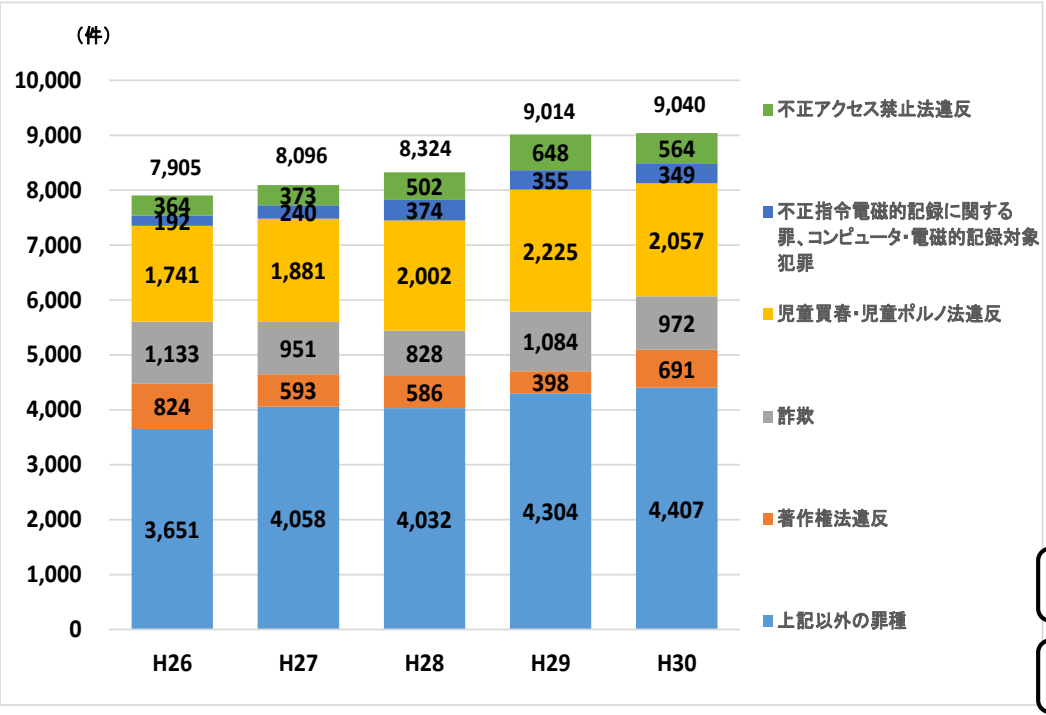
サイバー空間の脅威に対処するための資機材の整備

令　和　元　年　６　月　１　８　日
警　察　庁　長　官　官　房　企　画　課
（サイバーセキュリティ対策担当）

サイバー空間の脅威①　～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。大きくは不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪等、その他（詐欺、著作権法違反等）に分類される。
- 近年、サイバー犯罪の検挙件数は増加傾向にあり、平成30年中の検挙件数は9,040件と過去最多。

