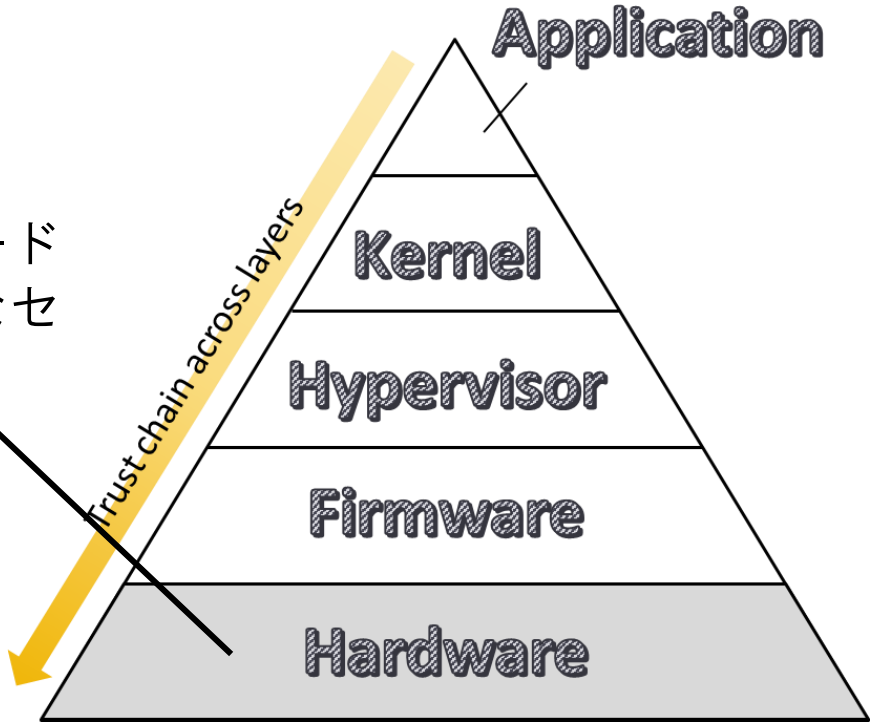
ハードウェアからの情報漏えいリスクとその対処法

奈良先端科学技術大学院大学
情報セキュリティ工学研究室
林　優一

情報機器に求められるハードウェアセキュリティ

情報システムにおいて各々のレイヤーでは
下位のレイヤを信頼しシステムが動作している

情報システムの根底の部分にあるハードウェアに脆弱性があった場合、重大なセキュリティ低下を招く恐れがある

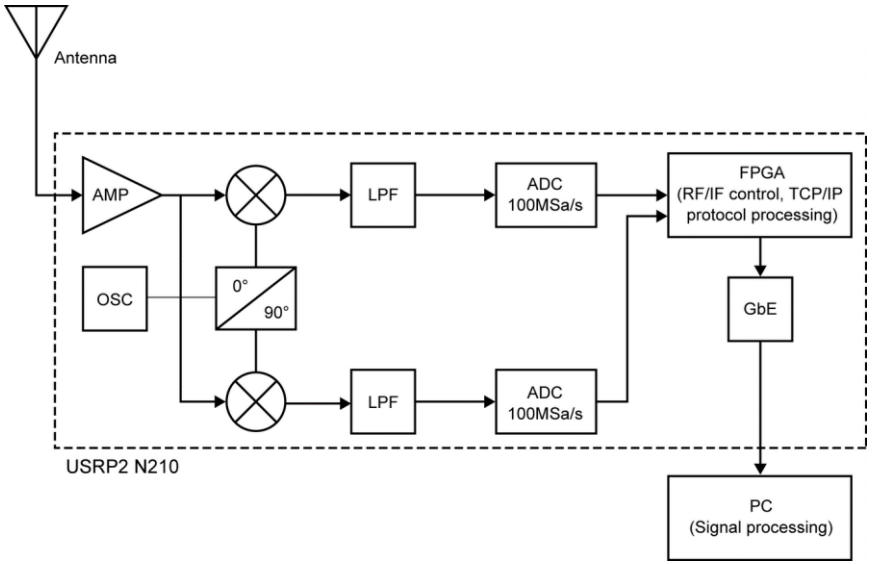


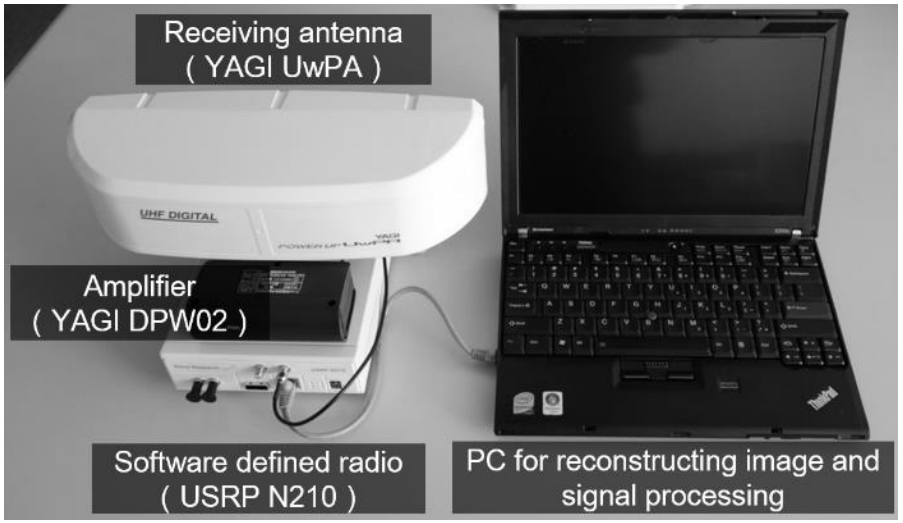
ハードウェアセキュリティの確保は情報セキュリティの中でも重要な課題の1つである。

