○　香川県警察におけるサイバーセキュリティ重点施策について

（令和４年６月１日付け香企画第 115 号）

令和３年９月、政府において新たな「サイバーセキュリティ戦略」が閣議決定され、警察庁においても、同戦略を踏まえ、「警察におけるサイバー戦略について」（令和４年４月１日付け警察庁乙サ発第１号ほか。）が発出されたことから、本県警察においては、「香川県警察におけるサイバーセキュリティ戦略について」（令和４年６月１日付け香企画第 114 号。以下、「県警察戦略」という。）を発出し、サイバー空間の脅威への対処に関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、この県警察戦略に基づき、県警察が重点的に取り組むべき施策について、「香川県警察におけるサイバーセキュリティ重点施策の策定について」（平成 30 年 11 月７日付け香企画第 323 号。）を見直し、新たに、「香川県警察における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。

別添

香川県警察におけるサイバーセキュリティ重点施策

1　体制及び人的・物的基盤の強化

⑴　サイバー空間の脅威に対処するための体制の構築

サイバー部門の人材、資機材等リソースの拡充を進めるとともに、部門一体となった広報啓発活動・被害防止対策の企画・実施等が実効的に行われるよう、サイバーセキュリティ総括責任者を中心とする関連部門の連携体制を一層強化する。

また、各部門においても事案対応等に際し、必要な時は遅滞なくサイバー部門の支援を要請することとし、そのため、「香川県警察サイバーセキュリティ戦略推進委員会」の下に事案対応に関する専門部会、対策班等を設置するなど、これら連携が円滑に行われる体制を構築する。

⑵　優秀な人材の確保及び育成

ア　優秀な人材の確保

サイバー関連分野の知見を有する人材を確保するため、高等専門学校や大学等への採用活動の強化、情報処理に係る資格保有者に対する採用試験の加点等、優秀な人材の確保のための取組を推進する。

また、民間事業者等での勤務経験を有するなど専門的知識・能力を持つ者の中途採用、任期付き採用等による積極的な登用を推進する。

イ　民間の知見の活用等教養内容の充実

高度で専門的な知識やノウハウを有している県内外の民間団体、事業者、学術機関等による研修や、事業者等への一定期間の職員の派遣等を推進する。

また、県警察学校における部内教養等の充実を図る。

ウ　教養環境の整備

警察庁が整備するサイバー警察人材活用プラットフォームを活用し、高度で実践的な教養の受講機会を確保する。

エ　専門捜査員の育成

サイバー犯罪対策担当部門及びサイバー攻撃対策担当部門の職員に相互に併任をかけるなどにより、これらの職員をサイバー捜査に従事させ経験をより多く積ませるほか、先進的な専門捜査力を有する都道府県警察との合同・共同捜査への積極的な参画及び人事交流の推進等により、捜査員の能力の向上を図る。

また、サイバー事案捜査の適性及び能力を有する人材については、検定の取得状況や教養の受講歴等の人材育成の実施状況に関する情報を部門横断的に集約・管理し、体系的かつ段階的な育成を図るとともに、サイバー事案捜査に関する高度な知識・技術を必要とする業務に継続的に従事させるなど、その特性を踏まえた適材適所の人材配置に努める。

オ　高度専門人材の育成

情報技術解析部門において、各技官の能力に応じた適切な教養計画を策定するとともに、高度な専門知識・技能を有する職員による職場教養を推進し、高度専門人材の育成を図る。

カ　ハイブリッド人材の育成

高度専門人材と専門捜査員等を対象としたサイバーセキュリティコンテストについて、両者混合のチームにより参加するほか、相互の教養への参加、人事交流の拡大等により、人的交流・知見共有等を促進し、捜査・解析の両者に精通した優秀な人材層の充実を推進する。

キ　捜査能力等を有する技官の育成

情報技術解析部門から、人事交流で県警察に出向してきた職員に、サイバー部門での勤務経験を積ませること等により捜査能力等を有する技官を育成する。

ク　キャリアパス等の構築

優秀な人材の更なる活躍や、政策的観点の習得等の人材育成を図るため、サイバー警察局・サイバー特別捜査隊への出向等の人事交流を推進する。

また、極めて高度な専門技術・捜査技能等を有する人材に対し、本人の希望に基づき長期にわたり同一ポスト又は関連するポストを務め、高度な知見を蓄積・活用できるキャリアパスの確立等、士気高く勤務できる環境の整備と、その能力に応じた処遇改善を推進する。

