平成２９年７月

企業と組織の
ネットトラブル
対応マニュアル

鳥取県サイバーセキュリティ対策ネットワーク

パソコン使用時の突然のネットトラブル、先ずは何をするべきかをご説明します。

　標的型メール、ランサムウェア・・・
　こうしたネットトラブルをテレビニュースや新聞記事で目にする機会が増えてきました。
　このマニュアルでは、企業や組織のパソコンでネットトラブルが発生した時、先ず何をすればよいかを単純明快＆コミカルにご案内します。

もくじ

情報セキュリティ対策チェックシート

- 事情に照らし合わせて、以下の項目をチェックしてください。
- チェック終了後は、裏面の説明をご覧ください。

チェック①
- ☐ WindowsUpdateを行うなど、常にソフトウェアを最新状態にしていますか

チェック②
- ☐ 組織内外で個人パソコンの業務使用を許可制にするなど、業務で個人所有パソコンを使用することの是非を明確にしていますか

チェック③
- ☐ パスワードを他人が見えるような場所に貼らないなど、第三者の目に触れないよう管理していますか

チェック④
- ☐ ログイン用のパスワードを定期的に変更していますか

チェック⑤
- ☐ パソコンにはウイルス対策ソフトを導入していますか

チェック⑥
- ☐ ウイルス対策ソフトを自動更新し、常に最新の状態を保っていますか

チェック⑦
- ☐ システムのバックアップを定期的に行っていますか

チェック⑧
- ☐ 情報管理の大切さを定期的に説明するなどのように、職員（従業員）に意識付けを行っていますか

チェック⑨
- ☐ 重要情報の流出や紛失、盗難があった場合の対応手順書を作成するなどの事故が発生した場合に備えた準備をしていますか

チェック⑩
- ☐ 組織のルールに情報セキュリティ対策に関する事項が含まれているなど、情報セキュリティ対策の内容が明確化されていますか

このチェックシートは、
独立行政法人情報処理推進機構(IPA)
「５分でできる！ 自社診断シート」を参考にして
鳥取県サイバーセキュリティ対策ネットワークが
作成したものです。

チェックできない項目がある場合は、セキュリティ対策について不十分な点があるようです。
裏面の解説やマニュアル関連ページを参考にして
改善やステップアップを検討しましょう。

☆ セキュリティ対策に対する社内の意識調査
☆ 組織内教養の効果を図る簡易測定ツール
　として、繰り返しご活用いただくことをおすすめします。

鳥取県サイバーセキュリティ対策ネットワーク

● 該当しなかった項目を中心に、改善ポイントを検討しましょう。

① WindowsUpdateを行うなど、常にソフトウェアを最新状態にしていますか

端末を安全な状態に保つために、OS(基本ソフト)や端末にインストールされている各ソフトウェアのバージョンを最新のものへ更新しましょう。
ソフトウェアのバージョンが最新であるかを確認するツールも公開されています。

② 組織内外で個人パソコンの業務使用を許可制にするなど、業務で個人所有パソコンを使用することの是非を明確にしていますか

個人のパソコンを業務に使用したために、自社や取引先の端末がウイルスに感染してしまったり、会社のオンラインバンクが不正送金被害に遭ってしまった事例もあります。
機密情報の持ち出しなどのリスクも含め、個人パソコンの業務使用に関するルールを設けておく必要があります。

③ パスワードを他人が見えるような場所に貼らないなど、第三者の目に触れないよう管理していますか

不正アクセス被害や情報漏えいの大きな原因の一つは、不適切なパスワード管理です。
パスワードを書いた付箋をデスクやパソコンに貼ったり、パスワードをメモしたテキストファイルをインターネット端末内に保存することは、不適切な管理方法と言えます。

④ ログイン用のパスワードを定期的に変更していますか

登録していたパスワードが、何らかの原因で流出した場合、第三者に悪用される恐れがあります。 パスワードは定期的に変更し、複数のウェブサイトなどで同一パスワードを使い回さないことが大切です。

⑤ パソコンにはウイルス対策ソフトを導入していますか

端末内のウイルスチェックのほか、悪意のあるウェブサイトなどへのアクセスを防ぐ効果も期待できるため、必ず信頼できるウイルス対策ソフトを導入しましょう。
ただし、ウイルス対策ソフトだけを入れておけば安全とは言い切れません。
ソフトウェアの更新、ファイアーウォールの設置など複数の対策を行いましょう。

⑥ ウイルス対策ソフトを自動更新し、常に最新の状態を保っていますか

ウイルス対策ソフトのバージョンやウイルス情報を記録した定義ファイルが古いままだと十分な機能が果たせません。
新たなウイルスは、日々増え続けています。ウイルス対策ソフトの自動更新機能を有効化して、常に最新の状態を保ちましょう。

⑦ システムのバックアップを定期的に行っていますか

ランサムウェアなどによってファイルが開けなくなったり、機械の故障や誤操作などで情報が消失したりするリスクに備え、定期的にバックアップを行うなどの対策をしておきましょう。

⑧ 情報管理の大切さを定期的に説明するなどのように、職員（従業員）に意識付けを行っていますか

デジタルデータから紙媒体に至るまで、情報管理とは何か？守るべき情報とは何か？誰が管理するのか？など明確にして、組織の一人一人が把握しておく必要があります。
営業秘密など、情報管理が適切に出来ていなければ、トラブルとなったときに法律的に戦うことも難しくなる場合もあり、情報管理は組織全体で取り組むべき問題です。

⑨ 重要情報の流出や紛失、盗難があった場合の対応手順書を作成するなどの事故が発生した場合に備えた準備をしていますか

トラブルが発生したときの初期対応として誰が何をすべきか？どんな場合に、どこへ連絡するのか？組織幹部への報告事項は？被害回復の手順は？原因・被害規模調査依頼先は？公表の有無は？などを事前に取り決めておくなどして、被害、損害を素早く最小限に食い止める準備が必要です。

⑩ 組織のルールに情報セキュリティ対策に関する事項が含まれているなど情報セキュリティ対策の内容が明確化されていますか

情報セキュリティ対策とは「重要な情報を守る施策」ということです。
そして、組織の「情報資産」を守るための情報セキュリティ対策を具体的にまとめた社内ルールのことを「セキュリティポリシー」と言います。
組織の規模や業種に関わらず、セキュリティポリシーの策定を行っていない場合は、早期策定を検討しましょう。

内部不正・営業秘密漏えい対策チェックシート

● 内部不正・営業秘密漏えい対策の基本的な内容です。
各項目を参考にして、対策状況を確認してみましょう。

チェック①
- □ 内部不正の対策が経営者の責任であることを組織内外に示す「基本方針」を策定し、役職員に周知徹底していますか

チェック②
- □ 基本方針に基づき、対策を実施するためのリソースが確保されるよう、必要な決定、指示をしていますか

チェック③
- □ 経営者は、内部不正対策の総括責任者の任命及び管理体制と実施策の承認を行っていますか

チェック④
- □ 総括責任者は、基本方針に則り、組織横断的な管理体制を構築し、実施策を策定していますか

チェック⑤
- □ 重要情報を把握し、重要度に合わせて格付け区分し、取り扱い可能な内部者の範囲を定めていますか

チェック⑥
- □ 情報システムを管理・運営する担当者は、利用者ID及びアクセス権の登録・変更・削除等の設定手順を定めて運用していますか

チェック⑦
- □ 重要情報の格納場所や取り扱う領域等を物理的に保護するために、壁や入退室管理策によって保護していますか

チェック⑧
- □ 個人のモバイル機器及び記録媒体の業務利用及び持込み制限をしていますか

チェック⑨
- □ 組織のネットワークは、重要情報を不正に持ち出し可能なファイル共有ソフトやSNS、外部のオンラインストレージ等の使用を制限していますか

チェック⑩
- □ 重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を定めた期間に従って安全に保護していますか

チェック⑪
- □ システム管理者のアクセス履歴や操作履歴等のログ・証跡を記録して保存するだけでなく、そのログ・証跡の内容を定期的にシステム管理者以外が確認していますか

チェック⑫
- □ すべての役職員に繰り返して教育を実施し、組織の内部不正対策に関する方針及び重要情報の取り扱い等の手順を周知徹底していますか

チェック⑬
- □ 教育を徹底的に繰り返して実施し、教育内容を定期的に見直して更新していますか

チェック⑭
- □ 内部不正の影響範囲を特定するために、事象の具体的状況を把握し、被害の最小限化や影響の拡大防止策を実施し、必要に応じて組織内外の関係者との連携体制を確保していますか

チェック⑮
- □ 内部不正と思しき事象が発生した場合についての通報制度を整備し、通報受付を複数設置し、必要に応じて通報者の匿名性を確保していますか

※　このチェックシートは、独立行政法人情報処理推進機構(IPA)「組織における内部不正防止ガイドライン 付録Ⅱ：内部不正チェックシート」を参考にして鳥取県サイバーセキュリティ対策ネットワークが作成したものです。

内部不正・営業秘密漏えい対策Ｑ＆Ａ

Ｑ１

「基本方針」をどのように策定すればよいかわかりません。

Ａ１

社内での重要情報の保護・管理の徹底、及び社外への説明責任の観点から、以下の３項目を最低限定めましょう。

① 経営者は経営課題の一つとして、リスク管理を行う必要があることを認識しその一環として内部不正を防止し、重要情報を保護・管理することの重要性を示します。
② 保護・管理すべき重要情報を識別し、その重要情報に関して事業上の重要性を示します。重要情報とは、組織に大きな影響を与える情報です。
③ 重要情報の保護・管理に関する実施体制を策定し、見直しを行いつつ継続的な活動であることを示します。実施体制には、内部不正対策の実施上、整備すべき体制を記載し、最低限責任者を示すことが必要です。

Ｑ２

重要な情報にはどのような情報があるのかわかりません。

Ａ２

重要情報は、各部門の業務内容や取り扱う情報によって異なります。

例えば、営業部門であれば顧客情報や関係者限りの営業情報等になります。

また、開発部門であれば、開発物や設計書等が重要情報と考えられます。

Ｑ３

営業秘密とはどういう情報ですか。

Ａ３

【不正競争防止法第２条第６項】この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

技術やノウハウ等の情報が「営業秘密」として不正競争防止法で保護されるためには、以下の３要件を全て満たすことが必要です。

営業秘密の３要件

秘密管理性 秘密として管理されていること

営業秘密保有企業の秘密管理意思が、「社外秘」表示などの秘密管理措置によって従業員等に対して明確に示され、当該秘密管理意思に対する従業員等の認識可能性が確保される必要があります。

有用性 有用な営業上または技術上の情報であること

当該情報自体が客観的に事業活動に利用されていたり、利用されることによって、経費の節約、経営効率の改善等に役立つものであること。
現実に利用されていなくてもかまいません。

設計図、製法、製造ノウハウ
顧客名簿、仕入先リスト
販売マニュアルなど

非公知性 公然と知られていないこと

保有者の管理下以外では一般に入手できないこと。

刊行物等に記載された情報や特許として公開されている情報は該当しません。

参考　独立行政法人情報処理推進機構(IPA)「組織における内部不正防止ガイドライン」 https://www.ipa.go.jp/files/000057060.pdf
経済産業省知的財産政策室「営業秘密の保護・活用について」 http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/1702tradesec.pdf

鳥取県内企業対象

情報セキュリティ対策に関するアンケート調査結果

鳥取県サイバーセキュリティ対策ネットワークでは、サイバー犯罪被害の未然防止対策を推進することを目的として県内企業の情報セキュリティ対策に対する意識調査や実態把握のためのアンケートを実施しました。

○ 調査対象期間
　平成28年９月５日（月）～ 同月30日（金）

○ 調査対象
　一般社団法人鳥取県情報産業協会、鳥取県商工会議所連合会
　一般社団法人鳥取県法人会連合会、鳥取県経済同友会(順不同)
　に加入する鳥取県内企業174社

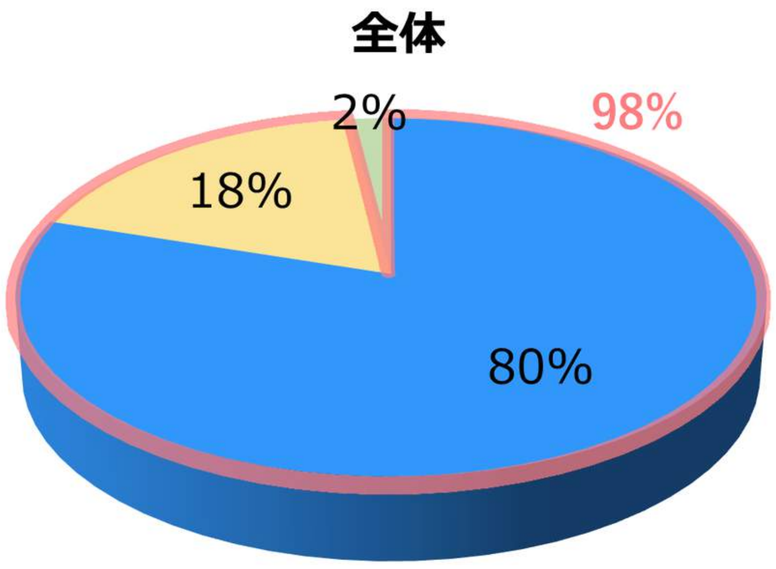
○ 形式・集計概要
　選択式のアンケート(全38問)に対し、無記名による回答
　アンケート送付数：174　回答数：110 (回答率63.2%)

アンケート調査にご回答いただきました企業の皆様には、ご多忙にもかかわらず、ご協力いただき誠にありがとうございました。

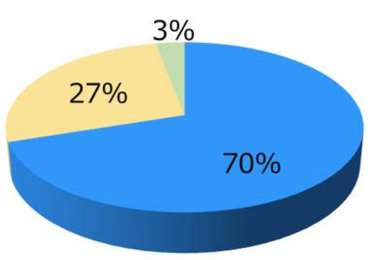
特徴的な15の回答結果をご紹介します

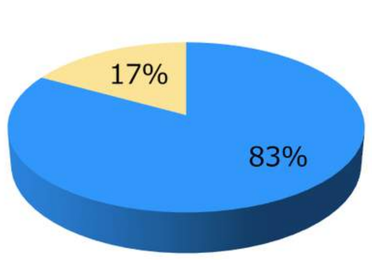
① 情報セキュリティは必要だと感じるか

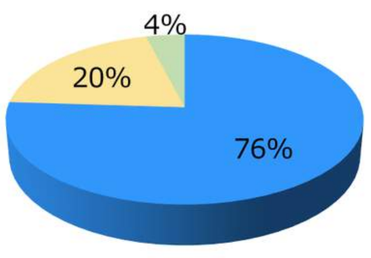
■ 必要と感じる　■ どちらかと言えば必要と感じる　■ 必要と感じない　■ わからない

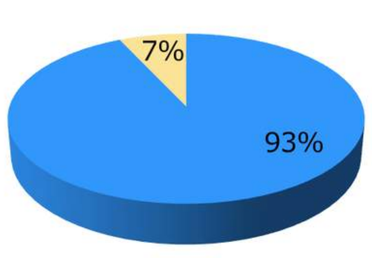


「必要と感じる」または
「どちらかと言えば必要と感じる」
と回答した企業が全体で95%を
超えています。



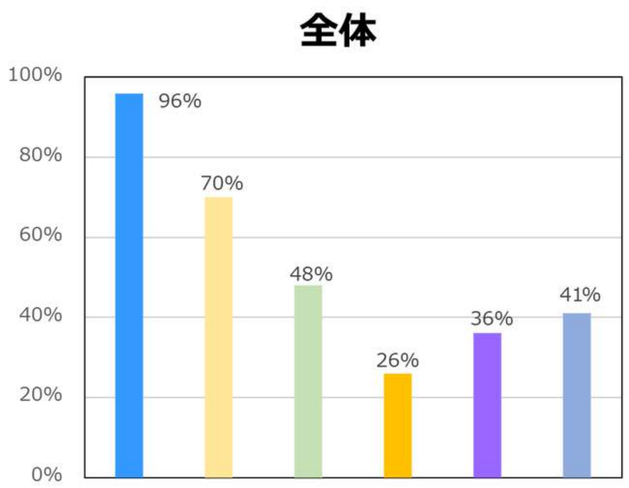




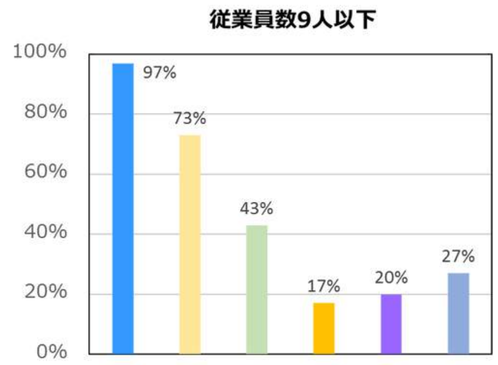


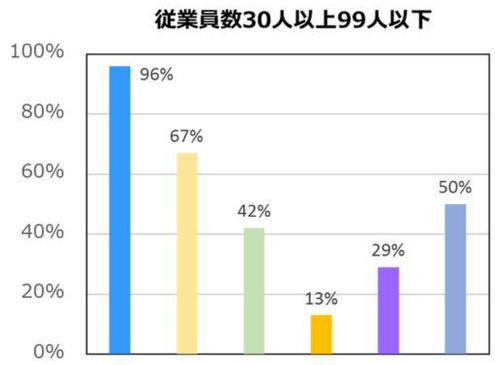
情報セキュリティ対策の現状

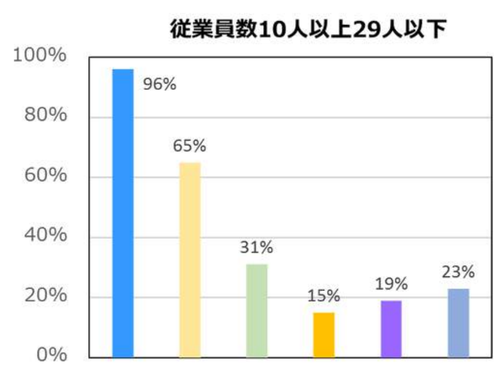
② 自社で認識しているサイバー攻撃や情報漏えい等に関する脅威の種別（複数回答可）

