

業務重点推進状況
令和7年10月

サイバーセキュリティ対策の推進について



警察本部

目 次

第 1	サイバー空間をめぐる脅威の情勢	
1	サイバー犯罪等に関する相談受理状況	4
2	サイバー犯罪の検挙状況	5
3	インターネットバンキングに係る不正送金の情勢	6
4	ランサムウェアの情勢	7
第 2	サイバー空間の脅威に対する警察の対処体制等	
1	サイバーセキュリティ・捜査高度化センター	8
(1)	サイバー企画課	8
(2)	サイバー捜査課	8
2	兵庫県警察サイバー攻撃対策隊	8
3	近畿管区警察局兵庫県情報通信部情報技術解析課との連携	8
4	その他	8
第 3	サイバー空間の脅威に対する警察の取組	
1	サイバー人材の確保	9
(1)	情報通信技術に素養のある人材の確保	9
(2)	効果的なサイバー人材の採用募集活動に向けた取組	9
2	サイバー人材の育成	9
(1)	全職員の対処能力向上	9
(2)	各部門等で活躍する捜査員の育成	10
(3)	高度な専門的知見及び捜査力を有する人材の育成	10
3	民間知見の活用	10
(1)	任期付き警察官の採用等	10
(2)	民間企業派遣研修の実施	10
(3)	「兵庫県警察サイバーセキュリティ対策アドバイザー」の活用	10
4	全国警察が協働した取組	11
(1)	全国協働捜査方式等を活用した取締りの推進	11
(2)	国境を越えたサイバー犯罪等に対する実態解明の推進	11
5	実態把握と部門間連携の推進	12
(1)	サイバー犯罪相談窓口の運用	12
(2)	各種支援活動	12
6	官民連携の推進	13
(1)	「兵庫県サイバー犯罪対策ネットワーク」の取組	13
(2)	民間企業との連携	13
(3)	広報啓発活動の推進	14
(4)	犯罪に関するインフラへの対処	15
7	サイバー攻撃対策	16
(1)	サイバーテロ対策	16
(2)	サイバーエスピオナージ対策	17
(3)	実態解明の推進	17

凡 例

本資料で使用している用語の意義は、次のとおりである。

- サイバー犯罪 高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪

- サイバー攻撃 サイバーテロ（サイバーテロに至るおそれのあるものを含む。）及びサイバーエスピオナージ

- サイバーテロ 重要インフラの基幹システムに対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害であって、電子的攻撃による可能性が高いもの

- サイバーエスピオナージ 情報通信技術を用いた諜報活動

- 重要インフラ 情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）、医療、水道、物流、化学、クレジット、石油及び港湾の15分野における社会基盤

第1 サイバー空間をめぐる脅威の情勢

1 サイバー犯罪等に関する相談受理状況

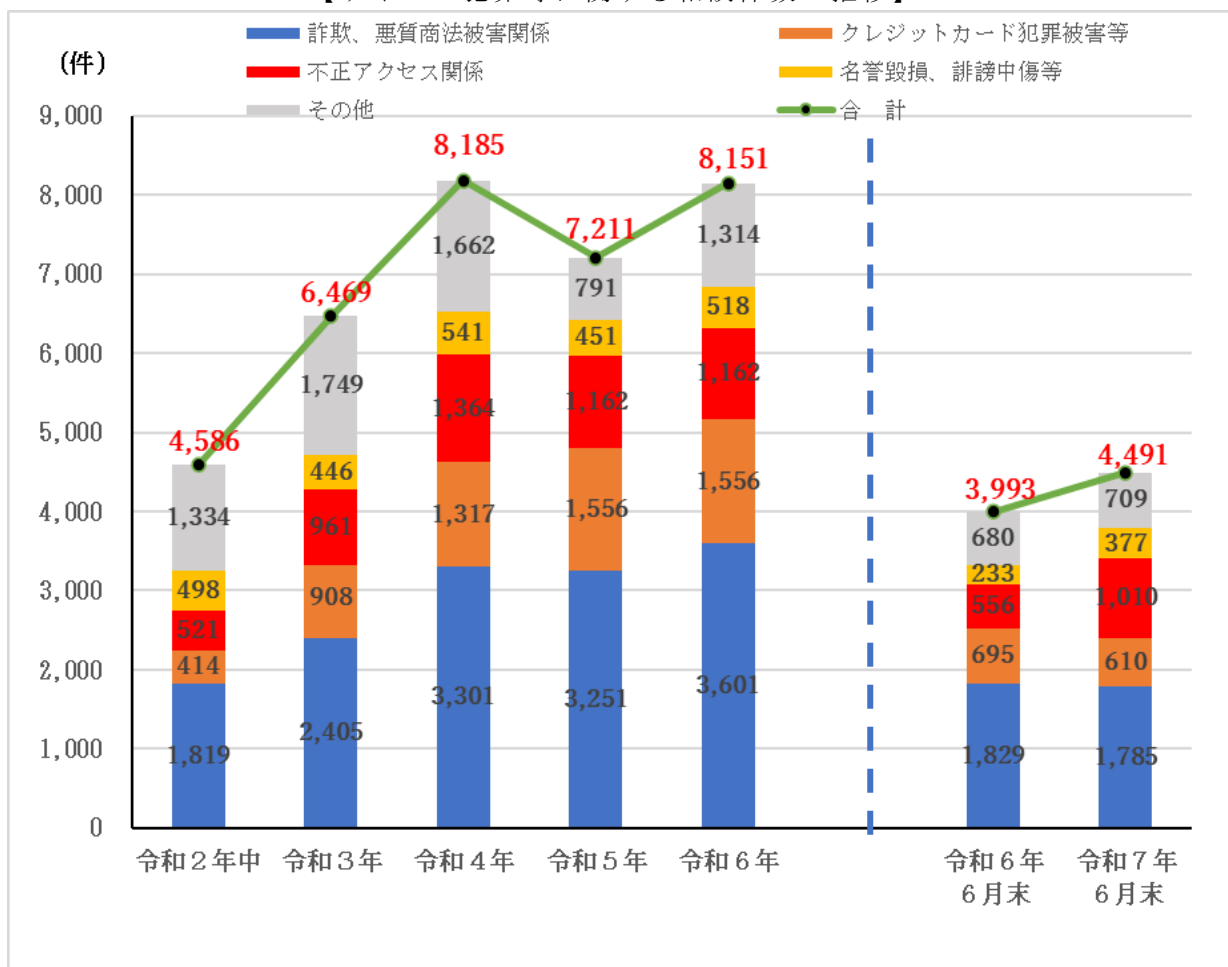
警察本部や警察署に寄せられたサイバー犯罪等に関する相談は、令和7年6月末現在、4,491件と、前年同期と比べ、498件増加している。

