サイバー犯罪と捜査
～なぜ犯人は捕まったのか～

ヤフー株式会社 コーポレート統括本部
政策企画本部 上山 達也

2016年6月15日（水）@九州大学
14:50～16:00（講義）
16:00～16:20（小テスト）

自己紹介

- **上山 達也（うえやま たつや）**
- ヤフー株式会社 コーポレート統括本部 政策企画本部
- ネットセーフティ企画部 リーダー・表示対応マネージャー

	兵庫県川西市出身(18)→岡山市(22)→広島市(25)→東京
1997年4月	食品会社入社(広島市)
2000年4月	ヤフー株式会社入社（カスタマーサポート部）
2002年8月	法務部
2010年10月	リスクマネジメント部 広告審査
2013年4月	ネットセーフティ企画室・政策企画室
2014年1月	現職

政策企画とは？

政策企画ブログ 2016年4月1日

http://publicpolicy.yahoo.co.jp/2016/04/0110.html

この20年はインターネットを巡る法制度についての議論に関わり、その整備や発展とともに歩んできた年月でもあります。今回は、その歴史の一部をご紹介します。

- Yahoo!オークションと**古物営業法**
- Yahoo!パートナーと**出会い系サイト規制法**
- 検索エンジンと**著作権法**
- インターネットと**公職選挙法**（ネット選挙）
- フィッシング行為と**不正アクセス禁止法**
- 海外事業者と**消費税法**

事例1：知恵袋

- ヤフー知恵袋に「ヤフー女性社員を待ち伏せしませんか」と書き込み。

→ 脅迫？

→ 業務妨害、有罪、罰金50万円

事例2：書店万引き

- ヤフーオークション（ヤフオク）に書店で万引きした書籍を出品。大学生。400万円以上の取り引きか。

事例3：ヤフオク

- ユニバーサル・スタジオ・ジャパン（USJ）の年間パスを使用し、パーク内でグッズを万引き、インターネット・オークションを通じて処分、販売していた。28歳・男性。
- 「4月から年間パスで27回ＵＳＪに入り、グッズを万引きしてネットオークションで転売した。約50万円になった」と供述

事例4：広告

「腹いせで」ヤフーに勝手に広告発注ＵＳＥＮ元社員逮捕 **産経新聞 6月1日(水)23時59分配信**

インターネット検索大手「ヤフー」に勝手に広告を発注し、有線放送大手「ＵＳＥＮ」に数千万円の広告料を発生させたとして、警視庁が背任容疑で、ＵＳＥＮ元 社員で埼玉県内の３０代の男を逮捕していたことが１日、捜査関係者への取材で分かった。

http://headlines.yahoo.co.jp/hl?a=20160601-00000602-san-soci

Yahoo! JAPANのスポンサードサーチって？

Yahoo! JAPANの検索結果ページにクリック課金型の広告が掲載できます！

Yahoo! JAPANは、日本最大級のポータルサイトであり、一カ月あたり、実に約680億回も閲覧されています。
（2015年度第2四半期　決算説明書より四半期期中平均）

スポンサードサーチを使えば、より多くの人にYahoo! JAPANの検索結果に目立つ位置で、あなたの会社や商品・サービスをアピールできます。

最短1日※から掲載もOK！
Yahoo! JAPANで、新しいお客様を集めよう。

こういうのも関係しました

- パソコン遠隔操作事件
- 英国人女性殺人犯逃亡事件
- 京都大学入試 知恵袋カンニング事件

サイバー犯罪

サイバー犯罪のいろいろ

分類（by 警察庁）

1. ネットワーク利用犯罪 (児ポ、詐欺、わいせつ、知財侵害、ほか)
2. 不正アクセス禁止法違反
3. コンピュータ・電磁的記録対象犯罪及び不正指令電磁的記録に関する罪

※ 平成26年中のサイバー空間をめぐる脅威の情勢について
http://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf

