サイバー空間の脅威に対処するための
新たな産学官連携の在り方
～日本版 NCFTA の創設に向けて～

平成 25 年度総合セキュリティ対策会議　報告書

総合セキュリティ対策会議

はじめに

近年めざましい発展を遂げている情報通信ネットワーク、とりわけインターネットは、私たちの生活の利便性を向上させるにとどまらず、社会・経済活動の根幹を支える重大なシステムとして機能するに至っている。その一方で、サイバー犯罪の増加、インターネット上の違法・有害情報の氾濫、コンピュータ・ウィルスの蔓延が社会問題となるとともに、サイバー空間に対する国民の不安感も急速に高まっており、今、正に官民が連携してより効果的な情報セキュリティ対策を検討・実施するべき時期を迎えている。

「総合セキュリティ対策会議」は、情報セキュリティに関する産業界等と政府機関との連携の在り方、特に警察との連携の在り方について意見交換を行うことを目的として、平成 13 年度以降開催されているものである。当会議においては、情報セキュリティに関する有識者にとどまらず、電気通信事業、コンテンツ事業、コンピュータ製造・販売業、ソフトウェア産業等の各種事業に関する知見を有する方々、さらに、法曹界、教育界、防犯団体の方々という広い分野の有識者により、幅広い意見交換が活発に行われており、平成 13 年度以降、毎年度、様々な内容の報告書を取りまとめてきた。そして、こうした意見交換の結果は、例えば、平成 18 年６月のインターネット・ホットラインセンターの運営開始、平成 20 年５月のファイル共有ソフトを悪用した著作権侵害対策協議会の発足、平成 21 年６月の児童ポルノ流通防止協議会の発足、平成 24 年の不正アクセス禁止法の改正等の取組に結び付いている。

本年度は、「サイバー空間の脅威に対処するための産学官連携の在り方～日本版 NCFTA の創設に向けて～」をテーマに選定し、米国において多大な成果をあげ、米国内外で高い評価を得ている NCFTA を参考に日本版 NCFTA の創設について検討した。各委員には、それぞれが属する企業・組織における知見を背景としつつも、中立的な立場で、関係者が講じるべき具体的な取組等について議論を行っていただいた。本報告書は、これらの議論の結果を取りまとめたものであり、今後の情報セキュリティの向上及び安全・安心なインターネット社会の発展の一助となれば幸いである。

平成 26 年１月

総合セキュリティ対策会議委員長

前田雅英

総合セキュリティ対策会議の目的

昨今の官民を挙げた取組により、情報技術の急速な進展や高度情報通信ネットワーク社会が実現されつつあり、市民生活や社会・経済活動のあらゆる分野において、情報技術及び情報通信ネットワークが活用されるようになっている。

特に、インターネット等の活用により生活の利便性が向上するなど、高度情報通信ネットワーク社会の光の部分が拡大する一方、サイバー犯罪が年々増加するなど、その陰の部分とも言うべき、情報セキュリティに対する脅威も増大しつつある。情報通信ネットワークの安全性及び信頼性を確保し、国民がこれを安心して利用することができるようにすることは、高度情報通信ネットワーク社会の形成にとって不可欠な条件であり、情報セキュリティの確保は喫緊の課題となっている。

情報セキュリティについては、①情報セキュリティに対する脅威の舞台であるインターネット等の情報通信ネットワークが社会・経済活動の根幹を担う存在であり、産業界等が発展させてきたものであること、②情報セキュリティに対する脅威に的確に対処するためには、急速に発展している高度な技術の活用が必要であること等から、情報通信ネットワークに関わる広範な層の協力によってこそ確保されるものであると言える。

それゆえ、情報セキュリティに関する警察の活動も、産業界を始めとする多くの関係者・関係機関との連携が不可欠である。情報セキュリティに関する産業界等と警察との連携については、都道府県レベルでは「プロバイダ連絡協議会」等を通じた各種の取組がなされていたものの、国レベルではかかる広範な官民連携の場が設けられていなかったところ、平成 13 年５月に東京で開催されたＧ８ハイテク犯罪対策・官民合同ハイレベル会合（東京会合）においては、産業界等と法執行機関との連携を各国内でも議論することの重要性が改めて確認された。

総合セキュリティ対策会議は、こうした状況を受けて、情報セキュリティに知見を有する各界の有識者による意見交換の場として開催に至ったものであり、当会議における議論が産業界等と警察による情報セキュリティ対策の参考となることを期待するものである。

【これまでの議題】

平成 13 年度	情報セキュリティ対策における連携の推進
平成 14 年度	情報セキュリティに関する脅威の実態把握・分析
平成 15 年度	官民における情報セキュリティ関連情報の共有の在り方
平成 16 年度	インターネットの一般利用者の保護及び知的財産権侵害に関する官民の連携の在り方
平成 17 年度	インターネット上の違法・有害情報への対応における官民の連携の在り方
平成 18 年度	インターネット・ホットラインセンターの運営の在り方及びインターネットカフェ等における匿名性その他の問題と対策
平成 19 年度	Winny 等ファイル共有ソフトを用いた著作権侵害とその対応策
平成 20 年度	インターネット上での児童ポルノの流通に関する問題とその対策
平成 21 年度	インターネット・オークションにおける盗品の流通防止対策
平成 22 年度	安全・安心で責任あるサイバー市民社会の実現に向けた対策
平成 23 年度	サイバー犯罪捜査における事後追跡可能性の確保
平成 24 年度	・官民が連携した違法・有害情報対策の更なる推進 ・サイバー犯罪捜査の課題と対策

目　次

～本編～

～資料編～

発表資料

本　　編

サイバー空間の脅威に対処するための新たな産学官連携の在り方
～日本版 NCFTA の創設に向けて～

近年、サイバー空間を巡る脅威が大きく変化している。すなわち、情報通信技術の急速な発展を背景に、国の治安や安全保障に重大な影響を及ぼしかねない脅威が世界規模で猛威をふるっている。

これまでサイバー空間の脅威への対処は、基本的に、産業界、学術機関、法執行機関それぞれにおいて個別の事象に対して事後的に行われてきた。しかしながら、こうした脅威に対しては、各主体ごとの個別的・事後的な対処では十分に対応できないことが明らかになりつつあり、産学官（警察）が連携した形でのプロアクティブ、すなわち、先制的・包括的な対応が必要であること、また、そのためには、国際的な規模での連携も必要であることが認識されつつある。