ケ　顕著な実績に対する適切な賞揚等

内外の競技大会における成績や情報処理に係る資格の取得等に対し表彰や昇任試験における加点を行うなど、適切な賞揚を推進するとともに、特に顕著な実績を挙げた職員に対しては、昇給等の処遇面も含め適切な措置を講ずる。

⑶　職員全体の対処能力の向上

サイバーセキュリティ等に係る修養の重要性を周知徹底するとともに、採用時や昇任時等節目ごとに設けた教養機会を有効に活用するための教養内容の見直し、教養機会の拡大、初任科生等を対象とした教養資料の整備等を推進する。

また、職員の自己研鑽を促進するため、教養資料の配布、警察部内でのサイバーセキュリティ競技会等を拡充する。

⑷　資機材の充実強化

ア　サイバー事案対処に関する資機材及び解析用資機材の充実・強化

サイバー事案への対処を行うための資機材及び解析用資機材の増強・機能強化を推進し、組織全体の対処能力向上を図る。

イ　解析用資機材の適切な活用

サイバー部門において、適正な手続を確保しつつ迅速かつ的確な情報技術の解析を実施し、情報の抽出を効果的に行うため、資機材の基本的な利用方針を定めるとともに、解析手続の適正化を図る。

⑸　警察における情報セキュリティの確保等

ア　連携体制の確立

ぜい弱性情報等情報セキュリティインシデントに発展し得る情報の早期把握が、組織内のセキュリティ確保と広報啓発等を通じた社会全体の防御力向上といった対内・対外両面において有用であることから、サイバーセキュリティ総括責任者を中心とした情報セキュリティ体制とサイバー部門の間で円滑な情報共有が行われる体制を構築する。

また、組織内の情報セキュリティインシデントに適切に対処するため、サイバーセキュリティ総括責任者を中心とした情報セキュリティ体制とサイバー部門が連携した実効的なＣＳＩＲＴ体制を構築する。

イ　全警察職員の情報リテラシー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、最新の情報通信技術に関する特性とそのリスクを始めとした情報セキュリティに係る教養等により、全警察職員の情報リテラシーの向上に向けた取組を推進する。

ウ　情報流出防止対策の推進

インターネット端末等における不正プログラムの挙動検知等の多層防御を講じるとともに、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。

エ　情勢に応じた情報セキュリティ対策の推進

情報セキュリティ監査、情報システムのぜい弱性試験等の結果や機器・ソフトウェアのぜい弱性情報等を基に、情報セキュリティ上のリスクに適切に対処するなど、情報セキュリティをめぐる情勢に応じた情報セキュリティ対策を推進する。

また、すべての通信を信用しないことを前提に対策を講じること、いわゆる「ゼロトラスト」等情報セキュリティ対策に係る動向の調査・研究に取り組むなど、中長期的な観点からの対策も推進する。

オ　ＣＳＩＲＴの対処能力強化の推進

ＣＳＩＲＴにおいて、情勢の変化を捉えた実践的な訓練・教養を実施するなど、対処能力の強化を推進する。

２　実態把握と社会変化への適応力の強化

⑴　通報・相談への対応強化による実態把握の推進

ア　警察への通報・相談の促進

政府の「サイバーセキュリティ戦略」（令和３年９月 28 日閣議決定）において、「サイバー犯罪に関する警察への通報や公的機関への連絡の促進によって、サイバー犯罪の温床となっている要素・環境の改善を図る」とされているなど、警察のみならず政府・社会全体として取り組むべき課題とされている点も踏まえ、被害通報を促進するための広報啓発に取り組むとともに、民間事業者とも連携して、通報・相談促進に向けた気運の醸成に取り組む。

イ　相談対応の充実等

通報・相談に適切に対処するため、１(3)のとおり、警察職員全体の対処能力

の向上を図るとともに、対処に専門的知見を要する相談等を受理した場合には、サイバー部門に遅滞なく伝達する手順を確立するなど、部門間連携により適切な対応体制を構築する。

