

デジタル時代の評価

－ クラウドサービスの安全性評価と Web 情報を活用した評価技術の紹介 －

奥村 明俊

独立行政法人 情報処理推進機構 (IPA)

1. 緒言

我が国のデジタル改革基本方針では、デジタル社会の目指すビジョンとして「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」を掲げている[1]。その実現に向けて、デジタル化による成長戦略、医療・教育・防災・子ども等の準公共分野のデジタル化、デジタル化による地域の活性化、誰一人取り残されないデジタル社会、デジタル人材の育成・確保などの施策を展開している。このような施策をスピーディかつ確実に実施していくためには、行政が保有するデータ、民間データ、過去の施策の結果に関するデータなど多様なデータに基づき、できるだけ正確に現状を把握し、実施しながら効果等を適時的確に把握する評価プロセスが重要となる[2]。

近年、デジタルトランスフォーメーション(DX)の推進等によって生活や業務のデジタル化が進むとともに、急速にクラウドサービス化が進んでいる。総務省の調査報告書[3]によれば、従業員 100 人以上の企業 2,223 社について、クラウドサービスを利用していると回答した割合は 68.5%で、2019 年の 64.5%より 4 ポイント増加した。サービス利用の効果について「非常に効果があった」または「ある程度効果があった」と回答した企業が 8 割を超えた。今後も企業や組織での DX の進展とともにクラウドサービスの利用は更に加速していくと考えられる。他方で、2021 年はクラウドサービスの利用者の設定ミスに起因するセキュリティインシデント、不正アクセスやクラウドの開発環境のスクリプトが改ざんされるといったインシデントが報告されている[4]。デジタル社会のビジョンの実現には、セキュリティ対策と DX 推進の両立が不可欠である。そのためには、セキュリティや DX の取り組みについて事業者や企業を評価する仕組みや手法を構築していかなければならない。

本稿では、クラウドサービスの安全性評価の取組みと企業の DX 活動を評価する技術について紹介する。まず、クラウドサービスの安全性評価として、クラウドサービスのセキュリティ認証の概要、政府情報システムのためのセキュリティ評価制度 (ISMAP: Information system Security Management and Assessment Program) について述べる。次に、企業の DX 活動評価として、現在の状況と Web 情報を活用した自動評価技術について概説する。

2. クラウドサービスの安全性評価

2.1 クラウドサービスのセキュリティ認証

クラウドサービスの導入においてセキュリティを評価する際、サービス事業者が取得しているセキュリティ認証が参考となる。サービス事業者はセキュリティ認証を取得することにより、ある基準に適合していることを客観的に示すことができる。つまり、そのサービスの利用を検討する組織が求めるセキュリティ基準を満たしているかの判断材料を提供できる。サービス利用者はセキュリティ認証を参考にすることで、顧客情報を預けるような SaaS サービスについて、セキュリティ面で事業者は十分な準備をしているか等の判断が容易になる。クラウドサービスに特化したセキュリティ認証制度として、JASA-クラウドセキュリティ推進協議会(JCISPA:JASA Cloud Information Security

Promotion Alliance)が認証する CS マーク[5]と ISO/IEC27001、27017 のクラウドセキュリティ認証[6]があげられる。また、一般社団法人日本クラウド産業協会では、総務省等が定めた各種ガイドライン、「クラウドサービスの安全・信頼性に係る情報開示指針(情報開示指針)」を基に、サービス事業者が安全・信頼性に係る情報を適切に開示していることを認定する制度を運用している。情報開示指針は、利用者によるクラウドサービスの比較・評価・選択等を容易にすることを目的として総務省が発行しているものであり、2022 年 2 月に追加された「AI を用いたクラウドサービスの安全・信頼性に係る情報開示指針(ASP・SaaS 編)」を合わせ、8 分野の情報開示指針から構成される[7]。サービス事業者は、情報開示指針を基に開示項目を整理し公表することにより、クラウドサービスの安全・信頼性を示すことができる。サービス利用者は、セキュリティ認証による確認ができなかったサービスの対策について、同指針を参考にしてサービス事業者に問い合わせ等が可能となる。次節では、今後参考となる制度として、政府情報システムのためのセキュリティ評価制度 (ISMAP) [8]について述べる。

