

**官民連携を通じたサイバー犯罪に
対処するための人材育成等**

平成 26 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、効果的なサイバーセキュリティ対策を官民が連携して検討・実施する必要性が高まっている。

「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、平成 26 年の一般財団法人日本サイバー犯罪対策センターの創設等の取組に結び付いている。

本年度は、「官民連携を通じたサイバー犯罪に対処するための人材育成等」をテーマに選定し、官民連携を通じたサイバー犯罪に対処するための人材育成の在り方について、サイバーセキュリティ人材の育成に関する政府の方針や警察におけるサイバー犯罪に対処するための人材育成の取組状況を踏まえつつ、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 27 年 3 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きている。

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 G 8 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
平成 25 年度	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～

目 次

～本編～

第1章 サイバー犯罪捜査を取り巻く現状と課題	1
1. サイバー犯罪捜査を取り巻く情勢	1
2. サイバー犯罪捜査員の育成に向けた課題	1
(1) 現状と問題点	1
(2) 課題	2
3. 中核捜査員の拡充の必要性	3
(1) 中核捜査員の果たすべき役割	3
(2) 中核捜査員の必要人数	4
第2章 官民連携を通じた中核捜査員の拡充に向けた取組	6
1. 中核捜査員の拡充に向けた課題	6
(1) 現状と問題点	6
(2) 課題	6
2. 今後取り組むべき事項	7
(1) 実践的な資格制度の整備	7
(2) 実践的な研修の実施	8
(3) 官民の人事交流	9
おわりに	10
平成 26 年度総合セキュリティ対策会議委員名簿	11
平成 26 年度総合セキュリティ対策会議の開催状況	12

～資料編～

発表資料

- ◆ サイバー犯罪に対処するための人材育成について…………… 1
- ◆ 民間企業における人材育成の取組…………… 7
- ◆ 富士通“セキュリティマイスター”認定制度ご紹介……………11
- ◆ デジタルフォレンジック関連の人材育成－警察と民間－……………18
- ◆ (ISC)²概要と資格制度について……………30
- ◆ 民間企業におけるインターン受け入れ例……………48
- ◆ 日本マイクロソフト：警視庁との交流プログラム……………55

