

目 次

- | | | |
|---|-------------------------|-----|
| 1 | 日本造船業の現状と艦艇調達基盤の維持（その2） | 1 頁 |
| 2 | 多層防衛戦略の次に来る新生戦略 | 3 頁 |

目 次

- | | | |
|---|---------------------|------|
| 1 | 戦後の造船業界の動向について | 1 頁 |
| 2 | 現役時代を振り返って思うこと | 9 頁 |
| 3 | 企業現場における保全教育・指導のあり方 | 11 頁 |

日本造船業の現状と艦艇調達基盤の維持(その2)

主任研究員 宗吉道之

はじめに

昨今の資源高騰は、国内はもとより国際的にも各分野で大きな問題となっています。

国内の造船業界にあつては、商船の受注船価が回復し赤字受注の峠を越えたと思ったとたん、鋼材単価の上昇、搭載機器の価格アップ等により、またしても会社の業績の大きな負担要因となっています。

本稿では、昨年に引き続き「日本造船業の現状と艦艇調達基盤の維持」について考察します。

日本造船業の現状

日本は、下表のとおり韓国に平成17年に国別受注量(総トン数、シェア)で逆転され、平成19年には中国にも追い越されました。

暦年 国名	2004年(平成16年)			2005年(平成17年)			2007年(平成19年)		
	隻数	千総トン数	シェア(%)	隻数	千総トン数	シェア(%)	隻数	千総トン数	シェア(%)
日本	680	28,860	37.4	536	16,502	27.5	606	20,667	12.5
韓国	513	24,976	32.4	450	21,609	36.0	1,231	67,962	41.2
中国	480	10,974	14.2	517	10,621	17.7	1,698	58,012	35.2
世界合計	2,704	77,200	100	2,696	60,000	100	4,851	164,833	100

注1：Lloyd's Register 資料(World Shipbuilding Statistics)から作成、2007年は速報値
2：対象は100総トン数以上の船舶

平成19年の日本国内主要造船会社の決算は下表のとおりであり、船価上昇後の受注船の建造が本格化し、ユニバーサル造船の赤字幅も縮小、全社ともに前期と比較して業績が回復しています。

(単位：億円)

会社名 区分	三菱重工業	三井造船	ユニバーサル 造船	IHI	川崎重工業	住友重工業
売上高	2,839	3,023	1,869	1,608	1,413	513
営業利益	40	137	△41	24	32	約90
受注高	3,536	3,788	1,593	2,790	2,513	651

注：出典は海事プレス、各社とも船舶部門の連結

一方、平成19年の韓国造船会社の決算(12月)も下表のとおりであり、前期と比較して売上高及び営業利益ともに増収・増益となっています。

(単位：10億ウォン)

	現代重工	サムスン重工	大宇造船海洋	S T X造船	韓進重工HD	現代尾浦造船
売上高	9,778	8,292	7,368	4,513	1,700	2,898
営業利益	1,262	491	473	168	105	385

注：出典は海事プレス、各社とも造船・海洋部門を計上

以上の状況から日本の造船会社は、韓国等の造船所との競争力を維持するため更なる効率化、合理化が必要だと言えます。

艦艇調達基盤の維持

昨今の風潮から「防衛装備品の生産・調達基盤の維持」について論じると、『また古い体質の者が業界と結託して…』と非難されるかも知れませんが、私は防衛装備品調達の基盤の維持とは「防衛装備品を計画的に整齊と整備でき、限られた防衛予算(=税金)を無駄なく使用し、我が国が防衛に供し得る品質の防衛装備品を取得できる状態を施策によって意図的に作り出す」ことだと考えています。

艦艇調達は、平成11年度から原則として競争契約に移行し、競争契約に付された艦艇については大幅に契約金額が下がり契約がなされました。受注造船所は、当然、契約金額の低下分を社内と下請け会社に応分に負担させています。

一方、鋼材単価の上昇は、成立予算の材料単価が低いためその影響分を予算でカバーできないことから、造船所及び搭載装備品製造会社の中では『赤字受注はコンプライアンスに反することから、防衛装備品の受注を控える…』等の意見が出ていると聞き及んでいます。

