金型企業のためのサイバーセキュリティ実践講座　【第2回】

技術情報管理認証制度の特徴と認証取得準備のポイント

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

コロナ禍という言葉が語られ始めて約２年が過ぎようとしている今，経済や社会環境の変化が「事業の継続」に甚大な影響もたらしている。

阪神淡路大地震や東日本大地震を契機に，事業継続計画（BCP[1)]）という言葉が中小企業の中にも認知され，毎年繰り返される局地的風水害や，COVID-19の世界的感染拡大の中で，あらためて注目されている。

そして，もう一つ事業継続として無視できないものが「情報セキュリティインシデント[2)]」である。「ウイルス感染」という言葉が示す通り，目に見えない巧妙かつ心理的側面を突いて，情報の搾取や漏えいを引き起こし，企業の事業活動の生死にまで影響を及ぼすものとなっている。

また事業継続には，インシデントが発生した際の初動対応から復旧に至る危機管理対策に加えて，事前対策を中心としたリスクマネジメントの考え方と取り組みも必要となる。これらの考え方については，**表１**を参照いただくとして，今号の実践講座では，技術情報管理認証制度（以降「認証制度」と記述）の特徴をあらためて整理するとともに，認証取得に向けた準備の要点を解説する。

認証取得を目指す企業の方々の参考としていただき，まだ認証取得を考えていない企業にも自社の情報管理を見直し，認証取得を検討いただく契機となればありがたい。

表１　事業継続に必要なリスクマネジメントと危機管理の考え方

視点	リスクマネジメント	危機管理
目的	✓ 損失の最小化と収益の最大化	✓ 不測の事態発生時の適切な対応
取り組みのアプローチ	✓ リスクの特定・分析・評価（影響度と発生可能性） ✓ リスク対応(事前の対策) ✓ モニタリング及びレビュー	✓ 危機発生時の対応と平時の備え ✓ インシデントの見える化（報告の徹底と再発防止） ✓ 事業継続計画(BCP)の作成
対策	✓ リスクの低減 ✓ リスクの移転 ✓ リスクの回避 ✓ リスクの受容	✓ 初動対応 ✓ 緊急対策 ✓ 復旧対策 ✓ 再発防止策

1）BCP（Business Continuity Plan）事業継続計画：
企業が自然災害や事件・事故などの緊急事態において，損害を最小限にとどめ，中核事業の継続や早期復旧を可能とするための連絡体制や，代替の方法・手段などを取り決めた計画。

2）情報セキュリティインシデント：
マルウェアの感染やコンピュータへの不正アクセスなど，情報セキュリティに関する事件や事故のこと。

技術情報管理認証制度の特徴

前号のテーマは「サイバー攻撃から事業を守るために今すべきこと」だったが，情報管理の対象は，サイバー攻撃への防御だけとは限らない。最近も，あるマルウエア[3]の感染経路を調査した結果が報道されていたが[4]，感染のうち74％が”不正なソフトをみずからインストールしたこと”が原因とのことだった。こうした従業員の情報セキュリティ意識の低さや，内部不正による情報漏えい，情報システムの障害に伴う業務停止といった，外部からの攻撃以外の脅威にも十分目を配る必要がある。また良かれと思って行った（忖度した）例外対応が，結果として情報の漏えいにつながることもある。私の経験でも，”昔の経緯を知らずに，いつの間にか例外だったことが通常の対応になって，管理基準が曖昧になっていた”という事例を見かけることが間々ある。

こうした中，日本金型工業会（以降「金型工業会」と記述）では，昨年度から認証制度の審査機関となり，会員企業への情報セキュリティ対策のレベルアップ支援に取り組んでいる。

「認証」と聞くと，金型工業会の会員企業でも多くの企業が取得されているISO9001の品質管理の認証があり，同様に情報セキュリティ分野でもISMS認証[5]やプライバシーマーク認証[6]が知られている。また中小企業向けには，自己宣言型の「セキュリティアクション[7]」を情報処理推進機構[8]（IPA）が推進している。

