資料5

政府機関の情報セキュリティ対策の現状と課題

各府省庁の対策上の現状と課題

各府省庁の現状

- **体制**
  - セキュリティ担当者が手薄で、負荷が非常に大きい
  - 省内のシステム全体の把握や調整が困難
- **教育**
  - 全職員に座学での教育を行うのは困難。現状で、e-Learning環境もない。
  - 幹部向けの平易な教育資料が必要。
- **実施手順書**
  - 整備は遅れている。（担当者不足、システムが多い。）
- **予算**
  - 一部改善されたが、まだ省内での優先順位は低く、予算確保が難しい。
  - 内閣官房で予算・定員要求の後押し、または予算枠を確保できないかとの要望あり。

政府機関の情報セキュリティ対策の評価の視点

《情報セキュリティ対策の浸透度合を測定する評価指標》

政府機関の情報セキュリティ対策の浸透度合を測定する評価指標の一つとしては、政府機関統一基準に基づく個々の対策の実施率を用いることが可能。

対策の実施率は、特定時点のスナップショットとして表面的な様相の測定には適しているが、情報セキュリティ対策の浸透度合という意味では、各府省庁内の幹部や職員のセキュリティ意識の高さなどの測定には直接結びつかないため、それ以外の評価指標も検討する必要がある。

政府機関統一基準に基づく対策の実施率

$$\text{対策の実施率} = \frac{\text{〔その時点で対策が実施されている対象の数〕}}{\text{〔対策を実施すべき対象の総数〕}}$$

- 政府機関統一基準は、政府機関が最低限遵守すべき対策であり、その実施率は特定時点のスナップショットとして表面的な様相の測定が可能。
- 経年度比較など、時点間の差分をとることにより、変化の方向を測定可能。

注） 各府省庁の端末とウェブサーバに関する情報セキュリティ対策の総合評価については、7月25日の情報セキュリティ政策会議で実施。

例）個々の対策の実施率の例

【基本遵守事項】行政事務従事者は、アンチウィルスソフトウェア等にかかわるアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持すること。

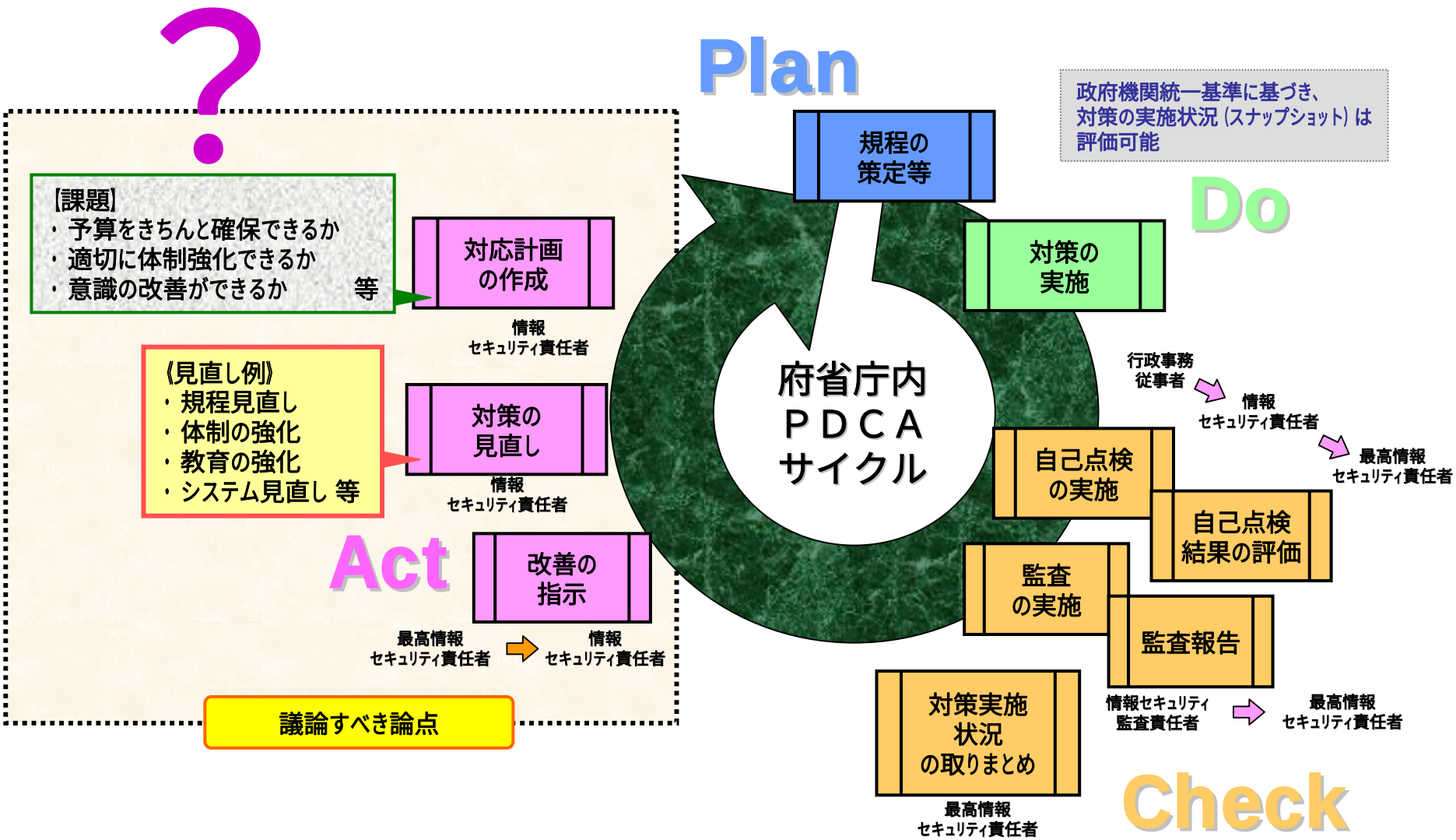
という対策に対する実施率は、〔対策の実施率〕 ＝ 〔上記対策が実施されている端末の数〕 ÷ 〔対象となる端末の総数〕で表され、例えば、1000台の端末のうち、上記対策を実施している端末が750台であれば、実施率は75％（下記の4段階の評価では、「C評価」）となる。

評価の例

A評価 ： 実施率 ＝ 100％（完全実施）、
B評価 ： 実施率が80％以上100％未満
C評価 ： 実施率が60％以上80％未満
D評価 ： 実施率が60％未満

論点：各府省庁内のＰＤＣＡサイクルをどう評価するか①

各府省庁内において、情報セキュリティ対策の見直しの進捗度合は、職員の意識や幹部のリーダーシップに依存しており、何らかの評価指標が必要。



論点：各府省庁内のＰＤＣＡサイクルをどう評価するか②

各府省庁内のＰＤＣＡサイクルのうち、「情報セキュリティ対策の見直し（Act）」について評価指標が新たに必要。

府省庁内ＰＤＣＡサイクル

	主な内容	評価
Plan	・規程の策定 （統一基準の反映） ・各種計画の策定等	規程等の内容の検査による評価が可能
Do	・対策の実施	政府機関統一基準に基づき対策の実施率（ｽﾅｯﾌﾟｼｮｯﾄ）による評価が可能
Check	・自己点検の実施 ・監査の実施　等	自己点検、監査の手法等について検査による評価が可能
Act	・改善の指示 ・対策の見直し ・対応計画の作成　等	どう評価するか 《今回、主に議論いただく論点》