特に偽サイト等を利用した詐欺や投資・ロマンス詐欺をはじめとする詐欺、悪質商法被害関係（39.7%）、フィッシングメールなどによる不正アクセス関係（22.4%）、クレジットカード犯罪被害（13.5%）に関する相談が多く寄せられている。

新たな手口として、証券口座に不正アクセスし、株式を不正取引する手口が本年3月ころから急増した。

新たな手口や被害が拡大するおそれのある手口については、早期に実態解明を進め、SNS等を活用した広報啓発を行うとともに、警察庁に報告することで、民間事業者への働きかけや全国警察が協働した取組を行っている

【サイバー犯罪等に関する相談件数の推移】



その他は「オークション被害関係」、「児童買春、児童ポルノ等」、「コンピュータウイルス等」、「迷惑メール関係」、「違法ホームページの通報」、「プロバイダとのトラブル」等の相談区分の総数を示す。

2 サイバー犯罪の検挙状況

サイバー空間の公共空間化が加速し、あらゆるサービスにインターネットが活用されている一方で、インターネットが犯罪インフラとして様々な犯罪に利用されており、検挙罪名も多岐にわたっている。

また、海外や複数の都道府県にまたがり、組織的に敢行される事案も多く、警察庁の調整のもと、複数の都道府県警察の合同捜査による検挙活動を進めている。

【サイバー犯罪の検挙件数の推移】

区分	年別							
	令和2年中	令和3年中	令和4年中	令和5年中	令和6年中	令和6年6月末	令和7年6月末	前年同期比
不正アクセス禁止法違反	13	31	18	14	21	5	5	±0
コンピュータ・電磁的記録対象犯罪等	33	43	54	61	65	17	29	+12
電子計算機使用詐欺等	31	42	54	59	62	15	25	+10
不正指令電磁的記録作成・供用等	0	0	0	0	0	0	0	±0
その他	2	1	0	2	3	2	4	+2
ネットワーク利用犯罪	376	455	405	435	430	175	348	+173
詐欺	70	212	170	111	87	35	75	40
ストーカー規制法違反	39	42	51	49	53	25	31	+6
脅迫	51	16	36	42	25	12	36	+24
児童ポルノ禁止法違反	70	61	34	60	39	26	29	+3
犯罪収益移転防止法違反	16	19	18	50	86	18	50	+32
その他	130	105	96	123	140	59	127	+68
合計	422	529	477	510	516	197	382	+185
全国の検挙件数	9,875	12,209	12,369	12,479	13,164	5,838	6,625	+787

「ネットワーク利用犯罪」とは、犯行の手段としてインターネット等を利用した犯罪で不正アクセス禁止法違反及びコンピュータ・電磁的記録対象犯罪等を除いた犯罪をいう。

【検挙事例】

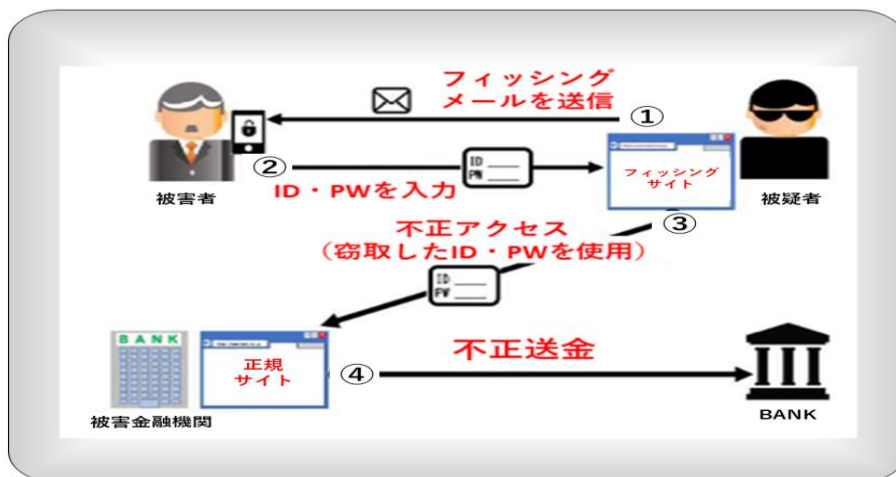
関東管区警察局サイバー特別捜査部において、クレジットカード関連犯罪の情報分析により浮上した被疑者を関係する15都道府県警察に情報提供がなされ、本県においては、匿名性の高い通信アプリを利用し、クレジットカード情報を不正に入手した被疑者を割賦販売法違反で検挙。さらに、同クレジットカード情報を不正に使用し、ECサイトで商品を購入し、商品の受け子方に配送させていたため、受け子とともに、私電磁的記録不正作出・同供用及び窃盗で検挙した。

