Control Self-Assessment

CSAアンケート雛形ファイル　解説

2020年6月25日版

CIAフォーラム

CSA実践研究会（ No.d2 ）

CSAアンケート雛形ファイルとは－1

- CSAアンケートを実施する前提
  - 企画者：コーポレートなリスク管理部門及び内部監査部門
  - 目　的：情報セキュリティ管理について、グループの状況把握と改善
  - アンケート回答者：各子会社のシステム担当者
- 下記の情報セキュリティに関する9つのリスクが対象
  - PCの盗難、紛失による漏洩
  - 外部記憶媒体の盗難、紛失による漏洩
  - メールの誤送信による漏洩
  - 社内PCのウィルスやスパイウェア感染による漏洩
  - ネットワーク上のハッキングによる漏洩
  - 情報機器処分時のデータ消去が不十分だったことによる漏洩
  - データの不適切な廃棄（管理）による漏洩
  - 社員の故意による漏洩
  - 委託業者からの漏洩

CSAアンケート雛形ファイルとは-2

- CSAアンケート雛形ファイルのポイント
  - 特別なアプリが不要で加工が容易なExcelファイル
  - 整備状況と運用状況に分けて評価
    - 情報セキュリティ以外のリスクでも適用できる方法
  - レベル評価をしやすいよう運用状況の項目毎の設問数を統一（各項目6問）
  - 設問数：整備状況　6問、運用状況　10項目60問
  - 回答が容易な選択式
    - フリーコメント欄も設置
  - 項目毎にレベル判定され、結果がその場ですぐにわかる
    - 評価結果まとめ表シートも作成
  - 集計が容易

CSAアンケート雛形ファイルの構成

- CSA実施者用シート

  表紙

  1. 整備状況の評価
  2. 運用状況の評価
  3. 評価結果まとめ
  4. 改善活動

- CSA企画部門用のシート（CSA実施時には非表示）

  a. 回答用選択肢
  b. 評価基準
  c. 総合評価
  d. 評価結果計算
  e. 回答集計
  f. コメント集計

Control Self-Assessment

Control Self-Assessment

CSA実施者用シート

表紙
1. 整備状況の評価
2. 運用状況の評価
3. 評価結果まとめ
4. 改善活動

表紙

情報セキュリティに関するCSA質問票

実施するCSAの標題を入れます。

本CSAは貴社の情報セキュリティリスクへの対応状況を自己評価することで、コントロール上の弱点、課題等を早期に発見し、適切に改善活動を行うことを目的に実施するものです。

この質問票は次の4つのシートで構成されています。

1. 整備状況に関する設問
2. 運用状況に関する設問
3. 評価結果まとめ
4. 改善活動

1，2の設問を全て回答すると「3. 評価結果まとめ」に結果が自動的に表示されます。
評価結果を確認の上、「4. 改善活動」に必要事項を回答してください。

＊回答はすべて選択式です。該当するものをリストから選択してください。
＊未回答の項目があると、結果が正しく表示されませんので、すべての設問に回答してください。
＊補足すべき事項等がありましたら、適宜フリーコメント欄を利用してください。

実施者がスムーズ回答できるよう下記の 内容を簡潔に記載します。
・実施目的
・質問票の構成
・入力時の留意事項 など

↓回答日・所属・氏名をご記入ください。

回答日:	年　月　日
社名:	
組織名:	
氏名:	

回答を集計分析する際に必要な情報を収集できるよう項目を設定します。
「回答日」セルは3. 評価結果まとめシートにリンクしています。
「社名」セルは下記のシートにリンクしています。
－3. 評価結果まとめ
－e.回答集計
－f.コメント集計

クリックして回答をスタート

ハイパーリンクで「1. 整備状況シート」に飛びます。

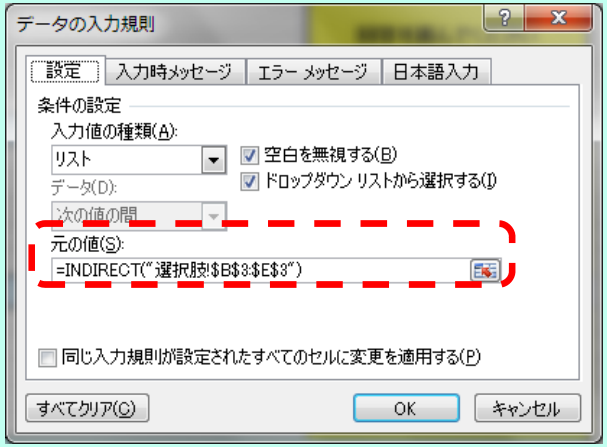
1．整備状況シート－①

《整備状況に関する設問》	
下記の設問について、該当する回答を選択してください。	
（選択肢：①全てある／全て行っている　②一部ある／一部行っている　③ない／行っていない）	
1 次の項目の情報セキュリティに関する基本ルールがありますか。	
1） 目的・基本方針	回答を選んでください
2） 定義	
3） 適用範囲	
4） 責任体制と運用	
5） リスクアセスメント	
6） モニタリング（内部監査・自己点検）	
2 管理・対応ルールの確認	
【データ・ID管理】次の項目の管理ルールがありますか。	
1） 機密情報の取り扱い（情報管理台帳、機密レベルの設定）	回答を選んでください
2） データ管理（保管・複製・廃棄・バックアップ等）	
3） 外部記憶媒体管理（CD、DVD、USBメモリ等）	
4） ユーザ管理（ID、アクセス権限、パスワード等の本人認証方法）	
5） 特権ID管理（権限設定、貸出ルール、パスワード）	
6） 物理的アクセス管理（サーバルーム、機密文書書庫等）	
【インフラ管理】次の項目の管理ルールがありますか。	
1） ハードウェア管理（PC、サーバ、プリンタ他）	回答を選んでください
2） ソフトウェア管理	
3） システム開発・運用管理	
4） ネットワーク管理	
5） 外部委託管理	
【トラブル対応】次の項目の対応ルールがありますか。	
1） 障害（故障・システムエラー等）への対応	回答を選んでください
2） PC、外部記憶媒体等の紛失、盗難への対応	
3） ウィルスへの対応	
4） セキュリティ侵害への対応	
5） 災害発生時の対応	
3 次の項目について定期的な啓発活動を行っていますか。	
1） 情報セキュリティ全般・情報セキュリティ基本ルール	回答を選んでください
2） 機密情報の取り扱い（機密レベル）	
3） データの保管、複製、廃棄、バックアップ等の管理ルール	
4） ID,パスワード等の管理ルール	
5） ネットワーク利用（イントラ・インターネット）に関するルール	
6） CD、DVD、USBメモリ等の管理ルール	
7） トラブル発生時（盗難、紛失、災害、故障、ウィルス感染等）の対応ルール	
4 次の項目についてモニタリング・監視（定期・常時）活動を行っていますか。	
1） E-mailの送受信	回答を選んでください
2） 社内からのインターネットアクセス	
3） 社内ネットワークへの外部からのアクセス	
4） 社有PCへの外部デバイス接続（USBメモリ、ハードディスク他）	
5） 社有PCの操作	
6） 特権IDの操作	
7） 上記1）～6）のログの保管と分析	

