

# 米国国防省 コンピュータ(HDD) データ消去3つのガイドライン


このガイドラインへのアクセス方法



# http://www.dhra.mil/perserec/osg/



DEFENSE HUMAN RESOURCES ACTIVITY  
U.S. DEPARTMENT OF DEFENSE

Search Defense Human R 

OVERVIEW HEADQUARTERS LEADERSHIP  COMPONENTS

OVERVIEW > PERSEREC > OSG

## PERSEREC

[Home](#)  
[History](#)  
[Vision](#)  
[Initiatives](#)  
[Past Achievements](#)  
[Products](#)  
[Selected Reports](#)  
[Grant Program](#)  
[FAQs](#)  
[Contact Us](#)  
[Privacy Policy](#)  
[Accessibility](#)

## Online Guide to Security Responsibilities

### Download and Installation Instructions

You may wish to print out these instructions. This download is a "zipped" file. After clicking on "Click here to Download" (below), follow instructions on how to save (chose save rather than open from dialog box options), unzip and extract the zipped files. You will need to select the location where the Online Security Guide files will be stored. You will find them in that location in a folder called OSG.

To view these files, open the OSG folder and scroll down to the file index.htm. A double-click on this file opens the Online Security Guide program.

For quick access to this program in the future, you have two options. One is to simply bookmark this URL in your browser. The other is to right-click on index.htm and select Create Shortcut. This creates a new file called Shortcut to index.htm. This file can be renamed Online Security Guide or OSG and then dragged and dropped to any convenient location, such as your Desktop.

MD5 checksum: 7fdb1e7d1e246cd96d4adb1a63f5de63

[Click here to download](#)




[About DoD](#)  
[Top Issues](#)  
[News](#)  
[Photos & Videos](#)  
[DoD Careers](#)  
[FOIA](#)  
[No Fear Act](#)  
[Accessibility Policy](#)  
[Privacy Policy](#)  
[Link Disclaimer](#)

# Click here to download 赤丸クリック



DEFENSE HUMAN RESOURCES ACTIVITY  
U.S. DEPARTMENT OF DEFENSE

Search Defense Human R 

OVERVIEW HEADQUARTERS LEADERSHIP  COMPONENTS

OVERVIEW > PERSEREC > OSG

## PERSEREC

- Home
- History
- Vision
- Initiatives
- Past Achievements
- Products
- Selected Reports
- Grant Program
- FAQs
- Contact Us
- Privacy Policy
- Accessibility

## Online Guide to Security Responsibilities

### Download and Installation Instructions

You may wish to print out these instructions. This download is a "zipped" file. After clicking on "Click here to Download" (below), follow instructions on how to save (chose save rather than open from dialog box options), unzip and extract the zipped files. You will need to select the location where the Online Security Guide files will be stored. You will find them in that location in a folder called OSG.

To view these files, open the OSG folder and scroll down to the file index.htm. A double-click on this file opens the Online Security Guide program.

For quick access to this program in the future, you have two options. One is to simply bookmark this URL in your browser. The other is to right-click on index.htm and select Create Shortcut. This creates a new file called Shortcut to index.htm. This file can be renamed Online Security Guide or OSG and then dragged and dropped to any convenient location, such as your Desktop.

MD5 checksum: 7fdb1e7d1e246cd96d4adb1a63f5de63

[Click here to download](#)



- About DoD
- Top Issues
- News
- Photos & Videos
- DoD Careers
- FOIA
- No Fear Act
- Accessibility Policy
- Privacy Policy
- Link Disclaimer

# ファイルを開く

The screenshot shows a web browser window with a menu bar at the top containing: ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H). The main content area displays the 'DEFENSE HUMAN RESOURCES ACTIVITY' website. The page title is 'DEFENSE HUMAN RESOURCES ACTIVITY U.S. DEPARTMENT OF DEFENSE'. The navigation menu includes: OVERVIEW HEADQUARTERS LEADERSHIP COMPONENTS. The breadcrumb trail is: OVERVIEW > PERSEREC > OSG. The main content area features a sidebar with links: PERSEREC, Home, History, Vision, Initiatives, Past Achievements, Products, Selected Reports, Grant Program, FAQs, Contact Us, Privacy Policy, and Accessibility. The main content area is titled 'Online Guide to Security Responsibilities' and includes a 'Download and Installation Instructions' section. A 'Click here to download' link is visible. At the bottom of the page, there are links for: About DoD, Top Issues, News, Photos & Videos, DoD Careers, FOIA, No Fear Act, Accessibility Policy, Privacy Policy, and Link Disclaimer. A yellow download dialog box is overlaid on the page, displaying the text: 'dhra.mil から osg.zip (3.11 MB) を開くか、または保存しますか?'. The dialog box has three buttons: 'ファイルを開く(O)', '保存(S)', and 'キャンセル(C)'. The Windows taskbar at the bottom shows the system tray with the date and time: 2018/09/03 8:46.

