위협관리시스템(TMS) 소프트웨어 분리발주 BMT 사례

이상복*, 곽행신*, 신석규*
*한국정보통신기술협회 S/W시험인증센터
e-mail:{jangpo, kwak, skshin}@tta.or.kr

A Case on TMS(Threat Management System) BMT Software Separated Acquisition

Sang-Bok Lee*, Hang-Sin Kwak*, Seok-Kyoo Shin*
*S/W Quality Evaluation Section 4, S/W Quality Evaluation Center,
IT Testing & Certification Laboratory

요 약

공공부분 S/W사업은 분리발주가 원칙이고 일괄발주가 예외지만 현재 많은 공공부분 S/W사업은 일괄발주 사업으로 진행되고 있다. 일괄발주는 SI업체가 S/W업체도 선택하여 입찰 및 개발하기 때문에 발주자가 원하는 품질 좋은 S/W를 선택할 수 없고, 발주자가 S/W를 업그레이드 및 확장할 때 SI업체에 의존하게 되는 단점이 있다. 이런 단점을 보완하고, S/W분리발주를 활성화시키기 위해 지식경제부(구 정보통신부)에서는 S/W분리발주 매뉴얼을 작성하여 보급 및 교육을 하고 있으며, 발주처에서는 품질이 우수한 S/W를 선택하기 위한 S/W분리발주 BMT를 공인된 시험기관인 한국정보통신기술협회(TTA) SW 시험인증센터에서 BMT를 실시하고 있다. 본 논문은 위협관리시스템(TMS) S/W분리발주 BMT를 공인된 국가 시험인증기관인 한국정보통신기술협회(TTA) SW시험인증센터에서 수행한 사례를 기술하였다

1. 서론

일괄발주 방식에서는 SI업체가 S/W를 선택하여 S/W사업을 진행하므로 발주기관에서 원하는 우수한 품질의 S/W를 사용할 수 없었으며, S/W개발회사는 SI업체에 납품하는 SW의 정당한 가격도 보상받지 못하는 상황도 발행하게 되었고, 전체 공공부분 SW사업 및 SW산업 기반을 취약하게 만드는 원인을 제공하기도 하였다.

공공부분 S/W사업은 분리발주가 원칙이나 현재 대다수의 공공부분 S/W사업은 일괄발주로 진행되고 있다. 이에 지식경제부(구 정보통신부)에서는 발주기관에서 필요로 하는 품질이 우수한 S/W를 발주하기 위해 SW분리발주 매뉴얼을 보급하여 S/W분리발주를 활성화시키기 위해 부단한 노력을 하고 있다.

S/W분리발주 사업에서 여러 S/W업체들이 사업에 참여하고 있으며 제안한 SW중에 발주처에서 요구하는 제품을 선택하기 위해 BMT를 수행하게 되었으며, 발주처에서는 BMT 수행 시 공정한 시험을 수행할 수 있는 기관, 풍부한 경험과 노하우를 갖추 기관에서 BMT를 수행하기를 원하고 있다. 국내에서는 정부공인 시험인증 기관인 한국정통신기술협회(TTA) SW시험인증센터에서 SW분리발주 BMT를 수행하여 풍부한 경험이 있고, S/W시험인증센터에서는 발주처에서 요구하는 BMT를 공정하게 수행하여 몇몇 기관에서 SW사업이 성공적으로 수행되었으며, 이러한 노력으로 인해 첨차 BMT를 통한 S/W분리발주 사업도 증가하는 추세이다.

본 논문에서는 S/W분리발주 BMT 사례를 기술하여 S/W분리발주 BMT에 대한 정보를 제공하는데 목적이 있다. 2장에서는 SW분리발주 BMT 소개 및 절차에 대해 설명하고 3장에서는 한국정보통신기술협회(TTA) SW시험인증센터에서 수행한 위협관리시스템(TMS) BMT를 소개하고, 4장에서는 침입방지시스템 BMT 수행 방법을 설명하였다. 최종적으로 5장에서는 결과 및 향후 진행방향에 대해서 기술하였다.

