EU諸国及び米国における情報共有体制に関する調査報告書

2017年3月

内閣官房　内閣サイバーセキュリティセンター(NISC)

※本調査はNISCの委託により、マカフィー株式会社が実施したものです。

目次

１．本調査の概要

①　背景と目的

我が国の重要インフラにおける情報共有強化の施策への活用を目的として、EU諸国及び米国における情報共有体制等に関する調査を実施した

■背景

国民生活及び経済活動は、様々な社会インフラによって支えられており、特に情報通信、電力、金融等、その機能が停止又は低下した場合に多大なる影響を及ぼしかねないサービスは、重要インフラとして官民が一丸となり重点的に防護していく必要がある。今日、重要インフラサービスの提供には、情報システムが幅広く用いられており、サイバー攻撃等による障害の発生を可能な限り減らすとともに、仮に障害が発生した場合には、これを速やかに検知し、迅速な復旧を図ることが重要である。

政府は、「重要インフラの情報セキュリティ対策に係る第3次行動計画」（平成26年5月19日情報セキュリティ政策会議決定、平成27年5月25日サイバーセキュリティ戦略本部改訂）（以下「行動計画」という。）において、重要インフラとして13分野を選定し、各種施策とその対象となる重要インフラ事業者等を定めるとともに、内閣官房内閣サイバーセキュリティセンター（以下「NISC」という。）及び各重要インフラ所管省庁が連携し、重要インフラ分野内、分野間及び官民間において情報共有を行い、必要な情報セキュリティ対策に取り組んでいる。

近年、サイバー攻撃は、複雑化・巧妙化し続けており、多様な脅威に的確に対抗するためには、官民が連携してサイバー攻撃の可能性がある障害情報等を共有していくことが重要である。

■目的

我が国では、「サイバーセキュリティ戦略」（平成27年9月4日サイバーセキュリティ戦略本部決定）等に基づき、情報共有の強化を行うこととしているところ、本調査では、重要インフラの情報セキュリティ対策の向上及びそれによる安定的なサービス提供を目的とした政策の企画立案等に活用するため、EU諸国(英国、ドイツ、オランダ、フランス)及び米国における情報共有体制やその背景（環境の変化）に関する調査を行うものである。

② 調査手法

本調査では文献等調査及びヒアリング調査を手法として用いる

■文献等調査

- ✓ 各国政府の政策、公開資料、*Web*ページ等より得られる情報から、**情報連絡、情報提供の経路、及び各重要インフラ分野間における情報共有の状況を調査する**。
- ✓ 過去の*NISC*の類似調査等の資料を積極的に活用し、調査実施においては**各調査以降の状況変化及び重要と考えられる最新情報の調査に焦点を当てる。**
- ✓ *ENISA*（欧州ネットワーク情報セキュリティ庁）の持つ**欧州における各重要インフラ分野の*ISAC*を含めた情報共有に関する取り組みについての最新情報を確認し調査を行う。**

■ヒアリング調査

- ✓ 文献等調査を行った**各国政府機関、情報共有組織及び重要インフラ事業者に関する質問を行い、情報共有の実態等を引き出す。**
- ✓ 単純な訪問先からのヒアリングに終始することなく、**日本国内及び過去の類似調査で得られた知見を積極的に発信し、ヒアリング先にとってもメリットのある議論**を行う。
- ✓ 情報共有体制が**機能した事例（グッドプラクティス）**または**機能しない事例（他の体制・手段の活用等が有益または優先と判断された事例）**について集中して聞き出す。

