サイバーセキュリティ分野における研究開発への期待

菊池　浩明
明治大学

NICTサイバーセキュリティシンポジウム2016

菊池 浩明Hiroaki Kikuchi

- 総合数理学部 先端メディアサイエンス学科 教授
- 略歴 明治大学卒
  富士通研究所，東海大学情報通信学部教授、カーネギーメロン大学計算機科学科訪問研究員などを経て2013年明治大学
- 電子情報通信学会ICSS研究会専門委員会顧問，
  JPCERT/CC理事，
  情報処理学会CSEC研究会顧問，理事（2014-2015)
  情報ネットワーク法学会理事

- JISAプライバシーマーク審査委員会・委員
- NICT映像センサー使用大規模実証実験検討委員会・委員長
- 内閣官房IT戦略室　パーソナルデータに関する検討会技術検討WG・構成員
- 経済産業省マルチステークホルダープロセスの試行及び検証に関する検討委員会・アドバイザー会議委員長

サイバーセキュリティの今

年金機構へのサイバー攻撃

- 2015年6月2日
  - 日本年金機構から，氏名，基礎年金番号など125万件が流出.
  - 5月8日に電子メールの添付ファイルで感染（遮断せず業務継続)
  - 5月19日警視庁相談
  - 5月28日NISCが外部と不正な通信を検出.

パリ同時テロ

- 2015年11月13日
  - コンサートホール，カフェ，サッカー場などを標的とした同時多発テロ
  - 128名死亡
  - ISの犯行声明
  - 18日容疑者と銃撃戦2名死亡
  - 22日ベルギー，警戒最高レベル，地下鉄駅閉鎖

Anonymous 日本を標的

- DDoS攻撃
  - 太地町，油壺マリンパーク(9/5)，しながわ水族館(11/3)
  - 観光局(10/10)，厚労省(11/21)
  - 東洋経済(10/23)，毎日新聞(11/4)，日経新聞(11/10)
  - 五輪組織委(11/6)

アップル対FBI

- 2016年2月
  - 2015年12月米国カリフォルニア州サンバーナディノ14名殺害テロ事件
  - FBIは容疑者のiPhoneのパスコードを求める
  - アップル「危険な先例になる」と反発.

NTT東日本　中継サーバー解約

- 2015年11月27日
  - 警視庁がサーバー業者を逮捕
  - 12万4千件個人情報，インターネットバンキング8500万円不正送金
  - 通信回線の解約をNTT東日本に要請
  - 電気通信事業法，憲法「通信の秘密」
  - 12月9日解約

フィンテックへの期待

- 2016年2月1日
  - 三菱東京UFJ銀行がブロックチェインを用いた「行内通貨」を開発
  - 国際送金，振込手数料を低減
  - 現金と可換に

フィンテックの悪用

- 2016年2月16日
  - 米ロサンゼルスの病院，救命救急室にハッキング
  - ランサムウェア(TeslaCrypt)によりファイルを暗号化し，拡張子 .vvv を付ける
  - 360万ドルのビットコインの身代金

サイバー攻撃の傾向

- 現実世界とサイバー空間の距離が近づいた
  - ISとのサイバー戦争
  - IoTデバイス，車や制御システムもターゲットに
- 政府やキャリアは，（現実世界の）安全性と（サイバー空間）の狭間で当惑している
  - Apple v.s. FBI, 警視庁 v.s. NTT東
- 新しい技術に新しい脆弱性
  - ビットコインやTorの悪用

「完全防御」から「侵入」の想定へ

- もはや絶対に安全は保証不能
  - 年金機構は実は頑張っていた
  - 利用者権限で動くランサムウェア
  - 不特定多数と通信する業務の必要性
- 侵入されても頑強な体制へ
  - もしもの想定がない組織のもろさ
  - 人間系の誤りは不可避
  - *fail-safe security*

侵入されても耐性のある
サイバーセキュリティの技術

fail-safeなセキュリティ

侵入前提のセキュリティ技術

- 1. サイバー演習
- 2. CSIRT
- 3. 出口対策
- 4. 内部犯行対策

1. サイバー演習

- 総務省「実践的サイバー防御演習(CYDER)」
  - 2013年より3回
  - 2015年度，全8回，計101組織(応募345)，275名，
  - 12のマイルストーン
    - » 事象発見，通報，収集，証拠保全
    - » 可否判断
    - » 原因推定，復旧，再発防止
- セプター
  - 官公庁　25，
  - 地方自治体　32，
  - 金融　27
  - 独法　6

http://biz.nikkan.co.jp/news/nkx0220151027abau.html

標的型攻撃演習

- 訓練サービス (GSX)
  - 訓練メールの送信
  - クリック率のレポートと教育

http://www.gsx.co.jp/informationsecurity/attackmailtraining.html

2. CSIRT

- computer security incident response team (CSIRT)
  - 1988 CERT
  1. SOC(Security Operations Center) 検出
  2. Incident Response Team 対応
  3. Forensic investigators　保全
  4. Engineering team

