

新入社員等研修向け
情報セキュリティマニュアル Rev.3

一般社団法人 JPCERT コーディネーションセンター

2010年4月14日
(更新：2014年3月26日)

目次

はじめに	3
1 企業等における PC 端末利用者のための基本的な情報セキュリティ対策	4
1.1 発生し得る問題事象	5
1.1.1 頻繁に見られるインシデント	5
1.1.2 インシデントによる被害の例	6
1.1.3 組織に与えるインパクト	6
1.2 インシデントの原因及び発生を抑止するための対策	9
1.2.1 全般的な原因と対策	9
1.2.2 Web サイトに関連するインシデントの原因と対策	20
1.2.3 電子メールに関連するインシデントの原因と対策	24
2 インシデント発生時における基本的な対応	36
2.1 インシデントの発生に気が付いた時、まずどうすればよいのか	37
2.2 セキュリティ担当者が取るべき一般的な対応	38
おわりに	40
参考文献・資料	41

はじめに

新年度を迎え、社会人研修や業務セミナーなどが活発になる時期ですが、電子メールやPCの利用に関するマナーやセキュリティ対策は、もはや新人研修には欠かせない項目となっています。この文書は、企業や組織の教育担当者や情報セキュリティ担当者に向けて、新入社員等に情報セキュリティに関する知識を教える際のガイドライン、研修資料のベースとなるような情報やトピックを、JPCERT コーディネーションセンター（以下「JPCERT/CC」といいます。）がまとめたものです。Rev.3 では、昨今の情報セキュリティインシデントの発生状況やスマートフォンなどの新しいデバイスなどに関して追記しました。

なお、教育担当者や情報セキュリティ担当者向けのメッセージをコラム形式（「教育担当者・システム管理者の方へ」という囲み記事）で記載することで、新入社員向けのコンテンツとして直接利用できる部分と、そうでない部分を区別できるようにしています。

また、本編の補助教材として、初心者にはセキュリティ意識を高めてもらうために、クイズ形式の資料を作成しました。クイズは簡単なものですが、考え方やアプローチを身に付けることを意識できるように工夫してあります。本編と併せて、セキュリティ対策やインシデント対応に関する社内ルールの教育、研修等にご活用いただければ幸いです。

※各 Web 資料は、2014 年 3 月 3 日において、最終アクセス確認をいたしました。

1 企業等における PC 端末利用者のための基本的な情報セキュリティ対策

教育担当者・システム管理者の方へ

個人情報の漏えいをはじめ、情報セキュリティ上の問題に関する報道が後を絶たない昨今、各企業においては、それぞれ情報セキュリティに関する社内ルールを定めたり、情報セキュリティの担当者を置いたりして、対策を進めていらっしゃると思います。しかしながら、せっかくルールを周知しても、意義や目的の分からないルールは、忘れられたり、無視されたりすることが少なくありません。社内の情報セキュリティに関するルール等の徹底を図るためにも、どんな PC の使い方がセキュリティ上の問題事象を発生させるのか、またそのような情報セキュリティ上の問題が会社にどのような被害をもたらすか、そのような被害を発生させないためにはどう対処すればよいのか、といったことを新入社員の段階から周知しておくことは、企業や組織にとって重要なことであるといえます。

電話の応対やビジネスマナーを身に付けることと同様に、セキュリティに関する正しい知識や対応方法を新入社員のうちから身に付けてもらうようにしましょう。

1.1 発生し得る問題事象

セキュリティ上問題のある PC の利用や注意を欠いた PC の操作は、情報セキュリティ上の脅威であり、問題事象（以下「インシデント」といいます。）を引き起こす可能性があります。

1.1.1 頻繁に見られるインシデント

企業において、一般的に起こりがちなインシデント、日頃からの注意を怠ると発生してしまうインシデントとしては、以下のようなものがあります。

- ソフトウェアのセキュリティ上の弱点（以下「脆弱性」といいます。）について、製品開発者から修正プログラムが公開されているにもかかわらず、適切な対応をせずに放置したために、その脆弱性が第三者に攻撃されて「マルウェア」に感染

「マルウェア」とは、「malicious software」が短縮された語で、コンピュータウイルスのように、コンピュータやネットワーク上で、利用者の意図に反した害のある動作を行うように設計されたソフトウェアやプログラムの総称です。（本書では、コンピュータウイルスをマルウェアと表記します。）

- セキュリティ対策が不十分な PC（OS やアプリケーションの修正プログラムを怠っている、ウイルス対策ソフトを最新の状態に更新していない等）で、悪意のあるプログラムを埋め込まれた Web サイトを閲覧したために、マルウェアに感染
- ID やパスワードを、安易なものに設定したり、不用意に公開したりしたために、第三者がその ID やパスワードを悪用して情報システムに不正に侵入
- 安易なデータの持ち出しによる情報漏えい（媒体の置き忘れ、自宅 PC のマルウェア感染、取引先情報が入ったスマートフォンの紛失等）
- USB メモリ等の記録媒体の安易な使用によるマルウェア感染
- 電子メールの誤送信による情報漏えい
- 電子メールに添付された不正なファイルを開くことによるマルウェア感染
- ブログ、SNS、掲示板、Twitter 等への安易な書き込みによる情報漏えい、及び漏えいした情報を悪用した標的型メール攻撃等によるマルウェア感染

1.1.2 インシデントによる被害の例

マルウェア感染や不正侵入等のインシデントが発生した場合、例えば、以下のような被害の発生が想定されます。

- PC やファイルサーバ内のデータが窃取されて悪用される（個人情報や企業秘密の漏えい。マルウェア感染や不正侵入に気付いて対処するまで情報を窃取され続ける可能性があります）
- PC やファイルサーバ内のデータが破壊されたり、改ざんされたりする（業務継続に支障）
- マルウェアに感染した 1 台の PC から、社内ネットワーク上の他の社員の PC やシステムに感染が拡散する（業務の継続に支障）
- マルウェアに感染した PC が、他組織のシステムに対する DDoS 攻撃などの道具として悪用される

「DDoS 攻撃」とは、マルウェアなどによって行われる分散型サービス不能攻撃で、主に Web サイトなどのサーバに大量のデータを送りつけて、システムを麻痺させるものです。DDoS 攻撃では、マルウェアに感染した多数の PC が攻撃に悪用されます。

- 管理の甘いサーバが不正アクセスされ、フィッシングサイトを立てられたり、マルウェアに感染させるための攻撃サイトに仕立てられたりする（悪意ある攻撃に加担させられる）
- 自社の Web サイトが改ざんされ（不正なコードの埋め込み等）、サイトを閲覧したユーザにマルウェアをダウンロードさせてしまう（信用の失墜）

1.1.3 組織に与えるインパクト

前項に示したようなインシデントが発生した場合、業務の中断や復旧のための経費等の直接的な被害のみならず、例えば、個人情報や取引先から提供を受けている秘密情報等が漏えいした場合は、損害賠償責任などの債務が生ずることもあります。さらに、取引先からの信用の失墜や市場でのイメージダウンなど社会的評価の低下を招き、その後の事業に大きなダメージを与えてしまう可能性さえあります。

昨今、規模の大小を問わず多くの Web サイトが改ざんの被害を受けています。Web サイト改ざんが発生した場合、改ざんされた Web サイトを閲覧したユーザの PC 等が、マルウェアに感染するケースが多く、改ざんを受けた企業は、自社サイトの改ざん箇所の修正や情

報漏えい等の被害の有無の確認といった復旧対応に加えて、サイト利用者への謝罪や問い合わせ対応に追われることにもなります。

企業内のシステムがマルウェア感染の被害を受けた場合、その被害額は中小企業で 1 社当たり平均 430 万円、大企業では 1 億 3000 万円にも上るという試算¹があります。また、個人情報の漏えいに関する損害賠償金額に関し、「もし被害者全員が損害賠償請求したら」という仮定に基づき、リスク定量化の手法によって損害賠償額の想定を行った場合、2011 年度の日本国内の想定賠償額の総額は 1,899 億円と想定することができ、各情報漏えいインシデントにおける一人当たりの想定損害賠償額の平均値は、4.8 万円以上と計算されるとの調査、分析データもあります²。情報セキュリティに関するインシデントには、金銭的被害が伴う場合が少なくないことを肝に銘じておきましょう。

¹ IPA - 2005 年 企業における情報セキュリティ事象被害額調査報告書 (情報処理推進機構 ウィルス被害額算出モデル研究会)

http://www.ipa.go.jp/security/fy17/reports/virus-survey/documents/2005_model.pdf

² 2011 年 情報セキュリティインシデントに関する調査報告書 (日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ、情報セキュリティ大学院大学 原田研究室 廣松研究室)

http://www.jnsa.org/result/incident/data/2011incident_survey_ver1.2.pdf

教育担当者・システム管理者の方へ

インシデントが発生してしまった場合には、被害を最小化するために、社員がルールに従って迅速かつ適切な対応を行う必要があります。対応ルールを把握していない新入社員が初期の判断を誤ることで、関係部署への報告や組織的な対応が遅れてしまい、被害が拡大することも懸念されます。

加えて、インシデントを引き起こした者は、自身の責任問題に考えが及び、インシデントを秘匿してしまう可能性もあります。まずは、インシデントを適切に収束させることが重要であることを周知徹底しましょう。

また、インシデントが発生した時にそれを認識できなければ、せっかく定めた対応ルールも無駄になってしまいます。目に見える被害や不具合がない状態でも、ログ監視、ソフトウェアの状態チェック、各種モニタリングの仕組み等により、インシデントを認識することができる体制を作っておくことも重要です。