③ ヒアリング対象国

文献等調査より得られた情報を基にヒアリング調査対象国(英国、ドイツ、オランダ)を選定した。

国名	ヒアリング対象とした理由	文献等調査より得られた情報	
		情報共有に関する事項	その他の特徴
英国	政府と民間が協力してサイバーセキュリティに取り組んでいるとともに、各業界が情報共有に注力しているので、日本の施策の参考となる取組等について聞くことができると思われるため。	• 法律による規制は少なく、情報連絡は事業者の自主性に依存 • 各業界が自主的な取組によって共有すべき情報の内容を定義 • サイバー犯罪の情報収集に注力 • オリンピック以降、情報共有に注力	• National Cyber Security Centre (2016年10月設立)に多額の資金と人材を投入 • 他国に比べ、サイバー犯罪による被害額が大きいためセキュリティに注力 • 自国のサイバーセキュリティ戦略が国際標準となるよう策定に注力 • 法律による規制が弱い
ドイツ	法律によるインシデント報告の義務があるが、官民での情報共有が活発に行われており、どういった取組、施策によって活発に情報共有が行われているか聞くことができると思われるため。	• 官民ともに情報共有に注力 • サイバーセキュリティ戦略の「重要インフラ防護」の中で情報共有強化について言及 • 他国に比べ情報共有機関の数が多い	• 他国に比べ、サイバー犯罪による被害額が大きいため、セキュリティに注力 • 重要インフラ事業者等が多い • 法律による規制が強い
オランダ	ENISAから、オランダのISACの活動は盛んであるとの情報を得ており、ISACにおいて情報共有を活発に行う上でのポイント等と聞くことができると思われるため。	• ISACの活動が活発 • 情報共有を含む重要インフラのサイバーセキュリティに注力	• セキュリティに対する政府の投資金額が大きい • 政府、民間ともにセキュリティへの取組が活発

２．EU諸国及び米国における情報共有体制に関する文献等調査及びヒアリング調査結果概要

①　EUにおける情報共有の仕組み(1/2)

【法体系】

- Cybersecurity Strategy of the European Union
  (EUサイバーセキュリティ戦略)
- The Directive on security of network and information systems (the NIS Directive)
  (NIS指令)
- A Digital Single Market Strategy for Europe (DSM)
  (欧州デジタル単一市場戦略)
- The EU General Data Protection Regulation (GDPR)
  (EU一般データ保護規則)

【主な政府機関】

- The European Union Agency for Network and Information Security (ENISA)
  (欧州ネットワーク情報セキュリティ庁)
- Europol （欧州刑事警察機構）/European Cybercrime Centre (EC3)（欧州サイバー犯罪センター）
- CERT-EU（EUコンピュータ緊急対応チーム）

【情報共有組織】

- European Network for Cyber Security（ENCS）（欧州サイバーセキュリティネットワーク）
- EE-ISAC（欧州エネルギー業界情報共有分析センター）
- European FI-ISAC（欧州金融業界情報共有分析センター）

① EUにおける情報共有の仕組み(2/2)

【現状】

ENISAの分析結果※１より、情報共有の方向性(アプローチ)について以下の3つに分類されている。

・法律による「従来の規制」

・法規制により基礎づけられる共同規制と情報共有組織が自主的に設定したルールの双方を活用する「共同規制及び自主規制」

・規制に囚われず教育等を中心とした「その他」

その中で「共同規制及び自主規制」を採用している情報共有組織は、情報共有が活性化しているとの分析結果が出ており、各国の実態・文化等に合わせた形にするべきとまとめられている。また、情報共有組織において、情報の受け手だけが増えていく状態に陥りやすいという問題点があり、その解決策の１つとして、関係者が直接集まる定期会合等を開催することが述べられている。

【情報共有に関するインセンティブ】

ENISAの分析結果※２より、インセンティブは大きく「経済的インセンティブ」と「非経済的インセンティブ」に分類される。

- 経済的インセンティブの例
  - ・脆弱性やサイバー攻撃による敏速な対応によるリスク軽減
- 非経済的インセンティブの例
  - ・良質な情報が情報共有の価値を高め、信頼関係を構築できる
  - ・対話型による情報報告が情報共有の意識を高め、共有の価値やリスクを認識できる
  - ・(業界に特化している等)限られた情報共有ができる

【情報共有体制に関する参加組織内での障壁】

ENISAの分析結果※２には、重要インフラ分野の情報共有において以下のような問題についての記載がある。

・質の低い（活用しづらい）情報による弊害

・不十分な管理体制による弊害

これらの原因は「共有された情報の分析、フィードバック能力」と「共有される情報の管理」の問題に行き着く。

また、PPP※3について、は以下の様な記載がある。

・専門的なセキュリティ情報が政府機関に限定され開示できない

・関係者が持つ偏った見解が情報共有組織と法執行機関の活動の障壁となる

※１ Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches（サイバーセキュリティ情報共有：規制的及び非規制的アプローチの概要）
※２ Incentives and Barriers to Information Sharing（情報共有の障壁とインセンティブの分析研究結果）
※３ 官民パートナーシップ：Public-Private Partnership for Critical Infrastructure Protection

