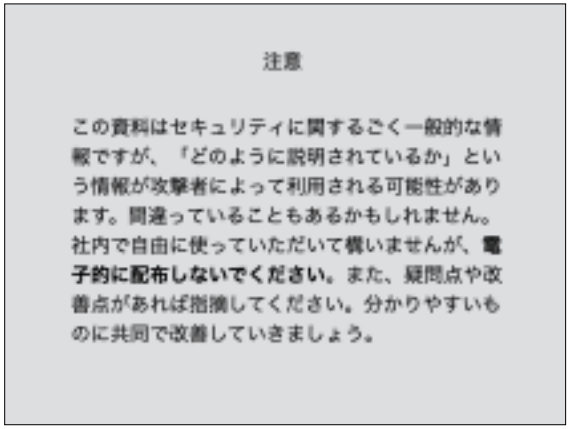
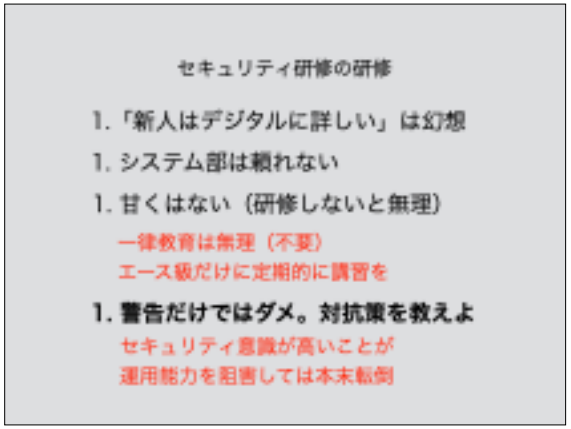
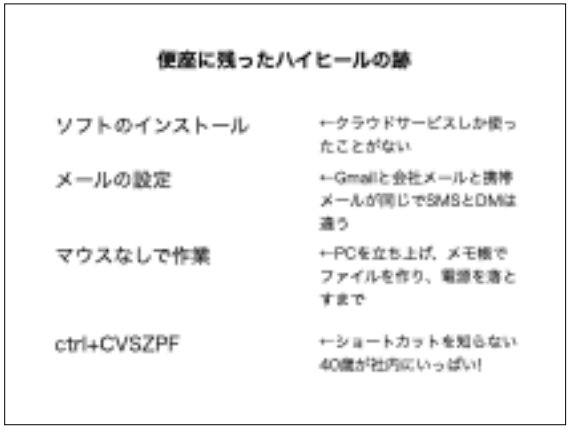


この資料は、セキュリティに関する一般的な情報ですが、「どのように説明されているか」という情報が攻撃者によって利用される可能性があります。電子的には配布しないでください。この資料は、記者クラブ加盟社は自由に使っていただいて構いませんが、疑問点や修正・追加した場合は、日本記者クラブの記者ゼミに提出してください。分かりやすいものになるよう、共同で改善していきましょう。

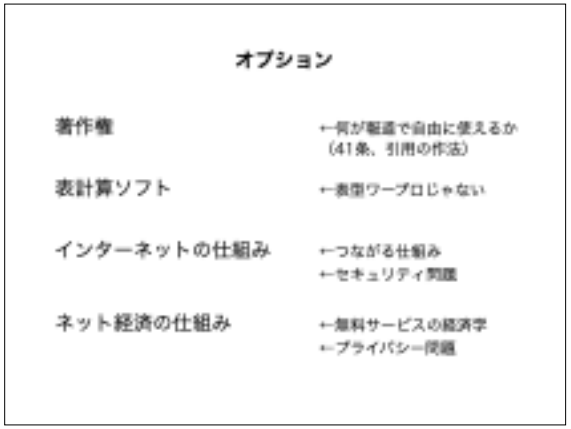


「新人はデジタルに詳しい」は幻想です。Excelが使える新人の比率は2000年頃と変わっていません。なぜ入社試験でチェックしないのでしょうか？　システム部も頼れません。もし丸投げすれば、何もかも禁止されるでしょう。記者クラブのPC講習で、紹介したソフトを一本もインストールできない社がありました。便利な機器・ソフトだからこそ情報が漏れるのです。セキュリティ研修はfoolproofではありません。

新人研修では、セキュリティ研修の前にパソコン研修をしましょう。残念ながら、コンピューターを自在に使いこなす新世代が参入してくるという未来はこの業界には来ませんでした。



大卒新人には必ずパソコン講習が必要。学生のデジタルリテラシーはバラバラで、かつ、すべての学生が「自分のパソコンの使い方が正式だ」と思っている。（家庭環境や大学のゼミなどで作法はバラバラ）



これらの点は学校で教えられているかもしれない。
ただし、著作権の41条（時事の事件を構成した著作物や、事件の過程で見聞きされた著作物は、報道の目的上正当な範囲内で、利用することができる）は、学校で教える話とは恐らく正反対の話。

新人研修では、セキュリティ研修の前にパソコン研修をしましょう。残念ながら、コンピューターを自在に使いこなす新世代が参入してくるという未来はこの業界には来ませんでした。

生成AIブーム

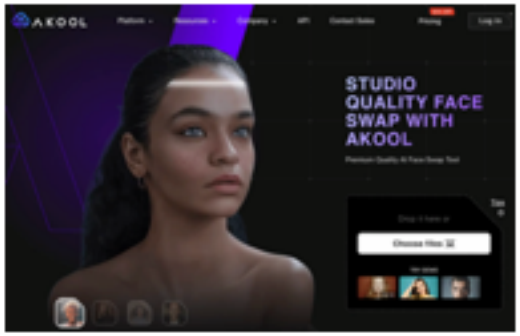
RVC: Retrieval-based-Voice-Conversion

https://github.com/svc-develop-team/so-vits-svc

中国Alibaba: EMO（Emote Portrait Alive)

https://www.youtube.com/watch?v=VU71kcn9Y

AKOOL: Face Swap



AI安倍晋三元総理(2022/9/25)

東京大学A研究会

Taylor Swift (2024/1)

Microsoft Designer

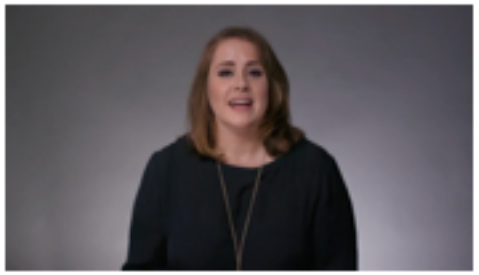
安倍晋氏の生成ＡＩ偽動画も(読売)

BBC Verify: How to spot AI fakes in the US election

BBC Verify: How to spot AI fakes in the US election

Is This Video Even Real?(2019/8)

NYT Opinion



ウクライナ紛争（2014-）

軍事作戦と連動した最初のサイバー戦争

政府機関・テレビ局などにDDos攻撃

公的機関のサイトを止めると同時に生かしておいたSNSなどでフェイクニュースをばら撒く

通信網に対する攻撃

Viasatの衛星通信網に侵入、モデムのソフト更新でワイパー挿入/標的後は通信会社に物理的に侵入

電力網への攻撃

2015.12.23 ウイルスBlackEnergyによるコントロールセンターの麻痺

Excel/Wordのマクロを使ったSpear Phishing

ジーメンスのSCADAを乗っ取る

ウイルスによる物理的破壊

「データが消えるだけ/リセットすれば直る」ではない例

Aurora発電機テスト(2007)

発電機と送電網の同期を外して電流を逆流させ、発電機を破壊

Stuxnet(2009頃)

USBで感染。ジーメンスのSCADAを乗っ取り、イラン・ナタンツのウラン濃縮工場を破壊

独製鉄工場(-2014)

メールで感染。製鉄工場のPCL(programmable logic controllers)を改変、高炉を破壊

RaaS:Ransomware as a Service

ウイルス感染と利用の分業

CryptoLocker(2013-)

特定の拡張子のファイルをRSAで暗号化

Trickbot(2016-)

ロシア・ウクライナのサイバー犯罪グループ

Lockbit(2019-)

HDを勝手に暗号化し身代金を要求

大阪総合医療センター(2022)

給食センター経由でEbioに感染

名古屋港運協会(2023/7)

Lockbit3

徳島・半田病院(2021/10)

Lockbit。医療機器のアップデート用VPNから侵入

Pegasus（2021-）

イスラエルNSOのスパイウエア

政治家・宗教家・NGO・記者など5万件の電話番号

記者180人のiPhoneからスパイウエアを確認

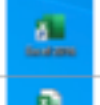
完全に携帯電話を乗っ取る

WhatsApp/Signalなどの暗号化対応メッセージソフトも解読
カメラ・マイクを自在にオンにできる

ゼロクリック攻撃

iMessageを使ったゼロクリック攻撃/宅配便の追跡リンクも併用

クリック＝PCに対する命令に許可を与えること

アイコン	対象	命令	行われること
	フォルダ	フォルダの 中身を表示せよ	ファイル検索と アイコン表示
	プログラム （ショートカット）	プログラムを実行 せよ	**無制限**
	（関連づけられた） ファイル	関連づけられた プログラムを実行し ファイルを開け	別のプログラム立ち上げ 起動マクロの実行 （再計算）

ファイルを開くと誤認させ、プログラムを実行し、ウイルスをインストールする

対策: 右クリックで確認

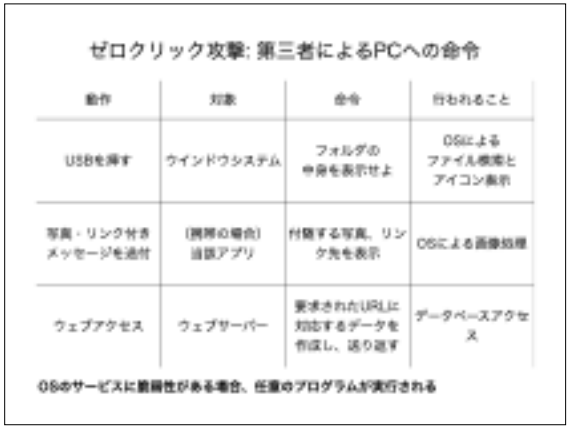
「何で開くか」自覚的になろう。
ダブルクリックしていいのは
自分が作ったドキュメントだけ

「読み取り専用」で開く
マクロは解除しない

リンクのクリック＝ブラウザにファイルを開かせる**許可**

GMailに添付できないファイル

メールの差出人は自由に変更可（なりすまし簡単）



ゼロクリック攻撃: 第三者によるPCへの命令

動作	対象	命令	行われること
USBを挿す	ウインドウシステム	フォルダの中身を表示せよ	OSによるファイル検索とアイコン表示
写真・リンク付きメッセージを送付	(興味の場合)当該アプリ	付随する写真、リンク先を表示	OSによる画像処理
ウェブアクセス	ウェブサーバー	要求された URL に対応するデータを作成し、送り返す	データベースアクセス