インシデント発生後の対応や日頃の監視作業については、以下の資料を参考にしてください。

JPCERT/CC CSIRT マテリアル

https://www.jpcert.or.jp/csirt_material/

1.2 インシデントの原因及び発生を抑止するための対策

教育担当者・システム管理者の方へ

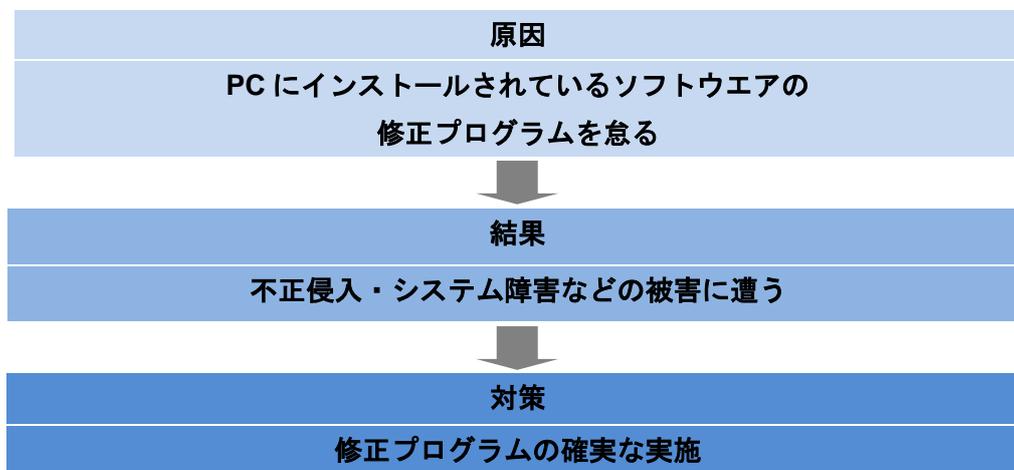
インシデントによる被害の発生を抑止するためには、以下の資料などを参考に、新入社員に対して、インシデントの原因と被害の発生を抑止するための対策に関する基本的な情報を理解させておくことが重要です。

JPCERT/CC インシデントハンドリングマニュアル

https://www.jpCERT.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf

1.2.1 全般的な原因と対策

1.2.1.1. PC にインストールされているソフトウェアのアップデートを怠る



ソフトウェアは、最初にインストールした状態でずっと使い続けられるものではなく、セキュリティ上の脆弱性対応のための修正プログラム適用等のメンテナンスを継続しながら使うものであることを、認識しましょう。PC にインストールされている OS やアプリケーションについては、最新の修正プログラムを適切に適用し、脆弱性の解消を怠らないことが最も基本的かつ重要な対策であるといえます。

また、一部の PC には出荷状態で様々なアプリケーションがプリインストールされている場

合があります。自身が普段使用していないソフトウェアだからといって攻撃に使用されないわけではないので、これらについても最新の修正プログラムを適宜適用するか、使用していないのであれば、アンインストールするようにしましょう。

Microsoft Windows や Microsoft Office 製品については、初期状態で修正プログラムの自動更新 (Microsoft Update) が行われるようになっていますが、Web ブラウザ、ワープロソフト、ユーティリティソフトなどには、自動更新機能がないものや手動で設定しないと機能しないものもあります。

以下の URL や使っているソフトウェアのヘルプ機能などを参照して、自動更新機能の設定方法や手動での更新方法などを調べておきましょう。

Windows Update 利用の手順

http://www.microsoft.com/japan/security/bulletins/j_musteps.msp

Acrobat 9.1/Adobe Reader 9.1 アップデートインストール手順 (Windows)

<http://kb2.adobe.com/jp/cps/235/235294.html>

無料 Java のダウンロード (Version7 Update51、日本語)

<https://java.com/ja/download/>

JUST オンラインアップデートの使い方

<http://support.justsystems.com/faq/1032/app/servlet/qadoc?QID=043657>

修正プログラムの適用は、時間がかかったり、業務を中断して行わなければならないかったりする場合もあるので、後回しにされがちです。しかしながら脆弱性に関する情報が公開されると、直後からその脆弱性を狙った攻撃が発生することもあります。製品開発ベンダから修正プログラムが公開された時は、システム管理者等の指導の下、なるべく早く適用するように心掛けましょう。

修正プログラムが製品開発ベンダから提供されるまでの間に、対象となる脆弱性を狙う攻撃を「ゼロデイ攻撃」といいます。このゼロデイ攻撃が発生しているとの情報があった場合には、製品開発ベンダから修正プログラムが提供されるまでの間は、そのアプリケーションについて、利用を見合わせる、または、十分慎重を期して利用するほかはありません (製品開発ベンダから修正プログラムが提供される前であっても、ウイルス対策ソフトで攻撃の検出等が可能となる場合もあります)。事態が深刻であればあるほど、

製品開発者からの修正プログラム修正プログラムの提供も迅速に行われるはずですので、これらのソフトウェアの更新に関する情報に注意し、修正プログラム修正プログラムが公開された際には直ちに適用するようにしてください。

修正プログラムは、すべてのセキュリティ対策の基本ですから、常日頃から怠らないようにしてください。

教育担当者・システム管理者の方へ

使用しているソフトウェア全てについて、どのような脆弱性が発見され、修正プログラムが出回っているのか、その適用が必要なのか、といった情報については、各社員に個別に収集する作業を強いることにならないよう、各組織における情報セキュリティ担当者やインシデントへの緊急対応を行う組織（CSIRT：Computer Security Incident Response Team）が責任をもって収集し、自社の情報システムにとって対応が必要な情報か否かを判断した上で、対応方法を社内に指示、周知することが望ましいといえます。

このような担当者や組織が存在する企業では、一般の社員に対し、担当部署からの指示に迅速に対応すべきこと（どの部署が責任を有しているのかも含め）を周知する必要があります。

一方、セキュリティ担当者や CSIRT のような組織がない企業では、Microsoft Update やその他ソフトウェアのアップデートに関する情報を、各社員が独自に収集して対応することになります。そのため、各社員に対し、修正プログラムに関する情報の収集の仕方や収集した情報に基づく対処の仕方を周知しておくことが必要です。

（続く）

(続き)

また、情報セキュリティ担当者やインシデントへの緊急対応を行う組織が存在する組織であっても、一般社員が無断でソフトウェアをインストールすると、そのソフトウェアが管理対象からはずれた状態で使用され続け、結果として修正プログラムが適用されず、マルウェアに感染してしまうという事態が生じる可能性もあります。このため、一般社員に対しては、ソフトウェアの無断インストールを禁止し、必ず許可を得た上でソフトウェアをインストールするよう徹底することをお勧めします。

ソフトウェアの無断インストールの危険性については、「1.2.1.4 ソフトウェアの無断インストール」の部分も参照してください。

なお、市場に流通しているソフトウェアの脆弱性情報は、以下のサイトをチェックすることで調べることができます。

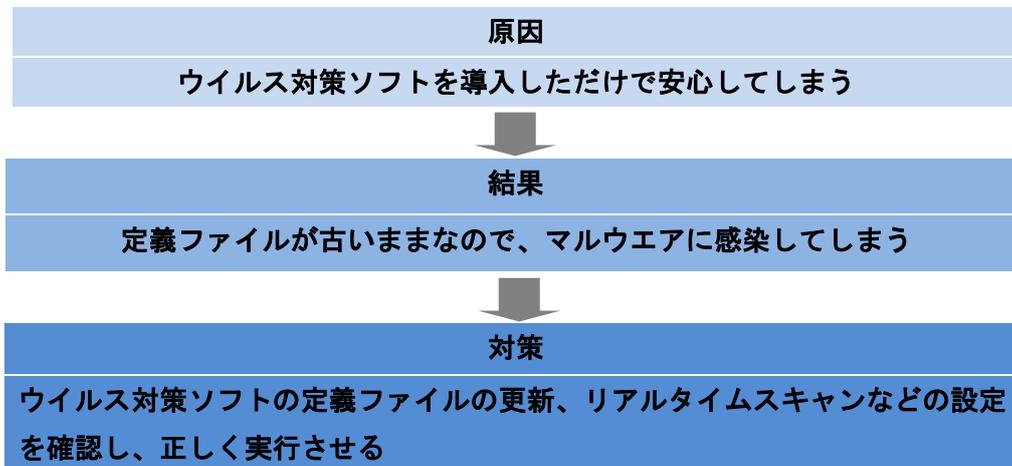
JVN (Japan Vulnerability Notes)

<https://jvn.jp/>

JVN iPedia

<http://jvndb.jvn.jp/>

1.2.1.2. ウイルス対策ソフトを導入しただけで安心してしまふ

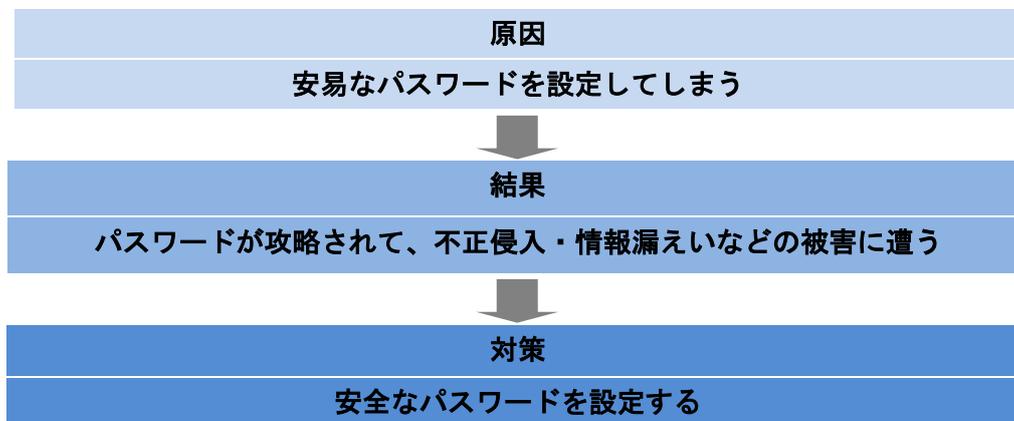


ウイルス対策ソフトは、インストールしただけでは十分ではありません。マルウェア感染予防のためには、定義ファイルを常に最新の状態に保つことが必要です。一般的なウイルス対策ソフトは、初期状態で定義ファイルの自動アップデートや定期的なウイルススキャン（検索）、そしてファイルアクセスを常時監視するリアルタイムスキャンの自動実行が有効になっています。この設定を自分の判断で変更すると、定義ファイルのアップデートやリアルタイムスキャンの自動実行が無効になってしまい、ウイルス対策ソフトの用をなさなくなってしまう可能性がありますので、設定の変更は十分慎重に行いましょう。

