セキュリティ班 (ゆるセキュΔ)
活動報告書

立命館コンピュータクラブ
2018 年度後期プロジェクト活動

-Leader-
藤原浩一 *

-Members-
立川泰暉　廣田公大朗

2019/2/11

* 情報理工学部　情報理工学科　セキュリティ・ネットワークコース　二回生

目次

1　はじめに

文責：藤原浩一

このプロジェクトは，立命館コンピュータクラブの 2018 年度後期プロジェクト「セキュリティ班（略称，ゆるセキュΔ)」である．昨今，2020 年東京オリンピックに向けて国のセキュリティを強化するなどの施策を講じていることもあり，世間的にもセキュリティが身近にある問題であることが認識されている．また，企業だけではなく，個人のスマートフォンやネットワークカメラなどの IoT 化が進んでいるため，今まで以上にセキュリティに対する理解意識を持つ必要があると考えられる．本プロジェクトは，セキュリティに対する理解と意識を少しでも向上させるために立ち上げたものになる．IT 技術者として，実際に攻撃手法について学び，インシデントに対してどのような点が危険であるのかの理解を深めた．

2　活動概要

文責：藤原浩一

このプロジェクトでは以下の二つを大きく行なった．

- CTF
- ブレインストーミング

3　CTF

文責：廣田公大朗

セキュリティを知るため，CTF を実際に体験することでセキュリティ技術の基礎を学んだ．CTF 初心者が多かったため，常設 CTF の一つであり，難易度の低い Cpaw CTF を利用した．CTF の問題をとき，班内で問題の復習・解説をしあった．CTF 経験のある班員は，より難易度の高い問題に挑戦した．

4　ブレインストーミング

CTF を通してセキュリティ技術の一端を学んだあと，昨今のセキュリティ分野における課題について議論を交わした．

4.1　宅ふぁいる便情報漏洩

文責：廣田公大朗

これは宅ふぁいる便運営会社がユーザのパスワードを平文で保存していたことが大きな原因とされている．パスワードを保持，管理する上でハッシュ化して不正アクセスを受けても流出しないようにするのが最低限の対策であると結論づけた．

4.1.1　パスワード管理のための安全なハッシュ化

安全にパスワードを保持するにはハッシュ化 (文字列をハッシュ関数を用いて不可逆なハッシュ値という値を求める)

例: hash = MD5(“hogefuga”)

hash: 56bde24b2b0fd23d0b032c8aa128a86c

というように hogefuga という文字列 (キー) が意味を持たない値に変換されるこの場合は MD5 と呼ばれるアルゴリズムを用いてハッシュ化したが，MD5 は有名な文字列に対してはハッシュ値が対応付けられて元の文字列が再現されてしまう脆弱性があるため，パスワード管理に対しての利用は不適切である．そのため SHA-2 と呼ばれるアルゴリズムがパスワードのハッシュ化に広く使われている．ハッシュ化する際は異なるキーから同じハッシュ値が生成される衝突や，レインボーテーブル攻撃を妨げるために元となるキーにソルトという値を合わせてハッシュ化したり，多重にハッシュ化することで解析時間を伸ばすストレッチングなどを組み合わせてパスワードを管理するのが良い．

4.2　国によるポートスキャン

文責：藤原浩一

現在，国が日本国内の IP アドレスに接続されている IoT 機器に対してポートスキャンを行い，脆弱性の状況を確認すると発表している. 我々としては，国が行うポートスキャンを止めることはできないが，中のデータが見られないように防ぐ対策は行えると考えている．

4.2.1　ポートスキャンについて

特定のアドレスに対して，空いているポートをスキャンして探すという目的である.HTTP であれば 80 番ポート，SSH であれば 22 番ポートが開放されている. しかしながら，使用していない不要なサービスが起動していると，不要なポートも開放されることがある. このポートを探し出すことがポートスキャンである. また，ポートによっては，脆弱性を含むサービスが起動していることもあるので，攻撃される危険性もある．

5　おわりに

文責：藤原浩一

セキュリティ班の活動を通して各々が技術者として気をつけるべき問題点を知ることができた．この経験を今後の活動や実装に活かすことが望まれる．