資料３－３

# JISEC（CC）認証スキームを拡張する形とした発展JISEC認証スキーム（仮称）の検討

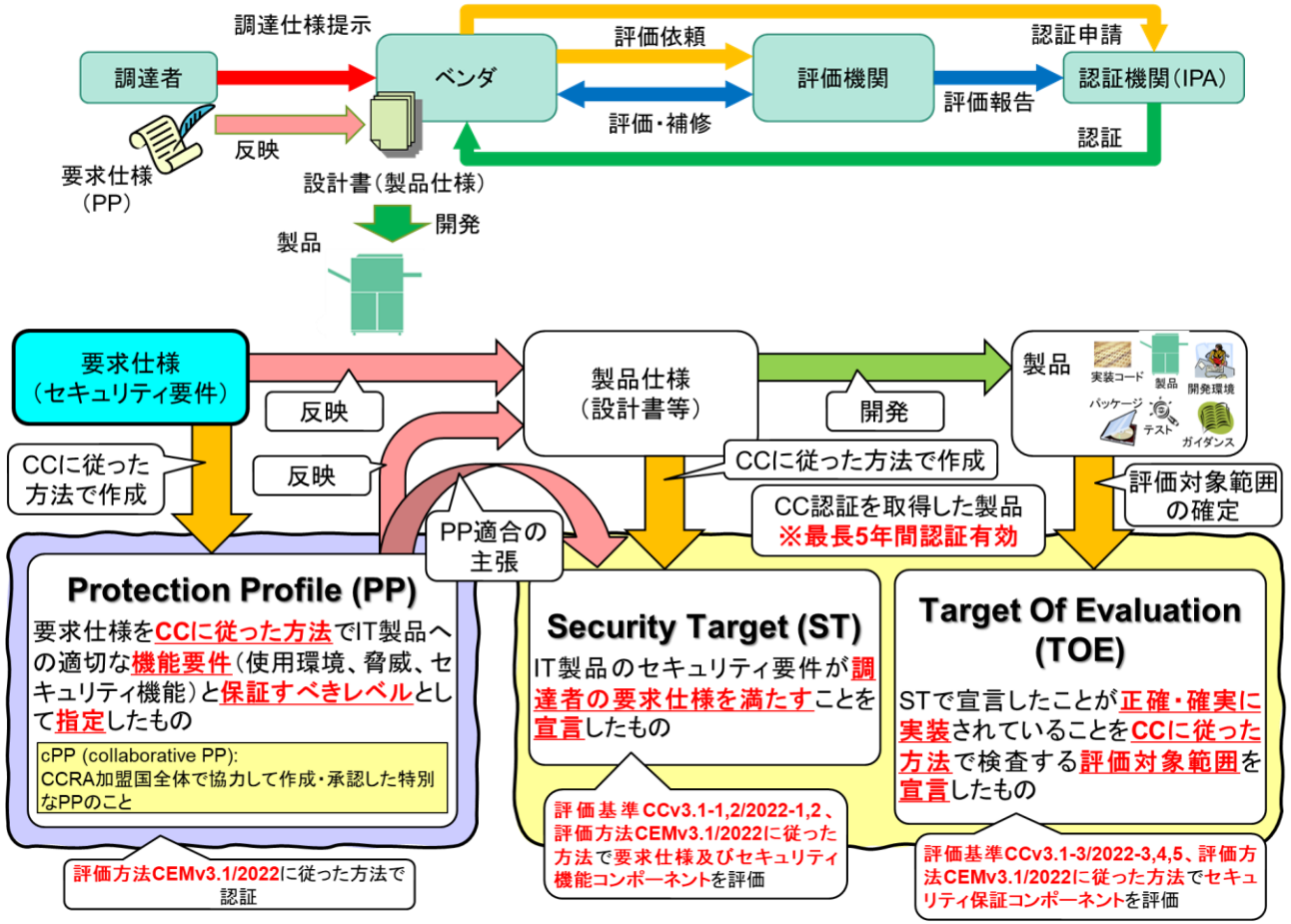
独立行政法人情報処理推進機構（IPA）
セキュリティセンター　セキュリティ技術評価部