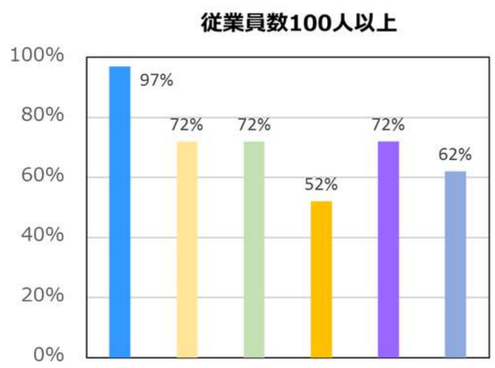


- コンピュータウイルス
- ID･パスワードが窃取され、ユーザなりすましによる不正アクセス
- ぜい弱性を突かれたことによる不正アクセス
- 内部犯行（内部不正）
- Dos攻撃
- 標的型攻撃







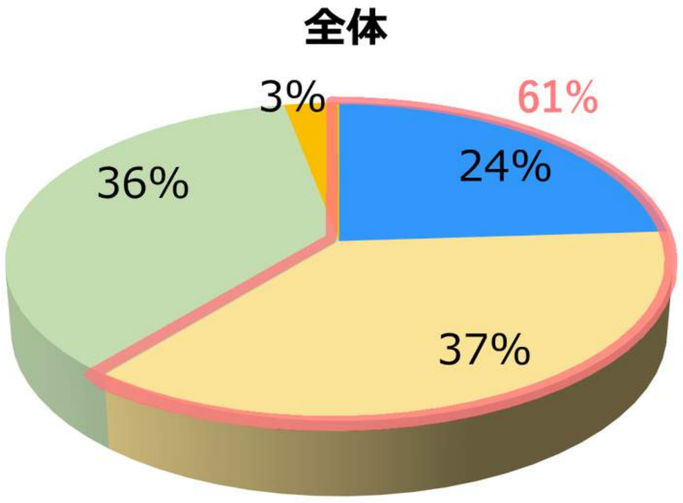


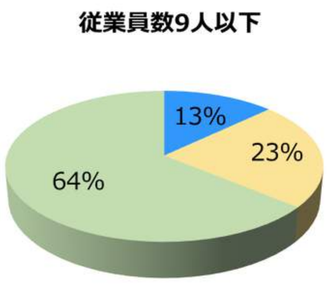
「コンピュータウイルス」「不正アクセス」を脅威と認識していると回答した企業が全体で70%を超えています。

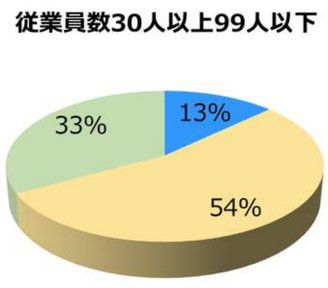
従業員数が多い企業の方が「Dos攻撃」や「標的型攻撃」、「内部犯行」を脅威と回答している割合が高くなっています。

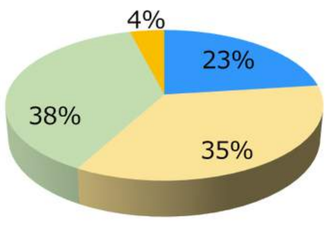
③ 自社における情報セキュリティ対策の体制

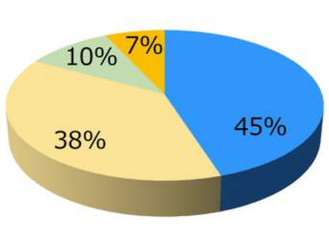
- 専門部署（担当者）がある
- 兼務だが担当者が任命されている
- 組織的には行っていない（各自の対応）
- わからない











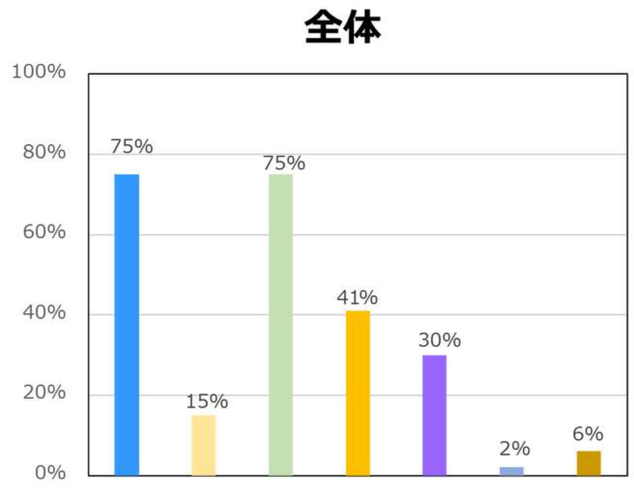
従業員数の少ない企業ほど専門部署の設置や担当者が任命されていない傾向にあります。

また、
従業員数100人未満の企業の3割以上で情報セキュリティ対策が各従業員に任せられている状況です。

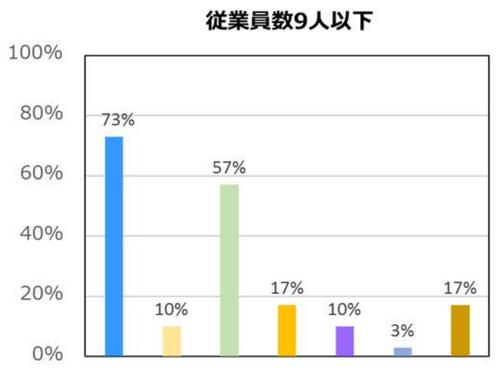
情報セキュリティ対策の現状

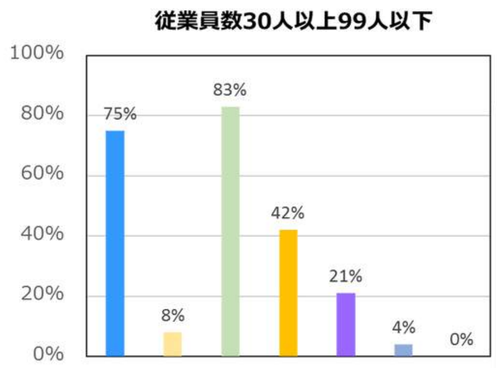
④ 業務用端末※において実施している情報セキュリティ対策

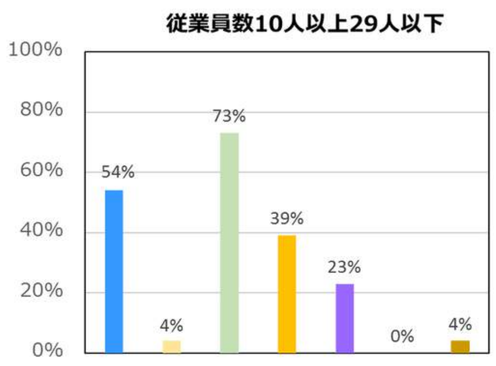
※ パソコン、スマートフォン、タブレットなど

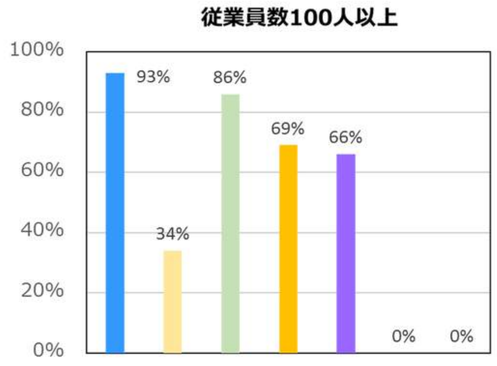


- 端末のパスワード設定
- 紛失･盗難時のデータ消去
- セキュリティソフトの導入
- 端末と社内システムの接続をシステム管理
- 利用ルールの策定（アプリケーションの導入制限等）
- その他
- 特に実施していない



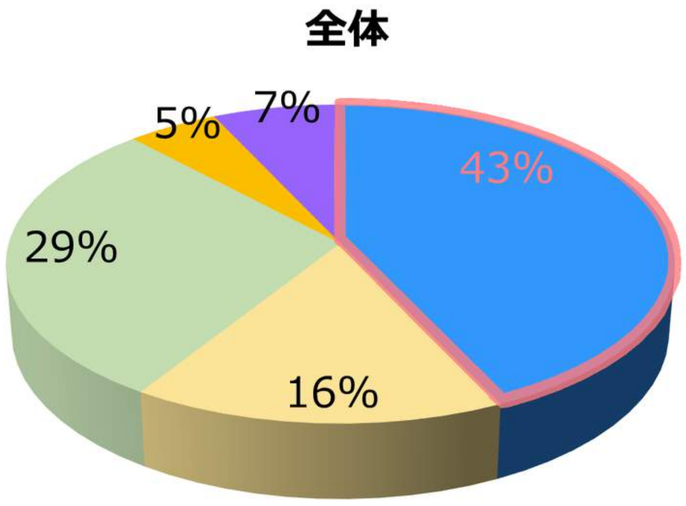


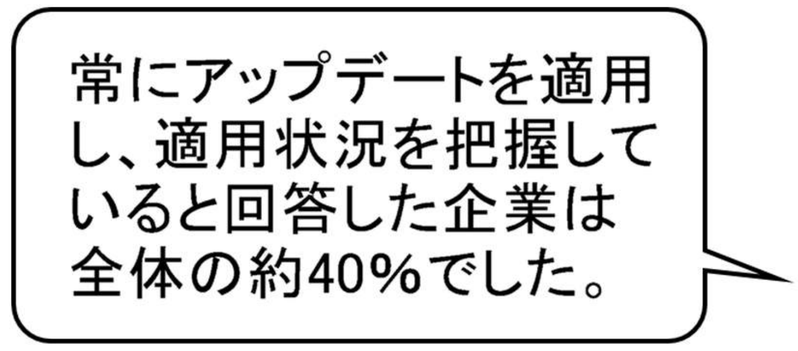


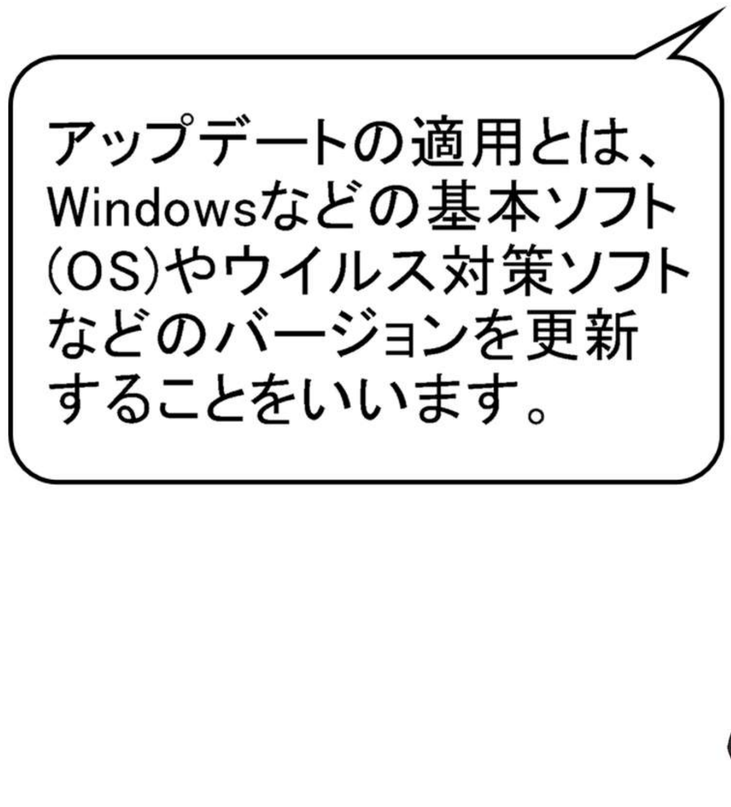


⑤ パソコン等のアップデート適用状況

- 常に適用し、適用状況も把握している
- 常に適用する方針・設定だが、実際の適用状況は不明
- 各従業員に任せている
- ほとんど適用していない
- わからない





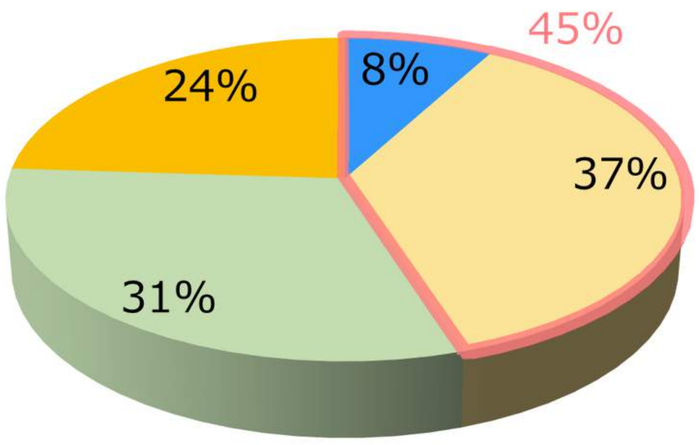


コンピュータウイルスの感染と被害状況

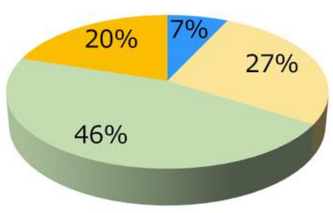
⑥ 平成27年度中のコンピュータウイルス感染

ウイルスに感染した
ウイルスを発見したが、感染には至らなかった
ウイルスをまったく発見しなかった
わからない

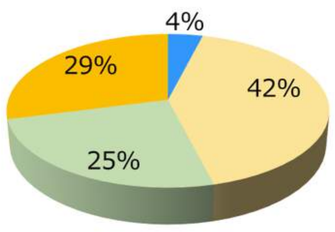
全体



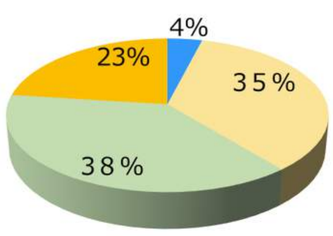
従業員数9人以下



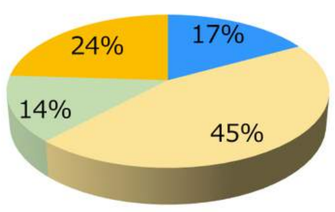
従業員数30人以上99人以下



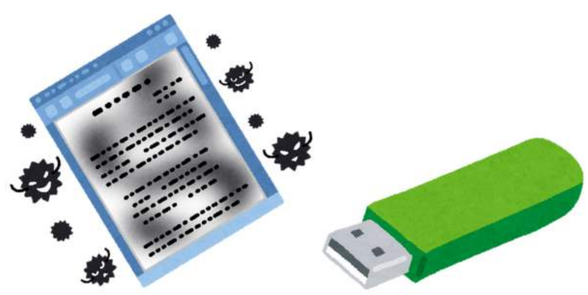
従業員数10人以上29人以下



従業員数100人以上

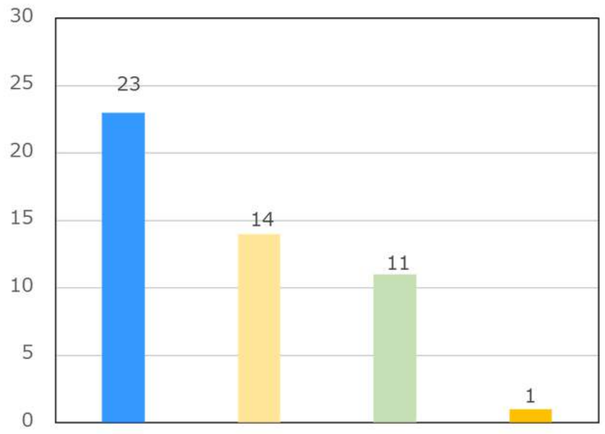


「ウイルスに感染した」
「ウイルスを発見したが感染しなかった」と回答した企業は全体で合わせて45%
「わからない」と回答した企業は会社規模を問わず20%を超えています。



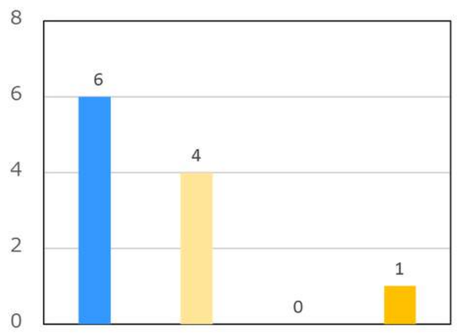
⑦ ウイルスに感染した影響で生じた被害 (複数回答可)

全体

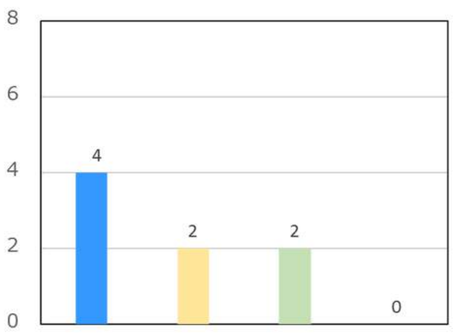


データの破壊、システム停止等による業務停滞
個人情報、営業秘密等の情報流出
ウイルスメールの発信等による取引先等への被害拡大
その他

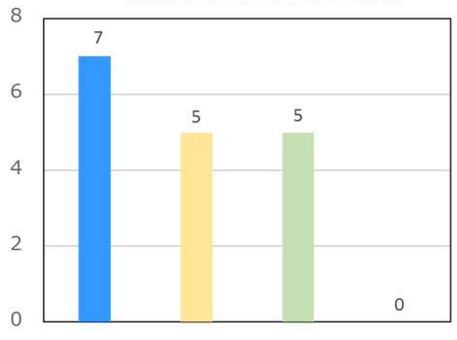
従業員数9人以下



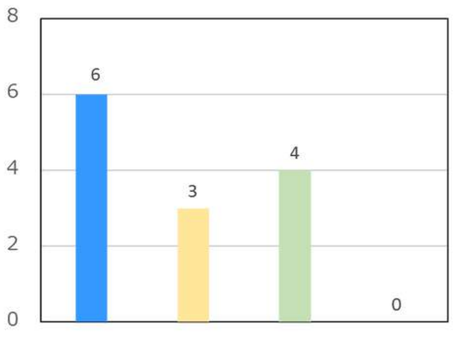
従業員数30人以上99人以下



従業員数10人以上29人以下



従業員数100人以上



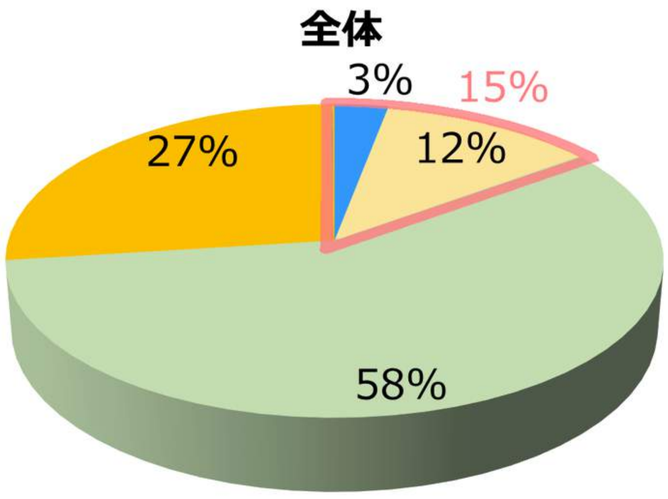
「データの破壊、システム停止等による業務停止」の被害が23件と全体では最多
「個人情報、営業秘密等の情報流出」の被害も14件の回答があり、現実に被害が発生しています。

