IETF 情報交換会・座談会 - IETF123より – SCITTを中心とした活動報告＋α

2025/10/23（木）

青木 信雄

アジェンダ

- 自己紹介・概要
- SCITTにおける活動報告
- コラム：IETF124の活動予定
- コラム：標準化関連活動をindividualへ
- ~~コラム：標準化人材が空洞化してしまったら何が起こるか（次回以降）~~

自己紹介 & 概要

- 氏名：青木信雄
- 所属：総合研究大学院大学 先端学術院先端学術専攻 情報学コース
  （教育提供の基盤機関: 大学共同利用機関 国立情報学研究所）
- 関連活動時の所属：N/A
- 関連活動：
  - IETF124 Montreal: R7情報通信分野の国際標準化会議 参加者募集（NRI）
  - IETF121 Dublin: R6情報通信分野における国際標準化動向調査者（NTTデータ経営研）
    - テーマ名：透明性・説明責任の観点からのIoTを主軸とする情報通信技術の標準化動向調査
  - IETF118 Praha: IETF2023年度 IETF参加支援（JPNIC）
- 調査対象機関：Internet Engineering Task Force (IETF) SCITT WG
- 対象技術：サプライチェーン・セキュリティ

SCITT WGの最新動向と見どころ

- Supply Chain Integrity, Transparency, and Trust WG
  - charter-ietf-scitt-01
  - ファームウェアを含むソフトウェア（e.g., コンポーネント, アーティファクト）のサプライチェーン情報を提供するためのTechnical Flowを標準化し、アーキテクチャを構成する本質的な構成要素を網羅する

- An Architecture for Trustworthy and Transparent Digital Supply Chains
  - draft-ietf-scitt-architecture-22 RFC Ed Queue
  - サプライチェーン上におけるライフサイクルを検証可能なStatement発行によって実現

- SCITT Reference APIs
  - draft-ietf-scit-scrapi-05 In WG Last Call
    - コンセンサス・メインキングの準備、実装の数併せ中
  - 上記アーキテクチャ上でStatement発行を行うためのAPIを定義

SCITT WGの最新動向と見どころ

- Supply Chain Inte
  - charter-ietf-scitt
  - ファームウェアを
    サプライチェーン
    アーキテクチャを
- An Architecture f
  - draft-ietf-scitt-ar
  - サプライチェーン
- SCITT Reference
  - draft-ietf-scit-sc
    - コンセンサス・メ
  - 上記アーキテクチ

Supply Chain Integrity, Transparency, and Trust (scitt)

About | Documents | Meetings | History | Photos | Email expansions | List archive »

Search

Document	Date	Status	IPR	AD/Shep-herd
Active Internet-Draft (1 hit)				
draft-ietf-scitt-scrapi-05 (27 pages) **SCITT Reference APIs**	2025-07-02	I-D Exists; In WG Last Call; Review: httpdir Early		
Active with the IESG Internet-Draft (1 hit)				
draft-ietf-scitt-architecture-22 (41 pages) **An Architecture for Trustworthy and Transparent Digital Supply Chains**	2025-10-10 New	RFC Ed Queue : EDIT; Submitted to IESG for Publication : Proposed Standard; Reviews: iotdir secdir IETF Last Call genart IETF Last Call httpdir Early; Dec 2023		Deb Cooley ✉, Amaury Chamayou ✉
Related Internet-Drafts and RFCs (1 hit)				
draft-nobuo-scitt-use-cases-extension-00 (6 pages) **Supply Chain Use Cases to Design Secure Computing Systems for SCITT Extension**	2025-07-07	I-D Exists		

SCITT Arch.

[1]

