「管理者権限の管理策の検討 中小企業における現状を踏まえて-」

A study of the management measures on the administrator rights " focus on the present conditions at the small and medium-sized enterprises "

情報セキュリティ大学院大学
丹木就之

概要：　管理者権限は,システムの稼働環境を設定かつ変更し，システムを安定させ，変更をコントロールする目的で使われる．しかし，管理者権限は使用上で幾つかの問題を起こす可能性がある.管理者権限の管理不備は、例えば内部からの不正アクセスや情報持ち出しなど，情報漏えいやデータ改ざん，システム停止など事故を起こすリスクがある．その原因は，担当者の技量の未熟や管理者不在時のルール不備など，運用管理上の問題である．今回，原田研究室情報セキュリティアンケート調査から管理者権限の運用面に関する現状を把握し，組織規模や業界から比較した管理者権限の重要視する管理方法の特徴に関して考察をした

管理者権限とは

情報ネットワークシステムには（サーバー,メール,インターネット,LAN）など様々な種類が存在する。これらは、それぞれ対応する管理者の設置と管理者権限の使用がある。管理者権限は、代表的なものとして、Windowsではadministrator権限、MacやUnixなどはroot権限と呼ばれている。

管理者権限の使用による利点として

システムの稼働環境を定義し、かつ変更する場合、制御の機能となる

情報システムにおける管理者権限は、一般従業員の不正な使用の防止やウイルス対策の一部として可能である

止が可能である

しかし、運用面において課題が存在する、それは

度に留め、安全性の向上を考えると管理を厳密にする必要性が生じ管理工数が増大する

例：職務分掌の問題等（開発と運用・申請データ投入と承認が同一のIDや人材）

管理者権限の運用においては

想定される不正利用のリスクと運用のバランスを考えた管理が必要である

ISO/IEC 27002 9.2.3特権的アクセス権の実施の手引

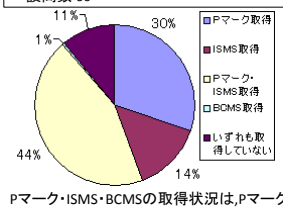
質問：管理者権限（特権ID）に関して重視している施策
これは、SO/IEC 27002 9.2.3特権的アクセス権の実施の手引き詳細な管理事項8項目を基本とし「情報システムの管理者権限（特権ID）の運用に関して組織の属性（企業規模や保持するIAMSやPマークなどの認証等）によって重要視する特徴があるのではいか」と考え、調査結果から「資格を取得していない企業にも応用できる」と想定した。

1.**「使用者の限定」**使用者を必要な人のみに限定している
2.**「使用者の権限最小限化」**使用する権限を要求事項に基づいて最小限に限定している
3.**「承認プロセスの記録・許可」**承認プロセスを記録し,承認されるまで使用を許可しない
4.**「退職など不要IDの対策」**特権業務のアサインが外れた時の手続きを定めている（異動・退職等）
5.**「IDの使い分け」**管理者権限（特権ID）と通常業務で使用するIDを分けている
6.**「力量のレビュー」**管理者権限（特権ID）使用者に関して、力量をレビューしている
7.**「使用手順の制定」** システムの構成管理機能に応じて,管理者権限（特権ID）の使用手順を定めて運用している
8.**「共有パスワードの管理方法の制定」** 管理者権限（特権ID）を共有している場合は、秘密認証情報（パスワード等）の管理方法を定めている
9.**「その他」**・10.**「無回答」**

出典：北原幸彦・竹田栄作・中野初美・山下真・原田要之助 ISO/IISE27002情報セキュリティ管理策の実践のための規範　日本規格協会出版

原田研究室アンケート調査

日本国内のプライバシーマーク取得企業、ISMS認証取得企業、官公庁、教育機関などからランダムに選んだ4,500の情報セキュリティシステム担当者を対象とした情報セキュリティ調査
・実施期間　2015年7月から8月
・回答数352
・調査方法　郵送によるアンケートの送付
・設問数 60



Pマーク・ISMS・BCMSの取得状況は,Pマークが30%,ISMSが14%,ISMSとPマークの両方取得が44%,いずれも取得していない11%であった.

