セキュリティキャンプ２０１３
セキュアなシステムを作ろうクラス
セキュリティの見える化を考えるゼミ
テーマ#03「利用者を置いてけぼりにしない
セキュリティを考えてみよう」資料

熊猫さくら

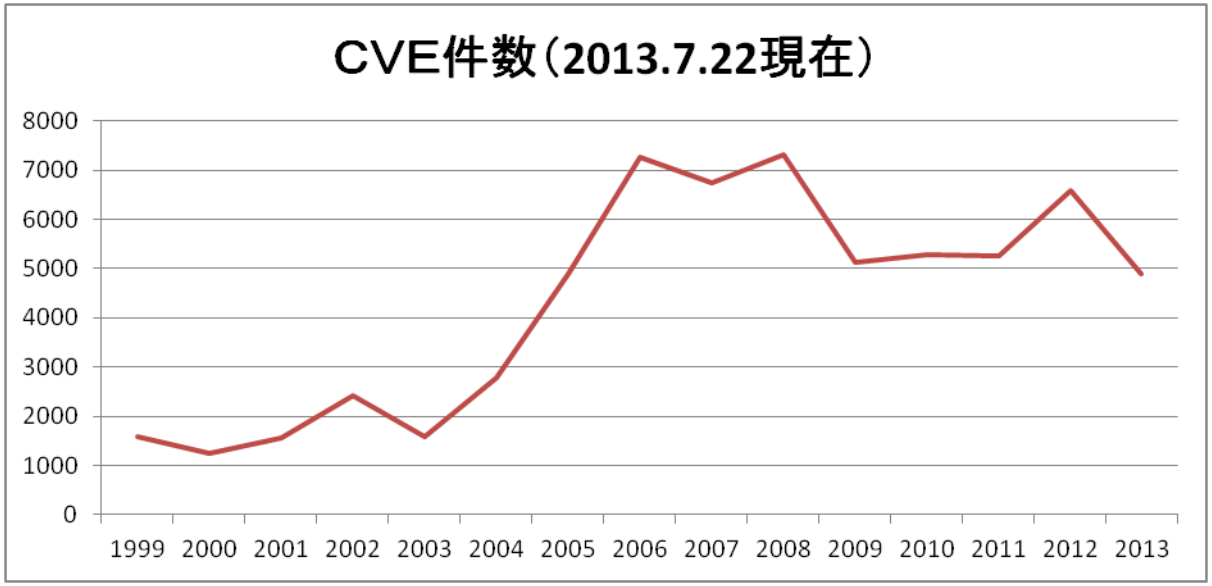
2013/8/13-2013/8/17

本書の内容

- 世間にあるようなセキュリティの教科書ではありません。
- 熊猫が日頃思っている、「我々はセキュリティのために
  どれだけ損をしているのだろうか」ということの片鱗を
  書いています。
- 熊猫の経験に基づく独断と偏見で書いたものですので、
  鵜呑みにしないこと。セキュリティのあるべき姿について、
  考えるきっかけにしてほしいです。今はセキュリティに
  関わっている意識のない人でも、５年後、１０年後に
  思い出してほしいです。

質問： CVE って知っていますか？

- Common Vulnerabilities and Exposures
  - ソフトウェアに関する脆弱性データベースの例
  - 膨大な件数



  - 全ての脆弱性に CVE 番号が割り当てられている訳ではないので、実際の件数はもっと多い筈。

利用者にとっての CVE

- CVSS （ Common Vulnerability Scoring System ）というスコアがあるけれど
  - 誰でも簡単に悪用できるものもあれば、本当に悪用できるのか怪しいものもある。

- 利用者にとっての関心事は、自分や自分のシステムが影響を受けるかどうか。
  - でも、普通の人には CVE の重要度・影響範囲を判断することは難しい。
    - バグの重要度・影響範囲を判断することも難しい訳ですから。

