<SSL 인증서 보안 이슈>

About SHA2, SSLv3

2014-10

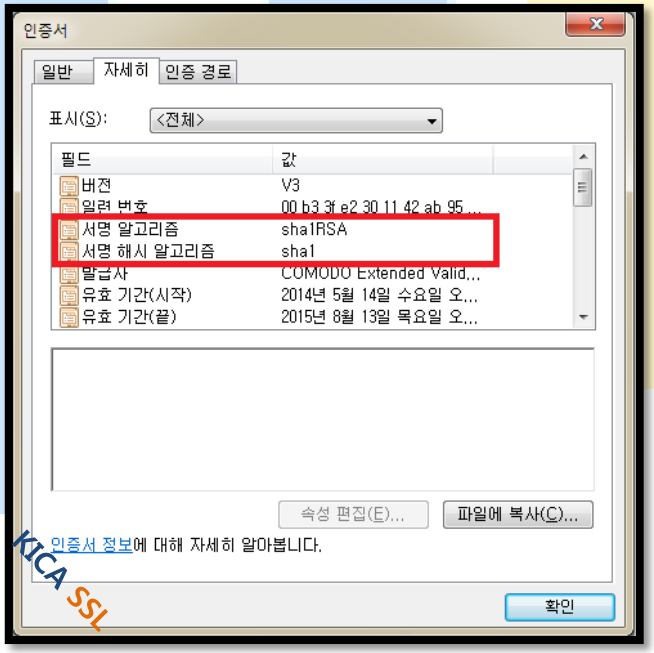
한국정보인증

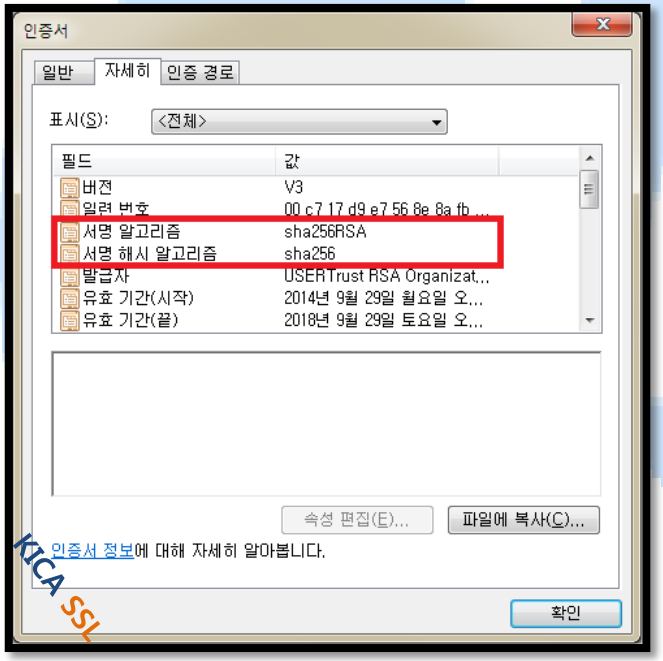
[SHA-2]

HASH 함수 중의 하나로, HASH는 *임의의 길이의 데이터*를 입력 받아 *고정된 길이의 데이터*(**해시 값**)로 출력합니다.

"동일한 데이터인 경우 동일한 해시 값을 갖는다." 에 기초하여 메시지 **무결성**(오류/변조 탐지)을 확인하기 위하여 사용됩니다. 하지만 "서로 다른 데이터라도 동일한 해시 값을 가질 수 있다."는 해시 함수의 충돌 오류 및 보안 취약점을 해결 하기 위하여 SHA-2, SHA-3 사용을 권장하고 있습니다.

