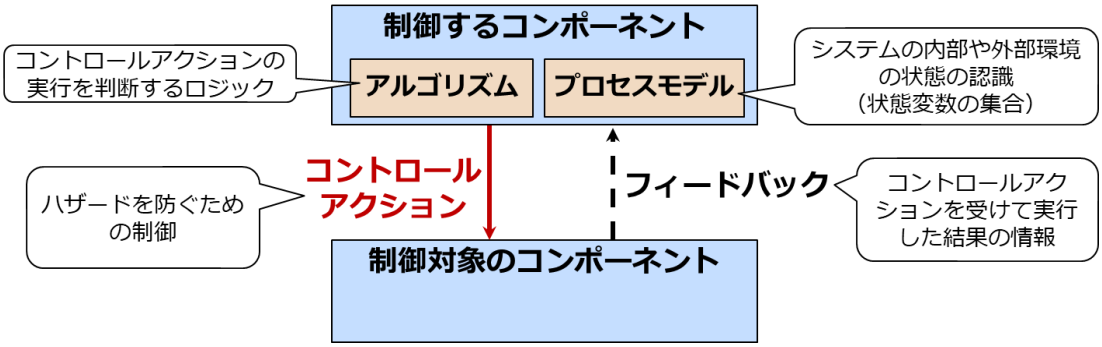
タイトル：コントロールストラクチャー（CS 図）は物理モデルではない

STAMP におけるコントロールストラクチャーとは何か？
MIT が発行して公開している STPA Handbook では次のように定義している。
（https://psas.scripts.mit.edu/home/get_file2.php?name=STPA_Handbook_Japanese.pdf　p.23）

> *階層的なコントロールストラクチャーは、フィードバックコントロールループで構成されたシステムモデルである。有効なコントロールストラクチャーは、システム全体の動作に制約を強制する。*

この定義文言は、STAMP を理解している人が読めば秀逸と感じるが、STAMP を学び始めたばかりの人にとっては本意を理解し難いかもしれない。「システムをモデル化するということね」としか伝わらない可能性があり、そして、いざ実践しようというときに勘違いするケースがとても多い。本文書では代表的な勘違い例を示し、勘違いしたまま先の分析ステップに進んで混乱・苦労・徒労が無いように早めに気付きを与えることが本文書の目的である。正しいコントロールストラクチャー図（CS 図）を描くにはどうすれば良いかという解説は他の文書に譲る。

下図がハザードを防ぐ（安全制約を守る）ために**誰が、何を、どう制御しているか**を描く**STAMP の基本モデル**である。



上記を言葉では理解したつもりでも、いざ CS 図を描いてみると勘違いしていることがとても多い。特に、対象システムに精通した技術者であればあるほど、陥り易い勘違いがある。その勘違いをしないように STPA Handbook では次のように助言を付している。

STPA Handbook　p.26

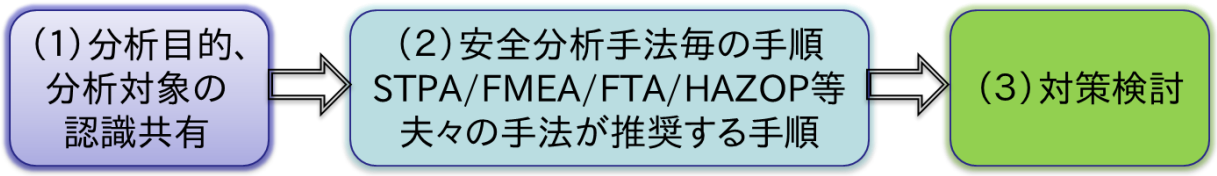
◆ コントロールストラクチャーは**物理モデルではない**。
STPA に使用される階層コントロールストラクチャーは、物理ブロック図、概略図、又は配管及び計装図のような物理モデルではない。
（筆者注釈）例えば、ハードウェア構成図は典型的な物理モデルである。

◆ コントロールストラクチャーは**実行可能なモデルではない**。
コントロールストラクチャーは、実行可能なモデルやシミュレーションモデルではない。
（筆者注釈）システム機能の実行に必須であっても、今着目しているハザードに直接関与しないならば、省略しても良い。また、実装依存の構成部分は、一般的には抽象化した方が良い。

