

令和4年6月20日
サイバー攻撃被害に係る情報の
共有・公表ガイダンス検討会

警察活動から見た通報・相談の重要性について

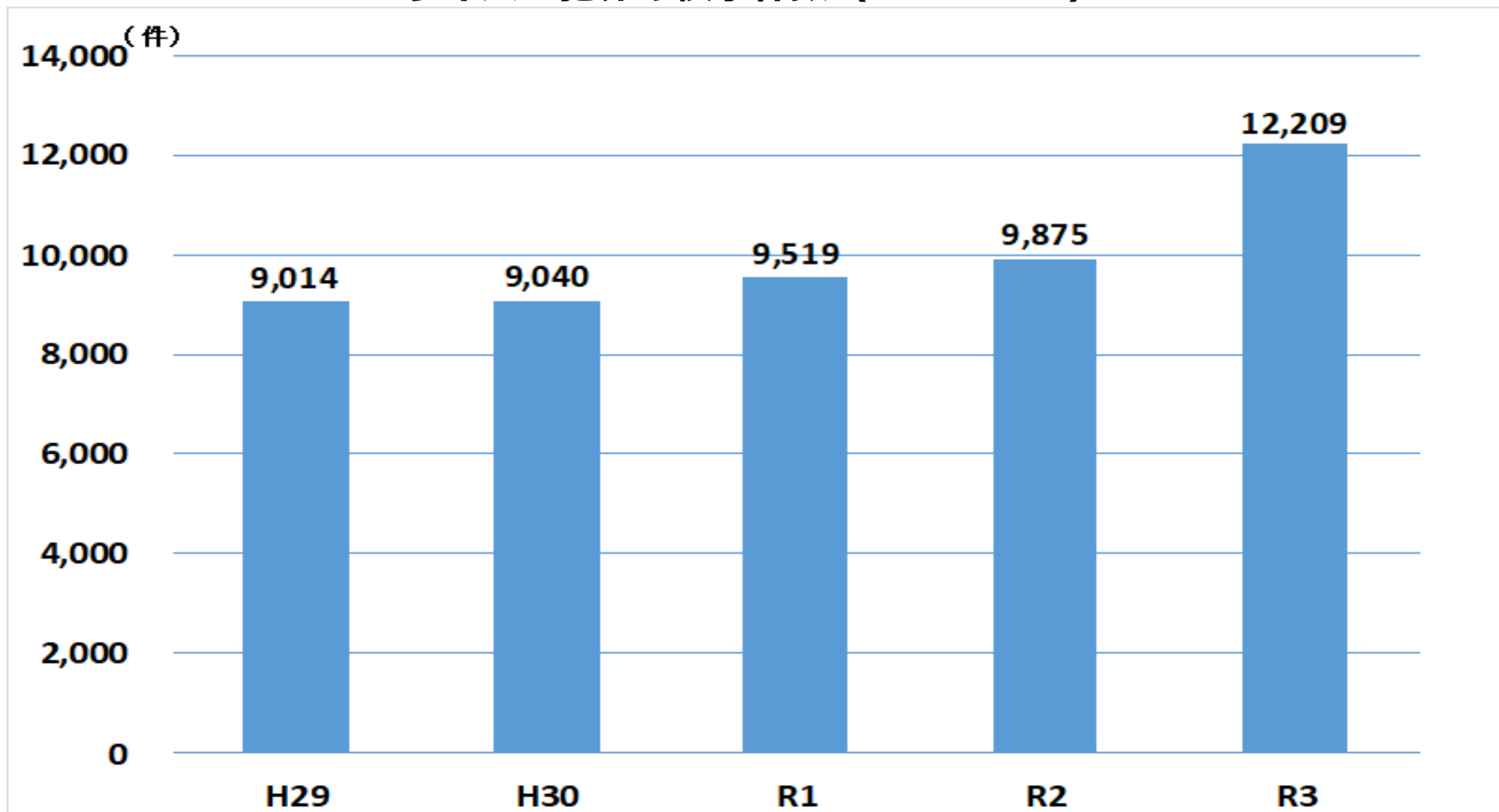
警察庁サイバー警察局
サイバー企画課

サイバー空間をめぐる脅威の情勢

サイバー空間をめぐる脅威の情勢

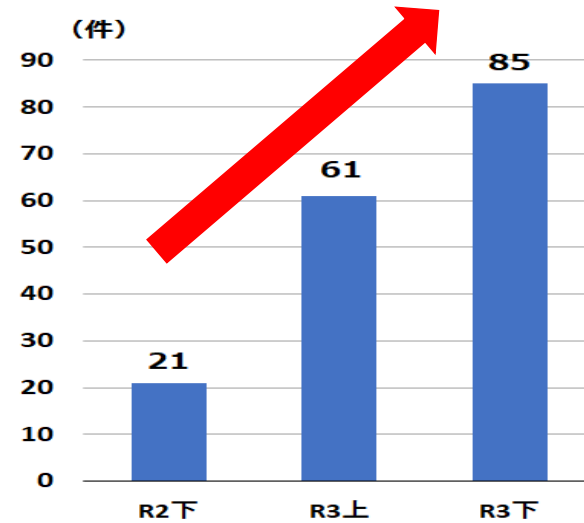
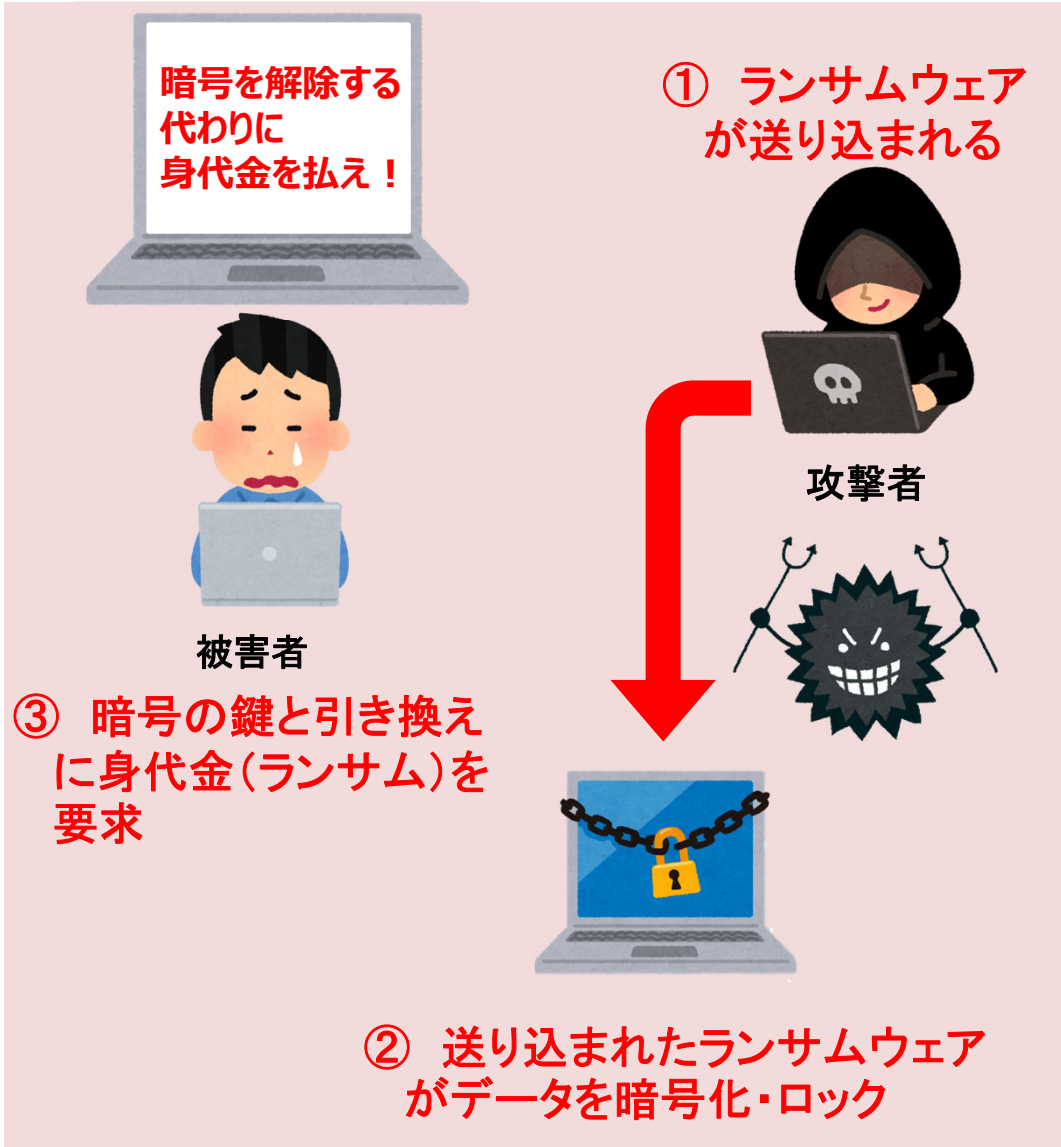
令和3年におけるサイバー犯罪の検挙件数は12,209件で、前年と比べて増加

サイバー犯罪の検挙件数（H29～R3）

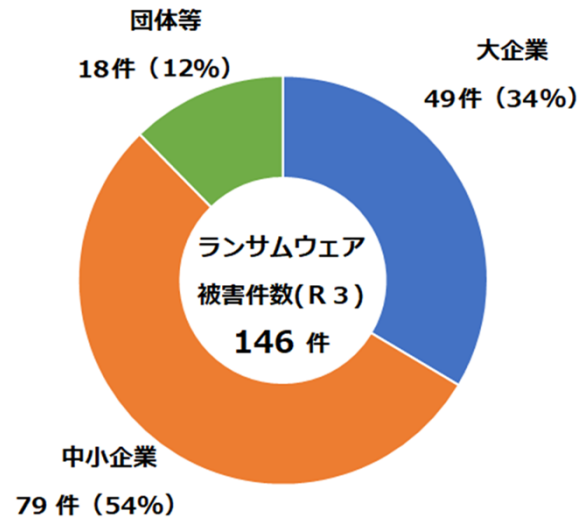


サイバー空間をめぐる脅威の情勢

我が国の企業・団体等におけるランサムウェア被害



被害の報告件数は大幅に増加



企業の規模を問わず被害が発生

サイバー空間をめぐる脅威の情勢

政府機関、重要インフラ事業者等のシステムをダウン、破壊し、又は情報を窃取する
サイバー攻撃が世界的規模で発生

我が国の情勢

内閣府等に対する不正アクセス

- 2021年1月、内閣府等が、使用するファイル共有ストレージのぜい弱性を悪用した不正アクセスを受けていたことが判明
- 不正アクセスを受けたファイルに含まれていた231名分の個人情報流出した可能性

国外の情勢

米国の水道システムへの不正アクセス

- 2021年2月、米国フロリダ州オールズマー市において、水道システムに何者かが不正に侵入し、水酸化ナトリウムの濃度を通常の100倍以上に設定しようとする事案が発生したとの報道

