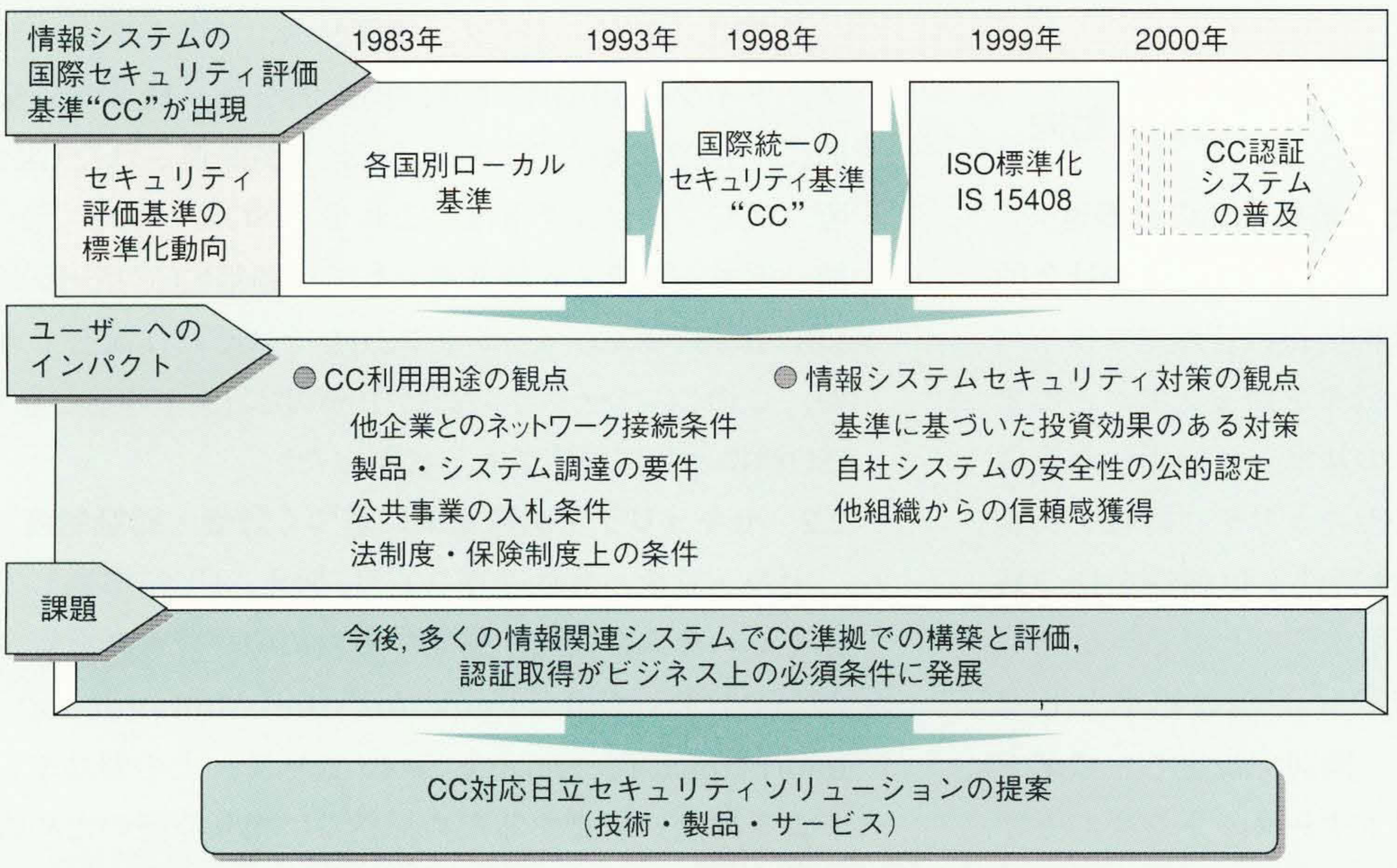
情報システムに対するセキュリティ国際評価基準の動向と日立製作所の対応

Trends of International Evaluation Criteria for Information System Security and Hitachi's Approach

永井康彦 *Yasuhiko Nagai*　畠山靖彦 *Yasuhiko Hatakeyama*
手塚 悟 *Satoru Tezuka*　中村孝男 *Takao Nakamura*



注：略語説明
CC（Common Criteria）
ISO（国際標準化機構）
IS（International Standard）

情報システムセキュリティ対策へのCCの影響と日立製作所の取組み

今後の情報関連機器・システムでは，セキュリティ国際評価基準（CC）準拠が必須条件となる。日立製作所は，実績のあるセキュリティ評価技術を基盤に，投資効果が見込まれる標準対応の技術・製品・サービスの開発に取り組んでいる。

