2018 年 3 月 9 日

諸外国におけるサイバーセキュリティの情報共有に関する調査

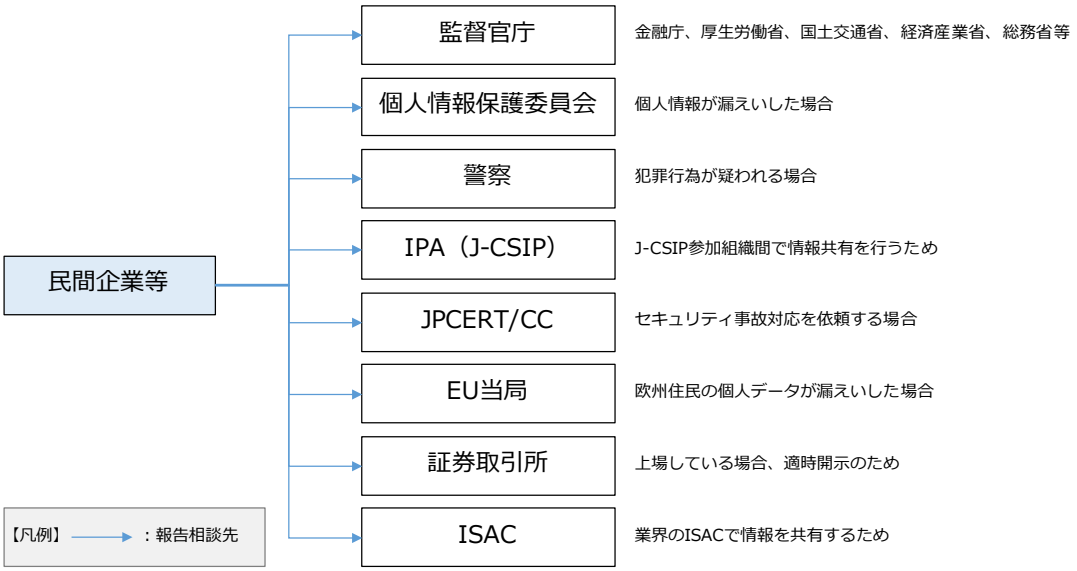
【要旨】

- 諸外国では、「サイバーセキュリティに関する法規制」を強化することにより官民の情報共有を促進し始めている。日本としては、これらの法規制によって諸外国のサイバーセキュリティ対策が実質的に強化されるのか、また官民の情報共有が徹底されるのかを見極める必要がある。

国・地域	主なサイバーセキュリティに関する情報共有政策
米国	2015 年 2 月の大統領令に情報共有の促進が明記される。その後、業界ガイドラインで、情報セキュリティ事故検知後 72 時間以内に当局へ通知する義務等の厳しい規制が課される。
EU	欧州住民の個人情報漏えい検知後 72 時間以内に当局へ通知する義務等を課し、違反した企業は高額の制裁金対象となる。また、EU 加盟国に対して重要インフラ保護の国内法制度化を指示。
英国	英国の重要インフラ事業者が効果的なサイバーセキュリティ対策を怠った場合、最大 1700 万ポンド（日本円：約 26 億円）以下の制裁金を課す。
シンガポール	情報セキュリティ事故をセキュリティ庁（CSA）へ報告することを義務化。違反した事業者には、10 万シンガポールドル（約 820 万円）以下の制裁金、2 年以内の懲役が課される。
韓国	民間企業で発生した事故は、未来創造科学部を経由して国家サイバー安全センター（NIS）へ情報収集する体制を構築。

- 現在の日本では、情報漏えい等のセキュリティ事故が発生した場合、報告すべき公的機関等が複数あり、また事故の内容によって報告先や報告内容も複雑に変わる。そのため、まずは、サイバーセキュリティ事故発生時の報告先や報告様式等を整備する必要がある。その後、諸外国の法制度や動向を研究し、日本においても法規制を含めて、情報共有を促進する施策について慎重に検討すべきである。
- また、日本ではサイバーセキュリティの情報源が多くあり、膨大な情報から自組織に関係するものを選別しなければならず、セキュリティ人材の負荷が高まっている。今後は、組織に必要となる情報を自動的に判別し、自動的に対策を実装できる仕組みが必要である。

日本のサイバーセキュリティ事故時の報告先となる公的機関等



IPA（独立行政法人 情報処理推進機構）、J-CSIP（サイバー情報共有イニシアティブ）、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）、ISAC（セキュリティの情報共有と分析を行う組織）

1. 本調査の論点

日本では、2014 年 11 月に成立したサイバーセキュリティ基本法を大きな起点とし、産官学がサイバーセキュリティの強化について、相応の努力をしてきた。経団連が 2017 年 12 月に公開した政策提言「Society 5.0 実現に向けたサイバーセキュリティの強化を求める[1]」の中では、「価値を創出する視点」と「危機管理の視点」の両面から、サイバーセキュリティの確保に積極的に取り組むことが重要であり、経営者の意識改革が鍵を握るとした。

また、世界的にもサイバーセキュリティへの関心は高まっている。世界経済フォーラム（WEF）の「The Global Risks Report 2018[2]」では、今後 10 年で発生する可能性があるリスクの第 3 位に「サイバー攻撃」、4 位に「データ詐欺や盗難」等、デジタル分野の脅威を挙げた。また、PwC が 2018 年 1 月に発表した「第 21 回世界 CEO 意識調査[3]」では、企業の成長に対する脅威として「サイバー脅威」が第 4 位であった（昨年の調査では第 10 位）。

このような中、欧米やアジアの諸外国では、より先進的かつ戦略的な政策等の取り組みに着手している。一方で、日本は 2018 年夏を目途に、サイバーセキュリティ戦略やサイバーセキュリティ基本法の改正を検討している段階だ。本調査報告書では、諸外国の動向を踏まえ、日本が取り組むべき情報共有の課題について、以下の論点で整理する。

