

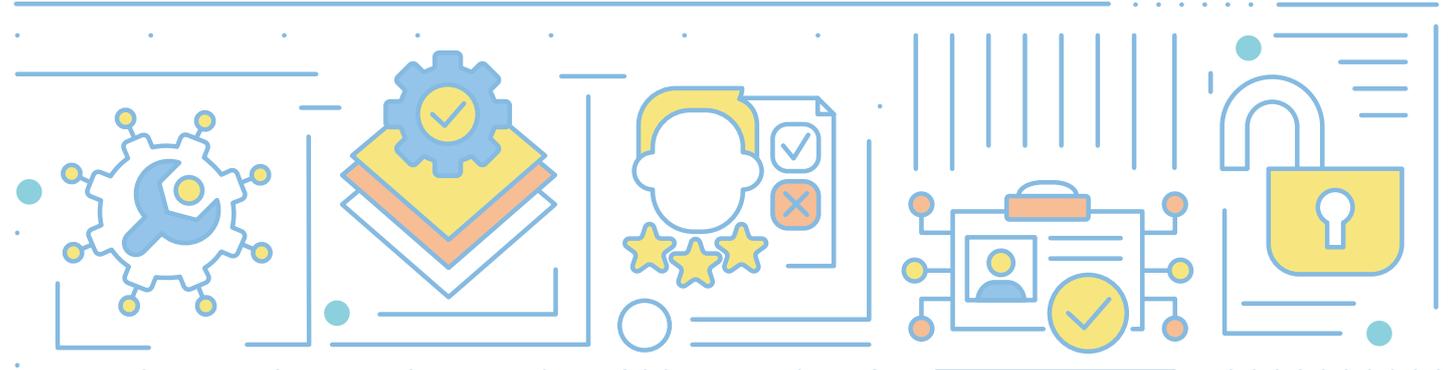


企業規模別に見る

日本企業のID・アカウント運用管理の実態 2023

「クラウド利活用時代の、日本企業のID・アカウント運用実態調査2022」調査結果の概要

大手企業 (5,000人以上)、中堅企業 (500~4,999人)、中小企業 (100~499人)
で異なるID・アカウント運用管理の実態とは？



はじめに

2020年のコロナ禍を経て、多くの企業はリモートワーク環境を整備するために、さまざまなシステムやアプリケーションのクラウド化を進めたり、リモートワークに適したデバイスの活用を進めたりしてきました。そして現在、多くの企業ではシステムやサービスにアクセスするためのID・アカウントが増加するとともに、その管理が重要な課題となりました。

例えば、ID・アカウントの管理者にとって、従業員の入社や退職、部署の変更などによって、管理負荷が増大するという問題があります。また、セキュリティ面でも、ID・アカウントの不正利用による情報漏えいなど、新たなセキュリティリスクが懸念されます。

そこで本レポートでは、アンケート結果をもとにID・アカウント管理の導入状況や課題などを、大手企業・中堅企業・中小企業^{*}にそれぞれ分類し、それぞれの実態をご紹介します。今後の自社にとって適切なID・アカウント管理を実現するためにも、ぜひご一読ください。

※本資料では、従業員規模により下記のように分類しています。

大手企業：5,000人以上、中堅企業：500～4,999人、中小企業：100～499人

目次

エグゼクティブサマリー	3
1 ID・アカウント運用管理の実態	4
2 ID・アカウント管理の課題.....	8
3 SaaS利用の拡大とその働き方の多様化	11
4 これからのID・アカウント管理とゼロトラスト	13

調査概要

アンケート名 ● クラウド利活用時代の、日本企業のID・アカウント運用 実態調査2022

調査手法 ● 自社ハウスDB上でのオンラインパネル調査

調査対象 ● ① 株式会社ソフトクリエイトの保有リード：132件（「立場」情報に「協業・売り込み」、
“販社・パートナー”、“その他”を含まない、マーケティングメール受信許可リード）
※ソフトクリエイト関係者はすべて除外

② Web調査：275件

※合計407件のうち、中小企業(106件)、中堅企業(101件)、大手企業(65件)を対象に集計

調査集計期間 ● ① 2022年10月5日～14日

② 2022年12月9日～12月29日

調査企画 ● 株式会社ソフトクリエイト/株式会社エクスジェン・ネットワークス/2BC株式会社

調査実施 ● 株式会社ソフトクリエイト/株式会社エクスジェン・ネットワークス

エグゼクティブサマリー

総評

ID・アカウント管理の 共通かつ最大の課題は「複雑化」、 解決策は規模に応じて見極めたい



現代の企業において、さまざまなサービスやシステムにアクセスするために必要なID・アカウントの管理が重要な課題となっています。しかし、ID・アカウント管理の実情や課題は企業規模により異なることから、本資料では、大手企業、中堅企業、中小企業に分類して調査を実施しました。

企業規模別に分類したところ、大手企業がID・アカウント管理に関する先行的な取り組みを実施し、中堅・中小企業がそれに追従するかのように取り組んでいる様子が伺えました。例えば、ID・アカウント管理の専用ツール導入やクラウド化、ゼロトラストへの取り組みでは、いずれも企業規模が大きくなるほど取り組みが進んでいることがわかりました。

また、大手・中堅企業の半数はID・アカウントの源泉情報が「人事システム」であるのに対し、中小企業は3割でした。ゼロトラスト環境構築に向け、人事情報とIDの連携については課題が多いと考えられます。

クラウドサービス（主にSaaS）の利用が拡大する今、いずれの規模の企業も従来のID・アカウント管理では限界を迎えたとともに、セキュリティ上の脅威も増加しています。その結果、ID・アカウント管理の最大の課題はいずれの企業も「複雑化」であり、それぞれの規模に応じた対応が求められています。

※本資料では、従業員規模により下記のように分類しています。
大手企業：5,000人以上、中堅企業：500～4,999人、中小企業：100～499人

各論

ID・アカウント管理における現状と課題

大手企業

- 現状**
- 専用ツール導入状況...オンプレミスは38.5%、IDaaSは21.5%
 - 関連会社・海外会社の管理も必要
 - ID・アカウント管理の源泉情報は「人事システム」が55.4%
- 課題**
- 複雑化への対応、担当者依存・ブラックボックス化からの脱却
 - パスワードレス認証への取り組み

中堅企業

- 現状**
- 専用ツール導入状況...オンプレミスは32.7%、IDaaSは15.8%
 - 管理担当者を設定し、運用・管理が比較的行えている
 - ID・アカウント管理の源泉情報は「人事システム」が54.5%
- 課題**
- 複雑化への対応、クラウド化推進、多要素認証やSSOの推進

中小企業

- 現状**
- ExcelやCSVでの管理が中心、正社員以外にパート・アルバイトも多い
 - 専用ツール導入はオンプレミスで16.0%、IDaaSは7.5%
 - ID・アカウント管理の源泉情報は「人事システム」が29.2%
- 課題**
- 複雑化への対応、運用ルール策定が必要、SSOの導入率が低い

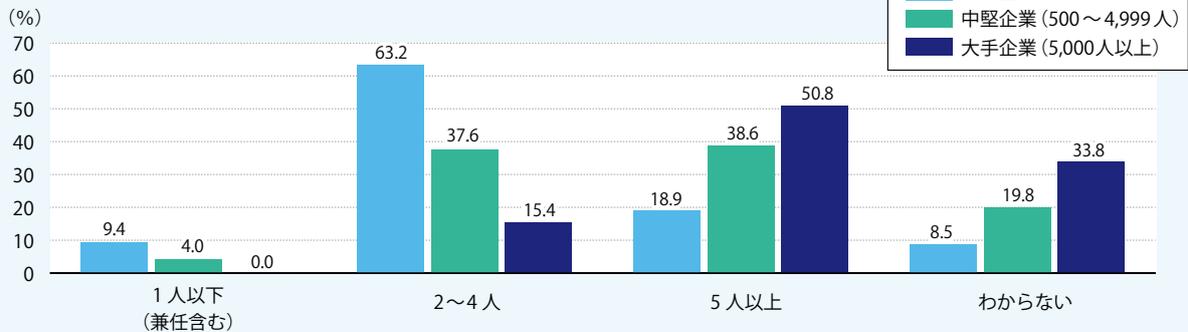
1 ID・アカウント運用管理の実態

ID管理ツール・SSO導入は大手が先行、 中小はADやExcelでの管理が多数

リモートワークの普及やクラウドサービス利用拡大、セキュリティ対策の重要性といった観点から、ID・アカウント管理の重要性が指摘されています。このような状況下、ID・アカウント運用管理の実態を企業規模ごとに見ていきましょう。

