

論理設計学

イントロダクション

佐藤証 西9-613

akashi.satoh@uec.ac.jp

<http://satoh.cs.uec.ac.jp/ja/lecture/CircuitDesign/index.html>

講義資料

電気通信大学 情報理工学研究科 佐藤研究室



The University of
Electro-Communications
SATOH Lab

佐藤研究室 > 講義 > 計算機アーキテクチャ基礎論

ホーム

メンバー

設備

研究

講義

文献

リンク

サイトマップ

▶ 計算機アーキテクチャ基礎論

- ▶ 1. コンピュータアーキテクチャ <演習>
- ▶ 2. ノイマン型コンピュータ <演習>
- ▶ 3. 命令セットアーキテクチャ <演習>
- ▶ 4. ハーバードアーキテクチャ <演習>
- ▶ 5. 論理設計学 <演習>
- ▶ 6. 計算機アーキテクチャ基礎論 <演習>
- ▶ 7. テクチャ <演習>
- ▶ 8. 大学院技術英語 <演習>
- ▶ 9. 割込みアーキテクチャ <演習>
- ▶ 10. パイプラインアーキテクチャ <演習>

<http://satoh.cs.uec.ac.jp/ja/lecture/CircuitDesign/index.html>

パスワード : TOMATO

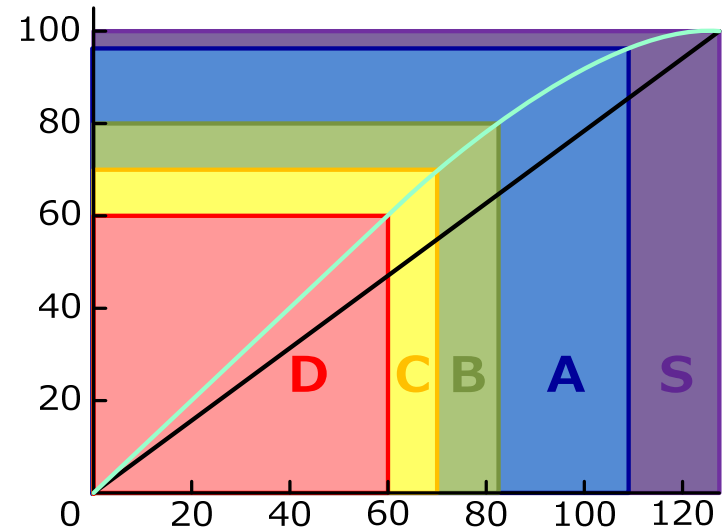
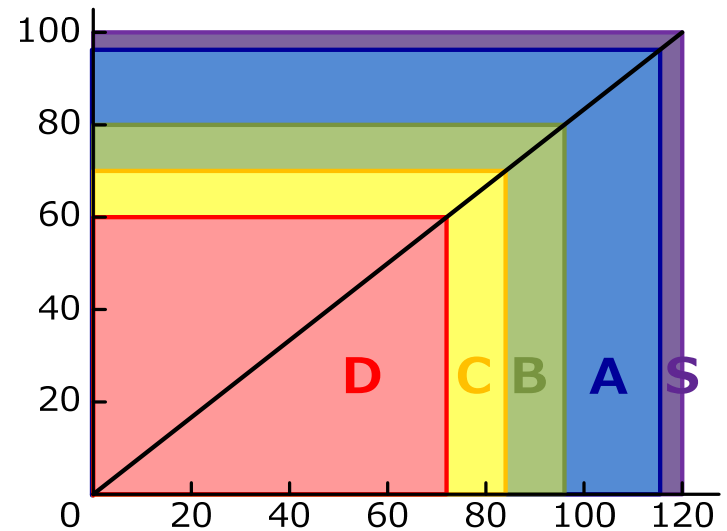
教科書



- 岩本洋監修、堀桂太郎著
- オーム社
- ISBN4-274-50600-2
- 本体2,484円

成績

- 毎回、授業の最初10分間に復習の小テストを行います
 - 教科書・ノート参照不可
 - 5点×12回=60点
- 期末試験
 - ノート参照可
 - 教科書・プリント持ち込み不可
 - 配点60点



講義スケジュール

●第 1回	『アナログとディジタル』	5/11
●第 2回	『2進数と基底変換』	5/18
●第 3回	『論理演算とベン図』	5/25
●第 4回	『カルノー図とゲート回路』	6/1
●第 5回	『組合せ回路』	6/8
●第 6回	『順序回路』	6/15
●第 7回	『前半の復習 (Part.1)』	6/22
●第 8回	『前半の復習 (Part.2)』	6/29
●第9,10回	『シフトレジスタ, カウンタ』	7/6
●第11回	『様々な組合せ回路』	7/13
●第12回	『演算回路』	7/20
●第13回	『簡易電卓を作る』	7/27
●第14回	『後半の復習』	8/3
●第15回	『デジタル回路の研究』	8/10

