知らないけどきっとそう。 RSS

<前の日

2017-02-26 SHAttered で Git の SHA-1 ハッシュを衝突させられるか試す

https://shattered.it/ のリリースを受けて、Git において、違うファイルをコミットしたにも関わらず、それらのコミットを参照する SHA-1 ハッシュが同じである状態を実現できるかを試しました。

同じ SHA-1 ハッシュを持つ PDF ファイルで可能か

https://shattered.it/ で公開されている、SHA-1 ハッシュが同じ PDF ファイルを、それぞれ空のレポジトリにコミットします。

```
$ wget https://shattered.it/static/shattered-1.pdf https://shattered.it/static/shattered-2.pdf
$ diff shattered-1.pdf shattered-2.pdf
Binary files shattered-1.pdf and shattered-2.pdf differ
$ shasum shattered-1.pdf shattered-2.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  shattered-1.pdf
38762cf7f55934b34d179ae6a4c80cadccbb7f0a  shattered-2.pdf
```

```
$ cp shattered-1.pdf shattered.pdf
$ git --git-dir=.git-1 --work-tree=. init
Initialized empty Git repository in /path/to/.git-1/
$ git --git-dir=.git-1 --work-tree=. add shattered.pdf
$ GIT_AUTHOR_DATE='Fri Feb 24 15:00:00 JST 2017' GIT_COMMITTER_DATE='Fri Feb 24 15:00:00 JST 2017' git --git
[master (root-commit) e95789a] test
 1 file changed, 0 insertions(+), 0 deletions(-)
 create mode 100644 shattered.pdf
$ git --git-dir=.git-1 --work-tree=. log --pretty=fuller
commit e95789af5bf00006938d8ab048ab51c9b68711a6
Author:     asannou <asannou@example.com>
AuthorDate: Fri Feb 24 15:00:00 2017 +0900
Commit:     asannou <asannou@example.com>
CommitDate: Fri Feb 24 15:00:00 2017 +0900

    test
```

shattered-1.pdf をコミットしたときの SHA-1 ハッシュは e95789af5bf00006938d8ab048ab51c9b68711a6 です。

```
$ cp shattered-2.pdf shattered.pdf
$ git --git-dir=.git-2 --work-tree=. init
Initialized empty Git repository in /path/to/.git-2/
$ git --git-dir=.git-2 --work-tree=. add shattered.pdf
$ GIT_AUTHOR_DATE='Fri Feb 24 15:00:00 JST 2017' GIT_COMMITTER_DATE='Fri Feb 24 15:00:00 JST 2017' git --git
[master (root-commit) ded44e8] test
 1 file changed, 0 insertions(+), 0 deletions(-)
 create mode 100644 shattered.pdf
$ git --git-dir=.git-2 --work-tree=. log --pretty=fuller
commit ded44e864ff901c3bb6367f13ad6aeb0b6c0cfa0
Author:     asannou <asannou@example.com>
AuthorDate: Fri Feb 24 15:00:00 2017 +0900
Commit:     asannou <asannou@example.com>
```