

NISC



National Information Security Center

**「情報セキュリティの観点から見た
行政情報システムの望ましいあり方」と
「行政情報システムの企画・設計段階からの
セキュリティ確保に向けた取組み
(セキュリティ・バイ・デザイン[SBD])」について
【NISC素案】**

2007年12月12日

内閣官房情報セキュリティセンター(NISC)

<http://www.nisc.go.jp/>

1. 現状と課題

- ①「最適化指針(CIO連絡会議)」に基づいて行政情報システムの最適化が進められているものの、情報セキュリティの観点からは、具体的取組みが明らかにされていないのではないか？
- ②政府機関統一基準によって、各府省庁が遵守すべき事項を明確化している一方、統一基準第4部、第5部において、どのような取組みを行うことが目標達成となるのか、目標達成までの「過程」及び「過程の進め方」が明らかではないのではないか？

2. 今後の取組み(案)

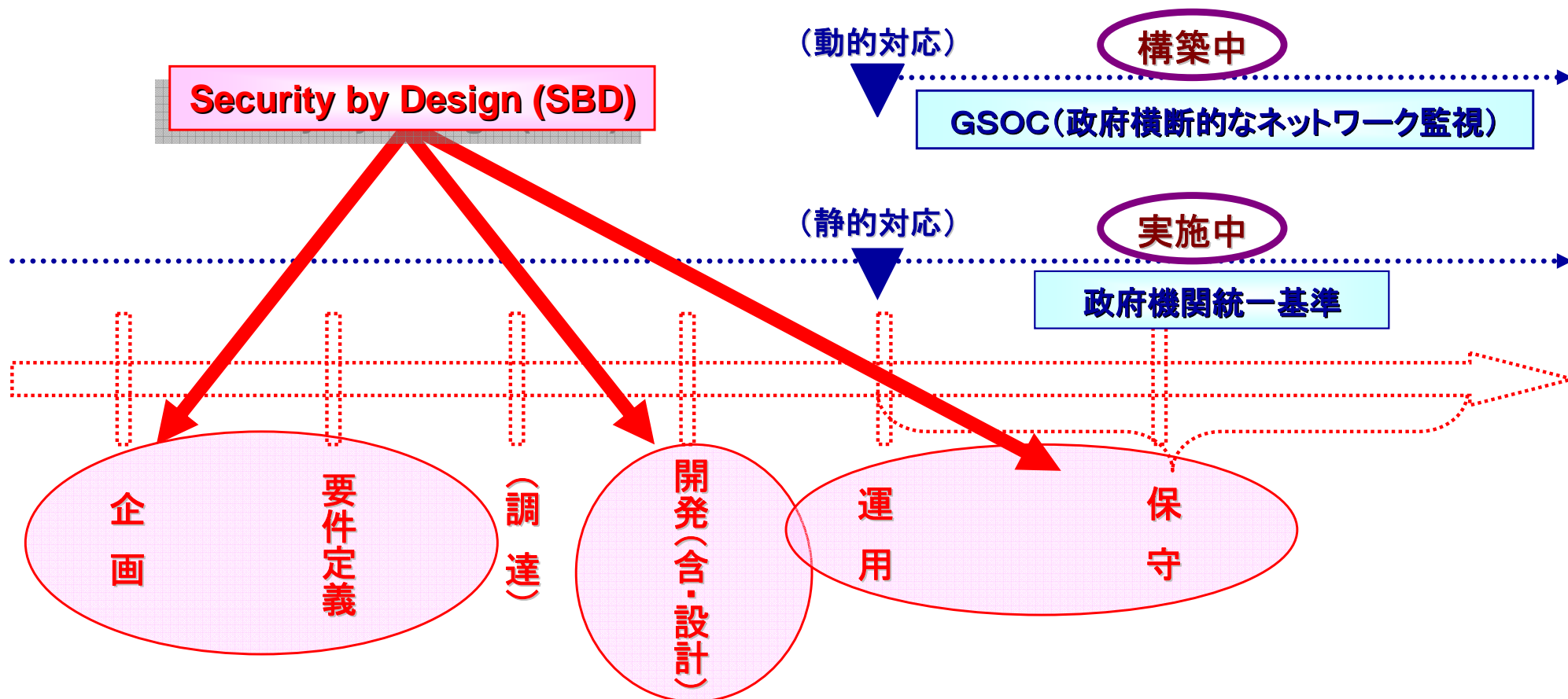
- ア)「最適化指針」の補完など、行政情報システムの情報セキュリティの取組みを進めるべく、また、
イ) 政府機関統一基準の目標の実現に必要な取組みを容易化することで、行政情報システム全体にセキュリティの観点から必要な要素を確実に盛り込むとともに、過剰・不要なセキュリティ投資を防止するべく、
- ①「情報セキュリティの観点から見た望ましい行政情報システムのあり方」について示す
 - ②新しく構築される個々の行政情報システムについて、(利便性や効率性とのバランスを維持しつつ)情報セキュリティの観点を着実かつ容易に盛り込むような取組みを進める [構築の各段階における点検リストの作成]
 - ③企画から運用・保守まで行政情報システムの情報セキュリティを担保するための方策を示しこれの実現を目指す

