データベースセキュリティ安全度セルフチェック
統計データ

データベース・セキュリティ・コンソーシアム
DB セキュリティ安全度セルフチェック WG

Ver. 2.1　2010.02.15

目　次

1. はじめに

1.1. 目的

データベース･セキュリティ･コンソーシアム（以降、DBSC）から公開している「データベースセキュリティ安全度セルフチェック（以降、安全度セルフチェック）」の利用データからの統計を考察とともに公開することで、データベースに格納されている重要なデータを守るためのデータベースセキュリティを、より一層、適切に実施される様、啓発することを目的とする。

1.2. 前提事項

当資料は、安全度セルフチェックの利用データから導き出された統計を表及びグラフ化し、それぞれについて考察やコメントを記載した。

安全度セルフチェックの診断項目は、同じく DBSC から発行されている「データベースセキュリティガイドライン 2.0 版」をもとに作成しており、各対策の「必須／推奨」については情報資産の重みが「中」のものを想定している。

なお、当資料中にある「診断結果レベル」とは、安全度セルフチェックにより診断された結果であり、以下の通りとなっている。

レベル	説　明
A	重要とされる対策は十分に実施されている状態
B	いくつかの重要とされる対策が実施できてなく、不足している対策実施の検討が望まれる状態
C	実施できていない重要とされる対策が多く、早急な対策実施の検討が必要な状態
D	セキュリティ対策ができてなく、抜本的な改善･対策実施の検討が必要な状態

1.3. 注意事項

当資料は、2010 年 1 月 15 日時点の安全度セルフチェックの利用データをもとに作成している。

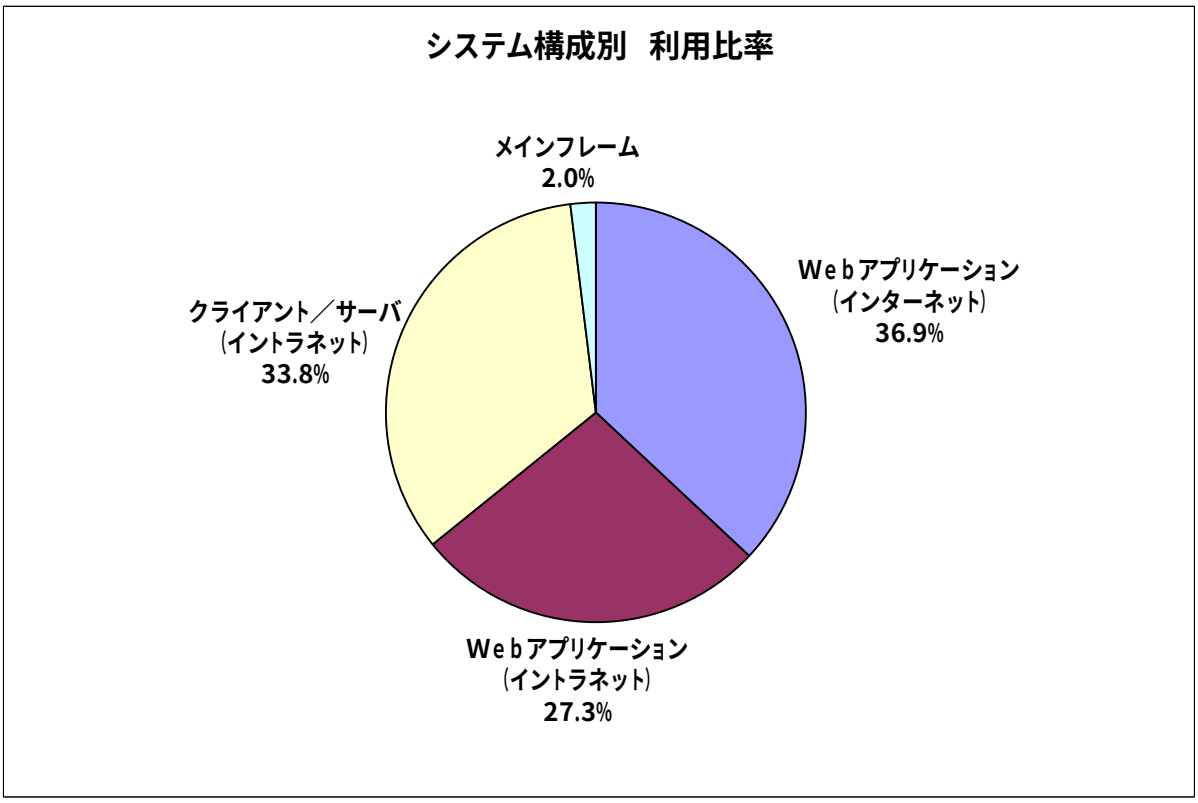
- 集計期間　　: 2009 年 2 月 17 日 ～ 2010 年 1 月 15 日
- セルフチェック件数　: 198 件