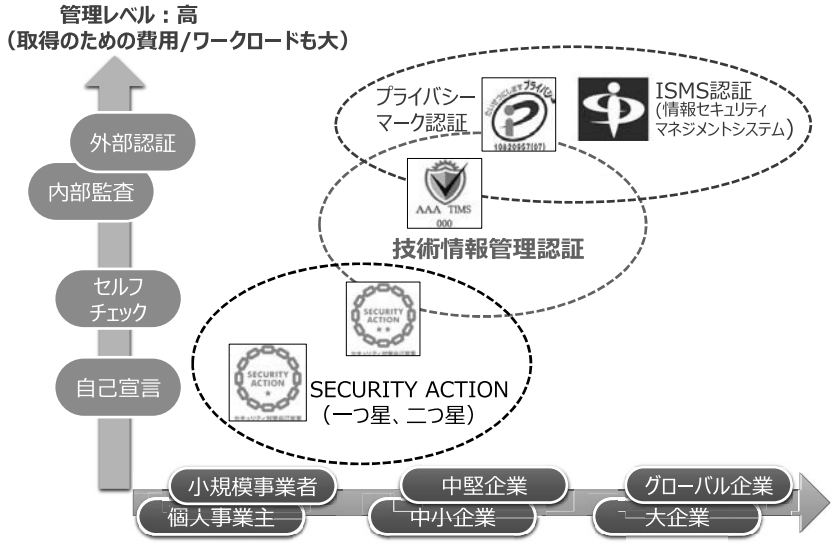


図１　情報セキュリティ分野でのさまざまな認証／自己宣言の位置付け

3）マルウェア（malware）：
英語のmalicious（マリシャス：悪意のある）にsoftware（ソフトウェア）の２つの単語が組み合わさった造語で，不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。個々の種類については，NPO法人日本ネットワークセキュリティ協会（JNSA）のURLを参照。（https://www.jnsa.org/ikusei/03/08-01.html）

4）2021年11月８日　NHKの報道「マルウエア感染の7割余不正ソフトのインストールが原因か」を指す。
（https://www3.nhk.or.jp/news/html/20211108/k10013338171000.html）

5）ISMS（Information Security Management System）情報セキュリティマネジメントシステム：
組織の情報セキュリティの目標を達成するための仕組み。リスクマネジメントプロセスを適用して情報の機密性，完全性及び可用性をバランス良く維持・改善していくことで，利害関係者にもリスクの適切な管理について信頼を与える。

6）プライバシーマーク制度：
日本産業規格「JIS Q 15001個人情報保護マネジメントシステム―要求事項」に適合して，個人情報について適切な保護措置を講ずる体制を整備している事業者等にプライバシーマークを付与し，事業活動に関してその使用を認める制度。

7）セキュリティアクション（SECURITY ACTION）：
中小企業自らが，情報セキュリティ対策に取り組むことを自己宣言する制度。IPAが推進しているが，対策状況等をIPAが認定するものではない。

8）情報処理推進機構（IPA: Information-technology Promotion Agency, Japan）：
経済産業省所管の独立行政法人で，情報セキュリティ，IT人材の育成，ソフトウェアエンジニアリングなど，IT分野における国家レベルの計画やビジョンに盛り込まれた各種事業に取り組んでいる。

これらと今回の認証制度との位置付けを，企業規模と取得の難易度を軸として**図１**にまとめてみた。

あくまでも概念図だが，この制度は，中小・中堅企業にとって比較的負荷を掛けずに，国の認証を取得できるものと位置付けることができる。

一方で，この認証基準が「企業や顧客の情報資産を守り，外部の関係者に対して，情報セキュリティの取り組みレベルの高さを示すのに十分なものか」という点で見ていくと，以下の特徴が挙げられる。

【技術情報管理認証制度の特徴】

１．基礎的な事項として定めるもの
- ①　適切な管理をする必要がある技術情報の見極め（特定）をすること
- ②　選択制の措置のうち必要な措置を決定すること
- ③　責任者を置くこと
- ④　情報へのアクセス管理を実施すること

