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

1. Sec03-01
2. 改版履歴
   1. 2020年5月14日　加筆訂正
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. 【参考】「中小企業向けサイバーセキュリティ対策の極意」を引用

ドキュメントを参照: [guidebook](http://www.sangyo-rodo.metro.tokyo.jp/chushou/shoko/cyber/jigyou/guidebook/)

* + 1. 東京都が中小企業の経営者向けに、 サーバーセキュリティ対策として認識すべきことをイラストを交えてまとめたもの
    2. 経営者が認識すべきことであるが、 それを認識させるためにも、 担当者が理解していることが重要

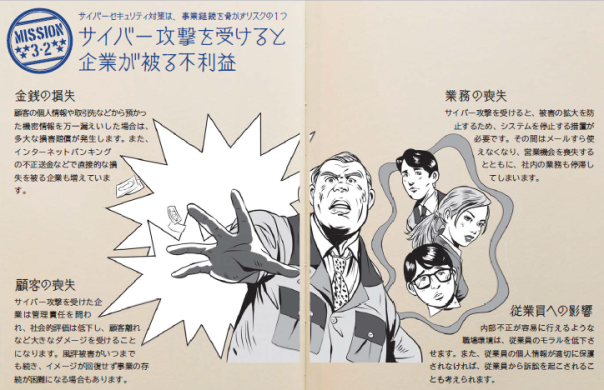
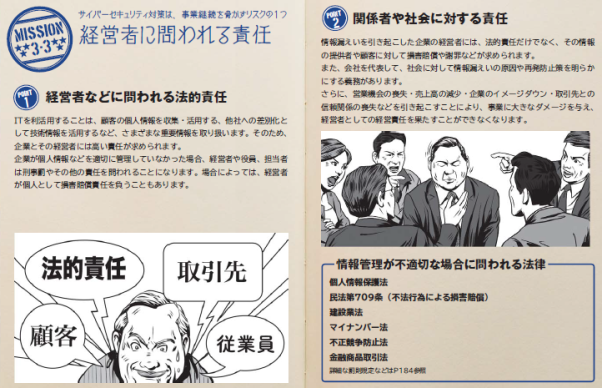
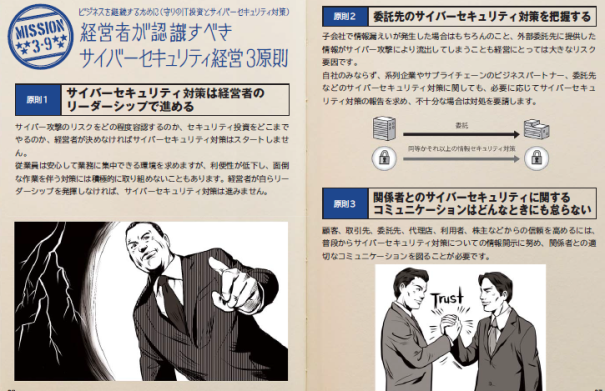
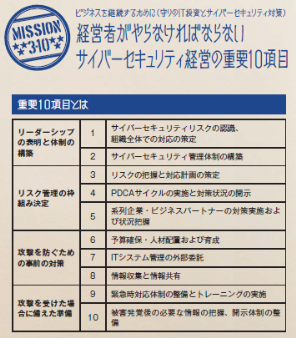
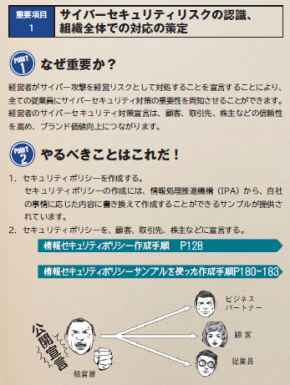
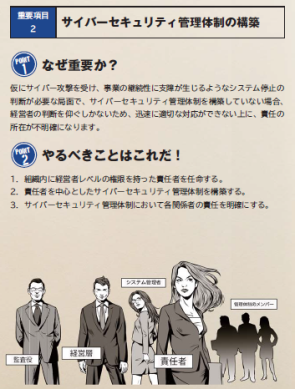
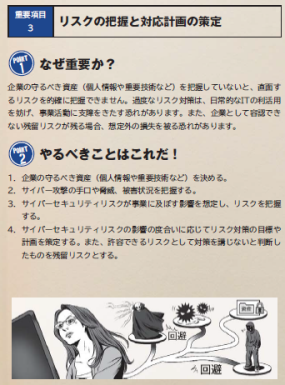
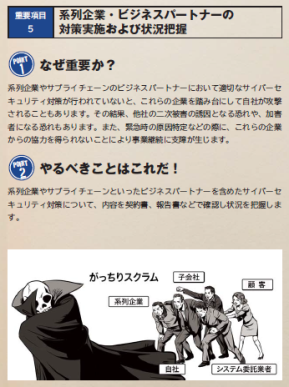
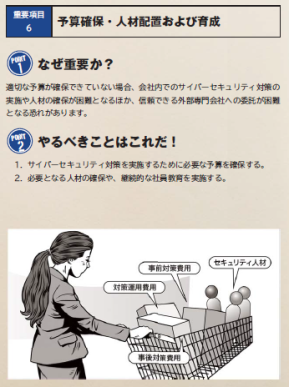
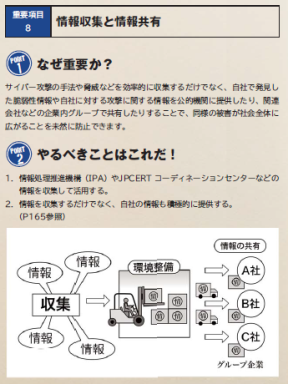
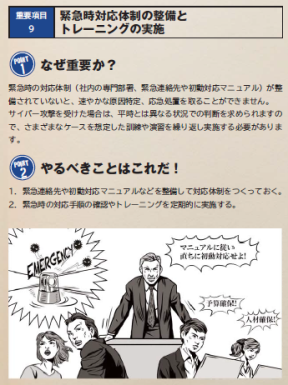
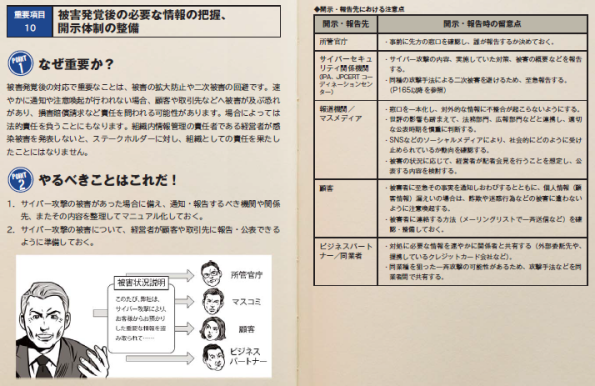
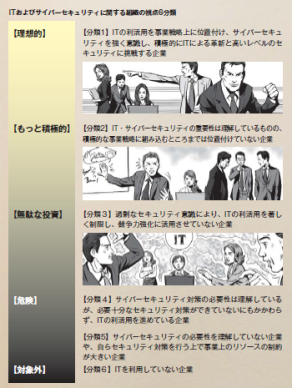
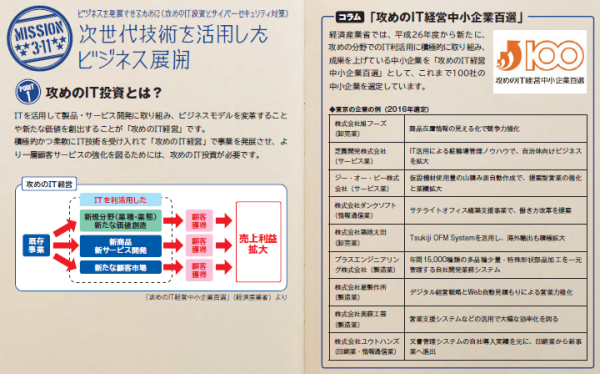
1. 【参考】企業経営のためのサイバーセキュリティの考え方の策定について【NISC】

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

* 1. 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－
     1. グローバルな競争環境の変化
     2. 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
     3. 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
     4. ⇒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
  2. 基本的な考え方
     1. 二つの基本的認識
        1. ＜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. ＜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
     2. 三つの留意事項
        1. ＜①情報発信による社会的評価の向上＞
           1. 「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。
           2. 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. ＜②リスクの一項目としてのサイバーセキュリティ＞
           1. 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。
           2. 経営層のリーダーシップが必要。
        3. ＜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＞
           1. 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。
           2. 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。