国家レベルで実行されたサイバー攻撃のアトリビューション

- 平成28年から29年までの間、日本のレンタルサーバの偽名契約を行ったとして、**中国共産党員の男**を検挙
- 本件捜査等を通じて、同レンタルサーバがJAXAを含む約200の組織に対するサイバー攻撃に悪用されたこと、その攻撃には、**中国人民解放軍61419部隊を背景に持つサイバー攻撃集団が関与**した可能性が高いことが判明
- 警察では、これらの組織に個別に連絡することで、被害拡大を阻止

通報・相談を受けた警察の対応

サイバー事案の捜査・実態解明の重要性

サイバーセキュリティ戦略（令和3年9月28日閣議決定）

○ サイバー攻撃に対する抑止力の向上

我が国は、悪意ある主体の行動を抑止し、国民の安全・権利を保障するため、サイバー空間における脅威について、平素から同盟国・同志国と連携し、政治/経済/技術/法律/外交その他取り得る全ての手段と能力を活用し、断固たる対応をとる。（中略）**サイバー攻撃に関する非難等の外交的手段や刑事訴追等の手段も含め、然るべく対応していく。**

【サイバー事案捜査】

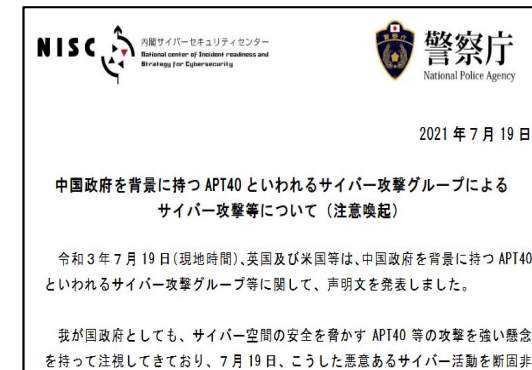
- サイバー空間の越境性を背景に、サイバー事案捜査に際しては、捜査共助等を通じた国際捜査を進めた上で、各国捜査機関等の捜査結果を補完しあうことによって連携する国際共同捜査（犯人の検挙、インフラのテイクダウン）が進められる



出典：<https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malwareemotet-disrupted-through-global-action>

【パブリック・アトリビューション】

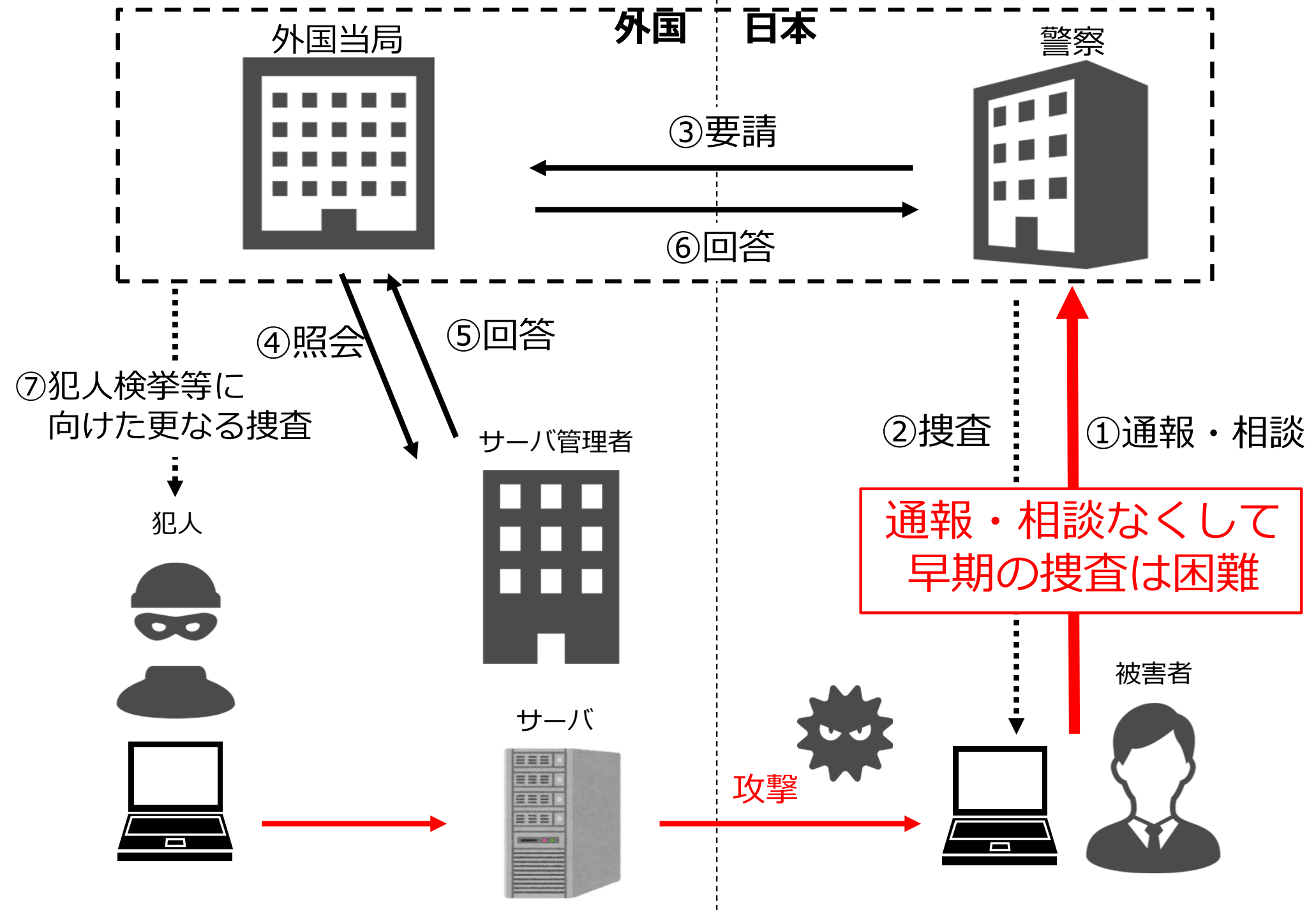
- 捜査や調査によって明らかになった情報を分析し、特定された事実から攻撃者等への非難等の表明を行う