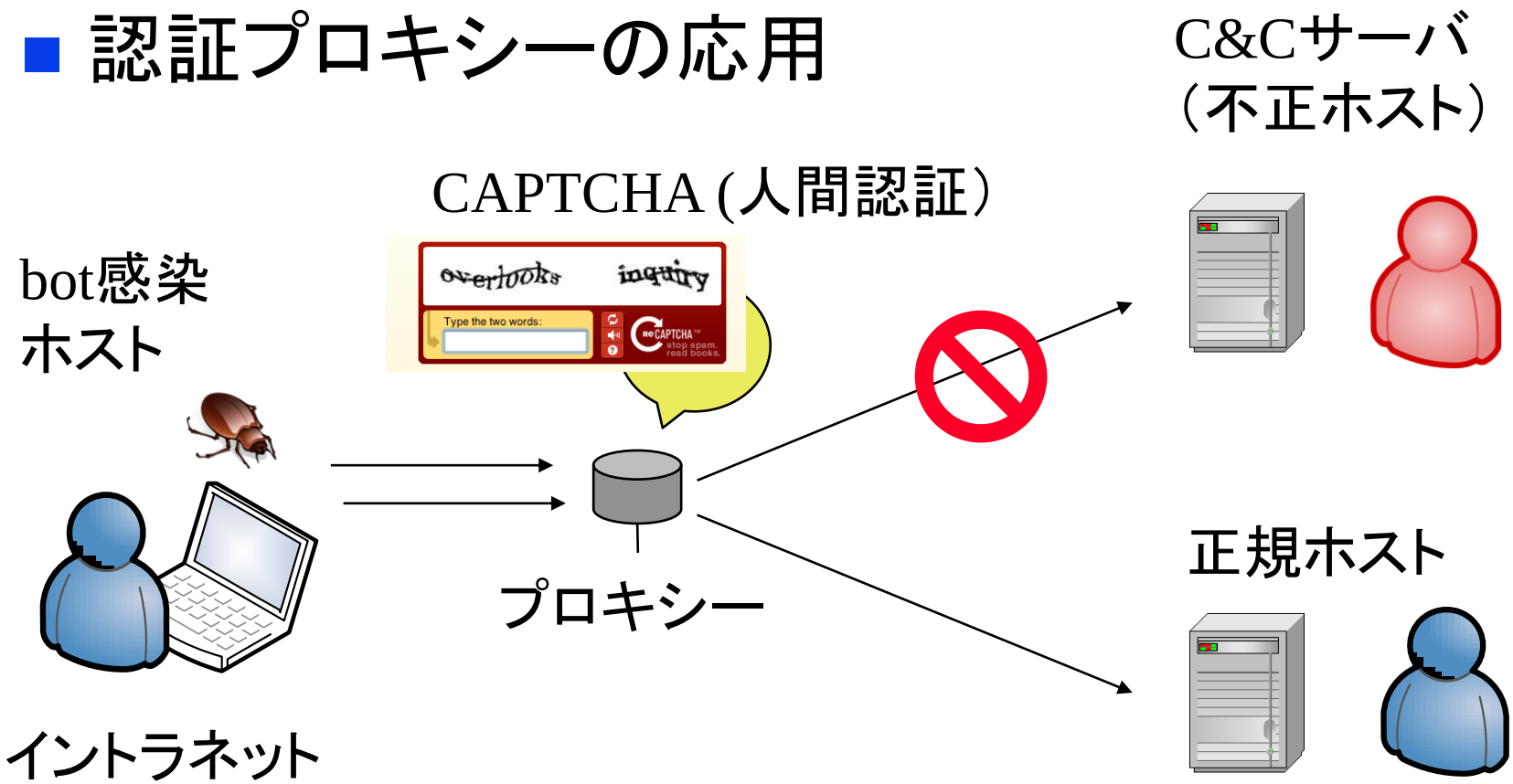
日本シーサート協議会 NCA

- 2007年設立
  - JPCERT/CC事務局
  - 会員間情報共有
  - ワーキンググループ
  - 年次会合
- 106組織
  （waiting 90組織）

http://www.nca.gr.jp/

3. 出口対策

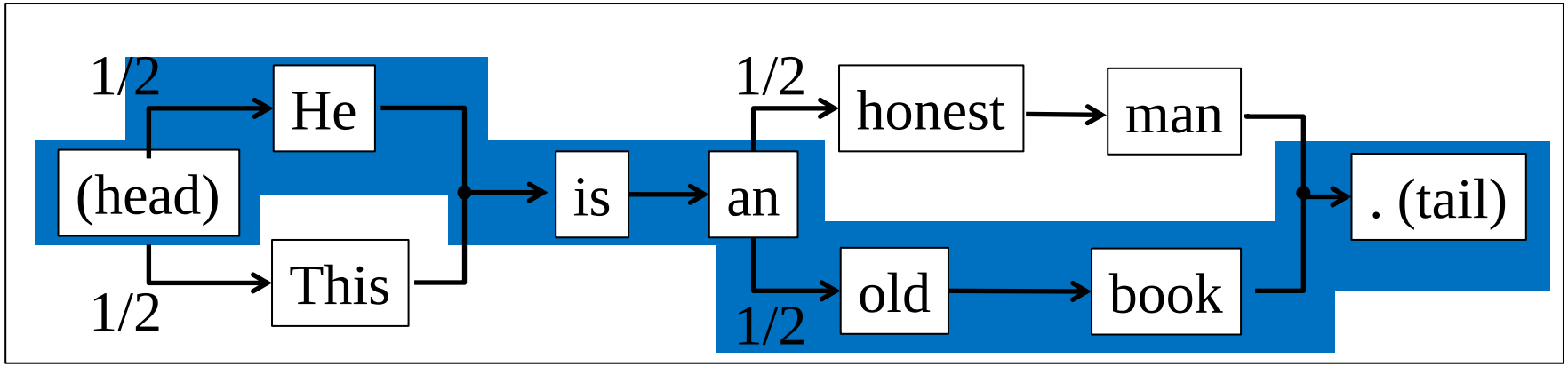
- 認証プロキシーの応用



Word Salad CAPTCHA

- Markov chain of order *N*
  - State *N*+1 depends on the states of the former *N* units.

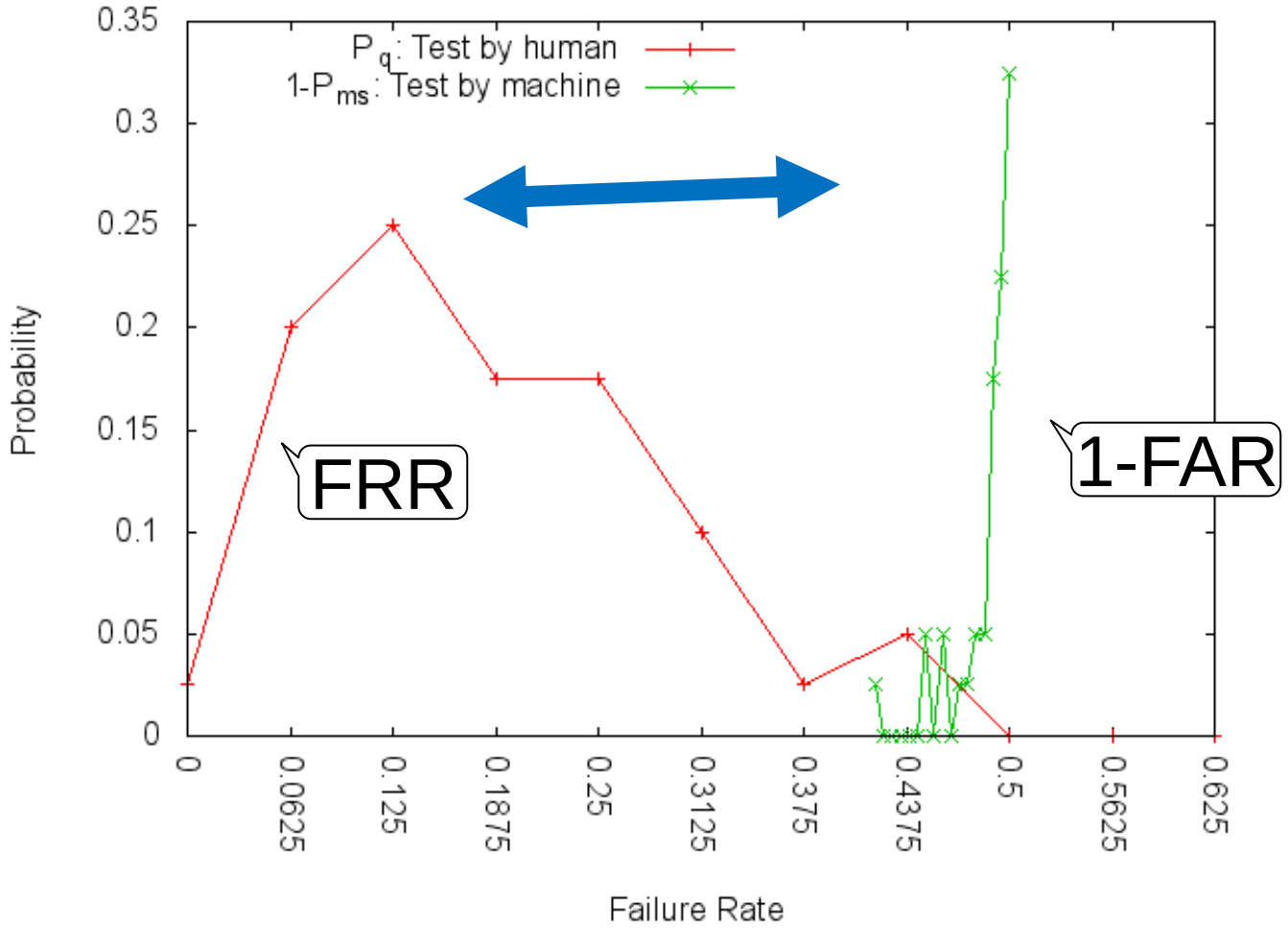
Example: *N* =1, corpus { He is an honest man. / This is an old book.



