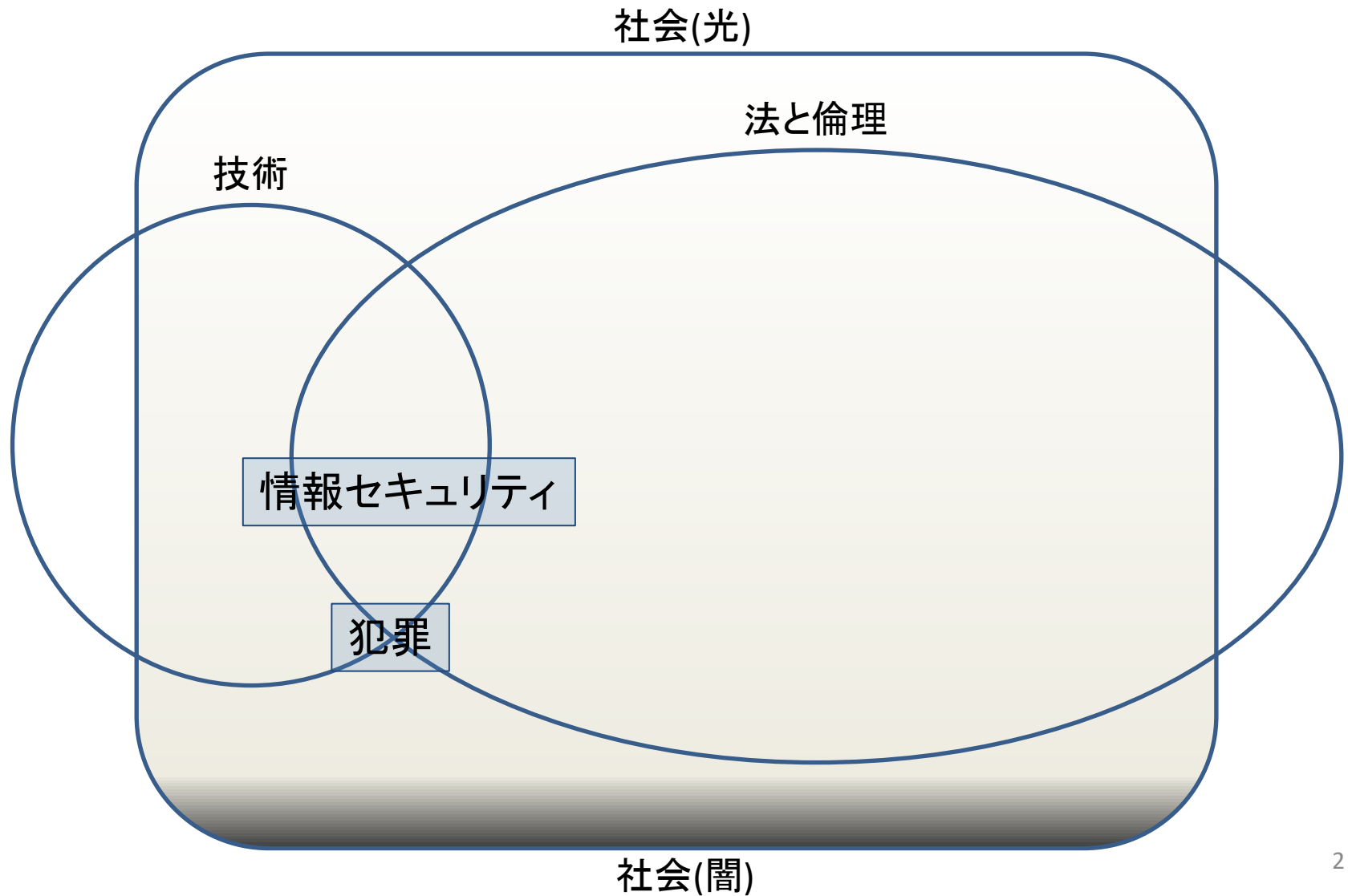


情報セキュリティと情報倫理

第7回 コンピュータ犯罪

2022/11/11

今日の内容



教科書・参考書

- 参考書
 - 情報セキュリティ概論
 - 4.マルウェア
 - 11.インターネットでのトラブル
 - IT社会の法と倫理
 - 7章 コンピュータ犯罪

歴史は繰り返す

- 電話の登場

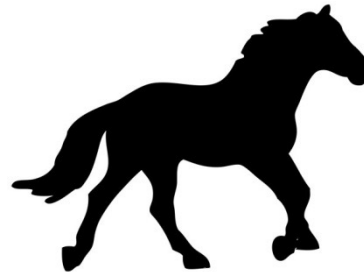
- 電話が犯罪に利用される



- 車の登場

- 強盗の逃走手段が馬から車に

犯罪＝技術×人



技術それ自体は意図を持たない

情報技術の影響

- 従来からある違法行為の助長
 - 詐欺(だまし取る)
 - 横領(他人または公共のものを不法に奪う)
 - 窃盗(他人の財物をこっそりぬすむ)
 - 文書偽造,破壊行為,営業妨害,...
- 新しい形態の違法行為
 - 不正アクセス(無権限アクセス)
 - ウイルス作成罪

Q: デジタル万引きは犯罪か？

- 本を盗んだわけではないが・・・
 - － 窃盗の延長？



子供にどう説明する？

今日のトピック

- サイバー犯罪の諸相と問題解決
 - ネットワーク利用犯罪
 - さまざまなネットトラブル
- 最近の事例
 - 大規模DDoS攻撃
- セキュリティの原則
- コンピュータ犯罪の事例

