情報セキュリティ基本方針（案）

本会は、考古学や文化財、文化遺産に関する研究や教育・普及・運動などの各種の会員の活動を促進し、その問題や課題の社会化と学術化に関して、研究大会や例会を実施し、会誌や出版物の編集をおこなってきた。今後も、会員のそれぞれの活動の場として、高度情報化社会における情報資産を事故・災害・犯罪などの脅威から守り、会員と社会の信頼に応えるべく、本会の情報セキュリティ基本方針を定める。

1．考古学研究会における運営体制と情報セキュリティ基本方針の整備

本会では、情報セキュリティの維持及び改善のために必要な管理体制を整備し、必要な情報セキュリティ対策を常任委員会の正式な方針として定める。

2．法令、契約上の要求事項の遵守

本研究会の常任委員ならびに事務局員は、会活動で利用する情報資産に関連する法令等及び会員とのセキュリティ要求事項を遵守する。

3．関連諸委員・事務局員の取り組み

本会の常任委員・事務局員は、情報セキュリティの維持及び改善のために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確実なものとする。

4．違反ないし事故への対応

本会は、情報セキュリティに関わる法令等及び会員の情報セキュリティ事故への対応のための体制を整備し、違反及び事故の影響の低減に努める。

決定後は、日付・代表委員名等がはいります

行動指針(案)

Ⅰ　情報セキュリティ管理体制

１．情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ管理委員会を常任委員会に常置する。情報セキュリティ管理委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

情報セキュリティ管理委員会　責任者：代表委員

＜情報セキュリティ部門＞

システム管理	担当者：ＩＣＴ委員長
コンプライアンス	担当者：法務委員会委員長

＜インシデント対応部門＞

インシデント対応	担当者：総務委員会委員長
個人情報・苦情対応	担当者：法務委員会委員長

２．情報セキュリティ部門の取り組み

（１）情報セキュリティの点検

情報セキュリティ部門担当者(ＩＣＴ委員会委員長)は、情報セキュリティ基本方針の実施状況について 12 月に点検を行い、その結果を情報セキュリティ管理委員会責任者(代表委員)に報告する。情報セキュリティ部門では、責任者への報告とその開示に基づき、以下の点を考慮し、必要に応じて改善計画を立案する。

ア　情報セキュリティ基本方針が有効に実施されていない場合、その原因の特定と改善

イ　情報セキュリティ基本方針に定められたルールが、新たな脅威に対する対策として有効でない場合は、同方針の改訂

ウ　情報セキュリティ基本方針に定められたルールが、関連法令や取引先の情報セキュリティに対する要求を満たしていない時は、同方針の改訂

（２）情報セキュリティに関する情報共有

情報セキュリティ管理委員会責任者(代表委員)と部門担当者(ＩＣＴ委員長)は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、常任委員会で共有する。

＜専門機関＞

・独立行政法人情報処理推進機構
・JVN (Japan Vulnerability Notes)
・個人情報保護委員会

（３）IT 機器運用管理について

ア　管理体制

システム管理者は、ＩＴ基盤の運用にあたり情報セキュリティ対策を考慮し製品又はサービスを選択する。ＩＴ基盤の情報セキュリティ対策及び関連仕様は、情報セキュリティ管理委員会責任者(代表委員)及び情報セキュリティ部門担当者(ＩＣＴ委員会委員長)が承認する。

