## **国等の基本文書、白書、解説文書**

* 1.   基本文書
     1. （法律・基本計画・各種方針等）
     2. 経済財政運営と改革の基本方針（骨太方針）【閣議決定】
        + 経済財政運営と改革の基本方針2021【経済財政諮問会議にて策定中】
        + https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/2020/decision0717.html
     3. IT総合戦略室\_デジタル・ガバメント実行計画【内閣府】
        + https://cio.go.jp/guides
        + デジタル・ガバメント推進標準ガイドライン解説書【内閣府IT総合戦略室】
          - https://cio.go.jp/guides#kaisetusyo
        + デジタル・ガバメント推進標準ガイドライン実践ガイドブック【内閣府IT総合戦略室】
          - https://cio.go.jp/guides#guidebook
     4. デジタル社会形成基本法【内閣府】
        + https://cio.go.jp/node/2734
  2.   基本文書（サイバーセキュリティ関連）
     1. （法律・基本計画・各種方針等）
     2. サイバーセキュリティ基本法
        + https://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/basic/legal/11.html
     3. サイバーセキュリティ戦略【NISC】
        + https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf
     4. サイバーセキュリティ2020【NISC】
        + https://www.nisc.go.jp/active/kihon/pdf/cs2020.pdf
     5. セキュリティ関連NIST文書【IPA】
        + https://www.ipa.go.jp/security/publications/nist/index.html
     6. 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】
          - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf
          - https://www.ipa.go.jp/files/000071204.pdf
     7. 重要インフラの情報セキュリティ対策に関する主な資料【NISC】
        + https://www.nisc.go.jp/active/infra/siryou.html
        + 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(ZIP)【NISC】
          - https://www.nisc.go.jp/active/infra/files/tebikishorev.zip
     8. サイバーセキュリティ研究開発戦略【NISC】
        + https://www.nisc.go.jp/conference/cs/kenkyu/dai16/pdf/16shiryou0201.pdf
  3.   各種白書・年次報告書類
     1. 情報通信白書【総務省】
        + https://www.soumu.go.jp/johotsusintokei/whitepaper/
     2. AI白書【IPA】
        + https://www.ipa.go.jp/ikc/our\_activities/rs\_01.html
     3. 情報セキュリティ白書【IPA】
        + https://www.ipa.go.jp/ikc/our\_activities/rs\_03.html
     4. IT人材白書【IPA】
        + https://www.ipa.go.jp/jinzai/jigyou/about.html
     5. 迷惑メール白書2020 参考編／資料編
        + https://www.dekyo.or.jp/soudan/aspc/wp.html
     6. 情報セキュリティ10大脅威【IPA】
        + https://www.ipa.go.jp/security/vuln/10threats2021.html
  4.  情報セキュリティマネジメント（ISMS）関連
     1. ISMS適合性評価制度【JIPDEC】
        + https://isms.jp/isms.html
     2. 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【JIPDEC】
     3. ISMSユーザーズガイド-JISQ270012014(ISO\_IEC270012013)対応【JIPDEC】

