**Sec01-01-03\_「中小企業向けサイバーセキュリティ対策の極意」【本文案】**

* 改訂履歴
  + 【2021年3月18日】Mission2、Mission3の改訂内容を反映
  + 【2021年3月16日】InDesignファイルから変換したEPUBの内容を反映
  + 【2021年3月12日】改訂版反映準備
  + 【2021年2月1日】3-10の校正案
  + 【2021年1月12日】打ち合わせ内容の反映
  + 【2020年12月21日】参考文献リンク先修正
  + 【2020年12月14日】全体再確認
  + 【2020年10月29日】お役立ち情報リンク（人材育成、GDPR関連）の更新
  + 【2020年10月16日】参考文献、相談・届出先リスト追加
  + 【2020年10月9日】人材育成関連内容追記
  + 【2020年9月15日】内容追記
  + 【2020年8月25日】Sec01-01-02と整合
  + 【2020年8月14日】Sec01-01-03から分離
* 概要
  + リンク
    - html版
    - MindManager版（Download）
    - Docx版（Download）
  + 凡例
    - 冊子体及び冊子体ベースWebページ
    - 冊子体既存項目（見出し・項番等の軽微な修正は含む）
    - 冊子体追加項目（大きな修正を含む）
    - 改訂箇所
    - 作成せず
    - 参考資料
    - 担当
  + 別添：Sec01-01-02\_「中小企業向けサイバーセキュリティ対策の極意」【目次案】
* **【Mission0】 はじめに**
  + **改版箇所**
    - **国の「サイバーセキュリティ戦略」に沿ったセキュリティ対策を実施するために**
    - **NISC等の資料の反映、テレワークの継続化**
  + ケーススタディー１：なぜ、こんな小さな会社が狙われたの？
  + ケーススタディー２：ある日突然、銀行口座の預金残高が消えた！
    - **【補足説明材料】**
      * 人員不足〜以下囲みコラムの平成２７年度 ―平成XX年度の最新に更新⇒数字のみ修正
  + ケーススタディー３：取引先企業への踏み台にされた
    - **【補足説明材料】**
      * サプライチェーン紹介のページへのリンク
  + ケーススタディー４：EMOTET、ランサムウェアの被害にあった？
  + ケーススタディー５：BEC攻撃事例⇒海外の取引先からのメール
  + ケーススタディー６：昨今の産業を巡るサイバーセキュリティに係る状況
    - **【補足説明材料】**
      * 「昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について」【2020年6月12日METI】等を参考に。
  + ケーススタディー７：サイバーセキュリティ保険に入っていれば
  + **【補足説明材料】**
    - ケーススタディーX：サプライチェーンセキュリティの必要性が高まっていること
    - ケーススタディーX：セキュリティ対策を怠ると他社に迷惑をかけることもある
    - ツイッター被害 乗っ取り、詐欺悪用相次ぐ
    - サイバー被害 通知義務化 個人情報漏洩の全員に　企業の対応不可避
    - ***改訂箇所：「はじめに」(p.8～9)を改訂***
      * 「サイバーセキュリティ経営ガイドライン・概要＞の説明を全体的に修正。
      * 「情報セキュリティ白書2020」を参考に
      * IoTやAIの活用といった最近の情勢を踏まえる
* **【目次】**
* **【Mission1】　知っておきたいサイバー攻撃の知識**
  + 1-1：標的型攻撃による情報流出
  + 1-2：ランサムウェアを使った詐欺・恐喝
    - **【補足説明材料】**
      * **【囲みコラム】「No More Ransam」　の紹介**
  + 1-3：Webサービスからの個人情報窃取
    - **【補足説明材料】**
      * **【囲みコラム】割賦販売法の改定とクレジットカードのセキュリティ**
  + 1-4：集中アクセスによるサービス停止
    - **【補足説明材料】**
      * **【囲みコラム】内容更新**
        + Subtopic
  + 1-5：内部不正による情報漏えいと業務停止
    - **【補足説明材料】**
      * 中小企業経営者サイバーリスク意識調査2019【2020年1月日本損害保険協会】を参照のこと。
  + 1-6：Webサイトの改ざん
    - **【補足説明材料】**
      * ECサイトの改ざんを事例で入れる
  + 1-7：インターネットバンキングの不正送金
    - **【補足説明材料】**
      * **【囲みコラム】不正送金を阻止するには**
  + 1-8：悪意のあるスマホアプリ
    - **【補足説明材料】**
      * **グラフ最新化**
      * **【囲みコラム】スマートフォン決済不正アプリ**
  + 1-9：巧妙・悪質化するワンクリック詐欺
  + 1-10：Webサービスへの不正ログイン
    - **【補足説明材料】**
      * **【囲みコラム】不正ログインを…多要素認証の取り込み（NIST800-63-3対応）**
  + 1-11：公開された脆弱性対策情報の悪用
  + 1-12：IoT機器を踏み台にした攻撃
    - **【補足説明材料】**
      * **【囲みコラム】対策はこれだ…NICT　「NOTICE」の実証事例の結果を追加**
      * 【囲みコラム】IoTとデータ利活用の全体像【総務省】
  + 1-13：中小企業におけるサイバー攻撃被害の例
    - **【補足説明材料】**
      * 経産省：お助け結果「た昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について」
      * 経産省：最近のサイバー攻撃の状況を踏まえた経営者への注意喚起
      * **＜統計データのアップデート＞**
        + １．１節「サイバーセキュリティ経営ガイドラインの背景と位置づけ」で 参照している統計データをアップデート。それに伴い説明文も修正。
  + **1-14：なりすましECサイトの被害と回避策**
    - **【補足説明材料】**
      * ***改訂箇所：Mission1-12　(P.41)のあとに追加***
      * 事業者サイド
        + ウェブサイト開設等における運営形態の選定方法に関する手引き【2018年5月IPA】
        + なりすましECサイト対策マニュアル【2015年3月一般社団法人セーファーインターネット協会】
      * 利用者サイド
        + なりすましサイトの見極め方、被害の内容に応じた相談先、届け出先
  + **1-15：ビジネスメール詐欺の被害と回避策**
    - **【補足説明材料】**
      * ***改訂箇所：Mission1-12　(P.41)のあとに追加***
* **【Mission2】　すぐやろう！対サイバー攻撃アクション**
  + 概要
    - 改訂のポイント
      * 冊子版は、敢えて改訂する必要があるか？
      * EPUB、Web版は、情報セキュリティ10大脅威レベルでリライトするか？
  + 2-1：サイバー攻撃に対して何ができるか
  + 2-2：OSとソフトウェアのアップデート
    - すぐやろう
      * ■パソコンのOSは可能な限り自動更新にする
      * ■インストールしているソフトウェアは、常に最新の状態にする
    - ＜OSのアップデート＞
      * ●パソコンのOSは可能な限り最新の状態を保つようにする。自動更新が利用できる場合は、自動更新機能を有効にする。
      * ●サポートが終了した古いOSは使わない※。
      * ●業務に利用するスマートフォンのOSは機種ごとの情報を常に調べて手動で更新する。
    - ＜ソフトウェアのアップデート＞
      * ●全てのソフトウェアを最新版にする。
      * ●自動更新機能がある場合は必ず設定する。
      * ●自動更新が設定できないものについては、定期的に脆弱性情報をチェックする。
    - セキュリティ上の脆弱性が攻撃対象に！
      * OSは、日々新たなセキュリティ上の脆弱性が発見されています。サイバー攻撃はこの脆弱性を利用してウイルスを潜入・繁殖・拡散させます。
      * また、OSだけでなく、Microsoft Office製品やAdobe Acrobat Readerなど、多くの人が使用している製品のセキュリティホールも攻撃の対象となっています。OSもソフトウェアも常に最新版にしておくことが大切です。
    - 脆弱性情報はここから入手
      * JPCERT コーディネーションセンターが運営・提供している脆弱性に関するメーリングリストやJVN（脆弱性対策情報ポータルサイト）などから、自分が使っているソフトウェアに関する脆弱性情報を入手だ。
  + 2-3：ウイルス対策ソフト・機器の導入
    - すぐやろう
      * ■ウイルス対策ソフトウェア（セキュリティソフト）がインストールされているか、また最新バージョンになっているかを確認する
    - ＜個別のパソコンに導入するタイプ＞
      * 個別のパソコンに導入するウイルス対策ソフトウェアには自動的に更新する機能が付いています。最近のウイルス対策ソフトウェアは脆弱性スキャンやWeb脅威対策、URLフィルターなど多くのセキュリティ機能が付いています。
    - ＜ネットワークの出入り口に設置するタイプ＞
      * オフィスのネットワークとインターネット網との間の出入り口部分に、統合型セキュリティ機器（UTM）を導入することで、二重にセキュリティを強め外部への情報漏えいや被害拡大を防ぐことができます。UTMは複数のセキュリティ機能を1つのハードウェアに統合し、集中的に管理します。
    - ウイルス対策ソフトは必ず最新のものに
      * ウイルスは毎日たくさんの新種が登場している。そのために、ウイルス対策ソフトを新しいウイルスに対応できる状態に保つ必要がある。ウイルス対策ソフトには、ウイルスを発見して駆除するプログラムを自動的に更新する機能が付いている。この機能を利用するか、毎日このプログラムの更新だ。
      * メールの添付ファイル、ダウンロードしたファイル、USBメモリーやCDなどの外部記憶媒体に格納されたファイルも、必ずウイルスチェックを行ってから使うことだ。
  + 2-4：定期的なバックアップ
    - すぐやろう
      * ■重要データは、定期的に別媒体へバックアップを取って保存する
    - ＜バックアップの方法＞
      * ●ハードディスク（HDD）やDVDなどの外部記憶媒体に保存
      * ●重要情報はネットワークと切り離して保存
      * ●保管方法を決めておく（保管場所や保管媒体など）
      * ●バックアップ媒体のセキュリティ対策も同時に実施
      * ●必要に応じて1つ前のデータも保存
    - 定期的バックアップの重要性
      * ビジネスで利用するデータは、削除誤りなどの人的ミスやハードウェア障害、ソフトウェア障害など多様な要因によって破損する危険があります。これらのリスクから業務データを守るためには、定期的なバックアップが不可欠です。
      * 重要なデータのバックアップがあれば、万が一データが消失してしまっても、速やかにビジネスを復旧させることができます。
      * バックアップには、使っているPCが壊れたときのために重要なデータを外付けのHDDなどにバックアップする方法や、クラウドへバックアップする方法があります。クラウドの場合、保管するデータセンターの場所が会社から遠いところにあったり、複数のデータセンターで相互にバックアップしていたりと、社内で保管するより安心な場合もあります。
      * クラウドの活用に際しては、管理担当者の選定や利用範囲と権限の明確化、利用者が使うパスワードなどの認証機能を適切に設定・管理するなどの点に留意が必須です。
    - Windowsのバックアップ機能を活用だ！
      * 定期的バックアップのために市販のバックアップソフトウェアを使う方法もあるが、Windowsには自動バックアップ機能が付いている。一度設定すれば指定したフォルダーを定期的にバックアップしてくれる。保管場所としてはネットワークから切り離すことができる外付けのハードディスクがお薦めだ。
  + 2-5：パスワードの管理
    - すぐやろう
      * ■ パスワードを強化する
      * ■ID・パスワードを盗まれないようにする
    - ＜パスワードの強化＞
      * 他人に推測されやすいパスワード（ニックネームや誕生日など）は使わない。
      * ●長いパスワード（推奨は10桁以上）にする。
      * ●推測しづらく自分が忘れないパスワードにする。
      * ●他人の目に触れるような場所に、パスワードを残さない。
      * ●いろいろなWebサービスで同じID・パスワードを使い回さない。
    - パスワードの使い回しは危険
      * パソコン本体はもちろん、メールやSNS、各種アプリや会員サイトなどのWebサービスを使うときに必要となるのがID（アカウント）とパスワード。1つのパスワードを使い回している場合、それが流出すると、ほかのサービスも乗っ取られてしまう可能性が高くなります。
    - 対策を講じないと……
      * IDやパスワードを盗まれて不正にログインされることで、会社にも個人にもさまざまな被害が発生します。
      * ・自分が利用しているインターネットバンキングから知らない口座に振り込まれた。
      * ・ショッピングサイトで勝手に高額な買い物をされた。
      * ・知らないうちに迷惑メールを大量に送信させられた。
      * など、他人に迷惑をかけることになるケースもあります。
    - 多要素認証でより安全に
      * 通常はIDとパスワードを使って本人であることを確認するが、さらにもう1つ別のパスワードで認証する方法がさまざまなオンラインサービスで使われている。また複数の要素を使って認証する多要素認証も多く使われている。
  + 2-6：アクセス管理
    - すぐやろう
      * ■データや社内ネットワークへのアクセスについて利用者の制限やIDの管理を行う
      * ■職務や業務、役割によってもIT機器や情報に対してアクセスの管理・制限を行う
    - ＜ネットワークなどへのアクセス管理＞
      * ●社内のパソコンやIT機器、ネットワークなどへアクセスする場合、職務を実施するために必要な情報に限定したり利用者を制限したりする。
      * ●職務の変更や人事異動があったら、利用者のアクセス権限を見直す。
    - ＜情報へのアクセス管理＞
      * ●会社の重要情報を機密性※1、完全性※2、可用性※3の観点から評価し、情報資産の重要度を仕分ける（情報資産管理台帳の作成はP175参照）。
      * ●情報ごとにアクセス権を設定する。
      * ●アクセス権の設定ではID・パスワードの使い回しを禁止する。
      * ※1 アクセスを許可された者だけが必要な情報にアクセスできること
      * ※2 情報および処理方法が正確であること、かつ完全であること
      * ※3 認可された利用者が必要なときに情報および関連する資産にアクセスできること
    - 何が防げるの？
      * 例えば「社外秘」の情報はこれらにアクセスできる利用者も制限する必要があります。つまり、この情報を利用できるのは誰かを設定するということです。それがアクセス権の設定です。
      * ネットワーク上の共有フォルダーやWebページにアクセス権を設定すると、特定のユーザーだけが利用できるようになるので、重要なデータを保護できます。
    - 無線LANのアクセスに注意だ
      * 社内で無線LAN（Wi-Fi）を使う会社が飛躍的に増えている。しかし「簡単に接続できる」「社内の人しか使わないから」といった理由で、接続時のパスワードを設定していない企業も少なくない。無線LANが社内ネットワークに直結している場合、誰でも簡単に侵入できる可能性がある。無線LANには必ずパスワードを設定し、接続できる権限を持った人間と端末を決めておくべきだ。
  + 2-7：紛失や盗難による情報漏えい対策
    - すぐやろう
      * ■ 原則は情報の持ち出し禁止
      * ■パソコンやUSBメモリーなどの記憶媒体やデータを外部に持ち出す場合、盗難・紛失などに備えて、パスワード設定や暗号化などの対策を実施する
    - ＜情報持ち出しの対策＞
      * ●パソコンや記憶媒体を持ち出す場合の規定を設ける。
      * ●利用者の認証（ID・パスワード設定、USBキーやICカード認証、指紋認証など）を行う。
      * ●保存されているデータに対して、重要度に応じてHDD暗号化、パスワード設定などの技術的対策を実施する。
      * ●紛失情報が何かを正確に把握するため、持ち出し情報の一覧を作り、管理を行う。
      * ●ノートパソコンまたはタブレット端末に保存するデータは最小限にする。
      * ●電子媒体はケースに入れ、USBメモリーはタグ、ストラップ、鈴などを付ける。
      * ●不要な場所に持ち出さない。
      * ●携行時の注意
      * ・電車内では肌身離さず、網棚に置かない。
      * ・自動車内には保管しない。
      * ・他者からのぞき見されない状態で扱う。
    - 紛失・盗難対策の基本はパスワード
      * パソコンやモバイル端末などの情報が収められた機器は、起動の際にパスワードをかけたり、ファイルそのものにもパスワードを設定したりするなどの対策を事前に行っておくことで、盗難・紛失時に情報を簡単に見られないようにすることができます。
    - 街なかのフリーWi-Fiに注意だ
      * 公共施設をはじめ街なかには多くのAP（アクセスポイント）が設置されている。だが、APすべてが万全のセキュリティ対策を講じているとは限らない。中には利便性を追求し最低限の対策に留めるAPも存在し、使い方によっては通信内容を盗まれる可能性がある。
      * また必ずしも『暗号化＝安心』というわけではない。例えば「偽AP」だ。この場合、暗号化に関係なく通信内容が盗まれる。
      * 便利なフリーWi-Fiだが利用する際、少なくとも次の点は確認だ。
      * ・接続するフリーWi-FiのAP名の確認
      * ・接続後、ID・パスワード等の入力画面になった場合、URLが「https://」で始まっているか
      * ・ブラウザに鍵マークが表示されているか
      * 特にテレワーク等、機微な情報を扱う際は不特定のAPは避けるべきだ。
  + 2-8：持ち込み機器対策
    - すぐやろう
      * ■テレワーク等で機器を社外に持ち出す際や私物機器類を会社に持ち込む場合には、セキュリティと使い方のルール（例）を設ける
    - ＜使い方ルール＞
      * 表形式
      * パソコン※自宅のパソコン で業務を行う場合 も含む
        + ・データや情報を持ち出す場合は会社ルール（P66参照）に準拠する
        + ・ウイルス対策ソフトおよびアプリケーションなどは会社指定のものを導入
        + ・情報セキュリティ事故の発生に備えて担当者への連絡体制を確認する
        + ・作業開始前に端末のOSやソフトウェアが最新か確認
        + ・機密情報を送信する際には暗号化する
        + ・テレワークなどで会社機器を社外に持ち出す場合、フリーWi-Fiなどには接続しない
        + ・基本的に私物機器は社内に無断で持ち込まない
        + ・私物機器は社内LANへの接続を禁止する
        + ・家族や友人への会社機器の貸与を禁止する
      * スマートフォン、タブレット端末、携帯電話など
        + ・会社で指定したアプリケーション以外は使わない
        + ・社内パソコンに接続する前には必ずウイルス対策ソフトでチェックする
        + ・ウイルス対策ソフトなどは会社指定のものを導入
        + ・業務情報と私的な情報を混在させない
        + ・家族や友人への貸与を禁止する
      * USBメモリー、外付けHDD
        + ・社内パソコンに接続する前には必ずウイルス対策ソフトでチェックする
      * 共通
        + ・個人のメールアドレスに業務用データを添付して送信しない
        + ・社用メールアドレスで受信したメールを個人のアドレスに転送することを禁止する
    - 私物端末による脅威とは
      * ●感染した私物端末が不正プログラムなどで遠隔操作される。
      * ●私物端末でデータを持ち出される。
      * ●感染した私物端末から社内のネットワークに感染が広がる。
      * ●感染した私物端末のテザリング機能を利用して外部への通信が行われ、情報が漏えいする。
    - 持ち込み機器にもウイルス対策ソフトを
      * 私物の機器は原則として持ち込み禁止にするのが安全だが、実際には私物端末を業務に利用するニーズも増えている。その場合は持ち込みを許可する端末に必ずウイルス対策ソフトをインストールさせることだ。ソフトによっては、USBメモリーなどを差し込んだら自動的にチェックを求める機能が付いているものもある。
  + 2-9：電子メールの安全利用
    - すぐやろう
      * ■誤送信しないように宛先や内容、添付ファイルの確認をする
      * ■原則としてファイルを添付しない
      * ■万一必要な場合は、添付ファイルを暗号化する
    - ＜誤送信対策＞
      * ●送信ボタンを押す前に、必ず宛先を再確認する。いったん送信トレイに保存するように設定すれば、送信前に宛先を再確認することができる（メールソフトとバージョンによって異なります）。
      * ●大量のアドレスへ同報メールを送るときなどはそれぞれの受信者にアドレスが分からないようにBCCを使う。
    - ＜添付ファイルの暗号化＞
      * メールを安全に送受信するために添付ファイルを簡単に暗号化することができます。
      * ●アプリケーションソフトにある暗号化機能を利用する。
      * ●圧縮・解凍ソフトの暗号化機能を利用する（パスワードを設定する）。
      * なお、パスワード付きZIPファイルをなどをメール添付で送り、後からパスワードを別のメールで送ることは、「Emotetなどのマルウェアに悪用される」「受信者の作業負荷を高める」といった理由で、禁止する動きが広がっています。
    - ＜電子メールのなりすまし対策＞
      * ビジネスツールとして広く普及する電子メール。しかし、近年は「なりすまし」や標的型攻撃も登場しています。その対策手段の1つが「送信ドメイン認証技術」の導入です。この中には、送信元のメールサーバーのIPアドレスを認証に用いるの「SPF」と暗号化技術を用いて認証する電子署名方式の「DKIM」の2方式があり、さらに両者の結果を利用する「DMARC」があります。
    - 添付ファイルはなるべく減らす！
      * 電子メールを使ったサイバー攻撃の多くは、添付ファイルに仕込まれたウイルスや不正プログラムによるものだ。
      * だからビジネス上のやり取りでは添付ファイルを減らすことが、防御の第一歩だ。
      * ファイルを送るにはWeb上で提供されている無料転送サービスも使うことができる。
      * 添付ファイルを減らすことは、メールサーバーや通信回線の負荷の軽減にもつながる。
  + 2-10：標的型攻撃メールへの対応
    - すぐやろう
      * ■ 不審な電子メールは開かない
      * ■ 標的型攻撃メールを見分ける
    - 入り口対策、潜伏期間対策から出口対策
      * ウイルスの侵入防御
        + □OSやアプリケーションの脆弱性の解消
        + □スパムメールのフィルタリング
        + □従業員教育
        + ・不審なメールを開かない
        + ・ウイルス対策ソフトを適切に導入
      * ウイルスの早期発見
        + □ウイルス対策ソフトによる各機器の感染チェック
        + □不審な通信などの監視
      * 外部への情報漏えい防止
        + □統合型セキュリティ機器（UTM）によるデータ送信のチェック
    - 巧妙な標的型攻撃メールの事例
      * これは、とある会社の社員に届いたメールです。その会社が加盟する健康保険組合からの「医療費通知のお知らせ」というメールだったので、添付されていた「医療費通知のお知らせ」というファイルを開きました。クリックした途端に不正プログラムが動きだし、遠隔操作ツールが実行されてしまいました。添付ファイルはワードのアイコンになっていましたが、拡張子は「doc」でも「docx」でもなく、「医療費通知のお知らせ.exe」という不正プログラムだったのです。
      * これは実際にあった事例です。同じように、取引先を偽装して、「請求明細」や「明細書」というタイトルの不正プログラムが送られてきた事例もあります。 ※警察庁発表によると2019年には、確認された標的型攻撃メールは5300を超える。
    - こんな添付ファイルに注意だ
      * ●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
  + 2-11：迷惑メール発信への対応
    - すぐやろう
      * ■ウイルス対策ソフトで迷惑メールをブロック
      * ■統合型セキュリティ機器（UTM）※で迷惑メールの送信をチェック
      * 最近ではスマートフォンなどへの迷惑メールが日常茶飯事となっているため、その危険性があまり言われなくなっていますが、迷惑メールはサイバー攻撃の予兆の1つであることを認識しましょう。
    - ＜迷惑メールの発信は受け取り拒否につながる＞
      * 迷惑メールと判断された送信元のIPアドレスを管理する「ブラックリスト」といわれるデータベースがあります。ウイルス対策ソフトの中には、このブラックリストを参照して、このリストに登録されたメールサーバーからのメールは受け取りを拒否する機能を持ったものもあります。もし、あなたの会社が迷惑メールを発信してブラックリストに登録され取引先で受け取り拒否されたら、事業に大きな支障が生じます。
    - ＜万が一ブラックリストに登録されてしまったら＞
      * 取引先で受け取り拒否されたら、拒否した理由が記されたメールが送られてきます。そこに参照したブラックリスト名とURLが記載されています。
      * ブラックリストを登録・管理している団体のWebサイトに行き、送信元IPアドレスを入力し、リストから削除するための手順を確認してください。ただし、ブラックリストを管理している団体のほとんどは海外の団体ですから、削除依頼は英語で行う必要があります。
    - 迷惑メールを発信していないかをチェック！
      * もし、あなたの会社のメールサーバーが迷惑メール発信の踏み台にされているか疑わしいと思ったら、すぐにメールサーバーの通信量を調べよう。迷惑メールの踏み台となっている場合は、毎日数十万通のメールを発信しているはずだ。
  + 2-12：安全なWebサイト利用
    - すぐやろう
      * ■不用意に信頼できないサイトへアクセスしないようにする
      * ■パスワードをブラウザー※に保存しない
    - ＜フィッシングサイト＞
      * ●メールの送信者欄（Fromアドレス）は偽装できるため、なりすましメールに注意する。
      * ●必要に応じて、金融機関が推奨するセキュリティソフトなどの導入も検討する。
      * ●カード番号や暗証番号を入力するような依頼がメールで来ることはなく、もしそのようなメールが金融機関などから届いた場合は、送信元に電話で問い合わせたり、ホームページを見たりして真偽を確認する。
    - ＜ワンクリック詐欺（不正請求）につながるサイト＞
      * ●信頼できないサイトにはアクセスしない。
      * ●アクセスしても安易なダウンロードはしない。
      * ●ウイルス対策ソフトなどの警告画面が表示された場合は次に進まない。
    - 詐欺サイトにご注意を！
      * フィッシングサイトなどの詐欺サイトが巧妙化している。正式なものと「URLが1文字だけ」違うといった騙されやすいサイトもあるので要注意だ。検索などで調べた場合でも、該当のサイト名やURLスペルが合っているかをよく確かめよう。
      * 同時に鍵マークがURL表示窓に出ているかも確認しよう。この鍵マークをクリックするとサイト運営組織の実在を証明する電子証明書※の内容を確認することができる。しかし、鍵マークがあっても詐欺サイトの可能性がある。
      * また、詐欺サイトへの誘導にはメールやSMSも使われる。メールやSMSに記載されたURLや電話番号を安易にクリックしてはいけない。メールソフトやWebブラウザーにフィッシングサイト判別機能があればこれらを活用するのも1つの手だ。
  + 2-13：閲覧制限
    - すぐやろう
      * ■業務に不要なWebサイトへのアクセスを制限する
    - ＜URLフィルタリング＞
      * 特定のURLアドレスを持つWebサイトとのアクセスを制限します。アクセス制限には次のような方法があります。
      * ●商用サービスとURLデータベースを使った規制
      * フィッシングサイトやウイルスを配布するような不正なWebサイトのアドレスをURLデータベースから取得し、Web（URL）のフィルタリングを行うことで、アクセスを制限します。
    - ＜キーワードによる規制＞
      * ●キーワードによる規制
      * ブラウザーに対し入力するキーワードを管理者が事前に規制します。
    - 何が防げるの？
      * インターネットの業務外利用を制限することによって、安全でないWebサイトの利用や不正プログラムのダウンロードを防ぐことができます。
    - 閲覧制限への対策は比較的手薄!?
      * 2020年の新型コロナ禍に際して、感染拡大防止の観点から多くの企業でテレワークが導入された。しかし、総務省が実施した「テレワークセキュリティに関する実態調査」（2020年10月）からは、テレワーク導入に際しての経営課題がセキュリティの確保にある点が分かる。また、同調査の「各種サイバー攻撃に関する対策の実施状況」からは、Webサイトのフィルタリングなどの閲覧制限対策が比較的手薄になっている姿も浮かび上がる。
  + 2-14：重要情報の洗い出し
    - すぐやろう
      * ■機密性、完全性、可用性の観点から重要度を評価する
    - ＜情報セキュリティの三大要件＞
      * 適切な情報管理を行うために3つの観点から重要度を評価し、重要度の高いものを優先して対策を行いましょう。
      * 機密性
        + アクセスを許可された者だけが情報にアクセスできる

