情報ネットワーク特論
情報セキュリティとその背景

名古屋大学 情報基盤センター
情報基盤ネットワーク研究部門
嶋田 創

情報セキュリティの話の流れ

- 情報セキュリティ(サイバー攻撃対策)とその背景
  - 近年増えるサイバー攻撃
  - ネットワークを経由しないサイバー攻撃
- ネットワークを介した様々なサイバー攻撃
  - 防衛側の機器とその運用
  - サイバー攻撃耐性の強いネットワーク運用
- マルウェア
  - マルウェア発見方法
  - どのようにマルウェアを解析するか?
- ネットワーク・フォレンジクス
  - どのように攻撃範囲や被害を追跡するか?

情報セキュリティにおける「情報」

情報: 価値のあるもの→守らなくていけないもの

- 情報を持っている人(管理する人)はその情報を取られないように守らなくてはなりません
- 悪い人にとっては、盗み出す対象となります

- 人によって価値の受け取り方が異なる点がやっかい
  - ジャニーズの〇〇がこっそり贔屓しているお店
  - ××鋼板の配合はマンガンxx%、クロムyy%...
- この点が、セキュリティホールになったりします
  - 情報の価値を理解できていない人が管理をおろそかに…
  - あるいは、攻撃者が情報の価値を理解していない人に流出を促すとか…

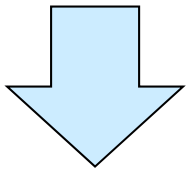
情報をどう守る?どう盗む?

- 情報を持っている人(管理する人)
  - 誰にでも読めなくする: 暗号化
  - 読める人を制限する: (パスワード)認証
    - ネットワーク上でも同じ
- 情報を盗もうとする人
  - 認証/暗号化を破る
  - 認証/暗号化情報を聞き出す
    - パスワードを聞き出す
    - 暗号鍵を盗み出す
    - こちらもネットワーク上でも同じ
- 亜種: 情報の利用をじゃましようとする人

→ひっくるめてサイバー攻撃扱い

Q: なぜサイバー攻撃が行われるのか

- 厳密にはサイバー攻撃を利用した犯罪(サイバー犯罪)
- 疑問
  - その攻撃手段への発想力を活かせば高収入で社会的地位の高い職業につけるのでは?



- A: 金になるから
  - 普通の職業についていたら一生かかっても稼げない金が手にはいるなら?
  - 所属する国によっては投資効率という面でも効率が高かったりする

お金になる情報

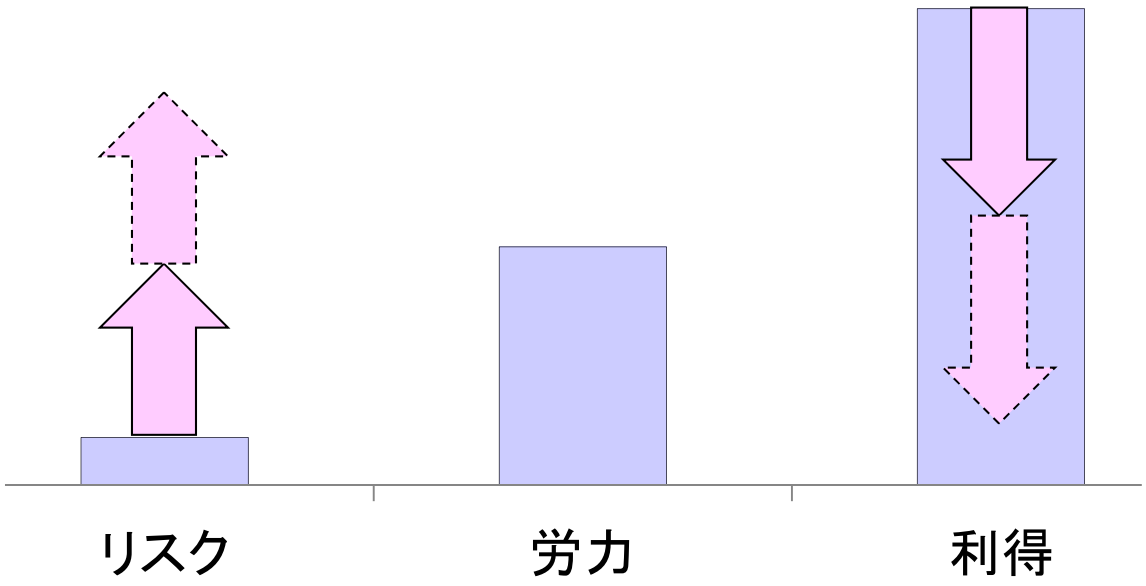
- クレジットカード情報
  - 悪用の他に、ブラックマーケットで売るという手も
    - フルセット揃うと1つにつき数十$程度
- 銀行(オンラインバンキング)決済情報
- 企業秘密
  - 他にも、どうしても手に入らない技術を手に入れるためとか
  - 某国は軍事技術に利用できる技術を一生懸命盗もうとしています
- 脅迫ネタ
  - 機密情報を手に入れた
  - 亜種: サービス不能(DoS)攻撃をかけるぞ

情報や攻撃の価格

- 本人認証に使われる情報: $1-$3
  - 社会保障番号、生年月日、など
- クレジットカード: $4-$20
  - どこで発行されたかによって価値が違う
- Remote Administration Trojan（RAT）: $20-$50
- ウェブサーバ乗っ取り: $100-$200
- DDoS攻撃: $60-$90 / day
- 感染して乗っ取ったコンピュータ: $120-$200 / 1000台

現状のサイバー犯罪

- 現在のサイバー犯罪はリスクに対して利得が大きすぎ
- リスクを上げて利得を減らす必要がある
- ただし、サイバー犯罪は世界規模なので、リスクを上げれない国家があることを考えておく必要がある
  - というか、そのような国を前提に考える必要がある



現情報攻撃側と防御側の勢力バランス

まあ、今までが悲観的なので想像できますが…

- 情報セキュリティ技術者の方が分が悪い
- そもそも後手後手に回ることになる
  - 犯罪者側は未発見の攻撃手段を1つ見つければ良い
  - 犯罪者は市販の情報セキュリティ技術を試せる
- さらに、法律などが足をひっぱることがある
  - 脆弱性解析などにおいて
- また、守りたい物を持っている企業が敵に回ることもある
  - 脆弱性を指摘すると、指摘された方から脅迫されたりとか