規模に応じて増える管理者、大手企業は「5人以上」が過半数

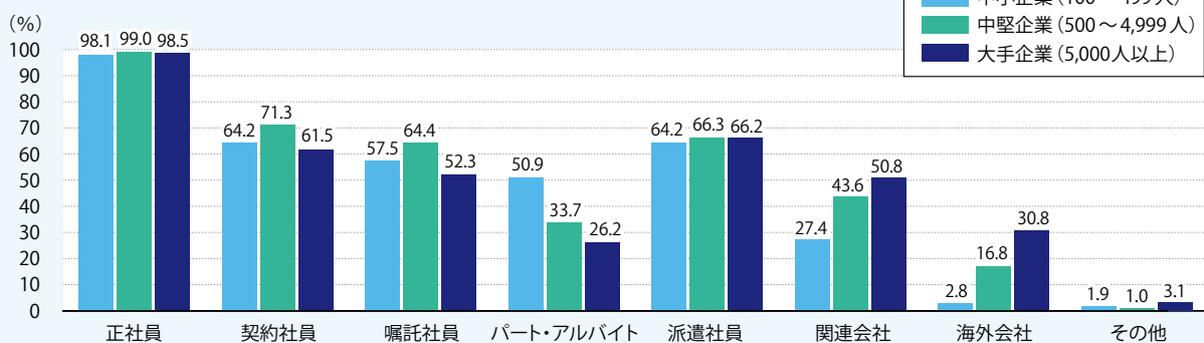
01 自社のID・アカウントに関わっている管理者数



ID・アカウントに関わっている管理者数は、中小企業では「2~4人」が63.2%で最多、中堅企業は「2~4人」が37.6%、「5人以上」が38.6%でほぼ同様、大手企業は「5人以上」が50.8%で最多となりました。この結果からは、企業規模が大きくなるほど管理者数が増える傾向がありました。その理由としては、企業規模が大きくなるほど、IDメンテナンス対象となるシステムが増えること、ユーザー権限や組織が複雑化し、管理運用の負担が大きくなっていることなどが考えられます。

大手・中堅は「関連会社・海外会社」、中小は「パートなど」の利用が増える

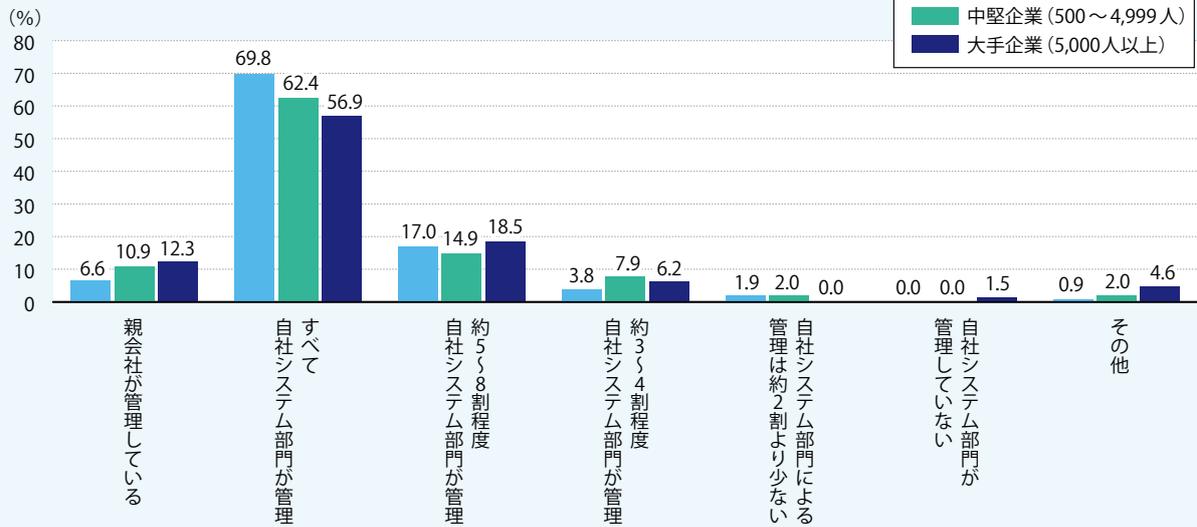
02 自社で導入しているシステム（業務系・基幹系・情報系）の利用者（複数回答可）



自社システムの利用者は、いずれの規模の企業も正社員はほぼ100%、契約社員・派遣社員は60%以上となりました。規模別の特徴を見ると、中小企業は「パート・アルバイト」が50.9%と他よりも20%近く多い結果になりました。一方、規模が大きくなるほど「関連会社」「海外会社」での利用者が増える傾向が見られました。

「すべて情シス管理」中小企業は約70%だが大企業では約60%、企業規模で異なる体制

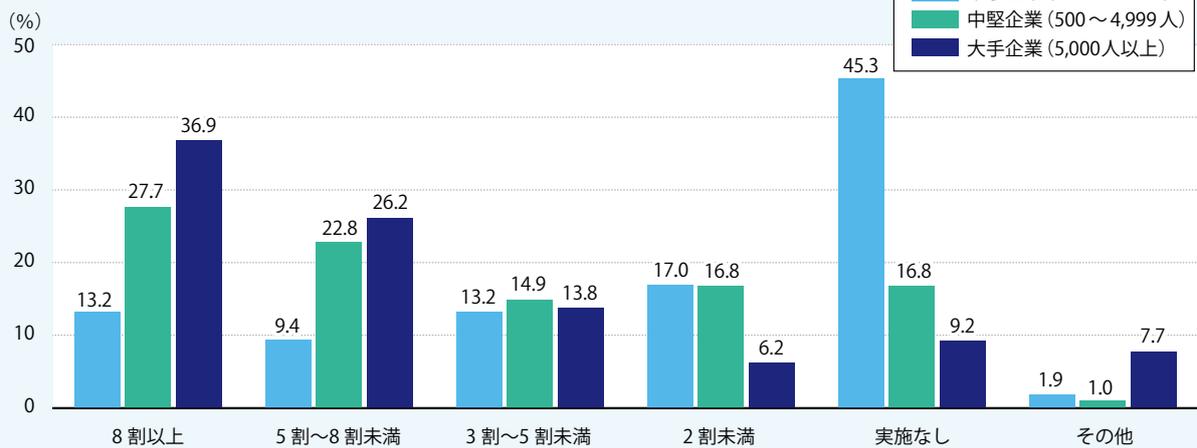
03 自社のID・アカウント管理主体



ID・アカウントの管理主体では、いずれの企業規模でも「すべて自社システム部門が管理」が最多です。しかし、企業規模が大きくなるほど減少傾向にあり、中小企業では69.8%であるのに対し大手企業では56.9%と10%以上の差が生じる結果となりました。一方、「約3~4割」「約5~8割」を合わせると約20%となることから、自社システム部門がID・アカウントを管理しきれない実情も伺えます。管理漏れによるリスクを回避するためには、ID管理が必要となると考えられます。

