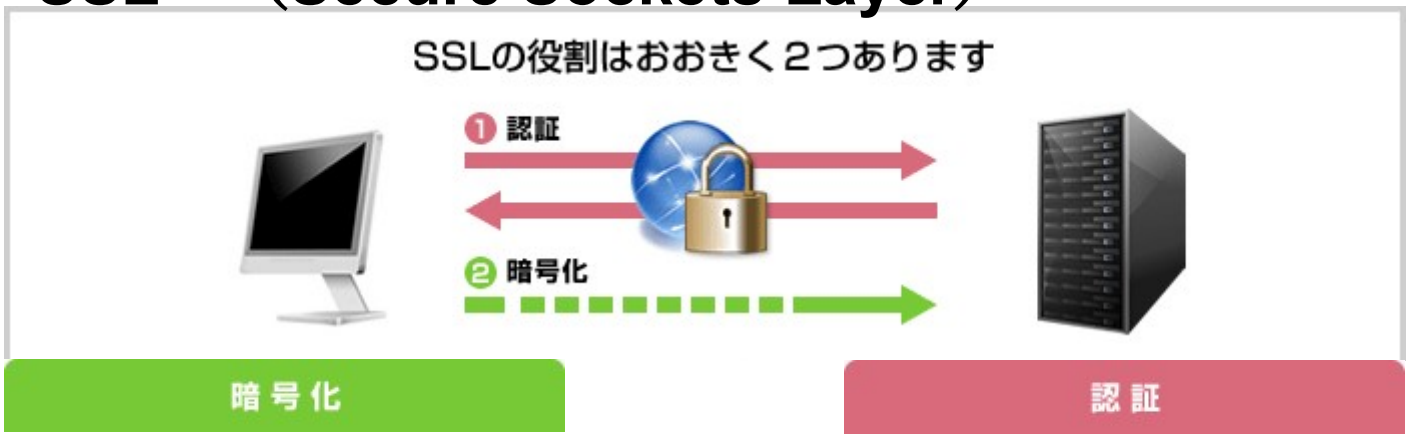
7.乗っ取り（LINE・FACEBOOK等）

今回は、この中でいくつかのセキュリティに関することをお知らせします。

ＳＳＬについて

ＳＳＬについて

SSL　（Secure Sockets Layer）



①暗号化

SSLを利用すると、通信される情報を暗号化します。

万が一情報の送受信中に情報を見られても
暗号化によって大切な情報が守られます。

②認証

SSLは様々な方法で認証されたサーバにしか発行されません。

SSLを持っているということは信頼性を証明するものです

簡単に言うとよってユーザに安心感を与えることができます。

1.やりとりされるデータの「暗号化」
2.Webサイトの「所有者の証明」

認証レベル

ドメイン認証　「DV（Domain Validation）」認証レベル１