論理設計学

1. アナログとデジタル



アナログとデジタル

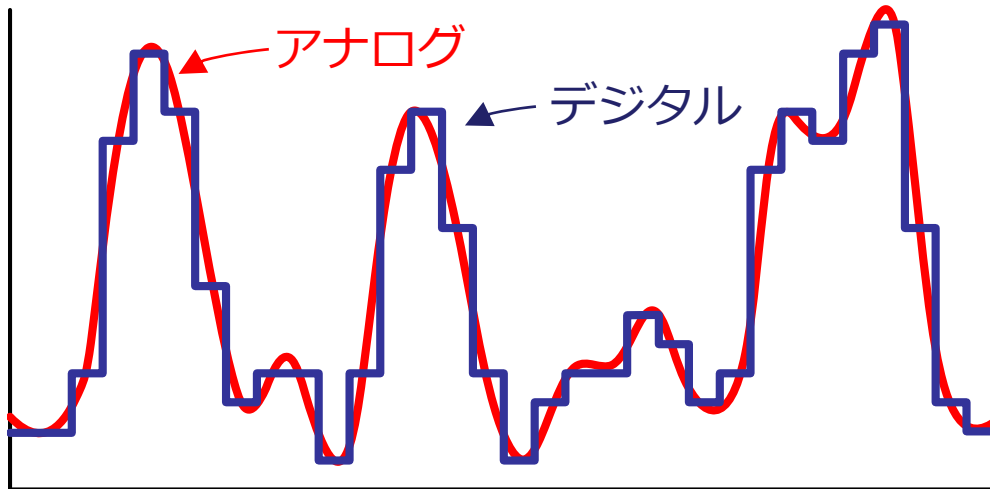
- アナログ (analogue)
 - 連続して変化する量の表現方法
 - 英語のanalogous (類似) に由来する
- デジタル (digital)
 - 有限の桁による離散的な表現方法
 - 英語のdigit (数字, 桁, 指) に由来する



ROLEX GMT Master II



G-Shock GWF-1000TM



アナログ時計の秒針はアナログ？デジタル？

デジタルの利点

- ノイズに強い・誤り検出・訂正が可能
- コピーによる劣化がない
- データの多彩な後処理が可能
- デバイス技術の進歩による機器の小型化
- データメディアの高密度化・大容量化
- 高速通信，マルチメディア化



レコード



黒電話



ビデオテープ



アナログ放送



CD



スマートフォン



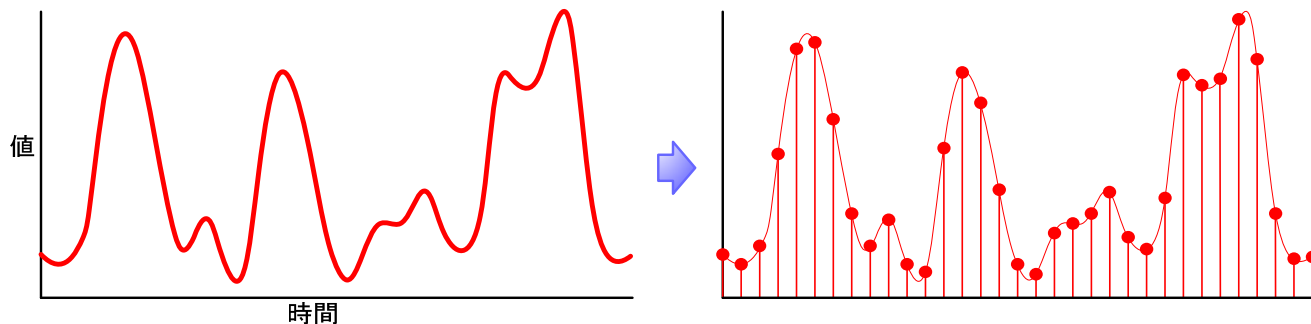
HDDレコーダ



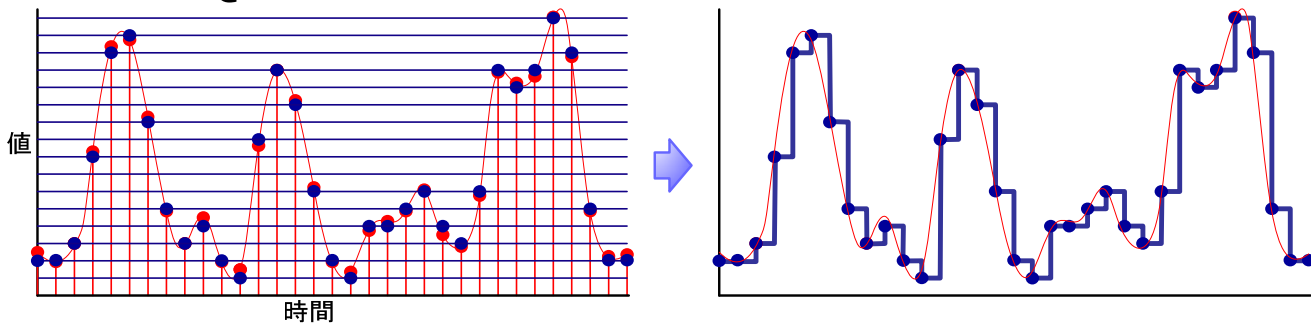
デジタル放送

サンプリングと量子化

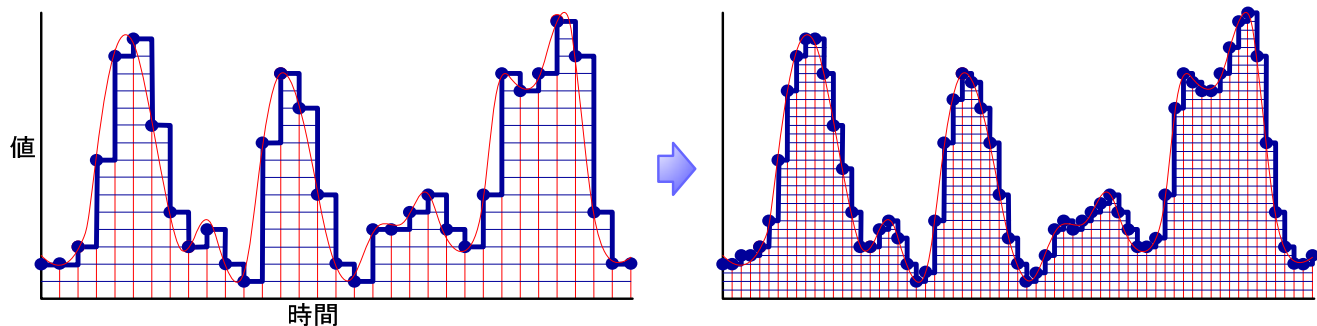
● サンプリング (Sampling)



