JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

セキュリティランキングWG
最終活動報告

奥原　雅之
富士通株式会社（WG有志代表）

2009 年 6 月3日

1. 活動報告編

1.1 当初の活動目的

- １．WGの活動目的
  - 情報開示の充実度や取り組み姿勢、社会貢献活動などにも着目した、JNSA版情報セキュリティランキングを定期的に公表する。上位ランキング企業がどういう取り組みをしているかを把握するとともに、真摯に取り組む企業を讃える仕組みとして定着を目指す。
- ２．WGの年間活動予定
  - ランキング評価シートの設計・見直し、ランキング調査・公表、上位ランキング企業に対するヒアリング
- ３．予定成果物
  - ランキング結果

1.2 活動経緯

2006年11月	活動開始
2007年～2008年	ランキング決定のための評価（採点方法を検討
2008年5月	様々な事情によりこのころからWG活動を休止
2009年5月	最終報告を実施してWGクローズすることでメンバー合意
2009年6月	最終報告会（本日） WGお開き

1.3 目的達成状況

- ここまでに達成したもの
  - 評価用チェックシートの完成
  - 試験的評価の実施による実用性確認
- 達成しないで終わったもの
  - 同一条件による多数企業の評価・比較
  - ランキングの公表
- せめて達成して終わろうとしているもの
  - 最終報告 ⇦ 今ここ
  - 評価用チェックシートの公開

2. 評価用チェックシート

2.1 評価の基本方針

- 企業が「どの程度真剣にセキュリティに取り組んでいるか」を評価する
  - 「形だけやっている」「仕方なくやっている」は減点したい
  - 「独自の取り組み」を評価したい
- 企業の協力を得なくても評価できるよう外部からわかる情報（Webなど）で評価する
  - 「勝手ランキング」を可能にする
  - 評価の根拠が第三者にもわかる

2.2 評価の仕組み（1）

- 10個のカテゴリ（各300点満点）の合計点（3000点満点）で評価する。

A01　個人情報保護方針(プライバシーポリシー)

A02　個人情報の開示、訂正、利用停止

A03　個人情報の取得、利用

A04　個人情報保護体制

A05　第三者認証の有無（Pマーク、TRUSTe、ISMSなど）

A06　トップメッセージとその他の活動

A07　SSLの使用、サーバー証明書の妥当性など

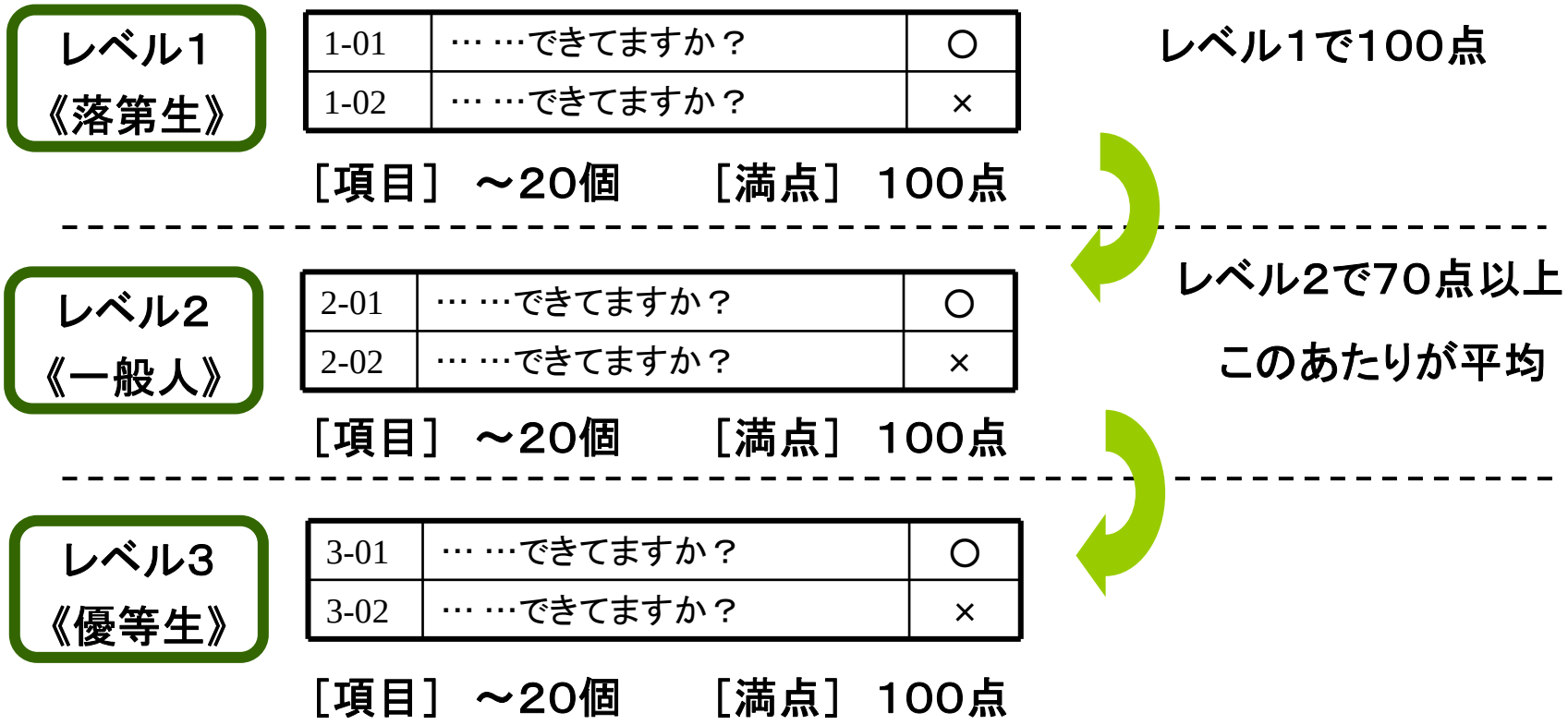
A08　Cookieの取扱い、Webビーコンなど Web利用に関する個人情報保護の言及