「半数以上のシステムがSSO対応」大手企業は約60%、中小企業は約20%

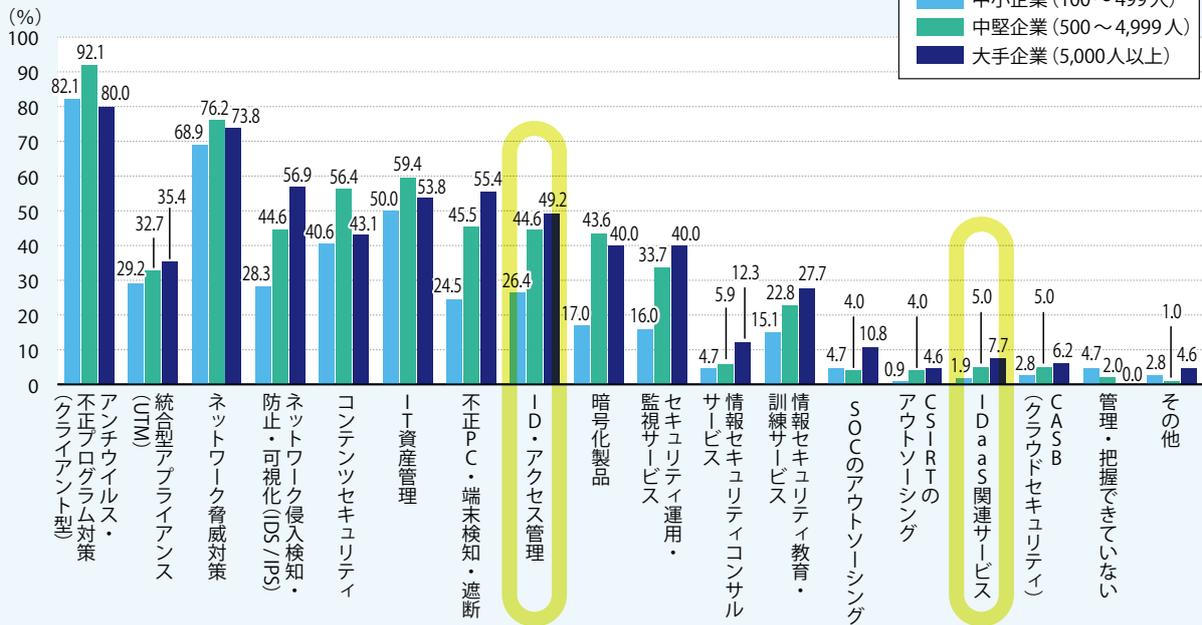
04 自社のシステム(業務系・基幹系・情報系システム)におけるSSO対応状況



ID/パスワード入力の負荷を減らすことができるSSOの導入は大手企業が率先して進めている様子が伺えます。大手企業の自社システムにおけるSSO対応状況は「8割以上」が36.9%、「5~8割未満」が26.2%となり、両者を合わせると半数以上がSSOに対応していることがわかりました。同じく「5~8割未満」+「8割以上」の結果を見てみると、中小企業では約20%、中堅企業では約50%となり、規模が小さくなるほどSSO対応が遅れていることがわかりました。

ID管理製品導入は、大手が先行、中堅は約半数、中小は30%未満

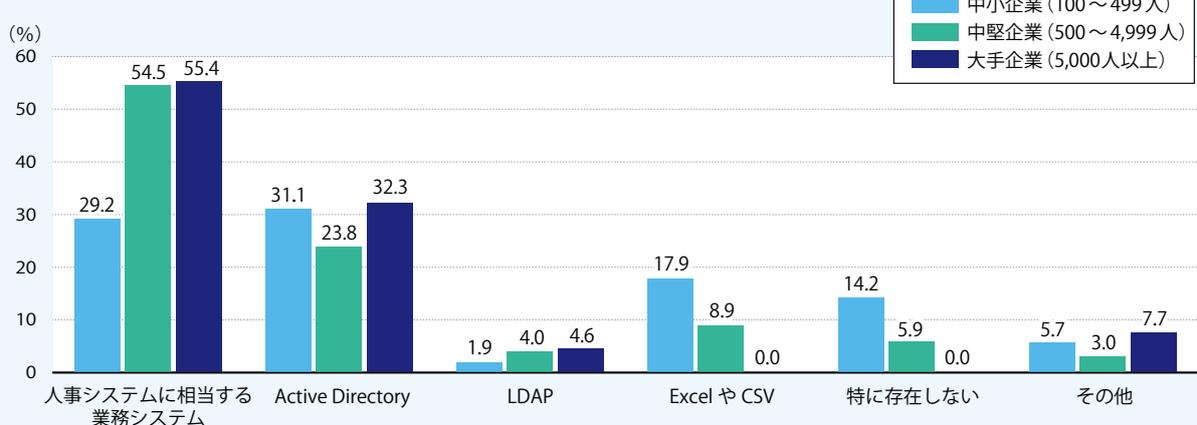
05 自社で導入しているセキュリティ対策製品・サービス (複数回答)



自社で導入しているセキュリティ対策製品・サービスのうち、「ID・アクセス管理」と「IDaaS関連サービス」に注目します。いずれも企業規模が大きくなるほど増加する傾向があり、「ID・アクセス管理」は大手企業では49.2%、中小企業では26.4%と20%以上の差がありました。「IDaaS関連サービス」は大手企業が7.7%、中堅企業が5.0%、中小企業は1.9%と、大手が先導するものの、いずれの企業規模でも現在は普及段階であると考えられます。

源泉情報は、大手・中堅では「人事システム」が最多、中小では「AD」が最多

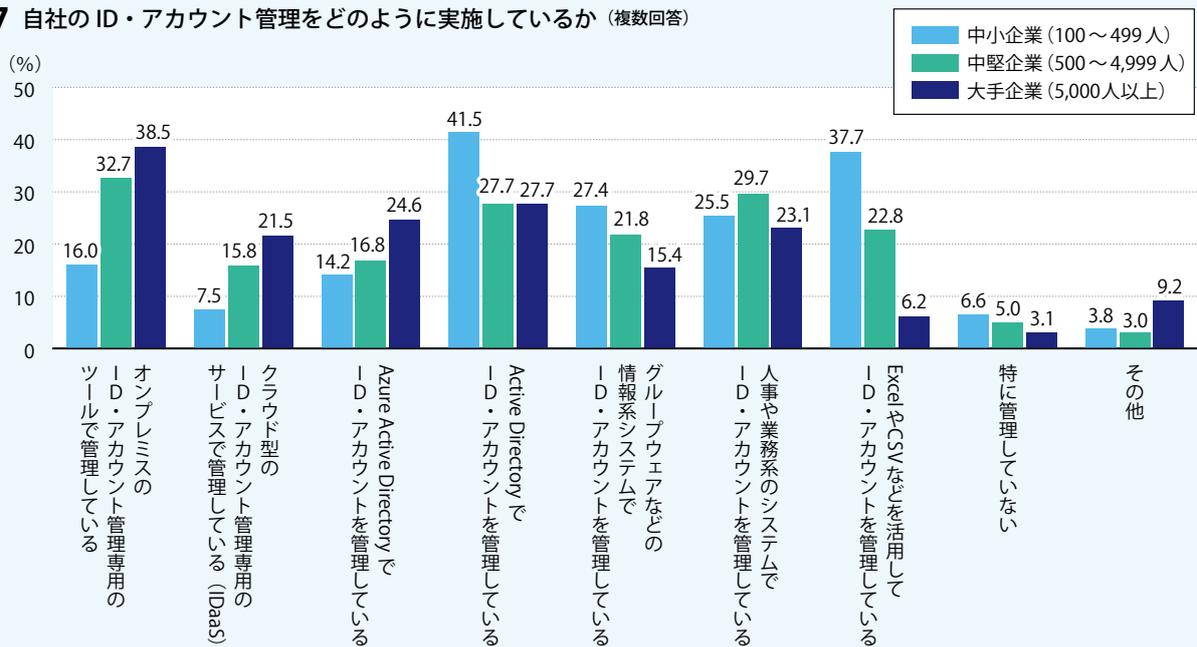
06 自社のID・アカウント管理の元となる社員情報のデータソース (源泉情報)



自社のID・アカウント管理の元となる、社員情報のデータソース(源泉情報)は、大手企業・中堅企業とも約半数が「人事システムに相当する業務システム」で最多、中小企業は「Active Directory」が31.1%で最多となりました。この結果からは、大手・中堅企業では、人事情報とID・アカウントを紐付けて管理し、アカウント生成・削除を効率化する動きが表れているとも考えられます。今後、HR Techがますます普及していくことを考えると、ID・アカウント製品との連携により、セキュリティ対策を含め多くのメリットが得られることが予測できます。

大手・中堅は専用・人事系ツールなどでID管理、中小はAD・Excelなどでの管理が多い

07 自社のID・アカウント管理をどのように実施しているか（複数回答）



自社のID・アカウント管理の実施方法について見ていきましょう。まず、「オンプレミスのID・アカウント管理専用のツールで管理」は大手企業が38.5%、中堅企業が32.7%、中小企業が16.0%となり、規模が大きくなるほど導入が増えていることがわかりました。この傾向は、「IDaaS」や「Azure Active Directory」にも見られました。