イ　ＩＴ基盤情報のセキュリティ対策

ＩＴ基盤の運用の際には以下の技術的情報セキュリティ対策を考慮する。

①サーバー機器の情報セキュリティ要件

②サーバー機器に導入するソフトウェア

③ネットワーク機器の情報セキュリティ要件

＊各要件やソフトウェアなどは、システム管理者が選定を実施し、情報セキュリティ部門担当者（ＩＣＴ委員会委員長）が承認する。

ウ　ＩＴ基盤の運用

システム管理者は、ＩＴ基盤の運用を行う際には以下を実施する。

①システム管理者は、機器の管理画面にログインするためのパスワードは初期状態のまま使わず、推測不可能なパスワードを設定して運用する。

②通信ログの保存期間は 3 年間とし、ログファイルの保存状況について、システム管理者が定期的に確認する。

③システム管理者は、管理外のインターネット接続がないか、許可なく接続された機器や無線LAN機器はないか、不審な通信が行われていないかを定期的に確認する。

④システム管理者は、脅威や攻撃に関する情報収集を行い、必要に応じて共有する。

（4）委託管理

ア　委託先評価基準と選定と評価

情報資産の処理あるいは授受を伴う業務を外部の組織に委託する場合は、委託先の情報セキュリティ管理について、下記の評価基準に基づいて評価する。

①経営者による情報セキュリティ基本方針がある

②情報セキュリティ管理責任者を置いている

③情報セキュリティ対策を定める規定等を整備している

④情報セキュリティ事故に対する対応手順がある

⑤全ての従業者に情報セキュリティに関する教育を実施している

⑥従業者から秘密保持に関わる誓約書等を取得している

⑦顧客の情報を扱う領域への入退室を管理している

⑧顧客の情報の保管について施錠管理を実施している

⑨機器・媒体の盗難防止措置を講じている

⑩媒体の無断複製、不正持出しを防止する措置を講じている

⑪媒体の移送、受け渡し時の保護措置を講じている

⑫媒体の安全な消去、廃棄の手順を整備している

⑬業務で使用するサーバー・パソコンのウィルス対策を行っている

⑭業務で使用するサーバー・パソコンは利用者認証機能を設定している

⑮業務で使用するサーバー・パソコンに利用制限等を設け管理している

以上の評価基準に準拠し、その調査結果に基づき情報セキュリティ部門担当者（ＩＣＴ委員会委員長）は委託先を選定し、情報セキュリティ管理委員会責任者（代表委員）の承認を得て、委託先を決定する。

また、委託先の評価については委託開始後、定期的に評価する機会を設ける。情報セキュリティ部門担当者（ＩＣＴ委員会委員長）は、委託先における評価基準の実施に関して不備又は変更が認められた場合は、双方協議のうえ、対処を検討し、書面で合意する。なお、その実施は以下による。

①委託先事業所に訪問して現場を観察する。
②委託先の管理責任者にインタビューする。
③委託先に書面で確認事項を通知し、実施状況について報告してもらう。

３．インシデント対応部門の取り組み

（１）対応体制

情報セキュリティインシデントが発生した際には、インシデント対応部門担当が情報セキュリティ管理委員会を招集し、下記のインシデントレベルと影響範囲を判断して対応する。

L3. 個人情報漏えい・会員への直接的影響
L2. 会事業や運営に間接的な影響が予想
L1. システム運用の不具合・トラブルなど
＊インシデントの具体例　情報漏えい・流出、データ改ざん・消失・破壊、ウィルス感染など

（２）対応手順

上記情報セキュリティインシデントレベルに応じて、下記の対応手順を講じる。

【L3 のインシデント】

①発見者は即座にインシデント対応担当者に報告する。インシデント対応担当者は情報セキュリティ管理委員会に報告し対応を協議する。
②情報セキュリティ管理委員会は原因を特定するとともに、二次被害が想定される場合には防止策を実行する。
③インシデント対応担当者は被害者/本人対応を準備する。
④インシデント対応担当者は問い合せ対応を準備する。
⑤インシデント対応担当者は影響範囲・被害の大きさによっては報道発表の準備を申請する。
⑥インシデント対応担当者は情報セキュリティ部門を総括し、サイバー攻撃等の不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に情報セキュリティ部門担当者を通じて届け出る。
⑦インシデント対応担当者は個人情報の漏えいの場合には監督官庁に届け出る。

【L2 のインシデント】

①発見者は即座にインシデント対応担当者に報告する。インシデント対応担当者は情報セキュリティ管理委員会に報告し対応を協議する。
②情報セキュリティ管理委員会はシステム管理担当者による原因特定と応急処置を指示、あわせて、法務委員会を立ち上げ、間接的影響の範囲を試算し対応を検討、情報セキュリティ管理委員長に報告する。
③インシデント対応担当者は会員に周知するとともに情報セキュリティ部門のシステム管理担当者に連絡する。
④電子データの破壊など場合はシステム管理担当者が復旧を実行する。
⑤機器の場合はシステム管理担当者が修理、復旧、交換等の手続きを行う。
⑥書類・フィルム原本の場合は情報セキュリティ部門担当者が可能な範囲で修復する。
⑦システム管理担当者は原因対策を実施する。
⑧情報セキュリティ管理委員長は影響範囲の全ての組織・人に対応結果及び対策を公表する。

