

情報漏えい対策のしおり

企業（組織）で働くあなたへ
7つのポイント !!



IPA

独立行政法人 情報処理推進機構
セキュリティセンター

<http://www.ipa.go.jp/security/>

本対策のしおりは、企業(組織)で働くあなたに、情報漏えい対策の7つのポイントを示すものです。

本来、企業(組織)として情報漏えい対策を行う場合は、それぞれの企業(組織)において、情報漏えい対策のセキュリティポリシーを策定し、それを守る必要があります。

あなたが、本対策のしおりで示す内容を守ってさえいれば、企業(組織)の大切な情報(データ)を漏えいさせないわけではありません。

本対策のしおりに示す7つのポイントは、あなたが企業(組織)で業務を遂行する上での、あなた自身が情報漏えいを起こさないために、あなたの心構えとしてお読み下さい。

企業(組織)で働くあなたへ…7つのポイント

(1) 企業(組織)の情報資産^(*1)を、許可なく、持ち出さない

持ち出し禁止

(2) 企業(組織)の情報資産を、未対策^(*2)のまま目の届かない所に放置しない

安易な放置禁止

(3) 企業(組織)の情報資産を、未対策のまま廃棄しない

安易な廃棄禁止

(4) 私物(私用)の機器類(パソコンや電子媒体)やプログラム等のデータを、許可なく、企業(組織)に持ち込まない

不要な持ち込み禁止

(5) 個人に割り当てられた権限^(*3)を、許可なく、他の人に貸与または譲渡しない

鍵を掛け、貸し借り禁止

(6) 業務上知り得た情報を、許可なく、公言しない

公言禁止

(7) 情報漏えいを起こしたら、自分で判断せずに、まず報告

まず報告

1.企業(組織)の情報資産を、許可なく、持ち出さない

自宅などで業務を実施するために、勝手に企業(組織)のパソコンや、業務情報が格納された電子媒体あるいは書類を持ち帰ることは、ご法度(禁止されていること)ですよ…と仰うことです。

JNSA(NPO 日本ネットワークセキュリティ協会)の調査によると、情報漏えいの原因は、紛失・置忘れ(29.2%)、盗難(19.0%)であり、これだけで全体の約半数を占めています。情報資産を持ち出すと、このような事故につながりかねず、危険性が高いことは無視できません。

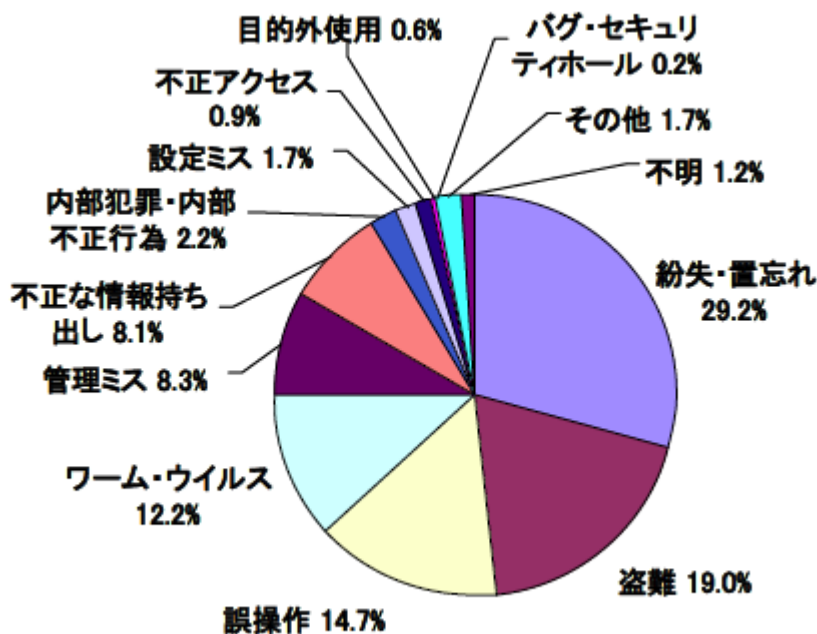


図1 個人情報漏えい原因の件数割合
(以下の URL に示す JNSA 調査資料から引用)