● 量子化 (Quantize)



サンプリングと量子化を細かくするほど元波形に近づく



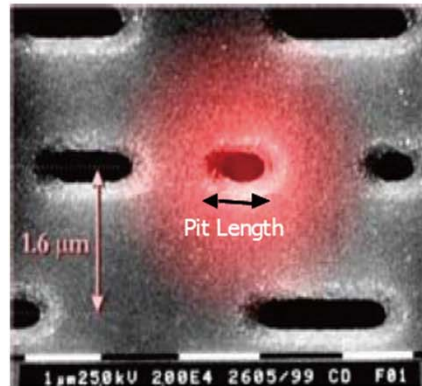
サンプリングと量子化

COMPACT
disc
DIGITAL AUDIO

DVD
AUDIO

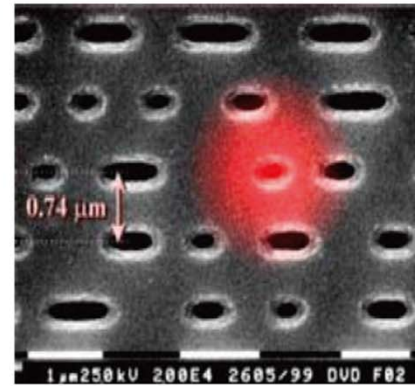
Blu-ray Disc

CD 0.7GB



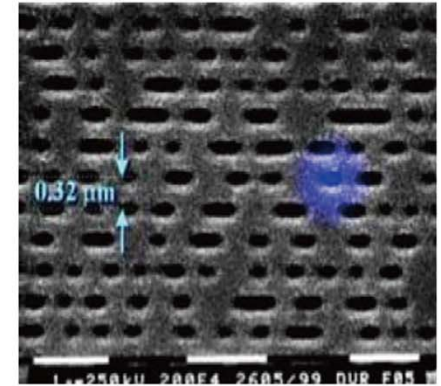
トラックピッチ : 1,6 μm
最短マーク長 : 0,8 μm

DVD 4.7GB



トラックピッチ : 0,74 μm
最短マーク長 : 0,4 μm

Blu-ray Disc 25GB



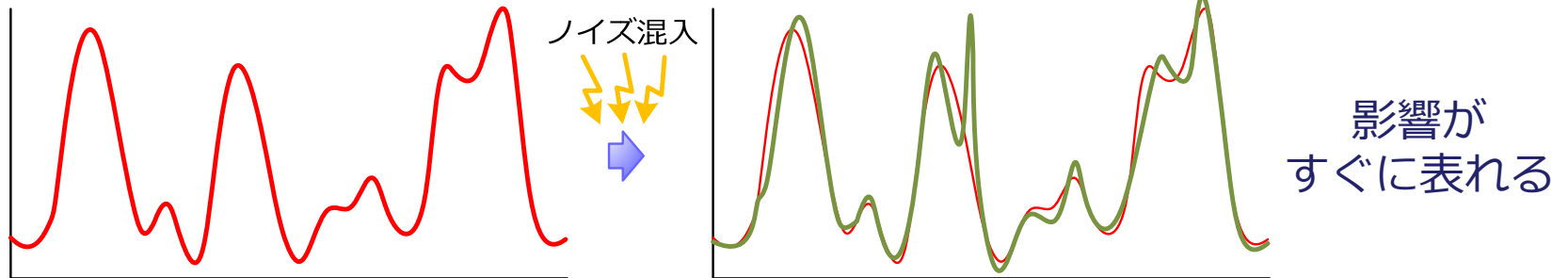
トラックピッチ : 0,32 μm
最短マーク長 : 0,15 μm

http://www.ieice-hbkb.org/files/08/08gun_02hen_03.pdf

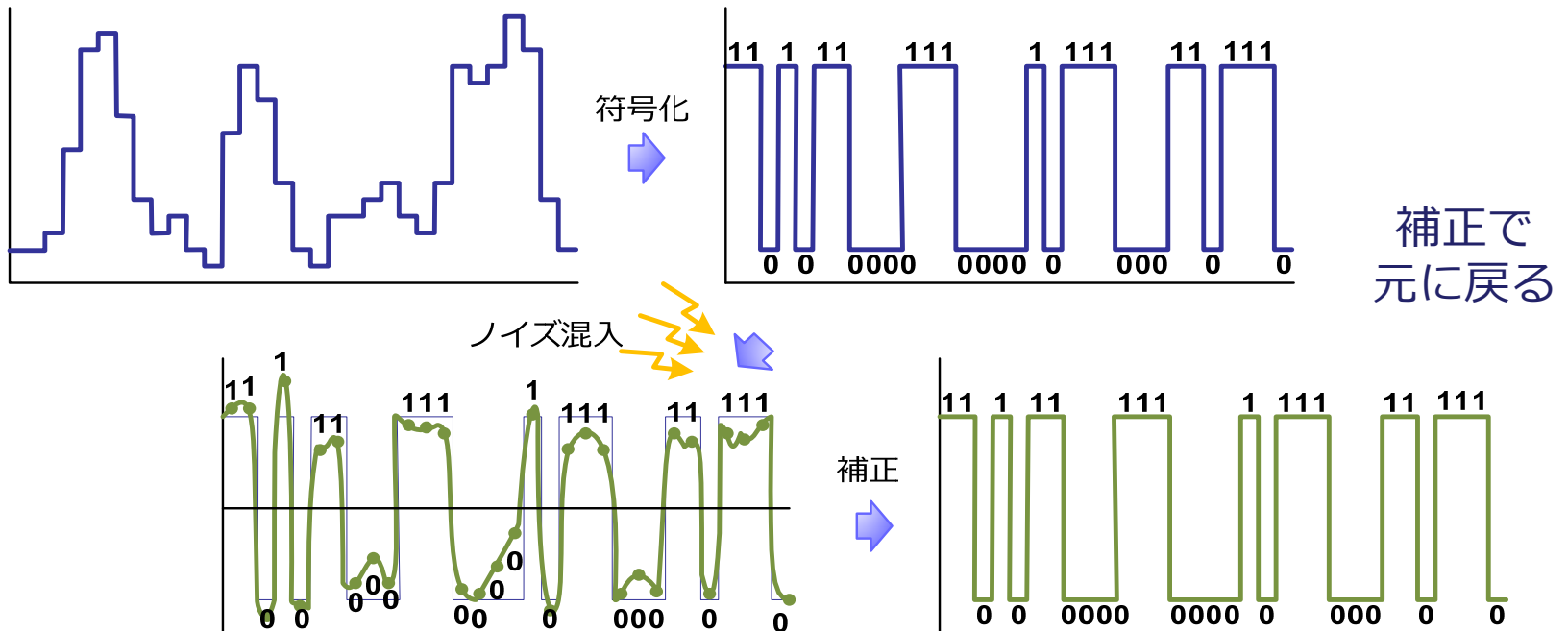
	CD	DVD-Audio	BD-Video
サンプリング周波数	44.1 kHz	192 kHz (最大)	192 kHz (最大)