２．具体的な措置の中で選択制とするもの
- ①　保管容器や立入制限区域の物理的強度
- ②　警備体制等のソフト面での対応
- ③　情報システムのセキュリティの確保　等

３．基礎的なレベルのものからハイレベルなものまでを列挙し，基準を参照しつつ，ステップアップをしていくことが可能なこと

「選択制」や「ステップアップ」という言葉から分かる通り，企業が置かれた環境に応じて，取るべき施策を選択しながら，少しずつセキュリティレベルを高めていくことができ，一般的な認証制度で見られるような，基準として設定されたバーを最初からすべてクリアすることは求められていない。この点が，中小企業にとっても取り組みやすく，また一定のセキュリティレベルにあることを対外的に示せることから，制度として有効なものと言える。

準備作業のスタートにあたって

認証取得を目指すに当たっては，やみくもにスタートするのではなく，以下の要件について十分な検討が必要となる。

- ●　認証取得目的／目標の明確化と全従業員の理解
- ●　認証は取得して終わりではなく継続的に改善
- ●　経営層や管理者層のリーダーシップ

これらの検討を踏まえた上で，金型工業会に認証審査の申し込みを行い，準備に入ることになるが，ここでも他の認証機関にはない金型工業会のユニークな取り組みがある。つまり“落とすための審査”ではなく，“会員企業の情報セキュリティレベルを底上げする”という方針のもと，指導助言業務と認証審査業務とをセットで提供しており，前段の指導助言業務では，専門家による伴走型の支援により，会員企業の実情に即した準備ができる。

表２は，後述するチェックシートの考え方に沿って主な準備項目を挙げたものだが，専門家の指導助言を受けるに際しておすすめしたいのは，その前提とも言える「自らの事業活動を俯瞰的に眺め，情報の流れを整理しておく」ことである。

日々の事業活動の中に登場する関係者（部門）と，大まかな情報の流れを図示し，どこでどんな情報管理が必要かを整理し，認識を共有化することで，チェックシートに記入する際に，評価の対象範囲や現状について見落としを減らすことができる。

参考までに**図２**に，私が昨年度の指導助言業務で用いたものを，一般的な製造業に汎用化してみたので，自社の状況，環境に置き換えてみていただき，事前の現状把握を進めていただきたい。

この図の中で特に意識したいのは，図中の矢印

表２　準備作業として取り組む基本的な項目

項目	認証審査の準備作業として取り組む基本的な項目
1	重要技術情報を特定して、識別できるようにすること
2	情報管理の責任者や担当者を定め、組織横断型の推進体制を設けること
3	情報管理に必要な以下の項目について、規程や手順などを定め、運用に必要な様式類を用意すること *情報の入手から廃棄に至るプロセス *情報の保管とアクセス制限 *万一事故が発生した際の対応 *外部の委託先に求めること
4	上記1～3についての役員、従業員への教育計画を作成しておくこと

