

技術ノート KGTN 2014050701

現象

[GGW3.2.1] 技術ノート KGTN#2013110601 の SYMEVENT 関連の情報を得たが、この情報から BSOD の原因は分かるか？

説明

SYMEVENT 関連の情報をもとに GraphOn 社で調査を行ったところ、BSOD を引き起こしたと思われる原因が分かりました。

The issue occurs in version 3.2 when a session closes while the "csrss.exe" process is displaying a dialog box. It is uncommon for "csrss.exe" to display a dialog box, but it does display a dialog box when a hard error (e.g., unhandled access violation) occurs in a process. In the crash you reported, the "csrss.exe" was displaying a hard error dialog.

When a session closes, the logon process enumerates all top level windows running in the session and terminates the processes that created the windows. The logon process is supposed to skip (not terminate) critical processes, but in version 3.2, it did not skip "csrss.exe". Since "csrss.exe" is a critical system process, a BSOD occurs when the logon process terminates it. In version 4.0.1 and later, the logon process does not terminate "csrss.exe". Customers running version 3.2 can work around the issue by making the registry change described below.

```
HKLM\SYSTEM\CurrentControlSet\Control\Windows\ErrorMode REG_DWORD 2
```

何らかの原因で Windows のハードエラーが発生し、**csrss.exe** がダイアログボックスを表示したと思われます (通常 **csrss.exe** がダイアログボックスを表示することはありません)。GG はログアウト時にセッション中で動作しているトップレベルのウィンドウを強制終了させますが、この時 **csrss.exe** のダイアログボックスが存在すると **csrss.exe** も強制終了の対象となり、この結果 BSOD が発生します。本質的な原因はハードエラーですが、対症療法として下記のレジストリ (の値) を設定することでハードエラーの表示を抑止し、BSOD を回避することが出来ます。なお、モード 2 を設定することで「常にイベント ログにエラーをログし、ハード エラーに [ok] を返します。ポップアップは表示されません」という動作になります (マイクロソフト社の知識ベース KB128642 より)。

```
HKLM\SYSTEM\CurrentControlSet\Control\Windows\ErrorMode REG_DWORD 2
```

Last reviewed: May 07, 2014

Status: DRAFT

Ref: KGTN#2013110601, CASE#40786, KB128642

Copyright © 2014 kitASP Corporation