量子化ビット数	16 bit	24 bit (最大)	24 bit (最大)
チャンネル数	2 ch	2 ch	5.1 ch
ビットレート(LPCM)	1.4 Mbps	9.6 Mbps (最大)	27.4 Mbps (最大)
ディスク容量	650MB/720MB	4.7GB(一層)	25GB(一層)
レーザー	780nm 赤外線	650nm 赤	405nm 青

ノイズ混入 & ひずみの影響

● アナログ信号

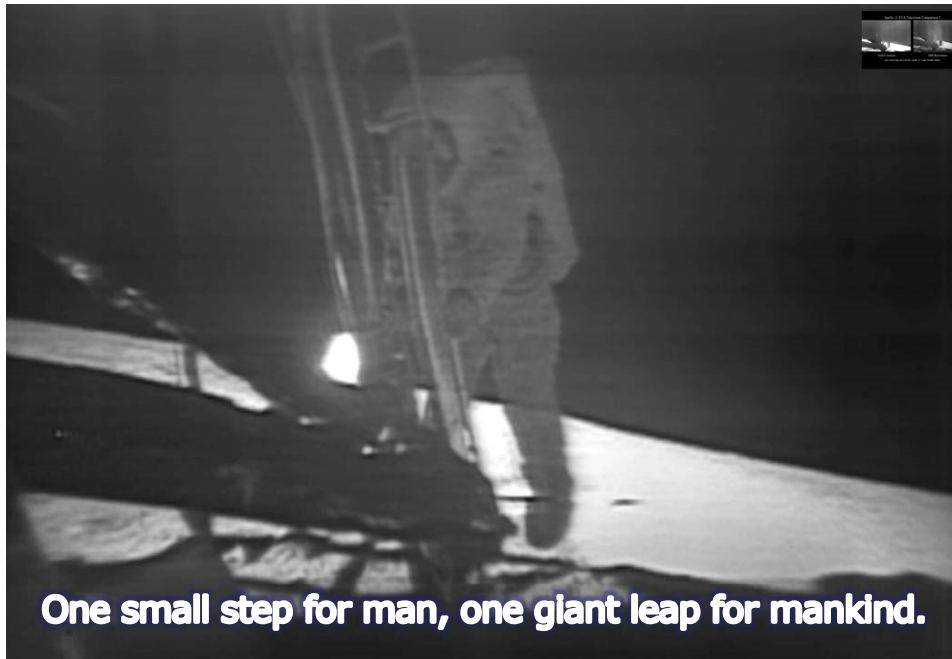


● デジタル信号



デジタル通信の先駆け

- PCM（パルス符号変調）によるデジタル通信はアポロ宇宙船からの中継や長距離電話等で1960年代に実用化された



1969年7月20日、アポロ11号のニール・アームストロング船長は人類初の月面着陸に成功した

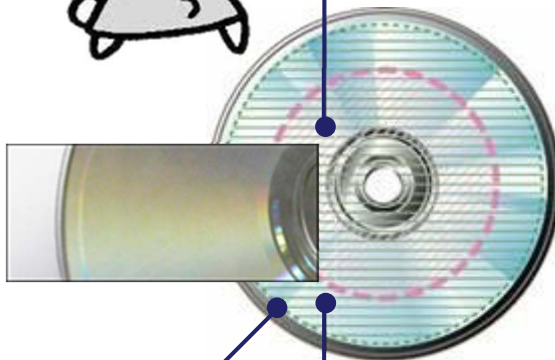
デジタルの欠点

- アナログはエラーが増えても品質が劣化するだけで再生可能だが、デジタルは一定以上のエラーが起こると復号がまったくできなくなる
 - CD/DVD/BDでは容量の約13%が誤り訂正用のパリティデータ
 - コピー防止音楽CDはPCで読めないようにわざとエラーを混入しているが、CDプレーヤーは前後のデータからアナログ補正して再生する



