XII. 전자 서명 컴포넌트 및 관리(Electronic Signature Components and Controls)(Sec. 11.200)

122. Proposed Sec. 11.200 sets forth requirements for electronic signature identification mechanisms and controls. Two comments suggested that the term "identification code" should be defined. Several comments suggested that the term "identification mechanisms" should be changed to "identification components" because each component of an electronic signature need not be executed by a different mechanism.
섹션 11.200은 전자 서명 확인 메커니즘 및 관리에 관한 기준을 제시하고 있다. "ID 코드"의 의미를 정의해야 한다는 의견이 2건 있었다. "ID 메커니즘"을 "ID 컴포넌트"로 변경해야 한다는 의견이 다수 있었다. 전자 서명의 각 컴포넌트를 서로 다른 메커니즘으로 실행할 필요는 없기 때문이라는 이유에서다.

The agency believes that the term "identification code" is sufficiently broad and generally understood and does not need to be defined in these regulations. FDA agrees that the word "component" more accurately reflects the agency's intent than the word "mechanism," and has substituted "component" for "mechanism" in revised Sec. 11.200. The agency has also revised the section heading to read "Electronic signature components and controls" to be consistent with the wording of the section.
"ID 코드"는 충분히 일반적이고 이해에 무리가 없으며, 이 규정에서 그 의미를 정의할 필요는 없다고 생각한다. "메커니즘"보다는 "컴포넌트"가 FDA의 의도를 보다 정확히 반영한다는 의견에 동의하여, 섹션 11.200의 "메커니즘"을 "컴포넌트"로 변경했다. 또한 이 섹션의 문구에 맞추어 섹션 제목을 "전자 서명 컴포넌트 및 관리"로 수정했다.

123. Proposed Sec. 11.200(a) states that electronic signatures not based upon biometric/behavioral links must: (1) Employ at least two distinct identification mechanisms (such as an identification code and password), each of which is contemporaneously executed at each signing; (2) be used only by their genuine owners; and (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.
섹션 11.200(a)는 생체 인식/행동 링크를 바탕으로 하지 않는 전자 서명은 (1) 최소한 두 개의 뚜렷한 확인 메커니즘(예, ID 코드와 패스워드)을 갖추고 서명을 할 때마다 각각이 동시에 실행되며, (2) 진짜 소유자 본인만 사용해야 하고, (3) 본인 이외의 다른 사람이

전자 서명을 사용고자 할 때는 두 명 이상이 함께 하도록 관리해야 한다고 규정하고 있다.

Two comments said that proposed Sec. 11.200(a) should acknowledge that passwords may be known not only to their genuine owners, but also to system administrators in case people forget their passwords.
패스워드를 잊어버리는 경우에 진짜 소유자 이외에도 시스템 관리자도 패스워드를 알 수 있다는 점을 섹션 11.200(a)에서 인정해야 한다는 의견이 2건 있었다.

The agency does not believe that system administrators would routinely need to know an individual's password because they would have sufficient privileges to assist those individuals who forget passwords.
시스템 관리자는 패스워드를 잊어버린 사람을 지원할 충분한 권한을 가질 수 있기 때문에, 다른 사람의 패스워드도 알 필요가 있다고 생각하지 않는다.

124. Several comments argued that the agency should accept a single password alone as an electronic signature because: (1) Combining the password with an identification code adds little security, (2) administrative controls and passwords are sufficient, (3) authorized access is more difficult when two components are needed, (4) people would not want to gain unauthorized entry into a manufacturing environment, and (5) changing current systems that use only a password would be costly.
패스워드만 전자 서명으로 수용해야 한다고 주장한 의견이 다수 있었다. (1) 패스워드와 ID 코드의 조합은 보안성 강화에 도움이 되지 않으며, (2) 운영 측면의 관리와 패스워드면 충분하고, (3) 두 개 컴포넌트가 필요하다면, 허가 받은 접근이 보다 어려울 수 있으며, (3) 사람들은 제조 환경에 허가 없이 들어가기를 원하지 않고, (5) 패스워드만을 사용하는 현재의 시스템을 변경하려면 많은 비용이 든다는 이유를 들었다.