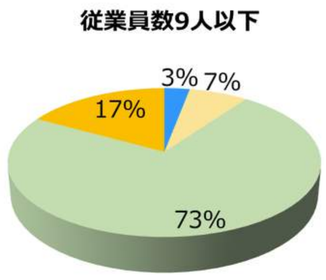
サイバー攻撃被害の現状

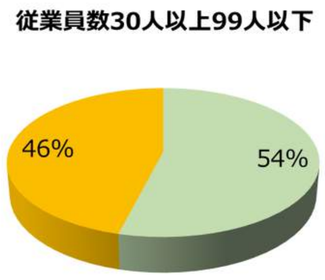
⑧ 平成27年度中、自社のサーバやパソコンが受けたサイバー攻撃※

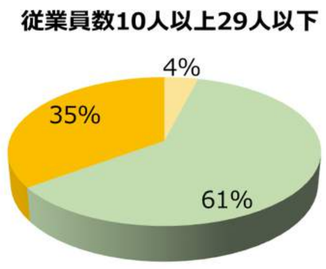
※ 不正アクセス、DoS攻撃、標的型攻撃など

- サイバー攻撃で被害にあった
- サイバー攻撃を受けたが、被害には至らなかった
- サイバー攻撃をまったく受けなかった
- わからない





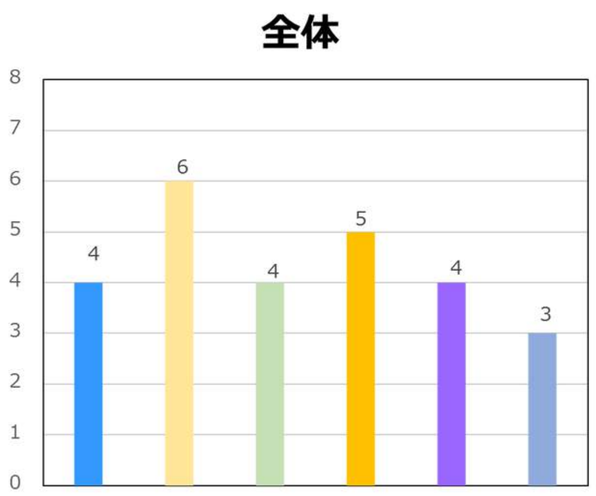




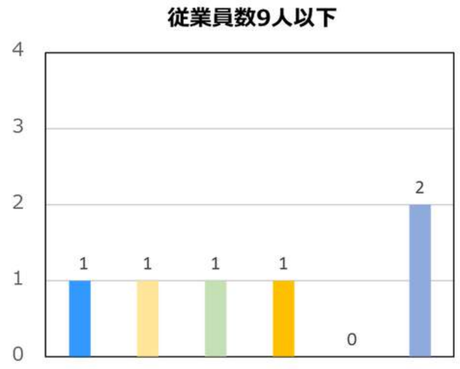
サイバー攻撃を受けたと回答した企業は全体で15%
わからないと回答した企業は全体で27%でした。

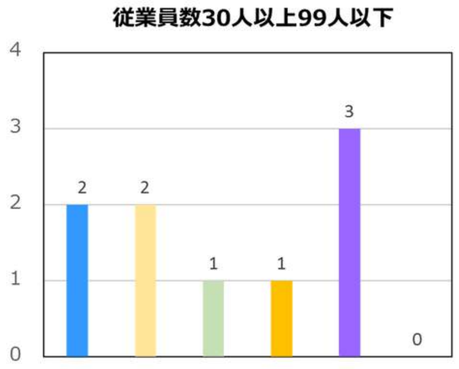
サイバー攻撃とは、コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取、破壊、不正プログラムの実行等を行うことを言います。

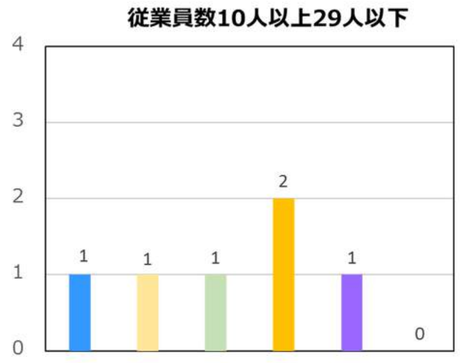
⑨ 自社が受けたサイバー攻撃の被害としてあてはまるもの

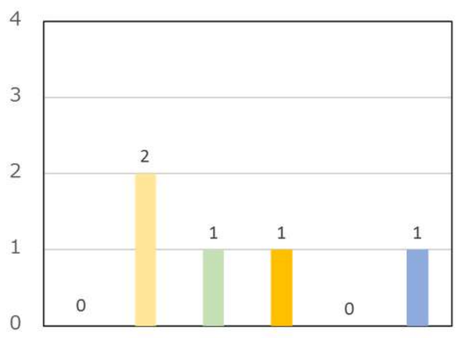


- Webサイトの改ざん、サービス停止等による業務停滞
- 業務サーバの内容が改ざん、サービス停止等による業務停滞
- 提供しているネットサービスへの第三者のなりすましによる不正使用
- 取引先の企業、個人への被害拡大
- 重要情報(個人情報、営業秘密、技術情報)が盗まれた
- その他



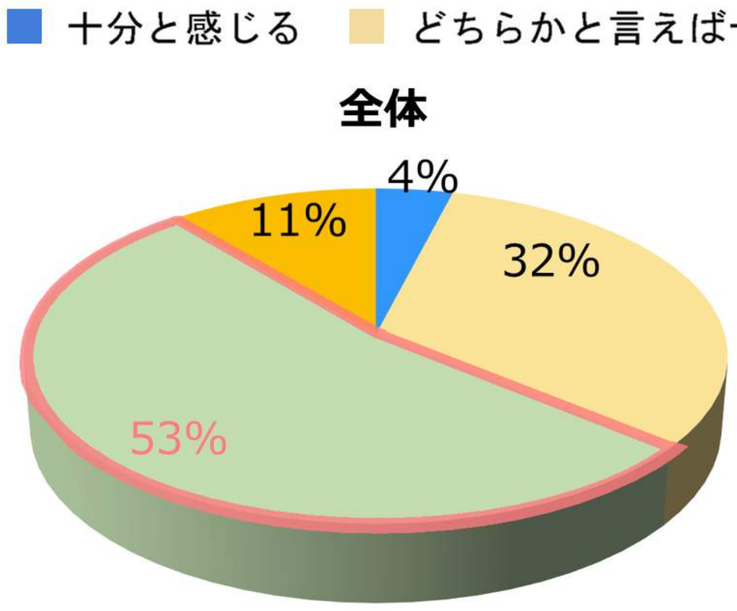


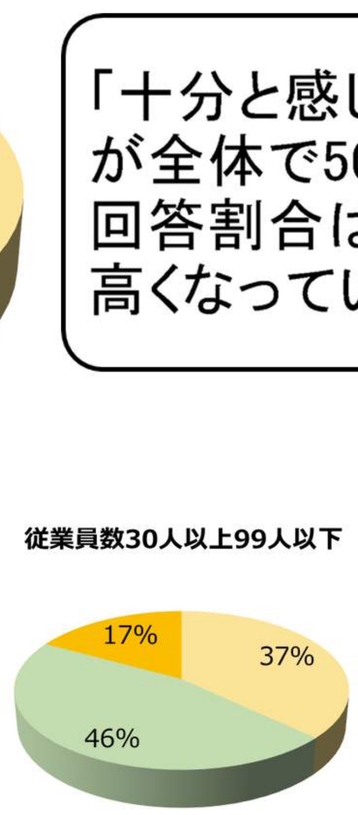


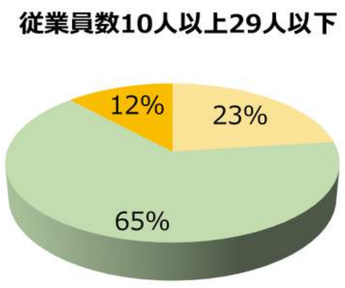


企業規模に関わらず被害種別にも偏りがないという結果で、攻撃対象が特定の企業規模に限定されていないことが読み取れます。

⑩ 外部からサイバー攻撃を受けた場合の対策は十分と感じるか



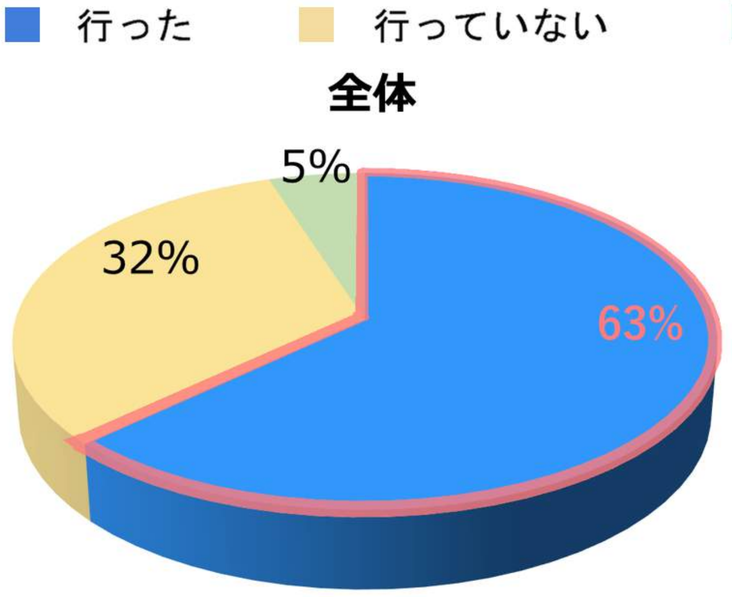


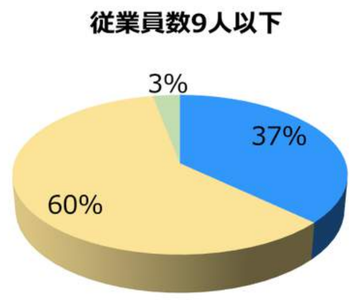


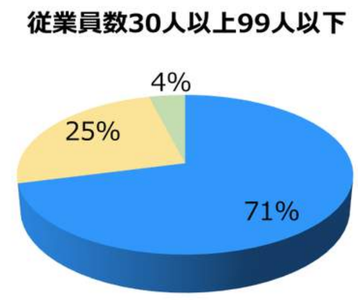
「十分と感じない」と回答した企業が全体で50%を超えています。
回答割合は、少人数企業の方が高くなっています。

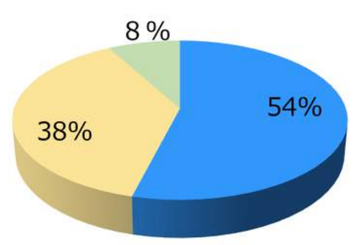
新たな対策の導入を検討していたりその必要性を感じている企業の割合が高いと言えます。

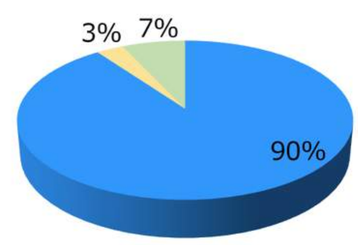
⑪ 過去３年間にIT投資を行ったか











従業員数の少ない企業では半数近くがまだIT投資を行っていないようです。

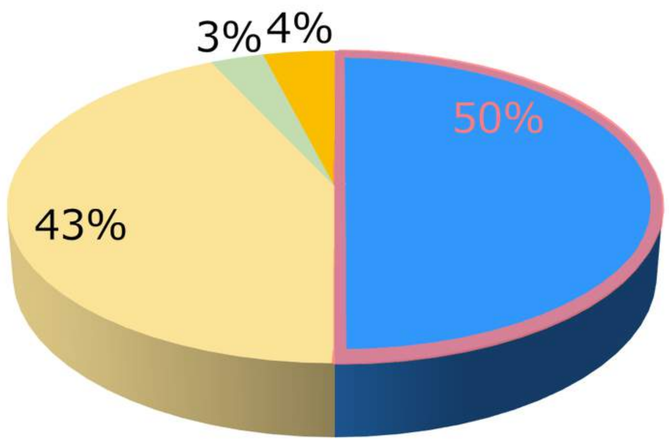
IT投資とは、情報化または効果的な情報技術の利活用のためにかける費用のことをいいます。

相談窓口利用状況

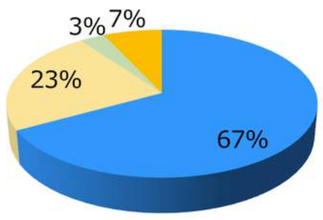
⑫ 問題発生時、警察の相談窓口を利用したいと思うか

■ したいと思う
■ 警察への相談は面倒なのでできるだけ相談したくない
■ まずは、警察以外の相談先に相談する
■ 警察には相談しない

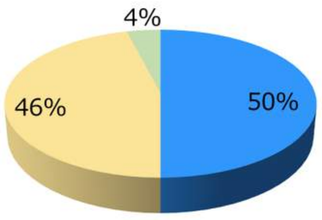
全体



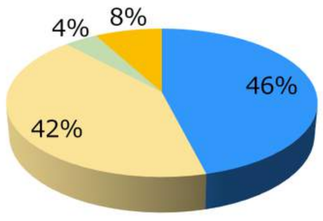
従業員数9人以下



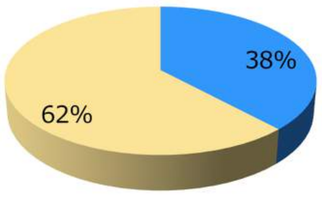
従業員数30人以上99人以下



従業員数10人以上29人以下



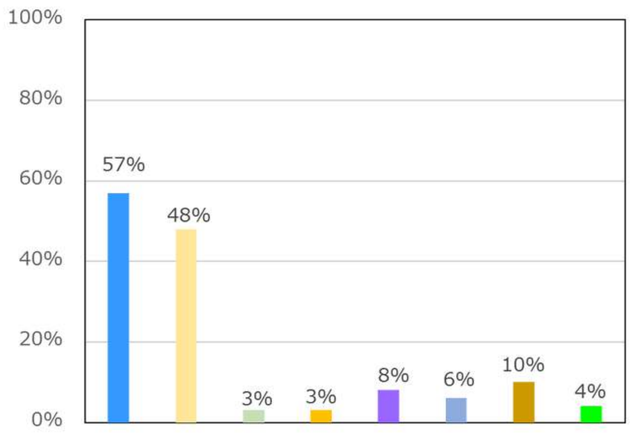
従業員数100人以上



警察への相談を希望する企業は全体で半数
警察以外の相談先を希望する企業も多いようです。

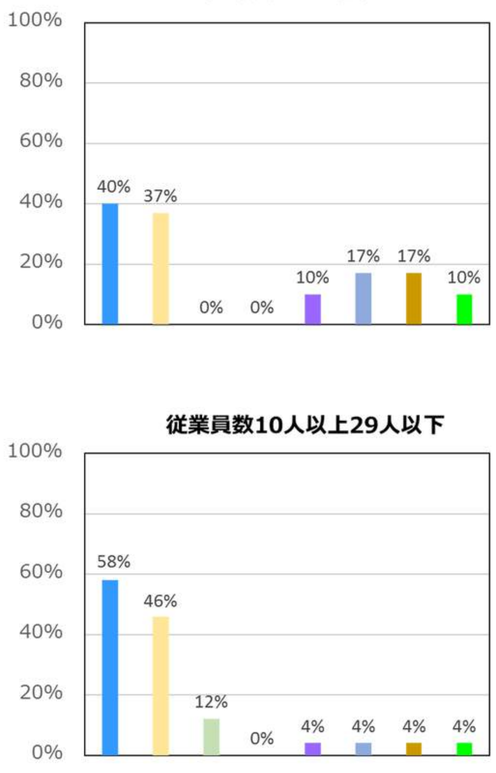
⑬ 情報セキュリティに関する相談先はどこか(複数回答可)