A09　サイトポリシー＆リンクポリシー

A10　社会貢献的取り組み

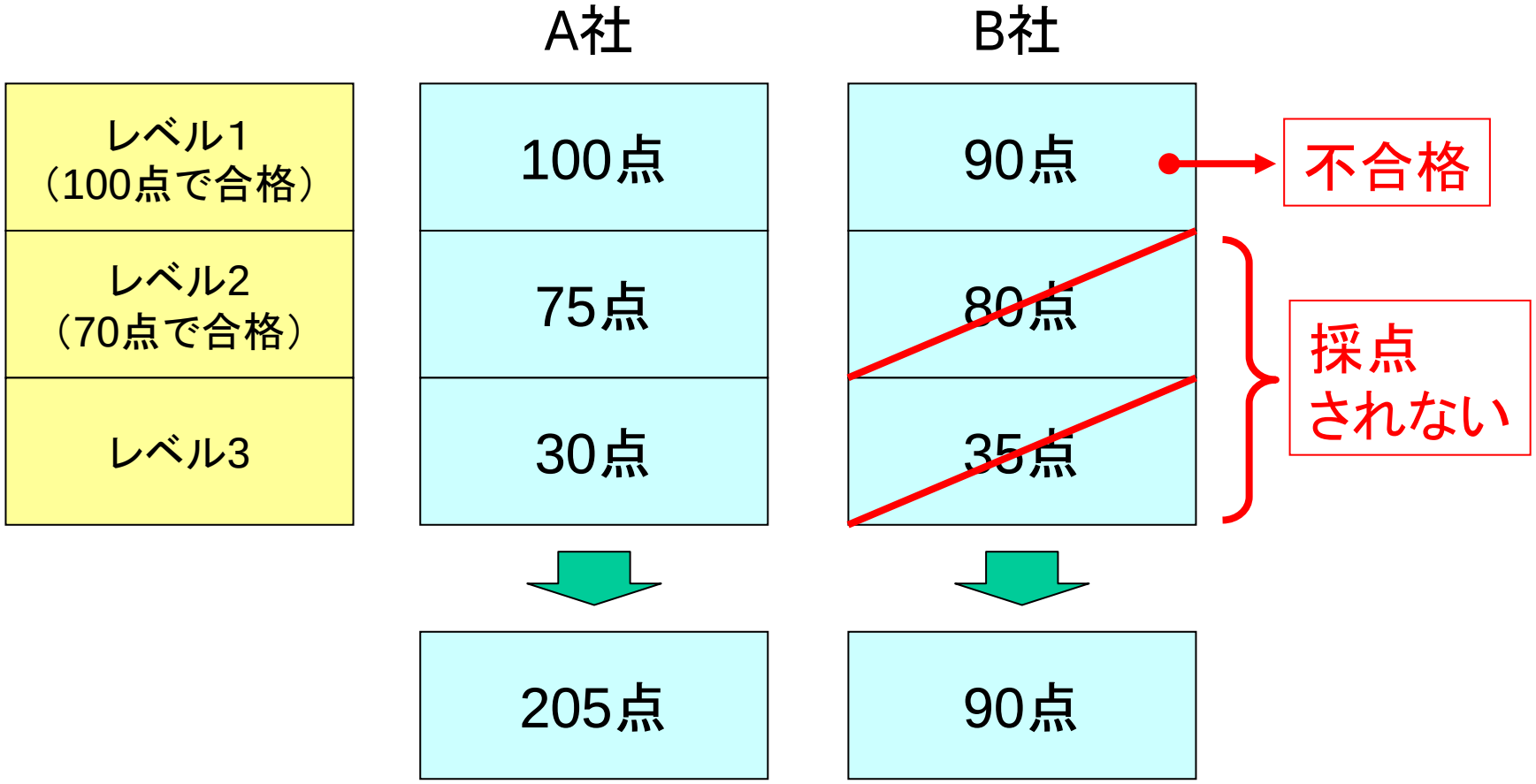
2.2 評価の仕組み(2)

- 各カテゴリは「3段階足切り制」(下位レベルが合格しないと上位は採点されない)



2.2 評価の仕組み(3)

- 「3段階足切り制」の例



2.3 質問項目例(A02)

レベル	カテゴリ	前提条件	項番	評価項目	具体的な取り組み項目	採点基準	配点
1	個人情報の開示等	なし	A02-1-01	個人情報の開示、訂正、利用停止に関して述べられているか	個人情報の開示、訂正、利用停止が可能な事が述べられている。	個人情報の開示、訂正、利用停止が可能な事が述べられている。	100

レベル	カテゴリ	前提条件	項番	評価項目	具体的な取り組み項目	採点基準	配点
2	個人情報の開示等	なし	A02-2-01	具体的な開示等の方法が書かれているか？	個人情報の開示、訂正、利用停止を行うための具体的な手順が示されている。	個人情報の開示、訂正、利用停止を行うための具体的な手順が示されている。	50
			A02-2-02	開示手数料が載せられているか？	手数料が載っている	手数料が載っている	25
			A02-2-03	開示請求の書式が提供されているか？	PDFファイル等で書式が用意されており、利用者がダウンロードできる。	PDFファイル等で書式が用意されており、利用者がダウンロードできる。	25

レベル	カテゴリ	前提条件	項番	評価項目	具体的な取り組み項目	採点基準	配点
3	個人情報の開示等	なし	A02-3-01	開示手数料が適正か？(1000円以下)		開示手数料が 500円以下　１（＝30点） 1000円以下　0．５（＝15点） 1000円超　０（＝0点）	30
			A02-3-02	開示方法が分かりやすく適切か？		開示請求の方法が、手順として示されているか？	40
			A02-3-03	開示請求に必要以上の情報を要求していないか？	勤め先、勤め先の連絡先、本籍等を要求していないか	基本4情報以外の情報を要求していないこと(ただし、本人確認書類を除く)	30