ミニレポート

- 「コンピュータを使った犯罪にひっかからない為に心がけるべきこと」を、コンピュータやインターネットにあまり詳しくない人（例えば、親戚の子供、自分の親または知合いのおじさん、おばさん）に説明するなら、どういう説明をするのが適切かを考え、その説明内容を簡潔に示しなさい。
- 提出先: Moodle
 - <https://moodle.cis.kit.ac.jp/mod/assign/view.php?id=230358>
- 提出期限: 次回講義開始時

ネットワーク利用犯罪

犯罪行為等	関連する法律等
出会い系サイト関連犯罪	児童売春・児童ポルノ禁止法 青少年健全育成条例
ネット犯行予告	業務妨害罪, 脅迫罪
誹謗・中傷	侮辱罪, 名誉棄損罪
わいせつ物頒布	わいせつ物陳列罪, 猥褻物販売目的所持罪
著作権侵害	著作権法

- 行為自体は昔からある
- 高度な技術は不要

出会い系サイト関連犯罪

- 面識のない男女が出会う
- 未成年の被害が多い
 - 売買春、暴行、窃盗、殺人
- 出会い系サイト規制法(18才未満の利用禁止)
 - SNS, ブログなどでの子供の被害は残る

使用制限も含めた教育が必要

ネット犯行予告

- ネット上で予告するだけでも犯罪
 - 2ch小女子事件(2008)
 - 「明日午前11時に丹後小学校で小女子を焼き殺す」
 - 小女子は(コウナゴ)のことで冗談のはずが...
 - [Twitterバスジャック予告事件\(2011\)](#)
 - 「明日、午前9時36分 品川行きのバスをジャックする。みんなみんな殺して肉の塊にしてやる。」
 - 実は兵庫県に住む中学生の少年(15)
 - 「反響の大きな書き込みをすることでフォロワーを増やしたかった。勉強のストレスも発散したかった」

ネット犯行予告(続き)

- パソコン遠隔操作事件(2012)
 - 犯罪予告の書き込みにより4名を逮捕
 - パソコンの送信元IPアドレスが根拠
 - 実際は真犯人がPCを遠隔操作していた
 - PC遠隔操作事件で、警察は“完敗”！

侮辱・名誉棄損

- 「公然と」相手の名誉を損なう事実を述べる
 - － 公然：不特定・多数人に対して
 - － 名誉を損なう：客観的な社会的評価を落とす
- SNS上のやりとりも「公然」に該当する

わいせつ物頒布

- わいせつな文書、図画、電磁的記録に係る記録媒体その他の物を頒布し、又は公然と陳列
 - Webサーバ上に該当データを掲載
 - ファイル交換ソフトで気付かずに配付
- 国による法律の違い
 - 日本では違法でも他の国では合法(逆もある)
- 子供の保護
 - フィルタリング機能で有害Webサイトを遮断

著作権侵害

- 複製権・公衆送信権の侵害
 - 違法アップロード
- 違法ダウンロード
 - 違法アップロードされたものと知りながらダウンロードすると違法
- TPP(環太平洋連携協定)の影響
 - 保護期間: 作者の死後70年(2018年末より)
 - 著作権侵害の一部非親告罪化

ネットトラブル

- ネットいじめ
- ネットが発端となった暴行事件
 - 佐世保小6女児同級生殺害事件(2004)
 - ネット掲示板の書き込みが引き金に？
- セク스팅グ(sexting)
 - 自分の裸体の写真や動画等をやり取りすること
 - ネット流出や元恋人からのいやがらせ
 - 子供は事の重大さに無自覚
 - 男女ともに被害に遭う可能性

セキュリティの原則

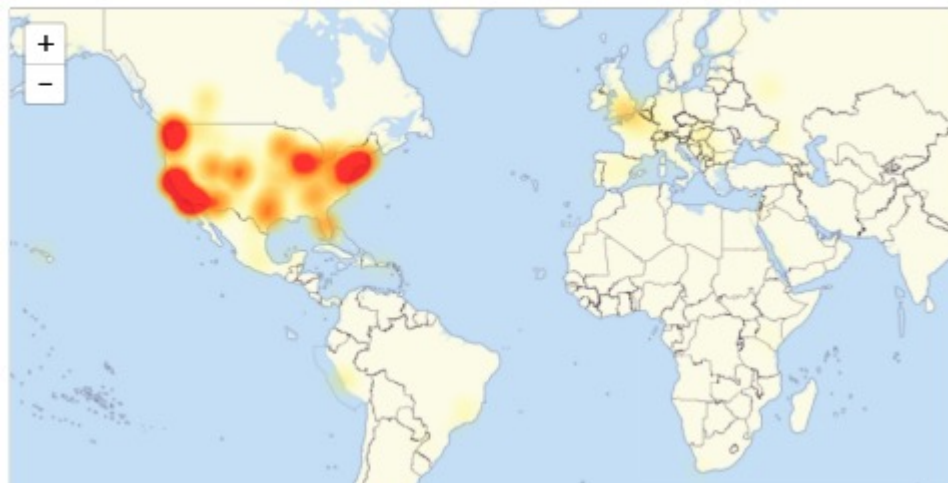
- 桶の理論
 - 最も弱い部分がセキュリティ水準を決める



大規模DDoS攻撃(分散サービス停止攻撃)

- 米DNSサービスに大規模DDoS攻撃で米国でTwitterやSpotifyが長時間ダウン(2016/10/22)

