Sec01-02\_IT・サイバーセキュリティ関連\_調査・分析した各種文献等の内容要約へのインデックス

参照:

[Page not found &middot; GitHub Pages](https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02.html);

1. 目的
   1. リストアップした文献の検索用インデックス
   2. 分類毎のファイル内に整理した文献の要約あり
2. 改訂履歴
   1. 【2020年12月10日】内容再確認
   2. 【2020年10月9日】情報追加
   3. 【2020年10月1日】情報追加
   4. 【2020年8月4日】アイコンデザイン変更
   5. 【2020年7月30日】2020年7月に収集精査した文献及び記事の追加

リレーションシップ:

エクスポート先 [参考文献等へのリンク](#jB060qnA/0Gw1eo50YGJew==);

* 1. 【2020年7月2～3日】2020年1月から6月までに収集精査した文献及び記事の追加

リレーションシップ:

エクスポート先 [2020年2期追加分（本文ファイル取り込み済）](#E5J6274NoUeDBZI6wSkoVw==);

* 1. 【2020年6月15日】最新文献追加
  2. 【2020年6月8日】DAX95\_知の共有化関連アーカイブ内インデックスに2019年1期から2018年1期までの調査資料をリストアップ
  3. 【2020年6月5日】Sec01-04\_IT・サイバーセキュリティ関連各種施策等のインデックス及び内容要約、DAX95\_知の共有化関連アーカイブ内インデックスに2019年2期までの調査資料を追加【検索用】
  4. 【2020年5月25日】Web、極意で参照する情報へのマーキング
  5. 【2020年5月21日】資料タイトルの検索を容易にするために、Sec01-02-50～63、Sec01-04に登録された資料のインデックスを記載
  6. 【2020年4月23日】Sec01-02をSec01-50へ移行し、今後分割する。Sec01-20はインデックスページとする。

1. 凡例
   1. 内容要約を作成済の文献



* 1. 内容要約を整理する予定の文献



* 1. 内容要約を未作成の文献



* 1. 詳細編への反映待ちの文献



1. **Sec01-02-50\_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**

参照:

[Page not found &middot; GitHub Pages](https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-50.html);

* 1. **Sec01-02-52\_各種ガイドブックの内容要約\_啓発情報提供サイト**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-52.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-52.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-52.html>;

* + 1. 中小企業サイバーセキュリティ対策の極意ポータルサイト【東京都】



参照:

[トップページ](https://cybersecurity-tokyo.jp/);

* + 1. ここからセキュリティ！情報セキュリティ・ポータルサイト【IPA】



* + 1. みんなでしっかりサイバーセキュリティ【NISC】



* + 1. 基礎知識｜国民のための情報セキュリティサイト【総務省】



* + 1. 一般利用者の対策｜国民のための情報セキュリティサイト【総務省】



* + 1. 企業・組織の対策｜国民のための情報セキュリティサイト【総務省】



* + 1. @police－被害事例と対処法【警察庁】



* 1. **Sec01-02-53\_各種ガイドブックの内容要約\_一般ユーザ向け【零細企業を含む】**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-53.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-53.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-53.html>;

* + 1. インターネットを安全に利用するための情報セキュリティ対策９か条 【NISC・IPA】



* + 1. ネットの危険からお子様を守るために、 保護者ができる3つのポイント 【2017年4月6日政府広報】



* + 1. ネットワークビギナーのための情報セキュリティハンドブックVer.2.11（小冊子） 【2017年02月08日NISC】



* + 1. マンガで学ぶサイバーセキュリティ【NISC】【初心者向け】



* + 1. IPA 対策のしおり【IPA】



* + 1. 「やられたかな？その前に」【2015年10月14日 ISOG-J】



* + 1. 2017年度版「撃退！迷惑メール」迷惑メール対策BOOK【迷惑メール相談センター】



* 1. **Sec01-02-54\_各種ガイドブックの内容要約\_一般企業向け【特に中小企業】**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-54.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-54.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-54.html>;

* + 1. 「Bib10-08「知の共有化」に関連した国等の政策の要約」を参照
    2. 「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関する検討会」の報告書の中小企業部分抜粋



* + 1. 中小企業向け「はじめての個人情報保護法」～シンプルレッスン～【2017年6月個人情報保護委員会】



* + 1. Sec01-02-20 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）⇒独立文書化



* + 1. SECURITY ACTION【2017年4月IPA】



* + 1. 中小企業における組織的な情報セキュリティ対策ガイドラインチェック項目【2012年9月3日IPA】



* + 1. 中小企業における組織的な情報セキュリティ対策ガイドライン事例集【2012年9月3日IPA】



* + 1. 中小企業における情報セキュリティの普及促進に関する共同宣言



* + 1. 特定個人情報の適正な取扱いに関するガイドラン （事業者編）（個人情報保護委員会）



* + 1. 個人情報の 保護に関する法律ついての分野別 ガイドライン（各府省庁）



* + 1. 秘密情報の保護ハンドブック（経済産業省）【旧版？】



* + 1. インシデント対応マニュアルの作成について（組織内CSIRT 構築の参考資料）【2015年JPCERT/CC】



* + 1. 昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について【2020年6月12日METI】



参照:

[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. **Sec01-02-55\_各種ガイドブックの内容要約\_一般企業向け【SK3】**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-55.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-55.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-55.html>;

* + 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】



* + 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【2020年6月3日IPA】



参照:

<https://www.ipa.go.jp/files/000072309.pdf>;

* + 1. CISO等セキュリティ推進者の経営・事業に関する役割調査【2018年6月28日IPA】



* + 1. －別冊－CISO等セキュリティ推進者の経営・事業に関する役割プラクティス【2018年6月28日IPA】



* + 1. 情報セキュリティ 10 大脅威2018【2018年3月IPA】



* + 1. 監査人の警鐘 ‐ 2018年 情報セキュリティ十大トレンド【2018年1月5日JASA】



* + 1. 2017年セキュリティ10大ニュース【2017年12月So-net】



* + 1. サイバーセキュリティ経営ガイドライン Ver2.0【2017年11月16日METI】



* + 1. 情報セキュリティ白書2017【2017年7月IPA】



* + 1. 匿名加工情報の事例集（JIPDEC認定個人情報保護団体対象事業者向け）【PDF】【2017年7月JIPDEC】



* + 1. 改正個人情報保護法（2017年5月改正施行）対応



* + 1. 「企業における営業秘密管理に関する実態調査」報告書について【2017年3月17日IPA】



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



* + 1. 【てびき】情報管理も企業力～秘密情報の保護と活用～【2016年12月5日METI】



* + 1. 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】



* + 1. 企業（組織）における最低限の情報セキュリティ対策のしおり+1【2015年8月21日 2017年6月30日IPA】【第5版】



* + 1. 【旧版】サイバーセキュリティ経営ガイドライン解説書Ver.1.0【2016年12月IPA】



* + 1. 【旧版】サイバーセキュリティ経営ガイドライン解説書Ver.1.0別添：被害事例集【2016年12月IPA】



* + 1. 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】



* + 1. 情報セキュリティポリシーサンプル改版（1.0版）【2016年3月29日JNSA】



* + 1. すぐ役立つ！法人で行うべきインシデント初動対応 ~「不審な通信」その時どうする~【2016年11月1日トレンドマイクロ】



* + 1. 2016 年インシデント事例から学ぶ「Web サイトのセキュリティ対策」【トレンドマイクロ】



* + 1. 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】



* + 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. 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



* + 1. 情報セキュリティ読本　四訂版- IT時代の危機管理入門 -【2014年11月4日IPA】



* + 1. 米国の「20の重要なセキュリティ対策」及びオーストラリアの「35の標的型サイバー侵入に対する軽減戦略」【2010年】



* + 1. コンピュータセキュリティインシデント対応ガイド（NIST SP 800-61）【2008年3月NIST】



* + 1. JIPDEC経営読本「情報管理はマネーです」【2017年JIPDEC】



* + 1. IPAテクニカルウチ「ランサムウェアの脅威と対策」【2017年1月IPA】



* + 1. IPAテクニカルウチ「標的型攻撃メールの例と見分け方」【2017年1月IPA】



* + 1. 情報漏えい発生時の対応ポイント集(第3版) 【2012年10月IPA】



* + 1. 「高度サイバー攻撃対処のためのリスク評価等のガイドライン 付属書」 【2016年10月NISC】



* + 1. 『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】



* + 1. **モバイルセキュリティ関連**
       - Sec01-02-50各種ガイドブックの内容要約(働き方改革関連)へ移動
       - 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【202年4月9日NISC】



* + - * ●MDM導入・運用検討ガイド【経済産業省】



* + - * ●情報セキュリティ対策の基本 スマートフォン編 - IPA【IPA】



* + - * ●スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン【経済産業省】



* + - * ●私物端末の業務利用におけるセキュリティ要件の考え方【内閣官房】



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



* + - * ●テレワークではじめる働き方改革－テレワークの導入・運用ガイドブック－【厚生労働省】



* + - * ●テレワークセキュリティガイドライン第４版【総務省】



* + - * ●導入事例　大分県庁　【Soliton】



* + 1. NISTガイドライン



* + - * Mobile Device Security: Cloud and Hybrid Builds
        + Executive Summary
        + Approach, Architecture, and Security Characteristics
        + How-To Guide
  1. **Sec01-02-56\_各種ガイドブックの内容要約\_重要インフラ・政府機関向け【独法を含む】**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-56.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-56.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-56.html>;

* + 1. サイバーセキュリティ基本法（2016年4月15日改正）
    2. 【未整理】サイバーセキュリティ2018【2018年7月25日NISC】



* + 1. サイバーセキュリティ2017【2017年８月25日NISC】



* + 1. 重要インフラの情報セキュリティ対策に係る第4次行動計画【2017年4月18日NISC】



* + 1. サイバーセキュリティ戦略【2015年９月４日閣議決定】



* + 1. 政府機関の情報セキュリティ対策のための統一規範



* + 1. 政府機関等の情報セキュリティ対策の運用等に関する指針



* + 1. 政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）



* + 1. 政府機関向け「アマゾン ウェブ サービス」対応セキュリティリファレンス



* + 1. 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の策定について【2015年5月NISC】



* + 1. 地方公共団体における情報セキュリティポリシーに関するガイドライン【2015年3月総務省】



* 1. **Sec01-02-57\_各種ガイドブックの内容要約\_法令・規則・規約**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-57.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-57.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-57.html>;

* + 1. 施策・政策・統計
       - サイバーセキュリティ基本法（2016年4月15日改正）
       - 【校正中】サイバーセキュリティ戦略（案）（2018年6月2日NISC）



* + - * サイバーセキュリティ戦略（2015年9月4日閣議決定）



* + - * サイバーセキュリティ2016【2016年サイバーセキュリティ戦略本部】
      * 「政府機関等の情報セキュリティ対策のための統一基準群（平成28年度版）」（2016年8月31日サイバーセキュリティ戦略本部決定）
      * 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】



* + - * サイバーセキュリティ関連施策に関する平成29年度予算重点化方針
      * 情報セキュリティ白書2017【2017年7月IPA】



* + 1. ISMS
       - 情報セキュリティマネジメント（ISMS）に準拠した対策【ISO/IEC27001:2013（管理項目35, 管理策114）】



* + - * ISMSユーザーズガイド -JIS Q 27001:2014対応【2014年4月14日JIPDEC】
      * 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



* + - * 情報セキュリティマネジメント（ISMS）に準拠した対策【ISO/IEC27001:2013（管理項目35, 管理策114）】



* + 1. NIST CSF　(重要インフラにおけるサイバーセキュリティフレームワーク)



* + - * 重要インフラにおけるサイバーセキュリティフレームワーク1.0版（CSF)【2014年2月12日NIST】
      * CSF フレームワークコア
    1. NIST SP 800-37 (連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド： セキュリティライフサイクルによるアプローチ)



* + 1. NIST 800-46 Guid to Enterprise Telewok,Remote Access,and Bring Your Own Devicee (BYOD) Securrity



参照:

[NIST.SP.800-46r2.pdf](file:///J:\Cloud_Storage\OneDrive%20-%20ＮＰO知的資源イニシアティブ（ＩＲＩ）\git_repository_Duo\Sharing_Knowledge3\MindManager3\nvlpubs.nist.gov\nistpubs\SpecialPublications\NIST.SP.800-46r2.pdf);

* + 1. NIST SP 800-53 (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)



* + 1. NIST SP 800-61 (コンピュータセキュリティインシデント対応ガイド)



* + 1. NIST SP 800-63 (電子的認証に関するガイドライン)



* + 1. NIST SP 800-113 Guide to SSL VPNs

参照:

[nistspecialpublication800-113.pdf](file:///J:\Cloud_Storage\OneDrive%20-%20ＮＰO知的資源イニシアティブ（ＩＲＩ）\git_repository_Duo\Sharing_Knowledge3\MindManager3\nvlpubs.nist.gov\nistpubs\Legacy\SP\nistspecialpublication800-113.pdf);

* + 1. CSC20 （効果的なサイバー防御のための重要なセキュリティコントロール）



* + 1. Top35 （標的型サイバー侵入の軽減戦略）
    2. GDPR（General Data Protection Regulation：一般データ保護規則）



* 1. **Sec01-02-58\_各種ガイドブックの内容要約\_未整理**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-58.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-58.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-58.html>;

* + 1. 【未整理】NIST SP.800-82R2　Guide to Industrial Control Systems (ICS) Security



* + 1. 【未整理】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】



* + 1. 【未整理】NIST Special Publication 800-171r1 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



* + 1. 【未整理】クラウドコンピューティングのためのセキュリティガイダンスv4.0



* + 1. 【未整理】危険な12の落とし穴　クラウドの重大セキュリティ脅威＋2017インシデント事例集【一般社団法人日本クラウドセキュリティアライアンス（CSAジャパン）】



* + 1. 【未整理】「つながる世界」を破綻させないためのセキュアなIoT製品開発13のステップ【CSAジャパン　IoTワーキンググループ】



* + 1. 【未整理】IoTへのサイバー攻撃仮想ストーリー集



* + 1. 【未整理】国内標的型サイバー攻撃分析レポート



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



* 1. **Sec01-02-59\_各種ガイドブックの内容要約\_その他資料**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-59.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-59.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-59.html>;

