JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

SNSの安全な歩き方
～セキュリティとプライバシーの課題と対策～

2012年1月25日(水)

守屋　英一（もりや　えいいち）

日本IBM　経営品質　情報セキュリティ推進室　シニア・セキュリティ・アナリスト

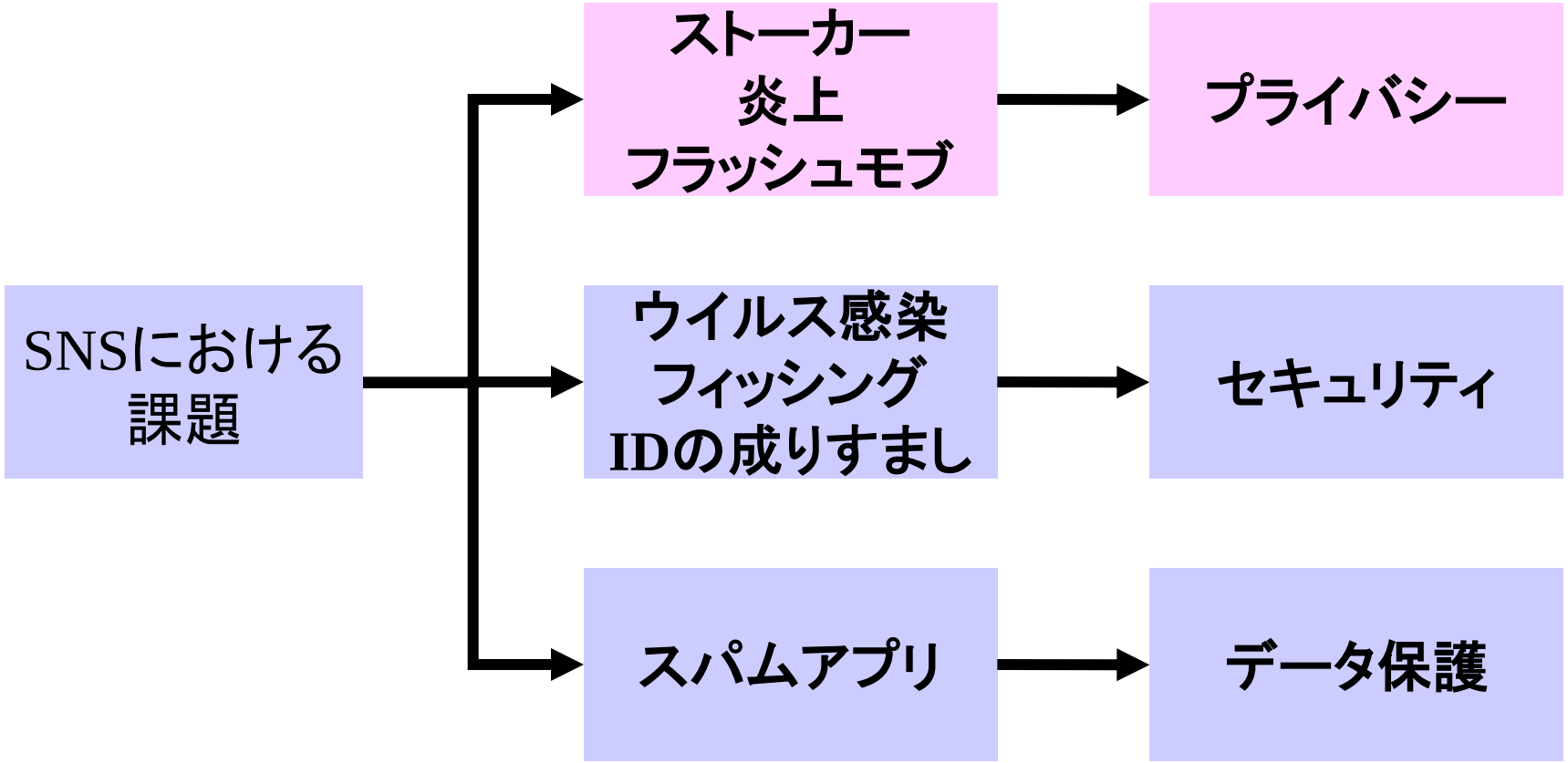
■経歴・担当業務
- 2001年より10年間、セキュリティ・オペレーション・センターの運用責任者
- 2011年より、社内の不正アクセス事件対応およびISMS内部監査を担当

■専門分野
- コンピュータ・セキュリティに関する研究、海外セキュリティ動向調査

■社外活動
- 経済産業省　CTAPP　運用・技術WG　構成員
- 不正アクセス防止対策に関する官民意見集約委員会　構成員
- 内閣官房情報セキュリティセンター「ウイルスの振る舞い分析」構成員
- IPA情報処理推進機構「10大脅威」 構成員
- 日本セキュリティオペレーション事業者協議会　構成員
- 日本シーサート協議会　構成員

