資料 1-2

サイバー攻撃等に備え、政府機関等において取り組むべき対応について

平成 25 年 1 月 30 日
内閣官房情報セキュリティセンター(NISC)

政府機関等に対する標的型攻撃の顕在化など、サイバー攻撃による脅威が益々高まっている状況にあることから、各府省庁においては、以下の取組みを推進し、政府機関等における情報セキュリティ対策の充実強化に努められたい。

記

1. 標的型攻撃等に備えた対策の早期点検及び重点実施

標的型攻撃に備えた対策について、自組織の重要システムにおける対応状況を速やかに点検し、必要な対策があれば、可能なものから速やかに実施する。

また、予算措置を伴う重要な対策については、優先度に応じた重点的な投資計画を検討し、限られた人員・予算の中で効果的な対策を実施する。

2. 障害・事故等の発生に備えた体制の充実強化

障害・事故等が発生した際、迅速かつ適切に対処するための政府一体となった枠組みを構築するため、各府省庁は、本年度末までに CSIRT 等の機能を有する体制を整備する。

NISC は、各府省庁の PoC (Point Of Contact) 会合を開催し、CSIRT 等の機能の維持向上を図る。

※PoC:CSIRT の顔として他の CSIRT との信頼関係を構築したり、情報共有の窓口としての役割を果たす者。

3. 平素からの情報収集の強化と情報共有の徹底

各府省庁は、その業務において得たサイバー攻撃に係る情報を、可能な限り速やかに NISC に連絡する。

NISC は、収集・集約された情報をサイバー攻撃に対する初動対処、被害の拡大防止及び再発防止に活用するため、情報連絡を行った府省庁の同意を得た上で、各府省庁に対して積極的な情報提供を行う。