警察におけるこれまでの取組等

令　和　６　年　７　月
警察庁サイバー警察局

警察の体制

○　従来、サイバー事案への対処では、**各都道府県警察が捜査権限を執行し、警察庁は必要な指示や調整等を実施。**

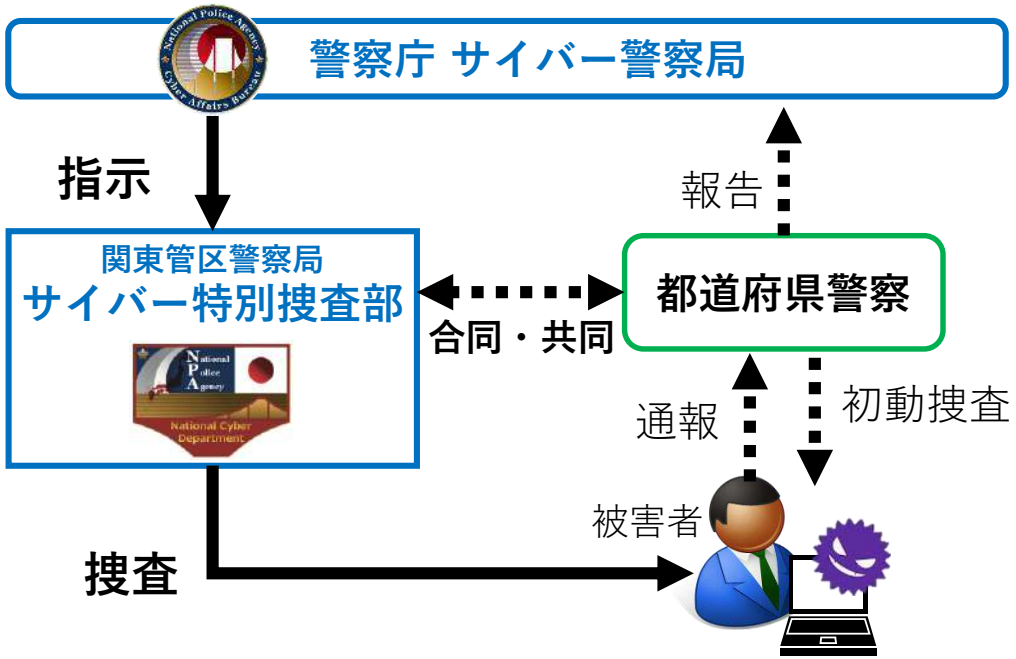
○　サイバー空間には国境がないことから、特に**重大サイバー事案への対処では、**外国捜査機関等との連携が不可欠であり、**都道府県警察の捜査のみを前提とする仕組みでは、対処に支障。**

○　令和４年４月、警察庁に**サイバー警察局**を設置するとともに、**重大サイバー事案における捜査権限の執行を行うサイバー特別捜査隊**を設置（令和６年４月より**サイバー特別捜査部**に昇格）

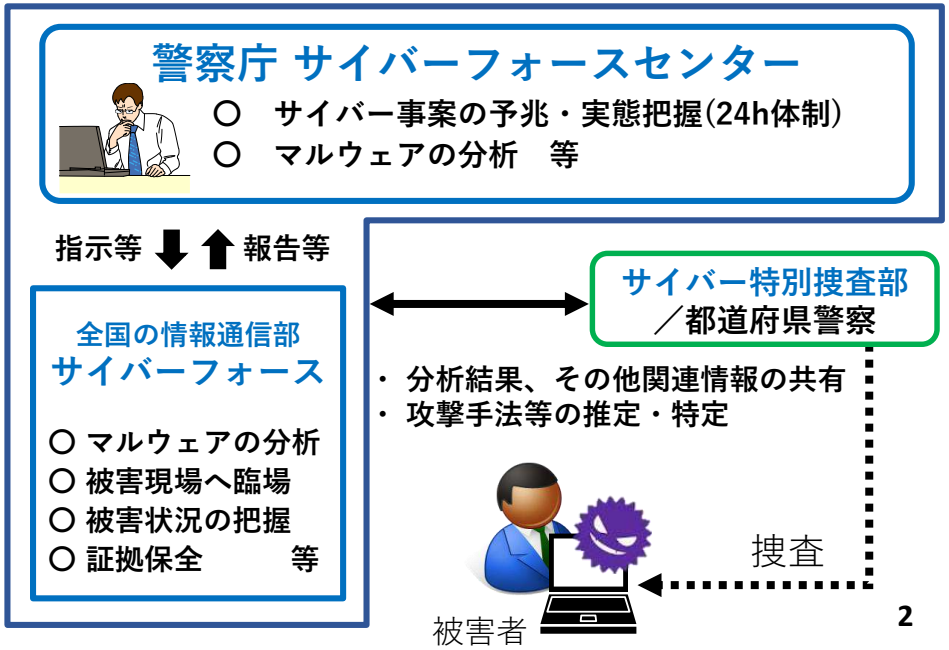
○　**他方、次々と変化する手口や高度なサイバー攻撃に対処するため**、警察庁及び全国の情報通信部に**サイバー事案対策の技術支援を行う部隊である**サイバーフォース（警察庁にあってはサイバーフォースセンター）を設置しているところ。

