ICH運営委員会　M2専門家作業部会　勧告
医薬品規制情報の伝送に関する電子的標準（ESTRI）
ファイルの完全性－MD5

［仮訳］

Ver 1.0　2010年6月10日

表題:ファイルの完全性－MD5

日付:2010年6月10日

背景:

ICH参加3地域において、規制情報を安全に電子的交換する必要性が認識されている。この安全な情報交換の実現においては、送信者側が意図した通りに受信者側が受け取ったことを保証するための方法が重要である。

勧告:

ファイルの完全性を保証するために「チェックサム」の利用が勧告される。チェックサムやハッシュ・サムは、伝送や保管中に偶発する可能性があるエラーを検出するために、デジタルデータの任意のブロックから計算される固定長のデータである。データの完全性は、チェックサムを再計算し、保存しているチェックサムと比較することによって、その後いつでも検証することができる。もしチェックサムが一致しなければ、（意図的であるか否かに関わらず）データはほぼ確実に変更されている。

電子的な提出においては、伝送される個々のファイルに対するチェックサムを含むべきである。この目的のために、MD5 メッセージダイジェストアルゴリズム（MD5）を利用することを勧告する。チェックサムの利用は、ファイルの伝送において、以下のような多くの利点を提供する。

- ファイルとともに提出されたチェックサムと計算によって求められたチェックサムを比較することで、ファイルの完全性を検証することができる。
- ファイルが規制当局の保管中に変更されていないことを検証するためにチェックサムを用いることができる。これは特にファイルをある記録媒体から別の記録媒体に移行する場合に有益である（例えば、磁気テープにファイルをバックアップした場合）。

適切な実装方法は交換メッセージに関するESTRIの仕様により定義される（例えば、ESTRI eCTDの仕様にはチェックサムを格納する明確な方法を定義している）。

規制当局における内部セキュリティとアクセスコントロールのプロセスによって、提出されたファイルの完全性が維持されるべきである。

条件:なし

備考:

MD5は、Internet Engineering Task Force（IETF）RFC1321で定義したオープン・スタンダードである。MD5の設計には明らかな欠点があり、他のアルゴリズムの使用が推奨され始めていることを、ICH M2は認識している。しかしながら、MD5はファイルの完全性を検証する目的には十分である。