## **各実施事項毎の参考情報【経営者、管理者向け】**

* 1.   サイバーセキュリティ全般
     1. 企業経営のためのサイバーセキュリティの考え方【NISC】
        + （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）
        + https://www.nisc.go.jp/active/kihon/pdf/keiei.pdf
     2. サイバーセキュリティ経営ガイドライン【METI】
        + https://www.meti.go.jp/policy/netsecurity/mng\_guide.html
     3.  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【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）を策定しました
          - https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html
          - 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～
          - https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf
     4. サイバーセキュリティ協議会【METI】
        + サイバーセキュリティ協議会
          - https://www.nisc.go.jp/conference/cs/kyogikai/
        + 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】
          - https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html
        + 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】
          - https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai\_houkoku.html
     5. 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】
        + https://www.ipa.go.jp/security/fy28/reports/scrm/index.html
     6. 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】
        + https://www.ipa.go.jp/security/keihatsu/sme/guideline/
  2.   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】
     1. https://www.meti.go.jp/policy/netsecurity/mng\_guide.html
     2. 重要１０項目全般に関連する参考情報
        + サイバーセキュリティ経営ガイドライン解説書 [Ver.2.0]（IPA）
          - （サイバーセキュリティ経営ガイドラインの３原則、重要１０項目を具体的に実施するための考え方につい解説。）
          - https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html
        + 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）
          - (中小企業がセキュリティ対策に取り組む上でのポイントを解説したガイドライン。最低限対策が求められる
          - 「情報セキュリティ5か条」や、企業のセキュリティ対策状況を診断する「5分でできる！情報セキュリティ自社診断」等の付録も提供。)
          - https://www.ipa.go.jp/security/keihatsu/sme/guideline/
        + ISO/IEC 27002:2013（ISO/IEC）
          - （情報マネジメントシステムの仕様を定めた国際標準規格であり、情報セキュリティ管理のベストプラクティスを提供。）
        + Framework for Improving Critical Infrastructure Cybersecurity [Version 1.0]（NIST）
          - 重要インフラに係わる企業向けに実施すべきセキュリティ対策を「特定」、「防御」、「検知」、「対応」、「復旧」の5つの機能に分類し、さらにそれらの機能を22のカテゴリーで提示した米国のガイドライン。重要インフラ以外の企業でも活用可能。）
          - https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
        + SP800-53 [Rev.4]（NIST）
          - （連邦政府機関が実施すべきセキュリティ対策を提示した米国のガイドライン。米国連邦政府向けのクラウドサービスを提供する際に、本ガイドラインへの準拠が要求される場合がある。）
          - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
        + SP800-171 [Rev.1]（NIST）
          - （連邦政府機関以外の組織及び情報システムに対するCUI11を保護する上で実施すべきセキュリティ対策を提示した米国のガイドライン。米国連邦政府関係の業務を受託する際に、本ガイドラインへの準拠が要求される場合がある。）
          - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
     3. 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）の確保」に関連する参考情報
        + ITのスキル指標を活用した情報セキュリティ人材育成ガイド[2015年5月]（IPA）
          - （サイバー攻撃等を防ぐためにどのような対策が必要で、その対策を実施するためにはどのような人材が必要なのかを例示し、人材育成を行うためのヒントをまとめたガイドライン。）
          - https://www.ipa.go.jp/files/000039528.pdf
        + 職場の情報セキュリティ管理者のためのスキルアップガイド[2015年9月]（IPA）
          - （セキュリティ上の脅威を取り上げ、被害を防ぐためにはどのような対策を実施すべきかを例示し、セキュリティ管理者としての役割を具体的に提示したガイドライン。）
          - https://www.ipa.go.jp/files/000047872.pdf
     4. 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」に関連する参考情報
        + 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）
          - （本ガイドラインの4章にてリスク分析の手法を解説。また、リスク分析の実施を支援するリスク分析シートも付録して提示。）
          - https://www.ipa.go.jp/security/keihatsu/sme/guideline/
     5. 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」に関連する参考情報
        + 「高度標的型攻撃」対策に向けたシステム設計ガイド[2014年9月]（IPA）
          - （標的型攻撃対策として、システム内部への侵入を前提とした上で、侵害拡大防止及び監視強化を目的とした内部対策について解説したガイドライン。）
          - https://www.ipa.go.jp/files/000046236.pdf
        + 高度サイバー攻撃への対処におけるログの活用と分析方法[1.0版]（JPCERT/CC）
          - （サイバー攻撃への備えと効果的な対策の観点から、一般的に利用される機器に攻撃者の活動の痕跡をログとして残すための考え方、それらのログから痕跡を見つけ出す方法等を記載したガイドライン。）
          - https://www.jpcert.or.jp/research/apt-loganalysis.html
        + 組織における内部不正防止ガイドライン [第4版]（IPA）
          - （組織における内部不正を防止するために実施すべき対策として、10の観点（コンプライアンス、職場環境等）のもと30項目の対策を提示したガイドライン。）
          - https://www.ipa.go.jp/files/000057060.pdf
        + 秘密情報の保護ハンドブック [平成 28 年 2 月]（経済産業省）
          - （秘密情報の漏えいを未然に防止するための対策例を集めて紹介したハンドブック。）
          - http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html
     6. 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」に関連する参考情報
        + 情報セキュリティマネジメントシステム（ISMS）適合性評価制度（JIPDEC）