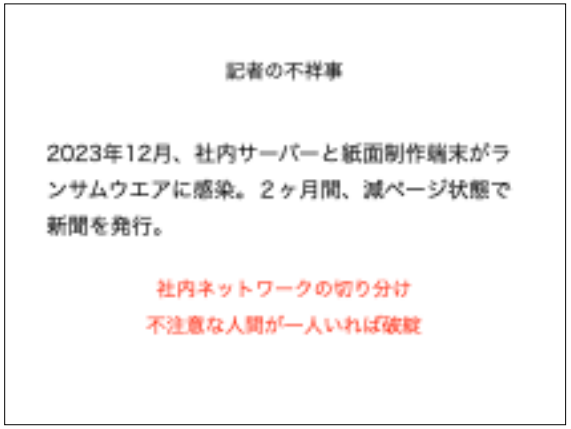
OSのサービスに脆弱性がある場合、任意のプログラムが実行される

OSのアップデートは必須

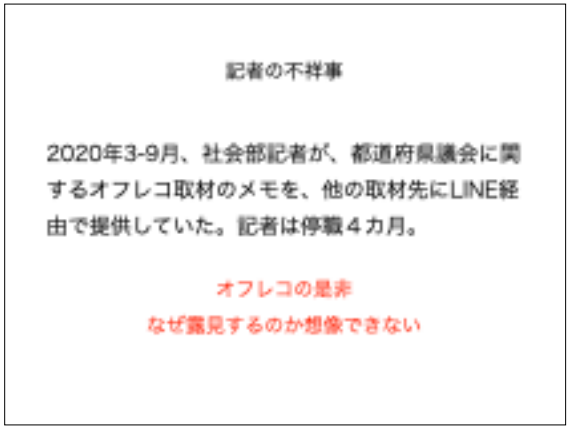
iOS 17.4とiPadOS 17.4

1.事例

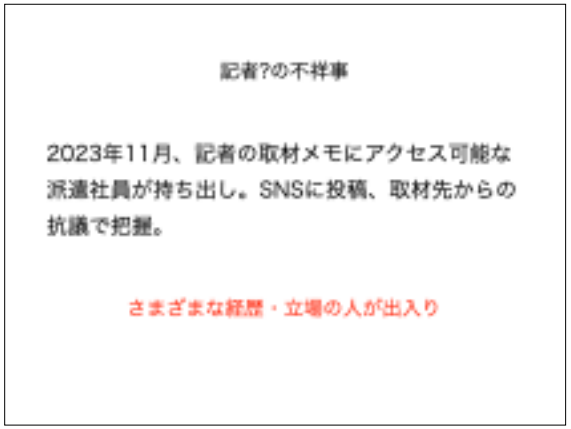
警察・自衛隊担当記者や特派員と文化部記者とが同じセキュリティ・ルールを守ることは、現実的ではありません。しかし、甘く考えるとどうなるか、愚かな先輩、愚かな会社の事例を胸に刻んでください。



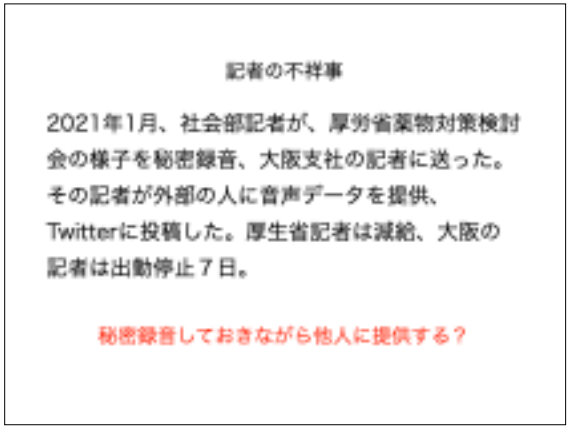
2023年12月19日、長野日報の社内サーバーと紙面端末十数台がランサムウエアに感染。翌年2月20日まで減ページ状態で新聞発行を余儀なくされた。
教訓：社内ネットワークのレベルは会社の規模によって違う。基幹部分を切り分けてないなら、ウイルスや情報漏洩のリスクは社員のセキュリティ教育に全面的に依存する。



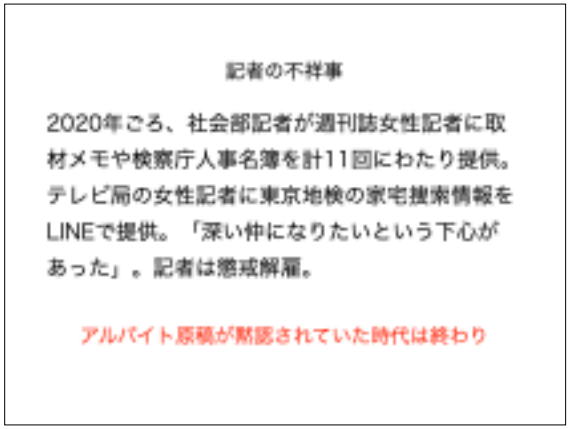
2020年3-9月、社会部記者が、都道府県議会に関するオフレコ取材のメモを、他の取材先にLINE経由で提供していた。記者は停職４カ月。
教訓：オフレコ条件に応じておきながら、嬉々としてその情報を当てに行き、オフレコがバレる最低の事案。



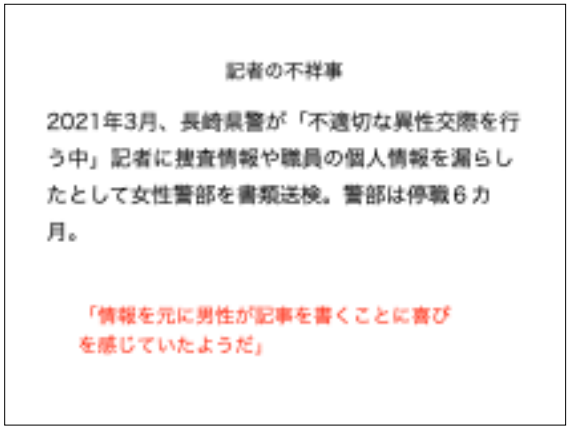
2023年11月、編集局のネットワークにある取材メモや企画書を字幕などを担当する派遣社員（アクセス権限あり）が印刷して持ち出し、SNSに投稿。アクセス記録から関与を確認。
教訓：局は文書にパスワードをつけるなどの対策。



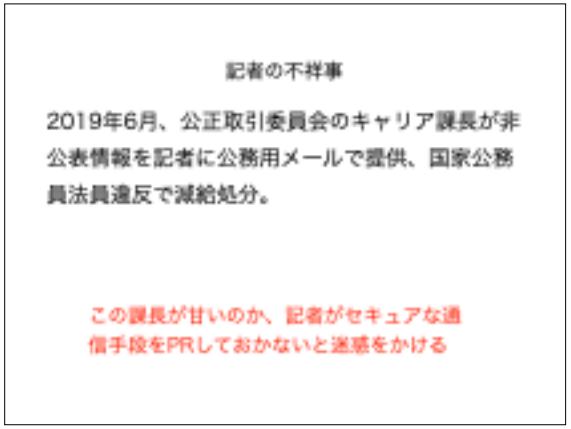
2021年1月、社会部記者が、厚労省薬物対策検討会の様子を制限に反して録音、大阪支社の記者に送った。その記者が外部の人に音声データを提供、Twitterに投稿した。厚生省が抗議。厚生省記者は減給、大阪の記者は出勤停止７日。
教訓：秘密録音しておきながら他人に提供する



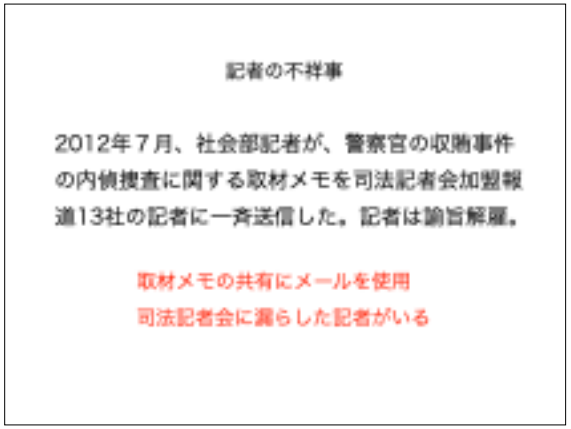
2020年ごろ、社会部記者が週刊誌女性記者に取材メモや検察庁人事名簿を計11回にわたり提供。テレビ局の女性記者に東京地検の家宅捜索情報をLINEで提供。「深い仲になりたいという下心があった」。記者は懲戒解雇。
教訓：他メディアでのアルバイト原稿が黙認されていた時代はそろそろ終わり



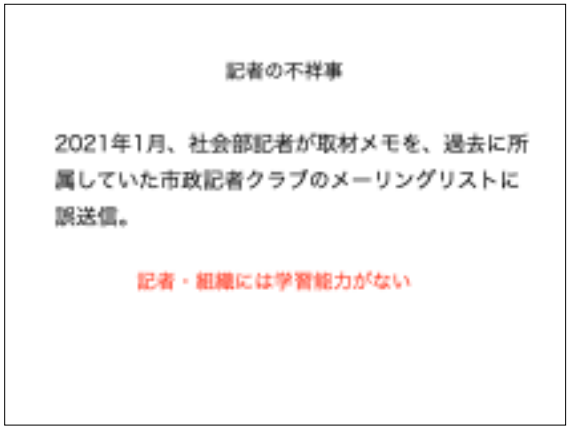
2021年3月、長崎県警が「不適切な異性交際を行う中」記者に捜査情報や職員の個人情報を漏らしたとして女性警部を書類送検。警部は停職６カ月処分を受け依願退職。「８月ごろ、県内の観光地で２人が食事をしていたとの目撃情報が県警に寄せられ、発覚した」というのは本当か、疑う必要がある。



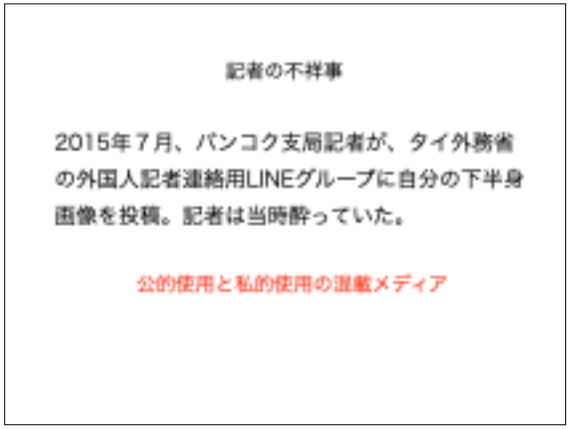
2019年6月、公正取引委員会のキャリア課長が「記者が情報を元に取材することで独禁法違反を申告する企業が出てくるのではないか」と考え、非公表情報を記者に公務用メールで提供したとして、国家公務員法員違反で減給処分。



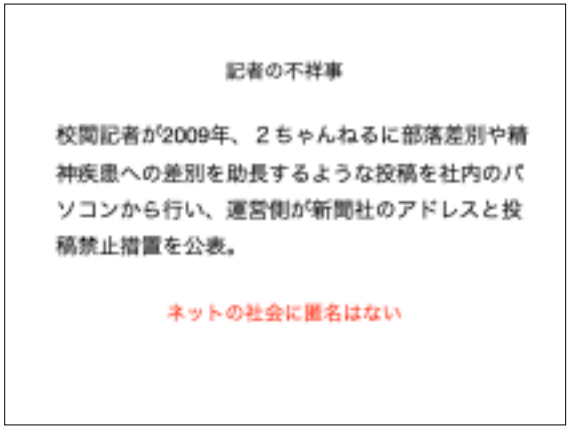
2012年７月、社会部記者が、警察官の収賄事件の内偵捜査に関する取材メモを司法記者会加盟13社の記者にメールで一斉送信した。記者は諭旨解雇。
教訓：悪いのはメールで送らせた県警キャップ。記者会にも腐ったミカンがいて、外部に漏らした。