情報漏えい防止、アクセス権の設定

* + - * 完全性
        + 情報と処理方法が正確でかつ完全である

改ざん防止・検出

* + - * 可用性
        + 許可された利用者が必要なときに情報と関連資産にアクセスできる

電源対策、システムの二重化

* + - ●個人情報とは
      * ①氏名、②住所、③電話番号、④メールアドレス、⑤生年月日、⑥性別　など
    - ●これも個人情報（紙媒体／データベース）
      * ①各種会員の申込書
      * ②顧客の氏名が表記される売上伝票
      * ③顧客氏名や会員コードが入っているもの
      * ④アンケートなど氏名を記入させるもの
      * ⑤特定の個人を識別できるメールアドレス情報
      * ⑥防犯・監視カメラに記録された本人と判別できる映像　など
    - 企業の各部門で保有している情報資産の例
  + 2-15：重要情報の保管
    - すぐやろう
      * ■ オフィスへの入退室を管理する
      * ■クリアデスク・クリアスクリーンを徹底する
      * ■ 重要情報を一元管理する
      * ■ 保管室への入退室を管理する
      * ■ 重要書類の持ち出しを管理する
      * ■重要情報廃棄の基本ルールを徹底する
    - ＜オフィス全体の入退室管理＞
      * 最終退室者は以下を行います。
      * ●全員のパソコンがシャットダウンされ、プリンターなど周辺機器の電源が切られているか確認する。
      * ●全ての出入り口の施錠を確認する。
      * ●退室時刻と退室者氏名を管理簿に記録する。
    - ＜入退室管理（訪問者）＞
      * オフィスに見知らぬ人がいることは、セキュリティ上問題があります。整理整頓が行き届いていたとしても、見ず知らずの人に勝手に情報を盗み見されたり、持ち出されたりすることもあるかもしれません。
      * ●訪問記録に記入してもらう。
      * ●名刺をもらう。
      * ●知らない人には声をかける。
      * ●訪問した人をオフィスに1人で残さない。
    - ＜クリアデスク・クリアスクリーンの徹底＞
      * ●重要書類、スマートフォン、重要な情報を保存したUSBメモリーやCDなどの電子媒体を業務以外のときは机上に放置せず、クリアデスクを徹底する。
      * ●離席時にはパソコンの画面をロックし、クリアスクリーンを徹底する。
      * ・スクリーンセーバーの起動時間を10分以内に設定し、パスワードを設定
      * ・スリープモードの起動時間を10分以内に設定し、解除時のパスワード保護を設定
      * ・離席時には［Windows］＋［Ｌ］キーを押してパソコンをロック（Windowsの場合）
    - ＜重要情報の一元管理＞
      * 机の上に放置した情報は、誰かに持ち去られたり、盗み見られたりする危険にさらされています。関係者以外が見たり、触れたりすることができないように、重要情報は放置せず、一元管理する必要があります。保管場所を定め、作業に必要な場合のみ持ち出し、終了後に戻すようにしましょう。
    - ＜保管室への入退室管理＞
      * ●保管室への入退室者を制限する。
      * ●施錠忘れを防ぐために入退室者と時間の記録を残す。
      * ●机の上をチェックする。
      * ●パソコン（モニターも）や機器の電源をチェックする。
      * ●消灯をチェックする。
      * ●施錠をチェックする。
    - ＜重要書類の持ち出し＞
    - ＜スタンドアロンのパソコンによる管理＞
      * ネットワークを経由した感染と情報流出を防ぐために、最重要情報についてはネットワークに接続をしていないスタンドアロンのパソコンで管理し常時ネットワークには接続しない。
    - ＜重要情報廃棄の基本ルール＞
      * サーバー・パソコン※リース物件返却・売却含む
        + ・システム担当がハードディスクを取り出し破壊
        + ・システム担当がデータ抹消ツールにより完全消去
        + ・専門のデータ消去サービスを利用する。ただし、依頼先の会社の信頼度も考慮して業者を選定する
      * 外付けハードディスク
        + ・システム担当が破壊
        + ・システム担当がデータ抹消ツールにより完全消去
      * CD・DVDなどのディスク
        + ・利用者がシュレッダーで細断
        + ・利用者がディスクの両面にカッターなどでキズを入れる
      * USBメモリー
        + ・システム担当がデータ抹消ツールにより完全消去
      * 重要書類
        + ・利用者がシュレッダーで細断
        + ・大量の場合はシステム担当が溶解処分を専門業者に依頼し、廃棄証明書を取得
      * これらの方法を企業・組織の情報資産の重要度に応じて組み合わせ、最適な方法を取ることが重要です。
    - 廃棄資産の転売で行政情報流出の危機に
      * 2019年11月、個人情報を含む神奈川県の大量の行政データが蓄積されたハードディスク（HDD）が転売される事案が明らかになった。
      * これは、リース契約満了によって県が返却したHDDのデータ消去（物理破壊）を委託された企業の社員がデータ消去の不十分な状態で一部を持ち出し、ネットオークションで販売したために発生した。
      * この事案を受け、神奈川県庁は同年12月16日に再発防止検討チームを発足。外部に出たHDDは21日までに全て回収し、2020年1月27日に情報流出防止策を決定した。同月、総務省も「県情報を保存するために使用した情報機器からの情報流出防止策」を発出。原因特定とデータ抹消措置の作業完了まで県職員が立ち会い確認するなどの今後の再発に向けた具体的な防止策を明らかにした。
* **【Mission03-A】経営者は事前に何を備えればよいのか【守り】**
  + 概要
    - サブタイトル【組織維持のために】 経営者、 管理者が、自組織の現状として認識すべきこと
      * 管理者が知っておくべきこと（管理者を設置していない場合は経営者が自ら知っておくべきこと）
    - 総論
      * サイバーセキュリティの被害に遭った場合、 組織の存立が危ぶまれる事態になりえることを自覚する ・世の中で起こっているセキュリティ被害を対岸の火事だと思っている経営者、 ITは導入しているにも関わらずセキュリティ対策のための費用はないとして対策に後ろ向きの経営者、 最も重要な情報にアクセスする権限を持ちながら、 セキュリティに関しての意識の低い経営者。 これらの経営者が最大のセキュリティリスク
      * 国は、 大企業のみならず、 中小企業も、 「サインバーセキュリティ経営ガイドライン」を参照することを求めている
    - **3-A-1: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。**
      * **改版理由**
        + **中小企業の情報セキュリティ対策ガイドラインの改版（第２版⇒第３版） 差分を説明する**
        + 組織の社会的責任の認識
  + **3-1：サイバーセキュリティ対策が経営に与える重大な影響**
    - ビジネスの継続のためにはITの活用は不可欠
      * 中小企業にとって、業務の効率化、生産の効率化、人材確保は重要な課題であり、業務、生産工程などの運用コストの削減・効率化のために、ITは大きな柱として活用されています。より一層の業務効率の改善や生産力向上を目指して、モバイル端末の活用や外部クラウドサービスの活用も進んでいます。
    - ITの活用にはサイバー攻撃などへの備えが必要
      * ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、サイバー攻撃など）で事業資産や社会的信用が失われ、早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性があります。 サイバー攻撃は事前のセキュリティ対策によって、防御が可能です。
    - サイバーセキュリティ対策は経営者が自ら実行
      * サイバーセキュリティリスクは経営に重大な影響を及ぼす可能性がある一方で、投資効果が見えにくいことから、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップを発揮することが必要不可欠です。
    - **【補足説明材料】**
      * 情報セキュリティ対策は、 経営に大きな影響を与えます！
      * 経営者が法的・道義的責任を問われます！
      * 組織として対策するために、 担当者への指示が必要です！
        + 中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】
      * セキュリティ侵害を受ける70～80%が人為的なミス、 故意
      * サイバーセキュリティ対策の中で最もコストがかかるのが技術的対策。 しかし全てのリスクに対して技術的対策をすることは困難。 悪意があれば技術的な対策はすり抜けられる
      * 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。
      * 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。
  + **3-2：情報セキュリティ対策を怠ることで企業が被る不利益**
    - 金銭の損失
      * 顧客の個人情報や取引先などから預かった機密情報を万一漏えいした場合は、多大な損害賠償が発生します。また、インターネットバンキングの不正送金などで直接的な損失を被る企業も増えています。
    - 顧客の喪失
      * サイバー攻撃を受けた企業は管理責任を問われ、社会的評価は低下し、顧客離れなど大きなダメージを受けることになります。風評被害がいつまでも続き、イメージが回復せず事業の存続が困難になる場合もあります。
    - 業務の喪失
      * サイバー攻撃を受けると、被害の拡大を防止するため、システムを停止する措置が必要です。その間はメールすら使えなくなり、営業機会を喪失するとともに、社内の業務も停滞してしまいます。
    - 従業員への影響
      * 内部不正が容易に行えるような職場環境は、従業員のモラルを低下させます。また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。
    - **【補足説明材料】**
      * (1) 金銭の喪失,(2) 顧客の喪失, (3) 業務 の喪失, (4) 従業員 への影響
        + Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】

* + **3-3：経営者に問われる責任**
    - 経営者などに問われる法的責任
      * ITを利活用する際には、顧客の個人情報を収集・活用する、他社への差別化として技術情報を活用するなど、さまざまな重要情報を取り扱います。そのため、企業とその経営者には高い責任が求められます。
      * 企業が個人情報などを適切に管理していなかった場合、経営者や役員、担当者は刑事罰やその他の責任を問われることになります。場合によっては、経営者が個人として損害賠償責任を負うこともあります。
    - 関係者や社会に対する責任
      * 情報漏えいを引き起こした企業の経営者には、法的責任だけでなく、その情報の提供者や顧客に対して損害賠償や謝罪などが求められます。
      * また、会社を代表して、社会に対して情報漏えいの原因や再発防止策を明らかにする義務があります。さらに、営業機会の喪失・売上高の減少・企業のイメージダウン・取引先との信頼関係の喪失などを引き起こすことにより、事業に大きなダメージを与え、経営者としての経営責任を果たすことができなくなります。
    - 海外の法律への対応も必要
      * サイバーセキュリティへの注目は世界中で高まっており、関連法案が世界各国・地域で施行されています。近年はWebなどで個人情報を比較的容易に収集でき、海外との直接取引も容易です。事業展開の中でこうした活動を行っている場合には、諸外国の法律に抵触しないように注意が必要です。
      * （例）・欧州連合（EU）：EU 一般データ保護規則（General Data Protection Regulation：GDPR）
      * ・中華人民共和国：中国サイバーセキュリティ法（CS法）
      * ・アメリカ合衆国：「NIST SP800-171」（米国政府の調達品に関するセキュリティガイドライン）
    - サイバーセキュリティ対策の情報開示
      * ５G、IoTやAIをはじめとしたICT利活用が社会・経済のあらゆる場面に浸透しつつある中、有効なサイバーセキュリティ対策を講じることは企業の経営課題となっています。加えて、企業の社会的責任を果たし、ステークホルダーからの信頼を得るためには、それらの情報を適切に開示することも重要な視点となっています。
    - **【補足説明材料】**
      * (1) 経営者などに問われる法的責任
        + ・個人情報・他社から預かった秘密情報・自社の秘密情報・株価に影響を与える可能性のある未公開内部情報
      * (2) 関係者や社会に対する責任
        + ・営業停止、 売上高の減少、 企業イメージの低下などで、 自社に損害をもたらずだけでなく、 取引先に対する信頼関係の喪失、 業界やサービス全体のイメージダウン・法令順守・顧客・取引先・従業員

Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】

* + - * **【Web版】**
        + 【参考】情報セキュリティ対策を怠ることで企業が被る不利益 【中小企業の情報セキュリティ対策ガイドライン案】

資金の喪失

顧客の喪失

業務の喪失

従業員への影響

* + - * + 【参考】経営者が負う責任【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】

経営者などに問われる法的責任

個人情報

他社から預かった秘密情報

自社の秘密情報

関係者や社会に対する責任

営業停止、 売上高の減少、 企業イメージの低下などで、 自社に損害をもたらずだけでなく、 取引先に対する信頼関係の喪失、 業界やサービス全体のイメージダウン

* + - * + 【参考】経営者が認識すべき「3原則」【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】

Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン

原則１ 情報セキュリティ対策は経営者のリーダシップのもとで進める

経営者は、 IT活用を推進する中で、 情報セキュリティ上のリスクを認識し、 自らリーダーシップを発揮して対策を進めることが必要です

原則２ 委託先における情報セキュリティ対策まで考慮する

原則３ 情報セキュリティに関する関係者とのコミュニケーションは、 どんなときにも怠らない

* + - * + 経営者として取り組むべき「重要 7項目の取組」【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】

取組１ 情報 セキュリティ に関するリスクを認識し組織全体での対応方針を定める

情報セキュリティ対策を組織的に実施する意思を、 関係者に明確に示すために、 情報セキュリティに関する方針を定め、 要求に応じて提示できるようにしておきます。

取組２ 情報セキュリティ対策を行うための資源（予約、 人材など）を確保する

情報セキュリティ対策を実施するために、 必要な予算と人材を確保します。

取組３ 情報セキュリティのリスクを把握し、 どこまで情報セキュリティ対策を行うのかを定めたうえで担当者に実行させる

事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、 必要十分な対策を検討させます。

取組４ 情報セキュリティ対策に関する定期的な見直しを行う

取組3で定めた情報セキュリティ対策について、 定期または随時に見直して、 必要な改善や追加の対策を決めるように担当者に指示します。

取組５ 業務委託する場合や外部ITシステムやサービスを利用する場合は、 自社で必要と考える対策が担保されるようにする

契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、 合意する必要があります。

取組６ 情報セキュリティに関する最新動向を収集する

新たな脅威に備えるようにします。 また、 知り合いやコミュニティへの参加で情報交換を積極的に行い、 得られた情報について、 業界団体、 委託先などと共有します。

取組７ 緊急時の社内外の連絡先や被害発生時に行うべき内容について準備しておく

情報セキュリティ対策を実施するとともに、 万が一のインシデントに備えて、 緊急時の連絡体制を整備します。 さらに、 その連絡体制がうまく機能するかをチェックするためインシデントを想定した模擬訓練を定期的に行うと理想的です

* + - * + 【Web版コラム】組織の姿勢3分類(企業経営のためのサイバーセキュリティの考え方の策定について （2016年8月2日）【NISC】より)