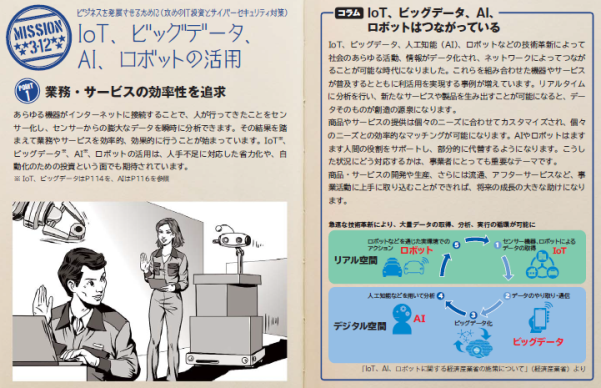
1. サイバーセキュリティ対策として考慮すべき事項
   1. サイバーセキュリティ対策は、 事業継続を脅かすリスクの１つ。
      1. わかっていますか？
         1. Subtopic  
            
         2. 情報セキュリティ対策は、 経営に大きな影響を与えます！
         3. 経営者が法的・道義的責任を問われます！
         4. 組織として対策するために、 担当者への指示が必要です！
            1. 中小企業の情報セキュリティ対策ガイドライン（第2.1版）【2017年5月10日IPA】

ドキュメントを参照: [000055520.pdf](http://www.ipa.go.jp/files/000055520.pdf)

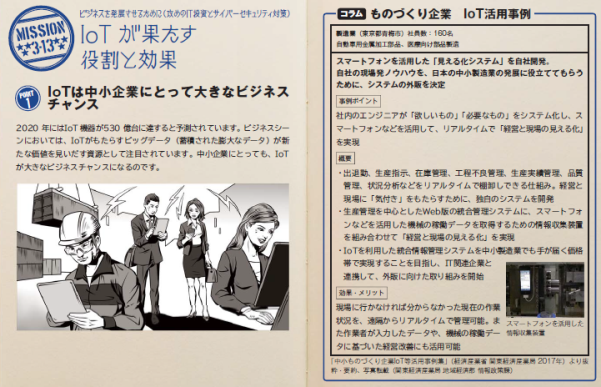
* + - 1. セキュリティ侵害を受ける70～80%が人為的なミス、 故意
      2. サイバーセキュリティ対策の中で最もコストがかかるのが技術的対策。 しかし全てのリスクに対して技術的対策をすることは困難。 悪意があれば技術的な対策はすり抜けられる
      3. セキュリティー被害を受けた場合、 その被害に対し会社が被る損害の可能性が高い順に投資をすることが重要。
      4. また、 システムを入れる際に、 セキュリティーも同時に入れるなど、 ITとセキュリティー対策を一緒にすることも大切である。
      5. 更に、 経営者を含め、 社員全員に対し、 セキュリティーポ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。
    1. 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. Subtopic  
          
       2. (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
    2. 経営者が負う責任
       1. Subtopic  
          
       2. (1) 経営者などに問われる法的責任
          1. ・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
       3. (2) 関係者や社会に対する責任
          1. ・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
  1. 【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. Subtopic  
        
     2. 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。
     3. （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
        1. 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。
        2. 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。
        3. 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。
     4. （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
        1. 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。
        2. 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。
     5. （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
        1. 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。
        2. 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。
        3. 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。
  2. 【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. Subtopic  
        
     2. 経営者は、 CISO等に対して、 以下の１０項目を指示し、 着実に実施させることが必要である。
     3. （１）サイバーセキュリティリスクの認識、 組織全体での対応の策定
        1. Subtopic  
           
        2. 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）を策定していますか？
        3. 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。
        4. 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。
     4. （２）サイバーセキュリティリスク管理体制の構築
        1. Subtopic  
           
        2. サイバーセキュリティ対策を行うため、 経営者とセキュリティ担当者をつなぐ仲介者としてのCISO等からなる 適切なサイバーセキュリティリスクの管理体制の構築は出来ていますか？
        3. 各関係者の責任は明確になっていますか？
        4. また、 防犯対策など組織内のその他のリスク管理体制と整合をとらせていますか？
     5. （３）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
        1. Subtopic  
           