The comments generally addressed the need for two components in electronic signatures within the context of the requirement that all components be used each time an electronic signature is executed. Several comments suggested that, for purposes of system access, individuals should enter both a user identification code and password, but that, for subsequent signings during one period of access, a single element (such as a password) known only to, and usable by, the individual should be sufficient.
전자 서명을 할 때마다 모든 컴포넌트를 사용해야 한다는 기준과 관련하여, 전자 서명에 2개 컴포넌트가 필요한지 여부를 거론한 의견이 있었다. 시스템 접근성 측면에서 사용자

ID 코드와 패스워드 모두를 입력해야 하지만, 1회 접속 기간 동안에 일어나는 이후의 서명인 경우에는 당사자만 알고 사용할 수 있는 단일 요소(예, 패스워드)면 충분하다고 주장한 의견이 다수 있었다.

The agency believes that it is very important to distinguish between those (nonbiometric) electronic signatures that are executed repetitively during a single, continuous controlled period of time (access session or logged-on period) and those that are not. The agency is concerned, from statements made in comments, that people might use passwords that are not always unique and are frequently words that are easily associated with an individual. Accordingly, where nonbiometric electronic signatures are not executed repetitively during a single, continuous controlled period, it would be extremely bad practice to use a password alone as an electronic signature. The agency believes that using a password alone in such cases would clearly increase the likelihood that one individual, by chance or deduction, could enter a password that belonged to someone else and thereby easily and readily impersonate that individual. This action could falsify electronic records.
연속적인 단일 통제 기간(접속 섹션 또는 로그온 기간) 동안 반복적으로 하는 (비생체인식성) 전자 서명과 그렇지 않은 전자 서명을 구분하는 것이 중요하다고 본다. 의견에 제시된 사항을 통해, 사람들이 고유하지 않고 때로는 개인과 용이하게 연계시킬 수 있는 단어로 된 패스워드를 사용할 수 있다고 생각한다. 이에 따라 비생체인식성 전자 서명이 연속적인 단일 통제 기간 동안 반복하여 사용되지 않는다면, 패스워드만 전자 서명으로 사용하는 것은 매우 좋지 않은 방법이라 할 수 있다. 그런 경우에 패스워드만 사용하면, 우연이건 추정에 의해서건 다른 사람의 패스워드를 입력하여 용이하고 수월하게 그 사람을 가장할 가능성이 명확히 증가할 것이라 확신한다. 이러한 행위는 전자 기록서를 변조할 수 있다.

The agency acknowledges that there are some situations involving repetitive signings in which it may not be necessary for an individual to execute each component of a nonbiometric electronic signature for every signing. The agency is persuaded by the comments that such situations generally involve certain conditions. For example, an individual performs an initial system access or "log on," which is effectively the first signing, by executing all components of the electronic signature (typically both an identification code and a password). The individual then performs subsequent signings by executing at least one component of the electronic signature, under controlled conditions that prevent another person from impersonating the legitimate signer. The agency's concern here is the possibility

that, if the person leaves the workstation, someone else could access the workstation (or other computer device used to execute the signing) and impersonate the legitimate signer by entering an identification code or password.
반복적으로 서명하는 상황이 있을 수 있고, 이럴 때는 비생체인식성 전자 서명의 각 컴포넌트를 서명을 할 때마다 사용할 필요가 없을 수 있다는 점을 인정한다. 그런 상황은 일반적으로 특정 조건과 관련이 있다는 점을 알게 되었다. 예를 들어 누군가가 처음 시스템에 접근하거나 "로그온"할 때는 전자 서명의 모든 컴포넌트(일반적으로 ID 코드와 패스워드)를 사용해 효과적으로 첫 서명을 한다. 다음부터는 다른 사람이 합법적인 서명자를 가장하지 못하게 하는 통제 조건에서 전자 서명 가운데 최소한 1개 컴포넌트만 활용해 서명을 계속한다. 여기서 우려되는 부분은, 그 사람이 워크스테이션을 벗어났을 때, 다른 누군가가 워크스테이션(또는 그 서명을 실행하는데 사용되는 다른 컴퓨터 장치)에 접근하여 ID 코드나 패스워드를 입력해 합법적인 서명자를 가장할 수 있다는 점이다.

The agency believes that, in such situations, it is vital to have stringent controls in place to prevent the impersonation. Such controls include: (1) Requiring an individual to remain in close proximity to the workstation throughout the signing session; (2) use of automatic inactivity disconnect measures that would "de-log" the first individual if no entries or actions were taken within a fixed short timeframe; and (3) requiring that the single component needed for subsequent signings be known to, and usable only by, the authorized individual.
그런 상황에서는 다른 사람을 가장하지 못하게 엄격한 관리 대책을 강구하는 것이 매우 중요하다. 그런 관리 대책으로는 (1) 서명 세션 동안 워크스테이션에 항상 가까이 있도록 요구하고 (2) 일정 시간 동안 입력이나 행위가 없으면 첫 번째 사람을 "디로그"하는 자동 비활성 접속 차단 대책을 활용하며 (3) 이후의 서명에 필요한 단일 컴포넌트는 허가 받은 자만이 알고 있으며 그 사람만이 사용할 수 있는 것으로 하는 방법이 있다.

