

軍과 OSS

2018 5 14

고건

오픈소스 소프트웨어 재단 이사장
이화여자대학교 석좌교수

Why OSS in DoD?

- 종속 탈피
- 초연결
- 보안
- 예산
- 자주국방 ← 기술독립 ← OSS

```
Local:      opensource /software-andthe/
Remote:    departmentofdefense @ origin
Head:      24m24el @ (http://github.com/opensource/
```

```
Untracked files:
  emacs-mew.org
```

```
Unstaged changes:
  modified      emacs-linux.org
  modified      emacs.org
```

```
Unpushed commits:
24m24el No need to specify fixed width.
3fae22d Default keys foremw.
2a70flc Better initialization of Emacs.
```

```
: dot-files*
```

```
/w/technical/emacs :master
~/work/dot-files :master
README.md          emacs-f2.org
bin                emacs-fixes.org
build.el           emacs-irc.org
~/work/dot-files :master
```

```
TITLE: Open Source Software and
the Department of Defense
```

```
DATE: 2016 AUG 20
```

```
AUTHOR: Ben FitzGerald, Peter L.
Levin, and Jacqueline Parziale'
```

```
#+TAGS: emacs technical
```

OPEN SOURCE SOFTWARE & THE DEPARTMENT OF DEFENSE

Ben FitzGerald, Peter L. Levin, and Jacqueline Parziale

Foreword by
General Hugh Shelton, U.S. Army (Ret.)



Center for a
New American
Security

- Everything was going well for us militarily in Haiti until the

White House asked me to send information in a specific format.

백악관에서 Haiti 상황을 양식에 맞춰 보고해달라는 지시 t support

the format they desired. My team contacted the vendor for help and,

predictably, they refused to modify the software to help us. This is a

story **그러나 SW 회사는 코드 수정 요구를 거절** Some vendors think

they own you forever.

만일 그 SW가 OSS 였다면? – 제때에 조치 가능

- Today, the U.S. Department of Defense (DoD) is one of the largest

consumers of open source in the world.

미 국방성은 세계에서 OSS를 가장 많이 사용중

Hugh Shelton, 前 미육군 장성
2016 8월

CIA Software Developer Goes Open Source, Instead

BY NOAH SHACHTMAN 08.04.10 | 10:40 AM | PERMALINK

총 같은 무기를 오직 업자만 clean/fix/modify 할 수 있다면?

- Imagine if only the manufacturer of a rifle were allowed to clean, fix, modify or upgrade that rifle.
- This is where the military finds itself: one contractor with a monopoly on the knowledge of a military software system."

SW 관련 정보를 업자만 독점?

이것이 Closed SW가 초래하는 결과이다

Why OSS in DoD?

- 종속 탈피
- 초연결
- 보안
- 예산
- 자주국방 ← 기술독립 ← OSS



FEDERAL NEWS RADIO



Technology

Defense

Causey

Your Job

Your Money

Contracting

On DoD: Open source software in the Defense Department



By Jared Serbu @jserbuWFED

September 14, 2016 11:00 am ⌚ 1 min read

Share



On DoD: Open source software in the Department of Defense

09/14/16 11:00



00:00



[Download audio](#)

The Defense Department spends billions of dollars each year to buy and build software — not just in its enterprise IT systems, but, increasingly, as a vital aspect of each and every one of the weapons systems the military places on the battlefield.

Or, as Defense secretary Ashton Carter put it earlier this week:


“In today’s world, there’s no point in having all of our ships, planes and tanks unless you can connect and secure it all. We spend an enormous amount of effort and money on this, and it’s one of the areas where we welcome people to come and help us.”

But a [new report](#) from the [Center for a New American Security](#) argues the department needs a drastically different approach to building and buying software to break a longstanding habit of buying proprietary systems and move to a world of open source.

- As Defense secretary Ashton Carter put it earlier this week:
- "In today's world, there's no point in having all of our ships, planes and tanks **unless you can connect and secure it all.**" We spend an **오늘날엔 군함, 전투기, 탱크 모두 초연결 안되면 쓸모가 없다** areas where we welcome people to come and help us."
- **DoD는 과거 Closed SW 고집을 과감히 탈피하고 OSS도 활용해야** the department needs a drastically **different approach to building and buying software** to break a longstanding habit of buying proprietary systems and **move to a world of open source.**

Why OSS in DoD?

- 종속 탈피
- 초연결
- 보안
- 예산
- 자주국방 ← 기술독립 ← OSS



CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF DEFENSE

Search Chief Information Officer

HOMEABOUT DOD CIO TOP PRIORITIESIN THE NEWS OPPORTUNITIES LIBRARY CONTACT US

Open Source Software FAQ

DoD Open Source Software (OSS) FAQ

Frequently Asked Questions regarding Open Source Software (OSS) and the Department of Defense (DoD)

미국 국방성 CIO – OSS FAQ

Factors to understand the policies and legal issues relating to the use of open source software do not constitute legal advice and any legal questions relating to specific situations should be referred to legal counsel. References to specific products or organizations are for information only, and do not constitute an endorsement of the product/company.

