コモンクライテリア承認アレンジメント
運営委員会（MC）

ビジョンステートメント

文書番号:　2012-09-001（2012年10月翻訳第1.0版）
バージョン:　2.0
日　　付:　2012年9月
題　　名:　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

背景

これまでのCCRAでの活動は、かなり、CC/CEMの開発と、各国の認証制度間でのCC/CEM適用のハーモナイゼーションにフォーカスしてきた。 最近、CCRA加盟国の政府機関と製品ベンダ、評価機関が協力し、プロテクションプロファイル開発を促進することに関し、CCRA加盟国間では関心が高まっている。 そのようなプロテクションプロファイルは、複数の国での政府調達のために活用されることを意図している。

しかしながら、よりPPを中心とする方法でのCC及びCCRAの活用に移行するには、CCRA加盟国がどのようにプロテクションプロファイルを開発・適用していくかについてのハーモナイゼーションも必要となっている。 本文書は、CCRAのこれらへの適応のキーポイントについてハイライトを当て、続いて 運営委員会（MC: Management Committee)がそのようなプロテクションプロファイルの適切な取扱いに関して合意に至った基本的なフレームワークについて説明する。

本フレームワークは、CCRA加盟国の関心事を考慮することを保証するとともに、製品ベンダ、評価機関及びその他の利害関係者がその作業に参加し、影響を及ぼすことができることを同様に保証する。また、成果物となるプロテクションプロファイルが公平な競争のためのツールとなることも保証する。

本文書は、プロテクションプロファイル作成を管理するために必要なフレームワークにフォーカスしたMCのビジョンを表しており、CCRA自体に必要な変更に対処するものではない。 MCのビジョンは、今後の改訂で更に改善・拡大されていく予定である。 本文書に関するコメントや提案があれば、各国の認証制度を通して、CC開発委員会（CCDB: CC Development Board)に送っていただきたい。

今後の CCRA 活用のキーポイント

1. 一般的に市販されている情報通信技術を用いた認証製品における一般的なセキュリティレベルは、これらの製品の価格やタイムリーな利用可能性に大きな影響を与えることなく、向上させる必要がある。
2. その目標を支援し、合理的で比較可能で再現可能、しかも費用対効果の高い評価結果を達成するために、共同プロテクションプロファイル（「cPP: collaborative Protection Profile」）及びサポート文書を開発するテクニカルコミュニティ(TC)を構築することによって、標準のレベルを高める必要がある。
3. 相互承認は、cPPの達成可能な共通レベルに基づいたものであるべきである。
4. TCは、規定されるべきで、cPPは類似製品に関して複数の製造者がそれぞれ独自のSTを提供しているようなすべての製品クラスについて開発されるべきである。
5. 適用可能である場合、cPPはそれぞれ独自のSTの代わりに適用されるべきである。 cPPが存在しない場合、又は適用可能でない場合に限定して、独自のSTが適用されるべきであり、その場合にはCCRA相互承認は、EAL2までに限定されるべきである。
6. CCは、TCがcPPを開発するために使う単なるツールボックスとして維持される。
7. cPPを超える評価レベルは、以下のような状況のみに限定されるべきである。
    - 各国の要件（国家安全保障上の要件など）
    - 以下のような各利害関係者間の合意：
        i. 二国間協定
        ii. SOGIS-MRA、及びその他の同様なコミュニティ

    cPPのレベル以上のCCRA相互承認はない。
8. プロテクションプロファイル(「cPP」) や サポート文書は、認証製品が期待されるセキュリティレベルを達成していることを保証するために、脆弱性分析の要件に対処する。

CCRAにおける承認は、認証書に関連しており、他の国々がCCやCEMに準拠した他の認証制度によって行った作業を承認することのみを意味するという点に注意が必要である。 これは、cPPに適合する製品がほとんどの状況で使用されることを意図しているが、ある特定の状況で使用される認証製品を受け入れるにあたり、認証が常に十分であるとは限らない。その他の要件や法令を適用することができる。

もう一点注意すべきことは、cPPは新しいものであるが、CCとCCRAへの追加的な適用であるということである。現存のSTやPPの適用は依然として適用されるが、それらのCCRA相互承認はEAL2までに限定されるべきである。

フレームワークとしての目的

CCとCCRAの今後の方向性についての上記のキーポイントを促進するために、以下の目標が定義されている：

理想的には技術分野に一つのテクニカルコミュニティ(TC)によって、必要とされ作成される共同プロテクションプロファイル(「cPP」)、及びそれを補足するサポート文書が、複数の国でデファクトスタンダードとなり、それが政府調達での活用を推奨されると考えられる。 この取り組みによって、利用可能な製品が増え、適合した比較可能な製品の選択が、以下のように可能となるだろう：

