

安全の視点から見た データ改ざん問題への提案

向殿 政男 Masao Mukaidono
明治大学 名誉教授

1 はじめに

大手企業によるデータの改ざん問題が最近、新聞や雑誌紙上ににぎわしている。「我が国のモノづくりの現場が劣化しだした」とか、「いや、昔から現実には行われていたものが最近騒がれてきたにすぎない」、などいろいろな見方がある。しかし、どんな理由があっても、データを改ざんすることは契約違反であり、コンプライアンス違反である。顧客や社会からの信頼を喪失させる重大な事態であることは間違いがない。品質管理の面、また管理体制の面、更には人材育成の面からなど、いろいろな視点から原因と対策の議論をすることができるとは思われるが、ここでは、安全の視点を中心に眺めてみることにする。

2 データ改ざんの現状について

データ改ざん、いわゆるデータの書き換え、データ偽装、又はデータねつ造、更にはデータ隠蔽等の問題には、国会で問題にされている森友学園への国有地払下げ問題や防衛省のイラク派遣日報問題等の政府レベルから、健康食品の過大広告の消費者レベルまで、実に幅広いものがある。ここでは、素材メーカーがアルミ素材の品質データを顧客の基準に達していなかったにもかかわらず、合うようにデータを改ざんして出荷した問題、自動車メーカーが完成検査で無資格者に検査をさせて資格者の印を押させて出荷した問題、などのモノづくりを中心に最近話題になっている問題について考えてみることにする。なお、ここでのデータ改ざんとは、契約、標準、法規等に存在する基準に対して、適合していなくてもあたかも適合しているかのようにデータを書き換え

て、顧客には不適合がないように伝えることを意味している。これらの問題は、悪くすると人命に関わるような安全問題につながる可能性を含んでいる。

データ改ざんが、会社内のどのレベル、どの範囲で行われていたかは重要である。個人レベルで行われる場合もあるだろうが、現実には、会社内の担当グループのレベル、部・課レベルで行われており、時には会社レベルで行われている場合もある。また、短期的につじつまを合わせるためにデータを改ざんしたのか、長期的に継続して行われていたのかの違いもある。今回問題になっているのは、個人のレベルでもなく、短期的なものでもない。さらに、データ改ざんを行っていたレベルとも関係するが、この事実を経営トップは知っていたのか、トップに報告されていたのかも、原因を究明し再発防止策を立てるためには重要なキーポイントとなる。トップが全く知らないうちにある部署で

長年慣行として行われていたとすれば、社長にとっては一種のサイレントチェンジ（知らない間に実質が変わっていた）かもしれないが、知らなかったでは当然済まされない。企業トップは、それを許してきたマネジメントの責任を負わなければならないからである。

素材メーカーの場合を見てみよう。長期的かつ広範囲にデータを改ざんして基準を満たしていない不適合品を出荷していた。不適合品出荷先は 688 社、改ざんをしていた事業所・子会社は 19 拠点に及ぶとされている。また、長年慣習として行われていて、担当部署を経由して役員になった人も含めて役員のうち 3 人は、データ改ざんの事実を認識していたといわれている。アルミニウムのような素材の場合は、多くの企業で使用され、最も厳密な基準を要求するところもあれば、そうでないところもある。一般的には最も厳しい基準に合わせて製造し、一般の顧客企業ともその基準で契約する。しかし、現実には、その基準を満たすことが技術的にも価格的にも難しい場合には、その顧客企業に個別に相談をして、基準以下であるが使用には問題ないかを確認し、問題ない場合には、基準を満たしていないが出荷することを認めてもらう手続きを踏んで出荷する（トクサイ：特別採用）。現実には問題がないのであれば、毎年同じ手続きをするのが面倒であるなどの理由から、データの方を改ざんして、顧客企業に内緒でそのまま出荷してしまう、すなわち、

データ改ざんの発生である。基準の方を変えてもらうなり、トクサイの手続きをすれば済む話なのであるが、この不正行為がコンプライアンス上、及び、顧客企業からの信頼を得る上で、いかに間違っていたことであるかに気が付かないところに大きな問題がある。

