Vol.2020-DPS-184 No.5
Vol.2020-EIP-89 No.5
2020/9/10

民間企業におけるセキュリティ・クリアランスの研究

宇都田賢一[1]

概要：サイバー空間で自社の事業を保護するためには、海外を含めた情報共有が有効とされている。本研究では、民間企業が事業を継続し拡大させるために、いわゆるセキュリティ・クリアランスを活用し、より効果的に情報共有活動等に参加するためにはどのような組織が望ましいかを、米国の法制度等を参考とし検討を行った。

キーワード：情報共有、セキュリティ・クリアランス、サイバー空間

Research on Security Clearance in Private Sectors.

KENICHI UTSUDA[†1]

Abstract: To protect the business of private sectors on the Cyber space, information sharing with domestic and foreign countries is an effective way. In this study, I suggested what kind of organization is desirable for private sectors to participate in information sharing activities more effectively by utilizing security clearances continuing and expansion their business, referring to the legal system of the United States.

Keywords: information sharing, security clearance, cyber space

1. はじめに

総務省・通信利用動向調査[1]によると、令和元年度時点で個人のインターネット利用は 89.8%、企業のインターネット利用は、平成 30 年時点で 99.5%である。このようにインターネットが日々の生活や企業活動に不可欠となる一方で、インターネット等の情報通信ネットワークを利用することによるリスクが顕在化していることも事実である。また同調査によると、平成 30 年にインターネット等の情報通信ネットワークを利用することによる何らかの攻撃を受けた企業の割合は 54.4%であり、決して見過ごすことができない数字である。では、実際の攻撃にはどのようなものがあるのかを考えてみる。独立行政法人情報処理推進機構（IPA）の 10 大脅威の組織編[2]によると、1 位は標的型攻撃による機密情報の窃取であり、攻撃（犯罪）集団、国家組織の支援を受けた攻撃（犯罪）集団が関わっていることが示されている。IPA のサイバースキュー隊（J-CRAT）の 2019 年度上半期レポート[3]では、「他国の政府機関が関係していると推定されるステートスポンサードのエスピオナージに対応していくためには、各組織がインシデント対応を成熟させて外部連携力を強化していくことで、わが国としての対応力を高めていくことが必要不可欠である。」とされている。

このように、サイバー攻撃への対処として情報共有が重要とされているが、一方で情報共有を行う相手が信頼できるかどうかを計ること、いわゆるセキュリティ・クリアランスが必要と考えられる。本稿では、米国が政府契約事業者に適用するセキュリティ・クリアランス制度と、日本のサイバーセキュリティ協議会、特定秘密保護法を比較し、日本でセキュリティ・クリアランスが求められる企業が取ることができると考えられる手法を検討したものである。

2. 米国におけるサイバー情報共有活動と、産業保全としてのセキュリティ・クリアランス

2.1 サイバー情報共有活動

日本の経済産業省の調査報告によると、2015 年 2 月、当時の Barack Obama 大統領は、大統領行政命令第 13691 号「民間セクターサイバーセキュリティ情報共有）」[4]で、米国国土安全保障省（United States Department of Homeland Security：DHS）に対して、「重要インフラ防護プログラムを通じて、情報共有及び分析組織（Information Sharing Organization : ISAO）のメンバーである民間セクターの個人にクリアランス（機密書類取扱資格）を付与する効果的な手段を開発すること」を指示した。なお DHS が所管する官民のサイバー情報共有プログラムは、下記の 3 つがあるとされている[5]。

- Automated Indicator Sharing （AIS）
- Cyber Information Sharing and Collaboration Program （CISCP）
- Enhanced Cybersecurity Services （ECS）

この 3 つのうち ECS が、機密情報（sensitive and classified cyber threat information）を扱うため、セキュリティ・クリアランスが求められるとされている。

1 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY.

