データ消去に関する海外規格の動向

2016/04/11
早稲田大学　瀧澤和子

概要：
本報告書では、上書処理などによるデータ抹消分野で先進する米国の政府ガイドラインおよびその普及状況を調べた。連邦行政府、州政府および大学の「データ消去規定」などを調査した結果、米国では、NIST「800-88」(2006 年版または 2014 年発行の Revision.1)もしくは DoD の「5220.22-M」に準拠した規定を策定している機関が多い。3 回上書きから 1 回上書き方式への移行が官公庁に目立ったほか、2000 年代中盤以降は、消去方法に関する意思決定フローの確立や、作業の検証および記録が重視されるようになり、消去作業を確実に実行できる態勢へと議論の中心が移った。

1. 米国政府機関・研究所等のデータ抹消規格

1.1 リサイクル市場の拡大と消去方式

米国では、コンピュータのリサイクル市場規模が拡大しており、官公庁でも民間教育機関等への払下げや転売など再利用が日常的に行われている。しかし、2003 年に MIT の大学院生（当時）が、中古 HDD を購入しデータを復元できるか実験したところ、入手した計 158 の磁気ディスクの大半から、個人情報などが復元可能だった[1]。この研究は、単なるファイル削除や再フォーマットの実行だけで PC をリユース・廃棄しているユーザーが多く、かつ、そうしたデータ消去法ではセキュリティ上懸念があることを問題提起し、媒体をクリーンにする技術の検討を行ったものである。なお、米国では、過去に、社会保障番号(Social Security Number) や通院履歴などの機微な情報を含んだ PC が中古市場に流通する事件も起きている。

1.2 上書によるデータ消去：DoD 方式と NIST 方式

1956 年に初めて世に登場した磁気ディスクは、1980 年代には世間の主流となった。

米国商務省（Department of Commerce）傘下の米国標準技術研究所(National Institute of Standards and Technology: NIST)は、磁気ディスクのデータの主な消去方法を整理し、Clearing（消去）としてデータの上書きによる抹消、Purging（除去）として（Enhanced）Secure Erase や磁気破壊（degaussing)、Physical Destruction（物理的破壊）として破壊（disintegrate)、断片化（shred)、粉砕（pulverize)、焼却・融解（incinerate）を挙げている[2]。

本稿では、磁気消去や物理的破壊と違って媒体の再利用が可能であり、証拠保全媒体と

しても利用できる上書によるデータ抹消を中心に述べる。米国では、複数の政府機関が、上書によるデータ抹消方法の方式を公開しており、近年に至るまで頻繁に改訂している。主な違いは、書き込むデータの内容と上書回数、および検証(verification)を要求するかどうかである。後述の通り、米国国防総省（Department of Defense: DoD）または NIST 方式の知名度が国際的にも高く、本稿で行った調査（3 章参照）でも、これらが米国で広くデータ消去の指針とされていることが確認できた。

DoD の国防保安局 (Defense Security Service: DSS) は、NISPOM （National Industrial Security Program）の運用マニュアルの一部として、1973 年に『DoD 5200.28-M』[3]を発行し、0、1、固定値による 3 回の上書方式を示した(p.41)。機密度の高い情報に関しては、機器の物理的破壊や消磁のみを認めており、磁気消去によるデータ抹消の信頼性を評価しているものの、1995 年には、『5220.22-M Supplement.1』[4] (p.81)において、上書 3 回（固定値、補数、乱数、その後検証を実施）方式を発表した。米国コンピュータ・セキュリティ・センター（The National Computer Security Center : NCSC）は DoD の規格を支持、米国軍（陸海空軍）も、3 回の上書きによる抹消方式を推奨し[5][6][7][8]、90 年代には 3 回方式が上書抹消におけるデファクト・スタンダードとなった。

しかし、2000 年代に入り、技術革新によって書込密度の向上と不良セクタの減少が実現したことを受け、2006 年に NIST が『Special Publication 800-88 (Guidelines for Media Sanitization)』のなかで「2001 年以降に製造された HDD（15GB 超）では 1 回の上書きによる消去が妥当」だとした[9]。カリフォルニア大学サンディエゴ校（University of California San Diego）を母体とする Center for Magnetic Recording Research[1]Memory and Recording Research （CMRR）も同様の研究成果を発表し[10]、データ上書きによる抹消のなかでは、固定値による 1 回書込が次第に主流になってきた。

表 1　米国政府機関等の主要な規格・ガイドライン

規定名称	発行年	組織名	書込内容	上書回数
800-88	2006	NIST	固定値	1
800-88 Revision 1	2014			
5220.22-M Sup.1	1995	DoD	固定値、補数、乱数	3
Army Regulation 380–19	1998	US Army(陸軍)	固定値、補数、乱数	3
NACSO P-5239-26	1993	US Navy (海軍)	固定値、補数、乱数	3
Air Force System Security Instruction 5020	1996	US Air Force (空軍)	固定値、補数、乱数	3

[1] 当時の名称。2015 年 7 月以降は Center for Memory and Recording Research（CMRR）に改称。

1.3 リスクアセスメントとデータ消去

その後、2007 年 10 月に示された『Clearing and Sanitization Matrix』では、DoD は、最高機密を含む媒体を除いて、1 回上書きによる磁気ディスクのデータ抹消も認めた[11]が、NIST との上書き回数論争以降、『5220.22-M』のなかで抹消の具体的な方式に言及を避けるようになった[12]。National Security Agency (NSA)は、ストレージ機器に関する消去マニュアル最新版では、磁気消去または破壊のみを機密情報消去の選択肢として認めている[13]。

NIST は「800-88」において、各媒体が含んでいる情報機密度などのリスク評価に基づき、各機関がデータ抹消の方法や技術を判断してデータ消去を行うべきとして、データ消去に関する意思決定フローの例を提示している[2][9]。2014 年の改訂版『800-88 Revision.1』(p.32)では、「データ抹消は 1 回以上の上書き（ゼロ書き込みなどの固定値）によるが、複数回のデータ上書きも選択的に実行できる」との記載変更もなされ、[2]上書き抹消における適切な書込み回数よりも、むしろ、適切な消去技術を選択する判断基準に議論の対象がシフトした形だ。

