

ITセキュリティ法制とデジタル・フォレンジック

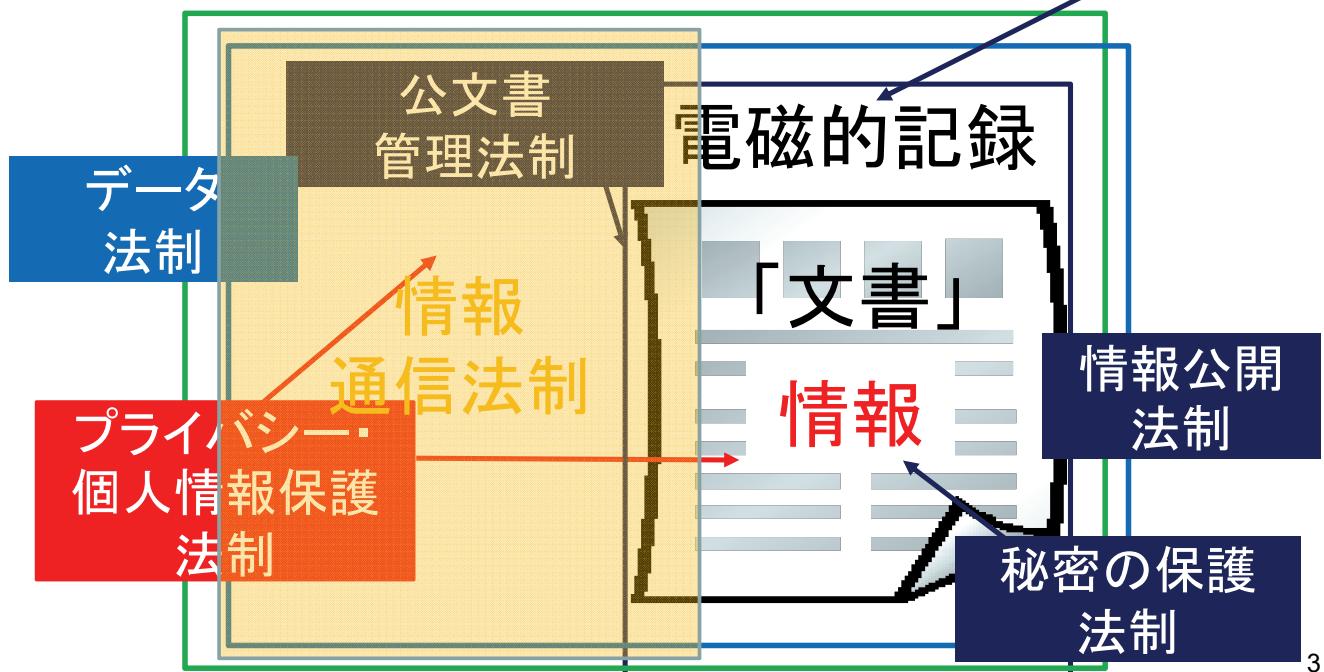
湯淺 墾道
情報セキュリティ大学院大学 教授
デジタル・フォレンジック研究会 理事

IDF第16期総会時講演会 2019年5月10日(金)