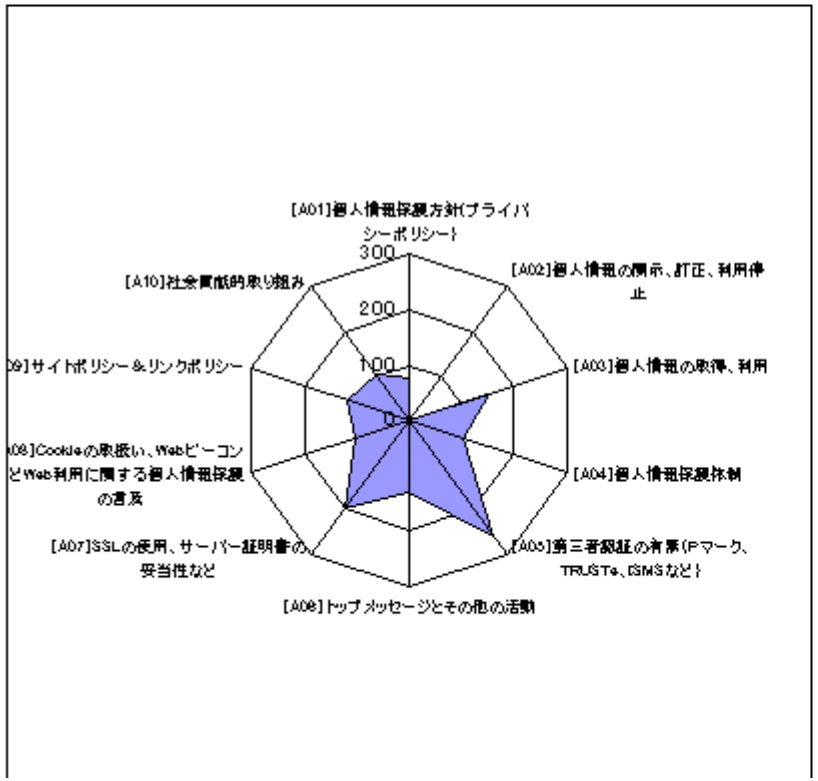
2.4 評価チェックシート（イメージ）

JNSAランキングWG

情報セキュリティランキング・チェックシート【査定版】

調査対象	株式会社HJ
調査日	2007年12月20日
調査者	関原　雅之（JNSA ランキングWG）

サマリー



レベル1合格点数		100
レベル2合格点数		70

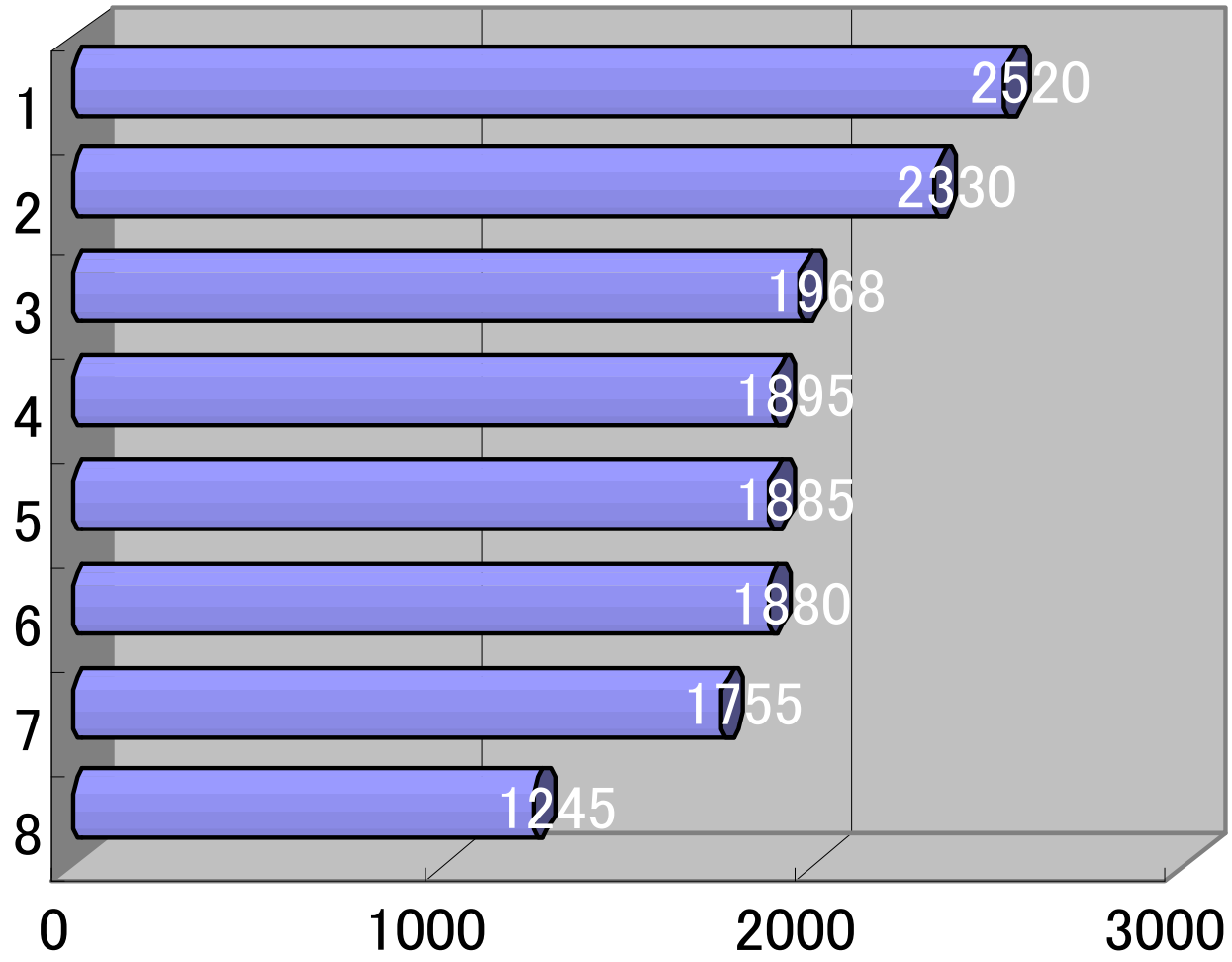
カテゴリ	レベル	得点
[A01]個人情報保護方針(プライバシーポリシー)	1	75
	2	0
	3	0
[A02]個人情報の開示、訂正、利用停止	1	0
	2	0
	3	0
[A03]個人情報の取得、利用	1	100
	2	50
	3	0
[A04]個人情報保護体制	1	100
	2	0
	3	0
[A05]第三者認証の有無（Pマーク、TRUSTe、ISMSなど）	1	100
	2	100
	3	50
[A06]トップメッセージとその他の活動	1	100
	2	30
	3	0
[A07]SSLの使用、サーバー証明書の妥当性など	1	100
	2	100
	3	0
[A08]Cookieの取扱い、WebビーコンなどWeb利用に関する個人情報保護の言及	1	100
	2	0
	3	0
[A09]サイトポリシー＆リンクポリシー	1	100
	2	20
	3	0
[A10]社会貢献的取り組み	1	100
	2	0
	3	0
[A01]個人情報保護方針(プライバシーポリシー)		75