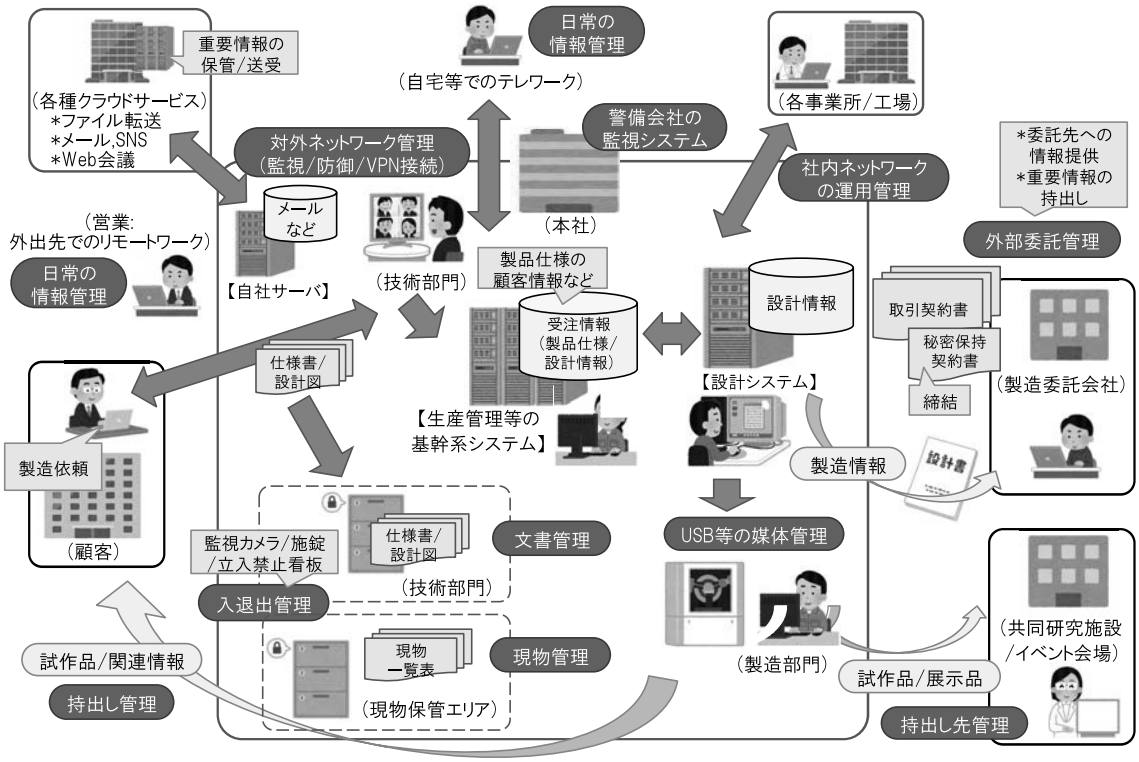


図２　企業を取り巻く情報/現物の流れの俯瞰図

表３　重要技術情報の考え方

重要情報として取り扱う必要があるもの		具体的な技術情報の例
一子(一家)相伝とされるもの		金型の設計図や試作品
製品を分析しただけでは模倣が難しいもの		製造装置や製造プロセスに関する情報
特許等で権利化しても対応が難しいもの	⇔	研究･開発情報
取り扱い者を限定する必要があるもの		顧客や取引先から預かった技術情報
常に正確な内容で保管･更新が必要なもの		製造や業務に関するマニュアル類
		技術者が持っているノウハウ

で表現した情報の流れにおいて,

① どんな重要情報がやり取りされているか,

② 情報へのアクセス制限ができているか,

③ 顧客や業務委託先間のやり取りは決まったルールで行われているか,

という点である。これらについては後述のチェックシートにおいても，確認すべき点として必須項目に挙げられている。

以下に,「①どんな重要情報がやり取りされているか」について少し掘り下げてみたい。

情報管理に初めて手を付ける企業が，準備フェーズで最初に検討しておくことは，重要情報をどこまで絞り込むかという点である。例えば，認証制度の目的である「重要技術情報」に限定するのか，この際だからと「従業員などの個人情報」や「業務で使用している各種重要情報」も含めた会社全体の情報管理にまで範囲を拡げるのかによって，対策の検討や実施の負荷は大きく変わってくる。

また「重要技術情報」といっても内容や考え方は**表３**のようにさまざまであり，企業によってその重要度や守るべき優先順位は異なる。

管理の対象を拡げることは容易だが，拡げるほどに日常の業務負荷や対策に必要な投資は大きくなる。この点を考慮すると，冒頭に述べた「事業継続」の観点から“これだけは失ってはならない情報”に絞って認証取得に臨むのも一案かと思う。ま

たこのアプローチは，“段階的にレベルアップしていく”という認証制度の特徴を活かした効果的な取り組みとも合致している。

一方，社内の情報管理がすでに仕組みとして運用されている企業にとっては，“重要技術情報の管理と，従来から運用している情報管理との整合性をどう取るか”という点が最初に検討するポイントになる。これは，情報管理の推進体制や規程・ガイド類の整合性などにも関係してくるが，例えば「情報管理台帳」でも，記載する個々の情報の管理項目の過不足や，「機密・社外秘・一般」といった管理レベルの考え方を，既存のものに合わせるか，さらに高度なレベルを設定するかなどの細かな検討も行う必要がある。