3 インターネットバンキングに係る不正送金の情勢

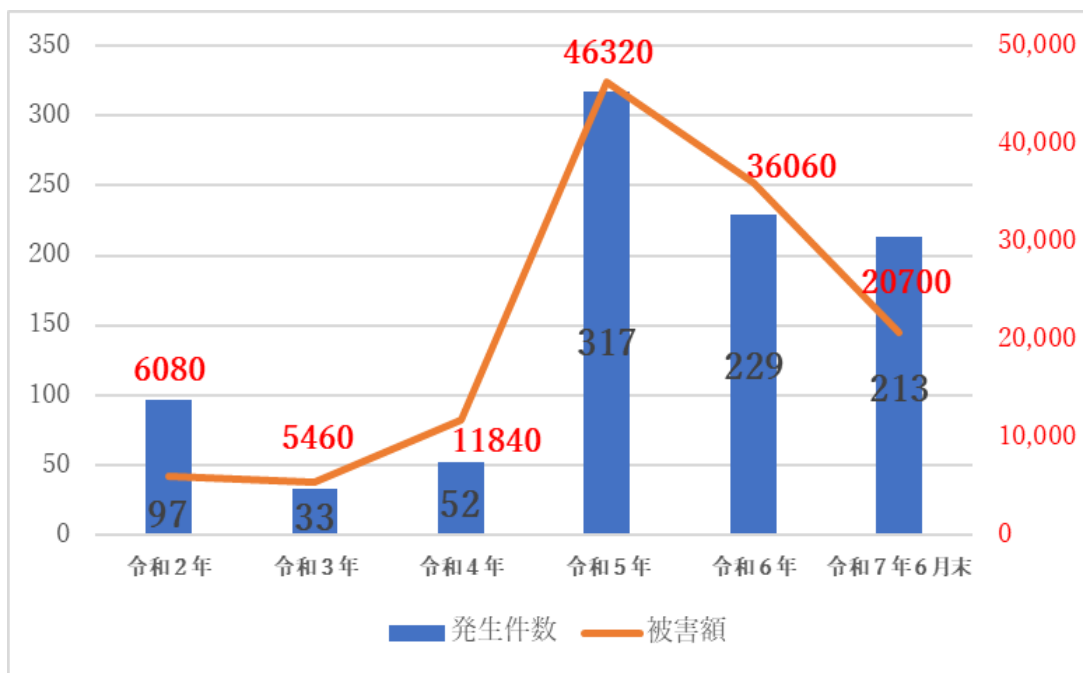
インターネットバンキングに係る不正送金事犯の発生件数は、令和7年6月末現在、213件(+111件)、被害額は約2億700万円(+8,750万円)で、前年に比べ増加しており、深刻な情勢である。

その被害の多くは、金融機関等のメールやショートメッセージを装ったフィッシングによるものである。

【フィッシングによる不正送金の概要】



【インターネットバンキングに係る不正送金の発生状況（兵庫県）】



年別区分	令和2年	令和3年	令和4年	令和5年	令和6年	令和7年6月末	前年同期比	
兵庫	発生件数	97	33	52	317	213	+111	
	被害額	約6,080万円	約5,460万円	約1億1,840万円	約4億6,320万円	約3億6030万円	約2億700万円	+8,750万円
全国	発生件数	1,734	584	1,136	5,575	4,320	2,552	+867
	被害額	約11億3,300万円	約8億1,970万円	約15億1,950万円	約87億2,960万円	約85億9,440万円	約38億8,590万円	+15億6,460万円

注 発生件数等は暫定値。

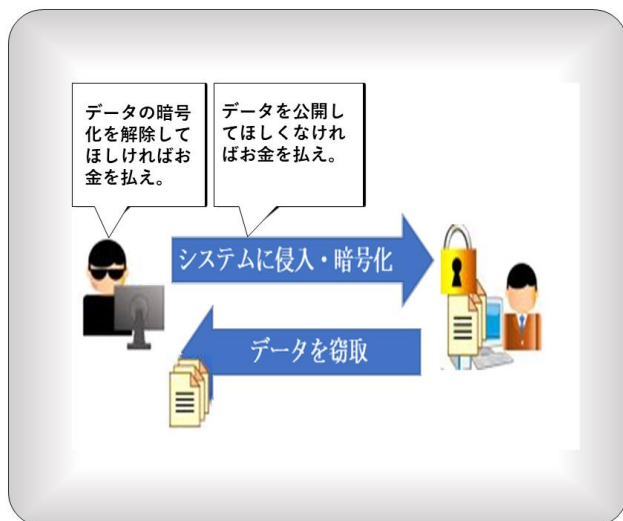
4 ランサムウェアの情勢

ランサムウェアとは、端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラムである。

近年では、データの暗号化のみならず、データを窃取した上で「対価を支払わなければデータを公開する。」などと対価を要求する二重恐喝（ダブルエクストーション）の手口のほか、中小企業が狙われ、サプライチェーン（供給網）に被害が及ぶものが見られるが、高額な対策費用や狙われないという過信などもあり、中小企業の対策は進んでいない。