3. 評価試行結果

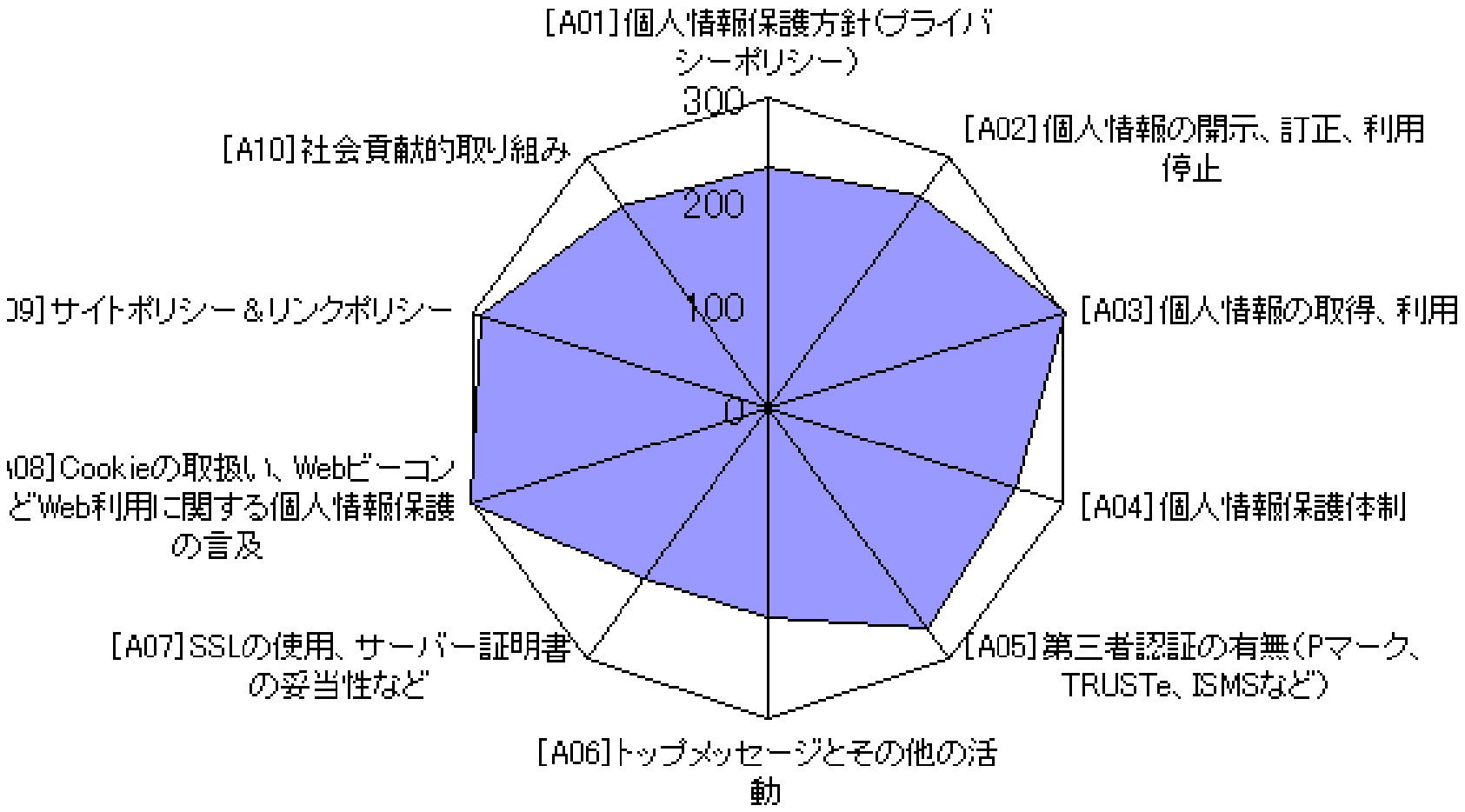
はじめにお読みください

- 調査期間中に何度かチェックシートのチューニングを実施しているため、一部違う評価指標で測定した結果が混在しています。
- 調査時点のWebなどの内容に基づいていますので、現在の評価とは異なる部分があります。
- 調査員による見落としがある可能性があります。また調査員による評価のばらつきもあります。

