品質管理・信頼性管理・セキュリティ



品質管理·信頼性管理·セキュリティでのCIOの役割

- ◆ どんな問題が発生するのか想像し、それに対する適切な指示を行う。
- ◆ 予算査定や調達などで、失敗プロジェクトの「入り」をコントロールしたが、走り出したプロジェクトを円滑に送り出し、運用を続けさせる「出」をコントロールするのが、ここでのCIOの役割である。

品質管理·信頼性

品質管理を行うための前提

- ◆ 基礎データをそろえる
 - > システム規模はわかっているか
 - 何がしかのデータを元に、共通尺度であるFPを算出
 - 価格→FP、画面数→FP、KLOC→FP
 - ➤ WBSはかけているか
 - ・ 進捗と品質をあわせて管理するのであれば、基礎となるWBSがしっかりかけている必要がある
 - WBSは網羅性があるのか?WPは10日前後か?
 - ▶ 日常の各種数値を記録しているか
 - バグ数、テスト項目数・・・・
 - トドキュメンテーションの充実
 - 最低整備すべきドキュメントの整備

品質や信頼性を向上させるためのポイント

- ◆ システムの品質や信頼性を向上させるには以下の取り組みが重要である。
 - > さまざまな障害を想像できる力を身につける
 - これが不足していると設計書を見たときにチェックポイントがつかめない
 - 日経コンピュータの動かないコンピュータなどを見て、さまざまなケースをイメージできるよう にトレーニングする
 - ▶ データに基づき沈没しつつあるプロジェクトを予見する
 - 沈没するプロジェクトはさまざまな危険信号を発している
 - ▶ 楽観的に考えない
 - プロジェクトマネージャは、特に前半において、希望的観測により問題の対策を遅らす場合が多い。ユーザ、ベンダの双方に同じ傾向があるので注意が必要である
 - ▶ 品質の悪いシステムを防ぐために
 - 入りを制す
 - 正しい予算や計画にすることでコントロールを行う
 - » 予算査定や調達などで、失敗プロジェクトの「入り」をコントロール
 - 流れを制す
 - 開発工程をモーターすること、傾向把握からコントロールを行う
 - » 走り出したプロジェクトが外れた方向に進んでいないか「流れ」をモニター
 - 内容的にはレビューで潰していく
 - 出を制す
 - 納品の検査で納品前後のコントロールを行う
 - » 運用側で受け入れられるのか「出」をコントロール

認証は信用できるのか

- ◆ ISO9000を取得している企業のプロダクト品質は高いのか?
- ◆ CMMを持っている企業の品質は高いのか?
- ◆ No!!
- ◆ 見せ掛けだけの認証取得をしている企業が多い
 - ▶ ISO14000を持っているのに真夏にスーツで名刺交換して〈る企業とか
 - ▶ つまりは、理念が浸透していない
- ◆ CMMが出てきたときの企業の反応
 - ▶ ISO9000を持っているのになんで必要なんだ?
 - CMMはマイルストンではなくプロセスで品質を確保する
- ◆ CMM認証企業への質問
 - あなたは何にかかわりましたか?
 - ➤ CMM取得部門からの支援とは具体的になんですか?
- ◆ ISO9000取得企業への質問
 - ▶ ドキュメント以外での品質管理は何をしていますか

品質は人で担保する

- ◆ 品質管理に知見のある人をPMにすることで品質に関する意識 を高めることができる。
- ◆ チームをきちんと見極める
- ◆ 品質担当者は誰ですか
- ◆ 品質管理はどのように行いますか
- ◆ 品質指標値はありますか

要求仕様書(RFP)作成担当と品質の満足度

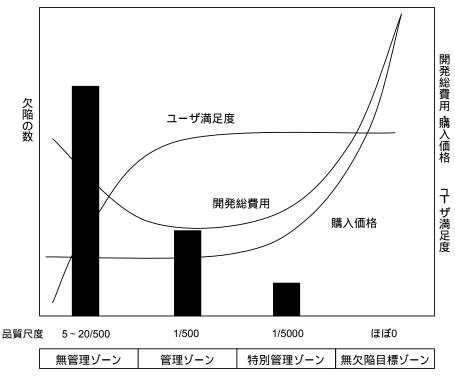
		0%	20%	40%	60%	80%	1009
拠业	要求仕様書はほとんど自社で作成(n=124)	179		'	72%		11%
100人月未避	ベースは自社で作成し、細部は委託先が作成(n=256)	15%		7	3%	;	13%
100	すべて委託先が担当している(n=124)	12%		72	%		6%
5	要求仕様書はほとんど自社で作成(n=82)	12%		62%		269	6 333
要求仕様書はほべつのべつスは自社で作成し、細部すべて委託	ベースは自社で作成し、細部は委託先が作成(n=147)	7%		65%		28%	
100	すべて委託先が担当している(n=59)	7%		68%		25%	688
T T	要求仕様書はほとんど自社で作成(n=47)	13%		62%		269	688
500人月以上	ベースは自社で作成し、細部は委託先が作成(n=94)	7%		63%		30%	797797 649.950
200	すべて委託先が担当している(n=37)	5%		59%		35%	
		N P		□ある程	度は満足	口不	満

品質・信頼性を向上させるためのアプローチ

- ◆ドキュメンテーションの充実
- ◆ ソフトウェアメトリックスの利用
 - ⇒ 詳細は、ソフトウェア開発データ活用ガイドブック
- ◆ チェックのポイント
 - ▶ 入りを制する
 - おかしな計画になっていないか
 - ▶ 流れを制する
 - 外れた方向に進んでいないか
 - ▶ 出を制する
 - 受け入れてよいのか
- ◆ 契約段階でベンダを巻き込んでいくことが重要

品質はむやみに要求すればよいと言う話ではない

- ◆ まず始めに、品質と価格のバランスを理解する必要がある。高度な品質を求めると、 それに対応して指数関数的に開発費用がかかるようになる。また、逆に品質が低い と対応費用が必要となり、安く開発を行ったとしても結局は高いコストが必要になることも多い。ユーザ満足度を意識して品質レベルを決めていく必要がある。
 - ▶ セキュリティについても同様のことが言えるので、コストと信頼性のバランスを熟考の上、セキュリティレベルを考えていく必要がある。



Good Enough Quality を目指す

注1 品質尺度: (納入時から安定稼働期迄の欠陥個数)/欠陥費用(万円) 注2 開発総費用と購入価格のギャップはテスト結果の確認、修正結果の確認のため に要するユーザ側の付加増加費用をイメージ化したもの

参考:稼働率の目標

	SLA項目	レベル1	レベル2	レベル3	レベル4	レベル5
1	稼働率	98%以下	99%	99.9%	99.99%	99.999%以上
2	バックアップ機	なし	あり (部分的)	あり (2/N+1台)	あり (Hot stand by)	あり (Hot stand by)
3	サービス停止時間 ()時間/年	172時間	86時間	8.6時間	50分	5分
4	到着時間	1-6時間(昼) 12時間(夜間	1-6時間	1-3時間(昼) 6時間(夜間	常駐 ケースによっ ては2時	常駐
5	修復時間 ・故障修復 ・再立ち上 げ) 6時間-12時間 10分-1時間	6時間-12時間 10分-1時間	3時間-6時間 10分-1時間	間 3時間-6時間 0分-10分	3時間-6時間 即時
6	費用 ・構築 費用	1.0倍 1.0倍	1.2~1.8倍 1.1~1.3倍	1.2~3倍 1.3~2.0倍	1.5~4倍 2.0~3倍	4~6倍 3~4倍
7	システム構成 (例 必要な機能		NAS	SAN、NAS クラスタリン グ ロードバランシング	SAN クラスタリン グ pート*ハ*ランシンク*	SAN クラスタリング ロードバランシング 三重化、四重化
8	ペナルティ			対象	対豪化	対象
9	(参考)アプリ開発費 用	1倍	1倍	1~2倍	2~3倍	3~5倍 3

各種ソフトウェアメトリックス調査

- ◆ ソフトウェアに関しては多くのデータが公表されている。
 - ▶ ユーザ視点での評価
 - JUAS(日本情報システムユーザ協会)
 - ▶ ベンダ視点での評価
 - IPA(情報処理推進機構)
 - 日科技連
 - ▶ 国際調査
 - ISBSG (International Software Benchmarking Standards Group)



JUAS http://www.juas.or.jp/



IPA http://www.ipa.go.jp/



日本科学技術連盟 http://www.juse.or.jp/



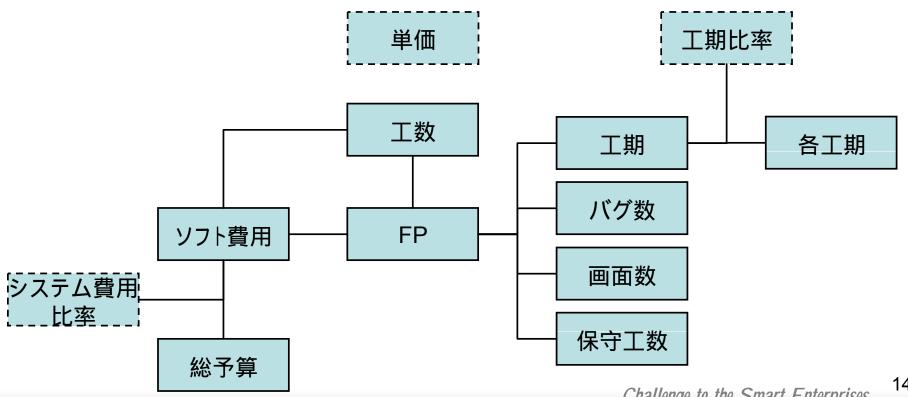
ISBSG http://www.isbsg.org/

各種学会

- ·情報処理学会
- ・ソフトウェア科学会

各種データの関係

◆ ソフトウェアの開発はこれまで経験に依存するところが多かったが、ベンダ内では生 産データを蓄積し、異常プロジェクトの検出に努力している。これらを共通化しようと いう取り組みも始まっており、情報処理推進機構ではソフトウェア開発白書を刊行し ている。また、情報システムユーザ協会では経済産業省と連携して、ユーザから見た 生産性データの蓄積をソフトウェアメトリックス2007として作成している。

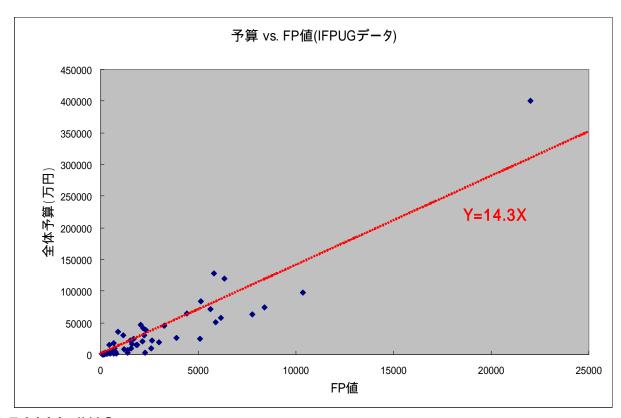


過去のデータを分析する意味

- ◆ 今後、ソフトウェアメトリックスを活用していくためには、過去のデータを分析することが重要である。
 - > 自組織の弱点を把握
 - システムが適正価格で購入されてきたのか?
 - これまで失敗したプロジェクトの原因はなんだったのか
 - > 自組織の傾向を把握
 - 統計とは違った自社、業界特有の傾向を知る
 - 今後の対策用に整理する
 - ▶ ソフトウェアメトリックス活用の練習
 - 開発中のシステムにいきなり導入すると、現場の理解も得られないし、実施している本人も混乱する。

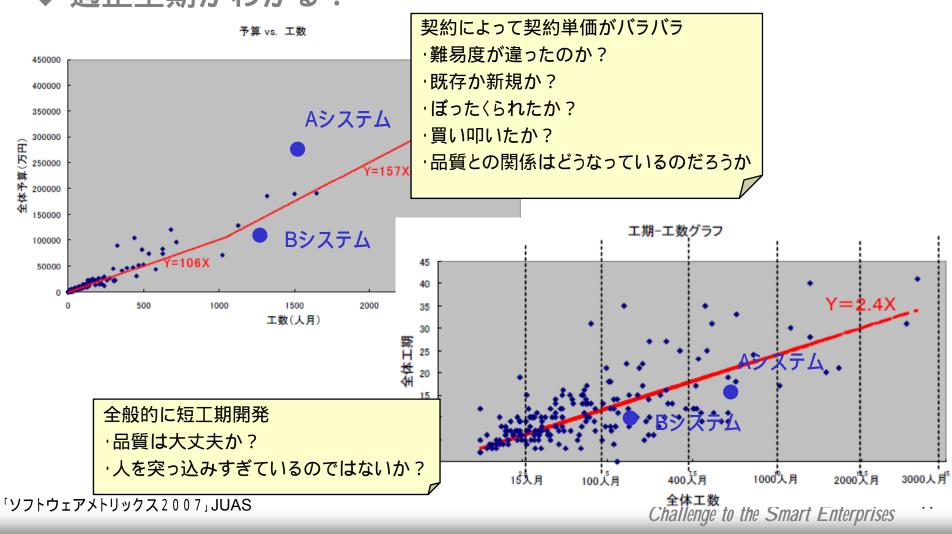
基礎データとしてのFPの算出

◆ FPでないシステムは、予算やステップ数を元に概算のファンクションポイントを推定する。ファンクションポイントを基軸にすることで、開発中の各種情報を横串の比較、推定することが可能になる。



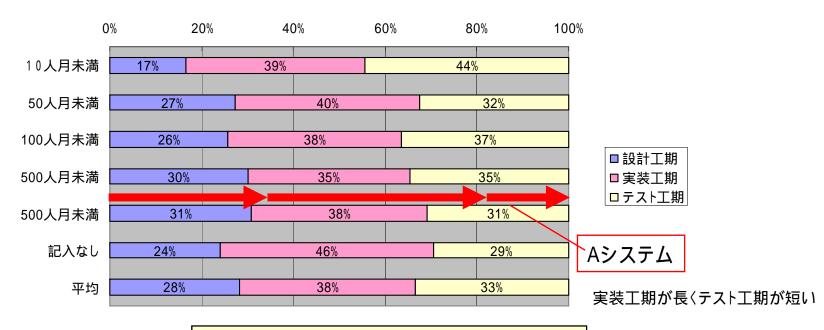
過去データ分析の例

- ◆ 高い買い物か安い買い物かわかる!
- ◆ 適正工期かわかる!



過去データ分析の例

◆ 工期配分が適正かわかる!



テスト工程が短すぎる

- ・品質は大丈夫か?
- ・計画時のスケジュールはどうなっていたのか?
- ·何か遅延の原因があったのか?

過去データ分析の例

- ◆ 適正な品質レベルかわかる!
- ◆ 保守工数が適正かわかる!

	Aランク	Bランク	Cランク	Dランク	Eランク	Fランク
欠陥率	0	0.25未満	0.5未満	1未満	3未満	3以上
割合	9.7%	33.1%	18.8%	17.5%	14.9%	5.8%
件数	15	51	29	27	23	9

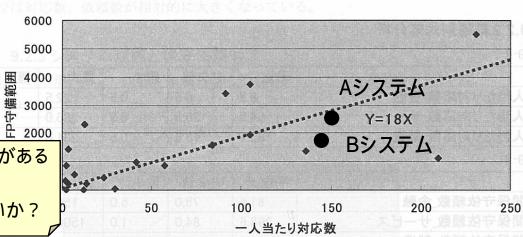
Aシステム

Bシステム

導入時の品質が悪いものがある

- ・目標品質は?
- ・難易度は?
- ·欠陥レベルは?

1人当たり対応数VSFP守備範囲



FP保守範囲が狭いのに対応数が多いシステムがある

- ・納品品質が低かったのではないか?
- ・運用マニュアルが整備されていないのではないか?

演習

◆ システム概要

▶ 3部門で持っていた販売システムを統合し、顧客情報を一元管理するシステムであり、先進の技術を導入しリアルタイムレスポンスを実現するシステムである。

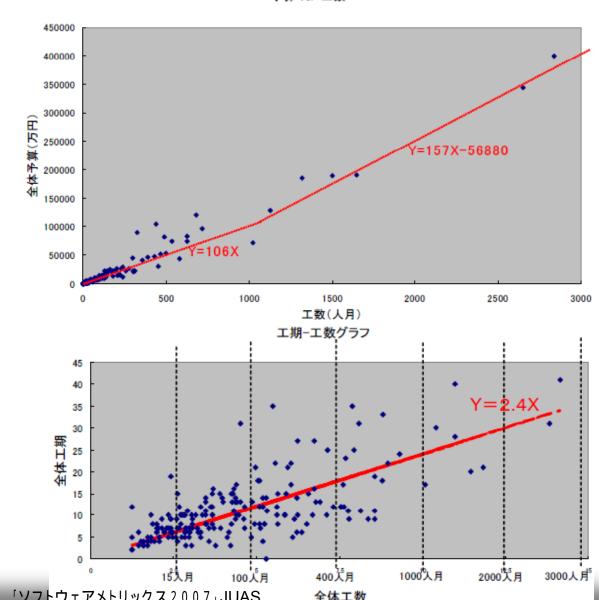
◆ データ

- ▶ 予算 25000万円(設計から導入まで)
- ▶ 工数 350人月
- ⇒ 計画工期 10ヶ月(設計:実装:テスト=2ヶ月:4ヶ月:4ヶ月)
- ▶ 実績工期 10ヶ月(設計:実装:テスト=3ヶ月:5ヶ月:2ヶ月)
- ▶ 欠陥率(フォロー不具合数:総合テスト2での不具合数) 0.63(62:32)
- ➤ FP保守範囲 750FP/人
- ▶ 一人当たり対応数 82件/人
- ◆ 利用部門の感想
 - ▶ 時々止まるが、前のシステムもこんなものだったのであきらめている。
- ◆ システム部門の感想
 - ▶ 他のシステムに較べて、手間がかかる気がする

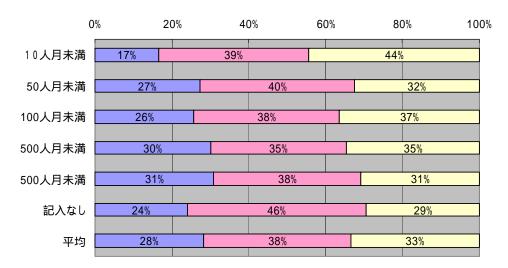
◆ 問題

- 各データをグラフ上にプロットして〈ださい
- ▶ そのシステムの現状に関する評価をしてください
- ▶ どこでプロジェクトマネージャは手を打つべきだったか考えて〈ださい

予算 vs. 工数

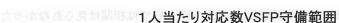


演習

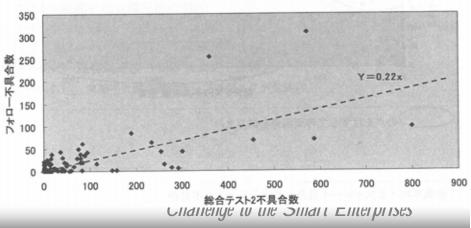


□設計工期 □実装工期 □テスト工期

	Aランク	Bランク	Cランク	Dランク	Eランク	Fランク
欠陥率	0	0.25未満	0.5未満	1未満	3未満	3以上
割合	9.7%	33.1%	18.8%	17.5%	14.9%	5.8%
件数	15	51	29	27	23	9



カットオーバー後の欠陥数vs総合テスト2欠陥数



メトリックス調査に補正は必要か?

