集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
② 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。(21 条)

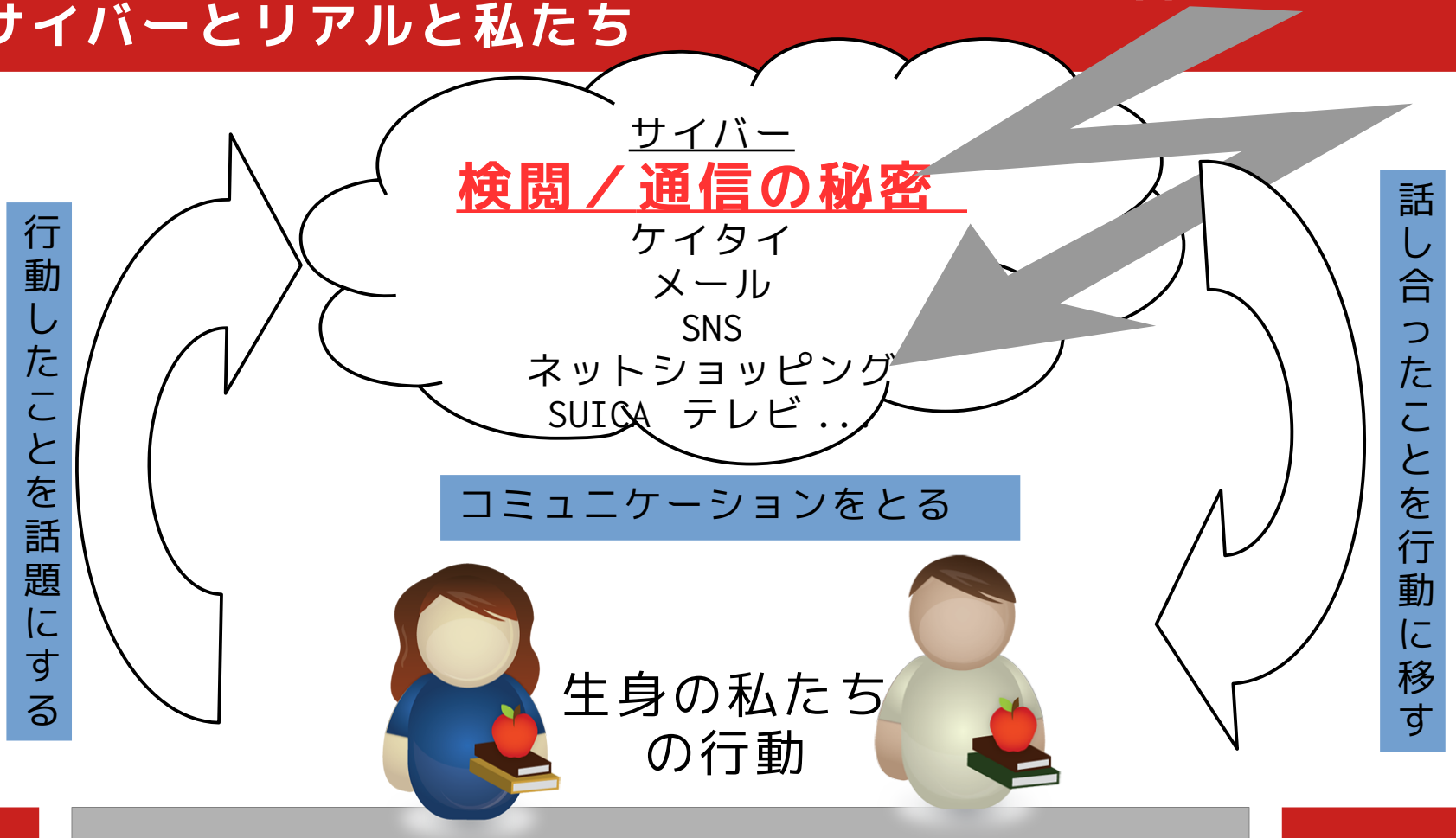
警察法改悪を許すとどうなるか？

小倉利丸 (JCA-NET)

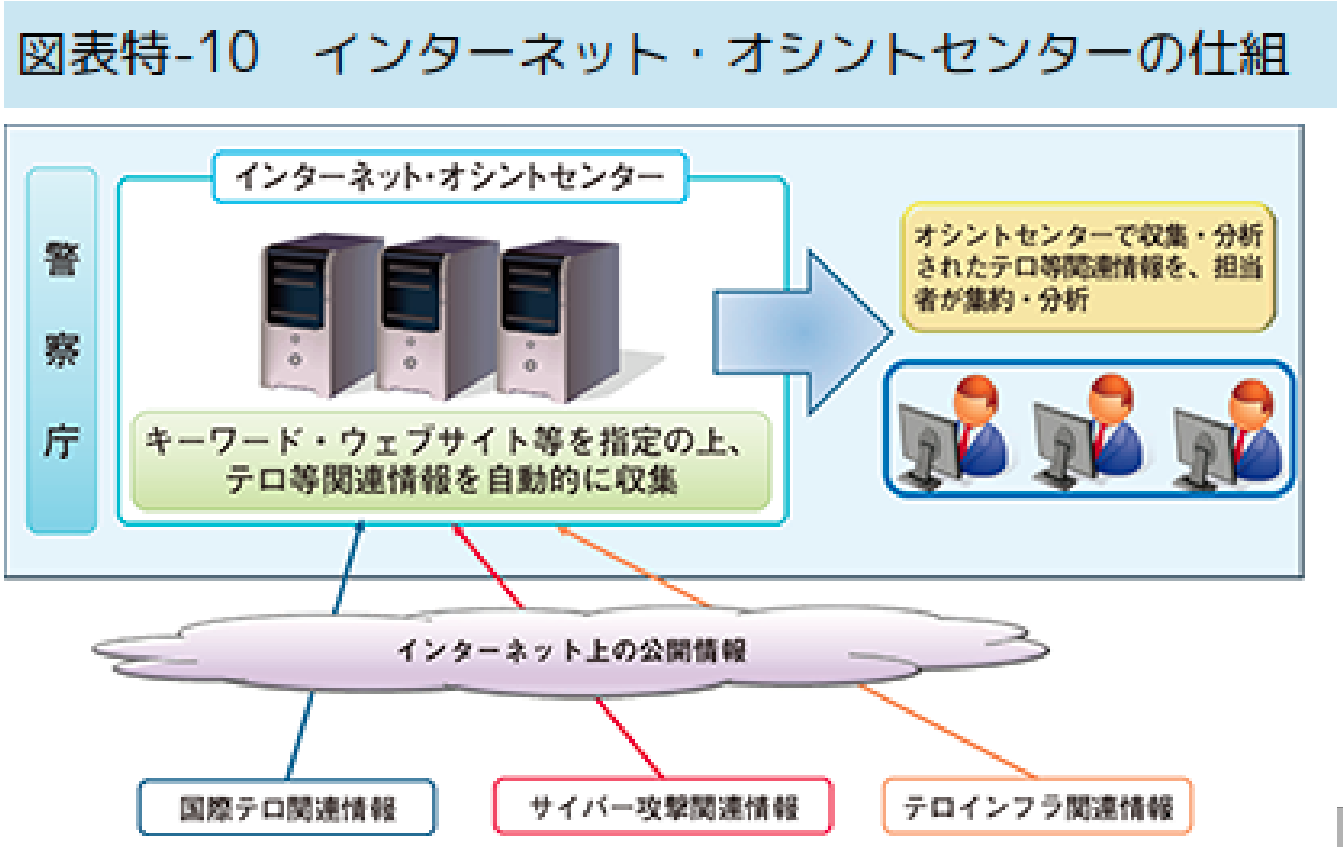
ネットにおける集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
② ネットの検閲は、これをしてはならない。ネットの通信の秘密は、これを侵してはならない。

サイバーとリアルと私たち

サイバー警察局はここを狙う



警察がすでにやっていること



「インターネット上の情報収集・分析の重要性がこれまで以上に増しているところ、インターネット上に公開されたテロ等関連情報の収集・分析を強化するために、平成 28 年 4 月、警察庁警備局に「インターネット・オシントセンター」を設置した。」（2016 警察白書）

情報通信局　情報技術解析課と警備局が連携

集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
② 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。（21 条）

警察法改悪を許すとどうなるか？

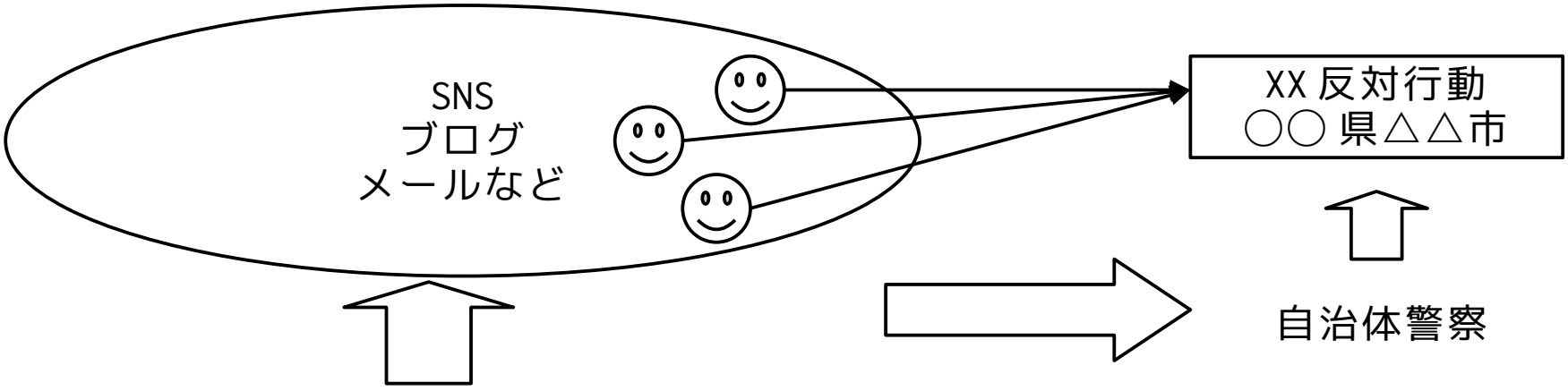
小倉利丸（JCA-NET）

ネットにおける集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
② ネットの検閲は、これをしてはならない。ネットの通信の秘密は、これを侵してはならない。

- **盗聴法、共謀罪（話し合いの犯罪化）**
- **マイナンバーと官民情報共有**
- **ビッグデータ＋ＡＩ＋５Ｇ**

サイバーとリアル

- **必ず捜査はリアルな現場と繋がる**
- **人々のコミュニケーションと現実の行動の両面を統合的に監視**



- 全国各地から集まった抗議参加者を追跡して動静を把握し情報蓄積。
- ネットとリアル両面でのハイブリッド捜査が可能になる。
- 人々の権利としての異議申立てを事前・事後にわたり監視し予防することに

警察法改悪のポイント

サイバーとリアルは切り離せない . . . あなた自身とあなたのスマホが切り離せないように . . .