          - （情報セキュリティマネジメントシステムにおける国際標準規格 ISO/IEC27001 に基づいて第三者認証を行う制度。）
          - https://isms.jp/isms.html
        + サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度（JIPDEC）
          - （産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムにおける国際標準規格 IEC62443-2 に基づいて第三者認証を行う制度。）
          - https://isms.jp/csms.html
        + 情報セキュリティ管理基準（経済産業省）
          - （情報セキュリティマネジメントの構築から具体的な管理策に至るまで包括的な内容を含み、国際標準規格ISO/IEC27001 とも整合を持った基準。）
          - http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html
        + 情報セキュリティ対策ベンチマーク（IPA）
          - （Web 上で質問に答えることによって、自社のセキュリティ対策の実施状況を散布図、レーダーチャート、スコア等で表示するツール。自社の対策状況を他社の対策状況と比較することも可能。）
          - http://www.ipa.go.jp/security/benchmark/
        + 安全なウェブサイトの作り方 [第 7 版]（IPA）
          - （セキュリティを考慮した Web サイトを作成するための技術的な対策を提示したガイドライン。別冊としてWeb サイトに脆弱性が存在していないかを確認するためのテスト項目を提示したウェブ健康診断仕様等も提供。）
          - https://www.ipa.go.jp/security/vuln/websecurity.html
        + JVN（IPA、JPCERT/CC）
          - （日本で使用されているソフトウェア等の脆弱性関連情報とその対策情報を提供する、脆弱性対策情報ポータルサイト。）
          - https://jvn.jp/
     7. 指示７「インシデント発生時の緊急対応体制の整備」に関連する参考情報
        + CSIRT 構築マテリアル（JPCERT/CC）
          - （組織的なインシデント対応を行うための CSIRT を構築する上で、「構想フェーズ」、「構築フェーズ」、「運用フェーズ」のそれぞれの段階で考慮すべきポイントを解説したガイドライン。）
          - https://www.jpcert.or.jp/csirt\_material/
        + CSIRT 構築に役立つ参考資料（日本シーサート協議会）
          - （CSIRT の構築に際し、構築初心者／経営者向け説明時／構築担当者の企画・構築・運用の各段階におけるドキュメント類をまとめた参考資料集。）
          - http://www.nca.gr.jp/activity/build-wg-document.html
     8. 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」に関連する参考情報
        + 事業継続ガイドライン [平成 25 年 8 月改定]（内閣府）
          - （事業継続計画の策定・改善にあたって、事業継続の必要性を明示し、実施が必要な事項、望ましい事項等を提示したガイドライン。）
          - http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03.pdf
     9. 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および状況把握」に関連する参考情報
        + 情報サービス・ソフトウェア産業における下請適正取引等の推進のためのガイドライン [平成29年3月]（経済産業省）
          - （下請適正取引等の推進を図ることを目的として策定したものであり、個人情報保護やセキュリティ対策に係る取り組み等の考慮すべき事項を解説したガイドライン。）
          - http://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf
        + SECURITY ACTION セキュリティ対策自己宣言 （IPA）
          - （中小企業がセキュリティ対策に取り組むことを自己宣言する制度。）
          - https://www.ipa.go.jp/security/security-action/
     10. 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および提供」に関連する参考情報
         + 届出・相談・情報提供（不正アクセスやウイルス等に関する届出）（IPA）
           - （コンピュータウイルス、不正アクセス、脆弱性関連情報等に関する届出を行う際の届出様式、届出先、届出状況等を提供する Web サイト。）
           - https://www.ipa.go.jp/security/outline/todoke-top-j.html
         + 標的型サイバー攻撃特別相談窓口（IPA）
           - （標的型サイバー攻撃を受けた際に、専門的知見を有する相談員が対応する窓口。）
           - https://www.ipa.go.jp/security/tokubetsu/
         + サイバー情報共有イニシアティブ（J-CSIP）（IPA）
           - （重要インフラで利用される機器の製造業者、電力業界、ガス業界、化学業界、石油業界、資源開発業界、自動車業界、クレジット業界において情報共有と早期対応を行うための活動。）
           - https://www.ipa.go.jp/security/J-CSIP/
         + @police（警察庁）
           - （サイバー犯罪・サイバーテロの未然防止及び被害の拡大防止を図るために、ネットワークセキュリティに関する様々な情報を提供する Web サイト。）
           - https://www.npa.go.jp/cyberpolice/
  3.   DX関連
     1. Society5.0【内閣府】
        + https://www8.cao.go.jp/cstp/society5\_0/
     2. サイバーフィジカルシステム（CPS)【JEITA】
        + https://www.jeita.or.jp/cps/about/
     3. 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～【METI】
        + https://www.meti.go.jp/shingikai/mono\_info\_service/digital\_transformation/20180907\_report.html
     4. 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】
        + https://www.meti.go.jp/press/2018/12/20181212004/20181212004.html
     5. DX時代における企業のプライバシーガバナンス【METI】
        + https://www.meti.go.jp/policy/it\_policy/privacy/privacy.html
     6. 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】
     7. 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【METI】
        + https://www.ipa.go.jp/ikc/reports/20200514\_1.html
     8. DXレポート2中間取りまとめ【METI】
        + https://www.meti.go.jp/press/2020/12/20201228004/20201228004.html
     9. DXの推進に関するお役立ちコンテンツ一覧【IPA】
        + https://www.ipa.go.jp/ikc/imanavi.html
     10. DX促進に向けた文書を公開～企業ビジネスモデルの変革によるDX実現を後押し～【2020年11月IPA】
         + https://www.ipa.go.jp/ikc/reports/20200609.html
         + プラットフォームデジタル化指標について【2020年6月】
           - https://www.ipa.go.jp/files/000082761.pdf
     11. 【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】
           - https://www.ipa.go.jp/ikc/reports/20200528.html
         + 【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】
           - https://www.ipa.go.jp/files/000082761.pdf
         + 【参考】DX推進セミナー～DXの実現に向けた取り組み～