神田　雅透

# ITセキュリティ評価及び認証制度(JISEC)

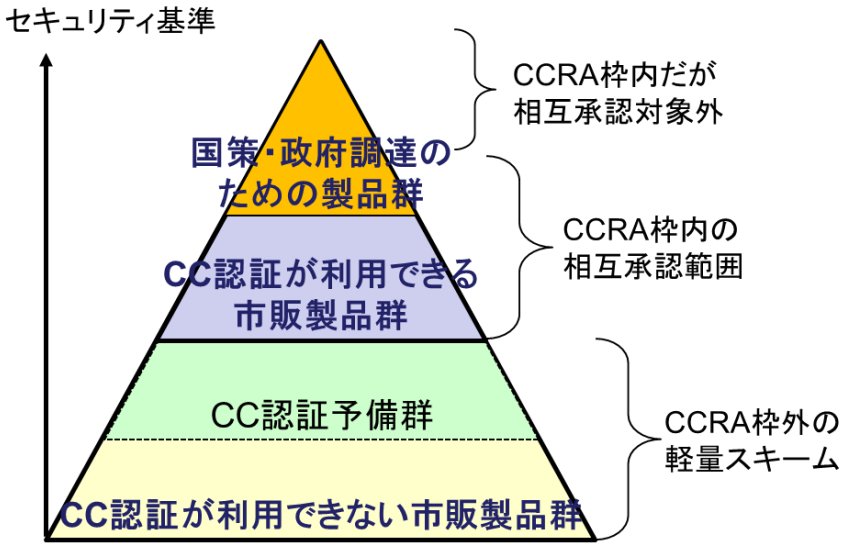
**国際標準ISO/IEC 15408（Common Criteria）に基づき、IT製品・システムのセキュリティ機能の適切性・正確性を客観的に評価・認証する日本の制度**

- IT製品やシステムのセキュリティ要求仕様に基づき、セキュリティ機能がライフサイクル全般に渡って適切に設計され、正しく実装されていることを仕様書等を対象に客観的に検査
  - セキュリティ機能要件（特定した脅威・リスクに対抗するセキュリティ機能を適切に選択）
  - セキュリティ保証要件（セキュリティ機能の正確性をライフサイクル全体として保証）
- 保証要件の評価検証の深さに依存して評価保証レベルをEAL1～EAL7まで設定
- CC認証承認アレンジメント（CCRA）加盟31ヶ国間で相互承認を実施



# 発展JISEC認証スキーム（仮称）の実現性の検討

- **認証取得目的を4つに整理し、意義を明確化した上で、各々の目的に応じた水準での認証を可能した制度見直しを検討中**
  - a. 国の安全保障に資する高度な信頼性確保を可能とする認証スキーム（原則EAL4相当）
  - b. 政府調達に必須とされる信頼性確保を念頭においた認証スキーム（EAL1, EAL2相当）
  - c. 国産品の国際流通・競争力強化を視野に入れた認証スキーム（EAL1, EAL2相当）
  - **d. コンシューマー向けのCC認証水準には達しない軽量認証スキーム**




- 発展JISEC認証スキーム（仮称）で目指す目標
  - 特に低レベルについては短期間で認証発行できる軽量スキーム
    - 政策当局、民間ユーザーの双方が、各々のニーズに沿った形で認証制度を活用できるようなスキームとして実現
    - 認証取得に必要なコスト、時間を削減
    - セキュリティ要件を共通的に適合プロテクションプロファイルの形で規定
  - JISEC認証スキームを利活用可能
    - レベルによっては認証制度の公平性・中立性維持原則（ISO/IEC17025認定機関利用）を確保
    - 日本独自制度ではあっても、国際相互承認／多国間相互承認の交渉余地があるような形での運用（＝技術的ハーモナイズ＆評価結果の信用性）
  - 発展JISEC認証スキームからCC認証へ、特に人材面や評価面で活用できることはシームレスに活用
    - 特に評価要員・認証要員の新規育成に寄与