* + 1. マイナンバー制度とマイナンバーカード【総務省HP】



* + 1. 自治体CIO育成研修集合研修SLAの考え方【総務省】



* + 1. ICTの進化が雇用と働き方に及ぼす影響に関する調査研究（平成28年情報通信白書）【2016年総務省】



* 1. **Sec01-02-60\_各種ガイドブックの内容要約\_働き方改革関連【SK3】**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-60.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-60.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-60.html>;

* + 1. ●情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン【厚生労働省】



* + 1. ●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】



* + 1. ●テレワークセキュリティガイドライン第４版【総務省】



* + 1. 働き方改革を実現するために有用なITツールの種類と活用事例
    2. ゼロから学べるテレワーク導入完全ガイド【V-CUBE】
    3. **モバイルセキュリティ関連**
       - ●MDM導入・運用検討ガイド【経済産業省】



参照:

<https://www.jssec.org/dl/MDMGuideV1.pdf>;

* + - * ●情報セキュリティ対策の基本 スマートフォン編 - IPA【IPA】



参照:

<https://www.ipa.go.jp/files/000059213.pdf>;

* + - * ●スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン【経済産業省】



参照:

<https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000142.html>;

* + - * ●私物端末の業務利用におけるセキュリティ要件の考え方【内閣官房】



参照:

<https://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/byod.pdf>;

* + - * ●導入事例　大分県庁　【Soliton】



参照:

<https://www.soliton.co.jp/case_study/pref-oita.html>;

* + - * NISTガイドライン



* + - * + Mobile Device Security: Cloud and Hybrid Builds

Executive Summary

参照:

<https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4a-draft.pdf>;

Approach, Architecture, and Security Characteristics

参照:

<https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4b-draft.pdf>;

How-To Guide

参照:

<https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4c-draft.pdf>;

* 1. **Sec01-02-62\_各種ガイドブックの内容要約\_【参考】IT関連**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-62.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-62.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-62.html>;

* + 1. （原本は「Bib10-08国の事業が実施に至るまで」）
    2. IT戦略本部
    3. 高度情報通信ネットワーク社会形成基本法（IT基本法）（2015年2月1日改訂施行）
       - 「世界最先端IT国家創造宣言」の改定（高度情報通信ネットワーク社会推進戦略本部（IT戦略本部））（2016.5.20閣議決定)



* + 1. 電子行政オープンデータ戦略（2012年7月4日IT戦略本部）【再掲】



* + 1. 電子行政オープンデータ推進のためのロードマップ（2013年6月14日IT戦略本部決定）
    2. 官民データ活用推進基本法（平成28年法律第103号）
    3. 「オープンデータ基本指針」（案）「オープンデータ基本指針」（案）【2017年5月23日官民データ活用推進基本計画実行委員会】



* + 1. 世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画【2017年5月30日付け閣議決定】



* + 1. 「政府情報システムの整備及び管理に関する標準ガイドライン」(2015年3月19日更新、 2014年12月3日各府省CIO連絡会議決定）および「実務手引書」
    2. 人材育成・人材確保
       - IT人材白書2017【2017年4月25日IPA】



* + - * 情報技術者試験
      * iコンピテンシディクショナリ
    1. 人材育成・人材確保【セキュリティ関連】
       - ■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】



* + - * 情報処理安全確保支援士試験チェックシート



* 1. **Sec01-02-63\_各種ガイドブックの内容要約\_次世代環境及び技術関連**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-63.html>;

* + 1. 詳細ページ
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-02-63.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-02-63.html>;

* + 1. AI
       - IoT、 ビッグデータ、 AI等に関する 経済産業省の施策について【2016年3月METI】



* + 1. IoT
       - IoTセキュリティガイドラインver1.0【2016年7月5日総務省・経済産業省】



* + - * 安全なIoTシステムの創出【2016年3月1日NISC】



* + - * コンシューマ向けIoTセキュリティガイド【2016年6月24日JNSA】



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



* + - * Guide to Industrial Control Systems (ICS) Security【NIST SP.800-82R2】【JPCERT和訳】



* + - * 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ソリューション領域へのスキル変革の指針【2018年4月10日IPA】



* + - * IoTソリューション領域へのスキル変革の指針\_参考文献【2018年4月10日IPA】



* + - * 【未整理】IoTへのサイバー攻撃仮想ストーリー集【一般社団法人日本クラウドセキュリティアライアンス（CSAジャパン）】



* + - * 【未整理】「つながる世界」を破綻させないためのセキュアなIoT製品開発13のステップ【CSAジャパン　IoTワーキンググループ】



* + - * 【未整理】工場における産業用IoT導入のためのセキュリティファーストステップ【2018年8月JPCERT/CC】



* + - * 【未整理】「IoTセキュリティ基盤を活用したが安心安全な社会の実現に向けた実証実験」の結果の公表【2018年6月総務省情報流通行政局】



* + - * 旧版
        + 【未整理】IoTセキュリティ総合対策プログレスレポート2018【2018年7月　サイバーセキュリティタスクフォース】



* + - * + 【未整理】「IoTセキュリティ総合対策」（文書）【2017年12月　総務省情報流通行政局】



* + - * 【未整理】「IoTセキュリティ総合対策」について（講演会スライド）【2018年2月28日　総務省情報流通行政局】



* + - * 【未整理】IoTセキュリティ総合対策プログレスレポート2019【2018年5月　サイバーセキュリティタスクフォース】



* + - * IoT・5Gセキュリティ総合対策（案）【2019年6月総務省サイバーセキュリティタスクフォース】



* + 1. クラウド
       - クラウドセキュリティガイドライン活用ガイドブック2013年版【METI】



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



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



* + - * + ■ISMSクラウドセキュリティ認証の概要（スライド）【JIPDEC】



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



* + 1. 教育分野
       - 教育分野におけるクラウド導入に対応する情報セキュリティに関する手続きガイドブック【総務省】



* + - * 教育ＩＣＴの新しいスタイルクラウド導入ガイドブック2015【総務省】



* 1. **Sec01-04\_IT・サイバーセキュリティ関連各種施策等のインデックス及び内容要約**

参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-04.html>;

* + 1. IT関連のインデックス部分は、「DAX95\_知の共有化関連アーカイブ内インデックス」に併合予定。 内容要約部分はそのまま。



* + 1. **内容要約ページ**
       - https://bluemoon55.github.io/Sharing\_Knowledge3/MindManager3/Sec01-04.html



参照:

<https://bluemoon55.github.io/Sharing_Knowledge3/MindManager3/Sec01-04.html>;

* + 1. 知的財産関連
       - 「Bib10-08「知の共有化」に関連した国等の政策の要約」を参照
       - 「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関する検討会」の報告書の中小企業部分抜粋



参照:

<http://www.meti.go.jp/press/2017/04/20170419002/20170419002.html>;

* + 1. 次世代IT技術及び市場動向
       - 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】



参照:

<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】



参照:

<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】



参照:

<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】



参照:

<https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf>;

* + - * クラウドセキュリティガイドライン活用ガイドブック2013年版【METI】



参照:

<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】



参照:

<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】



参照:

<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】



参照:

<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】



参照:

<https://www.isms.jipdec.or.jp/seminar/cloud/shiryou-2.pdf>;

* + - * 教育分野におけるクラウド導入に対応する情報セキュリティに関する手続きガイドブック【総務省】



参照:

<http://www.soumu.go.jp/main_content/000417633.pdf>;

* + - * 教育ＩＣＴの新しいスタイルクラウド導入ガイドブック2015【総務省】



参照:

<http://www.soumu.go.jp/main_content/000358976.pdf>;

* + 1. システム化及びサイバーセキュリティ管理規約等
       - 人材育成・人材確保
         * ■iコンピテンシ・ディクショナリ【IPA】



参照:

<https://icd.ipa.go.jp/icd/>;

* + - * + ■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】



参照:

<http://www.ipa.go.jp/files/000039528.pdf>;

情報セキュリティ強化対応スキル指標のご紹介

参照:

<http://www.ipa.go.jp/jinzai/hrd/security/>;

* + - * ISMS関連
        + ■ISMSユーザーズガイド-JISQ27001:2014(ISO/IEC27001:2013)対応【JIPDEC】



* + - * + ■ISMSユーザーズガイド-JISQ27001:2014(ISO/IEC27001:2013)対応-リスクマネジメント編【JIPDEC】



* + - * 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
        + 参考資料

情報セキュリティマネジメントシステム(ISMS)適合性評価制度の概要



https://www.isms.jipdec.or.jp/about/index.html

参照:

<https://www.isms.jipdec.or.jp/about/index.html>;

ISMS認証機関一覧

https://www.isms.jipdec.or.jp/lst/isr/index.html

参照:

<https://www.isms.jipdec.or.jp/lst/isr/index.html>;

ISMS認証取得組織検索

https://www.isms.jipdec.or.jp/lst/ind/index.html

参照:

<https://www.isms.jipdec.or.jp/lst/ind/index.html>;

* + - * 情報セキュリティマネジメント（ISMS）に準拠した対策【ISO/IEC27001:2013（管理項目35, 管理策114）】



* + 1. 施策・政策・統計（サイバーセキュリティ戦略本部）

参照:

<http://law.e-gov.go.jp/htmldata/H26/H26HO104.html>;

* + - * サイバーセキュリティ基本法（2016年4月15日改正）
      * 【校正中】サイバーセキュリティ戦略（案）（2018年6月2日NISC）



参照:

<https://www.nisc.go.jp/conference/cs/dai18/pdf/18shiryou01.pdf>;

* + - * サイバーセキュリティ戦略（2015年9月4日閣議決定）



* + - * サイバーセキュリティ2016【2016年サイバーセキュリティ戦略本部】

参照:

<https://www.nisc.go.jp/active/kihon/pdf/cyber-security2016.pdf>;

* + - * 「政府機関等の情報セキュリティ対策のための統一基準群（平成28年度版）」（2016年8月31日サイバーセキュリティ戦略本部決定）
        + http://www.nisc.go.jp/active/general/kijun28.html

参照:

<http://www.nisc.go.jp/active/general/kijun28.html>;

* + - * 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】



参照:

<http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf>;

* + - * + http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf

参照:

<http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf>;

* + - * + サイバーセキュリティ戦略本部

参照:

<http://www.nisc.go.jp/conference/cs/index.html>;

http://www.nisc.go.jp/conference/cs/index.html

参照:

<http://www.nisc.go.jp/conference/cs/index.html>;

* + - * 情報セキュリティ白書2016【2016年7月IPA】



参照:

<https://www.ipa.go.jp/security/publications/hakusyo/2016.html>;

* + - * サイバーセキュリティ関連施策に関する平成29年度予算重点化方針

参照:

<http://www.nisc.go.jp/active/kihon/pdf/yosanhoshin29.pdf>;

* + - * サイバーセキュリティ政策の評価に係る基本方針

参照:

<http://www.nisc.go.jp/active/kihon/pdf/cs_hyouka_houshin.pdf>;

* + - * 情報セキュリティ白書2017【2017年7月IPA】



参照:

<https://www.ipa.go.jp/security/publications/hakusyo/2017.html>;

* + 1. ① 関係機関の能力向上

1. **DAX95\_知の共有化関連アーカイブ内インデックス**

****

* 1. 「DAX95\_知の共有化関連アーカイブ内インデックス」から抜粋
  2. **ソフトウェア開発標準**
     1. Bib04-07 共通フレーム2013とユーザのための要件定義ガイド 【MindManager→html】【SK2】



参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib04-07.html>;

* + 1. 【削除】【XMIND】Bib03-11調達における留意点
    2. 【確認後削除】Bib03-12調達仕様書（案） ⇒Bib40-01に含む？？？？

参照:

[Page not found &middot; GitHub Pages](https://bluemoon55.github.io/Sharing_Knowledge/Digital_Archives/Deliverables/mind2html/Bib03-12);

* + 1. Bib06-06政府情報システムの整備及び管理 に関する標準ガイドライン【構成のみ】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib06-06.html>;

* 1. **iコンピテンシ・ディクショナリ**
     1. 組織一般
        + Bib06-05最低限知っておくべき情報処理技術 （ITリテラシー） 【MindManager→html】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib06-05.html>;

* + - * Bib10-02経営者向けセキュリティ対策のポイント 【MindManager→html】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib10-02.html>;

* + 1. 図書館分野
       - Bib03-02図書館情報システムに関連するガイドライン・タスク・必要なスキル・LOD・未来に向けて 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib03-02.html>;

* + - * 【内容校正中】Bib03-04デジタルトランスフォーメーション時代のMLA業務のタスク 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib03-04.html>;

* + - * 【？】Bib03-05図書館情報システム構築のタスクプロフィール（政府標準ガイドライン準拠） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib03-05.html>;

* + - * Bib03-08システム構築コンテンツ構築に必要なスキル知識要素の抜粋 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib03-08.html>;

* + - * Bib03-0601図書館員に必要なITスキル要素 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib03-0601.html>;

* + - * Bib03-0602図書館業務のタスクプロフィール 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib03-0602.html>;

* + - * Bib10-09データサイエンス領域のスキル標準「ITSS+」 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib10-09.html>;

* + - * Bib10-10セキュリティ領域のスキル標準「ITSS+」 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib10-10.html>;

* + 1. iCD解説
       - Bib06-07iコンピテンシ・ディクショナリ（IPA） 【MindManager→html】【SK2】

参照:

[iコンピテンシ・ディクショナリ （2015年正式公開（IPA））](https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib06-07.html);

* + - * Bib04-02タスクディクショナリ （タスク小分類415項目） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib04-02.html>;

* + - * Bib04-03スキルディクショナリ (スキル424項目・知識8256項目) 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib04-03.html>;

* + - * Bib04-04タスク毎に必要なスキル詳細 （タスク小分類415項目） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib04-04.html>;

* + - * 【XMIND】Bib04-06iコンピテンシディクショナリ\_04スキルディクショナリ (スキル424項目・知識8256項目から抜粋) （別ファイルで更新中）【SK2】

参照:

[Page not found &middot; GitHub Pages](https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib04-06.html);

* + - * 【XMIND】Bib05-01iCDスキルディクショナリ (スキル424項目・知識8256項目から抜粋) 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib05-01.html>;

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

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib10-11.html>;

