8. WORM 技術と暗号化技術

さまざまな法規制や内部統制への対応が求められる中、企業のさまざまな活動を記録しているデータの長期保存が必須となってきた。これらのデータは企業側からすると業務が適法の元で遂行されたことを証明するための証拠となり、捜査機関側からは犯罪の有無を判断するための材料となる。そこで、長期保管が必須のデータについては、データの操作や編集、改ざん、破棄ができない形態で保管されている必要がある。これらを実現する技術が WORM（Write Once, Read Many）である。

ここでは、WORM が求められるようになった背景、主な利用分野、技術のほか、重要データの保護という観点から暗号化についても解説する。

8.1. 電子データの真偽性・原本性の証明に不可欠な WORM

WORM とは、データが一度メディアに書き込まれると、編集、変更、上書き、消去などが通常の手段によって物理的に編集、変更できないデータ記録技術をいう。このことが犯罪捜査の確実な証拠や監査証跡になることを意味することになる。電子データの場合にはデータの真偽性・原本性を問われることが多く、証拠として受け入れられるためには、内容や日付などが作為的に変更されていないことの証明が必要である。例えば、電子メールの内容や送受信のログが証拠となるには、それらが作成されてから適切な時期に更新不可能な状態に移行されていること（＝WORM メディアへの書き込み）が必要となる。

実は WORM デバイスの登場は、最近のことではなく、すでに 1980 年台初期から光磁気デバイスが用いられてきた。最初の WORM デバイスは、5.25 インチまたは 12 インチの MO ディスクである。現在は、磁気テープをはじめ、光ディスク（DVD-R/BD-R、Archival Disc）、HDD WORM、フラッシュメモリーなどで幅広く使われている技術となっている。

8.2. 米 SOX 法の制定を契機にニーズが高まる

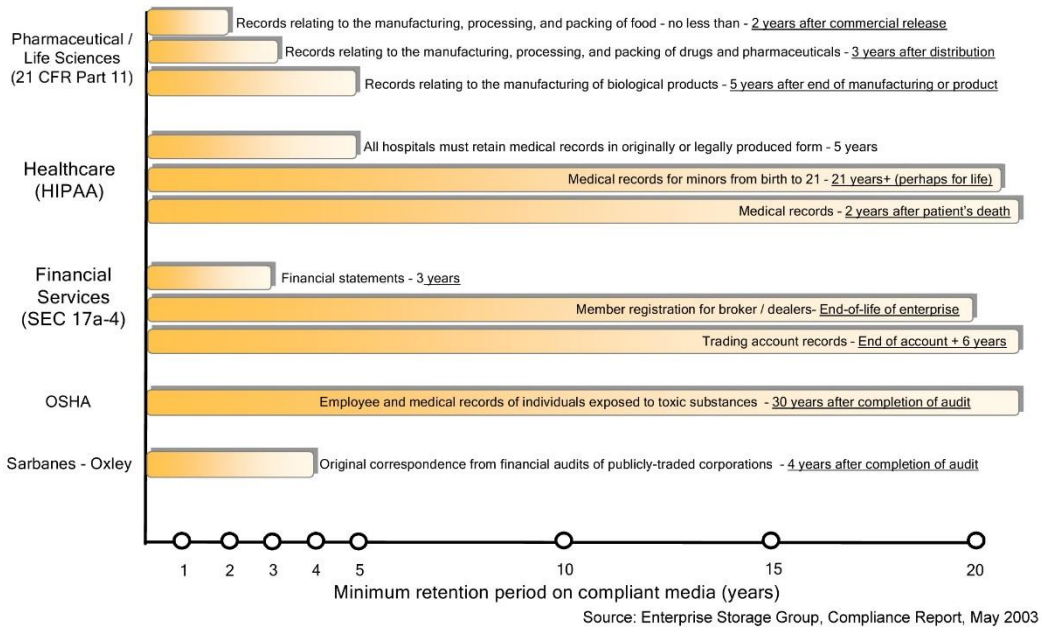
2000 年代になって改めて WORM が注目されるようになってきたのは、アメリカで企業の金融スキャンダルが相次いだ結果として、アメリカ企業改革法（SOX 法）が制定されたことが大きい。

SOX 法とは、過去の不祥事の反省から、企業の内部統制を強化し、企業の会計の信頼性を高め、管理・点検体制を整備することを義務付けた法である。これにより、企業は監査を的確に実施するため、重要データの保存が課題となり、契約関係を促進するため電子メール利用が増大する中で、データをより厳密に永久保護するための法令が要求されてきた。SOX 法の制定によって、企業規模を問わず厳しい財務監査要求がアメリカ国内のすべての株式会社と、アメリカ市場で株式取引を行うすべての外資系企業に適用されることとなった。法人財務の大部分が電子管理されているため、IT システムとデータも厳しい監査基準の下に置かれることになったのである。

この法令はデータ保存規定を義務付けており、企業財務記録の改ざんまたは破壊を行った場合は、たとえそれが召喚令状発行前に行われたものであったとしても処罰される。

米 SOX 法のほか、アメリカ証券取引法（改正法）、情報公開法（イギリス）、日本においては、日本版 SOX 法、e-文書法、個人情報保護法といった法令、さらに EU の一般データ保護規則(GDPR：General Data Protection Regulation)も発効されており、業務における情報ライフサイクル管理(ILM：Information Lifecycle Management)機能に対する需要が大きく増加している。今では、WORM デバイスはこの分野で不可欠なものとなり、重要な役割を果たしている。

