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

平成 23 年 3 月

巻頭言

高度情報社会である現代社会を支える、欠くことのできない基盤インフラストラクチャとして、インターネット技術を中心としたコンピュータシステムが、現在その中心的役割を担っている。しかし、電気、水道、ガス、電話、鉄道などといった、明治以来100年以上の時間をかけて進歩を続け、人々への安定したサービス供給を実現してきている既存のインフラストラクチャに対し、1960年代に研究開発が開始され、以来主に研究者や技術者だけに利用されてきたインターネット技術は、まだ技術的には十分成熟したいわゆる枯れた(安定した)とは言い難い発展途上の技術にも関わらず、一般にWindows95登場以降といわれているように、わずかこの10年余りの短い期間に、急激に広く市民レベルまで普及し利用されるようになった。その結果、以下のような問題が顕著になってきている。

まず、巨大なシステムが内包する不具合の問題がある。

一般に、巨大なシステムになればなるほど、そのシステムを構成するハードウエアやソフトウエアには、開発時に予期しない不具合(バグ)が混入する。この不具合を解消するためには、十分な試験による不具合検出とそれに対する対応が必要であり、多くの人手および期間、資金が必要となる。しかし、昨今のインターネット技術によるコンピュータシステムは、そのような試験と不具合対応が時間をかけて十分になされていない状況で、急激に普及したため、多くのバグを含んだまま社会インフラストラクチャの一部となってしまった。

これらのバグのうち、一般に「セキュリティホール」と呼ばれる、悪意のある第三者がこの不具合を利用することにより、システムの破壊や不正アクセス、情報流出などにつながるバグの存在が、特に問題となっている。もちろん、開発元ではこれらのバグを解消するための努力が日夜行われ、発見されたセキュリティホールを修正するパッチが発行されてはいるが、それ以上に急激にシステムが発展を続け、システムやソフトウエアの規模が拡大すると共に、新たな機能が日々追加されている昨今では、それに伴う新たなバグの混入を防ぐことは不可能に近く、バグのない安全・安心なシステムを実現するのは現状非常に困難である。

次に、コンピュータシステムの運用体制に関わる問題がある。

先に挙げた、電気、水道、ガス、電話、鉄道など、従来の社会インフラストラクチャは、その運用管理は、企業や公益法人など、技術的に信頼のおけるいわゆる専門(プロ)集団によりなされており、ユーザの側はその利用に際して、特段の知識や能力は必要とされていない。これに対し、インターネット技術によるコンピュータシステムは、ユーザ側のLANやPCの運用管理にもそれなりに知識や能力が必要である。さら

に、近年そのようなシステムの価格が下がり、企業や家庭に容易にシステムの導入が可能となった反面、大量に導入されるシステムそれぞれの運用管理に、十分なそれ専門の人手や予算をかけることができず、それらの運用管理が、特段の知識や能力を持たない一般ユーザの手に任されているのが、現状である。その結果、不十分なシステム設定や設定ミスが原因で、上述のバグとは異なる、ヒューマンエラーによる「セキュリティホール」が生じ、大きな問題となっている。

以上のように、インターネット技術を中心としたコンピュータシステムは、他の従来の社会インフラストラクチャとは異なり、運用管理にそれなりの知識や能力をユーザ側に要求するが、実際のところ官公庁の現場ではそのような人材は不足しているのが現状である。そのため、官公庁によるこのようなシステムの調達導入時にも、必ずしも調達側である官公庁側にそのような人材が参画しているとは限らない。その結果、調達側の知識や認識不足により、セキュリティ対策の十分なされていないシステムが導入され、後日セキュリティ事故に遭遇する事例が見受けられる。また、知識や認識不足により、セキュリティ対策を適切に考慮したシステム設計を調達側が行えないため、そのようなセキュリティ攻撃の驚異に過剰に反応した結果、網羅的に必要以上のセキュリティ対策を導入することとなり、その分調達コストが必要以上に大きくなってしまう事例も見受けられる。

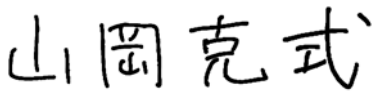
このような現状をふまえ、官公庁のシステムで適切なセキュリティを実現するためには、システムに関する特段の知識や能力を持つ人材の存在を前提とせずに、調達システムの企画・設計段階から情報セキュリティ対策を適切に組み込む必要があることから、そのような方策の検討を目的として、本検討会「情報セキュリティを企画・設計段階から確保するための方策に係る検討会」は設置された。本検討会には、システムのセキュリティ設計に関する経験や知見を有する有識者のみならず、官公庁の調達に対して応札・納入側の立場となる複数のシステム関連事業者にも検討会構成員やオブザーバとして御参画いただき、適切なセキュリティを適正な価格で設計実現することにより、ややもすると利害が相反する立場にある調達側と応札側の双方にとって好ましいWin-Win状態の実現を目指して、単なる双方の立場からの利益代表としてではなく、相互の立場を尊重しながら本音で意見をぶつけ合い、検討を重ねてきた。その結果をここに報告書としてまとめるものである。

本検討会での議論の結果考案された「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」は、政府調達において、特段の知識や能力を持つ人が仕様策定に参画していなくても、適切なセキュリティ要件の策定を可能にするマニュアルであり、調達側のセキュリティ要件策定支援ツールと位置づけられるとともに、専

門的知識や能力の差異から調達側と応札側の間で生じる、策定されたシステムで実現するセキュリティ要件に関する認識のずれを解消し、適正価格で適切なセキュリティの実現を可能とする。

セキュリティ事故の被害は、直接攻撃された組織のみにとどまらず、影響が世界中に及ぶ可能性もある。本報告書、および本検討会の成果物であるセキュリティ要件策定マニュアルが、広く官公庁の調達に、調達側応札側双方によって利用されることにより、セキュリティ事故防止の実現に大いに寄与することを、検討会一同心より願っている次第である。

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 座長
山岡 克式



目次

第1章　検討の背景と目的

1.1. 検討の背景

行政機関における電子政府をはじめ様々な関連分野において情報通信技術の積極的な利活用が進む中、情報システムは業務推進において不可欠な存在となっており、システム化対象となる業務はより大規模化、複雑化してきている。こうした情報通信技術と業務活動との密接度の高まりにより、システム化に係る要件において一層の緻密化が求められるとともに、それまでの局所的な業務効率化と比べて、上流工程で決めなければならない事項が複雑化かつ増加してきている。

こうしたことから、これまで主として各府省情報化統括責任者（CIO）連絡会議において、電子政府構築をはじめとする政府機関の情報システムに係る調達のあり方や見直しの方針について検討を行い、指針等を策定してきた。平成15年には「電子政府構築計画」を策定し、国民の利便性・サービスの向上のための取組、ITを活用した業務改革を行うための取組、電子政府の推進体制の整備・充実のための取組等を進めるとともに、その後、平成18年には業務・システムのその時点におけるあるべき姿への到達を計画的に推進するための指針として「業務・システム最適化指針（ガイドライン）」を策定している。さらに、情報システムに係る政府調達において、適切な工程の進捗管理や成果物の品質管理を目指し、最小限のコストで戦略的な調達を行うために、平成19年には、「情報システムに係る政府調達の基本指針」が策定されている。

情報システムに係る調達全体において上記のような取組が進められる一方、非機能要件のうち特にセキュリティ要件は曖昧、過不足な調達となることが多く、結果としてシステムの実態によらず全網羅的な過剰なセキュリティ対策や設計・開発工程での手戻り、運用開始後のセキュリティ事故等の問題を生じさせる可能性がある。