近年のサイバー攻撃の特徴

- 愉快犯的な物はほぼ無くなった
  - かつてのコンピュータウイルスのような拡散は少ない
  - 悪さをする人が便利なようにどんどん改良 →マルウェア
- 手間暇かけるようになった
  - 事前に目標の挙動を確認して罠をしかける
    - 目標への侵入後も即目的の活動をしない場合もあり
  - 某標的型攻撃では数ヶ月かかって目標達成
- 活動は静かに行われる
  - 発見されるのを防ぐため
  - 発見防止のために証拠隠滅までやる

情報セキュリティ人材問題(1/2)

- じゃあ? セキュリティ技術者が増えれば問題は解決する?
  →一朝一夕には増えません
- そもそもNHKがニュースにするぐらい不足[1]

[1] http://www.nhk.or.jp/kaisetsu-blog/100/202598.html

情報セキュリティ人材問題(2/2)

- Chief Information Security Officerに月給100万クラスを準備しても、でも要求レベルの人が来ないことも
  - 法律家や警察などの論理にも精通しているのが望ましいような人
- 大学の公募も苦労しているようです
  - 「情報セキュリティ技術者を育てるぜ」とコースは作ったは良いが、良い先生があつまらないという所が多々ある
  - JREC-INを見ると、某地方国立大が何度も公募を出し直していたり

→教育できる人がいないから人材が増えないという悪循環

- そもそも、情報セキュリティは情報技術の中でも若い分野
  - 当然、それに比例して人材が少ない
  - うちの研究室の前教授(50前後)が最長老クラス
    - 本来ならばもっと上の人が担当する委員会の委員まで担当することになって忙しそう

セキュリティへのコスト意識の問題(1/2)

- そもそも、セキュリティ対策は、警察や消防と同じで必要無ければ嬉しい組織
  - 仕事が無いのが一番な組織
  - でも、警察や消防を不要と言う人はいないが…
  - 企業としても、直接利益を産まない所には投資しにくい
- 同様の事例として、Windows XPをまだ使う例
  - 設計が古くて情報セキュリティ的には好ましくないのだが…
  - ユーザ側としては、まだ十分に使えるOS

セキュリティへのコスト意識の問題(2/2)

- セキュリティ人材へのコスト意識
  - 実際にある募集: 薬剤師の試験雇用のパートさんより安い!
  - 人材は不足しているけど突っ込むお金はもっと不足していて、経営者のコスト感覚は致命的に不足している

求人情報

就業時間	09:00〜17:45
仕事内容	■情報セキュリティガイドラインの評価支援業務1)情報セキュリティガイドラインの評価分析 2)評価分析の結果報告書等のドキュメント作成情報漏えい防止、アクセス権の設定、改ざん防止・検出、電源対策、システムの二重化などの対策状況を確認して、評価分析、報告資料を作成します。即日〜約2ヶ月間のお仕事となりますので、ご経験を活かしたい方はぜひご応募下さい♪
雇用形態	派遣
賃金形態	時給
賃金	1,600円

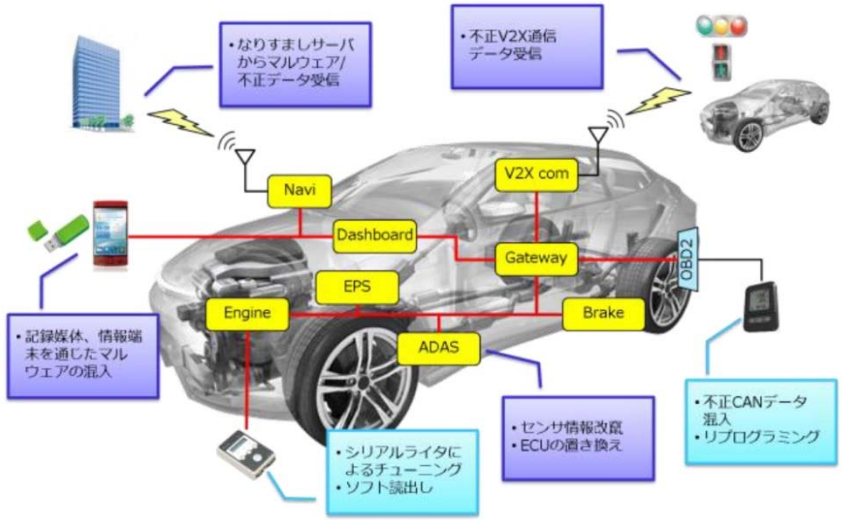
攻撃対象の増加(1/2)

- Internet of the Thing(IoT)
  - ヘルスケア用途など有望だが…

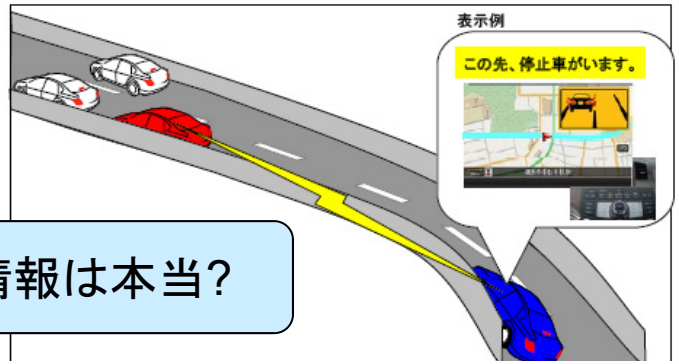
  →攻撃対象や踏み台利用の増加
- 車載ネットワーク/車間ネットワーク
  - コスト削減や交通事故削減に有望だが…
  - 車の制御システムを妨害したり
  - 他の車や信号に偽の情報を送ったり

