

WG3 Status Report

15th NEAOSS Promotion Forum

Study on Standardization and Certification
Working Group of NEA OSS Promotion Forum

Cheju, Korea, 2016-11-16

Table of Contents

- Introduction
- FOSS Supply Chain Risk Management
- FOSS Governance
- Technology requirement of mobile terminal browser
- OPENTHOS
- Survey of OSS in Big Data Platform
- Work Plan

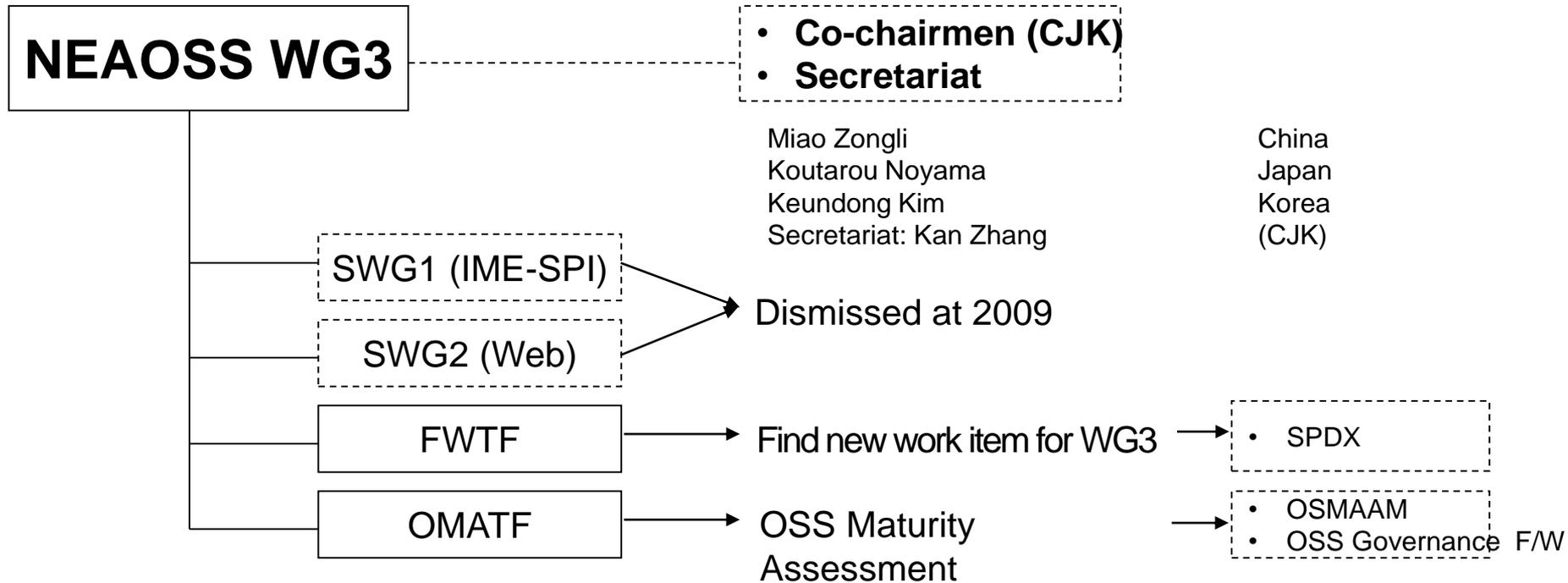
Introduction-Role of WG3

NEAOSS Forum formed

“WG3: Standardization and Certification Study” in order to study

Open Source Software standardization and certification in July 2004

WG3 structure and Officers

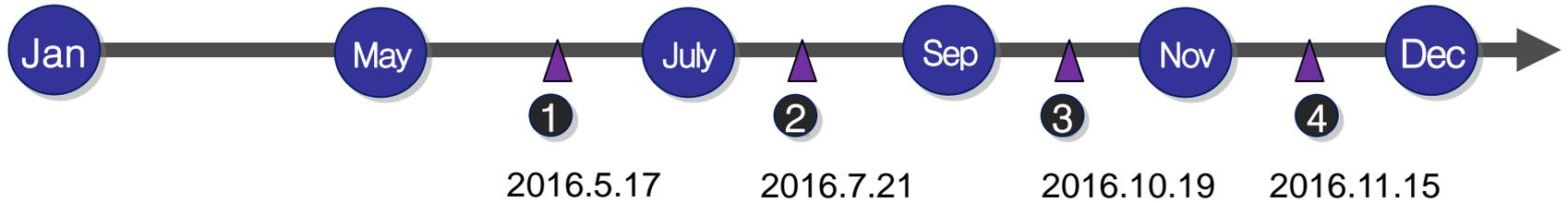


❖ Note: All activities/decisions are per NEAOSS WG3 directives

Recent Meeting Activities

2016

2017



1

Beijing

- Evaluation Methodology of Government R&D Project
- FOSS Supply Chain Risk Management
- Open Source Software Hub

2

Tokyo

- Survey of OSS in Big Data Platform and Data Analysis Result
- FOSS Supply Chain Risk Management
- Standard Status of Smart terminal

3

Beijing

- Introduction of the OpenTHOS
- FOSS Governance Guide
- OASIS(Open Adoption Support Information System)

4

Cheju

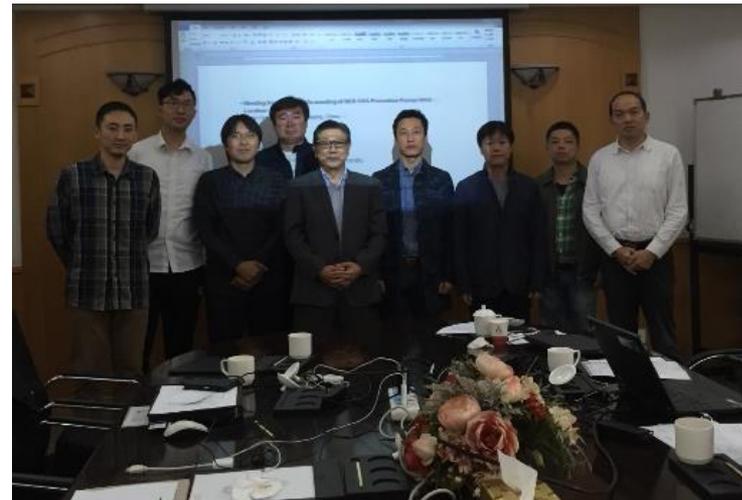
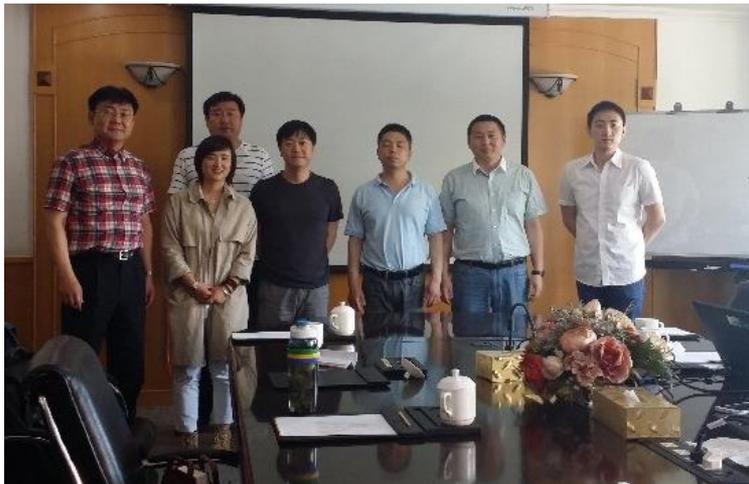
- Preparation for 15th NEA OSS Promotion Forum
- WG3 Work Plan in 2017