■ 憲法で保障されている通信の秘密、表現の自由、思想信条の自由の領域を専門に捜査する機関の創設

■ 地方自治を否定し、中央政府の権限強化

警察法改悪のポイント

■ 憲法で保障されている通信の秘密、表現の自由、思想信条の自由の領域を専門に捜査する機関の創設

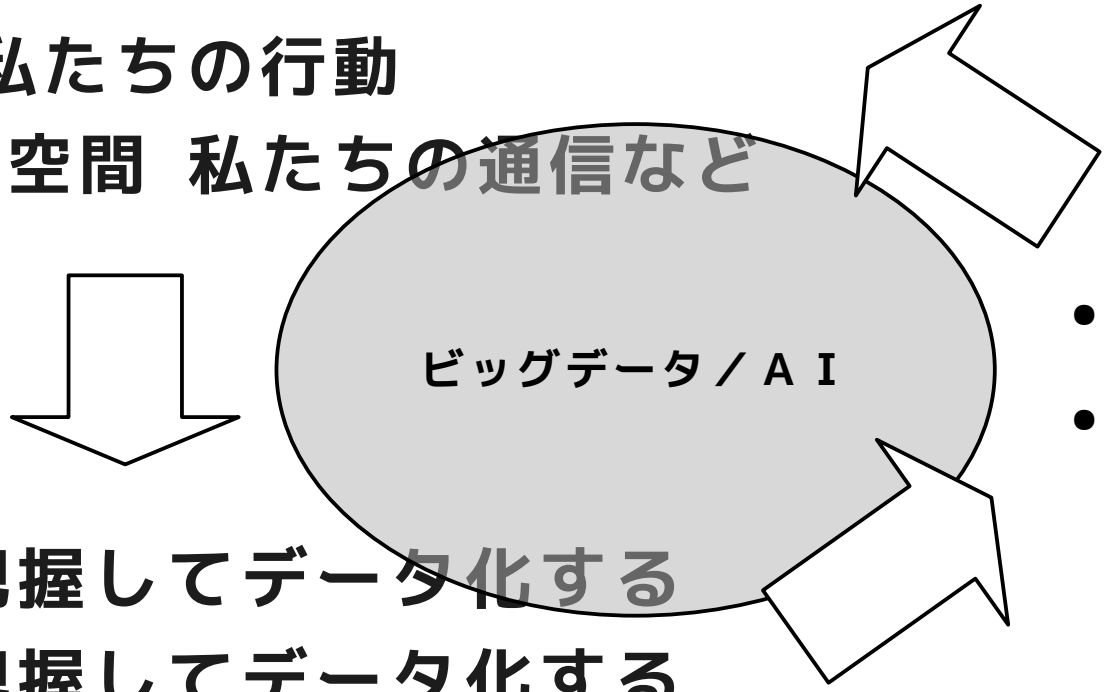
■ 地方自治を否定し、中央政府の権限強化

――――――――警察法改悪が目指しているのは――――――――

- 通信局の解体
- 警察庁長官官房に情報機能を統合
- サイバー警察局の新設
- 関東管区警察局を事実上の全国対象の国家警察に格上げ

サイバーとリアルと私たち

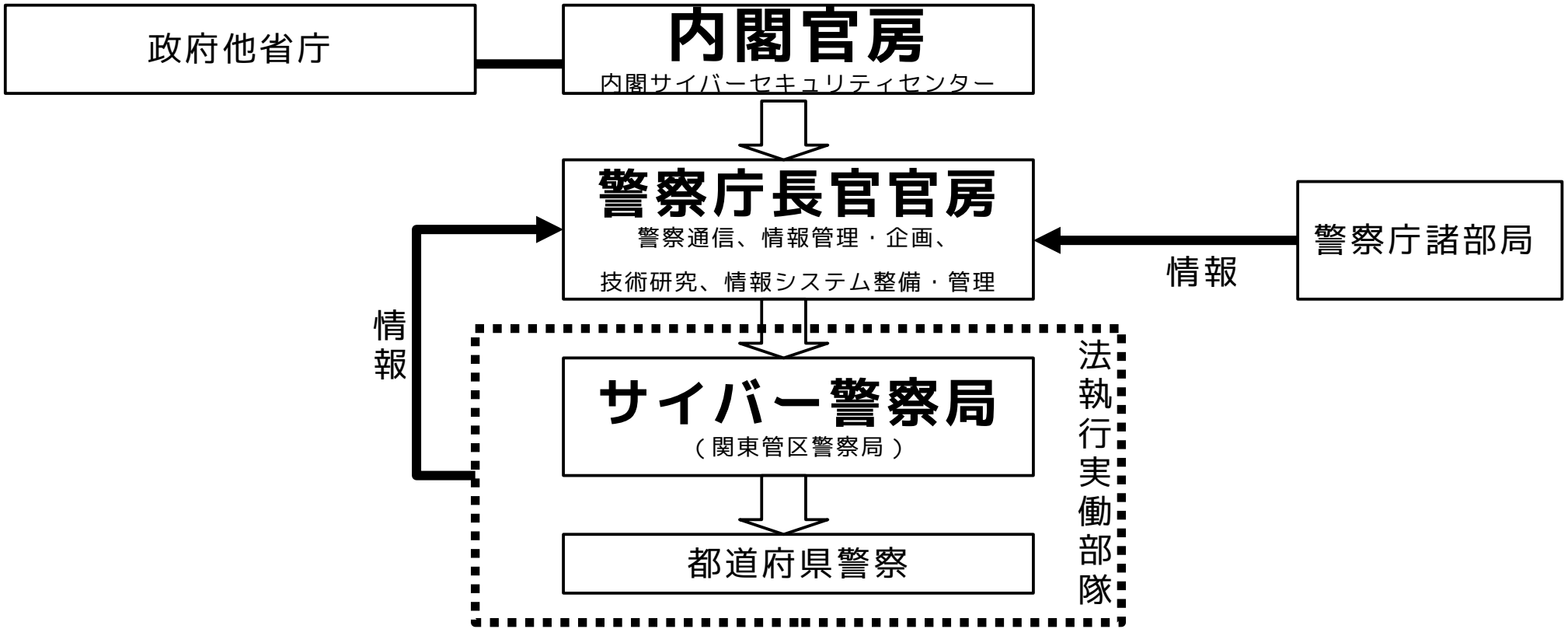
- 実空間　私たちの行動
- サイバー空間　私たちの通信など



- 行動の予測
- 行動変容を促す

- 行動を把握してデータ化する
- 通信を把握してデータ化する

警察法改正後：情報システムの観点から



自民党改憲草案の制度的先取り

「改憲草案」

「第　21　条（表現の自由）

1　集会、結社及び言論、出版その他一切の表現の自由は、保障する。

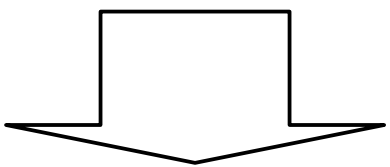
2　前項の規定にかかわらず、公益及び公の秩序を害することを目的とした活動を行い、並びにそれを目的として結社をすることは、認められない。

3　検閲は、してはならない。通信の秘密は、侵してはならない。」

サイバー空間を「国益」に従属させ、反政府活動を違憲にする意図がある

警察や政府だけでは不可能なことがある

- プロバイダーの個人情報
- 民間が保有する個人情報
- 民間 IT 企業の技術や特許
- 「検閲」ができない
- 通信の秘密を侵害できない



官民一体となった取り組みが不可欠

民間 IT 企業による警察機能の肩代わり（資本の政治権力化）

警察法改悪は、中央集権型の警察組織構築だが、戦前型の国家警察への回帰ではないことに注目する必要がある

- **民間 IT 企業が警察などの監視技術インフラを提供している**
- **民間企業が公権力の一部を担うことが前提となった法改正である**
  - 私たちが契約しているプロバイダー
  - 私たちが利用する端末 (Google 、 Apple)
  - ネットショッピングサイト
  - SNS を提供する企業 (Line 、 Facebook など)

通信局の解体

サイバーフォース

- インターネット 24 時間監視
- 警備部門、生活安全部門と連携
- 重要インフラ事業者への情報提供、共同訓練、官民連携
- サイバー攻撃事案では、都道府県警察と連携して被害防止と証拠保全の技術対応