           - https://www.ipa.go.jp/ikc/seminar/20200302.html
  4.   テレワーク関連
     1. テレワーク実施者の方へ【NISC】
        + https://www.nisc.go.jp/security-site/telework/
        + 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】
          - https://www.nisc.go.jp/active/general/pdf/telework20200414.pdf
     2. ★テレワーク総合情報サイト【総務省】
        + https://telework.soumu.go.jp/
     3. テレワークセキュリティガイドライン（第５版）【総務省】
        + https://www.soumu.go.jp/main\_sosiki/cybersecurity/telework/
     4. インターネットの安全・安心ハンドブック【NISC】
        + https://www.nisc.go.jp/security-site/handbook/
     5. サイバーセキュリティ経営ガイドライン【METI/IPA】
        + https://www.meti.go.jp/policy/netsecurity/mng\_guide.html
     6. 中小企業の情報セキュリティ対策ガイドライン【IPA】
        + https://www.ipa.go.jp/security/keihatsu/sme/guideline/
     7. ★テレワーク総合ポータルサイト【厚生労働省】
        + https://telework.mhlw.go.jp/info/doc/
        + テレワークの適切な導入及び実施の推進のためのガイドライン
          - https://www.mhlw.go.jp/content/000759469.pdf
        + テレワークの適切な導入及び実施の推進のためのガイドライン（リーフレット）
          - https://www.mhlw.go.jp/content/000766329.pdf
        + 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】
          - https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/H28hatarakikatakaikaku.pdf
     8. テレワークを行う際のセキュリティ上の注意事項【IPA】
        + https://www.ipa.go.jp/security/announce/telework.html
     9. テレワーク勤務のサイバーセキュリティ対策！ 警視庁
        + https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/telework.html
  5.   AI関連
     1. 「AI利活用ハンドブック～AIをかしこく使いこなすために～」
        + https://www.caa.go.jp/policies/policy/consumer\_policy/meeting\_materials/review\_meeting\_004/ai\_handbook.html
     2. AI・データの利用に関する契約ガイドライン【METI】
        + https://cio.go.jp/node/2651
  6.   IoTセキュリティ関連
     1. 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】
        + https://www.ipa.go.jp/files/000063605.pdf
     2. IoT・5Gセキュリティ総合対策【2019年8月総務省】
        + https://www.soumu.go.jp/main\_content/000641510.pdf
        + 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】
          - https://www.soumu.go.jp/main\_content/000688845.pdf
     3. IoTセキュリティチェックリスト【JPCERT/CC】
        + https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html
     4. 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」】
        + http://www.iotac.jp/wg/security/
        + IoTセキュリティガイドライン ver1.0概要
          - https://www.soumu.go.jp/main\_content/000428394.pdf
     5. 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】
        + https://www.soumu.go.jp/main\_content/000688845.pdf
     6. 【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】
        + http://www.iotac.jp/wp-content/uploads/2016/01/03\_%E8%B3%87%E6%96%99%EF%BC%93-%E7%B5%8C%E7%94%A3%E7%9C%81%E8%AA%AC%E6%98%8E%E8%B3%87%E6%96%99.pdf
     7. IoTセキュリティチェックリスト
        + https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html
     8. IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）
        + https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html
     9. 【削除】IoTセキュリティ対応マニュアル産業保安版
        + https://www.meti.go.jp/policy/safety\_security/industrial\_safety/sangyo/hipregas/files/security\_manual.pdf
     10. 「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】
         + https://www.nisc.go.jp/active/kihon/res\_iot\_fw2016.html
  7.   IT-BCP関連
     1. IT-BCP【平成25年NISC】
  8.   インシデント対応
     1. 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】
        + https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM\_Guideline\_app\_C.xlsx
  9.   個人情報保護関連
     1. GDPR（General Data Protection Regulation：一般データ保護規則）k【個人情報保護委員会】
        + https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/
     2. 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】
        + https://www.meti.go.jp/press/2020/08/20200828012/20200828012.html
  10.   システム開発・運用（外部委託）
      1. 政府機関等の対策基準策定のためのガイドライン【NISC】
         + https://www.nisc.go.jp/active/general/kijun30.html
      2. 改正民法に対応した「情報システム・モデル取引・契約書」を公開 ～ユーザ企業・ITベンダ間の共通理解と対話を促す～【IPA】
         + https://www.ipa.go.jp/ikc/reports/20191224.html
  11.   人材育成
      1. デジタルリテラシー関連
         + 「デジタルリテラシー協議会」
           - https://www.dilite.jp/
         + 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
      2. iCD関連
         + iコンピテンシディクショナリ（iCD）について
           - https://www.ipa.go.jp/jinzai/hrd/i\_competency\_dictionary/index.html
      3. 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
           - https://www.ipa.go.jp/jinzai/itss/itssplus.html
           - データサイエンス領域