◆ コントロールストラクチャーは**機能モデルである**。
コンポーネントおよびその接続は物理的な性質のものではなく、対象システムの機能的なコントロールストラクチャーをモデル化する。

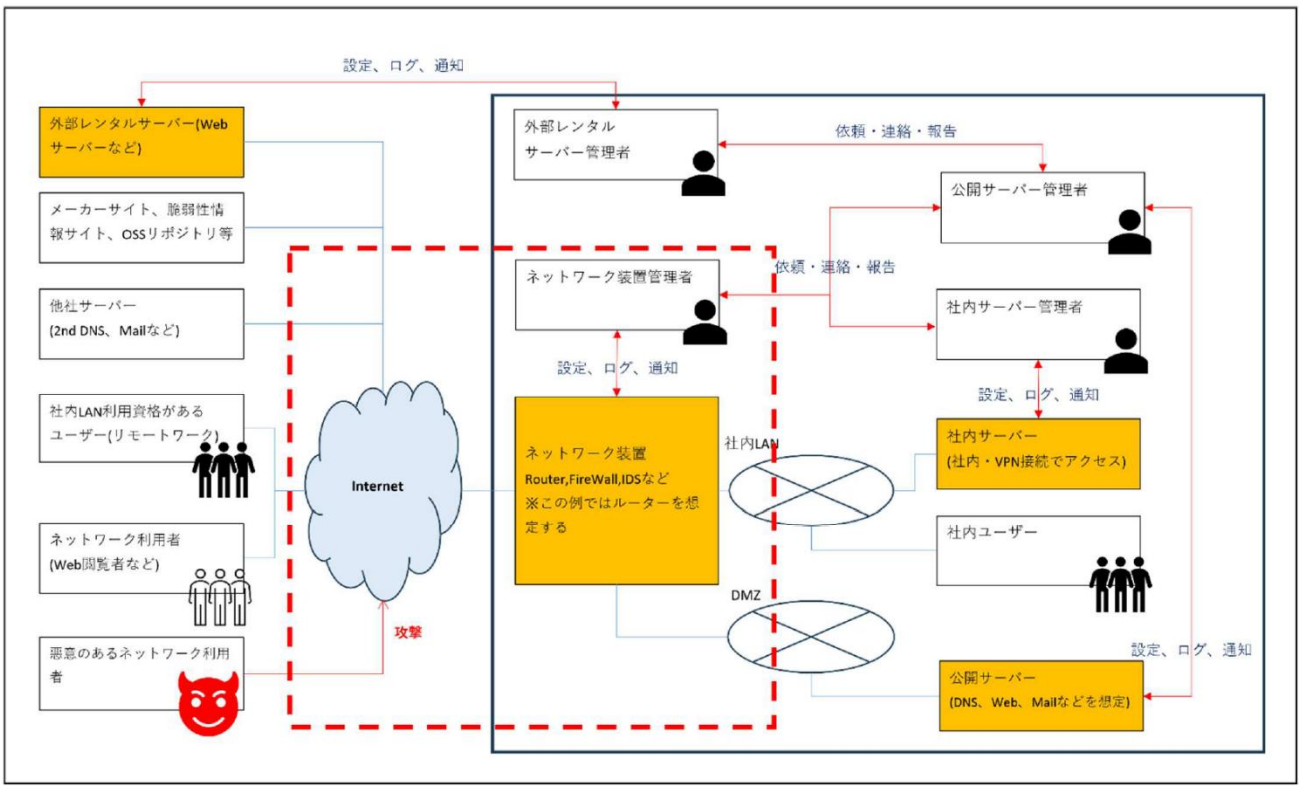
更に筆者は下記も助言として付け加えたい。

◆ CS 図は**システム仕様全てを実現するため**の機能モデルではない。
CS 図は対象となるアクシデント／**ハザードを防ぐため**の機能モデルである。
安全分析するには最初（下図、安全分析の一般的手順の(1)）に対象システムの概要をステークホルダー間で共通認識する必要がある。そのときにはシステムの概念図や、場合によってはサブシステムを組み合わせた（機能）ブロック図、システム構成図を用いることが多い。そのシステム構成図やブロック図は、システム仕様を実現させるための機能ブロック図であるが、そのブロック図をそのまま CS 図として使ってしまう、という勘違いがとても多い。