また、防衛装備品の維持補修等に必要な汎用性のない純正部品については、従来、随意契約(その際、要求元が地方の場合は代理店等を通じ書類を契約相手方に送付して契約)としていたものを、最近は何でも安易に公募方式とし入札することにしたため、契約相手方を地方まで来させ入札させていると聞いています。

これは各省庁の随意契約件数がカウントされることから、単に随意契約を減らすことだけに囚われ、契約相手方に無用の負担を掛ける行為だと思います。

私は、汎用性のある装備品について当然競争契約を実施すべきと考えますが、防衛省独自の仕様により調達される主要装備品は当然、随意契約とすべきであると考えています。

日本の場合は、「武器輸出三原則」の制約もあり製造数が限られることから、防衛装備品の単価は輸入品と比較し割高となります。

欧米においては、「主要ビークル及びその動力源は国産」が常識であり、国内に技術がないものは止む無く輸入しています。

防衛装備品(軍需品)を輸出する国は、輸入国との紛争を考慮し高度な技術は供用せず装備品を輸出しているのが現状です。

そのため節操もなく安易に何でも輸入することは、有事において真に役に立つ防衛力の整備とはならないことを肝に銘じるべきです。

おわりに

日本の海上防衛力(=防衛省海上自衛隊艦艇)の整備は、この国が存在する限り終わりのない事業です。

防衛省(=海上自衛隊)は、艦艇の建造及び維持修理を民間造船会社に依存していますが、商船等と比較し利益率が少ない(最近赤字受注も想定される)艦艇建造事業から民間造船会社が撤退することも懸念されます。

今後とも艦艇の建造及び維持修理を民間造船会社に依存するのであれば、次のことを考慮する必要があります。

- ・ 随意契約する船と競争契約する船を分け、競争契約とする船の仕様書については調達予定の数年前から、競争契約に耐えうる仕様書を作成する必要があります。この場合、仕様書の作成にあたっては外注による等部外力の活用を考慮する。
- ・ 原価監査要員を増員し詳細な原価を把握することにより、次契約に反映させるなど赤字受注をさせない。
- ・ 護衛艦等建造に高度な技術を要する艦艇については、我が国の防衛基盤維持の観点から随意契約とし、造船会社の操業度を考慮のうえ発注する。
- ・ 1番艦については、受注希望の造船会社が真に防衛省の要求する艦艇を建造可能かを厳正に評価するシステムを構築する。

多層防衛戦略の次に来る新生戦略

研究員 菊池 浩

まえがき

情報セキュリティに係わる最近のインターネット情報には、多層防衛戦略の次に来る戦略として、広域防衛戦略(Defense-in-Breadth Strategy)、フルスペクトラム防衛戦略(Full Spectrum Defense Strategy)、ソフトウェア保証戦略(Software Assurance Strategy)などの用語が散見される。次に来る戦略としたが、これらによって多層防衛戦略がフェードアウトするのではなく、多層防衛戦略は新たな戦略の一部として引き継がれ、その重要性が後退することはない。

今回は、このような昨今の様々な新生戦略の現状及び広域防衛戦略を明確に定義している国家標準技術院(NIST)の特別出版物を紹介する。

新生戦略の現状

これらの新生戦略は、公開されている情報を見る限り、いずれも効果的かつ効率的なセキュリティの確保を目的として、そのセキュリティに係わる対象範囲をより拡大して捉えたものと理解できる。つまり、進化し続け、ますます巧緻化するセキュリティ脅威の攻撃から情報システムのセキュリティを確保するためには、慣行として常識化されている既存・既知の技術的、人的及びプロセス的セキュリティによる防衛に、例え綿密な設計の基に多層防衛戦略を導入したとしても、限界が生じるというのが新生戦略誕生の理由である。

このような新生戦略の考え方は、既に千年紀の幕開け当初から存在しており、例えば米国防総省のCIOオフィスは、2001年に「ますますその巧緻化及び多数化する脅威に対抗するには、多層防衛戦略から広域防衛戦略に移行する必要がある。」と公言している。しかしながら、その後における国防総省の情報保証¹戦略は、引き続き多層防衛戦略の導入を推し進めており、未だに、広域防衛戦略の具体像は無論のこと、その明確な定義さえも公表されていない。