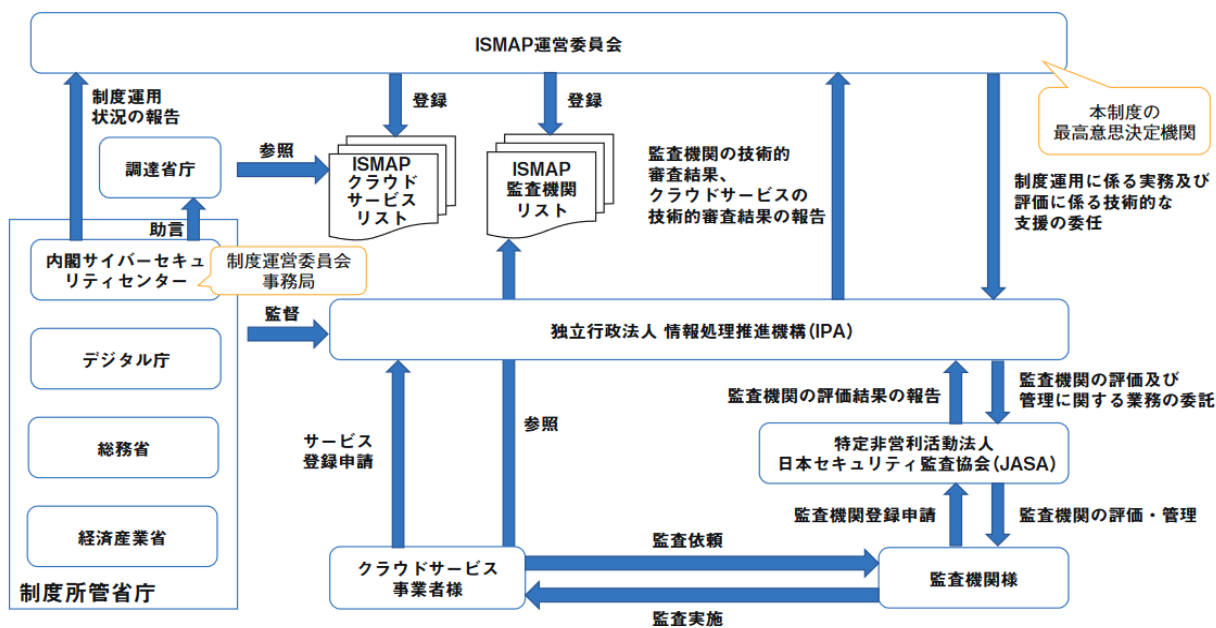
2.2 政府情報システムのためのセキュリティ評価制度 (ISMAP)

ISMAP (ISMAPP) は、政府が求めるセキュリティ要件を満たしているクラウドサービスをあらかじめ評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、クラウドサービスの円滑な導入に資することを目的とした制度である。従来、政府調達にあたっては、個々のクラウドサービスが実施していると表明する情報セキュリティ対策の実施状況を、調達者が直接確認することが必要であったが、本制度により、この確認を省略でき負担を軽減できる。

2018 年 6 月に公開された「政府情報システムにおけるクラウドサービスの利用に係る基本方針[9]」では、「クラウド・バイ・デフォルト原則」が掲げられた。これを踏まえ、経済産業省と総務省は、適切なセキュリティ要件を満たすクラウドサービスを導入するために必要な評価方法等を検討し、2020 年 1 月に「クラウドサービスの安全性評価に関する検討会とりまとめ」を公開した[10]。また、同月のサイバーセキュリティ戦略本部会合において「政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて」が決定された[11]。上記検討会において、2019 年 6 月から、政府情報システム調達に応募するクラウド事業者が遵守すべきセキュリティ管理基準 (ISMAP 管理基準) の検討が行われた。ISMAP 管理基準は、国際規格をベースに「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 30 年度版)[12]」、「NIST SP800-53 rev.4」等を参照して作成されたものである。