サイバー犯罪の検挙件数の推移



サイバー犯罪の例

不正アクセス

他人のID・パスワードを無断で使用したり、コンピュータプログラムのぜい弱性を衝くことによって、本来は利用する権限のないコンピュータ等を利用する行為

ウイルス作成、取得、供用

不正プログラム（不正な動作を行う意図で作成された悪意のあるソフトウェアの総称）を作成、取得、供用する行為

その他

その実行に不可欠な手段として、インターネットを利用する犯罪行為

メールやスマホアプリを利用した詐欺

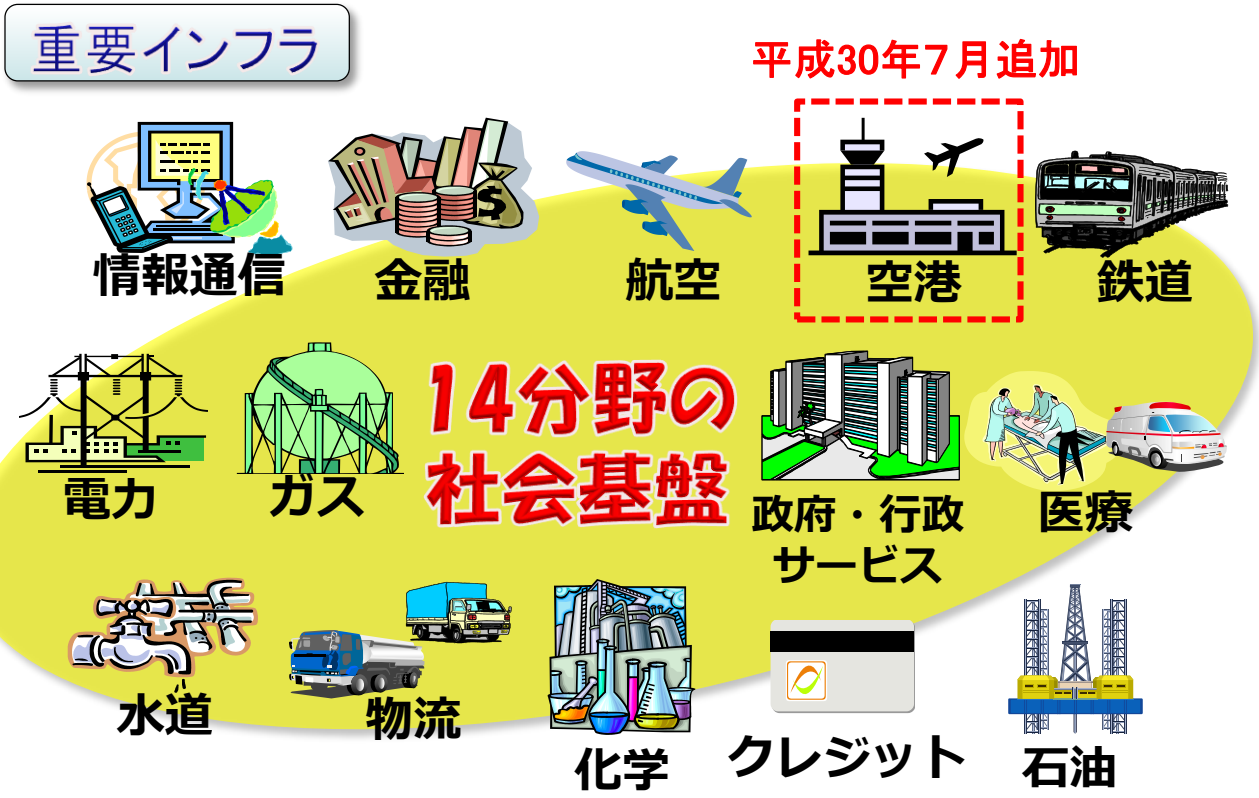
著作物の不正な公衆送信

ネット上の児童買春・児童ポルノ

ネット上の脅迫やストーカー行為

サイバー空間の脅威②　～サイバー攻撃～「サイバーテロ」

- ■ <u>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電子的攻撃による可能性が高いもの</u>
- ■ サイバーテロが発生し、インフラ機能の維持やサービスの供給が困難になれば国民生活や社会経済活動に重大な被害が生じるおそれがある



海外における事例（ウクライナにおける大規模停電）

平成27年12月、ウクライナにおいて大規模な停電が発生。

同国の電力会社の一つは、システムへの不正な侵入を受け、30箇所以上の変電所との通信が切断されたことにより、８万の顧客が停電の影響を受けたと発表。

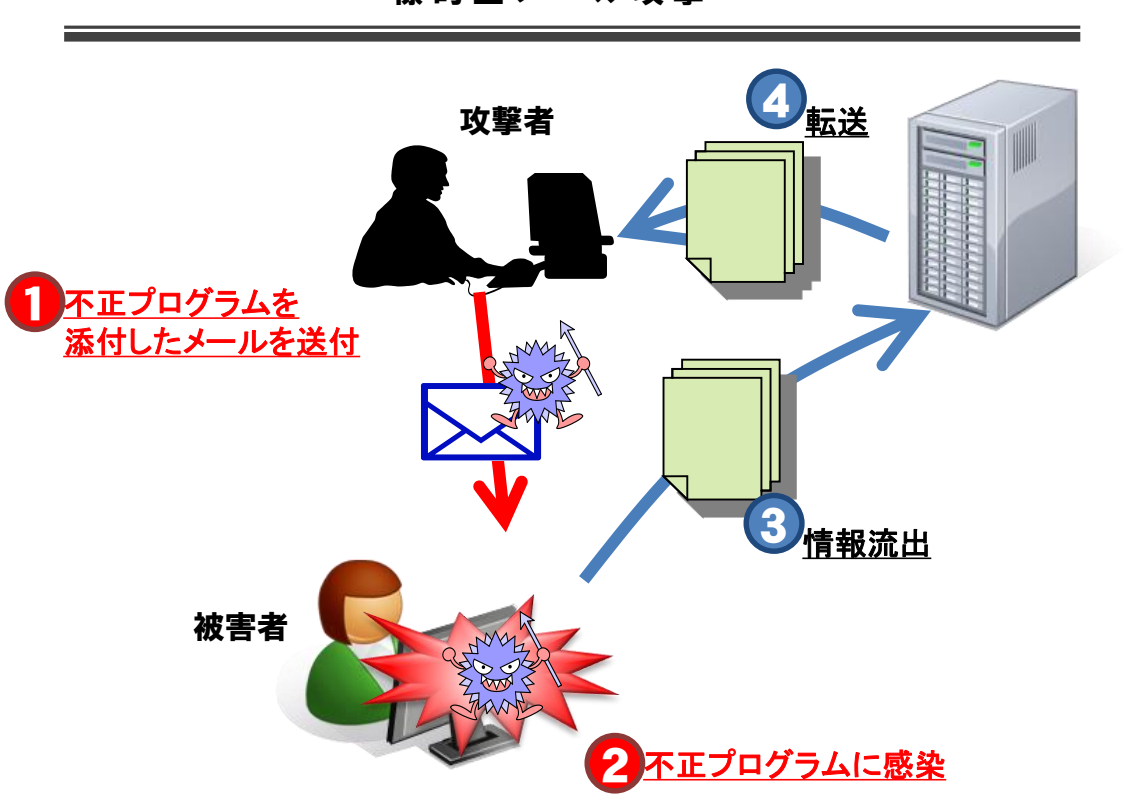
また、平成28年12月、これに関連するとみられるサイバー攻撃による停電が発生したことが報じられている。

