2010年8月21日連続シンポジウム第1回

英国におけるインフォメーション・コミッショナーの組織と権限
−わが国の第三者機関創設への示唆−

筑波大学大学院
図書館情報メディア研究科
准教授　石井夏生利

1

インフォメーション・コミッショナー制度

2

英国とICO(Information Commissioner's Office)

- 英国：グレートブリテン及び北アイルランド連合王国
- イングランド、ウェールズ、北アイルランド、スコットランド
- 英国の面積：24.3万平方キロ
- 英国の人口：約6140万人
- ICOの本部事務所：マンチェスター
- ICOの地域事務所：ベルファスト(北アイルランド)
  エジンバラ(スコットランド)
  カーディフ(ウェールズ)

インフォメーション・コミッショナー (Information Commissioner)

- 1998年データ保護法に基づく監督機関
- 「データ保護登録官」→「データ保護コミッショナー」→「インフォメーション・コミッショナー」
- 初代(1984年9月～)
  エリックハウ(Eric Howe)氏
- 二代目(1994年9月～)
  エリザベス・フランス(Elizabeth France)氏
- 三代目(2002年11月～)
  リチャード・トーマス(Richard Thomas)氏
- 四代目(2009年6月～)
  クリストファー・グレアム(Christopher Graham)氏

4

1998年データ保護法の用語

- 個人データ＝生存する個人に関する識別可能な情報からなるデータ
- データ管理者＝個人データの取扱目的及び態様を決定する者
- データ主体＝個人データの主体である個人
- 取扱い＝個人データの取得、保有、利用、提供、抹消等、一連のプロセスを含む。

5

1998年データ保護法のポイント

- データ保護原則の遵守
- インフォメーション・コミッショナーへの通知
- アクセス権

6

データ保護登録官としての役割(1984年データ保護法)

登録件数の推移

1984-1985	1985-1986	1986-1987	1987-1988	1988-1989
ー	133,000	125,000	150,000	170,000
1989-1990	1990-1991	1991-1992	1992-1993	1993-1994
153,000	160,000	164,500	166,327	188,766
1994-1995	1995-1996	1996-1997	1997-1998	1998-1999
202,476	201,434	212,943	224,909	229,693

1984年法に関する統計データは、*The first report of the Data Protection Commissioner on the 16th year of operation of the Data Protection Act 1984* (2000)に基づき作成。

7

インフォメーション・コミッショナー制度と通知件数

通知件数の推移

1999-2000	2000-2001	2001-2002	2002-2003	2003-2004	2004-2005
243,681	220,455	198,519	211,251	251,702	259,296
2005-2006	2006-2007	2007-2008	2008-2009	2009-2010	
ー	287,000	304,000	317,165	328,164	ー

手数料の一部引き上げ

各年のICOの年次報告書をもとに作成。

8

通知事項その1

- データ管理者の氏名及び住所
- 企業の登録番号(任意)
- 連絡先の詳細
- 個人情報の取扱いに関する一般的な説明
  - ✓個人情報の取扱目的　e.g. 負債情報の収集や調査など
  - ✓データ主体の説明　e.g.　従業員又は患者など
  - ✓データの類型に関する説明　e.g. 雇用や財政状態の詳細
  - ✓データ受領者の一覧　e.g.　中央政府や金融機関など
  - ✓欧州経済地域外にデータを移転するか否かに関する情報

ICO「Notification Handbook」7頁より作成
(http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/notification_handbook_final.pdf)。

9

個人情報の取扱いに関する一般的な説明の例

Provision of financial services and advice

Data subjects are:	• customers and clients; • complainants, correspondents and enquirers; and • advisers, consultants and other professional experts.
Data classes are:	• personal details; • family, lifestyle and social circumstances; • employment details; • financial details; and • goods or services provided.
Recipients are:	• data subjects themselves; • relatives, guardians or other persons associated with the data subject; • business associates and other professional advisers; • financial organisations and advisers; and • ombudsmen and regulatory authorities.
Transfers:	• none outside the EEA.