1999年に，セキュリティ国際評価基準（CC：Common Criteria）がIS（International Standard）15408としてISO（国際標準化機構）標準となる。この評価基準は，製品・システムに必要となる基本的なセキュリティ機能要件とその機能品質の保証要件，および7段階の保証レベルを規定している。ユーザー情報部門担当者や製品開発者，システム設計・構築を行うSE（Systems Engineer）は，このCC規定要件から自身の対象製品・システムに必要な要件を選択してセキュリティ基本仕様書（情報システム セキュリティ ポリシー）を作成し，開発・構築を行うこととなる。また，この基準に基づく評価・認証制度が確立され，設定した保証レベルに対応する評価・認証を指定の評価・認証機関から取得することとなる。

標準化以降，EC（Electronic Commerce），金融，公共，医療分野が先行し，顧客の調達要件や他企業との接続条件，海外納入の前提条件，法制度・保険制度上の条件としてCCが活用され、特にネットワーク接続される情報関連製品・システムでは，CC準拠がビジネス上の必須条件になるものと予想される。このような動向に対して，日立製作所は，先進的で実績のあるセキュリティ評価技術を基盤に，CCベース統合構築手順の開発をはじめとする技術・製品・サービスの開発に取り組んでいる。

1 はじめに

1999年春にセキュリティ国際評価基準“CC（Common Criteria）”がIS（International Standard）15408としてISO（国際標準化機構）で標準化される。この評価基準は，情報関連製品・システムに必要となるセキュリティ施策の要件集を規定したものである。また，この評価基準に基づいて開発・構築された製品・システムは，政府または指定の民間の評価・認証機関の評価・検証による認証を取得することにより，セキュリティ施策に関して公的に保証されたものとなる。このため，標準化以降，顧客の調達要件や他企業との接続条件，海外納入の前提条件，法制度・保険制度上の条件としてこの評価基準が活用され，多くの情報関連製品・システムについてCC準拠での開発や認証を取得することが，ビジネス上の必須条件になるものと予想される。

欧米の多くの国はTCSEC（Trusted Computer System Evaluation Criteria）やITSEC（Information

Technology Security Evaluation Criteria)などの国別評価基準と評価・認証制度の基盤をすでに持っており，CCへの移行が容易である。一方，これら先進諸国に比べて，このような基盤を持たないわが国の対応が急がれる。

ここでは，CCの概要と動向，および日立製作所の先進的で実績のあるセキュリティ評価技術[1]を基盤にした技術開発，製品・サービスビジネス開発への取組みについて述べる。

2 セキュリティ国際評価基準の概要と動向

2.1 セキュリティ評価の目的と国際標準化の必要性

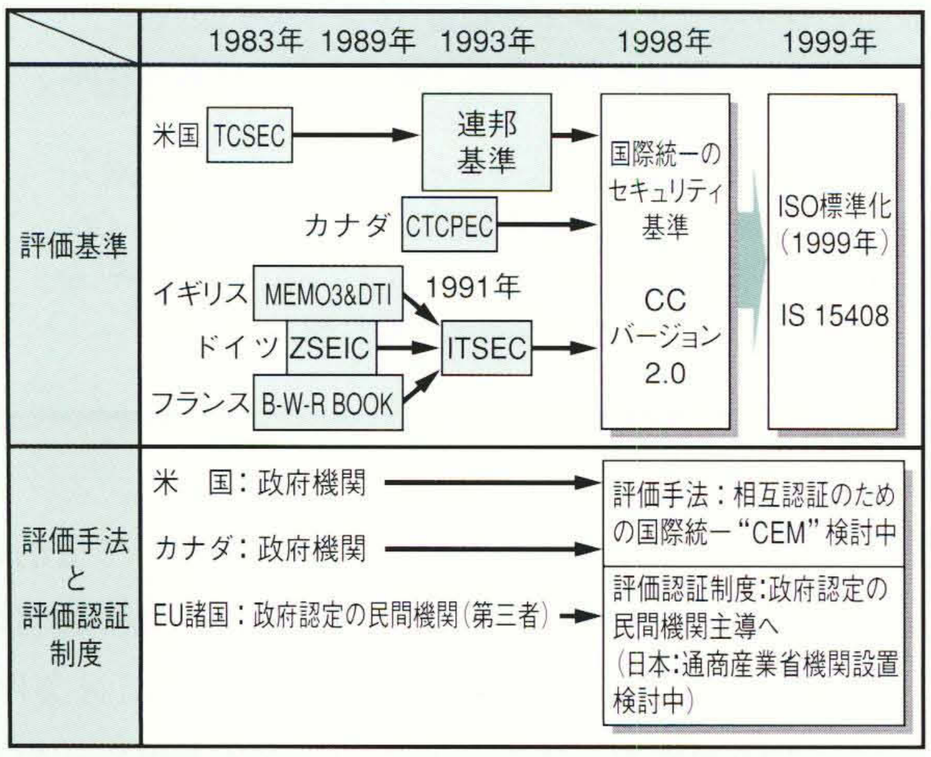
セキュリティ評価の目的は，企業財産の保護や社会的責任を果たすために，企業の機密情報の管理やプライバシー情報の管理の施策を，投資効果を踏まえて，どこまでやればよいかを評価するための基準と評価手法を提供することにある。企業は，このセキュリティ評価を実施することにより，必要十分な機密性や信頼性を持つ製品・システムを調達したり，利用することができる。