A collaborative version of this document is published in Intellipedia-U at [https://www.intelink.gov/wiki/Open_Source_Software_\(OSS\)_FAQ](https://www.intelink.gov/wiki/Open_Source_Software_(OSS)_FAQ)

Contents

- 1 Frequently Asked Questions regarding Open Source Software (OSS) and the Department of Defense (DoD)
- 2 Defining Open Source Software (OSS)
 - 2.1 Q: What is open source software (OSS)?
 - 2.2 Q: What are synonyms for open source software?
 - 2.3 Q: What are antonyms for open source software?
 - 2.4 Q: Is this related to "open source intelligence"?
 - 2.5 Q: Is there a name for software whose source code is publicly available, but does not meet the definition of open source software?
- 3 OSS and DoD Policy
 - 3.1 Q: What policies address the use of open-source software in the Department of Defense?
 - 3.2 Q: Isn't using open source software forbidden by DoD Information Assurance Policy?
- 4 General information about OSS
 - 4.1 Q: Is open source software commercial software? Is it COTS?
 - 4.2 Q: Why is it important to understand that open source software is commercial software?
 - 3 Q: Are "non-commercial software", "freeware", or "shareware" the same thing as open source software?

제 회사 SW는
절대 믿어도
됩니다



Close여서
안전
합니다

<http://dodcio.defense.gov/Open-Source-Software-FAQ/>



CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF DEFENSE

비공개 상용 SW - 보안 우수?

For at least 7 years, Borland's InterBase (a proprietary program) had embedded in it a "back door";

상용 데이터베이스에 back-door가 있다는걸 모르고 DoD는 7년간 사용했다

When the program was released as OSS,
within 5 months this vulnerability was found and fixed.

그 SW가 OSS화 되자 5개월 만에 OSS 커뮤니티가 back-door를 발견해냈다

This shows that proprietary software can include functionality that could be described as malicious, yet remain unfixed – and that at least in some cases OSS is reviewed and fixed. cleared, for example

펜타곤 - 전담기구

"DDS"

(Defense Digital Service)

<https://www.dds.mil/>

Our Mission

"often our progress is hindered
by outdated tools and practices
that lag far behind private sector standards"



SECTION 2: RESPONSIBILITIES AND FUNCTIONS

DIRECTOR, DDS. The Director, DDS:

a. Plans and conducts pioneering work to deliver improved digital services to the DoD using knowledge of the latest practices in software development, consumer internet technologies, and technology management approaches by:

(1) Supporting adoption of best-in-class software practices, including agile development methodologies and open-source practices, for the development and deployment of new and existing digital services.

(2) Utilizing the most effective means for improving digital services based upon quantitative and qualitative assessments of users' needs.

(3) Deploying top talent, in a variety of skillsets spanning technology, strategy, business, and management to support redesign of DoD's digital services.

(4) Initiating efforts to identify and evaluate cyber security vulnerabilities and deficiencies in DoD digital services and makes recommendations on the departmental prioritization of cyber security red teams.

DDS – 최근 수행 프로젝트

국방성 SW에 대해
“Hack 펜타곤” 시행
정부 차원
최초 시도



Hack The Pentagon

The Defense Digital Service launched [Hack the Pentagon](#), the first [bug bounty program](#) in the history of the federal government. The program won praise from Secretary of Defense Ash Carter, who wrote: “I am confident this innovative initiative will strengthen our digital defenses and ultimately enhance our national security.”

<https://www.dds.mil/>

RESULTS THAT EXCEEDED EXPECTATIONS



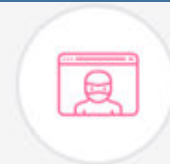
13 MINUTES

행사 개시
13분만에
버그 발견



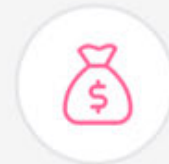
200 REPORTS IN 6 HOURS

행사
6시간만에
200개 버그



1410 HACKERS

전세계서
1410명
참여



\$75,000 BOUNTIES PAID

당일 나간
보상금만
7만 5천 달러

DDS – 최근 수행 프로젝트



Hack The Pentagon

The Defense Digital Service launched [Hack the Pentagon](#), the first [bug bounty program](#) in the history of the federal government. The program won praise from Secretary of Defense Ash Carter, who wrote: "I am confident this innovative initiative will strengthen our digital defenses and ultimately enhance our national security."



Hack The Air Force 2.0

Working closely with the Department of the Air Force, the Defense Digital Service [launched its fourth bug bounty program](#), targeting unclassified Air Force systems for the second time. With the largest payout in any government bug bounty program to date, Hack The Air Force 2.0 awarded \$125,000 in bounties for 110 vulnerabilities discovered. Open to hackers from 32 countries, this competition continues our work on broadening the community of hackers paid by DoD to find new vulnerabilities while building upon our partnership with Twenty-Fourth Air Force (Air Forces Cyber).

