Vol.2015-SPT-16 No.8
Vol.2015-EIP-70 No.8
2015/11/20

管理策の実施状況から見る特権ID（管理者権限）の現状と課題

丹木就之[†1]　原田要之助[†1]

概要：情報システムにおいて管理者権限（特権 ID）は，重要な機能である．管理者権限の使用は，システムの稼働環境を定義し，かつ変更を制御し，設定の整合性を保つことが可能になる．しかし，管理者権限は，組織において便利な反面，取り扱いには注意を払い管理をしなければならない．それは，悪意を持って管理者権限を使用した場合，内部不正への手段になる．今回，管理者権限の運用に関して，先行する報告書やガイドラインから不正使用のリスクとその背景，一般的な防止策の整理を行った．また，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調査をした．

キーワード：情報システム，管理者権限，特権的アクセス，不正使用，管理策

A study of the current status and issues of the privileges ID at the view from management measure

NARIYUKI TANGI [†1]　YOUNOSUKE HARADA[†1]

Abstract: The administrator right (special privilege ID) is an important function of the information system. The use of the administrator rights defines the operation environment of the system and keeps consistency and can be controlled the system changes. However, it is convenient means. On the other hand, the organization must pay more attention to the handling and manage the use of administrator rights. With the malice use of administrator rights, it may cause internal miss use of IT system. I have studied about risks of the unauthorized use of information systems, and its background and general preventive measures from preceding reports and guidelines focusing on the use of the administrator rights. In addition, I grasped the present conditions about the operative aspect of the administrator rights from Harada laboratory's information security questionnaire survey and investigated with respect to features on the importance on the operation of administrator right which judged from the situation of organization scale and trade.

Keywords: Information system, Administrator right, Internal miss, Operation of administrator right

1. はじめに

総務省の通信動向調査では[1],平成 25 年度の雇用規模 100 人以上の企業においてインターネット普及率は 99.9%.クラウドサービスの利用は,平成 24 年度 28.2%,平成 25 年度には 33.1%までに拡大している.資本金の規模が 50 億円以上の大企業について見ると,50%以上クラウドを使用している.現在,わが国におけるほぼ全ての企業が情報システムを利用していると判断できる.情報システムは,パソコンやスマートフォンを代表として,それに関連する情報ネットワークシステム（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.それらに対応して管理者が設置され管理者権限の使用がされている.これらの権限がないと十部に管理できないので重要となる.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.これらの管理者権限は,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．しかし,情報システムにおける管理者権限は,重要な機能であるが運用には細心の注意を払う必要がある.それは,悪意を持って使用した場合,内部不正につながる.また,システム管理者は,様々な情報システムの変更権限を保有している場合もあり,不正行為を働くと,情報漏えいやシステム停止などの重大な問題を引き起こし兼ねない．すなわち,管理者権限の悪用は,システムの停止や混乱などビジネスに致命的な損害を与えることで,社会的信用の失墜で企業価値を大きく下げることに繋がる.

ウイルスなど外部からの攻撃に対しては,防御体制を万全に行っているが,内部犯行者からの攻撃は十分な対策が備えられていないケースも考えられる.情報システムが社会,経済活動において利用されるようになるにつれ,情報システムに関する不正事件の発生は,企業・組織において大きな影響を与える.すなわち,管理者権限は,権限を持った者がモラルハザートを起こした場合,内部不正の道具となる.

今回,管理者権限の運用に関して不正使用のリスクとその背景,防止策に関して整理と問題提起を行い,原田研究室のアンケート調査によって,現状の運用面に関する状況の把握と業種別に判断した運用上の特徴に関して研究を行なった.