本 編

第1章 サイバー犯罪捜査を取り巻く現状と課題

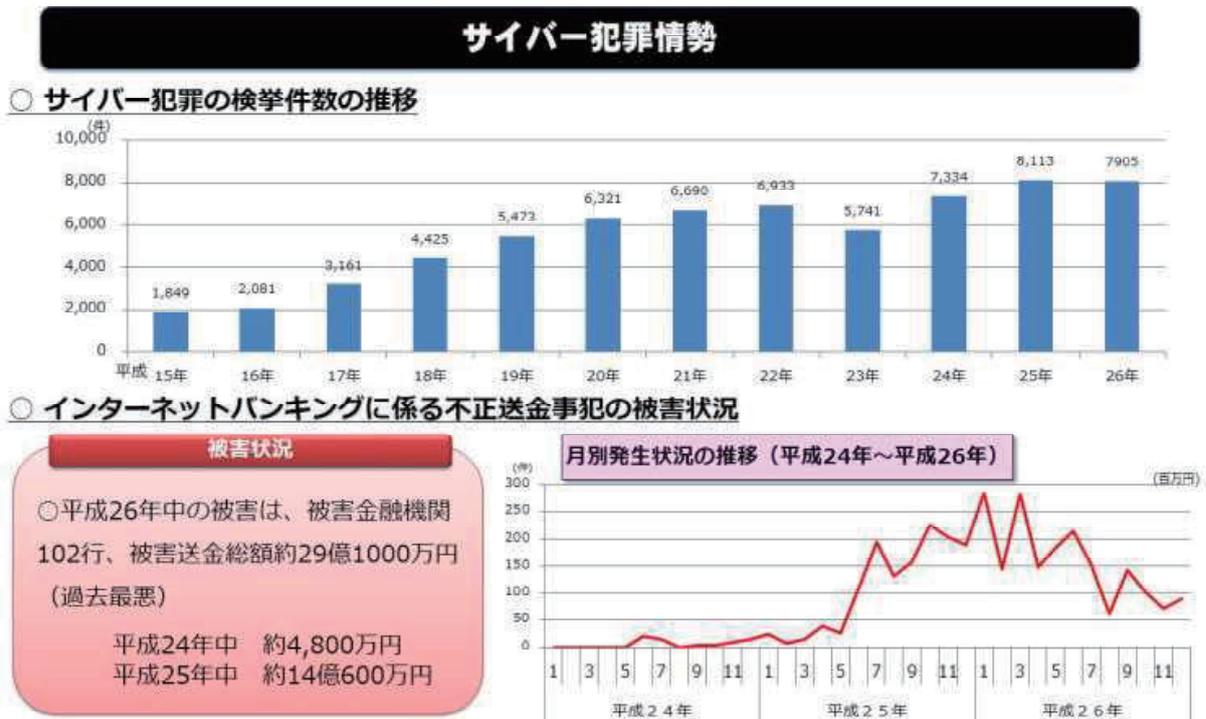
1. サイバー犯罪捜査を取り巻く情勢

近年、サイバー犯罪は、マルウェアの高機能化、匿名化のための技術・手段の利用等により、利用される技術の高度化や手口の巧妙化が急速に進行している状況にある。

特に、インターネットバンキングに係る不正送金事犯については、以前から欧米諸国を中心に多額の被害が発生していたところ、平成25年6月以降、我が国でも被害が急増しているが、このことは、グローバルに敢行されているサイバー犯罪が我が国にも初めて本格的に到来したことを意味しており、今後も、欧米諸国等で多大な被害が発生しているサイバー犯罪の脅威が我が国に波及する可能性は否定できない。

さらに、あらゆるモノがインターネットにつながるIoT(Internet of Things)が今後急速に進展することが予想されているところ、サイバー空間と現実空間との融合が深まる中で現実空間にも多大な影響を及ぼすサイバー犯罪が発生することが懸念される。特に我が国では東京オリンピック・パラリンピック開催に向けて一層その動きが加速化される可能性があることに留意する必要がある。このほか、IT環境のクラウド化の進展による捜査の困難化も懸念される。