공군 SW도
32개국 참여
110개 버그
12만 5천불
보상금 나감



HOME

ABOUT ▾

LEADERS ▾

U.S. DEPARTMENT OF DEFENSE

HOME > NEWS > ARTICLE

DoD Invites Vetted Specialists to 'Hack' the Pentagon

보안 전문가들에게 펜타곤을 해킹해보라고 초청했다

Air Force Tech. Sgt. Randal Collmer, 1st Communications Maintenance Squadron infrastructure theater maintenance section chief, and Air Force Staff Sgt. Bradley Anderson, 1st CMXS special communications maintenance technician, work to test their training network at Kapaun Military Complex, Germany, Jan. 8, 2016. The 1st CMXS supports bases around Europe by working side by side to improve and optimize the bases networks. The Defense Department is launching a pilot program to allow vetted computer security specialists to do their best to hack DoD public Web pages. Air Force photo by Staff Sgt. Armando A. Schwier-Morales

PRINT | E-MAIL



1

WASHINGTON, March 2, 2016 — The Defense Department is launching a pilot program in April to allow vetted computer security specialists to do their best to hack DoD public web pages, Pentagon Press Secretary Peter Cook said today.

"Hack the Pentagon" is the first cyber bug bounty program in the history of the federal government, Cook said in a statement issued today.

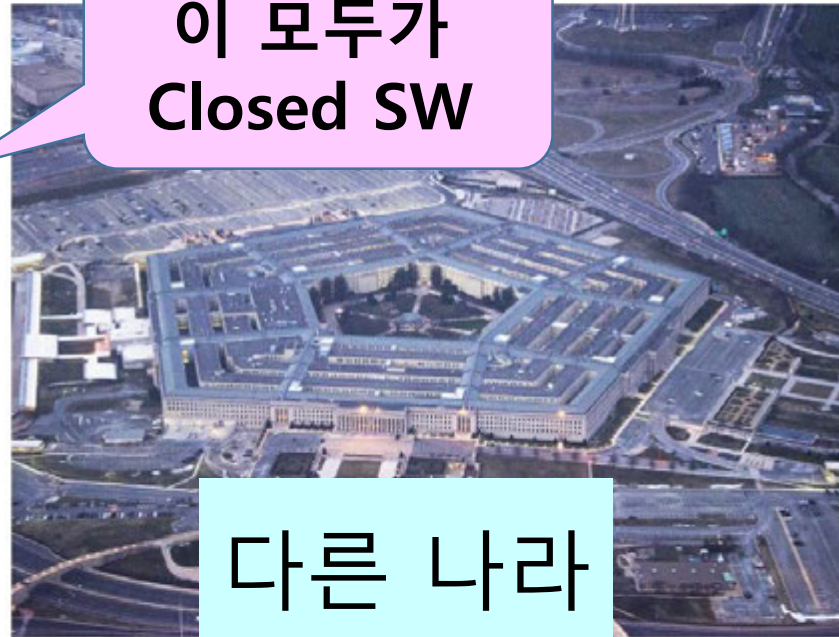
미국 정부 역사상 최초 시도

펜타곤 SW를
해커들에 공개하자
그들은
수천개 버그를
찾아냈다

LILY HAY NEWMAN SECURITY 11.10.17 07:00 AM

THE PENTAGON OPENED UP TO HACKERS—AND FIXED THOUSANDS OF BUGS

이 모두가
Closed SW



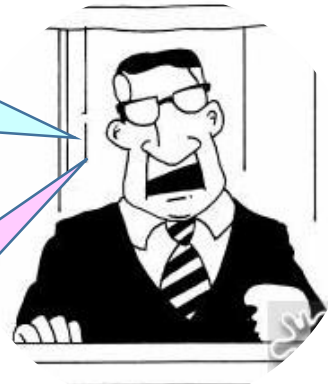
RON SACHS/ALAMY

다른 나라
SW들은?

THE UNITED STATES government doesn't get along with hackers. That's just *how it is*. Hacking protected systems, even to reveal their weaknesses, is illegal under the Computer Fraud and Abuse Act, and the Department of

제 회사 SW는
절대로
믿어주세요

Closed 여서
절대 안전
합니다



DDS의 전문가 협의회 발표 (Youtube 비디오)

발표자: 펜터곤 DDS 소속 Lawyer

DoD가 OSS도 채택해야 하는 이유

첫째

DoD는 가장 앞선 기술을 써야 하므로

둘째

DoD는 보안이 매우 중요하므로

**미국 관료들이 신기술을
못따라 가고 있는 것이
매우 중대한 문제이다**

Open Source at the Department of Defense - Why it matters



Modern technology and cyber security for the U.S. government is fundamentally dependent on modern software development practices. Sharon Woods of the Department of Defense (DoD) shares how open source is a critical in improving the DoD's technological relevance and security.

This presentation was recorded on May 23, 2017 at GitHub Enterprise Summit Washington D.C.



Sharon Woods

General Counsel(고문 변호사), **DDS**

LinkedIn

Sharon Woods is the General Counsel for the Defense Digital Service (**DDS**) at the U.S. Department of Defense (DoD). She provides legal counsel and bureaucracy hacking expertise for a team of private sector technologists working on high impact challenges at the Pentagon. She is also the **project lead** for Code.mil, an experiment in open source at DoD. Prior to joining DoD, she was an attorney for the U.S. Department of the Navy, specializing in information technology acquisitions. She holds **a law degree** from the Washington College of Law, American University and bachelors from Johns Hopkins University.