また、より適切かつ円滑な対応を可能とするための相談対応の充実や官民連携の強化を推進する。

さらに、被害企業等における業務の早期復旧等に配慮した初動捜査を推進する。

⑵　実態解明と実効的な対策の推進

ア　効果的な分析の推進

実態解明から被害防止対策までの広範な活用を念頭に置き、警察内のサイバー関連情報に加え、関係機関・団体や事業者から提供される情報等多様な情報の分析を推進する。

また、サプライチェーンの複雑化等により、サイバー事案に係る影響範囲等の想定が困難となる状況においても適切な事案対処等を可能とするため、平時から関係機関・団体や事業者等と連携した分析評価を推進する。

イ　捜査関連情報等に対する分析の充実・高度化及び厳正な取締りの推進

サイバー事案の捜査や通報・相談等を通じて事案を把握した場合は、被疑者の検挙だけでなく、犯行手口等の実態解明や被害の未然防止・拡大防止を図る観点も不可欠であることから、一つの事案のみに着目するのではなく、サイバー事案に係る情勢を的確に捉え、攻撃者につながる可能性のある情報その他の広範な関連情報を総合的に収集・分析・評価し、サイバー事案において特定の攻撃グループ、国家機関等が関与していることを明らかにするなど、より広い範囲での実態解明を進めるとともに、サイバー事案の厳正な取締りを推し進め、警察庁を通じて関係省庁と連携し、解明された情報の適切な公表による更なる被害の抑止、いわゆる「パブリック・アトリビューション」に取り組む。

また、被害の未然防止・拡大防止、犯罪インフラ対策等も視野に入れ、より広範な視点から捜査関連情報等に対する分析に取り組む。特に、ランサムウェアについては、多業種にわたって甚大な影響を及ぼしていることから、関係行政機関、団体等が連携してサイバー事案の分析を行い、被害の再発や未然防止・拡大防止に向けた取組を推進する。

ウ　実態解明のための分析・解析の高度化・効率化

特定のグループや国家機関等が関与するサイバー攻撃等、被疑者の検挙が一般的に困難である事案に対しても、実態解明と対策の推進は有効であることから、マルウェアの多様化・耐解析機能の実装等に対処していくため、機械学習の活用等を進めて解析態勢を強化し、解析の高度化・効率化を図る。

エ　インターネット上の脅威情報等の収集及び分析の高度化

児童ポルノや規制薬物広告、自殺誘引情報等の違法・有害情報に厳正に対処するため、インターネット・ホットラインセンターからの通報及びサイバーパトロール等を通じて把握した情報を端緒として、事件化や削除依頼等を積極的

に推進する。

3　部門間連携の推進

⑴　事案認知における部門間連携

警察署等において、関係部門が連携した適切な相談受理がなされるよう関係部門の連携を推進する。

また、通報・相談された内容が、警察署・警察本部間及び警察本部・警察庁間において、早期に整理・共有・分析される情報伝達がなされるよう、組織間の連携を推進する。

⑵　捜査における部門間連携

ア　サイバー事案対処における連携の推進

ランサムウェアによる攻撃を始めとする高度な情報技術を悪用したサイバー事案について、サイバー部門を中心に、端緒の的確な把握及び積極的な捜査を推進するとともに、最新の技術・サービス動向に関する情報や知見を収集し、より多角的な捜査手法を検討・活用の上、効果的な手法については関係部門で共有する。

また、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。

イ　適切な部門間の分担及び連携の推進

サイバー事案のうち、捜査に当たり高度な専門的知識及び技術を要さないものについては、各事件主管課において主体的に捜査を行うほか、サイバー部門において、各事件主管課を適切に支援し、部門間の分担及び連携を推進する。

ウ　合同・共同捜査等の推進

各都道府県警察の管轄区域を越えて行われるサイバー事案に対して、サイバー捜査情報共有システム等を活用して管轄を越えた情報共有に努めるとともに、合同・共同捜査及び捜査共助をより積極的に推進するなど、効率的かつ効果的な捜査を実施する。