WG3 Documents Server

■ Totally :

- WG3 Meeting: 38
- WG3 Documents: 276

- 文件名
- 人 WG3_N276_WG3 Chairman's Statement (draft version) on the 33th
- 人 WG3_N275_Korea MB's report of OASIS on the 33th WG3 meeting
- 人 WG3_N274_Korea MB's report of FOSS Governance Guide on the
- 人 WG3_N273_Korea MB's report of SCRUM standard guideline on th
- 人 WG3_N272_Korea MB's status report on the 33th WG3 meeting.p
- 人 WG3_N271_Japan MB's report on the 33th WG3 meeting.pdf
- 人 WG3_N270_China MB's report on the 33th WG3 meeting.pdf
- 人 WG3_N269_Meeting Report of the 33th meeting of NEA OSS Pror



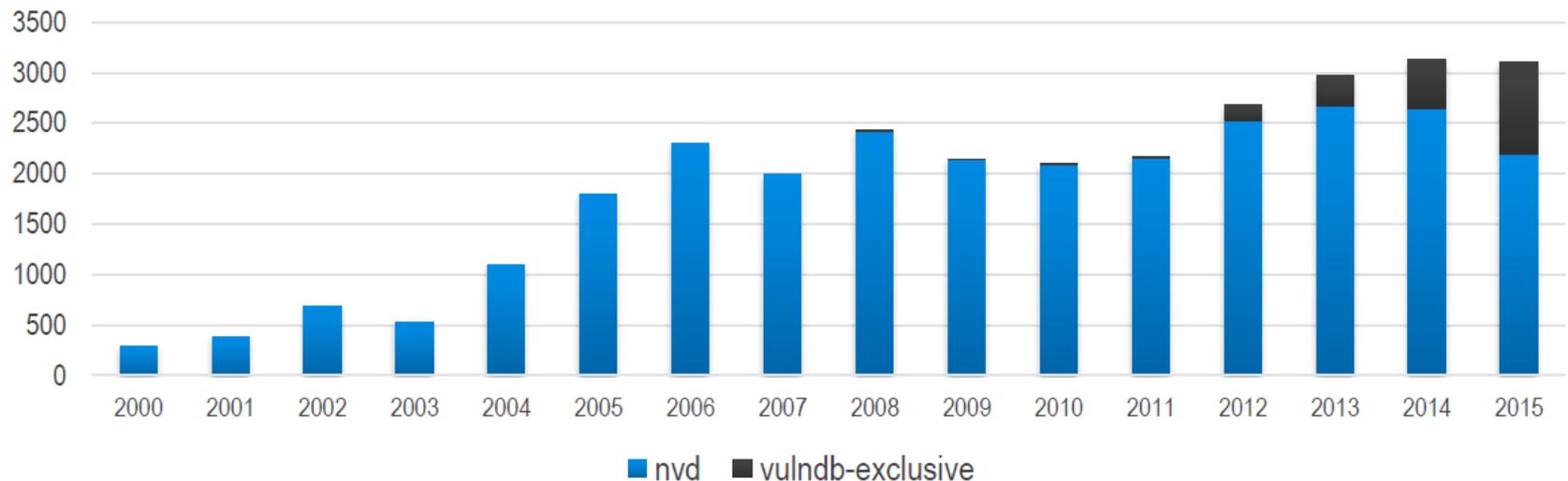
- 25th meeting
- 25th pre-meeting
- 26th meeting
- 26th pre-meeting
- 27th meeting
- 28th-1 meeting
- 28th-2 meeting
- 29th meeting
- 30th meeting
- 31th meeting
- 32th meeting
- 33th meeting

FOSS Supply Chain Risk Management

Background

- “By 2016, Open Source Software will be included in mission-critical applications within 99% of Global 2000 enterprises.” Gartner, Inc.
- “78% of companies run on open source software.” 2015 the future of open source

Open Source Vulnerabilities Reported Per Year



Reference: Black Duck Software knowledgebase, NVD, VulnDB

FOSS Supply Chain Risk Management



Heartbleed



Shellshock



Freak



Ghost



Venom

Component: OpenSSL

Bash

OpenSSL

GNU C library

QEMU

Introduced: 2011

1989

1990's

2000

2004

Discovered: 2014

2014

2015

2015

2015

Found by: Riku, Antti,
Matti,
Mehta

Chazelas

Beurdouche

Qualys
researchers

Geffner

FOSS Supply Chain Risk Management

- **Why Legal Teams Care about Open Source Security?**
- Open source risk management is not limited to license compliance.
- Legal teams are increasingly aware of security obligations & risks.

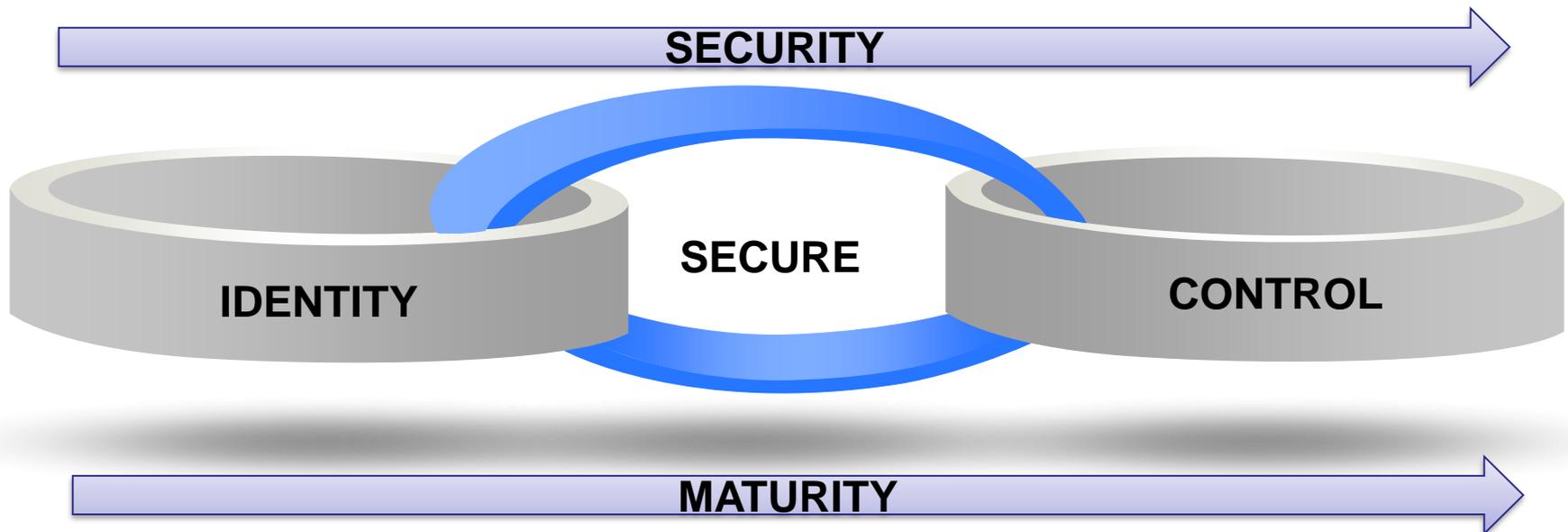
- **Internal/External Reporting**
 - Executive management, Directors, Regulatory Agencies
- **Litigation Risks**
 - Lawsuits from customer/patient/financial data loss
- **Regulatory Penalties**
 - HIPAA, PCI, SOX
- **Loss of company IP/secrets**
- **Damage to company reputation from high-visibility breaches**