2.3 ISMAP の運用

ISMAP のフローを図 1 に示す。ISMAP においては、政府機関等が調達するクラウドサービスに要求される基本的な情報セキュリティ管理・運用の基準を満たすセキュリティ対策を実施していることが確認されたクラウドサービスが、ISMA クラウドサービスリスト(サービスリスト)に登録される。政府機関がクラウドサービスを調達する場合、サービスリストに登録された



(注)制度運用に係る実務及び評価に係る技術的な支援をIPAが行い、うち、監査機関の評価及び管理に関する業務についてJASAに再委託する。

図1 クラウドサービスの安全性評価の制度のフロー (出典 参考文献[8])

サービスを選定候補とする。また、監査実施機関は、あらかじめ本制度で定める要求事項を満たすことが確認され、本制度が公表する ISMAP 監査機関リスト(監査機関リスト)に登録される。クラウドサービス提供者は、監査機関リストに登録された機関による監査を受け、ISMMap 運用支援機関である IPA を通じて ISMAP 運営委員会にサービス登録申請を行う。申請を受けた ISMAP 運営委員会は審査を行い、承認されたサービスがサービスリストに掲載される。府省庁などの調達者は、サービスリストを使って調達先候補を選ぶ。なお、本制度の運用に係る実務及び評価に係る技術的な支援は IPA が行い、そのうち、監査機関の評価及び管理に関する業務について

は、IPA から特定非営利活動法人日本セキュリティ監査協会 (JASA) に委託している。

ISMMap は、2020 年 6 月に運用が開始された。ISMMap の所管は 2022 年 1 月現在、内閣サイバーセキュリティセンター (NISC)、デジタル庁、総務省、経済産業省であり、最高意思決定機関として ISMAP 運営委員会を設置し、事務局は NISC に置き、運用実務は IPA が担当している。制度の概要、基準規程類、監査機関リスト、及びサービスリストは、図 2 に示すように ISMAP ポータルサイト[13]で公開されている。2022 年 6 月 1 日時点で登録されている監査機関は 5 機関、また、クラウドサービスは 34 サービスである。ISMMap で公開さ



図2 ISMAP ポータルサイトの画面

れる情報は、重要インフラ分野等を始めとする民間においても参照されることで、クラウドサービスの適切な活用の推進が期待される。登録されたクラウドサービスを利用しただけでは情報システム全体のセキュリティが十分に確保されることにはならない。適切な設定を行うことに加え、情報システム全体のセキュリティリスクを分析し、適切な対策を行うことが求められる。

3. 企業の DX 活動評価

3.1 DX 活動の推進状況

DX は、経済産業省が発表した DX 推進ガイドライン[14]によると「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること」と定義されている。技術は手段であり、目的は組織的な変革である。変革には、推進責任者が必要であるが、組織の構成員全員の意識改革や行動変容が求められる。経済産業省は、企業における DX 推進のために 2018 年 9 月に DX レポート[15]を公開し、企業内面への働きかけと、市場環境整備による企業外面からの働きかけの両面から政策を展開してきた。日本企業は、新型コロナウイルス感染症 (COVID-19) の影響により事業継続の危機にさらされテレワークなど社内の IT インフラや就業に関するルールを変更し環境変化への対応を進めているが、米国企業に比較すると大きく遅れている[16]。経済産業省が作成した DX 推進指標 [17]の自己診断に取り組み、結果を提出した企業の中でも、8 割以上の企業は DX にまったく取り組んでいないか、取り組み始めた段階であり、先行企業と平均的な企業の DX 推進状況は大きな差がある[18]。各企業において DX の取り組みが進まないパターンとして、DX の目的が分からない、何をすれば DX になるのかが分からない、DX をどう進めるか分からない、といった問題が指摘されており、DX を進展させるために必要な経営層の意識改革が提言としてまとめられている [14]。さらに、DX を進展させる上で指針となる、DX 推進ガイドラインや DX 推進指標の他、デジタルガバナンスのあるべき姿を示したデジタルガバナンス・コード[19]、各業界の企業群の DX 推進の進捗を客観的に評価するためのスキームとして、DX 認定制度[20]、DX 銘柄選定[21]などが整備されつつある。このような評価スキームによる調査は、各企業の経営層が自社の DX に関わる経営戦略を立案・遂行する上でのベースとなる。

