

ISACA 東京支部基準委員会有志（久保美香、小林清志、福田重遠、山崎雅也）

2026 年 7 月 15 日

COBIT30 周年の振り返り

2026 年は、COBIT フレームワークが誕生してから 30 年の節目にあたります。これを記念して、ISACA 国際本部から COBIT に関する寄稿記事がいくつか公開されています。

今回は、その中からマーク・トーマス氏（ISACA Hall of Fame）による「30 Things COBIT Taught Us About Governing Technology」を取り上げました。この記事に示された 30 のポイントについて、有志メンバーが特に印象に残った内容をまとめました。改めて、30 年経っても、ガバナンスの課題は簡単には解決できないものだと感じました。

要約：COBIT が伝えてきた大切なこと

COBIT が 30 年にわたって伝えてきた大切な考え方は、技術をただ管理することではありません。技術を組織や社会にとって価値あるものにするために、どのように方向づけ、活用していくかという点です。

そのためには、制度や手続きだけでなく、組織の文化、信頼関係、部門を越えた協力が欠かせません。どれほど立派なルールや仕組みを作っても、それを使う人たちの理解や協力がなければ、ガバナンスは十分に機能しません。

主なポイント

- ・ガバナンスは、組織が進むべき方向を示すものです。一方、マネジメントは、その方向に向かって実行することです。
- ・ルールやチェックリストだけに頼りすぎると、形だけの管理になり、本来の価値を生みにくくなります。
- ・文化、行動、信頼といった目に見えにくい要素が、実はガバナンスを支える大切な土台になります。
- ・透明性や倫理といったデジタルトラストは、後から追加するものではなく、最初から仕組みに組み込む必要があります。
- ・各部門が別々に動くのではなく、組織全体で価値を生み出すことが重要です。

今も繰り返されている課題

COBIT は長い間、ガバナンスの重要性を示してきました。それでも、多くの組織では同じような問題が今も起こっています。

その理由の一つは、組織が目に見えて管理しやすいものに頼りがちだからです。たとえば、ルール、手続き、チェック項目は確認しやすく、管理しているように見えます。しかし、それだけでは本当の意味でのガバナンスにはなりません。

本来大切なのは、組織の中で信頼を築き、関係者が協力し、同じ目的に向かって動けるようにすることです。役割や責任を明確にすることも必要ですが、それが責任の押し付け合いや部門間の壁になってしまつては逆効果です。ガバナンスは、組織全体で価値を生み出すための仕組みとして考える必要があります。

AI 時代に必要な考え方

AI が広がる時代には、ガバナンスも変化に合わせて見直していく必要があります。決まったルールを守るだけでなく、技術の変化、組織の状況、人々の行動に合わせて、継続的に改善していくことが大切です。重要なのは、統制を増やすことではありません。信頼を高め、部門同士が協力しやすくし、組織の中の無駄な摩擦を減らすことです。よいガバナンスとは、組織がより速く、より安全に、そしてより価値のある判断をできるようにするための仕組みです。

※.参照記事

30 Things COBIT Taught Us About Governing Technology



May 29, 2026

Guest Author: Mark Thomas, CGEIT, CRISC, CDPSE, AAIR, COBIT Assessor |
President, Escoute LLC | ISACA Hall of Fame

Thirty Years. Three decades of helping organizations stop treating technology like a magic box and start governing it like the strategic asset it actually is. [COBIT](#) turns 30 this year, and if you've spent any meaningful time in this profession, the framework has almost certainly shaped how you think whether you realize it or not.

I've been working with COBIT since the days when "governance" meant a binder on a shelf and "alignment" meant IT got invited to the budget meeting once a year. So, in honor of the anniversary, here are 30 things COBIT has taught us about governing technology: lessons that have aged remarkably well as the world around us has changed beyond recognition.

1. Governance and management are not the same thing. One sets direction. The other executes against it. Confusing the two is how organizations end up with boards approving sprint backlogs and CIOs setting risk appetite.