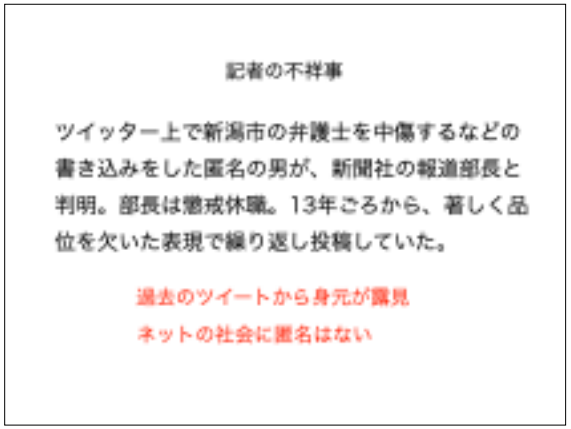
2021年1月、社会部記者が、個人名を含む取材メモを同僚に送ろうとして、過去に所属していた市政記者クラブのメーリングリストに誤って送信。読売新聞は「読売新聞記者にも届いた」と報道。
教訓：記者にも組織にも学習能力がない



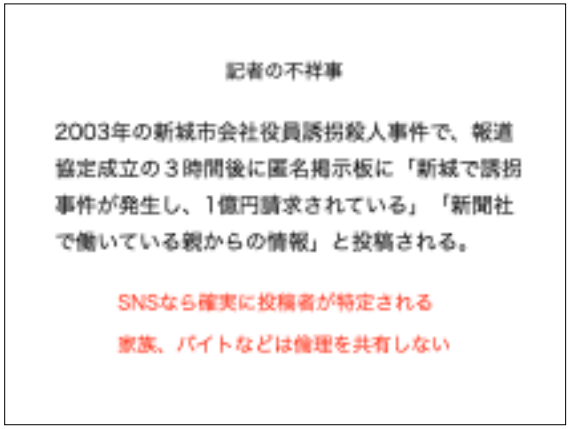
2015年７月、バンコク支局記者が、タイ外務省の外国人記者連絡用LINEグループに自分の下半身画像を投稿。記者は当時酔っていた。
教訓：公的に使用するメディアを私的通信にも使っていた。宛先違いのミスは頻繁にある。



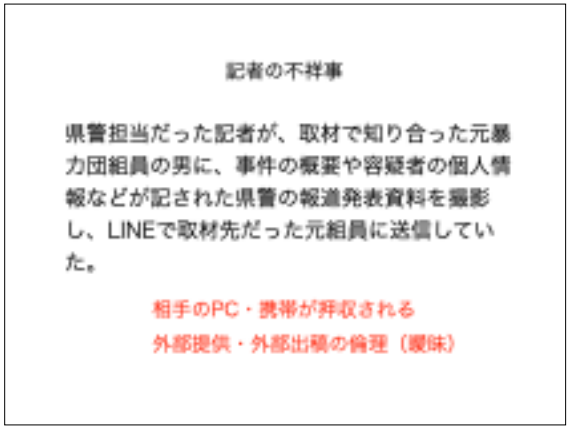
校閲記者が2009年、２ちゃんねるに部落差別や精神疾患への差別を助長するような投稿を社内のパソコンから行い、運営側が新聞社のアドレスと投稿禁止措置を公表。
教訓：会社が書き込みを禁止していない。ネットに匿名はない



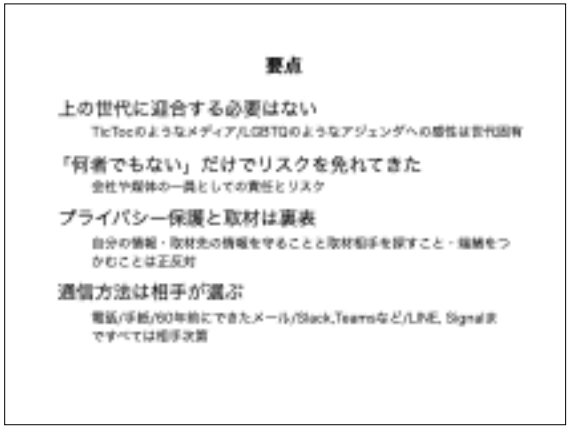
ツイッター上で新潟市の弁護士を中傷するなどの書き込みをした匿名の男が、新聞社の報道部長と判明。部長は懲戒休職。13年ごろから、著しく品位を欠いた表現で繰り返し投稿していた。
教訓：ネットの社会に匿名はないことを教育していない



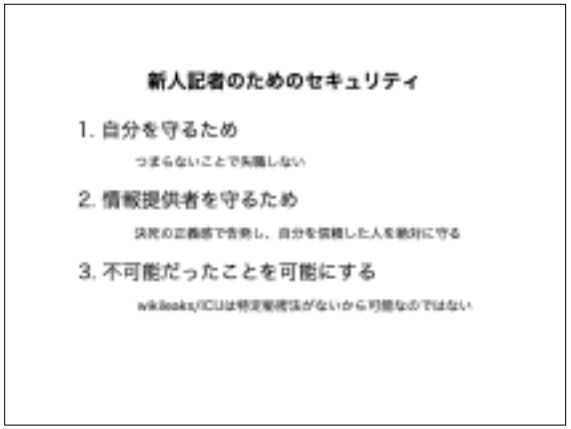
2003年の新城市会社役員誘拐殺人事件で、報道協定成立の３時間後に匿名掲示板に「新城で誘拐事件が発生し、1億円請求されている」「新聞社で働いている親からの情報」と投稿される。
教訓：SNSなら確実に投稿者が特定される。



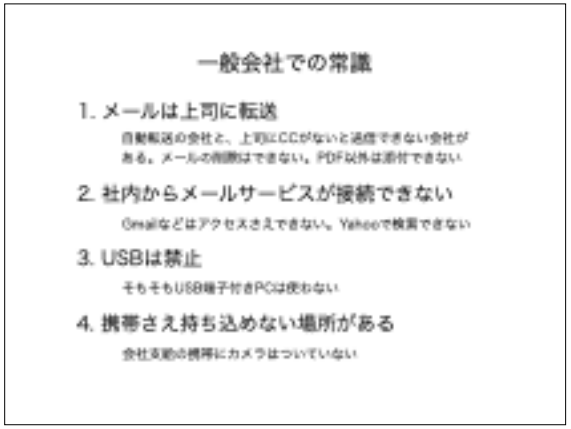
2018年4月、県警の報道用広報文を写真に撮り、知り合いの元暴力団組員にLINEで複数回送信していた。記者は停職１カ月。
教訓：通信には相手がいて、相手がセキュアである保証はない



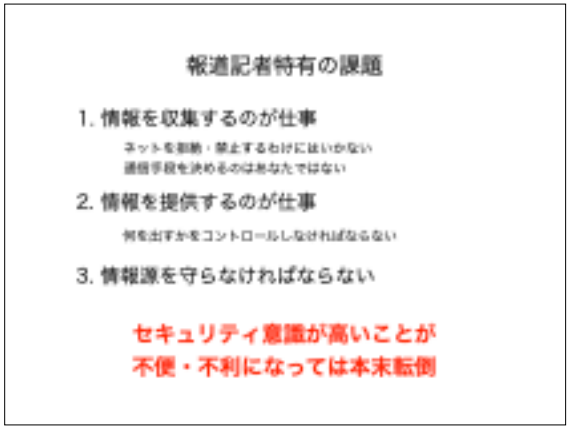
Nobodyだった皆さんにセキュリティ意識がないのは当然です。気にしていたら、GmailもFacebookも使えません。いわゆる「Nothing to hide」論です。昨年も「別にセキュリティなんて気にしない」と堂々と答えた新人記者がいました。問題は、nobodyである記者が接触する相手は、大抵の場合、somebodyであることです。



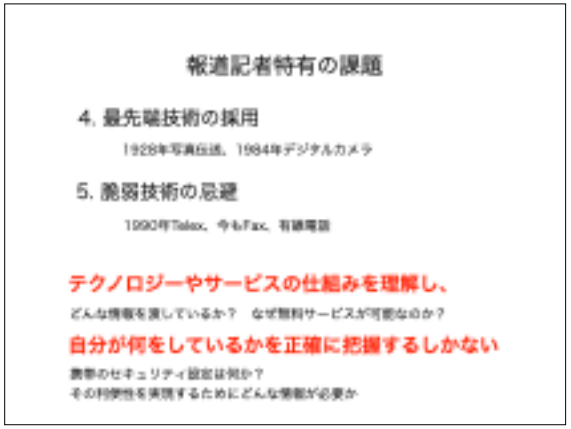
セキュリティに関する講習をする理由は３つあります。「自分を守るため」は、会社や取材先の情報を漏らしたりして、失職しないということです。失職しなかったとしても、記者としての未来はありません。「情報提供者を守るため」は、決死の正義感で告発し、記者としての自分を信頼した人を絶対に守るためです。「不可能だったことを可能にする」は、パナマ文書のような、完全匿名通信や巨大データの取得が可能になるということです。



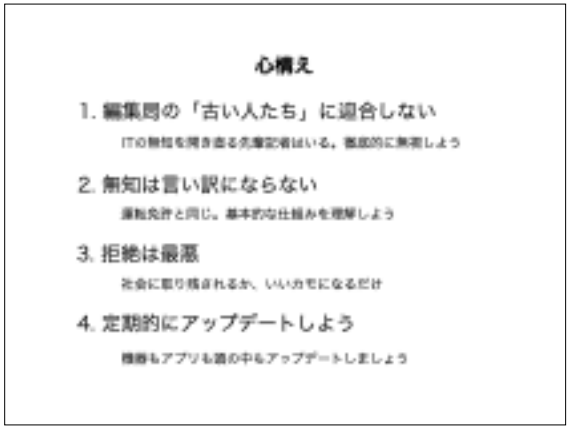
編集局は非常に自由ですが、無知である自由もあります。一般会社の常識を知らない人も多いです。例えば、米企業と商売をする会社は全メールをCD-Rなどに保存することが事実上義務付けられています。カメラ付き携帯の持ち込み禁止やUSBのないPCしか認めないのは、業界によっては常識です。社内でFacebookを開いたり、Twitterを見ることが許される会社は例外的です。



報道記者のセキュリティは、一般企業のように「禁止」では不可能です。電話番号やメールアドレスを秘密にすれば、広く情報は得られません。取材結果を公表するのがミッションですが、守らなければならない情報も同時に抱えることになります。この矛盾を乗り越える唯一の方法は、テクノロジーの仕組み、サービスの経済構造、情報の利用のされ方などを理解し、誰から何を守らなければならないかを主体的に考える必要があります。



テクノロジーに対するメディアの態度は微妙です。世界最先端の技術が報道で採用され、それが一般に普及していく過程と、最先端ではあっても脆弱な技術を忌避して古いテクノロジーを愛用する過程が並存しています。どちらが正しいというわけではなく、臨機応変に対応していかなければなりません。



講師の知る限り、定期的に記者向けのセキュリティ研修がある会社はありません。セキュリティが軽視されてきた理由は、先輩記者たちの無知・拒絶・開き直りです。新人記者の皆さんは彼らを反面教師として、ご覧のような心構えをしてください。デジタル社会を乗りこなすには運転免許が必要です。

写真というメディア（媒体）は100年以上の歴史がありますが、使われ方が全く変わりました。フラッシュが一発勝負時代には１枚の写真がピュリッツァー賞に選ばれました。みなさんは生まれたころの写真が「アルバム」にまとめられている最後の世代です。デジカメが普及した頃、データをパソコンに転送できないお年寄りのためにUSBアルバムが登場し、パソコンが得意な人はバカにしたものです。いまでは最も合理的なデータの保存方法です。（2019年5月の32GBメモリは430円）。ただし、データは10年は持ちません。なにもかも

