ISO/IEC JTC 1/SC 27/WG 3 Zoom 会合報告

2021 年 XX 月 XX 日

報告者：SC27/WG3 国内参加者一同

1. 場所：Zoom

2. 開催日：2021 年 5 月 25 日（月）～28 日（水）

3. 出席者（参加登録者）：
カナダ、中国、ドイツ、スペイン、フランス、英国、韓国、マレーシア、ポーランド、米国、ルクセンブルク、インド、コスタリカ、南アフリカ、ロシア、イスラエル、スイス、オーストラリア、リトアニア、シンガポール、トルコ、インドネシア、デンマーク、ベルギー、日本（伊藤、山田、堀、濱口、坂根、谷澤、武岡、仲野、釼吉、半村、清本、甲斐（敬称略））、SC37、ISO/TC 22/SC 32、CCUF：計 137 名

4. 会合の概要
Convener はスペイン Miguel Bañón 、Convener support 兼 Secretariat は甲斐により議事が進行された。各プロジェクトの審議結果は、本議事録及び「WG 3 Recommendations, Virtual (via Zoom) April 12th - 15th, 2021 (WG3 N2087)」を参照の事。

5. リエゾン報告
5.1 CCDB
CCDB からは、今後 CC/CEM（ISO/IEC 15408/18045）の開発を SC27/WG3 へ移管する旨報告があった。しかしながら、CC 評価では CC/CEM の一部を評価レポートにコピペする必要があるが、そのような商用目的での無償引用は ISO の著作権により禁じられているため、早々にその問題を解決してほしいという要望もなされた。WG3 からは SC27 Plenary で問題提起し、早期解決に取り組む旨報告を返している。

5.2 CCUF
CCUF からも上記同様著作権上も問題点を指摘する声が寄せられた他、ISO/IEC 15408/18045 の出版の時期に関して問合せがあった。WG3 からは 2021 年内の出版を目指している旨報告を返している。

5.3 SC37
山田様、お願い出来ますでしょうか？

5.4 ITU-T FG-QIT4N/SG 17
リエゾンオフィサより WG3 に関連するプロジェクト(ISA-62443-2-3 Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment、IEC TS 62443-6-1 Security evaluation methodology for IEC 62443-2-4、IEC TS 62443-6-2 Security evaluation methodology for IEC 62443-4-2)の進捗状況に関する報告が為された。

5.5 ETSI ISG QKD
QKD 関連プロジェクトの進捗状況報告があったが、WG3 よりは 23837 のレビューを依頼するリエゾン文書を返している。

5.6 TC22/SC32/WG11
QKD 関連プロジェクトの進捗状況報告があったが、WG3 よりは 23837 のレビューを依頼するリエゾン文書を返している。

5.7 IEC/TC 65
CMUF(Cryptographic Module User Forum)から、19790 等の暗号モジュール試験関連の標準の改訂作業に貢献したいという理由から、WG3 へのリエゾン申請があった。しかしながら、申請を受理する前にまず ISO 側で CMUF の適格性を調べる必要があるため、その手続きを経た後リエゾン関係を締結し、19790 等の改訂作業に参加することになる。

5.8 CMUF
TCG は TPM 仕様の改訂作業を進めているが、TPM 仕様の ISO 版である ISO/IEC 11889:2015 の定期見直しも同時に進行している。TCG はその定期見直し審議結果も考慮しながら ISO/IEC 11889:2015 の改訂を進めたいとのことである。

6. WG3 Road Map
今回議論は無かった。

7. Project 15408: Evaluation criteria for IT security
Part1: Introduction and general model
Part2: Security functional components
Part3: Security assurance components
Part4: Framework for the specification of evaluation methods and activities
Part5: Pre-defined packages of security requirements
今回は FDIS 文書作成中のため editing session は無かった。改訂 15408 の出版は 2021 年内を目指しているが、改訂量が多く毎回の会議で 500、600 個のコメント審議をしていたため、文書として成熟しておらず表現上の問題（似たような記述が重複しているなど）が見受けられるため、改訂 15408 が出版後速やかにそれら問題を解決するため、PWI “Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045”を設立することで合意された。

8. Project 18045: Methodology for IT security evaluation
ISO/IEC 15408 と同様である。

9. Project 17825: Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
坂根様、お願い出来ますでしょうか？

10. Project 19790: Security requirements for cryptographic modules
坂根様、お願い出来ますでしょうか？

11. Project 20897-2: Physically unclonable functions Part2: Test and evaluation methods
堀様・濱口様、お願い出来ますでしょうか？

12. Project 22216: Introductory guidance on evaluation for IT security
本会議にて 1st DTR 投票結果が審議されたが、コメントが一つのみであったため殆ど議論はない。出版されることで合意された。