追記ディスクの
寿命は10年程度

エラーだらけのPCMデータ



ライセンスID
PC用プレーヤー+データ

レーベルゲートCD
BS-129



COPY CONTROL CD



このCDの音源をパソコンで再生するには、インターネット接続が必要です。

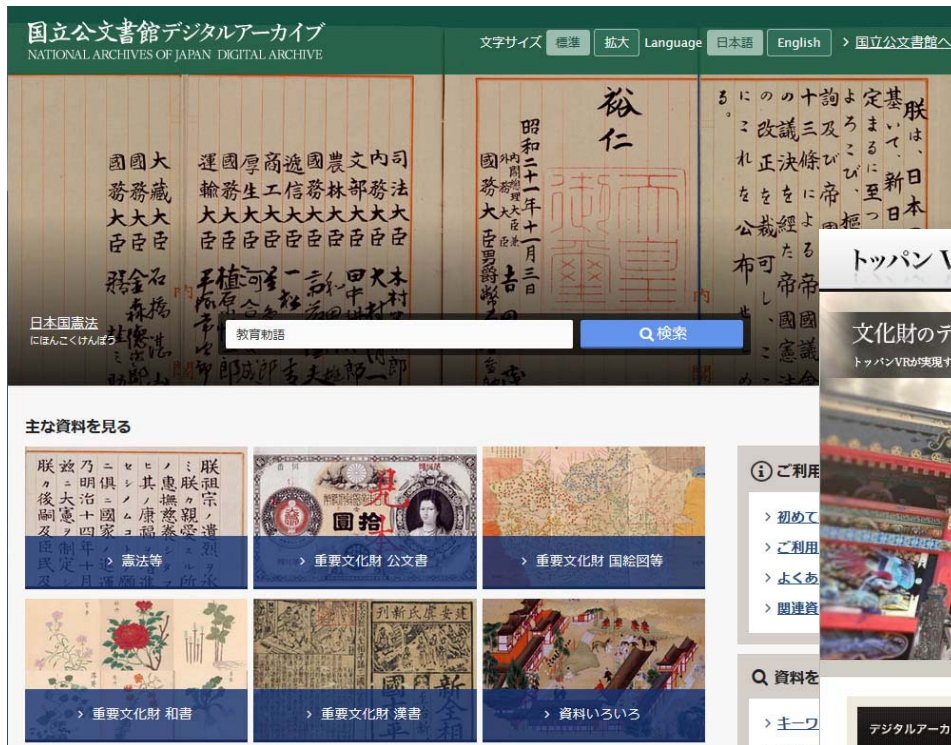


ロゼッタストーン (前196年)

プトレマイオス5世の頌徳碑の一部

デジタルアーカイブ

- 博物館・美術館・公文書館や図書館の収蔵品を始め有形・無形の文化資源（文化資材・文化的財）等をデジタル化して記録保存を行うこと.デジタル化することによって,文化資源等の公開やネットワーク等を通じた利用も容易となる. (wikipedia)