攻撃者に将来のサイバー攻撃の意図をためらわせる上で、サイバー事案の犯人検挙を含め様々な面でコストを課すことが重要（我が国に対する攻撃への抑止力）

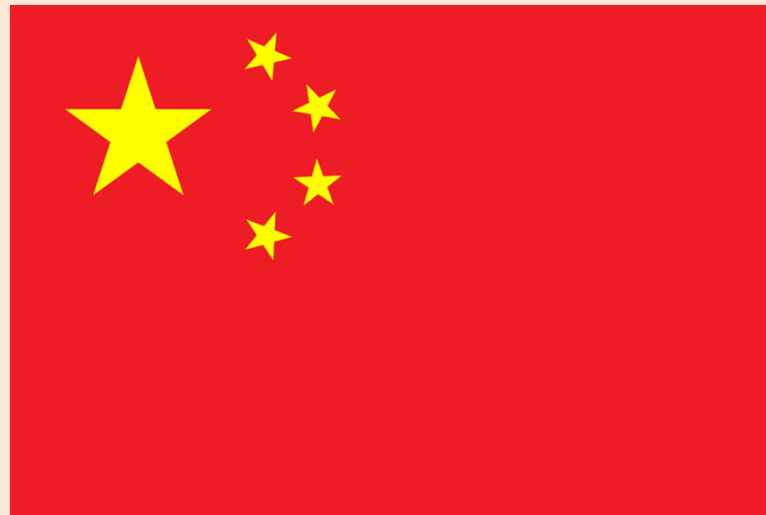
外交手段や刑事訴追には、法執行機関等での捜査・実態解明が不可欠

海外からのサイバー攻撃と捜査の仕組み



捜査機関としての実態解明

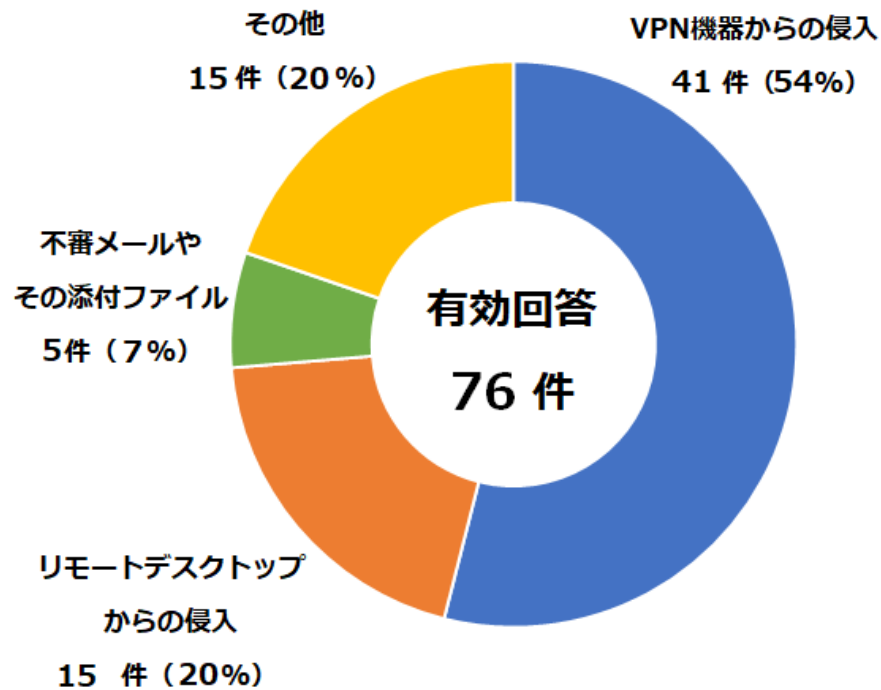
- 平成28年から平成29年までの間、住所、氏名等の情報を偽って日本のレンタルサーバの契約に必要な会員登録を行ったとして、令和3年4月、**中国共産党員の男を検挙**
- 本事件の捜査を通じ、契約された日本のレンタルサーバがJAXA等に対するサイバー攻撃に悪用されたことを把握するとともに、その攻撃には、**中国人民解放軍61419部隊を背景に持つTickと呼ばれるサイバー攻撃集団**が関与した可能性が高いことが判明



被害実態の調査

警察庁に報告された国内の企業・団体等におけるランサムウェア被害に関し、
被害実態の調査を実施

【調査結果（感染経路）】



【被害事例】

- コロナ禍において広く利用されるようになったVPN機器やリモートデスクトップ等の脆弱性を悪用されてシステムに侵入され、感染。
- 脆弱性については更新ファイルを当てるなどして最新の状態を維持していたにもかかわらず、認証パスワードが脆弱であったため、システムに侵入され、感染。

