

解説

セキュリティ評価基準 コモンクライテリアが変わる —ベンダもユーザも乗り遅れるな!—

金子 朋子^{†1} 村田 松寿^{†2}

^{†1} (株) NTT データ ^{†2} (独) 情報処理推進機構

筆者らは、情報技術セキュリティの評価基準である Common Criteria (CC) に関して、評価機関、ベンダ、研究者が集まる国際会議に出席した。同会議において 2014 年 9 月 8 日付で、本評価基準に基づく評価結果を相互に承認する国際的なアレンジメントである CC 承認アレンジメントの改訂版発効が発表された。新しいアレンジメントに基づき、今後 CC 承認アレンジメント (CCRA) 加盟各国が製品ベンダや評価機関、研究者と協力し技術分野ごとに共通の PP (cPP: Collaborative PP) を開発するとともに、加盟各国の政府調達での cPP 活用を促進することが新たに宣言された。本稿では、CC について、① CC とは何か? ② CC における認証制度はどのようになっているのか? ③ 本会議で発表された cPP 活用により、国際社会における CC はどのように変わっていくと想定できるのかについて、所見を述べたい。

1. はじめに

コモンクライテリアって何の評価基準? → IT セキュリティ評価基準

IT 製品・システムの安全性を保証することは難しい。利用者は当然、安全に IT 製品・システムを利用できることを望む。安全な IT 製品・システムの安全機能はセキュリティ機能と呼ばれ、個人情報や機密情報を窃取されたり、システムの稼働を妨害されたりすることがないように管理する機能である。セキュリティ機能には①動作しないことはない②不当な干渉をうけることはない③動作不能に陥ることはないことが要求される [1]。

一般の IT 機能であれば、利用者はその機能について、実際に利用してみることで保証されていることを確認できる。セキュリティ機能については、不測の事態を発生させてセキュリティ機能が正確かつ有効に動くことを確認することが必要だが、これは利用者には非常に困難である。そのため、開発者側で、IT 製品・システムの安全性を確認しなければならない。

セキュリティ機能が間違いなく動作することの確からしさを「セキュリティ保証」と呼ぶ。このセキュリティ保証を確認するのが、「IT セキュリティ評価」である。この「IT セキュリティ評価」のための確認手法は ISO

規格として、国際規格になっている。この国際規格の IT セキュリティ評価基準が CC (Common Criteria : ISO/IEC 15408) である [2], [3]。

また国家レベルで、第三者による確認の制度と確認結果を国際的に認め合う相互承認制度も確立されている。

2. CC とは

2.1 CC の成り立ちの経緯・歴史

1980 年以前は欧米各国の軍用システムはセキュリティ要件の厳しい特注仕様による調達のみであった。その後、PC や LAN の登場等、デジタル処理や通信技術の急速な進歩に伴い、軍用システムにおいても民生 IT 製品を活用するため、1983 年に米国にて TCSEC (Trusted Computer Security Evaluation Criteria : 通称オレンジブック) が制定され、これに適用する製品が調達されるようになった。欧州の各国の評価基準も 1991 年より欧州共通基準である ITSEC (Information Technology Security Evaluation Criteria) ベースに移行していたが、さらに米国の TCSEC と欧州の ITSEC を共通化する目的で 1996 年 Common Criteria v1.0 が制定された。

CC は、欧米 6 カ国により、1996 年に開発され、1999 年に ISO/IEC 15408 が規格化され、2000 年に欧米 13 カ国による CCRA が創設された。日本は 2001 年に IT セキュリティ評価および認証制度 (JISEC) を開始し、2003 年に CCRA に加盟した。2005 年に第三者による評価方法

を定めた「ITセキュリティ評価のための共通方法 (CEM: Common Evaluation Methodology)」がISO/IEC 18045として規格化された。現在は2012年9月に公開されたCC v3.1改訂第4版, CEM v3.1改訂第4版がIT製品に対するセキュリティ評価のための基準・評価方法として、広く利用されている (図1を参照)。