[인증서에 적용된 알고리즘 확인하는 방법]





[SHA-2 인증서 전환 스케줄]

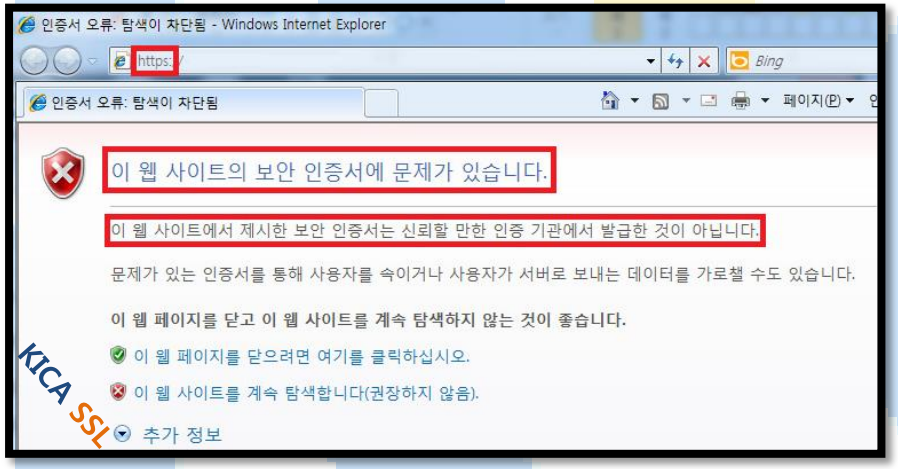
2015년 7월
Microsoft社 SHA-2 전환 가속화

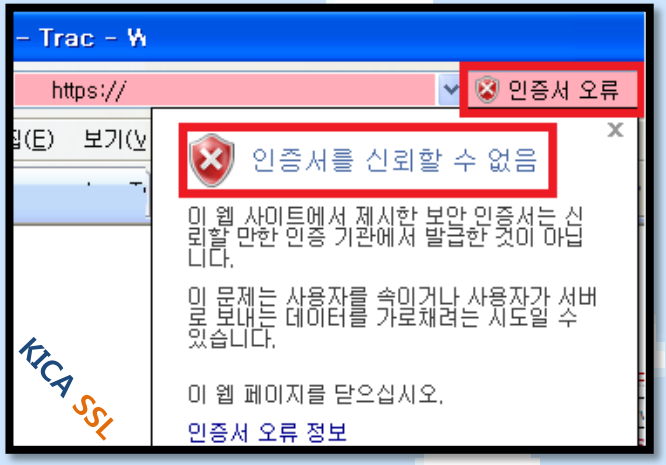
2016년 1월
만료일 기준 - FireFox, Chrome SHA-1 인증서 거절
Microsoft社 SHA-1 코드사인 인증서 거절
한국정보인증 및 COMODO SHA-1 인증서 발급 중단

2017년 1월
Microsoft社 SHA-1 SSL 인증서 거절

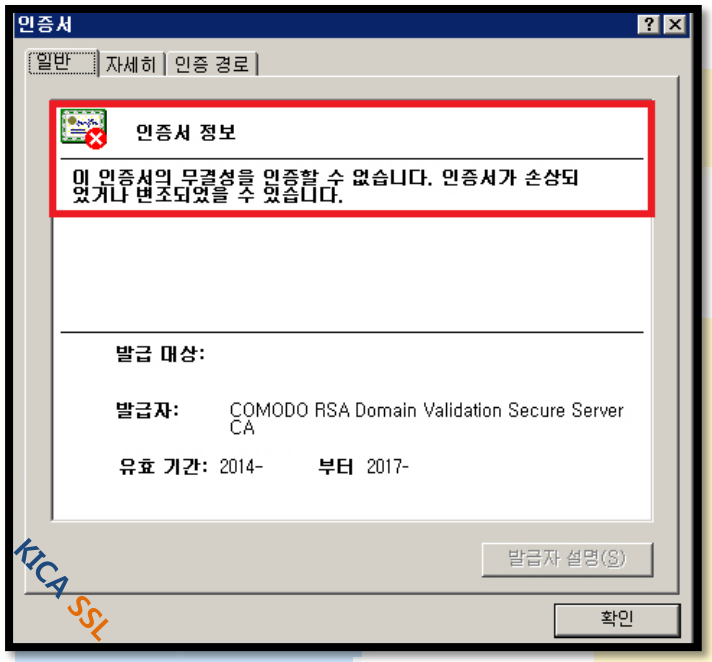
주요 브라우저에서는 SHA-1이 적용된 인증서는 앞으로는 안전하지 않은 인증서로 식별할 예정입니다.