回答の選択肢はプルダウンメニューです。
「a.選択肢シート」の「整備状況用」を利用しています。

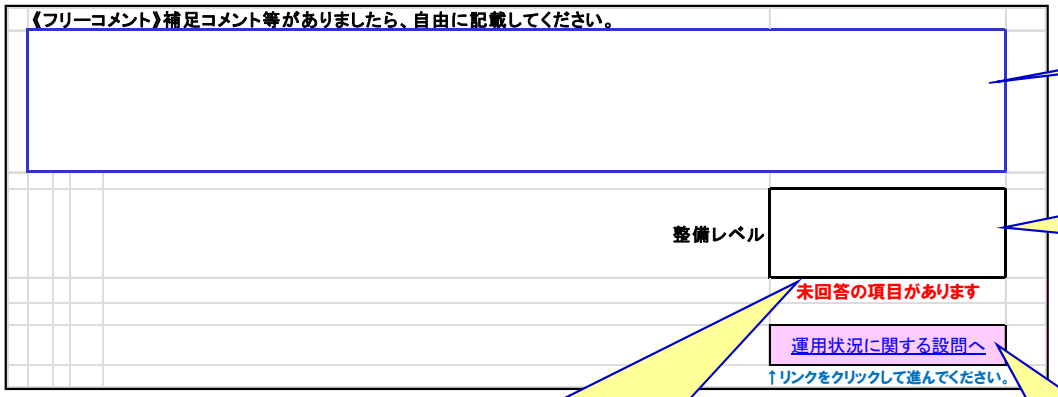
【回答用選択肢】				
整備状況用	回答を選んでください	①全てある	②一部ある	③ない
	回答を選んでください	①全て行っている	②一部行っている	③行っていない
運用状況用	回答を選んでください	①Yes	②No	

選択肢の内容や数を変更する場合は、「a. 選択肢シート」の該当部分を変更します。
選択肢の数を変更した場合は、「データの入力規則」の設定も変更してください。



条件付書式により、セルはレベルに応じた色になります。

1．整備状況シート－②



選択肢だけでは回答しにくい場合がありますので、最後にフリーコメント欄を設置しています。
コメント集計シートにリンクしています。

回答結果について、評価基準シートの基準に基づき整備レベルを計算して表示します。
全ての設問に回答を入力しないと、結果が表示されないよう関数を設定しています。
また、条件付書式でセルはレベルに応じた色になります。

回答欄の「回答を選んでください」をカウントし、未回答項目がある場合は「未回答の項目があります」と表示します。

ハイパーリンクで「2．運用状況シート」に飛びます。

評価基準は下記の通り、項目毎の回答をポイント化して、集計値で整備レベルの評価を行っています（評価基準シート参照）。
評価結果計算シートで集計し、関数（VLOOKUP）で該当する「整備レベル」を表示します。

	ポイント	
	設問1,3,4	設問2
①全てある/全て行っている	5	3
②一部ある/一部行っている	3	1
③ない/行っていない	0	0

整備レベル	
レベルA	24～21ポイント
レベルB	20～12ポイント
レベルC	11～6ポイント
レベルD	5～0ポイント

評価基準を変更する場合は、評価基準シートを変更します。

1．整備状況シート－③

Control Self-Assessment

《回答事例》

《整備状況に関する設問》		
下記の設問について、該当する回答を選択してください。		
（選択肢：①全てある／全て行っている　②一部ある／一部行っている　③ない／行っていない）		
1 次の項目の情報セキュリティに関する基本ルールがありますか。		
1）	目的・基本方針	②一部ある
2）	定義	
3）	適用範囲	
4）	責任体制と運用	
5）	リスクアセスメント	
6）	モニタリング（内部監査・自己点検）	
2 管理・対応ルールの確認		
【データ・ID管理】次の項目の管理ルールがありますか。		
1）	機密情報の取り扱い（情報管理台帳、機密レベルの設定）	①全てある
2）	データ管理（保管・複製・廃棄・バックアップ等）	
3）	外部記憶媒体管理（CD、DVD、USBメモリ等）	
4）	ユーザ管理（ID、アクセス権限、パスワード等の本人認証方法）	
5）	特権ID管理（権限設定、貸出ルール、パスワード）	
6）	物理的アクセス管理（サーバルーム、機密文書書庫等）	
【インフラ管理】次の項目の管理ルールがありますか。		
1）	ハードウェア管理（PC、サーバ、プリンタ他）	①全てある
2）	ソフトウェア管理	
3）	システム開発・運用管理	
4）	ネットワーク管理	
5）	外部委託管理	
【トラブル対応】次の項目の対応ルールがありますか。		
1）	障害（故障・システムエラー等）への対応	①全てある
2）	PC、外部記憶媒体等の紛失、盗難への対応	
3）	ウィルスへの対応	
4）	セキュリティ侵害への対応	
5）	災害発生時の対応	

期的な啓発活動を行っていますか。		
	般・情報セキュリティ基本ルール	②一部行っている
	い（機密レベル）	
	、廃棄、バックアップ等の管理ルール	
	管理ルール	
	ントラ・インターネット）に関するルール	
	モリ等の管理ルール	
	難、紛失、災害、故障、ウィルス感染等）の対応ルール	
ニタリング・監視（定期・常時）活動を行っていますか。		
	ネットアクセス	②一部行っている
	の外部からのアクセス	
	デバイス接続（USBメモリ、ハードディスク他）	
	の保管と分析	
ント等がありましたら、自由に記載してください。		
整備レベル		B

2. 運用状況シート-①

評価基準シートの基準に基づき、設問毎に運用レベルを計算して表示します。
評価基準を変更する場合は、評価基準シートを変更します。
条件付書式でセル色はレベルに応じた色に変わります。

項目単位のレベル		
	Yesの数	ポイント
レベルH	6	5
レベルM	5～3	3
レベルL	2～0	0

《運用状況に関する設問》

下記の設問について、該当する回答を選択してください。(選択肢:①Yes ②No)

1 データの不適切な管理(保管・廃棄等)による情報漏洩への対応			運用レベル
1)	リスクアセスメントに基づいて、機密情報の管理レベル、管理方法を定めていますか。またそれを定期的に見直していますか。	回答を選んでください	
2)	機密情報について、情報管理台帳を作成して管理していますか。	回答を選んでください	
3)	機密情報を記録した紙媒体・記憶媒体の保管、廃棄方法等のルールを周知徹底していますか。	回答を選んでください	
4)	機密情報についてその内容に応じた機密レベルを明示するとともにアクセス権限を明確にして管理していますか。	回答を選んでください	
5)	機密情報を廃棄した場合は記録を残していますか。	回答を選んでください	
6)	機密書類は、シュレッダーまたは機密処理ボックスなど、管理レベルに応じた方法で処分していますか。	回答を選んでください	
フリーコメント			未回答あり

