該電子文書の原本性を確保し証拠性を高めることを目的として、当時刻認証局を運営する。

1.3.2　用誓　づ킏

b) 戦争、暴動、変乱、争乱、労働争議
c) 放射性物質、爆発性物質、環境汚染物質
d) 通信回線の不通
e) その付[illegible]　　争構[illegible]６物

当時刻認証局は、機密扱いとした情報を、本規定又はＴＫＣシステム

2.7 個人情報の扱い

当時刻認証局は、利用者から提供される個人情報を、本サービスを提供する為に必要な範囲内でのみこれを使用するとともに、不正な手段による個人情報の取得は行わないものとする。また、当時刻認証局は、業務上必要な期間を経過した後は、個人情報の廃棄、又はその他の処理を行う。

当時刻認証局は、個人情報への不正アクセス、個人情報の紛失、改ざん、漏洩、その他の危険に対し合理的な安全保護措置を講保護個人の取得本ス段紛保護

の監査を行う炳ｐ蠖頑ｐ繧ｽ澄

4.3.6　監査情報の保管期間

監査情報は永久保管する。

4.3.7　監査指摘事項への

講ずる。アーカイブデータのバックアップは、定期的に外部記憶媒体に取得し、適切な入退室管理が行われている室内に設置された施錠可能な場所に保管する。

4.4.4　アーカイブデータのバックアップ

アーカイブデータは、所定の方法、手順によりバックアップを行う。

4.4.5　記録へのタイムスタンプ要件

記録に時刻情報を付与するコンピュータのシステム時

秒以内に維持する。

4.8.2　タイムスタンプユニットの時刻精度

当時刻認証局は、当時刻認証局の使用する TSU の時刻精度を、NTA に対して１秒以内に維持する。

4.8.3　時刻のトレーサビリティ

当時刻認証局は、当時刻認証局が運営・管理する TSU に対する時刻監査記録を TAA から取得・保管する事により、TST の時刻の

6　技術的管理

6.1　鍵ペア生成とインストール

6.1.1　鍵ペア生成

当時刻認

6.2.6　暗号モジュールへの秘密鍵格納

TSU の秘密鍵は、暗号モジュール内で生成され格納される。

6.2.7　秘密鍵活性化方法

暗号モジュール内の秘密鍵の活性化は、複数の鍵管理者の下により所定の操作で行う。

6.2.8　秘密鍵破棄方法

暗号モジュール内の秘密鍵の破棄は、複数の鍵管理者の下により所定の操作で行う。尚、暗号モジュールを破棄目的等で室外に持ち出す場合には、複数の鍵管理者の下で所定の手続きに徑ｐ×鵙

6.