†1 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

Vol.2015-SPT-16 No.8
Vol.2015-EIP-70 No.8
2015/11/20

2. 管理者権限の運用

2-1. 利点と課題

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.具体例として,
①リスクの回避
1.ファイルやフォルダにアクセス制限をかけることにより情報の閲覧や破壊・削除されるリスクからの回避
2.従業員の不用意な操作によりシステム関連の重要なファイルやディレクトリを誤って削除されるリスクからの回避
3.従業員の意図的な設定の変更により,システム破壊などパソコンやタブレット端末,情報システム関連の動作が不安定になるリスクからの回避
4.管理者権限を必要とするマルウエアが侵入するリスク低減（回避）
②システムの制御
1.ハードウェアの使用に関して,従業員が独断で追加や削除を行なうことの制御機能
2.Firewallの設定を従業員が勝手に変更できないための制御機能
③情報システムの集中管理
従業員のパソコンやタブレット端末に対してOSやアプリケーションソフトのバージョンやアップデート状況の集中管理による業務効率向上
などの利点がある.しかし,運用面において課題が存在する.それは,業務効率を優先するとリスク対策を必要最低限度に留め,安全性の向上を優先すると管理を厳密にすることになり管理工数が増大する.管理者権限の使用は,それぞれの環境で想定されるリスクと運用のバランスを考慮した管理が必要になる. 一例として原田は【2】,職務分掌の問題を挙げている.これは,開発と運用,申請データ投入と承認が同一のIDや人材で運用をせざるを得ない状態などが存在し大きな課題として指摘している.

2-2. 先行研究

小松は[3],企業のセキュリティ対策に関して「技術的対策,組織的対策,物理的対策,人的対策など,費用とその効果に見合う対策を選択する必要がある」述べている.管理者権限の運用には,業種や企業規模,職場環境,予算など背景面とリスクを総合的に考え運用する必要がある.

島らによると[4],内部不正に関し「顧客名簿や技術ノウハウ等の重要情報や情報システム等の情報資産の窃取,持ち出し,漏洩,消去・破壊等を対処とし,内部者が退職後,在職中に得た情報を漏洩する行為等に関しても内部不正として取り扱う」と判断を行っている.内部不正は,退職した従業員も含めて対策を検討する必要がある.

Wang [5]は,内部不正のその他の技術的な対策として侵入検知,Firewall,暗号化,アクセスコントロールなどがあるが内部者への脅威に対しては,情報の不正な閲覧やシステム破壊の対策が弱い.内部不正の行為は,組織内部から直接攻撃を行う.高速ネットワークの利点を生かしサーバー内のデータベースに直接アクセスをしてデータの盗用や破壊を行う.また,企業は部署や組織ごとに管理体制や管理者（権限）が異なる場合もある.異なった管理体制では,部署や組織ごとに違った権限を持っているため,様々な種類の情報に対応する監督者や管理者が必要になる.更に,簡単な文字列によるパスワード設定などが不正操作を起こし易い背景を大きくしている原因と述べている.

2-3 . 国内ガイドラインから見る不正使用防止策

IPA「内部不正防止ガイドライン」[6]では,システム管理者（管理者権限を含む）による内部不正の防止策として,
①システム管理者の決定は,適正を満たす者を任命する.更に複数の管理者の中から相互監視ができるようにし,設定作業が正しく実施されたかを他のシステム管理者が確認をする
②一人のシステム管理者に権限が集中せず分散をする
③作業内容や日時が記載された報告書を作成し,更に別のシステム管理者が報告書の確認をするなど相互監視を行う
④特権を必要とする操作以外では,特権IDの操作の禁止
⑤利用者とシステム管理者を識別するために,利用者ごと,システム管理者ごとに利用者ID,システム管理者IDを割り当てパスワード等で認証する
⑥管理者パスワードを他の利用者に不正使用されないように単純な文字列で設定をせず定期的に更新をする
⑦他の利用者にID及びパスワード・ICカード等の貸与禁止
などを挙げている.これらの防止策は,内部不正防止の基本原則「犯行を難しくする・捕まるリスクを高める・犯行の見返りを減らす・犯行の誘因を減らす・犯罪の弁明をさせない」に効果があり,経営者が積極的に取り組むことが重要である.

3. 原田研究室アンケート調査

第 3 章では,第 2 章で取上げた管理者権限の運用面に関する課題に関して,アンケート調査を利用し現状の状況を報告する.