警察庁サイバー局に組み込まれる？
指示から直接捜査に関与？
より国益重視になるだろう

通信局の解体

情報通信局

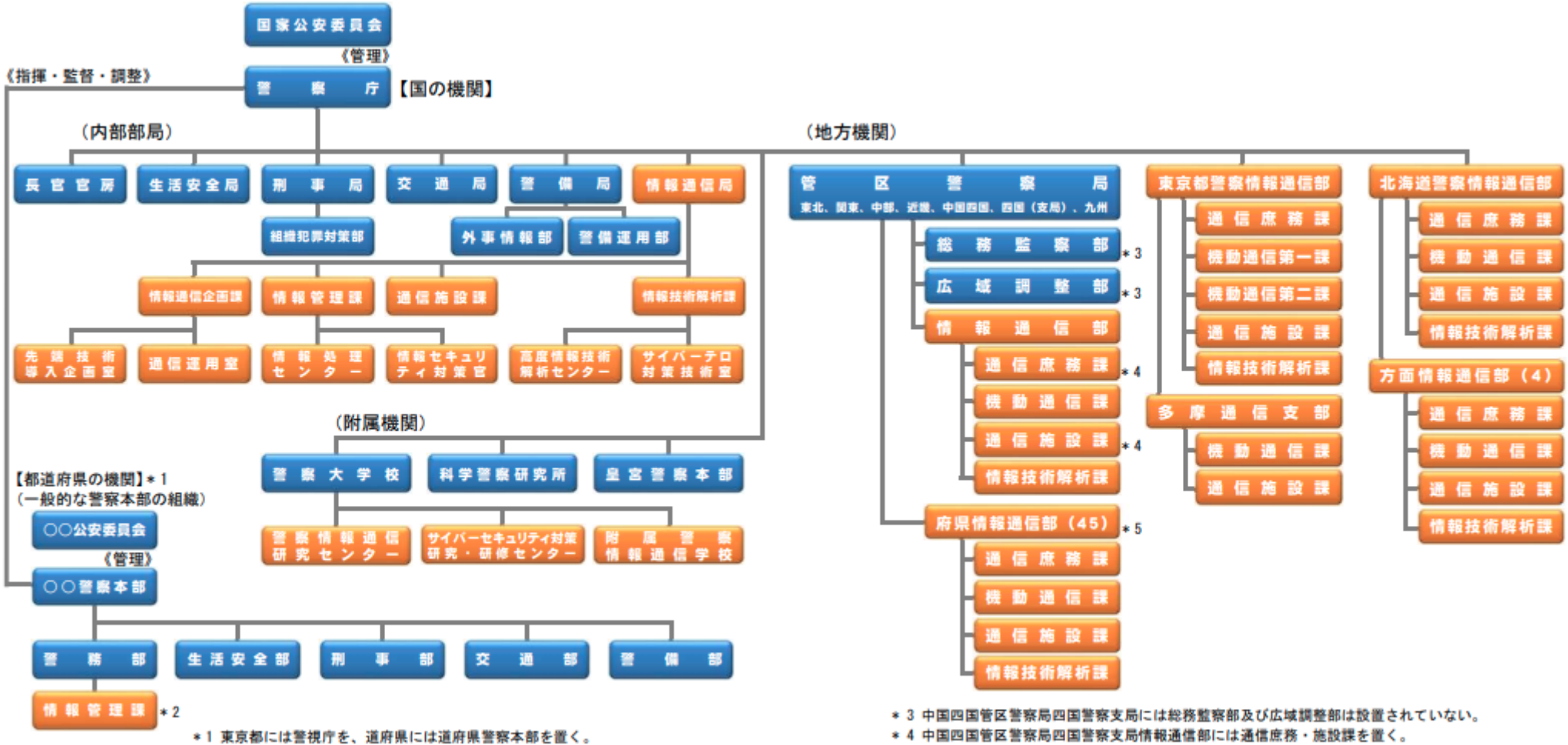
- **「警察通信」** 無線多重回線、電気通信事業者の専用回線等により構成される警察基幹通信網を整備。現場映像等を撮影し、警察本部等に伝送
- **「情報管理」** 都道府県警察が保有する情報を全国的に共有できるようにするため、警察庁のデータベースを整備
- **「情報技術解析」** 電子機器に関する警察活動に技術的な面から支援
- **海外**の関係機関との連携・協力