3.2 Web 情報を活用した DX 活動評価

DX に関する活動評価は、図 3 に示すように、評価項目の設計、項目の回答作成、評価や可視化といった人手によるプロセスで行われることが多い。



図 3 DX の評価プロセス

こうした評価は、自己評価、第三者評価を問わず、テーマの多様性や対象の規模が大きいほど、手間や費用等のコストも増大する。IPA は、国立研究開発法人情報通信研究機構 (NICT) と協力して、評価を自動化するシステム、WISDOM-DX を開発した[22]。WISDOM-DX では、評価項目を 5W1H (いつ、誰が、どこで、何を、なぜ、どうやって) の質問タイプでモデル化し、Web データに基づく質問応答システム WISDOM X[23]を用いて企業の DX 活動に関する回答を自動生成し、過去の優良事例を学習データとして評価する。評価を自動化することで評価コストを低減し、各企業や調査機関がタイムリーに DX に関する評価を実施できることを目指す。

DX の優良企業について調査したところ、優良企業は DX に対する取組みや評価などが Web 上に多く掲載されていることが分かった。また、自ら、広報、IR、プロモーションなどを通じて、企業経営や IT 技術活用の方向性、具体的な戦略、戦略を進めるための体制、環境整備の方策、戦略の達成状況などの情報を発信している。優良企業の情報には、経営面に関わるものと DX を実現する IT に関わる活動について、それぞれ優れた企業ならではの共通性がみられる。このような Web データの特徴を活かして、評価を自動化するシステム WISDOM-DX を開発した。WISDOM-DX は、Web データから得られた企業に関する DX 情報と優良企業の事例との類似度などから機械学習を用いて評価する。WISDOM-DX のシステム構成を図 4 に示す。

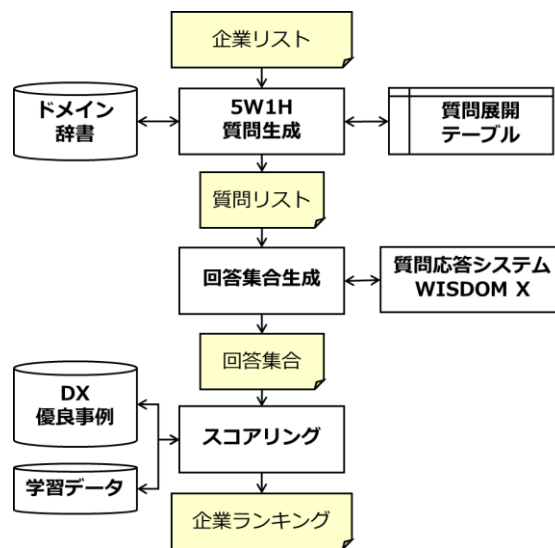


図 4 WISDOM-DX のシステム構成

5W1H 質問生成は、入力された企業リストの各企業の DX 活動について、質問展開テーブルとドメイン辞書の表現を組み合わせて 5W1H の形式で質問文を生成し質問リストとして出力する。回答集合生成は、質問リストの質問文を質問応答システム WISDOM X[23]に入力し、その出力を質問文ごとに回答集合として出力する。スコアリングは、回答集合を入力として Web 掲載の情報量や DX 優良事例との類似度などから、各企業の DX 活動のスコアを算出してランキングを出力する。DX 優良事例は、過去に優れた事例として公開された企業の取組みに関するテキストデータであり、学習データは、過去に優れた DX 活動の企業として選定された企業を正例、それ以外を負例とする二値データである。