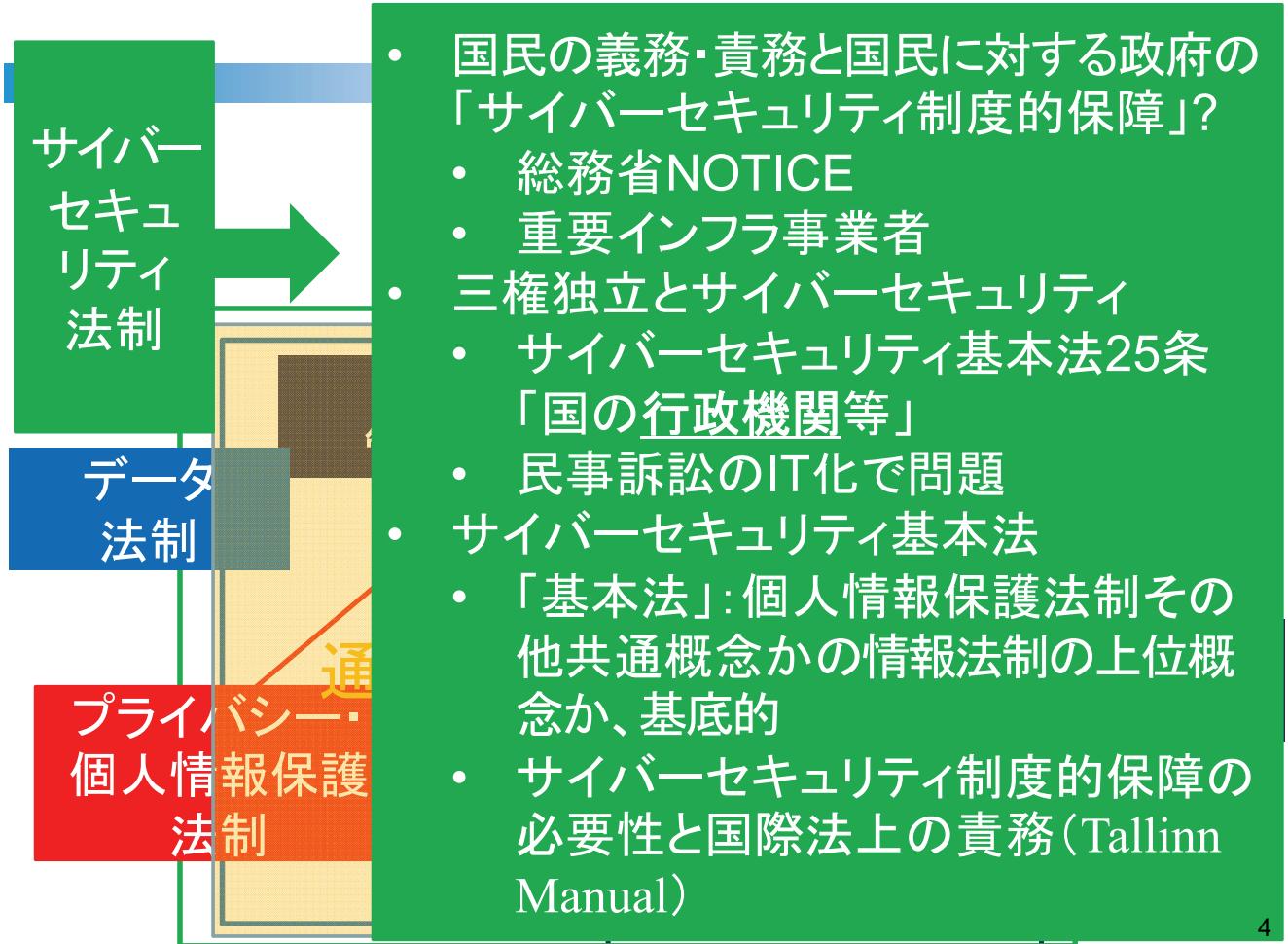
1

セキュリティに関する法の動き

刑事法
民事法



3



4

IoTセキュリティとデジタル・フォレンジック

5

NICT法改正

- 電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律
 - 「国立研究開発法人情報通信研究機構(以下「機構」という。)は、平成三十六年三月三十一日までの間、特定アクセス行為を行い通信履歴等の電磁的記録を作成すること、特定アクセス行為による電気通信の送信先の電気通信設備に係る電気通信事業者に対し、送信型対電気通信設備サイバー攻撃のおそれへの対処を求める通知を行うこと等の業務を行うこととする。」
- 国立研究開発法人情報通信研究機構法の一部改正
 - 第二条
 - (略)
 - 2 機構は、第十四条及び前項に規定する業務のほか、平成三十六年三月三十一日までの間、次に掲げる業務を行う。
 - 一 特定アクセス行為を行い、通信履歴等の電磁的記録を作成すること。

6

- 機構の端末設備又は自営電気通信設備を送信元とし、アクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信元とする電気通信の送信をおこなう行為であって、当該アクセス制御機能を有する特定電子計算機である電気通信設備に電気通信回線を通じて当該アクセス制御機能にかかる他人の識別符号(当該識別符号について電気通信事業法第52条第1項または第70条第1項第1号の規定により認可を受けた技術的条件において定めている基準を勘案して不正アセス行為から防御するため必要な基準として総務省令で定める基準を満たさないものに限る。)を入力して当該電気通信設備を作動させ、当該アクセス制御機能により制限されている当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備の特定利用をし得る状態にさせる行為をいう。
- 不正アクセス禁止法の定める不正アクセスの構成要件から除外

