Expand - Collapse

- Sec01-08-3 相談対応手順書（マニュアル）
  - 【2018年7月4日】資料送付手続き更新
  - 目的
    - 具体的な相談対応時の回答の均質化を目指す
  - 相談受付対応手順
    - 用件のカテゴリの確認
      - 相談か？
      - 資料請求か？
    - 何の相談か？二次対応へのディスパッチ
      - どんな事象が起きているのかの概要を確認
      - セキュリティ被害の可能性がある⇒【緊急】へ
      - セキュリティ対策に不安がある⇒【平時の備え、啓発】へ
      - セキュリティ以外の相談⇒【セキュリティ以外】へ
      - 資料請求の場合
  - **クイックリスト掲載案件の相談対応手順**
    - 相談のきっかけ
      - どこでこの窓口を知ったか？
      - 既にどこかに相談したか？
    - 正確な状況把握のために相談者の立場を確認
      - 相談者は経営者か？システム管理者か？一般の従業員か？
        - セキュリティ担当者、システム管理者から状況を聞く
        - システム管理者がいない場合は、運用保守支援業者がいるか確認
    - 【緊急】どんな環境で何が起きているかを確認
      - まずは落ち着いて今起きている事象を確認しましょう
      - セキュリティ問診票「『やられたかな？その前に』ガイド～ 『やられてる』！と思ったら ～」【ISOG-J】(pdf形式)
    - 緊急
      - 【緊急】セキュリティ侵害の可能性があるが、どこに問い合せていいかわからない?
        - どんな相談か？
        - 【相談】セキュリティ関連の各種相談、問合せ窓口の紹介
        - 「サイバーセキュリティ相談・届出先クイックリスト」を参考に
      - **【緊急】情報の漏えい・改ざんが起きているようだ（ウィルス感染、不正アクセス、改ざん、データ喪失、情報漏えい等）**
        - どんな被害か？

Expand - Collapse

- ウイルス感染？
- Webサーバ改ざん？
  - izumino.jp/Security/def_jp.htmlで改ざん情報が挙がっているか確認
  - www.aguse.jpでサーバの仕様を確認
  - wget等でhttpdのデーモン名、バージョン等を確認
  - ・・・
  - 緊急対応
    - 【窓口回答】【ガイドブック】P.140「改ざん・消失・破壊・サービス停止発生時の対応」を紹介
    - 【相談】「情報セキュリティ事故対応ガイドブック（情報セキュリティ大学院大学）等」に沿って対応の流れを助言
- 情報漏えい・流出？
  - ・・・
  - 緊急対応
    - 【窓口回答】【ガイドブック】P.138「情報漏えい・流出発生時の対応」を紹介
    - 【相談】「情報セキュリティ事故対応ガイドブック（情報セキュリティ大学院大学）等」に沿って対応の流れを助言
- 犯罪の可能性がある場合は
  - 【相談】内容が高度な場合は、警視庁サイバー犯罪対策課
  - 【届出】内容が比較的単純な場合は、被害の証拠を揃えて、所轄の警察署
- 対応策の相談の場合は
  - 【相談】IPA情報セキュリティ安心相談窓口
- 実被害にあった場合は
  - 同様の被害を拡大させないために
  - ウイルス・不正アクセス届出
    - 【届出】IPAセキュリティセンター
  - インシデント報告・届出
    - JPCERT/CC

- **【緊急】なりすましECサイト被害**
  - 実被害者は顧客
  - 【相談】なりすましECサイトを立ち上げられた事業者からの相談
    - なりすましECサイト対策協議会のHPを紹介
      - サイト内の「なりすましECサイト対策マニュアル」を参照
      - サイト内に注意喚起のお知らせを掲載
      - 問合わせ対応用文書の作成【例文あり】

Expand - Collapse

- なりすましECサイトのプロバイダーに削除要請【例文
- 顧客に対して
  - 【届出】被害の証拠を揃えて、所轄の警察署へ
- 【相談】なりすましECサイトと知らずに取引をした利用者からの相談
  - 消費者ホットライン（国民生活センター）を紹介
- 実被害にあっている場合
  - 【届出】被害の証拠を揃えて、所轄の警察署へ
- なりすましECサイト標準回答
  - ●緊急対応
    - 他のお客様の被害が拡大しないように、また、他の利用者からの苦情に対応するために、「なりすましECサイト対策マニュアル」に従って、対応することをお勧めします。
    - ☆なりすましECサイト対策協議会
      - https://www.saferinternet.or.jp/narisumashi/
      - 「なりすましECサイト対策マニュアル」
      - https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf
    - 具体的には、
    - ①問い合わせ対応
      - 顧客対応からの問い合わせに対しての文面例
      - http://www.saferinternet.or.jp/system/wp-content/uploads/template002.docx
      - 実被害者は、偽サイトで振り込んでしまった方ですので、被害者の所轄の警察署に被害届を出すように促してください。
    - ②被害拡大防止
      - サイト内等で、他の利用者に対して注意喚起してください。
      - http://www.saferinternet.or.jp/system/wp-content/uploads/template001.docx
    - 実例として、下記のようなページがあります。
      - 「当店と誤認させるようなウェブサイト（なりすましECサイト）について」
      - https://namaenouta.jp/docs/attention.html
  - ●風評被害について
    - 「なりすましECサイト対策マニュアル」に従って、自社サイトで利用者に注意喚起等を行うことによって、「ユーザー（お客様）が逆に怖がってしまう」という事例は聞いていません。偽サイト、偽メールを騙られた多くのサイトは、マニュアルにあるような対応を取っています。

Expand - Collapse

- 他に被害が拡大しないようにすることが、正規のECサ
あり、お客様への注意喚起を含めて、マニュアルに記載されているような対策を講じることにより、説明責任を果たすことで、社会的信用の喪失を防げると思います。
- このような処置をきちんと行うことにより、セキュリティ意識のあるECサイトとして、逆に信頼に繋がると思います。

- ●相談及び届出
  - 犯罪の可能性のある相談窓口は、警視庁サイバーセキュリティ犯罪対策課（03-3431-8109）であり、お掛けになった電話番号でよろしいと思いますが、相談が多く混み合っているものと思われます。
  - なりすまされたECサイトからの被害届を、警察が受理し立件できると判断するかは難しいところです。
  - なりすまされたECサイトの被害として、
  - 著作権法違反、商標権侵害、不正競争防止法違反、詐欺罪等の法令違反の可能性はありますが、なりすまされたECサイトの被害を立証できる証拠を揃えることが困難なのが実情です。

- **【緊急】「ビジネスメール詐欺」により偽振込先に振り込んでしまった**
  - 2017年JALでの実被害
  - 【相談】法的にどんな対応ができるか？
    - 【相談】法テラスに相談
    - 自社と取引先のどちらにも損害賠償責任があり得る
  - 【届出】被害の証拠を揃えて、所轄の警察署へ
  - 【相談】再発防止のために何をすればいいか
    - 【例】日経コンピュータ記事
      - 自社と取引先のどちらかのメールへの不正アクセスが発端
      - ①職員全員に詐欺メールの手口を周知
      - ②偽口座に振り込んだと気が付いたら即座に銀行に連絡、送金を止められる可能性がある
      - 事前にメールを盗み見られている可能性があるので、当該職員のメールアカウントをリセット
      - メールシステムのログインは2段認証、異なる端末からのログイン警告等を導入
      - ③原因追及の体制を整えておく
        - 自社のメールに不正アクセスがなかったかどうかの分析・証明で自社を守る
    - 【相談】IPA情報セキュリティ安心相談窓口に相談
    - 【届出】フィッシング対策協議会のサイトで届出

