報道資料

平成 25 年 1 月 10 日

内閣官房情報セキュリティセンター（NISC）

情報セキュリティ対策推進会議幹事会・危機管理関係省庁連絡会議幹事会合同会議の開催について

昨今の政府機関等に対するサイバー攻撃の発生状況を踏まえ、本日午後、各府省庁の情報セキュリティ担当課長等を構成員とする「情報セキュリティ対策推進会議幹事会・危機管理関係省庁連絡会議幹事会合同会議」を開催し、情報交換を行うとともに、情報集約の重要性に鑑み、政府におけるサイバー攻撃等への対処態勢の強化等について要請しました。

その概要は以下のとおり。

1. 政府におけるサイバー攻撃等への対処態勢の強化について

サイバー攻撃に係る対策の迅速かつ的確な推進を図るため、平成22年12月27日に行った申合せ「政府におけるサイバー攻撃等への対処態勢の強化について」（情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議）の再度徹底を図りました。（別添参照）

2. 政府機関において取り組むべき今後の対応について

①政府機関における障害・事故等に備えた体制整備

各府省庁において、本年度末までに CSIRT 等の機能を有する体制を整備し、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。

各府省庁の PoC (Point Of Contact) 会合の開催。

※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。

②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。

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。

【本報道発表に関する問い合わせ先】
内閣官房情報セキュリティセンター（NISC）
（1について）
内閣参事官　水田　裕滋　　電話　03－3581－3768
（2について）
内閣参事官　三角　育生　　電話　03－3581－3959

政府におけるサイバー攻撃等への対処態勢の強化について

平成 22 年 12 月 27 日
情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議
申合せ

情報通信技術の発達した現代社会は、いわゆるサイバー攻撃の脅威にさらされており、我が国においても大規模なサイバー攻撃事態が発生する可能性がある。このため、以下の施策を講じることにより、政府におけるサイバー攻撃等への対処の取組をさらに強化していく必要がある。

1. 大規模サイバー攻撃事態等における政府の初動対処態勢の整備

○　内閣官房及び各府省庁は、相互に連携し、初動対処訓練を実施するとともに、その結果を踏まえ、対処の在り方に関する検討を行うことなどを通じ、大規模サイバー攻撃事態等が発生した際に、「緊急事態に対する政府の初動対処体制について（平成１５年１１月２１日閣議決定）」等に基づく迅速かつ適切な初動対処をとるための態勢を整備する。

2. 平素からの情報収集の強化と情報共有の徹底

○　サイバー攻撃事態に対し、政府として迅速かつ的確に対処するためには、平素から、各府省庁が収集したサイバー攻撃に係る情報が速やかに内閣官房に集約され、各府省庁等の必要な範囲に適時・適切に共有されることが極めて重要である。

・　このため、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内閣官房情報セキュリティセンターに連絡する。

・　また、内閣官房情報セキュリティセンターは、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。