# 赤丸すべてはい(E)をクリック

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

DEFENSE HUMAN RESOURCES ACTIVITY  
U.S. DEPARTMENT OF DEFENSE

Search Defense Human R

OVERVIEW HEADQUARTERS LEADERSHIP COMPONENTS

OVERVIEW > PERSEREC > OSG

**PERSEREC**  
Home  
History  
Vision  
Initiatives  
Past Achievements  
Products  
Selected Reports  
Grant Program  
FAQs  
Contact Us  
Privacy Policy  
Accessibility

**Online Guide to Security Responsibilities**  
Download and Installation Instructions

You may wish to print out these instructions. This download is a "zipped" file. After clicking on "Click here to Download" (below), follow instructions on how to save (chose save rather than open from dialog box options), unzip and extract the zipped files. You will need to select the location where the Online Security Guide files will be stored. You will find them in that location in a folder called OSG.

To view these files, open the OSG folder and scroll down to the file index.htm. A double-click on this file opens the Online Security Guide program.

For quick access, click on the link to download the files to your browser. The other is to right-click on index.htm, select "Save As" and save the files to your computer. The files will be renamed Online Security Guide or OSG and then index.htm.

MD5 checksums

既にあるファイルが存在します。

現在のファイル

6 KB (5,384 バイト)	更新日時: 2012/04/11 13:52:56
6 KB (5,384 バイト)	更新日時: 2012/04/11 13:52:56

名前をつけて保存(A)