このようにサイバー犯罪捜査を取り巻く情勢が今後一層厳しさを増していくことが予想される中で、サイバー犯罪に対処するための人材育成は焦眉の問題と言える。



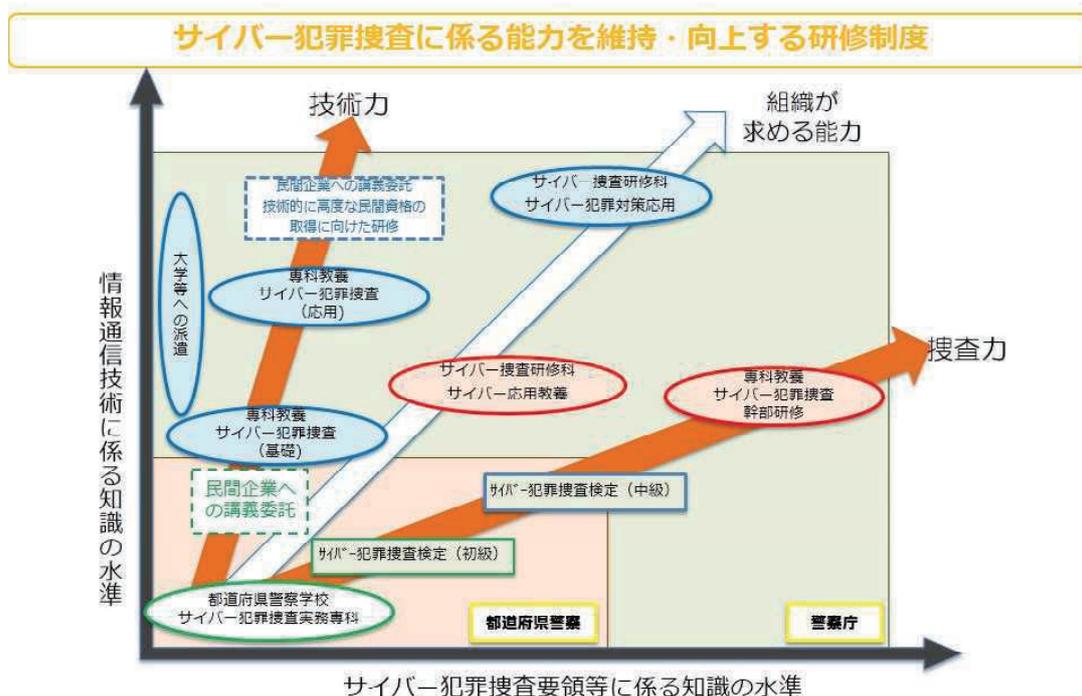
2. サイバー犯罪捜査員の育成に向けた課題

(1) 現状と問題点

警察においては、これまでもサイバー犯罪情勢に対応するために必要な体制の強化が図られているところであるが、急速に進むサイバー犯罪の高度化・巧妙化、解

析対象となるHD（ハードディスク）等の大容量化等に的確に対応していくため、サイバー犯罪捜査を実質的にリードすることができる高い専門性を有した捜査員を確保する必要性が高まりつつある。

現在、警察においては、このような高い専門性を有した捜査員を確保するために、直面するサイバー犯罪の捜査に必要な研修が実施されるなど、一定の取組が行われているところであるが、高度化・巧妙化するサイバー犯罪に的確に対処するための人材育成・登用に向けて、今後更に体系的な取組が行われることが望ましい。



(2) 課題

警察においては、これまでも産・学の関係者の有する先進的な知見と高度な技術を最大限に活かすための取組が進められてきたところであるが、今後一層厳しさを増していくことが予想されるサイバー犯罪捜査を取り巻く情勢に的確に対処していくためには、産・学の専門家と一層実効性のある連携を確保しつつ、サイバー犯罪捜査をリードしていくことができる専門的な知見と高度な技術を兼ね備えた捜査員を拡充していく必要がある。

そして、サイバー犯罪捜査をリードしていく捜査員が産・学との連携の結節点としても機能し、その役割を円滑に果たすためには、こうした捜査員が相応の能力を有していることを産・学からも分かるよう、その保有する能力を資格等により明確にすることが望ましいと考えられる。

以上のような状況を踏まえ、今後、警察庁において、このような高い専門性を有した捜査員の拡充に向けて、人材育成方針を含め、取り組んでいくべき各種の方策が策定され、都道府県警察に対して示されることが望ましい。

3. 中核捜査員の拡充の必要性

(1) 中核捜査員の果たすべき役割

現在、各都道府県警察のサイバー犯罪捜査担当部門においては、一般的に捜査主任官を中心に5名ないし7名程度で構成されるサイバー犯罪捜査班が一つの活動単位とされているところ、サイバー犯罪捜査を的確に推進していくためには、この活動単位の中に、捜査主任官の捜査指揮を主に技術面からサポートすることができる高い専門性を有した捜査員が含まれていることが望ましい。このような捜査員は、捜査主任官をCEOになぞらえた場合においてCTOに相当する者であり、正にサイバー犯罪捜査において中核捜査員と位置付けられる者である。このような中核捜査員は、①PC、スマートフォン等のコンピュータやネットワークに関する知識によりITやセキュリティに造詣が深いことはもとより、②犯罪ツール等のサイバー犯罪に用いられた技術・手法に関する知識や③コンピュータ、マルウェア等の解析に関する知識を有することを前提として、捜査の現場において、これらの技術面の知識を総合的に活用して、犯罪被害の実態を見極め、犯人の特定・犯行の裏付けに必要な捜査すべき事項、解析すべき事項の抽出、分析を行う役割を果たすことが期待されることとなる。