* 1. **ITスキルレベル評価制度**
     1. Bib04-05スキル概要と情報処理試験（熟達度レベル評価判定） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib04-05.html>;

* + 1. Bib06-04ITパスポート 試験シラバス 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib06-04.html>;

* + 1. Bib05-02IT基礎 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib05-02.html>;

* + 1. Bib05-03離散数学 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib05-03.html>;

* + 1. Bib05-04応用数学 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib05-04.html>;

* + 1. Bib05-05情報に関する理論 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib05-05.html>;

* + 1. Bib05-06通信に関する理論 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib05-06.html>;

* + 1. Bib05-07コンピュータ基礎 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib05-07.html>;

* + 1. Bib05-13情報セキュリティマネジメントシラバス 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib05-13.html>;

* + 1. Bib06-09応用情報技術者試験シラバス 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib06-09.html>;

* + 1. Bib06-10IT ストラテジスト試験（レベル４）シラバス 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib06-10.html>;

* 1. **次世代社会（デジタル変革）**
     1. **AI白書2019**
        + DAX25-20-00【書籍】 AI白書2019\_目次 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-00.html>;

* + - * DAX25-20-01【書籍】 AI白書2019\_第１章AIが壊すもの、創るもの 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-01.html>;

* + - * DAX25-20-02【書籍】 AI白書2019\_第2章技術動向 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-02.html>;

* + - * DAX25-20-03【書籍】 AI白書2019\_第3章利用動向 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-03.html>;

* + - * DAX25-20-04【書籍】 AI白書2019\_第4章制度政策動向 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-04.html>;

* + - * DAX25-20-04-01国の施策要約【AI白書2019\_第4章制度政策動向より】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-04-01.html>;

* + - * DAX25-20-05【書籍】 AI白書2019\_第5章AIの社会実装課題と対策 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-05.html>;

* + - * DAX25-20-05-5-6-3社会実装推進の方向性（テンプレート例） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-20-05-5-6-3.html>;

* + 1. DAX20-04人工知能に関する基礎知識（まとめ） 【MindManager→html】【SK2】



参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-04.html>;

* + 1. 人工知能に関する文献のポイント
       - DAX20-0401-1人工知能に関する文献のポイント（引用1） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0401-1.html>;

* + - * DAX25-01【書籍】絵でわかる人工知能【2017年三宅陽一郎】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-01.html>;

* + - * DAX25-02【書籍】人工知能「超入門」ディープラーニングの可能性と脅威（Impress QuickBooks) 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-02.html>;

* + - * DAX25-03【書籍】よくわかるディープラーニングの仕組み【谷田部卓】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-03.html>;

* + - * DAX25-04【書籍】ビジネスで使う機械学習【谷田部卓】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-04.html>;

* + - * DAX25-05【書籍】非エンジニア、文系、ビジネスマンのための人工知能入門：数式が苦手なあなたにおすすめ 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-05.html>;

* + - * DAX25-06【書籍】人工知能（AI）活用時代に必要とされる能力とは？ビジネスで差がつく「データサイエンス力」 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-06.html>;

* + - * DAX25-08【書籍】2020年を見据えたグローバル企業のIT戦略 IoT編【2015年11月27日入江宏志】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-08.html>;

* + - * DAX25-09【文献】平成28年度情報通信白書【総務省】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-09.html>;

* + - * DAX25-10【記事】人間の仕事を奪う｢AI｣の過去･現在･未来【2017年04月15日東洋経済】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-10.html>;

* + - * DAX25-11【文献】IT人材白書2017【2017年4月25日IPA】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-11.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】 【MindManager→html】【SK2】



参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-12.html>;

* + - * DAX25-13【文献】科学技術イノベーション総合戦略2017（案）【2017年4月21日】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-13.html>;

* + - * DAX25-14【文献】新産業ビジョン【2017年5月METI】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-14.html>;

* + - * 【資料名のみ】DAX25-15【文献】人工知能技術戦略（案） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-15.html>;

* + - * DAX25-16【文献】知的財産推進計画2017（2017年5月16日内閣官房知的財産戦略本部） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-16.html>;

* + - * DAX25-17【文献】「デジタルトランスフォーメーション」【2016年9月ベイカレント・コンサエルティング】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-17.html>;

* + - * DAX25-18【書籍】60分でわかる！ディープラーニング最前線 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-18.html>;

* + - * DAX25-30【書籍】いまこそ知りたいAIビジネス 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX25-30.html>;

* + 1. DAX20-0402-1 ITロードマップ2018年版【2018年3月NRI】 【MindManager→html】【SK2】

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【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2.html>;

* + - * DAX20-0402-2-0 ITの最新トレンド 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-0.html>;

* + - * DAX20-0402-2-1 IoT 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-1.html>;

* + - * DAX20-0402-2-2 人工知能とロボット 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-2.html>;

* + - * DAX20-0402-2-3 クラウドコンピューティング 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-3.html>;

* + - * DAX20-0402-2-4 モバイルとウェアラブル 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-4.html>;

* + - * DAX20-0402-2-5 ITインフラストラクチャと仮想化 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-5.html>;

* + - * DAX20-0402-2-6 開発と運用 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-6.html>;

* + - * DAX20-0402-2-9 巻末　最新トレンドを理解するためのITの基礎知識 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-2-9.html>;

* + - * DAX20-0402-99 InnovationRoadmap2030 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-99.html>;

* + 1. DAX20-0402-3
       - DAX10-20 Society5.0に向けた人材育成【文科省】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX10-20.html>;

* + - * **DAX20-0402-3 IT人材白書2018 【MindManager→html】**【SK2】

****

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-3.html>;

* + - * DAX20-0402-3-1 Society 5.0 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-3-1.html>;

* + - * **DAX20-0402-3-3 プログラミング＆リベラルアーツ【2018年5月12日週刊ダイヤモンド】 【MindManager→html】**【SK2】

****

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-3-3.html>;

* + - * DAX20-0402-3-4 サイバー経済を生き残る法【2018年4月30日PRESIDENT大前研一】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX20-0402-3-4.html>;

* + 1. DAX21
       - **DAX21\_デジタルトランスフォーメーション（DX） 【MindManager→html】**【SK2】

****

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX21.html>;

* + 1. DAX22AI・データの利用契約
       - 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） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX22-01.html>;

* + - * DAX22-02 AI・データの利用に関する契約ガイドライン（データ編） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX22-02.html>;

* + - * DAX22-03 AI・データの利用に関する契約ガイドライン（AI編） 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX22-03.html>;

* + 1. DAX43
       - **DAX43-01 デジタルアーカイブの過去から未来 【MindManager→html】**【SK2】

****

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX43-01.html>;

* + - * 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 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX43-01-1.html>;

* + - * DAX43-90知の共有化に関連するキーワードと関連 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX43-90.html>;

* + 1. DAX46
       - **DAX46-01次世代情報システム構築フレームワーク 【MindManager→html】**【SK2】

****

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX46-01.html>;

* + 1. DAX47【2020年新規】
       - **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」 【MindManager→html】**【SK2】

****

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX47-01.html>;

* + 1. DAX48【2020年新規】
       - **DAX48-01\_2020\_図書館情報学研究(図書館システム・オープンデータ)要約版 【PPTX→Mindmanager→html】【SK2】**

****

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX48-01_2020.html>;

* + - * DAX48-10\_2015\_見たことのない図書館を考える【2015年1月10日同志社大学】 【PPTX→Mindmanager→html】【SK2】



参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/DAX48-10_2015.html>;

* 1. **デジタルアーカイブジャパン（ナショナルアーカイブ・次世代図書館サービス）**
     1. Bib10-0602「未来の図書館を作るとは」（長尾元館長）で示されたこと【全編】 【MindManager→html】【SK2】



参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib10-0602.html>;

* + 1. Bib10-01情報化社会の進展と次世代情報システム【枠のみ】
    2. Bib03-03知識インフラ構築の一翼を担う 組織の活動 【MindManager→html】【SK2】



参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib03-03.html>;

* + 1. Bib03-07MLAサービスシステム構築に向けた外部機関の支援【期待】 【MindManager→html】【SK2】

参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib03-07.html>;

* + 1. Bib10-06AIを活用した知の共有化の進展への期待 【要約】 【MindManager→html】【SK2】



参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib10-06.html>;

* + 1. Bib10-07次世代図書館サービスの実現形でのタスクと必要なスキル・知識【詳細】 【変換エラーのため、xmind→html】



参照:

<https://bluemoon55.github.io/Sharing_Knowledge/Digital_Archives/Deliverables/mind2html/Bib10-07%20次世代図書館サービスの実現形でのタスクと必要なスキル・知識【詳細】.html>;

* + 1. 国の施策
       - Bib10-08\_2016年度までの国等の情報政策 【MindManager→html】

参照:

[Page not found &middot; GitHub Pages](https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib10-08_2016.html);

* + - * Bib10-08「知の共有化」に関連した国等の政策の要約 【MindManager→html】【SK2】



参照:

<https://bluemoon55.github.io/Sharing_Knowledge2/MindManager2/Bib10-08.html>;

* + - * 【旧版】【XMIND】Bib03-09知財計画2015
      * 【旧版】【XMIND】Bib06-08国の情報政策
  1. **参考文献等へのリンク**

****

リレーションシップ:

開始点 [【2020年7月30日】2020年7月に収集精査した文献及び記事の追加](#Aksa61RMNkWVtGspHf5TRw==);

* + 1. 【2020年7月2日時点でDAX95内「参考文献等へのリンク」に未反映】
    2. 専門員リストアップ未整理分
       - PDF版
         * 早出氏

スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン（案）【2020年8月3日METI】

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

Draft SP 800-172: Enhanced Security Reqs for CUI | CSRC

参照:

<https://csrc.nist.gov/News/2020/draft-sp-800-172-enhanced-security-cui>;

ユーザのための要件定義ガイド 第2版要件定義を成功に導く128の勘どころ【2020年9月28日IPA】

* + - * + 石井氏

「AI利活用ハンドブック～AIをかしこく使いこなすために～」(パンフレット版)【2020年7月消費者庁】

参照:

[「AI利活用ハンドブック～AIをかしこく使いこなすために～」の公表について | 消費者庁](https://www.caa.go.jp/notice/entry/020727/);

インターネットトラブル事例集（2020年版）

ニューヨークだより2020年9月号「アメリカにおけるデジタルトランスフォーメーション（DX）の現状」

* + - * 電子書籍版
        + 石井氏

ゼロトラストネットワークとは？仕組みやメリットデメリットについて徹底解説

参照:

[ゼロトラストネットワークとは？仕組みやメリットデメリットについて徹底解説](https://cybersecurity-jp.com/security-measures/33227);

* + - * 所在情報のみ
        + 石井氏

政府情報システムにおけるゼロトラスト適用に向けた考え方

参照:

[政府情報システムにおけるゼロトラスト適用に向けた考え方 | 政府CIOポータル](https://cio.go.jp/dp2020_03);

SP800-207 Second Draft（ゼロトラスト）

参照:

[SP 800-207 (Draft), Zero Trust Architecture | CSRC](https://csrc.nist.gov/publications/detail/sp/800-207/draft);

* + 1. 2020年2期追加分（本文ファイル取り込み済）

リレーションシップ:

開始点 [【2020年7月2～3日】2020年1月から6月までに収集精査した文献及び記事の追加](#X9pFcC/uZk+/tDPNjltRtg==);

* + - * 電子書籍形式
        + サイバー保険を活用するための7つのポイント｜Q&A形式で解説



参照:

[サイバー保険を活用するための7つのポイント｜Q&amp;A形式で解説](https://www.secure-sketch.com/blog/cyber-insurance-tips);

* + - * + 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】



* + - * + Web会議サービスを使用する際のセキュリティ上の注意事項【2020年7月14日IPA】



* + - * + IPv6セキュリティ ～問題点と対策～ - JPNIC



* + - * + Zero Trustの大本命 SDPについて【2019年9月20日C&S\_Enngineer\_Voice】



* + - * + 【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口【2020年4月27日IPA】



* + - * + E2272 - データサイエンス，機械学習，AIの責任ある運用のために | カレントアウェアネス・ポータル



* + - * + 生徒向けの使えるリンク集が「学校図書館の自殺行為」と言われた ～ 学校図書館の存在意義とデジタルトランスフォーメーション（DX） | HON.jp News Blog



* + - * + テレワークが暴いた“不都合な真実”　ポスト・コロナに「中間管理職」がごっそり淘汰されるワケ：時事ドットコム



* + - * + AIがデジタルトランスフォーメーションの起爆剤に？“ミニDX”から始める企業変革【2020年5月29日ITmedia】



* + - * + テレワークだからこそ知っておきたいラテラルフィッシング 狙われるMicrosoft 365｜Digital Arts Security Reports｜デジタルアーツ株式会社



* + - * + 新しい情報サービスのかたちを目指しています | よむナガノ 県立長野図書館ブログ



* + - * + NTTドコモ「おサイフケータイのタッチレス対応」の成果と課題、今後目指す世界は？ | ペイメントナビ



* + - * + 世界の電子認証基準が変わる：NIST SP800-63-3を読み解く



* + - * + いまからでも知っておきたい５G元年のセキュリティ対策 | ミツイワ株式会社



* + - * + アメリカの図書館はコロナ禍にどう立ち向かっているか？ | HON.jp News Blog



* + - * + 複雑で強いのに忘れにくいパスワードの作り方と、正しい管理法 japan.norton.com



* + - * + 人工知能と人間のよりよい共生のために rad-it21.com



* + - * + 「イノベーションを推進できる人材は従来のスキルマップにいない」　ガートナー



* + - * + 説明可能なAIとは？　Googleの「Explainable AI」に触れながら解説 | Ledge.ai



* + - * + 地方都市では「10Gbps」がCATVで広がる！ あなたの街でも“裏メニュー”で提供中かも!?　同軸から光への移行で進化するケーブルテレビ網 internet.watch.impress.co.jp



* + - * 通常ファイル
        + テレワークを行う際のセキュリティ上の注意事項【2020年7月15日改訂IPA】



参照:

[テレワークを行う際のセキュリティ上の注意事項：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/security/announce/telework.html);