② 英国における情報共有の仕組み(1/3)

【法体系】
- National Cyber Security Strategy 2016 to 2021
（国家サイバーセキュリティ戦略2016-2021）

【主な政府機関】
- National Cyber Security Centre (NCSC)（国家サイバーセキュリティセンター）
- Centre for Protection of National Infrastructure(CPNI)（国家インフラ保護センター）
- Warning, Advice and Reporting Point (WARP)（警告、アドバイス及びレポートポイント）
- Action Fraud（英国不正報告センター）

【情報共有組織】
- Cyber-security Information Sharing Partnership（CiSP）（サイバーセキュリティ情報共有パートナーシップ）

【現状】

英国では、情報共有について、政府と民間企業との間でPPPを採用している。従来、英国はサイバーセキュリティ専門の政府機関を設置せず、各政府機関が独立していた。そして、企業のサイバーセキュリティ対策はCPNI等が提供する重要インフラ業界専門のセキュリティガイドライン等を中心として、企業の自主性に任せていた。しかし、昨年制定された「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等をNCSC(2016年10月設立)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。

② 英国における情報共有の仕組み(2/3)

【サイバー空間における国際的な法規制等に関する英国のスタンス】

「国家サイバーセキュリティ戦略2016-2021」において、各国とサイバー空間におけるパートナーシップの構築を国際法の合意によって強化する旨が述べられている。具体的な項目として、以下の6つが記載されている。

・サイバー犯罪行為への執行機関の役目
・海外のサイバー脅威に対する刑事責任の追及促進
・国際法の促進に伴うサイバーアプリケーションの開発強化
・国際パートナーとしての多国間協定の安全保障
・海外のサイバー脅威に対する刑事責任の追及促進
・国際法適用合意に伴う個人と国家の安全保障の確立

【共有している情報】

インシデント情報(ヒヤリハット含む)、脅威情報、早期警戒情報、ガイドライン、グッドプラクティス、監視レポート、 他の参加組織からの助言など

【共有の手段】

情報共有ツール(CiSP)、定期会合、個別会合、電子メール、電話等のコミュニケーションツール、メンバー限定のWebサイトなど

② 英国における情報共有の仕組み(3/3)

【情報共有に関するインセンティブ】

「国家サイバーセキュリティ戦略2016-2021」には、インセンティブになりうる内容として以下の4つが記載されている。

・公共と民間事業による適切なサイバーセキュリティの事業投資の確保と業界スキルの促進

・新興企業の支援や新興企業支援・投資による専門職へのサイバー部門強化

・すべての組織への英国NCSCによる的確で質の良いアドバイスサポート

・サイバーセキュリティ経済発展のため国益を駆使した企業団体へのリスク管理

ヒアリングにおいては、特に政府からや報告者へのインセンティブはないが、企業のレピュテーションリスク低減や得られる情報がインセンティブであることが挙げられた。

【情報共有を活性化する上での改善点】

ヒアリングにおいて、以下の点が挙げられた。

・人材育成の強化
・各省庁との連携の強化
・他分野との繋がりの強化
・情報共有のメリットを広める

【その他特筆すべき事項】

ヒアリングにおいて、以下の点が挙げられた。

・英国NCSCは事業者へのセキュリティ支援を行っている
・セキュリティに競争の概念はなく、業界全体のセキュリティレベルを上げるために情報共有は必要である

③ ドイツにおける情報共有の仕組み(1/3)

【法体系】
- Cyber Security Strategy for Germany
  （サイバーセキュリティ戦略）
- IT Security Act
  （ITセキュリティ法）

【主な政府機関】
- German Federal Office for Information Security(BSI)
  （ドイツ情報セキュリティ庁）

【情報共有組織】
- UP KRITIS
  （重要インフラ防護に係る官民対話プラットフォーム）
- Alliance for Cyber Security
  （サイバーセキュリティアライアンス）
- Cyber Security Sharing and Analytics (CSSA)
  （サイバーセキュリティ情報共有分析）

