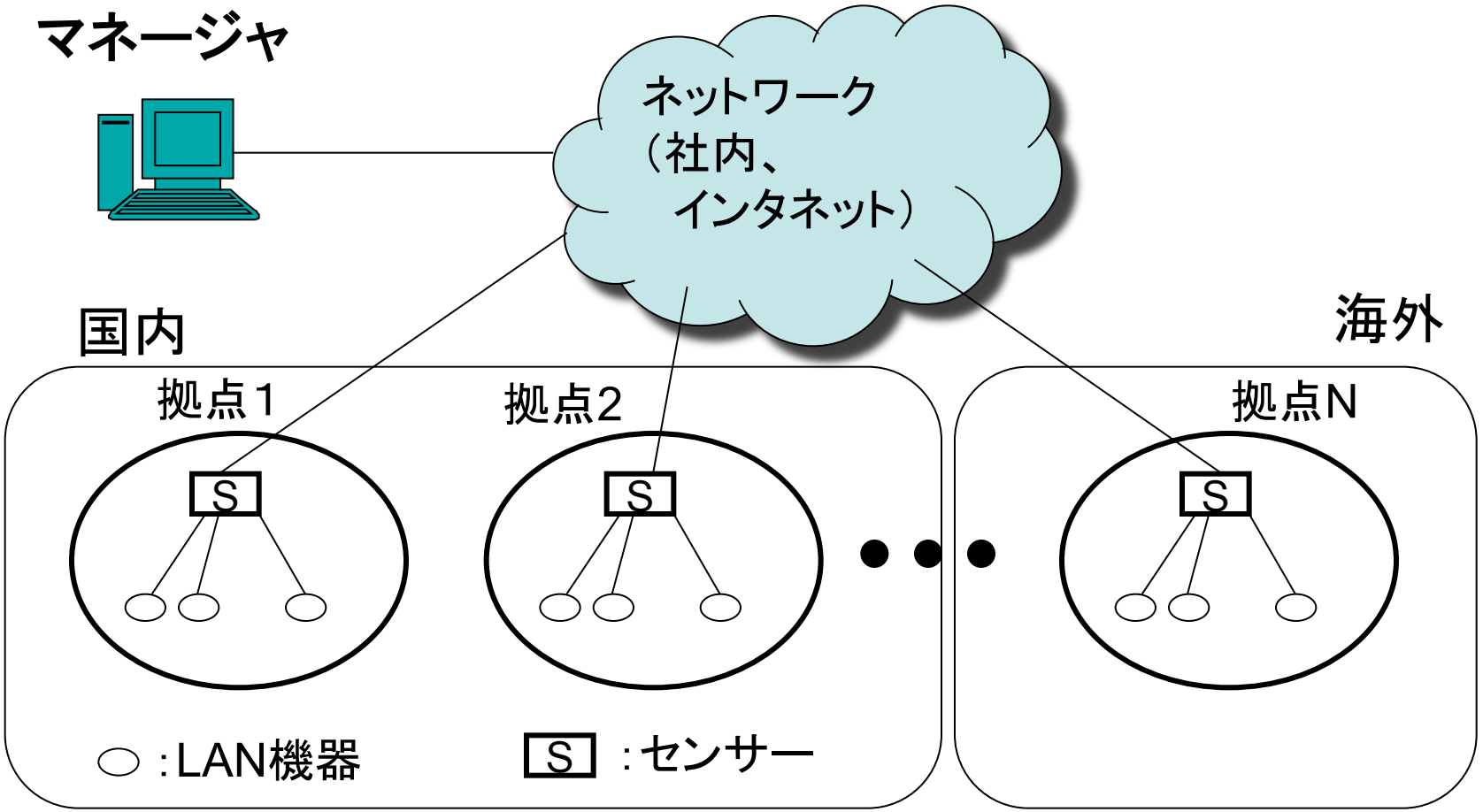
D-CaseによるLANアプリケーションのディペンダブル設計

2012年12月20日

株式会社　サイバー創研

LANアプリケーションの概要



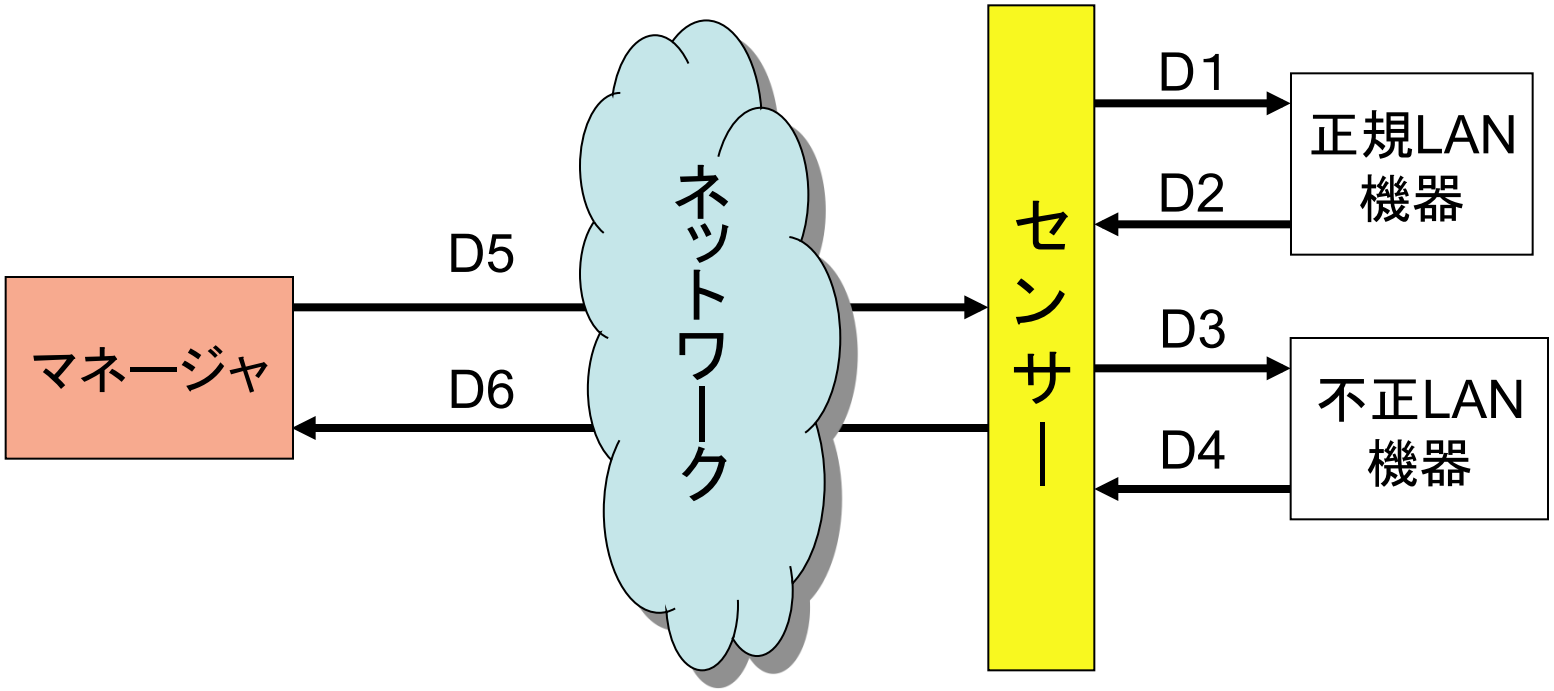
- 不正なLAN機器の検知と遮断
- センサーはユーザの各拠点（海外の拠点）に設置
- マネージャが管理できるセンサーの台数の上限は2000台
- センサーが管理できるLAN機器の台数の上限は1000台

