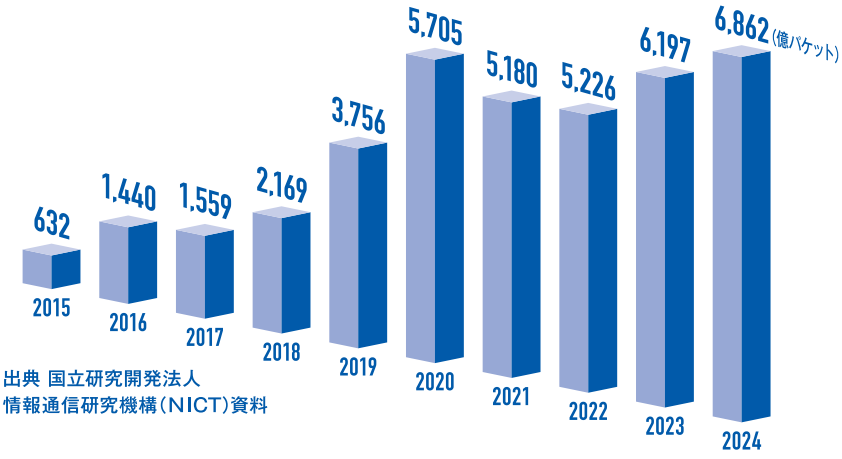
みんなで備えよう。

新・サイバー防御、はじまる。

なんで サイバー防御が 必要なの？

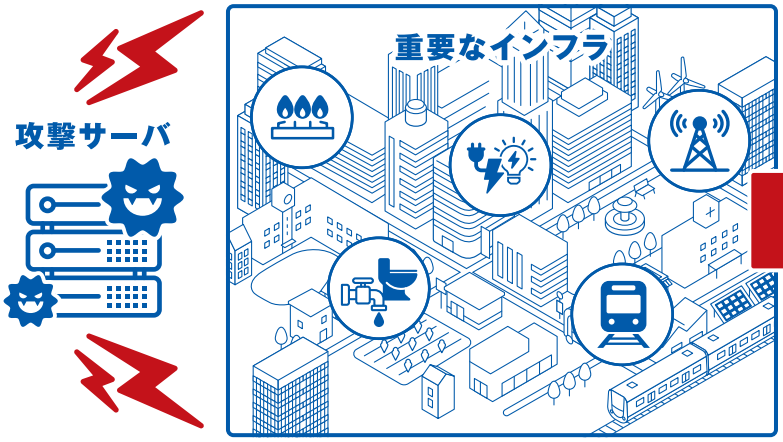
サイバー攻撃のリスクは、高まる傾向。国家を背景とする攻撃グループも存在することから、政府や自治体、インフラを担う企業などが狙われると私たちの生活に重大な危機が生じかねません。