図1.Pマーク,ISMS,BCMSの取得状況(n=352)

基本データの調査結果

業種別の判断では,「情報通信業」（通信業,放送業,情報サービス業,ソフトウェア業,インターネット附随サービス業,映像・音声・文字情報制作業を含む）が47%と最も多く次いで「大学」が19%,サービス業が9%であった.

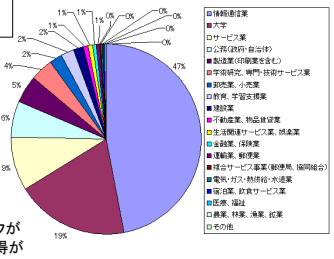
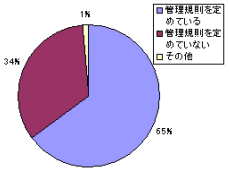


図2.業種に関して(n=352)

管理規則の制定に関して

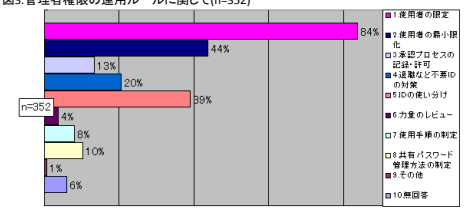
「管理規則を定めている」が65%と「管理規則を定めていない」が34%であり管理者権限の運用には不正利用のリスクが存在していること証明する.



管理者権限（特権ID）の運用ルールに関して

管理者権限（特権ID）の運用において重視している施策の調査では、回答数の多かった項目は,1.「使用者の限定」84%(295件)と2.「使用者の最小限化」44%(154件),次いで5.「IDの使い分け」39%(137件)であった.

図3.管理者権限の運用ルールに関して(n=352)



また,回答数の少ない結果として6.「力量のレビュー」4%(13件),7.「使用手順の制定」8%(28件),8.「共有パスワードの管理方法の制定」10%(36件)と3.「承認プロセスの記録・許可」13%(47件)の順であった.

図4.管理者権限に関して重視している施策(n=352)

研究結果（一例）

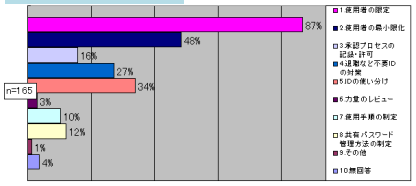


図5.管理者権限に関して重視している施策/情報通信業(n=165)

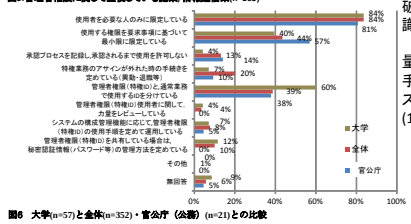


図6　大学(n=57)と全体(n=352)・官公庁（公務）(n=21)との比較

情報通信業（通信業,放送業,情報サービス業,ソフトウェア業,インターネット附随サービス業,映像・音声・文字情報制作業を含む）に関して

情報通信業は,1.「使用者の限定」(87%)と2.「使用者の最小限化」(48%)の回答が多く,本来アクセス権のない従業員による重要情報の閲覧や意図的な情報システムへのシステム破壊と言ったリスク対策に意識が強い事が分かった.
　少なかった回答として6.「力量のレビュー」(3%)や7.「使用手順の制定」(10%)8.「共有パスワードの管理方法の制定」(12%)であった..

課題の解決案

リスクの把握，経営への影響を考えることが不可欠である．経営トップから一般社員，協力会社に至るまで，リスク認識を共有する環境の構築が必要！

Need to your advice

- **管理者権限を使用することにより、どのような利点があるか？また、想定される不正使用リスクとは？（問題点など）**
- **管理策1-8でどれが一般的には重要視すると思われるか、逆にどれが軽視するのか**
- **9「その他」とはどのようなものが考えれるか**
- **無回答に関してどのような理由が考えられるか**
- **管理策を徹底できない環境はどのように運営（管理）をすべきなのか（不正使用の防止策・現状など）**
- **研究へ向けたアイデア・ガイドライン・参考書・文献など**