防　衛　取　得　研　究　　第七巻　第一号　平成２５年６月

保全教育に関する概念整理及び情報セキュリティとの関係

研究員　　六畑　方之

1　はじめに

本件は防衛基盤整備協会（ＢＳＫ）が行う「情報セキュリティの知識普及等事業」（公益目的事業３、以下、「公３」という。）の一部としての保全教育の範囲・内容・あり方の明確化に資するため、保全教育及び情報セキュリティに関して、その概念を整理したものである。

2　整理の手順

概念の整理に当たっては、まず、保全、秘密保全及び保全教育の概念並びにそれらの関係を明らかにするとともに、情報セキュリティの代表的な定義を概念化した後、ＢＳＫの行う「保全教育」と「情報セキュリティの知識普及等事業」（公３）との関係を明らかにする。

3　保全、秘密保全及び保全教育の概念（図１）

(1) 保全の目的

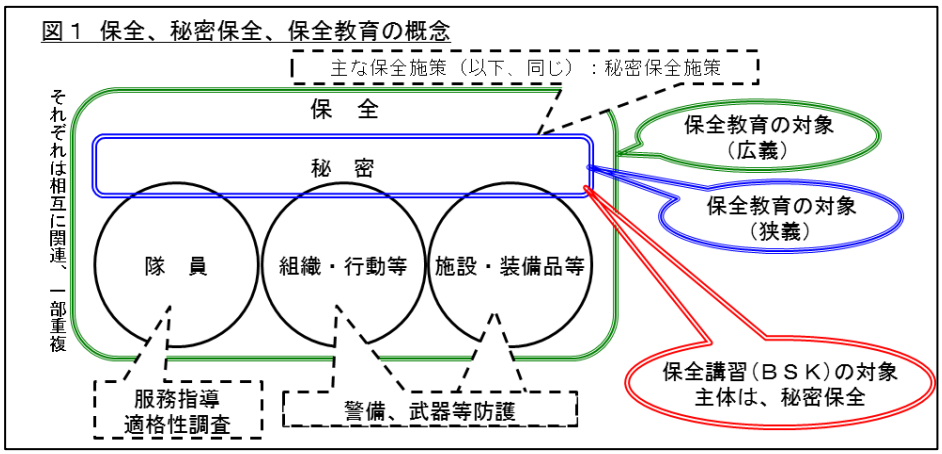
防衛省において、「保全の目的は、敵の情報及び謀略活動等を無力化して、我が行動の秘匿及び部隊の安全を確保するにある。」と記述※１されている。

（※１）「保全の目的」については、陸自教範参照

(2) 保全業務の定義及び秘密保全の位置付け

この保全の目的を達成するために、保全の業務として何を行うか、言い換えれば、保全業務の種類・内容は、①秘密保全、②隊員保全、③組織・行動等の保全及び④施設・装備品等の保全※２の４つに分けられる。秘密保全は（情報）保全業務の１つである。また、この４つの業務は一部が重複するとともに、相互に関連※３している。

図１　保全、秘密保全、保全教育の概念



（※２）情報保全業務の実施に関する訓令（防衛庁訓令第７号。１５．３．２４）参照

（※３）　例えば、隊員保全を徹底することにより、秘密の保全が保たれる、あるいは逆に、秘密を保全することにより、部隊の行動を保全できる、というようなことである。

なお、これらの業務を達成するための代表的な手段・施策は、秘密保全については防衛省訓令等に基づく各種秘密保全施策、隊員保全に関しては服務指導、適格性調査等並びに組織・行動等の保全及び施設・装備品等の保全に関しては警備、武器等防護等である。

(3) 保全教育の概念

保全教育を広義に捉えれば、前号の４つの保全業務すべてが対象となる。しかしながら、実態上（狭義）は、秘密保全が教育の対象※4とされることが多く、また、この教育が秘密保全のために行う施策の大きな柱でもある。

そして、ＢＳＫの行っている「保全講習」の対象は、この狭義の保全教育（実態上は後述する、防衛省の規定する「装備品及び役務の調達における情報セキュリティ」を含む。）の１つである。

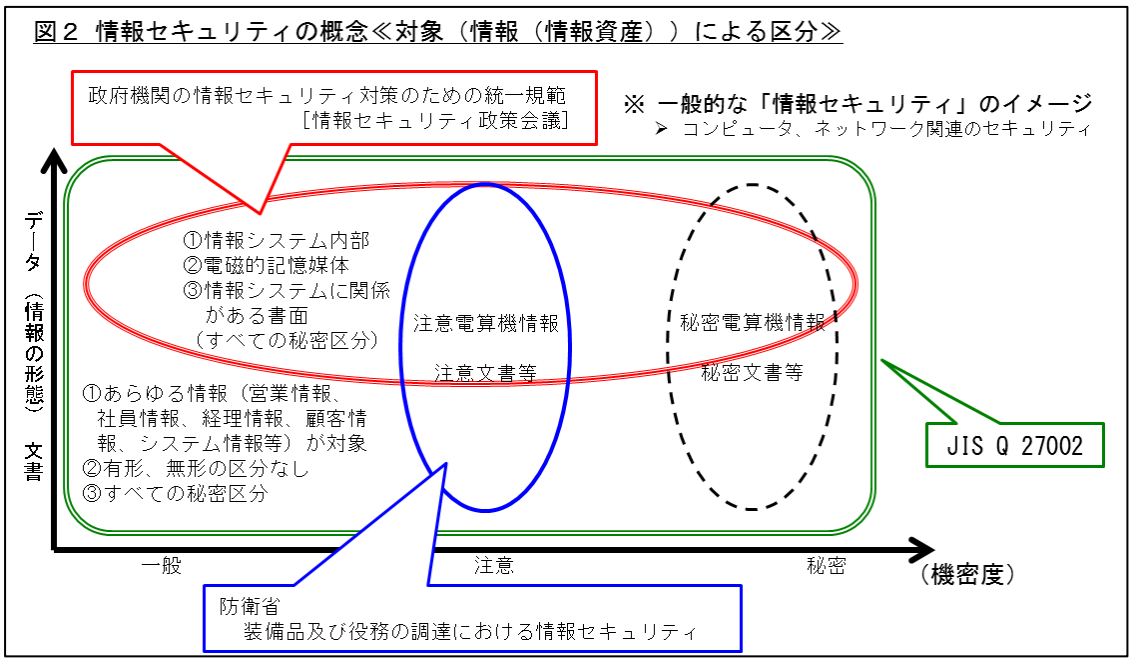
（※4）保全教育の目的は、秘密（防衛秘密、特別防衛秘密）の保全（保護）に必要な知識の徹底及び意識の高揚を図ることにある。［秘密保全に関する訓令第９条　等］