Level3 outage map



出典:<http://tinyurl.com/ht2nye5>

- DNSへの大規模DDoS攻撃、関与のIPアドレスは数千万と判明

何が起きたのか？

- 攻撃されたDyn社の調査結果(2016/10/26)
 - IoTマルウェア「Mirai」に感染した数千万台のデバイスから攻撃
- 大規模DDoS攻撃は防犯カメラが踏み台に、中国メーカーがリコール表明(2016/10/25)
 - 管理者のパスワードが固定で変更不可
- 史上最大級のDDoS攻撃に使われたマルウェア「Mirai」公開、作者がIoTを悪用
(2016/10/04)

現在の状況

- 攻撃用の知識・技術はすぐに利用される
 - ツールの公開から攻撃まで3週間
 - ゼロ・デイ(zero day)アタックも
- インターネット大手企業でも防御しきれない
 - 侵入はされないがサービス停止
- 弱い箇所が狙われる
 - 初期パスワードが修正されないままの機器
 - 特定企業・個人に対する標的型攻撃

ビデオ

- デモで知る！ 標的型攻撃によるパソコン乗っ取りの脅威と対策
 - <https://www.youtube.com/watch?v=dSWrKh5FHKA>
- そのメール本当に信用してもいいんですか？
～標的型サイバー攻撃メールの手口と対策～
 - <https://www.youtube.com/watch?v=5K9U0-ASQM8>
- ランサムウェア「WannaCry (WannaCryptor)」感染実演デモ
 - <https://www.youtube.com/watch?v=duN9dYG4q3s>

セキュリティが脆弱になる理由

- 現場へのプレッシャーでセキュリティが低下
 - 20年間「00000000」のままだった核ミサイル発射コード
 - 詳細原文(英語)は[こちら](#)
 - 誤射防止のため「大統領から伝えられる秘密コード」
- 当時の背景
 - 冷戦状態。「撃たれる前に撃つ」の時代。
- 現場で起きていたこと
 - 「確実に核ミサイルを発射できるよう」に00000000に設定
 - 「00000000」から変えないよう現場指導

厳しくするだけでもダメ



パスワード変更の例



「初期パスワードは必ず変更してください」
「パスワード忘れたら手数料1万円がかかります」

初期パスワードは危険
新パスワード忘れてもダメ

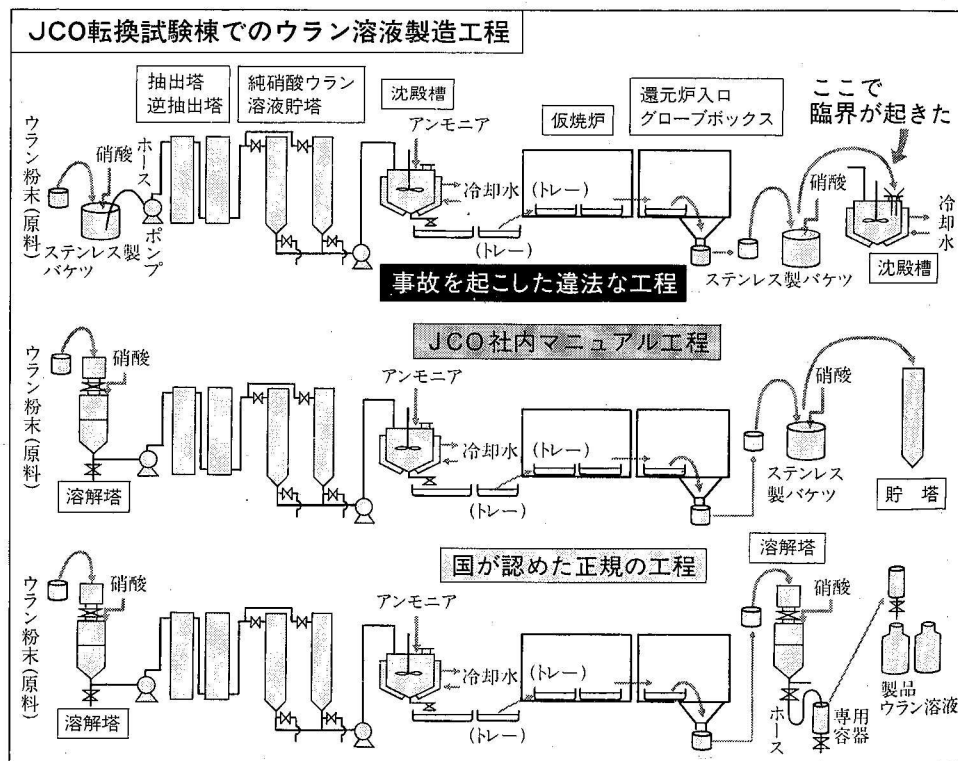
パスワード忘れたら困るなあ。
手帳に書いておこう。



東海村JCO臨界事故(1999)



- ウラン溶液が臨界状態に→作業員2名死亡
 - 正規の工程とは別の裏マニュアルもさらに無視



- 貯塔での作業は時間がかかる
翌日に間に合わせるため沈殿槽利用
臨界量以上に溶液を投入

背景

- 当初、納品1回あたり取扱量は臨界量以下
 - 原理的に安全
- 10回分を1回で納入するよう契約変更
 - 液体10ロットでの納入に変更
 - ppm単位で均一であることを要求
- 当時のJCOの経営状況
 - 売り上げ大幅減少
 - 人材流出

教訓

- 技術・規則だけではセキュリティは守れない
- 人間の振る舞いを考慮することが不可欠
 - 強いプレッシャーは規則違反の動機付け
- 最も弱い部分がセキュリティ水準を決める
 - 危険の存在を知らないとルールは無視される
 - 全体の底上げが不可欠