The agency's objective in accepting the execution of fewer than all the components of a nonbiometric electronic signature for repetitive signings is to make it impractical to falsify records. The agency believes that this would be attained by complying with all of the following procedures where nonbiometric electronic signatures are executed more than once during a single, continuous controlled session: (1) All electronic signature components are executed for the first signing; (2) at least one electronic signature component is executed at each subsequent signing; (3) the electronic signature component executed after the initial signing is only used by its genuine owner, and is designed to ensure it can only be used by its genuine owner; and (4) the electronic signatures are administered and executed to

ensure that their attempted use by anyone other than their genuine owners requires collaboration of two or more individuals. Items 1 and 4 are already incorporated in proposed Sec. 11.200(a). FDA has included items 2 and 3 in final Sec. 11.200(a).
반복 서명인 경우에 비생체인식성 전자 서명의 모든 컴포넌트가 아닌 일부의 사용을 수용하는데 있어서 FDA가 목표로 하는 부분은, 기록서 변조를 불가능하게 하는 것이다. 단일의 연속적인 통제 세션 동안 비생체인식성 전자 서명을 1회 이상 하는 경우에 다음의 절차를 모두 준수함으로써 그 목표를 달성할 수 있다고 생각한다. (1) 첫 서명 시에는 모든 전자 서명 컴포넌트를 사용하고, (2) 이후의 서명마다 최소한 1개의 전자 서명 컴포넌트를 사용하며, (3) 최초 서명 이후에 사용하는 전자 서명 컴포넌트는 진짜 소유자만이 사용하며 진짜 소유자만이 사용할 수 있도록 설계하고, (4) 진짜 소유자 이외의 다른 사람이 사용하려고 할 때는 2사람 이상이 함께 참여하도록 요구하는 식으로 전자 서명을 관리하고 사용한다. 1번과 4번은 이미 섹션 11.200(a)에 포함되어 있다. 그러므로 최종 규정에서는 2번과 3번을 추가했다.

The agency cautions, however, that if its experience with enforcement of part 11 demonstrates that these controls are insufficient to deter falsifications, FDA may propose more stringent controls.
하지만 파트 11 시행 경험이 쌓이면서 이 정도 관리로는 변조를 방지하기에 충분하지 않다고 밝혀지면, 보다 엄격한 관리 방안을 제시할 수 있다.

125. One comment asserted that, if the agency intends the term "identification code" to mean the typical user identification, it should not characterize the term as a distinct mechanism because such codes do not necessarily exhibit security attributes. The comment also suggested that proposed Sec. 11.200(a) address the appropriate application of each possible combination of a two-factor authentication method.
"ID 코드"가 일반적인 사용자 확인 코드를 의미하는 것이라면, 그런 코드는 보안 특성을 갖지 않기 때문에 이를 뚜렷한 메커니즘이라 볼 수 없다고 주장한 의견이 1건 있었다. 또한 섹션 11.200(a)는 2개 요소로 구성된 인증 방법의 다양한 조합 각각을 적절하게 적용하는 부분도 다루어야 한다고 제안했다.

The agency acknowledges that the identification code alone does not exhibit security attributes. Security derives from the totality of system controls used to prevent falsification. However, uniqueness of the identification code when combined with another electronic signature component, which may not be unique (such as a

password), makes the combination unique and thereby enables a legitimate electronic signature. FDA does not now believe it necessary to address, in Sec. 11.200(a), the application of all possible combinations of multifactored authentication methods.
ID 코드만으로는 보안 특성을 발휘하지 못한다는 점을 인정한다. 변조 방지를 위한 시스템 관리의 총합을 통해 보안이 확보된다. 하지만 고유하지 않을 수 있는 다른 전자 서명 컴포넌트(예, 패스워드)와 조합될 때는 ID 코드의 고유성이 그 조합을 고유하게 만들고 합법적인 전자 서명을 가능하게 한다. 여러 요소로 구성된 인증 방법의 가능한 모든 조합을 섹션 11.200(a)에서 다룰 필요는 없다고 생각한다.

