SSLデフォルト設定の調査
- サーバ編 -

No.	Cipher Suite			SSL/TLS Version	OpenSSL 0.9.8r ※1						OpenSSL 1.0.0e						IIS 6.0	IIS 7.0	IIS 7.5
	Hex Value	Cipher Suite	Cipher Suite (OpenSSL Short Name)		Ubuntu 11.10 Sever ※2	Red Hat Enterprise Linux 5.4	Red Hat Enterprise Linux 6.1 ※2	Windows Server 2003 SP2	Windows Web Server 2008 SP2	Windows Server 2008 R2 SP1	Ubuntu 11.10 Sever	Red Hat Enterprise Linux 5.4 ※2	Red Hat Enterprise Linux 6.1	Windows Server 2003 SP2	Windows Web Server 2008 SP2	Windows Server 2008 R2 SP1	Windows Server 2003 SP2	Windows Web Server 2008 SP2	Windows Server 2008 R2 SP1
					s1	s2	s3	s4	s5	s6	s7	s8	s9	s10	s11	s12	s13	s14	s15
1	0x0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5	EXP-RC4-MD5	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○	○		
2	0x0004	TLS_RSA_WITH_RC4_128_MD5	RC4-MD5	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	0x0005	TLS_RSA_WITH_RC4_128_SHA	RC4-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
4	0x0006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	EXP-RC2-CBC-MD5	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○	○		
5	0x0007	TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA	SSL 3.0 / TLS 1.0	○		○	○	○	○		○		○	○	○			
6	0x0008	TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○			
7	0x0009	TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○	○		
8	0x000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
9	0x0011	TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○			
10	0x0012	TLS_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-DES-CBC-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○	○		
11	0x0013	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
12	0x0014	TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○			
13	0x0015	TLS_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○			
14	0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○			
15	0x001E	TLS_KRB5_WITH_DES_CBC_SHA	KRB5-DES-CBC-SHA	SSL 3.0 / TLS 1.0		○							○						
16	0x001F	TLS_KRB5_WITH_3DES_EDE_CBC_SHA	KRB5-DES-CBC3-SHA	SSL 3.0 / TLS 1.0		○							○						
17	0x0020	TLS_KRB5_WITH_RC4_128_SHA	KRB5-RC4-SHA	SSL 3.0 / TLS 1.0		○							○						
18	0x0022	TLS_KRB5_WITH_DES_CBC_MD5	KRB5-DES-CBC-MD5	SSL 3.0 / TLS 1.0		○							○						
19	0x0023	TLS_KRB5_WITH_3DES_EDE_CBC_MD5	KRB5-DES-CBC3-MD5	SSL 3.0 / TLS 1.0		○							○						
20	0x0024	TLS_KRB5_WITH_RC4_128_MD5	KRB5-RC4-MD5	SSL 3.0 / TLS 1.0		○							○						
21	0x0026	TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA	EXP-KRB5-DES-CBC-SHA	SSL 3.0 / TLS 1.0		○							○						
22	0x0027	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_SHA	EXP-KRB5-RC2-CBC-SHA	SSL 3.0 / TLS 1.0		○							○						
23	0x0028	TLS_KRB5_EXPORT_WITH_RC4_40_SHA	EXP-KRB5-RC4-SHA	SSL 3.0 / TLS 1.0		○							○						
24	0x0029	TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5	EXP-KRB5-DES-CBC-MD5	SSL 3.0 / TLS 1.0		○							○						
25	0x002A	TLS_KRB5_EXPORT_WITH_RC2_CBC_40_MD5	EXP-KRB5-RC2-CBC-MD5	SSL 3.0 / TLS 1.0		○							○						
26	0x002B	TLS_KRB5_EXPORT_WITH_RC4_40_MD5	EXP-KRB5-RC4-MD5	SSL 3.0 / TLS 1.0		○							○						
27	0x002F	TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○		○	○
28	0x0032	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE-DSS-AES128-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○		○	○
29	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○			
30	0x0035	TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○		○	○
31	0x0038	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE-DSS-AES256-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○		○	○
32	0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	SSL 3.0 / TLS 1.0	○	○	○	○	○	○	○	○	○	○	○	○			
33	0x0041	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
34	0x0044	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	DHE-DSS-CAMELLIA128-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
35	0x0045	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
36	0x0062	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DES-CBC-SHA	SSL 3.0 / TLS 1.0													○		