Vol.2020-DPS-184 No.5
Vol.2020-EIP-89 No.5
2020/9/10

2.2 産業保全としてのセキュリティ・クリアランス

次に、米国の企業に求められているセキュリティ・クリアランスについて概観する。米国では、政府契約事業者（Contractor）向けに、機密情報の扱いに関する手順や要件を定める、国家産業保全プログラム（National Industrial Security Program : NISP）がある。また、その運用のために、国家産業保全プログラムマニュアル（National Industrial Security Program Operation Manual （DoD 5220.22-M）: NISPOM）が提供されている[6]。NISPOM は全 11 章から構成されており、特に第 2 章では、米国の政府契約事業者に求められる Facility Clearance（FCL）、政府契約事業者の従業員を対象とした Personal Security Clearance（PCL）に関して記されている。

3. 日本におけるサイバー情報共有活動と特定秘密保護法

3.1 サイバーセキュリティ協議会

サイバーセキュリティ協議会は、2018 年 12 月に改正された「サイバーセキュリティ基本法」によって創設が定められ、2019 年 4 月 1 日に設立された組織である。この協議会は、内閣サイバーセキュリティセンター（NISC）が事務局を担い、我が国のサイバーセキュリティに対する脅威に積極的に対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行うことを目的としている。サイバーセキュリティ協議会の設立根拠となるサイバーセキュリティ基本法の義務規定、罰則規定は、下記が記載されている[7]。

- 守秘義務関係（第 17 条第 4 項、第 38 条）
  第 17 条第 4 項　協議会の事務に従事する者又は従事していた者は、正当な理由がなく、当該事務に関して知り得た秘密を漏らし、又は盗用してはならない。
- 第 38 条　第十七条第四項又は第三十一条第二項の規定に違反した者は、一年以下の懲役又は五十万円以下の罰金に処する。

自組織単独ではまだ確証を得るに至っていない専門的な分析内容等を積極的に提供し合い、具体的な対策情報等を作出したり、対策情報等の精度向上等に積極的に協力する「タスクフォース」は、サイバーセキュリティ協議会規約第 6 条 4 項で、次のいずれかに該当する加入構成員は、特例がある場合を除きタスクフォースに参加することができないとされている[8]。

一 日本の国籍を有しない人
二 外国政府又はその代表者
三 外国の法人又は団体
四 法人又は団体であって、前各号に掲げる者（以下この号において「外国法人等」という。）がその議決権の過半数を有するものその他これに準ずる事情があると認められるもの（当該外国法人等が当該加入構成員の経営等を支配しているとは明らかに認められないものを除く。）

3.2 特定秘密保護法

平成 25 年に制定された特定秘密の保護に関する法律では、「行政機関の長は、公になっていないもののうち、その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であるものを特定秘密として指定する」としている[9]。また、特定秘密の取扱いの業務を行うことができる者は、適性評価により特定秘密の取扱いの業務を行った場合にこれを漏らすおそれがないと認められた行政機関の職員若しくは事業者の従業者又は都道府県警察の職員に限られている。また特定秘密を扱う企業は「適合事業者」と呼ばれ、特定秘密保護法第五条第 4 項～6 項でその扱いが定められている。適合事業者に求める実際の運用は、行政機関ごとの通達により示されているようであるが、装備品等の調達に係る秘密等の保全又は保護の確保について（通達）」（防経装第 19072 号） [10]を参考とすることができる。

4. 日米の情報共有制度とセキュリティ・クリアランスの比較

前項までに記載した日米の情報共有とセキュリティ・クリアランス制度の主な比較を表 1 に示す。

表 1　日米のサイバーセキュリティ情報共有とセキュリティ・クリアランスの比較

	米国	日本
サイバーセキュリティにおける情報共有体制とセキュリティ・クリアランス	・ISAC 間の情報共有を行う ISAO が存在する ・セキュリティ・クリアランスが求められる情報共有機能が存在する	・ISAC のみ（サイバーセキュリティ協議会に複数に ISAC が参加し、ISAC 間で情報共有されている可能性はある） ・サイバーセキュリティ協議会に参加する個人国籍、外国組織を制限しているが、米国のセキュリティ・クリアランス（に相当する）特定秘密保護法とはリンクしていない
契約事業者が秘密を扱う上での基準（産業保全）	・NISPOM で定義されている	・特定秘密保護法で定義されている