2. 관련연구.

2.1 소프트웨어 분리발주 BMT

분리발주는 H/W, S/W 등을 일괄하여 계약하지 않고 각각 구분하여 발주 및 계약하는 형태를 말하며 개별시스템 단의 또는 패키지 S/W 등의 분리하여 BMT수행 후 우수한 제품을 선정하는 발주 형태를 소프트웨어 분리발주 BMT라 한다.

o 분리발주 대상사업 및 S/W의 기준

- S/W사업중 예산기준으로 총사업규모가 10원 이상인 사업에서 단일 S/W가액이 5천만원 이상인 경우는 해당 S/W를 분리발주 실시(SW분리발주 가이드라인)
- 총사업규모가 10억원 미만 단일 S/W가액이 5천만원 미만이라도 GS인증 등 품질인증을 받은 S/W는 분리발주 검토(기획예산처 예산편성지침)
- 품질인증을 받지 않은 S/W도 시스템 품질향상 등을 위해 필요하다고 판단될 경우 분리발주 가능[1]

2.2 소프트웨어 분리발주 BMT 절차

(1) BMT 대상선정
- 발주기관은 BMT 대상을 선정하여 TTA에 BMT 수행 요청

(2) BMT 수행계획 수립
- BMT 대상 및 제안요청서 분석
- 발주기관의 의견을 반영하여 BMT 환경, 평가항목 및 절차 등 BMT 수행계획 수립

(3) BMT 수행계획 심의
- BMT 심의위원회를 구성하여 BMT 수행계획 심의 의뢰
- BMT 평가항목, 세부평가항목 및 항목별 배점 등 심의
- TTA는 BMT 심의위원회에서 심의한 결과를 BMT 수행계획에 반영하고 발주기관에 통보

(4) 사업수행계획 공고
- 발주기관은 제안요청서, 제안안내서, 및 BMT 수행계획 공고

(5) 제안설명회 및 의견 수렴회 개최
- 발주기관은 제안요청서 및 제안안내서 내용 설명
- TTA가 BMT 수행계획서 설명
- BMT 참여업체는 사업수행계획에 대해 의견 제시
- 발주기관은 의견 수렴 결과를 TTA 통보

(6) BMT 세부 수행계획 수립
- TTA는 의견수렴 결과를 반영하여 세부평가항목, BMT 시나리오, 예상 결과, BMT 일정, 투입인력 및 업체 준비사항 등 BMT 세부수행계획 수립

(7) BMT 접수
- BMT 참여업체는 BMT 신청서, BMT 대상 제품 및 기타 요청 자료 제출
- TTA는 BMT 참여업체에 업체별 BMT 일정 및 BMT 세부 수행계획 통보

(8) BMT 환경구축
- TTA는 BMT 수행에 필요한 BMT 환경(하드웨어, 소프트웨어, 네트워크 등) 구축
- 서버 및 클라이언트 장비에 운영체제 및 성능시험도구 설치

(9) BMT 수행
- BMT 대상제품 설치
- 평가항목(기능성, 성능, 사용성, 안전성 등)별로 BMT 수행(BMT 수행 시, BMT 참여 업체 담당자 참석)

(10) BMT 결과서 작성
- BMT 결과서 작성 후, BMT 심의위원회에 BMT 결과 심의 의뢰

(11) BMT 결과 심의
- BMT심의위원회는 BMT 결과 심의
- TTA는 BMT심의위원회 심의결과를 반영한 BMT 결과서를 발주기관에 송부

3. S/W분리발주 BMT 고려 사항

S/W분리발주 BMT 수행 전 발주처, BMT수행기관, 제안업체의 고려사항에 대해서 간략하게 기술한다.