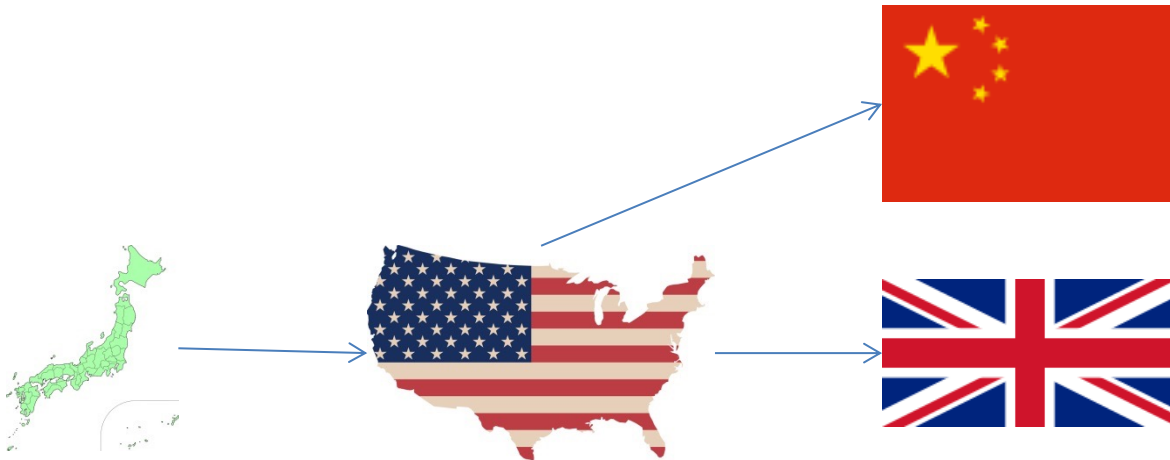
コンピュータ犯罪の事例

コンピュータ犯罪の類型

- 犯罪者による類型
 - インサイダー
 - 従業員 など
 - アウトサイダー
 - クラッカー, 競業者, 犯罪者集団 など
- 被害程度による類型
 - 実害なき不法侵入
 - 損壊行為, 窃盗, 恐喝, 重要サービスの停止

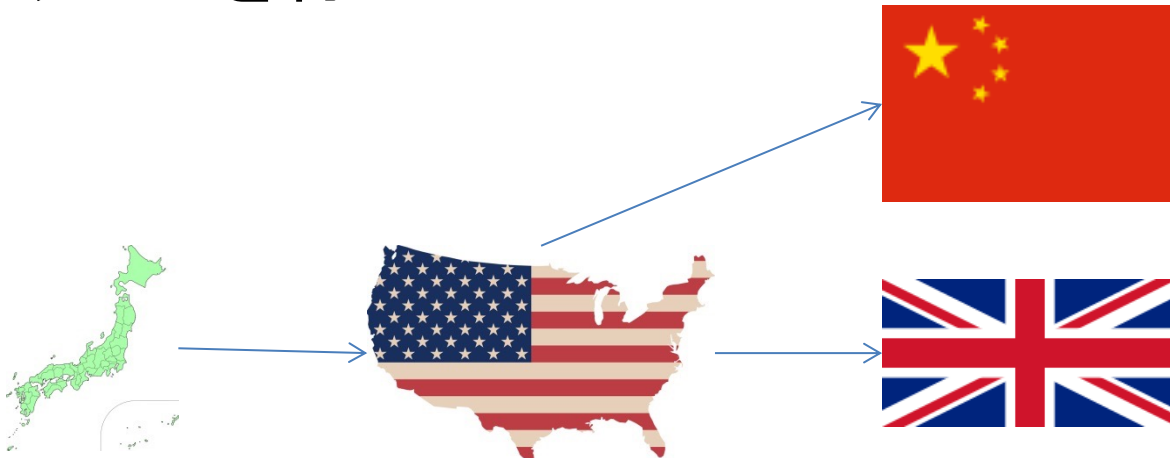
コンピュータ犯罪の特徴

- ネットワーク経由（場所の自由度が高い）
- 匿名性が高い
- 物理的ではない犯罪の場合が多い



Q:犯罪が行われたのはどこ？

- 日本にいるものが
 - 米国にあるコンピュータにログインし
 - ネット経由で英国にあるファイルを盗み出し
 - 中国にあるコンピュータに保存するために無権限アクセスを行った



競業者による攻撃

- 企業の重要な情報
 - 新製品, プロダクト・マーケットリサーチ, 顧客リスト, 価格ポリシー ...
- 産業スパイ
- 潜入, 盗用, 文書コピー
 - 情報化によりコンピュータネットワーク経由で
 - 情報量が大きく, 痕跡も追いにくい.
- ソーシャルエンジニアリング
 - 人間の心理的な隙につけ込んで情報を入手
 - 社内の誰か(上級職)になりすました電子メール
- 特定の個人や団体を対象: スピア型 or ターゲッテッド型

横領:雇用者をペテンに

- 横領(他人または公共のものを不法に奪う)
 - 委託された者が, 委託された財産を不正に着服
- 多くは, インサイダーによる犯罪
 - 特別な知識・技術は不要
 - 財務処理の複雑さ
 - コンピュータの複雑さと匿名性

横領や窃盗のパターン

- 保険会社の従業員が偽保険証券をでっちあげ、保険会社に保険金を請求する
- 従業員が他の銀行の口座に資金を振り込む
- 偽会社の架空の購入注文を作成して商品を転売
- コンピュータのデータを競業者に売り渡す

