

[OSS 라이선스 이슈사례] 미 국방부의 Opensource 활용

한국소프트웨어진흥원
한글과컴퓨터 컨소시엄

<문서 정보>

일자	VERSION	변경내역	작성자
2008.10.08	0.1	초기 작성	박준완
2008.11.03	1.0	내용 추가 작성	박준완

목 차

1. 문서 개요	4
가. 문서의 목적	4
나. 참고사항	4
2. 공개SW 라이선스 신규 이슈 정보	5
가. 이슈사항	5
나. 원문	5
다. 이슈내용	8
3. 이슈사항이 공개SW에 미치는 영향	10
4. 참고사항	10

1. 문서 개요

본 문서는 공개SW 도입컨설팅 사업의 공개SW 라이선스 분석지원 사업을 통해 현 산업에 적용되고 있는 라이선스 사례 및 신규 라이선스 이슈에 대한 정보를 제공하기 위해 제작되었다.

가. 문서의 목적

다음과 같은 세부적인 목적을 달성하기 위하여 작성되었다.

- 라이선스 사례 및 신규 라이선스 이슈 정보 제공

나. 참고사항

- 공개SW 라이선스의 시장 변화에 대해 확인할 수 있다.
- 기존 공개SW 라이선스에 대한 분쟁 사례에 대해 확인할 수 있다.

2. 공개SW 라이선스 신규 이슈 정보

가. 이슈사항

구 분	내 용	비 고
이슈 정보	미국방부(펜타곤)의 Opensource 활용	
발표 일자	2008-10-08	
홈페이지	www.gcn.com	

나. 원문

Pentagon : Open source good to go

Military IT folks wondering if their use of Apache, Perl, Linux and other open source software is copacetic with the brass will soon get some answers from the Defense Department's Office of the Chief Information Officer.

The office is preparing a memorandum that further clarifies how open source may be procured and used within the services.

The memo should answer many lingering questions still surrounding the open source, said Daniel Risacher, the data strategy leader for the Office of Secretary of Defense who is drafting the memo. The draft may point out some potential benefits as well.

"Those factors that are in favor of open source have not been appreciated to date," said Risacher, speaking at the Red Hat Government Users and Developers conference, being held today. The DOD CIO office is aiming to release the memo by early November.

From Risacher's description of the draft, the memo may reinforce the acceptability of using open source software within the Defense Department, as well as for other federal agencies. It may even broaden procedures for procuring commercial software.

"Those mandates [in which] we have to consider commercial off-the-shelf software, we have to apply that to open source software as well," Risacher said. "And that is not well appreciated within government."

Risacher said that he first started working on the memo last summer at the behest of the Defense Deputy CIO, David Wennergren. Although widely used in federal government, open source software, due to its unusual form of distribution, has raised questions among regulation-minded program managers.

In 2004, the Office of Management and Budget, issued a memorandum, M-04-16, that called on agencies to exercise the same procurement procedures for open source as they would for commercial software, as per guidelines set in OMB Circulars A-11 and A-130 and the Federal Acquisition Regulation policies. And in 2003, then-defense CIO John Stenbit issued memo reminding services that any open source software they use should be held to the same levels of security and licensing accountability as commercial software.

The new memo aims to address various questions that have arisen since these memos.

One of the primary issues to be addressed is if open source software is a form of commercial off-the-shelf software (COTS). The Defense Department has a number of mandates that compel the services to seek COTS software packages before commissioning custom code. If open source is COTS, then it needs to be included in the procurement process.

It is, Risacher confirmed. Risacher notes that COTS is generally defined as "software that is for sale, lease or licensed to the public, and is available to the government as well." Open source fits under this definition.

The memo should also dispel lingering ideas that open source software may not be used because it is a form of shareware or freeware. A 2003 policy, titled Information Assurance Implementation (8500.2) states that the military should not use "freeware" or "shareware" software.

Risacher noted that the policy stated shareware and freeware should not be used

because the "government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government," as the policy states. Obviously, Risacher argued, open source would not apply to these conditions.

The memo will also confirm that it is acceptable for an agency to contribute source code back into a public open source project. It is acceptable, Risacher qualified, assuming the agency has the rights to the code, that releasing the code is in the government's interest and that sharing the code does not violate any other government restrictions, such as the International Traffic in Arms Regulations (ITAR). Risacher also cautioned that government employees may not copyright any work that they do, so any contributions will be in the public domain.