4　情報セキュリティの概念（図２）

情報セキュリティについては、さまざまな概念で語られている。

情報セキュリティとは、「情報の機密性、完全性及び可用性を維持すること。さらに真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。」（ＪＩＳ　Ｑ２７００２）と定義されているが、この定義は「目的的定義」であって、この定義における情報をどのように捉えるかによって、様々なイメージになる。

図２　情報セキュリティの概念≪対象（情報（情報資産））による区分≫



(1) 一般的なイメージ

情報セキュリティと言う場合、一般的には、コンピュータ、ネットワーク関連のセキュリティのことをイメージする。すなわち、セキュリティの対象となる情報の形態は、紙ベースの文書が主ではなく、パソコン等の機器で取り扱われるデータが対象である。この場合に、すべての段階の機密度の情報が対象となる。

政府の「情報セキュリティ政策会議」が決定した「政府機関の情報セキュリティ対策のための統一規範（２４．４．２６改定）」によれば、「この規範の対象とする情報は、①情報処理及び通信に係るシステム（以下「情報システム」という。）内部に記録された情報、②情報

システム外部の電磁的記録媒体に記録された情報及び③情報システムに関係がある書面に記載された情報とする。」となっており、一般的な「情報セキュリティ」のイメージと合致する。

⑵ 広義の情報セキュリティ（日本工業規格ＪＩＳ）

「情報セキュリティマネジメントの実践のための規範（ＪＩＳ　Ｑ　２７００２）」（以下「ＪＩＳ規範」という。）を解説したＩＰＡ（情報処理推進機構）発行の「情報セキュリティ教本」によれば、「ＪＩＳ規範における情報とは、営業情報、社員情報、経理情報、顧客情報、システム情報等をいう。」とされ、「情報資産」と同義と解説している。また、ＪＩＳ規範では、「資産」を「情報、ソフトウェア資産、物理的資産、サービス、人、資格等、無形資産」に分類するとともに、電子的に保存されたものに限らず、紙に書かれたもの、会話として話されるものまで「情報」の中に含めている。

これらのことから、最も広義の情報セキュリティの概念の対象では、情報の区分から言えば、形態としては紙からデータまで、機密性の観点からは機密度のない一般情報から秘密までの広い幅で捉えられている。ＩＳＭＳもこのイメージと同じの概念である。しかしながら、関連文書の内容からは、この概念の中でも、パソコン等の電子媒体及びそれで取り扱う情報が主なセキュリティの対象となっている。

⑶ 防衛省における装備品及び役務の調達における情報セキュリティ

防衛省における装備品及び役務の調達における情報セキュリティの概念の範囲は、対象とする情報を注意文書等及び注意電算機情報等※5としている。情報の形態上は、焦点はパソコン等関連情報であろうが、データから文書まで幅がある。

（※5）装備品等及び役務の調達に関する情報のうち、取扱い上の注意を要する文書等及び注意電子計算機情報の取扱いについて（通達）（防防調４６０８号。１９．４．２７）第１に規定する「取扱い上の注意を要する文書等」及び同通達第８に規定する「注意電算機情報」並びにこれらの情報を利用して作成される情報をいう。「装備品等及び役務の調達における情報セキュリティの確保について（通達）（防経装第９２４６号。２１．７．３１）」