- **【緊急】実在する企業名で架空請求を受けた場合**

Expand - Collapse

- 身に覚えのない請求の場合は、くれぐれも相手に連絡をとっ
  じたりしない
- 不安な方や不審な点のある方
  - 【相談】消費者ホットラインに相談
  - 【相談】所轄の警察署生活安全課に相談
- 【届出】フィッシング対策協議会のサイトで届出

【緊急】PC、スマホの動きがおかしくなった、データが壊れたようだ

- 【相談】PCベンダー、プロバイダー、販売店等、保守業者に問い合せることを助言
- その他

平時の備え

情報セキュリティ侵害に遭わないように事前に何をすればいいか

- まず「中小企業向けサイバーセキュリティ対策の極意」の入手（ダウンロード）し、内容を確認することを助言
- 内容を確認後、不明な点があれば、再度相談を受け付ける

より詳細な対策内容を知りたい場合は

- 内容を確認し、「相談対応のためのハンドブック（手持ち参考資料）」に記載の参考文献、Webサイト、セミナー等を紹介する

これから検討の標準回答

- 情報セキュリティーのための投資については、全てのリスクに対して技術的対策をすることは困難。
- セキュリティー被害を受けた場合、その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要になることを考えること。
- また、システムを入れる際に、セキュリティーも同時に入れるなど、ITとセキュリティー対策を一緒にすることも大切である。
- 更に、経営者を含め、社員全員に対し、セキュリティーポリシーや【ガイドブック】を作成したり、併せてITパスポートの試験を受けさせることも大切である。

啓発（教育・学習）

- 情報セキュリティ対策の必要性を認識し、網羅的な対策を知るには？
- まず「中小企業向けサイバーセキュリティ対策の極意」の入手（ダウンロード）し、内容を確認することを助言
- 「相談対応のためのハンドブック（手持ち参考資料）」に記載の参考文献、Webサイト、セミナー等を紹介する

セキュリティ以外

消費生活全般に関する苦情や問合せ

- 【相談】消費者ホットライン

Expand - Collapse

- 嫌がらせ、ネットストーカー
  - 【相談】所轄の警察署の生活安全課
- 人権侵害
  - 【相談】みんなの人権110番
- 個人情報の取り扱い
  - 【相談】個人情報保護委員会

- 資料請求
  - 資料送付基準に合致しているか確認
    - 都内の中小企業事業者か？
    - 営利目的ではないか？
  - 必要部数の確認
    - HPでPDF版をダウンロードできるようになっているのでそちらも活用できる
    - 10冊以内なら無料で送付
      - FAXで送付先を送ってもらう
      - ゆうパックで、郵送依頼書とともに管理へ
        - 郵送依頼書の明細欄は、数量とサイズを記入（単価は不要）
        - 封筒は、60サイズ
        - 50冊段ボール箱は、80サイズ
    - 11冊以上は、取りに来ていただく。無理な場合は着払いで送付
      - FAXで送付先を送ってもらう
      - ゆうパック（着払い）で郵便局に持ち込み
    - 50冊（1箱）以上で、後納の場合
      - 受付
        - FAXで送付先受領
          - FAX番号:03-5388-1461
        - FAXがない場合は、下記の操作を伝え、電子申請での受け付ける
          - Googleで検索「東京都 サイバーセキュリティ 電子申請」
          - 検索結果上位の「東京都電子申請 中小企業サイバーセキュリティ対策相談」
          - 相談入力フォームまで画面遷移して、送り先を入力してもらう
      - 送付準備
        - 送り先確認
        - 送り状作成（PCで作成可）
        - 郵送依頼票に記入、押印
          - 単価、金額は記載不要。備考にサイズ記入

Expand - Collapse

- 50冊は80サイズ、100冊は100サイズ

料金後納郵便物差出票に、氏名、個数を入力して、2部プリントアウト、押印

- ¥¥Fv2710¥調整課¥調整課内共有¥!!!!!!!!!後納郵便

管理へ

- 郵便ビズカード借用

郵便局へ

- 料金後納郵便物差出票1部返却受領
- 後納郵便物等取扱表を受領

管理へ

- 郵送依頼票提出
- 料金後納郵便物差出票提出
- 後納郵便物等取扱表提出

控え

- 先方からの依頼FAX等
- 送り状控え

【ガイドブック】に沿った案件別FAQ

作成方法

- 【ガイドブック】のMission1をベースに事象別で分類
- 過去の相談記録、【ガイドブック】、事前調査資料等に基づいて、内容を分類して汎化したQ＆Aを作成し、相談対応者用手元資料の１つとする【相談回答の均質化】
- 提示する対策は、Misson2～4をベースに。また、IPA等の参考情報サイトも合わせて提示。
- Q&A項目毎に、分類（キーワード）、質問例、回答例（対応策、ナビゲーション先）、参考にした情報、質問者に参考になる情報の所在場所等を記述し、端末で検索可能なものとする

01.個別サイバーセキュリティ事象の相談【Mission１】

- 01.セキュリティ事象全般

02.迷惑メール・スパムメール

迷惑メールが届いている。セキュリティ対策ソフトから警告メッセージが出て迷惑メールフォルダーに残っている。このPCは安全か？

- メール本文や、添付ファイルを開いていなければ大丈夫と思われる
- 削除して、ごみ箱を空にする

成りすましと思われるメールが来ている

- 相手に連絡をしたり、要求に応じない

スパムメールが頻繁に届くようになった

Expand - Collapse

- プロバイダにスパムメールのメールアドレスを通知
- 最悪の場合は、メールアドレスを変更
- 【相談】IPA情報セキュリティ安心相談窓口に相談

サイバーセキュリティではないが、迷惑FAXが多いが、回避方法は？

- 電話番号による受信拒否
- 受信時の紙出力の停止

03.標的型攻撃による情報流出

- 【ガイドブック】P.18 を紹介

組織第1位　標的型攻撃による情報流出

- 企業や民間団体や官公庁等、特定の組織を狙う、標的型攻撃による攻撃が引き続き発生している。メールの添付ファイルやウェブサイトを利用してPCにウイルスを感染させられると、別のPCに感染を拡大され、最終的に個人情報や業務上の重要情報が窃取される。
- 【窓口回答】【ガイドブック】P.34,P.64 を紹介
- 【相談】IPA情報セキュリティ安心相談窓口へ

標的型メール標準回答

- 標的型メールは、業務や個人に関係しそうな内容を装ったメールを送り、信用させて、メールの添付ファイルを開かせてウイルスに感染させたり、メール内のURLを開かせて悪意のあるサイトや偽サイトに誘導させるもの。
- 対策としては、通常のセキュリティ対策が行った上で、特に、従業員が、不審なメールであることに気が付くことが重要。通常受け取らないメールを受信した時、その送信元、内容を確認し、少しでも不審を持った場合は、絶対に開かない。どうしても業務上内容を確認する必要がありそうな場合は、送信元に偽装メールでないことを確認することを徹底させる

