マンガで知ろう

企業向け

情報セキュリティ対策マニュアル

マンガで知ろう

企業向け 情報セキュリティ対策マニュアル

目次

CONTENTS

ポリス まろん　　ポリス みやこ

京都府警察シンボルマスコット

会社の状態を知ろう

自社診断チェックシート

チェックシートにより自社の状態を知れば、問題点が見えてきます。
チェックをした上で、３つのマンガをお読みください。

Check Sheet

独立行政法人情報処理推進機構（IPA）資料を参考に作成

Q1	パソコンにはマルウェア※1対策ソフトを入れるなど、パソコンを守る対策をしていますか？	□はい □いいえ
Q2	OS（基本ソフト）のアップデートを行うなど、常にソフトウェアを最新の状態にしていますか？	□はい □いいえ
Q3	重要情報※2の入ったデータを暗号化したり、複雑なパスワードで管理するなどの対策をしていますか？	□はい □いいえ
Q4	重要情報の入ったデータのバックアップを定期的に実施したり、インターネットと直接やりとりしないパソコンで管理するなどの対策をしていますか？	□はい □いいえ
Q5	件名や内容が不自然なメールの添付ファイルやURLをむやみにクリックせず、送信者に確認するなどの注意を払ったり、メール等認証技術を導入するなどの対策をしていますか？	□はい □いいえ
Q6	情報管理の大切さを定期的に教養するなど、従業員に意識付けをしていますか？	□はい □いいえ
Q7	重要情報の持ち出し制限を設けるなど、情報に関するルール作りをしていますか？	□はい □いいえ

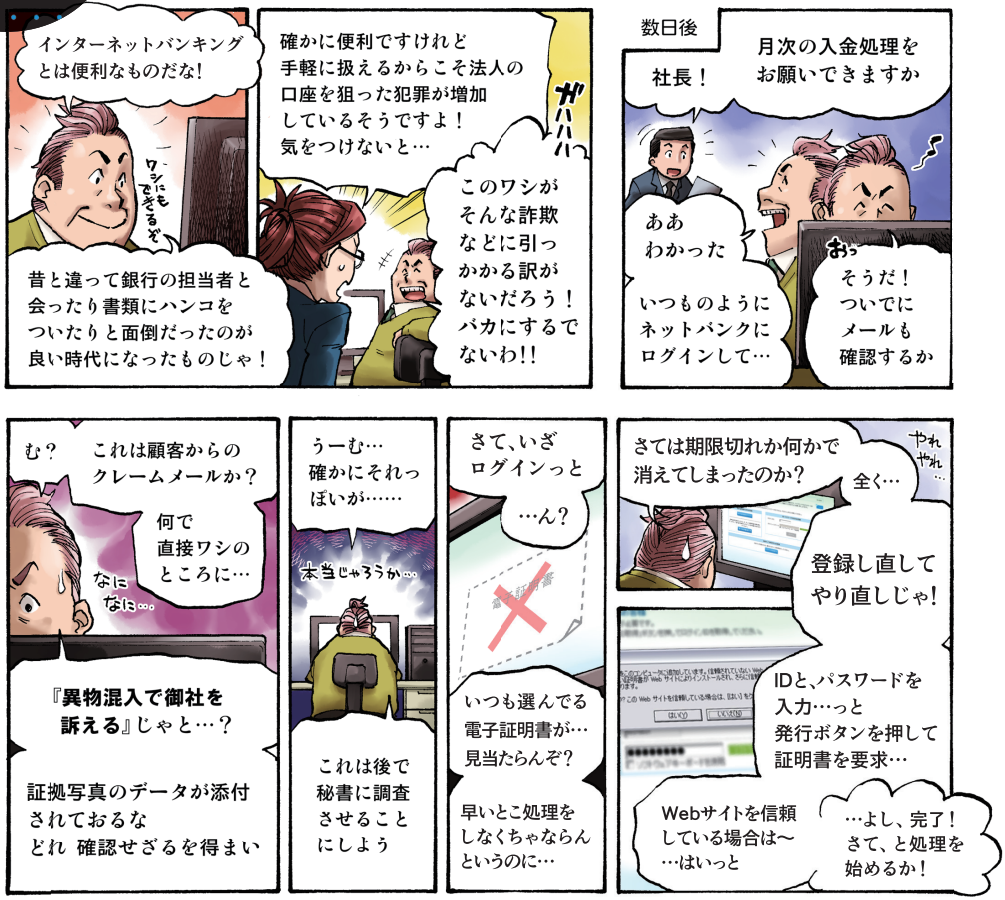
※1　**マルウェア**とは、ウイルスのみならず、不正にパソコンを操作するバックドアなどのスパイウェア、強制的に広告を表示するアドウェア、嘘の情報で購入を促す偽セキュリティ対策ソフトなど、コンピュータの利用者が意図しない動作をする不正なプログラムの総称

