技術情報管理認証取得への取り組み

一般社団法人日本金型工業会　認証運営委員会委員（主席審査員）　川名　正幸

前回の「認証制度の特徴と認証取得準備のポイント」に引き続き，今号では認証審査の重要なポイントである，「アクセス制限」や「顧客や取引先との情報の受け渡しルール」について，審査を通じて気になった点や私見も交え，具体的対策の考え方を解説したい。また，能力成熟度モデルで見た情報管理の段階的レベルアップの考え方にも触れるので，まだ認証取得を検討されていない方々にも参考にしていただけるとありがたい。

コーヒーポットから想像できたこと，できなかったこと

インターネットの商用利用が解禁された1993年，筆者も今や死語となったネットサーフィン[1)]を初めて体験し，情報コンテンツ時代の到来を予感し衝撃を受けた覚えがある。

中でも英国ケンブリッジ大学のある研究室に置かれた，トロイの部屋のコーヒーポット（Trojan Room coffee pot）[2)]のモノクロ画像（**図1**）は，世界中の誰もがネットワークを通じて，リアルタイムに同じ映像を目にすることができる点から，インターネットが持つ可能性に注目が集まった。

一方で，これが情報セキュリティの脅威として，

図1　トロイの部屋のコーヒーポット

どれほど重大な意味を持つかについては，当時思いが至らなかったし，世の中の意識も薄かったように思う。

今日，インターネットを介したビデオ通話，親や子供の見守りカメラは，ごく身近なものとなった。街の防犯カメラが犯罪抑止と犯人追跡に有用なものとなり，オンライン診療も徐々に普及が進んでいる。

反面，過去に「Mirai」（ミライ）[3)]と呼ばれる

1）ネットサーフィン
Webサイトの情報コンテンツを，興味の赴くまま，次から次へとリンク先をクリックしながら閲覧していく行為。
2）コーヒーポット
ケンブリッジ大学の研究室の学生が，コーヒーを飲みたくなった時に，離れた場所にあるコーヒーポットの状況を確認したいという理由から，カメラをインターネットに接続して確認するという仕組みを作った。
3）マルウェア（ウイルス）の「Mirai」（ミライ）
ネットワークカメラや家庭用ルーターなどの機器を遠隔操作できるマルウェア。セキュリティを意識していない製品や，ユーザも出荷時のID/パスワードをそのまま使用しているケースも多く，Miraiはこのような脆弱性の高い機器に感染し，それを踏み台とした大規模DDoS攻撃に用いられた。

マルウェア感染が大きな話題になったように，アクセス制限の脆弱性を突いた不正アクセスによる情報漏えいやシステムダウンも日々発生している。また以前から注意喚起されてきたにも拘わらず，いまだに初期パスワードのままの監視カメラから，オフィスや工場内の映像が日々筒抜け（だだ洩れ状態）の企業があることも事実である[4)]。

技術情報管理認証における アクセス管理のポイント

情報管理を担う方々は，上述のような情報セキュリティリスクについて十分認識されていると思うが，一方で情報搾取の手口はますます巧妙化され，不正アクセスにより被害を受けた企業からは「まさかわが社が…思っても見なかった」という声を多く耳にする。

こうした状況下，情報へのアクセスを適切にコントロールしていくには，前号でも触れた通り，組織的対策，人的対策，物理的対策，技術的対策と，幅広い視点が求められる。

認証審査のチェックシートにおいても，**表１**に示す通り，アクセス制限について，それぞれの視点から実態の確認を求めている。以下，日々の運用における確認ポイントや，対策を進めるに当たっての考慮点を述べたい。

（1） 人的アクセスの制限

審査する側の重要な視点として，アクセス制限を行うための「人の異動」を，どこまでタイムリーに把握し，管理リスト（管理システム）にデータを反映しているかという点がある。