ウイルス対策ソフトの有効期限が切れると、定義ファイルのアップデートが行われなくなります。期限切れのウイルス対策ソフトを使い続けているかどうかともチェックしてください。

また、昨今の企業の知財などを狙ういわゆる標的型攻撃では、ウイルス対策ソフトで検知されにくいマルウェアが使用されています。ウイルス対策ソフトの能力を過信せず、1.2.1.1.章で述べたようにOSやソフトウェアの適切な更新といった基本的な対策を徹底することを忘れないでください。

1.2.1.3. 安易なパスワードを設定してしまう



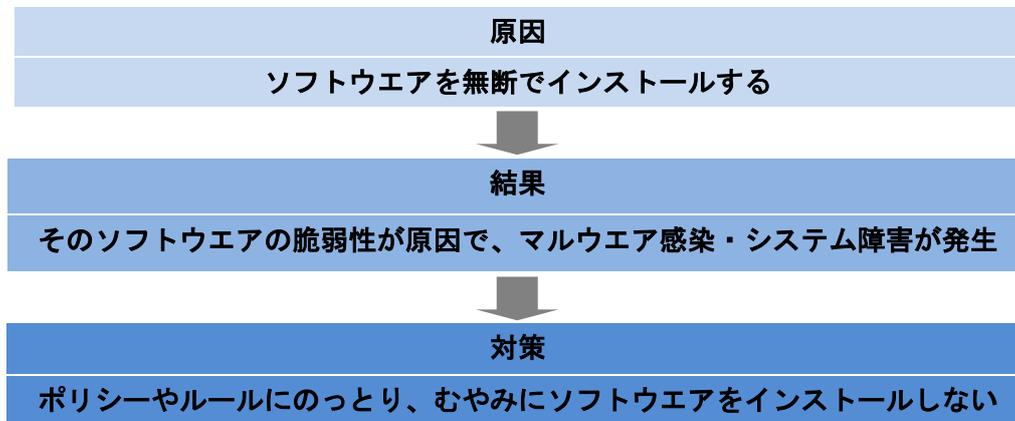
ログインパスワードは、なるべく長い文字列とし、他人に推測されにくいようにしましょう。短いパスワードや安易なパスワードは、総当たり攻撃（ブルートフォース攻撃：機械的な処理により可能な組み合わせすべてを試す攻撃方法）で割り出されてしまう可能性があります。また、辞書に載っているような一般的な単語の組み合わせでは、辞書データを使った攻撃（辞書攻撃）で簡単に割り出されてしまいます。

総当たり攻撃を回避するためにパスワードを定期的に変更する運用が効果的であるとする見解もありますが、定期的に変更すると、ついつい覚えやすい簡単なパスワードを設定するようになりがちです。そのような事態は本末転倒といわざるを得ません。実際にどのようなパスワードを設定したらよいかについては、後述の「1.2.4 特に新入社員が起こしがちな問題への対応」の「安全なパスワードの作り方を知る」を参照してください。

また、ノート PC などの外部へ持ち出す機器の取り扱いについては十分に注意してください。ノート PC が紛失や盗難に遭った場合、たとえログインパスワードなどを設定していたとしても、攻撃ツールなどによる総当たり攻撃や辞書攻撃などによってパスワードが破られ、結果として内部に保存していた機密情報などが流出する危険性があります。このような事態を想定し、外部へ持ち出す機器には機密情報などを保存せず、やむを得ず保存する場合は個別に暗号化するようにしましょう。

なお、ユーザ認証のための ID やパスワードを Web ブラウザに記憶させる機能については、記憶させた ID やパスワードを窃取するマルウェアも存在していますので、リスクを十分に考慮した上で使用してください。

1.2.1.4. ソフトウェアを無断でインストールする



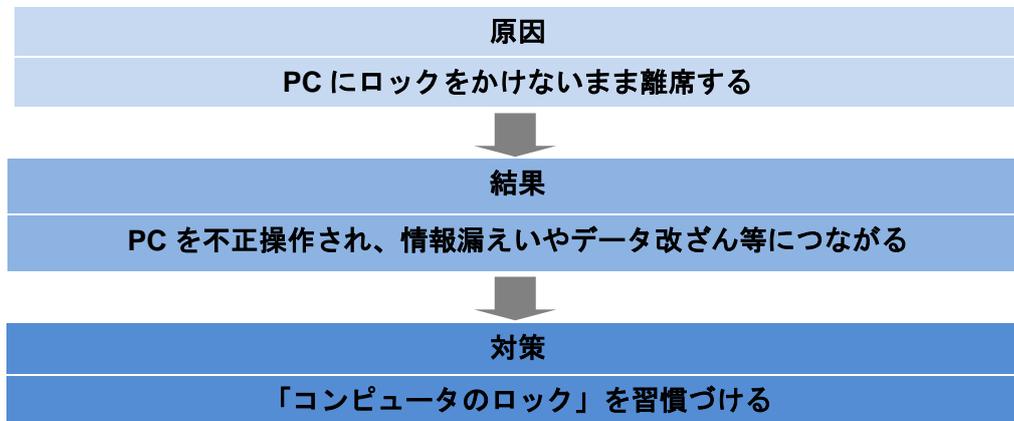
便利そうだからという理由で、システム管理者や情報セキュリティ担当者等に無許可でソフトウェアをインストールするのは大変危険です。通常、企業におけるソフトウェア管理というと、ライセンスの管理に注目が集まりがちですが、脆弱性対策も非常に重要です。ライセンス料の発生しない無償のツールであるからという理由でシステム管理者に無断でソフトウェアをインストールすると、そのソフトウェアの脆弱性を突く攻撃を受けた場合、対策が後手に回ったり、原因の究明が遅れてしまったりする原因になってしまいます。

1.2.1.1 に記載のとおり、ソフトウェアは、最初にインストールした状態でずっと使い続けられるものではなく、セキュリティ上の脆弱性への対応のためのアップデートや修正プログラムの適用等のメンテナンスを継続しながら使うものです。無断でインストールされたソフトウェアは、企業の管理プロセスの対象外となり、結果的に利用している PC がマルウェアに感染する原因となってしまう可能性があります。

また、無料のセキュリティ対策ソフトを装ったマルウェアによる被害は毎年のように発生していますし、2013 年にはクラウドサービスと連携した IME（文字入力補助ソフト）により、PC で入力した文章などの情報が意図せず外部に送信されてしまっていたという事態も発生しています。

リスクに曝されるのは、会社の情報資産であることを肝に銘じ、使用するソフトウェアはシステム管理者や情報セキュリティ担当者の許可を得たものにしましょう。

1.2.1.5. PC にロックをかけないまま離席する



秘密文書などを不用意に机の上に広げたまま放置すべきでないのと同様に、作業中の PC の画面をそのままにして席を外してはいけません。第三者に PC 内の機密情報にアクセスされたり、マルウェアをインストールされたりする危険性があります。特にオフィス内に外部の人間が頻繁に出入りするような場所では注意が必要です。

PC の前を離れる時には必ずログオフする、もしくは PC をロックする習慣をつけましょう。Microsoft Windows を使っている場合、Windows キー+L で「コンピュータのロック」が簡単に行えます。また、スクリーンセーバーロック（設定によって、数分でスクリーンセーバーを自動起動し、スクリーンセーバーの解除をパスワードにて行う）も可能ですが、スクリーンセーバーが起動されるまでの空白時間が存在するので、注意が必要です。

なお、Macintosh (OS X) でコンピュータ画面をロックしたり、スリープ解除後にパスワードを要求したりする方法は、以下の URL を参照してください。

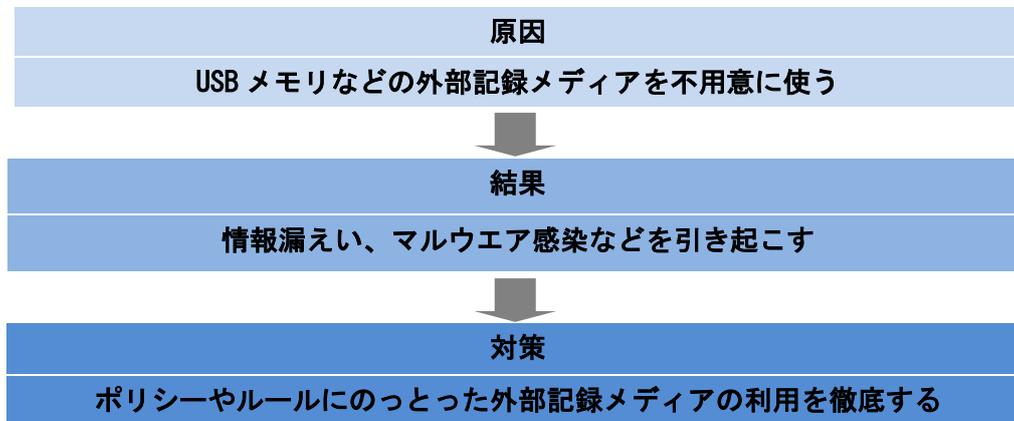
Mac OS X 10.6: コンピュータの画面をロックする

http://support.apple.com/kb/PH6895?viewlocale=ja_JP

OS X Mavericks: Mac のスリープ解除後にパスワードを要求する

http://support.apple.com/kb/PH13915?viewlocale=ja_JP&locale=ja_JP

1.2.1.6. USBメモリなどの外部記録メディアを不用意に使う



自宅での作業や取引先とのデータ受け渡しのために、USBメモリなどにデータを保存して社外に持ち出したいこともあるでしょう。しかしながら、社外に持ち出されたUSBメモリなどが紛失や盗難に遭うリスクはゼロではありませんので、情報漏えいの可能性が否定できません。組織で決められたデータの持ち出しやデータ消去のポリシーを理解し、不用意な外部記録メディアの利用は控えましょう。