【レベル１】自らセキュリティ対策を行う上で、 事業上のリソースの制約が大きい企業

主に中小企業等でセキュリティの専門組織を保持することが困難な企業。 小企業・零細企業の多く

小企業・零細企業の多く。 家庭も。

（主に中小企業等でセキュリティの専門組織を保持することが困難な企業）

ITを十分に活用していない組織、 サイバーセキュリティが自社の問題と認識していない組織

情報リテラシーの向上

個人情報、 企業機密、 知的財産

預かり情報

インターネットバンキング

最低限のサイバーセキュリティ対策

【レベル2】IT・セキュリティをビジネスの基盤として捉えている企業

（IT・サイバーセキュリティの重要性は理解しているものの、 積極的な事業戦略に組み込むところまでは位置づけていない企業）

高リスクの許容

必要以上のサイバーセキュリティ対策のため、 業務の効率化、 競争力強化を阻害している企業

【守りのIT投資】ITを活用した業務効率化、 生産性向上、 労働力確保を図っている組織

仮想化技術の適用

運用・保守コストの削減

【守りのセキュリティ対策】網羅的で費用対効果の高い対策の実施

【レベル3】ITの利活用を事業戦略上に位置づけ、 サイバーセキュリティを強く意識し、 積極的に競争力強化に活用しようとしている企業

（積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）

ITを成長エンジンとして活用【成長戦略より】

コスト削減から価値創造へ

中小企業の生産性向上、 人材不足の解消の糸口に

投資

情報化投資

革新的投資

研究開発等

経済的競争能力投資

職員の研修・訓練、 ブランディング、 マーケティング、 経営コンサルティングの外部委託

【攻めのIT投資】新技術、 新サービスを戦略的に活用した新ビジネス展開

【攻めのセキュリティ対策】攻めのセキュリティ対策（未知のリスクを許容）

クラウドサービス

IoT

第4次産業革命

ビッグデータ

AI

ブロックチェーン

テレワーク、 サテライトオフィス

* + **3-4：投資効果（費用対効果）を認識する**
    - サイバーセキュリティ対策にかかる費用の項目
      * サイバー攻撃に対するセキュリティ対策には、次のような項目があります。これらの項目を実現するためには、当然費用が発生します。
    - セキュリティ対策の投資効果を考える
      * あなたの会社のインターネット接続と業務システムが1週間停止した場合のビジネスへの影響度を考えたことがありますか？当然その間はメールもやり取りできないため、営業機会はなくなります。また、この時代にメールも送受信できないということで取引先との信頼関係もなくなります。それらの損失を数字に置き換えたものがセキュリティ対策の投資効果です。
    - 【コラム】セキュリティ対策は経営上の「投資」と位置付ける！
      * IDC Japanが2020年1月に実施した国内企業878社の情報セキュリティ対策の実態調査結果によると、2020年度の情報セキュリティ投資見込みについて38％の企業が2019年度を上回ると回答しています。総務省「通信利用動向調査（令和元年）」においても55.2%の企業が「何らかの被害を受けた」と回答。対策には相応のコストが必要なものの、近年は中小企業を含むサプライチェーンを狙った攻撃も増えています。こうした観点も鑑み、やむを得ない「経費」でなく、ITを利活用した積極的な経営への「投資」と位置付けることが重要です。
    - **【補足説明材料】**
      * セキュリティ対策の投資は、 人的対策、 管理的対策、 物理的対策、 それでもカバーできないことを技術的対策
      * サイバーセキュリティはやむを得ない「費用」でなく、 ITを利活用した積極的な経営への「投資」と位置付ける
  + **3-5：ITの活用診断**
    - 自社のIT活用状況を診断する
      * IT化において中小企業が注意したいのは、「IT化の範囲を一気に広げ過ぎない」という点です。中小企業が短期間であらゆる業務にITを導入しようとすると、コストの増大だけでなく、スケジュールが煩雑になり結果的に中途半端なクオリティーのシステムになるリスクがあります。下記の診断ツールが利用できます。
      * IT活用診断ツール
        + 中小企業基盤整備機構：IT経営簡易診断
        + 情報処理推進機構：DX推進指標
    - IT活用診断のカギは費用対効果
      * IT導入の目的は、既存ビジネスの効率化や新ビジネス展開などであり、IT化のための投資が、それによって得られる利益を上回っている場合は、投資を削減すべきです（参考「ITガバナンス」
      * IT化による想定利益＞IT化投資額 （IT導入、運用、セキュリティ対策費）
    - ITおよびサイバーセキュリティに関する組織の視点6分類
    - **【補足説明材料】**
      * **IT活用診断ツールのコンテンツ最新調査**
        + DX推進指標　自己診断結果分析レポート（IPA）の「背景」を参照
      * 費用対効果
        + IT化による想定利益＞IT化投資額（IT導入、 運用、 セキュリティ対策費）
        + IT化の目的は、 既存ビジネスの効率化、 新ビジネス展開等であり、 IT化のための投資が、 IT化によって得られる利益を上回っている場合は、 IT化投資を削減すべきである
      * 視点6分類
        + 「企業経営のためのサイバーセキュリティの考え方」を参考に、 分類を追加してみたもの

【参照】「企業経営のためのサイバーセキュリティの考え方」【2016年8月3日NISC】

* + - * + 【理想的に】ITの利活用を事業戦略上に位置づけ、 サイバーセキュリティを強く意識し、 積極的に競争力強化に活用しようとしている企業

（積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）

ITの利活用と情報セキュリティ対策のバランスが取れている企業

情報のオープン化、 外部情報の活用、 機密情報の保護をきちんと行い、 ITの利活用により新しいサービスを展開

* + - * + 【もっと積極的に】IT・セキュリティをビジネスの基盤として捉えている企業

（IT・サイバーセキュリティの重要性は理解しているものの、 積極的な事業戦略に組み込むところまでは位置づけていない企業）

ITを積極的に活用してビジネスの発展を目指すことが必要

* + - * + 【無駄な投資】過剰なセキュリティ意識により、 ITの利活用を著しく制限し、 ITの利活用を競争力強化に活用させていない企業

ITの利活用と情報セキュリティ対策のバランスが取れていなく、 費用対効果の悪い企業

基本姿勢として、 情報は全て機密、 IT環境は必要最低限に利用を制限

必要以上のセキュリティ対策により、 無駄に費用をかけ、 業務効率、 サービスの向上を阻害している企業

過剰なセキュリティ意識により、 ITの利活用を著しく制限し、 競争力強化に活用させない企業

過剰なリスク意識により、 インターネットでの情報発信、 情報収集や、 IT活用による業務効率を向上させる意識のない企業

セキュリティ偏重の判断は、 業務の現場の不便をもたらし、 柔軟な発想や市場変化に対する機敏性を損なわせる。 最悪の場合、 ビジネスイノベーションの規格をも潰してしまう。

組織内のITリテラシーの向上が十分でないために、 低いレベルの人に合わせたセキュリティ対策のために、 意識の高い人の業務の効率化を阻害している

リスクを再評価して過度にならない適切なセキュリティ対策の再構築が必要

* + - * + 【危険】情報セキュリティ対策の必要性は理解しているが、 必要十分なセキュリティ対策が出来ていないにも関わらず、 ITの利活用を進めている企業

ITの利活用と情報セキュリティ対策のバランスが取れていない企業

（IT・サイバーセキュリティの重要性は理解しているものの、 積極的な事業戦略に組み込むところまでは位置づけていない企業）

業務効率とのバランスが取れているセキュリティ対策を実施しようとしている企業

情報セキュリティポリシーの策定と実践、 定期的な監査

創造力、 発想力のある人材の育成

ITスキルと知識を持った人材の育成が必要

* + - * + 【危険】情報セキュリティの必要性を理解していない企業 自らセキュリティ対策を行う上で、 事業上のリソースの制約が大きい企業

（主に小企業・零細企業でセキュリティの専門組織を保持することが困難な企業）

まずは、 最低限の情報セキュリティ対策を理解し、 コストを掛けずに効果の大きいことから実施することが必要

* + - * + 【対象外】ITを利用していない企業

サイバーセキュリティ侵害が起こりえず、 対象外だが、 業務効率化のためにITの活用を促すか？？

情報セキュリティ対策は必要

* + **3-6：サイバーセキュリティ対策診断**
    - サイバーセキュリティ投資（コスト）とは
      * サイバーセキュリティの投資（コスト）としては、P94に示した対策費用以外にも、さまざまなコストがあります。
    - サイバーセキュリティ対策はどこまでやればよいのか
      * これで万全というサイバーセキュリティはありません。特に、技術的対策にどれだけ投資してもリスクは残ります。管理的対策や人的対策を優先する方が効果的です。想定被害額を上回るセキュリティ対策費を費やすことは現実的ではありません。セキュリティ対策費が、セキュリティ侵害による想定被害額を上回っている場合は、対策費を削減すべきです。
      * 問題は残ったリスク（残留リスク）によって発生した被害の想定被害額が、支出可能な対策費を上回っている場合は、事業継続が困難になりますので、支出可能な対策費に収まるように残留リスクを下げる対策を講じるか、支出可能な対策費を捻出する必要があります。
      * 残留リスクをどこまで許容できるかは、まさに経営者の判断です。
    - 【コラム】「ITガバナンス」と6つの原則
      * IT活用は今や企業戦略の中で不可欠となっています。この観点から経営層には組織価値を高め、ITシステム戦略の策定や運用に必要となる組織能力である「ITガバナンス」が求められています。その成功には、経営層が次の6原則を実践することが肝要とされています。以下、要約して紹介します。
      * 1.責任：役割に責任を負う人は、その遂行権限を持つ
      * 2.戦略：情報システム戦略は現在と将来を考慮して、そのニーズを満たす必要がある
      * 3.取得：情報システムの導入は短期・長期の両面で効果・リスク・資源のバランスを考慮した意思決定に基づく必要がある
      * 4.パフォーマンス：情報システムは現在および将来のニーズを満たす必要がある
      * 5.適合：情報システムは関連する全ての法律および規制に適合する必要がある
      * 6.人間行動：情報システムのパフォーマンス維持に関わる人間行動を尊重する必要がある
      * 参考：経済産業省「システム管理基準」
        + https://www.meti.go.jp/policy/netsecurity/downloadfiles/system\_kanri\_h30.pdf
    - **【補足説明材料】**
      * 費用対効果
        + セキュリティ侵害による想定被害額（経済的損失、 社会的信用）＞セキュリティ対策費
        + セキュリティ対策費が、 セキュリティ侵害による想定被害額を上回っている場合は、 対策費を削減すべきである
        + セキュリティ侵害発生時に許容可能対策費>残留リスクによる想定被害額
        + 重大なセキュリティ侵害が発生した時の想定被害額が、 支出可能な対策費を上回っている場合は、 事業継続が困難になる。 支出可能な対策費に収まるように、 残留リスクを下げる対策を講ずるか、 支出可能な対策費を捻出する必要がある
        + ただ、 技術的対策はどれだけ投資してもリスクは残る。 管理的対策、 人的対策を優先するほうが効果的である
        + 残留リスクをどこまで許容できるかは、 経営者の判断である
  + **3-7：情報セキュリティ対策診断**
    - 情報セキュリティ対策を診断する
      * 企業（組織）はセキュリティ上の脅威に取り囲まれています。
      * ・個人、顧客、企業（組織）情報を脅威から守る。
      * ・会社内の設備を脅威から守る。
      * 情報セキュリティ対策は常に新たな脅威に対応する必要があり、継続的に自社の対策状況を診断する必要があります。
    - やってみよう！情報セキュリティ対策診断
      * ・わが社のセキュリティ対策は大丈夫か？
      * ・セキュリティ対策予算を増額したいが、どこにどう使ったらいいのか分からない。
      * ・まだ取り組んでいないセキュリティ対策を考えたい。
      * ・自社の情報セキュリティ対策状況はどこが弱点で、どこが強いのか知りたい。
      * こうした要望に応えて、情報処理推進機構（IPA）では、「情報セキュリティ対策ベンチマーク」を提供しています。
      * 情報セキュリティ対策ベンチマークは、設問に答えるだけで、自社のセキュリティレベルを他社との比較で診断することのできるシステムです。
      * 散布図、レーダーチャート、スコア（点数）などの診断結果が自動的に表示されます。
    - **【補足説明材料】**
      * 物理的なセキュリティ対策も合わせて実施しているか。 物理的セキュリティ対策は、 直接的にはサイバーセキュリティ対策ではないが、 IT関連機器の設定変更など、 サイバーセキュリティ侵害のきっかけを作る可能性がある
  + **3-8：業務の効率化、 サービスの維持のために**
    - 守りのIT投資と攻めのIT投資
      * 守りのIT投資という言葉を聞いたことがありますか。
      * 従来、IT活用は業務効率化やコスト削減を目的として、定型業務の自動化に集中していました。近年、売り上げ増加を目指したIT投資を「攻めのIT投資」と呼ぶようになり、従来のIT投資を「守りのIT投資」と呼んでいます。
    - 業務の効率化にITを活用
      * 経営者のみなさんが重視している経営課題の1つは、業務効率化やコスト削減です。
      * 改善活動による業務効率化という手法は以前から展開されています。IT活用は、受発注業務や経理業務など、定型・繰り返しが多い業務プロセスを自動化、簡便化することに適しています。
    - 生産性の向上やサービス向上のためにITを活用
      * ITを活用すれば、コスト削減だけでなく、業務のスピードアップ、品質向上、ミス低減など、生産性の向上にもつながります。また、生産状況の見える化などを通して、工程管理や生産管理など生産性を大幅に向上することも可能です。また、顧客サービスのスピードアップなどを通して、サービス力の向上にもつながります。
    - **【補足説明材料】**
      * 業務の効率化、 サービスの維持のために
        + 中小企業にとって、 業務の効率化、 生産の効率化、 人材確保は重要な課題であり、 業務、 生産工程等の運用コストの削減、 効率化のためにITを活用してきた。
        + より一層、 効率化を図っていかなければ、 ビジネスは継続できず、 モバイル端末の活用、 外部クラウドサービスの活用も、 効率化に有効な手段の一つとして普及が進んできている
        + しかし、 ITを活用してどんなに利便性の高いサービスを提供しても、 どんなに業務を効率化しても、 緊急事態（自然災害、 大火災、 感染症、 テロ、 セキュリティ侵害、 、 ）が発生して、 事業資産（人・もの（情報及び設備）・金）、 社会的信用が失われ、 早期復旧ができない場合は、 事業の継続が困難になり、 組織の存立さえも脅かされる可能性がある。
        + 業務やサービスの改善のために、 インターネットに接続してITを活用する際には、 同時に、 サイバー攻撃等への備えが必要である
        + ITを活用したサービスの構築・運用に掛かる費用は、 経費ではなく先行投資。 リスクに見合った情報セキュリティ対策は、 サービスの構築・運用の中で実施すべき先行投資であり、 緊急事態が発生した後に対処する経費として想定してはいけない
        + ITを導入する際に、 併せてセキュリティ対策をすることにより、 コストを削減できる
  + **【補足説明材料】**
    - **【コラム】クラウドサービスのメリットは？**
      * ITシステムに関する技術に詳しい人材がいない場合は、 外部サービスを利用したほうが、 コストとセキュリティ対策との両面から有利な場合も多い
      * ・社内サーバーが不要・IT投資のリスク軽減・常に最新でメンテナンスが不要・導入や維持に関する社内担当者の負担軽減
    - **【コラム】クラウドサービス導入の留意点**
      * できるだけしっかりした会社から提供されているサービスを選ぶために
      * 取り扱う情報の格付及び取扱制限を踏まえ、 情報の取扱いを委ねることの可否を判断する
      * クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定
      * クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、 委託先を選定する際の要件とする
      * クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、 情報の流通経路全般を見渡した形でセキュリティ設計を行った上でセキュリティ要件を定める
      * クラウドサービスに対する情報セキュリティ監査による報告書の内容 、 各種の認定・認証制度の適用状況等から、 クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断する
    - **【Web版コラム】生産性向上のための「デジタル・ワークプレイス」**
      * 【担当：中山】
      * 【参考】DAX20-0402-1 ITロードマップ2018年版【2018年3月NRI】
      * デジタル化時代のデバイスやテクノロジーを駆使して、働くプロセスや場所・コミュニケーション、コラボレーションのあり方を 新たに組み立てようとする考え方
      * 生産性向上のための「デジタル・ワークプレイス」の導入におけるサイバーセキュリティ対策
      * 従業員エクスペリエンスを向上（働き方改革等）するシステムの導入におけるサイバーセキュリティ対策
      * テレワークソリューション
        + Sec01-02-60\_各種ガイドブックの内容要約(働き方改革関連)
        + 従業員にとって、いつでもどこでも柔軟な働き方ができるインフラやアプリケーションが一貫して提供されることで、 仕事をする上での利便性やユーザビリティが向上する
        + **【コラム】テレワークではじめる働き方改革テレワークの導入・運用ガイドブック【厚生労働省】**

システム方式

リモートデスクトップ

仮想デスクトップ

クラウド型アプリ

会社PC持ち帰り

端末デバイス

リッチクライアント

シンクライアント

タブレット型PC

スマートフォン

携帯電話

セキュリティ

本人認証

端末認証

端末管理

暗号化通信

ストレージ暗号化

* + - * + **【コラム】テレワークセキュリティガイドライン（第4版）【2018年4月総務省】**

Sec01-02-60\_各種ガイドブックの内容要約(働き方改革関連)

テレワークセキュリティガイドライン第４版【総務省】

* + - * + **【コラム】電子印鑑の活用**
        + 【コラム】私用端末のビジネス利用

スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書 【2015年 5月21日NISC】

* + - **【コラム】事業継続計画（BCP）の一環としてのサイバーセキュリティ対策（明文化）**
      * 【担当：石井（茂）】
      * ***改訂箇所：Mission4-1( p.134～144)を改訂***
      * 事前だけでなく事後の「緊急時対応」も含めた一連の対応として、 フェーズごとの対策
        + 特定
        + 防御
        + 検知
        + 対応
        + 復旧
  + **3-9：経営者が認識すべきサイバーセキュリティ経営の3原則**
    - 【原則1】サイバーセキュリティ対策は経営者のリーダーシップで進める
      * サイバー攻撃のリスクをどの程度容認するのか、セキュリティ投資をどこまでやるのか、経営者が決めなければサイバーセキュリティ対策はスタートしません。
      * 従業員は安心して業務に集中できる環境を求めますが、利便性が低下し、面倒な作業を伴う対策には積極的に取り組めないこともあります。経営者が自らリーダーシップを発揮しなければ、サイバーセキュリティ対策は進みません。
    - 【原則2】委託先のサイバーセキュリティ対策を把握する
      * 子会社で情報漏えいが発生した場合はもちろんのこと、外部委託先に提供した情報がサイバー攻撃により流出してしまうことも経営にとっては大きなリスク要因です。
      * 自社のみならず、系列企業やサプライチェーンのビジネスパートナー、委託先などのサイバーセキュリティ対策に関しても、必要に応じてサイバーセキュリティ対策の報告を求め、不十分な場合は対処を要請します。
    - 【原則3】関係者とのサイバーセキュリティに関するコミュニケーションはどんなときにも怠らない
      * 顧客、取引先、委託先、代理店、利用者、株主などからの信頼を高めるには、普段からサイバーセキュリティ対策についての情報開示に努め、関係者との適切なコミュニケーションを図ることが必要です。
    - **【補足説明材料】**
      * 経営者は、 以下の３原則を認識し、 対策を進めることが重要である。
        + 【旧版】サイバーセキュリティ経営ガイドライン Ver 1.１【2016年12月8日METI】
        + 【旧版】中小企業の情報セキュリティ対策ガイドライン（第2版）
        + （１）経営者のリーダーシップが重要。 経営者は、 IT活用を推進する中で、 サイバーセキュリティリスクを認識し、 リーダーシップによって対策を進めることが必要

ビジネス展開や企業内の生産性の向上のためにITサービス等の提供やITを利活用する機会は増加傾向にあり、 サイバー攻撃が避けられないリスクとなっている現状において、 経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である。

また、 サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった後、 企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。

このため、 サイバーセキュリティリスクを多様な経営リスクの中での一つとし適切に位置づけ、 その対応方針を組織の内外に明確に示しつつ、 経営者自らがリーダーシップを発揮して経営資源を用いて対策を講じることが必要である。 その際、 変化するサイバーセキュリティリスクへの対応や、 被害を受けた場合の経験を活かした再発防止も必要である。

* + - * + （２）自社以外（ビジネスパートナー等）にも配慮。 自社は勿論のこと、 系列企業やサプライチェーンのビジネスパートナー、 ITシステム管理の委託先を含めたセキュリティ対策が必要

サプライチェーンのビジネスパートナーやITシステム管理の委託先がサイバー攻撃に対して無防備であった場合、 自社から提供した重要な情報が流出してしまうなどの問題が生じうる。

自社のみならず、 サプライチェーンのビジネスパートナーやITシステム管理の委託先を含めたセキュリティ対策を徹底することが必要である。

* + - * + （３）平時からのコミュニケーション・情報共有。 平時及び緊急時のいずれにおいても、 サイバーセキュリティリスクや対策、 対応に係る情報の開示など、 関係者との適切なコミュニケーションが必要

事業のサイバーセキュリティリスクへの対応等に係る情報開示により、 関係者や取引先の信頼性を高める。

万一サイバー攻撃による被害が発生した場合、 関係者と、 平時から適切なセキュリティリスクのコミュニケーションができていれば，関係者や取引先の不信感の高まりを抑え、 説明を容易にすることができる。 また、 サイバー攻撃情報（インシデント情報）を共有することにより、 同様の攻撃による他社への被害の拡大防止に役立つことを期待できる。

事業のサイバーセキュリティリスク対応として平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにする　などのコミュニケーションを積極的に行うことが必要である。