【現状】

ENISAの報告書等において、ドイツは法規制が強いと見られているが、BSIが公開したThe State of IT Security in Germany 2016（2016年度ドイツITセキュリティ報告書）において、UP KRITISは「BSIのリーダーシップによる情報共有の成功例」であり、成功の鍵は官民による協調的な運営と記載されている。

また、Alliance for Cyber Securityにおいても、「自主的なインシデント報告」が活発に行われ、最新のサイバーセキュリティの技術動向、メンバー間の知識・経験の共有等が進んでいることが記載されている

③　ドイツにおける情報共有の仕組み(2/3)

【サイバー空間における国際的な法規制等に関するドイツのスタンス】

　サイバーセキュリティ戦略では、国際社会における情報通信技術のグローバル化に焦点を当て、サイバー空間のセキュリティを保護できるよう国際協調の重要性が記載されている。

　例として、「情報通信技術の世界的な性質を考えると、国際的な調整と、安全保障政策に焦点を当てた外国との適切なネットワークが不可欠である。」とし、「国連だけでなく、EU、欧州評議会、NATO、G8、OSCE、その他の多国籍組織の協力を通じてサイバー空間を保護するための国際社会の一貫性と能力を確保する」等の記載がある。

【共有している情報】

インシデント情報、早期警戒情報、脆弱性情報、ITセキュリティに関する状況の情報や警告、ドイツセキュリティ機関等から提供される現状のレポート、 CERTとの情報交換、提言、調査や研究など

【共有の手段】

情報共有ツール(MISP)、定期会合、個別会合、電子メール、電話等のコミュニケーションツールなど

③　ドイツにおける情報共有の仕組み(3/3)

【情報共有に関するインセンティブ】

　　ITセキュリティ法(2017年7月発令)において、インシデント報告義務の違反について、罰金が設定されている。これは、負のインセンティブと捉えることができる。ただし、法令が発効してから２年間の実施期間を与えられているため、現在、この罰金は適用されない。

【情報共有を活性化する上での改善点】

ヒアリングにおいて、以下の改善点が挙げられた。

・迅速に情報共有を行う仕組み
・フィードバックされる情報の質・精度向上
・罰則ではない情報共有の活性化を後押しする仕組み

【その他特筆すべき事項】

ヒアリングにおいて、以下の点が挙げられた。

・政府の担当者の技術レベル、信頼関係によって情報共有が上手くいくかが変わる

④ オランダにおける情報共有の仕組み(1/3)

【法体系】
- National Cyber Security Strategy
（第二次サイバーセキュリティ戦略）
- Dutch Data Processing and Cybersecurity Notification Obligation Act
（オランダデータ処理及びサイバーセキュリティ通知義務法）

【主な政府機関】
- National Cyber Security Centrum（NCSC）
（国家サイバーセキュリティセンター）
- General Intelligence and Security Service of the Netherlands（AIVD）
（総合情報保安局）
- National Police
（オランダ警察）

【情報共有組織】
- Information Sharing and Analysis Centers（ISACs）
（情報共有分析センター）

【現状】
オランダでは、政府と民間企業、大学等が協力して情報共有に取り組んでおり、ISACの活動が活発であるという情報がENISAから得られた。ただし、オランダの各業界のISACが公開している資料等は確認できなかった。

④　オランダにおける情報共有の仕組み(2/3)

【サイバー空間における国際的な法規制等に関するオランダのスタンス】

　第二次サイバーセキュリティ戦略において「刑法を含む法律の改正と強化によるサイバー犯罪に対する国際的な取組」と「紛争予防における専門技術の集積地（ハブ）としてのサイバー外交推進」の2テーマを設定している。前者は、オランダは欧州において先導的な役割を担うべく、EuropolのEC3を例とする国際的なパートナーシップを強化し、拡大するという内容であり、後者は「サイバー外交」を推進するにあたり、国際的な専門家と政策立案者、外交官、軍関係者、NGOの集積地を目指すという内容である。