５　保全教育と情報セキュリティ知識普及等事業（公３）の関係（図３）

⇒　情報セキュリティ知識普及等事業（公３）としての保全教育とは何か？

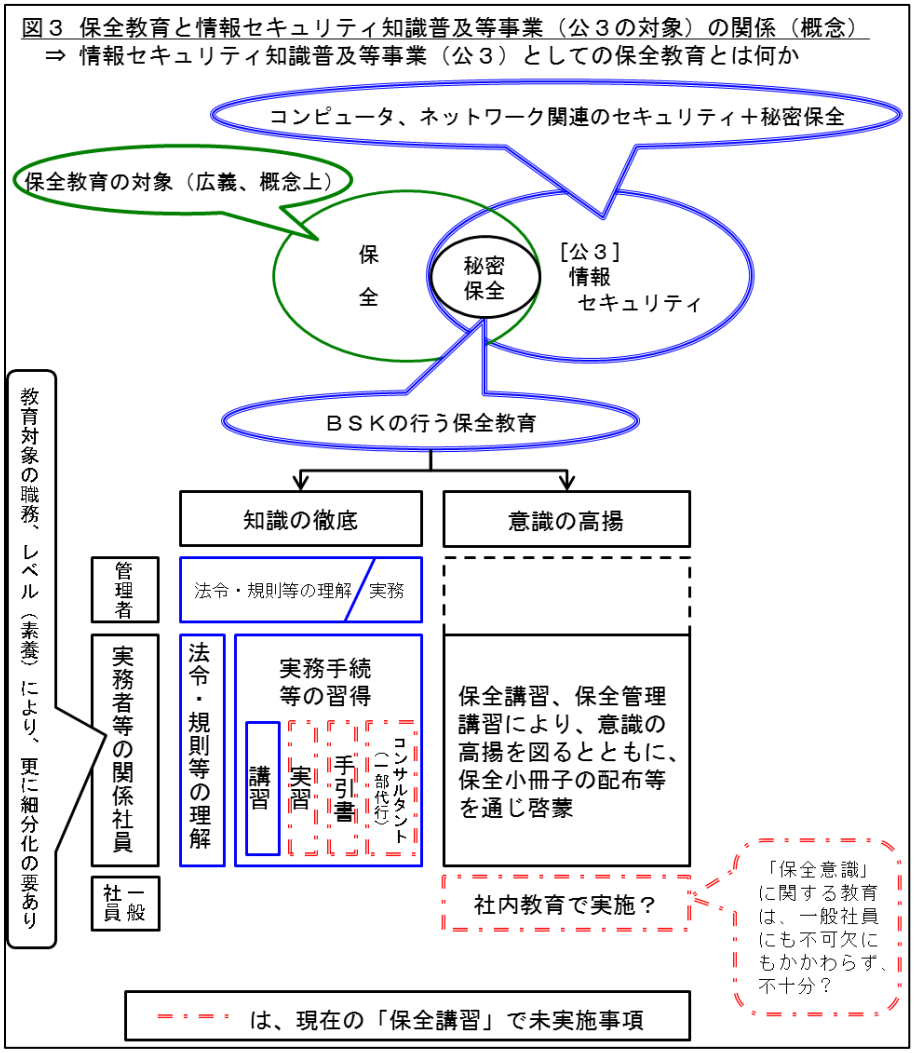
⑴ ＢＳＫの情報セキュリティ事業

ＢＳＫの情報セキュリティ事業には、秘密に関する保全講習が含まれることから、範囲としては、第４項第１号の「一般的なイメージ」である「コンピュータ、ネットワーク関連のセキュリティ」に加え、「秘密保全」の範囲である。

○　情報セキュリティの知識普及等事業（公３）
- 保全講習（装備品調達、建設）等事業
- 情報セキュリティ懸賞論文の表彰事業
- 情報セキュリティ技術セミナーの実施事業
- 情報セキュリティ講演会事業
- 機関誌「防衛調達と情報セキュリティ」の発刊事業
- 情報セキュリティ懸賞論文の表彰事業
- 情報セキュリティに関する調査研究事業
- 保全小冊子の発行事業
- 情報セキュリティの啓発事業
- 情報セキュリティ講習事業

(2) ＢＳＫの行う保全教育

ア　ＢＳＫの情報セキュリティ事業が前号のような範囲である中にあって、ＢＳＫ事業として行う保全教育は、広義の「保全教育」のうち、ＢＳＫの情報セキュリティ関連事業として規定した「主として防衛関連企業の担当者等に情報セキュリティに関する知識の普及、教育、研究、啓蒙等の諸活動を通じて、防衛基盤の強化に寄与することを目的としたもの」（公益認定説明資料）に含まれる事業でなければならず、図３の上部分のようなイメージとなる。「情報セキュリティ知識普及等事業（公３）」の範囲の中でＢＳＫが行う「保全教育」としては、ほぼ「秘密保全」の範囲に止まる。



イ　保全教育の目的は、「知識の徹底」及び「意識の高揚」（第３項第３号※４「訓令条文」参照）である。

知識の徹底とは、①法令・規則の理解及び②実務手続等の習得である。管理者クラスは、①法令・規則の理解を促進することが主である。特に、実務者クラスにとっては、②実務手続等の習得のためには、「Ⓐ講習」、「Ⓑ実習」、「Ⓒ手引書（マニュアル本）による自学研鑽」及び「Ⓓコンサルタント（一部代行）」等の手段が考えられる。ＢＳＫが現在行っているのは「Ⓐ保全講習」であり、Ⓑ～Ⓓによって実務能力を向上させることも「保全教育」の範疇に捉えることができる。特に、実務者クラスに対する教育については、本来であれば、教育対象の職務、レベル（素養）により、更に細分化（少なくとも、初心者（予定者）と経験者）することが必要である。

意識の高揚のためには、実務者クラスに対しては、ＢＳＫの行う保全講習、保全管理講習により、意識の高揚を図るとともに、保全小冊子の配布等及び実務者自身の自覚によって、継続的に、保全の目的・重要性、危機意識の付与、当事者意識の涵養等を図られてい

る。なお、特に、「保全意識（サイバー対策等の情報セキュリティを含む）の高揚」については、一般社員には、社内教育でその高揚を図ることが不可欠であるとの認識は各企業も持っているにもかかわらず、全ての企業が十分に実施できているわけではないものと推測する。

６　結　び

保全教育及びＢＳＫの行う情報セキュリティの知識普及等事業（公３）の概念並びにその関係を整理した結果、防衛関連企業にとって必要な保全教育、すなわち、保全に関する知識の徹底及び意識の高揚を図るために、現行の「保全講習」以外にもＢＳＫとして貢献することを今後の拡大事業として検討する余地があるものと考える。

外部組織・要員に対するリスクアセスメントとその管理策について

主任研究員　榊　　勝

１．はじめに

情報セキュリティの事件・事故は、内部組織以外にも外部委託先からの情報漏洩など、外部組織・要員が関わることによって発生する。

そこで内部組織に外部組織・要員が関わることによって発生するリスクを軽減する管理策が求められている。

２．ISMS における外部組織・要員について

外部組織・要員については、情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項（JIS Q 27001:2006）6.2 外部組織において、次のように規定している。

目的　：外部組織によってアクセス、処理、通信又は管理される組織の情報及び情報処理施設のセキュリティを維持するため。

A.6.2.1 外部組織に関係したリスクを識別しなければならない。

A.6.2.2 顧客にアクセスを許す前に、明確にしたすべてのセキュリティ要求事項を満たすように対処しなければならない。

A.6.2.3 第三者との契約は、関連するすべてのセキュリティ要求事項を取り上げなければならない。

このように、先ず、外部組織・要員が関わることで発生するリスクを特定する。そして、リスクアセスメントからリスク対応までを、その組織が関わる前に実施することを求められている。しかし、業務の多忙さに取り紛れ、事前に十分な時間が取れないことも実情であり、往々にそのときになって考えるということになりがちである。

それでは、どのように対応したらよいのか。その管理策及び実施については、情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範（JIS Q 27002:2006）の規格に沿って考察していくこととするが、JIS Q 27001 の「…しなければならない」という要求に対して、JIS Q 27002:2006 は「…することが望ましい」と一般的手引きを提供するものとなっていることを考慮して議論を展開していくこととする。

３．外部組織の定義

内部組織に関わる（アクセスする）外部組織とは、どのような組織が考えられるのだろうか。JIS Q 27001 及び JIS Q 27002 の中から該当すると思われるものをピックアップしてみることとする。