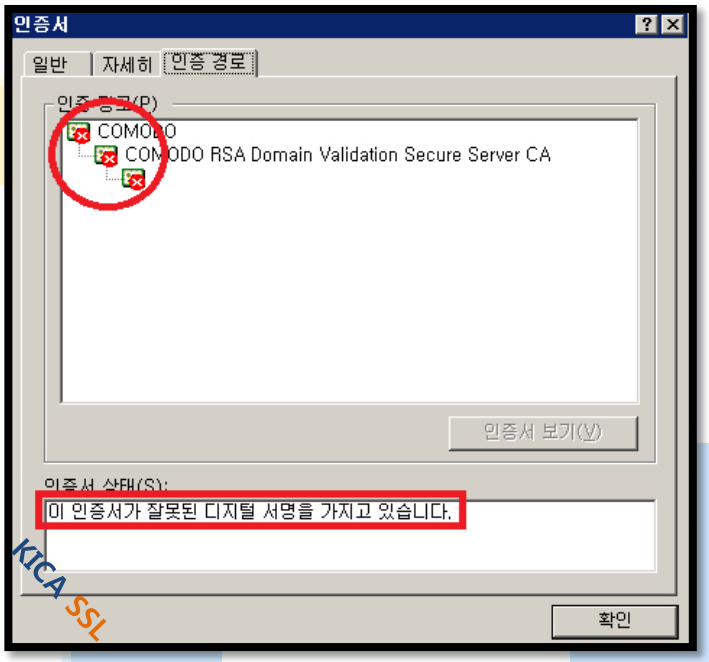
<안전하지 않은 사이트 예제 화면 - IE>



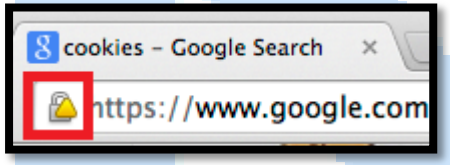


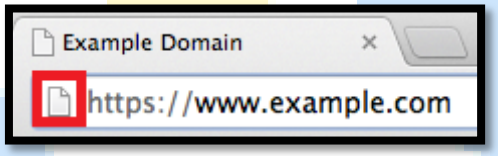
<안전하지 않은 사이트 예제 화면 – Microsoft Windows 환경>





<안전하지 않은 사이트 예제 화면 – 구글 Chrome>





[SHA-2 인증서 지원 정보]

- **SHA-2 인증서 적용 전 사이트 이용자의 환경 및 인증서가 설치/운용 될 서버의 환경을 확인하여 주시기 바랍니다.**

브라우저(Browser)	서버(Server)	운영체제(OS)
Adobe Acrobat/Reader 7	Apache (OpenSSL 0.9.8o+)	Android 2.3+
Blackberry 5+	OpenSSL 0.9.8o+ 적용된 제품	Apple iOS 3.0+
Chrome 26+, and Linux, Mac OS X 10.5, Vista+	Windows Server 2003+(KB 968730)	Apple OS X 10.5+
Firefox 1.5+	Windows Server 2008+	Blackberry 5.0+
Internet Explorer 7+ (Win7+, Vista, XP SP3)	Java based servers - 1.4.2+	ChromeOS
Java 1.4.2+ based products	Oracle WebLogic v10.3.1+(bug8422724)	Windows 7+
Konqueror 3.5.6+	Oracle Wallet Manager 11.2.0.1+	Windows Outlook 2003+ (Vista+)
Mozilla 1.4+	IBM Domino 9+	Windows Phone 7+
Mozilla (NSS 3.8+ (since April 2003))	IBM HTTP Server GSKit 7.0.4.14+	Windows Vista
Netscape 7.1+	Websphere GSKit 8+	Windows XP SP3+ (KB 968730)
Opera 9.0+	Cisco ACE module software version A4(1.0)	
OpenSSL 0.9.8o+ 적용된 제품	Citrix Receiver(Mac 11.8.2, Windows 4.1(std), Windows 3.4(ent), Windows 8/RT(1.4), Windows Phone 8(1.1))	
Safari (Mac OS X 10.5+)		
Windows Phone 7+		