모든 SW를 OSS로? – No

그러나 어떤 SW들은

그것이 해킹되서 뚫릴 경우

다른 모든 SW와 Data를 위험에 노출시킴

예: OS 통신 DB 등

그러한 SW는 전세계 최고 전문가들에게 검증 받아야 – OSS

OSS에 대한 무지/오해

MISCONCEPTIONS ABOUT THE SECURITY OF OPEN SOURCE SOFTWARE

Discussion of open source software in national security is often dismissed out of hand because of technical security

OSS를 사용하면 국방부가 작업한 부분도 공개해야한다 -(X)

Using open source licensing does not mean that changes to the source code must be shared publicly

- The ability to see source code is not the same as the ability to modify deployed software in production.
- Using open source components is not equivalent to creating an entire system that is itself open sourced.

As In-Q-Tel's Chief Information Security Officer Dan Geer explains, security is “the absence of unmitigatable surprise.”²³ It is particularly difficult to mitigate surprise with closed proprietary software, because the source code, and therefore the ability to identify and address its vulnerabilities, is hidden. “Security through obscurity” is not an effective defense against today's cybersecurity threats.

In this context, open source software can generate better security outcomes than proprietary alternatives. Conventional anti-malware scanning and intrusion detection are inadequate for many reasons, including their “focus on known vulnerabilities” that miss unknown threats, such as zero-day exploits. As an example, a DARPA-funded team built a flight controller for small quadcopter drones based on an open source autopilot readily downloaded from the Internet. A red team “found no security flaws in six weeks with full access [to the] source code,” making their UAV the most secure on the planet.²⁴

OSS에 대한 무지/오해

MISCONCEPTIONS ABOUT THE SECURITY OF OPEN SOURCE SOFTWARE

Discussion of open source software in national security is often dismissed out of hand because of technical security concerns. These are unfounded.

To debunk a few myths:

- Using open source licensing does not mean that changes to the source code must be shared publicly.
- The ability to see source code is not the same as the ability to modify deployed software in production.

상대방이 내 코드를 볼 수 있다면
상대방이 내 코드를 바꿀 수도 있다? ----- No

왜?

모든 OSS는 안전하게(100% 검증된 암호화 기법으로)
저장, 수정, 배포, 설치되기 때문 (예: github)

secure on the planet.²⁴

github - 전세계 학계 산업계로 부터 보안 검증 받음

Why OSS in DoD?

- 종속 탈피
- 초연결
- 보안
- 예산
- 자주국방 ← 기술독립 ← OSS

OSS의 경제성

- 미국 국방부(DoD)는 OSS 기반의 Linux, JBoss 및 가상화를 사용한 결과 회계연도 2015년까지 510만 달러의 비용을 절약하고 민첩성과 유연성을 높일 수 있게 되었다고 밝혔다.

“OSS로 대체하자 510만 달러 예산을 절감했다”

- 출처: “국방분야 공개SW 현황 조사”, 2017 12월, 75쪽

DoD는 매우 오래 전부터 OSS를 써왔다

- After all, DoD has a long history of using and creating open source software, and adopting policies to support these practices. Earlier this year,

DoD뿐만 아니라 NSA를 위시한 정부도 갈수록 OSS를 많이 쓴다

software community and modernize software practices at the agency. DoD is joined by a growing list of U.S. federal agencies adopting open source, including the National Security Agency and National Aeronautics and

전세계 다른 정부들도 효율성, 보안, 혁신성 때문에 OSS를 많이 쓴다

- We are encouraged to see governments around the world collaborating and embracing open source to promote efficiency, innovation, and security.

2003년부터
DoD가
OSS를
사용한 예

Quick List of FOSS Software Used in the U.S. DoD

A	ACE	ACE ORB (TAO)	ACID	AMANDA	Apache	Autoconf	Automake
B	bash	Bastille	BIND				
C	C++ Boost	CIS Benchmarks	Colt	Condor	COPS	Crack	CVS
	CVW	Cvwin					
D	DDD	DiVuLibre					
E	EADSIM	Emacs	eTrust	Expect			
F	FreeBSD						
G	GateD	gawk (awk)	GCC	GDB	Ghostscript	GNAT	GnuPG
	gnuplot	grep					
H	h2n	HOSTS					
I	ImageMagick						
J	JADE	Jakarta	Jaxen	JBoss	JDOM	Jikes	jSIP
K	Kaffe						
L	LaTeX	Linux	Linux (Red Hat)	Linux firewalls	Lsof		
M	m4	Majordomo	make	Maxima	MIMesweeper	MRTG	MTR
	MySQL						
N	Nessus	NetBSD	NetSaint	nload	Nmap	ntop	NTP
O	Octave	OpenBSD	OpenMap	OpenOffice	OpenSSH	OpenSSL	
P	Perl	Perl CGI scripts	PerlLDAP	PHP	PingScan	Procmal	
Q	Qmail						
R	R	RealSecure	RRDtool	RTLlinux	RWhois	RXVT	
S	Samba	SARA	SATAN	Saxon	SCA	sed	SELinux
	Sendmail	SNARE	Snort	Squid			
T	Tcl/Tk	TCP Wrappers	Tomcat	Top	Tripwire		
U							
V	VisAD	VOCAL	VTK				
W	Webmin	WebTAS	Weka	WU-FTPD			
X	Xalan	Xerces	XFree86	XGobi	Xpatch		
Y							
Z	zlib	Zope					

Source: Use of Free and Open-Source Software (FOSS)
in the U.S. Department of Defense,
Version 1.2.04, Jan. 2, 2003, MITRE.