- ◆ ソフトウェアのメトリックスデータは統計的に処理されているので、もっと詳細なデータが知りたいことがある。
- ◆ たとえば、言語により生産性が大きく異なることが 知られている。

言語	レベル	LOC/FP
アセンブラ	1.00	320.00
С	2.50	128.00
C + +	5.00	64.00
COBOL	3.00	106.67
FORTRAN	3.00	106.67
P o w e r B u il d e r	20.00	16.00
SQL	25.00	12.80
V B	10.00	32.00
平均	7.63	92.35

「ソフトウェア見積もりの全て」共立出版 平均は、adaなどの言語を含む15言語の平均 レベルは、アセンブラを1としたときの生産性

Source Code Language	Conversio n Ratio (LOC Per Function Point)
Basic Assembly	575
JCL	400
Macro Assembly	400
C	225
C Cobol74(Cobol I) FORTRAN	220
FORTRAN	210
Cobol85(Cobol II)	175
Pascal	160
PL/1	126
RPG I	120
RPG II/III	110
Natural	100
C+ +	80
Java	80
dBaseIII	60
Focus	60
Clipper	60
oracle	60
Sybase	60
dBaseIV	55
Perl	50
JavaScript	50
VBScript	50
Shell Script	50
SAS	50
APL	50

資料 DCG

様々な補正が可能

- ◆ アーキテクチャー別の補正値
- ◆ 新規開発、再開発別の補正値
- ◆ 言語別の品質

SLOCあたりの不具合数

言語平均標準偏差COBOL0.0750.160C0.0510.100VB0.1030.206Java0.1220.330

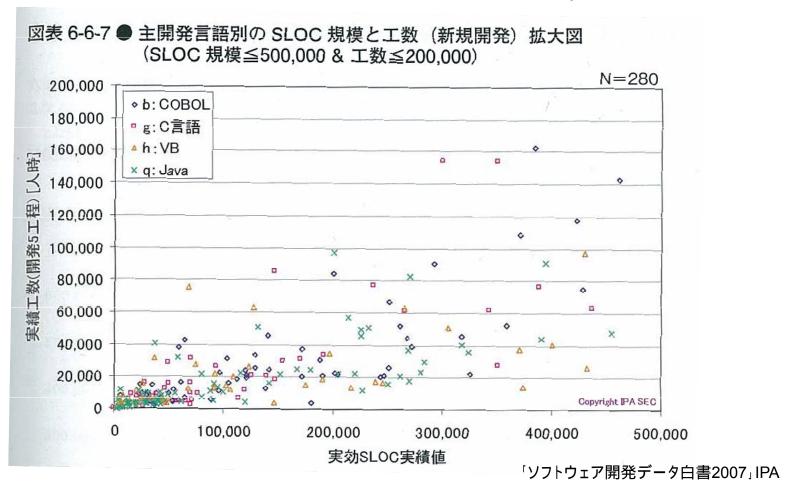
SLOCあたりの不具合数

言語	平均	標準偏差
新規開発	0.119	0.375
改修·保守	0.175	0.694
再開発	0.181	0.417
拡張	0.077	0.192

「ソフトウェア開発データ白書2007」IPA

BUT! 現段階では補正をしなくてもよい

◆ エンジニアリングはまだ夜が明けたばかり。



欠陥除去には何が有効か

- ◆ 全ての工程できちんと検査をしていくことが重要なのはもちろん、 前工程で問題点を潰していくことが重要。
- ◆ 後工程でバグが見つかると、上流工程で発見されたバグの数倍の労力(コスト、時間)がかかる。
 - 要求段階での修正コストを1とすると、アーキテクチャ設計時で3、システムテスト段階で10、出荷後で10~100倍と言われている

	欠陥除去率の最悪の場合の結果(%)				
		最小	中央値	最大値	
設計インスペクション	×				
コードインスペクション	×	30	40	50	
品質保証	×	30	40	30	
正規のテスト	×				

欠陥除去率の最悪の場合の結果(%)					
		最小	中央値	最大値	
設計インスペクション	×	政人		取八世	
コードインスペクション	×				
品質保証	Ť.	32	45	55	
正規のテスト	×				
設計インスペクション	×				
コードインスペクション	×	37	53	60	
品質保証	×	31	55	00	
正規のテスト					
設計インスペクション	×				
コードインスペクション		43	57	66	
品質保証	×	43	37	00	
正規のテスト	×				
設計インスペクション					
コードインスペクション	×	45	60	68	
品質保証	×	40	00	00	
正規のテスト	×				

		欠陥除去率	の最悪の場合	の結果(%)
		最小	中央値	最大値
設計インスペクション	×			
コードインスペクション	×	50	65	75
品質保証		30	05	75
正規のテスト				
設計インスペクション	×			
コードインスペクション		53	68	78
品質保証		33	00	70
正規のテスト	×			
設計インスペクション	×			
コードインスペクション		55	70	80
品質保証	×	00		00
正規のテスト				
設計インスペクション				
コードインスペクション	×	60	75	85
品質保証		00		00
正規のテスト	×			
設計インスペクション				
コードインスペクション	×	65	80	87
品質保証	×			
正規のテスト				
設計インスペクション				
コードインスペクション		70	85	90
品質保証	×			
正規のテスト	×			

		欠陥除去率の最悪の場合の結果(%)		
		最小	中央値	最大値
コードインスペクション	×	75	87	93
品質保証 正規のテスト		. 0	<u> </u>	
設計インスペクション コードインスペクション 品質保証 正規のテスト	×	77	90	95
設計インスペクション コードインスペクション 品質保証 正規のテスト	×	83	95	97
設計インスペクション コードインスペクション 品質保証 正規のテスト	×	85	97	99

	欠陥除去率	欠陥除去率の最悪の場合の結果(%)				
	最小	中央値	最大値			
設計インスペクション						
コードインスペクション	95	99	99.99			
品質保証	95	99	33.33			
正規のテスト						

情報システム予算の内訳

- ◆ 予算におけるハードウェア、ソフトウェア、パッケージソフト、通信、運用など サービス、省内担当職員人件費、その他は、平成17年度情報処理実態調 査から、企業においては以下の比率になる。
 - この数値をもとに、要求されている予算の妥当性を検証していく、但し、あくまでも企業における平均値であり、システムの特性に寄って費用比率は変わってくるのであくまで上記の数値は参考値である。

分類	比率	備考
ハードウェア	17.4%	買い取り、減価償却、レン タル、リース等
ソフトウェア	3 1 . 5 %	買い取り、減価償却、レン タル、リース、開発・カス タマイズ関連費用等
通信関連	3 . 8 %	
運用などサービス	25.2%	データ入力、運用・保守委 託料、教育、外部派遣要員 等
職員人件費	14.2%	
その他	7 . 5 %	

Challenge to the Smart Enterprises

工期と満足度の関係

◆ 標準的な工期に対して短工期、長工期の分布が25%になるようにして分析を行うと以下の結果がある。標準的な工期に対して短工期で行う場合にはリスクが高まることから、短工期開発にする理由を確認するとともに、短工期開発で行う場合のリスク回避対策(優秀なPMを配置する等)を提示させる必要がある。

工期	乖離度	顧客満足度(プロジェクト全体)								
		満足	やや不満	不満	未回答	総計(割合)			
長工期	件数	34	13	0	3	50	24.8%			
	割合	68.0%	26.0%	0.0%	6.0%	100.0%				
適正工期	件数	68	28	4	4		51.5%			
	割合	65.4%	26.9%	3.8%	3.8%	100.0%				
短工期	件数	29	15	2	2	48	23.8%			
	割合	60.4%	31.3%	4.2%	4.2%	100.0%				
総計	件数	131	56	6	9	202	100.0%			
	割合	64.9%	27.7%	3.0%	4.5%	100.0%				

工期短縮に対する対策

◆ 工期短縮に対しては適切な対応を行う必要がある。

尺度	25%工期延長	標準	25%工期短縮	25%以上工期短縮
式	3.4×(人月)1/3	2.7×(人月)1/3	2.0×(人月)1/3	1.4×(人月)1/3
工期設定	金融等欠陥の発生	提案モデル	・顧客の要望	外的対応/工期制約
の考え方	を無くしたい品質		流通業	対コンペ戦略、新商品の販
	重視			売、株式の上場、企業の統
				合など
工程管理	充分なシステムテ	中日程計画の充実	中日程計画の充実	小日程計画の充実
上の対応	スト期間の確保	(役割分担別	(週間別管理)	(日別管理)
策		WBS 管理)		
その他の対応策	・品質重視のテスト計画書、テストケースの緻密化・安定稼動のための分割立上等	 ・WBS による全体 計画と局面化開発の徹底 ・レビュトケーの初底 ・テ実ン・データのアントーのアントーのアントーのアントーのアントーのアントーのアントーのアントー	同 左 + (下 記) ・標準化の徹底と ・標準化のある一 ・標準のが ・ ・ ・シネのが ・ ・シスの部分 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	同 左 + (下 記) ・ベテランプロマネの投入 と会社あげての協力及 び監視 ・パート図での計画 ・ベストメンバーム選出 ・クリーンルー配置 ・開発促進ツールの採用 ・顧客主体のテストチーム 設置 ・パッケージの活用 ・部品の再利用 ・オープンな進捗情報管理

注 WBS: Work Breakdown Structure

RAD: Rapid Application Development

DOA: Data Oriented Approach

図表 5-1-15 工期評価尺度と対策

仕様の明確度と満足度の関係

◆ 情報システムの調達において、仕様が曖昧なことがよく指摘されるが、仕様は明確に定義することが重要である。下表のように、仕様が曖昧であると工期遅延を発生することが多くなり、満足度も低くなることが多い。このような傾向を念頭に置き、仕様作成時には仕様の明確さを、プロジェクトメンバ、リーダ、プログラムマネジメントオフィスの各段階で十分に確認する必要がある。

仕様明確	中								遅延度 20%以上
江塚明畑	泛	予定より早い							20%以上の割合
-11-244 (件数		15	2	1	2		20	10.0%
非常に 明確	割合		75.0%	10.0%	5.0%	10.0%		100.0%	
777	平均工期遅延率		0.0%	6.7%	11.1%	42.9%		5.1%	
454513	件数	7	75	8	7	6	1	104	6.7%
かなり 明確	割合	6.7%	72.1%	7.7%	6.7%	5.8%	1.0%	100.0%	
177	平均工期遅延率	-29.68%	0.00%	6.18%	13.96%	26.13%	66.67%	1.57%	
11-11-	件数	7	38	8	5	10	4	72	19.4%
やや 曖昧	割合	9.7%	52.8%	11.1%	6.9%	13.9%	5.6%	100.0%	
PS P/I	平均工期遅延率	-31.3%	0.00%	6.65%	14.22%	27.27%	54.17%	5.48%	
-11-244 (件数		3			3	1	7	57.1%
非常に 曖昧	割合	0	42.9%	0.0%	0.0%	42.9%	14.3%	100.0%	
-X-7/	平均工期遅延率		0.00%			41.61%	50%	24.98%	
	件数	14	131	18	13	21	6	203	13.3%
合計	割合	6.9%	64.5%	8.9%	6.4%	10.3%	3.0%	100.0%	
	平均工期遅延率	-30.47%	0.00%	6.47%	13.84%	29.63%	55.56%	4.07%	

4样	 明確度			1 座 / ポロン*	5 L A (t)					
1上1水上	归唯这		顧客満足度(プロジェクト全体)							
		満足	やや不満	不満	未回答	総計				
非常に明確	件数	18	1		1	20				
	割合	90.0%	5.0%	0.0%	5.0%	100.0%				
かなり明確	件数	85	27	2	6	120				
	割合	70.8%	22.5%	1.7%	5.0%	100.0%				
やや曖昧	件数	40	30	5	2	77				
	割合	51.9%	39.0%	6.5%	2.6%	100.0%				
非常に曖昧	件数	3	3		1	7				
d.	割合	42.9%	42.9%	0.0%	14.3%	100.0%				
合計	件数	146	61	7	10	224				
	割合	65.2%	27.2%	3.1%	4.5%	100.0%				

仕様の明確度とプロジェクト遅延

◆ 更に仕様変更であるが、仕様変更が大きなものは遅延も生じやすく満足度にも問題が生じがちであるので、このような傾向を念頭に置き、仕様作成時に仕様内容を、プロジェクトメンバ、リーダ、プログラムマネジメントオフィスの各段階で十分に確認する必要がある。

仕樣変更発生度		遅延度							
11 恢复史	光土反	予定より早い	予定通り	10%未満	20%未満	50%未満	それ以上	総計	20%以上 の割合
	件数	1	6			2		9	22.20%
変更なし	割合	11.11%	66.7%	0.0%	0.0%	22.2%	0.0%	100.0%	
	平均工期遅延率	-71.4%	0.0%			32.2%		-0.8%	
軽微な	件数	9	102	9	8	12	3	143	10.50%
変更が	割合	6.29%	71.3%	6.3%	5.6%	8.4%	2.1%	100.0%	
発生	平均工期遅延率	-30.31%	0.00%	7.00%	12.93%	29.41%	55.56%	2.89%	
大きな変	件数	4	22	9	4	6	3	48	18.80%
更が発	割合	8.33%	45.8%	18.8%	8.3%	12.5%	6.3%	100.0%	
生	平均工期遅延率	-20.6%	0.00%	5.94%	16.35%	26.11%	55.56%	7.50%	
重大な	件数					2		2	100.00%
変更が	割合	0.00%	0.0%	0.0%	0.0%	100.0%	0.0%	100.0%	
発生	平均工期遅延率					36.03%		36.03%	
	件数	14	130	18	12	22	6	202	13.90%
合計	割合	8.2%	63.9%	7.4%	5.7%	11.5%	3.3%	100.0%	
	平均工期遅延率	-30.47%	0.00%	6.47%	14.07%	29.37%	55.56%	4.15%	

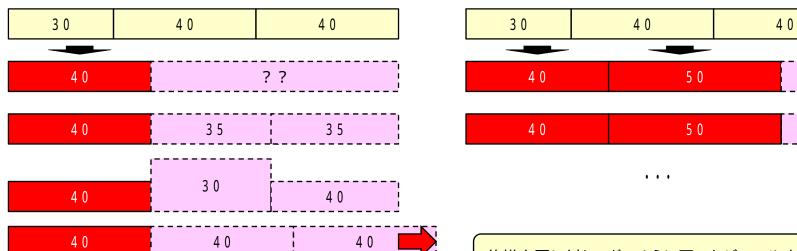
仕様変更発生度		П	ユーザ満足度(プロジェクト全体)								
山脉友丈	. 无土反	満足	やや不満	不満	未回答	総計					
変更なし	件数	8	3			11					
	割合	72.7%	27.3%	0.0%	0.0%	100.0%					
軽微な 変更が	件数	109	38	2	8	157					
を 発生 大きな変	割合	69.4%	24.2%	1.3%	5.1%	100.0%					
大きな変更が発	件数	28	17	5	3	53					
牛	割合	52.8%	32.1%	9.4%	5.7%	100.0%					
重大な変更が	件数	1	1			2					
発生	割合	50.0%	50.0%	0.0%	0.0%	100.0%					
合計	件数	146	59	7	11	223					
口前	割合	65.5%	26.5%	3.1%	4.9%	16040%					

Challenge to the Smart Enterprises

仕様変更と欠陥率

◆ 当然のことながら仕様変更が発生したものは変更しないものに対して作業にゆがみが生じることから欠陥率も大きくなる傾向がある。

仕樣変更発生度	件数	平均換算欠陥率	最大欠陥率
変更なし	8	0.36	0.73
軽微な変更が発生	140	0.57	11.89
大きな変更が発生	56	0.54	4.38
重大な変更が発生	1	0.03	0.03
合計	205	0.81	11.89

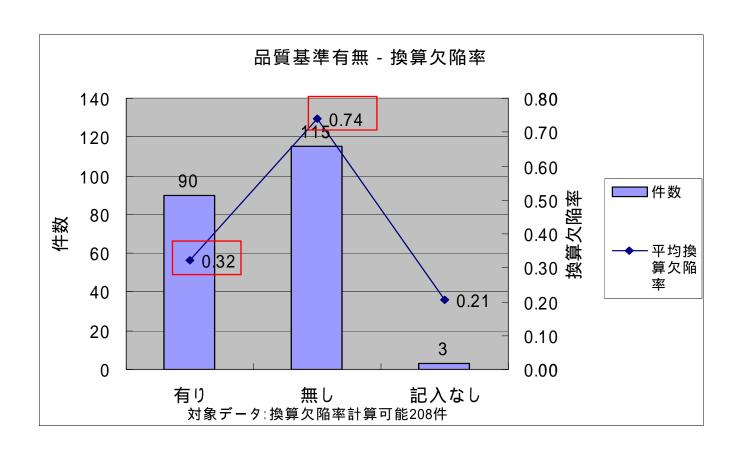


「ソフトウェアメトリックス2008」JUAS

仕様変更に対してどのように再スケジュールするのか

品質基準の有無と満足度

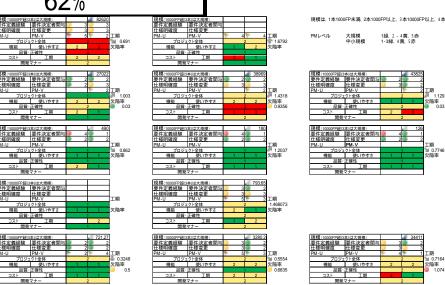
◆ 品質基準があるものは、やはり品質がよい。



参考:満足度を意識する

- ◆ 品質と正確性はまだ満足度向上の余地があり、それが、プロジェクト全体の満足度向上にも貢献できるものと考えられる。
- ◆ 意識して取り組んでいく必要がある

プロジェ	クト全体	63%		
機能	使いやすさ	75%	69%	
品質:	正確性	57%		
コスト	工期	51%	64%	
開発	マナー	62%		



ベンダPMの重要性

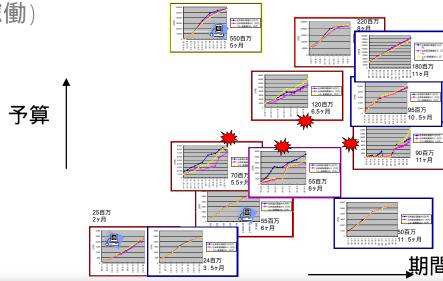
◆ また、PMスキルが高いほど欠陥率が低いとの傾向がある。特に未経験者がPMの場合には、途中の確認を行うなど注意が必要である。

			PMスキル(ベンダ)							
		1	2	3	4	5	記入なし	計		
換算欠陥率	件数	54	35	54	30	5	30	208		
	平均	0.27	0.49	0.7	0.42	1.54	0.82	0.55		
	最大	1.69	2.95	9.06	1.83	4.38	11.89	11.89		
	最小	0.00	0.00	0.00	0.00	0.02	0.00	0.00		

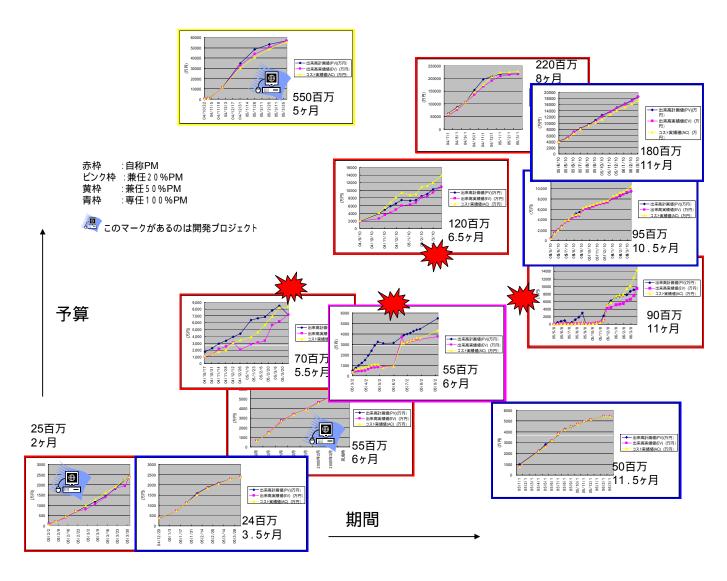
PMスキル
1.多数の中・大規模プロジェクトの管理を経験
2.少数の中・大規模プロジェクトの管理を経験
3.多数の小・中規模プロジェクトの管理を経験
4.少数の小・中規模プロジェクトの管理を経験
5.プロジェクト管理の経験なし