2. Technology doesn't deliver value. Decisions about technology deliver value. The platform isn't the win. What you choose to do with it is.

3. Every framework needs a tailoring step. COBIT out of the box is a buffet, not a meal. The discipline is in choosing what to put on the plate.

4. If you can't measure it, you can't govern it. And if your metrics only measure activity instead of outcomes, you're governing the wrong thing.

5. Risk and value are two sides of the same coin. You don't manage one without the other. Pretending otherwise is how organizations end up with bulletproof security and irrelevant products.

6. Interested parties have needs. Those needs cascade. From enterprise goals to alignment goals to governance and management objectives, the cascade isn't bureaucracy – it's the connective tissue that keeps strategy from dying in translation.

7. RACI charts are not a substitute for accountability. They're a tool for clarifying it. If your RACI has eight people marked "A" on a single decision, you don't have accountability, you have a committee.

8. Process capability is a journey, not a destination. Level 5 isn't the goal for every process. The goal is the right level for the value at stake.

9. Culture eats process for breakfast. I've watched million-dollar process redesigns get steamrolled by a single executive who refuses to follow them. COBIT's behavior and culture components exist because the soft stuff is the hard stuff.

10. Information is an asset. Treat it like one. That means lifecycle, ownership, classification and accountability – not just storage.

11. People are a governance component, not a resource. Resources are consumed. People are developed.

12. Services, infrastructure and applications are interdependent. Govern them in silos and you'll get siloed outcomes.

13. Principles, policies and frameworks are different things. Principles are timeless. Policies are situational. Frameworks are structural. Mixing them up is how you end up with a 400-page policy that nobody reads.

14. The board isn't the audience for your control catalog. They're the audience for outcomes, exposures and trade-offs. Save the control IDs for the auditors.

15. Audit is not governance. Audit verifies governance is working. The two are confused constantly, and it's been to the detriment of both professions.

16. Compliance is a floor, not a ceiling. If your governance program's ambition is "pass the audit," you're already losing.

17. Strategic alignment isn't a slide deck. It's a continuous practice of making sure technology decisions and enterprise decisions are pointed at the same goals. The day you stop doing it is the day they start drifting apart.

18. The business doesn't want IT alignment. It wants outcomes. Stop trying to get a seat at the table and start serving the meal.

19. Frameworks don't fail. Implementations fail. When someone tells you, "We tried COBIT and it didn't work," what they usually mean is "We copied a template and skipped the thinking."

20. Governance scales down. It's not just for *Fortune* 500 companies. A 50-person organization needs governance too — it just looks different.

21. Design factors matter. The same problem in two different organizations almost never has the same answer. Industry, threat landscape, risk appetite and enterprise strategy all change the math.

22. You can't outsource accountability. You can outsource execution. You can outsource operations. You cannot outsource the consequences of a bad decision.

23. The Three Lines aren't a turf war. They're a system of checks designed to keep the enterprise honest with itself.

24. Continuous improvement requires continuous feedback. Annual reviews are not continuous. They're annual.

25. Technology changes outpaces governance, every time. The job isn't to keep up. It's to build governance that's adaptable enough to absorb change without

breaking.

26. Digital trust isn't a feature. It's a consequence. It's what happens when governance, security, privacy, quality and ethics are all working together. You don't bolt it on; you build toward it.

27. AI didn't invent new governance problems. It just made the old ones impossible to ignore. Accountability, transparency, bias oversight — these were on the agenda long before generative AI showed up, but in today's environment it's critical to stop ignoring these problems now.

28. Governance without ethics is just compliance theater. Doing what's allowed and doing what's right are not always the same thing. The framework points the way, but the judgment is human.

29. A framework is a map, not the territory. COBIT will not tell you what to do. It will tell you what to think about. The difference matters.