<http://www.jnsa.org/result/2006/pol/insident/070720/>

さらに、P2P ファイル交換ソフトの利用による情報漏えい事故が多発していることを考えても、企業(組織)管理者の目の行き届かないところで、情報資産を利用することは、ハイリスクであると言えます。

持ち出し許可があつたとしても、あなたが管理を怠らないことが前提です。あなたの不注意が原因で、盗難や紛失・置忘れが起こる可能性があるならば、余程の事情がない限り、情報資産の持ち出しは避けるべきです。

『大切な情報は持ち出さない』、『仕事を家に持って帰らない』と仰うことを原則とすべきでしょう。



持ち出しの許可を得た場合

許可を得て持ち出した情報資産で、やってはいけない例・・・

- ・ 大切な情報を、管理下でないパソコン(例えばネットカフェのパソコン)で利用する
- ・ 業務で持ち出したパソコンを、不必要に、企業(組織)外のネットワークに接続する
- ・ 業務で持ち出したパソコンを、業務以外の目的で利用したり、他人に貸したりする

安全が確認できない環境での情報資産の利用も注意が必要と言うことです。

企業(組織)の情報資産のうち、企業(組織)内で使用しているパソコンを、業務上、許可を得てから持ち出した場合は、そのパソコンの設定や使用方法にも注意する必要があります。

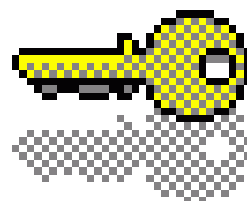
持ち出したパソコンを社外のネットワーク(インターネット)環境で使用し、ウイルスに感染。そのパソコンを企業(組織)内のネットワーク環境に接続して、ウイルスを企業(組織)内に広めてしまったというのも、よくある話です。この問題は、セキュリティ対策が不十分であった場合が原因ですが、一般的に企業(組織)内の保護された環境と、企業(組織)外の管理されてない環境の違いを理解せず、対策が不十分になることが多いようです。感染したウイルスがスパイウェアであった場合は、情報漏えいの原因となります。持ち出すパソコンには、十分なセキュリティ対策を実施すべきです。

企業(組織)の情報資産のうち、いわゆる業務情報(データ)を、業務上、許可を得てから持ち出す場合は、これらのデータを暗号化することをお勧めします。

データを暗号化することにより、万一、それらのデータを格納した電子媒体(パソコン本体あるいは FD/CD/DVD/HD/USB メモリ等)を盗まれたり、紛失したりしても、大切なデータを、ある程度、情報漏えい事故から保護することができます。

同じ理由で、業務情報(データ)を、許可を得てメール送信する場合でも、メールそのものを暗号化するか、添付するデータを暗号化することをお勧めします。万一、メールの送信先を間違えたり、メールを盗聴されたりしても、暗号化していれば、大切なデータを、ある程度、情報漏えい事故から保護することができます。

データの暗号化を行う方法としては、一般的には、暗号化のためのアプリケーションを使用する方法があります。この場合は、暗号文を復号するためにパスワードが必要で、場合によってはデータの受け取りをする人に、同一のアプリケーションが必要な場



合もありますので、ご注意ください。

Microsoft の Word や Excel のように、文書やシート/ブックの保護(読み取りパスワードによる保護)を行えるものもあります(『9.参考情報』を参照下さい)。

しかしながら、持ち出すデータを暗号化しているから、これで情報漏えいは起こさないと考えるのは、不十分です。暗号化は、データを保護することが目的であり、情報漏えいそのものを防止するものではありません。