2.2 CCの概要

ITセキュリティ評価の国際規格であるCCは開発者が主張するセキュリティ保証の信頼性に関する評価の枠組みを規定したものである。

CCは、3分冊になっており、パート1には評価対象 (TOE: Target of Evaluation) 製品・システムのコンセプト (概念) および一般モデル、セキュリティ目標 (ST: Security Target) やプロテクションプロファイル (PP: Protection Profile) に記載すべき内容が規定されている (図2)。

ST (セキュリティターゲット) は、ITセキュリティ評価を行う評価対象に関するセキュリティ仕様と、ど

- 1983. 米国 TCSEC 制定 (商用への適用の広がり)
- 1991.6. 英独仏蘭: 各国評価基準から、ITSECとして統合し、v1.2を公開
- 1996. 米英仏独加蘭: Common Criteria v1.0 (TCSECとITSECを統合)
- 1999.6. ISO/IEC 15408: 1999として国際規格 (IS) として承認 (=CCv2.1)
- 2000.5. CCRA 創設
- 2001.4. 日本: ITセキュリティ評価および認証制度 (JISEC) を開始 (認証機関: NITE)
- 2003.10. 日本: CCRAにCAP (認証国) として加盟
- 2005. ISO/IEC 15408: 2005 発行 (CCv2.3), ISO/IEC 18045: 2005 発行 (CEM v2.3)
- 2012.9. CCRA: CC v3.1 r4/CEM v3.1 r4 リリース
- 2014.9. CCRA: 新 CCRA への署名が完了し、発効する

図1 ISO/IEC 15408 関連の年表

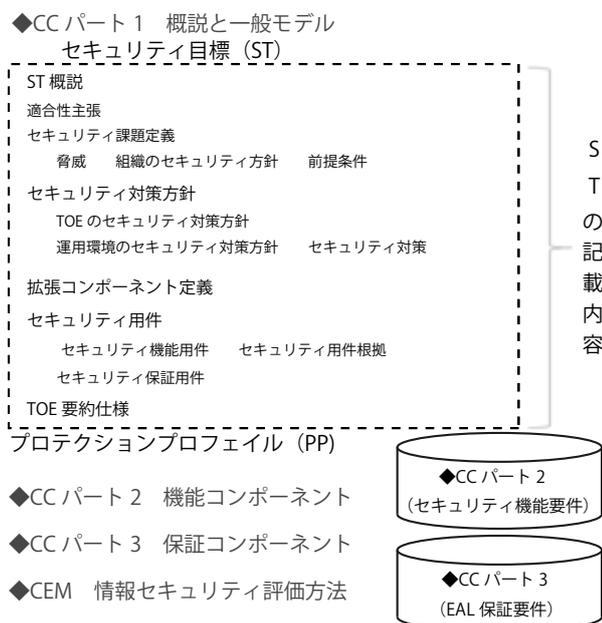


図2 CC構成とSTの記載内容

の程度の評価を行うかについて、CCに基づいて記述したIT製品に関するセキュリティ仕様書である。STでは、保護資産とそれに対する脅威等のセキュリティ課題を洗い出し、セキュリティ課題への対策方針を決定し、対策方針を満たすセキュリティ機能要件を記述する (図3)。STにより、利用者・開発者は、対象製品・システムが適切性すなわち「情報資産を守るために必要十分な機能をもっているか」を確認できる。

STは個別の対象製品・システムに対する文書であるが、それに対してPP (プロテクションプロファイル) とは、主に対象製品分野ごと、または技術分野ごとに、必要なセキュリティ要件を記述したもので、STのひな型としての位置付けにある。ITセキュリティ評価を受ける製品は、STにおいて関連するPPへの適合主張を行い、必要なセキュリティ要件が満たされていることを第三者によって確認される。