個人に対する適格性	・パーソナルセキュリティクリアランス	・特定秘密保護法による適性検査
企業に対する適格性	・ファシリティクリアランス	・特定秘密保護法による適合事業者
個人や企業の適格性に関するガイドライン	・DHS、DoD などがさまざまなガイドライン等をしめしており、解説書や教育教材などもある。	・法令や所管官庁が発行する省令や訓令といった文書はあるが、それらの解説書、教育ドキュメントは、米国並みには示されていない。
秘密の範囲	・Sensitive Information、Classified Information と表記され、民間企業が参加するサイバーセキュリティの領域でも同様の表現が用いられている。	・特定秘密保護法の規定による秘密、サイバーセキュリティ協議会の TLP の利用があり、各々ラベル付けはされているが、相互の互換性はない
親会社と子会社の関係	・NISPOM にセキュリティ・クリアランス上の扱いが示されている。	・特定秘密保護法、サイバーセキュリティ協議会ともに、具体的な定めはない。
企業の取締役等に対するセキュリティ･クリアランス	・NISPOM やその他ガイドラインで、企業で有する権限を表す役職名を用いて、具体的に示されている	・「秘密に係る情報に接する全ての者（秘密に係る情報に接する役員（持分会社にあっては社員を含む。」となっており、具体的な役職名では示されていない。

筆者が抽出した項目による比較の差分は表 1 に示すとおりであるが、セキュリティ・クリアランスが求められる企業において、役員以上、とりわけ取締役の求められる要件は重要であり、本稿ではその部分にフォーカスを当て、セキュリティ・クリアランスが求められる企業が取ることができると考えられる手法を検討する。

5. 本稿でモデルとする企業体制

大久保[11]によると、日本のユーザー企業や、多くの IT ベンダーにおける一般的なセキュリティ組織体制は、図 1 のように定義されている。

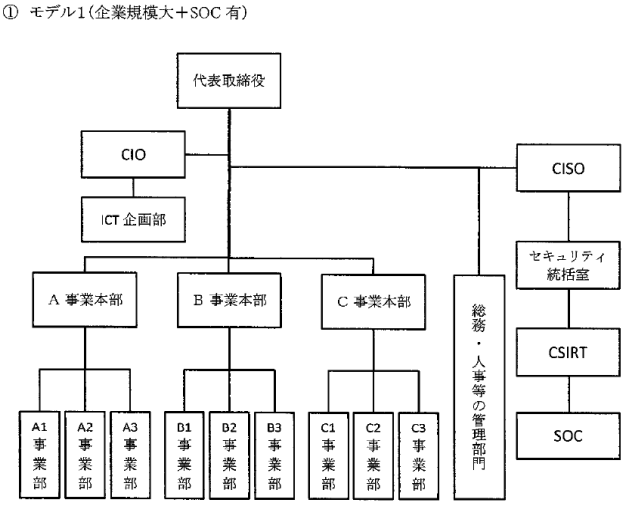

図 1　一般的なセキュリティ対応体制

このモデルに対し、(1) 〜 (3) の 3 つの視点を加えたものを、図 2 に示す。

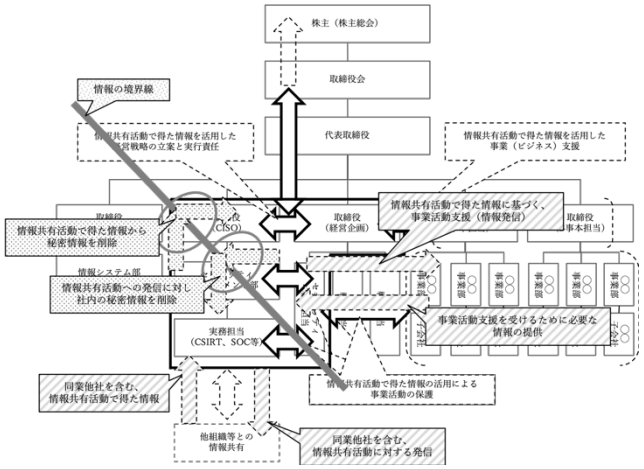

図 2　大久保のモデルの拡張（本稿のモデル）

(1) 取締役会、株主総会

NISPOM では、原則として取締役会は、米国籍で構成されることが求められる。そのため、図 1 のモデルに対し取締役会、および、株式を公開する企業において取締役を選任する株主（総会）を追加する。

(2) 経営企画機能

株式会社日本総合研究所が行った調査である「経営企画部門の実態」[12]によると、経営企画機能が新規事業の推進、ICT の利用推進を経営企画機能が担っている企業が増益していることが示されている。また、セキュリティを成長投資として考慮する事は不可欠であることから、経営企画部門が情報共有活動でえた情報を、企業の事業活動に活用する役割を担う部門として位置づける。