「すべて」、「キャンセル」はこのアーカイブに適用する。

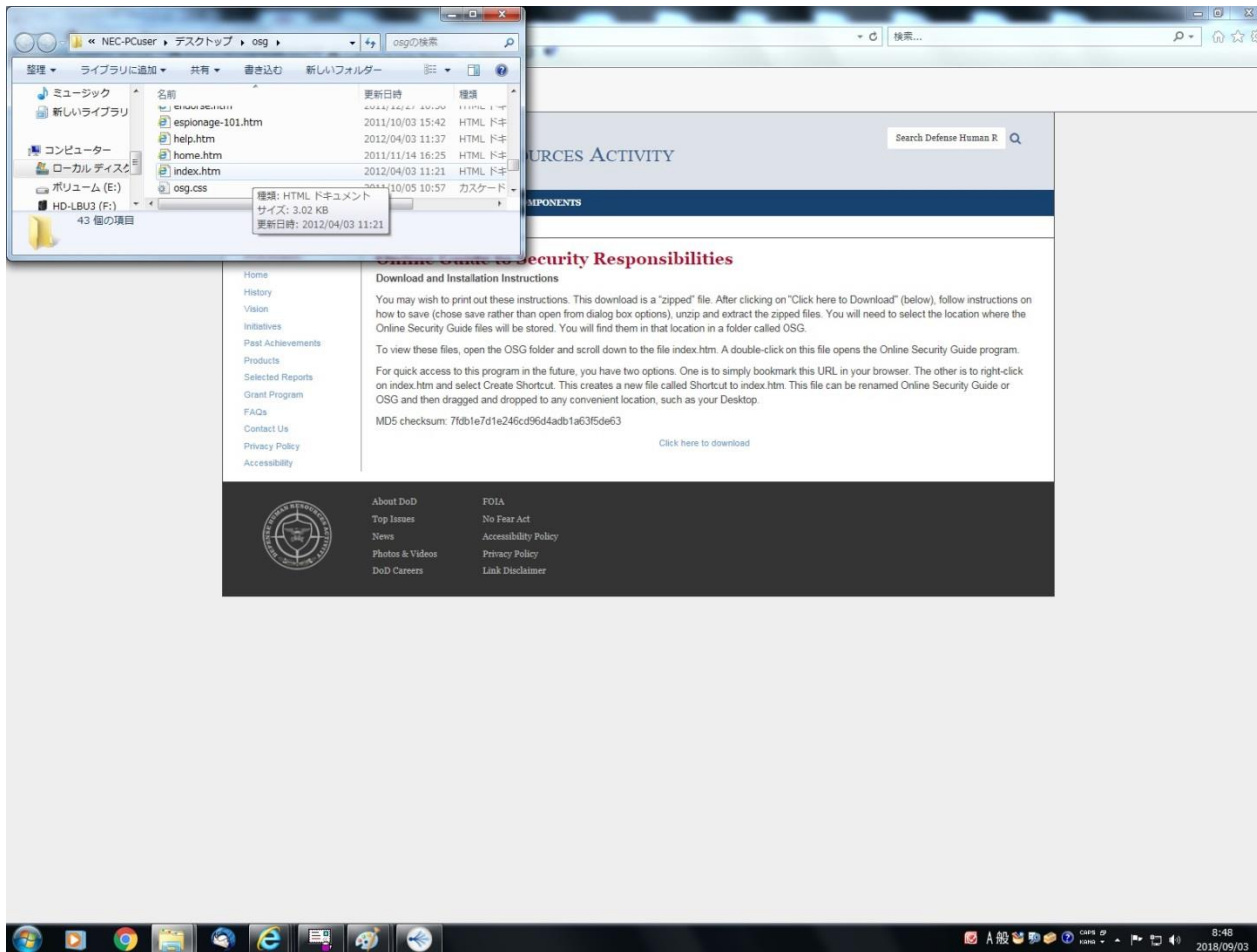
現在のセッション

はい(Y) いいえ(N) **すべてはい(E)** すべていいえ(O) キャンセル

About DoD  
Top Issues  
News  
Photos & Videos  
DoD Careers

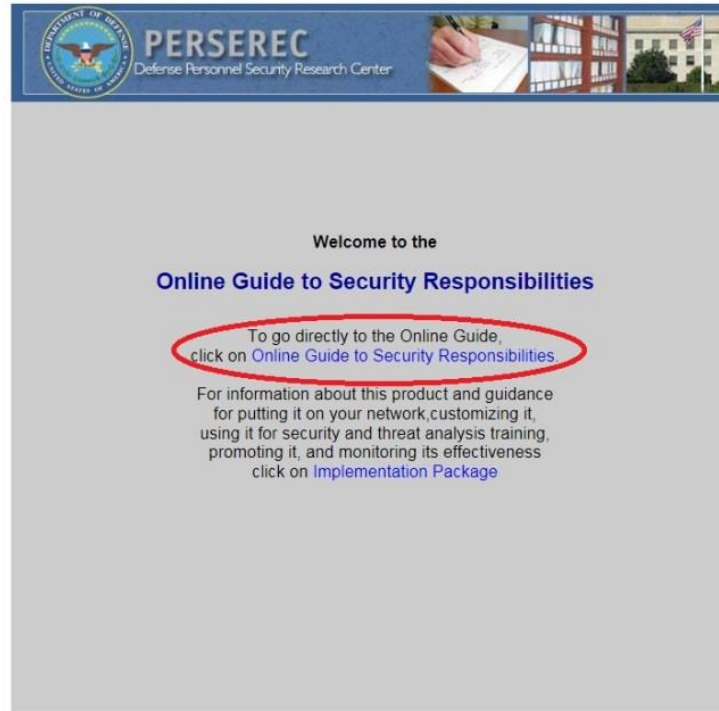
12:58  
2018/09/03

# Index. Himをクリック



# オンラインガイドのセキュリティ・・・をクリック

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)



The screenshot shows the top portion of a web browser window. At the top is a menu bar with the following items: 文件(F), 编辑(E), 显示(V), 收藏夹(A), 工具(T), and 帮助(H). Below the menu bar is a banner for the PERSEREC (Defense Personnel Security Research Center) website. The banner includes the Department of Defense seal on the left, the text 'PERSEREC Defense Personnel Security Research Center' in the center, and three small images on the right: a hand writing on a document, a bookshelf, and a building with an American flag. The main content area has a light gray background and contains the following text:

Welcome to the

**Online Guide to Security Responsibilities**

To go directly to the Online Guide,  
click on [Online Guide to Security Responsibilities](#).