- なぜ、情報共有は必須なのか
- なぜ、諸外国では情報共有が進むのか
- 日本の現状と課題

[1] http://www.keidanren.or.jp/policy/2017/103.html

[2] https://www.weforum.org/reports/the-global-risks-report-2018

[3] https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2018/gx.html

2. なぜ、サイバーセキュリティの情報共有が必須なのか

IoT、仮想通貨、自動運転車等のデジタル技術が発展する一方で、サイバー空間における脅威は増大している。もはや 1 つの組織だけでサイバー攻撃に対峙することは不可能になっているため、情報共有活動によって攻撃動向や防御手法に関する情報（図表 1）を入手し、被害を未然に防ぐ、若しくは攻撃を受けても被害を最小化する必要がある。

経済産業省が公開している「サイバーセキュリティ経営ガイドライン」でも、「情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供（指示 10）」と明記されており、経営者が指示すべき重要 10 項目の内の 1 つとして、情報共有活動を挙げている。

最も効率的な情報共有は、同業他社のセキュリティ事故情報である。同じ業界であれば、同じ攻撃手法が用いられることが想定されるため、いち早く情報を入手し、自社のセキュリティ強化に繋げることは非常に有効である（図表 2）。しかし、同業他社の情報を合法的に入手することは困難である。そのため、国の主導でサイバーセキュリティに関する情報を共有し、被害を防ぐ、若しくは被害を受けても最小化する必要がある。

このように、サイバー空間の脅威情報等を情報共有することは、他社で発生した被害を自社で未然に防止することができる等、大きなメリットがある。一方で、国がどこまで情報共有に対する強制力を行使するかについては、後述の通り各国の考えが政策に表れだしている。

図表 1　脅威情報の種別

情報の種別	具体例
攻撃に関する情報	攻撃者の目的／手口／人物像、攻撃手法やツール、利用される脆弱性、発生した事故情報等
防御や検知に関する情報	攻撃で用いられるファイル名／IP アドレス／ドメイン名、標的型メール攻撃の件名／送信元情報等

図表 2　脅威情報を共有することのメリットや留意事項

情報共有のメリット	• 自社では得られない有用な情報の入手 • 業界に特化した攻撃情報の入手 • 報道等では公開されない攻撃情報の入手 • 他組織で実施した防御手法に関する情報の入手 • 政府や警察機関等からの支援
情報共有の留意事項	• 政府機関等に情報提供する動機付け • 情報共有相手に対する信頼 • 機密情報や個人情報の取り扱い • データ共有の標準化、互換性 • 情報共有による法的責任

3. 官民連携で出遅れる日本

国連機関である国際電気通信連合（ITU）が 2017 年 7 月に発表した「Global Cybersecurity Index（GCI）[4]」によると、日本は世界の中で第 11 位（全体の 12 番目）にランクされている。この調査は、法、技術、組織、能力構築、連携という 5 つの要素に焦点を絞って、134 カ国のサイバーセキュリティ能力を評価し、25 個の基準で各国を格付けしたものである。

GCI の 25 個の評価項目の内、日本は「評価基準」、「動機付けの仕組み」、「官民連携」の 3 つの分野で Initiating（初期段階）と評価されており、サイバーセキュリティ上位国との相違が明らかになった（図表 3）。サイバーセキュリティ分野でリードする諸外国は、定期的に国や組織のサイバーセキュリティを評価し、課題を解決するために制裁金制度を含む法規制等で官民連携を強化しつつある。本調査報告書では、諸外国がこれらの項目について、具体的にどのような取り組みを行っているのかを明確にし、日本の課題を考察する。

図表 3 Global Cybersecurity Index における日本のウィークポイント

#	Member State	GCI Score	Cybersecurity metrics	Incentive mechanisms	Public-private partnership
1	Singapore	0.925			
2	United States of America	0.919			
3	Malaysia	0.893			
4	Oman	0.871			
5	Estonia	0.846			
6	Mauritius	0.830			
7	Australia	0.824			
8	Georgia	0.819			
8	France	0.819			
9	Canada	0.818			
10	Russian Federation	0.788			
11	Japan	0.786			

【凡例】 Leading Maturing Initiating

Cybersecurity metrics（評価基準）：国レベルのサイバーセキュリティ成熟度評価基準を定め、定期的に定量的に評価するもの
Incentive mechanisms（インセンティブの仕組み）：自国のサイバーセキュリティに対する動機付けや支援
Public-private partnerships（官民連携）：官民が協力して、インシデント予防や対応に協力する仕組み

