

防衛取得研究 第一巻 第三号 平成19年12月

目次	防衛省における経费率算定基準の変遷について	1頁
	情報セキュリティ意識教育について	6頁

防衛省における経費率算定基準の変遷について

主任研究員 草地 八寿郎

1. まえがき

防衛装備品は市場価格のあるものを除き特注品であるため、その価格決定は通常原価計算方式による積み上げによって求められている。その原価計算方式というひとつの構造体の核になるのが経費率であり、防衛省では「調達物品等の予定価格の算定基準に関する訓令」の中でその扱いを規定している。昭和37年に最初の基本となるもの（Ⅰ期）が作られて以来、数次にわたる改正がなされてきているが、大きく変更されたのは平成も10年以降になってのこと（Ⅱ期）である。いったん大改正がなされると、その後は5年を待たずして再度大幅改正（Ⅲ期）となった。ここではこの間の背景、状況等について概観してみることとする。

なお、紙幅の関係から支払利率及び利益率に絞って話を進めていくこととしたい。

2. 共通の考え方

Ⅰ期からⅢ期を比較すると、支払利率及び利益率において顕著な差が見られるが、他の部分ではさほど大きな違いは見られない。また、防衛省の経費率算定に当たっては共通項といったものがあり、改正がなされたからといってもそれらには基本的に同じ考え方が流れている。ひとつには防衛産業を含めた我が国全産業の平均的な力（財務上の数値）を測定、分析しその結果（水準）を契約上の価格に反映させるということである。そこには世界標準のレベルに合わせるとか防衛特有のレベルはかくあるべしという考え方はない。また、二つの考え方がある場合は原則として低い率を採用という考え方、さらには数値上の急激な変化を避けるため出来るだけ数値は平均化するという調整事項的考え方がⅠ期からⅢ期を通じて共通にある。

3. 第Ⅰ期（昭和37年5月制定）

防衛庁発足後に最初に制定されたもので、防衛庁発足からはかなりの年月が経過しているが、企業会計審議会が同年11月に原価計算基準を発表したこととおそらく関係があるものと思われる。このⅠ期では規則類の変更、経済状況の変化等に伴って幾多の修正・変更を加えられながらも、こと支払利子、利益等に関しての考え方はこの後30数年間の長期にわたって、殆ど変更されることなく基準として用いられた。なお今後の説明において網掛け部分は「標準的数値（統計値）」であり、年度ごとに設定する経費率の基準となるものである。

（1）支払利率

- ・支払利率は実績支払利率及び計算支払利率のうちいずれか低率のものを適用するものとする。

$$\cdot \text{実績支払利率}(\%) = \frac{\text{期間支払利息} + \text{期間社債利息} + \text{期間社債発行差金償却}}{\text{期間総原価}} \times 100$$

$$\cdot \text{計算支払利率}(\%) = \frac{\text{借入資本期間平均実額} \times \text{標準実績金利}^{(*)}}{\text{期間総原価}} \times 100$$

(*) 標準実績金利：借入金の加重平均的な利率

(2) 利益率

- ・利益率は基準計算利益率の率とする。
- ・基準計算利益率は基本払込資本利益率による計算利益率と基本自己資本利益率による計算利益率の相加平均値とする。

$$\cdot \text{基本払込資本利益率}(\%) = \frac{\text{標準実績配当率}}{1 - (\text{標準実績内部留保率} + \text{標準税率} + \text{標準賞与率})} \times 100$$

$$\cdot \text{基本自己資本利益率}(\%) = \text{基本払込資本利益率} \times \frac{\text{払込資本}}{\text{自己資本}}$$

$$\cdot \text{基本払込資本利益率による計算利益率}(\%) = \frac{\text{払込資本} \times \text{基本払込資本利益率}}{\text{総原価 (年換算)}} \times 100$$

$$\cdot \text{基本自己資本利益率による計算利益率}(\%) = \frac{\text{自己資本} \times \text{基本自己資本利益率}}{\text{総原価 (年換算)}} \times 100$$

実際の計算式の適用に当たっては、当該事業の実情を考慮する等必要な調整を行うことができるとしているが、理論的には基本払込資本利益率による利益率及び基本自己資本利益率による利益率双方とも甲乙付け難しとして、相加平均値を適用するものである。

なお、この期間において、当初は総原価に加えて支払利子にも利益率を乗じ

ていたが、その後利益率は総原価のみを対象とした。また産業経理協会による種々の検討案も提案されはしたが、結果的に骨格としての考え方は変わっていないのでⅠ期と総称することとする。