3.3 WISDOM-DX の有効性検証

WISDOM-DX の有効性検証のため、DX 銘柄 2021 調査 [21] の回答企業 464 社から、有識者によって選定された DX の優良企業 48 社を検索するタスクを設定した。DX 銘柄は、経済産業省と東京証券取引所によって、デジタル技術を前提とするビジネスモデル等の抜本的変革による成長・競争力強化である DX に取り組んでいる企業に与えられる称号である。有識者らが「経営ビジョン・ビジネスモデル」「戦略」「戦略実現のための組織・制度等」「戦略実現のためのデジタル技術の活用・情報システム」「成果と重要な成果指標の共有」「ガバナンス」の項目などから DX 銘柄 2021 と DX 注目企業 2021 の 48 社を選定した。この 48 社を DX 優良企業として、464 社をランキングして検索する実験を行った[24]。比較のためのベースライン手法として、汎用的な Web 検索エンジンである Google 検索の検索件数を利用したランキング手法を用いた。このベースライン手法は、評価対象の 464 社について、企業名と“デジタルトランスフォーメーション”の 2 つのキーワードの AND 検索を Google Custom Search で実行し、検索件数の大きい順に 464 社をランキングするものである。実験結果として、WISDOM-DX とベースライン手法の Precision-Recall 曲線を図 5 に示す。

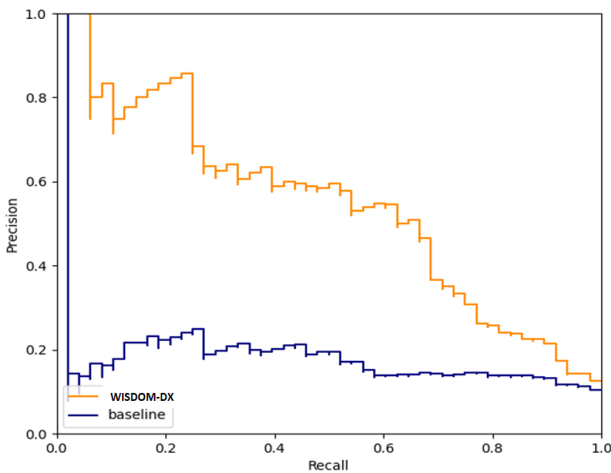


図 5 WISDOM-DX とベースライン手法の Precision-Recall 曲線

Precision-Recall 曲線は、検索における適合性と再現性を評価する尺度である。検索精度の評価指標である Precision-Recall 曲線の下面積、AUPR (Area Under the Precision-Recall Curve) は、WISDOM-DX が 0.541、ベースライン手法が 0.181 であった。WISDOM-DX は、ベースライン手法の約 3 倍であった。WISDOM-DX によるランキング上位 48 社のうち DX 優良企業に該当する企業は 27 社であり、一致率は 56.3%であった。ベースライン手法による一致率は 22.9% (上位 48 社中 11 社)であった。期待値は 10.3% (48/464)なので、WISDOM-DX の一致率は、期待値の 5 倍以上、ベースライン手法の約 2.5 倍であった。

WISDOM-DX 上位 48 社において一致しない 21 社のうち 17 社がメディアや業界団体による DX 関連の受賞企業か、経済産業省による DX 認定企業であることが分かった。WISDOM-DX 上位 48 社中 44 社 (91.7%) は、自社の DX 推進に関して主導的に一定水準以上の活動を実施していることが確認できた。一致しない 21 社のうち 4 社は、自社として DX に関する受賞や選定や認定の実績はないが、他社と共同で

DX に取り組んでいること、他社の DX を支援する活動を行っていることが分かった。他社との取組みについてどう評価するか議論が必要であるが、Web データから自社の活動と他社との共同活動を識別することが課題である[24]。

評価された企業に自社のランキングの妥当性に関して、アンケート調査を行った。「自社のランキングは妥当と思うか」に対する回答結果を表 1 に示す[24]。6 割以上の企業が、肯定的な意見であった。残りの約 4 割は、ランキングの理由がわからないなどの理由から、分からないや否定的な意見となった。アンケートでは、他社の名前を公開せず対象企業のみランキングを示したことが主たる要因と思われるが、ランキングの根拠となった Web 情報の提示など説明機能の充実が課題である[24]。

