21 CFR Part 11 에 대한 고찰

Version 1.0 – 2003/03

현재 문제점으로 대두되고 있는 전자기록 및 전자서명에 관한 법령인 21 CFR Part 11 에 대한 깊이 있는 이해를 돕기 위하여 만들었습니다.
또한 최근 발표된 21 CFR Part 11 개정 공고에 대한 내용을 포함하여 향후 전망을 다루고 있습니다.
본 문서의 내용에 이의가 있거나 질문이 있으신 분은 연락해 주시기 바랍니다.

IVS
유재훈
ryuhoon@intizen.com
www.validation.co.kr

목 차

1. 서론

최근에 컴퓨터를 이용한 작업이 더 많아짐에 따라 컴퓨터에 대한 의존도는 점점 높아만 가고 있다.

이런 환경에서 FDA 의 법령인 21 CFR Part 11(이하 Part 11)[1]은 전자기록과 전자서명의 특정주제에 대한 구체적인 법으로 광범위한 분야에 영향을 미치는 법령이다. 또한 자동화 시스템에 대한 특별한 법이 없는 현실에서 Part 11 을 참조하는 분야가 더욱 넓어졌다.

Part 11 은 많은 논의 과정을 거쳐서 만들어 졌다. 그러나 Part 11 은 대상 범위의 모호성으로 인하여 법을 집행하는 FDA 의 내부뿐만 아니라 법을 따라야 하는 의료보건 산업계에 많은 논쟁거리를 만들어 법의 집행을 더디게 만들었다. 또한 Part 11 의 효력발생일인 1997 년 8 월 20 일은 Y2K 버그가 발생하는 2000 년과 시기적으로 가까워 산업계는 Part 11 을 충족하는 신규 시스템 도입에 불안감을 가지고 있었다.

결국, Part 11 은 따라야 하지만, 규제기관에서 직접적으로 문제를 제기하지 않는 한 따르지 않는 법령이 되었다. 이런 이유로 산업계의 사람들은 Part 11 에 대하여 막연하게 제목만 알고, 제대로 이해하지 않고 있으며 심지어는 Part 11 에 관련된 컨설턴트나 강사들 사이에서도 Part 11 해석에 이견을 보이고 있었다. 특히 국내의 경우는 상황이 심각하다. (Part 11 과 GAMP 를 동일한 것으로 생각하는 경우도 종종 있다)

2003 년 2 월 FDA 는 중요한 지침[2]을 발표하였다. 이 지침은 초안이기는 하지만 Part 11 이 개정될 것이라고 밝히고 있다. 또한 Part 11 관련된 기존 지침을 모두 회수한다고 발표하였다. 발표된 지침에 따르면 Part 11 은 모호한 적용 범위를 축소하여 작지만 명확한 범위를 설정하는 방향으로 개정될 것이다. 이러한 개정은 FDA 가 Part 11 의 준수를 현재보다 좀더 강요하는 결과로 나타날 것이다.

본 문서는 이런 시점에서 다음 사항에 대하여 논의할 것이다.

- 기존 Part 11
- 기존 Part 11 의 문제점
- 향후 Part 11 의 전망
- Part 11 에 관련 고려 사항

또한 본 문서는 Part 11 의 개정이후 Version 2.0 으로 갱신될 것이다.
본 문서에서 사용되는 용어는 'GAMP 용어해석[3]'을 참조한다.

2. 기존 Part 11

Part 11 의 효력 발생일은 1997 년 8 월 20 일이다. FDA 는 Part 11 의 적용대상을 효력발생일 이후에 사용하는 모든 시스템으로 생각한다. 따라서 현재 사용하는 시스템이 효력발생일 이전부터 사용되었거나 이후부터 사용되었거나 상관없이 현재 사용하고 있고, FDA 의 기존법령에 따라 규제 대상이라면(cGMP 에 관련된다면) Part 11 에 따라야 한다.

Part 11 내용을 서술적으로 설명하기에는 어려움이 있기 때문에 다음과 같은 표를 만들었다. 표에는 Part 11 각 조항원문과 해당하는 요약된 해석이 있다. 각 조항의 원문과 요약된 해석을 비교하여 읽어보기 바란다.

본 장에서는 내용에 대한 자세한 설명은 하지 않고 단지 조항별 내용만을 설명하였다. 특정 주제에 관련된 Part 11 의 적용이나 Part 11 전반적인 이해에 관련된 내용은 본 문서의 5 장 'Part 11 에 관련 고려 사항'에 있다.

Part 11 조항

Section	Sub.	Content
11.1 Scope		
11.1 Scope	(a)	The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper. Part 11 은 전자기록, 전자서명, 전자기록에 행하여 지는 수기서명이 신뢰성 있고, 기존 종이기록, 수기서명과 동일하기 위한 기준이다.
11.1 Scope	(b)	This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means. Part 11 은 당국의 규정 내에서 만들어지고, 수정되고, 유지되고, 보관되고, 조회되고, 보내어지는 전자적인 형식의 기록에 적용한다. Federal Food, Drug, and Cosmetic Act / Public Health Service Act 에 제출하는 전자기록에도 적용한다. 전자수단을 통하여 보내는 종이기록에는 적용하지 않는다. # 종이로 저장되고 유지되는 컴퓨터 시스템은 포함하지 않는다 – 워드프로세서 # 팩스는 적용되지 않는다.
11.1 Scope	(c)	Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997. Part 11 의 요구사항을 만족할 때, 수기서명과 동일하다고 판단할 것이다. (특히 1997 년 8 월 20 일에 이후부터 적용)
11.1 Scope	(d)	Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required.

		종이 기록이 특별히 필요하지 않는 한, Sec. 11.2 에 따라, Part 11 의 요구사항에 일치하는 전자기록이 종이기록을 대신하여 사용될 것이다.
11.1 Scope	(e)	Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection. Part 11 에 따라 유지되는 컴퓨터 시스템, 제어기, 관련문서는 FDA 실사에 이용할 수 있도록 준비되어야 한다.
11.2 Implementation		
11.2 Implementation	(a)	For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met. 당국에 제출하지 않지만 유지해야 하는 전자기록과 전자서명은 Part 11 의 요구사항을 만족해야 한다.
11.2 Implementation	(b)	For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that: 당국에 제출하는 전자기록과 전자서명은 다음과 같다.
11.2 Implementation	(b) (1)	The requirements of this part are met; and Part 11 의 요구사항을 만족해야 한다.
11.2 Implementation	(b) (2)	The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission. 당국이 인정하는 전자형식의 제출물 형태가 docket(소송 사건 일람표) No. 92S-0251 에 분류되어 있다. Docket 에는 허용되는 전자형태와 제출물의 접수처를 규정한다. Docket 에는 규정되지 않은 접수처로 수신된 전자적 형태의 문서는 인정되지 않는다 # 당국에 제출하는 문서도 전자기록과 전자서명이 가능하다.
11.3 Definitions		
11.3 Definitions	(a)	The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part. 법령 Section 201 에서 정의한 동일한 용어를 사용한다.
11.3 Definitions	(b)	The following definitions of terms also apply to this part: 또한 다음 용어를 적용한다
11.3 Definitions	(1)	Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)). 법령(Act)은 Federal Food, Drug, and Cosmetic 법령을 의미한다.
11.3 Definitions	(2)	Agency means the Food and Drug Administration.