企業(組織)の情報資産を持ち出す場合は、次に述べる『企業(組織)の情報資産を、未対策のまま目の届かない所に放置しない』ことが重要となります。

2.企業(組織)の情報資産を、未対策のまま目の届かない所に放置しない

具体的な、やってはいけない例から考えてみましょう。

- ・ 業務上大切な書類を机の上に放置したまま席を離れる、あるいは帰宅する
- ・ 離れた場所にあるプリンタに出力した書類を、すぐに取りに行かない
- ・ 起動中のパソコンを他の人が利用できる状態で席を離れる(パスワードロックしない)
- ・ モバイル可能なパソコンを机の上に放置して帰宅する
- ・ 大切な情報が格納された電子媒体や書類を、鍵のかかるキャビネットなどにしまわない
- ・ 個人宛の伝言メモを誰でも見えるところにおく

こんなこと、言われなくても…と思われるでしょうが、大事なことです。

例えば、「保存期限の過ぎた重要書類を、破棄する目的で集積したけれども、廃棄業者が来るまで置き場所がないので、誰でも通ることのできる廊下に積み上げていた」なんてよくある話です。

自分では、気を付けていると言っても、みんなで気を付けていないと…やはり情報漏えいが起こることがあります。

業務上大切な書類や電子媒体、モバイル可能なパソコン…使わない時は、きちんと鍵のかかるキャビネットなどに格納するようにして下さい。

業務途中で席を離れる場合、起動中のパソコンには、パスワードロックのできるスクリーンセーバーが動作するように設定するとか、コンピュータロック(『9.参考情報』を参照下さい)を掛けましょう。

些細なことですが…伝言メモは、伏せて置くのがマナーです。

不特定多数の人たちの目に触れる場所には、各種の情報資産を晒さないように心掛けましょう。



許可を得て、企業(組織)の情報資産を、持ち出す場合も…

- ・ 大切な情報が詰まったカバンを電車の網棚において居眠りをした
- ・ 大切な情報が詰まったカバンを持って、居酒屋やパチンコ店に立ち寄った

なんて言うのも、かなり危ない状況です。



3.企業(組織)の情報資産を、未対策のまま廃棄しない

企業(組織)内で業務に使用していたパソコンを、ハードディスクをきちんと消去しないまま廃棄し、そこから情報漏えいすることは、よく聞かれる話です。

同様に、業務情報を格納した電子媒体や書類を、安易にゴミ箱に捨てたために、情報漏えいしたと言うのも、よく聞かれる話です。

最近では、パソコンのハードディスクの内容を完全に消去するサービスを行う企業もありますが、このようなサービスを受けるか、企業(組織)内で廃棄のための手順や技術を確立し、それに従う必要があります。もし、あなたが働く企業(組織)に、このようなルールがないならば、あなたから提案してみてもいいかもしれません。

重要な書類や電子媒体を、一般ごみと一緒にゴミ箱にポイ捨てるなど言語道断と言うことです。



重要な書類であれば、管理者の管理下あるいは専門の業者で、細かく裁断するとか溶解処分することをお勧めします。

FD や CD/DVD の電子媒体の場合も、再利用が出来ないのであれば、裁断(破碎)してから処分することをお勧めします。

4. 私物(私用)の機器(パソコンや電子媒体)やプログラム等のデータを、許可なく、企業(組織)に持ち込まない

これも具体的な、やってはいけない例から考えてみましょう。

- ・ 私物(私有)のパソコンを持ち込んで、企業(組織)のネットワークに接続した
- ・ 業務に必要なのない情報(データ)を、業務中に利用した
- ・ 業務に必要なのない私物(私有)のプログラムを、業務中に利用した
- ・ 業務に関係のないフリーウェアあるいはシェアウェアであるプログラムをインターネットからダウンロードした
- ・ 業務に関係のない Web サイトを業務用のパソコンで閲覧した
- ・ 業務で使用する電子メール(アドレス)を、私用で利用した
- ・ 情報を格納することのできる USB メモリなどの外部記憶装置を持ち込んで、業務用のパソコンに接続した