そこで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、企画段階から情報セキュリティ対策を考慮し、セキュリティ要件を適切に組み込むことが必要不可欠との認識のもと、情報セキュリティ政策会議において「セキュア・ジャパン2007」の決定以降、「第二次情報セキュリティ基本計画」の決定、「国民を守る情報セキュリティ戦略」の決定により、継続して方策の検討及び取組を進めることとなった。

同戦略の下、毎年の政府の重点施策の年度計画として情報セキュリティ政策会議で決定された「情報セキュリティ2010」では、「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」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」等がとりまとまったところである。

1.2. 検討の目的

前述の背景の中、行政情報システムにおける情報セキュリティ対策を考慮したライフサイクル管理の強化の実現に向け、企画・設計段階から適切に情報セキュリティ対策を組み込む方策を検討するため、2009年3月、内閣官房情報セキュリティセンターを事務局とし、関連分野の経験・知見を有する有識者やシステム関連事業者を構成員とする「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」（以下「SBD検討会」という。）が設置された。

SBD検討会の開催経緯と構成員について以下に示す。

表 1　SBD 検討会等の開催経緯

開催日	会合	審議事項
平成21年3月13日（金）	第１回	・システム整備のセキュリティ機能に関わる課題の抽出と今後の展開アプローチについて
平成21年8月5日（水）	第２回	・今年度の検討計画及び今後の要検討課題等説明 ・関連活動紹介
平成22年2月3日（水）	第３回	・これまでの作業状況に関する説明 ・関連研究の紹介 ・関連事業の紹介
平成22年3月19日（金）	第４回	・リスク要件リファレンスモデル（ＲＭ）について ・検討会関係者からのご意見報告 ・政府機関のシステム調達におけるＲＭの活用 ・関連する取組紹介（非機能要求グレード検討会）
平成22年6月25日（金）		第１回　各府省庁説明会
平成22年6月30日（水）	第５回	・情報システム・ソフトウェア取引におけるトラブル事例について ・情報システムの企画段階（調達段階）におけるセキュリティ要件の導出方法に関する検討
平成22年10月29日（金）	第６回	・事例紹介「最近のサイバー攻撃手法と考えられる対策」 ・情報システムの企画段階（調達段階）におけるセキュリティ要件の導出方法に関する検討（2）
平成23年1月18日（火）	第７回	・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）概要 ・マニュアル活用事例

開催日	会合	審議事項
平成23年1月21日（金）		第２回　各府省庁説明会
平成23年1月31日（月） ～ 平成23年2月21日（月）		パブリックコメント
平成23年3月30日（水）	第８回	・検討会報告書（案）について ・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（案）について

構成員等名簿

（50音順　敬称略）

座長	山岡　克式	東京工業大学大学院理工学研究科 集積システム専攻　准教授
	有村　浩一	Telecom-ISAC Japan　企画調整部　部長
	一條　倫子	一般社団法人電子情報技術産業協会 インダストリ・システム部　部長代理（情報システム担当）
	鵜飼　裕司	独立行政法人情報処理推進機構 セキュリティセンター
	大高　敏孝	富士通株式会社品質保証本部品質マネジメント推進統括部長 （任期：2010 年 12 月迄）
	尾股　達也	一般社団法人情報サービス産業協会企画調査部長
	甲斐　成樹	独立行政法人情報処理推進機構 セキュリティセンター
	柏木　雅之	独立行政法人情報処理推進機構 ソフトウェア・エンジニアリング・センター エンタプライズ系プロジェクト　研究員
	勝田　正彦	株式会社日立製作所 情報・通信グループ 戦略統括部　副参事
	金谷　延幸	株式会社富士通研究所セキュアコンピューティング研究部主任研究員
	佳山　こうせつ	富士通株式会社 クラウドセキュリティセンター インテグレーション部　情報セキュリティアドミニストレータ
	川口　修司	三菱総合研究所　情報技術研究センター クラウドセキュリティグループ
	楠　正憲	マイクロソフト株式会社 技術統括室 最高技術責任者(CTO)補佐
	窪田　文啓	外務省情報化統括責任者（CIO）補佐官
	篠原　郁二	日本電気株式会社 政策調査部　担当部長
	鈴木　律郎	一般社団法人情報サービス産業協会 企画調査部　技術課長
	高倉　弘喜	名古屋大学 情報基盤センター 情報基盤ネットワーク研究部門
	高橋　正和	マイクロソフト株式会社　チーフセキュリティアドバイザー
	只野　完二	株式会社日立製作所 情報・通信システム社 プロジェクトマネジメント統括推進本部 ソフトウェアエンジニアリング技術開発部　部長
	寺田　真敏	独立行政法人情報処理推進機構 セキュリティセンター
	富樫　一哉	JPCERT コーディネーションセンター (JPCERT/CC)
	永田　隆治	一般社団法人情報サービス産業協会企画委員会政策検討部会副部会長
	西村　元也	厚生労働省情報化統括責任者（CIO）補佐官
	野村　邦彦	内閣府情報化統括責任者（CIO）補佐官

早貸　淳子	JPCERT コーディネーションセンター（JPCERT/CC）
春山　智	株式会社 NTT データ 技術開発本部 ＩＴアーキテクチャ＆セキュリティ技術センタ　課長
平林　元明	内閣府情報化統括責任者（CIO）補佐官
前野　裕一	株式会社日立製作所 公共システム事業部 官公システム統括部　部長
真鍋　敬士	JPCERT コーディネーションセンター（JPCERT/CC）
丸山　康隆	日本電気株式会社 官公ソリューション事業本部 パブリックサービス推進本部　シニアエキスパート
満塩　尚史	環境省情報化統括責任者（CIO）補佐官
宮坂　肇	株式会社 NTT データ 技術開発本部 ＩＴアーキテクチャ＆セキュリティ技術センタ　部長
三好　眞	株式会社アイ・エス・レーティング　代表取締役社長
矢島　秀浩	独立行政法人情報処理推進機構 セキュリティセンター　センター長
安田　晃	前　総務省情報化統括責任者（CIO）補佐官

オブザーバー

内閣官房 情報通信技術（ＩＴ）担当室
警察庁 情報通信局 情報管理課
総務省 行政管理局 行政情報システム企画課
総務省 情報流通行政局 セキュリティ対策室
総務省　情報流通行政局　情報流通振興課
経済産業省 商務情報政策局 情報処理振興課
経済産業省 商務情報政策局 情報セキュリティ政策室
防衛省 運用企画局　情報通信・研究課 情報保証室

第2章　政府機関の情報システムの調達に係る課題と解決の方向性

2.1. 政府機関の情報システムの調達に係る現状の整理

政府機関の情報システムの調達においては、「情報システムに係る政府調達基本指針」（平成 19 年 3 月 1 日各府省情報化統括責任者（CIO）連絡会議決定）（以下「調達指針」という。）に基づいて取組が進められているところ。我が国政府機関の保有する情報システムは「図 1　政府情報システムの現状等についての公表（平成 22 年 9 月 3 日　総務省）」のとおり約 2,000 程度存在している。