PMの資格をどう考えたらよいか

◆ 情報処理技術者やPMP(Project Management Professional)などのプロジェクトマネジメント専門技術者の有無とプロジェクト管理手法であるEVMの結果を比較することにより、認定された技術者を導入した場合と導入しない場合の品質の差異などを分析したものがある。下図は、右に行〈ほど実施期間が長〈、上に行〈ほど開発金額が大き〈なるようにEVMのデータをプロットしたものである。(正常なプロジェクトは右肩上がりにグラフが上がっていき、計画と実績があまりずれない)このグラフには業務分析プロジェクトと開発プロジェクトが含まれるが、開発プロジェクトはグラフ中にコンピュータマークを付けているが失敗が少ない傾向がある。それに対し赤で囲まれたプロジェクトは、プロジェクトマネージャの資格は持っていないが自称プロジェクトマネージャが実施しているプロジェクトであるが、多〈のプロジェクトが失敗に終わっている。逆に資格者が配置されている青いプロジェクトでは失敗プロジェクトは存在していない。(黄色は資格を持ったPMが50%以上稼働、ピンク色は資格を持ったPMが20%以上稼働)



参考:拡大



そのほかの技術者も必要

◆ 政府調達では以下のように定義している。

情報システムに係 る工程等	資 格	ITスキル標準 ³⁶ における職種
1. 情報システム	・システムアナリスト	・コンサルタント
化計画の策定	・技術士 (情報工学部門)	・IT アーキテクト
2. 要件定義等	・システムアナリスト	・コンサルタント
	・アプリケーションエンジニア	・IT アーキテクト
	技術士(情報工学部門)	
3. 設計・開発	・アプリケーションエンジニア	・ITスペシャリスト
4. 結合・総合テ	・ソフトウェア開発技術者	・アプリケーションスペシャリスト
スト等	・テクニカルエンジニア(ネットワ	・カスタマサービス
	一ク、データベース又は情報セキ	
	ュリティ)	
	・基本情報技術者	
	・システム監査技術者	
	技術士(情報工学部門)	
5. 受入テスト	・アプリケーションエンジニア	・ITスペシャリスト
6. 移行	・ソフトウェア開発技術者	・アプリケーションスペシャリスト
	・テクニカルエンジニア(ネットワ	・カスタマサービス
	一ク、データベース又は情報セキ	
	ュリティ)	
	・基本情報技術者	

欠陥とは何か

- ◆ バグ管理のツールであるBugzillaの定義では以下の通りである。
 - ➢ Blocker
 - 開発やテストができ名くるくらい重大なもの
 - > Critical
 - クラッシュやデータ損出につながるもの
 - > Major
 - ・ 機能が動かないもの
 - > Minor
 - 機能は動くが、手続きが必要など完全ではないもの
 - > Trivial
 - 機能に影響を与えない記述ミスなど
 - > Enhancement
 - 機能強化要望

欠陥はどこまで許されるのか

- ◆ システムの品質において、欠陥の含まれる割合は重要であるが、一般的に以下のように分布しており、通常のシステムとしてはBランク以上の品質が望まれ、少なくともCランクは満たしていることが望まれる
- ◆ ここで欠陥率とは、「ユーザが発見した欠陥数(顧客側総合テスト以降、フォローまで出発見された欠陥)」÷ プロジェクト全体工数である。 つまり欠陥率 0.25とは4人月あたり1個のバグということである。

	Aランク	Bランク	Cランク	Dランク	Eランク	Fランク
欠陥率	0	0.25未満	0.5未満	1未満	3未満	3以上
割合	9.7%	33.1%	18.8%	17.5%	14.9%	5.8%
件数	15	51	29	27	23	9

欠陥の影響はどのくらいか

◆ 欠陥はMTTFとも関連があり、それを基に要求品質を設定していく必要がある。

KLOCあたりの欠陥レベル	平均故障間隔(MTTF)	品質レベル(参考)
30以上	2分以下	
20 ~ 30	4~15分	
10 ~ 20	5~60分	
5 ~ 1 0	1~4時間	
2 ~ 5	4~24時間	E~Fクラス相当
1 ~ 2	24~160時間	Eクラス相当
1以下	ほとんど故障しない	A~Dクラス相当

プロトタイプレベル

商用ソフトレベル 10-2000件/1000時間 高信頼性ソフトレベル 0.1-10件/1000時間

ソフトウェア開発の定量化手法第二版、共立出版

電球が切れる確率1000時間に一回 バイクに乗って怪我をする確率1000時間に0.143回

「ソフトウェアテスト手法」高橋、湯本

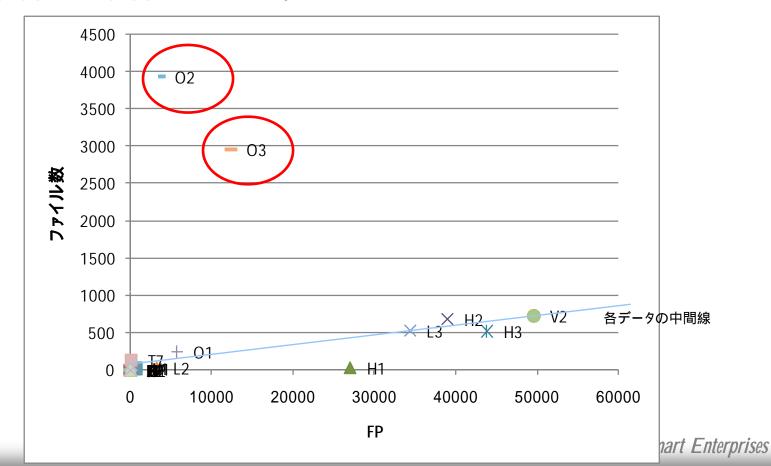
欠陥率と満足度の関係

◆ 欠陥率のみでユーザの満足度が決まるわけではないが、やは り、Cランク以上のシステムが満足という顧客評価を得られる割 合が高くなっている。

欠陥率		顧客満足度(品質)					
		満足	やや不満	不満	未回答	計	満足率
0	件数	10	4	1		15	66.7%
	平均	0.00	0	0		0	
0.25未満	件数	36	13	1		50	72.0%
	平均	0.10	0.13	0.05	0.15	0.11	
0.5未満	件数	21	6	1		28	75.0%
	平均	0.36	0.36	0.48	0.33	0.36	
1未満	件数	14	11	1		26	53.8%
	平均	0.68	0.68	0.54	0.65	0.68	
3未満	件数	13	7	2		22	59.1%
	平均	1.79	1.80	1.53	2.08	1.79	
3以上	件数	8	1			9	88.9%
	平均	5.63	4.35			5.49	
計	件数	102	42	6		150	68.0%
	平均	0.87	0.67	0.69	0.8	0.81	

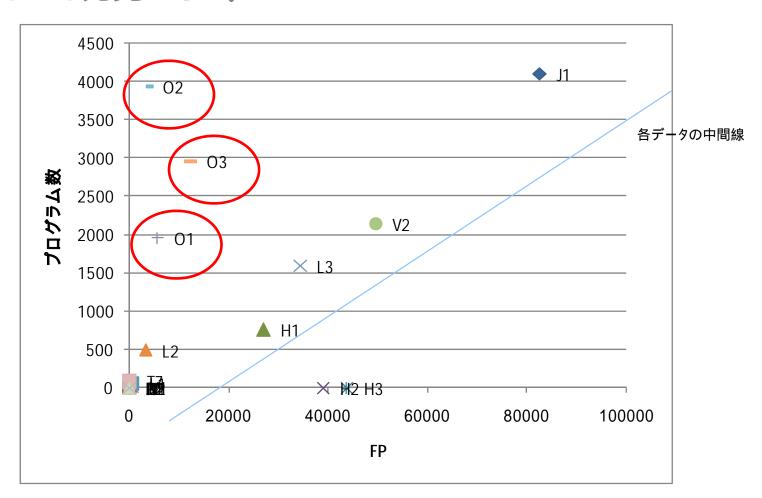
システムの構造は大丈夫か?

- ◆ 設計が終わると見える規模あたりのファイル数
- ◆ ファイル数が異常に多いシステムが発見できる。
- ◆ このようなPJは、作りに問題があるのではないか。
 - ▶ 保守性への影響も想定される。



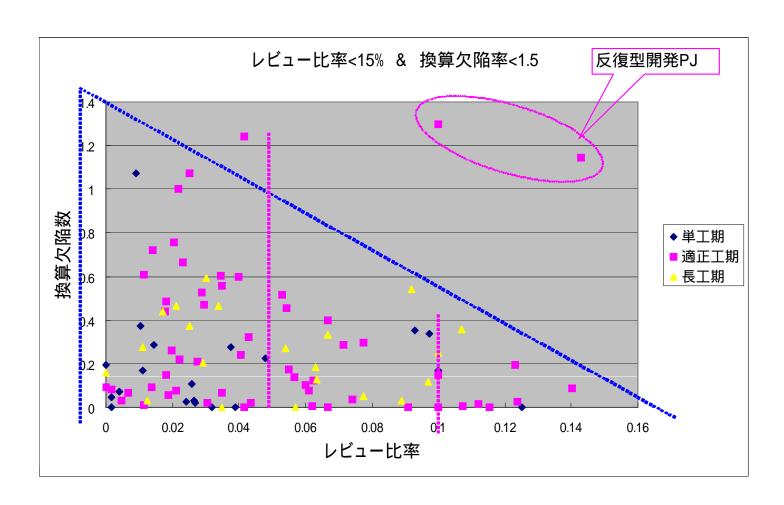
システムの構造は大丈夫か?

◆ ファイル同様に、プログラムの分割が細かいレベルで行われているものも発見できる。



レビュー

◆ 当然のことながら、レビューをすれば欠陥は少なくなる。



正しいレビューの実施

- ◆ レビューは役割分担やチェックリストなどを用意した上で計画的に実施することが重要である。ただし、現場に過剰な負荷をかけてはいけない。
 - > アドホックレビュー
 - 作業途中で必要に応じて実施するレビュー
 - > パスアラウンドレビュー
 - メール配布などによるレビュー依頼
 - > ペアレビュー
 - 作成者とレビューアが成果を確認
 - > ウォークスルー
 - 業務の流れに沿って作成者が説明を行うレビュー
 - > チームレビュー
 - 計画された成果物レビューなど
 - > インスペクション
 - モデレータ、記録者など役割を指定して行う査察的、厳格なレビュー

重点レビュー項目

- ◆ ISO9126にも規定されるソフトウェア品質特性に基づきレビュー を行っていく
 - > 機能性
 - 合目的性、正確性、接続性、整合性、セキュリティ
 - > 信頼性
 - 成熟性、障害許容性、回復性
 - > 使用性
 - 理解性、習得性、操作性
 - > 効率性
 - 実行効率性、資源効率性
 - > 保守性
 - 解析性、変更作業性、安定性、試験性
 - > 移植性
 - 環境適応性、移植作業性、規格準拠性、置換性

基本設計のレビュー密度

- ◆ ソフトウェア開発データ白書によると以下の通りである。
 - > 1000FPあたり
 - 平均77.1件
 - **≻** KLOCあたり
 - 平均3.9件
 - > ページあたり
 - 平均0.393件

レビューにおけるカバレッジ

◆ CMMレベル5を持つInfosysでは以下の基準でレビューを行っている。

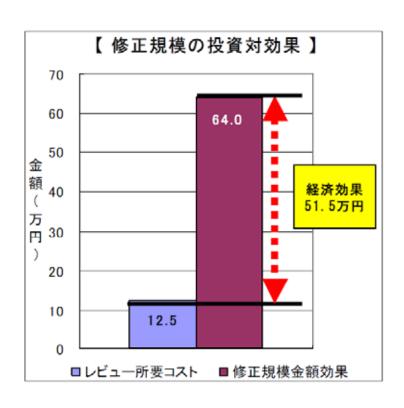
Infosysのレビュー	·能力ベースライン
	8671 トークフィン

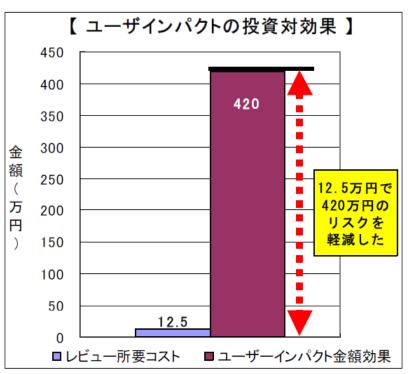
IIIIOSYSOFF CA BETT	<u> </u>			
レビュー項目	準備のカバレッジ率	グループレビューの カバレッジ率	表面的/軽微な欠陥 の欠陥密度	致命的/重大な欠陥 密度
要件		5-7page/時	0.5-1.5欠陥/page	0.1-0.3欠陥/page
ハイレベル設計		4-5page/時(または 200-250仕様文/時)	0.5-1.5欠陥/page	0.1-0.3欠陥/page
詳細設計		3-4page/時(または 70-100仕様文/時)	0.5-1.5欠陥/page	0.2-0.6欠陥/page
コード	160-200LOC/時	4-6page/時	0.01-0.06欠陥 / LOC	0.01-0.06欠陥/page
統合テスト計画		5-7page/時	0.5-1.5欠陥/page	0.1-0.3欠陥/page
統合テストケース		3-4page/時		
システムテスト計画		5-7page/時	0.5-1.5欠陥/page	0.1-0.3欠陥/page
システムテストケース		3-4page/時		
プロジェクト管理計画および構成管理計画	4-6page/時	2-4page/時	0.6-1.8欠陥/page	0.1-0.3欠陥/page

ソフトウェア開発のためのプロジェクトマネジメント入門、ソフトバンクパブリッシング

レビューの効果

◆ レビューを行いバグを防ぐことで、未然に無駄な支出を防止することが可能である。





日本科学技術連盟第23年度(2007年度) 分科会成果報告 第1分科会「ソフトウェアプロセス評価・改善」 グループA (論文)レビューの質と価値の定量化の提案

レビューの質を高める取り組み

◆ レビューが正しく行われていたかは、以下のようにチェックリストで管理できる

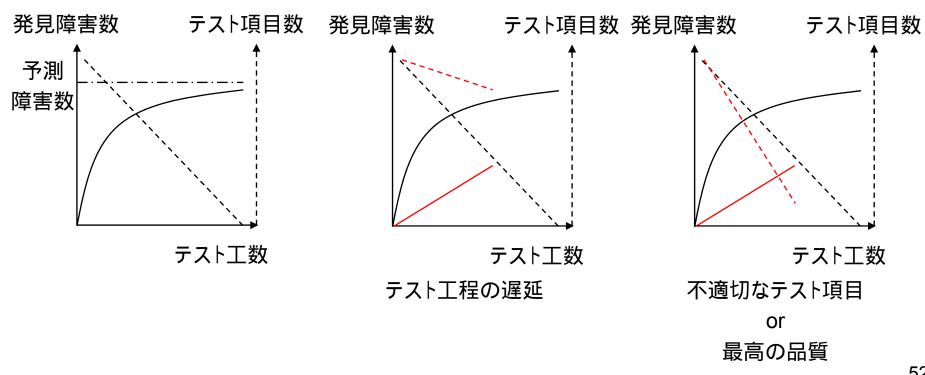
表 2. レビューの質チェック票

1	レビューの目的/狙いが明確だったか	良い	まあ良い	やや改善の 余地有り	改善の 余地有り	
2	レビュー物件の対象範囲は適切に示されていたか (前回との差分などが明確だったか)	良い	まあ良い	やや改善の 余地有り	改善の 余地有り	
3	必要な資料は全て事前配布/提示されていたか	80%以上	80~50%	50~10%	10%以下	
4	資料はいつ頃事前配布されていたか (資料に目を通す期間は確保されていたか)	十分余裕が 有った	期間が有った	期間が十分 では無かった	事前配布無し または直前	
5	レビュー会議前に資料に目を通したか	80%以上	80~50%	50~10%	10%以下	
6	レビュー物件の内容は十分伝わったか	80%以上	80~50%	50~10%	10%以下	
7	全員が満遍なく発言していたか	全員発言 していた	半分以上は 発言していた	半分 しか い	012完了度	Q1·目的 100 Q2·範囲提示 下限
8	レビューリーダのファシリテートは適切だったか	良い	まあ良い	や. <u> </u>		03.事前配布
9	的外れな指摘/コメントが少なかったか	全く無し	殆ど無し	少		25
10	脱線することが少なかったか	全く無し	殆ど無し	少 010 1648		04 配布時期
11	参加者で問題領域をカバーできていたか (レビュー参加者の人選は適切だったか)	100%	80%以上	80	I	U- III-TI PENE
12	予定のレビュー対象範囲が完了したか	100%	80%以上	80 09.8935	n	Q5-事前準備
	うせば海明等22年度/2007年度) 公利今代用起失 第14				Q8.同会進行	Q6.内容理解 Q7.活性化

日本科学技術連盟第23年度(2007年度) 分科会成果報告 第1分科会「ソフトウェアプロセス評価・改善」 グループA (論文)レビューの質と価値の定量化の提案 51 *Challenge to the Smart Enterprises*

テストには科学的データがあるが活用されていないことが多い。

- ◆ テストではバグがあることは証明できるが、バグが無いことを証明することはできない。
 - ▶ ただし、コストとバランスの取れたレベルを実現することはできる
- ◆ FPあたりのテスト項目数



テスト項目数と項目密度

- ◆ 規模あたりのテスト項目数と項目比率は以下のとおりである。
- ◆ 特に、項目は多ければよいというものではなく、比率よく配分しなければならない。

	検査項目総数
制御系	30-50件/KLOC
業務系	20-25件/KLOC

	項目比率
基本/正常	50-60%
異常/障害	10-20%
限界/境界	5-10%
周囲条件/インタフェース	20%

第48回SEA-SPIN Meeting ソフトウェアテストと品質

工程	ケース数
単体テスト	7.5/FP
	(5-15/FP)
結合テスト	2.5/FP
	(0.5-8/FP)
総合テスト(1)	1.2/FP
	(0.6-10/FP)
総合テスト(2)	-

2007JUAS QCDワーキング 参考10/KLOC=1/FP

FPあたりのケース密度

◆ まだ、データ数が少なく、今後のデータの充実が望まれる。

		~10人月	~50人月	~ 100人月	~500人月	500人月超	記入なし	総計
件数		2	5	5	6	3	3	24
ベンダ内	平均(CASE/FP)	0.7	2.8	3.0	12.7	1.8	0.8	4.8
	最大(CASE/FP)	1.2	5.9	9.9	31.4	3.2	1.4	31.4
テスト	最小(CASE/FP)	0.3	0.1	0.1	2.8	0.5	0.1	0.1
顧客側テ	平均(CASE/FP)	0.7	0.1	0.6	2.2	0.2	0.2	0.8
I — :	最大(CASE/FP)	1.3	0.3	1.3	6.9	0.4	0.4	6.9
\ \\	最小(CASE/FP)	0.0	0.0	0.0	0.0	0.1	0.0	0.0

言語別、開発種別ごとのケース密度

◆ 結合テスト、総合テストなどのケース密度が、言語別、開発種別々に提供されている

ソフトウェア開発データ白書2008 P240

主要開発言語別SLOCあたりの総合テストケース数の基本統計量(改良開発)

(ケース数/Kstep)	N	最小	中央	最大	平均
全体	124	0.019	10.188	796.881	45.464
COBOL	43	0.019	6.392	82.875	13.589
C言語	32	1.250	17.114	796.881	84.459
VB	19	0.723	18.784	215.700	47.879
Java	30	0.115	7.896	604.000	48.027

