  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】

1.   改訂履歴
   1.   【2020年8月25日】Sec01-01-02と整合
   2.   【2020年8月14日】Sec01-01-03から分離
2.   凡例
   1.  目次掲載項目
   2.   冊子体及び冊子体ベースWebページ
   3.    既存項目（見出し・項番等の軽微な修正は含む）
   4.    追加項目（大きな修正を含む）
   5.     担当
   6.   改訂箇所
   7.   参考資料
3.   本編ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー
   1.  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】
   2.   【Mission0】 はじめに
      1.   改版理由
         1.    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
         2.    NISC等の資料の反映、テレワークの継続化
      2.    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？
      3.    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！
         1.   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
      4.    ケーススタディー３：取引先企業への踏み台にされた
         1.   サプライチェーン紹介のページへのリンク
      5.    ケーススタディー４：EMOTET、ランサムウェアの被害にあった？
      6.    ケーススタディー５：サイバーセキュリティ保険に入っていれば
      7.     ケーススタディーX：「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。

ドキュメントを参照: [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を取りまとめました （METI/経済産業省）](https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html)

* + 1.   改訂箇所：「はじめに」(p.8～9)を改訂
       1.   「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。

ドキュメントを参照: [サイバーセキュリティ経営ガイドライン（METI/経済産業省）](https://www.meti.go.jp/policy/netsecurity/mng_guide.html)

* + - 1.   IoTやAIの活用といった最近の情勢をふまえる
  1.   【目次】
  2.   【Mission1】　知っておきたいサイバー攻撃の知識
     1.    1-1：標的型攻撃による情報流出
     2.    1-2：ランサムウェアを使った詐欺・恐喝
        1.   【囲みコラム】「No More Ransam」　の紹介
     3.    1-3：Webサービスからの個人情報窃取
        1.   【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
     4.    1-4：集中アクセスによるサービス停止
        1.   【囲みコラム】内容更新
     5.    1-5：内部不正による情報漏えいと業務停止
     6.    1-6：Webサイトの改ざん
     7.    1-7：インターネットバンキングの不正送金
        1.   【囲みコラム】不正送金を阻止するには
     8.    1-8：悪意のあるスマホアプリ
        1.   グラフ最新化
        2.   【囲みコラム】スマートフォン決済不正アプリ
     9.    1-9：巧妙・悪質化するワンクリック詐欺
     10.    1-10：Webサービスへの不正ログイン
         1.   【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）
     11.    1-11：公開された脆弱性対策情報の悪用
     12.    1-12：IoT機器を踏み台にした攻撃
         1.   【囲みコラム】IoTとデータ利活用の全体像【総務省】

ドキュメントを参照: <https://www.soumu.go.jp/ict_skill/pdf/ict_skill_1_1.pdf>

* + 1.    1-13：中小企業におけるサイバー攻撃被害の例
       1.   ＜統計データのアップデート＞
          1.   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。
    2.    1-XX：なりすましECサイトの被害と回避策
       1.   改訂箇所：Mission1-12　(P.41)のあとに追加
       2.  事業者サイド
          1.   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】

ドキュメントを参照: [000066952.pdf](https://www.ipa.go.jp/files/000066952.pdf)

