WP.37

欧州国連統計委員会・経済委員会、欧州統計家会議　　欧州委員会
欧州共同体統計局
(EUROSTAT)

統計データの機密保持に関する UNECE/Eurostat 合同ワークセッション
(マンチェスター、2007 年 12 月 17 日から 19 日)

主要議題(iii):適用(SDC 方法の実用的な実施、NSI 及びソフトウェアにおける実際の問題を含む)

研究環境における実際の開示検出

補助論文

Felix Ritchie（英国国家統計局）作成

研究環境における実際の開示検出

Felix Ritchie*

* 国家統計局、Cardiff Road, Newport, South Wales NP10 8XG

電子メール：felix.ritchie@ons.gov.uk

摘要：未加工の機密データアクセスの需要は増え続けており、NSI は管理された研究施設を設置する方法で対応した。しかし、最も一般的な統計的開示検出及び抑制(SDDC)アプローチは、研究環境が作り出す無制限の成果物の受入れに悪戦苦闘している。主な問題は、データの未知の変換に対する、審査を必要とし得る成果物の量を管理する際の SDC ルールの考案である。

研究施設はこれまでと異なる SDDC アプローチを必要としている。英国の ONS は、(1) 研究者向けの現行訓練プログラム、(2)成果物のクラスに基づくルールに基づいて、成果物のチェックに費やされる時間が少しでも安全でない成果物に集中できるようなアプローチを策定した。

モデルの関数形に基づく「安全な」成果物と「安全でない」成果物の定義付けによって、機密保持のチェックの効率及び安全確保は向上しているが、容易ではない。本論文では、幅広いアプローチの概要を示した上で、分析成果物に対する英国のルール（及びそれに課される条件）がどのように展開されてきたかを示す具体的な例を提示する。

1　研究環境における開示抑制

需要の分散後、ここ数年にわたって、国家統計局(NIS)による研究データセンター(RDS)及び他の研究施設の提供は増え続けている。これらは開示抑制に複数の問題を引き起こしている。RDC は、専門家が極めて詳細なデータにアクセスし、このデータの選択、歪曲、変換及びリンクを興味深い様々な新しい方法で行うと共に、開示性評価が必要になる複雑な成果物を作成する場所になるべく設計されている。

開示抑制システムは以下であることが望ましい。

- 透明性があること。
- 一貫していること。
- 一定レベルの開示リスクを保障すること。
- 不当に研究成果物を制限しないこと。

Ritchie (2007)で述べたように、RDC の成果物には、自動的な開示抑制ルール及び厳格なルールは規定されていない。このため、どの NSI もその RDC について手動の開示チェックを行っており、ニュージーランド統計局、カナダ統計局又は NORC／NIST[参考文献]が作成したもの等の NSI のスタッフ及び研究者向けの指針を設定している。しかし、成果物の潜在的に無限な範囲は問題である。つまり、指針一式はどうすれば安全を確保するだけ詳細に、有用になるほど十分に柔軟にそして、公正であるほど十分に一貫してあらゆる種類の成果物を網羅できるかということである。

Ritchie (2007)で提言したように、成果物を一定のクラスに分類することは、実行可能な RDC チェックシステムを構築する上で極めて効果的である。同論文では、英国の国家統計局(ONS)は既にかかる分類を策定しつつあると述べた。

本論文の目的は、前回の論文で提起された概念の一部をどうすれば実用化できるかについて詳しく述べることである。本論文では特に、以下について説明する。

- 安全な成果物と安全でない成果物の定義をルールに転換する方法。
- この定義の基礎をデータではなく関数形に置く必要の程度。
- 有効な成果物の分類を定義付けるステップの一部。

本論文では、最も支持の高い SDC 指針がどのようにこのモデルに適合されたかも示す。

2　動物園研究の分類

Ritchie (2007)で述べたように、研究環境に向けた開示抑制メカニズムの設計は動物園の設計と似ている。特定の動物に関する不確かさが存在する可能性はあるが、多種多様な動物を、泳ぐもの、飛ぶもの、水を必要とするもの、不注意な飼育員を食べてしまうグループに分類することは可能である。飼育場は、特定の蛇又は蛇種を考慮に入れて設計されない可能性があるが、動物園が保存を目指す蛇の多くを有効に収容し、健康に保てるものでなければならない。この動物は次いで「安全な」と「安全でない」に分類することが可能で、動物園の所有者は安全でない動物の方に時間を集中的に費やすことができる。