選択肢だけでは回答しにくい場合がありますので、設問毎にフリーコメント欄を設置しています。
「f. コメント集計シート」にリンクしています。

回答の選択肢はプルダウンメニューの2択(①Yes ②No)です。
「a. 選択肢シート」の「運用状況用」を利用しています。

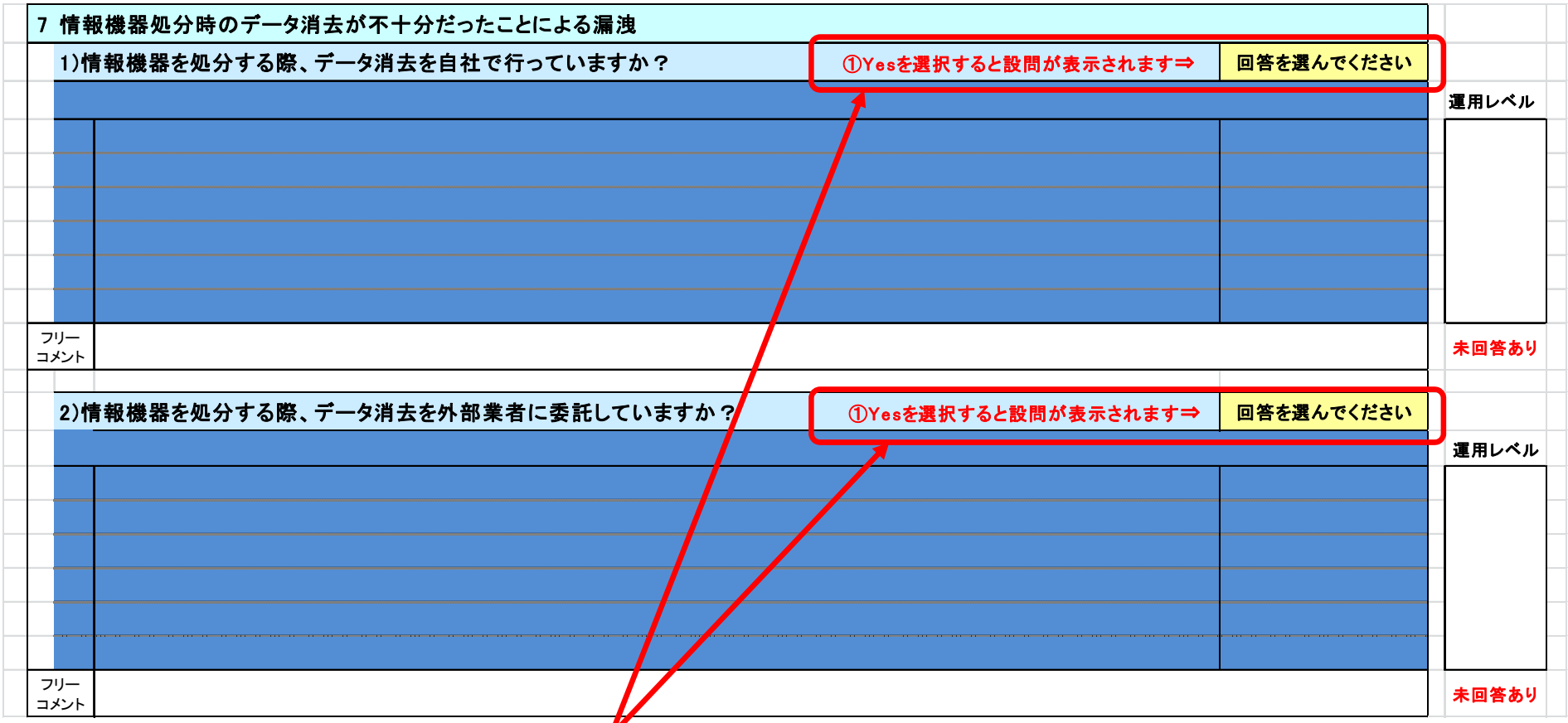
【回答用選択肢】				
整備状況用	回答を選んでください	①全てある	②一部ある	③ない
	回答を選んでください	①全て行っている	②一部行っている	③行っていない
運用状況用	回答を選んでください	①Yes	②No	

選択肢の内容や数を変更する場合は、「a. 選択肢シート」の該当部分を変更します。
選択肢の数を変更した場合は、「データの入力規則」の設定も変更してください。(「1. 整備状況シート-①」を参照)

回答欄の「回答を選んでください」をカウントし、未回答項目がある場合は「未回答あり」と表示します。

2. 運用状況シート-②

該当なしとなる可能性がある設問-1



該当なしとなる可能性がありますので、最初に事象があるかを確認する設問を追加しています。
事象がないのに回答をしないように、「条件付書式」を利用し、設問のセルおよび文字色を青に着色して、非表示にしています。

2. 運用状況シート-③

該当なしとなる可能性がある設問-2

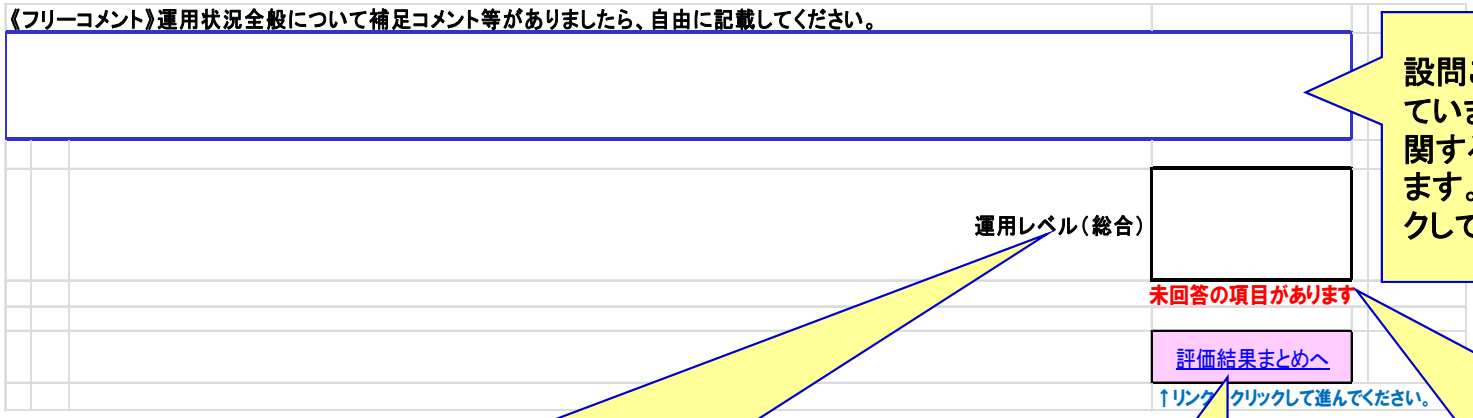
①Yesを選択すると「条件付書式」が解除され、設問が表示されます。
後は他の設問と同じ仕様です。

7 情報機器処分時のデータ消去が不十分だったことによる漏洩			
1)情報機器を処分する際、データ消去を自社で行っていますか？	①Yesを選択すると設問が表示されます⇒	①Yes	
【自社で実施】			運用レベル
1）	データ消去についての社内で統一したルールと手順はありますか。	回答を選んでください	
2）	データ消去を一元的に行う部署は決まっていますか。	回答を選んでください	
3）	データ消去は、専用のデータ消去ソフトの利用、強磁気破壊装置の利用、ハードディスクの物理的破壊のいずれかの方法で行っていますか。	回答を選んでください	
4）	データ消去作業は複数名で行っていますか。	回答を選んでください	
5）	対象となった機器が全台漏れなく作業されたことを確認していますか。	回答を選んでください	
6）	データ消去作業後に、サンプル等で確実にデータが消去されたことを確認してますか。	回答を選んでください	
フリーコメント			未回答あり
2)情報機器を処分する際、データ消去を外部業者に委託していますか？	①Yesを選択すると設問が表示されます⇒	②No	
			運用レベル
			N/A
フリーコメント			

②Noを選択すると「条件付書式」により、セルおよび文字色が「黒」に変わります。

②Noを選択した場合は、N／A と表示されます。

2. 運用状況シート-④



設問ごとにフリーコメント欄を設置していますが、最後に運用状況全般に関するフリーコメント欄を設置しています。「f. コメント集計シート」にリンクしています。

各設問の結果（レベル）を数値化して集計し、評価基準シートの基準に基づき、運用レベルを計算して表示します。
全ての設問に回答が入力されないと、結果は表示されないよう関数を設定しています。

回答欄の「回答を選んでください」をカウントし、未回答項目がある場合は「未回答の項目があります」と表示します。

ハイパーリンクで「3. 評価結果まとめ」に飛びます。

評価基準は下記の通り、項目毎の回答をポイント化して、集計値で整備レベルの評価を行っています（「b. 評価基準シート」参照）。
「c. 評価結果計算シート」で集計し、関数（VLOOKUP）で該当する「運用レベル」を表示します。