情報システムに求められるハードウェアセキュリティ

公共空間におけるタブレット・スマホからの電磁波を通じた情報漏えい例（ハードウェアセキュリティ）

電磁波を通じた情報取得のためのセットアップ

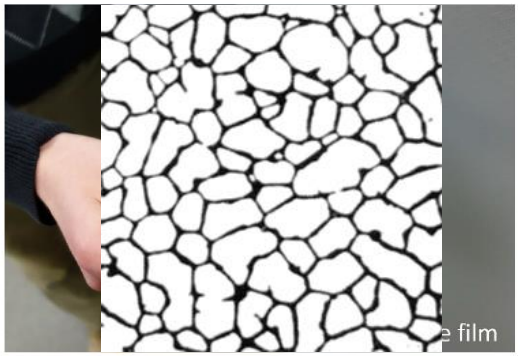


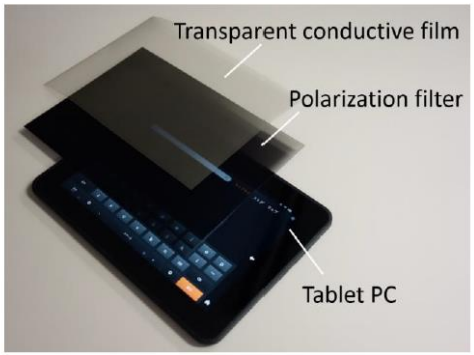


電磁シールドを用いた盗視対策

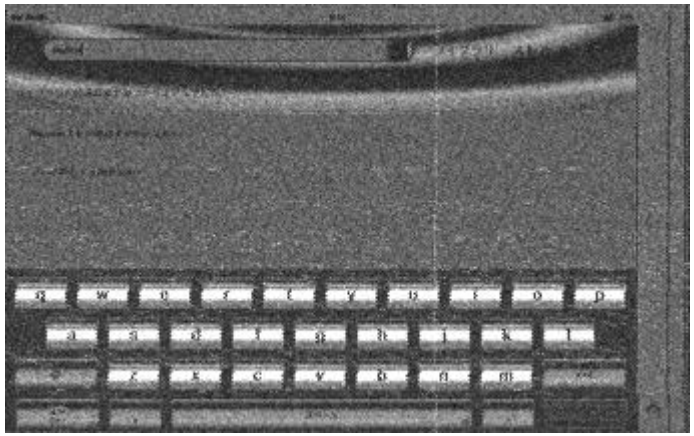
本検討ではデバイスの製造後に適用可能な電磁波シールドベースの対策を採用

シールドにはランダムなメッシュ構造有する透明導電膜を使用

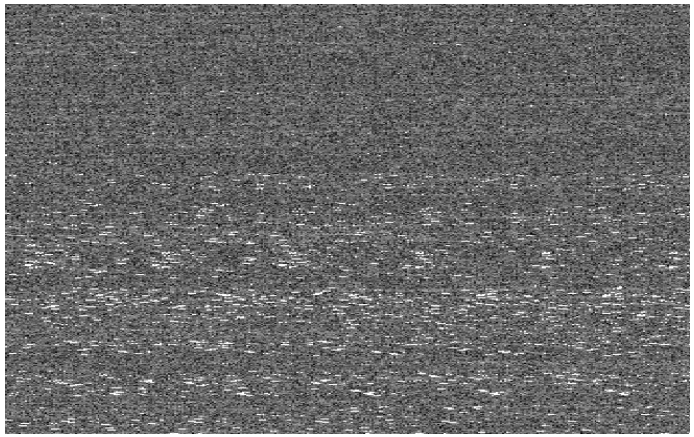




タッチスクリーンへのデータの入力を可能にするために、一定の厚さの偏光フィルタをモニタとシールドの間に挿入