"*He is an old book*." (, and so on.)

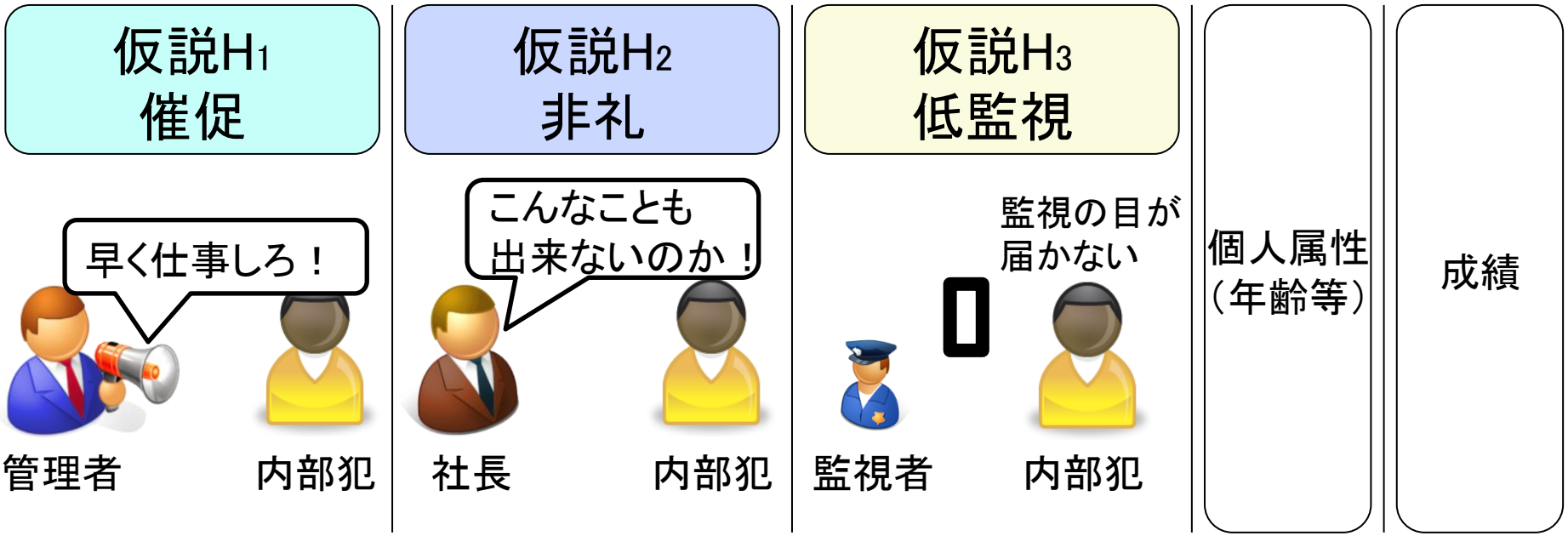
Yamaguchi, Kikuchi, "CAPTCHA System by Differentiating the Awkwardness of Objects", NBiS 2015, IEEE.

Comparison of Failure Rate between Human and Bots



4. 内部犯行の誘発要因

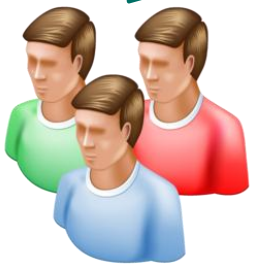
- **本質的な**内部犯行を誘発する要因はどれか？



新原，菊池，「eラーニングをモデルとした内部犯行の予測因子の識別」，CSS 2015

実験方法：クラウドソーシングの利用

・本人確認書類の提出が確認済
・作業承認率が95%以上



被験者

①作業受託
③完了報告
⑥費用支払
（496円/名）

Lancers
クラウド
ソーシングサイト

⑤被験者承認

実験管理者

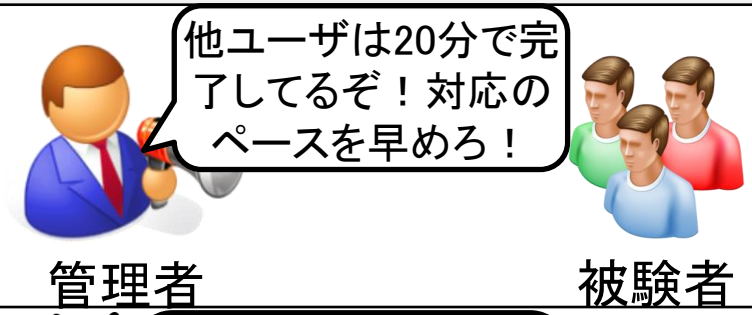
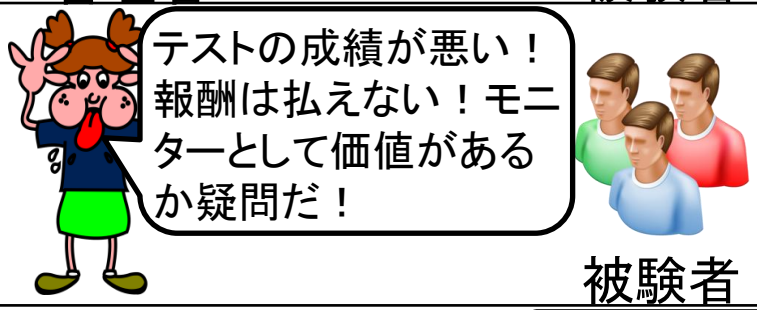
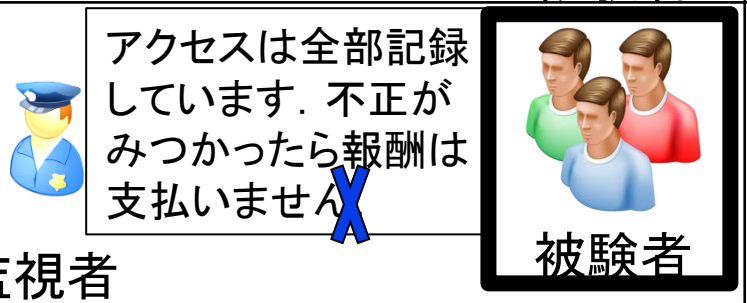
②受講