* + - * 【コラム】経営者として取り組むべき「重要7項目の取組」 【中小企業の情報セキュリティ対策ガイドライン（第2版⇒第3版）】
  + **3-10：【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**
    - 経済産業省と情報処理推進機構（IPA）がまとめた「サイバーセキュリティ経営ガイドラインVer2.0」を基に、経営者が情報セキュリティ全般を統括する「最高情報セキュリティ責任者（CISO）」に指示すべき重要10項目をまとめました。
    - **【補足説明材料】**
      * ガイドライン改訂前の主な課題
        + 昨今のサイバー攻撃の巧妙化により入口出口対策などの事前対策だけでは対処が困難。
        + 米国のサイバーセキュリティフレームワークでも事前対策だけでなく、事後（検知、対応、復旧）対策を要求。
        + 一方で従来のガイドラインはCSIRTの構築などの「対応」に関する項目はあるものの、 「検知」や「復旧」に関する内容が弱く、国際的な状況を踏まえるとガイドラインとの整合性が不十分。
      * 改訂のポイント（経産省発表）
        + 重要10項目の整理

新規に２項目（(5)対策実施と(8)復旧）追加するとともに、既存の項目を再整理。

重要１０項目の並びについても、３原則、及び作業の時系列を意識して再整理。

(7)の参考資料として付録C「インシデント発生時に組織内で整理しておくべき事項」を新規に追加。

* + - * + 事後対策の強化 ～検知・復旧対策の実施～

重要項目 指示5として「攻撃の検知」に関する、「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」を追加

重要項目 指示8 として「復旧」に関する、「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」を追加

* + - * + サプライチェーン対策の強化

重要項目 指示9の「サプライチェーンのビジネスパートナーや委託先等を含めたサイバーセキュリティ対策の実施及び状況把握」において、 委託先におけるリスクマネーの確保や委託先の組織としての活用の把握（ISMSやSECURITY ACTION） 等の留意点を追記

セキュリティ要件を満たさない事業者、製品、サービスはグローバルサプライチェーン、国内サプライチェーンからはじき出されるおそれ

* + - * + 事後対策の強化 ～インシデント発生時の対応～

インシデント発生時に組織として調査しておくべき事項をまとめた付録Cを追加

* + - * 【参考】
        + 最近のサイバー攻撃の状況を踏まえ、経営者の皆様へサイバーセキュリティの取組の強化に関する注意喚起を行います【2020年12月18日METI】
      * **サイバーセキュリティ経営ガイドライン2.0版（新版）**
        + 経営者は、CISO等に対して、以下の１０項目を指示し、 着実に実施させるとともに、 実施内容についてCISO等から定期的に報告を受けることが必要である。 自組織での対応が困難な項目については、外部委託によって実施することも検討する。
        + ＜情報共有活動における情報提供の記載を強調＞
    - ３．１．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
        + 指示すべきことはこれだ

・サイバーセキュリティリスクを経営リスクの1つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定させる

* + - * + やるべきことはこれだ

・組織全体の対応方針を組織の内外に宣言できるよう、セキュリティポリシーを策定

・セキュリティポリシーを従業員へ周知徹底

・セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示す

* + - * + **【補足説明材料】**

サイバーセキュリティリスクを経営リスクの一つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定させる。

対策を怠った場合のシナリオ

・経営者がサイバーセキュリティリスクへの対応を策定し、 宣言していないと、 サイバーセキュリティ対策などの実行が組織の方針と一貫したものとならない。

・トップの宣言により、ステークホルダー（株主、顧客、取引先など）の信頼性を高め、 ブランド価値向上につながるが、 宣言がない場合は、 企業におけるサイバーセキュリティへの重要度がステークホルダーに伝わらず信頼性を高める根拠がないこととなる。

【要約前】【3-1例】やるべきことはこれだ

セキュリティポリシーの策定

経営者が組織全体の対応方針を組織の内外に宣言できるように

経営者が企業の経営方針と整合を取り、サイバーセキュリティリスクを考慮

情報システムのみではなく、製造、販売、サービス等、事業に応じた対応方針

・セキュリティポリシーを従業員へ周知徹底

セキュリティポリシーは従業員が容易にアクセス可能な場所への掲載、従業員教育を実施などにより周知徹底

・セキュリティポリシーを一般公開

・セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示し、信頼性を高める。

※CISOとは、組織内の最高情報セキュリティの統括責任者であり、この役職を持った人材を確保できない場合は、経営者のその責を負う。

【3-1例】やるべきことはこれだ

経営者が企業の経営方針と整合を取り、サイバーセキュリティリスクを考慮したセキュリティポリシーを策定

経営者が組織全体の対応方針を組織の内外に宣言できるように

情報システムのみではなく、製造、販売、サービス等、事業に応じた対応方針を検討

セキュリティポリシーは従業員が容易にアクセス可能な場所への掲載、従業員教育を実施などにより周知徹底

セキュリティポリシーは従業員が容易にアクセス可能な場所（社内ポータルサイト等）への掲載、従業員教育を実施するなどによって周知徹底を図る。

・セキュリティポリシーを一般公開

・セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示し、信頼性を高める。

* + - * 指示２ サイバーセキュリティリスク管理体制の構築
        + 指示すべきことはこれだ

・サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる

* + - * + やるべきことはこれだ

・CISOは、責任範囲を明確にしたサイバーセキュリティリスク管理体制を構築

・取締役、監査役はサイバーセキュリティリスク管理体制を監査

・セキュリティ・バイ・デザインの観点を踏まえて体制を構築

・経営者のリーダーシップの下で体制を構築

* + - * + **【補足説明材料】**

サイバーセキュリティ対策を行うため、 サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。

その際、組織内のその他のリスク管理体制とも整合を取らせる。

対策を怠った場合のシナリオ

・サイバーセキュリティリスクの管理体制を整備していない場合、 組織としてサイバーセキュリティリスクの把握が出来ない。

・組織内におけるその他のリスク管理体制との整合を取らないと、 組織全体としてのリスク管理の方針と不整合が生じる恐れがある。

【要約前3-2】やるべきことはこれだ

・CISOは、サイバーセキュリティリスク管理体制を構築

責任範囲を明確に

・CISO等は、経営リスクに関する会議に参加

取締役、監査役はサイバーセキュリティリスク管理体制を監査

構築、運用されているか

セキュリティバイデザインの観点を踏まえて

企画・設計段階からサイバーセキュリティ対策を考慮した体制を構築

経営者のリーダーシップの下で体制構築

「サイバーセキュリティ体制構築・人材確保の手引き」

【3-2例】やるべきことはこれだ

・CISO等は、サイバーセキュリティリスク管理体制を構築

責任範囲を明確に

・CISO等は、経営リスクに関する会議に参加

取締役、監査役はサイバーセキュリティリスク管理体制を監査

構築、運用されているか

企画・設計段階からサイバーセキュリティ対策を考慮した体制を構築

セキュリティバイデザインの観点を踏まえて

「サイバーセキュリティ体制構築・人材確保の手引き」を参考に

「サイバーセキュリティ体制構築・人材確保の手引き」

* + - * 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
        + 指示すべきことはこれだ

・サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる

* + - * + やるべきことはこれだ

・サイバーセキュリティ対策に必要な費用の確保

・セキュリティ対策に必要な人材の確保

・セキュリティ人材育成、キャリアパスを設計検討

・外部の組織が提供するセキュリティ研修等の活用を検討

・各部門においてもセキュリティを意識した業務遂行ができるようにする

* + - * + **【補足説明材料】**

サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。

対策を怠った場合のシナリオ

・適切な予算確保が出来ていない場合、 組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、 信頼できる外部のベンダへの委託が困難となる恐れがある。

・適切な処遇の維持、改善ができないと、 有能なサイバーセキュリティ人材を自社にとどめておくことができない。

【要約前3-3】やるべきことはこれだ

サイバーセキュリティ対策に必要な費用の確保

・従業員向けやセキュリティ担当者向けなどの研修等の予算

継続的に役割に応じたセキュリティ教育を実施する。

セキュリティ対策に必要な人材の確保

セキュリティ人材育成、キャリアパスを設計検討

組織内のIT人材育成の戦略の中で、外部人材の採用も含めて

組織内で雇用することが困難な場合、専門ベンダも活用

外部の組織が提供するセキュリティ研修等の活用を検討

自組織でセキュリティ人材の育成が困難な場合

各部門においてもセキュリティを意識した業務遂行ができるように

セキュリティ人材のみならず

「サイバーセキュリティ体制構築・人材確保の手引き」

【3-3例】やるべきことはこれだ

サイバーセキュリティ対策に要する費用を確保

・明確にしたサイバーセキュリティ対策に必要な費用

・従業員向けやセキュリティ担当者向けなどの研修等の予算

継続的に役割に応じたセキュリティ教育を実施する。

セキュリティ人材育成、キャリアパスを設計検討

組織内のIT人材育成の戦略の中で、外部人材の採用も含めて

組織内で雇用することが困難な場合、専門ベンダも活用

外部の組織が提供するセキュリティ研修等の活用を検討

自組織でセキュリティ人材の育成が困難な場合

「サイバーセキュリティ体制構築・人材確保の手引き」を参考に

「サイバーセキュリティ体制構築・人材確保の手引き」

* + - ３．２．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
        + 指示すべきことはこれだ

・経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる

・その際、サイバー保険の活用や守るべき情報について専門ベンダーへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる

* + - * + やるべきことはこれだ

・経営戦略の観点から守るべき情報を特定し把握

・守るべき情報に対して、発生しうるサイバーセキュリティリスクを把握

・把握したリスクに対して、実施するサイバーセキュリティ対策を検討（リスクの低減策、回避策、移転策）

・実施できない場合は、残留リスクとしての識別も

・法令上の取り扱いも考慮したリスクの特定と緊急時の情報の保護が行えるような対策も検討

・製品・サービス等においても、セキュリティ・バイ・デザインの観点を踏まえて、対策を考慮

* + - * + **【補足説明材料】**

経営戦略の観点から守るべき情報を特定させた上で、 サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、 リスクに対応するための計画を策定させる。

その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、 残留リスクを識別させる。

対策を怠った場合のシナリオ

・企業の経営戦略に基づき、各企業の状況に応じた適切なリスク対応を実施しなければ、 過度な対策により通常の業務遂行に支障をきたすなどの不都合が生じる恐れがある。

・受容できないリスクが残る場合、想定外の損失を被る恐れがある

【要約前3-4】やるべきことはこれだ

経営戦略の観点から守るべき情報を特定し把握

組織における情報のうち、経営戦略の観点から、それらがどこに保存されているか等

守るべき情報に対して、発生しうるサイバーセキュリティリスクを把握

（例えば、経営戦略上重要な営業秘密の流出による損害）

把握したリスクに対して、実施するサイバーセキュリティ対策を検討

（リスクの低減策、回避策、移転策）

リスクの低減策:リスクの発生確率を下げる対策

リスクの回避策:リスクが発生する可能性を除去する対策

リスクの移転:リスクを他社等に移す対策

実施的できない場合は、残留リスクとしての識別も

サイバーセキュリティ対策の実施が不要と判断したリスクについては、発生確率や、発生したときの損害等を考慮して

法令上の取り扱いも考慮したリスクの特定と緊急時の情報の保護が行えるような対策も検討

法令上、安全管理措置が義務づけられている情報については、法令上の取り扱いも考慮したリスクの特定と緊急時に速やかに情報の保護が行えるような対策となっているかも検討する。

製品・サービス等において、企画・設計段階からサイバーセキュリティ対策を考慮

セキュリティバイデザインの観点を踏まえて

「サイバーセキュリティ体制構築・人材確保の手引き」を参考に

「サイバーセキュリティ体制構築・人材確保の手引き」

【3-4例】やるべきことはこれだ

経営戦略の観点から守るべき情報を特定し把握

組織における情報のうち、経営戦略の観点から、それらがどこに保存されているか等

守るべき情報に対して、発生しうるサイバーセキュリティリスクを把握

（例えば、経営戦略上重要な営業秘密の流出による損害）

把握したリスクに対して、実施するサイバーセキュリティ対策を検討

（リスクの低減策、回避策、移転策）

リスクの発生確率を下げる対策

リスクが発生する可能性を除去する対策

リスクを他社等に移す対策

サイバーセキュリティ対策の実施が不要と判断したリスクについては残留リスクとして識別

リスクの発生確率や、発生したときの損害等を考慮して

法令上の取り扱いも考慮したリスクの特定と緊急時の情報の保護が行えるような対策も検討

法令上、安全管理措置が義務づけられている情報については、法令上の取り扱いも考慮したリスクの特定と緊急時に速やかに情報の保護が行えるような対策となっているかも検討する。

製品・サービス等において、企画・設計段階からサイバーセキュリティ対策を考慮

セキュリティバイデザインの観点を踏まえて

「サイバーセキュリティ体制構築・人材確保の手引き」を参考に

「サイバーセキュリティ体制構築・人材確保の手引き」

* + - * 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
        + 指示すべきことはこれだ

・サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる

* + - * + やるべきことはこれだ

・重要業務を行う端末、ネットワーク、システム又はサービス（クラウドサービスを含む）には、多層防御を実施

・アクセスログや通信ログ等からサイバー攻撃を監視・検知する仕組みを構築

・従業員に対する教育を行い、適切な対応が行えるよう日頃から備える

・製品・サービス等においても、セキュリティバイデザインの観点を踏まえて、企画・設計段階からサイバーセキュリティ対策を考慮

* + - * + **【補足説明材料】**

サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる。

対策を怠った場合のシナリオ

・サイバーセキュリティリスクに応じた適切な対策が行われていない場合、 サイバー攻撃が発生した場合の被害が拡大する可能性がある。

・技術的な取組を行っていたとしても、攻撃の検知・分析とそれに基づく対応ができるよう、 適切な運用が行われていなければ、サイバー攻撃の状況を正確に把握することができず、 攻撃者に組織内の重要情報を窃取されるなどの、 致命的な被害に発展する恐れがある。

* + - * 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
        + 指示すべきことはこれだ

・計画を確実に実施し、改善していくため、サイバーセキュリティ対策をPDCAサイクルとして実施させる

・その中で、定期的に経営者に対策状況を報告させた上で、問題が生じている場合は改善させる

* + - * + やるべきことはこれだ

・サイバーセキュリティリスクに継続して対応可能な体制（プロセス）を整備する（PDCAの実施体制の整備）

・サイバーセキュリティリスク管理に関するKPIを定め、組織内の経営リスクに関する委員会においてその状況を経営者に報告する

・新たなサイバーセキュリティリスクの発見等により、追加的に対応が必要な場合には、速やかに対処方針を修正する

・サイバーセキュリティ対策の状況について、情報セキュリティ報告書、CSR報告書等への記載を通じて開示を検討する

* + - * + **【補足説明材料】**

計画を確実に実施し、改善していくため、サイバーセキュリティ対策をPDCAサイクルとして実施させる。

その中で、定期的に経営者に対策状況を報告させた上で、 問題が生じている場合は改善させる。

また、ステークホルダーからの信頼性を高めるため、対策状況を開示させる。

対策を怠った場合のシナリオ

・PDCA（Plan[計画]、Do[実行]、Check[実施状況の確認・評価]、Act[改善]）を実施する体制が出来ていないと、 立てた計画が確実に実行されない恐れがある。

・最新の脅威への対応ができているかといった視点も踏まえて組織のサイバーセキュリティ対策を定期的に見直さないと、 サイバーセキュリティを巡る環境変化に対応できず、 新たに発生した脅威に対応できない恐れがある。

・適切な開示を行わなかった場合、社会的責任の観点から、 事業のサイバーセキュリティリスク対応についてステークホルダーの信頼を失うとともに、 インシデント発生時に企業価値が大きく低下する恐れがある。

* + - ３．３．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
        + 指示すべきことはこれだ

・影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT等）を整備させる

・被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明できる体制を整備させる

* + - * + やるべきことはこれだ

・緊急時において、以下を実施できるような対応体制を構築する

・サイバー攻撃による被害を受けた場合、速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築する

・インシデント収束後の再発防止策の策定、所管省庁等への報告手順も含めて演習を行う

・緊急連絡網として社外を含む情報開示の通知先一覧を整備し、対応に従事するメンバーに共有しておく

・緊急時に組織内各部署が速やかに協力できるよう予め取り決めをしておく

・関係法令を確認し、法的義務が履行されるよう手続きを確認しておく

・インシデントに関する被害状況、他社への影響等について経営者に報告する

* + - * + **【補足説明材料】**

影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を 速やかに実施するための組織内の対応体制（CSIRT等）を整備させる。

被害発覚後の通知先や開示が必要な情報を把握させるとともに、 情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。

また、インシデント発生時の対応について、 適宜実践的な演習を実施させる。

対策を怠った場合のシナリオ

・緊急時の対応体制を整備していないと、 原因特定のための調査作業において、 組織の内外の関係者間のコミュニケーションが取れず、 速やかな対処ができない。

・速やかな情報開示が行われない場合、 顧客や取引先等にも被害が及ぶ恐れがあり、 損害賠償請求など責任を問われる場合がある。

・法的な取り決めがあり、 所管官庁等への報告が義務づけられている場合、 速やかな通知がないことにより、 罰則等を受ける場合がある。

・演習を実施していないと、不測の事態が起こった際に、 担当者が緊急時に適切に行動することが出来ない。

* + - * 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
        + 指示すべきことはこれだ

・サイバーセキュリティ対策のPDCAについて、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる

・システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる

* + - * + やるべきことはこれだ

・系列企業やサプライチェーンのビジネスパートナーやシステム管理の委託先等のサイバーセキュリティ対策の内容を明確にした上で契約を交わす

・個人情報や技術情報等の重要な情報を委託先に預ける場合は、情報の安全性の確保が可能であるかどうかを定期的に確認する

・系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先等がSECURITY\_ACTIONを実施していることを確認する

・緊急時に備え、委託先がサイバー保険に加入していることが望ましい

* + - * + **【補足説明材料】**

インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、 復旧に向けた手順書策定や、復旧対応体制の整備をさせる。

BCPとの連携等、組織全体として整合のとれた復旧目標計画を定めさせる。

また、業務停止等からの復旧対応について、適宜実践的な演習を実施させる。

対策を怠った場合のシナリオ

・重要な業務が適切な時間内に復旧できず、 企業経営に致命的な影響を与える恐れがある。

・演習を実施していないと、不測の事態が起こった際に、 担当者が緊急時に適切に行動することが出来ない。

* + - ３．４．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
        + 指示すべきことはこれだ

・サイバーセキュリティ対策のPDCAについて、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる

・システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる

* + - * + やるべきことはこれだ

・系列企業やサプライチェーンのビジネスパートナーやシステム管理の委託先等のサイバーセキュリティ対策の内容を明確にした上で契約を交わす

・個人情報や技術情報等の重要な情報を委託先に預ける場合は、情報の安全性の確保が可能であるかどうかを定期的に確認する

・系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先等がSECURITY\_ACTIONを実施していることを確認する

・緊急時に備え、委託先がサイバー保険に加入していることが望ましい

* + - * + **【補足説明材料】**

監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCAについて、 系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる。

* + - * + システム管理等の委託について、 自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。
        + 中小企業自らがセキュリティ対策に取り組むことを宣言する制度
        + 対策を怠った場合のシナリオ

・系列企業やサプライチェーンのビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないと、 これらの企業を踏み台にして自社が攻撃されることもある。 その結果、他社の２次被害を誘発し、 加害者となる恐れもある。 また、緊急時の原因特定などの際に、 これらの企業からの協力を得られないことにより事業継続に支障が生ずる。

・システム管理などの委託業務において、自組織で対応する部分と委託する部分の境界が不明確となり、 対策漏れが生じる恐れがある。

* + - ３．５．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
      * 指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び 提供
        + 指示すべきことはこれだ

・社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、情報共有活動へ参加し、積極的な情報提供及び情報入手を行わせる

・入手した情報を有効活用するための環境整備をさせる

* + - * + やるべきことはこれだ

・情報共有を通じたサイバー攻撃の防御につなげていくため、情報を入手するのみならず、積極的に情報を提供する

・IPAやJPCERT/CC等による脆弱性情報などの注意喚起情報を、自社のサイバーセキュリティ対策に活かす

・CSIRT間における情報共有や、日本シーサート協議会等のコミュニティ活動への参加による情報収集

・IPAに対し、告示（コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準）に基づいてウイルス情報や不正アクセス情報の届出をする

・JPCERT/CCにインシデントに関する情報提供を行い、必要に応じて調整を依頼する

* + - * + **【補足説明材料】**

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、 サイバー攻撃に関する情報共有活動へ参加し、 積極的な情報提供及び情報入手を行わせる。

また、入手した情報を有効活用するための環境整備をさせる。

対策を怠った場合のシナリオ

・情報共有活動への参加により、 解析した攻撃手法などの情報を用いて、 他社における同様の被害を未然に防止することができるが、 情報共有ができていないと、社会全体において常に新たな攻撃として対応することとなり、 企業における対応コストが低減しない。