質問：バグと脆弱性の違いって何でしょう？

- 「バグではありません、仕様です。」というのはよく聞くけれど、「バグではありません、脆弱性です。」というのはあまり聞かないかな？

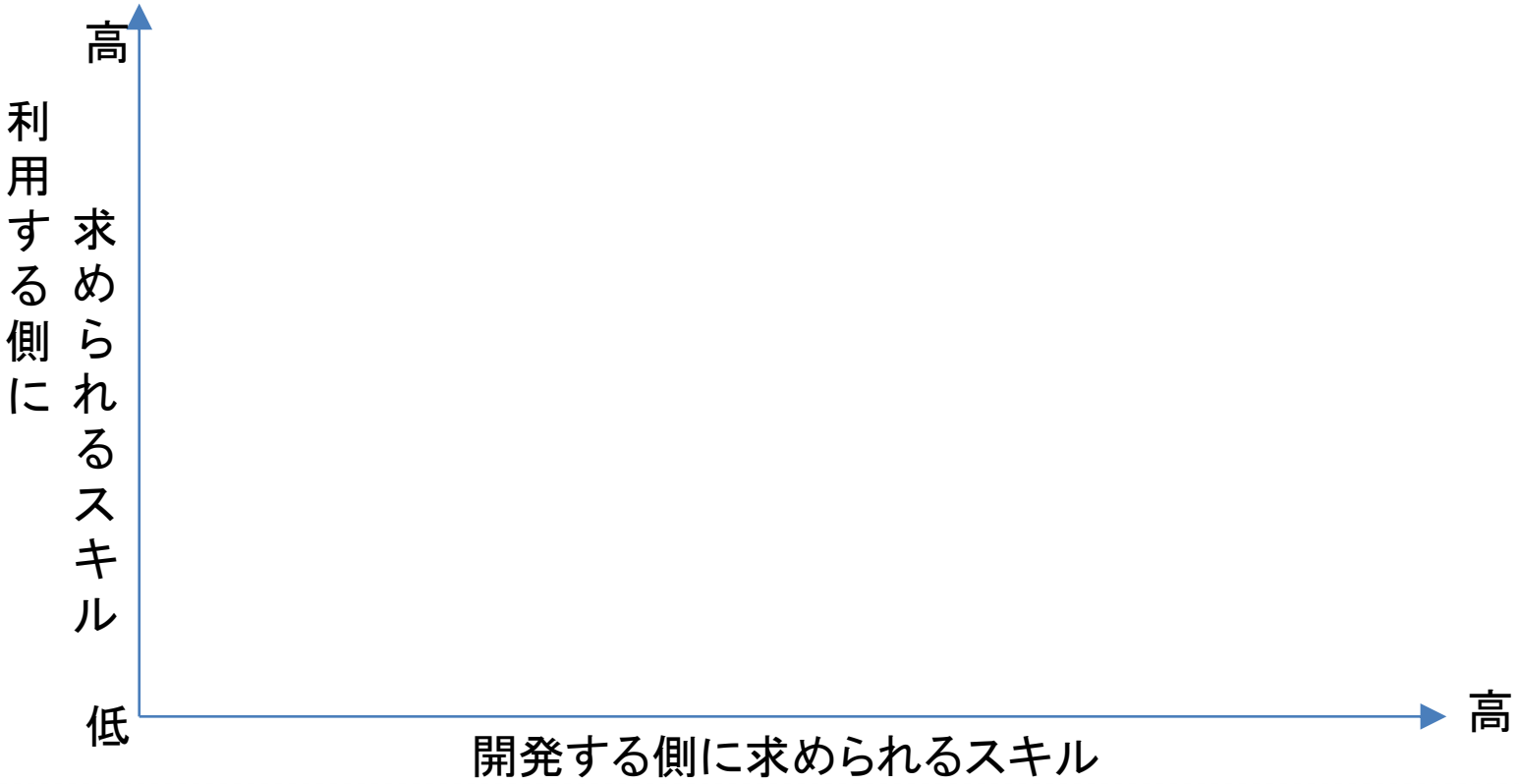
- バグの内、悪用できるものが脆弱性？それとも、仕様通りでも悪用できるものなら脆弱性？