なお、CCのセキュリティ要求仕様を決定していく手順は認証取得を必要としない各種情報システムにおいてもセキュリティ要求分析に利用可能な規定になっている。

CCのパート2ではTOEのセキュリティ機能要件 (SFR: Security Functional Requirement) が規定されている。IT製品のセキュリティ機能を細かいコンポーネント (セキュリティ機能の部品) としてSTに記述するための文法 (SYNTAX) についてのリファレンスブックとして、機能要件がカタログ的に列挙されている。このカタログ化されたセキュリティ機能要件こそが、セキュリティ機能の必要十分性を評価するために欠かせないものである。実際のセキュリティ機能要件の利用方法としてはパラメタやリストを特定することにより、準形式的な記載ができる。

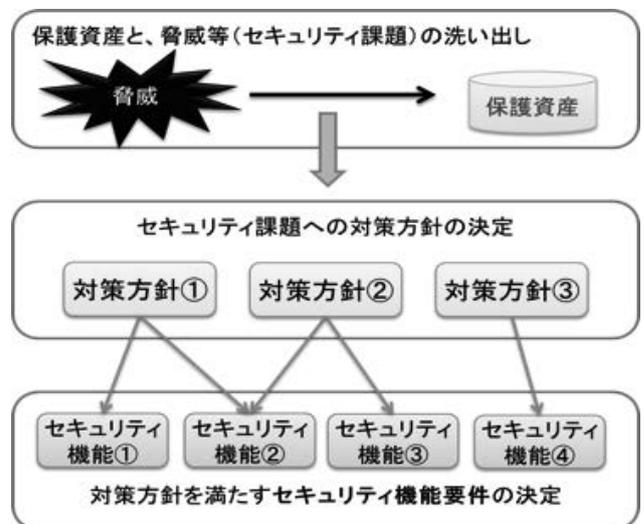


図3 STのセキュリティ機能への論理展開

CCのパート3にはセキュリティ保証要件 (SAR: Security Assurance Requirement) が規定されている。定義された機能要件の正確性を「どの範囲まで評価して保証するのか」、「どこまで詳細に評価するのか」を規定する評価保証パッケージとして評価保証レベル (EAL: Evaluation Assurance Level) が図4のように規定されている。評価保証レベルはセキュリティ機能の保証の度合いを示す。

どの範囲まで評価して保証するのかという点では、図5に示すようにライフサイクル全体として評価に必要な証拠資料や開発者への要求事項、評価者のアクション等が保証クラスごとに規定されており、脆弱性を生み出さない仕組みがライフサイクル全般にわたって作られているかが確認される。

3. CC 認証制度

3.1 認証制度 (国内外)

2000年5月に、欧米13カ国が認証製品を相互に承認

保証範囲		CCRA における相互承認の対象
EAL1	機能仕様 (外部 IF), 利用者ガイダンス等	
EAL2	内部設計, 配布手続き, 開発者テスト, 開発資料からの脆弱性分析等	
EAL3	開発現場のセキュリティ, 開発者テストの深さ (詳細度) 分析等	
EAL4	ソースコード, 開発環境 (ツール) 等	
EAL5	準形式的 (フローチャート等の図式を用いた曖昧ではない) 設計資料等	
EAL6, 7	各国の制度による (軍需品など特別な用途のため)	評価方法の規定 (CEM)

図4 評価保証レベル (EAL)