暗号化するだけ

企業認証「OV（Organization Validation）」 認証レベル２

企業の実在性を証明

ＥＶ認証　　「EV（Extended Validation）認証レベル３

こう思っていませんか？

SSLは所詮、裏方。

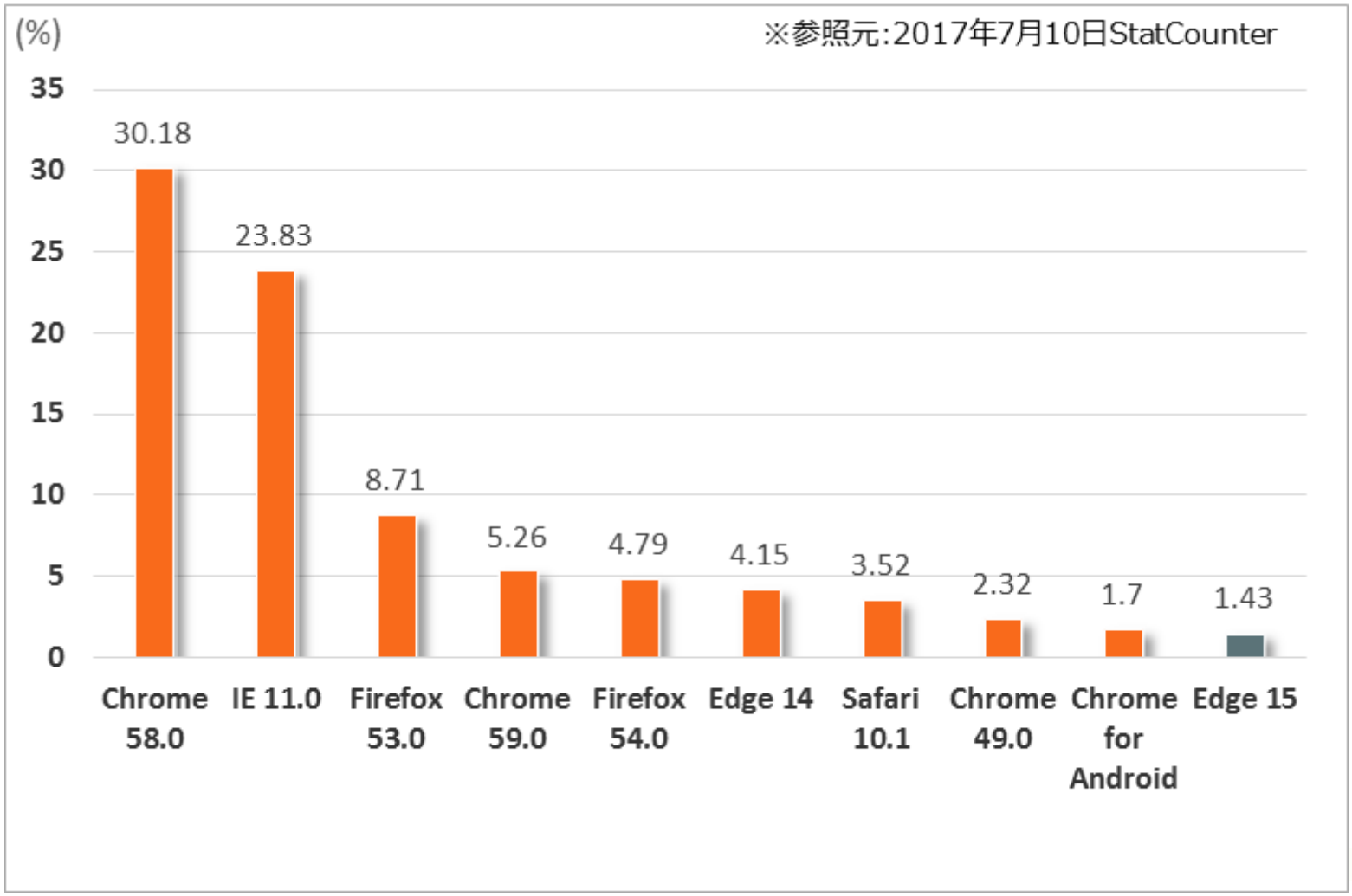
対策していなくても、他人にはわからない。

どのようにして、皆さまと関わりがあるのか？

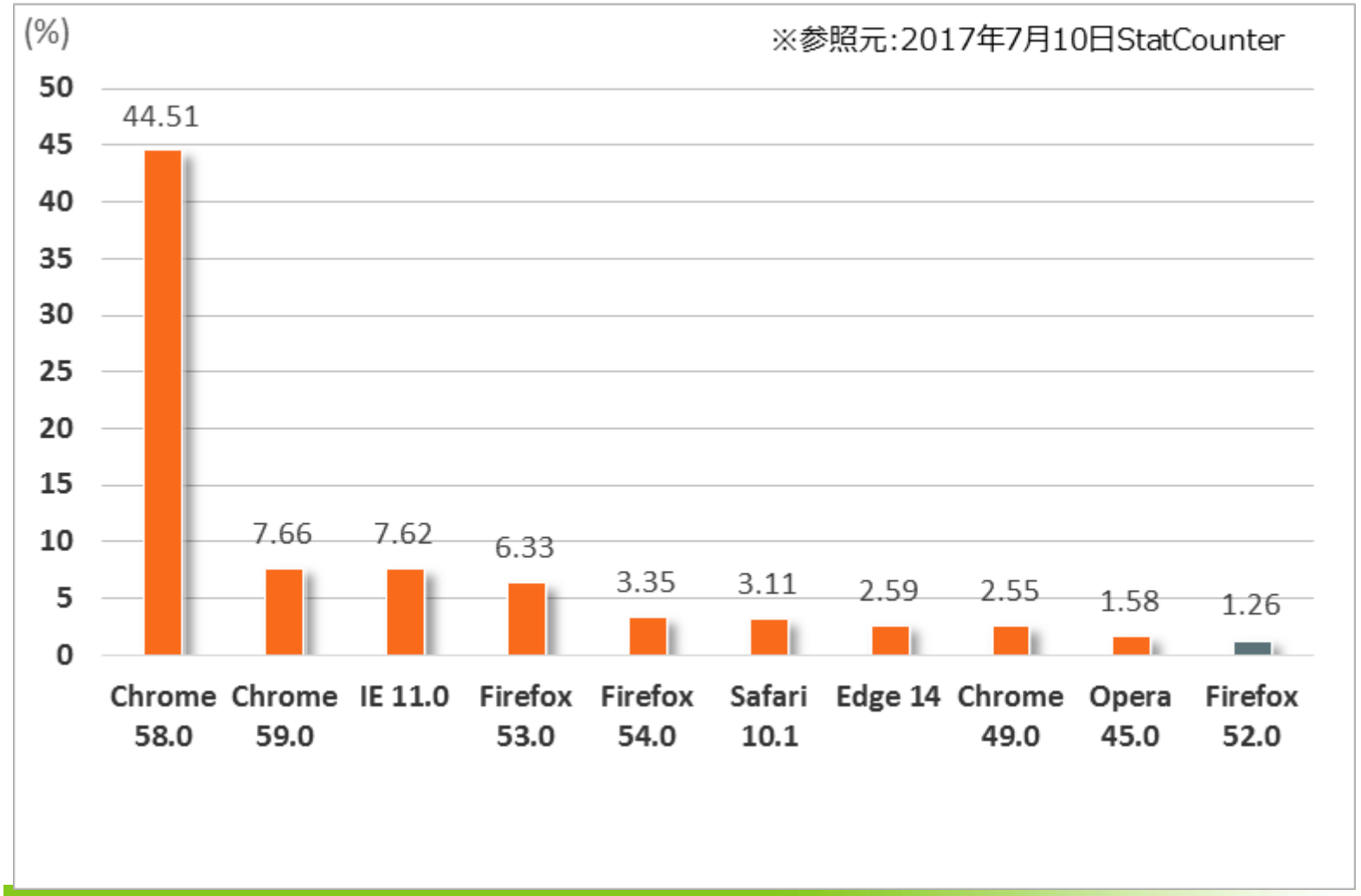
それでは
次の質問です。

自分でホームページを開いて見たことがない
方はいますか？

WEBブラウザ シェア （日本）



WEBブラウザ　シェア　（海外）



ホームページをアクセスするためのルール

http

Hypertext Transfer Protocol

https

Hypertext Transfer Protocol Secure

初めに

ホームページアドレスを入力した際にこんなマークを見たことはありませんか？

今後このマークが赤字で表示されると言われております。

常時ＳＳＬ化とは

ウェブサイトのすべてのページを暗号化することを常時SSLといいます。
常時SSLは、ウェブサイト内のログインページやフォームなど特定のページだけでなく、その他すべてのページをSSL化することで、ログイン情報や決済情報だけでなく、Cookieへの不正アクセス（盗聴）も防止することができます。

SSL化されたウェブサイトは、URLの頭が「HTTPS」となり、通信の暗号化が保証されます。これにより、ユーザは安心してウェブサイトから個人情報や決済情報を提供することができ、第三者による盗聴を心配する必要がなくなります。

