Rsupport - Security white paper

2015. 4.28.

- 배경: '보안'을 바라보는 알서포트의 관점
- 원격 서비스, 편리한 만큼 안전해야

- 기술적 보안: 보안 취약점 점검 및 보호 대책 적용
- 인증 및 액세스
- 데이터 보호
- 네트워크 보안

- 물리적 보안: 데이터 센터 운영 및 관리
- 외부인 침입 통제
- 안전한 서버 운영

- 관리적 보안: 보안 체계 수립 및 운영
- 개인 정보 보호
- 보안 표준 기준 준수

- 결론: 원격 서비스 선택의 기준은 '보안'
- 보안 기준 준수를 넘어 '보안 커스터마이징'까지

- Appendix

1. 알서포트 원격 서비스의 강력한 보안 설정
2. 알서포트의 서버 보안 가이드
3. 용어 설명

배경
- '보안'을 바라보는 알서포트의 관점

원격 서비스, 편리한 만큼 안전해야

알서포트는 원격 기술 전문 기업으로, 2002년부터 원격 지원, 원격 제어, 원격 화상 회의 등 전문화된 B2B/B2C 원격 서비스를 제공하고 있습니다. 이러한 원격 서비스의 기본 목표는, 다양한 산업 분야에 종사하는 고객들이 각자 처해 있는 다양한 환경 속에서 유무선으로 연결된 IT서비스와 각종 디바이스를 보다 '편리하게 활용할 수 있도록' 하는 데에 있습니다.

이를 위해 알서포트의 원격 서비스가 추구하는 '편리함'은 다음의 네 가지 요소를 포함하고 있습니다.

1. **쉽다**: 누구나 어떤 환경에서든 간단한 절차를 통해 원격 접속을 할 수 있다.
2. **빠르다**: 원격 접속 완료까지의 시간이 짧고, 원격 접속 후의 제어 속도가 빠르다.
3. **안정적이다**: 전 세계 어디서나, 어떤 네트워크 환경에서도 끊김 없이 원격 접속을 유지할 수 있다.
4. **안전하다**: 원격 접속을 통해 송수신되는 정보는 어떤 경우에도 노출되지 않도록 안전하게 보호한다.

상기 네 가지 요소 중 1번~3번까지는 알서포트가 아닌 다른 회사의 서비스에서도 찾아낼 수 있을지도 모릅니다. 그러나, 4번의 '안전하다'를 만족시키기 위해서는 기술적, 조직적 지원은 물론 물리적 관리까지 필요하기 때문에, 이는 가장 갖추기 힘든 요소입니다. 따라서 원격 서비스의 품질을 구분짓는 가장 중요한 요소는 쉽고 빠르면서 안정적으로 송수신되는 데이터를 결국 어떻게 처리하느냐, 즉 '얼마나 안전한가'일 것입니다.

알서포트는 상기 네 가지 요소를 모두 갖춘 원격 서비스 제공을 위한 기술과 인프라를 갖추고 있으며, 서비스의 모든 단계에서 보안성을 고려하여 기술적/물리적/관리적 측면의 철저한 보안 대책을 수립 및 적용하고 있습니다.

기술적 보안
- 보안 취약점 점검 및 보호 대책 적용

인증 및 액세스

알서포트의 원격 지원 인증에 사용되는 접속 코드는 랜덤 6자리 숫자로 제공되고, 생성된 접속 코드는 상담사와의 원격 연결을 위해 일회성으로 사용되며 제 3자의 임의 접근은 원천 차단됩니다. 또한 모든 원격지원 세션은 원격 접속 페이지에서 다른 사용자들의 원격지원 리스트를 표시하지 않습니다.