【L1 のインシデント】

①発見者は発見次第、情報セキュリティ部門担当者に報告する。
②情報セキュリティ部門担当者はシステム管理担当者と原因を特定、応急処置を実行する。
③電子データの場合はシステム管理担当者がバックアップによる復旧もしくは再作成・入手を実行する。
④機器の場合はシステム管理担当者が修理、復旧、交換等の手続きを行う。

⑤書類・フィルム等の原本の場合は情報セキュリティ部門担当者が可能な範囲で修復する
⑥情報セキュリティ部門担当者は原因対策を実施し、経過を情報セキュリティ管理委員長に報告する。

Ⅱ　情報資産の管理・保護・利用

１．情報資産の管理・保護

（1）情報資産の特定とその重要度

本研究会の運営に関して必要で価値がある情報及び会員の個人情報（以下「情報資産」という）を特定し、「情報資産管理台帳」に記載する。情報資産の機密性における重要度は、以下の基準に従って評価する。

【重要度】

ア　高程度機密：法律で安全管理措置が義務付けられている情報
　　守秘義務の対象として指定されている情報
　　漏えいすると会員個人や会運営に大きな影響がある情報
イ　中程度機密：漏えいすると会運営と会事業に大きな影響がある情報
ウ　低程度機密：漏えいしても会運営と会事業に影響はないが、倫理上機密性を保持すべき情報
エ　公開：学術成果や活動成果、報告など、その他公開により益する情報

（2）情報資産の分類と表示

情報資産の重要度は以下の方法で表示する。

ア　電子データ　　保存先のサーバーのフォルダに重要度を記載
イ　書類など　　保存先キャビネット、ファイル、バインダに重要度を明示
＊以上が難しい場合も、「情報資産管理台帳」に機密性評価値を明記

（3）情報資産の管理責任者

情報資産の管理は代表委員が統括し、各項目について当該情報資産を保有する小委員会長が責任を担う。

ア　電子データ：ＩＣＴ委員会委員長
イ　会誌投稿原稿・記事テキスト：編集委員会委員長
ウ　会事業運営関連：総務委員会委員長
エ　会員個人情報：法務委員会委員長

（4）技術的安全管理措置

情報資産の適正な取り扱いのために、以下の技術的安全管理措置を講じる。

ア　アクセス制御：事務取扱担当者及び当該事務で取り扱う個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う
イ　アクセス者の識別と認証：個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証するものとする。
ウ　外部の不正アクセス等の防止：情報システムを外部からの不正アクセス又は不正ソフトウェアから保護するため、安全管理措置を講じる。
エ　情報漏えい等の防止：個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するため、安全管理措置を講じる。

（5）統合CMSへのアクセス制御と認証

ア　アクセス制御の方針

各種の情報資産を扱う情報システム又はサービスに対するアクセス制御は以下の方針に基づいて運用する。

①「情報資産管理台帳」の利用者範囲に基づき、利用者の業務・職務に応じた必要最低限のアクセス権を付与する。

②特定の情報資産へのアクセス権が、同一人物に集中することで発生し得る不正行為等を考慮し、複数名に分散してアクセス権を付与する。

イ　利用者の認証・アカウントの登録・アカウント管理およびパスワードの設定

情報資産を扱う統合CMSは、以下の方針に基づいて利用者の認証を行う。

①利用者の認証に用いるアカウントは、利用者１名につき１つを発行する。

②複数の利用者が共有するアカウントの発行を禁止する。

利用者の認証に用いるアカウントは、代表委員又は情報セキュリティ部門担当者（ＩＣＴ委員会委員長）の承認に基づき登録する。また、利用者の認証に用いるアカウントが不要になった場合、システム管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になる日の翌々日までに実施する（総会の翌々日）。

