

# How to tackle the IT security evaluation in Canon

Nobuhiro TAGASHIRA

Shuzo KANEKO

Canon Inc.

# Contents

---

1. Canon's current status
2. Background
3. Experiences - Evaluation
4. Experiences - Assurance Continuity
5. Conclusion

# Contents

---

1. Canon's current status
2. Background
3. Experiences - Evaluation
4. Experiences - Assurance Continuity
5. Conclusion



# Common Criteria engineers in Canon Group

- **Personnel Training** for CC at ECSEC\*<sup>1</sup>
  - ECSEC is the Evaluation facilities in JISEC\*<sup>2</sup>
- **ST Training Course** by ECSEC
  - Over 50 trainees (include E-Learning)
- **In-house CC Training**
  - Over 150 trainees
- Etc
  - **In-house IT Security Lectures**
    - ◆ Over 100 attendees



\*1 ECSEC : Electronic Commerce Security Technology Laboratory Inc.

\*2 JISEC : Japan Information Technology Security Evaluation and Certification Scheme

# Contents

---

1. Canon's current status
- 2. Background**
3. Experiences - Evaluation
4. Experiences - Assurance Continuity
5. Conclusion

# Background in Canon

- We have been regarding the Security Products as important, are developing the Security Products.

Example :

- 2002/11 EOS-1Ds w/ DVK-E1
- 2003/05 iR3350i series w/ Security Kit A1



iR3350i series

Security Kit A1



# Background – Social background

---

- Computer Processed Personal Data Protection Act
  - An OA apparatus maker, like Canon, has to manufacture the OA apparatus, which can deal with Personal Information securely.
- Corporate Social Responsibility (CSR)
  - A maker who manufactures the apparatus with security function, has to give a sense of security to users.

# Background - Acquisition Policy

- Some Acquisition Policies were changed in US and Other Countries around 2000-2001

## ex. NSTISSP No. 11 in Jan. 2000

- Effective 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products must be evaluated by :
  - ◆ CCRA
  - ◆ NIAP Evaluation and Validation Program
  - ◆ NIST FIPS validation program

# Background - Competitors' Trend

---

- **Apr. 2001 – Sharp (MFP)**
  - Data Security Kit (AR-FR1/AR-FR2/AR-FR3) for Sharp Imager Family (FR-287, AR-337, AR-407, and AR-507) in CCEVS (US Scheme)
  
- **Nov. 2001 – Ricoh (Document storage system)**
  - TrustyCabinet UX V1, Version 1.01 in TUVIT (German Scheme)
  
- **Jun. 2002 – Ricoh (MFP)**
  - imagio Neo 350/450 Series in TUVIT

## Background in Canon (2)

---

We need to improve  
the security function of Products further.