ICO「Notification Handbook」9頁より。

Purpose form

You must quote your security number or the form will be returned.

Data controller name:	
Registration number:	
Security number:	
Purpose title:	See Section 3.1.8 of the notification handbook for a full list
Write a brief description here – only if none of the standard purposes apply:	
Data subject codes:	See Section 3.1.9 of the notification handbook for a full list
Write additional descriptions here – only if none of the standard descriptions apply:	

11

ICO「Notification Handbook」41頁より。

Purpose form

Data class codes:	See Section 3.1.10 of the notification handbook for a full list
Write additional descriptions here – only if none of the standard descriptions apply:	
Recipient codes:	See Section 3.1.11 of the notification handbook for a full list
Write additional descriptions here – only if none of the standard descriptions apply:	
Transfers:	☐ None outside EEA ☐ Worldwide Name individual countries below See Section 3.1.12 of the notification handbook for a full list of the countries in the EEA
If there are more than 10 countries indicate worldwide	

12

ICO「Notification Handbook」41頁より。

通知事項その2

- 安全保護措置に関する説明
  - ✓情報セキュリティポリシー
  - ✓物理的セキュリティ
  - ✓情報へのアクセス制限
  - ✓事業継続計画
  - ✓従業員教育
  - ✓セキュリティ侵害が発生した際の発見及び調査
- 取引上用いる名称
- 通知義務の対象外となる取扱いに関する説明
- 自主的な通知
- 代理人の連絡先
- 手数料
- 署名

ICO「Notification Handbook」18～19頁より。

13

通知義務の例外

- コンピュータ処理以外の情報の取扱い
- 従業員管理を唯一の目的とする取扱い(給与支払いを含む)
- (自らの事業活動との関連で)広告、マーケティング、広報活動を唯一の目的とする取扱い
- 会計処理や記録を唯一の目的とする取扱い
- 非営利組織が会員管理その他の目的で取り扱う場合
- 司法機能を果たすための取扱い
- 個人的、家庭的又は家事目的での取扱い(娯楽目的を含む)
- 公的記録の維持を唯一の目的で取り扱う場合

ICO「Notification Handbook」20頁、23頁より。

14

手数料制度の改定(2009年10月1日～)

改正前	一律35ポンド	
改正後 :2段階方式	Tier 2 ・総収益2590万ポンドかつ従業員250人以上のデータ管理者 ・職員250人以上の公的機関	£500
	Tier 1 ・上記以外(従業員250人未満の企業など)	£35

ICO「Notification Handbook」3頁より。

15

コミッショナーをサポートする人たち

執行部

デービッド・スミス 副コミッショナー兼データ保護担当理事	グレアム・スミス 副コミッショナー兼情報公開担当理事	ヴィクトリア・ベスト 組織開発担当理事	サイモン・エントウイスル 事業担当理事	スーザン・フォックス 総務担当理事

非執行部

ロバート・チルトン博士 理事	デービッド・クラーク 理事(2009年11月まで)	サー・アリスター・グレアム 理事(2009年11月まで)	ニール・メイサム 理事(2009年11月から)	イーニド・ローランズ 理事(2009年11月から)	デーム・クレア・ティッケル 理事

監査委員会

ロバート・チルトン博士　委員長	デービッド・クラーク (2009年11月まで)	ニール・メイサム (2009年11月から)	グレアム・スミス

ICO年次報告書(2009/2010)
(http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2010.pdf) 16
49頁より作成。

ICOの組織：職員の人数

2005-2006	2006-2007	2007-2008
245	262	261
2008-2009	2009-2010	–
282	327	–

各年のICOの年次報告書より作成。

17

純支出勘定

		2009-2010 £'000	2008-2009 £'000
支出	人件費	10,693	9,297
	減価償却費	921	540
	その他支出	8,127	7,856
	合計	**18,820**	**17,153**
収入	事業活動からの収入	13,192	11,310
	その他収入	17	50
	合計	**13,209**	**11,360**
純支出		**5,611**	**5,793**