원격 지원 시스템의 관리자(예. 콜센터 관리자)는 사용자(예.상담사)의 네트워크 또는 장비의 위치를 제한할 수 있습니다. 관리자는 관리 페이지에서 지정 IP 또는 IP 그룹, Mac Address 를 설정 등록하고, 사용자는 허용되는 위치에서만 원격 상담 에이전트 로그인 후 상담을 시작할 수 있습니다. 또한 관리자는 사용자에게 등급별로 직접 제어 또는 간접 제어 권한을 부여할 수 있습니다. 간접 제어 권한의 사용자는 마우스/키보드

직접 제어가 제한되며 레이저 포인터, 그리기 도구를 통한 안내 및 사용법 지시를 할 수 있습니다.

외부에서(예. 외부 용역 업체) 내부 시스템에 원격 접근해야 하는 경우, 안전한 작업을 위하여 일회성 접근 권한을 제한적으로 부여할 수 있습니다. 이 경우, 권한 부여 후 지정 시간 이내에 1회만 접속이 가능하고 모든 원격 작업 로그가 저장됩니다. 또한 OTP, SMS, E-mail을 이용한 사용자 이중 인증으로 더욱 안전 합니다.

데이터 보호

접속 정보를 암호화 처리 없이 평문(plain text)으로 전송하면 스니핑(Sniffing)에 의해 해커에게 고스란히 노출될 위험이 있습니다. 안전한 데이터 전송을 위해서는 로컬에서 1차 암호화를 통하여 전송될 데이터에 대한 보안 처리를 거쳐야 합니다. 알서포트는 모든 원격 세션에서 전달되는 데이터를 End-To-End에서 256-bit AES (Advanced Encryption Standard)[1] 압축 암호화하여 전송합니다.

원격 지원을 하기 위해서는 제어 권한에 대한 고객의 사전동의가 필요하고, 고객의 사전동의가 있는 경우에만 화면공유 및 원격 지원이 가능합니다. 고객이 동의를 한 경우라도, 고객은 원격 지원 세션 중에 언제든지 상담사로부터 키보드/마우스 제어 권한을 회수할 수 있습니다. 또한 상담사가 원격 지원 중 파일 송수신, 화면 녹화/저장/캡쳐 등의 기능을 실행하고자 하는 경우, 사전 동의와는 별도로 기능 실행 시마다 고객의 추가 동의를 받도록 하여 고객 데이터를 안전하게 보호합니다. 뿐만 아니라 원격 지원 종료 후에는 지원을 받은 고객 PC의 원격지원 모듈을 모두 삭제할 수 있습니다

원격 지원 및 제어를 위한 채팅 및 파일 송수신 시 주고 받았던 모든 기록은 로그로 기록되며, 서버로 전송되어 안전하게 관리됩니다.

네트워크 보안

알서포트의 보안 서버는 SSL 웹 서버 인증서를 사용합니다. 원격 지원 세션 연결 시 강력한 2048-bit SSL (Secure Sockets Layer)[2] 암호화 통신을 제공합니다. SSL 웹 서버 사용으로 PC와 서버 사이에 전송되는 모든 데이터에 대해서 암호화 통신을 제공함으로써, 악의적인 공격자의 스니핑(Sniffing) 공격에도 해독이 불가능한 상태로 안전하게 데이터를 전송합니다.

알서포트는 원격 서비스 사이트 접속 시 HTTPS 통신을 통한 안전한 웹 접근을 제공하며, 원격 지원 웹 서버는 외부에서 액세스 할 수 있는 페이지에 중요 데이터를 저장하지 않습니다. 클라이언트 PC 및 서버에 최신 보안 패치를 적용하며, 메시지/요청/응답 등의 세션에서 잘못된 재전송 공격을 방지하기 위한 방침을 수립하여 적용하고 있습니다.

물리적 보안
- 데이터 센터 운영 및 관리

외부인 침입 통제

알서포트는 전 세계 데이터 센터를 기반으로 한 알서포트 전용 그리드 망을 구성하고 이 망을 기반으로 서비스를 운영, 관리합니다. 현재, 알서포트의 중계 서버는 한국, 일본, 유럽(네덜란드, 아일랜드), 호주, 브라질, 미국, 싱가포르 등 8개국의 15개 edge에 위치하고 있으며, 각 데이터 센터는 24(hour) x 7(date) x 365(day) 유인 체제로 운용되고 있습니다.

