## 概要

* 1. 改版履歴
     1. 2021年5月31日\_候補大幅追加
     2. 2021年5月25日\_仕掛かり分チェック
     3. 2021年5月13日\_全編にわたってリストアップ
  2. アイコン凡例
     1.  Web版に追補する候補
     2.  執筆中、仕掛かり中
     3.  冊子体追記候補
     4.    担当

## **Mission1**

* 1.  1-3：Webサービスからの個人情報窃取
     1.   【Web版Appendix】I本人に認証サービス（３Dセキュア）クレジットカードの認証方式を追加
        +  【Web版Appendｘ引用先】割賦販売法の改定とクレジットカードのセキュリティ「改正割賦販売法について」PD経済産業省　商取引監督課２０１８年４月
        +  https://www.caa.go.jp/policies/policy/local\_cooperation/local\_consumer\_administration/meeting\_001/pdf/meeting\_001\_180419\_0017.pdf
  2.  1-4：集中アクセスによるサービス停止
     1.   【Web版Appendix】集中アクセスによるサービス停止　「コラム」中小企業DDos攻撃の被害事例
        +  事例ー＞DDosの攻撃内容の説明に大規模で巧妙なDDos攻撃の増加傾向に懸念アカマイ、短期間で2度の大規模DDos攻撃を緩和事例を分かりやすく追加Akamai (アカマイ) Web セキュリテ
        +  https://www.lac.co.jp/service/product/akamai.html
  3.  1-6：Webサイトの改ざん
     1.   【Web版Update】ECサイトの脆弱性をついた事案も発生
        +   ★【Web版Appendix】脆弱性診断システム適用範囲について、脆弱性診断Tool
        +   【Web版Appendix】Metasploit Framework
        +   【Web版Appendix】OWASP ZAP
     2.   ★【Web版Appendix】共通脆弱性識別子CVE(Common Vulnerabilities and Exposures)
  4.  1-7:インターネットバンキングの不正送金
     1.   【Web版Appendix】詐欺サイトもSSL化が当たり前　フィツシング詐欺被害回避の方法
        +  ラック株式会社
  5.  1-10：Webサービスへの不正ログイン
     1.   【Web版Appendix】IDと認証セキュリティ
  6.  1-12：IoT機器を踏み台にした攻撃
     1.  【Web版Appendix】NICT「NOTICE」の実証事例の結果
  7.  1-13：中小企業におけるサイバー攻撃被害の例
     1.   【Web版Appendix】POINT２中小企業を含んだサプライチェーンが狙われている
        +  ＜ーサプライチェーンセキュリティの必要性を追加又は主要な参考文書引用先を例示
        +  サプライチェーンセキュリティの必要性
        +  サイバーセキュリティ経営ガイドラインの改定ポイント 経済産業省商務情報政策局サイバーセキュリティ課
        +  https://www.meti.go.jp/policy/netsecurity/downloadfiles/overview.pdf
        +  IPA　NIST関連文書 https://www.ipa.go.jp/security/publications/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
          -  Protecting Controlled Unclassified Information in Nonfederal Systems
     2.   【Web版Appendix】サプライチェーンの情報セキュリティマネジメント IS02703, NIST\_SP800-61（サプライチェーンマネージメント）
     3.  【Web版Appendix】★サプライチェーンコンソシアムSC3の概要（IPA、経済産業省）
  8.  1-14：ビジネスメール詐欺（BEC)に注意
     1.   【Web版Appendix】トレンドマイクロ　「ビジネスメール詐欺の被害に遭わないために、知って知っておくべき兆候をBEC被害の事例（具体的）に追加
        +  https://blog.trendmicro.co.jp/archives/tag/bec
     2.   【Web版Appendix】ビジネスメール詐欺の被害」と回避策
        +  法人間の外国送金の資金をだまし取る詐欺にご注意追加　(BEC (Business E-mail Compromise) / foreign remittance fraud）
          -  全国社団法人全国銀行協会