*** 司法省の助成金が550万ポンド**

ICO年次報告書(2009/2010)72頁、75頁より作成。

18

人件費

	2009-2010 £'100	終身被雇用者 £'100	その他 £'100	2009-2010 £'100
給与	8,650	8,082	568	7,469
社会保障費	544	516	28	498
その他年金費用	1,512	1,447	65	1,354
合計	10,706	10,045	661	9,321
外部派遣に関連した回収額	(13)	(13)	-	(24)
正味費用総額	**1,0693**	**10,032**	**661**	**9,297**

19

ICO年次報告書(2009/2010)81頁より作成。

給与（コミッショナー及び幹部）

	2009-2010 £'000	2008-2009 £'000
クリストファー・グレアム（2009年6月29日から）	105-110	-
リチャード・トーマス（2009年6月28日）	30-35	150-155
デービッド・スミス	70-75	70-75
グレアム・スミス	80-85	75-80
サイモン・エントゥイスル	80-85	75-80
スーザン・フォックス	55-60	50-55
ヴィクトリア・ベスト	50-55	50-55

20

ICO年次報告書(2009/2010)61頁より作成。

1998年データ保護法とインフォメーション・コミッショナー

21

所管する5つの情報保護法制

- 1998年データ保護法(Data Protection Act 1998)
- 2000年情報自由法(Freedom of Information Act 2000)
- 2003年プライバシー及び電子通信規則(Privacy and Electronic Communications Regulations 2003)
- 2004年環境情報規則(Environment Information Regulations 2004)
- ヨーロッパ共同体における空間情報のための基盤に関する規則(Infrastructure for Special Information in the European Community 2009)

22

1998年データ保護法

- 「当該情報の取得、保有、利用又は提供を含む、個人に関する情報の取扱いの規制ために新たな規定を設けるための法律」(An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information)
- 1998年7月16日成立、2000年3月1日完全施行
- 1995年EU個人データ保護指令に対応
- 全6章75条、附則1-16にて構成

23

データ保護原則

- 第1原則　公正かつ適法な取扱い
- 第2原則　限定された目的のための取扱い
- 第3原則　目的適合性
- 第4原則　正確性・最新性
- 第5原則　必要期間限定性
- 第6原則　データ主体の権利適合的取扱い
- 第7原則　安全性確保
- 第8原則　十分な保護のない第三国への移転制限

24

インフォメーション・コミッショナーの地位・処遇

地位	女王から独立した法執行機関
	単独法人
任命	開封勅許状
任期	5年、再任可
退任	辞職又は両院の解任請求による。
定年	65歳に達する日の属する職務年度の満了時又は15年の勤務満了時
俸給・年金	下院の決議による。
必要経費	議会が主務大臣に付与した額から支給

25

インフォメーション・コミッショナーの一般的権限

- 第Ⅵ章　雑則及び総則

コミッショナーの権限

第51条　コミッショナーの一般的義務

「(1)　データ管理者による善良な実務の遂行を促進し、また、とりわけ、データ管理者による本法の義務の遵守を促進するように本法に基づき自らの権能を行使することは、コミッショナーの義務である。」