데이터 센터의 출입통제는 생체인식 보안 시스템으로 관리되고 있으며, 정보 보안 관리 책임자에 의해 교육을 받은 전담 기술자에 한해 출입 권한을 부여합니다. 출입 로그와 CCTV촬영 기록이 3개월 이상 저장되고 전용 운용 단말에 대한 상세한 계정 관리와 작업 로그 저장으로 더욱 강력한 보안을 유지하고 있습니다. 일반 업무 네트워크에서 격리된 전용 네트워크를 사용하며 외부 방문자는 출입이 불가합니다.

안전한 서버 운영

알서포트의 원격 서비스는 글로벌 수준의 클라우드 서비스(아마존, MS Azure)를 사용하므로 보안 상의 어떤 위협에 대해서도 가장 빠르고 효율적으로 대처할 수 있습니다.

알서포트는 원격 클라우드 서비스를 사용하는 고객들이 늘 안정적으로 서비스를 이용할 수 있도록 만반의 대응 체계를 갖추고 있습니다. 서버 구성을 이중화하여, 천재지변으로 특정 데이터센터가 불능 상태가 된다 하더라도 다른 데이터센터를 통해 안정적인 서비스 제공이 가능합니다.

관리적 보안
- 보안 체계 수립 및 운영

개인 정보 보호

알서포트는 정보보호 관련 법규를 준수합니다. 대륙별, 국가별 관련 법령 또한 엄격히 준수하며, 국가 간의 개인정보 데이터 이전에 대한 관한 개인정보보호법을 엄격하게 지킵니다.

알서포트는 정보 보안 및 개인 정보를 관리하는 조직을 별도로 운영하고, 매년 정보보호정책/지침을 개정하여 연간 계획에 따라 수행하며 정보 보안에 대한 사내 규칙을 제정하고 이를 시행하고 있습니다.

정보 보안 및 개인 정보 관리에 관한 교육·훈련을 의무화하여, 정보 관련 조직의 책임자와 담당자에 대해 연 2회 전문 교육(사내 교육, 외부강사 초빙교육, 외부 교육 등)을 실시하고 있습니다. 또한 일반 직원에 대해서도 보안 의식을 고취하기 위한 정기 교육을 진행하고 있으며, 정보 관리 업무에 종사하는 직원은 정규직 고용 계약만 가능하도록 하여 내부에서의 공격 위험을 최소화하고 있습니다.

모든 정보 시스템 장비(서버, 클라이언트 PC 등)는 관리 대장 및 자산 데이터베이스로 관리하고 있으며 보유 기록 매체 관리 대장을 별도 관리합니다.

알서포트 직원이 정보 시스템에 로그인 할 때는 반드시 ID(계정)와 암호를 사용하여 액세스 인증을 실시하며, 비밀번호 설정 조건(문자, 숫자의 조합 및 자리 수 등), 변경 빈도 등의 관리 사항을 규칙으로 정하고

이를 준수하고 있습니다. 엑세스한 사용자 등급에 따라 권한과 자원(디스크 공간, 메모리량, 대역폭 등)의 사용을 허용 및 거부할 수 있도록 운영하고 있습니다.

보안 표준 기준 준수

알서포트는 개인정보보호 국내/외 보안 표준 기준을 준수하며 다음과 같은 활동을 수행하고 있습니다.

- 국가보안기술연구소(NSRI) 보안 가이드 준수

알서포트의 모든 원격 제품은 국가보안기술연구소(NSRI)의 소프트웨어 업데이트 체계 보안 가이드를 준수하여, 모든 모듈은 전자서명 기반으로 인증된 정보로만 업데이트 됩니다.

- 비밀번호 단방향 암호화 제공

개인정보보호법 관련 권고안에서 제시하는 SHA-2 기반의 SHA-256 해쉬 알고리즘[3]을 사용합니다.