重要情報の機密度に応じてアクセス権限を付与（設定）することは，一旦はできても，採用，異動，退職の情報を継続的に更新していくことが必須となる。

また対象者は従業員に加えて，一緒に働く協力会社要員や出入りの業者など幅広く，すべての雇用管理を人事部門が行っているとは限らないことから，最新情報を反映・維持するためには，関係する幅広い部門との情報連携が必要となる。

表１　認証審査チェックシートにおけるアクセス制限

項目	アクセス制限の内容	対策のカテゴリー
人的アクセスの制限	アクセス権を有する者のみが重要情報を取り扱うことができるようにしている。	人的対策（組織的対策※）
管理対象情報が保管容器に保管できるものの物理的アクセスの制限	重要情報を保管容器に施錠して保管するとともに、持ち出して取り扱う場所についても限定している。	物理的対策（組織的対策※）
管理対象情報が保管容器に保管が困難な場合等の物理的アクセスの制限	重要情報が立入制限区域で管理されており、権限を有する者のみが取り扱うことができるようにしている。	
	重要情報を外部で保管する場合には、秘密保持、施錠、巡回監視等の適切な管理を行うための契約を締結している。	
管理対象情報が電子情報の場合のアクセスの制限	重要情報の入ったPCや記録媒体の持ち出しの管理や、ID、パスワード等の認証によるアクセス制限を適切に行っている。	技術的対策（組織的対策※）
	重要情報を外部のデータセンター等で管理する場合には、その信頼性を確認した上で秘密保持契約を締結している。	

※規程/ガイド類の整備や契約書の締結などの組織的対策は共通に必要となる

4）現在も「監視カメラ　覗き見」などのワードで検索すると，ライブWebカメラを検索できるサイトなどが出てくる。防犯のために監視カメラを設置したのに，犯罪者からも丸見えということが生じないよう，パスワード設定などに十分な注意が必要となる。
＊例　https：//www.insecam.org/en/bycountry/JP/

したがって，誓約書を取る際や，オフィス内への入館（入室）許可証の発行など，さまざまなタイミングをとらえて対象者の把握・更新を行い，あわせて対象者に漏れがないかのチェックを定期的に行う必要がある。

また，こうした仕組みが構築できた上で，運用においては従業員や管理者への意識付けとして，「例外を作らない」ことを心がけたい。「顔見知りだから」，「役員だから」，「重要な取引先だから」という，いわゆる「忖度」により，制限区域への入室時のテールゲート[5]や，許可申請手続きの省略などが発生することのないように，情報管理委員会などの経営レベルでの指示・徹底が望まれる。

(2)　物理的アクセスの制限

認証審査の準備などでは，「保管容器（キャビネなど）は常に施錠しておかなければいけないのか。仕事の効率が落ちてしまい徹底できない」との質問や意見をいただくことがある。

当然のことながら，運用できないルールを作っても意味がなく，対策の実効性と仕事の効率性とのバランスを考えた運用ルールが求められる。

審査基準のチェックシートでは，金型の設計情報や試作品，顧客から預かった金型などの重要情報が保管容器に収納できる情報と，工場内の製造設備や各製造工程における金型の部品や仕掛品などの保管容器に収容できない情報とで，対策を分けた記述となっている。

しかし，具体的な運用ルールを検討するに当たっては，「保管容器（キャビネなど）」での収納管理と「立入制限区域（執務室や工場など）」としての管理をセットで考え，**表２**に示したゾーニング[6]のレベルに応じた多層防御を図りたい。

例えば，設計図のようにキャビネに収納できたとしても，仕事の効率性を考え，就業時間中は施錠せず，執務室としてのドアの施錠や監視カメラによる牽制でアクセス制限をかけることも考えられる。

情報の機密性が低ければ，執務室も施錠せず，建物の出入り口だけの施錠管理とすることもあり得るし，逆に顧客によっては，同じゾーニングレベルにおいても，特別のキャビネや施錠での保管・管理を求められる場合もある。