出典：http://styknews.info/novyny/ns/2015/12/23/frankivsk-na-pivgodyny-zalyshyvsia-bez-svitla-foto

サイバー空間の脅威③　～サイバー攻撃～「サイバーインテリジェンス」

- **情報通信技術を用いた諜報活動**
- **政府機関や先端技術を有する企業から、外交交渉における国家戦略等の機密情報や軍事技術への転用も可能な先端技術の窃取を図るサイバー攻撃**

サイバーインテリジェンスの手口の例



国内における事例

①　平成28年10月、富山大学水素同位体科学研究センターに対するサイバー攻撃により、同大学職員のコンピュータが不正プログラムに感染し、外部のサーバとの間で不審な通信が発生していたことが明らかとなった。

②　平成30年２月、国立研究開発法人産業技術総合研究所に対し、外部から不正アクセスがあったことが確認され、同年７月、当該不正アクセスが同研究所のメールシステムや管理用ネットワーク内のシステムに対するものであり、未公表の研究情報や個人情報等の窃取又は閲覧が行われた可能性があるとの調査結果が発表された。

サイバー空間の脅威の特徴

① 加害者が被害者と対面することなく敢行される非対面型犯罪であり、近年、その問題が顕在化

- SNS(※)等のインターネット上のやり取りから凶悪犯罪に至る事例が発生
- 情報通信技術の普及・進展に伴い、スマートフォン等が犯罪に悪用される事例が増加

※ ウェブサイト内で多人数とコミュニケーションがとれるウェブサイト等のうち、出会い系サイトを除いたものの総称

② 地理的・時間的制約を受けることが少なく、短期間のうちに不特定多数の者に被害を及ぼしやすい

- 被害拡大の防止、被害の未然防止を図ることが困難なケースも。
- 国際捜査共助の枠組みの活用、外国捜査機関等との連携の推進等が重要

③ 匿名性が高く、犯行の痕跡が残りにくい

- 匿名化ツールが使用されることがあるほか、いわゆるダークウェブ(※)が各種犯罪の温床となっているとの指摘

※ 匿名接続を実現するためのソフトウェア等を使用しなければ接続できないウェブサイト

政府・警察におけるサイバーセキュリティ対策推進体制

サイバーセキュリティ戦略本部（H27.1設置）

○本部長：内閣官房長官　○副本部長：オリパラ担当大臣
○本部員：国家公安委員会委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣、IT政策担当大臣、有識者

サイバーセキュリティ戦略(平成30年７月27日閣議決定)

4.2.1 国民・社会を守るための取組

サイバー空間の脅威の深刻化に伴い、多くの国民がサイバー犯罪に不安感を持つようになっており、社会全体におけるサイバーセキュリティへの危機意識は高まっている。(略)