ケース1

- ■緊急対応として
  ・まず、最新のウイルス対策ソフトで感染の確認を行ってください。
  ・現在まだウイルス対策ソフトで検知できないウイルスに感染している可能性もあるので、数日後に再度確認してください。
  ■ウイルスに感染していた場合
  ・もし感染しているようでしたら、全端末もネットワークから切り離して、ウイルスチェックをするとともに、感染していた場合は駆除してください。
  ・ウイルスの種類によって、どのような被害があるか、そのあとの対応として何をすべきかが変わってきます。
  ●ウイルス届出
  IPAセキュリティセンターのウイルス届出窓口に連絡してください。
  電話：03－5978－7518
  ■今後のための暫定対策
  最低限の対策として、全職員「情報セキュリティ5か条」等を読んで、気を

Expand - Collapse

付けるようにしてください。
http://www.ipa.go.jp/security/keihatsu/sme/guideline/
被害に遭っても、原状復帰できるように、日頃、重要なファイルは外部ハードディスクにバックアップして、ネットワークから切り離しておくことも重要です。
■恒久的対策
・事前の必要最低限の対策にはそれほどの費用が掛かりませんが、被害にあってから対応しようとすると相当大きな費用が掛かる可能性もあります。
・様々なセキュリティ上のリスクに対応するために、情報セキュリティ対策のルールを明文化して、役員を含めて全職員がルールを遵守していることを定期的に確認してください
対策の参考として、最近公開された資料として
中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】
http://www.ipa.go.jp/security/keihatsu/sme/guideline/
があります。

- ケース2
  - １　不審と思われるメールの見分け方
    昨今の標的型メールは巧妙化しており、見分けるのが非常に困難となっておりますが、一般的な注意点は以下のとおりです。
    ・日本語の言い回しが不自然なメール
    ・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異なるメール
    ・これまで届いたことがない公的機関からのお知らせ
    ・心当たりがないが、興味をそそられる内容
    ・心当たりのない決済や配送通知
    ・自分に送られてくることがおかしいメール
    ・件名に「緊急」など、ことさらに添付ファイルの開封を促すメール
    ・日ごろメールで」やり取りすることのない種類のファイルが添付されているメール
    ・ＩＤやパスワードなどの入力を要求する添付ファイルやＵＲＬが記載されたメール
  - ２　不審と思われるメールを受信した場合の「よりベスト」な対応方法
    不審なメールは開かないことが一番です。
    また、不審と思われるメールが届いた場合、社内のセキュリティ管理者に速報するよう、意識づけておくことが大切です。
  - ３　万一、開いてしまった場合の対応方法
    ランサムウェア等に感染してしまった場合、ネットワーク上の他の端末に影響を及ぼすことがあることから、当該端末をネットワークから切り離す事が必要です。
    とはいえ、こうした場合、問題が発覚した時にはすでに手遅れとなることが考えられます。
    特にランサムウェア等の被害を受けた場合、端末内の情報を暗号化され

Expand - Collapse

てしまうことから、事前の対策として、重要データのバッ
組みを導入し、いざという場合に備えることをお勧めします。

４　不審メールを開かないためのより実践的で具体的な取り組み（他社の例などご教示いただければ幸いです。）

実際の企業さんの取組みについては、申し訳ありませんが、こちらで取りまとめた資料がなく、ご紹介ができません。

不審メールを開かないための取組みについては、いかに社員一人一人に意識付けをするかに尽きます。

しかし意識の低い方は一定数存在しますし、意識していても、人間ですので間違いがありますから、１００%の対策を取るのは事実上不可能です。

３のご回答でもご説明しましたが、攻撃を防止する対策を講じるとともに、攻撃を受けてしまった時の対策（バックアップなど）を確実にしておくことが必要かと思います。

６　その他、標的型攻撃メールについて留意すべき事項などがありましたら、ご教示いただければと思います。

東京都では、サイバーセキュリティに関する【ガイドブック】を発行した。

そのほかにも、ＩＰＡで公開している下記サイトが参考になるかと思いますのでご確認ください。

・ここからセキュリティ
https://www.ipa.go.jp/security/kokokara/

・ランサムウェアの脅威と対策 ～ランサムウェアによる被害を低減するために～IPA
https://www.ipa.go.jp/files/000057314.pdf

- 04.ビジネスメール詐欺
  - 【例】2017年JALでの実被害
  - 組織第3位　ビジネスメール詐欺
    - 「ビジネスメール詐欺」（Business E-mail Compromise：BEC）は巧妙に細工したメールのやりとりにより、企業の担当者を騙し、攻撃者の用意した口座へ送金させる詐欺の手口である。詐欺行為の準備としてウイルス等を悪用し、企業内の従業員の情報が窃取されることもある。これまでは主に海外の組織が被害に遭ってきたが、2016年以降、海外取引をしている国内企業でも被害が確認されている。
    - 【窓口回答】【ガイドブック】 P.18を紹介
    - 【届出】被害の証拠を揃えて、所轄の警察署へ
    - 【相談】IPA情報セキュリティ安心相談窓口に相談
    - 【届出】フィッシング対策協議会の届出受付メールアドレス（info@antiphishing.jp）に、メールを転送、もしくは、フィッシングメールのタイトル、本文、差出人名、送信日時、概要などを記載の上、送信する
  - 【相談】法的にどんな対応ができるか？
    - 【相談】法テラスに相談

Expand - Collapse

- 自社と取引先のどちらにも損害賠償責任があり得る
- 【届出】被害の証拠を揃えて、所轄の警察署へ
- 【相談】再発防止のために何をすればいいか
  - 【例】日経コンピュータ記事
    - 自社と取引先のどちらかのメールへの不正アクセスが発端
    - ①職員全員に詐欺メールの手口を周知
    - ②偽口座に振り込んだと気が付いたら即座に銀行に連絡、送金を止められる可能性がある
    - 事前にメールを盗み見られている可能性があるので、当該職員のメールアカウントをリセット
    - メールシステムのログインは2段認証、異なる端末からのログイン警告等を導入
    - ③原因追及の体制を整えておく
      - 自社のメールに不正アクセスがなかったかどうかの分析・証明で自社を守る
  - 【相談】IPA情報セキュリティ安心相談窓口に相談
  - 【届出】フィッシング対策協議会のサイトで届出

05.マルウェア（ウイルス）による被害

051.ウイルス感染

- 無料のウイルス対策ソフトを導入しているがそれだけで大丈夫か
  - 無料でもウイルス対策はできる
  - 有償の対策ソフトは、Webサイトの閲覧、個人情報の流出防止も可能
    - 最近のアンチウイルス製品は、エンドポイント製品という表現に変わり、アンチウイルス機能だけでなく、エンドポイントレベルで必要とされる様々な対策が実装された統合型セキュリティを提供することが一般的。
  - 未知のウイルスもあり、対策ソフトを入れても感染する場合がある
  - 相手の手口や傾向を理解して、常に注意することが重要
- まだウイルスワクチンソフトで駆除できないマルウェアに感染した。どうしたらいい？
  - ネットワークから切り離す
  - 最新のソフトで除去を試みる
  - 感染した後の状況に応じて復旧を試みる
  - 完全に痕跡をなくすためには、PCの初期化が必要
  - 障害対応のために定期的にバックアップしておく