また工場内では，特別の製造工程や，より高度

表２　施設内のゾーニングの考え方（日本金型工業会が用意した情報管理規程のひな形ファイルより）

領域区分	内容	例
レベル１	部外者の立ち寄りができ、従業員の同伴により入室が可能となる領域	事務所受付，応接室，食堂
レベル２	常時施錠等の入退出の管理が行われ、入室は原則従業員のみとし、部外者の入室は事前の許可を必要とする領域	事務執務室，金型の開発設計室，倉庫，工場，検査室
レベル３	業務上必要な関係者に限定し、入退出の都度記録を取る等の高度のセキュリティ対策が必須となる領域	サーバールーム、重要情報の保管室

5）テールゲート
共連れとも呼ばれ，通行許可者の後をついて警備を潜り抜ける行為で，正規に認証していない人間が管理ログに残らないため，セキュリティゲートにより通過する一人ひとりを検知するなど，共連れを防ぐ対策が求められる。

6）ゾーニング
セキュリティレベルにあわせて事業所や工場のレイアウトを設定し，入室制限などを適切に設けていく考え方。
来訪者や権限を持たない者が機密情報に触れないようにしてセキュリティレベルの向上が実現できる。反面，認証機器などの導入コストや，事務所内の導線も踏まえた業務の効率性とのバランスを見極める必要がある。また，消防法や建築基準法などの各種法令に適合するかどうかの確認も必要となる。

な秘密情報について，作業区画や部屋の窓をブラインドで隠すなど，個別の対応が必要となる。

このような対策は，ある意味当たり前の考え方だが，運用上重要なことは，情報を取り扱う担当者個人の一存で行ったり，周囲が黙認したりするのではなく，リスクをどこまで許容するかの視点から，情報管理委員会などでの経営レベルで判断し，会社のルールとして明確にしていくことである。