* + **【補足説明材料】**
    - **【Web版コラム】サイバーセキュリティ経営ガイドライン実践状況の可視化ツールβ版**
      * 可視化ツールβ版について
        + 2020年3月25日公開
        + サイバーセキュリティの実践状況を企業自身がセルフチェックで可視化するための サイバーセキュリティ経営ガイドラインベースの可視化ツールです。
      * ツールのダウンロード
    - **【Web版コラム】サイバーセキュリティ経営ガイドライン 実践のためのプラクティス**
      * サイバーセキュリティ経営ガイドライン 実践のためのプラクティス集第2版
* **【Mission03-B】経営者は事前に何を備えればよいのか【攻め】**
  + 概要
    - **3-B-1: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)**
      * 【持続的発展のため】組織の発展を目指した戦略的なIT活用とサイバーセキュリティ対策
  + **Mission3-11 次世代技術を活用したビジネス展開**
    - 要旨
      * 【要旨】DX時代→中小も対応しないと→対応するには新たなセキュリティ対策も
    - 攻めのIT投資とは？
      * ITを活用して製品・サービス開発に取り組み、ビジネスモデルを変革することや新たな価値を創出することが「攻めのIT経営」です。 柔軟かつ大企業に先駆けてIT関連の次世代技術やデジタル情報を活用していくことが中小企業の発展につながります。 デジタル情報やIT技術の進展を受け入れ、それを活用して顧客サービスの強化を図る企業に今大きなビジネスチャンスが訪れています。
    - 各種の支援策も充実
      * 感染症対策や働き方改革の必要性が高まる中、テレワーク等の実現のためにデジタルツールに関心があっても、導入・定着に至らない中小企業に向けた支援も充実しています。その1つが「中小企業デジタル化応援隊事業」（2020年9月開始）。全国の中小企業とIT専門家をマッチングし、そのデジタル化・IT化を促進しています。
    - **【コラム】DX推進はビジネス飛躍のチャンス**
      * これから目指す社会は、「超スマート社会」いわゆる「Society5.0」
        + 政府は、サイバー空間（仮想空間）とフィジカル空間（現実空間）を連携し、すべての物、情報、人を1つにつなぐ「サイバー・フィジカル・システム」（CPS）によって量と質の全体最適を図る社会像として「Society5.0）を提唱し、その考えが「デジタル社会の実現に向けた改革の基本方針」（2020年12月閣議決定）の背景となっています。IoTやビッグデータ、ロボット、AI、5Gなどの技術革新（いわゆる第4次産業革命）により、Society5.0は現実になりつつあります。
      * DXは、新たな技術を活用したビジネスの変革
        + 新しいITおよびデジタル情報を活用して、ビジネスを変革させるのが「デジタルトランスフォーメーション（DX）」です。DXにより新時代に対応した新たなサービスを創造し、ビジネスを飛躍させることができます。
      * DX推進のためには、セキュリティも強化
        + 一方、どんなに良いサービスを展開しても、セキュリティ侵害があっては事業が継続できません。ITシステム運用継続計画（IT-BCP）を明確にして、サービス設計の段階から十分なセキュリティ対策を考慮することが重要です。
      * 中小企業のビジネスの拡大・発展に向けて
        + そのためには、ビジネス、デジタルのスキルとともに、セキュリティ対策のスキルを併せ持った人材が必要です。DXに対応した新たなビジネスの拡大・発展のためには、経営者は、業務や組織、企業風土の変革を含めて、明確なビジョンを持ち、「攻めのIT投資」を牽引する強いリーダーシップが求められます。
    - **【補足説明材料】**
      * Society 5.0【内閣府】
      * 産業界におけるデジタルトランスフォーメーションの推進【METI】
      * デジタルトランスフォーメーションの加速に向けた研究会の中間報告書『DXレポート2（中間取りまとめ）』【METI】
      * 【要約前校正案】【3-11コラム】攻めのIT投資により、DXの推進
        + Society5.0イメージ
        + •これから目指す社会は、「超スマート社会」いわゆる「Society5.0」

今までは、インターネットの登場により、容易に情報の共有が可能な情報社会が形成されて、情報化社会（Society4.0）と言われてきました

近年、サイバー空間（仮想空間）とフィジカル空間（現実空間）を連携し、すべての物や情報、人を一つにつなぐ「サイバー・フィジカル・システム」（CPS）により、量と質の全体最適を図る社会として、政府により「超スマート社会」として新たに「Society5.0」というコンセプトが提唱されました。

※Society5.0 (https://www8.cao.go.jp/cstp/society5\_0/)

* + - * + •いわゆる第４次産業革命での新たな技術の進展が実用レベルに

IoTやビッグデータ、ロボット、AIや５Gなどの一連の技術革新（いわゆる第4次産業革命）により、Society5.0の社会の実現が現実のものとなりつつあります。

* + - * + •「第４次産業革命」の技術を活用して、ビジネスを変えていくことがDX

こうした技術革新のIT技術、デジタル情報をビジネスに応用し、競争力を維持・強化を図るのが「デジタルトランスフォーメーション（DX）」です。

DXは、単なる老朽化したシステムの改修による業務の効率化に留まらず、新しいビジネスモデルへの変革はもちろん、業務や組織、企業風土の変革も含みます。

* + - * + •DXは中小企業にとっても、新たなビジネスチャンス

顧客との関係性を持ったビジネスでの競争力を強化には、「サプライチェーン」を構成する組織体全体での対応が必要です。

各組織の経営戦略と密接に関わり、経営者の積極的な関与がなければ、組織の存続も危ぶまれます。

中小企業にとっても、大企業に先立って対応することにより、新たな時代に対応したサービスを創造し、ビジネスを飛躍させるチャンスが生まれます。

* + - * + •DX推進のためにもセキュリティを強化

どんなに良いサービスを展開しても、セキュリティ侵害があってはビジネスの発展は望めません。サービスを継続的に展開するためは、十分なセキュリティ対策が必要です。

「事業継続計画」（BCP)の中で、DXへの対応とともに、セキュリティ侵害による被害を最小限にする対応も明確にすることが重要です

* + - * + • ビジネスの拡大・発展に向けて

こうした未来に向けた追い風が吹いている今、DXに対応した新たなビジネスの拡大・発展のためには、ビジネスとデジタルのスキルを併せ持った人材育成と獲得が必須です。

経営層にはまさに、これらの実現のために、人材確保、セキュリティ対策を含めた「攻めのIT投資」への判断が求められているのです。

* + - * 【削除】【検討過程メモ】*【3-11コラム】攻めのIT投資により、DXの推進*
        + 概念図

※Society5.0とは、狩猟社会（Society1.0）、農耕社会（Society2.0）、工業社会Society3.0）、情報社会（Society4.0）に続く新たな社会

* + - * + 「Society5.0」とはサイバー空間（仮想空間）と現実世界を融合させた社会

サイバー空間（仮想空間）と現実世界を融合させて経済発展と社会的課題を解決する「Society5.0」。

この新たな社会の実現に向けた取り組みが、さまざまなレベルで加速しています。

Society5.0においては、あらゆるものがインターネットに接続し、様々な情報がビッグデータとして収集され、活用されます。

* + - * + Society5.0の実現手段としての「デジタルトランスフォーメーション（DX）」

Society5.0を支える技術として注目されるのがIoTやビッグデータ、ロボット、AIなどです。

AI技術を用いてこれらを高度にデータ分析し、例えばロボットを通じたサービス提供をすることで人手不足の解消を実現していきます（一連の技術革新を「第4次産業革命」とも呼びます）。

技術革新をビジネスに応用し、競争力の強化を図るのが「デジタルトランスフォーメーション（DX）」

* + - * + 「攻めのIT投資」は、DXのための投資

DXは、単なるデジタル化とは違います。ビジネスモデルの変革はもちろん、業務や組織、企業風土の変革も含みます。

* + - * + ビジネスの拡大・発展を図るために、「攻めのIT投資」が必要

そのためDXは経営戦略と密接に関わり、経営者が積極的に関与する必要があります。

さらにDX推進には、十分なセキュリティ対策への配慮はもちろん、ビジネスとデジタルのスキルを併せ持った人材育成と獲得が必須です。

こうした未来に向けた追い風が吹いている今、経営層にはまさにビジネスの拡大・発展に向けた「攻めのIT投資」への判断が求められているのです。

* + - * + 中小企業のビジネス発展のチャンス

IoT、 ビッグデータ、 ロボット、 AI等の技術、 クラウドコンピューティングやモバイル環境で活用できるようになったことは、 少ない投資で事業を立ち上げることが可能であり、 中小企業、ベンチャー企業や個人の活躍のまたとないチャンスである

IT化、 デジタル化の進展を受入れ、 それを活用して顧客との関係性強化を図る企業は、 大きなビジネスチャンスを得ることが期待できる。

* + - * + サイバーセキュリティ対策が重要

ビジネスの拡大・発展のための「攻めのIT投資」は、 確立していない世界であり、 セキュリティリスクも高くなる。

ビジネスの企画、構築段階からセキュリティバイデザインでの設計が必要

* + - * **【ポイント】現状認識**
        + Society5.0とは、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会課題の解決を両立する、人間中心の社会
        + 今は、その実現を可能にする、 IoT、 ビッグデータ、 ロボット、 AI等の技術革新による、 第4次産業革命の入口にいる

【参照】IT人材白書【IPA】

* + - * + あらゆるものがインターネットに接続するIoTの広がり、 あらゆる情報がビッグデータとして活用され、 AI技術により、 様々な分野で定型的な業務はもとより、 人海戦術では不可能だった業務まで、 AI技術を適用したサービス、 ロボットの適用が始まっている
        + 既存のビジネスや業務に新技術を取り入れるだけでなく、 ビジネスモデルを変え、 経済活用のみならず、 個人の生活や社会構造まで影響が及ぶ
        + DXとは、 あらゆる情報がデジタル化され、 IT技術によって、 社会や産業、 企業、 人のあり方や働き方が変わっていくこと
        + DXが進むにつれて、 発展するビジネスと縮小するビジネスが明確になっていく
        + 時代環境が大きく変わる時、 それにそぐわないビジネスは淘汰されていく
        + 匠の技的な高度な伝統的技能を要する作業や、 旧来の延長線で仕組みの高度化、 洗練により、 生き残れるビジネスもあるが、 現状維持のビジネスの多くは、 相対的に意義を失う可能性が高い
        + IoT、 ビッグデータ、 ロボット、 AI等の技術、 クラウドコンピューティングやモバイル環境で活用できるようになったことは、 少ない投資で事業を立ち上げることが可能であり、 中小企業、ベンチャー企業や個人の活躍のまたとないチャンスである
      * 組織の責任者として
        + 時代の潮流を捉えて、 組織が社会の変化の中で、 時代に適合して発展できる道を探り、 ビジョンをはっきり示すことが重要であり、 それは責任者の責務
        + DXを実現するには、 ビジネスとデジタルのスキルを併せ持った人材の育成と獲得をしていく必要がある
      * 実務者として
        + 自らもDXの流れの中にあることの意識
        + 求められるのは、 周囲を巻き込みながら改革を進める能力やビジネスとデジタルを結び付けて 全体をデザインする能力を持った人材になること
        + 目の前の業務だけにとらわれることなく、 広く視野を持って進むべき道を探り、 学ぶ。 勉強会やコミュニティなど、 学びの場は周囲にある。 自己研さんによって能力を高めれば高めただけ、 社会をリードしていく人材になっていく
      * 組織を発展させるために経営者、 管理者が認識し、 実践すべきことは？
        + 柔軟にかつ大企業に先駆けて、 IT関連の次世代技術、 デジタル情報を活用していくことが、 中小企業の発展につながる。 デジタル情報、 IT技術の進展を受入れ、 それを活用して顧客サービスの強化を図る企業に、 大きなビジネスチャンスがある。
        + ビジネスの拡大・発展のための「攻めのIT投資」は、 確立していない世界であり、 セキュリティリスクも高くなる。
        + 次世代技術を活用したビジネス展開
      * **「攻めのIT経営中小企業百選」事例⇒ IPAのDXへの取組を取り込む （６月１０日付　「DX推進に向けた文書を公開」参照）**
      * **【コラム】Society5.0からDXへの対応の必要性【攻めの姿勢の企業に向けて】**
        + **【参考】デジタルアーキテクチャ・デザインセンター憲章**

https://www.ipa.go.jp/dadc/about/dadc-charter.html

伝えるポイント

DADCの使命と目的で目指すところが、Society5.0の実現手段としてのDXの推進の方向性。これが企業の攻めの姿勢で実施すべき事項を示している。

DXを推進することの必然性と、その実現のためにサイバーセキュリティ対策もしっかりやらなければならないことを伝える

1.実現すべき世界（Society5.0）のビジョンと課題

Society5.0の進展に伴い、多様なステークホルダーがリアルタイムかつ複合的に連携し複雑化したシステムが、生活や産業の基盤を形成しつつある。

こうした中で、Society5.0、つまり、サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済発展と社会的課題の両方を解決する、人間を中心とした社会を実現するにあたり、特にサイバー・フィジカルの融合領域を中心に、大きく二つの課題が顕在化しつつある。

ソフトウェアだけでなく、ハードウェアや制度も含む社会システムや産業構造の全体について、それが果たす役割を機能の観点から見直す中で、その要素の位置づけや要素間の役割分担や関係性を適切に明確化すること等を通じ、全体としての総合的な信頼性を安定的に確保すべきこと

海外の巨大IT企業等による独占・寡占が繰り返し進むなど、変化が激しく将来の不透明性が高まる中で、日本が自律的にイノベーションを起こす基盤を形成すべきこと

2.ビジョン実現のために求められること

3. センターの使命・目的

4. 5つの役割・実施内容

5. 7つの運営方針

* + - * + **デジタルトランスフォーメーションの加速に向けた研究会の中間報告書『DXレポート2（中間取りまとめ）』**

https://www.meti.go.jp/press/2020/12/20201228004/20201228004.html

伝えるポイント

DADCの使命と目的で目指すところが、Society5.0の実現手段としてのDXの推進の方向性。これが企業の攻めの姿勢で実施すべき事項を示している。

DXを推進することの必然性と、その実現のためにサイバーセキュリティ対策もしっかりやらなければならないことを伝える

* + - * **【Web版コラム】攻めの姿勢の企業向け**
        + 【Web版コラム】ITの利活用を事業戦略上に位置づけ、 サイバーセキュリティを強く意識し、 積極的に競争力強化に活用しようとしている企業

デジタルトランスフォーメーション

最先端の技術を生かし、 コスト削減だけでなく、 ビジネスの推進にどう貢献するか

DXの目指すところ

「ITの浸透が、 人々の生活をあらゆる面でより良い方向に変化させること」

DX時代には

企業がこれからのビジネスで勝ち残っていくためには、 新しい製品、 サービス、 パートナーシップ、 ビジネスモデルなどを創造し、 新たな価値を創出していく必要があるという

プラットフォームの構成

「クラウド」「ビッグデータ／アナリティクス」「ソーシャル技術」「モビリティ」

プラットフォームの上にイノベーションアクセラレーター」の技術

イノベーションを後押しするIoT、 AIや機械学習などの認知システム、 ロボティクス、 AR（Augmented Reality、 拡張現実）／VR（Virtual Reality、 仮想現実）、 3Dプリンティングなど

デジタルトランスフォーメーション、 インダストリー4.0、 Society5.0、 、 、

データを効率的に集積し、 それをAIのディープラーニング機能などを活用して認識・加工し、 自らの企業活動に生かしていけるかが、 企業の成長の可否を決める時代がすぐそこまで来ている【日経1月4日13面　佐藤康博】

IT化、 デジタル化の進展を受入れ、 それを活用して顧客との関係性強化を図る企業は、 大きなビジネスチャンスを得ることが期待できる。

人工知能（AI）, ディープラーニング, ビッグデータ, IoT, M2M. 仮想現実（AR）, ３Dプリンタ等を活用した新サービスが、 一般化する前に先駆的に取り入れるベンチャー的企業（イノベーター、 アーリーアダプター）

CtoB

多様な消費者ニーズに対応して、 きめ細やかで丁寧なモノづくりが企業の持続的発展に不可欠な要素となる【日経1月4日13面　佐藤康博】

競争力強化

新サービス、 新技術を活用した生産性の向上

新サービス、 新技術を活用した新ビジネス展開

大手企業と中小企業、 ベンチャー企業との協業

新サービス、 新技術は新ビジネスのチャンスだが、 セキュリティ上のリスクも大きい

* + - * + 【Web版コラム】企業経営のためのサイバーセキュリティの考え方の策定について【NISC】

基本方針－サイバーセキュリティは、 より積極的な経営への「投資」へ－

グローバルな競争環境の変化

ITの発展によるビジネスの変革が、 消費者向けのビジネスから企業間取引へと拡大

サイバー空間と実空間の融合がさらに進み、 チャンスもリスクも一層増大

サイバーセキュリティをやむを得ない「費用」でなく、 積極的な経営への「投資」と位置づけ、 企業としての「挑戦」と、 それに付随する「責任」として取り組むことが期待される

基本的な考え方

二つの基本的認識

＜①挑戦＞サイバーセキュリティは、 利益を生み出し、 ビジネスモデルを革新するものであり、 新しい製品やサービスを創造するための戦略の一環として考えていく

＜②責任＞全てがつながる社会において、 サイバーセキュリティに取り組むことは社会的な要求・要請であり、 自社のみならず社会全体の発展にも寄与する

三つの留意事項

＜①情報発信による社会的評価の向上＞

「セキュリティ品質」を高め、 品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。

そのような取組に係る姿勢や方針を情報発信することが重要。

＜②リスクの一項目としてのサイバーセキュリティ＞

提供する機能やサービスを全うする（機能保証）という観点から、 リスクの一項目としてのサイバーセキュリティの視点も踏まえ、 リスクを分析し、 総合的に判断。

経営層のリーダーシップが必要。

＜③サプライチェーン全体でのサイバーセキュリティの確保＞

サプライチェーンの一部の対策が不十分な場合でも、 自社の重要情報が流出するおそれあり。

一企業のみでの対策には限界があるため、 関係者間での情報共有活動への参加等が必要。

* + - * + 【Web版コラム】IT活用の必然性

IT活用するためにセキュリティ対策を実施する

セキュリティ対策は目的ではない。

業務の効率化のためにITを活用する。

必要以上のサイバーセキュリティ対策は、 業務の効率化を阻害する

単なる効率化だけではビジネスの競争に勝ち残れない

これまで企業のITシステムは、 業務、 生産工程等を効率化して、 経営を安定化させることに重きが置かれてきた。

組織の発展のためにはITの活用が重要

これからはデジタルトランスフォーメーションの時代の時代と言われている。 社会の進展に対応したサービスを展開するためにITを活用する

IT化、 デジタル化の進展を受入れ、 それを活用して顧客との関係性強化を図る企業は、 大きなビジネスチャンスを得ることが期待できる。

デジタルトランスフォーメーションに対応することが重要

10分で分かる！ 近未来予想図202X | nikkei BPnet 〈日経BPネット〉：日経BPオールジャンルまとめ読みサイト

デジタルトランスフォーメーション時代には、 創造力、 技術力を持ったベンチャー企業など、 ビジネスチャンスあり

柔軟にかつ大企業に先駆けて、 デジタルトランスフォーメーションに対応していくことが、 組織の発展につながる。

人海戦術、 定型化した作業、 精密作業は、 匠の技レベルでなければはシステム、 機械に置き換わっていく。

「つながる工場」「インダストリー4.0」「自動運転」「スマートアグリ」

人工知能（AI）, ディープラーニング, ビッグデータ, IoT, M2M. 仮想現実（AR）, ３Dプリンタ等のデジタルを、 ITを駆使した新サービスを、 一般化する前に先駆的に取り入れることが重要

* + - * + 【Web版コラム】ITを活用したサービスを継続するためには、情報セキュリティ対策は必須

セキュリティ侵害は組織の存続が脅かす

ITを活用してどんなに利便性の高いサービスを提供しても、 どんなに業務を効率化しても、 緊急事態（自然災害、 大火災、 感染症、 テロ、 セキュリティ侵害、 、 ）が発生して、 事業資産（人・もの（情報及び設備）・金）、 社会的信用が失われ、 早期復旧ができない場合は、 事業の継続が困難になり、 組織の存立さえも脅かされる可能性がある。

事業を継続できるように

どんな緊急事態が発生しても、 事業を継続できるようにする対策を明示しておくことが必要

サービスの向上を図るために

情報資産（保有情報（媒体に依らず）、 情報機器、 情報システム）に対する情報セキュリティ上のリスクを低減させる

セキュリティ対策は先行投資

ITを活用したサービスの構築・運用に掛かる費用は、 経費ではなく先行投資。 リスクに見合った情報セキュリティ対策は、 サービスの構築・運用の中で実施すべき先行投資であり、 緊急事態が発生した後に対処する経費として想定してはいけない