欧米では，従来，セキュリティ評価の標準としてITSECやTCSECに代表される，国別で規定した標準を用いてきた。しかし，近年のインターネットを中心とするEC(Electronic Commerce)の活性化などに対応して，国際的ネットワーク・システムを構築する際に各国で標準が不統一では安全性の確保を保証しにくいことが問題となってきた。また，企業どうしの接続や取り引きでの要件としてのシステムの機密性や信頼性に関する相互認証，すなわち，特定の国で認証取得したものが自動的に他の国でも認証されたものとして扱われることへの要求が高まってきた。このような背景から，セキュリティ評価基準と相互認証のための評価手法の国際標準化と，評価・認証制度の確立が必要となってきた。

そこで，米国，カナダ，イギリス，フランス，オランダ，ドイツの6か国により，国際的な統一標準作成を目的に，1993年からCCプロジェクトが推進された(**図1**参照)。CCプロジェクトは，これまでISOと連携しながら，統一セキュリティ評価基準として1996年にCCバージョン1.0，1998年にCCバージョン2.0をそれぞれ作成してきたが，このCCバージョン2.0が1999年にIS 15408となり，ISO標準として規定されるに至った。

2.2 セキュリティ国際標準に基づく評価・認証制度

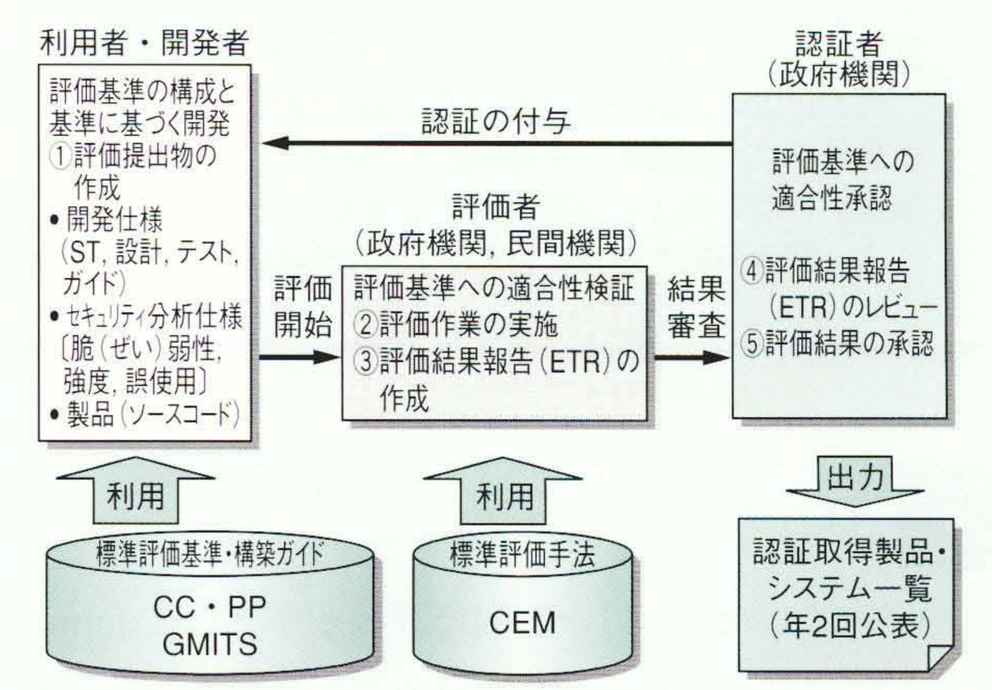
セキュリティ評価基準“CC”に加え，CCに準拠して製品やシステムを開発，構築するためのプロセスを規定した“GMITS(Guidelines for the Management of Information Technology Security)”や，その製品やシステムを評価，認証するため，さらに相互認証のための統一評価手法“CEM”についても現在，標準化作業が進められている。これらの標準化によって評価・認証制度が設立され，製品・システムの国際的なセキュリティ評価・



注：略語説明
CTCPEC(Canadian Trusted Computer Product Evaluation Criteria)
EU(欧州連合)，CEM(Common Evaluation Methodology)

図1　国際標準化の歴史と動向

従来の国別セキュリティ評価基準から欧米6か国加盟のCCプロジェクトが作成した評価基準“CC”がISO標準となり，国際統一の評価基準が誕生することとなった。



注：略語説明
ST(Security Target)，PP(Protection Profile)
ETR(Evaluation Technical Report)

図2　セキュリティ国際標準に基づく評価・認証制度

セキュリティ国際評価基準に基づいて開発，構築された製品・システムは，政府または民間の評価機関での評価と政府機関の認証を受けることとなる。

認証が今後実施されることとなる(**図2**参照)。

図2に示す評価・認証制度では，利用者または開発者は，CCとGMITSを利用して製品やシステムの開発・構築を行い，その成果物である規定の仕様書やソースコードなどを評価機関に提出して評価・認証の申請をすることとなる。評価機関では，CEMを利用して評価作業を実施し，その作業結果として評価結果報告“ETR”を作成して，認証機関に提出する。認証機関では，ETRを検証して合格ならば，開発者や利用者に対して対象製品・システムに関する認証を付与するとともに，認証取得製品・システム一覧に追加して，年2回ホームページなどで公表するという評価プロセスが基本的に実行されることとなる。