○　24時間体制でのサイバー攻撃の予兆・実態把握、マルウェアの分析等のほか、被害発生時には、被害状況の把握、証拠保全等を実施。

【重大サイバー事案の捜査における各組織の関係】



【サイバー事案対策の技術支援に係る各組織の関係】



サイバー攻撃に対する警察の主な取組・枠組み

(1) サイバー攻撃に対する捜査や実態解明、国際連携

- **サイバー攻撃に対する捜査**のほか、サイバー攻撃に用いられたマルウェアの解析結果や捜査情報等を総合的に分析するなどにより、**攻撃者及び手口に関する実態解明を推進。**
- 平素からの情報交換や、国際刑事警察機構（ＩＣＰＯ）等を通じて、**外国捜査機関等との国際捜査協力を推進。**

(2) パブリック・アトリビューション、各種注意喚起

- 捜査情報等に基づき、関係国とも連携し、**サイバー攻撃の攻撃者を公表し、非難することでサイバー攻撃を抑止する取組（パブリック・アトリビューション）を推進。**

  【事例】令和５年9月、警察庁は、ＮＩＳＣのほか、米国のＮＳＡ、ＦＢＩ及びＣＩＳＡとの連名で、中国を背景とする「BlackTech」のサイバー攻撃に関する注意喚起を実施。

- 被害の未然防止・拡大防止を目的として、重要インフラ事業者等に対して**サイバー攻撃に関する注意喚起(※)を実施。**

(3) C2サーバのテイクダウン

- **Ｃ２サーバとしての不正な機能を停止（テイクダウン）するよう、サーバを管理する事業者等に依頼するなどの対策を実施。**

(4) サイバーテロ対策協議会

- 各都道府県警察及び重要インフラ事業者等で構成され、全ての都道府県に設置。
- **サイバー攻撃の脅威等に関する情報共有**やサイバー攻撃の発生を想定した**共同対処訓練等を実施。**

(5) サイバーインテリジェンス情報共有ネットワーク

- 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8,600の事業者等との間で構成。
- **サイバー攻撃に関する情報を集約**するとともに、これら情報を総合的に分析し、**分析結果に基づく注意喚起等を実施。**