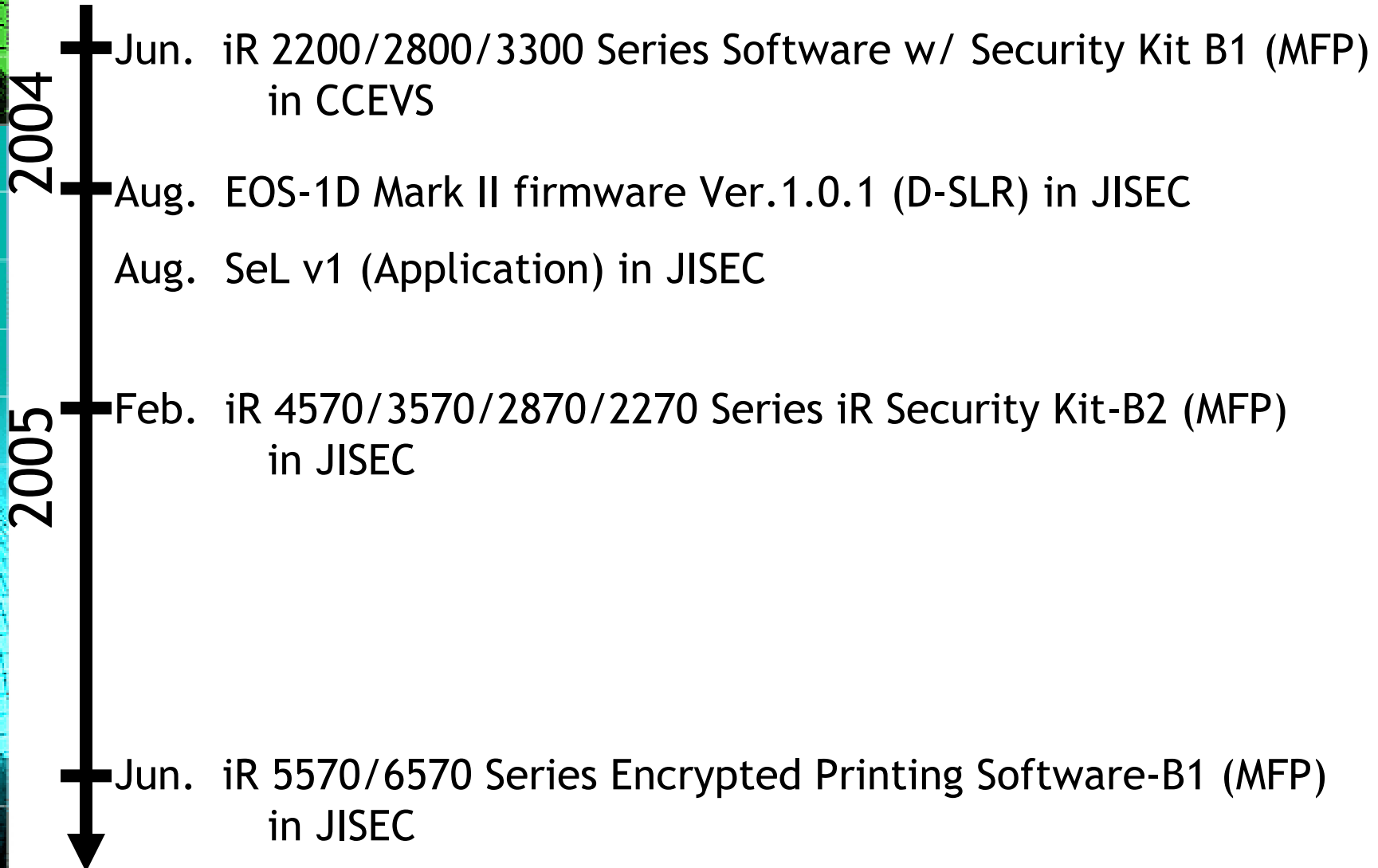
We choose a Third Party Evaluation and  
Validataion.

# Contents

---

1. Canon's current status
2. Background
- 3. Experiences - Evaluation**
4. Experiences - Assurance Continuity
5. Conclusion

# Some experiences of Eval./Valid. (1)



# Some experiences of Eval./Valid. (2)

- Period point of view

	Period
<b>1st MFP</b> <b>(iR 2200/2800/3300 Series Software w/ Security Kit B1)</b>	<b>over 1 year</b>
<b>D-SLR</b> <b>(EOS-1D Mark II firmware)</b>	<b>190 days</b>
<b>APP (SeL)</b>	<b>230 days</b>
<b>2nd MFP</b> <b>(iR 4570/3570/2870/2270 Series iR Security Kit-B2)</b>	<b>255 days</b>
<b>3rd MFP</b> <b>(iR 5570/6570 Series Encrypted Printing Software-B1)</b>	<b>302 days</b>