項目単位のレベル		
	Yesの数	ポイント
レベルH	6	5
レベルM	5～3	3
レベルL	2～0	0

運用レベル	
レベルA	50～45ポイント
レベルB	44～35ポイント
レベルC	34～10ポイント
レベルD	9～0ポイント

評価基準を変更する場合は、評価基準シートを変更します。

3．評価結果まとめシート－①

表紙とリンクして自動的に表示されます。

設問への回答前

評価結果まとめ

社名：　　回答日：　　年　　月　　日

1．整備状況

	1．基本ルール	2．管理ルール			3．啓発活動	4．モニタリング	ポイント合計	整備レベル
		データ･ID	インフラ	トラブル対応				
各項目のレベル							0	
ポイント	未回答	未回答	未回答	未回答	未回答	未回答		

	ポイント	
	設問1,3,4	設問2
①全てある/全て行っている	5	3
②一部ある/一部行っている	3	1
③ない/行っていない	0	0

整備レベル	
レベルA	24～21ポイント
レベルB	20～12ポイント
レベルC	11～6ポイント
レベルD	5～0ポイント

2．運用状況

	1．データ管理	2．社有PC	3．外部記憶媒体	4．ネットワーク利用	5．ウィルス・スパイウェア	6．ハッキング	7．情報機器処分		8．社員の故意	9．委託業者	ポイント合計	運用レベル
							自社	外部委託				
Yesの数	0	0	0	0	0	0	0	0	0	0		
各項目のレベル											0	
ポイント	0	0	0	0	0	0	0	0	0	0		

＊無の場合は5ポイントで計算します。

項目単位のレベル		
	Yesの数	ポイント
レベルH	6	5
レベルM	5～3	3
レベルL	2～0	0

運用レベル	
レベルA	50～45ポイント
レベルB	44～35ポイント
レベルC	34～10ポイント
レベルD	9～0ポイント

3．総合評価ランク

《総合評価》

整備＼運用	D	C	B	A
A	C	B	A	A
B	C	C	B	A
C	D	C	C	B
D	D	D	C	C

改善活動へ

↑リンクをクリックして進んでください。

ハイパーリンクで「4．改善活動」に飛びます。
「改善活動」に関する回答を求めない場合は非表示又は削除してください。

入力された回答は、「b．評価基準シート」および「c．総合評価基準シート」の基準に従いポイント化して集計し、評価結果は「d．集計結果計算シート」に表示されます。
「3．評価結果まとめシート」は「d．集計結果計算シート」の結果をリンクして表示しています。

3．評価結果まとめシート－②

《回答事例》

整備状況の回答を設問ごとにレベルとポイントで表示し、整備レベルのポイント合計と整備レベルの全体評価が表示されます。

評価結果まとめ　　社名：6B株式会社　　回答日：2015年　12月　21日

1．整備状況

	1．基本ルール	2．管理ルール			3．啓発活動	4．モニタリング	ポイント合計	整備レベル
		データ･ID	インフラ	トラブル対応				
各項目のレベル	M	H	H	H	M	M	18	B
ポイント	3	3	3	3	3	3		

	ポイント	
	設問1,3,4	設問2
①全てある/全て行っている	5	3
②一部ある/一部行っている	3	1
③ない/行っていない	0	0

整備レベル	
レベルA	24～21ポイント
レベルB	20～12ポイント
レベルC	11～6ポイント
レベルD	5～0ポイント

2．運用状況

	1．データ管理	2．社有PC	3．外部記憶媒体	4．ネットワーク利用	5．ウィルス・スパイウェア	6．ハッキング	7．情報機器処分		8．社員の故意	9．委託業者	ポイント合計	運用レベル
							自社	外部委託				
							有	有				
Yesの数	3	5	3	6	6	4	2	5	4	6	27	C
各項目のレベル	L	M	L	H	H	M	L	M	M	H		
ポイント	0	3	0	5	5	3	0	3	3	5		

＊無の場合は5ポイントで計算します。

項目単位のレベル		
	Yesの数	ポイント
レベルH	6	5
レベルM	5～3	3
レベルL	2～0	0

運用レベル	
レベルA	50～45ポイント
レベルB	44～35ポイント
レベルC	34～10ポイント
レベルD	9～0ポイント

2．総合評価ランク

C

！改善が必要です。

《総合評価》

整備＼運用	D	C	B	A
A	C	B	A	A
B	C	C	B	A
C	D	C	C	B
D	D	D	C	C

改善活動へ

↑リンクをクリックして進んでください。

運用状況の回答を設問ごとにYesの数、レベルとポイントで表示し、運用レベルのポイント合計と運用レベルの全体評価が表示されます。

運用レベルと整備レベルの全体評価に基づき、マトリックスで総合評価ランクが判定され、A~Dの４段階で表示されます。
レベルに応じて、メッセージも表示されます。（「改善が必要です」など）

4. 改善活動シート-①

改善策の策定を評価と同時に行わない場合はこのシートは非表示にします

改善状況回答前-①

表紙とリンクして自動的に表示さ

改善活動

社名：6B株式会社

1. 評価結果

整備レベル	運用レベル	総合評価ランク
B	C	C
！改善が必要です。		

《総合評価》

整備＼運用	D	C	B	A
A	C	B	A	A
B	C	C	B	A
C	D	C	C	B
D	D	D	C	C

整備レベル、運用レベル、総合評価が評価結果まとめシードとリンクして自動的に表示されます。

2. 改善方針

レベルがM・Lの項目について、改善状況、改善時期の回答をお願いします。
補足事項等がありましたら、適宜フリーコメント欄を利用してください。

設問毎の整備レベルが自動的に表示されます。

1）整備状況

＊「回答を選んでください」が表示された項目について、回答を選んでください。

	1. 基本ルール	2. 管理ルール			3. 啓発活動	4. モニタリング
		データ･ID	インフラ	トラブル対応		
評価結果	M	H	H	H	M	M
改善状況	回答を選んでください				回答を選んでください	回答を選んでください
改善時期	回答を選んでください				回答を選んでください	回答を選んでください
フリーコメント						

レベルM、Lの項目については、「回答を選んでください」が表示されます。
回答者には改善状況、改善時期をプルダウンメニューから選択してもらいます。
なお、レベルHの項目は回答不要のため、条件付書式でセル色が「グレー」に着色されます。

4. 改善活動シート-②

改善状況回答前-②

2）運用状況

＊「回答を選んでください」が表示された項目について、回答を選んでください。

	1. データ管理	2. 社有PC	3. 外部記憶媒体	4. ネットワーク利用	5. ウィルス・スパイウェア	6. ハッキング
評価結果	L	M	L	H	H	M
改善状況	回答を選んでください	回答を選んでください	回答を選んでください			回答を選んでください
改善時期	回答を選んでください	回答を選んでください	回答を選んでください			回答を選んでください
フリーコメント						

＊「回答を選んでください」が表示された項目について、回答を選んでください。

	7. 情報機器処分		8. 社員の故意	9. 委託業者
	自社	外部委託		
	有	有		
評価結果	L	M	M	H
改善状況	回答を選んでください	回答を選んでください	回答を選んでください	
改善時期	回答を選んでください	回答を選んでください	回答を選んでください	
フリーコメント				