13. Project 23532-1: Requirements for the competence of IT security testing and evaluation laboratories - Part 1 Evaluation for ISO/IEC 15408
2nd DTS 審議後最終版が提出され TS として出版予定だったが、本 TS は適合性評価に関連する内容を含んでいるため、CASCO (Conformity AsseSsment COmmittee)からコメントが提出されていた（＊1）。会議前に CASCO とそれらコメントを審議した後 3rd DTS が作成され、現在 DTS 投票中である。

＊1）CASCO より、適合性評価を実施する機関（評価機関、試験機関、認証・認定機関等）の評価・認定プロセス（能力要件を含む）に関わる標準を開発する場合は、予め CASCO 側からの了

承を得る必要があるという指摘があり、今後 WG3 で関連する標準を開発する場合（PWI を設立する場合）、リエゾンオフィサ経由で CASCO に周知する必要がある。

14. Project 23532-2 Requirements for the competence of IT security testing and evaluation laboratories - Part 2 Testing for ISO/IEC 19790
同上。

15. Project 23837-1: Security requirements, test and evaluation methods for quantum key distribution - Part 1: Requirements
谷澤様・武岡様、お願い出来ますでしょうか？

16. Project 23837-2: Requirements for the competence of IT security testing and evaluation laboratories - Part 2 Test and evaluation methods
谷澤様・武岡様、お願い出来ますでしょうか？

17. Project 24485: Security properties, test and evaluation guidance for white box cryptography
会議中 3rd DTR 投票結果の審議が為され出版に進む事で合意されたが、その後 ISO 側から、TR は最新技術動向等を纏めた単なるレポートであり、その文中に ISO 標準と同様に requirements、recommendations、permissions（shall、should、may）を含んではいけない、タイトルに guide や guidance を含んではいけない（guide や guidance は recommendation(should) のみを含む文書のタイトルのみ使用可能だが、TR は recommendation を含んではいけないため、タイトルに guide や guidance を含んではいけない)、という指摘があり、現在対応中である（過去は許容されていたが、最近は ISO directive part2 に準拠する傾向が強まっている）。

18. Project 24759: Test requirements for cryptographic modules
坂根様、お願い出来ますでしょうか？

19. Project 29128-1: Verification of cryptographic protocol- Part1:Framework
29128 自体の議論は殆どコメントが無いこともあり、1st DIS に進む事で合意された。しかし、15408 評価に適する形で文書が取り纏められていないため、新たに Part 2（最新研究結果や best practice 等を元にした暗号プロトコル仕様自体の評価アクティビティを ISO/IEC 15408-4 に従い纏めたもの）、Part 3（暗号プロトコル仕様に従い正しく実装されていることを確認する評価アクティビティ）の開発を開始することで合意され、会議後に NWIP 投票に掛けられる。

20. Project 5891: A General Framework for Runtime Hardware Security Assessment
仲野様、お願い出来ますでしょうか？

21. Project 5895: Multi-Party Coordinated Vulnerability Disclosure and Handling
伊藤様、お願い出来ますでしょうか？

22. Project 9569: Towards creating an extension for patch management for ISO/IEC 15408 and ISO/IEC 18045

23. PWI 5896: Cybersecurity assurance of complex systems based on ISO/IEC 15408
SoS(System of System)等複雑なシステムのセキュリティ保証を検討するPWIだが、議論に参加していないため内容は不明。

24. PWI 5908: ISO/IEC 15408 in the cloud
クラウド環境ではIT製品が多数使用されているが、それらの製品は定期的に保守（パッチ提供等）されるため、スナップショット評価である現在のISO/IEC 15408評価では、セキュリティ評価の実施が難しいとの問題意識から、本PWIが立ち上がっている。ただ今回殆ど議論は無かった

（CCUFでも同様のWGを立ち上げ、サポート文書（評価アクティビティを取り纏めたもの）の開発を目指しているとのことである）。

25. PWI 7677: Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045

26. PWI 19792 Revision of ISO/IEC 19792:2009 Security evaluation of biometrics
山田様、お願い出来ますでしょうか？

27. PWI 7680: Requirements for the competence of IT security conformance assessment body personnel

28. NP 29128-2: Verification of Cryptographic Protocols - Part 2: Evaluation Methods and Activities for Cryptographic Protocols