052.ランサムウェアを使った詐欺・恐喝

- 【ガイドブック】P.20 を紹介

Expand - Collapse

- 個人第2位 組織第2位　ランサムウェアによる被害
  - 　ランサムウェアとは、PCやスマートフォンにあるファイルの暗号化や画面のロックを行い、復旧させることと引き換えに金銭を要求する手口に使われるウイルスである。2017年は、OSの脆弱性を悪用し、感染した端末が接続しているネットワークを経路として感染を拡大させるタイプも登場している。また、感染した端末だけではなく、その端末からアクセスできる共有サーバーや外付けHDDに保存されているファイルも暗号化されてしまう。組織内のファイルが広範囲で暗号化された場合、事業継続にも支障が出る可能性がある。
  - 【窓口回答】【ガイドブック】P.20 を紹介
  - 【相談】IPA情報セキュリティ安心相談窓口へ
  - 【届出】被害の証拠を揃えて、所轄の警察署へ
  - ランサムウェア標準回答
    - ランサムウェアウイルスに感染し、暗号化させられて使用できなくなった場合、
    - 暗号化を解除するため、相手の要求金額を支払ったとしても、必ず暗号化を解除してもらえなかった事例も多々あると聞いていますので、ランサムウェアウイルスに感染させられないためにも、最新のセキュリティー対策ソフトを入れ、大切な情報はバックアップしておくことや、不審なメールやＵＲＬを開いたりしないよう指導教育を徹底すること。
- ケース1
  - １　ランサムウェアウイルスに感染し、暗号化させられて使用できなくなった場合、暗号化を解除するため、相手の要求金額を支払ったとしても、必ず暗号化を解除してもらえなかった事例も多々あると聞いていますので、ランサムウェアウイルスに感染させられないためにも、最新のセキュリティー対策ソフトを入れ、大切な情報はバックアップしておくことや、不審なメールやＵＲＬを開いたりしないよう指導教育を徹底すること。
    ２　標的型メールに対する注意すべきこと
    標的型メールは、業務や個人に関係しそうな内容を装ったメールを送り、信用させて、メールの添付ファイルを開かせてウイルスに感染させたり、メール内のURLを開かせて悪意のあるサイトや偽サイトに誘導させるもの。

    対策としては、通常のセキュリティ対策が行った上で、特に、従業員が、不審なメールであることに気が付くことが重要。通常受け取らないメールを受信した時、その送信元、内容を確認し、少しでも不審を持った場合は、絶対に開かない。どうしても業務上内容を確認する必要がありそうな場合は、送信元に偽装メールでないことを確認することを徹底させる
- ランサムウェアに感染したので調査業者を紹介してほしい
  - システム管理者、PC保守会社、PC購入元に確認
- ランサムウェアの危険性及び対策を教えてほしい

Expand - Collapse

- ウイルスか、外部からの侵入により、ファイルが暗号化
  めに、一定期間内に金銭を要求

- 対策
  - ウイルス対策ソフト、侵入防止機能の実装
  - ファイルを定期的にバックアップ、ネットワークから切り離し

053.アドウェアによる詐欺

- 個人第10位　偽警告⇒アドウェア等
  - 　PCやスマートフォンでウェブサイトを閲覧中に、突然「ウイルスに感染している」等の偽警告を表示し、利用者の不安を煽り、偽警告の指示に従わせ、個人情報等を窃取される被害が発生している。偽警告は本物の警告と誤認されるように巧妙な細工が施されており、被害者は信じて指示に従ってしまう。
  - 【窓口回答】【ガイドブック】 P.34を紹介
  - 【相談】IPA情報セキュリティ安心相談窓口へ
  - 【届出】被害の証拠を揃えて、所轄の警察署へ

- ケース1
  - ウィルス対策ソフトで確認
    見つからなくても「警告」の他にも情報窃取等のおそれがあるので、クリーンインストールを勧める。
    それにあたり、内蔵ハードディスクからのデータバックアップ方法について説明。
    委託した業者についても、法外な手数料を取られないように注意喚起。
    悪質な手口であり、１万円の件については、警察に相談することをすすめた。
    今後、怪しい画面は絶対開かないこと。

- PC画面に「ウイルスに感染している」との表示がされた
  - ウイルス対策ソフト以外からの表示は、アドウェアの可能性がある
  - 表示を止めて無視する

06.フィッシング詐欺・なりすまし

061.なりすまされたECサイトの被害

- ケース１
  - ●緊急対応
    他のお客様の被害が拡大しないように、また、他の利用者からの苦情に対応するために、「なりすましECサイト対策マニュアル」に従って、対応することをお勧めします。
    ☆なりすましECサイト対策協議会
    https://www.saferinternet.or.jp/narisumashi/
    「なりすましECサイト対策マニュアル」
    https://www.saferinternet.or.jp/system/wp-

Expand - Collapse

content/uploads/narisumashi_manual.pdf
具体的には、
①問い合わせ対応
　顧客対応からの問い合わせに対しての文面例
http://www.saferinternet.or.jp/system/wp-content/uploads/template002.docx
実被害者は、偽サイトで振り込んでしまった方ですので、被害者の所轄の警察署に被害届を出すように促してください。
②被害拡大防止
サイト内等で、他の利用者に対して注意喚起してください。
http://www.saferinternet.or.jp/system/wp-content/uploads/template001.docx
実例として、下記のようなページがあります。
「当店と誤認させるようなウェブサイト（なりすましECサイト）について」
https://namaenouta.jp/docs/attention.html
●風評被害について
「なりすましECサイト対策マニュアル」に従って、自社サイトで利用者に注意喚起等を行うことによって、「ユーザー（お客様）が逆に怖がってしまう」という事例は聞いていません。偽サイト、偽メールを騙られた多くのサイトは、マニュアルにあるような対応を取っています。
他に被害が拡大しないようにすることが、正規のECサイト運営者の責務であり、お客様への注意喚起を含めて、マニュアルに記載されているような対策を講じることにより、説明責任を果たすことで、社会的信用の喪失を防げると思います。
このような処置をきちんと行うことにより、セキュリティ意識のあるECサイトとして、逆に信頼に繋がると思います。
●相談及び届出
犯罪の可能性のある相談窓口は、警視庁サイバーセキュリティ犯罪対策課（03-3431-8109）であり、お掛けになった電話番号でよろしいと思いますが、相談が多く混み合っているものと思われます。
なりすまされたECサイトからの被害届を、警察が受理し立件できると判断するかは難しいところです。
なりすまされたECサイトの被害として、
著作権法違反、商標権侵害、不正競争防止法違反、詐欺罪等の法令違反の可能性はありますが、なりすまされたECサイトの被害を立証できる証拠を揃えることが困難なのが実情です。

- ケース２
  - ●考察
    ◆法令違反の可能性
    □ ※警視庁のサイバー犯罪対策課に問い合せたところ、下記のような可能性を示唆された。しかし、それを所轄の警察署で被害届を受理し立件できると判断するかはわからない