テレワークを行う際のセキュリティ上の注意事項

所属する組織や企業からテレワーク環境が提供されている場合

所属する組織や企業からテレワーク環境が提供されていない場合

修正プログラムの適用

セキュリティソフトの導入および定義ファイルの最新化

パスワードの適切な設定と管理

不審なメールに注意

USBメモリ等の取り扱いの注意

社内ネットワークへの機器接続ルールの遵守

ソフトウェアをインストールする際の注意

パソコン等の画面ロック機能の設定

テレワーク時に特に気をつけるべき注意事項

テレワークを始める前に

テレワークで使用するパソコン等は、できる限り他人と共有して使わないようにしてください。共有で使わざるを得ない場合は、業務用のユーザーアカウントを別途作成してください。

ウェブ会議のサービス等を新たに使い始める際は、事前にそのサービス等の初期設定の内容を確認してください。特にセキュリティ機能は積極的に活用してください。

自宅で行う場合

自宅のルータは、メーカーのサイトを確認のうえ、最新のファームウェアを適用（ソフトウェア更新）（\*1）してください。

公共の場で行う場合

カフェ等の公共の場所でパソコン等を使用するときはパソコンの画面をのぞかれないように注意してください。

公共の場所でウェブ会議を行う場合は、話し声が他の人に聞こえないように注意してください。

公衆Wi-Fiを利用する場合は、パソコンのファイル共有機能をオフ（\*2）にしてください。

公衆Wi-Fiを利用する場合は、必要に応じて信頼できるVPNサービス（\*3）を利用してください。

デジタルデータ／ファイルだけではなく、紙の書類等の管理にも注意してください。

* + - * + NISC第25回会合【2020年7月21日】

参照:

[�T�C�o�[�Z�L�����e�B�헪�{��](https://www.nisc.go.jp/conference/cs/index.html);

サイバーセキュリティ2020（2019年度年次報告・2020年度年次計画）【2020年7月21日NISC】



サイバーセキュリティ関係施策に関する令和３年度予算重点化方針（案）



政府機関等の情報セキュリティ対策のための統一基準群の見直し（骨子）



政府情報システムのためのセキュリティ評価制度（ISMAP）の取組状況について



委託先等で発生した政府機関の要保護情報に係るセキュリティインシデントの情報共有に関する申合せについて



IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せの改正について



東京2020大会に向けた取組状況について



サイバーセキュリティ協議会の取組状況



2020年サイバーセキュリティ月間 結果報告



* + - * + 中小企業は大企業に比べてサイバー攻撃への対策が不十分 - 専門家が警鐘



参照:

[中小企業は大企業に比べてサイバー攻撃への対策が不十分 - 専門家が警鐘 | マイナビニュース](https://news.mynavi.jp/article/20200725-1169679/);

Mimecastは7月20日(米国時間)、公式ブログ「Why SMBs Are Under-Prepared for Cyberattacks｜Mimecast Blog」で、中小企業は大企業に比べてサイバー攻撃に対する十分な対策を行えておらず、もし攻撃者に狙われたら重大な被害がもたらさられるおそれがあると警告している。公式ブログでは、中小企業が十分なセキュリティ対策を行えない理由を分析した上で、限られた予算でサイバーレジリエンス(回復力)を高める方法について紹介している。

Mimecastによると、サイバー攻撃の43％が中小企業を対象にしているという調査結果があるにもかかわらず、大企業に比べてこれらを防止するための対策が不十分なことが多く、セキュリティプログラムを構築する計画すらないケースもあるとのこと。これらの準備不足な企業がサイバー攻撃に遭った場合、データ侵害などによって壊滅的な被害を被る危険性があり、対策の強化は必須の課題と言える。

しかし現実には、中小企業がサイバー攻撃への対策を強化できないさまざまな要因がある。例えば、ITスタッフ数が足りなかったり、予算が少ないためにセキュリティやバックアップの手順が洗練されていかったりすることなどが挙げられる。また、従業員のセキュリティに対する認識が不足しており、ソーシャルエンジニアリング攻撃やフィッシング詐欺の被害に遭うリスクが高いということもある。

そこでMimecastでは、中小企業が限られた予算内でセキュリティ対策を強化するために、次のような方法を提案している。

従業員のセキュリティ意識向上のためのトレーニングを実施する

出張や旅行中のサイバーリスクについて従業員を教育し、可能な限り出張前にデバイスから機密データを削除する

サードパーティの接続を監視し、ビジネスパートナーから受けるセキュリティ上の脅威を評価する

リスクと脆弱性の評価および発見を支援する外部のコンサルタントを雇う

サイバー攻撃のインシデントに対する対応計画を作成する

ベストプラクティスを含むサイバーセキュリティポリシーを設定する

ソフトウェアを迅速に更新する

リモートの作業員がファイアウォールで保護されていることを確認する

基本的な戦略としては、電子メールのセキュリティやマルウェアの保護、バックアップなどを行うクラウドベースのセキュリティ製品を採用することを挙げている。それに加えて、上記のような対策を行うことで、サイバー攻撃に対するリスクを大幅に軽減できるとのことだ。

* + - * + 在宅勤務に3つの脅威\_サイバー攻撃にどう備える【2020年7月27日日経新聞】



参照:

[在宅勤務に3つの脅威　サイバー攻撃にどう備える　　:日本経済新聞](https://www.nikkei.com/article/DGXMZO61875010S0A720C2X11000/);

* + - * + 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】



参照:

[�����ȁb�uIoT�E5G�Z�L�����e�B�����΍� �v���O���X���|�[�g2020�v�̌��\](https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00068.html);

* + - * + 重要インフラ専門調査会第22回会合



参照:

[�d�v�C���t����咲����](https://www.nisc.go.jp/conference/cs/ciip/index.html);

「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく情報共有の手引書【2013年7月13日NISC】



重要インフラを取り巻く情勢について【2013年7月13日NISC】



関係省庁の取組状況について【2013年7月13日NISC】



* + - * + サイバー被害 通知義務化\_個人情報漏洩の全員に　企業の対応不可避【2020年7月16日日経】



* + - * + Web会議サービスを使用する際のセキュリティ上の注意事項【2020年7月14日IPA】



* + - * + 政府情報システムの整備及び管理に関する標準ガイドライン【2014年12月3日政府CIO】



参照:

<https://www.soumu.go.jp/main_content/000325350.pdf>;

* + - * + 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



参照:

[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](https://www.pwc.com/jp/ja/knowledge/column/spa/vol29.html)

;

* + - * + 中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた実現可能性調査成果報告書【2020年4月14日IPA】



* + - * + 中小企業向けサイバーセキュリティ製品・サービスに関する情報提供プラットフォーム構築に向けた実現可能性調査成果報告書（概要版スライド）【2020年4月14日IPA】



* + - * + DX 推進指標 自己診断結果 分析レポート【2020年5月28日IPA】



* + - * + Wi-Fi利用者向け 簡易マニュアル（令和2年5月版）【2020年5月総務省】



* + - * + Wi-Fi提供者向け セキュリティ対策の手引き（令和2年5月版）【2020年5月総務省】



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



* + - * + NIST SP 800-113 Guide to SSL VPNs



* + - * + ビジネスメール詐欺の実態調査報告書【2020年3月25日JPCERTCC】



* + - * + 証拠保全ガイドライン第８版【2019年12月9日デジタル・フォレンジック研究会】



* + - * + 政府情報システムのためのセキュリティ評価制度（ISMAP）について【2020年6月3日内閣官房・総務省・経済産業省】



* + - * + サイバー攻撃の現状【公安調査庁2020】



* + - * + 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-実証参加企業事例集-【2020年4月21日IPA】



* + - * + 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（概要版）-【2020年4月21日IPA】



* + - * + 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（全体版）-【2020年4月21日IPA】



* + - * + テレワーク等への継続的な取組に際してセキュリティ上留意すべき点について【2020年6月11日NISC】telework20200611



* + - * + 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（本文）【2020年6月12日METI】



* + - * + プラットフォーム変革手引書案について【2020年6月NEDO】



* + 1. 2020年2期（現在46文献）
       - 図らずもテレワーク普及で企業のデジタルトランスフォーメーションが一気に推進【2020年6月5日野村直之】



* + - * サイバーセキュリティにおけるAI活用の最先端【2020年6月5日ZDNet】



* + - * ebook-remote-playbook



* + - * 成長戦略による変革後の生活・現場(Society 5.0)【2017年5月30日未来投資会議】siryou1

 

* + - * + イメージ図〜⾰新的技術を活かして⼀⼈⼀⼈のニーズに合わせたサービス提供による社会課題の解決と成⻑のフロンティア〜
      * 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】

 

* + - * + フィッシング対策協議会からの公式ガイドライン
      * サイバーセキュリティ経営ガイドライン Ver2.0実践のためのプラクティス集【2020年6月3日IPA】

 

* + - * + サイバーセキュリティ経営ガイドライン Ver2.0に対応したプラクティスの改訂版
      * 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【202年4月9日NISC】

 

* + - * + コロナウイルス対策に対応したテレワークでの留意点
        + 資料１ 政府機関等におけるテレワークにかかる留意事項（注意喚起）
        + 資料２ 重要インフラ事業者等におけるテレワークにかかる留意事項（注意喚起）
        + 資料３ テレワーク実施者の方へ ～あなたのセキュリティは大丈夫ですか？～
        + 資料４ テレワークにかかる留意事項（情報共有）
      * アジャイル開発が支えるDXの取り組み200521\_agile【ZDNet】



* + - * 在宅勤務用ネットワークの45％にマルウェア発見　テレワークはなぜ危険か【2020年5月31日TechTarget】



* + - * AIがデジタルトランスフォーメーションの起爆剤に？“ミニDX”から始める企業変革【2020年5月29日ITmedia】



* + - * いまさら聞けない「コンテナ」と「仮想マシン」の根本的な違いとは？【2020年5月22日TechTarget】



* + - * IoT・5Gセキュリティ総合対策【2019年8月総務省】

 

* + - * + 本文書は、今般、「IoTセキュリティ総合対策」策定・公表後の様々な状況変化などを踏まえつつ、IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方について検討し、「IoT・5Gセキュリティ総合対策」として整理したものである。
      * 「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」調査報告 【2020年5月15日IPA】

 

参照:

[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：IPA 独立行政法人 情報処理推進機構](https://www.ipa.go.jp/ikc/reports/20200514_1.html);

* + - * + 企業におけるDX取組状況や先進事例、及び先端デジタル領域において不足が懸念されるIT人材の学び直しや流動実態等の調査を実施し、その結果を報告書として公開
        + 報告書ポイント
        + 報告書概要編
        + 報告書詳細編
      * インターネットの安全・安心ハンドブックVer4.10【2020年4月20日NISC】

 

* + 1. 2020年1期（129文献）
       - 自治体の偽サイト相次ぐ、給付金で各機関が注意喚起【2020年5月14日 日本経済新聞】



* + - * ゼロから学べるテレワーク導入完全ガイド【V-CUBE】



* + - * Web制作要件シート【2020年3月25日Lancers】



* + - * NTTドコモが300の実証から見いだした、5Gビジネスでも「高速大容量」が重要な理由【2020年3月17日ITMedia】



* + - * 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【2020年3月26日IPA】

 

* + - * AI社会実装推進調査報告書【2018年6月19日IPA】

 

* + - * + スライド形式
      * 「これからの人材のスキル変革を考える～DX時代を迎えて～」【2019年7月4日IPA】

 

* + - * + スライド形式
      * 5G・新サービス・新商品発表会【2020年3月18日DOCOMO】

 

* + - * + スライド形式
      * サイバーセキュリティ人材育成取組方針～事業継続と価値創出に向けた産学官連携の推進～【2020年3月18日NISC】

 

* + - * + セキュリティマインドを持った企業経営ワーキンググループ報告書～事業継続と価値創出に向けた産学官連携の推進～

参照:

<https://www.nisc.go.jp/conference/cs/pdf/jinzai-keiei2018set.pdf>;

* + - * + サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書 ～「戦略マネジメント層」の育成・定着に向けて～

参照:

<https://www.nisc.go.jp/conference/cs/pdf/jinzai-sesaku2018set.pdf>;

* + - * 日本企業の8割が「2025年の崖」から転落すると、有識者が口をそろえる理由【2020年3月17日日経XTECH】



* + - * IoT・アナリティクス時代におけるスマートシティの実現方法を考える【2020年3月18日ジョンソンコントロールズ】



* + - * 情報セキュリティ10大脅威2020【2020年3月10日IPA】

 

* + - * 情報セキュリティ10大脅威2020各脅威の解説資料【2020年2月IPA】

 

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

 

* + - * + デジタルトランスフォーメーション、略してDXがホットワードになっており、企業はデジタル、データでビジネスを変革する必要に迫られています。既にこれによりデジタルビジネスの成功を収めた企業も出てきており、今後もこの流れがしばらく続きそうです。
        + 一方、近年ではIT技術の急速な成長に法規制が追い付いておらず、プライバシー侵害が問題になるケースも多く見受けられました。
        + そんな中、エポックメーキングな出来事となったのが、2018年5月のGDPR (EU一般データ保護規則)の施行です。以降、プライバシー侵害に高額な制裁金が科されるようになり、カリフォルニア州消費者プライバシー法(CCPA)発効等、各国もGDPRに追随するようになってきました。ISO27701:2019のような統一規格も出てきています。つまり、データを攻めに活用する際、適切な管理を求められるようになってきたということです。
        + この流れの中、2020年1月16日に米国国立標準技術研究所(NIST)がプライバシーフレームワーク 1.0 (以下、NIST PF)を策定しました。NIST PFは法規制でも認証でもない参考とすべきフレームワークという位置づけであり、必須で遵守すべきものではないのですが、NIST サイバーセキュリティフレームワーク(NIST CSF)のように、世界中で参考にされることが見込まれます。
      * 監査人の警鐘-2020年情報セキュリティ十大トレンド【2020年1月6日JASA】

 

* + - * 「イノベーションを推進できる人材は従来のスキルマップにいない」　ガートナー



* + - * ドイツBSI「産業用制御システム（ICS）のセキュリティ -10大脅威と対策2019-」【2020年1月14日IPA】

 

* + - * サイバーセキュリティ関係法令\_Q&AハンドブックVer1.0【2020年3月2日NISC】

 