研究成果物に対する「安全な」と「安全でない」は、研究者にとっても NSI のスタッフにとっても明確な解釈である。

- **安全な成果物**：これは、NSI のスタッフが阻止される又は調整されるべき何らかの理由を確認でき**ない場合に公開される**ものである。
- **安全でない成果物**：これは、当該成果物がこの成果物に対する詳細な規準を満たしていることを研究者が NSI のスタッフに実証でき**ない場合に公開されない**ものである。

安全な成果物か安全でない成果物かに応じた立証責任の移行が論議されることに留意すること。安全な成果物の場合は、NSI チームは特定クラスの成果物は概ね、開示リスクはないと判断している。一般的ルールの例外になる特定の成果物について懸念を示すことがある。システムを適切に機能させるためには、この例外は以下であるべきである。

- 少数である。
- 十分に定義付けられている。
- 研究者にとってわかりやすく、研究の開始に先立って伝達される。

3 つ目は極めて重要である。研究環境に有効な SDC システムの策定には、研究者と NSI のスタッフ間の前向きな関係が不可欠であり、どちらの側にも予測外の事態が発生してはならない。例外を明確に特定することにより、研究者は　作成した結果の公開が容認可能であることに自信を持つことができる。

安全でない成果物に対しては、NSI は、成果物の開示性の範囲を成果物の公開準備が整っていない範囲と決定した。しかし、NSI は決定が変更される理由について研究者が事例に抗議する機会を残している。

安全でない成果物の公開可能性を主張する研究者は、特定のデータ及び文脈だけでなく開示抑制の原則も十分に認識している必要が明らかにある。このため、有効な SDC に必要な研究者の訓練は、こうした安全でない成果物 －そして特に、安全でない成果物を安全な成果物に変えられるものに主眼を置くべきである。当然ながら、研究者の訓練の中には、安全でない成果物そのものを阻止できるものもある。

3　「安全性」の判断

SDC に関する文献は、歴史的理由から、公開されるデータの特定の側面、つまり、占有性、外れ値、公開情報の利用等に焦点を当てている。これは、SDC に対する作業の大半が、データセットが有効に匿名化されている又は集計表が安全であることを確認するための詳細な調査であったためである。これによって、研究環境にも同様の技術を適用することに主眼が置かれるようになった。

これは適切ではない。標準的技術は、一連の侵入者シナリオの試験対象になり得る固定されたインプットデータセット及び有限な成果物の集まりに向けて設計される。研究環境のインプットデータセット及び成果物データは、SDC のルールが策定される時点では未知状態であり、有限な結果の集計表に行うものと同じ種類の各成果物の詳細分析を定めるのは実用的ではない。データセットの「安全性」を決定する鍵は、成果物の基礎となる関数形を調べることである。任意のデータセットに開示リスクが存在しない場合は、例えば、変数の「識別」集合の存在に起因する開示リスクが追加される可能性はない。

この技術はリスクが発生する根源を確実に絞り込むのにも役立つことに留意すること。例えば、線形回帰分析モデルでは、潜在的開示リスクは、平均値及び度数の継続的な公表に起因して発生する。このため、線形回帰分析モデルそのものは安全でも、補助的統計データが問題になる場合がある。

成果物の種類はそれぞれ、一次開示 ーつまり、単一の成果物から直接何かを推論できるか否かー及び差分検出による開示について、個別に評価する必要がある。評価では主要な変数(cardinal variables)及びカテゴリカル変数の両方を検討するべきである。

結果の分類は困難である場合がある。何かが根本的に安全であるが、多数の例外がある場合は、「安全でない」に分類する方が適切である。例えば、表 1 は、ONS のバーチャルミクロデータラボラトリー(VML)で現在用いられている分類の例である。

表 1　ONS における「安全な」成果物及び「安全でない」成果物の例

安全な	安全でない	不確か
一般的線形回帰分析	集計表	データの他の非線形集約表
パネル回帰分析	グラフ	
ハーフィンダール指数 [1]	四分位数	巨大な高頻度の集計表
共分散行列 [1]	クロス積行列	

1 制限が適用される、以下を参照。

「安全な」成果物の多くはさらなる制限を課される。この成果物は例外の発生源であり、NSI はこれを用いて成果物の公開の可否を決定する。この成果物は上述したように、数が少なく、研究者に知らされる。この 2 つの条件が達成できない場合は、その成果物は「安全でない」又は良くても「不確かな」に分類された。

「不確かな」要素はここでは複数の因子に起因して生じる。モデルがまだ調査されていない又は安全な成果物に対する例外の簡明な記述がない又は、労働集約的でない方法で安全性を実証する方法に対する合意がまだ成されていない可能性がある。

実際の例を調査する前に、さらに 2 つの点について考慮する必要がある。第 1 に、特定の関数形を踏まえると、理論的には、データ点の識別が可能になるようなデータの特定の組み合わせが常に存在する。「安全な」成果物は、この理論的識別可能性には、分析における実際の識別可能性が含まれない成果物である。