また、犯罪抑止に資する捜査活動を推進するほか、警視庁協働捜査班を活用し、効率的かつ効果的な捜査を実施する。

エ　サイバー特別捜査隊との連携

重大サイバー事案の対処に当たっては、サイバー特別捜査隊と連携して、効率的かつ効果的な捜査を実施する。

また、これらの取組が円滑に行われるよう、平素からサイバー警察局・サイバー特別捜査隊と関係部門との間で必要な連絡調整を推進する。

⑶　被害防止対策における部門間連携

サイバー部門においては、対策、情報収集・分析、捜査、解析等の様々な機能が相互に連携・協働しながら、任務を遂行することが不可欠であり、特に、被害防止対策においては、サイバー部門内における各機能の緊密な連携が重要である。例えば、捜査部門において入手した情報を、情報収集・分析部門が精緻な分析を行い、得られた知見を対策部門を通じて関係事業者に周知するなどの取組が

円滑に行われるよう、各機能を担当する部門間の緊密な連携を推進する。

4　国際連携の推進

⑴　信頼関係の構築

警察庁においては、国際会議の主催・参加等を通じて、外国捜査機関等との情報交換や担当者間の関係構築を図っていることから、県警察においても、外国捜査機関等との信頼関係構築の観点を踏まえ、外国捜査機関等からの共助要請に適切に対応する。

⑵　国際捜査における初動捜査の徹底

被害企業等からの通報・相談に適切に対応し、初動捜査を徹底するとともに、サイバー警察局、サイバー特別捜査隊等と緊密に連携して、迅速かつ的確な国際捜査を推進する。

5　官民連携の推進

⑴　産学官の知見等を活用した対策の推進

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、日本サイバー犯罪対策センター（ＪＣ３）をはじめ、産業界・学術機関・行政機関等で構成される香川県サイバーセキュリティ連絡ネットワーク、香川県サイバー攻撃対策協議会等と連携し、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・共有するなどの取組を推進する。

⑵　民間事業者等における自主的な被害防止対策の促進

関係行政機関、民間事業者・団体等と連携し、産業機械、医療機器、今後普及が想定される自動運転車等のＩｏＴ機器に関する脅威情報、インターネットバンキングに係る不正送金事犯、インターネット上の新たなサービスを悪用した事案等の情報を広く県民に共有する。

⑶　民間事業者等と連携した犯罪インフラ対策の推進

ア　他部門と連携した効果的な取組の推進

サイバー部門が被害防止対策において連携する民間事業者等は、他部門からも働き掛けを行っていることが多いことから、部門間で必要な調整を行うなど緊密に連携し、民間事業者等との良好な関係を構築するとともに、関係部門が一体となって効果的な取組を推進する。

イ　サービス提供事業者等への情報提供や働き掛け等の推進

サービス提供事業者、インフラ提供事業者（利用者にサービス提供がなされる際に利用されるインフラ等を提供する事業者）等において、犯罪インフラとして悪用されることを防ぐため、サービスの見直しや事後追跡可能性の確保等必要な対策が

とられるよう、悪用の危険性や被害実態等の情報提供及び働き掛けを推進する。

ウ　通信履歴の保存等に関する取組の推進

「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」の解説等を踏

まえ、プロバイダ等の関係事業者に対して通信履歴の保存や保存期間の延長に資する取組の推進について働き掛けを行う。

エ　本人確認徹底の要請等

データ通信専用ＳＩＭカード等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。

オ　ＳＭＳ認証の不正代行対策の推進

ＳＭＳ認証の不正代行について、関連する民間事業者との被害実態の情報共有を進めるとともに、法令違反に対する取締りを推進する。

カ　インターネットバンキングに係る不正送金事犯等対策の推進

インターネットバンキング及びキャッシュレス決済サービスをめぐるサイバー犯罪の対策について、金融機関・資金移動業者等への犯行手口に基づく注意喚起の実施、暗号資産取引口座を含む不正な送金先口座の凍結検討依頼等を推進する。

