サイバーセキュリティ基礎論

S12 - 14　Id:19534233　木曜３限

S1, 2, 22　Id:19535202　金曜３限

谷本　輝夫

tteruo [at] kyudai.jp

https://teruo41.github.io/lectures/csp2019

前回の感想から（１）

- 暗号がそんなに昔からあるのに驚いた
- 共通鍵暗号方式と公開鍵暗号方式の相違点がよくわかりました
- 高校で習ったことのある内容だった

前回の感想から（２）

- 鍵というもののイメージが湧きにくく少し難しい内容でした。実際に使われている鍵はパスワードのようなものですか
  - その通りです。覚えられないくらい長いパスワードのようなものです。
- 自分で暗号化する際には暗号化の種類を選べるのですか、それとも決まった暗号化の仕組みがあるのですか
  - 暗号化するソフトウェアによっては暗号の種類を選べるものもあります

前回の感想から（３）

- 共通鍵暗号についてなのですが、送信者と受信者で鍵を共通させるとありますが、だれにも知られることなく秘密裏に鍵を相手に知らせる方法としては具体的にどのような方法がありますか
  - 現在使われている方法は、郵便、電話、SMS（ショートメール）などです。これらは比較的安全に本人に情報を伝える方法だと考えられています。

前回の感想から（４）

- 復習の3問目でデータの完全性を保つために、データの暗号化だけでは不十分なのですか?暗号化されていれば改ざんされない気もするのですが…。
  - 暗号化の方法によります
- ハッシュ関数に関する疑問なのですが、ダイジェストにする際にダイジェストが元のデータより短くなる関係上同じハッシュ値を持つデータが複数存在しうると思うのですがどうなのですか？
  - その通りです。このことを衝突（コリジョン）といいます。ハッシュを使った情報システムを設計する際には衝突が起きてもシステムが壊れないように考えておく必要があります。実用されているハッシュ関数の設計時には衝突が起きる確率が十分小さくなるよう考慮されています。

前回の感想から（５）

- 安全性の種類の中で、計算量が多すぎて解くのは不可能だっていう『計算量的安全性』っていうのがあったと思うんですけど、バリ計算の早いコンピューターを開発すれば解くのは可能なんですが？また可能な場合、そんなコンピューターができたら、安全性がなくなりますよね？
  - その通りです。その時は暗号アルゴリズムを変更するか、鍵のビット数を増やす必要があります。

前回の感想から（６）

- 公開鍵暗号方式において、そもそも秘密鍵はどのようにして持つことができるのか(もともとその人のコンピュータに入っているものなのか)
  - 秘密鍵はいくつでも作れます。
- 公開鍵によって暗号化されたものをなぜ秘密鍵で復号できるのか
  - 残念ながらこの講義の中では説明しきれないので興味があればぜひ勉強してみてください

前回の感想から（７）

- 復習と感想を提出できる時間を延ばしてほしい
  - 複数のリクエストをいただいていますが、ほかのクラスとの兼ね合いもあるので難しいです。

講義予定

	日付	内容
第１回	４月１１、１２日	サイバーセキュリティ最新情報
第２回	４月１８、１９日	安全な設定（１）
第３回	４月２５、２６日	安全な設定（２）
第４回	５月９、１０日	研究倫理・情報倫理
第５回	５月１６、１７日	暗号技術を知る
第６回	５月２３、２４日	サイバーセキュリティと法律
第７回	５月３０、３１日	著作権
第８回	６月６、７日	社会科学