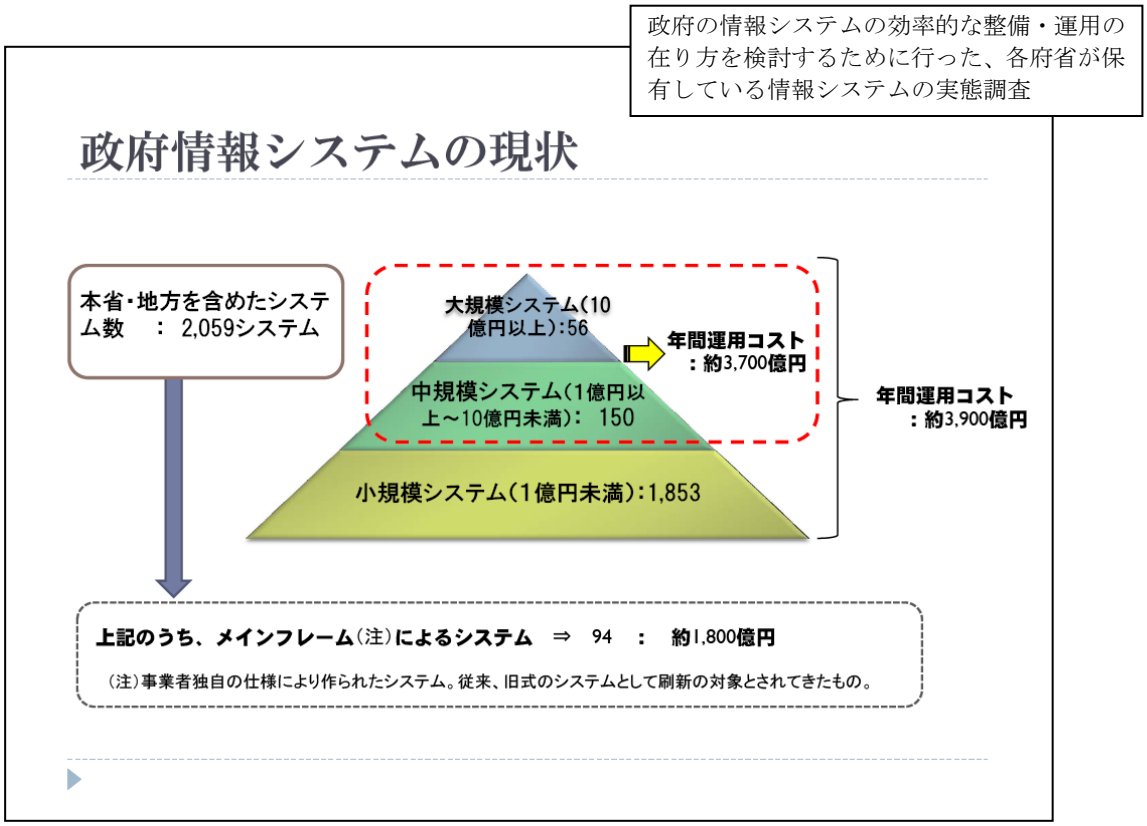


図 1　政府情報システムの現状等についての公表（平成 22 年 9 月 3 日　総務省）

調達指針においては、「調達仕様書」に記載する事項として「情報セキュリティ要件」が挙げられており、その「情報セキュリティ対策」の内容は、「『政府機関の情報セキュリティ対策のための統一基準』（平成 17 年 12 月 13 日情報セキュリティ政策会議決定（以下「統一基準」という。））及び適用個別マニュアル群に基づく各府省の情報セキュリティポリシー等において要求されている事項及び情報資産のリスクを十分に勘案した上で、各情報資産の重要度及びリスクに応じた対策を定義する。」と

された。統一基準は、その後、構成の見直しとして「政府機関統一管理基準（以下「統一管理基準」という。）」により、政府機関の横断的な取組みの一環として、情報セキュリティ対策の内容の整合化・共通化を促進するため、それぞれの府省庁が最低限行うべき情報セキュリティ対策を定め、「政府機関統一技術基準（以下「統一技術基準」という。）」により、統一管理基準に記載された情報セキュリティ対策を実施する上での具体的な技術基準を定めるとの方向となった。

これら統一基準群は、各府省庁が守るべき最低限の対策水準を定めることで、情報セキュリティ水準の向上を図ることを目的としたものであり、組織としての対策の網羅性を確保したものとなっているが、一方で、統一基準群は対策水準を定めたものであるがために、情報システムの調達において個別の特性を考慮し、その際に必要となるセキュリティ要件を調達仕様に具体的かつ適切に組み込むための手法を記載しているわけではない。

2.2. 政府機関の情報システムの調達に係る課題の抽出

前項の現状を踏まえ、本検討会においては、情報システムの発注側である政府機関及び受注側である民間事業者の双方の既存の枠組み（既存制度や開発方法論など）を踏まえつつ、相互にとって利益となる方法となるよう、課題抽出・意見の整理を行った。その結果を、以下の「表 2　システム調達における情報セキュリティ対策の課題及び意見」及び「図 2　政府機関の情報システムの調達に係る課題」に示す。

ここで特筆すべき点として、以下の３つの現状が明確となった。

(1) 発注側の政府機関の政府職員（調達担当者）は必ずしも情報システムの専門家ではない
(2) その結果、情報システムの調達、工程管理、運用などを自立して行うことが困難になる（情報セキュリティにおいても想定される脅威に対応した具体的かつ適切なセキュリティ要件策定が困難になる）
(3) 一方で、受注側としてシステムを供給する民間事業者は、調達仕様が不明確であるため、適確な実装方法の提案が困難であり、また、要件解釈のばらつきから公平な競争の妨げにもつながる

抽出した課題及び意見を踏まえ、現状の情報システム調達における曖昧な調達仕様を是正することで、発注側と受注側の合意形成の困難さから生じる相互の不利益の発生を回避し、また調達する情報システムの特性に応じて無駄がなくかつ現実の脅威に効果的な情報セキュリティ要件を策定する必要がある。

発注側と受注側の合意形成の困難さに起因して相互に不利益が生じた事例については、「情報システム・ソフトウェア取引トラブル事例集」（2010 年 3 月経済産業省委託事業）に多くの参考になる事例がまとめられている。当該事例集には、受注側（原告）が仕様書に明記されていない個別対応プログラムに係る追加の請負代金の支払いを発注側（被告）に求めた結果、発注側（被告）の支払いを容認する判決が下された事例や逆に受注側が追加負担を負うこととなった事例等が記載されている。このように調達における曖昧な合意形成は、相互に追加コストの危険性を生むばかりでなく、民間事業者にとっての政府調達の魅力を減退させるおそれもある。

また、曖昧なセキュリティ要件による調達はシステムの特性に応じたリスク分析を不十分にし、セキュリティ事故発生時の責任回避の観点のみが重視され、全網羅的かつ過剰なセキュリティ対策や調達費用の増加を招く可能性がある。

表 2 システム調達における情報セキュリティ対策の課題及び意見

発注者（政府職員）	受注者（民間事業者等）
■ システムの専門家ではない • 調達仕様書を自ら作成できず、ベンダー提案を基にせざるを得ない。 • ベンダーからの情報が難解かつ膨大なため、必要性を判断できない。 • 技術動向・環境変化が激しく、情報セキュリティの対応が困難になる。 • 経費積算は見積もりベースであり、工数が適切かを判断できない。 • 政府の制度・基準等が複雑なため、調達仕様書に反映できない。	**■ 適切な提案・設計が難しい** • 調達仕様書の曖昧さから合意形成や開発計画の策定が困難になる。 • 全行程でのセキュリティポリシーを一貫して確保することが難しい。 • 調達仕様書の記載が「○○準拠」のみのため仕様を読み取れない。 • 信頼性やセキュリティなどとコストとのバランスを確保できない。 • 実装要件の指定が不十分で、環境のバリエーションに対応しづらい。
■ 工程管理が難しい • 設計書等の技術的文書の問題点に気づかず、品質低下、機能不足、納期遅延等を招いてしまう。 • 知識・理解・労力不足によって、各工程の完了判断、検査を適切に行えない。	**■ 工程管理に支障を来す** • 各工程にて調達仕様との整合性を確保し開発を進めることが難しい。 • 各工程の確認が受注側に閉じており、発注側と共有されていない。
■ 適切に運用できない • 運用保守ベンダーに問題があっても、別ベンダーへの引継ぎが担保されず変更できない。	**■ 運用後に問題を残しかねない** • 緊急時の協力は惜しまないが、契約が十分なされないままでは、恒常的なセキュリティ確保は難しい。

