

○ 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)

情報通信技術の発達や社会のデジタル化の進展により、サイバー空間は、重要な社会経済活動が営まれる公共空間へと進化している。

様々な社会経済活動が、サイバー空間を通じて非対面・非接触で行われるものへと大きく移行する中、ランサムウェアによる被害が拡大するとともに、不正アクセスによる情報流出や、国家を背景に持つサイバー攻撃集団によるサイバー攻撃が明らかになるなど、サイバー空間における脅威は、極めて深刻な情勢が続いている。

こうした情勢を踏まえ、警察庁では、令和4年度にその組織を改正し、サイバー警察局を設置するとともに、関東管区警察局に重大サイバー事案の捜査等を行うサイバー特別捜査隊を設置した。

県警察においては、これまで「香川県警察におけるサイバーセキュリティ戦略の改定について」（平成30年11月7日付け香企画第322号。以下「旧通達」という。）に基づき、サイバー空間の脅威に関する諸対策を推進してきたところであるが、昨年9月に政府において新たな「サイバーセキュリティ戦略」が閣議決定されたことや、警察庁における組織改正を踏まえ、警察庁において「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、この度、別添のとおり、「香川県警察におけるサイバーセキュリティ戦略」を策定することとした。

各位にあっては、社会情勢の変化を見据えた取組を一層推進するため、本戦略に基づき、警察組織の総合力を発揮した効果的な対策を推進されたい。

別添

香川県警察におけるサイバーセキュリティ戦略

第1 情勢認識

デジタル化の進展等に伴い、サイバー空間は、全国民が参画する公共空間へと変貌を遂げ、今後の技術開発やインフラ整備の進展等により、実空間とサイバー空間が融合した社会の到来が現実となりつつある。

他方で、新しいサービスや技術を悪用した犯罪が続々と発生し、その手口は悪質・巧妙化の一途をたどっているほか、国家を背景に持つサイバー攻撃集団によるサイバー攻撃が明らかになるなど、サイバー空間をめぐる脅威は、極めて深刻な情勢が続いている。

こうした情勢の中で、サイバー空間の安全・安心を確保していくためには、県警察として、深刻化するサイバー空間の脅威に適切に対処できる態勢を整備するとともに、多様な主体と手を携え、社会全体でサイバーセキュリティを向上させるための取組を強力に推進する必要がある。

第2 サイバー事案への対処を担う主体

サイバー空間における脅威に的確に対処するには、各主体がそれぞれの役割を十分に理解し、相互に緊密な連携を図ることが重要である。

1 警察庁

サイバー空間をめぐる極めて深刻な情勢や、犯罪手口等が急速に変化する現状に対処するため、警察庁は、的確に情勢を把握し、政策機能をより一層発揮することにより、サイバー事案に対する警察組織全体の対処能力の向上を推進する必要がある。特にサイバー警察局は、警察庁内各局や国内外の多様な主体と連携し、サイバー政策の推進における中心的な役割を担う。

また、サイバー特別捜査隊は、外国捜査機関等との国際共同捜査に積極的に参画するなど、重大サイバー事案への対処を担う。

さらに、情報技術解析部門においては、幅広い捜査ニーズを捉えた的確な情報技術解析等を実施する。

2 県警察

サイバー特別捜査隊の設置に伴い、今後は同隊において重大サイバー事案の捜査等を推進することとなるが、これによって、県警察の責務は何ら減ずるものではない。

また、県民の安全・安心を確保するため、サイバー事案に関する実態把握から被害防止対策の浸透に至るまで、地域社会との連携の重要性は一層高まっていることから、県警察は、本部・署・交番等全ての組織を挙げて地域社会との連携を一層強化し、被害相談の受付・捜査・対策等を推進する役割を担う。

第3 推進事項

1 体制及び人的・物的基盤の強化

(1) サイバー空間の脅威に対処するための体制の構築

地理的な制約を受けないこと、高度な技術が用いられること等の特性を持つサイバー事案へ対処するためには、リソースを最大限に有効活用することが不可欠である。

こうした観点を踏まえつつ、サイバー部門の体制整備を推進するとともに、サイバーセキュリティ総括責任者を中心とするサイバー部門の連携体制を一層強化する。

(2) 優秀な人材の確保及び育成

構築した体制の機能を遺憾なく発揮するためには、サイバー事案への対処や国際的な感覚に秀でた多様な人材の確保・育成が不可欠であることから、こうした資質を有する者の採用及び育成を部門横断的かつ体系的に推進する。

特に、人材育成に関しては、民間の知見等を活用するほか、高度な教養機会の確保に向けた環境整備を推進するとともに、捜査員・技術者の垣根を越えた人的交流、知見の共有等を促進することにより、捜査と技術の両方に精通した人材層の充実を図る。

また、警察庁との人事交流により、サイバー事案に対する組織全体の対処能力の向上に努めるとともに、当該人事交流の趣旨を十分に踏まえた人事配置に配慮する。

このほか、内外で顕著な実績を挙げた職員に対し、適切な賞揚を行うこと等により、更なる能力の研鑽と職務への精励を促す。

(3) 職員全体の対処能力の向上

サイバー事案に関する地域住民からの多様な相談等に適切に対応するためには、部門を問わずサイバー・デジタル分野に係る対処能力を向上させることが必要であることから、組織全体として当該分野に係る能力の修養を教養の根幹に位置付け、対処能力の向上に向けた人材育成を推進する。

