原議保存期間	3年（平成31年3月31日まで）
有効期間	一種（平成31年3月31日まで）

庁内各局部課長
各附属機関の長
各地方機関の長　殿
各都道府県警察の長

警察庁丙総発第64号、丙人発第232号
丙生企発第110号、丙刑企発第64号
丙交企発第120号、丙備企発第93号
丙情企発第62号

平成27年9月25日
警察庁長官官房長
警察庁生活安全局長
警察庁刑事局長
警察庁交通局長
警察庁警備局長
警察庁情報通信局長

サイバーセキュリティ重点施策の策定について（通達）

情報通信技術の急速な発展に伴い、サイバー空間と実空間の融合が高度に深化した「連接融合情報社会」が到来しつつある。

一方、違法情報・有害情報の拡散に加え、日本年金機構に対するサイバー攻撃事案を始めとする我が国の政府機関、民間事業者等を狙ったサイバー攻撃やインターネットバンキングに係る不正送金事犯等のサイバー犯罪等が多発し、それらの中には、最新の高度な技術を悪用する事案や我が国の安全保障に影響を及ぼし得る事案も見られるなど、サイバー空間の脅威は深刻化している。

また、平成28年は、伊勢志摩サミット及び関係閣僚会合の我が国での開催が予定されており、サイバー空間の脅威への対処に万全を期す必要がある。

このような状況の中、平成27年９月４日に、政府においては、サイバーセキュリティ基本法(平成26年法律第104号)に基づき、サイバーセキュリティ戦略を閣議決定し、警察においても、同戦略を踏まえつつ、「警察におけるサイバーセキュリティ戦略の制定について」(平成27年９月４日付け警察庁乙官発第13号ほか。以下「警察戦略」という。）を発出し、サイバー空間の脅威に対する取組を一層推進することとしたところである。

この度、警察戦略に基づき、警察が注力して取り組むべき施策を定めるため、昨年９月に策定した「サイバーセキュリティ重点施策2014－2015」（平成26年９月10日付けサイバー空間の脅威に対する総合対策委員会決定。以下「旧重点施策」という。）を見直し、「サイバーセキュリティ重点施策」を別添のとおり策定したので、各位にあっては、その効果的な推進に努められたい。

なお、旧重点施策は廃止する。

別添

サイバーセキュリティ重点施策

第１　サイバー空間の脅威に対する対処能力の強化

サイバー空間の脅威に的確に対処するため、サイバー空間における情報収集・分析機能及び対処態勢を強化するとともに、官民一体となって取締り環境を整備するなどサイバー空間の脅威に対する対処能力を強化する。

１　情報収集・分析機能の強化

(1)　情報収集・分析の推進

ア　新たな犯罪手口、脅威情報等の情報収集・分析の推進

新たな犯罪手口や脅威となり得る技術等を把握するため、あらゆる手段を活用して、サイバー空間の動向に関する情報等を収集・分析するとともに、その結果を全国警察で共有する。

イ　違法情報・有害情報の実態把握の推進

サイバーパトロールモニターその他外部人材の活用を推進するほか、児童ポルノや危険ドラッグの販売等の社会問題化している事犯に重点指向したサイバーパトロールを推進する。

ウ　サイバー攻撃やテロに関する情報の収集・分析の推進

都道府県警察サイバー攻撃特別捜査隊等においてサイバー攻撃に関する情報の収集を推進し、警察庁サイバー攻撃分析センターにおいてサイバー攻撃に関する捜査情報や技術情報等の集約・分析を推進するとともに、サイバーフォースセンターにおいて、リアルタイム検知ネットワークシステムによるインターネット観測を24時間体制で行い、サイバー攻撃の予兆・実態把握、不正プログラムの分析等を推進する。

また、インターネット上でテロとの関連性の高い情報を収集する技術等の活用を含め、サイバー空間における国際テロ組織の活動等に関する情報の収集・分析を強化する。

エ　カウンターインテリジェンス機能の強化

外国情報機関によるサイバーインテリジェンス等の対日有害活動の未然防止・解決を図るため、サイバーインテリジェンスに関する情報の集約・分析機能の強化を推進する。

(2)　関係機関等との情報交換

ア　関係省庁等との連携の推進

伊勢志摩サミットや2020年東京オリンピック・パラリンピック競技大会の開催等を見据え、サイバーセキュリティ戦略(平成27年９月４日閣議決定)を踏まえつつ、内閣サイバーセキュリティセンター（NISC）を始めとする関係省庁や公益財団法人東京オリンピック・パラリンピック競技大会組織委員会等との情報交換等を推進する。