* + - * 1.   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】
      1.  利用者サイド
         1.   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.    1-XX：ビジネスメール詐欺の被害と回避策
       1.   改訂箇所：Mission1-12　(P.41)のあとに追加
    2.    【削除】おさらいクイズ
  1.   【Mission2】　すぐやろう！対サイバー攻撃アクション
     1.   改訂のポイント
        1.  冊子版は、敢えて改訂する必要があるか？
        2.   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.    2-1：サイバー攻撃に対して何ができるか
     3.    2-2：OSとソフトウェアのアップデート
        1.   OSサポート状況の注記更新
     4.    2-3：ウイルス対策ソフト・機器の導入
     5.    2-4：定期的なバックアップ
        1.   OneDrive等クラウドストレージの利用
     6.    2-5：パスワードの管理
     7.    2-6：アクセス管理
     8.    2-7：紛失や盗難による情報漏えい対策
     9.    2-8：持ち込み機器対策
        1.   テレワーク等での持ち出し・持ち込み機器対策
     10.    2-9：電子メールの安全利用
     11.    2-10：標的型攻撃メールへの対応
         1.   事例は新規に
     12.    2-11：迷惑メール発信への対応
     13.    2-12：安全なWebサイト利用
         1.   【囲みコラム】詐欺サイトはこれ…内容更新する（NISC,IPAの資料参照）
     14.    2-13：閲覧制限
         1.   【囲みコラム】中小企業の規制は…事例を更新再調査
     15.    【Web版へ】2-14：重要情報の洗い出し
     16.    【Web版へ】2-15：重要情報の保管
     17.    【削除】おさらいクイズ
  2.   【Mission03-A】経営者は事前に何を備えればよいのか【守り】
     1.   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
     2.  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）
     3.  総論
        1.  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
        2.  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
     4.   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。
        1.   改版理由
           1.    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
        2.  組織の社会的責任の認識
        3.     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
        4.     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
           1.  (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
        5.     3-3：経営者に問われる責任
           1.  (1) 経営者などに問われる法的責任
           2.  (2) 関係者や社会に対する責任
           3.    【削除？】【囲みコラム】情報管理が不適切な場合に問われる法律
        6.     【参考：Web版】
           1.   【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】

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - * 1.   【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）】

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - * 1.  【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）】

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

   Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-20.html>

 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

 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

* + - * 1.  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）】

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

 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

 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

 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

 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

 取組６ 情報セキュリティに関する最新動向を収集する

 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

* + - 1.      【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)

ドキュメントを参照: [�Z�L�����e�B�}�C���h���������ƌo�c���[�L���O�O���[�v](https://www.nisc.go.jp/conference/cs/jinzai/wg/index.html)

* + - * 1.  【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

* + - * 1.  【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

* + - * 1.  【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

* + 1.   投資効果（費用対効果）を認識する
       1.     3-4：投資効果（費用対効果）を認識する
          1.  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
          2.  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
    2.   【自社の対策状況把握】自社のIT活用・セキュリティ対策状況を自己診断する
       1.    3-5：ITの活用診断
          1.   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

* + - * 1.  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

* + - * 1.  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

 「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】

ドキュメントを参照: <https://www.nisc.go.jp/conference/cs/jinzai/wg/index.html>

 【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

* + - 1.     3-6：サイバーセキュリティ対策診断
         1.  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

* + - 1.     3-7：情報セキュリティ対策診断
         1.   最新のツール情報を確認する、簡易版等
         2.  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
    1.   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）
       1.  組織を維持するために経営者、 管理者が認識し、 実践すべきことは？
       2.     3-8：業務の効率化、 サービスの維持のために
          1.  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

* + - 1.     【コラム】クラウドサービスのメリットは？
         1.  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
         2.  ・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
      2.     【コラム】クラウドサービス導入の留意点
         1.  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
         2.  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
         3.  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
         4.  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
         5.  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
         6.  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
      3.     【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」
         1.   【担当：中山】
         2.     【参考】DAX20-0402-1 ITロードマップ2018年版【2018年3月NRI】

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-1.html>

* + - * 1.  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
        2.  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
        3.  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
        4.    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)

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-60.html>

 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】

ドキュメントを参照: [01\_01.pdf](https://work-holiday.mhlw.go.jp/material/pdf/category7/01_01.pdf)

 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)

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-60.html>

  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】

ドキュメントを参照: [02shiryou0305.pdf](http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf)

* + - 1.     【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）
         1.   【担当：石井（茂）】
         2.   改訂箇所：Mission4-1( p.134～144)を改訂
         3.  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

* + - 1.     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
         1.  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】

ドキュメントを参照: [20151228002-2.pdf](http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf)

 【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.  （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。

* + - * 1.  （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。

* + - * 1.  （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。

* + - 1.     【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）】
      2.     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
         1.   改訂箇所：Mission3-10 (p.98～109)を改訂
         2.   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。