また、当資料を利用したことによって生じるいかなる損害に関しても、DBSC では一切の責任を負わないものとする。

2. アンケート項目別 利用比率

アンケートの項目別に安全度セルフチェックの利用比率を見ることで、データベースセキュリティへの関心度を知ることができる。

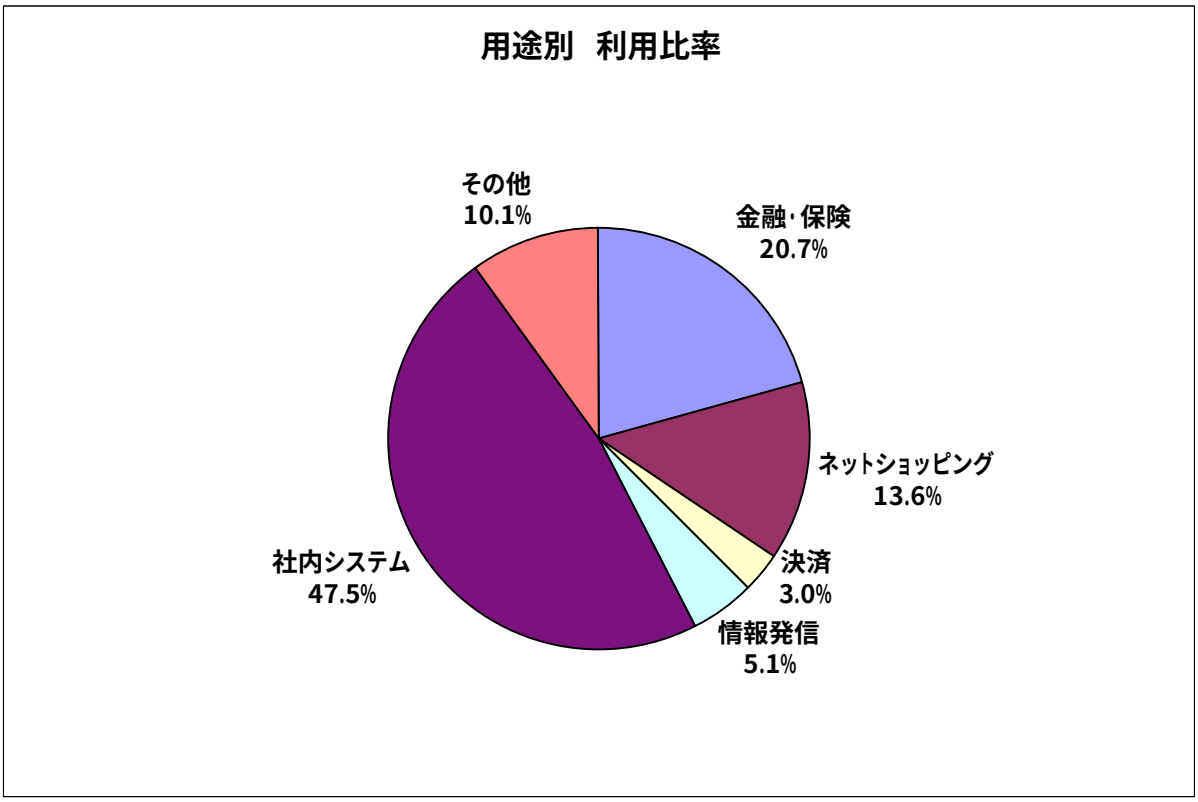
2.1. システム構成別 利用比率



システム構成別に見た場合、メインフレームを除いた各システムで、概ね均等に利用されている。

このことから、現在の主流と見られる Web アプリケーションだけでなく、従来型のクライアント／サーバのシステムも同様に、データベースセキュリティへの関心度が高いことが伺える。

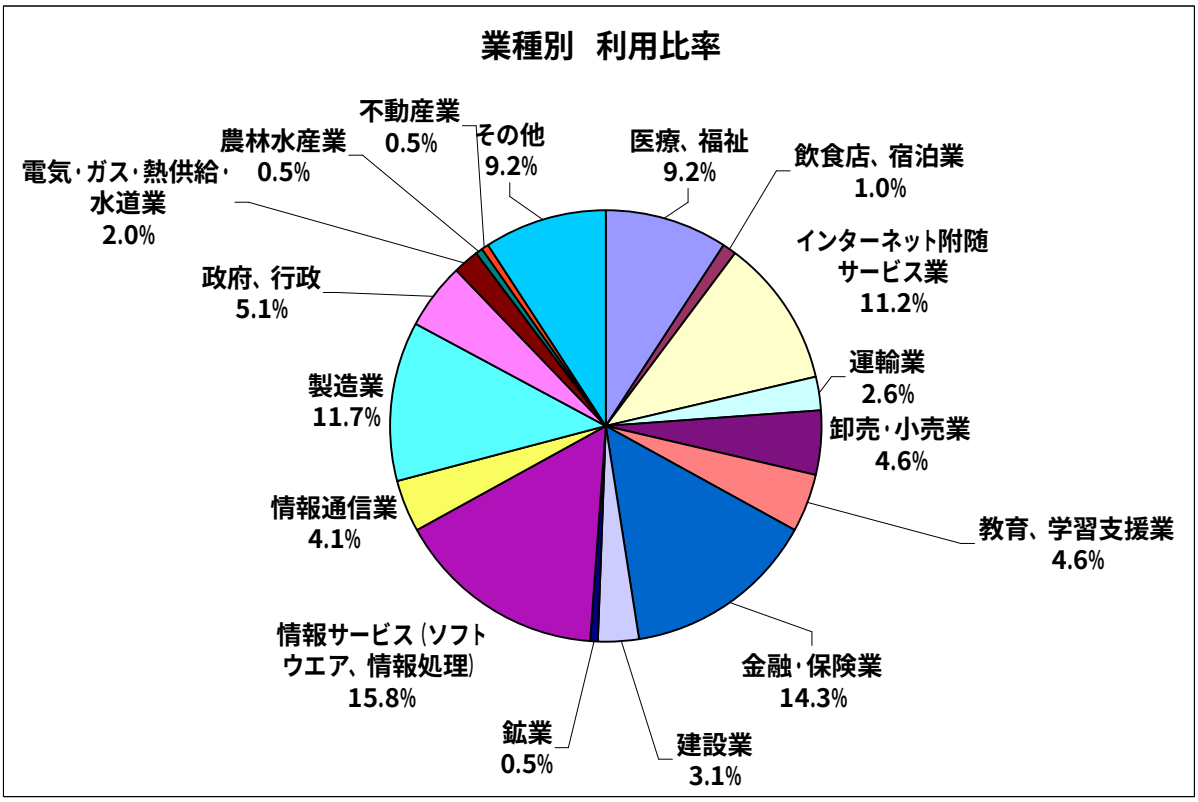
2.2. 用途別 利用比率



用途別に見た場合、「金融･保険」と「ネットショッピング」は個人情報をはじめとした機微な情報を取り扱うことからデータベースセキュリティへの関心度が高いと思われ、利用比率が高い結果となった。