警察が認知した情報は、警察庁に集約され、暗号化されたデータを復元するためのツール開発や、海外の捜査機関との国際共同捜査に反映させている。

ランサムウェア
「二重恐喝（ダブルエクストーション）」



ノーウェアランサム



【ランサムウェア被害の認知件数】

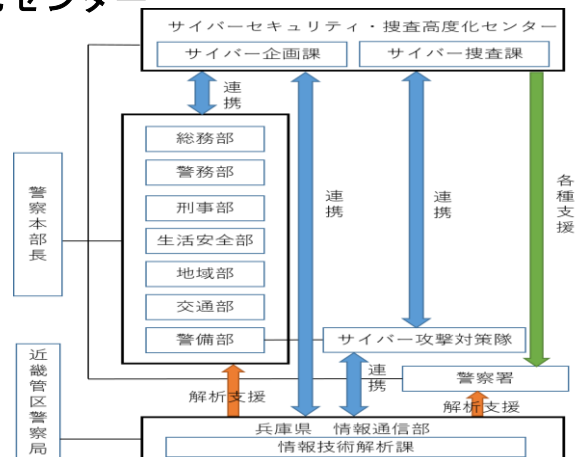
区分	年別	令和2年中	令和3年中	令和4年中	令和5年中	令和6年中	令和6年 (6月末)	令和7年 (6月末)	前年同期比
兵庫県	認知件数	1	9	11	7	10	2	5	+3
	うち二重恐喝	0	5	2	3	7	1	2	+1
	ノーウェアランサム	—	—	—	1	1	1	0	-1
全国	認知件数	21	146	230	197	222	108	116	+8
	うち二重恐喝	—	84	119	130	111	75	70	-5
	ノーウェアランサム	—	—	—	30	22	8	8	±0

注 令和元年以前の認知件数及び令和2年以前の二重恐喝件数の全国統計の公表無し。
ノーウェアランサムは令和5年上半期から集計。

第2 サイバー空間の脅威に対する警察の対処体制等

1 サイバーセキュリティ・捜査高度化センター

サイバー空間の脅威に対処する司令塔として既存各部に属さない警察本部長直轄の所属となるサイバーセキュリティ・捜査高度化センター（以下「サイバーセンター」という。）を新設し、令和6年4月から、円滑な連携を図るため、サイバー関連部署を一箇所に集約し、人材や機材等のリソースを一体的に運用できる体制を確立した。



(1) サイバー企画課

サイバー分野における県警察全体の司令塔として、部門の縦割りを排し、部門間連携による取組及び産学官の連携による地域社会全体のサイバーセキュリティに対する取組について、企画・立案及び促進を図るとともに、県警察内のサイバー人材の育成等を推進している。

(2) サイバー捜査課

関連する事件主管課と連携・調整した上で、高度なサイバー犯罪等に対する捜査を行うとともに、警察署を始め、各事件主管課に対する捜査支援、スマートフォンを始めとした電子機器等の解析などの技術支援等を推進している。

2 兵庫県警察サイバー攻撃対策隊

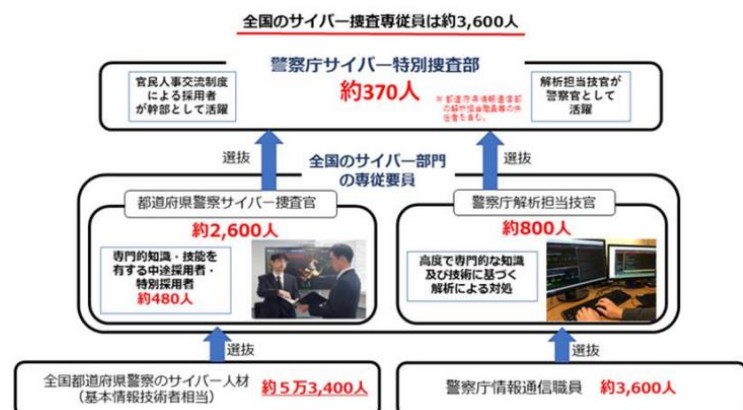
警備部公安第一課に「兵庫県警察サイバー攻撃対策隊」を設置し、サイバー攻撃に係る情報収集活動や、民間事業者等との連携に努めている。

3 近畿管区警察局兵庫県情報通信部情報技術解析課との連携

解析は、必要とされる技術レベルに応じて多段階の体制が整備されており、高度な解析が必要なものは、国の機関である近畿管区警察局兵庫県情報通信部情報技術解析課が解析にあっている。

4 その他

警察庁及び都道府県警察において、サイバー事案への対処体制や、国内外の多様な主体と連携する仕組みを整備している。



第3 サイバー空間の脅威に対する警察の取組

1 サイバー人材の確保

(1) 情報通信技術に素養のある人材の確保

県警察の採用試験において、情報通信技術資格を有する者等を対象とした特別区分採用枠である「サイバー捜査区分」による巡査採用に加え、令和7年度から、サイバー捜査区分よりも高度な専門知識・技術を有した即戦力となる高度人材を確保するため、一定の情報通信技術資格と同職歴を有する者を巡査部長、警部補の階級で中途採用する「サイバー捜査官選考」を新設するなどサイバー捜査を担う人材の確保に取り組んでいる。

(2) 効果的なサイバー人材の採用募集活動に向けた取組

新たなサイバー人材を獲得するため、警察官採用センターと連携して、情報通信技術に関する知識等を有する学生が在籍する大学・専門学校等への訪問や説明会などの採用活動を実施している。