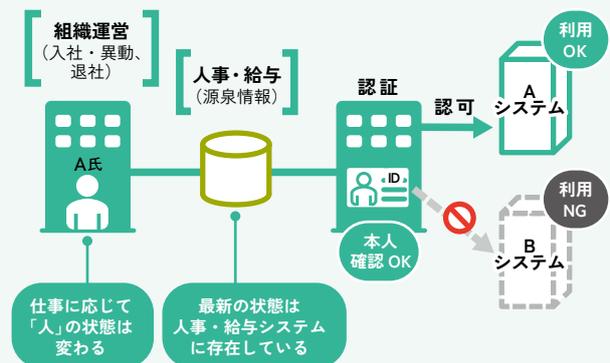
一方、「Active Directoryで管理」は中小企業が41.5%で他よりも10%以上多いことがわかりました。同様の傾向は「グループウェアなど」、「ExcelやCSVなど」でも表れていることから、ID・アカウント管理対象が少ないほど、専用ツール以外で管理している実態がわかりました。しかし、利用するサービスの増加など、ID・アカウント管理対象が増えていることから、今後、どのように変化するのか注目していきたい項目です。

コラム ①

人事情報とID情報は一致するべき

人事情報のデジタル化が進み、入社・退社や異動の情報が速やかに人事・給与システムに反映されるなど効率化をもたらしています。

この人事情報を源泉情報としてID管理を行う企業が、大手・中堅企業では約5割という結果でした (P.6・06のグラフ参照)。つまり、「人事情報 (源泉情報) とID情報は一致」することになり、右図でいうA氏の最新の人事情報がIDにも反映されているということになります。



まとめると、人事情報とID情報が一致することは次のようなメリットをもたらします。

- 人事情報を更新すると、IDの状態も最新化できるので運用がシンプルに
- IDの入力負荷の軽減や、入力・設定ミス、登録漏れの抑制
- 権限変更などが速やかに反映されることで、不正利用の抑止に

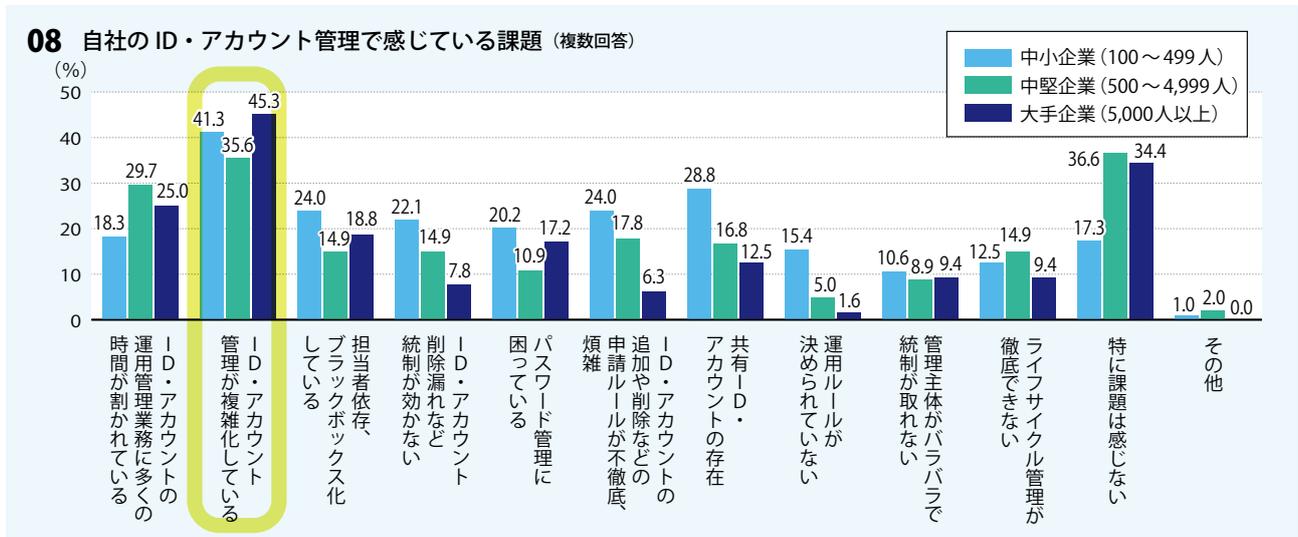
このように、人事情報とID管理を直結するテクノロジーの活用は、業務の効率化のみならず、セキュリティ強化の面も期待できます。しかし、近年、リモートワーク環境やクラウド化の普及で新たな課題も生まれました。 → P.12 コラム②に続く

2 ID・アカウント管理の課題

ID・アカウント管理の複雑化が最大の課題、 大手が先行しIDaaS導入も進んでいる

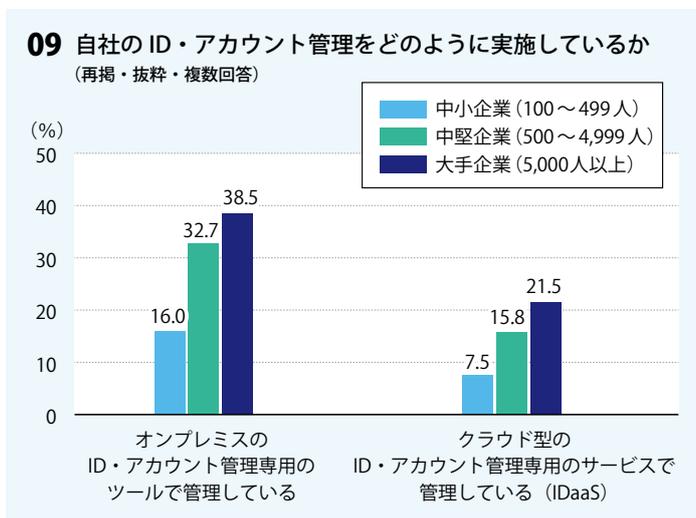
ID・アカウント管理の重要性が増す中で、管理担当者はどのような課題を抱えているのでしょうか。
この章では、直面している課題や、今後、実施したいと考えていることなどを取り上げます。

「ID・アカウント管理の複雑化」が最大の課題に



ID・アカウント管理における課題として、どの企業規模でも最多だったのが「ID・アカウント管理が複雑化している」となりました。「ID・アカウントの運用管理業務に多くの時間が割かれている」は大手企業では25.0%、中堅企業では29.7%と次に多い課題となりました。中小企業では、「共有ID・アカウントの存在」が28.8%、「ID・アカウントの追加や削除ルールなどが不徹底、煩雑」が24.0%となりました。

ID管理専用ツールはオンプレミス多数だが、IDaaS導入も進んでいる



ID・アカウント管理が複雑化する中、その解決策の1つとしてID・アカウント管理専用ツールの導入が進んでいます。企業規模が大きくなり管理対象ID・アカウントが増えると、Excelなどでの管理では難しくなり、専用ツールが必要になると考えられます。

そのうち、オンプレミス型の方が先行していて大手企業では38.5%、中堅企業では32.7%、中小企業では16.0%となっています。

一方、クラウド型のID管理サービスであるIDaaSは、大手企業では21.5%、中堅企業では15.8%、中小企業では7.5%となっています。後発のIDaaSですが、大手企業が先導して少しずつ普及が進んでいる様子が伺えます。

ID・アカウント管理のルール整備は大手・中堅が60%、中小では40%

大手・中堅の4割はルール整備できていない

自社のID・アカウント運用・管理業務について、企業規模ごとにさらに詳しく見ていきましょう。

まず、「ID・アカウントの追加、変更、削除ルールが整備されている」と回答した大手企業は56.9%、中堅企業は58.4%。60%近くがID・アカウントを管理する上での基本的なルールが整備できているとも言えますが、逆に言うと、回答していない4割近くはこのルールが整備されていないということになります。こうしたルールが整備されていないと、退職者アカウント経由での情報漏えいなどセキュリティインシデントの原因にもなりかねませんので、早急に対策すべきといえます。

また、「ID・アカウントの追加、変更、削除ルールに沿って運用できている」は大手企業では49.2%、中堅企業は59.4%。大手企業の約半数と中堅企業の約40%はID・アカウント管理ルールの運用に対しても課題を抱えている可能性があることがわかりました。