		당국(Agency)은 FDA 를 의미한다
11.3 Definitions	(3)	Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable. 생체인식(Biometrics)은 개인의 신체적 특징이나 독특하고 측정 가능한 특징이나 행동에 근거한 표준적인 행위에 기초하여 개인의 신원을 입증하는 방법을 의미한다.
11.3 Definitions	(4)	Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system. 폐쇄계(Closed system)는 시스템의 접근이 시스템의 전자기록 내용에 대하여 책임이 있는 사람에 의하여 통제되는 환경을 의미한다. # 단지 물리적 통제만을 의미하는 것은 아니다. 따라서 공공라인(인터넷, 전화)을 통한 시스템도 관리자가 존재한다면 경우에 따라 폐쇄계로 볼 수 있다. 그러나, 이럴 경우 부가적인 인증이 필요하다.
11.3 Definitions	(5)	Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. 디지털서명(Digital signature)은 서명자 확인과 자료의 완전무결을 확인할 수 있는 일련의 규칙과 일련의 매개변수로 처리되어지며, originator 확인을 암호적 방법에 근거한 전자서명을 의미한다. # '전자서명'의 일부인 '디지털서명'을 '전자서명'과 동의어로 생각해서는 안된다.
11.3 Definitions	(6)	Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. 전자기록(Electronic record)은 컴퓨터 시스템에 의해 생성되고, 수정되고, 유지되고, 문서화되고, 조회되고, 배포되는 디지털 형식의 문자, 그림, 자료, 소리, 사진 또는 다른 정보의 모든 조합을 의미한다.
11.3 Definitions	(7)	Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. 전자서명(Electronic signature)은 개인의 수기 서명과 동일한 법적 구속력을 가지며, 개인에 의하여 실행, 채택 또는 인증되는 일련의 기호를 컴퓨터 데이터화 한 것을 의미한다.
11.3 Definitions	(8)	Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark. 수기서명(Handwritten signature)은 불변의 형태로서 본인임을 확인하기 위해 현재 시행되거나 채택된 것으로 개인에 의해 수기로 작성된 서명 이름이나 법적 표시를 의미한다. # 만약 수기서명을 그림파일 등으로 관리할 경우 이것은 전자서명이 아니다. 그러나, 이럴 경우 이것은 전자기록으로 취급되어 전자기록과 동일한 통제를 해야 한다.
11.3 Definitions	(9)	Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic

		records that are on the system. 열린계(Open system)는 시스템의 접근이 시스템의 전자기록 내용에 대하여 책임이 있는 사람에 의하여 통제되지 않는 환경을 의미한다.
11.10 Controls for closed systems		Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: 폐쇄계에서는 신뢰성, 무결성, 비밀성을 확실히 하고, 서명자가 자신이 행한 전자기록을 부인할 수 없도록 설계된 절차와 통제에 따라 사용해야 한다. # 모든 생성되는 전자기록이 통제에 따라야 한다. # 단지 최종결과나 자료의 적합성만 통제대상이 아니다. # 컴퓨터 시스템의 내부감사가 필요하다.
11.10 Controls for closed systems	(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. 정확성, 신뢰성, 일관성 있는 수행, 무효한 것이나 수정된 기록을 인식하는 능력을 확실히 하기 위한 시스템 검증. # 모든 검증자료를 준비해야 한다. # 무효한 자료나 변경자료도 언제, 누가 어디서 처리했는지 알 수 있어야 한다
11.10 Controls for closed systems	(b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records. 당국에 의한 실사, 검토, 복사를 위해 인간이 판독 가능하고 적합한 전자형식으로 기록을 정확하고 완벽하게 생성시킬 수 있는 능력. # 폐기되거나 업그레이드된 시스템에서 반드시 구 시스템 장치를 유지할 필요는 없다. 그러나, 새로운 시스템에 완벽하게 자료를 이관하고, 이를 검증해야 한다
11.10 Controls for closed systems	(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period. 기록 보존기간 동안 정확하고 재빠른 조회를 가능하게 하는 기록의 보호
11.10 Controls for closed systems	(d)	Limiting system access to authorized individuals. 검증된 개인에게만 제한된 시스템 접근
11.10 Controls for closed systems	(e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. 전자기록을 생성, 수정, 삭제하는 조작자 행위를 날짜와 시간이 독립적으로 기록되고(time-stamp 된), 컴퓨터로 자동 생성되는 audit trail. 기록변경은 이전에 기록정보를 손상시키면 안 된다. audit trail 문서는 최소한 해당 전자기록의 보존기간 동안 보존되어야 하며 당국의 감토와 복사가 가능해야 한다. # audit trail 은 사용자의 작업과 상관없이 작동해야 한다.
11.10 Controls for	(f)	Use of operational system checks to enforce permitted sequencing of

closed systems		steps and events, as appropriate. 적절히 허가된 순차적인 순서와 업무로 실시되는 운영시스템 검사
11.10 Controls for closed systems	(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand. 오직 검증된 개인의 시스템 사용, 전자적 서명, 작업이나 컴퓨터 시스템의 입출력 장치의 접근, 기록의 수정, 직접 작업수행을 확인하는 인증검사. # 절차, 시스템의 논리적 접근통제, 정의된 전자서명뿐만 아니라 물리적인 접근통제도 관련된다.
11.10 Controls for closed systems	(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. 적절히 자료입력이나 운영지시의 출처 유효성을 확인하는 장비검사
11.10 Controls for closed systems	(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. 전자기록/전자서명 시스템을 개발하거나, 유지하거나, 사용하는 사람들이 그들에게 할당된 일을 수행할 수 있는 교육, 훈련, 경험이 있어야 한다.
11.10 Controls for closed systems	(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification. 기록과 서명의 변조를 막기 위하여 자신의 전자서명으로 이루어진 행위에 대하여 각 개인이 책임이 있음을 문서화한 정책의 확립과 준수 # 타인이 전자서명을 할 경우도 해당 전자서명도 본인이 서명한 것과 동일한 책임이 있다.
11.10 Controls for closed systems	(k)	Use of appropriate controls over systems documentation including: 다음을 포함하는 시스템 문서에 대한 적절한 통제:
11.10 Controls for closed systems	(k) (1)	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. 시스템 운영과 유지를 위하여 배포, 접근, 사용하는 문서의 적절한 통제.
11.10 Controls for closed systems	(k) (2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. 시스템 문서의 개발과 수정이 시간순서로 문서화되는 audit trail 이 유지되는 개정과 변경통제 절차. # 문서는 자동적으로 audit trail이 되어야 한다. # 문서관리 시스템을 사용하는 것이 바람직 하다.
11.30 Controls for open systems		Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality. 전자기록을 생성하고, 수정하고, 유지하고, 전송하기 위하여 오픈 시

		스템을 사용하는 사람은 생성과 접수 시점까지 전자기록의 신뢰성, 무결성, 비밀성을 확실히 하기 위해 고안된 절차와 관리를 따라야 한다. 그러한 절차와 통제는 Section 11.10(Closed system 의 통제)에 있고, 기록의 신뢰성, 무결성, 비밀성을 확실히 하는 문서의 암호화와 적절한 디지털 서명과 같은 추가적인 수단(open system 환경에서 필요한)이 있다.
11.50 Signature manifestations		
11.50 Signature manifestations	(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: 서명된 전자기록은 다음의 정보를 포함해야 된다:
11.50 Signature manifestations	(a) (1)	The printed name of the signer; 서명자의 인쇄된 이름 # 서명자의 이름은 유일하지 않다. # ID 는 이름의 대용품이 아니다.
11.50 Signature manifestations	(a) (2)	The date and time when the signature was executed; and 서명이 실시된 날자와 시간
11.50 Signature manifestations	(a) (3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature. 서명과 관련되는 의미(비평, 승인, 책임 또는 저작 같은)
11.50 Signature manifestations	(b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout). (b) (a)(1), (a)(2), (a)(3)에 분류된 항목은 전자기록과 동일한 제어가 필요하고 인간이 읽을 수 있는 형태(전자표시기 또는 인쇄물과 같은)의 일부로 포함되어야 한다. # 전자서명은 전자기록의 특수한 형태이다.
11.70 Signature/record linking		Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means. 전자기록에 실행되는 전자서명과 수기서명은 각각의 전자기록과 연결되어야 한다.
11.100 General requirements		
11.100 General requirements	(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. 각 전자서명은 각각 개인별로 유일해야 하며 다른 누군가가 재사용하거나 재서명할 수 없다. # 대리 서명을 할 경우, 대리자의 서명을 해야 한다.
11.100 General requirements	(b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual. 개개인의 전자서명 또는 전자서명의 모든 요소를 확립, 할당, 증명, 인증하기 전에 조직은 개개인의 신원을 확인해야 한다.
11.100 General requirements	(c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