消去方法の決定には、

媒体に含まれる情報の機密度…(1)

機器を再利用するか…(2)

媒体が組織のコントロールから離れるかどうか（所管）… (3)

媒体の種類と容量…(4)

要員の確保と担当者のスキル・知識…(5)

作業のために許容できる時間…(6)

などの要素をふまえる。(1)機密度に関しては、DoD 同様、最高レベルの機密情報を含んだ媒体の処分は物理的破壊に限定している。(2)(3)も重視され、記憶媒体を再利用するのか廃棄するのかによって、適切な抹消方法は変わり、媒体が組織の管理下を離れる場合（異なる部門での再利用、外部への転売・払下げなど）にも、より厳格な抹消処理が要求されるとする。

このような消去技術の検討、消去基準の策定は、Plan（計画）⇒Do（実行）⇒Check（確認）⇒Act（再実施）を一連のマネジメント・システムとしてとらえる PDCA サイクルでいう「P（Plan：計画)」にあたる（次頁図 1)。

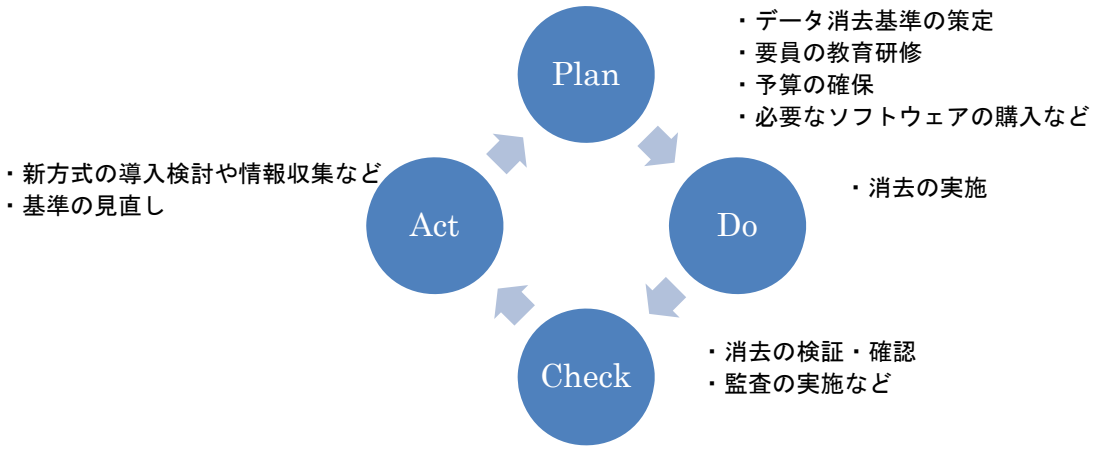
1.4 データ消去の確認・検証

NIST や空軍などが、抹消作業後の媒体から、データの 10%程度をランダムに抽出して、上書後の文字だけが復元できることを確認することで、抹消作業の検証（verification）をするよう求めている[2][6][14]。

NIST：10%以上
空軍：10%（推奨）
DoD（非公式文書での見解）：20%以上

前述の NIST（2014）では、複数人での抹消作業の実施や廃棄証明の取得などに言及し、ソフトウェア的な検証だけでなく、マンパワーによる確認を重視している。また、作業を業者などに委託する場合には、廃棄証明書を提出させるか、廃棄場所に同行するなどし、確実に消去が実施された証拠を得るよう記載している。これらは PDCA サイクルでいえば、Check に該当する（図 1）。米国では、データ抹消技術に関する議論が進み、消去が確実に行われたことを確認する仕組みを徹底する段階に入ったといえるのではないか。

図 1　データ消去マネジメントの考え方



1.5 新技術の導入

2006 年以降、NIST は、Secure Erase（ATA/Serial ATA のストレージ向けに用意されているコマンド）や暗号技術を応用した消去などにも言及するようになった[2][9]。3 章では、これら技術の米国での普及状況についても若干述べる。

2.　他国の政府機関・研究所等への広がり

米国以外にも欧米の複数国が上書きデータ消去に関するガイドラインを発行しているが、他国でも「NIST 型」または「DoD 型」消去が規定されている（表 2）。オーストラリア国防総省の情報セキュリティガイドラインは、p.147 で、2001 年以降に製造した 15GB

以上の HDD では 1 回以上の上書きでよいが、それ以前の HDD では 3 回以上の上書きを行うよう、NIST（2006 年）に沿った消去を規定している[15]。ニュージーランドでは、『情報セキュリティー・マニュアル（2011 年)』で、疑似乱数パターンを用いた 1 回の上書きがもっとも適切と規定していたが[16]、最新版（2015 年）では、オーストラリア同様に NIST（2006 年）とほぼ同じ考えを採用している[17]。カナダの『IT セキュリティー・ガイダンス（通称：ITSG-06)』は、DoD 同様に 3 回の上書きを要求しているが、部門内または同等の高セキュリティ環境下での再利用の場合には、1 回上書きによる消去を許容している。なお、いずれの国も、Secure Erase コマンドの使用を許容している[18]。

そのほか、個人研究者による上書方式として、ニュージーランドの大学に所属する研究者・グートマン（Peter Guttmann）による上書き方式などがある。データの抹消に完全を期するために 35 回もの上書きを要求する方式[19]だが、抹消作業完了までに長時間を要するため、実務上はほとんど用いられない。

表 2　米国以外の政府機関等の規格・ガイドライン

規定名称	発行年	国名	組織名	書込内容	上書回数	Secure Erase
Information Security Manual: Controls	2015	オーストラリア	Department of Defense	固定値	1（～2001 3回）	○
Information Security Manual	2015	ニュージーランド	Communications Security Bureau（通信保安局）	固定値	1	○
ITSG-06	2006	カナダ	Communications Security Establishment	固定値、補数、乱数	3（一部1回も可）	○