Expand - Collapse

★ 著作権法違反
□ 偽サイトで商品情報を複製して表示
★商標権侵害？
□ 商標登録された情報が複製されていた場合
★不正競争防止法違反
□ 販売する意思がないにも関わらず、利用者の個人情報だけを取得する
★詐欺罪
□ 財産上不法の利益を得たりするもので、適用が困難
◆ 警察の対応
□ 不正競争防止法違反であれば生活経済課、特殊詐欺であれば刑事課
□ 現状では、警察庁は、情報収集だけで何もしないと思われます

●対処案
◆利用者から、賠償請求等を受けないようにするためにも、警察に被害届を受理されることが重要
◆ しかしながら、現在の対応では、被害届が受理されない可能性が高い
◆まず、弁護士に相談
★ 警察に被害届を出す前に、弁護士にどのような手続きで法的対処をすべきかを相談する
★ 相談先候補
□ 法テラス（日本司法支援センター）
□ ☎0570-078374
◆ 偽サイトの削除要請
□ GoogleにインデキシングされたURLの削除はきりがない
□ リダイレクト先のURLを提供しているプロバイダに削除要請する
□ ※IPA（情報処理推進機構）に確認したが、IPAでは代行はしないとのこと
◆ 利用者からの苦情に対応するために
□ 「なりすましECサイト対策マニュアル」に従って、自社サイトで利用者に注意喚起する
□ なりすましECサイト対策協議会
□ https://safeinternet.or.jp/narisumashi/

- 元従業員が自社名義のホームページを無断で開設した
  - 元従業員のアカウントを削除する。
  - 元従業員が把握している管理者権限の認証情報を変更する。

- 062.なりすましサイトの利用者の被害
  - ●状況
    ・実際には使えないソフトの購入を促すアドウェアと思われる
    ●緊急対応
    ・登録キーが生成できなくて利用できないのであれば、「犯罪」の疑いがある
    ・犯罪の可能性があるので警視庁サイバー犯罪対策課に再度連絡する（テー

Expand - Collapse

プが流れたのは混み合っているからかと思われる）
・または、証拠資料を揃えて、所轄の警察署に届ける
●原因
・なぜアドウェアがインストールされたかはわからないとのことだが、何らかのサイトを見に行ったか、インストールしたソフトにバンドルされていたかと思われる
●今後の対応
・これからもアドウェアが表示されるなら、PCを初期化したほうがいいかもしれない
・アドウェアが表示されたら、まずはそれを消すことを検討すること
・アドウェアの表示に従って、クレジット番号を入れたりして注文しないこと

- 架空請求
  - 身に覚えのない請求の場合は、くれぐれも相手に連絡をとったり、支払いに応じたりしない
  - 不安な方や不審な点のある方
    - 【相談】消費者ホットラインに相談
    - 【相談】所轄の警察署生活安全課に相談
  - 【届出】フィッシング対策協議会のサイトで届出

063.なりすまされた利用者の被害

- 個人第1位　インターネットバンキングやクレジットカード情報の不正利用
  - 　ウイルス感染やフィッシング詐欺により、インターネットバンキングの認証情報やクレジットカード情報が攻撃者に窃取され、不正送金や不正利用が行われている。2017年は、インターネットバンキングの被害額は減少傾向だが、新たに仮想通貨取引所の利用者を狙った攻撃が確認されている。
  - 【窓口回答】【ガイドブック】P.30,P.68を紹介
  - 【緊急】銀行、カード会社に届出
  - 【届出】銀行、カード会社が、所轄の警察署に届出
    - 被害者は銀行、カード会社となるため

07.Web サービスからの個人情報の窃取

- 【ガイドブック】P.22 を紹介

- 個人第6位 組織第6位　ウェブサービスからの個人情報の窃取
  - 　2017年も引き続き、ウェブサービスの脆弱性が悪用され、ウェブサービス内に登録されている個人情報やクレジットカード情報等の重要な情報を窃取される被害が発生している。それらの情報を窃取されると、攻撃者により顧客や利用者の個人情報を悪用して不審なメールを送信されたり、クレジットカードを不正利用される可能性がある。
  - 【窓口回答】【ガイドブック】P.22を紹介

Expand - Collapse

- 【相談】IPA情報セキュリティ安心相談窓口へ
- 【届出】被害の証拠を揃えて、所轄の警察署へ

⊟ ブライダル関係のお店でお客様の情報を登録したら、そのお客様に他のブライダル関係のメールが届くようになった

- 消費者ホットラインに相談

⊟ 08.集中アクセス（DoS攻撃等）によるサービス停止

- 【ガイドブック】P.24を紹介

⊟ 組織第9位　サービス妨害攻撃によるサービスの停止

- 　ウイルスに感染し、ボットネット化した機器からDDoS（分散型サービス妨害）攻撃が行われ、ウェブサイトやDNSサーバーが高負荷状態となり、利用者がアクセスできなくなる被害が確認されている。2017年は公式のアプリストアに公開されたスマートフォンアプリがボットネット化し、DDoS攻撃が行われている。
- 【窓口回答】【ガイドブック】P.26 を紹介
- 【相談】IPA情報セキュリティ安心相談窓口へ

⊟ メールでビットコインを支払わないとDDoS攻撃をすると予告されたがどうしたらいい？

⊟ 多少のDDoS攻撃でネットワークが停止しないような対策

- インターネットルータの辺りでのDDoS攻撃の検知とアクセス制限

- プロバイダへの通知

⊟ 09.内部不正による情報漏えいと業務停止

- 【ガイドブック】P.26 を紹介

⊟ 組織第8位　内部不正による情報漏えい

- 　組織内部の従業員や元従業員により、私怨や金銭目的等の個人的な利益享受のため組織の情報が不正に持ち出されている。また、組織の情報持ち出しのルールを守らずに不正に情報を持ち出し、さらにその情報を紛失し、情報漏えいにつながることもある。内部不正が発覚した場合、組織は、原因追求等の対応に追われ、また社会的信用の失墜等にもつながる。
- 【窓口回答】【ガイドブック】P.26を紹介
- 【相談】IPA情報セキュリティ安心相談窓口へ

⊟ ケース1

- ■原因
  システムがわかる管理者がいないため
  ■緊急対応
  嫌がらせ、盗撮行為は、ストーカー行為に相当するので、管轄の警察署の生活安全課に相談するように
  ■暫定的対策
  退職者のIDは削除する

Expand - Collapse

全ての機器の管理者権限のパスワードを定期的に変更
■恒久的対策
システム管理、セキュリティ管理ができる情報処理技術を保有する人材を育成もしくは確保する
その人材が中心となって、システム化、セキュリティ対策を体系的に実施する