顧客　　：　外部組織の中でも性質が異なるもので、顧客満足度を考慮した対応が必要となる。

第三者　：　当該問題に関して、当事者と無関係であると認められる個人又は団体と定義しているが、その第三者は、セキュリティレベルの高い組織の情報又は情報処理施設が関係するアクセス・処理・通信・管理に関わることも想定している。

契約相手：　組織が契約を締結したサービス提供業者、下請負業者、人材派遣業者等契約相手である下請負業者を指し、情報セキュリティエリアで組織の業務に従事する場合（構内請負者）もある。

４．外部組織が関わる業務を考慮したリスクアセスメント

A.6.2.1 では、外部組織が関わる業務を考慮したリスクアセスメントを行い、アクセスを許可する前に適切な管理策を実施することが求められている。

それでは、「外部組織が関わる業務を考慮したリスクアセスメント」とは、具体的にどのようなリスクアセスメントを指しているのか。ISMS ユーザーガイド-JIS Q 27001:2006(ISO/IEC 27001:2005)対応-平成 20 年 1 月 31 日(第 2 刷)を参考に考察していくこととする。

組織の外部組織のアクセスに関連するリスクの識別においては、先ず、外部組織による情報及び情報処理施設への次のようなアクセスを明確に把握しておく必要がある。

(1)物理的アクセス（事務所、コンピュータ室、文書保管庫などへのアクセス）
(2)論理的アクセス（組織のデータベース、情報システムなどへのアクセス）
(3)組織のネットワークと外部組織との間の接続（常時接続、リモートアクセスなど）
(4)アクセスの実施場所の区別（事業所の構内又は構外）

そして、これらのアクセスにおける脅威と脆弱性を特定して、それらのリスクレベルを算定し、そのリスクが受容できるか、又は対応が必要であるかを判断することになる。

５．外部組織における要員の捉え方

外部組織における要員とは、具体的には次のような活動を行う要員である。

(1)ネットワークプロバイダ、保守及びサポートサービスの要員
(2)体系的なセキュリティサービス提供業者
(3)IT システムの外部委託先
(4)IT システム、ソフトウェアの開発者及び供給者
(5)清掃等の提供業者
(6)短期契約の職員、実習生

６．外部組織・要員に関わるリスクアセスメント

外部組織のアクセスに関連するリスクの識別においては、前述した組織の情報を取扱う要員を考慮することが望ましいとしている。そのリスクアセスメントのロジックとしては、外部組織と同様に、要員のアクセスにおける脅威と脆弱性を特定し、それらのリスクレベルを算定し、そのリスクが受容できるか、又は対応が必要であるか判断することになる。

７．外部組織・要員のリスクアセスメントの方法

外部組織に関係したリスクの識別は、当該組織の情報及び情報処理施設へのアクセスという面からのリスクアセスメントと、具体的に活動するその外部組織の要員に対するリスクアセスメントの両面から成り立つと考えられる。

では、外部組織・要員のリスクアセスメントの手法としては、具体的にどんな方法が適切であるかについて述べる。

(1)　ベースラインアプローチ

前段の当該組織の情報及び情報処理施設へのアクセスという面からのリスクアセスメントは、資産を対象としたリスクアセスメントでは困難な面があることから、先ずは、あらかじめ一定の確保すべきセキュリティレベルを設定し、実装するのに必要な対策を選択し、対象となるシステムに一律に適用することを目指すベースラインアプローチ手法を採用するのが適切であるという考え方がある。

ベースラインアプローチにおいては、先ず、組織の達成する情報セキュリティ管理について「ベースライン」と呼ばれる独自の「対策の標準」を作成する。

一般の情報セキュリティに関する基準や、業界等で採用されている標準やガイドラインなどを参照して、組織全体で共通のセキュリティ対策を実施し、実現可能な水準の管理策を採用して組織全体でセキュリティ対策に抜け漏れが無いように補強していくアプローチである。

そして、外部組織・要員に対して、実際にどのような管理を導入するか広く管理策について情報収集し、組織が要求する情報セキュリティの管理水準が、達成可能なベースラインであるかどうかの検討をする必要がある。

(2)　ギャップ分析

ベースラインアプローチの次の手順として、外部組織・要員に対して、組織の定める基準への準拠状況を把握するためにギャップ分析を実施する必要がある。

ギャップ分析は、基準で要求される管理レベルと組織の管理レベルの現状を比較し、「大きな差が認められる箇所」「明らかに管理策の適用を必要としている個所」「過度に管理策が適用されている個所」等を確認することである。

具体的には、それぞれの資産を対象に、現状の対策の度合いと組織によって

定められた「要求される保証の度合い」との乖離を確認するものである。「要求される保証の度合い」は、一律ではなく、資産の属性や性質、組織における重要度により資産ごとに決定される。

ただ、ベースラインアプローチのみでは、高い水準でセキュリティ対策が実装されるべきリスクの高いシステムについて、対応策が不充分になる可能性がある。

(3) 詳細リスクアセスメント

次にリスクアセスメントの手法として、資産ごとに関連するリスクの識別を個別に実施する詳細リスクアセスメントについて考察することとする。

詳細リスクアセスメントにおいては、先ず、リスクアセスメントの対象範囲を明確にしなければならない。安易に範囲を狭め、慎重な明確化を怠ると、後で不必要な作業が発生したり、抜けが見られたりする。そして、リスクが顕在化する頻度は、脅威が発生する可能性、管理上の弱点につけ込まれる可能性の他に、資産の攻撃者からの魅力の度合いによることにも考慮する必要があるが、外部組織・要員の詳細リスクアセスメントにおいて、具体的な情報資産の対象・形態を明確にする必要がある。その方法は、外部組織・要員に対してはなじまないという意見もあるが、一つの例示として、サービス・人という情報資産の形態が考えられる。

その詳細リスクアセスメントの手順を確認すると、先ず、情報資産を洗い出し、グループ化を経て識別して資産目録を作成し、情報資産価値を評価、個々の情報資産がさらされる脅威の識別、管理上の問題点などによる脆弱性の識別を行うことになる。

次に、アセスメントにおいては、情報資産の機密性、完全性又は可用性(ＣＩＡ)の喪失を考慮する必要がある。つまり、具体的な情報資産の機密性、完全性又は可用性が損なわれた時の事業上の損害を評価することである。そのリスク値は、資産の価値(ＣＩＡ毎)×脅威×脆弱性となる。