この点、情報セキュリティ分野の先進国である米国では、サイバー空間の脅威に対処するための産学官の情報共有と協力を促進する枠組みとして、NCFTA（National Cyber-Forensics & Training Alliance）が平成９年に設立されている。この NCFTA は、“Industry First”をモットーとして、産業界が直面するサイバー空間の脅威に産学官が共同して対処するため、それぞれが持つ情報を共有・分析し、法執行機関の犯罪捜査、民間企業における情報セキュリティ、学術界における人材育成に大きく貢献している。

そこで、平成 25 年度の総合セキュリティ対策会議では、「サイバー空間の脅威に対処するための産学官連携の在り方～日本版 NCFTA の創設に向けて～」をテーマとして選定して議論を行った。本報告書は、我が国におけるサイバー空間の脅威への対処に向けた産学官連携の新たな枠組みの構築に向け、日本版 NCFTA 創設の意義、設立に向けた論点、具体的な活動等について議論の結果を取りまとめたものである。

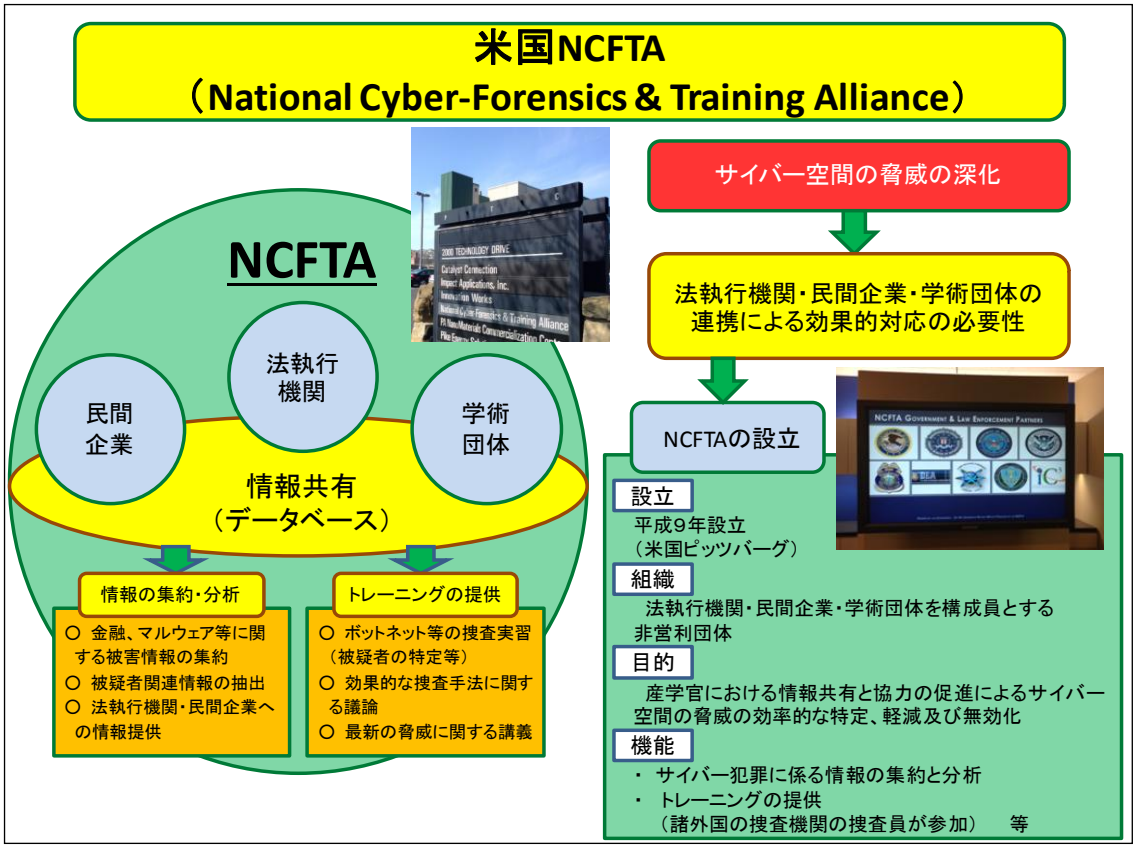
第１　日本版 NCFTA 創設の意義

１　NCFTA の概念

米国 NCFTA は、急速に複雑化・国際化するサイバー空間の脅威、特に産業界が直面する脅威への効果的な対処（脅威の特定、軽減及び無効化）を可能とするため、産業界、学術機関及び法執行機関が保有するサイバー空間の脅威に関する情報を業界横断的かつリアルタイムに収集・分析し、サイバー空間の脅威に共同で対処するための結節点として、平成９年に創設された（米国における非営利団体法人の資格取得は平成 14 年）。

創設以来、“One Team, One Goal”を掲げ、産学官が一体となって先制的・包括的な対応を行うことにより、例えば、サイバー空間における金融サービスを悪用した犯罪の捜査に関連して数千万ドルの犯罪収益の押収や被害の未然防止に貢献するなど、サイバー空間の脅威に起因する被害の予防、拡大防止、検挙等に多大な成果をあげ、米国内外で高い評価を得、各国において同様の取組が試みられている。

図１　米国 NCFTA の概要



2　我が国の産学官連携に関する現状と課題

(1)　脅威の深刻化

サイバー空間は、今や国民生活や社会経済活動に不可欠な社会的インフラとなっており、一度重大なサイバー犯罪やサイバー攻撃が行われた場合には、国の治安や安全保障に重大な影響を及ぼしかねない状況が生じている。

また、インターネットバンキングに係る不正送金事案*1のように組織的背景を有すると見られる者による犯行や国家や企業を対象とした機密情報の窃取、重要なデータの破壊等を目的とする攻撃が顕在化しており、従来と比べて脅威の質が変化している。

そして、このような脅威は、国境に関係なく極めて急速かつ広範に展開しており、一つの企業・業界等では十分に対処できないこと、そして、脅威が現実のものとなってから事後的に防御措置を講じる「受け身の対応」では根本的なサイバー空間の安全安心の確保につながらないことが明らかとなっている。すなわち、こうした脅威から国家と国民を守るためには、法執行機関が中心となって、国際的な規模で連携したプロアクティブな対処が不可欠となっている。