# Effect from some experiences of Eval./Valid.

- Canon Development point of view

## Before

- The security functions were implemented.
- No one knows CC/ISO 15408

## After

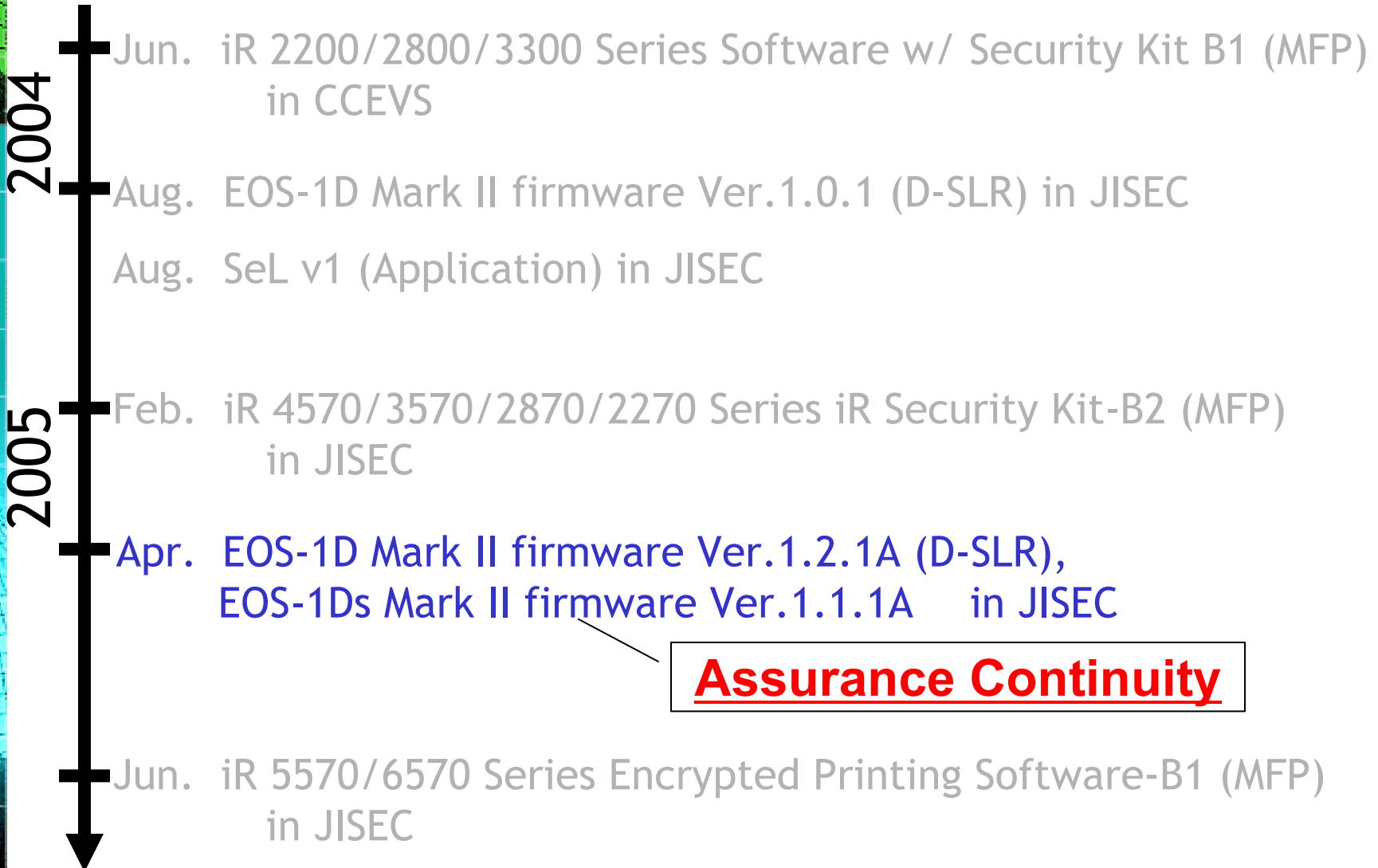
- The verified appropriate security functions were implemented
  - ◆ based on Security Target
  - ◆ based on Top-Down Design Policy
- Improvement of Development Process
  - ◆ Many developers know CC/ISO 15408

# Contents

---

1. Canon's current status
2. Background
3. Experiences - Evaluation
- 4. Experiences - Assurance Continuity**
5. Conclusion

# An experience of Assurance Continuity



# What is Assurance Continuity? (1)

- CC has some Problems.
  - Time-consuming, Expensive, ...