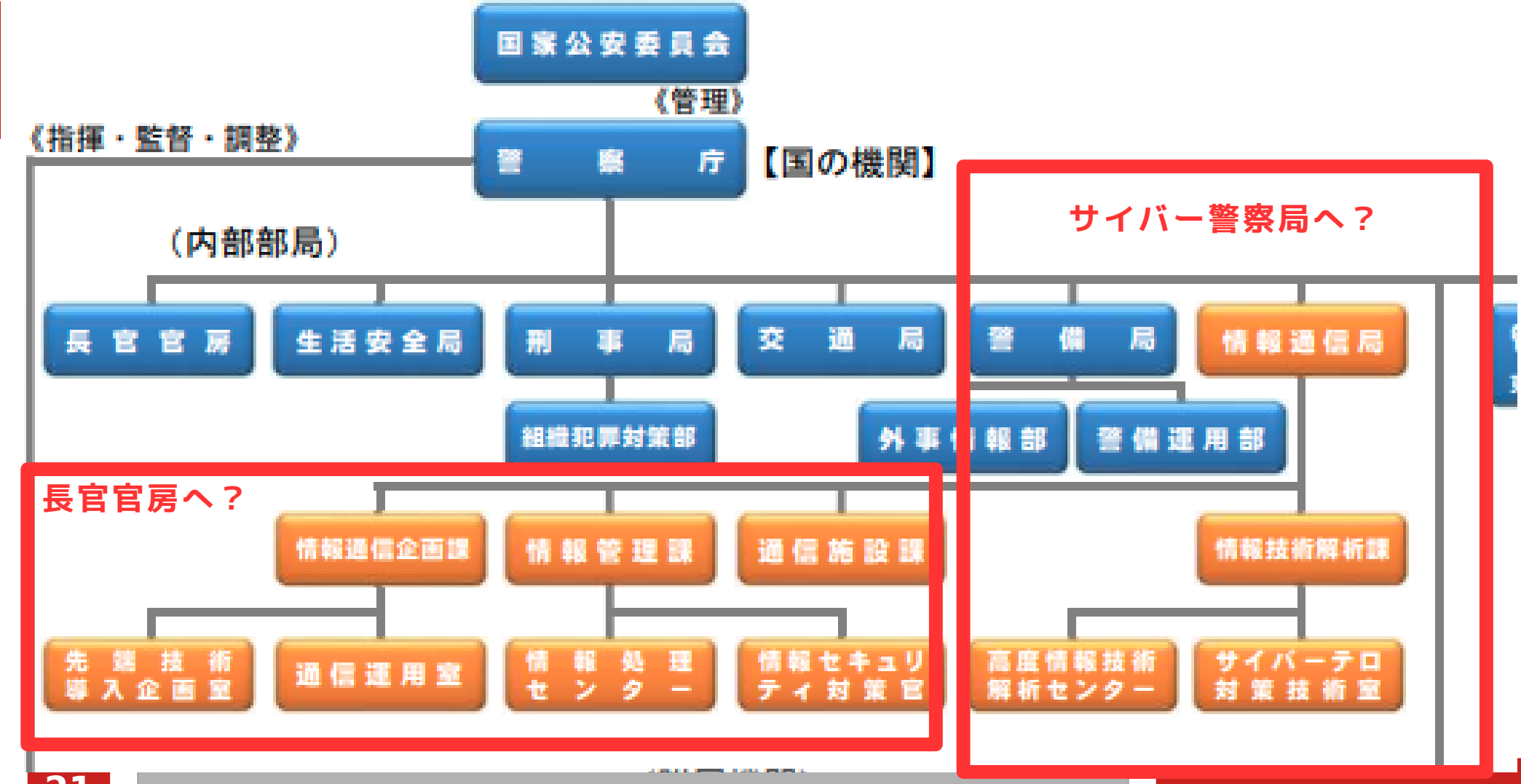
長官官房

- 警察通信に関すること
- 情報管理、企画、技術研究
- 情報システムの整備、管理

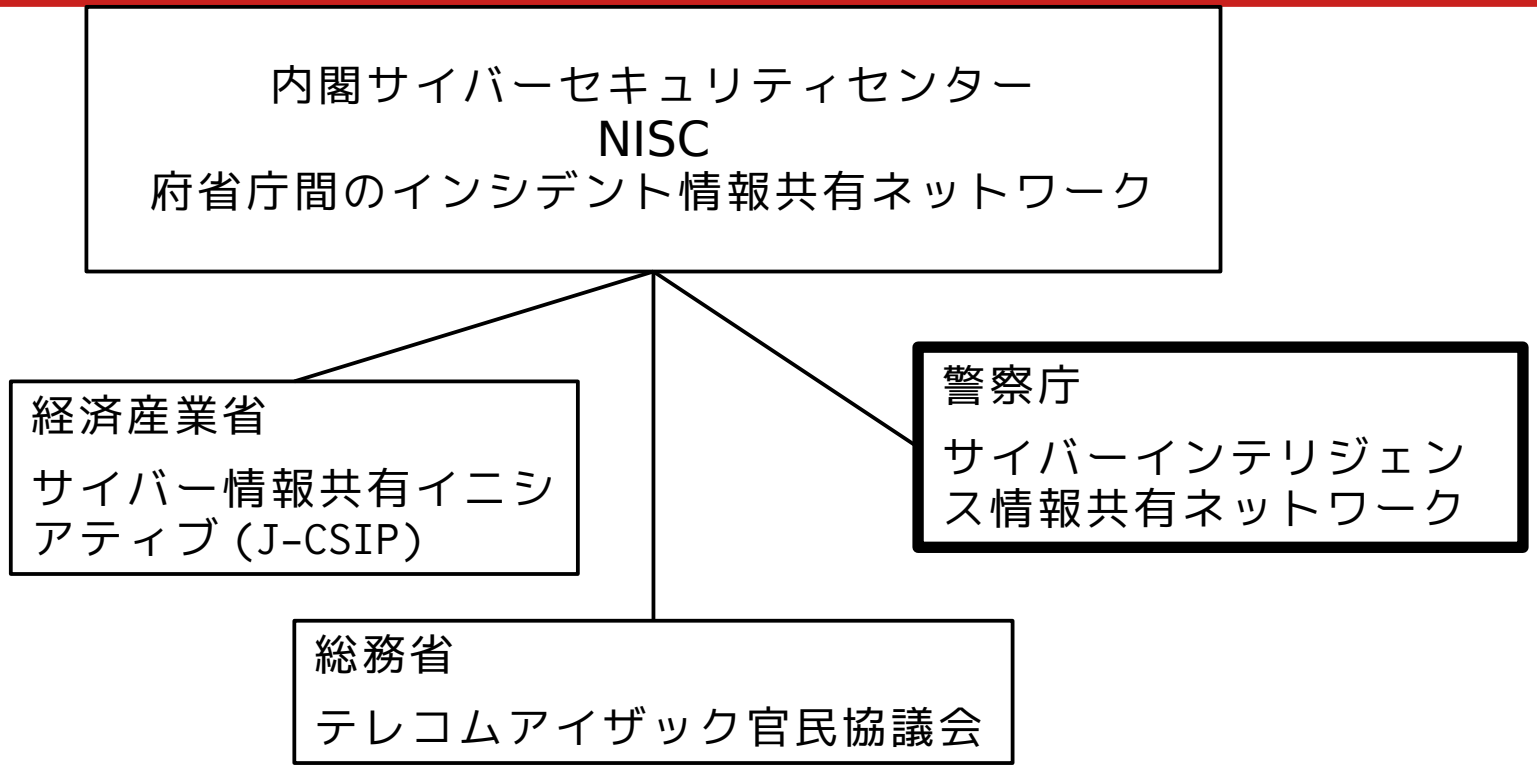
サイバー警察局

- 犯罪取り締りのための情報解析


国家公安委員会
《管理》
《指揮・監督・調整》
警察庁
【国の機関】
（内部部局）
長官官房
生活安全局
刑事局
交通局
警備局
情報通信局
組織犯罪対策部
外事情報部
警備運用部
情報通信企画課
情報管理課
通信施設課
情報技術解析課
先端技術導入企画室
通信運用室
情報処理センター
情報セキュリティ対策官
高度情報技術解析センター
サイバーテロ対策技術室
（附属機関）
警察大学校
科学警察研究所
皇宮警察本部
警察情報通信研究センター
サイバーセキュリティ対策研究・研修センター
附属警察情報通信学校
【都道府県の機関】＊1
（一般的な警察本部の組織）
○○公安委員会
《管理》
○○警察本部
警務部
生活安全部
刑事部
交通部
警備部
情報管理課
＊2
＊1 東京都には警視庁を、道府県には道府県警察本部を置く。
＊2 総務部（室）のある警察本部においては、総務部（室）に情報管理課を置く。
（地方機関）
管区警察局
東北、関東、中部、近畿、中国四国、四国（支局）、九州
総務監察部
＊3
広域調整部
＊3
情報通信部
通信庶務課
＊4
機動通信課
通信施設課
＊4
情報技術解析課
府県情報通信部（45）
＊5
通信庶務課
機動通信課
通信施設課
情報技術解析課
東京都警察情報通信部
通信庶務課
機動通信第一課
機動通信第二課
通信施設課
情報技術解析課
多摩通信支部
機動通信課
通信施設課
北海道警察情報通信部
通信庶務課
機動通信課
通信施設課
情報技術解析課
方面情報通信部（4）
通信庶務課
機動通信課
通信施設課
情報技術解析課
＊3 中国四国管区警察局四国警察支局には総務監察部及び広域調整部は設置されていない。
＊4 中国四国管区警察局四国警察支局情報通信部には通信庶務・施設課を置く。
＊5 府県情報通信部の数の内訳は、東北６、関東10、中部６、近畿６、中国四国９、九州８である。


国家公安委員会
《管理》
《指揮・監督・調整》
警　察　庁
【国の機関】
（内部部局）
長官官房
生活安全局
刑事局
交通局
警備局
情報通信局
組織犯罪対策部
外事情報部
警備運用部
長官官房へ？
情報通信企画課
情報管理課
通信施設課
先端技術導入企画室
通信運用室
情報処理センター
情報セキュリティ対策官
サイバー警察局へ？
情報技術解析課
高度情報技術解析センター
サイバーテロ対策技術室

政府内部の情報共有



警察では、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 7,520 の事業者等（平成 29 年 1 月現在）との間で、情報窃取を企図したとみられる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構築しており、このネットワークを通じて事業者等から提供された情報を集約するとともに、これらの事業者等から提供された情報及びその他の情報を総合的に分析し、事業者等に対し、分析結果に基づく注意喚起を行っている。

重要インフラの情報セキュリティ対策に係る第４次行動計画

官民連携による重要インフラ防護の推進

重要インフラにおいて、機能保証の考え方を踏まえ、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

重要インフラ(全14分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

NISCによる調整・連携

重要インフラ所管省庁

- 金融庁　［金融］
- 総務省　［情報通信、行政］
- 厚生労働省［医療、水道］
- 経済産業省［電力、ガス、化学、クレジット、石油］
- 国土交通省［航空、空港、鉄道、物流］

関係機関等

- 情報セキュリティ関係省庁　［総務省、経済産業省等］
- 事案対処省庁　［警察庁、防衛省等］
- 防災関係府省庁　［内閣府、各省庁等］
- 情報セキュリティ関係機関　［NICT、IPA、JPCERT等］
- サイバー空間関連事業者　［各種ベンダー等］

「重要インフラの情報セキュリティ対策に係る第４次行動計画」

安全基準等の整備・浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化

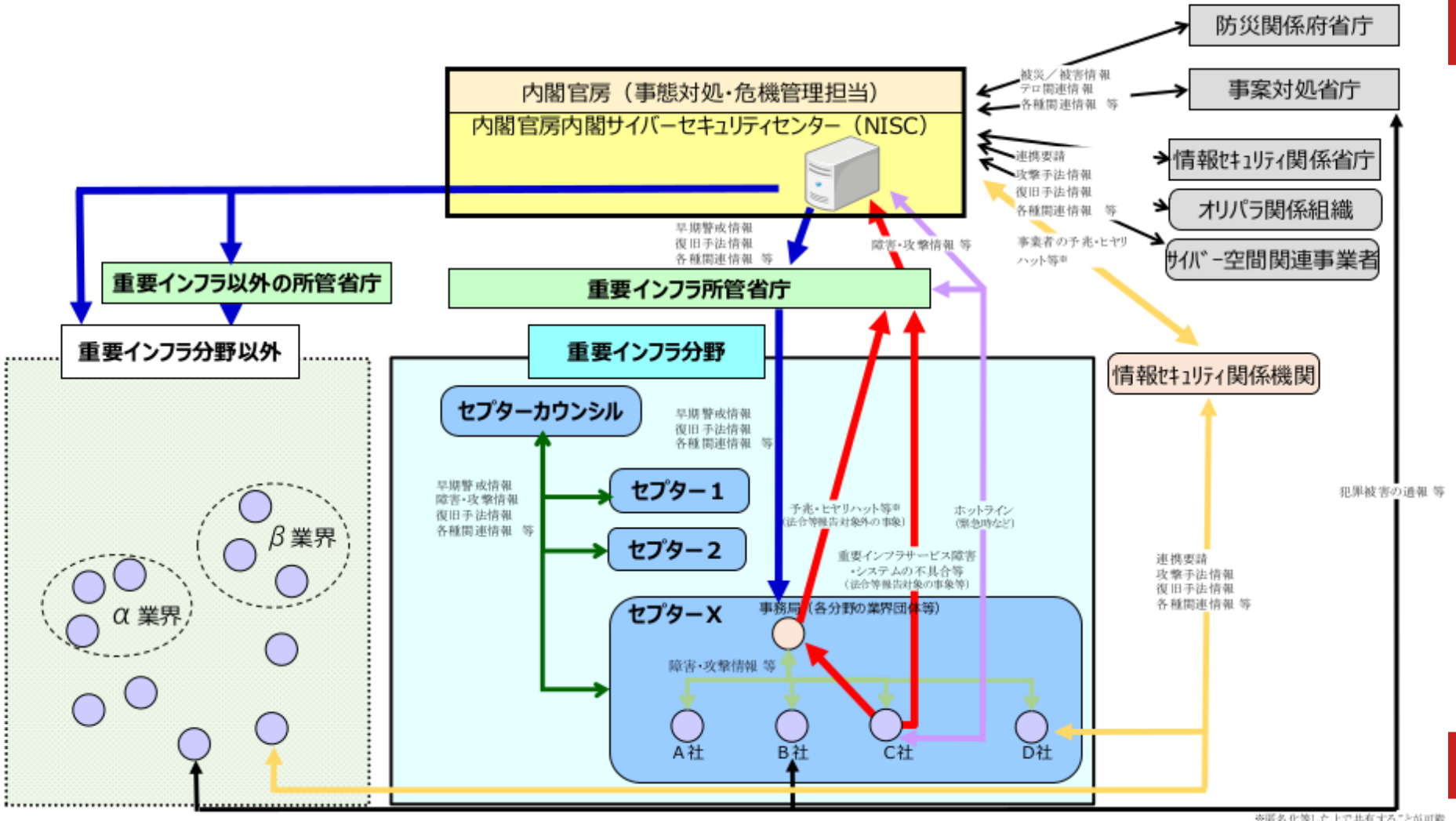
リスクマネジメント及び対処態勢の整備

リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

第４次行動計画における情報共有体制



反対声明の骨子：通信の秘密、民主主義の基盤そのものへの脅威

(1) 言論・表現を専門に取り締る警察組織の新設。

- 電子メール、 SNS などによるコミュニケーションの領域に特化した捜査機関
- 憲法や電気通信事業法などで「通信の秘密」が保障されている領域
- コミュニケーションの自由は、言論、表現の自由、思想信条や信教の自由の必須条件
- 民主主義の基盤をなすもの
- 一般の市民だけでなく報道機関、選挙など政治活動の場、医療関係者や弁護士など人権に関わって活動する人々の基盤をなす