さらに、企業実在認証付きの証明書やEV証明書がサイトに入っている場合には、アクセスしているウェブサイトに証明書が入っていることが確認できるため、擬似サイトやなりすましサイトへの誘導を防ぐことが出来るといったメリットがあります。

グーグル・ヤフー・ＹＯＵＴＵＢＥ等はすでに常時ＳＳＬ化をしております。

近い将来、ブラウザーのアドレスバーに赤い文字でこのサイトは危険ですと表示されたら、
ホームページを見に来られた方がサイトを見るでしょうか？

ホームページを持たれている方は常時SSL導入をお勧めします。

ID（アカウント）
乗っ取り対策について

ID（アカウント）が乗っ取られると

IDが乗っ取られるとなにが起こるのでしょうか。

1.インターネットバンキングでの不正送金
2.インターネットショッピングでの不正購入
3.SNSサイト・オンラインゲームの不正操作
4.メールの盗み見等の情報の不正入手
5.知人になりすましての情報操作や発信

上記のことが起こる可能性があります。

ID（アカウント）が乗っ取られないようにするためには

警察庁発表によると、不正ログイン行為の手口の内訳では、
アカウント利用者の
「パスワード設定・管理の甘さにつけ込んだもの」
「インターネット上に流出・公開されていたID／パスワードを入手して悪用」
「不正アクセス」によるもののようです。

悪意のあるものは、入手したIDをいろいろなサービス
（SNS・ネットバンキングメール・ショッピングサイト等）で
不正アクセスを試みますので、パスワードの使いまわしは
しないように心がけてください。

ウイルス対策と情報漏えい
セキュリティ対策について

コンピューターウイルスの感染経路

コンピューターウイルスはどのように感染するのでしょうか？

1.ホームページの閲覧

現在のWebブラウザは、ホームページ上でさまざまな処理を実現できるように、各種のプログラムを実行できるようになっています。これらのプログラムの脆弱性を悪用するウイルスが埋め込まれたホームページを閲覧すると、それだけでコンピュータがウイルスに感染してしまう危険があります。最近では、Webブラウザへ機能を追加するプラグインソフトの脆弱性（ぜいじゃくせい）を利用した感染方法が増加しています。

かつては怪しいWebサイトを訪問しなければ大丈夫と思われていましたが、最近では正規のWebサイトが不正侵入を受けて書き換えられ、ウイルスが仕込まれてしまうケースも急増しています。

この場合は、正規のWebサイトを閲覧しても、ウイルスに感染してしまうことになります。

2.信頼できないサイトで配布されたプログラムのインストール

あたかも無料のウイルス対策ソフトのように見せかけて、悪意のあるプログラムをインストールさせようとする「偽セキュリティソフト」の被害が増えています。その代表的な手口は、ホームページなどで「あなたのコンピュータはウイルスに感染しています」のようなメッセージを表示し、利用者を偽のウイルス対策ソフトを配布するWebサイトに誘導する方法です。

コンピューターウイルスの感染経路

3.電子メールの添付ファイル

電子メールの添付ファイルもウイルスの感染経路として一般的です。電子メールに添付されてきたファイルをよく確認せずに開くと、それが悪意のあるプログラムであった場合はウイルスに感染してしまいます。

かつては、電子メールで実行形式のファイル(ファイルの拡張子が.exeのファイル)が送られてきたときには特に注意するように言われていましたが、最近はファイル名を巧妙に偽装し、文書形式のファイルに見せかけて悪意のあるプログラムを実行させ、ウイルスに感染させる事例もあります。

また、文書形式のファイルであっても、文書を閲覧するソフトウェアの脆弱性を狙った攻撃も増加していることから、メールに添付されてきたファイルを安易に開くのは危険な行為です。

4.USBメモリからの感染

多くのコンピュータでは、USBメモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されています。この仕組みを悪用して、コンピュータに感染するウイルスがあります。
このようなウイルスの中には、感染したコンピュータに後から差し込まれた別のUSBメモリに感染するなどの方法で、被害を拡大させるものもあります。