* + - * 1.   改訂のポイント（経産省発表）

ドキュメントを参照: [20180309\_Hiroshi\_itou.pdf](https://www.jssec.org/dl/20180309_Hiroshi_itou.pdf)

 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

* + - * 1.   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。

 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

 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。

 指示２ サイバーセキュリティリスク管理体制の構築

 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。

 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。

 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

 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

 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

 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

 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

 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

 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

 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

ドキュメントを参照: [security-action](https://www.ipa.go.jp/security/security-action/)

 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

 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。

 ＜情報共有活動における情報提供の記載を強調＞

* + - 1.     【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
         1.    可視化ツールβ版について

ドキュメントを参照: [checktool](https://www.ipa.go.jp/security/economics/checktool/)

 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。

* + - * 1.  ツールのダウンロード

ドキュメントを参照: [000081169.xlsx](https://www.ipa.go.jp/files/000081169.xlsx)

* + - 1.    【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
         1.    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

ドキュメントを参照: <https://www.ipa.go.jp/files/000072309.pdf>

* 1.   【Mission03-B】経営者は事前に何を備えればよいのか【攻め】
     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)
        1.  【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
        2.     Mission3-11 次世代技術を活用したビジネス展開
           1.    【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
           2.   すでにデジタルトランスフォーメーション(デジタル変革)は始まっている

 現状認識

 今は、 IoT、 ビッグデータ、 ロボット、 AI等の技術革新による、 第4次産業革命の入り口にいる

  【参照】IT人材白書2017【2017年4月IPA】

ドキュメントを参照: [about.html](https://www.ipa.go.jp/jinzai/jigyou/about.html)

 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

 デジタルフォーメーション（デジタル変革）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

 第4次産業革命が進むにつれて、 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等の技術を、 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、 それは経営者の責務

 「デジタルトランスフォーメーション」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

 個人として

 自らも「デジタルトランスフォーメーション」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

* + - * 1.   「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）
      1.    【Web版コラム】攻めの姿勢の企業向け
         1.    【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

* + - * 1.      【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】

ドキュメントを参照: [keiei.pdf](http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf)

 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。

* + - * 1.    【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

ドキュメントを参照: [kmy](http://www.nikkeibp.co.jp/atcl/tk/DTrans/kmy/)

 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

* + - * 1.    【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

* + - * 1.    【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】

ドキュメントを参照: [20160705002.html](http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html)

   ■安全なIoTシステムの創出【2016年3月1日NISC】

ドキュメントを参照: [03shiryou05.pdf](http://www.nisc.go.jp/conference/cs/kenkyu/dai03/pdf/03shiryou05.pdf)

   ■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】

ドキュメントを参照: [iot](http://www.jnsa.org/result/iot/)

   ■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】

ドキュメントを参照: [Security\_Guidance\_for\_Early\_Adopters\_of\_the\_Internet\_of\_Things\_J\_160224.pdf](https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf)

 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】

ドキュメントを参照: [20140314004-3.pdf](http://www.meti.go.jp/press/2013/03/20140314004/20140314004-3.pdf)

   ■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】

ドキュメントを参照: [01ryutsu03\_02000073.html](http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html)

 ■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】

ドキュメントを参照: [JIP-ISMS517-10.pdf](https://www.isms.jipdec.or.jp/doc/JIP-ISMS517-10.pdf)

   ISMSクラウドセキュリティ認証の概要（スライド）【JIPDEC】

ドキュメントを参照: [shiryou-1.pdf](https://www.isms.jipdec.or.jp/seminar/cloud/shiryou-1.pdf)

   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】

ドキュメントを参照: [shiryou-2.pdf](https://www.isms.jipdec.or.jp/seminar/cloud/shiryou-2.pdf)

 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】

ドキュメントを参照: [02shiryou0305.pdf](http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf)

 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】

ドキュメントを参照: [tech\_20160520.html](http://www.mri.co.jp/opinion/column/tech/tech_20160520.html)