また、「社内システム」が 45%超と多かったのは、ほとんどの企業が社内システムを所有し、絶対数が多いためと考えられる。

2.3. 業種別 利用比率

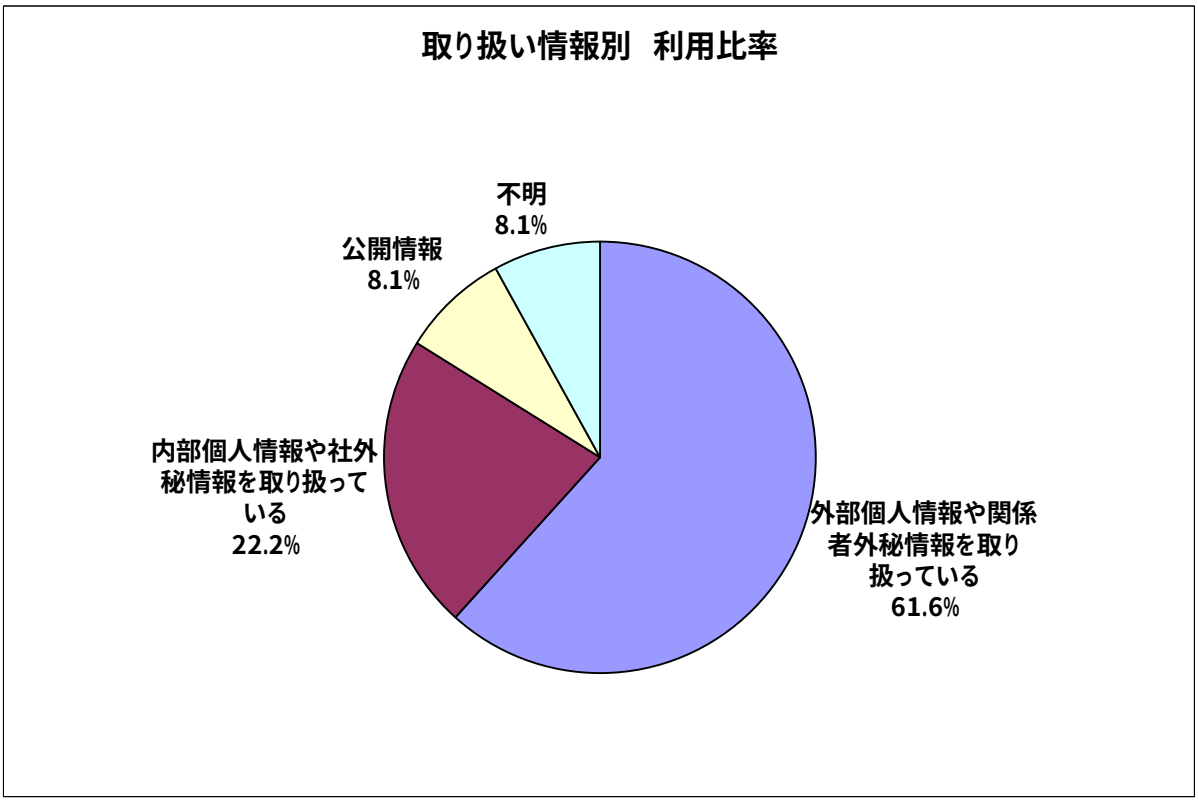


業種別に見た場合、各業種とも満遍なく利用されていることがわかる。

中でも、「医療、福祉」「インターネット附随サービス業」「金融・保険業」「情報サービス」「製造業」は利用比率が高い結果となった。

反面、「卸売・小売業」「情報通信業」「政府、行政」は、重要インフラを担っている業種の割に利用比率が低い結果となった。

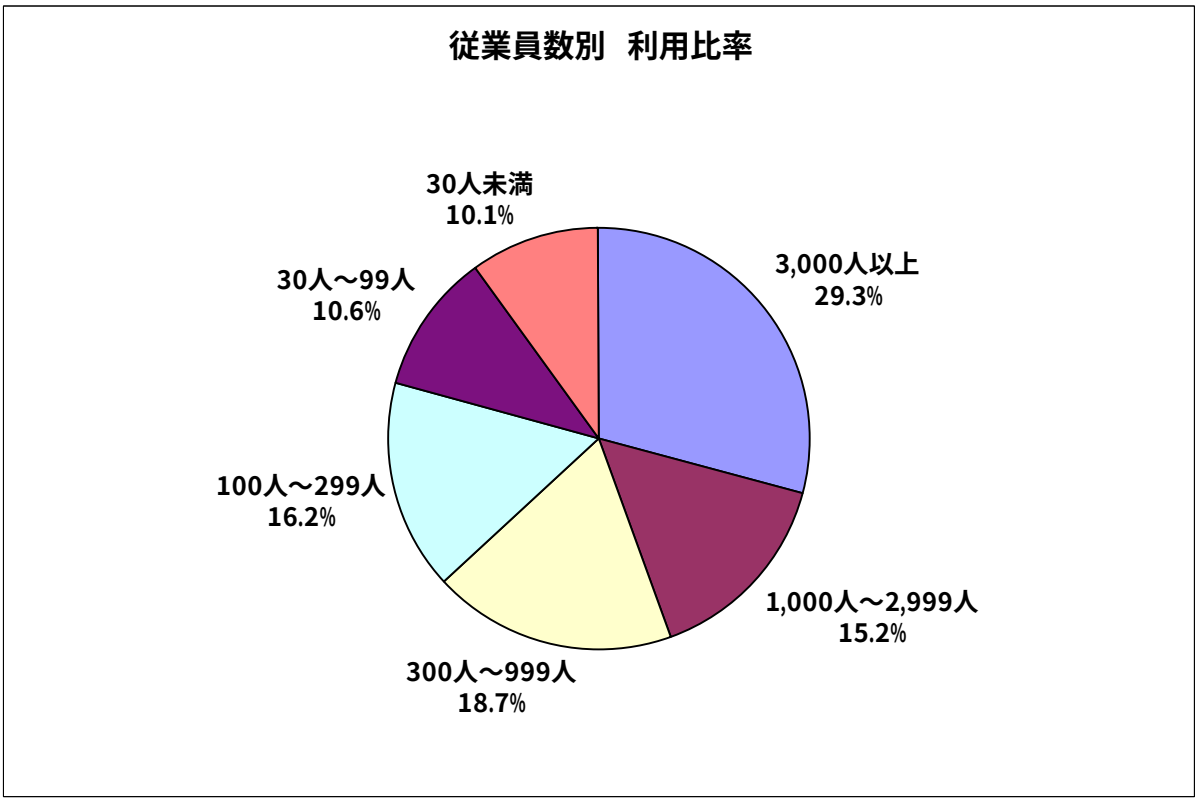
2.4. 取り扱い情報別 利用比率



取り扱い情報別に見た場合、やはり「個人情報や機密情報」などの情報を取り扱っているシステムほど、利用比率が高い結果となった。

この結果は、「取り扱っている情報の重要度が高いもしくは機微であるほど、情報を守ることが求められるため」と考えられる。

2.5. 従業員数別 利用比率



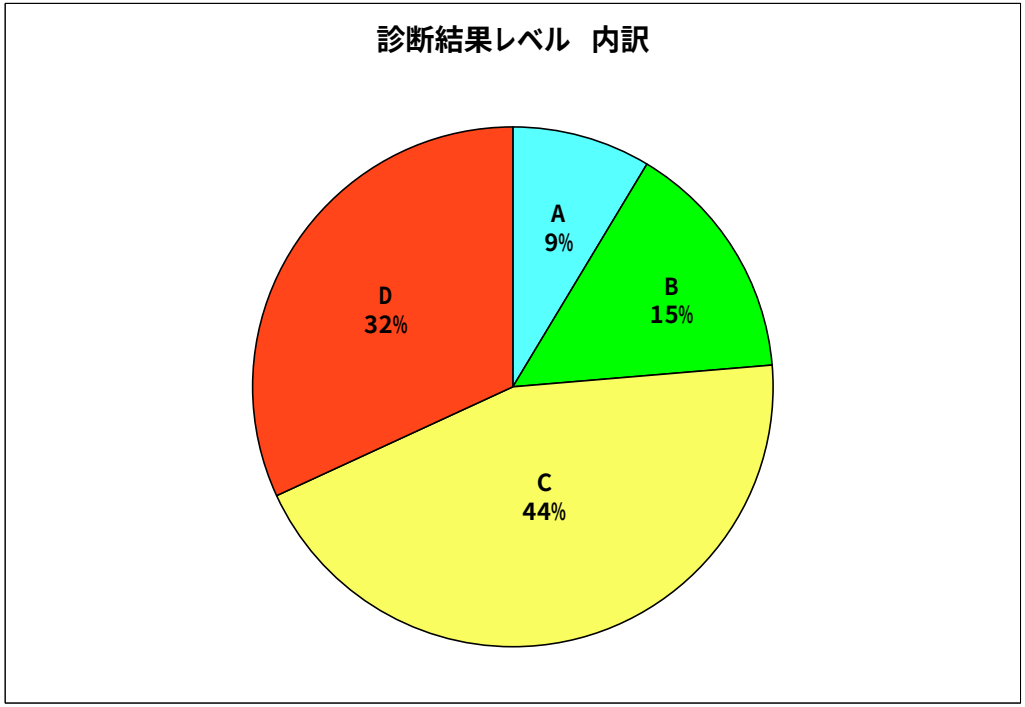
従業員数の多い／少ないに関係なく、満遍なく利用されていることがわかる。

従業員数が少ない企業のサイトであっても個人情報は取り扱うことが想定される。そのため、「重要な情報を守る」という観点から見れば、取り扱っている顧客数や個人情報数の多い／少ないに関係なく、十分なセキュリティ対策が必要である。