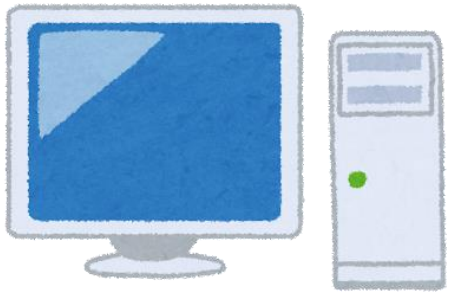
対策前（アンテナ-タブレット:50 cm）



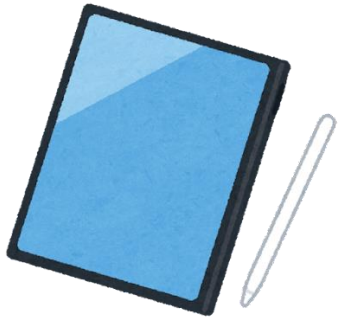
対策後（アンテナ-タブレット:50 cm）

脅威の対象となるデバイス

LAPTOP



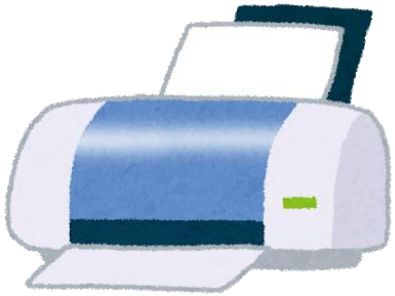
DESKTOP



TABLET

SMARTPHONE

KEYBOARD



PRINTER

SMART SPEAKER

HEADSET

SPEAKERPHONE

ここから本日の話

神奈川県HDD転売・情報流出事件の概要

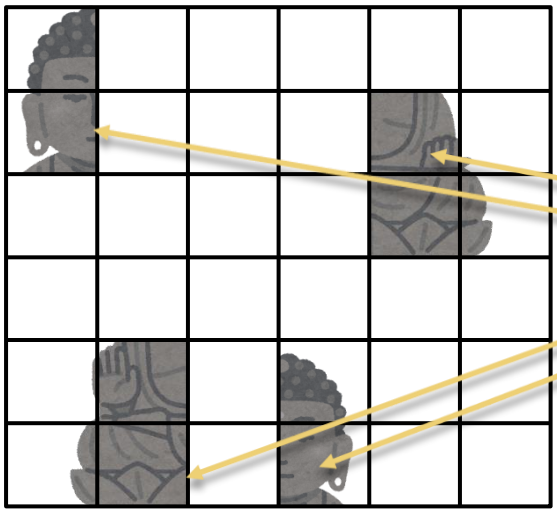
神奈川県庁で個人情報や機密情報を含む行政文書の保存に使われていた3TBのHDD（ハードディスクドライブ）18個がインターネットオークションサイトで転売され、情報が流出