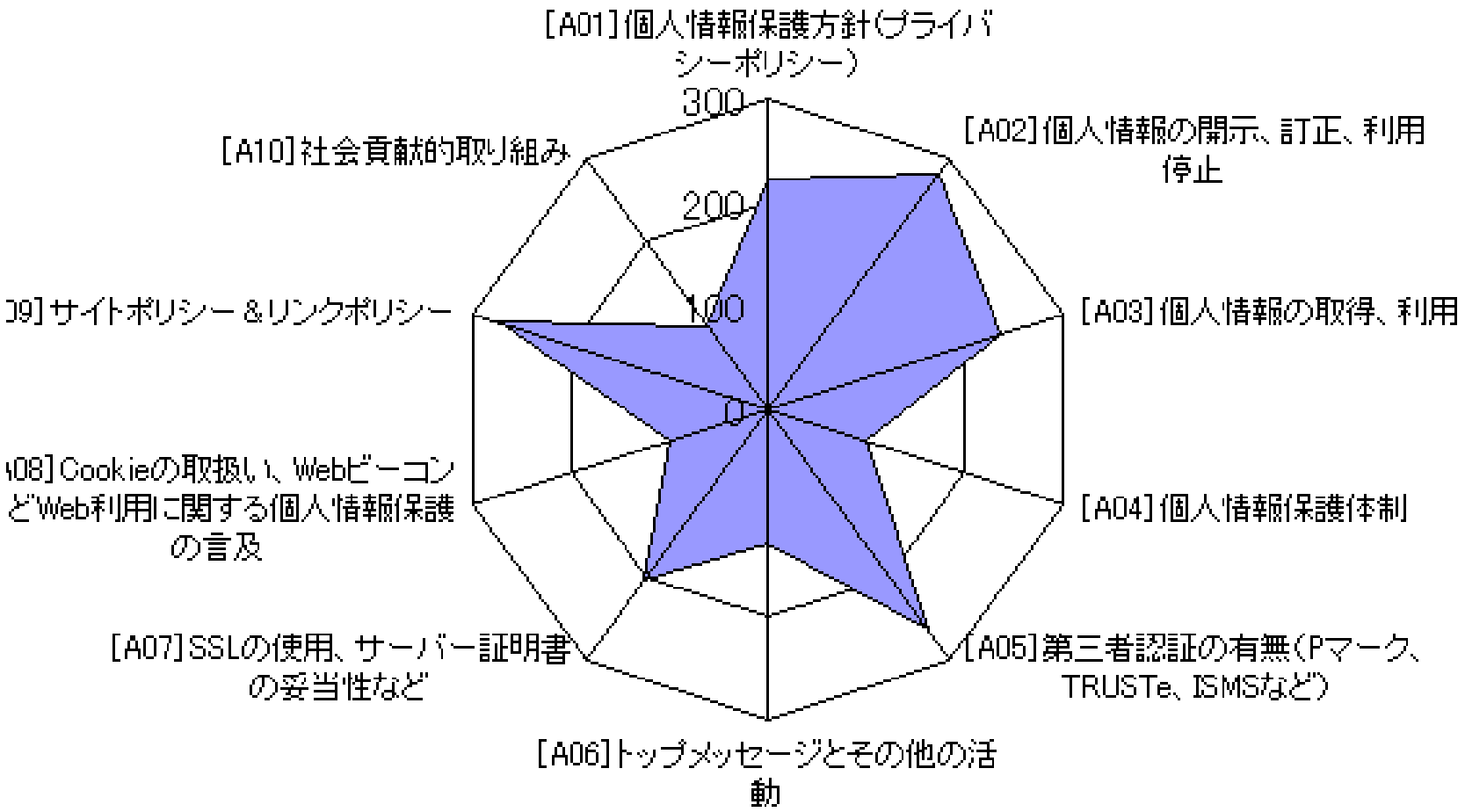
3.1 電機業界ランキング（例）



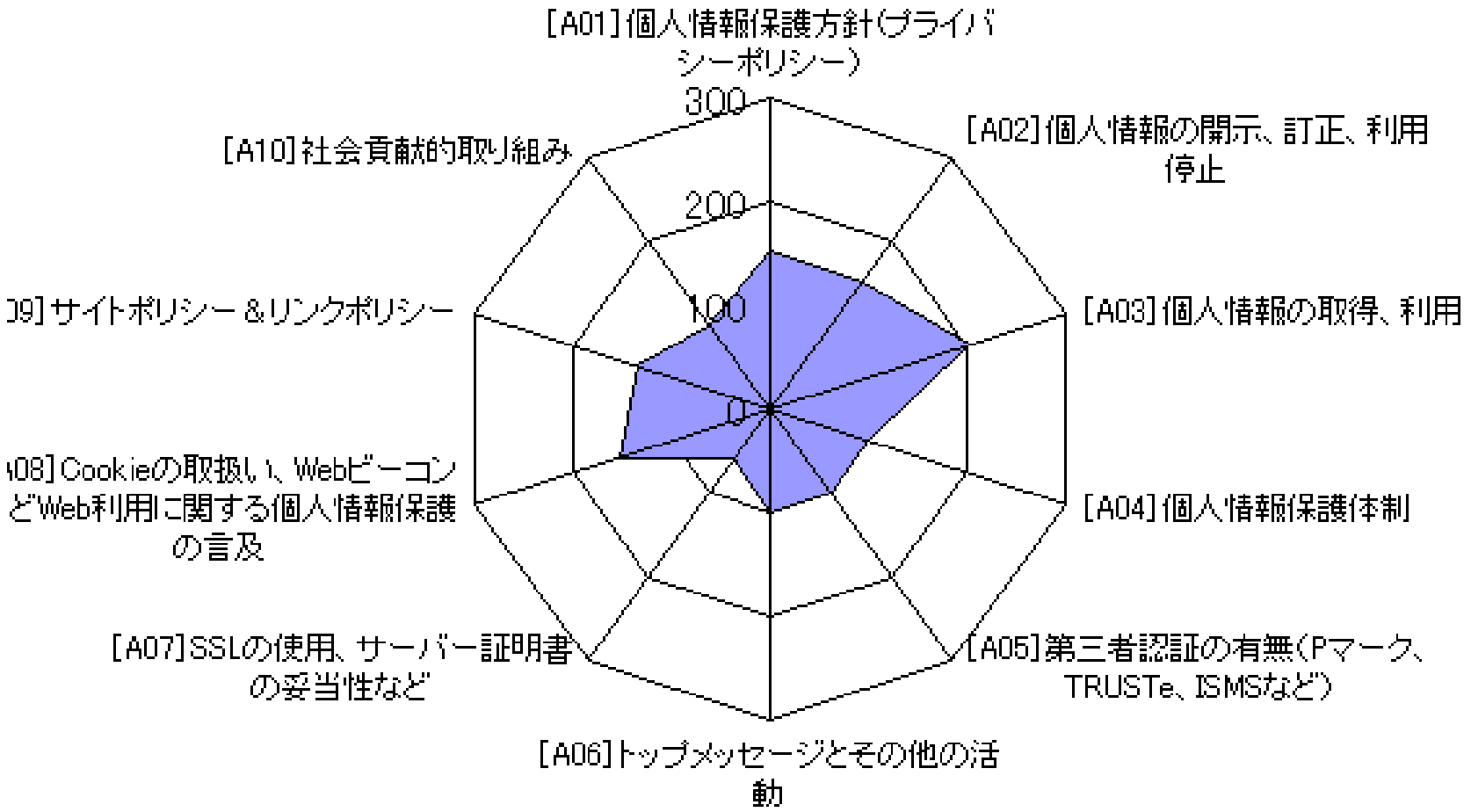
3.1-1 電機業界1位