30. The best governance is invisible. When it's working, nobody notices. When it's broken, everyone does. That's the standard.

Thirty years in, COBIT has become a key way of thinking about how technology creates and protects value at enterprise scale. The specific objectives will keep evolving. The underlying discipline — clarity of purpose, accountability, measurement and continuous improvement — won't.

Happy birthday, COBIT. The next 30 years are going to be even more interesting!

< 日本語訳 >

以下、日本語訳です。

この 30 年間、COBIT は、組織がテクノロジーを「魔法の箱」のように扱うのをやめ、実際には戦略的資産であるものとして、適切にガバナンスすることを支援してきました。COBIT は今年で 30 周

年を迎えます。この分野で一定の経験を積んできた人であれば、自覚しているかどうかにかかわらず、COBIT はほぼ間違いなく、その考え方に影響を与えてきたはずです。

私は、「ガバナンス」といえば棚に置かれた分厚いバインダーを意味し、「整合性」といえば IT 部門が年に一度だけ予算会議に呼ばれることを意味していた時代から、COBIT に関わってきました。そこで、この節目を記念して、テクノロジーをガバナンスするうえで COBIT が私たちに教えてくれた 30 のことを紹介します。これらは、私たちを取り巻く世界が見違えるほど変化した今でも、驚くほど色あせない教訓です。

1. ガバナンスとマネジメントは同じものではありません。

一方は方向性を定め、もう一方はそれに沿って実行します。この二つを混同すると、取締役会がスプリントのバックログを承認したり、CIO がリスク選好を決めたりするような組織になってしまいます。

2. テクノロジーそのものが価値を生むものではありません。テクノロジーに関する意思決定が価値を生むのです。

プラットフォームを導入すること自体が成功ではありません。それを使って何をするかが重要です。

3. どのフレームワークにも、自組織に合わせて調整するステップが必要です。

COBIT は完成した料理ではなくビュッフェのようなものです。大切なのは、皿に何を選んで載せるかを見極めることです。

4. 測定できなければ、ガバナンスすることはできません。

そして、指標が成果ではなく活動量だけを測っているなら、ガバナンスしている対象を間違えています。

5. リスクと価値は、同じコインの表裏です。

片方だけを管理することはできません。そうでないふりをすると、堅牢なセキュリティはあるのに、誰にも必要とされない製品を持つ組織になってしまいます。

6. 利害関係者にはニーズがあり、そのニーズは段階的につながっていきます。

企業目標から整合目標、さらにガバナンス目標やマネジメント目標へとつながる流れは、官僚的な手続きではありません。戦略が現場に伝わる途中で意味を失わないようにするための、組織をつなぐ組織的な筋道です。

7. RACI チャートは、説明責任の代わりにはなりません。

それは説明責任を明確にするための道具です。一つの意味決定に対して「A (Accountable)」が 8 人もいるなら、それは説明責任ではなく、委員会です。

8. プロセス能力は、到達点ではなく継続的な道のりです。

すべてのプロセスでレベル 5 を目指す必要はありません。重要なのは、対象となる価値に見合った適切なレベルを目指すことです。

9. 文化はプロセスに勝ります。

私は、数百万ドルをかけたプロセス再設計が、それに従おうとしない一人の経営幹部によって押しつぶされるのを見てきました。COBIT に行動や文化の構成要素が含まれているのは、「ソフトな要素」こそが実は最も難しいからです。

10. 情報は資産です。資産として扱うべきです。

それは、単に保存するだけでなく、ライフサイクル、所有者、分類、説明責任を考えるということです。

11. 人はガバナンスの構成要素であり、単なる資源ではありません。

資源は消費されますが、人は育成されるものです。

12. サービス、インフラ、アプリケーションは相互に依存しています。

それらをサイロごとにガバナンスすれば、結果もサイロ化します。

13. 原則、方針、フレームワークはそれぞれ異なるものです。

原則は時代を超えて有効であり、方針は状況に応じて変わり、フレームワークは構造を与えるものです。これらを混同すると、誰にも読まれない 400 ページの方針書ができあがります。