表 1 自社ランキングに関する妥当性

「ランキングは妥当と思うか」の回答	割合
そう思う	14.3%
ややそう思う	46.4%
わからない	32.1%
あまりそう思わない、思わない	7.1%

4. 結言

ISMAP で公開される情報は、重要インフラ分野等をはじめとする民間においても参照されることで、クラウドサービスの適切な活用の推進が期待される。2019 年 5 月 23 日に改定された NISC の「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) [25] は、「事業環境の変化を捉え、インターネットを介したサービス (クラウドサービス等) を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在について留意する」としており、国内の評価制度としては ISMAP が該当すると考えられる。情報システムのセキュリティ確保の責任は、一義的に当該システムの利用者である調達者が負うものである。本制度に登録されたクラウドサービスを利用したとしても、それだけでは情報システム全体のセキュリティが十分に確保されることにはならない。情報システムの調達者は、利用するクラウドサービスについて適切な設定を行うことに加えて、情報システム全体のセキュリティリスクを分析し、適切な対策を行うことが求められる。サイバーセキュリティ対策は、最高情報セキュリティ責任者 (CISO: Chief Information Security Officer) など一部の担当者に任せるものではなく、組織のすべての人が一定のリテラシーを身につけて実行することが必要である[28]。

DX 推進のためには、各企業が自ら簡単に DX に関する評価を実施できるようにすることが必要である。Web データに基づく質問応答システムと過去の優良事例を学習データとして、企業の DX 活動を自動的に評価するシステム WISDOM-DX を開発した。DX 銘柄 2021 の応募企業 464 社について実験した結果、上位 48 社に関して DX 優良企業との一致率は 56.3%であった。また、48 社の中の 91.7% は、主導的に一定水準以上の DX 活動を実施していることが確認できた。組織の DX 活動評価のために Web 情報活用は有効だと思われる。Web 情報には、DX だけではなく、ISMAP のサービスリスト、脆弱性対策情報データベース [26]、CISO の役割や業務内容[27]などサイバーセキュリティに関する多くの情報が提供されている。今後、DX 以外にもセキュリティやその他のテーマに関して Web 情報を活用した分析・評価技術を開発し、デジタル時代に適応した人や組織を育成する取り組みを進めていく。