eラーニング
サイト
（構築）

④ログ確認

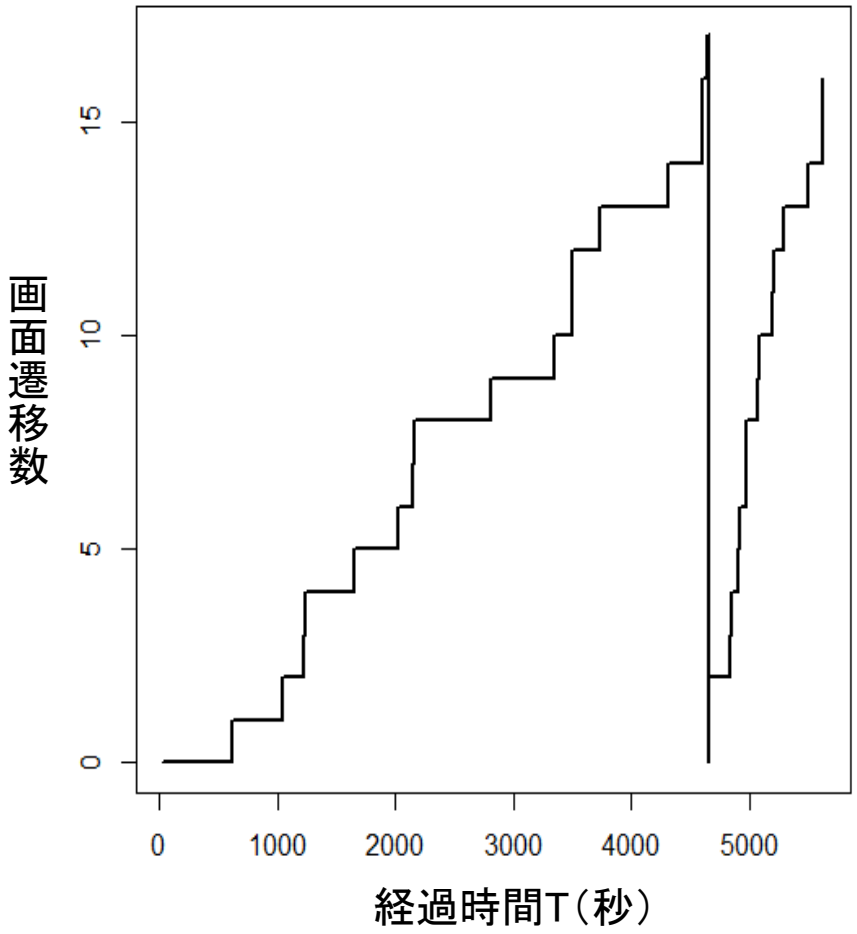
実験方法：本実験の疑似事象とグループ

【凡例】○・・・事象発生、－・・・事象未発生

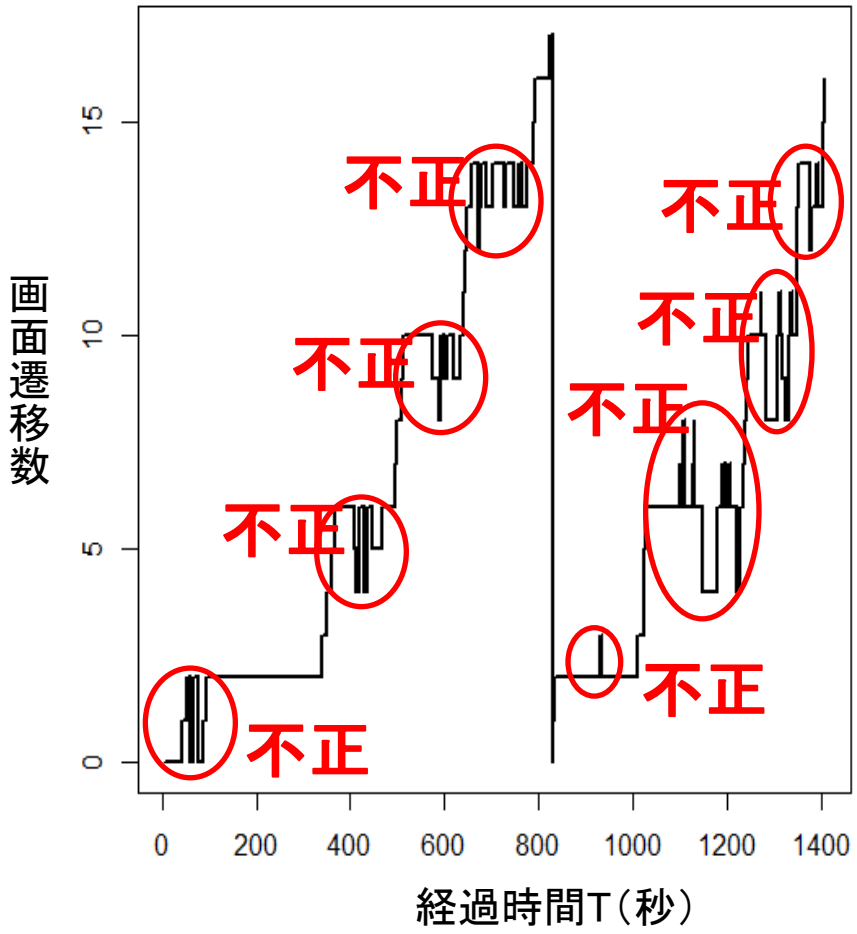
内部犯行誘発要因	擬似事象	グループ A	B	C	D
催促文言 (H_1)		○	－	－	－
失礼画像 (H_2)		－	○	－	－
低監視 (H_3)		－	－	○	－