 https://www.zenginkyo.or.jp/topic/detail/nid/3561/

* + - * +  ・発生している事案
        +  ・法人に対する対策事例

## **Mission2**

* 1.  2-8：テレワーク等での持ち出し・持ち込み機器対策
     1.   【Web版Appendix】VPNの脆弱性攻撃増加　テレワーク認証情報搾取
  2.  2-9：電子メールの安全利用
     1.   【Web版Appendix】＜電子メールのなりすまし対策＞
        +  SPF送信電子メール認証のイメージ図を追加する
  3.  2-10：標的型攻撃メールへの対応
     1.   【Web版Appendix】巧妙な標的型攻撃メール事例
     2.   【Web版Appendix】Emotetからの攻撃も含まれる事例（JPCERT/CC）
     3.   【Web版Appendix】IceIDウイルスダンローダ
     4.   【Web版Appendix】★EDP（エンドポイントセキュリティ）関連調査
     5.   【Web版Appendix】★TRUSTeマーク認証について調査概要
        +  信頼という名の個人情報認証 TRUSTe（トラストイー）は、信頼(TRUST)できる事業者選びの指標

## **Mission3**

* 1.  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
     1.   【Web版Appendix】MDM（Mobile Device Management）
        +  ビジネスで使用するスマートフォンなどのモバイルデバイスの、システム設定などを統合的・効率的に管理する手法。
  2.  3-3：経営者に問われる責任
     1.   【Web版Appendix】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)
  3.  3-5：ITの活用診断
     1.   【Web版Appendix】視点6分類
  4.  3-6：サイバーセキュリティ対策診断
     1.   【Web版Appendix】費用対効果
     2.   【Web版Appendix】セキュリティ診断Toolの紹介（ペネトレーションテストを含む）
  5.  3-8：業務の効率化、 サービスの維持のために
     1.  【Web版Appendix】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
     2.   【Web版Appendix】生産性向上のための「デジタル・ワークプレイス」
     3.  【Web版Appendix】テレワークではじめる働き方改革
     4.   【Web版Appendix】テレワークでのクラウドサービス活用等（総務省テレワークガイド）
     5.   【Web版Appendix】 Web会議サービスを使用する際のセキュリティ注意事項
        +  クラウドIPA　情報セキュリティ対策
        +  https://www.ipa.go.jp/security/announce/webmeeting.html
  6.  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.  【Web版Appendix】経営者として取り組むべき「重要7項目の取組」
  7.  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.  【Web版Appendix】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】
     2.  【Web版Appendix】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の活用【2021年夏アップデート予定】
     3.  【Web版Appendix】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
  8.  3-11：次世代技術を活用したビジネス展開
     1.   【Web版Appendix】【解説】DX推進はビジネス飛躍のチャンス
     2.   【Web版Appendix】「デジタルアーキテクチャ・デザインセンター（DADC）」の活動
     3.   【Web版Appendix】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
     4.   【Web版Appendix】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】
     5.   【Web版Appendix】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
     6.   【Web版Appendix】DXレポート（ITシステム2025年の崖の克服
     7.   【Web版Appendix】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
     8.   【Web版Appendix】【参考情報】ITの最新トレンド
     9.   【Web版Appendix】IoTや5Gを活用した新規セキュリティビジネスの紹介
  9.  3-12：IoT、 ビッグデータ, AI、 ロボットの活用
     1.   【Web版Appendix】攻めのIT投資対応、Society5.0時代に必要なセキュリティ対策【要素別】
        +  【Web版Appendix】IoT関連セキュリティ対応
        +  【Web版Appendix】クラウドサービスとセキュリティ
        +  【Web版Appendix】５Gセキュリティ対応
        +  【Web版Appendix】BYODセキュリティ対応
  10.  3-13：IoTが果たす役割と効果
  11.  3-14：人工知能（AI）が果たす役割と効果
      1.   【Web版Appendix】「AI白書」の要点
  12.  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.  【Web版Appendix】機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き【2021年4月20日METI】
      2.   【Web版Appendix】CMS認証　IEC63443認証　ISO 国際規格（ISO/IEC JTC 1）に提案し開発中
         +  ISO/IEC 27030（ITセキュリティ） 2018/4－
         +  • ISO/IEC 30147（IoT）
  13.  3-16：IoTを活用する一般利用者のための基本ルール
      1.   【Web版Appendix】IPA 安全安心なIoT実現に向けた重要ポイント
         +  ～「つながる世界の開発指針」と関連ガイド活用のススメ
         +  https://www.ipa.go.jp/files/000073864.pdf
  14.   【Web版Appendix】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.  【Web版Appendix】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
      2.  【Web版Appendix】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
      3.  【Web版Appendix】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
         +  【Web版Appendix】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
      4.  【Web版Appendix】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
      5.   【Web版Appendix】NIST SP800-53とNISTサイバ－セキュリティフレームワークの概要と利用方法
      6.   【Web版Appendix】スマートホームの安心・安全に向けたサイバー・フジカル・セキュリティ対策ガイドライン　経済産業省
      7.   【Web版Appendix】★サプライチェーンサイバーセキュリティについてISO27036をベースにその具体的 コントロールの導入と評価方法を中小企業向け導入対策
      8.   【Web版Appendix】★サプライチェーンコンソシアムSC3の概要（IPA、経済産業省）
      9.   【Web版Appendix】★IoT活用企業におけるプライバシー保護に関する考慮
         +  一般社団法人 重要生活機器連携セキュリティ協議会（Connected Consumer Device Security Council）