万が一、USBメモリなどが紛失、盗難に遭ったとしても、その内容が暗号化されていれば、情報漏えいのリスクを低減させることができます。現在、そのような機能を搭載したUSBメモリも市販されています。暗号化のパスフレーズも、解読のリスクを下げるため十分な長さで数字、記号を含めた強度の高いものを設定してください。

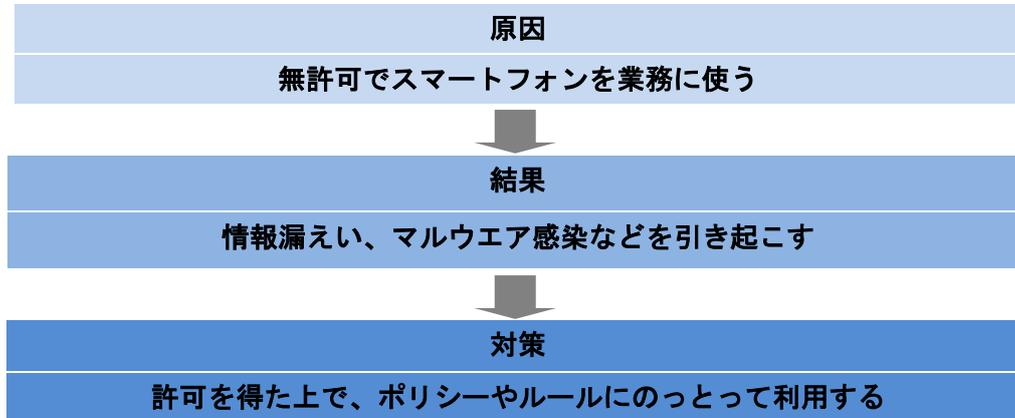
USBメモリなど外部記録メディアを利用する場合には、ウイルス対策ソフトのリアルタイムスキャンを利用したり、自動実行機能を無効にしたりするなどの対策を講じてください。

また、携帯型音楽プレーヤーやデジタルカメラ、ビデオカメラなどのデジタル機器経由でマルウェアに感染する事例もあります。管理状態が定かでないこれら機器を許可なく会社のPCに接続しないようにしましょう。

IPA「USBメモリのセキュリティ対策を意識していますか？」— USBメモリの安全な使い方を知ろう —

<http://www.ipa.go.jp/security/txt/2009/05outline.html>

1.2.1.7. 個人所有のスマートフォンの利用



スマートフォンの急速な普及に伴い、多くの新入社員がスマートフォンを友人、知人とのコミュニケーションなどに活用していると思います。企業活動においても、スマートフォンを利用する動きが広がっており、昨今のスマートフォンの高機能、高性能化の流れも受けて、多くの企業活動のシーンにおいてスマートフォンが活用されるようになってきました。

新入社員の皆さんも今後業務等へのスマートフォンの利用を考えていると思いますが、スマートフォンの利用については十分な注意が必要です。昨今のスマートフォンは高機能化の結果、PCと同程度の作業を行えるものも出てきており、スマートフォンに契約書や顧客リストなどの機密情報を保存して、外出先で編集・閲覧するシーンやメモ代わりに会議内容が書かれたホワイトボードを撮影するといったシーンも出てくると思います。そういった用途で使用しているスマートフォンを紛失したり、マルウェア感染や盗難の被害を受けたりした場合は、企業にとって重要な機密情報が外部に漏えいしてしまうことになります。私用で使っている分には、盗難や紛失などの問題が発生しても、個人の責任の範囲で対処すればよかったです。業務で利用するスマートフォンの盗難、紛失は企業の機密情報の漏えいなどにつながり、結果として企業に損害や影響を与える可能性があります。

このため、個人所有のスマートフォンを業務で利用する際は、事前に上司やシステム管理部門の許可を得た上で、スマートフォンの利用に関する規定やガイドラインに従って利用しましょう。もし、利用規定がない場合は、上司や先輩にスマートフォンを利用することを報告し、利用方法や注意点についてきちんと確認した上で利用するようにしましょう。

スマートフォン&タブレットの業務利用に関するセキュリティガイドライン

(日本スマートフォンセキュリティフォーラム)

http://www.jssec.org/dl/guidelines2011_v1.1.pdf

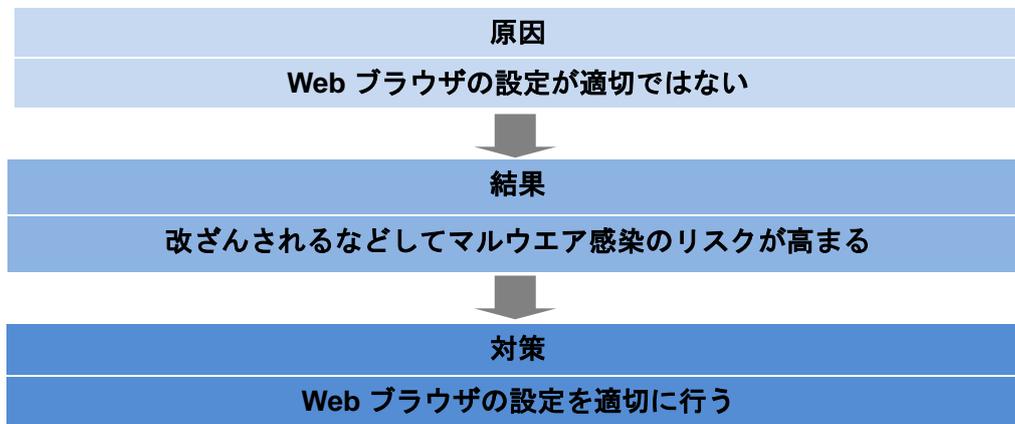
スマートフォンの安全な利活用のすすめ ～ スマートフォン利用ガイドライン ～

(日本ネットワークセキュリティ協会)

http://www.jnsa.org/result/2012/smap_guideline_v1.0.pdf

1.2.2 Web サイトに関連するインシデントの原因と対策

1.2.2.1. Web ブラウザの設定が適切ではない



Web サイトの中には、悪意をもって設置された危険なサイト（知らないうちにマルウェアをダウンロードさせるなど）があります。また、正規のサイトを改ざんし、危険なサイトに誘導するプログラムを埋め込むなどして、閲覧者の PC をマルウェアに感染させるといった攻撃も増えています。そのような Web サイトを閲覧した場合には、知らないうちに PC がマルウェアに感染してしまう可能性があります。

昨今の Web ブラウザにはセキュリティ機能が実装されているものが多く、ほとんどの場合、標準で動作するように設定されています。このセキュリティ機能により、一部の攻撃をブロックできる可能性があります。Web ブラウザの設定については、社内規程などに従った設定を行い、セキュリティレベルが低下するような設定変更は行わないようにしてください。

Internet Explorer の保護モードの機能

<http://windows.microsoft.com/ja-JP/windows-vista/What-does-Internet-Explorer-protected-mode-do>

Mozilla Firefox プライバシーとセキュリティの設定

<https://support.mozilla.org/ja/products/firefox/privacy-and-security>

Web ブラウザの設定で防げないマルウェアも、OS やアプリケーションの修正プログラムを適切に実施しておくことで、感染する可能性を大幅に低下させることができます。このた

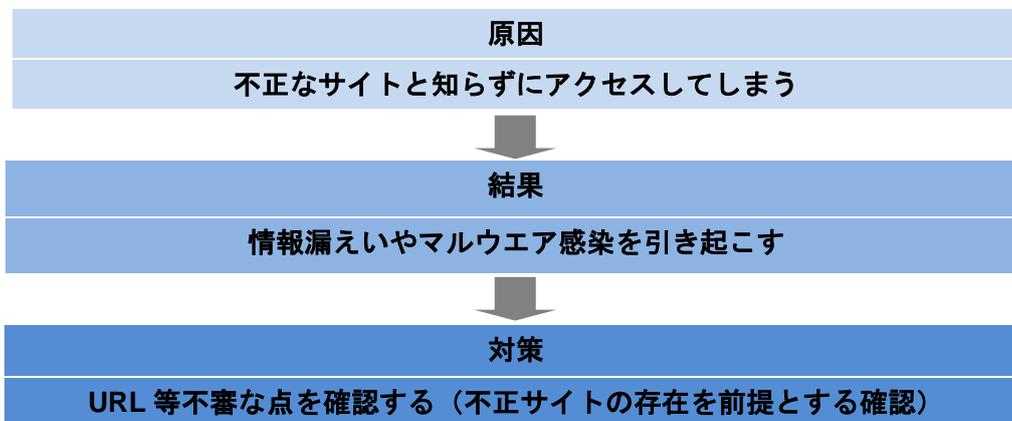
め、1.2.1.1. 章で述べたように OS やソフトウェアの適切な更新を心掛けましょう。

教育担当者・システム管理者の方へ

Web ブラウザのセキュリティ設定はむやみに変更しないことが基本となりますが、組織の業務の内容によっては、セキュリティレベルを更に上げる必要がある場合や、逆に業務上無効にできないサービスや機能が存在する場合があります。

どちらの場合も、業務効率とリスクに対する運用のガイドラインを定め、社内での周知を図ることが重要です。

1.2.2.2. 不正なサイトと知らずにアクセスしてしまう



迷惑メールなどに含まれている URL のリンクの中には、クリックした PC をマルウェアに感染させようとする危険な Web サイトに誘導するものがあります。このため、迷惑メールや、明らかに業務に関係のない不審な電子メールは、開かずに削除するようにしましょう。また、業務に関係があるかどうか分からない場合は、同僚や上司に相談したり、システム管理者に確認したりするようにしましょう。

迷惑メールの中には金銭詐取を目的としたフィッシング³メールが含まれていることがあります。フィッシングメールに誘導された偽のサイトで、個人情報や ID、パスワード、その他の情報を入力してしまうと、その情報が攻撃者の手に渡ってしまいます。