37	0x0063	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	EXP1024-DHE-DSS-DES-CBC-SHA	SSL 3.0 / TLS 1.0													○		
38	0x0064	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	EXP1024-RC4-SHA	SSL 3.0 / TLS 1.0													○		
39	0x0084	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
40	0x0087	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	DHE-DSS-CAMELLIA256-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
41	0x0088	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
42	0x008A	TLS_PSK_WITH_RC4_128_SHA	PSK-RC4-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
43	0x008B	TLS_PSK_WITH_3DES_EDE_CBC_SHA	PSK-3DES-EDE-CBC-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
44	0x008C	TLS_PSK_WITH_AES_128_CBC_SHA	PSK-AES128-CBC-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
45	0x008D	TLS_PSK_WITH_AES_256_CBC_SHA	PSK-AES256-CBC-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
46	0x0096	TLS_RSA_WITH_SEED_CBC_SHA	SEED-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
47	0x0099	TLS_DHE_DSS_WITH_SEED_CBC_SHA	DHE-DSS-SEED-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
48	0x009A	TLS_DHE_RSA_WITH_SEED_CBC_SHA	DHE-RSA-SEED-SHA	SSL 3.0 / TLS 1.0							○	○	○	○	○	○			
49	0xC002	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	ECDH-ECDSA-RC4-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
50	0xC003	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDH-ECDSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
51	0xC004	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
52	0xC005	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH-ECDSA-AES256-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
53	0xC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
54	0xC008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
55	0xC009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○		○	○
56	0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○		○	○
57	0xC00C	TLS_ECDH_RSA_WITH_RC4_128_SHA	ECDH-RSA-RC4-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
58	0xC00D	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	ECDH-RSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
59	0xC00E	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
60	0xC00F	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDH-RSA-AES256-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
61	0xC011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	ECDHE-RSA-RC4-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
62	0xC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○			
63	0xC013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○		○	○
64	0xC014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	SSL 3.0 / TLS 1.0							○	○		○	○	○		○	○
65	0x010080	SSL_CK_RC4_128_WITH_MD5	RC4-MD5	SSL 2.0	○	○	○	○	○	○							○	○	○
66	0x020080	SSL_CK_RC4_128_EXPORT40_WITH_MD5	EXP-RC4-MD5	SSL 2.0	○	○	○	○	○	○							○		
67	0x030080	SSL_CK_RC2_128_CBC_WITH_MD5	RC2-CBC-MD5	SSL 2.0	○	○	○	○	○	○							○		
68	0x040080	SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5	EXP-RC2-CBC-MD5	SSL 2.0	○	○	○	○	○	○							○		
69	0x050080	SSL_CK_IDEA_128_CBC_WITH_MD5	IDEA-CBC-MD5	SSL 2.0	○		○	○	○	○									
70	0x060040	SSL_CK_DES_64_CBC_WITH_MD5	DES-CBC-MD5	SSL 2.0	○	○	○	○	○	○							○		
71	0x0700C0	SSL_CK_DES_192_EDE3_CBC_WITH_MD5	DES-CBC3-MD5	SSL 2.0	○	○	○	○	○	○							○	○	○

※1: Red Hat Enterprise Linux 5.4では、OpenSSL 0.9.8系でサポートされている最新バージョンである「OpenSSL 0.9.8e-fips-rhel5」により調査を実施。
※2: Red Hat Enterprise Linux 6.1と Ubuntu 11.10 Server の OpenSSL0.9.8r 、Red Hat Enterprise Linux 5.4 の OpenSSL1.0.0e は、該当するOpenSSLがプラットフォーム側でサポートされていない（パッケージとして提供されていない）ため、それぞれソースからインストールして調査を実施。

SSLデフォルト設定の調査
－ クライアント編 －

No.	Cipher Suite		SSL/TLS Version	Internet Explorer (IE7)		Internet Explorer (IE8)				Internet Explorer (IE9)		
	Hex Value	Cipher Suite		Windows XP Service pack 3	Windows Vista Service pack 2	Windows XP Service pack 3	Windows Vista Service pack 2	Windows 7 Home Premium Service pack 1	Windows 7 Professional Service pack 1	Windows Vista Service pack 2	Windows 7 Home Premium Service pack 1	Windows 7 Professional Service pack 1