コンピューターウイルスの感染経路

5.ファイル共有ソフトによる感染

ファイル共有ソフトとは、インターネットを利用して他人とファイルをやり取りするソフトウェアのことです。自分が持っているファイルの情報と、相手が持っているファイルの情報を交換し、お互いに欲しいファイルを送り合ったりすることから、ファイル交換ソフトとも呼ばれています。
ファイル共有ソフトでは、不特定多数の利用者が自由にファイルを公開することができるため、
別のファイルに偽装するなどの方法で、いつの間にかウイルスを実行させられてしまうことがあります。

6.電子メールのHTMLスクリプト

添付ファイルが付いていなくても、HTML形式で書かれているメールの場合、ウイルスに感染することがあります。HTMLメールはホームページと同様に、メッセージの中にスクリプトと呼ばれるプログラムを挿入することが可能なため、スクリプトの形でウイルスを侵入させておくことができるのです。電子メールソフトによっては、HTMLメールのスクリプトを自動的に実行する設定になっているものがあり、その場合には電子メールをプレビューしただけでウイルスに感染してしまいます。

コンピューターウイルスの感染経路

7.ネットワークのファイル共有

ウイルスによっては、感染したコンピュータに接続されているファイル共有ディスクを見つけ出し、
特定のファイル形式など、ある条件で探し出したファイルに感染していくタイプのものがあります。
このようなウイルスは組織内のネットワークを通じて、他のコンピュータやサーバにも侵入して感染を
拡げる可能性があります。
とても危険度が高く、完全に駆除することが難しいのが特徴です。

8.マクロプログラムの実行

マイクロソフト社のOfficeアプリケーション（Word、Excel、PowerPoint、Accessなど）には、
特定の操作手順をプログラムとして登録できるマクロという機能があります。このマクロ機能を利用して感染す
るタイプのウイルスが知られており、マクロウイルスと呼ばれています。Officeアプリケーションでは、
マクロを作成する際に、高度なプログラム開発言語であるVBA（Visual Basic for Applications）を使用
できるため、ファイルの書き換えや削除など、コンピュータを自在に操ることが可能です。そのため、
マクロウイルスに感染した文書ファイルを開いただけで、VBAで記述されたウイルスが実行されて、
自己増殖などの活動が開始されることになります。

（出典：総務省）

コンピューターウイルスに感染すると

コンピュータウイルスに感染するとどうなるか。

コンピュータウイルスに感染すると、ウイルスに感染したと気が付きやすいものと気が付かないものがあります。

※ 気が付きやすいもの

1.パソコンや各種ソフトウェアが突然動かなくなる
2.画面上に意味不明なメッセージやアダルト広告のメッセージが表示される
3.画面上の表示が崩れる
4.ファイルが勝手に削除される
5.インターネットで最初に表示されるページが変わってしまう
6.特定のサイトがアクセスできなくなる

※ 気が付きにくいもの

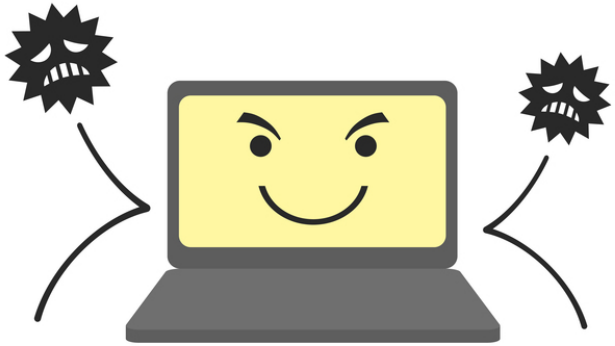
1.勝手にウイルス付きのメールを大量に配信されてしまう
2.パソコン内の写真などのデータを勝手に配布されてしまう
3.パソコン内のクレジットカード情報などの個人情報を盗まれてしまう
4.勝手にパソコンを操作される。