横領・窃盗：対策

- 重要な責務は交替制
 - 他の人が疑わしい行動に気づきやすくする
- 従業員個人にアカウントを発行
 - 共有アカウントを使用しない
- パスワードは、退職・解雇と同時に無効化
 - 退職した管理者による不正アクセス防止
- システム業務を一人の従業員に集中させない
 - 保険会社：証券発行と支払請求は兼ねない
- オーディットトレイル(audit trail, 監査証跡)の利用
 - 「いつ誰が何の操作を行った」の記録

オンライン詐欺

- オークション

- 落札した商品が送られてこない
- 届いた実物が説明とあまりにかけ離れている
- おとり入札による落札代金のつり上げ
- コピー商品の販売、不正転売

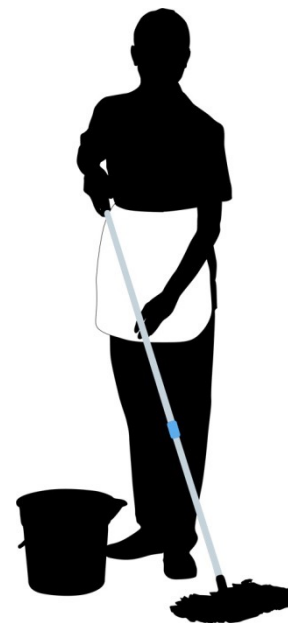


掘り出し物？ ぼったくり？



オークション業者の取り組み

- オークション業者の当初の立場
 - 「我々は詐欺行為や違法取引に責任を負わない」
- オークション健全化の取り組み
 - 出品者のレビュー
 - 不正出品の監視体制
 - 詐欺対策班の設置(100名規模)
 - 売り手のクレジットカード番号確認
- ただし、完璧な対策ではない
 - 架空レビュー、偽物の出品、etc



フィッシング(phishing)詐欺

- 本物と偽って機密情報を聞き出す詐欺
 - カード番号、パスワードなど
- フィッシング対策協議会
 - フィッシング(phishing)
 - 実在する組織を偽装した電子メールを利用
 - 個人情報を持ち明けるように誘い込む
 - カード番号、暗証番号、パスワード、等
 - フィッシングサイト(phishing site)
 - 本物そっくりのおとりサイト
 - 金融機関, クレジットカード会社等
 - 本物のサイトの素材を使うのでぱっと見は同じ


詐欺メール例

- 詐欺メール(フィッシング詐欺)にご注意ください

みずほダイレクトのご使用、有り難うございます。
このメールはみずほダイレクトご利用のお客様に配信しております。
この度、新たなセキュリティーシステムの導入に伴い、お客様情報の確認を行って
います。ご面倒をお掛けしますが必要事項の記入をお願いします。
手続きを怠るとみずほダイレクト使用中にエラーなどの発生が生じる可能性があります
ので大至急、手続きをお願いします。
以下URLより手続きにお進みください
<<http://xxxx.xxxxx.xxxx.com/>>
手続きを怠るとみずほダイレクト使用中にエラーなどの発生が生じる可能性があります
ので大至急、更新手続きをお願いします。
ご面倒をお掛けいたしますがご協力お願いいたします。
みずほ銀行
操作にお困りの際は 0120-xx-xxxx 一般ダイヤル(通話料有料) 東京:03-xxxx-xxxx 大
阪:06-xxxx-xxxx
商品関連のご質問は 0120-xx-xxxx 一般ダイヤル(通話料有料) 東京:03-xxxx-xxxx 大
阪:06-xxxx-xxxx

みずほ銀行をかたるフィッシング

(2012/09/12)

みずほ銀行

みずほダイレクト

[インターネットバンキング]

【重要】みずほダイレクトをご利用される方へのご注意(必ずお読みください)

お客さま番号を入力し、「次へ」ボタンをクリックしてください。

お客さま番号

次へ

お客さま番号は「ご利用カード」でご確認ください。


●個人情報の利用目的に関する事項

当行は、お客さまの個人情報について、下記(1)の業務内容に関し、下記(2)の利用目的の達成に必要な範囲内で取扱うこととし、その範囲を超えては取扱いいたしません。

(1)業務内容

- 預金業務、為替業務、両替業務、融資業務、外国為替業務およびこれらに付随する業務
- 投信販売業務、保険販売業務、金融商品仲介業務、信託業務、社債業務等、法律により銀行が営むことができる業務およびこれらに付随する業務
- その他銀行が営むことができる業務およびこれらに付随する業務(今後取扱いが認められる業務を含む)

みずほダイレクトヘルプデスク

 0120-3242-99

携帯電話・PHSからは03-3211-9324(有料)

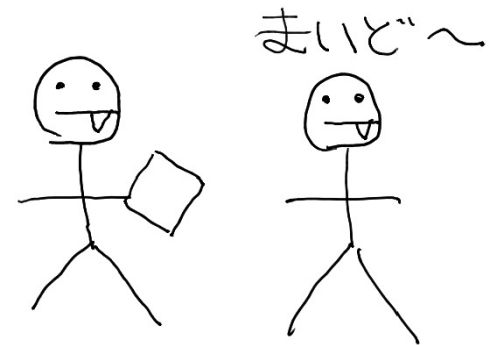
※システム調整のため一部ご利用できない時間があります。
※お客さまの個人情報はSSL(128bit)により暗号化して通信いたします。

[みずほ銀行トップ](#) [みずほダイレクトトップ](#)

Copyright (C)2011 Mizuho Bank, Ltd.