		전자서명을 사용할 사람은, 사용전이나 사용할 때, 그 전자서명 시스템이 전통적인 수기서명과 법적 구속력이 동일하다는 것을 당국에 증명해야 한다. (1997 년 8 월 20 일 이후)
11.100 General requirements	(c) (1)	The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. 증명서는 종이형태로 전통적인 수기서명이 되어 the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857 로 제출되어야 한다.
11.100 General requirements	(c) (2)	Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature. 전자서명을 사용할 사람은, 당국의 요청에, 서명자의 수기서명과 법적 구속력이 동일하다는 전자서명 상세의 추가적인 증명서나 증명을 제출해야 한다.
11.200 Electronic signature components and controls		
11.200 Electronic signature components and controls	(a)	Electronic signatures that are not based upon biometrics shall: 생체인식에 의거하지 않는 전자 서명은 다음과 같다:
11.200 Electronic signature components and controls	(a) (1)	Employ at least two distinct identification components such as an identification code and password. ID 와 암호 같은 적어도 2 개 이상 별도의 식별 구성요소를 사용한다. # 전자서명은 검토절차가 있어야 하며, 편리하면 안 된다. # 관리자도 암호를 알 수 없어야 한다.
11.200 Electronic signature components and controls	(a) (1) (i)	When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. 한번 또는 연속적인 기간동안 여러 번 서명을 실시할 때, 첫번째 서명은 모든 전자서명의 구성요소를 사용하여 실시되어야 한다: 이후의 서명은 하나 이상의 전자서명 구성요소를 이용하여 실시되어야 한다.
11.200 Electronic signature components and controls	(a) (1) (ii)	When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. 연속적이지 않은 기간동안 여러 번 서명을 실시했다면, 각 서명은 모든 전자서명 구성요소를 이용하여 실시되어야 한다.
11.200 Electronic signature components and controls	(a) (2)	Be used only by their genuine owners; and 서명 구성요소의 진짜의 주인에 의해서만 사용되어야 한다.
11.200 Electronic signature components and controls	(a) (3)	Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. 진짜 주인이외의 누군가에 의해 개인의 전자서명 사용 시도에 두개 이상의 구성요소가 필요하다는 것을 확실히 하기 위하여 관리하고 실행한다.
11.200 Electronic signature components and controls	(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. 생체인식에 의거하는 전자서명은 그들이 진짜의 주인이외의 누군가

		에 의해 사용할 수 없다는 것을 확실히 하기 위하여 설계되어야 한다.
11.300 Controls for identification codes/passwords		Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: ID 와 암호의 조합에 의거한 전자서명을 사용하는 사람은 그들의 보안과 무결성을 확실히 하기 위하여 통제되어야 한다.
11.300 Controls for identification codes/passwords	(a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. 각 ID 와 암호의 조합의 유일성 보존.
11.300 Controls for identification codes/passwords	(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). ID 와 암호 배포가 정기적으로 점검, 회수, 개정 (예를 들면, 암호기간 만료)
11.300 Controls for identification codes/passwords	(c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. 전자적 미인증 분실, 도난, 행방불명, 잠재적 위험 토큰, 카드와 식별코드와 암호정보를 생성하는 장치의 적절하고 엄격한 통제(분실관리 절차)
11.300 Controls for identification codes/passwords	(d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. ID 와 암호의 미승인 사용을 막고 미승인된 사용시도를 즉각적이고 긴급히 찾아내어 보고하는 취급보호 활동(조직적으로 관리) # password 오류 입력 3 회 이상일 때 id 사용금지 # login 후 5 분 이상 미 작업시 종료
11.300 Controls for identification codes/passwords	(e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner. 올바르게 작동하고 미 승인된 방법으로 변경되어 질 수 없는 ID 와 암호정보를 생성하는 토큰이나 카드와 같은 장치의 초기화와 주기적인 검사.

3. 기존 Part 11 의 문제점

기존 Part 11 은 전자기록과 전자서명에 대한 정의, 구성요소, 필요충족조건만을 단지 설명한다. 따라서, 어떤 곳에 적용해야 하고, 구축에 필요한 구성요소 무엇이고, 적합성 판단 기준은 무엇인가 등은 모두 FDA 의 법을 따라야 하는 산업계의 일이었다. 그러나 이런 일은 해당 실무자와 전문가에 의한 확실한 업무/절차정의, 구현방법 확립을 통하여 대부분 해결할 수 있는 문제였다.

Part 11 의 가장 큰 문제는 용어정의에 있다. 문제가 되는 전자기록의 정의에 대하여 살펴보자. 조항을 보면;

Section 11.3 Definitions

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

-- 해석하면

(6) 전자기록(Electronic record)은 컴퓨터 시스템에 의해 생성되고, 수정되고, 유지되고, 문서화되고, 조회되고, 배포되는 디지털 형식의 문자, 그림, 자료, 소리, 사진 또는 다른 정보의 모든 조합을 의미한다.

이 조항을 이해하려면 우선 컴퓨터 시스템(computer system)과 디지털 형식(digital form)에 대하여 생각해야 한다.

컴퓨터 시스템의 정의를 용어집[3,4]에서 찾아보면;

컴퓨터(Computer)는 1) 작동중에 인간의 관여없이, 수치계산과 논리작동을 포함하는 실제적인 계산을 수행하는 Functional Unit & Functional Programmable Unit, 2) 하나이상의 Processing Unit 과 주변장치로 구성된 Functional Programmable Unit, 3)내부적으로 저장된 프로그램으로 통제되는 Functional Programmable Unit 이다. 컴퓨터 시스템(Computer System)은 하나이상의 컴퓨터와 입/출력 장치로 구성된 Functional Unit 으로 프로그램과 프로그램 실행에 필요한 자료를 위한 일반적인 저장장치를 이용하며, 수치계산과 논리작동을 포함하여 사용자가 목적하는 자료조작을 수행하는 시스템이다.

용어정의에서 알 수 있듯이 컴퓨터(Computer)는 단순히 PC, 즉 일반적으로 사용되는 개인용 컴퓨터, 노트북, 서버 뿐만 아니라 전자적 회로를 내장한 거의 모든 장치를 포함한다.