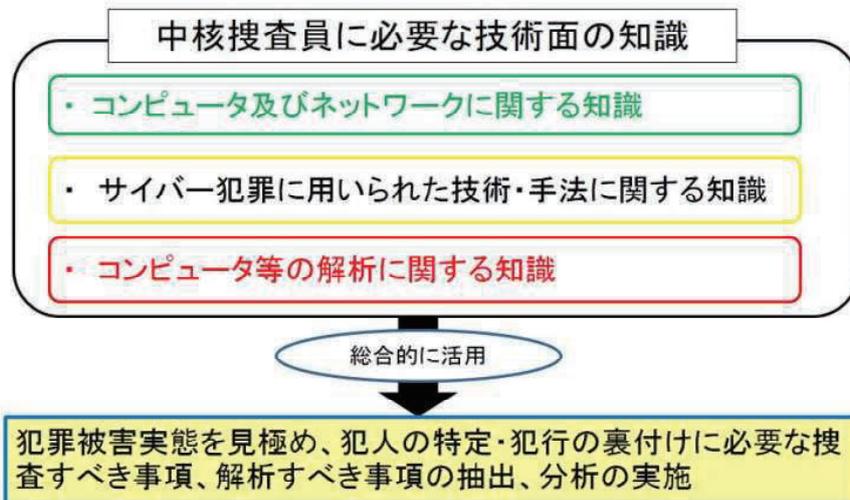
例えば、インターネットバンキングに係る不正送金事犯を認知した場合に中核捜査員に期待される役割は、捜査対象となる被害端末・サーバ等からマルウェア等の痕跡を抽出し分析を行ったり、侵入手口の特定向けてログの分析等捜査すべき事項を抽出したりしていくこととなる。

特に、昨今のサイバー犯罪捜査では解析対象となるHDの大容量化等が進みつつあることから、中核捜査員による解析すべき対象・事項の見立て、絞り込み、優先順位付け等により、捜査項目を早期に抽出し、速やかに捜査を進めていくことが、今後一層必要となるものと考えられる。

この点、委員からは、民間企業においても、サイバー空間で発生したインシデントの原因究明のための調査を行うに当たっては、システム全体を理解し包括的な対策を実施できるような人材が必要不可欠であることから、これと同様に、警察においてもサイバー犯罪の全体像を把握することができる人材を育成することは有意義であるとの指摘や、中核捜査員にはサイバー空間内の脅威の拡大防止に資するスキルも兼ね備える必要があるとの指摘のほか、IoTの進展に伴い、サイバー犯罪で用いられるツールの多様化が一層進むことから、中核捜査員が行うデジタル証拠の保全、収集、分析のために求められるスキルも定期的に見直しを行うことが重要ではないかとの指摘もあった。

中核捜査員層の拡充に当たっては、このような指摘も踏まえて取り組まれることが望ましい。

中核捜査員によるサポートとは



(2) 中核捜査員の必要人数

都道府県警察において、現在、中核捜査員に相当する捜査員は、民間企業等から転職した中途採用の警察官である特別捜査官を中心に100名程度存在するところであるが、サイバー犯罪捜査班が一般的に5名ないし7名程度で構成されていることから、仮に捜査員6名当たり1名の中核捜査員が必要とされるとして試算した場合、200名程度の要員が必要となってくる。したがって、今後、所要の体制を確保するためには、少なくとも100名程度の中核捜査員が新たに育成される必要がある。

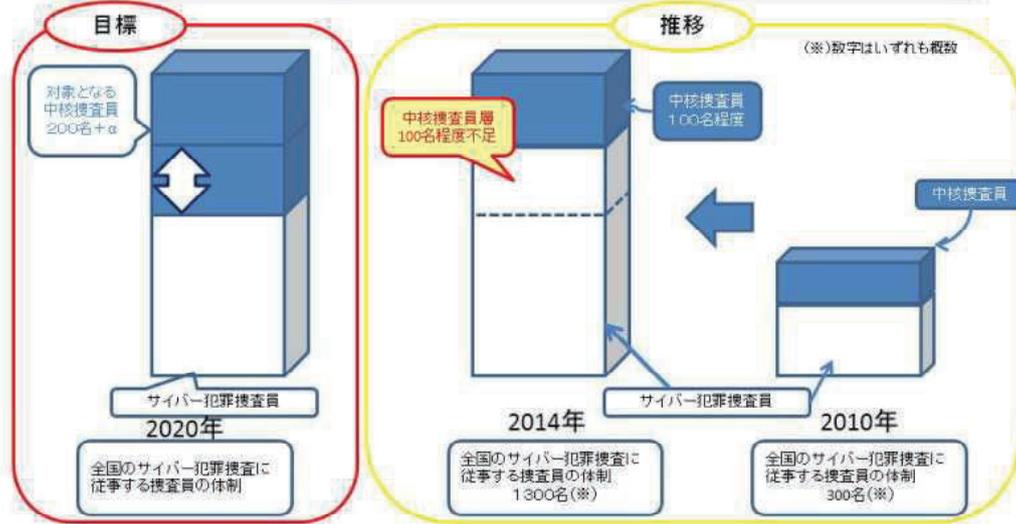
もっとも、今後、東京オリンピック・パラリンピック開催に向けて、様々なインフラやサービスが拡張されていく中で、IoTも急速に進展していくことが予想され、サイバー犯罪捜査を取り巻く情勢も一段と厳しさを増していくものと考えられることから、こうした状況の変化も考慮しつつ人材育成が進められていく必要があることは言うまでもない。