約20%の中小企業で、ID・アカウントの「削除ルール」が未整備

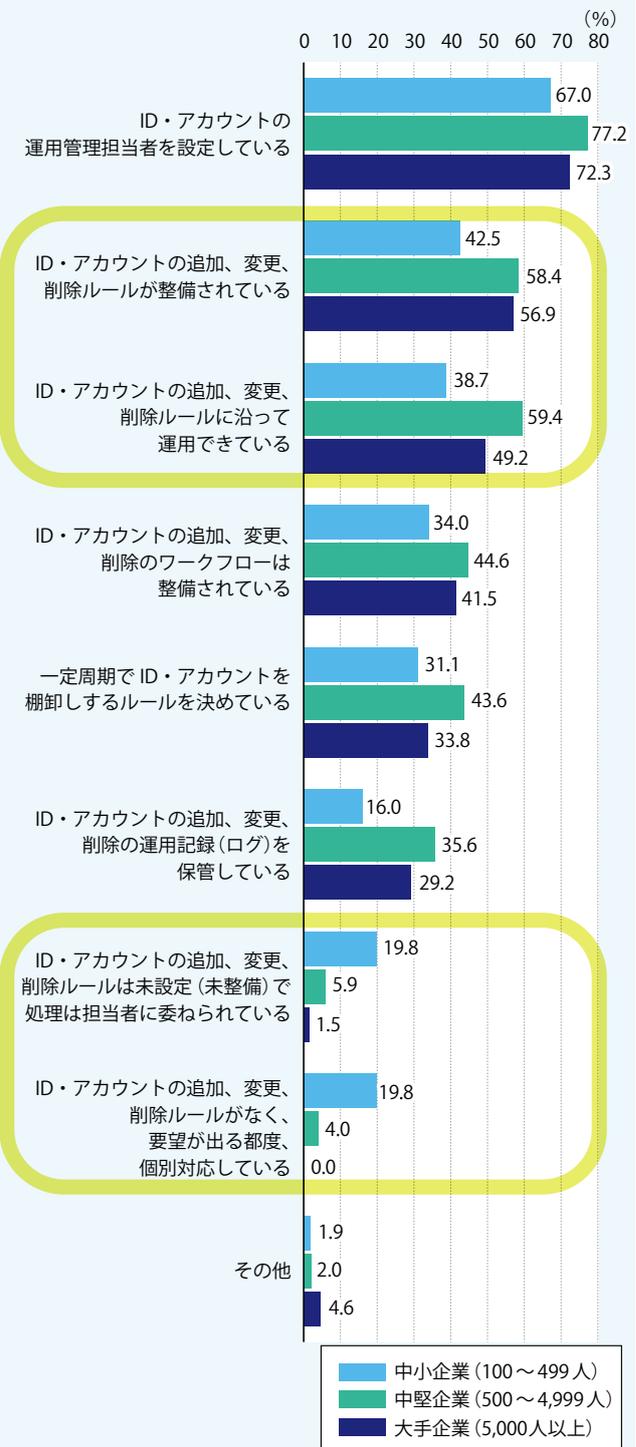
一方、中小企業を見ていくと、「ID・アカウントの追加、変更、削除ルール」が「未設定」あるいは「ルールがない」が約20%ということがわかりました。

ID・アカウント管理担当者まかせであったり、その都度担当者が対応しているものと考えられますが、このような状況では次のようなリスクが考えられます。

- 削除漏れしたアカウントからの不正アクセスや情報漏えい
- コンプライアンスや監査上のリスクがあり、関連企業やクライアント企業などから受発注における問題が生じるおそれがある
- アカウント発行や確認が手作業になるなどの理由から、業務効率の低下につながる

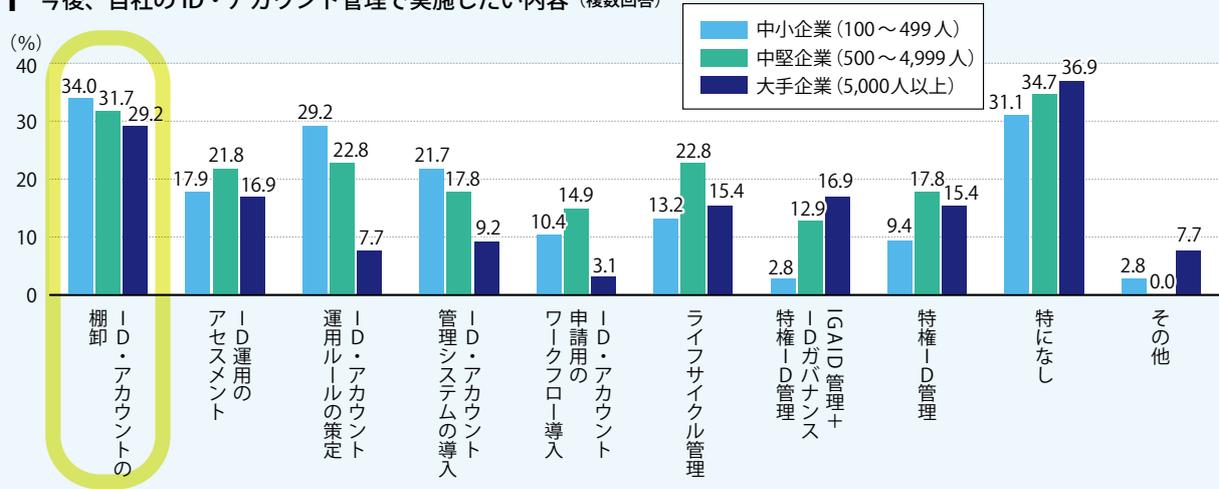
これはほんの一例ですが、こうしたリスクにつながらないよう、まずは最低限のルール策定から進めることも必要だと考えられます。

10 自社のID・アカウント運用・管理業務について
(複数回答)



今後、実施したいのは「棚卸」で30%以上、「ルール策定・システム導入」大手は完了か

11 今後、自社のID・アカウント管理で実施したい内容（複数回答）



自社のID・アカウント管理で、今後実施したい項目では、いずれの企業規模でも「ID・アカウントの棚卸」が最多となりました。企業規模ごとに2位以降についても見ていきましょう。

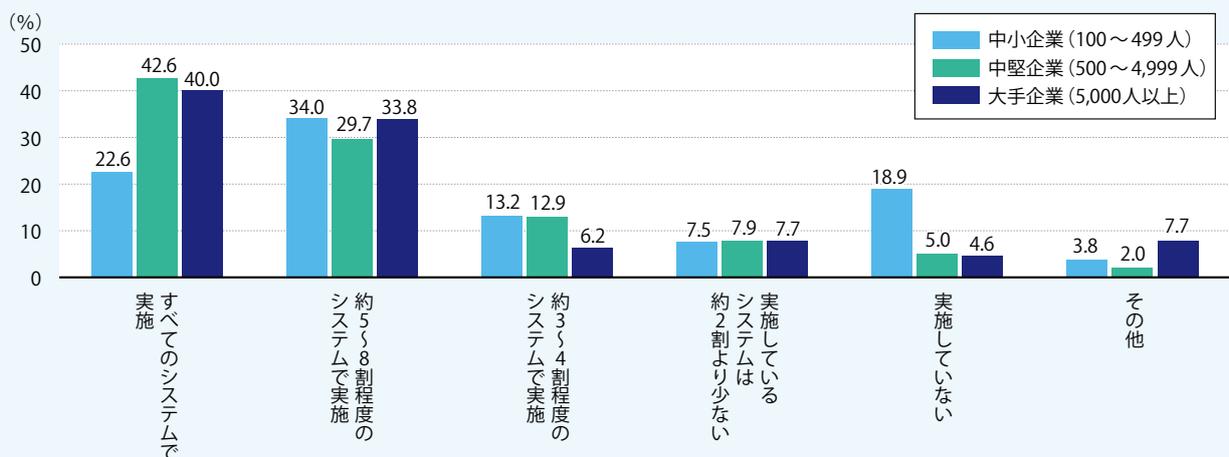
大手企業は「ID運用のアセスメント」が次いで16.9%と多いものの、全体的に15%以下となりました。

中堅企業では、「ID・アカウント運用ルールの策定」と「ライフサイクル管理」が22.8%、「ID運用のアセスメント」が21.8%となりました。

中小企業は全体的に「今後、実施したい項目」が高い傾向が見られました。「ID・アカウント運用ルールの策定」は29.2%、「ID・アカウント管理システムの導入」は21.7%と、今後の運用管理について模索している様子が伺えました。

大手・中堅の70%が「半数以上のID・アカウント棚卸」を実施、中小企業の未実施は約20%

12 ID・アカウント棚卸の定期的な実施状況（自社で導入している業務系・基幹系・情報系システム）



今後実施したい項目として多かった「ID・アカウント管理の棚卸」ですが、現状を見ると大手企業・中堅企業ともに「すべてのシステムで実施」が約40%、「約5~8割のシステムで実施」が約30%となり、約70%の企業が半数以上のシステムのID・アカウント棚卸を実施しているということがわかりました。