 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）

ドキュメントを参照: [rel160831b4.pdf](https://www.boj.or.jp/announcements/release_2016/data/rel160831b4.pdf)

 3Dプリンタ

 危険物製造、 著作権侵害

 ・・・

* + - * 1.     【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

* + - 1.     【コラム】DXレポート（ITシステム2025年の崖の克服
         1.    【参考】DAX21\_デジタルトランスフォーメーション（DX）

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX21.html>

* + - 1.     【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
         1.  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
         2.     【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

* + - * 1.     【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】

* + - * 1.     【Web版コラム】５Gセキュリティ対応

  【担当：早出】

* + - * 1.     【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】

* + - * 1.    【Web版コラム】APIセキュリティ
        2.    【Web版コラム】ブロックチェーンにおけるセキュリティ
        3.    【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
        4.     【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

ドキュメントを参照: [世界の電子認証基準が変わる：NIST SP800-63-3を読み解く &ndash; サポート − トラスト・ログイン byGMO【旧SKUID(スクイド)】](https://support.trustlogin.com/hc/ja/articles/115004031154-%E4%B8%96%E7%95%8C%E3%81%AE%E9%9B%BB%E5%AD%90%E8%AA%8D%E8%A8%BC%E5%9F%BA%E6%BA%96%E3%81%8C%E5%A4%89%E3%82%8F%E3%82%8B-NIST-SP800-63-3%E3%82%92%E8%AA%AD%E3%81%BF%E8%A7%A3%E3%81%8F)

 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

* + - * 1.     【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

 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

* + - 1.     【参考】ITの最新トレンド
         1.    【参考】DAX20-0402-3-1\_Society 5.0

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-3-1.html>

* + - * 1.    【参考】DAX10-20 Society5.0に向けた人材育成

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX10-20.html>

* + - * 1.    DAX20-04人工知能に関する基礎知識（まとめ）

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-04.html>

* + - * 1.    DAX20-0401-1人工知能に関する文献のポイント（引用1）

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0401-1.html>

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

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-1.html>

* + - * 1.    DAX20-0402-2 【図解】コレ１枚でわかる最新ITトレンド

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2.html>

* + - * 1.    DAX20-0402-2-0 ITの最新トレンド

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-0.html>

* + - * 1.    DAX20-0402-2-1 IoT

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-1.html>

* + - * 1.    DAX20-0402-2-2 人工知能とロボット

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-2.html>

* + - * 1.    DAX20-0402-2-3 クラウドコンピューティング

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-3.html>

* + - * 1.    DAX20-0402-2-4 モバイルとウェアラブル

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-4.html>

* + - * 1.    DAX20-0402-2-5 ITインフラストラクチャと仮想化

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-5.html>

* + - * 1.    DAX20-0402-2-6 開発と運用

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-6.html>

* + - * 1.  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）
      1.    3-12～14：活用すべき次世代技術要素と活用の留意点
         1.     3-12：IoT、 ビッグデータ, AI、 ロボットの活用

 【削除】中小企業での活用事例「IoTユースケースマップ」

 http://usecase.jmfrri.jp/#/

ドキュメントを参照: [usecase.jmfrri.jp](http://usecase.jmfrri.jp/#/)

 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

* + - * 1.     3-13：IoTが果たす役割と効果

 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】

ドキュメントを参照: [3\_01\_sano.pdf](https://www.iajapan.org/iot/event/2016/pdf/3_01_sano.pdf)

 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

* + - * 1.     3-14：人工知能（AI）が果たす役割と効果

 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】

ドキュメントを参照: [h28.html](http://www.soumu.go.jp/johotsusintokei/whitepaper/h28.html)

   DAX25-20-03【書籍】 AI白書2019\_第3章利用動向

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-03.html>

   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】

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-12.html>

* + - * 1.     【コラム】クラウドサービスのメリットは？
        2.     【コラム】クラウドサービス導入の留意点
        3.     【コラム】クラウドサービスの活用
      1.     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
         1.   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
         2.  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。
         3.  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
         4.  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
         5.  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
      2.     3-16：IoTを活用する一般利用者のための基本ルール
         1.   3-16とコラム併せて大幅に追記する
         2.   【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