(3) 情報の境界線

社外との情報共有を行う上で、セキュリティ・クリアランスが求められる（情報を扱う業務）組織と、そうでない

Vol.2020-DPS-184 No.5
Vol.2020-EIP-89 No.5
2020/9/10

（業務）組織の境界線を定義する。

次に、NISPOM が求めるファシリティ・クリアランスの要件、とりわけ取締役に求める要件の実装を考える。前述までの通り NISPOM では、原則として取締役会は、米国籍で構成されることが求められる。しかしながら市場は、取締役会に対しジェンダーや国際性の面を含む多様性と適正規模を両立させる形で構成されることを求めており、取締役に国籍の条件求めるセキュリティ・クリアランスへの対応が、必ずしもその会社経営に貢献するものとは言えない場合があると考えられる。そのための解決手法の一つとして、セキュリティ・クリアランスが必要とされる範囲をその企業の外に設置するモデルを検討する。本検討にあたり、図 2 で示した情報の境界線上で分離した組織を、図 3 に示す。

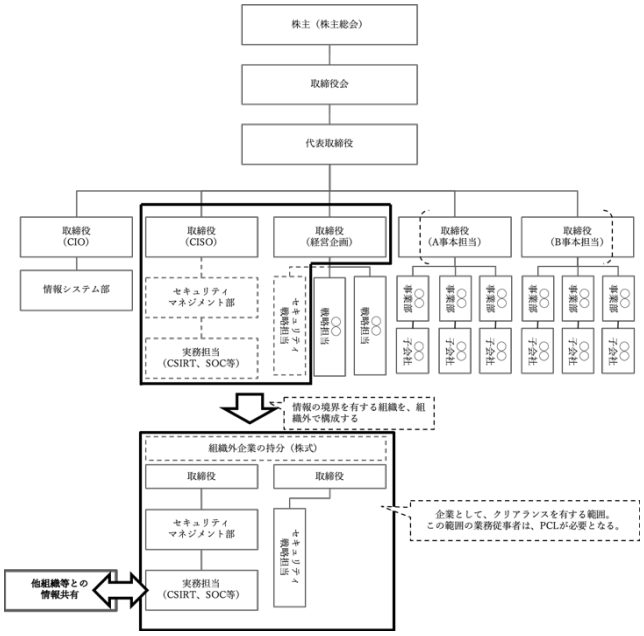

図 3　本稿のモデルから
セキュリティ・クリアランスが必要となる組織を
分離した体制

6. セキュリティ・クリアランスが必要となる企業の組織体制の提案

取締役の選任は株主の決議事項であることから、取締役が十分なセキュリティ・クリアランスをもって構成されるためには、株主の影響をコントロールする必要がある。その手段として、持分会社のうち社員の責任が有限である合同会社の適用を考慮する。合同会社は、出資者と経営者が同じ立場で、出資者全員が有限責任社員である形態のことである。よって持分会社では社員でなければ業務執行者となることができない。また持分会社では、持分（社員が会社に対して有する地位）の譲渡には、他の社員の承諾が必要となることや、社員の氏名および住所が定款の必要的記載事項とされており、持分の変更には、定款の変更が必要となる。そのため、株式を公開していない会社と同様、その会社の持分を自由に売買することができない。つまり、公開会社のように取締役を株主が選任するのではなく、会社（持分を有する社員）の意思のみで、取締役を選任できることになる。よって、企業外に設ける組織における、NISPOM をモデルとしたセキュリティ・クリアランスの対応は、以下のように整理することができる。

表 2　企業外に設ける組織における
セキュリティ・クリアランスへの対応

項目	企業外組織での対応
取締役（を含む、従業員）のパーソナルセキュリティクリアランス要件	全員、必要なレベルのセキュリティ・クリアランスを収録する
取締役の選任	株主総会、または、社員総会で行う
株主、または、社員	取締役が全株式（または持分）を有する

さて、図 3 で示した体制は、分離前の組織からみるとセキュリティ対応のアウトソースになることから、組織間の役割分担の考え方を、表 3 で検討する。

表 3　組織間の役割分担の考え方

	企業外に設ける組織で行う業務	インソース（分離前組織）で行う業務
情報共有活動に基づいた事業活動の保護	・事業リスクに直結する脆弱性情報などの収集と分析 ・事業体で実施した対策のコミュニティへの共有	・得た情報に基づく事業活動への実装
情報共有活動で得た情報に基づいた経営戦略の事業部門への展開	・情報共有活動で得た情報に基づく事業戦略の立案支援	・立案した事業戦略の実行
事業戦略の立案、および、取締役会の決定に基づく事業戦略の実行	・情報共有活動で得た情報に基づく経営戦略の立案支援	・立案した経営戦略の実行