(2)　産学官連携の現状

我が国では、産学官がそれぞれ、サイバー空間の脅威に対処してきており、その過程で、様々な形での連携も既に行われている。

例えば、通信業界では、主要な ISP 事業者*2等から構成される一般財団法人日本データ通信協会テレコム・アイザック推進会議（Telcom-ISAC Japan）が、業界内でシステムの脆弱性やサイバー攻撃等に関する情報を収集・分析・共有し、業界横断的にタイムリーな対策を講ずることを目的として活動している。

また、一般社団法人 JPCERT コーディネーションセンターは、インターネットを介して発生するシステムへの侵入やサービス妨害等の脅威について、業種横断的に日本国内のサイトに関する報告を受け付け、対応の支援及び再発防止のための対策の検討と助言を行っているほか、それらを通じて把握した発生状況、手口の分析などを踏まえた脅威の回避策を発信している。

警察においても、民間企業等との連携に取り組んでおり、例えば、アンチウイルスベンダー（ウイルス対策ソフト提供事業者）等との間で、警察が把握した不正プログラムの提供のための枠組みを構築し、当該不正プログラムによる更なる被害拡大をいち早く防止するために、その積極的な活用を図っている。また、違法・有害情報排除対策を推進するために、一般のインターネット利用者からの通報を受理し、その中から、あらかじめ定められた基準に従って違法情報・有害情報を選別し、警察への通報やサイト管理者等への削除依頼を行うインターネット・ホットライン業務を平成 18 年から民間に委託している。

---

*1　インターネットバンキングの ID・パスワード等を盗み取るウイルスを使用する手口等により、インターネットバンキングに不正にアクセスし、正規利用者の口座から不正送金する事案。不正送金元、不正送金先及び現金引出場所が複数の都道府県にまたがるなどしており、犯行組織の関与が指摘されている。

*2　Internet Service Provider の略。インターネットに接続するサービスを提供する事業者。

(3) 課題

(2)の取組等によりサイバー空間の脅威への対応には一定の成果が見られるものの、これらはいずれも個別具体の脅威に対して事後的に防御措置を講ずる受け身の対応となっている上に、脅威の質が変化する中でこれに先制的・包括的な対応を行い、脅威の大本を無効化し、以後の事案の発生を止めることは十分にできていない。

産学官の各主体を個別に見ると、産業界は、サイバー空間の脅威に日々曝され、サイバー空間で起きていることに関する生の情報やそれに基づく知見を有している一方で、サイバー犯罪を敢行している被疑者の検挙等脅威の大本を無効化する手だては有していない。

学術機関は、研究成果の蓄積に基づく高度な情報通信技術や知識等を有する一方で、産業界や警察との情報共有が必ずしも十分ではないために、サイバー空間の脅威との「実戦」において、その真価を発揮できていない。

警察について言えば、犯罪捜査等の警察活動を通じて、その限りで切り取ったサイバー空間の特定の脅威については詳細に把握しているが、サイバー空間全体を俯瞰できているわけではなく、情報の把握には限界がある。

このように、現状の取組では、産学官それぞれのサイバー空間の脅威への対処の経験を全体で蓄積・共有し、脅威に対して先制的・包括的に対応することができておらず、それ故に、それぞれの不足を補うことも、それぞれの知見を相互に十分に活用することもできていない。その結果、サイバー空間で起きていること、あるいは、近い将来起き得ることについて、各主体とも十分に把握できておらず、サイバー空間全体を俯瞰した上で脅威の根本を絶つという対処が欠落してしまっている。

3 日本版 NCFTA の必要性

我が国の脅威の現状及びそれに関する課題を踏まえると、サイバー空間の脅威に関する生の情報や脅威に対処するための技術・知見等を有する産業界と、情報通信技術に係る研究開発等を通じて貢献する学術機関、そして、証拠の差押えや被疑者の逮捕を始めとする捜査権限を行使できる警察等の間で、それぞれが持つサイバー空間の脅威への対処の経験を、その場限り・当事者限りのものとせず、全体で蓄積・共有し、個別的・事後的な受け身の対応ではなく、警察による捜査権限の行使を始めとする先制的・包括的な対応を可能とする産学官連携の新たな枠組み、すなわち、日本版 NCFTA を創設する必要がある。

このような連携の枠組みを構築することができれば、サイバー空間において日々脅威に曝されている産業界のニーズ（顧客からの信頼の維持、経済的損失の防止等）を踏まえ、犯罪の未然防止や被疑者の検挙を始めとする警察活動が効果的に行われるとともに、各企業にとって最適な対処が行われ、また、学術機関においては、実務に即した研究材料を得ることができ、サイバー空間の安全安心の確保につながることとなる。