内閣サイバーセキュリティセンター〔NISC〕（H27.1改組）

○サイバーセキュリティ戦略本部の事務局
○国全体のサイバーセキュリティ施策の企画、立案及び総合調整等を実施

捜査機関・事案対処省庁としてサイバー犯罪、サイバー攻撃の捜査と未然防止のための取組を推進する必要

各府省

○**警察庁**、総務省、外務省、経済産業省、防衛省、その他関係省庁
○各府省は、それぞれの所掌に基づき、国のサイバーセキュリティ戦略を踏まえた対策を推進

警察におけるサイバーセキュリティ対策の推進

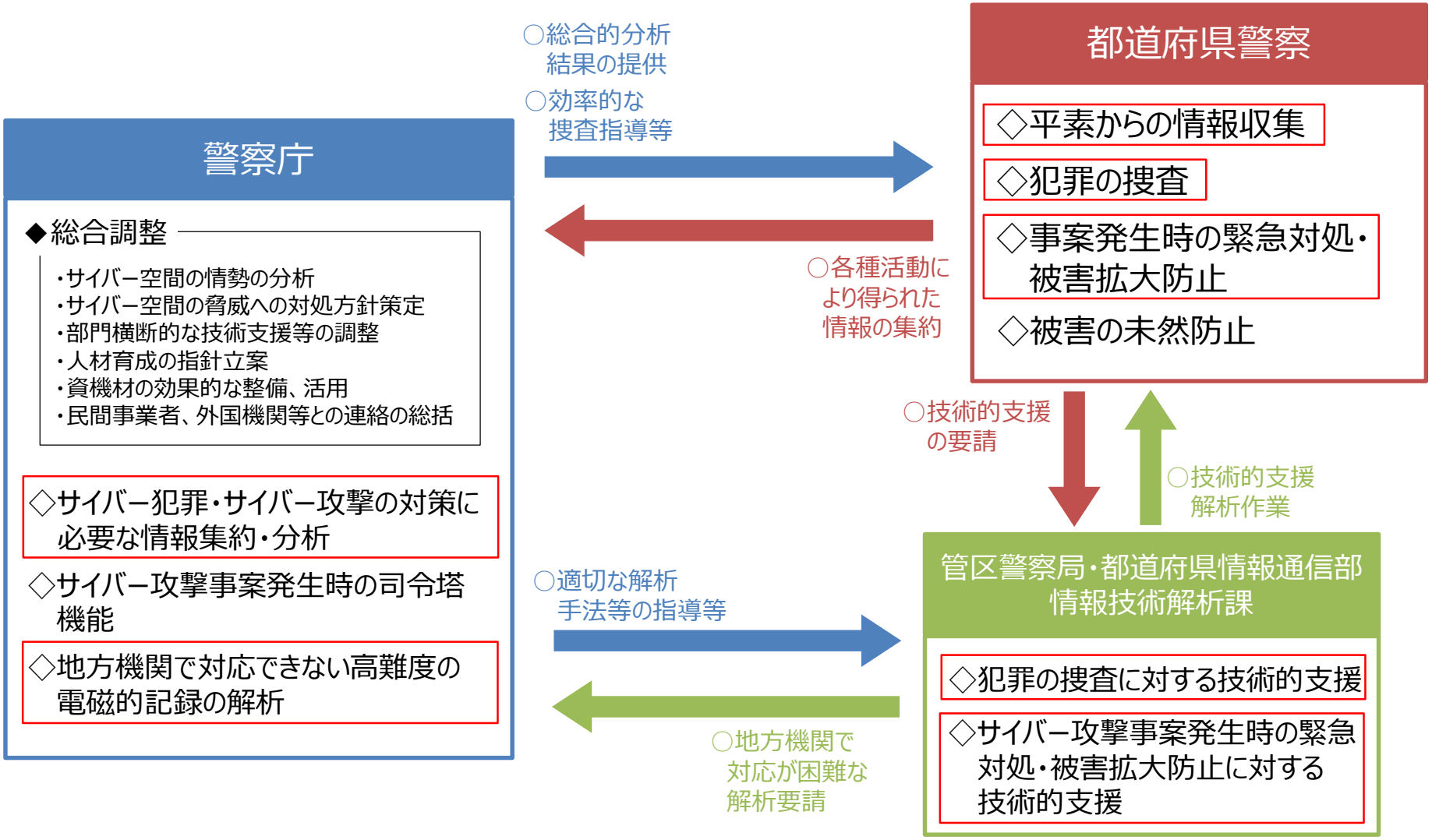
■　**平成30年７月、政府において「サイバーセキュリティ戦略」が閣議決定されたこと等を踏まえ、同年９月、「警察におけるサイバーセキュリティ戦略」を改定**

具体的取組

○サイバー空間の脅威への対応の強化として、「サイバー犯罪に対する捜査等の推進」、「国の公安を脅かす事案の防止及び対処」、「東京大会に向けた取組」等の推進
○警察における組織基盤の更なる強化として、「部門間連携の推進」、「情報収集・分析及び情報技術解析態勢の強化」の推進

本事業対象範囲

警察におけるサイバー犯罪・サイバー攻撃に対する取組



本事業の対象資機材は、主として上図の［　　］において使用されるが、同資機材の運用において得られた情報は、必要に応じて民間事業者等に提供され、被害の未然防止にも役立てられる。

活用事例　～サイバー犯罪捜査①～　証拠収集編

都道府県警
捜査部門

事件発生

周辺情報収集
サイバー犯罪捜査に必要な情報(不審な接続先のサイト、フィッシングサイトの情報等)をインターネット等から収集する。
主な使用資機材　**事件情報内偵用資機材**
構成品：デスクトップ型パソコン
ノート型パソコン
仮想環境用ソフトウェア　等

捜索差押え・検証等

押収物からの証拠収集・分析
押収物や、任意提出を受けたコンピュータ等のハードディスク内を探索し、立件に向けた証拠等（接続情報、ログイン情報、その他各種ログ等）を収集する。
主な使用資機材
▪電磁的記録分析用資機材
構成品：ノート型パソコン
分析用ソフトウェア等
▪ハードディスクコピー装置
構成品：アプライアンス製品(※)