[4] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx

4. なぜ、諸外国では情報共有が進むのか

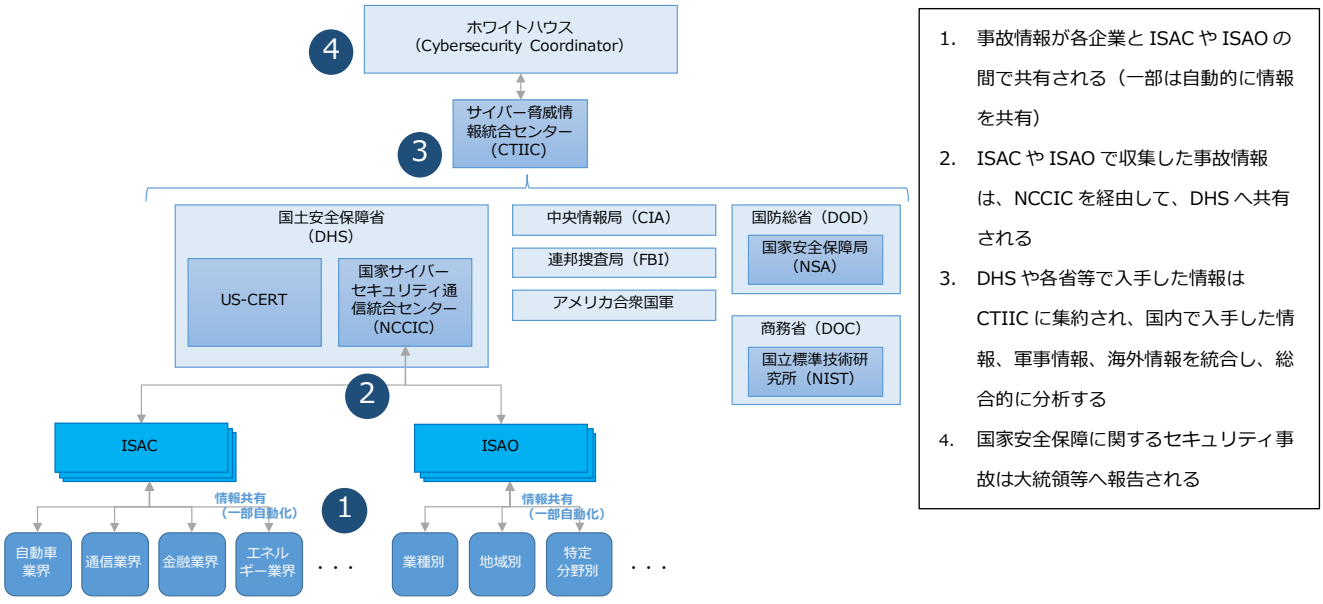
情報共有のインセンティブとなっているものは、自社で得られない脅威情報を入手できる、政府から支援を受けられる等が挙げられるが、諸外国において最も顕著な動機付けは「サイバーセキュリティに関する法規制」である。つまり、情報共有等を義務化し、違反した場合に制裁金や事業停止等の重い罰則を課すことが、重要インフラ事業者がサイバーセキュリティに投資をする最大の理由になっている。本章では、諸外国の情報共有について、主に法制度の面からまとめる。

① 米国の例（大統領令と業界ガイドラインによる規制）

米国では、重要インフラ事業者の業界（セクター）ごとに脅威や脆弱性に関する情報の共有・分析を行う「ISAC（Information Sharing and Analysis Center）」の設置が 1999 年頃から始まった。また、従来の重要インフラ分野に留まらず、一般の民間部門でも情報共有を広く進めるための組織が必要になっていることから、2015 年 2 月の大統領令 13691 号にて、「ISAO（Information Sharing and Analysis Organization）」の設置が推奨され、その後 ISAO は重要インフラ産業のみならず、各分野や地域毎に設立された。この ISAO では、情報共有の自動化を推進するために、フレームワーク/プラットフォーム/データ形式の標準化が進んでいる。

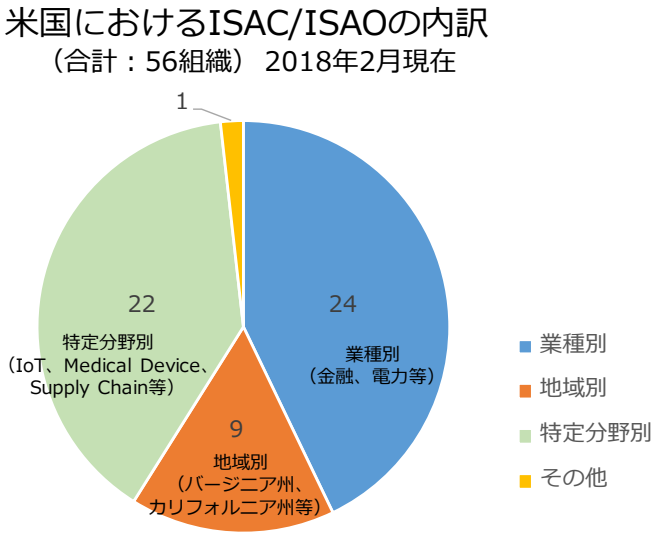
2018 年 2 月現在、米国には ISAC/ISAO が 56 組織[5]存在しており、これらの組織で収集したセキュリティ事故情報等は、国家サイバーセキュリティ通信統合センター（NCCIC）を経由して、国土安全保障省（DHS）へ共有する仕組みの構築を目指している（図表 4）。

図表 4 米国の情報共有の仕組み[6]



[5] https://www.isao.org/information-sharing-groups/

[6] https://www.ipa.go.jp/files/000044581.pdf （Page 6 を基に JCIC にて作成）



2015 年 2 月の大統領令 13691 号以降、民間企業から米国政府への情報提供に関する法制度が徐々に整備されている。まず、同年 10 月に可決された「サイバーセキュリティ情報共有法」では、民間企業が顧客のプライバシー侵害等を理由に情報共有を拒否できないような法整備を行った。これにより、主にアップルやグーグル等の IT 大手企業から米国政府がセキュリティ事故情報を得やすくなった。

また、医療機器や金融の特定業界では、厳しい罰則規定が設けられている。米国食品医薬品局（FDA）は、医療機器の脆弱性を発見した場合、60 日以内に修正し、利用者に通知することを要求している。ニューヨーク州金融サービス局（DFS）は、セキュリティ事故検知後の 72 時間以内に監督当局に通知する義務等を課し、違反した場合はニューヨーク州での金融免許を無効化する（図表 5）。

