

平成 23 年 4 月 28 日  
内閣官房情報セキュリティセンター(NISC)

## 「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」 の策定について

情報セキュリティ2010(平成22年7月22日情報セキュリティ政策会議決定)において、情報システムに係る政府調達に関して、情報セキュリティ対策が適切に組み込まれる仕組みの構築及び組み込むべき情報セキュリティ要件の取りまとめを行うとされました。

今般、「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)に係る検討会」(座長:山岡克式・東京工業大学大学院理工学研究科准教授)において、「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」等を取りまとめましたので、お知らせいたします。

### 1. 策定の背景

政府機関の情報システムにおいて適切に情報セキュリティ対策を講じるためには、情報システムのライフサイクル(企画・設計・開発・運用・廃棄)において、上流の企画段階から情報セキュリティ対策を考慮し、調達仕様にセキュリティ要件を適切に組み込むことが求められます。しかしながら、セキュリティ要件は曖昧、過不足な調達となりやすく、システムの特性に応じた調達となるよう注意が必要です。

こうした問題意識から、平成19年3月に、経験・知見を有する有識者やベンダーを交えて、「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)に係る検討会」を設置し、検討を開始しました。

### 2. 課題の抽出と解決策

上記検討会での議論において、調達仕様におけるセキュリティ要件の曖昧さや過不足は調達側と供給側の相互理解と合意形成を阻害し、調達側と供給側の双方に不利益を発生させる要因となることが確認されました。調達仕様におけるセキュリティ要件の曖昧さや過不足の発生は、特に仕様を作成する調達側の政府職員の情報セキュリティに対する知見に依存し、「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」を招かないようにする必要があります。

こうした課題を解決するために、情報システムの調達において調達側である政府職員がシステムの調達仕様書を作成するにあたり、必要な情報セキュリティ要件を定型化された作業によって導出できるよう支援するマニュアルを策定しました。また、本マニュアルを

供給側である民間事業者等も活用することで、システムのセキュリティ対策が相互により明確化されます。現状、全府省庁で約2000存在する政府情報システム全体の適切な情報セキュリティ対策につながっていくものと期待できます。

### 3. 成果物

◎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

- 「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」 [PDF](#)
- 「同 マニュアル 付録A. 対策要件集」 [PDF](#)
- 「同 マニュアル 付録B. 政府機関統一基準群対応表」 [PDF](#)
- 「同 マニュアル 付録C. マニュアル活用例」 [PDF](#)
- 「同 マニュアル 付録D. 用語解説」 [PDF](#)
- ・「同 マニュアル活用ワークシート」 [XLS](#)
- ・「同 マニュアル活用ワークシート」(活用例) [PDF](#)

◎「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」概要

[PDF](#)

◎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 報告書

[PDF](#)

### 4. 参考

情報セキュリティ2010（平成22年7月22日情報セキュリティ政策会議決定）

[http://www.nisc.go.jp/active/kihon/pdf/is\\_2010.pdf](http://www.nisc.go.jp/active/kihon/pdf/is_2010.pdf)

国民を守る情報セキュリティ戦略（平成22年5月11日情報セキュリティ政策会議決定）

<http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf>

#### <連絡先>

内閣官房情報セキュリティセンター

（政府機関総合対策促進担当）

参事官補佐 門司、中嶋、主査 渡邊

住所：〒100-0014 東京都千代田区永田町 2-4-12

E-Mail：i.nisc\_SBD@cas.go.jp