29. NP 29128-3: Verification of Cryptographic Protocols - Part 3: Evaluation Methods and Activities for Protocol Implementation Verification

30. PWI 5888: Evaluation criteria for connected vehicle information security based on ISO/IEC 15408
会議前に中国エキスパート等と協力し、今までの議論を踏まえNWIPを作成した。NWIPのスコープは、車載gateway等特に重要度の高いコンポーネントのセキュリティ要件や評価アクティビティを15408に従い定義する事である。事前にそのNWIPをSC32/WG11に提出し意見を求めたが、WG11議長より異論が出たためNWIPの修正を経て、NWIP投票に進む事で合意された。

31. Maintenance
寄書募集に対して、日本から機器の消費電力を観測することで不正な振る舞いを検知する技術に関する寄書が提出され、関係する部分を取り込むことが報告された。また、TR のドラフト版が提出され、概要に関して報告がなされた。これまでの議論の結果を踏まえ、ハードウェアの安全性を評価する手法とモニタリング回路の認証スキームが主な内容としてドラフトに記載されている。調査・検討が完了したことから、PWI を終了し、1st DTR 投票に進むことで合意された。

32. AOB: ISO/IEC 19790 Conference
複数の製品開発者や関係者間における情報流通手法である Multi-Party CVD に関する本件については、会合期間中 4/12(UTC)に WD へのコメント寄稿者とのミーティングが開催された。コメントの内容は主にエディトリアルな物であり、内容に関する大きな反対意見はなく、コメント寄稿者との合意形成が行われた。その後 4/13(UTC)の Plenary meeting にて、本件主エディタである米国の Josh Dembling 氏より活動状況(WD 作成、コメント寄稿者との合意形成状況等)について発表され、本件を 1st DTR Ballot に進める(2021 年 7 月までに 1st DTR を提出、その後 1st DTR ballot を開始、2022 年 10 月の SC27 WG3 Meeting に投票結果やコメントの結果発表、またそれら結果について 10 月のミーティングで議論する)旨提案され、反対意見はなく、承認された。

33. AOB: NP Remote biometric identification systems
山田様、ご存じでしたらお願い出来ますでしょうか？

34. 次回以降の WG 会合の予定
2021 年 10 月 25 日～28 日　　Zoom
2022 年 4 月 4 日～7 日　　Zoom
2022 年 10 月　　ハイブリット（ルクセンブルク）
2023 年 4 月　　USA

35. アクションアイテム

プロジェクト	タイトル	検討文書	配布(予定)日	コメント/投票締切日
17825	Testing methods for the mitigation of noninvasive attack classes against cryptographic modules	WG3 N2085 2nd WD	2021-07-29	2021-09-17
18045	Methodology for IT security evaluation	WG3 NXXXX 1st FDIS	2021-XX-XX	TBD
19790	Security requirements for cryptographic modules	WG3 N2057 2nd WD	2021-07-29	2021-09-17
23837-1	Security requirements, test and evaluation methods for quantum key distribution - Part 1: Requirements	WG3 N2060 2nd CD	2021-07-29	TBD
23837-2	Security requirements, test and evaluation methods for quantum key distribution - Part 2: Test and evaluation methods	WG3 N2061 2nd CD	2021-07-29	TBD
24759	Test requirements for cryptographic modules	WG3 N2063 2nd WD	2021-07-29	2021-09-17
29128	Verification of cryptographic protocols	WG3 N2065 1st DIS	2021-07-09	TBD
TR	Towards Creating an Extension for Patch Management for ISO/IEC 15408 and ISO/IEC 18045	WG3 N2066	2021-07-29	2021-09-17
TR	Multi-Party Coordinated Vulnerability Disclosure and Handling	WG3 N2067 1st DTR	2021-07-29	TBD
TR	A General Framework for Runtime Hardware Security Assessment	WG3 N2068 1st DTR	2021-07-29	TBD
PWI	Cybersecurity assurance of complex systems based on ISO/IEC 15408	WG3 N2054	提出済	2021-09-10
PWI	ISO/IEC 15408 in the cloud	WG3 N2055	提出済	2021-09-10
PWI	Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045	WG3 N2083	提出済	2021-09-10

PWI	Revision of ISO/IEC 19792:2009 Security evaluation of biometrics	WG3 N2053	提出済	2021-09-10
PWI	Requirements for the competence of IT security conformance assessment body personnel	WG3 N2084	提出済	2021-09-10
23837	Call for contributions on the definition of the term “information theoretic security”	WG3 N2056	提出済	2021-06-15

以上