自動車メーカーの無資格者による完成検査の問題も長い間、広く実行されていた。国内にある六つの完成車工場で資格をもたない従業員が完成車の検査をしていた。これは明らかに法律違反であった。なぜ、このようなことが日常的に行われるようになったのであろうか。もともと、大きな製品の製造では、各部品が製造過程で厳密に仕様どおりにつくられているか否かが検証（verification）されており、それらの全ての部品が組み合わさって最終的に完成品が出来上がるのであるが、その最終製品に対して本当に顧客の要求仕様を満たしているかどうかの妥当性確認（validation）が行われるのが普通である。特注品のように一品生産の大型機器や、大規模なソフトウェアシステムの制作などの場合には、この検証、妥当性確認のステップは必須であるが、自動車のようなライン生産に基づいた大量生産品では部品の段階でほとんど問題がなくなっており、完成品を改めて検査する必要が少なくなっている。事実、自動車の場合、我が国ではこの両検査を要求しているが、国によっては最終的な検査は必要としていない。現実には、最終段階で不具合が見つかる

ことはほとんどなく、必要性を実感していなかったのではないかなと思われる。安全性には問題がないと認識して、最後の検査が軽く見られ、法律で決められているから実施しているようなところがあり、資格のない従業員が検査することになったと思われる。それを有資格者のハンコを使って検査書類に押印していた。これは明らかに偽装であり、法律違反である。本当に、完成検査が不必要と思うならば、科学的根拠のもとに国に規制解除等を提案するのが本筋であろう。

ここでは、二つのデータ改ざんの例を紹介したが、現実には同じようなことが多くの分野で行われているのではないだろうか。データ改ざんの問題には、それぞれ個別の原因もあるだろうが、かなり共通した日本独自の原因が、また、もしかしたら世界共通の原因が潜んでいるのかもしれないと思われる。

3 データ改ざんと安全性について

データ改ざんを安全性の面から見てみよう¹⁾。新聞等では、すぐに安全性に問題が生じて事故につながるように報道する向きもあったが、今回の場合は必ずしもそうではない。事実、データ改ざんされた材料を購入して機械設備を製造、運用していた幾つかの企業が、直ちに当社の製品の安全性には問題がないことを公表している。データ改ざん問題は、必ずし

も安全性の問題ではないのである。

データ改ざんが問題視されるためには、まず、満たすべき基準や決まりがあるはずである。安全に関する基準には幾つかの種類がある。例えば、満たさなければ事故につながりかねない安全基準がある。それ以外にも安全に関する強制基準、JIS 基準、業界基準、社内基準等がある。大ざっぱには、この順番で後ろに行くほど「厳しい内容」になっていると思われる。ここでの厳しい内容とは、「守ることが難しくなる」という意味の厳しさである。一般には、安全基準が最も厳しい基準と考えたいが、内容的には実際は逆である。安全基準は、これを満たさないと事故に直結する可能性がある（もちろん、安全係数を掛けたりして余裕はもっているのが普通だが）、これ以下の悪いデータであってはならないという意味の最低の基準である。満たすべき基準のレベルとして安全基準は緩いということになる。ただし、守ることが厳しく求められているという意味からは厳しい基準である。法律で定められている強制基準はまさにそうである。強制基準は、これを満たさないと法律違反となり、強制基準は最低基準といわれることもある。この意味からは安全基準と同じレベルか、実際にはより厳しい基準となっているのが一般的である。一方、JIS 基準は任意基準であり、これを満たしていれば通常は問題ないレベルになっていると考えられる。強制基準

が存在する場合には、JIS 基準はそれを当然、満たしていなければならないから、JIS 基準は強制基準よりも等しいかそれ以上の厳しさの内容を要求している。さらに、業界としては、JIS 基準を満たしているのは当然で、それよりも厳しい内容にすることで社会の信用を得るために、業界基準を更に厳しく定めている場合が多い。JIS 基準よりも緩い業界基準を定めていたとすると社会的に問題視されるだろう。また、一流の企業は、業界の中でも更に厳しい社内基準で対応していることをアピールすることで、取引先や顧客の信頼を得るようにしている場合がある。この場合には、社内基準は、業界基準よりも更に厳しいものになっている。この関係を図示したのが図 1 である。

この図からわかるように、通常、社内基準と安全基準の間には相当の幅というか、ゆとりがある。社内基準に対してわずかにデータ改ざんをしたからといって、現実には必ずしもすぐには安全問題につながらないのが普通である。特に、鉄鋼や材料等の素材は、非常に幅広い分野の製造メー

カに使われているので、最も厳しい要求に対応するために、社内基準はかなり厳しいものになっているのが普通である。素材を使用する製造メーカは、データ改ざんによって、納入元の社内基準や契約した基準を満たしていないことを知った場合、直ちに自分の会社の製品の安全性に問題が生ずるか否かを確認する責任と役割がある。今回問題になっている各大手企業によるデータ改ざんの中には、納入先の顧客に事情や理由等を説明して安全性等が確認してもらえば、本来、ほとんど問題にならない事柄のようである。