- 안전한 코딩 가이드(Secure Coding Guide) 준수

정부에서 제공하는 개발 보안 가이드를 준수한 개발 및 검토를 실시하며, 관련된 사이버 보안 위협에 대한 대응 및 예방책을 수립하여 적용하고 있습니다.

- 10대 웹 보안 위협 대응 (OWASP)

매년 발표되는 10대 웹 취약점에 대응하여 관련 취약점들을 제거하고 각종 점검 툴을 통한 점검에 만전을 기하고 있습니다.

결론
- 원격 서비스 선택의 기준은 '보안 '

보안 기준 준수를 넘어 '보안 커스터마이징'까지

알서포트는 기술적/물리적/관리적 측면의 철저한 보안 관리를 통해 고객이 가장 편리하고 안전한 원격 서비스를 이용할 수 있도록 하고 있습니다.

또한 알서포트는 자체적인 보안 기준을 외부적으로도 엄격히 적용하여, 원격 서비스 제공을 위한 보안 환경을 고객사에 맞게 커스터마이징하기도 합니다.(이하,서버 제품) 원격 서비스를 이용하려는 고객사의 현재 암호화 방식이 알서포트의 보안 수준에 적합하지 않은 경우, 고객사의 기존 암호화 방식을 고도화하여 암호화 수준을 강화한 후에 서비스를 제공합니다. Admin 계정의 ID생성 규칙과 접속 가능 IP대역 설정, 비밀번호 규칙 변경은 물론, DMZ구간[4]의 Proxy를 경유하여 내부망 웹서버에 접근하는 방식으로 네트워크 보안을 강화할 수도 있습니다.

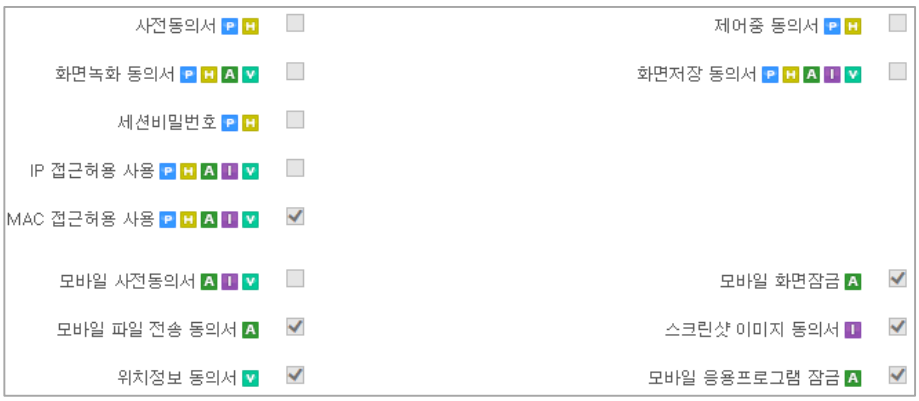
보안은 하루 이틀에 개선되지도, 완성되지도 않습니다. 지속적인 투자와 조직적 지원, 그리고 글로벌 수준의 물리적 환경이 동시에 갖춰질 때 비로소 빈틈없는 보안이 가능합니다. 알서포트는 이 모든 것을 고객의 안전한 서비스 이용을 위해 아낌없이 투자하고 있습니다. 이제는 보안 수준이 원격 서비스 선택의 기준입니다.

Appendix 1

알서포트 원격 서비스의 강력한 보안 설정: RemoteCall

- 개인정보 보호 관련 보안 설정

관리자에서 상담사의 옵션을 체크하여 개인정보보호 관련 보안 사항을 설정할 수 있습니다.



- 보안 등급 관리

관리자에서 이력 보관 주기, 비밀번호 수준, 로그인 실패 시 잠금 설정이 가능합니다.