* + - * + 【Web版コラム】次世代サービス、 技術の利用に当たってのサイバーセキュリティ対策

人工知能（AI）, ディープラーニング, ビッグデータ

M2M, 制御システム【情報セキュリティ白書2016】

IoT【情報セキュリティ白書2016】

IoT早期導入者のためのセキュリティガイダンス【CSA】

■IoTセキュリティガイドラインver1.0【2016年7月5日総務省・経済産業省】

■安全なIoTシステムの創出【2016年3月1日NISC】

■コンシューマ向けIoTセキュリティガイド【2016年6月24日JNSA】

■IoT早期導入者のためのセキュリティガイダンス【2016年2月24日CSA】

クラウドサービス

■クラウドセキュリティガイドライン活用ガイドブック2013年版【METI】

■クラウドサービス提供における情報セキュリティ対策ガイドライン【2014年4月総務省】

■クラウドセキュリティ関連ISO規格

ISO/IEC27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項（スライド）【JIPDEC】

ISMSクラウドセキュリティ認証の概要（スライド）【JIPDEC】

ISO/IEC27017:2015に基づくクラウドセキュリティの構築のポイント（スライド）【JIPDEC】

スマートデバイス

スマートフォン、 タブレット等

■スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書【2015年 5月21日NISC】

VR, MR, AR

エンターテインメント、 自動車業界、 広告業界、 教育、 宇宙産業 、 、

VR/AR技術の将来展望【2016年6月MRI】

VR（Virtual reality:仮想現実）

AR（Augmented reality：拡張現実）

MR（Mixed Reality：混合現実）

SR（Substitutional Reality：代替現実）

ブロックチェーン

仮想通貨

ブロックチェーンの安全性とセキュリティコンセンサス・ベイス（株）

3Dプリンタ

危険物製造、 著作権侵害

・・・

* + - * + 【Web版コラム】サイバーセキュリティ分野で機械学習が活用される背景と期待

サイバーセキュリティ分野で機械学習が活用される背景

従来型サイバーセキュリティ対策の限界

機械学習への期待

マルウェア検知への応用

ネットワーク異常検知への応用

ソースコードレビューへの応用

セキュリティ監視の運用支援への応用

機械学習を活用する上で押さえるべきポイント

誤検知の可能性が避けられない

判定結果の分析が困難である

全てに万能な機械学習アルゴリズムは存在しない

* + - * + **【コラム】DXレポート（ITシステム2025年の崖の克服**

【参考】DAX21\_デジタルトランスフォーメーション（DX）

* + - * + 【Web版コラム】攻めのIT投資対応、Society5.0時代に必要なセキュリティ対策

ディープラーニング、ロボット、ビッグデータ、IoT、クラウドサービス等 の技術の活用の必要性と、活用におけるセキュリティ対策の記述の充実

【Web版コラム】IoT関連セキュリティ対応

【担当：早出】

【参考】

NIST SP.800-82R2　Guide to Industrial Control Systems (ICS) Security　【再掲】

IoTセキュリティ　標準／ガイドライン　ハンドブック　2017年度版【2018年5月8日JNSA】

コンシューマ向けIoTセキュリティガイド【2016年8月1日JNSA】

IoT・5Gセキュリティ総合対策【2019年サイバーセキュリティタスクフォース】

IoT（ICS）サイバーセキュリティ対策ガイド編

1.フィジカルセキュリティスコープ

2.IoTリスクアセスメント

3.IoTサイバーセキュリティ攻撃のシナリオ

4.セキュリティ対策/ベストプラクティス

5.セキュリティギャツプ分析

6.IoTセキュリティインシデント事例

7.IoTセキュリティ基準と参考資料

8.IoTセキュリティのプレイヤー

9.（参考情報）

BCPとサイバーセキュリティ

【Web版コラム】クラウドサービスとセキュリティ

各種クラウドサービス

**クラウドセキュリティ**

クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年度版【METI】

クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版）2018年7月【総務省】

【Web版コラム】５Gセキュリティ対応

【担当：早出】

【Web版コラム】BYODセキュリティ対応

Mobile Device Security Corporate-Owned Personally-Enabled (COPE)【NIST SPECIAL PUBLICATION 1800-21】対応

【担当：早出】

【Web版コラム】APIセキュリティ

【Web版コラム】ブロックチェーンにおけるセキュリティ

【Web版コラム】インターネットアクセスにおけるセキュリティの新技術

【コラム】IDと認証セキュリティ

【担当：中山】

利便性とセキュリティの両立へ向けた新たな動向

NIST 800-63-3 電子的認証に関するガイドライン 対応

2要素認証

パスワード設定に関する要件の変更、パスフレーズの利用

【参照】世界の電子認証基準が変わる-NIST-SP800-63-3を読み解く

FIDO(Fast Identity Onlinbe)

パスワードに代わる認証手段として、 指紋や顔画面などを活用した生体認証や、 認証結果を完全にやりとりできる「FIDO」の普及が期待されている

モバイル認証（GSMA Mobile Connect）

携帯電話をWebサービス全般の汎用的な認証手段として利用するための「Mobile Connect」が注目されている

認証セキュリティとNIST SP 800-63の改定

「パスワードは定期変更すべき」「パスワードは複数の」文字種で混成すべき」などの、 従来は常識とされてきた対策についても、実効性や技術の進展に合わせた見直しが図られてる

【Web版コラム】AIが人間をアシストする「インテリジェント・ワークプレイス」の活用におけるサイバーセキュリティ対策

【担当：中山】

AIが従業員の能力を補い、人間が気づかない部分をコンピュータがアシストすることが可能になりつつある

Society5.0, Connected Industry, DX, CPS対応

〇第4次産業革命

※科学技術イノベーション統合戦略（内閣府）

※Society5.0

※Connected Industry

※AI白書2019

「【図解】コレ1枚でわかる最新ITトレンド」内のIoTの章

CPSとは

フィサイバージカルシステム(CPS)とは【ANTALYICS-NEWS.JP】

IoT、ビッグデータ、機械学習、クラウドサービス等の活用におけるサイバーセキュリティ対策

* + - * + 【参考】ITの最新トレンド

【参考】DAX20-0402-3-1\_Society 5.0

【参考】DAX10-20 Society5.0に向けた人材育成

DAX20-04人工知能に関する基礎知識（まとめ）

DAX20-0401-1人工知能に関する文献のポイント（引用1）

DAX20-0402-1 ITロードマップ2018年版【2018年3月NRI】

DAX20-0402-2 【図解】コレ１枚でわかる最新ITトレンド

DAX20-0402-2-0 ITの最新トレンド

DAX20-0402-2-1 IoT

DAX20-0402-2-2 人工知能とロボット

DAX20-0402-2-3 クラウドコンピューティング

DAX20-0402-2-4 モバイルとウェアラブル

DAX20-0402-2-5 ITインフラストラクチャと仮想化

DAX20-0402-2-6 開発と運用

デジタル・トランスフォーメーション(DX)時代に、「ビジネスを発展させるために」（攻めのIT投資）に活用すべきITと、 活用におけるサイバーセキュリティ対策（Society5.0時代のサイバーセキュリティ対策）

* + **3-12：IoT、 ビッグデータ, AI、 ロボットの活用**
    - 業務・サービスの効率性を追求
      * あらゆる機器がインターネットに接続することで、人が行ってきたことをセンサー化し、センサーからの膨大なデータを瞬時に分析できます。その結果を踏まえて業務やサービスを効率的、効果的に行うことが始まっています。IoT（Internet of Things／モノのインターネット）※、ビッグデータ※、AI（Artificial Intelligence／人工知能）※、ロボットの活用は、人手不足に対応した省力化や、自動化のための投資という面でも期待されています。
      * ※IoT、ビッグデータはP122を、AIはP124を参照
    - 【コラム】IoT、ビッグデータ、AI、ロボットはつながっている
      * IoT、ビッグデータ、人工知能（AI）、ロボットなどの技術革新によって社会のあらゆる活動、情報がデータ化され、ネットワークによってつながることが可能な時代になりました。これらを組み合わせた機器やサービスが普及するとともに利活用を実現する事例が増えています。リアルタイムに分析を行い、新たなサービスや製品を生み出すことが可能になると、データそのものが創造の源泉になります。
      * 商品やサービスの提供は個々のニーズに合わせてカスタマイズされ、個々のニーズとの効率的なマッチングが可能になります。AIやロボットはますます人間の役割をサポートし、部分的に代替するようになります。こうした状況にどう対応するかは、事業者にとっても重要なテーマです。商品・サービスの開発や生産、さらには流通、アフターサービスなど、事業活動に上手に取り込むことができれば、将来の成長の大きな助けになります。
      * 出典：「IoT、AI、ロボットに関する経済産業省の施策について」（経済産業省）より
    - **【補足説明材料】**
      * 深刻な人手不足に対応した、 省力化、 自動化のための投資
      * 人が行ってきたことをセンサー化し、 センサーからの膨大な情報を機械的に分析することにより、 今までできなかった高度な分析と、 その結果を踏まえて業務やサービスを効率的、 効果的に行える
  + **3-13：IoTが果たす役割と効果**
    - IoTは中小企業にとって大きなビジネスチャンス
      * 「5G」に代表される次世代通信技術などによってIoTデバイスは急速に普及し、2024年には10兆円を超える国内市場となる予測もあります。さらに政府が目指す「Society5.0」実現に向けた動きも追い風となり、ビジネスシーンにおいては、IoTがもたらすビッグデータ（蓄積された膨大なデータ）が新たな価値を見いだす資源として注目されています。中小企業にとっても、IoTは、例えば医療・介護、物流、製造業、交通、農業などさまざまな分野での活用が期待でき、大きなビジネスチャンスになるのです。
    - 【コラム】中堅・中小企業のIoT活用事例
      * 3DCADをクラウド環境で離れたところから利用可能に
      * 事例ポイント
        + 専門ソフトウェアの導入によって一般的なノートPCで、社内のハイスペックPCを高性能のままにリモート操作可能とした。客先や工場内など遠隔地のどこからでも社内の３DCADソフトをシームレスに利用して設計データの確認や修正が実現できる環境を構築した。
      * 概要
        + ・当該企業は板金加工を中心とした金属加工による部品製造や機械装置設計開発業務に従事。設計開発では3DCAD等のソフトウェアを利用。一般的なオフィスソフトを動作させるPCスペックでは足りずハイスペックな環境が必要であり、場所も設計者の机に限定されている。
        + ・設計に関して客先での打ち合わせや工場内確認を行う場合、3DCADのデータ参照が必要であり、設計者の机以外の場所で利用することができない。3DCADデータをプリントアウトした紙媒体を多く用いていた。修正や改編の度に紙とCADを行き来しなければならず膨大な手間が発生していた。修正ミスが起こる可能性も高い状況にあった。
      * 効果・メリット
        + 客先や工場内など遠隔地のどこからでも社内の3DCADソフトを利用して設計データの確認や修正を迅速に反映。情報セキュリティ面から見ても、データそのものや紙媒体を持ち運ぶ必要がなくなり、情報漏えいのリスクを最小限に抑えた形で外部での設計対応が可能に。
    - **【補足説明材料】**
      * 中小企業にとって、 経費削減と人材確保は大きな課題
      * 各種センサーによる自動測定や電子タグ等（RFID）を人やモノに貼り動きの情報を計測し収集することにより、 リアルタイムで状況が把握できる
      * その際に、 センサーが誤動作したり、 誤った情報を発信すると、 正確な状況を把握できなくなり、 業務やサービスが混乱する
      * IoT、 ビッグデータ、 AI、 ロボットは繋がっている
        + ①センサー、 機器、 ロボットによりデータが取得され、 ②データのやり取りや通信により③集約されることによりビッグデータ化し、 ④人工知能等を用いて分析され⑤ロボット等を通じて実環境でのアクションとして実行される

IoT、 AI、 ロボットに関する経済産業省の施策について【2016年2月METI】

* + - * + IoT、 ビッグデータ、 AI、 ロボットを利用することにより、 人が行ってきたことが効率化されるとともに、 これらを使いこなすことにより、 人の仕事の質を高める能力が付加価値となる
  + **3-14：人工知能（AI）が果たす役割と効果**
    - 急速に進化するAIを活用しよう
      * インターネットの検索エンジン、スマートフォンの音声検索アプリや音声入力機能、掃除ロボットなどの家電製品、さらに人型ロボットにも人工知能（AI）が搭載されています。身近となったAIを企業経営に活用することによって、経営上のさまざまな課題を解決するのみならず、新しい価値をも生み出します。例えば、大手調査機関では、日本においては2035年にAIによる労働生産性がベースラインで34%向上するという分析も行われています。
    - 【コラム】新しい価値を持った業務の創出
      * AIを含むICTの進化は雇用と働き方にも影響を及ぼします。 ・既存業務の人材不足の解消 ・不足している労働力の補完・省力 ・既存の業務効率・生産性の向上（省力化） ・新しい価値を持った業務の創出 などが期待されています。 ＜AIの進化で予想されること＞ ・労働力不足や過酷労働などの緩和 ・農業・漁業の自動化による人手不足問題の緩和 ・犯罪の発生予知、事故の未然防止 ・個々人の必要に応じたきめ細かいサービスの提供 ・医療データの活用などによる課題解決 ・職人の知識、ノウハウの体系化による維持と伝承
      * 国内のAIとIoT活用状況
        + 出典：財務省「最先端技術（IoT、AI等）の活用状況」（平成30年11月）を参考に作成
    - **【補足説明材料】**
      * 人工知能は、 中小企業の既存の業務の人材不足の解消に留まらず、 既存の人材で新たな業務を行えるようになることが期待できる。
      * 不足している労働力を補完する。 既存の労働力を省力化する。 既存の業務効率・生産性を高める。 既存の業務の提供する価値（品質や顧客満足度など）を高める。 これまでに存在しなかった新しい価値をもった業務を創出する。 既存の業務に取組む意欲や満足度を高める。 新しい業務に取組む意欲や満足度を高めること。
        + 【参照】平成28年度情報通信白書【総務省】
        + DAX25-20-03【書籍】 AI白書2019\_第3章利用動向
        + DAX25-12【文献】第四次産業革命を視野に入れた知財システムの在り方について【2017年4月19日METI】
      * 【コラム】
        + 【コラム】クラウドサービスのメリットは？
        + 【コラム】クラウドサービス導入の留意点
        + 【コラム】クラウドサービスの活用
  + 3-15：IoTを活用する際のサイバーセキュリティ上の留意点
    - IoTへの脅威
      * 次世代通信技術である5Gの進歩などを背景に、これから飛躍的に活用場面の増加が予想されるIoT機器ですが、一方でセキュリティ対策が十分とはいえないのが現状です。また、5Gが社会浸透していく中では、これまで以上にさまざまなリスクが生まれ、脅威の在り方もさらに多様化・複雑化することが予想されます。そのため、IoT機器をターゲットとしたサイバー攻撃が増大することも懸念されています。利用する際には、それを前提とした対策が欠かせません。
    - 図解
      * + インターネットから自動車の脆弱性を突かれ、ハンドルやエンジンなどが遠隔操作される
        + ホテルの部屋に設置してある通信機器・設備が不正に遠隔操作される
        + ペースメーカーや植え込み型除細動器が不正操作される
    - **【補足説明材料】**
      * IOTへの脅威　事例を最新に更新する ＊サンプル最新事例収集する
      * IoT装置は、 十分なセキュリティ対策がされていないものが多い。 特に以前のIoT製品に関しては管理者権限パスワードの変更手順や、 ファームウェアのアップデート機能はほとんど実装されていない。
      * 利用者側として、 IoT製品は十分なセキュリティ対策がされていないことを前提とした対策が必要
      * 製造者は、 IoT製品のファームウェアの自動アップデート機能を実装し、 脆弱性に対して速やかに対応する等の「IoT製品ガイドライン」に沿った対応が必要
      * 膨大な情報をビッグデータとして活用に当たっては、 「改訂個人情報保護法」の個人情報に該当する可能性の「グレーゾーン」の情報も増える。 また、 利用の仕方によっては著作権侵害になるケースもある。 さらに、 情報をビッグデータとして公開する際に、 故意・過失に関わらず、 機密性の高い情報を公開してしまう可能性もある
  + 3-16：IoTを活用する一般利用者のための基本ルール
    - IoTのセキュリティは製造サービス提供側とサービス利用者側の双方の意識が大切
      * 製造業を中心にIoTを利活用する動きが加速しています。
      * IoT機器はインターネットに接続しているネットワーク機器の一種。そのためパソコンと同様にサイバー攻撃のリスクがありますが、セキュリティ面がなおざりにされているものもあります。それらを利用するとサイバー攻撃によってシステムが使えなくなる、あるいは第三者への攻撃の踏み台となるかもしれません。
      * IoTのセキュリティは、製造サービス提供側とサービス利用者側の双方が注意を払わなくてはならないのです。
    - IoT機器やシステム、サービスの提供にあたっての指針
      * ■指針１　IoTの性質を考慮した基本方針を定める
        + IoT機器が原因で情報流出や社会インフラの停止などが起こった場合は、IoT機器やシステム、サービスの提供側の経営責任が問われることもあります。リスクを認識し、内部不正やミスに備えることが必要です。
      * ■ 指針２　IoTのリスクを認識する
        + 他の機器とつながることで、影響が広範囲になるリスクを想定することが大切です。不正操作や、廃棄機器からの情報漏えいリスクも考慮します。
      * ■指針３　守るべきものを守る設計を考える
        + つながる相手や状況に応じてつなぎ方を判断できる設計を検討しましょう。安全安心を実現するために設計が妥当かどうかの評価も必要です。
      * ■指針４　ネットワーク上での対策を考える
        + セキュアなゲートウェイを利用するなど、ネットワーク構成やセキュリティ機能の検討を行いましょう。初期設定もセキュリティに留意し、利用者にも注意喚起を行います。
      * ■指針５　安全安心な状態を維持し、情報発信・共有を行う
        + 出荷・リリース後も安全安心な状態を維持できるようソフトウェアをアップデートする手段を確保します。脆弱性について情報発信し、セキュリティに関する重要事項はユーザーへあらかじめ説明しましょう。
    - IoT機器の一般利用者のためのルール
      * ルール1:問い合わせ窓口やサポートのない機器やサービスの購入・利用を控える
        + 機器やサービスの問い合わせ窓口やサポートがない場合は、不都合が生じたとしても、適切に対処することが困難になりますので、サービスの購入・利用は控えましょう
      * ルール2:初期設定に気を付ける
        + 機器を初めて使用する際には、IDやパスワードの設定を適切に行います。パスワードの設定では、「機器購入時のパスワードを必ず変更する」「他の人とパスワードを共有しない」「他のパスワードを使い回さない」「不要なサービスや機能は有効化しない」に気を付けましょう。また、取扱説明書などの手順に従って、自分でアップデートを実施しましょう。
      * ルール3:使用しなくなった機器については電源を切る
        + 使用しなくなった機器や不具合が生じた機器をインターネットに接続したまま放置すると、不正利用されるおそれがあります。使用しなくなったWebカメラやルーターなどをそのまま放置せず、電源プラグを抜きましょう。
      * ルール4:使用しなくなった機器は必ずデータを消す
        + 情報が他の人に漏れることのないよう、機器廃棄・下取りなどのときは、事前にデータを削除しましょう。
    - Society5.0とIoT
      * Society5.0が目指す社会では、IoTによってPCやスマートフォンだけでなく家電製品や車、建物などあらゆるモノがサイバー（仮想）空間とフィジカル（現実）空間で融合されます。このため、IoT機器へのサイバー攻撃が成功すると、フィジカル空間にも影響を与える可能性が高まります。
      * 例えば、IoT製品などに感染するウイルス「Mirai」によりWebサイトが大規模なサイバー攻撃を受けました。さらに重要インフラや生産設備への攻撃による大規模な被害も発生しています。
      * IoT製品をはじめ、インターネット接続される多様な機器に適切なセキュリティ対策が行われずインターネット上に晒されアクセス可能な状態にある製品を監視し、被害を防止するために、「NOTICE（National Operation Towards IoT Clean Environment）」が行われています（P47ページ参照）。これはサイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行うもので、総務省、国立研究開発法人情報通信研究機構（NICT）及び一般社団法人ICT-ISAC が主体となって実施されています。
    - コラム　スマート東京実施戦略～東京版Society5.0の実現に向けて
      * 東京都は、「スマート東京実施戦略～東京版Society5.0の実現に向けて～」（2020年2月7日）を発表しました。デジタルの力で東京のポテンシャルを引き出し、都民が質の高い生活を送ることのできる、東京版Society5.0『スマート東京』の実現です。
      * 背景にあるのは、経済、テクノロジー、気候変動、人口構造の4場面で歴 史的な転換点に東京都が直面している危機感です。具体的には、5GやIoT技術を有効活用して公共施設や都民サービスのデジタルシフトを加速させます。さらに「デジタルツイン」と呼ばれる新技術（IoTやAI、ARなどの技術を用いて仮想空間に物理空間の環境を再現し、将来予測や適切な判断視座を得る）を活用し、都政のアップデート、 都民等のQOL（Quality of Life）向上、都内企業の生産性向上支援などを図ります。デジタルツインはすでに製造業などでは活用されつつあり、サプライチェーンをモデル化し、調達、製造、保管、輸送、販売をサイバー空間上で紐付けてモノやお金、情報の流れをシミュレーションすることが可能となっています。
  + **【補足説明材料】**
    - **3-16とコラム併せて大幅に追記する**
    - 【要旨】IoT, ビッグデータ, AI, ロボット等の新たなIT活用におけるサイバーセキュリティ対策
      * クラウドサービスの活用 「クラウドサービスとは」 具体的な活用事例　IaaS　メール、Apサービス、AWSの事例 「クラウドサービス利用の留意点」
      * CASYB（Cloud Access Secuity　Broker)のセキュリティ確保機能の事例
    - 【コラム】IoT活用企業におけるプライバシー保護に関する考慮事項とは | PwC Japanグループ
    - 【コラム】サイバー・フジカル・セキュリティ対策フレームワーク対応 NIST　SP800―161　サプライチェーンリスクマネージメント
    - **【コラム】サイバー・フィジカル・セキュリティ対策フレームワーク対応**
      * 【担当：早出】
      * 【コラム】サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）（2019年4月METI）対応
        + Society5.0, Connected Industriesの実現に向けて、産業界に求められるセキュリティ対策の全体像
      * 【コラム】**サプライチェーン全体での対策（中小企業向け）**
        + 対応計画（BCP対応）
        + 想定されるリスクと対策の整理