In addition to defining the relationship open source has with COTS, shareware and copyright, the memo may also articulate some of the possible advantages of deploying open source.

When we use the term "open source software," we are actually talking about three inter-related things, Risacher explained. One is the body of code of the software program, which, like the software itself, is freely available. Another aspect is the development methodology, which encourages volunteer developers to help write the code. And the third aspect of open source is the licensing, which sets the rules for the lightly-controlled creation and usage of the software.

Defense agencies could benefit from all these aspects, Risacher said. By using open-source software, the services can update their software as soon as a vulnerability is found or an update is needed, rather than wait for the vendor to supply a patch. Open source also promises faster prototyping of systems, and lower barriers to exit. And if a government-written application is released into open source, outside developers could work to fix the problem, lowering maintenance costs of software.

Open source also tends to have fewer restrictions than proprietary software, Risacher said.

"We have a lot of examples of restrictions in end user licenses that turn out to prevent the DOD from doing things [it] wanted to do," he said. "We find that problematic."

다. 이슈내용

팬타곤 : 오픈소스 순조롭다

by Joab Jackson

미 국방부의 IT 장교들에게 국방부 수석 정보원의 사무실에서 아파치, 펄, 리눅스 및 여러 오픈소스 소프트웨어를 사용하는 것이 훌륭하다는 좋은 답변을 얻을 것이다.

미 국방부에서는 오픈 소스가 서비스 내에서 사용 및 조달되는 것에 대한 각서를 준비하고 있다.

각서는 오픈소스 주변에 많은 여러가지 질문들에 대한 답변이 될 것이라고 각서의 초안을 작성중인 국방장관의 오피스 내에 데이터 전략 리더 Daniel Risacher가 말했다. 초안은 몇몇 잠재적인 이득을 지적할 지도 모른다.

Risacher은 RedHat 정부 사용자와 개발자 컨퍼런스에게 빗대어 말하면서 "공개자료를 찬성하고 있는 여러 요소들이 시대에 뒤떨어지기 위해 인정되지 않은 것" 이라고 말했다. DOD CIO오피스는 11월까지 각서를 발표할 예정이다.

Risacher의 초안의 내용을 토대로 각서는 다른 연방국들 뿐만 아니라 국방부 내의 오픈소스 소프트웨어 사용의 승인을 강화할 지도 모른다. 그것이 상업적인 소프트웨어 사용 절차를 확장할지조차 모른다.

"그런 명령들에서 우리는 상업적인 소프트웨어를 고려해야 한다. 우리는 오픈소스 소프트웨어에 그것을 또한 적용해야 한다" 라고 Risacher는 밝혔다. "그리고 그것이 정부 내에서 잘 평가되지는 않는다."

Risacher은 그가 처음으로 각서에 대해 일을 시작한건 지난 여름 Defense Deputy CIO인 David Wennergren의 부탁을 받고서라고 말했다. 연방정부에서 오픈소스 소프트웨어를 폭넓게 사용하지만 배급의 형태가 일반적이지 않아서, 규정을 가지려고 하는 프로그램 매니저 사이에 여러가지 질문을 떠올리게 했다.

2004년 경영예산 부서에서 각서를 통해 상업용 소프트웨어를 위해 가이드라인을 결정했을 때 똑같은 획득 절차를 발휘할 것을 요구한 M-04-16은 A-11와 A-130 OMB 회람과 연방 인수 규제 정책으로 부터 시작되었다. 그리고 2003년 그때 Defense CIO인 John Stenbit은 사용하는 모든 오픈 소스 소프트웨어가 상업용 소프트웨어의 보안과 라이선싱 책임의 정도가 똑같아야 한다는 각서를 만들었다.

새로운 각서는 이 각서 이후 생겨난 다양한 질문에 대해 검토할 예정이다.

중요한 이슈중의 하나는 오픈소스 소프트웨어가 상업적인 소프트웨어와 모양이 같은

경우이다. Defense Department는 서비스에 주문번호를 위임하기 전에 상업적인 소프트웨어를 찾는 많은 작업을 진행한다. 만약 공개자료가 상용 소프트웨어와 같은 모양을 같은다면 그 경우에는 같은 조달과정을 지켜야할 필요가 있다.