利用者の認証に用いるパスワードは、十分に強度のあるパスワードを用い、他者に知られないようにすることを条件とする。なお、本研究会の代表委員又は常任委員、会員以外の者にアカウントを発行する場合は、代表委員と情報セキュリティ部門担当者（ＩＣＴ委員会委員長）の承認と、情報セキュリティ部門コンプライアンス担当者（法務委員会委員長）のリテラシー教育の承認を得たうえで、秘密保持契約を締結しこれを実施する。

ウ　機器の識別による認証

情報資産を扱う情報システムに、ネットワーク接続によりアクセスする際の認証方式として、機器の識別による認証を用いる。

２．情報資産の利用

（1）情報資産の利用者

情報資産の利用を許可する範囲は、本会常任委員会委員ならびに事務局員とし、「情報資産管理台帳」に利用範囲欄に毎年の常任委員会名簿と担当者名簿を併記する。

（2）情報資産の研究会活動以外での利用について

情報資産を「利用者」以外の利用に供する場合は、以下を実施する。

ア　高～中程度機密各情報資産は、管理責任者からの利用の発議を常任委員会で決する。

イ　中～低程度機密各情報資産は、管理責任者の責任の下、委員会にて適宜判断する。

ウ　公開情報資産については、関連諸法に準拠し、著作権者との調整を適宜実施する。

エ　電子情報での情報のやりとりでは暗号化を前提とする。サーバーへの接続は固定IPによってのみ接続され、電子データ化された情報資産へはデジタル化対応委員会委員長が責任を有す。

（3）情報資産関連媒体の処分

高～低程度機密各情報資産の処分の場合は、以下の措置を実施する。

ア　書類・ファイルなど：細断・焼却など

イ　電子データ：媒体の破壊・焼却など　（初期化はしない）

（4）クラウドサービスや電子メールの利用

クラウドサービスについては、情報セキュリティ管理委員会責任者(代表委員)と情報セキュリティ部門担当者（ＩＣＴ委員会委員長)の許可のもとで、統合CMS内の定められたサーバー領域においてこれを実施する。なお、電子メールなどによる情報資産の移動（原稿や紙媒体のPDFなど、低程度機密の議事録など）は原則、本セキュリティーポリシーに違反するものであり、漏えいについては、発信者および受信者ともにその責任をおう。

３．個人情報の管理・利用

（1）本情報セキュリティ基本方針の定める個人情報とは

本研究会会員で、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述、記号その他の符号により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別できることとなるものを含む。）をいう。

ア　会員登録情報
イ　会員IDおよびパスワード
ウ　会員の表示名（SNSなどで表示される個人が特定される記号）
エ　個人情報データベース＊

＊個人情報を含む情報の集合物であって、特定の個人情報について電子計算機を用いて検索することができるように体系的に構成したもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして「個人情報の保護に関する法律施行令」(平成15年政令第507号。以下「個人情報保護法施行令」という。）で定めるもの。

（2）個人情報利用の特定とその通知

個人情報を利用できる事務の範囲は、会誌の発送、会費納入の通知、会費納入状況確認など会事業の運営事務に限定するものとし、利用に当たっては、具体的な利用目的を特定した上で、利用するものとする。また、特定した利用目的を超えて利用する必要が生じた場合には、当初の利用目的と相当の関連性を有すると合理的に認められる範囲内で利用目的を変更して、本人に通知を行い、変更後の利用目的の範囲内で利用するものとする。

本人との間で約款や契約などを締結することで、あらかじめ、本人に対し、その利用目的を明示することで、会事業の運営事務以外への利用も妨げない（例えば、研究分野の開示や、交流に関する会事業とは別の事業への賛助的役割の場合など)。また、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。この場合、情報セキュリティ管理委員会責任者の責任の下で利用することができる。

（3）個人情報の開示、訂正等、利用停止等

本人から、当該本人が識別される個人情報等に係る保有個人データについて、書面又は口頭により、その開示（当該本人が識別される個人情報等に係る保有個人データを保有していないときにその旨を知らせることを含む。以下同じ。）の申出があったときは、身分証明書等により本人であることを確認のうえ、開示をするものとする。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

ア　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
イ　本研究会の事業の適正な実施に著しい支障を及ぼすおそれがある場合
ウ　他の法令に違反することとなる場合