図２　日本版 NCFTA の概要

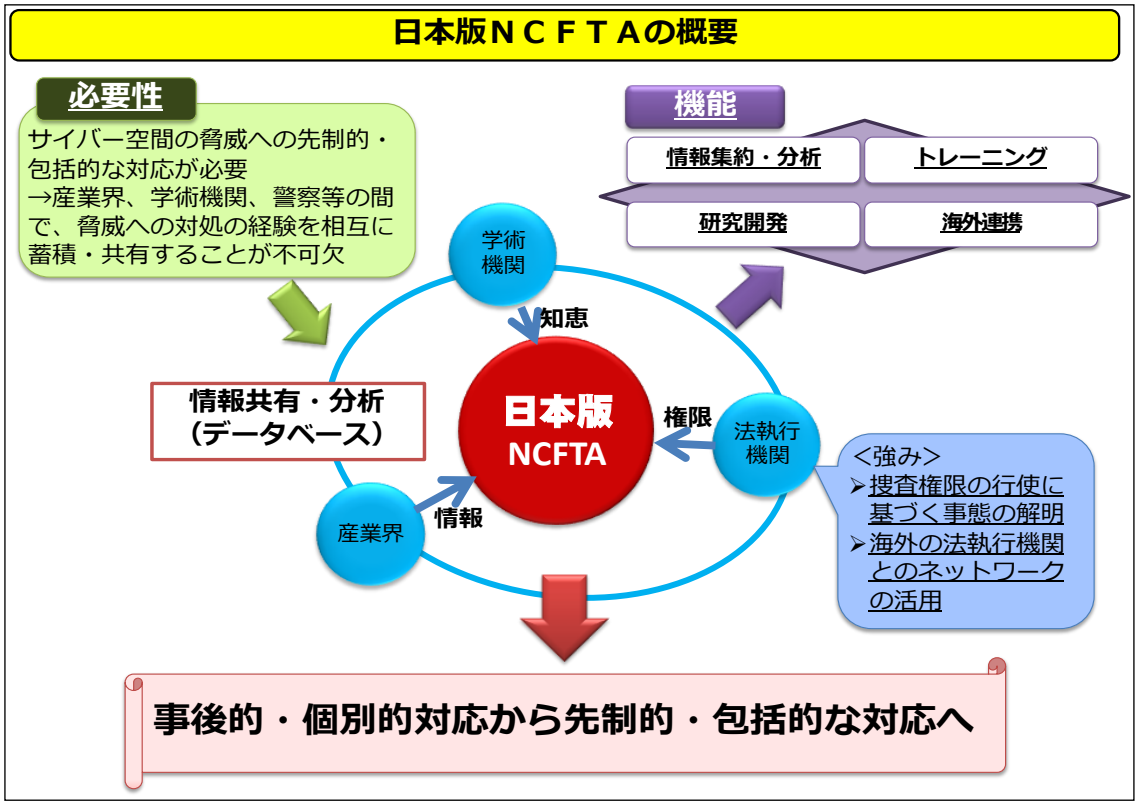
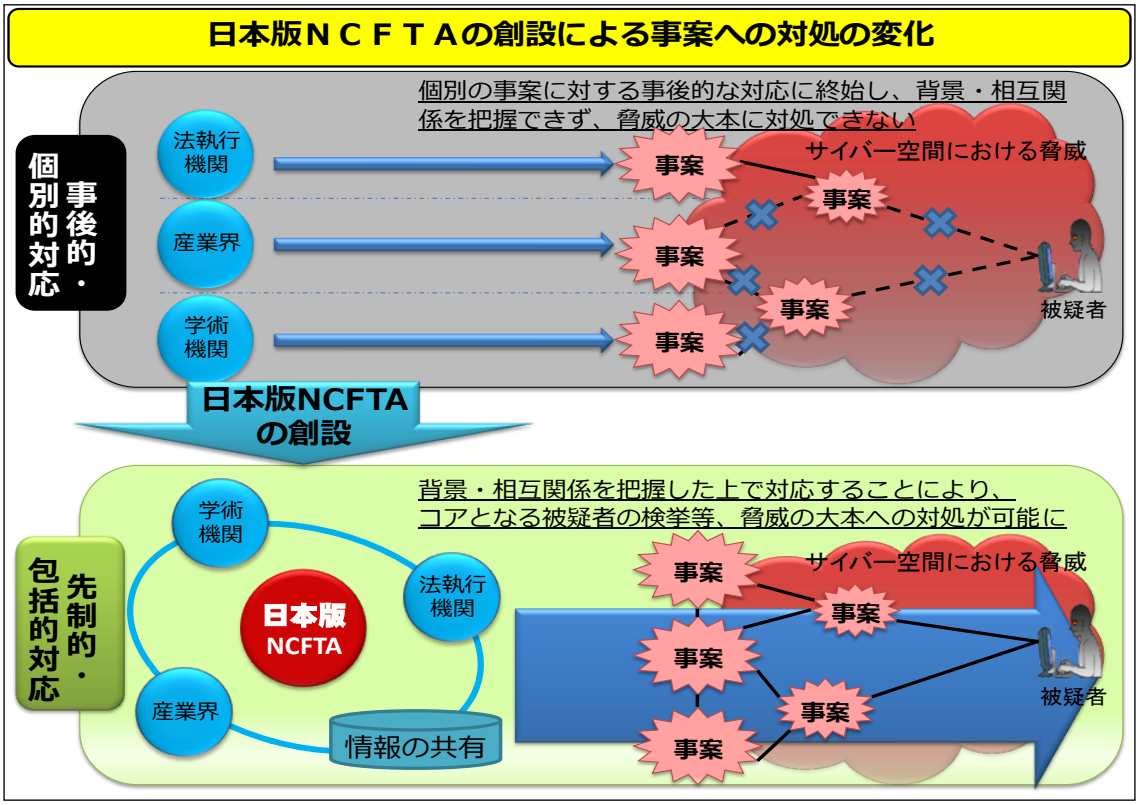


図３　日本版 NCFTA の創設による事案への対処の変化



第2　日本版NCFTAの設立

1　目的

日本版NCFTAは、産学官が同じ場を共有し、それぞれが持つサイバー空間の脅威への対処の経験等を全体で蓄積・共有するとともに、警察による捜査権限のより効果的な行使を含めサイバー空間の脅威を特定、軽減及び無効化するための先制的・包括的な対応を行うことを目的とする。

2　実施主体としての形態

組織の透明性・公平性が担保されるよう配慮すると同時に、サイバー空間の様々な脅威に対して柔軟かつ機能的に対処できる組織となるよう、日本版NCFTAの組織形態については、様々な選択肢が検討されるべきである。

3　体制

独立した組織としての業務の継続性を確保した上で、高度に専門的な枠組みとして機能するには、一定の職員を有する事務局に加え、情報を収集・整理する職員やそれらを分析する分析官、関連する各分野（法律、情報技術、海外の情勢等）に精通する専門家を配置するとともに、様々な分野から集まる者を効果的にコーディネートできる人材が必要となる。また、これらの職員等に、海外関係機関等との連携を図る上で必要となる素養を有する者が含まれるよう配慮する必要がある。

職員等については、短期的には、警察・企業等からの派遣・出向、インターンシップに基づく学生の受入れ等によって充てられることが考えられるところ、出向等することで当該職員等が待遇上の不利益を被ることがないように配慮する必要があるほか、出向等については、信頼関係の構築を図るために、出来る限り長期的な配置とすることが望ましい。また、中長期的には、日本版NCFTAとして独自に職員の採用・育成を行い、派遣・出向者と独自の職員の適切なバランスを確保していくことが望まれる。