				c1	c2	c3	c4	c5	c6	c7	c8	c9
1	0x0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5	SSL 3.0 / TLS 1.0	7		7						
2	0x0004	TLS_RSA_WITH_RC4_128_MD5	SSL 3.0 / TLS 1.0	1	12	1	12	12	12	12	12	12
3	0x0005	TLS_RSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0	2	3	2	3	3	3	3	3	3
4	0x0006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	SSL 3.0 / TLS 1.0	8		8						
5	0x0009	TLS_RSA_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	4		4						
6	0x000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	3	4	3	4	4	4	4	4	4
7	0x000D	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0									
8	0x0010	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0									
9	0x0012	TLS_DHE_DSS_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	10		10						
10	0x0013	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0	9	11	9	11	11	11	11	11	11
11	0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0									
12	0x002F	TLS_RSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0		1		1	1	1	1	1	1
13	0x0030	TLS_DH_DSS_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0									
14	0x0031	TLS_DH_RSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0									
15	0x0032	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0		9		9	9	9	9	9	9
16	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0									
17	0x0035	TLS_RSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0		2		2	2	2	2	2	2
18	0x0036	TLS_DH_DSS_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0									
19	0x0037	TLS_DH_RSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0									
20	0x0038	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0		10		10	10	10	10	10	10
21	0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0									
22	0x003C	TLS_RSA_WITH_AES_128_CBC_SHA256	SSL 3.0 / TLS 1.0									
23	0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256	SSL 3.0 / TLS 1.0									
24	0x003E	TLS_DH_DSS_WITH_AES_128_CBC_SHA256	SSL 3.0 / TLS 1.0									
25	0x003F	TLS_DH_RSA_WITH_AES_128_CBC_SHA256	SSL 3.0 / TLS 1.0									
26	0x0040	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	SSL 3.0 / TLS 1.0									
27	0x0041	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	SSL 3.0 / TLS 1.0									
28	0x0044	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	SSL 3.0 / TLS 1.0									
29	0x0045	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	SSL 3.0 / TLS 1.0									
30	0x0062	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	6		6						
31	0x0063	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA	SSL 3.0 / TLS 1.0	11		11						
32	0x0064	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA	SSL 3.0 / TLS 1.0	5		5						
33	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	SSL 3.0 / TLS 1.0									
34	0x0068	TLS_DH_DSS_WITH_AES_256_CBC_SHA256	SSL 3.0 / TLS 1.0									
35	0x0069	TLS_DH_RSA_WITH_AES_256_CBC_SHA256	SSL 3.0 / TLS 1.0									
36	0x0066	TLS_DHE_DSS_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0									
37	0x006A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	SSL 3.0 / TLS 1.0									
38	0x006B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	SSL 3.0 / TLS 1.0									
39	0x0084	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	SSL 3.0 / TLS 1.0									
40	0x0087	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	SSL 3.0 / TLS 1.0									
41	0x0088	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	SSL 3.0 / TLS 1.0									
42	0x0096	TLS_RSA_WITH_SEED_CBC_SHA	SSL 3.0 / TLS 1.0									
43	0xC002	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0									
44	0xC003	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0									
45	0xC004	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0									
46	0xC005	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0									
47	0xC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0									
48	0xC008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0									
49	0xC009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0		5		5	7	7	5	7	7