4. 第Ⅱ期（平成11年6月制定）

Ⅰ期の時代が余りにも長く続いている間に、原則は原則としていわゆる調整事項が幅を利かせるようになり、また過払い事案を契機として原価計算関係が行政監察対象にもなったことから、より透明性の高い算定基準が求められることとなった。その結果、部外の有識者等の意見も考慮して、種々の検討の結果制定されたものがⅡ期に相当する。考え方としては、支払利子と利益とを個別に扱うのではなく一体のものとして収益率的に見る。また、標準的支払利子及び利益率を基準（中心値）とし、標準的総資本回転率と個別企業の防衛生産部門を最も端的に表していると思われる総資本回転率との乖離程度に応じて個々に振り分けていく考え方である。

総資本支払利子及び利益率

$$\cdot \text{支払利子及び利益率(\%)} = \frac{\text{総資本支払利子及び利益}}{\text{総資本回転率}} \times 100$$

ここで

$$\cdot \text{総資本支払利子及び利益率(\%)} = \frac{(\text{借入資本} \times \text{標準実績金利} + \text{自己資本} \times \text{標準実績自己資本利益率} - \text{受取利息及び配当}) \times 1}{\text{総資本}} \times 100$$

総原価

$$\cdot \text{総資本回転率(\%)} = \frac{\text{総原価}}{\text{総資本}} \times 100$$

理論的には以上であるが、調整事項を関与させることによって、極端な率の排除は行うものとしている。但し、防衛産業の回転率の低さといった特性は特性として認めるという考え方である。

5. 第Ⅲ期（平成16年7月制定）

経費率の算定は、わが国産業界の平均的な力の測定と当該企業の財務諸表の分析によって行われる。発注側である防衛省としては、当該企業のうち防衛省発注品の製造という本来の経営目的に直接関連する費用のみを考慮すべきところであるが、決算によって開示される財務諸表上では他の経営目的のための費用とが一体となっている。企業によっては投資等によって得られる受取利息の方が支払利息を超えるという状況等も生じており、その扱いには以前から注意

を要していた。また利益の本質である契約履行に対する報酬、及び危険負担に対する補償の観点から、一律の利益率は不合理であるとの指摘も長年叫ばれていた。実際、国外の軍需品契約におけるインセンティブはきめ細かく規定され運用されている。さらにはバブル崩壊後の極度の経済不振が長らく継続している状況にあった。これらを踏まえた意向を取り入れようとしたのがこのⅢ期分に当たる。

(1) 利子率 (従来を支払利子率に相当)

(**)

$$\text{利子率(\%)} = \frac{\text{経営資本} \times \text{標準金利}}{\text{期間総原価}} \times 100$$

(**) 標準金利：平均的な負債及び資本の構成に基づく利率

これは、従前の借入金（貸方）に着目した計算から、先ず経営資産（借方）に着目し、それと表裏の関係にある経営資本のコストを計算するよう発想を転換したものである。負債、資本それぞれが特定の資産に結びついていないことから、資本のコストも考慮することとなった。

(2) 利益率

利益率は先ず平均値としての標準利益率を設定し、これに事業特性調整係数（資本回転率の考慮）を乗じて基準利益率とし、さらに基準利益率に契約履行難易度調整係数を乗じて算出する。即ち

$$\text{標準利益率(\%)} = \frac{\text{標準営業利益} - \text{標準経営資本} \times \text{標準金利}}{\text{標準総原価}} \times 100$$

$$\text{基準利益率} = \text{標準利益率} \times \text{事業特性調整係数}$$

$$\text{利益率} = \text{基準利益率} \times \text{契約履行難易度調整係数}$$

ここで

$$\text{事業特性調整係数} = \frac{\text{標準経営資本回転率}}{(\text{標準経営資本回転率} + \text{当該事業の経営資本回転率})} \times \frac{1}{2}$$

$$\text{標準経営資本回転率(\%)} = \frac{\text{標準総原価}}{\text{標準経営資本}} \times 100$$

6. 終わりに

このように見てくるとⅠ期からⅢ期に至る間に理論的な発想は大きく変わったといえる。特に支払利率及び利益率は、積み上げられた製造原価プラス一般管理・販売費であるところの総原価に最後の段階で乗じられるものであり、その数値の大小による影響は大きく、今後とも不断の研究が必要であると考えられる。