ただ、詳細リスクアセスメントをすべてのシステムに適応させることは、現実的に効率的でない面もあり、情報資産の形態によっては、機密性を考慮しないで、完全性、可用性だけを重視するという組織もある。いずれにしても最終的には、組織が判断することとなる。

(4) 組合せアプローチ

前述したどのアプローチを、どの様な場合に採用するかは一概に決められないが、一般的には、ベースラインアプローチと詳細リスクアセスメントを併用する組合せが効率的であるとされている。その目的は、前述したそれぞれのアプローチの弱点を相互に補完し合うことにより、ISMS 適用範囲全体のリスクアセスメントを効率的に実施することである。

つまり、ベースラインアプローチのみでは、リスクの高いシステムに対しては対策が不十分となる可能性があり、又詳細リスクアセスメントのみではす

べてのシステムに対応することは困難な場合があることから、組合せアプローチが効率的であると考えられるものである。

８．リスクアセスメントにおける留意事項

これまで展開してきたリスクアセスメントの体系的なアプローチにおいて、ISMSユーザーガイドでは以下の点に留意し、それらに組織的な対応をしなければならないとしている。

(1)留意事項

・資産の管理責任が不明確となるケース(資産の重要度や取扱い範囲が特定できない)

・リスクの判断基準が未整備(判断基準が個人的に偏る)

・セキュリティインシデントの情報収集が不十分(脅威、脆弱性を定量的に扱えない)

(2)組織的な対応

・前号の各留意事項に対応してそのリスクの低減に努力する。

・要員の不足、周知・教育の不徹底、規定文書や記録の不備へ対応する。

・前述したとおり、網羅的なリスクアセスメントを実施する。

・その際、担当者の経験に基づいて緊急性の高い対策の実施を優先する。

９．外部組織・要員のリスクに対応した管理策

A.6.2 外部組織の管理目的「外部組織によってアクセス、処理、通信又は管理される組織の情報及び情報処理施設のセキュリティを維持するため」において、以下のことを実施することが望ましいとしている。なお、セキュリィティ関連事項を決定し、要求事項を管理するためのリスクアセスメントの実施については、第７項で展開済みである。

(1)外部組織・要員による組織の情報処理施設へのアクセス、情報の処理及び通信に対する管理策

それでは、外部組織・要員によるアクセス等に対する管理策を考慮するとき、前述した次の４項目のアクセスに対応して展開することとする。

①物理的アクセス（事務所、コンピュータ室、文書保管庫などへのアクセス）

物理的アクセスにおいては、セキュリティエリアのセキュリティレベルに応じて、物理的入退管理策(A.9.1.2)として「鍵での施錠管理・入退室記録」「セキュリティカードシステム」等で対応し、さらにセキュリティレベルの高いエリアについては、取扱いに慎重を要するシステムの隔離(A.11.6.2)として「指紋認証システム」「顔認証システム」等で対応することとなる。

②論理的アクセス（組織のデータベース、情報システムなどへのアクセス）

論理的アクセスにおいては、先ず、外部組織・要員の資産利用の許容範囲(A.7.1.3)を明確にして文書化し、外部組織・要員のアクセスの管理として、利用者登録(A.11.2.1)の手順を備え、利用者パスワードの管理(A.11.2.3)をし、定期的に利用者アクセス権のレビュー(A.11.2.4)をしなければならない。

その際、システム又はサービスの中で発見した又は疑いをもったセキュリティ弱点は、どのようなものでも記録し、セキュリティ弱点として報告(A.13.1.2)するように要求しなければならない。

③組織のネットワークと外部組織との間の接続（常時接続、リモートアクセスなど）

外部組織との間の接続においては、外部から接続する利用者の認証(A.11.4.2)　・利用者の識別及び認証(A.11.5.2)を適切な方法で実施し、組織の境界を越えて広がっているネットワークについては、外部組織・要員のネットワークの接続能力を制限(A.11.4.6)・情報へのアクセス制限(A.11.6.1)をしなければならない。

④アクセスの実施場所の区別（事業所の構内又は構外）

事業所の構外からのアクセスにおいては、アクセスの実施場所を明確に区別し、例えば、テレワーキング(A.11.7.2)の場合、方針、運用計画及び手順を策定し、実施しなければならない。

(2)採用した管理策は、その外部組織との間で合意し、契約書へ明記

以上、前述した管理策は、次のようなプロセスとなる。例えば、第三者との契約におけるセキュリティ(A.6.2.3)要求事項としてセキュリティレベルを明確にして、外部組織との間で合意し、契約書・ＳＬＡ（セキュリティレベルアグリメント）に明記することとなる。また、誓約書を取り交わす等の秘密保持契約(A.6.1.5)または守秘義務契約を取り交わしておくことも重要である。

(3)周知徹底のための教育・訓練の実施

また、外部組織・要員にアクセスを許可する前に適切な管理策を実施することが望ましいとしていることから、契約に基づき、外部組織・要員に対して契約相手方の管理責任者を通じて、事前に情報セキュリティの意識向上、教育及び訓練(A.8.2.2)を実施し、周知徹底を図ってもらうことも重要なプロセスと考える。

(4)外部組織・要員の情報セキュリティ活動状況の監視及びレビュー

外部組織・要員の情報セキュリティ活動状況については、契約に基づき、提

供するサービス、報告及び記録を確認し、当該活動が適切で、有効で妥当であるか、監視及びレビュー(A.10.2.2)することも重要なプロセスと考えられる。

１０．外部組織・要員のリスクに対応した管理策の有効性の測定

前述した管理策を、情報セキュリティマネジメントシステム－要求事項(JIS Q 27001) 4.2.3ISMS の監視及びレビューc)において、「セキュリティ要求事項を満たしていることを検証するために、管理策の有効性を測定する」と規定している。つまり、外部組織・要員のリスクに対応した管理策が組織が期待した状態、基準値等に達しているか否か、その有効性を測定するとしている。

１１．管理策有効性測定結果のマネジメントレビュー

さらに、情報セキュリティマネジメントシステム－要求事項（JIS Q 27001）7.マネジメントレビューの 7.1 レビューへのインプット f)において、有効性測定の結果を提供しなければならないと規定し、次のプロセスとして 7.3 レビューからのアウトプット e)において、管理策の有効性測定方法の改善に関係する決定及び処置を含めなければならないとしている。