なお，実際の審査の中で目にした注意点を２点ほど紹介しておく。どちらも面倒で見逃しがちなことだが，運用の定着に向けた確認ポイントとして欲しい。

①数字キーを使った施錠で，一度も数字を変更しておらず，いったん番号を知られてしまえば，誰もがいつでも解錠できる

②就業後に重要情報の入ったキャビネを施錠しても，その鍵が入ったキーボックスの隠し場所は部外者も知っていて，いつでも誰でも重要情報を取り出すことができる。

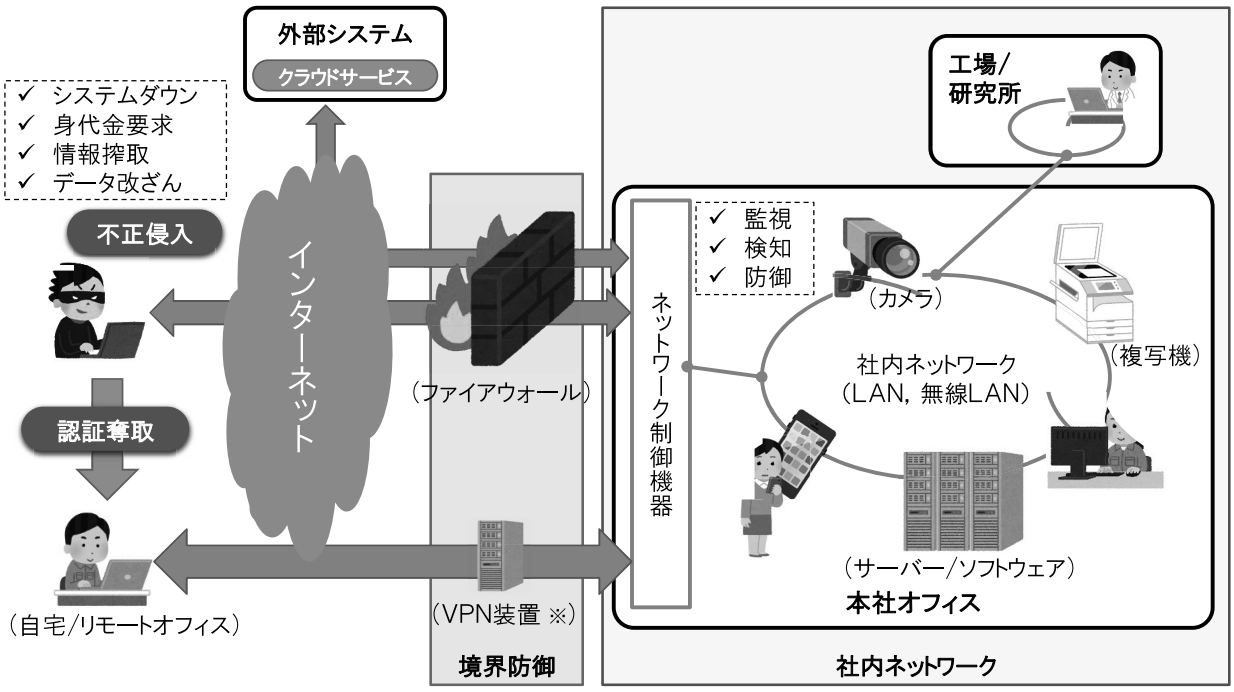
(3)　電子情報の場合のアクセスの制限

今回は一般に「サイバーセキュリティ」と呼ばれるネットワーク環境を中心とした技術的対策に絞って解説する。

中小企業の多くは社内のIT技術者が限られており，「どこまで対策を打てば良いのか分からない」とか，「何を選択すればよいか分からない」という声をよく耳にするが，当認証制度の特徴の通り，身の丈に合った対策（システム機能）を検討し，順次高度な機能へレベルアップしていけばよいとの回答に尽きる。

具体的な検討では，従来から対策の基本とされてきた**図２**に示すような「境界防御」[7]の考え方を取り入れ，以下の機能をどこまで導入するかという判断が必要となる。

①外部からの（外部への）アクセス経路を限定



※VPN(Virtual Private Network)：認証、暗号化、トンネリングの機能を使って、仮想的な専用線を構築し(プライベートネットワーク)、セキュリティリスクを低減する通信技術。インターネットや通信会社の閉域網など、用いるネットワークに複数種類があり、その特徴や費用を踏まえて適切な選択を行う。

図２　境界防御の考え方

7）境界防御
自社内のシステム（サーバー）とネットワークとの間（境界）を制御する考え方で，外部ネットワークと社内ネットワークとの境目に壁を作ることで，外部からの不正アクセスや，内部からの情報流出をブロックし，情報資産を安全に保護する考え方。

する（開閉する）機能
②外部からの（外部への）アクセスを記録する機能（ログ機能）
③不正と思われるアクセスを検知する機能
④不正アクセスを防御する機能

また，IoT[8]の普及とも絡んで最近注目されているのが，ネットワークの末端（先端）に繋がっている情報機器を，どうリアルタイムに管理・保護していくかというエンドポイントセキュリティの考え方である。

その目的は，サイバー攻撃を受けることも前提に，マルウェアの検知や除去などの初動対処をスムーズに行い，被害を最小限に抑えることにあり，ウイルス対策ソフトだけでなく，以下の機能を持つ各種ソフトウェア（EDR[9]）により，ネットワークに接続されている情報機器の保護と，万一の感染時の早期発見・被害拡大防止を目指している。

①ネットワークに繋がる情報機器全体をリアルタイムに監視する機能
②情報機器のログデータなどからサイバー攻撃の兆候を分析する機能
③情報機器へのマルウェア感染を検知した場合，被害の特定と拡大を防止する機能
④多種多様で大量な情報機器を，効率的に一元管理するための機能