2 サイバー人材の育成

(1) 全職員の対処能力向上

ア サイバー対処能力検定の実施

県警察全体のサイバー空間の脅威への対処能力の向上を図るため、全警察官を対象に、サイバー事案への対処に係る知識及び技能を検定する「サイバー対処能力検定」（更新制）を実施している。

イ 各種教養の実施

サイバー捜査手法、その他の対処要領を習得するための専科教養や、警察署において解析機器等を使用したハンズオン講習等を開催し、被疑者の特定方法やスマートフォンの解析方法など、実践的に体得させている。

また、教養内容に応じて、オンライン講習を併用するなどしている。



【警察署における講習の状況】



【ロールプレイング形式による教養状況】

(2) 各部門等で活躍する捜査員の育成

刑事部門、生活安全部門等、各部門の捜査において中核を担うことが期待される捜査員をサイバー捜査実務研修生としてサイバーセンターに配置し、1年間の研修プログラムにより専門的知識を習得させ、サイバー捜査能力の向上を図っている。

また、警察署勤務員を短期研修生としてサイバー捜査課に配置し、3か月間の実務研修によりサイバー捜査に係る知識と技術を習得させ、警察署において的確な初動対応を行うことができるよう育成している。

(3) 高度な専門的知見及び捜査力を有する人材の育成

サイバー捜査区分採用者等の専門的知識・技術を有する者を対象に、スマートフォン等の電磁的記録の解析を中心とした実践的な研修や専門的知識を要するサイバー捜査に従事させ、高度なサイバー犯罪等に適切に対処できる捜査員を育成している。

また、極めて高度な専門技術及び捜査力を有する者を「サイバー特別捜査官」として本部長が指定し、指定された者はサイバー関係事案の捜査指揮や各部門に対する支援、人材の育成を行う。

3 民間知見の活用

(1) 任期付き警察官の採用等

民間企業において、情報通信技術に関する技術者として活躍する人材を、1年間の任期付きで警察官として採用し、サイバー捜査や技術指導、捜査員への教養に活用している。



【任期付き警察官による教養状況】

また、任期終了後は「兵庫県警察サイバーテクニカルサポーター」として委嘱するなど、技術的なサポートを受けている。

(2) 民間企業派遣研修の実施

高度な情報通信技術を有する民間企業に捜査員等を3か月間から1年間派遣し、専門的な情報通信技術の知識・技能を習得させるとともに、民間企業との協力関係の構築による対処能力の強化を図っている。

(3) 「兵庫県警察サイバーセキュリティ対策アドバイザー」の活用

専門的知識を有する研究者、技術者等を「兵庫県警察サイバーセキュリティ対策アドバイザー」として委嘱し、捜査活動や被害防止対策について、専門的見地から指導や助言を受けている。



【アドバイザー参加のセキュリティフォーラム】

4 全国警察が協働した取組

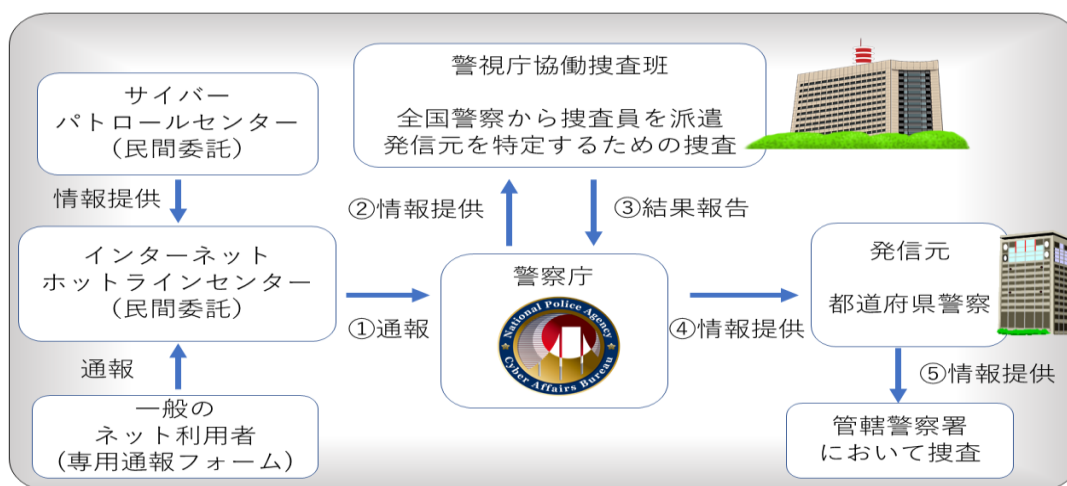
(1) 全国協働捜査方式等を活用した取締りの推進

警視庁に設置された「協働捜査班※₁」がインターネットバンキングに係る不正送金事犯の初期捜査やIHC※₂から通報を受けた情報に対する追跡捜査などを実施することで、捜査の合理化・効率化を図るとともに、検挙に向けた捜査を推進している。