https://www.ipa.go.jp/files/000063897.xlsx

* + - * + アジャイル領域

https://www.ipa.go.jp/files/000065571.pdf

* + - * + IoTソリューション領域

https://www.ipa.go.jp/files/000065568.pdf

* + - * + セキュリティ領域

https://www.ipa.go.jp/files/000058688.xlsx

* + 1. 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】
         * https://www.ipa.go.jp/ikc/reports/20190412.html
    2. サイバーセキュリティ関連
       - 情報セキュリティマネジメントに要求される知識と技能【シラバス】【情報セキュリティマネジメント試験】
         * https://www.jitec.ipa.go.jp/sg/
         * 【参考】【まとめ】情報セキュリティマネジメントに要求される知識と技能【シラバス】（Bib05-13）

https://bluemoon55.github.io/Sharing\_Knowledge2/MindManager2/Bib05-13.html

* + - * 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）
        + http://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf
    1. 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
         * https://www.jitec.ipa.go.jp/

## **法令・規則**

* 1.  サイバーセキュリティ関係法令\_Q&AハンドブックVer1.0
     1. https://www.nisc.go.jp/security-site/law\_handbook/index.html
  2. 迷惑メール関係法令・窓口等【迷惑メール白書2020】【P.142～145】
     1. https://www.dekyo.or.jp/soudan/data/anti\_spam/whitepaper/2020/wp2020.pdf