※2　**重要情報**とは、その情報が漏えいしたことによりビジネスに打撃を与えたり、組織の信頼失墜につながる情報、主に顧客情報、職員名簿、設計図面、開発スケジュール、仕入単価、取引額等がこれに当たります

問題点を把握してマンガを読み、解説を参考によりよい情報セキュリティ対策を講じましょう。

マンガで知ろう

その1・インターネットバンキングでの被害



その1 インターネットバンキングでの被害

解説

インターネットバンキングの口座から不正に他の口座に送金する被害が急増しています。警察庁の調べによると平成24年には約4800万円だった被害額が、平成25年に約14億600万円、平成26年には約29億1000万円に達しています。最近は法人口座が多く狙われており、平成26年では被害額のうち約10億8800万円が法人口座からの不正送金です。

インターネットバンキングからの不正送金被害は、**ほとんどがマルウェアかフィッシング**が原因です。**マルウェア**は、メールやWebサイトを通じてパソコンに感染し、遠隔操作したり、パスワードや乱数表、電子証明書などの認証情報を盗み取ったり、Webブラウザを乗っ取るなどして口座を自由に操作してしまいます。**フィッシング**はメールを使って偽のホームページに誘導し、同様にパスワード等を盗み出そうとする手口です。

対策

金融機関が勧めるセキュリティ対策に従いましょう

信頼できるマルウェア対策ソフトの導入や、金融機関が提供するセキュリティソフトの導入などが勧められていますので、それに従ってください。また、多くの金融機関が呼びかけている通り、公式サポートの終了したOSの継続使用は不正利用被害の危険が高まりますので避けましょう。

いつもと違う操作画面が出ていないか気を付けましょう

マルウェアは認証情報を盗み出すためにいつもと違う操作を利用者に求めてくることがあります。操作の画面が普段と違っていたら、マルウェアの感染を疑ってください。金融機関のWebページによくあるマルウェアの手口が紹介されていることがありますので、そちらを見たり、不安であれば金融機関に電話などで問い合わせてもよいでしょう。

マルウェア対策をしましょう

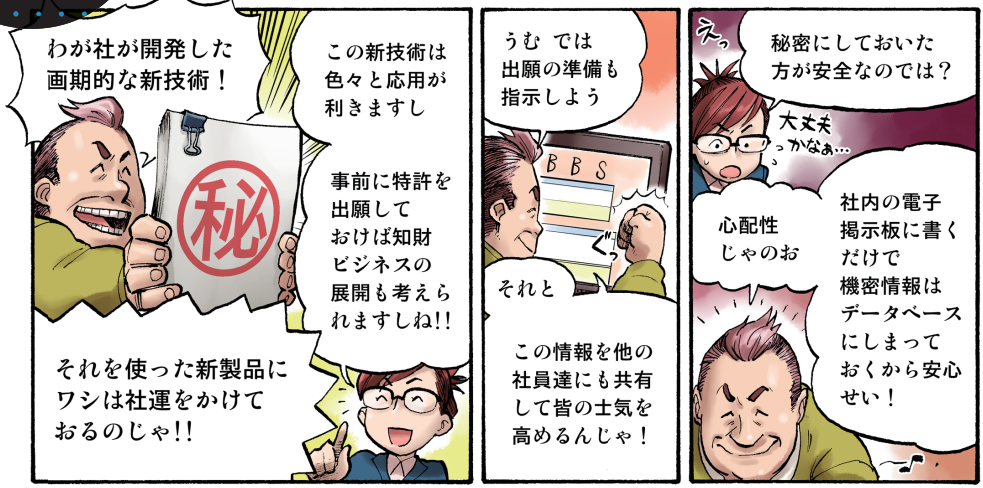
OSやソフトウェアを常に最新に保つため、更新のお知らせが来たらすぐに対応しましょう。マルウェア対策ソフトも、必ず導入してサポートを受けましょう。また、インターネット上で無料配布されているソフトウェアの中にはマルウェアが含まれることがあります。心配であれば店頭で売っているソフトを利用しましょう。