        2. サイバー攻撃の脅威に対し、 経営戦略の観点から、 守るべき資産を特定させた上で、 社内ネットワークの問題点などのサイバーセキュリティリスクを把握させていますか？
        3. その上で、 暗号化やネットワークの分離など複数のサイバーセキュリティ対策を組み合わせた多層防御など、 リスクに応じた対策の目標と計画を策定させていますか？
        4. また、 サイバー保険の活用や守るべき資産について専門企業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ていますか？
     6. （４）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
        1. Subtopic  
           
        2. 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として実施するフレームワークを構築させていますか？
        3. その中で、 監査（または自己点検）の実施により、 定期的に経営者に対策状況を報告させた上で、 必要な場合には、 改善のための指示をしていますか？
        4. また、 ステークホルダーからの信頼性を高めるため、 対策状況について、 適切な開示をさせていますか？
        5. 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。
     7. （５）系列企業や、 サプライチェーンのビジネスパートナー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
        1. Subtopic  
           
        2. 自社のサイバーセキュリティが確保されるためには、 系列企業やサプライチェーンのビジネスパートナーを含めてサイバーセキュリティ対策が適切に行われていることが重要。 このため、 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、 系列企業やサプライチェーンのビジネスパートナーを含めた運用をさせていますか？
     8. （６）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
        1. Subtopic  
           
        2. 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は出来ていますか？また、 サイバーセキュリティ人材の育成や適切な処遇をさせていますか？
        3. 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。
     9. （７）ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
        1. Subtopic  
           
        2. サイバーセキュリティ対策を効率的かつ着実に実施するため、 リスクの程度や自組織の技術力などの実態を踏まえ、 ITシステムの管理等について、 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ていますか？また、 ITシステム管理を外部委託する場合、 当該委託先へのサイバー攻撃等も想定し、 当該委託先のサイバーセキュリティの確保をさせていますか？
        3. 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。
     10. （８）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のための環境整備
         1. Subtopic  
            
         2. 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の参加と、 入手した情報を有効活用するための環境整備をさせていますか？
         3. 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。
     11. （９）緊急時の対応体制（緊急連絡先や初動対応マニュアル、 CSIRT）の整備、 定期的かつ実践的な演習の実施
         1. Subtopic  
            
         2. 適切な初動対応により、 被害拡大防止を図るため、 迅速に影響範囲や損害を特定し、 ITシステムを正常化する手順を含む初動対応マニュアル策定や組織内のCSIRT構築など対応体制の整備をさせていますか？また、 定期的かつ実践的な演習を実施させていますか？
         3. 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
     12. （１０）被害発覚後の通知先や開示が必要な情報の把握、 経営者による説明のための準備
         1. Subtopic  
            
         2. 外部に対して迅速な対応を行うため、 被害の発覚後の通知先や開示が必要な情報について把握させていますか？また、 情報開示の際、 経営者が組織の内外への説明が出来る体制の整備をさせていますか？
  3. 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
     1. Subtopic  
        
     2. 「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
        1. 【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】
     3. 【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
        1. （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）
        2. 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
        3. 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
     4. 【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
        1. （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）
        2. 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
     5. 【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
        1. 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
        2. 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
        3. 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
        4. 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
        5. 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
        6. 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。
        7. 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
        8. 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
     6. 【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
        1. 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
        2. （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）
        3. 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
        4. 情報セキュリティポリシーの策定と実践、 定期的な監査
        5. 創造力、 発想力のある人材の育成
        6. ITスキルと知識を持った人材の育成が必要
     7. 【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
        1. （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）
        2. 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
     8. 【対象外】ITを利用していない企業
        1. 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？？
        2. 情報セキュリティ対策は必要
  4. 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. Subtopic  
        
     2. 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？
     3. 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。
     4. 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。
     5. 次世代技術を活用したビジネス展開
     6. 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
        1. 現状認識
           1. 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)