１２．終わりに

以上、考察してきた外部組織・要員に対するリスクの識別、それに対応した管理策の採用・実施、セキュリティ要求事項を盛り込んだ契約書の締結、周知徹底のための教育・訓練の実施、そして外部組織・要員の情報セキュリティ活動状況の監視及びレビューという一連のプロセス、さらに、それら管理策の有効性の測定、その測定結果のマネジメントレビューという大きなプロセスへと、一つのプロセスからのアウトプットは、次のプロセスへの直接のインプットとなるというプロセスアプローチ的視点から対応することも重要であると考える。

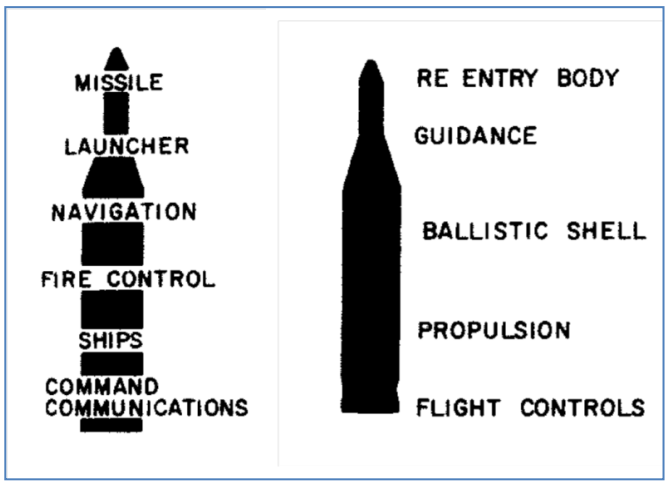
このプロセスアプローチは、大きくは情報セキュリティマネジメントシステムの Plan-Do-Check-Act（計画―実行―点検―処置）（PDCA）サイクルの有効性を確保することにも繋がると考えられる。

プロジェクトマネジメント（その３）
ワーク・ブレークダウン・ストラクチャ（WBS）の作り方

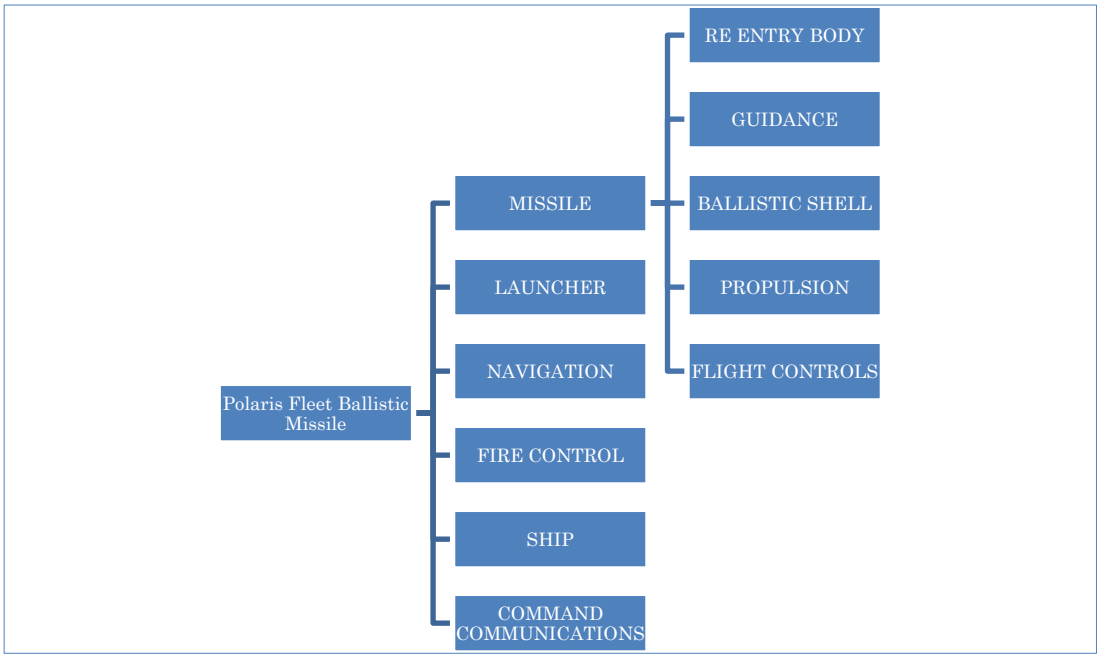
研究員　　福原 洋一

１　WBS の誕生

WBS は、プロジェクトマネジメントとして新しく開発されたものではなく、比較的古くからある概念です。１９５９年に「Application of a technique for research and development program evaluation, D.B Malcom, J.H. Roseboom, C.E. Clark, W. Fazar」により、スケジューリング技法として有名なＰＥＲＴ（Program Evaluation and Review Technique）が発表されました。著者のマルコム、ローズブーム、フェイザーは、米海軍の潜水艦発射型ポラリスミサイル開発プロジェクトのスケジューリング技法として PERT を開発し、成果をこの論文にまとめて発表しました。この PERT の論文の中に WBS の原型を見ることができます。この論文で示されものが左図です。



これを、現代の WBS で表わすと下図のようになります。



1962 年には、米国防総省（DoD）と米航空宇宙局（NASA）が示した「DoD and NASA Guide, PERT/Cost System Design」において WBS アプローチとして記述されています。1968 年に、米