MS Windows Server 2003 SHA-2 패치 다운로드 ☞

[SHA-2 인증서를 지원하지 않는 서버 정보]

- **각 제품의 일부 버전들은 SHA-2를 지원하지 않고 있으니 이점 참고하여 주시기 바랍니다.**

SHA-2 인증서를 지원하지 않는 서버
Juniper SBR
IBM Domino
Citrix Receiver models(일부, 자세한 모델은 링크 확인 (Citrix Receiver models 확인하러 가기 ☞)
Linux 13.0
IOS 5.8.3
Android 3.4.13
HTML 5 1.2
Playbook 1.0
Blackberry 2.2 / BlackBerry 1.0 Tech Preview
Cisco ACE module software versions A2 and A3

[SSLv3]

SSL 인증서를 이용한 암호화 통신시 사용하는 프로토콜 버전 중의 하나로 현재 권장사항은 TLS1.1, TLS1.2 입니다.

이 프로토콜은 인증서가 적용된 웹 서버(기타 장비등)에서 SSL Protocol 속성에서 확인 및 선택 적용할 수 있습니다.

[POODLE attack : Padding Oracle On Downgraded Legacy Encryption]

사용자와 서버간 통신시 TLS 상위 버전을 지원하지 않는 서버로 인해 사용자 환경이 취약해진 점을 노린 공격입니다.

[SSLv3 확인 방법 – openssl 이용]

openssl s_client -connect 연결주소:SSLport -ssl3

<SSLv3가 사용되지 않는 서버의 경우>

```
CONNECTED(00000003)

140128201074504:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure:s3_pkt.c:1257:SSL alert number 40
140128201074504:error:1409E0E5:SSL routines:SSL3_WRITE_BYTES:ssl handshake failure:s3_pkt.c:596: --- no peer certificate available --- No client certificate CA names sent --- SSL handshake has read 7 bytes and written 0 bytes --- New, (NONE), Cipher is (NONE) Secure Renegotiation IS NOT supported Compression: NONE Expansion: NONE SSL-Session: Protocol : SSLv3 Cipher : 0000 Session-ID: Session-ID-ctx: Master-Key: Key-Arg : None Krb5 Principal: None PSK identity: None PSK identity hint: None Start Time: 1413337595 Timeout : 7200 (sec) Verify return code: 0 (ok) ---
```