また、フルスペクトラム防衛戦略を提唱しているセキュリティ・ベンダーは最近、「ますますその進化と複雑化の速度を速めているマルウェア(悪意のあるソフトウェア)に対応するためには、多層防衛戦略と広域防衛戦略を合わせたフルスペクトラム防衛戦略の導入が焦眉の急となっている。」としている。しかしながら、その細部は公表されていない。

ソフトウェア保証戦略は、端的に言えば、従来からのソフトウェア保証の考え方にセキュリティを考慮したものである。とはいえ、現在、国防総省及び国土安全保障省が共

¹ 情報保証：Information Assurance。情報セキュリティに同じ。

催している「ソフトウェア保証プログラム」では、関連する専門分野として、情報保証、プロジェクト管理、システム・エンジニアリング、ソフトウェア取得、ソフトウェア・エンジニアリング、セイフティ及びセキュリティの6つを掲げており、ソフトウェアが主要構成となる情報システムのライフサイクルに及ぶセキュリティに対応するものであることが伺われる。このプログラムも現在進行中のものであり、その成果に期待したい。

このような新生戦略の現状にあっては、唯一明確な定義付けを行うとともにその具体例を示しているのが、国家標準技術院が最近出版した文書であり、次項にそれを紹介する。

国家標準技術院特別出版物に見る広域防衛戦略

国家標準技術院特別出版物「情報システムからのリスクの管理(NIST SP 800-39, Managing Risk from Information Systems, April 2008)」は、その「2.5 サプライチェーンに起因するリスクの管理(Managing Risk from Supply Chains)」において、「グローバルなサプライチェーンからのサイバー脅威の侵入によるリスクを低減するには、戦略的かつ全組織的な広域防衛(Defense-in-Breadth)アプローチを採用した包括的情報セキュリティ戦略を考慮すべきである」としている。また、同出版物の用語の解においては、広域防衛を「(例えば、製品やシステムの設計と開発、製造、梱包、組み立て、システム・インテグレーション、流通、運用、保守及び廃棄に至る)情報システムのライフサイクルにわたって、同システムを保護するための包括的な情報セキュリティ戦略をいう」と定義している。

以下に、広域防衛戦略の具体像を明らかにするため、2.5 項の記述内容から広域防衛に係わる主要箇所を抜粋翻訳して示す。

サプライチェーンとは、組織、人、活動、情報及び資源から構成されるシステムであり、おそらくは国際的な範囲に及ぶものであって、消費者に製品やサービスを提供するものである²。国内及び国際的なサプライチェーンは、合衆国が世界中の市場において製造又は維持される製品やサービスへの依存性をますます高めていることから、合衆国の国家及び経済の安全保障利益にますますその重要性を高めている。サプライチェーンにおける不確実性、及び国際的サイバー脅威のますますの巧緻化や広がり、組織の運用、資産、個人及び他の組織、並びに国家に及ぼす不利な影響が広がる潜在的可能性をますます増大させつつある。グローバルな商用サプライチェーンは、公共及び民間セクターの組織(例：連邦政府機関、契約者)において日常的に利用される情報技術製品に対

² 国内及び国際的サプライチェーンにおける製品やサービスの例としては、ハードウェア、ソフトウェア及びファームウェア情報システム用構成部品、データ管理サービス、電気通信サービス・プロバイダー、並びにインターネット・サービス・プロバイダーがある。

し、敵対性が悪意のある操作を行う機会を与えているのである。しかもこれらの情報技術製品は、合衆国の重要インフラのアプリケーションを支える情報システムに利用されているのである。このようなサプライチェーンのいずれかの箇所における悪意のある活動は、それら情報システムによって支えられているミッション/ビジネス・プロセスに対して、リスクの拡大をもたらすことになるのである。