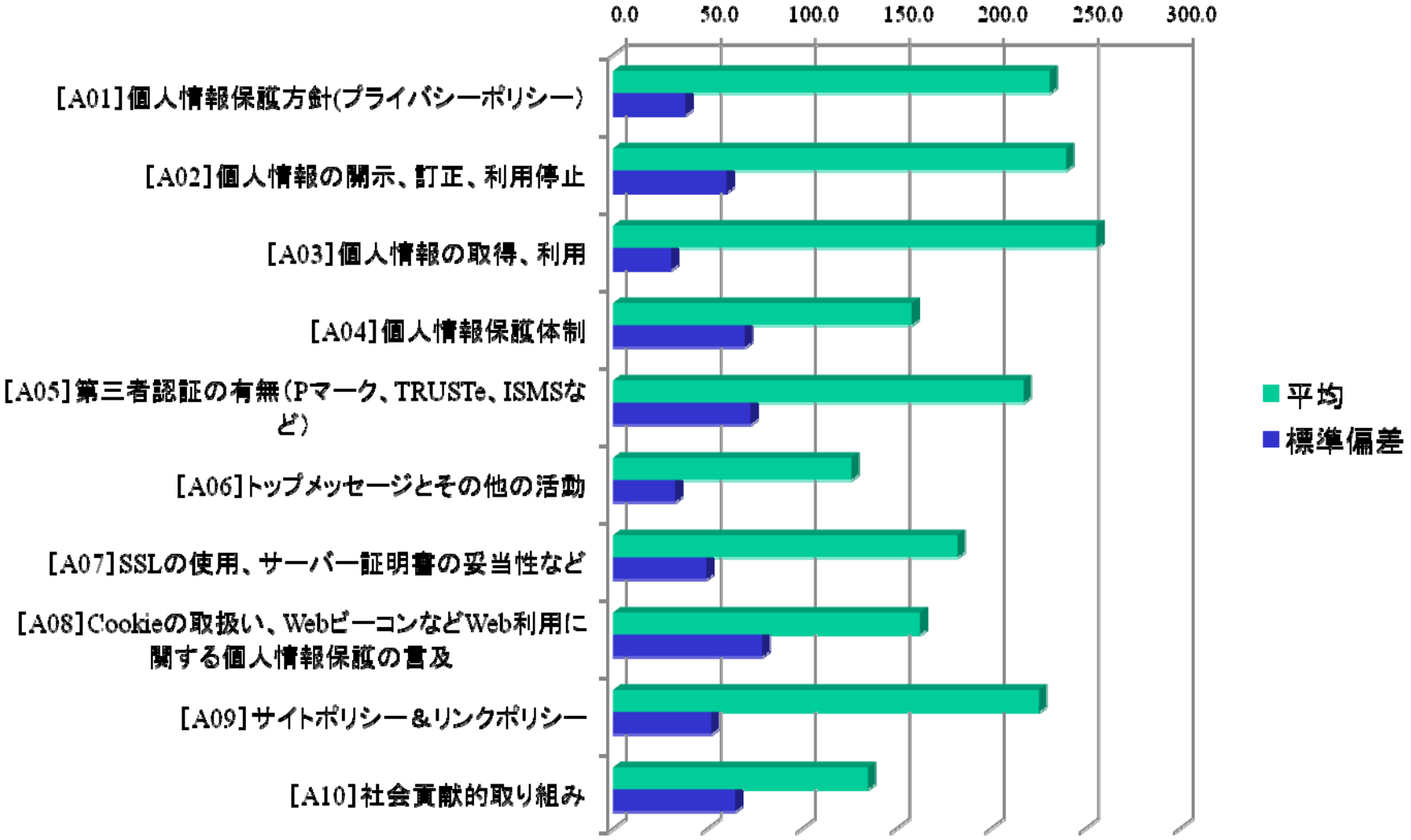
3.1-2 電気業界4位



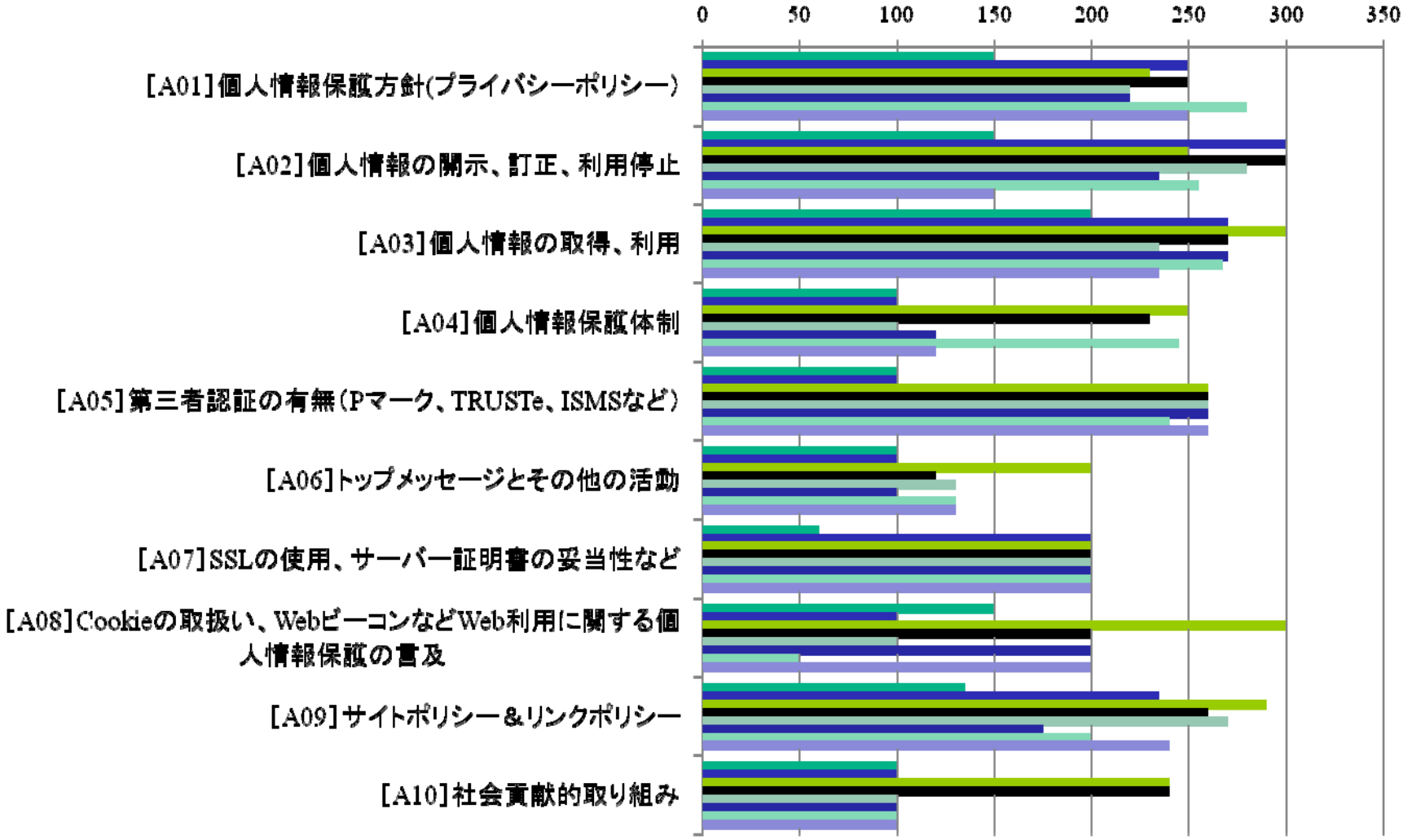
3.1-3 電気業界8位



3.2 カテゴリごとの得点分布(1)