FOSS Supply Chain Risk Management

- **Four factors that make open Source different**

1. Used everywhere
2. Easy access to code
3. Vulnerabilities are public
4. Exploits readily available

- **The Road to Secure Open Source Use**



FOSS Supply Chain Risk Management



Hub Internal Projects
Duck Hub ▾ 2.0

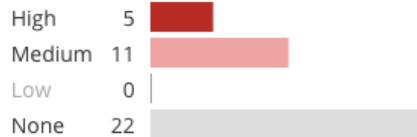
unknown Versions: 2 | Owner: [Dave Meurer](#) | Tier: 1 | Phase: Released | Distribution: External

☰ Components 🛡 Security 📁 Files 📊 Reports ⚙ Settings

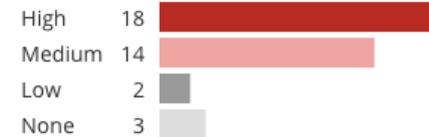
Security Risk



License Risk



Operational Risk



+ Add Component ✎ Edit 🚫 Ignore ↺ Unignore 🗑 Delete

Display Ignored

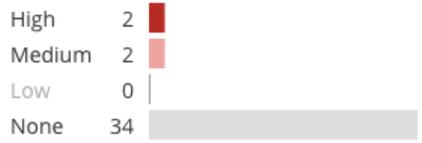
<input type="checkbox"/> Component ^	Version ⇅	License ⇅	Security Risk ⇅	Operational Risk ⇅	Match Type	Usage
<input type="checkbox"/> ANTLR	2.7.7	BSD 3-clause "New" or "Revised" License	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	<div style="width: 20px; height: 10px; background-color: red;"></div>	Automatic	Used
<input type="checkbox"/> Apache Commons FileUpload	1.2.2	Apache License 2.0	<div style="width: 10%; height: 10px; background-color: red;"></div>	<div style="width: 20px; height: 10px; background-color: red;"></div>	Automatic	Used
<input type="checkbox"/> Apache Commons Lang	3.1	Apache License 2.0	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	<div style="width: 20px; height: 10px; background-color: #f08080;"></div>	Automatic	Used
<input checked="" type="checkbox"/> Apache Struts	2.3.7	Apache License 2.0	<div style="width: 30%; height: 10px; background-color: red;"></div>	<div style="width: 20px; height: 10px; background-color: #f08080;"></div>	Automatic	Used
📁 1 file matched 📁 Apache Struts ▾ 2.3.7 Last Updated a month ago		⚡ Apache License 2.0	9 High 6 Medium 0 Low	0 High 1 Medium 0 Low	Match details: Exact	
<input type="checkbox"/> ASM	3.3	BSD 3-clause "New" or "Revised" License	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	<div style="width: 20px; height: 10px; background-color: red;"></div>	Automatic	Used
<input type="checkbox"/> ASM Commons	3.3	BSD 3-clause "New" or "Revised" License	<div style="width: 100%; height: 10px; background-color: #ccc;"></div>	<div style="width: 20px; height: 10px; background-color: red;"></div>	Automatic	Used

FOSS Supply Chain Risk Management


 Hub Internal Projects
Duck Hub ▸ 2.0

unknown
 Versions: 2 | Owner: [Dave Meurer](#) | Tier: 1 | Phase: Released | Distribution: External

Security Risks



Filter components...

Component	Vulnerabilities	
Apache Commons FileUpload 1.2.2	High	1
	Medium	1
	Low	1
Apache Struts 2.3.7	High	9
	Medium	6
	Low	0
Hibernate 4.1.0.Final	High	0
	Medium	1
	Low	0
jQuery 1.6.2	High	0
	Medium	1
	Low	0

15 Vulnerabilities in Apache Struts 2.3.7

Filter Vulnerabilities

Identifier ^	Published ↕	Base Score ↕	Exploitability ↕	Impact ↕	Status	Target date	Actual date
VulnDB 103918	Mar 3, 2014	10	10	10	Needs review	Never	Never
VulnDB 95405	Jul 18, 2013	6.8	8.6	6.4	Needs review	Never	Never
VulnDB 95406	Jul 18, 2013	4.3	8.6	2.9	Remediation Required	in 7 days	Never
NVD CVE-2013-1965	Jul 11, 2013	9.3	8.6	10	Remediation Required	19 days ago	Never
NVD CVE-2013-1966	Jul 11, 2013	9.3	8.6	10	Remediation Required	Never	Never
NVD CVE-2013-2115	Jul 11, 2013	9.3	8.6	10	Remediation Required	25 days ago	Never
NVD CVE-2013-2134	Jul 17, 2013	9.3	8.6	10	Remediation Required	19 days ago	Never

Description

Apache Struts 2 before 2.3.14.3 allows remote attackers to execute arbitrary OGNL code via a request with a crafted action name that is not properly handled during wildcard matching, a different vulnerability than CVE-2013-2135.

[View full record](#)

Base Score Metrics

- AV NETWORK
- A COMPLETE
- AC MEDIUM
- C COMPLETE
- AU NONE
- I COMPLETE

Published on Jul 17, 2013
 Updated on May 5, 2014

Remediation

Target date **✘** Jul 23, 2015 Reviewed by [demo1](#)
 Actual date --/--/---- Reviewed Jul 13, 2015
 Updated by [demo1](#)
 Updated Jul 13, 2015

Status Remediation Required ▾

needs fixing

FOSS Supply Chain Risk Management

Classification	Standard Development Organisation	Standard	Comments
1 Origins (sources) of supply chains	ISO SC27	ISO/IEC 27036: Guidelines for Security of Outsourcing	These are generic documents and not specific to SCI
2 Delivery and governance of the Supply Chain	NASPO (North American Security Products Organization) NIST		Nothing specific to SCI
3 Processing and configuration	ISO SC31 iNEMI Supply Chain study group HDPUG Supply Chain study group:	RFID supply chain applications Risk Modelling pilot Data Exchange pilot	Nothing specific to SCI
4 Integrity techniques	JTC1-SC27 Safecode Open Group	N10656: Update to ISO 27002: Security Techniques Open Trusted Technology Framework	Nothing specific to SCI
5 Verification and checks	ISO TC247	Fraud Controls and Countermeasures SEMI T20: Traceability (semiconductor industry)	Nothing specific to SCI

FOSS Supply Chain Risk Management

목 차

- WG3 has finished **FOSS SCRM standard guideline**
 - The requirements of OSS supply management
 - The governance for OSS SCRM
 - OSS profiling for SCRM
 - The guide of compliance for SCRM
 - SPDX Specification
 - The application of SPDX for SCRM