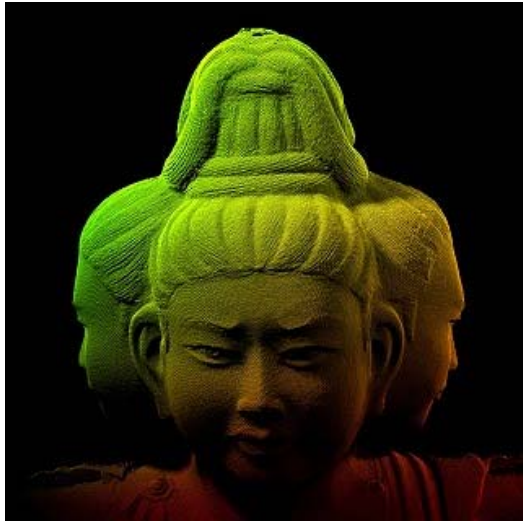
<https://www.digital.archives.go.jp/>



<http://www.toppan-vr.jp/bunka/>

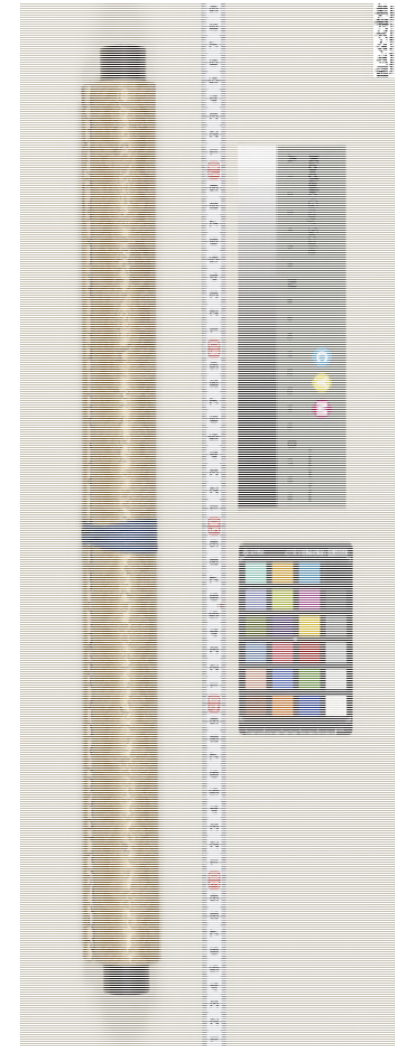
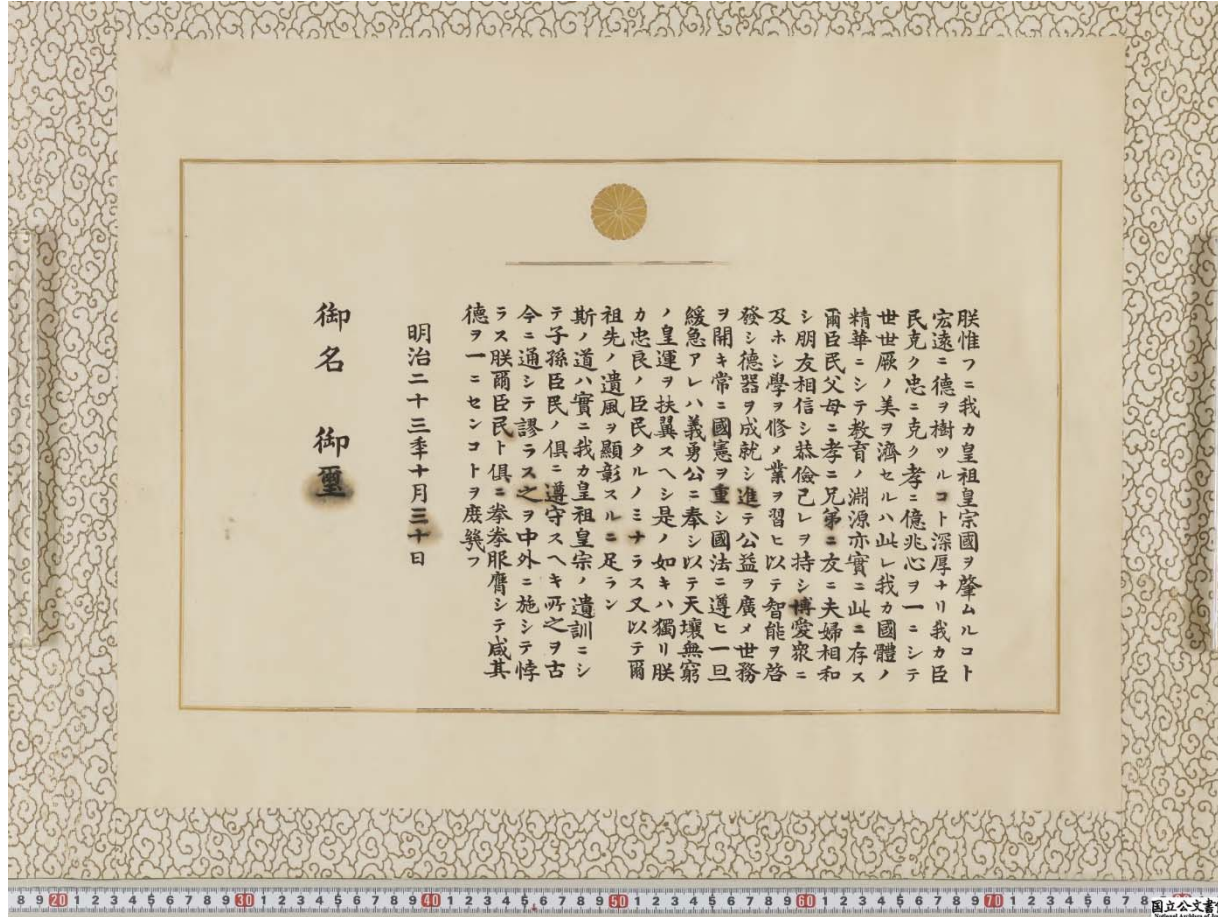
デジタルアーカイブ

- 文化財だけでなく世界遺産も



デジタルアーカイブ

- 文化財や記録メディア等の物は劣化してもデジタルデータは劣化しない



話題になったこんなものも・・・

デジタルデータの真正性

- 暗号技術でデジタルデータの改ざん・コピーが可能
- 印鑑・手書きの紙物の真正性は確認が難しい

別紙様式-2

日額旅費申請書兼報告書(学生用)	
旅行命令者 殿	申請日 平成 年 月 日
申請者 所属・職名 氏名・印	
本学学生に対し以下のとおり出張依頼しましたので、申請します。	
旅行者氏名	
専攻・学籍 No.	
用 務	☐ 調査研究補助 ☐ 資料収集補助 ☐ 研究成果発表補助 ☐ その他 上記の具体的な内容
用務先及び住所	
旅行 日	平成 年 月 日 ()
利用交通経路	
金	
【用務先が複数の場合 (通勤手当の支給を受け ている場合は、同手 当の支給対象交通機関 の運賃を除いた額)の のみ記入】	計 円
支 給 額	円 (財務課経理係で記入します。)
経 費 区 分	予算詳細コード () 名称 ()
研究 題 目 等	※材料費・共同研究費・委託研究費・受託事業費の研究課題を記載すること
出張報告詳細	
備 考	

本旅行についての資料(写)を添付してください。(学会の開催通知等)
出張報告詳細を、旅行終了後1週間以内に記載し学科長・主任等を経て発令部署に提出してください。
宿泊をする場合は、出張申請書兼旅行命令書(第1号様式)により出張申請をしてください。
上記のとおり旅行したことを確認しました。