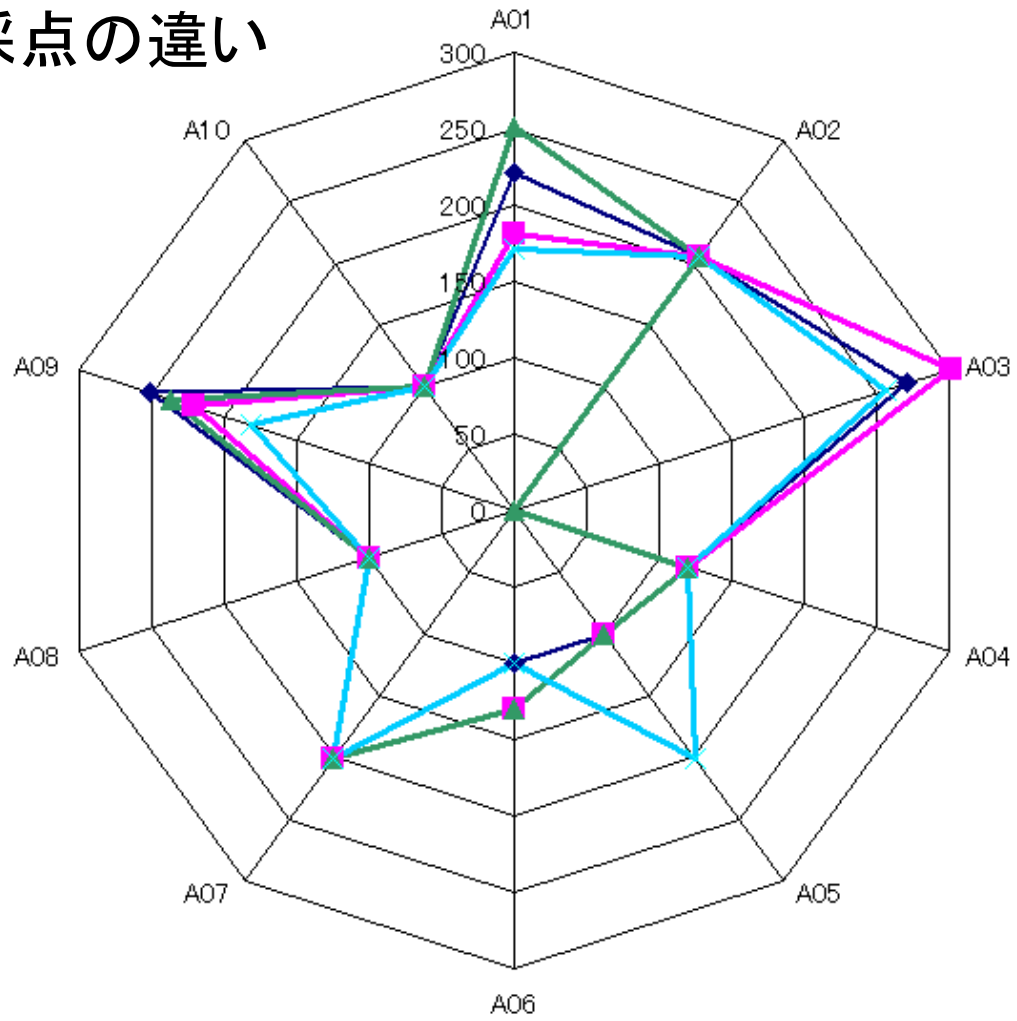


3.2 カテゴリごとの得点分布(2)



3.3 実施者によるばらつきの検証

４人の評価者による採点の違い



平均：1598点

3.4 わかったこと

- 同じ業界内ではそれほど広く分布しない（横並び文化？）。ただし、外資系は飛び出す傾向がある。
- 消費者に近い業界ほど得点が高くなる傾向がある。例えば小売業＞輸送業（旅客）＞輸送業（貨物）＞重工業・造船。
- Webに掲載されている文章はお手本があるものがあるらしい。流派に分かれたりもする。

3.5 課題

- 配点のバランス調整（個人情報保護に偏りすぎている気もする）
- 客観的に判断できるような指針作成
- 項目ごとの相関の分析（A項とB項は有意に相関があることなどの発見）
- Web以外の情報源の確認とクロスチェック

ご清聴ありがとうございました

【付録】チェック項目一覧

[A01]個人情報保護方針(プライバシーポリシー)

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	個人情報保護	なし	A01-1-01	個人情報保護方針が載っているか？	100
2	個人情報保護	なし	A01-2-01	理念が書かれているか？	20
	法令順守		A01-2-02	個人情報保護法遵守について書かれているか？	20
	個人情報の管理		A01-2-03	従業者の監督についてのべられているか？	10
			A01-2-04	委託先の監督ついてのべられているか？	10
	苦情・相談への対応		A01-2-05	問合せ先に具体的な部署が載っているか？	20
	継続的改善		A01-2-06	改定履歴が載っているか？	10
	代表者の氏名		A01-2-07	代表者氏名が載っているか？	10
3	個人情報保護	なし	A01-3-01	理念から個人情報保護を重視していると感じられるか？	20
			A01-3-02	個人情報の定義についてのべられているか？	20
			A01-3-04	個人情報取り扱い業者の定義について述べられているか？	20
	法令順守		A01-3-05	保護法以外で個人情報保護に関して守るべき法律について書かれているか？	20
	継続的改善		A01-3-06	継続改善の具体的な対応内容が載っているか？	20

[A02]個人情報の開示、訂正、利用停止

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	個人情報の開示等	なし	A02-1-01	個人情報の開示、訂正、利用停止に関して述べられているか	100
2	個人情報の開示等	なし	A02-2-01	具体的な開示等の方法が書かれているか？	50
			A02-2-02	開示手数料が載せられているか？	25
			A02-2-03	開示請求の書式が提供されているか？	25
3	個人情報の開示等	なし	A02-3-01	開示手数料が適正か？(1000円以下)	30
			A02-3-02	開示方法が分かりやすく適切か？	40
			A02-3-03	開示請求に必要以上の情報を要求していないか？	30

[A03]個人情報の取得、利用

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	個人情報の取得	なし	A03-1-01	個人情報取得時の利用目的の明示に関して述べられているか？	100
2	個人情報の取得	なし	A03-2-01	個人情報取得時の利用目的が具体的で分かりやすいか	50
	個人情報の利用		A03-2-02	目的外利用禁止について述べられているか？	50
3	個人情報の取得	なし	A03-3-01	監視カメラ、通話録音等による情報取得に関して述べられているか？	15
	個人情報の利用		A03-3-02	例外的な目的外使用について書かれているか（警察からの要請等）	15
			A03-3-03	具体的業務（事業）毎に使う目的が述べられているか？	20
			A03-3-04	個人情報の共同利用について述べられているか？	20
			A03-3-05	利用目的の変更に関して述べられているか？	15
			A03-3-06	未成年の個人情報取り扱いに関する記述があるか？	15