情報セキュリティ大学院大学原田研究室では,毎年,情報セキュリティ対策に関するアンケート調査[7]を行っている.2015 年度は,情報セキュリティマネジメントの取組み状況,情報セキュリティマネジメントの例外措置,情報セキュリティリスクの認識と支出の動向,情報セキュリティマネジメントの運用,事業継続に関わる取組みの実施状況,電子データの管理,個人情報漏えい事故のお詫び金,情報システムの管理者権限（特権 ID)等に関して調査を行っている.調

査の概要を以下に示す.

- 実施期間　2015 年 7 月から 8 月
- 対象組織　ISMS もしくは P マークの取得企業及び,大学と官公庁,教育機関などからランダムに選んだ 4,500 組織
- 回答数 346（2015 年 10 月 20 日現在）*2014 年度 437
- 調査方法　郵送によるアンケートの送付 設問数 60

本稿では,予備調査として 150 件の分析を行った.今後の分析結果によっては,結果が変化する可能性もある.

3-1. 仮説

本研究に関しては,2 つの設問を通して情報システムにおける管理者権限の運用に関して調査を行った.

質問 1：管理者権限（特権 ID）の運用ルールに関して管理規則の制定「はい・いいえ・その他」
この設問を通して管理者権限の使用に関して社内で規定された運用ルールが制定されていると判断を行なう.この設問を通して企業において管理者権限の運用に関して不正使用のリスク対策の意識が存在していると判断をする.

質問 2：管理者権限（特権 ID）に関して重視している施策（3 つまで選択）
これは,ISO/IEC 27002 9.2.3 特権的アクセス権[8][9]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資格等）によって重要視する特徴があるのではいか」と仮説をたて,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」
これは,ISO/IEC 27002 9.2 利用者アクセスの管理,9.2.1 利用者登録及び削除登録,9.2.2 利用者アクセスの提供に関連する.使用者の限定を行なうことにより,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を避けることができる可能性がある.また,管理者権限を使用する専門の人材が職場に存在し,特別な ID やパスワードとして企業内で認識していると判断をする.

2.「使用者の最小限化」
「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」
これは,ISO/IEC 27002 9.2 利用者アクセスの管理,9.2.1 利用者登録及び削除登録,9.2.2 利用者アクセスの提供に関連する.使用する権限を最小限化にすることにより管理者権限の使用において使用者の設定範囲に制限を掛けることができる.権限範囲を超えた無関係な情報の閲覧や情報システムの破壊を目的としたアクセスなどのリスクを低減させる.また,管理者権限を使用する人材とそれを管理する仕組み（人材）があると判断をする.

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」
これは,ISO/IEC 27002 9.2.2 利用者アクセスの提供に関連する.承認プロセスを設定することにより管理者権限の使用において従業員の独断の判断による,情報システムの設定の変更,重要情報の無関係な閲覧などのリスクの低減ができる.使用履歴の記録を行なうことにより使用者にログの保存を意思付けることにより牽制の仕組み（空気）が発生し管理者権限が悪用されるリスクを低減させる.また,管理者権限を使用する人材とそれを管理する仕組み（人材）があると判断をする.

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）」
これは,ISO/IEC 27002 9.2.5 利用者アクセス権のレビュー,ISO/IEC 27002 9.2.6 アクセス権の削除又は修正に関連する.ISO/IEC 27002 9.2.5 利用者アクセス権のレビューの実施の手引において以下の対策を取上げている.
①利用者のアクセス権を,定められた間隔で及び何らかの変更（例えば,昇進,降格,雇用の終了）があった後に見直す
②利用者の役割が同一組織内で変更された場合,そのアクセス権についてレビューし,割当てをし直す
③特権的アクセス権の許可は,利用者のアクセス権より頻繁な間隔でレビューする
④特権の割当てを定められた間隔で点検をして,許可されていない特権が取得されていないことを確実にする
⑤特権アカウントの変更は,定期的なレビューのためにログを取る
これらは,管理者権限の異動または不要となった特権 ID の使用権限の終了の手続きを定めることにより退職前にアクセス権限を保有していた従業員による退社後の情報ステムへのログイン,本来権限のない従業員の成りすましによるログインなど重要情報へ不正な閲覧やシステム破壊などを目的とした設定の変更などのリスクを低減させる.