■私物の情報機器を持ち込むことの危険性

持ち込んだ私物(私有)のパソコンやUSBメモリなどの外部記憶装置がウイルスに感染していた場合は、企業(組織)内の他のパソコンやサーバに、ウイルス感染を広げる可能性があります。そのウイルスがスパイウェアであった場合は、大切な業務情報がインターネットを通じて流出する可能性が考えられます。

■許可されていないプログラムの危険性

Web サイトからダウンロードしたり、外から持ち込んだりしたプログラムそのものが、スパイウェアである可能性もあります。業務に関係のないプログラムの利用は慎むべきです。

どうしても、業務に必要なプログラムであるならば、事前に安全な環境で動作確認を行って、管理者の許可・管理のもとで利用することをお勧めします。

■Web サイトの危険性

悪意のある Web サイトの場合、サイト上に指定された操作をするだけで、悪意のあるプログラムを実行させるものも多く報告されています。

ウイルスやスパイウェア対策が十分に施された環境であったとしても、対策ソフトが検知できないウイルスやスパイウェアも存在するので、注意が必要です。

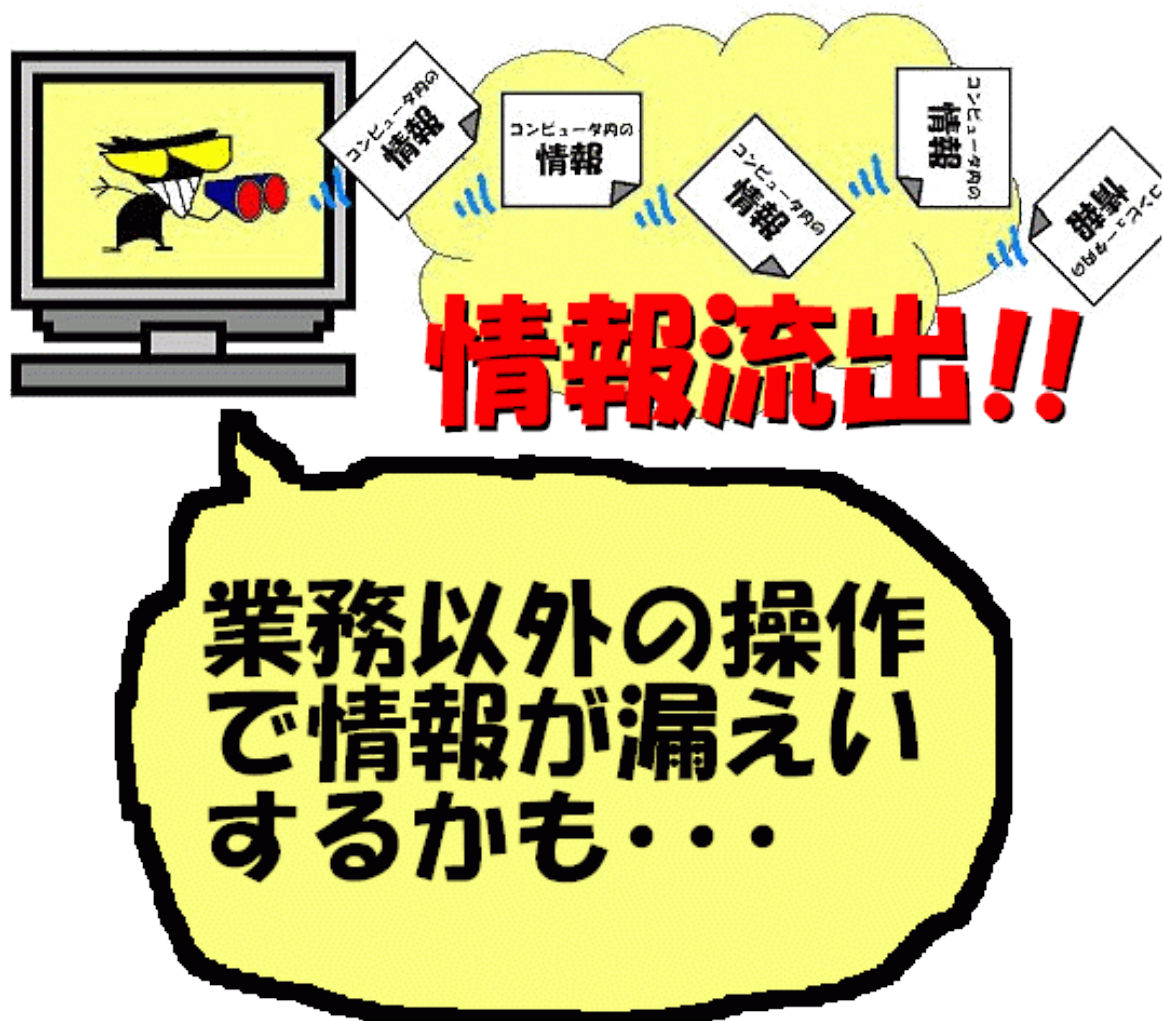
特に、不特定多数を狙わず、特定企業(組織)や個人を狙うスパイウェアも出現していますので、業務に関係のないプログラムの利用は避けるべきです。