디지털(digital)이란 데이터를 0 과, 1 의 두 가지 상태로만 생성하고, 저장하고, 처리하는 전자기술을 말한다. 따라서 디지털 형식(digital form)은 컴퓨터 시스템에서 사용되는 모든 자료를 말한다.(단지 MS-엑셀 파일, MS-Word 파일, HWP 파일만을 지칭하지 않는다)

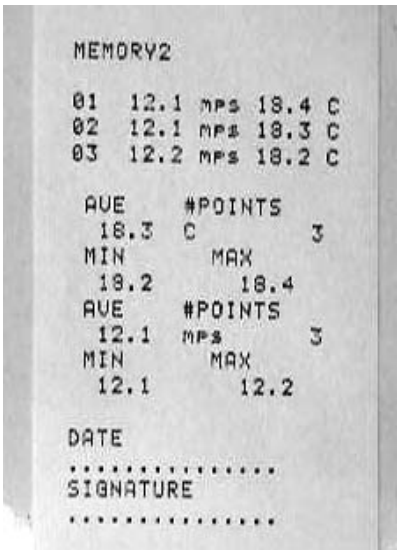
따라서 Section 11.3 (6) 조항에 정의된 전자기록은 모든 자동화 장치에서 사용되는 일시적/영구적 자료를 뜻한다. 그럼 모든 자동화 장치에서 전자기록을 사용하고 있으므로 Part 11 의 적용범위는 모든 자동화 장치를 포함하는가?

다음과 같은 경우를 생각해 보자.

다음 사진은 휴대용 풍속 측정계이다. 이 풍속계는 여러 번에 걸쳐 온도와 함께 풍속을 측정하여 자신의 메모리에 기록시킨다. 이후 측정이 종료되면 풍속계와 함께 제공되는 특수한 휴대용 프린터로 결과를 한번에 종이로 출력한다.

이런 형태의 휴대용 계측기는 많이 사용된다. 또한 결과는 검증자료로 사용되고 있다.

풍속계 **측정결과 출력지**



위의 풍속계는 전자기록을 사용하고 있을까?
Section 11.3 (6) 조항에 따라 생각하면 당연히 사용하고 있다. 풍속계는 전자기록을 생성했고, 자신의 메모리에 저장했고, 결과를 출력하기 위하여 특정기록을 조회했고, 프린터로 전송했고, 평균값과 최대/최소값을 위하여 기록을 조작했다.

이럴 경우 풍속계는 Part 11 의 적용대상인가?

만약 적용대상이라면, 해당 전자기록을 항상 보관하고 조회가능하고, audit trail 이 가능하고, 접근통제가 가능하게 할 수 있는가? 휴대용 측정 장치의 자료를 어떤 방법으로 관리할 것인가? 현실적으로 불가능 하다. 또한 위의 풍속계를 Part 11 의 대상으로 한다면 다른 비슷한 수준의 장치도 Part 11 의 대상이 된다. 즉 거의 모든 자동화 시스템/장치가 Part 11 의 대상이 된다. 대부분의 계측장치, 제어시스템, IT 시스템은 단지 의료보건분야에서만 사용하는 것이 아니다. 다른 분야에서 잘 사용하고 있는 장치나 시스템은 Part 11 의 영향으로 의료보건분야에서는 사용할 수 없다면, 의료보건 분야에는 모든 장치와 시스템을 Part 11 에 충족하도록 별도로 제작해야 한다. 이런 제한규정은 다른 분야에서 사용하는 자동화 시스템을 사용할 수 없도록 만들어, 결국 의료보건 분야를 기술적으로 낙후 시킨다.

다른의견으로는 결론적으로 사용하는 것은 출력된 종이기록지 이므로 Part 11 에 적용되지 않는다고 생각할 수 있다. 그럼 Part 11 의 대상이 되는 전자기록이란 무엇인가? 누가 어디에서 전자기록의 범위를 정의하고 있는가? 이러한 법령 해석은 다른조항을 만족시키기 위하여 일부조항을 왜곡해석한 경우다. 다른조항을 위하여 일부조항을 왜곡/무시한다면 해당 법령이 법으로써 의미가 있으며 준수할 필요가 있는가?

Part 11 은 적용대상을 조항의 정의대로 해석하면, Part 11 적용 대상이 너무 광범위 하여 통제 불가능하고, Part 11 의 대상을 축소/왜곡 해석하면 대상이 명확하지 않아 Part 11 을 유명무실한 법령으로 만든다.

Part 11 의 적용대상에 대하여 이전부터 많은 논의가 있었다. 그러나 누구도 확실한 대답을 하지 못했고, 관련 전문가뿐만 아니라 FDA 내부에서도 혼돈이 있었다.

4. 향후 Part 11 의 전망

기존 Part 11 은 앞 장에서 설명한 것과 같은 문제점을 가지고 있었다. 이 문제는 산업계뿐만 아니라 FDA 에게도 어려운 문제였다. Part 11 으로 인하여 산업계는 실질적인 이득이 없이 막대한 비용을 지불해야 하며, 의료보건 분야는 기술적으로 낙후 되었다. 따라서 미국 공공 보건을 위해 설립된 FDA 는 문제를 해결하기 위하여 Part 11 를 재검토 해야 한다고 생각했다.

2003 년 2 월에 FDA 는 매우 중요한 지침을 발표했다.(이 지침은 초안(draft)이다. 하지만 FDA 의 관행으로 생각할 때 초안일 지라도 충분한 의미를 가진다.)

> *FDA, Guidance for Industry(Draft), 21 CFR Part 11, Electronic Records; Electronic Signatures – Scope and Application, 2003. 2* [2]

이 지침은 다음과 같은 내용을 포함하고 있다.

- **Part 11 은 개정될 것이다.**
  기존 Part 11 의 문제를 해결하기 위하여 개정할 것이며, 현재 재검토하고 있다.

- **기존 관련 지침을 회수한다.**
  기존에 Part 11 관련해 있었던 5 개의 지침을 회수한다.
  - *Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures Validation* [5]
  - *Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures, Glossary of Terms* [6]
  - *Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures, Time Stamps* [7]
  - *Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures, Maintenance of Electronic Records* [8]
  - *Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures, Electronic Copies of Electronic Records* [9]

- **신규 개정 Part 11 이 발표되기까지 본 지침을 준수해야 한다.**
  본 지침은 Part 11 의 개정을 발표하기도 하지만 개정될 Part 11 의 방향에 대하여 설명되어 있다. 그러므로 산업계는 신규 법령이 나오기 전까지 본 지침에 준하여 업무를 진행해야 한다. 또한 레가시 시스템에 대해서는 지금 당장 준수여부를 실사하지는 않을 것이다. 하지만 개정이후에는 준수여부를 강요할 것이다.

- **향후 개정 방향 – Part 11 의 적용대상은 축소될 것이다.**
  현재와 같이 문제를 야기하는 Part 11 의 대상범위를 작게 축소할 것이다. 하지만 명확하게 규정될 것이다.

- **향후 개정 방향 – 검증, audit trails, 기록보존, 기록복사에 대하여 강화할 것이다.**
  검증, audit trails, 기록보존, 기록복사에 대한 내용이 자세히 추가될 것이다.

- **향후 개정 방향 – 기본 법령과의 연계를 강화할 것이다.**
  Part 11 관련 모든 전자기록은 기존법령에 따라야 하며 기존법령과 Part 11 이 상호 보완적으로 작용하도록 강요할 것이다.

문제가 되었던 전자기록의 포괄적인 기존 조항은 수정될 것이다. 최종적으로 전자 형식으로 유지되는 전자기록에만 적용될 것이다. 특히 종이기록을 만들기 위한 일시적인 컴퓨터의 사용은 대상에서 제외될 것이다. 따라서 대부분의 계측기와 제어기는 Part 11 의 대상이 아니다. 대부분의 IT 시스템은 대상이 된다. 만약, ERP, LIMS, 문서관리시스템, 물류시스템 등을 사용하고 있다면 Part 11 을 고려해야 한다.

전자서명과 관련해서는 특별한 내용이 없다. 전자서명과 관련해서는 기존 Part 11 조항이 상당히 잘 되어 있어 특별히 문제될 것이 없다. 하지만 전자서명은 전자기록의 일부분이므로 전자기록의 개정에 따라 변경되는 것을 준수하면 된다.

