セキュリティ評価基準コモンクライテリアとその認証制度の動向

金子 朋子† 村田 松寿‡

† 株式会社 NTT データ ‡独立行政法人情報処理推進機構

135-8671 東京都江東区豊洲 3-3-9 〒113-6591 東京都文京区本駒込 2-28-8

kanekotm@nttdata.co.jp mt-mura@ipa.go.jp

あらまし 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/IEC15408）である．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．本稿では①CC とは何か？②CC における認証制度はどのようになっているのか？③cPP 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ことが想定できるのかについて，考察する．

The Common Criteria for Information Technology Security Evaluation (CC) and the Trend of its Recognition Arrangement (CCRA)

Kaneko Tomoko† Murata Matsutoshi‡
NTTDATA† INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN ‡

135-8671 3-3-9 Toyosu koutou-ku Tokyo 113-6591 2-28-8 Honkomagome, Bunkyo-ku, Tokyo

kanekotm@nttdata.co.jp mt-mura@ipa.go.jp

Abstract

The probability that the security functionality operates correctly is called "Security Assurance". “ Information Technology Security Evaluation” ensures "Security Assurance". Common Criteria for “IT Security Evaluation” is standardized as the International Standard by the ISO. This International Standard of “IT Security Evaluation” is called as the CC（Common Criteria：ISO/IEC15408）. Also the mutual recognition arrangement was established globally to recognize the evaluation results by the testing labs as a third party. In this paper, we will discuss 3 aspects, such as 1.What is CC? ; 2. What is the certification schemes?; 3. What is the advantages for deployment of evaluated IT products against cPPs based on the CC in the global community in the near future?

0. はじめに

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/IEC15408）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．

1. CC とは

1.1　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 か国により，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 か国による 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/IEC18045 として規格化された．現在は 2012 年 9 月に公開された CCv3.1 改訂第 4 版，CEMv3.1 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．）

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（=CC v2.1）
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/IEC15408:2005 発行(CC v2.3), ISO/IEC18045:2005 発行(CEM v2.3)
2012. 9.　CCRA : CCv3.1r4／CEMv3.1r4 リリース
2014. 9.　CCRA : 新 CCRA への署名が完了し，発効する

図 1.　ISO/IEC15408 関連の年表

1.2　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）及び一般モデル，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，主に対象製品分野毎，又は技術分野毎に，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．