このほか、情報保全の観点からも、業務を行うに当たっては、活動拠点を設け、そこに必要な資料や資機材を設置し、所要のセキュリティを確保することが必要である。

4　運営リソースの負担

米国NCFTAの資金、人材、ノウハウその他の運営リソースについては、参加企業及び政府機関等がそれぞれ相応の負担をしており、日本版NCFTAにおいても、各主体の参加形態や特性等も勘案しつつ、それぞれが相応に負担するべきであると考えられる。

5　参加資格・推薦制度等

日本版NCFTAは、幅広い業界の企業等との間で協力関係を築くことが望ましい反面、産学官から提供される秘匿性の高い情報を扱うことが想定されるため、情報にアクセスする資格

を、信頼できる者に限定する必要がある。

このため、個別の企業等に関する日本版 NCFTA への参加の可否については、複数の参加主体からの推薦を要件とするなどの措置を講じる必要がある。また、欠格事由を定めるほか、信頼関係を損なう行為についての対応をあらかじめ合意しておくことが望ましい。

第３　日本版 NCFTA の活動

１　具体的な活動

日本版 NCFTA の目的は、産学官が同じ場を共有し、信頼関係を構築するための産学官の結節点となり、サイバー空間における脅威の特定、軽減及び無効化のための取組を行うことである。具体的な活動として、脅威の可能性の認識から発現までの各段階において、産学官が相互に連携して情報を集約・分析し、当該脅威の内容や程度に応じた最適な対処方法（警察の捜査への協力、企業への脅威情報の提供等）を速やかに実施するとともに、その過程で得られた情報を蓄積し、将来における対処等に活用する。

このような活動を行うため、日本版 NCFTA は、次の機能を有するものとするべきである。

（1）　情報集約・分析

ア　位置付け

日本版 NCFTA の活動の中心は、サイバー空間全体をグローバルに俯瞰した上で、企業等が曝されているサイバー空間の脅威を芽（兆し）の段階で特定し、それが如何なる脅威に発展するかを分析・評価し、脅威の内容や程度に応じて、捜査を始めとする最適な対処方法を導き出すことにある。すなわち、これらの活動を支える情報集約・分析機能は、日本版 NCFTA の中核をなすものである。この機能を十分に発揮するためには、データベースを用いるなどして、産学官それぞれが保有する情報（海外関係機関等との連携を通じて得た情報を含む。）を集約し、分析できるようにすることが重要である。

なお、具体的にどのような情報をどのような形でデータベースに蓄積するかは、運用に向けて更に検討を進める必要がある。例えば、不正プログラム（使用された時期、感染経路、被害業界、動作状況等）やチャット、掲示板におけるハッカー関連情報（書き込み場所、書き込み時期、ユーザー名、書き込み内容等）等、量が多く、フォーマット化しやすいものについては、データベースに入力・蓄積することが適当であると考えられる。

イ　基本的コンセプト

日本版 NCFTA の情報集約・分析機能については、次の点を基本的なコンセプトとすることが適当である。

(ｱ)　様々な業界を横断した情報の集約

サイバー空間の脅威を俯瞰するためには、多種多様な業界を網羅する情報が集約されている必要がある。したがって、幅広い業界の企業等と協力関係を構築し、業界横断的な情報を集約するものとするべきである。

他方で、そのような情報の集約は、日本版 NCFTA が目指す最終形であり、当面は、特定のテーマあるいは業界を対象に取組を開始し、その経験の集積を通じて、取組の対象を徐々に広げていくということも現実的な選択肢として考えられる。

(ｲ)　情報の流れの双方向性の確保

情報が産・学から官のみへ流れるなど、情報の流れが一方的な場合には、参加主体は

情報を提供することに価値を見いだせなくなり、産学官連携の枠組みは機能しなくなるおそれがある。したがって、日本版 NCFTA は、情報が、産官学の間で、また、業界を横断して共有されるものとするべきであり、この点について制度面・運営面の双方から留意する必要がある。

他方で、各主体が保有する情報の質・量に差があることは当然であり、情報の流れの双方向性を過度に徹底することは、却って情報の発信・共有を阻害しかねないことにも留意が必要である。

(ｳ) 産学官による重層的・複眼的な分析による脅威の実体の特定と解明

産学官は、それぞれの目的や視点から、サイバー空間の脅威に関する情報の集約・分析を行っている。日本版 NCFTA は、産学官が保有する情報を共有・分析する場として機能するべきであり、その過程において、各主体で様々な観点からの分析が行われ、より深みのあるものとなることが期待される。

(ｴ) 脅威の実体に応じた最適な対処方法の選択と速やかな実施

日本版 NCFTA の特徴は、脅威に対して、単に情報を収集・分析するだけでなく、対処までその射程に含めることであり、更に、警察をパートナーに加えることで、対処方法の選択肢として、迅速な法執行が担保されることにある。したがって、日本版 NCFTA を運用する上では、単に脅威の実体の特定や解明に満足することなく、警察の捜査への協力や企業への脅威情報の提供等、多様な選択肢の中から、産業界のニーズを踏まえて最適な対処方法を選択し、速やかに実施することこそが目的であることを参加する各主体が認識しておく必要がある。

(ｵ) 情報の責任ある共有

日本版 NCFTA は、参加主体に情報提供を強制するのではなく、各主体が、自らが保有する情報のうち、共有することを納得したものを提供する枠組みとするべきである。

すなわち、各主体は、日本版 NCFTA における情報の取扱い規定等を踏まえ、提供可能な情報を自らの責任に基づいて提供する。その際、提供に当たっては情報の取扱いを提供者が判断できるようにするなど、情報の提供を促す仕組みを検討する必要がある。また、情報共有に当たって特定の主体にのみ過度な負担がかからないような仕組みとすることにも配慮するべきである。

ウ 提供主体及び提供される情報

情報の提供主体となる産学官は、それぞれの観点から情報を収集しており、（分析の前段として、）それらを効果的に集約・共有する場となることが、日本版 NCFTA の第一の機能と言える。例えば、情報を「個別的脅威」「全体的脅威」「技術・研究成果」に分類した場合、産学官は、得意とする分野がそれぞれ異なるものと考えられるところ、

