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Cの残高を取得する．その後，Cの残高が AMOUNT より大きければ，C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C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，C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」→「C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，C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．

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

　Re-Entrancy 攻撃は，C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，「C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)