初めから CS 図が詳細で複雑になるのは、この勘違いによる場合が多い。

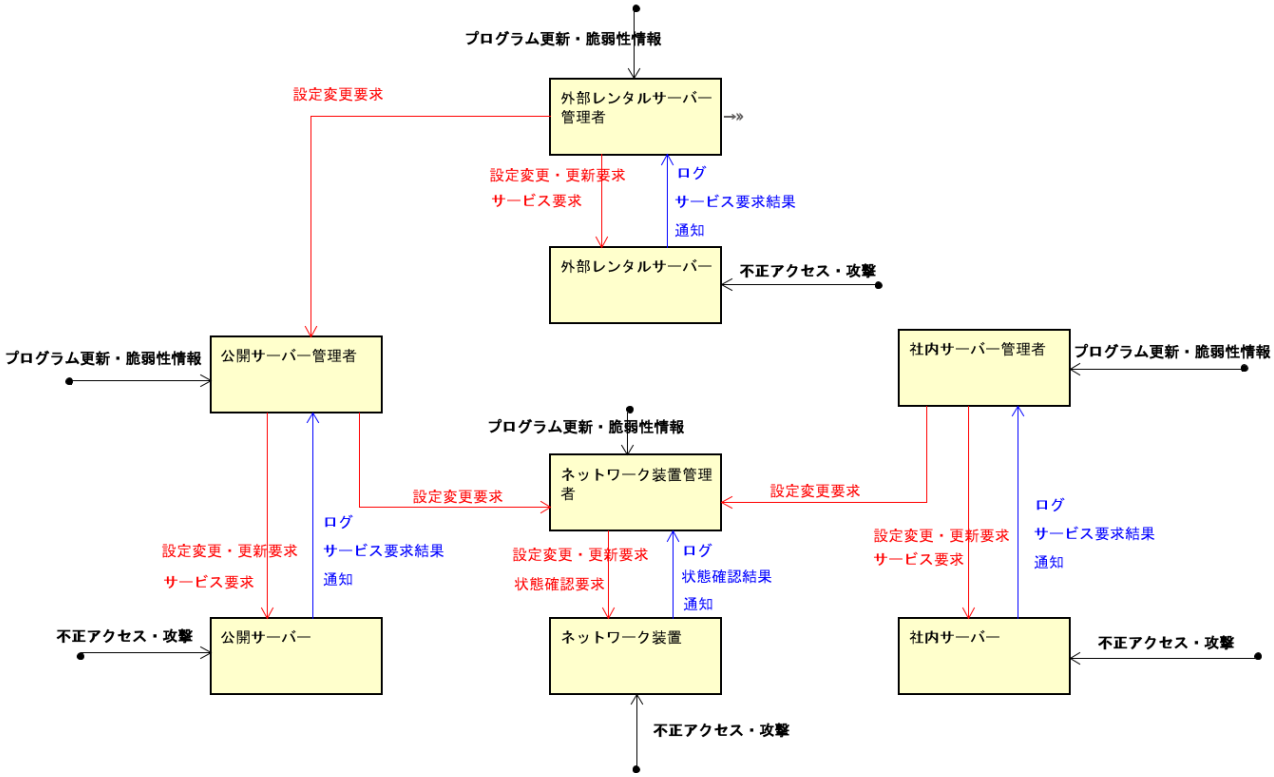
以下に例を示す。下図は、一般的な企業の小規模ネットワークを分析対象として、ステークホルダー間でシステム概要の認識を共有するために作成したシステム構成図（ポンチ絵レベルの概念図）である。システム概要を理解するにはポンチ絵がとても有益である。しかし、これがそのまま CS 図になる訳ではない点にも注意されたい。



●システム仕様を実現するためのシステム構成図をそのまま CS 図として使った、**誤った CS 図**の例。

下図は、分析目的と分析対象が明確になっていない（＝　分析するアクシデント／ハザードを特定できていない、今、関心のあるシステム境界を絞り切れていない）ときに陥り易い CS 図作成の勘違い例である。上記システム構成図の黒枠で囲った社内ネットワークシステムのコンポーネントを全て CS 図に組み込んで、配置を変えただけのモデルになっている。システム構成図をそのまま CS 図として描いてしまう、という典型的な勘違いである。