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」
これは,ISO/IEC 27002 9.2 利用者アクセスの管理,9.2.1 利用者登録及び削除登録,9.2.2 利用者アクセスの提供,ISO/IEC 27002 6.1.2 職務の分離に関係する.

Vol.2015-SPT-16 No.8
Vol.2015-EIP-70 No.8
2015/11/20

特権専用の ID を設けていることにより権限のない従業員による重要情報へのアクセスのリスクが低減させる.また,情報システム管理者のアカウントがロックされログインが不可能になった場合,特権専用のアカウント使用により管理用の情報システムにログインが可能である.管理者のアカウントロックが自動解除されるまでの間,待機行なうことがなくなる為業務効率は上がる.だが,特権 ID のアカウントやパスワードの無関係な従業員への流出による重要情報の閲覧や入手,意図的なシステム破壊などのリスクがある.

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」
これは,SO/IEC 27002 7.2 雇用期間中,ISO/IEC 27002 7.2.1 経営陣の責任,ISO/IEC 27002 7.2.2 情報セキュリティの意識向上・教育及び訓練に関連する.雇用期間中において,管理者権限を使用する人物の力量がその職務に見合っていることを検証し,不正利用を行なうような人物でないことを判断する.可能であれば定期的に管理者権限を使用する人物の力量調査を行なう従業員の会社に対する満足度は日々変化がある. 面談などによる力量調査は,モラルハザードを発生させるリスクの低減をさせ, 不正使用の防止策として内部牽制の一つの仕組みとして影響がある. 管理者は高い規範意識を備えた人物が理想的であり,定期的に面談などで運用面や情報セキュリティに関してスキルチェックや意識の確認などを行うことが望ましいが,業務時間の配分や人数構成などの問題から現実的に行なうのは, 選考の段階（履歴書・職務経歴書や委託・派遣先へスキルシートの提出など）までに留めている場合もある. 雇用時（面接時）の段階のみで力量を判断している場合,ISO/IEC 27002 7.1 雇用前,ISO/IEC 27002 7.1.1 選考,ISO/IEC 27002 7.1.2 雇用条件,ISO/IEC 27002 7.1.2 雇用条件などが関連する.

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」
これは,ISO/IEC 27002 9.2.2 利用者アクセス権の提供に関連する.管理者権限の運用手順の制定を行なうことにより適用範囲外の使用の制限が可能である.アクセスログの保存や複数人の作業に限定をさせることにより管理者権限の使用に関して内部牽制の環境を作り不正利用への抑止をする.また,管理者権限の運用手順の制定を行なわなくても危機管理の意識が高い人材が多く存在していると判断をする.

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」
これは,ISO/IEC 27002 9.2.4 利用者の秘密認証情報の管理に関連する.
①頻繁にパスワードを変更する
②離職や移動などで不要となった管理者パスワードを出来るだけ早く変更をする
③特権を与えられた利用者の間でパスワード伝達方法を定めている
などが考えられる.この対策を行なうことにより管理者パスワードの機密性を高め無関係な人物による管理用情報システムへのアクセスによる重要情報の閲覧やシステム破壊を目的とした設定変更などのリスクを低減できる.

9.「その他」
これは,1 から 8 以外の管理方法が企業において存在し管理規則を定めていると判断をする.一例として,管理者権限の運用に関して専用のシステムがある,専門の業者に委託しているなどが考えられる.

10.「無回答」
管理者権限の運用面に関して不正使用へのリスク認識が弱い・管理の仕組みが曖昧であるなど不正に利用される可能性を意味する.

3-2. 基本データの調査

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 59%と最も多く次いで「大学」が 10%,サービス業が 9%であった.