不正事象(1)画面遷移逸脱

正常パターン

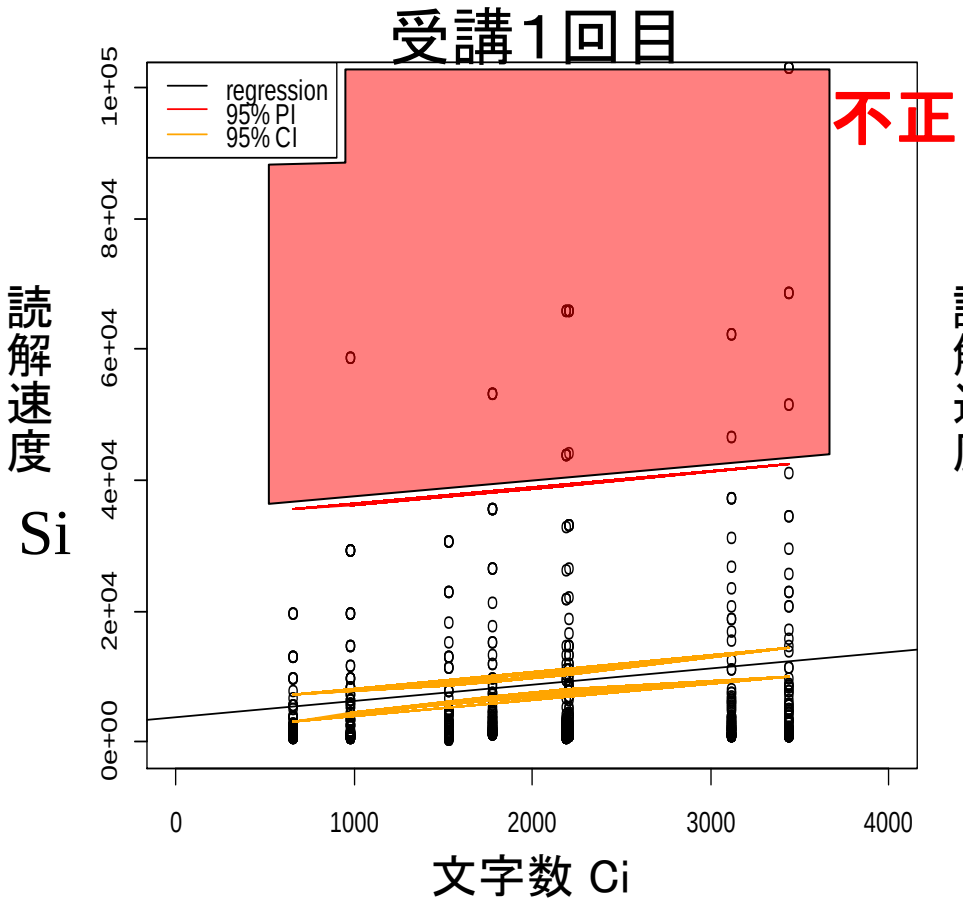


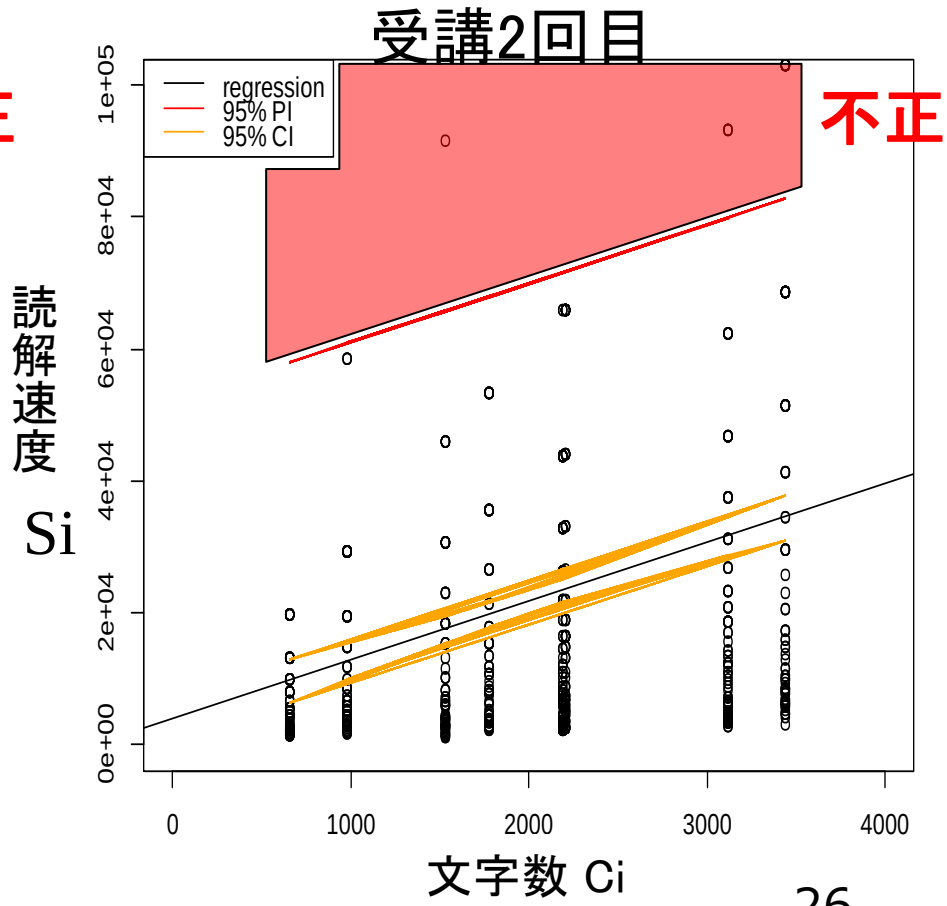
異常パターン



不正事象(2)教材未読回答

- i番目の教材の読解速度Si(文字数/分) $S_i = \frac{C_i}{T_i} \times 60$





実験結果：グループ別不正事象数

		内部犯行誘発要因	N	①画面遷移逸脱	（再掲）1−1	②教材未読回答	（再掲）1−1	③答案未回答	（再掲）1−1	④ＨＴＭＬソース等確認	（再掲）1−1
グループ	A	催促文言(H_1)	24	6	4	5	0	0	0	0	0
	B	失礼画像(H_2)	22	4	2	6	0	0	0	0	0
	C	低監視(H_3)	27	9	5	11	0	3	0	1	0
	D	―	27	9	4	1	0	1	0	0	0
合計			100	28	15	22	0	4	0	1	0

誘発要因毎の差は**なさそう**

誘発要因毎の差が**ありそう**

不正事象の発生ユーザ数が少ない

ロジスティック回帰分析：グループ別

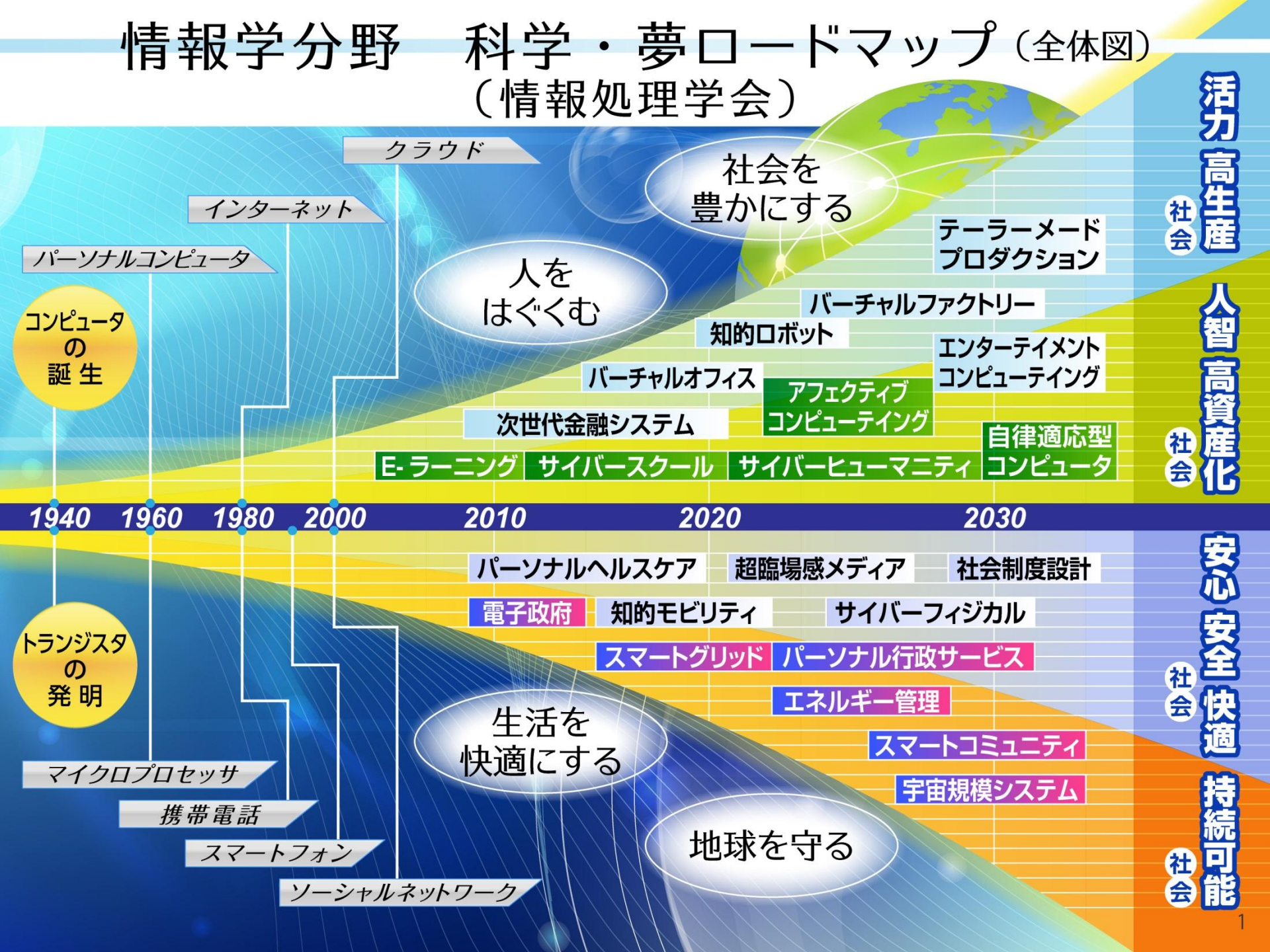
変数 （グループ）	推定値	標準誤差	Z値	P値
D(基準)	−3.258	1.019	−3.199	0.00138
A(催促文言)	1.923	1.136	1.693	0.09044
B(失礼画像)	2.277	1.125	2.023	0.04304 （95%有意）
C(低監視)	2.883	1.091	2.642	0.00824 （99%有意）