■誤った操作で情報漏えいする危険性

持ち込んだ私物(私有)のパソコンやUSBメモリなどの外部記憶装置を利用する際に、不用意に大切な業務情報が格納されてしまい、意図せずに情報を持ち出してしまう可能性があります。このような場合は、情報漏えい事故が発生した際の、情報の流失経路の特定が困難になります。

また、電子メールを私用で使った際に、誤って大切な業務情報を流出させる可能性や、ブログや掲示板への不用意な書き込みから、無意識のうちに、大切な業務情報を流出させる可能性もあります。

このような行為は慎むべきです。



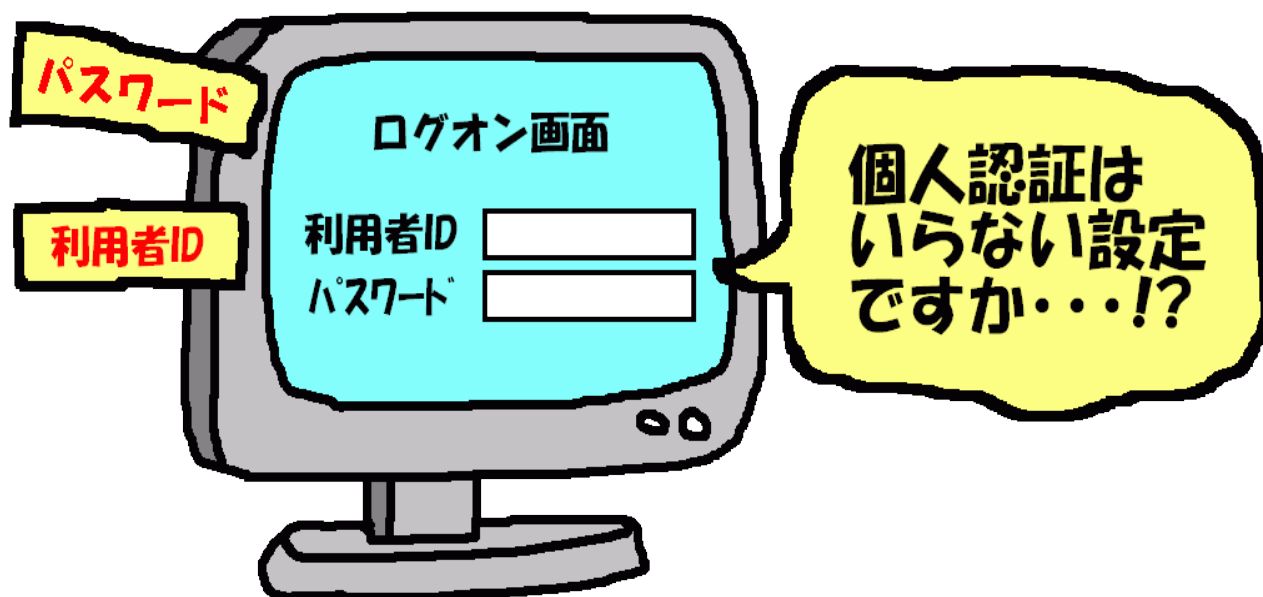
5.個人に割り当てられた権限を、許可なく、他の人に貸与または譲渡しない

企業(組織)では、業務や体制に応じて担当者に権限が与えられます。いわゆる職権などがこれにあたりますが、この職権を他の人に貸与または譲渡することは、通常ありえません。