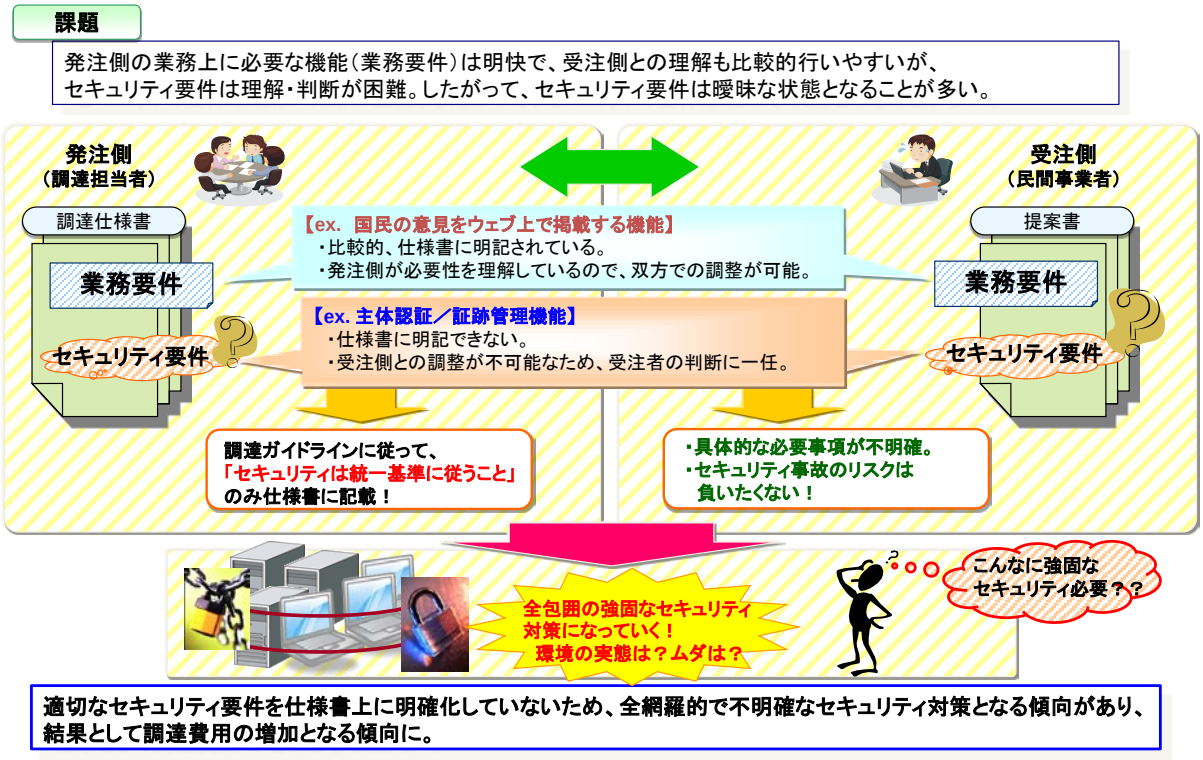


図 2 政府機関の情報システムの調達に係る課題

2.3. 政府機関の情報システムの調達に係る課題解決

本検討会においては、前項にて述べた課題の解決に向けて「図 3　情報システムの調達プロセスの全体像」に示すように政府機関の情報システムの調達プロセスの全体を俯瞰し、各段階の実態に着目して課題の発生要因を整理した。

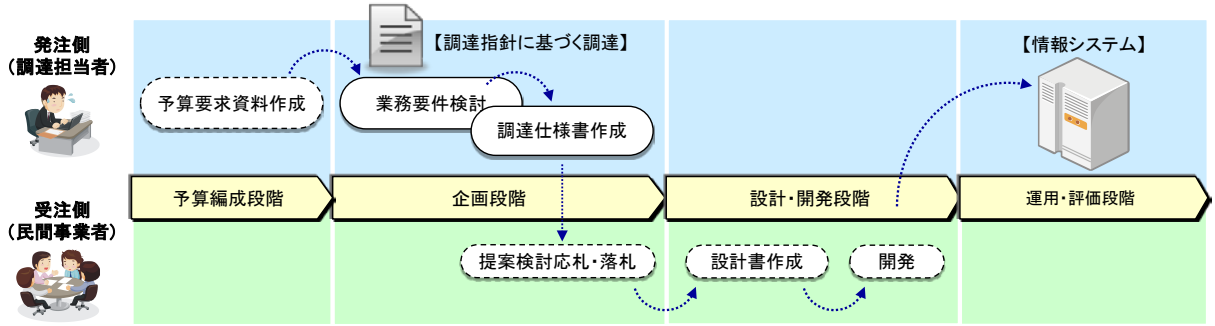


図 3 情報システムの調達プロセスの全体像

前項にて述べた課題は、「企画段階」において作成された不適切な調達仕様書が原因となって「設計・開発段階」以降が適切に行われないことに起因すると考えることができる。本検討会では、「企画段階」及び「設計・開発段階」以降のそれぞれに焦点をあて、以下のように具体的な２種類のアプローチに至った。

(1) 情報セキュリティ上の脅威の高度化に対応した設計・運用手法の確立

近年、情報セキュリティ上の脅威が高度化するとともに、脅威を取り巻く環境の変化も加速度的に増している。このような状況に対しては従来の全包囲的かつ一律的な手法では効果的な対策を期待することが難しく、より具体的に各脅威に対して集中的かつ効果的なセキュリティ対策を講じることが求められる。

そこで、本検討会では、サイバー攻撃防御分野の専門家集団の知見を結集し、最新動向を踏まえた具体的な脅威の振る舞いを分析することによって、各脅威の特性に応じた具体的な対応のための設計指針として「リスク要件リファレンスモデル（RM）」を整理する必要性に至った。

この設計指針は、調達プロセスにおける「設計・開発段階」以降のフェーズにおいて、例えば、セキュリティ対策機能の設計担当者が当該指針を用いるによって、調達仕様書にて対策が求められる脅威に対して効果的なセキュリティ対策機能を

より具体的かつ適切に設計することが可能になる。

本アプローチに関しては、「第 3 章 リスク要件リファレンスモデル（RM)」にて詳しく述べる。

(2) 調達仕様書に対する適切なセキュリティ要件の組み込み手法の確立

前項にて述べたとおり、各府省庁における情報システムの調達担当者は必ずしもシステムの専門家ではない。しかしながら、そのような調達担当者であっても、「企画段階」において調達仕様書にセキュリティ要件を適切に組み込まなければ、「設計・開発段階」以降の発注側と受注側の合意形成に関する深刻な問題の発生を招くとともに、最悪の場合、運用後のセキュリティ事故を発生させる可能性もある。