このように、米国では情報共有に関する法規制を急速に整備しており、今後も業界や地域ごとに新たな法規制が制定されると見込まれる。

図表 5　米国における情報共有に関する法規制

法規制	年月	概要
大統領令 13691 号	2015 年 2 月	産官学の幅広い分野にわたりサイバーセキュリティの情報共有を促進するため ISAO の設置を推奨
Cybersecurity Information Sharing Act（CISA）（サイバーセキュリティ情報共有法）	2015 年 10 月	サイバー脅威情報に関する官民共有手続きを整備。民間企業が共有する際の法的責任（プライバシー侵害等）を免除
医療機器のサイバーセキュリティ管理に関するガイドライン（米国食品医薬品局（FDA））	2016 年 12 月	医療機器の脆弱性の発見した場合、60 日以内に修正し、利用者に通知することを要求している。また、医療機器メーカーは、ISAO のメンバーに加入し、情報公開プロセスを整備することも要求
金融サービス企業に対するサイバーセキュリティ要件（ニューヨーク州金融サービス局（DFS））	2017 年 3 月	セキュリティ事故検知後の 72 時間以内に監督当局に通知する義務等、厳しい規制が課されており、違反した場合はニューヨーク州での金融サービス免許を無効化

② EU の例（厳格な法規制によるサイバーセキュリティ強化）

EU は、米国に比べ、サイバーセキュリティに関する法規制に積極的である。まず、2013 年に「EU サイバーセキュリティ戦略」を公表し、その後も EU 加盟国に対するサイバーセキュリティの情報共有を促進している（図表 6）。その中で、現在最も注目を集めているのが「EU の一般データ保護規則（General Data Protection Regulation；GDPR）」である。GDPR は、欧州住民の個人データを取り扱う全ての企業に対して、情報漏えい検知後の 72 時間以内に当局へ通知する義務を課した。また、違反した企業は高額の制裁金（前年度の全世界年間総売上額の 4%、または 2,000 万ユーロのいずれか高い方の金額が上限）が課せられる。

また、「NIS 指令（The Directive on Security of Network and Information Systems）」にも注視する必要がある。この指令では、EU 加盟国は自国の重要インフラ事業者に適切なセキュリティ対策を講じさせ、サービスに重大な影響を与えるセキュリティ事故の報告を義務付けることが記載されており、EU 加盟国は 2018 年 5 月までにこの規定を国内法制度化する。

図表 6　EU のサイバーセキュリティ政策動向

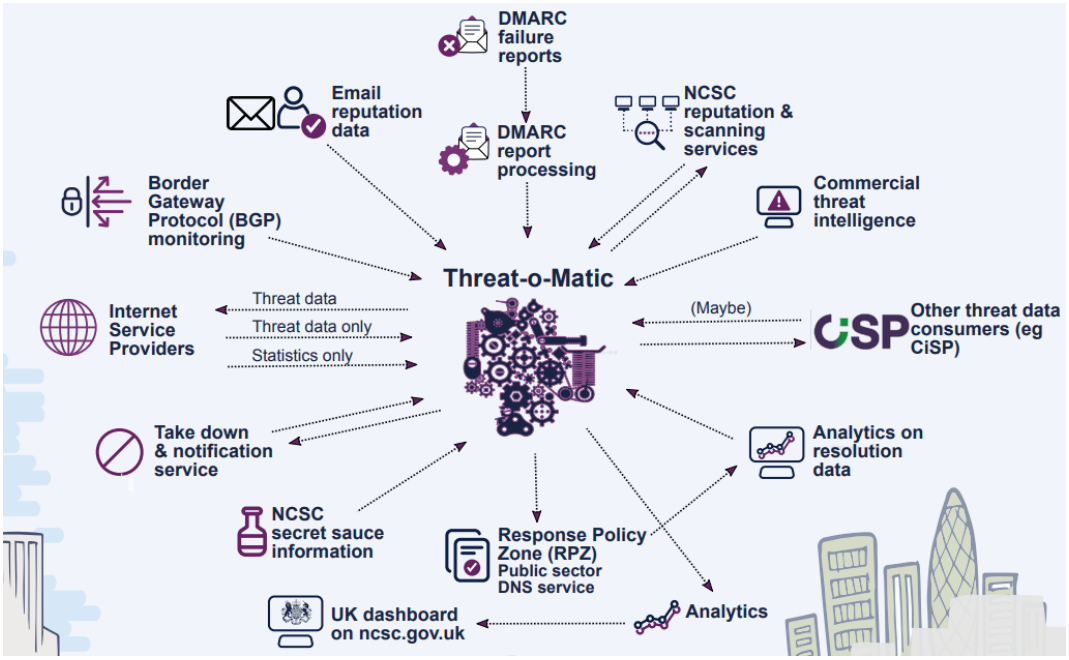
年月	内容
2013 年 2 月	「EU サイバーセキュリティ戦略」を公表。オープン、安全、セキュアなサイバースペースを目指す
2015 年 4 月	「セキュリティに関する欧州の行動計画」を公表
2016 年 7 月	cPPP（サイバーセキュリティに関する官民契約パートナーシップ）を構築。EU は、2020 年までに、€450M（約 600 億円）をこの取組みに投資する計画
2016 年 8 月	NIS 指令を発行。セキュリティ事故情報等の情報共有の推進等について記載されており、EU 加盟国に対して 21 か月以内（つまり、2018 年 5 月まで）に国内法制度化を義務付けた
2017 年 9 月	サイバーセキュリティ強化に向けた政策パッケージを公表。EU 内にサイバーセキュリティ庁設置するとともに、「ICT サイバーセキュリティ認証に関する規則案」を公表
2018 年 5 月	NIS 指令に基づき、EU 加盟国が重要インフラ事業者の保護に関する国内法制度の整備完了。 また、GDPR が施行され、情報漏えい検知後 72 時間以内に当局へ通知する義務等が課され、違反した企業は高額の制裁金対象となる

③　英国の例（効果的なセキュリティ対策を怠った場合、約 26 億円の制裁金を科す）

2015 年までの英国では、企業のサイバーセキュリティ対策は企業の自主性に任せており、情報共有に関しても各政府機関と企業が独自に情報を共有していた。しかし、「国家サイバーセキュリティ戦略 2016-2021」により、サイバーセキュリティ関連機能を GCHQ 内の NCSC（National Cyber Security Center）に集中させる方針が打ち出され、大幅な政策変更が行われた。