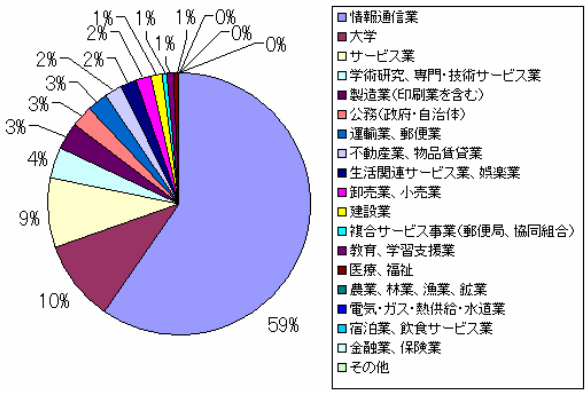

図 1　貴社・貴組織の業種（n=150）

従業員数は,50 人以下が 42%,次いで 101 人～300 人が 22%,51 人～100 人が 17%であった.従業員 300 人以下の中小企業が目立ち,更に 50 人以下の小規模な企業の回答が多かった.

Vol.2015-SPT-16 No.8
Vol.2015-EIP-70 No.8
2015/11/20

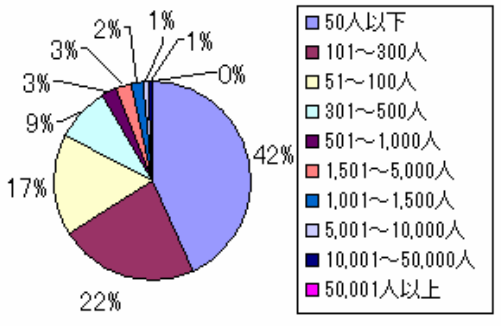

図 2　貴社の直近の従業員数(n=150)

売上高の調査では 10 億円から 50 億円が 29%,5 億円～10 億円が 21%,1 億円～3 億円未満 17%であった.

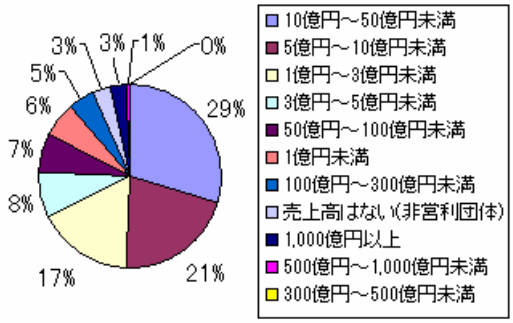

図 3　貴社の直近期の売上高(n=150)

所属に関しては,「総務部門」28%,「情報セキュリティ担当部門」24%,情報「システム管理部門」14%「社長室又は役員室」9%の順番であった.「総務部門」という回答が最も多く情報システムの管理者権限を持っている従業員は,総務部門の人材や職務などと兼任で管理をしている可能性がある.また,「情報システム開発部門」7%「企画部門」5%の回答も目立ち情報セキュリティ専門を意識した部署の確立がされていない.

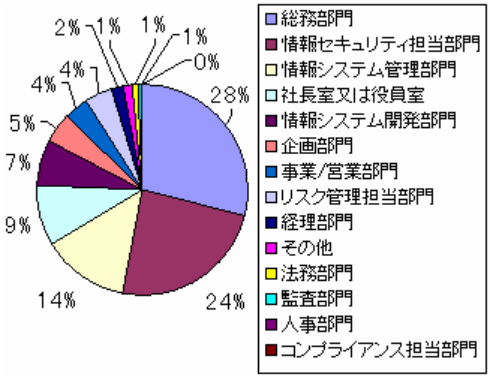

図 4　記入者の所属（n=150）

P マーク・ISMS・BCMS の取得状況は,P マークが 33%,ISMS が 15%,ISMS と P マークの両方取得が 49%,いずれも取得していない 3%であった.

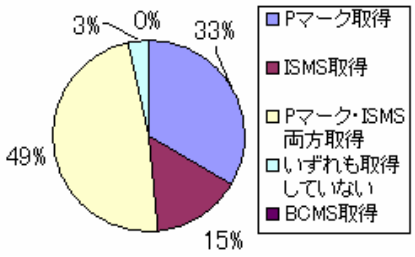

図 5　P マーク,ISMS,BCMS の取得状況(n=150)

3-3.　調査結果

管理者権限（特権 ID）の運用ルールに関しての調査では,「管理規則を定めている」が 67%と「管理規則を定めていない」が 27%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.