회수한다고 발표한 5 개의 Part 11 관련 지침은 상당히 좋은 내용을 가지고 있었다.(회수된 문서이지만 읽어보기를 권장한다) 하지만 Part 11 개정될 것이므로 회수하는 것이다. 개정이후 각 분야에 대한 신규 지침이 발간 될 것으로 예상된다.

강화하겠다고 발표한 검증, audit trails, 기록보존, 기록복사에 관한 내용은 기존 조항(Section 11.10)에 이미 있는 내용이었다. 그러나 기존 조항들이 너무 단순하고 단편적으로 되어 있었으므로 좀더 자세하게 변경될 것이다.

기존법령과의 연계강화는 당연한 사항이며 기존 Part 11 에도 있는 내용이다. 기존 Part 11 Section 11.1(a)는 'Part 11 법령은 전자기록, 전자서명, 전자기록에 행하여 지는 수기서명이 신뢰성 있고, 기존 종이기록, 수기서명과 동일하다고 인정하는 기준이다.'라고 Part 11 의 목적을 밝히고 있다. 즉, Part 11 의 대상이 되는 전자기록과 전자서명의 유지/보관해야 하는 법적 근거는 대부분 다른 법령에 있다. 따라서 FDA 실사는 단지 Part 11 에 국한되는 것이 아니라 다른 법령과 연계하여 고려될 것이다.

FDA 는 1997 년 8 월 20 일 이전부터 사용한 시스템을 '레가시 시스템'이라고 지칭한다. 레가시 시스템에 대한 FDA 의 생각은 확고하다. 그것이 레가시 시스템이거나 하이브리드 시스템(완벽하게 Part 11 의 규정을 만족하지 않지만 부분적으로 만족하는 시스템)이거나 상관없이 현재 사용중이라면 당연히 실사의 대상이다.

Part 11 개정의 가장 중요한 내용은 Part 11 의 적용대상 축소이다. Part 11 법령의 가장 근본적인 내용을 수정하는 것이다. Part 11 의 개정은 전자기록에 적용범위를 축소시키지만 대상을 명확하게 할 것이다. 이런 개정은 3 장에서 설명한 문제점을 해결하여, 집행은 되지 않고 논의만 많았던 Part 11 을 실효성 있는 법령으로 만들 것이다. FDA 는 명확한 신규 Part 11 에 따라 규제조치를 강화할 것이고 결국 **산업계는 Part 11 준수를 강요 받게 될 것이다.**

FDA 가 Part 11 을 강화하고 미국내에서 준수하는 회사가 많아 진다면, Part 11 은 전세계적으로 통용되는 법이 될 가능성이 있다. 왜냐하면 유럽/일본은 Part 11 과 같이 전자기록/전자서명에 관련된 법이 없으며 자동화 시스템에 대하여 강력한 영향을 미치는 GAMP 에도 전자기록/전자서명에 대한 내용을 없기 때문이다. 현재 유럽에서는 Part 11 에 대하여 많은 관심을 가지고 있다. 조만간 유럽은 Part 11 에 준하는 법을 만들거나 Part 11 을 차용해서 사용할 가능이 매우 높다.

5. Part 11 에 관련 고려 사항

5.1 추진과정

대부분의 사람들이 Part 11 이 장치나 소프트웨어에 관련된 법이라 생각하고 있으나 이것은 큰 오해다. Part 11 의 조항을 살펴보면 총 41 개 조항이 있으며 중복을 포함하여 업무관련 조항이 23 조항, 기술관련 조항이 19 조항이다. 절반 이상이 업무관련 조항이다. 이런 비율은 Part 11 이 개정된다고 해도 비슷할 것이다.

현재 일부 제품은 Part 11 을 준수한다고 광고하고 있다. 하지만 이것은 단지 기술적인 조항을 준수했다는 뜻이다. 이런 제품을 구입한다고 해도 Part 11 을 준수했다고 할 수 없다. 업무관련 조항을 준수하기 위해서는 우선적으로 회사의 내부규정을 수정해야 한다. 이 작업을 위하여 회사는 특별팀을 구성하여 내부규정을 수정하고 Part 11 의 대상을 확인하는 작업을 선행해야 한다.

내부규정을 수정하는 작업은 까다롭기는 하지만 불가능한 작업을 아니다. Part 11 의 업무관련 조항은 대부분 일반적인 정보관리 지침이다. 사원의 신원확인, 업무에 맞는 권한, 부적절한 행위에 대한 징계 등 일반적인 정보관리 지침은 대부분의 회사에서 일부 수용하고 있는 것들이다. 이런 규정을 좀더 체계적이고 치밀하게 규정하여 Part 11 업무관련 조항을 충족시키면 된다.

5.2 Validation

Part 11 에서 검증은 기술적인 조항에 관련된 사항이며, 대부분 소프트웨어 검증이다. 소프트웨어 검증은 본 문서에서 설명하기에는 너무 방대하다. 다음 문서를 참고하기 바란다.

FDA, Guidance for industry, 21 CFR Part 11; Electronic Records; Electronic Signatures Validation, 2001. 8 [5]

FDA, General Principles of Software Validation; Final Guidance for Industry and FDA Staff, 2002. 1. 11 [10]

GAMP Forum, GAMP4, The Good Automated Manufacturing Practice(GAMP) Guide for Validation of Automated System, ISPE, 2001.12 [11]

본 문서에서는 직접적으로 소프트웨어 검증에 대하여 다루지 않는다. 하지만 강조하고 싶은 사항은 검증 계획(Validation Plan)과 URS 의 작성이다. 비록 이미 만들어진 소프트웨어를 구입할 경우라도 검증 계획과 URS 는 반드시 사용자가 만들어야 한다.

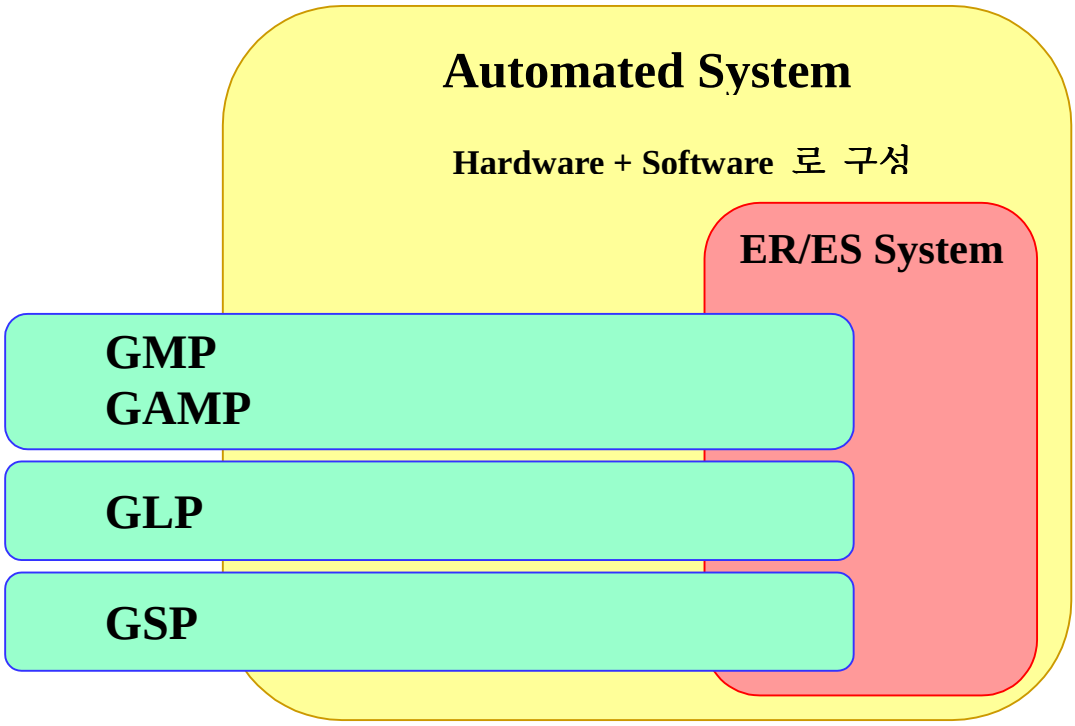
5.3 국내기업의 Part 11 준수여부

국내기업은 미국의 법령인 Part 11 을 준수해야 하는가? 이 질문에 대한 답은 회사마다 다르다.