미국 펜타곤은 2018년부터 OSS를 훨씬 더 크게 확대한다

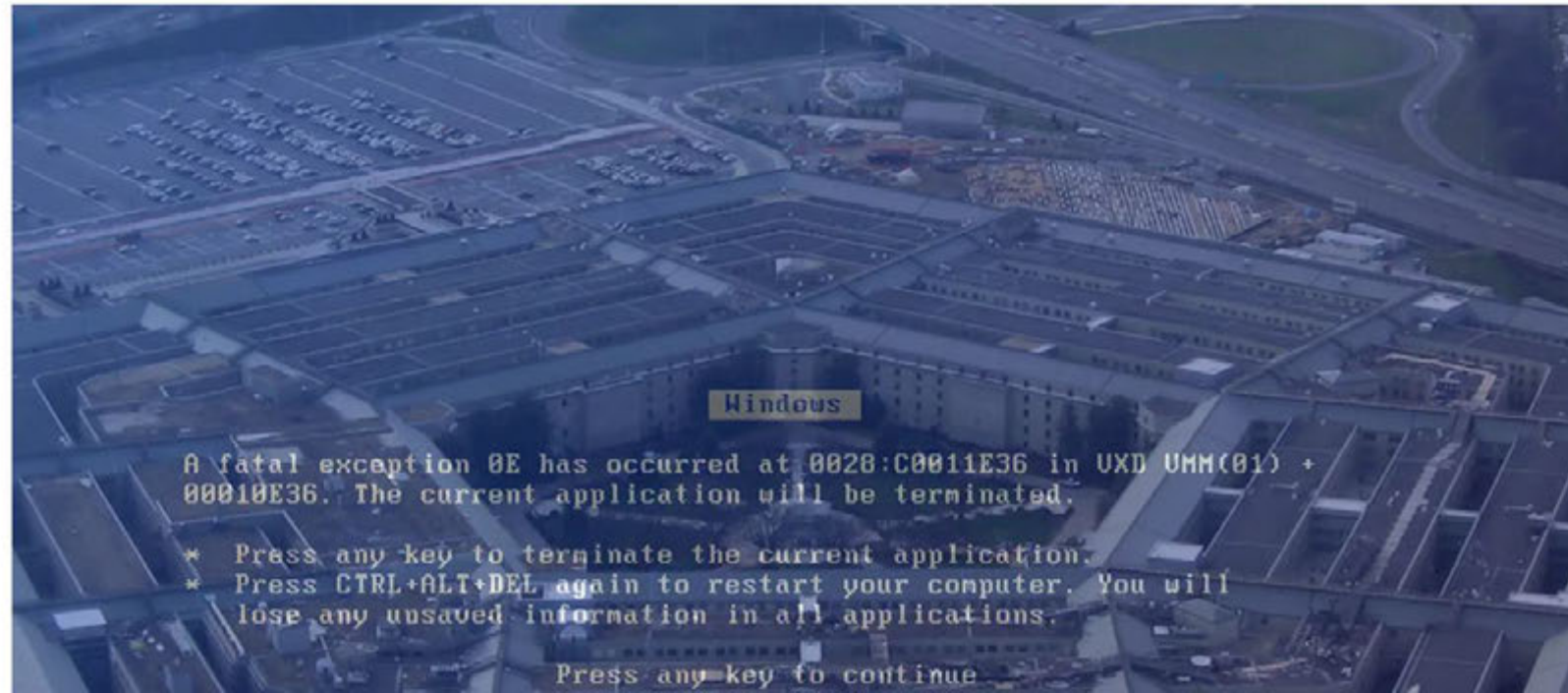
The **Pentagon** is set to make a big push toward open source software next year

The Pentagon is a software-intensive workplace

By Kelsey Atherton | Nov 14, 2017, 12:44pm EST

2017 11월 발표

f   SHARE



- Besides cost, 경비뿐 아니라 other compelling explanations for why the military 국방성 밖에서 기술은 빠르게 변하므로 technology outside the Pentagon simply advances faster than technology within it, and by availing itself to open-source tools, the Pentagon can adopt those advances almost as soon as the new code hits the web, without going through the OSS로 가야 기술변화에 빠르게 적응한다

- Open-source software is also more secure than closed-source software, by its very nature: the code is perpetually scrutinized by countless users across the planet, and any weaknesses are shared immediately. OSS는 Closed SW 보다 보안이 더 우수하다

NOAH SHACHTMAN SECURITY 08.04.10 10:40 AM

CIA SOFTWARE DEVELOPER GOES OPEN SOURCE, INSTEAD

CIA 개발자들도 OSS로



For three years, Matthew Burton has been trying to get a simple, useful software tool into the hands of analysts at the Central Intelligence Agency. For three years, haggling over the code's intellectual property rights has kept the software from going anywhere near Langley. So now, Burton's releasing it - free to the public, and under an open source license.