14. 取締役会は、統制項目の一覧を見る相手ではありません。

取締役会が見るべきなのは、成果、リスクへのさらされ方、そしてトレードオフです。統制 ID は監査人のために取っておきましょう。

15. 監査はガバナンスではありません。

監査は、ガバナンスが機能しているかを検証するものです。この二つはしばしば混同され、その結果、どちらの専門職にとっても不利益となってきました。

16. コンプライアンスは最低ラインであり、上限ではありません。

ガバナンスプログラムの目標が「監査に合格すること」だけであれば、その時点ですでに負けています。

17. 戦略的整合性は、スライド資料ではありません。

テクノロジーに関する意思決定と企業としての意思決定が、同じ目標に向かっているかを継続的に確認する実践です。それをやめた瞬間から、両者はずれ始めます。

18. 事業部門が求めているのは、IT との整合ではありません。成果です。

「テーブルにつく席」を得ようとするのではなく、食事そのものを提供することを考えるべきです。

19. フレームワークが失敗するものではありません。導入の仕方が失敗するのです。

「COBIT を試したがうまくいかなかった」と言う人が本当に意味しているのは、多くの場合、「テンプレートをコピーして、考えることを省略した」ということです。

20. ガバナンスは小規模組織にも適用できます。

Fortune 500 企業だけのものではありません。50 人規模の組織にもガバナンスは必要です。ただし、その形は異なります。

21. 設計要因は重要です。

同じ問題であっても、組織が違えば、同じ答えになることはほとんどありません。業界、脅威の状況、リスク選好、企業戦略によって、答えは変わります。

22. 説明責任は外部委託できません。

実行を外部委託することはできます。運用を外部委託することもできます。しかし、悪い意思決定の結果を外部委託することはできません。

23. 3 線モデルは縄張り争いではありません。

それは、企業が自らに対して誠実であり続けるために設計されたチェックの仕組みです。

24. 継続的改善には、継続的なフィードバックが必要です。

年次レビューは継続的ではありません。ただ年に一度行われるだけです。

25. テクノロジーの変化は、常にガバナンスを上回る速さで進みます。

重要なのは、その変化に追いつくことではありません。壊れることなく変化を受け止められる、適応力のあるガバナンスを構築することです。

26. デジタルトラストは後付けできる機能ではない。結果です。

ガバナンス、セキュリティ、プライバシー、品質、倫理がすべて連携して機能したときに生まれるものです。後から取り付けるものではなく、そこに向けて作り上げるものです。

27. AI は新しいガバナンス課題を生み出したわけではありません。

これまでの課題を、無視できないものにしただけです。説明責任、透明性、バイアスの監督といった課題は、生成 AI が登場する前から存在していました。現在の環境では、これらの問題をこれ以上無視しないことが重要です。

28. 倫理を欠いたガバナンスは、単なるコンプライアンスの見せかけにすぎません。

許されていることと、正しいことは、必ずしも同じではありません。フレームワークは方向を示しますが、判断するのは人間です。

29. フレームワークは地図であり、現実そのものではありません。

COBIT は何をすべきかを直接教えてくれるものではありません。何について考えるべきかを示してくれるものです。この違いは重要です。

30. 最も優れたガバナンスは、目立ちません。

うまく機能しているとき、人はそれに気づきません。壊れているときには、誰もが気づきます。それが基準です。

30 年を経て、COBIT は、企業規模でテクノロジーがどのように価値を生み出し、守るのかを考えるうえで、重要な考え方となりました。具体的な目標はこれからも進化し続けるでしょう。しかし、その根底にある規律——目的の明確化、説明責任、測定、継続的改善——は変わりません。

誕生日おめでとう、COBIT。次の 30 年は、さらに興味深いものになるでしょう。