I. The overview and need of OSS SCM	
1.1 The overview of OSS SCM	3
1.2 The purpose and need of OSS SCM	6
1.3 The scope of standard procedure of OSS SCM	6
II. The type and composition of general SW SCM	
2.1 Software Development Life Cycle(SDLC)	10
2.2 Component based Software Development Life Cycle(CLM)	12
2.3 Software Distribution Life Cycle(SDLC)	17
III. The requirements for OSS supply management	
3.1 The requirements related to component based development	21
3.2 The structure of OSS supply chain	32
3.3 OSS distribution life cycle	35
IV. The governance for OSS SCRM(Supply Chain Risk Management)	
4.1 The evaluation of OSS for SCRM	37
4.2 The purpose and organization for OSS SCRM	45
4.3 The implementation processes for OSS SCRM	50
4.4 The implementation guide for OSS SCRM	56
4.5 The validation for OSS SCRM	61
4.6 The education for OSS SCRM	76
4.7 The monitoring for OSS SCRM	82
V. OSS profiling for SCRM	
5.1 The overview and purpose of profiling for OSS SCM	86
5.2 The categorization and attribution of OSS profiling	87
5.3 Main OSS profiling	91
VI. The guide of compliance for SCRM	
6.1 GPL Compliance guide of SFLC	142
6.2 The feature and obligation of OSS license	165
VII. SPDX for SCRM	
7.1 The overview of SPDX	172
7.2 History of SPDX	172
7.3 SPDX Working Group	173
VIII. SPDX Specification	
8.1 The composition of SPDX	175
8.2 SPDX specification	176
IX. Supporting tool and service for SPDX	
9.1 SPDX Workgroup Tools	182
9.2 Community Tools	183
9.3 Commercial Tools	184
X. The application of SPDX for SCRM	
10.1 OSS Governance	185
10.2 The Standard procedure of OSS for SPDX	275
XI. SPDX License List	
XII. FAQ for SPDX	

We have supplied service for more than **1000** enterprises.

FOSS Governance

■ Definition

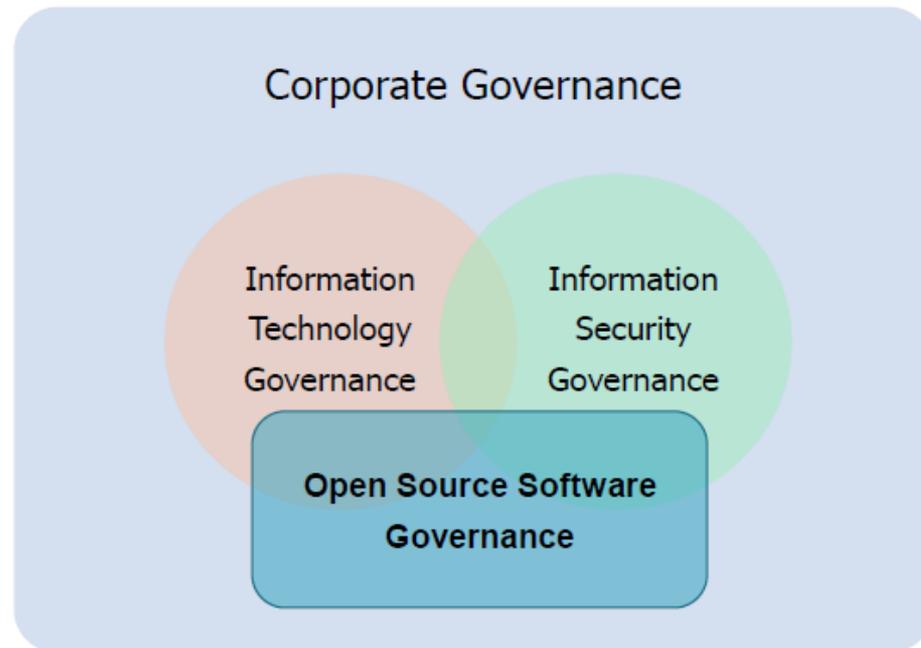
- ❑ Open-source governance (also known as open politics) is a **political philosophy** which advocates the application of the philosophies of the open-source and open-content movements to democratic principles to enable any interested citizen to add to the creation of policy, as with a wiki document. (https://en.wikipedia.org/wiki/Open-source_governance)
- ❑ Open source governance is the way an **organization controls** the use of open source software within their products and services, **supply chains and business management activities**, and the associated business and **legal processes**. (blackduck)

FOSS Governance

■ Purpose

- This guide provides a control framework and procedures for companies using open source, designed to help the accountability and compliance of enterprise open source.