クレジットカード詐欺

- 犯罪者が正当な小売店から商品をカードで購入
 - 本人が購入した後でしらばつくれるケースも...
- 小売店が詐欺目的のカード請求伝票を送付
- 偽造カードの使用
 - 領収書から番号を持ち出す
 - 直接電話して適当な口実で聞き出す
 - スキミング装置 (skimming)
- 名義を盗んだカード
 - 名簿情報を使って不正に開設
 - 真正の所有者が滅多に使わないカード番号を入手したうえで、請求書を転居届で回送させる



スキミング・カード偽造

- カードの磁気ストライプを読みとる
 - 読みとったデータで偽造カードを作成
- 自分の目を離れたカードは危ない
 - 更衣室
 - 店の支払い
 - カードは手元にあるので被害に気づきにくい
- オンラインでのカード利用
 - 「カード番号＋裏面のセキュリティコード」で可
 - クレジットカードの「写真」も実質スキミング



クレジットカード犯罪はなぜ深刻か

- 被害額は毎年数十億ドルと言われる
- セキュリティと利用者の利便性のトレードオフ
 - カード使用時の本人確認の厳格化
 - カード裏面の署名・写真の確認省略
 - レシート署名の形骸化
- 構造的な理由
 - カード詐欺の損害はカード発行会社が負担
 - 店側に積極的にチェックする動機が無い
 - 客足が減る方が困る
 - 結果的にカード利用者への負担に



クレジットカード詐欺の対策

- ICカード化による偽造困難化
 - CPU・メモリ(記憶装置)を搭載
 - 暗号技術により保存データ・通信内容を保護
 - 正規の装置でしか中身を読めない
 - 内容を読むにはPINコードが必要
- オンライン取引の保護
 - パスワード認証

A screenshot of a "Verified by Visa" online transaction confirmation screen. It displays transaction details and a password field.

VERIFIED
by VISA

ご本人確認の画面です
パスワードを入力してください

加盟店: Extra Commerce
ご利用金額: ¥10,500
ご利用日: 6/11/2001
カード番号: **** * 9010
パーソナルメッセージ: Happy Birthday
パスワード:
[パスワードを忘れた場合は?](#)

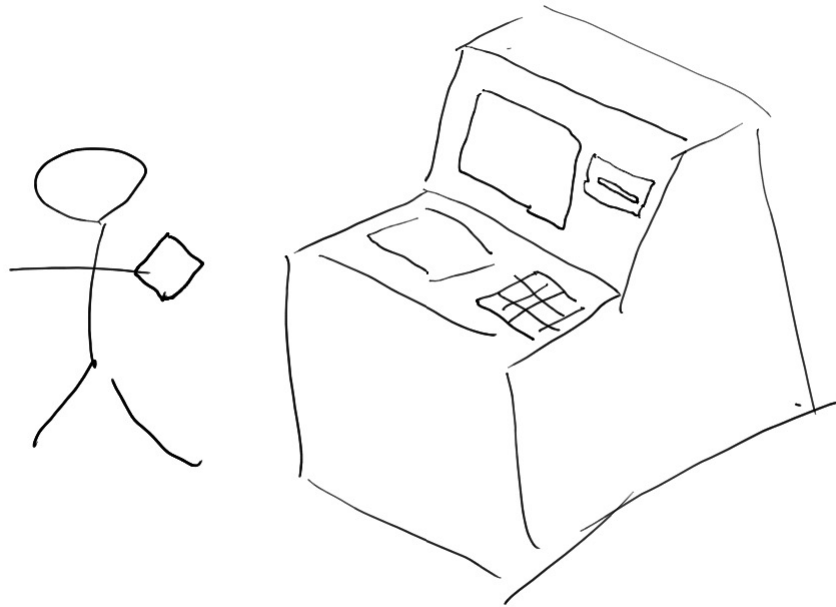
送信 ヘルプ キャンセル

画像出典 <http://www.smbc-card.com/mem/service/sec/iccard01.jsp>

画像出典 <http://web-seo.designcross.org/2010/01/3d.html>

ATM詐欺

- Q:どんな詐欺の手口が考えられますか？



ATM詐欺の事例

- 内部犯行
 - ATM装置設置会社の勤務者が、導入時パスワードを不正使用してキャプチャソフトを導入
- ATM偽装
 - ATM装置に模した装置を設置
 - カードを読み取り、入力された暗証番号を保存
 - 客にはエラーを表示
 - 夜間金庫の例(2004年7月, 静岡県, 2006年7月にも)
 - 偽ATM事件(2005年5月, ルーマニア)
 - ショルダーハッキング
 - 背後や望遠鏡, ビデオカメラで覗き見る
 - UFJ銀行の例



ATM詐欺の事例

- セブン銀行の事例(2013)
 - 【注意】セブン銀行が「ATMカード挿入口のスキミング機に注意」と警戒を呼びかけ



偽造カードによるATM詐欺

- ATM1800台から2時間で20億円引出し(2016)
 - 偽造カードでATM1800台から計20億円が一気に引き出された！ セキュリティーの脆弱性を突いた大胆手口とは...
- 経緯
 - 南アフリカ スタンダード銀行から情報流出
 - 偽造クレジットカードが1600枚作られる
 - 磁気ストライプ対応のATMで現金引出し
 - 2016/6/15(日)午前5時から約2時間半で一斉に引出し

