IT-Professor
アクセス権限管理基準

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 4 章(第12、13 条)の規定に基づき、IT-P グループの情報資産を適切に取り扱うためのアクセス権限管理について、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) アカウント

PC や情報システムなどネットワーク上の情報や機能を利用するために、従業員等個人に対し与えられた権利。

2) アクセス権限

情報システムなどネットワーク上の情報や業務アプリケーション等機能に対する、「参照・更新・実行」などの許可や制限。

3) 特権

情報システムの停止や設定変更など管理者に付与される権限や、特定用途で限定的に付与される権限など、通常または標準設定では許可されない特別な権限。

３．対象

1) 対象となる情報資産

・ 電子化情報

・ 情報システム(業務アプリケーション、データベース、ファイルサーバー、電子メール等)

４．役割

次のとおり、主な役割を定義する。

1) アクセス権限設定責任者

・ 情報資産を不正な取り扱いから保護するため、情報資産に対するアクセス権限の設定および従業員等へのアカウントの付与を適切に行い、管理する責任を負う。

・ アクセス権限の妥当性を定期的に点検し、適宜権限の設定または変更を行う。

2) 従業員等

・ 付与されたアカウントが第三者に盗用または使用されないよう、慎重に取り扱う責任を負う。

・ 自身に付与された権限の範囲を逸脱することなく、適切に情報資産を取り扱う義務がある。

5．遵守事項

情報資産を不正な取り扱いから保護し活用するため、情報資産およびこれを取り扱う従業員等に対して、本基準で定めた内容に基づきアクセス権限を適切に設定し管理しなければならない。

1) 従業員認証

IT-P グループネットワークへの参加にあたっては、あらかじめ IT-P グループの従業員等としての実在性および本人性が確認されなければならない。

2) アクセス権限の管理

i アクセス権限の設定

・ アクセス権限は、情報の機密性、情報システムの重要性に応じてあらかじめ設定されなければならない。

・ アクセス権限の設定にあたっては、「参照」、「作成・追加・更新・削除」、「実行」の権限を単独または組合せ、必要な範囲内に限定されるよう設定しなければならない。

・ 設定したアクセス権限は適宜見直しを行い、適切に権限の設定を変更しなければならない。

ii アカウントの付与

・ アカウントの付与は、予め定めた申請手続きに従い、実施しなければならない。

・ アカウントは従業員等の役割に応じ、適切に付与しなければならない。

・ アカウントの付与は個人単位とし、共有は原則禁止とする。

・ アカウントの付与状態を定期的に確認し、正確かつ最新状態を維持しなければならない。

・ 人事異動や業務分担の変更があった場合は、速やかにアカウントを変更しなければならない。また、不要となったアカウントは、速やかに削除・停止しなければならない。

・ アカウントの付与等に関する内容は、台帳等により記録し、不正使用から保護するため、安全に管理しなければならない。

iii 特権の管理

・ 特権アカウントは、一般アカウントと区別され、特権の割り当てや使用制限を行うなど、より厳密に管理しなければならない。

・ 特権アカウントを付与する場合、許可される者は限定・特定され、行使できる権限は必要最小限に制限しなければならない。また、取り扱う情報や情報システム等の対象、使用可能な有効期間についても必要最小限としなければならない。

・ 特権アカウントを付与した者のリストを作成し、利用状況を記録し適宜点検を行わなければならない。

・ ソフトウェア製品にあらかじめ組み込まれたアカウントの使用は原則禁止する。

3) アクセス履歴の管理

ⅰ 履歴の記録

非権限者による情報資産への不正なアクセスを検知するため、情報システム等対象を定め、アクセス履歴を記録しなければならない。

また、情報資産の機密性、重要性に応じて、アクセス内容についても記録しなければならない。

・ アカウント単位に、情報システムや各種資源ファイルなどへのアクセス履歴を記録すること。

・ 特権アカウントによるアクセス履歴は、ログインとログオフ時間、設定変更等実行内容、アクセスの成功および失敗等の内容について記録すること。

ⅱ 履歴の保存

・ アクセス履歴は、期限を定め、一定期間保存しなければならない。

・ アクセス履歴は、機密性に応じて漏洩、改ざん、破壊等を防ぐための措置を講じなければならない。

4) 従業員等によるアカウントの保護

・ 付与されたアカウントを他人に通知あるいは利用させてはならない。

・ アカウントの内容をメモし、不用意に身の回りに置くことや、他人に口外してはならない。

・ 他人が容易に推測可能なパスワードを使用してはならない。

・ パスワードは定期的に更新すること。

6．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には、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。

7．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。

8．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、2021 年 10 月 1 日より適用開始とする。