For information about this product and guidance  
for putting it on your network, customizing it,  
using it for security and threat analysis training,  
promoting it, and monitoring its effectiveness  
click on [Implementation Package](#)

# 赤丸をクリック

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)



UNCLASSIFIED

## Online Guide to Security Responsibilities

[Click here for the Know-it-All's Security Quiz](#)



WOW! THERE'S LOTS OF GOOD STUFF HERE

ABOUT THIS GUIDE  
HELP FOR FIRST-TIME USERS  
BACK TO OPENING SCREEN

Procedures For Protecting Information

Personal Conduct and Reporting Requirements

Foreign Threats To Protected Information

Computer and Other Technical Vulnerabilities

Understanding and Helping With Personal Problems

Espionage 101

Terrorism 101

[Complete List of Contents](#)



8:51 2018/09/03



# 黒丸をクリック

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)



## Computer Vulnerabilities

### Overview

- Secure Use of Office Network
- Secure Use of Personal Computer
- Secure Use of Portable Devices
- User Authentication and Passwords
- Email Pitfalls
- Malware and Email Scams

### Social Networking & Peer-to-Peer

- Social Engineering
- Social Engineering Case 1
- Social Engineering Case 2
- Insider Threat to IT Security
- Reporting Computer Violations
- Protecting Laptop and Other Portable Devices
- Disposal of Digital Storage Devices**

### Overview

Computer networks make enormous amounts of data available in one convenient location where it is vulnerable to unauthorized disclosure, theft, modification, or destruction. The greater the concentration, the greater the potential consequences of any security breach.

Cyberspace has become a fifth domain of warfare comparable to land, sea, air, and space, and the frequency and magnitude of cyber attacks on the United States have increased exponentially during the past 10 years. Successful cyber penetration of our military and civilian infrastructure and weapons development programs is a grave risk to our national security. This is discussed in the [Cyber Espionage](#) section of the [Short Course in Counterintelligence](#) module.

Foreign militaries have developed offensive capabilities in cyberspace, and more than 100 foreign intelligence services are trying to break into U.S. networks to gain access to proprietary, sensitive, or classified information. Hackers now probe this system thousands of times and automatically scan for weaknesses millions of times every day. Attacks on our computer networks also come from nongovernmental organizations, business competitors and gangs, as well as insiders with malicious intentions.

The Department of Defense has created the U.S. Cyber Command to fight this battle, which is, largely, a battle of wits between computer specialists. However, everyone with access to a computer holding sensitive information plays a role in this battle. The common saying that "security is everyone's responsibility" is especially true with computer security. It is essential that you understand the vulnerabilities of this medium that is changing the world because YOU, unknowingly, can endanger your employer's entire computer network. Any network is only as secure as its weakest link.

This module starts with security rules and procedures for the three conditions under which you use computers -- Secure Use of Office Network, Secure Use of Personal Computer, and Secure Use of Portable Devices. A fundamental security element of all computer usage is the user Authentication and Passwords procedures that control who has access to your computer. This authentication process is evolving and becoming more complex to keep up with advances in digital technology.

For most of us, email is an important part of our office and our private lives. [Email Pitfalls](#) discusses the various ways this part of our life can cause problems. At the

file:///C:/Users/NEC-PCuser/Desktop/osg/v1/comput/disposal.htm



8:56  
2018/09/03



## Disposal of Digital Storage Devices

Individuals and organizations often want to replace their existing desktop computers, laptops, and smaller devices such as PDAs or Blackberries that also have digital memories. What to do with the old ones presents a problem, as the old system memories typically contain sensitive government or business information or sensitive personal information such as social security numbers, credit card numbers, account numbers, IDs, and passwords.

Whether you give away your excess or outdated digital equipment, sell it on eBay or just set it at the curb with the rest of your trash, you need to take appropriate precautions to ensure that sensitive data is destroyed or remains protected and not inadvertently passed on to unknown others. The following paragraphs discuss policies and best practices to assist organizations and individuals in properly removing the data on their digital devices prior to their disposal or reuse.

Massachusetts Institute of Technology (MIT) conducted a study to determine what kind of information can be recovered from used hard drives. They bought 158 used hard drives from eBay and other sources. The computers had originally belonged to a variety of businesses ranging from banks to law firms. They discovered that only 12 of the 158 hard drives had had their data destroyed in a way that kept the data from being recovered. From the other 146 drives, they recovered thousands of credit card numbers, social security numbers, medical records, emails, and other sensitive information. <sup>1</sup>

Many people are under the false impression that when they delete a file this information is removed from the hard drive, but this is not the case. Deleting all your files does not delete the files from the hard drive. It just removes the information the hard drive needs to find the files; it does nothing to the files themselves.