## **一般ユーザ向け啓発資料【IT利用局面毎】**

* 1.  インターネット利用
     1. 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【NISC】
        + https://www.nisc.go.jp/security-site/blue\_handbook/index.html
     2. インターネットの安全・安心ハンドブック【NISC】
        + https://www.nisc.go.jp/security-site/handbook/index.html
     3. ネット接続製品の安全な選定・利用ガイド【IPA】
        + https://www.ipa.go.jp/security/vuln/report/notice/guideforconsumer.html
  2.  インターネットでの不正行為を発見した場合
     1. 違法情報・有害情報、誹謗中傷情報
     2. 違法・有害情報相談センターへの相談
  3.  ECサイト利用
     1.  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】
        + https://www.antiphishing.jp/report/guideline/consumer\_guideline2020.html
        + http://www.antiphishing.jp/report/consumer\_antiphishing\_guideline\_2020.pdf
     2.  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】
        + https://www.saferinternet.or.jp/wordpress/wp-content/uploads/narisumashi\_manual.pdf
  4.  電子メール
     1.  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】
        + https://www.soumu.go.jp/main\_sosiki/joho\_tsusin/d\_syohi/pdf/m\_mail\_pamphlet.pdf
     2.  チェーンメール対策BOOK\_「撃退！チェーンメール 」（2021年度版）【日本データ通信協会迷惑メール相談センター】
        + https://www.dekyo.or.jp/soudan/data/chain/chainbook.pdf
     3.  詐欺メール対策リーフレット「そのメール、詐欺カモ！？」（2021年度）【日本データ通信協会迷惑メール相談センター】
        + https://www.dekyo.or.jp/soudan/data/info/A4\_maildesagi.pdf
     4.  迷惑メール対策BOOK\_「撃退！迷惑メール」（2021年度版）【日本データ通信協会迷惑メール相談センター】
        + https://www.dekyo.or.jp/soudan/contents/info/pamphlet\_gm.html

## **サイバーセキュリティ関連組織が開設するポータルサイト**

* 1.  内閣サイバーセキュリティセンター（NISC）
     1. https://www.nisc.go.jp/
     2. みんなでしっかりサイバーセキュリティ
        + https://www.nisc.go.jp/security-site/index.html
     3. みんなで使おうサイバーセキュリティ・ポータルサイト
        + https://security-portal.nisc.go.jp/
  2.  情報処理推進機構（IPA）
     1. https://www.ipa.go.jp/
     2. 情報セキュリティ トップページ
        + https://www.ipa.go.jp/security/
     3. 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
        + https://www.ipa.go.jp/security/kokokara/
     4. SECURITY ACTION セキュリティ対策自己宣言
        + https://www.ipa.go.jp/security/security-action/
     5. サイバー情報共有イニシアティブ（J-CSIP）
        + https://www.ipa.go.jp/security/J-CSIP/
  3.  JPCERTコーディネーションセンター（JPCRT/CC）
     1. https://www.jpcert.or.jp/
     2. 緊急情報を確認する
        + https://www.jpcert.or.jp/menu\_alertsandadvisories.html
     3. 脆弱性対策情報データベース（JVN）
        + https://jvn.jp/
     4. JPCERT/CCに依頼する
        + https://www.jpcert.or.jp/menu\_reporttojpcert.html
  4.  総務省
     1. 国民のための情報セキュリティサイト（総務省）
        + https://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/
     2. リンク集｜国民のための情報セキュリティサイト - 総務省
        + https://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/link.html
  5.  経済産業省
     1. サイバーセキュリティ政策
        + https://www.meti.go.jp/policy/netsecurity/index.html
  6.  日本サイバー犯罪対策センター（JC3）
     1. https://www.jc3.or.jp/
  7.  情報セキュリティ広場（警視庁）
     1. https://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html
  8.  セーファーインターネット協会（一般社団法人）
     1. https://www.saferinternet.or.jp/