## **Mission4**

* 1.  4-7：大規模災害などによる事業中断と事業継続管理
     1.   【Web版Appendix】IT/BCPの範囲とフレームワーク
     2.   【Web版Appendix】ISO/IEC2203 事業継続

## **Mission5**

## **Information6**

* 1.  6-2：その他の主な報告・連絡・相談窓口等
     1.  【Web版Appendix】サイバーセキュリティ報告・連絡・相談窓口一覧【詳細資料】
  2.     6-3：セキュリティお役立ち情報リンク
     1.    【Web版Appendix】次世代ITおよびサイバーセキュリティ対策に関する文献、サイト一覧【詳細資料】
        +  ※内容を充実させ、最新情報として都度更新
        +  サイバーセキュリティ関連の基本文書（法律・基本計画・各種方針等）
        +  サイバーセキュリティ関連の各種白書・年次報告書類
        +  各実施事項の参考情報
          -  全般
          -  DX 関連
          -  IoTセキュリティ関連
          -  テレワーク関連
          -  AI関連
          -  インシデント対応関連
          -  個人情報保護関連

 GDPR

 SP 800-53 Rev.5 情報システムおよび組織のセキュリティおよびプライバシー管理

* + - * +  人材育成関連

 【追加】デジタルリテラシー領域「Di-Lite」

* + - * + 法令・規則
      *  各実施関連機関
        +  【追加】「デジタルリテラシー協議会」
    1.   【Web版Appendix】一般ユーザ向け：次世代ITおよびサイバーセキュリティ対策に関する啓発用資料【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
       -  ECサイト利用
       -  電子メール
       -  ・・・
    2.   【Web版Appendix】近い将来のITの利活用と必要な人材育成に資する資料
  1.  6-4：中小企業の情報セキュリティ対策ガイドライン
     1.    【Web版Appendix】6-4\_Appendix\_中小企業の情報セキュリティ対策ガイドラインの概要【構成】
     2.  できるところから始める
     3.  組織的な取り組みを開始する
        +  【Web版Appendix】6-4-X\_Appendix\_【付録4】情報セキュリティハンドブック（ひな型）の使い方（ポイント）
     4.  本格的に取り組む
        +   【Web版Appendix】6-4-X\_Appendix\_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】
        +     【Web版Appendix】6-4-1\_Appendix\_情報資産台帳の作成と詳細リスク分析
        +     【Web版Appendix】6-4-1\_Appendix\_情報セキュリティ関連規程に記載すべき項目の概要
     5.  より強固にするための方策
        +   【Web版Appendix】ACTION4 対策をより強化する
          -  ３クラウドサービスの情報セキュリティセキュリティ対策３段階で検討しましょう。、＜ー３段階の説明を追加する
        +   【Web版Appendix】ISMAP　情報セキュリティ監査ガイドライン　経済産業省
  2.  6-5：中小企業のためのクラウドサービス安全利用手引き
     1.   【Web版Appendix】クラウドセキュリティ監視Tool　CASBYの活用
     2.   【Web版Appendix】ゼロトラストセキュリティでは、新たな「境界」の考え方であるSDP（Software Defined Perimeter）展開されている
     3.   【Web版Appendix】「ゼロトラストモデル」とは―クラウド時代の次世代セキュリティモデル
  3.  6-6：IT活用に不可欠なIT人材の確保と育成
     1.    【Web版Appendix】6-6-1\_Appendix\_次世代技術を活用したビジネス展開のためのデジタルリテラシーの習得
        +  デジタルリテラシー領域「Di-Lite」
          -  マインド