全体

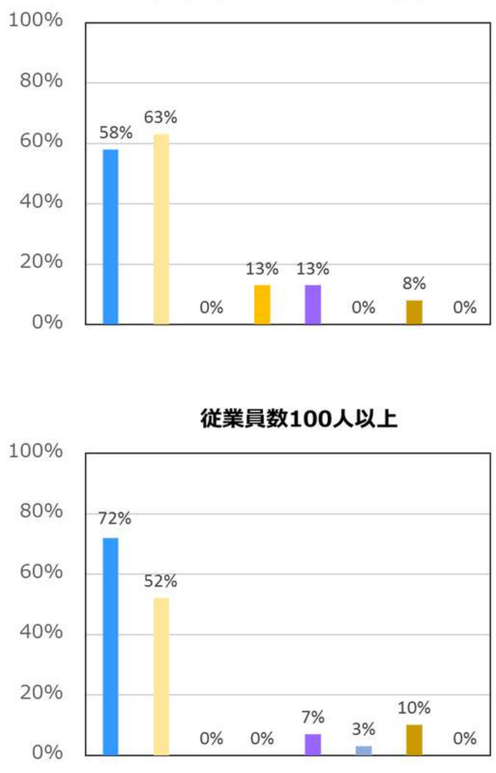


■ 社内の担当者
■ ITベンダ
■ 商工会議所・商工会・中小企業団体中央会
■ 鳥取県
■ 警察
■ どこに相談していいかわからない
■ その他
■ 特にない

従業員数9人以下



従業員数30人以上99人以下

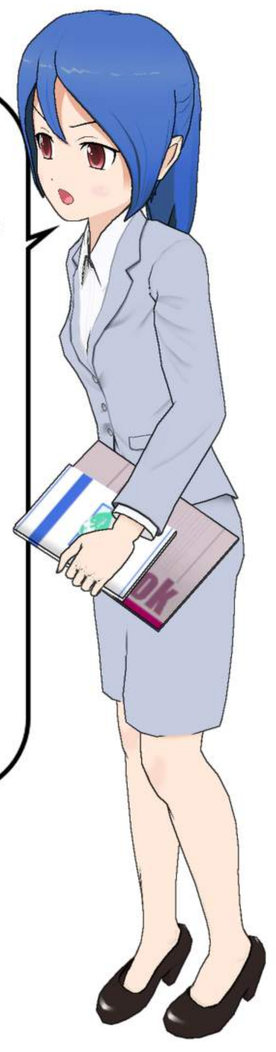


従業員数10人以上29人以下

従業員数100人以上

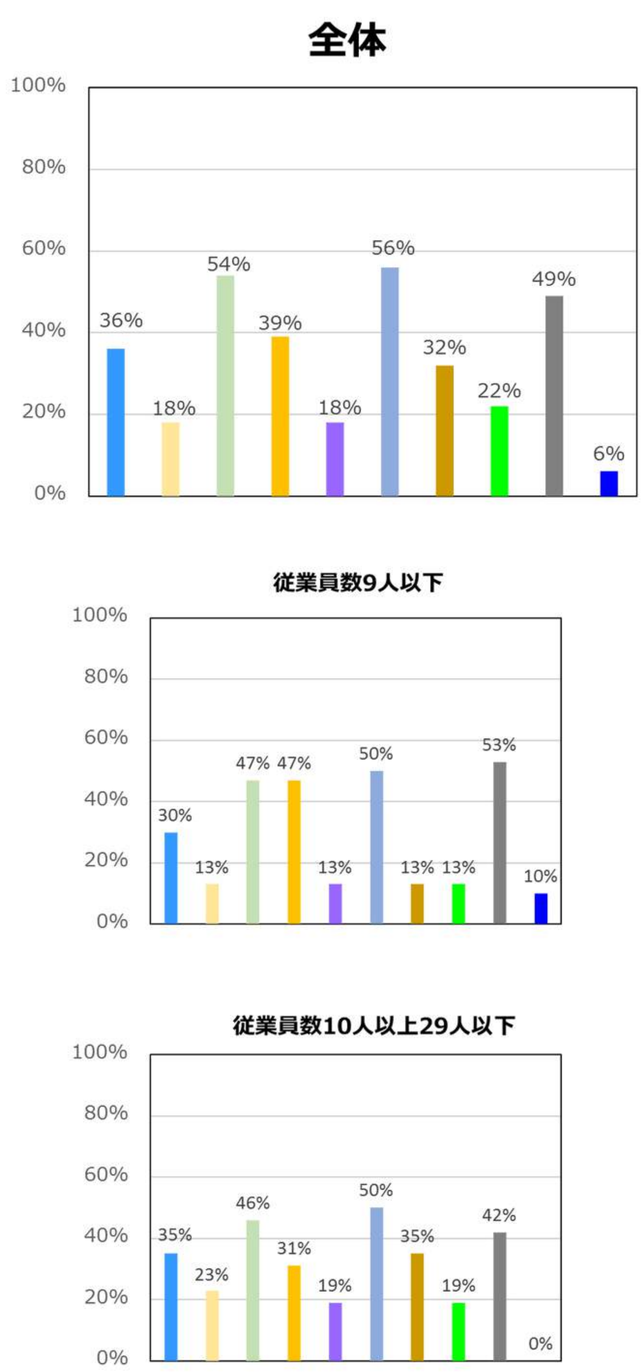
⑫の質問では、
警察への相談を希望する企業が多かったものの
実際の相談先としては、
警察も10%前後となっています。

気兼ねなく相談しやすい相談窓口を求めている企業が多いようです。

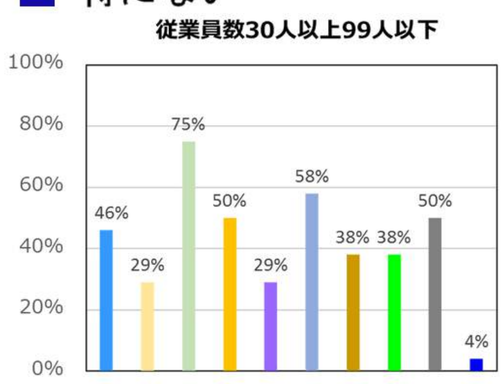


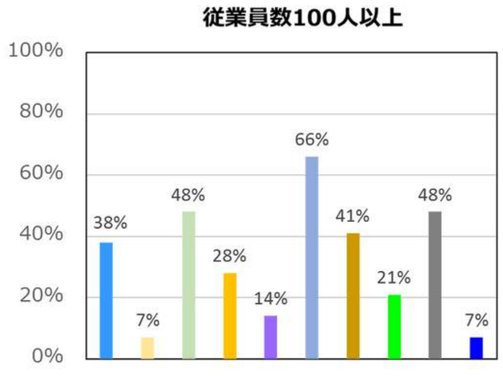
相談窓口に関する要望

⑭ 情報セキュリティ対策の相談窓口に期待すること(複数回答可)



- 情報セキュリティのルールの作り方の教示
- 情報セキュリティ対策を行う場合の資金援助制度の教示
- 企業が最低行うべき情報セキュリティ対策の教示
- 低料金で効果の高い情報セキュリティ対策の教示
- 安心できるITベンダの教示
- サイバー攻撃から企業を守るための方法の教示
- 内部不正から企業を守るための方法の教示
- 不正送金の被害に遭わないための方法の教示
- 被害にあった際の対処方法の教示
- 特にない



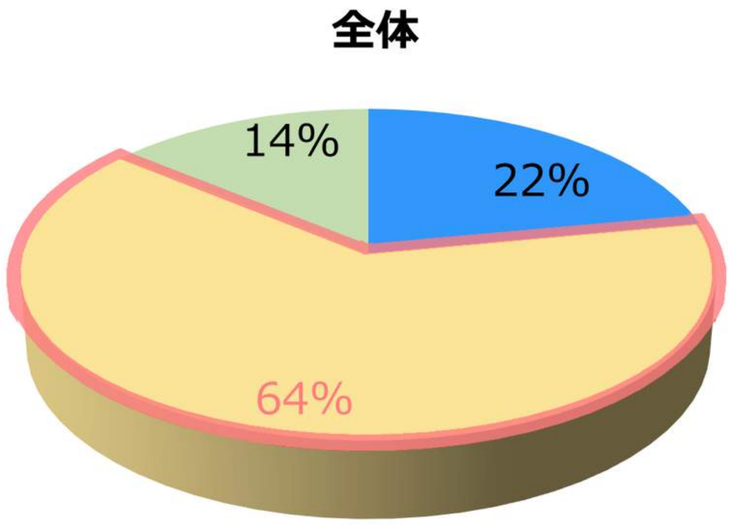


「最低限行うべき対策」
「サイバー攻撃から守る方法」
「被害への対処方法」
について相談したいという回答が企業規模を問わず50%前後となっています。

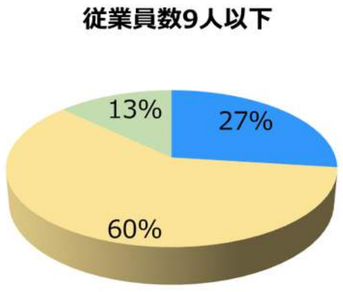
また、
コストパフォーマンス
の高い対策方法を求める
回答も多くなっています。

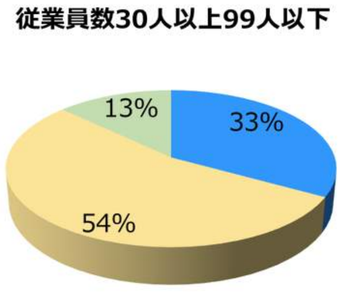
⑮ 情報セキュリティに関する相談窓口があれば利用するか

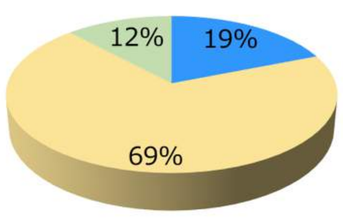
- 有償無償に関わらず、機会があれば利用したい
- 無償であれば利用したい
- 利用したいと思わない

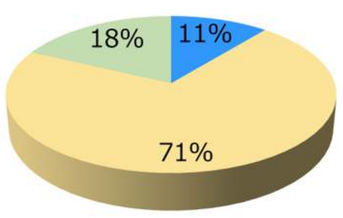


「無償であれば利用したい」と回答した企業が全体で60%を超える一方で、
「有償無償を問わず利用したい」と回答した企業も20%を超えています。









アンケート調査結果の一つとして言えることは、県内企業は「サイバー攻撃などの危険性と情報セキュリティ対策の必要性を感じつつ、被害予防に向けた投資の検討や被害発生時の対処など総合的な相談が可能な窓口を必要としている。」ということがわかりました！

メールの 添付ファイル を開く前に

メール文と一緒に届く「 添付ファイル 」

ワード、エクセル、パワーポイント
PDF、画像などのファイルの・・・

正体が
ウイルスかも?!

ウイルス付きの
ファイルが
入っている事も!!

でも、確認しないと
仕事できないっ！

履歴書.docx
作業工程表.xlsx
会議資料.pptx
議事録.pdf
現場写真.jpg

ファイルを開く前の 1 2 3

1 不審なファイルは開かない

送信元メールアドレスがフリーメールの場合は要注意！！
差出人のメールアドレスとメール本文の署名に記載された
メールアドレスが同一か確認する！！
メール本文の日本語が不自然な場合も！！

送信元が知人や取引先でも
第三者がなりすまして
いることもあります！

2 ウイルスチェック

添付ファイルは、必ずウイルスチェック
セキュリティ対策ソフトは必ず導入しておきましょう。

3 ファイルの拡張子を確認

セキュリティ対策ソフトだけでは対処しきれないウイルスもあります！
ファイルの拡張子から、ファイルの情報を確認することができます。
あなたの目で不審点を見破り、ウイルスファイルを撃退しましょう！！

ファイルの拡張子とは？！

拡張子は、ファイルの
「種類」を示す記号で
ファイル名の後に付く
「.」以下の英数字です

.doc　.txt　.pdf　.xls
.jpg　.png　.mp4
.exe
.js

[.doc .txt .pdf]は文書
[.xls .xlsx]は表計算
[.jpg .png]は画像
[.mp4]は動画
[.exe][.js]はプログラム

要注意

見た目は文書ファイルでも…
その正体は「ウイルス」かも
知れません。

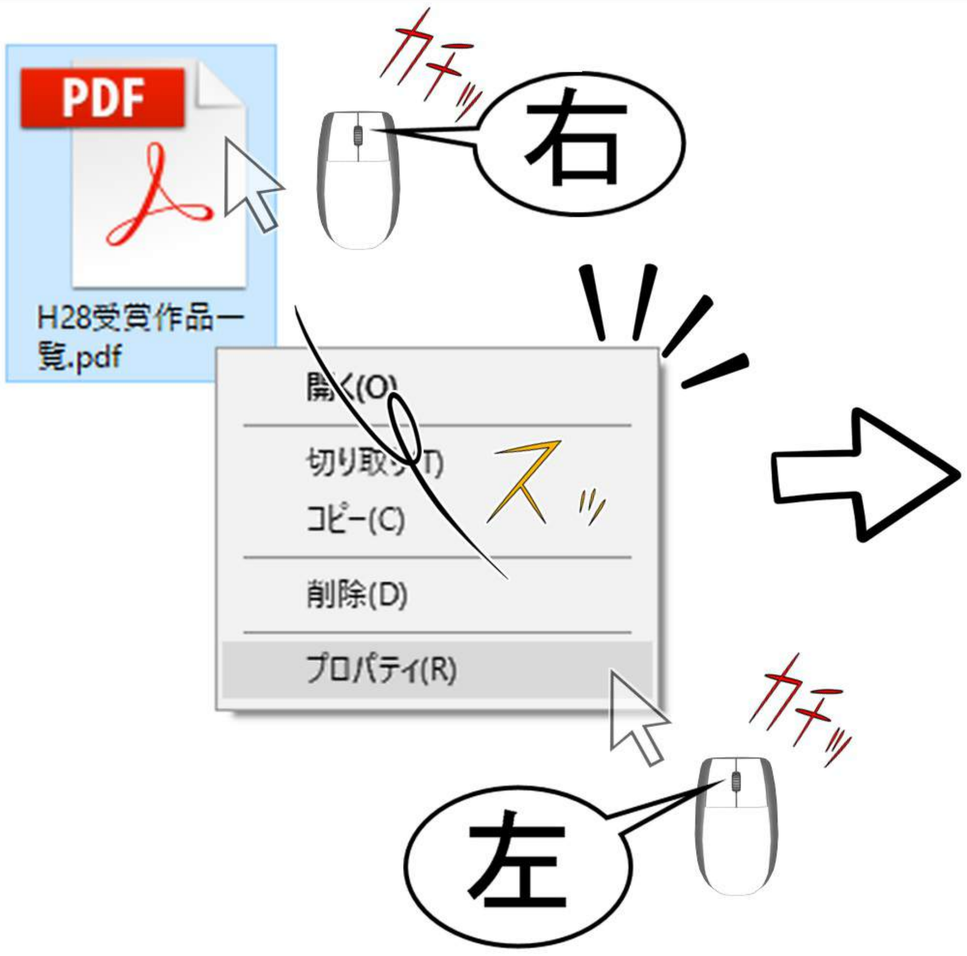
特に注意したい拡張子は [.exe] [.js]

この拡張子が付いている場合は
ウイルスの可能性があります。

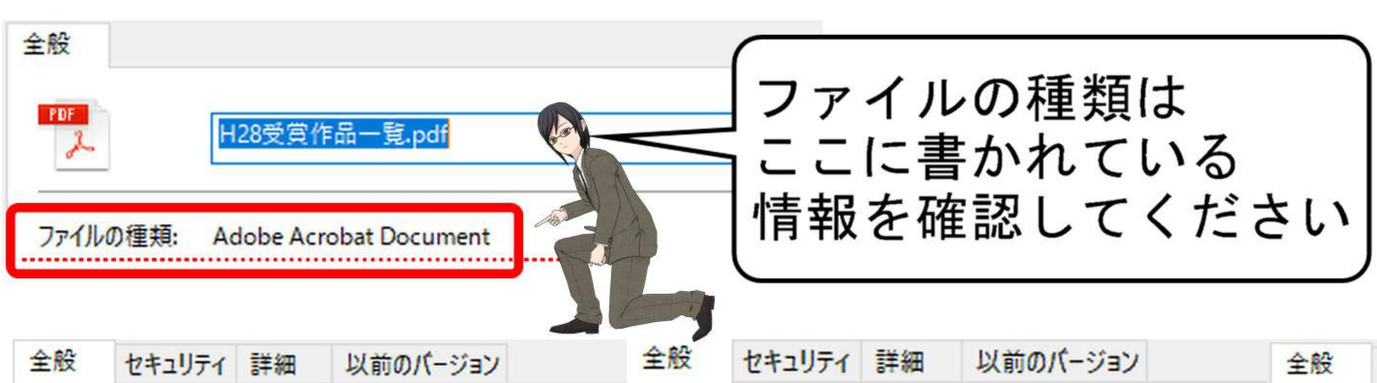
ファイルの拡張子を確認する方法については、裏面をご覧ください。
不審なメールに気づいた際は、組織内で情報共有し、被害防止を図りましょう。

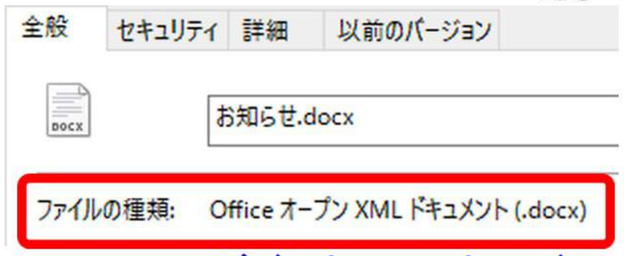
ファイル拡張子の確認方法

ファイルを右クリックし、詳細情報（プロパティ）を表示します

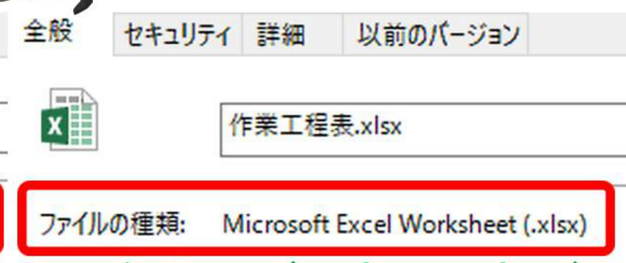


詳細情報（プロパティ）内の「ファイルの種類」を確認します

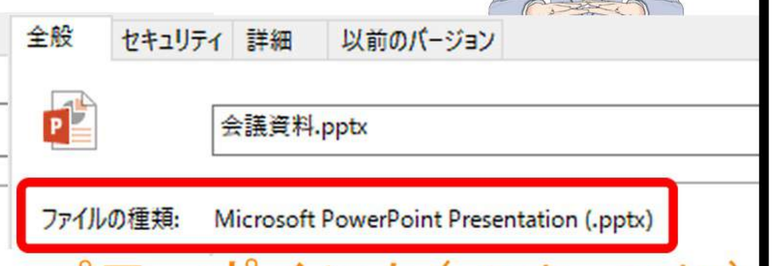




ワード(.doc .docx)



エクセル(.xls .xlsx)



パワーポイント(.ppt .pptx)

画像(.jpg .png .bmp)

アプリケーション(.exe)