こうした対策を導入するに当たっては，「その対策でできること，できないこと」を明確にしておきたい。万一不正アクセスにより情報漏えいが発生した際に，「何で防げてないの？」，「このソフトウェアを導入すれば万全だと言ってたのでは？」等々の誤解や批判を生じさせないだけでなく，情報システム全体の事業継続計画（BCP）の検討にも有効な情報となる。

これからのアクセス制御の考え方（境界防御からゼロトラストへ）

周知の通り，サイバー（ネットワーク）空間のセキュリティの脅威は増す一方で，それに対する防御の考え方や機能も日ごとに変化している。少し技術的な話題になってしまうが，今後を見据えたアクセス制御の考え方について触れておきたい。

クラウドサービスの普及により重要情報が社外に保管されるケースが急増し，コロナ感染対策としてリモートオフィスや自宅からのアクセスが常態化する中で，外部や自宅のネットワーク環境にまで管理対象を拡げる必要が生じている。さらにはスマホやタブレット端末からの情報アクセスへの対策も求められるなど，前述の境界型防御の課題が大きく表面化している。

こうした中で，新たなアクセス制御の考え方として「ゼロトラスト」という仕組み（機能）が注目されている。

図３に示す通り，「信頼できるネットワークは社外にも社内にもない」との考え方のもと，データ，アプリケーション，ID，情報機器それぞれの信頼度に基づいて，アクセス認証・認可する仕組みの構築を目指す。これにより，多様化する利用者や利用場所，社外への情報資産の保管に対応するとともに，ネットワークの境界を突破してくる高度な侵入に対応可能とする。

情報にアクセスするたびにその信頼性を評価し，認証していくことから，この考え方を実現するには，必要な機能を持ったITシステムの導入など費用と作業負荷を要する。

したがって，中小企業での普及にはまだハードルが高いと思われるが，その動向については注視していく必要がある。

8）IoT（Internet of Things）：モノのインターネット
情報機器をはじめ，家電，自動車，医療機器，産業機器など，さまざまな「モノ」がインターネットなどのネットワークに接続された，つながる世界のこと。
これらの「モノ」が所有する情報がネットワークを介して収集・分析・フィードバックされ，さまざまな形で活用されることで，新たなビジネスモデルや事業の付加価値が生まれる。

9）EDR（Endpoint Detection and Response）
PC，サーバー，スマートフォン，タブレットなどのネットワークに接続されているエンドポイントの操作や動作の監視を行い，サイバー攻撃を受けたことを発見次第対処するソフトウェアの総称。