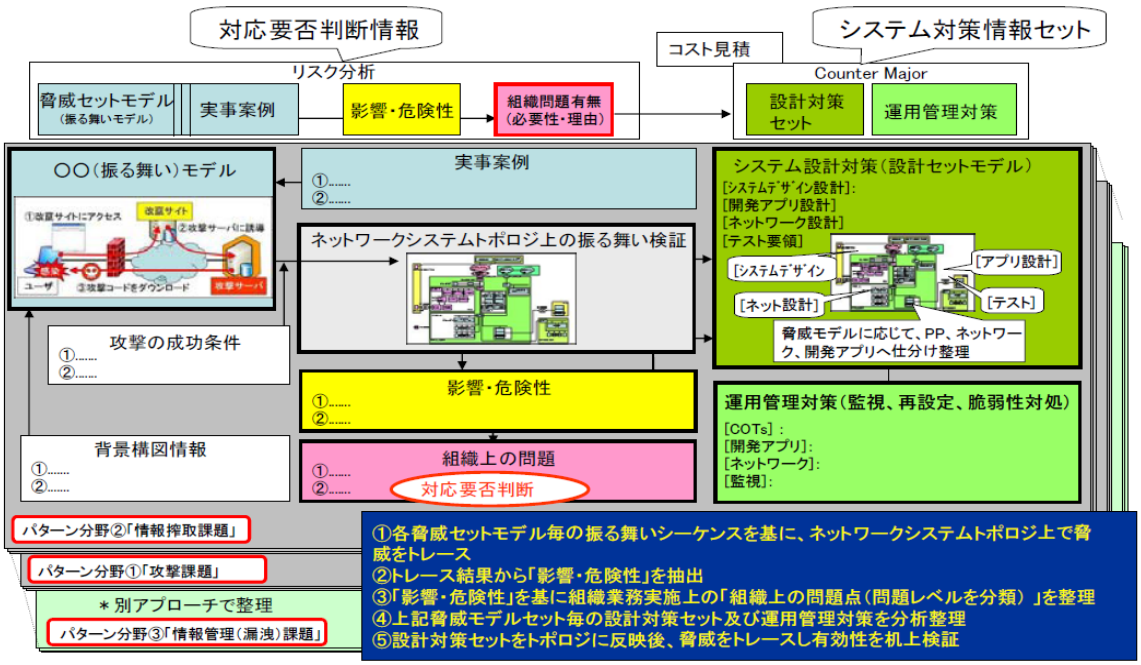
そこで、本検討会では「企画段階」の調達プロセスにおいて調達担当者が実施する「調達仕様書の作成作業」に焦点をあて、当該作業において調達担当者が直面している課題を分析し解決策を探ることによって、調達仕様書に記載すべきセキュリティ要件を調達担当者が自ら決定可能とする手法を検討することとした。

本アプローチに関しては、「第 4 章 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」にて詳しく述べる。

第3章　リスク要件リファレンスモデル（RM）[1]

リスク要件リファレンスモデル（以下「RM」という。）は、情報セキュリティ分野のうちサイバー攻撃防御分野に焦点をあて、情報システムにおけるサイバー攻撃防御のためのセキュリティ機能の設計指針を設計対策セットとして取りまとめたものである。

RM は「図 4　RM の構造概念」に示すとおり、サイバー攻撃の具体的な脅威の特性を分析してとりまとめた「脅威セットモデル」を元にして、情報システムに係る詳細なリスク分析を行い、「設計対策セット」を活用して効果的な対策を情報システムの設計に反映することを目指すものである。



平成 21 年度各専門分野情報共有スキームの連携性及び情報交換モデルの構築支援業務
「リスク要件リファレンスモデル作業部会　報告書（2010 年 3 月）」より抜粋

図 4　RM の構造概念

---

1 リスク要件リファレンスモデル（RM）に関する具体的検討は、「情報セキュリティに係る各専門分野の情報共有・連携推進会議」の「リスク要件リファレンスモデル作業部会」にて行われ、その詳細については、「内閣官房情報セキュリティセンターの調査研究」の平成 21 年度「各専門分野情報共有スキームの連携性及び情報交換モデルに関する検討（リスク要件リファレンスモデルドキュメント集等の作成）」において、公開されている。

脅威セットモデルの作成にあたっては、サイバー攻撃防御分野の専門家集団の知見を結集して、実際に発生したサイバー攻撃に関するマルウェアの振る舞いの特性を「図 5　振る舞いパターンの例（正規 Web 閲覧によるマルウェア感染の振る舞い）」のように分析、抽出することによって、最新の脅威を類型化している。

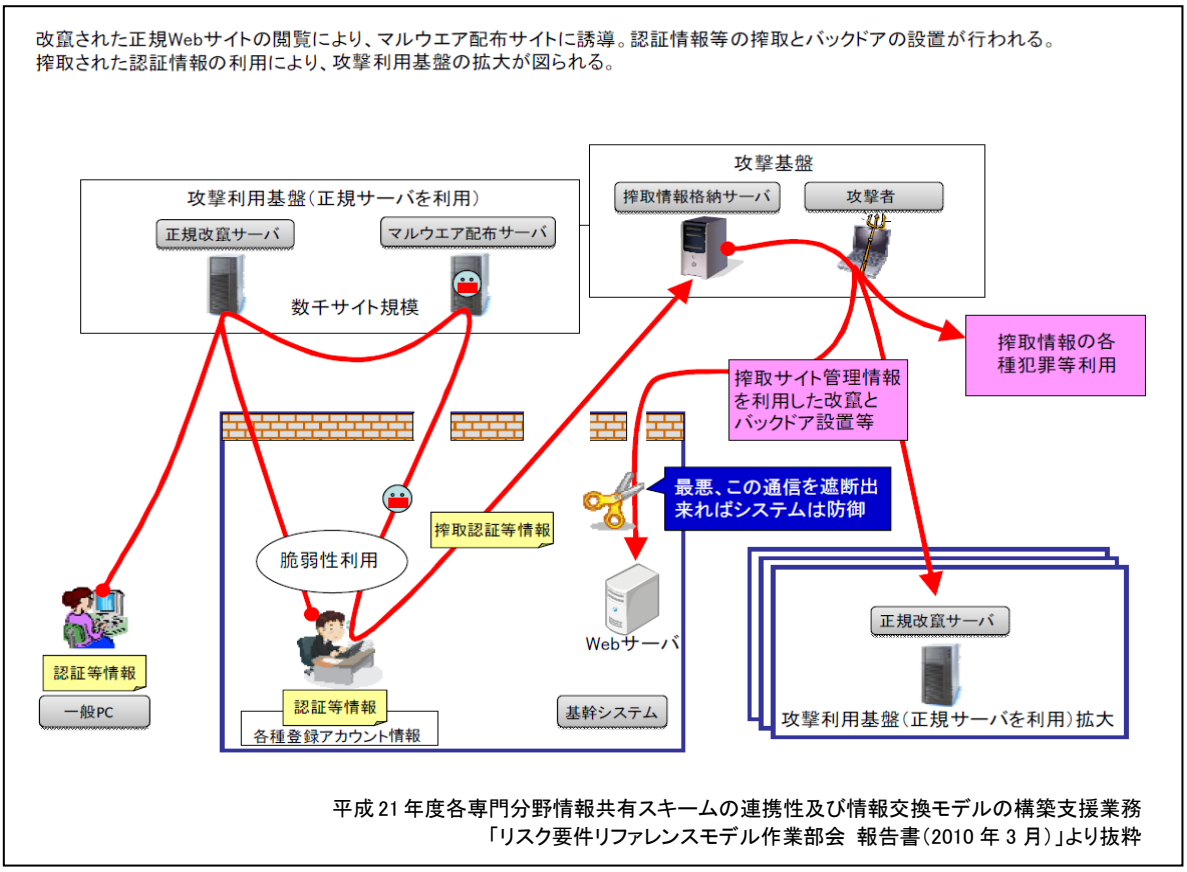


図 5　振る舞いパターンの例（正規 Web 閲覧によるマルウェア感染の振る舞い）

RM ではこのような脅威セットモデルによって、実際のサイバー攻撃を網羅的にカバーしつつ、サイバー攻撃発生のメカニズムを詳細に明らかにし、情報システムのセキュリティ機能が備えるべき適切な対策機能を明確化している。

「表 3　設計対策セット（抜粋）」は、この検討結果に基づいてとりまとめられた設計対策セットの一部である。情報システムの設計・開発にあたっては、この設計対策セットを活用することによって、従来と比較してよりセキュリティ機能を効果的かつ確実に備えることが可能となる。

