有効期間満了日　平成３４年３月３１日
熊サ対第１１９２号
平成３０年９月１２日

熊本県警察サイバーセキュリティ重点施策の策定について（通達）

本県におけるサイバーセキュリティ戦略については、「「サイバーセキュリティ重点施策の策定について（通達）」（平成 27 年 11 月 30 日付け熊サ対第 1685 号。以下「旧通達」という。）」に基づき取組を強化しているところであるが、警察庁通達「「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（依命通達）」（平成30年９月６日付け警察庁乙官発第11号）」及び「「サイバーセキュリティ重点施策の改定について（通達）」（平成 30 年９月６日付け警察庁丙総発第 60 号）」が発出されたことを踏まえ、新たに別添「熊本県警察サイバーセキュリティ重点施策」を策定し、諸対策に取り組むこととしたので、各所属にあっては、効果的な活動を推進されたい。

なお、本通達の発出をもって旧通達は廃止する。

別添

熊本県警察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への対応の強化

１　サイバー犯罪に対する捜査等の推進

(1)　高度な情報技術を悪用したサイバー犯罪に係る捜査の推進

高度な情報技術を悪用したサイバー犯罪について、サイバー犯罪対策課特捜係を中心に、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と共有する。

また、企業等のアクセス管理者に対して、不正アクセス行為を認知した場合は警察に通報するよう要請するなど、不正アクセス行為が潜在化しないように努める。

(2)　サイバー犯罪に関与する犯罪組織の取締り等の推進

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とともに、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。

また、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、引き続き、組織的なつながり等の実態解明を推進する。

(3)　効率的かつ効果的な捜査の推進

ア　適切な部門間の分担及び連携の推進

ネットワーク利用犯罪のうち、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。

また、サイバー犯罪対策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。

イ　各事件主管課がサイバー犯罪対策課に対して現場解析等の支援要請を行う場合は、各事件主幹課において、主体的にサイバー犯罪捜査を行う体制を構築するため、必ず各所属のサイバー犯罪指定捜査員（又は「サイバー犯罪捜査員」）を同行し、解析要領等の習得に努めること。

ウ　合同・共同捜査等の推進

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、サイバー犯罪捜査情報等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、効率的で効果的な捜査を立案・実施する。

また、複数の都道府県警察との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)　違法情報・有害情報対策

ア　インターネット上の違法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について、「全国協働捜査方式」を効果的に活用するとともに、サイバー犯罪対策課特捜係を活用し、より悪質性の高い情報に重点を指向した違法情報の取締りを推進する。

また、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の取締りを推進する。

イ　違法情報等の把握・削除依頼の推進

サイバーパトロールを推進し、違法情報や自殺誘引等情報を始めとする有害情報の積極的な把握に努める。

また、把握したこれらの情報については、サイト管理者等に対して削除依頼等を確実に行う。

(5)　インターネットを利用した児童を対象とする性犯罪の取締りの推進

児童ポルノの製造や児童買春等の児童を対象とする性犯罪は、児童の人権を著しく侵害する極めて悪質な行為であることから、こうした性犯罪に対する取締りを推進し、特に悪質な低年齢児童を性的好奇心の対象とする者によるインターネットを利用した児童ポルノ事犯等に対する取締りを徹底する。

また、ＳＮＳに起因する事犯についても、サイバーパトロール等を通じて端緒情報の把握に努め、必要な捜査を推進する。

(6)　新たな犯罪手口、脅威情報等の情報収集・分析の推進

産業機械、医療機器、今後普及が想定される自動運転車等に対する不正アクセスや不正プログラム感染等、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と共有する。

(7)　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、高度な技術を要する解析について、高度情報技術解析センターを活用するなど、犯罪の取締りのための情報技術の解析を推進する。

2　国の公安を脅かす事案の防止及び対処

(1)　脅威情報の収集・分析の推進

特定の攻撃集団等の関与の疑い、特定分野を標的とした攻撃の顕在化等のサイバー攻撃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、関連が疑われる事案の情報等の収集・分析を推進する。

(2)　実態解明及び被害防止の推進

サイバー攻撃事案発生時においては、警備第一課が主体となり、サイバー犯罪対策課を始め、県情報技術解析課、刑事部門等と連携して、迅速な初動措置、捜査その他の措置を的確に実施する。

また、捜査を通じてサイバー攻撃の実態解明に必要な情報を収集し、手口や事案のつながり等の攻撃の実態の分析を行うとともに、分析結果を元に被害の未然防止・拡大防止に係る措置を行うなど、被害の防止を図る。