また、アメリカ食品医薬品局（FDA：Food and Drug Administration）、医療保険の相互運用性と説明責任に関する法律（HIPAA：Health Insurance Portability and Accountability）などに代表されるように、金融分野や一般企業だけでなく、重要インフラ、医療、製薬分野におけるニーズも高まっている。



●WORM が利用されている主な分野

・一般企業 ……財務データ、研究・開発データ、取引情報、e メールなど
・原子力産業 ……原子炉作業記録
・製薬産業 ……医薬認定記録
・証券仲買人/証券会社 ……金融取引
・法律 ……必要書類
・政府機関 ……必要書類

データの不正な改ざんやアクセスログを残すといった証拠や監査証跡のための目的以外にも、WORM の活用がメリットとなるケースもある。それは改ざんを不可能とすることで、オペレーションミスによる大切なファイルの削除や上書きを防止し、情報の保護やセキュリティレベルの向上にも貢献することができるからである。

8.3. WORM デバイスとして魅力の大きいテープメディア

WORM 機能を持つストレージメディアの中で、特に企業ユーザーから高い支持を受けているのがテープメディアである。これはテープメディアが多くのメリットを持つ魅力的なメディアであるためである。中でもコストメリットは非常に高く、この点で HDD に対して大きな優位性を持つ。加えて LTO Ultrium（以下：LTO）は、同じドライブで通常のデータバックアップと WORM バックアップが可能であり、保存容量も WORM カートリッジの追加だけで拡張可能という柔軟性を持つ。

一方、光ディスクに対しても、大容量という点で優位性は非常に高い。CD や DVD は言うまでもなく、最近コンシューマ市場で普及が進む BD（ブルーレイディスク）でも 50GB（2 層）、Archival Disc でも 500GB(6 層)に過ぎない。これに対して、テープは最新の LTO-9 では 1 巻当たり 18TB、圧縮では 45TB もの大容量を持つ。

さらに、こうした光ディスクと比較すると処理スピードも非常に高速である。BD-R は現在 6 倍速で 27MB/秒、Archival Disc(SONY 製)で読み取りが 375MB/秒、ベリファイ記録時では 187.5MB/秒であるが、LTO-9 では読み取りも書き込みも最大 400MB/秒（圧縮時 1,000MB/秒）の転送速度を持つ。

以上の理由で、WORM を利用してデータ保存することが必要な環境では、テープメディアが支持されているのである。

8.4. LTO WORM テープ技術は多階層のセキュリティーシステムを使用

LTO 規格では、LTO-3 以降から WORM メディアをサポートしている。一般に WORM カートリッジは、書き換え（リード/ライト）可能な通常のデータカートリッジと外観上から容易に識別ができるようツートンカラーなどを採用している。

WORM テープは、CM（Cartridge Memory：非接触型の半導体記憶メモリー）とテープ表面に記録されているデータ［FID（Format Identification Data set）データ、EOD（End Of Data）データの位置情報など］をリンクすることで、整合性の取れた WORM テープであることを確認している。また、CM には WORM メディアであることが記録され、WORM のテープ表面にも、製造時に書き換え（リード/ライト）タイプのメディアとは異なる WORM 用の特別なサーボデータが書き込まれている。サーボデータの書き込みはメディアの製造時だけに行われるものであり、書き換えはできないので、WORM メディアが偽造されていないことを確認できる。ドライブはテープのロード時にサーボコードが WORM メディアのものと検知し、上書きを禁止する。

ドライブはテープのロード時やデータの読み書き時に上記のようなチェックを行う。こうして常に WORM の整合性を確認し、ドライブが WORM カートリッジを認識すると、上書きやデータ消去のコマンドを受け付けないようになっている。これら多階層のセキュリティーシステムを使用することで、WORM テープカートリッジとして保存されたデータの改ざん防止を保証している。

8.5. 重要データの保護に不可欠な暗号化機能

企業におけるコンプライアンスを巡っては、情報漏洩事故の多発などからバックアップの際のデータ暗号化が社会的にも強く求められるようになってきた。こうした命題に対応し、LTO-4 以降では暗号化機能をサポートしている。テープドライブ自体が暗号化機能を標準で実装し、ハードウエアベースの 256 ビットデータ暗号化機能（256-bit AES-GCM）に対応した。

これはテープドライブに暗号鍵を渡し、ドライブでデータを暗号化してカートリッジテープに書き込み、また、ドライブに暗号鍵を渡すことでデータの復号が可能となっている。暗号鍵の管理には、鍵管理の機能を持つライブラリー装置や、ライブラリー装置が暗号鍵サーバーと通信して必要な暗号鍵をドライブに渡す方法、また、バックアップソフトが鍵管理をするものもあり、利用環境に合わせて暗号化機能の運用ポリシーを設定することが可能である。ライブラリー装置が持つ鍵管理機能を使用した場合、既存のバックアップソフトウェアを変更せずにデータを暗号化できる。

LTO の暗号化機能では、ドライブがデータをテープに書き込む際に、暗号化と圧縮の処理をまとめて行なっている。このためサーバーやネットワーク上で暗号化を行う場合と異なり、比較的安価に、かつパフォーマンスを落とさず暗号化を行うことが可能である。しかも、データ圧縮後に暗号化するため、大容量データも効率よく保管することができる。以前のようにバックアップソフトウェアや専用の暗号化装置を使って暗号化を行う場合、データ圧縮やリード／ライト性能が低下するという問題があったが、LTO の暗号化機能によってこれも解消している。