一方で中小企業は「実施していない」が18.9%と高い状態で、「すべてのシステムで実施」が22.6%と、大手・中堅企業に比べて進んでいない状況となりました。

3

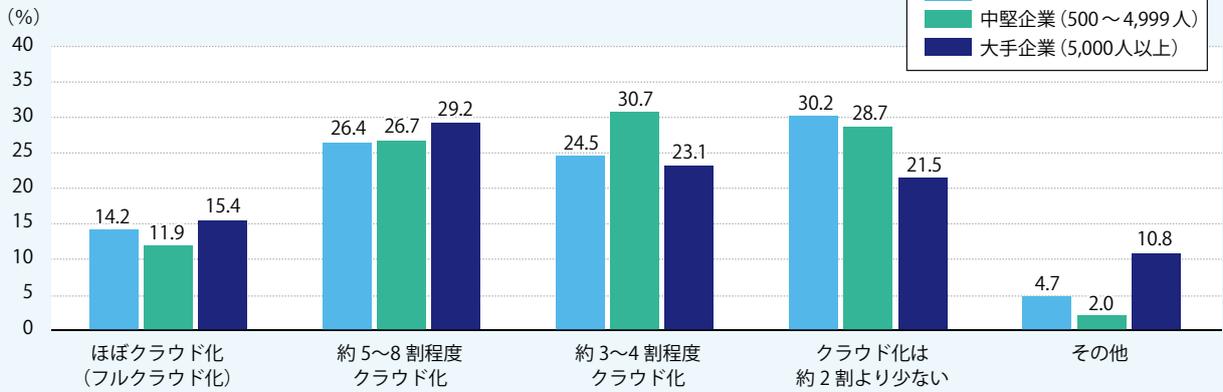
SaaS利用の拡大と働き方の多様化

クラウド化が企業規模を問わずに進む今、SaaSの一元管理は課題

多くの企業が従来のオンプレミスのアプリケーションからSaaS化を進めています。企業規模ごとにSaaS利用の現状と、管理状況について紹介します。

「5割以上～ほぼクラウド化」している大手企業は45%、脱オンプレミスが進む

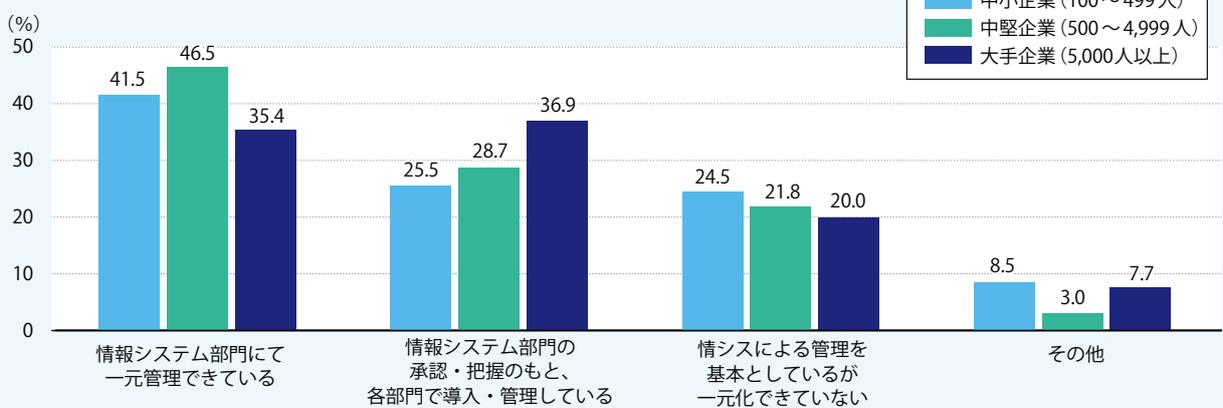
13 自社で導入しているクラウドサービス (SaaS) の利用状況



クラウドサービス(SaaS)の利用状況を見てみると、「約5～8割程度」と「ほぼクラウド化」を合わせると、大手企業は約45%、中堅企業は約39%、中小企業は約41%となりました。一方、「クラウド化は約2割より少ない」では、大手企業は21.5%、中堅企業は28.7%、中小企業は30.2%という結果になり、総じて企業規模が大きくなるほどクラウド化が進んでいることがわかりました。

SaaSを一元管理できていない大手・中堅は20%、中小では25%

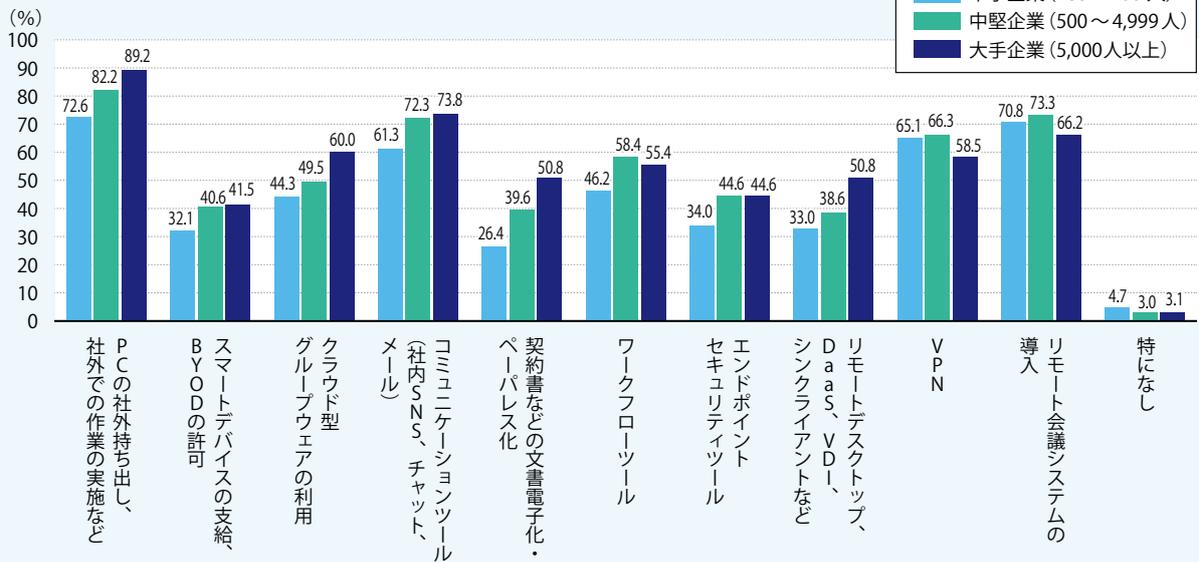
14 自社で導入しているクラウドサービス (SaaS) の管理状況



SaaSの管理状況を見てみると、「情報システム部門にて一元管理できている」あるいは「情報システム部門の承認・把握のもと、各部門で導入・管理」が多数派ですが、「一元化できていない」がいずれの規模の企業でも20～25%であることがわかりました。把握しきれないSaaSやそのID・アカウントはセキュリティインシデントの原因にもなりかねませんので、一定のルールのもと管理する体制が不可欠です。

場所を問わない働き方に向けたIT活用は、大手が先導し全体的に進んでいる

15 自社で多様な働き方を実現するために取り入れているIT施策（複数回答）



リモートワークの普及など新しい働き方に向け、どのようなIT施策が実施されているのでしょうか。「PCの社外持ち出し、社外での作業の実施など」は大手企業は約90%、中堅企業は約80%、中小企業では約70%と、すでに多くの企業では場所を問わない作業環境の実現に向けた取り組みが進められています。他にも、「コミュニケーションツール」「リモート会議システムの導入」など、社内外でのコミュニケーション充実に向けた取り組みが目立っています。「VPN」はセキュリティ上の課題があることが影響したのか、大手企業は他よりやや低い傾向が見られました。