グループA，B，Cのオッズ比は
6.84倍，9.75倍，17.9倍 (不正をしやすい)

サイバーセキュリティの未来

ビッグデータとプライバシー

情報学分野　科学・夢ロードマップ（全体図）
（情報処理学会）



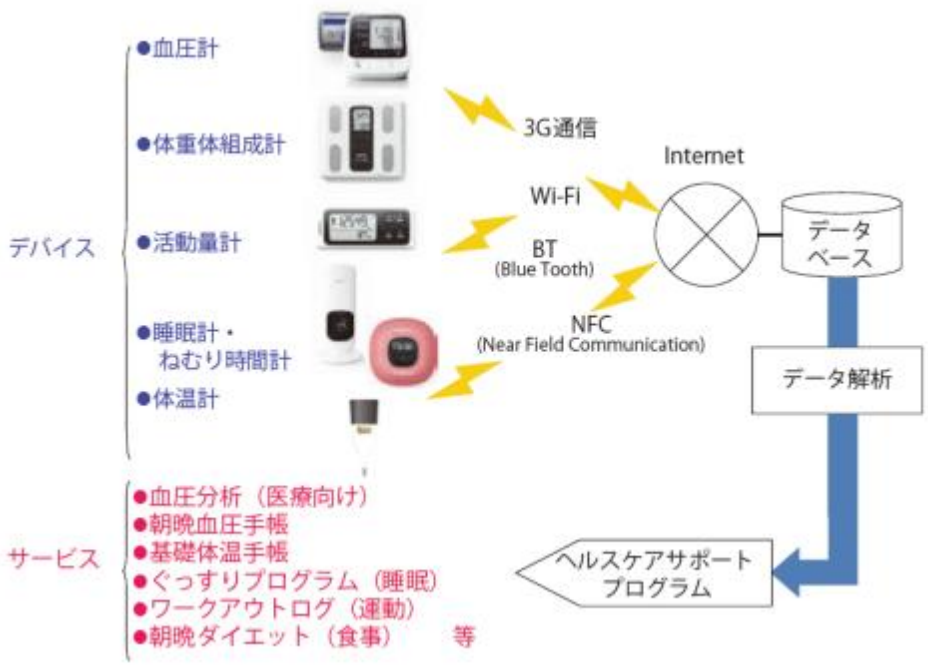
安心安全快適社会

	2010	2020	2030
パーソナルヘルスケア	カルテ（健康記録、診療記録）の電子化	医療データベースの病院間相互運用	健康記録、医療記録を自己管理 PHR(Personal Health Record) の実現
高齢化対策	遠隔見守り（家電製品とインターネットでの受動的な安否確認）の普及	介護福祉ロボット（介護やリハビリを受動的に支援）	介護エージェント（自律したロボットによる人手不要の介護や医療）
高度情報化交通システム	混雑状況などのセンシングと渋滞予測研究	安全運転支援（事故多発地点の同定と運転中注意喚起）の普及	無人自動運転の実現
サイバーセキュリティ	不正アクセスの早期検出・警告	トレースバック技術（攻撃先の追跡）の実用化	不正アクセスの完全防止、スパム撲滅
プライバシー	共通番号制度（年金、社会保障、納税のIDを共通化）の導入	匿名化措置されたデータの流通・活用	プライバシー保護データマイニング（個人情報を秘匿したままでパーソナライズサービスを実現）の実用化

パーソナルヘルスケア

- 超高齢化社会
  - 65歳以上が20%超.
- 生活習慣病
  - 運動・食事・睡眠
  - 病院ではなく，日常生活の中で計測

- センサーとサービス



中嶋宏，「生活習慣改善の継続支援技術」，情報処理 Vol. 56, 2015.

What is personal data

- The Data Protection Act 1988 (DPA)
  - Data which relate to a living individual who can be identified
  - (a) from those data,
    or
  - (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller of any other person in respect of the individual

高崎晴夫,「個人情報保護に係る法制度をめぐるEUの状況」, 情報処理, Vol. 55, 2014.

1. 欧州の動向

- EU一般データ保護規制案
  - 1995年のEUデータ保護指令の改正
  - 2014 LIBE委員会
    - （Civil Liberties, Justice and home affairs)
  - 法的拘束力の強化（「指令directive」から「規制regulation」へ.
  - 個人情報の拡大
    - 生体データ, 遺伝的データ, 健康データ
    - 仮名化データ (pseudonymised), プロファイリング
  - データ主体の権利の強化
    - 忘れられる権利, 削除権
    - プロファイリングへの異議申し立て

石井夏生利,「アメリカのプライバシー保護に関する動向」, 情報処理, Vol. 55, 2014.

2. 米国の動向

- 2012年消費者プライバシー権利章典
  - FTC法執行権限, 国際的相互運用性
- FTCレポート
  - Privacy by Design (PbD), 透明性, 教育目的収集の徹底, 差別阻止,
- データブローカー
  - Acxiom, busted in など, 個人データ収集やプロファイリングが合法的なビジネス.

3. 日本の動向.