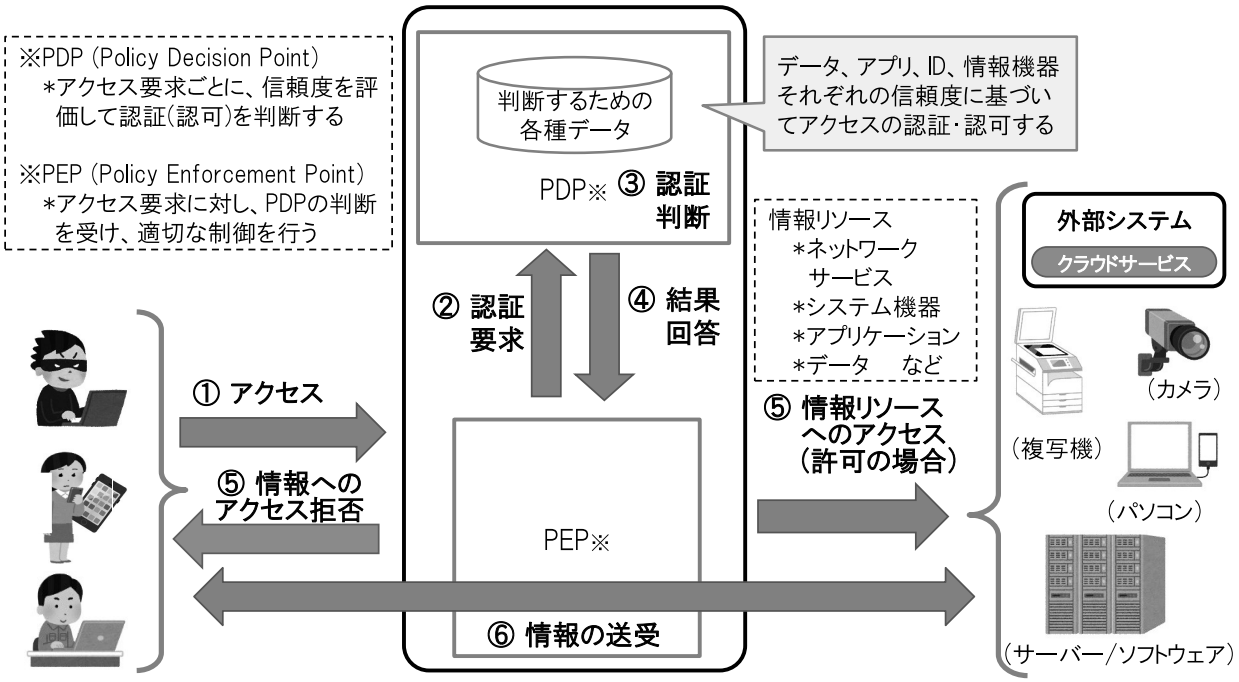


図3　ゼロトラストの考え方

顧客や業務委託先とのやり取りは決まったルールで行われているか

一般に顧客との間の情報管理の取り決めは，顧客側の要求に基づいて秘密保持契約書などにより明確になっていると思われるが，日々の活動での具体的な運用ルールの取り決めには，まだ改善を要する企業が多いと感じる。

例えばメールや電子ファイルのやり取りにおいて，誤送信を生じないために使用するツールやクラウドサービスについては，自社の都合だけでは対応が難しい場合もあり，相手先のシステム環境などを踏まえて個別に協議し決めていく必要がある。

筆者の経験でも，誤送信を防ぎ，効率的な情報共有を行うためにメーリングリストを用いることがあったが，メーリングリストの更新を怠ったがために，現在は無関係のメンバーに重要情報が流れる事態も散見された。またメールに代わって普及が拡大している，チャットを主体としたコミュニケーションツールでも，同様のリスクは顕在化しやすい。

要はここでも，情報管理（アクセス制限）の実効性は，現場の実態を理解した上で，面倒になりがちな運用を如何に継続していけるかの工夫次第ということになる。

もう一つの課題は，外部の協力会社に部品の製造などを委託する際のルールの取り決めかと思う。認証基準のチェックリストには「秘密保持契約書などを締結する」とあるが，過去の取引慣行で，注文書や口頭発注で委託されているケースや，他社では代替できない特有の技術など，さまざまな事情から対策の実施が進まない事情を見聞きする。

時間を要するが，まずは全委託先を対象に，提供している重要情報，取引額，保有技術などの現状把握とリスク評価を行い，類似の委託先を層別（グループ化）して対応策の検討を進めていってはどうだろう。

仮に，最低限求められる秘密保持契約書の締結も難しい場合は，与信管理の考え方と同様に，例外的な取引申請・承認のプロセスを設け，リスクを許容した取引継続の必要性を，経営レベルで判断することも必要と考える。

また，大学などとの共同研究開発や展示会で，重要情報を一定期間外部に保管する場合も，事前に想定されるリスクシナリオを想定し，契約等により管理ルールを明確化していく必要がある。

さらにはクラウドサービスのように，企業側で

個別の管理ルールを設定することが難しい場合は，サービス提供会社のシステム環境や信頼性について，IPA（情報処理推進機構）のチェックリスト[10]などを活用してリスク判断を行うことも有効な対策となる。

