



仙台CTF2018 セキュリティ技術競技会(CTF)

問題解説 雑学

平成30年11月10日
仙台CTF推進プロジェクト
五十嵐 良一



Trivia01

問題1

2018年1月4日(日本時間)に公開されたある脆弱性の論文では、説明のために以下のコードが用いられています。

```
1 ; rcx = kernel address
2 ; rbx = probe array
3 retry:
4 mov al, byte [rcx]
5 shl rax, 0xc
6 jz retry
7 mov rbx, qword [rbx + rax]
```

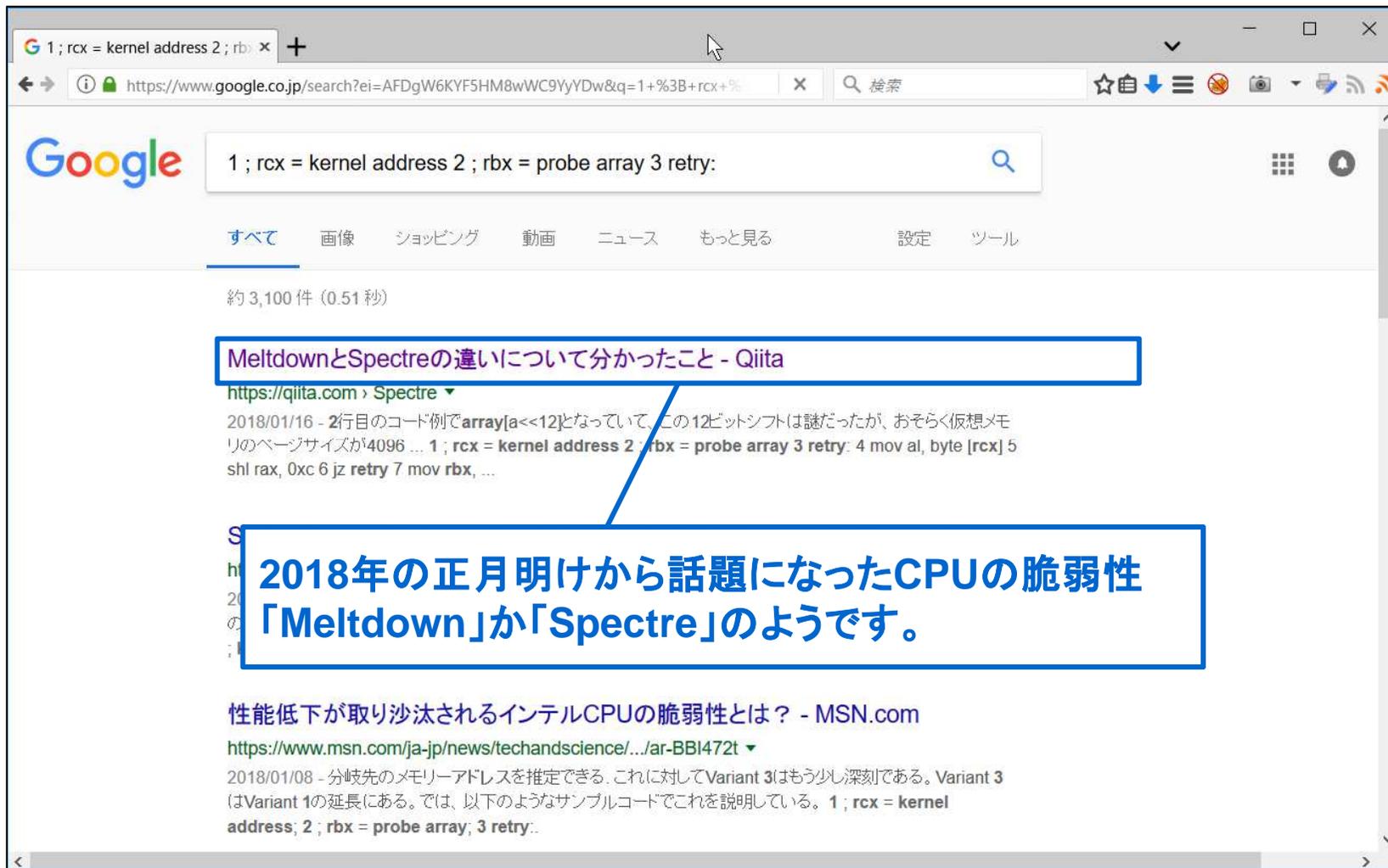
論文執筆者がこの脆弱性につけた名称を教えてください。

[フラグ]