コラム ②

P.7 コラム①より続く

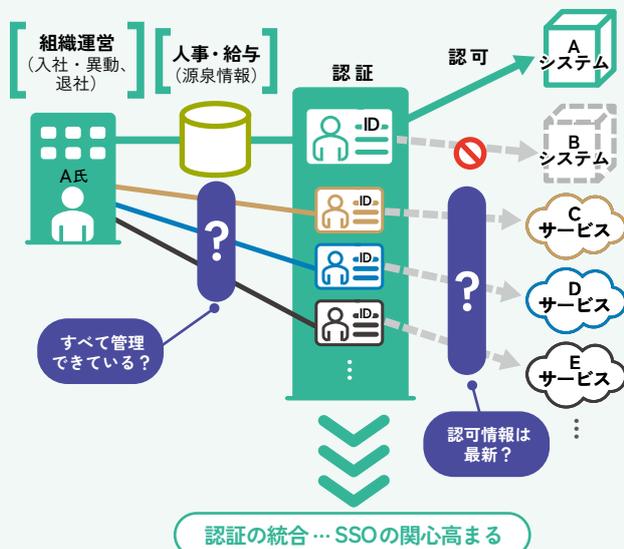
リモートワーク化で浮き彫りになったID管理の課題…まずは認証統合へ

これまで、リモートワークの普及に伴い、SaaSなどの利用も加速してきました。その結果、従来のシステムへのアクセスに加え、SaaSにアクセスするためのID/パスワードが増加したことで、次のような課題が生じました。

- ユーザー、管理者ともにID/パスワードの管理が複雑化
- 人事情報と連携できていない、人事異動者・退職者のID削除や権限変更漏れなどが発生しやすい

こうした課題のうち、IDによる「認証」統合に向けた普及が進んでいるのがSSOです。しかし、まだ「認可」の問題は解決されたわけではありません。

⇒ P.14 コラム③に続く



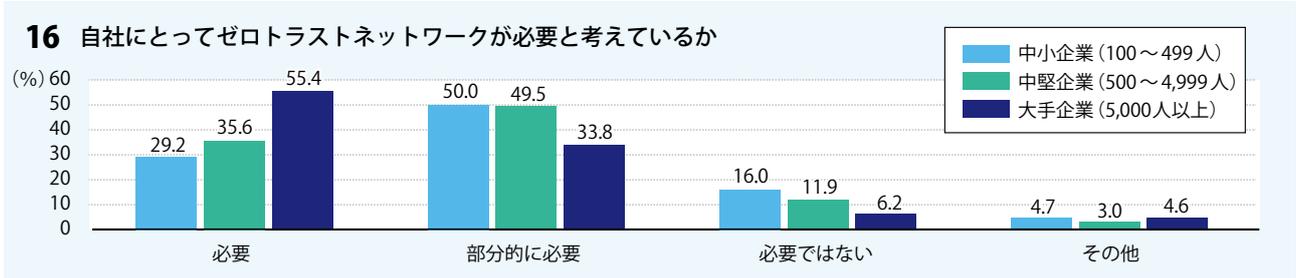
4

これからのID・アカウント管理とゼロトラスト

ゼロトラスト需要は拡大、SSOや多要素認証、パスワードレス認証が次のテーマ

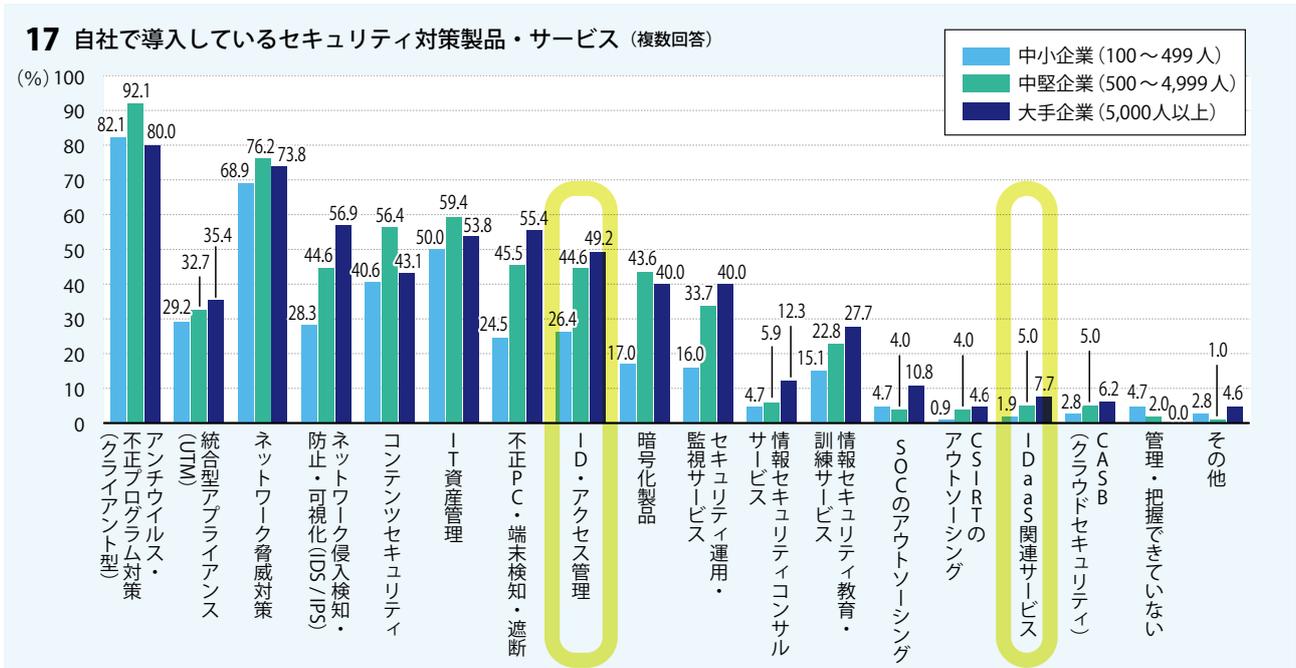
セキュリティ対策として境界防御のみでは限界があると知られてきた昨今、ゼロトラストの考え方が普及してきます。その時に重要となるID・アカウント管理について、セキュリティ対策とともに調査結果をまとめました。

ゼロトラストが部分的にでも「必要」な大手・中堅は約90%に上る



ゼロトラストが「必要」と考える大手企業は非常に多く、55.4%と過半数に上りました。また、「必要」と「部分的に必要」を合わせると、大手・中堅企業ともに約90%に上りました。一方、中小企業は「必要」が29.2%と少ないものの、「必要」と「部分的に必要」を合わせると約80%となり、その必要性の認識が広がっていることがわかりました。

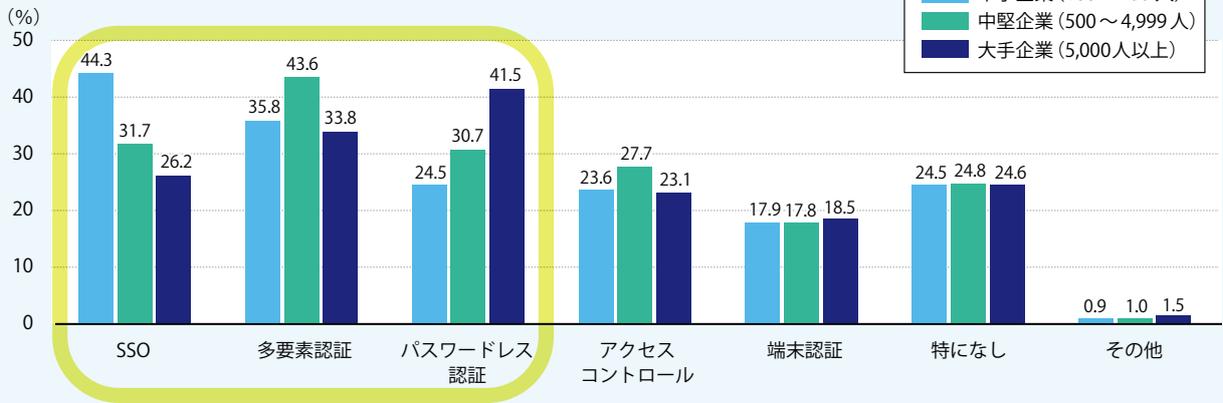
セキュリティ対策は境界防御が中心、ID管理/IDaaS導入は大手・中堅で約半数



ゼロトラスト推進に向け、従来型の境界防御からIDを新たな境界とした防御への切り替えが必要とされています。その中で、「ID・アクセス管理」は大手企業が49.2%、中堅企業は44.6%、中小企業は26.4%、「IDaaS関連サービス」は大手企業が7.7%、中堅企業は5.0%、中小企業は1.9%という結果でした。現状はまだ、多くの企業が従来型の境界防御が中心と考えられます。