Web サイト上で情報を入力する際には、アクセス先が正規のサービス提供会社の Web サーバであることに加え、入力した情報が SSL 暗号化通信によって保護されていることを確認しましょう。

Microsoft Windows Internet Explorer

SSL (Secure Sockets Layer) 証明書に関する情報を取得する

<http://windows.microsoft.com/ja-jp/windows-vista/get-information-about-secure-sockets-layer-ssl-certificates>

Mozilla Firefox

Web サイトへの接続が安全か確認するには

<https://support.mozilla.org/ja/kb/how-do-i-tell-if-my-connection-is-secure>

Google Chrome

ウェブサイト設定 (ページ内「サイトがセキュリティで保護された接続 (SSL) を使用しているか確認する」に記載あり)

<https://support.google.com/chrome/answer/95617>

アクセス先が正規のサービス提供会社の Web サーバであることは、そのサイトのドメインが、普段から使用している正規のサイトのドメインと一致しているかどうかで確認します。ただし、正規サイトと類似した偽のドメインを使用した攻撃も確認されていますので、ドメインを確認する場合は、類似したドメインが使用されていないかといった点についても注意するようにしましょう。類似ドメインについては、「コラム：類似ドメインについて」を参照してください。

また、Web サイトとの暗号化通信に使用される SSL サーバ証明書⁴から Web サイトの主体者 (サイトの持ち主) を調べることができますが、一般の SSL サーバ証明書については、

³ フィッシングとは：フィッシング対策協議会

https://www.antiphishing.jp/consumer/abt_phishing.html

⁴ サーバー証明書：総務省 国民のための情報セキュリティサイト

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/yougo/sa_gyou.htm

誰を主体者として記載するかの審査基準が必ずしも統一されておらず、SSL サーバ証明書
の存在のみでは、サイトの正当性を判断できません。ただし、最近では、証明書に記載さ
れる主体者の審査に一定の基準が設けられている **Extended Validation** 証明書(SSL/TLS サ
ーバ用の証明書の場合、**EV SSL** 証明書とも称される) による電子認証サービスが提供され
ており、証明書を発行する認証局によって、主体者の法的存在、アイデンティティ (法的
名称)、ドメイン名使用権等が基準に従って確認されています。閲覧するサイトにおいてこ
の証明書が利用されている場合は、アドレスバーが緑色になり、**Web** サイト所有者の名称
や所在地の要約と、証明書を発行した **CA** (認証局：サーバ証明書を発行する企業・組織)
の名称を交互に表示するラベルが表示されます (Microsoft Internet Explorer の場合)。

また、SSL 暗号化通信が行われていることは、**Web** ブラウザのアドレスバーに表示される
URL が「<http://> ……」ではなく、「<https://> ……」で始まっていることやアドレスバーの鍵
アイコンなどで確認することができます。

最近では、正規サイトかどうか簡単に判別できないような精巧なフィッシングサイトや、
正規のサイトが改ざんされて不正なプログラムが埋め込まれる事例も発生しており、危険
なサイトを見分けることは難しくなっています。

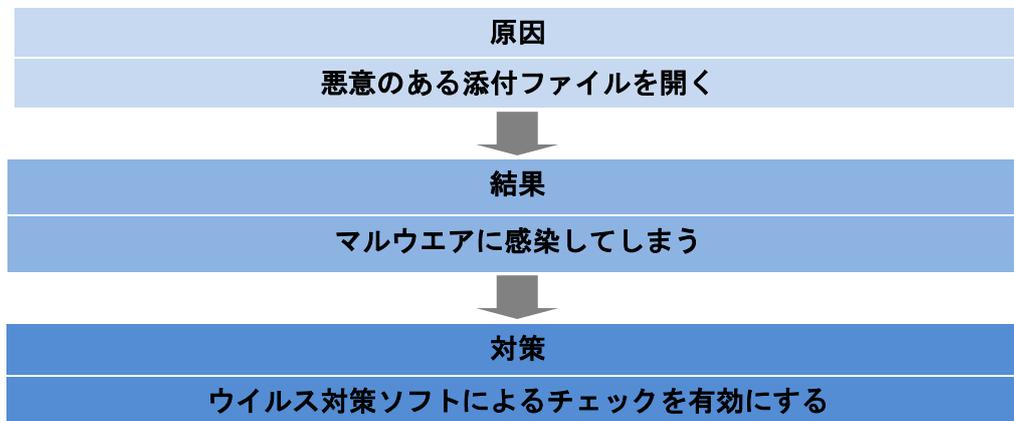
■ コラム：類似ドメインについて

閲覧者にあたかも正規サイトにアクセスしているように見せかけるた
めに、攻撃者が用意する攻撃サイト (フィッシングサイトなど) では類
似ドメインが使用されることがあります。類似ドメインには以下のよう
なものがあります。

- 1) 正規ドメインに似たもの
例) www.jpccert.or.jp *)[www](http://www.jpccert.or.jp) の後ろに「. (ドット)」がない
- 2) サブドメインに正規ドメインを使用するもの
(正規) www.jpccert.or.jp
(類似) www.jpccert.or.jp.example.com
誤入力を狙ったもの
例) www.jpccert.or.jp (jp の p を間違っ
て o と入力)

1.2.3 電子メールに関連するインシデントの原因と対策

1.2.3.1. 悪意のある添付ファイルを開く



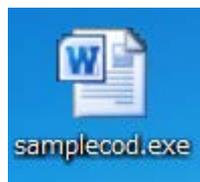
マルウェアが仕込まれた添付ファイルを実行させようとする電子メールは、後を絶ちません。見知らぬ人から送付された電子メールや、知っている人（企業）が送信者として表示されているが本文の書きぶりなどに不審な点がある電子メールに添付されたファイルは、不用意に開くことはせず、情報セキュリティ担当者に相談するなど慎重に対応しましょう。

特に添付ファイルの拡張子が“.exe”の場合（実行ファイル、自己解凍形式のファイルなど）は注意が必要です。ファイルを開く操作によってプログラムが実行され、自身でマルウェアをインストールしてしまうからです。

コラム：ファイル名の偽装

攻撃者は巧妙にマルウェアが仕込まれた添付ファイルを開かせようとするかもしれません。Windows の初期状態では、ファイルの拡張子は表示されないため、例 1 のように、アイコンを文書ファイルなどに偽装されると、一見して実行ファイルには見えなくなります。また、例 2 のようにファイル名をとて長い文字列にされた場合は、拡張子の .exe の部分が見えなくなる場合もあります。さらに、例 3 のように RLO (Right-to-Left Override) テクニックを使用して、拡張子を偽装されるかもしれません。

例 1：アイコン偽装



(この例では、実行ファイルと分かるように拡張子が表示される設定にしています。)

例 2：長いファイル名による拡張子を見えにくくするテクニック



(Windows7 以降の場合、ファイルをマウスで選択した場合は、拡張子まで表示されます。)

例 3：RLO によるファイル拡張子偽装



(*アイコンは事前に偽装済み)

教育担当者・システム管理者の方へ

警察庁が平成 25 年 8 月に公表した「平成 25 年上半期のサイバー攻撃情勢について」では、「やりとり型」攻撃と言われる標的型攻撃が急増しているとあります。お客様相談窓口等、業務上、見知らぬ人から送付されたメールの内容を確認しなければならない部署では、このような攻撃の被害に遭う可能性が高くなります。そのような部署では、社内のネットワークから切り離された環境を用意して添付ファイルの内容を確認する等、組織的にリスク回避のための措置を検討する必要があります。

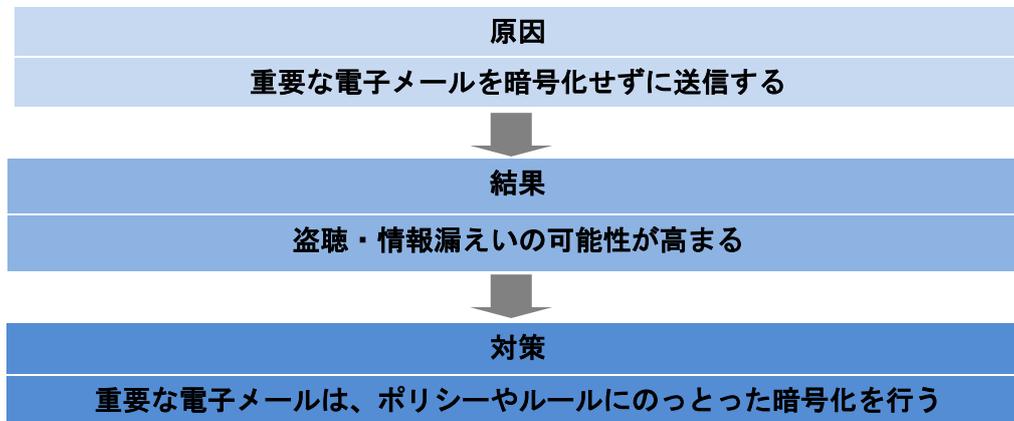
また、メールマガジンなどを発行している企業については、SPF/SenderID や DKIM の導入を検討することをお勧めします。送信者を詐称した迷惑メールが社会問題化している中、これらの技術は電子メールの送信者情報が詐称されているかどうかを受信者側で確認できるようにしてくれるものです。

SPF/SenderID や DKIM については、以下の資料を参照してください。

迷惑メール対策推進協議会 迷惑メール対策ハンドブック

http://www.dekyo.or.jp/soudan/anti_spam/report.html#hb

1.2.3.2. 重要な電子メールを暗号化せずに送信する



電子メールは、送受信の途中で第三者によって内容が盗み見られる可能性があります。電子メールを盗聴する方法としては、メールサーバやルータなどのネットワーク機器への不正な接続やアクセス、無線 LAN 通信の盗聴等が挙げられます。個人情報や企業秘密など第三者に見られてはいけない情報を電子メールでやりとりする場合には、必要に応じて電子メールそのものを暗号化して送信したり、重要な情報を添付ファイルにして、添付ファイルを暗号化して送信したりするようにします。