表 3 設計対策セット（抜粋）

トポロジモデル	振る舞いパターン	設計対策と運用管理対策	
		対策番号	対策の内容と効果
イントラネットモデル	振る舞いパターン 1：正規 Web 閲覧によるマルウェア感染（情報搾取）	A010	2 要素認証の導入により、管理 FTP の ID、パスワードが盗まれた場合でも Web サーバの改ざんを防止できる可能性が高まる。別系統の管理用 LAN(裏 LAN)設置とあわせて導入することでさらに効果は高くなる。
		A030	マルウェアが悪性サイトへの搾取情報送信に使用する HTTP 通信のヘッダー形式が RPC 標準から外れている点をチェックすることにより送信を遮断できる可能性がある。
		A040	侵入検知システム（IDS)を、SOC(Security Operation Center)と一対となった運用を行うことによって、マルウェアによる不正アクセスを検知し、アクセスを遮断できる可能性がある。さらに、IDS によるマルウェアの「異常な振る舞い(通信）」検知によりマルウェアによる搾取情報持ち出しを阻止できる可能性がある。
		A060	クライアント PC に未知のウィルス検出ソフトウェアを導入することにより、クライアント PC でのマルウェアの活動を停止できる可能性がある。
		C010	管理用 LAN(裏 LAN)の設置によって、管理 FTP の ID、パスワードが盗まれた場合でも Web サーバの改ざんを防止できる可能性が高まる。2 要素認証とあわせて導入することでさらに効果は高くなる。

平成 21 年度各専門分野情報共有スキームの連携性及び情報交換モデルの構築支援業務
「リスク要件リファレンスモデル作業部会 報告書（2010 年 3 月）」より抜粋

第4章　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

4.1. マニュアルの概要

「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」（以下「本マニュアル」という。）は、情報システムの調達プロセスにおいて、発注側の調達担当者が調達仕様書にセキュリティ要件を記載するための手順を定め、作業を支援するためのものである。また、情報セキュリティ対策に必要な予算を確保するための検討として、本マニュアルを予算編成段階から活用し、必要なコストを見極めることにも有効である。

本マニュアルは政府機関において情報システムの企画段階から情報セキュリティ対策を適切に組み込むため、セキュリティ要件の策定方法を解説している。もって、調達担当者が自ら調達するシステムの特性に応じて重要かつ効果的なセキュリティ要件を優先的に確実に調達仕様書に記載することを目的とする。

また、政府機関の情報システムが「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）」に基づいて調達される際、セキュリティ要件の策定にあたって活用されることを想定している。想定読者は、情報システムの調達を担当する調達担当者及び情報システムを供給する事業者である。

活用範囲としては、政府機関における「新規構築」及び「更改」を行う情報システム全般としている。特に企画段階から技術の専門家が参画することが難しい中小規模の情報システムの調達において有効である。

4.2. マニュアルの策定方針

本項では、本マニュアルの策定方針について述べる。以下で述べる方針に基づいて作成されたマニュアルの内容については、別添のマニュアル本体を参照いただきたい。

一般に、情報システムの調達における「企画段階」の作業は、予算要求等にあたり作成された事業概要資料（「図 6　事業概要資料の例」）に記載されたレベルの情報等を元にして行われる業務要件の検討作業が起点となる。

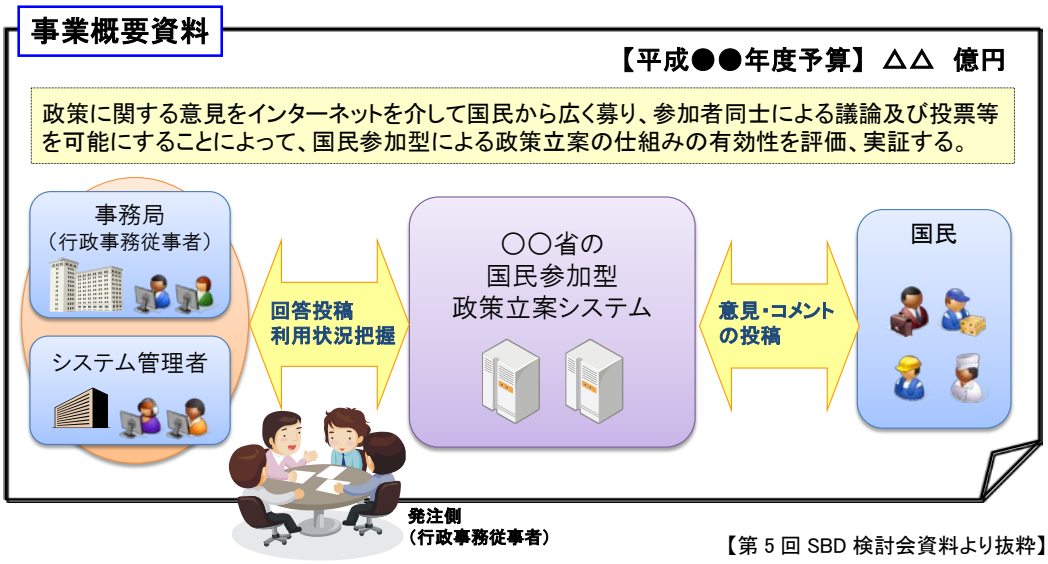


図 6 事業概要資料の例

本検討会では、このような業務要件の検討作業を起点としてセキュリティ対策に関する要件（以下「対策要件」という。）を定めるまでの作業プロセスとして下記の流れを想定し、この流れを支援するマニュアルを目指した。

① 情報システムを利用する主体の列挙
（情報システムに関わる人物やシステムを列挙する）
② 各主体の振る舞い（業務）の抽出
（主体の「目的・役割」を踏まえ、業務やサービスを洗い出して、取り扱う「情報」と「手段・環境」を合わせて整理する）
③ 対策要件の決定要因となる要素の抽出
（②の抽出結果の関係及び業務全体を俯瞰するシステム概要図を作成するとともに、業務要件の詳細化を図る）
④ 対策要件の決定
（③の抽出結果に基づいて「対策要件」を選定する）

上記のうち、本マニュアルが目的とするセキュリティ要件の策定に直接関係がある作業は上記の④である。①から③の作業は、④の検討に必要な業務要件の抽出を行うための作業である。

以下では、各作業に関して本マニュアルによる支援の考え方について述べる。

作業①　情報システムを利用する主体の列挙

調達担当者にとって主体を列挙する作業は、比較的取り組みやすい作業と言えるが、重要な主体の抽出漏れを防ぎ、各主体の特徴をできる限り具体化するといったことに有効と考えられる以下のような「作業上の観点」をマニュアル上に示すことによって、作業品質を確保することが必要であると考えられる。

(1) 洗い出す主体は、事業概要資料等の初期段階で明らかになっている情報から直接分かる範囲で良いものとする。
(2) 主体の基本的な「業務目的」や「役割」等の整理からはじめる。
(3) 利用者（エンドユーザ）だけでなく、システムの運用に関わる人物、連携する外部システム等を含めて抽出する。

また、上記の検討作業をできる限り定型化するため、「表 4　主体に関する検討結果の例」のように、検討すべき項目を明らかにする方法や検討例を示す方法が有効と考え、そのような工夫についても考慮してマニュアルを作成した。