- 脆弱性の名称(半角アルファベット小文字)
例: heartbleed

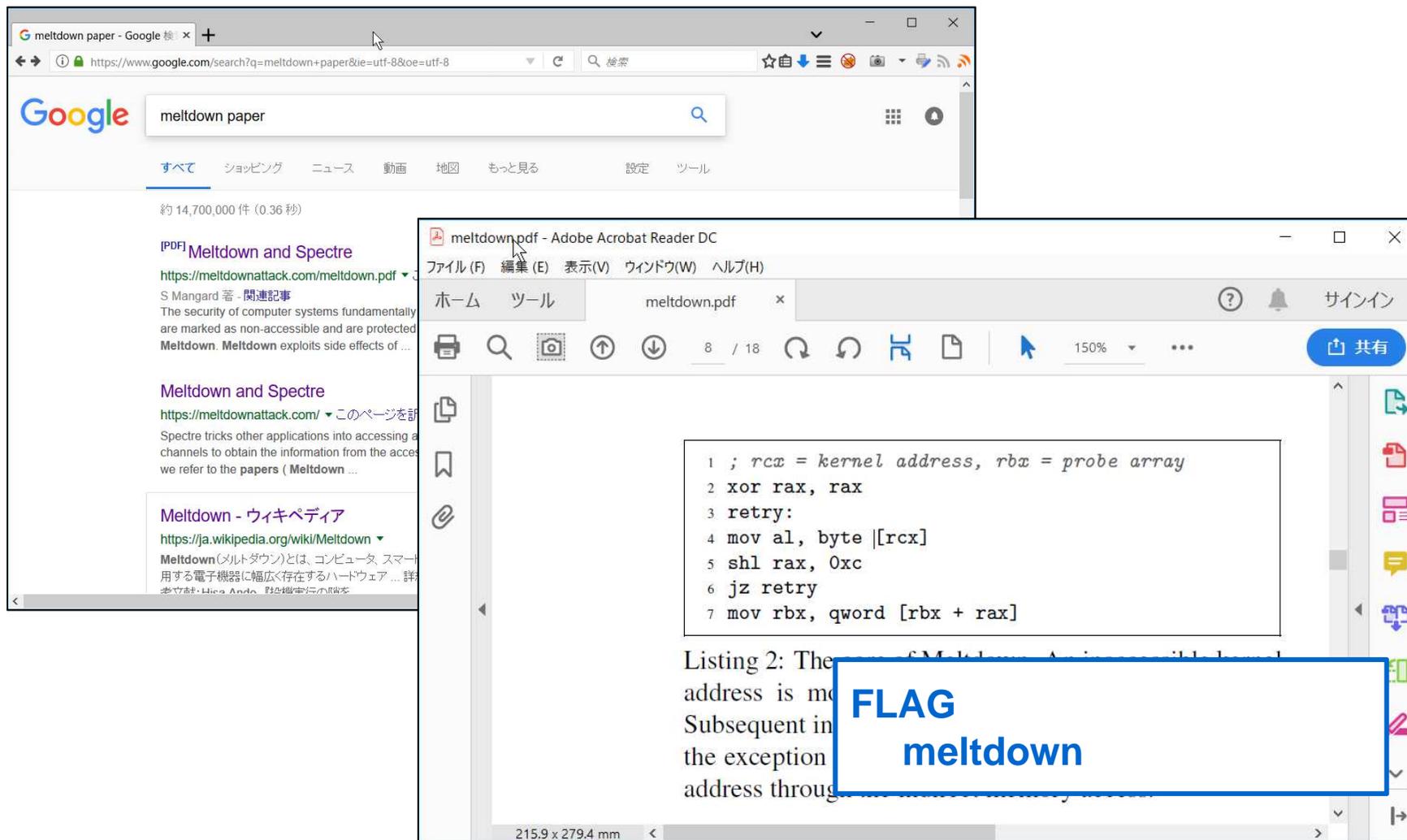
解説

- とりあえずアセンブリコード「1 ; rcx = kernel address 2 ; rbx = probe array 3 retry:」をググってみます。



解説

- 「Meltdown」の論文を確認すると、問題文のコードが記載されていることが分かります。





Trivia02

問題2

ブラウザで仮想通貨を発掘するCoinhiveなどのツールやマルウェアを利用し、他人のコンピュータの能力を勝手に使って仮想通貨のマイニングを行う行為の名称(通称)を教えてください。

[フラグ]

- 上記のような行為の名称(全角カタカナ)
例:クロスサイトスクリプティング

解説

- 「Coinhive 他人のコンピュータの能力を勝手に」などのキーワードでググってみます。

The image shows a Google search for "Coinhive 他人のコンピュータの能力を勝手に" and a corresponding Norton security alert. The search results include articles from norton.com, forbesjapan.com, and cnet.com. The Norton alert displays a message: "自分のPCやスマホが使われるcoinhive" and "2-3. ノートンにとってのcoinhive". A blue box highlights the text: "ノートンではcoinhiveを「JS.Webcoinminer」として定義、検出しています。英語ですが、こちらにその解説があります。ノートンの日本語公式ツイッターでも、「他人のPCで仮想通貨を勝手に採掘するクリプトジャッキングという手法」として定義しています。". Below this, another blue box highlights the text: "FLAG クリプトジャッキング". A message box says "攻撃を遮断しました。" with a "詳細を表示する" link. At the bottom, it says: "上記の通りノートンはcoinhiveを検出しますが、マルウェアの条件である「ウイルス」「ワーム」「トロイの木馬」に分類していません。「その他」としてしています。"



Trivia03

問題3

パソコンやスマホに残された不都合なデジタル記録を依頼により抹消する仕事屋を題材とした日本の小説で、2018年7月からドラマ放送もされた作品のタイトルを教えてください。

[フラグ]

- 作品のタイトル(半角アルファベット小文字)
例: scarecrow

解説

- 「パソコンやスマホに残された不都合なデジタル記録を依頼により抹消」などのキーワードでググってみます。