上記総合テストには、ユーザ受け入れ試験を含む

主要開発言語別SLOCあたりの総合テスト欠陥数の基本統計量(改良開発)

ケース数/Kstep	N	最小	中央	最大	平均			
全体	122	0.000	0.219	13.333	1.068			
COBOL	46	0.000	0.097	12.222	0.905			
C言語	30	0.000	0.338	13.333	1.339			
VB	18	0.036	0.576	4.917	1.160			
Java	28	0.000	0.123	10.000	0.988			

テスト計画書のメトリックスチェックの例

結合テスト計画書の確認項目

開発区別	新規	改良
言語		Java
規模(Kstep)		1200

目標設定値	下限	上限	実績	IPA参考
テストケース密度(ケース数/Kstep)			3.36	38.965
テストケース数			4032	
不具合検出率(不具合数 / Kstep)			0.051	1.401
不具合数			61.2	

テストケース項目比率

	比率	参考
基本/正常		50-60%
異常/障害		10-20%
限界/境界		5-10%
周囲条件/インタフェース		20%

第48回SEA-SPINソフトウェアテストと品質

移植であるためテストケース密度は低い。この時点で品 質は非常によいが、ケースが少ないため不具合の検証に 漏れがある可能性がある。今後もモニターしていく必要が



<u>ソフトウェア開発データ白書2008 P240</u>

王要開発言語別SLOCあたりの結合	<u> アストケー.</u>	人奴の基本	統計量(改	(艮開発)	
(ケース数/Kstep)	N	最小	中央	最大	平均
全体	104	0.321	24.889	1964.000	84.837
COBOL	32	0.321	15.285	82.438	22.695
C言語 VB	25	3.632	43.894	674.000	111.403
VB	15	1.445	32.061	631.064	115.358
Java	32	3.774	38.956	1964.000	111.955

主要開発言語別SLOCあたりの結合テスト欠陥数の基本統計量(改良開発)

ケース数/Kstep	N	最小	中央	最大	平均			
全体	102	0.000	1.126	42.357	2.770			
COBOL	34	0.000	0.457	5.226	1.181			
C言語	25	0.067	1.333	42.358	5.230			
VB	15	0.181	0.896	10.946	2.599			
Java	28	0.000	1.401	24.000	2.596			

シフェルニフト計画書の疎初項日

ノスノムノス 可凹音の唯心項目		
開発区別	新規	改良
言語		Java
規模(Kstep)		1200

目標設定値	下限	上限	実績	IPA参考	JUAS参考
テストケース密度(ケース数/Kstep)	2			7.896	22.7374
テストケース数	2400				
不具合検出率(不具合数 / Kstep)	0.02	0.08		0.123	
不具合数	24	96			

移植であるためテストケース密度は低いが、品質目標は 適正レベルといえる。

500人以上 平均 言語コンパー
ジョン5/7.63

ソフトウェア閏発データ白書 2008 P240

7717171717171717171717171710									
主要開発言語別SLOCあたりの総合テストケース数の基本統計量(改良開発)									
(ケース数/Kstep)	N	最小	中央	最大	平均				
全体	124	0.019	10.188	796.881	45.464				
COBOL	43	0.019	6.392	82.875	13.589				
C言語	32	1.250	17.114	796.881	84.459				
VB	19	0.723	18.784	215.700	47.879				
Java	30	0.115	7.896	604.000	48.027				

上記総合テストには、ユーザ受け入れ試験を含む

主要開発言語別SLOCあたりの総合テスト欠陥数の基本統計量(改良開発)

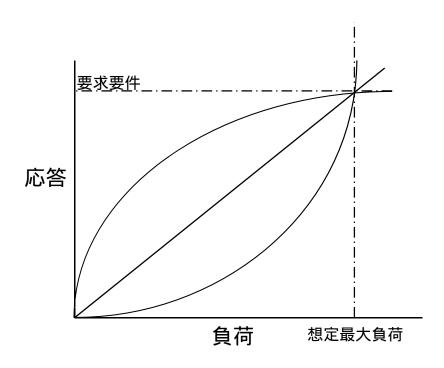
工女用光白品的00000亿分分泌日子人1个阳数00坐牛泌时里(以及闭光)								
ケース数/Kstep	N	最小	中央	最大	平均			
全体	122	0.000	0.219	13.333	1.068			
COBOL	46	0.000	0.097	12.222	0.905			
C言語	30	0.000	0.338	13.333	1.339			
VB	18	0.036	0.576	4.917	1.160			
Java	28	0.000	0.123	10.000	0.988			

<u>ソフトウェアメトリックス調査2008 P142</u>

		~ 10人月	~50人月	~100人月	~ 500人月	500人月超	記入なし	総計
件数	件数	2	37	15	26	5	4	89
ベンダ内テスト	平均	38.8	92.2	23.5	88	14.9	120.5	75.1
(ケース数/Kstep)	最大	41.1	963.4	125.1	916	30.5	456.1	963.4
(7 — Agg/Rstep)	最小	36.5	0	0.1	0	3.7	0.3	0
顧客側テスト	平均	5.2	37.9	26.9	13.6	1.4	2.6	24.5
顧客側リスト (ケース数/Kstep)	最大	10.4	588.5	347.4	80	4.1	5.2	588.5
(7 — Agx/Kstep)	最小	0.0	0.0	0.1	0.0	0.1	0.1	0.0

パフォーマンステスト

- ◆ システムにおける性能は非常に重要な要素である。
 - > 最大負荷時に要件を満たすのか
 - ▶ 想定負荷までの応答の状況はどうなっているのかなど検証していく必要がある
 - ▶ また、同じシステム上で並行稼動しているプロセスがある場合は、その 条件もテスト時に確認されているか検証する必要がある。

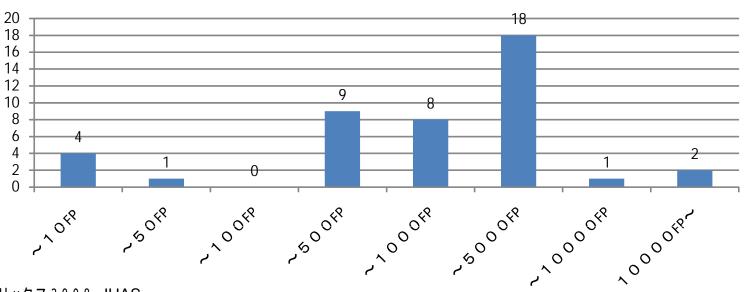


立ち上げの段階で適正な保守計画を行う

◆ データは少ないが数百から数千FPに一人の割合で要員を配置している。

平均 3652.4FP

一人あたりのFP保守守備範囲



「ソフトウェアメトリックス2008」JUAS

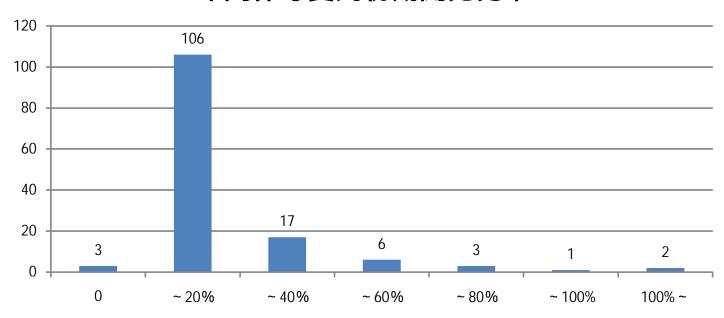
ライフサイクルコストとして適正か検証をしていく

初期費用に対する保守費用

◆ 年間保守費用は、初期開発費用の16.6%程度である。



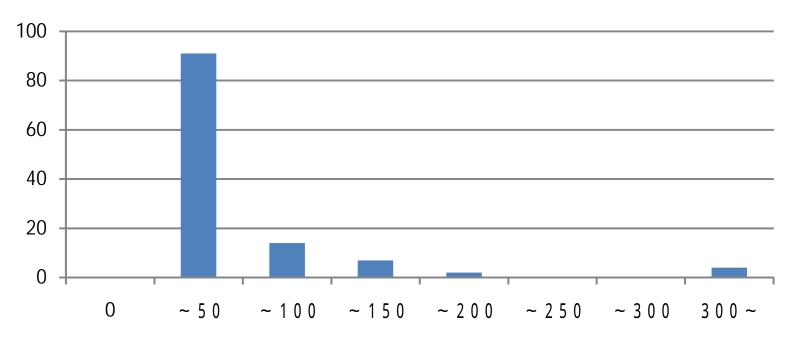
年間保守費用初期開発比率



画面あたりの保守費用

平均 102.1万円

画面あたりの年平均保守費用(万円)



カットオーバー時の品質の保守への影響

◆ 保守作業との関係はあるが、欠陥率のデータはまだ十分では ない。

平均保守作業期間

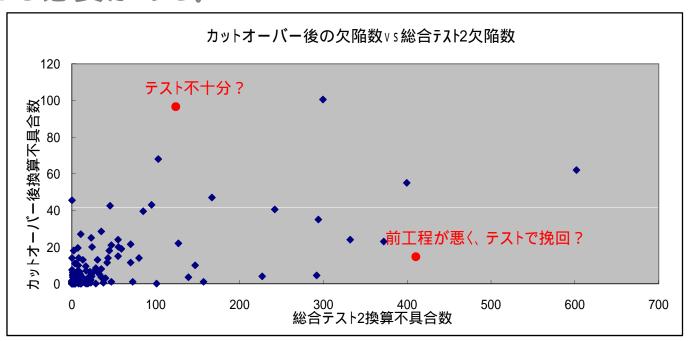
	半日以下	1日以内	3日以内	1週間以内	1月以内	1月以上
CO時の品質はよい	31.7%	19.4%	20.0%	12.1%	11.1%	5.7%
CO時の品質はよくない	29.9%	17.8%	14.3%	14.1%	14.3%	9.5%

CO時品質	初年度保守欠陥率	2年目以降保守欠陥率	受入確認即時合格率
非常によい	8.5%	6.3%	50.3%
よい	20.1%	11.7%	64.2%
普通	19.7%	13.4%	61.2%
やや悪い	22.1%	7.1%	81.2%
非常に悪い	9.0%	5.0%	95.0%

保守欠陥率 = 欠陥発生件数 / 保守作業実施件数

サービス開始後の品質は適正レベルか

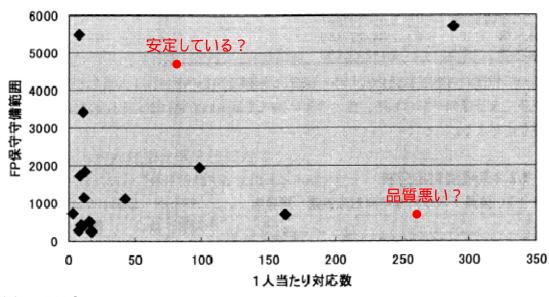
◆ またテスト中の欠陥数から稼働後の欠陥数を推定することができ、これと比較することにより品質の安定度を判断することが可能になる。テスト時の発生不具合数から、導入初期の不具合数を想定し、それを念頭に置いた運用を行い、異常な不具合の多さなどが見られるときは、テストデータの確認など必要な措置を講じる必要がある。



保守による品質の検証

- ◆ 規模あたりの欠陥数、フォロー時の欠陥の多さで品質の概要はつかめるが、長期にわたっても検証をすることが重要である。 保守要員がどのくらいの範囲を見ているのか、その中でどのくらいの対応をしているかという点からも対策が考えられる。
 - ➤ FP守備範囲が広〈、一人当たり対応数が多いものは、保守要員の人で不足による悪循環などが想定される。

1人当たり対応数VSFP守備範囲

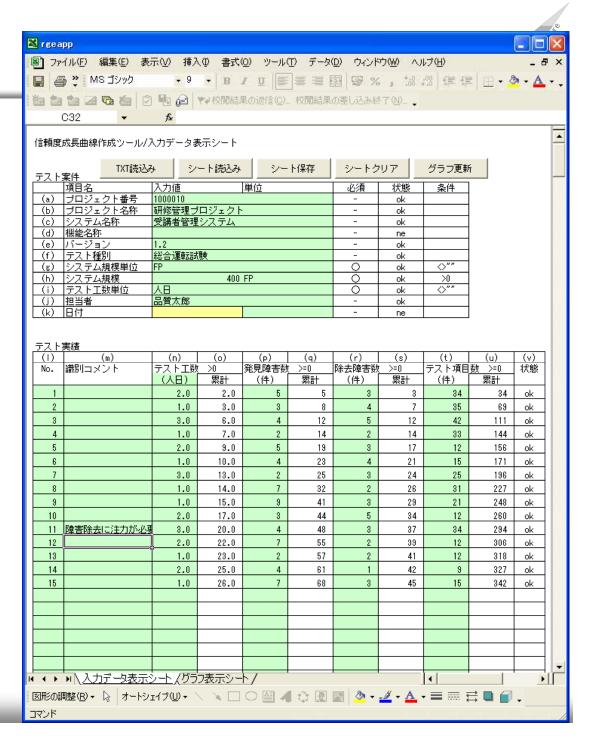


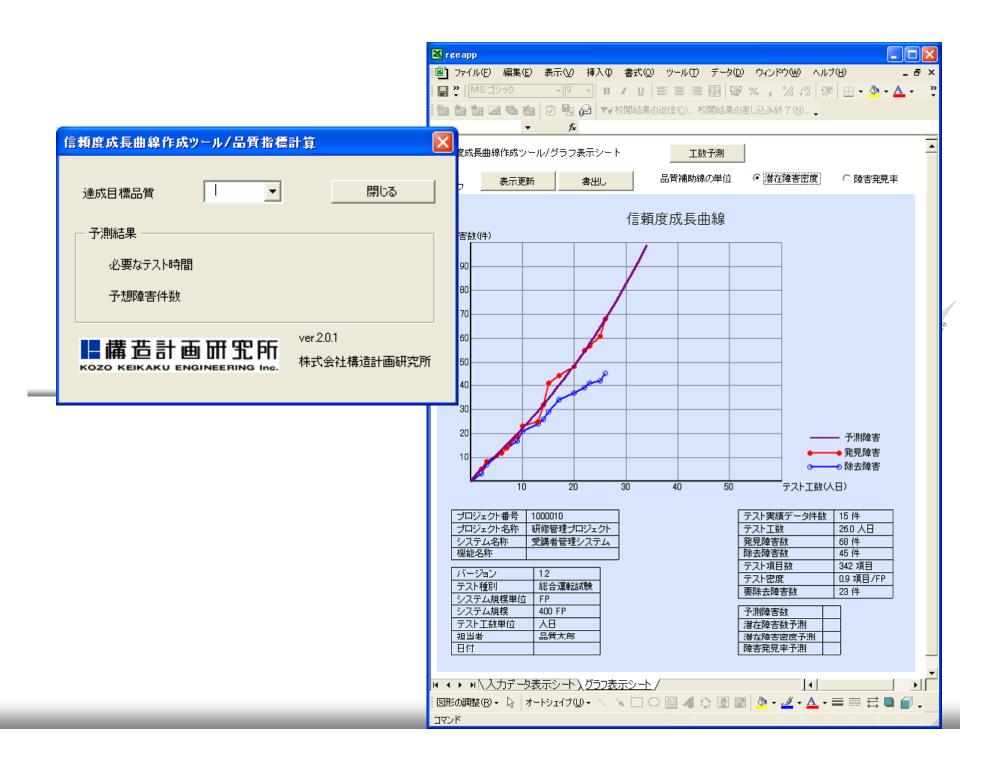
稼働率の目標

	レベル1	レベル2	レベル3	レベル4	レベル5
稼働率	98%以下	99%	99.9%	99.99%	99.999%以上
バックアップ機	なし	あり (部分的)	あり (2 / N + 1台)	あり (Hot stand by)	あり (Hot stand by)
サービス停止時間 ()時間/年	172時間	86時間	8.6時間	50分	5分
到着時間	1-6時間(昼) 12時間(夜間)	1-6時間	1-3時間(昼) 6時間(夜間)	常駐 ケースによって は2時間	常駐
修復時間 ・故障修復 ・再立ち上げ	6時間-12時間 10分-1時間	6時間-12時間 10分-1時間	3時間-6時間 10分-1時間	3時間-6時間 0分-10分	3時間-6時間即時
費用 ·構築費用 ·運用費用	1.0倍 1.0倍	1.2~1.8倍 1.1~1.3倍 (マニュアル)	1.2~3倍 1.3~2.0倍	1.5~4倍 2.0~3倍 (保守も)	4~6倍 3~4倍
システム構成(例) 必要な機能		NAS	SAN NAS クラスタリング ロードバランシング	SAN クラスタリング ロードバランシング 三重化	SAN クラスタリング ロードルランシング 三重化、四重化
ペナルティ			対象	対象	対象

