電子化情報取扱基準

2021 年 10 月

IT-Professor IT 部

更新履歴

	更新日	更新箇所	更新内容
1	2021/10	初版	

1. 趣旨・目的

この実施基準は、IT-Professor（以下、IT-Pと称す）グループ情報セキュリティポリシー第3 章(第10、11 条)の規定に基づき、電子化情報の生成から利用・保存・廃棄の過程における、機密性に応じた管理について、必要な基準を定めたものである。

2. 定義

本基準で用いる主な用語の定義は、以下のとおりとする。

1) 電子化情報

IT-P グループ情報セキュリティポリシーに規定する情報資産のうち、情報に該当するものをいう。電子化されたデータ、音声、画像等とし、伝達・保存手段としての媒介・媒体の如何を問わない。

3. 対象

1) 対象となる情報資産

・ 電子化情報

・ 電子化情報を保存した機器(PC、サーバー等)および外部媒体

4. 役割

次のとおり役割を定義する。

1) 電子化情報取扱責任者

・ 情報の漏洩または改ざん等から保護するため、自部門の電子化情報について従業員等が適切に取り扱えるよう管理する責任を負う。

2) 従業員等

・ 本基準および自部門の電子化情報の管理策に基づき、情報資産を取り扱う。

5. 電子化情報の機密区分

1) 電子化情報の機密区分

情報は、次に掲げる機密区分のとおり分類すること。

i「極秘」

秘密保全の必要性が特に高く、漏洩することにより、株主や顧客など外部利害関係者を巻き込み、企業活動に重大な損害を与えるおそれがある情報とする。

ii「秘」

秘密保全の必要性があり、漏洩することにより、企業活動に影響を与えるおそれがある情報とする。

iii「社外秘」

「極秘」、「秘」以外の情報で、情報開示規程に基づき開示している情報以外の情報とする。営業秘密、個人情報、プライバシー情報等、法令や社内の特別な定めに従い取り扱わなければならない情報は、本基準に加えて当該の法令・規程に従うこと。

2) 情報の分類

電子化情報取扱責任者は、本基準で定める機密区分に従い、情報を分類し、自部門の情報について従業員等が識別できるよう管理しなければならない。

なお、情報の分類は、適宜見直されなければならない。

3) 情報利用範囲の明確化

i「極秘」情報は、電子化情報取扱責任者によって、情報を取り扱う個人およびその所在が正確に把握されなければならない。

ii「秘」情報は、電子化情報取扱責任者によって、情報を取り扱う組織が把握されなければならない。

iii「社外秘」情報は、不用意な扱いがもたらすリスクから保護するため、業務上の必要性に応じて、適切な利用範囲を指定すること。

6. 情報の取り扱いに関する遵守事項

情報を漏洩または改ざん等の不正行為から保護し、適切に取り扱うため、本基準で定めた事項を遵守しなければならない。

1) 情報の取得、生成

i「極秘」、「秘」および「社外秘」情報には、次の方法等により機密区分と利用範囲を明記しなければならない。

- PC 等で取り扱う場合は、情報を表示する際に画面上で視認可能とする。
- 情報を印刷する場合には、印刷物に表示する。

・ 外部媒体に情報を保存する場合には、媒体上に印刷または貼付する。

ii 機密区分の異なる情報を組み合わせて新たな情報を生成する場合には、原則機密性が高い方の機密区分とすること。

iii 情報を取得した場合には、機密区分、利用範囲および取り扱い方法について、入手元と合意すること。

2) 情報の保管

「極秘」および「秘」情報は、安全性を確保のうえ、保管しなければならない。

・ コンピューターに保存する場合には、安全対策が施されたサーバーに保存し、利用範囲を限定すること。PC への保存は原則禁止とする。
・ 外部媒体に保存する場合には、外部媒体を施錠可能な保管庫に保管すること。必要に応じ、情報を暗号化すること。