↑ヘルスケアとIoT

↓車両制御システムへの攻撃



↓車間通信への攻撃

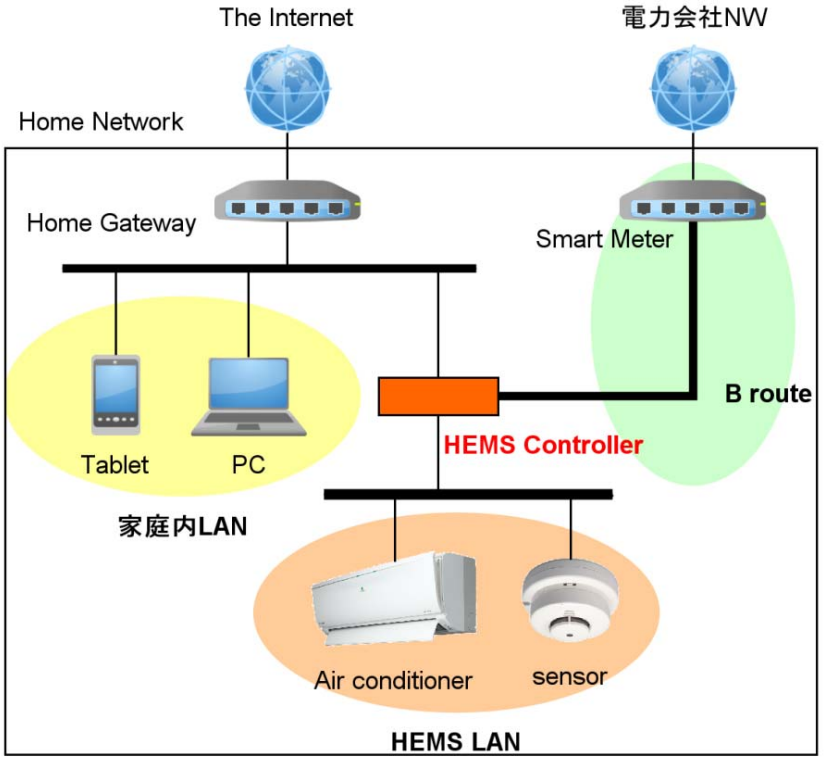


その情報は本当?

攻撃対象の増加(2/2)

- スマートグリッドの制御ネットワーク
  - HEMS (Home Energy Management Systemと連動)
  - 基本的に、家庭内LAN、HEMS LANとは分離されているはずだが…
  - 日本の住宅事情で複数サブネットのネットワーク線を通す構成できるの?

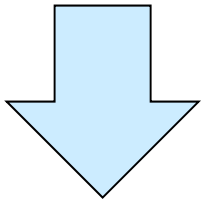
スマートグリッド普及者側が想定するネットワーク



通信量増大の問題(1/2)

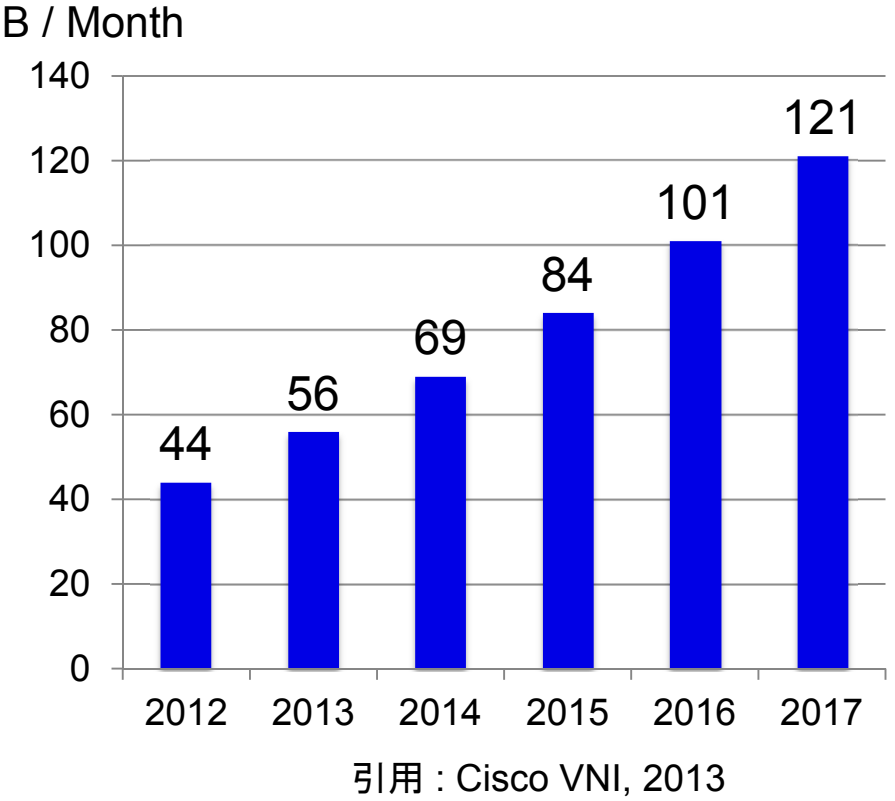
- 2017年のネットワーク接続デバイス 190億台
- 2017年の年間IPトラフィック量予測 1.4ZB
- IPトラフィック全体の年平均成長率 23%

トラフィックの増加に伴い
解析対象の増大



- 検査対象の増加
- DDoS攻撃の上限増加

→対策機器側の要性能向上

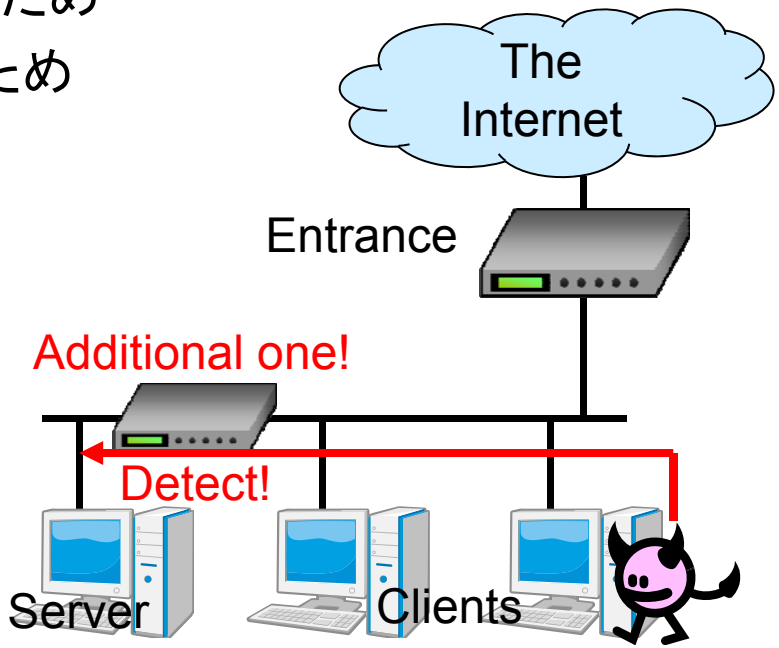


引用：Cisco VNI, 2013

通信量増大の問題(2/2)