* + - * ～情報システム・モデル取引契約書～第一版及び追補\_DX推進のため見直しにおける民法改正を踏まえた整理にあたって【2019年12月IPA】

 

* + - * + 各種ドキュメントあり
      * DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～【2019年7月4日IPA】

  

* + - * + （簡易版スライド）
        + （サマリー版スライド）
        + 本文
      * DX推進指標とそのガイダンス【2019年7月31日METI】

 

* + - * DX推進指標【2019年7月31日METI】

 

* + - * + DX推進指標とそのガイダンス【2019年7月31日METI】
        + DX推進における取締役会の実効性評価項目【2019年7月31日METI】
        + DX推進指標サマリー【2019年7月31日METI】
      * 「３つのシティ」実現に向けた政策の強化（2020年度）～2020年に向けた実行プラン～【2020年1月東京都】kyouka2020\_zentai

 

* + - * インターネット白書2019

 

* + - * + iwp2019-ch01-01-p041\_電子出版ビジネス-デジタル化を経て情報化へと転換する時機の到来
        + iwp2019-ch00-01-p001\_10大キーワードで読む2019年のインターネット
        + iwp2019-ch01-01-p022\_2018年のテレビとインターネットの動き
      * 2018年冬季オリンピックに関連して発生する可能性のあるサイバー攻撃及びその背景【2018年2月名和利男】



* + - * NIST SP 1800-4a\_Mobile Device Security Cloud and Hybrid Builds

 

* + - * コンピュータウイルス・不正アクセスの届出事例［2019年下半期（7月～12月）］【IPA】



* + - * 新春大予測\_20の「未来」展望、2020年の日本はこうなる【20200109日経コンピュータ】



* + - * 大競争時代のビジネスを勝ち抜く2020年の展望【日経BP総研イノベーションICTラボ主催セミナー】20200206170136



* + - * 人工知能サミット2019Review【2019年11月21日】20200206165946



* + - * よくある事例から考える効果的なセキュリティ対策【MS垣内】20200207093448



* + - * 政府がセキュリティ対策に「緊急提言」……えっこのレベル？と思ったあなたへ【2020年02月04日ITMedia】



* + - * 「中小企業の経営者のサイバーリスク意識調査2019」【2020年1月日本損害保険協会】

 

* + - * デジタル・ガバメント実行計画【20191220閣議決定】

 

* + - * + 全体編
        + 本文
        + 別紙
      * 断絶のDX【20191226日経コンピュータ】



* + - * サイバーセキュリティインシデント対応演習【20200116東京都戦略政策情報推進本部】



* + - * 2020年は何を信じよう？　サイバーセキュリティのゆく年くる年【2019年12月24日ITMedia】



* + - * 非金融分野におけるブロックチェーンの活用動向調査報告書【2019年12月IPA】



* + - * + （概要版）
      * 超人間・万能AI～グーグルが変えるデジタル社会の未来～【日経コンピュータ】



* + - * 「疑わしくないメール」にも疑いの目を\_猛威を振るうマルウェア「Emotet」に注意



* + 1. 2019年2期（144文献）
       - 中小企業の情報セキュリティ対策ガイドライン（第3版）

 

* + - * なりすましメール拡散のウイルス、日本に本格上陸【20191201日経新聞】



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



* + - * docomo\_ar2019\_統合報告書（アニュアルレポート）



* + - * 2040 年に向けた高等教育のグランドデザイン（答申）【要旨】

 

* + - * 文部科学白書2018\_第11章\_ICTの活用の推進

 

* + - * 文部科学白書2018\_特集1\_2040年に向けた高等教育のグランドデザイン

 

* + - * サイバー空間を巡る脅威の情勢とサイバーセキュリティ対策【警視庁本所警察署】



* + - * 第12回コラボレーションプラットフォーム資料【2019年11月25日IPA】



* + - * 世界に通じるAI人材の育て方【日経コンピュータ】



* + - * サイバー犯罪の脅威と現状【警視庁五日市警察署セミナー】



* + - * 迷惑メール関係法令・窓口等【迷惑メール白書2019】

 

* + - * よくある事例から考える効果的なセキュリティ対策【20191118MS】



* + - * 普通のエンジニアでも分かるディープラーニング概説【itmedia】



* + - * 迷惑メール白書2019 参考編／資料編

 

* + - * サイバーセキュリティ国際シンポジウム\_Security\_Mesures\_in\_IoT\_5G\_Era



* + - * サイバー・フィジカル・セキュリティユースケース～分析対象の明確化の参考として～【METI】

 

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



* + - * 【鼎談】DX時代のセキュリティは「NIST」に対応しなければ始まらない 西尾素己氏×洞田慎一氏×石川滋人氏 対談｜ビジネス+IT

 

* + - * サイバーセキュリティ政策の最新動向【2019年2月12日総務省】

 

* + - * サイバーセキュリティ政策の最新動向【2019年2月12日総務省】

 

* + - * 団体向けリスクマネジメント普及啓発セミナー（情報セキュリティ）第３回【2019年9月9日東京都中小企業団体中央会】



* + - * 働き方改革関連法案と2015年の壁から読み解く「働き方改革最新事業」【2019年10月VAIO】

 

* + - * 警視庁サイバー犯罪対策課相談マニュアル【警視庁】

 

* + - * 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【2018年4月 NIST CSF Ver1.1 IPA対訳】

 

* + - * 不正ログイン対策のための『多要素認証サービス』設定手順書



* + - * + Microsoft アカウント編
        + Apple ID 編
        + Google アカウント編
      * AIなんて怖くない



* + - * 注意情報｜フィッシング詐欺メール【例】



* + - * サイバーセキュリティ基本法で押さえておくべきポイント \_ マルウェア情報局



* + - * サプライチェーン・サイバーセキュリティ等に関する海外の動き【2019年4月4日経済産業省 商務情報政策局サイバーセキュリティ課】

 



* + - * + スライド版
      * スマートフォンはPCよりも安全？ （前編）：フィッシングのリスクはPCの3倍　ニュースに出ない、モバイルセキュリティの怖い話



* + - * 「サイバー・フィジカル・セキュリティ対策フレームワーク」策定後のWG1の進め方（案）【2019年4月4日METIサイバーセキュリティ課】

 



* + - * + スライド版
      * Society5.0を支えるセキュアトラスト基盤【2018年2月21日産業競争力懇談会COCN】



* + - * Society5.0を支えるトラストサービスとトラス基盤【2019年4月17日慶応大学手塚悟】



* + - * システム開発プロジェクトに存在する複数種類の契約形態【2019年8月14日アットマークIT】



* + - * 中小企業を巡るサイバーセキュリティの現状とその対策2【2019年8月7日湯浅先生】



* + - * 第10回コラボレーション・プラットフォーム資料【2019年7月29日IPA】



* + - * 中小企業向けサイバーセキュリティ政策について【2019年6月METIサイバーセキュリティ課】

 

* + - * 中小企業向けサイバーセキュリティ政策について【2019年6月METIサイバーセキュリティ課】



* + - * 中小企業を巡るサイバーセキュリティの現状とその対策１【2019年8月2日湯浅先生】



* + - * ディープラーニングハンズオンセミナー【株式会社キカガク】

 

* + - * + スライド版
      * サイバーセキュリティ経営ガイドラインを実践するための経営プラクティス【スライド】【2019年4月23日IPA】

 



* + - * + スライド版
      * サプライチェーンに死角【2019年7月2日日本経済新聞】



* + - * これからのAIの話をしよう（コンサル編）：「機械に代替されないデータサイエンティスト」に必要な能力とは？



* + - * 「AIやIoTに惑わされてはいけない」、DXに挑む4人が語った理念 \_ 日経 xTECH（クロステック）



* + - * 『経営とIT、サイバーセキュリティ対策の動向調査』【2019年8月5日デジタルハーツ】



* + - * 【AIなら何でもできるんじゃないの？】人工知能の可能性とよくある「誤解」【2019年7月10日キャリコネ】



* + - * mdse(COPE)-nist-sp1800-21-draft



* + - * IoT・5G セキュリティ総合対策（パブコメ案）【2019年6月総務省】



* + - * IoTセキュリティ総合対策プログレスレポート2019【2019年5月サイバーセキュリティタスクフォース】

 



* + - * AIと雇用（下） 業務高度化通じ競争力向上【2019年7月4日日経新聞】



* + - * 2020年及びその後を見据えたサイバーセキュリティの在り方～サイバーセキュリティ戦略中間レビュー～

 



* + - * ISAC



* + - * + 1\_Security\_Measures\_in\_IoT\_5G\_Era
        + 3-1\_Financials\_ISAC\_Japan
        + 3-2\_Japan\_Electricity\_ISAC
        + 3-3\_Software\_ISAC
        + 3-5\_ICT-ISAC\_Japan
        + 4\_2\_Comm\_ISAC
      * mpower



* + - * + 1-1\_MPOWER\_米国国防総省が求める脅威インテリジェンスの世界.pdf
        + 1-5\_MPOWER\_ＤＸ時代の価値創造を支えるIoTサプライチェーンセキュリティ.pdf
        + 1-7\_MPOWER\_働き方改革待ったなし！残業せずにファイアウォールのポリシー管理をする方法とは？.pdf
        + 1-10\_MPOWER\_最近のセキュリティ脅威動向と、対抗するセキュリティソリューションのご提供.pdf
        + 2-5\_MPOWER\_大学間連携によるサイバーセキュリティ体制の強化.pdf
        + 2-6\_MPOWER\_再考、エンドポイントセキュリティ　～インシデント発生時に慌てないための要諦～.pdf
        + 2-7\_MPOWER\_NECが語るCASB運用 生の声.pdf
        + 2-8\_MPOWER\_マイクロソフトのクラウド戦略からひも解くIoT活用ポイント.pdf
        + 3-10\_MPOWER\_クレディセゾンにおけるDX実践の軌跡.pdf
        + 3-3\_MPOWER\_AIとセキュリティ.pdf
        + 3-5\_MPOWER\_交通ISAC\_活動状況と設立に向けた取り組みについて.pdf
        + 3-6\_MPOWER\_【事例セッション】クラウドの安全利用を促進するためのCASBを用いた業務設計と運用.pdf
        + 3-8\_MPOWER\_【事例セッション】ビル制御システムのセキュリティと経産省ガイドライン解説.pdf
        + 4-1\_MPOWER\_デジタルエンタープライズを実現するハイブリットクラウドのセキュリティ強化ポイント.pdf
        + 4-2\_MPOWER\_サプライチェーンセキュリティを向上させる４つの転換点と先進例.pdf
        + 4-5\_MPOWER\_電力の安定供給を支える「電力ＩＳＡＣ」の取り組み状況について.pdf
        + K-1\_MPOWER\_情報共有のすすめ～行う利点、持続的な活動のために重要こと～.pdf
        + LS-5\_MPOWER\_頭を悩ますセキュリティ運用。検出から対応までに必要な準備とは.pdf
        + LS-7\_MPOWER\_経営層が理解しておくべきデジタル時代のCybersecurity.pdf
        + LS-8\_MPOWER\_IoT5G時代におけるセキュリティの新しい考え⽅ 既存技術のフル活用術.pdf
        + LS-9\_\_MPOWER\_リスクベースセキュリティ：最新の脆弱性管理とユーザ行動分析.pdf
        + MS-6\_MPOWER\_どんどん増えるSaaS, IaaSへの攻撃と情報漏洩を見据えた運用と対策.pdf
        + MS-9\_MPOWER\_日本の産業サイバーセキュリティの現在地とこれから.pdf
    1. 2019年1期（191文献）
       - ソネット防災マニュアル



* + - * 経済財政運営と改革の基本方針2019【2019年6月21日閣議決定】



* + - * + 【概要スライド】
      * 成長戦略実行計画案【2019年6月21日未来投資会議】



* + - * 「未来投資戦略2018」(概要)【2018年6月未来投資会議】



* + - * 「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」【2019年4月IPA】



* + - * + （サマリー版）
        + （報告書本編）
        + （参考資料）
      * IoTセキュリティチェックリスト【2019年6月27JPCERT日】



* + - * + 解説図
        + 利用説明書
      * AI戦略2019～人・産業・地域・政府全てにAI～【2019年6月11日統合イノベーション戦略推進会議決定】



* + - * 2018年6月 文部科学省・経済産業省からの報告書・提言まとめ～これからの学びってどうなるの？～【2018年6月ZKAI】



* + - * サイバーインシデント緊急対応企業一覧\_NPO日本ネットワークセキュリティ協会



* + - * ランサムウエアの脅威動向および被害実態調査報告書1.0版【2018年7月30日JPCERT】



* + - * 社会人の学び直し（リカレント教育）とキャリア・アップ - 内閣府



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



* + - * サイバーセキュリティ対策情報開示の手引き （案） 【総務省】



* + - * Society5.0に向けた学校ver.3.0【文部科学省】



* + - * ディープラーニングは何ができる？　エンジニア以外も知っておきたい注意点【2019年6月5日ITMedia】



* + - * 平成30年におけるサイバー空間をめぐる脅威の情勢等について【2019年3月7日警察庁】



* + - * 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【2019年METI】



* + - * サイバー対策へ新庁を　自民提言、25年創設めざす　\_日本経済新聞



* + - * 「持続可能な開発目標」(SDGs)について【外務省】



* + - * 民法改正でシステム開発の何が変わるのか？３つのポイントを徹底解説【2017年8月28日TopCourt】



* + - * 社会の価値を創造するデータ駆動型社会【2015年6月GLOCOM】



* + - * （シンギュラリティーにっぽん）プロローグ　２０４５年　ＡＩ社会、共存は：朝日新聞デジタル



* + - * 電子書類データに公的認証、改ざん防ぎ信用担保【2019年1月30日日本経済新聞】



* + - * 警視庁様サイバーセキュリティセミナー意見交換会資料【2019年1月29日総務省関東総合通信局】



* + - * 詐欺メール対策リーフレット「そのメール、詐欺カモ！？」2019年度版【迷惑メール相談センター】



* + - * 進化するＡＩ、人との共生は　超高齢化の支え、持続可能な社会探る【2019年1月3日ASAHI】



* + - * 迫りくるデジタルディスラプションの波【2018年秋PWC】



* + - * 社会人に役立つ人工知能本 三冊しかない説【2018年6月5日マスクド・アナライズ】



* + - * 知財立国　遠い道のり（複眼）【2019年1月22日日経新聞】



* + - * 統合イノベーション戦略【2018年6月15日閣議決定】



* + - * 突然CISOに任命されたら？CISOがサンドバックにならないための事前準備【2019年1月7日ZDNet】



* + - * 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 - 総務省



* + - * 次期年次報告・計画の策定に向けた進め方等について（サイバーセキュリティ戦略本部第21回会合（平成31年１月24日）資料３）



* + - * 新産業構造ビジョン【スライド】【2017年METI】



* + - * + （概要版）【スライド】
        + （詳細版）【スライド】
      * 新たな情報通信技術戦略の在り方第3次中間答申（概要)【2017年総務省】