JUAS·SRM第1巻

ツール例





IPAが提供する無料ツールEPM



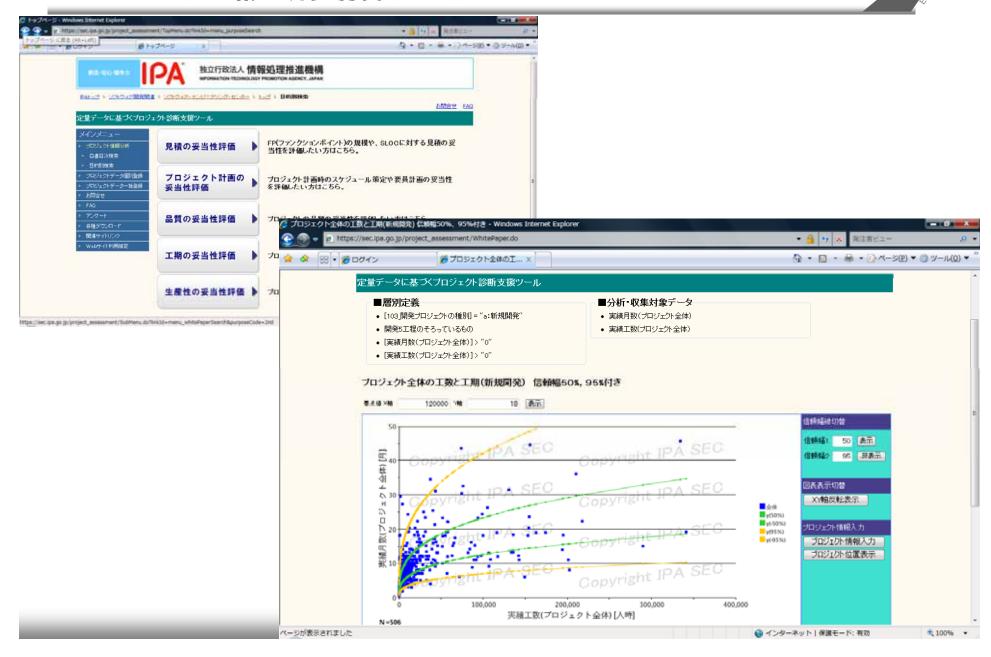
IPAが提供する無料ツールEPM



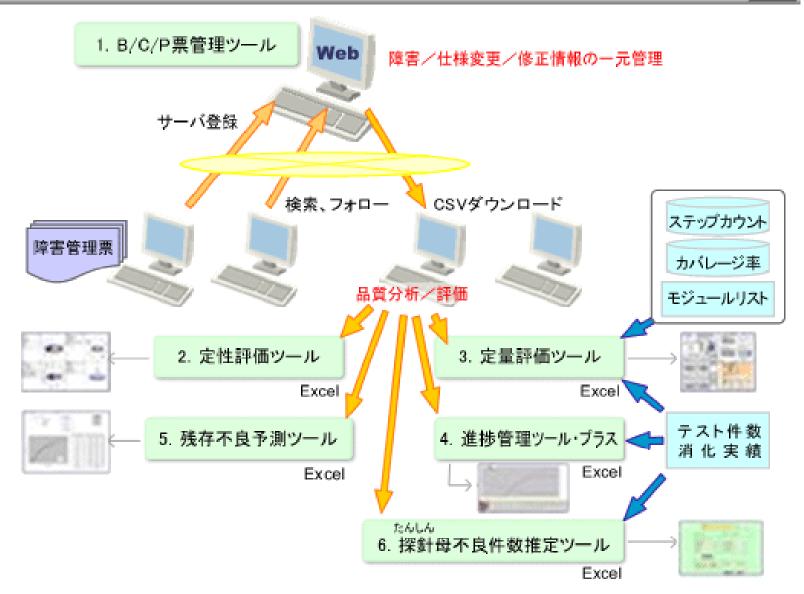
IPAが提供する無料ツールEPM



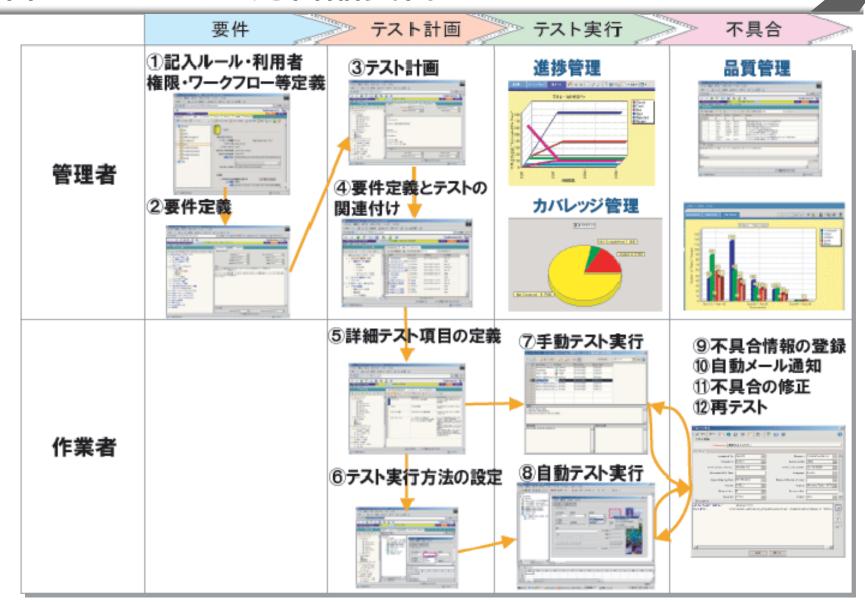
プロジェクト診断支援ツール



日立製作所QE一EXPERT



日立システムの総合品質管理



カットオーバー時の品質の保守への影響

◆ 保守作業との関係はあるが、欠陥率のデータはまだ十分では ない。

平均保守作業期間

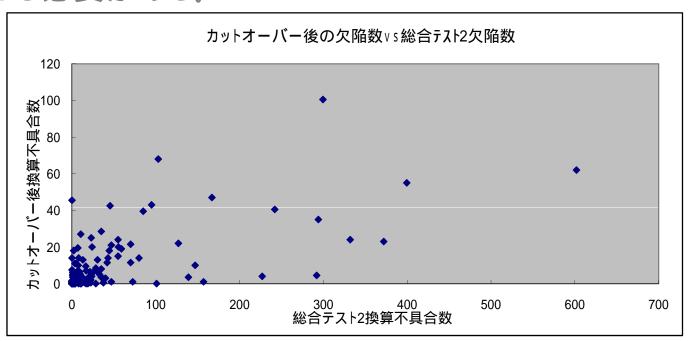
	半日以下	1日以内	3日以内	1週間以内	1月以内	1月以上
CO時の品質はよい	31.7%	19.4%	20.0%	12.1%	11.1%	5.7%
CO時の品質はよくない	29.9%	17.8%	14.3%	14.1%	14.3%	9.5%

CO時品質	初年度保守欠陥率	2年目以降保守欠陥率	受入確認即時合格率
非常によい	8.5%	6.3%	50.3%
よい	20.1%	11.7%	64.2%
普通	19.7%	13.4%	61.2%
やや悪い	22.1%	7.1%	81.2%
非常に悪い	9.0%	5.0%	95.0%

保守欠陥率 = 欠陥発生件数 / 保守作業実施件数

サービス開始後の品質は適正レベルか

◆ またテスト中の欠陥数から稼働後の欠陥数を推定することができ、これと比較することにより品質の安定度を判断することが可能になる。テスト時の発生不具合数から、導入初期の不具合数を想定し、それを念頭に置いた運用を行い、異常な不具合の多さなどが見られるときは、テストデータの確認など必要な措置を講じる必要がある。



信頼性向上

licus de la companya de la companya

信頼性向上のためのシステム設計・開発段階での施策

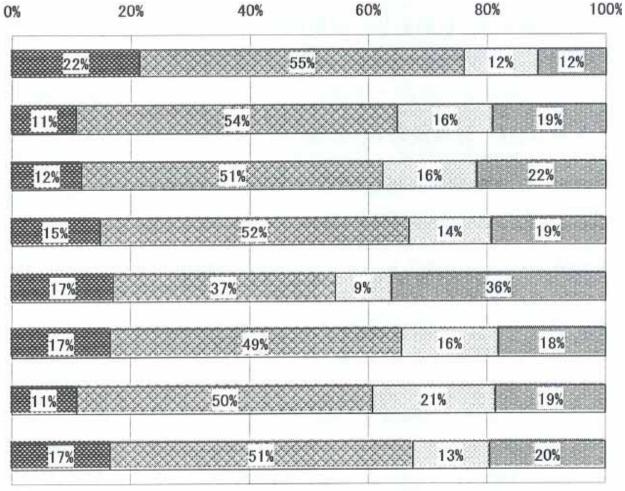
- ①全体(ハード、ソフト、ネットワーク、電源)の 信頼度を考慮したシステム構成(n=772)
 - ②オペレーションミスを起こさせない設計 (ユーザビリティ含む)の考慮(n=771)
 - ③システム信頼性を考慮した ソフトウェアの構成(n=771)
 - ④運用を考慮した設計(設計段階からの 運用担当者の参画)(n=771)

⑤開発の標準化(n=772)

⑥レビューの十分な実施(n=771)

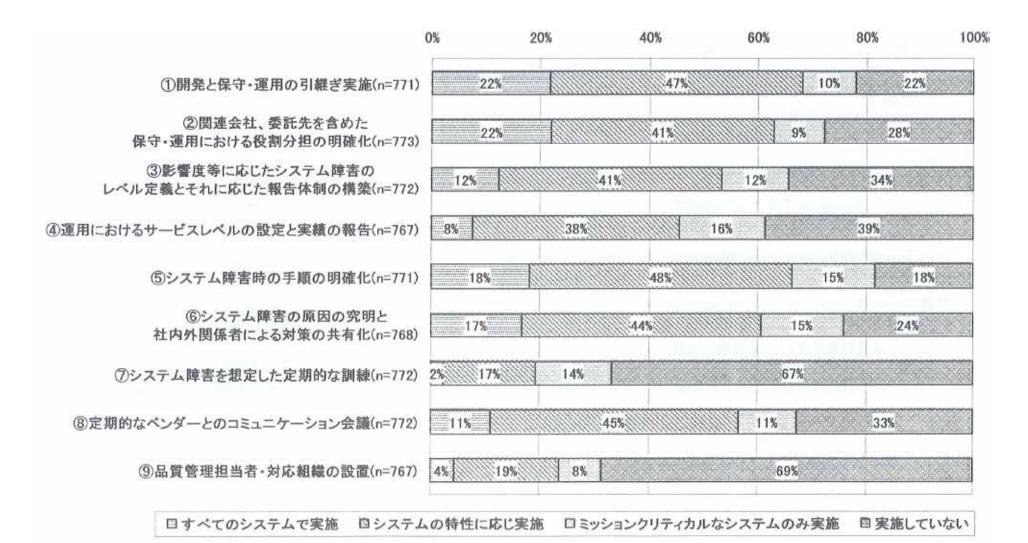
⑦十分なテスト期間の確保(n=772)

⑧エンドユーザーの検収への参加(n=770)



曽すべてのシステムで実施 閏システムの特性に応じ実施 □ミッションクリティカルなシステムのみ実施 閏 実施していない

信頼性向上のためのシステム保守・運用段階での施策

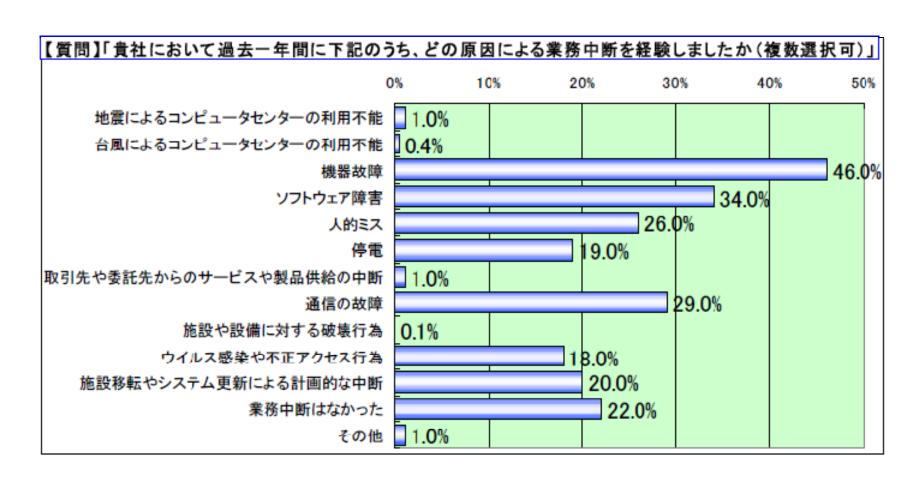


信頼性にかかわる事象

<.結果事象の分類定義> (東京証券取引所「危機管理への取り組み」より)

①局所被害	テロ(予告、破壊行為)等により当取引所は被害をうけているものの、外部関係機関 には特段の影響がない場合
②広域災害	大規模地震、風水害等により、当取引所及び外部機関がともに被害を受けている 場合
③システム障害	システムのハード障害、アプリケーション障害、通信回線障害等により、当取引所の 情報システムが利用不能となった場合

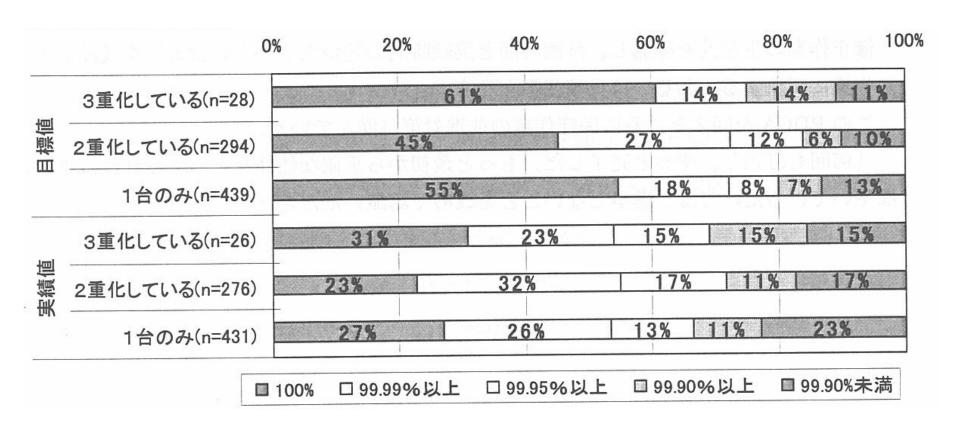
信頼性にかかわる経験



事業継続計画策定ガイドライン

ハード的にどこまで信頼性を確保できるのか

◆ 実は目的ほどに効果を発揮していない。



管理プロセス

【図表 1 BCM 構築の一般的な流れ】 ビジネスインパクト分析 事業継続に当たってのボトルネック(事業継続上、重要な 維持·管理 箇所・事象)を特定。事業継続上、ボトルネックを守るた めの対策検討・実施。 BCPの策定 効果検証· 継続的改善 ■会社としてのBCP方針の策定 ■組織体制の構築 ■目標復旧時間を設定しその事業体に応じたBCP作成 BCMの運営 BCPはあくまで計画であり、それをいかに企業内に浸透、 戦略的に活用するかという「マネジメントの視点」(= BCM) が重要。

事業継続計画策定ガイドライン

大学における感染症対策・事業継続計画BCP(Business Continuity Plan)例

脅威:感染症(特に心配されるのが鳥インフルエンザのヒトーヒト感染)

米国の想定では18ヶ月の流行期間(日本の想定は8週間)

罹患率25% 死亡率0.5-2%と予想(SARSやエボラ出血熱のような突然の感染症も予想される)

想定される状況

必要な対応

第一フェーズ(立ち上がり) 国内感染報告のニュース 外出自粛の世論 学生・職員への不安の蔓延

対応の周知

第二フェーズ(蔓延) 国内感染報告の増加 政府から社会活動制限依頼 学内に患者が発生 登校拒否学生の増加 職員も欠席 授業の中止 事務局の縮小 試験実施は困難 (学生、職員とも登校困難) ネット活動のみ実施

第三フェーズ(最流行) 企業活動が縮小 公共交通機関の運用も縮小 医療機関がパンク インターネットが大混雑 学生の10%が罹患、死者も発生 事務職員も同様 事実上、機能停止 全〈の機能停止 ネット活動のみ実施

時期や期間によっては、大学の運営、経営に深刻な 影響

第四フェーズ(終息) 患者数が減少し 社会活動の制限解除 解除通知を受けて徐々に回復

解除通知 後事務処理 ネット活動から実施 (e-Learning授業、テレビ会議) 新入生の減少 卒業生の滞留 等



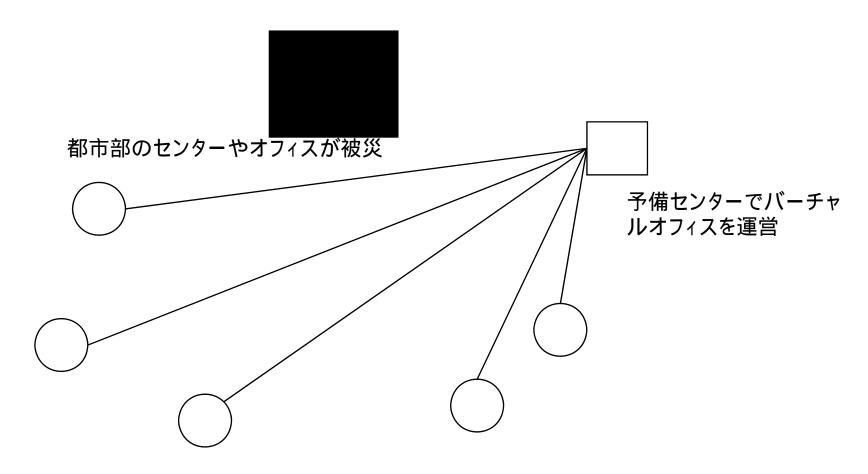
日頃から準備が必要 緊急用の容量も必要 回線確保ができない場合の想定も必要



ブロードキャストによる説明会 テレビ会議、テレワークによる運営 E-Learninngによる授業継続

BCP対策としてのテレワーク

◆ 米国では、ニューオリンズの災害以降、テレワークの推進が 加速



情報システムの信頼性向上に関するガイドライン

◆ METI

表 2 信頼性・安全性の水準に応じた必須・推奨事項及び関連規格等

	必須/推奨区分			実施区分			T mark 7	
実施項目	システムA			情報システム 利用者が実施	情報システム供給者が実施	情報システム 利用者・供給者 両者が合意	活用できる 規格・標準・基準・ 指針・資格等	
Ⅲ. 企画・開発及び保守・運用全体における事項								
1. 企画段階における留意事項							(4) (6) (10) (16)	
(1)信頼性・安全性水準の利用者・供給者間での合意	0	0	0			0	(18)	
(2) 発注仕様への機能要件及び非機能要件の取込と文書化	0	0	0	0				
2. 開発段階における留意事項								
(1) システムライフサイクルプロセスの確立と文書化	0	0	0		0]	
(2) 役割分担・責任権限の利用者・供給者間での合意	0	0	0			0]	
(3)機能要件の実現に向けた利用者・供給者間での合意	0	0	0			0		
(4) 非機能要件の実現に向けた利用者・供給者間での合意	0	0	0			0	(1) (2) (3) (4) (7)	
(5) 利用者によるシステム要件に関する見解の統一	0	0	0	0			(5) (6) (7) (8) (9) (10) (11) (13)	
(6) 定量的見積りの実施	0	0	0		0		(14), (15), (16), (17),	
(7)情報システムの複雑化の回避	0	0	0		0		(18)	
(8)情報システムの障害対応能力の向上	0	0	0	0	0			
(9) 誤操作等防止への配慮	0	0	0	0	0		1	
(10) テスト及びレビューの徹底	0	0	0	0	0		1	
(11) 検収基準の明確化	0	0	0	0	0		1	
3. 保守・運用段階における留意事項								
(1) 保守・運用に関する体制等の利用者・供給者間での合意	0	0	0			0	1	
(2) 企画・開発・保守・運用の全体を通じたリスク管理	0	0	0	0	0		(1) (2) (3) (5)	
(3) 保守・不具合の取扱方針の利用者・供給者間での合意	0	0	0			0	(7) (8) (9) (10)	
(4) 恒常的な運用状況の把握	0	0	0	0	0		(11) (14) (16) (17)	
(5) リリース手順等の整備と訓練	0	0	0	0	0		1	
(6) 問題追跡性の確保	0	0	0	0	0		1	
4. 障害対応に関する留意事項								
(1) 緊急時対応の利用者・供給者間での合意	0	0	0			0	1	
(2) 原因究明手順等の明確化	0	0	0	0	0		(6) (8) (9) (11)	
(3) 情報システム障害に関する情報の利用者・供給者間 での共有化	0	0	0	0	0		(14) (16) (17)	
(4) 関連・類似システムの障害情報収集	0	0	_	0	0		1	
5. システムライフサイクルプロセス全体における横断的な 留意事項								
(1) 経験則のみによらないプロジェクトマネジメントの 導入	0	©	0	0	0		(3) (5) (8) (10)	
(2) 定量データを活用した管理	0	0	0	0	0		(16) (17)	
(3) 健全なプロジェクト運営に向けた活動の実施	0	0	0	Ö	0		1	
(4) 第三者によるレビュー及び監査の実施	0	Ö	Ö	Ö	Ö		1	
(5) 仕様変更の取扱に関する利用者・供給者間での合意	0	0	0	Ŭ	,	0	1	
10/上体及文ツ板域に対する利用名・医相名同じツ目息								