インターネットバンキングは専用の機器で

インターネットバンキング専用のパソコンを用意してセキュリティ関係のソフトウェアのみを導入し、ほかのサイトの閲覧やメールの読み書きには使わないようにするとよいでしょう。マルウェア感染の危険が減らせます。

マンガで知ろう

その2・知的財産の被害



その2 知的財産の被害

解説

このところ、公共機関や企業を狙ったサイバー攻撃の被害が増えています。かつてのサイバー攻撃は技術の誇示を狙った愉快犯が多かったのですが、最近では組織内の**パソコン内のファイルなどの情報を密かに盗み取り、外部に送信する**例が増えてきました。これらの情報の中には企業にとって大切な個人情報や知的財産が多く含まれています。こうして集められた情報は、闇市場で売買されたり、海外の諜報機関に提供されたりしているとみられています。

多くのサイバー攻撃の発端は**標的型攻撃**と呼ばれるマルウェアの送り込みです。標的型攻撃では、漫画にもあるような「経営者必見！」などといった、**思わず開いてしまうような営業や情報提供を装ったメール**が多く使われます。**同じ組織の従業員や管理職に成りすまされる**例も多いので細心の注意が必要でしょう。しかも標的型攻撃で使われるマルウェアは、マルウェア対策ソフトウェアでは検出されにくいものです。また、**不正アクセス**による例も少なくありません。Webサーバやメールサーバなどインターネットに**直接接続されたサーバは特に不正アクセス対策が重要となります**。

対策

侵入したマルウェアの早期発見が重要です

インターネットバンキング被害での対応と同様のマルウェア対策は一定の効果がありますが、標的型攻撃の場合には完全に防ぐことは困難です。パソコンが普段と違う挙動をするようなら、マルウェア被害を疑ってみてください。可能であれば、外部への不審な通信がないか調べてみましょう。専門のセキュリティ業者に早めに相談することも必要でしょう。

重要な情報は多重に保護しましょう

たとえば重要な情報を含むファイルは暗号化したり、インターネットと直接やりとりしないパソコン等で処理するようにしたりすることは効果があります。暗号化の際のパスワードも複雑なものにして厳重に管理してください。

メールのなりすまし対策をしましょう

せめて自組織の従業員などに成りすまされないよう、メールのなりすまし対策技術を導入しましょう。DKIM※やSPF※といったドメイン認証、S/MIME※などメール認証の技術の導入を検討してください。取引先でも同様の対策が広がれば、その組織とのメールに関しては必要以上に用心する必要はなくなります。

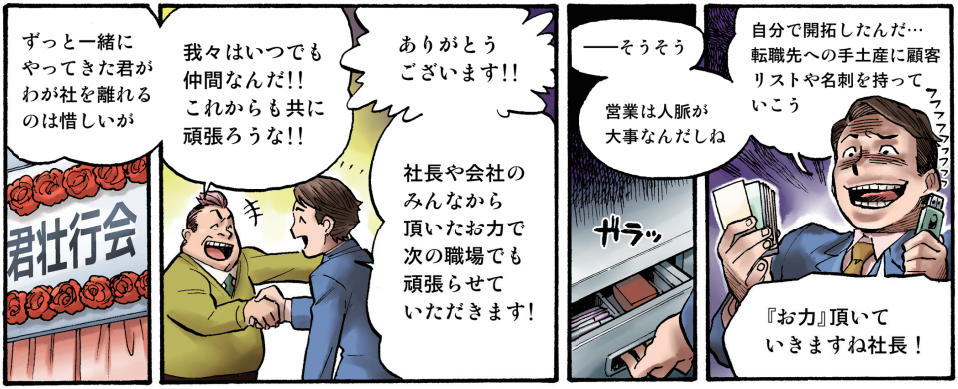
不正アクセス対策をしましょう。

普段利用するパソコンにはファイアウォールなどの対策が必須です。インターネットと直接やりとりするサーバに関しては、ソフトウェアを常に最新に保つことなどの脆弱性対策を行ってください。

