

昨今の状況

本年9月をはじめ、昨今、政府機関等における情報システムのウェブサイトが外部からの攻撃によって、改ざんされたり、一定の間、閲覧困難となるといった事案が顕在化
〔想定される脅威〕

- 情報システムの機能障害により、国民生活や社会経済上必要な**サービスの停止**
- 重要な**情報の漏えいや改ざん**

昨今の状況を踏まえ、早急に対応すべき措置

* 本年9月25日 幹事会において各府省庁に要請

1. 各府省庁において管理する情報システム等の再点検

⇒ **ウェブサイト**（外部委託等により構築・運用しているものを含む）に対しては、**既知の脆弱性を衝いた攻撃手法**が見受けられることから、以下の事項を中心に点検・実施

①改ざんの原因となる可能性が高い基盤ソフトウェアの**脆弱性情報を確認**

②**アップデートやパッチ適用等**が適切に行われていない場合は、速やかに対応

* 所管する重要インフラ事業者や独立行政法人、特殊法人、国立大学法人等に対しても同様

2. 障害・事故等の発生に備えた体制の充実強化

⇒ インシデント等の発生に際し、迅速かつ的確に対応するため、各府省庁において**CSIRT等の機能を有する体制**を早急に**整備**

3. 平素からの情報収集の強化と情報共有の徹底

⇒ NISCへの情報連絡と他の府省庁へのNISCからの情報提供の徹底（再確認）