Facebookページ：https://www.facebook.com/Privacyinfo

SNSにおける課題


SNSにおける
課題
ストーカー
炎上
フラッシュモブ
プライバシー
ウイルス感染
フィッシング
IDの成りすまし
セキュリティ
スパムアプリ
データ保護

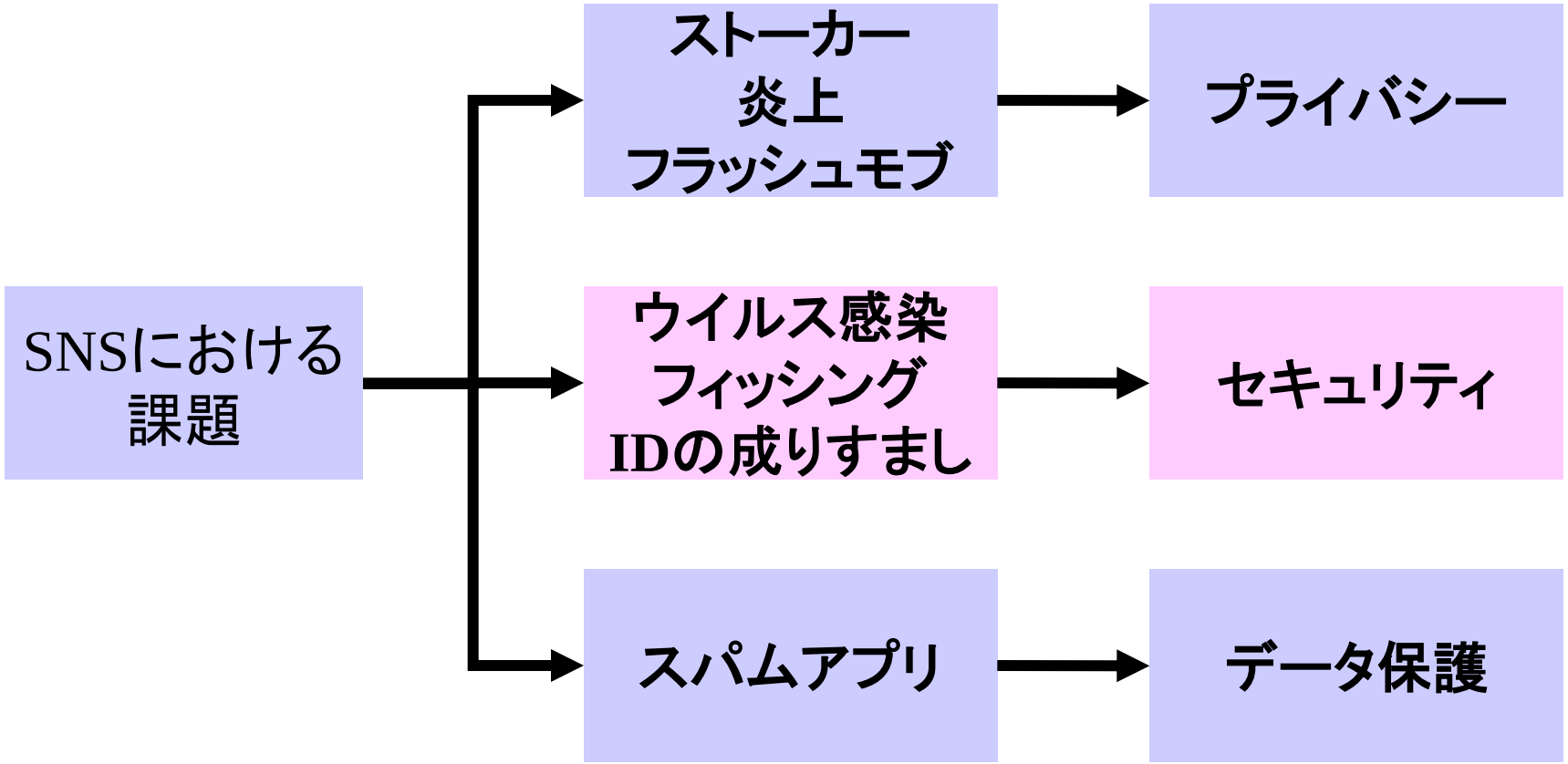
プライバシー

- 誹謗中傷による「炎上」
- うっかり発言、解雇や処分
- 個人情報を「成績化」するサービス
- 韓国で訓練日程や部隊配置計画が公に
- 設定ミスで、携帯電話の番号が公開
- うっかり「公開」で、1万5000人を招待