- 비밀번호의 보안 등급을 3가지 수준(약, 중, 강)으로 조절할 수 있습니다.
- 비밀번호 사용기간을 30일, 60일, 90일로 지정할 수 있습니다.
- 로그인 실패 시 1분 ~ 60분까지 로그인 잠금 설정이 가능합니다

- 모바일 응용 프로그램 사용 잠금

관리자에서 모바일 원격 지원 중 실행 또는 실행 불가한 앱을 등록하여 허용 목록(White List) 또는 잠금 목록(Black List)을 설정할 수 있습니다. (그림. Black List 설정 화면)

알서포트 원격 서비스의 강력한 보안 설정: RemoteView

- 원격제어 시 원격지 화면 잠금 기능

원격제어 시 “원격 화면 잠금” 기능을 이용하여 원격지 화면을 끄고 켤 수 있습니다.

- OTP, SMS, E-mail을 이용한 이중 인증

일회성 접속만 가능한 One Time기반의 Key를 생성하여 원격제어하는 경우, OTP, SMS, E-mail을 이용하여 원격제어 사용자를 이중으로 인증합니다. 이러한 이중 인증은 로그인 ID, PW가 노출된 경우라도 허가되지 않은 사용자의 접근을 차단합니다.

Appendix 2

알서포트의 서버 보안 가이드

알서포트는 서버에 대한 최소한의 보안 수준을 달성하고자, 서버 운영에 필요한 점검 항목과 그에 대한 대처 방안을 정하고 이를 기준으로 서버를 정기적으로 자체 점검함으로써 서버의 안정성과 보안성을 강화하고 있습니다.

- 윈도우 서버 보안 가이드

No	구분	점검 항목
1	계정관리	패스워드 최소길이 설정
2		패스워드 사용기간 제한
3		패스워드 복잡성
4		취약한 패스워드 사용
5		서버 그룹 별로 다른 계정 및 패스워드 설정
6		무자격 사용자 ID 제거
7		Guest 계정 사용안함
8		로그인 성공 여부 로그 기록
9		계정 잠금정책 설정
10		administrator 계정명 변경
11		Administrator 계정 설명 삭제
12		신규계정을 administrator로 생성하여 감사
13		암호 변경 할 수 없음
14	파일시스템	파일 권한 설정
15		사용자 디렉토리 접근 제한
16		관리목적 공유 폴더 해제
17		파일 및 디렉토리 보호
18		SAM 파일 접근 통제
19		로그 파일 점검
20	Network 서비스	불필요한 서비스 중지
21		터미널 서비스 환경 설정
22		레지스트리 보호
23		SNMP 보안
24	시스템 보안	로그 오프나 워크스테이션 잠김
25		이벤트 뷰어 설정
26		로그온 메시지 출력 진단
27		마지막 로그온 사용자 계정 숨김
28		로그온 하지 않은 사용자 시스템 종료 방지
29		보안 로그의 감사 기능 설정
30		SAM 보안 감사 설정
31		익명 로그온(Null Session) 비활성화
32	해킹 점검	웹쉘 점검
33		백도어 점검
34		루트킷 점검
35	감사	Server 접근기록 별도 저장 관리
36		저장된 접근기록의 정기적 점검
37		접근기록에 대한 액세스 권한관리
38		접근기록의 일정 기간 보관