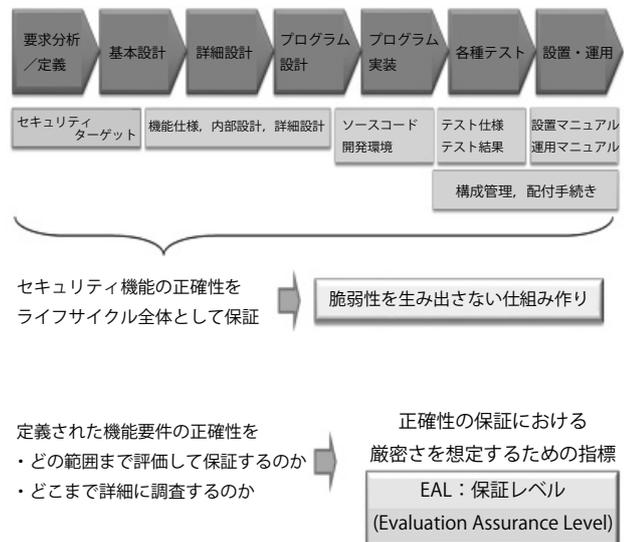


図5 ライフサイクル全体としての保証

するためのアレンジメント (CCRA: Common Criteria Recognition Arrangement) に合意して、主に国家安全保障に関連する市販のIT製品の政府調達のために活用が開始された。現在、26カ国が加盟しており、日本は2003年10月に認証書生成国として加盟した。中国、ロシアは、他国の評価結果を承認することに合意せず、自国制度に基づく評価を義務付けている (図6)。

日本では「ISO/IEC 15408 (JIS X5070): 情報セキュリティの評価基準」に基づくITセキュリティ認証制度が2001年に創設された。制度の目的は「市販のIT製品」を政府機関で安全に活用することである。2004年より (独) 情報処理推進機構 (IPA) が本制度を認証機関として運営している。

3.2 評価方法

ITセキュリティ評価は、CEMに基づき行われる。CEMは、さまざまな製品分野において共通的に適用で



図6 CCRA 加盟国

きるように評価方法が抽象的な表現で記述されている。そのため、評価の対象となる製品それぞれに当てはめた場合には、製品分野ごとの具体的なテストの考案は、評価者の能力に依存する部分がある。

スマートカードやICチップの評価においては、具体的なテスト方法・攻撃手法などの情報がサポート文書として策定され、評価時の必須技術文書として定められており、その他の技術分野においても今後策定が進んでいく。このような状況の中で、CC/CEMは具体的な評価手法の策定に伴い、評価のためのツールボックスとして、必要に応じて追加修正を加えメンテナンスしていくことになった。

3.3 評価実績

評価認証の実績は、製品ベンダの意向にしたがい、各国の認証機関のWebページに公開される。STおよび認証報告書の公開を条件として、CCRA認証マークが付与され、相互承認の対象となる。

国内での認証実績は、2014年10月末までに442件で、コピー・プリンタ・スキャナ等の複合機およびそのファームウェア等が約7割を占め、以下アクセス制御・データ保護関連が10%、データベース、スマートカード・ICチップ関連、ファイアウォール、特定アプリケーションと続く。デジタル複合機については、ほぼ100%がPP適合となっている。

海外では、表1に示すように公開されているITセキュリティ評価・認証の累計件数[4]は、2014年10月時点で2,470件を超えている。ただし、欧州では、全体の約半数程度が非公開となっており、さらに1,000件以上の実績がある。

欧州では、スマートカード・ICチップ評価が非常に多く実施されている。Eパスポート、ヘルスケアカード、Javaカード等がある。

現在、CCRAでは調達の対象となる認証製品について、認証書の有効性について3年ないし2年間という期限を設け、その期限内に脆弱性分析に関して再評価を行ったもののみを調達対象と認め、新たに認証書を発行する方向で各国の調整を図っている。

3.4 CCのメリット

IT製品を調達する際にCCの仕組みを活用するメリットとしては、調達側と供給側で別々のメリットがある。調達者が必要とするセキュリティ要件が、PP（もしくはST）に含まれていれば、そのPPに適合していること

を調達要件とすることで、評価機関が客観的に評価した信頼できる製品を調達できるというメリットがある。一方、ベンダ側としては、複数の国・政府機関から認証取得を要求されたとしても、CCRA加盟国において一度認証を取得すれば、他のCCRA加盟国においてもその認証は承認されるため、複数回評価・認証を受けるコストや期間を削減できるメリットがある。

中小企業やベンチャー企業であっても、ITセキュリティ評価を受けた認証製品であれば、国際的に認められたセキュリティ製品であることを大企業や政府の調達担当者に理解を得られやすく、新規の販路開拓が可能になり事業発展に寄与することができるなどメリットがある。