7

カリフォルニア州IoT セキュリティ法

- カリフォルニア州法
「接続される機器(コネクテッド・デバイス)の
セキュリティに関する法律」
 - 2018年9月制定、2020年1月施行予定
 - インターネットに接続される機器(コネクテッド・デバイス)のセキュリティを規制する
ものとしては全米初の州法
 - コネクテッド・デバイスの製造者に対して、
合理的な(reasonable)セキュリティ機能を
装備させることを義務づけ

8

- 「接続される機器の製造者は、当該機器に次のすべての基準を満たす一の合理的なセキュリティ機能または諸機能を装備しなければならない」
- (1) 機器の性質及び機能に適するもの、(2) 収集し、包有し、又は発信することができる情報に適するもの、及び(3) 機器および機器に含まれる情報を、不正アクセス、破壊、使用、改変または開示から保護するように設計したもの

9

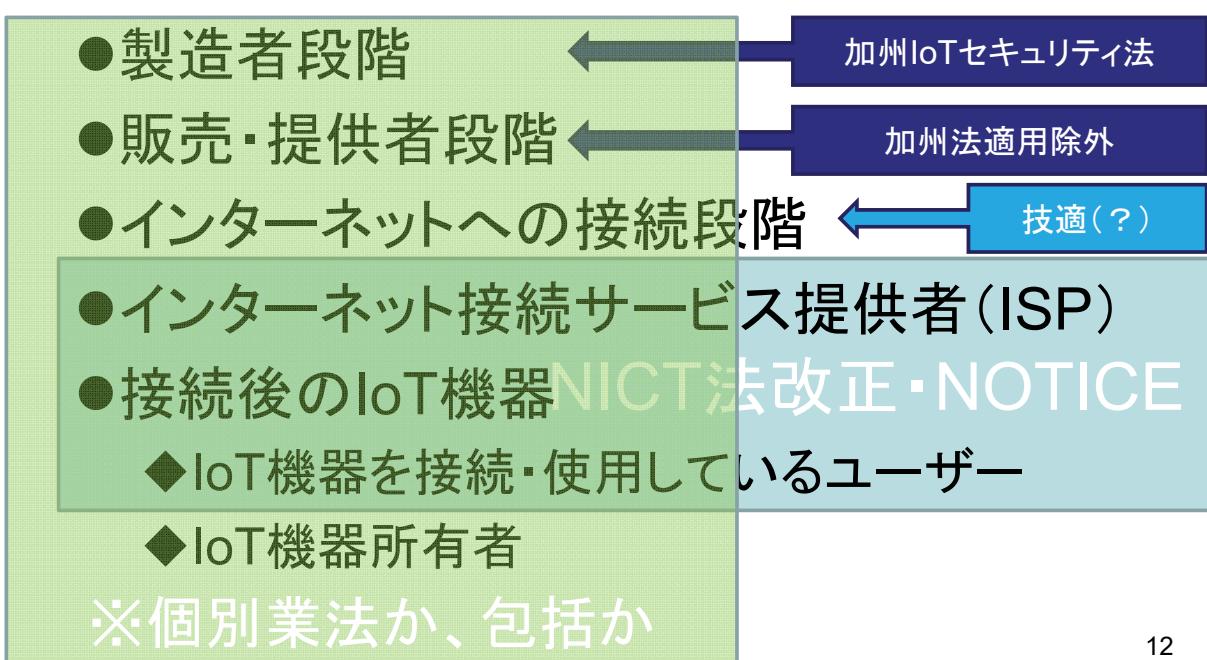
- 接続される機器がローカルエリアネットワークの外部に認証手段を備えている場合、あらかじめプログラムされたパスワードは製造された機器ごとに固有のものであること、または当該機器の初回アクセスが許可される前にユーザーが新しい認証手段を生成しなければならないセキュリティ機能を備えているときには、合理的なセキュリティ機能とみなされる
 - 事業者セーフ・ガード？
 - セキュリティ対策をパスワード対策に矮小化？

10

- 直接又は間接にインターネットに接続することができ、かつ、インターネットプロトコルアドレス又はブルートゥースアドレスを割り当てられた機器その他の物理オブジェクト
- 「その機能性が、その執行権限に従って連邦政府機関により公布された連邦法、規則またはガイダンスに基づくセキュリティ要件の対象となる接続機器には、適用されない」
 - HIPPA法、医療情報の機密保持法規制対象となる場合は適用除外