データ改ざんが、なぜ問題なのかといえば、それは、まず信頼問題に直結する行為だからである。社内基準だろうと何であろうとルールがある場合に、たとえ実質的に問題がなくても、ルールを破ってデータを改ざんすることは本来、不正であり、裏切りである。黙って基準に合うように改ざんするということは、信頼を裏切る行為、倫理にもとる行為、コンプライアンスに反する行為、すなわち信頼問題である。さらに、基準を守ることが契約に記されていれば

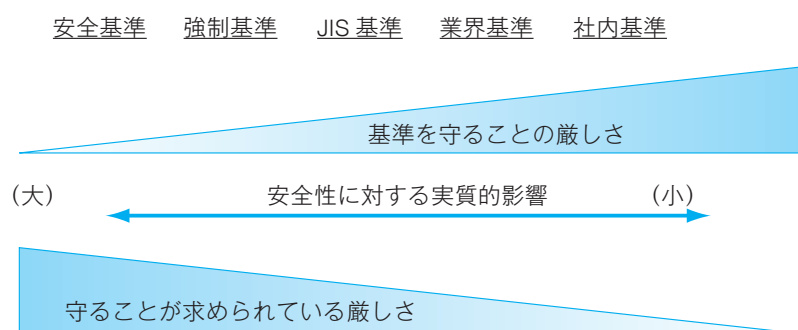


図 1 各種の安全に関する基準の関係

〔文献 1〕に基づき南波裕樹氏が作図²⁾]

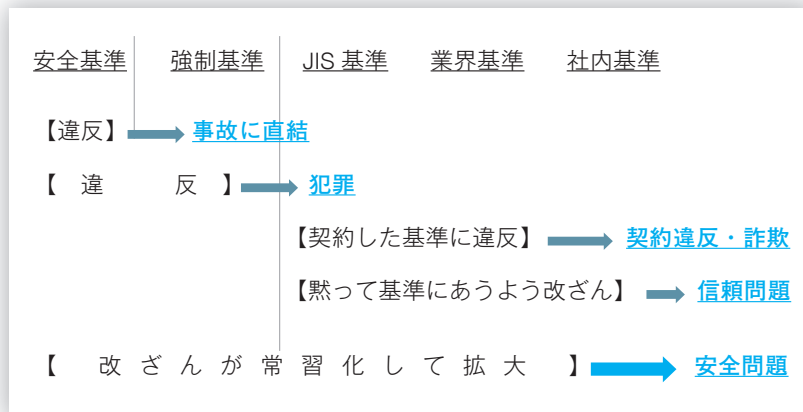


図2 データ改ざんは、契約違反、信頼問題、安全問題につながる

[文献 1)に基づき南波裕樹氏が作図²⁾]

契約違反や詐欺であり、強制基準に触れれば犯罪である。そして、データ改ざんが常習化して拡大してくるとそれこそ安全問題につながることになる（図2参照）。

4 データ改ざんの原因

なぜ、データ改ざん問題が生ずるのであろうか。ここでは、安全学³⁾に従い、組織的側面、人間的側面、技術的側面の三つに分類して、幾つかを思いつくままにリストアップしてみる。

(1) 組織的問題

- 収益性優先、高い収益目標設定
- 工程能力を超えた仕様の受注
- コスト削減圧力、生産性向上圧力、納期短縮圧力、納期厳守圧力
- 監査部門が機能していない
- 品質管理、監査等の権限を下位に委譲し、工場などに一任
- 不適合のときの責任、権限等が不明確
- 規格・ルールが古い、合理的

でない、現実にあっていない

- 社員の規範順守意識が鈍化した企業風土
- 企業のトップと現場とが隔離、ものが言えない風通しの悪い職場
- 品質管理や安全部門は非主流派、決まった主流ルートしか社長にならない慣習

(2) 人間的問題

- 経営陣のコンプライアンス意識の低下
- 現場に近い責任者ほど、自分で何とかしようと頑張る
- 上司に伝える前に、自分たちでなんとかできると考える
- 上司におもねる、顔を立てる、おもんばかり、忖度する
- 不適切行為が継続されると、その誤った倫理観が後輩に継承
- 知識不足、技能不足
- 不正や安全性には直接関係ないという意識
- 倫理観の欠如
- 手を抜きたがる、楽をしたがるなどの人間の特性

- 正常でないデータがたまに出されると無視したくなる、通常と同様と考えたがる（正常性バイアス）
- 人は変化を嫌う（定常化バイアス）
- タコつば化現象：自分が正しいと思い込む
- 顧客企業や消費者の過剰な品質要求