情報管理の段階的レベルアップの考え方（成熟度モデル）

これまで述べてきたことを整理すると，情報管理の推進には，現場のプロセスを可視化し，リスクマネジメントの考え方をもとに対策を検討・実施し，継続的に運用・改善していくことが必須要件と言える。このことは情報管理にとどまらず，企業の事業プロセス全体の成熟度を段階的に高めていくことにも関係しており，**図４**に示した「能力成熟度モデル」が参考になる。

このモデルでは５段階での成熟度が記述され，これから情報管理の段階的レベルアップを検討していく企業にとっては，自社の情報管理プロセスの現状がどのレベルにあるかを評価し，全従業員に対して意識を共有させて，取り組む目標を明確化できる。

また，すでに認証を取得されている企業は，さらに高い管理レベルを目指していただき，IT活用などにより，情報管理が全社の組織プロセスの効率化や自動化にも良い影響を与えることを，事例として示していただけることを期待したい。

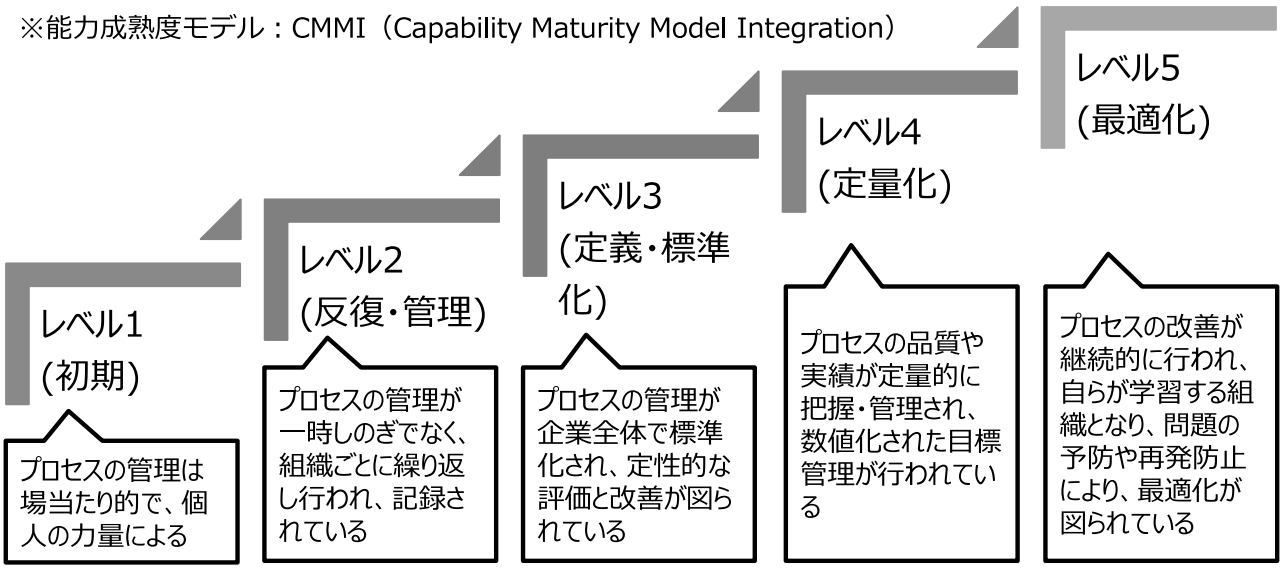


図４　能力成熟度モデルで見た組織プロセス

10）能力成熟度モデル：CMMI（Capability Maturity Model Integration）
カーネギーメロン大学ソフトウェア工学研究所（SEI：Software Engineering Institute）が，ソフトウェア開発組織のプロセスを改善するために，成熟度を計る指標として開発したCMMモデルが元になっている。その後さまざまな分野に汎用的に適用できる統合モデルとして，プロジェクト管理や人材開発などさまざまな分野で活用されている。