(4) 資機材の充実強化

サイバー事案への対処に必要な資機材及び解析用資機材の整備・高度化、情勢に応じた機能強化等を推進し、対処能力の向上を図る。

(5) 警察における情報セキュリティの確保等

警察を標的としたサイバー事案による被害を未然に防止し、又は最小化するため、ぜい弱性情報等の情報セキュリティインシデントに発展し得る情報の集約・組織的管理、職員の情報リテラシーの向上、情報セキュリティインシデントに対する対処能力の強化等を推進する。

2 実態把握と社会変化への適応力の強化

(1) 通報・相談への対応強化による実態把握の推進

新たなサービスや技術の開発等により急速に変化する情勢に対処するためには、平素から情報の収集・分析に努め、当該変化を早期かつ的確に把握することが不可欠である。

国民・事業者等からの通報・相談は、捜査の端緒となるだけでなく、サイバー空間をめぐる情勢の変化を把握する観点からも重要であることから、警察へ

の通報・相談が適切になされるよう、広報啓発等を通じた通報・相談しやすい気運の醸成や環境整備等を推進するとともに、通報・相談の直接の受け手として、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に努める。また、情報窃取の標的となるおそれの高い先端技術を有する事業者等との情報交換を積極的に推進する。

(2) 実態解明と実効的な対策の推進

事案対処に際しては、被疑者の検挙のみならず、犯行手口等の実態解明や被害の拡大防止等の観点が必要である。

国家の関与が疑われるものも含め、サイバー事案に対する厳正な取締りを推進し、実態解明を進めるとともに、警察庁等と連携し、解明された情報の適切な公表等を通じて、被害の未然防止・拡大防止、犯罪インフラ対策等を推進する。また、重要インフラ事業者等との実践的な共同対処訓練を実施する。

さらに、実態解明を進めるためには、インターネット上の情報収集、不正プログラムの解析等が必要であることから、先端技術を活用した分析・解析の高度化・効率化を推進する。

加えて、サイバーパトロール等により、違法情報・有害情報の把握に努め、その取締り等を推進する。

3 部門間連携の推進

限られた体制でサイバー事案に適切に対処するためには、事案認知・事案対処・被害防止対策等の各段階において、関係部門が連携することが不可欠である。

サイバー事案に対しては、サイバー部門のみならず、各事件主管課が主体的に捜査を推進することとするほか、特に、高度な情報技術が悪用され、組織的に敢行されるサイバー事案に対しては、関係部門が連携して、犯行手口や組織的なつながり等の解明を推進する。

また、相談受理・情報共有体制の構築、サイバー部門による技術支援の実施、事業者等との関係構築における協調等、組織の総合力を発揮するための部門間連携の体制強化を推進する。

4 国際連携の推進

国境を越えて敢行されるサイバー事案に適切に対処するためには、外国捜査機関等との強固な信頼関係の構築に取り組むことが重要である。

警察庁は、国際共同捜査への積極的な参画に向けた環境を整備するとともに、国境を越えて敢行されるサイバー事案に対処するため、外国捜査機関等との信頼関係を構築し、互恵的な関係を構築することから、県警察では、外国捜査機関等からの共助要請への適切な対応や、国際捜査の端緒の入手の観点から、初動捜査を徹底する。

5 官民連携の推進

(1) 産学官の知見等を活用した対策の推進

日本サイバー犯罪対策センター（JC3）等と連携し、産学官の情報や知見

を活用したサイバー事案に係る取締り及び被害防止対策を推進する。

また、サイバー分野において先端的な研究等を行っている学術機関との共同研究を推進する。

(2) 民間事業者等における自主的な被害防止対策の促進

サイバー事案による被害を防止するためには、警察による取組のみならず、民間事業者やインターネット利用者等も含めた社会全体における対策が重要であることから、関係機関、民間事業者・団体等と連携した効果的な広報啓発活動等を推進する。

(3) 民間事業者等と連携した犯罪インフラ対策の推進

新たなサービスや技術が、サービス設計の欠陥を突かれるなどして悪用され、犯罪インフラとして機能する例が認められるところ、犯罪インフラ化を阻止するためには、民間事業者等と連携して対応することが不可欠である。

サービスの悪用を防止する観点からのサービス設計の見直し、事後追跡可能性の確保等、民間事業者等において必要な対策が行われるよう、信頼関係の構築に努めるとともに、被害実態の情報提供等を通じた働き掛けを推進する。

(4) 地域において活動する多様な主体との連携

地域社会全体のサイバーセキュリティの水準を向上させるためには、警察だけでなく、地域において活動する多様な主体との連携が不可欠である。また、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、こうした視点を持って取り組むことが重要である。

そのため、サイバー防犯ボランティア等の地域に根ざした各主体の活動や学校教育とも連携して、サイバーセキュリティ人材の育成や各種防犯活動等を推進する。