イ　国際機関等との連携の推進

インターポールシンガポール総局(IGCI)等の国際機関との情報交換を推進する。

また、Ｇ７ローマ／リヨン・グループに置かれたハイテク犯罪サブグループや情報セキュリティ事案に対処する組織の国際的な枠組みであるFIRST(Forum of Incident Response and Security Teams)の会合等の国際会議に参加し、多国間における情報交換や協力関係の確立等に取り組む。

さらに、アジア大洋州地域サイバー犯罪捜査技術会議を開催し、解析技術やサイバー犯罪捜査に係る知識・経験等を共有する。

ウ　外国治安情報機関等との連携の推進

諸外国におけるサイバー犯罪・サイバー攻撃の手口や技術の動向、サイバー空間の脅威への対処に係る法制度や諸対策、職員の人材育成方策等について、平素から外国治安情報機関等との情報交換を推進する。

エ　民間事業者・団体との連携の推進

サイバー空間の脅威に対処するためには、警察による取締りのみならず、民間事業者等の知見を活用した取組が必要であることから、一般財団法人日本サイバー犯罪対策センター（JC3）と連携し、産業界・学術機関・法執行機関等それぞれが持つサイバー空間の脅威への対処経験を全体で蓄積・共有するなど、民間事業者・団体との連携を推進する。

オ　学術機関・研究者等との連携の推進

電子機器の解析やサイバー攻撃への対処に資する最先端技術に係る情報を取得するため､最先端の研究を行っている海外の研究機関への職員の派遣を推進する。

また、いわゆるハッカーは、ハッカーフォーラム等の場において様々な情報交換を行っていることから、ハッカーコミュニティーに参加するなどして、ハッカーとの協力関係を構築し、必要な情報を収集する。

２　サイバー攻撃に対する緊急対処態勢の強化

(1)　各警察機関・部門間の連携体制の強化

ア　事態対処能力の強化

国民生活や社会経済活動に影響を及ぼすおそれがある大規模サイバー攻撃事態（国民の生命、身体、財産若しくは国土に重大な被害が生じ、又は生じるおそれのあるサイバー攻撃事態をいう。）に対し、全国警察が一体となって迅速な初動措置、検査その他の措置を的確に行うため、各警察機関の緊密な連携による事態対処能力を強化する。

イ　技術支援の推進

警察庁のサイバーフォースセンターにおいて、サイバー攻撃に係る技術情報等の収集・分析を推進するとともに、被害の未然防止・拡大防止のため、全国のサイバーフォースにおいて、都道府県警察に対する技術支援を推進する。

(2)　関係機関等との連携体制の強化

サイバーテロ対策協議会等を通じ、平素から事案発生時の警察への速報及び証拠保全に関する働き掛けを行うなど連絡態勢の確立に取り組むとともに、基幹システムのシステム構成等に関する情報交換、民間有識者による講演、情報セキュリティの向上のための助言又は指導等を行う。

また、サービスの多様化・高度化に伴い、2020年東京オリンピック・パラリンピック競技大会等の大規模イベントにおいてサイバー攻撃の標的となることが懸念される事業者等との共同対処訓練を推進する。

3　サイバー空間をめぐる取締り環境の整備等

(1)　民間事業者等とのパートナーシップの構築の推進

警察と民間事業者がそれぞれの活動目的や立場を相互に理解し、それぞれの責務を適切に果たすため、「サイバー犯罪に対する警察と民間事業者の共同対処の推進について」（平成24年７月12日付け警察庁丙情対発第22号ほか）に基づき、警察と民間事業者との共同対処協定を締結するなど民間事業者等とのパートナーシップの構築を推進する。

(2)　事後追跡可能性の確保

ア　通信履歴の保存による事後追跡可能性の確保

総務省と連携し、「電気通信事業における個人情報保護に関するガイドライン」の解説の改正を踏まえ、関係事業者における通信履歴の保存に関する適切な取組を推進するなど必要な対応を行う。