4. 改善活動シート-③

《回答事例》

改善活動

社名：6B株式会社

1. 評価結果

整備レベル	運用レベル	総合評価ランク
B	C	C
！改善が必要です。		

《総合評価》

		運用			
		D	C	B	A
整備	A	C	B	A	A
	B	C	C	B	A
	C	D	C	C	B
	D	D	D	C	C

2. 改善方針

レベルがM・Lの項目について、改善状況、改善時期の回答をお願いします。
補足事項等がありましたら、適宜フリーコメント欄を利用してください。

「③改善の必要なし」を選択すると、改善時期欄は回答不要なため、条件付書式でブルーに着色されます。

1）整備状況

＊「回答を選んでください」が表示された項目について、回答を選んでください。

	1. 基本ルール	2. 管理ルール			3. 啓発活動	4. モニタリング
		データ・ID	インフラ	トラブル対応		
評価結果	M	H	H	H	M	M
改善状況	①今後改善の必要あり				③改善の必要なし	②現在、改善中
改善時期	③1年以内に完了					①3ヶ月以内に完了
フリーコメント						

改善状況欄、改善時期欄はプルダウンメニューから回答を選択します。

4. 改善活動シート-④

《回答事例》

2）運用状況

＊「回答を選んでください」が表示された項目について、回答を選んでください。

	1. データ管理	2. 社有PC	3. 外部記憶媒体	4. ネットワーク利用	5. ウィルス・スパイウェア	6. ハッキング
評価結果	L	M	L	H	H	M
改善状況	①今後改善の必要あり	①今後改善の必要あり	①今後改善の必要あり			③改善の必要なし
改善時期	②6ヶ月以内に完了	④完了時期未定	③1年以内に完了			
フリーコメント						

＊「回答を選んでください」が表示された項目について、回答を選んでください。

	7. 情報機器処分		8. 社員の故意	9. 委託業者
	自社	外部委託		
	有	有		
評価結果	L	M	M	H
改善状況	③改善の必要なし	③改善の必要なし	①今後改善の必要あり	
改善時期			②6ヶ月以内に完了	
改善状況	自社で処分することはあまりないため、リスクは大きくないと認識している。		既に改善に着手している。	

CSA企画部門用シート

（CSA実施者へ配付する際は非表示にします）

a. 回答用選択肢
b. 評価基準
c. 総合評価
d. 評価結果計算
e. 回答集計
f. コメント集計

a.回答用選択肢シート

【回答用選択肢】					
整備状況用	回答を選んでください	①全てある	②一部ある	③ない	
	回答を選んでください	①全て行っている	②一部行っている	③行っていない	
運用状況用	回答を選んでください	①Yes	②No		
改善検討	回答を選んでください	①今後改善の必要あり	②現在、改善中	③改善の必要なし	
改善完了時期	回答を選んでください	①3ヶ月以内に完了	②6ヶ月以内に完了	③1年以内に完了	④完了時期未定

プルダウンメニューに表示させる回答の選択肢です。選択肢の数、内容を変更する場合はこのシートを変更します。

b.評価基準シート

整備評価の基準

VLOOKUP参照用データ

設問1,3,4	設問2	項目レベル
0	0	L
3	1	M
5	3	H

ポイント数	レベル
5～ 0	D
11～ 6	C
20～ 12	B
24～ 21	A

整備レベル	
レベルA	24～21ポイント
レベルB	20～12ポイント
レベルC	11～6ポイント
レベルD	5～0ポイント

	ポイント	
	設問1,3,4	設問2
①全てある/全て行っている	5	3
②一部ある/一部行っている	3	1
③ない/行っていない	0	0

運用評価の基準

Yesの数	ポイント	項目レベル
3～ 0	0	L
5～ 4	3	M
6～ 6	5	H
該当なし	5	N/A

ポイント数	レベル
9～ 0	D
34～ 10	C
44～ 35	B
50～ 45	A

運用レベル	
レベルA	50～45ポイント
レベルB	44～35ポイント
レベルC	34～10ポイント
レベルD	9～0ポイント

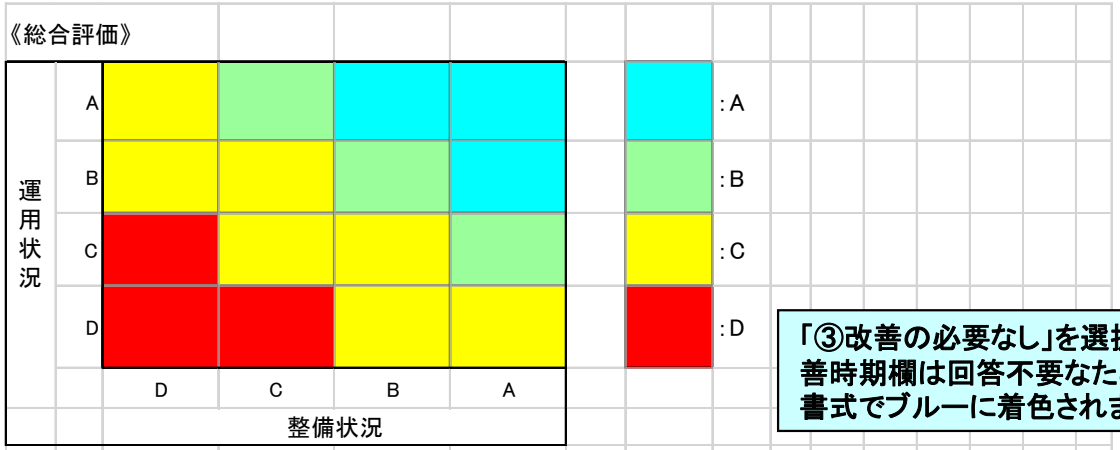
項目単位のレベル		
	Yesの数	ポイント
レベルH	6	5
レベルM	5～3	3
レベルL	2～0	0

レベルコメント

レベル	コメント
D	！！早急に改善が必要です。
C	！改善が必要です。
B	改善の余地があります。
A	問題ありません。

評価基準を判定するためのシートです。回答の集計結果でレベルを定めています。評価基準を変更する場合はこのシートを修正します。
ブルーに着色されている部分を「評価結果計算シート」が参照しています。
白い部分は、「評価結果まとめシート」、「評価結果計算シート」に表示している画像（表）の元データです。リンク貼付になっていますので、この表を修正すると、他のシートの図も自動で変更されます。

C.総合評価シート



「③改善の必要なし」を選択すると、改善時期欄は回答不要なため、条件付書式でブルーに着色されます。

《総合評価》

		運用			
		D	C	B	A
整備	A	C	B	A	A
	B	C	C	B	A
	C	D	C	C	B
	D	D	D	C	C

	総合評価1
AA	A
AB	A
AC	B
AD	C
BA	A
BB	B
BC	C
BD	C
CA	B
CB	C
CC	C
CD	D
DA	C
DB	C
DC	D
DD	D

総合評価判定するためのシートです。整備レベルの結果と運用レベルの結果のマトリックスで総合評価レベルを定めています。
赤枠の部分を「評価結果計算シート」の総合評価欄がVLOOKUPで参照しています。
総合評価の基準を変更する場合はこのシートの赤枠部分修正します。

d.評価結果計算シート

評価結果計算シート

1．整備状況

	基本ルール	管理ルール			啓発活動	モニタリング	合計	整備レベル
		データ・ID	インフラ	トラブル対応				
レベル	M	H	H	H	M	M	18	B
ポイント	3	3	3	3	3	3		
		ポイント基準が異なるため、LOOKUPの式に注意				未回答数	0	

	ポイント	
	設問1,3,4	設問2
①全てある/全て行っている	5	3
②一部ある/一部行っている	3	1
③ない/行っていない	0	0

整備レベル	
レベルA	24～21ポイント
レベルB	20～12ポイント
レベルC	11～6ポイント
レベルD	5～0ポイント

2．運用状況

	データ管理	社有PC	外部記憶媒体	ネットワーク利用	ウィルス・スパイウェア	ハッキング	情報機器処分		社員の故意	委託業者	合計	運用レベル
							自社	外部委託				
							有	有				
Yesの数	3	5	3	6	6	4	2	5	4	6	27	C
未回答数	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*		
レベル	L	M	L	H	H	M	L	M	M	H		
ポイント	0	3	0	5	5	3	0	3	3	5		
						＊無の場合は5ポイントで計算				未回答数	0	