Burton, a former Defence Intelligence Agency analyst and

CIA Software Developer Goes Open Source, Instead

한 회사가 SW 관련 정보를 독점하면

ALINK

one contractor with a monopoly on the knowledge of a military

그 회사에게만 유리한 반면 국가에는 software source code.

This is optimal only for the monopoly contractor, but

creates inefficiencies & ineffectiveness 비효율적이 되고 nt,

severely limits competition

경쟁을 못하게 막게 되며

reduction of opportunities for the industrial base,

wastes taxpayer-provided funds"

국민 세금을 낭비하게 된다

DOD's new rules promote open source

By Joab Jackson

Oct 27, 2009

New Defense Department **guidance** puts open-source software on the same level as commercial software and urges DOD agencies to evaluate it on an equal basis with

DoD 새 가이드라인 – OSS를 Closed SW와 동등히 대우

"To effectively achieve its missions, the Department of Defense must develop and update its software-based capabilities faster than ever, to anticipate new threats and respond to continuously changing requirements," wrote acting DOD Chief Information Officer David Wennergren, in a cover letter to the guidance, which was issued Oct. 16. "The use of Open Source Software can provide advantages in this regard."

The new guidance answers a wide variety of questions that have arisen within the military ranks about the use of open-source software, particularly around procurement and sharing. It supersedes



NEWS

DoD: Open Source As Good As Proprietary Software

The Department of Defense issues a memo outlining guidance for using open source software and for

OSS는 모든 면에서 다른 SW에 결코 뒤지지 않는다

source software saying it is equal to commercial software in almost all cases and by law should be considered by the agency when making technology purchase decisions.

따라서 법을 바꿔 OSS도 고려해야 한다

David Wennergren, deputy CIO of the U.S. Department of Defense (DoD).

In terms of guidance **DoD - 부 CIO 발표** definition of "commercial computer software" and that executive agencies are required to include open source when evaluating software that meets their computing needs.

Top 10 Open Source Hall of Famers

OSS 정책 기획

- OSS 위한 정책기획단(예: 미국 DDS)
- 국내외 민관 전문가 참여
- 정책 기획
- 기술, 보안, 인력양성, 변화관리, 예산 등
- 방향 제시

Why OSS in DoD?

- 종속 탈피
- 초연결
- 보안
- 예산
- 자주국방 ← 기술독립 ← OSS

역사의 교훈 - 기술 - 먹거리

- Then

- 굴뚝 산업
- 메모리 반도체
- 이동전화

- Now

- 4차 산업혁명



후발주자에게도 기회
인건비+토지+환경 ..
역공학



굴뚝 산업

Ford > Toyota > 현대 > 중국

GE > SONY > 삼성 > 중국

IBM > Microsoft > Oracle > Apple

IT 산업

후발주자에게 기회?

(X) 인건비+토지+환경 ..

(X) 역공학

- Then

- 굴뚝 산업
- 메모리 반도체
- 이동전화

- Now

- 4차 산업혁명

시론·기고 ▾

[기고] 日 반도체 죽인 美 반덤핑 조사, 한국 겨냥하나

안덕근 서울대 국제대학원 교수·무역위원회 무역위원



입력 : 2017. 12. 19 03:14

**80년대 세계 장악한 日 반도체, 美의 반덤핑 조사로 쇠퇴의 길****26년 만에 中 수출품 조사 시작... 우리 기업에 불똥 튀는 일 막아야**안덕근 서울대 국제대학원
교수·무역위원회 무역위원

미국이 통상 분야에서 26년 동안 쓰지 않았던 '비장의 무기'를 다시 꺼내 들었다. 미 상무부가 지난달 28일 중국산 알루미늄 합판에 직권으로 반덤핑 조사와 상계관세(수출국의 장려·보조금 지원을 받은 제품에 부과하는 관세) 조사를 시작한 것이다. 직권조사는 관련 업계의 읍소가 없더라도 특정국 수출품의 덤핑 여부를 조사하고 높은 관세를 부과하는 강력한 무역 제재 수단으로, 이번 직권조사는 1991년 캐나다산 목재에 대한 상계관세 조사 이후 처음이다.

통상 전문가들 사이에 미국의 반덤핑 직권조사는 '공포의 대상'이다. 직권조사를 마치면 어김없이 무시무시한 무역 보복이 뒤따랐기 때문이다. 1980년대 세계 시장을 석권했던 일본산 반도체에 대한 보복이 대표적이다. 미 상무부는 1985년 일본산 반도체 제품들의 덤핑 혐의에 대한 직권조사를 시작했다. 미·일 간 무역 역조로 두 나라 간 통상 마찰이 절정에 달했던 시기다. 직권조사가 진행 중이던 1986년, 일본 정부는



안덕근 서울대 국제
대학원 교수·무역위
원회 무역위원

합판에 직권으로 반덤핑 조사와 상계관세(수출국의 장려·보조금 지원을 받은 제품에 부과하는 관세) 조사를 시작한 것이다. 직권조사는 관련 업계의 읍소가 없더라도 특정국 수출품의 덤핑 여부를 조사하고 높은 관세를 부과하는 강력한 무역 제재 수단으로, 이번 직권조사는 1991년 캐나다산 목재에 대한 상계관세 조사 이후 처음이다.