捜査・検挙

技術的知見が必要な場合

管区・都道府県
情解部門

技術支援

差押え現場等における技術的な支援
差押え現場において、捜査部門が情解部門の支援を受けつつコンピュータ等を差し押さえるとともに、情解部門において押収物等に記録されたデータを抽出・可視化するなどの作業を機動的に行う。
主な使用資機材　**現場臨場用資機材**
構成品：ノート型パソコン
各種データ探索・復元用ソフトウェア等

複雑な解析や物理的に破損している場合

電磁的記録の解析
データ内の電子ファイルが破損していて内容を確認できない場合等、専門的な技能や資機材がなければ対応できない作業を行う。
主な使用資機材
▪ファイル復元用資機材
構成品：デスクトップ型パソコン
復元用ソフトウェア(別途整備)
▪証拠保全用資機材
構成品：アプライアンス製品（※）

より高度な技術や警察庁に整備した高度な資機材が必要な場合

警察庁
情解部門

高度な技術支援

高度な電磁的記録の解析
押収物等が物理的に損傷し、正常に動作しない場合など、機能回復等の作業を行う。
主な使用資機材（高度な資機材）
動作不良ハードディスク解析用工具
構成品：アプライアンス製品（※）

※アプライアンス製品
特定の機能や用途に特化した専用機器のこと

活用事例　～サイバー犯罪捜査②～　不正プログラム特定編

都道府県警捜査部門

被害の認知

被害状況の聴取

不正プログラムの痕跡収集・集約

不正プログラムの感染が疑われる被害者のコンピュータから、不正プログラムが動作する際に示す各種情報（不審なプログラムの起動状況、不審な接続先、情報の送受信状況等）を収集する。

主な使用資機材　**現場情報収集用資機材**

構成品：ノート型パソコン
抽出用ソフトウェア等

被害端末の受領

痕跡情報の警察庁集約

不正プログラムを悪用した手口の解明

不正プログラムの探索・解析

不正プログラムの探索・解析

被害者のコンピュータから、不正プログラムを探索し、検出された場合は、警察庁に設置された不正プログラムを自動解析する資機材により、不正プログラムの挙動を解析する。同資機材で解析できないものについては、ソースコード等を解析して、その挙動を明らかにする。

主な使用資機材

・不正プログラム解析補助装置

構成品：解析用サーバ接続用端末
解析用サーバ（警察庁本庁に設置）
等

・不正プログラム検証用資機材

構成品：デスクトップ型パソコン
仮想環境用ソフトウェア
プログラム解析用ソフトウェア
検証用ソフトウェア　等

管区・都道府県情解部門

難解な不正プログラムの解析

難解な不正プログラムの解析

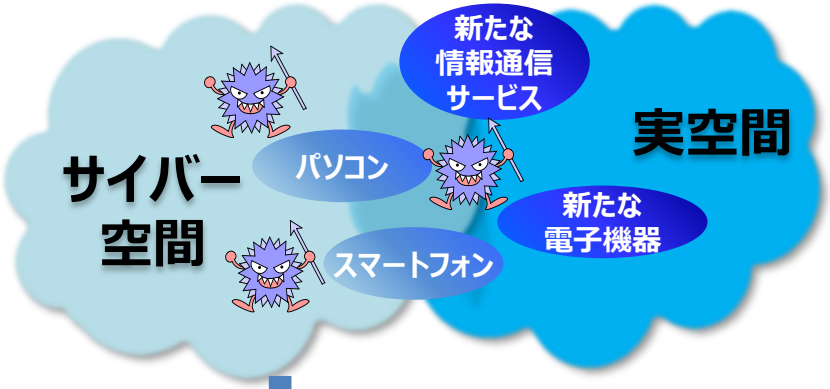
難読化技術が施された不正プログラムや特殊なOSのコンピュータを標的とした不正プログラム等に対し、ソースコード等を解析して、その挙動を明らかにする。

主な使用資機材
不正プログラム検証用資機材
（警察庁本庁版）

構成品：デスクトップ型パソコン
仮想環境用ソフトウェア
プログラム解析用ソフトウェア
検証用ソフトウェア（特殊OS対応）等

警察庁情解部門

国が整備するCS対策資機材に係る調整・連携の体制



○サイバー犯罪等の技術的トレンド
○製品の市場調査

資機材の機能・性能要望

都道府県警察

サイバー犯罪対策課　等
サイバー攻撃特別捜査隊　等

○サイバー犯罪捜査
○サイバー攻撃対処

都道府県情報通信部情報技術解析課

○都道府県警察に対する技術的な支援

警察庁担当部局

情報技術犯罪対策課
サイバー攻撃対策室
情報技術解析課

○整備計画の立案
○機能、性能の検討
○現行の整備基準検討
○整備の推進
（予算要求、執行）

着目点
○現行資機材が、犯罪に悪用される製品に対応できているか。
○現在の整備基準を増減させるべき要因（サイバー犯罪発生件数・相談件数の変化等）はないか
○過剰なスペックとなっていないか