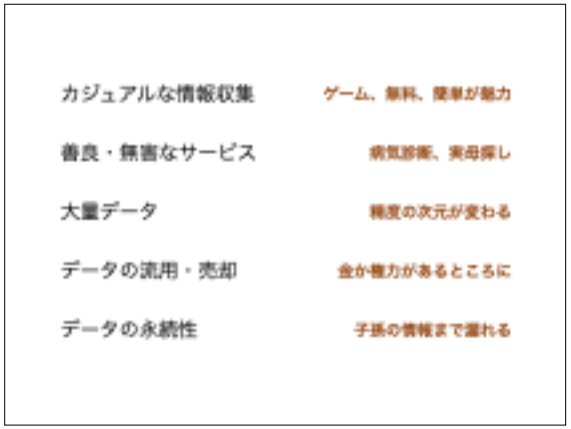
iCloudに入れるいまの赤ちゃんの写真は、何かのきっかけに失われてしまうかもしれません。

写真の技術革新は、報道の技術革新そのものです。それに従って記者の仕事も劇的に変わりました。

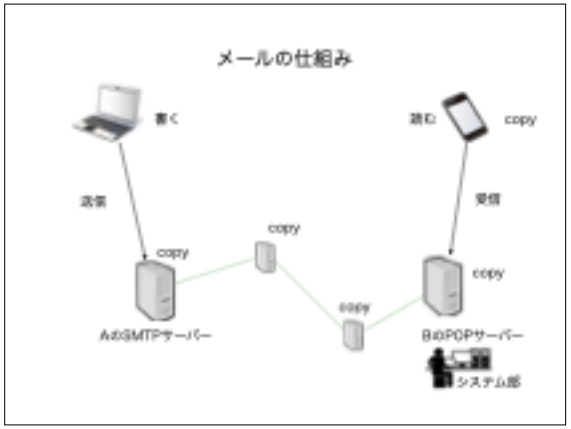
セキュリティ講習でメディアの話をしたのは、セキュリティが、テクノロジーそのものの発展と、その使われ方の変遷と無関係ではいられないからです。
ロンドンの選挙コンサルティング会社Cambridge Analyticaは、1人５ドルの約束で120問の質問に答えてもらい、その人の五大個人特質(Big Five factor)を計測した（32000人）。その支払いのためにFacebookのアプリにログインしてもらい、その際に「いいね」情報や本名、友人情報（5000万人分）を取得。そのデータから11州200万人の有権者の心理的特質を個別に推定し、選挙メッセージを

チューニングした。

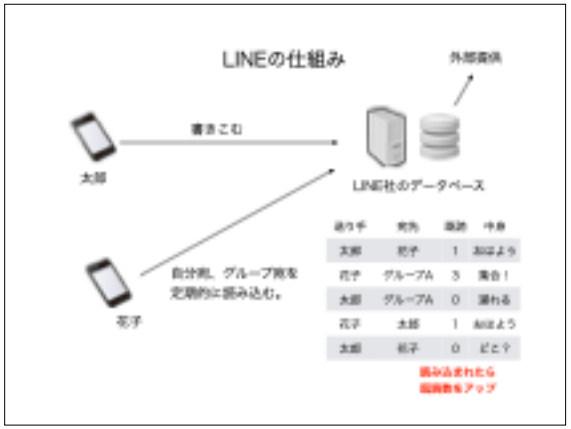
アメリカ西海岸で1974-86年に起きた60件以上の強姦殺人事件で、体液が冷凍されていた1980年の事件について、DNA情報をGEDMatch（里子が実親や親戚を探す遺伝子データベース）で調べ、10人以上の遠縁を発見。家系図を再構成して容疑者を絞り込み、ゴミからDNAを確認。元警官のJoseph DeAngelo容疑者を逮捕した。保険会社やMYCODE(DeNA)、23AndMe(Google)がどうして無料・格安のDNA検査サービスができるか、考えてみてください。



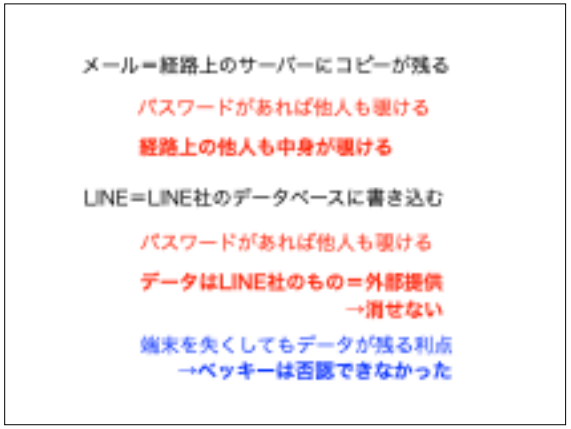
仕組みを理解しないと、自分が実は何をやっているのか、理解できません。たとえば、メールとLINEは何が違うのでしょうか？



電子メールは、ファイルのバケツリレー転送です。経由するコンピューターに大量のコピー（断片）が作られます。通常は削除されますが、方針次第で保存しておくこともできます。最後のPOPサーバーはユーザーによって削除されるまで何年でも保持します。その間、システム部の管理者は全員のメールを見放題です。



LINEの送受信は、LINE社のデータベースに対する書き込み、読み込みそのものです。削除は「削除扱い」にできるだけです。韓国資本のLINE社はデータを外部に提供すると明言しています。貴重なデータを削除するはずがありません。同社のエンジニアは、開始以来すべての書き込みをロストしていないことを誇っています。



社会に普及し、取材対象との連絡にも使われている以上、メールやLINEに背を向けることはできません。しかし、仕組みを知らないと、使ってはいけない場面で不用意に使ってしまうなど、重大な結果を引き起こすことになります。

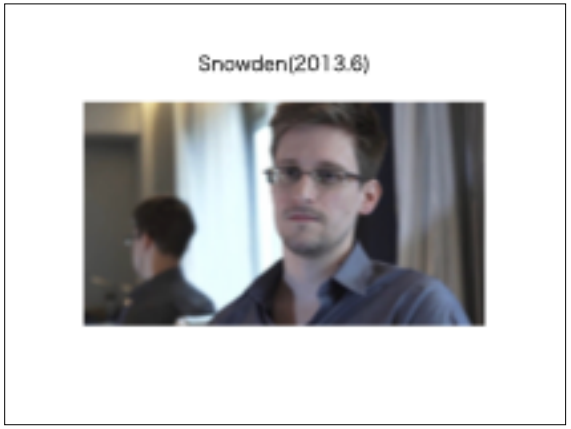
技術的な仕組みだけでなく、使い方・使われ方も十分に検討しましょう。実名か否か、相手があるか否か、正式な意見表明か暇つぶし・気晴らしか。それを使うことで得るものと失うものはその人の立場によって違います。例えば、Twitterは時に無名の人を有名人に引き上げますが、時に有名人を奈落の底にたたき落とします。
アカウントを持つ最大の問題点は、不用意な情報漏洩と、沈黙や無視さえ意味を持つと解釈されてしまうことです。

2017年5月、インディ500で佐藤琢磨が優勝したとき、“戦没者追悼記念日としてはuncomfortable”と呟いたデンバーポストの運動部記者が即日解雇されました。コロラドのアメリカ人の「つぶやき」としてはそれほど差別的とは思えませんが、社会の文脈上（スポーツ業界や東海岸メディア）では、そうは受け止められませんでした。SNSは「衆人環視で行う対面会話」をするのだと理解しましょう。決して不特定多数を相手にしてはいけません。

アメリカは、電子渡航認証ESTAの申し込みに、TwitterやFacebookのアカウントを記入するよう求めてきます。入国審査の理由は公開されませんが、2016年にはカナダの環境ジャーナリストがアメリカのパイプライン取材で入国を拒否されています。その是非はともかく、当局はソーシャルメディア上の言動もチェックしています。

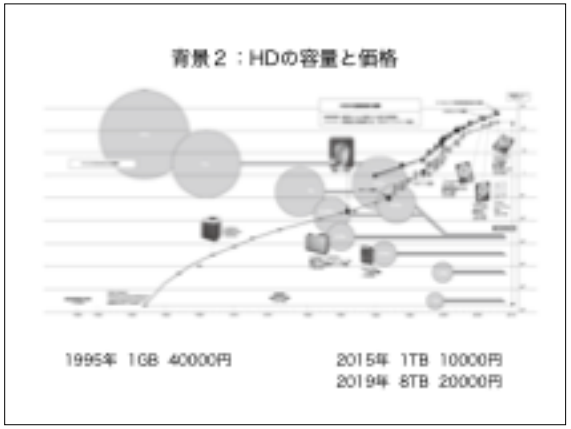
セキュリティに関心を払ってこなかった人のために、データ社会を体験してもらいます。GMailのアカウントを持っている人は、ログインしてmyactivityを開いてください。左上のメニューから「アクティビティ管理」を開き、Googleが自分に関して記録しているデータを見てください。これは、あなたが提供に合意していることになっています。赤面するだけならいいのですが、いったん被疑者になったらどのように解釈されうるか、想像してください。

セキュリティの現状を概観します。関心がない人にはSFのような話だと思うかもしれませんが、頭の片隅に置いてください。仕組み（技術）と運用（使い方）を結びつけて考えてください。



アメリカの記者がセキュリティに敏感になったきっかけは、2013年のSnowden事件です。エドワード・スノーデンは、NSA（国家安全保障局）が極秘で続けてきた個人情報監視活動を暴露した元CIA職員です。本や映画になっているのでご存知でしょう。（この資料で青い色で表示しているのは、彼が暴露したNSAのコードネームです）

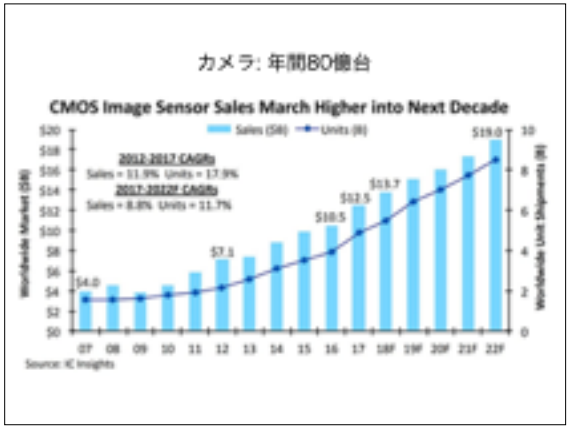
当局による情報収集が拡大した背景には、もちろん、2001年の9.11があります。直後に米国愛国者法が決まり、215条で「すべての人の有形物と、アメリカ人の電話のメタデータ」の収集が許可されます。2008年には海外情報監視法702条で、アメリカを出入りするインターネットバックボーンの監視が認められます。予算は年間１兆1000億円にまで肥大化しました。National Security Letters(NSL)というFBIが裁判所を経ることなく発行する行政的召喚状も認められ、Googleのメール、銀行の口座記録、Dropboxの中身を収集できるようになっています。



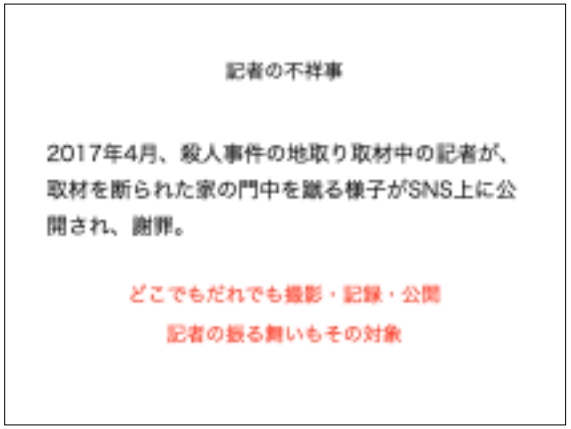
もう一つの背景はハードディスクの容量革命です。1995年に1GBが4万円だったハードディスクは2015年に1TB1万円以下まで安価になりました。民間の巨大なデータセンターが作られ、クラウドなら1ペタバイト（=1000TB）を年間1000万円で借りることができます。

