# 政府機関等の情報セキュリティ対策のための統一基準群の見直しについて

資料2

## 背　景

○ 最近のサイバー攻撃は、未知の不正プログラムの使用や脆弱性情報の公開直後の攻撃など、一層複雑化・巧妙化するとともに攻撃対象も拡大。国家の関与が疑われる洗練された高度なサイバー攻撃やIoT機器を踏み台とする攻撃が発生。また、世界的規模でのランサムウェアは、標的型攻撃に加え、ばらまき型攻撃の危険性をあらためて認識させた。

○ この様なサイバー攻撃から、行政サービスを守ることは重要な課題。2020年の東京オリンピック・パラリンピック競技大会の開催を控え、サイバー攻撃はさらに激しくなることも予想される。

サイバー攻撃の脅威の進展に対し、諸対策を逐次追加・改善していくという方策のみでは限界があるのではないか。新たに創出された技術をも活用し、将来的な情報セキュリティ対策の方向性を見据え、構造的に異なったアプローチが必要ではないか。

## 見直しに当たっての考え方の例　－情報セキュリティのベースラインの変化に対応－

- 事後の対処から事前の検知までといった①未知の不正プログラムによる被害の未然防止と、②サイバー攻撃を受けた際の被害の拡大防止の両面からの対策を導入することを目指すべきではないか。
- 常時セキュリティの状況を把握するため、情報システムの資産管理の自動化を行うことなどにより、監査・監視を効果的に実施することが有効ではないか。
- サイバー攻撃に対する防御技術の進展を踏まえ、仮に情報が流出しても読み取らせないような、システムの多層防御を超えた更なる安全対策の導入を目指すべきではないか。
- 府省庁とは異なり、独立行政法人等には行政事務業務だけでなく多様な業務形態があり、中間レビューを踏まえ、適切な対策を講じていくことが必要ではないか。
- 統一基準群の策定と戦略本部監査は対となるものであり、一巡した府省庁監査の結果から強化すべき点などについて統一基準群の改定に反映することが効果的ではないか。

## スケジュール