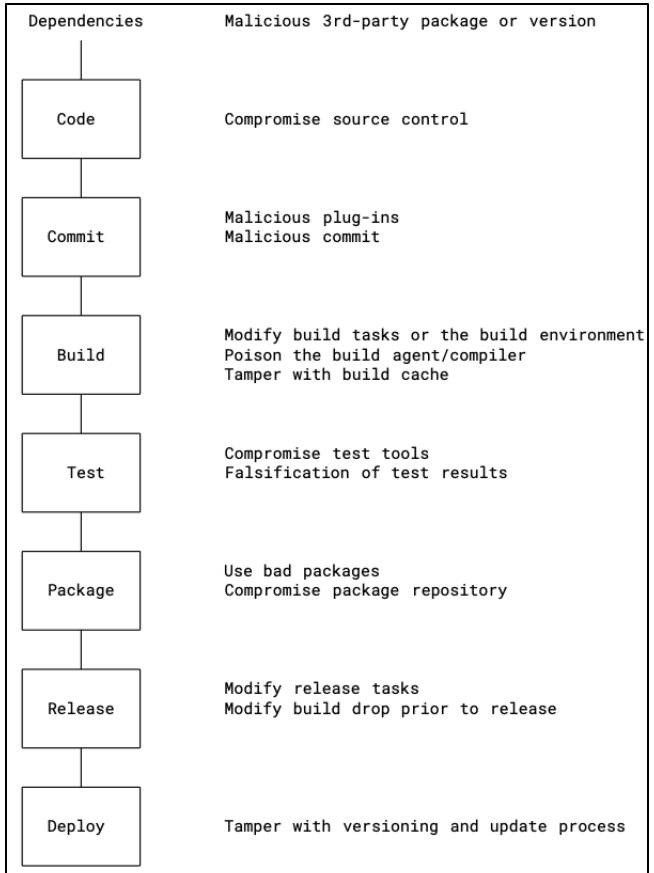
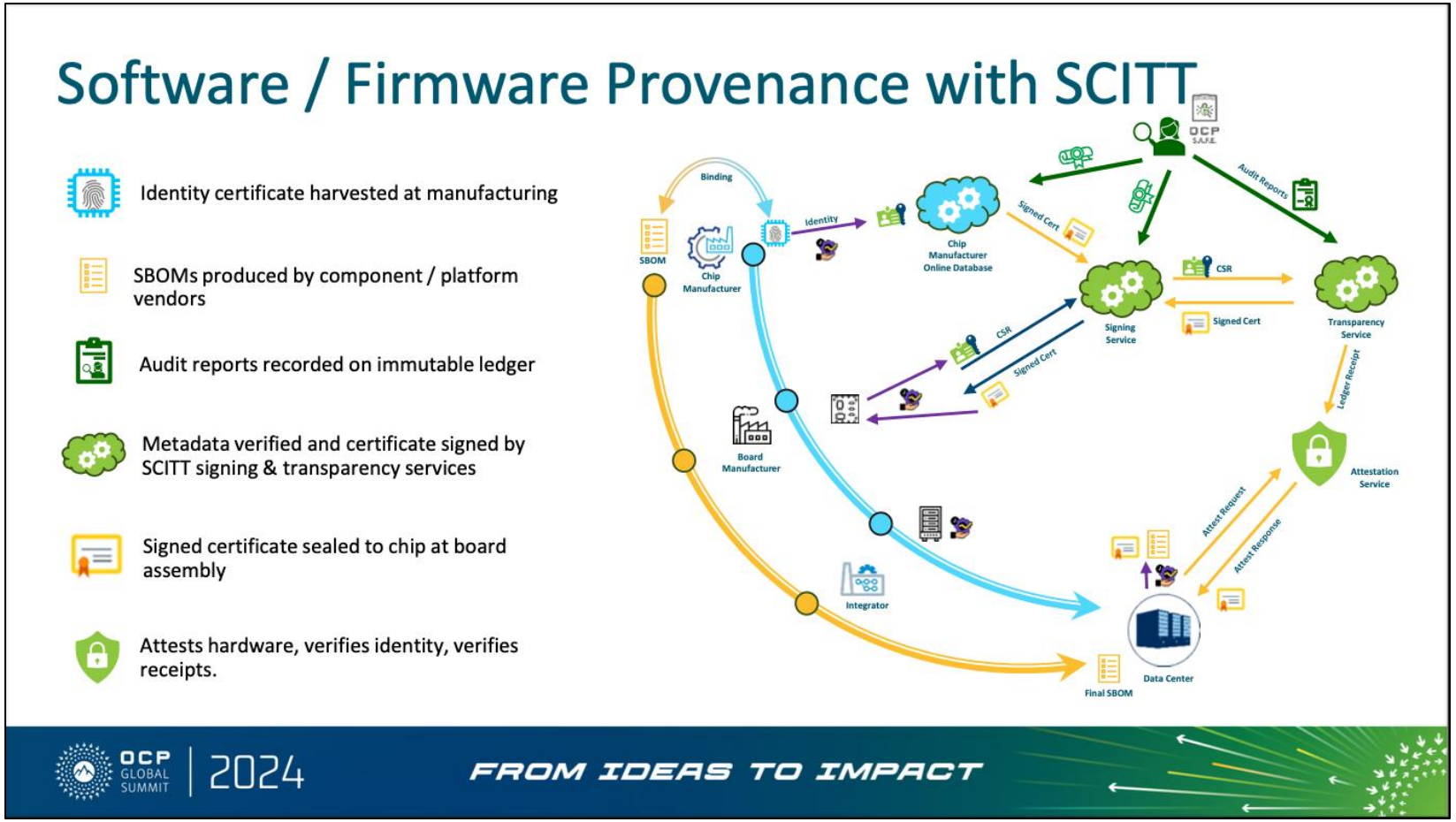