被害実態の把握という観点でも、被害に関する通報・相談が不可欠

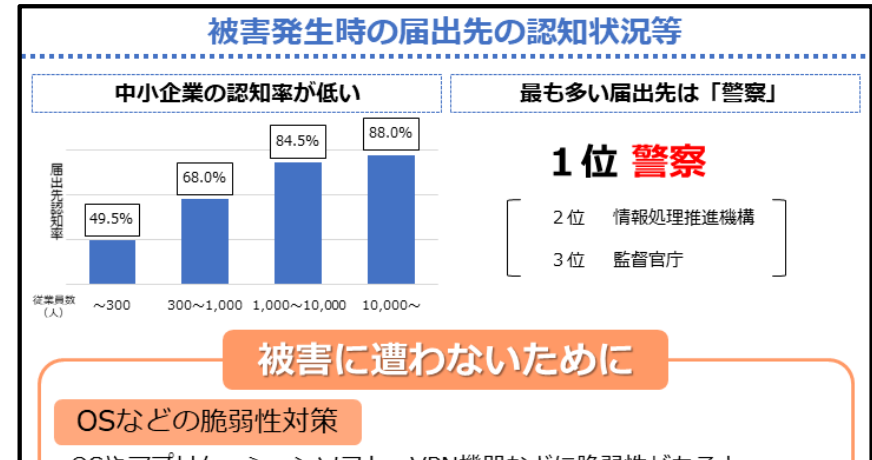
通報・相談の促進に向けた取組

警察庁ウェブサイトへの掲載

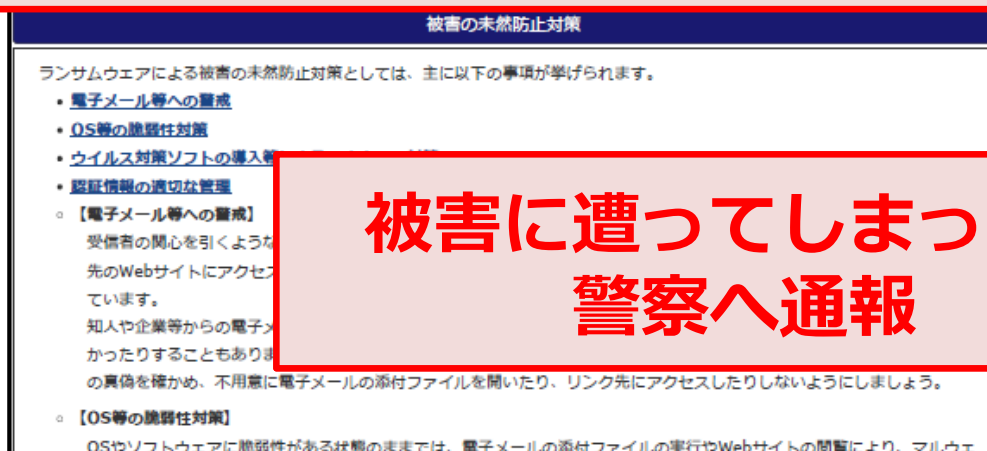
<https://www.npa.go.jp/cyber/ransom/index.html>