旅行命令者	決 裁 欄	発令時間管理員	発令時間管理員補助者
発令番号			
平成 年 月 日			
財務責任者殿 請求者氏名・印	上記の申請に基づき、旅費を請求します。		印

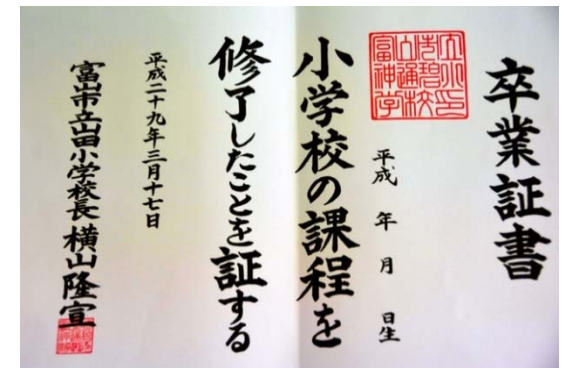
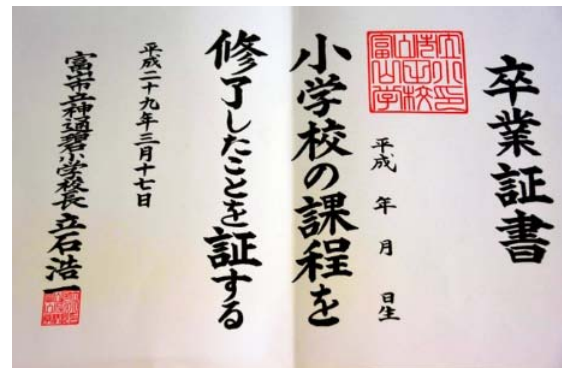


旅費払込請求書兼受領証

取 扱 票	
通知番号 00950-1-204851	口座番号 00950-1-204851
払込金額 1,000,000円	口座徴収料金 340円
取扱年月日 平成27年 9月 7日	取扱店 淀川新北野
大阪 貯金事務セン 一連番号 9424 000010000	

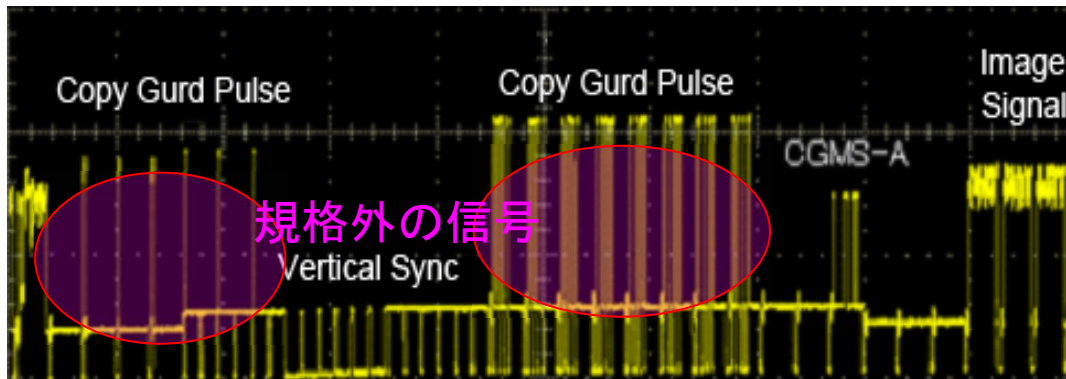
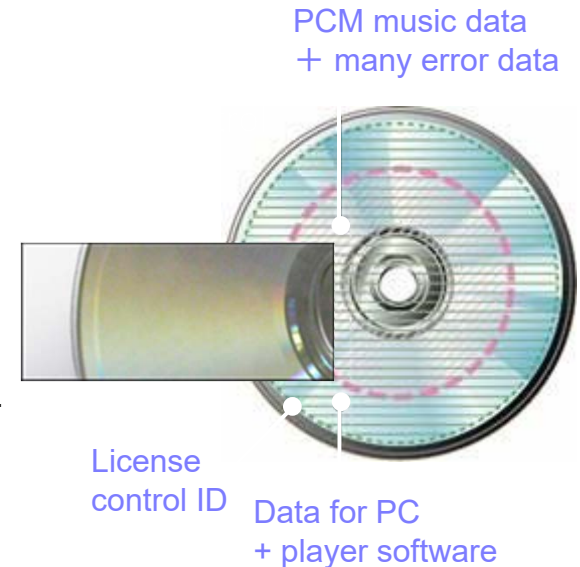
学校法人 森友学園
204851
0000000
107071-6-25
20412

すが、2口以上のご寄附をお願い致します。
文部省三郷小学校の寄附者録帳にお名前を



アナログコンテンツ保護技術

- 米国では海賊版によるビデオ・DVDの被害が年間数十万ドルあると言われる
- アナログコピー防止技術
 - マクロビジョン: 規格外の信号を映像信号に混ぜることで、録画機にエラーを発生させる
 - CGMS (Copy Generation Management System): 再生機コピー禁止信号を出力し受側が録画を中止
 - Copy Control CD: 多くのエラー信号を挿入することでCD-Rレコーダにエラーを発生させる
- コンテンツ事態は暗号化されていない