なお、開示は、書面により行うものとする。ただし、開示の申出をした者の同意があるときは、書面以外の方法により開示をすることができる。

訂正は、本人から、当該本人が識別される個人情報等に係る保有個人データの内容が事実でないという理由によって当該個人情報等に係る保有個人データの内容の訂正、追加又は削除（以下「訂正等」という。）を求められた場合には、その内容の訂正等に関して他の法令の規定により特別の手続が定められている場合を除き、利用目的の達

成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該個人情報等に係る保有個人データの内容の訂正等を行うものとする。

利用停止は、本人から、当該本人が識別される個人情報等に係る保有個人データが「利用目的外の利用」によって取り扱われているという理由又はその「取得」の方法が不正に行われて取得されたものであるという理由によって、当該個人情報等に係る保有個人データの利用の停止又は消去を求められた場合、又は「個人情報の提供」の内容に違反して第三者に提供されているという理由によって、当該個人情報等に係る保有個人データの第三者への提供の停止を求められた場合で、その求めに理由があることが判明したときは、遅滞なく、当該個人情報等に係る保有個人データの利用停止等又は第三者提供の停止を行うものとする。ただし、利用停止等又は第三者提供の停止を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

（4）個人情報の正確性の確保とその削除・廃棄

個人情報利用により特定された利用目的の達成に必要な範囲内において、特定個人情報等を正確かつ最新の内容に保つよう努めるものとする。また、関係事務を処理する必要がなくなった場合で、かつ、所管法令において定められている保存期間を経過した場合には、個人情報をできるだけ速やかに廃棄又は削除するものとする。ただし、その個人情報を復元できない程度にマスキング又は削除した場合には、保管を継続することができるものとする。

（5）個人情報に関する取り扱い責任者および苦情対応

取り扱いの責任は、本情報セキュリティ管理委員会の責任者に準じる。また苦情対応もインシデント対応部門において対応する。

（6）取り扱い状況を確認する手段の整備

取り扱いについては、その運用状況を確認するため、以下の項目をシステムログ又は利用実績として記録する。

ア　特定個人情報ファイルの利用・出力状況の記録
イ　書類・媒体等の持出しの記録
ウ　個人情報ファイルの削除・廃棄記録
エ　削除・廃棄を委託した場合、これを証明する記録等
オ　個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録

（7）　情報漏えいに関する事案に対応する体制の整備

情報漏えい等の事案の発生又は兆候を把握した場合には、事務取扱責任者は「情報セキュリティ基本方針」に定める安全管理措置に従って対応を行う。

Ⅲ　基本方針の変更

本基本方針は、考古学研究会常任委員会の議を経て改訂されるものとする。

学術リポジトリの運用指針（案）

考古学研究会の会活動における知的生産物(会誌掲載論文・記事・例会発表・会の催事など)は、本会の会員の貴重な財産として、同時にその社会的責務としてその公開により知が社会に共有され、活用されることが、今後の考古学研究会と考古学・文化財学のために重要である。

「私たちの考古学」として会誌を発行して以来、本会の社会的責務は、常に考古学の社会化による知の共有であった。現在のＩＴ技術の進展は、これらインターネットを通じて可能とし、国際的にも、国内的にもより広い社会の知の拡散を可能としている。現在、その主要な方式として、機関学術リポジトリによって研究や活動成果のオープンアクセスを目指す方向性が一般化しつつあるなかで、考古学研究会も会活動の一環として、その整備を進める。機関学術リポジトリを新たにその手段として位置づけ、整備・充実を図ることは、社会的要請にしっかりとこたえるべく本会の姿勢を明確に示す会活動ともなる。

１．学術リポジトリの意義

考古学研究会がオープンアクセスの学術リポジトリを構築する意義は、以下のようにまとめられる。

（1）会活動の主体である研究活動の社会に対する説明責任の履行
（2）研究・運動団体としてのブランド力や情報発信力の向上
（3）学術研究成果や運動や活動成果の永続的・効率的な蓄積
（4）活動の社会化による問題意識の共有や新たな視点での研究の発展
（5）学術情報公開に関する管理コスト全体の軽減
（6）膨大な比較・蓄積データのマイニングによる新しい研究・活動・運動の発展
（7）考古学に関する社会的関心や社会的意義の普及・啓発の推進
（8）研究会の知名度や認知度の向上とそれに伴う会活動の拡大
（9）地域社会における会の学術研究のフィードバックと蓄積
（１０）地域の活動や運動の成果や社会的影響に関する外部評価
（１１）活動記事の社会化による価値観の共有や知の深化
（１２）多くの研究を参照できることによる地域の新しい知の創造
（１３）被論文引用率の飛躍的な向上
（１４）学術論文の引用に関する剽窃や盗作などリテラシー違反に対する明確な根拠
（１５）関連学術分野の網羅的な検索と比較・検討の実施