LANアプリケーションの製品形態

	センサー	マネージャ
ハード	専用ハード（量産品）	推奨条件を満たす市販のWindows Server PC
ソフト	BIOS以外は独自に開発	Window用アプリケーションソフト
設置環境	ユーザの各拠点に設置されるが設置環境、設置環境に関する情報は、障害発生時に判明	ユーザのサーバールーム
運用時の状況	拠点では設置されていることさえ知らないケースが大半	SIあるいはユーザ企業の情報システムが常に状態監視

※センサーはユーザの海外拠点に持ち出されるケースもある

LANアプリケーションの構成



D1 , D2	①LAN機器が最初に送信するパケット　②名前取得
D3 , D4	①LAN機器が最初に送信するパケット　②遮断
D5 , D6	①センサーの状態確認　②センサー設定 ③更新版センサーソフト配信　④遮断テーブル更新

LANアプリケーションの品質責任

メーカはLANアプリケーションのセンサーとマネージャをSIに提供

センサー、マネージャ、マニュアル

SIはユーザ企業のネットワークに対してLANアプリケーションの構築と運用を提供

LANアプリケーションの品質責任

メーカはLANアプリケーションのセンサーとマネージャをSIに提供

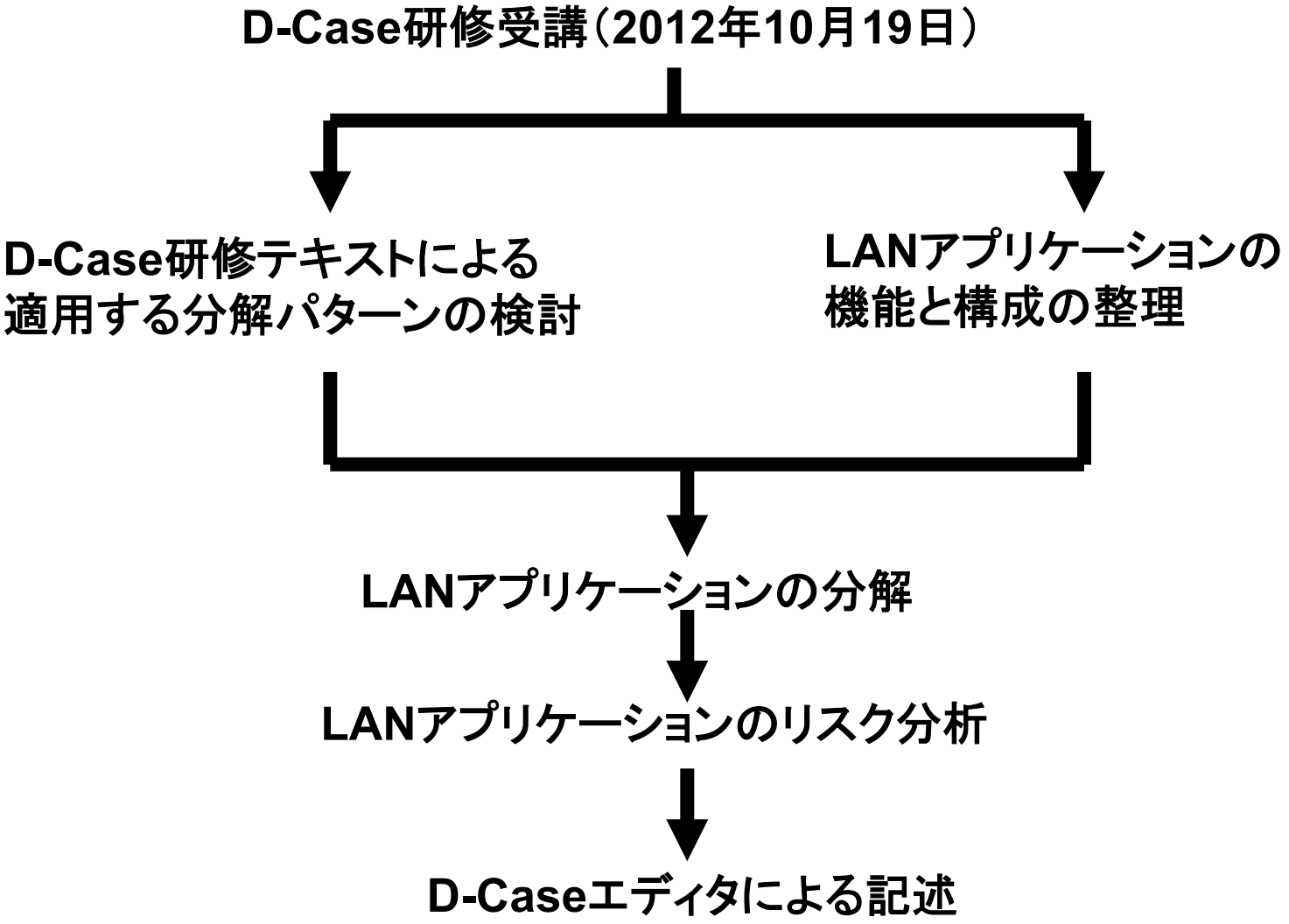
センサー、マネージャ、マニュアル

SIはユーザ企業のネットワークに対してLANアプリケーションの構築と運用を提供

- 各ユーザに導入したLANアプリケーションのシステムとしての品質責任はSI
- 障害が発生した場合には、障害の一次切り分けと対応はSIが担当する。
- 障害発生の原因がセンサーあるいはマネージャの品質に起因する場合には、メーカが責任を負う。