欧米では，従来標準での同様な評価・認証制度を移行，拡張して，この評価・認証制度を1998年からすでに開始している。また，評価機関を政府機関から政府認定の民間機関に移し，民間機関主導となってきている点が最近の動向としてあげられる。わが国ではまだこのような評価・認証制度が設立されていないが，通商産業省を中心に現在，検討が進められている。

2.3　セキュリティ国際評価基準“CC”の概要

2.3.1　CC(IS 15408)の規定内容[2)]

セキュリティ国際評価基準“CC”は，パート1：イントロダクションと全体モデル，パート2：セキュリティ機能要件，およびパート3：セキュリティ保証要件の三つのパートで構成されている。

パート2のセキュリティ機能要件は，評価対象非依存の機能要件のカタログ集であり，セキュリティ監査，セキュリティ通信，利用者データ保護，識別と認証，プライバシー，セキュリティ機能保護，資源利用，TOE(Target of Evaluation)アクセス，高信頼経路，暗号管理，およびセキュリティ管理の11の機能クラスに分類されている(**図3**参照)。さらに，おのおののクラス内で共通目的で使用する機能群を「ファミリィ」という単位で分類し，ファミリィの中に実際に使用される機能部品群をコンポーネントとして登録している，階層的な構造の要件集となっている。

一方，パート3のセキュリティ保証要件は，評価対象非依存の保証要件のカタログ集であり，PP(Protection Profile)評価，ST(Security Target)評価，構成管理，配布と操作，開発，ガイダンス文書，ライフサイクル，テスト，脆弱性分析，および保守の10の保証クラスに分類され，機能クラスと同様に，階層的な構造の要件集となっている。また，保証要件には，さらに“EAL(Evaluation Assurance Level)”と呼ばれる保証レベル(認証レベル)が規定されており，機能仕様書の検証などの簡単なテストで保証されるレベルから，仕様書記述として形式言語を使用し，上位レベル仕様書や製品テストなどの厳密な