통상 전문가들 사이에 미국의 반덤핑 직권조사는 '공포의 대상'이다. 직권조사를 마치면 어김없이 무시무시한 무역 보복이 뒤따랐기 때문이다. 1980년대 세계 시장을 석권했던 일본산 반도체에 대한 보복이 대표적이다. 미 상무부는 1985년 일본산 반도체 제품들의 덤핑 혐의에 대한 직권조사를 시작했다. 미·일 간 무역 역조로 두 나라 간 통상 마찰이 절정에 달했던 시기다. 직권조사가 진행 중이던 1986년, 일본 정부는 향후 5년간 일본 국내 시장의 20%를 미국산 반도체 제품에 내주고 일본산 반도체의 저가 수출을 중단하겠다는 내용의 반도체 협정에 서명했다. 미국의 압력에 굴복한 항복 문서였다. 이 협정 이후 세계 최대 시장인 미국에서 경쟁력을 잃은 일본 반도체 산업은 쇠퇴의 길을 걸었고, 후발 주자인 한국의 삼성전자에 선두 자리를 내줬다. 이처럼 막강한 힘을 갖고 있지만, 미국은 1991년 이후 한 번도 직권조사 기치를 반드히 내지 않았다. 냉전 해체 이후 세계 유일의 초강대국으로

ad.chosun.com/RealMedia/ads/click_fx.ads/www.chosun.com/news/L-19/.../792f2b2b4d56eb2f6138384143393431

세계 반도체 역사를 다시 쓴다

글 | 최양규 - KAIST 전자전산학과 교수 ykchoi@ee.kaist.ac.kr

1947년 트랜지스터 발명 이후 미국은 사실상 반도체 산업의 종주국이었다.

그러나 냉전시대에 미국은 반도체기술의 군사적인 응용에 역점을 둘 수 밖에 없었고, 민간소비자를 위한 가전과 같은 소비재 부문 응용기술 개발은 상대적으로 위축되었다. 2차 세계대전 패전후 전후복구에 열을 올리던 일본은 미국이 집중하지 않은 민간 소비재 부문에 집중하여 반도체 부문의 중흥기를 맞이할 수 있었다. 일본의 반도체 중흥기에 결정적인 기여를 한 또 다른 외부환경으로는 1949년 미국 법무부의 AT&T에 대한 반독점금지판결을 들 수 있다. 외부로의 기술 개방이 가능해져 외국 기업들도 기술료를 지불하면 자유롭게 쓸수 있게 된 것이다.

소니를 필두로 일본업체는 휴대용 트랜지스터 라디오를 개발하고 LCD TV의 시제품을 개발한 미국의 RCA를 추월하여 샤프와 세이코는 상용화된 LCD TV를 시장에 먼저 출시하였다.

반도체기술을 이용한 일본산 가전제품은 빠른 속도로 미국 시장을 잠식해 들어갔고, 미국은 큰 피해를 보게 되었다.

미국은 일본의 반도체 기술을 견제하기 위해 한국에 반도체 관련 기술 이전을 묵인했고 한국 반도체 산업은 전환기를 맞이할 수 있게 되었다.

- Then

- 굴뚝 산업
- 메모리 반도체
- 이동전화

- Now

- 4차 산업혁명

이동통신 - 유럽이 선점

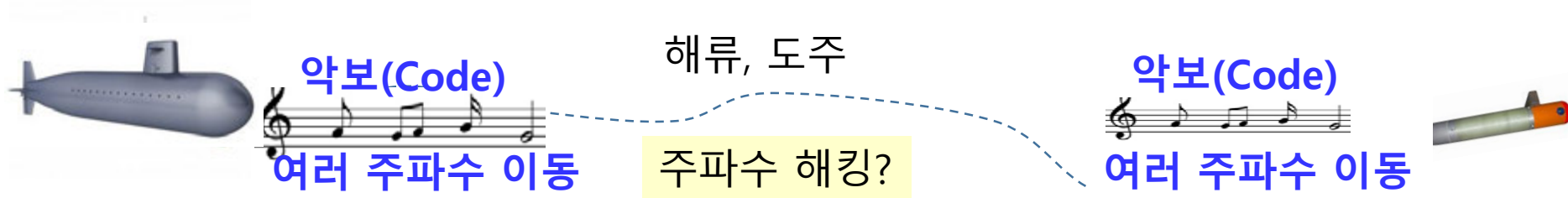
- 유럽 나라마다 상이한 표준
- 1982 EU 표준화 시작
- 1987 GSM/TDMA (12개국)
- 1991 상용화
- 1993 해외 진출
- 세계 이동통신 제패?
- UN ITU 제출



미국의 대응



- **CDMA** – 1942 군사용 특허 (여배우 헤디 라머)