（※）家庭用ルーターがサイバー攻撃に悪用されていたことを受け、令和５年３月に警察庁及び警視庁において、関係メーカーと協力した注意喚起を実施。

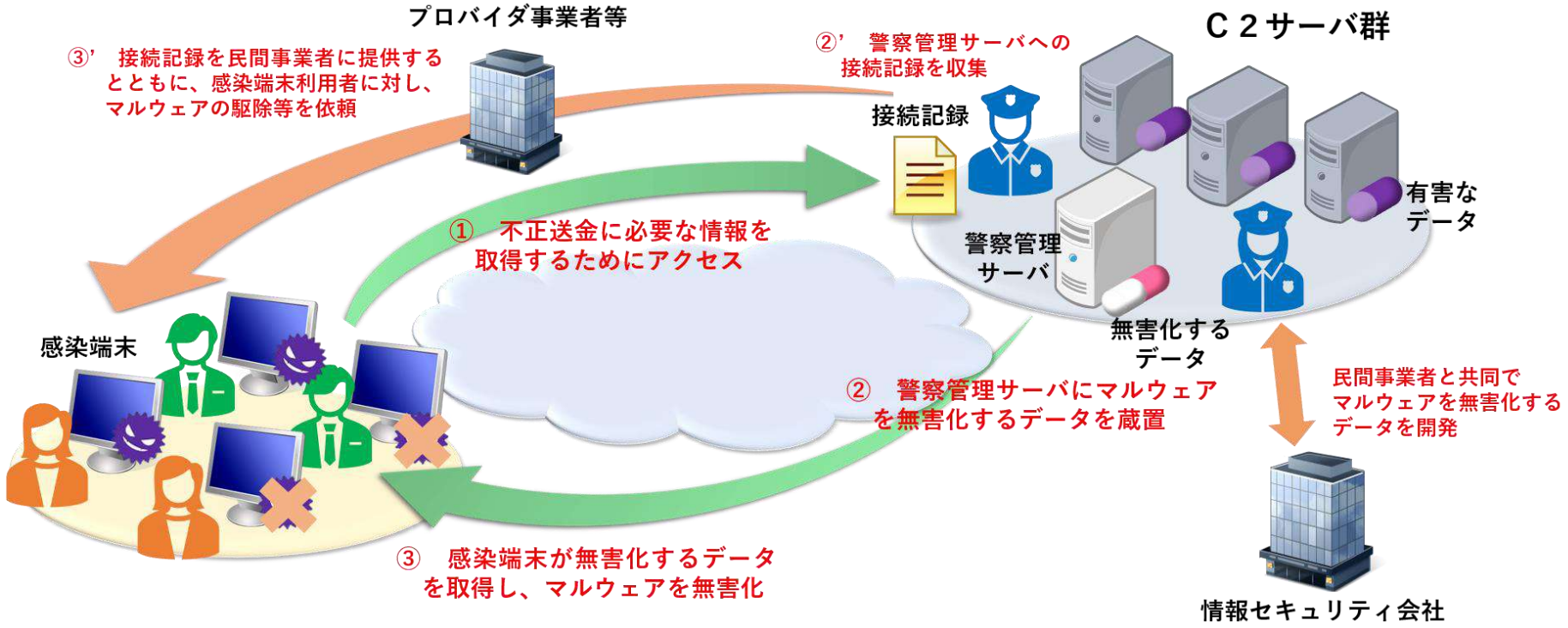
アクセス・無害化措置に関連する警察の取組事例①

【感染端末内のマルウェアの無害化措置】

インターネットバンキングに係る不正送金事犯に係るマルウェアによる被害拡大の防止（平成27年）

● 平成27年４月、警視庁では、インターネットバンキングに係る不正送金事犯に使用されている**マルウェアの感染端末の通信先となっているC2サーバに割り当てられていた失効済みのドメインを取得し、警察管理サーバに割り当て**ることで、当該マルウェアの**感染端末情報の収集**を実施。

● 加えて、感染端末が指令を取りに行くためにC2サーバに定期的にアクセスすることを逆手に取り、**指令に関するデータの代わりに、マルウェアを無害化するデータを警察管理サーバに蔵置し、感染端末内のマルウェアの無害化措置を実施。**