There is also a widespread belief that formatting a hard drive will completely remove all data. "This false understanding is derived from the somewhat misleading warning given before format operations: 'Warning: Formatting the disk will permanently remove all data.' However, formatting a disk does *not delete the actual data*. Only a small percentage of the data on the drive is actually overwritten.... Formatting complicates the recovery of fragmented files, but does not prevent it." <sup>2</sup>

Disposal of hand-held communications devices such as Personal Digital Assistants (PDAs), Blackberries, and various types of smart phones presents similar problems. A study of 160 discarded hand-held communications devices by the University of Glamorgan in Australia found that information had not been removed effectively from 43% of the Blackberries and 23% of the mobile smart phones. As a result, individuals were exposed to identity theft and organizations were exposed to loss of sensitive information to their competitors. <sup>3</sup>



**When you delete a file, most computer operating systems delete only the "pointer" which allows the computer to find the file on your hard drive. The file itself is not deleted until it is overwritten by another file. Just deleting a file is comparable to deleting a chapter heading from the table of contents of a book, but not removing the pages on which the chapter is written. Some networks may be configured to "wipe" or purge the hard drive when information is deleted, but most are not.**

### Regulations

Sanitization is the process of removing data from storage media so that it may not be easily retrieved or reconstructed. The types of media that need to be sanitized before they are reused, sold, or disposed of include compact disc drives, RAM, ROM,

# Physical Destruction(物理的な破壊)

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)



There are three basic approaches to sanitization to ensure the data is not recoverable. These are described briefly below. Each method has its own particular advantages and disadvantages, so the choice of method depends upon the particular circumstances, especially the level of classification or sensitivity and the type of media on which the data is stored. 4

## Overwriting

This is a process whereby a software program writes a combination of 0s and 1s over all the data on the hard drive. This process, which requires a special software program, covers previous data with multiple layers of magnetic flux, making the data unreadable. The more frequently the data is overwritten, the greater the security. Three to seven repetitions are normal. This process is also known as "wiping" the hard drive or "wiping out" the data. The overwriting must be done by a trained person who certifies that the process has been successfully completed.

An advantage of this process is that the hard disk is not destroyed, so the drive can then be reused. The computer can be given to a different person or office, sold, or donated to charity. Overwriting may also be less expensive than physical destruction or degaussing when used to sanitize just a few drives. On the other hand, the overwriting takes considerable time when done well (i.e., many overwrites), so it may not be cost-effective when sanitizing a large number of drives.

## Degaussing

Degaussing is the process of removing or neutralizing a magnetic field. It requires special equipment designed and approved for the type of media being sanitized. Equipment of the type required for degaussing a hard disk is expensive, so this process is used more often with smaller magnetic media such as floppy disks and backup tapes. Degaussing may do a more thorough job of sanitization than overwriting, but the drive is no longer usable after this process. The process requires approved equipment operated by a trained individual who certifies successful completion.

## Physical Destruction

The safest and surest way to sanitize a hard drive is to physically destroy it. This is an attractive option if the drive is to be discarded anyway and not reused. One common method is shred or drill four holes through the entire drive. Another approach is to pry the platters apart to the extent that each platter is sufficiently warped or distorted to make it inoperable. It can also be taken to a professional for destruction. Some consumer electronics stores will do this as a courtesy for individual customers worried about what will happen to their old hard drive.

Physical destruction is also a good, and certainly easier, alternative for sanitizing smaller digital memory devices that contain sensitive or personal information such as thumb or flash drives, PDAs, and iPods.

## References

1. "Drive Disposal Best Practices: Guidelines for Removing Sensitive Data Prior to Drive Disposal," Seagate Technology LLC, Publication Number TP582-1-0710US, October 2007. Accessed June 2010 at [www.seagate.com/docs/pdf/whitepaper/Disposal\\_TP582-1-0710US.pdf](http://www.seagate.com/docs/pdf/whitepaper/Disposal_TP582-1-0710US.pdf)
2. *Ibid.*
3. "One in Five Second Hand Mobiles Contain Sensitive Data," University of Glamorgan News Centre, accessed July 2010 at <http://news.glam.ac.uk/news/en/2008/sep/26/one-five-second-hand-mobiles-contain-sensitive-dat/>
4. "Drive Disposal Best Practices," *op. cit.*

HOME | COMPUTER VULNERABILITIES CONTENTS | TOP OF PAGE | HELP  
INFORMATION | CONDUCT | THREATS | TECH VULNERABILITY | ASSISTANCE  
ESPIONAGE 101 | TERRORISM 101