3.1발주처(기관)
- o S/W사업 계획수립 시 S/W에 대한 이해가 필요하며, BMT 관련하여 BMT 평가기관과 협의해야함
- o S/W사업일정 계획수립 시 BMT 일정도 포함시켜 일정을 수립해야함
- o S/W사업 및 BMT에 관련하여 업체에게 사전공지 해야함

3.2 BMT 수행기관
- o 발주처에서 제안하는 환경과 유사하게 BMT 시험환경(H/W, S/W)를 구성해야함
- o 객관적인 BMT 평가항목 및 평가방법을 도출해야함
- o 공정한 BMT를 수행해야함
- o BMT심의위원회 심의위원은 평가대상 제품 및 분야의 전문가를 위촉해야함

3.3 제안업체
- o 사업제안 설명회 및 BMT 설명회 개최 시 필히 참석하여 사업 및 BMT관련 정보를 확인해야함
- o 업체에서 제안하는 S/W제품 및 BMT 준비물을 철저히 준비하고 제출해야함

4. 위협관리시스템(TMS) SW분리발주 BMT

한국정보통신기술협회(TTA) S/W시험인증센터는 국내 유일 국가공인 S/W시험인증 기관으로 공신력 있는 시험을 수행하고 있어 S/W분리발주 BMT를 추진하는 발주처에서 BMT 의뢰하고 있다. 논문에서 기술하고 있는 위협관리시스템(TMS) S/W분리발주 BMT 사례는 발주처의 보안관제 시스템을 구축 시 S/W에 대한 BMT 사례이며 BMT 협의, BMT 환경, BMT 항목, 심의위원회, BMT 수행, BMT 결과 등 BMT에 관련한 일련의 제반사항, 절차 및 수행에 대해 기술하였다.

4.1 BMT 협의사항
- o 발주처에서는 S/W발주 사업의 일련의 정보(제안서, 요구사항, 구축 S/W제품 정보, 사업기간 등)의 정보를 TTA에 사전에 협의하기 위한 회의를 TTA에 BMT 담당자와 갖으며 대략적인 BMT 수행계획을 수립한다
- o TTA에서는 발주처에서 요구하는 BMT 정보를 바탕으로 BMT 세부계획을 작성하며 심의위원회를 구성하여 BMT에 관련한 정보를 심의위원회에 상정하여 충분한 검토를 받고 BMT를 수행한다.
- o BMT 환경, BMT 항목, BMT 배점은 발주처의 요구사항을 반영하여 시험 시나리오, 결과측정방법 및 BMT에 필요한 H/W 및 S/W(시험도구, 성능도구 등)를 공정하게 시험할 수 있도록 BMT를 수행하기 위한 모든 제반사항을 준비한다.
- o BMT 수행한 결과를 심의위원회 심의 이후 발주처에서 요구한 일정에 따라 결과서를 발송한다.

4.2 BMT 심의위원회

BMT 심의위원회의 역할은 BMT 수행 전에 BMT환경 및 BMT 항목 검토를 통해 BMT의 공정성을 확보하는 것이며 BMT 수행 중 발생한 이슈사항에 대한 검토한다. 또한 BMT 수행이 종료되고 결과에 대한 공정성과 정확성을 최종적으로 심의한다 대략적인 심의위원회 역할은 아래와 같다.

o BMT 환경 및 평가항목 심의
o BMT 이슈사항에 대한 검토 및 심의
o BMT 결과 심의

4.3 BMT 평가환경

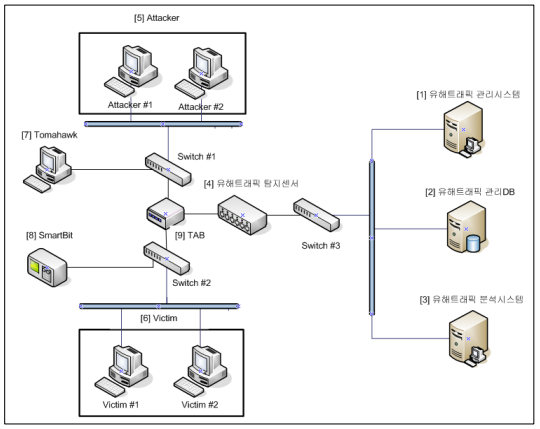
(1) 위협관리시스템(TMS)