3.　米国におけるデータ消去の実態調査

3.1　データ消去規定

①連邦行政府

米国では、情報セキュリティポリシーや IT 資産管理ポリシーの一部として、データ消去に関する組織の方針や手順（data sanitization policy など）を作成し、ウェブサイトで公開している官公庁も多い。本報告書では、各機関のウェブサイトに公開されている規定類を検索のうえ、閲覧結果から、規格の普及状況を判断した。

日本でいう環境省にあたる米国環境保護庁（Environmental Protection Agency）は、電子機器の再利用を促しており、『連邦政府向けの機器廃棄ガイドライン』(p.1)で、NIST 800-88 を参照するよう述べている[20]。他省庁向けの消去方針サンプルでは DoD にも言及

している[21]。

国土安全保障省（Department of Homeland Security）傘下の US-CERT（United States Computer Emergency Readiness Team）は、何回の上書きが十分であるか、専門家は合意していないとし、準拠規格を明言していない[22]。

米国の連邦行政部における、データ上書きによる消去方式および Secure Erase の採用状況を表 3 に示す。

表 3　米国連邦行政部のデータ消去方法

規格（文書）名	省庁	Secure Erase
明言せず	US-CERT	○
NIST	NASA	
	商務省	
	内国歳入庁	△ （規定本文で許可を明示してはいないが、準拠する NIST800-88 が使用を推奨）
	保健福祉省	
	調達局	
	環境保護庁	
DoD	退役軍人省	○
	FBI	―

退役軍人省（Department of Veterans Affairs)では、DoD 形式に則り、少なくとも 3 回の上書きまたは磁気消去を行うよう求めており、かつ、上書によるデータ抹消を省内の PC リユースに限定して認めている[23]。FBI として知られる司法省連邦捜査局の情報セキュリティ規定も、3 回の上書を要求している[24]。一方、内国歳入庁(Internal Revenue Service)や、保健福祉省（Department of Health & Human Services)、航空宇宙局（National Aeronautics and Space Administration: NASA)、商務省、および調達局(General Services Administration)の規定は、NIST に準拠している[25][26][27][28][29][30]。

本調査で確認した 9 省庁の規定のうち、4 機関が Secure Erase をデータ抹消の方法の選択肢として採用していた[22][23][27][29]。内国歳入庁など 4 機関では、規定内で Secure Erase による抹消を明示的に許可・推奨してはいないが、いずれも NIST に準拠した消去を規定しているため、実務上は使用が認められていると思われる[20][25][26][30]。

②州政府

表 4 の通り、全 50 州中 30 の州のデータ消去関連規定を発見し、確認した。そのうち、13 州が NIST 方式に準拠していた（1 回以上の上書きとの記載を含めると 14 州)。連邦行政府ほど顕著ではないが、連邦同様に NIST が普及していた。なお、オハイオ州およびテネシー州の規定には、上書き回数や準拠方式などの情報はなかった。「NIST

または DoD に準拠した消去」など、消去の選択に幅を持たせた（曖昧な記載の）州も散見された。なお、サウスカロライナ州では、破壊または磁気消去のみが許容されていた。

表 4　米国州政府のデータ消去規定

州名	発行元	名称／発行または最終改訂年	URL	方式
Alabama	State of Alabama	Information Technology Standard: Media Sanitization, 2011	http://cybersecurity.alabama.gov/documents/standard_681s3_media_sanitization.pdf	NIST or DoD
Arizona	Government Information Technology Agency	Statewide Standard P800-S880 Rev 2.0, 2008	https://aset.az.gov/sites/default/files/P800-S880%20Media%20San%2BDisp.pdf	3 回
Arkansas	Department of Information Systems, Arkansas	State Electronic Media Cleaning Guidelines, 2012	http://www.dis.arkansas.gov/policiesStandards/Pages/elecdisposal.aspx	NIST
California	California Information Technology Managers Academy, Class XVI	IT Best Practices: Asset Life Cycle	http://cio.ca.gov/opd/pdf/itma/XVI_Asset_Lifecycle.pdf	NIST
Colorado	Governor's Office of Innovation and Technology	Colorado Data Destruction Policy and Computer/Other Electronic Media End-of-Life Policy, 2004	https://www.coloradoci.com/bin-pdf/0200/elecmedia.pdf	DoD
Connecticut	CJIS Governing Board	CT CJIS Security Policy V. 1.0, 2014	http://www.ct.gov/cjis/lib/cjis/publications/CT_CJIS_Security_Policy_Final.pdf	3 回
Florida	Department of Management Services	Electronic Media Sanitization, 2009	http://www.dms.myflorida.com/content/download/59124/249647/file/IT	NIST
Georgia	Georgia Technology Authority	Media Sanitization - Vendor Return, 2008	https://gta.georgia.gov/psg/article/media-sanitization-vendor-return	NIST
Idaho	Idaho Technology Authority (ITA)	Cleansing Data From Surplus Computer Equipment, 2005	http://ita.idaho.gov/psg/g550.pdf	1 回以上
Illinois	Department of Central Management Systems	Electronics Recycling/Data Wipe Policy Memorandum, 2013	https://www.illinois.gov/cms/agency/recycling/Documents/2013Datawipe-DisposalPolicy.pdf	3 回
Kansas	Kansas Information Technology Executive Council	Information Technology Policy: Enterprise Media Sanitization and Disposal Policy, 2009	https://oits.ks.gov/docs/default-source/kitodocumentlibrary/ITEC-Policies/itecitpolicy7900.htm	NIST or DoD
Kentucky	Commonwealth Office of Technology	CIO-092 Media Protection Policy, 2014	http://technology.ky.gov/policy/Pages/CIO-092.aspx	NIST
Louisiana	State of Louisiana Office	Data Sanitization Standards and	http://www.doa.la.gov/OTS/pdfs/Standards/IT%20STD%201-17.p	1 回 or 3 回