要望のとりまとめ

警察庁長官官房

企画課（サイバーセキュリティ対策調整）
〔平成26年度設置〕

○担当部局の整備計画の把握
○把握結果を踏まえ、予算要求段階における
・整備推進内容の重複の解決
・整備基準の妥当性検討
等の調整・ヒアリングを実施

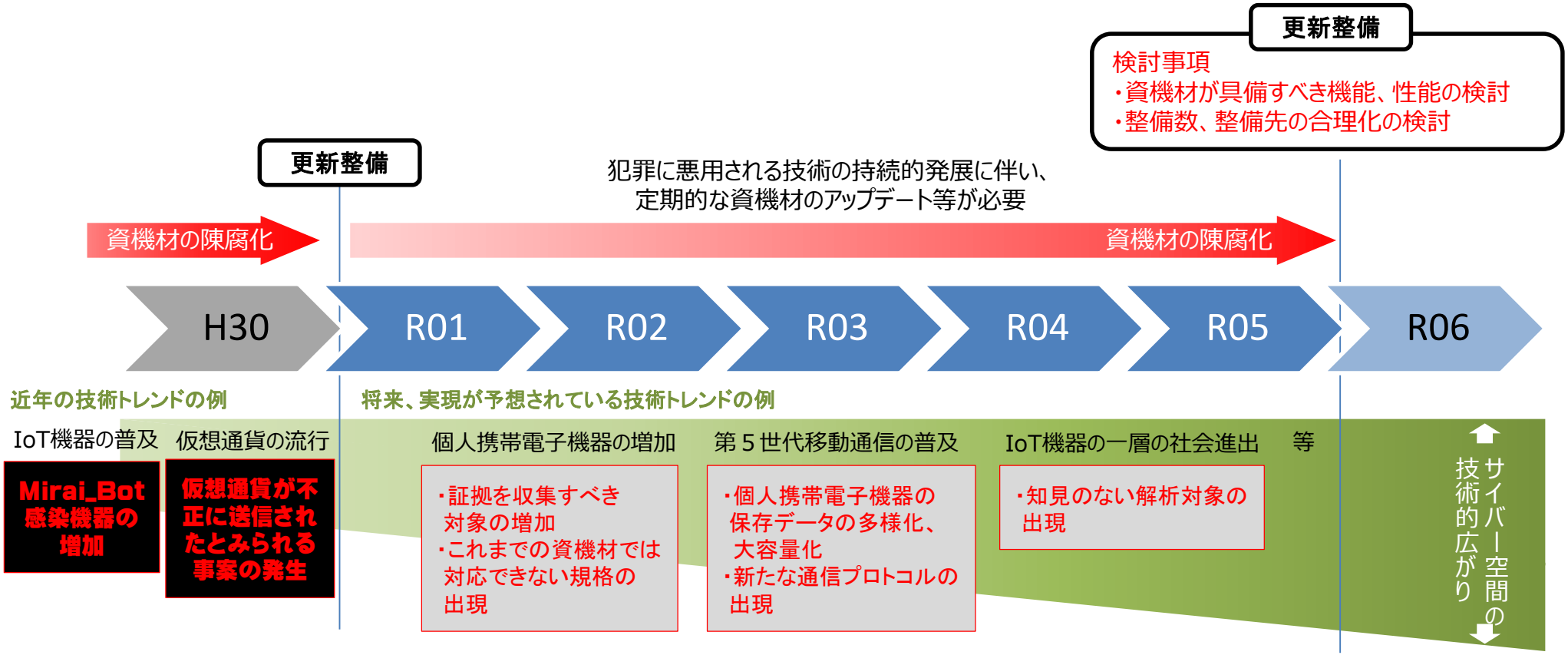
着目点
○機能・性能面から部門間での共有が図れないか
○整備の必要性や数量の妥当性は認められるか