Figure 1: Example SSC Life-Cycle Threats

[2]



[1]SCITT Arch.
[2] https://drive.google.com/file/d/1IlBcnI0xv4dr5TZJa_aqgfoDUGVdtc3Q/view?pli=1

Timeline

1. Hachathon121
2024/11/02
作業開始 & WG Chairとの関係性作り

2. Hachathon121
2024/11/03
提案の可能性を示唆

3. Hachathon121
2024/11/03
作業協力を打診

4. email
2025/03/13
作業再開を宣言

5. email
2025/03/14
作業内容へのCommentを貰う

6. Hackathon122
2025/03/15
提案の余地を列挙 & 作業内容の選定

7. Hackathon122
2025/03/16
問題提起 & 要件定義 & PoCの準備
ダイアグラム問題の解決策を用意

8. IETF122
2025/03/18
プレゼンテーションの委託 & 資料作成

9. IETF122 SCITT WG
2025/03/22
ダイアグラム問題の解決策の
ラフコンセンサス・メイキングが
取れてmicsに謝辞が載る
Arch. & APIのRFC化のための
スコープが定まる

10. Hackathon123
2025/07/19
Arch.のための
実装が出揃う
use-case I/D投稿

10. IETF123
2025/07/21
Arch.のWGLC
use-case I/D議論

11. OCP SanJose
2025/10/17
キラー・ユースケース
ハードウェアを含む
Root of Trustの検証を発見

10. Hackathon124
2025/11/2
新規提案I/Dの推敲
データモデルの改良
APIの実装を募る

12. IETF124
2025/11/4
APIのWGLC

13. IETF125
2026/03
新規提案I/D？

ダイグラム問題の解決策

- 拡張仕様の提案内容
  - “Statement about Statements”の導入

- 作業内容
  - 現在の仕様（SCITT Arch. & SCRAPI）のlimitationを指摘
  - 指摘したlimitationの解決策の簡単な一例を提案
  - 拡張作業の過程において，SCITTの利便性を向上させる見込みを指摘

[1]