州名	発行元	名称／発行または最終改訂年	URL	方式
	of Technology Services	Requirements: IT SOP 1-17	df	
Maryland	State of Maryland	Information Security Policy, 2013	http://doit.maryland.gov/publications/doitsecuritypolicy.pdf	NIST
Minnesota	Office of Enterprise Technology	Enterprise Security Information Sanitization and Destruction Standard, 2010	https://mn.gov/mnit/images/SEC_S_Information_Sanitization_and_Destruction.pdf	6 回
Mississippi	Mississippi Department of Finance & Administration	Letter of Certification of Disposal For Computer Storage Media	http://www.dfa.state.ms.us/Offices/SurProp/Forms/Computer%20disposal%20certification.pdf	DoD
New Jersey	State of New Jersey IT Circular	Information Disposal and Media Sanitization Standard、2015	http://www.nj.gov/it/ps/09-10-S1-NJOIT_152-01-NJOIT_Information_Disposal_Media_Sanitization_Standard.pdf	NIST
New York	New York State	IT Standard: Sanitization/Secure Disposal, 2014	https://www.its.ny.gov/sites/default/files/documents/Enterprise_Sanitization_Secure_Disposal_Standard_v1.1.pdf	NIST
Ohio	State of Ohio	IT Policy Disposal, Servicing and Transfer of IT Equipment, 2008	http://das.ohio.gov/Portals/0/DASDivisions/DirectorsOffice/pdf/policies/informationtechnology/ITP-E.1.pdf	不明
Oregon	Department of Administrative Services	Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery) Exhibit. A DSS Clearing and Sanitization Matrix, 2007	http://www.oregon.gov/DAS/OP/docs/DSS%20Clearing%20and%20Sanitization%20Matrix.pdf	NIST
Pennsylvania	Office of Administration	Information Technology Policy Data Cleansing Policy, 2013	http://www.oa.pa.gov/Policies/Documents/itp_sec015.pdf	NIST or DoD
Rhode Island	—	Media Handling and Security, 2007	http://www.doit.ri.gov/documents/policies/Operations/05-01%20Media%20Handling%20and%20Security.pdf	DoD or Guttmann
South Carolina	Division of Information Security (DIS)	Information Security and Privacy Standards, 2013	http://www.admin.sc.gov/files/InformationSecurityPolicy-DataProtectionandPrivacy.pdf	破壊 or 消磁
Tennessee	Department of Finance and Administration Office for Information Resources	Information Security Program Document Version 2.0, 2014	https://www.tn.gov/assets/entities/finance/oir/attachments/PUBLIC-Enterprise-Information-Security-Policies-v2.0_1.pdf	不明
Texas	—	Texas Administrative Code: Chapter 202 Information Security Standards, 2015	http://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=2&p_dir=&p_rloc=142456&p_tloc=&p_ploc=&pg=1&p_tac=142456&ti=1&pt=10&ch=202&rl=1&dt=&z_chk=&z_contains=	NIST or DoD

州名	発行元	名称／発行または最終改訂年	URL	方式
Utah	Department of Administrative Services	Enterprise Information Security Policy, 2013	http://www.das.utah.gov/policies/21-policies-and-procedures/46-enterprise-information-security-policy.html	NIST
Vermont	State of Vermont	Digital Media and Hardware Disposal Standard	http://dii.vermont.gov/sites/dii/files/PDF/Policies_Reports/Digital-Media-and-Hardware-Disposal-Standard.pdf	DoD (7 回)
Virginia	Virginia Information Technologies Agency	Information Technology Resource Management Standard: Removal of Commonwealth Data from Electronic Media Standard	http://vita.virginia.gov/uploadedFiles/VITA_Main_Public/Library/PSGs/RemovalCOVDataElectMediaStandardSEC51404.pdf	NIST
Washington	Office of the CIO, Washington State	Securing Information Technology Assets Standards	https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets-3	NIST
West Virginia	Office of Technology	Procedures for Sanitization, Retirement and Disposition of Information Technology Equipment	http://apps.sos.wv.gov/adlaw/csr/readfile.aspx?DocId=26599&Format=PDF	NIST

③大学

表 5 の通り、46 校の大学の規定を発見し、確認した。

DoD 方式準拠が 16 校あり、官公庁とは逆に、DoD に準拠した機関が最多であった。NIST 準拠をうたう機関は 8 校（1 回以上の上書きとの記載を含めると 10 校）にとどまった。

表 5　米国大学のデータ消去規定

大学名	州名	名称／発行または最終改訂年	URL	規格
Auburn University	Alabama	Electronic Data Disposal Policy and Procedures, 2015	http://www.auburn.edu/oit/it_policies/electronic_data_disposal.php	DoD （第一選択肢は消磁）
Stanford University	California	Data Sanitization Policy and Guideline, 2015	https://itservices.stanford.edu/security/data-sanitization NIST-BC Wipe	NIST
University of California, Berkeley	California	Secure Deletion Guideline	https://security.berkeley.edu/secure-deletion-guideline	DoD