126. One comment requested clarification of "each signing," noting that a laboratory employee may enter a group of test results under one signing.
시험 작업자는 하나의 서명으로 여러 시험 결과를 입력할 수 있다는 점을 지적하며, "each signing"의 의미를 명확히 해달라는 요청이 있었다.

The agency advises that each signing means each time an individual executes a signature. Particular requirements regarding what records need to be signed derive from other regulations, not part 11. For example, in the case of a laboratory employee who performs a number of analytical tests, within the context of drug CGMP regulations, it is permissible for one signature to indicate the performance of a group of tests (21 CFR 211.194(a)(7)). A separate signing is not required in this context for each separate test as long as the record clearly shows that the single signature means the signer performed all the tests.
"each signing"은 서명을 하는 매 순간을 의미한다. 서명이 필요한 기록서에 대한 기준은 파트 11이 아닌 다른 규정에 제시되어 있다. 예를 들어 다수의 분석 시험을 수행하는 시험 작업자인 경우, 의약품 CGMP 규정에 따라 하나의 서명으로 일련의 시험 수행을 표시할 수 있다(21 CFR 211.194(a)(7)). 하나의 서명이 그 서명자가 모든 시험을 수행했다는 의미를 기록서가 명확히 보여 준다면, 각각의 시험마다 별도로 서명할 필요는 없다.

127. One comment suggested that the proposed requirement, that collaboration of at least two individuals is needed to prevent attempts at electronic signature falsification, be deleted because a responsible person should be allowed to override the electronic signature of a subordinate. Several comments addressed the phrase "attempted use" and suggested that it be deleted or changed to "unauthorized use." The comments said that willful breaking or circumvention of any security measure does not require two or more people to execute, and that the central

question is whether collaboration is required to use the electronic signature.
전자 서명 변조 방지를 위해 2명 이상의 공동 작업이 필요하다는 기준을 삭제해야 한다는 의견이 1건 있었다. 책임자는 부하 직원의 전자 서명을 오버라이드할 수 있도록 허용해야 하기 때문이라는 것이다. "attempted use"라는 표현과 관련하여, 이를 삭제하거나 "무허가 사용(unauthorized use)"으로 바꾸자는 의견이 다수 있었다. 보안 대책을 고의적으로 깨거나 우회하는데 2명 이상이 필요한 것은 아니며, 전자 서명을 사용하는데 공동 작업이 필요한지 여부가 중요하다고 말했다.

The agency advises that the intent of the collaboration provision is to require that the components of a nonbiometric electronic signature cannot be used by one individual without the prior knowledge of a second individual. One type of situation the agency seeks to prevent is the use of a component such as a card or token that a person may leave unattended. If an individual must collaborate with another individual by disclosing a password, the risks of betrayal and disclosure are greatly increased and this helps to deter such actions. Because the agency is not condoning such actions, Sec. 11.200(a)(2) requires that electronic signatures be used only by the genuine owner. The agency disagrees with the comments that the term "attempted use" should be changed to "unauthorized uses," because "unauthorized uses" could infer that use of someone else's electronic signature is acceptable if it is authorized.
공동 작업 조항의 취지는, 모르는 상태로 비생체인식성 전자 서명 컴포넌트를 누군가 사용하지 못하게 하자는데 있다. FDA가 방지하고자 하는 상황 가운데 하나는, 어떤 사람이 방치해둔 카드나 토큰 같은 컴포넌트의 사용이다. 패스워드를 공개하여 다른 사람과 공동 작업을 해야 한다면, 배신과 폭로 위험성이 크게 증가할 것이므로, 이 조항은 그러한 행위를 억제하는데 도움이 될 것이다. FDA는 그런 행위를 용인하지 않으므로, 섹션 11.200(a)(2)는 전자 서명을 진짜 소유자인 본인만 사용하도록 요구하고 있다. "attempted use"를 "unauthorized uses"로 변경하자는 주장에도 동의할 수 없다. "unauthorized uses"는 허가를 받으면 다른 사람의 전자 서명 사용도 용인된다는 의미로 해석될 수 있기 때문이다.