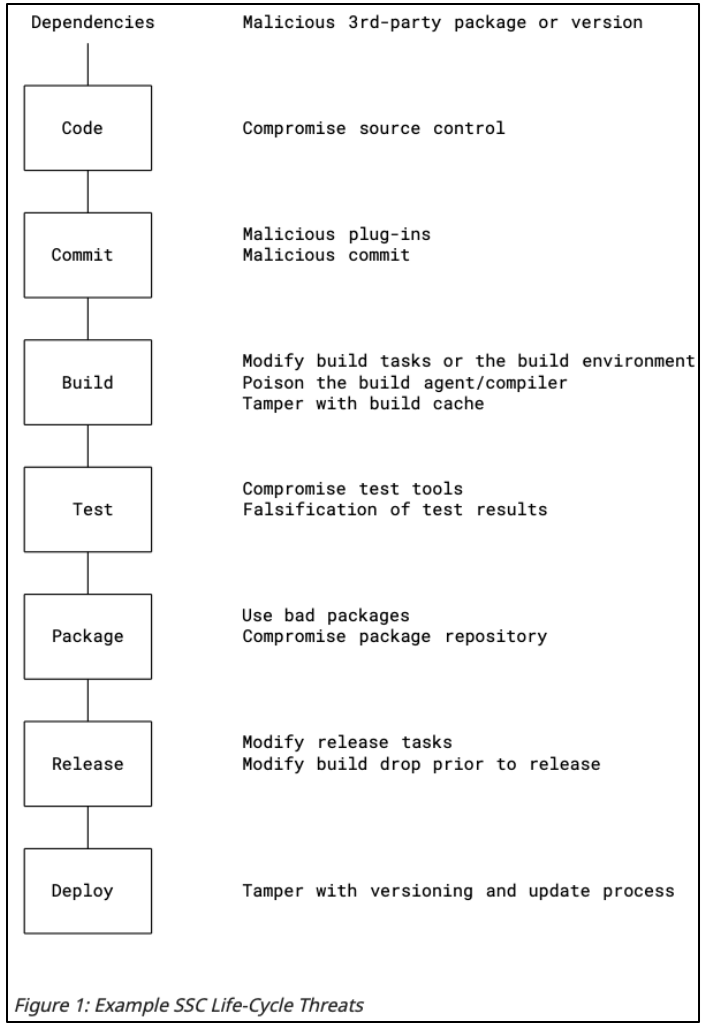
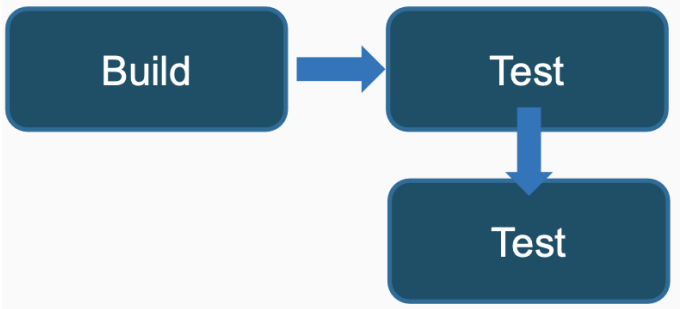
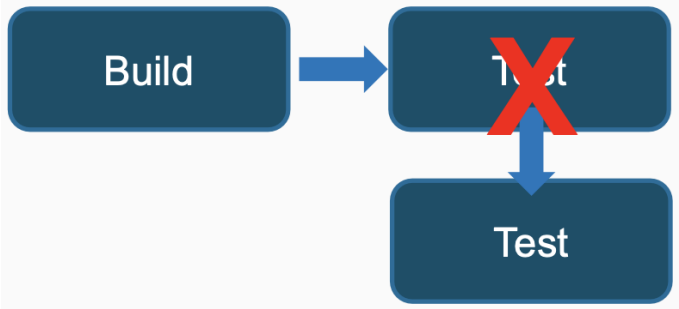


Figure 1: Example SSC Life-Cycle Threats

Current spec. [3]



Future spec. [3]



[3] https://datatracker.ietf.org/meeting/122/materials/slides-122-scitt-ietf-122-scitt-final-00.pdf