名義窃盗

- 社会的に他人になりすます
 - 今の時代、身元は「数字の羅列」でしかない
 - 口座番号、社会保障番号、運転免許番号、etc
- 深刻な被害の例
 - 勝手にクレジットカードを大量に作成・利用される
 - 勝手に借金され、返済を迫られる
 - 社会的信用の失墜(就職,ローン,賃貸契約,etc)
- 個人情報漏洩の怖さ
 - 他人があなたになりすますのが容易になる

詐欺対策

- セキュリティ技術向上と犯罪者技術の高度化との間でのいたちごっこ
 - ex.盗難カード確認の情報化→盗難届を出すまでに
 - ex.カードが届いたことの本人確認後に有効化
- 通常と異なる利用パターンを検出
 - 「情報化」の効果
- 高額取引のチェック, 引出し限度額の設定
- 生体認証技術 (biometrics) の導入
 - 指紋認証, 静脈認証
 - 生体認証は「漏洩しても変更がきかない」ことが欠点

デジタル偽造

- カラープリンタ, イメージスキャナの高性能化, 低価格化で比較的偽造が容易に
 - 紙幣, 証券, 書類, ...
 - 高度な技術(透かし, ホログラム, 特殊インク)
 - 所詮はいたちごっこに
 - 書類偽造の参考映画: Catch me if you can
- 偽造の容易性
 - 経済の安定性への脅威
 - 証拠写真・映像の信頼性



QRコード決済の事例

- QRコード決済
 - 支払い用QRコードをスマホで読めば支払い完了
 - <http://wechatpay.aplus.co.jp/>
- QRコード決済の落とし穴、中国
 - 「おつりが出せないから、QRコードで支払ってくれ」
 - 「支払いの確認が取れない、どのQRコードをスキャンした」
 - 「そのシールは支払い用のQRコードではないうえに、誰がいつ張ったのかわからない」
 - QRコードの上に偽のQRコードが貼られていた
 - 出典 <http://www.afpbb.com/articles/-/3130380>

偽造に対する防御

- 技術的な防御
 - セキュリティスレッド技術(\$100紙幣に導入)
 - ホログラム, 磁気層等の埋め込み
 - 機器のシリアルナンバーをコピーにプリント
 - XEROXの高級機
- 標的になりうる人員の訓練
 - c.f. 売り文句は「コイチのカツ」 買い物中に気づいた異変
- 法律改訂による防御
 - 発行小切手の番号と額面を銀行に予め送付
 - 小切手発行者にも責任を課す

写真のまやかし

- デジタル画像の改変の容易性
 - ある写真は改変されていないと信じられるか？
 - 犯罪現場の写真などは訴訟上の証拠にも
 - 速度自動取締り装置の写真等
 - 技術的には公開鍵暗号(+時刻サーバ)が利用可能
 - ex.National Geographics誌で表紙の中に2つのピラミッドが収まるように間隔を詰める加工を写真に施した事件
- →偽造の可能性に合理的な疑いをもつ必要性

一体、何が本物なのか？

- 女子高生Saya(2016)
 - 株式会社LogoscopeのVirtual Human Project
 - 作者は <https://twitter.com/mojeyuka>



出典 <http://www.logoscope.co.jp/jp/projects/virtual-human-projects>

デジタルヒューマン

- リアルなCG+AIにより仮想人物を生成
 - [Unreal Engine](#)
 - [デジタルヒューマンが切り開く、顧客コミュニケーションの新たな可能性](#)
 - <https://www.digitalhumans.jp/>
 - [Digital Human Reception Demo](#)
 - [Epic Games、超リアルなデジタルヒューマン作成ツール「MetaHuman Creator」をクラウドで提供へ](#)
[Webブラウザだけで制作可能に](#)

写真加工と言えばPhotoshop

- 自爆テロ犯に仕立て上げられてしまった男性
 - 元々の写真はバスルームでの自撮り画像(左)



- 尚、Adobeは偽造写真検出技術も研究している

映像中の人物の差替え

- Deep Fake
 - 顔写真1枚で簡単にディープフェイク映像を作成できる無料アプリ登場、中国で大人気に
 - カリフォルニア州、選挙とポルノ関連のディープフェイク動画を取締り対象へ

ハッカーとセキュリティ

クラッキングとは

- ハッカー (hacker)
 - 非常によく出来た洗練されたプログラムを書く
 - コンピュータの巨匠ともいえる(昔は...)
 - 知的なチャレンジ→エスカレート
- クラッカー (cracker)
 - 卑劣な心を持つハッカー?
 - 盗みや損害を与えたりするため, 権限なくコンピュータシステムに侵入する者?
 - 最近では, 金銭目的化

ハクティビズム

- 政治的主張を伴うハッキング(クラッキング)
 - hack(ハック):「合理的で創造的な行為」
 - hacktivism = hack + activism

活動区分	通称	例
法遵守的	ポリティカルコーディング	暗号通信用ソフト開発 P2P通信ソフト開発
法侵犯的	ポリティカルクラッキング	外交機密の暴露 特定団体Webの攻撃

参考 <http://credo.asia/2014/03/22/hacktivism/>

自動車のハッキング

- Charlie Miller&Chris Valasek(セキュリティ専門家)
 - [Jeepチェロキーの遠隔操作に成功\(2015.7\)](#)
 - エンジン、ステアリング、ワイパー
 - [Black Hat USA 2015:ジープのハッキングの全容が明らかに](#)
 - [技術報告書](#)
- 対象車種140万台リコール
 - ソフトウェアのアップデート