サイバー犯罪のいろいろ

分類　（by 私）

1. インフラとしてのインターネット利用
2. サービスを悪用したもの
3. 不正アクセス
4. サイバー攻撃

1. インフラとしての利用

- インタネット、通信の本質。
- 人と人のコミュニケーション
- メール、Twitter、SNSなど
- 通信の秘密を侵害してはならない
  - 日常的にモニタリングできない
  - 事後的に警察捜査に協力していく
  - 個別の通信に関して、通信の内容はもちろん、その通信の当事者の情報（利用者情報）についても通信の秘密により保護されている。

2. サービスを悪用

- オークション詐欺
- 知的財産権侵害物品の販売
- 児童ポルノ、わいせつ物の販売
- 未承認医薬品の販売、広告
- 無届貸金業（ヤミ金）の広告
- なりすましECサイト
- 殺害予告、犯罪予告など（業務妨害）

3. 不正アクセス

- 不正アクセス禁止法
- ネットバンキングでの不正送金
- SNS上でのなりすまし、プリペイドカードの購入もちかけ
- なりすましカード利用
- ゲームアイテム、ゲーム内通貨の窃取

4. サイバー攻撃

- 威力誇示型から利益追求型さらにサイバーテロへ
- ターゲット
  - 優良顧客のアカウント（ID、パスワード）
  - クレジットカード情報（番号、有効期限）
  - 企業の秘密情報、システム情報
- 攻撃手法
  - DDOS攻撃
  - SQLインジェクション
  - ソーシャルエンジニアリング
  - 標的型メール攻撃、ばら撒き型メール攻撃

実例紹介

実例紹介

1. なりすましECサイトでの通信販売
2. ヤフオク次点詐欺
3. SNSのっとり
4. IDの売買
5. 遠隔操作
6. 違法ダウンロード
7. プライベート写真を利用した脅迫
8. ストーカー

なりすましECサイトでの通信販売

「なりすましECサイト」とは、実在するサイトの外観（屋号、商標、サイト意匠・構成、使用している画像等）を模倣することにより、あたかも当該サイトである又は当該サイトと関係のあるサイトであるかのように消費者を誤認させ、商品代金をだましとったり、模倣品、海賊版その他購入しようとした品と全く別個の物を送りつけるサイトを指します。

典型事例

引用：http://www.saferinternet.or.jp/narisumashi/

ヤフオク次点詐欺

- 出品者になりすまし、次点落札者に連絡をし、お金を騙し取る。
- 2位、3位でオークションを落札できなかったものを騙す。

→ 次点詐欺と呼ばれている。

SNSのっとり

- リスト型攻撃で有効なID、パスワードリストを作成
- のっとり行為者がリストからアクセス
- ネットワーク型プリペイドカードなどの購入を促し、カード番号を詐取
- カード番号はオンライン上で消費される

IDの売買

- 脆弱性のあるシステムを攻撃
- リスト型攻撃で精製
- IDの価値を評価する
- IDの買取

遠隔操作

- 攻撃対象者をサイトへ誘導
- サイトを閲覧すると、遠隔操作用のマルウェアを不正にインストール
- 遠隔操作によりPCを操作

プライベート写真を利用した脅迫

- リベンジポルノ
- 脅迫罪、強要未遂罪での摘発事例

→ 2014年11月「私事性的画像記録の提供等による被害の防止に関する法律」が成立

- 公表罪と公表目的提供罪

参考：http://www.npa.go.jp/safetylife/seianki/shiseigazouboushi/

捜査機関とインターネット（捜査の流れ）

- 端緒
- サービスプロバイダへの捜査協力
- 接続プロバイダへの捜査協力
- 端末、契約者まではたどり着くが・・・
- 状況調査で行為者特定
  - 逮捕
  - 起訴
  - 刑事裁判、判決（有罪、無罪）