さらに、中小企業投資促進税制[5]においては、中小企業の情報システムのセキュリティ向上を狙って、オペレーティングシステム、仮想化ソフトウェア、データベース管理などの分野では、CC認証取得製品のみが税制優遇処置の対象になっており、CC認証取得はベンダ、ユーザ双方にとってビジネス上具体的なメリットをもたらしている。

CCにはセキュリティ要件として必要なものが含まれており、開発者が要件のチェックに利用することが可能であり、モバイルFeliCaのソフトウェア開発のように、品質確保のための活用がなされた事例も存在する[6]。また筆者の1人である金子らもCCの活用を意図して、

表1 CCRA 認証実績

カテゴリー	認証製品	アーカイブ製品	合計
アクセス制御	87	20	107
バイオメトリクス	3	0	3
境界保護 (FW)	125	55	180
データ保護	79	21	180
データベース	45	29	100
IDS/IPS	43	15	74
IC、スマートカード関連	778	13	58
鍵管理	36	10	791
デジタル複合機	223	87	310
ネットワーク関連	221	40	261
OS	106	37	143
デジタル署名	81	4	85
トラステッドコンピューティング	4	0	4
その他	230	78	308
合計	2,061	409	2,470

CCをアシュアランスケースと統合した開発方法論[7]を提案し、CC-Caseと名付けている。CCはセキュリティ業界における知見の集大成として、さまざまな利用が可能な評価基準である。

CCのメリットを①CCRAの仕組み、②CC認証取得、③評価基準活用のCCのメリットを調達者とベンダ別の観点で表2に示す。

4. CCの最新動向

4.1 制度改革の背景

これまで、日本では政府調達要件としてPPの作成が行われず、製品ベンダ主導で各社独自のSTに基づく評価・認証が行われてきた。このPP適合ではない独自STによる評価では自由な記述が可能である一方、STの内容が適切であるかどうかの文書審査に時間がかかる点や不適切なセキュリティ課題定義であると、評価が無意味となる点のデメリットが指摘されてきた。調達者にとって、適切なセキュリティ機能について評価されない独自STによる評価が行われたり、評価期間が長期間かかることでタイムリーな調達がしづらくなっていた。

一方、海外では、各国政府がそれぞれ独自のPPを作成し、複数のPPが乱立したため、少しずつ異なるPPのために製品ベンダはPPごとに複数の評価・認証が求められる事態となった。さらに、評価保証レベルEAL4（ソースコード、回路図まで確認するレベル）での評価にはおおむね18カ月という長期間がかかることになり、タイムリーな調達ができなくなっていた。

表2 CCのメリット

① CCRAの仕組みのメリット	
調達者	<ul style="list-style-type: none"> セキュリティ機能製品比較可能 評価結果を信頼できる プロテクションプロファイルを調達時の要件として活用可能
ベンダ	<ul style="list-style-type: none"> CCRA加盟国ではその国で認証を受けたものと同等に扱われる 調達者の信頼を得ることができる 認証製品は各国の調達対象となる
② CC認証取得のビジネス上のメリット	
ベンダ	<ul style="list-style-type: none"> 新規の販路開拓が可能になり事業発展に寄与 国内での認証が海外でもそのまま認証製品として通用するため、グローバルな市場に対応可能（ただし国際的にはプロテクションプロファイルへの適合が必要）
③ 評価基準活用による開発上のメリット	
ベンダ	<ul style="list-style-type: none"> ITセキュリティ評価のための共通言語であるCCに基づいて記述することでセキュリティ製品やセキュリティ機能の仕様が明確になり、比較可能 CCRAにおいて、CCのメンテナンスが継続して行われており、今後もITセキュリティ評価の基準として活用可能