表 4　主体に関する検討結果の例

【第 5 回 SBD 検討会資料より抜粋】

分類	分類の定義	主体の名称	目的／役割
利用者	情報システムの主たるサービス又は機能を利用する	国民	• 意見を政府や社会に知らしめたい • 他者の意見を知りたい • 政府や社会について他者と議論したい
サービス提供者	利用者にサービス又は機能を提供する	事務局	• 国民の意見を募って政策に活かしたい • 議論の活性化のために国民の意見に回答したい • 利用状況を把握し、不正利用は廃除したい • 外部システムが管理する意見もあわせて議論に活用したい
システム管理者	サービスの提供に支障を来さないように情報システムを維持管理する主体	システム管理者	• サービスを無停止で提供したい • 稼働状況を把握し、障害発生時には迅速に対応したい。 • 不正利用を検知し、廃除したい
外部システム	情報や機能を相互に提供する等の連携を行うシステム	他府省庁 意見募集システム	• 投稿された意見をシステム間にて相互に共有したい

※同一の分類に複数の主体があてはまる場合もある。

※この範囲を検討して記入する

作業② 各主体の振る舞い（業務）の抽出

各主体の振る舞い（業務）の抽出作業は、いわゆるユースケース分析の作業に相当するが、高度なユースケース分析の作業を行うことは本マニュアルが想定する利用シーンにはふさわしくないと考えられる。また、作業手順を定型的なものにするためには、検討結果として整理すべき情報もあらかじめ定めておく必要がある。

そこで、本検討会では比較的理解しやすい観点として、業務の「概要」、当該業務で取り扱う「情報」及び「利用環境・手段」といった観点を与え、これらを主体ごとに整理していく作業手順を定めることによって作業の定型化を図った。

このような考え方に基づいてマニュアルの検討過程において試行的に作成した検討結果の例が「表 5　主体の振る舞いに関する検討結果の例」である。

表 5 主体の振る舞いに関する検討結果の例

【第 5 回 SBD 検討会資料より抜粋】

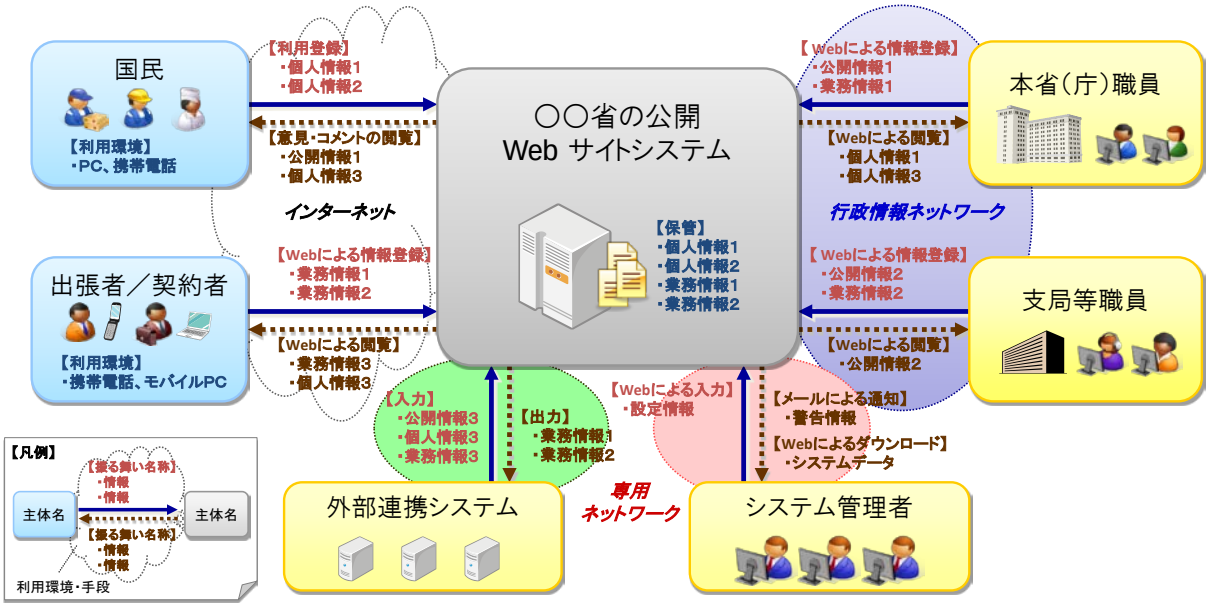
主体	振る舞いの名称		内容	利用環境･手段	情報
国民	①	利用登録	氏名、ニックネーム、メールアドレス、等の個人情報を入力し、サービスの利用資格を得る。	PC、インターネット	氏名、ニックネーム、性別、年齢、職業、地域、パスワード、等の個人情報
	②	意見･コメントの提出、投票	メールアドレスとパスワードによりログインし、意見や他者の意見に対するコメントを投稿したり、投票を行う。	PC、インターネット	意見、コメント （タイトル、本文、投稿者名、投稿日時）
	③	意見･コメントの閲覧	カテゴリごとに、投稿済みの意見やコメントを検索したり、一覧や個別表示により閲覧する。	PC、インターネット	意見、コメント （タイトル、本文、投稿者名、投稿日時）
事務局	①	意見に対する回答、修正	意見に対して事務局回答を投稿したり、国民に求めに応じて不適切な意見を修正、削除する。	PC、行政情報NW	回答、コメント （タイトル、本文、投稿者名、投稿日時）
	②	事務局からのお知らせ	サービスの一時停止や注意事項の伝達等の利用者に対する周知を行う。	PC、行政情報NW	お知らせの文面
	③	利用者の管理	登録済みの利用者の登録情報の確認、修正、等の管理業務を行う。	PC、行政情報NW	氏名、ニックネーム、性別、年齢、職業、地域、パスワード、等の個人情報
	④	利用状況の把握	利用者の登録状況、アクセス状況、投稿された意見やコメントの集計等を行う。	PC、行政情報NW	サイトまたはコンテンツごとのアクセス数、カテゴリごとの意見･コメント数、利用者の登録情報
	⑤	他システムとの連動	他府省庁意見募集システムが管理する意見を抽出の上、取り込み、議論に活用する。	PC、行政情報NW	他システムが管理する意見、コメント
システム管理者	①	システムのバックアップと復旧	障害時の復旧に備え、定期的にシステムのデータをバックアップしたり、障害発生時の復旧を行う。	PC、管理用NW	システムデータ、設定情報
	②	不正利用の監視、追跡	不正アクセス等を監視し、必要に応じて監視ログ等を元にして原因究明のための追跡を行う。	PC、管理用NW	アクセス、認証、利用状況の履歴(ログ)
他府省庁意見募集システム	①	意見･コメントの共有	事務局による操作により指定された意見及びコメントを提供する。	サーバ、専用NW	意見、コメント （タイトル、本文、投稿者名、投稿日時）

作業③　対策要件の決定要因となる要素の抽出

作業①及び作業②の作業結果から、セキュリティ対策の要件の決定要因となり得る要素を抽出、整理する必要がある。例えば、主体と主体の間でやりとりされる情報の流れのように作業①及び作業②の「検討結果の関係」を明らかにし、保護すべき情報や情報システムを特定することなどが求められる。

そこで、本検討会ではマニュアルの策定にあたり、作業①及び作業②の検討結果を「見える化」するために「システム概要図」と呼ぶ図にまとめる方法を検討した。また、そのような図に加えて、情報システムに関する共通的な業務要件を定型設問として規定し、調達担当者が定型設問に対する回答を試みることによって業務要件のさらなる詳細化を促すしくみを検討した。

なお、「図 7　システム概要図の作成例」及び「表 6　定型設問の例」は、以上のようなマニュアル作成のための検討にあたって試行的に作成した「システム概要図」及び「定型設問」の例である。



