

兵庫県警察におけるサイバー戦略の実施について（一般甲）

令和4年8月25日
兵警C I 一般甲第67号

兵庫県警察におけるサイバー戦略の実施について（一般甲）（要徹底）

対号 兵庫県警察におけるサイバーセキュリティ戦略の継続実施に
ついて（令和2年9月7日兵警C I 一般甲第78号）

兵庫県警察においては、深刻化するサイバー空間の脅威に適切に対処するため、対号に基づき各種対策を推進しているところであるが、社会情勢の変化を見据えた取組を一層推進するため、警察庁において警察におけるサイバー戦略が策定されたことを踏まえ、兵庫県警察においても兵庫県警察におけるサイバー戦略（別添）を策定し、これに基づき各種対策を推進することとしたので、各所属長は、所属職員に周知徹底の上、その実効を上げられたい。

なお、対号は、廃止する。

兵庫県警察におけるサイバー戦略

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、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、新しいサービス又は技術（以下「新サービス等」という。）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、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体制を整備するとともに、国内外の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 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（警察法（昭和29年法律第162号）第5条第4項第6号ハに規定するサイバー事案をいう。以下同じ。）に対処するためには、リソースを最大限に有効活用する必要があることから、警察本部長の強力な指導の下、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

ア 構築した体制の機能を遺憾なく発揮するため、サイバー事案への対処及び国際的な感覚に秀でた多様な人材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、捜査員と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。

イ 警察庁との人事交流により、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。

ウ 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) 警察職員全体の対処能力の向上

サイバー事案に関する県民、事業者等からの通報及び相談（以下「通報等」という。）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

向上させる必要があることから、警察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及び組織的管理、警察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) 通報等への対応強化による実態把握の推進

ア 新サービス等の開発等により急速に変化する情勢に対処するため、サイバーパトロール等により違法情報及び有害情報の把握に努めるなど、平素から情報の収集及び分析に努め、当該変化を早期かつ的確に把握する。

また、県民等からの通報等は、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、警察への通報等が適切になされるよう、積極的な広報啓発等により通報等がしやすい気運の醸成、環境整備等を推進するとともに、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。

イ 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

ア 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。

また、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不可欠であることから、人工知能等の先端技術を活用した分析及び解析の高度化及び効率化を推進する。

イ 関係機関等と連携し、解明された情報の適切な公表等を通じて、被害の未然防止及び拡大防止、犯罪インフラ対策等を推進するほか、重要インフラ事業者との実践的な共同対処訓練を実施する。

3 部門間連携の推進

(1) 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、限られた体制で適切に対処するため、事案認知、事案対処、被害防止対策等の各段階において、関係部門が連携して対応する。

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、組織的なつながり等の解明を推進する。

- (2) 相談受理体制及び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、警察の総合力を発揮するための部門間の連携体制の強化を推進する。

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り、外国捜査機関等からの共助要請への適切な対応及び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（J C 3）等と連携し、産学官の情報及び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・デジタル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、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

新サービス等が、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事例が認められることから、これを阻止するため、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、被害実態の情報提供等を通じた働き掛けを推進するとともに、個別の事業者等との信頼関係の構築に努める。

(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、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及び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、各種防犯活動等を推進する。