財政部門へ

サイバーセキュリティ対策用資機材の整備計画モデル

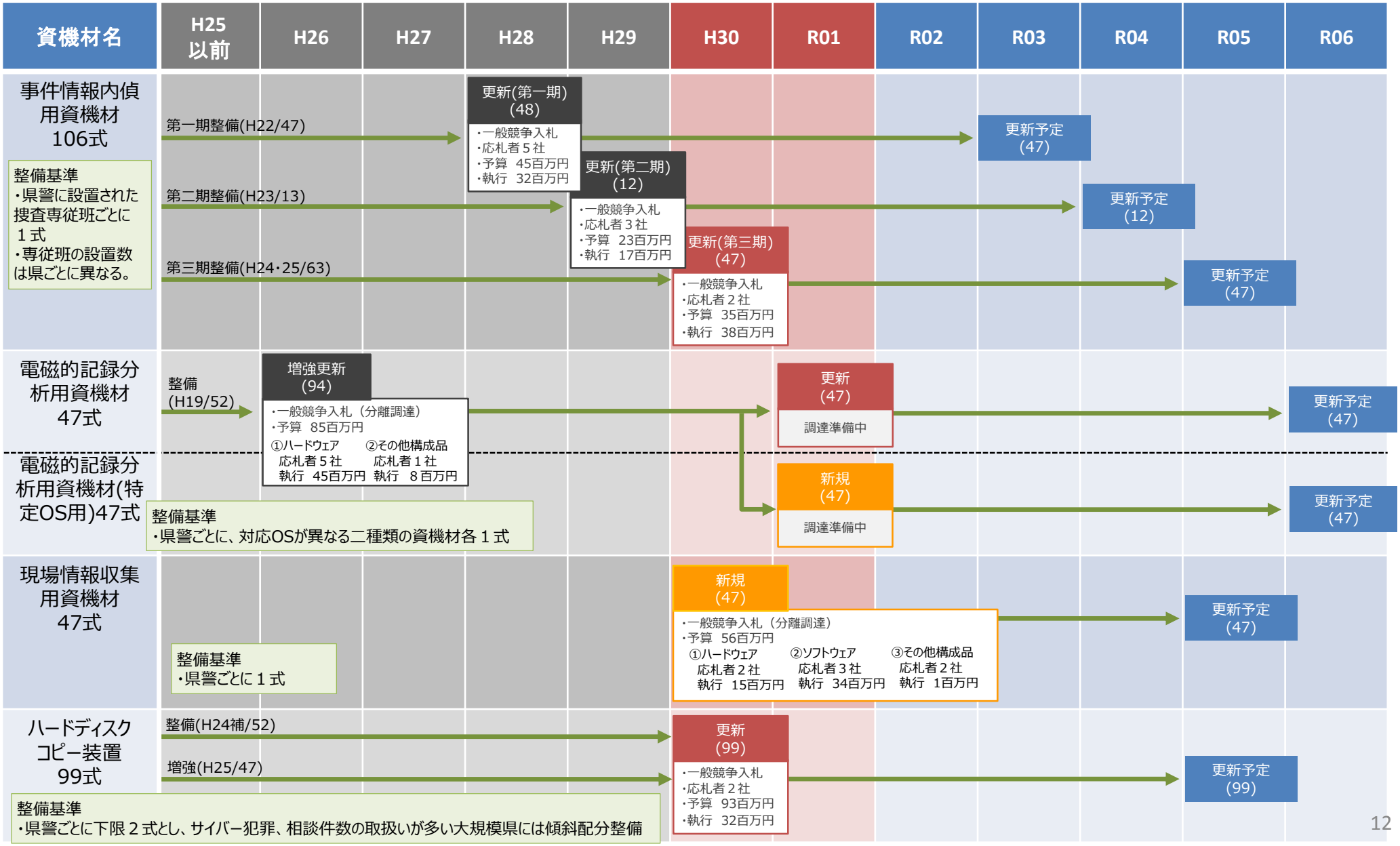
■　**サイバー犯罪・サイバー攻撃の質的・量的拡大や、新たなサイバー犯罪・サイバー攻撃の出現に対応するためには、資機材の定期的なアップデート等が必要であり、資機材を更新していく計画が必要**