- 리눅스 서버 보안 가이드

No	구분	점검 항목
1	계정 관리	root 계정 원격 접속 제한
2		패스워드 복잡성 설정
3		계정 잠금 임계값 설정
4		패스워드 파일 보호
5	파일 및 디렉토리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정
6		파일 및 디렉터리 소유자 설정
7		/etc/passwd 파일 소유자 및 권한 설정
8		/etc/shadow 파일 소유자 및 권한 설정
9		/etc/hosts 파일 소유자 및 권한 설정
10		/etc/(x)inetd.conf 파일 소유자 및 권한 설정
11		/etc/syslog.conf 파일 소유자 및 권한 설정
12		/etc/services 파일 소유자 및 권한 설정
13		SUID, SGID, Sticky bit 설정 파일 점검
14		사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정
15		world writable 파일 점검
16		/dev에 존재하지 않는 device 파일 점검
17		$HOME/.rhosts, hosts.equiv 사용 금지
18		접속 IP 및 포트 제한
19	서비스 관리	Finger 서비스 비활성화
20		Anonymous FTP 비활성화
21		r 계열 서비스 비활성화
22		cron 파일 소유자 및 권한 설정
23		DoS 공격에 취약한 서비스 비활성화
24		NFS 서비스 비활성화
25		NFS 접근통제
26		automountd 제거
27		RPC 서비스 확인
28		NIS, NIS+ 점검
29		tftp, talk 서비스 비활성화
30		Sendmail 버전 점검
31		스팸 메일 릴레이 제한
32		일반사용자의 Sendmail 실행 방지
33		DNS 보안 버전 패치
34		DNS ZoneTransfer 설정
35		Apache 디렉토리 리스팅 제거
36		Apache 웹 프로세스 권한 제한
37		Apache 상위 디렉토리 접근 금지
38		Apache 불필요한 파일 제거
39		Apache 링크 사용금지
40		Apache 파일 업로드 및 다운로드 제한
41		Apache 웹 서비스 영역의 분리
42	패치 관리	최신 보안패치 및 벤더 권고사항 적용
43	로그 관리	로그의 정기적 검토 및 보고
44	DB 관리	디폴트 ID 및 패스워드 변경 및 잠금
45		패스워드 복잡도 설정
46		불필요한 계정 삭제 및 잠금
47		원격에서 DB 서버로의 접속 제한
48	감사	Server 접근기록 별도 저장 관리
49		저장된 접근기록의 정기적 점검
50		접근기록에 대한 액세스 권한관리
51		접근기록의 일정 기간 보관

- MySQL 보안 가이드

No	구분	점검 항목
1	기본 보안정책	user 테이블 접근통제
2		패스워드 없는 root 계정 접속 확인
3		MySQL 데이터 스트림의 암호화 상태 검사
4		MySQL 계정의 암호정책 준수
5		Database 백업 수행 및 접근권한 관리
6		test 데이터베이스 삭제
7	접근통제	최소한의 접근만 허용하도록 설정
8		로그인 계정 생성/관리의 관리주체
9		root 계정의 사용/관리주체
10		불필요한 MySQL Login 계정 제거
11		root 권한의 mysqld 구동 방지
12		테이블에 대한 심볼릭 링크 허용 방지
13		Local Infile 비활성화
14	암호화	암호화 대상 정보의 암호화 여부
15	감사	Server 접근기록 별도 저장 관리
16		저장된 접근기록의 정기적 점검
17		접근기록에 대한 액세스 권한관리
18		접근기록의 일정 기간 보관
19	보안 패치	최신 보안패치 및 벤더 권고사항 적용

- SQL Server 보안 가이드

No	구분	점검 항목
1	기본 보안정책	SQL Server 불필요한 서비스 차단
2		SQL Server 서비스 계정의 별도 관리
3		로컬 Windows 운영체제의 암호정책 준수
4		로컬 Windows 운영체제의 계정잠금 정책
5		SQL Server 자체 계정의 암호정책 준수
6		Database 백업 수행 및 접근 권한 관리
7	접근통제	불필요한 Windows, SQL Server 계정의 접근통제
8		로그인 계정 생성/관리의 관리주체
9		sa 계정의 사용/관리주체
10		불필요한 SQL Server Login 계정 제거
11		guest 계정의 사용/접근통제
12	암호화	암호화 대상 정보의 안전한 암호 알고리즘 사용여부
13		일방향 암호화 사용여부
14		암호화 키 및 인증서의 관리
15	감사	Server 접근기록 별도 저장 관리
16		저장된 접근기록의 정기적 점검
17		접근기록에 대한 액세스 권한관리
18		접근기록의 일정 기간 보관
19	보안 패치	최신 보안패치 및 벤더 권고사항 적용