(3)　事案対処能力の強化

重要インフラ事業者、先端技術保有事業者、高度な研究を行う大学等に対し、平素から個別訪問等を通じ、信頼関係を醸成しつつ、連絡体制の確立に取り組むとともに、事業内容やセキュリティ対策の状況等の把握に努め、防護すべきシステムや情報の特性、サプライチェーンリスク等を考慮し、被害の実例に基

づいたセキュリティ対策について助言等を行う。
　また、サイバーセキュリティ推進協議会、サイバーテロ対策協議会を通じて、被害の未然防止・拡大防止に資する情報の共有を推進する。
　さらに、最新の脅威に関する情報等を踏まえつつ、重要インフラ事業者等の事業実態に即した実戦的な内容の共同対処訓練を実施する。その際、重要インフラ間の依存関係を始め、サイバー攻撃が発生した際の影響範囲等を考慮し、関係都道府県警察との協働も含めた広域的な視点を持って取組を進める。

(4)　サイバーフォースによる技術支援の活用

　警察庁のサイバーフォースセンター及び全国のサイバーフォースにおいて、警察に対する技術支援が推進されるので、被害の未然防止・拡大防止のため、サイバー攻撃に係る技術情報等の調査・収集・分析を推進する。

3　東京大会（２０２０年東京オリンピック・パラリンピック競技大会）に向けた取組

(1)　警察における態勢の確立

　警察において、サイバー攻撃対策、警備諸対策等が一体となった態勢を確立するとともに、警察庁に設置したセキュリティ情報センターと連携を図る。

(2)　大会関係機関等との連携の確立

　東京大会といった大規模イベントの安全かつ円滑な運営の確保を念頭に、関係省庁、関係事業者、外国治安情報機関等との円滑な情報共有等に係る態勢を確立し、関係事業者宛ての不審なメール等の情報の収集等、イベントの妨害を企図したサイバー攻撃への対策を推進する。
　また、個別訪問等を通じて大会の運営に影響する重要サービス事業者等との連携態勢を確立するとともに、事案発生を想定した共同対処訓練等を実施し対処能力の向上を図る。

(3)　国としての情報共有及び事態対処への寄与

　内閣官房に設置される「サイバーセキュリティ対処調整センター」と連携し、関係機関との情報共有を図るとともに、事案発生時は、関係機関と連携しつつ、サイバー攻撃事案の被害拡大防止を図り、大会運営への影響を最小限にとどめるとともに、捜査・実態解明を行う。

第２　警察における組織基盤の更なる強化

1　部門間連携の推進

(1)　警察における部門間の連携強化の推進

　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・調整を行うための態勢を確保し、部門間の連携強化を推進する。

(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関する人的基盤の強化

(1)　計画的な人材育成の推進

ア　サイバー犯罪対策課において、サイバー犯罪事件の対処に係る教養の充実強化を図り、サイバーエリートにサイバー捜査及び情報通信技術に関する知

識技能を習得させるとともに、東京大会までに育成体系区分毎の目標数を達成するよう計画的な人材育成を推進する。

イ　サイバー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事配置に努める。

(2)　人材育成基盤装置を活用した実践的な教養の推進

サイバー犯罪・サイバー攻撃の発信元の特定や実態解明に関する能力を向上させるため、サイバーセキュリティ対策研究・研修センターにおいて運用する人材育成基盤装置を活用し、高度な実践型演習等を受講させるとともに、警察官同士がサイバーセキュリティに関する知識・技能を競うコンテスト（ＣＴＦ競技会）を開催し、サイバー犯罪捜査の知識・技能の向上を図る。

(3)　人材確保のための取組の推進

採用試験及び昇任試験において、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効果的な採用・登用方策について検討する。

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等を検討する。

(4)　専門的捜査員の育成の推進

ア　部内教養や実務を通じた育成の推進

サイバーセキュリティ対策研究・研修センターが実施するサイバー捜査に係る高度な専門知識及び技術に関する研修を活用し、知識・技能の向上に努める。

また、サイバー攻撃対策部門の職員をサイバー犯罪捜査に従事させることにより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。

イ　情報技術解析部門との人事交流の拡大

サイバー犯罪・サイバー攻撃対策担当部門での勤務を希望する警察官等について、情報技術解析に関する知識・技能を向上させるため、情報技術解析部門との人事交流を拡大するとともに、帰任後は、当該職員の能力、適性等の事情を考慮した上で、その経験を活用できるサイバー犯罪・サイバー攻撃の捜査等へ優先的に従事させるなど、当該職員の希望を十分に配慮した人事配置を行う。

ウ　民間事業者等の知見の活用

情報通信技術に係る高度で専門的な知識やノウハウを有している民間事業者、大学等の学術機関等による研修や、民間事業者等への一定期間の人材派遣を図るなど、サイバー犯罪・サイバー攻撃に対処するために必要な高度で専門的な知識・技能を有する捜査員の育成を行う。