どのような内容ならば電子メールの暗号化が必要となるか、そもそも電子メールでどのような情報を送信してよいか等については、各会社のポリシーに従って判断します。

また、組織によっては、電子メールの内容の秘匿のための暗号化とは別に、送信者が誰であるかを示すことを目的に、電子メールの内容により電子署名を付すべき場合がルール化されている場合もあります。

電子メールの暗号化や電子署名の方法としては、PGP、S/MIME などがあります。詳細については以下の URL を参照してください。

JPCERT/CC はじめての暗号化メール (Thunderbird 編)

<https://www.jpCERT.or.jp/magazine/security/pgpquick.html>

IPA 電子メールのセキュリティ S/MIME を利用した暗号化と電子署名

http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.pdf

JPCERT/CC 電子メールソフトのセキュリティ設定について

<https://www.jpCERT.or.jp/magazine/security/mail/index.html>

電子認証局会議 電子署名活用ガイド

<http://www.c-a-c.jp/download/index.html>

■ コラム：公衆無線 LAN の利用上の注意

公衆無線 LAN の利用には注意が必要です。無線電波は、対象となる PC やルータなどのネットワーク機器に接続せずに傍受が可能です。

一般的な無線 LAN ルータは、盗聴やなりすまし対策として無線通信の暗号化機能や認証機能を提供していますが、一部の公衆無線 LAN サービスでは、これらの機能が提供されていなかったり、暗号化プロトコルとして脆弱である WEP が使用されていたりします。

このため、公衆無線 LAN サービスを利用する場合には、サービス内容(特にセキュリティ面)を事前に確認した上で、必要に応じて VPN で別途通信を暗号化するなどの対策を実施しましょう。(社内ポリシーで公衆無線 LAN サービスを使用する場合のルールが決まっている場合はそれに従ってください。)

1.2.4 特に新入社員が起こしがちな問題への対策

教育担当者・システム管理者の方へ

ビジネス上の慣習と同様に、情報セキュリティ上の注意事項も、多くの新入社員にとっては初めて目にするものです。ここでは新人が起こしやすいと思われる問題を事例ベースで整理してみました。その問題の対処方法も併せて記載していますので、「1 企業等における PC 利用者のための基本的な情報セキュリティ対策」と併せて、新人向けのセキュリティ研修の参考にしてください。

➤ P2P ファイル共有ソフトを使用しない

一部の P2P ファイル共有ソフト（Winny や Share など）を利用していると、著作権法に違反するファイルの提供や利用の積極的な意図がない場合でも、ファイルの中継を行うことにより著作権法違反の状態を招く可能性があります。なお、著作権法の改正により、2010 年 1 月から、著作権法上の違法ファイルと知っていてダウンロードする行為は、たとえ私的利用目的であっても違法になりました。P2P ファイル共有ソフトによる違法ファイルのダウンロードも、その適用を受ける可能性があります。

また、P2P ファイル共有ソフトの脆弱性を突いて、PC 上のファイルを流出させるマルウェアも存在しており、自宅で使用している PC がこのマルウェアに感染したために、持ち帰って使用していた業務用資料がネットワーク上に流出したという情報漏えい事件も発生しています。

業務用 PC はもちろん、個人所有の PC であっても業務用の情報を扱う可能性がある場合には、P2P ファイル共有ソフトの使用は控えましょう。いったんインターネットに流出してしまったデジタルデータは完全に消去することは不可能です。会社の業務資料等の情報が漏えいした場合には、漏えいした情報の回収（消去）のためのコストや信用の失墜、場合によっては損害賠償債務の負担等、会社に生じる損害は深刻なものとなってまいります。

また、会社の情報に限らず、個人の情報であっても、いったん流出してしまった場合の被害は自分が思っているより深刻ですから、P2P ファイル共有ソフトを安易に使うこと

は避けましょう。

さらに、自宅の PC については、家族で共用している場合、知らないうちに家族が P2P ファイル共有ソフトをインストールしている場合があります。P2P ファイル共有ソフトの利用に関する問題の認識を家族とも共有し、利用する PC の環境には注意を払うようにしましょう。

教育担当者・システム管理者の方へ

企業側においても、実際に発生している情報漏えい事件の多くが P2P ファイル共有ソフトの利用に起因していることに鑑み、業務データの持ち出しや業務データを利用することができる PC の制限等についてルールを定め、徹底することが重要です。

➤ 不必要な Web サイトの閲覧はしない

昨今の攻撃者は、不正なプログラムを仕込んだ Web サイトを使って、閲覧したユーザの PC をマルウェアに感染させ、PC 内から個人情報やアカウント情報、クレジットカード情報などを窃取して利益を得たり、他の攻撃のために悪用したりしようとしています。

かつては、攻撃者が別に用意した独自サイトに閲覧者を誘導する攻撃も多かったところですが、昨今は、正規の著名なニュースサイトや企業のサイトを改ざんし、攻撃のプラットフォームに使用されるようになっており、怪しいサイトに注意するというレベルでは回避が難しくなっています。このような攻撃を回避するための絶対的な対策はなく、攻撃に遭う可能性を低くするために、不必要な Web サイトの閲覧を控えるというのも一つの手です。

マルウェア感染等が発生した場合には、閲覧したサイトの履歴等を調査して、マルウェア配付サイトの閲覧の有無等を調査することが必要になります。著名なニュースサイトや企業の製品情報サイトを閲覧する場合であっても、悪意のあるプログラムが埋め込まれている可能性がゼロではないことを認識し、休み時間であっても、業務上、閲覧の必要性を説明することができないサイトは閲覧しないようにしましょう。(企業等のシステム管理者は、Web サイト改ざんの情報を入手した場合、自社の社員の閲覧の可能性等を考慮して、社内への注意喚起の発出や閲覧ログの確認等を検討することが多いので、シ

システム管理者が予期し得ないような（業務上の必要性がない）サイトの閲覧は、組織としてのセキュリティ対策の網からこぼれてしまう可能性が高くなります。）

一部では、職員が外部の **Web** サイトへアクセスすることを制限したり、許可されていない **Web** サイトにアクセスした際に警告を表示したりする仕組みを導入している組織があります。これは、悪意のあるプログラムが埋め込まれているような危険な **Web** サイトの閲覧について警告を表示し、ユーザの **PC** がマルウェアに感染しないようにするためものです。許可無く警告を無視して閲覧したり、警告を表示するサービスを無効化するといったことはしないようにしましょう。

また、攻撃サイトの中には、ゲームや音楽、壁紙などのコンテンツに隠してマルウェアをダウンロードさせるものがあり、そのようなサイトが、検索エンジンによる検索結果の上位項目に現れたり、検索キーワード連動広告として表示されたりすることがあります。検索エンジンによる検索結果だからといって、安易にクリックしてしまうと、マルウェア感染の被害を受けるかもしれません。コンテンツのダウンロードに当たっては、著作権の観点のみならず、マルウェア感染等のリスクの観点からも、正規のコンテンツ配信サービスの利用を心掛けましょう。

万が一これら攻撃サイトを閲覧してしまった場合であっても、**OS** やアプリケーション（ソフトウェア）を脆弱性のない状態に保ち、ウイルス対策ソフトを最新の状態に更新しておくことで、マルウェア感染による被害を最小限に抑えることができます。ソフトウェアの修正プログラム等の基本的な対策を怠らないことも重要です。

ちょっとした興味や好奇心から危険が潜むサイトにアクセスした場合にリスクに曝されるのは、会社の情報資産であることを認識しましょう。

➤ **フィッシング詐欺に気を付ける**

金融機関やインターネット上のサービスをかたるフィッシング詐欺が横行しています。フィッシングサイトの画面デザインは、正規のサイトと区別がつかないほど精巧なものが多く、**SSL** による暗号化通信であることを示す「鍵」のアイコンを表示させるフィッシングサイトも存在します。基本的には、閲覧する **Web** サイトの **URL** を確認することにより、正規サイトかどうかを見極めることが必要です。

また、**EV SSL** 対応ブラウザを利用して、**EV SSL** 証明書を利用しているサイトを閲覧すると、サイト運営者の名称等の情報を確認することができます。**EV SSL** 証明書を利用しているサイトの増加に伴い、このような証明書とブラウザによって表示される情報も正規サイトを見極めるための情報として用いることができるようになってきています。

➤ **電子メールの宛先 (To:や CC:) に多数のメールアドレスを入れない**

複数の相手に同時に電子メールを送る場合、宛先欄や CC:欄に多数のメールアドレスを記載すると、電子メールを受け取った人に、面識のない人のメールアドレスまで教えることになってしまうかもしれません。メールアドレスは、特定の個人を識別することができる場合に個人情報に該当する場合があるため、メールアドレスの取り扱いには十分気を付けましょう。

消費者庁 個人情報保護法に関するよくある疑問と回答より引用

http://www.caa.go.jp/seikatsu/kojin/gimon-kaitou.html#2_3

Q メールアドレスは、「個人情報」に該当しますか。

A 個人の氏名等を含んだリストがあり、その1項目としてメールアドレスが含まれている場合、リストは全体として、また、メールアドレスはその一部として、個人情報に該当します。

また、メールアドレスのみであって、ユーザー名及びドメイン名から特定の個人を識別することができる場合、そのメールアドレスは、それ自体が単独で、個人情報に該当します。

具体的には、多数の宛先に電子メールを送る場合は、宛先を列挙して送信することについて電子メールの受信者の了解が得られている場合を除き、Bcc:欄に宛先を列挙するか、メーリングリストを作った上でメーリングリスト宛てに送信するか、面倒でも1件ずつ送るようにしましょう。