ITサービス継続ガイドライン(案)」

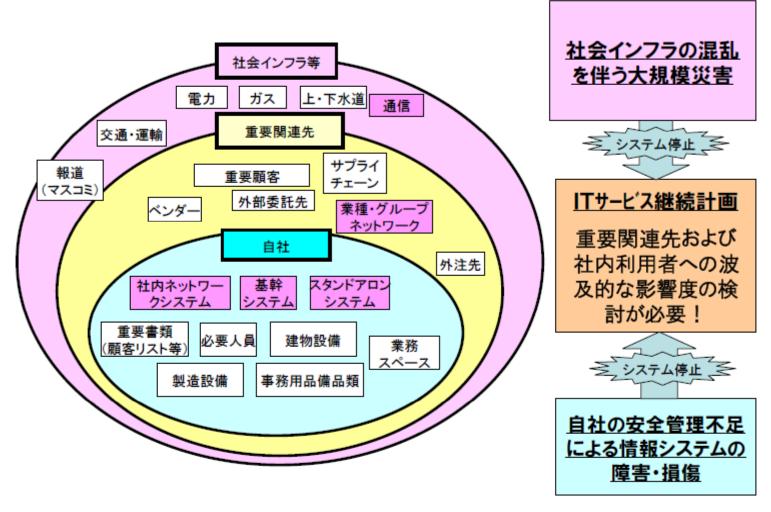


図 4.2-2 情報システムを取り巻く社会環境と IT サービス継続計画

ITサービス継続ガイドライン(案)」

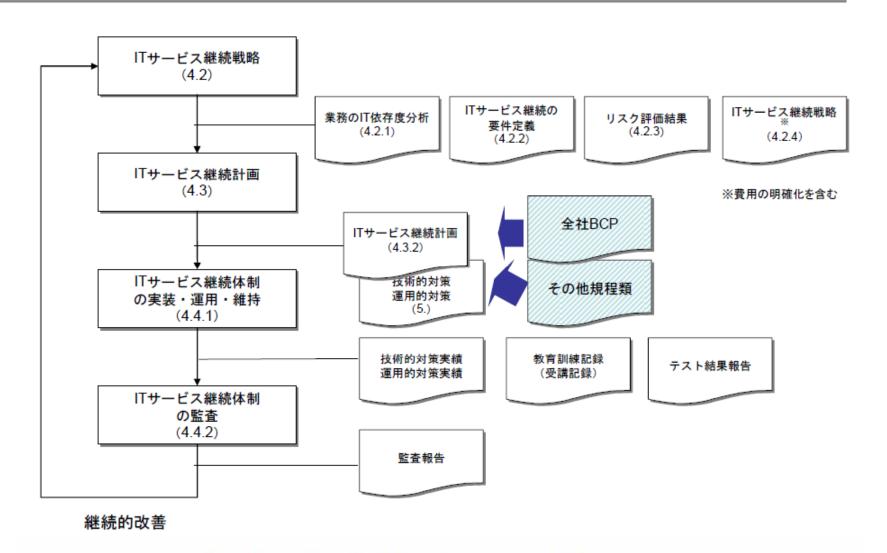


図 4.1-1 IT サービス継続マネジメントのフレームワーク

ITサービス継続ガイドライン(案)」

表 5.4-1 テストの種類と概要

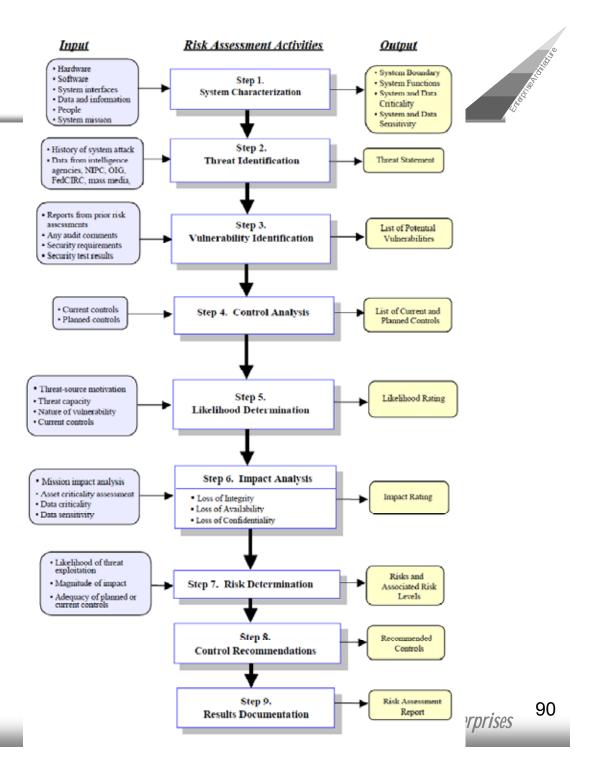
机上チェック ・ 計画の内容をレビューし、 不具合を修正する。 ・ 計画に定めた各種内容の 有効性を検証する。 早期に実施可能であり、事 要員も最小である。 対応手順の良否の検証 は難しい。 ウォークスルー ・ 計画に定めた各種内容の 有効性を検証する。 早期に実施可能であり、事 業への影響が少ない。必要 要員も最小である。机上チ ェックよりも、より末端の 対応手順を検証できる。 計画自身の整合性の 検証が中心であり、計 画発動時の具体的な 課題提示は難しい。 シミュレーション ・ 計画発動時に予想される 状況を前提として、計画の 実行に必要かつ十分な情 報が記載されていること を確認する。 状況を与えることで、より 深い計画の検証を行う。 あらかじめ与えられた状 況内であるが、これに沿っ て、例えば対応チームごと に対応手順内容を検証で きる。 必要要員は多くなる。	テストの種類	実施内容	メリット	デメリット
	机上チェック	・ 計画の内容をレビューし、	早期に実施可能であり、事	対応能力の向上や対
・ 計画に定めた各種内容の		不具合を修正する。	業への影響が少ない。必要	応手順の良否の検証
・ 計画に定めた各種内容の 有効性を検証する。 早期に実施可能であり、事 計画自身の整合性の 検証が中心であり、計 要員も最小である。机上チ ェックよりも、より末端の 対応手順を検証できる。		・ 計画に定めた各種内容の	要員も最小である。	は難しい。
有効性を検証する。 業への影響が少ない。必要 検証が中心であり、計画発動時の具体的な エックよりも、より末端の 対応手順を検証できる。 ・ 計画発動時に予想される 状況を与えることで、より 水況を前提として、計画の 実行に必要かつ十分な情 報が記載されていること を確認する。		有効性を検証する。		
要員も最小である。机上チェックよりも、より末端の対応手順を検証できる。 シミュレーション ・ 計画発動時に予想される状況を与えることで、より状況を前提として、計画の実に計画の検証を行う。実行に必要かつ十分な情報が記載されていることを確認する。	ウォークスルー	・ 計画に定めた各種内容の	早期に実施可能であり、事	計画自身の整合性の
エックよりも、より末端の 対応手順を検証できる。 ・ 計画発動時に予想される 状況を与えることで、より 状況を前提として、計画の 実行に必要かつ十分な情 報が記載されていること を確認する。 ・ は関提示は難しい。 ・ 必要要員は多くなる。 ・ 次のであるが、これに沿っ で、例えば対応チームごと に対応手順内容を検証できる。		有効性を検証する。	業への影響が少ない。必要	検証が中心であり、計
対応手順を検証できる。 ・ 計画発動時に予想される 状況を与えることで、より 必要要員は多くなる。			要員も最小である。机上チ	画発動時の具体的な
・ 計画発動時に予想される 状況を与えることで、より 必要要員は多くなる。 状況を前提として、計画の 深い計画の検証を行う。 実行に必要かつ十分な情 あらかじめ与えられた状 報が記載されていること 況内であるが、これに沿っ を確認する。 て、例えば対応チームごと に対応手順内容を検証で きる。			ェックよりも、より末端の	課題提示は難しい。
状況を前提として、計画の 深い計画の検証を行う。 実行に必要かつ十分な情 あらかじめ与えられた状 報が記載されていること			対応手順を検証できる。	
実行に必要かつ十分な情 あらかじめ与えられた状 報が記載されていること 況内であるが、これに沿っ を確認する。 て、例えば対応チームごと に対応手順内容を検証で きる。	シミュレーション	・ 計画発動時に予想される	状況を与えることで、より	必要要員は多くなる。
報が記載されていること		状況を前提として、計画の	深い計画の検証を行う。	
を確認する。 て、例えば対応チームごと に対応手順内容を検証できる。		実行に必要かつ十分な情	あらかじめ与えられた状	
に対応手順内容を検証できる。		報が記載されていること	況内であるが、これに沿っ	
きる。		を確認する。	て、例えば対応チームごと	
			に対応手順内容を検証で	
			きる。	Guanthye w the Sinart

87

	-			
ロールプレイング		テスト実施の途中で状況	計画を実行する判断者の	想定状況を多数設定
		を追加付与し、参加者の状	訓練になり、判断資料の手	するため、事前準備の
		況判断や意思決定の可否、	当てなどが確認できる。	負荷は大きい。参加者
		連絡体制などを検証する。		の十分な知識も必要
				となる。必要要員は多
				い。
実機訓練		実際の設備などを用いた	代替施設や設備に関して	業務に影響する可能
		テストを実運用及び実作	実際の手順を適用し、実効	性があり、周到な準備
		業で行えることを検証す	性の有無を確認できる。代	が必要である。現場レ
		る。	替システム切り替えなど	ベルで多数の要員確
			実際の手順を経験できる。	保も必要となる。
			替システム切り替えなど	ベルで多数の要員確

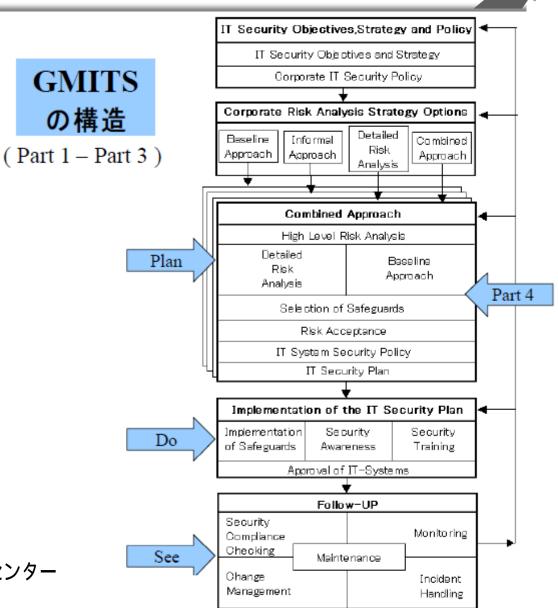
リスク管理

NIST

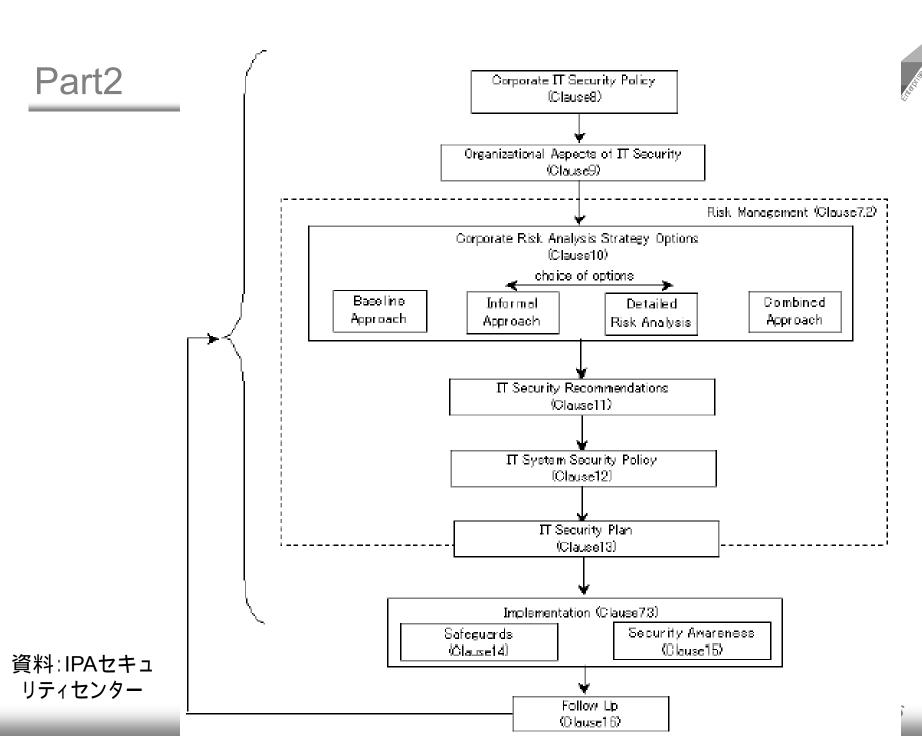


GMITS (The Guidelines for the management of IT Security)

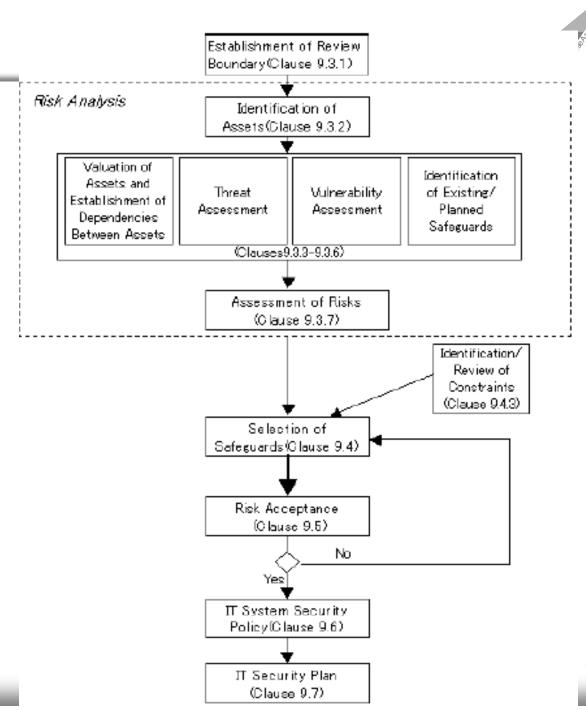
- Part 1 : Concepts and models for IT Security
- Part2: Managing and planning IT Security
- Part3: Techniques for the management of IT Security
- Part 4: Selection of safeguards
- Part 5: (Management guidance on network security



資料:IPAセキュリティセンター



Part3



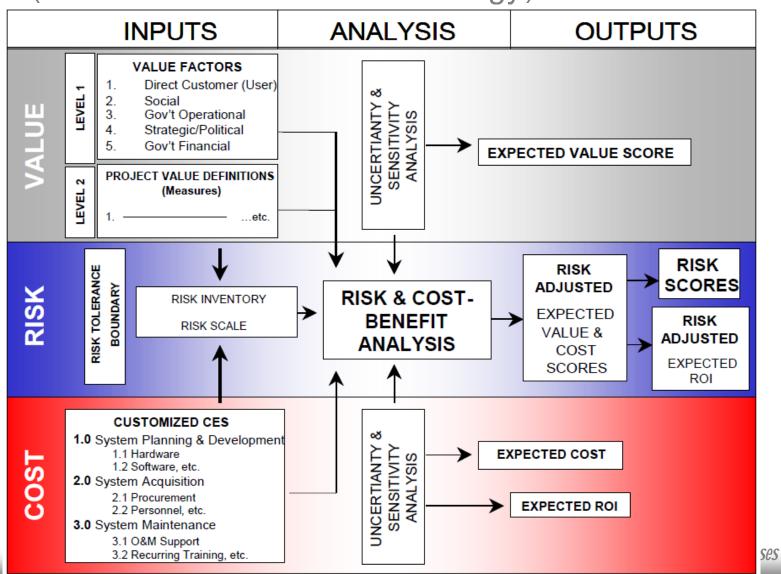
資料:IPAセキュリティセンター

リスク対策

- ◆ リスクコントロール
- ◆ リスクファイナンス
 - ▶ リスク保有
 - ▶ リスク移転

IT投資を考える上でもリスクは重要項目

VMM (Value Measurement Methodology)



迷惑度指数

◆ JUASの提案する方式

事故	迷惑度指 数	業務の重 要度	時間的要 素	影響範囲	影響地域	発生時の ピーク性	再発	可能性

リスクマトリックスによる管理

リスクマトリックス

ソヘノミニ	7777	77A				
リスク	インパクト					
発生見込	Low(10)	Mid(50)	High (100)			
High(1)	Low(10)	Mid (50)	High (100)			
Mid (0.5)	Low(5)	Mid (25)	Mid (50)			
Low (0.1)	Low(1)	Low(5)	Low(10)			



	μĮ	定	IJ	ス	ク	レベ.	ル
--	----	---	----	---	---	-----	---

High	運用は継続できるが、早急に対策を取らなければならない
Mid	適切な期間内に対策を取るか計画をしなければならない
Low	リスク対策を取るのか、リスクを受け入れるのかを判断しなければならない

リスク発生見込の定義

<u> </u>	元色のた我	
	ターゲットとしての魅力	コントロール可能性
		コントロールすることができない
Mid (0.5)	侵入者等にとってターゲットである	訓練していればコントロールできる
Low(0.1)	侵入者等にとって魅力のないターゲットである	十分対処できる

インパクトの定義

12/1/	**************************************		
	コストと損害	業務継続	生命への危険
High (100)	コスト的に大きな損害が出る	組織の目的実施に重大な支障が出る	生命の危険がある
Mid(50)	コスト的に損害が出る	組織の目的実施に支障が出る	けがなどのおそれがある
Low(10)	若干の損害が出る	組織の目的実施に注意が必要になる	

リスク管理表

リスク	判定リス クレベル	推奨される対策	優先度	実施する対策	必要な リソース	責任者	期限	備考

リスク分析表



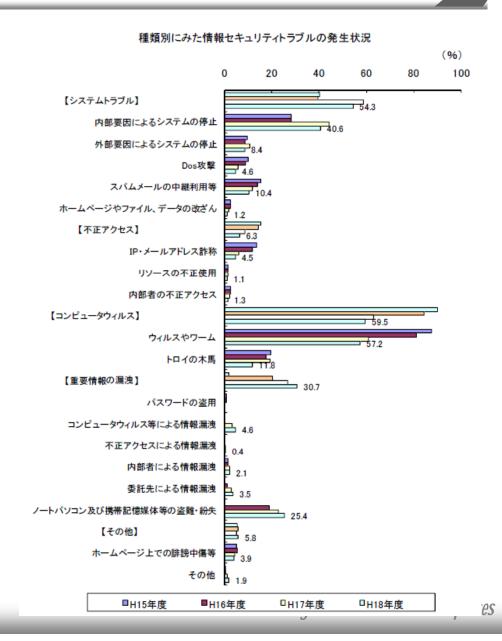
			育成レベル																																	
			物理的背威					技術的脅威									管理的脅威																			
No	情報資產名		自然災害				故				持ち出し				湯油				改さ	'n			ウィル	ス感染			故意による				ミスによる			備有		
			被害	親娘	生 樹!	, <i>i</i>	2男性 ベル L	被害	が開発	青睐 レベル (×)	建物性 レベル	被害	発生	骨球レベル	施育性 レベル	が	発生	骨膜 レベル (×	施養性 レベル	被害	発生	骨膚 レベル (X)	脆弱性 レベル	後書	発度レベル	骨膚 レベル (X)	単男性	ないと	発生	骨膚 レベル (X)	施男性 レベル	被害	親度レベル	骨減 レベル ×	単類性	·
	サーバ		_																																	
2	クライアントPC																																			
3	ネットワークプリンタ																																			
1	アプリケーションプログラム																																			
5	アプリケーションマニュアル																																			
6	パッケージプログラム																																			
7	パッケージマニュアル																																			
3	バックアップデータ																																			
9	職員名簿																																			
0	座席表																																			
1																																				
2																																				

		リスク評価																		
			物理的養成							技	析的青度				1					
No	情報資産名	自然災害		A MAR .		持ち出し		湯魚		改さん		ウィルス酸染		故意による		ミスによる		84		
		リスクの大きさ 州市田田田田田田・田田レベ ル)×田田田レベル	具体的なリスク	リスクの大きさ (1998年1997年)・北京レベ ル)×田田田 レベル)	具体的なリスク	リスクの大きさ (中国第二日 日本 ・ 会会レベ ル)× 日本 セベル)	具体的なリスク	リスクの大きさ (MMMLAPをは・他的レベ か)×開発をレベル	具体的なリスク	リスクの大きさ (1980年 1980年 1980年 イ ル) ※自動物レベル)	具体的なリスケ	リスクの大きさ (MMMMMの音楽・音楽レベ か×音響をベル	具体的なリスク	リスクの大きさ (2000 Man Palis - Malus ル) = 日日日 レベル)	異体的なリスケ	リスクの大きさ (物理ないを含・を含して か×自動性に対	具体的なリスク			
1	サーバ																			
2	クライアントPC																			
3	ネットワークブリンタ																			
4	アプリケーションプログラム																			
5	アプリケーションマニュアル																			
6	パッケージブログラム																			
7	パッケージマニュアル																			
8	バックアップデータ																			
9	職員名簿																			
10	座席表																			
11																				