## フランスの「CSPN認定」が参考

CSPN認定

低コストかつ低時間でセキュリティ製品から最初のレベルの信頼を得る必要がありますか? *First Level Security Certification (CSPN)* が解決策です。

2008 年に ANSSI によって設定された CSPN は、厳しい期限の下で実行される「ブラック ボックス」テストで構成されています。CSPN は、コモン クライテリア評価の代わりとなるものであり、そのコストと期間が障害となる可能性があり、求められる信頼レベルが低い場合に使用されます。この認定は、このサイトで公開されている ANSSI によって開発された基準、方法論、およびプロセスに基づいています。ANSSI と BSI の間で署名されたCSPN (First Level Security Certification) および BSZ (Beschleunigte Sicherheitszertifizierung) スキームのセキュリティ証明書の相互承認協定が

現在有効です。

# （参考）認証スキームの考え方（例）

| 信頼性の評価レベル | 高 | 中 | | 低 | | | |
|---|---|---|---|---|---|---|---|
| CCRA/相互承認の対象可否 | ○（相互承認対象外） | ○（相互承認対象） | | ×（相互承認対象外） | | | |
| | CC – EAL 4 | CC – EAL 2 | CC – EAL 1 | 発展JISEC(仮)－☆4 | 発展JISEC(仮)－☆3 | 発展JISEC(仮)－☆2 | 発展JISEC(仮)－☆1 |
| ソースコードチェック | ○ | × | × | × | × | × | × |
| ホワイトボックス侵入試験 | ○ | ○ | × | × | × | × | × |
| ブラックボックス侵入試験 | 中程度 | 基本強化 | 基本 | 基本 | 基本 | × | × |
| サイト訪問 | 必要 | | 不要（ただし、試験をオンサイトで実施する場合あり） | | | 不要 | |
| セキュリティ脅威分析 | 製品特性に応じた分析結果の明記が必要 | | | 対象脅威は事前指定（個別には不要） | | | |
| セキュリティ対策網羅性 | 製品特性に応じた脅威に対する対策網羅性の説明が必要 | | | 対象対策は機能要件・保証要件で事前指定（個別には不要） | | | |
| ST仕様書（セキュリティ機能仕様書） | 製品ごとに作成が必要 | | | 不要 | | | |
| セキュリティ機能要件 | ST仕様書に明記（申請者が指定） | | | 製品分野ごとに必須セキュリティ機能要件をPPで事前指定 | | | 全製品共通の必須セキュリティ機能要件をPPで事前指定 |
| | 脅威に対抗するのに必要な要件 | | | 強化要件 | 基本強化要件 | 基本要件 | 最低要件 |
| セキュリティ保証要件 | ST仕様書に明記（申請者が指定） | | | 製品分野ごとに必要セキュリティ保証要件をPPで事前指定 | | | 全製品共通の必須セキュリティ保証要件をPPで事前指定 |
| | 保証するレベルに応じた必要な要件 | | | 強化要件 | 基本強化要件 | 基本要件 | 最低要件 |
| セキュリティ評価 | 製品特性を考慮してCC/CEMの評価基準を適用した認証評価（Attack based or Specification based） | | | 事前設定した評価基準に従った第三者機関による適合性評価 | | | 事前設定した評価基準に従った適合性自己評価 |
| 評価報告書 | ST仕様書に依存 | | | 定型報告書／チェックリスト | | | |

