ID管理システム導入における現状把握チェックリスト

（第１版）

特定非営利活動法人　日本ネットワークセキュリティ協会
標準化部会　アイデンティティ管理　ワーキンググループ
チェックリスト作成分科会
２０１７年7月１２日

目次

ごあいさつ

本書は「ID 管理システム」導入時に課題となる「システム化の範囲」ついて、指標となるチェックリストを提示し、各企業や団体がどの程度 ID 管理ができているのか、またどの部分が不足しているのかを定量的に知ることが可能とするためのものである。
また、提案する SIer・ベンダにおいては、提案時におけるシステム化の範囲についての根拠とすることが可能となり、顧客との齟齬が発生しにくいメリットがある。

本書の作成にあたったワーキンググループには、ID 管理製品の開発・販売ベンダ、導入経験のある SIer・コンサルタント等が多数参加しており、特定の製品に偏向しないことを留意しつつも、ID 管理システムを導入するユーザ、SIer 等にとって有用となる知識・ノウハウを持ち寄った。

これから、ID 管理システムを導入検討する人には、プロジェクトの推進のツールとして、また、現在 ID 管理やロール管理システムを導入中の人にとっては、現在のプロジェクトをよりよくするためのチェックツールとして、活用していただけると考えている。

なお、本書は「日本ネットワークセキュリティ協会（JNSA)」の「アイデンティティ管理ワーキンググループ」にて複数年に渡って検討した内容となっており、ワーキンググループに参加いただいたすべての方々のご協力に深く感謝する。

本書があらゆる企業において、ID 管理システムの適切な導入・運用に貢献できれば幸いである。

特定非営利活動法人　日本ネットワークセキュリティ協会
標準化部会　アイデンティティ管理　ワーキンググループ
リーダ　宮川 晃一

１．チェックリスト作成の背景と目的

１－１．背景

クラウド利用の加速や企業 M&A などを背景とし、企業や組織における ID 管理やアクセス・コントロールの重要性は以前にもまして大きなものとなってきている。そのような環境において多くの企業において ID 管理・アクセス管理を目的とした IT システムの導入が検討され、実際に導入が進んでいるが、システム化を検討する段階において必ず直面する課題が「１．どのようにシステム化の検討を進めれば良いのか？」、そして「２．どこまで厳密に管理・制御を行う必要があるのか？」という点において圧倒的に情報が不足している、という事実である。

1 番目のシステム化検討の進め方については本ワーキンググループの主要成果物の一つである「クラウド環境におけるアイデンティティ管理ガイドライン（2013 年改訂）」にてある一定の指針を示すことが出来ているが、2 番目の実際どこまで厳密に管理・制御を行うべきか、という点については定量的な指標や水準と呼べるものが、業界に特化した規定の類を除き、ほぼ存在していないのが現状である。

このことにより、例えば ID 管理システムを導入しようと考えている企業や組織の担当者が必要と考えている取り組み内容と、IT ベンダやコンサルタントからの提案内容やコスト感に乖離が発生し、プロジェクト自体が頓挫するケースも散見されるため、ID 管理・アクセス管理における定量的な基準となりうる評価軸と評価基準を定めることが急務である。

１－２．目的

先に述べた通り、企業や組織の担当者の期待事項と IT ベンダ・コンサルタントの提案内容の乖離など、ID 管理システム導入プロジェクトの円滑な推進を妨げる様々な阻害要因がプロジェクトの各フェーズにおいて存在している。

ここで、今一度企業や組織における ID 管理システム導入を検討する際に課題となる事項を、導入対象となる企業・組織側、および導入を行う IT ベンダ・コンサルタント側の各目線から整理すると、やはり上流工程、特に企画（提案）フェーズにおける課題をクリアしておくことが、プロジェクトのスタートラインに立つうえで最も重要な事項としてとらえることが出来る。このフェーズで頓挫するとプロジェクト自体が始まらず、先のガイドラインに記載したプロジェクトの進め方のベストプラクティスを活用することすら不可能となるためである。