このように、組織外組織が行う情報共有活動で得た情報に基づく企業活動は、その情報に基づくさまざまな判断と実行が一体で考えるべきであることから、組織内企業と組織外企業の取締役は兼任とし、戦略立案と実行を一手に担うことが妥当と考えられる。

Vol.2020-DPS-184 No.5
Vol.2020-EIP-89 No.5
2020/9/10

7. 提案モデルを実現するにあたり、さらに検討を深めるべき課題

7.1 分離前の組織の取締役（会）と監査役が果たす役割

本提案モデルでは、情報の境界線を CISO と経営企画を所管する取締役に引いたが、情報共有コミュニティから直接、情報を得る立場にない取締役と監査役が果たすべき役割について検討する。内閣官房内閣サイバーセキュリティーセンターが発行する『サイバーセキュリティ関係法令 Q&A ハンドブック Ver1.0』[13]等によれば、情報共有コミュニティから得た情報の主要指標を監視し適切に取締役会で報告を行うことや、情報共有活動に参加し、業界の他社等と連携していることを示すことにより、取締役会のデューデリジェンスを果たすことができるものと考えられる。

また、中長期的に事業に影響を来すと考えられる情報、つまり各事業を所管する取締役の判断を求めるため、取締役会に報告するべき情報の扱いについて考える（この場合の取締役会は、必ずしも全員が、パーソナルセキュリティクリアランスを有していないことを想定する)。このようなケースでは、取締役会に報告する情報を、刑事罰を科すことができる営業秘密として保護することが考えられるが、その情報が十分に保護されるかは、詳細な検討が必要となる。

7.2 クリアランスを有する従業員に対するアウェアネス

米国先端セキュリティ育成センター（Official Center for Development of Security Excellence : CDSE）が提供している、ファシリティセキュリティオフィサー（Facility Security Officer : FSO）向けの教材[14]には、従業員のアウェアネス向上を図るさまざまな教材が掲載されている 。そのなかには、従業員が自ら学ぶことができる e-ラーニング、ポスター、アウェアネス向上を目的としたゲーム、秘密情報漏洩に至った事例が具体的に掲載され、FSO が従業員への教育を容易に行うことができることとなっている。

7.3 出向者の取り扱い

出向は、一般的に、所属する企業に在籍したまま（雇用契約を結んだまま)、出向先の企業とも雇用契約を結ぶ「在籍出向」と、所属する企業との雇用契約を解消し出向先と雇用契約を結ぶ「移籍出向」がある。移籍出向は、いわゆる転職と同じであるため、「在籍出向」で検討するべき事項を抽出する。表 4 は、在籍出向する社員が適用される規程のモデルである。

表 4　在籍出向する社員が適用される規程例

	出向元	出向先
出向する従業員の雇用関係	雇用関係がある	雇用関係がない
出向する従業員への業務指示	業務指示を行わない	業務指示を行う
出向する従業員が従う諸規程	出向先の規程より優先される規程がある	出向元の規程に定めがない事項は、出向先の規程に従う
出向する従業員に対する懲戒	懲戒解雇事由に該当する場合は、出向先に復帰したのちに出向元の規則により懲戒を行う	懲戒解雇以外は、出向先の定めに従う

在籍出向の場合、出向する社員に適用される規程は、出向先企業の規程より出向元企業の規程が優先されるケースがある。このようなケースでは、出向者による秘密の漏えい（特に、出向先から出向元への漏えい）を防ぐためには、出向先で知り得た秘密を出向者が出向元に漏らさないようにする誓約書を出向元が出向者と取り交わしているかを確認することも、有効な手立てと考えられる。

8. 結言

次項で本研究をラップアップするにあたり、本稿執筆中であった 2020 年 8 月 13 日に毎日新聞で報道された『「技術漏らさぬ人材」国が保証　欧米並みの資格、創設方針　先端分野、対中警戒』との記事に言及しておきたい[15]。本記事では、『政府は先端技術を扱う民間人について、信用度を保証する資格制度を創設する方針を固めた。政府が審査・保証することで、国際社会に対し機密情報を漏洩（ろうえい）する恐れのない人材だと裏打ちする』としている。本稿で述べたように米国では、パーソナルセキュリティクリアランスとファシリティクリアランスは一体で考慮されており、今後日本でも同様の検討が必要となると筆者は考えている。