キ　インターネット上の誹謗中傷への対応

インターネット上の誹謗中傷に係る相談に際し、その内容に応じて、関係する部署が連携して対応し、指導・助言、法務局人権擁護担当、違法・有害情報相談センター等の専門機関の教示等、相談者の不安等を解消するために必要な措置を講じるほか、刑罰法令に触れる行為が認められる場合には、捜査機関として適切に事件に対処する。

ク　クレジットカードの不正利用事案への対応

ｅコマース（電子商取引、ＥＣ）に関連するクレジットカードの不正利用事案に関し、組織犯罪性が疑われるこの種事案への取締りを強化するとともに、関係団体等と連携して、被害実態を踏まえた有効な対策を推進する。

ケ　フィッシング対策の推進

警察が業務を通じて把握したフィッシングサイト等の情報について、警察庁を通じてウイルス対策ソフト事業者等に提供するほか、サイバー防犯ボランティアが行うフィッシングサイトの無害化措置、いわゆる「テイクダウン」の活動支援に取り組む。

コ　判明した犯罪インフラのテイクダウン

サイバー事案で使用された不正プログラムの解析等を通じて把握したＣ２サーバ等判明した犯罪インフラについて、管理者等への情報提供・対応依頼を通じて確実にテイクダウンが行われるよう取り組む。

⑷　地域において活動する多様な主体との連携

ア　地域に根ざした各主体の防犯活動との連携

中小企業等においてサイバー空間の脅威に対して十分な対応ができていないとの指摘等も踏まえ、サイバー保険を取り扱う損害保険会社等と連携するなど中小企業等に対する広報啓発活動を推進する。また、知事部局や関係団体等と

連携した協議会やネットワーク等が構築されているところ、中小企業対策についても、香川県サイバーセキュリティ連絡ネットワークをはじめ、様々な協議会等に働き掛けるなどの取組を推進する。

イ　事業者との共同対処協定の拡大・充実

サイバー事案の潜在化防止や再発防止等を目的とした共同対処協定について、中小企業を含む広範な業界の企業、商工会など地域の産業組織等とも締結が進むよう取り組むとともに、協定締結後においても、平素から顔の見える関係を構築するなど実効性の向上に取り組む。

ウ　官民連携に係る取組の継続的推進

香川県サイバー攻撃対策協議会、サイバーインテリジェンス情報共有ネットワーク等を通じた脅威情報の提供や助言、事案発生を想定した共同対処訓練の実施やサイバー事案に関する情報の共有、未知の不正プログラム、不正接続先等の情報の共有等官民連携に係る取組を推進する。

エ　経済安全保障の観点を考慮に入れた対策の推進

経済安全保障の観点からもサイバーセキュリティ対策の推進は重要性を増していることから、サイバー事案により、我が国が保有する技術情報をはじめとする様々な情報が窃取されるリスクがあることや、サプライチェーンを構成する企業が打撃を受けるリスクがあることについて、関係行政機関と連携し、民間事業者・業界団体、研究機関等に注意喚起を行う。

オ　学校教育と連携したセキュリティ人材の育成

地域社会全体のセキュリティ水準を向上させるため、警察のサイバーセキュリティに関する知見を活用し、大学や高等専門学校等に対する講師派遣、出張講義等の取組を推進する。

また「第３次学校安全の推進に関する計画」（令和４年３月 25 日閣議決定）は、「国は、警察等の関係機関と連携しながら、教育委員会における教職員に対するサイバーセキュリティに関する研修の充実を促進する」としていることから、サイバー部門の職員を教育委員会における研修の講師として派遣するなどを通じて、地域社会全体のセキュリティ水準の向上を図る。

カ　サイバー防犯ボランティアの拡大・活性化

サイバー防犯ボランティアの拡大・活性化のため、各種イベント等において活動事例を紹介するなど広報活動を推進する。

また、政府の「サイバーセキュリティ戦略」及び「第３次学校安全の推進に関する計画」は、学校とサイバー防犯ボランティアの連携を図り、サイバーセキュリティに関する注意事項の啓発等に取り組むこととしていることから、小中学校、高等専門学校、大学等とも連携しながら効果的な取組を推進する。

さらに、有識者による教養の場を構築するなど、活動参加者の専門性の向上等サイバー防犯ボランティアの魅力を高め、その活性化を図る。