これらのリスクには、次が含まれる。

- (1) 悪意のあるコードその他のマルウェアが含まれている製品を情報システムに組み込んだ場合、当該情報システムには悪用可能なぜい弱性が導入されたことになる。
- (2) 適切なセキュリティを確実なものとするため、必要とされる多くのセキュリティ管理策の提供を商用情報技術製品に依存する場合、当該システムの信頼性を決定することが不可能又は困難となる。
- (3) 適切なセキュリティを確実なものとするため、(例：インストレーション、運用、保守など) 必要となる多くのセキュリティ管理策の提供を情報システム・サービス・プロバイダーに依存する場合、当該サービスの信頼性を決定することが不可能又は困難となる。

サプライチェーンからのリスクを低減するには、戦略的かつ組織全体に及ぶ広域防衛 (defense-in-breadth) アプローチを取り入れた包括的な情報セキュリティ戦略が考慮されるべきである。広域防衛アプローチは、システム開発ライフサイクル (すなわち、設計・開発、製造、梱包、組み立て、流通、システム統合、運用、保守及び廃棄の間) を通じた情報システム (システムを構成する情報技術製品を含む) の保護を支援するものである。この支援は、各ライフサイクル・フェーズにおけるぜい弱性の識別、管理及び除去、並びにリスクを低減するための補完的かつ相互補強的戦略の利用によって達成される。

このようなことから、可能であるなら、組織は次を実施すべきである。

- ベンダー及びサプライヤーが提供した情報技術製品及びサービスの出所を知ること。
- サプライチェーンにおいて、特定の有害な行為者が及ぼす不利な影響を局限化するため、様々なベンダー及びサプライヤーを利用すること。
- ベンダー及びサプライヤーが採用した情報技術製品の設計及び開発プロセスの透明性を求めること。
- 敵対性に悪意のある行為の機会を与えてしまう窓を削減するため、情報技術製品/サービスの取得決定時期と実際の製品/サービスの配送時期との間を短縮化

すること。

- マリシャス・コードの挿入確率を削減するため、情報技術製品及びシステムに対する標準パラメータの設定を利用すること。
- バイヤーの名称を含め、情報技術製品及びサービスの取得に係わる情報を保護すること。
- 情報技術製品及びサービスに対し、信頼性のある流通プロセスを導入すること。
- 新たに取得した情報技術製品に対しては、広範囲に及ぶ展開に先立つオンサイト・テストを行い、不正かつ隠された改ざんが行われる確率を削減すること。
- 信頼されたベンダー及びサプライヤーが提供する情報技術構成品を利用すること。
- 組織の階層化された防衛において、異なる部署のシステム管理者により、情報システムのアップグレード又は情報技術構成品の換装が行われる場合は、インサイダー脅威の削減を考慮すること。
- 外部の保守及びサービス・プロバイダーによる情報システムへのアクセスを厳しく制限し、悪意のある行為の発生確率を減少させること。

あとがき

空想科学映画や情報戦争の小説でのお話が身近に迫っているような感じをもたれるかもしれないが、その潜在的な現実化の可能性は否定できない。

2006年5月19日、米 국무省は、中国の **Lenovo Group** から購入した 15,000 台の **Lenovo ThinkCenter M51** デスクトップ・コンピュータ及び 1,000 台の **Lenovo ThinkCenter M51** ミニタワー・コンピュータからなる 16,000 台のコンピュータの利用について、セキュリティ上の問題から、センシティブな情報を取り扱うネットワーク上から外すと発表した。これは、「中国政府は、**Lenovo Group** に対する 27% の出資者となっている。したがって、中国の情報機関がその気になれば、不正行為を行うための秘密のハードウェア又はソフトウェアをパソコンに挿入することができる」との米議会や政府高官の指摘によるものであった。もちろん、**Lenovo Group** 責任者からの「途方もない空想だ」との批判もあった。

潜在的な実現可能性があるのであれば、セキュリティ上、何らかの対策を講ずるのは責任ある組織の対応と思われる。単に「国民からの税金を無駄にしないため、低価格のコンピュータの購入に決定した。」とする 米 국무省 調達 担当者 の 考え は、サイバースペース・セキュリティ上の観点から無理があったことは否めない。

この騒動から、今回紹介した国家標準技術院のサプライチェーンにおけるリスク低減策が、しみじみと実感できるのではなかろうか？

◎ 「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迄、御連絡下
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