전사적 IT인프라의 위협정보들을 수집/분석/경보/관리하는 정보보호 통합관리시스템이며, 실시간으로 공신력 있는 대외정보기관의 위협정보들을 수집/분석하여 정보보호 관리자에게 제공함으로써 각종 보안위협으로부터 사전대응 및 경/예보 체계를 구축하고 이를 통해 알려지지 않은 공격들에 대한 조기 대응을 유도하는 시스템을 가리키며 아래와 같은 제품 및 기능을 포함하고 있다.

o EMS, IDS, IPS 등을 기반으로 위협관리시스템 구성
o 정보수집, 정보분석, 대응기능, 종합상황관제, 네트워크 관리 기능 등 제공

(2) BMT 시험환경

발주처에서 제안 및 구성하고 있는 네트워크 환경과 유사하게 시험환경을 구축하며, 공격 클라이언트(Attacker), 공격대상 서버(Victim), 네트워크 TAB/Switch, 성능도구(Smartbits), 유해트래픽탐지센서, 유해트래픽 관리시스템, 유해트래픽 관리DB, 유해트래픽 분석시스템을 BMT 시험환경으로 구성한다. 아래 (그림 1)은 침입방지시스템의 BMT 시험 환경을 보여준다.



(그림 1) BMT 환경구성도

- Attacker : 유해트래픽 발생 도구를 사용하여 Victim을 공격함
- Victim : 공경대상 시스템
- SmartBits : 네트워크상에 트래픽을 발생해 실세계와 비슷한 네트워크 환경을 구축하기 위한 시험도구
- Tab/Switch : 인라인 방식으로 Tab를 이용하여 발생한 트래픽을 유해트래픽 탐지센서에 전송
- Tomahawk : 유해트래픽을 발생시키는 시험도구
- 위협관리시스템(TMS) : 유해트래픽 탐지센서, 관리시스템, 관리DB, 분석시스템으로 구성

4.4 BMT 평가항목

BMT 평가항목은 발주처의 요구사항을 최대한 반영하며 사업제안서에 기술된 사항을 기반으로 기능성, 사용성, 이식성, 효율성 등의 품질항목 기반으로 평가 항목을 도출한다.

위협관리시스템(TMS) BMT 사례에서는 발주처와 협의한 결과 기능성, 사용성, 이식성을 제외하고 효율성의 성능 평가항목인 유해트래픽 탐지센서의 성능(최대 처리량), 유해트래픽 탐지센서의 탐지능력 및 차단기능, 분석데이터 처리 능력의 성능항목에 대해서 BMT 수행을 결정하였다. 또한 보안전문가로 구성된 심의위원회에서 각 항목에 대한 객관성, 시험방법 및 환경에 대해서 심의를 거쳐 최종적으로 BMT 평가항목을 결정하였다[2].

<표 1> 평가항목

SW	평가항목	비 고
TMS	유해트래픽 탐지센서 처리 성능	
	유해트래픽 탐지센서 탐지 및 차단 성능	
	분석데이터 처리 성능	

4.5 BMT 수행

BMT 수행은 발주처에서 사업공고 마감과 동시에 제출한 업체를 대상으로 진행하며 사전에 사업설명회, BMT 설명회를 통해 BMT관련한 정보를 업체에 사전에 공지한다. 사업공지가 마감되면 업체에 시험일정이 통보되며 각 업체는 일정에 따라 BMT 평가를 받으며 평가원이 평가항목에 따라 평가를 진행한다.