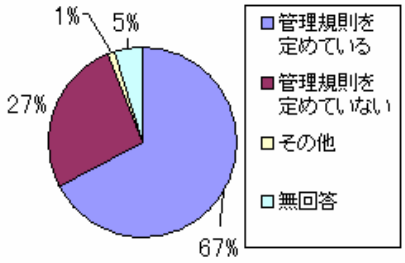

図 6　管理者権限の運用ルールに関して(n=150)

管理者権限（特権 ID）に関して重視している施策に関して回答数の多かった項目は,1.「使用者の限定」121 件と 2.「使用者の最小限化」63 件,次いで 5.「ID の使い分け」61 件であった.また,回答数の少ない結果として 6.「力量のレビュー」4 件,7.「使用手順の制定」17 件,8.「共有パスワードの管理方法の制定」19 件と 3.「承認プロセスの記録・許可」19 件であった.

また,無回答が全体 150 件中 12 件存在した.管理規則の制定に関して,12 件中 4 件は「管理規則を定めている」,6 件は「管理規則を定めていない」,2 件は「分からない」であった.この結果から管理者権限の運用面に関して不正使用へのリスク認識が弱い（曖昧な）企業も目立ち不正に利用される可能性が存在していることを証明する.

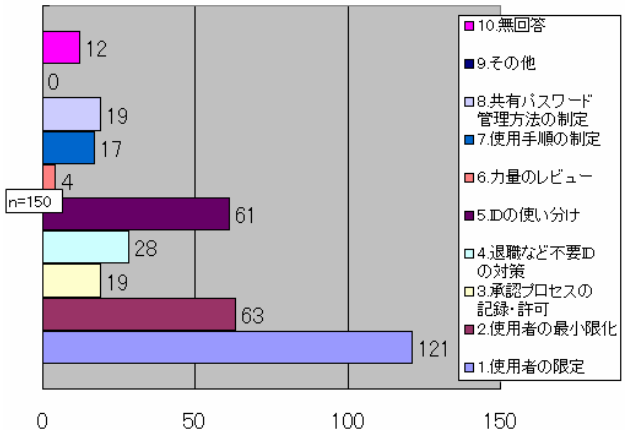

図 7　管理者権限に関して重視している施策(n=150)

Vol.2015-SPT-16 No.8
Vol.2015-EIP-70 No.8
2015/11/20

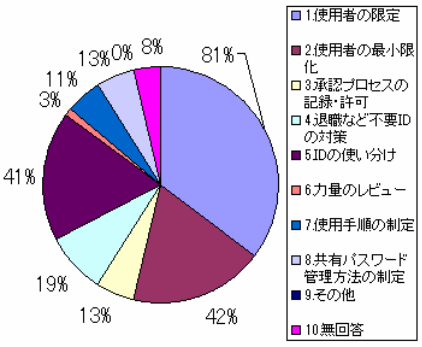

図 8　管理者権限に関して重視している施策(n=150)

3-4.　産業別の調査結果から考えられること

今回,「業種別」や「規模」で答数の多かったデータから「情報通信業」「大学」に絞って考察を行なった.結果を下記に示す.

3-4-1.　情報通信業

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）に関しての調査結果を図 9 図 10 に示す.

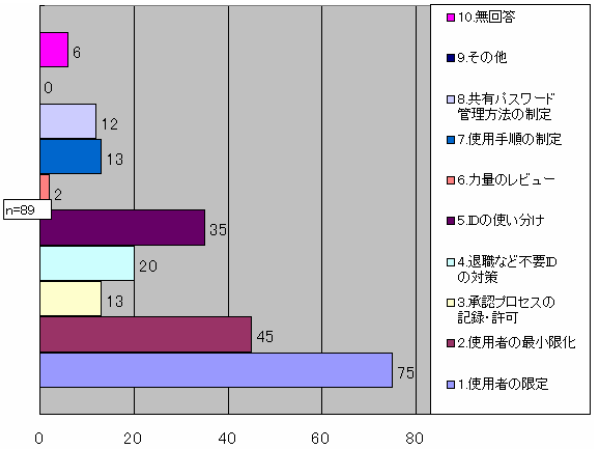

図 9　管理者権限に関して重視している施策/情報通信業

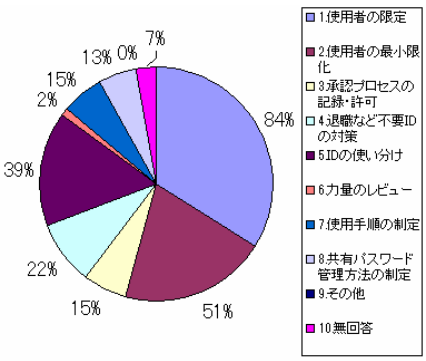

図 10　管理者権限に関して重視している施策/情報通信業 (n=89)

1.「使用者を必要な人のみに限定している」の回答が最多 75 件であった.