# データ消去3つの手法

- Overwriting
  - This is a process whereby a software program writes a combination of 0s and 1s over all the data on the hard drive. This process, which requires a special software program, covers previous data with multiple layers of magnetic flux, making the data unreadable. The more frequently the data is overwritten, the greater the security. Three to seven repetitions are normal. This process is also known as "wiping" the hard drive or "wiping out" the data. The overwriting must be done by a trained person who certifies that the process has been successfully completed.
  - An advantage of this process is that the hard disk is not destroyed, so the drive can then be reused. The computer can be given to a different person or office, sold, or donated to charity. Overwriting may also be less expensive than physical destruction or degaussing when used to sanitize just a few drives. On the other hand, the overwriting takes considerable time when done well (i.e., many overwrites), so it may not be cost-effective when sanitizing a large number of drives.
  -
- Degaussing
  - Degaussing is the process of removing or neutralizing a magnetic field. It requires special equipment designed and approved for the type of media being sanitized. Equipment of the type required for degaussing a hard disk is expensive, so this process is used more often with smaller magnetic media such as floppy disks and backup tapes. Degaussing may do a more thorough job of sanitization than overwriting, but the drive is no longer usable after this process. The process requires approved equipment operated by a trained individual who certifies successful completion.
- Physical Destruction
  - The safest and surest way to sanitize a hard drive is to physically destroy it. This is an attractive option if the drive is to be discarded anyway and not reused. One common method is shred or drill four holes through the entire drive. Another approach is to pry the platters apart to the extent that each platter is sufficiently warped or distorted to make it inoperable. It can also be taken to a professional for destruction. Some consumer electronics stores will do this as a courtesy for individual customers worried about what will happen to their old hard drive.
  - Physical destruction is also a good, and certainly easier, alternative for sanitizing smaller digital memory devices that contain sensitive or personal information such as thumb or flash drives, PDAs, and iPods.

# グーグル翻訳

- 上書き

- これは、ソフトウェアプログラムがハードドライブ上のすべてのデータに0と1の組み合わせを書き込むプロセスです。特別なソフトウェアプログラムを必要とするこのプロセスは、磁束の複数の層を有する以前のデータをカバーし、データを判読不能にする。データが頻繁に上書きされるほど、セキュリティが強化されます。3〜7回の繰り返しが正常です。このプロセスは、ハードドライブの「ワイピング」またはデータの「拭き取り」としても知られています。上書きは、プロセスが正常に完了したことを証明する訓練を受けた人が行う必要があります。
- このプロセスの利点は、ハードディスクが破壊されないため、ドライブを再利用できることです。コンピュータは、別の人や事務所に売ったり、慈善団体に寄付したりすることができます。上書きは、ほんの数台のドライブをサニタイズするのに使用すると、物理的な破壊や消磁よりも安価です。他方、上書きは、うまくいったとき(すなわち、多くの上書き)、かなりの時間を要するので、多数のドライブを消毒するときには費用効果がないかもしれない。

- 消磁

- 消磁は磁場を除去または中和するプロセスである。消毒されるメディアの種類に合わせて設計され承認された特別な装置が必要です。ハードディスクの消磁に必要なタイプの機器は高価であるため、このプロセスは、フロッピーディスクやバックアップテープなどのより小型の磁気媒体でより頻繁に使用されます。消磁は上書きよりも徹底した衛生処理を行うかもしれませんが、このプロセスの後でドライブはもはや使用できません。このプロセスでは、成功裡の修了を証明した訓練を受けた個人によって運営された認可済みの装置が必要です

- 物理的破壊

- ハードドライブを安全にする最も安全で確実な方法は、物理的にハードドライブを壊すことです。これは、ドライブをとにかくに破棄し、再使用しない場合には魅力的なオプションです。1つの一般的な方法は、細断処理またはドライブ全体に4つの穴を開けることです。別のアプローチは、各プラッタが十分に反り、または歪んで、動作不能になる程度にプラッタを引き離すことである。それはまた、破壊のための専門家に連れて行くことができます。いくつかのコンシューマエレクトロニクス店は、古いハードドライブに何が起こるか心配している個々の顧客の礼儀としてこれを行うでしょう。
- 親指やフラッシュドライブ、PDA、iPodなどの機密情報や個人情報を含む、より小型のデジタルメモリデバイスを消毒するには、物理的な破壊も良い方法です。