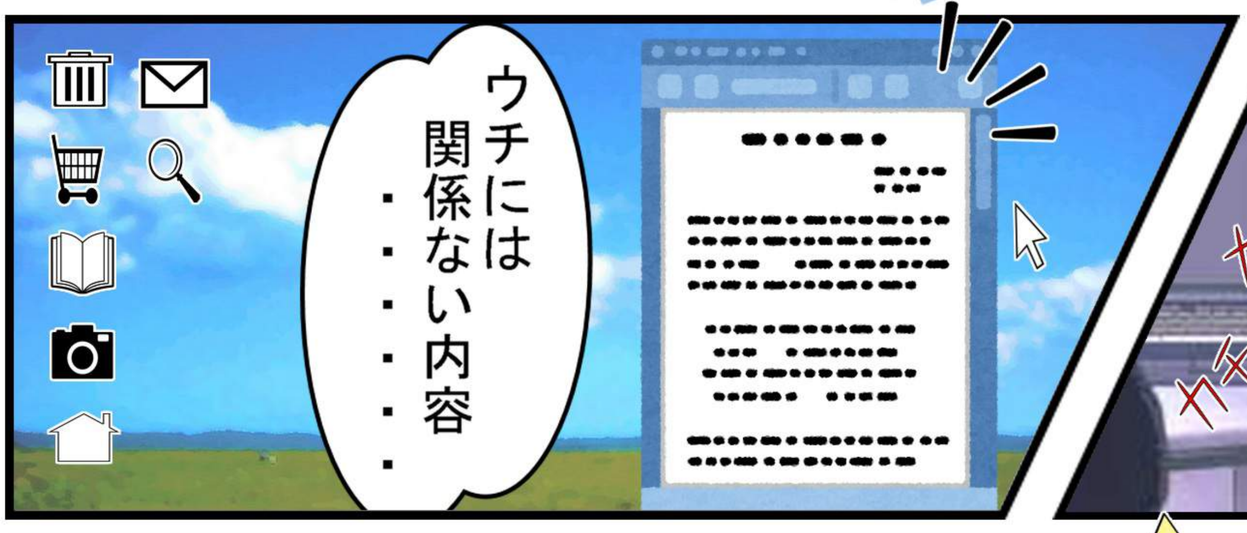
ファイル名とファイルの種類
を見比べて、食い違う点が
ないかを確認しましょう

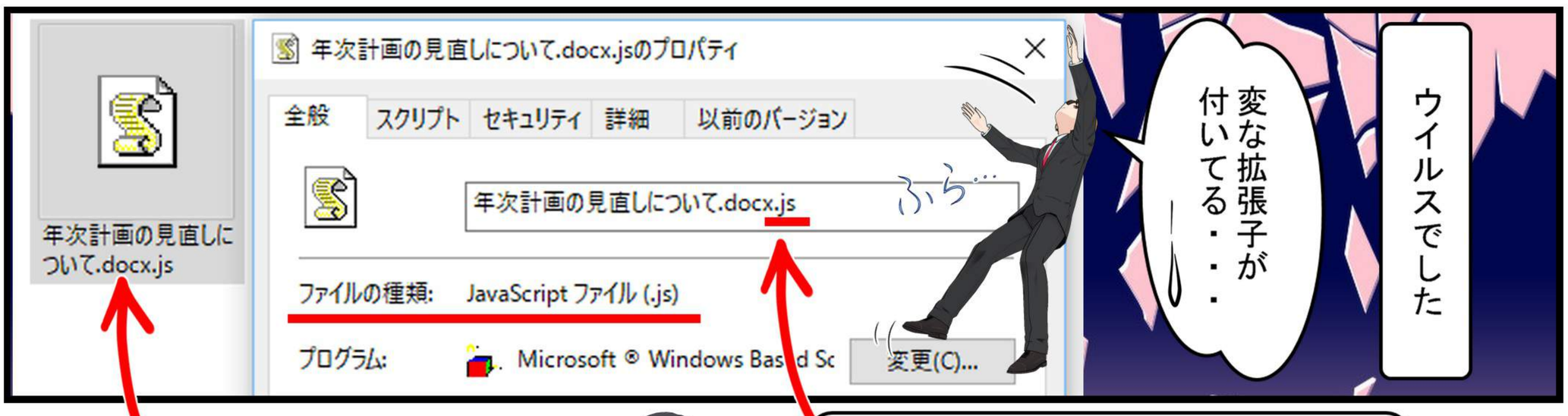
ウイルス付きファイルはこうなっています！！

見た目はエクセルファイルですが・・・
ファイルの種類が「ｱﾌﾟﾘｹｰｼｮﾝ(.exe)」
と表示されています。
これは、偽物のエクセルファイルです！

ウイルス付きファイルを一度でも開けば、感染してしまいます！！
偽物と思われるファイルは開かず、システム管理者へ連絡しましょう

不審なファイル を開いてしまったら





見た目は「プログラム
ファイル」であっても
文書ファイルとは限り
ません。

「.exe」や「.js」などの
拡張子を持つファイルは
プログラムファイルであり
ウイルスの可能性があります

拡張子の調べ方の詳細は⑬ページ「メールの添付ファイルを開く前に」の裏面をご覧ください。

対処方法 1 2 3

1 LANケーブルを抜きます

2 システム管理者へ連絡します

3 組織幹部へ連絡します

トラブルに対して組織幹部は、取引先・株主・警察などへの連絡や
原因・被害規模調査依頼、公表など多くの決断を求められます。
素早く被害、損害を最小限に食い止めるためにも即報しましょう。

無線LAN接続の場合は、切断方法を事前に確認しておきましょう。

システム管理者の方へ依頼する内容は、裏面をご覧ください。

システム管理者に依頼すること

１．添付ファイルとメール送信元の特定
２．マルウェア（ウイルス）の特徴などの確認
３．別端末、外部記憶装置の影響調査
４．情報流出事実の確認
５．組織幹部への説明

【システム管理者の方へ】

メールの送信元を早急に特定し、関係者への注意喚起をお願いします。

パソコンの初期化など復旧措置をする前にどのような被害にあったかを突き止めてください。

感染したマルウェアを特定し、その特徴を参考にして被害規模と原因を特定し、組織幹部へ報告してください。

組織幹部がすべきこと

１．情報流出対応
２．再発防止指示と教養
３．復旧措置
４．システムの見直し

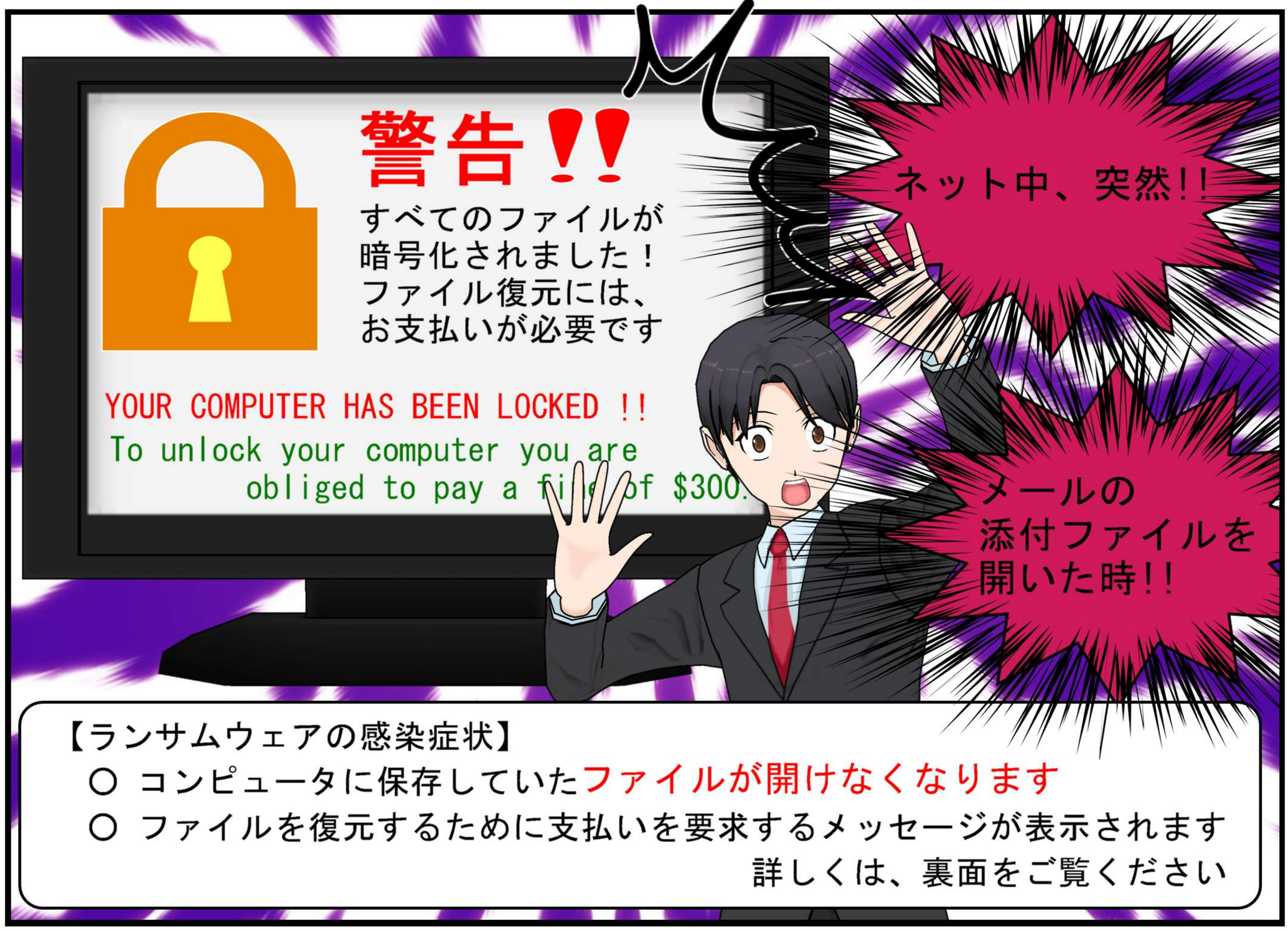
ウイルス対策ソフトだけでは防ぎきれないウイルスが急増しています。
・OS（基本ソフト）のバージョンは最新のものか
・ソフトウェアのバージョンは最新のものか
・機密情報は適切な場所に保存されているか
など定期的な確認を心掛けましょう。

【被害防止のために】

この事例は、「標的型メール」、「ばらまき型メール」による被害事例をモデルにしています。

こうしたケースでは、「.exe」ファイルを受け付けないシステムを採用するなど、システムの設定を見直すことも重要ですが、メールを取り扱う担当者へ正しい教養を行うことが非常に有効とされています。

ランサムウェアに感染したら



【ランサムウェアの感染症状】

○ コンピュータに保存していたファイルが開けなくなります

○ ファイルを復元するために支払いを要求するメッセージが表示されます

詳しくは、裏面をご覧ください

対処方法 1 2 3

1 LANケーブルを抜きます

2 パソコンの電源は
ONのまま触らずに

3 システム管理者へ
連絡します

無線LAN接続の場合は、切断方法を事前に確認しておきましょう。

システム管理者に依頼すること

１．マルウェアの特定
２．感染経路の特定
３．被害規模の特定
４．情報流出事実の確認
５．組織幹部への説明

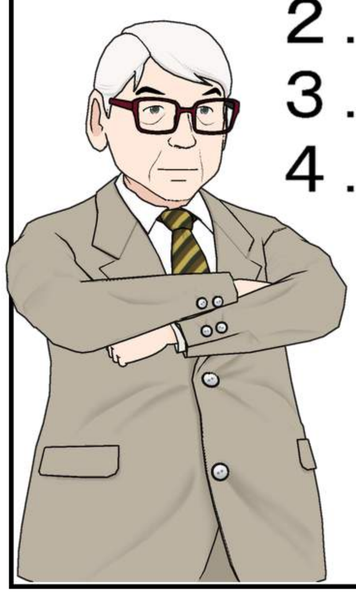
【システム管理者の方へ】

　パソコンの初期化など復旧措置をする前にどのような被害にあったかを突き止めてください。
　ランサムウェアは、NASなどネットワーク上のファイルにも被害が及ぶものもあります。
　感染したマルウェアを特定し、その特徴を参考にして被害規模と原因を特定し、組織幹部へ報告してください。

NAS：ネットワークアタッチトストレージ
　　コンピュータなどからネットワークを通じてアクセスできる外部記憶装置

組織幹部がすべきこと

１．情報流出対応
２．再発防止指示と教養
３．復旧措置
４．システムの見直し

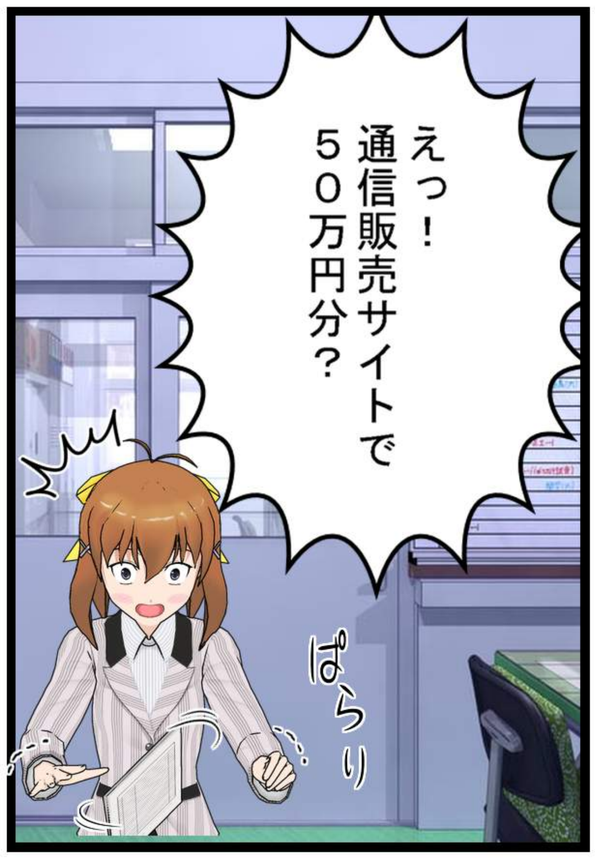


支払いをしても復元できる保証は
ありません！
データのバックアップがとれる
システムを構築しておきましょう！

【ランサムウェアとは？】

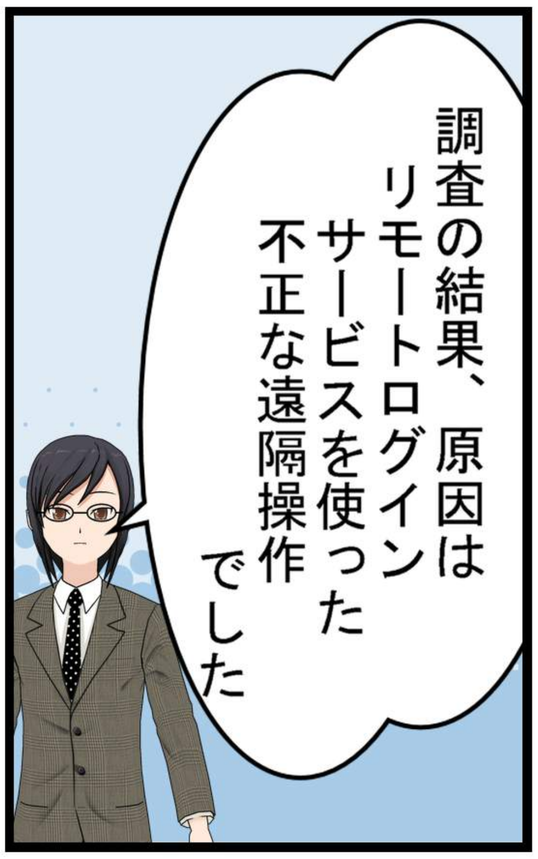
　コンピュータ・ウイルスの一種で、感染すると、コンピュータ内の画像や文書、場合によっては保存したデータ全てが暗号化され、利用することができなくなってしまいます。
　この暗号化されたデータは、ランサムウェアを作製した犯人しか元に戻すことができないため、それを盾に犯人は金銭を要求します。

自社のパソコンが遠隔操作されていたら



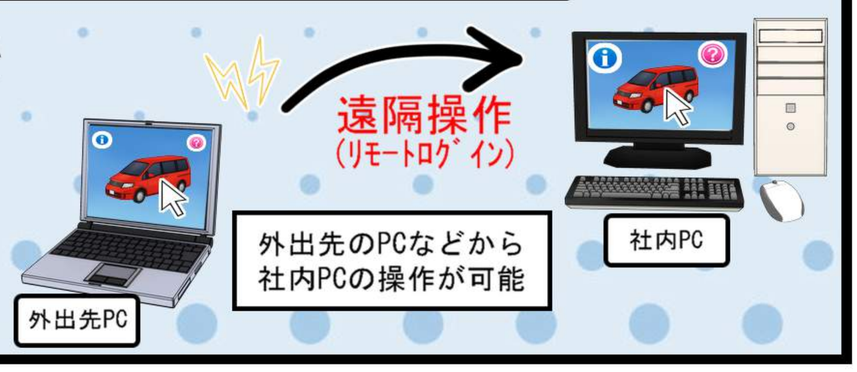
突如発生した
会社名義アカウントでの
商品大量購入・・・

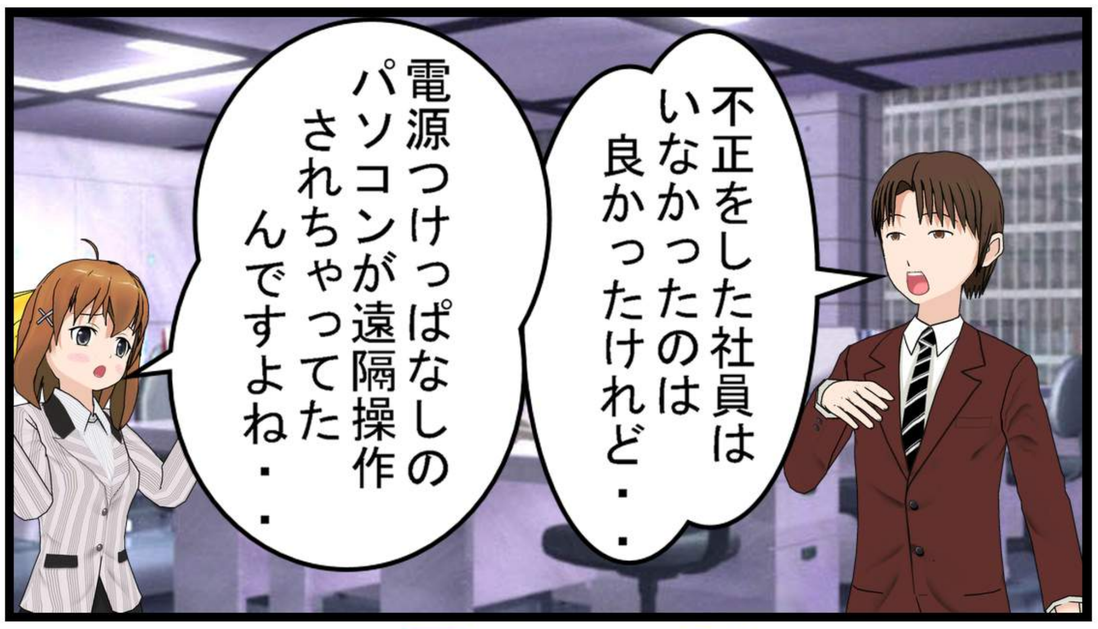
社員の誰も知らないうちに
通信販売サイトで注文
されていました

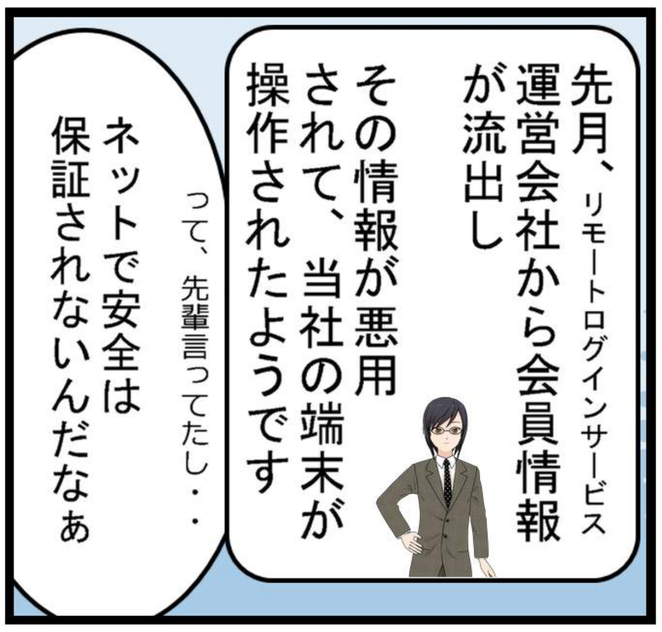


リモートログインサービスとは

外出先の端末から会社や自宅のパソコンなどを
操作することができるソフトのことです
無償のもの（条件付きも含む）で
Teamviewer,AnyDesk,Brynhildr,UltraVNC
などがあります