項目単位のレベル		
	Yesの数	ポイント
レベルH	6	5
レベルM	5～3	3
レベルL	2～0	0

運用レベル	
レベルA	50～45ポイント
レベルB	44～35ポイント
レベルC	34～10ポイント
レベルD	9～0ポイント

回答を集計し、評価結果からレベルを計算するシートです。計算結果は「3．評価まとめシート」にリンクしています。
集計結果に基づき、評価基準シートのレベルをVLOOKUPで参照し、表示しています。

e.回答リスト

Control Self-Assessment

《整備状況に関する設問》		
全てある（全て行っている）：1　一部ある（一部行っている）：2　ない（行っていない）：3	0	
1 情報セキュリティに関する基本ルール		未回答
2 管理・対応ルール		
データ・ID管理ルール		未回答
インフラ管理ルール		未回答
トラブル対応ルール		未回答
3 定期的な啓発活動		未回答
4 モニタリング・監視（定期・常時）		未回答
整備レベル／ポイント計		0

《運用状況に関する設問》		
Yes：1　No：0		
1 データの不適切な管理（保管・廃棄等）による情報漏洩への対応		0
1）リスクアセスメントに基づいて、機密情報の管理レベル、管理方法を定めていますか。またそれを定期的に見直していますか。		未回答
2）機密情報について、情報管理台帳を作成して管理していますか。		未回答
3）機密情報を記録した紙媒体・記憶媒体の保管、廃棄方法等のルールを周知徹底していますか。		未回答
4）機密情報についてその内容に応じた機密レベルを明示するとともにアクセス権限を明確にして管理していますか。		未回答
5）機密情報を廃棄した場合は記録を残していますか。		未回答
6）機密書類は、シュレッダーまたは機密処理ボックスなど、管理レベルに応じた方法で処分していますか。		未回答
2 PC・タブレット・スマートフォン等の盗難、紛失による情報漏洩への対応		0
1）PC・タブレット・スマートフォン等の業務への利用は社有のものに限定していますか。		未回答
2）社有のPC・タブレット・スマートフォン等について、台帳管理を行っていますか。		未回答
3）社有のPCの社外持出しを、制限・記録していますか。		未回答
4）社有のPC・タブレット・スマートフォン等の紛失・盗難が発生した際の連絡ルート・連絡方法は決まっていますか。		未回答
5）社有のPC・タブレット・スマートフォン等の紛失・盗難に備えた技術的な対策（暗号化等）を行っていますか。		未回答
6）社有のPC・タブレット・スマートフォン等の利用に関するルール等に違反した従業員に対し、注意、警告、懲罰等を行っていますか。		未回答
3 USBメモリ等の外部記憶媒体の盗難、紛失による情報漏洩への対応		0
1）USBメモリ等の外部記憶媒体の業務への利用は社有のものに限定していますか。		未回答
2）USBメモリ等の外部記憶媒体について、台帳管理を行っていますか。		未回答
3）USBメモリ等の外部記憶媒体の社外持出しを、制限・記録していますか。		未回答
4）USBメモリ等の外部記憶媒体の紛失・盗難が発生した際の連絡ルート・連絡方法は決まっていますか。		未回答
5）USBメモリ等の外部記憶媒体の紛失・盗難に備えた技術的な対策（暗号化等）を行っていますか。		未回答
6）USBメモリ等の外部記憶媒体の利用関するルール等に違反した従業員に対し、注意、警告、懲罰等を行っていますか。		未回答
4 ネットワーク利用による情報漏洩への対応		0
1）インターネットで閲覧できるサイトを制限していますか。		未回答
2）インターネットの利用状況の監視を行い、通信記録を一定期間保存していますか。		未回答
3）クラウドサービスの利用は禁止又は会社指定のサービスに限定していますか。		未回答
4）電子メールの利用状況の監視を行い、通信記録を一定期間保存していますか。		未回答
5）社有PCの社外ネットワーク（出張先のホテル、自宅など）への接続を禁止又は制限していますか。		未回答
6）ネットワーク利用に関するルール等に違反した従業員に対し、注意、警告、懲罰等を行っていますか。		未回答
5 社内PCのウィルスやスパイウェア感染による情報漏洩への対応		0
1）社外から持ち込んだ外部記憶媒体を社有PCで利用する前にウィルスチェックを行っていますか。		未回答
2）社有PCについて、月に1回以上、ウィルスチェックを実施していますか。		未回答
3）社外からの電子メールの添付ファイルについて、ファイルを開く前にウィルスチェックを実施していますか。		未回答
4）ウィルス検知ソフトウェアおよびウィルス定義ファイルは常に最新版となるよう更新していますか。		未回答
5）インターネットから社有PCにソフトウェアをダウンロードすることを禁止又は制限していますか。		未回答
6）ウィルス検知または感染した際の対応方法を社内に周知徹底していますか。		未回答

6 ネットワーク上のハッキングによる情報漏洩への対応		0
1）ユーザーIDの棚卸を定期的に行っていますか。		未回答
2）パスワードを定期的に変更するシステムとなっていますか。（変更しないとシステム利用不可となるようなシステム）		未回答
3）特権IDの管理は一元的に行い、必要に応じ貸し出すとともに、パスワードをその都度変更していますか。		未回答
4）ネットワーク内のPC全てに侵入防止ソフト及びウイルス除去ソフトを入れ、OSも含めて常に最新の状態に保っていますか。		未回答
5）共有サーバ（ファイルサーバ）内の情報を暗号化していますか。		未回答
6）Firewall、侵入検知システム（IDS）、侵入防御システム（IPS）などの侵入対策を行っていますか。		未回答
7 情報機器処分時のデータ消去が不十分だったことによる漏洩		
1)情報機器を処分する際、データ消去を自社で行っていますか？　①Yesを選択すると設問が表示され		回答を選んでください
【自社で実施】		0
1）データ消去についての社内で統一したルールと手順はありますか。		未回答
2）データ消去を一元的に行う部署は決まっていますか。		未回答
3）データ消去は、専用のデータ消去ソフトの利用、強磁気破壊装置の利用、ハードディスクの物理的破壊のいずれかの方法で行っていますか。		未回答
4）データ消去作業は複数名で行っていますか。		未回答
5）対象となった機器が全台漏れなく作業されたことを確認していますか。		未回答
6）データ消去作業後に、サンプル等で確実にデータが消去されたことを確認してますか。		未回答
2)情報機器を処分する際、データ消去を外部業者に委託していますか？　①Yesを選択すると設問が表示され		回答を選んでください
【外部業者へ委託】		0
1）データ消去についての社内で統一したルールと手順はありますか。		未回答
2）外部業者への依頼を一元的に行う部署は決まっていますか。		未回答
3）外部業者がどのような方法でデータ消去しているかを把握していますか。		未回答
4）データ消去後、委託業者から破壊証明書を入手していますか。		未回答
5）対象となる機器を全台漏れなく外部業者に引き渡したことを確認していますか。		未回答
6）データ消去作業後に、サンプル等で確実にデータが消去されたことを確認してますか。		未回答
8 社員の故意による情報漏洩への対応		0
1）守秘義務など情報セキュリティに関する誓約書を従業員から入手していますか。		未回答
2）PCのファイルの操作やアプリケーションの利用を監視、記録するシステムを導入していますか。		未回答
3）退職した従業員（社員・派遣社員等）のIDを即時に削除していますか。また、異動した場合は速やかにアクセス権限を変更していますか。		未回答
4）社外へのメール送信時に上司の内容確認、送信承認を行うシステムが導入されていますか。		未回答
5）個人所有の端末（PC、タブレット、スマートフォン）の社内ネットワークへの接続を禁止又は制限していますか。		未回答
6）入退出管理、監視カメラ等、社員の行動を監視するシステムが導入されていますか。		未回答
9 委託業者からの情報漏洩への対応		0
1）外部委託先の選定基準、契約手続き(適正な作業契約のため、契約手続および責任者の承認手続き)は、明確に定められていますか？		未回答
2）安全性確保のため、機密保護、安全運行等に関する項目を盛り込んだ作業契約を締結していますか？		未回答
3）外部委託先の要員のセキュリティ管理を適切に行うため、外部委託内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種のルールの遵守を義務付け、教育をしていますか？		未回答
4）外部に委託した作業内容を確認するため、業務組織の整備を行うとともに、作業契約に基づき管理、検証を行っていますか？		未回答
5）外部委託先から情報漏洩が発生した場合の業務手順は、明確になっていますか？		未回答
6）外部委託先の監査権限を持つことを明確に取り決めていますか？		未回答
運用レベル（総合）		0