また暗号評価が不十分なために、脆弱性が顕在化する可能性があり、乱数生成や暗号プロトコルなど評価に必要なセキュリティ機能がCCに定義されていなかった。

さらに製品分野に対応したPPごとに求められるセキュリティレベルにバラツキがあり、別な製品の脆弱性により、同一ネットワークに潜在的な脆弱性が残存した。そこでネットワーク製品に共通するセキュリティ機能をネットワーク基盤PPとして定めることでレベルの統一を図る必要が生じた。こういう事態になったことで、ベンダ側からスムーズにタイムリーな調達をし、コスト削減したいという要望が強くなされ、CC認証制度は改革の必要にせまられた。これまでのITセキュリティ評価における問題を解決するために、各国政府ならびに最新技術の知見を持つ製品ベンダの技術者、評価機関が協力して、各技術分野にひとつのPPをcPP (collaborative Protection Profile) として開発し、CCRA加盟国が政府調達において最大限に活用することに2012年9月に合意した。それと同時に、CCRAの公式サイト[8]にMC Vision Statement [9]として発表された。

4.2 ICCC 2014 への参加と海外におけるcPP活用促進

筆者らは、2014年9月9日から11日にインド／ニューデリーで開催された「第15回 国際コモンクライテリア会議ICCC 2014」に参加した。2013年9月16日に、インドが18カ国目の認証書生成国（CAP）として承認されて、今回のICCCの開催国となり、3日間の日程でICCCが開催された。参加者は、約250名であった。CCRA MC (Management Committee：運営委員会) 議長のDag Ströman氏より、CCRA新アレンジメントの発効と今後の運営について、CCRA CCDB (Common Criteria Development Board：CC開発委員会) 議長のDavid Martin氏よりCCDBおよびcPP開発の最新情報についての報告があった。

その後、3つのトラック（1. CCのビジネス上の価値、2. CC技術、3. CCの方向性）に分かれ、54件の発表があり、筆者の1人である村田はトラック1で「Scheme Update of Japan（日本の認証実績・政府調達での活用に向けた取り組み等の最新状況）」について話し、筆者の1人である金子はトラック2で研究テーマである「コモンクライテリアに基づいたセキュリティ分析と保証の統合手法CC-Case」について話した[10]。

ICCC 2014に先立って開催されたITセキュリティ評価・認証に関する国際承認アレンジメントCCRA会合

では、2014年9月8日にこのステートメントに基づきCCRA新アレンジメントへCCRA全加盟国26カ国が署名を完了し、このcPPへの適合評価およびそれ以外のITセキュリティ評価についてはEAL2までをCCRAでの相互承認の適用範囲とすることになった。従来のPPとcPPの違いを表3に示す。

cPPはテスト重視であり、実際のセキュリティを保った上でタイムリーな調達が可能になる。すでにこの取り組みに先行する米国では、ITセキュリティ評価を90日以内に完了する目標を達成しつつある。

STによる文書審査中心の評価→cPPまたはPPに適合するための技術分野ごとのテストや脆弱性分析中心の評価に移行

4.3 国内：経産省の調達とセキュリティ要件

日本での政府調達におけるIT製品の調達方針は、「政府機関のセキュリティ対策のための統一基準」（政府セキュリティ政策会議決定）の中で定められている。平成26年度版の統一基準では、IT製品を調達する際には「IT製品の調達のためのセキュリティ要件リスト」（経済産業省策定）を参照し、利用環境における脅威を分析した上で、当該機器等に存在する情報セキュリティ上の脅威に対抗するためのセキュリティ要件を策定することが求められている。

「IT製品の調達のためのセキュリティ要件リスト」には、各製品分野ごとにセキュリティ上の脅威と脅威に対抗するためのセキュリティ要件としてPPが記載されており、PPに適合した評価済みの製品の調達が推奨され