これと同様に、企業(組織)では、業務で使用する情報や機器にも、利用者権限が担当者ごとに与えられています。つまり、利用者 ID ごとに利用権限が定義されていて、利用者 ID はパスワードまたは個人認証で保護されます。

これらの利用者 ID やパスワードを共有したり、貸し借りしたりすることは、情報セキュリティ上、非常に大きな問題を引き起こす可能性があります。

業務の担当者を識別するために利用者 ID とパスワードが設定されているのに、このパスワードを安易に貸し借りする行為は、愚かと言わざるをえません。同じ理由で、貸し借りしなくとも、パスワードなどを忘れないように、パソコンに貼り付けておくことも、セキュリティ上愚かな行為です。



権限には必ず責任が付いてきます。責任を果たすために、不注意とも思われる行為は慎みましょう。

他の人に与えられた、利用者 ID およびパスワードを使用する行為は、なりすましと呼ばれ、不正アクセス禁止法(不正アクセス行為の禁止等に関する法律)^(*)に抵触します。

6.業務上知り得た情報を、許可なく、公言しない

業務上の情報を、意図的に、知らない人にベラベラしゃべる人はいないと思われませんが・・・気の合う仲間と雑談している時に、何気に口にした情報を、誰かが聞いているかも知れません。

ショルダーハッキングと呼ばれる行為は、いわゆる肩越しに盗み見る行為のことを言います。盗み聞きや盗み見など、「壁に耳あり、障子に目あり」を忘れずに、ということなのです。

これも具体的な、やってはいけない例から考えてみましょう。

- ・ 居酒屋で・・・上司の悪口や仕事の話大声でしゃべる
- ・ 電車の中、携帯電話で仕事の話をする(マナー違反でもありますが)
- ・ 出張で、新幹線の中、パソコンで仕事をする(持ち出し OK?)
- ・ 会社の帰り道、電車の中で資料のレビューをする(持ち出し OK?)
- ・ 不特定多数の人が集まる集合ビルの喫煙所で仕事をする
- ・ 業務に関係のないブログや掲示板に、自己紹介のつもりで、仕事の話アップした

数え上げるとキリがないようですが、これらの行為もセキュリティ上危険度の高いものであると言えます。悪意のある人はどこにいるかわかりません。偶然聞いた情報や盗み見た情報から、大きな情報漏えいへと発展する可能性もあります。自分が情報漏えい源にならないよう、このような行為は慎まなければなりません。

さらに、

- ・ 企業(組織)外からの電話・・・友人と称して、休みの人の連絡先や、その人の仕事の内容を聞かれた
- ・ システム管理者を名乗る人からの電話・・・利用者ID やパスワードを聞かれた
- ・ 会員登録と称して、仕事の内容を事細かに入力させる登録画面

のような、ソーシャルエンジニアリング^(*5)手法を用いたアプローチがあるかも知れません。

『不注意でした』では済まされない情報漏えい、日ごろの心掛けが大切ということになります。

システム管理者です…
問題が発生したので…
利用者の再登録が必要で
す…こちらで対応しま
すので…
利用者IDとパスワードを
教えてください…



7.情報漏えいを起こしたら、自分で判断せずに、まず報告

何らかの誤りで情報漏えいを起こしたり、あるいは情報漏えいを発見したりした場合は、自分で何とかしようとする前に、上司や管理者に報告して下さい。

自分の会社(組織)のことだけでなく、個人情報を漏えいされた最終的な被害者、顧客、取引先、株主、親会社、子会社、従業員など情報漏えいによって被害を受ける様々な関係者の被害を最小限に抑える必要があります。