対処方法 1 2 3

1 リモートログインサービスの利用を
中止し、パスワードを変更しましょう

2 不正購入があれば、販売元へ連絡し
不正購入事実を説明しましょう

3 遠隔操作されたPCは、徹底的な
ウイルスチェックをしましょう

※　リモートログインサービスの利用自体をすべて否定するものではありません。

裏面にリモートログインサービス使用時の注意点を掲載しています。

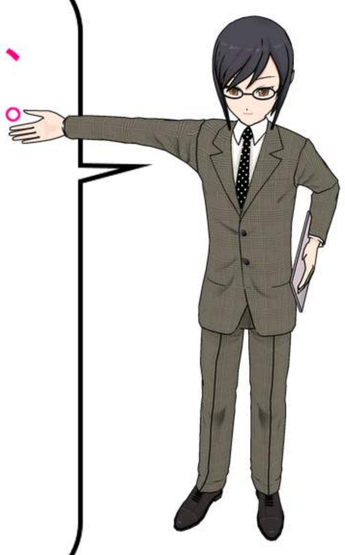
リモートログインサービスをお使いの方へ

リモートログインソフトを起動させたまま退社したところ、第三者から不正なログインを受けて遠隔操作され、通信販売サイトで商品の不正購入が行われた事例が増えています。

インターネット経由で遠隔地のパソコンを操作できるという
利便性と危険性をよく理解した上で、適切な運用を心掛けましょう。

念頭に置いておきたいこと

インターネット経由で遠隔(リモート)操作ができるということは、
端末が不正ログインなどの危険に晒されていると認識しましょう。



- ○ 本当にリモートログインサービスが必要ですか？
- ○ ログインできる「人」は限定されていますか？
- ○ 端末に保存されている情報は、情報漏えいが発生しても
  取り返しがつく程度のものですか？
- ○ 無断で利用している人はいませんか？
- ○ お使いのリモートログインサービスは、信頼できますか？

不正ログインを防ぐために

1　ログイン履歴を確認する

サービスサイトへアクセスし、ログイン履歴を確認しましょう。

2　二段階認証を有効にする

ワンタイムパスワードなどを利用した二段階認証を設定しましょう。

3　ホワイトリストを使用する

自社の端末に接続できるユーザを限定しましょう。

システム管理者の方へ

第三者にリモートログインされた端末は、ブラウザなどに保存されているアカウント情報を盗み出して、各種通信販売サイトやオンラインバンキングでの不正送金を行う、バックドアをインストールするなどの被害が出ていると言われています。
バックドアを放置すれば、新たな被害につながる恐れがあります。
不正ログインを受けた端末を初期化するなど徹底した再被害防止対策を施しましょう。
また、パスワードは複雑で強固なものに設定しましょう。

**リモートログインサービスは有償のものも複数あります。
利用される際は、信頼できるサービスを選びましょう。**

自社のウェブサイトが見られなくなったら

対処方法 1 2 3

1 ウェブサイト管理者へ連絡します

2 サーバの管理者へも連絡します

3 組織幹部へ報告します

ウェブサイトの運営を支える人たち

各種契約によって違いはありますが、ウェブサイト運営には様々な人たちが関わっています。
ウェブサイトの制作や管理を外部委託している場合の例を見てみましょう。

ウェブサイト管理者（制作者）

ウェブサイトを管理（制作）する人です。
サイトの改ざんなどの問題が発生したときに、復旧やウェブサイトの一時停止などの対応をお願いします。

ウェブサーバ管理者

ウェブサイトのデータを置くウェブサーバを管理する人です。
発生した問題の原因調査などをお願いします。

ウェブサーバ所有者

ウェブサーバを所有する人です。
ウェブサーバの管理者と所有者が別々の場合があります。
ウェブサーバ管理者が原因調査を行う際に協力をお願いします。

緊急時の連絡先をココへ
メモしておきましょう！

ウェブサイト・サーバ管理者へ依頼する内容は、裏面をご覧ください。

ウェブサイト管理者に依頼すること

１．ウェブサイト公開設定の確認
２．ウェブサイト公開の一時停止・代替措置
３．データ改ざんの有無の確認
４．組織幹部への説明
５．復旧等の措置

ウェブサーバ管理者に依頼すること

１．レンタルサーバであれば契約先へ即報
２．Webサーバ、DNSサーバのログを調査し原因を特定
３．情報流出の有無を確認
４．組織幹部への説明
５．復旧等の措置

組織幹部がすべきこと

１．情報流出対応
２．再発防止措置
３．復旧措置
４．システムの見直し

ウェブサイトへの攻撃は、ウェブサイトを閲覧できなくするだけのものもあれば、サーバ内の情報流出を狙うものもあります。

サーバ内に機密情報を置いていないか、公開設定は適切に設定されているか、詳細なログが保存される設定がなされているかなど、管理者等と連携して確認しておきましょう。

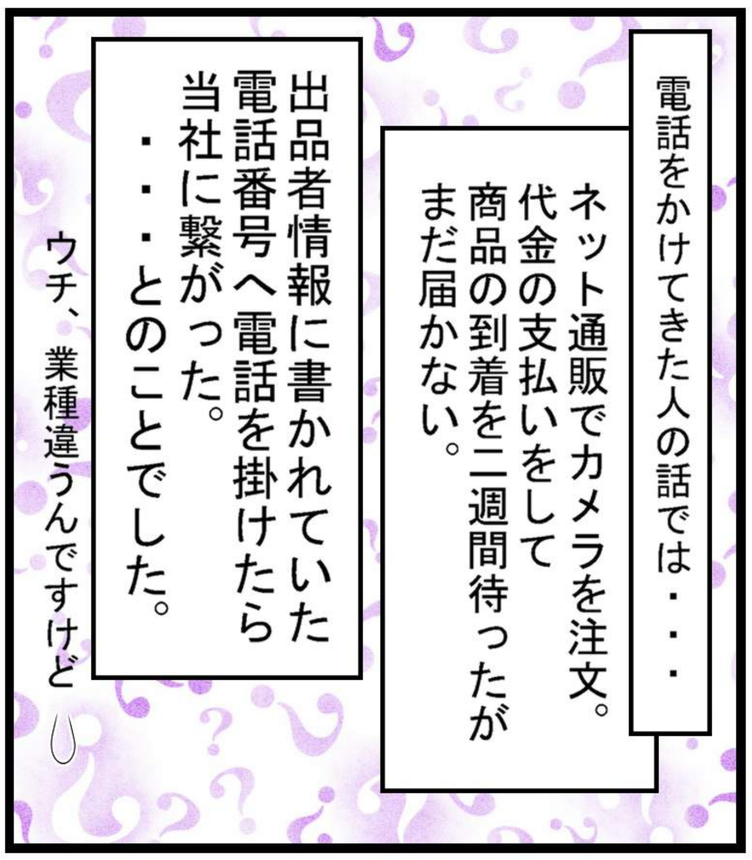
【ウェブサイト・サーバ管理者の方へ】

CMSなどのウェブサイト構築等に使用されるソフトウェアの脆弱性を突いた攻撃の特徴として、ウェブサイトを構成するファイルに不正なコードを埋め込み、サイト閲覧者を別サーバへアクセスさせ、マルウェア感染させる場合があります。

原因調査に当たられる際、公開ディレクトリ内に不審なファイルが置かれてはいないか、CMSディレクトリ下のファイルに難読化されたコードが埋め込まれていないか、ウェブアクセスログにコマンドインジェクションなどが疑われるPOSTログがないかなどの確認をお願いします。

CMS：コンテンツマネージメントシステム（Webサイトを管理・更新できるシステム）
POSTログ：POSTメソッドのログ（HTTP通信でWebブラウザなどからサーバへ送るリクエストの種類の一つ）

ウェブサイト情報が 無断流用 されていたら



対処方法 1 2 3

1 問合せには自社が無関係であることを説明しましょう。

2 問題の通信販売サイトのURLや情報の掲載状況を確認しましょう。

3 ウェブサイト管理者へ連絡して注意喚起文の掲載を依頼しましょう。

警察への通報もしましょう。

偽った出品者情報などを掲載している通信販売サイトは、詐欺サイトです。
詐欺被害者の拡大や自社の風評被害を防ぐためにも、警察へ通報しましょう。

【警察への連絡先】
鳥取県警察本部内
警察総合相談電話　0857-27-9110
サイバー犯罪対策室　0857-23-0110（代表）
通報する際は、問題の通信販売サイトのURLや掲載内容などを事前に確認しておきましょう。

事例では、ウェブサイトから自社情報のみを盗用されたケースをご紹介しました。
ウェブサイトを運用する上では、「安全性」の確保に向けた対策を行う必要があります。
ぜひ裏面の「ウェブサイトを安全に運用するために」もご覧ください。

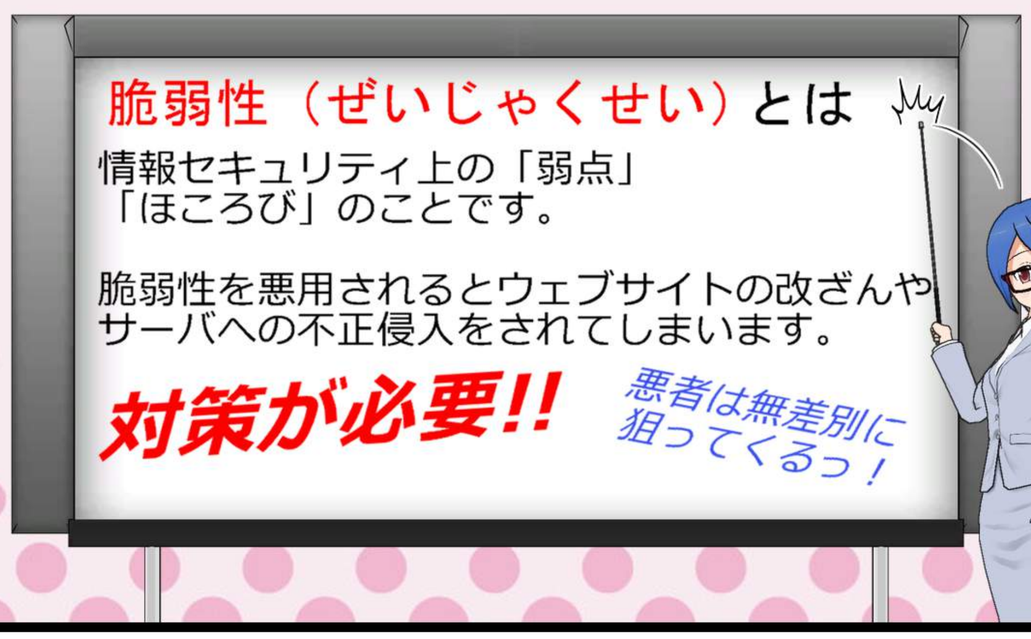
ウェブサイトを安全に運用するために

突然ですが、ご質問です。

あなたのウェブサイトに当てはまるものはありますか？

□ サイト利用者の個人情報をウェブ上で入力させている。
□ 個人情報やクレジットカード情報などの重要情報を、ウェブサーバ上で管理している。
□ 顧客等から預かった情報をウェブサーバや社内のPCに置くことがある。
□ 自社の重要情報をウェブサーバや社内のPCに置くことがある。
□ 自社のサイト上に以下のいずれか１つ以上の機能・画面がある。
　・ユーザ登録
　・登録済みユーザのログイン
　・ユーザによるフォームへの入力（問合せ、掲示板等を含む）
　・入力された情報の確認のための表示
　・ユーザへのメールの自動送信
　・サイト内の検索と結果表示
　・アクセスログやメール等の内容の画面表示
□ サイト構築に使用したウェブサイト構築用のソフトウェアが最新のバージョンではない。
□ ウェブサイトを構築した後でメンテナンスや修正を行っていない。

1つでも該当する項目があれば、ウェブサイトの脆弱性対策を行いましょう。



ウェブサイトの改ざん・不正侵入をされると・・・

個人情報や機密情報の漏えい
ウイルスをばらまく
詐欺サイトに作り替えられる
他のサイトへの攻撃に使われる

など、セキュリティ上の問題を引き起こして、顧客、取引先、他の企業などにも迷惑をかけてしまいます。

オンラインショップでは徹底した対策を！

☆ 個人情報、顧客情報等の重要な情報を預かっている
　安全な管理を怠って個人情報を流出させた場合、罰則の適用や顧客等から損害賠償を求められることがあります。

☆ ウェブサイトに脆弱性となりやすい機能がある
　ユーザ登録画面や入力欄フォーム等に脆弱性があると、不正侵入や情報の盗み出しに悪用される可能性があります。

☆ ウェブサイトの構築後にメンテナンスをしていない
　ウェブサイト構築用のソフトウェアが古いバージョンの場合、構築したウェブサイトに 脆弱性が残っていることがあります。

対策の第一歩

各種ソフトウェアの更新　最重要

ログのチェック　☜日頃、どんな攻撃を受けているかを知りましょう！

定期報告　☜委託契約内容に加えましょう！

技術的な対策は、ここには書ききれません。
システムが古いまま運用されていると、攻撃のターゲットにされてしまいます。
攻撃やターゲットを探すための通信も含めて、不審な通信は絶え間なく続いています。
定期的なログのチェックを行い、状況に応じた技術的対策を実施しましょう。

参考・引用
「安全なウェブサイト運営にむけて～企業ウェブサイトのための脆弱性対応ガイド～」
独立行政法人情報処理推進機構（IPA）

防犯カメラ映像が流出していたら

鳥取県内でもインターネットに接続するタイプの防犯カメラの映像が
意図せず海外サイトなどで公開されていた事例があります。

このタイプの防犯カメラは「ネットワークカメラ」と呼ばれています。
異常があった場合は、すぐにカメラの設置・管理者へ連絡しましょう。

カメラ＆ネットワーク設置・管理者の対処方法 1 2 3

1 ネットワーク設定の確認と
パスワードの変更

2 社内のネットワーク接続機器の
ネットワーク設定の確認

3 組織幹部への報告と助言

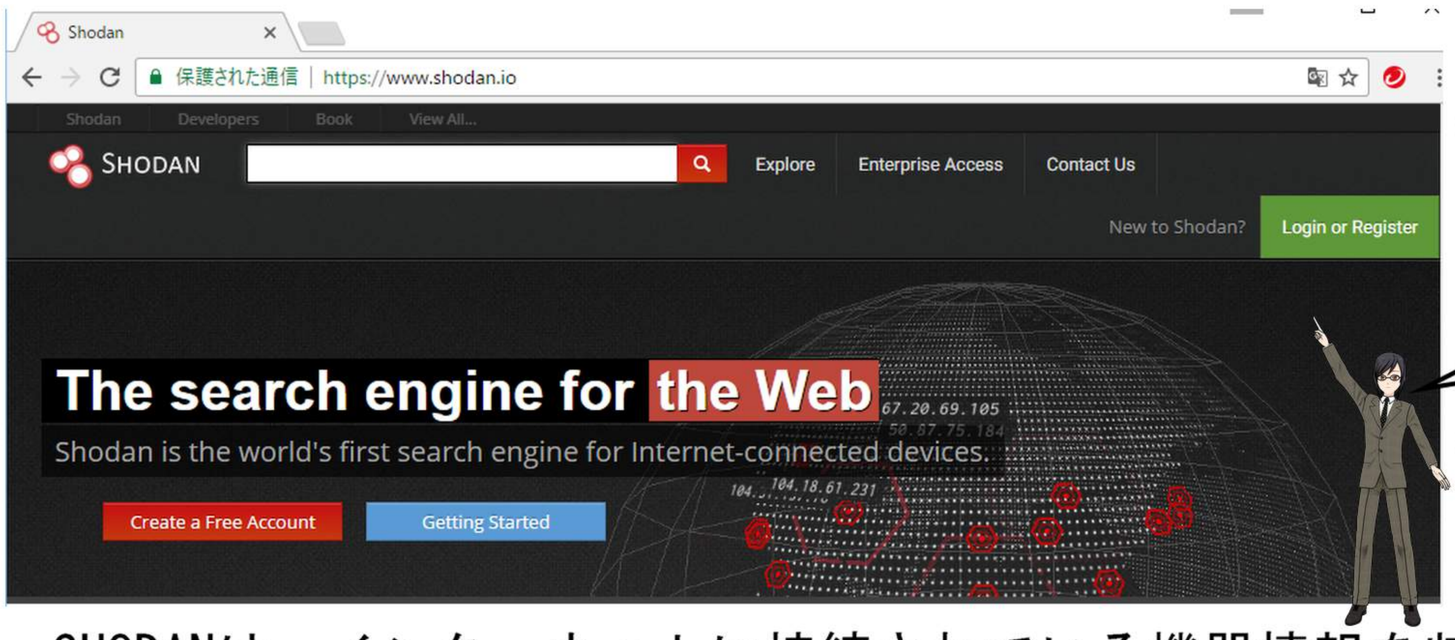
組織幹部の方へ

ネットワークカメラなどが不正アクセスされ悪用されるケースが増えています。
カメラへの接続に必要なパスワードが初期設定のままで運用されている場合が
最も狙われやすくなっています。

ネットワークカメラに限らず、ルーター、ネットワーク対応ハードディスク、
コピー機、テレビ、エレベーターなどネットワークに接続されているものすべて
が適切な設定で運用されているかを管理者と連携して確認してください。