セキュリティ

セキュリティの状況

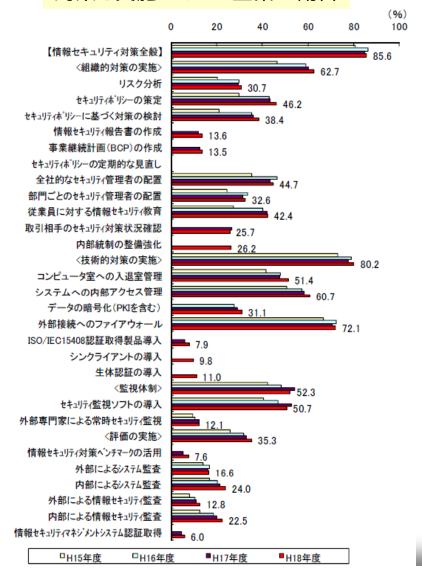
◆ 平成19年情報処理実 態調査,経済産業省



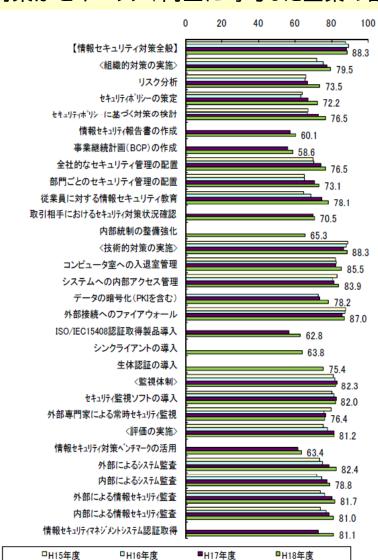
セキュリティ対策

◆ 平成19年情報処理実態調查,経済産業省

対策を実施している企業の割合



対策がセキュリティ向上に寄与した企業の割合



電子政府基本方針の整理

- ◆ 電子政府基本方針から求められる事項は以下のとおりです。
 - ▶ 政府機関の情報セキュリティ対策のための統一基準(第三版)
 - <u>組織と体制の整備、情報についての対策、情報セキュリティ要件の明確化に基づく対策、情報システム構成要素についての対策、個別事項についての</u>対策として整理され、網羅的にセキュリティの基準を設定している
 - ➤ 行政機関におけるIT人材の育成·確保指針
 - PJMOの役割
 - 企画段階では、最適化計画の作成における、業務・システムの現状分析、業務の十分な見直しや情報システムを安全・安心に活用するためのセキュリティ面の十分な検討
 - 運用・保守段階では、SLAの管理指標などを活用したシステム運用状況の定期 的な把握、制度改正などの環境変化に伴う機能追加などの<u>保守業務の管理及</u> び障害発生時の事業者に対する適切な指示やセキュリティの運用
 - > 電子政府推進計画
 - 情報セキュリティ対策等として以下に言及
 - 効果的な情報通信技術の導入
 - 情報セキュリティ対策
 - 府省共通的なセキュリティ機能向上の推進
 - 個人情報保護対策

個別マニュアル群の整備

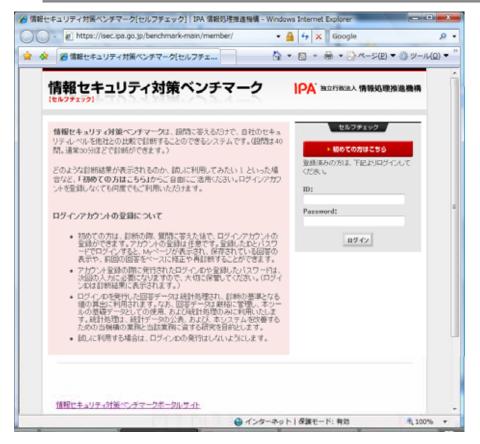
政府機関統一基準適用個別マニュアル群

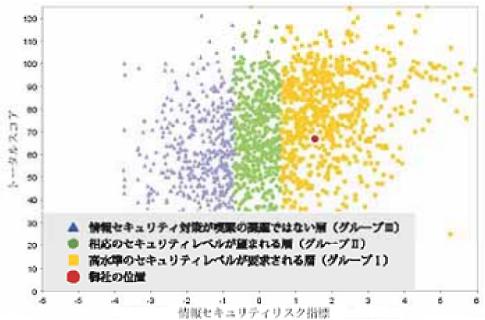
政府機関統一基準適用個別マニュアル群とは、各府省庁が「政府機関の情報セキュリティ対策のための統一基準」(以下、 政府機関統一基準と呼ぶ)に基づき策定した省庁基準を、実際に適用する際に対策を円滑に実施するための文書(実施手順、規程及びマニュアル等)を作成する際の参考資料として作成したものです。

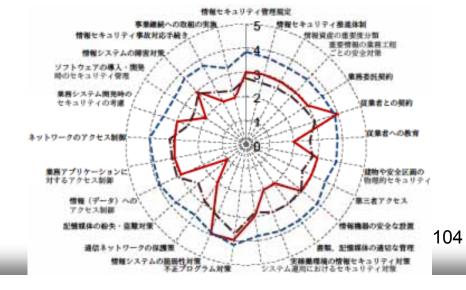
統一基準	マニュアル		対応する	統一基準
章番号	番号	マニュアル名称	初版 (052版)	第2版 (071版
第2章	DM2-01	政府機関統一基準で定める責任者等の役割から見た遵守事項一覧	0	0
	DM2-02	人事異動等の際に行うべき情報セキュリティ対策実施規程 策定手引書	0	0
		人事異動等の際に行うべき情報セキュリティ対策実施規程 雛形	0	0
	DM2-03	違反報告書に関する様式 策定手引書	0	_
	DM2-04	例外措置手順書 策定手引書	0	0
		例外措置手順書 雛形	0	0
		例外措置申請・終了報告書に関する様式 策定手引書	0	_
		例外措置申請・終了報告書	Q	_
	DM2-05	障害等対処手順書 策定手引書	0	-
		障害等対処手順書 難形	0	-
		障害等報告書に関する様式 策定手引書	0	_
		障害等報告書	0	_
		障害等再発防止策報告書に関する様式 策定手引書	0	_
		障害等再発防止策報告書	0	_
	DM2-06	自己点検の考え方と実務への準備 解説書	0	0
	DM2-07	情報セキュリティ監査実施手順 策定手引書	0	-
第3章	DM3-01	情報の格付け及び取扱制限に関する規程 策定手引書	0	0
	DM3-02	情報取扱手順書 策定手引書	0	0
		情報取扱手順書 雛形	0	0
		機密性3情報印刷書面管理表に関する様式 策定手引書	0	0
		機密性3情報印刷書面管理表	0	0
		機密性3情報移送・提供許可申請書に関する様式 策定手引書	0	0
		機密性3情報移送・提供許可申請書	0	0
		機密性2情報移送・提供居出書に関する様式 策定手引書	0	0
	1	機密性2情報移送・提供層出書	0	0
第4章	DM4-01	情報システムにおける情報セキュリティ対策実施規程 策定手引書	0	- 366
		情報システムにおける情報セキュリティ対策実施規程 雛形	0	- 36
	DM4-02	セキュリティホール対策計画に関する様式 策定手引書	0	- 36
		セキュリティホール対策計画	0	- 36
第5章	DM5-01	庁舎内におけるPC利用手順 PCの取扱編 策定手引書	0	- 36
		庁舎内におけるPC利用手順 PCの取扱編 雛形	0	- 36
	DM5-02	庁舎内におけるクライアントPC利用手順 電子メール編 策定手引書	0	- 86
		庁舎内におけるクライアントPC利用手順 電子メール編 繋形	0	- 36
	DM5-03	庁舎内におけるPC利用手順 ウェブブラウザ編 策定手引書	0	- 86
		庁舎内におけるPC利用手順 ウェブブラウザ縄 雛形	0	- 36
	DM5-04	モバイルPC利用手順 策定手引書	0	- 36
		モバイルPCの利用手順 観形	0	- 36
	DM5-05	サーバ設定確認実施手順 ウェブサーバ縄 策定手引書	Ö	36
		電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程 策定手引書	٥	*
		電子メールサービス提供ソフトウェアのセキュリティ維持に関する規程 雛形	0	- 36
第6章	DM6-01	機器等の購入における情報セキュリティ対策実施規程 策定手引書	Ö	ő
		Man 4 - Mar 11 - 1017 WINTER C. 1 - 7 / 1 /2 MCMORNE MACT 21		

内閣府

IPAツール







CSAJセキュリティチェックシート

セキュリティ・可用性チェックシート(上位概念定義)