また、委員からは、民間企業においても、インシデントへの対応については、複数のアナリスト等が相互の知見を活用しつつ行う必要がある場合が多いことから、サイバー犯罪捜査についても、サイバー犯罪捜査班各班に1名程度配置される中核捜査員だけではなく、専門的知識を有する警察内外の者と情報共有して連携しつつ行われることが必要であるとの指摘があった。

したがって、特に高度な技術を用いて行われるサイバー犯罪に的確に対処するためには、先進的な知見を有する産・学の関係者との実効性のある連携が確保されるとともに、より多くの捜査員が中核捜査員として活躍できるよう人材育成に向けた各種の取組が積極的に進められていくことが望ましい。

サイバー犯罪捜査体制の推移と目標

被害の深刻化に伴い、サイバー犯罪捜査員の増員が急速に進められてきたが、次々と出現する高度な技術を用いた新たな手口に対応するための中核捜査員層が不足



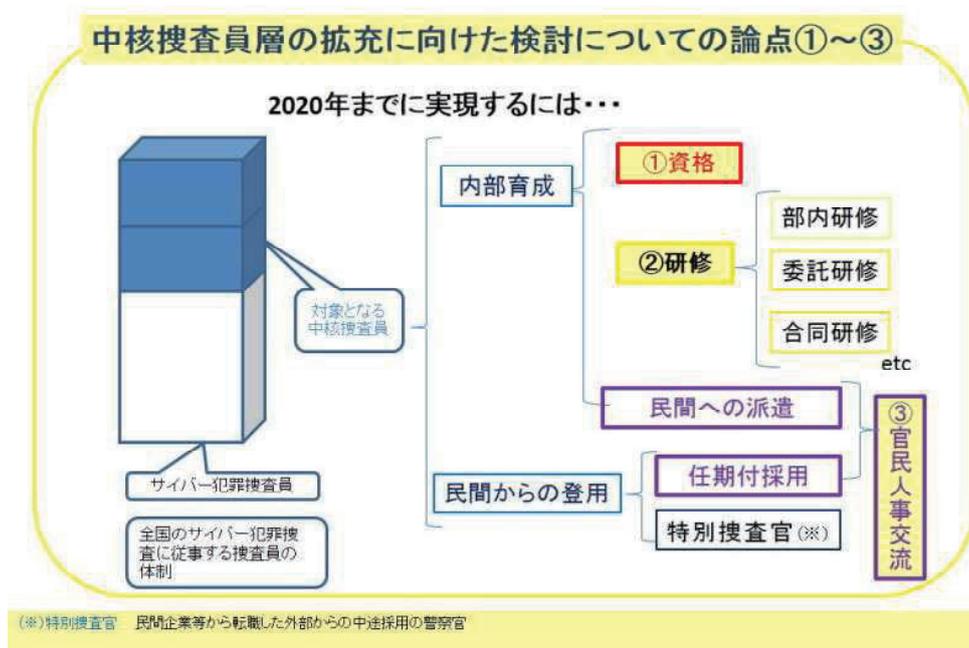
第2章 官民連携を通じた中核捜査員の拡充に向けた取組

1. 中核捜査員の拡充に向けた課題

(1) 現状と問題点

警察における中核捜査員層を拡充するための取組としては、大きく分けて、内部育成と民間からの外部登用の二つの方策が考えられる。中核捜査員の内部育成については、①能力の評価のための資格制度の整備、②能力の向上・維持のための研修の実施及び③官民の人事交流の一環としての民間への捜査員の派遣を通じて行われることが考えられる。

一方、民間からの登用については、産・学から専門的知見を有する者を特別捜査官として中途採用することのほか、産・学から現在の職場への復帰を前提として一定の雇用期間・条件等を定めて任期付採用職員として受け入れることが考えられる。