イ　公衆無線LANの事後追跡可能性の確保

政府における公衆無線LANのサイバーセキュリティの確保のための施策と連携を図りつつ、サイバー空間における事後追跡可能性の確保の観点から、関係機関等と連携して必要な対策を検討する。

ウ　データ通信カード契約時における本人確認徹底の要請等

データ通信カード契約時における公的書類による本人確認の徹底について民間事業者の取組を注視しつつ、関係省庁等と連携しながら、関係事業者に対し適切な指導を推進するとともに、インターネットカフェにおける利用者の本人確認、コンピュータの使用状況の記録の保存等の防犯指導を推進する。

(3)　国際連携の推進

ア　国際捜査共助の枠組みの活用

外国のIPアドレスの契約情報や通信履歴等が捜査上必要となる事案について、ICPOルート、外交ルート、刑事共助条約(協定)及びサイバー犯罪に関する条約に基づくルートのほか、Ｇ７・24時間コンタクトポイント等を活用して積極的な捜査共助を要請し、迅速かつ的確な国際捜査を推進する。

イ　職員派遣の推進

サイバー犯罪・サイバー攻撃の主体・手口等に関する情報の交換等について、国際機関、外国治安情報機関等との連携を強化するため、リエゾンオフィサーの派遣を推進する。

ウ　諸外国に対するキャパシティビルディングの推進

国境を越えて行われるサイバー犯罪・サイバー攻撃に対する諸外国の対処能力の向上を図るため、JICA課題別研修（サイバー犯罪対処能力向上）等を通じ、我が国のサイバー空間の脅威にへの対処等に関する情報提供やサイバー犯罪・サイバー攻撃に係る捜査技能に関する支援等を推進する。

特に、広範な分野で我が国と密接な関係を有する東南アジア諸国連合（ASEAN）加盟国について、日・ASEANサイバー犯罪対策対話等の枠組みを通じ、積極的な情報共有、人材育成等を推進する。

第２　サイバー空間の脅威の低減

民間事業者等における適切な対策を促すための広報啓発活動に加え、犯罪抑止に資する徹底した捜査活動や新たな手法等の検討を推進することで、サイバー空間の脅威を低減する。

１　サイバー空間の脅威に立ち向かう社会全体の意識の向上

(1)　官民一体となった実態把握、啓発活動の推進

ア　総合セキュリティ対策会議の開催

サイバー空間の脅威に対処するため、総合セキュリティ対策会議を開催し、有識者、関連事業者等と、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検討する。

イ　社会全体におけるセキュリティ意識の向上

インターネットバンキングに係る不正送金事犯やスマートフォン等における新たなサービスを悪用した事案等について注意喚起を行うとともに、情報セキュリティに関する講習等において、基本的な知識の普及啓発活動を実施するなど、様々な機会を活用して社会全体におけるセキュリティ意識の向上に向けた取組を推進する。

ウ　事業者等におけるサイバー攻撃に対する意識の向上

サイバーテロ対策協議会や各種のセミナー等において、先端技術を有する事業者等に対してサイバー攻撃情勢に関する講演を行うことにより、サイバー攻撃に関する危機意識を醸成し、サイバー攻撃対策の促進を図る。

エ　教育機関等との連携の強化

大学院、大学、高等専門学校等の高等教育機関と連携し、警察におけるサイバー空間の脅威に関する講演を行うなど、高度な専門人材の育成に向けた取組の支援を推進する。

オ　インターネット観測結果の広報

インターネット観測により分析したDoS攻撃の発生やサイバー攻撃に関連する行為等の動向等に関する情報を「@police」で広く一般に公開し、一般のインターネット利用者等に対して、サイバー空間の脅威に対する適切な対策を促す。

カ　海外の偽サイト等に対する対策の推進

都道府県警察で相談又は被害届を受理した海外の偽サイト等に関する情報を集

約し、違法性の認定、連絡の困難性の確認等をした上で、ウイルス対策ソフト提供事業者等に提供し、これらのサイトを閲覧しようとするインターネット利用者のコンピュータ画面に警告表示を行うなどの対策を推進する。

(2)　民間の自主的な被害防止活動の推進

自治体や大学、民間事業者等と連携して、サイバー空間における自主的な防犯活動を行うボランティアを育成・支援するなど、社会全体でサイバー犯罪に立ち向かう気運の醸成に向けた取組を推進する。