大学名	州名	名称／発行または最終改訂年	URL	規格
University of California, Riverside	California	Methods of Data Sanitization Recommendations & Procedure, 2013	http://cnc.ucr.edu/security/dsmethods.html#erase	複数回
University of Northern Colorado	Colorado	Media Disposition and Sanitation Procedure, 2006	http://www.unco.edu/it/Policies/MediaDisposition&SanitationProcedure.pdf	NIST
University of Delaware	Delaware	Windows whole disk erase: Disk Eraser, 2013	https://www.udel.edu/it/help/pii/erasing/wde_windows.html	ツール名称
University of Hawaii	Hawaii	Securely Deleting Electronic Information, 2015	http://www.hawaii.edu/askus/706	ツール名称
Loyora University Chicago,	Illinois	Secure Deletion Procedure, 2015	http://www.luc.edu/its/itspoliciesguidelines/securedeletionprocedure/	ツール名称
Northwestern University	Illinois	Disposal of Northwestern University Computers, 2013	http://www.it.northwestern.edu/policies/disposal.html	DoD
University of Illinois	Illinois	Standards and Guidelines: Disposal of Digital Media Standard, 2013	http://accc.uic.edu/policy/disk-scrubbing	DoD (1 回)
Eastern Illinois University	Illinois	Information Security Guidelines for Media Sanitization and Disposal	http://www.eiu.edu/its/security/policies/Information%20Security%20Guidelines%20for%20Media%20Sanitization%20and%20Disposal%20-%201.pdf	3 回 （磁気ディスク以外は NIST）
Indiana University	Indiana	Secure Data Removal	https://protect.iu.edu/online-safety/protect-data/data-removal.html	ツール名称
Indiana University–Purdue University Indianapolis	Indiana	Disposition of Electronic Media, 2014	http://www.engr.iupui.edu/sites/cnc/techpolicies/disposition-of-electronic-media.php	DoD
Purdue University	Indiana	Media Disposal Guidelines, 2011	http://www.purdue.edu/securepurdue/docs/policies/MediaDisposalGuidelines.pdf	DoD
Kansas State University	Kansas	Media Sanitization and Disposal Policy, 2009	http://www.k-state.edu/policies/ppm/3400/3436.html#procedures	3 回(NIST)
University of Kansas	Kansas	KUMC Computer Equipment Disposal and Media Sanitization	http://policy.ku.edu/KUMC/information-resources/equipment-disposal	DoD
Louisiana State University,	Louisiana	IT-STD 1-17 Data Sanitization	http://www.doa.la.gov/OTS/pdfs/Standards/IT%20STD%201-17.pdf	1 回以上
University of Massachusetts Boston	Massachusetts	Standards for the Redistribution and Disposition of Computer Equipment and Electronic Storage Devices, 2007	http://media.umassp.edu/massedu/policy/CompEquipElecStorageDevDisp.pdf	DoD （1 回）
Massachusetts Institute of Technology	Massachusetts	Removing Sensitive Data, 2015	http://kb.mit.edu/confluence/display/istcontrib/Removing+Sensitive+Data	複数回
Michigan State University	Michigan	How to sanitize data for disposal - TB6567, 2012	http://techbase.msu.edu/article.asp?id=6567&service=techbase	ツール名称

大学名	州名	名称／発行または最終改訂年	URL	規格
University of Michigan Health and Retirement Study	Michigan	Data Destruction Policy and Procedures, 2014	http://hrsonline.isr.umich.edu/sitedocs/rda/DataDestructionPolicyProcedures.pdf	ツール名称
Western Michigan University	Michigan	Office of Information Technology, Data Wiping Software	http://wmich.edu/it/policiesdatawipesoftware	ツール名称
University of Minnesota	Minnesota	Media Sanitization, 2014	http://it.umn.edu/enterprise-standards/information-security-standards/media-sanitization	NIST
KU School of Medicine	Missouri	Disposal and Media Sanitization	http://wichita.kumc.edu/Documents/wichita/its/KUSMW_equip_disposal.pdf	DoD
University of Missouri	Missouri	Disposal of Digital Files and Media	http://www.umsl.edu/technology/security/files/pdfs/pdfs/Policy%20for%20the%20Disposal%20of%20Electronic%20Files%20and%20Media.pdf	DoD (用途によって異なる)
Montana Tech University	Montana	Information Technology Policy 1308 - Disposal of Computer Storage Devices	http://www.mtech.edu/accreditation/exhibits/standard5/IT/Required%20Exhibits/2/Montana%20Board%20of%20Regents%20IT%20Policies/1308.htm	DoD
Columbia University	New York	Data Sanitization / Disposal of Electronic Equipment Policy, 2008	http://policylibrary.columbia.edu/files/policylib/imce_shared/Data_Sanitization_Policy_-_final.pdf	ツール名称
Cornell University	New York	Best practices for media destruction, 2014	http://www.it.cornell.edu/security/how.cfm?cat=6&tip=57	DoD
New York University	New York	Standard for Destruction and Disposal of Electronic Equipment, 2015	http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/standard-for-destruction-and-disposal-of-electronic-equipment-an.html	DoD
Syracuse University	New York	Information Technology Standard for Data Sanitizing: Information Technology and Services Information Security Standard, 2014	http://its.syr.edu/infosec/docs/policies/Data_Sanitizing.pdf	Guttmann
University at Buffalo, The State University of New York	New York	Standards for Securing Regulated Private Data Policy, 2011	https://www.buffalo.edu/content/dam/www/ubit/it-policies/StandardsRegPrivData.pdf	DoD
University of North Carolina at Chapel Hill	North Carolina	UNC-Chapel Hill Campus Standards for Electronic Media Disposal, 2014	http://help.unc.edu/help/unc-chapel-hill-campus-standards-for-electronic-media-disposal/	DoD (部署内の譲渡の場合、再フォーマットも可)
University of Cincinnati	Ohio	Media Sanitization, 2013	https://www.uc.edu/content/dam/uc/infosec/docs/general/Standard_9_1_8_Electronic_Media_Sanitization.pdf	DoD
Carnegie Mellon University	Pennsylvania	Guidelines for Data Protection	http://www.cmu.edu/iso/governance/guidelines/data-protection/media-sanitization.html	NIST