3. 診断結果レベル別 利用比率

診断結果のレベルを様々な切り口で分析することで、データベースセキュリティの対策実施度の傾向や、実施レベルの高低の理由などを知ることができる。

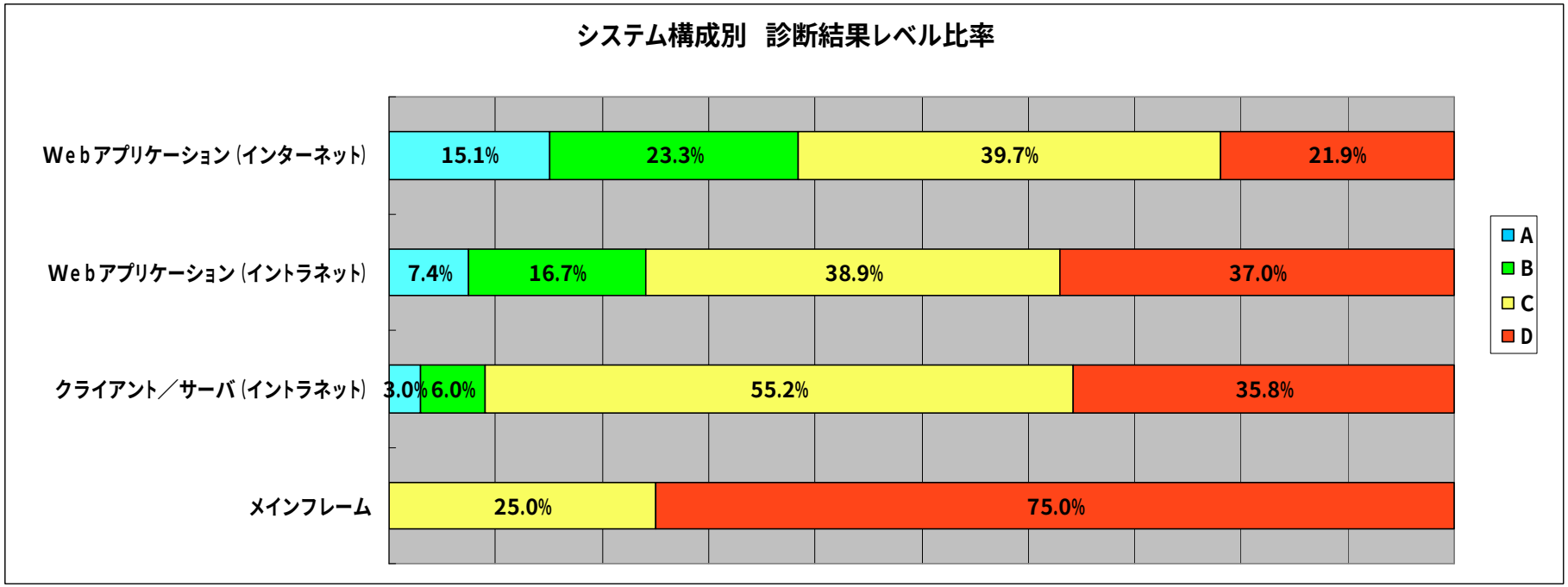
3.1. 診断結果レベル 内訳



診断結果レベルはCとDで80%程度を占めており、特にレベルDは「必須」とされている対策の半分以上ができていないレベルである。
ガイドラインで「必須」と定義されている対策は、「該当システムにおいて対応しなければ、セキュリティ上問題があると判断される対策」とされている。その必須対策のほとんどが実施できていないレベルDと判定されたシステムは、非常に危険な状態であると言える。

また、レベルCにおいても、実施できていない「必須」対策が多い状態であることから、至急、見直しを検討すべきである。

3.2. システム構成別 診断結果レベル比率

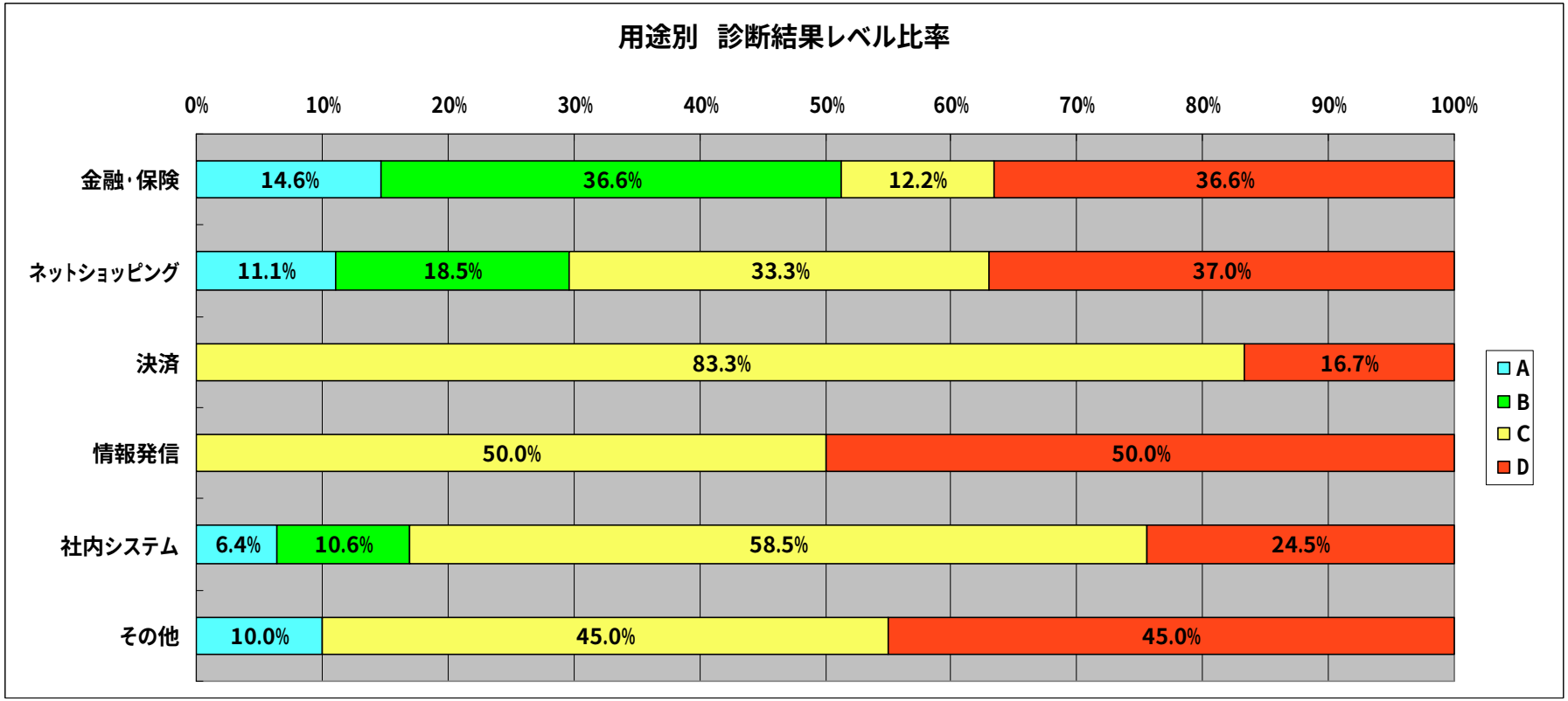


システム構成別に診断結果のレベルを見ると、「Web アプリケーション（インターネット）」が一番診断結果のレベルが高いことがわかる。以降、「Web アプリケーション（イントラネット）」「クライアント／サーバ（イントラネット）」「メインフレーム」と続いている。