2　高度な情報技術を用いたサイバー犯罪に対する戦略的な捜査の推進

(1)　組織的なつながり等の実態解明の推進

インターネットバンキングに係る不正送金事犯に対処するため、サイバー犯罪特別対処班を活用し、効率的かつ効果的な捜査を実施するとともに、事案に応じて、関係部門が連携し、組織的なつながり等の事態解明を推進する。

(2)　関係機関・団体と連携した被害防止対策の推進

インターネットバンキングに係る不正送金事犯による被害が深刻化していることから、金融機関との連携を強化し、インターネットバンキングのセキュリティ機能強化のための注意喚起、不正送金に悪用される口座を凍結するための口座情報・凍結口座名義人情報やフィッシングサイト情報の提供等を行うとともに、不正プログラムに感染した端末の利用者等が判明した場合には、プロバイダ等を通じて注意喚起を行う。

(3)　合同・共同捜査の推進

都道府県警察の管轄区域を越えて行われるサイバー犯罪に対して、効率的で効果的な捜査を実施するため、サイバー犯罪捜査情報等共有システム等を活用して犯罪の実態を把握するとともに、合同・共同捜査及び捜査共助を積極的に推進する。

また、複数の都道府県警察における一斉取締りを実施するなど、犯罪抑止に資する捜査活動を推進する。

(4)　新たな捜査手法等の導入の推進

平素より最新の情報通信技術やインターネット上の新たなサービスの動向を踏まえ、新たな捜査手法の導入を図るとともに、これを全国警察で共有する。

3　サイバー犯罪への犯罪組織の関与の実態解明及び取締りの推進

(1)　犯罪組織の関与の実態解明の推進

暴力団等の犯罪組織がサイバー犯罪に関与して得た収益を資金源としている実態がみられることから、関係部門が緊密に連携して、犯罪組織の実態解明に資する情報の収集・分析を徹底する。

(2)　サイバー犯罪に関与する犯罪組織の取締りの推進

サイバー空間を悪用する犯罪組織の更なる実態解明を図るため、犯罪組織により敢行されるインターネット上における出会い系サイトを利用した児童買春周旋事犯、インターネットを利用した薬物密売事犯、ＳＮＳを利用した偽造在留カードの取引事犯等の取締りを推進する。

4　違法情報・有害情報対策の推進

(1)　違法情報・有害情報の積極的な取締りの推進

インターネット・ホットラインセンターから通報される違法情報・有害情報について、「全国協働捜査方式」を効果的に活用した捜査活動を推進するとともに、より悪質性の高い情報に重点を指向した違法情報・有害情報の取締りを推進する。

(2)　悪質なサイト管理者等に対する積極的な措置の推進

合理的な理由なく違法情報の投稿を放置・助長しているサイト管理者や海外サイトにおける国内関係者の刑事責任の追及も視野に入れた取締りを推進する。

5　インターネットを利用した児童を対象とする性犯罪等の対策の推進

(1)　サイト事業者に対する働き掛けの推進

サイト事業者の規模や提供しているサービスの態様に応じた児童被害防止対策として、サイト事業者に対する実効性あるゾーニングの導入やミニメールの内容確認を始めとするサイト内監視体制の強化に向けた働き掛けを推進する。

(2)　保護者や児童等に対する広報啓発活動の推進

児童による出会い系サイトの利用の防止やコミュニティサイトに起因する児童被害防止はもとより、児童の健全な成長を著しく阻害するインターネット上の違法情報・有害情報の閲覧を防止するため、児童、保護者、教育関係者等に対し、フィルタリングの必要性等に関する広報啓発活動を推進する。

(3)　インターネット異性紹介事業者の実態把握と取締りの推進

インターネット異性紹介事業の利用に起因する児童買春を防止するため、事業者の実態把握を徹底し、法令違反行為に対して的確な指導及び行政処分を行うとともに、悪質な法令違反行為については厳正な取締りを推進する。

(4)　サイバー補導の推進

被害児童の早期発見・保護を図るため、サイバーパトロールによって、援助交際を求めるなどインターネット上の児童による不適切な書き込みを発見し、書き込みを行った児童と接触して直接注意・指導する「サイバー補導」を推進する。