➤ **業務に関する話をブログや SNS などで公開しない**

業務時間内に業務と関係のないブログの書き込みを行うことは禁止されている場合が多いと思いますが、業務時間外であっても、仕事の内容や取引先に関する情報をブログや Twitter や Facebook などの SNS で公開することは控えましょう。SNS もユーザ数が数十万、数百万という単位になれば、もはや不特定多数の者が見ている公開サイトと同様に評価すべきでしょう。ブログや SNS などに業務その他の企業活動に関する話が投稿されていると、その企業の情報管理の在り方が問われることにもなります。また、それらの情報を第三者が閲覧して、不正な目的（なりすましメールの送付等）のために利用する可能性があります。

同様に、スマートフォンのカメラでむやみに社内を撮影したり、その写真を SNS に掲載したりしないようにしましょう。撮影者が気付いていないところで、撮影してはいけない機密事項が写っているかもしれません。

➤ インターネットサービスの特性を理解して使う

インターネットには様々なツールが公開されており、これらをうまく使うことで仕事の効率化や簡便化を図ることができます。しかしながら、こういったツールの利用には注意が必要です。例えば、海外の取引先から送られてきた英文メールを理解するために翻訳サイトにメールの内容をそのまま入力すると、その内容が翻訳サイトに全て送られてしまうことになります。同様に、オンラインのグループサービスを使用してメンバー間のメールや情報を交換したり、スケジュール管理サイトに自身の予定や顧客との打ち合わせに関する情報を掲載したりすることも、情報漏えいにつながる可能性を秘めています。また、一部サービスでは登録した情報が一般に公開、共有できる場合があり、特に初期状態が一般公開する設定となっているサービスは登録した情報が第三者にも閲覧されてしまう可能性があります。

とはいえ、このような便利なツールを使わない手はないので、社内ポリシーで外部サービスの利用が許可されているか確認の上で、情報がどのように扱われるのか、どこまで第三者に公開されるのか、サービスの設定は初期状態で適切なのかなど、サービスの特性を事前に確認し、情報を入力する場合は固有名詞や日時情報を削ったり、別の文字に置き換えたりするなどの配慮をした上で利用するようにしましょう。

■ 教育担当者・システム管理者の方へ

ブログや SNS、地図ツールなどのインターネット上のサービスを業務で利用する場合は、企業側において各サービスの利用方法に関するルールやマニュアルを組織的に整備することが必要でしょう。また、このような問題は、フリーソフトの利用においても発生する可能性があります。フリーソフトの利用についても、使用してよいソフトウェアの周知や制限を行うなどの対策を行いましょう。

➤ SNS で他者を誹謗中傷しない

インターネットの匿名性という点を悪用して誹謗中傷する行為が後を絶ちません。いわゆる「炎上」や「祭り」というような多くのネットユーザの関心を引く状態になった場合、SNS 等に公開された情報などから誹謗中傷を行ったユーザが割り出され、個人だけではなく個人が所属する組織に対する過剰なまでの抗議行動が発生する場合があります。匿名で利用している SNS だから大丈夫と考えて、安易に他者を誹謗中傷した結果、自分のみならず、所属する組織の信頼に傷をつける可能性もあります。そもそも、他者を誹謗中傷する行為は道義的に許される行為ではありませんので、社会人としてそういった行為は慎みましょう。

➤ 電子メールの添付ファイルの取り扱いには気を付ける

電子メールは送信元の表示を偽ることが容易なため、たとえ送信元として表示されている人が信頼できる相手であったとしても、その電子メールが本人から送付されたものである保証はありません。特に最近では、企業の知財等の窃取をもくろんで、知人や取引先などをかたってメールを送りつける標的型攻撃が多発しています。

このため、添付ファイル付きの電子メールの取り扱いには細心の注意を払う必要があります。電子メールの件名や本文等から不審に感じる場合には、安易に添付ファイルを開かずに、送信者に確認したり、情報セキュリティ担当者に相談したりするなど、慎重に対応しましょう。

➤ 安全なパスワードの作り方を知る

パスワードは様々なサービスのユーザ認証に使われています。サービスやシステムごとに異なるパスワードを管理するのは確かに煩雑ですが、あらゆるサービスに同じパスワードを利用していると、万が一あるサービスを利用するためのパスワードが漏えいした場合、すべてのサービスの利用が危険に曝されてしまうため、使い分けを検討する必要があります。実際 2013 年には、何らかの方法で入手した大量のユーザ ID とパスワードの組み合わせのリストを使用し、オンラインサービスに不正にログインを試みる「パスワードリスト攻撃」と言われる攻撃が発生しています。もっとも、多数のパスワードを管理しなければならないために、各パスワードが覚えやすい推測可能な安易なものになってしまうとパスワードを設定する意味がなくなってしまうので、用途に応じた適切な設定を心掛けましょう。

安全なパスワードの作り方のポイントを以下に示します。

- 電話番号や誕生日など、個人情報を基にした文字列は使用しない
- 単語をそのまま使用しない（辞書単語、固有名詞など）
- ユーザアカウントと同じ文字列を含めない
- アルファベットの大文字、小文字、数字、記号を混ぜる
- パスワードの長さは8文字以上が望ましい
- 複数のサービスで同じパスワードを使い回さない

ここまで条件があると、どのようにパスワードを作成したらいいのか分からないという人も多いかと思います。以下に一例を示しますので、覚えやすく強度の高いパスワードの設定を心掛けてください。

1. 8文字以上で自分が覚えやすい文字列を考える（記号・数字が入るとよい）
例) securinu#02
2. 一部を意図的に大文字に置き換える
例) secUriNu#02
3. 単語を使う場合、意図的に誤植（自分で覚えやすいもの）を含める
例) seQriMu#02

自分が忘れさえしなければ、変換ルールは独自のものがかまいません。一般的には、**S**と**\$**記号の入れ替え、**0**（ゼロ）と**O**または**o**（オー）の入れ替え、**1**（いち）と**l**（エル）の入れ替え、**2**と**Z**（z）の入れ替えなどが使われますが、あまり一般化されたルールだと想像されやすくなります。これらをうまく組み合わせて、パスワード条件を満たす文字列を考えましょう。

なお、以下のサイトで、作ったパスワードの強度を確認することができます。

Microsoft パスワードのチェックーパスワードは強力か？

<https://www.microsoft.com/japan/protect/yourself/password/checker.mspix>

2 インシデント発生時における基本的な対応

教育担当者・システム管理者の方へ

どんなに情報セキュリティ対策を実施してもインシデントが発生する確率を 0%にすることはできません。インシデントが発生してから、被害の拡大防止のための対応方法の調査、検討を始めるようでは、その間にも会社の情報が漏えいし続けたり、社内システムへのウイルス感染が拡大し続けたりして、取り返しのつかない事態を招いてしまいます。平時から、インシデントが発生した場合に各社員や担当部署が誰に報告し、どのような対応を取るべきかなどのルールを定め、周知しておくことが重要です。

新入社員は、社内のシステムの平時の状況に関する知識が少ないために、インシデント等の異常な事態が発生しても、そのことにすぐには気付かない可能性があります。また、仮にインシデントの発生に気が付いても、正しい対処方法を理解していないため、必要な関係部署への連絡が遅れ、結果的に被害が拡大してしまうことが懸念されます。

ここでは、新入社員が理解しておくべき、インシデントへの一般的な対応手順をまとめました。併せて、セキュリティ担当者が取るべき一般的な対応についても整理していますが、重要なことは、企業や組織のポリシーに従ったインシデントへの対応方法や報告ラインなどが組織として整備されていること、及びそれを新入社員に理解させ、実践させるための手段が整えられていることです。この機会に、自社のインシデント対応ポリシー及びその周知、徹底の方法に問題がないか（組織の実態に合わないものになってしまっていないか等）、確認されることを推奨します。

2.1 インシデントの発生に気が付いた時、まずどうすればよいのか

(1) 冷静に、どんな異常なことが起きたのかを把握する

まず、落ち着きましょう。冷静さを失ってしまったために、インシデントの被害や影響範囲が拡大してしまうこともあります。落ち着いて、どのような「普段と違う異常なこと」が発生していて、(可能であれば) 今どのような状況なのかを把握しましょう。分かる範囲でメモを取りましょう。その際、時刻情報を含めて記録することが重要です。

(2) 手順の確認

セキュリティポリシーや対応マニュアルにより、既に対応手順がルール化されている場合は、その内容に従いましょう。非常時に備え、セキュリティポリシーや対応マニュアルなど必要な資料は、事前に内容を確認しておき、すぐに参照できるようにドキュメントの保管場所を覚えておきましょう。

(3) 責任者、担当者への連絡

セキュリティポリシーや対応マニュアルなど事前に定められた連絡手順に従い、組織内の責任者やインシデント対応チーム (CSIRT) などの担当者に連絡し、その後の対応について指示を仰ぎましょう。

教育担当者・システム管理者の方へ

新入社員など、何が危険なのかがよく分かっていないような場合には、「分からなければ、放置しないでまず報告」という方針を徹底させましょう。

(4) 作業記録の作成

時刻情報を含める形で、自分が実施した作業や判断の内容を可能な限り記録しましょう。また、対応マニュアルに従って自分でインシデント対応作業を実施した場合には、以下の項目を記録しましょう。これらの作業記録は、インシデント対応作業手順を後日評価するために使えるだけでなく、作業中に副次的に障害が発生した場合などには、作業手順のポリシーなどを見直すための重要な資料となります。

- インシデントの発見、発生日時
- 発見者（通報者）
- インシデントの内容
- インシデントと疑った理由
- インシデントの発生直前から報告するまでに行った作業

2.2 セキュリティ担当者が取るべき一般的な対応

このセクションの内容は、本来セキュリティ担当者が取るべき対応についての解説になりますが、インシデント対応フローの全体像を一般社員が把握しておくことも有効であるため、参考までに紹介します。なお、以下のフローは、あくまでも一般的に想定されるインシデント対応フローであり、実際には各企業に最適化されたフローが定められていると考えられますので、あくまでも参考事例であることに留意してください。