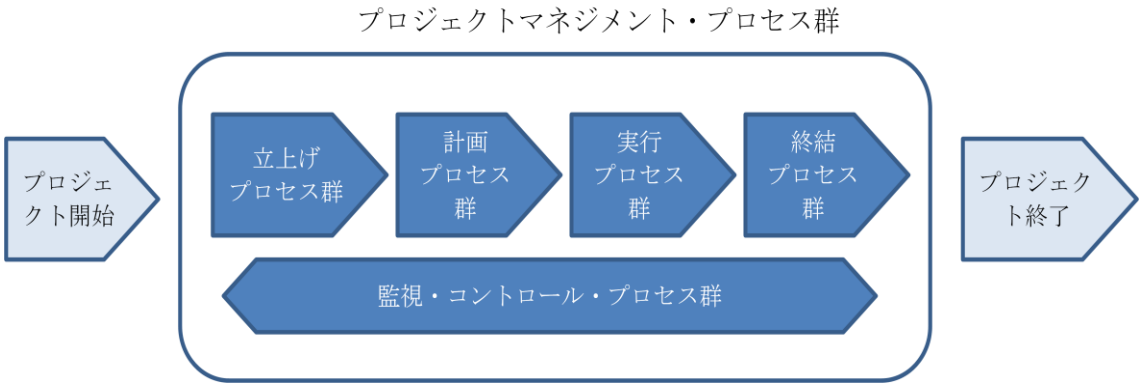
国防総省が制定した「MIL-STD-881」により、WBS の概念が確立されました。1969 年には、プロジェクトマネジメント協会（PMI:Project Management Institute）が設立され、1987 年に「プロジェクトマネジメント知識体系」が、1996 年に「プロジェクトマネジメント知識体系ガイド（PMBOK®:Project Management Body of Knowledge）」が出版されると、WBS の概念は広く民間にも普及しました。

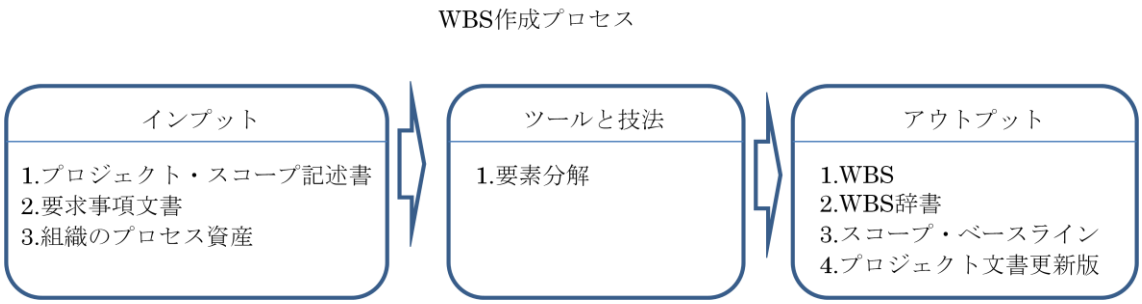
２　ワーク・ブレークダウン・ストラクチャ（WBS）について

大規模で複雑なプロジェクトでは、プロジェクトの初期段階で、その全体像がはっきりしているものは稀です。こうしたプロジェクトの全体像を俯瞰するために WBS を作成します。WBS 作成の一般的手順は次の通りです。

①プロジェクトの目的を定める。
②製品、サービスなどの成果物を特定する。
③その他の作業をすべて特定する。
④WBS の要素をコントロールしやすいレベルまで分解する。

PMBOK®においては、WBS は計画プロセス群に属する WBS 作成プロセスの主要なアウトプットです。





WBS を使用すると、プロジェクトの全体像の把握、プロジェクト関係者間のコミュニケーションが容易となります。

また、WBS はプロジェクト計画書に含まれ、プロジェクトのベースラインとなります。プロジェクトの間は、コスト、スケジュール、品質などのあらゆる面で使用されます。

３　WBS の定義

プロジェクトを各作業要素に分解し、管理しやすいようにしたものがワーク・ブレークダウン・ストラクチャーです。WBS は、スケジューリング、コスト見積もり、監視、コントロールなど他のプロジェクトマネジメント・プロセスでも利用します。

WBS はプロジェクトの計画と実行で使用され、プロジェクトの成否を左右する重要なツールです。WBS に問題があると、プロジェクトのコスト、スケジュールにおける問題発生に繋がります。プロジェクトの成功は、WBS の善し悪しにかかっています。

プロジェクトの特徴により WBS も異なるので、状況や目的に応じて WBS の表現方法もいくつかあります。現在、多く使われている WBS には、アウトライン形式、表形式、ツリー形式があります。それぞれの例を以下に示します。

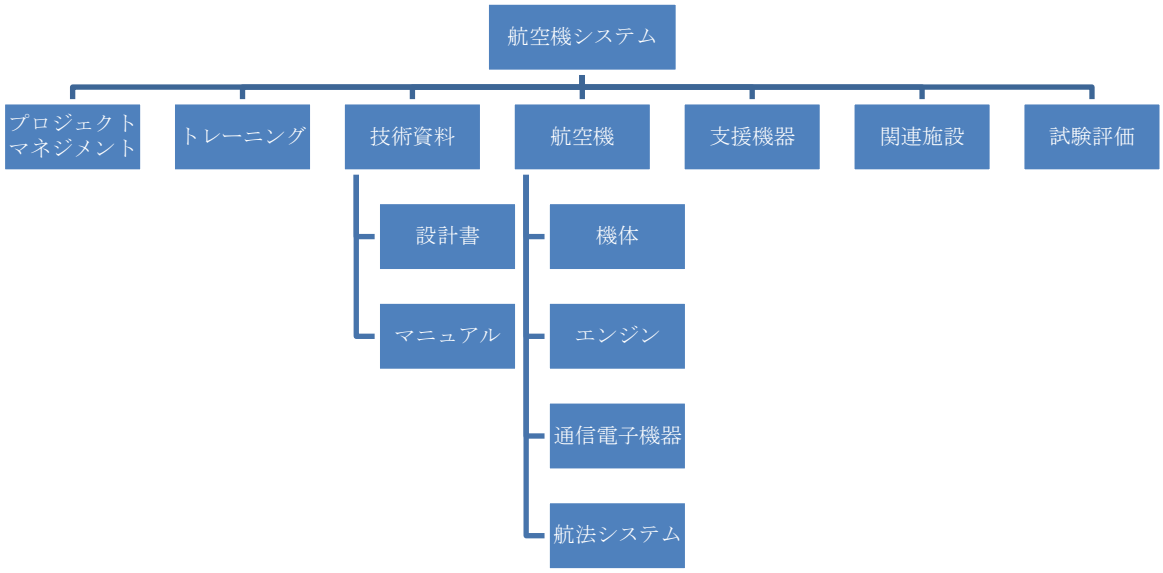
「アウトライン形式のＷＢＳ（航空機システム)」

1 航空機システム
- 1.1 トレーニング
- 1.2 技術資料
  - 1.2.1 設計書
  - 1.2.2 マニュアル
- 1.3 航空機
  - 1.3.1 機体
  - 1.3.2 エンジン
  - 1.3.3 通信電子機器
  - 1.3.4 航法システム
- 1.4 支援機器
- 1.5 関連施設
- 1.6 試験評価
- 1.7 プロジェクトマネジメント