- 近年では、対外接続部のみの不正通信は不十分
  - 標的型攻撃でセキュリティ意識の弱い部署を狙って組織内へ侵入
  - 侵入した部署から標的となる部署に攻撃をしかける
- 内部ネットワークの監視の必要性
  - 重要なマシン(e.g. サーバ)を保護するため
  - 重要な部局の仕事に影響を出さないため

対外接続部での監視に比べて
最低10倍のトラフィックをさばく必要



サイバー攻撃/犯罪対策をじゃまするもの(1/3)

内部側から(悪くないのも含む)

- セキュリティ対策への無理解
  - セキュリティ対策やEnd of Life機器の更新予算をかけてくれない
- 勝手なサイバー攻撃対策作業
  - 勝手にリカバリディスクを使ってノートPCを初期状態に戻すとか
  - ヘタすると、警察から「主犯が証拠隠滅を行った」と見られます
- 移動する無線LAN接続のクライアント
  - 外部で接続した時にマルウェアを拾ってきて内部でばらまいたりとか

サイバー攻撃/犯罪対策をじゃまするもの(2/3)

犯罪者側から

- そもそもマルウェア側に対策が行われるのを検知する機能があったりする
  - マルウェア内に偽ドメインを埋め込む →偽ドメインの名前解決があったら解析されている
  - 標的以外のIPアドレスの範囲からの通信があったら検知と判断
  - そもそも、起動時にGoogleなどのメジャーなサービスへの接続性を確認したりする
- 対策しようとするとDDoSをかけてきてじゃましようとしたりする

サイバー攻撃/犯罪対策をじゃまするもの(3/3)

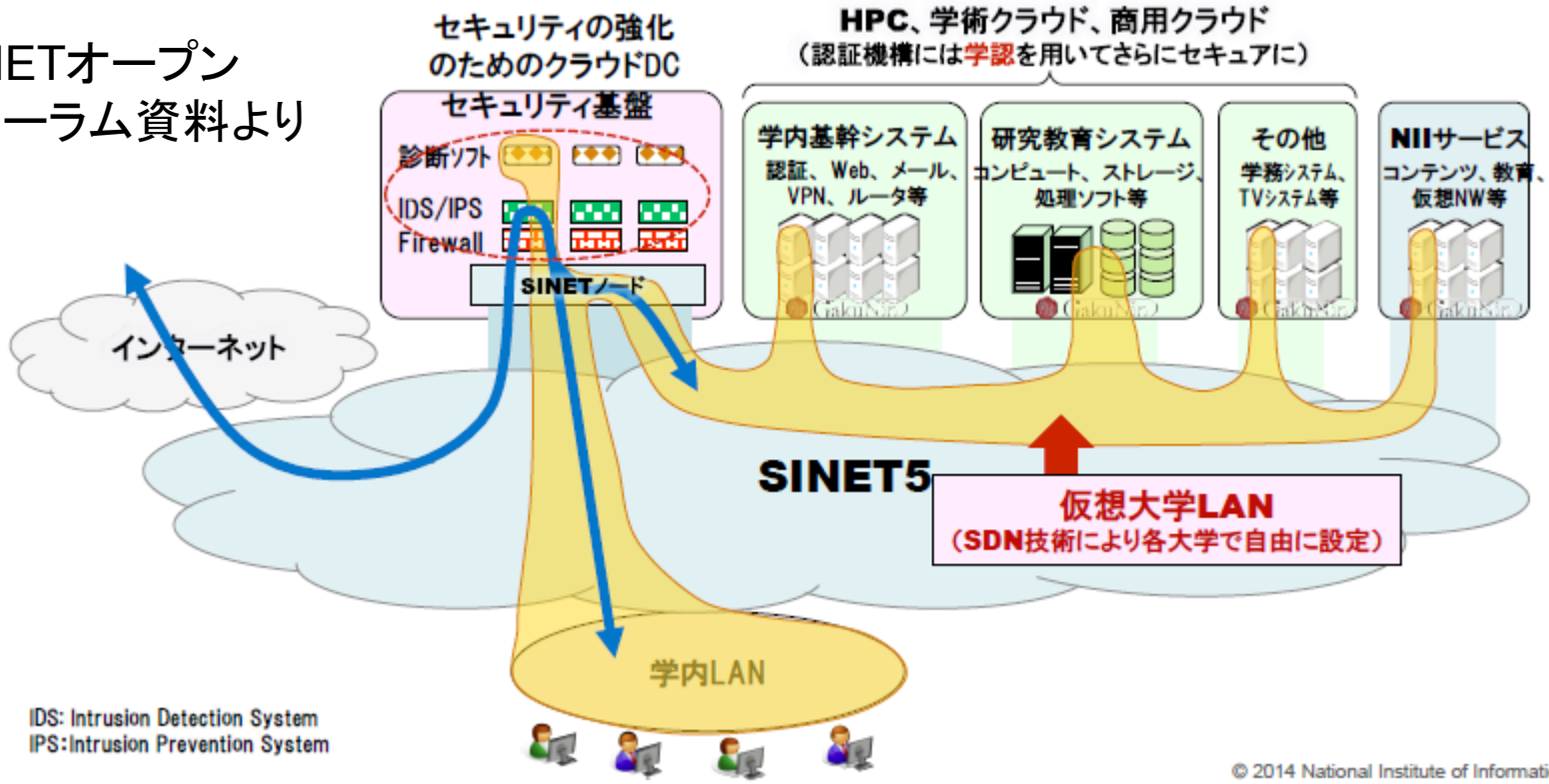
ソフトウェア/サービス開発側から

- あまり使われない機能の追加&デフォルト有効によるセキュリティ・ホール追加
  - OpenSSLのheartbleed
  - bashのshellshock
- 右肩上がりの目標はいい加減な所でやめて欲しいのだが…
  - 新たな機能を追加すれば新たな人が無限呼び込めるとか考えているの?
  - どこかで一旦、安定に入ってもいいと思う
    - もちろん、必要性が出てきたら開発再開でいいけど
  - 最近はFirefoxがその領域に入っているので嫌な感じ

セキュリティ側から見えている希望(1/3)

- クラウドコンピューティングを利用した集中防御
  - SINETもクラウドを作成して大学の情報セキュリティを担う方向
  - ただ、運営者を信頼できるかという問題はつきまとう

