資料２－３

継続的なセキュリティ対策強化の考え方について

継続的なセキュリティ対策強化の考え方について

サイバーセキュリティ対策推進会議申合せ（案）

サイバーセキュリティ対策強化の基本的な考え方について、以下及び別添概念図の通り申し合わせる。

サイバー空間には攻撃者が存在し、特に標的型攻撃においては政府機関を狙うために攻撃者は日々その手法を進化させ、また狙った組織の弱点を探る努力を続けていることに鑑み、次の考え方に基づき、着実かつ持続的なセキュリティレベルの向上を図ることとする。

① 定常的なセキュリティ対策の改善をPDCAサイクルによって実施
② インシデント発生の際の緊急策についても確実に措置・確認・報告する
③ インシデント対応を通して得られた課題は将来的な対策の礎としてPDCAサイクルにフィードバックする

こうした取組の進捗状況は、以下により確認する。

① 定期的（年一回、例えば2月のサイバーセキュリティ月間など）な自己点検
② 第三者的な確認として、NISCによるマネジメント監査とペネトレーションテストを実施

継続的なセキュリティ対策強化の考え方

事案への対処

緊急策

措置

- システム総点検により他機関への同じ攻撃を防止
- インシデント対応体制の見直し
- システム構成を含む防護策の抜本的見直し

確認

報告

自己点検（毎年2月）

課題

定常的な改善（攻撃の進化への対応）

P

D

- システムセキュリティ対策の計画的な強化
- 監視・情報共有による攻撃の未然防止
- 研修や訓練を通した人材の育成・充実

C

A

NISCによる確認

- 監査によるポリシー遵守状況や体制の確認
- ペネトレーションテストによるシステム防御の確認