最近の主流で且つ、比較的新しいシステムが多いと思われる「Web アプリケーション」でのセキュリティ対策実施度が高く、その中でも、外部の人間が利用するインターネット経由で利用するシステムの方が、社内利用となるイントラネットで使用するシステムよりも対策が実施されている結果となった。

また、メインフレームに関しては回答数が少ない（4 件）ために上記結果をそのまま鵜呑みにすることはできないが、「データベースで行うセキュリティ対策はあまり実施していない」という結果となっている。

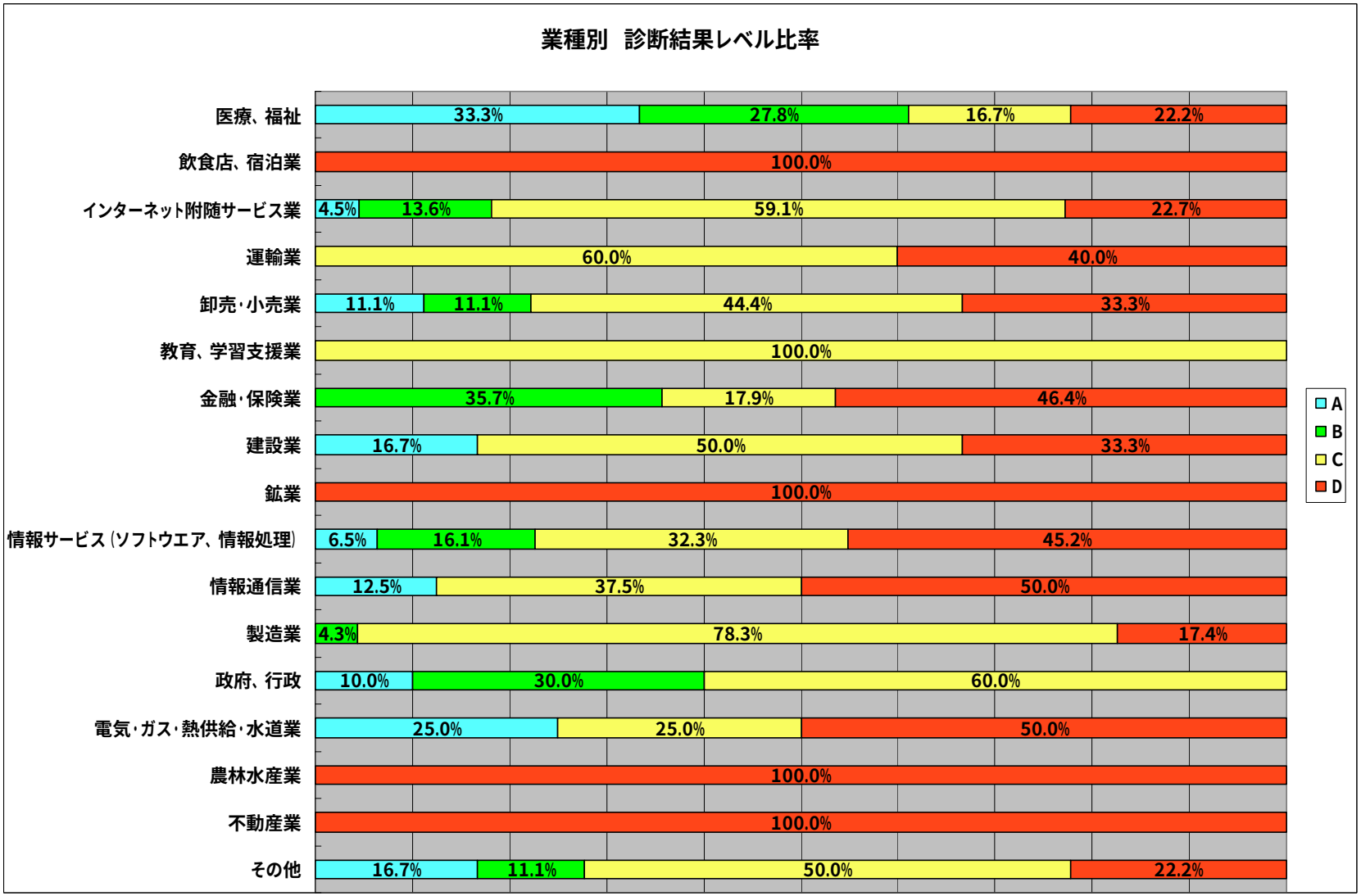
3.3. 用途別 診断結果レベル比率



用途別に診断結果のレベルを見ると、「金融･保険」は、レベル A＋B と C＋D で概ね半数ずつとなり、セキュリティ対策の実施度が 2 極化する傾向が見られた。
また、「社内システム」はセキュリティ対策を全く実施していないわけではないが、検討中や整備中というケースもあるのかも知れないが、まだまだ不十分な実施状況であると言える。

また、「決済」、「情報発信」、「社内システム」は、セキュリティ対策を全く実施していないわけではないが、まだまだ不十分な実施状況であると言える。

3.4. 業種別 診断結果レベル比率



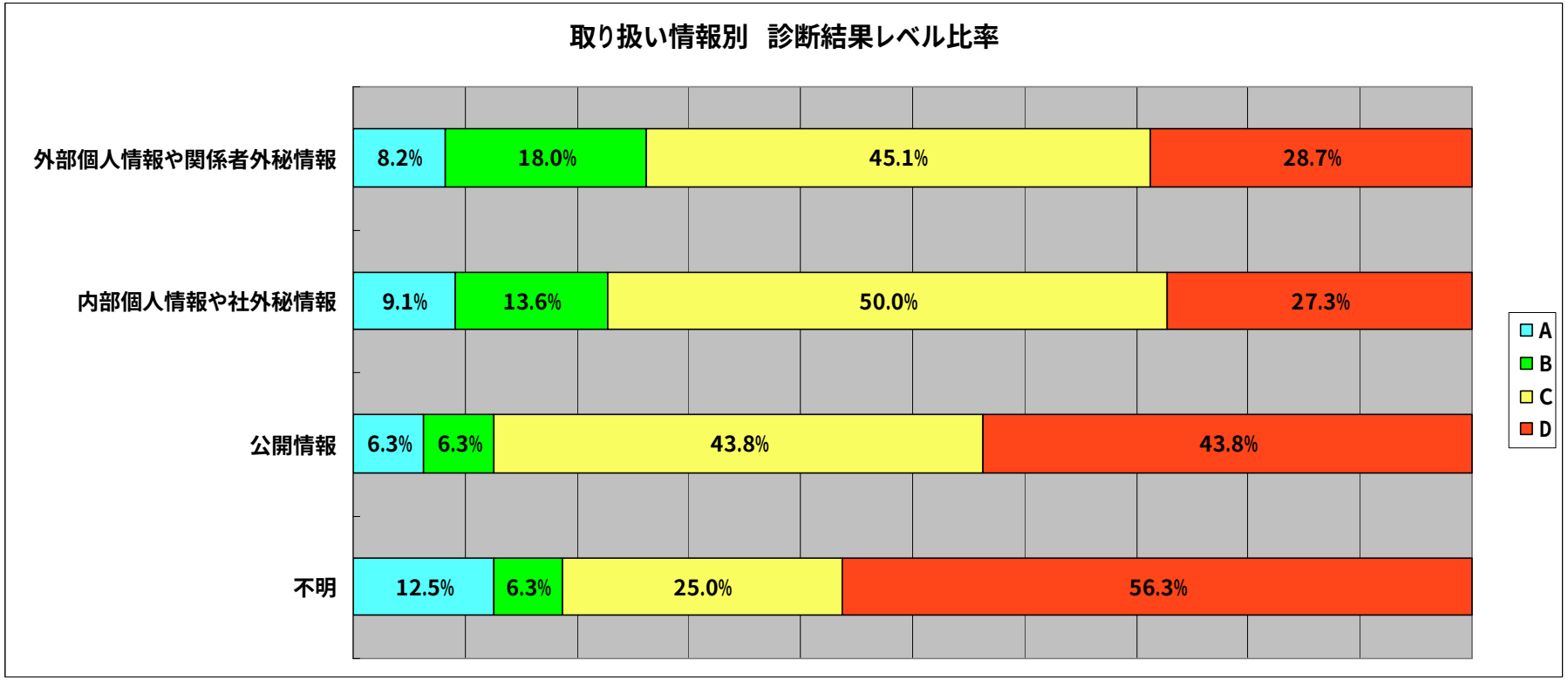
「医療、福祉」は診断結果のレベルが比較的高い結果となったが、取り扱っている情報を考慮すると、レベル D が 20%以上存在していて、非常に危険な状態と言える。