※₁ 全国警察から派遣された捜査員により構成している。

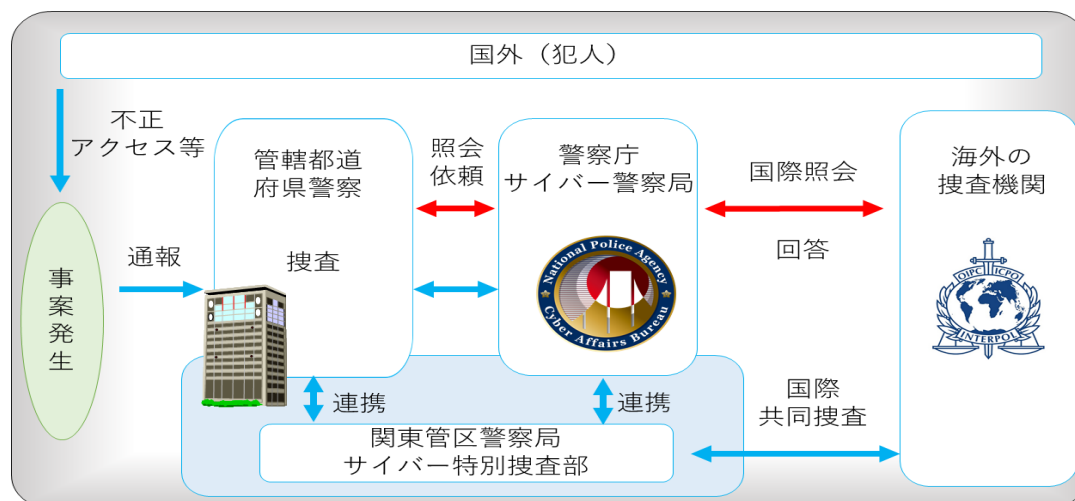
※₂ インターネットホットラインセンターの略称。

インターネット上の違法情報の通報を受け付け、警察庁への通報やプロバイダへの削除依頼等を行う民間団体で警察庁が業務委託している。



(2) 国境を越えたサイバー犯罪等に対する実態解明の推進

国境を越えて行われるサイバー犯罪等に対しては、警察庁サイバー警察局を通じて外国の捜査機関に国際照会を実施するとともに、国の捜査機関である「関東管区警察局サイバー特別捜査部」が都道府県警察と連携して共同で捜査を進め、その結果等を用いて外国捜査機関との情報交換、国際共同捜査等を推進している。



5 実態把握と部門間連携の推進

(1) サイバー犯罪相談窓口の運用

サイバー捜査課に相談専従員を配置し、県民から寄せられるインターネットに関するトラブル等の相談を受け付け、対処要領を教示するとともに、法令に触れる内容や新たな犯行手口等今後、被害が拡大するおそれのある相談については、警察署等と連携し積極的に対処することとしている。

警察庁や警察庁が委託する I H C に通報フォームが設置され、全国警察で対処していくための仕組みを確立している。

(2) 各種支援活動

サイバー犯罪等への対処は、サイバー捜査課のみならず警察署及び警察本部各部門が所掌に応じて担っているところ、それらが適切に行われるよう、サイバー捜査支援室を設置し、サイバー捜査課の人材及び捜査資機材を生かして警察署等に対する各種支援活動を行っている。

ア 初動支援

サイバー犯罪等への初動対応に際しては、証拠となるデータが時々刻々と失われるため迅速性が特に求められるところ、専門的な知識を有する捜査員を警察署に派遣し、初動対応を支援している。

例 通信ログの照会、精査等を行い、犯罪を敢行したアクセス元を特定

イ 技術支援

サイバー犯罪等に係る捜索現場に捜査員を派遣し、証拠となるデータ等の適切な保全・収集に当たるほか、押収したパソコンやスマートフォン等の電磁的記録の解析を行っている。

ウ その他の支援

インターネット上の犯行予告や自殺予告等の緊急対応が求められる事案について、犯人検挙による犯行の未然防止や自殺予告者の保護を目的に、通信事業者等に対する緊急での情報開示要請を 24 時間体制で実施している。

エ 分室の設置

広い県土を有する兵庫県の地理的な特性に鑑み、本部から遠方の警察署に対する捜査支援を行うため、姫路警察署及び尼崎南警察署に分室を設置し、各々、県北西部の警察署及び阪神地域の警察署に対する初動支援及び技術支援を実施しており、これにより、迅速な支援の展開、人的・物的リソースの有効活用が可能となっている。

6 官民連携の推進

(1) 「兵庫県サイバー犯罪対策ネットワーク」の取組

県内のサイバーセキュリティ対策の強化を図るため、専門的な知見を有する有識者・団体をオブザーバーとして、県下の金融機関、教育機関、自治体関係者等とネットワークを構築し、最新の手口の情報を共有するなど、産学官連携による被害防止対策を推進している。



【兵庫県サイバー犯罪対策ネットワーク】

ア ネットワークの拡充

企業を狙ったサイバー犯罪は、日々そのターゲットを変化させていることから、それらに適切に対処するため、ネットワーク会員の拡充を図っており、情勢に応じて、随時、新たにセキュリティ企業、団体の参画の働きかけを行っている。

イ 企業対象サイバーセキュリティセミナーの開催

企業のサイバーセキュリティ意識の高揚と対策の促進を図るため、商工会議所等と連携して、「サイバーセキュリティセミナー」を開催している。

令和5年度からは同セミナーの神戸会場を「サイバーセキュリティフォーラム」として位置付け、2月のサイバーセキュリティ月間に合わせ大規模に実施している。

(2) 民間企業との連携

県内企業等におけるサイバーセキュリティ対策の意識向上と対策の推進及び県警察のサイバー対処能力の強化を図るため、情報セキュリティ企業等と協定を締結し、連携した活動を推進している。