図 2　CC 構成と ST の記載内容

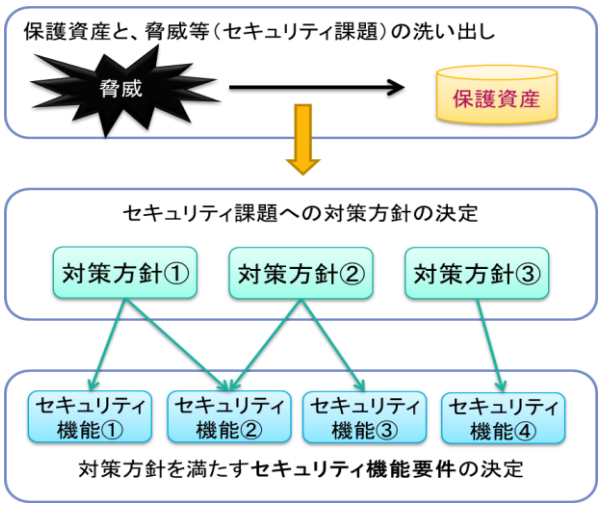

図 3.ST のセキュリティ機能への論理展開

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．

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亘って作られているかが確認される．

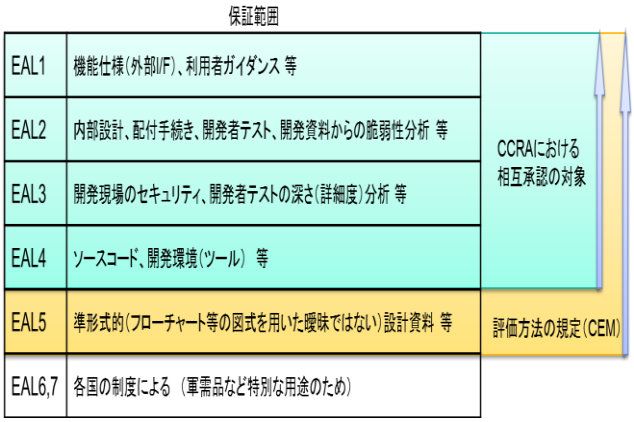

図 4. 評価保証レベル（EAL）

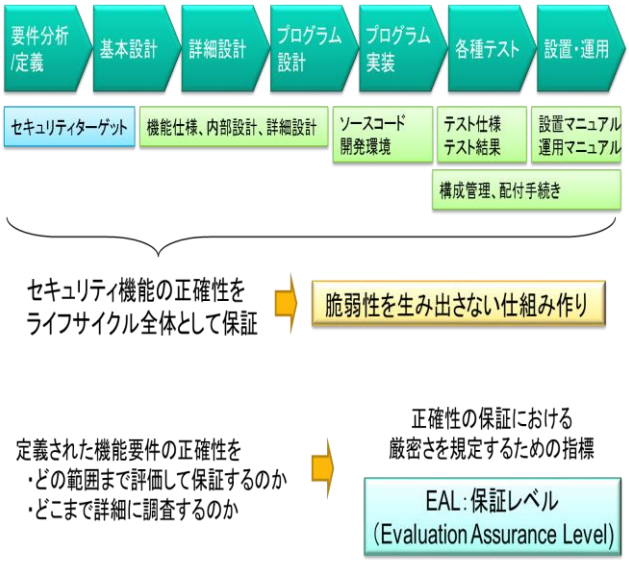

図 5. ライフサイクル全体としての保証

2. CC 認証制度

2.1 認証制度（国内外）

2000 年 5 月に，欧米 13 か国が認証製品を相互に承認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 か国が加盟しており，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．

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 年より独立行政法人情報処理推進機構（IPA）が本制度を認証機関として運営している．

図 6. CCRA 加盟国

2.2 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，製品分野毎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．

2.3 評価実績

評価認証の実績は，製品ベンダの意向に従い，各国の認証機関のウェブページに公開される．ST 及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、2015 年 3 月末までに 467 件で、コピー・プリンタ・スキャナ等の複合機及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，2015 年 8 月時点で 2700 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 1000 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．

表 1.CCRA 認証実績（2015 年 8 月時点）

カテゴリー	認証製品	アーカイブ製品	合計
アクセス制御	73	39	112
バイオメトリクス	3	0	3
境界保護（FW）	110	80	190
データ保護	65	47	112
データベース	30	45	75
IDS/IPS	21	41	62
IC，スマートカード関連	851	14	865
鍵管理	30	18	48
デジタル複合機	128	107	235
ネットワーク関連	214	93	307
OS	104	47	151
デジタル署名	85	5	90
トラステッドコンピューティング	6	0	6
その他	284	165	449
合計	2004	701	2705

2.4 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．

更に，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]．また筆者の一人である金子らも CC の活用を意図して，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，様々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．

表 2. CC のメリット

①CCRA の仕組みのメリット

調達者	・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	・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

②CC 認証取得のビジネス上のメリット

ベンダ	・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	・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

3. CC の最新動向

3.1 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 毎に複数の評価・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 か月という長期間かかることになり，タイムリーな調達ができなくなっていた．

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，各国政府並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．

3.2 ICCC2014 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 ICCC2014」に参加した．2013 年 9 月 16 日に，インドが 18 か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 及び 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，筆者の一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組み等の最新状況）」について話し，筆者の一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].

表 3. 従来の PP と cPP の違い

	PP	cPP
対象範囲	製品分野	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 か月～	6 か月以下（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

ICCC2014 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 か国が署名を完了し，この cPP への適合評価及びそれ以外の 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．

3.3 国内：経産省の通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，各製品分野毎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．

4. 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共に日米主導の 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 又は PP に適合するため技術分野ごとに定められたテスト及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．

更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].

5. おわりに

本稿を読んでいただいた皆様の中には，CC を全く知らなかった方，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ゃると思う.

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 製品に関わる開発者や政府調達要件に関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.

デジタル複合機以外の様々な分野において，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なかで，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.

表 4. cPP 適合評価に備えたアクション

情報収集：CCUF へ参加し，情報収集(現在，参加費無料)
1)ウェブ及びメーリング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 又は PP を記載(調達者のみ)

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 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. 尚，本稿は情報処理学会デジタルプラクティスに掲載された招待論文[11]を一部修正し、統計値をアップデートしたものである.

参考文献

1) 田渕治樹：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 ｎ あ ex.html
4) CCRA 認証実績：http://www.commoncriteriaportal.org/products/stats/
5) 中小企業投資促進税制：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.55No.9（2014）
8) CCRA の公式サイト：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 ICCC 実行委員会（インド STQC、CII）：15th International Common Criteria Conference -Meeting the Technology Challenges", 2014, ISBN: 978-93-83842-70-4
11) 金子 朋子，村田 松寿，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！―，情報処理学会 デジタルプラクティス Vol.6 No.1 (2015)