危険な設定ミス

- 携帯電話番号と携帯アドレスを公開
- プライベートな写真を公開
- 誕生日の公開
- 住所の公開
- 投稿が公開になっている
- 位置情報

SNSにおける課題


SNSにおける
課題
ストーカー
炎上
フラッシュモブ
プライバシー
ウイルス感染
フィッシング
IDの成りすまし
セキュリティ
スパムアプリ
データ保護

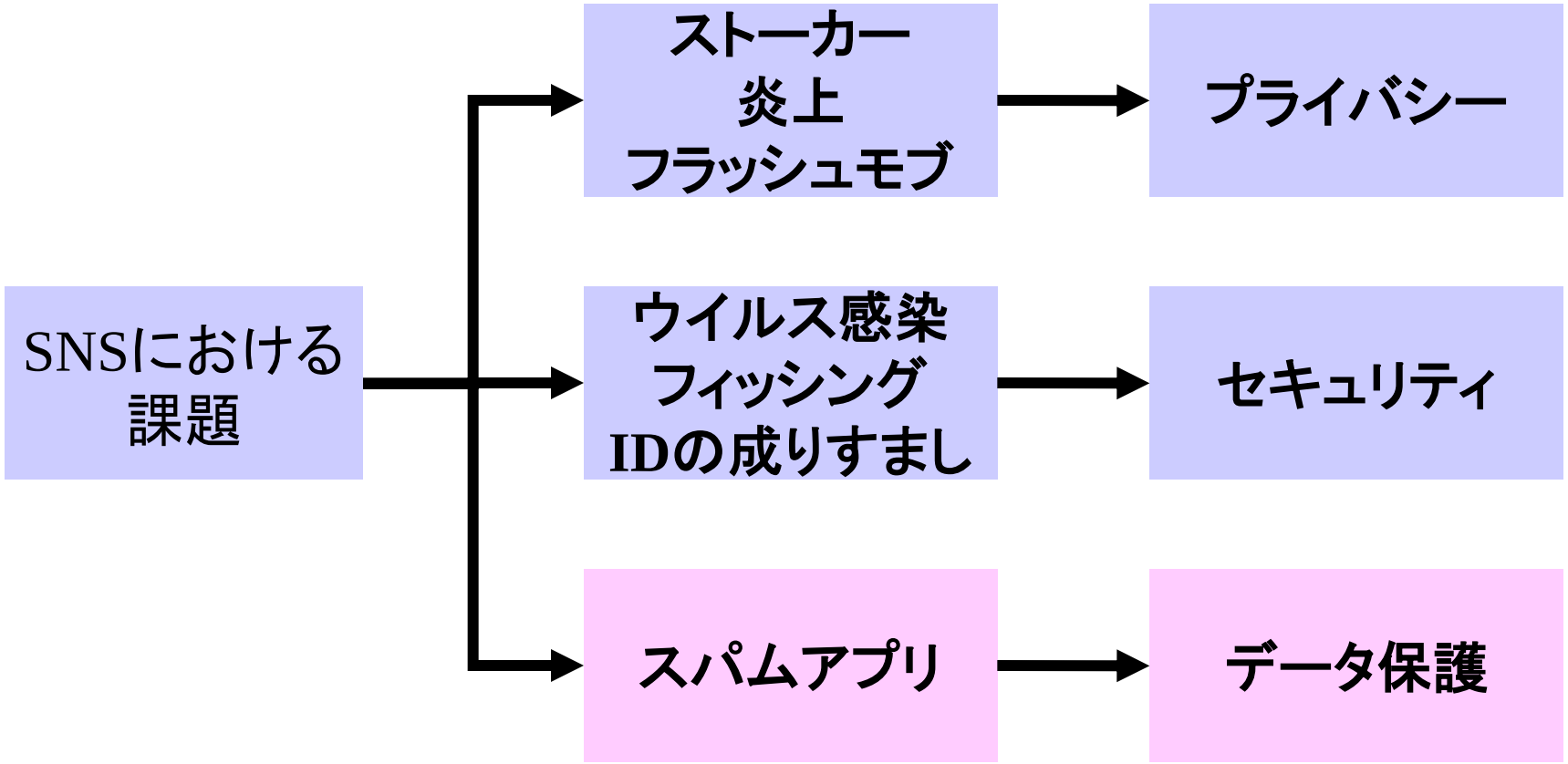
セキュリティ

- 有名人の死亡は、サイバー犯罪の合図
- 偽造の「いいね！」ボタンを使った手口
- IDの使いまわし
- 秘密の質問を推測
- アカウントを持っていなくても危険