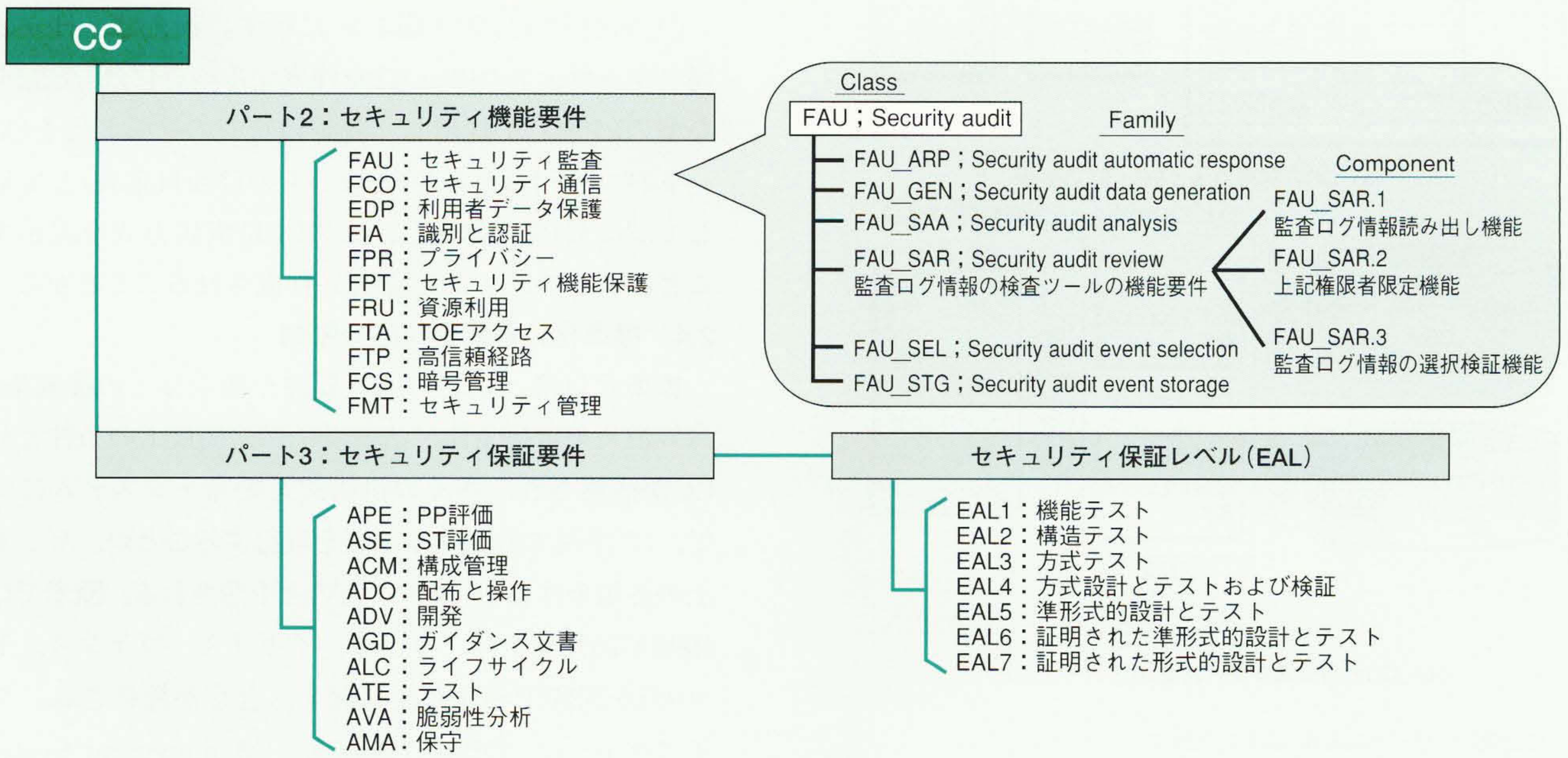


図3　セキュリティ国際評価基準“CC”の規定内容

CCは，製品・システムに基本的に必要とされるセキュリティ機能要件，保証要件と保証レベルをそれぞれ規定した要件のカタログ集である。

テストも実施して保証されるレベルまで，7段階のレベルが定義されている。高いレベルほど評価提出物，保証要件，評価内容が多くなり，高度に，厳密に検証することが要求される。したがって，TCSECなどの従来標準では，高い認証レベル取得には強制アクセス制御機能などの高度なセキュリティ機能をサポートすることが要求されたのに対して，CCでは機能の追加ではなく，機能の品質の高さによって高いレベルが認証される点で大きく相違することに注意する必要がある。

なお，この保証要件は，ISO9000(品質システムの国際規格)と重複する要件を含むが，現時点では無関係に規定されており，各利用者はISO9000の認証を取得していても，CC保証要件の視点で見る必要がある。

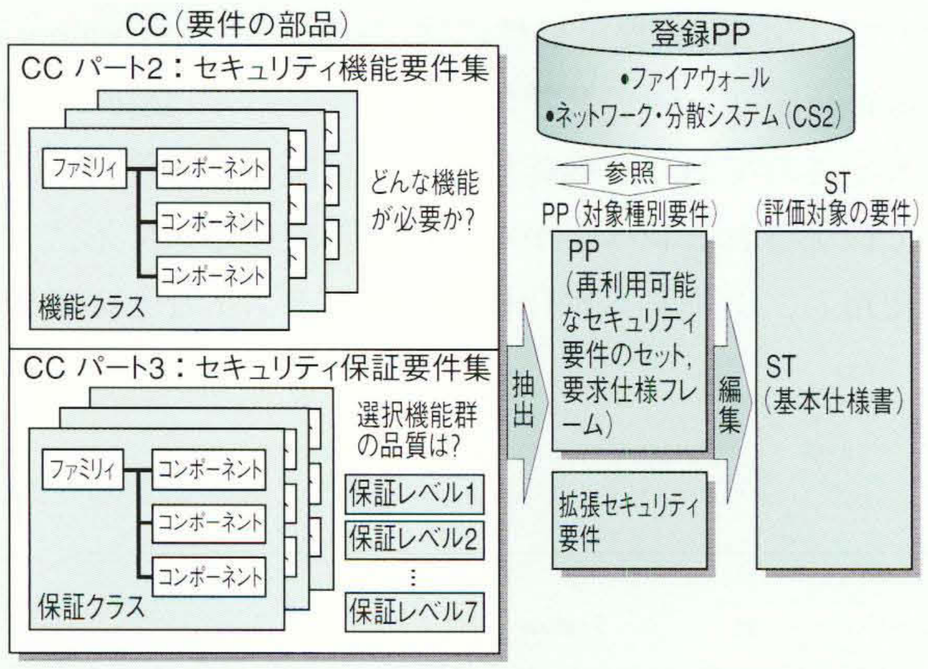
2.3.2　CCの利用方法

CCに準拠して製品・システムを開発，構築し，認証取得するためには，CCの機能要件・保証要件を利用した規定の形式のセキュリティ要求仕様書(調達仕様書)と基本仕様書を作成することが必要となる。要求仕様書は「プロテクションプロファイル(PP)」，基本仕様書は「セキュリティターゲット(ST)」とそれぞれ呼ばれる。