「表形式の WBS（航空機システム）」

レベル 1	レベル 2	レベル 3	レベル 4
1　航空機システム			
	1.1　トレーニング		
	1.2　技術資料		
		1.2.1　設計書	
		1.2.2　マニュアル	
	1.3　航空機	1.3.1　機体 1.3.2　エンジン 1.3.3　通信電子機器 1.3.4　航法システム	
	1.4　支援機器		
	1.5　関連施設		
	1.6　試験評価 1.7　プロジェクトマネジメント		

「ツリー形式の WBS（航空機システム）」



4　WBS 作成

WBS の作成手法には、トップダウン、ボトムアップ、WBS 標準、WBS テンプレートなどがあります。それぞれの手法には利点と欠点があるので、プロジェクトの目標、前提条件、制約条

件に応じて適切な手法を選ぶ必要があります。

このうちトップダウンアプローチは、プロジェクトの特性やスコープが明確になっていない場合、ステークホルダーとの合意を得る必要がある場合、適切な前例が無い場合や、プロジェクトチームの WBS 作成経験が少ない場合などに向いています。

トップダウンアプローチで WBS を作成する手順は次の通りです。

・ステップ１
　プロジェクトの目的を定める。
・ステップ２
　プロジェクトの最終成果物（製品またはサービス）を決める。
・ステップ３
　最終成果物作成に必要なプロジェクトの要素成果物を定義する。
・ステップ４
　要素成果物を管理しやすい詳細レベルまで要素分解する。
・ステップ５
　合意が取れるまで WBS の改訂を繰り返す。

こうしてできる WBS の最下位の要素をワークパッケージと呼びます。

WBS 作成の際、注意すべき事項、WBS が備えていなければならない必須の特性は次の通りです。

・要素成果物指向で要素分解されている。
・プロジェクト・スコープを定義している。
・ステークホルダー（利害関係者）にスコープを説明できるようなレベルまで、作業が明確になっている。
・スコープで定義した作業内容が１００％含まれている。
・プロジェクトマネジメントを含め、中間で完了する作業または要素成果物が含まれてる。
・各レベルで要素分解された要素が親レベルの作業を１００％含んでいる。

５　米国防総省の WBS

PMBOK®と米国防総省の WBS には相違点があります。PMBOK®の WBS はあらゆるプロジェクトに適用できるように作られているのに対し、米国防総省の WBS は米国防総省の取得する製品、成果物を対象としています。このため、米国防総省の WBS は対象範囲が狭いのですが、該当する分野では大変役に立ちます。

米国防総省の WBS は MIL-STD-881 として規定されました。その後、MIL-HDBK-881 に改訂され、現在は、MIL-HDBK-881A となっています。MIL-HDBK-881 では、米軍の取得する下記の兵器システムの WBS テンプレートが用意されています。

・航空機システム
・電子／自動化ソフトウェア・システム
・ミサイル・システム

・弾薬システム
・海上システム
・宇宙システム
・陸上移動システム
・無人飛行物体

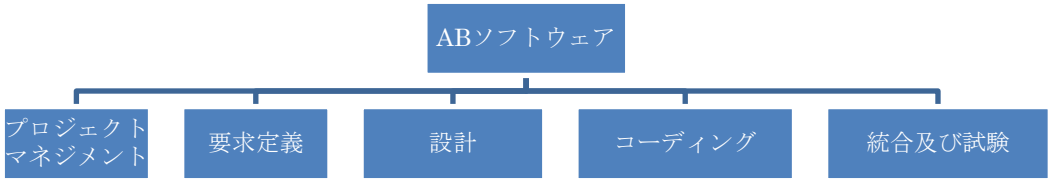
MIL-HDBK-881 で規定される WBS は、PMBOK®よりも狭い範囲を対象としており、次のような特徴があります。

・大規模プロジェクトが主対象
・成果物指向で、WBS の要素は器材、データなど識別可能なもの。
・フェーズは不可　プロジェクトのフェーズは WBS の要素として使えない。
・発注者、受注者、サブコントラクターなど全てのプロジェクト参加者が実施する作業を漏れなく洗いだせる。

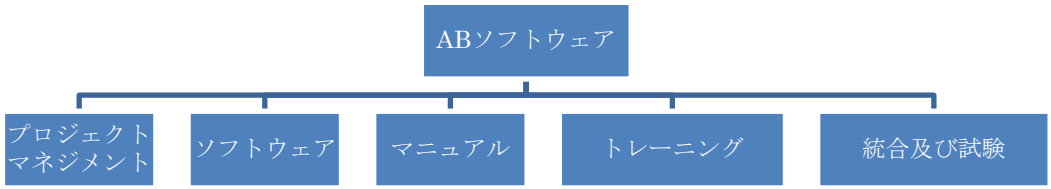
このため、航空宇宙産業等の大規模プロジェクトにおいては、MIL-HDBK-881A が大変参考となります。

最後に、MIL-HDBK の観点から、良い WBS と悪い WBS の例を紹介します。
下に示した 2 つの例、どちらが良い WBS か判りますか。

「WBS 例 1」



「WBS 例 2」



MIL-HDBK の WBS の特徴の 3 項目「フェーズは不可」という点からみると、例 1 は悪い WBS の例です。

参考文献

1「Application of a technique for research and development program evaluation, D.B Malcom, J.H. Roseboom, C.E. Clark, W. Fazar」1959

2「MIL-HDBK-881A, DEPARTMENT OF DEFENSE HANDBOOK: WORK BREAKDOWN STRUCTURES FOR DEFENSE MATERIEL ITEMS」2005

3「実務で役立つ WBS 入門、Gregory T. Haugan」2005

4「ワーク・ブレークダウン・ストラクチャー実務標準 第 2 版」2008