Regarding electronic signature "overrides," the agency would consider as falsification the act of substituting the signature of a supervisor for that of a subordinate. The electronic signature of the subordinate must remain inviolate for purposes of authentication and documentation. Although supervisors may overrule the actions of their staff, the electronic signatures of the subordinates must remain a permanent part of the record, and the supervisor's own electronic signature must

appear separately. The agency believes that such an approach is fully consistent with procedures for paper records.
전자 서명 "오버라이드"와 관련하여, 부하 직원의 서명을 관리자의 서명으로 대체하는 행위를 FDA는 변조로 간주한다. 입증 및 문서화 측면에서 그 부하 직원의 전자 서명은 그대로 유지되어야 한다. 관리자가 부하 직원의 행위를 좌우할 수 있지만, 부하 직원의 전자 서명은 그 기록서의 영구적인 일부로 유지되어야 하며, 관리자의 전자 서명은 별도로 있어야 한다. 이와 같은 방식이 종이 기록서에 적용되는 절차와도 완전히 일치한다고 생각한다.

As a result of the revisions noted in comments 123 to 127 of this document, Sec. 11.200(a) now reads as follows:
123번 항목부터 127번 항목까지의 의견을 반영하여, 섹션 11.200(a)를 다음과 같이 수정했다.

(a) Electronic signatures that are not based upon biometrics shall:
생체 인식을 바탕으로 하지 않는 전자 서명은 다음 사항을 충족해야 한다.

(1) Employ at least two distinct identification components such as an identification code and password.
확인 코드 및 패스워드 같이, 최소한 두 개의 뚜렷한 확인 컴포넌트를 갖춰야 한다.

(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.
관리 대상 시스템의 연속적인 단일 접속 기간 동안 한 사람이 일련의 서명을 하는 경우, 첫 서명은 모든 전자 서명 컴포넌트를 이용해 실시하고, 이후 서명은 그 사람만 실행할 수 있고 그 사람만 사용하도록 설계된 최소 한 개의 전자 서명 컴포넌트를 이용해 실시한다.

(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.
관리 대상 시스템의 연속적인 단일 접속 기간 동안 1회 이상 서명을 하지 않는 경우, 각 서명은 모든 전자 서명 컴포넌트를 이용해 실시한다.

(2) Be used only by their genuine owners; and
진짜 소유자 본인만 사용해야 한다.

(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.
전자 서명을 본인 이외의 다른 사람이 사용하고자 할 때는 두 명 이상의 공동 작업이 필요하도록 관리하고 운영한다.

128. Proposed Sec. 11.200(b) states that electronic signatures based upon biometric/behavioral links be designed to ensure that they could not be used by anyone other than their genuine owners.
섹션 11.200(b)는 생체인식/행동 링크에 기반한 전자 서명은, 본인 이외의 다른 사람이 사용할 수 없도록 설계해야 한다고 규정하고 있다.

One comment suggested that the agency make available, by public workshop or other means, any information it has regarding existing biometric systems so that industry can provide proper input. Another comment asserted that proposed Sec. 11.200(b) placed too great an emphasis on biometrics, did not establish particular levels of assurance for biometrics, and did not provide for systems using mixtures of biometric and nonbiometric electronic signatures. The comment recommended revising the phrase "designed to ensure they cannot be used" to read "provide assurances that prevent their execution."
생체 인식 시스템에 관하여 FDA가 갖고 있는 정보를 워크숍이나 기타 방법으로 공개하고 업체도 의견을 제시할 수 있는 기회를 갖자고 제안한 의견이 1건 있었다. 또한 섹션 11.200(b)는 생체 인식 시스템을 너무 강조하고 있으며, 생체 인식 시스템의 보증 수준을 제시하지 않았고, 생체 인식 및 비생체인식 전자 서명을 복합적으로 활용하는 시스템에 대한 사항은 없다는 주장이 있었다. "designed to ensure they cannot be used"를 "provide assurances that prevent their execution"으로 수정하자고 제안했다.

The agency's experience with biometric electronic signatures is contained in the administrative record for this rulemaking, under docket no. 92N-0251, and includes

recommendations from public comments to the ANPRM and the proposed rule. The agency has also gathered, and continues to gather, additional information from literature reviews, general press reports, meetings, and the agency's experience with this technology. Interested persons have had extensive opportunity for input and comment regarding biometrics in part 11. In addition, interested persons may continue to contact the agency at any time regarding biometrics or any other relevant technologies. The agency notes that the rule does not require the use of biometric-based electronic signatures.
생체 인식 기반 전자 서명과 관련한 FDA의 경험이 이 규정 제정 관련 문서(문서 번호 92N-0251)에 포함되어 있으며, 여기에는 ANPRM과 규정안에 대한 의견과 권고 사항이 담겨 있다. 또한 FDA는 참고 문헌, 일반 언론 기사, 회의, 이 기술의 활용 경험을 통해 정보를 추가로 확보했으며, 앞으로도 확보할 것이다. 파트 11의 생체 인식과 관련하여 의견을 제시할 기회는 많이 있었다. 또한 생체 인식 또는 기타 관련 기술에 대하여 언제든지 FDA에 문의할 수 있다. 이 규정은 생체 인식 기반 전자 서명의 사용을 요구하고 있지는 않다.