(3) 広報啓発活動の推進

ア サイバー犯罪被害防止教室の開催

サイバー企画課の附置機関である「サイバー情報発信室」に専任講師を配置し、児童や保護者など様々な世代を対象にインターネット上のトラブルやサイバー犯罪の事例及びその対策について啓発を行う「サイバー犯罪被害防止教室」を開催して、サイバー犯罪に係る被害防止意識を高めている。



【サイバー犯罪被害防止教室の開催状況】

年度別 対象別	令和2年度		令和3年度		令和4年度		令和5年度		令和6年度		令和6年度 6月末		令和7年度 6月末		前年同期比	
	回数	受講者数	回数	受講者数	回数	受講者数	回数	受講者数	回数	受講者数	回数	受講者数	回数	受講者数	回数	受講者数
小学校	78	8,528	62	9,117	933	15,213	122	18,496	133	21,346	34	5,966	31	5,955	-3	-11
中学校	25	3,835	20	4,793	43	11,034	59	17,777	51	15,774	20	7,750	14	4,357	-6	-3,393
高校	47	9,847	39	9,642	72	19,544	63	17,517	76	20,705	40	13,365	27	7,984	-13	-5,381
その他	48	1,823	43	2,478	115	91,91	141	8,634	155	10,727	46	4,299	47	5,242	+1	+943
計	198	24,033	164	26,030	323	51,982	385	62,424	415	68,552	140	31,380	119	23,538	-21	-7,842

※ 「その他」は、大学・専門学校・高齢者大学・教員・保護者・企業等の職員研修等
令和4年度までは「サイバー犯罪防犯センター」として実施した回数を計上。

イ SNS等を活用した取組

サイバーセンターの公式SNSアカウントや「サイバー情報発信室」の専用ウェブサイト、兵庫県サイバー犯罪対策ネットワークの会員に対する情報共有等において、被害防止のための注意事項や最新のサイバーセキュリティ情報等を発信しているほか、子どもがインターネットを安全に利用するためのポイントをまとめたサイバー防犯標語「あひるのおやこ」等を活用した広報啓発活動を行っている。



【サイバー情報発信室専用ホームページ】



【公式SNSアカウント】



ウ サイバー防犯ボランティアと連携した取組

インターネットに精通した個人（大学生、専門学生を含む。）等を「サイバー防犯ボランティア」として登録し、防犯情報の発信、街頭キャンペーン等による啓発活動、県民を対象とした講演等の活動を連携して行っている。

（令和7年6月末現在、219人が登録。）



【ボランティアの活動状況】

(4) 犯罪に関するインフラへの対処

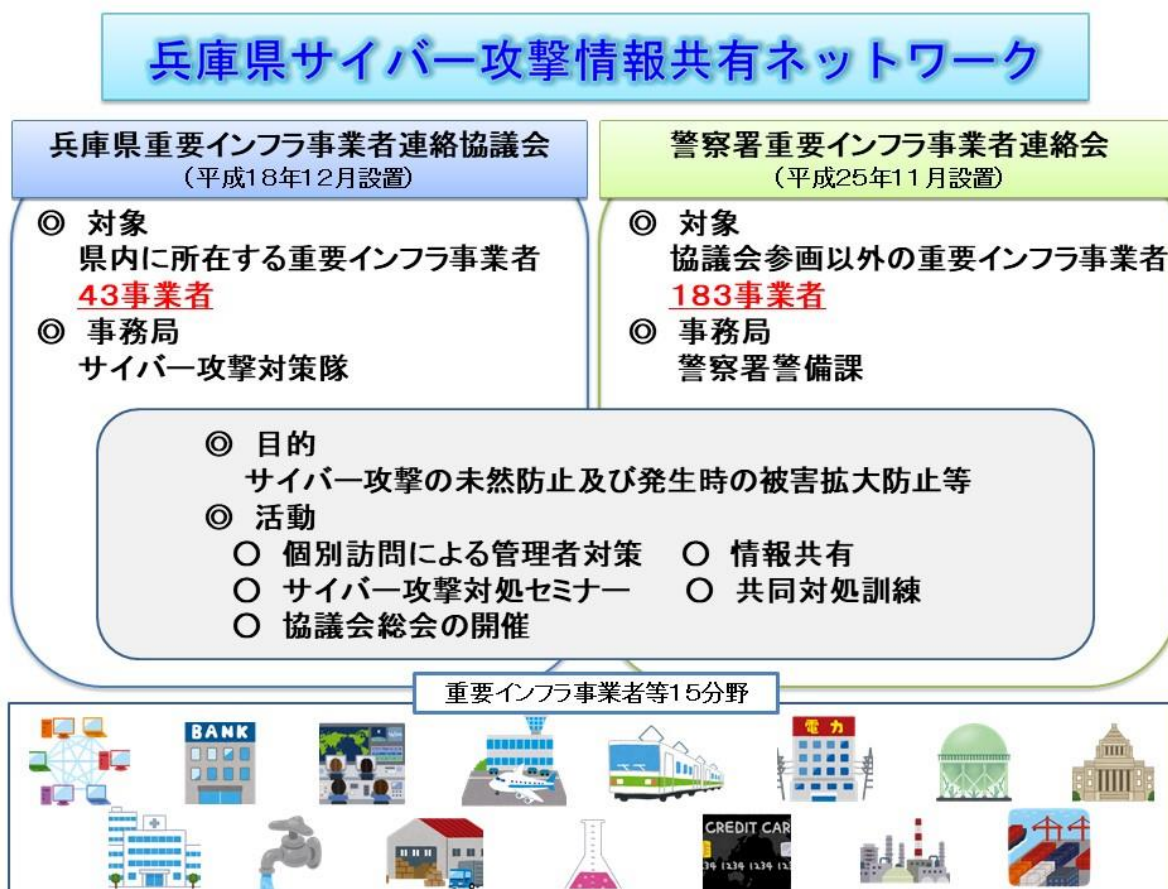
インターネットバンキングに係る不正送金対策、証券口座不正取引対策、フィッシングサイト対策、クレジットカード不正利用対策など、各業界団体・事業者に対し、警察庁及び都道府県警察が一体となって被害防止、拡大防止に向けて取り組んでいる。