【共有している情報】

インシデント情報、早期警戒情報、脆弱性情報、ガイドライン、教育プログラム、物理セキュリティ及びサイバーセキュリティ情報など

【共有の手段】

定期会合、個別会合、電子メール、電話、チャット等のコミュニケーションツール、Webサイト、オープンソースを使った情報共有データベースなど

④ オランダにおける情報共有の仕組み(3/3)

【情報共有に関するインセンティブ】

オランダNCSCによると、ISACにおける会合の出席者は参加組織の常勤の従業員1名のみに限定している。参加者を絞ることで経営層からISACでの活動に専念しやすいよう、支援を得ることが容易となると記載されている。これは組織参加者個人へインセンティブとして作用していると考えられる。

ヒアリングにおいては、NCSCがインシデント報告をした事業者へ支援を行うこと、重要インフラ事業のために24時間365日、相談窓口を設置などが挙げられた。また、規制や罰則ではない参加者の利益となる方法が効果的と考えられている。

【情報共有を活性化する上での改善点】

ヒアリングにおいて、以下の改善点が挙げられた。

・人材育成の強化
・ISACモデルを重要インフラ分野以外に展開
・セキュリティの専門性強化

【その他特筆すべき事項】

ヒアリングにおいて、以下の点が挙げられた。

・オランダNCSCは規制機関でもなく、犯罪捜査の機関でもない中立的な立場を取っている
・オランダNCSCは事業者へのセキュリティ支援を行っている
・対面のコミュニケーションは必須であり、これによって情報共有は円滑に進む

⑤ フランスにおける情報共有の仕組み

【法体系】
- The Law on Military Programing 2014-2019 (LPM 2014-2019)
（軍事計画法）
- National Digital Cybersecurity Strategy
（国家デジタルセキュリティ戦略）

【主な政府機関】
- National Agency for Information Systems Security (ANSSI)
（国家情報システムセキュリティ庁）

【情報共有組織】
- French Information Security Club（CLUSIF）
（フランス情報セキュリティクラブ）

【現状】

フランスにおける重要インフラ分野の情報共有はANSSI主導の下、防衛分野として発達している。情報共有の重要性についてはサイバーセキュリティ戦略に記載されているものの、防衛分野は国家機密であるため、情報共有の推進に関する記載は確認できなかった。

【サイバー空間における国際的な法規制等に関するフランスのスタンス】

「国家デジタルサイバーセキュリティ戦略」において「欧州、デジタル戦略の自律性、サイバースペースの安定性」が記載されている。具体的には「フランスは、加盟国とともに、欧州のデジタル戦略的自治のためのロードマップを推進する」「国際機関への影響力を強化し、最小限の保護を適用している国々に対しても同意を得た上でサイバーセキュリティ能力を構築し、サイバー空間全体の安定に寄与する」等の項目として設定している。

⑥ 米国における情報共有の仕組み(1/2)

【法体系】
- Executive Order 13691（大統領令13691号）
- Cybersecurity Information Sharing Act (CISA)（サイバーセキュリティ情報共有法）
- Presidential Policy Directive /PPD-41（大統領政策指令PPD-41）

【政府機関】
- National Cybersecurity and Communications Integration Center (NCCIC)
（国家サイバーセキュリティ・通信統合センター）

【情報共有組織】
- E-ISAC（電力業界情報共有分析センター）
- Water ISAC（水道業界情報共有分析センター）
- Financial Service ISAC（金融サービス業界情報共有分析センター）
- Industrial Control System Information Sharing and Analysis Center (ICS-ISAC)
（産業制御システム業界情報共有分析センター）

【現状】

FCC(連邦通信委員会)が公開している、情報共有の障壁に関するレポートにおいて、各通信会社はCOMM-ISAC（通信ISAC）への参加を通じて、「ISAOの発展に協力している」と記載されている。その他、AISを利用したNCCICとのサイバー脅威インディケータのリアルタイム共有促進、US-CERTの任務への協力等が挙げられている。さらに、ISAOを広げる活動にも積極的である。

また、「個別企業と政府機関間での情報共有についての準備」について記載されており、情報共有組織を通さず、個別に政府機関と情報共有を進めようとしている動きとして注目される。