Timeline

1. Hachathon121
2024/11/02
作業開始 & WG Chairとの関係性作り

2. Hachathon121
2024/11/03
提案の可能性を示唆

3. Hachathon121
2024/11/03
作業協力を打診

4. email
2025/03/13
作業再開を宣言

5. email
2025/03/14
作業内容へのCommentを貰う

6. Hackathon122
2025/03/15
提案の余地を列挙 & 作業内容の選定

7. Hackathon122
2025/03/16
問題提起 & 要件定義 & PoCの準備
ダイアグラム問題の解決策を用意

8. IETF122
2025/03/18
プレゼンテーションの委託 & 資料作成

9. IETF122 SCITT WG
2025/03/22
ダイアグラム問題の解決策の
ラフコンセンサス・メイキングが
取れてmicsに謝辞が載る
Arch. & APIのRFC化のための
スコープが定まる

10. Hackathon123
2025/07/19
Arch.のための
実装が出揃う
use-case I/D投稿

10. IETF123
2025/07/21
Arch.のWGLC
use-case I/D議論

11. OCP SanJose
2025/10/17
キラー・ユースケース
ハードウェアを含む
Root of Trustの検証を発見

10. Hackathon124
2025/11/2
新規提案I/Dの推敲
データモデルの改良
APIの実装を募る

12. IETF124
2025/11/4
APIのWGLC

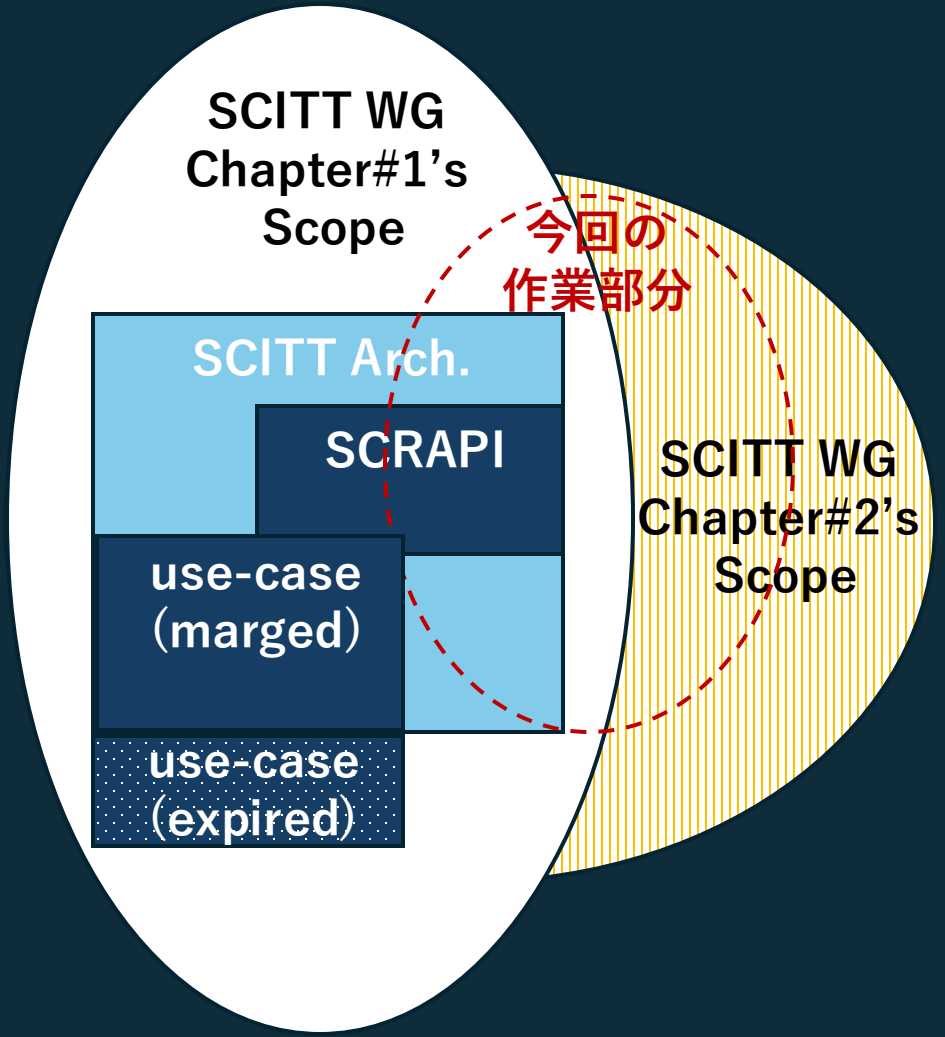
13. IETF125
2026/03
新規提案I/D？

IETF123で使用したスライドを使って、
ぼちぼち追っていきます

Use case extension

- Nobuo Aoki

Use case extension
- Nobuo Aoki



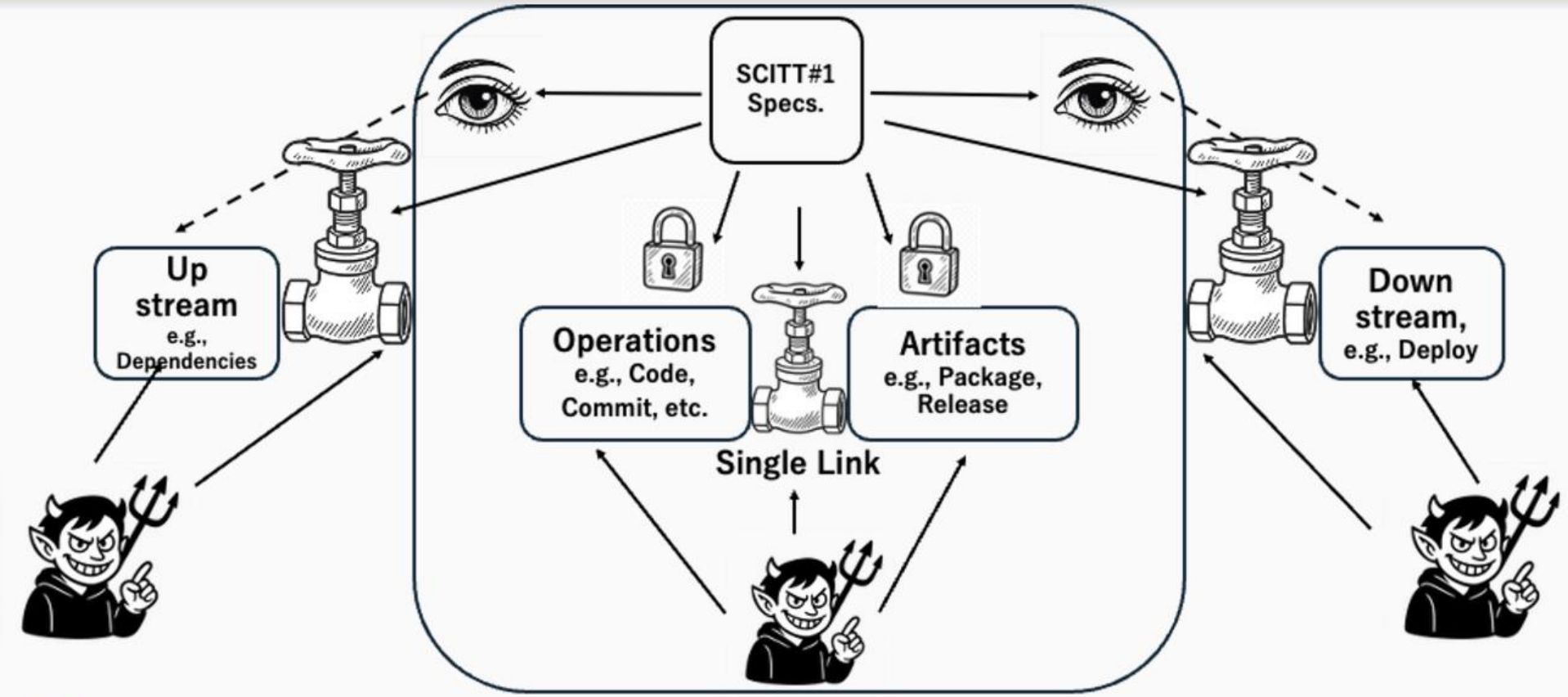
Quick Recup: Use Case Extension I-D

- Extension Request for maximize the appeal of SCITT WG
  - **SCITT** WG is no **S**oftware supply **C**hain **I**ntegrity, **T**ransparency, and **T**rust, but **S**upply **C**hain **I**ntegrity, **T**ransparency, and **T**rust
  - Add Hardware and Computer Architecture Layer
- Main reason author wanted WG support in the draft
  - Revision of chapter#2 for Post SCITT Spec.
  - Consensus is most important

Problem Statement: Level 1/3

- How to comprehensively provide Supply Chain Security information for a Computing Host resource (Software & Hardware)?

SCITT Chapter#1 Specs. Advantages



✅ Delivery of supply chain information throughout the E2E supply chain

Related Specs. to Supply Chain Security

- IETF RFC 9472
  - A YANG Data Model for Reporting Software Bills of ...
  - Successful mapping of SBOM and vulnerabilities
- x-BOM (i.e., Statement for SCITT)
  - SBOM, HBOM, E-BOM, M-BOM, etc.
- Others
  - OpenSSF some project, OCP S.A.F.E. Program, etc.

What are the Challenges in the SCITT Chapter#1 and Other Specs.