表１）上流工程におけるプロジェクト推進を阻害する要因の例

フェーズ	導入対象となる企業・組織の目線	IT ベンダ・コンサルタントの目線
企画（提案）フェーズ	● 進め方がわからない ● 自組織の現状がわからない ● あるべき姿がわからない ● 必要な予算がわからない ● ベンダの見積もりが高額 ● 企画の通し方がわからない	● 導入対象の企業・組織が何を求めているのかわからない ● 現状がわからない ● わからないのに総額コストの提示を要求される
要件定義フェーズ	● 自社にあったあるべき姿がわからない ● IT ベンダ・コンサルタントの提示するソリューション・システム化計画の妥当性がわからない	● 過剰と思える機能要求があった時、一般的に妥当な達成水準が示せず、カスタマイズが増え、コスト増となる

この工程において不明な点が多いと、IT ベンダやコンサルタントは「わからないことを、わかるようにするためのフェーズ」が必要と判断し、企業・組織側へ必要となるコストを要求する。しかし、企業・組織側がそのコストの計上する気がなかったり、必要性を組織内で説明できず計上できなかったりすると、そこで企画自体が頓挫することも多い。

また、よくわからない状態のまま見切り発車で企業・組織が RFP を作成してしまい、IT ベンダやコンサルタントは不明点＝リスクととらえて予算を大幅に超えた提案が行われてしまい、プロジェクト自体が頓挫する、という不幸な事態に見舞われる。

本チェックリストは、プロジェクトを開始する際に行うべき現状分析を客観的に行うための評価項目および評価基準を作成することにより、特に上流工程におけるプロジェクトの頓挫を少しでも減らすことを最大の目的としている。

１－３．目標とスコープ

本チェックリストの作成にあたり、本ワーキンググループでは 2 つの目標を策定した。1 つ目は現状分析を行う際に使用する「評価項目の策定」であり、先に挙げた本ワーキンググループの主要成果物である「クラウド環境におけるアイデンティティ管理ガイドライン」の付録であるテンプレート「要件定義の観点一覧」、およびクラウドセキュリティアライアンスが発行している「CCM（クラウド・コントロール・マトリクス）」を参考に、１．全般、２．データ源泉、３．対象システムの 3 つの観点で評価項目を整理している。2 つ目は各評価項目に関する評点の基準値を設定した「評価基準の策定」である。企業・組織は評価軸に沿っ

て現状調査を行い、評価基準と照らし合わせることで現状の把握度合を客観的に評価することが出来、ベンダはシステム導入対象となる企業・組織の現状把握の度合によりプロジェクトのリスクを定量的に分析することが可能となる。

尚、2つ目の評価基準の策定に関しては、1つ目の評価項目を利用した現状分析を行った結果のデータをある程度蓄積・分析を行った上で例えば業界や組織の規模などから基準値を策定していくといったアプローチが必要となるため、本書における策定スコープからは外しており、2017 年度以降で順次策定を進めていく予定である。

表2）目標とスコープ

目標	内容	スコープ
評価項目の策定	企業・組織が現状分析を行う際の評価軸・項目の一覧。以下の観点で項目を整理。 １．法令、管理ポリシー／ルール ２．ID データ（対象、保証レベル、整理状況） ３．対象システム（概要、ID 関連機能）	○
評価基準の策定	評価項目ごとの達成度合いの基準値（業界単位など）	× （FY17 以降）

２．チェックリストの利用方法

２－１．評価軸・項目に関する基本的な考え方

前章でも述べた通り、本チェックリストは企業・組織の現状分析を支援することを目的としている。そのため、評価軸・項目は例えば「パスワードの複雑性を満たしているか？」などといった具体的な施策の内容を確認するのではなく、「各項目についてどこまで把握しているか？」を確認することに重点を置いている。

２－２．チェックリストの構成

前章で述べた通り、本チェックリストは企業・組織の現状を「法令／管理ポリシー」、「IDデータ」、「対象システム」の３つの観点より評価するものである。各観点はカテゴリ、サブカテゴリ、実際の評価項目という順で細分化されており、評価実施者は最下層の評価項目それぞれについて現状評価を行い、結果を記入していく。