耐用年数を５年と設定した資機材の整備計画



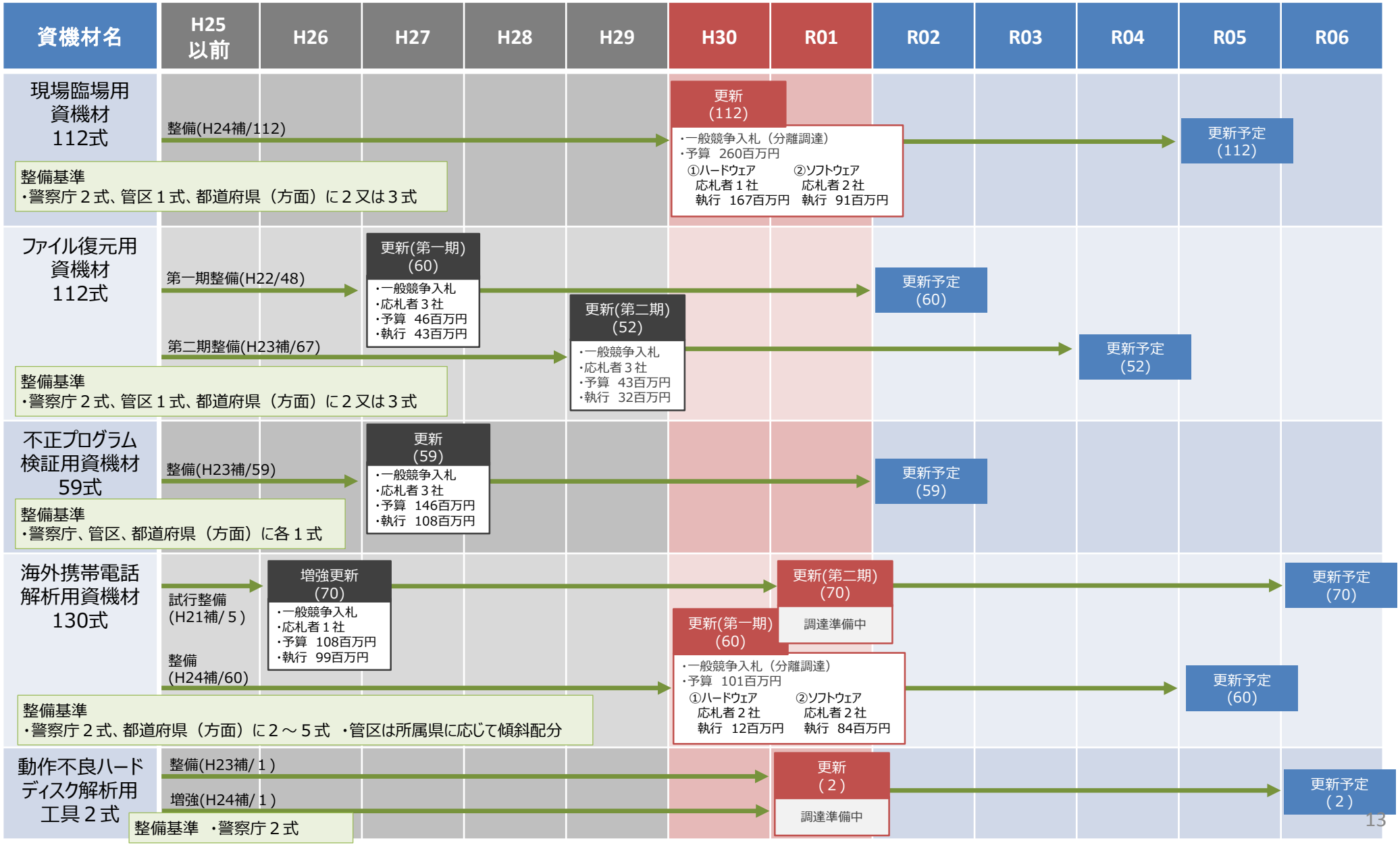
サイバーセキュリティ対策用資機材の整備計画（抄）

サイバー犯罪捜査において使用する主要資機材



サイバーセキュリティ対策用資機材の整備計画（抄）

技術的支援において使用する主要資機材



今後の課題

■ インターネットに接続される機器の数は年々増加しており、2020年には家電、自動車、医療機器、産業機器等約400億の機器が接続される「モノのインターネット（IoT）」が形成されると言われている。

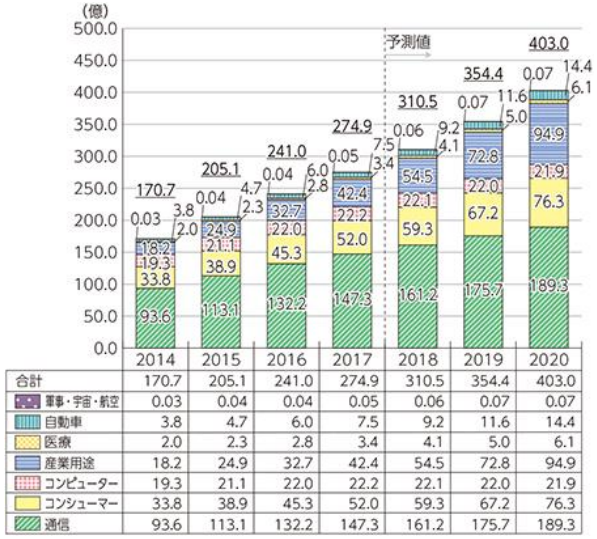
⇒ サイバー犯罪・サイバー攻撃の標的や踏み台になる電子機器の数や種類が増加

⇒ 資機材に求められる機能・性能が高度化・多様化

サイバー空間の脅威に対処するための人材育成の推進
平成30年度公開プロセス

新たなサイバー空間の脅威に対処するための資機材の整備

出典：独立法人情報処理推進機構（IPA）ホームページ
（https://www.ipa.go.jp/security/iot/index.html）



	2014	2015	2016	2017	2018	2019	2020
合計	170.7	205.1	241.0	274.9	310.5	354.4	403.0
軍事・宇宙・航空	0.03	0.04	0.04	0.05	0.06	0.07	0.07
自動車	3.8	4.7	6.0	7.5	9.2	11.6	14.4
医療	2.0	2.3	2.8	3.4	4.1	5.0	6.1
産業用途	18.2	24.9	32.7	42.4	54.5	72.8	94.9
コンピューター	19.3	21.1	22.0	22.2	22.1	22.0	21.9
コンシューマー	33.8	38.9	45.3	52.0	59.3	67.2	76.3
通信	93.6	113.1	132.2	147.3	161.2	175.7	189.3

世界のIoTデバイス数の推移及び予想
出典：「平成30年版情報通信白書」（総務省）