現在、警察においては、サイバー犯罪捜査のための部内検定制度が運用されており、民間委託を含めて能力に応じた研修も実施されているところであるが、中核捜査員の能力を評価するための検定制度は運用されておらず、中核捜査員の能力の向上・維持に必要な研修も必ずしも十分に実施されていない。さらに、中核捜査員に必要な能力・スキルについて、産・学と意見交換するスキームも整備されていない。

また、民間への捜査員の派遣について実績を有する都道府県警察は少数にとどまっており、民間からの外部登用については、特別捜査官としての中途採用に関しては多くの都道府県警察において実績を有するものの、任期付採用に関しては現在のところ実績がない。

(2) 課題

中核捜査員層の拡充に向けて、産・学における先進的な人材育成等の仕組みを参

考にした上で検討が進められることが有効であると考えられるが、その際、産・学との連携により中核捜査員層拡充のための効果的かつ持続的なスキームを構築するためには、①能力の評価方法・資格制度、②能力の向上・維持のための研修制度、③官民の人事交流制度のいずれの仕組みの検討に当たっても、警察のみならず、産・学それぞれにおいてもメリットを享受できる方策が模索されることが望ましい。

民間の先進的な取組を踏まえると、中核捜査員層の拡充のためには、中核捜査員に必要なスキルを特定したスキルマップを作成するとともに、必要なスキルを習得するまでの研修カリキュラム体系を構築していくことが望ましい。その上で、研修の適宜の段階に対応する形で、現在保有しているスキルが目標とするスキルと比較してどのレベルにあるのかを明確化するため、能力の評価方法・資格制度を設定し、中核捜査員層レベルまで能力の向上・維持を図るために研修を行っていくことが望ましい。

なお、中核捜査員は、IT・セキュリティに関するスキルや法制度面の知識はもとより、産・学との連携を一層進めていくためにも、これらの技術の実際のビジネスへの活用実態を始めとしたITビジネスに関する知識についても備えておくことが望ましい。

2. 今後取り組むべき事項

以上のような課題を踏まえ、今後警察において取り組むべき事項について、以下のとおり取りまとめた。

(1) 実践的な資格制度の整備

中核捜査員層の拡充に当たっては、まず、捜査員の能力を評価するための資格制度を整備し、各捜査員のサイバー犯罪捜査に必要なスキルレベルを明確化し、各捜査員が能力の向上や維持に努めていく目標となる指標を用意する必要がある。

中核捜査員の保有する能力をこのような指標に基づき評価するための資格制度をより実践的なものとするためには、中核捜査員が捜査において捜査主任官を技術面からサポートする役割を果たす存在であることに鑑み、当該資格は、専門的な知見や高度な技術を有する産・学の関係者とも共通の理解を有しつつ実効性のある連携を行うことができるレベルの能力を有していることを示すものであることが必要である。

したがって、中核捜査員に係る資格制度を整備するに当たっては、産・学などの民間の資格を活用することが望ましい。

さらに、国境を越えて敢行されるサイバー犯罪の捜査に当たっては、外国捜査機関等との国際的な連携が必要であることから、中核捜査員に係る資格制度を整備するに当たっては、グローバルに通用する資格制度を参考とすることが望ましい。

また、ブラックハッカーと異なり、中核捜査員には、高いスキルと共に、犯罪捜査を遂行する上で必要な正義感や倫理観も兼ね備えていることなどが求められることから、こうした資質を資格の保有により一定水準確保できることが望ましい。

この点、(ISC)² (アイエスシースクエア)が認定するCISSP等の資格は、認定継続要件として倫理規約の遵守を求めており、また、ベンダーニュートラルな資格の中でもグローバルな資格として認知度が高く、米国国防総省においても活用されているなど実績もあることから、今後、制度を整備していく上で参考とすべきものと考え

えられる。

こうした資格制度の整備は、警察と産・学との間の効果的な情報共有・分析に資するとともに、円滑な官民人事交流にも資するものと考えられる。

また、こうした資格制度の整備により犯罪対策にも有効な高レベルのサイバーセキュリティ水準が示されることから、これがセキュリティ対策に取り組んでいる企業等の関係者に対する一つの指標としても機能することとなれば、中核捜査員に必要とされるスキルの社会への浸透により、最終的には我が国社会全体のサイバーセキュリティ水準の向上にもつながることが期待される。