以下の表のとおり、それぞれが得意とする分野についての情報を提供することが期待される。

	①個別的脅威	②全体的脅威	③技術・研究成果
産業界	◎ （個別の被害情報等）	◎ （不正プログラムの流行状況等）	○ （個別の脅威への対処を通じた研究の成果等）
学術機関	△ （研究の過程で入手した情報等）	△ （研究の過程で入手した情報等）	◎ （学術的な研究の成果等）
法執行機関	◎ （犯罪捜査（海外法執行機関等との連携を含む。）関連情報等）	○ （海外法執行機関等との連携を通じて得た情報等）	△ （犯罪捜査等のための技術研究の成果等）

① 個別的脅威

個々の不正プログラムの動作・特徴、C&C サーバ[*3]、踏み台[*4]の所在等、個別の事案を精査することで明らかになる脅威。

② 全体的脅威

サイバー犯罪の流行傾向、ボットネット[*5]の動向等、グローバルな観点からサイバー空間全体を俯瞰することで明らかになる脅威。

③ 技術・研究成果

サイバー空間の脅威において用いられ得る最新の情報技術等、個別的脅威及び全体的脅威のいずれにも関係する技術情報。

（◎ 関連する情報の積極的な提供が期待されるもの。
○ 関連する情報の提供が期待されるもの。
△ 関連する情報に関する協力が期待されるもの。）

エ 情報の取扱いに係るルール

イ記載のコンセプトを具現化するためには、情報の取扱いに係るルールとして、以下の点を定める必要がある。

(ア) 利用目的の明確化

日本版 NCFTA の活動を行う上で十分な情報を収集し、また、情報を適切に取り扱うためには、何のためにどのような情報を集めるのか、すなわち、情報の利用目的が明らかにされている必要がある。

---

*3 Command and Control server の略。攻撃者の命令に基づき動作するコンピュータ・ウイルスに感染したコンピュータに指令を送り、制御の中心となるサーバのこと。

*4 スパムメールの発信や他サーバへの不正アクセスを行うことを目的として不正に利用されるサーバのこと。

*5 コンピュータ・ウイルスに感染したコンピュータ及びこれらに攻撃者の命令を送信する C&C サーバからなるネットワークのこと。

(ｲ)　秘密の保持の観点への配慮

効果的な情報の集約・分析が行われるためには、情報の提供者と利用者との間の信頼関係が大前提となる。この信頼関係を構築する上では、信頼できる者のみが情報を共有し、あるいは情報にアクセスすることが担保されることが不可欠である。このためには、新規加入の際に、複数の参加主体からの推薦を条件とするほか、参加主体に関するセキュリティクリアランスや、情報にアクセスする者から情報が漏えいすることを防止するための措置等を講ずる必要がある。

また、情報が適切に管理されることも必要であり、情報の秘密区分及び取扱い者の区分の設定や情報の保管・運搬の方法等、ソフト・ハード両面からの堅固な情報保全措置のほか、情報及び当該情報を元にした成果の対外的な発表の可否を判断するためのプロセス等を定める必要がある。

(ｳ)　証拠化のためのプロセスの検討

日本版 NCFTA においては、サイバー空間の脅威への最適な対処を行う観点から、警察の捜査への協力を行うことも見込まれる。このため、参加主体からの情報を警察に提供するための手続や、警察が当該情報を証拠化する際に踏むべき手続をあらかじめ明らかにしておくことが重要である。

オ　情報共有のイメージ

集約・分析された情報の共有については、参加主体に応じて様々な形が想定される。例えば、産業界の中で、アンチウイルスベンダーを始めとする情報セキュリティ企業とそれ以外の被害を受ける側の企業とでは、日本版 NCFTA に提供できる情報も日本版 NCFTA に求めるものもおのずから異なるだろう。このような観点から、日本版 NCFTA における情報共有の在り方及び企業等の参加の在り方については、例えば、次のようなものが考えられる。

頻度 / 範囲	随時	１回／２～３週間	１回／１～６か月
A会員 （職員派遣 ・費用負担）	①警報・脅威予測 ②集約情報の分析結果 ③集約情報へのアクセス	④サイバー通報	⑤レポート ⑥セミナー
B会員 （費用負担）	①警報・脅威予測 ②集約情報の分析結果	④サイバー通報	⑤レポート ⑥セミナー
非会員 （一般）	①警報・脅威予測		⑥セミナー

①　警報・脅威予測

脅威の態様に応じて、会員であるか否かを問わず提供する情報。

例えば、サイバー空間において予想される脅威の動向等、公表することが日本版

NCFTA の活動の支障とならず、かつ、今後の被害を防止・軽減するために一般に提供することが有益と考えられる情報を発信すること等が考えられる。

② 集約情報の分析結果

日本版 NCFTA において分析された二次情報。

例えば、会員間相互の情報共有を目的として行われる会議への参加資格を付与し、当該会議に参加することで、日本版 NCFTA において分析された情報を入手することができるようにすること等が考えられる。

③ 集約情報へのアクセス

データベースに蓄積されるなどした一次情報。

例えば、データベースにアクセスする権限を付与することで、自らのニーズに応じた独自の分析を可能にすること等が考えられる。

④ サイバー通報

会員を対象として、定期的に発信される情報。

例えば、詳細な検挙情報等が考えられる。

⑤ レポート

日本版 NCFTA の分析官が特定の脅威の動向や今後の見通し等について分析するもののほか、海外関係機関等のレポートや検挙事例等を入手し、可能な範囲で共有すること等が考えられる。

⑥ セミナー

特定のセクター（例えば、金融機関）を対象として、当該セクターに対するサイバー空間の脅威の中長期的な動向等を周知する目的で、セミナーを実施すること等が考えられる。

(2) 研究開発

日々新たな技術や手口が出現するサイバー空間の脅威を特定、軽減及び無効化するためには、脅威の実情に即した技術等の研究開発が不可欠である。

他方で、現状では、脅威の実例について公表されているものが質・量ともに不十分であり、学術機関に対して研究開発の材料が十分に提供されていない、あるいは、産業界や警察が抱える研究開発へのニーズが学術機関と共有されていないとの指摘もある。