[A04]個人情報保護体制

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	（該当なし）		A04-1-01		100
2	体制	なし	A04-2-01	全社を統括して個人情報保護を推進する体制が構築されているか	20
	責任者		A04-2-02	全社を統括して個人情報保護を推進する責任者（チーフ・プライバシー・オフィサーなど）が設置されているか	20
	教育・研修実施機関		A04-2-03	全社的な教育・研修活動を実施する機関（機能）があるか	20
	内部監査実施機関		A04-2-04	全社的な内部監査を実施する機関（機能）があるか	20
	問い合わせ窓口	社外の個人情報を収集、預託している場合	A04-2-05	社外からの個人情報の問い合わせ窓口があるか	20
3	評価	なし	A04-3-01	個人情報保護の実施状況に係る（定性的・定量的に）評価する仕組みが構築されているか	20
	事業継続		A04-3-02	個人情報保護に係る事業継続計画が策定されているか	20
	危機管理		A04-3-03	個人情報の流出など、有事の際に適切に対処できる機関（機能）があるか	15
	関連資格		A04-3-04	関連資格を有する社員が相当数いる、または有資格者を増やす取り組みがあるか	15
	内部監査員		A04-3-05	内部監査員が相当数いる、または内部監査員教育が実施する機関（機能）があるか	15
	体制		A04-3-06	グループ会社や海外拠点をも包含した体制であるか	15

[A05]第三者認証の有無(Pマーク、TRUSTe、ISMSなど)

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	(該当なし)		A05-1-01		100
2	第三者認証	(なし)	A05-2-01	何らかのセキュリティ関連の認証を取得している	100
3	第三者認証	個人情報を取り扱う場合	A05-3-01	Pマークを取得している	20
		(なし)	A05-3-02	ISMSを取得している	40
		(なし)	A05-3-03	TRUSTeを取得している	40

[A06]トップメッセージとその他の活動

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	ネガティブ情報	ネガティブ情報がある	A06-1-01	ネガティブ情報がある場合はその内容を積極的に開示している	70
	事故後の対応	事故が発生したことがある	A06-1-02	発生した事故の掲載に関して、謝罪の内容が含まれている。	30
2	トップメッセージ、企業理念	トップメッセージ又は企業理念が掲載されている	A06-2-01	トップメッセージ又は企業理念に該当する方針として情報セキュリティや個人情報保護が唱えられている	50
	行動規範	行動規範や行動基準が掲載されている	A06-2-02	行動規範、行動基準で機密情報や個人情報の適切な利用・管理を掲げている	30
	BCP	事業継続に関する記述がある	A06-2-03	具体的にBCPは策定されていないが、事業継続（継続可能な社会）に関する意思表示がある	20
3	情報セキュリティ報告書	情報セキュリティ報告書を発行(公開)している	A06-3-01	情報セキュリティ報告書を発行している	50
	BCP	BCPを公開している	A06-3-02	BCPを公開している	50

[A07]SSLの使用、サーバー証明書の妥当性など

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	電子証明書	自己発行証明書を利用している場合	A07-1-01	正しい証明書検証の手段を提供している	20
		第三者発行証明書を利用している場合	A07-1-02	信頼できる第三者から証明書を入手している	20
		電子証明書を利用している場合	A07-1-03	電子証明書が正しく運用されている	20
		電子証明書に関する説明コンテンツがある場合	A07-1-04	説明の内容が正しい	20
	暗号化	個人情報など保護するべき情報を取り扱っている場合	A07-1-05	保護するべき情報の送受信を行うページが暗号化（SSL）などで正しく保護されている	20
2	（該当なし）		A07-2-01		100
3	（なし）	（なし）	A07-3-01	その他特に特筆するべき取り組みをしている。	100

[A08]Cookieの取扱い、Webビーコンなど Web利用に関する個人情報保護の言及

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	SSLの使用	SSLを利用しており、その旨の説明文がある	A08-1-01	SSLの説明に技術的な誤りがない	100
2	Web利用の言及	（なし）	A08-2-01	Webビーコンの利用についてのポリシーが明記されている	50
		（なし）	A08-2-02	Cookieの利用についてのポリシーが明記されている	50
3	（なし）	（なし）	A08-3-01	その他特に特筆するべき取り組みをしている。	100

[A09]サイトポリシー＆リンクポリシー

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	-		A09-1-01		100
2	著作権	なし	A09-2-01	ウェブサイト上の著作物に対して、著作権の帰属に関する注意書きがある	20
			A09-2-02	商標やロゴマーク等の権利の帰属に関する注意書きがある	20
	損害発生時の責任	なし	A09-2-03	コンテンツ等の利用により何らかの損害が発生した場合に関する記述がある	20
	リンク	なし	A09-2-04	リンクをする場合の手続き等に関しての記述がある	20
	問い合わせ	なし	A09-2-05	ウェブサイトに関するお問い合わせ方法に関しての記述がある	10
	準拠法	なし	A09-2-06	準拠法に関する記述がある	5
	管轄裁判所	なし	A09-2-07	管轄裁判所に関する記述がある	5
3	著作権	なし	A09-3-01	著作物の複製、改変、転載等に関する記述がある	10
			A09-3-02	著作物を許諾を得て利用する場合のルールに関する記述がある	10
			A09-3-03	著作物の利用が不適切な場合の許諾取り消しに関する記述がある	5
			A09-3-04	商標やロゴマークの無許可の利用が違法である旨の記述がある	10
	コンテンツに対する責任	なし	A09-3-05	構成、利用条件、コンテンツ等の予告無しの変更の可能性がある旨の記述がある	10
	リンク	なし	A09-3-06	リンクをする場合のURL等の記述がある	10
			A09-3-07	リンクをする場合のバナーに関する記述がある	10
			A09-3-08	リンクを禁止する場合の条件等の記述がある	5
			A09-3-09	リンク許諾の取り消しに関する記述がある	5
			A09-3-10	リンク時のHTML記述方法に関する記述がある	5
	利用環境	なし	A09-3-11	推奨利用環境に関する記述がある	5
			A09-3-12	ウェブサイト利用時の禁止事項に関する記述がある	5
	その他	なし	A09-3-13	RSSによる更新情報の提供に関する記述がある	5
			A09-3-14	海外向け製品に関する記述がある	5

[A10]社会貢献的取り組み

レベル	カテゴリ	前提条件	項番	評価項目	配点
1	（該当なし）		A10-1-01		100
2	総合	（なし）	A10-2-01	何らかの情報セキュリティに関する社会貢献活動をしている。	80
			A10-2-02	Webアクセシビリティに配慮している。	20
3	普及・啓発	取り組んでいれば加点	A10-3-01	情報セキュリティに関する子どもや保護者、教職員などに対する教育（講師派遣）を行っているか	20
			A10-3-02	情報セキュリティに関する各種コンテンツ（冊子・ポスター・Webサイトなど）を制作・提供しているか	20
			A10-3-03	情報セキュリティの普及・啓発を目的としたフォーラム、コンソーシアム等に積極に参画しているか	20
	研究助成		A10-3-04	情報セキュリティに関する研究助成を行っているか	20
	研究活動		A10-3-05	情報セキュリティに関する学会・NPO等で積極的に研究活動に従事しているか	20