通常は“従来の運用で足りない部分を補足する”考え方で検討を進めることになると思われるが，金型工業会ではこうした検討に役立つひな形を用意しているので，参考にしていただきたい。

②のアクセス制限と③の自社以外との情報のやり取りのルールについては，企業の規模や環境によって検討の対象範囲が異なるが，細かく見ていくと以下の視点から現状整理と共通認識が望まれる。具体的な確認事項や対策の検討ポイントについては，次号で解説したい。

②：敷地／建物，共有スペース／事務室／秘密情報保管室，日中／夜間／休日，入退出のチェック方法／監視／記録，正社員／派遣社員／パート社員，顧客／業務委託・協力会社社員／来訪者／見学者／不審者，本社／国内事業所／社外／自宅／海外，自社施設内システム／クラウドサービス，ネットワーク／データ／ログインID／パスワード，不正アクセスの監視／検知／防御／記録

③：子会社／関連会社等のグループ企業，顧客／仕入先／外注先（二次請け，三次請け），共同研究先／イベント・展示会主催者，秘密保持の契約書／誓約書，書類／試作品／電子情報の受け渡し方法の取り決め，情報漏えい等の発生時の報告義務／定期的報告／必要時の監査

金型工業会で使用されるチェックシートの特徴

次にチェックシートの構成について見ていく。

認証審査で用いるチェックシートは詳細項目まで含めると200項目を超えるが，そのほとんどは各企業特有の環境に応じた選択項目であり，実際の認証審査も，基本的には必須の15項目について行われるので，チェックシートを埋める作業負担はさほど大きくない。

指導助言業務の最初に，必須項目の15項目についてセルフチェックを行うことからスタートし，その結果を指導助言の担当専門家と認識を共有し，認証審査の実施までに必要な対策を取り，運用フェーズに入れるよう準備を進めていく。

チェックシートにおいても独自の工夫があり，専門家によって判断のバラツキがないように，個々のチェック項目ごとに適合可否の判断基準が明記され，公平な審査を受けることができる。またその判断基準は，本番の認証審査で用いるチェックシートと同様で，以下の二つの視点から記述されている。

① 情報管理に関する組織体制や規程・ガイド類の整備状況などの形式要件について

② 形式要件の内容が正しく運用されているかという，具体的な運用管理状況について

※実際に運用管理できていることを示す記録や，運用管理システムの稼働状況に加え実際のオフィス，工場の入退出管理の状況などを現場で確認する。

審査をする側の立場で見ると，「最低限の形式要件が整えられているか」という点は，認証審査を受ける上でのスタートラインとなる。したがって情報管理をゼロからスタートする企業においては，金型工業会にて用意された各種のひな形ファイルを活用して，まずは形式要件を整えることが必要不可欠であるが，「規程やガイドはあるけれど，作りっぱなしで現状に合っていない」，「規則が形式的過ぎて実際には守られていない（運用できていない）」という状況に陥らないよう考慮が必要である。

私が経験した中でも，作成して以降，一度も改定されていない規程があり，その結果，複数の規程やガイドの間で整合性が取れなくなってしまったという実例も目にしている。また審査時には，

形式要件が具体的に運用管理できていることを示すことになる。その完璧さは求められないものの，対策のレベルアップを課題として，順次改善していく考え（計画）があることの確認は求められる。

特に審査時には，“現場の環境に合わせて無理なく効率的に運用できているか”（運用開始前であれば「できそうか」）という継続性の視点が重要となる。例えていうと，達成レベルをある時点の瞬間風速で見るのではなく，一定期間の平均風速が一定レベルに達しているかという視点で見ていることになる。

また今年度は新たに，金型事業と関係の深い一般社団法人自動車工業会，一般社団法人自動車部品工業会（以降「自工会／部工会」と記述）が作成した「サイバーセキュリティガイドライン」のチェックシート50項目との整合性を確認し，金型工業会のチェックシートの適合判断基準に取り入れている。