「金融・保険」は用途別に見た時と同様、セキュリティ対策の実施度が 2 極化する傾向が見られた。

「政府、行政」はレベル D が存在していないことから、何らかのセキュリティ対策が実施されていることが伺える。

いくつかの業種は、全くセキュリティ対策が実施されていない結果となった。但し、これらの業種は母数が少ないため、今後の推移を見守ることとする。

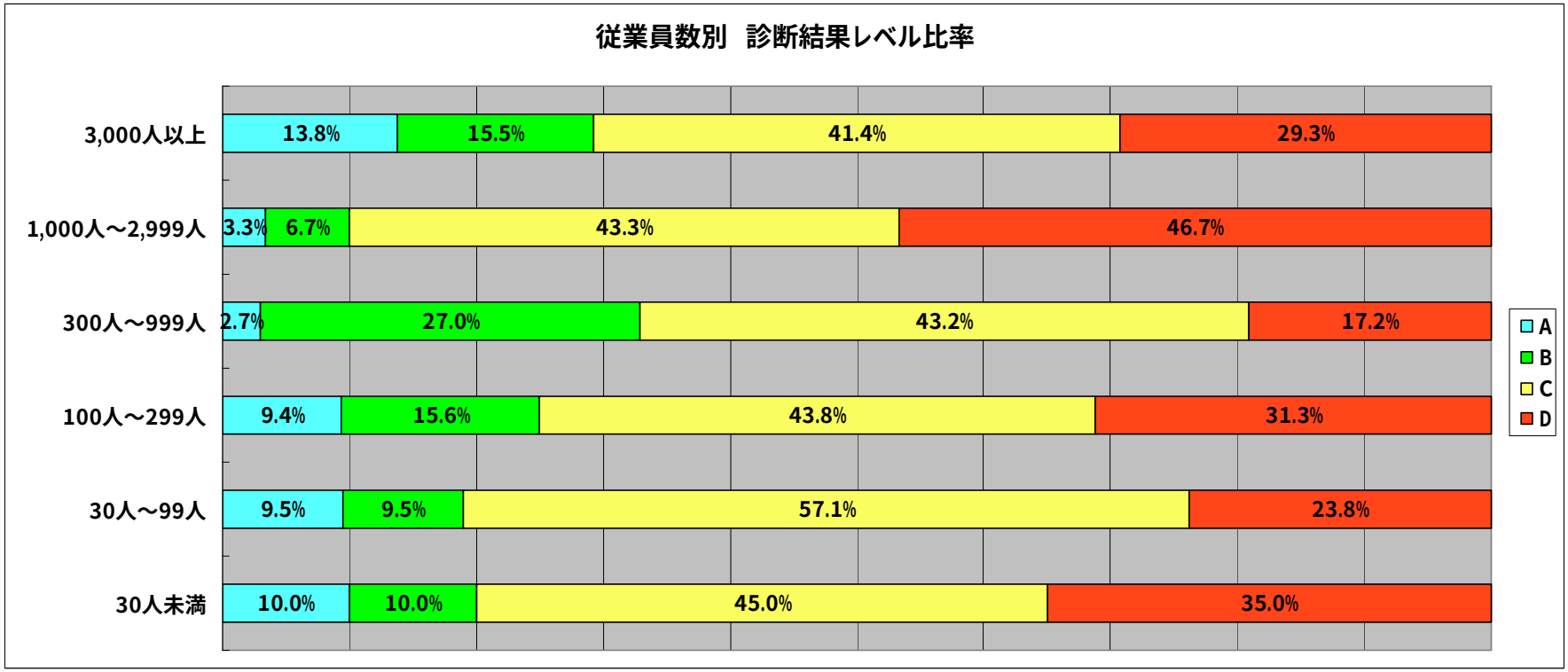
3.5. 取り扱い情報別 診断結果レベル比率



取り扱い情報別に診断結果のレベルを見ると、個人情報などの機微な情報を取り扱っているシステムではセキュリティ対策が比較的、実施されていることが伺える半面、ほとんど対策が実施されていないレベル D も 30%近く存在している。これは非常に危険な状態である。