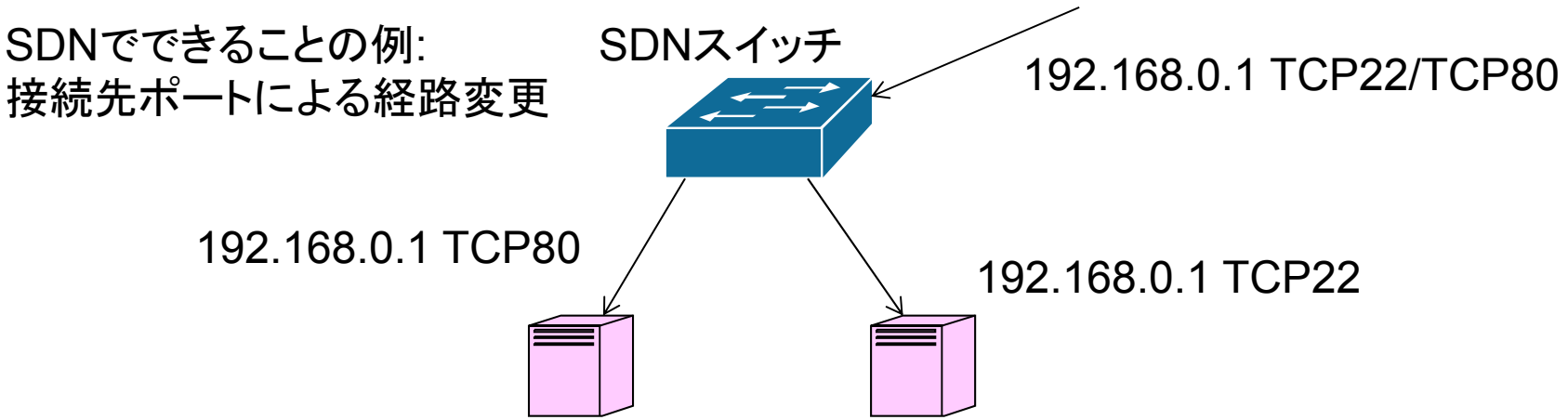
SINETオープン
フォーラム資料より



セキュリティ側から見えている希望(2/3)

- SDN(Software Defined Network)による柔軟なネットワーク
- SDNの特徴
  - ソフトウェアのような柔軟な経路選択ルール作成
    - 送信先ポート、送信元IPアドレス/ポート、など
  - 同一IPアドレスに対してTCP/UDPのポートに応じて経路選択可能

  →マルウェアの通信のみ捻じ曲げることが可能



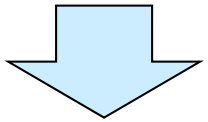
セキュリティ側から見えている希望(3/3)

- ビッグデータ処理の応用
  - 通信解析、マルウェア分類、などへの応用
  - 異常な通信ではなく、通常の通信の定義からの情報セキュリティ適用
  - ビッグデータに向けた計算機の能力向上研究の進歩
- 人が足りないなら自動化すれば良いという目標の研究
  - 熟練情報セキュリティ技術者の知識適用の自動化
  - 別に100%を目指す必要はない
    - 自動化で80%を除外できるならば、人の負荷は1/5に

USBを利用した(物理的な)(セキュリティ)攻撃(1/2)

USBは色々とplug and playができて便利だが、本当にそのUSBデバイスつなげて大丈夫?

- 学会で予稿集配布されている共用USBメモリは大丈夫?
- そもそも、学会で個別配布されたUSBメモリでも大丈夫?
- そのUSB接続で充電するデバイスは大丈夫?
  - 電子タバコにマルウェアが入っていた事例
- 正体不明のUSBメモリが置いてあったので、持ち主を探そうとして中身を見るためにPCに接続して大丈夫?



対策案: USB/microSDをNASにできるWiFiルータを利用する?

USBを利用した(物理的な)(セキュリティ)攻撃(2/2)

もっと怖いUSB経由攻撃デバイス

- Killer USB
  - 内部にコンデンサと昇圧回路を持つ
  - USBの電源線からチャージした電力を±110Vで信号線に流し込む

  →過電圧によりデバイスを破壊
    - 運が悪ければSSD/HDDなども…
- Bad USB
  - USBの認証用ファームウェアレベルで攻撃をしかける

ソーシャルエンジニアリング

- 最終的に計算機を使うのは人間
  →人間をセキュリティホールと考えた攻撃
- よくある手口
  - 欺術によるパスワード入手: 非常を装ってコールセンターを騙す
  - 欺術によるマルウェア設置: 知人を騙ってマルウェア送付
  - より低レベルな方法: 覗き見、手続きにはパスワードを書いて下さい、など

- この分野の良書紹介:
  Social Engineering: The Art of Human Hacking
  - ケビン・ミトニックという有名クラッカーの著書
  - 日本語版もありましたが、絶版になっています
    - “欺術”という言葉はその日本語版タイトル

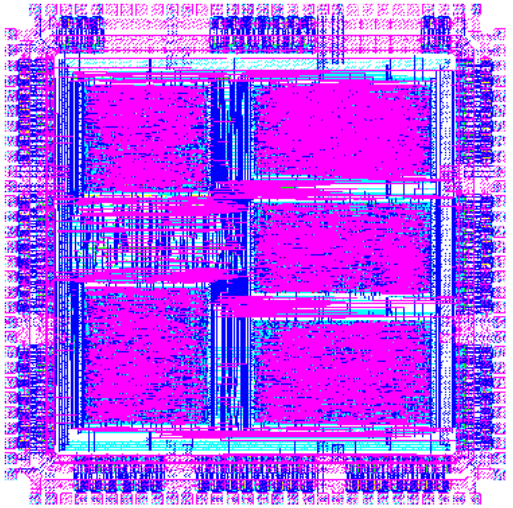
ハードウェアレベルでの攻撃

- 情報はカネになるので、カネと手間をかけた攻撃も行われます
  - 「かけたカネ<得られるカネ」ならばかける価値はある
- ハードウェアレベルでのセキュリティ攻撃も行われます
  - チップ物理解析
  - サイドチャネル攻撃
- カネをかけてパスワード/暗号鍵解読専用マシンを設計することもあります
  - 厳密にはここに含めるのは正確でないのですが