CSAJ/JCSSA情報システムの信頼性向上のための取引慣行・契約に関する検討委員会

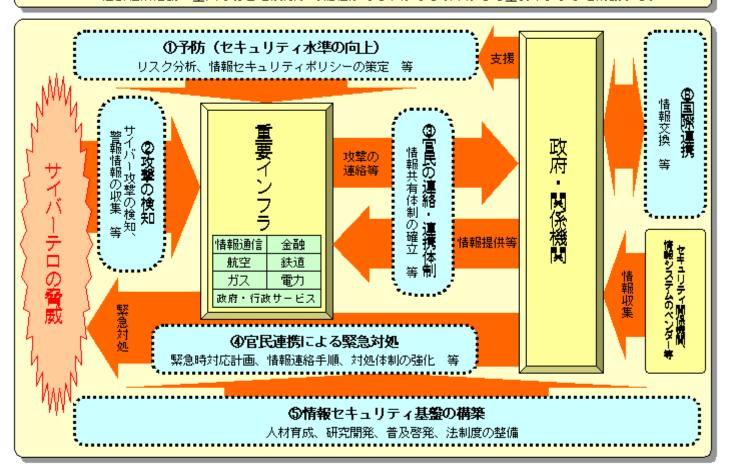
技術的セキュリティ対策	-														
対策項目	リスクの詳細	レベル1	参考 レベル2	1		L & II 4			務での対応 仕様、候補製品	<u>~</u>					
	情報を参照している人が、本人	何も決められていない	個人を認識できる	レベル3 本人認証の強化	46.0	的カフ	レヘル4 5人認証		メリルウレヘンレ	11.惊、 恢 開 妥 面	寺				
情報を参照している人が本人で あることを証明する。		情報を誰が参照しているか特定	パスワードを利用して、個人を認識できるようにする。	特定のカードやログインの二重化などで、本人認証を強化する。	生体認	証等を)せ、定期 施する。							
アクセス権 個人情報、企業情報によって、ア クセスできる人を制限・管理す る。	誰でも情報アクセスできるようになっていると、削除、改ざん、複製、持ち出しされたりする。	何も決められていない 情報に誰でもアクセスできてしま う。	コンピュータ単位で設定できる サーバ単位、フォルダ単位で、個人・グルーブがアクセスできよう に設定する。	認証情報に基づき資源単位で アクセス権が設定できる ファイル単位で、個人・グルーブ がアクセスできるように設定す る。	の収集 アクセン 集・分析	分析 スされが 近できる	でアクセス iができる た情報 (口 る。	グ)を収							
暗号化	情報機器(コンピュータやUSBメ	何も対策されていない	モパイルコンピュータやUSBメ	全てのコンピュータについて、	を	217/12 113 123	対策協能 パスサードを利用する	リスクの保険 バスワードが展開付着な目的な ボスケードが展開付着な目的な	-061 7007-78880401	製造いた。 ・代表1 ・記載のスタードをする中のに変更する。 ・記載の大い月間に、パスタードを変更する。 ・パスタードは、機能などの大利の、ドラロデする。	レベル1 (文明の: ホャ月等 IC: パスケードを変更する。 パスケードは、機能なもの: パギリン・ドスケードを 水密性: 一種類なよの次字様の使用: を設定する。	L-1064 ボードの名が複数のアカウンドをもつ場合は、それ タードの名が有数のであります。また、一つのパス ウードの名のが複数にやすいパスケードを設定しな	2011年 日本	16 10088 1131	参考文献 JS Q 2000 2000(6) - 知時整理局 - 集手通用総計マニンア 上租 庁立内における中心総用手展庁に の可収録 様本的権能でニック3 政治 ニートの日本の自然、以2 (3)
情報を暗号化して、紛失・盗難・ 盗聴の対策を施す。	モリなど)が盗難又は紛失するこ	社外に持ち出すデータ、社内の	モリ単位で暗号化して持ち出す 社外に持ち出すコンピュータ、 USBメモリなどの中に入っている	データを暗号化する 社内のコンピュータ、社外に持ち 出すコンピュータ、業務で使用す	1		F-1-7-7人の機能を減防する	チムにおうかではに、情報を選 えいしていまうをそれがある。 あった情報機能がスットワーでに 物質があると、情報が満たいする	本置目やそこなよンドゥードと指摘を終ってそない。	の関節のアルド語(こ。パスワードを変する。 パスワードは、原数をおんが成り、ドスマード パスコードは、原数を多点をはられない。 パスコードは、原数を多点をはられない。 イスコードを数すると、カンスードのアイルで は同様になった。 ののパスマードのでは、アルス・カンス・ルート ののパスマードのでは、アルス・インス・インス・ ののパスマードのでは、アルス・インス・ ののパスマードのでは、アルス・ ののパスマードのでは、アルス・ ののパスマードのでは、アルス・ ののパスマードのでは、 のののののでは、 ののののでは、 ののののでは、 ののののでは、 ののでは、 ののでは ののでは ののでは ののでは ののでは ののでは ののでは ののでは ののでは	代書館、三種様以上の文字様の使用を設定する。 本書館の本正なコンピュードの利用をいり、アル 機関を 核形に 装飾して 接続を担じまる。	ウードが名次が構造しやすいだなウーを設定した。 ・機能性が実、認要では、生体設定を使用する。 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・		ANA	の数長艦 端末的機能(データ3) 政治 2-ドロ付金の数数(12) の
		-	データを暗号して持ちだす。	るUSBメモリ、外付けHDD、	12		前所者が本人であることを証明 しま選手を	おそれがある。 利用者の参加が公司できない と、機関がは、利用者が協議を そこな時に対けへ過ぎには なるそれがある。	ーおのコンピューナモーつのアカウントで、複数の何 作者が使用する。	・技術コンにも一手のログを取得する。 ・EthylosolDプスクント、FCエワードを利用して、利用を を進力する。	・無限コンピューテのロアを取得する。 一般のコンピューテに対して、一人との使用を収集	・生体製造・動植・性検索型(など) 年利用して、利用者		A1182	
				CD/DVDなど情報を書き込める ものに対して暗号化をする。	3		業務ソフトウェアを機能量はで使	不正に取成して性外へ過ました 甘名あぞれがある。 パスマードの物理がされている いと、子正な影響や情報達えい	製製のデは取得しない。 パスワードを要視しない。	- 例のコンピュータを機能の利用者では使用させな し 一部は、ログを影響する。 - 製品機能を使用して、コンピュータを利用する。	例文ののードウログインの二番代などで、本人認証 実施する。 但2007年取得する。 位3007年取得する。	の名人間は今天香であ、 1年 - 美生間は今天香に、間は後度を上げる。 一貫はログを取得する。 ア・生性間接を利用してパエワードを使わない。		ATIES	#####OREST#11919#### 608-8# #18 411 ####
					4		第四クストラルアの近世時間を 関する	が確認できないおそれがある。 単数シブトウェアの数であれるこ 対策されていると、情報が盗まれ ままそれがある。	単核シフトウェアの多使用可見を監視しない。	・ 単格ソフトウェア心系要用時間を影響する。 ・一定時間に上利用されないで、シレンを影響する。	・東部ンフトウェアの多使用地向を監視し、協力する。	- 連携・アフトウェアの本使用時間を監視し、警告して、 都断する。	-	ATTE	MR(1)
ウイルス等の悪意あるプログ ラムの取り扱い及び検出する機 能の導入	る悪意あるプログラム(ウイルス やスパイウェア等)により、システ	何も決められていない ウイルス対策を実施していない。	ウイルス等を検出し侵入を停止・警告できる コンピュータ上で悪意あるプログ	全システムに対するウイルス 対策と集中管理 ネットワーク機器やコンピュータ	6		BE-07701168876	をおそれがある。 国もが協議を開業できるように なっていると、情報の他がみや選 えいのおそれがある。	ワーパミン協能に進てもアッセスできる。 情報を機関レイスに分配しない。 情報にアクセスした機型を影響しない。	・サーバ上の機能にアクミス機能されて、機能が応い 利用を記念者できないようにする。 ・機能にアクミスルを維持を取得しない。	福祉を重要支票に続けれる。 を描して、重要支票に利用をマグループを投でプラ を描して、企業支票に利用をマグループを投でプラ を描してからは、原理を影響する。 は2世界を出すことにより、整理する対象を減らし、 が開発してのこのを示が、 がにする。とを表が、 がにする。とを表が、 がにする。とを表が、 がにする。とを表が、 がにする。とを表が、また。	ご・アラウスの磁性を定形的に監査して、情報の待ちを りした問題があれば発きする。		KND	
悪意あるプログラムから情報資	ムが利用できなくなる、データが		ラムを検出して削除し、警告でき	など複数の対象に対して、悪意	7	単など	E4.0	と、現代が施えにするおそのたが ある。	テーアを味可だしない	・技術に持ち出すコンピュータ、電子機構、LOBAを1、 作行(THOD, COLDIDGE) かやのゲータを暗得化す 6。	を持ちてンビュード、利用に持ち出すコンビュード、 数子物は「CISSO をり、かけでMCD、CD/OVOG()に 対して物句を含する。	・投資のエンビューデ、技術に持ち出すコンビューデ ・電子構成、USA、4年、各刊THOD、CD/THOGE / IC がして開発化させる。 ・使年時には国際が専用必要となる。		A-031	
産を守る。	消去される、情報が外部に漏え いしてしまう、などのおそれがあ		ర ,	あるプログラムを検出、削除する ための機能を導入し、被害状況	8		8-17-7538488680 676	ネットワーク上のテータが直接を れると、情報が消えにするさそれ かある。	行のに連るデードは平文で通信する。 196の通信は暗号化(196.通信/にない。	-madesepe, m.ess c. 114,	担めた出る情報を、事前に利力で確切的できる。 6. 104の適位を確切的は11.適位などです。	コンピュータのも見信する情報メールののパテータ なども、利力、利力にかかからず、すべて事前に指す がして過信する。 つかの通信を確信と、300通信などでする。		X (0.3)	
	S.			の収集や定義ファイルの更新を	9		NGM+HETA	様のご復報がからは、関手に 他のイフルで機能が過去しても おそだがある。 様の間が必要に出来すると、様 のとしたゲーナを集りされて、様	#067.001	製造が445~ト以上の機能化を使用する。AII 405~ ト以上など、 ・現代開発、平文・選集の文字列、のままソフトウェア上	最長が130C+PG上の機能化を使用する/AG 12 C+PG上など、 機能は、機能としてソフトウェア上で影響する。	- 株式製を構成的に、発展のパスワードをで発展す	\vdash	A1032	
				集中的に管理できる。	10	個人規則 (201/PE)	日本ストラープラリの出版です。 日本人を初回する	のとしたタードを集付がた。 能が遊光にするホモにがある。 サーバのストンサード機能にお する使んが熱やの撃を受ける	AZYYEXIDEBLUIC	A STATE OF S	THE STATE OF THE S	・ 機関機の所作については、システム的に影響者は所 ・ 計算するなどを ・ 計算が記述をプラフリスを検討・電響する。 ・ 計算が必定を選挙を終め、計算する計算を一定など、ま	-	Killer	
ネットワークの運用 ネットワークを流れるデータ量の 管理をする。	ネットワーク障害や大量のデータ 転送により、ネットワークが正常	何も決められていない ネットワーク管理ツールもしくは	管理ツールを導入する 障害検知やネットワーク負荷を	冗長化する、使用状況を監視 して記録できるようになる	11	ウイルス円数	BEAG 7077A BERETS	Erminitos orpare Elbitosentras.	ウイルス列集を実施しない。	様人する。 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	担人する。 小型からのアウミスログを取引して、定期的にしが 1する。 一番目のもフログラム・ウイルス・スパイウェア・ボ・ニ によって、アナミのゲーチに付着していないが、使出して製 物する。	報人であ、 ・ボラアの工程会になる。 自動的に連帯する仕組 みを基入する。 ・ボロシャのアクリスログを取得して、定期的にしばー する。 ・ 番組を12073と、フィルス・スパイウェア・ボコ に、ーチ上のデーサに付着していないか、検索して報 数する。		Kuto	
	に利用できなくなるおそれがあ る。	サービスを導入していない。	検知するツール、サービスを導 入する。	ネットワーク機器を冗長化して大量データに備えたり、ネットワーク障害時にネットワークが利用で	12		2-ACS(CREEK) 707	ウエバイウェア等(に20,93年 ムが利用できなした。データが 満まされる。機能が外部に満入 いしてしま)、などのおそのがあ も、	P−ルのワイル3月度を実施しない。	・利用の第2フビニーやのクイルスが開催の途を指す の対象を構造しても、 ・基度点をプログラムを検点した環境・システム影響を に通常する。 ・通常点をプログラムやイルス・ボールに参加して にはなり、検索する。 ・フィルスを開発しま物・システム影響をご適合す ・フィルスを開発しま物・システム影響をご適合す	・ スタムのグラブスムの対象を開け、中位でも4 転号を入する。 ・ 他のからコンピュータのフィルスが開発対象を発生 ・ 利用をもプロプラムを検が、影響及び・ステムを参 ・ 人のでは、アメリカを受け、ステムを参 ・ 本意本もプロプラムを使が、また、ステムを参 ・ 本意本もプロプラム・フィルス・スパイウェア・スティ	・システムの変更を71に回りを検討的にも様式でも検 数を進入する。 ・ 通道あるプログラムによるストリフラ連合を負債的 に関わるフレジムーやロフィルス対策以及を把握す が見出るが成人する。 ・ 通道あるフリファムを担塞 ・ 通道ある システク 単一・ エン・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		X.EU	
				きなくなるのを回避したりする。	13			のエバイウェア等。ガメールから 使人すると、シェテムが利用でき なくなる、データが出来される。 情報が外部に達えいしてしまう。 たどのなるれの進る。		ウイルスを検索した場合、システム物理をご通知す 6.	おごかけしていないか、検索する。 メールに添けしている差差あるプログラムを駆除する。 つくルスの行動性があるものを検索する。 つくルスを検索した場合、システム管理者に通解す	おこの付いていないか、検索する。 ・メールにお付いている形象をプログラムを解除する。 ・つくルスの可能性があるものを検索する。 ・つくルスを検索した場合、システム管理をご通報す			
保守	ハードウェア保守がされていない 何も決められていない	何も決められていない	障害発生時に対応する	定期保守を実施する	14		ABV-REGRY 6	連邦メールが使入すると、トラフィック課法 システム条件の理 3に 長根あるプログラムの使人 長君あるののヴィッへの転送 な	通数メールを対象にない。	・被称メールの対抗を終こなり、知をつける。	通数メールの何回をおこない、現職を確定施り分け も、	・ 他的スールの対抗をおこない。 音楽なき位内からの 受信を折断する。		X-1640	
OSやアプリケーション、ハードの 保守を行なう。		メンテナンス作業をやっていな い。	障害が発生した時点で、保守作 業を実施する。	定期的に機器の点検、整備を行 い、耐用期間を過ぎた部品は交	15		中間の10年1094日本町田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	単数にする原金であるでくり回数 を対けられていると、単数が単心等 を、トラフィック地位、影響をあって ジファムの変化、たまり上の地位 終えに、などのかそのである。 行列之のキャルファル	MASS CHORECTERS EDITOR	を見まれないにもプロックする。 「他できなシンドムードに進入されたウイルスが出来」	・ はまれたはなーライ・大きを向して、カナゴ(単位で 他のでくせプロックする。 ・ はのなってなのサネシサ・ド電車がを集中的に	電子がないは、をプロックする。 ・養性がは多サーチペースを使用して、カナジの単位で おめがくが見なってき。 ・世帯位の他、196年できた。 対策を対象 1964ですが を対象に対象があった。 対策を対象を対象を対象 ・対象にあるするサイトがあてプロックする。 ・対象にあるするサイトがあてプロックする。		ANE CO	- 説の機能の連載セキュリティ対象のた のの例 - 選手 第2版 (421 セキュリ ティホール対象の(432 千正プログラ ム対象7 (32)
				換する。	16		10-408411	報信できていない。 製造時代の の通れ、ボジャー海れ、管理状 分の受理が関係、などのあそれ がある。		・ ウイルス機能が終	機能性を・・アップデート状況・ウイル工程形式別	・サインデートの同 ・ウイル工程を対象 ・会観的なレポート生成機能			
	OS、ミドルウェアの保守がされていないと、不具合の発生や、セ	何も決められていない メンテナンス作業をやっていな	障害発生時に対応する 障害が発生した時点で、不具合	定期保守を実施する 定期的に不具合修正版を取得 し、予備機でテストをおこない、	17		ファンサーで製作する ファンサーで製作する表現れる プログラムを検索する	ATRATES PIPATR MTEDICS P-PIDES TO METERINE LEDERINGS TPODICTERNICION DOTO ALAMORISONO DOTO ALAMORISONO DOTO ALAMORISONO	ファクサ上ではずってのプログラムを実行する。	・	10年の1つからなどを収入を収入。 日本のでする。 10年の1つからは、日本のでは、日本のでする。 で、日本のできませる。 イオーンファイルに対し、11、12、13をあるプログリ 上を検討するための情報を導入する。 本書的なんかのようを持ちては、USAステフレットを ありを指する。	ののマイクランのスパイウンアを担こ。自然の見てから ののマイクランのスパイウンアを担こ。自然の見てか のでは、これでは、これでは、一番をあるプログラ を加まり、一つに、これでは、一つに、これでは、これでは、これでは、これでは、これでは、これでは、これでは、これでは		KWO	
	キュリティホールによって情報が 漏洩するおそれがある。	υ 1 ₀	修正版の適用を実施する。	し、T1個機でデストをのこない、 適用する。	18	33479e-A	5317-79-EXEMPER	がれると、ウイルスに関係してしまう。 最低がら加工業人に対していました。 とこのようなのでは、 またりでは、これのようなとなった。	N->ワーンサービス利用に関する方針を構定しな	- ネン・ワーフリーと11別所に関する方面を構成する。	ネッケーンサーマス利用に関する方針を構定する	- #++ D-00 - KINNCHFANNEHZFA.		ANG	
	アプリケーション保守がされてい	何も決められていない	障害発生時に対応する	定期保守を実施する	19		E-1-7-7上の後重を減出する	に物面にない。 他内外のも不足 なアウシスを増せ、情報が強え いてもあそれがある。 あ・トラークを被称 元内される 特置が他のには例できない。 そとアウスなどのかずかに対 あが場合いてあかりである。	ト カンステムに適切なホスト他などを設定しない。 カンステムに適切なホスト他などを選定できる設定を ない。	・他のクランを使用する。 ・他のステムに使用なおストをなるを設定する。 ・のののためでなどによりのストをなるを包含に確定する。 をも、	他のからの他国立会実立したのかおりする。 他のから地域の企業ならなったに関する。 ポッショーです。任文別共に対するログを監視し、会 更におって整合する。 現直音句のよる心体など、無対に対する。 使言の他が必然とと関する。 使言の他が必然と支援的に関する。 使言の他が必然と支援的に対する。	・日からの他日よりますもののおけずる。 日からの他日よります。 日本シラーファーと対所に対するロケを放布。 数に必って会合する。 必要に必って、他なも数的に成布する。 ※要の場合サンエアムで競別人が選手る。 ・そこな支援地位を向かりに成布する。		A.11.43	
	ないと、不具合や期待する正しい 結果が得られないおそれがあ	メンテナン人作業をやっていな い。	障害が発生した時点で、修正版 の適用を実施する。	定期的に修正版を取得し、予備 機でテストをおこない、適用す			直端が明月及び車階級定用 ボードを指揮する	必予機能化するおそれである。 記事・程理用ボードへあますりた 大を受けると、システム型を正に 哲学されたの情報が構えていたの するまそれがある。	から、単位をボートへはでもアフセスできる。	・放棄の機能が発生のヴに残す。 ・記事、管理用ポートに適切なアフリス機能が定する。	「京系、管理用ボートに得けなアクリス種を設定する ・管理用ボットワークは連定のネットワーフとは別に対 前、一般的用をかくしな対象的、協関的にアクリスト	・ 近新・田塔用ボートに借いなアクリス権を設定する。 ・田俊用ボルトワーフは通常のボットワークはご覧に乗 車」、一般の何をからはできる。		ATTAL	
	8.			الله الله الله الله الله الله الله الله	22		8+17-78MRHHF6	#680 KD/86. 8117-70 MCC/815 KB/CD/ 6 85 C/775 18 KB/CD/	担内をットワークに担めからアクセスできる。	・投資ネットワークへは充分からのアクセスを開止す の	形物にする。 ・町内まいワーケの一部資産のお、町内からのアウ はおかけせる。	対象にする。 ・密線用メルワーフへのアクセスログを監修し、不正 ログウミスを整合する。 セ・利用にいるボスシス・ワーク・ごなによれるから27 ウラスフをは、他のス・レーフークをからにいまする。		A11.48	
機器運用監視	システムの状況を把握できない	何も決められていない	運用状況を遺隔で、手動で把	運用状況を自動で把握、記録	23		8+17-7機模を制御する	がある。 ス・ドフートへの機能を図る文 他しないが、不正アクセスや情報 終えいが発生するおそれがあ	までもあっトワーフが出来に使用できる。	-BA-9CHIOSISEO(TS.	利用者等におってつつ変形を2010年のよう。 アクセスを反に対する通灯なモニテリングを実施し で、同窓地には必要的に設めても、	利用者をよって一つ世界をコンドニールする。 ・プラスを与に対する者になってコンプを実施し で、東京時には自動的に登みずる。		A1148	
サーバ、ネットワーク機器の稼働監視を行う。	ことにより、障害の対応が遅れて 情報システムへのアクセスが長	サーバ、ネットワーク機器の稼働状況を監視していない。		ができる 稼働状況を常時把握し、異常が	24	OF SERVICE	2417-7.2-91278MM 76	も、 のは、かまからのできなし、 かっとが機能が強人すると、 のは、トラーク機能が予定に変 できないな、機能のエールが利用 できないなったりするおそれがあ を・トラーリの利用が確切によ	対策にない。 確心はネットワーフサーミス利用に関する方面を実	Aの主要的に、中国に対して内部キャンフ・フを中間 他にする。 他がルーティングなど、間定的なルーティングを制能 する。 小国のでのボットフーンフェム人的に関する方面を	へは不を使用し、外部に対って内部ネッショフをネル 他にする。 他はずなみのネッション発展に対って、ルータ・フ 対象をロイルを主義する。 かまからのネッションマーとよ利用に関する方針	マルー・ファー・マの日本のローにはなり、 スー・ティング機能を終した記録をいまり一つなどを 地形する。		AMD	
	時間停止するおそれがある。		ర ,	あれば通知する。	25		NUSTABRESHEREN FO	かけたれたで、機能施工にしたで するませんかある。 小型の円をきない。単型できない と、小型の中心をデアウスで、 機能施工にしたで開かるアナム	製品を10mでもアフセスできる。	-1-75. (117-F1265)582000576.	利用者に対して定期的に用は、銀用する。 アスプードの機能を行る意即の信頼を使る実施する。 6	・ 記録をしか、てお願りに用む、概念する。 お願りのと記述者を行い、たかのの表別がおき機関す りつきておけるとのとのと思想はなる。より展文を形 財産のは記さを持てる。	-	ATTE	
					12		8ットワーク上の改置を実施する	が特点したでするおそれがある。 まっトワーでも連絡があまれる 何質を表のに関系できないと、ギ	すべての祝養がネットワークに拒絶できる。	・ネットワーウにアクリスする発展情別機構を、CD機 例 パータルンなどを利定する機能を購入する。	スのワーリにアウミスする出業権的機関を、CD パータンなのを対定する機器を基人する。	EU-CARRE		A1143	
障害発生時の対応	システム障害時の対応手順が決	何も決められていない	障害発生時は代替機を手配	障害発生時は予備システムに	2/		通信を暗引化する	とアクセスなどの例を時に対応 か長期にするおそれがある。 連位を暗むとしていないが、ホラ アクセスがうわれたり、情報高ス	通信を明むだこのL(- 外部への通信を暗む化する。	●おい訳定した方数に成ってアクセス可否を自動的 に制御する。 	・ より他力な機能を向北/MX12MC++以上などを形 形する。		A3122	
障害時の対応マニュアルの整備 をする。	められていないと、適切に対応で きず、復旧が遅延するおそれが	システム障害時の対応を決めて いない。	する 代替機を手配し、到着後交換す	手動で切り替える 障害が発生した場合は、予備機	20		日で新聞で使用することによーす を簡優する	グリングラフトは「日本の にはなってするまでにがある。 毎日でおけしてにははコンピュー タフルケを開発できまります。これ 新り換えしてもあったがある。	個人を有コンピュードを使用する。	・明月実施のコンビューデで作業する。 サイブのデータがサーバリにあり、コンピューギビは	会社交易のコンドューデで有限をする。 ・デベアのデータがサーバリにあり、コンドュータに1	明月支援のコンビューデで放棄をする。 は、デルスのボータのマード上におり、コンピューテには のデースの「おおって」と		A1172	
∠ > ⊘ ,	さり、後口が延延りるのでれがある。	V 1.0* A 10	る。データはバックアップを利用	厚舌が発生した場合は、TM機 に手動で切替える。データはバッ	29	\$76-\$1200	841-4154614T(00)		利用者によるアラウス機能の変更をしない	ー特殊者するが、コンピューサビロデーすが保存であ ロ(する。 ファイルのアクセスログを取得する。 ・利用者を実際し、利用者者にアクセス形面の名な様	・ディアのダータリマーパンとは、コンピュータに ・特殊数学のグ、コンピュータにはゲータを扱ってき にできる。 ・特殊数になゲータは、一定特別で映画的に活合 ・ 特殊数単の実施システム・エグラで入る機体を開催	部位でもない代配をにする。 ・ファイルのアクロスログを取得する。 す ・コンビルーを取る通信データを確定化する。 す ・アフロスログを取得して、範囲をログラロスについて		Ama	
			する。	クアップを利用する。	30	X P & (08)	の利用を担保する 利用者の向けずましを扱く	できると、機関は人の場合ができ をこれによる情報達えいののそれ がある。 別等者ののグラン協能が表現さ れる人、向でするによく関う者	NECT!	他、およびファイルシステムを区的する。 をのはW ATMHOLOU Selection (世界) などの、間切場的 サースなソファウェアで機能すれない機能を構入する。 パスワートなどの回回機能を確かを入して、機能化す	を ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	日発動的に整治する。 変型施収上のログオン共和が発生した場合に、整 機能に通知する。	-	AULET	
データの保護 データが改ざんされないように防			特定のデータ、情報が保護さ れている	すべてのデータ、情報が保護 されている	31			がログオンしから、機能療力にし たりするおそれがある。		ジェスター・ログの回馈機を暗号をして、他的化す をは10回答である。 ジスタートの他切断用が切れた場合、アカウントを無 別だする。	金数百数を扱くなるに、一定時間内に連携したログ オンを制度する。 ログオン時間の原列を開始時間等性報道した環境には 所を手限制的にログオフする。 ログオン時間の同様の関係が自然的関係が立た。 製剤はコンジューラを目標する。	(株) (地) (水) (水) (水) (水) (水) (水) (水) (水) (水) (水			
御する。	したりするなどのおそれがある。	策を施さない。	データ・情報をパスワードや暗号 化で保護する。	すべてのデータを暗号化やアク セス権で保護する。	32		さらレーティングシステム変更終 に開発ソフトウェアの動作を検証 する	でんしーティングシステム変更所に無数シフトラッチ十分に規定しないは、年齢的の特別、新たない。研究のの表現を明確の失敗を、などのあそれがある。	MECOL(ポペレーティングシステムに変更があった場所、都度 変更を記録する。	電視でボージを取り予報には、ボベレーテンジ エタムの変更に必要なした。一つシステムは競技者 、セキュリテ・実施などによるボベレーテンジウステ への言意でがけなりような意味で、シスキムの実施 物理、10時でも予報を支払。 まで、ロボークランステムに対する更多を設定する ま実施に、同様で発生した場合に関係するを受ける のまた。同様で発生した場合に関係するを提供する。	・ 高泉田田、日マモンデーを表示なってもあるない之を あるためである。 あるためではませき様式で行うなのの最初度の予測を定 の の の の の の の の の の の の の		2013	
ログ管理	情報システムの適切な監査ログ	何も決められていない	ログの取得のみ	ログを取得し、定期的なレ	33	##LAK (16-) 738308921 Pr	TO TO	外部の何者を立い。回記できない と、外部からのそうアフリスで、 情報選入いしたり情報システム か得点しなりずまれそれがある。	mar-or(・外部の情報システムにプリセステを終に、ゲートウェ くちて利用をの認証を実施する。 ・外部からのアリセスは、一部外のみて見り付ける。	中部がくの間景には、ハードフェデキー及びバス フードを利用する。	・ ・ ・ ・ ・ ・ ・ ・		Ama	
情報の持ち出し履歴をとって監 査の証跡資料として管理する。	が管理されていないと不正な出 来事に気づ〈事ができないおそ	ログを取得していない。	ログを保存する。	ポートを行う ログを保存し、内容を分析し報告	34		を対する 関する を対するコンピュードの利用を開	をパイル中の情報機関の定義と 打る気性を含して(ま)と、情報 が構えいするのそれがある。	PERCOLL.	・利子(おな)だよードは、デードの場合があいたは パードディスク/スツードを利用する。	RI-GARIE	#AT6.		A1127	
	木争に対し、争かできないのでれがある。			する。	35		P-EBST0	と、情報が施えいするおそれが ある。	removal (できる形態の実施されたネットワークサービスを利用 する。	外部へのグラウスに対してののグラキニタリングし で、必要所に口の傾的に登れてる。 ・他点質のボットワークは、VPN等の暗号がもしく(は) クセス制度が実施されるボットワークサービスを利用 する。	市部へのアウミエに対してののアキモニタンフし で、必要時に自動的に関係する。 ・地域ないのイントへのアウミスに自動的に進形する。 ・地域をロネッツーフに、1998年の報告をもんだり できる財産が実施されたネッツーフサービスを利用		And	
		ī										7.00	1		

重要インフラに対する対策

重要インフラのサイバーテロ対策に係る特別行動計画の概要

目的

いわゆるサイバーテロなど、情報通信ネットワークや情報システムを利用した、国民生活や社会経済活動に重大な影響を及ぼす可能性があるいかなる攻撃からも重要インフラを防護する。



身近なセキュリティの改善

- ◆ セキュリティの基礎の周知と意識の改革
 - ▶ テクノロジー、パスワードは絶対ではない
 - 一旦入ったら根こそぎ取られる
 - ・ 暗号化ソフトも必要
 - ▶ PCが故障したときの手順は決まってますか?
 - ▶ そうはいっても、パスワードは重要
 - パスワード教育は重要だが、あまりやられていない。