D-Caseによるディペンダブル設計（作業シーケンス）

研修受講前は、D-Caseに関する予備知識はほぼ皆無



分解パターンの選択

研修テキスト（D-Case入門）の121ページに記載されている
7種類の分解パターン

①システム分解　②機能分解　③属性分解　④機能分解
⑤完全分解　⑥単調分解　⑦具体分解

分解パターンの選択

研修テキスト（D-Case入門）の121ページに記載されている7種類の分解パターン

①システム分解　②機能分解　③属性分解　④機能分解
⑤完全分解　⑥単調分解　⑦具体分解

- ユーザのネットワークにLANアプリケーションを構築するのはSIである
- やりたいことは、LANアプリケーションという製品がディペンダブルであることを社内のレビュー者とSIに説明できるようにすることである
- LANアプリケーションのセンサーとマネージャは単独でも機能を実現できる1つのサブシステムとみなすことができる

分解パターンの選択

研修テキスト（D-Case入門）の121ページに記載されている7種類の分解パターン

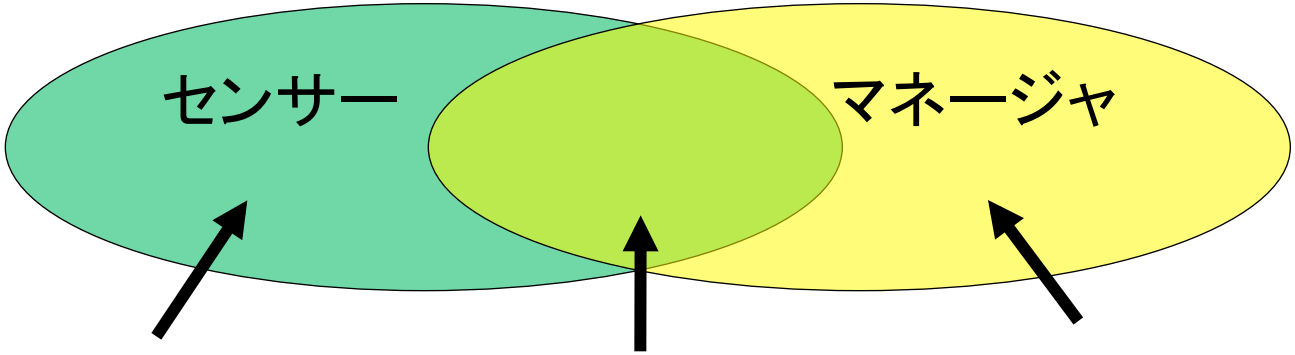
①システム分解　②機能分解　③属性分解　④機能分解
⑤完全分解　⑥単調分解　⑦具体分解

・ユーザのネットワークにLANアプリケーションを構築するのはSIである
・やりたいことは、LANアプリケーションという製品がディペンダブルであることを社内のレビュー者とSIに説明できるようにすることである
・LANアプリケーションのセンサーとマネージャは単独でも機能を実現できる1つのサブシステムとみなすことができる

今回はシステム分解を採用

システム分解によるLANアプリケーションのリスク分析

・LANアプリケーションはセンサーとマネージャで構成される
・センサーとマネージャは、単独で動作することができる
・障害が発生した場合の原因究明は、構成要素単位で行う