그것을 Risacher는 확인했다. Risacher는 일반적으로 상용 소프트웨어가 "소프트웨어는 판매되어야 하고 일반적인 라이선스 또는 임대 가능하며, 정부에서 사용할 수 있어야 한다"고 정의했다. 이 정의아래 오픈소스는 포함된다.

또한 각서는 오픈소스 소프트웨어가 프리웨어나 셰어웨어와 같기 때문에 사용해서 안 된다는 오래된 아이디어를 쫓아야 한다고 한다. 2003년 정책에 Information Assurance Implementation(8500.2)에는 국방부에서 프리웨어나 셰어웨어를 사용하지 말아야 한다고 되어있다.

Risacher은 정책에서 프리웨어나 셰어웨어를 사용하지 말아야 한다고 한 이유는 "정부는 원소스에 접근할 수 없거나 정부를 대신해 수정할 사람이 없을 경우"이기 때문이라고 말한다. 명백히 Risacher는 오픈소스 소프트웨어가 이 정책에 적용되지 않는다고 얘기한다.

또 각서는 오픈소스 프로젝트에서 소스코드를 제공받는 것은 받아들이기만 한다고 확인할 것이다. 그것은 International Traffic in Arms Regulation(ITAR)에 있는 어떤 다른 정부의 규칙을 위반하지 않는다는 것을 의미한다. 그래서 모든 Copyright가 공공의 도메인에 있을 것이며 모든 일을 저작권으로 보호할 수 없다고 경고했다.

상용 소프트웨어와 오픈소스와의 관계를 정의하는것에 추가로 셰어웨어와 copyright를 정의한다. 각서는 아마 오픈소스를 널리 퍼지게 하는데 가능한 유리한 몇가지가 될 것이다.

우리가 오픈소스 소프트웨어를 사용할 때, 3개의 관련되는 것에 대해 Risacher는 설명했다. 첫번째는 소프트웨어 프로그램 코드의 내용을 말하며, 그 자체로 소프트웨어 자신을 가리키며, 자유롭게 사용할 수 있다는 점이다. 또 다른 것은 지원한 개발자를 독려하여 코드를 쓰도록 돕게하는 발전 기법이다. 마지막 3번째는 소프트웨어의 사용과 창조를 위한 규칙을 설명하는 라이선싱이다.

Risacher는 Defense Agencies 들이 이 모든 것으로부터 이익을 얻을 수 있었다고 말했다. 오픈소스소프트웨어를 사용함으로써, 서비스는 취약점을 찾거나 업데이트 패치를 공급할 판매자를 기다릴 필요없이 필요에 의해 바로바로 소프트웨어를 업데이트할 수 있다. 만약 정부가 사용하는 프로그램이 오픈소스로 발표된다면 외부 개발자들이 소프트웨어의 비용 아래로 문제를 해결할 수 있다.

Risacher는 오픈소스 소프트웨어가 상용 소프트웨어보다 더 적은 제한을 가지고 있는 경향도 있다고 말했다.

3. 이슈사항이 공개SW에 미치는 영향

오픈 소스 소프트웨어를 사용하는데 있어서 가장 큰 문제점으로 꼽는 것이 소스가 오픈됨에 따른 안정성, 즉 보안에 관련된 문제이다. 이번에 세계에서 가장 보안이 강력한 곳으로 알려져 있는 미 국방성의 오픈소스에 관련된 옹호의 글이 발표되면서 기존에 오픈소스에 부정적인 시각을 가지고 있던 많은 회사들이 생각을 돌릴 수 있는 계기가 마련되었다. 이후 DOD CIO에 의해 발표될 각서에서는 공개SW가 상용 SW에 비해 낡은 점들과 공개SW 사용시 주의해야할 사항들이 포함될 것으로 생각되며, 이 각서가 발표된 이후 시장에 오픈소스에 대한 인식이 좀더 많은 변화를 보일 것으로 기대된다.

4. 참고사항

http://www.gcn.com/online/vol1_no1/47320-1.html?page=1

<http://www.opensource.org>