- 10.Web サイトの改ざん
  - 【ガイドブック】P.28 を紹介
  - Webサーバがハッキングされた場合の対処療法は
    - WebサーバをDMZに設置し、外部からの変更用ポートの閉鎖
    - ファイルを定期的にバックアップ
- 11.インターネットバンキングの不正送金
  - 【ガイドブック】P.30 を紹介
  - ネットバンキングのセキュリティ対策
    - ●予防策
      銀行サイト指定の対策アプリの利用
      2段階認証、ログイン端末通知
      【窓口回答】【ガイドブック】P.30,P.68を紹介
      ●緊急時対応
      【緊急】銀行、カード会社に届出
      【届出】銀行、カード会社が、所轄の警察署に届出
      被害者は銀行、カード会社となるため
- 12.悪意のあるスマホアプリによる攻撃
  - 【ガイドブック】P.32 を紹介
  - 個人第4位　スマートフォンやスマートフォンアプリを狙った攻撃の可能性
    - 　不正アプリを利用者がインストールしてしまうことで、スマートフォン内の重要な情報を窃取されたり、不正に操作される被害が確認されている。また、データの暗号化等を行うランサムウェアに加えて、2017年は個人情報を公開すると脅すランサムウェアも確認されている。さらに、これらの不正アプリは公式マーケットにも紛れ込んでおり、公式マーケットであってもインストール前にアプリの信頼性について確認する等の警戒が必要である。
    - 【窓口回答】【ガイドブック】P.32を紹介
    - 【相談】IPA情報セキュリティ安心相談窓口へ
  - 業務での私物端末使用における留意点
    - 端末の盗難防止、パスワードロック、紛失時の遠隔ロック
    - 重要ファイルは保存しない
    - 社内システムへのログインは、2段認証、端末認証
    - インストールするアプリの信頼性を認識
- 13.巧妙・悪質化するワンクリック詐欺

Expand - Collapse

- 【ガイドブック】P.34 を紹介

個人第8位　ワンクリック請求等の不当請求

- 　PCやスマートフォンを利用中にアダルトサイトや出会い系サイト等にアクセスすることで金銭を不当に請求されるワンクリック請求の被害が依然として発生している。1度のクリックによる請求だけでなく、複数回のクリックをさせることで、請求の正当性を主張して不当請求されてしまう事例も確認されている。
- 【窓口回答】【ガイドブック】P.34を紹介
- 【相談】IPA情報セキュリティ安心相談窓口へ
- 【届出】被害の証拠を揃えて、所轄の警察署へ

14.Web サービスへの不正ログイン

- 【ガイドブック】P.36 を紹介

「あなたのサーバが丸見えなので、対策の指導料をくれとのメールあり。「shodan」サイトで検索して見つけたよう。

- 実際に閲覧可能なっているかは不明であり、具体的に有りうるのかは、IPA情報セキュリティ安心相談窓口に相談

ハッキング攻撃を受けているのでその対策等を教えてもらいたい。

- 入り口、出口対策、DDoS攻撃の防御／フィルタリング等の技術的な対策が必要
- 運用保守業者に相談
- ITコーディネータ等に相談

個人第5位　ウェブサービスへの不正ログイン

- 　ウェブサービスに不正ログインされ、金銭的な被害や個人情報が窃取される等の被害が確認されている。2017年に確認されたウェブサービスへの不正ログインの多くがパスワードリスト攻撃により行われている。インターネットには多数のウェブサービスが存在しており、ウェブサービスの利用者がパスワードの使いまわしや推測されやすいパスワードを使用している場合に、不正ログインが行われてしまう。
- 【窓口回答】【ガイドブック】P.36を紹介
- 【届出】被害の証拠を揃えて、所轄の警察署へ

15.公開された脆弱性対策情報の悪用

- 【ガイドブック】P.38 を紹介

組織第4位　脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加

- 　脆弱性対策情報の公開は、脆弱性の脅威や対策情報を広く呼び掛けられるメリットがある。一方、その情報を攻撃者に悪用され、対策前のシステムを狙う攻撃が行われている。また、近年では脆弱性情報の公開後、その脆弱性を悪用した攻撃が本格化するまでの時間が短くなっている傾向がある。
- 【窓口回答】【ガイドブック】P.38を紹介

16.ネット上の誹謗・中傷【10大脅威より】

Expand - Collapse

- 【ガイドブック】P.40 を紹介

個人第3位　ネット上の誹謗・中傷

- 　コミュニティサイト（ブログ、SNS、掲示板等）上で、個人や組織に対して誹謗・中傷や犯罪予告をする書き込みが行われている。コミュニティサイトへの書き込みは、匿名性や手軽さから安易に投稿してしまう傾向にある。また、SNSを使った犯罪は社会的な問題となっており、2017年は殺人事件まで発展した事例もあった。
- 【相談】法務省人権擁護局　みんなの人権110番へ
- 【相談】コミュニティサイトの運営者に削除要請
- 【相談】法的対応は、法テラスへ
- 【届出】被害の証拠を揃えて、所轄の警察署へ

GoogleMapの口コミで誹謗中傷された。削除してもらうためには？

- Googleに削除要請
- 名誉棄損、営業妨害の疑いがある場合は、証拠を揃えて、所轄の警察署に相談

17.IoT 機器の不適切な管理【10大脅威より】

個人第9位　IoT 機器の不適切な管理

- 　昨今、IoT機器の利用が進んでいるが、利用者はIoT機器がネットワークに接続されている機器であることを意識せずに利用してしまい、適切な管理が行われていない。そのような管理されていないIoT機器が攻撃者に狙われ、分散型サービス妨害（DDoS）攻撃等に悪用されてしまう被害が確認されている。
- 【窓口回答】【ガイドブック】P.40,P.120を紹介
- 【相談】IPA情報セキュリティ安心相談窓口へ

組織第7位　IoT 機器の脆弱性の顕在化

- 　2016年に引き続き、IoT機器の脆弱性を悪用しウイルスに感染させることで、インターネット上のサービスやサーバに対して、大規模な分散型サービス妨害（DDoS）攻撃が行われる等の被害が確認されている。また、国内で発売されているIoT製品において脆弱性が発見されており、機器を乗っ取られる、または撮影機能等を悪用して個人情報を窃取されるといった危険性があることが公表されている。
- 【窓口回答】【ガイドブック】P.40,P.120を紹介
- 【相談】IPA情報セキュリティ安心相談窓口へ

18.情報モラル欠如に伴うセキュリティ問題の発生【10大脅威より】

個人第7位　情報モラル欠如に伴う犯罪の低年齢化

- 　2017年も未成年者がIT犯罪の加害者として逮捕、補導される事件が確認されている。IT犯罪に悪用できるツールや知識がインターネットを通じて誰でも入手・利用できるようになったことで、情報モラルの欠如した未成年者が、IT犯罪に手を染めやすくなっている。また、未成年者のPCやスマートフ

Expand - Collapse

ォンの所持も当たり前となってきており、教員や親の監視
い。

- 【相談】警視庁少年相談室ヤング・テレホン・コーナーへ（☎03-3580-4970）
- 【相談】IPA情報セキュリティ安心相談窓口へ
- 【窓口回答】家庭内でもモラルの教育を促す

組織第5位　セキュリティ人材の不足

- 　セキュリティ上の脅威は今後さらに増大するだけでなく、新たな脅威も発生し続けていくことが予想される。これらの脅威に対応するためにはセキュリティの知識、技術を有するセキュリティ人材が欠かせないが、圧倒的に不足しており、問題視されている。セキュリティ人材が手薄の組織では、十分なセキュリティ対策、対応をとることが難しく、脅威の増大に伴い実被害につながることも考えられる。
- 【窓口回答】【ガイドブック】P.104を紹介
- 【窓口回答】情報処理技術者試験のシラバスに沿った網羅的なスキル・知識の習得
- 【窓口回答】iコンピテンシ・ディクショナリに沿った業務に必要なスキル・知識の選択的な習得