センサー単独で提供できる機能

センサーとマネージャの相互作用で提供できる機能

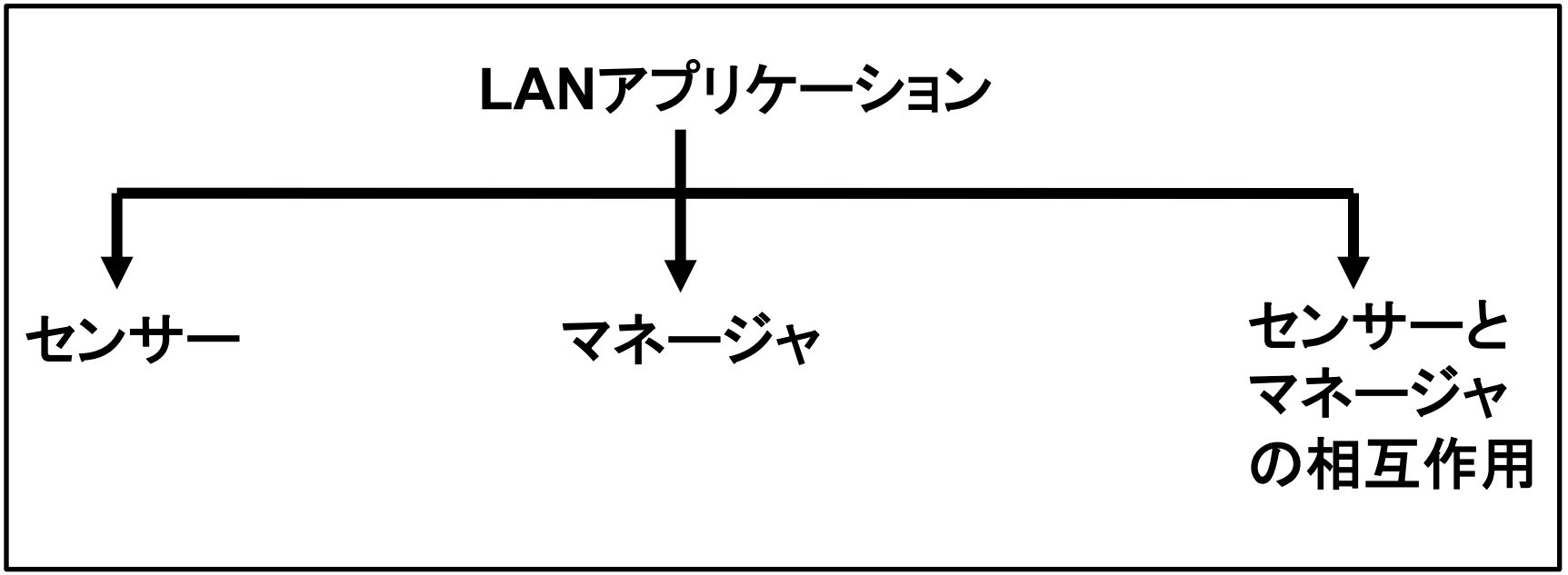
マネージャ単独で提供できる機能

今回はシステム分解を採用して、次の3つがディペンダブルであることを主張する。
①センサー　②マネージャ　③センサーとマネージャの相互作用

サブシステムで実現できる機能

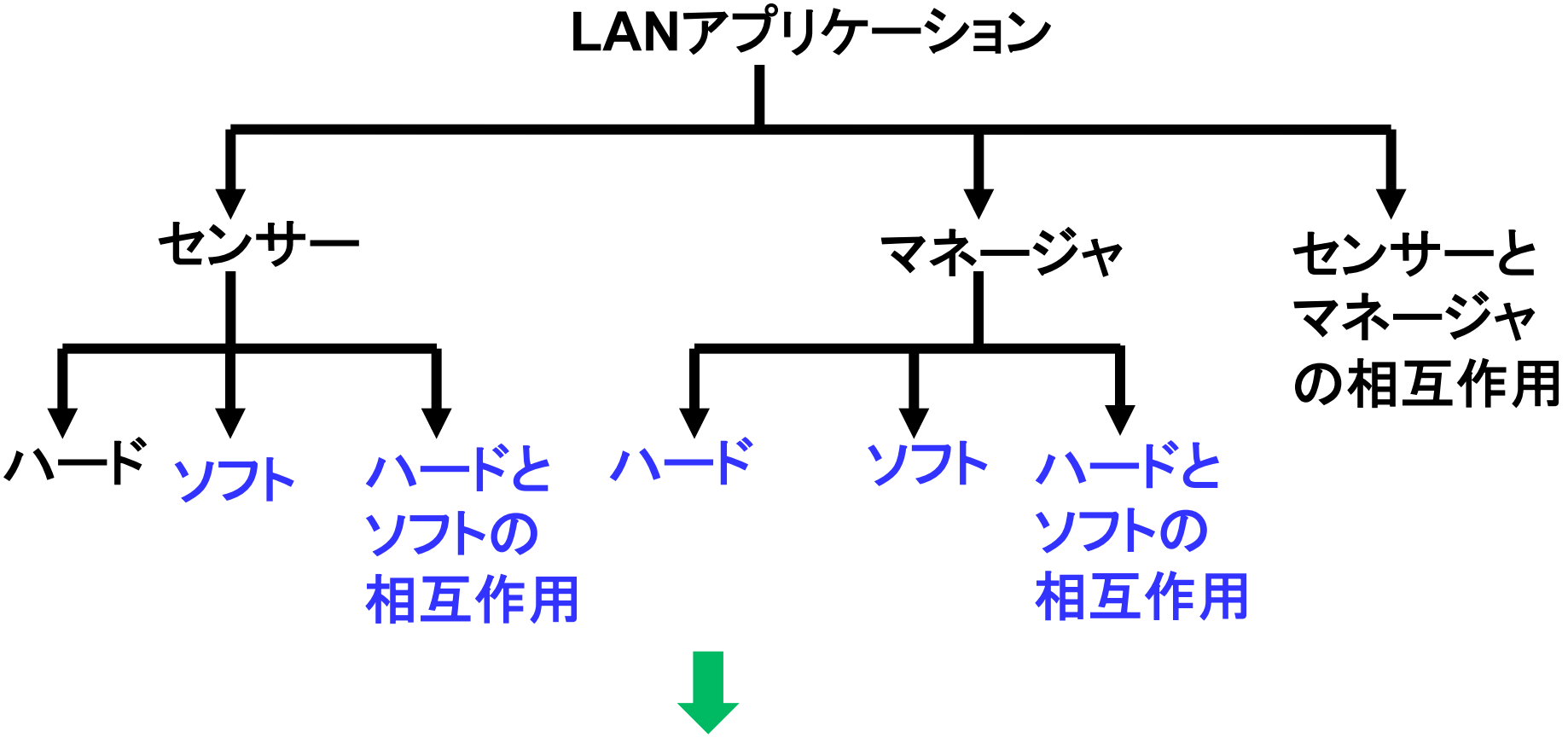
サブシステム	サブシステムで実現できる機能
センサー	・不正なLAN機器の検知と遮断 ・CPUの温度、CPU使用率、メモリ使用量を設定された時間間隔で2次記憶媒体に記録 ・CPUの温度による動作クロックの切替え ・ソフト処理での異常発生時の自動再起動 ・マネージャとネットワークで接続されている場合には、通信状態の監視
マネージャ	・センサーとの間の通信が切断される前にセンサーから収集した情報の編集と画面への表示 ・冗長化構成をしている場合には、設定された時間間隔で待機系マネージャとの情報交換 ・センサーとネットワークで接続されている場合には、通信状態の監視
センサーとマネージャの相互作用	・マネージャからセンサー更新版ソフト更新版遮断テーブルの配布 ・センサーからマネージャに未知のLAN機器を検出したことの通知 ・マネージャによるセンサーの状態確認