評価の観点は下表のとおりである。

表３）評価の観点

評価の観点	解説
法令／管理ポリシー	対応すべき法令や社内ルールの把握度合や、管理ポリシー・標準の策定度合
ID データ	管理対象となる ID データの把握度合、源泉の状況（保証レベルなど）の把握度合
対象システム	連携対象となるシステムに関する状況・仕様の把握度合 ※連携対象となるシステム単位で評価

観点毎のカテゴリ、サブカテゴリは下表（表４～６）の通りである。

表４）法令／管理ポリシー

カテゴリ	サブカテゴリ	解説
法令関係	個人情報保護	業界毎の状況を含め、遵守すべき関連法規とその対応状況の把握度合
	業界固有関連法規類	
管理ポリシー/ルール	認証	ID、アクセス管理に関連する管理ポリシーや組織内のルールの策定、対応状況の把握度合
	ID 管理	
	ロール/アクセス権管理	

表５）ID データ

カテゴリ	サブカテゴリ	解説
管理対象	ー	管理対象となる ID の種別の把握度合（利用者、管理者、ユーザ以外、など）
保証レベル	正社員	各 ID の源泉における登録プロセスの正当性、正確性に関する把握度合
	非社員（派遣など）	
	社外利用者	
データ整理	マスタ	管理対象の ID に関連するマスタや取得できる属性、取得できる範囲などの把握度合
	属性	
	取得可能範囲	

表６）対象システム

カテゴリ	サブカテゴリ	解説
概要	用途/業務	対象システム全般に関する情報の把握度合
	システム	
	利用者数	
識別	識別子	ID 体系等の識別情報に関する把握度合
認証	認証方式	認証関連機能の状況に関する把握度合
	パスワード管理	
ID 管理	ライフサイクル全般	ID 管理関連機能の状況に関する把握度合
	削除/無効化	
	外部 I/F	
ロール/アクセス権限管理	ロール管理	ロール、アクセス管理関連機能の状況に関する把握度合
	特権 ID	

また、前章でも述べた通り、各評価項目を策定する上で、「クラウド環境におけるアイデンティティ管理ガイドライン」の付録であるテンプレート「要件定義の観点一覧」、およびクラウドセキュリティアライアンスが発行している「CCM（クラウド・コントロール・マトリクス)」を引用・参照しているため、項目毎に引用・参照元を記載しており、評価者が必要に応じて当該ドキュメントを参照することで詳細な要求事項などを確認することを想定している。

表７）引用元

引用元（略称）	引用元	参照先（Web サイト等）
CCM	クラウドセキュリティアライアンス発行「CCM（クラウド・コントロール・マトリクス）日本版バージョン 3.0.1」 引用箇所として CCM Control ID を記載（例：IAM-XX）	http://www.cloudsecurityalliance.jp/ccm_wg.html
ガイドライン	本 WG 発行「改訂新版 クラウド環境におけるアイデンティティ管理ガイドライン」 引用箇所としてテンプレート番号を記載（例：テンプレート XX）	http://www.jnsa.org/result/2013/idm_guideline.html

２－３．各項目の評価方法

各評価項目はカテゴリ、サブカテゴリ、観点、チェック項目の順にブレークダウンされており、最下層のチェック項目に関して把握度合を 4 段階で評価を行う。

表８）評価基準と評点

評点	評価	評価基準の例
4	おおよそ把握できている	調査済みで明文化・オーソライズされている状態
3	ある程度は把握できている	担当者レベルで把握している状態
2	少ししか把握できていない	担当者レベルでも把握しきれていない状態
1	ほぼ把握できていない	誰が担当者なのか把握できていない状態

尚、各項目について評価を行ったのち、カテゴリ毎に評点の平均値を取得して現状の把握状況の評価を行う。ただし、対象システムの観点については要件定義フェーズで重点的に調査を行うべきシステムを明確化するため、システム毎に評価を行う。