これに続き、成果物は真の統計的成果物であると仮定する必要がある。悪意のある研究者は有効な統計的結果に見えるが、実は検出を避けるためだけに構築された統計データを構築する可能性がある。意図的な虚偽の扱いは本論文の対象外である。

4　例

本セクションでは、成果物の具体的な評価を探求する。方法の異なる側面を例証するために、成果物の選定のみを扱う。詳細な例は VML(2007)で確認又は参照できる。

4.1　データの線形変換

データの線形集約に向けて、

$$\partial f(x)/\partial x = C$$

$$f(x)\text{-}f(y) = f(x\text{-}y)$$

この時、C はほぼ一定である。最初の方程式からは、他の変数に関係なく個々のデータ点を評価できることがわかる。従って、データ点は全て、潜在的開示リスクであり、個々に評価する必要がある。

2 番目の方程式を見てわかるように、*f(x)*が単一の測定値に適用される際に有用なデータを生成する関数である場合は、*f( )*の差別検出における開示リスクが存在することになる。

このため、線形集約は全て、「安全でない」に分類しなければならず、データチェックに対する高い要求及び、差分検出による現実的な開示リスクが発生する。これらはいずれも線形集約の数学的形式に固有のものである。このため、この分類は全ての線形集約、つまり、集計表、グラフ、平均値、度数に言及する。この分類は集計表としても表現し直すことが可能な四分位数、最大値及び最小値も網羅する。

集計表の公開に対する SDC 関連のほぼ全ての文献が、データの問題、母集団一意等に焦点を当てるのはこのためである。集計表はデータの線形集約であるため、その構造の中では安全とみなすことはできない。安全は、変数及び標本の適切な選択を通じて得るべきものである。ソースデータと成果物である集計表間の線形関係を、例えば、再符号化又は丸めによって断ち切るような別の方法もある。

4.2　線形回帰係数

単純な線形回帰分析に対する、予測係数の関数形を考えてみよう。

$$f(X, y) = \hat{\beta} = (X'X)^{-1} X'y$$

Ritchie (2006)で実証するように、一般に差分検出に起因する開示リスクはなく、非線形干渉は個別データ点が解析できないことを意味する。従って、これは安全な成果物とみなされる。

これは、カテゴリカル変数及び主要な値に当てはまる。他の全ての変数と直交するカテゴリカル変数を組み込んだモデルの差分検出に起因する潜在的開示リスクが存在するように見えるが、測定値が識別される可能性は、利用可能な平均値の有無によって異なり、利用可能な平均値が存在する場合は、数値を識別するより直接的方法が存在する。

検討すべき限られた例外はいくつかある。これを以下に示す。

- 説明変数が全てカテゴリカル変数である場合は、これは明らかに集計表であり、そのようなものとして評価する必要がある。或いは、これが有効な統計モデルになるための自由度が不十分な場合は、正確な数値を決定すればよい。
- 説明変数が全て侵入者に知られる可能性がある場合は、個体の数値が予測される可能性がある。適合度が特に適切な場合は、これは、真の値に十分近似になることにより、機密性の制限を履行しない可能性がある。
- データが 1 つの客体(1 人の個人に関する繰り返し観測)に由来する場合は、これは、特に他の客体に比べて、その客体に関する情報源になる可能性がある。

1 つ目は、分析成果物としての単なる集計表の誤分類である。2 番目は理論的問題になるが、実際には、適合度は必ずしも実行可能な程度に適切でないように見える(ニュージーランド統計局[参考文献]の研究は、99%に近似の R2 を示唆している)。予測の精度に対する単純な試験及び対応策はいずれも、簡単に利用できる。詳細については Ritchie (2006)を参照。

3 番目の例外は上の 2 つよりも興味深い。どの有益な情報が引き出され得るかは明らかでないため、現在の予防ベースの ONS は、単一の客体に基づく回帰分析を禁止している。

4.3 外積行列及び共分散行列

外積行列を考えてみよう。

$$M = X'X$$

これは安全でない成果物である。度数及び合計値はいずれかの定数又はカテゴリカル変数との相互作用で識別されるため、これは、線形集約とみなすべきである。

今度は単純な回帰分析で生成される分散共分散行列を考えてみよう。

$$V = (X'X)^{-1}\hat{\sigma}^2$$

これは公開すべきか。研究者は σ の推定値を入手できるという仮定に基づくと、V を外積行列に変換するのは極めて簡単であり、安全ではない。従って、この単純な共分散行列は安全ではない。