* + - * 1.     【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
        2.  【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
        3. 【参考】旧版

 問合せ窓口やサポートがない機器やサービスの購入・利用を控える：インターネットに接続する機器やサービスの問合せ窓口やサポートがない場合、 何か不都合が生じたとしても、 適切に対処すること等が困難になる。 問合せ窓口やサポートがない機器やサービスの購入・利用は行わないようにする。

 初期設定に気をつける・機器を初めて使う際には、 IDやパスワードの設定を適切に行う。 パスワードの設定では、 「機器購入時のパスワードのままとしない」、 「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」等に気をつける。 ・取扱説明書等の手順に従って、 自分でアップデートを実施してみる。

 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状態のまま放置すると、 不正利用される恐れがあることから、 使用しなくなった機器は、 そのまま放置せずに電源を切る。

 機器を手放す時はデータを消す：情報が他の人に漏れることのないよう、 機器を捨てる、 売るなど機器を手放す時は、 事前に情報を削除する。

   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】

ドキュメントを参照: [20160705002.html](http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html)

* + - 1.     【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
         1.   【担当：早出】
         2.      【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

* + - * 1.   【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

* + - 1.      【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
         1.     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
      2.      【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
      3.    【削除】おさらいクイズ
  1.   【Mission04⇒Mission5】もしもマニュアル
     1.   【担当：石井（茂）】
     2.    4-1：緊急事態応用マニュアルの作成
     3.    4-2：基本事項の決定
     4.    4-3：漏えい・流出発生時の対応
     5.    4-4：改ざん・消失・破壊・サービス停止発生時の対応
     6.    4-5：ウイルス感染時の初期対応
     7.    4-6：届け出および相談
     8.    4-7：大規模災害などによる事業中断と事業継続管理
        1.   IT/BCP　範囲とフレームワーク再検討する
           1.  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
     9.    【削除】ワークショップ
  2.   【MISSION5】やってみよう！サイバー攻撃対策シミュレーション
     1.    5-1：サイバー攻撃前夜
     2.    5-2：攻撃発生その瞬間
     3.    5-3：サイバー攻撃直後
     4.    5-4：潜入拡大
     5.    5-5：顧客への被害拡大 取引先への被害拡大
     6.    5-6：サイバー攻撃の発覚
     7.    5-7：原因が判明 ウイルス感染が原因
     8.    5-8：再発防止策の作成
     9.    5-9⇒6-X：復旧回復
     10.    5-10：EMOTET、ランサムウェア対策
  3.   【Mission6】　インフォメーション
     1.    6-1：もしかしてサイバー攻撃？ここに連絡を！
        1.   警視庁、IPA、東京都？、、？
     2.    6-2：やられる前に、しっかり予防を！
        1.  イベントドリブンに！
        2.     「相談・届出先クイックリスト」から抜粋

ドキュメントを参照: <https://bluemoon55.github.io/Presentation_Doc/Cyber/相談・届出先クイックリスト（張り紙用）.pdf>

* + 1.    6-4：情報セキュリティ用語解説
       1.  削除する。
    2.    6-5：セキュリティお役立ちリンク
       1.     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
       2.     【Web版コラム】セキュリティお役立ちリンク【詳細版】
          1.     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
          2.      「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

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02.html>

* + - * 1.      「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

ドキュメントを参照: [CSM\_Guideline\_v2.0.pdf](https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf)

* + - * 1.      「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

ドキュメントを参照: <https://www.soumu.go.jp/main_content/000545372.pdf>

* + - 1.     【Web版コラム】サイバーセキュリティ経営チェックシート
         1.      「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。

* + - 1.    【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）
      2.    【Web版コラム】システム管理者としての基本技術の解説
         1.  【Web版コラム】システム管理者としての基本技術の解説
         2.  （安全・安心ハンドブック（NISC）等を参照）
         3.  ※クレジットカード　PCI/DSS（Payment Card Industry Data Security Standard）
         4.  ※ブロックチェーン技術の応用
         5.  ※Wifiセキュリティ
      3.    【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
         1.     「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】