Appendix 3

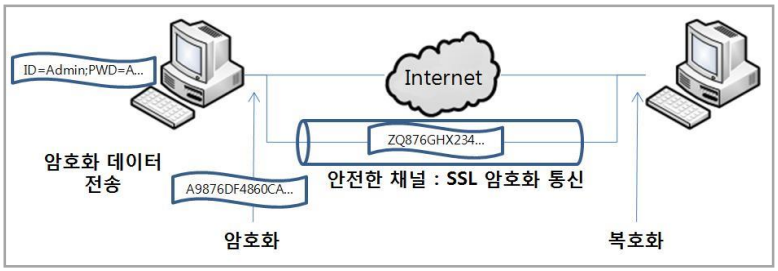
용어 설명

- AES (Advanced Encryption Standard)[1]

고급 암호화 표준(AES, Advanced Encryption Standard)은 2001년 미국 표준 기술 연구소(NIST)에 의해 제정된 암호화 방식으로서 암호화/복호화 과정에서 동일한 키를 사용하는 대칭 키 알고리즘입니다. 이전의 DES(Data Encryption Standard), 3DES보다 훨씬 안전한 암호화를 제공합니다.

- SSL (Secure Sockets Layer)[2]

SSL은 클라이언트와 서버 간의 정보를 암호화함으로써 도중에 해킹을 통해 정보가 유출되더라도 정보 내용을 보호할 수 있게 해 줍니다. SSL은 응용 프로그램과 TCP/IP 사이에서 동작하며, 데이터의 암호화, 서버의 인증, 메시지의 무결성을 제공해 줍니다 .



- SHA-2 기반의 SHA-256 해쉬 알고리즘[3]

SHA(Secure Hash Algorithm, 안전한 해쉬 알고리즘) 함수들은 서로 관련된 암호학적 해시 함수들의 모음입니다. 이들 함수는 미국 국가안보국(NSA)이 1993년에 처음으로 설계했으며 미국 국가 표준으로 지정되었습니다. 그 중 SHA-2 기반의 SHA-256은 32비트 워드를 사용하는 해쉬 함수이며, SHA-1 또는 SHA-0보다 암호학적 공격이 더 힘든 것으로 알려져 있습니다.

- DMZ구간[4]

Demilitarized Zone. 내부 자원을 보호하기 위해 내부망과 외부망 사이에서 접근 제한을 수행하는 영역을 말합니다.

RSUPPORT Co.,Ltd. | Connecting Lifestyle | www.rsupport.com

Korea

138-827 서울시 송파구 위례성대로 10
(방이동 44-5) 에스타워 11,12,15층
전 화 : +82-70-7011-3900
팩 스 : +82-2-479-4429
기술문의 : support.kr@rsupport.com
구매문의 : sales.kr@rsupport.com
기타문의 : info.kr@rsupport.com

Japan

〒105-0001 東京都港区虎ノ門1-2-20
第3虎の門電気ビル
TEL : +81-3-3539-5761
FAX : +81-3-3539-5762
お問い合わせ : support.jp@rsupport.com
Sales : sales.jp@rsupport.com
Info : info.jp@rsupport.com

USA

333 Sylvan Ave. STE#110,
Englewood Cliffs, NJ 07632, USA
TEL : +1-888-348-6330
FAX : +1-888-348-6340
Tech : support.us@rsupport.com
Sales : sales.us@rsupport.com
Info : info.us@rsupport.com

China

北京市朝阳区广顺南大街16号嘉美中心
写字楼1210
电话 : +86-10-8256-1810
传真 : +86-10-8256-2978
支持咨询 : support.cn@rsupport.cn
业务咨询 : sales.cn@rsupport.cn
销售咨询 : info.cn@rsupport.cn

Carbonless Support · Compatible with Windows 7 · Microsoft GOLD CERTIFIED Partner · intel · Connecting lifestyle RSUPPORT