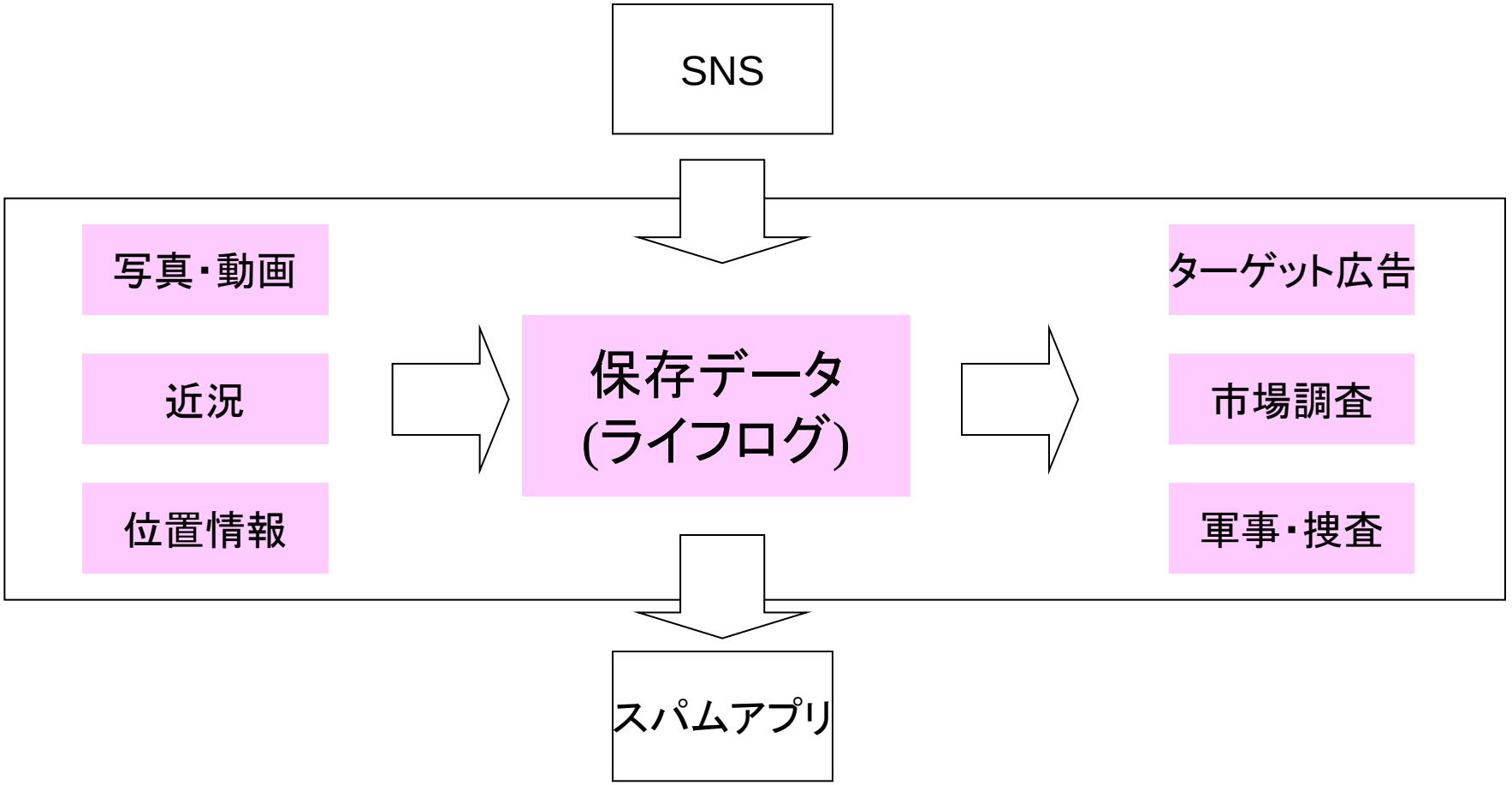
(仮)受動的標的型攻撃

- ターゲッティング広告で標的を絞り、不正なウェブサイトに誘い込む攻撃
  - キーワード
  - 国は25カ国まで選択可能
  - 勤務先、学歴、居住地、性別、年齢、誕生日
  - 好きなもの、趣味・関心、カテゴリ
  - 交際ステータス