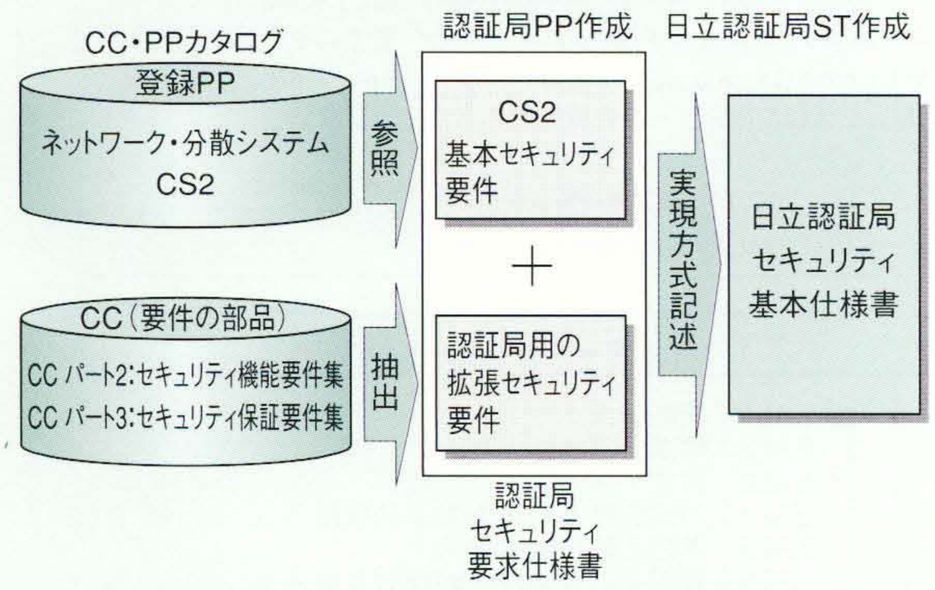
TOEの利用者または開発者は，TOEに関して必要となるセキュリティ機能コンポーネントをCCパート2のセキュリティ機能要件から選択，抽出(登録されてないコンポーネントは拡張機能要件として独自定義)する。さらに，認証取得したい保証レベルを設定し，その保証レベルに必要な保証要件のコンポーネントをCCパート3のセキュリティ保証要件から選択，抽出することにより，そのTOEのPPを作成する。STの作成では，PPに記述された要件に対する，そのTOE固有の具体的な実現方式を追加記述する〔**図4**(a)参照〕。

STが実現方式を記述しているので，TOEに依存した仕様書になるのに対し，PPは要件レベルの記述であり，TOE種別に共通の再利用が可能な要求仕様書となる。そこで，PPを国際的に共有するために，PPの登録制度も検討されている。TOEに関係する既登録PPが存在する場合，利用者または開発者は，基本的に登録PPを再利用してPP・STを作成しなければならない。現在，ファイアウォールやネットワーク・分散システムモデルのPP原案が作成されている。特に，“CS2”と呼ばれる後者のPPは，情報関連システムの基盤となるものであり，情報システムの企画・構築を担当するユーザー情報部門関係者や製品・システムの開発・構築を担当するベンダ開発者，SE，コンサルタントにとって重要なものである。

CC利用の具体例を**図4**(b)に示す。例えば，日立認証局ソフトウェアのPP・STを作成する場合には，CS2をひな型のPPとして採用し，認証局特有の拡張要件をCCパート2やパート3から選択(ないものは独自定義)して追加して認証局PPを作成し，このPPに実現方式を記述することによって日立認証局STが作成されることとなる。



(a) CCの利用方法とPP・STの関係



(b) CC利用の具体例(認証局ソフトウェア)

注：略語説明　CS2(Commercial System 2)

図4　CCの利用方法と具体例

CC要件カタログと登録PPから必要な要件を参照，選択して，対象製品・システムのPP・STを作成する。

2.4　標準化の影響と対応の動向

標準化以降，顧客の調達要件や他企業との接続条件，海外納入の前提条件，法制度・保険制度上の条件としてCCが活用され，多くの情報関連製品・システムについて，CC準拠での開発や認証を取得することが，ビジネス上の必須条件になっていくものと予想される。欧米では，1998年10月に米国，カナダ，イギリス，フランス，ドイツの5か国間で相互認証に関する合意が締結され，ファイアウォール，DBMS(Database Management System)などのCC認証取得製品の市場投入が開始されてきている。加えて，従来標準のTCSECやITSECで認証済みの

製品は，それぞれ相当するCC認証レベルに自動認証されることから，CC認証製品の展開が進むものと予想される。また，ドイツでは，ECや医療分野の電子署名関連サービスを提供するシステムに対して，CCのEAL5の評価・認証を条件として制度化し，イギリスでは，情報セキュリティ保険の保険料査定にCC認証レベルを利用するなど，CC認証の活用の動きも立ち上がりはじめている。

このような海外の動向の中で，まだCC認証製品もなく，評価・認証機関も準備中であるわが国の早急な対応が求められる。一般商用で必要な認証レベルはEAL4であると言われており，海外製品もこのレベルまでは取得していることから，日本製品もこのEAL4取得が基本的な目標となる。これに対応しないと海外市場でのビジネスチャンスを失うだけでなく，国内市場でも調達要件をクリアできなかったり，ユーザーがネットワーク接続できなくなるといった深刻な問題を招く懸念がある。