具体的には、サイバー犯罪に的確に対処するために必要とされるスキルが中核捜査員に係る資格制度において明示されることが、犯罪対策にも有効な高レベルのスキルを保有する人材の育成、高水準のセキュリティサービスを提供する主体の出現等の呼び水となり、我が国社会全体のサイバーセキュリティ水準の向上にも寄与し得るものと期待できる。

特に、高度な技術を悪用したサイバー犯罪の捜査に当たっては、中核捜査員が産・学との連携において中心的な役割を担っていくことから、捜査に必要なIT・セキュリティに関するスキルを特定・更新して、資格に係るスキルマップを改訂していく作業枠組みについては、産・学・官の連携による検討をベースとした形にすることが望ましい。この点、サイバー空間内の脅威の無効化を目指す産・学・官の連携の枠組みである一般財団法人サイバー犯罪対策センター等の情報共有の枠組みを活用することも考えられる。

また、委員からは、民間企業においても、資格制度の運用に当たり資格取得者にメリットを付与する仕組みが必要であるとの指摘のほか、インシデントの原因究明のためには攻撃者の意図を読み取ることを含め一定の経験値が必要であるとの指摘があったことから、中核捜査員に係る資格制度を運用するに当たっても、資格者に何らかの形でメリットを付与することを検討するほか、実際の捜査経験等の実績も事案の全体像を把握するために必要な分析力の一要素として考慮される形にすることが望ましい。

(2) 実践的な研修の実施

民間企業においても、インシデントへの対応に係る経験値を原因究明に向けた分析力の一要素として重視していることから、中核捜査員層の拡充のためには、経験不足を補う形の実践型の研修を職員に提供していくことが重要である。

警察においては、これまでも内部研修のほか、民間の知見を活用した委託研修が実施されているところであるが、今後、より深刻化するおそれのあるサイバー犯罪に全国警察がいずれも的確に対処することができるよう、捜査を通じて把握された現在進行形の脅威や被害の発生状況等に関する情報や捜査を通じて得られた反省・教訓点をこれまで以上にタイムリーに取り込みつつ、研修の実施項目をカスタマイズしていくとともに、研修の実施に当たり疑似ネットワーク環境の利用等により実際に近い形で訓練していくことが望ましい。

また、捜査を通じて把握されたものを含め、最新のサイバー空間内の脅威情報を素材とする事例研究を官民合同で実施すれば、官民双方の対処能力が向上することはもとより、異なる視点からの分析・意見交換を通じて、警察側にはITビジネスに

関する知識を身に付ける機会となる一方、民間企業側には犯罪者の視点から自身の展開しているビジネスを見直し、防犯面のノウハウを習得する機会となるほか、大学等の側には脅威に対処する上での法制・技術面の課題等を認識する機会となるなど、官民双方がメリットを享受することが期待でき、我が国社会全体のサイバーセキュリティ水準の向上にもつながることが期待される。

なお、事例研究を通じた官民合同研修については、一般財団法人日本サイバー犯罪対策センターにおいても今後行うことが予定されているところである。

(3) 官民の人事交流

民間企業に捜査員を一定期間派遣することは、最新のIT・セキュリティ技術を習得する上で有益であるのみならず、民間企業との協力関係の構築にも資することとなりサイバー犯罪対策を推進する上でも有益であると考えられる。実際、これまでの捜査員の派遣事例を見ても、帰任後も派遣先で培ったスキルや人的つながりを活かして活躍する捜査員が多数認められ、有益な取組であると評価できる。

現在、警察において、サイバー犯罪捜査員の中でも一定水準以上の専門的な知識を有している者が選抜され民間企業に派遣されているところであるが、受入先の企業においても、実地業務に従事するに当たり一定の資格の取得を要件としているところも認められる。このような事例を踏まえると、今後、捜査員の能力を評価するための資格制度を産・学にも通用する形で設定し、派遣する捜査員の保有する能力を客観的に証明できるようにしていくことが望ましいと考えられる。