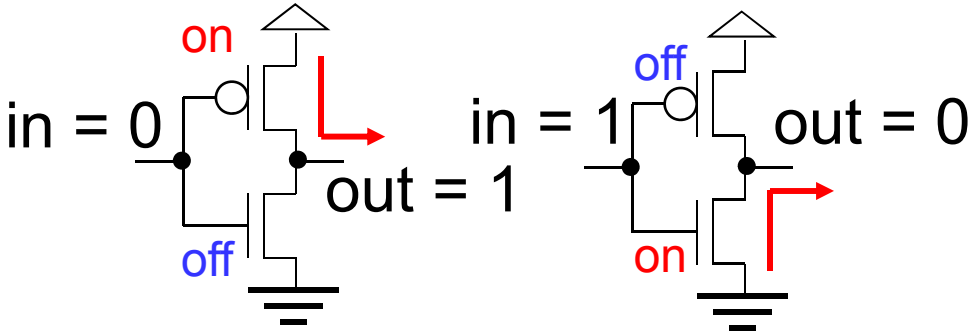
チップ(集積回路)物理解析

- チップ上のトランジスタや配線を解析
- 回路に埋め込まれた暗号鍵などを解析
  - 0 = 電圧なし = GND(マイナス)側に接続
  - 1 = 電圧あり = VDD(プラス)側に接続
- 最近の半導体プロセスで製造された物では難しい
  - トランジスタ等が非常に微細化されている
  - トランジスタの上に少なくとも数層の配線層が存在

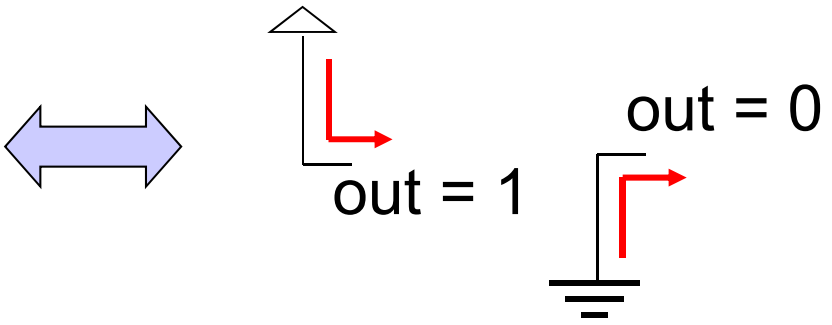
チップ上の回路レイアウト



CMOSによるNOT(論理否定)回路



回路に埋め込まれた定数



サイドチャネル攻撃

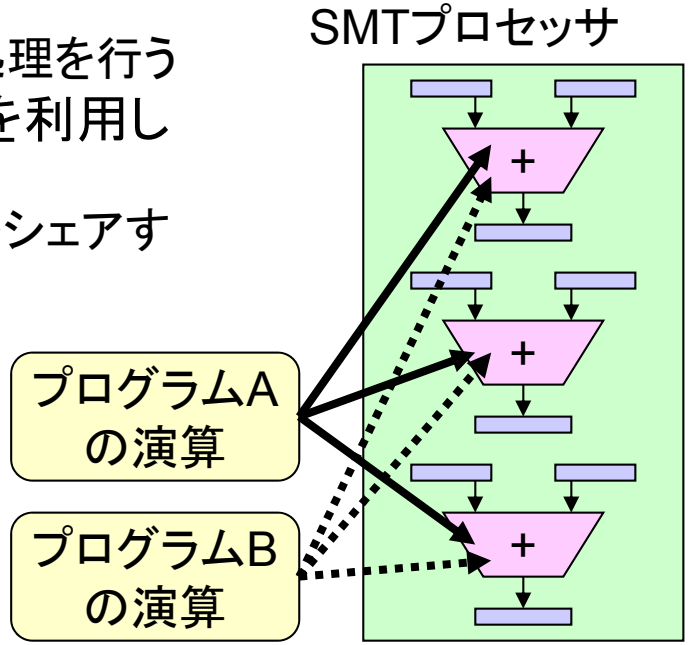
- 暗号処理等によって他の部分に出る影響を調査して暗号鍵等を推測
  - 基本的に、非常に多くの試行と結果の統計処理が必要
  - 完全な暗号鍵を推測できなくても、鍵空間を狭めることができれば…
- 自動化しやすいので、こちらの方がホットな攻撃方法
- 代表的なサイドチャネル攻撃
  - 応答時間解析
  - 故障解析
  - 電力解析
  - 電磁波解析

応答時間解析(1/2)

- 暗号鍵の数値によって演算時間が変わることがある
  - 例: 乗算において、0の桁があればその桁の処理は飛ばせる
- これを暗号鍵の推測に用いる
  - 計算が早ければ0の桁の多い暗号鍵では?
  - 比較用に作成したの暗号鍵の演算時間と比較
- 対策: 演算が簡単になる暗号鍵でも同じ演算時間になるように回路/プログラムを構成
  - 例: 0の桁があってもちゃんとその桁の加算処理を行う
- Simultaneous Multi-Threading(SMT)処理を利用した応答時間解析もある
  - SMT: 同時に複数のプログラムで演算器等をシェアするプロセッサ構成
  - 暗号鍵に応じた応答時間を変化させるように工夫したプログラムをぶつける

2進数乗算の桁処理飛ばし

```
   0110          0110
 x 0101        x 0111
 ------        ------
   0110          0110
 0110          0110
 ------        ------
 011110        0110
               ------
               101010
```

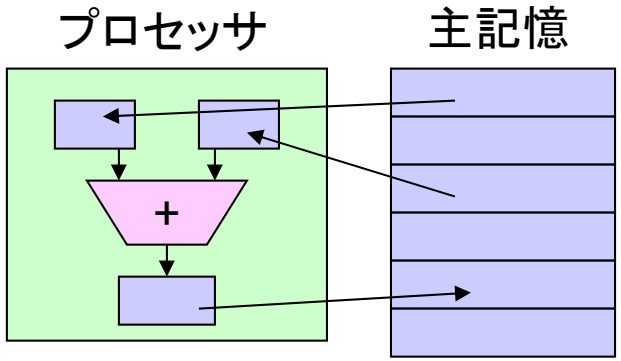


応答時間解析(2/2)