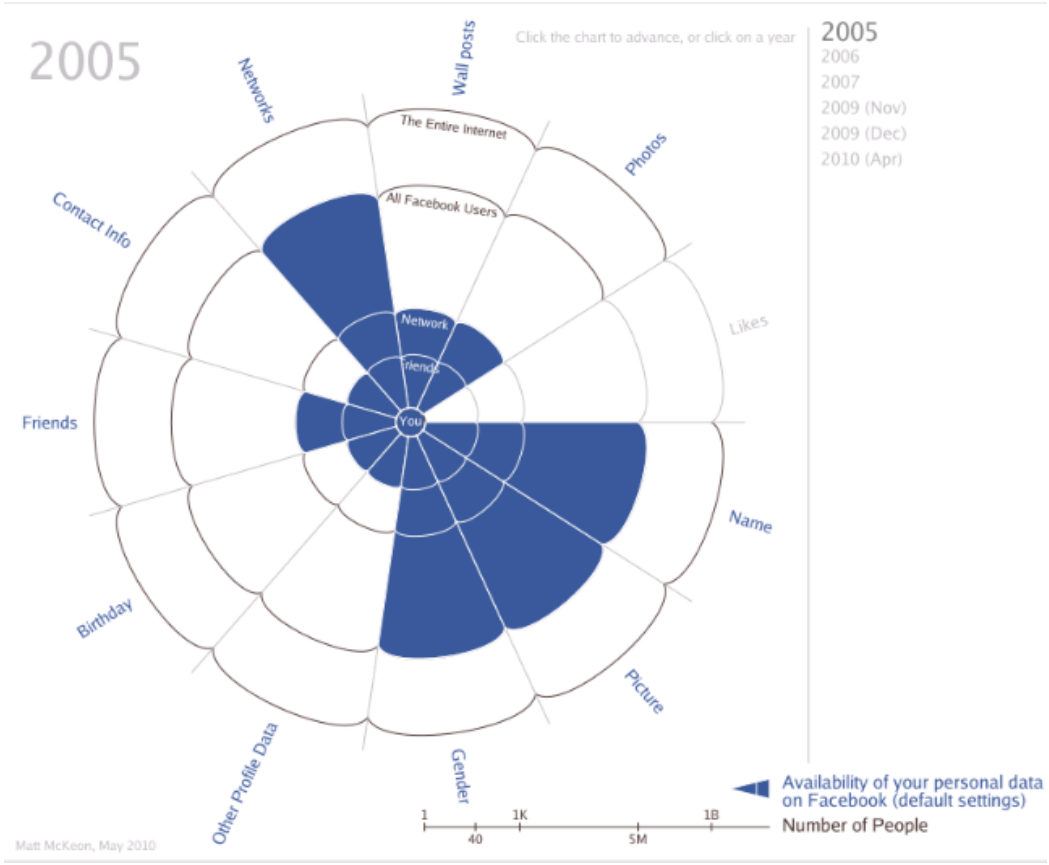
SNSにおける課題


SNSにおける
課題
ストーカー
炎上
フラッシュモブ
プライバシー
ウイルス感染
フィッシング
IDの成りすまし
セキュリティ
スパムアプリ
データ保護

データ保護

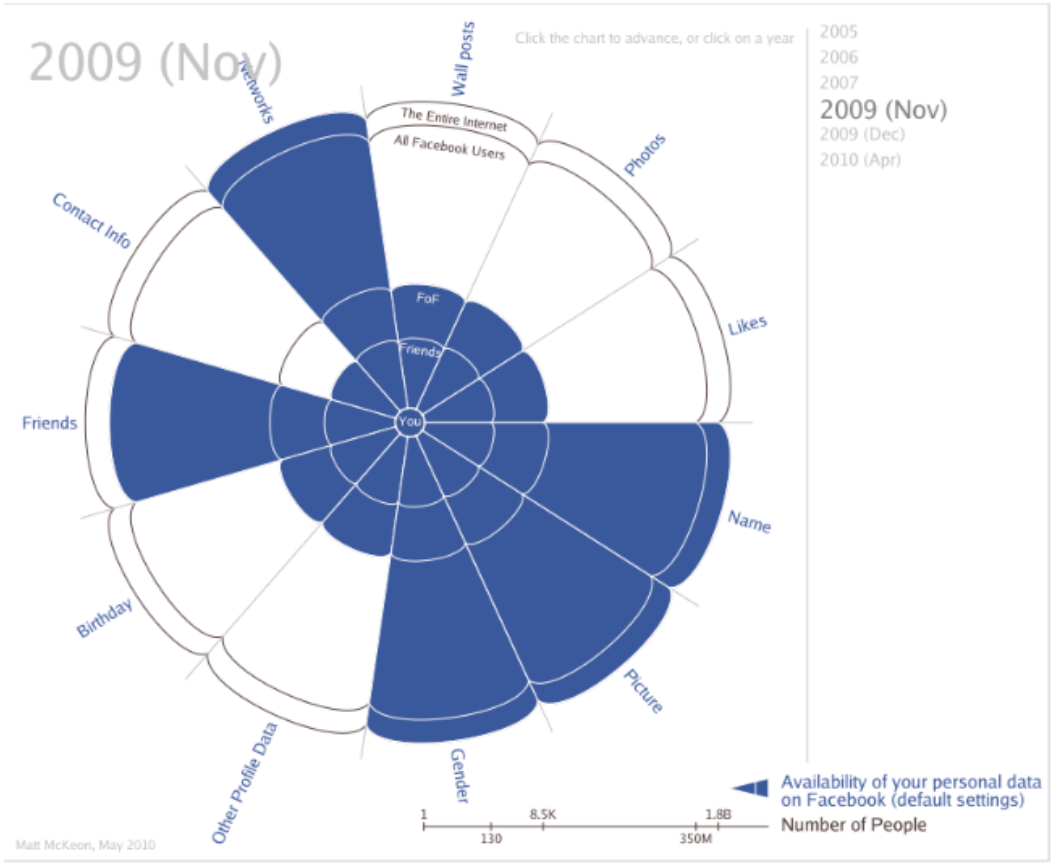


2005年



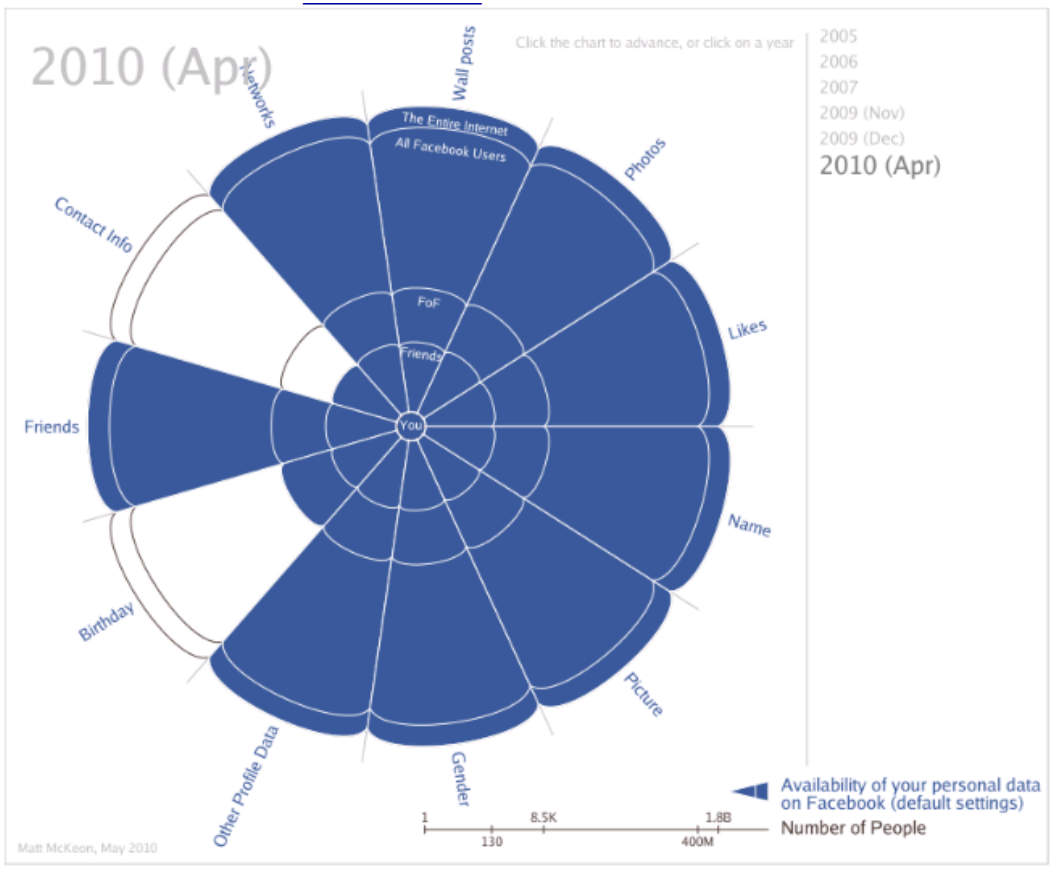
参照：The Evolution of Privacy on Facebook
http://www.mattmckeon.com/facebook-privacy/