ソフトウェアの脆弱性とセキュリティ技術の関係？

- 脆弱性の発生を予防するために、様々なセキュリティ技術が考案されている。
  - 世界的に使われているものから、自分で考えて自分で使っているものまで。

質問：セキュリティ技術にはどんなものがある？

- 例えば、「開発する側に求められるスキルのレベル」と「利用する側に求められるスキルのレベル」を軸に考えてみた場合、どんなものがある？



例：バグを埋め込まないセキュアなコーディング手法

- 30000+30000 は 60000 なのに、
  30000+40000 は 4464 なの？

- 悪用できるかどうか以前に、期待通りの結果を出すために
  必要なもの。

- 開発する側、利用する側の双方に基本的なスキルが
  必要になるけど、敷居は低い方であると思う。

例：暗号化／乱数化／アクセス制御機構

- 高度な数学的・論理的知識から生まれたもの。
  - 複雑さゆえにミスに気がつきにくい。

- 利用する側にも、それなりのスキルが必要で敷居が高い。
  - 理論上は結構強固だけど、現実はどうなのだろう？

アクセス制御によるセキュリティの限界？

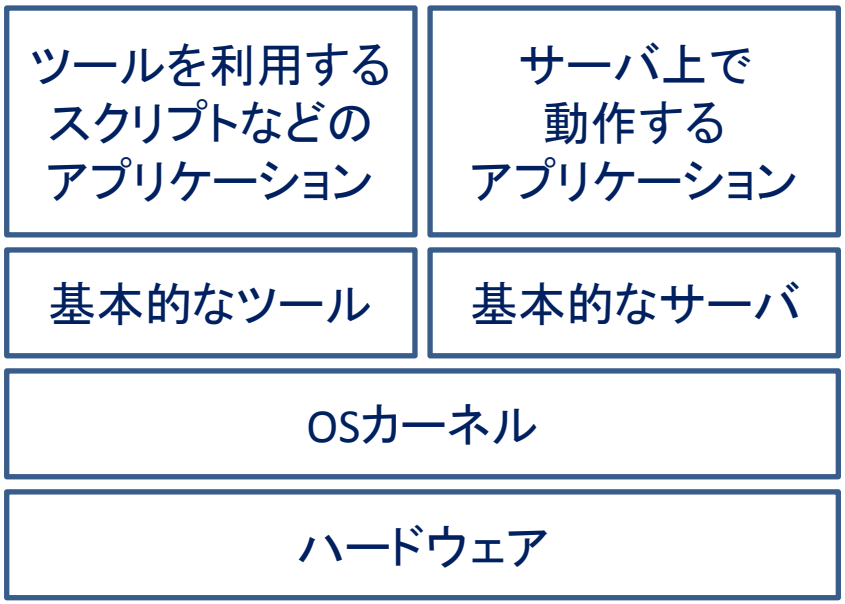
- 情報の使われ方が変化してきている。
  - 分業による外注化
    - 関係者全員に一律に同じレベルのセキュリティに関するスキルを強制できなくなった。
  - コピーの容易さ
    - ネットワークの発達／ストレージの発達／クラウド技術の発達により、情報の所在を把握することが難しくなった。
- 情報にアクセスできるかだけでなく、どのように情報が使われるかも重要。
  - １台のコンピュータ内での情報のアクセス可否は制御できたとしても、アクセスが認められた後のことは制御できない。

質問：ソフトウェアによるセキュリティ技術にはどんな問題がある？

- ソフトウェアやコンピュータの知識を持ち合わせていない人にとっては全く意味不明な世界ですが、ある程度持ち合わせている人でも苦労している問題点もありますよね？

問題点：防衛対象の範囲が広すぎる。

- ハードウェアやＯＳのレイヤーから、アプリケーションのレイヤーまで
  - 一ヶ所でも突破されたら負け
    - 萎縮してしまう



問題点：その割に、ソフトウェアに起因する問題にしか対処できない。

- 基本的に脅威を解消するのではなく問題を先送りするだけ。
  - 実は、暗号化や乱数化による防御（プライバシーとして隠蔽すること）は、攻撃する側にとっても都合のいいものになることがある。
- 理想のセキュリティとは「他人には絶対に解読されない強力な暗号」と考える人もいるけれど、それでは犯罪者が隠しておきたい秘密も隠すことができてしまう。
  - セキュリティ技術は犯罪者の犯罪行為を助長するために存在するのか？
  - 技術は全員に対して中立？　技術を習得している人にだけ味方する？

問題点：利用する側のスキルを考慮したものが少ない。

- セキュリティのための機能とセキュリティではない機能との違い？
  - セキュリティではない機能は、必要なもの・使いたいものだけ使えれば目的を達成できる。
  - セキュリティのための機能では、目的を達成できるとは限らない。守りたいものを守りきることができて初めて、目的が達成される。
- 様々な情報が錯綜していて、どれが最適な選択肢なのかを判断できない。

問題点：セキュリティのための機能は、あらゆる脅威に対応できるものではない。

- 開発する側にはもちろん、利用する側にも高度なスキルが必要になっている。
  - 専門家が作ったものはハードルが高く、従来の考え方を続ける限り、利用者に使ってもらうのは難しい。