경우	준수여부
국내에 제품 판매	준수할 필요 없다.
미국에 제품 수출	준수해야 한다. 주요사안의 경우 사전 통보해야 한다
미국에 제품 수출계획	준수해야 한다. 실사에 대비해야 한다.
유럽에 제품 수출	준수할 필요 없다. 향후 Part 11 에 준하는 법을 만들거나 Part 11 을 차용해서 사용할 가능이 매우 높다.

5.4 GAMP 와 관계

다른 분야와 Part 11 의 관계는 그림과 같다. 간혹 Part 11 를 GAMP 와 동일한 것으로 생각하는 사람이 있는데 이것은 매우 잘못된 생각이다. GAMP 란 Good Automated Manufacturing Practice 의 약자로 GMP 와 같이 재조에 사용되는 자동화 시스템에 관련된 규정이다. 당연히 검증을 해야 한다.(현재 여러 분야에서 다양한 각도로 접근하고 있다. ISPE 산하 기관 중 'GAMP Forum'이 가장 권위 있는 기관이며 'GAMP 4[11]'를 발간하였다.) Part 11 은 단지 전자기록과 전자서명에 관한 법이다. 물론 Part 11 에 적용을 받는 시스템이 GAMP 에 해당하는 시스템이지만 Part 11 대상이 아니라고 해서 GAMP 대상이 아닌 것은 아니다. Part 11 의 개정으로 내장형 PLC 로 작동되는 장치(멸균기, 건조기 등)는 Part 11 의 대상이 아닐 가능이 높다. 이런 장치들은 Part 11 의 대상이 아닐지라도 하드웨어 검증은 물론 **소프트웨어 검증을 해야 한다.**



5.5 전자문서관리 시스템

전자문서관리 시스템은 Part 11 을 준수하는데 매우 중요한 시스템이며 전자문서관리 시스템 자체가 Part 11 의 대상이다. Part 11 Section 11.10 (k)에는 전자기록/전자서명 시스템의 사용, 유지, 개발에 관련된 모든 문서를 관리해야 한다고 나와 있다. 이런 문서관리는 기존의 종이 시스템으로도 관리가 가능하지만 전자문서관리 시스템을 사용할 경우 더 많은 이점이 있다.

현재 기업환경의 변화로 많은 분야의 기업들이 전자문서관리 시스템을 도입하였고 도입하려 하고 있다. 이미 많은 수의 전자문서관리 시스템이 시장에 출시되어 있다. 그러나 Part 11 의 영향을 받지않는 분야를 위하여 만들어진 전자문서관리 시스템은 Part 11 을 충분히 만족시키지 못한다. 그러므로 전자문서관리 시스템을 도입할 때 많은 주의가 필요하다. 전자문서관리 시스템을 판매하는 공급자는 Part 11 이 무엇인지도 알지 못하는 상태에서 계약의 성립을 위하여 Part 11 를 충족시킬 수 있다고 말할 수 있다. 하지만 Part 11 을 만족시키기 위해서는 단순한 사용자 편리나 부가기능뿐만 아니라 자료구조부터 새롭게 설계해야 한다. 그러므로 전자문서관리 시스템을 도입하려는 회사에서는 Part 11 에 대하여 충분히 이해하고 전자문서관리 시스템을 판매하려는 공급자에 Part 11 에 대하여 잘 설명해서 힘들게 만들었지만 버려야 하는 결과가 나오지 않도록 해야 한다.

전자문서에 대하여 '전자문서의 Life Cycle 과 종류[12]' 참조하기 바란다.

5.6 Internet 과 Part 11

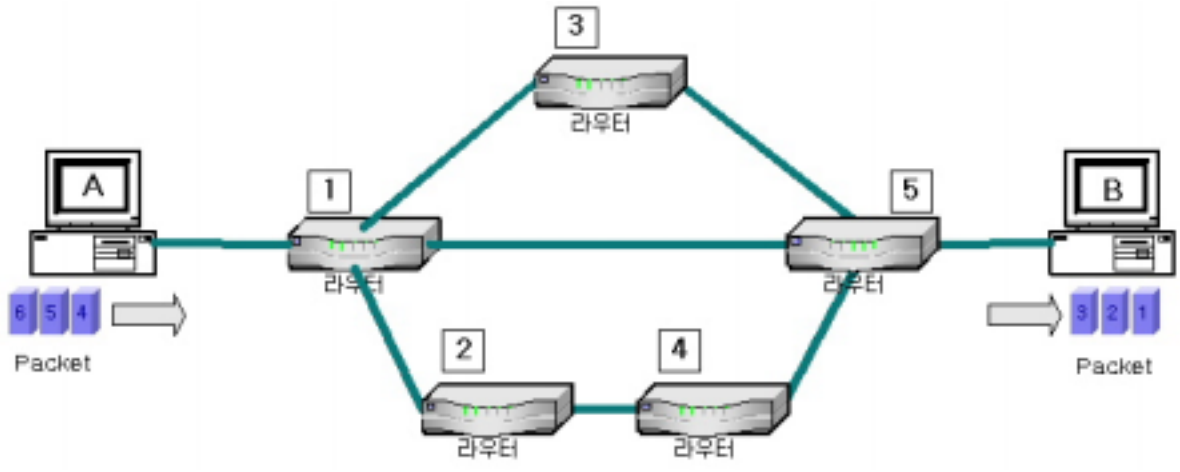
급속한 IT 기술의 발전과 초고속 통신망의 대중화로 인터넷이 없는 업무환경은 생각할 수도 없도록 변했다. 이제는 많은 소프트웨어가 인터넷을 이용하도록 만들어 지고 있다. 아직까지 의료보건 산업계에서는 규제대상이면서 인터넷을 이용한 시스템은 거의 사용되지 않았다. 하지만 곧 사용될 것이고 사용할 수 밖에 없는 상황에 될 것이다.

Part 11, GAMP, GMP, 검증에 관련해서 인터넷은 해결이 불가능한 골치덩어리이다.

우선 첫번째 이유는 인터넷은 전체 관리자가 없다는 것이다. 인터넷은 자발적인 네트워크로 각 단위 네트워크를 상호연결 시킨 전세계에서 가장 큰 네트워크이다. 단위 네트워크에는 관리자가 존재하지만 인터넷 전체에 대한 관리자가 없다. 최근 2003 년 1 월 25 일 국내에서 발생한 인터넷마비 사태는 이러한 문제점을 극단적으로 보여준다. 바이러스에 인한 무작위 대량공격에 대하여 일부 ISP 업체(한국통신, 하나로 등)의 노력만으로는 인터넷 전체를 관리/감독 할 수 없었다. 이러한 문제 단지 국내 ISP 업체나 대한민국 정부에서 해결할 수 없는 전세계적인 문제이다.