2009年



参照：The Evolution of Privacy on Facebook
http://www.mattmckeon.com/facebook-privacy/

2010年



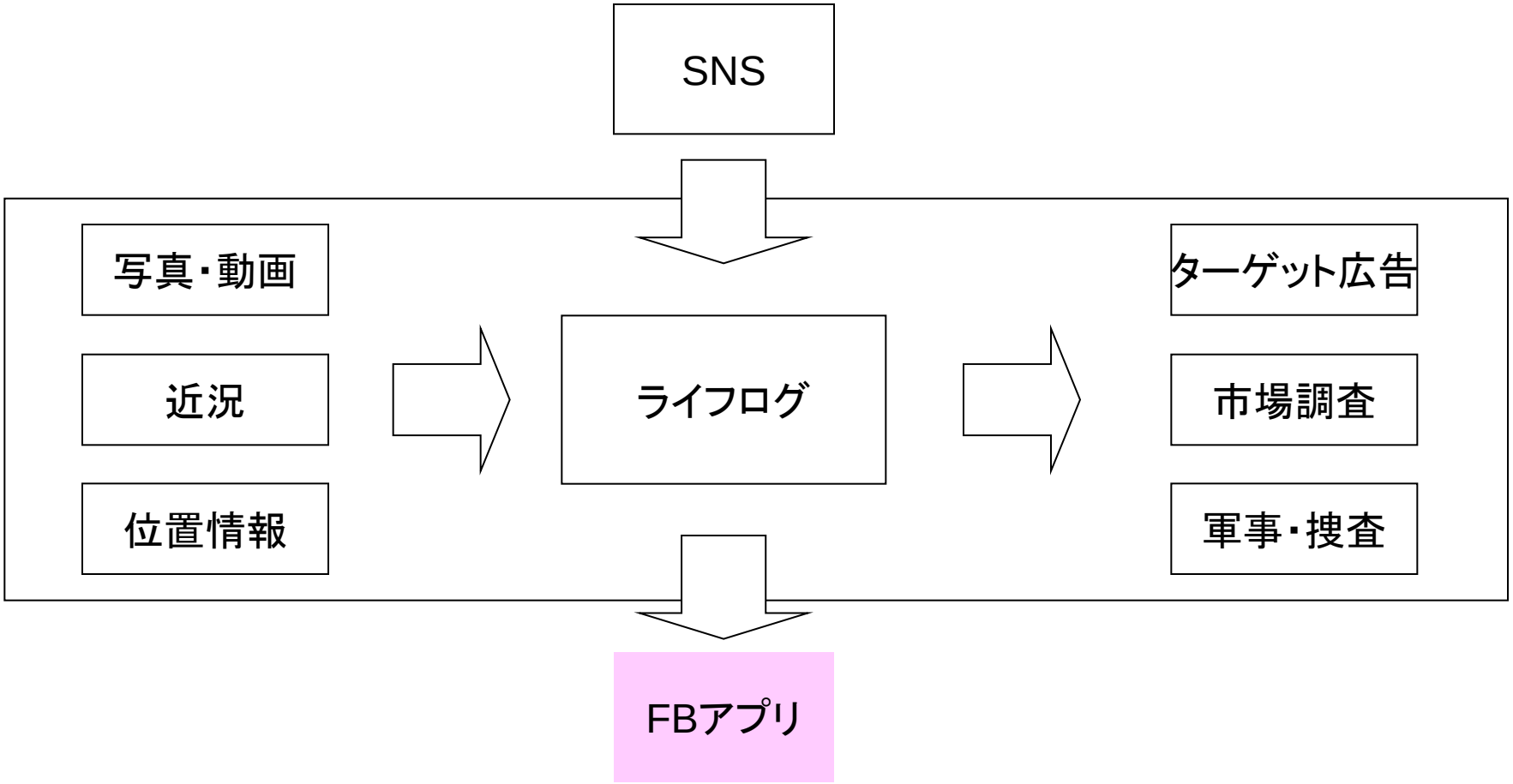
参照：The Evolution of Privacy on Facebook
http://www.mattmckeon.com/facebook-privacy/

Facebookのプライバシー設定の遷移

- サービス開始から2010年4月に至るまで、Facebookがデフォルトの「プライバシー設定」を変更した事を示したグラフである。

- 年々、プライバシー情報のデフォルト設定が緩くなっていっており、個人情報が公になっている。

データの流出？



フェイスブック　アプリケーション

- 2007年　Facebook Applicationを発表
- 友人の誕生日カレンダーを作ってタグ付けし、広めていくタイプや花やケーキなどのグラフィックで記念日や誕生日メッセージを送るアプリ（通称：グリーティング系）
- 一人がこのアプリを使い始めると、他の友人のウォールに書き込まれ、その人から別の友人へと広まる。

See the Earth Day 2011 Greeting Card I made for you!