6　サイバー攻撃に対する緊急対処、捜査及び実態解明の推進

(1)　総合的かつ一体的な態勢の確保の推進

警察庁、管区警察局及び都道府県警察におけるサイバー攻撃事案への対処態勢の確保を推進し、同事案発生時には、関係部門が連携して、迅速な初動措置、捜査その他の措置を的確に実施する。

(2)　被害の未然防止・拡大防止に向けた取組の推進

サイバーインテリジェンス情報共有ネットワーク、不正プログラム対策協議会、サイバーインテリジェンス対策のための不正通信防止協議会等の枠組みを通じて、セキュリティ関連事業者及び先端技術を有する事業者等との間でサイバー攻撃に関する情報を共有するとともに、NISCを通じて政府機関等とも必要な情報共有を推進し、サイバー攻撃による被害の未然防止・拡大防止を図る。

7　情報技術の解析を活用した捜査の推進

(1)　積極的な情報技術の解析の推進

情報通信技術の高度化に対応するため、必要な解析用資機材を整備するとともに、高度情報技術解析センターにおいて、高度な技術を要する解析を推進するなど、情報技術の解析に必要な態勢を強化し、犯罪捜査部門に対する積極的な技術支援を推進する。

(2)　情報技術の解析の適切な活用に向けた取組の推進

犯罪に悪用された電子機器等に保存されている電磁的記録の解析を犯罪捜査に的確に活用するため、必要な技術的な知識や手続に関する知識について、情報技術解析部門による巡回教養等を実施するなど、情報技術の解析の適切な活用に向けた取組を推進する。

第３　サイバー空間の脅威への対処に係る組織基盤の強化

複雑・巧妙化するサイバー空間の脅威に対する対処機関としての警察の質的・量的な能力向上は、いずれの部門にとっても喫緊の課題であり、部門間の連携強化、体制の確保、警察職員の能力向上等により、サイバー空間の脅威への対処に係る組織基盤を強化する。

１　部門間の連携強化

(1)　都道府県警察等における部門間の連携強化の推進

管区警察局、都道府県警察等において、警察組織の総合力を発揮した効果的な対策を推進するため、サイバー空間における情報の収集・分析並びにサイバー空間の脅威への対処に係る人的基盤及び物的基盤の強化その他の取組の連携・調整を図るための態勢を整備し、部門間の連携強化を推進する。

また、サイバー空間の脅威への対処に係る全国会議を開催し、各都道府県警察等における好事例を全国警察で共有するほか、顕著な実績に対する的確な賞揚を実施し、捜査能力の更なる研鑽を促す。

(2)　人的資源及び物的資源の部門横断的な活用の推進

サイバー犯罪・サイバー攻撃への対処に従事する警察職員の能力、配置状況、資機材の機能及び配備状況等について把握し、人的資源及び物的資源の部門横断的な活用を推進する。

２　サイバー空間の脅威への対処に係る人的基盤の強化

(1)　人材確保のための取組の推進

採用試験に情報セキュリティに係る資格保有者を加点するなど、サイバー空間の脅威への対処に関する素養のある人材の採用方策について検討する。

また、任期付き任用や中途採用、特別職の公務員としての採用等により、民間事業者等から専門的知識・能力を有する者を積極的に登用する。

さらに、あらゆる機会を通じ、情報セキュリティに係る資格を保有するなどサイバー犯罪・サイバー攻撃捜査に適性を有する人材を的確に把握し、適切な人材配置を推進する。

(2)　全警察職員の対処能力の底上げに係る取組の推進

全ての警察職員のサイバー空間の脅威に関する意識を向上させるとともに、サイバー空間があらゆる犯罪に悪用され得ることから全捜査部門における的確なサイバー空間の捜査を可能とするほか、日々高度化するサイバー犯罪・サイバー攻撃への対処を可能とするため、人材育成方針を策定するとともに、同方針を踏まえつつ、民間企業への業務委託、サイバー犯罪捜査検定制度の活用等による効率的な教養を推進する。

(3)　専門的捜査員の育成の推進

専門的捜査員がトップレベルの知識等を修得・維持するため、最先端のサイバー空間の脅威への対処に関する情報や技術を有する民間事業者が実施する研修等の積極的な活用を推進するとともに、既に一定の知識を有している捜査員を民間事業者等に派遣するほか、大学・専門学校等が開設している情報セキュリティに係る講座の受講等を奨励する。