(1) BMT 수행 시 고려사항

o 제안업체에 수에 따라 순번과 일정을 정하며, 해당업체는 일정에 맞추어 BMT 진행함
o BMT 참석할 수 있는 업체 담당자는 3명까지 참석가능하며 사전에 업체 담당자 정보를 TTA에 제공해야함
o BMT 수행 중 이슈사항이 발생하며 BMT 평가 담당자에게 제기할 수 있음
o 평가 담당자의 지시를 불이행하거나 업체 준비가 소홀히 하여 BMT 수행이 불가능할 경우 평가담당자가

BMT를 중지시길 수 있으며 업체는 이의를 제기할 수 없음

(2) 평가항목에 대한 평가 방법

o 유해트래픽 탐지센서 처리량 성능측정 : 다양한 사이즈의 트래픽을 시험도구를 이용하여 IGbps만큼 트래픽을 발생하여 손실 없이 유해트래픽 탐지센서가 처리할 수 있는 최대량을 측정함

<표 2> 처리량 기준

처리여부	평가기준	비 고
처리량	975M 이상 ~ 1,000M 이하	
	950M 이상 ~ 975M 미만	
	925M 이상 ~ 950M 미만	
	900M 이상 - 925M 미만	
	900M 미만	

o 유해트래픽 탐지 및 차단 성능측정 : 다양한 사이즈의 트래픽을 600Mbps 만큼 백그라운드 트래픽을 시험도구를 사용하여 발생하고, 심의위원회에서 선택한 20개의 유해트래픽을 Tomahawk 및 Attack 도구를 사용하여 발생시켜 유해트래픽 탐지센서가 탐지하고 차단하는 성능을 측정함

<표 3> 탐지비율

탐지여부	평가기준	비고
탐지비율	85% 이상	
	65%이상 ~ 85%미만	
	45%이상 ~ 65%미만	
	45%이상 ~ 65%미만	

o 분석데이터 처리양 : 시험도구를 이용하여 발생한 여러 유형의 트랙픽을 유해트래픽 탐지센서가 처리한 데이터를 분석서버에서 분석한 처리량을 측정

<표 4> 분석 처리률

처리능력	평가기준	비 고
처리시간(초)	5초	
	4초	
	3초	
	2초	
	1초	

4.6 BMT 결과 통보

측정한 BMT 결과를 가지고 보고서를 작성하며 보고서 내용에는 BMT 환경, BMT 평가항목, BMT 결과를 기술한다. 또한 BMT결과에 각 업체별 BMT 결과, 항목별 BMT 결과를 비교테이블 형식으로 제공하고, 발주처에만 결과서가 통보된다. BMT 결과를 발주처에 통하기 전에 BMT 결과 심의위원회를 개최하며 BMT수행 이후 나온 결과를 객관적인 관점에서 최종적으로 심의한다.

4.7 분리발주 BMT 사례 정보

S/W분리발주 BMT 사례에 대한 정보를 확인하기 위해서는 한국정보통신기술협회(TTA) SW시험인증센터에 문의가 가능하고, http://www.tta.or.kr 및 http://www.goodsoftware.or.kr 홈페이지의 분리발주 페이지에 가면 분리발주 BMT 목록 및 자세한 정보를 확인할 수 있다[3].

5. 결론

본 논문에서는 위협관리시스템(TMS) S/W분리발주 BMT 사례를 기술하여 S/W분리발주 사업의 핵심인 BMT 수행에 대한 정보를 제공함으로서 발주처에서 성공적으로 공공부분 S/W사업을 수행할 수 있고, 국내 S/W 품질은 높이는 기회가 될 수 있으며 S/W산업 진흥에도 큰 도움이 될 것이다.

아직까지 국내 공공부분 S/W사업에서 S/W분리발주 사업은 미흡한 실정지만 성공적으로 진행된 S/W분리발주 사업의 사례가 지속적으로 증가한다면 앞으로 S/W사업은 일괄발주가 아닌 S/W분리발주 사업으로 진행될 것이며, S/W분리발주의 핵심인 BMT도 중요한 부분을 차지하게 될 것으로 예상된다.

참고문헌

[1] 정부통신부 “분리발주 매뉴얼 2007”

[2] S/W시험인증센터 “BMT 평가방법연구보고서”, 한국정보통신기술협회

[3] http://www.goodsoftware.or.kr