総合評価	

項目毎の回答を一覧にまとめたシートです。
結果の集計に利用できます。

e.回答リスト　-入力例-

Control Self-Assessment

《整備状況に関する設問》

全てある（全て行っている）：1　一部ある（一部行っている）：2　ない（行っていない）：3

	D2カンパニー	
1 情報セキュリティに関する基本ルール	H	5
2 管理・対応ルール		
データ・ID管理ルール	H	1
インフラ管理ルール	H	3
トラブル対応ルール	H	3
3 定期的な啓発活動	M	3
4 モニタリング・監視（定期・常時）	M	3
整備レベル／ポイント計	B	18

《運用状況に関する設問》

Yes：1　No：0

1 データの不適切な管理（保管・廃棄等）による情報漏洩への対応	L	0
1）リスクアセスメントに基づいて、機密情報の管理レベル、管理方法を定めていますか。またそれを定期的に見直していますか。		1
2）機密情報について、情報管理台帳を作成して管理していますか。		0
3）機密情報を記録した紙媒体・記憶媒体の保管、廃棄方法等のルールを周知徹底していますか。		0
4）機密情報についてその内容に応じた機密レベルを明示するとともにアクセス権限を明確にして管理していますか。		1
5）機密情報を廃棄した場合は記録を残していますか。		0
6）機密書類は、シュレッダーまたは機密処理ボックスなど、管理レベルに応じた方法で処分していますか。		1
2 PC・タブレット・スマートフォン等の盗難、紛失による情報漏洩への対応	M	3
1）PC・タブレット・スマートフォン等の業務への利用は社有のものに限定していますか。		0
2）社有のPC・タブレット・スマートフォン等について、台帳管理を行っていますか。		0
3）社有のPCの社外持出しを、制限・記録していますか。		1
4）社有のPC・タブレット・スマートフォン等の紛失・盗難が発生した際の連絡ルート・連絡方法は決まっていますか。		1
5）社有のPC・タブレット・スマートフォン等の紛失・盗難に備えた技術的な対策（暗号化等）を行っていますか。		1
6）社有のPC・タブレット・スマートフォン等の利用に関するルール等に違反した従業員に対し、注意、警告、懲罰等を行っていますか。		1
3 USBメモリ等の外部記憶媒体の盗難、紛失による情報漏洩への対応	M	3
1）USBメモリ等の外部記憶媒体の業務への利用は社有のものに限定していますか。		1
2）USBメモリ等の外部記憶媒体について、台帳管理を行っていますか。		0
3）USBメモリ等の外部記憶媒体の社外持出しを、制限・記録していますか。		1
4）USBメモリ等の外部記憶媒体の紛失・盗難が発生した際の連絡ルート・連絡方法は決まっていますか。		1
5）USBメモリ等の外部記憶媒体の紛失・盗難に備えた技術的な対策（暗号化等）を行っていますか。		1
6）USBメモリ等の外部記憶媒体の利用関するルール等に違反した従業員に対し、注意、警告、懲罰等を行っていますか。		1
4 ネットワーク利用による情報漏洩への対応	M	3
1）インターネットで閲覧できるサイトを制限していますか。		1
2）インターネットの利用状況の監視を行い、通信記録を一定期間保存していますか。		1
3）クラウドサービスの利用は禁止又は会社指定のサービスに限定していますか。		1
4）電子メールの利用状況の監視を行い、通信記録を一定期間保存していますか。		1
5）社有PCの社外ネットワーク（出張先のホテル、自宅など）への接続を禁止又は制限していますか。		0
6）ネットワーク利用に関するルール等に違反した従業員に対し、注意、警告、懲罰等を行っていますか。		1
5 社内PCのウィルスやスパイウェア感染による情報漏洩への対応	H	5
1）社外から持ち込んだ外部記憶媒体を社有PCで利用する前にウィルスチェックを行っていますか。		1
2）社有PCについて、月に1回以上、ウィルスチェックを実施していますか。		1
3）社外からの電子メールの添付ファイルについて、ファイルを開く前にウィルスチェックを実施していますか。		1
4）ウィルス検知ソフトウェアおよびウィルス定義ファイルは常に最新版となるよう更新していますか。		1
5）インターネットから社有PCにソフトウェアをダウンロードすることを禁止又は制限していますか。		1
6）ウィルス検知または感染した際の対応方法を社内に周知徹底していますか。		1

6 ネットワーク上のハッキングによる情報漏洩への対応	H	5
1）ユーザーIDの棚卸を定期的に行っていますか。		1
2）パスワードを定期的に変更するシステムとなっていますか。（変更しないとシステム利用不可となるようなシステム）		1
3）特権IDの管理は一元的に行い、必要に応じ貸し出すとともに、パスワードをその都度変更していますか。		1
4）ネットワーク内のPC全てに侵入防止ソフト及びウイルス除去ソフトを入れ、OSも含めて常に最新の状態に保っていますか。		1
5）共有サーバ（ファイルサーバ）内の情報を暗号化していますか。		1
6）Firewall、侵入検知システム（IDS）、侵入防御システム（IPS）などの侵入対策を行っていますか。		1
7 情報機器処分時のデータ消去が不十分だったことによる漏洩		
1）情報機器を処分する際、データ消去を自社で行っていますか？　①Yesを選択すると設問が表示されます②No		
【自社で実施】	N/A	5
1）データ消去についての社内で統一したルールと手順はありますか。		対象外
2）データ消去を一元的に行う部署は決まっていますか。		対象外
3）データ消去は、専用のデータ消去ソフトの利用、強磁気破壊装置の利用、ハードディスクの物理的破壊のいずれかの方法で行っていますか。		対象外
4）データ消去作業は複数名で行っていますか。		対象外
5）対象となった機器が全台漏れなく作業されたことを確認していますか。		対象外
6）データ消去作業後に、サンプル等で確実にデータが消去されたことを確認してますか。		対象外
2）情報機器を処分する際、データ消去を外部業者に委託していますか？　①Yesを選択すると設問が表示されます①Yes		
【外部業者へ委託】	M	3
1）データ消去についての社内で統一したルールと手順はありますか。		0
2）外部業者への依頼を一元的に行う部署は決まっていますか。		1
3）外部業者がどのような方法でデータ消去しているかを把握していますか。		1
4）データ消去後、委託業者から破壊証明書を入手していますか。		1
5）対象となる機器を全台漏れなく外部業者に引き渡したことを確認していますか。		1
6）データ消去作業後に、サンプル等で確実にデータが消去されたことを確認してますか。		0
8 社員の故意による情報漏洩への対応	M	3
1）守秘義務など情報セキュリティに関する誓約書を従業員から入手していますか。		1
2）PCのファイルの操作やアプリケーションの利用を監視、記録するシステムを導入していますか。		1
3）退職した従業員（社員・派遣社員等）のIDを即時に削除していますか。また、異動した場合は速やかにアクセス権限を変更していますか。		1
4）社外へのメール送信時に上司の内容確認、送信承認を行うシステムが導入されていますか。		0
5）個人所有の端末（PC、タブレット、スマートフォン）の社内ネットワークへの接続を禁止又は制限していますか。		1
6）入退出管理、監視カメラ等、社員の行動を監視するシステムが導入されていますか。		1
9 委託業者からの情報漏洩への対応	H	5
1）外部委託先の選定基準、契約手続き(適正な作業契約のため、契約手続および責任者の承認手続き)は、明確に定められていますか？		1
2）安全性確保のため、機密保護、安全運行等に関する項目を盛り込んだ作業契約を締結していますか？		1
3）外部委託先の要員のセキュリティ管理を適切に行うため、外部委託内容や作業の範囲に応じて、セキュリティポリシーをはじめとした各種のルールの遵守を義務付け、教育をしていますか？		1
4）外部に委託した作業内容を確認するため、業務組織の整備を行うとともに、作業契約に基づき管理、検証を行っていますか？		1
5）外部委託先から情報漏洩が発生した場合の業務手順は、明確になっていますか？		1
6）外部委託先の監査権限を持つことを明確に取り決めていますか？		1
運用レベル（総合）	B	35
	BB	
総合評価	B	