**One Solution = Assurance Continuity**

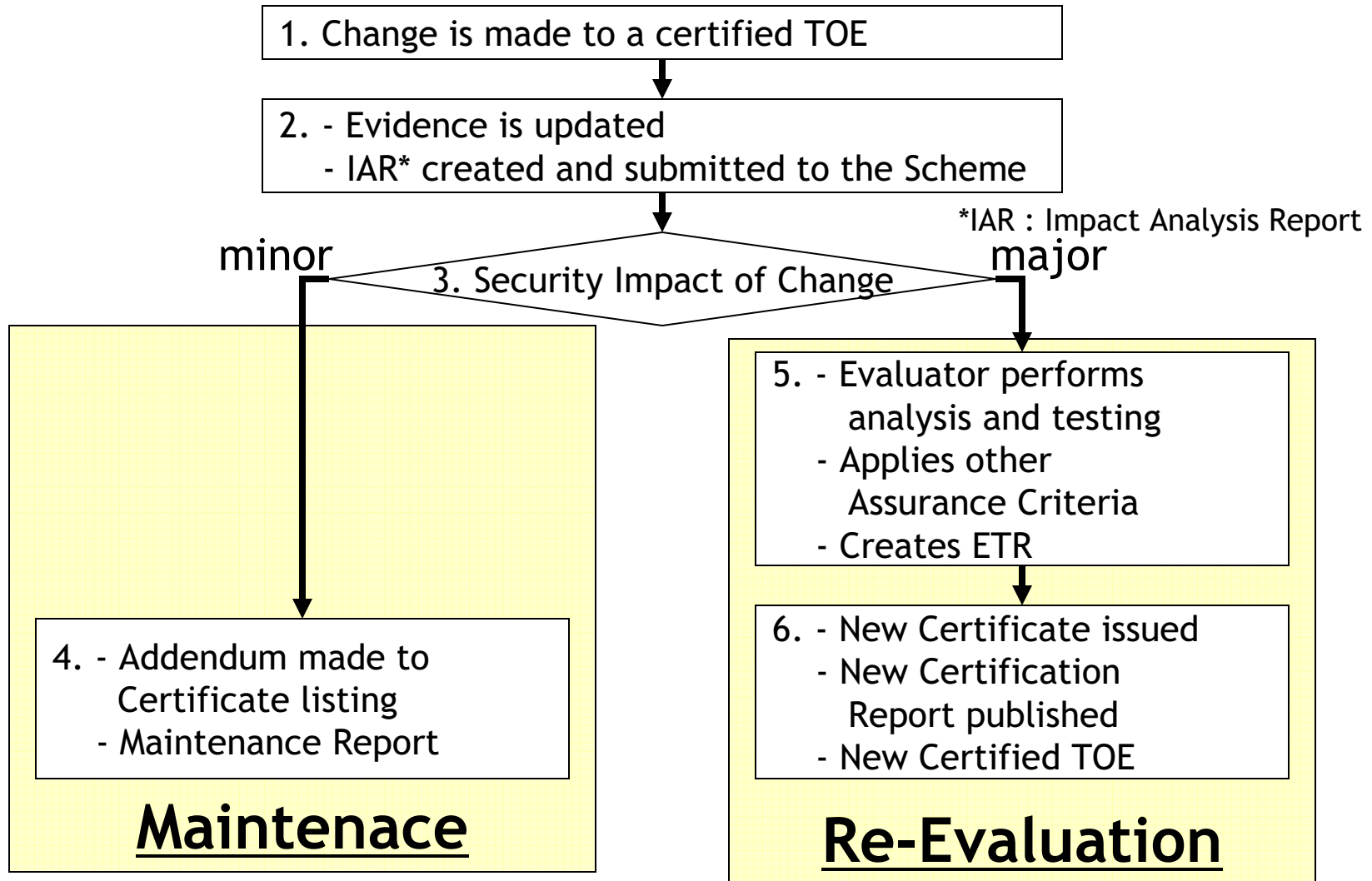
- In Feb. 2004, "Assurance Continuity" was released.

"Assurance Continuity recognises that as changes are made to a certified TOE or its environment, evaluation work previously performed need not be repeated in all circumstances. Assurance Continuity therefore defines an approach to minimising redundancy in IT Security evaluation, allowing a determination to be made as to whether independent evaluator actions need to be re-performed." from Section 2.1 of "Assurance Continuity"

That is to consider the product version related to certified TOE as the certified TOE.

# What is Assurance Continuity? (2)

From Section 2.1 of "Assurance Continuity".



# What is the Target of Assurance Continuity?

- Some quite similar products : **EOS-1D Mark II**, **EOS-1Ds Mark II**
  - Same Security Function, same I/Fs
  - Same Development Environment
    - ◆ Same Development Buildings and same floor
    - ◆ Same Src Repository
  - Some different Non Security Functions
    - ◆ Image Sensor (8.5m pixel vs. 16.7m pixel)
    - ◆ Continuous shooting speed
    - ◆ etc.