3　日立製作所のCCへの取組み

3.1　技術開発への取組み

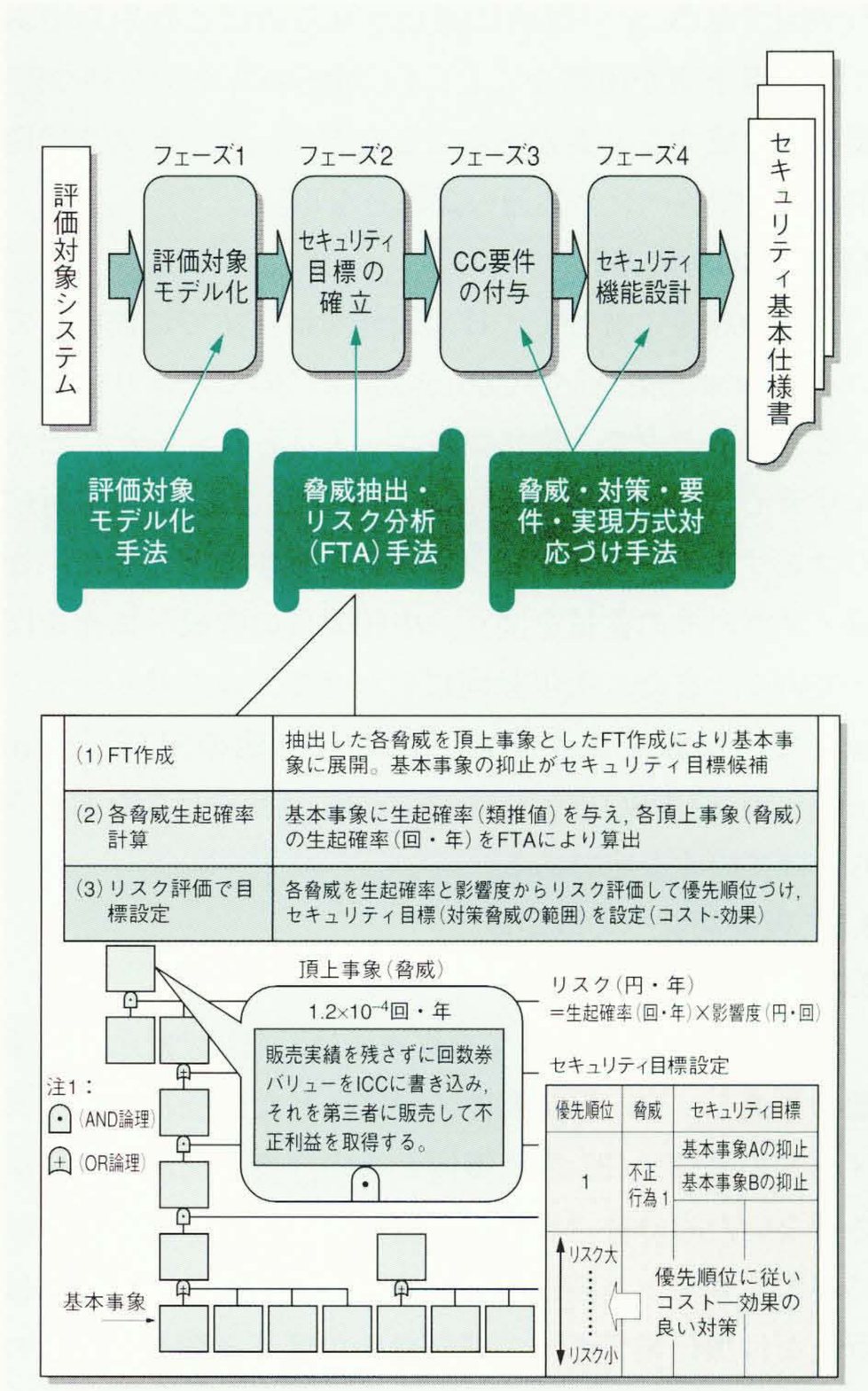
3.1.1　技術課題

CC準拠で製品を開発し，システム構築して認証取得をするには，PP・STの作成が必須となる。しかし，現状ではこのPP・STを作成する手順がなく，TOEに関する脅威の抽出，脅威に対する対策目標や対策目標に対してのCC要件の定義が作成者の知識・能力に依存することから，膨大な作成時間がかかる。また，作成内容の品質を保証することが困難なものとなっている。

3.1.2　CCベース統合構築手順の開発

日立製作所は，PP・ST作成作業を効率的，手続き的に行え，作成内容の均一性や妥当性を保証するための，GMITSを含むCC準拠の統合構築手順[3]を開発した。

この手順は，評価対象定義(TOEモデル化)からセキュリティ基本設計書(ST)作成までをフェーズ分けして，段階的に支援するものである(**図5**参照)。セキュリティ分析・評価技術の専門家でない一般の開発者やSEが，PP・STを効率的に作成するために役立てることができる。また，この手順で脅威に対する対策目標設定に使用しているFTA(Fault Tree Analysis)応用リスク分析・評価手法では，日立製作所が先進的に情報システムのセキュリティ評価[1]に適用してきた実績とノウハウを持っているものであり，リスクの大きさの順にコスト—効果の良い対策目標を定量的な評価値によって設定することができる。したがって，セキュリティ対策をどこまで行うかの客観的な指標が明示され，セキュリティへの投資効果を把握することができるようになる。なお，この手順はSE向けのセキュリティ計画ガイドとして提案し，CCベースのシステム セキュリティ コンサルテーションサービスを手始めに，活用を展開する考えである。