ただし、これは以下の一般的な関数形には当てはまらない。

$$V = \left[(X'WX)(Z'Z)^{-1}(X'WX)\right]^{-1}\hat{\sigma}^2$$

Z=X でなく、W が単位行列でない場合は、これは選別不能にはなり得ない。これは W が既知の場合も当てはまる。例えば、W は、上記より複雑なモデルはもとより、ロバストな回帰分析又は不均一分散シナリオでも、単位行列にはならないため、これは、有用な結果である。

V と予測係数ベクトルの組合せから何か推論できるか。両方の情報にアクセスできる研究者の場合は、

$$V\hat{\beta}/\sigma^2 = (X'X)^{-1}(X'X)(X'y) = (X'y)$$

これは問題になる可能性がある。例えば、X 内の 2 つのカテゴリカル変数は、1 つの既知の測定値においてのみ異なるが、実際は、この測定値は VML では極めて低い開示リスクとして容認される。

つまり、当該モデルが単純な重み付けされない OLS でない限り、分散共分散行列は安全なように見える。

4.4 ハーフィンダール指数

ハーフィンダール指数は、ある業種における 1 つの会社の占有性を反映するものである。

$$H = \sum_i s_i^2 \qquad s_i = x_i / \sum_i x_i$$

一見したところでは、これは安全な成果物のように見える。市場に 2 つより多く会社が存在する限り、個々の数値は解明できない。

ただし、二次項の利用は問題を引き起こす。2 番目に大規模な会社が有意な規模でない限り、√H は最大規模の会社のシェアの良好な近似になる。SDC 評価者にとって厄介な問題は、この近似の良好性が会社の相対的規模及び、裾野規模によって異なることである。規模が上位 2 位の会社 のシェア(S1 及び S2) の標本値及び『裾野』を組み込んでこれを示したものが表 2 である。

表 2　S1 の近似値である H、最大企業のシェア

S1	***S2***	***S3-S50***	***H***	***S1-S2***	***√H の近似性***
27%	1.5%	1.5%	.08	26%	8%
32%	20.0%	1.0%	.15	12%	20%
37%	15.0%	1.0%	.16	22%	10%
S1	***S2***	***S3-S10***	***H***	***S1-S2***	***√H の近似性***
30%	10.0%	7.5%	.15	20%	27%
37%	15.0%	6.0%	.19	22%	17%
56%	40.0%	0.5%	.47	16%	23%

この表を見ると、同業社が 10 社又は 50 社ある、ある産業の上位 2 社及び他の会社に対する一連の数値がわかる。単純な関係は存在しない。√H 全体の最大値の近似値から見て安全な最後の項目も、通常、占有性試験を通過しない。

従って、H は安全な統計データになりそうだが、H の値だけに基づいてカテゴリー的にそう言うのは難しく、それゆえに、ONS は研究者が以下であることを証明できる限り、ハーフィンダール指数を許可している。

- 測定値が 2 つより多くある。
- √H が一定の比率で最大値を超える。
- 占有性規準が達成されている。

これは、納得できる状況ではない。この追加条件は H の安全性を確実に保障するが、研究者が提示し、SDC のスタッフがチェックする情報を 4 件以上要求するためである。

5 結論

本論文は、実際の SDC システムにおいてセキュリティ、一貫性及び効率をどう組み合わせるかについて、Ritchie(2007)の構想の一部を具体化したものである。本書に示す例では、相対的な透明性評価方法を複数クラスの成果物にどう適用できるかを明らかにした。

本書で示す構想の多くは、NSI が作成した SDC マニュアルの中で既に黙示的に示されている。本論文の主な目的は、SDC アプローチを評価する共通の枠組みをある程度提示することである。本書は、国際基準の策定における継続的な動向に照らして、このアプローチを、国際協力の拡大及び透明性向上の確立に役立つような『リスク格付け』を研究成果物に設定することに向けた一歩にすることを意図している。

謝辞

本原案に対する論評をいただいた Rhys Davies と Philip Lowthian に謝意を表する。

参考文献

Enright, J., McDonald, S., Corscadden, L., Jewell, E., O'Sullivan, J., Zeng, I., Nair, B.,and Bentley, A. (2006) *Confidentiality Best Practices Manual.* Mimeo: Statistics New Zealand

ONS (2007) *Disclosure Control Standard for Business Surveys.* Mimeo: Office for National Statistics

Ritchie, F (2006) *Disclosure Control of Analytical Outputs.* Mimeo: Office for National Statistics

Ritchie, F (2007) *Statistical Disclosure Control in a Research Environment.* Mimeo:Office for National Statistics

VML (2007) *VML Default SDDC Methods.* Mimeo: Office for National Statistics