こうならないためにウイルス対策は重要です。

※ ＳＳＬとウイルス対策の違い

ＳＳＬは通信の暗号化 WEBサイトの所有者の証明。

ウイルス対策は個々のＰＣに対しての対策。



情報漏えい

社員が出先でパソコンをなくした。
ＩＤ・ＰＷが盗まれた等

コンピュータウイルス被害

コンピュータウィルスにかかってしまいウィルスをばらまかれた等

不正アクセス

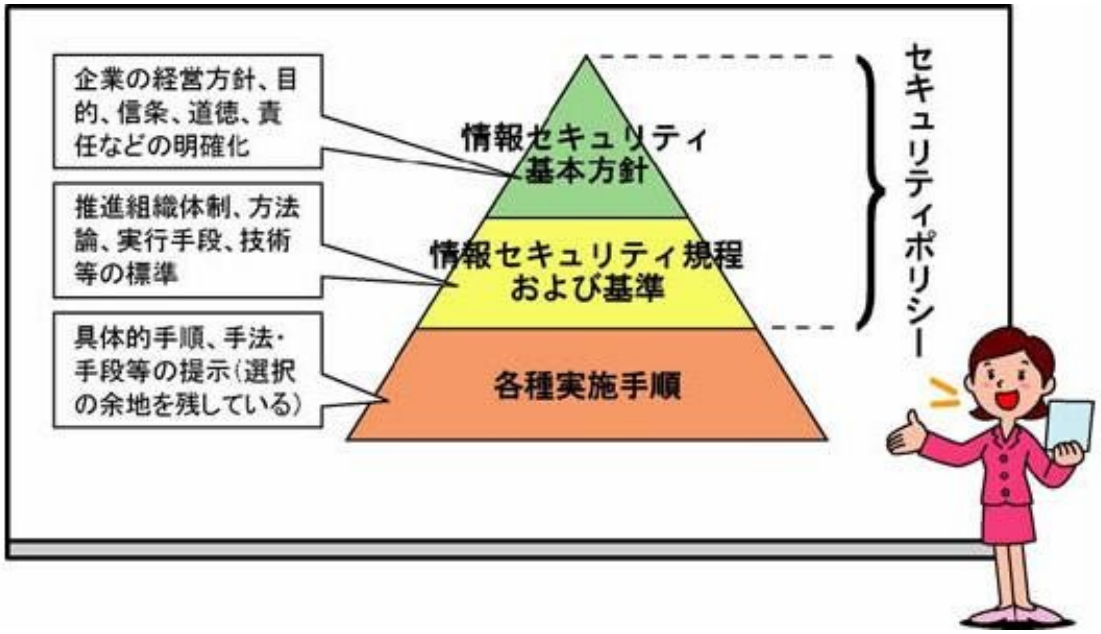
社内のパソコンに侵入された。
退社した社員に不正にログインされた

解決するには
セキュリティーポリシーの策定が重要

セキュリティポリシーとは

セキュリティーポリシーとは、企業の「情報資産」を守るための対策を具体的にまとめた社内ルールのことです。

経営者の声明文であり、企業として情報セキュリティにどのように取り組むかを表明する文書です。
企業の経営方針、目的、責任などを明確にします。



セキュリティ対策の基本的なこと

1.ID・PWの紛失に注意する。

2.パスワードは定期的に変える。

8文字以上、記号と大文字・小文字・数字をまぜる。
例・・1TotVE&yS

3.ウィルス対策ソフトの導入を行う。

パソコン内のウイルスなど、悪意のあるプログラムを
検出・削除を行う役割。

4.ファイアウォールの導入を行う。

外部のネットワークから不正にアクセスしようとするものや、
不正にパソコンから出ていくデータを遮断する役割。

安全に利用するために

**経営者が、インターネットの使用のリスクを
理解し、信用を失墜しないために、
どうしたらよいかを考えて社内で共有し実行すること
が重要である。**

**自分で判断せずわからない場合は信頼のおける
専門家に相談してください。**

ご清聴ありがとうございました。