50	0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0		6		6	8	8	6	8	8
51	0xC00C	TLS_ECDH_RSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0									
52	0xC00D	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0									
53	0xC00E	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0									
54	0xC00F	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0									
55	0xC011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	SSL 3.0 / TLS 1.0									
56	0xC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0									
57	0xC013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	SSL 3.0 / TLS 1.0		7		7	5	5	7	5	5
58	0xC014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	SSL 3.0 / TLS 1.0		8		8	6	6	8	6	6
59	0xfeff	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	SSL 3.0 / TLS 1.0									
60	0x00ff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV										

SSLデフォルト設定の調査
－ クライアント編 －

No.	Cipher Suite		Firefox (Firefox 3.6)						Firefox (Firefox 7/Firefox 8※) ※Windows XP Service pack 3のみFirefox 8の調査を実施						
	Hex Value	Cipher Suite	Windows XP Service pack 3	Windows Vista Service pack 2	Windows 7 Home Premium Service pack 1	Windows 7 Professional Service pack 1	Mac OS X	Ubuntu 11.10 Desktop	Windows XP Service pack 3		Windows Vista Service pack 2	Windows 7 Home Premium Service pack 1	Windows 7 Professional Service pack 1	Mac OS X	Ubuntu 11.10 Desktop
			c10	c11	c12	c13	c14	c15	c16(v7) Firefox 7	c16(v8) Firefox 8	c17	c18	c19	c20	c21
1	0x0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5													
2	0x0004	TLS_RSA_WITH_RC4_128_MD5	25	25	25	25	25	25	25	25	25	25	25	25	25
3	0x0005	TLS_RSA_WITH_RC4_128_SHA	26	26	26	26	26	26	26	26	26	26	26	26	26
4	0x0006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5													
5	0x0009	TLS_RSA_WITH_DES_CBC_SHA													
6	0x000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	35	35	35	35	35	35	35	35	35	35	35	35	35
7	0x000D	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA													
8	0x0010	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA													
9	0x0012	TLS_DHE_DSS_WITH_DES_CBC_SHA													
10	0x0013	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	31	31	31	31	31	31	31	31	31	31	31	31	31
11	0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	30	30	30	30	30	30	30	30	30	30	30	30	30
12	0x002F	TLS_RSA_WITH_AES_128_CBC_SHA	27	27	27	27	27	27	27	27	27	27	27	27	27
13	0x0030	TLS_DH_DSS_WITH_AES_128_CBC_SHA													
14	0x0031	TLS_DH_RSA_WITH_AES_128_CBC_SHA													
15	0x0032	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	18	18	18	18	18	18	18	18	18	18	18	18	18
16	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	17	17	17	17	17	17	17	17	17	17	17	17	17
17	0x0035	TLS_RSA_WITH_AES_256_CBC_SHA	9	9	9	9	9	9	10	10	10	10	10	10	10
18	0x0036	TLS_DH_DSS_WITH_AES_256_CBC_SHA													
19	0x0037	TLS_DH_RSA_WITH_AES_256_CBC_SHA													
20	0x0038	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	5	5	5	5	5	5	6	6	6	6	6	6	6
21	0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	10	10	10	10	10	10	5	5	5	5	5	5	5
22	0x003C	TLS_RSA_WITH_AES_128_CBC_SHA256													
23	0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256													
24	0x003E	TLS_DH_DSS_WITH_AES_128_CBC_SHA256													
25	0x003F	TLS_DH_RSA_WITH_AES_128_CBC_SHA256													
26	0x0040	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256													
27	0x0041	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	24	24	24	24	24	24	24	24	24	24	24	24	24
28	0x0044	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	16	16	16	16	16	16	16	16	16	16	16	16	16
29	0x0045	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	15	15	15	15	15	15	15	15	15	15	15	15	15
30	0x0062	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA													
31	0x0063	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA													
32	0x0064	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA													
33	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256													
34	0x0068	TLS_DH_DSS_WITH_AES_256_CBC_SHA256													