* + - * 政策討議（AI戦略）論点【スライド】【2018年2月1日内閣府】



* + - * 撃退！迷惑メール　2018年度版【迷惑メール相談センター】



* + - * 政府のIoT機器調査、無差別の「力業」に踏み切った背景は【2019年2月14日ITMedia】



* + - * 政府のサイバーセキュリティに関する予算【2019年1月24日サイバーセキュリティ戦略本部 】



* + - * 撃退！チェーンメール2019年度版【迷惑メール相談センター】



* + - * 情報リテラシー啓発のための羅針盤コンパス【2019年3月1日LAC】



* + - * + 参考スライド集
      * 平成30年度データ関連人材育成プログラム公募説明会配布資料【文科省】



* + - * 全体を通した論点と今後の方向性について【2018年3月第４次産業革命に対応したスキル標準検討WG】



* + - * 多くの企業でDXはまだ初期段階に、Dellが全世界を調査【20190206atmarkIT】



* + - * 多くの企業でDXはまだ初期段階に、Dellが全世界を調査【20190206atmarkIT】



* + - * 人工知能の研究開発目標と産業化のロードマップ【スライド】【2018年3月31日人工知能技術戦略会議】



* + - * 人工知能技術戦略実行計画（案）の概要【スライド】【2018年6月26日人工知能技術戦略会議事務局】



* + - * ブラウザにパスワードを保存するのはアリなのか？【2019年1月29日Bizコンパス】



* + - * メールの相手、本当は誰だ\_手の内を知って対策を【2018年12月20日日経コンピュータ】



* + - * ビジネスITにおけるPoCの重要性－確実なコンセプト検証のためのポイント－



* + - * データ活用時代に最もアツい職業「データサイエンティスト」になるには？必要なスキルセットをチェックしよう



* + - * データ利活用戦略による新たなフロンティアの開拓へ【2019年4月関西経済同友会】



* + - * + 【SummaryPPT】
        + 【文書】
      * データ・サイエンティストのブームは終焉を迎えるのか？ \_ Oracle 日本



* + - * データサイエンティストを目指して勉強した1年間まとめ - Qiita



* + - * データサイエンティストを目指すなら知っておきたい学習方法



* + - * データサイエンティストの定義は？必要スキルは？現役データエンジニア／アナリストと考えた結論 - エンジニアHub｜若手Webエンジニアのキャリアを考える！



* + - * デジタルトランスフォーメーション（ＤＸ）に向けたスキル変革の方向性



* + - * 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. 1.0【2018年12月12日METI】



* + - * デジタルトランスフォーメーション(DX)が既存市場と社会に影響を及ぼす3つの事例【2019年02月7日FINCH】



* + - * デジタルトランスフォーメーション【2018年11月20日BIZHINT】



* + - * 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】



* + - * サイバー対策、五輪前に　重要インフラに指針【2019年1月15日日本経済新聞】.pdf



* + - * サイバー・フィジカル・セキュリティ対策フレームワーク（パブコメ案）【2019年1月9日METI】



* + - * サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集【2019年3月25日IPA】



* + - * + 付録2：プラクティス一覧
      * サイバーセキュリティ戦略パンフレット【2018年7月NISC】

 

* + - * サイバーセキュリティ意識・行動強化プログラム～「参加・連携・協働」の実現を目指して～【2019年1月24日サイバーセキュリティ戦略本部 】

 

* + - * サイバーセキュリティ協議会について【スライド】【2019年4月1日NISC】

 

* + - * サイバーセキュリティ協議会の「規約」等の概要【2019年4月1日NISC】

 

* + - * コレ1枚で分かる「『デジタルトランスフォーメーション』の真意と『デジタライゼーション』との違い」【2019年01月18日atmarkIT】



* + - * インダストリー4.0成功の鍵【2018年秋PWC】

 

* + - * イノベーションを生み出す「デザイン思考」とは【2019年3月27日atmarkIT】



* + - * 【冊子】Strategy＆ Foresight vol.17 2018 Autumn ～特集：インダストリー4.0 成功の鍵【2018-11-28 PwC Japan】

 

* + - * 「デザイン思考でデジタル変革する」って何するの？　最初の一歩とは【2019年3月27日atmarkIT】



* + - * 「企業IT利活用動向調査2019」速報結果～GDPR未対応企業が3割超に上り、個人情報のグローバル対応が課題に。インシデント認知率ではWeb不正アクセスとなりすましメールが増加【2019-03-27JIPDEC】

 

* + - * 「むしろスキルがなければ給与が下がる可能性」、求められるデータサイエンティスト人材になる方法論をプロにイチからいろいろ聞いてみた - GIGAZINE



* + - * 「IoTセキュリティ総合対策」について【2018年2月28日総務省情報流通行政局サイバーセキュリティ課】

 

* + - * NICT法附則第8条第2項に規定する業務の実施に関する計画の認可申請の概要【スライド】【2019年1月総務省サイバーセキュリティ統括官室】

 

* + - * Mostly\_Harmless：SIerからユーザー企業へ　いよいよ始まった“IT人材の大移動”はDX推進の起爆剤となるか？



* + - * IT人材の今と未来（IT人材白書別冊）【2017年6月IPA】

 

* + - * AI社会実装推進調査報告書【2018年6月19日IPA】

 

* + - * AI時代は人事評価の再考が必要\_画一的な成果主義は適さない【2018年12月20日日経コンピュータ】



* + - * AI人材の実態【2018年12月20日日経コンピュータ】



* + - * AI・データの利用に関する契約ガイドライン【2018年6月METI】



* + - * + （概要資料）
        + （全体編）
        + （AI編）
        + （データ編）
      * 2019年版：データサイエンティスト・機械学習エンジニアのスキル要件、そして期待されるバックグラウンドについて - 六本木で働くデータサイエンティストのブログ



* + - * 2020年に向けて企業が開始すべきIT関連行動、ガートナージャパンが4つのポイントを発表【2019年3月26日atmarkIT】



* + - * 2019年度経済産業省IT関連施策について～Society5.0実現に向けたイノベーション環境の整備～【2019年1月METI大臣官房政策企画委員】

 



* + - * + スライド
      * 2019年度経済産業省IT関連施策について～Society5.0実現に向けたイノベーション環境の整備～【2019年1月METI大臣官房政策企画委員】

 

* + - * + 講演録
      * 2018年セキュリティ重大ニュース【2018年12月25日SO-NETセキュリティ通信】



* + - * 【書籍】InDesign操作とデザインの教科書



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

 



* + - * + （第1版）
        + k2opt
        + ＜参考＞オリパラ向けリスクアセスメント・ガイドラインとの関係について
        + 別紙１ 業務の阻害につながる事象の結果の例
        + 別紙２ 結果を生じ得る事象（脅威）の例
        + 別紙３\_様式１ リスクアセスメントの実施目的の確認
        + 別紙３\_様式２ 優先サービスの選定
        + 別紙３\_様式３ 優先サービスの影響度分析
        + 別紙４ リスク源の例
      * 重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第1版）別紙４ リスク源の例



* + - * サイバー・フィジカル・セキュリティ対策フレームワーク【2019年4月18日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(案)のパブリックコメントで寄せられた御意見に対する考え方【2019年4月18日METI】
        + 【全編】
        + ポイント
        + 概要
        + サブトピック
        + サイバーフィジカルシステム(CPS)とは【analytics-news.jp】
    1. 2018年2期（260文献）
       - （けいざい＋）情報銀行：上　自分で決めて情報提供：朝日新聞デジタル



* + - * （けいざい＋）情報銀行：下　記憶より詳細、管理に課題：朝日新聞デジタル



* + - * （変わる安全保障　防衛大綱改定）サイバー空間、米朝攻防　ウイルスで世界混乱、米がハッカー訴追：朝日新聞デジタル



* + - * 「AI」と「機械学習」は何がどのように違うのか？【2018年11月28日Gigazine】



* + - * 「IoTセキュリティ基盤を活用した安心安全な社会の実現に向けた実証実験」の結果の公表【2018年6月総務省情報流通⾏政局サイバーセキュリティ課】



* + - * 「インターネットの安全・安心に関する世論調査」の概要【2018年11月内閣府政府広報室】



* + - * 「つながる世界」を破綻させないためのセキュアなIoT製品開発13のステップ【2017年5月CSAジャパン】



* + - * 「連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド： セキュリティライフサイクルによるアプローチ」（NIST SP 800-37）【2010年2月NIST】

 

* + - * 【概要版】新産業構造ビジョン(PDF形式：2,781KB)【2017年5月30日METI】



* + - * 【図解】経産省300ページの“新産業構造ビジョン”を1分で理解[インフォグラフィック]



* + - * 60分でわかる！ディープラーニング最前線60分でわかる！\_IT知識



* + - * 2018年も「金銭狙い」で変化続けるフィッシング、最新の手口は【atmarkit】



* + - * 2019年セキュリティ予測\_WatchGuard\_Security\_Predictions\_for\_2019



* + - * 20181204203434【資料】産業分野におけるサイバーセキュリティ政策【METI】



* + - * AIは「単なる関数」、数学は「言語の一つ」、「文系出身」でも問題ない――Pythonで高校数学の範囲から学び始めよう【2018年10月10日ITMedia】



* + - * AI社会実装推進調査報告書【2018年6月22日IPA】



* + - * AI人材育成について【2018年4月4日未来投資会議 構造改革徹底推進会合】



* + - * CAIQ\_v3.0.1-09-01-2017\_FINAL【NIST】



* + - * CCDS 製品分野別セキュリティガイドライン\_v1.0【2017年5月29日CCDS セキュリティガイドラインWG】【NIST】



* + - * CISOハンドブックVer.1.1β【2018年5月JNSA】



* + - * CSA\_CCM\_v.3.0.1-09-01-2017\_FINAL【NIST】



* + - * CSA\_Guidance\_V4.0\_J\_V1.1\_20180724【NIST】



* + - * CSF Ver1.1【2018年4月NIST】



* + - * DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～【2018年9月21日METI】



* + - * + （サマリー）（PDF形式：1,301KB）
        + （簡易版）（PDF形式：2,693KB）
        + （本文）（PDF形式：4,895KB）
      * Guide to Industrial Control Systems (ICS) Security【NIST SP.800-82R2】【JPCERT和訳】



* + - * iaas\_technical\_evaluation\_guide\_v1



* + - * IoT へのサイバー攻撃仮想ストーリー集【2017年8月1日CSAジャパン】



* + - * 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】

 

* + - * IoTセキュリティのためのブロックチェーン技術の活用【2018年10月3日CSA】



* + - * IoTセキュリティ総合対策プログレスレポート2018【2018年7月サイバーセキュリティタスクフォース】

 

* + - * IoTにおけるブロックチェーンの適用可能性について【2017年日本総研】



* + - * IoT開発におけるセキュリティ設計の手引き【2018年4月IPA】



* + - * ITによる社会変革の歩み【概念図】【METI】004\_01\_01



* + - * NIST Special Publication 800-171r1 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【IPA和訳】

 

* + - * NIST.SP.800-181



* + - * NISTIR8200【2018年11月NIST】



* + - * NISTIR8202【2018年10月NIST】



* + - * NISTSP800-82r2\_20160314



* + - * NISTのサイバーセキュリティフレームワークVer1.1について

 

参照:

[54.NISTのサイバーセキュリティフレームワークVer1.1について : そこからセキュリティ　～セキュリティ管理者の小ネタの箱](http://sokokara-security.blog.jp/archives/26054653.html);

* + - * SEC BOOKS：「つながる世界の開発指針」の実践に向けた手引き［IoT高信頼化機能編］【2017年6月15日IPA】000059278



* + - * SEC BOOKS：「つながる世界の開発指針」の実践に向けた手引き［IoT高信頼化機能編］【2017年6月15日IPA】000059278



* + - * Society 5.0 に向けた人材育成～社会が変わる、学びが変わる～ （概要）【2018年7月MEXT】



* + - * Society 5.0 に向けた人材育成～社会が変わる、学びが変わる～ （本文）【2018年7月MEXT】



* + - * STOP! パスワード使い回し!キャンペーン2018【2018年8月JPCERTCC】



* + - * イノベーターのための最新のメモの取り方のガイド



* + - * ウェブサイト開設等における運営形態の選定方法に関する手引き第1.1版【2018年5月30日IPA】

 

* + - * クラウドサービス管理基準経済産業所省



* + - * 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】

 

* + - * クラウド化推進社会と政府のセキュリティ戦略【20181108NISC三角育生】

 

* + - * サイバー・フィジカル・セキュリティ対策フレームワーク（パブコメ案）【経済産業省サイバーセキュリティ課】



* + - * サイバーセキュリティ基本法の一部を改正する法律案【概要図】【2018年NISC】



* + - * サイバーセキュリティ経営ガイドラインVer 2.0【2017年11月16日METI】



* + - * サイバーセキュリティ経営ガイドライン解説書Ver.1.0 【2016年12月IPA】



* + - * サイバーセキュリティ戦略【2018年7月27日閣議決定】cs-senryaku2018

 

* + - * サイバーセキュリティ戦略・サイバーセキュリティ2018の概要【2018年7月27日閣議決定】cs-senryaku-cs2018-gaiyou

 

* + - * サイバーセキュリティ戦略の全体概要【2018年7月27日閣議決定】cs-senryaku2018-zentaigaiyou



* + - * サイバーセキュリティ戦略の詳細概要【2018年7月27日閣議決定】cs-senryaku2018-shousaigaiyou



* + - * サイバー攻撃、専守防衛は限界　「敵陣潜入」新潮流に【2018年10月31日日経新聞】



* + - * サプライチェーンサイバーセキュリティ等に関する海外の動き【2018年8月3日METIサイバーセキュリティ課】

 

