

JCA-NET セミナー

2020/8/28

小倉利丸

toshi@jca.apc.org

目次

- ブラウザの設定を見直す
 - 検索エンジン
 - プライバシー関連の設定
 - スマホの設定を見直す（広告 ID のリセット）
- ブラウザそのものを変更する
 - Tor ブラウザ

目次（続）

- ブラウザは私たちの行動をどのように把握するのか
- なりすましメール（フィッシング詐欺メール）対策
- メールのプライバシー——暗号化メールサービスを使う
 - Protonmail
 - Tutanota

- ⚠ リスクの可能性のある場所
- 👮 捜査機関などによるアクセス
- 👮 プロバイダー、企業などによる個人情報収集・追跡
- 👤 違法なアクセス(ハッキング、マルウェア)

送信者アリス

- ボブにメールを送信
- ネットショッピング
- 検索サイトで調べ物
- SNSを使う
- 捜査機関による検索・押収

受信者ボブ

- アリスからメールを受信

ボブの契約プロバイダー

- 受信メールはサーバに保存
- サーバ管理者はメールにアクセスできる
- 捜査機関等がプロバイダーに対して任意・令状で情報提供を求める。

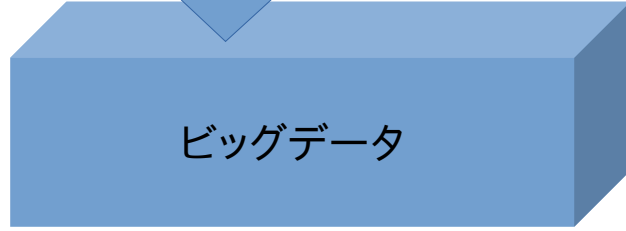
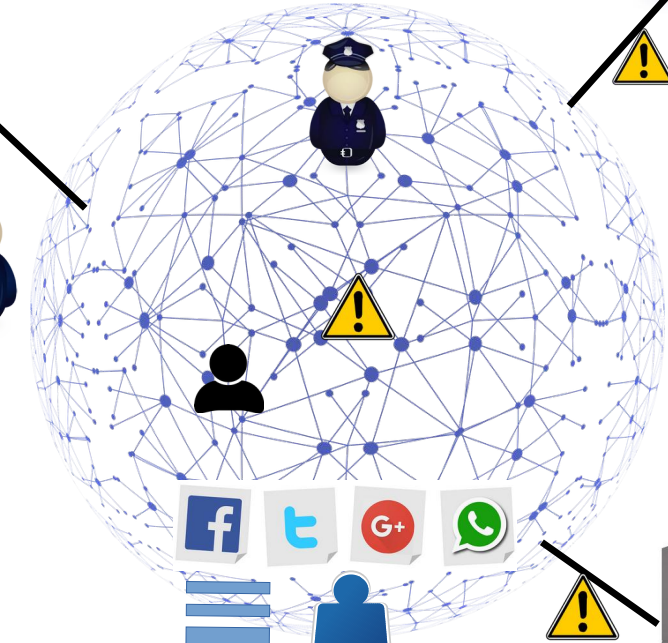
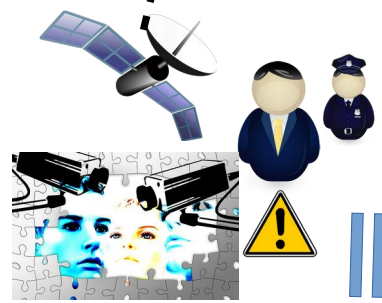
アリスがアクセスするショッピングサイト、検索サイト、SNSサイト

- クッキーやログ情報
- 行動追跡
- 履歴の蓄積と分析
- 支払い関連の個人情報
- 検索行動の追跡
- スマホ電話帳、広告ID、カメラ情報など
- アプリ連携
- アンケートなど
- 捜査機関等が任意・令状で情報提供を求める。

アリスの契約プロバイダー

- いつ誰にメールを送信したのかなどネットアクセスログ
- アリスの契約関連個人情報
- 捜査機関等がプロバイダーに対して任意・令状で情報提供を求める。

**GPS
監視
カメラ**



連携企業など

- 金融機関
- データ解析会社
- 広告スポンサーなど

ブラウザの設定を見直す

- 検索エンジン

- google 検索を使わない
- 検索ユーザーを追跡しない検索エンジンを選択する
 - DuckDuckGo <https://duckduckgo.com/>