取り扱っている情報の種類に関係なく、情報漏えいや改ざんなどが起こりにくくする様、セキュリティ対策を実施することが必要である。

3.6. 従業員数別 診断結果レベル比率



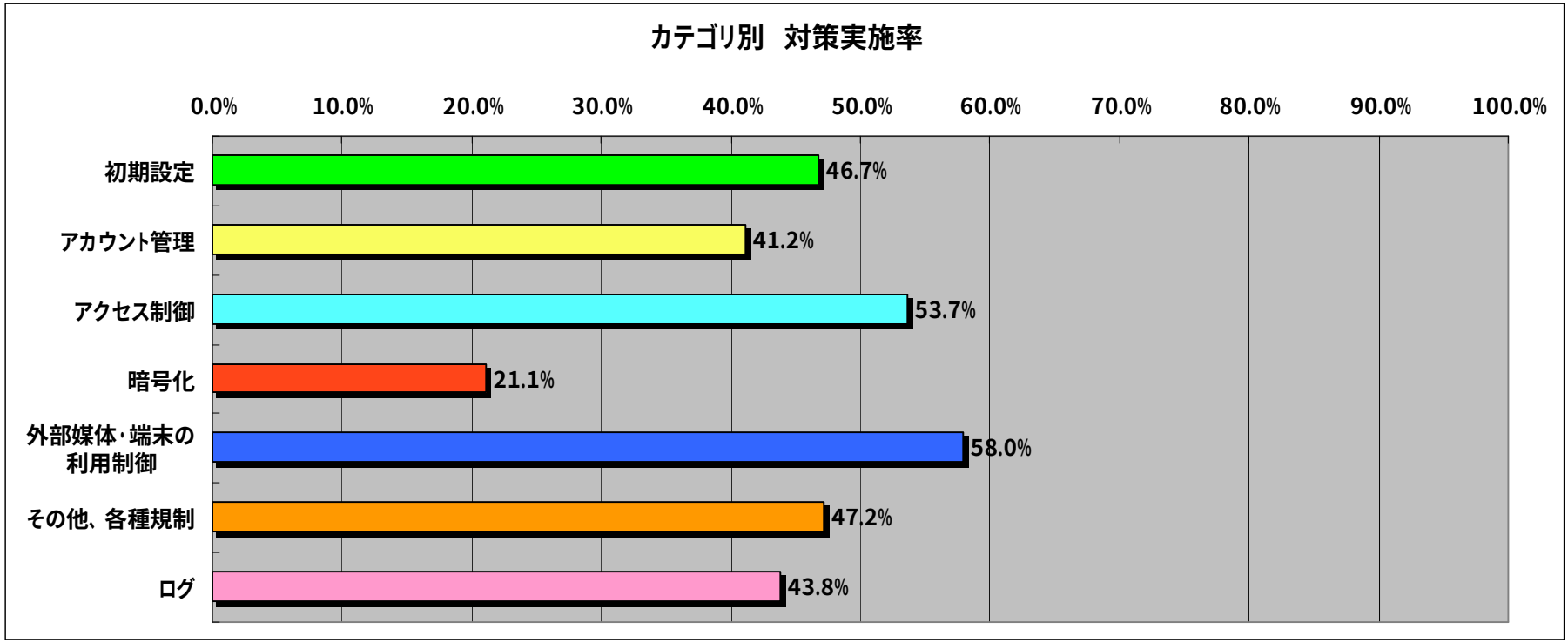
セキュリティ対策の実施レベルと従業員数の多い／少ないとの関連付けは見られなかった。
しかし、「1,000～2,999 人」だけ、他と比べて低い診断結果となった。

従業員数の多い／少ないに関係なく、被害に遭ってしまうことのない様、十分なセキュリティ対策の実施が必要である。

4. カテゴリ別 対策実施率

データベースセキュリティの対策実施率（実施できている率）をカテゴリ別に分析することで、対策の種類ごとの実施傾向を知ることができる。

4.1. カテゴリ別 対策実施率



カテゴリ別の対策実施率が一番低いのは「暗号化」であるが、「初期設定」や「アカウント管理」、「アクセス制御」の実施レベルまでもが、非常に実施率が低いということが問題である。

先ず、「初期設定」でできる対策を実施しないことには、該当のデータベースを堅牢にすることはできない。

更に、アカウントを適切に管理していなければ詳細なアクセス制御を実施することはできず、ログを取得しても操作した人物を特定することはできない。また、ア

クセス制御が適切に実施されていなければ容易に不正行為が可能となってしまう。

しかし、「初期設定」や「アカウント管理」、「アクセス制御」だけを実施しても万全ではなく、「暗号化」や「ログ」をはじめとした複数の対策を実施することで補完し合い、対策漏れをなくして、重要なデータを保護することが求められる。

4.2. システム構成･カテゴリ別 対策実施率

	初期設定	アカウント管理	アクセス制御	暗号化	外部媒体･端末の利用制御	その他、各種規制	ログ
Web アプリケーション（インターネット）	58.6%	53.6%	58.2%	38.1%	61.6%	54.6%	54.5%
Web アプリケーション（イントラネット）	38.0%	37.0%	43.5%	15.6%	49.6%	38.0%	37.0%
クライアント／サーバ（イントラネット）	42.2%	32.8%	60.1%	8.4%	61.8%	49.3%	39.9%
メインフレーム	*25.0%*	*9.4%*	*0.0%*	*0.0%*	*40.0%*	*4.2%*	*6.3%*

システム構成･カテゴリ別に対策実施率を見ると、「Web アプリケーション（インターネット）」に比べて「Web アプリケーション（イントラネット）と「クライアント／サーバ」はほとんどのカテゴリで対策実施率が低い結果となっている。

また、「メインフレーム」に関しては回答数が少ない（4 件）ため、今後の推移を見守ることとする。

4.3. 用途･カテゴリ別 対策実施率

	初期設定	アカウント管理	アクセス制御	暗号化	外部媒体･端末の利用制御	その他、各種規制	ログ
金融･保険	50.6%	52.1%	61.0%	42.0%	63.9%	63.4%	57.3%
ネットショッピング	48.1%	38.4%	49.1%	28.9%	55.6%	41.4%	34.3%
決済	*50.0%*	*62.5%*	*16.7%*	*16.7%*	*33.3%*	*30.6%*	*62.5%*
情報発信	55.0%	31.3%	45.0%	14.0%	34.0%	28.3%	27.5%
社内システム	44.7%	39.0%	56.6%	12.1%	63.0%	46.8%	41.2%
その他	41.3%	31.3%	46.3%	15.0%	45.0%	38.3%	43.8%

用途･カテゴリ別に対策実施率を見ると、「金融･保険」では比較的多くのカテゴリで対策が進んでいるが、その他の用途では全体的に低めの数値となった。

また、「決済」に関しては回答数が少ない（6 件）ため、今後の推移を見守ることとする。

4.4. 業種･カテゴリ別 対策実施率

	初期設定	アカウント管理	アクセス制御	暗号化	外部媒体･端末の利用制御	その他、各種規制	ログ
医療、福祉	58.3%	63.9%	65.3%	61.1%	70.0%	73.1%	75.0%
飲食店、宿泊業	*12.5%*	*6.3%*	*0.0%*	*0.0%*	*10.0%*	*8.3%*	*0.0%*
インターネット附随サービス業	54.5%	47.7%	46.6%	28.2%	48.2%	43.9%	50.0%
運輸業	40.0%	22.5%	30.0%	28.0%	40.0%	30.0%	20.0%
卸売･小売業	27.8%	36.1%	50.0%	17.8%	55.6%	38.9%	33.3%
教育、学習支援業	61.1%	37.5%	94.4%	13.3%	91.1%	61.1%	50.0%
金融･保険業	43.8%	38.8%	58.0%	19.3%	57.1%	54.8%	42.9%
建設業	58.3%	47.9%	25.0%	10.0%	46.7%	22.2%	41.7%
鉱業	*25.0%*	*37.5%*	*50.0%*	*0.0%*	*40.0%*	*0.0%*	*25.0%*
情報サービス（ソフトウエア、情報処理）	39.5%	36.3%	38.7%	18.7%	51.0%	38.2%	30.6%
情報通信業	43.8%	31.3%	46.9%	12.5%	45.0%	37.5%	43.8%
製造業	41.3%	35.9%	67.4%	4.3%	71.3%	55.1%	38.0%
政府、行政	75.0%	47.5%	70.0%	24.0%	76.0%	55.0%	60.0%
電気･ガス･熱供給･水道業	18.8%	28.1%	12.5%	0.0%	60.0%	25.0%	43.8%
その他	50.0%	50.0%	0.0%	0.0%	60.0%	50.0%	50.0%

