サイバーセキュリティ緊急対策パッケージについて

資料3

- AIの進展により、サイバー攻撃は増加し、その被害も大規模化しています。基本的な対策の不備により、多くの事案で被害につながっています。
- これは一時的なものではなく、長く続くものであり、社会全体で一丸となって対応することが必要です。
- 攻撃を受けることを前提に、社会の機能を止めない、止まってもすぐに立ち直る「サイバーレジリエンス」を確保します。
- **そのために政府も、待たずに動く。国民の皆さんとともに我が国全体の対処能力を高めていく。**

自ら率先して守りを固め、被害を待たずに動き、立ち直るまで支える

目指す方向	今回の主要な施策
社会全体で **「当たり前の備え」を整える**	• 政府のシステムをAIで総点検します。また、企業・自治体のシステムの点検を専門チームが支援します。 • 顔写真などの画像を使わずに本人確認ができる仕組みや、必要以上に個人情報を持たない仕組みを広げます。
攻撃やその兆しを **「先回りして見つけ、解明する」**	• 民間企業や海外の関係機関と協力して、サイバー攻撃に関する情報を集め、AIも活用して分析します。 • 分析で得られた情報を社会に還元し、社会全体のセキュリティ対策を後押しします。
攻撃や被害の状況に応じて **「切れ目なく、対応する」**	• 被害のおそれがある段階から実際に被害が発生した段階まで、官民の専門チームが企業の対応を支援します。 • 海外とも連携してサイバー攻撃に悪用される基盤への対応を進め、攻撃者の活動を困難にします。
被害に遭っても **「ひとりにしない」**	• どの窓口に相談しても、関係機関が連携し、必要な支援につなげます。 • 詐欺や偽情報などによる二次被害を防ぐ取組を強化します。