アメリカ国内の電話の全通話を録音しても年間300PB、全アメリカ人を24時間録画しても年間2エクサバイトです。当局にとっては夢のようなことが技術的にも費用的にも可能になりました。できることはやるのが情報機関です。

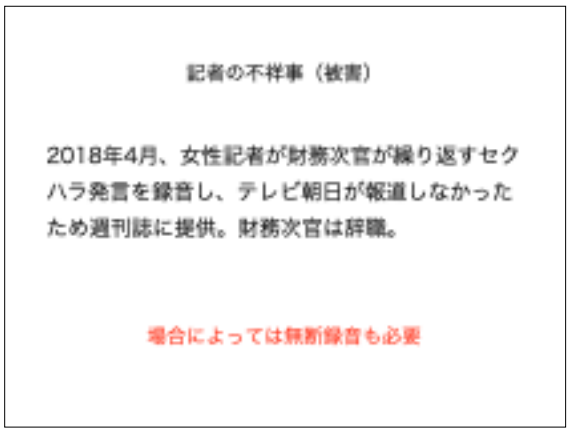
もう一つはメモリーの小型化です。1TBにはヒトが一生で聞き取るすべての音声情報が記録できます。



ヒトが全世界で2-3億人生まれるだけなのに、画像センサーは年間80億個も生産（当然消費も）されています。



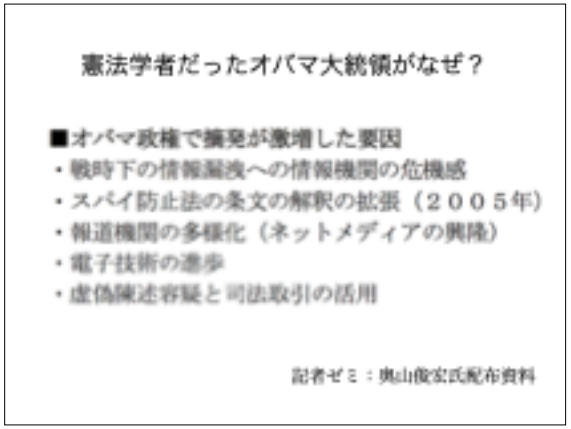
2017年4月、千葉県松戸市でベトナム人女児が殺された事件を取材していた共同通信記者がインターホン越しに取材を申し込んで断られ、門柱付近を蹴った。この様子がインターネットに公開され、住民に謝罪。

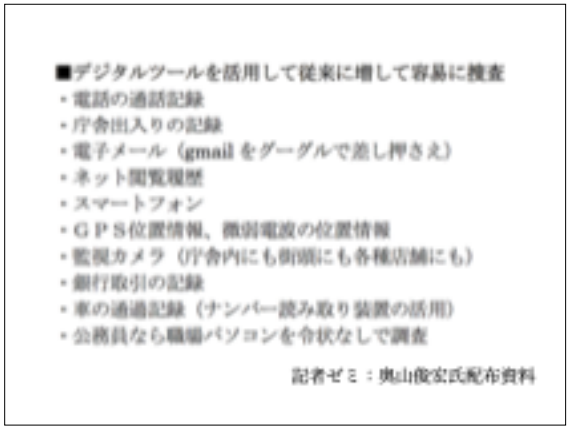


2018年、取材目的で福田氏と会食をするたびにセクハラ発言があり、自らの身を守るために録音、上司にセクハラの事実を報じるべきではないかと相談したが報道見送り。女性社員は週刊誌に録音の一部を提供。

NSAは2013年、ユタ州に12EBのデータセンター（1500億円）を建設しました。ちなみにGoogleは全世界のデータセンター合計で15EBの容量を持っています。

全データ保存は個人情報問題にとって革命的です。過去に向かってデータを遡れることで、実質的に法的規制が無効になるからです。





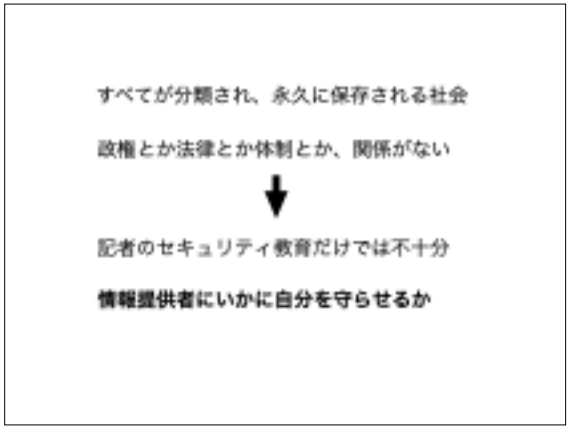
内部調査で自由にできる（令状がいらない）

■デジタルツールを活用して従来に増して容易に捜査

- 電話の通話記録
- 庁舎出入りの記録
- 電子メール（gmail をグーグルで差し押さえ）
- ネット閲覧履歴
- スマートフォン
- ＧＰＳ位置情報、微弱電波の位置情報
- 監視カメラ（庁舎内にも街頭にも各種店舗にも）
- 銀行取引の記録　　事実上自由に使える
- 車の通過記録（ナンバー読み取り装置の活用）
- 公務員なら職場パソコンを令状なしで調査

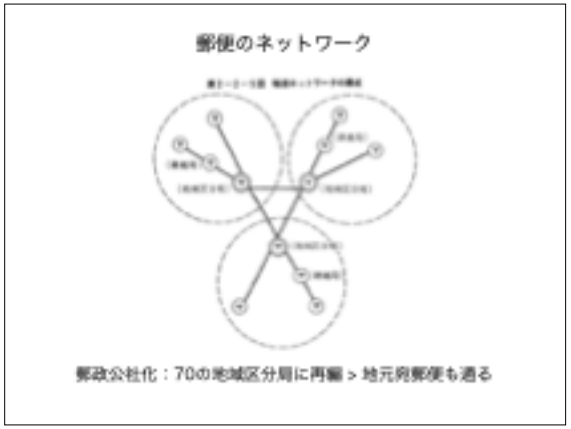
記者ゼミ：奥山俊宏氏配布資料

捜査関係事項照会



導入で紹介した通り、セキュリティは技術と使い方の双方から検討する必要があります。ここから、媒体別に注意点を説明します。

アナログの郵便でさえ、古き良き通信手段のままではありません。



国内の郵便ネットワークは、民営化されてから70の地域区分局に再編されています。郵便物は地元宛てのものでも必ず地域区分局を通るようになりました。そこで、郵便物は郵便番号を読み取るためすべてスキャンされます。

郵便番号は、機械で仕分けをするために1968年に導入されたものです。郵政省は（番号だけでなく）宛名すべてを撮影しています。テロ対策の一環で、報道機関に届く郵便物はX線スキャンもされています。日本でどの程度保存されているのかは分かりませんが、アメリカでは年間1600億通の郵便の表裏の画像を保存しています。全量保存されているということは、差出人不明の郵便物も投函場所と時間を検索できるということになります。

1979年のアメリカ大使館人質事件では、アメリカの外交官が大使館を放棄する際にシュレッダーで処分した書類を、イラン政府が女子高生を使って何ヶ月もかけて復元しました。

現在では、コンピューターを使って高速で復元できるようになりました。つまり、シュレッダーも無力化されつつあります。こうまでして復元されるおそれがあるほどの重要文書を扱う取材を経験することは恐らくないでしょうが、技術動向には関心を持ち続けてください。

ファックスが遅れるコピー機は保存する必要がある！

尾行

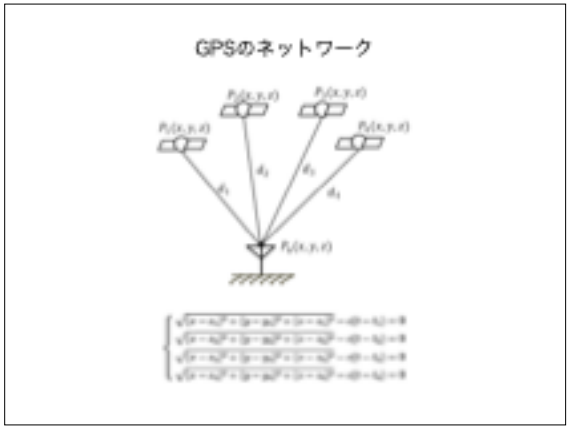
信じられないでしょうが、１人の尾行には20人が必要だと言われています。コストは月2000万円です。現代の尾行は非常に安価です。

Nシステム（1987）

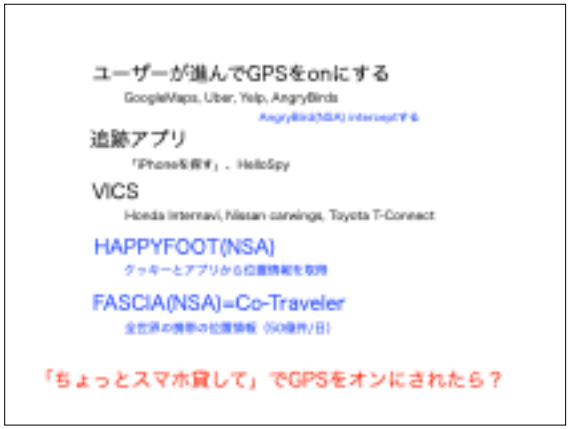
Nシステムは1987年に導入されました。当初は手配車両と盗難車の追跡が目的でした。2006年には愛媛県警の警官の私用PCから画像10万枚が流出しました。「一定期間後は破棄される」という警察の説明は嘘で、データは保存され、かつ、管理も甘いことが確実です。赤外線フラッシュを併用し、画像解析技術も格段に進歩した現在、ナンバーの自動読み取りエラーは非常に少なくなっています。どの記者の車も過去にさかのぼって検索可能です。

防犯カメラ

その他の人物トラッキング手法も開発されています。日本ではあまり話題になりませんが、ロンドンの街頭カメラ（100万台以上）の顔認識が有名です。FBIは5200万人分の顔情報データベースを保有しています。歩き方認識の研究も進んでいます。それぞれの精度は今ひとつですが、組み合わせて使われた場合、個人が検索可能になります。



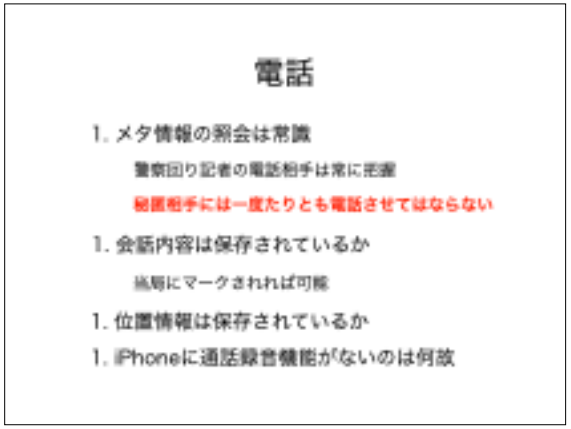
GPSは最も強力な尾行手段です。電波状態の悪い場合でも数十メートルの誤差で場所を特定できます。