⑥ 米国における情報共有の仕組み(2/2)

【サイバー空間における国際的な法規制等に関する米国のスタンス】

CISAでは、「国務省は、サイバースペースにおける国際行動に関する合意を得るための外交戦略を策定し、サイバー又は知的財産犯罪の起訴及び防止に関する各国と協議しなければならない」との記載がある。

National Cyber Incident Response Plan(国家サイバーインシデント対応計画)では、NCCICとISACに対して、諸外国との情報共有、協力体制について推奨する記載がある。

【情報共有に関するインセンティブ】

NIST SP 800-150「Guide to Cyber Threat Information Sharing（サイバー脅威情報共有ガイド）」では、インディケータ情報の使用例を挙げ、より積極的な情報共有活動を促している。これらは、サイバーセキュリティ技術者にとってのインセンティブと考えることが可能である。

また、CISAにおいて、サイバーセキュリティの脅威指標や防御措置を他の団体又は、政府と自発的に共有した企業は、法的に保護されるとの記述がある。

【情報共有体制に関する参加組織内での障壁】

FCCの情報共有の障壁に関するレポートに以下の4つが記載されている。

- 運用上の障壁：情報共有に必要なリソースの再配分を適切に行うためには、多くの脅威情報源をフィルタリングし、その中から利用適用可能なものを検証して優先順位を定義する必要があるため、複雑で時間がかかるとされている。
- 技術的障壁：容量、正確性、品質、適時性及び情報共有に使用すべき統一された標準フォーマットと受け入れられた情報の技術的な取扱いの困難性に起因する問題が存在する。
- 経済的障壁：必要なインフラの構築、データ購入、専門人材すべてがコストとなり、複数の異なるフォーマットのデータ受信・解析との提携にもコストが発生する。
- 法的/政策的障害：サイバーセキュリティは米国の法律では比較的未定義であったため、情報共有を取り巻く様々な法的懸念が存在する。

3．まとめ

どの国においてもサイバーセキュリティを統括する機関を設置し、そこにインシデント情報等を集約している。当該機関の窓口担当者は長期間在職し、民間企業との信頼関係を構築している。また、情報共有組織の多くは、情報共有に特化したシステムを活用していることが確認できた。一方で、情報共有に関わるインセンティブ制度を積極的に採用する国はあまり見受けられなかった。

項目	EU	英国	ドイツ	オランダ	フランス	米国
サイバーセキュリティを専門とする政府機関に情報を集中させているか	○	○	○	○	○	○
法令にインシデント報告義務が規定されているか	○	ー	○	○	○	ー
国家サイバーセキュリティ戦略に情報共有の推進について記載されているか	○	○	○	○	ー	○
情報共有組織の運営について、協調的なアプローチを採用しているか	○	○	○	○	ー	○
情報共有の枠組に警察機関、情報機関が協力しているか	○	○	ー	○	○	ー
情報共有において、インセンティブに関する制度はあるか	ー	ー	ー	ー	ー	○ (免責)
情報共有に特化したシステムを使用しているか	ー	○	○	ー (検討中)	ー	○

４．考察

ヒアリング調査において、多くのヒアリング対応者が「信頼(Trust)」関係が重要と強調していた。この、「信頼(Trust)」を前提として、文献等調査及びヒアリング調査結果から得られた情報共有の促進において、考慮すべき「5つの要素」及び、3つの取組を以下に示す。

情報共有を促進する際に考慮すべき要素	概要
Efficiency (効率性)	簡単かつリアルタイム性のある情報共有の仕組みがあること
Accuracy (正確性)	共有される情報の精度と技術力向上の仕組みがあること
Neutral (中立性)	情報共有組織は、規制機関でない、中立な立場であること
Unified (統一性)	情報共有組織は、単一窓口であること、かつ階層の少ない構造であること
Regulation (規制)	国民性に合わせた重要インフラ企業の政府機関へのインシデントのレポート義務の在り方

情報共有を促進するための取組

・セキュリティ人材の高度化及び定着化による信頼関係の構築

・単一の窓口への集約及び共有が可能な情報共有プラットフォーム（ツール）の構築

・集約した情報の分析・発信機能の強化