報道資料

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）

情報セキュリティ対策推進会議第９回会合の開催について

本日、「情報セキュリティ対策推進会議」（議長：杉田内閣官房副長官）の第9回会合が開催され、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、再度徹底が図られました。その概要は以下のとおり。

政府機関等における最近のサイバー攻撃事例等

政府機関等に対するサイバー攻撃の発生状況を踏まえ、本年1月10日に開催された「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」において、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がなされた旨の報告がありました。（資料1参照）

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

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、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ついて再度徹底が図られました。（資料2参照）

①標的型攻撃等に備えた対策の早期点検及び重点実施

②政府機関における障害・事故等に備えた体制(CSIRT 等)の整備

各府省庁の PoC (Point Of Contact) 会合を開催し、CSIRT 等の機能を維持向上

※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

情報の機密性の要求度に応じたセキュリティ対策の重点強化

機微な取扱いが必要な情報等を扱う業務領域について、リスク評価を行い、外部の脅威（標的型攻撃等）から重要な情報を守るために必要な対策の計画的・重点的な実施に関する取り組みの方向性について報告がありました。（資料3参照）

（詳細については別添資料参照）

【本件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）
内閣参事官　三角　育生
電話　03－3581－3959

※　本会合の会議資料等は、内閣官房情報セキュリティセンターのホームページに公表しております。
http://www.nisc.go.jp/conference/suishin/index.html

政府機関等における最近のサイバー攻撃事例等について

資料1

最近の攻撃事例 （新聞報道のあった主な事案）

- ○ H24.10 GhostShellを名乗るハッカーによる世界各国100大学（日本の5大学を含む）への不正アクセス及びネット上への情報掲載に関する報道
- ○ H24.11 JAXA（宇宙航空研究開発機構）におけるウイルス感染及び情報流出の可能性に関する報道
- ○ H24.12 JAEA（日本原子力研究開発機構）におけるウイルス感染及び情報流出の可能性に関する報道
- ○ H25.1 農林水産省からのTPP関連情報流出の可能性に関する報道

CISO等連絡会議幹事会・危機管理関係省庁連絡会議幹事会合同会議（1/10）において、各府省庁等に対し下記の対応措置を要請

対 応 措 置

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
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
   - ② 標的型攻撃等に備えた対策の早期点検及び重点実施

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)

資料2

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。

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。

情報の機密性の要求度等に応じたセキュリティ対策の重点強化について　資料3

脅威の変化

内部規律違反（ファイル共有ソフトの使用、USBメモリの紛失等）による情報漏えい

外部からの攻撃（標的型攻撃等）による情報窃取等

社会経済環境の変化

IT依存度の一層の高まり

厳しい財政状況（限られた人員・予算）

従来の統一基準の役割

情報セキュリティ水準の全体的な底上げ

統一基準の見直し
リスク評価手法の策定

今後の対策強化に向けた取組

○ 実施すべき対策のベースラインを明確化し、全体的な底上げ対策を着実に実施

○ 各府省庁が業務で扱う情報の機密性の要求度等に応じた対策を重点強化

- 機微な取扱いが必要な情報等を扱う業務領域について、リスク評価を行い、外部の脅威（標的型攻撃等）から重要な情報を守るために必要な対策を検討
- 各府省庁のCISO（最高情報セキュリティ責任者）が残存リスクを把握し、限られた人員、予算の中で講ずるべきセキュリティ対策（投資）を計画的・重点的に実施