<SSLv3가 사용되는 서버의 경우>

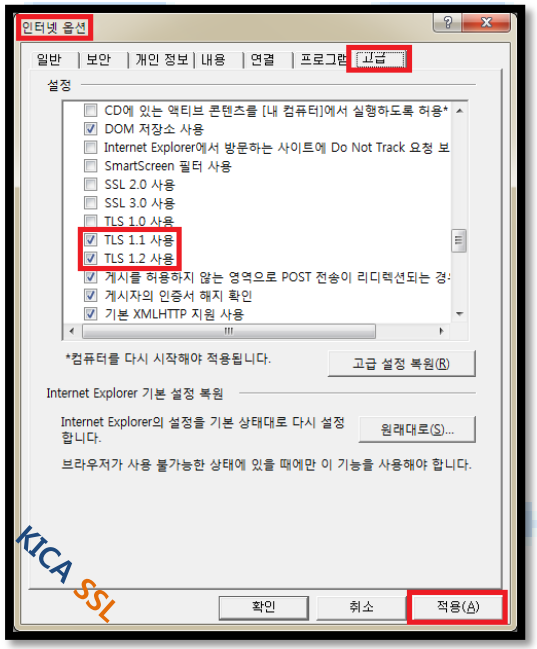
```
CONNECTED(00000003) depth=2 C = US, O = Bigger Inc., CN = Big CA verify return:1 depth=1 C = US, O = "Bigger, Inc.", CN = Big CA verify return:1 depth=0 serialNumber = -912hgd9qgwf9uewqgfiu239gf2309fg, OU = HT98723987, OU = See www.example.com/resources/cps (c)14, OU = Domain Control Validated - Big(R), CN = your.server.example.org verify return:1 --- Certificate chain 0 s:/serialNumber=-912hgd9qgwf9uewqgfiu239gf2309fg/OU=HT98723987/OU=See www.example.com/resources/cps (c)14/OU=Domain Control Validated - Big(R)/CN=your.server.example.org i:/C=US/O=Bigger, Inc./CN=Big CA 1 s:/C=US/O=Bigger, Inc./CN=Big CA i:/C=US/O=Bigger Inc./CN=Bigger CA --- Server certificate -----BEGIN CERTIFICATE----- ... -----END CERTIFICATE----- subject=/serialNumber=-912hgd9qgwf9uewqgfiu239gf2309fg/OU=HT98723987/OU=See www.example.com/resources/cps (c)14/OU=Domain Control Validated - Big(R)/CN=your.server.example.org issuer=/C=US/O=Bigger, Inc./CN=Big CA --- No client certificate CA names sent --- SSL handshake has read 3035 bytes and written 354 bytes --- New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA Server public key is 2048 bit Secure Renegotiation IS supported Compression: NONE Expansion: NONE SSL-Session: Protocol : SSLv3 Cipher : DHE-RSA-AES256-SHA Session-ID: 68FA1758EE91651850A158CF784F37BD929F0E553EFFEF6D089AEBEA1420055D Session-ID-ctx: Master-Key: 3836341955FA70674AE189C30FB44FE85537D17C9B1CF9FB7BF444155A944D080D3130801502488994DA9F1CE9DAF0D8 Key-Arg : None Krb5 Principal: None PSK identity: None PSK identity hint: None Start Time: 1413337513 Timeout : 7200 (sec) Verify return code: 0 (ok) ---
```

[해결책]

사용자의 현재 주요 브라우저는 TLS 1.1 이상을 지원하고 있습니다. 사용자 및 서버에서는 TLS 1.1 이상을 사용 할 수 있도록 설정하며, SSLv3 이하는 사용하지 않도록 설정합니다.

<사용자 환경 예>

TLS1.1 이상 프로토콜이 MS IE 8 의 경우 지원하나 기본 설정은 사용 안함으로 설정되어 있으며, MS IE 11 부터는 기본 사용으로 설정 되어 있습니다.



<Server 환경 예>

✓ **Openssl 기반 서버의 경우 ssl.conf 파일의 속성 중 아래와 같이 사용 할 수 있습니다.(OpenSSL 1.0.1 이상)**

SSLProtocol +TLSv1.1 +TLSv1.2 -SSLv2 -SSLv3

관련 취약점을 해결하고자 Openssl 에서는 아래와 같은 버전으로 업데이트를 권장하고 있습니다.

- OpenSSL 0.9.8 : 0.9.8zc로 업데이트
- OpenSSL 1.0.0 : 1.0.0o로 업데이트
- OpenSSL 1.0.1 : 1.0.1j로 업데이트