サイバー警察局は、高度な技術力を駆使して、こうした活動そのものを犯罪の疑いの目をもって捜査対象に据えることになります。

反対声明の骨子：自治体警察の骨抜きと警察の中央集権化

(2) 都道府県の警察の枠組を超えて警察庁が捜査権限を持つことが可能な組織再編。

- 警察庁みずからが各都道府県の警察の枠組を超えた捜査権限をもつ
- 各都道府県警察の権限は大幅に後退する
- 将来、更に「サイバー」以外の分野での警察の中央集権化への道筋をつけるもの
- 警察庁長官官房が、情報技術に関連する広範囲にわたる権限を持つ
- 技術が重要な役割を果す「サイバー」領域に関しては、民主主義的な検証が行なえず、警察が思いのままに網羅的な監視技術を拡大させうるものになる

戦前の国家警察の反省から生まれた自治体警察の枠組は、事実上骨抜きにされる

反対声明の骨子：膨大な警察保有データとサイバー特高警察の到来

- 警察保有情報 写真約 1170 万件、指紋 1135 万件、ＤＮＡ型 141 万件など膨大に
- 2021 年上半期、 Line だけで 1,421 件の情報開示
- 捜査機関の民間通信事業者への問い合わせ件数も膨大な数
- 人々のコミュニケーションがインターネットのメールや SNS を中心に
- ビッグデータと呼ばれる膨大な個人情報収集の仕組みが普及
- AI 解析で人々の行動や考え方に影響を及ぼすことができる時代

サイバー警察局は、私たちの日常的なコミュニケーションを常時監視・分析し、
取り締る言論警察、思想警察あるいはサイバー特高警察になりうる危惧

以上から、私たちは、警察法の一部を改正する法律案に強く反対します。

警察庁「概要」から改正案の問題点を指摘します(左が「概要」)

警察法の一部を改正する法律案（概要）

1　背景

◆ サイバー空間は誰もが参加する公共空間に

◆ 世界中から直接攻撃を受ける

◆ コロナ禍はサイバー空間の脅威を増進

- ➢高度な専門技術を有する集団による執ようなサイバー攻撃
- ➢攻撃手法が常時拡散・高度化
- ➢サイバー対策における国際連携の重要性

サイバー空間は「通信の秘密」によって保護された空間であり、民主主義の基本をなす言論空間であること

事態をかなり誇張。「攻撃」はあるが、現状でも十分セキュリティを確保できているから、多くの人々が日常的に利用可能になっている。

この三つの項目は「コロナ」とは無関係。コロナ対策ということで批判をかわす心理作戦にすぎない。

「国際連携」として警察庁が意図しているのは、暗号技術の規制などプライバシー侵害技術を通信事業者や捜査機関に導入させようとするもの。各国の捜査機関が同調して暗号規制強化を推進している。

2　改正の概要

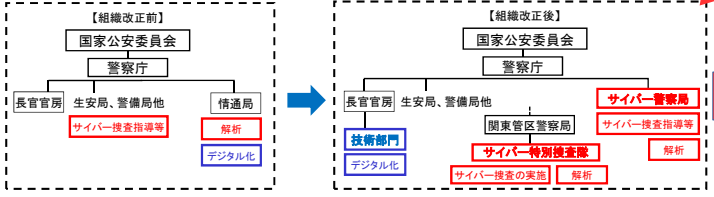
①　警察庁の組織改正

◆ サイバー警察局の新設

- ・ 捜査指導、解析、情報集約・分析、対策等を一元的に所掌

◆ 情報通信局の所掌事務を長官官房に移管

- ・ 警察業務のデジタル化、科学技術の活用等を推進



ビッグデータ化とAIによる「犯罪」予測など行政警察型の捜査が警察組織全体で採用される。自治体警察の理念と反する「一元的」な管理

長官官房に「技術部門」を設置して「技術」の秘匿性を高めている。

情報を 一手に握る官房が全ての部局の上に立つことになるから、「長官官房」が諸部局よりも上位の位置を占めるはず。

②　重大サイバー事案に対する対処能力の強化

◆ 国家公安委員会・警察庁が重大サイバー事案に対処するための事務を所掌

◆ 重大サイバー事案に対処するための事務を関東管区警察局が分掌（全国管轄）

- ・ サイバー特別捜査隊※が全国を管轄とし、重大サイバー事案の捜査（国際共同捜査を含む）を実施

（※ サイバー特別捜査隊の関東管区警察局への設置は下位法令事項）

【重大サイバー事案】

① 国・地方公共団体の機関や重要インフラ等に重大な支障が生じる事案

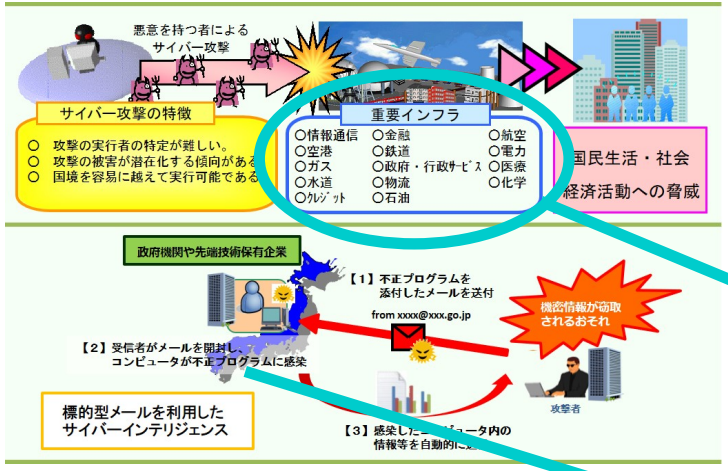
② 対処に高度な技術を要する事案（マルウェア事案等）

③ 海外からのサイバー攻撃集団による攻撃

警察が用いる技術の仕様そのものを国会など第三者が検証できる仕組みがなく、歯止めがない。この歯止めがない限り、警察に高度な技術を使わせるべきではない

情報関連のシステムを長官官房とサイバー警察局が事実上掌握することになるので、自治体警察の独立性はほとんど不可能になる。

「重大サイバー事案」の定義はない。事実上「サイバー事案」と同じと考えていいだろう。「重大」という文言は法案を通すためのレトリック



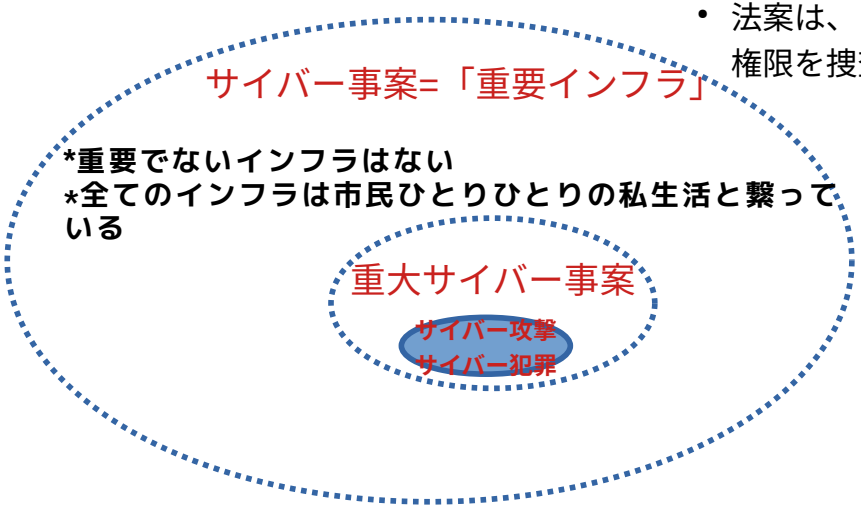
上図：https://www.npa.go.jp/joutuu/i/012-01-600.jpg

サイバー攻撃について

左図は警察庁が作成したサイバー攻撃についての概念図である。

法案は通信の秘密を侵害する違憲立法であり、電気通信事業法にも違反する

- すべての情報通信ネットワークには、「インフラ」を通じて市民ひとりひとりのプライベートな通信やコミュニケーションが繋がっている。
- 「サイバー攻撃」を防ぐ最前線にいるのは、サーバーの管理者であり市民ひとりひとりである。
- 不正プログラムを網羅的に発見するためには捜査機関が全ての人々のメールやSNS等の内容を 把握しなければならない。
- 法案は、こうしたネットワーク全体を網羅的に監視する権限を捜査機関に与えようとしている。