2016 年 10 月設立された NCSC では、重要インフラ事業者のガイダンス作成、中小企業や個人に対するアドバイス、人材育成のためのトレーニング等を実施している。また、英国へのサイバー攻撃に半自動的に対応するため、「Active Cyber Defence（ACD）プログラム」をインターネットサービス事業者（ISP）と共に構築し、政府機関へ展開している（図表 7）。

図表 7　英国 NCSC が推進する Active Cyber Defence（ACD）プログラム [7]



2018 年 1 月 28 日、英国政府は重要インフラ事業者に対して、効果的なサイバーセキュリティ対策を怠った場合、「最大 1700 万ポンド（日本円：約 26 億円）以下の制裁金を科すことがあると発表した [8]。業界専門の規制当局が任命され、重要インフラが保護されているかを評価し、指摘する体制とした（図表 8）。

前述の通り、EU の NIS 指令では、EU 加盟国に対して、重大な影響を与えるセキュリティ事故の報告義務について、2018 年 5 月までに法制度化するよう指示していた。この NIS 指令に基づき、英国でサイバーセキュリティ法令を発行した形だ。対象となる重要インフラ事業者は、エネルギー（電気、石油、ガス）、運輸、水道、通信会社、医療会社、デジタルインフラ企業等であり、サイバーセキュリティ対策を講じること、セキュリティ事故や IT 障害が発生した場合は速やかに業界の規制当局へ報告する義務が課せられる。

今回、具体的な制裁金の金額が公表されたことにより、重要インフラ事業者のサイバーセキュリティ投資が加速すると考えられる。また、他の EU 加盟国も、英国に追随する制裁金規定を設ける可能性も考えられる。

[7] https://www.ncsc.gov.uk/active-cyber-defence

[8] https://www.gov.uk/government/news/government-acts-to-protect-essential-services-from-cyber-attack

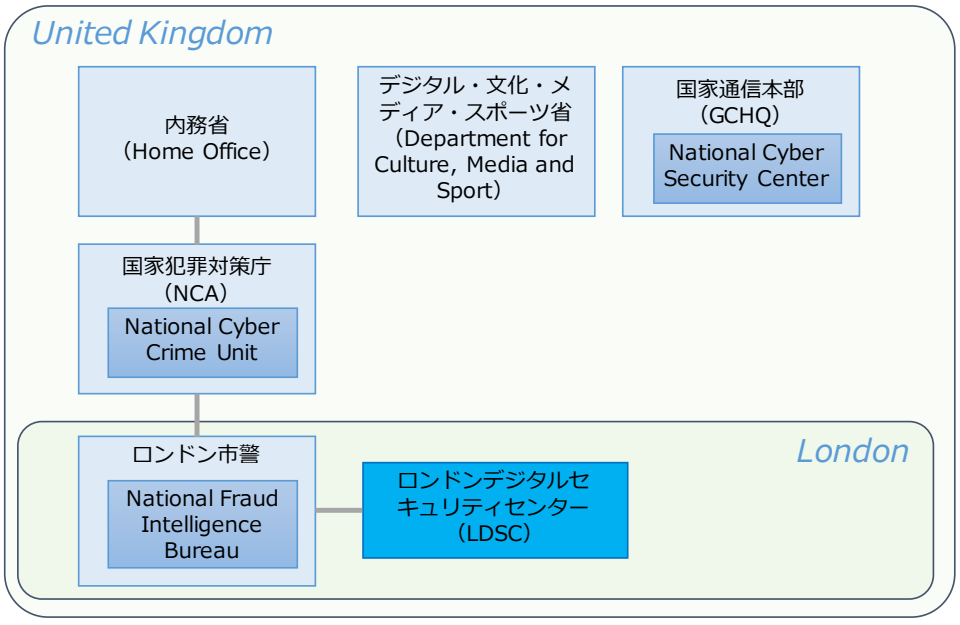
図表 8　英国が 2018 年 1 月に発表したサイバーセキュリティ法の概要

項目	説明
罰則規定	英国の重要インフラ事業者が効果的なサイバーセキュリティ対策を怠った場合、最大 1700 万ポンド（日本円：約 26 億円）の制裁金が課される
アセスメント（監査・監督）	業界専門の規制当局が任命され、重要インフラが保護されているかを評価し、指摘
対策基準となるガイダンス	NCSC が新しいガイダンスを発行。重要インフラ事業者は準拠する必要がある 1. NIS 指令の説明 2. NIS 指令 - トップレベルの目標 - 3. 関連するガイダンス 4. サイバーアセスメントフレームワーク（CAF）

また、英国では中小企業支援として、「デジタル・文化・メディア・スポーツ省」や「ロンドン市」が独自のサイバーセキュリティ施策を実施している。デジタル・文化・メディア・スポーツ省では、主に中小企業の補助金制度や人材育成支援を行っている。また、ロンドン市では、ロンドンデジタルセキュリティセンター（LDSC）を 2015 年 10 月に設立。主に小規模企業（従業員 249 名以下）がサイバー犯罪から自らを保護し安全なオンライン環境で活動できるよう支援するため活動している。英国のサイバーセキュリティ体制と概要は、図表 9 の通り。

図表 9 英国のサイバーセキュリティ体制と概要

組織名	主な活動内容
NCSC（National Cyber Security Center）	NCSC は、政府諜報機関である国家通信本部（Government Communications Headquarters：GCHQ）の一部で、英国のサイバーセキュリティリスクの軽減と耐性を向上させること目的に 2016 年に設立
デジタル・文化・メディア・スポーツ省	小規模企業を対象としたサイバーセキュリティ対策のための助成金制度があり、サイバーセキュリティ対策、専門家によるアドバイス等が助成金対象
ロンドンデジタルセキュリティセンター（LDSC）	ロンドン市長とロンドン警視庁（MPS）、ロンドン市警（CoLP）のジョイントベンチャーとして 2015 年 10 月に設立した NPO。主に小規模企業（従業員 249 名以下）を支援するために活動。会員特典や定期的なイベントを実施