- Key-aspects of Supply Chain Security in Cybersecurity
  - Outstanding commander
  - Shield wall

Example case:
HW
SW (e.g., System SW)
SW (e.g., Virtualization Infra.)
SW (App. SW Package)
SW (App. SW Configuration)

e.g., HBOM
e.g., SBOM
e.g., SBOM
e.g., SBOM
e.g., something statement

Even if statements format is perfect, there is ambiguity in the relationships between the statements and some parts remain unclear

Picture Citation from https://en.wikipedia.org/wiki/Shield_wall

Problem Statement: 2/3

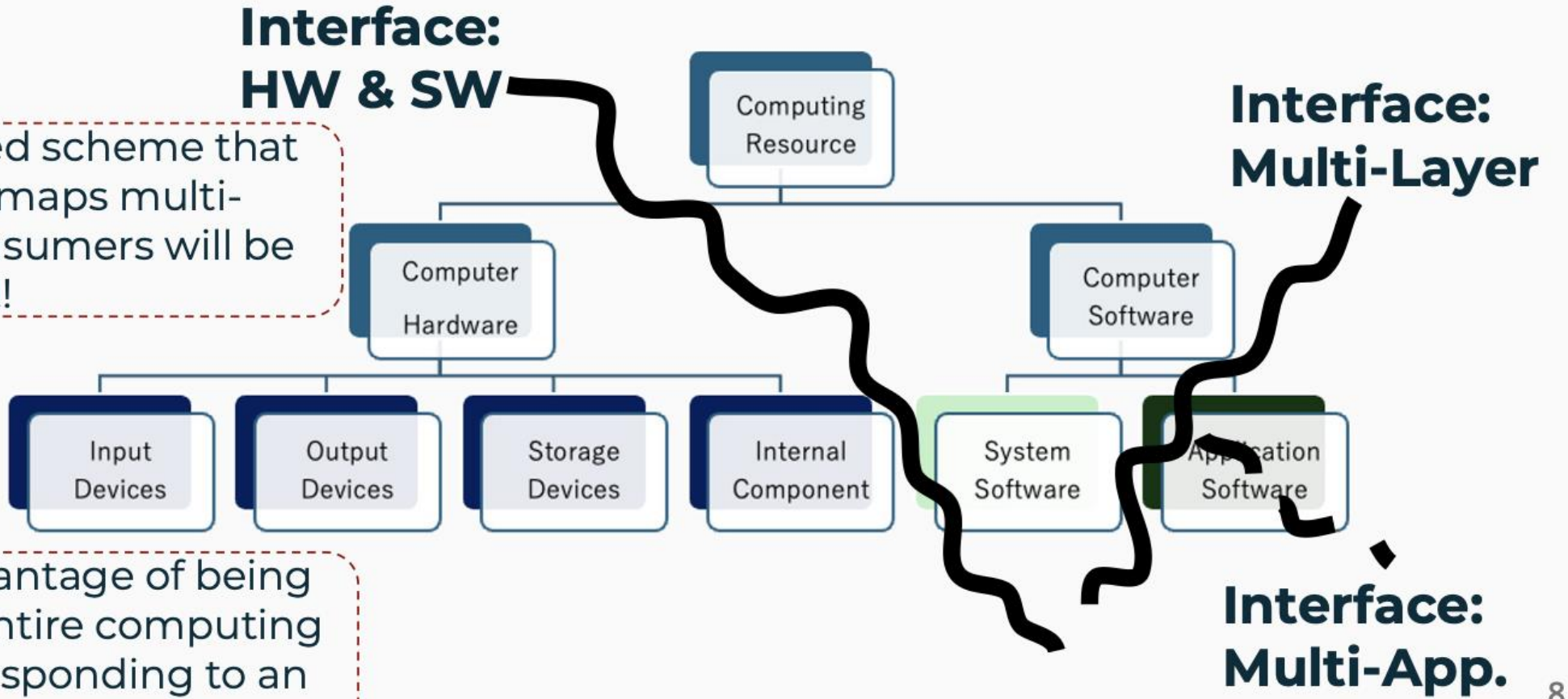
- How to comprehensively provide Supply Chain Security information for a computing resource (Software & Hardware)?

- To express the entire computing resource, isn't it necessary to combine types of statements?

Boundary of Responsibility for Stakeholders in Computing Resource

If there is an extended scheme that comprehensively maps multi-statements, end-consumers will be happy!!

There is also the advantage of being able to present the entire computing component when responding to an incident easily!!



Problem Statement: 3/3

- How to comprehensively provide Supply Chain Security information for a computing resource (Software & Hardware)?