✓ **JAVA 기반 서버의 경우 server.xml 파일의 속성 중 아래와 같이 사용 할 수 있습니다.**

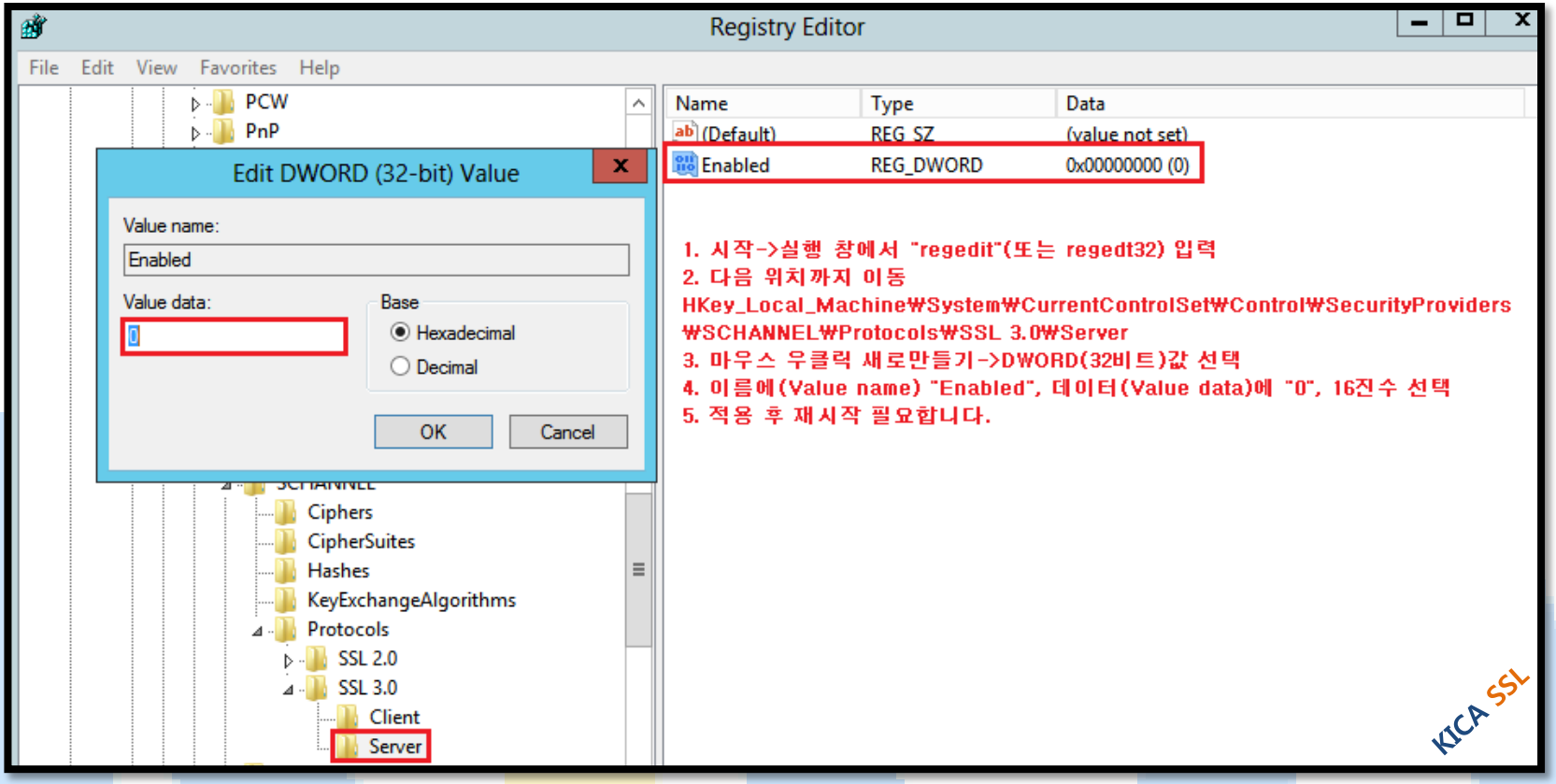
sslProtocol="TLS" sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1"

관련 사이트 : http://wiki.apache.org/tomcat/Security/POODLE

✓ **Oracle 에서는 아래 페이지에서 상품별 패치를 가이드 하고 있습니다.**

관련 사이트 : http://www.oracle.com/technetwork/topics/security/poodlecve-2014-3566-2339408.html

✓ **Windows 서버의 경우 아래와 같이 처리 할 수 있습니다.**



[주요 브라우저 지원 정보]