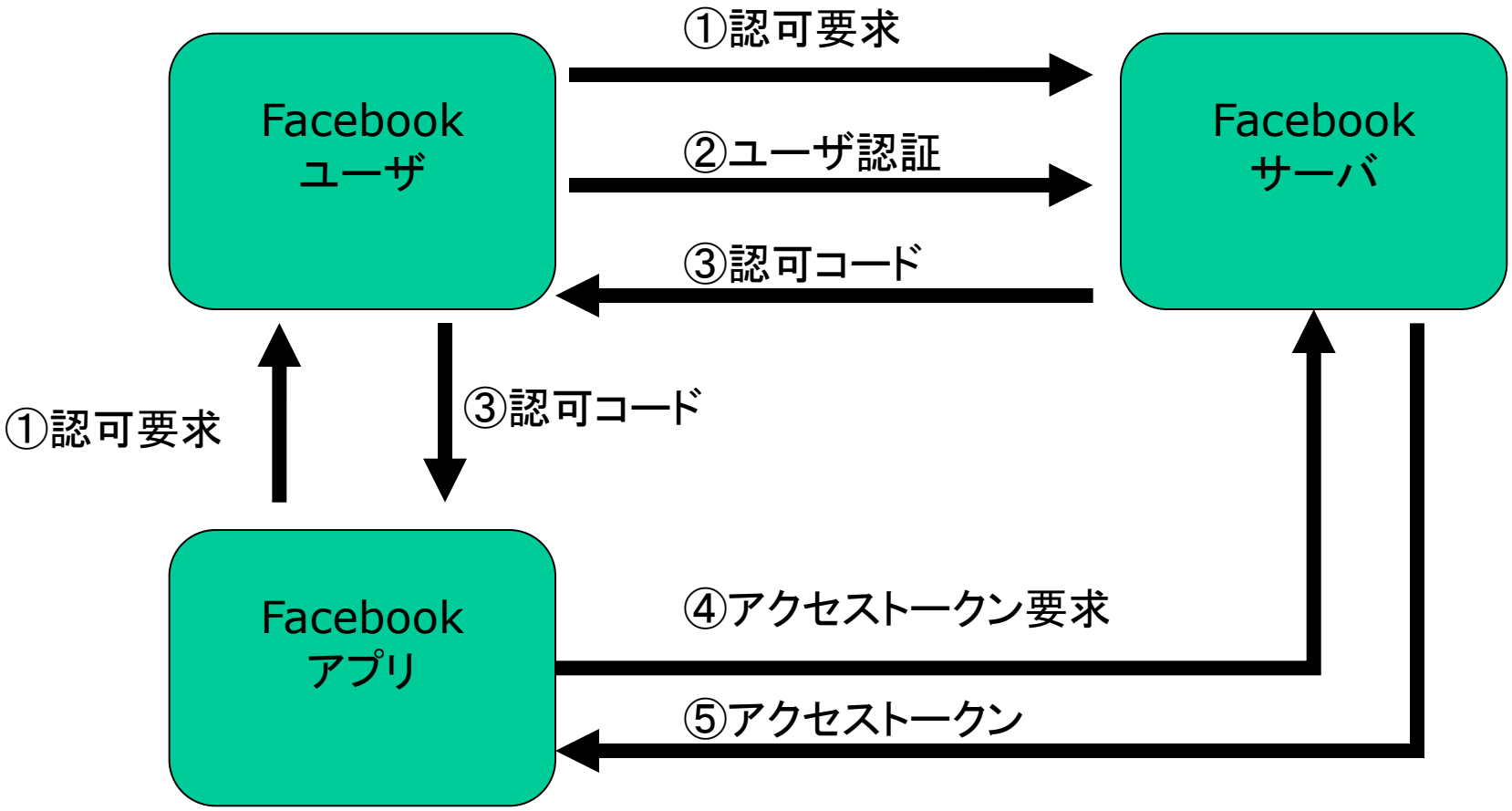
I Created a Special Easter 2011 Greeting Card for You!

Happy Easter 2011!

Friend’s permissions (Greetings)

- Friends Permissionsとは？ Facebookから友達のデータが提供される。しかし、無制限にデータが提供された場合、プライバシー上問題が生じる恐れがある。そこで、アプリケーションがユーザーに友達のデータ提供について許可を求める仕組みになっている。これをFriends Permissionsと呼ぶ。
- Friends Permissionsは「アプリの許可」のダイアログボックスに必要なアクセス許可を求めるメッセージが表示される。

OAuth2.0



参照:スマートにプログラミング facebook アプリ開発 p14

Friend's permissions

Set config	Friends permission	Description
経歴	friends_work_history	経歴へのアクセスを提供
生年月日	friends_birthday	誕生日へのアクセスを提供
家族と交際ステータス	friends_relationships	ユーザーの家族や個人的なリレーションシップへのアクセスを提供
恋愛対象	-	-
政治観と宗教・信仰	friends_religion_politics	ユーザーの宗教と政党へのアクセスを提供
利用しているWebサイト	friends_website	ユーザーのWebサイトのURLへのアクセスを提供
オンライン状況	friends_online_presence	ユーザーのオンライン/オフラインの情報へのアクセスを提供
近況アップデート	friends_status	ユーザーの近況のステータスメッセージへのアクセスを提供
私の写真	friends_photos	アップロードした写真へのアクセスを提供
動画	friends_videos	アップロードしたビデオへのアクセスを提供