大学名	州名	名称／発行または最終改訂年	URL	規格
University of Pennsylvania	Pennsylvania	Secure Data Deletion, 2015	http://www.upenn.edu/computing/security/privacy/data_clear.php	NIST
Brown University	Rhode Island	Data Removal Recommendations, 2014	https://it.brown.edu/computing-policies/electronic-equipment-disposition-policy/data-removal-recommendations	**複数回**
University of South Carolina School of Medicine	South Carolina	Electronic Data Disposal Policy	http://ccr.med.sc.edu/Electronic%20Data%20Disposal%20Policy.doc	3 回
University of Tennessee	Tennessee	Media Sanitization Best Practice, 2008	https://security.tennessee.edu/pdfs/msbp.pdf	NIST
Baylor University	Texas	Disposition of Computer Equipment, 2014	http://www.baylor.edu/its/index.php?id=43834	DoD（準拠できない場合は破壊）
University of Texas at Tyler	Texas	Computer Redistribution/Disposal Policy and Procedures	https://www.uttyler.edu/iso/files/ComputerRedistributionPolicyandProcedures.pdf	**ツール名称**
University of Utah	Utah	University Rule 4-004L: Information System Media Handling Rev. 0.（**制定中**）	http://regulations.utah.edu/it/rules/Rule4-004L.php	NIST
George Mason University, College of Science	Virginia	Data Sanitization Policy, 2014	https://cos.gmu.edu/wp-content/uploads/2014/03/College-of-Science-Data-Sanitization-Policy.pdf	**ツール名称**
University of Vermont	Vermont	Disposal of Surplus Computers and Electronic Waste	https://www.uvm.edu/it/security/erase/	**複数回**
Longwood University	Virginia	Electronic Data Disposal Standards, 2011	http://www.longwood.edu/infosec/39048.htm	1 回以上
University of Washington	Washington	Computer Disposal Policy	http://www.washington.edu/facilities/finadmin/movingandsurplus/surplussing	NIST
University of Wyoming	Wyoming	Electronic Devices and Media Transfer/Sale/Disposal Procedures, 2006	http://www.uwyo.edu/administration/fiscal/property/_files/docs/electronic%20devices%20and%20media%20transfer.doc	DoD

準拠する規格（文章）名でなく、抹消作業に指定するソフトウェアを例示列挙する大学が 10 校あり、官公庁の規定と比べて、より実務的な規定が目立った。DoD 準拠の Darik's Boot and Nuke （通称 DBAN）のほか、Eraser などのフリーソフトウェアの記載率が高かったが、シェアウェア、商業ソフトも利用されている。大学のデータ消去規定は、事務局や担当者が閲覧するだけでなく、抹消規格に関する知識のない学生たちにも理解できるよう媒体の消去方法を指示する「作業マニュアル」でもあるためか、作業画面をキャプチャするなどして、より具体的な記載をした機関も見られた。以下、名前が挙がっていたソフトウェア・ツール名を表 6 に示す。

表 6　データ抹消ソフトウェアの例

名称
Darik's Boot and Nuke (DBAN) [2]　(Free)
Active@KillDisk by L Soft Technologies, Inc[3]. (Free)
Eraser by Heidi Computers, LTD (Free)
Wiperaser XP by LIVeye, SDC (Shareware)
BC-WIPE[4] (shareware) by Tucows, Inc.
GDISK by Symantec, Inc.
DriveScrubber by iolo[5]

ここでは、とくに、イリノイ州の関連制度および大学の規定内容を紹介する。

Almeling ほか法曹家 4 名の調査によれば、イリノイ州は、全米の連邦地方裁判所のなかでもっとも営業秘密に関する訴訟が多い州で、かつ、同州の州法は、営業秘密訴訟において、州法のなかではもっとも適用される割合が高い[31]。訴訟を念頭に置いたクリーンな媒体を準備するにあたって、合理的に求められる消去方法を判断する意味でも同州の状況は参考になると思われる。特徴的な点は、イリノイ州にある調査対象大学のいずれも、DoD 規格の準拠または 3 回以上の上書抹消を求める規定を整備していたことである。同州では、州法（*Illinois Public Act 97-0030*）で、磁気ディスクのデータは、3 回以上の上書を実行するよう義務づけている[32] (10 回の上書きによる抹消が求められていた[33]が、作業に長時間を要するため、ほとんど遵守されず、2006 年に 3 回へと要件が緩和された)。

同州のイリノイ大学（University of Illinois）では、媒体が組織の管理を離れるかどうかを考慮して、消去方法を決定する。学部内や個人間の譲渡には、1 回の上書によるデータ抹消を認めているが、学外への譲渡に関しては、DBAN の DoD Short モードによる抹消を必須と規定している（次頁表 7)。同大学では、Secure Erase や、暗号鍵の削除によるデータ抹消など、規定された選択肢も幅広く、データ消去への意識が高い。

[2] http://www.dban.org/
[3] http://www.killdisk.com/downloadfree.htm
[4] www.jetico.com
[5] http://www.iolo.com/products/drivescrubber/?siteID=je6NUbpObpQ-GuqYaeTv7j6AS6mHcydfTg

表 7 イリノイ大学における上書抹消

媒体の用途	必須	推奨
大学の余剰品	1 回上書き （DBAN【クイックイレースモード】など）	DBAN【DoD Short モード】 または同等の消去法
部門間の譲渡	1 回上書き	DBAN【DoD Short モード】 または同等の消去法
個人間の譲渡	1 回上書き	DBAN【DoD Short モード】 または同等の消去法
学外への譲渡	DBAN【DoD Short モード】	DBAN【DoD Short モード】 または同等の消去法
ベンダーへの 不良品の返品	ベンダーからの文書による証明	—

出典：イリノイ大学ホームページ　http://accc.uic.edu/policy/disk-scrubbing を和訳

官公庁、大学を問わず、調査対象全体に、抹消の検証、廃棄証明のどちらかまたは両方を求める規定が見られた。証明書の記載事項は特に統一されてはいないが、抹消ソフトウェア名など方法の情報および媒体の詳細情報を含むのが一般的である。官公庁のフォーマット例としては、NIST が廃棄証明書のサンプルを公開している[2]ほか、「Computer Hard Drive Certificate DLA Form 2500: Certificate of Hard Drive Disposition (旧 DLIS Form 1867)」などがある[34]。なお、前述の *Illinois Public Act* でも、(1)機器のシリアルナンバー、(2)使用したソフトウェア名称、(3)処理担当者の名前、作業日、および担当者のサインを含めた証明書の提出が要求される。

DoD 方式にのっとった抹消が行えない場合は物理的に破壊するよう規定したベイラー大学（Baylor University）や磁気消去を優先するオーバーン大学（Auburn University）もあった。