自社の経営方針に基づき全体のバランスを考えながら被害の最小化を図ることが重要です。

■ 情報漏えい発生時の対応ポイント集

<http://www.ipa.go.jp/security/awareness/johorouei/>

すばやい対応によって、問題を最小限に止められる可能性が高まります。

8.用語の説明

(*1)情報資産

情報資産とは、業務情報(プログラムも含む)および業務情報を格納する機器類(パソコン、電子媒体、紙等)のことです。

(*2)未対策

未対策とは、セキュリティ上の対策が施されていない状態のことです。

(*3)権限

権限とは、資産を扱うために与えられたものです。セキュリティの基本事項として**最小権限**というものがあり、権限は可能な限り狭い範囲で与えることが重要です。

(*4)不正アクセス禁止法(不正アクセス行為の禁止等に関する法律)

「不正アクセス行為の禁止等に関する法律(いわゆる不正アクセス禁止法)」は、1999年8月6日に参院本会議で可決、成立しました。一部を除き、2000年2月13日から施行されました。また、2000年7月1日からは、残りの項目である援助規程(第6条)も施行されました。実際の条文に関しては、以下をご参照下さい。

<http://www.ipa.go.jp/security/ciadr/law199908.html>

また、警察庁の解説が下記にあります。

<http://www.npa.go.jp/cyber/legislation/gaiyou/gaiyou.htm>

<http://www.npa.go.jp/cyber/legislation/gaiyou/main.htm>

国家公安委員会による「不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規則」は、下記にあります。

http://www.npa.go.jp/cyber/legislation/kitei/enjyo_kitei.htm

その他に、不正アクセス行為によりコンピュータに障害が発生した場合や、データの破壊が行われたような場合には、威力業務妨害等の罪に該当する場合があります。

(*5)ソーシャルエンジニアリング

ネットワークの技術やコンピュータ技術を用いずに、人間の心理や社会の盲点を突いて、パスワードなどの機密情報を入手する方法。

例えば、言葉巧みにパスワードを聞き出す、廃棄物から重要な情報を読み取る、社員になりすまして盗み見や盗み聞きをする、など。

ソーシャルワーク、ソーシャルハッキング、ソーシャルクラッキングと呼ばれることもあります。

9.参考情報

- 2006 年度 情報セキュリティインシデントに関する調査報告書(JNSA)
<http://www.jnsa.org/result/2006/pol/incident/070720/>
- セキュリティ At Home
<http://www.microsoft.com/japan/protect/default.mspx>
- 不正アクセス行為の禁止等に関する法律
<http://www.ipa.go.jp/security/ciadr/law199908.html>
- 不正アクセス行為は処罰されます！
<http://www.npa.go.jp/cyber/legislation/gaiyou/main.htm>

IPA 対策のしおり シリーズ

<http://www.ipa.go.jp/security/antivirus/shiori.html>

- IPA 対策のしおり シリーズ(1) ウイルス対策のしおり
- IPA 対策のしおり シリーズ(2) スパイウェア対策のしおり
- IPA 対策のしおり シリーズ(3) ボット対策のしおり
- IPA 対策のしおり シリーズ(4) 不正アクセス対策のしおり
- IPA 対策のしおり シリーズ(5) 情報漏えい対策のしおり
- IPA 対策のしおり シリーズ(6) インターネット利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(8) スマートフォンのセキュリティ対策のしおり



IPA

独立行政法人 情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込2丁目28番8号
(文京グリーンコートセンターオフィス16階)

URL <http://www.ipa.go.jp/security/>

【情報セキュリティ安心相談窓口】(コンピュータウイルスおよび不正アクセス)

URL <http://www.ipa.go.jp/security/anshin/>

E-mail anshin@ipa.go.jp