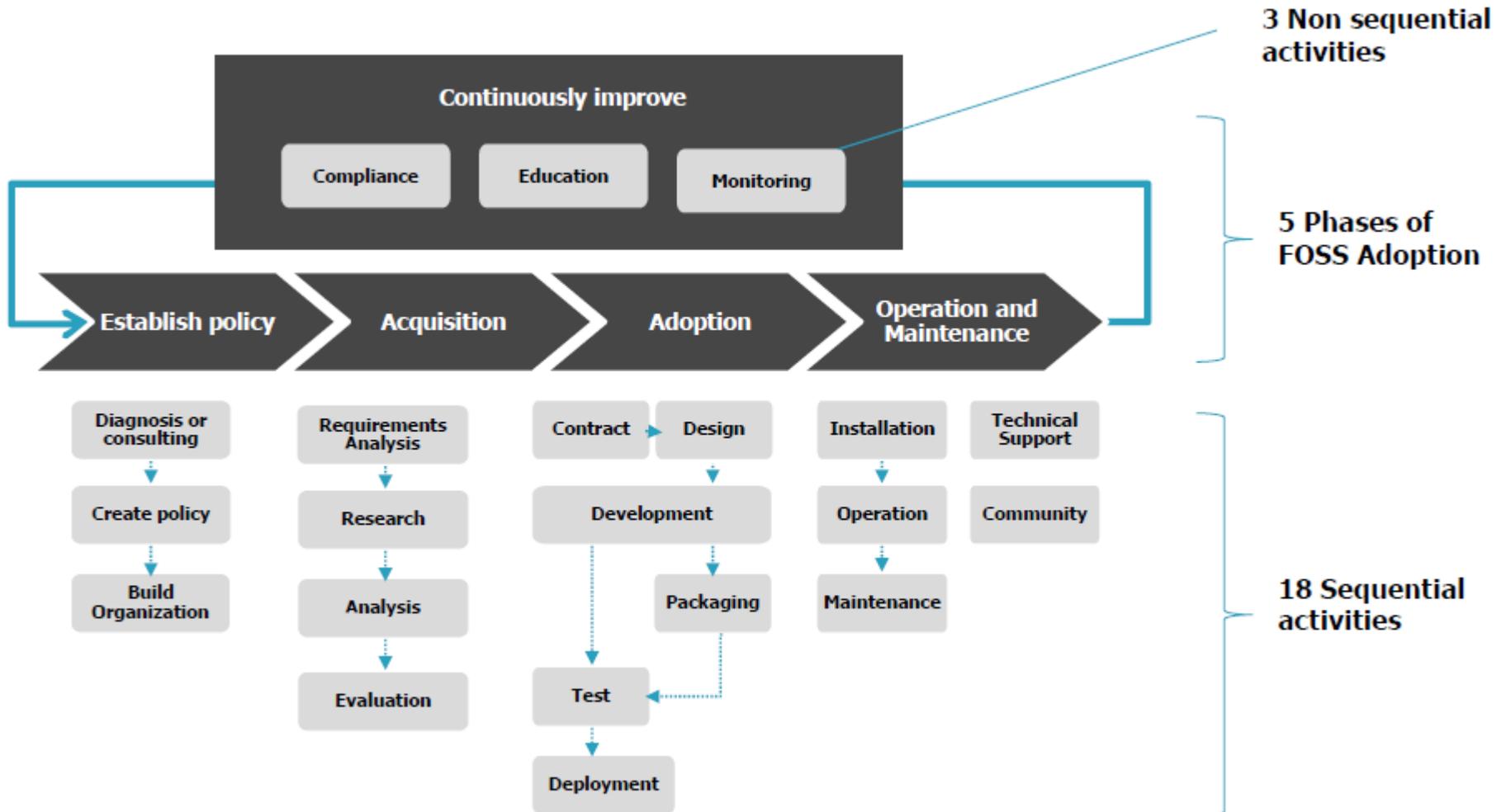
■ Scope



Scope of open source governance

FOSS Governance

■ Structure of FOSS Governance framework



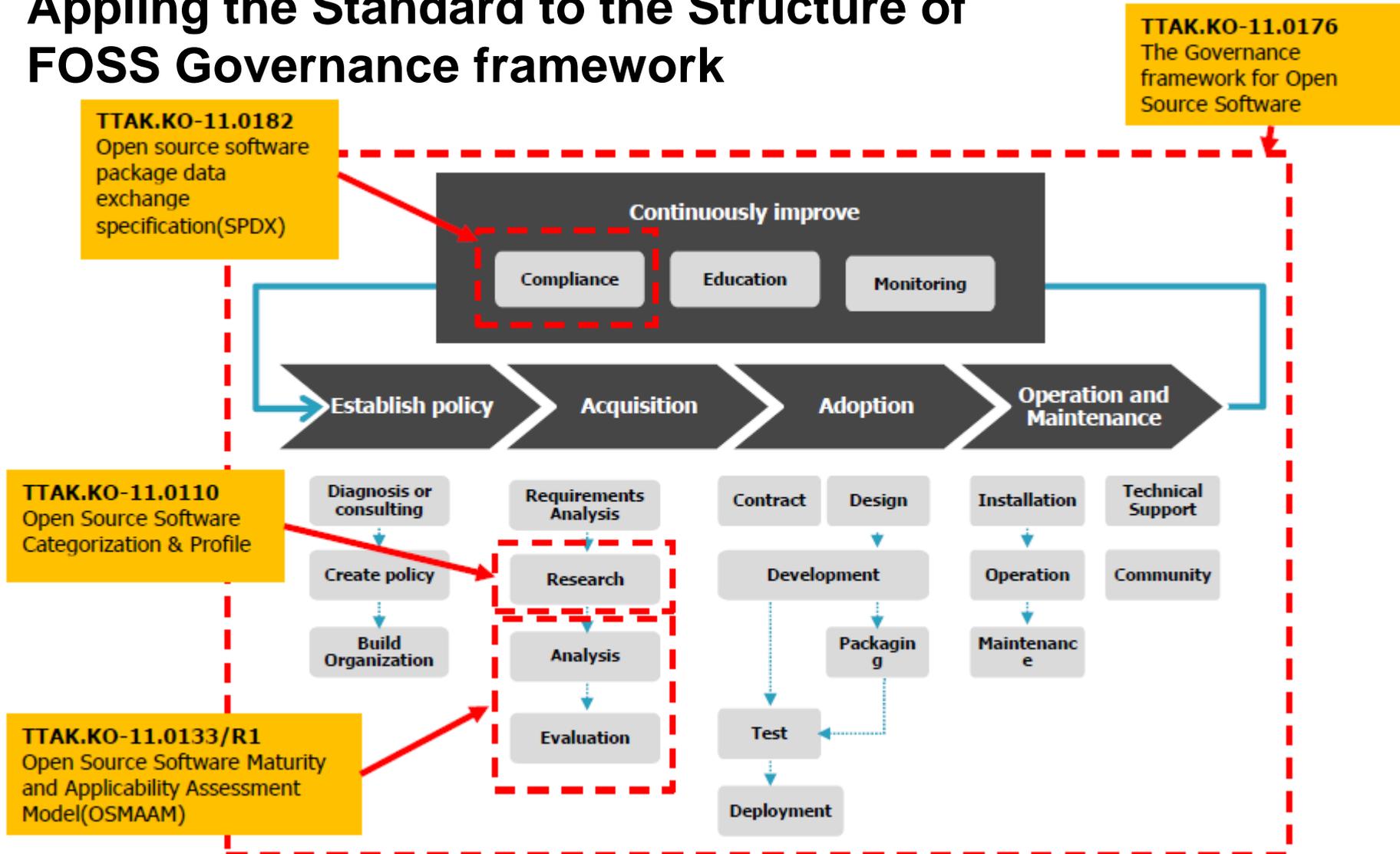
FOSS Governance

■ Four standards in Korea

No.	Name of the Standard
TTAK.KO-11.0110	Open Source Software Categorization & Profile
TTAK.KO-11.0133/R1	Open Source Software Maturity and Applicability Assessment Model(OSMAAM)
TTAK.KO-11.0182	TTAK.KO-11.0182 Open source software package data exchange specification(SPDX)
TTAK.KO-11.0176	The Governance framework for Open Source Software

FOSS Governance

■ Applying the Standard to the Structure of FOSS Governance framework

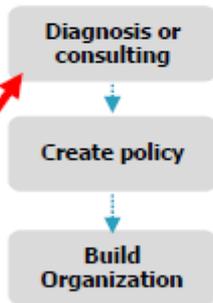
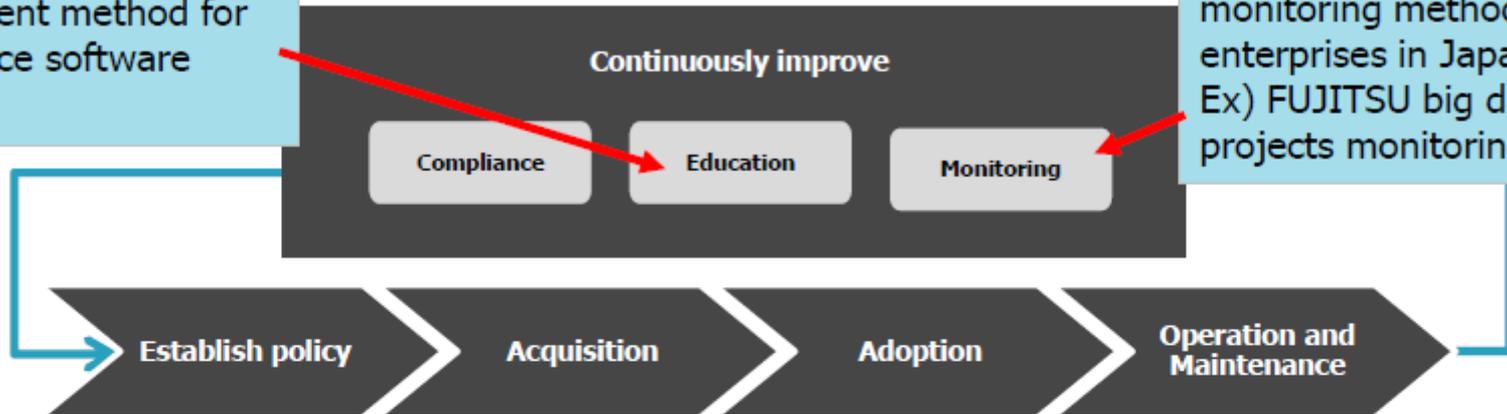


FOSS Governance

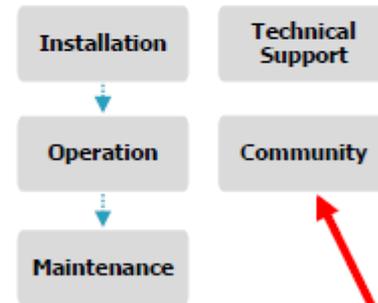
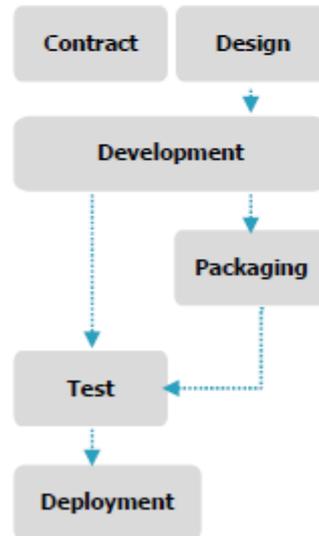
Future Work Overview

The Competency management method for open source software engineers

The open source projects monitoring method of enterprises in Japan. Ex) FUJITSU big data FOSS projects monitoring method



Open Source Organization Maturity Diagnostic Model.