サプライチェーンを構成する企業のフィジカル空間での繋がり

フィジカル空間とサイバー空間の繋がり

サイバー空間とサイバー空間の繋がり

* + - 【コラム】NIST SP800-171 「連邦政府外のシステムと組織における管理された非格付け情報の保護」 改訂Revishon2対応
      * NIST SP 800-171 の要求事項と「サイバー・フィジカル・セキュリティ対策フレームワーク」との対応表
    - 【コラム】NIST　SP800-53 「連邦政府情報システムおよび連邦組織のための セキュリティ管理策とプライバシー管理策」改訂Rev4.0対応
* **【Mission04】もしもマニュアル**
  + 4-1：緊急事態応用マニュアルの作成
  + 4-2：基本事項の決定
  + 4-3：漏えい・流出発生時の対応
  + 4-4：改ざん・消失・破壊・サービス停止発生時の対応
  + 4-5：ウイルス感染時の初期対応
  + 4-6：届け出および相談
  + 4-7：大規模災害などによる事業中断と事業継続管理
    - **【補足説明材料】**
      * IT/BCP　範囲とフレームワーク再検討する
        + セキュリティ侵害も事業継続を脅かすリスクの一つであり、事業継続計画には、セキュリティ対策の事前対応も含める必要がある
* **【MISSION5】やってみよう！サイバー攻撃対策シミュレーション**
  + 5-1：サイバー攻撃前夜
  + 5-2：攻撃発生その瞬間
  + 5-3：サイバー攻撃直後
  + 5-4：潜入拡大
  + 5-5：顧客への被害拡大 取引先への被害拡大
  + 5-6：サイバー攻撃の発覚
  + 5-7：原因が判明 ウイルス感染が原因
  + 5-8：再発防止策の作成
  + 5-9：復旧回復
  + 5-10：EMOTET、ランサムウェア対策
* **【Mission6】　インフォメーション**
  + 6-1：もしかしてサイバー攻撃？ここに連絡を！
    - 警視庁、IPA、東京都？、、？
  + 6-2：やられる前に、しっかり予防を！
    - **【補足説明材料】**
      * イベントドリブンに！
      * **「相談・届出先クイックリスト」から抜粋**
        + 相談・届出先

スライド

**＜＜＜＜インシデント対応＞＞＞＞**

**■一般的な情報セキュリティ相談**

●IPAセキュリティセンター情報セキュリティ安心相談窓口

☎ 03-5978-7509 -可能な限り公開されているFAQを参照してから相談

**■犯罪の可能性がある場合の相談窓口**

●警視庁　サイバー犯罪対策課

☎ 03-5805-1731　（都庁からは9110-7861-3038, 3089）

**■サイバー犯罪の届出**

●警視庁☎ 03-3581-4321（交換）

管轄の警察署名を確認し転送を

**■フィッシング詐欺に関連するメールやサイトにアクセスした場合のメール相談**

**【ビジネスメール詐欺は、自社と取引先のどちらにも損害賠償責任があり得る】**

●フィッシング対策協議会

**■迷惑メール相談センター　（日本データ通信協会）**

不特定多数へ同意を得ずに送られる広告宣伝目的メール　 ☎ 03-5974-0068

**■なりすましECサイトを作られた事業者の対策ガイド**

事業者：①問合わせ対応メモ　②サイト内注意喚起 ③プロバイダ削除要請

利用者：警視庁サイバー犯罪対策課、管轄の警察署

●なりすましECサイト対策協議会

違法情報の通報:

**■インターネット上での違法・有害情報の相談・通報**

●「違法・有害情報センター」(総務省系)

【削除依頼は行わない】

Webでユーザ登録してから具体的な相談

●「インターネット・ホットラインセンター」: (警察庁・総務省　フォームで通報)

**■消費生活全般に関する苦情や問合せ**

●消費者ホットライン【国民生活センター】☎ 188番

**■法律相談**

●法テラス（日本司法支援センター）☎0570-078374

**■個人情報の取り扱いに関する相談**

個人情報保護委員会 ☎ 03-6457-9849

**■嫌がらせ、ネットストーカーの相談**

●管轄の警察署の生活安全課ブラウザで警察署一覧検索

**■人権相談**

●「法務省人権擁護局　みんなの人権110番 ☎ 0570-003-110

**■インシデント報告・届出**

●JPCERT/CC ☎03-6811-0610

インシデント対応依頼 ☎03-6271-8901

（サイトの改ざん箇所の特定や、改ざんされた際の復旧手順。サーバへの侵入やDoS攻撃が発生した際の対処。マルウエアに感染した際の駆除方法、復旧方法。）

●IPA J-CRAT／標的型サイバー攻撃特別相談窓口

E-mail tokusou@ipa.go.jp　☎ 03-5978-7599

**＜＜＜＜恒久的対策＞＞＞＞**

**■IT化・セキュリティ対策支援企業(ITコーディネータ)**

**●情報セキュリティ対策支援サイト**（IPA)

●IPAセキュリティプレゼンター検索（IPA)

●情報セキュリティサービス基準適合サービスリスト（IPA)

●サイバーインシデント緊急対応企業一覧　(JNSA)

●ITコーディネータ協会　「経営とIT化相談」窓口

●東京都テレワーク推進センター ☎0120-970-396

●テレワークのセキュリティあんしん相談窓口　ネットで申込み（総務省⇒LAC）

●テレワーク相談センター(厚労省委託) ☎0120-91-6479

●東京都中小企業振興公社ワンストップ総合相談☎03-3251-7881

**■IT化・セキュリティ対策助成制度等**

● SECURITY ACTION

中小企業自ら取り組みを宣言する制度　☎03-5978-7508

●IT導入補助金（サービス等生産性向上IT導入支援事業）(終了)

●サイバーセキュリティ対策促進助成金（東京都）「標的型メール訓練」

事前支援

●中小企業の情報セキュリティマネジメント指導業務(METI補助事業)【主に事前支援、登録セキスぺを派遣】（今年度は募集終了）

事後支援

●中小企業向けサイバーセキュリティお助け隊（サイバーセキュリティ事後対応支援実証事業）(IPA)【主に事後支援】（現在、東京都はなし）

**＜＜＜＜参考情報サイト＞＞＞＞**

●「ここからセキュリティ！」:ポータルサイト（事象・対象）(IPA)

●JC3 情報提供 注意喚起情報

・**JC3:あなたのパスワードが侵害されました**

・不正送金等

●JPCERT/CC　注意喚起

・**マルウエア Emotet の感染に関する注意喚起**

●迷惑メール相談センター

・迷惑メール・チェーンメール関連パンフレット

●迷惑メール関連の関係法令・窓口等(迷惑メール白書2019より)

●中小企業の情報セキュリティ対策ガイドライン　第3版電子版(IPA)

・　情報セキュリティ5か条、5分でできる！情報セキュリティ自社診断

●国民のための情報セキュリティサイト (総務省)

* + **6-4：セキュリティお役立ち情報リンク**
    - **【補足説明材料】**
      * 主な文献・リンクのリストアップとそれらを典拠とした内容の要約
      * **【校正案】【6-3】サイバーセキュリティお役立ちリンク**
        + 本編で更新中
        + 作成方針

サイバーセキュリティ対策に有用な文献、Webページを列挙する

URLは、可視化される必要はなく、電子版でアンカータグの形で埋め込む

「極意」では、スペースに限りがあるので、主な文献、サイトを選別

* + - * + 「極意」でリストアップするお役立ちリンク

赤字は、既にリストアップされているリンク

青字に、リンクを追加する候補

* + - * + リストアップ候補

サイバーセキュリティに関連する国等の基本文書、白書、解説文書

基本文書（法律・基本計画・各種方針等）

サイバーセキュリティ基本法

サイバーセキュリティ戦略【2018年７月閣議決定】

サイバーセキュリティ2020【NISC】

セキュリティ関連NIST文書【IPA】

NIST関連

サイバーセキュリティフレームワーク（NIST\_CSF）【NIST】

重要インフラのサイバーセキュリティを改善するためのフレームワーク【NIST】

NIST SP800-172\_制御された未分類の情報を保護するための強化されたセキュリティ要件：NIST Special Publication 800-171の補足【2021年2月】

**ISMS適合性評価制度**【JIPDEC】

ISMS関連

JIS Q 27002\_2014 情報技術?セキュリティ技術?情報セキュリティ管理策の実践のための規範

ISMSユーザーズガイド-JISQ270012014(ISO\_IEC270012013)対応【JIPDEC】

各種白書・年次報告書類

情報通信白書【SOUMU】

AI白書【IPA】

情報セキュリティ白書【IPA】

IT人材白書【IPA】

迷惑メール白書2019 参考編／資料編

情報セキュリティ10大脅威【IPA】

各実施事項毎の参考情報【経営者、管理者向け】

サイバーセキュリティ全般

企業経営のためのサイバーセキュリティの考え方【NISC】

（Mission3-5、Page.89\_ITおよびサイバーセキュリティに関する組織の視点6分類のベースとなる資料）

サイバーセキュリティ経営ガイドライン【METI】

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）関連

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました

サイバーサプライチェーンリスク. マネジメント

サイバー・フィジカル・セキュリティ対策フレームワーク ～Society5.0 における新たなサプライチェーン （バリュークリエイションプロセス）の信頼性の確保に向けて～

サイバーセキュリティ協議会

サイバーセキュリティ協議会

昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書【METI】

中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊-成果報告書【METI】

サイバーサプライチェーンリスクマネジメント調査報告【IPA】

サイバーセキュリティ対策に関する参考情報【サイバーセキュリティ経営ガイドラインVer 2.0関連】

重要１０項目全般に関連する参考情報

指示３に関連する参考情報

指示４に関連する参考情報

指示５に関連する参考情報

指示６に関連する参考情報

指示７に関連する参考情報

指示８に関連する参考情報

指示９に関連する参考情報

指示１０に関連する参考情報

DX関連

Society5.0

サイバーフィジカルシステム（CPS)

DXレポート ～ITシステム「2025年の崖」克服とDXの本格的な展開～

デジタルトランスフォーメーションを推進するためのガイドライン（DX推進ガイドライン）Ver.1【2018年12月METI】

デジタル・トランスフォーメーション（DX）推進に向けた企業とIT人材の実態調査

DXレポート2中間取りまとめ

DXの推進に関するお役立ちコンテンツ一覧【IPA】

【解説書等】

【参考】DX推進指標自己分析結果分析レポート【2020年5月28日IPA】

【参考】プラットフォームデジタル化指標について【2020年6月IPA】

【参考】DX推進セミナー～DXの実現に向けた取り組み～

テレワーク関連

テレワーク実施者の方へ【NISC】

テレワークを実施する際にセキュリティ上留意すべき点について【2020年4月9日NISC】

テレワークの推進【総務省】

テレワークセキュリティガイドライン第４版【2018年4月総務省】

テレワーク総合ポータルサイト【厚生労働省】

テレワークではじめる働き方改革\_テレワークの導入・運用ガイドブック【2019年12月厚生労働省】

テレワークを行う際のセキュリティ上の注意事項【IPA】

テレワーク勤務のサイバーセキュリティ対策！ 警視庁

AI関連

AI利活用ハンドブック

「AI利活用ハンドブック～AIをかしこく使いこなすために～」

IoTセキュリティ関連

欧州ネットワーク情報セキュリティ機関（ENISA）「IoTのベースラインセキュリティに関する提言」概要【2018年1月19日IPA】

IoTセキュリティチェックリスト【JPCERT/CC】

IoTセキュリティガイドライン ver1.0【総務省と経済産業省による「IoT推進コンソーシアム　IoTセキュリティワーキンググループ」】

IoTセキュリティガイドライン ver1.0概要

**IoT・5Gセキュリティ総合対策プログレスレポート2020**【2020年5月サイバーセキュリティタスクフォース】【総務省】

【スライド資料】IoT機器への対策を含むサプライチェーンサイバーセキュリティの強化【2018年METI商務情報政策局】

IoTセキュリティチェックリスト

IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）

【削除】IoTセキュリティ対応マニュアル産業保安版

「安全なIoTシステムのためのセキュリティに関する一般的枠組」【NISC】

インシデント対応

インシデント発生時に組織内で整理しておくべき事項（サイバーセキュリティ経営ガイドライン\_付録C）【METI】

個人情報保護関連

GDPR

DX企業のプライバシーガバナンスガイドブックver1.0【2020年8月3日METI】

**人材育成**

iCD関連

**iコンピテンシディクショナリ（iCD）について**

ITSS+関連

**ITSS+・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報**

データサイエンス領域

アジャイル領域

IoTソリューション領域

セキュリティ領域

DX関連

デジタル・トランスフォーメーション推進人材の機能と役割のあり方に関する調査【2020年5月15日IPA】

サイバーセキュリティ関連

**サイバーセキュリティ体制構築・人材確保の手引き**(サイバーセキュリティ経営ガイドライン：付録F)（PDF形式）（令和2年９月30日公開）

情報処理技術者試験

**情報処理技術者試験・情報処理安全確保支援士試験**

**法令・規則**

**サイバーセキュリティ関係法令\_Q&AハンドブックVer1.0**

迷惑メール関係法令・窓口等【迷惑メール白書2019】【P.142～145】

一般ユーザ向け啓発資料【IT利用局面毎】

インターネットでの不正行為を発見した場合

違法情報・有害情報、誹謗中傷情報

ECサイト利用

利用者向けフィッシング詐欺対策ガイドライン【2020年6月フィッシング対策協議会】

利用者向けフィッシング詐欺対策ガイドライン【2020年6月フィッシング対策協議会】

なりすましECサイト対策対応マニュアル【2015年3月セーファーインターネット協会】

電子メール

特定電子メールの送信の適正化等に関する法律のポイント（2020年度版）【日本データ通信協会迷惑メール相談センター】

チェーンメール対策BOOK\_「撃退！チェーンメール 」（2020年度版）【日本データ通信協会迷惑メール相談センター】

詐欺メール対策リーフレット「そのメール、詐欺カモ！？」（2020年度）【日本データ通信協会迷惑メール相談センター】

迷惑メール対策BOOK\_「撃退！迷惑メール」（2020年度版）【日本データ通信協会迷惑メール相談センター】

関連機関の参考サイト

内閣サイバーセキュリティセンター（NISC）

みんなでしっかりサイバーセキュリティ

みんなで使おうサイバーセキュリティ・ポータルサイト

情報処理推進機構（IPA）

情報セキュリティ

ここからセキュリティ

SECURITY ACTION セキュリティ対策自己宣言

サイバー情報共有イニシアティブ（J-CSIP）

JPCERTコーディネーションセンター（JPCRT/CC）

緊急情報を確認する

脆弱性対策情報データベース（JVN）

JPCERT/CCに依頼する

総務省

国民のための情報セキュリティサイト（総務省）

リンク集｜国民のための情報セキュリティサイト - 総務省

**経済産業省**

**サイバーセキュリティ政策**

日本サイバー犯罪対策センター（JC3）

情報セキュリティ広場（警視庁）

**セーファーインターネット協会（一般社団法人）**

・

・

* + - * 【素材の列挙】主な文献のリスト
        + 基本文書

サイバーセキュリティ経営ガイドライン2.0版【METI】

「情報セキュリティ白書2020」【IPA】

中小企業の情報セキュリティ対策ガイドライン（第3版）【IPA】

* + - * + 背景・根拠文書

国等の施策の基本計画・実施計画・白書類

経済財政運営と改革の基本方針（骨太方針）【閣議決定】

AI戦略2019～人・産業・地域・政府全てにAI～【2019年6月11日統合イノベーション戦略推進会議決定】

サイバーセキュリティ基本法

サイバーセキュリティ戦略【2018年７月閣議決定】

サイバーセキュリティ2020【NISC】

企業経営のためのサイバーセキュリティの考え方【NISC】

IT総合戦略室\_デジタル・ガバメント実行計画【CAB】

情報通信白書【SOUMU】

AI白書【IPA】

情報セキュリティ白書【IPA】

IT人材白書【IPA】

次世代情報化社会の概念と課題

Society5.0\_DX関連\_第4次産業革命

サイバーセキュリティ関連

次世代情報化社会への対応のための実施方針・実施手順

DXの実現に向けた取り組み【2020年6月IPA】

「デジタル・トランスフォーメーション（DX）推進に向けた企業とIT人材の実態調査」【2020年5月15日IPA】

プラットフォームデジタル化指標について【2020年6月IPA】

サイバーセキュリティ関連

DX時代における企業のプライバシーガバナンス【METI】

SOUMU\_IoT・5Gセキュリティ総合対策【2019年8月SOUMU】

IoT・5Gセキュリティ総合対策プログレスレポート2020【2020年5月サイバーセキュリティタスクフォース】【SOUMU】

グループ・ガバナンス・システムに関する実務指針（グループガイドライン）【METI】

サイバー・フィジカル・セキュリティ対策フレームワーク【METI】

政府機関等の対策基準策定のためのガイドライン【NISC】

重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書【NISC】

重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第1版）【NISC】

NIST\_関連文書

NIST CSF　(重要インフラにおけるサイバーセキュリティフレームワーク)

重要インフラにおけるサイバーセキュリティフレームワーク1.0版（CSF)【2014年2月12日NIST】

CIS-Controls Version-7-cc-FINAL

NIST 800-46 Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

NIST SP800-60情報セキュリティ第 I 巻：情報および情報システムのタイプとセキュリティ分類のマッピングガイド【2004年6月NIST】

NIST SP800-171 「連邦政府外のシステムと組織における管理された非格付け情報の保護」 改訂Revishon2対応

NIST SP800-172\_制御された未分類の情報を保護するための強化されたセキュリティ要件：NIST Special Publication 800-171の補足【2021年2月】

NIST.SP.800-181

NIST　SP800-53 「連邦政府情報システムおよび連邦組織のための セキュリティ管理策とプライバシー管理策」改訂Rev4.0対応

連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド：セキュリティライフサイクルによるアプローチ)【SP800-37】【2010年2月NIST】

NIST SP 800-61 (コンピュータセキュリティインシデント対応ガイド)

NIST SP 800-63 (電子的認証に関するガイドライン)

NIST SP 800-113 Guide to SSL VPNs

CSC20 （効果的なサイバー防御のための重要なセキュリティコントロール）

Top35 （標的型サイバー侵入の軽減戦略）

NIST SP.800-82R2　Guide to Industrial Control Systems (ICS) Security

欧州ネットワーク情報セキュリティ機関（ENISA）「IoTのベースラインセキュリティに関する提言」概要【2018年1月19日IPA】

JIPDEC\_ISMS関連文書

JIS Q 27002\_2014 情報技術?セキュリティ技術?情報セキュリティ管理策の実践のための規範

ISMSユーザーズガイド-JISQ270012014(ISO\_IEC270012013)対応【JIPDEC】

サイバーセキュリティ対策支援事業（サイバーセキュリティ協議会・お助け隊等）【METI】

昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書【METI】

中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊-成果報告書【METI】

中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた実現可能性調査成果報告書【METI】

「中小企業の経営者のサイバーリスク意識調査2019」【METI】

令和2年度中小企業の情報セキュリティマネジメント指導業務【2020年10月2日IPA】

「事業案内チラシ」

「指導内容について

「よくある質問」

昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書【METI】

次世代IT及びセキュリティ人材育成

iCD関連

iCD解説

Bib06-07iコンピテンシ・ディクショナリ（IPA）

Bib04-02タスクディクショナリ （タスク小分類415項目）

Bib04-03スキルディクショナリ (スキル424項目・知識8256項目)

Bib04-04タスク毎に必要なスキル詳細 （タスク小分類415項目）

Bib05-01iCDスキルディクショナリ (スキル424項目・知識8256項目から抜粋)

