一般社団法人粉体粉末冶金協会

情 報 セ キ ュ リ テ ィ 対 策 基 準

この情報セキュリティ対策基準は，一般社団法人粉体粉末冶金協会（以下「当会」という.）が定めた情報セキュリティポリシーに基づき，当会の情報セキュリティ確保のために実施すべき対策基準を定めたものである.

1. 組織・体制

当会の情報セキュリティ対策に係る役割，権限及び責任を次のとおり定める.

（1）情報セキュリティ総括責任者

情報セキュリティ総括責任者を置き，代表理事たる会長がその任にあたる．情報セキュリティ総括責任者は，情報セキュリティに関するすべての責任及び最終決定権限を有し，情報セキュリティに関する事項を総括し，必要な指示・指導を行う.

（2）総務委員会

当会の情報セキュリティに関する事項は，総務委員会が所管するものとする．情報セキュリティポリシーに基づき，情報セキュリティ対策基準等重要事項を定めるとともに，情報セキュリティ対策基準に関する評価・見直し等を行う.

（3）情報セキュリティ責任者

情報セキュリティ責任者を置き，常務理事または事務局長をもって充てる．情報セキュリティ責任者は，総務委員会での審議・決定，情報セキュリティ総括責任者の指示等に基づき，当会内において情報セキュリティ対策に係る指示・指導を行う責任と権限を有する.

（4）情報資産管理担当者

情報資産を作成又は入手した職員等（派遣職員，委託業者，共同開催機関を含む）は，情報資産管理担当者として，当該情報資産をポリシーに基づき適正に管理する.

2. 情報セキュリティ侵害の阻止

当会は，当会の情報資産への情報セキュリティ侵害を阻止するため，必要な措置をとることができる.

（1）不正アクセス等への対応

当会の情報資産への不正アクセスが認められた場合，当会は，所定の手続きに基づいて，当該対象者，当該情報機器またはそれを接続するネットワークに対し，事態を警告し，対策をとるよう勧告し，さらには，定常的な利用を停止するなどの抑止措置をとることができる.

（2）アクセス制限

当会は，情報の内容に応じて，アクセス可能な利用者を定め，不正なアクセスを阻止するべく必要なアクセス制限を行うことができる．利用者は，アクセス権限のない情報にアクセスしたり，許可されていない情報を利用したりしてはならない.

3. 当会内外の情報セキュリティを侵害する行為の抑止

当会の内外を問わず，あらゆる研究・教育機関，企業，組織，団体，個人等の情報資産を侵害してはならない．また，情報セキュリティに関連する諸法規，条約ならびに当会が定める規程等を遵守しなければならない.

4. 情報資産の分類と管理

当会の提供する情報に関しては，それが果たす役割と影響を十分認識し，常にその情報の正確性と健全性に配慮しなければならない．また，情報提供の際には，関連する諸法規，条約ならびに当会が定める規程等を遵守しなければならない．

（1）情報資産の管理者

当会の管理する情報資産は，総務委員会が管理しなければならない．当会の管理するシステムおよびネットワークは，総務委員会が認めた情報セキュリティ責任者が管理しなければならない．当会の管理するシステムおよびネットワークに個人および自主管理ドメインの機器を接続した場合，当該機器内の情報は，その機器および自主管理ドメインのシステム管理者と利用者が管理しなければならない．

（2）非公開情報資産

個人情報，事務，研究・教育等の非公開情報を不当に利用してはならない．情報は適切に管理されなければならず，権限のない情報に対してアクセスを行ったり利用したりしてはならない．情報の盗難・漏洩等を防止するため，非公開情報を扱うネットワークは，暗号化や盗聴防止策を講じるよう配慮する．また，情報が記録された媒体は，適切に管理されなければならない．

（3）限定公開情報資産

特定の利用者に特定の情報を公開する場合，その情報の登録・閲覧は，許可された者が許可された操作だけを行えるように，認証，アクセス制御等を実施しなければならない．非公開情報を扱う場合と同じく，ネットワークは，暗号化や盗聴防止策を講じるよう配慮する．さらに，異常な登録，閲覧および操作が行われていないか，定期的に調査・確認しなければならない．

（4）公開情報資産

あらゆる公開情報を不当に利用してはならない．情報は改竄，破壊されないように適切に管理されなければならない．また，非公開情報を公開する場合には，個人情報の漏洩，プライバシーや著作権の侵害に十分注意し，公開できる情報だけを抽出し，公開してよい形に加工しなければならない．情報が記録された媒体は，適切に管理されなければならない．

（5）情報機器および記憶媒体の処分

非公開・限定公開・公開を問わず，情報機器および記憶媒体を破棄する場合は，その処分方法に注意しなければならない．

5. 情報セキュリティならびにポリシーの評価と更新

（1）情報セキュリティの評価と更新

当会の情報資産を守るために，常に最新の情報を取得し，適切な物理的・技術的・人的セキュリティが実施されているか定期的に評価・調査を実施しなければならない．改善が必要と認められた場合は，速やかに情報セキュリティの更新を行わなければならない．

（2）ポリシーの評価と更新

情報セキュリティの調査とともに，ポリシーの実効性を定期的に評価し，改善が必要と認められた場合には，変更内容および実施時期の決定を行い，高いセキュリティレベルを持ち，かつ遵守可能なポリシーに更新しなければならない．

一般社団法人　粉体粉末冶金協会

（2022 年 12 月 22 日　理事会承認）