言い換えると，認証を取得することは，基本的には自工会／部工会のチェック項目を満たしているレベルということになる。もちろん自工会／部工会のガイドラインは「認証」ではなく，企業がセルフチェックとして活用するためのものなので，あくまでも一つの考え方としてご理解いただきたい。

また今回発表された50項目は基本的レベルを記載したもので，今後継続的にレベルの高いチェックシートを追加していく計画が示されている。このことから金型工業会としても，認証取得された企業のフォローアップ支援[9)]を計画するなどの，継続的なレベルアップの支援体制がますます必要となる。

経営者のリーダーシップが必須要件

今号の最後に，情報セキュリティ対策における経営者のリーダーシップについて触れておきたい。

一般に，情報セキュリティ対策は「組織的」，「人的」，「物理的」，「技術的」の４つの視点から語られるが，チェックシートの必須15項目においても，

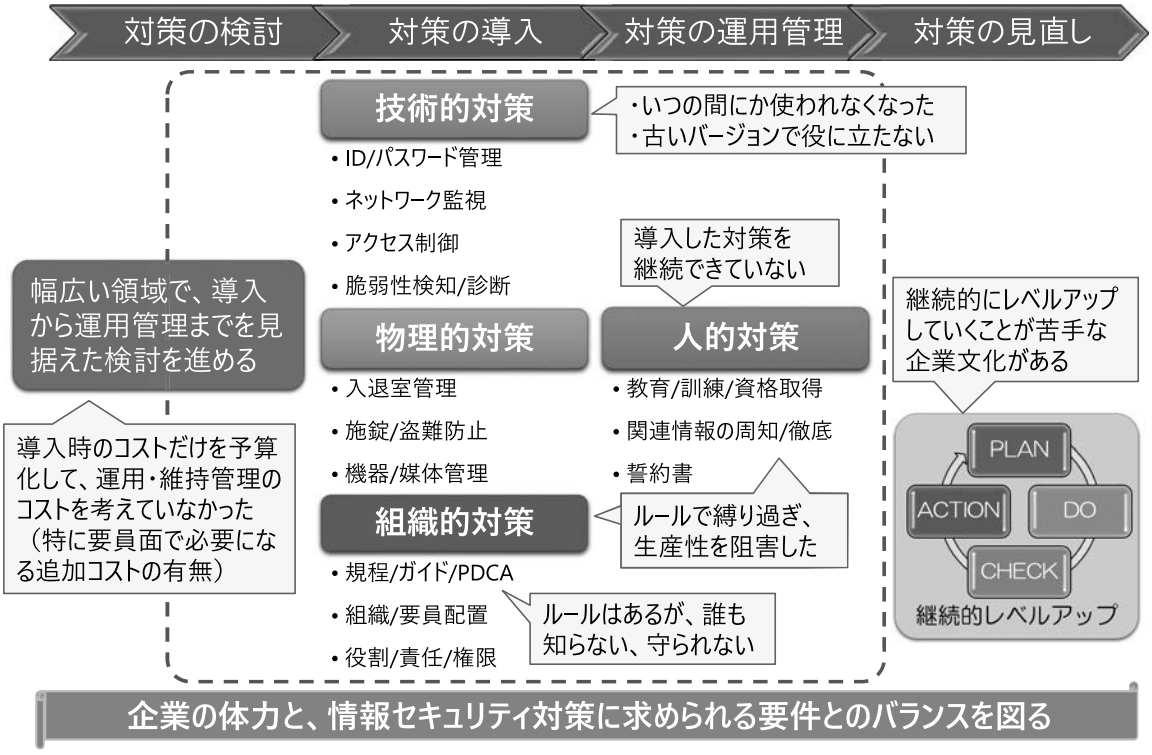


図３　情報セキュリティ対策の取り組み全体図

9）フォローアップ支援：
金型工業会では３年後の更新審査を意識した対策として，今年度，専門家の２回の訪問指導によるフォローアップ支援を実施している。

これらの視点で確認が求められている。

一方で**図３**の吹き出しに示したように，対策を打ってはみたものの，その実効性を高めていくには多くの取り組み課題がある。そして，取り組み課題のすべてに関わるのが経営者のリーダーシップである。