④　シンガポールの例（サイバーセキュリティ法に違反した場合、制裁金と懲役を課す）

冒頭に紹介した通り、ITU が 2017 年 7 月に発表した「Global Cybersecurity Index（GCI）」で、第一位となったシンガポールでは、遡ること 2015 年 4 月にサイバーセキュリティ庁（Cyber Security Agency of Singapore：CSA）が設立され、サイバーセキュリティに関する専門機関と位置付けられた

その翌年の 2016 年 10 月には、「シンガポールサイバーセキュリティ戦略」を発表した。このサイバーセキュリティ戦略では、シンガポールの重要な情報通信インフラの強靭性を強めることやサイバーセキュリティのエコシステムを開発すること等の戦略が明記された（図表 10）。

図表 10　シンガポールのサイバーセキュリティ戦略概要

シンガポールの サイバーセキュリティ戦略概要	• シンガポールの重要な情報通信インフラの強靭性を強めること • 企業や関係団体の力を集結すること • 熟練労働者、先進的企業、研究開発等、サイバーセキュリティのエコシステムを開発すること • 強力な国際的パートナーシップ構築を推進すること

2018 年 2 月、シンガポール議会は「サイバーセキュリティ法」を可決した [9]。この法案では、重要インフラ事業者は、セキュリティ事故発生時に CSA へ報告する義務があるとした。また、違反した事業者には、10 万シンガポールドル（約 820 万円）以下の制裁金、2 年以内の懲役という罰則が課される。また、サイバーセキュリティ事業者はライセンス制とし、違反した場合の罰則（罰金や懲役）も明記された。

図表 11　シンガポールのサイバーセキュリティ法案

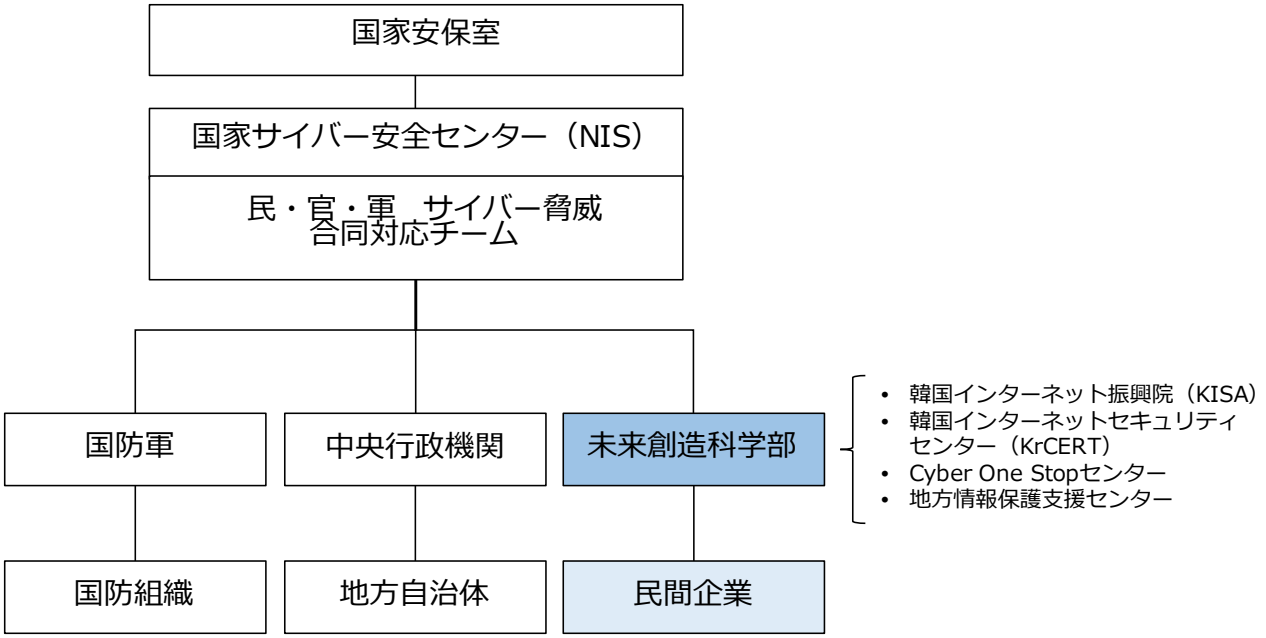
シンガポールの サイバーセキュリティ法案	• 重要インフラ事業者は、サイバー攻撃を受けた場合、直ちに CSA に通知し、事故情報を共有しなければならない • CSA には、事故調査のための強力な権限が与えられる • 違反した重要インフラ事業者には、10 万シンガポールドル（約 820 万円）以下の罰金、2 年以内の懲役という罰則が課される • サイバーセキュリティ企業は免許制とし、違反した場合の罰則（制裁金や懲役）が課される

[9] https://www.channelnewsasia.com/news/singapore/cybersecurity-bill-passed-in-parliament-mps-raise-questions-on-9929208