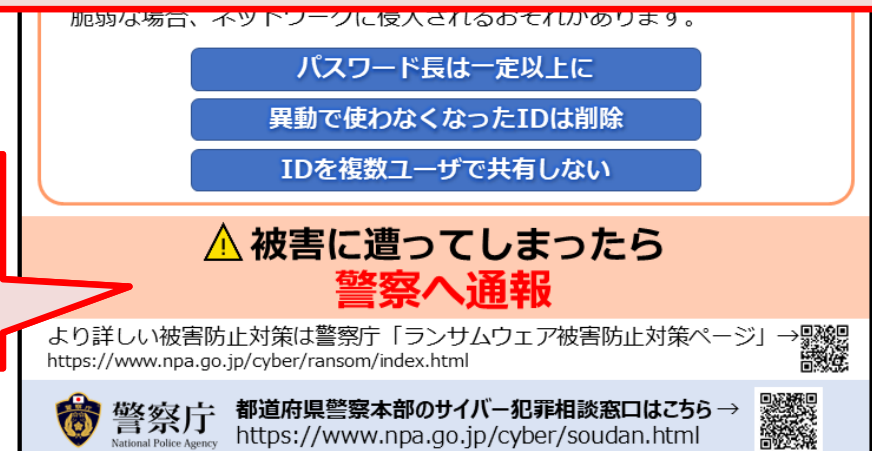
広報啓発チラシの作成・配布



ランサムウェアの被害に遭われた場合は、最寄りの警察署又は各都道府県警察のサイバー犯罪相談窓口に通報してください。



被害に遭ってしまったら
警察へ通報



通報・相談の促進に向けた取組

地域で活動する多様な主体との連携

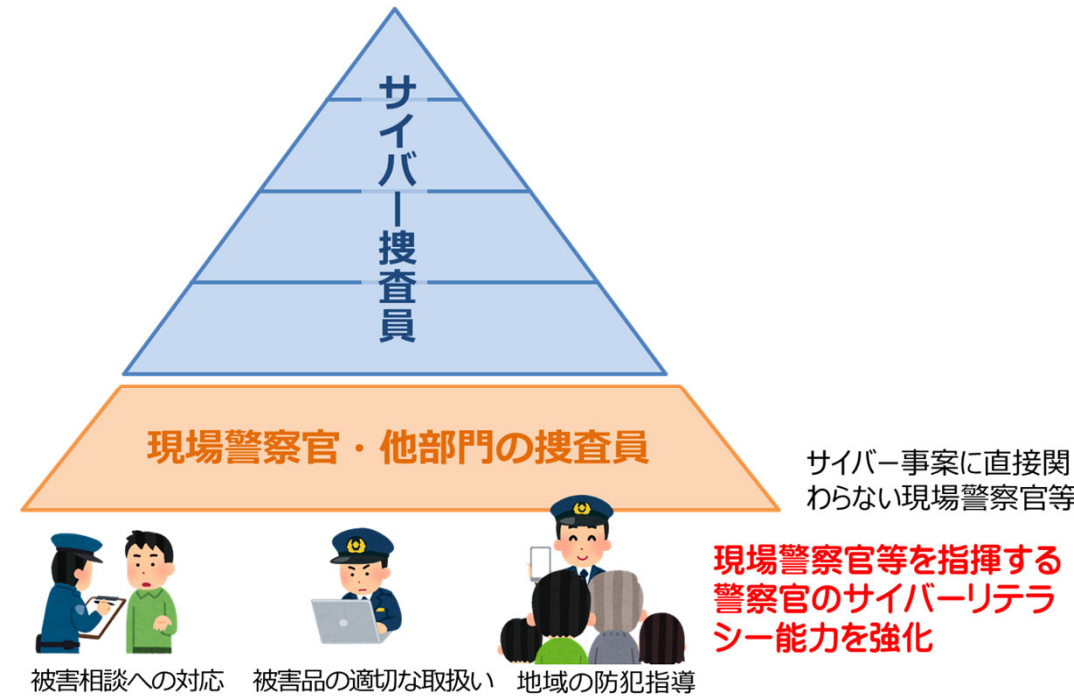
- 商工会、地域の産業組織等との顔の見える関係の構築
- 重要インフラ事業者等との間で協議会の設置
- 共同対処協定の締結 等



通報・相談の更なる促進

通報・相談対応の充実

- 全警察職員の情報リテラシー向上と部門間連携 等



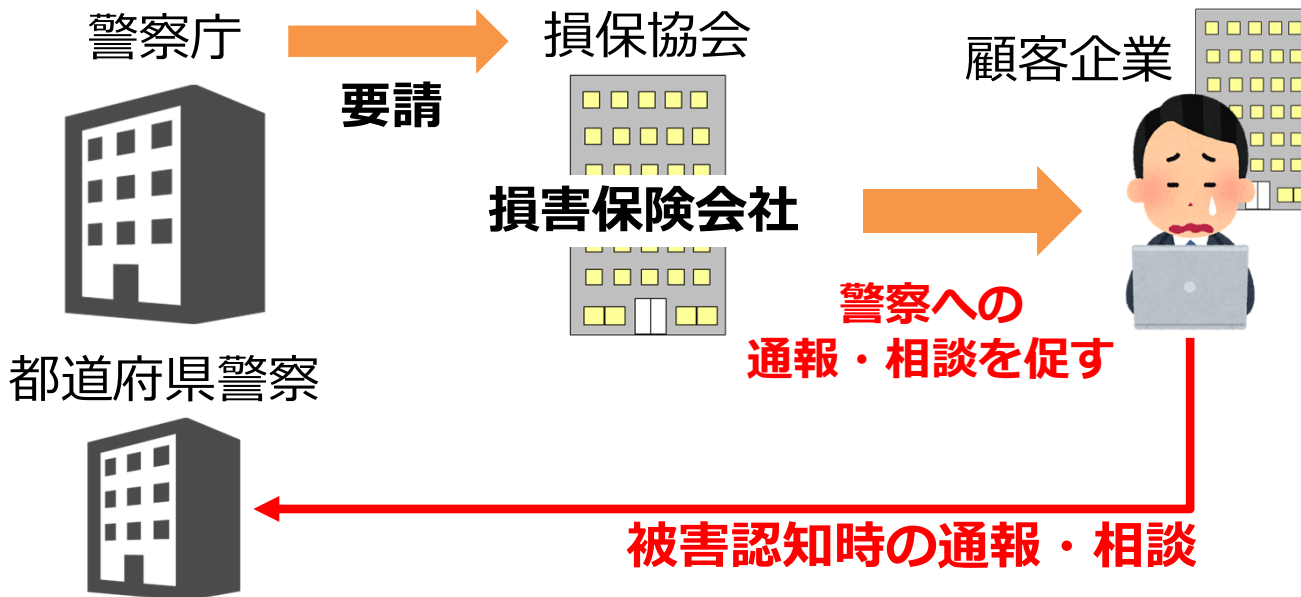
警察における
通報・相談への対応強化

通報・相談の促進に向けた取組(取組事例)

サイバー保険等を取り扱う損害保険会社との連携

サイバー事案の認知時に速やかに警察に通報するよう、
損害保険会社がサイバー保険の顧客に助言

**損害保険会社と連携し、
顧客に対して通報・相談を促す**



配布チラシ

企業の皆様へ **サイバー犯罪の被害は警察へ通報を!**

社会のデジタル化の進展に伴い、業務に関するデータをオンラインで取り扱う機会が増加する中、企業を標的としたサイバー犯罪も発生しています。

サイバー犯罪による深刻な被害

ランサムウェア

「ランサムウェア」と呼ばれるコンピュータウイルスに感染すると、パソコンやサーバに保存しているデータが暗号化され使用できなくなり、データを復元する対価として金銭を要求される。