日本版 NCFTA は、サイバー空間の脅威への対処に資する研究開発が行われるよう、産官と学の結節点として、学術機関に対して、産官が研究開発の分野に求めるニーズを提供するとともに、研究開発の成果に対する検証にも貢献することが期待される。なお、サイバー空間における多様な脅威に対処するためには、情報処理に関する技術だけでは不十分な場合も想定されることから、様々な分野の専門家との間で協力関係を構築することが望ましい。

(3) トレーニング

日本版 NCFTA では、集約された情報を利用してトレーニングプログラムの開発及び提供を行うことも想定されている。

このトレーニングの主たる対象は、警察等の法執行機関職員とすることが考えられるが、トレーニングプログラムの開発状況や必要性等に応じて、トレーニングの対象を企業の情報セキュリティ担当者等に拡大することも検討に値する。

なお、プログラムを作成するための材料となる情報の蓄積や講師の選定等の準備を踏まえると、前述の情報集約・分析等と同時期にトレーニングを開始することは困難であり、情報の集約・分析について一定の実績が積み上げられた後に行うことが現実的であろう。

トレーニングプログラムの開発及び提供の効果が実証されれば、将来的には、アジア地域の法執行機関職員のトレーニングセンターとしての機能を果たすことも期待される。

また、日本版 NCFTA は、サイバー空間の脅威への具体の対処を通じて、参加者（産学官における優れた技術や知見を有する者を想定）が実践的スキルを修得・向上させる場として機能することも望まれるほか、学術機関から学生をインターンシップ等により受け入れることで、広く国における情報セキュリティに係る人材育成に貢献することも考えられる。

(4) 海外連携

日本版 NCFTA は、我が国におけるサイバー空間の脅威に総合的に対処するための産学官の連携組織として、米国やカナダの NCFTA 等の海外関係機関はもとより、警察を通じてユーロポール EC3[*6]、ICPO[*7]の IGCI[*8]等の海外法執行機関等と連携することが想定され、米国 NCFTA 最高責任者からも日本版 NCFTA との連携への期待が表明されている。

海外関係機関等と実効ある連携を行うためには、日本版 NCFTA が、海外関係機関等が欲する情報を蓄積し、発信することが重要となる。例えば、日本において発生しているものの、日本国内の産学官を対象とする直接の脅威ではないためにこれまで十分に把握されていなかった脅威に関する情報等を蓄積し、これを基に情報交換を行うことで、海外関係機関等との連携をより深められるものと考えられる。

2 効果的運用に向けた取組

(1) 信頼関係の構築

情報の集約・分析を始めとする日本版 NCFTA における全ての活動の前提となるのが、参加主体間の信頼関係の構築である。例えば、提供した情報がどのように活用されているのかが分からない、あるいは、職員たる出向者の頻繁な異動により人的紐帯を築く暇がないということになれば、信頼関係を構築することは困難になり、全ての活動に支障を来すこととなる。

したがって、長期的な職員出向、新規加入の際の複数の参加主体からの推薦、参加主体に関するセキュリティクリアランスの実施、情報にアクセスする者との NDA[*9]の締結等の実効ある秘密の保持、情報共有が一方的になった場合の是正措置等について、それらの在り方を、情報集約・分析の観点のみならず、枠組みを長期間にわたり維持する観点からも検討する必要がある。

---

*6 European Cybercrime Centre の略。Europol（European Police Office:EU の法執行機関であり、EU 加盟国警察機関の活動を支援している。）に設置された機関で、サイバー犯罪に対処するため、各種知識や情報の蓄積、捜査支援、トレーニングの提供、他の組織等との協力関係の構築等を行っている。

*7 International Criminal Police Organization の略。国際刑事警察機構。各国の警察機関を構成員とする国際機関であり、国際犯罪に関する情報の収集と交換、犯罪対策のための国際会議の開催や国際手配書の発行等を行っている。

*8 INTERPOL Global Complex for Innovation の略。フランスに本部を置く ICPO 事務総局を補完する組織として平成 26 年にシンガポールで業務開始予定。犯罪及び被疑者の特定、トレーニングの提供、他の組織等との協力関係の構築等を目的としており、サイバー犯罪対策を主要な取組分野の一つとしている。

*9 Non-Disclosure Agreement の略。秘密保持契約のこと。

(2)　産学官それぞれに参加するメリットがあること

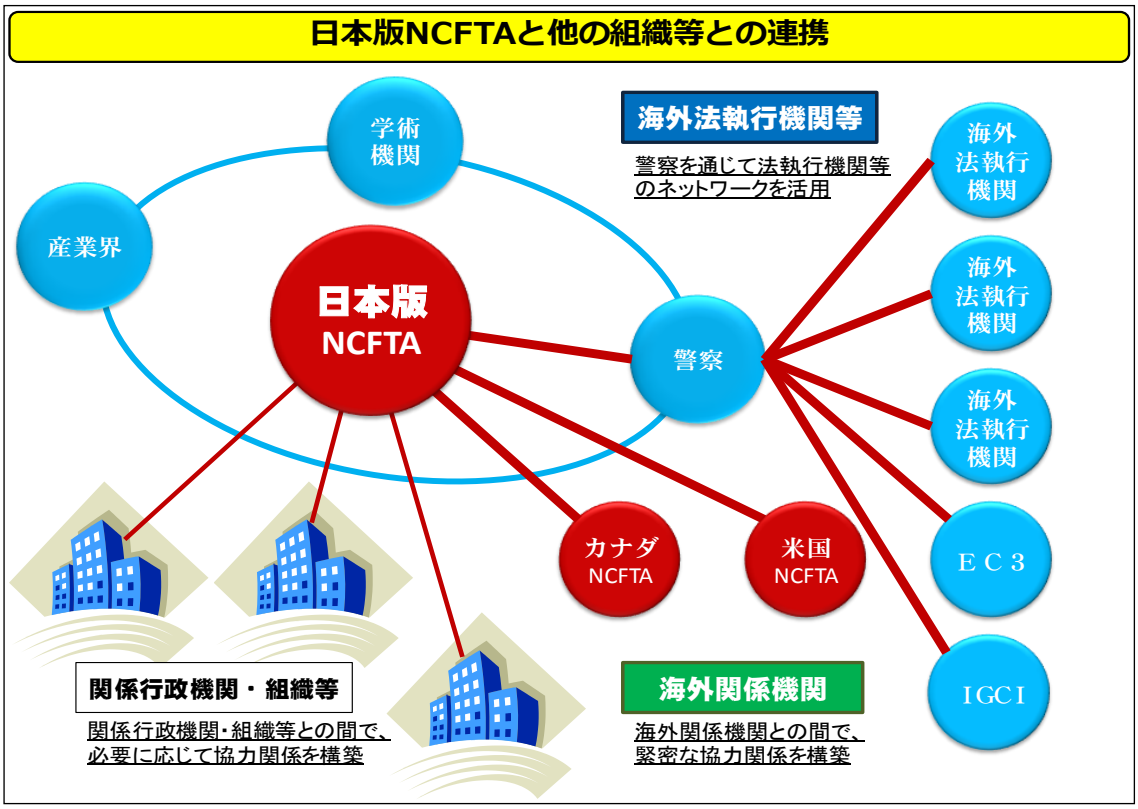
各主体にとって、日本版 NCFTA に加わることにメリットがなければ、枠組みは長続きせず、また、一部の主体にのみ過度な負担を強いるものであっても機能しない。産学官が対等なパートナーとして参画し、着実に成果をあげ、それぞれがメリットを享受できる枠組みとすることが必要である。