インシデントが発生した部署からの報告を受けたセキュリティ担当者は、一般的には、以下のような手順でインシデントへの対応を進めます。

(1) 事実の確認

どのようなインシデントが起こっているのか、事実関係や影響範囲などを確認します。場合によっては、発見者・報告者へのヒアリングも行います。

(2) ネットワーク接続の遮断やシステムの停止

被害が拡大する恐れがある場合には、経営層や関連部署と連携をとりながら、ネットワークやシステムの全体もしくは一部を遮断または停止するといった対策を検討する必要があります。さらに、この後の調査等に備え、システムの状態を保存（記録）することも必要になります。

(3) 要因の特定と対応方針の検討

インシデントが発生した要因（原因）を特定し、特定した要因に対して、どのような対策（インシデントの拡散や二次被害の防止策の検討を含む。）が可能か検討します。インシデントの要因の排除や対策のために、攻撃元その他の第三者に対して調整を行う必要がある場合には、JPCERT/CC に報告して、攻撃元やインシデントの原因となっているサイト等に対する調整等の対応を依頼することができます。

(4) システムの復旧

インシデントの要因を特定し、排除したら、システムの復旧を図ります。システムへの

侵入により管理者権限を奪われた場合や、何らかの改ざんやデータの破壊が行われた場合には、ウイルス対策ソフトなどでは検知できないマルウェアが組み込まれている可能性があるため、復旧に当たっては、障害を取り除いたシステムを単に再稼働するのではなく、他に影響が残っていないか詳細を調査しましょう。もし、詳細な調査が困難な場合は、データのバックアップをとった上で OS の再インストールからのシステムの再構築についても検討してください。

事業継続性を考慮し、代替機を用意して、インシデントが発生しているシステムと一時的に置き換える等の運用も有効です。ただし、ネットワーク上の問題や脅威が排除されない状態での復旧は、同じ問題を繰り返すことになりかねないので、ある程度の原因究明や一定の対策と併せて行います。また、代替機を急ぎょ用意するような場合は、インストールされているソフトウェアのアップデート状況、ハードウェアの動作状態も確認する必要があります。

(5) 作業結果の報告

作業終了後、各フェーズにおける記録に基づいて、インシデントの影響範囲や対応全般の作業内容、作業にかかったコスト（時間、費用など）、損失（確認された範囲内で）、対応において発見した課題や問題点をまとめ、責任者に報告します。

(6) 作業の評価、ポリシー・運用体制・運用手順の見直し

作業報告に基づいて、必要に応じ、情報セキュリティ対策の運用に関するポリシー等の見直しを行います。また、これまでの運用体制や運用手順、更に実際に行ったインシデント対応作業に問題がなかったかどうかを確認します。

JPCERT/CC では、企業等において発生したコンピュータセキュリティインシデントに関し、当該企業等からの報告（依頼）に基づき、事態の把握や解決策の検討、被害の拡大抑止等を支援するため、国内外の関係機関と連携して、攻撃元への調整等の対応支援活動を行っています。また、国内外におけるインシデントの事例を収集し、同様の被害が拡散しないよう注意喚起等の啓発活動を行っています。

JPCERT/CC が行っているインシデント対応支援活動は、以下のページで紹介しています。

はじめての JPCERT/CC(インシデント対応)

<https://www.jpCERT.or.jp/about/brief/page1.html>

JPCERT/CC へのインシデント報告（インシデント対応調整依頼）は、以下のページから行うことができます。

JPCERT/CC インシデントの報告(Web フォーム)

<https://form.jpccert.or.jp/>

おわりに

この文書は、新入社員の入社が多く、情報セキュリティインシデントが発生しがちなこの時期に、企業や組織の教育担当者や情報セキュリティ担当者に向けて、組織内の PC の利用に関する注意点を中心に、新入社員教育を行う場合の参考になることを期待して公開するものです。

併せて、この時期に各組織の情報セキュリティポリシーやインシデント対応ポリシーその他の情報セキュリティに関する社内ルールの点検や、社内への周知状況を再確認いただく契機になることを期待しています。

情報セキュリティ上の脅威は、日に日に変化するものであり、いったん定めた情報セキュリティに関するポリシーやルールがいつまでも有効であるというものではありません。また、各企業の業務実施のための IT 利用の実態も変化するでしょうから、定期的なポリシーの見直しは不可欠であるといえます。この機会に、セキュリティ対策やインシデント発生時の対応に関する社内ルールの見直し、周知の確認を行われてはいかがでしょうか。

参考文献・資料

- (1) JPCERT/CC
CSIRT マテリアル
https://www.jpcert.or.jp/csirt_material/
- (2) JPCERT/CC
はじめての JPCERT/CC インシデント対応
<https://www.jpcert.or.jp/about/brief/page1.html>
- (3) JPCERT/CC
インシデントの報告
<https://www.jpcert.or.jp/form/>
- (4) JPCERT/CC
技術メモ コンピュータセキュリティインシデントへの対応
<https://www.jpcert.or.jp/ed/2002/ed020002.txt>
- (5) JPCERT/CC
初心者のためのセキュリティー講座 インターネットでの不正行為その傾向と対策
<https://www.jpcert.or.jp/magazine/security/im9801jc.pdf>
- (6) JPCERT/CC
技術メモ 安全な Web ブラウザの使い方
https://www.jpcert.or.jp/ed/2008/ed080002_1104.pdf
- (7) JPCERT/CC
電子メールソフトのセキュリティ設定について
<https://www.jpcert.or.jp/magazine/security/mail/index.html>
- (8) 総務省
国民のための情報セキュリティサイト 事故・被害の事例
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/index.html
総務省
国民のための情報セキュリティサイト サーバー証明書
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security_previous/yougo/sa_gyou.htm
- (9) 一般財団法人日本データ通信協会(JADAC)
迷惑メール対策推進協議会 迷惑メール対策ハンドブック
http://www.dekyo.or.jp/soudan/anti_spam/report.html#hb
- (10) 独立行政法人情報処理推進機構(IPA)
2005年 企業における情報セキュリティ事象被害額調査報告書
http://www.ipa.go.jp/security/fy17/reports/virus-survey/documents/2005_model.pdf

- (11) 独立行政法人情報処理推進機構(IPA)
電子メールのセキュリティ S/MIME を利用した暗号化と電子署名
http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.pdf
- (12) 独立行政法人情報処理推進機構(IPA)
PKI 関連技術解説
<http://www.ipa.go.jp/security/pki/index.html>
- (13) 独立行政法人情報処理推進機構(IPA)
コンピュータウイルス・不正アクセスの届出状況[4月分]について
「USB メモリのセキュリティ対策を意識していますか？」－ USB メモリの安全な使い方を知ろう
<http://www.ipa.go.jp/security/txt/2009/05outline.html>
- (14) 電子認証局会議(CAC)
電子署名活用ガイド
<http://www.c-a-c.jp/download/index.html>
- (15) フィッシング対策協議会
フィッシングとは
https://www.antiphishing.jp/consumer/abt_phishing.html
- (16) 特定非営利活動法人日本ネットワークセキュリティ協会」(JNSA)
2008年 情報セキュリティインシデントに関する調査報告書
http://www.jnsa.org/result/2008/surv/incident/2008incident_sruvey_v1.3.pdf
- (17) 特定非営利活動法人日本ネットワークセキュリティ協会」(JNSA)
セキュリティ被害調査ワーキンググループ、情報セキュリティ大学院大学 原田研究室 廣松研究室
2011年 情報セキュリティインシデントに関する調査報告書
http://www.jnsa.org/result/incident/data/2011incident_survey_ver1.2.pdf
- (18) NTT 技術ジャーナル 2006 vol.18 No4 (日本電信電話株式会社)
技術基礎講座【NTT-CERT Security Tips】第6回インシデントへの対応
<http://www.ntt.co.jp/journal/0604/files/jn200604068.pdf>
- (19) 日本マイクロソフト株式会社
安全性の高いパスワードの作成
<http://www.microsoft.com/japan/protect/yourself/password/create.mspx>
- (20) 日本マイクロソフト株式会社
パスワードのチェッカーパスワードは強力か？
<https://www.microsoft.com/japan/protect/yourself/password/checker.mspx>
- (21) 日本マイクロソフト株式会社
Windows Update 利用の手順
http://www.microsoft.com/japan/security/bulletins/j_musteps.mspx

- (22) 日本マイクロソフト株式会社
Windows の自動実行機能を無効にする方法
<http://support.microsoft.com/kb/967715/ja>
- (23) 日本マイクロソフト株式会社
Internet Explorer の保護モードの機能
<http://windows.microsoft.com/ja-JP/windows-vista/What-does-Internet-Explorer-protected-mode-do>
- (24) アップルジャパン合同会社
Mac OS X 10.6 のコンピュータの画面をロックする
http://support.apple.com/kb/PH6895?viewlocale=ja_JP
- (25) アドビシステムズ株式会社
Acrobat 9.1/Adobe Reader 9.1 アップデートインストール手順 (Windows)
<http://kb2.adobe.com/jp/cps/235/235294.html>
- (26) 日本オラクル株式会社
無料 Java のダウンロード(JRE 7、日本語)
<http://java.com/ja/download/>
- (27) 株式会社ジャストシステム
JUST オンラインアップデートの使い方
<http://support.justsystems.com/faq/1032/app/servlet/qadoc?QID=043657>

文書の引用・転載・再配布について

- 文書の引用は自由に行っていただけます。

引用に際しては、引用元名、資料名、URL を明示していただけるようお願いいたします。
また、引用をしていただく際は、お手数をおかけして恐縮ですが、引用先文書、時期、内容等の情報を JPCERT/CC 広報 (office@jpcert.or.jp) までメールにてお知らせいただけるよう、ご協力をお願いいたします。

[記載例]

引用元: JPCERT コーディネーションセンター

「新入社員等研修向け情報セキュリティマニュアル Rev.3」

<https://www.jpcert.or.jp/magazine/security/newcomer.html>

- 転載、再配布に当たっては、転載・再配布先、時期、内容等の情報を JPCERT/CC 広報 (office@jpcert.or.jp) までメールにてご連絡ください。