



ECObjectsにおけるFDA対応

電子記録を作成・変更・保存・発信する目的でクラウドシステムを使用する者は、電子記録の確実性・完全性、および、適切な機密性を保持し、電子記録への署名者が署名を容易に無効にできないように手続き、および、管理を行わなければならない。

21 CFR Part11要件	EC Objectsでの対応
<p>正確で完全な記録のコピーを人が読める形式、および、電子的な形式で当局の査察、審査、複写に応じた出力を行う能力があること</p>	<p>PDF出力、Excel出力、CSV出力、XML機能、および、印刷機能で対応</p>
<p>システムへのアクセスは、許可された権限をもつ個人に限定されていること</p>	<p>ユーザ管理機能で登録されたユーザのみシステムへアクセス可能となる</p>
<p>コンピュータで自動的に生成された確実なタイムスタンプによるオーディットレール(後日の追跡調査のための履歴)を使用し、オペレータのシステムへの接続、電子記録の作成・変更・削除の行為の記録を日付・時間とともに、元の記録とは別に独立して記録すること。記録の変更は、元の情報を読めなくてはならない。このようなオーディットレール文書は、当該の電子記録の保管義務期間以上を保管されなければならない。また、当局の査察・複写の要請に応じて添付しなければならない</p>	<p>検索履歴、端末接続ログ、更新履歴、ワークフロー承認、履歴、等々のオーディットレールを記録保存することができる</p>
<p>権限チェックを実施することによって、権限をもつ個人のみがシステムを使用し、記録に電子署名し、コンピュータもしくは操作システムの出力装置を操作し、記録を変更し、もしくは手動操作を実施することを確実にしなければならない</p>	<p>ユーザID毎に権限を設案することができる</p>
<p>システム文書の作成・変更が時間にそって履歴情報を維持・ドキュメント化できるようオーディットレールを管理すること</p>	<p>文書は時間軸をもって履歴管理し、また、検索履歴も管理する</p>

署名された電子記録は、下記事項に示す署名に付随したすべての情報を含まなければならない

21CFR Part11要件	E C Objectsでの対応
署名者の印字氏名、署名実施日と時間を記録できること	すべてのドキュメントは、実行日時を保持している。 ユーザIDと署名の実行日時も記録することができる
署名の意味(審査、承認、責任、否認、完了、完了不可)が明確にできること	プロセスに応じて、ワークフローにて承認、否認、完了、完了不可の設定が可能
署名の偽造ができないこと	ユーザID + パスワード + 署名 + ドキュメントにより、電子署名を生成する(ハッシング)
電子記録における電子署名の関連が保たれること 電子署名もしくは電子記録の上になされた手書き署名は、署名がなされた当該の電子記録と一対一で対応し、削除 / コピー / 転送を不可能とし、虚偽の電子記録が作成されないことを確実にしなければならない	電子署名は削除、変更ができない

21CFR Part11要件	ECObjectsでの対応
識別コード / パスワードのような少なくとも2つの別々の認識要素を使用すること	電子署名は、システムにログインしたユーザIDとパスワード+署名により構成される
システムにアクセス後、一定の継続期間中に署名を行う場合には、一回目の署名では、電子署名の構成要素のすべてを使用しなければならない。それ以降については、その個人にしか入力できない個人専用の少なくとも一つの電子署名構成要素を使用しなければならない	署名、文字入力により電子署名を行う
二人の個人が同一の組み合わせの認識コードとパスワードを持たぬよう、認識コードとパスワードの組み合わせの唯一性を維持すること	同じユーザIDが複数存在することはできない。また、パスワードはユーザIDに対して一意、署名文字はドキュメントに対して一意になる
業務処理に対する保護手段を設け、承認されていない認識コードやパスワードの使用を防止し、それらが不正使用されようとした場合には、不正使用を検出し、即座にシステム管理組織に報告するとともに、必要な場合には、経営組織に報告すること	ログイン再試行回数を設定することが可能であり、再試行回数を超えた場合、そのIDは無効となる
認識コードおよびパスワードが定期的にチェック / 回収 / 改定されることを確実にすること(パスワードの陳腐化防止等)	パスワードの有効期間および、失効前の警告日数を指定することができる

「ハッシュ関数」とは

ハッシュ関数は、次のような特徴を持ったアルゴリズムであり、あるデータについてハッシュ関数を使用して計算した値を、ハッシュ値あるいはメッセージダイジェストと言います。

ハッシュ関数の特性

- 元データの長さに関係なく、ハッシュ値はハッシュアルゴリズムごとに決められた一定の長さ（160ビット等）になる。
- 元データが少しでも違えばハッシュ値が大きく異なるため、改ざんの発見が容易である。
- ハッシュ値から元データを推測することは不可能。

このような特性により、ハッシュ関数は元データに対する改ざんの検知を可能にし、元データを一定長に短縮することで、暗号時の処理時間を必要最小限に抑えることを可能にします。ハッシュ関数として使用されるアルゴリズムには、SHA-1などがあり、それぞれに生成されるハッシュ値の長さが異なります。



ハッシュ関数

ハッシュ値

3fd052a1690a0fcd05e2b3da7d12dc…
(元データのサイズにかかわらず固定の長さ)