- 보안
- 가격/성능 – 공백(40%) 활용
- 고난도 기술 – 분산 Clock의 동기화(by GPS)
- Qualcomm – 군 통신회사

출처: 데이브 목 지음, 박정택 옮김, The Qualcomm Equation,
열정이 있는 지식기업 퀄컴이야기, 굿모닝북스

GPS

- In **1997**, U.S. Secretary of Transportation:
 - "Most people don't know what GPS is.
 - Five years from now,
 - Americans won't know how we lived without it."
 - (참고: EU GSM 상용화는 1991)
- CDMA를 이해하는 전문가가 없었음
- GPS was developed in **1970s** by U.S. DoD

<https://www.thoughtco.com/global-positioning-system-1434622>

- 정부
 - “CDMA로 유럽 GSM을 이겨내자”
- 민간
 - “CDMA를 아는 사람이 없었음”(군사비밀)
 - “대규모 상용화 검증 안됐다” (해군용 > San Diego실험 > NY실험)
 - Scalable?
 - 왜 민간에게 모험/투자 요구하나?
- 퀄컴(CDMA 회사)
 - 도산 위기
 - 큰 지역에서 Reference Site 필요 – 수많은 기지국, 단말기로
 - 미국 국내 – 미국 회사들의 거부 – 외국에서 실험/증명해야

1995년 6월 9일

Why in Korea? - 미국 핵심 군사기술이



당시 언론 보도

“한국에서 CDMA가 상업적으로 크게 성공하며

이를 바탕으로 퀄컴은 이동통신계의 거대기업이 되었다.

특이한게, CDMA를 쓰는 나라는 한국 빼고는 없었다.”

출처: (CDMA – 나무위키)

90년대 중반까지만 해도

CDMA 기술을 상용화한 나라는 우리나라 밖에 없어

세계 이동통신업계에서 한국은 “이동통신 부문의 섬”라는 말까지 나돌았다

출처: (“한국 CDMA가 세계시장 석권한다”, 2002 4 18, 주간조선)

중국과 CDMA

- 중국도 이미 GSM - 뒤늦게 CDMA 채택 요구
- 당시 중국 숙원사업은 “WTO 가입” - 미국의 반대
- (WTO 가입-CDMA 채택) 맞바꾸기
- CDMA 채택 조건
 - 중국은 퀄컴의 CDMA 라이선스를 불법도용하지 않는다
 - 중국내 기존 GSM와 호환되게 한다
 - 퀄컴은 CDMA/GSM 통합형 GSM 1x 제품 개발

WTO deal could boost cdmaOne in China

BY REILY GREGSON ON JANUARY 1, 2001

ARCHIVED ARTICLES, CARRIERS

It is known that the U.S. stance on China's entry into the WTO has changed following the MoU between China's MII and Qualcomm.

support for a nationwide cd
forward to participating in t



"U.S. stance on WTO changed
following MoU between
China MII & Qualcomm"
January 1, 2001

한국에 정통부를 만들어
CDMA를
확실히 챙기겠습니다



- “많은 사람들이 우려했지만 CDMA 방식을 김영삼 대통령이 결정했다” - 박성득 전 정통부 차관
- 당시 CDMA를 반대했던
 - 정부(상공부) 통신전문가(이상철 박사 등) 기업(삼성 등)



[CDMA 10년, 그리고 미래]CDMA를 일군 사람들

발행일 : 2006.04.20



삼성전자도 처음엔 CDMA를 반대했다

CDMA 도입결정은 91년 9월, 당시 체신부 송언종 장관과 윤동윤 차관 때 이뤄졌다.

현재 정통부에 남아있는 당시 관계자로는 신용섭 현 전파방송국장과 서석진 현 광대역융합과장 등 극소수다

서 과장은 당시 관리단으로 2년간 파견근무를 했다. 상충한 이해관계 속에서 사업이 빠격거리지 않도록 원활한 의사소통을 말아야 했으니, 당시 관계자들은 "온갖 잡음 속에서도 사업이 진행될 수 있도록 하기 위해 소신있게 행동한 공무원들에게 감사하다"고 말한다.

- Then

- 굴뚝 산업

기술(역공학) 시장(인건비)

- 메모리 반도체

일본 견제 – 시장/기술 제공

- 이동전화

EU 견제 – 시장/기술 제공

- Now

- 4차 산업혁명

기술(OSS 교육) 시장(공공이 앞장서야)

과거 대학 SW 교육

- HW SW 高價
- No Source Code
- 이론, 논문만 → "Technology"?
- SW 사용법 교육만

OSS – 무료, 소스코드, Free(학생 마음대로)

공공이 OSS에 앞장서야

OSS 수강 신청 극히 저조



국내에 OSS 프로젝트가
없기 때문

왜 OSS 활용 안하나?



OSS 인력이 없기 때문에

OSS는 역공학 - 인력양성 - 기술자립 유일한 통로

공공→OSS 채택

OSS 생태계

민간→OSS 채택

4차혁명 動力

DoD IT 견인 사례

- **ENIAC** 컴퓨터 – 탄도 대형컴퓨터
- **COBOL** 사무처리 프로그램 언어
- 해군 무선통신 **CDMA** 스마트폰
- **GPS** 무인차, LBS
- **이미테이션** - WW2 독일 암호 FINTECH
- **Arpanet** – 인터넷 Google Facebook
- **CMMI** - 소프트웨어 품질 관리