登録者へのメールを誤ってCCで送ってしまった

- 消すことはできない
- サイト等で謝罪文を掲載する
- 場合によっては損害賠償も必要

19.犯罪のビジネス化【10大脅威より】

組織第10位　犯罪のビジネス化（アンダーグラウンドサービス）

- 　犯罪に使用するためのサービスやツールがアンダーグラウンド市場で取り引きされ、これらを悪用した攻撃が行われている。攻撃に対する専門知識に詳しくない者でもサービスやツールを利用することで、容易に攻撃を行えるため、サービスやツールが公開されると被害が広がるおそれがある。
- 【相談】警視庁　サイバー犯罪対策課へ（？）

- 90.セキュリティ事象か不明

02.全般的なサイバーセキュリティ対策の相談

01.組織的対応

010.全般的対策

情報セキュリティ侵害に遭わないように事前に何をすればいいか

- まず「中小企業向けサイバーセキュリティ対策の極意」の入手（ダウンロード）し、内容を確認することを助言
- 内容を確認後、不明な点があれば、再度相談を受け付ける

より詳細な対策内容を知りたい場合は

Expand - Collapse

- 内容を確認し、「相談対応のためのハンドブック（
に記載の参考文献、Webサイト、セミナー等を紹介する

- これから検討の標準回答
  - 情報セキュリティーのための投資については、全てのリスクに対して技術的対策をすることは困難。
  - セキュリティー被害を受けた場合、その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要になることを考えること。
  - また、システムを入れる際に、セキュリティーも同時に入れるなど、ITとセキュリティー対策を一緒にすることも大切である。
  - 更に、経営者を含め、社員全員に対し、セキュリティーポリシーや【ガイドブック】を作成したり、併せてITパスポートの試験を受けさせることも大切である。
- 情報セキュリティ対策の必要性を認識し、網羅的な対策を知るには？
  - まず「中小企業向けサイバーセキュリティ対策の極意」の入手（ダウンロード）し、内容を確認することを助言
- 迷惑メール対策
  - １　迷惑メール対策としては、不審なメールを絶対開かないこと。併せて、不審なメールを開かないよう経営者を含め社員全員に徹底指導すること。また、メールレンタルサービスに対し、不審なメールに対しては、フィリタリングを掛けられないかを確認する。
    ２　情報セキュリティーのための投資については、全てのリスクに対して技術的対策をすることは困難。セキュリティー被害を受けた場合、その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要になることを考えること。また、システムを入れる際に、セキュリティーも同時に入れるなど、ＩＴとセキュリティー対策を一緒にすることも大切である。更に、経営者を含め、社員全員に対し、セキュリティーポリシーや【ガイドブック】を作成したり、併せてＩＴパスポートの試験を受けさせることも大切である。

- 011.管理的対策
- 012.人的対策
- 013.技術的対策
  - 一般論としての緊急対応、恒久的対策
    - ■中小企業向けの一般論として緊急対応、恒久的対策
      Webサーバがどんなウイルスに感染して、サーバ内のファイルを改ざんしたのか、メンテナンスする人や、外部から利用する人のPCに、ウイルスを感染させようとしているのかわからないので、一般論として原因究明と対応策の回答になりますのでご了承ください。
      ●Webサーバに不正アクセスされて、ウイルスが埋め込まれたのであれば、
      ★緊急対応として

Expand - Collapse

・ただちにメンテナンス中の表示にしているようですが、Webサーバへのアクセスが可能であれば、さらに重大なファイルの改ざんや不正プログラムが埋め込まれる可能性があります。ただちにサーバを止めて、再発防止策を講ずるべきです。
★原状保全（専門機関での調査分析のため）として
・原因調査のためにWebサーバのファイルをバックアップし保存する
★原因調査（なぜ情報セキュリティ侵害が起きたか）として
・Webサーバ内のファイルに改ざんされたものがないか、本来存在しないファイルがないかを確認する
・Webサーバに何らかの脆弱性があります。Webサーバのログ等を確認して、ファイル転送等、不正なアクセスを確認してください。
★復旧策として
・確認できた事象に対する再発防止のための改善策を、システムの専門家、コーディネータと相談して対応してください。
●届出
★「ハッキングされてウイルス感染した」という実被害がありますので、ウイルス・不正アクセス届出機関である「IPAセキュリティセンター」https://www.ipa.go.jp/security/　03-5978-7518に届出ていただき、再発防止にご協力願えればと思います。
★また、電子計算機損壊等業務妨害罪等の犯罪の可能性もありますので、警視庁にご相談されることもお勧めします。
●恒久的対策（再発防止策）
★ルールの策定
・情報セキュリティ侵害の原因の多くが、人為的なミスもしくは悪意によるものです。
・最低限守るべきルールを明確にして、それを守らせることが重要です。
★セキュリティがわかるシステム管理者の確保
・厳しい財政事情のなかで、ITの導入、情報セキュリティ対策は二の次になる状況は理解しますが、何かあってからでは手遅れです。
・「ホームページ管理者が不在」ということですが、ホームページの構築、情報セキュリティ対策を外部に委託するにしても、専任でなくても発注者としてある程度の知見を持った人材が必要です。情報処理技術者試験の１つである「ITパスポート試験」に合格するレベルのスキルと知識を持った人材を確保することが望まれます。
●情報セキュリティ対策の重要性
・営業促進のためにホームページを立ち上げても、一度情報セキュリティ侵害に遭うと、復旧のための経済的損失、さらに社会的信用が失われ、事業の継続、組織の存立が脅かされる可能性があります。
・一般的に、事前に対策をするための費用に比べ、セキュリティ侵害が発生して対処する費用のほうが高くなります。
・Webサーバを立ち上げる投資に、情報セキュリティ対策を含めて実施することをお勧めします。

⊟ UTMを導入した場合は、従来からのファイアウォールは撤去していいか？

Expand - Collapse

- UTM（Unified Threat Management；統合脅威管理）ファイアウォールの機能は持つ
- UTMのような高価なシステムを導入する際は、被害に遭った場合の被害額を評価して、過剰設備にならないように。

- 014.物理的対策
- 015.緊急時対応
- 018.セキュリティ人材確保

- 03.不正アクセス全般
- 04. 情報漏えい全般
- 09.参考情報

- 09.その他
  - 01.相談窓口について
  - 02.セミナー依頼
  - 03.【ガイドブック】等の入手、活用
  - 04.セキュリティ対象外
    - 消費生活全般に関する苦情や問合せ
      - 【相談】消費者ホットライン
    - 嫌がらせ、ネットストーカー
      - 【相談】所轄の警察署の生活安全課
    - 人権侵害
      - 【相談】みんなの人権110番
    - 個人情報の取り扱い
      - 【相談】個人情報保護委員会
  - 05.電波系
    - PC上に外部からのメッセージが書き込まれている
      - 状況を正確に把握できる画面や事象の資料がなければ判断できない
  - 20.その他