捜査機関の助けをかりなくても不正プログラムを発見する方法は既に存在している。

スノーデンの告発にあるように、捜査機関による網羅的なネット監視は、市民的自由を侵害し、人権とプライバシーを侵害する性格へと変質する危険性が大きい。

この仕組みは、必然的に通信の秘密を侵害することになる。

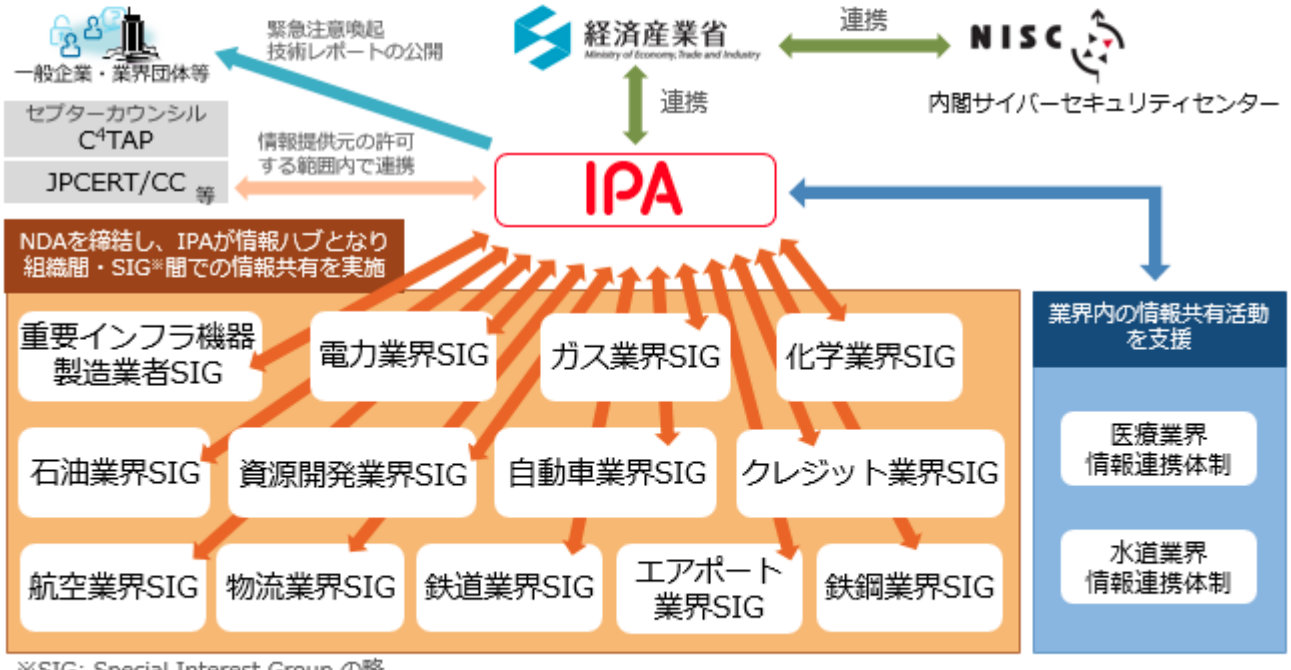
2022/2/22 2.6実行委 https://www.jca.apc.org/no-cyberpolice/

J-CSIP

Initiative for Cyber Security Information sharing Partnership of Japan

J-CSIPは、公的機関であるIPAを情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取り組みです。

具体的には、IPAと各参加組織（あるいは参加組織を束ねる業界団体）間での秘密保持契約（NDA）の締結等により、参加組織およびそのグループ企業において検知されたサイバー攻撃等の情報をIPAに集約。情報提供元に関する情報や機微情報の匿名化を行い、IPAによる分析情報を付加した上で、情報提供元の承認を得て共有可能な情報とし、参加組織間での情報共有を行っています。



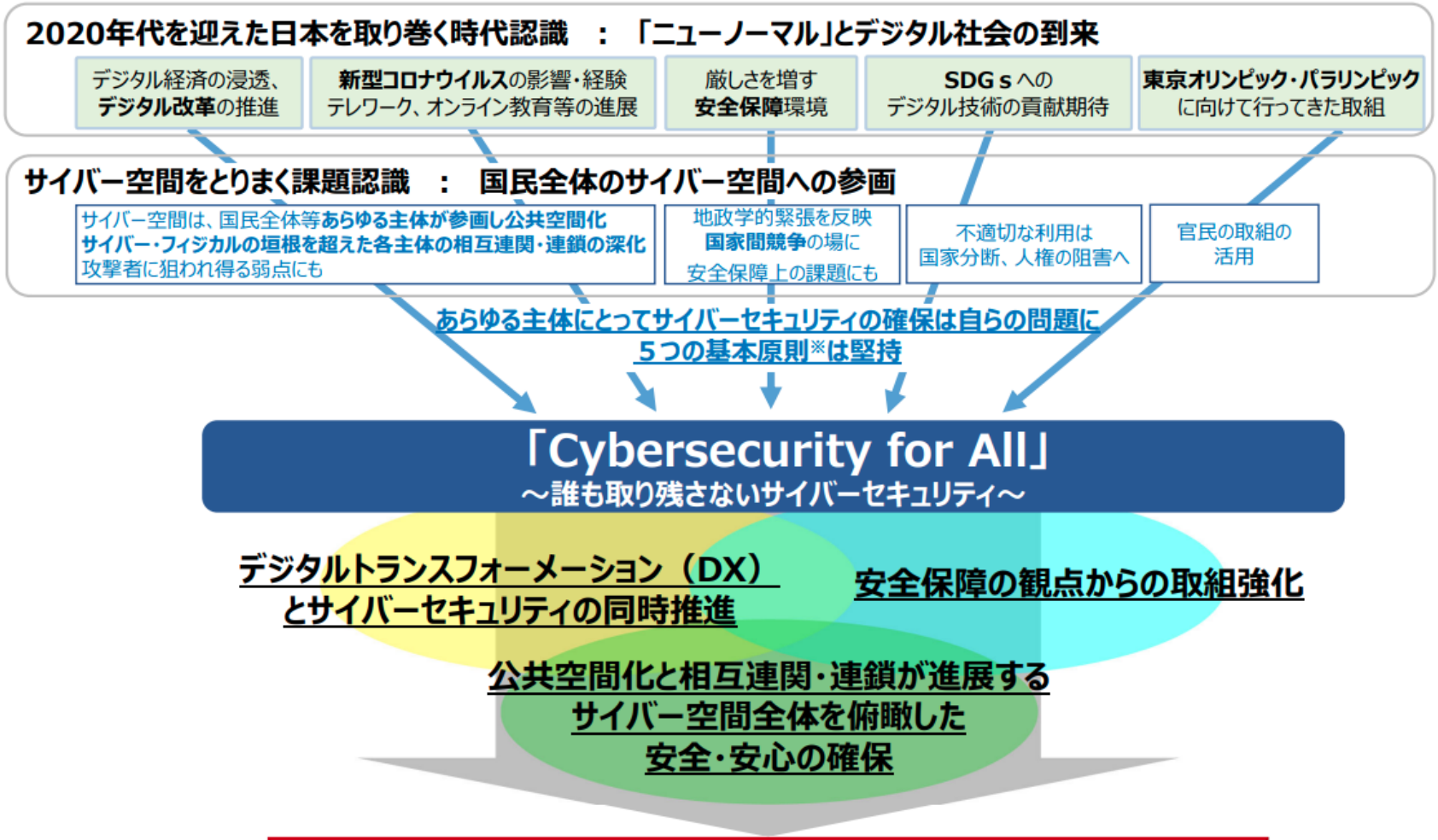
※SIG: Special Interest Group の略

https://www.ipa.go.jp/security/J-CSIP/index.html

IPA は、サイバー攻撃による被害拡大防止のため、 2011 年 10 月 25 日、経済産業省の協力のもと、重工、重電等、重要インフラで利用される機器の製造業者を中心に、情報共有と早期対応の場として、サイバー情報共有イニシアティブ（ J-CSIP ： Initiative for Cyber Security Information sharing Partnership of Japan ）を発足させました。その後、全体で 13 の SIG （ Special Interest Group 、類似の産業分野同士が集まったグループ）、 262 の参加組織による情報共有体制と、 IPA が特定業界内の情報共有活動を支援する 2 つの「情報連携体制」をそれぞれ確立し、現在、サイバー攻撃に関する情報共有の実運用を行っています。

次期サイバーセキュリティ戦略の課題と方向性

資料１－１



※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

「サイバー事案」の具体的なターゲットは何？

- 国内の課題
- 外国捜査機関との連携

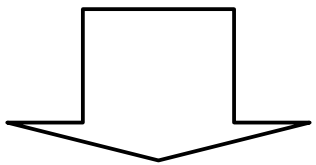
国内の課題

- ネット犯罪（詐欺、恐喝、著作権侵害、ポルノ、違法商品販売 ...）
- ビッグデータ、 AI に対応した情報技術高度化（全省庁共通）
- 自治体の再編・統合と中央政府への権力集中（全省庁共通）
- 国家安全保障（経済安全保障）への対応（ICT 産業への監視）
- 国家安全保障に私生活を包含するシステム構築（マイナンバー、プロバイダーやプラットフォーム企業との連携）

「サイバー事案」の具体的なターゲットは何？

国際連携を念頭に置くと

- テロ・サイバー戦争対策：国連サイバー犯罪条約が検討に
- 子どもの性的搾取関連：各国がネット監視強化の立法化へ



市民運動、社会運動にとって治安弾圧の手段としての国家警察への反対は合意がとりやすいが、ネットが関わる子どもの性的搾取への対策を持ち出されると反対の声が分断されかねない。

政府のサイバーセキュリティ全体の構図

サイバー犯罪対策等の強化

サイバー空間の公共空間化を踏まえ、サイバーセキュリティ戦略（令和３年９月28日閣議決定）では、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おり、警察は、警察庁にサイバー事案に係る政策を一元的に担うサイバー警察局（仮称）と国の捜査部隊としてのサイバー特別捜査隊（仮称）を創設し、地域に密着した活動を展開する都道府県警察と合わせて警察全体としてセキュリティ確保に向けた取組を推進することとしている。

内閣官房は、警察庁と連携し、警察による重要インフラ事業者等との協力等の必要な取組を支援し、重要インフラ事業者等を取り巻くサイバー空間の安全性・信頼性の確保を図る。（重要インフラのサイバーセキュリティに係る行動計画案。2022）