中小は「SSO」、中堅は「多要素認証」、大手は「パスワードレス認証」がネクストステップ

18 今後、自社で認証強化を実施したい内容 (複数回答)



今後、自社で認証強化を実施したい内容として、「SSO」、「多要素認証」、「パスワードレス認証」が企業規模に応じて特徴的な傾向を示しています。

中小企業は「SSO」が44.3%で、企業規模が大きくなるほど減少傾向となり、これはすでに対応済みであると考えられます。中堅企業は「多要素認証」が43.6%と高く、中小企業はまだスコープ外、大手企業は対応済みと推測できます。大手企業は「パスワードレス認証」が41.5%で、中堅・中小は検討中かそれ以前と推測されます。認証強化を検討している企業は、自社の企業規模とあわせてこの結果を参考にしてみたいかがでしょうか。

コラム ③

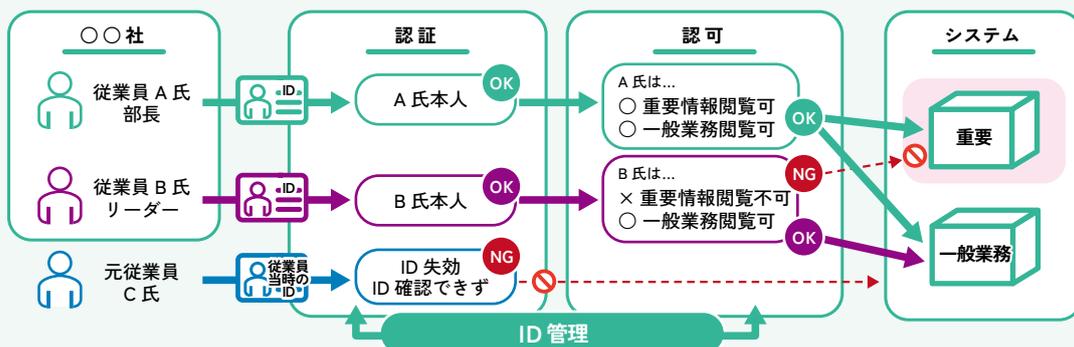
P.12 コラム②より続く

ゼロトラストの実現に向け、源泉情報とIDの直結が必要

「人事情報(源泉情報)とID情報は一致」することがシンプルなID管理の基本です。しかし、SaaSの増加などでIDが増加し、その管理は複雑化しました。そこで、「認証」を統合するためにSSOの採用が進んでいます。さらに「認証」の強化に向けて多要素認証やパスワード認証を検討している企業が増えています。

一方、「認可」ではIDによる都度評価を行うことが課題となっていました。それには、人事情報(源泉情報)とIDの追加・更新・削除のサイクルを直結し、IDの鮮度を保つことが必要です。そうすることで、「認証」と「認可」情報を最新の状態維持できるようになります。

このように、源泉情報との直結、認証、認可といったそれぞれのポイントを押さえておけば、ゼロトラスト環境の実現に向け一歩近づくことになります。ID管理製品を検討する際には、これらを統合的に管理できることをポイントにしてみたいかがでしょうか。



まとめ

人事情報とIDを直結できる統合認証基盤でゼロトラスト推進へ

IDが新たな境界線となった今、認証用・認可用のIDは常に最新化すべき

多くの企業がID・アカウント管理の複雑化を課題として挙げる中、その実態をアンケート調査結果とコラムで読み解いてきました。これまでの流れをID管理の歴史とともに整理します。

- ① 人事情報（源泉情報）とID情報が一致するべき
- ② クラウド、リモートワーク利用で増加したIDを管理するために認証統合（SSOの普及）
 - … ハイブリッドクラウドの時代へ、境界防御セキュリティは限界を迎える
- ③ 認証統合により、認可のためのIDを最新化しその都度確認する必要がある
 - … ゼロトラスト時代の到来

ゼロトラスト時代に入り「IDがセキュリティの新たな境界線」となった今、認証用のID情報と認可用のID情報をセットで最新化する仕組みが求められるようになったのです。これが、ID管理の「新たな複雑化」をもたらしています。

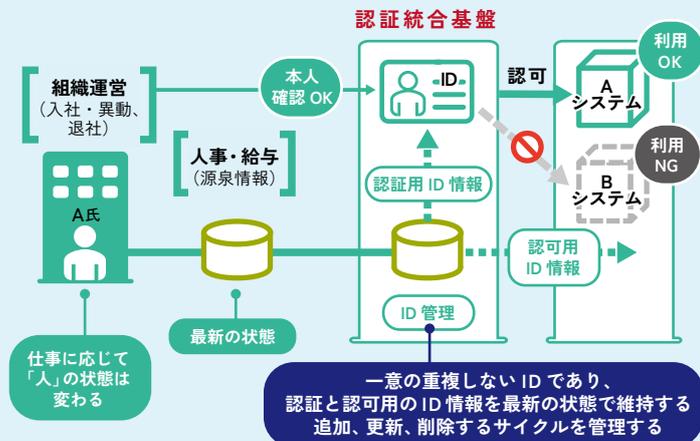


ID管理の「新たな複雑化」を解消するために

ゼロトラストの根幹は、人事情報から「その人本人か? (認証)」、「利用権限をその都度IDで確認 (認可)」するという仕組みを持つことです。人事情報(源泉情報)と直結し、常にIDの鮮度を保ち、IDのライフサイクル管理を適正に行う認証統合基盤を持つことが、先に挙げた「新たな複雑化」の解決策となります。

今、大手企業では認証の強化と効率化のためにSSOや多要素認証の導入を先行し、中堅企業・中小企業はこれに追従していることが今回のアンケート結果から読み取れました。

このように、人事情報からID情報・認証・認可の情報が直結している体制を構築することが、ゼロトラストセキュリティの実現に向けて不可欠であり、今後、企業規模を問わずに進むべき道筋であると言えます。



ゼロトラストを支える統合認証ID基盤

<div style="display: flex; flex-direction: column; align-items: center; justify-content: center;"> <div style="background-color: #2e8b57; color: white; padding: 5px; margin-bottom: 5px;">認証</div> <div style="background-color: #1e90ff; color: white; padding: 5px; margin-bottom: 5px;">認可</div> <div style="background-color: #0070c0; color: white; padding: 5px;">ID管理</div> </div>	認証統合 SSO <ul style="list-style-type: none"> ● 認証強化 ● シングルサインオン
	アクセス権限管理 <ul style="list-style-type: none"> ● 組織、役職に応じた権限管理 ● 適切なライセンス付与・はく奪
	アカウント管理 <ul style="list-style-type: none"> ● 各システムへIDの更新、追加、削除 ● パスワードのリセット、変更
	属性情報管理 <ul style="list-style-type: none"> ● システム固有の属性情報管理 ● 認可情報の生成、更新、削除
	ライフサイクル管理 <ul style="list-style-type: none"> ● 入退社、有効期限や適用日の管理 ● 源泉情報との直結がIDの鮮度を保つ

おわりに

本資料では、大手企業、中堅企業、中小企業に分類し、取り組み状況をより具体的に解説しました。本資料を通じて、ID・アカウント管理に取り組んでいる多くの企業において重要な施策の1つであることをご理解いただくとともに、セキュリティレベルの向上や組織の生産性向上にお役にてください。

また、最新のID・アカウント管理の動向やおすすめ情報は随時提供していますので、ぜひ下記URLよりご覧ください。ご相談もまた、下記の連絡先よりお問い合わせください。

エクスジェン・ネットワークスのプロダクトの紹介



オンプレミス型：統合ID管理パッケージ

>>> 日本固有のID運用課題を解決する



SaaS型：ID連携に強いIDaaS

>>> シンプル、簡単なID運用を実現する



2022年度 統合ID管理パッケージ市場

年間出荷本数 1位

※出典：デロイト トーマツ ミック経済研究所発刊
『個人認証・アクセス管理型セキュリティソリューション市場の現状と将来展望 2023年版』
<https://mic-r.co.jp/>

ID・アカウント管理に関するご相談はこちら

<https://www.exgen.co.jp/>

資料公開 2023年5月



USE INNOVATIVE TECHNOLOGY.

エクスジェン・ネットワークス株式会社

〒101-0052 東京都千代田区神田小川町 1-11 千代田小川町クロスタ 11F

| TEL : 03-3518-8055 | FAX : 03-3518-8056 | E-mail : idminfo@exgen.co.jp |

<https://www.exgen.co.jp/>