- 提示する対策項目【Mission2に沿って】
  - 01.全般
  - 011.全般（サイバー攻撃に対して何ができるか）
    - 【ガイドブック】P.46 を紹介
  - 02.情報セキュリティ5か条+2の備え
    - 【ガイドブック】P.48 を紹介
    - 022.OS とソフトウェアのアップデート
      - 【ガイドブック】P.48 を紹介

Expand - Collapse

- 023.ウイルス対策ソフト・機器の導入
  - 【ガイドブック】P.50 を紹介
- 024.定期的なバックアップ
  - 【ガイドブック】P.46 を紹介
- 025.パスワードの管理
  - 【ガイドブック】P.54 を紹介
- 026.アクセス管理
  - 【ガイドブック】P.56 を紹介
- 027.紛失や盗難による情報漏えい対策
  - 【ガイドブック】P.58 を紹介
- 028.持ち込み機器対策
  - 【ガイドブック】P.60 を紹介

03.電子メールへの備え

- 031.電子メールの安全利用
  - 【ガイドブック】P.62 を紹介
- 032.標的型攻撃メールへの対応
  - 【ガイドブック】P.64 を紹介
- 033.迷惑メール発信への対応
  - 【ガイドブック】P.66 を紹介

04.今やろう！　インターネット利用への備え

- 041.安全な Web サイト利用
  - 【ガイドブック】P.68 を紹介
- 042.閲覧制限
  - 【ガイドブック】P.70 を紹介
- 051.重要情報の持ち出し
  - 【ガイドブック】P.72 を紹介
- 052.重要情報の保管
  - 【ガイドブック】P.74 を紹介

10.経営者が主導する対策【Mission3】

- 【ガイドブック】P.79 を紹介
- サイバーセキュリティ対策は、 事業継続を脅かすリスクの 1 つ
  - サイバーセキュリティ対策が経営に与える重大な影響
    - 【ガイドブック】P.80 を紹介
  - サイバー攻撃を受けると企業が被る不利益

Expand - Collapse

- 【ガイドブック】P.82 を紹介

経営者に問われる責任
- 【ガイドブック】P.84 を紹介

投資効果（費用対効果）を認識する
- 【ガイドブック】P.86 を紹介

自社の IT 活用 ・ セキュリティ対策状況を自己診断する 3・5 IT の活用診断

サイバーセキュリティ投資診断
- 【ガイドブック】P.90 を紹介

情報セキュリティ対策診断
- 【ガイドブック】P.92 を紹介

ビジネスを継続するために （守りの IT 投資とサイバーセキュリティ対策）

業務の効率化、サービスの維持のために
- 【ガイドブック】P.94 を紹介

経営者が認識すべきサイバーセキュリティ経営 3 原則
- 【ガイドブック】P.96 を紹介

経営者がやらなければならないサイバーセキュリティ経営の重要 10 項目【2.0版】
- 【ガイドブック】P.98 を紹介

サイバーセキュリティリスクの管理体制構築
- 指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定
- 指示２ サイバーセキュリティリスク管理体制の構築
- 指示３ サイバーセキュリティ対策のための資源（予算、人材等）確保

サイバーセキュリティリスクの特定と対策の実装
- 指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
- 指示５ サイバーセキュリティリスクに対応するための仕組みの構築
- 指示６ サイバーセキュリティ対策におけるPDCAサイクルの実施

インシデント発生に備えた体制構築 3
- 指示７ インシデント発生時の緊急対応体制の整備
- 指示８ インシデントによる被害に備えた復旧体制の整備

サプライチェーンセキュリティ対策の推進
- 指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

ステークホルダーを含めた関係者とのコミュニケーションの推進

Expand - Collapse

- 指示１０ 情報共有活動への参加を通じた攻撃情報の入手及び 提供

⊟ ビジネスを発展させるために （攻めの IT 投資とサイバーセキュリティ対策）

⊟ 次世代技術を活用したビジネス展開
- 【ガイドブック】P.110 を紹介

⊟ 【コラム】「攻めの IT 経営中小企業百選」
- 【ガイドブック】P.111 を紹介

⊟ IoT、ビッグデータ、AI、ロボットの活用
- 【ガイドブック】P.112 を紹介

⊟ 【コラム】IoT、ビッグデータ、AI、ロボットはつながっている
- 【ガイドブック】P.113 を紹介

⊟ IoT が果たす役割と効果
- 【ガイドブック】P.114 を紹介

⊟ 【コラム】ものづくり企業　IoT 活用事例
- 【ガイドブック】P.115 を紹介

⊟ 人工知能（AI）が果たす役割と効果
- 【ガイドブック】P.116 を紹介

⊟ 【コラム】新しい価値を持った業務の創出
- 【ガイドブック】P.117 を紹介

⊟ IoT を活用する際のサイバーセキュリティ上の留意点
- 【ガイドブック】P.118 を紹介

⊟ IoT を活用する一般利用者のための基本ルール
- 【ガイドブック】P.120 を紹介

⊟ 【コラム】クラウドサービスの活用
- 【ガイドブック】P.122 を紹介

⊟ セキュリティホールを減らす網羅的 ・ 体系的な対策の策定方法

⊟ 新・5 分でできる自社診断シート
- 【ガイドブック】P.124 を紹介

⊟ 情報セキュリティハンドブックひな形（従業員向け）
- 【ガイドブック】P.126 を紹介

⊟ 情報セキュリティポリシーの明文化
- 【ガイドブック】P.128 を紹介

⊟ 情報資産管理台帳の作成
- 【ガイドブック】P.130 を紹介

Expand - Collapse

- 20.もしもマニュアル（緊急時対応手順）【Mission4】
  - 【ガイドブック】P.133
  - 緊急時対応用マニュアルの作成
    - 【ガイドブック】P.134 を紹介
  - 基本事項の決定
    - 【ガイドブック】P.136 を紹介
  - 漏えい・流出発生時の対応
    - 【ガイドブック】P.138 を紹介
  - 改ざん・消失・破壊・サービス停止発生時の対応
    - 【ガイドブック】P.140 を紹介
  - ウイルス感染時の初期対応
    - 【ガイドブック】P.143 を紹介
  - 届け出および相談
    - 【ガイドブック】P.145 を紹介
  - 大規模災害などによる事業中断と事業継続管理
    - 【ガイドブック】P.146 を紹介
  - 【ワークショップ】自社でやろう　サイバー攻撃への対応リアクション
    - 【【ガイドブック】】P.148 を紹介
  - 30.
  - 20.その他
- 相談対応時参考資料・Webサイトへのリンク
  - IPA情報セキュリティ安心相談窓口
  - なりすましECサイト対策協議会
    - 対策マニュアル
  - 警視庁情報セキュリティ広場
    - 警察署一覧
- 汎用の手順書へのリンク
  - サイバーセキュリティ相談・届出先クイックリスト
  - 情報セキュリティ緊急対応ガイド【汎用】
  - 相談対応の手引きレファレンスリスト【相談員用】
  - サイバーセキュリティ対策相談対応の手引き（メモ）
  - その他の相談対応手順（未整理分）
    - 「ここからセキュリティ」
    - 他機関事例
      - 警視庁のFAQ

- IPAのFAQ

Expand - Collapse