- 開発する側がいつの間にか専門家になってしまい、利用者にとって使えないという過ちを犯す。
  - でも、開発している背景を利用者が知ろうとしないからという問題もある。

セキュリティについての意識が変化してきている？

- アクセス制御って何のためにやっているんだっけ？
  - 記録メディアの紛失などのようにアクセス制御では防げない問題が多発し、アクセス制御を回避できてしまう脆弱性が絶え間なく発見されているという状況。
  - ソフトウェアによるセキュリティ技術には期待できないのではという疑念。
- 情報の流れが見えなくなった。
  - ソフトウェアではなく人の判断／行動に依存する割合がどんどん拡大している。
  - 情報の流れが見えないことが、犯罪の温床になっている。

質問：ソフトウェアではないセキュリティには どんなものがある？

- ソフトウェアの脆弱性を突こうとするのは人間です。
- でも、ソフトウェア以外の脆弱性を突こうとするのも 人間です。
- だから、セキュリティにはソフトウェアでは対処できない 「人の考え方や行動に依存する領域」がある筈です。

例：社会や組織のルール

- 法律や取り締まりを回避したいとか思っていませんか？
  - スピード違反や飲酒運転などの検問を誤魔化したいとか思っていませんか？

- ソフトウェアの不備を突くのは、社会や組織のルールの不備を突くのと似ていませんか？

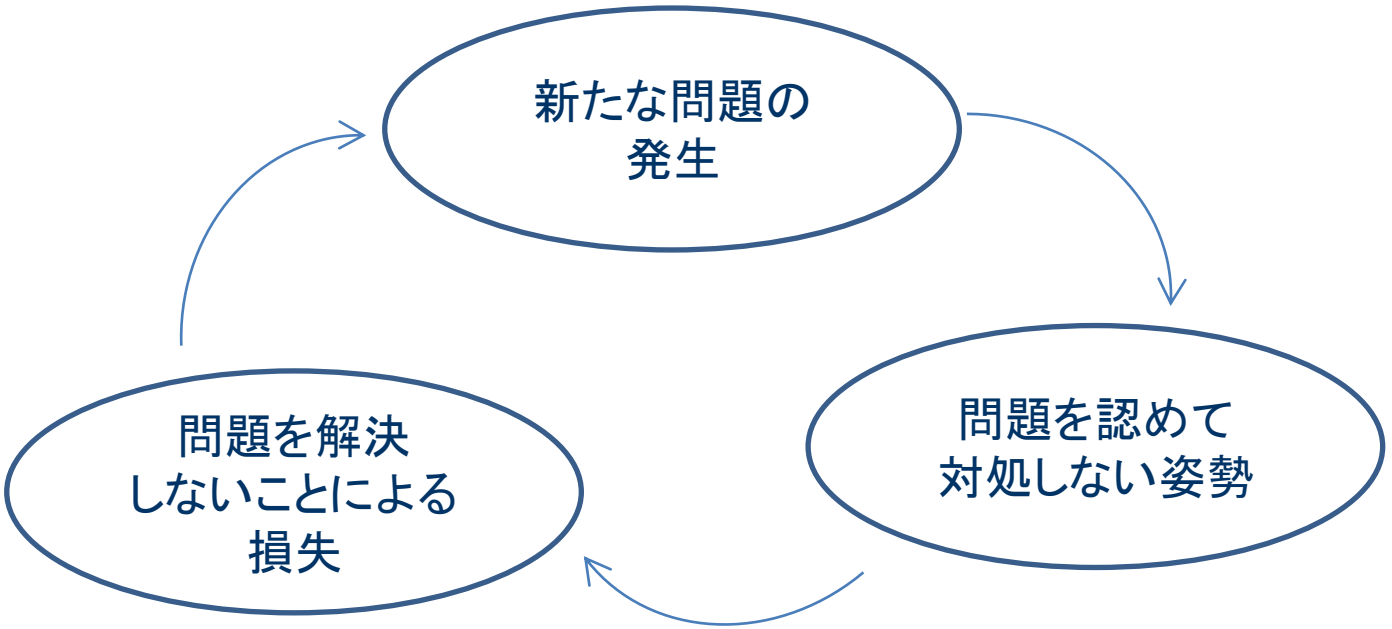
社会のルールに起因する問題の例

- 金の流れ（個人の収入や支出など）をプライバシーと称して隠すことで、問題が見えなくなる。
  - ワーキングプア・ブラック企業
  - 国家間の制度の差異を利用した脱税・節税
  - 生活保護の不正受給