- To express the entire computing resource, isn't it necessary to combine types of statements?

- Is it possible to map multi-statement supply chain security information?
  - E.g., Extended YANG/MUD-Based Schema to serve as adhesive for interface

Next Steps:

- Review and harden in relevant expert groups: SCITT, RATS, where else? Any non-IETF places like Linux Foundation?
- Then several possible routes forward:
  - Make a SCITT profile, or use SCITT building blocks in a different WG?
  - Make new individual scheme I-D to cover use-case I-D
  - YANG/MUD-Based format exploration

Feedback＆Next Action

- フィードバック
  - SCITT Chapter#2を発行すべきかどうか
    - セキュアなハードウェアを使用することと、ハードウェアがセキュアであるという証言は、同値と扱えるか、それとも異なるものと扱うべき事柄か
  - コンセンサスを確認するには、SCITT WGだけで十分かどうか
    - Hankが誰を呼ぶべきか、SCITTの現Spec.を策定するためにスコープを切る過程で離れた人、彼らを呼び戻す必要性を考えるべき
    - SCITT Arch. & APIのRFC化とは独立で別途考えるべき

- Next Actions
  - ~~地道にuse-caseを貯めていき、コンセンサスを取りやすくする~~
  - 逆に、Root of Trustの検証に絞り込み、ボトムアップ的に進める
    - YANG/MUDのデータモデルの改良しては、対応するuse-caseを増やす
    - コンセンサスの取りやすいuse-caseをHackathonのロビー活動で収集
    - draftのdocumentとしての品質を高める
    - いいタイミングのcut-offで提案して、コンセンサスを取る

コラム：IETF124の活動予定

Hackathon

- 作戦：SCITT WG meetingでは直接I/Dを扱わない
  - SCITT Arch. & APIのRFC化に最大限meeting時間を優先
  - Hackathon resultを通例で報告しているため、その時間を活用して、次何の作業しますか？に誘導していきたい
    - e.g., ソフトウェア+ハードウェア
      e.g., ソフトウェア+ソフトウェア

[4]

A YANG Data Model for Multi-Statements of SCITT

- **Champions**
  - Nobuo AOKI n_aoki@ieee.org
- **Member**
- **Project Info**

  We propose an extension for SCITT as an **A YANG Data Model for Multi-Statements** to provide integrated Supply Chain information for the computer system protection.
  During the hachathon, we will solicit additional adaptable use cases and explore flexible YANG models that complement area not coverd by exisitang Supply Chain Security specifications.
  However, we will take care **not to impact the ongoing RFC making work for the pioneering SCITT Architecture and SCITT SCRAPI**.
  Upon discovering the SCITT and RATS tables, attempt to join them to facilitate consensus-building discussions.
- **Hackathon Work Item**
  - Looking for SCITT tables in Hackathon room
  - uploading revised draft version 00 w/o ToDO
  - soliciting use-case
  - developing a prototyping YANG schemer

[4] https://wiki.ietf.org/en/meeting/124/hackathon

コラム：標準化関連活動をindividualへ

自己紹介 & 概要

- 氏名：青木信雄
- 所属：総合研究大学院大学 先端学術院先端学術専攻 情報学コース
- 関連活動：
  - IETF124 Montreal: R7情報通信分野の国際標準化会議 参加者募集（NRI, 個人）
  - IETF121 Dublin: R6情報通信分野における国際標準化動向調査者（NTTデータ経営研, 総研大）
    - テーマ名：透明性・説明責任の観点からのIoTを主軸とする情報通信技術の標準化動向調査
  - IETF118 Praha: IETF2023年度 IETF参加支援（JPNIC, 総研大）
  - IETF116 Yokohama: 2022年度 資料調査として旅費執行(KDDI財団, 広島市大)
- 調査対象機関：Internet Engineering Task Force (IETF) SCITT WG
- 対象技術：サプライチェーン・セキュリティ
- マドリード会合のオンライン活動
  - Individualな参加者として自費（参加登録料）
  - Regulation Consideration: 外為法[5]に留意する
    - 基本的にPublic Domainへ公知のものとしてから、標準化活動に引用して利用
    - キャッチオールに概要するものは, 公知の署名技術（e.g., COSE）を議論中では引用して利用

[5] https://laws.e-gov.go.jp/law/324AC0000000228/