一方、今後、民間からの登用に当たっては、特別捜査官としての中途採用にとどまらず、より高度かつ最新のスキルを警察に取り込むとともに、民間にも捜査を通じて得られるサイバー犯罪対策に関するスキルをフィードバックするために、任期付採用職員としての受け入れも検討されることが望ましい。民間から中核捜査員として求められる一定のスキルを保有している資格者を受け入れることができれば、実際の捜査経験が無いという点はあるものの、サイバー犯罪捜査の中で一定の役割を果たすことが期待でき、受け入れ終了後も相互の円滑な交流が期待できる。

特に、官民双方に通用する資格制度の整備を前提として、相互の派遣者に必要なスキルについてあらかじめ取決めしておくことにより、職務内容も明らかになることから、円滑な人事交流を拡大していくことが可能になるものと考えられる。

もっとも、中核捜査員に係る資格制度の整備については一定の期間を要すると考えられることから、官民人事交流については、試行的に進めていくことが望ましいと考えられ、実際の交流を通じて、求められる能力要件等を明らかにしていくことが効率的であると考えられる。官民人事交流を通じて、中核捜査員に必要なスキルが浮き彫りになり、制度の整備に寄与することも期待される。

おわりに

今回の総合セキュリティ対策会議においては、中核捜査員の拡充に向けた人材育成方策として警察において優先的に取り組むべき事項について検討を行った。

会議では、サイバー犯罪捜査に従事する中核捜査員の育成・登用を議題の中心にしたところであるが、我が国全体としてサイバー空間内の脅威の無効化に向けてセキュリティ対策を効果的に進めていくためには、その他の捜査員はもちろんのこと、産・学の立場からサイバー空間内の脅威に対処している関係者と共に対処能力を向上させていくことが必要不可欠であるとの視点に立ち、現状と課題を分析し、サイバー犯罪に対処するための人材育成等につき、産・学・官の連携により相乗効果の期待できる対応方策を取りまとめた。

今後、警察においては、本報告書において提言を行った中核捜査員の拡充に向けた取組について、可能なものから早急に着手・実行されることが望ましい。

この点、平成26年5月に情報セキュリティ政策会議（当時）において決定された「新・情報セキュリティ人材育成プログラム」の中で「我が国の情報セキュリティの水準を向上させるため、とりわけ、政府機関等は自ら率先して人材育成に積極的に取り組んでいくことが重要である。」と言及されているところであるが、我が国において質量共に不足していると言われているサイバーセキュリティに関する人材を創出していくためにも、まずは、現にサイバー犯罪と対峙し、そのために多くの人材を必要としている警察において、産・学との人事交流を活発に行っていくなど、産・学との連携を強化しつつ、積極的に人材育成・登用に取り組んでいくことが求められる。

また、サイバー空間内の脅威に対処するためのセキュリティ人材の育成方策については、本来、大学等の教育研究機関の役割も含め、5年ないし10年程度の長期的な視点に立って検討されるべきものであるが、本報告書における提言を踏まえた取組が今後のサイバーセキュリティに関する人材育成のモデルケースになることが期待される。

以上のような取組により、新しいIT関連技術・サービスが出現・普及しても、国民が安全に安心して利用することができるようになり、ひいては、これらの技術・サービスの活用による我が国経済・社会の発展につながるものと考えられる。

平成26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
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
衣川 俊章	(ISC) ² JAPAN 代表
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
坂 明	(一財)日本サイバー犯罪対策センター 理事
佐々木 良一	東京電機大学 未来科学部教授
下道 高志	日本オラクル(株) 製品戦略統括本部 戦略ビジネス推進部 テクノロジーディレクター
関口 和一	日本経済新聞社 論説委員兼編集委員
田井 祥雅	マカフィー(株) セールスエンジニアリング本部 執行役員 本部長
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ー・ チーフテクノロジーデザイナー
徳田 敏文	日本IBM(株) グローバル・テクノロジー・サービス事業 ITSデリバリー セキュリティ&ネットワークサービス セキュリティ・サービス担当部長
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 本部長
中野目 善則	中央大学 法学部教授
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 静雄	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
山下 眞一郎	富士通(株) クラウド事業本部 サイバーディフェンス室 セキュリティテクノロジーセンター シニアマネージャー

計 24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26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27年1月22日（木）

第2回会議 平成27年2月10日（火）

第3回会議 平成27年3月19日（木）