26

「善良な実務」(good practice)とは

- 本法の遵守
- データ主体及び他の者の利益に鑑み、コミッショナーが望ましいと思う個人データの取扱いに関する実務

インフォメーション・コミッショナーの具体的権限・義務

- 国民に対する情報提供、助言
- 実施基準の策定及び配布

普及・啓発

- 通知に基づく登録
- 登録事項の無料公開

登録事項の管理

- 執行通知等の送達
- 立入調査権
- 訴追権限

法の遵守監視・執行

- 両議院に対する年次報告の提出
- 会計報告書を作成し、監査を受け議会に提出

報告書の提出

- 国際協力等

その他

28

行動基準

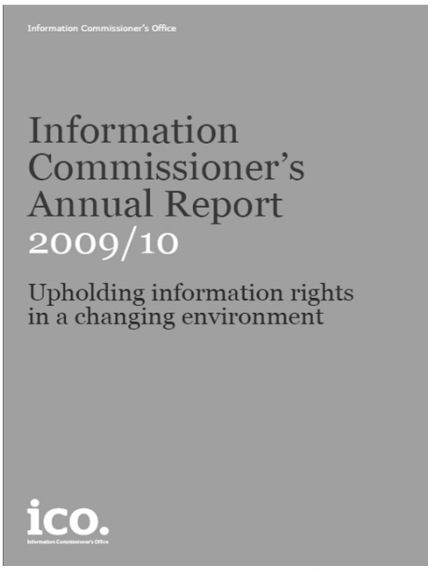
プライバシー通知	プライバシー通知実施基準
CCTV	2008年CCTV実施基準
個人情報共有	個人情報共有の枠組に関する実施基準
雇用実施基準	雇用実施基準の早わかりガイド：中小企業にとっての理想的取組
	雇用実施基準
	雇用実施基準：補足ガイダンス
電気通信	電気通信に関する番号情報及び公正な取扱いに関する実施基準

29

インフォメーション・コミッショナーの活動

30

ICOによる年次報告書の公表



Contents

Our mission statement	6
Your information rights	7
Information Commissioner's foreword	8
Our Corporate Plan aims, 2009 to 2012	12
Our year at a glance	14
Educating and influencing	16
Resolving problems	26
Enforcing	36
Developing and improving	44
Governance	48
Information requests to the ICO	50
Accounts	52

ICO年次報告書(2009/2010)13頁の表紙及び5頁より。

31

コミッショナーの3ヶ年計画(2009-2012)

- 教育・啓発
- 問題解決
- 法執行
- ICO(Information Commissioner's Office)の発展と改善

ICO年次報告書(2009/2010)13頁の図より。

32

教育・啓発（2009-2010年）

- 欧州データ保護日(European Data Protection Day)
- 個人情報に関する約束(Personal Information Promise)
- 青少年への啓発(Reaching young people)
- プライバシー大使の起用(Recruiting Privacy ambassadors)
- 欧州外における個人データの安全な取扱い(Safety processing personal data outside Europe)
- データ保護担当者会議(Data Protection Officer Conference)
- プライバシー通知実施基準(Privacy notices code of practice)
- プライバシー影響評価(Privacy Impact Assessments)
- 保存期間の短縮(Securing shorter retention periods)
- 国際連携(International liaison)

ICO年次報告書(2009/2010)21～24頁参照。

33

個人情報に関する約束

Promise

I (name and title),
on behalf of (name of organisation)
promise that we will:

1. value the personal information entrusted to us and make sure we respect that trust;
2. go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
3. consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
4. be open with individuals about how we use their information and who we give it to;
5. make it easy for individuals to access and correct their personal information;

ICO「I on behalf of promise that we will:」
(http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/pip_120109.pdf)参照。

34

欧州外の安全な個人データ取扱い：拘束的企業準則

- 1995年EUデータ保護指令第25条(「十分な保護レベル」を有しない第三国への個人データ移転の禁止)に対応する制度。
- 主に多国籍企業が、BCRの要件と手続を満たせば、個別の同意を取らずして第三国の系列企業に個人データを移転することができる。
- 各国のデータ保護機関が許可権限を有している。
- ICOは、2009年4月以降、5件を許可。

37

問題解決

1999 - 2000	2000 - 2001	2001 - 2002	2002 - 2003	2003 - 2004	2004 - 2005
4,985	8,875	12,479	12,001	11,664	19,460
2005-2006	2006-2007	2007-2008	2008-2009	2009-2010	―
22,059	23,988	24,851	25,509	33,234	―