- これらの製品についての適切なセキュリティ機能が改善される

- セキュリティ保証の達成可能な共通レベルが定義される
- 競争が増加し、ゆえに調達の費用を抑えられる

実現手段

テクニカルコミュニティが複数の利害関係者より構成されることで、以下を実現する：

- 各国政府や任命された代表(CCRA加盟国)と協力するのは：
    - それぞれのcPPの受入れを最大限にするため；
    - 技術分野ごとの利用可能なcPPの数を制限するため；
    - cPPの開発費用を分担するため。
- cPPの対象範囲における製品ベンダと協力するのは：
    - 最先端技術を含めるため；
    - 公正な競争を促進するため；
    - 適合製品の数及び受入れを最大限にするため。
- CCRAの下で承認されたITセキュリティ評価機関と協力するのは：
    - 複数の評価機関の間での一貫性を提供するため；
    - 有効な保証アクティビティについて合意するため。

管理運営体制（ガバナンス構造）

- CCDBは、CCRA運営委員会にそれぞれの技術分野についての承認を求める。
- CCDBは、提案されたPP(サポート文書も含めて)を、合意された投票手続きに沿って、cPPとして受け入れる。
    - ベースライン要件(以下参照)を満たすPPのみが受入れの対象となり得る。
    - 十分な支援コミュニティが活動しているPPのみが受入れの対象となり得る。
- cPP及びCCRA加盟国のウェブサイトへの参照(リンク情報)が、追加のガイドライン、推奨事項や調達ポリシーの概要とともに、加盟国の詳細化等があればそれらを含めて、CCポータルに掲載される予定である。
- CCDBによって任命されるか、又は承認されたテクニカルコミュニティは、cPPやサポート文書の初期の策定及びその後のメンテナンスについて責任を負う。
    - 規約(会員の規則や投票手続き等を記述)や定期的なリエゾンステートメントが必要となる。
    - 作業中／中間のアウトプットについては、関心を持つ者すべてに公開しなければならず、CCポータルにおいて参照される。

ベースライン要件

- すべてのcPPは、相互承認をサポートするため、CCとCEMの従来のフレームワークに適合しなければならない。cPPを補足するサポート文書は、必要に応じてCEMへの解釈を与えるために作られることが期待される。cPPやサポート文書がセキュリティニーズを表現できていないという根拠が論証されるときは、CC及び/又はCEMが修正され、通常の承認手続きの対象となることがある。

- すべてのcPPは、すべてのCCRA認証制度に適用できるような要件のみ含まなければならない、特に国の適合性評価制度に依存するようなものであってはならない。
- すべてのcPPは、適切な標準化団体によって定義された、暗号プリミティブ/プロトコルに関する参照標準を明示的に規定してもよい。 cPPは、その他の「国家承認プリミティブ/プロトコル」の使用も認めるべきであり、そうすれば各国が自国向けに詳細化することができる。 相互承認のために暗号評価方法をハーモナイズさせることは、CCDBにおいて別途討議されている話題である。
- すべてのcPPは、EAL2まで、又は評価アクティビティが認証制度間で再現可能であることを示す根拠をTCが論証できる場合にはより高いレベル(EAL4まで)のCCパート3に基づく保証要件を含まなければならない。 拡張された保証コンポーネントの使用については、根拠が提供されなければ避けるべきであり、なおかつ、通常の承認手続きの対象となる。
- cPPは、セキュリティ保証の達成可能な共通レベルを定義しなければならず、かつ認証製品が期待されるセキュリティレベルを達成していることを保証するために、脆弱性分析の要件に対処する。 cPPに定義されていない保証アクティビティは、CCRAの下では相互承認されず、cPPへの適合を主張する認証書は、更に高いレベルの及び/又は追加の保証要件を含めてはならない。
- すべてのcPPは、共通のセキュリティ保証要件のミニマムセットを定義しなければならない。 cPPへの適合を主張するCCRA認証書は、cPP内に明記されたもの以外の追加のセキュリティ機能を含んではならない。その認証書の相互承認がEAL2(及びFLR)までの保証コンポーネントに限定される場合、追加のセキュリティ機能は、STに定義され、別に評価されることが強く推奨されている。
- cPPが存在しない事例、又はcPPが適用されない事例については、その認証書の相互承認がEAL2(及びFLR)までの保証コンポーネントに限定される場合、評価は製品のSTに対して行われる。 これは、標準的なPP及びそれらのPPへの適合を主張する製品についても適用される。

PP 開発

- cPPに明記されている保証要件に関連するCEMワークユニットは、なお適用されるが、必要に応じてサポート文書にて詳細化されることが期待されている。

脚注

上記のステートメントは、2012年9月17日に行われた会合においてCCMCのビジョンとして共有されたものである。すべての国がcPPのコンセプトについて合意し、cPPベースのアプローチの追加が、再現可能で、比較可能で、有効な評価結果を達成するのに役立つことに合意した。

2ヶ国が、non-cPPの相互承認をEAL2までに限定したビジョンステートメントのセクションに関して、意見の不一致を表明した。上記のビジョンステートメントに関してCCMCの完全な合意を得るために、追加のワークショップが計画されている。