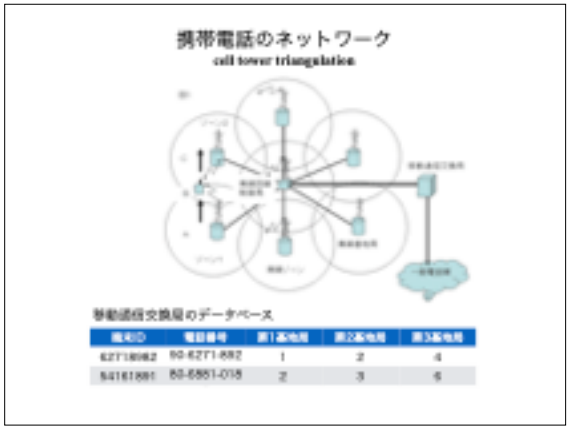
GPSはあまりに便利なため、ユーザーは自ら進んで位置情報を提供します。自動車もVICSという仕組みで自ら位置情報、運行情報を送出しています。NSAは、企業に位置情報の提供を強いたり、通信を傍受したりして、全世界の携帯電話の位置情報を毎日50億件収集していると報道されました。自分の携帯の設定→プライバシー→位置情報サービスを点検してください。あなたも提供しているはずです。

警察は令状なしで容疑者の車にGPS端末を設置して行動を追跡しています。最近の裁判で2006年から実施していたことが明かされました。読売新聞の報道で、広報や捜査書類にGPS使用の形跡を残さないように運用されていることが明らかになりました。警察回り記者の車を点検したことがありますか？

位置情報が全量保存されると、新しい検索も可能になりました。
NSAは、監視相手と地理的に交差した人を探す交差検索、同じ場所でoffになった携帯の所持者を探す密会検索など、アイデア豊かな検索システムを開発しています。

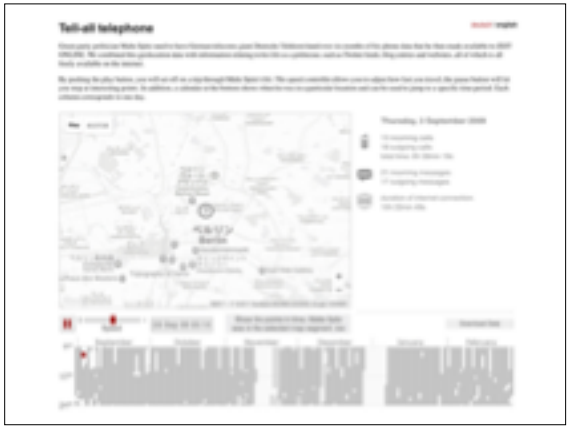


電話が盗聴されていることは常識です。アメリカで義務化（1994）されていることもあり、電話の中継機器には盗聴機能が標準装備されています。それでも、令状が必要だった「古き良き時代」の盗聴は、FBIですら通話相手が家族だったら電話を切ったと言われています。アフガニスタンやバーレーンなどの小国では、全通話録音システムが稼働しています。日本でも、どの電話番号でも東京で盗聴できるシステムが運用されています。



携帯電話は、自分の位置を絶えず基地局に報告して呼び出しを待つシステムです。最大３つの基地局を登録し、三角形の中にいることを交換局に知らせます（Cell Tower Triangulation）。

電源を入れている限り、一定間隔で電波を受信し基地局を確認し、基地局が変わるたびに位置を再登録します。新幹線に乗ると、全く使わなくても電池が急激になくなるのはこのためです。



電話会社はその位置情報をすべて保存しています。
この図は、ドイツの政治家Malte Spitz（緑の党）がドイツテレコムを訴えて、自分に関するすべてのデータ（半年分）を提出させたものを、ツァイト紙がインタラクティブ地図に表示したものです。ちなみに、ATTのSMS保存期間は７年です。

アメリカでは、位置情報を利用して広告を配信するベンチャー企業があります。
英国の防衛産業Cobhamは、呼び出し音を鳴らさないで電話をかけ、精度１メートルで位置を特定するBlind callシステムを開発しています。Sprint(米携帯電話会社)は、捜査機関への位置情報開示サービスを月間30ドルと定めています。信じがたいことですが、NSAは携帯電話のマイクを遠隔操作でonにできると言われています。

ミシガン州警察は2010年、令状なしで、労働争議予定地周辺にいた携帯電話のリストを携帯電話会社に要求しました。ウクライナ政府は2014年、キエフのデモの場所にいた携帯電話所持者に「あなたはデモ参加者として登録されました」というショートメッセージを送りました。NSAは最大29カ国で全通話にアクセス可能だと言われています。

IMSI-catcherという偽の携帯型・携帯電話基地局もあります。商品名はStingRay。携帯電話のIDと位置を取得し、可能であれば、簡易暗号モードを端末に提案して通話内容を録音します。（ただし、4Gシステムには対応していないそうです）

とはいえ、携帯電話を持たないという選択肢は想像できません。そこで、電波を外部に出さないように包み込む電磁シールドが売られています。
tinfoil-hatとは、宇宙人に脳を操作されないように被るアルミ箔の帽子のことですが、現代の我々には全く笑えません。

電子メールに添付されたファイルを開き、コンピューター・ウイルスに感染させてしまうのは論外です。添付ファイルはtxt、csv、pdf以外は絶対に開かないと決めてください。「お知らせ.pdf.exe」などに引っかかってはいけません。
おすすめは、編集局に「公衆便所PC」を置き、そこにメールを転送して開くことにすることです。

時々漏洩するパスワードのデータを見ると、多くの人が極めて単純なパスワードを使っていることがわかります。このデータは、ハッカーがパスワード推測に悪用します。

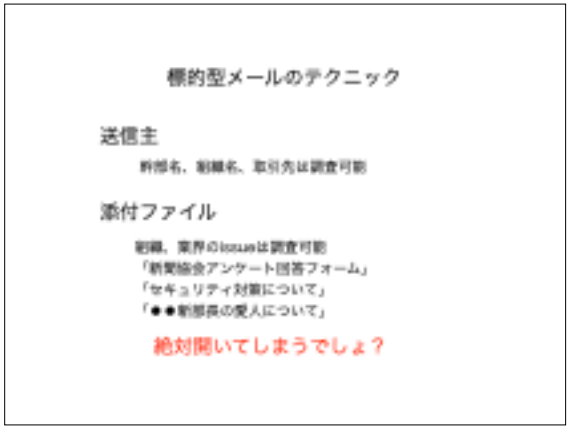
同じパスワードの使い回している場合、サイトAで漏れたパスワードがサイトBで使われる恐れがあります。単語・名前・単純な文は厳禁です。なお、複雑なパスワードを記憶する専用アプリがあります。

ソーシャル・エンジニアリングとは、純粋に技術的なハッキングではなく、出入り業者を装って社内に侵入したり、システム部員を騙ってパスワードを聞き出したりする「社会的ハッキング」のことです。データ漏洩の85%はソーシャル・エンジニアリングによるものだと言われています。システム部員の前でパスワードを打たされたことはありませんか？

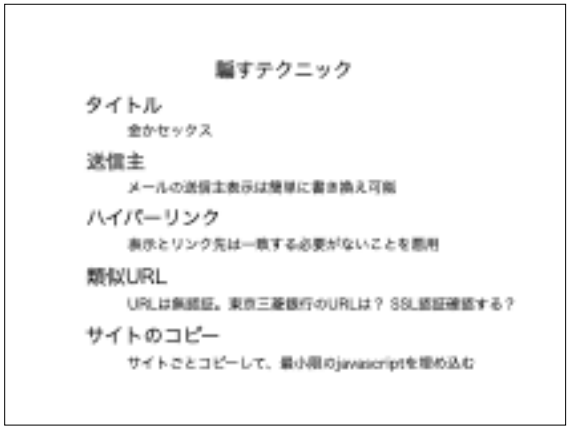
Phishingは、メールで利用者を偽のサイトに誘い込み、パスワードなどを騙し取る詐欺の手口です。最初のころは無作為メールで、100万人に1人でも騙されればペイする「バカ探し」でした。現在は「標的型メール」といわれる手法が流行っています。特定の個人、組織を狙い、周辺情報を駆使して騙すのです。

新入社員のみなさんは今後メールアドレスを名刺に刷ってまでも「配る」ことになります。利用しているサービス業者から早晩、アドレスが漏洩することもあるでしょう。悪意はなくても入力ミスで他人に使われることもあります。歳を取ればこのようなフィッシングメールが届くようになります。こんなメールに騙されるバカではないと誰もが思います。でも、初めて車を買った直後に「ETCが解約されます」というメールが偶然届けばだれもが不安に襲われます。出張のために航空券を買い、クレジットカードの限度額に引っかからないか、かすか

にでも心配があれば、偶然届いたメールを開いてしまいます。それがこの詐欺が消えない理由です。

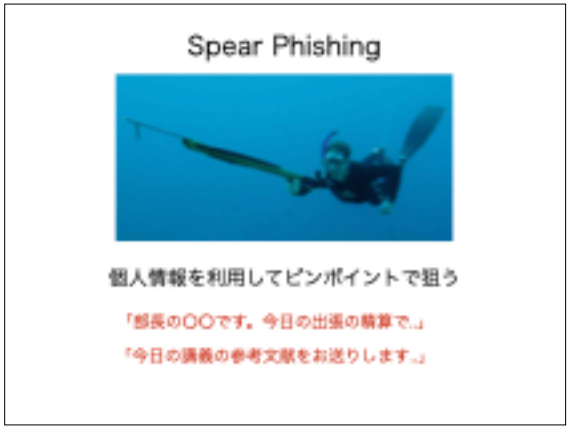


標的型フィッシングメールは非常に巧妙です。メールで送信主の名前を偽装することは簡単です。幹部や取引先、業界団体の名前は公知の事実です。新聞・雑誌を読めば業界の話題を想像することができます。「新聞協会アンケート回答フォーム」「セキュリティ対策について」「●●新部長の愛人について」などの添付ファイルを開いてしまう人は少なくありません。

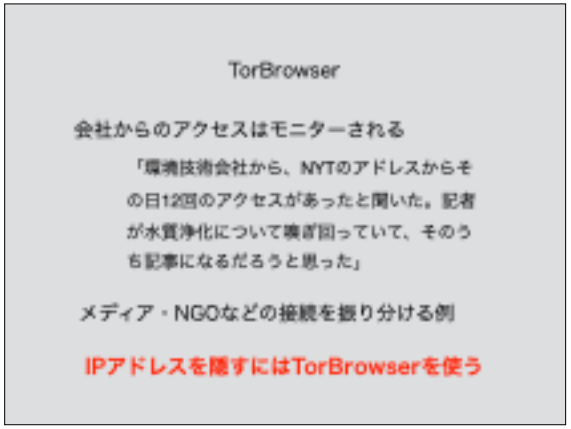


フィッシング詐欺は、このようなテクニックを使って、受信者の無知につけ込みます。本物そっくりのサイトをコピペで作り、パスワードを入力させる手法は、公衆無線LANの乗っ取りでも使われます。

会社がセキュリティ診断テストを業者に依頼することもあります。こんなことされたら開いてしまいますよね。



NSAは、OPEC幹部などを相手にメールでリンクを送り、サイトを閲覧したターゲットにウイルスを感染させる手法で、成功率80%を収めました。中国が開発したと思われるGhostNetというウイルスは、ダライ・ラマなど103カ国の政治家、経営者、記者のPCから見つかりました。中国特派員のパソコンは要注意です。



「環境技術会社から、NYTのアドレスからその日12回のアクセスがあったと聞いた。記者が水質浄化について嗅ぎ回っていて、そのうち記事になるだろうと思った」という裁判書面があります。一部の企業がメディア・NGOからの接続をモニターし、場合によってはページを振り分ける例があります。調査していること自体を隠すにはTorBrowserや外部回線を使う必要があります。製薬会社などは検索サイトの利用を禁じています。何をやっているか、バレるからです。