富士通リースが2019年春に神奈川県にリースしているサーバからこのHDDを取り外し、契約に基づいたHDDの処分を処理会社のブロードリンクに外部委託

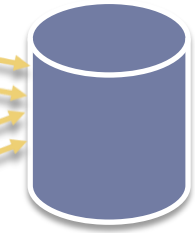
同社の担当者がHDDの一部を持ち出してオークションサイトで転売し、このうち9個を購入したIT企業経営の男性がHDDの中身をデータ復元ソフトで確認したところ、神奈川県の公文書と思われるデータを発見して新聞社に情報提供したことから、新聞社が県に確認して流出が判明

・個人情報や機密情報を含む行政文書の保存時に平文での保存が行われていた。
・リースが終了したHDDの破棄プロセスの確認が不十分であった。
・事件に関わった各機関がISO/IEC 27001の認証を取得していたにも関わらず、現場では、情報セキュリティに関するリスクマネジメントが不十分であった。

記憶媒体からのデータの読み書きと消去

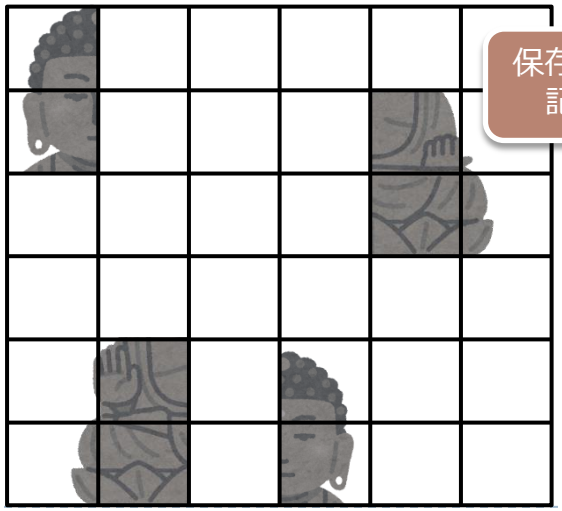


記憶媒体内部の保存領域



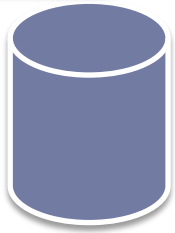
保存情報を示す
データベース

データの
読み書き



記憶媒体内部の保存領域

保存されているデータは
記憶媒体に存在する



保存情報を示す
データベース

データの消去

記憶媒体からの情報漏えいを防ぐための手段

- 記憶媒体に書き込むデータは暗号化する
  - Windowsでは「BitLocker」を利用する
  - mac OSでは「FileVault」を利用する

- 記憶媒体を破棄/返却する前にデータ消去を行う
  - 論理削除
  - 論理フォーマット
  - 物理フォーマット
  - 専用ソフトウェアによる消去
  - 強磁気による消去
  - 物理破壊による消去

記憶媒体におけるデータ消去

データの消去方法	論理削除・論理フォーマット	物理フォーマット	専用ソフトウェアによる消去	磁気消去	物理破壊
適用媒体	HDD, SSD	HDD, SSD	HDD, SSD	HDD	HDD, SSD
故障時への適用可否	×	×	×	○	○
再利用の可否	○	○	○	×	×
情報漏えいリスク	×	△	○	○	△
処分方法	譲渡・返却・廃棄	譲渡・返却・廃棄	譲渡・返却・廃棄	破棄	破棄