The open source community management techniques of enterprises in China. Ex) HUAWEI, ALIBABA ...

Technology requirement of mobile terminal browser

■ Background

PC : interactive terminal = 2:3 (2007)

PC : smart terminal = 1:10 (Now)

smart terminal will reach 33 billion in 2020 \approx 4.3 / person

■ Purpose

- This standard applies to the design, development and test of mobile terminal browser

Technology requirement of mobile terminal browser

■ Scope

Run-time System Requirements

- Network
- Platform
- Memory
- Screen
- Keyboard
- Input Method
- ...

Protocol Requirements

- Markup Language
- Transfer Protocol
- Security Protocol
- Image Format
- Audio and Video Format
- Cache
- ...

Function Requirements

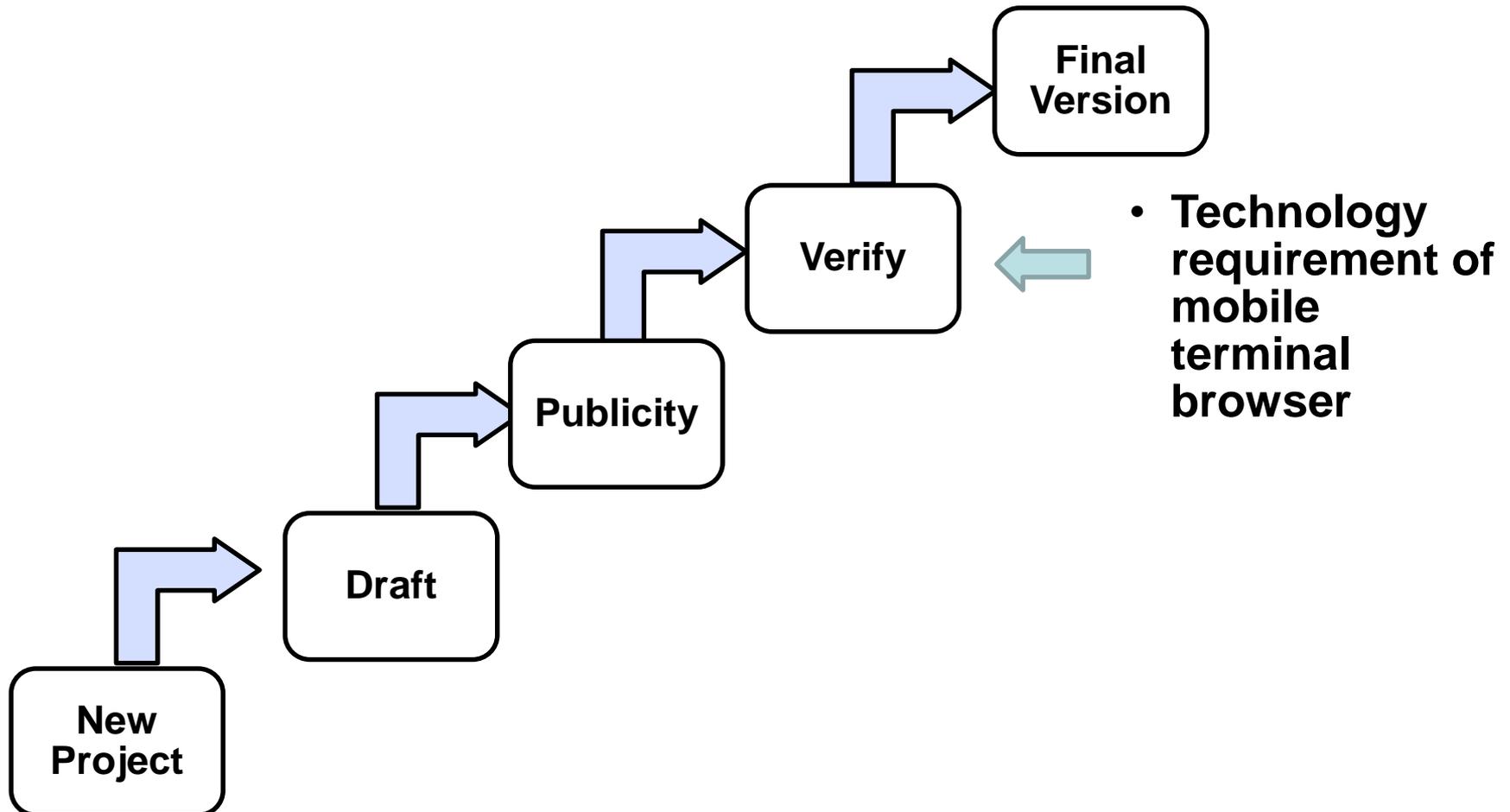
- Display
- Operation
- Network
- Address Bar Function
- Download Function
- Upload Function
- Bookmark Function
- Security Function
- Cache Function
- ...

Software Design Requirements

- Design Rules
- Analytical Page Requirements
- Performance Requirements
- Core Requirements
- Cache Requirements
- ...

Technology requirement of mobile terminal browser

■ Standard Status



OPENTHOS

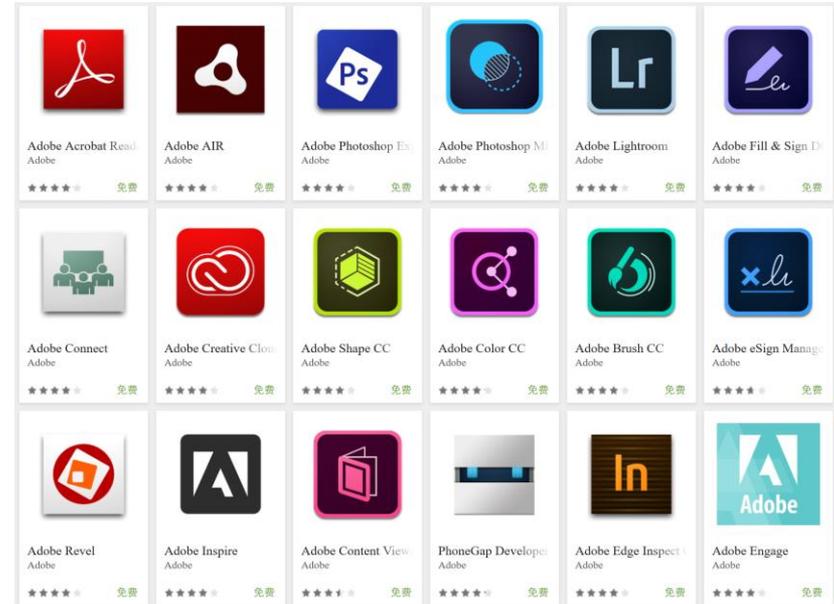
- **Background**
- **Problem**
- **What**
- **How**
- **Purpose**