米国 NCFTA が成功した理由として、サイバー空間の脅威による被害を最も受けやすい立場にある企業が NCFTA の意義や効果を認め、積極的に活動に参画していることが挙げられる。日本版 NCFTA が成功する上でも、この種の企業が日本版 NCFTA の意義・効果を認め、積極的に参画することが不可欠であることを肝に銘じる必要がある。

(3)　既存の組織等との適切な連携

警察が参画する日本版 NCFTA は、捜査権限の行使に基づく事態の解明や海外の法執行機関等とのネットワークの活用等の点で、既存の他の組織や枠組みにはない特徴を有する。他方で、このことは、日本版 NCFTA がサイバー犯罪対策の全てを担うことを意味するわけではなく、また、それぞれの必要性に基づいて構築・運用されている既存の組織等の意義を減じるものでもない。むしろ、発展と変化を続けるサイバー空間に対峙する上で、多層的・重層的、相互補完的な形で存立する団体が、相互の連携を通じて、それぞれの長所や利点を活かして活動をより一層効果的なものとすることで、全体としてサイバー空間の脅威への対処に万全を期すことが可能となる。関係する行政機関等との適切な連携もまた同様に重要であると言えよう。

図４　日本版 NCFTA と他の組織等との連携



(4) 国民の理解の獲得

日本版 NCFTA は幅広い情報を集約することから、情報の取扱いに留意すると同時に、分析に際しては、その結果のもたらす重要性を認識して正確性に慎重を期す必要がある。また、日本版 NCFTA の活動について、必要に応じて対外的に適切な説明がなされることが望ましい。

第４　設置に向けた更なる検討の推進

日本版 NCFTA を創設し、運用を開始するためには、組織の在り方（組織形態、体制、職員の出向元等）や運用リソースの負担の在り方、活動の実施方法、集約・分析の対象となる情報の範囲、情報保全の仕組み等について速やかに具体化する必要がある。

このためには、日本版 NCFTA の趣旨に賛同し、その活動に貢献する意思と能力を有する主体の参加を募り、警察と共に、創設に向けた実務的・具体的な検討を行うことが重要である。

新たな組織の創設に向けては、短期的な取組と中長期的な取組を分けて考えることが現実的である。短期的には、米国 NCFTA という成功例を参考としつつ、現実に利用可能な資源の活用、既存の組織との連携等を通じて、可能な限り速やかに、まずは「始める」ことが重要である。

そして、一定期間の試行と検証を経て、成功事例を積み重ねることで、徐々に、しかし確実に地に足のついた信頼関係を構築すること、そして、常に改善に努めることが重要である。このためには、例えば、対象テーマや業種を限定した上での部分的な試行も検討に値する。

中長期的には、より効果的に機能するための組織の在り方や情報の取扱い等について、法整備の必要性の有無等も含めて検討することが適当である。

平成 25 年度総合セキュリティ対策会議委員名簿

前田　雅英 （委員長）	首都大学東京　法科大学院教授
石井　延幸	シスコシステムズ(同)　パブリックセクター事業 営業推進グループ　部長
岩井　博樹	デロイト トーマツ リスクサービス(株)　マネジャー
尾形　わかは	東京工業大学大学院　イノベーションマネジメント研究科教授
片山　建	日本マイクロソフト(株)　法務・政策企画統括本部 政策企画本部　次長
桑子　博行	違法情報等対応連絡会　主査
小屋　晋吾	トレンドマイクロ(株)　執行役員　統合政策担当部長
佐々木　良一	東京電機大学　未来科学部教授
関　　聡司	楽天(株)　執行役員　渉外室室長
関口　和一	日本経済新聞社　論説委員兼編集委員
寺田　真敏	(株)日立製作所　ＨＩＲＴチーフコーディネーションデザイナ
外村　慶	(株)シマンテック　執行役員　セールス エンジニアリング担当
中野目　善則	中央大学　法科大学院教授
西嶋　勉	富士通(株)　リスク・コンプライアンス本部 情報セキュリティインシデント対策部長
西本　逸郎	(株)ラック　取締役　最高技術責任者
則房　雅也	日本電気(株)　ナショナルセキュリティ･ソリューション事業部 主席技術主幹
林　　紘一郎	情報セキュリティ大学院大学　教授
藤川　春久	セコムトラストシステムズ(株) 情報セキュリティサービス本部 常務取締役本部長
藤原　靜雄	中央大学　法科大学院教授
別所　直哉	ヤフー(株)　執行役員　社長室長
宮下　正彦	弁護士
本橋　裕次	マカフィー(株)　サイバー戦略室長

計　２２人（敬称略・５０音順）

【オブザーバー】　内閣官房、総務省、法務省、経済産業省

平成 25 年度総合セキュリティ対策会議の開催状況

第１回会議　　平成 25 年７月４日(木)

第２回会議　　平成 25 年８月６日(火)

第３回会議　　平成 25 年９月６日(金)

第４回会議　　平成 25 年９月 27 日(金)

第５回会議　　平成 25 年 10 月 29 日（火）

第６回会議　　平成 25 年 11 月 28 日（木）

第７回会議　　平成 25 年 12 月 24 日（火）