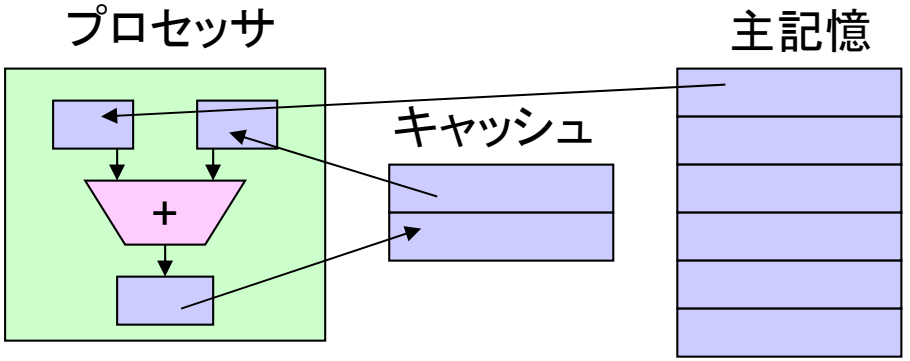
- 演算器以外でも応答時間解析はできる
  - キャッシュ: プロセッサ直近の高速メモリ
    - 処理すべきデータがキャッシュ載っていると処理時間が短くなる
    - 設計時に増減が容易なため、製品によってサイズが異ることが多い
  - 暗号鍵によってキャッシュ効果が異なることが起こりうる

    →暗号鍵の推測に用いる

キャッシュなしの計算機構成(第1回)

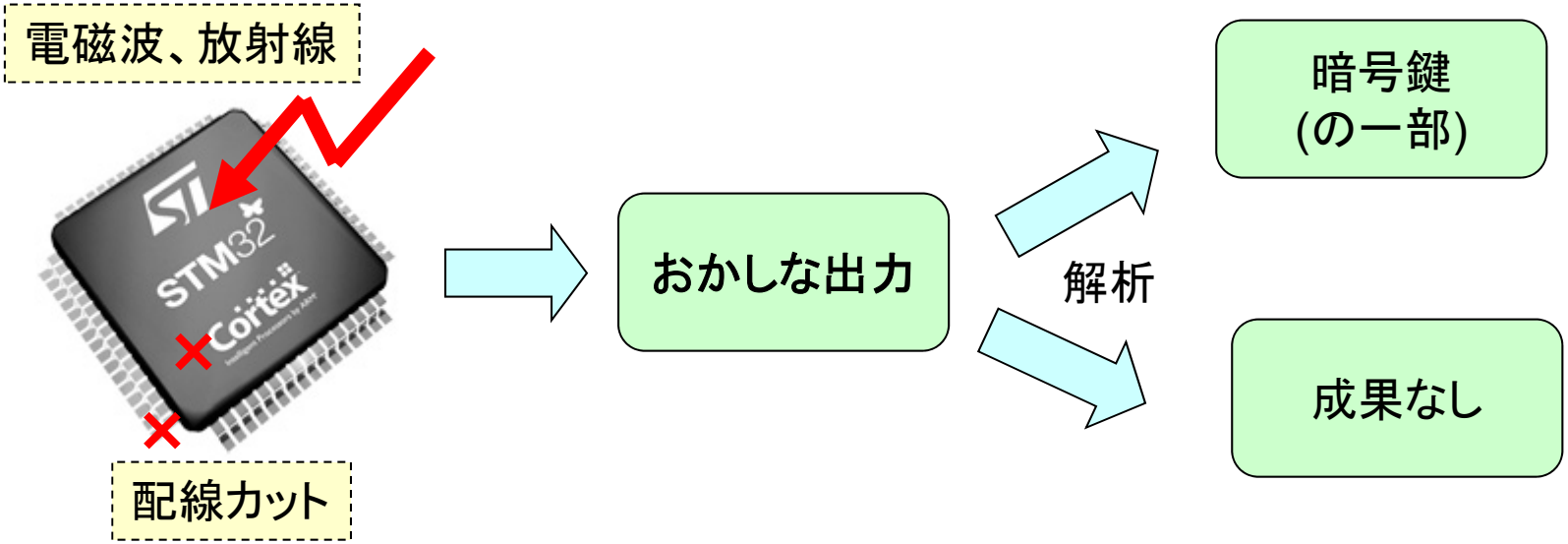


キャッシュありの計算機構成



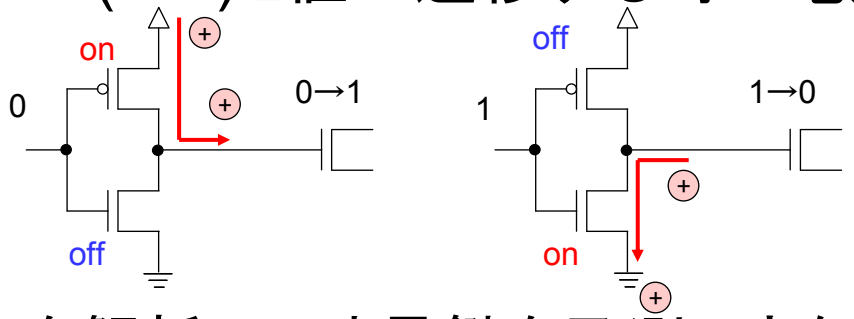
故障解析

- チップに意図的に故障を起こして出力の変化を見る
  - 配線を切ってみる
  - 光、熱、電磁波、放射線を加えてみる
- 変化した出力から暗号鍵を推測できないか?