裏面の関連コラムもご覧ください。

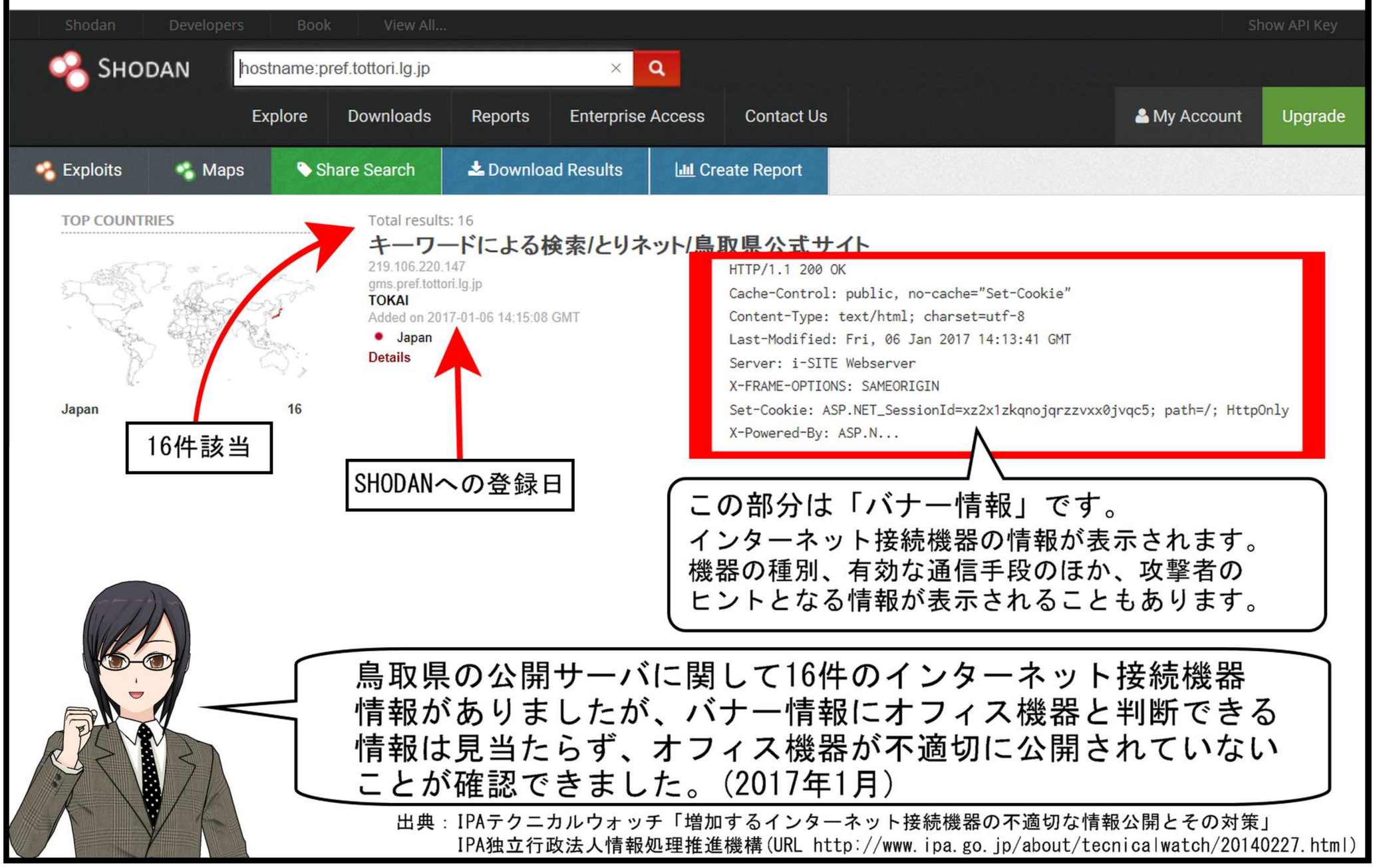
ネットワーク接続機器のチェック方法
（ネットワーク管理者向け）



SHODANのURLは
https://www.shodan.io
です。
アカウント作成は無料
です。

SHODANは、インターネットに接続されている機器情報を収集して公開しているウェブサイトです。
SHODANを利用して、自己が把握している以外の機器がインターネット上に公開されていないかを確認することができます。

IPアドレスで検索する場合の入力方法
「net:219.106.220.142」
ホスト名で検索する場合の入力方法
「hostname:pref.tottori.lg.jp」
※「とりネット／鳥取県公式ウェブサイト」の例です。
実際には、自組織のIPアドレス、ホスト名を入力してください。

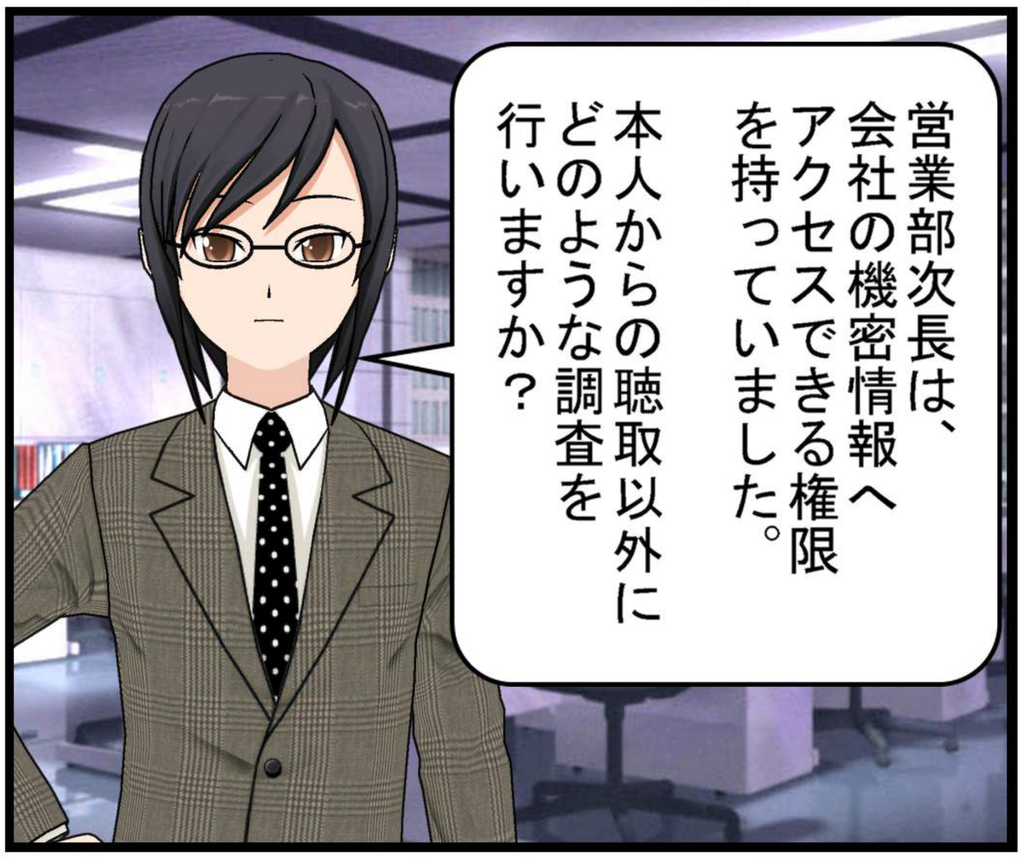


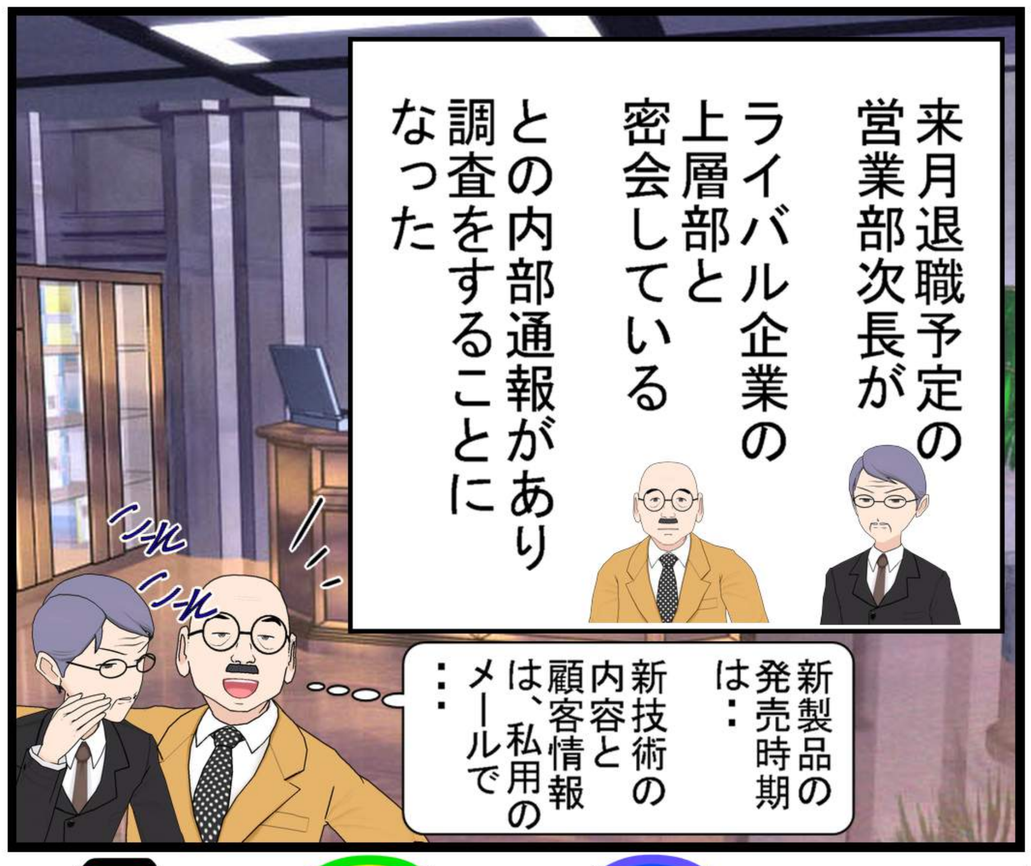
鳥取県の公開サーバに関して16件のインターネット接続機器情報がありましたが、バナー情報にオフィス機器と判断できる情報は見当たらず、オフィス機器が不適切に公開されていないことが確認できました。(2017年1月)

出典：IPAテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」
IPA独立行政法人情報処理推進機構(URL http://www.ipa.go.jp/about/tecnicalwatch/20140227.html)

把握していなかったインターネット接続機器、古いサーバなどを発見し設定の見直し、撤去などの対処をしましょう。

内部不正で秘機密情報が流出したら





対処方法 1 2 3

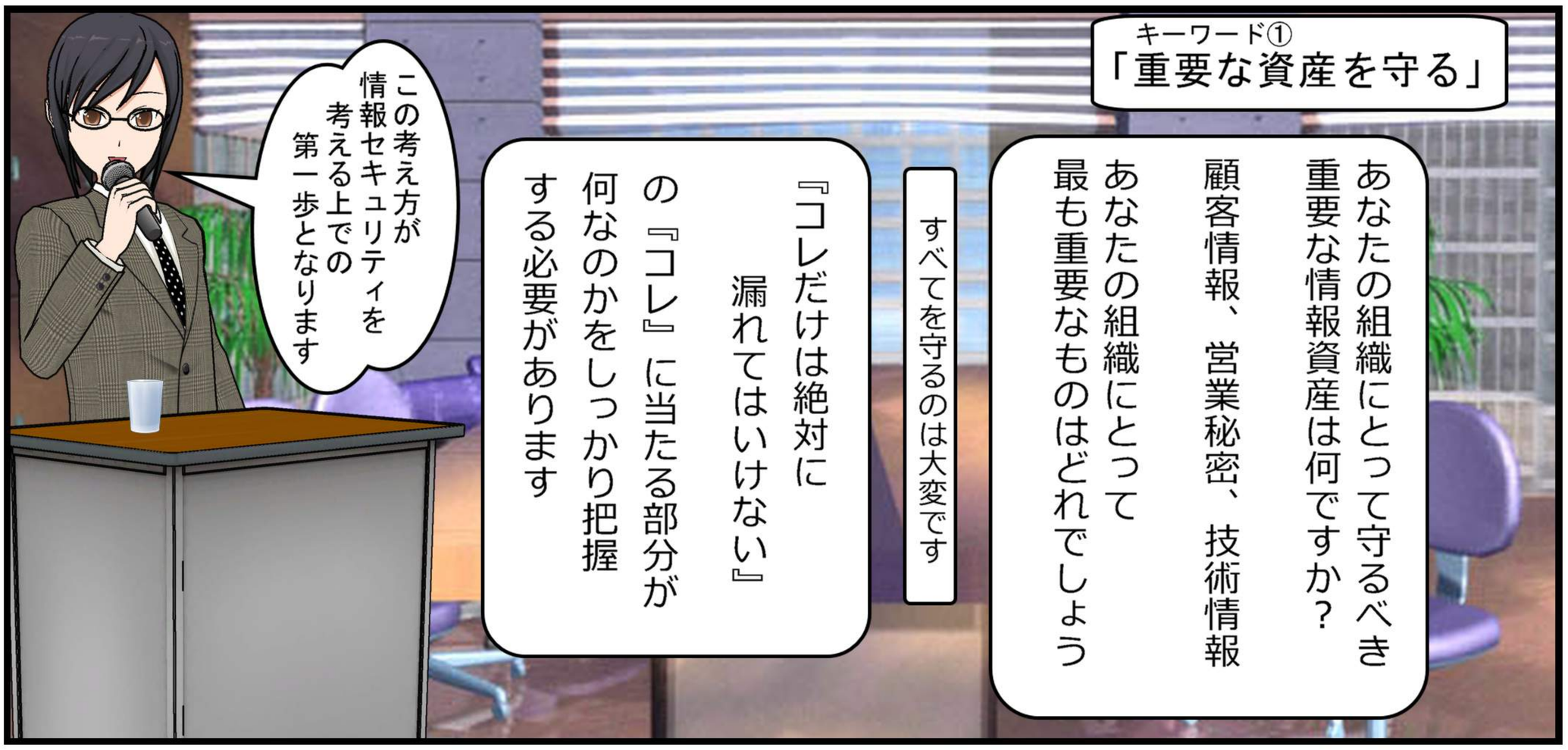
1. 情報機器及び記録媒体の持ち出し記録などの確認
2. 情報システムにおけるログ、データの確認
3. 証拠となり得るデータやログの保存と警察などへの提出準備

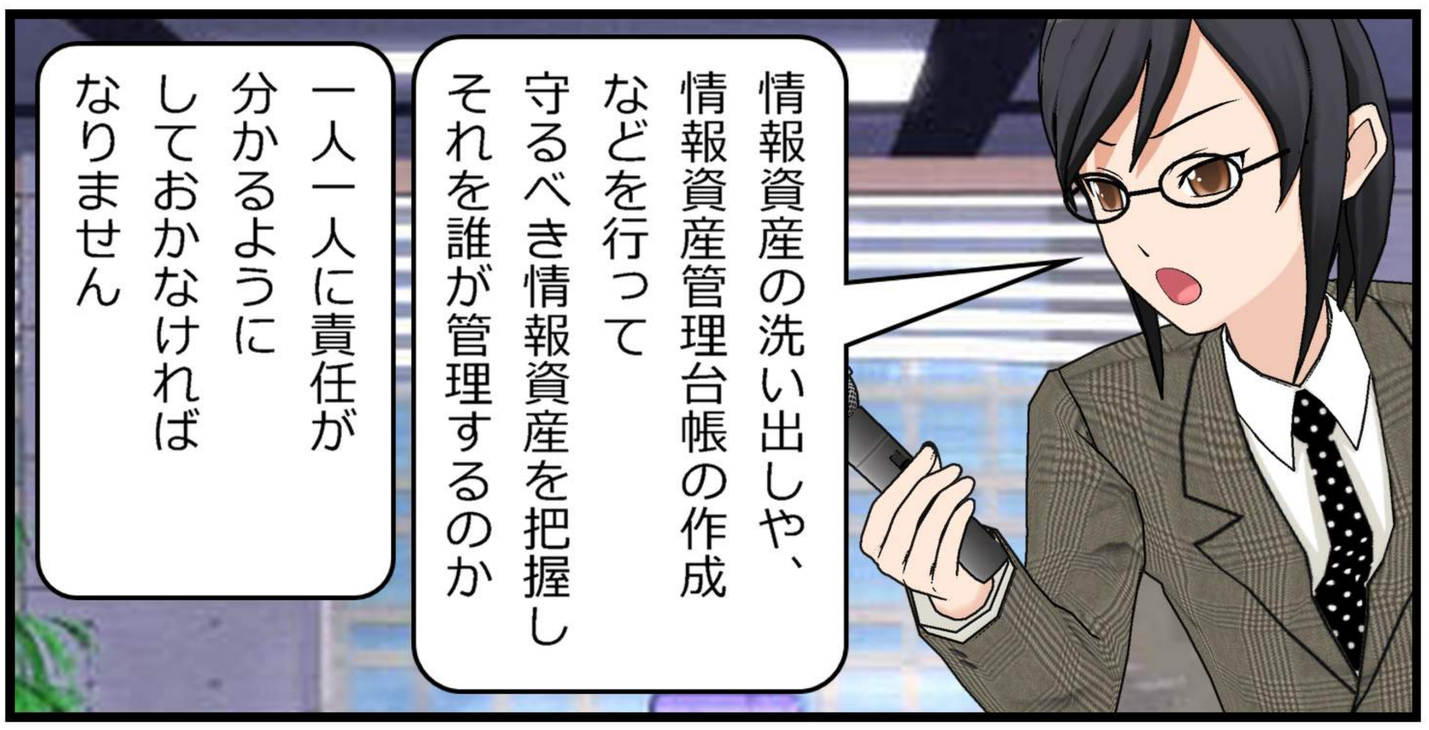
端末のデータやログの保存について

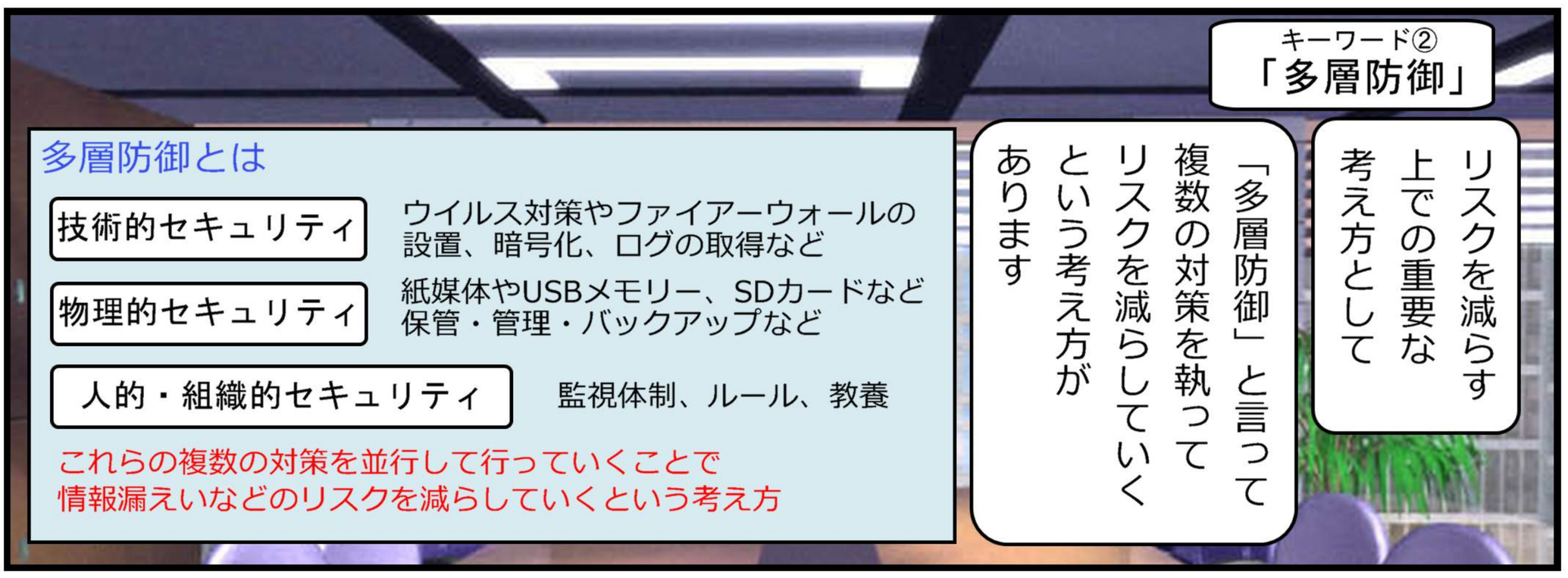
調査対象のPCやUSBメモリーの内容を保全しておくためには、出来る限り対象物の物理コピー（イメージコピー）をしましょう。