11

■ IoTセキュリティ法規制のあり方



12

民事訴訟のIT化とデジタル・フォレンジック

13

方向性(とりまとめ骨子案)に関する議論

■ 民事訴訟手続

- ①e提出 (e-Filing)
- ②e法廷 (e-Court)
- ③e事件管理 (e-Case Management)
 - ✓ 3つのeの同時実現か、段階的実現化か

■ 対象

- 民事訴訟
- 破産、家事は今回は見送りの公算
 - ✓ 将来的に破産、家事も視野に入れるか

14

「未来投資戦略2018」

■「未来投資戦略2018」(第2 具体的施策) (P55~56)

- [3]「行政」「インフラ」が変わる
 - ◆ 1. デジタル・ガバメントの実現(行政からの生産性革命)
 - vi) 世界で一番企業が活動しやすい国の実現
 - » ①裁判手続等のIT化の推進

<http://www.kantei.go.jp/jp/singi/keizaisaisei/>

15

■ 司法府による自律的判断を尊重しつつ、民事訴訟に関する裁判手続等の全面IT化の実現を目指すこととし、以下の取組を段階的に行う。

- まずは、現行法の下で、来年度から、司法府には、ウェブ会議等を積極的に活用する争点整理等の試行・運用を開始し、関係者の利便性向上とともに争点整理等の充実を図ることを期待する。

※3つのeの段階的実現を採用

16

- 次に、所要の法整備を行い、関係者の出頭を要しない口頭弁論期日等を実現することとし、平成34年度頃からの新たな制度の開始を目指し、法務省は、来年度中の法制審議会への諮問を視野に入れて速やかに検討・準備を行う。司法府には新たな制度の実現を目指した迅速な取組を期待し、行政府は必要な措置を講ずる。
※実現時期は駆け引き、平成34年度頃に
※行政府が司法府の必要な措置(予算)

17

- さらに、所要の法整備及びシステム構築などの環境整備を行い、オンラインでの申立て等を実現することとし、法務省は、必要な法整備の実現に向け、来年度中の法制審議会への諮問を視野に入れて速やかに検討・準備を行う。※**1年間で法制審議会**
- また、法務省は、オンラインでの申立て等の実現に向けたスケジュールについて、司法府の環境整備に向けた検討・取組を踏まえた上で、**来年度中に**検討を行う。

18

今後のスケジュール

■ 実務者研究会 or WG 最高裁+法務省+日弁連?

■ 法制審議会 通常は2年以上

■ システム設計、実装 通常は2年以上

再生会議事務局は3年めどを期待



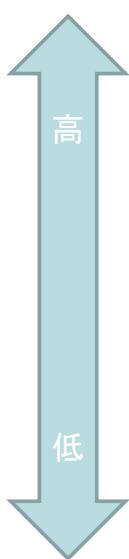
【選択肢】

- ・ 法改正を必要としない電子化
- ・ 民事訴訟法の改正または裁判手続等のIT化に係る特別法の制定

19

機密性

■ 民事裁判に係る諸情報の機密性



- 作成途中の裁判官の判決文、メモ等
 - » 裁判官同士の評議の秘密(裁判所法75条)
- 証拠
 - » 知的財産、営業秘密等に係る情報
 - » 原告・被告の利益に係る情報
- 非公開で行われた審理の書類
- 個人情報、プライバシー情報(戸籍や住民票、送達関係書類)
- 訴訟記録(閲覧等制限あり)
 - » 謄写は当事者と利害関係人のみが可
- 訴訟記録(閲覧等制限なし)

20

完全性

■ 民事裁判に係る諸情報の完全性

- 改ざん、否認、滅失等の防止
- なりすましの防止
 - ◆ 本人確認とアクセス権限
 - ◆ 原告・被告
 - ▶ 法人や団体の場合
 - ◆ 代理人
 - ▶ 事務所単位か代理人単位か
 - ◆ 訴訟代理権の電子的確認(?)