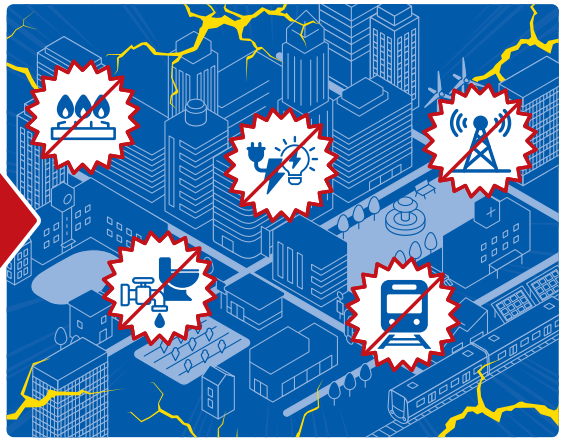
出典 国立研究開発法人
情報通信研究機構（NICT）資料

あらゆるパソコン、スマホ、サーバには 約13秒に1回の攻撃試み

サイバー攻撃の脅威は、まるで自然災害。



多数のインフラがサイバー攻撃を受けると…



被災直後のように一斉にダウン！

サイバー防御の 強化は、 世界で進む。

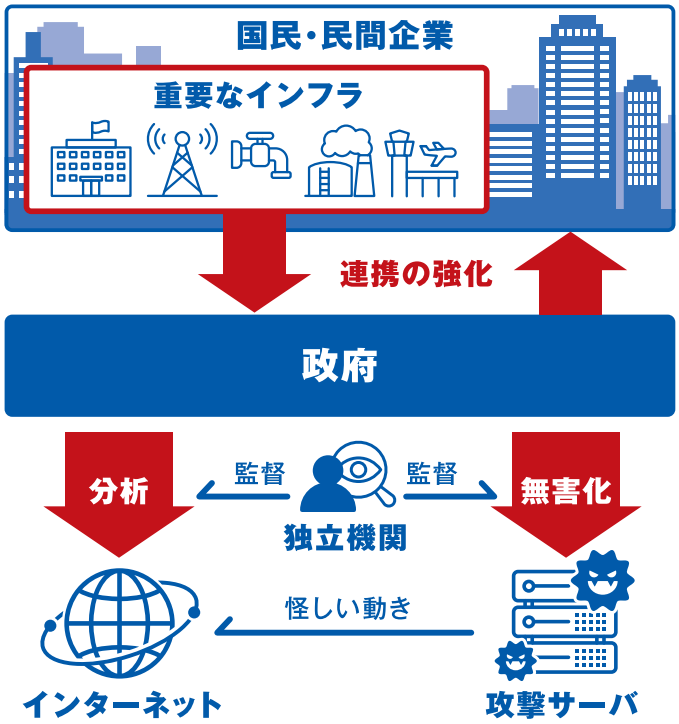
欧米主要国では、以前より、国家安全保障などの目的のために外国関係の通信情報を利用しています。また、近年、政府からの情報提供や重要インフラ事業者による報告の義務を制度化するなど、この分野での取組が先行しています。

例えるなら、新しいサイバー防御って…

官民連携を強化してサイバー空間上の「パンデミック」に立ち向かうこと。

それが、「能動的サイバー防御」

「能動的サイバー防御」NEW3ポイント!



❶官民連携の強化

重要なインフラを担う事業者が、サイバー攻撃を受けた場合などにおける政府への報告を義務化します。報告された情報は、他の情報と合わせて政府で分析のうえ幅広い組織にフィードバックし、各企業においてサイバーセキュリティの強化に活用いただけます。

❷通信情報の利用

攻撃サーバなどを検知するため、通信事業者と連携して、政府は、通信情報を取得・分析します。この際、独立機関のチェックを受けるなど、「通信の秘密」に十分配慮した仕組みとしています。

❸攻撃サーバの無害化

サイバー攻撃による重大な被害を防止するため、警察・自衛隊が、攻撃サーバなどをアクセス・無害化します。無害化に際しては、独立機関のチェックを受けるなど適正性を確保する仕組みとしています。

効果

- より**早期**にサイバー攻撃を把握
- より**効果的**にサイバー攻撃に対応することが可能に
- 攻撃サーバなどの**無害化**も可能に

それって本当に大丈夫なの？Q&A

Q1　守られるのはインフラを担う大企業だけなの？

電力などのインフラを担う大企業だけではありません。通信情報や被害報告を分析し、その結果をフィードバックすることで、地域で活躍する企業や自治体を含めた、幅広い組織のサイバーセキュリティ強化を支援します。

Q2　電話、メールの中身が見られてしまうの？

一般の利用者がやり取りする通話やメールの内容を政府が見ることはありません。分析のために利用されるのは、「IPアドレス」や「コマンド」といったコンピュータ向けの機械的な情報に限られます。これらの機械的な情報は、「コンピュータの住所」や「サーバへの指令内容」などを文字列や数値で表現したものであり、日常的な言葉とは異なるものです。

Q3　政府が都合よく通信情報を使うんじゃない？

専門の独立機関が政府による通信情報の利用を監督します。また、政府職員が通信情報を不正に利用したり漏えいしたりした場合は罰則の対象となるなど、幾重にもセーフガードを設けています。

Q4　無害化措置って、こちらからサイバー攻撃を仕掛けることとは違うの？

無害化措置は、サイバー攻撃の被害拡大を防止するための必要最小限度の措置です。サイバー攻撃により重大な被害が発生するおそれがある場合、攻撃に使用されているサーバなどにアクセスして不正なプログラムの停止・削除などを行うことを想定しています。対象となるサーバなどを物理的に破壊するなど、その本来の機能に大きな影響を与えることは想定しておらず、サイバー攻撃を仕掛けることとは違うものです。

内閣官房
サイバー安全保障体制整備準備室

能動的サイバー防御

内閣官房HP サイバー安全保障に関する取組ページ→