<http://www.blogcdn.com/www.autoblog.com/media/2013/02/2014-jEEP-cherokee-1.jpg>

地上波デジタル放送視聴用ソフト

- デジタル暗号放送の視聴ソフト
 - 技術詳細は非公開なのに何故かネット上に掲載
 - この少年はそれを元に地上波デジタル用に改造
 - B-CASカード無しで無料チャンネルを視聴できる**



クラッキングの重大性

- 貧弱なセキュリティがある限り問題である.
- CERT (The Computer Emergency Response Team)
 - JPCERT/CC (<http://www.jpcert.or.jp/>)
 - インターネットのセキュリティ問題への対処
 - 情報収集と広報
- 多くの不正侵入は報告されないことが多い
 - 恥の文化(?), 過度の信頼性低下 (株価低下?)
 - クラック行為の助長, 信頼性の低下 ...
- Morrisワーム (1988年)
 - インターネットの全システムの10%を停止に
 - 簡単に防げる脆弱性が放置されていることを実証

悪意なきハッキング

- 「権限のないコンピュータシステムへのアクセス」に対する(自称無害の)ハッカーの主張
 - 損害は発生していない. 無害なレクリエーションであり, 知的な挑戦だ
 - 管理者からみれば侵入者の意図・活動内容は不明確
 - システムのセキュリティの弱点を明示している
 - よいセキュリティがないからいけない
 - 弱点について弱点を明らかにすることは恩恵か?
 - 情報をコピーする行為は盗みでは無い
 - プライバシー, 知的財産権
 - 通信会社は儲けすぎだから, 少々のだだ乗りは問題ない
 - 泥棒は泥棒

Chaos Computer Club



- 目標: あらゆるコンピュータや技術的なインフラへの自由なアクセスを守ること
 - 記事: [セキュリティの欠陥を暴く](#)
- 活動事例
 - 銀行のシステムに侵入し、13万マルク引出し
 - 翌日、返金
 - iPhone 5sのTouchID(指紋認証)の回避

機密保持によるセキュリティの維持

- 脆弱性情報をクラッカーから隔離すればよい？
 - 「脆弱性」は現に存在している
 - 情報は暴かれてしまう可能性がある
- 機密保持を考えることは無意味では無い
 - 少なくとも時間稼ぎにはなる
- 倫理的な問題
 - 放置されている脆弱性は知らせるべきか？
 - 放っておけば大勢の被害者,公開すれば格好の餌食
- 現在の業界ルール
 - 脆弱性を見つけたらCERTに報告
 - 開発元が脆弱性を解決した後に脆弱性を公開

セキュリティの改善

- セキュリティの確保を主たる設計目標にする
 - (技術面の) 安全性を確保する技術はある
 - ex. Firewall, IDS, IPS, 暗号化, 電子署名
- 公開性と容易性 vs. セキュリティ
- 完全なる防衛は存在しない
- ユーザへの教育
 - よいパスワード管理手法
 - 他者に推測されにくく自分では覚えられる長いもの
 - パスワードマネージャの利用

法律による線引き(日本)

- コンピュータへの無権限アクセス
 - 「違法」と明文化されています
 - 悪意の有無は問わない
- 危害を与える恐れのあるプログラムの作成
 - いわゆる「コンピュータウイルス作成罪」
 - 不正指令電磁的記録作成・提供罪として規程
 - 「**正当な理由無く**」作成・配付すると有罪

Coinhive事件(2018)

- Coinhive
 - Webサイトに設置するJavaScriptプログラム
 - 閲覧者のPCで仮想通貨を採掘
 - 採掘益の7割がサイト運営者に配分される
- 神奈川県警などが全国で21名を検挙
 - 「Coinhiveは不正指令電磁的記録に該当」
- Webデザイナーの一人が正式裁判を請求
 - 1審:無罪,2審:有罪(罰金10万円),3審:無罪(2022)
 - 判決:「利用者の意図に反するプログラムではあるが、社会的に許容される範囲内で不正性は認められない」

セキュリティはなぜ脆弱なのか

- 歴史的要因
 - インターネットは研究者の通信手段としてスタート
 - 自由なアクセス, 利用の利便性, 情報共有の容易性
- 技術的要因
 - 複雑系ゆえの予測困難
 - 常に何らかの誤りはある
 - ネットワーク接続, 利用に必要なスキルの低下
 - より多くの個人情報, 重要情報の蓄積
- 人的要因
 - 快適さの追及、ヒューマンエラー
 - 知的好奇心、自己顕示欲、金銭欲、思想信条、etc.
 - 重大な問題が発生するまで対策をしないことが多い

総括

- コンピュータ犯罪も、基本的には「人」の問題
 - コンピュータ(情報化)がツールに
 - コンピュータに特化しない対策
 - 何があり得るのか、手口を知る必要あり
 - 秘密情報は安易に聞かれない「はず」
 - 「常識化」
- トレードオフ
- 利便性とセキュリティ

ミニレポート(再掲)

- 「コンピュータを使った犯罪にひっかからない為に心がけるべきこと」を、コンピュータやインターネットにあまり詳しくない人(例えば、親戚の子供、自分の親または知合いのおじさん、おばさん)に説明するなら、どういう説明をするのが適切かを考え、その説明内容を簡潔に示しなさい。
- 提出先: Moodle
 - <https://moodle.cis.kit.ac.jp/mod/assign/view.php?id=230358>
- 提出期限: 次回講義開始時

参考資料

- Catch me if you can
 - 小切手偽造で有名な天才詐欺師の自伝を映画化



- 技術者倫理とリスクマネジメント



- オーム社
 - ISBN:978-4274068720