OPENTHOS

■ Purpose

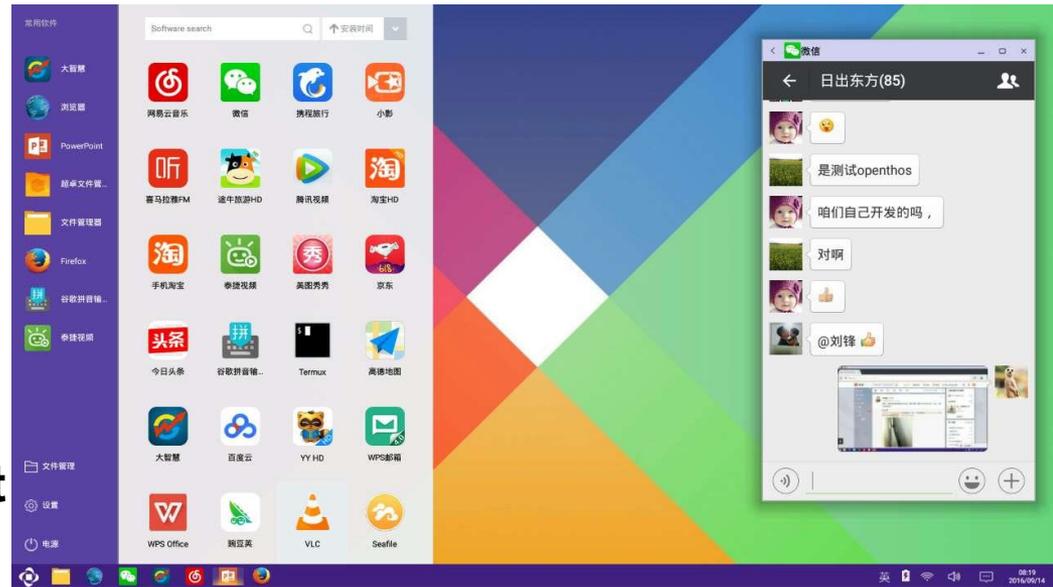
- High performance OS
- Android ecosystem
 - Developers
 - User
- High Security
- Cross-platform



OPENTHOS

■ Characters

- ❑ Multi-Windows Mngt
- ❑ Phone & Pad supported
- ❑ Mouse & Touch supported
- ❑ Print supported
- ❑ High performance
 - ❑ 60 frames/second
 - ❑ Low delay
- ❑ Low hardware requirement
- ❑ Unitive user information
 - ❑ Real-time backup
 - ❑ Synchronization between devices
 - ❑ High security
 - ❑ High reliability
- ❑ OPENThos Cloud



OPENTHOS

OPENTHOS

■ Community

□ Committers

- Tsinghua
- Tongfangpc
- emindsoft
- ...

■ Status

□ IOS version available

- Download : 700 in August

□ Source Code

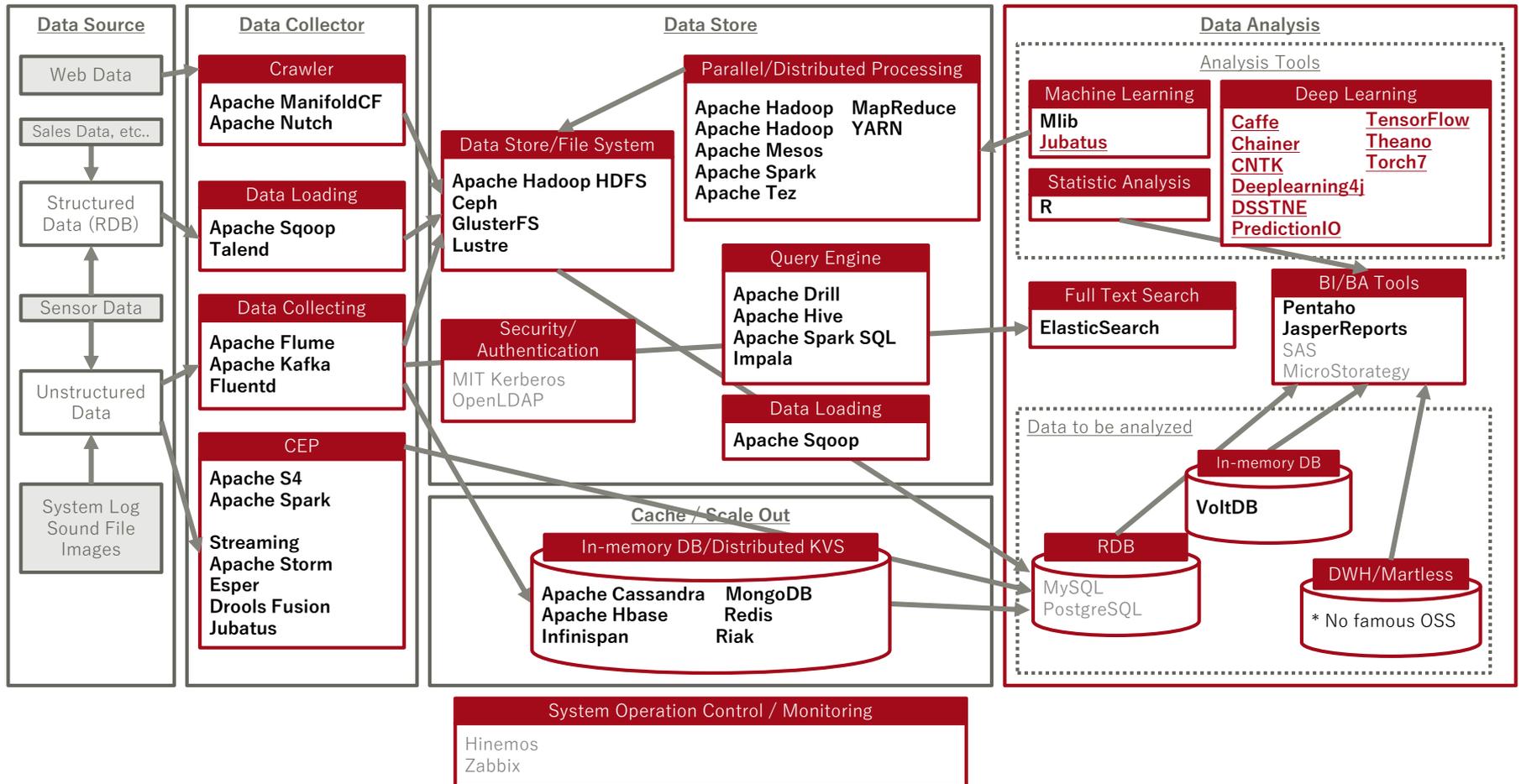
- <https://github.com/openthos>

□ 2016.12 - release on Tongfang PC



Survey of OSS in Big Data Platform

■ Structure



Survey of OSS in Big Data Platform

■ Survey Category

Developers' Activity

How active are developers?

Number of committers

Mailing list Numbers

top committer

Ratio of active days

Users' Activity

How popular is the software?

Books in Amazon

Mailing list Mails

Stars in GitHub

Followers on Twitter

Quality of Software

Can we use the software without defects?