(5)　警察全体の対処能力の底上げ

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、サイバー犯罪捜査検定及びサイバー犯罪捜査実戦塾等を開催し､全ての警察官に基本的なサイバー捜査要領に関する知識を取得させる。

また、サイバー空間の脅威に対して、部門横断的かつ効果的な対処がなされるよう、幹部を含めた専科教養を実施するなど、幹部に対する教養を推進する。

(6) 情報技術の解析に係る教養の推進

ア 解析能力・事案対処能力の向上に係る教養の推進

最新のサイバー攻撃・防御手法や不正プログラム解析技術といった民間事業者の知見を活かした研修、附属警察情報通信学校における技術的教養、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に情報技術の解析に従事する職員を参加させ、解析能力・事案対処能力の向上を図る。

イ 電磁的記録の適正な取扱い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、県情報技術解析課と連携し、巡回教養等を実施するなど、電磁的記録の適正な取扱いに向けた取組を推進する。

3 情報収集・分析及び情報技術解析態勢の強化

(1) 脅威の実態解明を支える情報収集・分析態勢の強化

脅威情報の収集・分析に資する技術・サービスの活用等により、サイバー犯罪・サイバー攻撃や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・分析及び実態解明のための態勢を強化する。

(2) 資機材の整備の推進

サイバー空間をめぐる情勢や最新の情報通信技術に対応するため、サイバー犯罪・サイバー攻撃対策に必要な資機材、情報技術の解析に必要な資機材等の整備・拡充を推進する。

4 新たな技術の活用及び研究開発の推進

(1) 人工知能（ＡＩ）等の新たな技術の業務への活用に関する検討

民間事業者等から、人工知能（ＡＩ）等の新たな技術を活用した事例に関する情報を収集し、当該技術を活用することによる効果やリスクを分析しつつ、警察における業務の高度化・効率化に関する検討を推進する。

(2) ダークウェブからの情報収集・脅威情報の分析手法の確立等

サイバー犯罪・サイバー攻撃を未然に防止するため、ダークウェブにおける情報の収集技術を調査し、その手法を確立することにより、ダークウェブに流通する情報の収集・蓄積・分析を推進する。

(3) 効率的な不正プログラム解析手法の開発等

複雑化・巧妙化する不正プログラムに対応するため、高度な解析を効率的かつ効果的に行うことができる手法を開発し、サイバー犯罪・サイバー攻撃への対処能力の向上を図る。

5 警察における堅牢な情報セキュリティ対策

(1) 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。

(2) 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。

(3)　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結果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。

(4)　ＣＳＩＲＴの対処能力強化の推進

警察における情報セキュリティインシデントに対し、組織的な対処が図られるよう、警察に設置された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、ＣＳＩＲＴの対処能力の強化を推進する。

第３　国際連携及び産学官連携の推進

１　国際連携の推進

(1)　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。

また、より迅速な国際捜査の在り方について、警察庁と連携し、検討を進める。

(2)　外国治安情報機関等との情報交換

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、職員の人材育成等について、警察庁を通じ、平素から外国治安情報機関等との情報交換を推進する。

２　産学官の知見等を活用した対策の推進

(1)　日本サイバー犯罪対策センター（ＪＣ３）等との連携の推進

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、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。

(2)　インターネットバンキングに係る不正送金事犯等の被害防止対策の推進

金融機関等との連携を強化し、セキュリティ機能強化のための注意喚起、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)　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、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。

(4)　海外の偽サイト等に対する対策の推進

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サイバー犯罪対策課で集約し、違法性の認定、連絡の困難性の確認等をした上で警察庁に通報して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。

(5)　事後追跡可能性の確保

ア　公衆無線ＬＡＮの事後追跡可能性の確保

総務省が発行している「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」に基づき、地方公共団体等における公衆無線ＬＡＮのサイバー空間における事後追跡可能性の確保に資するサイバーセキュリティ対策を働き掛ける。

イ　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、不備が確認された場合は、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あっては、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　民間事業者等における自主的な被害防止対策の促進

(1)　社会全体におけるセキュリティ意識の向上

関係省庁、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。

(2)　児童や保護者等に対する広報啓発活動の推進

インターネットの利用に起因する子供の性被害防止やインターネット上の違法情報・有害情報の閲覧防止のため、児童、保護者及び教育関係者等に対し、被害の現状及びフィルタリング等の対策に関する広報啓発活動を推進する。

(3)　サイバー防犯ボランティアの活動支援

「ＫＣ３」を始めとしたサイバー防犯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。

(4)　インターネット観測結果の広報

警察庁ウェブサイト「@police」で広く一般に公開される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の動向等に関する情報を活用し、重要インフラ事業者や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。