Bib10-11 アジャイル開発「ITSS+」

ITSS+関連

ITSS+・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報

データサイエンス領域

Bib10-09データサイエンス領域のスキル標準「ITSS+」

ITSS＋「データサイエンス領域」改訂版2019

（参考）ITSS＋「データサイエンス領域」新旧比較（Excel形式）

データサイエンティストのためのスキルチェックリスト/タスクリスト 概説

アジャイル領域

ITSS＋アジャイル開発の進め方【2018年4月IPA】

Bib10-11 アジャイル開発「ITSS+」 【MindManager→html】【SK2】

アジャイル領域へのスキル変革の指針）

なぜ、いまアジャイルが必要か？

Society5.0時代になぜアジャイルが 必要なのか

アジャイルソフトウェア開発宣言の読みとき方

アジャイル開発のベースにあるマインドセットや原則について

ビジョンとプロダクトの橋渡し（プロダクト責任者）

プロダクト・サービスとして価値を届けるために「プロダクト責任者」が主導するプロセスと役割について

アジャイル開発の進め方

アジャイル開発のプロセスと開発チームの 役割について

〈参考〉従来型ロールとアジャイル型ロールの比較表

参考文献

IoTソリューション領域

IoTソリューション領域へのスキル変革の指針

タスクリスト（Excel形式）

参考文献

セキュリティ領域

Bib10-10セキュリティ領域のスキル標準「ITSS+」

**ITSS+「セキュリティ領域」改訂版（EXCEL)**

情報処理技術者試験関連

Bib04-05スキル概要と情報処理試験（熟達度レベル評価判定）

IPA以外

**サイバーセキュリティ経営ガイドライン：付録F\_サイバーセキュリティ体制構築・人材確保の手引き（PDF形式）（令和2年９月30日公開）**

法令・規則

サイバーセキュリティ関係法令\_Q&AハンドブックVer1.0

迷惑メール関係法令・窓口等【迷惑メール白書2019】

実施手順（管理者向け）

サイバーセキュリティ経営ガイドラインVer2.0【METI】

サイバーセキュリティ経営ガイドライン Ver2.0

付録C インシデント発生時に組織内で整理しておくべき事項（Excel形式）（平成29年11月16日公開）

**付録F サイバーセキュリティ体制構築・人材確保の手引き（PDF形式）（令和2年９月30日公開）**

サイバーセキュリティ経営ガイドラインの改訂ポイント（PDF形式）（平成29年11月16日公開）

中小企業の情報セキュリティ対策ガイドライン第3版【IPA】

情報セキュリティ10大脅威【IPA】

インターネットの安全・安心ハンドブック（ネットワークビギナーのための情報セキュリティハンドブックVer 4.10）【NISC】

GDPR関連

NIST CSFとの併用で効果を最大化するフレームワーク～NISTプライバシーフレームワークの活用方法～【2020年02月18日コンサルタント星野靖】

2020年1月16日に米国国立標準技術研究所(NIST)がプライバシーフレームワーク 1.0 (以下、NIST\_PF)を策定しました。 NIST\_PFは法規制でも認証でもない参考とすべきフレームワークという位置づけであり、必須で遵守すべきものではないが、NISTサイバーセキュリティフレームワーク(NIST\_CSF)のように、世界中で参考にされることが見込まれる。

中小企業向け「はじめての個人情報保護法」～シンプルレッスン～【2017年6月個人情報保護委員会】

特定個人情報の適正な取扱いに関するガイドラン （事業者編）（個人情報保護委員会）

個人情報の 保護に関する法律ついての分野別 ガイドライン（各府省庁）

匿名加工情報の事例集（JIPDEC認定個人情報保護団体対象事業者向け）【PDF】【2017年7月JIPDEC】

改正個人情報保護法（2017年5月改正施行）対応

「企業における営業秘密管理に関する実態調査」報告書について【2017年3月17日IPA】

組織における内部不正防止ガイドライン（日本語版） 第4版ガイドライン【2017年1月31日IPA】

【てびき】情報管理も企業力～秘密情報の保護と活用～【2016年12月5日METI】

マイナンバー制度とマイナンバーカード【総務省HP】

テレワーク関連

テレワークではじめる働き方改革\_テレワークの導入・運用ガイドブック【2019年12月厚生労働省】

テレワークを実施する際にセキュリティ上留意すべき点について【2020年4月9日NISC】

テレワークセキュリティガイドライン第４版【2018年4月総務省】

情報システム担当者のためのテレワーク導入手順書【2016年3月総務省】

情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン【2018年2月22日厚生労働省】

Wi-Fiセキュリティ対策【SOUMU】

中小企業等担当者向けテレワークセキュリティの手引き【SOUMU】

情報漏えいを防ぐためのモバイルデバイス等設定マニュアル【IPA】

インシデント対応

情報セキュリティ事故対応【IISEC】

**サイバーセキュリティ経営ガイドライン\_付録Cインシデント発生時に組織内で整理しておくべき事項【METI】**

フィッシング・BEC・迷惑メール等【EMOTET】

迷惑メール白書2019 参考編／資料編

ビジネスメール詐欺の事例から見る騙しの手口【2017年4月3日J-CSIP】

ビジネスメール詐欺の実態調査報告書【2020年3月25日JPCERTCC】

マルウェア「Emotet」の感染攻撃に注意喚起--基本的な防御策の徹底を【ZDNet】

実施手順（一般ユーザ向け）

TCYSS\_「中小企業向けサイバーセキュリティ対策の極意（初版）」【東京都】

なりすましECサイト対策対応マニュアル【2015年3月セーファーインターネット協会】

チェーンメール対策BOOK\_「撃退！チェーンメール 」（2020年度版）【日本データ通信協会迷惑メール相談センター】

利用者向けフィッシング詐欺対策ガイドライン【2020年6月フィッシング対策協議会】

特定電子メールの送信の適正化等に関する法律のポイント（2020年度版）【日本データ通信協会迷惑メール相談センター】

詐欺メール対策リーフレット「そのメール、詐欺カモ！？」（2020年度）【日本データ通信協会迷惑メール相談センター】

迷惑メール対策BOOK\_「撃退！迷惑メール」（2020年度版）【日本データ通信協会迷惑メール相談センター】

AI利活用ハンドブック

「AI利活用ハンドブック～AIをかしこく使いこなすために～」

違法・有害情報相談センターへの相談フォーム

* + - * 主な情報サイトのリスト
        + ここからセキュリティ！ 情報セキュリティ・ポータルサイト【IPA】
        + みんなでしっかりサイバーセキュリティ【NISC】
        + 国民のための情報セキュリティサイト【総務省】
        + 中小企業の情報セキュリティマネジメント指導業務【IPA】
        + 中小企業サイバーセキュリティ対策の極意ポータルサイト【東京都】
        + インターネット安全・安心相談【警察庁】
  + 【Web版コラム】セキュリティお役立ちリンク【詳細版】
    - **主な文献のリストアップと複数文献を典拠とした内容の要約を纏める**
      * 「Sec01-02\_サイバーセキュリティ関連\_各種ガイドブックの内容要約\_インデックス 」 を参考としてリストと要約を抜粋
    - 「サイバーセキュリティ経営ガイドライン」Ver2.0 付録B サイバーセキュリティ対策に関する参考情報の内容の反映
    - 「テレワークセキュリティガイドライン第4版」【総務省】参考リンク集の内容を反映
  + 【Web版コラム】サイバーセキュリティ経営チェックシート
    - 「サイバーセキュリティ経営ガイドライン」Ver2.0 付録A サイバーセキュリティ経営チェックシートの内容の反映
      * 本チェック項目とNISTが提供するサイバーセキュリティフレームワーク10との対応関係も合わせて提示されている
      * ＜NISTのサイバーセキュリティフレーワークとの対応関係の提示＞
        + 付録Aの各チェック項目について、NISTのサイバーセキュリティフレームワークと対応する項目を提示。
  + 【Web版コラム】IoT機器調査及び利用者への注意喚起プロジェクト（NOTICE対応）
  + 【Web版コラム】システム管理者としての基本技術の解説
    - 【Web版コラム】システム管理者としての基本技術の解説
    - （安全・安心ハンドブック（NISC）等を参照）
    - ※クレジットカード　PCI/DSS（Payment Card Industry Data Security Standard）
    - ※ブロックチェーン技術の応用
    - **※Wifiセキュリティ**
  + 【Web版コラム】経営者向けサイバーセキュリティ経営のための啓発資料
    - 【Web版コラム】「Sec01-02\_サイバーセキュリティ関連\_各種ガイドブックの内容要約\_インデックス」から「経営者向け」資料を抜粋【再掲】
    - 【Web版コラム】Sec03-02\_経営者向けサイバーセキュリティ経営の体系的啓発資料
    - 【Web版コラム】DAX43-01-1 ECサイトのサイバーセキュリティ対策の実践のために必要なスキル・知識
    - 【Web版コラム】DAX20-0402-3 IT人材白書2018
      * IT 事業・IT 業務の現状
        + （1）IT事業・IT業務の拡大傾向
        + （2）IT企業とユーザー企業の連携
      * ６節スキル標準と i コンピテンシ ディクショナリ
        + 1. 第４次産業革命に向けたIT人材の育成

（1）データサイエンス領域

（2）セキュリティ領域

* + - * + 2. i コンピテンシ ディクショナリ

（1）iCDコンテンツの進化

（2）iCD活用企業の拡大

（3）グローバル連携

* + - 【Web版コラム】Sec01-02-10 ウェブサイト開設等における運営形態の選定方法に関する手引き
    - 【Web版コラム】DAX25-20-03【書籍】AI白書2019\_第3章利用動向
    - 【Web版コラム】DAX25-20-05-5-6-3社会実装推進の方向性（テンプレート例）
    - 【Web版コラム】DAX22-01 AI・データの利用に関する契約ガイドライン（概要資料）
  + 6-5：中小企業の情報セキュリティ対策ガイドライン【第3版】
    - 「中小企業の情報セキュリティ対策ガイドライン第3版」の位置づけ、全体、活用方法、構成目次と要約を引用。IPAのページへリンク
    - 6-5(1)：本編の概要説明
    - 6-5(2)：情報セキュリティ5カ条
    - 6-5(3)：情報セキュリティ基本方針
    - 6-5(4)：新・5分でできる自社診断シート
      * Subtopic
      * 組織として最初に取り組むべき、 情報セキュリティ対策の自社診断シート
      * 組織においてあまり費用をかけることなく実行することで効果がある情報セキュリティ対策を25項目に絞られてます
      * 組織として最初に取り組むべき情報セキュリティ対策の自社診断シート　基本的対策、 従業員としての対策、 組織としての対策、 全25項目
      * 【参考】
        + 【参考】Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン

中小企業の情報セキュリティ対策ガイドライン https://www.ipa.go.jp/security/keihatsu/sme/guideline/

* + - * + 情報セキュリティ対策ベンチマーク https://www.ipa.go.jp/security/benchmark/
      * Part1 基本的対策
        + №1 パソコン等の脆弱性対策

1.Windows Update※1 を行うなどのように、 常にOS やソフトウェアを安全な状態にしていますか？

* + - * + №2 パソコン等のウイルス対策

2.パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル※2 を自動更新するなどのように、 パソコンをウイルスから守るための対策を行っていますか？

* + - * + №3 パソコン等のパスワード管理

3,パスワードは自分の名前、 電話番号、 誕生日など推測されやすいものを避けて複数のウェブサイトで使いまわしをしないなどのように、 強固なパスワードを設定していますか？

* + - * + №4 重要情報へのアクセス(権)管理

4.ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、 重要情報に対する適切なアクセス制限を行っていますか？

* + - * + №5 脅威情報等の情報共有

5.利用中のウェブサービス※3 や製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？

* + - * Part2 従業員としての対策
        + №6 標的型攻撃メール対策等

6.受信した不審な電子メールの添付ファイルを安易に開いたり 本文中のリンクを安易に参照したりしないようにするなど、 電子メールを介したウイルス感染に気をつけていますか？

* + - * + №7 電子メールの誤送信防止

7.電子メールを送る前に目視にて送信アドレスを確認するなどのように、 宛先の送信ミスを防ぐ仕組みを徹底していますか？

* + - * + №8 電子メールでの重要情報漏えい対策

8.重要情報をメールで送る時は重要情報を添付ファイルに書いてパスワード保護するなどのように、 重要情報の保護をしていますか？

* + - * + №9 無線LANのセキュリティ対策

9.無線LAN を利用する時は強固な暗号化を必ず利用するなどのように、 無線LAN を安全に使うための対策をしていますか？

* + - * + №10 インターネットを介したトラブル防止

10.業務端末でのウェブサイトの閲覧やSNS への書き込みに関するルールを決めておくなどのように、 インターネットを介したトラブルへの対策をしていますか？

* + - * + №11 重要情報のバックアップ等の保全対策

11.重要情報のバックアップを定期的に行うなどのように、 故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？

* + - * + №12 重要情報の事務所等での管理

12.重要情報を机の上に放置せず書庫に保管し施錠するなどのように、 重要情報の紛失や漏えいを防止していますか？

* + - * + №13 重要情報の持ち出し等の管理

13.重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、 盗難や紛失の対策をしていますか？

* + - * + №14 パソコン等の第三者利用制限

14.離席時にコンピュータのロック機能を利用するなどのように、 他人に使われないようにしていますか？

* + - * + №15 事務所等への不正侵入対策

15.事務所で見知らぬ人を見かけたら声をかけるなどのように、 無許可の人の立ち入りがないようにしていますか？

* + - * + №16 事務所等での重要機器の管理

16.退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、 盗難防止対策をしていますか？

* + - * + №17 事務所等での入退出管理

17.最終退出者は事務所を施錠し退出の記録（日時、 退出者）を残すなどのように、 事務所の施錠を管理していますか？

* + - * + №18 不要になった重要情報の廃棄管理

18.重要情報を廃棄する場合は、 書類は細断したり、 データは消去ツールを使ったりするなどのように、 重要情報が読めなくなるような処分をしていますか？

* + - * Part3 組織としての対策【要確認】
        + №19 守秘義務等の従業員への徹底

19.採用の際に守秘義務や罰則規定があることを知らせるなどのように、 従業員に秘密を守らせていますか？

* + - * + №20 従業員へのセキュリティ意識付け

20.情報管理の大切さなどを定期的に説明するなどのように、 従業員に意識付けを行っていますか？

* + - * + №21 BYOD対応のセキュリティ対策

21.社内外での個人所有のパソコンやスマートフォンの業務利用を許可制にするなどのように、 業務で個人所有端末の利用の可否を明確にしていますか？

* + - * + №22 取引先とのセキュリティ協議

22.契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、 取引先に秘密を守ることを求めていますか？

* + - * + №23 外部サービスのセキュリティ対策

23.クラウドサービスなど外部サービスを利用する時は利用規約やセキュリティ対策を確認するなどのように、 サービスの安全・信頼性を把握して選定していますか？

* + - * + №24 BCPを踏まえたセキュリティ事故対策

24.秘密情報の漏えいや紛失、 盗難があった場合の対応手順書を作成するなどのように、 事故が発生した場合に備えた準備をしていますか？

* + - * + №25 セキュリティルールの策定と運用

25.情報セキュリティ対策（上記1～24 など）を会社のルールにするなどのように、 情報セキュリティ対策の内容を明確にしていますか？

* + - * さらなる情報セキュリティ対策の検討するには
        + 「5 分でできる！情報セキュリティ自社診断」の次のステップとして、 ガイドラインを活用したポリシーの策定やベンチマークでの自己診断を実施してみよう。
    - 6-5(5)：情報セキュリティハンドブックひな形（従業員向け）
      * 従業員向け情報セキュリティハンドブック 【中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】】 【付録2をサンプルとして】
    - 6-5(6)：情報セキュリティポリシーサンプル
    - 6-5(7)：情報セキュリティ関連規程の明文化
      * 6-5(8)：情報セキュリティポリシーサンプル
        + 自社の情報セキュリティポリシー 【中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】】 【付録３ツールBをサンプルとして】
    - 6-5(9)：情報資産台帳の作成
    - 3-20⇒6-5(10)：リスク分析シート
      * どんな情報資産があるか
        + ビジネスに影響を与える重要度の高い情報資産の洗い出し

重要度とは？

機密性、 完全性、 可用性それぞれの評価値から3段階で判定

* + - * どんな脅威があるか
        + サイバー攻撃，情報漏えい，故意，過失，誤謬びゅう，不正行為，妨害行為，サービス妨害，
        + 風評，炎上，SPAM（迷惑メール），ファイル共有ソフト
        + 物理的脅威

（事故，災害，故障，破壊，盗難，不正侵入 ほか）

* + - * + 技術的脅威

（不正アクセス，盗聴，なりすまし，改ざん，エラー，クラッキング ほか）

* + - * + 人的脅威

（誤操作，紛失，破損，盗み見，不正利用，ソーシャルエンジニアリング ほか）

* + - * どんな情報資産にどんな脆弱性があるか
        + 現状の対策で、 重要度の高い情報資産ごとにどんな脆弱性があるか

脆弱性のレベル

バグ，セキュリティホール，人為的脆弱性

* + - * + 被害発生の可能性は？

対象となる情報資産ごとの【脅威の発生頻度x脆弱性のレベル】を３段階で

* + - * 情報資産ごとのリスクの大きさは？
        + リスク値＝重要度x被害発生可能性
      * どんな予防的対策を取るか？
      * 予防的対策を取っても残るリスクは？（情報資産ごとの残留リスク）
      * リスクは許容範囲か
        + セキュリティ侵害をどこまで許せるか
      * 予防できなかったセキュリティ侵害が起きた場合
        + どこまで対策をしてもリスクはゼロにならない。 残留リスクによりセキュリティ侵害があった場合、 対応策を明確にしておく
      * リスク分析シート（情報資産台帳・脅威の状況・脆弱性チェック） 【中小企業の情報セキュリティ対策ガイドライン（第3版）【2019年12月19日IPA】】
    - 6-5(11)：中小企業のためのクラウドサービス安全利用の手引き
  + 6-6：IT人材育成・人材確保
    - 【担当：中山】
    - ITSS
      * 【参考】ITSS+（プラス）・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報
    - 【参考】IT人材白書2017,2018,2019
      * DAX20-0402-3 IT人材白書2018
        + IT 事業・IT 業務の現状

（1）IT事業・IT業務の拡大傾向

（2）IT企業とユーザー企業の連携

* + - * + ６節スキル標準と i コンピテンシ ディクショナリ

1. 第４次産業革命に向けたIT人材の育成

（1）データサイエンス領域

（2）セキュリティ領域

2. i コンピテンシ ディクショナリ

（1）iCDコンテンツの進化

（2）iCD活用企業の拡大

（3）グローバル連携

* + - * 【特集】デジタルトランスフォーメーション時代のIT人材【2017】
      * デジタル化に携わる人材【2019】
      * 人工知能に携わる人材【2019】
    - iコンピテンシ・ディクショナリ(iCD)
      * iコンピテンシディクショナリについて
      * IT関連タスク毎に必要なスキル、スキルの土台となる知識
      * 【参考】
        + Bib06-07iコンピテンシ・ディクショナリ（IPA）
        + Bib04-02タスクディクショナリ （タスク小分類415項目）
        + Bib04-03スキルディクショナリ (スキル424項目・知識8256項目)
        + Bib04-04タスク毎に必要なスキル詳細 （タスク小分類415項目）
        + Bib05-01iCDスキルディクショナリ (スキル424項目・知識8256項目から抜粋)
    - 情報処理技術者試験制度
      * 【ポイント】全従業員は、社会人の常識とされる「ITパスポート試験レベル」のスキルを！
  + **6-7：情報管理が不適切などの場合の処罰など**
    - 制度・施策
      * IoT機器調査及び利用者への注意喚起プロジェクト（NOTICE対応）
      * 情報セキュリティサービス審査登録制度及びシステム監査基準（2018年改訂）【METI/IPA】
        + 情報セキュリティ監査サービス
        + 脆弱性診断サービス
        + デジタルフォレンジックサービス
        + セキュリティ監視・運用サービス
      * 中小企業のサイバーセキュリティ対策支援体制のモデル構築（サイバーセキュリティお助け隊）（2019年～）【METI/IPA】
        + 昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について【2020年6月12日METI】
      * 【参考】サイバーインシデント緊急対応企業一覧【JNSA】
        + インシデント緊急対応費用
    - 関係法令：法律違反の可能性への対応方法の解説
      * **関連法規の改訂対応**
      * セキュリティ事象に関連する法規の内容要約、事象毎に適用の可能性のある法律名、条文を整理する
      * ガイドブックのMission1-1～13を例に適用が想定される法律名、条文を例示
      * サイバーセキュリティ関係法令\_Q&AハンドブックVer1.0【2020年3月2日NISC】
      * サイバーセキュリティ基本法
      * 不正アクセス禁止法
      * 個人情報保護法
        + 個人情報保護に関するガイドライン，特定個人情報の適正な取扱いに関するガイドライン，マイナンバー法施行令 （行政手続における特定の個人を識別するための番号の利用等に関する法律施行令）
      * 刑法
        + 不正指令電磁的記録に関する罪（ウイルス作成罪）, 電子計算機使用詐欺罪, 電子計算機損壊等業務妨害罪, 電磁的記録不正作出及び供用罪, 支払用カード電磁的記録不正作出等罪, 詐欺罪
      * その他のセキュリティ関連法規
        + 電子署名及び認証業務等に関する法律, プロバイダ責任制限法, 特定電子メール法
      * 知財関連
        + 著作権法, 産業財産権法, 不正競争防止法,
      * 労働関連・取引関連法規
        + 労働基準法, 労働者派遣法, 男女雇用機会均等法, 公益通報者保護法, 労働安全衛生法, 下請法, インターネットを利用した取引, 特定商取引法, 電子消費者契約法
      * その他の法律・ガイドライン・技術者倫理
        + IT基本法，e-文書法（電磁的記録），電子帳簿保存法，コンプライアンス，情報倫理・技術者倫理
      * **GDPR対応**
        + GDPR（General Data Protection Regulation：一般データ保護規則）に対応した個人情報情報保護策について記述
      * **ネットプライバシー（個人攻撃等）**
      * 「情報システム・モデル取引・契約書」
        + DAX47-01\_改正民法に対応した「情報システム・モデル取引・契約書」
* **付録**
  + 付-2：主な参考文献→【主な転載、引用文献】
    - 本書で引用した文献名一覧
  + 付-3：用語解説インデックス
    - 参考資料
      * NISC\_小さな中小企業とNPO向け情報セキュリティハンドブック
        + 用語集・情報セキュリティ関連ウェブサイト一覧・索引
      * ビジネス担当者のための用語ガイド：IoT編
      * Sec01-08-9\_ICT関連用語集