このように、米国ではデータ消去規定を整備した機関が多いが、ユタ大学（University of Utah）などは、NIST 準拠であることは明記しているものの、ポリシーの詳細は制定中であった。上位のポリシーにおいて、適切なデータ消去を行うように一文を規定するにとどめ、具体的なデータ消去方法が明示されていないこともあった。また、容易に規定を発見できない機関も複数あった（規定を非公開または未作成）ことも記しておく。そのほか、業者の連絡先のみを掲載しているなど、業者に一任しており、データ消去に対して意識が低いと思われる機関なども発見された。

3.2　消去の実施状況

情報公開への要求に応えるため、一部の行政機関や州政府が、廃棄・再利用前後の PC の一部を抽出してデータ抹消状況を監査のうえ、報告書として公開している。

① 連邦行政府

NASA の監査部門は、一部の PC が機密情報を含んだまま外部へ譲渡されたり、宇宙センターへの一般客が、公開エリアに設置された PC から機密情報が閲覧可能だった、と

いう、インシデントを契機として、監査報告書『IT 機器の廃棄に関するレビュー』（2010年度）を発行している。当報告書では、原因として、(i)NASA 内部のセキュリティ委員会または DoD が未承認の抹消ソフトウェアを使用する拠点の存在、(ii)一部拠点のデータ消去規定の未整備、(iii)ベリファイプロセスの実施不足および担当者の理解不足、の 3 点が指摘された[35]。とりわけ、ベリファイの実施が不十分なことが問題視されている。公共機関では、機器の廃棄・再利用にあたって、適切に在庫を管理するとともに、情報漏洩を防いでいることを第三者に説明する責任があるとして、適切な抹消技術の導入とともに、実施の確認と記録を重視している。

② 大学

カリフォルニア大学リバーサイド校（University of California, Riverside）では、データ消去の学部別実施状況を公開している。以下、表 8 に示す。この大学の規定では、複数回の書込による上書抹消のほか、磁気破壊、物理的破壊を使い分けて適切なデータ消去を行うよう指示しており、本表を見ると、Anderson graduate School of Management、Computing & Communications などの学部では、規定を遵守した消去が行われているのが見て取れる。しかし、複数の学部で消去方法が pending（保留）とされており、規定の遵守状況にはばらつきがある。おそらく、規定策定済みの他機関でも同様だと思われるが、詳細は、実地調査などの追加調査を要する。

表 8　カリフォルニア大学における磁気ディスクのデータ消去方法

組織名	方法 1	方法 2	方法 3
Anderson graduate School of Management	DBAN（上書消去）	物理的破壊	N/A
Finance & Business Operations	Active Kill Disk（上書消去）	N/A	N/A
Biomedical Sciences	再フォーマット	DBAN	N/A
Chancellor/ EVC office	HDD と磁気の保持	N/A	N/A
Computing & Communications	上書消去	磁気消去	物理的破壊
図書館	機密情報はネットワーク上にのみ保存、個人 PC に保存不可	フォレンジック・ツールによる上書消去	専門業者による物理的破壊
UNEX	物理的破壊	N/A	N/A
VCSA Tech Services	Norton Wipedisc（上書消去）	再利用前のサーバーの上書きおよびリロード	N/A
Vice Chancellor University Advancement	サーバー：物理的破壊	ワークステーション・ラップトップ：DBAN（上書消去）	Treos: ハードウェアリセット
CNAS,COE,CHASS, GSOE, VCR, 大学院	保留		

出典： カリフォルニア大学リバーサイド校ホームページ

http://cnc.ucr.edu/security/dsorgpract.html を和訳、加筆

4. 考察

HDD などに対するデータ抹消方式の研究開発および普及に主導的役割を果たしている米国では、DoD または NIST の規格が広く利用されている。90 年代は 3 回上書方式が主流だったが、社会・技術の変化にともない、2000 年代中盤以降、NIST や CMRR の説が広く賛同を得て、実務上は上書き回数 1 回の抹消が主流になってきたといわれる。本調査で米国官公庁および大学のデータ消去規定を閲覧調査したところ、NIST 方式を採用する組織が多かった。ただし、州法で磁気ディスクに対する 3 回上書き抹消を求める州もあり、DoD 規格準拠または 3 回のデータ上書きを求める機関（特に大学）もいまだ見られた。なお、その場合でも、内部の譲渡に関しては 1 度の上書き処理を認めるなど、一部媒体には 1 回上書きを適用しているケースがあった。

媒体ごとに適切なデータ消去方法を選択するための組織の意思決定の基準策定、抹消の検証および確認の重視など、確実な消去を行うため、いわばデータ消去に関するマネジメントとでもいうべき態勢づくりを重視する傾向が 2000 年代以降の規格文書に見られ、調査対象機関でもそれを裏付ける規定が散見された。

本調査では、ウェブサイトで公開されている規定類の閲覧調査が主であり、実施実績の情報は少なかった。今回調査対象とした機関の担当者へのインタビュー調査なども行い、データ消去のより正確な実態を把握したいと考えている。

参考文献（全て 2016 年 4 月 1 日時点）

[1] Garfinkel, Shelat, Remembrance of Data Passed: A Study of Disk Sanitization Practices, *IEEE Security & Privacy*, Vol.1, Issue 1 (2003).

[2] National Institute of Standards and Technology, Guidelines for Media Sanitization, Special Publication 800-88, Revision 1 (2014). http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

[3] U.S. Department of Defense, DoD 5200.28-M ADP Security Manual, pp.41 (1973). http://biotech.law.lsu.edu/blaw/dodd/corres/pdf2/p520028m.pdf

[4] U.S. Department of Defense, National Industrial Security Program: Operating Manual, DoD 5220.22-M-Supp-1 (1995). http://www.dtic.mil/whs/directives/corres/pdf/522022MSup1.pdf

[5] National Computer Security Center, NCSC-TG-025 Ver.2: A Guide to Understanding Data Remanence in Automated Information Systems (1991). https://fas.org/irp/nsa/rainbow/tg025-2.htm

[6] US Air Force, Air Force System Security Instruction 5020: Remanence Security, (1996) https://cryptome.org/afssi5020.htm#Chapter 2