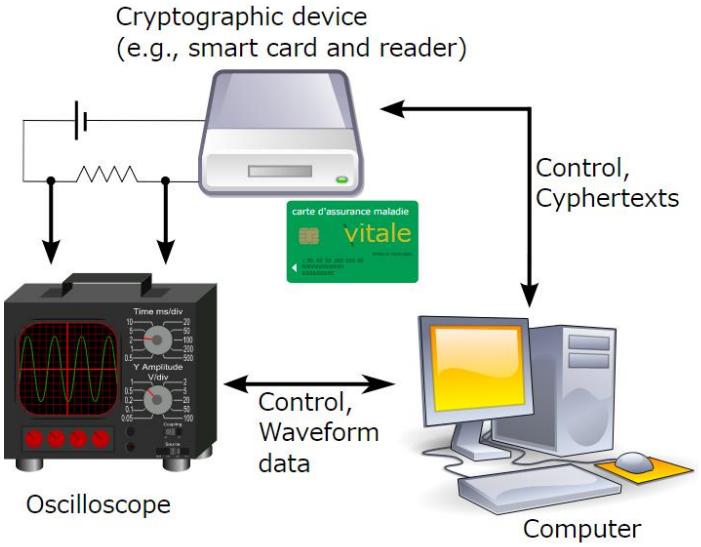
ソフトウェアによる消去

規格名	制定日	上書き回数	上書きパターン
米国 NIST SP 800-88 Rev.1	2006	1回	規定せず
米国 NISP Operating Manual (DoD 5220.22-M)	2006		
米国 国防総省 Unclassified Computer Hard Drive Disposition	2001	3回	ある文字, その補数の文字, 任意文字
米国 海軍 Staff Office Publication NAVSO P-5239-26	1993	3回	ある文字, その補数の文字, 乱数文字
米国 空軍 System Security Instruction 5020	1996	4回	0, 1, 任意文字
英国 HMG Infosec Standard 5, Baseline Standard		1回	0
英国 HMG Infosec Standard 5, Enhanced Standard		3回	0, 1, ランダム文字
カナダ Communications Security Establishment Canada ITSG-06	2006	3回	1または0, その補数の文字, 擬似乱数文字
ドイツ BSI	2004	2-3回	一様でないパターン, その補数の文字
Peter Gutmannのアルゴリズム	1996	最大35回	1, 0, 乱数文字をパスごとに混在
ブルース・シュナイアーのアルゴリズム	1996	7回	1, 0, 擬似乱数文字を5回

データの完全消去を定めた政府規格や業界標準が複数種類か存在する。全ての規格が着目している主要ファクターは「上書き回数」である。いくつかの規格では削除処理のベリファイ（再確認）や上書きパターンの表示について定められている。完全消去処理には、隠しセクタや代替セクタ処理で退避された領域の消去処理も要求される。

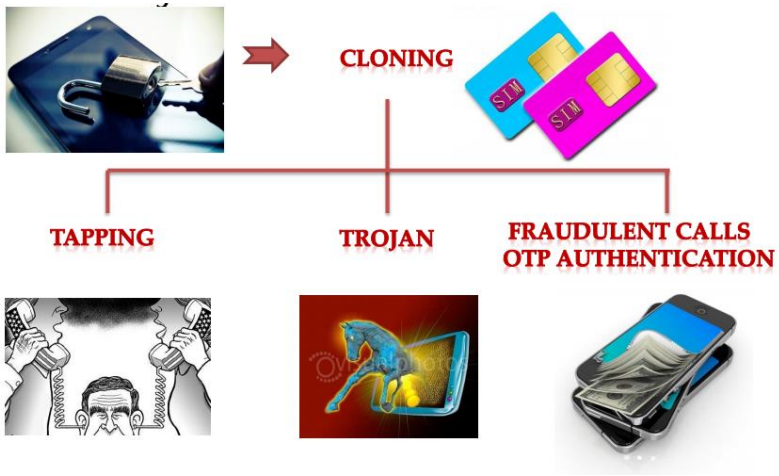
Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World