* + - * サプライチェーンサイバーセキュリティ等に関する海外の動き【2018年8月3日METIサイバーセキュリティ課】



* + - * セキュリティインシデントに関する被害コスト調査【2018年8月28日トレンドマイクロ】



* + - * セキュリティプレゼンターカンファレンス2018



* + - * ディープラーニングで翻訳プログラムを0から作った人がその仕組みを複雑な数式ではなく図で解説するとこうなる【2018年10月12日gigazine】



* + - * データポータビリティとAIネットワーク社会【2018年12月10日生貝直人】



* + - * デジタル トランスフォーメーション：本当の原動力は、テクノロジではなく人間【Microsoft】



* + - * デジタル・トランスフォーメーション成功への羅針盤【2018年4月13日ダイヤモンドクオータリー】



* + - * デジタルトランスフォーメーション（ＤＸ）に向けたスキル変革の方向性（検討用）000065688



* + - * デジタルトランスフォーメーションとは？ 〜その定義と事例〜



* + - * デジタルトランスフォーメーションに必要な技術と人材【2018年IPA社会基盤センター】000067935



* + - * なぜ日本は人工知能研究で世界に勝てないか　東大・松尾豊さんが語る“根本的な原因”【2018年09月18日ITMedia】



* + - * なりすましECサイト対策マニュアル【2015年3月セーファインターネット協会】



* + - * なりすましメールからの保護【20181211トレンドマイクロ】



* + - * ビジネス担当者のための用語ガイド：IoT編【SAS】



* + - * 安全なIoTシステムの創出【2016年3月1日NISC】.pdf



* + - * 違法・有害情報相談センターへの相談資料一式



* + - * 汚職等非行防止ガイドブック（平成30年度版）【2018年7月コンプライアンス推進部】



* + - * 解説クラウド・セキュリティ・ガイダンス【2010年CSA】



* + - * 官民ITS構想・ロードマップ2018（案）【2018年6月内閣官房IT総合戦略室】



* + - * + （ポイント）
        + （本文）
      * 管理職向けサイバーセキュリティ研修資料【工学博士伊藤寛】



* + - * 危険な12の落とし穴　クラウドの重大セキュリティ脅威＋2017インシデント事例集【2018年5月CSAジャパン】



* + - * 経営リスク管理から考えるSecurity by Design【20181108NTT先端技術三宅功】

 

* + - * 工場における産業用 IoT 導入のためのセキュリティ ファーストステップ【2018年8月JPCERTCC】



* + - * 講習能力養成セミナー2018【2018年8月6日IPA】



* + - * 産業サイバーセキュリティ強化へ向けたアクションプラン【2018年5月30日METI産業サイバーセキュリティ研究会（第2回）】



* + - * 産業分野におけるサイバーセキュリティ【20181108METI奥家敏和】



* + - * 次期サイバーセキュリティ戦略骨子【2018年7月内閣府】



* + - * 終わる「セキュリティ至上主義」、拡がる「セキュリティ格差社会」【2018年11月2日】



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



* + - * 重要生活機器の脅威の事例集 Ver.1.2【2015年9月1日一般社団法人重要生活機器連携セキュリティ協議会（CCDS）事務局】CCDS\_CaseStudies\_v1\_2



* + - * 乗っ取り＆詐欺新防衛術32【2018年8月日経PC21】



* + - * 情報セキュリティに関わる利点、リスクおよび推奨事項【2009年IPA翻訳】



* + - * 情報漏えいを防ぐためのモバイルデバイス等設定マニュアル－実践編【2018年9月4日IPA】



* + - * + －AcrobatDC-Acrobat2017 での設定方法
        + －Office2016－Office365での設定方法
        + －Windows10 での設定方法
      * 人工知能の研究開発目標と産業化のロードマップ【2017年3月31日人工知能技術戦略会議】100862412



* + - * 人工知能の社会実装イメージイラスト【スライド】【NEDO作成】100867494



* + - * 人工知能開発は「儲けないと意味がない」　東大・松尾豊さんが見た“絶望と希望”



* + - * 人工知能技術戦略（とりまとめ）【2017年3月31日人工知能技術戦略会議】100862413



* + - * 人工知能技術戦略実行計画【表】【2018年8月17日内閣府人工知能技術戦略会議】keikaku



* + - * 人手での対応は限界、5G時代のサイバー攻撃対策に「自動化」が必要な理由【2018年10月4日ビジネスIT】



* + - * 世界最先端デジタル国家創造宣言・官民データ活用推進基本計画（案）【2018年6月IT戦略本部】



* + - * + （案）（概要）
        + （案）及び別表（案）
      * 制御システム セーフティ・セキュリティ要件検討ガイド【2018年3月19日IPA】000064729



* + - * + （ケーススタディ編）（1.83MB）
        + （基本編）（4.79MB）
      * 制御システムセキュリティ運用ガイドライン2017年改訂版【日本電気制御機器工業会】



* + - * 制御システムのセキュリティリスク分析ガイド（8.33MB）【2018年10月16日IPA】000069436



* + - * 成長戦略の方向性（案）【2018年10月5日内閣官房日本経済再生総合事務局】



* + - * 政府機関等の対策基準策定のためのガイドライン （平成 30 年度版）【2018年7月25日NISC】



* + - * 対話AIビジネス業界の俯瞰図（出典：慶應義塾大学環境情報学部 山口真吾 教授）



* + - * 第5回「2018年のセキュリティ事件に関する意識調査」【mcafee2018】



* + - * 第５期科学技術基本計画の概要5gaiyo



* + - * 知財のビジネス価値評価検討タスクフォース報告書～ 経営をデザインする ～【2018年5月12日知財のビジネス価値評価検討タスクフォース】houkokusho



* + - * + 【テキスト】
        + 【スライド】
      * 知的財産計画2018【2018年6月12日知的財産戦略本部】chizaikeikaku2018



* + - * + 【本文】
        + 【概要】【スライド】
      * 知的財産戦略ビジョン 【2018年6月12日内閣府知的財産戦略推進事務局】chizai2018\_smmry



* + - * + （サマリー）
        + （「価値デザイン社会」における人やビジネスのイメージ例）【スライド】
        + 「価値デザイン社会」を目指して～【本文】
        + エグゼクティブサマリー【テキスト】
        + 知的財産戦略ビジョン及び知的財産推進計画2018のポイント【スライド】【2018年6月12日知的財産戦略本部】chizai2018\_point
      * 著作権の保護と制限の規定がもうすぐ変わる【20181113hon.jp】



* + - * 統合イノベーション戦略（概要）【総合科学技術・イノベーション会議】siryo1-3



* + - * 統合イノベーション戦略推進会議について【2018年7月内閣府】



* + - * 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【迷惑メール対策推進協議会】



* + - * 日本の中小企業は、とっくにデジタル・トランスフォーメーションを実践している



* + - * 日本企業の「デジタルトランスフォーメーション」を支援するマイクロソフト　その具体的な取り組みと、重視している4つの領域とは【日経ビジネス】



* + - * 日本企業も対策待ったなし？米国のセキュリティ基準「NIST SP800-171」が与える大きなインパクト【2018年9月18日クラウドWatch】



* + - * 米国におけるサイバーセキュリティ人材育成の取組について（NIST.SP800-181）【スライド】【2017年12月NISC】



* + - * 防御不能マルウェアやインフラ標的の同時多発サイバー攻撃——ウォッチガードが2019年のセキュリティ動向を予測【2018年11月29日AtmarkIT】



* + - * 未来投資戦略2018概要



* + - * 迷惑メール対策book「撃退！迷惑メール 」2018年第11版 【迷惑メール対策推進協議会】



* + - * 迷惑メール白書2018【迷惑メール対策推進協議会】



* + 1. 2018年1期4-7（126文献）
       - 〈参考〉従来型ロールとアジャイル型ロールの比較表【2018年4月IPA】000065437



* + - * 「AI・データの利用に関する契約ガイドライン」【2018年6月15日METI】



* + - * + 概要資料
        + 全体編
      * 「CISO等セキュリティ推進者の経営・事業に関する役割調査」報告書【2018年6月28日IPA】



* + - * 「セキュリティ対応組織の教科書 v2.1」 (PDF形式) 【2018年3月30日】Textbook\_soc-csirt\_v2.1



* + - * 「セキュリティ対応組織の教科書 別表 v2.0」 (PDF形式)【2018年3月30日】Textbook\_soc-csirt\_v2.0\_appendix



* + - * 「セキュリティ対応組織成熟度セルフチェックシート」 (Excel形式) 【2018年3月30日8】Textbook\_soc-csirt\_v2.1\_maturity-checklist



* + - * 「重要インフラの情報セキュリティ対策に係る第４次行動計画」の概要【2017年NISC】



* + - * 「他のセキュリティ対策ソフトはもういらない」とアピールするWindows Defenderの現状【2018年04月10日ITmedia】



* + - * 【雑誌】個人情報規制GDPRの脅威【2018年6月2日週刊ダイヤモンド】



* + - * 【図解】コレ１枚でわかる最新ITトレンド



* + - * 2018年に心配される事業継続計画（BCP）のリスクトップ10【2018年6月21日TechTarget】



* + - * 2018年の最先端バックエンドエンジニアに必要なスキルについて考えてみました。【2018年05月28日Qiita】



* + - * AIがエンターテインメントを変える（PDF 3,284KB）【pwc】SF15\_04



* + - * AIによる「効率化」と人間による「クリエイティブ」の幸せな関係【2017年9月宣伝会議】



* + - * AIの戦略的活用に向けて（PDF 5,987KB）【pwc】SF15\_03



* + - * AIの要素技術が出揃ってきた今こそ、利用技術の強さで勝つ（PDF 477KB）【pwc】SF15\_00\_02



* + - * AIブームを支える「機械学習」～AIの現実的な始め方とは？【2018年7月18日】



* + - * AI概論－技術／応用動向概観とビジネス活用への提言（PDF 629KB）【pwc】SF15\_01



* + - * CIS-Controls Version-7-cc-FINAL



* + - * CISO 等セキュリティ推進者の経営・事業に関する役割プラクティス【2018年6月28日IPA】



* + - * CISOハンドブック v1.1β【2018年4月27日JNSA】



* + - * Creating Project Pages using the command line - User Documentation



* + - * 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】000063605



* + - * GDPR が与える影響と準拠に向けた4つのステップ (KPMGコンサルティング版)GDPRebook KPMG



* + - * GDPR が与える影響と準拠に向けた4つのステップJA-CNTNT-eBook-MGC0001688



* + - * Guide to Industrial Control Systems (ICS) Security【NIST SP.800-82R2】【JPCERT和訳】NISTSP800-82r2\_20160314



* + - * HTMLに著作権なんてあるわけないでしょ【2018年4月4日ITMedia】180404\_news009



* + - * ICTの進化によるこれからのしごと【情報通信白書平成30年版】【2018年7月総務省】n4500000



* + - * 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】IoTSecurityWG\_Report\_2017



* + - * IoTソリューション領域へのスキル変革の指針\_参考文献【2018年4月10日IPA】000065569



* + - * IoTソリューション領域へのスキル変革の指針【2018年4月10日IPA】000065568



* + - * ITSS+（プラス）：IPA 独立行政法人 情報処理推進機構



* + - * ITSS＋アジャイル開発の進め方【2018年4月IPA】000065606



* + - * ITセキュリティ評価及び認証制度の概要【2017年3月17日IPA講座資料】cc\_semi\_20170317



* + - * IT製品の調達におけるセキュリティ要件リスト活用ガイドブックPDFファイル【2018年2月IPA】000038924



* + - * NIST SP800 NIST SP800シリーズに見る シリーズに見るBCPとContingency Planning【2006年2月1日IPA菅野】000015360



* + - * NIST SP800-60情報セキュリティ第 I 巻：情報および情報システムのタイプとセキュリティ分類のマッピングガイド【2004年6月NIST】000025339



* + - * society5\_0とは【内閣府】



* + - * アジャイルソフトウェア開発宣言の読みとき方【2018年4月IPA】000065601



* + - * アジャイル領域へのスキル変革の指針\_はじめに【2018年4月IPA】000065571



* + - * 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】000066952



* + - * エンジニアのためのブロックチェーン基礎講座PPT【2017年12月27日株式会社ゼタント】



* + - * クラウドネイティブ時代のアジャイル開発事始め【2018年4月6日bizcompass】



* + - * 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】IoTSecurityWG\_Report\_Ver1



* + - * コンピュータセキュリティインシデント対応ガイド(NISTによる勧告)【2008年3月NIST】000025341



* + - * サイバー・フィジカル・セキュリティ対策フレームワークの概要【METI商務情報政策局サイバーセキュリティ課】002\_05\_01



* + - * サイバー・フィジカル・セキュリティ対策フレームワークの策定に向けて【METI】001\_06\_00



* + - * サイバーセキュリティ2018【2018年7月25日NISC】



* + - * サイバーセキュリティの現状と経済産業省としての取組【2018年3月9日METI】20180309\_Hiroshi\_itou



* + - * サイバーセキュリティ戦略（案）【2018年6月7日NISC】18shiryou01



* + - * サイバーセキュリティ戦略（案）・サイバーセキュリティ 2018（案）【2018年7月25日NISCサイバーセキュリティ戦略本部第18回会合資料】



* + - * サイバーセキュリティ対策の推進【情報通信白書平成30年版】【2018年7月総務省】n6500000



* + - * サイバーレスキュー隊(J-CRAT)技術レポート2017【2018年3月IPA】000065284



* + - * デジタルトランスフォーメーション（ＤＸ）に向けたスキル変革の方向性－全体イメージ－000065688



* + - * 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】000545372



* + - * 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】01\_01



* + - * プログラミング＆リベラルハーツ【2018年5月12日週刊ダイヤモンド】



* + - * ブロックチェーン技術のテクノロジーアセスメント【東京大学公共政策大学院】GraSPP-P-17-001



* + - * 開発者のためのセキュリティ解説書（ガイダンス編）【2014年3月IPA】SecureGuide



* + - * 機械学習はどうやって使うのか——意外と地道な積み重ね【2018年5月22日atmarkIT】180522\_news010



* + - * 経済財政運営と改革の基本方針2018【2018年6月15日閣議決定】shiryo\_02



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



* + - * 重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）【2018年4月4日NISC】



* + - * 重要インフラの情報セキュリティ対策に係る第４次行動計画【2018年7月25日改正NISC】



* + - * 情報セキュリティに関するサプライチェーンリスクマネジメント調査- 調査報告書 - 【2017年3月30日IPA】



* + - * 情報セキュリティ事故対応ガイドブック【情報セキュリティ大学院大学】



* + - * 情報漏えい発生時の対応ポイント集【2012年10月18日IPA】rouei\_taiou



* + - * 世界を変えたデジタルディスラプター - nikkei BPnet Special



* + - * 先手必勝！基礎から学ぶGDPR--基本的な内容と対応が必要なケースを解説MS\_GDPR\_a4\_171213



* + - * 知識偏重から脱却　迷走した「ゆとり」 【日本経済新聞】



* + - * 知的財産戦略ビジョン【2018年6月12日内閣府知的財産戦略推進事務局】chizai2018\_smmry



* + - * + （サマリー）
        + ～「価値デザイン社会」を目指して～
      * 統合イノベーション戦略（素案）（概要）【2018年6月5日】