⑤　韓国の例（政府機関がワンストップ相談窓口を設置）

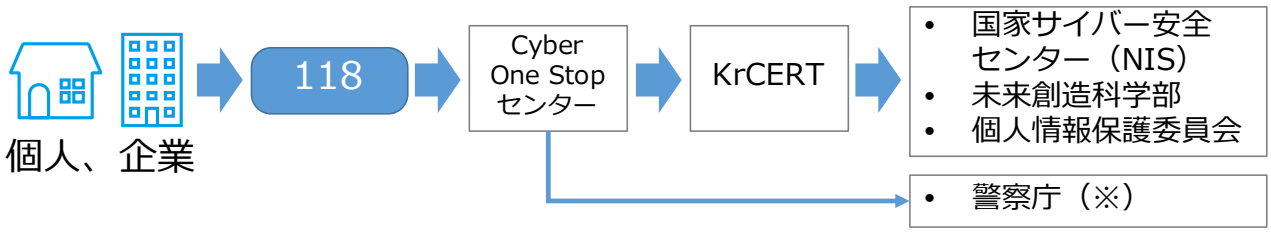
韓国のサイバーセキュリティ体制は、「国家安保室」が中心となって、民・官・軍が連携する体制である。民間企業で発生したセキュリティ事故情報の共有等は、「未来創造科学部」を経由して、国家サイバー安全センター（NIS）へ情報集約される。未来創造科学部には、サイバーセキュリティに関する 4 つの組織があり、それぞれが連携してサイバーセキュリティ強化に対する施策や事故対応支援を行っている（図表 12）。

図表 12　韓国のサイバーセキュリティ体制図



韓国では、企業や国民に対して、サイバーセキュリティに関する電話相談窓口（118 電話相談センター[10]）を開設しており、サイバーセキュリティ関連の問い合わせを受け付けている。セキュリティ確保に関する相談、セキュリティ事故発生時の支援依頼を行う場合、「118」へ電話を掛け、KISA に設置された Cyber One Stop センターが対応を行う。重要事故は、KrCERT を経由して NIS へ報告されるとともに、事件性のあるセキュリティ事故は Cyber One Stop センターに常駐する警察が対応する（図 13）。

図 13　韓国のインシデント支援体制



（※）警察庁が KISA 内に Cyber One Stop センターを設置。サイバー分野の専門家を同センターに専門警察官として配属させ、118 電話相談センターへの相談内容の内、警察の措置及び相談が必要なものについては、連携して迅速に対応

[10] http://www.kisa.or.kr/customer/ars.jsp 及び https://www.kisa.or.kr/business/violation/violation1_sub1.jsp

また、KISA では、「地方情報保護支援センター[11]」の運営を行っており、サイバーセキュリティに関する相談や技術支援を実施している。地方情報保護支援センターは、韓国全土に 6 か所あり、以下のサポートサービスを地域の中小企業向けに提供している（図表 14）。

図表 14 韓国 KISA のサイバーセキュリティ支援サービス [12]

項目	説明
DDoS サイバー待避所サービス	DDoS 攻撃を受けているサイトへの DDoS トラフィックを別ネットワークに迂回させ、分析・遮断することで、サイトが正常に運用できるようにする支援サービス
Web 点検サービス	企業のウェブサイトの安全な運営を目的に、リモートによるセキュリティ対策の点検を行い、結果報告書を作成
ソフトウェア保証診断（Secure Coding）サービス	ソフトウェアのプログラムに関わる脆弱性の点検を行い、結果報告書を作成
WHISTL サービス	ウェブサイトのセキュリティ強化のため、Webshell（バックドア）及び悪性コード探知プログラムを提供
CASTLE	ウェブサイトのセキュリティ強化のため、ファイアウォールサービスを提供
DNS シンクホールサービス	マルウェア感染した端末を攻撃者が操作できないように、感染端末と攻撃者のサーバ（C&C サーバ）との通信を遮断するサービス
ハッキングに関するリスク探知サービス	企業システムへのハッキングに関するリスクを探知・補完できる診断サービス（サービス費用の 50%を KISA が負担）
ウイルス対策プログラムの提供	特定の悪性コードを診断・対策できるプログラムを提供

2015 年に「情報保護産業振興法」が施行されたことに伴い、韓国では 2016 年に企業に対する「情報保護準備度評価制度 [13]」を導入した。情報セキュリティに努めた企業を評価する制度で、高いレベルの認証を受けた中小企業は入札や契約で優遇される。

有効期間は 1 年（年に 1 回の更新）。自己診断評価書を作成して評価機関に提出後、書面評価と現地評価を実施し、評価結果をまとめる。評価は B から AAA まである。B は基本的な情報保護管理活動が用意されている状態、A は対処能力が限定的、AAA は「優良」で侵害の脅威の予防から対処までが可能であるとの評価となる（図表 15）。

図表 15　韓国の情報保護準備度評価制度

評価	想定する企業
AAA	重要インフラ事業者
AA	多くの個人情報を保有する企業
A	大企業（非 ICT 事業者）
BB	中堅の ICT 事業者
B	中小企業（非 ICT 事業者）

[11] http://www.kisa.or.kr/business/protect/protect4.jsp

[12] https://www.boho.or.kr/event/secSupportService.do 及び https://www.krcert.or.kr/webprotect/dnsSinkhole.do