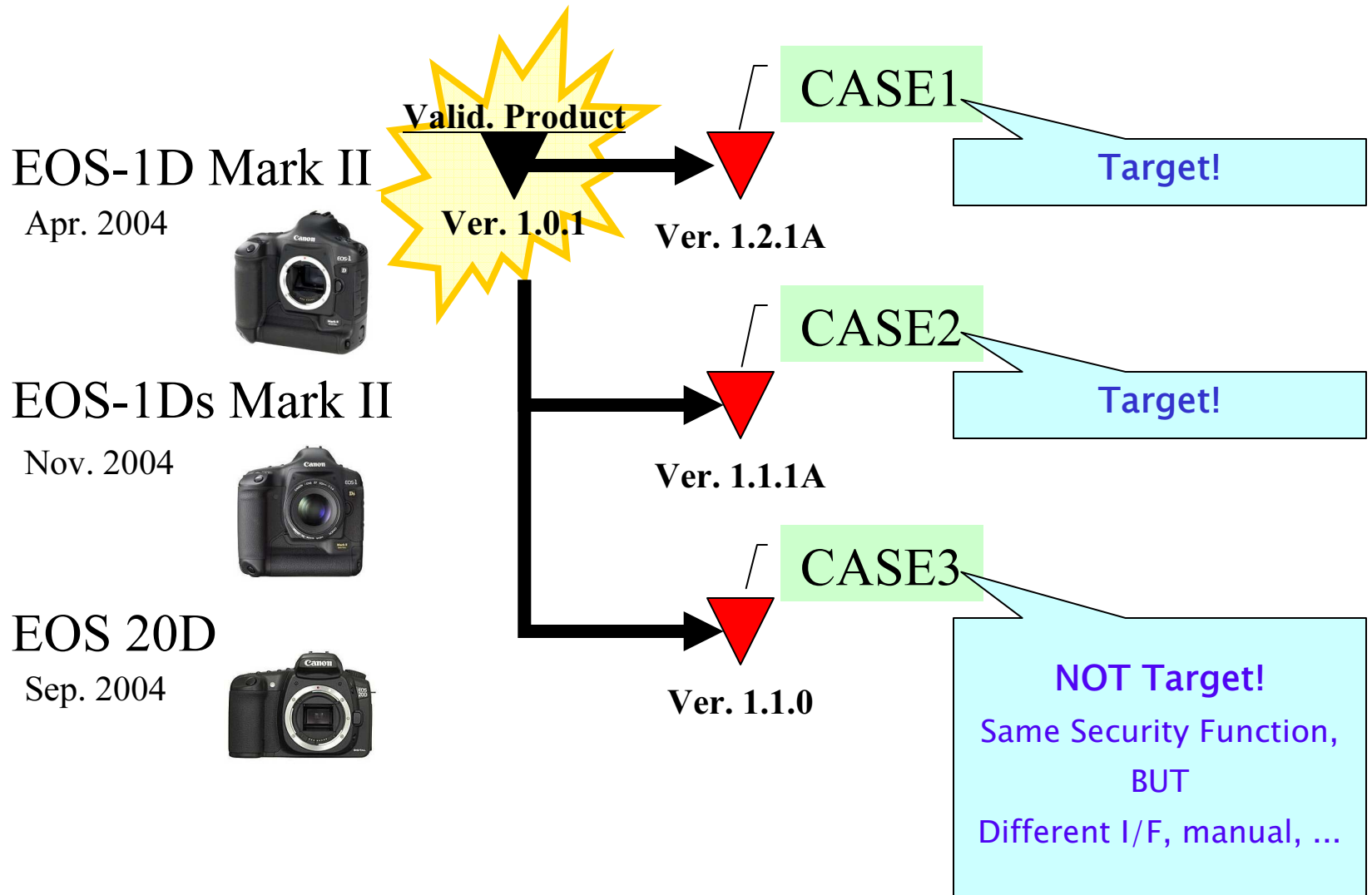


**EOS-1D Mark II**



**EOS-1Ds Mark II**

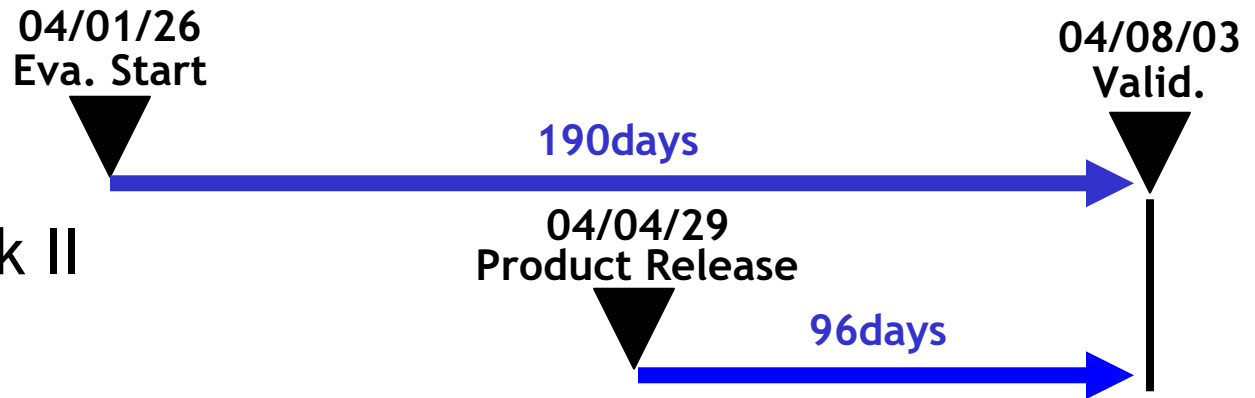
# What is the Target? (2)



# Consideration – Eval./Valid. period

## 1<sup>st</sup> Validation

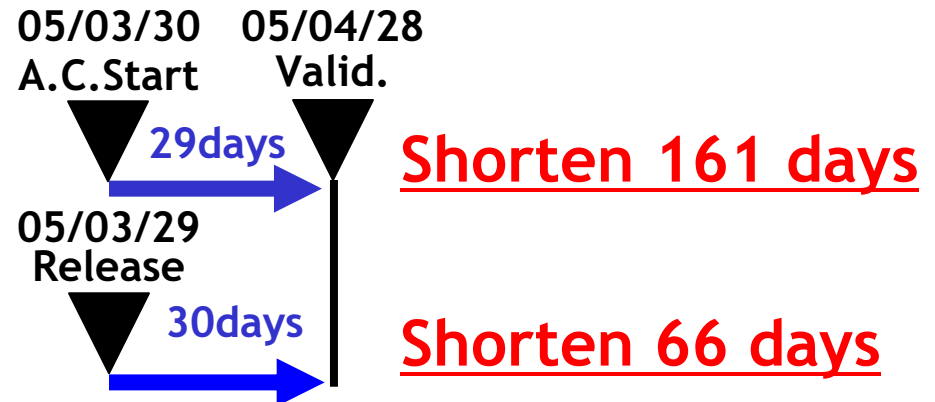
- EOS-1D Mark II Ver.1.0.1



## 2<sup>nd</sup> Validation

(Assurance Continuity)

- EOS-1D Mark II Ver.1.2.1A
- EOS-1Ds Mark II Ver.1.1.1A



# From an experience of Assurance Continuity

- Assurance Continuity is very effective means :
  - From shortening time  
(include cost reduction)
  - From the possibility to unfold the related Product
- Therefore
  - We must **develop a series of the Product** and we must **determine the TOE**, in consideration of Assurance Continuity.

# Contents

---

1. Canon's current status
2. Background
3. Experiences - Evaluation
4. Experiences - Assurance Continuity
5. Conclusion

# Conclusion (1)

---

- In Canon,
  - Enforce to tackle the IT security evaluation structurally and methodically in whole Canon.
    - ◆ To improve products
    - ◆ To improve development process
    - ◆ To reduce overall cost using Assurance Continuity
  - Note  
Not all Canon Products will be evaluated by Third Party,  
but all Canon Products will be evaluated using CC.

# Conclusion (2)

- For CC project / Schemes,
  - Eval./Valid. is still time-consuming and expensive
  - Assurance Continuity is a good solution,
    - but it is not the radical solution
    - ◆ Since it is a "Continuity", that means 2<sup>nd</sup>.
  - CC Scheme does not spread widely (Especially in Japan)

**We hope that CC ver. 3 is good solution!**

- There are many (Int'l) STDs to improve the Product
  - ◆ Software/System Life Cycle Processes
  - ◆ IT Security Evaluation, CMVP, ...

**Fusion of the Eval. method and the Devlp. method  
or  
Separation of Eval. method and the Devlp. method**

# Thank you

**Nobuhiro TAGASHIRA**  
**tagashira.nobuhiro@canon.co.jp**

**Shuzo KANEKO**  
**kaneko.shuzo@canon.co.jp**

**Canon Inc.**