アクセス・無害化措置に関連する警察の取組事例②

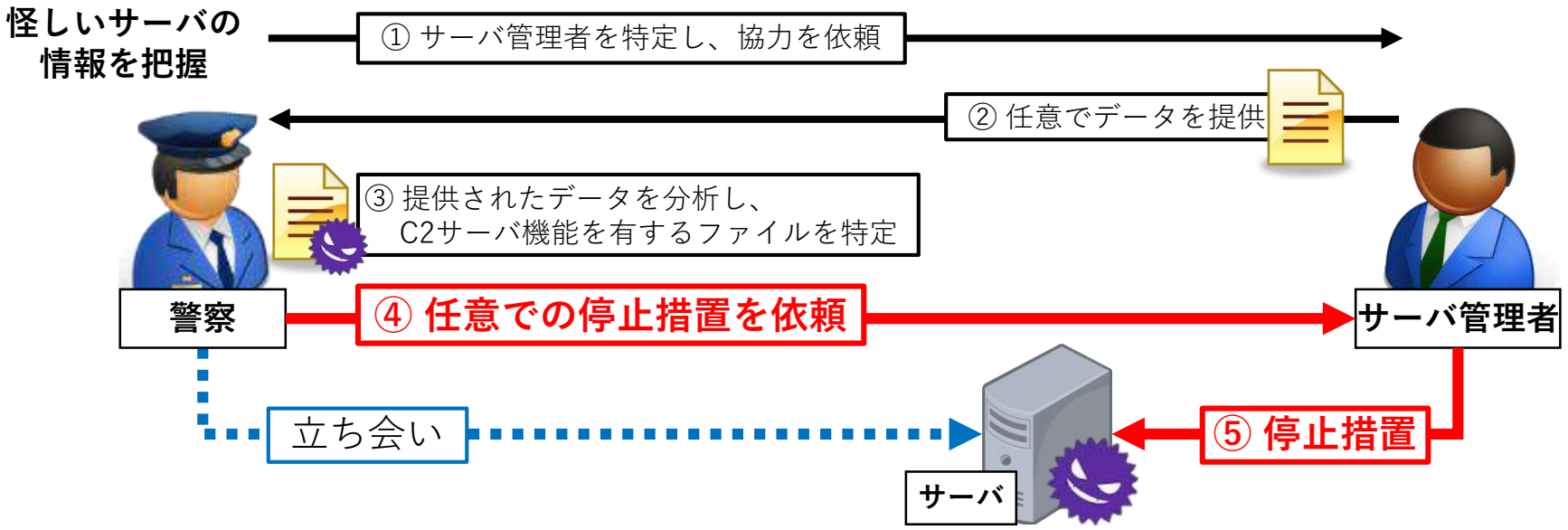
【任意の協力に基づくC2サーバの無害化措置】

不正アクセス事案における無害化措置（令和４年）

- 令和４年７月、警察において、あるwebサイトが改ざんされ、Ｃ２サーバとして利用されている疑いがある旨の情報を把握。
- **サーバ管理者（webサイト運営会社）を特定し、協力を依頼。**提供されたデータを精査し、**サーバ内の不審ファイルがＣ２サーバの機能を有することを特定。**
- **管理者の協力のもと、Ｃ２サーバの機能を停止**
  - ✓ サーバ内の不審ファイルの削除

不正指令電磁的記録供用事案における無害化措置（令和５年）

- 令和５年６月、警察において、マルウェアの通信先（C2サーバ）の疑いがあるサーバの情報を把握。
- **サーバ管理者（webサイト運営会社）を特定し、協力を依頼。**提供されたデータを精査し、**サーバ内の不審ファイルがＣ２サーバの機能を有することを特定。**
- **管理者の協力のもと、Ｃ２サーバの機能を停止。**
  - ✓ サーバ内の不審ファイル及び関連フォルダの削除
  - ✓ そのほか、使用していないwebサイトを閉鎖