注2：略語説明　FT(Fault Tree)，ICC(IC Card)

図5　CCベース統合構築手順の概要
評価対象定義からPP・ST作成までを段階的に支援する手順・手法を提供し，作業の効率化と均一化を図る。

3.2　サービスビジネスへの取組み

3.2.1　CC対応上の課題

国際的に認められたセキュリティ評価基準が提供されることにより，公的な基準に準拠したセキュリティ対策や，法的・ビジネス的要件を達成しなくてはならない必要から，企業システムのCC対応のニーズが今後急速に立ち上がるものと考える。その際に，CC対応の新しいサービスビジネス市場が開拓される可能性がある。しかし，

わが国ではCCが一般的に認知されるのはこれからであり，市場予測が困難なこと，CC対応のスキルを持つSE要員を育成する必要があることなどが，サービスを展開するうえで各ベンダ共通の課題となる。

3.2.2 CC対応方針

上記の課題に対して，日立製作所は，すでに提案している“Secureplaza”や“Compassport”のセキュリティサービス体系の中で，現状顧客ニーズのあるシステム セキュリティ コンサルテーション サービスとして，CC対応のコンサルテーションビジネスを提案するとともに，知識・ノウハウの蓄積を図り，中核要員の育成・拡充を図っていく。また，市場動向に合わせて，コンサルテーションでの経験を生かすことにより，他のSI(System Integration)やSO(System Operation)サービスなどを立ち上げていく予定である。

3.3 製品開発への取組み

3.3.1 CC対応上の課題

CCに対応した製品開発を行うには，(1) 設計・開発手順の見直し，(2) 保証要件に規定された評価提出ドキュメントの整備，(3) 評価機関からの評価の出戻りを発生させないための自己評価の実施，および (4) 評価・認証に要するコストと期間への配慮が必要となる。これらは新たな付加作業であり，開発効率の低下と開発コストの増加を招くことが各ベンダ共通の課題となる。

3.3.2 CC対応方針

上記の課題に対して，日立製作所は，ツールなどの開発・活用による効率的な製品開発の維持と，モデルプロジェクトによるCC対応試行により，技術者育成とノウハウの蓄積を図る方針でCC対応作業を進めている。また，製品のCC対応を効果的に実現していくために，国際間の動向や国内制度の整備状況，市場ニーズ動向などを総合的に判断して，認証取得目的と対コストバランスの明確化を行い，対応分野や製品，対応時期を明確化していく考えである。

4 おわりに

ここでは，セキュリティ国際評価基準“CC”の概要と動向，およびCCに対応する日立製作所の技術開発，製品・サービス開発に関する取組みについて述べた。

今後，国内評価機関の設立を境に，わが国でもこのCC対応の本格的ニーズが高まってくるものと予想する。日立製作所は，先進的で実績のあるセキュリティ評価技術を核に，動向を踏まえた製品対応とサービス体制を確立し，ユーザーのニーズにこたえていく考えである。

参考文献

1) 宝木，外：金融機関におけるシステムセキュリティ技術，日立評論，**70**，3，103～108(昭63-3)
2) 田淵：「セキュリティ評価基準」の詳細と対策，日経コンピュータ，1998年12月21日号，159～163，1999年1月4日号，124～133
3) 織茂，外：セキュリティシステム構築のための計画手順の提案，情報処理学会コンピュータ セキュリティ シンポジウム'98論文集，Vol. 98，No.12，75～80(1998)

執筆者紹介

永井康彦
1985年日立製作所入社，システム開発研究所 セキュリティシステム研究センタ 所属
現在，セキュリティシステム構築・評価技術の研究開発に従事
電子情報通信学会会員，電気学会会員，日本航空宇宙学会会員
E-mail：y-nagai @ sdl. hitachi. co. jp

手塚　悟
1984年日立製作所入社，システム開発研究所 セキュリティシステム研究センタ 所属
現在，セキュリティシステム応用技術の研究開発に従事
情報処理学会会員
E-mail：tezuka @ sdl. hitachi. co. jp

畠山靖彦
1978年日立製作所入社，情報・通信グループ 情報システム事業本部 情報システム事業部 ネットワーク＆サービス本部 ネットワークビジネス企画部 所属
現在，ネットワーク事業の企画に従事
E-mail：yhatake @ system. hitachi. co. jp

中村孝男
1977年日立製作所入社，情報・通信グループ ソフトウェア事業部 計画部 所属
現在，セキュリティ関連ほかの製品企画に従事
情報処理学会会員
E-mail：nakamura @ soft. hitachi. co. jp