Ｂ　５　－　１

５年保存（常） （令和９年12月31日まで）

ＦＮ．Ｂ５－１－０
鹿サ対第２９号
鹿　務第１５４４号
鹿　会第２２４号
鹿　相第１３０号
鹿　監第６６号
鹿　情第７８号
鹿生企第２１５号
鹿人少第１４３号
鹿生環第６６号
鹿刑企第１０５号
鹿捜一第１５７号
鹿捜二第５２号
鹿組対第１２７８号
鹿科研第３１号
鹿交企第３０８号
鹿交指第７４号
鹿　公第９２号
令和４年６月３０日

各部長
各参事官　殿
各所属長

本部長

担当	企画指導係	TEL	[redacted]

鹿児島県警察におけるサイバー戦略について（通達）

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。

本県警察においては，これまで，「鹿児島県警察サイバーセキュリティ戦略の改定について（通達）」（平成31年３月18日付け鹿サ対第１号ほか。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「サイバーセキュリティ戦略」（令和３年９月28日閣議決定）が策定されたことや，警察庁における組織改正を踏まえ，社会情勢の変化を見据えた取組を一層推進するため，このたび，別添のとおり，鹿児島県警察におけるサイバー戦略を策定することとした。

各位にあっては，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。

なお，この通達は令和４年６月30日から施行し，旧通達は同年６月29日限り廃止する。

別添

鹿児島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，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，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　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こととなる。

関東管区警察局に設置されるサイバー特別捜査隊にあっては，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い，情報技術解析部門にあっては，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こととなる。

２　本県警察

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，本県警察の責務は何ら減ずるものではない。

また，国民の安全・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，本県警察においては，警察本部・警察署・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，警察庁においては，サイバー警察局，サイバー特別捜査隊，全国の情報通信部等を含むサイバー部門全体の体制整備を推進している。

また，本県警察においては，「鹿児島県警察サイバーセキュリティ対策委員会設置

要綱の制定について（通達）」（令和４年６月８日付け鹿サ対第23号ほか）に規定するサイバーセキュリティ総括責任者を中心として，サイバー事案に対処するための人材，資機材等リソースの拡充を進めるとともに，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，関連部門の連携体制を一層強化する。

加えて，全ての所属においても，事案対応等に際し，必要な時は遅滞なくサイバー犯罪対策課の支援を要請することとし，そのため，あらかじめサイバーセキュリティ総括責任者との連携を担う者をそれぞれの所属に配置するなど，これら連携が円滑に行われる体制を構築する。

(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，警察庁と本県警察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意する。

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，更なる能力の研さんと職務への精励を促す。

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国内外の民間団体，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。

ウ　専門捜査員の育成

本県警察においては，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兼務をかけるなどにより，これらの職員をサイバー事案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。

エ　ハイブリッド人材の育成

警察庁においては，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る競技を新設しているところ，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。

オ　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，本県警察からサイバー警察局・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一定の者に対し，その能力が明らかになるような施策を行い，人事に活用するなどキャリアパスの確立を行い，士気高く勤務できる環境の整備を推進する。

カ　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に対する表彰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措置を講ずる。

(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，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。

よって，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，職員の自己研さんを促進するため，教養資料の配布，部内でのサイバーセキュリティ関連競技大会を拡充する。

(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，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。

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，警務部長を中心とした情報セキュリティ体制とサイバー犯罪対策課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，警務部長を中心とした情報セキュリティ体制とサイバー犯罪対策課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はじ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ずるとともに，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，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

(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。

県民・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。特に，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。

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，サイバー犯罪対策課に遅滞なく伝達するなど，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。

(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不可欠である。

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，関係省庁等と連携し，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・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。

ア　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，関係機関と連携して，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。

なお，サイバー警察局においては，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も念頭に，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こととしていることから，その点にも留意した情報の集約や分析に取り組む。

イ　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，解析の効率化・高度化を図る。

また，実態解明に不可欠であるＩｏＣ等の大量データの総合的な分析，データ間の関連性検証等に多くの人材を投入しているところ，この種の作業を効率的に推進し，より高度な分析・判断等に人材投入を行うことが可能となるよう，人工知能等先端技術の導入について検討を進める。

ウ　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。

また，警察庁においては，インターネット上の脅威情報を収集・分析するリアルタイム検知ネットワークシステムについて，能動的に犯罪の端緒等を検知・発見し，犯罪捜査を通じた実態解明と対策に資する情報を提供するための機能増強を図ることで，情報収集・分析を高度化することとしている。

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，警察の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，サイバー犯罪対策課のみならず，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。

なお，相談受理・情報共有体制の構築，サイバー犯罪対策課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連携の体制強化を推進する。

(1)　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。

(2)　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はじ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，サイバー犯罪対策課を中心に，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全国警察で共有する。

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，サイバー犯罪対策課において，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本県警察との連携

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本県警察が連携して，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本県警察の関係部門との間で必要な連絡調整を推進する。

(3)　被害防止対策における部門間連携

サイバー犯罪対策課においては，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，サイバー犯罪対策課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

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となる。

本県警察における取組においては，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。

また，外国捜査機関等との信頼関係構築の観点も踏まえ，外国捜査機関等からの共助要請にも，適切に対応する。

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

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）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・共有するなどの取組を推進する。

また，学術機関との間において，機械学習に係る学習データ等，双方に有用な情報の共有等も含めた実効的な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。

関係機関，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。

(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，被害実態の情報提供等を通じた働き掛けを推進する。特に，本県警察においては，個別の事業者等との信頼関係の構築に努める。

ア　他部門と連携した効果的な取組の推進

サイバー犯罪対策課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　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，関係機関等と連携しながら，関係事業者に対して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。

エ　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，警察庁にあっては，関連する業界団体等と被害実態の情報共有を推進しているところ，本県警察にあっては，法令違反に対する取締りを推進する。

オ　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。

カ　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ずるほか，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。

キ　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，警察庁にあっては，関係団体等と連携して，被害実態を踏まえた有効な

対策を推進しているところ，本県警察にあっては，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。

ク　フィッシング対策の推進

警察庁においては，フィッシングサイト等について，警察が把握した情報をウイルス対策ソフト事業者等に提供するほか，スミッシングについては，フィッシングサイトに誘導するショートメッセージの遮断に向けて，ＪＣ３とも連携して，関係事業者の取組に必要となる捜査関連情報等の共有に取り組むこととしていることから，本県警察では関連情報の収集等に取り組むとともに，県民・事業者等に対して，フィッシングの手口に関する情報提供や注意喚起等の広報啓発等を推進し，被害拡大防止を図る。

ケ　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。

(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。

警察庁にあっては，地域における連携が円滑に行われるよう，関係省庁・業界団体等との連携強化に努めているところ，本県警察にあっては，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。

ア　地域に根ざした各主体の防犯活動との連携

警察に対して，中小企業等に対するサイバー空間の脅威に対しての十分な対応ができていないとの指摘等もあることから，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，都道府県の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，これらの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

サイバーテロ対策協議会，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」としており，サイバー犯罪対策課等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し，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おり，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，サイバー犯罪対策テクニカルアドバイザー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。