두번째 이유는 인터넷의 특성인 '동적전달경로'에 있다. 인터넷은 파일을 전송할 때 일정크기의 패킷(Packet)[1]으로 나누어서 비연결형 통신방식으로 자료를 전송한다. 다음 그림을 보자

[1] [패킷]
패킷이란 원래 우체국에서 취급하는 "소포"를 말하는데, 화물을 적당한 크기로 분할해서 행선지를 표시하는 꼬리표를 붙인 형태이다. 데이터 통신망에서 말하는 패킷이란, 데이터와 호 제어 신호가 포함된 2 진수, 즉 비트 그룹을 말하는데, 특히 패킷교환 방식에서 데이터를 전송할 때에는 패킷이라는 기본 전송 단위로 데이터를 분해하여 전송한 후, 다시 원래의 데이터로 재조립하여 처리한다. 전자우편이나 HTML 파일, GIF 파일, 기타 어떤 종류의 파일이라도, 이것을 인터넷을 통해 한 장소에서 다른 장소로 보내려 할때, TCP/IP 의 TCP 계층은 이 파일을 전송하기에 효율적인 크기로 자르게 된다. 분할된 각 패킷들에는 각각 별도의 번호가 붙여지고 목적지의 인터넷 주소가 포함되며, 각 패킷들은 인터넷을 통해 서로 다른 경로를 통해 전송될 수 있다. 보내어진 패킷들이 모두 도착하면, TCP 계층의 수신부에서 패킷들을 원래의 파일로 다시 재조립한다.



그림에서 컴퓨터 A 에서 컴퓨터 B 로 패킷을 전송하는 전달경로의 수는 다음과 같다.

1) 1 → 3 → 5
2) 1 → 5
3) 1 → 2 → 4 → 5

우리가 일반적으로 생각되는 최단 경로는 2)번이다. 그러나 이런 경로는 단지 라우터(Router)[2] 개수만을 생각한 것이고 각 연결 선로의 속도는 고려하지 않은 것이다. 선로의 속도는 유동적이며 라우터는 이런 유동적인 속도를 고려하여 스스로 경로를 설정한다. 결국 파일의 전송경로는 사전에 결정되지 않고 경우에 마다 다르다. 이 현상은 인트라넷으로 구축된 회사내부의 네트워크에서도 나타날 수 있다. 이러한 '동적전달경로'는 인터넷의 시초가 되었던 ARPANET 의 특성 때문이다. (ARPANET 은 미국 국방성이 군사 목적으로 개발한 것으로 전쟁발생시 특정 지역이 파괴되어도 통신을 유지할 수 있도록 고안된 네트워크이다.)

관리자가 없고 경로가 동적으로 변하는 네트워크를 사용하는 시스템을 신뢰할 수 있는가?

의료보건 산업계에서는 모든 것을 검증하여 사용한다. Part 11 의 대상이 되는 시스템도 검증해야 한다. 그러나 인터넷은 '동적전달경로' 특성으로 검증 대상(전달경로)을 알 수 없다. 따라서 인터넷을 검증하기 위해서는 인터넷 전체를 검증해야 한다. 현실적으로 불가능하다. 그럼 FDA 는 인터넷을 대체할 수 있는 신뢰할만한 네트워크를 제시할 수 있는가? 또한 제시된 신뢰할만한 네트워크를 위하여 의료보건 산업계는 막대한 인프라스트럭처 비용을 지불할 것인가? 불가능하다. 그럼 인터넷을 안사용 할 수 있는가? 인터넷을 사용하지 않는 것은 의료보건 산업계의 기술적 낙후만을 초래할 것이고 현재 인터넷은 적절한 수단으로 널리 사용되고 있다. 이러한 딜레마는 FDA 도 잘 알고 있다.

그래서 소극적이나마 대안책은 인터넷 말단 단말기인 '컴퓨터 시스템 검증'과 회사내부의 '네트워크 인프라스트럭처 검증'이 있다. 그러나 이것도 쉬운일은 아니다. 컴퓨터 시스템 검증은 하드웨어 검증과 소프트웨어 검증으로 나눌 수 있는데 핵심은 통신을 담당하는 소프트웨어의 검증이다. 하지만 통신을 담당하는 소프트웨어는 대부분 운영시스템이 담당하고 있으며 우리가 사용하는 대부분의 운영시스템은 Microsoft 사의 Windows 이다. Microsoft 사는 미국 정부에 대해서도 아주 국한

[2] [라우터]
라우터는 동일한 전송 프로토콜을 사용하는 분리된 네트워크를 연결하는 장치로 네트워크 계층간을 서로 연결한다. 경로 배정표(routing table)에 따라 전송할 패킷이 다른 네트워크로 보내야 하는지 자신의 네트워크로 보내야 하는지를 결정한다. 그리고 여러 경로 중 가장 효율적인 경로를 선택하여 패킷을 보낸다. 라우터는 흐름제어를 하며, 인터네트워크 내부에서 여러 서브네트워크를 구성하고, 다양한 네트워크 관리 기능을 수행한다.

적으로 프로그램 소스를 제공한다. 현실적으로 검증은 불가능하다. 따라서 우리에게는 컴퓨터 시스템의 하드웨어를 검증하는 것과 회사내부의 네트워크 인프라스트럭처 검증만이 남아 있다. 인터넷의 가용성, 범위, 크기를 생각할 때 참으로 초라한 대안이다.

최근에 이러 문제를 극복하기 위하여 인터넷을 이용한 프로그램에서는 암호화 기술을 이용하여 자료는 전송하는 것이 새로운 대안이다.(하지만 여전히 초라하다) 암호화 기법으로는 SSL(Secure Sockets Layer), HTTPS(Secure Hypertext Transfer Protocol), ActiveX, DLL 등을 사용할 수 있다.

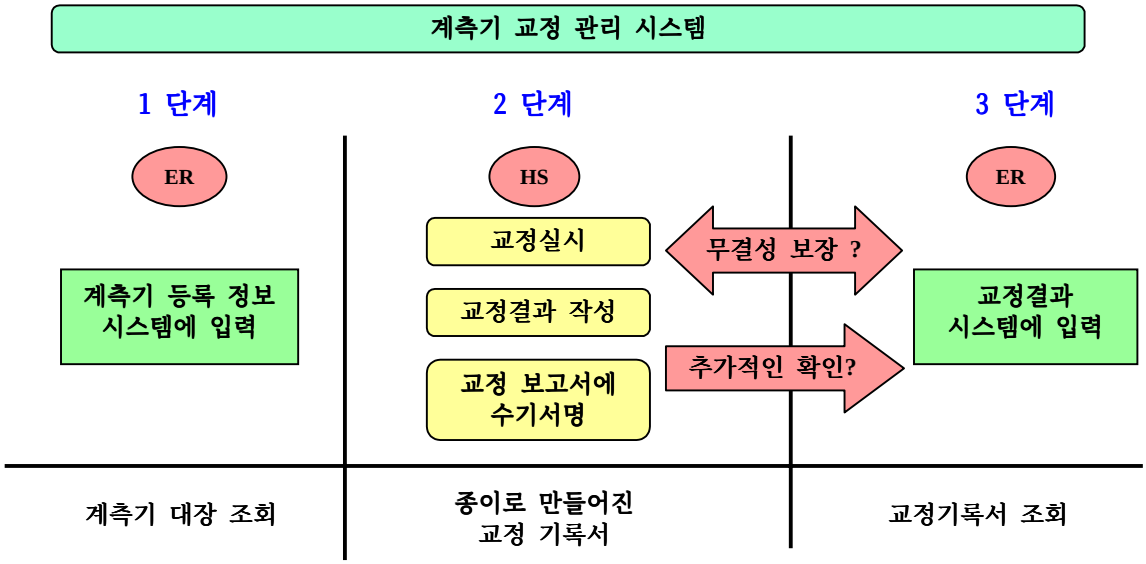
5.7 하이브리드 시스템 (Hybrid System)

하이브리드 시스템이란 Part 11 을 따르는 완벽한 전자기록과 전자서명 시스템과 전통적인 수기기록과 수기서명 시스템 사이에 있는 시스템으로 부분적으로 Part 11 를 충족하는 시스템이다. 현재 대부분은 시스템은 하이브리드 시스템으로 생각할 수 있다.