各年のICOの年次報告書をもとに作成。

38

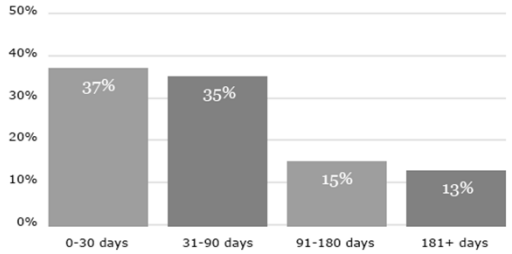
問題解決

Received in year	33,234
Closed in year	32,714

Work in progress at 31 March this year: 7,251

Work in progress at 1 April last year: 6,680

Age of work in progress on 31 March 2010

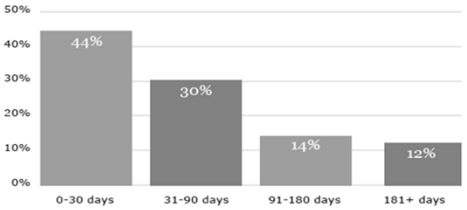


ICO年次報告書(2009/2010)34頁の図より。

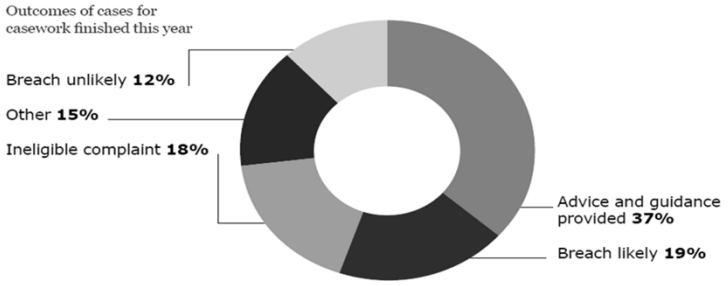
39

問題解決

Age of casework at closure	
30 days or less	44%
90 days or less	74%
180 days or less	88%



Outcomes of cases for casework finished this year

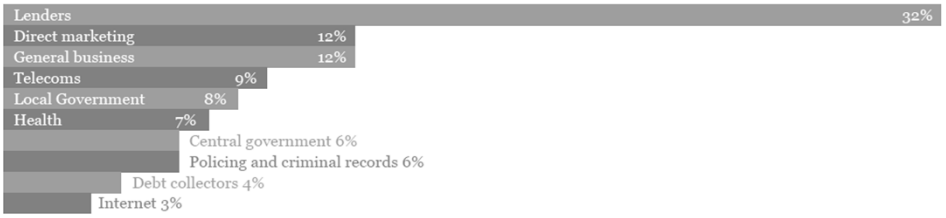


40

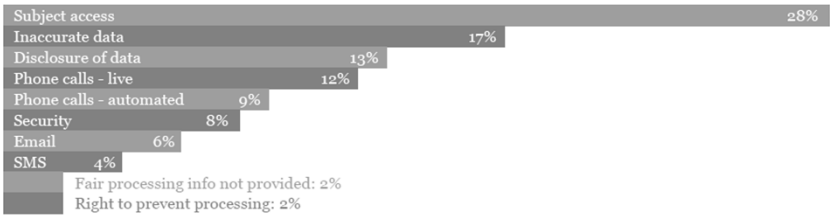
ICO年次報告書(2009/2010)35頁の図より。

問題解決

The top 10 areas generating most complaints where sector is specified



Top 10 reasons for complaining



ICO年次報告書(2009/2010)35頁の図より。

41

法執行：執行通知

1999-2000	2000-2001	1998-1999	2001-2002	2002-2003	2004-2006
1	4	5	4	4	–
2006-2007	2007-2008	2008-2009	2009-2010	–	–
5	9	6	15	–	–

各年のICOの年次報告書をもとに作成。

42

法執行：セキュリティ侵害

Department of Health – formal undertaking

In May 2007 the ICO was alerted to a security breach which allowed sensitive personal details about junior doctors, including religious beliefs and sexual orientation, to be seen by anyone accessing the Medical Training Application Service website. The ICO required the Department of Health to sign a formal undertaking to comply with the principles of the Data Protection Act and in particular required the Department to encrypt any personal data on their website which could cause distress to individuals if disclosed. They were also required to train staff on compliance with the Act.

