技術ノート KGTN 2018121301

現　象

[GGH4.8-6.X] ソフトバンクで発生した通信障害は，エリクソン社の機器の証明書の期限切れだと言われているが，GG で同様の現象が発生する可能性はないのか？

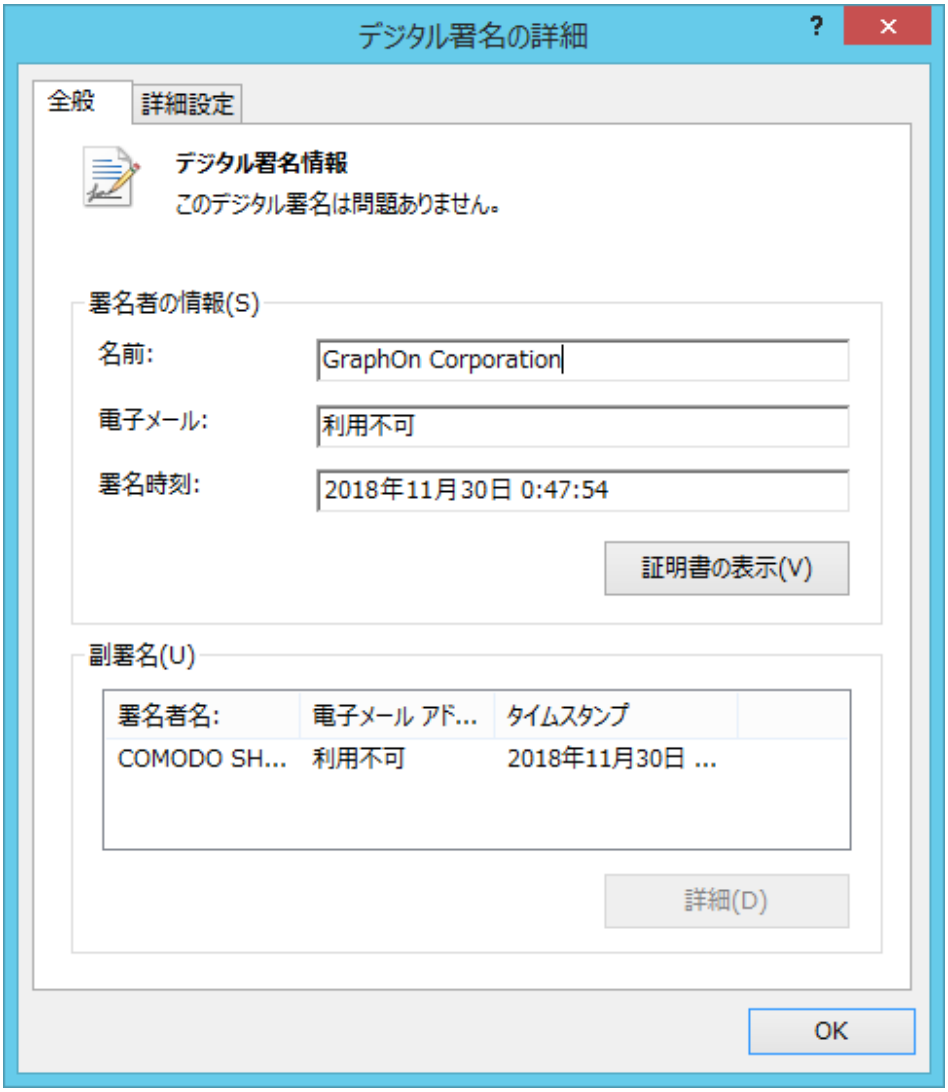
説　明

この件に関する GraphOn 社の開発責任者のコメントは次の通りです：

> The press release mentioned software with an expired certificate, but it's not clear about what type of certificate expired and what led to the problem. I did not read anything that suggested GO-Global might have the same problem. GO-Global's binaries are signed with a code-signing certificate that is valid at the time the product is built. If the code-signing certificate expires at a later date, that does not weaken the protections that the certificate provides to products that were signed with it while it was valid. The code-signing certificate must only be valid at the time it is used to sign the binaries.
>
> プレスリリースで，は期限切れの証明書付きのソフトウエアが原因だと書かれていましたが，期限切れした証明書の種類や問題の原因については書かれていませんでした．このため，GO-Global で同様の問題が起きるかどうかを示唆する情報は読み取ることが出来ませんでした．
>
> GO-Global のバイナリ（ソフトウエア）は，製品を作成した時に期限が有効なコードサイニング証明書で署名されます．このコードサイニング証明書が後に期限切れになった時も，（タイムスタンプを設定して署名していますので）証明書が有効な時と同様に機能します．つまり，コードサイニング証明書はバイナリの署名に使用する時点でのみ有効でなければなりません．

タイムスタンプについては，下記ページをご覧下さい．
https://comodo.jp/support/codesign/dtl_49

> **タイムスタンプサーバとは?**
>
> 解決方法
> たとえどのような暗号化を施した鍵ペア（秘密鍵と公開鍵）であっても 多くの時間をかければ解読しうることは数学的に証明されておりますので、デジタル証明書が有効期限をもつことはセキュリティの大原則です。
>
> お客様の署名したデジタルIDは、その満了日に期限切れとなります。しかしながら、大抵のソフトウェアは、1年間よりも長く利用される製品として設計されております。
>
> あなたの証明書が期限切れになるたびに、ソフトウェアを廃棄などしなければな らないことを避けるために、タイムスタンプサービスを利用することをご紹介い たします。
> お客様がソフトウェア（コード）に署名をする時、お客様のコードのハッシュ値 と署名された日時を認証局に送信します。
> こうすることでお客様の署名されたデジタルIDが期限切れになっても、その署名 済みのプログラムを破棄・再署名等をする必要はなくなります。
> 取得されたコード証明書の有効期限切れ後であっても有効期間内に署名したプロ グラムを有効に使えるようにするために[マイクロソフト署名コード] 等の多く の署名ツールではこのようにタイムスタンプを指定する機能を兼ねそなえております。



GO-Global のバイナリにはタイムスタンプ(副署名)が設定されているため，署名に使用したコードサイニング証明書が期限切れになった後も機能します.

Last reviewed: Dec 13, 2018
Status: DRAFT
Ref: CASE#52886