警察組織内にサイバー部門の司令塔を担う

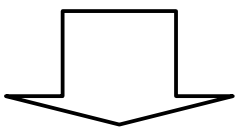
機能と、専門の実働部隊を創設することを検討するなど、対処能力の強化を図る。

「サイバー攻撃」

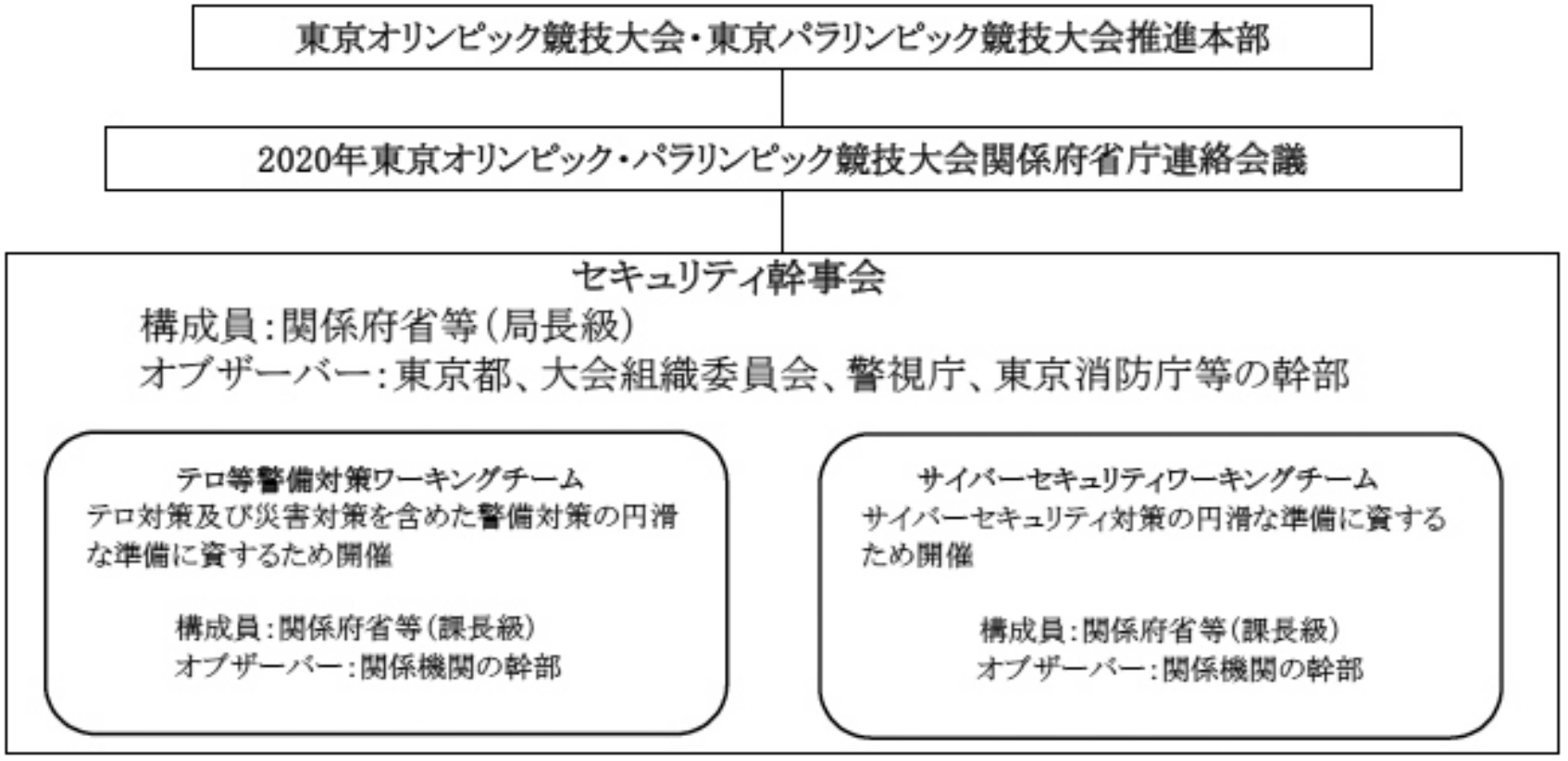
例えばウクライナで今起きている戦争の場合

現実の地理空間での軍事行動とサイバー空間での軍事行動の一体化

- **重要インフラへのサイバー攻撃**
- **ネット監視の強化**
  - 「敵」とみなされる人々への監視 **国境を越えた反戦平和の連帯が阻害される**
  - 政府に批判的な言論の監視 **国家安全保障を口実とした検閲**
  - 偽情報（流言飛語）への監視 **プロパガンダと不都合な事実の隠蔽**



戦争反対の声を抑圧、多様な議論の封殺、戦争の加速化



（注）　セキュリティ幹事会は平成26年10月に設置された。27年6月のオリパラ推進本部の設置以前は、2020年オリンピック・パラリンピック東京大会等に関する閣僚会議（27年6月廃止）がその役割を担っていた。また、27年7月の2020年東京オリンピック・パラリンピック競技大会関係府省庁連絡会議の設置以前は、2020年オリンピック・パラリンピック東京大会関係府省庁連絡会議（27年7月廃止）がその役割を担っていた。

オリンピックの場合

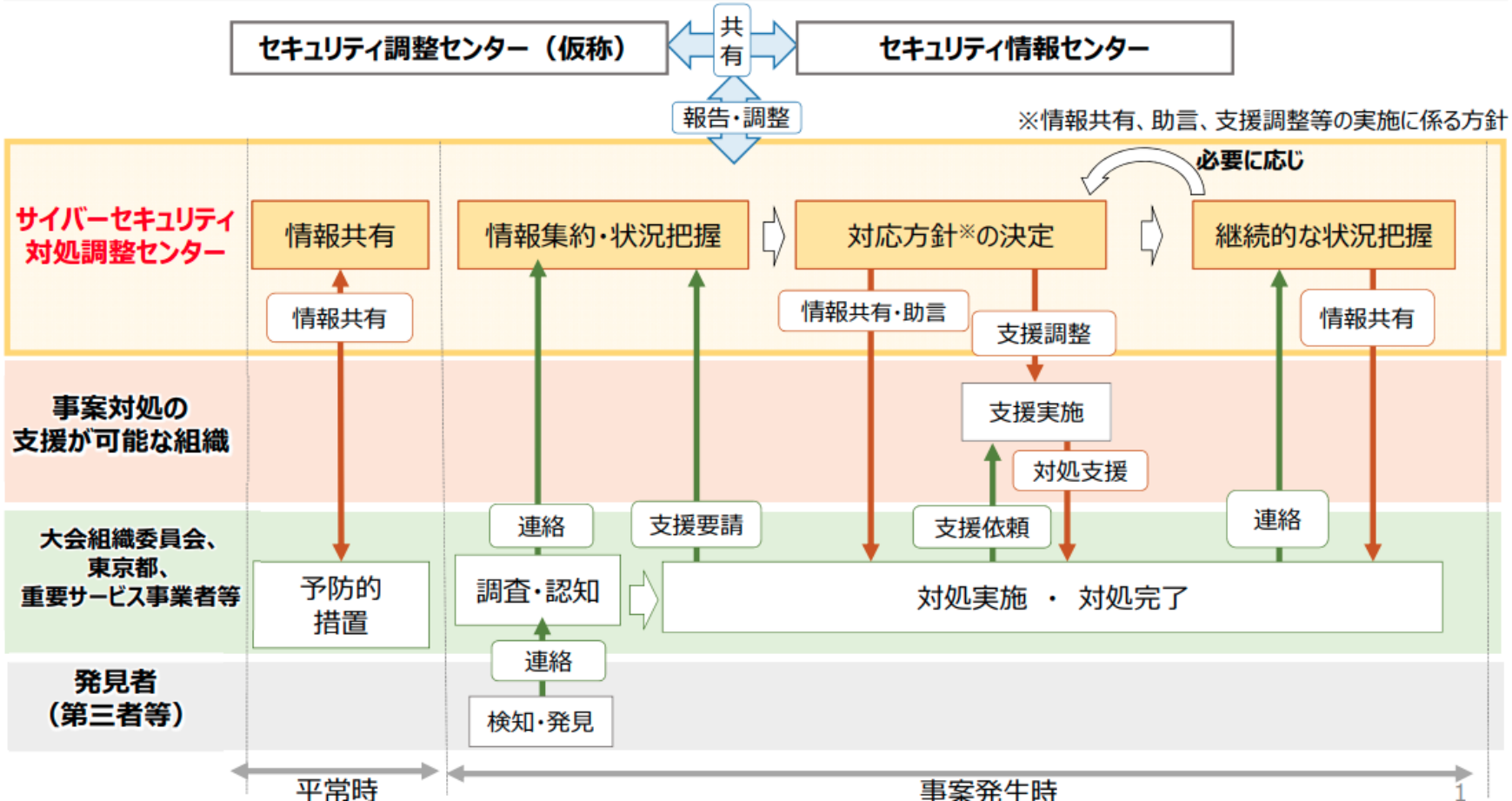
- 2017 年「 2020 年東京大会に向けたセキュリティ基本戦略」「オリパラ・テロ対策推進要綱」を策定
- 「オリパラ推進本部」の下に各省庁を横断した「セキュリティ幹事会」を設置。自治体もまきこんだ大規模な監視システムを構築
- セキュリティ情報センター (警察庁)、国際テロ対策等情報共有センター (仮称)(内閣官房)、サイバーセキュリティ対処調整センター (内閣官房) などが設置され、「国際テロ情報収集ユニット」等の活動が拡大・強化
- 共謀罪成立
- 2018 年春の通常国会 2020 年東京オリンピック競技大会・東京パラリンピック競技大会の準備及び運営の推進に関する政府の取組の状況に関する報告」の中心課題も、もっぱらセキュリティ対策とリスク管理に置かれた。

オリンピックの場合

- 従来の入国審査での生体情報の利用に加えて、航空会社が保有する旅客情報の収集強化
- 空港、山手線などの鉄道車内や駅構内などの公共の場所での顔認証や個人識別機能付の監視カメラの設置
- インターネット通信への監視強化などが計画
- ボランティア管理では、マイナンバーと顔認証を併用することを計画
- オリンピック観戦チケット購入についてもマイナンバーの導入を計画
- 聖火リレーなどのイベントを口実に、日本全国で日常的にテロ対策訓練

サイバーセキュリティ対処調整センターについて

➢ 2020年東京オリンピック競技大会・東京パラリンピック競技大会のサイバーセキュリティに係る脅威・インシデント情報を収集し、これら情報を大会組織委員会を始めとした関係機関等に提供、必要があるときには関係機関等のインシデント対処に対する**対処支援調整**を実施