参考文献

- デジタル庁: デジタル社会の実現に向けた重点計画, 2022.
[<https://www.digital.go.jp/policies/priority-policy-program/> (cited 2022-Aug-9)]
- 総務省: デジタル時代にふさわしい政策形成・評価の在り方に関する提言(政策評価審議会提言), 2022.
[https://www.soumu.go.jp/menu_news/s-news/hyouka_220531000157635.html (cited 2022-May-31)]
- 総務省: 令和 2 年通信利用動向調査報告書(企業編), 2020.
[https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR20200_002.pdf (cited 2020-Sep-25)]
- IPA: クラウド情報セキュリティ, 情報セキュリティ白書 2022, 2022: 186-193
- JCISPA(JASA -クラウドセキュリティ推進協議会): CS マーク
[<https://jcispa.jasa.jp/> (cited 2022-May-23)]
- 一般社団法人情報マネジメントシステム認定センター: ISMS 適合性評価制度 [<https://isms.jp/isms.htm>] (cited 2022-May-23)]
- 総務省: クラウドサービスの安全・信頼性に係る情報開示指針における AI を用いたクラウドサービスの安全・信頼性に係る情報開示指針(ASP・SaaS 編)の追加
[https://www.soumu.go.jp/menu_news/s-news/01ryutsu06_02000306.htm (cited 2022-May-23)]
- 内閣官房・総務省・経済産業省: 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
[https://www.ismap.go.jp/sys_attachment.do?sys_id=e4b5c5e41bfec150f18c65fa234bcb82 (cited 2020-Jun)]
- 各府省情報化統括責任者(CIO)連絡会議: 政府情報システムにおけるクラウドサービスの利用に係る基本方針, 2021
[https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf (cited 2022-May)]
- 経済産業省: クラウドサービスの安全性評価に関する検討会とりまとめ
[<https://www.meti.go.jp/press/2019/01/20200130002/20200130002-1.pdf> (cited 2022-May)]
- サイバーセキュリティ戦略本部: 政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて, 2020 [<https://cio.go.jp/node/2649>] (cited 2020)
- NISC: 政府機関等のサイバーセキュリティ対策のための統一基準群
[<https://www.nisc.go.jp/policy/group/general/kijun.html> (cited 2022-May)]
- ISMAP: 政府情報システムのためのセキュリティ評価制度,
[<https://www.ismap.go.jp> (cited 2022-Sep)]
- 経済産業省: 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) ver1.0, 2018.
[https://www.meti.go.jp/policy/it_policy/dx/dx_guideline.pdf (cited 2018-Dec)]
- 経済産業省: 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.
[<https://www.meti.go.jp/press/2018/09/20180907010/20180907010-3.pdf> (cited 2018-Sep)]
- IPA: DX 白書 2021 日米比較調査にみる DX の戦略, 人材, 技術, 2021.
[https://www.ipa.go.jp/ikc/publish/dx_hakusho.html (cited 2021-)]
- デジタルトランスフォーメーションの加速に向けた研究会: DX レポート 2 (中間取りまとめ) (2020).
[<https://www.meti.go.jp/press/2020/12/20201228004/20201228004-2.pdf> (cited 2020-Dec-28)]
- 経済産業省: 「DX 推進指標」とそのガイダンス, 2019.
[<https://www.meti.go.jp/press/2019/07/20190731003/20190731003-1.pdf> (cited 2019-Jul)]
- 経済産業省: デジタルガバナンス・コード, 2020.
[https://www.meti.go.jp/shingikai/mono_info_service/dgs5/pdf/20201109_01.pdf (cited 2020-Nov-9)]
- 経済産業省: DX 認定制度(情報処理の促進に関する法律第三十一条に基づく認定制度), 2020.
[https://www.meti.go.jp/policy/it_policy/investment/dx-nintei/dx-nintei.html (cited 2022-Aug-8)]
- 経済産業省: デジタルトランスフォーメーション銘柄(DX 銘柄) 2021, 2021.
[https://www.meti.go.jp/policy/it_policy/investment/keiei_meigara/dx-report2021.pdf (cited 2021-Jun)]
- IPA: WEB データに基づく企業の DX 活動の自動分析・評価システム「WISDOM-DX」を開発, 2021
[<https://www.ipa.go.jp/ikc/info/20211006.html> (cited 2021-Oct)]
- 国立研究開発法人情報通信研究機構(NICT): WISDOM X (ウィズダム エックス)とは? [<https://www.wisdom-nict.jp/#top>] (cited 2022-Aug)]
- Okumura, A. et al.: WISDOM-DX: An Automatic DX Evaluation System Using a QA System Based on Web Information, In the Proceedings of DICOMO2022, pp.1286-1300, Jul.2022.
- NISC: 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策定指針(第 5 版)
[<https://www.nisc.go.jp/pdf/policy/infra/shishin5.pdf> (cited 2022-Sep)]
- JVN iPedia: 脆弱性対策情報データベース
[<https://jvndb.jvn.jp/index.html> (cited 2022-Aug)]
- 定非営利活動法人日本ネットワークセキュリティ協会 社会活動部会 CISO 支援ワーキンググループ: CISO ハンドブック 業務執行として考える情報セキュリティ Ver. 1.1β, 2018
[https://www.jnsa.org/result/2018/act_ciso/data/ciso-handbook_v011b.pdf (cited 2022-Aug)]
- 奥村明俊: デジタル時代の人と組織に関する評価~サイバーセキュリティ人材と企業の DX 活動の評価の紹介~, 第 42 回医療情報学連合大会(第 23 回日本医療情報学会学術大会), 2022 年 11 月 18 日発表予定