２－４．評価実施の例

本チェックリストには評価を実施する場合のサンプルを 2 パターン添付しているので、実際に評価を行う場合はサンプルを参考に評価を実施していただきたいが、ここで数項目実際の評価を行う場合の例を示しておく。

表９）評価実施の例

観点	カテゴリ	サブカテゴリ	評価項目	現状	評点
法令／管理ポリシー	管理ポリシー／ルール	認証	SSO システム、及び各アプリケーション認証方式は組織内で標準化されているか	一部の担当者で標準化を進めようと言う試みは行われているが全体へ適用されてはいない	2
ID データ	保証レベル	非社員（派遣など）	非社員の ID 登録を行う際の身元保証の実施状況を把握しているか	派遣社員の採用は部署単位で実施しており、身元確認に関するルールは存在しない	1
対象システム	ID 管理	外部 I/F	外部システムから ID を操作する I/F の有無、I/F 仕様を把握しているか	導入ベンダへ確認する必要がある	1

各項目について評価を終えると、自動的に各サブカテゴリの評点平均が計算され、評価結果グラフの作成が行われる。（対象システムが複数存在する場合は評価項目をコピーして追加評価を行い、グラフ対象となるデータ範囲の拡張を行う必要がある）

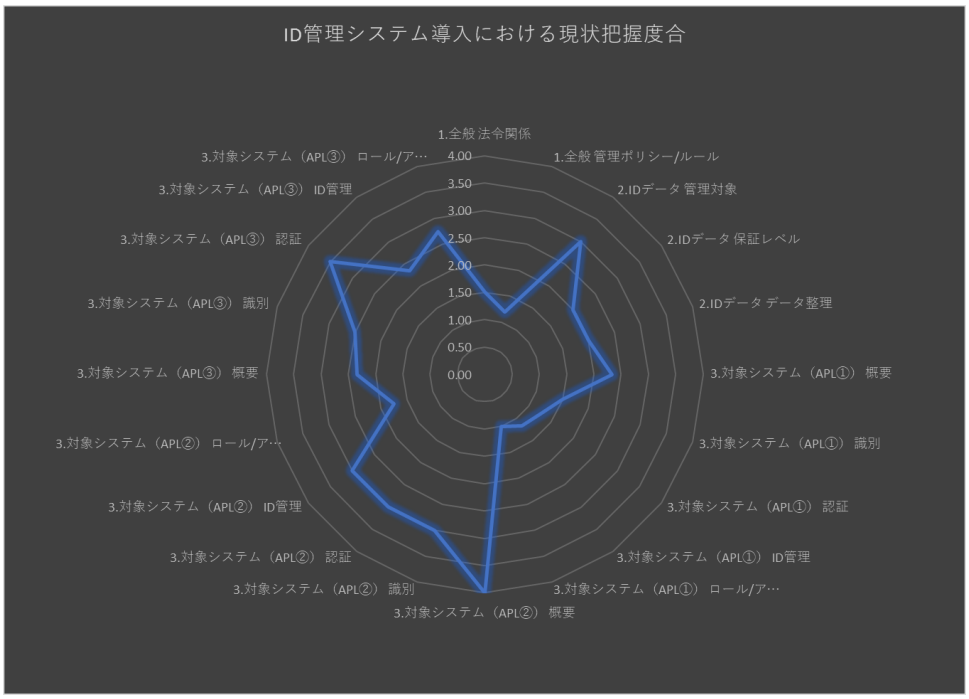

図１）評価結果グラフのサンプル

２－５．評価結果の利用方法

現バージョンのチェックリストでは基準となる評点を定めていないため、作成されたレーダーチャートを見て、把握できている点、出来ていない点の濃淡を把握し、把握できていない点については要件定義フェーズで重点的に調査を行う、という形で利用することを想定している。（評価基準の策定は 2017 年度以降に対応する予定である）