2.「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」の回答が 45 件であった.

5.「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」が 35 件で 3 番目に回答が多かった.

一方,少なかった回答として,

6.「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.「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.「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」

であった.

結果から情報通信業は,1.「使用者の限定」と 2.「使用者の最小限化」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」や 7.「使用手順の制定」8.「共有パスワードの管理方法の制定」であった.これは,使用する人材の力量調査に関し,雇用の段階のみで判断を行っている可能性がある.使用手順の制定においても,情報サービスの従業員は,全体的に情報システムの仕事や管理者権限に関して理解や危機管理の意識がある.更には,アンケートの回答元が情報システムのアウトソースをしている請負企業も考えられ,企業全体で運用手順の制定を行なわなくてもセキュリティの意識が各従業員において比較的高い人材が多いと判断をする.

3-4-2.　大学

大学に関しての調査結果を図 11 図 12 に示す.

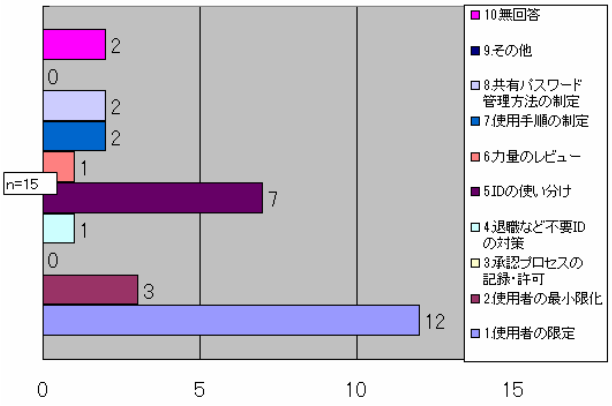

図 11　管理者権限に関して重視している施策/大学

Vol.2015-SPT-16 No.8
Vol.2015-EIP-70 No.8
2015/11/20

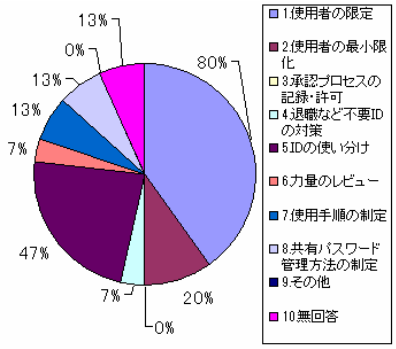

図 12　管理者権限に関して重視している施策/大学 (n=15)

1.「使用者を必要な人のみに限定している」の回答が最多 12 件であった.

5.「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」が 7 件で 2 番目に多かった.

また少なかった回答として,

3.「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.「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）」

6.「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」

であった.

大学は,1.「使用者の限定」や 5.「ID の使い分け」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.管理者権限を使用する専門の人材が職場に存在し,特別な ID やパスワードとして企業内で認識していると判断をする.また,特権専用の ID を設けていることにより権限のない従業員による重要情報へのアクセスなど不正利用のリスクを低減できる.

一方,回答が少なかった回答は,3.「承認プロセスの記録・許可」,4.「退職など不要 ID の対策」6.「力量のレビュー」であった.大学は,業務効率を重視し従業員の独断の判断による管理者権限の使用に任せている傾向がある.管理者による承認プロセスや使用履歴のログはされていない.これは,従業員の独断の判断による管理者権限の使用が可能である.情報システムの設定の変更,重要情報の無関係な閲覧,退職前にアクセス権限を保有していた元従業員による情報ステムのログインなど悪用をされるリスクがある.力量調査に関しては,定期的にされておらず使用する人材の雇用の段階のみで使用する人材の力量を判断していると判断する.