35	0x0069	TLS_DH_RSA_WITH_AES_256_CBC_SHA256													
36	0x0066	TLS_DHE_DSS_WITH_RC4_128_SHA													
37	0x006A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256													
38	0x006B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256													
39	0x0084	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	8	8	8	8	8	8	9	9	9	9	9	9	9
40	0x0087	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	4	4	4	4	4	4	4	4	4	4	4	4	4
41	0x0088	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	3	3	3	3	3	3	3	3	3	3	3	3	3
42	0x0096	TLS_RSA_WITH_SEED_CBC_SHA	23	23	23	23	23	23	23	23	23	23	23	23	23
43	0xC002	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	21	21	21	21	21	21	21	21	21	21	21	21	21
44	0xC003	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	33	33	33	33	33	33	33	33	33	33	33	33	33
45	0xC004	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	22	22	22	22	22	22	22	22	22	22	22	22	22
46	0xC005	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	7	7	7	7	7	7	8	8	8	8	8	8	8
47	0xC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	11	11	11	11	11	11	11	11	11	11	11	11	11
48	0xC008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	28	28	28	28	28	28	28	28	28	28	28	28	28
49	0xC009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	12	12	12	12	12	12	12	12	12	12	12	12	12
50	0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	1	1	1	1	1	1	1	1	1	1	1	1	1
51	0xC00C	TLS_ECDH_RSA_WITH_RC4_128_SHA	19	19	19	19	19	19	19	19	19	19	19	19	19
52	0xC00D	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	32	32	32	32	32	32	32	32	32	32	32	32	32
53	0xC00E	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	20	20	20	20	20	20	20	20	20	20	20	20	20
54	0xC00F	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	6	6	6	6	6	6	7	7	7	7	7	7	7
55	0xC011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	13	13	13	13	13	13	13	13	13	13	13	13	13
56	0xC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	29	29	29	29	29	29	29	29	29	29	29	29	29
57	0xC013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	14	14	14	14	14	14	14	14	14	14	14	14	14
58	0xC014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	2	2	2	2	2	2	2	2	2	2	2	2	2
59	0xfeff	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	34	34	34	34	34	34	34	34	34	34	34	34	34
60	0x00ff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV	○	○	○	○	○	○	○	○	○	○	○	○	○

SSLデフォルト設定の調査
－ クライアント編 －

No.	Cipher Suite		Google Chrome (Chrome 15)						Opera (Opera 11.52)						Safari (Safari 5.1.1)				
	Hex Value	Cipher Suite	Windows XP Service pack 3	Windows Vista Service pack 2	Windows 7 Home Premium Service pack 1	Windows 7 Professional Service pack 1	Mac OS X	Ubuntu 11.10 Desktop	Windows XP Service pack 3	Windows Vista Service pack 2	Windows 7 Home Premium Service pack 1	Windows 7 Professional Service pack 1	Mac OS X	Ubuntu 11.10 Desktop	Windows XP Service pack 3	Windows Vista Service pack 2	Windows 7 Home Premium Service pack 1	Windows 7 Professional Service pack 1	Mac OS X
			c22	c23	c24	c25	c26	c27	c28	c29	c30	c31	c32	c33	c34	c35	c36	c37	c38
1	0x0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5													7				
2	0x0004	TLS_RSA_WITH_RC4_128_MD5	26	26	26	26	26	26	22	22	22	22	22	22	1	12	12	12	19
3	0x0005	TLS_RSA_WITH_RC4_128_SHA	27	27	27	27	27	27	21	21	21	21	21	21	2	3	3	3	18
4	0x0006	TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5													8				
5	0x0009	TLS_RSA_WITH_DES_CBC_SHA													4				
6	0x000A	TLS_RSA_WITH_3DES_EDE_CBC_SHA	36	36	36	36	36	36	27	27	27	27	27	27	3	4	4	4	21
7	0x000D	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA							24	24	24	24	24	24					
8	0x0010	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA							26	26	26	26	26	26					
9	0x0012	TLS_DHE_DSS_WITH_DES_CBC_SHA													10				
10	0x0013	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	32	32	32	32	32	32	23	23	23	23	23	23	9	11	11	11	27
11	0x0016	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	31	31	31	31	31	31	25	25	25	25	25	25					26
12	0x002F	TLS_RSA_WITH_AES_128_CBC_SHA	28	28	28	28	28	28	20	20	20	20	20	20		1	1	1	17