注※　DKIM, SPFはどちらもメールが確かにその組織から送信されたことを証明する技術です。S/MIMEはメールの送信者アドレスと内容が正しいことを証明できる技術です。

マンガで知ろう

その3・組織における内部不正



その3 組織における内部不正

解説

我が国でこれまで発生した大量の**情報漏えい事件の多くは内部犯行によるものです**。特に、業務委託先の従業員や退職者による情報持ち出しの例が多く報告されています。平成11年に発覚した自治体の住民基本台帳漏えい事件や、平成26年に大きな話題となった通信教育事業者からの個人情報漏えいも、業務委託先から持ち出されたものでした。また平成26年1月には、退職者が元の勤務先のパソコンにあらかじめ仕込んでおいた遠隔操作ソフトウェアを操作して顧客情報を持ち出し、新しい勤務先での営業に転用するという事件が起きています。

（独）情報処理推進機構による「組織における内部不正防止ガイドライン」では、内部不正防止の基本原則として**「犯行を難しくする」「捕まるリスクを高める」「犯行の見返りを減らす」「犯行の誘因を減らす」「犯行の弁明をさせない」**を挙げています。この原則に沿って業務の進め方を見直していくことが必要です。

また、情報漏えい防止のための**法の整備**も進んでいます。平成27年、不正競争防止法が改正され、顧客名簿や技術情報などを含む営業秘密の不正な持ち出しに対して、被害に対する原告の立証責任が軽減されたほか、被害自体が発覚した時点から警察が行動できるよう非親告罪とされました。

対策

情報の管理についてルール化を進め、従業員に意識付けをしましょう

重要な情報に関しては、それが利用できる従業員をあらかじめ制限したうえで、社外への持ち出しに対し報告を義務付けるなどルール化を進めましょう。従業員教育も随時行い、意識付けを徹底するようにしてください。さらに、内規や法に基づく罰則についても教育しておくと大きな抑止力になります。内部犯行の通報窓口の整備なども有効でしょう。

情報が管理しやすい情報システムを導入しましょう

情報管理の徹底と働きやすさを両立するためには、ICTをうまく活用することが重要です。情報を重要度に応じた格付けを行い、バックアップなどが必要な管理をした上で、各従業員の権限に応じてアクセス制限や持ち出し制限などが行われれば、投資に見合う業務効率の向上とセキュリティの両立が達成できるでしょう。

業務委託時には事故抑止に注意しましょう

業務委託先で情報の持ち出しや紛失が発生した場合の責任の所在や範囲などをあらかじめ契約条件に明記しておきましょう。また、作業の際に業務委託元の従業員の立ち合いなどの監視を行うことは大きな抑止力となります。