各実施者の赤枠の部分をコピーして一覧にするとヒートマップになります（次ページ参照）。

e.回答リスト　－ヒートマップ－

《整備状況に関する設問》 全てある（全て行っている）：1　一部ある（一部行っている）：2　ない（行っていない）	A社		B社		C社		D社		E社		F社		G社		H社		I社		J社		K社		L社		M社		N社		O社		P社		Q社	
1 情報セキュリティに関する基本ルール	M	3	H	5	H	5	H	5	M	3	H	5	H	5	M	3	M	3	H	5	M	3	M	3	H	5	L	0	H	5	M	3	H	5
2 管理・対応ルール																																		
データ・ID管理ルール	H	3	H	3	H	3	H	3	M	1	M	1	M	1	M	1	H	3	H	3	H	3	M	1	H	3	L	0	H	3	H	3	H	3
インフラ管理ルール	H	3	H	3	H	3	H	3	M	1	M	1	M	1	M	1	M	1	H	3	H	3	M	1	H	3	L	0	H	3	H	3	H	3
トラブル対応ルール	H	3	H	3	H	3	H	3	M	1	H	3	M	1	H	3	M	1	H	3	H	3	M	1	H	3	L	0	H	3	H	3	H	3
3 定期的な啓発活動	M	3	H	5	H	5	H	5	H	5	M	3	H	5	M	3	M	3	H	5	M	3	M	3	H	5	L	0	H	5	H	5	M	3
4 モニタリング・監視（定期・常時）	M	3	H	5	H	5	H	5	M	3	H	5	M	3	M	3	H	5	M	3	H	5	M	3	H	5	L	0	H	5	M	3	H	5
整備レベル／ポイント計	B	18	A	24	A	24	A	24	B	14	B	18	B	16	B	14	B	16	A	22	B	20	B	12	A	24	D	0	A	24	B	20	A	22

《運用状況に関する設問》 Yes：1　No：0																																		
1 データの不適切な管理（保管・廃棄等）による情報漏洩への対応	L	0	H	5	H	5	H	5	H	5	M	3	H	5	L	0	L	0	M	3	M	3	L	0	H	5	L	0	M	3	M	3	H	5
2 PC・タブレット・スマートフォン等の盗難、紛失による情報漏洩への対応	M	3	H	5	H	5	M	3	M	3	M	3	L	0	H	5	M	3	M	3	M	3	H	5	H	5	L	0	H	5	H	5	H	5
3 USBメモリ等の外部記憶媒体の盗難、紛失による情報漏洩への対応	L	0	M	3	H	5	H	5	H	5	H	5	M	3	M	3	M	3	M	3	H	5	M	3	H	5	L	0	M	3	H	5	H	5
4 ネットワーク利用による情報漏洩への対応	H	5	H	5	H	5	H	5	M	3	L	0	M	3	M	3	M	3	M	3	H	5	H	5	H	5	L	0	M	3	H	5	H	5
5 社内PCのウィルスやスパイウェア感染による情報漏洩への対応	H	5	M	3	M	3	H	5	L	0	H	5	M	3	H	5	M	3	M	3	M	3	M	3	H	5	M	3	M	3	H	5	H	5
6 ネットワーク上のハッキングによる情報漏洩への対応	M	3	M	3	M	3	M	3	H	5	H	5	M	3	M	3	M	3	M	3	M	3	M	3	H	5	L	0	M	3	M	3	M	3
7 情報機器処分時のデータ消去が不十分だったことによる漏洩																																		
1)情報機器を処分する際、データ消去を自社で行っていますか？	①Yes		①Yes		①Yes		②No		②No		②No		②No		①Yes		②No		②No		②No		②No		②No		①Yes		①Yes		②No		①Yes	
【自社で実施】	L	0	M	3	H	5	N/A	5	N/A	5	N/A	5	N/A	5	M	3	N/A	5	N/A	5	N/A	5	N/A	5	N/A	5	L	0	M	3	N/A	5	M	3
2)情報機器を処分する際、データ消去を外部業者に委託していますか？	①Yes		①Yes		①Yes		①Yes		①Yes		①Yes		①Yes		②No		①Yes		①Yes		①Yes		①Yes		①Yes		②No		①Yes		①Yes		②No	
【外部業者へ委託】	M	3	M	3	H	5	M	3	M	3	L	0	H	0	N/A	0	M	0	M	3	L	0	M	3	M	3	N/A	5	M	3	M	3	N/A	5
8 社員の故意による情報漏洩への対応	M	3	H	5	M	3	H	5	H	5	H	5	M	3	M	3	M	3	H	5	M	3	M	3	M	3	L	0	M	3	H	5	H	5
9 委託業者からの情報漏洩への対応	H	5	H	5	H	5	H	5	M	3	M	3	H	5	L	0	M	3	H	5	M	3	L	0	H	5	L	0	H	5	H	5	H	5
運用レベル（総合）	C	27	B	40	B	44	B	44	B	37	C	34	B	35	C	30	C	29	B	36	C	33	C	30	A	46	D	8	C	34	B	44	A	46

	A社	B社	C社	D社	E社	F社	G社	H社	I社	J社	K社	L社	M社	N社	O社	P社	Q社
	BC	AB	AB	AB	BB	BC	BB	BC	BC	AB	BC	BC	AA	DD	AC	BB	AA
総合評価	C	A	A	A	B	C	B	C	C	A	C	C	A	D	B	B	A

B：35～44ポント

f.コメントリスト

	社名：	
	コメント内容	
整備状況		
運用状況	1. データ管理	
	2. 社有PC	
	3. 外部記憶媒体	
	4. ネットワーク利用	
	5. ウィルス・スパイウェア	
	6. ハッキング	
	7. 情報機器処分	
	自社	
	外部委託	
	8. 社員の故意	
	9. 委託業者	
	全般	

各項目のフリーコメントを一覧表にまとめたシートです。