3-4-3.　情報通信業と大学との比較

情報通信業と大学を比較した場合,ともに 1.「使用者の限定」の回答が多かった.この結果から管理者権限の運用は,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を避ける意識が高いと判断する.大学においては 2.「使用者の最小限化」の回答が情報通信業と比較し少なかった（情報通信業は全体 89 件中 45 件で全体の 50%,大学は 15 件中 3 件で全体の 20%）. この結果から,権限範囲を超えた無関係な情報の閲覧や情報システムの破壊を目的としたアクセスなどのリスクも考えられる.これは,悪用されるリスクと管理者権限の運用における作業効率（業務効率）を比較した場合,作業の効率性を重視していると判断をする.

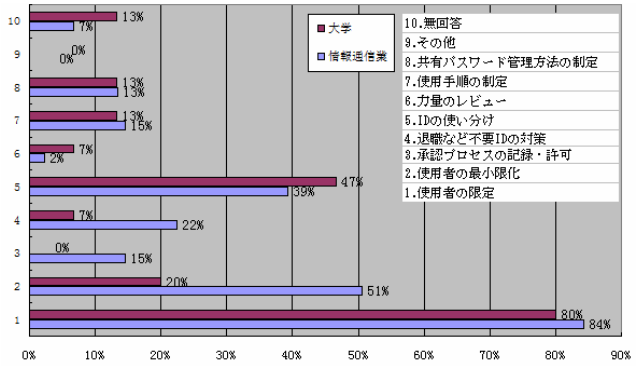

図 13　情報通信業(n=89)と大学(n=15)の比較

4.　まとめと考察

内部不正とは,組織内部における情報にアクセス権限を持った者が目標達成のために悪用し被害を与える行為である.管理者権限の運用ルールの制定は,業種や企業規模など属性からの違いがあると考える.運用ルールの制定には複雑な背景（環境・企業の規模・業種・予算）と想定されるリスクを考慮し総合的に判断を行なう必要がある.今回のアンケート調査の結果から ISMS 認証を取得していない中小規模の情報通信業や大学に対しては,「使用者の限定」「ID の使い分け」は応用（適用）が出来る可能性があると判断をする.また,情報通信業と大学ともに「力量のレビュー」に関しては,実施状況が少なく定期的な力量調査は行なわず管理者権限の使用する人材に関して力量調査を面接や履歴書・職務経歴の確認など雇用の段階のみで判断を行っていると考える.

謝辞

本調査あたりご指導頂いた情報セキュリティ大学院大学の教授,原田研究室の先輩、同僚の皆様に謹んで感謝の意を表する.

参考文献

1)　総務省　平成 25 年通信利用動向調査の結果 p.5 別添 p.6 http://www.soumu.go.jp/johotsusintokei/statistics/data/140627_1.pdf
2)　原田要之助　監査の視点からみた特権管理の必要性と課題 DIT 特権 ID 管理ソリューションセミナー pp.16-21 (2011).
3)　小松文子　企業の営業秘密保護と情報セキュリティ対策

情報処理学会研究報告 p.3 (2014) .
4) 島成佳・小松文子・小川博久・岡松さやか・高木大資 内部不正インシデント防止策と有用な職場環境に関する分析と考察 マルチメディア,分散,協調とモバイルシンポジウム pp.1218-1219(2015) .
5) Hui Wang Research On Security Architecture MSIS For Defending Insider Threat 2010ACADEMY PUBLISHER AP-PROC-CS-10CN007 pp.389-390 (2010)
6) IPA 組織における内部不正ガイドライン p.6 pp.30- 31 (2015). http://www.ipa.go.jp/files/000044615.pdf
7) 情報セキュリティ大学院大学原田研究室 情報セキュリティアンケート調査 http://lab.iisec.ac.jp/~harada_lab/survey.html
8) 北原幸彦・竹田栄作・中野初美・山下真・原田要之助 ISO/ISE27002 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(2015) .
9) 日本工業標準調査会 http://www.jisc.go.jp/app/pager?id=1331762