ブラウザの設定を見直す

- 検索エンジン



**私たちはあなたの個人情報を保存
しません。絶対に。**

私たちのプライバシーポリシーはシンプルです。ユーザーの情報収集は一切致しません。

**私たちはあなたを広告で追跡しま
せん。**

私たちは、あなたの検索履歴を保存しません。したがって、インターネット経由であなたを追跡して、それを広告主に販売することはありません。

**私たちは、プライベートブラウジ
ングモードでも、それ以外でも、
あなたを追跡しません。**

他社の検索エンジンはあなたの検索をプライベートブラウジングでも追跡しています。私たちは追跡しません。

• DuckDuckGo のインストール方法



a) DuckDuckGo のサイトにアクセス
b) 右上の「プライバシー保護をシンプルに」をクリックすると左のようなメニューが表示される

c) 「アプリと拡張機能入手」をクリック

d) 下図のようなページにとぶので、使っているブラウザ（自動表示サレマス）を選択するかスマホアプリサイトを選択してインストール



ブラウザの設定を見直す

- プライバシー関連の設定
 - Google 関連のサービスを停止する
 - 位置情報を使わない
 - クッキーやキャッシュを定期的に消去する
 - 内蔵のカメラは物理的に塞いでおく。(レンズにカバー)

ブラウザの設定を見直す

そもそもブラウザは何をしているのか？

「毎年開かれるデベロッパーカンファレンスで、米国時間5月7日、Googleはプライバシー保護に関する2つの機能の追加を明らかにした。1つはクッキーのコントロールによって、広告業者がウェブサイトをまたいでユーザーの行動をトラッキングすることを制限する機能。もう1つは新しいフィンガープリント対策だ。」

<https://jp.techcrunch.com/2019/05/11/2019-05-07-chrome-privacy-security-changes/>

ブラウザの設定を見直す

- クッキー

- ユーザーのコンピュータやデバイスにファイルとして保存される小さな情報
- ウェブサイトやアプリは、ユーザーが誰なのかを特定できる。
- ユーザーにとっては、ウェブサイトにログインしたままの状態にしておくことができるので便利
- そのサイト上のユーザーの行動を追跡するのに利用されることもある
- 異なるウェブサイト間で動作するものもあり、ユーザーのウェブサイト間の移動を追跡する
- ユーザーがどこに行ってどこを訪問したか、といったプロフィールを構築することも可能になる

ブラウザの設定を見直す

- フィンガープリント（指紋）
 - ウェブサイトや広告業者が、ユーザーが使っている**ブラウザに関する情報**をできるだけ詳しく収集するための手法
 - 使用しているプラグインや機能拡張から、動作してるデバイスについては、そのメーカー、モデル、画面の解像度などの情報も対象となる
 - そうした情報を集めて、**ユーザーごとに異なるデバイスの「指紋」**として採取するのだ
 - クッキーを使っていないので、ユーザーがシークレットモードやプライベートブラウズ機能を利用していても、ウェブサイトはブラウザのフィンガープリントを見ることができる

ブラウザの設定を見直す

- Google をビジネスに使っている企業はどのようなことができちゃうのか。

<https://www.youtube.com/watch?v=e0tVGxuIeG8>

- 消費者対象のビジネスから「有権者」に対する政治権力による意識操作へ

企業が顧客のニーズや行動を予測したり、行動を誘導する技術はそのまま政府や捜査機関などが利用可能な技術でもある

- ブラウザを通じて政府サイトにアクセス
- SNS での情報発信

ブラウザの設定を見直す

個人情報との繋がり

- 長期にわたって変化しない個人情報
 - 名前 住所 電話番号 生年月日
- 携帯端末の機器特定の情報
 - International Mobile Subscriber Identity (IMSI) 番号：携帯電話会社によってユーザーに割り当てられ、SIMカードに保存
 - モバイルデバイスには、ハードウェアに「焼き付けられた」IMEI (International Mobile Equipment Identity) 番号

ブラウザの設定を見直す

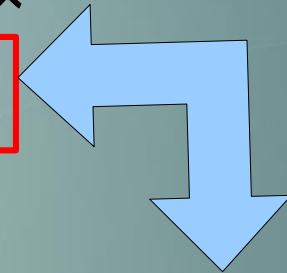
個人情報との繋がり

- 長期にわたって変化しない個人情報

- 名前 住所 電話番号 生年月日

- 携帯端末の機器特定の情報

- International Mobile Subscriber Identity (IMSI) 番号：携帯電話会社によってユーザーに割り当てられ、SIMカードに保存
- モバイルデバイスには、ハードウェアに「焼き付けられた」IMEI (International Mobile Equipment Identity) 番号



より匿名性の高いブラウザ

- Tor ブラウザ

<https://www.torproject.org/>



Donate Now

[About](#) [Documentation](#) [Support](#) [Community](#) [Blog](#) [Donate](#)

English (en) ▾

Download Tor Browser ↓

Browse Privately.
Explore Freely.

Defend yourself against tracking and surveillance. Circumvent censorship.