アプリによる情報へのアクセス履歴

設定場所:「ホーム」→「プライバシー設定」→「アプリとウェブサイト」→「設定と編集」
→「利用しているアプリ」→「設定を編集」→「編集(確認したアプリを選択)」

フェイスブックアプリ

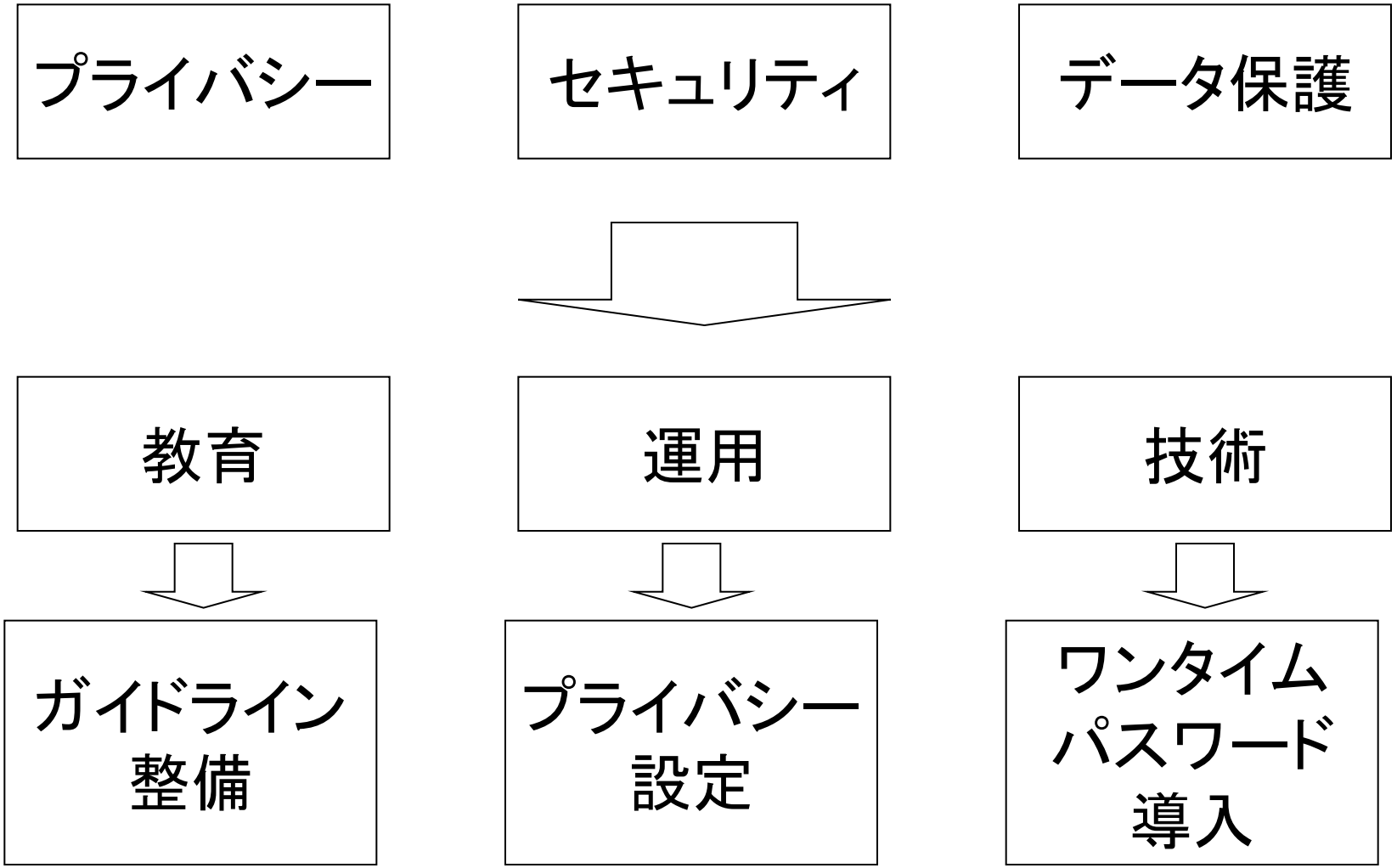
Number	APP Name	Information which can be accessed
1300万人	Badoo	•基本データへのアクセス •メールの送信 •自分の名前を使ったFacebookへの投稿
80万人	Friends Photos	•基本データへのアクセス •メールの送信
62万人	Greetings	•基本データへのアクセス •メールの送信 •自分の名前を使ったFacebookへの投稿 •データへのアクセスを常に許可 **•他の人が私と共有した情報へのアクセス**
36万人	Cards	•基本データへのアクセス •メールの送信 •自分の名前を使ったFacebookへの投稿 •データへのアクセスを常に許可 •他の人が私と共有した情報へのアクセス
32万人	YouLike	•メールアドレス •あなたのプロフィール情報: 生年月日、出身地、好きなもの、位置情報 •あなたの写真

生年月日、出身地、居住地、好きなもの、音楽、テレビ番組、映画、本、好きな言葉、写真、動画

規約違反によるアプリ停止

- アプリの機能・挙動が規約違反を犯している。
  - ユーザーの同意を得ないで、メッセージを操作する行為
- ユーザーからスパム報告を受ける。
  - 許可なくユーザーのウォールへの書き込み
  - 意味もなく友達のウォールに拡散させる行為
- アプリの管理者アカウントが停止になる。
  - 実名以外を使用した場合
  - 管理者のアカウントを複数人で共有して使用した場合

まとめ


プライバシー
セキュリティ
データ保護
教育
運用
技術
ガイドライン
整備
プライバシー
設定
ワンタイム
パスワード
導入