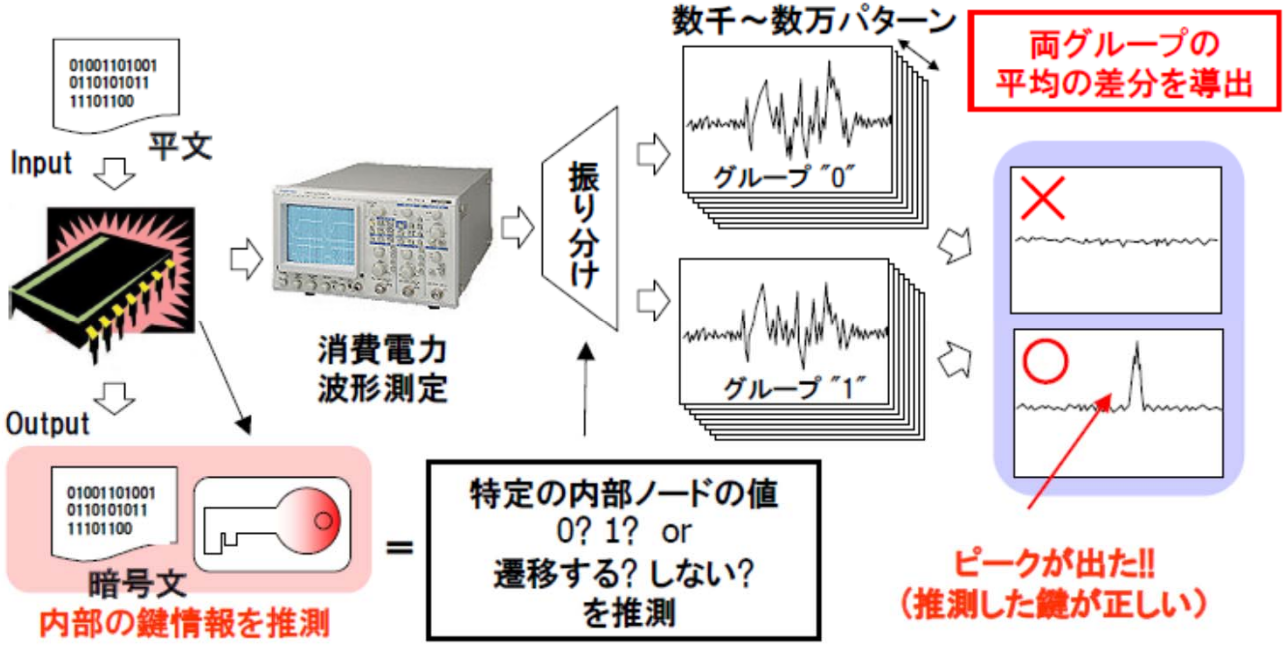


電力(差分)解析(1/2)

- 回路は0→1(→0)と値が遷移する時に電源から電荷が移動

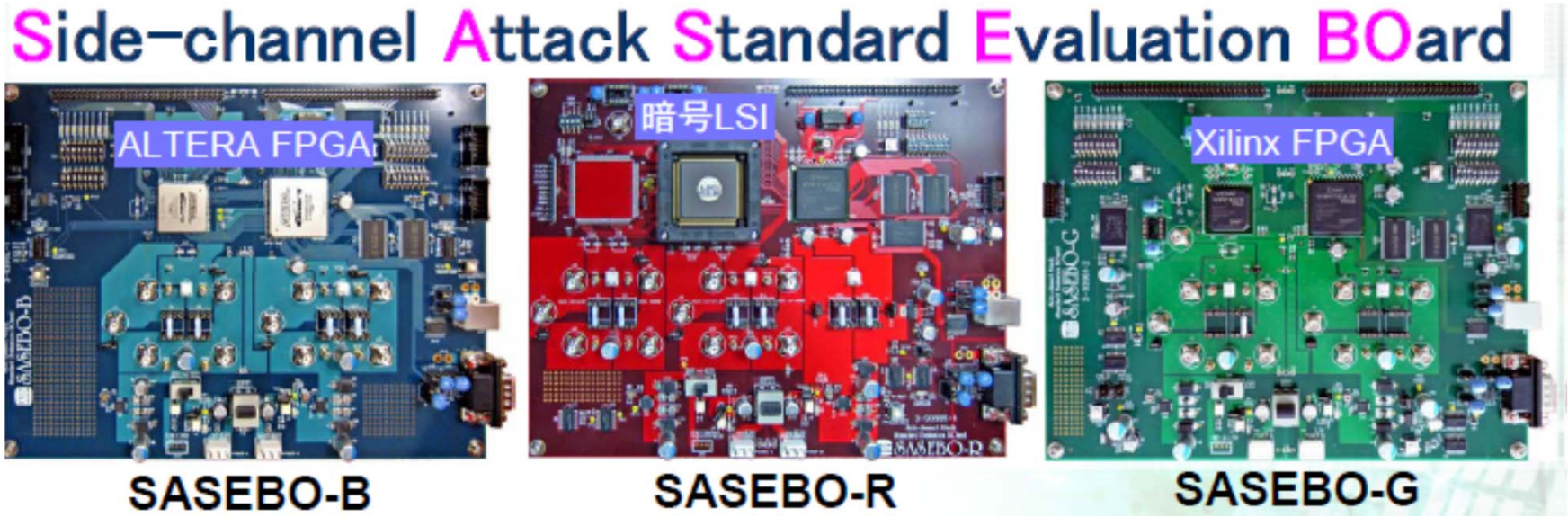


- 消費電力を解析して暗号鍵を予測できないか？



電力(差分)解析(2/2)

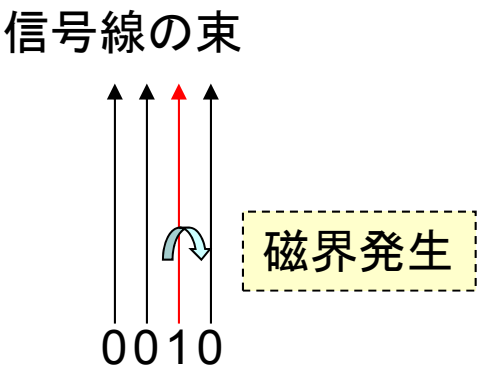
- 対策: 相補的な結果を出力する演算を行う、など
  - 論理を反転させたデータの演算を行う、ANDの論理演算と同時にORの論理演算を行う、など
- 国内では、産総研のSASEBOプロジェクトが有名(現在は後継プロジェクトへ)
  - 成果を対サイドチャネル攻撃の国際標準に働きかけ

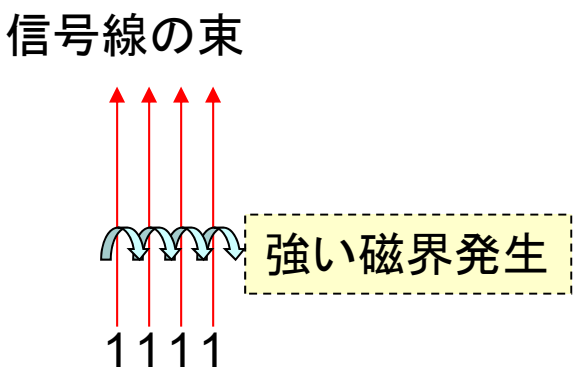


電磁波解析

- チップ上で演算処理を行うと電磁波が発生します
  - 電流が流れると電界/磁界が発生します
- チップ上の複数の配線上に”0000”なデータと”1111”なデータが流れると差は出るか?

  →電界/磁界が合成され、電磁波の強度の差として出る
  - これを統計的に解析
- 対策: 0/1を反転させた(負論理)のデータを同時に流す、など





暗号鍵解読専用ハードウェア

- 例: EFF DES Cracker
  - DESを解読するのに作成された専用HW
    - ソフトウェアによる攻撃での解読時間41日を56時間に短縮
- 最近では、FPGAのような書き換え可能HWの大規模化も進んでいる
  - 専用HWではないが、メニーコアやGPGPUにも暗号鍵解読を加速中