捜査協力の根拠

- 刑事訴訟法
  - 捜査関係事項照会（第197条 第2項）任意
  - 利用規約での取り決め
    - ヤフーの利用規約

4. 個人情報の第三者への提供

前項であらかじめ同意いただいている場合以外についても、以下の場合には、当社は個人情報を第三者に提供することがあります。

（1） 裁判所から、法令に基づく開示を命じる判決もしくは命令を受けた場合、または、警察などの公的機関から、捜査権限を定める法令に基づき正式な照会を受けた場合

（2） 当社または提携先のサービスの利用に関連して、お客様が法令や本利用規約、ガイドラインなどに反し、第三者または当社の権利、財産、サービスなどを保護するために必要と認められる場合であって、本人の同意を得ることが困難な場合

（3） 人の生命、身体および財産などに対する差し迫った危険があり、緊急の必要性がある場合であって、本人の同意を得ることが困難な場合

（4） その他、個人情報保護法上許容される場合

捜査協力の根拠

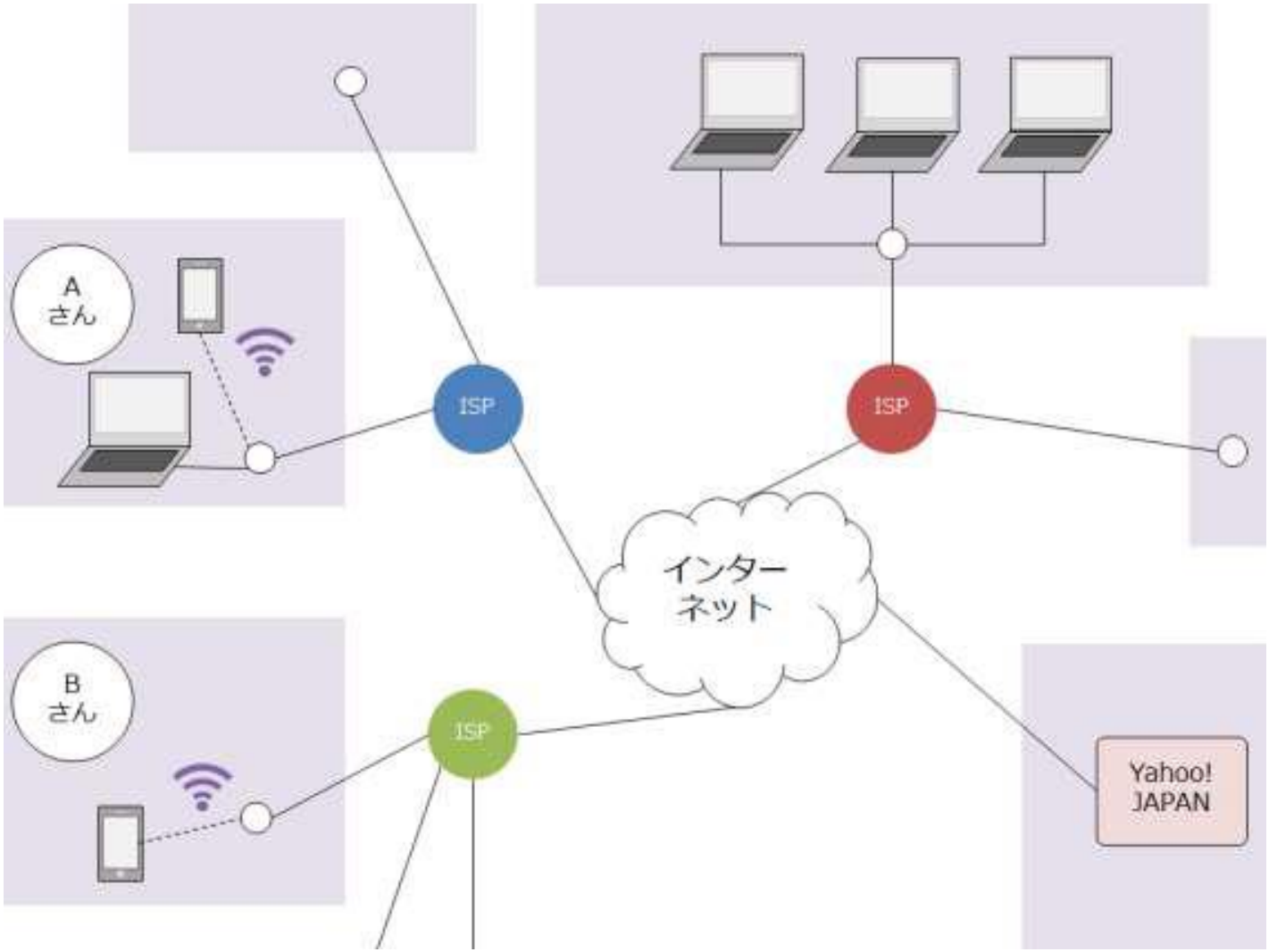
- 刑事訴訟法
  - 差押　（第99条 ～）強制
    - 通信の秘密を侵害した場合に、事業者に対して刑事罰あり（電気通信事業法）
    - 通信の秘密を侵害するような情報については、強制力のある差押の手続きで対応。
    - 主にメールの内容や一対一のメッセージの内容
    - 裁判所が捜査機関からの請求により発行する令状により執行（差押令状、通称フダ）