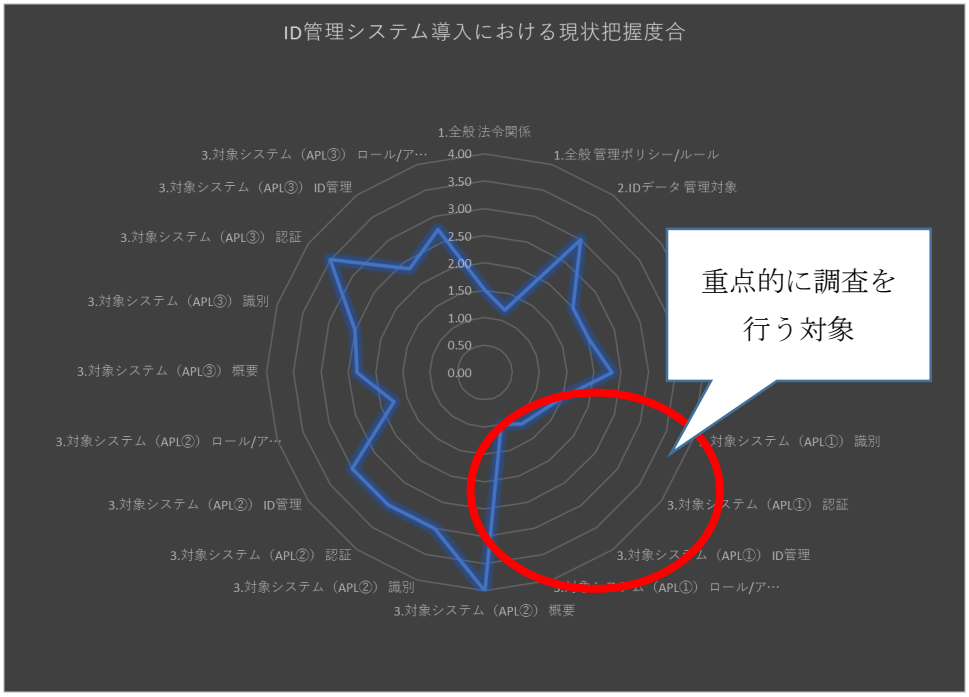

図２）評価結果の利用例

２－６．利用上の留意点

一般にチェックリストを利用した評価を行う場合に発生する課題として、「チェックリストに記載されている事項を満たすことが目的となってしまう」という手段の目的化の発生が挙げられる。本取り組みにおいても、そのようなリスクが存在することを把握しており、評価項目毎に「チェックの目的」との関連を記載している。チェックリストを利用する企業・組織の担当者、または IT ベンダ・コンサルタント各位においては、各項目を評価する際に「なぜ評価すべきなのか」「チェックリストに記載されていない項目であっても自組織にとっては確認すべき事項はないのか」について十分に検討して本チェックリストを利活用していただきたい。

３．チェックリスト作成分科会メンバ（社名五十音順）

WGリーダ

日本電気株式会社　宮川　晃一

チェックリスト作成分科会　リーダ

伊藤忠テクノソリューションズ株式会社　富士榮 尚寛

チェックリスト作成分科会　メンバ

株式会社アイピーキューブ　貞弘 崇行
株式会社インテック　木村 慎吾
SCSK 株式会社　深澤 聡
NEC ソリューションイノベータ株式会社　内田 健一
NEC ソリューションイノベータ株式会社　瀧沢 則之
株式会社エヌ・ティ・ティ・データ　山田 達司
エヌ・ティ・ティ・データ先端技術株式会社　杉村 耕司
KPMG コンサルティング株式会社　深谷 貴宣
日本アイ・ビー・エム株式会社　板倉 景子
日本電信電話株式会社　駒沢 健
日本マイクロソフト株式会社　安納 順一
富士通関西中部ネットテック株式会社　今堀 秀史
株式会社マインド・トゥー・アクション（サブスクライバ）　中島 浩光

協力団体

一般社団法人　日本クラウドセキュリティアライアンス（CSA ジャパン）