[13] https://www.kisis.or.kr/kisis/subIndex/36.do

5. 日本の現状と課題

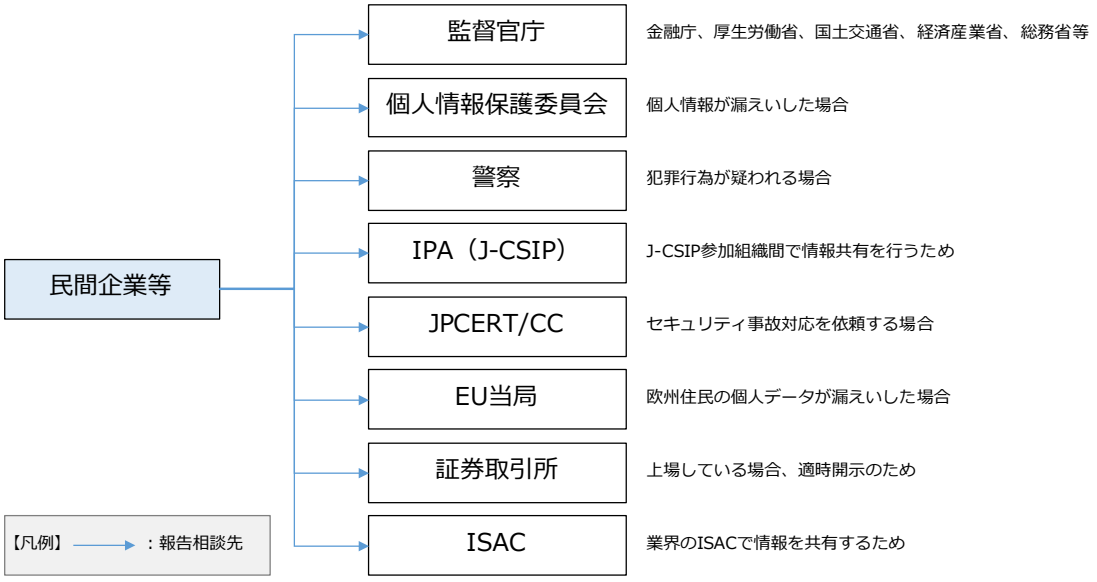
【日本の現状】

日本では、2014 年 11 月にサイバーセキュリティ基本法が国会で可決し、その後 2016 年 4 月に改正法が成立した。サイバーセキュリティ基本法では、「国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする（第十四条）」と明記されており、いわゆる重要インフラ事業者が情報共有を含むサイバーセキュリティ確保を促進するよう定めた。しかしながら、諸外国が整備し始めつつある「法規制による情報共有の強化」に関しては、日本ではいまだ整備できていない。

仮に日本で、諸外国のように、「セキュリティ事故検知後 72 時間以内に当局への報告」を義務付けた場合、日本ではどこに何を報告した時点で報告完了とするのかを定義する必要がある。日本企業で情報漏えい等の事故が発生した場合、報告すべき公的機関等が複数あるためだ（図表 16）。また、複数の報告先があるだけではなく、事故の内容によって報告先も複雑に変わる。

実際に、警察、IPA（独立行政法人 情報処理推進機構）、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）への報告相談件数をみると、企業や国民の報告相談先がばらばらであることがわかる（図 17）。この報告相談内容は、それぞれ目的や趣旨が異なるため、一概に件数だけで判断することはできないが、国内に報告先が複数ある証左といえよう。

図表 16 セキュリティ事故発生時の報告先となる公的機関等



図表 17 各組織へのセキュリティ事故報告数（平成 29 年度上期（2017 年 4 月から 9 月末まで））

組織名	報告相談内容	件数
警察	不正アクセス等、コンピュータ・ウイルスに関する相談件数 [14]	6,848
IPA（J-CIPS）	情報提供数 [15]	1,270
JPCERT/CC	報告されたセキュリティ事故総数 [16]	10,221

[14] http://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf

[15] https://www.ipa.go.jp/security/J-CSIP/index.html

[16] https://www.jpcert.or.jp/ir/report.html

また、サイバー攻撃に関する脅威情報や脆弱性情報を入手する情報源（ソース）も多岐にわたる。組織の CSIRT[17]の担当者は、複数の情報源やコミュニティ（図表 18）から 24 時間態勢で最新の情報を入手し、膨大な情報量から自組織に関係する情報を選別し、対処が必要な場合は関係部署に連絡し対策を講じるよう連絡しなければならない、しかし、セキュリティ人材不足の昨今では、いつ発生するかわからない脅威に対して、万全の態勢を敷くことは非常に困難である。

複数の情報源から膨大な情報を人手で選別することは現実的ではないため、人手を介さずに自動的に情報共有する仕組みが整いつつある。米国国土安全保障省（DHS）は、官民でサイバー攻撃の脅威情報を迅速に共有する取り組みとして、自動インディケーター共有（AIS）を推進しており、NISC（内閣サイバーセキュリティセンター）もプログラムに参加している [18]が、まだ日本中には広がっていない。

図表 18　主な脅威・脆弱性情報源（セキュリティベンダーの脅威・脆弱性情報は除く）

組織名【サービス名】
内閣サイバーセキュリティセンター【注意・警戒情報】
内閣サイバーセキュリティセンター、セプターカウンシル
警察庁【@Police】
IPA 【ICATalerts】
IPA 【JVNiPedia】
IPA、JPCERT/CC【JVN 脆弱性レポート】
IPA、J-CIPS
JPCERT コーディネーションセンター
フィッシング対策協議会
日本シーサート協議会（NCA）
地方公共団体情報システム機構（J-LIS）
警視庁サイバーセキュリティ対策本部
日本サイバー犯罪対策センター（JC3）
セキュリティ対策推進協議会　【SPREAD】

【日本の課題】

- 将来的には、日本でもサイバーセキュリティ事故に関する報告義務や罰則規定等を法制度化することを検討すべきであるが、まずは、サイバーセキュリティ事故発生時の報告先を整備する必要がある。その際は、「どのような項目を」、「どのような粒度で」、「どのような様式」で報告すべきかを明確にする必要がある。
- また、情報収集に関しては、自組織に必要となる情報を自動的に判別し、自動的に対策を実装できる仕組みが必要である。そのためには、政府機関が主導して「データ共有の標準化」や「様々な機器や環境での互換性の確保」を推進する必要がある。

[17] Computer Security Incident Response Team の略。サイバー攻撃による情報漏えいや障害等、インシデントに対処するための組織

[18] http://www.mofa.go.jp/mofaj/files/000275181.pdf

[本調査に関する照会先]

主任研究員　上杉謙二　uesugi@j-cic.com

主任研究員　平山敏弘　hirayama@j-cic.com

一般社団法人　日本サイバーセキュリティ・イノベーション委員会
Japan Cybersecurity Innovation Committee (JCIC)
〒107-0062 東京都港区南青山 2-2-8DF ビル 6F
https://www.j-cic.com