■ニューヨークやロンドンの地下鉄，オランダ国内で使用されているスマートカードの鍵をサイドチャネル解析で取得した報告．

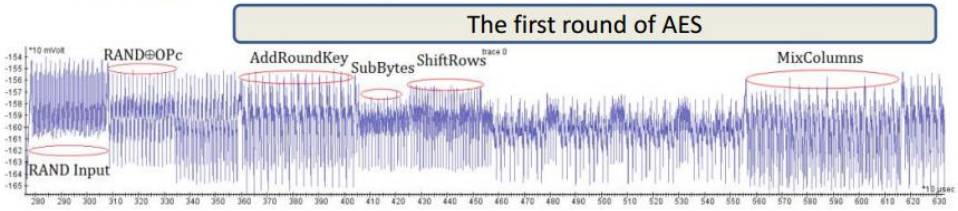


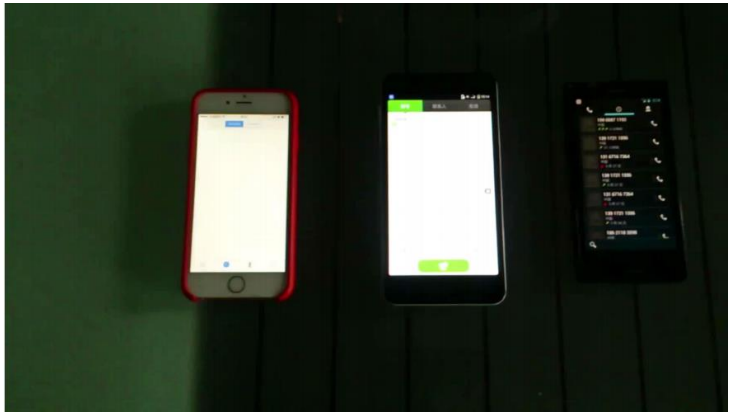
http://www.chesworkshop.org/ches2011/presentations/Session%205/CHES2011_Session5_1.pdf

Cloning 3G/4G SIM Cards with a PC and an Oscilloscope: Lessons Learned in Physical Security



Identify the segment of interest (simple power analysis) and zoom-in for further analysis.





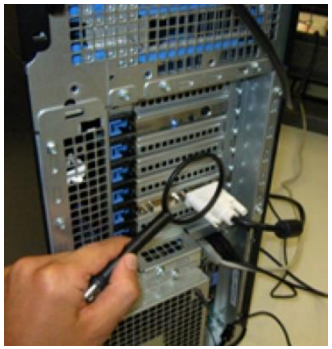
Making phone calls from a USIM and its duplicate to another phone.

https://www.blackhat.com/docs/us-15/materials/us-15-Yu-Cloning-3G-4G-SIM-Cards-With-A-PC-And-An-Oscilloscope-Lessons-Learned-In-Physical-Security.pdf

Defend encryption systems against side-channel attacks

- 大規模（SoC）システムに対する攻撃の報告.

Intel のAES-NI（サイドチャネル攻撃に耐性を有するという命令セット）を放射電磁波を用いて攻撃可能であることを報告



Intelプロセッサからの
放射電磁波計測の様子

The new Intel instructions set offer fast AES encryption/ decryption, which is protected against side channels attacks…

- Intel AES-NI (Advanced Encryption Standard New Instructions)
  - AESによる暗号化/復号を実行する新しい命令セット
  - Xeonなどに2009年から順次搭載

http://www.edn.com/design/systems-design/4438932/2/ Defend-encryption-systems-against-side-channel-attacks

まとめ

- 上位層のセキュリティと同様に物理層におけるセキュリティの確保も重要

- 物理層に対する不正なアクセスに備えたセキュリティ対策を行う
  - 記憶媒体の暗号化
  - 記憶媒体破棄時には適切な消去法を選択する

- 重要度の高い情報に関しては、より高度な攻撃も想定した対策を準備する必要がある