表3 従来のPPとcPPの違い

対象範囲	PP 製品分野	cPP 技術分野
作成者	調達者（政府機関・認証機関）	国際的テクニカルコミュニティ（製品ベンダ、調達者、評価者、認証者）
評価保証レベル	EAL3～4	原則 EAL1～EAL2
評価期間	18カ月～	6カ月以下（米国は90日以下を目標に推進中）
評価品質	評価者の能力に強く依存（評価機関・国によるバラツキ）	具体的なテスト、評価手法をサポート文書として規定することで、必要な品質を確保
暗号評価	CC/CEMに詳細な規定なし	サポート文書に詳細なテスト方法を記載。将来的にCC/CEMに盛り込む計画

ている。本リストでは現在日本国内で実績のあるデジタル複合機、ファイアウォール、IDS/IPS、OS（サーバーOS）、データベース管理システム、スマートカード（ICカード）の6分野になっている。今後順次拡充を目指しており、USBメモリが候補となっている。これにより、調達者・利用者はセキュリティ知識がなくても、セキュリティ要件リストを基に製品の調達・購入が可能となる。

5. 今後の課題

現在、欧米の製品ベンダが中心となって、cPP開発の主導権を取っているが、デジタル複合機（MFP）の分野においては、日本の製品ベンダが10社以上集まり、米国の製品ベンダとともに日米主導のMFP PPを開発している。

モバイルデバイス（スマートフォンをはじめ、その他の製品分野においてもグローバルな市場における主導権を日本が取るためには、cPP開発の母体となるテクニカルコミュニティに多くの日本ベンダの開発者の方の参画が必要となっている。

また、これまで日本で行われてきた製品ベンダ独自のSTによる文書審査中心の評価・認証が、今後はcPPまたはPPに適合するため技術分野ごとに定められたテストおよび侵入テストをはじめとする脆弱性分析を中心としたセキュリティ評価に移行する。特に、CVE等の脆弱性データベースを探索し、欠陥仮定法を活用した攻撃手法により、重大な脆弱性がないこと・顕在化しないことを侵入テストによって確認する等の、安全なIT製品の政府調達に寄与していくための新たな仕組みづくりが重要な課題となってくる。

さらに今後は情報系システムの大規模なSI現場において利用可能なPPも含め、PPの利用促進が活発化していくことが期待される。また世界では多くの製品・システムにPPが存在する。またCCの業界での最近の動向では、これまでPPの開発は主としてセキュリティ製品の調達者である政府機関や認証機関が行ってきたが、現在、最新技術を持つ製品ベンダが業界ぐるみで連携して調達者や評価者、認証者と共同でcPPを実現しようとしている[7]。

6. おわりに

本稿を読んでいただいた皆様の中には、CCをまったく知らなかった方、国際規格としてのCCの概要は知っ

ていても CCRA は知らなかった方、CC も CCRA も知っているが近年の動向は知らなかった方と、いろいろな方がいらっしやと思う。

日本での CC は限られた分野のみで活用されているが、欧米においては、幅広い分野で PP が作成され活用されており、これらを基に今後国際的な統一基準 (cPP) として作成されていく流れになってきている。IT セキュリティ評価の実績のある IT 製品にかかわる開発者や政府調達要件にかかわるベンダだけでなく直接、関係ないと思っている方にも、今後は影響があるかもしれない。

3 年後、加盟国 26 カ国の相互承認は すべて共通の基準 (cPP) に基づいて 実施される！！

デジタル複合機以外のさまざまな分野において、グローバルな市場における最低限必要 (ベースライン) なセキュリティ機能の仕様が cPP として作成されていく中で、グローバルな市場での主導権を日本が取るために、変化していく CC の活用にもっと多くの開発者が目を向けてほしい。3 年後には多くの cPP が開発され各国の政府調達で活用されると予測されるが、確定してから行動を始めたのでは遅きに失する可能性が高いからである。グローバルな調達に向けて、現在、モバイルデバイスやタブレット等に関する cPP の作成については、一部のベンダを中心に検討も始まっているが、もっと多くの人に cPP の開発に参画してほしいと筆者らは考えている。自由に意見のいえるコミュニティ作りも一案であろう。調達者、開発者双方にとって必要となる cPP 適合評価に備えたアクションについては、表 4 にリストアップしている