LANアプリケーションのシステム分解



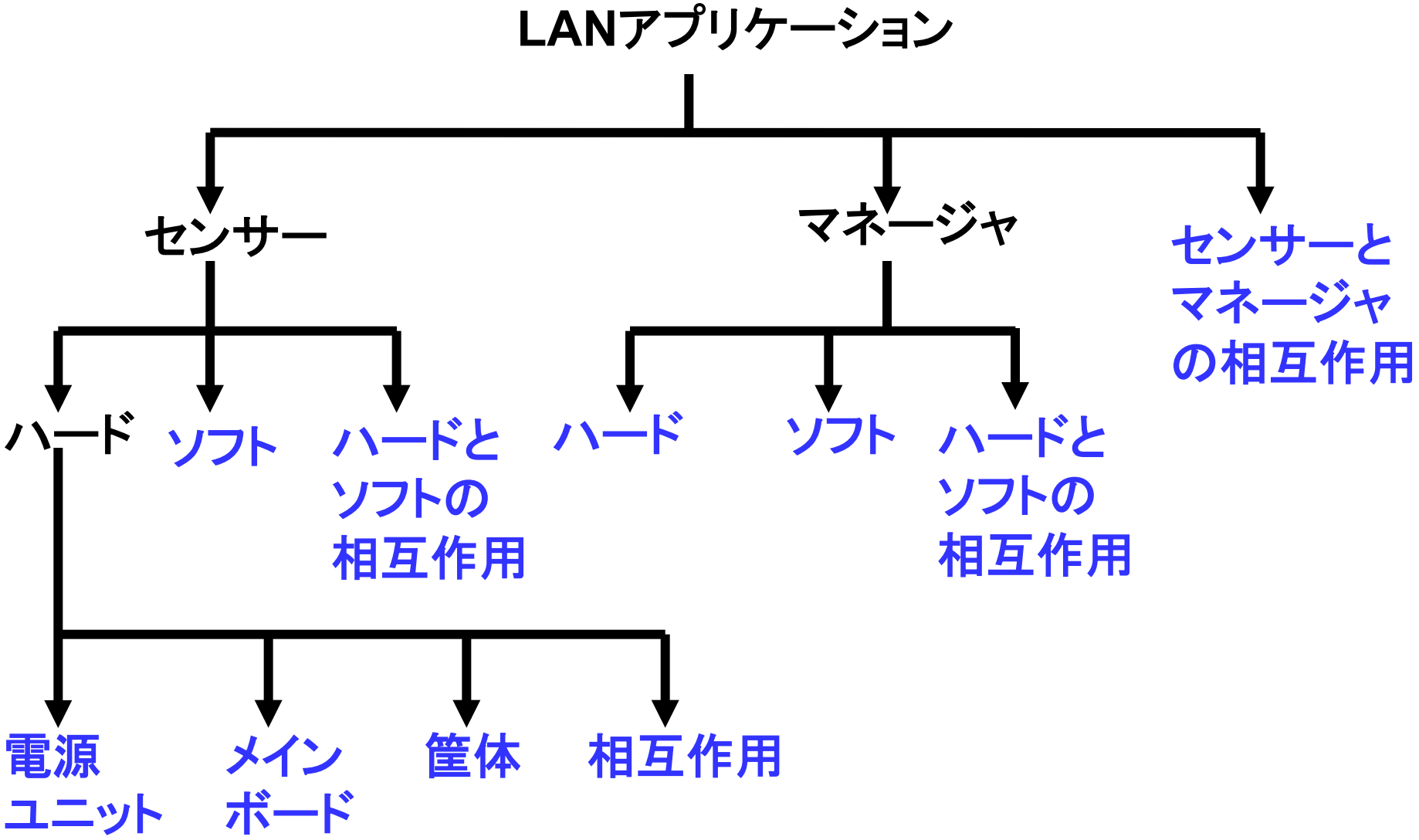
センサーとマネージャは、ハード、ソフト、ハードとソフト
の相互作用に分解する

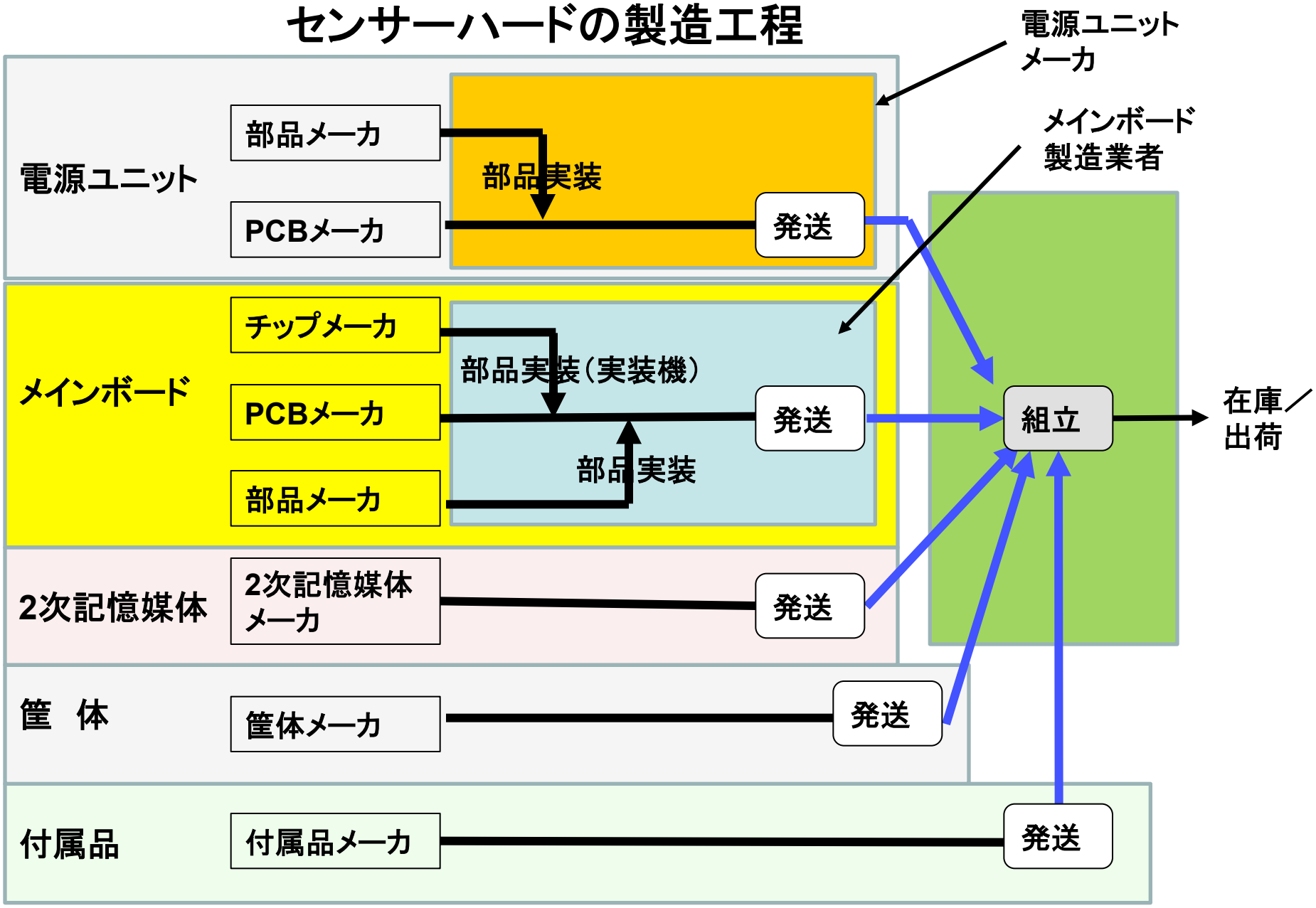
LANアプリケーションのシステム分解

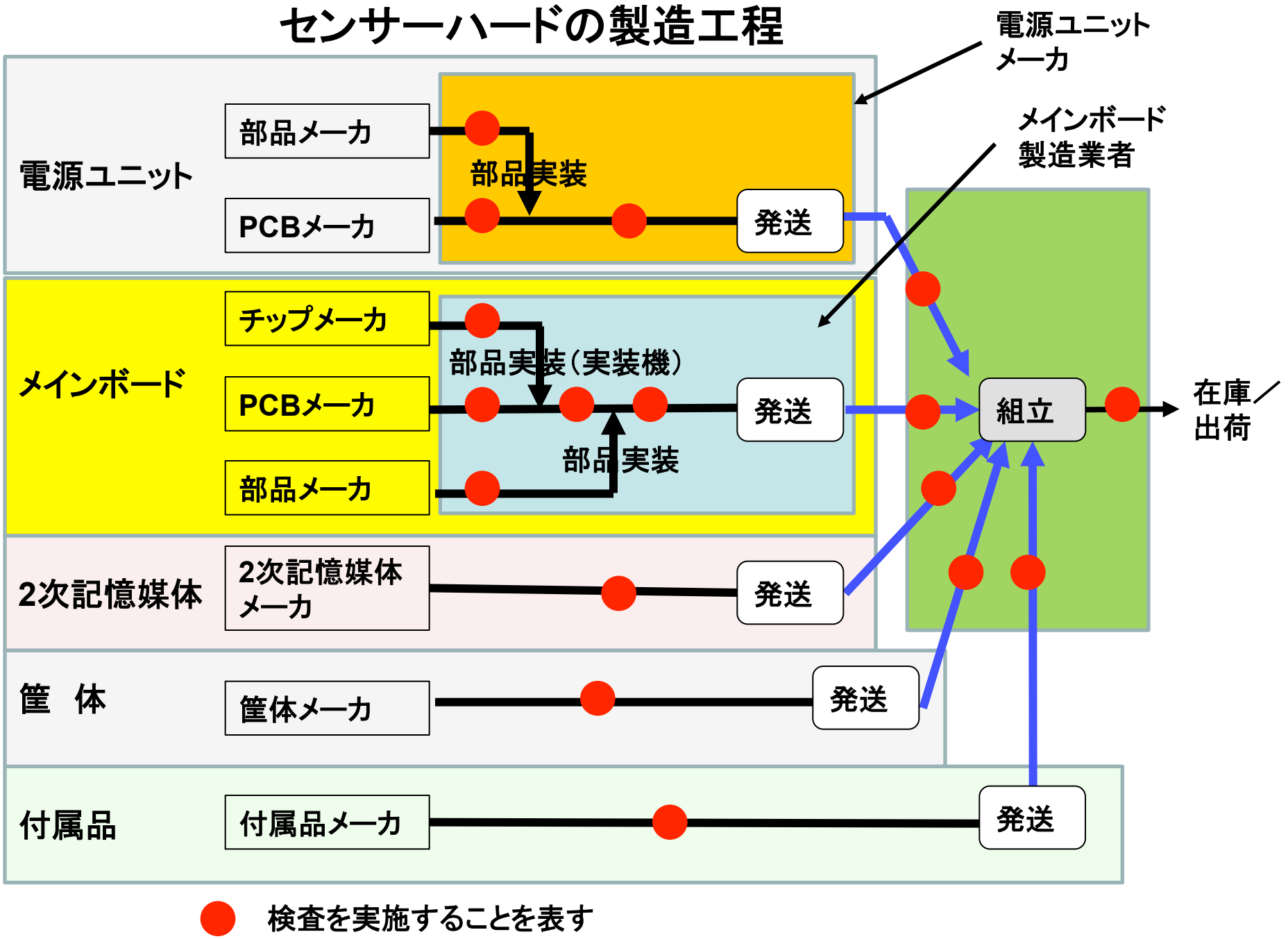


センサーハードは、さらに、電源ユニット、メインボード、
筐体、ハード間の相互作用に分解する

LANアプリケーションのシステム分解




センサーハードの製造工程
電源ユニット
メーカ
メインボード
製造業者
電源ユニット
部品メーカ
PCBメーカ
部品実装
発送
メインボード
チップメーカ
PCBメーカ
部品メーカ
部品実装（実装機）
部品実装
発送
組立
在庫／
出荷
2次記憶媒体
2次記憶媒体
メーカ
発送
筐　体
筐体メーカ
発送
付属品
付属品メーカ
発送


センサーハードの製造工程
電源ユニット
メーカ
メインボード
製造業者
電源ユニット
部品メーカ
部品実装
PCBメーカ
発送
メインボード
チップメーカ
部品実装（実装機）
PCBメーカ
発送
部品実装
部品メーカ
2次記憶媒体
2次記憶媒体
メーカ
発送
筐　体
筐体メーカ
発送
付属品
付属品メーカ
発送
組立
在庫／
出荷
検査を実施することを表す