7 サイバー攻撃対策

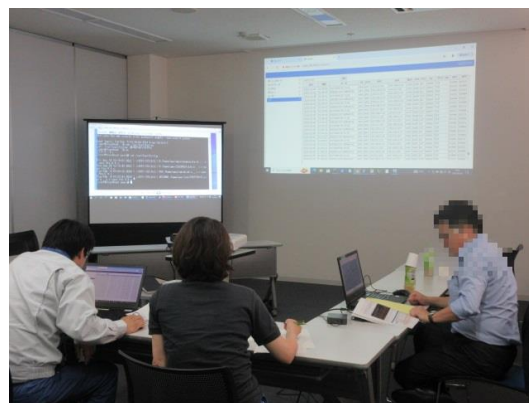
(1) サイバーテロ対策

官民でサイバー攻撃に関する情報を共有し、社会全体でサイバー攻撃に対処するための枠組みとして、「兵庫県サイバー攻撃情報共有ネットワーク」を構築している。

同ネットワークは「兵庫県重要インフラ事業者連絡協議会」と「警察署重要インフラ事業者連絡会」で構成され、個別訪問による管理者対策やサイバー攻撃対処セミナーの開催などを通じて連携を強化し、サイバー攻撃被害の未然防止等を図っている。



【サイバー攻撃対処セミナー】



【サイバー攻撃共同対処訓練】

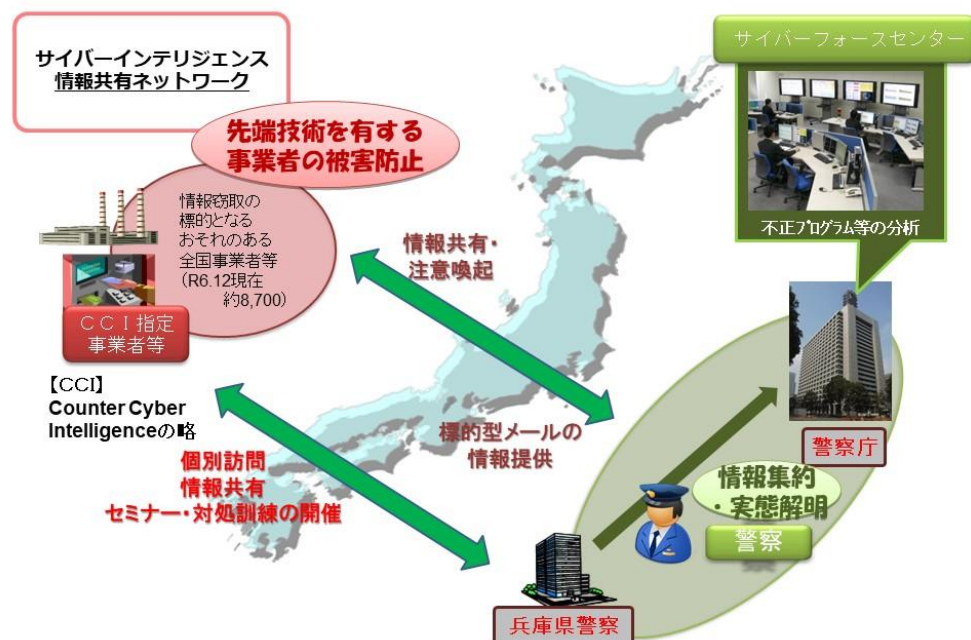
(2) サイバーエスピオナーズ対策

情報窃取の標的となるおそれの高い先端技術を有する全国約 8,700 の事業者等との間で、サイバー攻撃に関する情報共有を行う「サイバーインテリジェンス情報共有ネットワーク」を警察庁が構築しており、事業者等から提供された情報を集約するとともに、総合的に分析した結果に基づき注意喚起等を実施している。

県警察としては、個別訪問による管理者対策を実施するとともに、最新のサイバー攻撃情勢やソフトウェアのぜい弱性に関する情報を提供するなどして連携を強化し、サイバー攻撃の被害防止を図っている。

また、サイバー攻撃対処セミナーや共同対処訓練を開催して、事業者のサイバー攻撃に対する危機意識の醸成を図っている。

サイバーエスピオナーズ対策に係る警察の取組



(3) 実態解明の推進

県内の事業者に対するサイバー攻撃事案が発生した場合、当該事業者と連携し、被害状況の早期把握、証拠資料の保全、被害拡大、再発防止を図るほか、被疑者検挙に向けた捜査を行うこととしている。

また、サイバー攻撃を受けたコンピュータや不正プログラムを解析するなどして、攻撃者及び手口に関する実態解明を推進している。

攻撃の発信元等が海外のコンピュータであることが判明した場合には、警察庁を介して、国際刑事警察機構（ICPO）等を通じた国際捜査共助の要請を行っている。

解明した手口等は、「兵庫県サイバー攻撃情報共有ネットワーク」を通じて共有し、未然防止に役立てている。