- コストに見合った適切な対価が支払われているかを判断する方法が無い。

社会のルールに起因する問題を隠し続けることの問題

- 問題が固定化されてしまう。
  - 何のために秘密にしているの？
    - 被害者が苦しみ続けるため？



事件が与える無意識の影響

- 事件が起きるとニュースとなり、それがネットやＴＶなどで伝わってきます。同種の事件を何度も聞かされている ことによって、感覚がマヒしてしまっていませんか？
  - 「自分も真似しちゃえ」とか「隠しきれない／逃げ切れない方が悪い」とか「騙される方が悪い」とか思っていませんか？

ソフトウェアのセキュリティも大変だけど

- 社会のセキュリティも大変なことになっていると思います。
  - その根底にあるものは何でしょう？

その答えは「欲望」・・・ということなのかな？

- 「楽して儲けたい？」

- 株・ギャンブル・犯罪の差異って何でしょう？
  合法か非合法か以外に差異はあるのでしょうか？
  - 誰かが得をすると誰かは損をしている。
  - 知らない間に侵略する側になっていませんか？

- お金は全員に対して中立？　お金を持っている人にだけ味方する？

ソフトウェアの違法コピー

- 何故発生するのでしょうか？
  - 不当に高価と思われているのでしょうか？
- 無断／違法コピーの対象はソフトウェアに限りませんよね？
  - ブランドとかもコピーされていますよね？
- コピーする方が悪いのでしょうか？それとも、コピーされる方が悪いのでしょうか？

何故そのようになる？

- コストが見えないから？
  - ソフトウェアで起業して成功している人の存在。
  - 「楽して儲けているのでは」という疑心暗鬼に陥っていませんか？

- ソフトウェアの開発や保守は結構大変なんです。
  - みんなで協力して良いものを作っていこうとする「オープンソース」という動きが広がってきています。

相互不信感が発生する理由？

- インターフェース（契約）だけの関係で動いている。
  - やっていることが見えない。
  - 外の世界を体験できない／他者の視点を持てない。
    - 隠すこと／独占することが力の源泉であるから。

- 独占的な立場にある組織って、不誠実な対応が多いと思いませんか？
  - 保身のためのセキュリティ？
  - 外の世界が見えていないし、外に世界を見せない。

解決策は、貢献やコストを見えるようにすること？

- 富を配分してきた社会から負担を配分する社会へ変化してきている。
  - 負担をする上で納得感や公平感をもたらすためには見える化が大事では？

- 全て記録するなんていう手間をかけずに済めば嬉しいけれど。
  - 自発的にできないのなら、プライバシーとして隠し続けてきた部分に踏み込むことが避けられないのかな？

質問：そもそも、何故セキュリティに煩わされているのかを考えたことはある？

- 知らない間にセキュリティ意識を植え付けられているけれども、誰のためのセキュリティなの？

- 世界を相手に戦う時代とか言うけれど、我々が脅威としている相手って誰なの？
  - 同業他社？　闇の勢力？　社員や協働者？

弱肉強食なセキュリティで幸せになれるの？

- 弱者や障害者への配慮は？
  - 今のセキュリティは弱者か否かに関わらず巻き込まれる。
  - 誰もが老いる。
    次の世代に搾取されたい？今のうちに搾取して逃げ切る？

- 誰のためのセキュリティなの？
  - 自分が加害者でありつつも、被害者になるのを
    避けるため？
  - 加害者にも被害者にもならないようにするためには、
    どうすれば良い？

結局、セキュリティって何なの？

- セキュリティの教科書の内容は古くないか？
  - インターネット普及前の考え方を引きずっていないか？
- セキュリティに関わる人たちの意識が古くないか？
  - 隠ぺいによるセキュリティは問題解決になるのか？
- コラボレーションの芽を潰していないか？
  - 協力できないのは社会的なシステムの問題では？

真摯な生き方をしませんか？

- コストや問題点を明らかにして議論することを躊躇わない。
- 利用者を置いてけぼりにしないセキュリティのためには、考え続けること、そして、行動を続けること。
- 空気を読まないのは恥ずかしいことではない。頑固さは必ず何かの影響を与えます。行動として何ができるかを考えてみよう。現実に流されたら負けです。

まとめ

- 現在のセキュリティ教育は、人ではなく技術にばかり注目している。
- セキュリティの根底には、疑心暗鬼や相互不信がある。
- 隠すことによるセキュリティでは問題は解決しない。