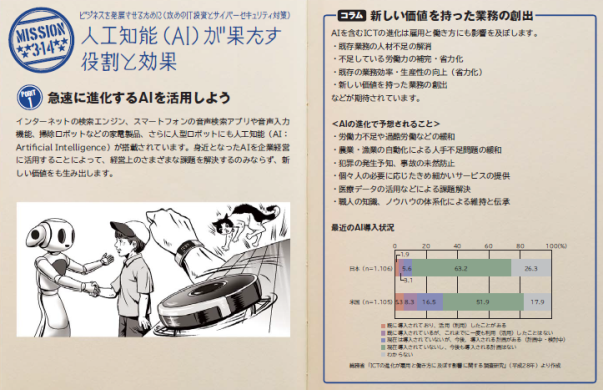
* + - * 1. あらゆるものがインターネットに接続するIoTの広がり、 あらゆる情報がビッグデータとして活用され、 AI技術により、 様々な分野で定型的な業務はもとより、 人海戦術では不可能だった業務まで、 AI技術を適用したサービス、 ロボットの適用が始まっている
        2. 既存のビジネスや業務に新技術を取り入れるだけでなく、 ビジネスモデルを変え、 経済活用のみならず、 個人の生活や社会構造まで影響が及ぶ
        3. デジタルフォーメーション（デジタル変革）とは、 あらゆる情報がデジタル化され、 IT技術によって、 社会や産業、 企業、 人のあり方や働き方が変わっていくこと
        4. 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
        5. 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
        6. 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
        7. 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
    1. IoT、 ビッグデータ, AI、 ロボットの活用
       1. Subtopic  
          
       2. 中小企業での活用事例「IoTユースケースマップ」
          1. http://usecase.jmfrri.jp/#/

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

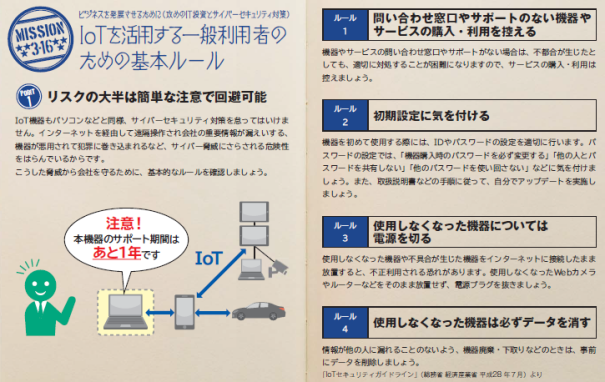
* + - 1. 深刻な人手不足に対応した、 省力化、 自動化のための投資
      2. 人が行ってきたことをセンサー化し、 センサーからの膨大な情報を機械的に分析することにより、 今までできなかった高度な分析と、 その結果を踏まえて業務やサービスを効率的、 効果的に行える
    1. IoTが果たす役割と効果
       1. Subtopic  
          
       2. 中小企業にとって、 経費削減と人材確保は大きな課題
       3. 各種センサーによる自動測定や電子タグ等（RFID）を人やモノに貼り動きの情報を計測し収集することにより、 リアルタイムで状況が把握できる
       4. 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
       5. IoT、 ビッグデータ、 AI、 ロボットは繋がっている
          1. 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】

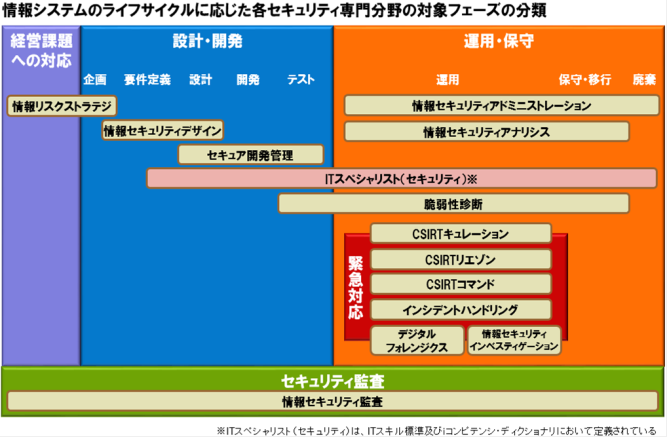
ドキュメントを参照: [3\_01\_sano.pdf](https://www.iajapan.org/iot/event/2016/pdf/3_01_sano.pdf)

* + - * 1. 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. 人工知能（AI）が果たす役割と効果
       1. Subtopic  
          
       2. 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。
       3. 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。
          1. 【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)

* + 1. 活用する際のサイバーセキュリティ上の留意点
       1. Subtopic  
          
       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. IoTを活用する一般利用者のためのルール
       1. Subtopic  
          
       2. •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。
       3. •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。
       4. •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。
       5. •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。
          1. 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. サイバーセキュリティ対策に必要なスキルと知識
   1. 情報システムのライフサイクルに応じた各セキュリティ専門分野の対象フェーズの分類
      1. Subtopic  
         