8.1 本研究のまとめ

本研究では、米国・NISPOM をリファレンスとして、日本の特定秘密保護法、サイバーセキュリティ協議会と比較し、セキュリティ・クリアランスが求められる企業が取ることができる組織体制を検討した。改めてその要点をまとめると以下のようになる。

- 日本の企業では、米国・NISPOM と比較し、下記の考慮が必要であることが確認できた。
  - 取締役が有するクリアランスが明確に維持する体制が求められること
  - そのために、企業が外国から受ける影響を明確に排除する体制を構築すること

これらに対する対応として、下記の提案を行った。

- 情報の境界線を定義し、セキュリティ・クリアランスが求められる範囲を明確にした

- セキュリティ・クリアランスが求められる企業の事業に影響を与えないために考慮すべき事項を抽出した
- セキュリティ・クリアランスが求められる範囲を企業の外に設置することを提案した

しかしながら、セキュリティ・クリアランスが求められる企業の経営責任、監査役の役割、従業員の教育や内部不正に関する点は、米国と日本の制度を取り上げるまでにとどまり、具体的な提案までは至らなかったため、今後継続して検討していきたい課題である。

謝辞 本研究についてご指導いただいた情報セキュリティ大学院大学の湯淺墾道教授、討論の際にご意見を頂戴した湯淺研究室の皆様に，謹んで感謝の意を表する。

参考文献

[1] “令和元年通信利用動向調査の結果（別添 2）”, https://www.soumu.go.jp/johotsusintokei/statistics/data/200529_1.pdf, （参照 2020-07-15）
[2] “情報セキュリティ 10 大脅威 2020”, https://www.ipa.go.jp/security/vuln/10threats2020.html, （参照 2020-07-15）
[3] “サイバーレスキュー隊（J-CRAT）活動状況［2019 年上半期］”, https://www.ipa.go.jp/files/000079070.pdf, （参照 2020-07-15）
[4] “Executive Order -- Promoting Private Sector Cybersecurity Information Sharing”, https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari, （参照 2020-08-17）
[5] “Information Sharing and Awareness”, https://www.cisa.gov/information-sharing-and-awareness, （参照 2020-07-15）
[6] “National Industrial Security Program （NISP）”, https://www.dcsa.mil/mc/ctp/nisp/, （参照 2020-07-18）
[7] “サイバーセキュリティ協議会について”, https://www.nisc.go.jp/conference/cs/kyogikai/pdf/kyogikai_gaiyou.pdf, （参照 2020-07-15）
[8] “サイバーセキュリティ協議会規約”, https://www.nisc.go.jp/conference/cs/kyogikai/pdf/kyogikai_kiyaku.pdf, （参照 2020-07-15）
[9] ”特定秘密の保護に関する法律 説明資料”, https://www.cas.go.jp/jp/tokuteihimitsu/gaiyou.pdf, （参照 2020-07-15）
[10] “装備品等の調達に係る秘密等の保全又は保護の確保について（通達）”, https://www.mod.go.jp/gsdf/tercom/img/file569.pdf, （参照 2020-07-15）
[11] 大久保英樹.「情報セキュリティ人材」の人材育成に関する研究 - 人的規模・育成コスト・人材活用の観点から - .情報セキュリティ大学院大学, 2020, p.34-35 情報セキュリティ大学院大学
[12] “経営企画部門の実態”, https://www.jri.co.jp/MediaLibrary/file/column/study/pdf/160406_keiei2.pdf, （参照 2020-07-15）
[13] “サイバーセキュリティ関係法令 Q&A ハンドブック Ver1.0”, https://www.nisc.go.jp/security-site/files/law_handbook.pdf, （参照 2020-07-15）
[14] “Training & Awareness, https://www.cdse.edu/toolkits/cybersecurity/training.html, （参照 2020-07-15）
[15] “「技術漏らさぬ人材」国が保証 欧米並みの資格、創設方針 先端分野、対中警戒”, https://digital.asahi.com/articles/DA3S14585191.html, （参照 2020-08-13）