回答までの流れ

捜査の流れ（実例：ヤフオク）

1. 詐欺発生
2. オークションID、Yahoo! JAPAN ID、振込先銀行口座、相手の連絡先等の確認
3. オークションID、Yahoo! JAPAN ID からYahoo! JAPAN へ捜査関係事項照会
4. オークションのログ、Yahoo! JAPAN ID のログ、Yahoo! JAPAN ID の登録情報などを回答
5. 登録情報が容疑者本人のものであることはまれ
6. ログ上に保存されたIP アドレスから接続プロバイダを割り出し、当該時刻（タイムスタンプ）にそのIP アドレスを利用していた者の契約者情報を差押
7. 被疑者が絞られてくる

IPアドレスから契約者情報？



サイバー犯罪捜査の課題（私見）

- 被疑者と被害者の物理的距離が離れている。ちょっとした事件でも全国規模の捜査になる。（全国協働捜査方式、サイバー犯罪特別処理班などの活用が進んでいる。）
- 相談を受ける捜査員による状況把握力
- 被疑者が海外にいる場合の追跡困難性

民事対応

- 名誉毀損、プライバシー権侵害などの人格権侵害
- 著作権、商標権、パブリシティ権などの知的財産権侵害
- プロバイダ責任制限法

→ 送信防止措置と発信者情報開示

- 申立者、投稿者、サービス運営者の関係

プロバイダ責任制限法

- 一定の要件を満たす場合に、サービス運営側（プロバイダ）の責任を制限するもの。

→ 送信防止措置（削除）が出来る要件

→ 発信者情報開示が出来る要件

→ 投稿者への意見照会手続き方法などを規定

プロバイダ責任制限法に関する申告を行う方へ（ヤフー株式会社）
http://docs.yahoo.co.jp/info/notice47.html

まとめ

- 捜査機関は、刑事訴訟法上の手続きにより、サービス利用者の情報、ログなどを入手している。
- 通信の秘密に関わるものは裁判所の令状に基づき対応している。
- 民事手続きの基本はプロバイダ責任制限法によるもの。
- その他、権利侵害等による不法行為に基づく損害賠償請求（民法709条）など。

小テスト ○ ×？

Q1. ヤフーなどのサービス提供事業者は警察からの問合せに対応する法律上の義務がある。

Q2. 犯罪の行為者を特定するには、IPアドレスさえ分かれば十分である。

Q3. 金銭のトラブルなど私人間の問題は警察などの捜査機関が解決してくれる。

Q4. プロバイダ責任制限法は送信防止措置（削除）と発信者情報の開示の手続きなどを定めた法律である。

Q5.講義の感想をお聞かせください。