- 2015年2月18日 「閣議決定案」
- 個人情報の定義
  - 現行法にもどる（特定の個人を識別出来る情報）
- 利用目的の変更禁じ
- 匿名加工情報
  - 届け出不要. 他の情報と照合は禁止

個人情報の範囲の明確化

保護法改正のポイント

- 1. 個人情報の定義の明確化
  - 個人識別符号（第2条2項），要配慮個人情報（第2条3項）
- 2. 個人情報の有用性確保
  - 匿名加工情報（第2条9項）
  - 認定個人情報保護団体による個人情報保護指針（第53条）
- 3. 個人情報の保護を強化
  - 個人情報データベース等提供罪（第83条）
- 4. 個人情報保護委員会の新設と権限
  - 新設（第5章）
- 5. 個人情報の取り扱いのグローバル化
  - 国境を越えた適用（第75条），外国執行局への情報提供（第24条）
- 6. オプトアウトなど
  - 届出厳格化（第23条2項），利用目的の変更禁止（第15条2項）

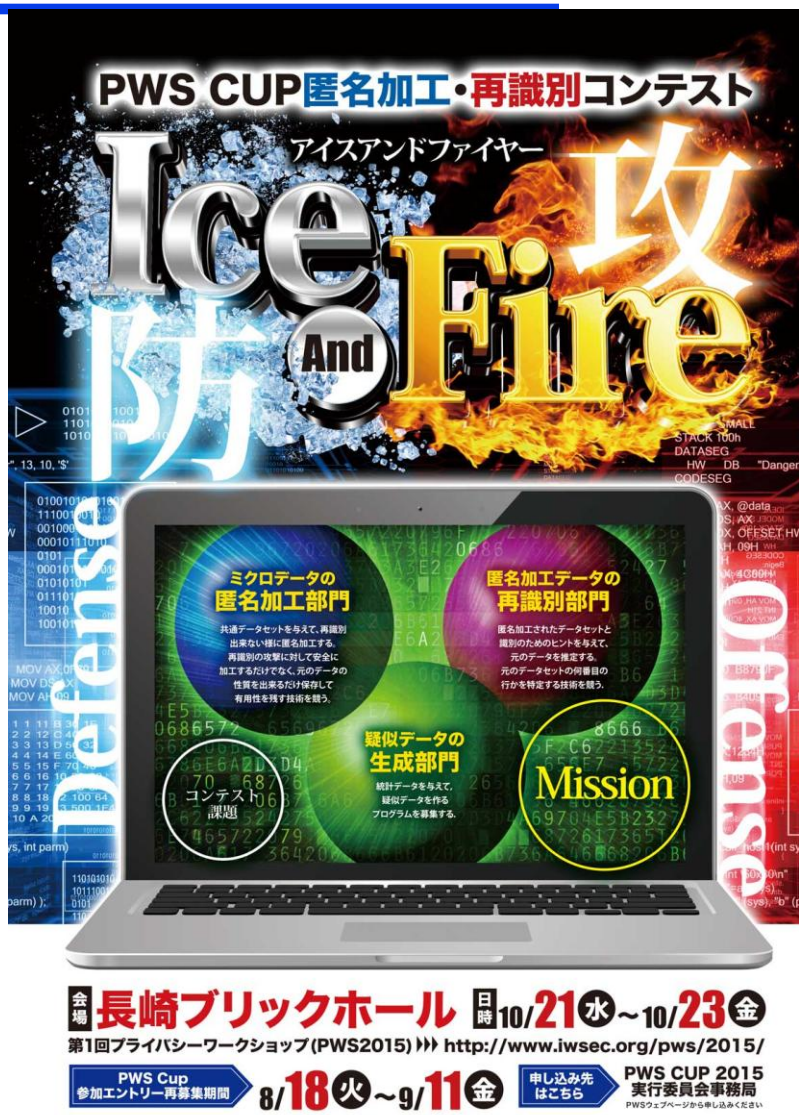
課題

- 匿名加工の方法
  - 個人情報保護指針？k-匿名が必要か？kはいくらか？ℓ-多様性は？t-近似性は？差分プライバシー
  - 有用性と安全性のトレードオフ
- リスクと安全性の評価
  - 誰が評価するのか？個人情報保護委員会？認定個人情報保護団体？
- 加工方法やリスクのデータ依存
  - 個人情報データを提供してくれない
  - 研究者ごとに都合のいいデータ利用

匿名加工・再識別コンテスト

- 第一回PWSCUP 2015
  - 2015年10月21日，22日
  - 長崎ブリックホール
  - 情報処理学会CSEC研究会PWS実行委員会主催
  - 企業・大学17チーム，81名参加申し込み．
  - 本戦: 13チーム20名．

