実践セキュリティ特論II 　Blockchain理論　第三回課題

28G23027 川原尚己

1. 次のAttackコントラクトは，EtherStoreコントラクトに対してRe-Entrancy 攻撃を 実行するSolidtyコードである．攻撃機序を説明せよ．

　まず，Attackコントラクトの５行目から７行目において，攻撃対象のコントラクトの残高を取得する．その後，の残高がAMOUNTより大きければ，からAMOUNTだけの残高を引き出す．ここまでは通常の操作であるが，今回の攻撃ではここでfallback関数という特殊な処理を行うことにより，再びよりAMOUNTの量だけ残高を引き出すことができる．Re-Entrancy攻撃では，より残高を引き出すたびにfallback関数を使用することにより，何度でも残高を引き出すという攻撃である．

　このような攻撃が可能となる原因は，処理が「残高の引き出し」→「の残高の更新」という順に行われているからである．残高の引き出しを行ったときにfallback関数を呼び出すことによって，の残高を更新させずに引き出し操作を行うことができる．

1. SolidityにおけるRe-Entrancy 攻撃の対策を考察せよ．

　Re-Entrancy攻撃は，の残高を更新する前に引き出していたことが脆弱性となっていたため，「の残高の更新」→「残高の引き出し」の順に操作を行うことで防ぐことができると考えられる．

　あるいは，出金処理中は他の処理を受け付けないようにすることでfallback関数を拒否することができると考えられる．

参考文献：

[1]: <https://recruit.gmo.jp/engineer/jisedai/blog/reentrancy-and-verification-tool/>

(Ethereum最凶の脆弱性をコントラクト実行の仕組みから読み解く&検査ツール紹介，GMO，2021)

[2]: <https://qiita.com/blueplanet/items/7a56b10fe5aea477bf8c>

(初心者向け Solidity セキュリティ入門：Re-Entrancy 攻撃と対応方法，2022)