Bug resolution rate

Vulnerabilities

Blocker/Critical Bug resolution rate

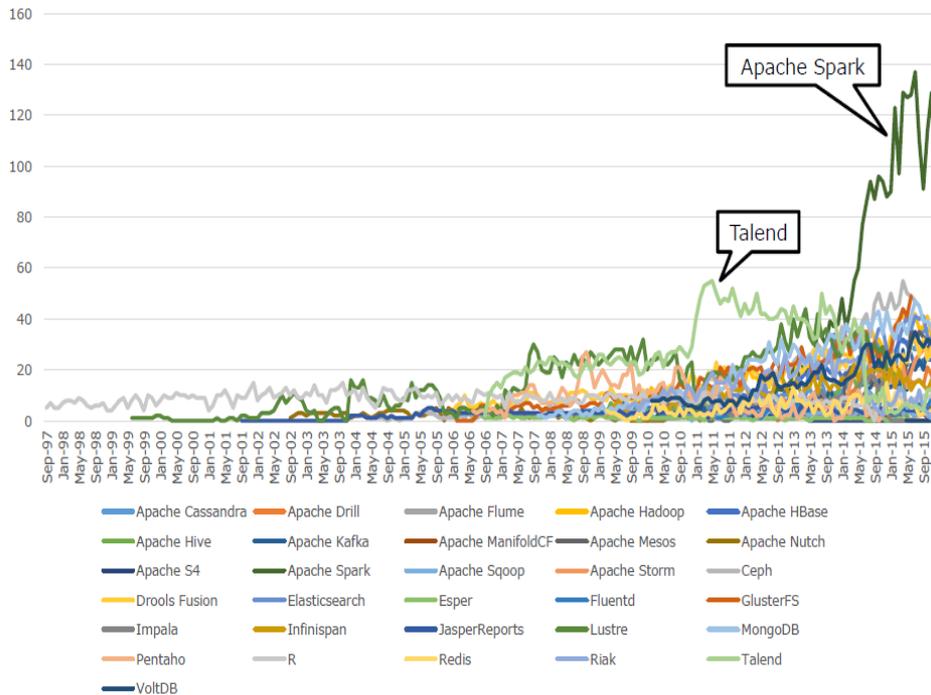
Duplications

Survey of OSS in Big Data Platform

■ Survey Result

Number of committers (monthly)

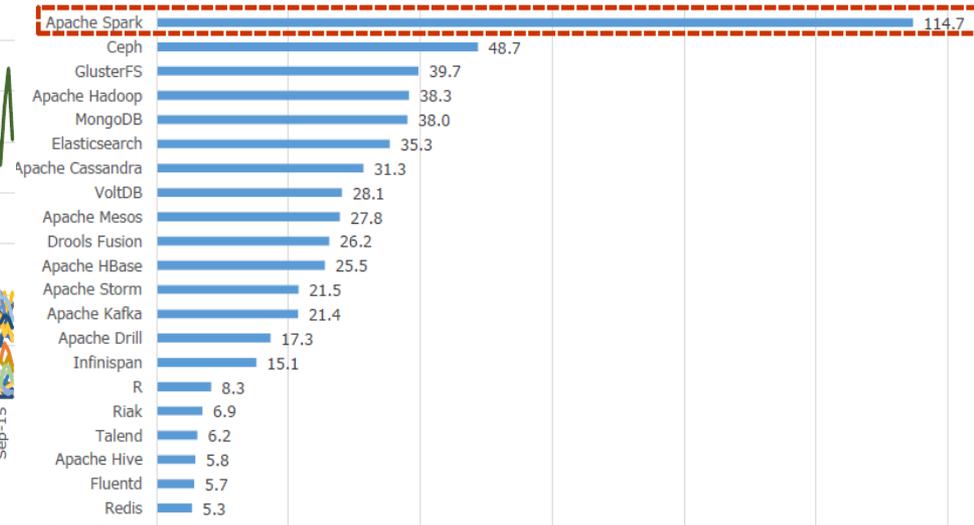
■ Apache Spark is rapidly increasing from 2014



Average number of committers in month

■ Over 100 committers make some commits to Apache Spark

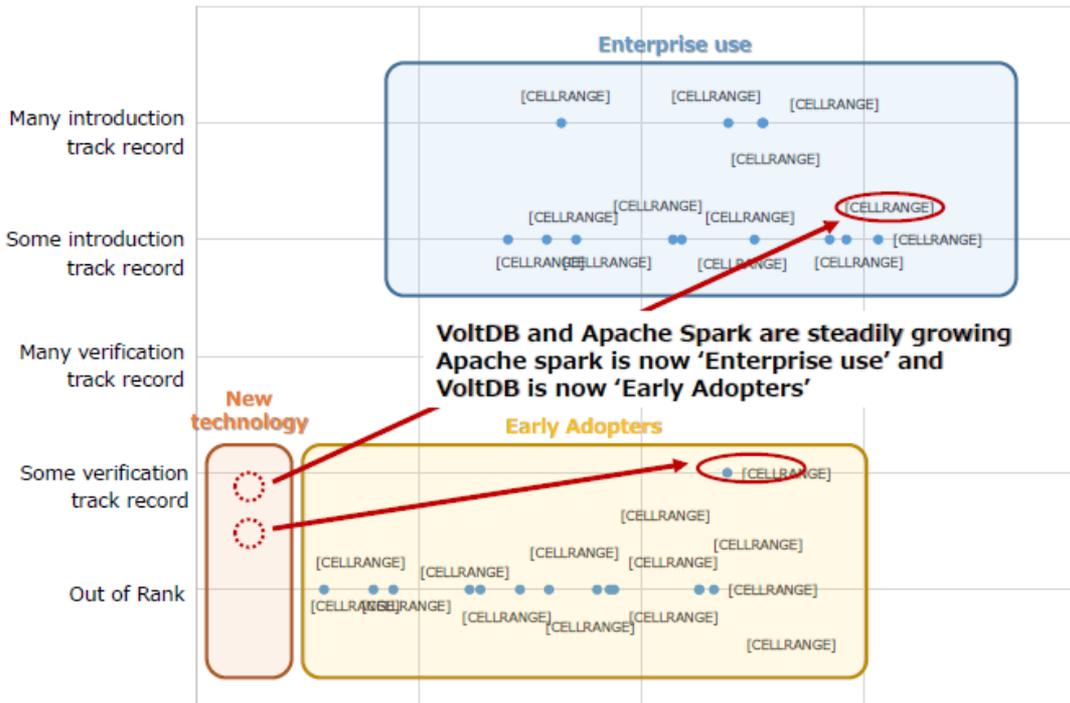
□ 2013 : 27.8 → 2014 : 72.1 → 2015 : 114.7



Survey of OSS in Big Data Platform

■ Survey Summary

Summary



■ Survey Conclusion

- We can build the Big Data Platform only with OSS
 - Enterprise supports are getting better
 - However, it is necessary to check the functions and quality of softwares
- Apache Spark and the ecosystem are **hot**
- Developers for Elasticsearch may be **hardworkers**
- MongoDB and Ceph are going to be **stable**

Work Plan of WG3 in 2017

- OASIS(Open source Support Information System)
- Assessment Model of Open R&D project for Government
- Applying FOSS Supply-Chain Risk Management Guide
- OpenTHOS Project
- Promote the application of WG3 achievements in CJK.

Thank you very much!

谢谢

ありがとうございました

감사합니다