組織の情報セキュリティについて裏面もご覧ください。

情報資産を守るために
～　大切な二つのキーワード　～





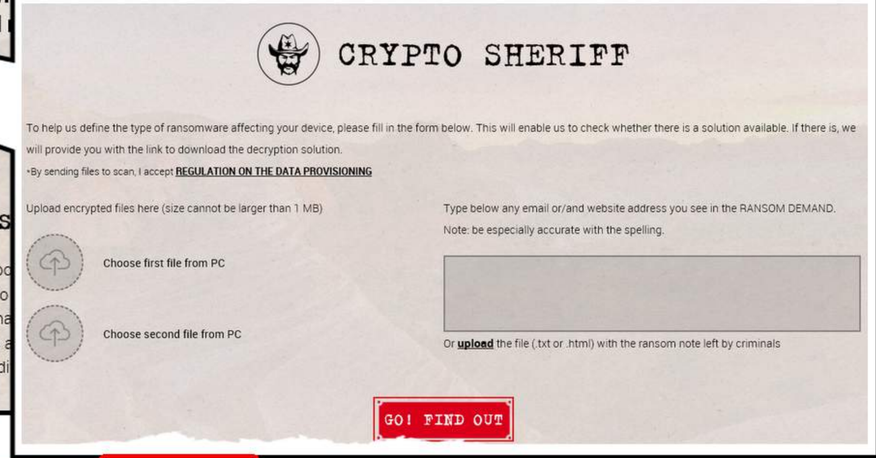


個人情報漏えい問題の多くは、人為的ミスが原因となっています。
技術的な対策だけではなく、一人ひとりの情報への関与の仕方などのルール決めといった「人の対策」を並行して推進しましょう。
このルールのことを「セキュリティポリシー」と言います。

参考
鳥取県サイバーセキュリティ対策ネットワーク
人材育成セミナー「組織の情報セキュリティ」
講師　独立行政法人情報処理推進機構（IPA）
石田淳一　氏
日時　２０１６年５月２０日（金）
於　鳥取県警察本部５階大会議室

付録①　ランサムウェア対策サイト「NO MORE RANSOM！」のご紹介

https://www.nomoreransom.org/



「NO MORE RANSOM」は
欧州刑事警察機構(ﾕｰﾛﾎﾟｰﾙ)内に設置されたサイバー犯罪対策の専門機関「欧州サイバー犯罪センター」と民間IT企業などによって立ち上げられたランサムウェア対策サイトです。
暗号化されて開けなくなったファイルの復号化ツールを提供しています。

※　紙面の都合上、一部省略しています

YES をクリックすると、暗号化されたファイルを診断し、ランサムウェアの種別を診断するページへ切り替わる

NO をクリックすると、ランサムウェアの情報が表示される

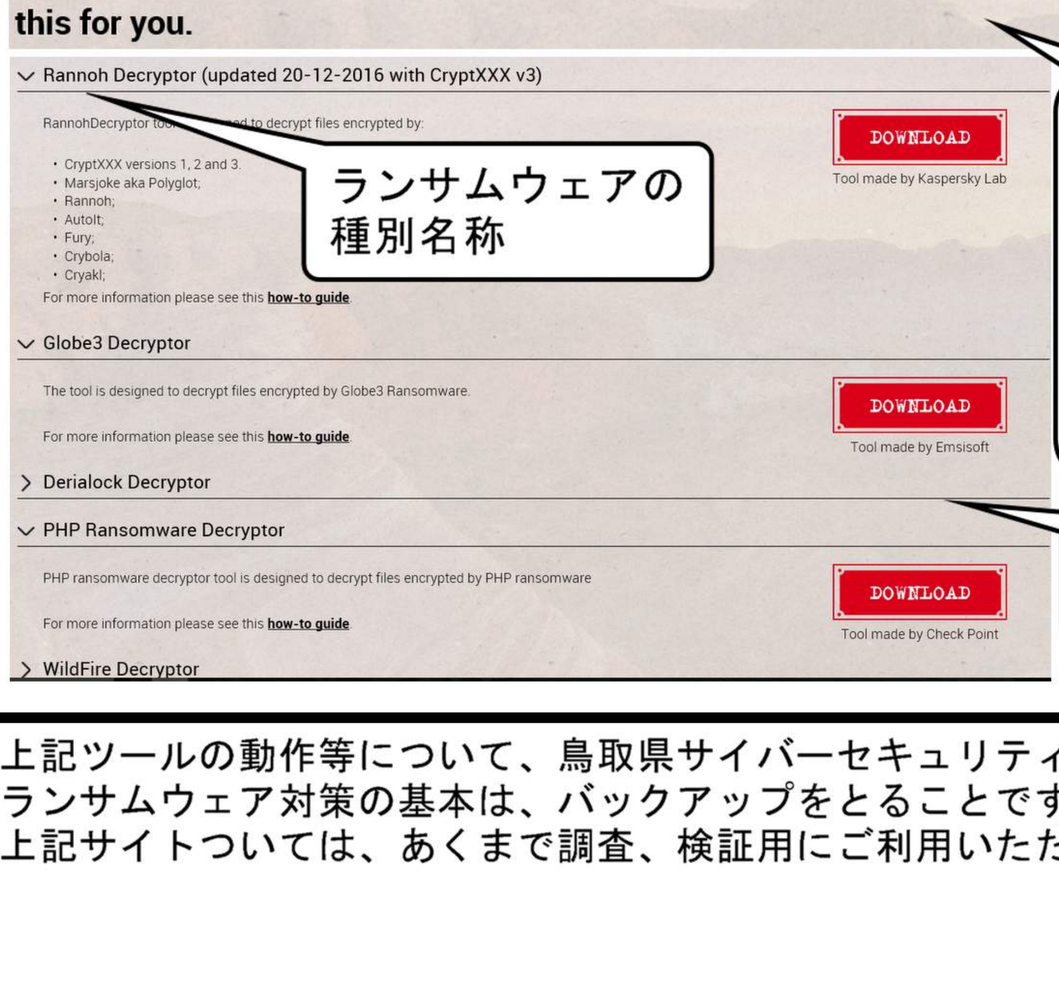
ランサムウェアの種別に応じた複合ツールをダウンロードします。

各復号ツールのダウンロード先

DECRYPTION TOOLS

復号ツールダウンロードページ

IMPORTANT! Before downloading and starting the solution, read the how-to guide. Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files. Any reliable antivirus solution can do this for you.



ランサムウェアの種別名称

重要！
ツールをダウンロードし問題解決にあたる前に「how-to guide（手引き）」を読んでください。
まずは、システムからマルウェアを削除してください。
削除しなければ、繰り返し暗号化されてしまいます。
信頼性の高いセキュリティ対策ソフトであれば、マルウェアを削除することができます。

ダウンロードできるツールは２０種類以上

上記ツールの動作等について、鳥取県サイバーセキュリティ対策ネットワークが保証するものではありません。
ランサムウェア対策の基本は、バックアップをとることです。
上記サイトついては、あくまで調査、検証用にご利用いただきたくご紹介するものです。

付録②　システムは最新？！「MyJVNバージョンチェッカ」のご紹介

http://jvndb.jvn.jp/apis/myjvn/vccheck.html

最終更新日：2016/12/21

JVN iPedia　脆弱性対策情報データベース

MyJVN >> 一般利用者の方へ >> MyJVN バージョンチェッカ

| 概要 | 利用方法 | 動作環境 | 対象ソフトウェア製品 | よくある質問と答え（FAQ） |

MyJVN バージョンチェッカ

概要

MyJVN バージョンチェッカは、利用者のPCにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツールです。

MyJVN バージョンチェッカの利用の流れは、以下の 3 ステップとなります。
①MyJVN バージョンチェッカの起動
②チェック結果の確認
③バージョンが古い場合は最新バージョンに更新

MyJVN バージョンチェッカの起動

JRE がインストールされている場合には、お使いのOSに合わせて「MyJVN バージョンチェッカ起動」と表示されている部分をクリックすることで、MyJVN バージョンチェッカを起動できます。

JVN
HOME
JVNとは
脆弱性レポートの読み方
脆弱性サマリー一覧
VN-JP
VN-JP
脆弱性情報の届出

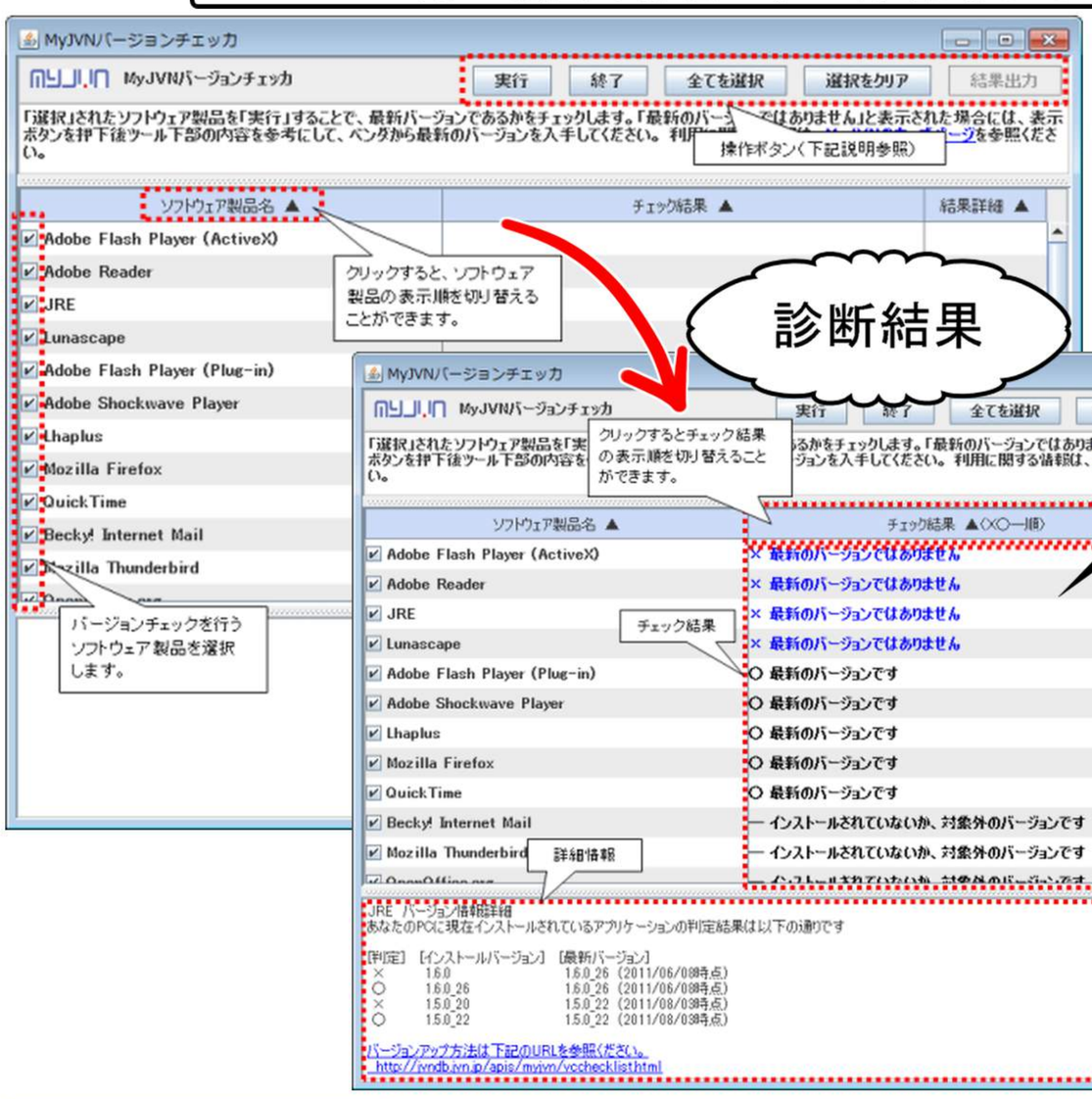
COMPATIBLE

OVAL ADOPTER oval.mitre.org

「MyJVNバージョンチェッカ」は、パソコン内の各種ソフトウェアのバージョンが最新の状態であるか否かを診断するツールです。

JVN は、"Japan Vulnerability Notes" の略です。日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトです。
脆弱性関連情報の受付と安全な流通を目的とした「情報セキュリティ早期警戒パートナーシップ」に基いて、2004年7月よりJPCERT コーディネーションセンターと独立行政法人情報処理推進機構(IPA)が共同で運営しています。
※　リンク先からの引用です。

※　紙面の都合上、一部省略しています



「最新のバージョンではありません。」と表示されたソフトウェアは安全のために更新する必要があります。

チェック結果	意味
○ 最新のバージョンです	インストールされているソフトウェア製品は IPA が確認している最新のバージョンであることを示しています。
× 最新のバージョンではありません	インストールされているソフトウェア製品は IPA が確認している最新のバージョンでないことを示しています。
― インストールされていないか、対象外のバージョンです	リストアップされているソフトウェア製品がインストールされていないか、古いバージョンのため、チェック対象外となっていることを示しています。

標的型メールや改ざんされたウェブサイトには、ソフトウェアの脆弱性を狙ったマルウェアが仕掛けられている場合が多くあります。
各ソフトウェアでは脆弱性を修正するためのバージョンアップが行われており、古いバージョンのままではマルウェア感染の危険性が高まります。
MyJVNバージョンチェッカを使って古いバージョンのままになっているソフトウェアを洗い出し、古いものが見つかれば、その都度、バージョンアップを行いましょう。

※　画像、説明文は上記サイト内の引用です。

MyJVNバージョンチェッカの詳しい利用方法は、上記サイト内に掲載されています。

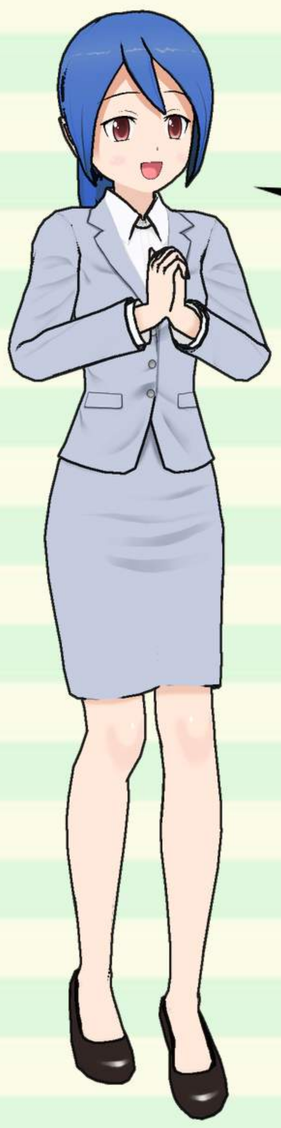
鳥取県サイバーセキュリティ対策ネットワークについて

鳥取県内のIT産業系団体・経済団体・教育機関・行政機関が協力して、
県内企業、自治体、学校、そして県民の皆様の生活や経済活動上の
ネット被害やトラブルを抑えていくための様々な取組を行っています。

現在、以下の団体・組織が参加しています。

一般社団法人鳥取県情報産業協会
鳥取県インターネットプロバイダ防犯連絡協議会
一般社団法人鳥取県法人会連合会
鳥取県経済同友会
鳥取県商工会議所連合会
鳥取県商工会連合会
鳥取県中小企業団体中央会
一般社団法人生命保険協会鳥取県協会
鳥取県金融機関防犯協議会
国立大学法人鳥取大学
公立学校法人公立鳥取環境大学
学校法人藤田学院鳥取看護大学
学校法人藤田学院鳥取短期大学
独立行政法人国立高等専門学校機構米子工業高等専門学校
鳥取県
鳥取県教育委員会
鳥取県警察本部（事務局）

【平成29年７月現在｜順不同】



各参加団体・組織が協力して、
・ 情報セキュリティに関するセミナーの開催
・ サイバー犯罪被害防止などに関する情報提供
・ 情報モラルなどに関する広報啓発活動
を展開しています。

自治体、経済団体、学校など県民の皆様にとって、馴染みの深い団体・組織が情報発信やセミナー参加の窓口となっています。

お問い合せ
鳥取県警察本部生活安全部生活環境課
サイバー犯罪対策室（事務局）
電話　0857-23-0110(代表)

又は、身近な参加団体を通じて
お問い合わせください。

原作・原案：鳥取県サイバーセキュリティ
対策ネットワーク

作　　画：鳥取県警察本部

※ご使用上の注意事項
営利の目的としない使用に限ります
表紙・本題・解説部分とも、改編は一切行わないでください
ロゴやキャッチコピー等の追加も一切行わないでください