さらには、データを盗み取った上、「対価を支払わなければデータを公開する」などと金銭を要求するダブルエクストーション(二重恐喝)という手口も発生している。

不正アクセスやコンピュータウイルスによる情報漏えい

パスワード管理の甘さやシステムの脆弱性を悪用して企業のネットワークに侵入するなどの不正アクセス、業務に関連するメールを装って送付されたメールの添付ファイルを開いたことによるコンピュータウイルスへの感染等により、個人情報や機密情報が盗み取られる。テレワーク環境を狙った攻撃も発生している。

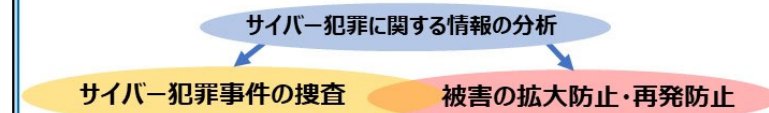
サイバー犯罪の実態を明らかにし、被害を拡大させないためには、被害を潜在化させないことが重要です。

このような被害にあわれたら、**最寄りの警察署**または**都道府県警察本部のサイバー犯罪相談窓口**へ

警察では、サイバー犯罪に対する様々な対策を行っています

警察へ寄せられたサイバー犯罪に関する情報を分析し、**事件捜査**を行うほか、**被害企業における対策に必要な情報の提供・助言**、**他の企業等への被害拡大を防止するための注意喚起**等の被害防止のための取組を行っています。