Download Tor Browser ↓

より匿名性の高いブラウザ

- Tor ブラウザ

<https://www.torproject.org/>



Download for Windows

Signature ⓘ



Download for OS X

Signature ⓘ



Download for Linux

Signature ⓘ



Download for Android

[Download in another language or platform](#)

[Download the latest alpha build](#)

[Download Tor Source Code](#)

上記のリンク先から日本語版を選択してインストールます。

なりすましメール（フィッシング詐欺メール）対策

情報処理推進機構の調査では「フィッシングによる個人情報等の詐取」が脅威の2位

<https://www.ipa.go.jp/security/vuln/10threats2019.html>

フィッシング対策協議会

<https://www.antiphishing.jp/>

利用者向けフィッシング詐欺対策ガイドライン

https://www.antiphishing.jp/report/pdf/consumer_antiphishing_guideline.pdf

いったん詐取された個人情報を奪い返す方法はありません。

なりすましメール（フィッシング詐欺メール）対策

フィッシングメールの例

JCA-NET を装ったメール

メールのヘッダ

From: "jca.apc.org" <info@taosolutions.co.jp>
To: xxxxxxxx@jca.apc.org
Date: Wed, 26 Aug 2020 11:25:07 +0000
Subject: 【バージョンアップ】メンテナンス作業のお知らせ

なりすましメール（フィッシング詐欺メール）対策

フィッシングメールの例

メール本文（一部）

平素は【 jca.apc.org 】インターネットサービスをご利用いただき誠にありがとうございます。

サーバーのメンテナンスを実施しています。

以下のリンクに従ってサービスをアップグレードしてください

（中略）

Copyright (C) Jca Co.,Ltd. All Rights Reserved

なりすましメール（フィッシング詐欺メール）対策

- ショッピングサイトの場合は、メール本文のリンクではなくブラウザからユーザログインして確認する
- 自分の名前がきちんと明記されていない場合はフィッシングメールと判断してよい
- メール本文にある会社のロゴ、住所などは信用してはいけない

送信者アリス

- ボブにメールを送信
- ネットショッピング
- 検索サイトで調べ物
- SNSを使う
- 捜査機関による検索・押収

- ⚠ リスクの可能性のある場所
- 👮 捜査機関などによるアクセス
- 👤 プロバイダー、企業などによる個人情報収集・追跡
- 👤 違法なアクセス(ハッキング、マルウェア)

受信者ボブ

- アリスからメールを受信

ボブの契約プロバイダー

- 受信メールはサーバに保存
- サーバ管理者はメールにアクセスできる
- 捜査機関等がプロバイダーに対して任意・令状で情報提供を求める。

アリスがアクセスする
ショッピングサイト、検索サイト、SNSサイト

- クッキーやログ情報
- 行動追跡
- 履歴の蓄積と分析
- 支払い関連の個人情報
- 検索行動の追跡
- スマホ電話帳、広告ID、カメラ情報など
- アプリ連携
- アンケートなど
- 捜査機関等が任意・令状で情報提供を求める。

アリスの契約プロバイダー

- いつ誰にメールを送信したのかなどネットアクセスログ
- アリスの契約関連個人情報
- 捜査機関等がプロバイダーに対して任意・令状で情報提供を求める。

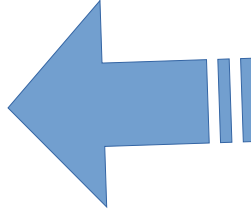
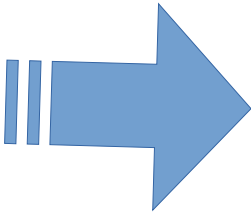
**GPS
監視
カメラ**



ビッグデータ

連携企業など

- 金融機関
- データ解析会社
- 広告スポンサーなど



メールのプライバシー—暗号化 メールサービスを使う

メールは「葉書」のようなもの。

サーバーに保管されたメールは第三者によって
閲覧されるリスクがある

- メールサーバと送受信が暗号化されているサービス
を使う
- 信頼できるメールサービスを使う
- Protonmail <https://protonmail.com/jp/>
http://www.alt-movements.org/no_more_capitalism/hankanshi-info/knowledge-base/category/mail_security/protonmail/
- Tutanota <https://www.tutanota.com/ja/>
どのようにしてGoogleを捨てるか

まとめ

- 検索エンジン Google をやめる。(DuckDuckGo などに変更する)
- ブラウザのプライバシーやセキュリティの設定を見直す(クッキー、広告 ID など)
- ブラウザをより安全なものに変更する
- フィッシング詐欺対策 (差出人アドレスを確認)
- 暗号化メールを使ってみる (Protonmail / Tutanota)

もっとくわしく知る

マジックミラーの裏側で：企業監視テクノロジーの詳細(電子フロンティア財団)