情報セキュリティ意識教育について

研究員 是永 信孝

1 はじめに

秘密保全、情報セキュリティの重要性がクローズアップされ、技術的管理策、管理的管理策が施され、運用的管理策の一部として秘密保全教育、情報セキュリティ教育が行われているが、情報漏えいが後を絶たないのが現状である。

今回は秘密保全教育、情報セキュリティ教育に焦点を当て考察する。なお、秘密保全は、秘密情報のセキュリティであることから、事後、情報セキュリティ教育に包含して記述する。

2 情報セキュリティ教育の現状と問題点

情報セキュリティの教育は、知識教育、技能教育、意識教育に区分される。知識教育、技能教育の分野については、わが国においても、教育内容、到達基準などが示され、十分とは言えないが実施されているが、意識教育については、大部分実施されていないのが現状で、実施されても教育効果が上がらず、教育担当者からは、「本人の自覚に待つしかない」などの言葉が聞かれる。

情報セキュリティ意識教育が行われず、または、行っているのに効果が上がらない原因は、大きく以下の3つであると考えている。

その一つは、わが国の情報セキュリティ教育に関する基準、書籍などには情報セキュリティ意識の必要性について記述されているが、情報セキュリティ意識とは何か、意識教育の教育内容、到達基準などが具体的に示されていない。また、知識・技能教育については、これまでの学校教育の経験などから、その実施要領はイメージできるが、意識教育の実施要領について経験がなくイメージできない。

二つ目は、情報の特性に因るものである。情報は、法的には「無体物」とされ、目に見えにくい。また、意識の基盤となるリスクを構成する要素である情報資産の価値についても見えにくい。情報資産の価値は、知っているだけ、取り扱うだけでは生じない。情報を使用して重要な判断を行う、また、物造りなどに使用してはじめて価値を生じるものである。その価値の認識については、情報の使用によって利益を得た、または情報の漏えい等により損害を受けた人にしか認識できにくい。また、リスクを構成する要素である情報セキュリティ上の脅威及び脆弱性も目に見えにくい。

三つ目は、人間の特性によるものである。災害時の住民の避難などについて研究されている群馬大学工学部教授 片田敏孝氏の講演によると、「自分にとって都合の悪い情報を無視したり、過小評価してしまう人の特性」を「正常化の偏見 (normalcy bias)」と呼ぶ。その具体例の一つとして、交通事故と宝くじのそれぞれに対していただく、期待 (不

安)の違いを挙げ、交通事故に遭って死亡する確率は、宝くじの1等に当選するより高い。にもかかわらず、会社からの帰りに車に跳ねられると考えている人はほとんどいない。一方で宝くじには当選を期待して、多くの人が人気の売場に行列を作る。すなわち、自分に都合の悪いことについては「自分だけは大丈夫」「自分には関係ない」とする意識である。

3 情報セキュリティ意識とは

情報セキュリティ意識の具体的な教育内容の一例について紹介する。

本資料は、米国防総省が2005年に制定した「情報保証要因改善プログラム」(DoD 8570.1-M)に「導入及び意識向上訓練プログラムに盛り込むべき事項」として示されている。

「導入及び意識向上訓練プログラムに盛り込むべき事項」

- (1) 組織及び承認されたユーザーにとっての情報保証の重要性
- (2) 関連する法律、ポリシー及び手順、並びにそれらがどのように承認されたユーザーに影響を及ぼすか(例:著作権、倫理、行動基準)
- (3) スクリプト、キディー、クラッカー、ハッカー、抗議者、又はテロリスト・グループ若しくは外国に雇われたスパイなどの外部脅威の例
- (4) 悪意ある若しくは不的確な許可されたユーザー、テロリスト・グループ若しくは外国に雇われたユーザー、不満を抱いている従業員若しくは軍人、ハッカー、クラッカー、自ら招いた意図的若しくは意図しない損害などの内部脅威の例
- (5) 収集された非秘密情報が潜在的に有する取扱に慎重を要するレベルの高まり
- (6) ソーシャル・エンジニアリングから受ける承認されたユーザーのリスク
- (7) 重要なシステム情報及び手順を保護する一般的手法
- (8) ネットワークで接続されたシステムにおけるリスク共有の原則(一人の人物が受け入れたリスクがどのようにネットワーク全体に及ぼすことになるか)、及び物理的環境における変更の原則(例:水害、火事、塵埃)
- (9) リモート・アクセス関連のリスク(例:テレコミュティンク、作戦展開中、又は臨時勤務中)
- (10) Eメール状況(関連文書(DoDD 2500)などのプライバシー問題に係わる法的要求事項、及び給与、医療及び人事記録を含むシステムの保護の必要性)
- (11) マリヤス・コードの知識(例:論理爆弾、トロイの木馬、マリヤス・モバイル・コード、ウイルス及びワーム)。これらには、これらの攻撃方法、情報システムに損害を与える方法、不注意若しくは意図的な導入方法、及びユーザーによるこれら影響の軽減可能方法を含む。
- (12) 分散サービス妨害(DDoS)攻撃の影響、及びそれらを軽減することが可能なユーザー