企業の皆様からの情報提供がサイバー空間の安全につながります



警察庁

都道府県警察本部のサイバー犯罪相談窓口はこちら→
<https://www.npa.go.jp/cyber/soudan.html>

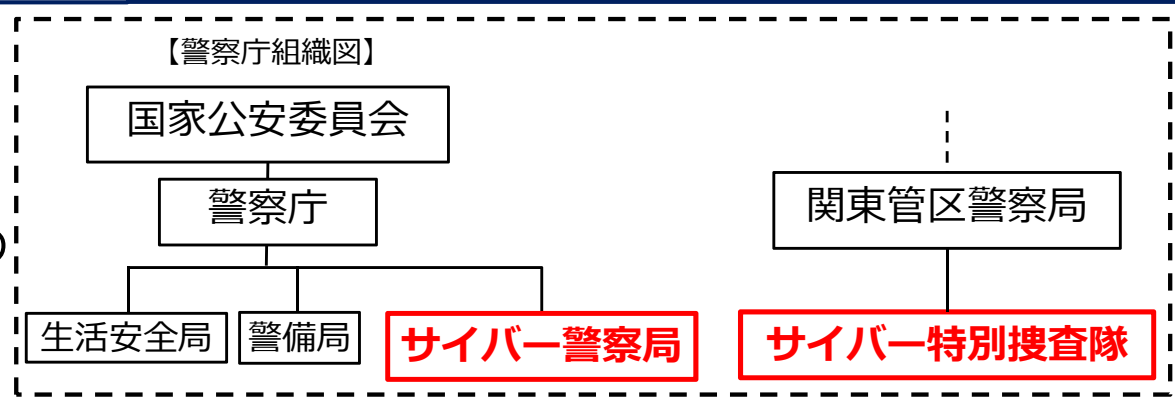


サイバー警察局・サイバー特別捜査隊の今後の取組 ～国際連携と官民連携～

サイバー警察局・サイバー特別捜査隊

サイバー警察局・サイバー特別捜査隊

- I 警察庁にサイバー警察局を設置
- II 関東管区警察局に重大サイバー事案の捜査を行うサイバー特別捜査隊を設置



サイバー警察局・サイバー特別捜査隊の取組

海外機関



警察

産業界



国際連携を通じた犯人検挙

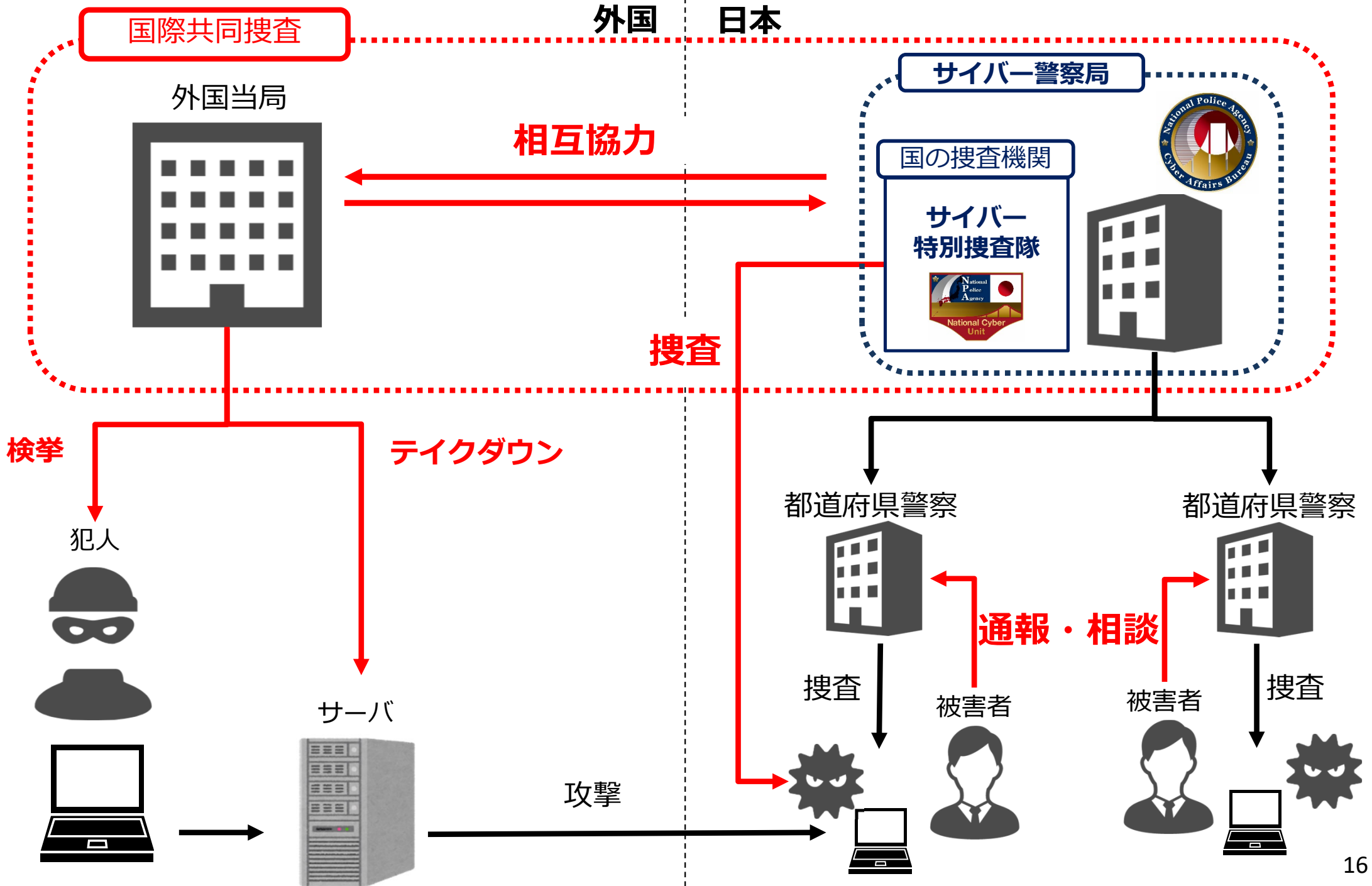


官民連携を通じた被害防止対策



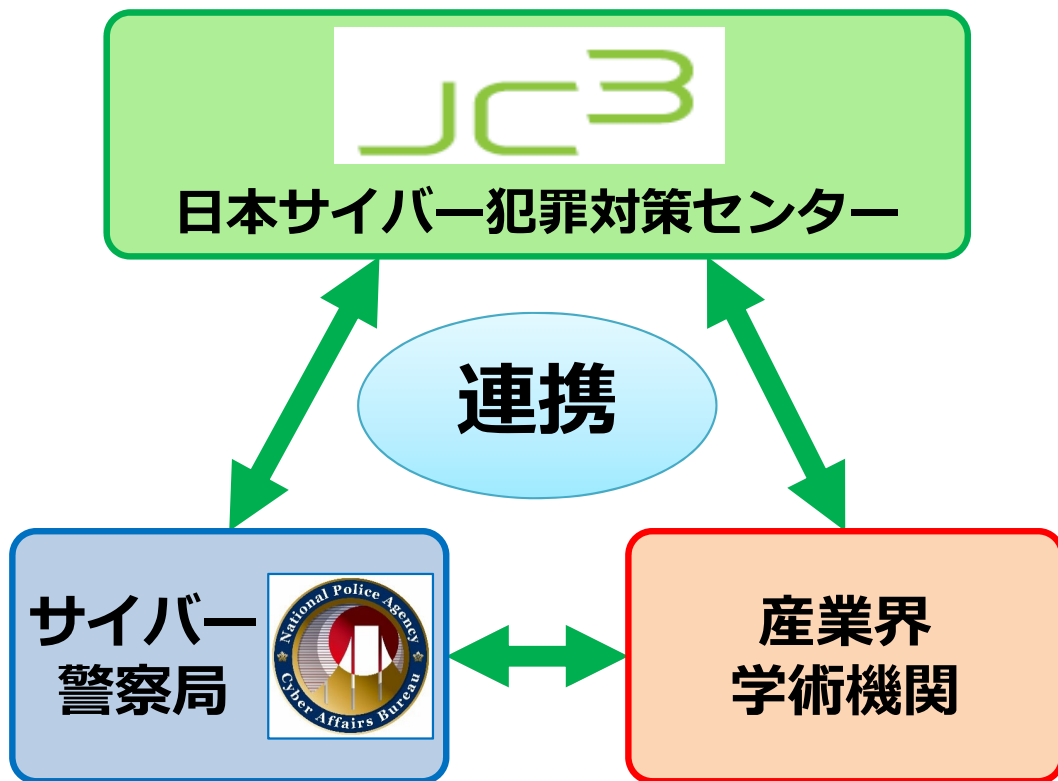
JC3
日本サイバー犯罪対策センター
JC3 : Japan Cybercrime Control Center

国際連携による犯人捜査



被害の未然防止等に向けた官民連携の推進

J C 3 を軸とした官民連携



サイバーテロ対策協議会

- 各都道府県警察において、管内の重要インフラ事業者等との間で協議会を設置
- サイバー攻撃に関する情報共有、対処訓練を実施



被害実態についての情報共有を充実化

サイバー空間の安全・安心のため、**官民連携を一層推進**

通報・相談の重要性

- サイバー事案に係る捜査
- 捜査機関としての実態解明
- 被害実態の調査
- 防犯対策への活用

いずれにおいても、
通報・相談が不可欠

サイバー警察局が中心となり、
通報・相談の促進に向けた取組を強化

国際連携による犯人検挙
官民連携を通じた被害の未然防止等の推進