また、全国警察が参加する捜査技能に関する競技会を開催するなど、都道府県警察における専門的捜査員の育成を促す。

(4)　幹部教養の推進

サイバー空間の脅威への対処が警察のいずれの部門にとっても重要な課題となっていることから、脅威に対し部門横断的かつ効果的な対処がなされるよう、幹部を対象とした専科教養の実施を検討するなど、幹部に対する教養を推進する。

(5)　サイバーセキュリティ研究・研修センターにおける教養の推進

サイバーセキュリティ研究・研修センターにおいて、専門的捜査員に対する専門的知識及び技術に関する研修を実施するとともに、全部門の捜査員を対象に実際の事案を想定した実践的な訓練等を行うなど、サイバー空間における警察全体の対処能力の向上を図る。

(6)　解析能力の向上に係る教養の推進

民間事業者の知見を活かした研修や全国の解析担当職員が参加可能なネットワーク接続型訓練環境を活用した実践的な訓練、高度情報技術解析センターにおける高度な技術的訓練等の実施により、情報技術の解析に従事する職員の解析能力の向上を図る。

(7)　情報収集・分析能力の向上のための体制整備に向けた検討の推進

サイバー空間をめぐる情勢に関する情報を収集・分析し、的確な対策を企画・立案するため、人材育成方策等について必要な検討を行う。

3　サイバー空間の脅威への対処に係る物的基盤の強化

(1)　捜査基盤の整備の推進

技術の進歩やサイバー空間をめぐる情勢に対応するため、サイバー犯罪・サイバー攻撃への対策に必要な資機材の整備・拡充を推進する。

(2)　解析用資機材の整備の推進

サイバー犯罪・サイバー攻撃への対策及び犯罪の取締りを技術的に支援するため、最新の情報通信技術に対応可能となる必要な資機材等の整備・拡充を推進する。

4　サイバー空間の脅威への対処に係る研究開発の推進

(1)　インターネット観測技術の高度化に関する研究推進

サイバー攻撃の解明、攻撃者の追跡、組織の把握等に資する観測技術について、民間事業者等の知見を活用しつつ、新たな観測・分析手法を検討する。

(2)　大規模産業型制御システムに対するサイバー攻撃への対処能力の強化に関する調査研究等の実施

大規模産業型制御システムについて、システムの構成、セキュリティの考え方、サイバー攻撃の可能性、攻撃発生時の影響等についての調査研究を実施するとともに、実際の対処に当たる警察職員が大規模産業型制御システムに対するサイバー攻撃対策を実施できるようにするための訓練を実施することにより、大規模産業型制御システムに対するサイバー攻撃への対処能力の強化を図る。

(3)　匿名化通信技術等に関する研究の推進

Tor等の匿名化通信の発信元の特定及び悪用による被害防止のためのアクセス防御手法に関する調査研究を実施する。

また、不正プログラム解析に有効な手段となる揮発性メモリからデータを抽出する手法に関する調査研究を実施する。

5　警察における堅牢な情報セキュリティの実現

(1)　全警察職員の意識の向上に係る取組の推進

警察情報セキュリティポリシーに基づき、警察が保有する情報の組織的な管理を徹底するとともに、情報セキュリティに関する情報等を適時に周知するなど、全警察職員の情報管理に関する意識の向上に向けた取組を推進する。

(2)　情報流出防止対策の推進

インターネットを利用する職員を対象とした標的型メール攻撃対処訓練を実施するなど、効果的な情報流出防止対策を推進する。

(3)　警察の情報システムにおける情報セキュリティの向上

ソフトウェアのぜい弱性情報等を基に警察の情報システムに係る情報セキュリティ上のリスクに適切に対処するとともに、インターネットと接続された情報システムにおいて扱うことのできる情報の範囲を徹底するなど、警察の情報システムにおける情報セキュリティの向上を図る。

(4)　CSIRTの態勢強化の推進

警察における情報セキュリティ上のリスクに対し、組織的な対処が図られるよう、警察庁及び都道府県警察に設置されたCSIRTについて効果的な運用方策を検討するなど、CSIRTによる情報セキュリティインシデントに対する対処について、態勢の強化を推進する。