デジタルに取り組むスタンス、マインド

* + - * +  知識体系

デジタル活用分野/適用事例

デジタル知識

* + - * +  スキル

使う、作る/なおす

より上手に使う/広める

発想する/活用方針を示す

新たに作る/教える

* + - *  「Di-Lite」のベースとなるカリキュラム
        +  ITパスポート試験（IPA実施)
        +  データサイエンティスト検定リテラシーレベル（JDLA実施)
        +  G検定（JDLA実施)
      *    【Web版Appendix】6-6-2\_Appendix\_近い将来のITの利活用と必要な人材（「サイバーセキュリティ研究開発戦略」の要約）
    1.   6-6-10\_Appendix\_iコンピテンシ・ディクショナリ(iCD)
  1.  6-7：情報セキュリティ関連法令
     1.   【Web版Appendix】プライバシイ保護法の国際化とCBPR認証（Cross　Border Privacy Rule
     2.   【Web版Appendix】改正民法と瑕疵担保期間の延長
     3.   【Web版Appendix】個人保護保護法の改正（デジタル庁）
  2.  6-X：デジタルリテラシー
     1.   【Web版Appendix】6-X-X\_Appendix\_組織人として持つべきデジタルリテラシー【スキル項目と啓発資料】
        +  経営者として
        +  システム管理者として
        +  従業員として
  3.  6-X：個人情報保護・プライバシーへの対応
     1.   【Web版Appendix】プライバシイバイデザイン　７原則　DX企業のプライバシ－ガバナンスガイド　経済産業省
     2.   【Web版Appendix】改正個人情報保護のポイント
        +  ・利用停止
        +  ・漏えい等報告、本人通知
        +  ・不適正利用の禁止
        +  ・認定団体制度の充実
        +  ・公表事項等
        +  ・仮名加工情報
        +  ・個人関連情報
        +  ・越境移転
  4.   ６－X：クラウドサービスを利用する際の情報セキュリティ対策調査
     1.   【Web版Appendix】1）ISMSクラウドセキュリティ認証(ISO27001/ISO27017) 2）CSマーク 3）CSA STAR認証(CSA Security) 4）StarAudit Certification 5）FedRAMP 6）SOC2,SOC2＋
     2.   【Web版Appendix】★クラウドアクセス可視化・制御ソリューション CASB(Cloud Access Security Broker)
     3.   【Web版Appendix】★ISMSクラウドセキュリティ認証(ISO27001/ISO27017
     4.   【Web版Appendix】★JNSA「緊急事態宣言解除後のセキュリティ・チェックリスト解説書」 日本セキュリティネットワーク協会
     5.   【Web版Appendix】★eKYCとは
        +  KYCをオンライン上で実現するための仕組みです。本人確認を電子的に行うことから、eKYC（electronic Know Your Customer）と略して呼ばれます。
        +  2018年に改正された「犯罪による収益の移転防止に関する法律」により、「オンラインで完結する自然人の本人特定事項の確認方法」として、以下の4つの方法が認められるようになりました。
        +  「本人確認書類の画像」と「本人の容貌の画像」の送信
        +  「本人確認書類のICチップ情報」と「本人の容貌の画像」の送信
        +  「本人確認書類の画像もしくは本人確認書類のICチップ情報」の送信と事業者による「銀行などへの顧客情報の照会」
        +  「本人確認書類の画像もしくは本人確認書類のICチップ情報」と「事業者による顧客名義口座への少額振り込みと、そのインターネットバンキング記録の画像」の送信
     6.   【Web版Appendix】★FIDO2認証が主要な認証方式として有効化
        +  ・多要素認証機能のクラウドサービスを開始 Akamai 社 多要素認証機能のクラウドサービス「Akamai MFA」の国内提供を開始したと発表しました。 FIDO2（Fast IDentity Online）に準拠し、スマートフォンの専用アプリで利用できるようにしています。
     7.   【Web版Appendix】★海外の主要規格との対応関係
        +  NIST Cybersecurity Framework のサブカテゴリと「サイバー・フィジカル・セキュリティ対策フレー ムワーク」対応表のマッピング
     8.   【Web版Appendix】★MITRE ATT ＆CK　セキュリティ攻撃パターン分類の利用方法
     9.   【Web版Appendix】★OWASP（The Open Web Application Security Project）とは、
        +  Webアプ有名な取り組みの1つとして「OWASP Top 10」の 公表