また皆様のご意見・ご要望は以下の相談窓口 (IPA 技術本部 セキュリティセンター 情報セキュリティ認証室

表 4 従来の PP と cPP の違い

情報収集：CCUF へ参加し、情報収集 (現在、参加費無料)
1) Web およびメールリストによる情報共有 2) 年 3 回の Face To Face 会合 3) 電話会議等への参加
cPP 開発への参画：特定の技術分野に関する cPP の開発
1) 認証機関との連携 (cPP の提案) 2) 発足した iTC への参画 3) 海外 CCRA 加盟の政府機関との連携 (調達者のみ) 4) 国内外の業界各社との連携 (ベンダのみ)
cPP または PP に基づく調達の実施
調達要件に該当する cPP または PP を記載 (調達者のみ)

jisec@ipa.go.jp, Tel.03-5978-7538 担当:村田・真鍋・中村) にお寄せいただきたい。

国際的に cPP 活用促進に大きく舵が切られた新時代の CC について、日本からも多くの知見が集まり、納得できる cPP がさまざまな技術分野で作成されていくことを期待したい。

7. 謝辞

本稿を執筆するにあたり、多大な協力をいただいた共同推敲者の (株) 日立製作所 吉野松樹様、IPA 技術本部セキュリティセンター情報セキュリティ認証室の方々、その他関係各位に深く感謝の意を捧げます。

参考文献

- 1) 田淵治樹：国際規格による情報セキュリティの保証手法，日科技連 (2007).
- 2) Common Criteria for Information Technology Security Evaluation, <http://www.commoncriteriaportal.org/cc/>
- 3) セキュリティ評価基準 (CC/CEM), <http://www.ipa.go.jp/security/jisec/cc/index.html>
- 4) CCRA 認証実績. <http://www.commoncriteriaportal.org/products/stats/>
- 5) 中小企業投資促進税制における認証製品リストの公開, https://www.ipa.go.jp/security/tax/zeisei_list.html
- 6) 栗田太郎：モバイル FeliCa のソフトウェア開発における品質確保のための構造と実践～抽象度の制御やコミュニケーションの活性化に向けて～，情報処理学会デジタルプラクティス，Vol.1, No.3, pp.148-157 (2010).
- 7) 金子朋子，山本修一郎，田中英彦：CC-Case—コモンクライテリア準拠のアシュアランスケースによるセキュリティ要求分析・保証の統合手法，情報処理学会論文誌 (ジャーナル，Vol.55, No.9 (2014).
- 8) CCRA の公式サイト，<http://www.commoncriteriaportal.org>
- 9) CC 及び CCRA の適用についての今後の方向性に関するビジョンステートメント，http://www.ipa.go.jp/security/jisec/ccra/documents/vision_statement_J.pdf
- 10) 第 15 回 ICC 実行委員会 (インド STQC, CII) : 15th International Common Criteria Conference-Meeting the Technology Challenges, ISBN: 978-93-83842-70-4 (2014).

金子 朋子 (正会員) kanekotm@nttdata.co.jp
博士 (情報学)。 (株) NTT データ品質保証部所属。2013 年情報セキュリティ大学院大学博士後期課程修了。同大学院客員研究員。文部科学省認定プログラム・サーティフィケート取得者 (情報セキュリティスペシャリスト，ソフトウェアスペシャリスト)

村田 松寿 (非会員) mt-mura@ipa.go.jp
1980 年早大理工学部電気工学科卒。同年松下電送機器 (株) 入社。1985 年に世界初の MS-Windows 搭載製品、画像処理 LSI、S/MIME 搭載 IFAX、IPv6 関連の開発の後、2002 年よりパナソニックの製品セキュリティおよび ISMS ガバナンスを担当。2008 年 (独) 情報処理推進機構。2010 年より CCRA に日本の認証機関として参画，MFP TC 議長。

採録決定：2014 年 12 月 9 日
編集担当：吉野松樹 ((株) 日立製作所)