* + - * 難解なブロックチェーン、仕組みをひも解く【2018年5月30日日経ビジネス】



* + - * 日本の企業文化がセキュアなソフトウェア開発を阻害、CA Technologiesの調査【2018年7月10日　＠IT】



* + - * 日本の社会課題にAIをどう生かすか（PDF 585KB）【pwc】SF15\_02



* + - * 未来投資戦略2018概要【2018年6月15日閣議決定】shiryo\_03-1



* + 1. 2018年1期1-3（112文献）
       - 「オープンデータ基本指針」【概要スライド】【2017年5月30日高度情報通信ネットワーク社会推進戦略本部】data\_shishingaiyou



* + - * 「オープンデータ基本指針」【概要スライド】【2017年5月30日高度情報通信ネットワーク社会推進戦略本部】data\_shishingaiyou.pptx



* + - * 「オープンデータ基本指針」【本文】【2017年5月30日高度情報通信ネットワーク社会推進戦略本部】data\_shishin



* + - * 「オープンデータ基本指針」【本文】【2017年5月30日高度情報通信ネットワーク社会推進戦略本部】kihonsisin



* + - * 「自分たちでできないことはやらない」　分業でセキュリティ強化を図る「京王SIRT」【2018年3月14日ITMedia】180227\_news009



* + - * 「日本の従業員はセキュリティへの関心が薄い」――A10が企業のサイバー攻撃への意識調査公開【2018年3月13日AtmarkIT】180313\_news027



* + - * 【スライド】【2017年7月28日ＡＩネットワーク社会推進会議】000499630



* + - * 【スライド】ＡＩネットワーク化が社会・経済にもたらす影響～先行的評価～【2017年7月28日ＡＩネットワーク社会推進会議】000499629



* + - * 【スライド】AIネットワーク化の本質と将来【2019年3月13日長尾真京都大学名誉教授】000489413



* + - * 【スライド】ＡＩネットワーク社会推進フォーラム（国際シンポジウム）【概要】【2019年3月13日】000499719



* + - * 【スライド】報告書2017― ＡＩネットワーク化に関する国際的な議論の推進に向けて―【概要】【2017年7月28日ＡＩネットワーク社会推進会議】000499632



* + - * 06政府情報システムの整備及び管理 に関する標準ガイドライン.xmind



* + - * 31.情報セキュリティセミナー+マネジメントコース入門編.pptx



* + - * 20180113113747【雑誌】60分完全理解ビジネスのための使えるAI【2017年7月8日週刊東洋経済】



* + - * AIの技術革新の進展による社会への影響について【松尾豊】0000113714



* + - * Amazon PODのPDFとEPUBを一緒に作る！『出版業界気になるニュースまとめ2017』の作り方〈制作編〉



* + - * API活用で未来を拓け 〜APIエコノミー、成功のカギ〜 Review C16090081-001



* + - * API活用で未来を拓け 〜APIエコノミー、成功のカギ〜 Review



* + - * EC-Infographic仮訳（中小企業向けの簡単にまとめられたGDPR説明）



* + - * EU一般データ保護規則（GDPR）の概要と企業が対応すべき事項【情報センサー2017年2月号】



* + - * EU一般データ保護規則が改正個人情報保護法に与える影響【2017年08月31日渡邉雅之弁護士】



* + - * GDPR（General Data Protection Regulation：一般データ保護規則）【個人情報保護委員会】



* + - * IoT時代の組み込みシステム開発はどう変わる【ITmedia】161122\_news028



* + - * ISMSユーザーズガイド-JIS Q 27001\_2014(ISO\_IEC 27001\_2013)対応-リスクマネジメント編【JIPDEC】JIP-ISMS113-30-1954



* + - * ISMSユーザーズガイド-JISQ270012014(ISO\_IEC270012013)対応【JIPDEC】JIP-ISMS111-30-6676



* + - * ISOIEC27001-2013-12-3



* + - * iモードの呪縛成功体験が裏目に



* + - * I情報セキュリティ管理基準（平成２８年改正版）【METI】S\_Management\_Standard\_H28



* + - * 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.html



* + - * 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.mhtml



* + - * m051-セキュリティの常識を覆すサイバー犯罪の転換期2\_2017 年 年間セキュリティラウンドアップ【トレンドマイクロ】



* + - * NIST基準のサイバーセキュリティ対策評価、Secureworksが提供開始【2017年12月7日ASCII】



* + - * Python3入門第0.84.1 版【2017年11月中村勝則】python\_main



* + - * Questions and Answers - Data protection reform package【2017年5月24日EU委員会】Factsheet-20170524QandA



* + - * SEC BOOKS ユーザのための要件定義ガイド～要求を明確にするための勘どころ～【2017年3月10日IPA SEC】000057293



* + - * アジャイル開発向けモデル契約案について【2012年5月23日IPA】000005404



* + - * エンタープライズクラウド戦略第2版 Barry Briggs および Eduardo Kassner【2017年マイクロソフト】



* + - * グーグル社員が「労働時間」を問われない理由【2017年11月BusinessInsider】



* + - * コミュ力もリーダーシップもいらない。Googleが考える、本当に“優秀な人材“とは



* + - * コンピュータセキュリティインシデント対応ガイドSP800-61 rev.1翻訳版【2008年03月NIST】000025341



* + - * サイバーセキュリティに関するフレームワークとISMS【NTTデータ】



* + - * サイバーセキュリティの転換と変革information-security-survey2016【pwc】



* + - * サイバーセキュリティ経営ガイドライン Ver2.0(PDF形式：872KB)【2017年11月16日METI】20171116003-1



* + - * サイバーセキュリティ経営ガイドライン Ver2.0付録C インシデント発生時に組織内で整理しておくべき事項(EXCEL形式：48KB)【2016年11月16日METI】20171116003-2.xlsx



* + - * サイバーセキュリティ経営ガイドラインも推奨 今こそ求められている「サイバー攻撃に対応したBCP」【2018年3月2日ZDNET】



* + - * セキュリティとモラルのガイドブック2017【カルベルスキー】Kaspersky\_GuideBook2017\_A4single



* + - * セキュリティプレゼンター支援利用マニュアル第１版【2017年12月IPA】



* + - * そのメールは詐欺だ！　手口が「進化」、対策は３つ



* + - * デジタルアーカイブに関する取り組みについて【2017年9月内閣府知的財産戦略推進事務局】siryou1



* + - * なんで勉強しなきゃいけないの【瀧本哲史】



* + - * フィッシングメールやランサムウェア被害が拡大した2017年、マカフィーが10大セキュリティ事件ランキングを発表【2017年12月20日InternetWatch】



* + - * フィンテックで社会が一変Innovation Roadmap 2030(5)



* + - * プログラマーの仕事がついになくなる？　2020年を占う「10大テクノロジートレンド」【ITmedia】



* + - * ブロックチェーン技術を活用したサービスに関する国内外動向調査報告書(PDF形式：1,571KB)【2016年4月28日METI】20160428003-2



* + - * ブロックチェーン技術を活用したサービスに関する国内外動向調査報告書（概要）(PDF形式：1,729KB)【2016年4月28日METI】20160428003-1



* + - * 応用情報技術者試験（レベル３）シラバスVer4.0【2016年5月IPA】



* + - * 我が国におけるデジタルアーカイブ推進の方向性エグゼクティブ・サマリー【2017年4月内閣府】houkokusho\_機械学習とは？【SAS】wp-machine-learning-primer-108796-jp



* + - * 技術ナビゲーション2017【2017年4月19日CIAJ】tech\_navigation2017



* + - * 共通フレーム2013の概説【IPA】000027415



* + - * 共通フレーム2013解説【2016年1月IPASEC】seminar\_tokyo\_20160113-01



* + - * 決裁文書の削除部分は近畿財務局職員のひそかな告発だった？「特例の原因は安倍昭恵夫人」の隠されたメッセージ



* + - * 効果的なサイバー防御のためのCISクリティカルセキュリティコントロール バージョン 6.0【2015年10月15日CIS】CIS-CSC\_v6.1\_Japanese\_Final\_r1



* + - * 国際的な議論のためのＡＩ開発ガイドライン案【2017年7月28日ＡＩネットワーク社会推進会議】000499625



* + - * 国内企業が実践するAIによるデジタルトランスフォーメーション【2018年03月23日ZDNet】WP\_NEC\_AI\_1803\_01



* + - * 産業サイバーセキュリティセンターの事業案内パンフレット【IPA】000062153



* + - * 重要インフラのサイバーセキュリティを向上させるためのフレームワーク1.0版 【2014年2月12日NIST】000038957



* + - * 情報セキュリティ10大脅威 2018【2018年3月IPA】000065376



* + - * 情報セキュリティとサイバーセキュリティにまつわる誤解【2018年3月13日日経x-tech】



* + - * 情報セキュリティ技術の国際標準化動向の最新報告【NICT中尾康二】S2\_nakao



* + - * 情報セキュリティ事故対応ガイドブック（PDF：全90ページ、1.47MB）【情報セキュリティ大学院大学】jiko-情報セキュリティ事故対応ガイドブックjiko-flow\_checksheet.xlsx



* + - * 新しい経済政策パッケージ【2017年12月8日内閣府】20171208\_package



* + - * 新ビジネスの可能性広げるブロックチェーンの仕組み



* + - * 人工知能が本当にかしこくなったときの最初の仕事はなにか【2017年12月13日ascii.jp】



* + - * 人工知能の研究開発目標と産業化のロードマップ【2017年3月31日人工知能技術戦略会議】100862412



* + - * 人工知能の未来- ディープラーニングの先にあるもの【松尾豊】000400435



* + - * 人工知能技術戦略（とりまとめ）【2017年3月31日人工知能技術戦略会議】100862413



* + - * 請負契約と準委任契約の相違点



* + - * 第５期科学技術基本計画【本文】【2016年1月閣議決定】5honbun



* + - * 第５期科学技術基本計画の概要【2016年1月閣議決定】5gaiyo



* + - * 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（検討会報告書の概要）【2017年4月19日METI】20170419002-2



* + - * 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（参考資料）【2017年4月19日METI】20170419002-3



* + - * 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（本文）【2017年4月19日METI】20170419002-1



* + - * 知的財産戦略ビジョンに関する専門調査会（第１回）資料３専門調査会におけるビジョンの検討の進め方siryou3



* + - * 知的財産戦略ビジョンに関する専門調査会（第１回）資料４将来予測のためのデータと兆し【2017年12月26日】siryou4



* + - * 著作権法の一部を改正する法律案（案文・理由） （PDF202KB） 【2018年2月文化庁】1401718\_003



* + - * 著作権法の一部を改正する法律案（概要） （PDF85KB） 【2018年2月文化庁】1401718\_001



* + - * 著作権法の一部を改正する法律案（参照条文） （PDF231KB） 【2018年2月文化庁】1401718\_005



* + - * 著作権法の一部を改正する法律案（新旧対照表） （PDF279KB） 【2018年2月文化庁】1401718\_004



* + - * 著作権法の一部を改正する法律案（要綱） （PDF59KB） 【2018年2月文化庁】1401718\_002



* + - * 超上流から攻めるIT化の原理原則17ヶ条【IPA】000005109



* + - * 東京都職員共済\_こころの健康づくり実践ガイドP24（全体版）



* + - * 複雑化している国内の「モバイル決済サービス」を総整理する【2017年12月12日ITmedia】171212\_news036



* + - * 米国FISMA（連邦情報セキュリティマネジメント法）プロジェクトにおける情報セキュリティの先進的な取り組み【2010年2月17日JASA】tko20100217



* + - * 保存版！Synology NASを使うなら知っておきたい17のギモンにお答えします！【2017年12月12日】



* + - * 報告書2017【概要スライド】-AIネットワーク化に関する国際的な議論の推進に向けて－【2017年7月28日AIネットワーク社会推進会議】000499632



* + - * 報告書2017【本体】-AIネットワーク化に関する国際的な議論の推進に向けて－【2017年7月28日AIネットワーク社会推進会議】000499624



* + - * 報告書２０１７－ＡＩネットワーク化に関する国際的な議論の推進に向けて－【2017年7月28日ＡＩネットワーク社会推進会議】000499624



* + - * 本棚の中のニッポン　海外の日本図書館と日本研究ISBN978-4-305-70588-4



* + - * 未来の図書館、夢にとりつかれた男【2018年2月19日日経XTECH】



* + - * 未来投資戦略2017（ポイント）【2017年6月9日閣議決定】



* + - * 未来投資戦略2017（具体的施策）【2017年6月9日閣議決定】



* + - * 未来投資戦略2017（全体版）【2017年6月9日閣議決定】miraitousi2017\_t



* + - * 滅びゆくのはマンガ文化か、出版社か、それとも表現の自由か【2018年3月29日P2Pとかその辺のお話】



* + - * 理系経営学はAIに「忖度」をさせるか？人間の意思決定を、数字で科学する。【広告特集企画・制作朝日新聞社メディアビジネス局】



* + - * 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【SP800-53R4】【2013年4月NIST】000056415



* + - * 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【SP800-53R4】【2013年4月NIST】NIST.SP.800-53r4



* + - * 連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド【SP800-37】【2010年2月NIST】000025329