「組織的対策」における，部門横断的な委員会の設置や，規程・ガイド類の整備に加えて，さまざまな「技術的対策」について，自社に必要かの投資判断が求められる。

サイバー攻撃という点では，どこまで技術的な防御機能を高めているかの「技術的対策」に目が向くが，費用とのバランスで高い技術レベルの対策を継続して運用できるかも，経営者の投資判断のポイントとなる。特に製造業では，前述したようにネットワーク上のサイバー空間だけでなく，工場や事務所などの施設全体における「物理的対策」にも同様の投資判断が求められる。

また，さまざまな組織的，技術的，物理的の各対策をとっても，従業員が運用できなかったり，知らなかったりではせっかくの投資が活かされない。この観点は「人的対策」として，全従業員だけでなく，役員を含む全員の意識と知識を高めていくことが必須であり，この面においても，経営者の理解と自ら率先して取り組むことが必須となる。

経営者の皆様には，このような合わせ技での対策で実効性を高めていくことについて，理解と実践をお願いしたい。

以上，認証取得の準備について解説したが，次号では，前述の②情報へのアクセス制限ができているか，③顧客や業務委託先間のやり取りは決まったルールで行われているか，について触れるとともに，情報管理の段階的レベルアップの考え方についても，成熟度モデルをもとに解説できればと思う。

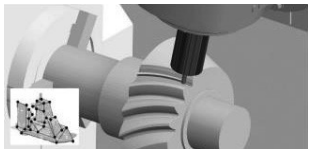
DMG森精機，「デジタルツインテストカット」にスーパーコンピュータ「富岳」の利用を開始

DMG森精機㈱は，工作機械のテスト加工をデジタル化する「デジタルツインテストカット」の計算処理に「富岳」を利用した高速化を実現した。

2021年２月より開始した「デジタルツインテストカット」は，実際の加工における工作機械の動的な稼働状態をコンピュータ上で再現し，サイクルタイムをはじめとする加工結果を算出する技術で，最短２営業日で加工結果を回答する。しかし，複雑な曲面で構成されるブレードや金型などは解析時間が長くなる傾向にあった。

そこで理化学研究所のスーパーコンピュータ「富岳」にデジタルツインテストカットを実装することによって，実際には８時間かかる加工を98%削減する10分で結果を算出することを可能にした。


実機でのテストカット


デジタルツインテストカットのイメージ図

切込み2mm×1刃当り送り量2mmを可能にした荒加工用工具

㈱MOLDINOは，荒加工用工具アルファ高送りラジアスミル「TR4F」に“5000形”のラインアップを追加し，2021年12月20日より発売を開始した。

同社は2020年４月に金型の荒加工用に，独自の工具設計により一刃送り2mm以上の高送り加工を実現したアルファ高送りラジアスミル「TR4F4000形」を発売した。その中で，TR4F4000形の最大軸方向切込み量1.2mmに対して，より切込み量を大きく取れる工具のニーズも明らかになったことから，インサートサイズを従来の12タイプから15タイプに拡大した刃先交換式荒加工用工具「アルファ TR4F5000形」を開発した。

「TR4F5000形」は，広い断面積と拘束面積を持つ独自のインサート形状により，切込み量2mmでも一刃当りの送り量2mmを超える高能率荒加工が可能。また独自の不等分割方式，切り屑排出性を高めたボディ形状などの採用により，切削時のビビり振動，突き出し量の長い金型形状部加工での切り屑詰まりなどを抑制。ダイカスト金型や樹脂金型，プレス金型の高能率荒加工，取り代が変動しやすい鋳物ワークや肉盛り溶接材の荒加工などに効果を発揮する。

インサートは片面４コーナ仕様。ホルダ：φ63～φ125（全10アイテム），インサート：５材種（1アイテム）で，価格はホルダが￥61,820～￥129,540（消費税別）。