SNSは個人情報の宝庫です。

2011年、オーストラリアの法学部生が、Facebookに自分自身の個人情報の開示申請をしました。開示された1200ページ分の情報は、自分自身の書き込みだけでなく、リンクをクリックして閲覧したすべての外部ページのコピーも含まれていました。

PRISMはスノーデンが暴露したNSAのコードネームで最も有名なものです。Google, Facebook, Microsoft, Apple, Yahoo, Skypeなど９社から指定した人物の情報提供を受ける仕組みです。アメリカだから問題になっただけで、ロシアはネット上のほぼすべての活動を監視していると言われています。TOM-Skypeは Microsoftが中国向けに作ったSkypeです。「アムネスティ」など禁止語を打つと保存し、3万人のネット警察が監視します。

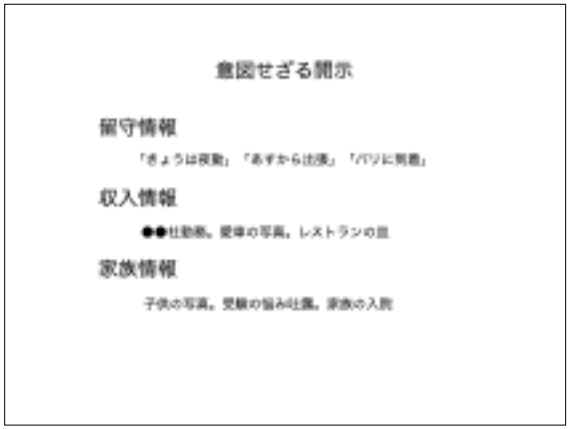
無線LANは、喫茶店やホテルなど、会社の外で使う時に注意が必要です。

自宅に設置したことがある人なら知っていますが、アクセスポイントを設置することは簡単です。このテレビ映像は、あるカフェで、カフェの名前を騙ったアクセスポイントを勝手に作り、接続した他の客のパスワードを盗み見る様子です。

２年前に明らかになったDarkhotelという仕組みは、高級ホテルの無線LANにウイルスを仕込み、泊まった企業幹部が接続PCへブラウザの偽のUpdate情報を発行し、ウイルス付きブラウザをインストールさせます。ウイルスはキーロガーになっていて、すべてのキー操作を盗みます。外出先でのUpdateは非常に危険です。

無線LANで騙すことは簡単です。実際にはハッカーのPCに接続しているだけでも、そのPCがインターネット全体のように振る舞えば、利用者は騙されてしまいます。PC上に作った偽のFacebookやGmailのサイトを信用し、パスワードを打ってしまいます。
第三者のLAN上でパスワードを入力したり、Updateを適用することは厳禁です。

我々は市民として、ましてや記者として情報の送り手でもあります。セキュリティを厳しくして外部からデータを守っていても、自ら情報を漏らしてしまうことがあります。「問うに落ちず語るに落ちる」場合です。



自分の何気ない書き込みが情報になりうることに注意しましょう。Facebookで外車を自慢し、海外旅行を自慢した結果、留守宅を狙われる事件もアメリカ・ニューハンプシャーで発生しています。ちなみに、犯人は、家主が帰ってこないことを確信してパーティーを始めたために逮捕されました。

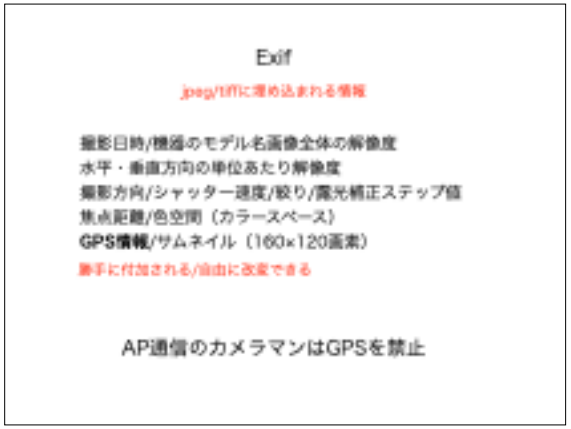
どうして選ばれなかったのか？

赤福事件、飛騨牛事件

信頼できるかどうか、普段から試されている

内部告発者の保護

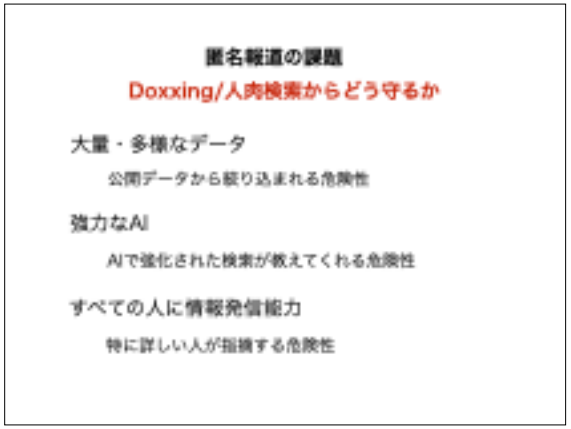
写真は要注意です。



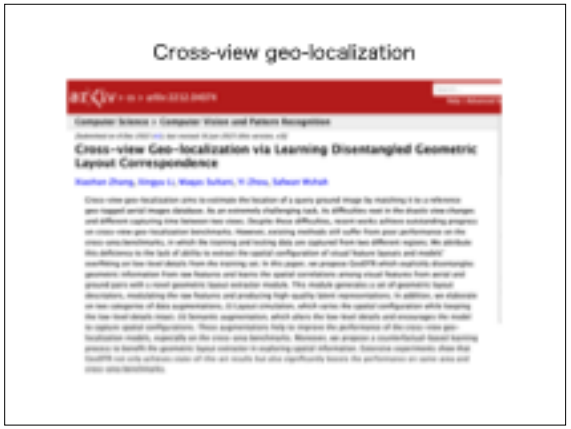
デジカメの画像にはExifというメタデータが埋め込まれています。問題は、iPhoneやプロ用カメラがGPS情報も埋め込んでしまうことです。ゴルフを取材するカメラマンにとってはありがたい機能だそうですが、その情報は自由に改変できます。このため、AP通信のカメラマンはGPS情報の埋め込みをオフにするように命じられています。

もっとも、場所が分かる写真を使ってしまえば、GPSをオフにしても同じです。
問題は「場所が分かる写真」は人によって違うことです。匿名の取材相手の手元だけを写した写真でも、一点ものの指輪なら個人が特定されてしまいます。それを知っている人が一人でもSNSで呟けば終わりです。文章でも同じです。「年子の妹と５歳下の弟がいる高１」は大きな街でも一人しかいないかもしれません。

左はマンションのベランダから撮った写真です。みなさんにとっては何の特徴もない都会の風景ですが、私には間違いなく名古屋市西区の光景です。右はモザイクを入れた成人式の写真です。呉服屋さんには恐らく住所も氏名も分かります。



匿名報道の課題は、doxxing/人肉検索から取材対象を守ることが難しくなっていること。Googleの最新AI、Geminiはストリートマップの写真を学習に使っていると言われています。



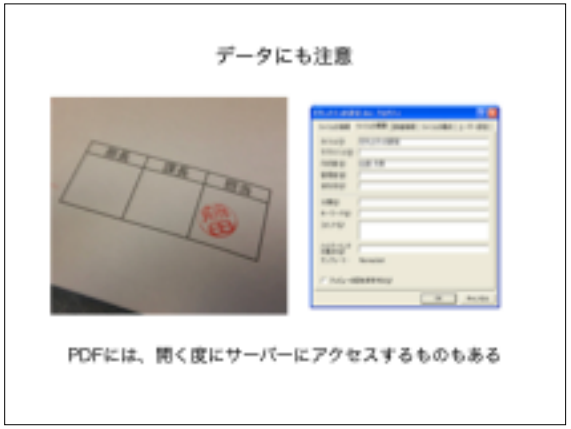
Cross-view Geo-localizationは風景写真とマッチする地形を空撮・衛星データから検索する技術。

捏造が発覚した理由（取材相手の抗議）は全く想像外。

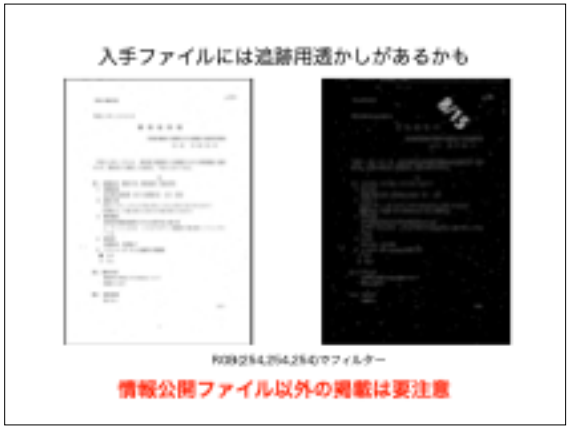
なお、写真を否定的に捉える必要は全くありません。
ワシントン大学の研究者は、ホテル宿泊者に部屋の写真をアップロードすることを呼びかけ、児童売春の売り込み写真の撮影場所を特定するプロジェクトを進めています。

ホノルルマラソンでは、沿道で撮影された写真から突き止められたゼッケン番号と参加者データベースが照合され、参加したアダルトビデオ女優の本名が公表されてしまった例があります。

徳島県警の鑑識課員は、写真に映った被害者の、瞳に反射した容疑者の姿を見つけました。要は使い方次第です。



いわゆる西山事件では、決済印から漏洩部署が特定されました。
ワードの文書には、作成者・管理者情報が埋め込まれています。PDFには、開く度にサーバーにアクセスするものがあります。誰が閲覧したか、追跡する機能です。ファイルを開けるときは、絶対にオフライン（ネットに繋がっていない状態）にしましょう。



何気ない画像にも追跡用データが埋め込まれているかもしれません。
表示の例は、RGB(254,254,254)の画素だけを抜き出した例です。入手したデータをそのまま公開するのは危険です。十分に恣意的な加工を必ず施しましょう。

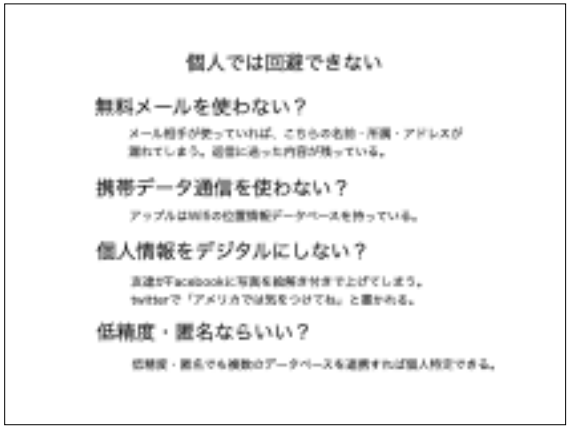
セキュリティとは関係ありませんが、記者の心情として「暗号化されて送られた情報は真実に違いない」と思ってしまうことにも注意してください。文書だけでなく写真も映像もフェイクかもしれません。見分けることが不可能なほど精巧なCGが個人で制作できる時代です。米CBSのダン・ラザーを失職させたキリアン文書は、Microsoft Wordで印刷した紙を何度もコピー機にかけて作った「偽古文書」でした。

パソコンには自分のPGP鍵だけでなく、取材先の情報も入っています。ゴミ箱を空にしただけではファイルは消えません、ただ見えなくなるだけです。買い替え・廃棄する時、まだ動いているなら、専用のソフトでディスクを完全に消去してください。起動しなくなった場合はハードディスクを自分でハンマーで壊してください。中古で売るのも、業者任せも論外です。