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02.html>

* + - * 1.     6-X：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

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec03-02.html>

* + - * 1.     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

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX43-01-1.html>

* + - * 1.     DAX20-0402-3 IT人材白書2018

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-3.html>

 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

* + - * 1.     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

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-10.html>

* + - * 1.     DAX25-20-03【書籍】AI白書2019\_第3章利用動向

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-03.html>

* + - * 1.     DAX25-20-05-5-6-3社会実装推進の方向性（テンプレート例）

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-05-5-6-3.html>

* + - * 1.     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）

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX22-01.html>

* + 1.     6-4：中小企業の情報セキュリティ対策ガイドライン【第3版】
       1.    「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
       2.     6-4：情報セキュリティ5カ条
       3.     6-4：情報セキュリティ基本方針
       4.     6-4：新・5分でできる自社診断シート
          1.  【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

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-20.html>

   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/

ドキュメントを参照: [guideline](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/

ドキュメントを参照: [benchmark](https://www.ipa.go.jp/security/benchmark/)

* + - 1.     6-4：情報セキュリティハンドブックひな形（従業員向け）
         1.    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】

ドキュメントを参照: [中小企業の情報セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - 1.    6-4：情報セキュリティポリシーサンプル
      2.    6-4：情報セキュリティ関連規程の明文化
         1.   6-4：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】

ドキュメントを参照: [中小企業の情報セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - 1.    6-4：情報資産台帳の作成
      2.    3-20⇒7-X：リスク分析シート
         1.  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

* + - * 1.  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）

* + - * 1.  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

* + - * 1.  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

* + - * 1.  どんな予防的対策を取るか？
        2.  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）
        3.  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

* + - * 1.  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

* + - * 1.    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】】

ドキュメントを参照: [中小企業の情報セキュリティ対策ガイドライン：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - 1.    6-5：中小企業のためのクラウドサービス安全利用の手引き
    1.    6-6：IT人材育成・人材確保
       1.   【担当：中山】
       2.   【参考】IT人材白書2017,2018,2019
          1.    DAX20-0402-3 IT人材白書2018

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-3.html>

 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

* + - * 1.  【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】
        2.  デジタル化に携わる人材【2019】
        3.  人工知能に携わる人材【2019】
      1.   iコンピテンシ・ディクショナリ(iCD)
         1.  iコンピテンシディクショナリについて

ドキュメントを参照: [i\_competency\_dictionary](https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/)

* + - * 1.  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
      1.   情報処理技術者試験制度
    1.    6-7：情報管理が不適切などの場合の処罰など
       1.    制度・施策
          1.     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）
          2.     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】

ドキュメントを参照: [touroku.html](https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html)

 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

* + - * 1.     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】

ドキュメントを参照: [20190517002.html](https://www.meti.go.jp/press/2019/05/20190517002/20190517002.html)

   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】

ドキュメントを参照: [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を取りまとめました （METI/経済産業省）](https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html)

* + - * 1.     【参考】サイバーインシデント緊急対応企業一覧【JNSA】

ドキュメントを参照: [emergency\_response](https://www.jnsa.org/emergency_response/)

 インシデント緊急対応費用

* + - 1.    関係法令：法律違反の可能性への対応方法の解説
         1.   関連法規の改訂対応
         2.  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
         3.  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
         4.    サイバーセキュリティ基本法
         5.    不正アクセス禁止法
         6.    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）

* + - * 1.    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

* + - * 1.    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

* + - * 1.    知財関連

 著作権法, 産業財産権法, 不正競争防止法,

* + - * 1.    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

* + - * 1.    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

* + - * 1.    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

* + - * 1.    ネットプライバシー（個人攻撃等）
        2.    「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」

ドキュメントを参照: <https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX47-01.html>

* 1.   付録
     1.    付-2：主な参考文献
        1.  本書で引用した文献名一覧
     2.    付-3：用語解説インデックス
        1.  索引