3. セキュア・ジャパン2007での記述(2008年度の重点施策部分)

- ・電子政府の情報セキュリティを企画・設計段階から確保する(Security by design)ための方策の強化
【内閣官房、総務省及び関係府省庁】

電子政府として構築が進みつつある各種業務・システムに適切に情報セキュリティ要件が取り入れられることは必要不可欠であり、情報セキュリティを基本コンセプトとして取り入れた情報システムの企画・設計が行われるための方策を強化する。

- ・政府機関は、政府機関統一基準及びGSOCの取組みによって、行政情報システムのシステムライフサイクルについて動的対応（外部脅威を監視し、時には緊急対応を行う）、静的対応（システムライフサイクルの各段階で着実に取組むべきことを実施する）双方の対応を図りつつある。
- ・今般、行政情報システムの企画段階から運用・保守段階まで、情報セキュリティ確保（≡統一基準の目標を満たす）のための具体的取組みを明確にするとともに、実現のための取組みを検討する。



1 「行政情報システムの望ましいあり方」(案)

- ① 機密性、完全性、可用性を保証できること
- ② 運用・保守までのセキュリティが企画段階において考慮されていること
- ③ リスク変化に応じ、構築後も柔軟に対応可能なこと
- ④ 国民の視点から安心・安全と感じられる水準なであること
- ⑤ 妥当な範囲内で障害への対応が迅速・確実なこと
- ⑥ …
- ⑦ …

あるべき
取組み

- ① 企画段階から保守段階までの一貫した取組み
- ② 客観的・合理的な取組み(行政情報システム全体にセキュリティの観点から必要な要素を確実に盛り込むとともに、過剰・不要なセキュリティ投資を防止する)

現状と
課題

現状と課題

- ① 統一基準(静的対応)……ゴール(基準)の提示に留まる(ゴールへ到る方法が不明)
- ② GSOC(動的対応)……構築中

すべきこと

- ゴール(基準)へ至るための道筋の提示。
 - (①企画から保守までの一貫した取組み(開発者や利用者も視野に入れて)、
 - ②客観性・合理性に裏付けされたシステム構築の実現、
 - ③その際は既存のスキームを最大限活用)

2 「セキュリティ・バイ・デザインの取組み」(案)

- ① 「初年度パイロットプロジェクト(試行)方式」として、試行後に取組みを正式に確定。3年計画でシステムライフサイクル全体にわたる取組みの枠組みを完成

※取組みの具体的なスケジュールについて検討・調整

- ② 取組むべき事項は、パイロットプロジェクトで実効性などについて検証後に正式確定

ア システムの類型化の妥当性

(特に、機微系システムは担当府省庁の自主的・高水準な取組みの推進を期待)

※パイロットプロジェクトにむけ、類型化を行うための「検討軸」を検討・調整

イ 企画から保守までの点検の妥当性

- ・手引書(参考)
- ・企画段階
- ・要件定義段階～開発段階
- ・運用段階～保守段階
- ・コーディング

- ③ 取組み主体

ア システム構築担当府省庁及び開発者による自己点検

イ 発注者及び開発者以外の政府内第三者による確認 [機微系は当然に除く]

※既存のスキームを最大限活用した効果的・効率的なスキームの検討・調整