브라우저	버전	OS	SSL Protocol					SHA-2
			SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	
Internet Explorer	4, 5, 6	Windows 3.1, 95, 98, ME, NT 3.51, NT 4, 2000 Mac OS, OS X Solaris, HP-UX(v6 제외)	지원	지원	비활성화	미지원	미지원	미지원
	6	Windows XP	지원	지원	비활성화	미지원	미지원	SP3 필요
	7, 8	Windows XP	비활성화	지원	지원	미지원	미지원	SP3 필요
	6	Windows Server 2003	지원	지원	비활성화	미지원	미지원	KB 938397, 968730 패치 필요
	7, 8	Windows Server 2003	비활성화	지원	지원	미지원	미지원	KB 938397, 968730 패치 필요
	7, 8, 9	Windows Vista/ Server 2008	비활성화	지원	지원	미지원	미지원	지원
	8, 9, 10	Windows 7 /Server 2008 R2	비활성화	지원	지원	비활성화	비활성화	지원
	10	Windows 8 /Server 2012	비활성화	지원	지원	비활성화	비활성화	지원
	11	Windows 7, 8.1 Server 2008 R2, 2012 R2	비활성화	지원	지원	지원	지원	지원
	Mobile 7, 9	Windows Phone 7, 7.5 / 7.8	비활성화	지원	지원	미지원	미지원	지원
	Mobile 10	Windows Phone 8	비활성화	지원	지원	비활성화	비활성화	지원
	Mobile 11	Windows Phone 8.1	비활성화	지원	지원	지원	지원	지원

브라우저	버전	OS	SSL Protocol					SHA-2
			SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	
Google Chrome	1–9	Windows OS X Linux Android iOS Chrome OS	비활성화	지원	지원	미지원	미지원	지원
	10–21		미지원	지원	지원	미지원	미지원	지원
	22–25		미지원	지원	지원	지원	미지원	지원
	26–29		미지원	지원	지원	지원	미지원	지원
	30–37		미지원	지원	지원	지원	지원	지원
	38		미지원	지원	지원	지원	지원	지원

브라우저	버전	OS	SSL Protocol					SHA-2
			SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	
Mozilla Firefox	1	Windows OS X Linux Android Firefox OS	지원	지원	지원	미지원	미지원	미지원
	1.5		지원	지원	지원	미지원	미지원	지원
	2		비활성화	지원	지원	미지원	미지원	지원
	3–7		비활성화	지원	지원	미지원	미지원	지원
	8–22 ESR 10, 17		미지원	지원	지원	미지원	미지원	지원
	23		미지원	지원	지원	비활성화	미지원	지원
	24–26 ESR 24		미지원	지원	지원	비활성화	비활성화	지원
	27-32		미지원	지원	지원	지원	지원	지원
	ESR 31 33		미지원	지원	지원	지원	지원	지원

✓ **Firefox 34(11 월 25 일 릴리즈 예정)에서는 SSL v3 비활성화가 기본 적용됩니다.**

브라우저	버전	OS	SSL Protocol					SHA-2
			SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2	
Apple Safari	1	Mac OS X10.2, 10.3	미지원	지원	지원	미지원	미지원	미지원
	2–4	Mac OS X10.4	미지원	지원	지원	미지원	미지원	미지원
	3–5	Mac OS X10.5, 10.6 Mac OS X 10.7	미지원	지원	지원	미지원	미지원	지원
	6	Mac OS X 10.7 OS X 10.8	미지원	지원	지원	미지원	미지원	지원
	7	OS X 10.9	미지원	지원	지원	지원	지원	지원
	3	iPhone OS 1and2	미지원	지원	지원	미지원	미지원	미지원
	4, 5	iPhone OS 3,iOS 4	미지원	지원	지원	미지원	미지원	지원
	5, 6	iOS 5,6	미지원	지원	지원	지원	지원	지원
	7	iOS 7	미지원	지원	지원	지원	지원	지원
	8	iOS 8	미지원	지원	지원	지원	지원	지원
	3–5	Windows	미지원	지원	지원	미지원	미지원	미지원

기타 문의사항이 있으신 경우 아래 연락처로 연락 부탁 드립니다.

TEL : 02-360-3065

E-mail : webmaster@sgssl.net