情報セキュリティを企画・設計段階から確保するための方策（SBD(Security by Design)）

問題認識： 行政情報システムの企画・設計段階から情報セキュリティ対策を考慮すべき

SBD検討会構成員
（座長）東工大 山岡准教授
（委員）大手ベンダー、システム関連事業者関連団体、府省庁CIO補佐官　等
（オブザーバ）関連府省庁　等

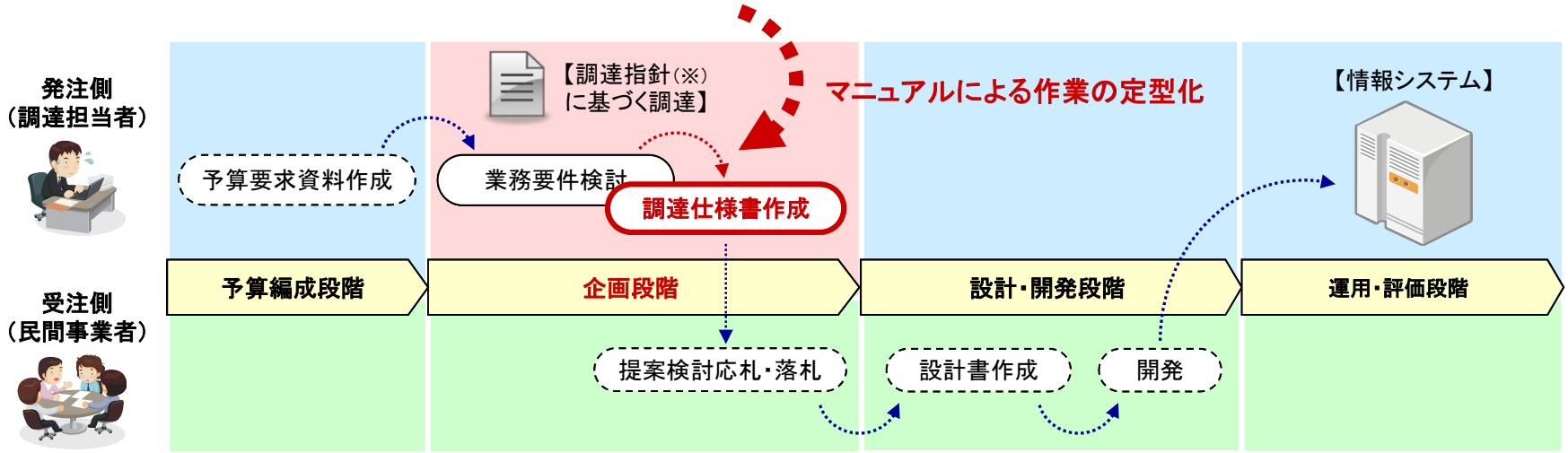
『情報セキュリティを企画・設計段階から確保するための方策に係る検討会（SBD検討会）』を設置

■ 検討課題
- ✓ 調達仕様書の「**情報セキュリティ要件の不明瞭さ**」から、調達者と供給者の合意形成に支障を来す。
- ✓ 結果として、「**不公平な調達**」、「**過度なセキュリティ対策**」、運用開始後の「**セキュリティ事故**」を招くおそれ。

■ 解決方針
- ✓ 調達担当者が調達仕様書作成時に「**情報セキュリティに係る仕様**」を適切に組み込める方法を確立する。

検討成果

『情報システムに係る政府調達におけるセキュリティ要件策定マニュアル』
- 調達担当者がシステム特性に応じて「**調達仕様書にセキュリティ要件を記載する方法**」を解説
- 「**対策要件集**」及び「**対策要件選定作業の定型化**」等のツールによる調達担当者の支援



※ 調達指針：情報システムに係る政府調達の基本指針（H19.3.1 CIO 連絡会議決定）

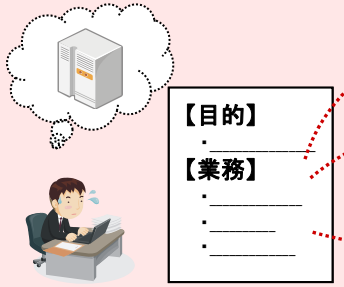
『情報システムに係る政府調達におけるセキュリティ要件策定マニュアル』による作業の定型化

【マニュアル利用場面】 調達指針に基づく調達において、調達仕様書に盛り込むべきセキュリティ要件を検討する際に以下の作業を行う。

■ 業務要件の検討 （対象業務をシステム概要図にまとめ、定型設問に回答する）【※ 他の方法による代替可】

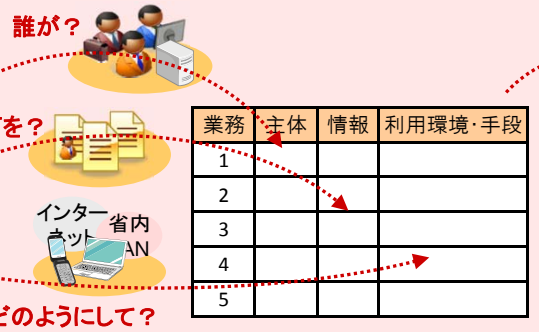
ステップ1

目的及び業務を洗い出す



ステップ2

業務の特徴を3つの観点から整理する



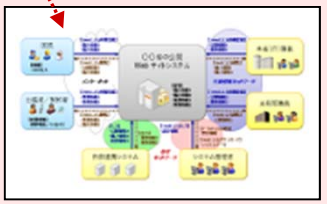
業務	主体	情報	利用環境・手段
1			
2			
3			
4			
5			

ステップ3

システム概要図を表記ルールに基づいて作成し、要件を俯瞰する

表記ルール

【システム概要図】



ステップ4

定型設問により業務要件を詳細化する

【定型設問】

人数規模は？
1日の利用時間帯は？
情報の提供範囲は？

■ セキュリティ要件の策定 （業務要件を判断条件にあてはめ対策要件を決定する）

ステップ5

判断条件を判定し、対策要件ごとの実施レベルを検討する

ステップ1～4の検討結果

判断条件	結果
A	○
B	○
C	×
：	：

外部アクセスはあるか？
重要度の高い情報を扱うか？

判断条件の結果から、対策要件集の各対策要件の実施レベル（低位以下か、中位以上か）を機械的に決定

対策要件	実施レベル
不正通信の遮断	低位
マルウェア感染防止	中位～高位
証跡の管理・蓄積	低位
：	：

【対策要件集（※）】

ステップ6

実施レベルを確定し、対策要件を決定する

対策要件集の解説を参考にし、各対策要件の実施レベルを最終決定

対策要件	実施レベル
不正通信の遮断	低位
マルウェア感染防止	中位
証跡の管理・蓄積	低位
：	：

【対策要件集】

ステップ7

調達仕様書に反映する

対策要件集に記載された仕様書記載例から実施レベルに対応するものを参考にして反映

【対策要件集】 【調達仕様書】

（※）侵害対策、不正監視等の24種類の対策要件、3段階の実施レベル（対策の強度）に応じた仕様書記載例に関する解説