As the agency's experience with biometric electronic signatures increases, FDA will consider holding or participating in public workshops if that approach would be helpful to those wishing to adopt such technologies to comply with part 11.
생체 인식 기반 전자 서명과 관련한 경험이 늘어나고 파트 11 준수를 위해 그런 기술을 채택하고자 하는 자에게 도움이 된다면, 워크숍을 개최하거나 참여할 생각이다.

The agency does not believe that proposed Sec. 11.200(b) places too much emphasis on biometric electronic signatures. As discussed above, the regulation makes a clear distinction between electronic signatures that are and are not based on biometrics, but treats their acceptance equally.
섹션 11.200(b)가 생체 인식 기반 전자 서명을 지나치게 강조한다고 생각하지 않는다. 위에서 설명한 바와 같이, 이 규정은 생체 인식 기반 전자 서명과 그렇지 않은 전자 서명을 명확히 구분하고 있으나, 두 전자 서명의 수용성은 동일하게 취급하고 있다.

The agency recognizes the inherent security advantages of biometrics, however, in that record falsification is more difficult to perform. System controls needed to make biometric-based electronic signatures reliable and trustworthy are thus different in certain respects from controls needed to make nonbiometric electronic signatures reliable and trustworthy. The requirements in part 11 reflect those differences.

하지만 생체 인식 기술은 기록서 변조가 보다 어렵다는 점에서 내재적으로 보안성이 더 좋다는 점을 인정한다. 그러므로 생체 인식 기반 전자 서명을 신뢰성과 신빙성을 갖춘 것으로 만드는데 필요한 시스템 관리는 비생체인식 기반 전자 서명의 신뢰성과 신빙성을 확보하는데 필요한 관리에 비하여 일부 측면에서 다르다고 할 수 있다. 파트 11의 기준은 이런 차이를 반영하고 있다.

The agency does not believe that it is necessary at this time to set numerical security assurance standards that any system would have to meet.
현재로써는 모든 시스템이 충족해야 할 절대적인 보안 보증 표준을 설정할 필요는 없다고 생각한다.

The regulation does not prohibit individuals from using combinations of biometric and nonbiometric-based electronic signatures. However, when combinations are used, FDA advises that requirements for each element in the combination would also apply. For example, if passwords are used in combination with biometrics, then the benefits of using passwords would only be realized, in the agency's view, by adhering to controls that ensure password integrity (see Sec. 11.300).
생체인식 및 비생체인식 기반 전자 서명을 조합하여 활용하는 것을 금지하고 있지 않다. 하지만 이렇게 조합하여 활용한다면, 조합을 구성하는 각 요소에 대한 기준들도 적용될 것이다. 예를 들어 패스워드와 생체인식 기술을 조합하여 사용한다면, 패스워드의 완전성 보증을 위한 관리 기준(섹션 11.300)을 준수해야 패스워드 사용의 혜택이 실현될 수 있으리라 생각한다.

In addition, the agency believes that the phrase "designed to ensure that they cannot be used" more accurately reflects the agency's intent than the suggested alternate wording, and is more consistent with the concept of systems validation. Under such validation, falsification preventive attributes would be designed into the biometric systems.
또한 의견에서 제시한 문구에 비하여 "designed to ensure that they cannot be used"라는 표현이 FDA의 의도를 보다 정확하게 반영하고 있으며, 시스템 밸리데이션 개념과도 더 일치한다고 생각한다. 시스템 밸리데이션 관점에서는 변조 방지 특성 요소가 설계 단계에서 생체인식 시스템에 포함되어야 할 것이다.

To be consistent with the revised definition of biometrics in Sec. 11.3(b)(3), the agency has revised Sec. 11.200(b) to read, "Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other

than their genuine owners."

섹션 11.3(b)(3)의 생체인식에 대한 수정된 용어 정의에 맞추어, 섹션 11.200(b)를 다음과 같이 수정했다. "생체 인식 기반 전자 서명은 본인 이외의 다른 사람이 사용할 수 없도록 설계한다."