参加エントリー	8/18～9/11
予備戦（匿名加工）	8/24～9/24
予備戦（再識別）	9/25～10/9
本戦	10/21 2時間

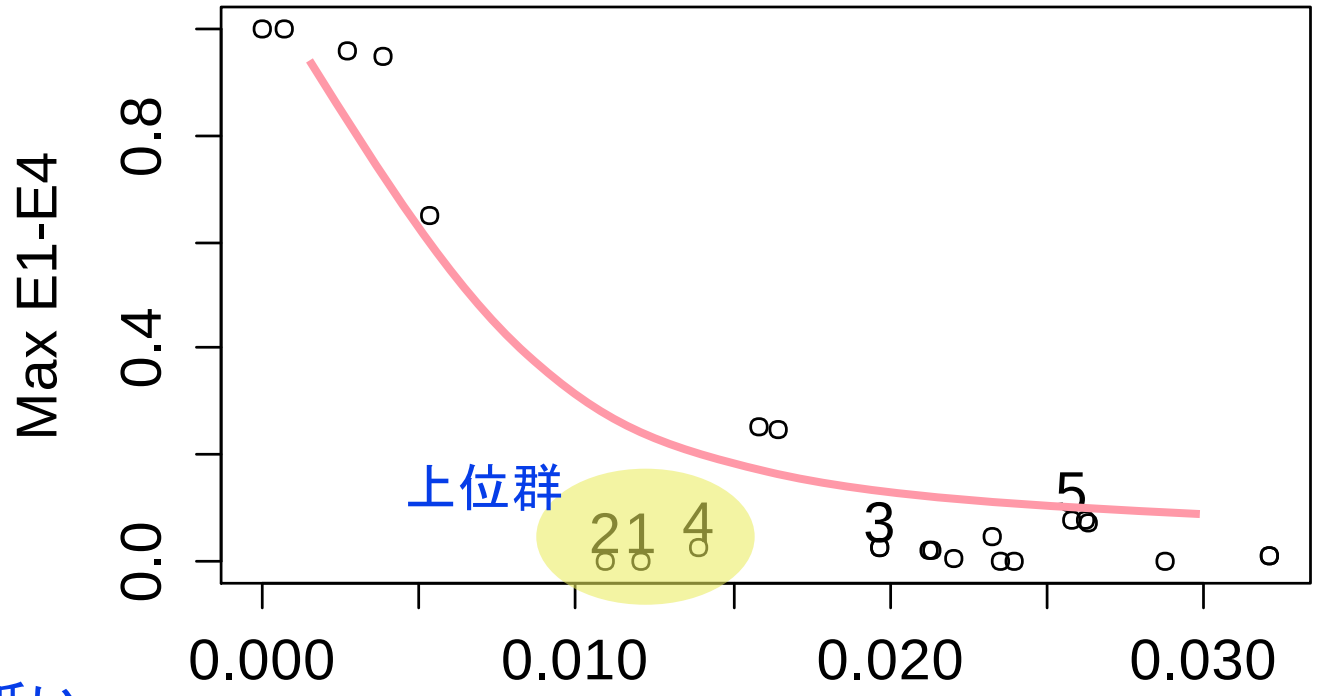


有用性Uと安全性Eのトレードオフ

危険
再識別率高

安全性
（再識別率）

安全
再識別率低い



小さな加工
有用性高い

U5
有用性

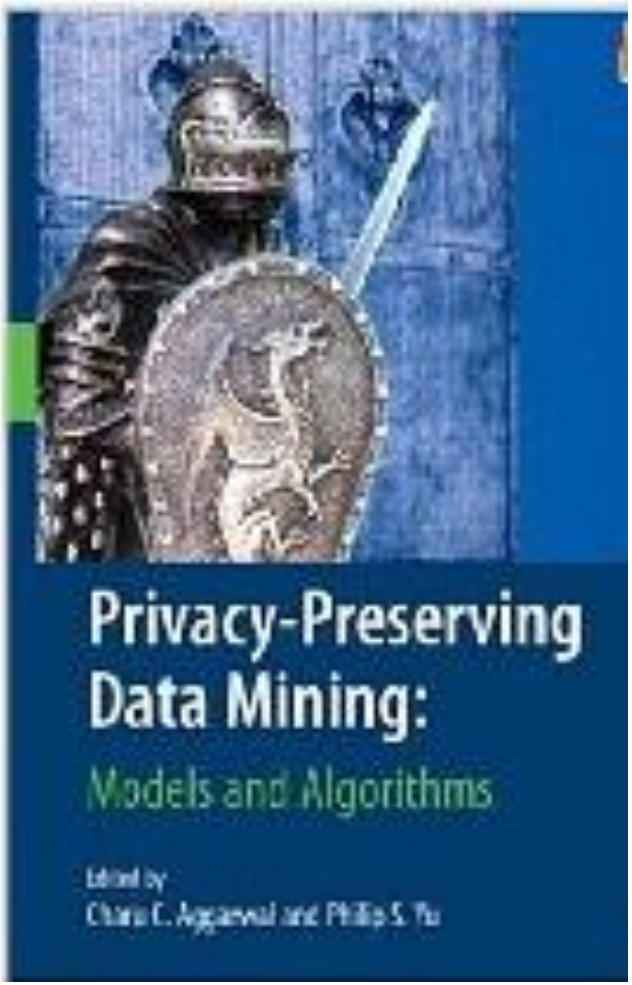
大きな加工
有用性低い

Privacy-Preserving Data Mining

- Privacy-Preserving Data Mining: Models and Algorithms

  By Charu C. Aggarwal , Philip S. Yu, Springer, 2009.

- 準同型性などの高機能暗号を応用した精度も安全性も高いプロトコル
  - 改正法の匿名加工情報とはみなされない.



NICTに期待すること

国立研究法人

- 目的(抜粋)
  - 一定の自主性を発揮しつつ、中長期的な視点に立って執行することが求められる科学技術に関する試験、研究又は開発に係る
  - 我が国における科学技術の水準の向上を通じた国民経済の健全な発展その他の公益に資する
  - 研究開発の最大限の成果を確保

（独立行政法人通則法の一部を改正する法律）

NICTにやって欲しい研究

- 1. 危険性があり教育機関などでは困難になってきた研究
  - honeypot, 人を使う実証実験，長期間の観測を要するセキュリティ疫学研究
- 2. 我が国における科学技術の水準を誇る最先端の研究
  - 世界記録の樹立，トップカンファレンス
- 3. （もうからないけど公益に資する）誰もが欲するが誰もやらない研究
  - 標準化，異分野間の統合，研究データの提供，ライブラリの公開

NICTにやって欲しくない研究

- Googleがやっている研究（およびその真似）
- 民業圧迫になる研究，特定の企業が資する研究
- （応用が見えない）研究のための研究
- 机上の空論，荒唐無稽な研究
- （他の組織が真似をしては困る様な）プライバシーの配慮が足りない研究

大阪ステーションシティ顔認証

- 実験概要
  - 2014年4月から2年間
    (2013年11月25日プレスリリース)
  - 大阪駅ビル構内92台のカメラ
  - 独立行政法人 情報通信研究機構 NICT
  - 目的：大規模災害時の避難誘導の目的
  - 顔認証，歩容認証など
  - 加工データをJR西日本に提供予定（第三者提供）

朝日新聞 2014年1月6日

多くの反発

- 反論
  - 「監視社会を拒否する会」3月5日
  - 「共通番号制と監視社会化に反対する北摂市民ネットワーク」
- NICTの対応
  - 3月11日実験は延期.
  - 4月1日第三者委員会の設置

朝日新聞 2014年3月5日夕刊

反対派の主な主張

- 憲法13条 プライバシー権（自己情報コントール権）の侵害
  - 「承諾なしにみだりに容貌・姿態を撮影されない自由を有する」（1969年最高裁）
- 実験の方法やデータの利用目的が不明確
  - 秘密裏に実験が行われる懸念．公共空間をまるごと実験区域にし，承諾なしに実験対象とするのは人権侵害だ．
- 顔のデータは個人情報ではないか（個人情報保護法）
  - 「元の映像が復元できない情報に置き換えるので個人情報ではない」というが一方的だ．

第三者委員会の報告

- プライバシー権は侵害しているが，利益衡量の点で，実質的な侵害はない．
- レピューテーションリスクを考慮して，利用者への説明が不足している．
- 人流統計情報は，個人識別性が十分に低減している（していなくても低減することは容易）
- 一度取得した個人情報を速やかに消去したら，保有個人情報の義務を免れるのか．映像情報消去後の特徴量情報は識別比特定情報

第三者委員会からの提言

1. 実験手順や実施状況等を定期的に確認し公表すること．決められた手続きに従っているか確認不能．
2. 個人識別のリスクを市民に対して事前に説明すること
3. 撮影を回避する手段を設けること．

例） 実験場所を分割し，実験を拒否するが通過するエリアを用意

4. 映像センサーの存在と稼働の有無を利用者に一目瞭然にすること

例）センサーに実験名称の看板，非稼働にはカバー．

5. 人流統計情報の提供に際しては委託契約又は共同研究契約を締結すること
6. 安全管理措置を徹底すること
7. 本実証実験に関して適切な広報を行うこと

例）実験の実態に即した展示ブースの設置

NICT殿へ（まとめ）

- 現在，サイバーセキュリティの攻撃は多様化，深刻化しており，社会的な影響も大きい
- 短期的には，侵入を完全に阻止するのだけでなく，侵入を想定した対策を考えよ
- 長期的には，法整備を行い，より安全な暗号技術の応用の時代に備えよ
- 独立研究機関としての任務を自覚し，我が国の水準を高める研究を率先せよ.
- プライバシー権や個人情報保護法への配慮を行い，利用者への啓蒙を進めてセキュリティ技術の普及を務めよ.