アクセス権限の管理はしっかりと

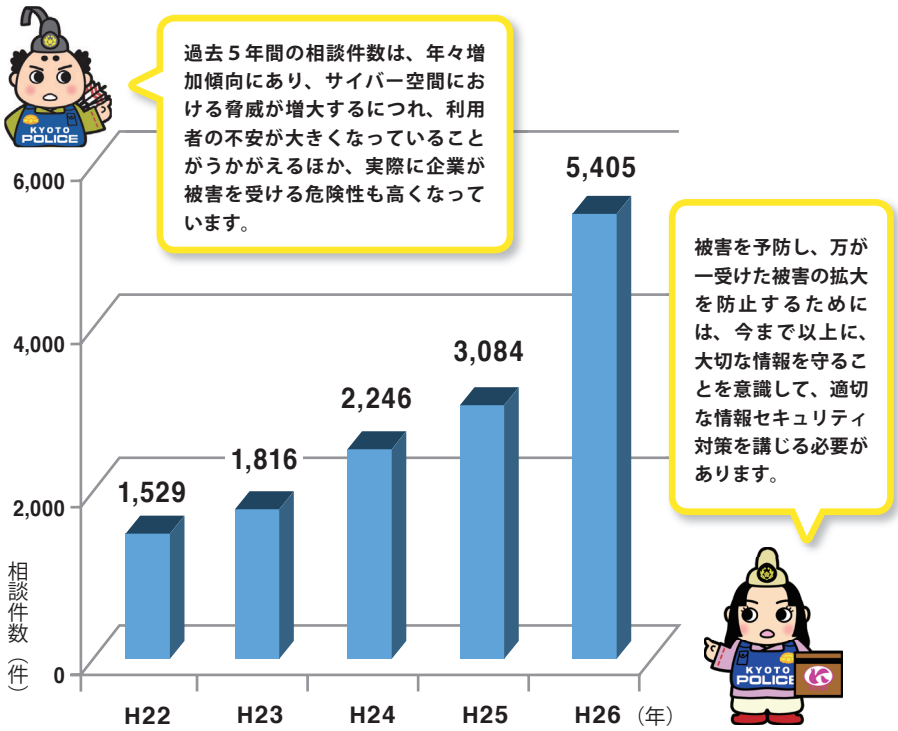
退職者が出た時や業務委託契約が終了したときなどは、パスワードの変更など、すでにアクセス権がなくなった人がアクセスの方法を知ったままになっていることのないように注意してください。

グラフで知ろう

京都府警察に寄せられた

サイバー犯罪相談件数推移

■サイバー犯罪相談件数推移（平成22年～平成26年）　※情報提供を含む



顧客の信頼を損なわないために

まずは基本的な備えから‼

聞いて知ろう

企業向け 各種相談窓口一覧

情報セキュリティ対策に関する相談

例 情報セキュリティ対策・情報漏えい・情報流出等

京都中小企業情報セキュリティ支援ネットワーク（Ksisnet）
IT 相談窓口（公益財団法人京都産業 21 お客様相談室）

URL: http://www.ki21.jp
Email: okyaku@ki21.jp　TEL: 075-315-8660

特許等知的財産に関する相談

例 発明、考案、意匠、商標等の産業財産権に関するもの

京都府知的財産総合サポートセンター（一般社団法人京都発明協会）

URL: http://kyoto-hatsumei.com/
Email: hatsumei@ninus.ocn.ne.jp　TEL: 075-326-0066　FAX: 075-321-8374

マルウェア、不正アクセス等に関する技術的相談・報告先

例 ウイルス、不正アクセス、ウェブサイト改ざん、標的型メール攻撃等に関する技術的なもの

独立行政法人情報処理推進機構（IPA）情報セキュリティ安心相談窓口

URL: https://www.ipa.go.jp/security/anshin/index.html
Email: anshin@ipa.go.jp　TEL: 03-5978-7509　FAX: 03-5978-7518

一般社団法人JPCERTコーディネーションセンター

URL: https://www.jpcert.or.jp/form/
Email: info@jpcert.or.jp　TEL: 03-3518-4600　FAX: 03-3518-2177

犯罪に関する相談・情報提供

例 サイバー空間におけるトラブル・サイバー犯罪に関するもの

京都府警察

URL: http://www.pref.kyoto.jp/fukei/anzen/seiki_h/cyber/cyber06.html
TEL: 075-451-9111（代表）

京都府警察スローガン

千年を守る　未来を創る

作　　画：キノシタ ヒロシ（京都精華大学マンガ学科卒）
企画・制作：IT コンソーシアム京都
上原哲太郎（立命館大学情報理工学部教授）
中山貴禎（株式会社アズジェント）
京都精華大学事業推進室
独立行政法人情報処理推進機構（IPA）
一般社団法人 JPCERT コーディネーションセンター
京都府警察本部
協　　力：京都府
京都市

使用における注意事項

平成27年10月制作