２． 学術リポジトリの趣旨

考古学研究会学術リポジトリは、本会の会活動や会誌に反映された会員の知的生産物を収集し、その社会化と将来における蓄積・保存を目的に、それを電子的なデータ形式により、無償で発信・提供することにより、本会の学術研究の発展にすするとともに、広く社会に対する貢献を果たそうとするものである。

３．学術リポジトリの公開

考古学研究会学術リポジトリの公開は、本会会員向けには該当著作物刊行後すみやかに、会員以外には刊行２～３年後（検討中）に行う。

４．リポジトリに登録される資料

考古学研究会学術リポジトリは、考古学研究会の会活動や開始に反映された会員の知的生産物のうち、次の各項目のいずれかに該当するものを登録の対象とする。

（1）会員によって会活動と関連して生産された論文や記事等の、学術的・社会的意義のあるもの

（2）会員によって会活動と関連して生産された発言や録音・映像・写真等の、学術的・社会的意義のあるもの

（3）かつて会員であった者の（1）および（2）に関連するもの

（4）（1）・（2）・（3）いずれもが著作権(関連諸)法の申し合わせの中で、本会と著作権者の間で合意が文書により形成されたもの

５．登録と著作権およびその他権利者との関係

考古学研究会学術リポジトリで公開しようとする会員ならびにかつての会員(以下：登録資料対象者)のみに著作権および各種情報公開に関する権利が帰属しない場合は、以下のとおりとする。

（1）著作権が登録者を含め複数の者に帰属する場合は、登録資料対象者は法務委員会に対し、リポジトリ登録について、他の著作権者の許諾が得られていることを文書で通知し、法務委員会はこれを精査し確認する。

（2）著作権が登録資料対象者以外の個人や団体に帰属しているとき、登録資料対象者は法務委員会に対し、リポジトリ登録について、著作権者の許諾が得られていることを文書で通知する。著作権者があらかじめ許諾の方針を社会的に明らかにしている場合はその限りではない。

（3）登録資料対象者が登録しようとする内容の公開が登録資料対象者本人以外の肖像権あるいはその他の情報に関する権利と抵触すると想定される場合は、登録資料対象者は法務委員会に対し、リポジトリ登録について、各種情報公開に関する権利の許諾が得られていることを文書で通知し、法務委員会はこれを精査し確認する。

（4）登録資料対象者の著作権は、公開によって、考古学研究会に移転しない。リポジトリ登録後も、著作権者のもとに留保される。

（5）考古学研究会は、先の著作権関連事項をリポジトリに明記し、利用者に著作権(関連諸)法の遵守を求めるとともに、当該の複製物や二次使用が出来るだけ制限される技術的対応を行う。

（6）登録資料対象者の登録しようとする内容の公開が、肖像権など各種情報公開に関する権利に抵触する可能性がある場合は、法務委員会の下で精査の上、公開に制限を行う。

６．登録された資料の抹消

以下の場合、登録された資料を抹消する場合がある。抹消は、法務委員会の法奥により常任委員会で決定する。

（1）法務委員会の精査により、著作権あるいは各種情報公開に関する権利に関し、登録資料対象者から提出された文書に疑義が生じた場合。

（2）登録資料対象者から削除の申請があった場合。

（3）登録資料が、著しく社会的に不適切と法務委員会によって判断される場合。

（4）公開された登録資料により特定の個人や団体に直接的な社会的影響が及ぶ状況が生じ、客観的にこれが観察された場合。

（5）登録資料が、公序良俗や各種法令に違反する場合、また、特定の個人や団体に言及することで間接的な影響が想定されることが法務委員会によって判断される場合。

７．本指針の変更について

本指針は、法務委員会の発議により考古学研究会常任委員会の議を経て改訂されるものとする。