3) バックアップ

i 原本の完全性を保つために、適宜バックアップを取得すること。

ii バックアップは、原本の機密区分に従い取り扱わなければならない。

4) 複製

i 情報の複製は必要最小限に留めること。特に、「極秘」および「秘」情報の複製は、電子化情報取扱責任者の許可がある場合に限る。

ii 複製された情報は、原本の機密区分に従い取り扱わなければならない。

5) 情報の持ち出し、送信

i 「極秘」および「秘」情報の持ち出しおよび送信は、電子化情報取扱責任者の許可がある場合に限る。

ii ネットワークにて「極秘」および「秘」情報を送信する場合には、情報の漏洩、改ざんからの保護策を講じなければならない。必要に応じ、次の対策を実施すること。

・ 情報の暗号化
・ 通信経路の暗号化

・ 情報への電子署名の付与

なお、電子メールによる「極秘」および「秘」情報の送信は、原則禁止とする。

6) 情報の消去

保管期間が経過した場合等、不要になった情報は速やかに消去しなければならない。特に、「極秘」および「秘」情報は、情報の復元性を排除するため、以下の手段に拠らなければならない。

・ 消去ツール等を利用し、情報が復元できないよう完全に消去すること。

・ 外部媒体等で、消去ツールが利用できない場合には、媒体を破壊する、傷付ける等の処置により、情報を読み取れないようにすること。

7) 情報取扱状況の記録、点検

i 「極秘」および「秘」情報を取り扱う従業員等は、当該情報の取り扱い行為を記録しなければならない。

ii 「極秘」および「秘」情報の電子化情報取扱責任者は、当該情報の漏洩、盗難、改ざん、破壊等を検知するため取り扱い状況を点検すること。

7. 従業員等の注意義務

従業員等は、日常の業務において、情報を漏洩および改ざん等不正行為から保護しなければならない。

1) 電子化情報の特性

電子化情報は、瞬時に流通でき、一度に大量の情報を扱え、改ざんおよび複製等を容易に行うことができる特性を持っており、慎重に取り扱う必要がある。

2) 情報の利用

従業員等は、電子化情報を利用する際に、情報を保護するための措置を講じなければならない。

・ PC から離れる場合には、電源の切断、ログオフまたはスクリーンセーバーのパスワードロック機能等により、他者の不正利用を防止すること。

・ 外部媒体の利用が終了した場合には、机上およびPC のドライブ内等に放置せずに、所定の場所に保管すること。

・ 情報を印刷した場合には、印刷物をプリンターに放置せず、速やかに回収すること。

3) 電子メールの取り扱い

従業員等は、電子メールを利用する際に、情報を保護するための措置を講じなければならない。

・ 電子メールの送信にあたっては、送信先のメールアドレスに間違いが無いか確認のうえ、送信しなければならない。
・ 電子メールによる情報の送信は、全ての送信先に対して情報の複製が送信されるとともに、送信元のメールデータに送信済みの情報が保存されることに留意すること。
・ 電子メールの自動送信機能(自動返信、自動転送等を含む)は、従業員等が情報の機密性に応じた扱いができない状態で送信されるおそれがあるため、原則使用禁止とする。
・ 重要機密情報を含む資料をファイル化して外部にメールで送信する場合には、必ずファイルを暗号化（パスワードをかける）すること。暗号化を解くパスワードは、ファイルを添付したメールには記載せずに、必ず別メールで送信しなければならない。

8. 例外事項

法令または別途定められた規程等により特別の定めがある場合は、責任体制に基づき適切に判断し処理しなければならない。

9. 公開の範囲

本基準は、「社外秘」とし、IT-Pグループの従業員等を対象に公開する。

10. 改廃

本基準は、定期的に見直しを行うこととし、IT部にて適宜改定を行うこととする。
また、改定が必要と判断された場合は、速やかに変更を行い、責任体制(情報セキュリティ管理体制)を通じ、その内容をすべての従業員等に周知することとする。

附則

本基準は、2018年10月1日より適用開始とする。