この勘違いの主原因は、分析しようとしている（つまり、ステークホルダーが最も関心を寄せている）アクシデント／ハザードを特定（絞り込み）できていないことであろう。

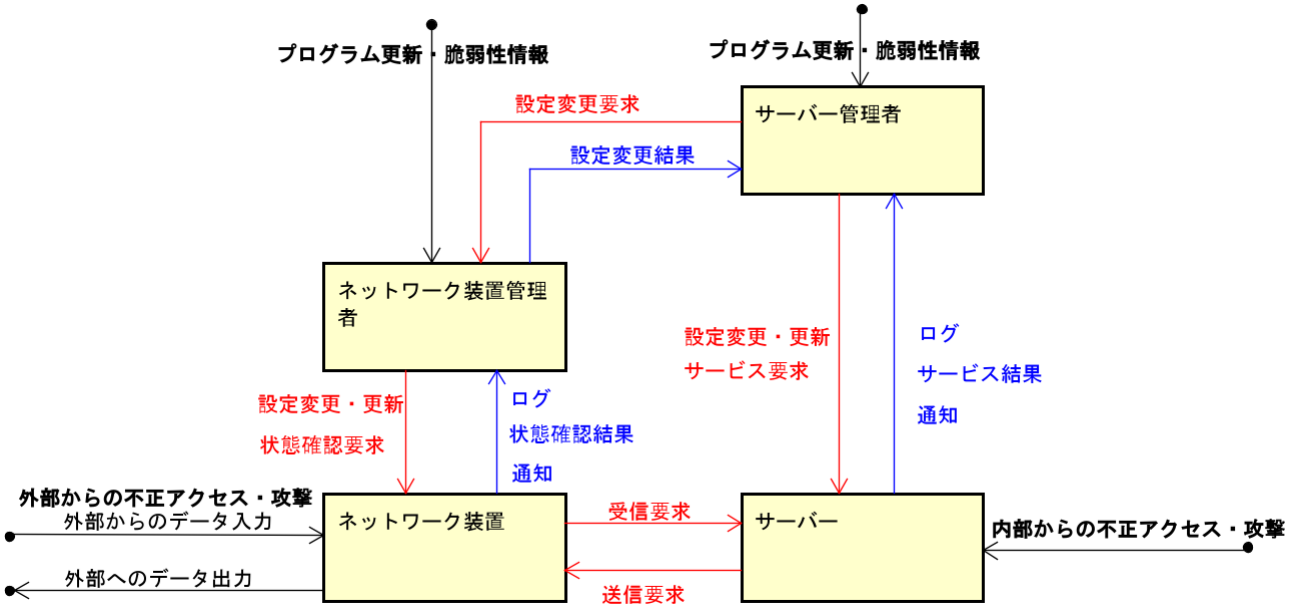


●ステークホルダーが関心を持つアクシデント／ハザードにフォーカスした**正しい CS 図**の例。

社内システムにおける『ネットワーク装置に関連するアクシデント／ハザードについて安全分析する』ことをステークホルダー間で認識共有した場合には、下図のような CS 図が正しい CS 図の一例である。

これから分析しようとするアクシデント／ハザードが絞り込めていれば、直接関与しない構成部分を省略したり、抽象化したりして、関心事の分析のみに集中できるようになる。例えば、下図では外部レンタルサーバーを省略しているし、社内サーバーと公開サーバーは抽象化して一つのサーバーとしている。

この例では、アクシデントを「システム利用者にサービスを提供できない」として、そのハザードを「社内システム機器間で設定変更が不徹底・不一致である」、「社内システムに既知脆弱性未対応の機器が有る」、「社内システム機器の設定変更に誤りがある」と定義した。そのため、直接制御できない外部レンタルサーバーは分析対象の範囲外であり、社内サーバーと公開サーバーは区別する必要がない。または、外部レンタルサーバーも直接制御できるならば、「サーバー」として一括りにして良い。



（2025/7/22　石井 正悟）