業種･カテゴリ別に対策実施率を見ると、「医療･福祉」と「政府･行政」、「教育、学習支援業」については、多くのカテゴリで各対策の実施率が高かった。

反対に、「金融･保険業」と「情報サービス（ソフトウエア、情報処理）」については、全体的に低い数値となった。「金融･保険業」については、取り扱っている情報の性質から、もっと高い数値となってもよいものと思われる。

また、対策から見た場合、「アカウント管理」と「暗号化」「ログ」の実施率が低い業種が多かった。

先にも述べたが、アカウント管理は、他の対策の「アクセス制御」や「ログ」などにも関係してくる様に、非常に重要な対策であるため、必ず実施して欲しい。

なお、回答数が少なかった「飲食店、宿泊業（2件）」「鉱業（1件）」については、今後の推移を見守ることとする。

4.5. 取り扱い情報･カテゴリ別 対策実施率

	初期設定	アカウント管理	アクセス制御	暗号化	外部媒体･端末の利用制御	その他、各種規制	ログ
外部個人情報や関係者外秘情報を取り扱っている	48.8%	42.1%	58.6%	24.4%	63.4%	53.0%	47.5%
内部個人情報や社外秘情報を取り扱っている	45.5%	44.6%	47.7%	19.1%	56.4%	40.9%	43.8%
公開情報	39.1%	33.6%	40.6%	6.3%	43.8%	38.5%	26.6%
不明	42.2%	32.0%	45.3%	16.3%	35.0%	29.2%	32.8%

取り扱い情報･カテゴリ別に対策実施率を見ると、個人情報の種類（外部個人情報／内部個人情報）や機密情報の種類（関係者外秘／社外秘）の違いに関わらず、機微な情報を保有している場合は、対策実施率に大きな差は見られなかった。

また、機微な情報を持たない「公開情報」のシステムの対策実施率は低くなっている。

しかし、機微な情報を取り扱っているにも関わらず、「アカウント管理」や「アクセス制御」をはじめに、多くの対策が実施されていないため、十分な対策が実施されているとは言えない状態である。

4.6. 従業員数･カテゴリ別 対策実施率

	初期設定	アカウント管理	アクセス制御	暗号化	外部媒体･端末の利用制御	その他、各種規制	ログ
3,000 人以上	50.4%	40.9%	59.9%	24.5%	58.6%	52.0%	50.4%
1,000 人～2,999 人	37.5%	32.9%	40.8%	12.0%	46.7%	35.0%	22.5%
300 人～999 人	47.3%	42.6%	52.7%	21.1%	64.3%	50.9%	39.9%
100 人～299 人	39.1%	40.6%	49.2%	17.5%	60.0%	46.4%	43.8%
30 人～99 人	54.8%	49.4%	58.3%	21.9%	63.8%	48.4%	52.4%
30 人未満	52.5%	43.8%	58.8%	30.0%	52.0%	45.0%	55.0%

従業員数･カテゴリ別に対策実施率を見ると、従業員数が 100 人未満である規模の企業の方が、大企業よりも各対策の実施率が高いという結果がでた。

この結果から以下の様な理由を推測してみた。

- 100 人未満の企業はシステムに携わる人数も少なく、セキュリティ対策を実施する場合にも柔軟に対応できていると考えられる。
- 企業規模が大きくなると、「アプリケーション部門」「ネットワーク部門」「データベース部門」などの分業制が進み、部門ごとの制約や各種事情などからセキュリティ対策の実施に対し、柔軟な対応が難しくなっていると考えられる。
- 3,000 人以上の企業規模で、対策実施率が 50%を超えているカテゴリが一番多くなっている。これは、セキュリティ対策の予算が十分に採られているためと考えられる。

5. 総評

以上、安全度セルフチェックの利用データから様々な切り口で統計データを取得し、それぞれ分析及び当 WG の意見を述べてきた。

当 WG では、安全度セルフチェックを利用する人はセキュリティに対する意識の高い人が多いと思っていたため、対策実施率はもう少し高い数値がでるものと予想していたが、P.15 の「4.1. カテゴリ別 対策実施率」のグラフからもわかる様に、実際にはほとんどのカテゴリで対策実施率が 50%にも満たない状態であった。この結果から、「データベースセキュリティ対策の実施状況は不十分である」と言える。

今回の統計データで注目したいのは、「アカウント管理」と「アクセス制御」の対策実施率の関係である。この2つのカテゴリでは、「アクセス制御」よりも「アカウント管理」の対策実施率が低くなっている。

この「アカウント管理」の対策は、「アクセス制御」や「ログ」などの対策の有効性に大きく影響する性質を持つ。例えば、共有アカウントを利用している様な場合ではアクセス制御を詳細に設定することはできないし、ログを取得しても操作した人物を特定することは、ほとんど不可能である。

つまり、先ず「アカウント管理」を適切に設定及び運用し、その上で必要最小限の機能やデータへのアクセス権限を付与することで、不要な機能やデータへのアクセスを防ぎ、万が一アカウントを不正利用されてしまった場合でも被害を最小限に抑えることが可能となるなど、「アクセス制御」が正しく機能する。

また、「ログ」についても、必要な操作及び項目をログに取得した際、アカウントが正しく記録されることで、操作した人物を特定することが可能となる。

今回の統計データから導き出される提案としては、「アクセス制御」や「ログ」を有効にするために「アカウント管理」を優先的に推進して欲しい。

この他、「暗号化」は他の対策に比べて対策実施率が特に低いが、この「暗号化」の対策は他の対策とは切り離し、単独でも実施できる。そこで、十分に調査及び検討した上で、該当システムにとって適切な手法や実施箇所（データ、ネットワークなど）を決めて導入することを推奨する。

これら「ログ」と「暗号化」は PCIDSS でも実施を求められている様に、重要な対策であるため是非見直して欲しい。

また、用途別や業種別に見ると、金融・保険業や情報サービスなどはレベル D が半数近くを占めていることから、比較的対策が進んでいるシステムと、ほとんど対策が実施されていないシステムに 2 極化している傾向が見られた他、社内システムなどは当サイトの利用件数が多くセキュリティへの関心があると見られるが、対策があまり進んでいない状況が顕著に現れている。

現在のシステムの中核となるデータベースには重要な情報が格納されており、中には個人情報が含まれているケースも多々ある。ひとたび情報漏えいしたり、改ざんされたりしてしまった場合は、顧客や取引先企業への謝罪や損害賠償だけでなく、イメージダウンによる経営損失や風評被害なども避けられない。その様な事態を防ぐためにも、ネットワークやアプリケーションでの対策だけでなく、上記の様なデータベースでの対策をデータベースセキュリティガイドラインに従って実施することで、より安全なシステムとする必要がある。

安全度セルフチェックの実行結果として表示された「実施できていない対策と、想定されるリスク」については、DBSC から公開されている「データベースセキュリティガイドライン http://www.db-security.org/report/dbsc_guideline_ver2.0.pdf（主に第 4 章）」を参考に検討し、実装前に再度、安全度セルフチェックを活用して診断結果のレベルが“A”となる様、十分な対策を実施して欲しい。

以上