(3) 技術的問題

- データ取得の機械化ができていない
- 不正防止のチェック機構が機械化されていない
- データ管理が人間的な処理に任されている
- 事故情報等のデータを共有するシステムができていない
- 評価の自動化、見える化ができていない

5 データ改ざんの防止対策について

不正の原因の三要素（不正のトライアングル）が、表1のように米国の犯罪学者であるドナルド R. クレッシー（Donald Ray Cressey：1919–1987）により提案されている。前項のデータ改ざんの原因をこの三つの要素に分類してみることもできるだろう。データ改ざんという不正は、表1の三要素のどれか一つをなくせば、防ぐことにつながる。ここではこれ以上深入りしないが、以下に二つのことを提案したい。一つ目は技術的な対策であり、二つ目

表1 D.R. クレッシーの不正の三要素²⁾

1. pressure (圧力, 動機)	不正を起こす動機
2. opportunity (機会)	不正をしても、露見しない方法や環境が揃っている
3. justification (正当化)	皆がやっていることだから、誰にも迷惑をかけないからなど、自分に言い聞かせてルールを破る

が安全文化の醸成による対策である。

大量のデータを人間だけに依存して処理するのは難しい時代になってきており、技術的な対応が可能な時代になってきている。技術的な防止対策として、コンピュータによる自動的なデータ取得を行い、人手を介さない技術の採用がある。これにより、改ざんや後戻りできない仕組みを構築することができる。特に、最近、AI, IoT, ビッグデータの活用が可能になり、不正の検出やルール・法律違反等の検出も自動化することが可能である。また、自動化により、無駄な長時間労働を防ぐことができ、各種の現場への圧力に対してゆとりある対応の可能性が高まるはずである。

二つ目の対策は、個人の倫理観だけでは、データ改ざんの防止は現実にはかなり困難と思われることに基づく。例えば、ある個人が周りの人がデータ改ざんに関与していると知ったとき、一人止めるべきだと提言しても、昔からやっている、黙っていればわからない、本質的な問題ではない、間に合わなくて大きな損害が出たらどうするのだなどと言われれば、これに反抗することは現実的にかなり困難と思われる。内部告発という手もあり得るが、それなりの勇気が

必要で現実には難しいのではないだろうか。チェックを厳密にしてみたり、見つけた場合には厳罰に処したりして規律を強化したところで、我が国の文化にはなじまない可能性がある。不正の事実を気軽に指摘でき、それが素直に受け入れられる環境にするのが最も望ましい。これには、企業全体の風通しの良い企業文化や安全を最も大事と考える安全文化を醸成するしかない。遠回りかもしれないが、結局は、コンプライアンスや安全を大事にする文化を醸成、構築していくのが最も実効性のある有効な方法であると考えられる。

6 おわりに

データ改ざんは、改ざんをしたか (YES)、しないか (NO) の二値で議論されるが、安全や品質にとって、大事なことはその量、すなわち大きさや幅が本質であることを忘れてはならない。現実の安全問題や品質問題では、少しくらいならば許容するという幅があることが本来の姿であるが、法律やルールの違反は YES, NO の二値論理に基づいている。データ改ざん問題が必ずしも安全問題でないと主張したのはこのようなことに基づいている。また、顧客企業や消費者が過剰なまでの品質要

求や安全要求をする問題、及び、ルールや規則は本来の目的である安全や品質を向上させるためのツール (道具) であるのに、本質にはあまり影響のないそのツールの使い方に対する不正に対して、マスコミ等が過剰なまでにバッシングをする問題も気になるところであるが、ここではこれらの問題を指摘しておくにとどめておきたい。

データ改ざん問題の防止には、他の不祥事防止と同様にトップの価値観と関与が最も大事である。コンプライアンスや安全の問題は利潤の問題と天秤にかけるものではない。ものには順番があり、安全があつて、そしてコンプライアンスあつての利潤の追求であるという経営者倫理は、従業員に要求させる倫理観よりはるかに先になければならない。

ここでは、データ改ざんの例を紹介したが、事実に基づいて、それが安全問題なのか、信頼問題なのか、コンプライアンス問題なのか、それとも安心問題なのかを、そしてその原因の背景はどこにあるのかを冷静に見極める目をもちたいものである。

参考文献

- 1) 向殿政男：随筆“データの改ざんと安全性”，標準化と品質管理，Vol.71, No.2, 2018, 日本規格協会
- 2) 南波裕樹：なぜ製品不祥事が繰り返されるのか～企業の視点から安全文化確立への課題を考える～，EAJ シンポジウム第13回安全工学フォーラム，日本工学アカデミー，2018.3
- 3) 向殿政男 (2016)：入門テキスト安全学，東洋経済新報社