[7] US Army, Army Regulation 380–19: Information Systems Security (1998). http://fas.org/irp/doddir/army/r380_19.pdf

[8] US Navy, Remanence Security Guidebook Module 26 : NAVSO P-5239-26, Chapter 3.3 (1993) http://fas.org/irp/doddir/navy/5239_26.htm

[9] National Institute of Standards and Technology, Guidelines for Media Sanitization, Special Publication 800-88 (2006). http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50819

[10] Hughes and Coughlin, Tutorial on Disk Drive Data Sanitization, Center for Magnetic Recording Research (2007). http://cmrr.ucsd.edu/people/Hughes/documents/DataSanitizationTutorial.pdf

[11] U.S. Department of Defense, Defense Security Service, Industrial Security Program Office, Industrial Security Letter, October 1, pp.18-19 (2007). http://www.dss.mil/documents/pressroom/isl_2007_01_oct_11_2007_final_agreement.pdf

[12] U.S. Department of Defense, National Industrial Security Program: Operating Manual, DoD 5220.22-M (2006). http://www.dss.mil/documents/odaa/nispom2006-5220.pdf

[13] National Security Agency, Central Security Service Policy Manual 9-12 (Storage Device Sanitization Manual) (2014). https://www.nsa.gov/ia/_files/Government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf

[14] Department of Defense Memorandum, Disposition of Unclassified DoD Computer Hard Drives (2001). http://www.au.af.mil/au/holmcenter/AFJROTC/documents/DispositionofUnclassifiedDoDComputerHardDrives.pdf

[15] Australia Department of Defense, Australian Government Information Security Manual: Controls, pp.147 (2015). http://www.asd.gov.au/publications/Information_Security_Manual_2015_Controls.pdf

[16] New Zealand Government Communications Security Bureau, Information Security Manual,pp.154 (2011). http://www.nzic.govt.nz/assets/Publications/GCSB-NZ-Information-Security-Manual-2011.pdf

[17] New Zealand Government Communications Security Bureau, Information Security Manual pp.281, (2015). http://www.gcsb.govt.nz/assets/GSCB-NZISM/NZISM-MAY-2015-v2.3.pdf

[18] Communications Security Establishment, Canada, IT Security Guidance: Clearing and Declassifying Electronic Data Storage Devices (ITSG-06) pp.6, 12, (2006).

https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg06-eng.pdf

[19] Gutmann, P, Secure Deletion of Data from Magnetic and Solid-State Memory. In: Proceedings of the Sixth USENIX Security Symposium, San Jose, CA, July 22-25, pp. 77–90 (1996). http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

[20] U.S. Environmental Protection Agency, Media Sanitization Considerations for Federal Electronics at End-of-Life, pp.1 (2012).
http://www.epa.gov/sites/production/files/documents/sanitization.pdf

[21] U.S. Environmental Protection Agency, Sample Policy and Guidance Language for Federal Media Sanitization (2012).
http://www.epa.gov/sites/production/files/documents/sanitization_sample.pdf

[22] Linda Pesante, Christopher King, and George Silowash, U.S. Computer Emergency Readiness Team, Disposing of Devices Safely, pp.2 (2012).
https://www.us-cert.gov/sites/default/files/publications/DisposeDevicesSafely.pdf

[23] U.S. Department of Veterans Affairs, VA Handbook 6500.1: 2008 20420 Transmittal Sheet Electronic Media Sanitization, pp.46.
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=416&FTy

[24] U.S Department of Justice Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Security Policy, pp.48.
https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center

[25] Internal Revenue Service, IRS Publication 1075 Media Sanitation Requirements Explained (2015).
https://www.irs.gov/uac/IRS-Publication-1075-Media-Sanitation-Requirements-Explained

[26] U.S. Department of Health & Human Services, Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals (2013).
http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

[27] National Aeronautics and Space Administration NASA Shared Services Center, D NSPWI_2800-0008: Data Center Guidelines for Digital Media Sanitization, pp.8 (2015).
https://searchpub.nssc.nasa.gov/servlet/sm.web.Fetch/NSPWI_2800-0008_Data_Center_Guidelines_for_Digital_Media_Sanitization_Rev_0003.pdf?rhid=1000&did=1849379&type=released

[28] National Aeronautics and Space Administration Office of the Chief Information Officer, Standard Operating Procedure: Digital Media Sanitization (2011).
http://www.nasa.gov/pdf/419924main_ITS-HB_0035-%20_.pdf

[29] Department of Commerce, Property Bulletin #5 (2011).
http://www.osec.doc.gov/ofm/OAP/PPMTD/Documents/Property_Bulletins/Property%20

Bulletin%20FY11-5,%20DOC%20Media%20Sanitization.pdf

[30] General Services Administration, GSA Bulletin FMR B-34 Disposal of Federal Electronic Assets (2012).
http://www.gsa.gov/portal/mediaId/188555/fileName/FMR_Bulletin_B-34__Disposal_of_Federal_Electronic_Assets.action

[31] David S. Almeling et al., A Statistical Analysis of Trade Secret Litigation in Federal Courts, 45 *GONZAGA L. REV.* pp.306, 310.

[32] Illinois General Assembly, The Data Security on State Computers Act (Public Act 93-0306 as amended by Illinois Public Act 97-0390) .
http://www.ilga.gov/legislation/publicacts/fulltext.asp?name=093-0306

[33] Illinois General Assembly, Public Act 93-0306.
http://www.ilga.gov/legislation/publicacts/93/093-0306.htm

[34] Defense Logistics Agency, Computer Hard Drive Certificate DLA Form 2500, Certificate of Hard Drive Disposition.
http://www.dla.mil/Portals/104/Documents/DispositionServices/Receiving/Usable/DISP_DL2500P.pdf

[35] National Aeronautics and Space Administration, Office of Audits, Preparing for The Space Shuttle Program's Retirement: A Review of NASA'S Disposition of Information Technology Equipment (2010).
https://oig.nasa.gov/audits/reports/FY11/IG-11-009.pdf

・各州政府および大学のウェブサイト
本文中（表 4 および表 5）に記載