ザーによる軽減可能方法

- (13) 適切なログオン、パスワードの利用、秘密情報の漏えい防止、Eメール・セキュリティなどの情報保証手順の遵守によるシステム情報セキュリティに自らが招く損害の防止方法
- (14) 組み込まれたソフトウェア及びハードウェアの脆弱性、国防総省におけるそれらの情報の収集方法（例：IAVA）及び承認されたユーザーに及ぼす影響
- (15) 国防総省システムに係わる禁止及び不正活動（例：ピアール・ツー・ピアール・ファイル共有、賭け事、個人的利用及び金儲け）
- (16) 情報の漏えい、承認されない又は不審な活動の報告要求事項及び手順、並びに連絡先情報保証オフィス
- (17) 情報の秘密区分、並びに NIPRNet 及び SIPRNet 上での情報の取扱の違い
- (18) 国防総省システム上でのライセンス制限を含むソフトウェア問題、暗号化、並びに媒体のサニタイゼーション及び手順
- (19) 情報作戦警戒指令（Information Operation Condition : INFOCON）の定義、及びそれが承認されたユーザーに及ぼす影響
- (20) 追加の情報及び訓練に係わる情報源

以上の中から情報セキュリティ意識に関する内容を抽出し、まとめると、情報セキュリティ意識を構成する主要な内容は、以下のように考えられる。

- ① 情報セキュリティ上のリスクを感じ取るマインド（心）
- ② 自分にもインシデントが起こるかも知れない、自分に関係するとする当事者意識
- ③ 情報セキュリティ上の対策（管理策）を実行する意志

4 情報セキュリティ意識教育の要領

意識教育の実施要領の基本は、「実践陶冶」と言われている。すなわち、知識を理解の域に高め、実際の経験・体験を通じ体感し、納得、または身にしみて感じることによりはじめて意識として定着するものである。従って、教育と言うより、訓練と呼ぶ方が適切と考えられる。なおこの際、問題点の項で取り上げた情報及び情報セキュリティ上のリスクが目に見えにくいことを考慮して、「リスク等の見える化」、正常化の偏見が起こらないように身近な事項を教育材料に使用するなどの配慮が必要となる。

教育・訓練要領の第1は、日常行っている業務の場での教育・訓練である。その題材は、「ヒヤリ・ハット」事例である。「ヒヤリ・ハット」とは、作業中・運転中に事故が起きそうな状況に出会いヒヤリとしたり、ハットしたことを記録し、その原因を全員で究明し再び事故の要因とならないようにする安全衛生活動である。安全管理及び品質管理の場面で導入されている。これは米国の安全技師ハインリッヒが発表した「1：29：300」の法則、すなわち「1件の重大事故が発生する背景には、29件の軽傷事故と300件のヒヤリ・ハットがある」に基づくもので、ヒヤリ・ハットの段階で地道に対

策を考え、実行して、良い習慣（意識）として身に付けていくものである。

そのためには、「ヒヤリ・ハット報告」の奨励が必要となる。業務を行う際に「ヒヤリ・ハット」した場合、即座に報告することである。この際、「ヒヤリ・ハット」を起こしたことについて厳しく指導してはいけない。「良く報告をした」、全員で「ヒヤリ・ハット」体験を共有しようとする態度が大切である。

その実施要領は、まず最初に「なぜヒヤリ・ハットで収まったのか」を考えさせ、事故にいたらず、「ヒヤリ・ハット」で納めることができたセキュリティ上の対策（管理策）の有効性を印象づけることが必要である。次にヒヤリ・ハットの原因となった要因について検討し、対策事項を考えさせ、その場で対策事項の演練を実施する。

次に大切なことは、現場小グループのリーダーによる「ヒヤリ・ハット」の掘り起こしである。情報セキュリティ上のヒヤリ・ハットは何もしなければ潜在化してしまい、また目に見えにくいため、現場を預かる小グループのリーダーの情報セキュリティ上のヒヤリ・ハットを見抜き、掘り起こすことのできる知識・技能・意識が必要となる。意識教育は現場小グループのリーダーの情報セキュリティに関する知識・技能・意識の向上がポイントとなる。