하이브리드 시스템은 여러 가지 종류가 있으며 경우마다 다르다. 하지만 하이브리드 시스템은 결국 Part 11 을 준수하는 시스템으로 변경해야 한다. 각 경우마다 해결책은 다르다. 경우에 따라서는 처음부터 다시 만들어야 한다.

최근 들어 Part 11 에 대한 준수정책으로 전자기록과 수기서명을 사용하는 시스템에 대하여 종종 들을 수 있다. 의료보건 산업계에서는 이러한 하이브리들 시스템이 Part 11 을 부분적으로 준수하면서도 회사업무에는 충격을 조금만 주는 좋은 해결책으로 생각하는 경향이 있는 것 같다. 그러나 이러한 하이브리드 시스템은 차라리 도입하지 않는 것이 좋다. 다음의 예를 생각해 보자.

계측기 교정 관리 시스템
: 이 시스템은 계측기 세부 자료를 등록한 후 해당 시스템을 이용하여 계측기의 교정시기를 조회하여 대상 계측기를 교정하고 실시한 교정결과를 시스템에 등록하여 이후 교정결과를 조회할 수 있는 시스템이다.



위와 같은 하이브리드 시스템의 경우 2 단계까지의 사용에는 아무런 문제가 없다. 하지만 이후 시스템에서 교정결과를 조회하기 위해서는 3 단계과정이 필요하다. 2 단계에서 서명한 자료는 종이이

므로 수기서명한 교정결과를 시스템에 입력해야 한다. 수기서명 자료와 시스템에 입력한 자료의 무결성을 보장할 수 있는가? 만약 자료의 무결성을 유지하기 위하여 교정결과를 입력하는 과정에서 추가적인 확인절차를 거친다면 이것은 전자서명과 다를 것이 없다. 또한 자료의 불일치로 문제가 생길 경우 원본자료로 인정되는 것은 수기서명된 종이자료이므로 결과적으로 전지기록은 불필요한 자료가 된다.

결국 이러한 전자기록+수기서명의 하이브리드 시스템은 불필요한 업무만을 만들고 Part 11 의 준수에는 아무런 도움이 되지 않는 시스템이다. 이런 시스템의 도입은 많은 사람을 힘들게 만들 것이다.

5.8 국내전자서명법과의 관계

국내에는 전자서명법이 존재한다. 이법은 1999 년에 재정하여 지금까지 시행되어온 법이다. 국내의 전자서명법은 여러 가지 전자서명 중에서 '공인전자서명'을 중심으로 만들어진 법이다.

'공인전자서명'은 RSA[3]의 공개/개인키 암호화 시스템을 사용한 디지털 서명이다.(Part11 에서 열린 계일 때 권장하는 방법)

Part11 은 특정 조직내에서 수기서명을 대처할 방안으로 만들어진 법인데 반하여 국내 전자서명법은 국내에서 전자서명의 안전성, 신뢰성, 공증성을 확립하기 위하여 만들어진 법이다. 따라서 국내의 전자서명법과 Part 11 를 유사한 것으로 생각하거나 비교하는 것은 무의미하다.

5.9 Audit Trail

Audit Trail 은 Part 11 을 준수하는 시스템이라면 반드시 있어야 하는 기능이며 Audit Trail 에 대한 기술적 타당성 조사와 검증이 필요하다. Audit Trail 은 전자기록의 등록, 변경내용을 확인할 수 있고, 부적절한 자료조작을 찾아낼 수 있고, 수행자의 부인방지를 불가능하도록 한다.
이런 이유로 Audit Trail 은 자동적으로 생성되야 하며 날짜와 시간이 독립적으로 기록되며(time-stamp 된) 가능하다면 누가, 무엇에 대한 정보를 포함해야 한다. 자동으로 생성되므로 당연히 서명 없이 생성된다. Audit Trail 은 전자기록에 대한 부가적인 기록이므로 해당 전자기록의 보존기간과 동일하게 보존해야 한다.

만약 전자기록/전자서명 시스템이 DBMS(데이터베이스 관리 시스템)를 이용하도록 구축되었다면 DBMS 의 기능인 Trigger 를 이용하여 아주 쉽게 구현할 수 있다. Trigger 를 이용한 Audit Trail 은 자료에 대해서만 작동하므로 작업의 행위에 대한 Audit Trail 이 아니라 자료에 대한 Audit Trail 이다. 하지만 Trigger 는 모든 전자기록에 대하여 작동하므로 Part 11 을 충분히 준수한다.

---

[3] RSA (Rivest-Shamir-Adleman)
RSA 는 1977 년에 Ron Rivest, Adi Shamir 와 Leonard Adleman 에 의해 개발된 알고리즘을 사용하는 암호화 및 인증 시스템이다. RSA 알고리즘은 가장 보편적으로 사용되는 암호화 및 인증 알고리즘으로서, 넷스케이프와 마이크로소프트 웹브라우저 기능의 일부로 포함된다. 이 암호화 시스템의 소유권은 RSA Security 라는 회사가 가지고 있다.
이 알고리즘은 두 개의 큰 소수(소수는 그 숫자와 1 로만 나누어지는 수이다)들의 곱과, 추가 연산을 통해 공개키와 개인키를 만든다. 만들어진 공개키와 개인키는 암호화/복호화에 사용된다.
개인키는 공개키에 의해 암호화된 텍스트를 복호화하는데 사용된다. 그러므로, 만약 누군가에게 메시지를 보내는 상황을 가정하면, 중앙의 관리자로부터 수신자의 공개키를 찾은 다음, 그 공개키를 사용하여 보내는 메시지를 암호화하여 보낸다. 수신자는 그것을 받아서, 자신의 개인키로 복호화한다. 추가적으로 메시지를 암호화하는 것 외에도, 발신자는 자신의 개인키를 사용하여 디지털 서명을 암호화해서 함께 보냄으로써, 그 메시지가 틀림없이 발신자에게서 온 것임을 수신자에게 확신 시켜줄 수 있다. 메시지를 받은 사람은, 발신자의 공개키를 이용해 메시지를 복호화할 수 있다.

참고문서

1. FDA 21 CFR Part 11 Electronic Records; Electronic Signatures: Final Rule.
2. FDA, Guidance for Industry(Draft), 21 CFR Part 11, Electronic Records; Electronic Signatures – Scope and Application, 2003. 2
3. 유재훈, GAMP 용어해석, www.validation.co.kr, 2003. 2
4. FDA, Glossary of Computerized System and Software Development Terminology, 1995
5. FDA, Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures Validation
6. FDA, Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures, Glossary of Terms
7. FDA, Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures, Time Stamps
8. FDA, Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures, Maintenance of Electronic Records
9. FDA, Guidance for industry(Draft), 21 CFR Part 11; Electronic Records; Electronic Signatures, Electronic Copies of Electronic Records
10. FDA, General Principles of Software Validation; Final Guidance for Industry and FDA Staff, 2002. 1. 11
11. GAMP Forum, GAMP4, The Good Automated Manufacturing Practice(GAMP) Guide for Validation of Automated System, ISPE, 2001.12
12. 유재훈, 전자문서의 Life Cycle 과 종류, www.validation.co.kr, 2003. 2