- November 2007, ICO began to record all instances of data security breaches.

2008-2009	2009-2010
319	464

ICO年次報告書(2007/2008)36頁より (http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2007_08.pdf)。

43

法執行: データ保護に関する正式な保証

2007-2008	2008-2009	2009-2010
9	14	57

DATA PROTECTION ACT 1998
UNDERTAKING

Data Controller: Birmingham Children's Hospital NHS Foundation Trust

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part 1 of schedule 1 to the Act, and in particular that:

(1) Adequate measures are put in place to ensure that data security policies are adhered to consistently across all data controller departments. Such measures would seek to ensure that the unauthorised removal of encryption software against the data controller's security policies is prevented, thereby removing any potential for unauthorised access to that personal data.

44

ICOのウェブ・サイトのうち、バーミンガム子供病院とICO間で交わされた2010年7月14日付覚書を記したページの抜粋 (http://www.ico.gov.uk/upload/documents/library/data_protection/notices/bch_nhs_foundation_trust_undertaking.pdf)

法執行：起訴等

年度	1999 - 2000	2000 - 2001	2001-2002	2002 - 2003	2003-2004	2004-2005
起訴	145	23	66	91	―	―
無罪又は 取下げ	15	2	16	11	―	―
有罪	130	21	33	80	45	55
警告	―	12	13	11	―	―
年度	2005-2006	2006-2007	2007-2008	2008-2009	2009-2010	―
起訴	―	―	―	14	―	―
無罪又は 取下げ	―	―	―	5	―	―
有罪	31	53	103	16	9	―
警告	―	―	―	9	―	―

45

各年のICOの年次報告書をもとに作成。

ICOの発展と改善

ICO
Information Commissioner's Office

↳ ico.
Information Commissioner's Office

82% of organisations are aware of the ICO

73% of customers rated our website as excellent

- **Committed** We care about upholding information rights.
- **Team workers** We work together as one ICO team, sharing information and expertise.
- **Focused** We give priority to activities that make the biggest contribution to achieving our mission.
- **Effective** We work productively and efficiently to produce high quality and timely outcomes, offering best value for customers and citizens.
- **A model of best practice** We do not ask others to do what we are not prepared to do ourselves.
- **Alert** We are alert to the perspectives and needs of all our stakeholders - and to the potential impact of new developments in our business.
- **Fair** We treat everybody we deal with fairly and with integrity and respect. We are inclusive in our approach.
- **Always learning** We are always learning and developing professionally.

ICO年次報告書(2009/2010)44～45頁の図より。

監査

- 2010年7月5日　国防省(MoD)
- 2010年7月23日　環境食糧省(DEFRA)
- 2010年7月30日　英国関税歳入庁(HMRC)

第51条7項「コミッショナーは、データ管理者の同意を得て、善良な実務を遵守するために、個人データの取扱いを評価することができ、その評価の結果をデータ管理者に知らせるものとする。」

47

最近の動き：刑事罰の強化

- 個人データの不正取得、漏えい行為、5,000ポンドまでの罰金刑に最大2年までの拘禁刑が追加(2008年5月8日)。
- 深刻なデータ保護原則違反に対し、50万ポンドまでの制裁金を課すことができるようになった(2010年4月6日)。

48

第三者機関に求められる要件

- 独立性
- 官民双方をチェックできる機能
- 財政的基盤
- 法律に基づく明確な執行権限の付与
- 法律を正しく理解させるための工夫
- バランス感覚を持った専門職員の配置

49