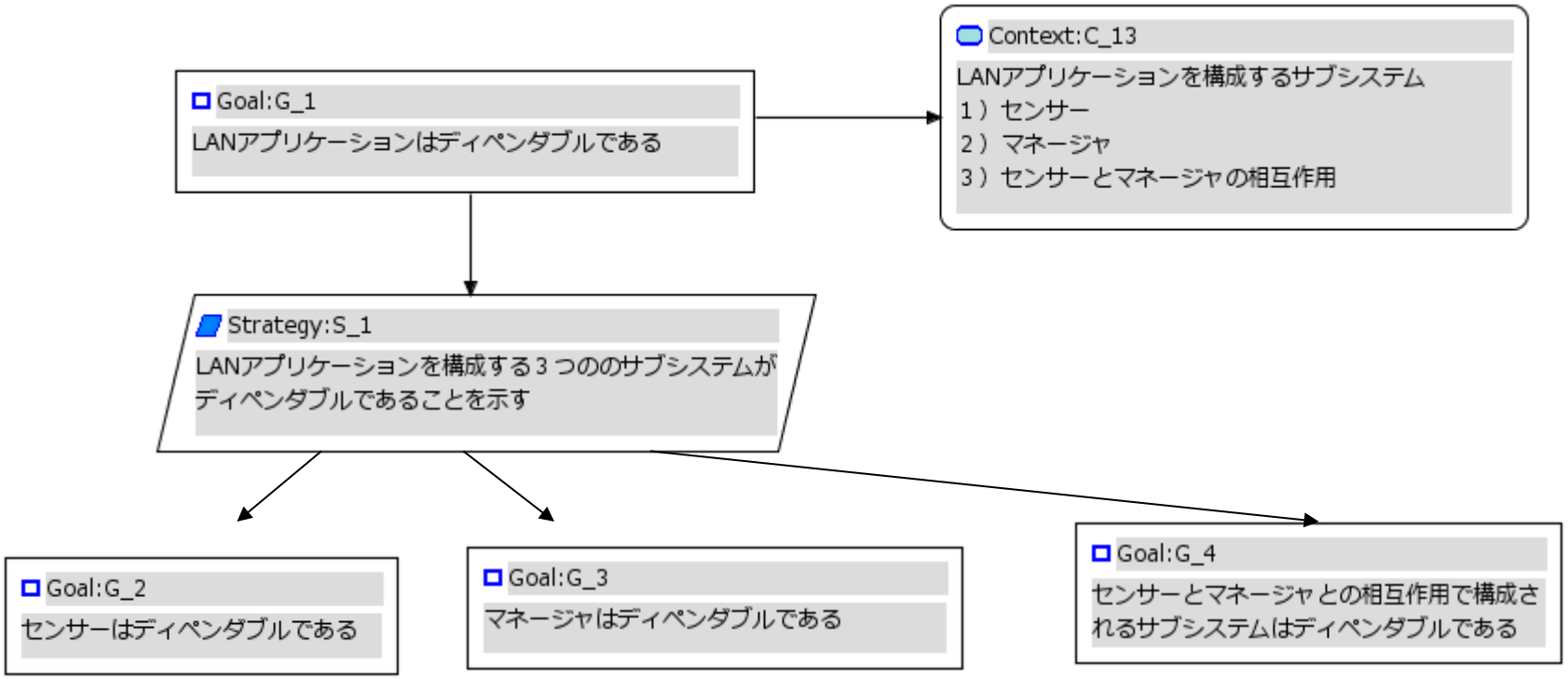
センサーハードの相互作用に関するリスク分析（一部）

	リスクを引き起こす要因	リスク	属性
1	CPUの放熱量に対する筐体の熱容量が小さい	CPU温度上昇による動作停止	信頼性
2	筐体表面からの放熱能力の能力不足	CPU温度上昇による動作停止	信頼性
3	電源ユニットやCPUと筐体の換気孔との位置のずれ	CPU温度上昇による動作停止	信頼性
4	電源ユニットのDC供給能力のマージンがメインボードの消費電力に対して小さい	メインボードの起動不能	信頼性
5	筐体の換気孔から金属片が混入する	ショートによる発火 電源ユニットの過電流の発生によるICの焼損	安全性

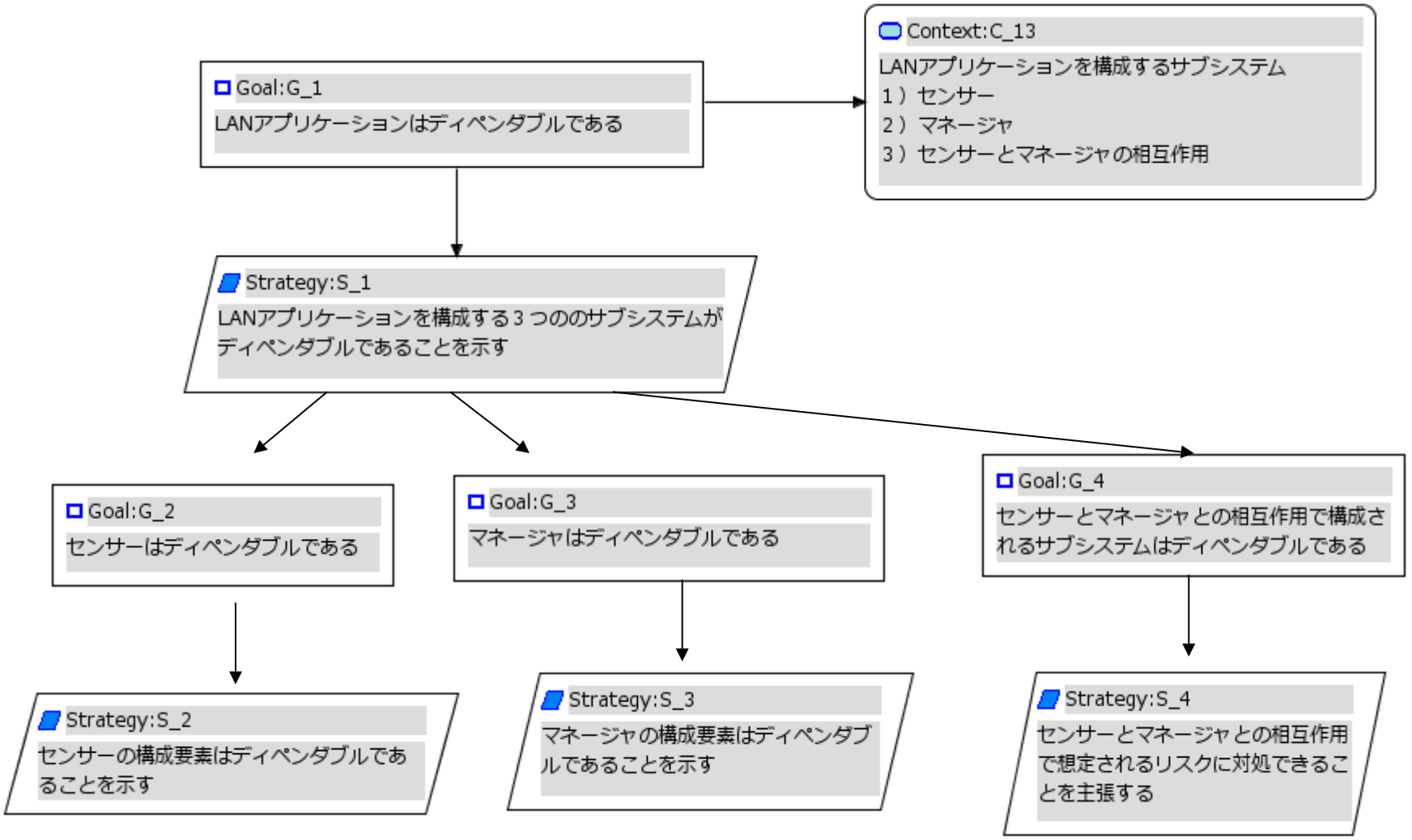
センサーハードとセンサーソフトの相互作用に関するリスク分析（一部）

	リスクを引き起こす要因	リスク	属性
1	PCIバス上でのデータエラーの発生	通信不能	信頼性
2	2次記憶媒体への高頻度のアクセスの長時間の継続	2次記憶媒体の損傷	信頼性
3	2次記憶媒体への書き込み制限回数を超えた書き込み	2次記憶媒体の損傷	信頼性
4	CPUの生産中止によるCPUの切替えによるCPUおよび周辺ICの変更に伴うドライバソフトの変更	従来は発生していなかった障害の発生	一貫性
5	2次記憶媒体のディスクフルの発生	センサー動作停止	信頼性