21

可用性

■ サイバー攻撃

- 裁判の電子化システム
- 当事者

■ 海外からアクセスする場合

- 当該国政府によるブロッキング

22

証拠の電子化

- 裁判所に提出段階になって原本データ 자체を極めて精巧に編集することを可能とし、かつ、現行の弁論等での原本確認の手続も困難
- 改ざん証拠の提出を容易にする(改ざん発見を困難にする)温床となるおそれ
- 提出証拠の原本自体が改変・事後創出の恐れ
- 真実擬制、過料制裁

23

- データを一旦印刷したものを、PDF化したデータ
- インシデント当時に記録されたメタデータが全くないデータ



- メタ情報の焼き直しであり証拠価値が低い
- 改ざん等の立証が必要と考える当事者
 - メタ情報等を活用してデジタル・フォレンジック

24

- 訴訟手続の電子化に伴い原本が電子データ(電磁的記録)の場合にそれがオンラインで証拠として提出されることも想定されるが、証拠の電子データの取扱いについては慎重な検討が必要である。電子データは改ざんを行うことも可能となることから、原本確認については紙の場合と異なり、テキストだけではなく、メタデータ、ログ情報やバックアップ・データとの照合などデジタル・フォレンジックの技術を用いた運用が必要となる。この運用は、「経済社会一般で通用しているIT技術や電子情報に対する信頼性、社会認識等を前提とする制度設計」(12頁5~6行目)に不可欠であると同時に、「行政機関や民間の取引におけるセキュリティ水準と同程度」(12頁2~3行目)の水準にとどまるもので、極めて高度かつ厳格なセキュリティを課すものではない。また、刑事訴訟においては、証拠取り調べにおいて鑑定制度を通じデジタル・フォレンジックが運用されているところであり、民事訴訟の原本確認のあり方について検討する際には参考となると考えられる。

25

フェイクニュース・虚偽情報流布と デジタル・フォレンジック

26

在外選挙へのインター ネット投票導入

- 投票環境の向上方策等に関する研究会における検討
 - 次回参議院議員選挙
 - ◆少なくとも実現を目指として現実的 possibility を検討
 - 前提
 - ◆マイナンバーカードの海外利用
 - 現時点で最も現実的な電子的本人確認手段
 - 法制度改正が前提
 - ◆既存の投票方式と併用
 - ◆各地方公共団体が独自設置するのではなく集中方式
 - ただし現行法を前提という制約

27

選挙セキュリティ

- “Election Security”
 - 第1段階
 - 有権者の民意形成への介入と世論誘導によって選挙結果に影響を与えるとする段階
 - 政党、候補者へのサイバー攻撃と情報の暴露
 - フェイクニュース、個人情報を利用したマイクロターゲティング
 - 第2段階
 - 投票所を案内したり開票結果を公表したりする選挙管理機関のウェブサイトへの攻撃や選挙に関するニュースサイトへの攻撃等によって選挙に混乱をもたらそうとする段階
 - 第3段階
 - 選挙管理機関へのサイバー攻撃や電子投票機へのサイバー攻撃等によって有権者名簿や投票記録それ自体を改ざんする等、直接的に選挙結果を操作しようとする段階

28

フェイクニュースとサイバーセキュリティ

■ 谷脇康彦『サイバーセキュリティ』(岩波新書、2018年)148-149頁

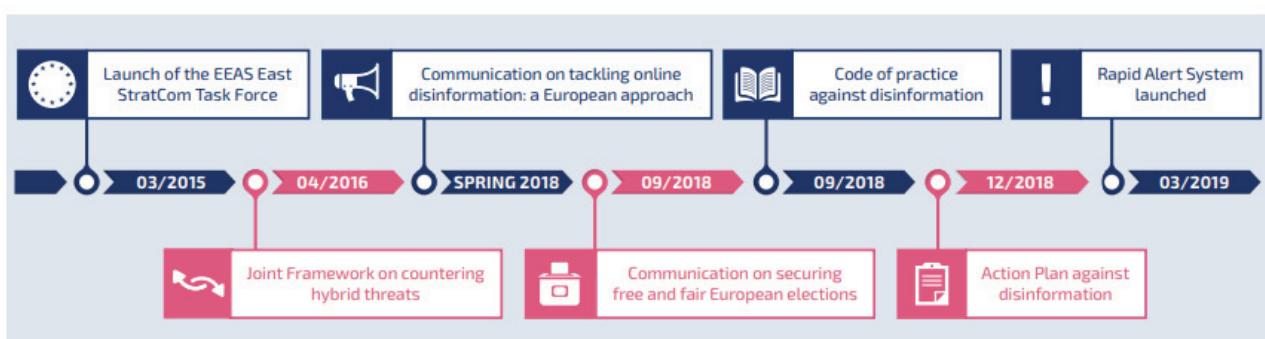
- 「ネット上の偽(フェイク)ニュースをめぐる議論がますます深刻化しています。(中略)こうした情報資産のCIAを確保するという視点からみると、情報の完全性が悪意をもって操作される、つまり偽情報が拡散される状況はサイバーセキュリティが確保されていない状況といえます。このため、情報の完全性を破り、偽情報を意図的に流通させる行為も広い意味でサイバー攻撃であり、その対策に関する議論もサイバーセキュリティ政策の射程に入ってくるものととらえることができます。」