オリンピックの場合

サイバーセキュリティ対処調整センター

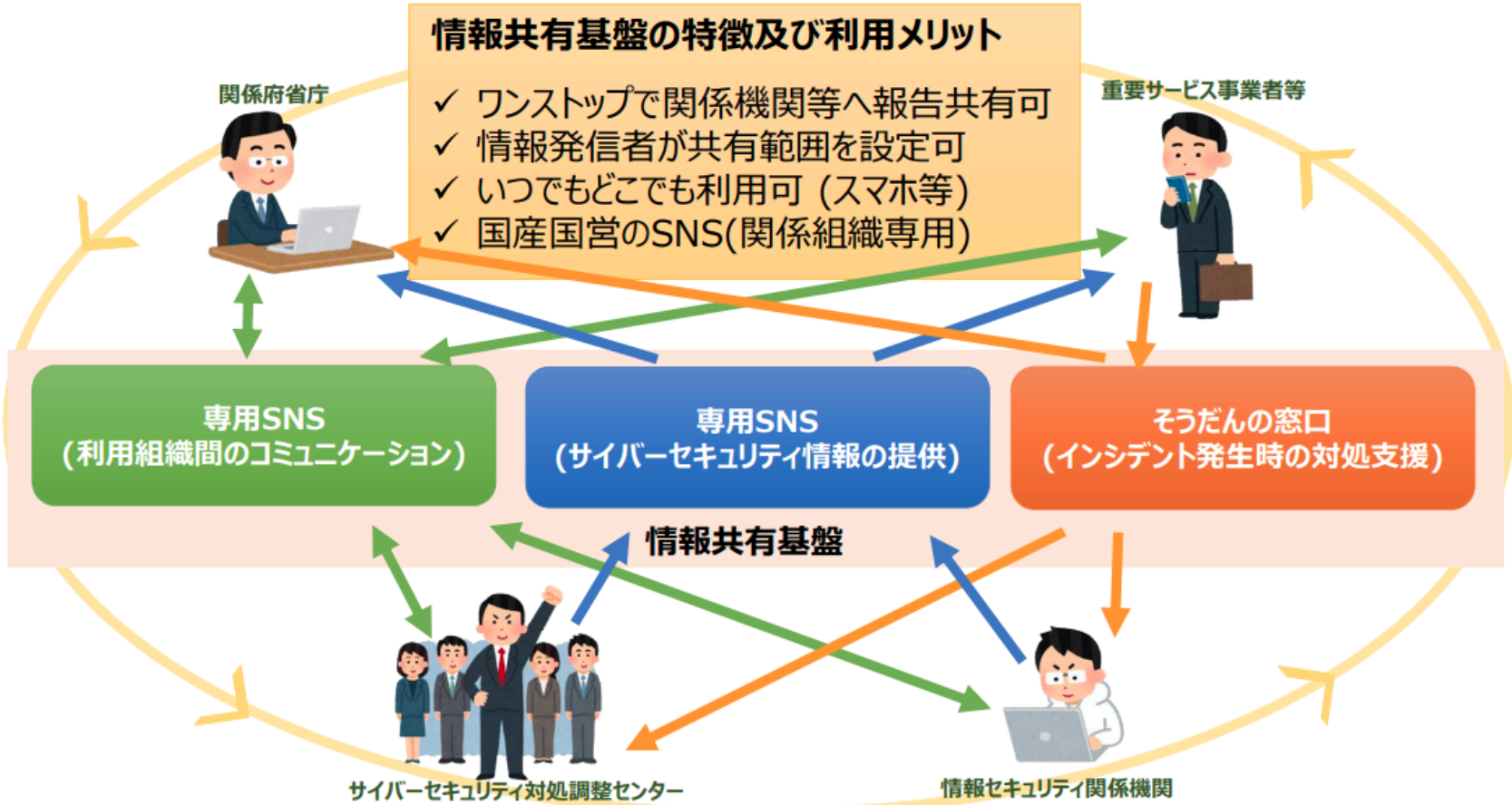
2020年東京オリンピック競技大会・東京パラリンピック競技大会のサイバーセキュリティに係る脅威・インシデント情報を収集し、これら情報を大会組織委員会を始めとした関係機関等に提供、必要があるときには関係機関等のインシデント対処に対する対処支援調整を実施

2019年4月より、対処調整センターは利用組織(※)に情報共有基盤を介してサービスを提供する。

※ 大会組織委員会、会場管理者、東京都、会場のある地方公共団体、重要サービス事業者等、スポーツ関連団体、情報セキュリティ関係機関、政府機関、警察等を想定している。

情報共有基盤について

- 2019年4月より、対処調整センターは利用組織(※)に情報共有基盤を介してサービスを提供する。
- 情報共有基盤を活用して、連絡体制確立のための演習・訓練を開催予定。



※大会組織委員会、会場管理者、東京都、会場のある地方公共団体、重要サービス事業者等、スポーツ関連団体、情報セキュリティ関係機関、政府機関、警察等を想定している。

情報共有基盤の運用開始について

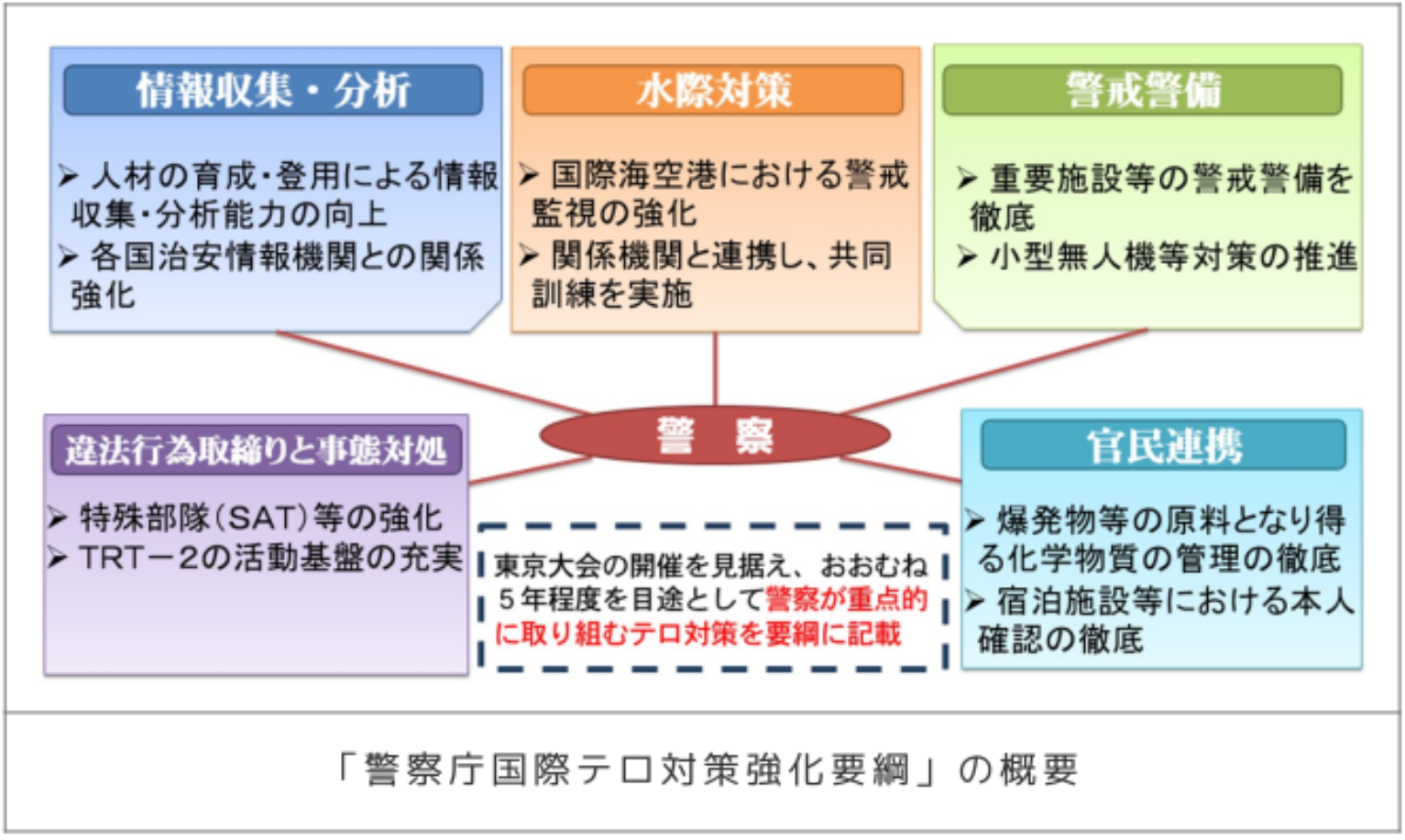
内閣官房
内閣サイバーセキュリティセンター
NISC

対処調整センターは、本年４月から運用を開始。情報共有基盤については、準備ができ次第、利用案内を行い、利用者登録が完了した組織から順次利用を開始する。
2020大会関係組織は、9月に予定している演習までに参加していただきたい。
現時点での予定は以下の通り。

■凡例
準備・調整期間
利用案内・登録
利用開始

利用者	2019年4月	2019年5月	2019年6月～
情報セキュリティ関係組織			
大会組織委員会、関係府省庁、東京都			
重要サービス事業者等、スポーツ関連団体等、他			
ラグビーWC関係組織			
G20関係組織	・・・以降、会合毎に個別調整	・・・以降、会合毎に個別調整	・・・以降、会合毎に個別調整

オリンピックの場合



「警察庁国際テロ対策強化要綱」の概要

廃案のためのアクションを

警察法改悪は、自民党改憲草案に明記されている現行憲法 21 条の言論表現の自由、通信の秘密など基本的人権を根底から否定する流れのなかに位置付けられる法改正である。

戦前の国家警察とは質的にも異なって、官民一体となった統治機構の大転換のなかで、情報通信産業の警察化が進められるものだ。

警察法改悪には「反対」以外の選択肢はありえない。