13	0x0030	TLS_DH_DSS_WITH_AES_128_CBC_SHA							19	19	19	19	19	19					
14	0x0031	TLS_DH_RSA_WITH_AES_128_CBC_SHA							18	18	18	18	18	18					
15	0x0032	TLS_DHE_DSS_WITH_AES_128_CBC_SHA	19	19	19	19	19	19	17	17	17	17	17	17		9	9	9	22
16	0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	18	18	18	18	18	18	16	16	16	16	16	16					23
17	0x0035	TLS_RSA_WITH_AES_256_CBC_SHA	10	10	10	10	10	10	10	10	10	10	10	10		2	2	2	20
18	0x0036	TLS_DH_DSS_WITH_AES_256_CBC_SHA							9	9	9	9	9	9					
19	0x0037	TLS_DH_RSA_WITH_AES_256_CBC_SHA							8	8	8	8	8	8					
20	0x0038	TLS_DHE_DSS_WITH_AES_256_CBC_SHA	6	6	6	6	6	6	7	7	7	7	7	7		10	10	10	24
21	0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	5	5	5	5	5	5	6	6	6	6	6	6					25
22	0x003C	TLS_RSA_WITH_AES_128_CBC_SHA256							15	15	15	15	15	15					
23	0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256							5	5	5	5	5	5					
24	0x003E	TLS_DH_DSS_WITH_AES_128_CBC_SHA256							14	14	14	14	14	14					
25	0x003F	TLS_DH_RSA_WITH_AES_128_CBC_SHA256							13	13	13	13	13	13					
26	0x0040	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256							12	12	12	12	12	12					
27	0x0041	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	25	25	25	25	25	25											
28	0x0044	TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	16	16	16	16	16	16											
29	0x0045	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	15	15	15	15	15	15											
30	0x0062	TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA													6				
31	0x0063	TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA													11				
32	0x0064	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA													5				
33	0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256							11	11	11	11	11	11					
34	0x0068	TLS_DH_DSS_WITH_AES_256_CBC_SHA256							4	4	4	4	4	4					
35	0x0069	TLS_DH_RSA_WITH_AES_256_CBC_SHA256							3	3	3	3	3	3					
36	0x0066	TLS_DHE_DSS_WITH_RC4_128_SHA	17	17	17	17	17	17											
37	0x006A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256							2	2	2	2	2	2					
38	0x006B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256							1	1	1	1	1	1					
39	0x0084	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	9	9	9	9	9	9											
40	0x0087	TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	4	4	4	4	4	4											
41	0x0088	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	3	3	3	3	3	3											
42	0x0096	TLS_RSA_WITH_SEED_CBC_SHA	24	24	24	24	24	24											
43	0xC002	TLS_ECDH_ECDSA_WITH_RC4_128_SHA	22	22	22	22	22	22											11
44	0xC003	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	34	34	34	34	34	34											12
45	0xC004	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	23	23	23	23	23	23											9
46	0xC005	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	8	8	8	8	8	8											10
47	0xC007	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	11	11	11	11	11	11											3
48	0xC008	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	29	29	29	29	29	29											4
49	0xC009	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	12	12	12	12	12	12								5	7	7	2
50	0xC00A	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	1	1	1	1	1	1								6	8	8	1
51	0xC00C	TLS_ECDH_RSA_WITH_RC4_128_SHA	20	20	20	20	20	20											15
52	0xC00D	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	33	33	33	33	33	33											16
53	0xC00E	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	21	21	21	21	21	21											13
54	0xC00F	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	7	7	7	7	7	7											14
55	0xC011	TLS_ECDHE_RSA_WITH_RC4_128_SHA	13	13	13	13	13	13											7
56	0xC012	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	30	30	30	30	30	30											8
57	0xC013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	14	14	14	14	14	14								7	5	5	5
58	0xC014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	2	2	2	2	2	2								8	6	6	6
59	0xfeff	SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA	35	35	35	35	35	35											
60	0x00ff	TLS_EMPTY_RENEGOTIATION_INFO_SCSV								○			○	○					