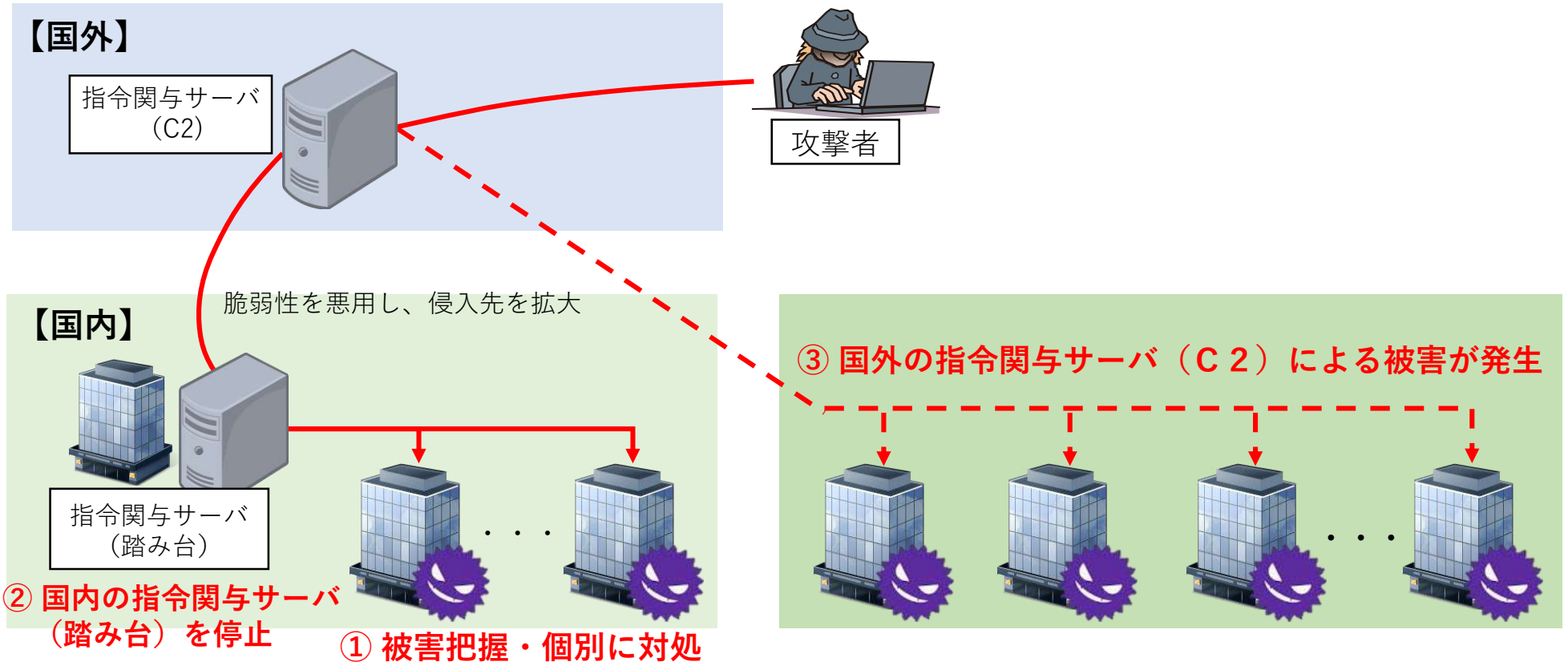


無害化措置ができれば被害防止につながる可能性のある事例①

同一のC2サーバが使用され被害が拡大した事例

- 国内事業者Aにおいて、マルウェアに感染していることが発覚。
- 調査したところ、**国内の指令関与サーバ（踏み台）及び国外の指令関与サーバ（C2）を特定。**
- 国内の指令関与サーバ（踏み台）については、**サーバ管理者の任意の協力に基づいて停止措置を実施。**

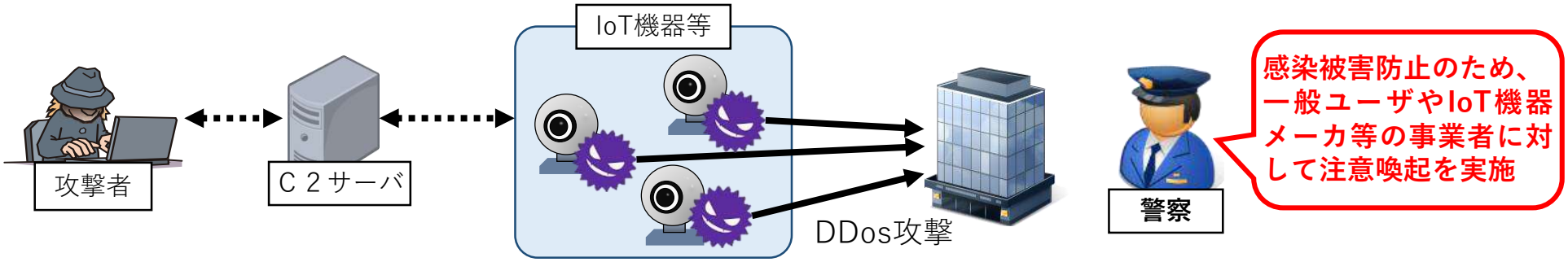
⇒ **国内の指令関与サーバ（踏み台）停止後も、国外の指令関与サーバ（C2）による被害が発生**



無害化措置ができれば被害防止につながる可能性のある事例②

IoT機器等を踏み台としたサイバー攻撃を踏まえた注意喚起（平成28年～）

- 平成28年、国外において、IoT機器等に感染してDoS攻撃を行うマルウェア「Mirai」を使用したと見られるDDoS攻撃の被害が発生。
- 同年、警察庁のサイバーフォースセンターにおいて、**「Mirai」に感染したIoT機器等が発信元と見られる不審な通信の増加を観測。**
- **同年10月、警察庁では、ウェブサイトを通じて注意喚起を実施**するとともに、**一般財団法人日本サイバー犯罪対策センター（JC3）等と連携し、関係事業者に対する注意喚起を実施。**
  - ✓ ユーザ名、パスワードを推測されにくいものに変更。
  - ✓ 特定の接続先のみへのアクセス許可等、適切なアクセス制御の実施。
  - ✓ 最新のぜい弱性情報の確認とファームウェアの最新化等の適切な対策の実施。
- **平成28年以降も、**警察庁のサイバーフォースセンターにおいて、**「Mirai」の感染活動が観測されたことを踏まえ、ウェブサイトを通じた注意喚起を実施。**



⇒ IoT機器等の感染対策について再三周知しているものの、**現在でも、依然として「Mirai」に感染したIoT機器等が多数稼働している状況が確認**されている。