【第 5 回 SBD 検討会資料より抜粋】

図 7　システム概要図の作成例

表 6 定型設問の例

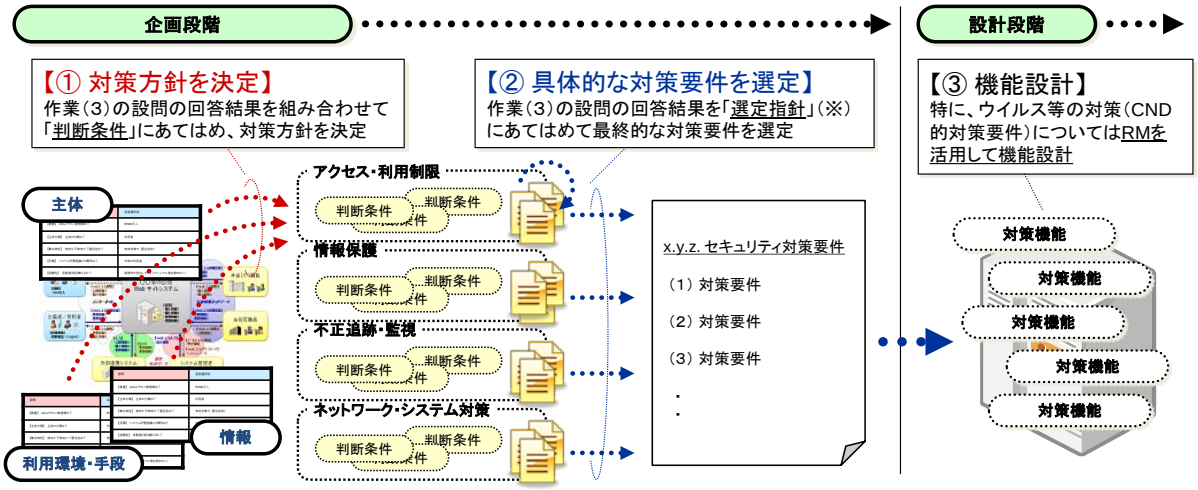
【第 7 回 SBD 検討会資料より抜粋】

ID	観点	設問
A-1	主体	【数量】 おおよその人数規模は？
A-2		【主体分類】 主体の分類は？
A-3		【集合特性】 特定か不特定か？
A-4		【所属】 システム所管組織との関係は？
A-5		【頻度】 1人あたりのアクセス頻度は？
A-6		【信頼性】 役割どおりに振る舞えるか？
B-1	情報	【数量】 おおよそのデータ量は？
B-2		【所有者】 情報の所有者は誰か？
B-3		【範囲】 公開・提供可能な範囲は？
B-4		【改変】 不正改変時の影響度は？
B-5		【取扱】 閲覧のみか？変更が発生するか？
B-6		【保存】 システム内に保存するか？
B-7		【検証】 完全性の事後検証は必要か？
C-1	利用環境・手段	【伝達手段】 情報を送受信する方法は？
C-2		【処理環境】 サーバ又は端末の種類は？
C-3		【通信環境】 利用するネットワークは？
C-4		【通信環境】 外部からの遠隔利用は必要か？
C-5		【信頼性】 異常停止の許容時間は？

作業④　情報システムを利用する主体の列挙

作業③までの作業によって対策要件の検討に必要な業務要件を抽出した上で、作業④では、当該業務要件を踏まえ調達仕様書に記載すべき対策要件を決定する。

本検討会では、「図 8　対策要件の選定及び調達仕様書への反映の流れ」に示すように「判断条件」と呼ぶ条件を作業③までで検討した業務要件にあてはめることによって、調達仕様書に記載すべき対策要件が半自動的に選定されるしくみを検討した。検討にあたっては、判断条件が調達担当者に理解可能なものである必要があることにも留意した。「表 7　判断条件の例」は、本マニュアルの作成にあたって試行的に作成した判断条件の例である。



【第 5 回 SBD 検討会資料より抜粋】

図 8　対策要件の選定及び調達仕様書への反映の流れ

表 7　判断条件の例

【第 6 回 SBD 検討会資料より抜粋】

ID	項目	観点分類	判断条件	判断結果(例)
A	外部アクセスの有無	利用環境･手段	インターネット等の通信回線を介して情報システムにアクセスして業務や情報システムの管理を行うか	はい／いいえ
B	情報の重要度	情報	漏えいした場合や正常にアクセスできない場合に、深刻な被害を被る可能性がある重要性の高い情報を取り扱う情報システムであるか	はい／いいえ
C	情報受信後の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保管する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか	はい／いいえ
D	利用者の限定要否	主体	情報システムの利用者は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか	はい／いいえ
E	アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか	はい／いいえ
F	複数組織による利用	主体	情報の取り扱い方や利用目的等が異なる複数の組織等の間で共用されるか	はい／いいえ

また、このような判断条件に基づく対策要件選定のしくみを確立するためには、選定の候補となる対策要件の網羅及び一覧化も必要である。そこで、本検討会では、そのような一覧情報として「対策要件集」を作成している。対策要件集には、調達仕様書に記載すべき仕様書の記載例、仕様書に記載する際に情報システムの特性に応じてカスタマイズすべき点とその方法等も記載した。

さらに、情報システムが求めるセキュリティレベルに応じて、対策の実施レベルは異なると考えられることから、仕様書の記載例は「低位」、「中位」、「高位」の３段階に対応するものを用意し、「低位」であるか「中位」以上であるかについては判断条件によって自動的に判別可能な手順とし、「中位」と「高位」の選択については、対策要件集に示す選定の考え方を踏まえ、調達担当者が決定する手順とした。

なお、上記の判断条件に基づく対策要件の選定のしくみは、情報システムに関するリスクアセスメントの簡易手法の一種と捉えることもできる。

第5章　本報告書等の今後の取り扱い

本検討会の成果については、情報システムの調達を行う政府機関及び供給者である事業者双方で広範に共有され、双方の意思疎通を図り、適切な情報セキュリティ対策がなされることが期待される。そのため、内閣官房情報セキュリティセンターは、積極的に本成果物の普及・利用促進を行う。引き続き、各府省庁の情報システムの調達に関わる全ての部署に働きかけを行い、実際の調達仕様書にどのように本成果が反映されるか検証していく。さらに、実際の利用にあたっては、利用者からの問合せ対応、作業支援などを行い、活用の成果を導く。

また、あわせて、本成果物の改善も行っていく。利用する中でのフィードバックとして、たとえば、本成果物で求める作業の内容や要素の加除修正などにより、使いやすさと効果の向上を行うことや、あるいは、本成果物の活用により作成された調達仕様書のセキュリティ対策が適当であるかを確認し、必要な対策を反映することなどである。さらには、新たな脅威の顕在化等による環境変化に対応していく必要があり、これらに対応した改善も行っていく。

なお、政府機関における情報システムの調達は「情報システムに係る政府調達の基本指針」等により政府の取組が進められているところである。本成果物もこれら取組の一環として活用されるが、引き続き、改訂等の際にこれらの取組に協調していくことが必要である。

これらに加えて、本成果は政府機関のみならず、情報システムの調達を行う公的機関等においても利用可能であり、利用の拡大で本成果による情報セキュリティ対策の効果をより期待できる。そのため、これら公的機関等への普及においても取り組んでいく。

第6章　今後の課題

本検討会において議論のあった、情報セキュリティと費用のバランスを考えた証跡管理、可用性の確保に係る対策のあり方、情報システムの調達に係る検収時の適正性判断等は、さらに検討や利用によるフィードバックを深め、本成果物の効果を向上させることが望ましい。

なお、本検討会では、情報システムのライフサイクルに応じた取組とは別に情報システム調達に係る予算確保や執行のあり方、調達業務を適切に行う能力をもつ職員の育成の必要性についても指摘があった。こうした課題についても、将来的に検討していくことが求められる。

以上