29

フェイクニュース

■ EU

- Disinformation対策
- SNS、プラットフォーマーに対して自主規制要求



● Action Plan against Disinformation

フェイクの検証にデジタル・フォレンジック技術を活用(動画・画像フォレンジック、データの改ざんフォレンジック等)



<https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation>

31

■ アメリカ

- 国土安全部 選挙システムの重要インフラ指定(2017年1月)
- 大統領令「合衆国選挙における海外からの介入に際する制裁に関する大統領令」
Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election (2018年9月)
 - ◆ 法執行機関と情報機関の協力
 - ◆ 選挙後、45日以内に介入について調査
 - ◆ 介入が認められた場合は制裁

32

■ 大統領令第8条

- 「外国からの干渉」
- 「選挙に関し、外国政府又は外国政府の代理人若しくは代理として行動する者の隠ぺい的、詐欺的、欺瞞的若しくは不法な行為又は企てであって、選挙への影響、選挙の結果若しくは報告の結果に対する信頼を傷つけ、若しくは変更し、又は選挙の過程若しくは制度に対する国民の信頼を損なう目的若しくは効果を有するものを含む。」
 - ◆「影響」「変更」「効果」の検証に、デジタル・フォレンジック技術も活用

33

限定提供データとデジタル・フォレンジック

限定提供データ

■ 改正不正競争防止法(令和元年7月施行)

- ビッグデータ時代を念頭に営業秘密に該当しない一定のデータについても法的保護
 - ◆例:
 - 自動走行用の地図データ(ダイナミック・マップ)
 - センサから収集したデータを分析・加工したデータ
- ID・パスワードなどの技術的な管理を施して提供されるデータ(限定提供データ)を不正に取得・使用等する行為を禁止
- 無権限者に不正に取得・使用・提供された場合の法的救済(差し止め)

デジタル・フォレンジックの利活用

35

AIフォレンジックの必要性と課題

例：自動運転

- テスラ 2016年5月7日にフロリダ州で事故、初の自動運転中の死亡事故
- 「テスラ Model S」の運転者（ジョシュア・ブラウン）が、トレーラートラックと衝突して死亡



<https://www.ntsb.gov/investigations/AccidentReports/Pages/HWY16FH018-preliminary.aspx>

37

- 事故原因をNTSB（国家運輸安全委員会）が調査



<https://www.ntsb.gov/investigations/AccidentReports/Pages/HWY16FH018-preliminary.aspx>

38

Facebookの場合

■ Transcript of Mark Zuckerberg's hearing, Commerce and Judiciary committees U.S. Senate, April 10, 2018.

- FLAKE: There are obviously limits, you know, native speakers that you can hire or people that have eyes on the page. Artificial intelligence is going to have to take the bulk of this. How — how much are you investing in working on — on that tool to — to do what, really, we don't have or can't hire enough people to do?
- ZUCKERBERG: Senator, I think you're absolutely right that over the long term, **building A.I. tools is going to be the scalable way to identify and root out most of this harmful content.** We're investing a lot in doing that, as well as scaling up the number of people who are doing content review.

39

- AIによるフェイクニュースの生成・発信
- AIによるフェイクニュースの効果的な流布(流布先・流布方法分析を含む)
- AIによる個人の政治的 意思形成や投票行動の代理・代行

- AIによるフェイクニュースの検知
- AIによるフェイクニュースのアトリビューション、流布対象者の検知と通知
- AIによって誘導された 政治的 意思や投票行動の検知

AIの利活用が多方面で本格化
AIの判断過程のフォレンジックの必要性が高まる

40