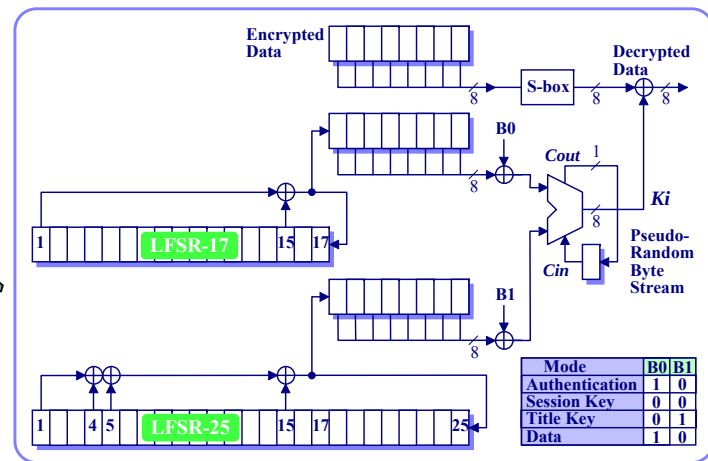
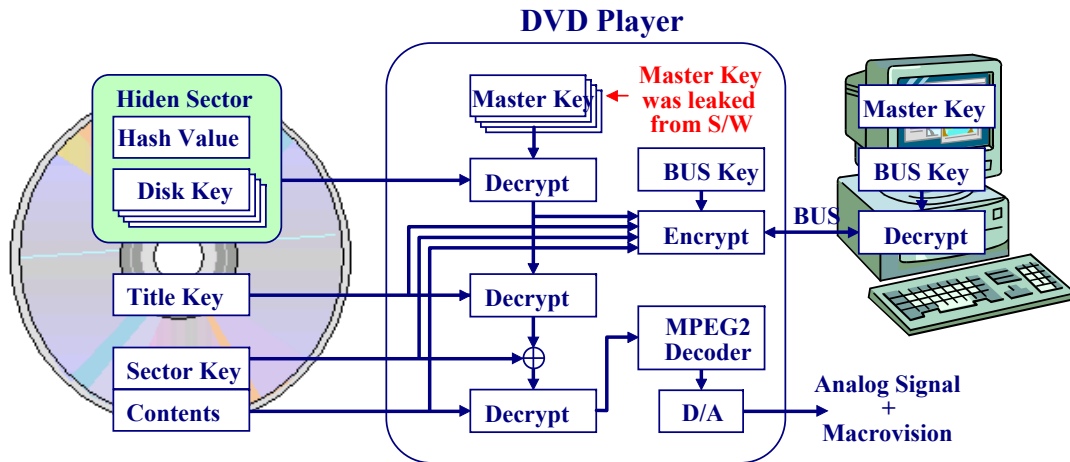
規格外の信号を修正することで簡単にコピーが可能



録画機がCGMS信号を検知して動作を停止した状態

デジタルコンテンツ保護技術

- CSS (Content Scrambling System)はDVD-video専用に開発されたコピー防止技術
- コンテンツデータはマスタ/ディスク/タイトル/セクタ鍵という階層構造を持つ鍵管理システムによって暗号化される
 - CSSはDVD再生ソフトの不備によってマスタ鍵が露呈し完全に破られてしまった
- 非常に脆弱な暗号アルゴリズムを使用している
 - コストの制限から、コンテンツデータはLFSRを用いた簡単な擬似乱数生成器の出力とXORされるだけであった
 - 武器輸出規制の問題から鍵長はわずか40ビット



DeCSS

- 1999年に15歳の少年がDVDコピーソフトDeCSSを開発し世界中に広まる
- 2000年8月にNY州連邦地裁がハッカー向け雑誌『2600』のWebでのDeCSS掲載を禁止
- 2004年2月にカリフォルニア州控訴裁判所が上記判決を憲法違反として撤回
- 現在はDVDライター等に備わっている



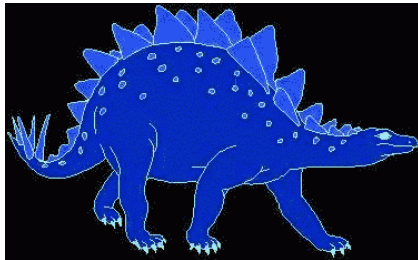
Tシャツ\$15
タイ\$34



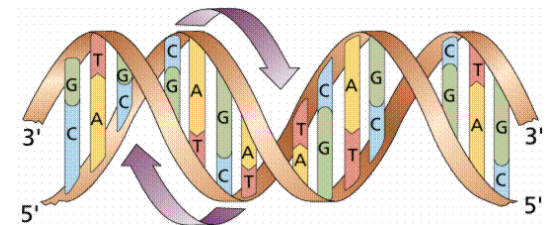
DeCSS Haiku



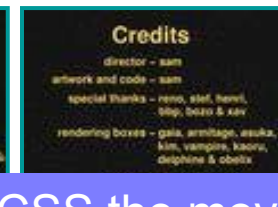
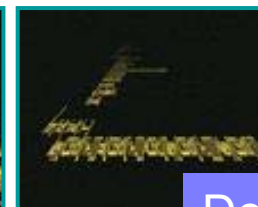
DeCSS マインスーパー



Steganography



DeCSS DNA



DeCSS the movie

進化するコンテンツ保護技術

- 米国では海賊版によるビデオ・DVDの被害は年間数十万ドルと言われる
- コンテンツ保護技術は半導体製造技術の進歩とブロードバンドネットワークの拡大に伴って進化し続けている
 - アナログ式→コピー回数制限→LFSR式→64ビットブロック暗号C2→AES
 - ビデオテープ→DVD→メモ리카ード/HDD→ネットワーク対応