現行のJISEC(CC)認証スキーム

今回検討する認証スキーム

# 今後の調整課題

## ■ 発展JISEC認証スキーム（仮称）の位置づけの明確化

- ➢ 政策的なオーソライズ、政府調達対象など、需要が見込める認証制度とする
- ➢ 関連する既存の認証制度と連携・合流する

## ■ 発展JISEC全体として、スキームを維持する体制の整備

- ➢ 要求基準・適合基準等の作成体制を整備する
- ➢ 認証要員・評価要員を確保・育成する

# 認証機関・評価機関の役割の考え方の整理

| | | ベンダー | 評価機関 | 認証機関 | 概要 |
|---|---|---|---|---|---|
| 自己適合宣言 | A | 対象製品を自ら評価し、チェックシート等で自己適合宣言を実施<br>発展JISEC認証(仮)のうち、特に低レベル(☆1)で許容する方向 | ー | **ベンダーからのチェックリスト等の情報が正しい(＝ミスや不正がない)**ことを前提として、届出自動受付 | ● 信頼する場所：ベンダー<br>● **ベンダーがミスや不正をしないことがベース**＝ベンダーの信頼性に全面的に依存＝**ベンダーのミスや不正があっても検出できない**<br>● ミスがあったときの是正指示、サーベイランス実施体制、不正があったときのペナルティ措置などの信頼性確保の検討が別途必要 |
| | B | 対象製品の評価を評価機関に依頼し、その結果で自己適合宣言を実施<br>発展JISEC認証(仮)のうち、特に中レベル(☆2)で求めることを検討 | 対象製品の評価を実施し、評価報告書とチェックシートを作成<br>※中立性担保義務なし | **ベンダーからのチェックリストや評価報告書が正しい(＝不正がない)**ことを前提として、届出自動受付 | ● 信頼する場所：ベンダー＜評価機関<br>● **ベンダーと評価機関の信頼性をベース**＝評価報告書の**品質が評価機関の評価能力によって異なり**、結果として認証レベルが大きく左右する恐れあり＝中立性担保義務がないので、ベンダーと評価機関が**結託すると不正があっても検出できない**<br>● **「機器検証サービス登録事業者」と「評価機関」との関係整理**が必要<br>● ミスがあったときの是正指示、サーベイランス実施体制、不正があったときのペナルティ措置などの信頼性確保の検討が別途必要 |
| 第三者認証 | C | 対象製品の評価を評価機関に依頼<br>発展JISEC認証(仮)のうち、特に高レベル(☆3～4)で目指す方向 | 第三者として対象製品の評価を実施し、評価報告書を作成<br>※中立性担保義務あり | **評価機関からの評価報告書が正しい**ことを前提として、手順書・ガイドライン・ガイダンスに従い、**必要な内容が評価報告書に記載されていることを確認(＝形式チェック)**し、問題がなければ認証する | ● 信頼する場所：評価機関＞認証機関<br>● **評価機関の信頼性をベースに認証機関が認証**＝評価機関が実質的な評価責任を負う＝評価報告書の**品質が評価機関の評価能力によって異なり**、結果として認証レベルが左右される恐れあり<br>● 自動検証ツールや報告書作成ツールなどの自動化支援ツールを開発・提供や、評価ガイダンス・ガイドラインを定めるなどで、評価機関間の能力ブレを解消するなどの対策が必要になるかもしれない<br>● 認証機関は、(個別製品ではなく)**評価機関の能力審査(≠中立性・公平性審査)や評価ガイダンス・ガイドラインの作成を実施できる**要員を持つ必要あり |
| | D | 対象製品の評価を評価機関に依頼<br>現行JISEC(CC)認証のやり方 | 第三者として対象製品の評価を実施し、評価報告書を作成<br>※中立性担保義務あり | **第三者**として、手順書に従い、**評価報告書の内容を確認(＝内容チェック)**し、内容に問題があれば差し戻す。 問題がなければ、認証機関が認証報告書を自ら作成した後、認証する | ● 信頼する場所：評価機関＜認証機関<br>● 評価内容を含めたすべての**評価責任を認証機関が一義的に負う**＝認証機関に最終責任を一元化＝評価報告書の品質、認証レベルのブレが少ない<br>● 評価報告書の**内容を確認し、評価機関を指導できるスキルを持つ**認証要員が認証機関にも必要<br>● よく言えば「評価機関と認証機関による第三者評価ダブルチェックで認証信頼度が高い＝評価自体のミス発見や不正防止に寄与」<br>● 悪く言えば「作業が冗長。二度手間＝期間・コストに悪影響」 |

# （参考）認証機関・評価機関・ベンダーの関係