LANアプリケーションのD-Case展開（第1階層）



LANアプリケーションのD-Case展開（第1、2階層）



D-CaseによるLANアプリケーションのディペンダブル設計の記録（1／2）

作業工数

作業内容	作業時間
LANアプリケーションの機能と構成の概要の整理	5時間
分解パターンの選択（試行錯誤を含む）	30時間
LANアプリケーションのシステム分解	10時間
システム分解した各サブシステムのリスクの列挙と属性付与	62時間
D-Caseエディタでの記述	110時間
作業時間合計	217時間

システム分解した各サブシステムのリスクの列挙と属性付与に要した時間

	大分類	中分類	小分類	要した時間	リスクの数
1	センサー	ハード	電源ユニット	5時間	18
2			メインボード	6時間	19
3			筐　体	2時間	6
4			ハード相互作用	8時間	16
5		ソフト		10時間	25
6		ハードとソフトの相互作用		5時間	11
7	マネージャ	ハード		2時間	4
8		ソフト		8時間	18
9		ハードとソフトの相互作用		4時間	8
10	センサーとマネージャの相互作用			12時間	23
合　計				62時間	147

D-CaseによるLANアプリケーションのディペンダブル設計の記録（2／2）

	LANアプリケーション構成要素		Context	主張	戦略	証跡
1	センサー	電源ユニット	1(16)	83	30	71
2		メインボード	1(17)	60	21	42
3		筐　体	1(6)	20	7	13
4		ハード相互作用	1(16)	54	18	43
5		ソフト	1(25)	124	41	60
6		ハードとソフトの相互作用	1(11)	35	11	27
7	マネージャ	ハード	1(4)	13	4	10
8		ソフト	1(18)	56	18	38
9		ハードとソフトの相互作用	1(8)	24	8	16
10	センサーとマネージャの相互作用		1(23)	70	23	48
		合　計	10(144)	539	181	368

Contextの数
（　)内の数値はContextに記載されているハザードの個数である

リスク分析のメリットとデメリット

メリット

1）リスクとリスクを引き起こす要因について、関連付けができる

2）想定しているリスクを社内のレビュー者やSIに明確に説明できる

3）万が一、障害が発生した場合の原因解析に活用できる

リスク分析のメリットとデメリット

メリット

1）リスクとリスクを引き起こす要因について、関連付けができる

2）想定しているリスクを社内のレビュー者やSIに明確に説明できる

3）万が一、障害が発生した場合の原因解析に活用できる

デメリット

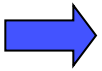
ごまかしがきかないので、リスクを想定できる能力がSIなどの外部にわかってしまう

リスク分析の障害発生時の原因解析への応用

センサーで発生した障害
センサーの動作停止

リスク分析の障害発生時の原因解析への応用

センサーで発生した障害
センサーの動作停止



センサーの停止を知る手段
マネージャがセンサーからレスポンスが返ってこないときに、マネージャの画面にセンサー停止と表示される

リスク分析の障害発生時の原因解析への応用

センサーで発生した障害
センサーの動作停止

センサーの停止を知る手段
マネージャがセンサーからレスポンスが返ってこないときに、マネージャの画面にセンサー停止と表示される

マネージャ画面の表示内容から想定される原因

センサーハード	センサーソフト
・電源ユニット ・メインボード ・2次記憶媒体	・無限ループ ・デッドロック ・ ・

リスク分析とD-Caseファイルの記載内容結果を活用

D-Case関するコメント

	項　目	説　　明
1	IPAの非機能要求グレードとのD-Caseで定義されている属性との関係	IPAの非機能要求グレードには可用性など同じ属性が使用されている。情報システムについては、D-Caseと非機能要求グレードとの関係を明確してほしい。
		IPAの非機能要求グレードでは、情報システムにインフラ性の強さに応じてグレードを設定しているので、D-Case設計でのリスク分析に活用できる可能性がある
2	リスク分析	リスクとリスクを引き起こす要因との関係を体系的に整理できる
		系統的にリスク分析を実施するので、従来の方法よりもリスク分析での検討漏れが少なくなることが期待できる。
		対象とする製品やシステムに関する知識や経験に依存せずに、体系的なリスク分析ができるようになると良い。

D-Caseエディタに関するコメント(1/2)

	項　目	説　　明
1	D-Caseエディタの利用者の拡大	D-Caseエディタはソフト開発環境上で作成されているので、ワードやエクセルのように誰でも使えるツールにすることが必要である。
2	D-Caseエディタで作成したファイルのレビュー	個々の流れを説明することはできるが、全体を見せることができないので、レビュー時の見せ方が難しい。
3	D-Caseエディタで作成したファイルの位置づけ	メーカが作成している各種の開発ドキュメントとの関係を明確にする必要がある ・D-Caseエディタで作成した資料の追加 ・従来のドキュメントの置き換え
4	仕様変更時の対応	エクセルやワードで作成したドキュメントでは色はフォントなどで変更部分が容易に区別できる。D-Caseエディタではどのような方法をありえるか。

D-Caseエディタに関するコメント(2/2)

	項　目	説　　明
5	サイズが大きなファイルの作業性	D-Caseエディタで作成する規模が大きくなると、特定の箇所を見つけるのに苦労する。
6	D-Caseエディタの継続性	D-Caseエディタはソフト開発環境の上で作成されているが、普及させるには永続的にメンテナンスを継続させる仕組みが必要である。 紙での印刷を想定されていないため、 D-Caseエディタの維持環境の維持運営がしっかりしないと普及は難しい。
7	接続できるノードの制限	D-Caseエディタはあまりにも接続が自由であり、どのノードとも接続できる。論理的に接続できるはずのないノードは色を薄くするか表示されないなど、改善が必要である。
8	メニューの不要な項目	ProjectやRunで表示される項目がD-Caseエディタの使用時に不要であれば、削除すべきである。