IT企業がプライバシーを守ってくれると期待する人がいるかもしれません。セキュリティを重視している企業であることを強力にPRしているからです。しかし、彼らにその気はありません。グーグルは「知られたくないことがあるなら何もしないことだ」と言っています。中間がないのです。

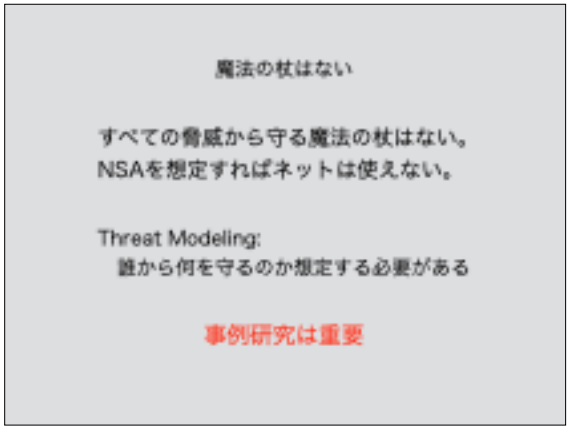
当局の情報提供要求に抵抗した企業もあります。しかし、Ciscoは輸送中のルーターに細工されました。暗号開発のRSAはバックドア付き乱数発生プログラムを強要されました。これらは氷山の一角で、全貌は分かりません。すべての交渉は秘密にするよう法的に命じられているからです。NSAは、製品の初期設定を甘めにするよう企業に要望したり、暗号の国際会議で民間人を装って、強度の低い暗号を提案したりしていました。国家の安全保障という名目に逆らえる民間企業はほとんどありません。

OSやソフトには、情報漏洩のBug（欠陥）もあります。意図的なBackdoor（裏口）もあると言われています。Backdoorを指摘されてもBugだと言えばいいので、すべてが闇の中です。ウイルス対策ソフトがウイルスではないかと疑っている人もかなりいます。

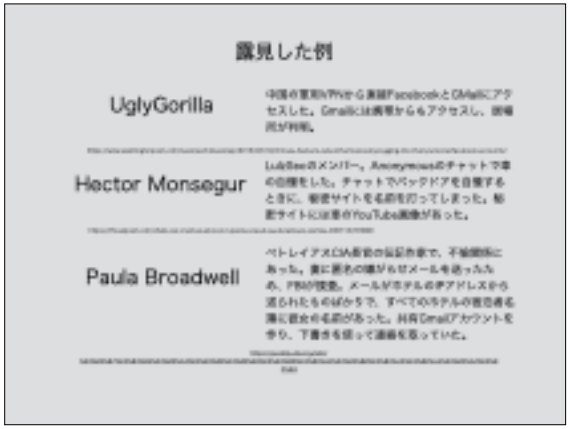


ここまで説明してきましたが、セキュリティ上の危険を個人で回避できることは限られています。通信には相手があるからです。暗号メールで送った内容を通常メールで丸ごと返信されたら水の泡です。これが、セキュリティを個人任せにせず、組織として取り組む理由の一つです。

現状を「怖い」と避けるのは最悪です。いわゆる盗聴法の賛否の議論とは別の次元で、自ら守ることができることは自ら守るべきです。
フリン大統領補佐官辞任のきっかけは、FBIの盗聴のリーク情報です。現場の記者は、「けしからん」と批評するより、抜いてくるべきです。



【時間があれば】すべての脅威から守る魔法の杖はありません。NSAに監視されていると想定すればインターネットは使えません。誰から何を守るのか想定して、対策を決める必要があります。これをThreat Modelingといい、システム部の仕事です。われわれができることは事例を追うことです。ネット担当記者はそれを報じることも必要です。



【事例】UglyGorillaは中国のハッカーです。中国の軍用VPNから直接GMailにアクセス。Gmailには携帯からもアクセスしてしまったため居場所が判明しました。Paula Broadwellはペトレイアス CIA長官の伝記作家で、不倫関係にあった。妻への嫌がらせメールは、ホテルのIPアドレスから送られたものばかりで、全ホテルの宿泊者名簿に彼女の名前がありました。長官と共有Gmailアカウントを作り、下書きを使って連絡を取っていました。

【事例】2013年4月、APのツイッターが乗っ取られ、ホワイトハウスで爆発という偽ニュースが流されました。担当記者に同僚を装ったPhishingメールで「この記事を読め」と送り、パスワードを打たせる手法でした。

【事例】FBIが、情報漏洩事件の捜査でニューヨークタイムズ記者の信用情報、銀行記録、電話、旅行記録を入手していたという記事です。情報リークが問題になった時、当然、記者が犯人探しの有力捜査対象になります。

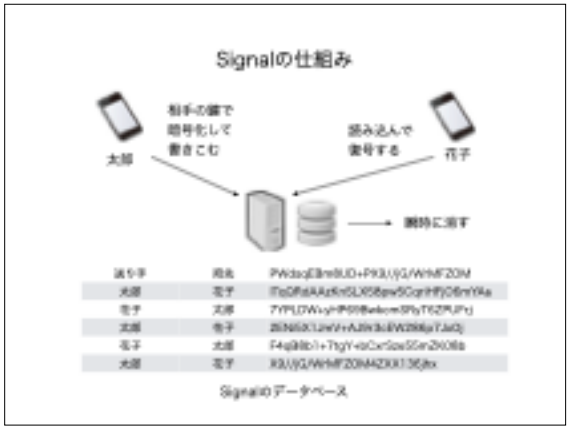
【事例】シリアの内幕を描いたドキュメンタリー映画の監督がPCを押収され、保存されていた資料や映像から大量のシリア国民が逮捕された事例です。

【事例】2016年３月、米司法省は、アメリカの銀行とダムにサイバー攻撃を行ったとしてイラン人７人を訴追しました。

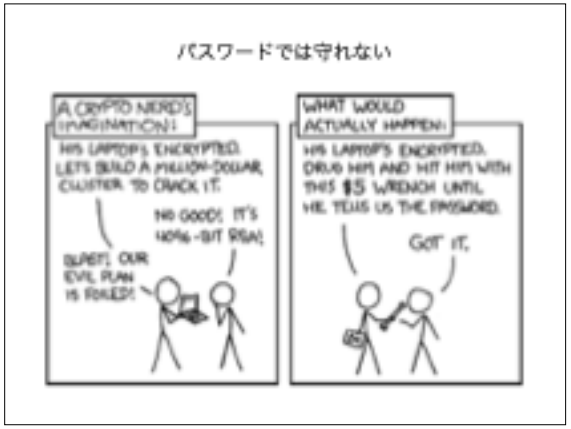
【事例】Tickと呼ばれるグループが、10年前から日本のテクノロジー企業や放送機関のネットワークにトロイの木馬（Daserf）を仕込み、社内のメールやプレゼン資料を盗み出していました。

【事例】2016年５月、ロシアのハッカーが、Gmailや米Yahooメールのパスワード２億7200万件分盗み出し、売りに出されました。

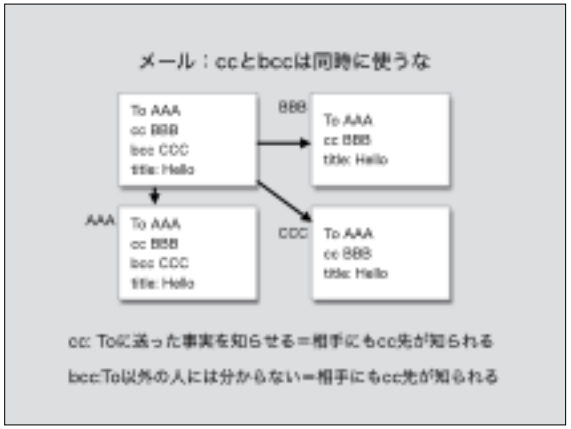
実習として、PGPメールとSignalを使ってみましょう。PGPメールの使い方は別冊子を参照してください。PGPの唯一の弱点は、パスフレーズの漏洩です。そこでSignalで通信してみましょう。Signalも公開鍵暗号による通信です。PGPメールとは違い、双方の携帯以外にはどこにも保存されず、時限付きのメッセージも可能です。（ここで実習。実際に講師と連絡する）



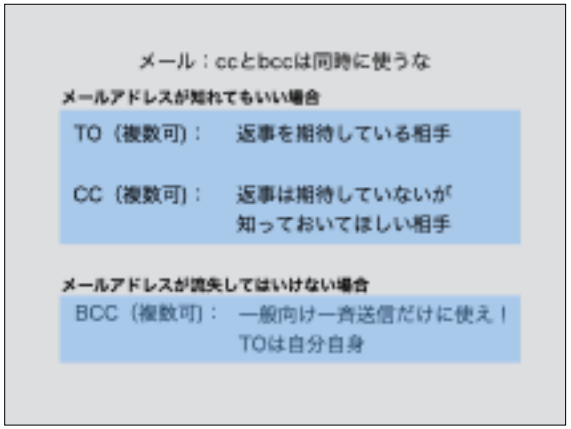
【参考】Signalは公開鍵暗号を使ってメッセージを交換します。サーバーはメッセージ内容を保存しません。保存しても意味がないからです。一度消えると本当に消えてしまいます。アメリカでデータが押収されたことがありますが、最直近のメッセージが送られた時間しか得られませんでした。



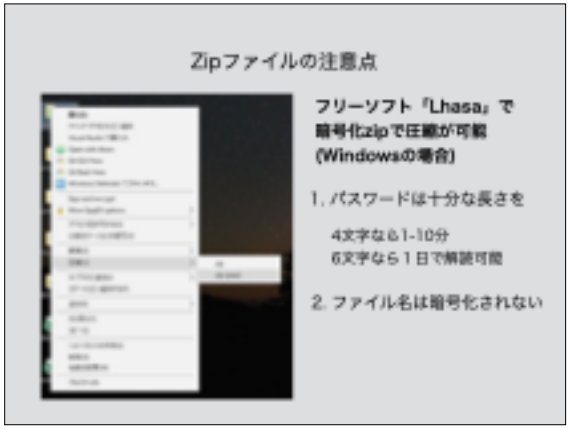
【参考】これは、100万ドルのシステムで暗号を解くよりも、5ドルのレンチで脅せばよいという、有名な漫画です。本当に情報提供者を守るには、記者にも暗号を解けなくする必要があります。一つの例は、情報提供者が記憶不能な程度に長いパスワードでZIP暗号化したものを、PGPメールで送り、直後に時限付きSignalでパスワードを送るという手法です。（ここで実習。講師からZIPファイルを添付したPGPメールと、Signalでパスワードを送る）



【参考】メールのccとbccの使い方について研修を受けたことがありますか？読者・視聴者への連絡に一斉メールを使い、全員にメールアドレスを知らせてしまう事例が後を絶ちません。



【参考】ルールを明確にしましょう。
①通常はbccを使わない
②一斉送信の場合は、必ずTOを自分自身にし、すべてをBCCにする（CCと併用しない）



【参考】Zipファイルの注意点

Zipファイルは、複数のファイルが入ったフォルダを丸ごと圧縮したファイルです。Windowsの場合、Lhasaというフリーソフトを使うと、簡単にパスワード付きZipを作ることができます。パスワードは15-20文字程度の長さにしないと安全ではありません。また、内部のファイル名は暗号化されません。暗号化されるのは、あくまでファイルの中身だけです。

一部の企業では、添付ファイルが自動で暗号化Zipファイルに変換されるサービスが使われています。メールを送ると、直後にパスワードを知らせるメールが追伸される仕組みです。誰から何を守っているのでしょうか？