大事故の事例を教育材料として取り上げている例を見受けるが、次の理由により適当でない。

- ① 大事故の場合は、刑罰の重さ、影響の重大性などインパクトは大きいですが、突き詰めるところ、恐怖心に基づく印象付けであり、「セキュリティはなぜ破られたか」ブルース・シュナイアー著（日経 BP）によると、恐怖心に基づくものは、対応を行う際に、間違った対応、又は過剰反応を起こしやすいとされている。
- ② 自分の経験・体験とかけ離れているため、正常化の偏見を起こしやすい。
- ③ 意識教育を継続的に行うための事例の数に乏しい。

教育・訓練要領の2番目は、実際の業務と類似した教育・演習の場を設け、経験・体験させ、体感することにより、意識として身に付けさせることである。

教育・訓練要領の3番目は、教育担当者の巡回指導、管理者等による抜き打ち点検・検査、及び即時の現地・現物指導が必要である。

教育・訓練要領の4番目は、上級管理者が情報セキュリティに取り組む姿勢、情報セキュリティを考慮した日常業務の進め方を身をもって示すことにより感化することである。

また、意識は時間の経過とともに薄れていくことから、継続的に意識教育を行うとともに、意識向上のメッセージを繰り返し発していく必要がある。

米商務省の国家標準技術院が2003年示した「情報セキュリティ意識向上及び訓練プロ

グラムの構築 (NIST SP 800-50)」に「意識向上メッセージの普及方法」の一例が示されているので紹介する。

意識向上メッセージの普及方法

- ☆ 意識向上メッセージ付きツール (例: ペン、見出し、付箋紙、メモ帳、応急手当キット、メッセージ付きディスク、しおり、フリスビー、時計、gotcha カード)
- ☆ ポスター、「やるべき事及びやってはいけない事のリスト」、又はチェックリスト
- ☆ スクリーンセーバー及び警告バナー/メッセージ
- ☆ ニュースレター
- ☆ デスク・ツー・デスク・アラート (例: ハードコピーで明るい色の 1 ページ会報—各デスクに 1 枚、又はオフィス内の回覧—組織のメール・システムにより配布)
- ☆ 組織全体に及ぶ電子メール・メッセージ
- ☆ ビデオテープ
- ☆ ウェブベース・コンピュータベースによる講習 (e ランニング)
- ☆ 情報セキュリティデー、又は同様の行事
- ☆ セキュリティ連絡情報付きのポップアップ・カレンダー、月ごとのセキュリティ警告 (security tip)、その他
- ☆ マスコット
- ☆ クロスワード・パズル
- ☆ 賞品プログラム (例: 飾り額、マグカップ、感謝状)

5 おわりに

セキュリティ意識の重要な部分を占めるリスクを感じ取るマインドは、リスク (情報資産の価値、脅威、脆弱性) に関する知識なくしては生まれず、セキュリティ対策を実施できる技能を保持しなければ対策を実施する意志も生まれない。知識教育、技能教育、及び意識教育がバランス良く噛み合っ初めて、情報セキュリティ教育の効果が上る。

また、情報及び秘密は、情報を取り扱う人、秘密を取り扱う人だけでは、守ることができない。情報セキュリティ意識は、組織に属する人全員に必要な情報リテラシーといえる。

参考文献

- ・「セキュリティはなぜやぶれたのか」ブルース・シュナイアー著 日経 BP 社
- ・「情報資産のリスクマネジメント」小見志郎著 株式会社ぎょうせい
- ・「自分だけは大丈夫」セキュリティ対策を妨げる「正常化の偏見」 Itpro 記者の眼
- ・「情報保証要員改善プログラム (DOD 8570. 1-M)」 米国防総省

- ・「情報セキュリティ意識向上及び訓練プログラムの構築 (NIST SP 800-50)」米商務省国家標準技術院

◎ 「防衛取得研究」掲載の署名記事と見方はいずれも執筆者個人のもので、
(財)防衛調達基盤整備協会ないし執筆者の所属する機関の見方を代表する
ものではありません。

なお、記事の無断転載は禁じます。転載する場合には当協会までご連絡下
さい。

発行人 宇田川 新一

編集者 島 健治

発行所 (財)防衛調達基盤整備協会 防衛調達研究センター
TEL 03-3235-0711