   2. セキュリティ領域のスキル標準「ITSS+」【2017年6月5日】
      1. 専門的なセキュリティ業務の役割の観点により、 経営課題への対応から設計・開発、 運用・保守、 セキュリティ監査における13の専門分野を具体化
      2. 新たに創設された国家資格「情報処理安全確保支援士(登録セキスペ)」が想定する業務を包含
   3. 【閉じる】専門分野【詳細】
      1. 情報リスクストラテジ
         1. 自組織または受託先における業務遂行の妨げとなる情報リスクを認識し、 その影響を抑制するための、 組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定等を推進する。 自組織または受託先内の情報セキュリティ対策関連業務全体を俯瞰し、 アウトソース等を含むリソース配分の判断・決定を行う。
      2. 情報セキュリティデザイン
         1. 「セキュリティバイデザイン」の観点から情報システムのセキュリティを担保するためのアーキテクチャや、 ポリシーの設計を行うとともに、 これを実現するために必要な組織、ルール、プロセス等の整備・構築を支援する。
      3. セキュア開発管理
         1. 情報システムや製品に関するリスク対応の観点に基づき、 機能安全を含む情報セキュリティの側面から、 企画・開発・製造・保守などにわたる情報セキュリティライフサイクルを統括し、 対策の実施に関する責任をもつ。
      4. 脆弱性診断
         1. ネットワーク、 OS、 ミドルウェア、 アプリケーションがセキュアプログラミングされているかどうかの検査を行い、 診断結果の評価を行う。
      5. 情報セキュリティ
         1. 組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに、 対策の立案や実施（指示・統括）、 その見直し等を通じて、 自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。 また、 利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。
      6. 情報セキュリティアドミニストレーション
         1. 組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに、 対策の立案や実施（指示・統括）、 その見直し等を通じて、 自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。 また、 利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。
      7. 情報セキュリティアナリシス
         1. 情報セキュリティ対策の現状に関するアセスメントを実施し、 あるべき姿とのギャップ分析をもとにリスクを評価した上で、 自組織または受託先の事業計画に合わせて導入すべきソリューションを検討する。 導入されたソリューションの有効性を確認し、 改善計画に反映する。
      8. CSIRTキュレーション
         1. 情報セキュリティインシデントへの対策検討を目的として、 セキュリティイベント、 脅威や脆弱性情報、 攻撃者のプロファイル、 国際情勢、 メディア動向等に関する情報を収集し、 自組織または受託先に適用すべきかの選定を行う。
      9. CSIRTリエゾン
         1. 自組織外の関係機関、 自組織内の法務、 渉外、 IT部門、 広報、 各事業部等との連絡窓口となり、 情報セキュリティインシデントに係る情報連携及び情報発信を行う。 必要に応じてIT部門とCSIRTの間での調整の役割を担う。
      10. CSIRTコマンド
          1. 自組織で起きている情報セキュリティインシデントの全体統制を行うとともに、 事象に対する対応における優先順位を決定する。 重大なインシデントに関してはCISOや経営層との情報連携を行う。 また、 CISOや経営者が意思決定する際の支援を行う。
      11. インシデントハンドリング
          1. 自組織または受託先におけるセキュリティインシデント発生直後の初動対応 （被害拡大防止策の実施）や被害からの復旧に関する処理を行う。 セキュリティベンダーに処理を委託している場合には指示を出して連携する。 情報セキュリティインシデントへの対応状況を管理し、 CSIRTコマンドのタスクを担当する者へ報告する。
      12. デジタルフォレンジクス
          1. 悪意をもつ者による情報システムやネットワークにを対象とした活動の証拠保全を行うとともに、 消されたデータを復元したり、 痕跡を追跡したりするためのシステム的な鑑識、 精密検査、 解析、 報告を行う。
      13. 情報セキュリティインベスティゲーション
          1. 情報セキュリティインシデントを対象として、 外部からの犯罪、 内部犯罪を捜査する。 犯罪行為に関する動機の確認や証拠の確保、 次に起こる事象の推測などを詰めながら論理的に捜査対象の絞り込みを行う。
      14. 情報セキュリティ監査
          1. 情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、 リスクアセスメントに基づく適切な管理策の整備、 運用状況について、 基準に従って検証又は評価し、 もって保証を与えあるいは助言を行う。