ネットワーク装置の安全分析　レビュー記録

2025/7/22 作成

■安全分析の経緯

STAMP/STPA を学び、規模の大きくない安全分析をトライしてみることになったため、テーマとして一般的な中小企業のネットワーク管理に関する安全分析を行ってみようと考えました。実施してみると想像していたよりも分析する内容が広がりすぎてしまい、簡単には分析が終わらないことに気が付きました。

このためネットワークの構成要素の一部であるネットワーク装置（ここではルーターを想定している）とネットワーク装置管理者の間の安全分析に範囲を狭めて安全分析を実施し、STAMP Workbench を用いて「broadbandrouter.stmp」を作成しました。

この分析結果に対し、有識者にレビューをいただき分析方針を検討したので、その内容を要約します。

■レビュー内容の要約

有識者	作成したネットワーク装置の安全分析ではハザードとアクシデントの定義に課題がある事を指摘。 • STAMP/STPA 解析のアクシデント定義を再整理中。 • 9 件のアクシデントを提示し、以下のように分類・再定義を提案： o 通信停止系（A1, A3, A4）→「ネットワーク装置が誤動作しインターネット接続が停止する」に集約。 o VPN 利用不可（A5）→ 致命的損失ではないため除外。 o 不正アクセス（A2, A6）→ 「情報漏洩」に一本化。 o 脆弱性（A7）→ 原因でありアクシデントではないため除外。 o 動作ログ保存失敗（A8）・通知失敗（A9）→ 対策でありアクシデントではないため除外。
安全分析者	o 新規アクシデント案：「DDoS 攻撃の踏み台として利用される」 • 「ユーザー」と「管理者」の違いが曖昧であると指摘。 • サービス内容の具体化が必要。
有識者	• セキュリティ問題は STPA 教材からは除外すべきと助言。 「ユーザー」と「管理者」の損失の違いについて説明。 o ユーザーの損失：ネットワークの可用性低下による業務停止。 o 管理者の損失：情報漏洩、サービス停止、DDoS 攻撃への加担など。 • 損失の影響範囲は、どちらの損失も会社の業務遅延や信用毀損につながると認識。 • 復旧時間について、短時間でも頻繁に発生すれば問題になるため、アクシデントの定義に時間の長短は含めない方針を表明。
安全分析者	• STPA 教材としてはセキュリティ問題を除外すべきとの意見を受け、社内で今後の方針を検討する意向。 • 「ネットワークの可用性が低下する」では損失が曖昧。 • 例：「メールが届かず受注を逃す」など、具体的な損失を挙げるべき。
有識者	• STPA では複数の損失を同時に扱うと混乱するため、1 つに絞って分析すべきと助言。 • セキュリティ分野への STPA 適用は実験的な試みであると説明。 • 「インターネット接続が停止する」こと自体がアクシデントと考えていたが、損失の具体化の必要性を認識。
安全分析者	• IPA の例（踏切事故）を引き合いに出し、アクシデントの粒度について再考。

- 「損失」の定義が曖昧であると指摘。
- 例：有料セミナーの中止は具体的な損失になる。
- 「本当に大事な損失を防ぐ」という視点が重要で STPA の本質であり「イベント」ではなく「損失」から出発すべき。

有識者
- STAMP のパラダイムシフト（信頼性→安全制御）を強調。
- STPA HANDBOOK と「はじめての STAMP/STPA」を参照し、損失の定義の重要性を再確認。

安全分析者
- 「インターネット接続が長時間停止し業務が止まる」という損失表現を提案。
- 「イベント」や「状態」よりも、「損失とは何か」を明確にすることが重要。
- ハザードは「損失に至る前の兆候」として捉えると理解しやすく、損失を具体的に定義することで、原因やシナリオ、制御構造図の設計がしやすくなる。
- 「インターネット接続が長時間停止し業務が止まる」で、どのような業務がどの程度止まるとどんな損失が出るか、具体例を挙げて考えることが大切。
- 「長時間の停止を防ぐ」だけでは一般的な対策しか導けない。より具体的な損失を想定することで、より実効性のある対策が導き出せる。

有識者
- 業務停止による具体的な影響を列挙（メール、会議、ファイル共有、警備システムなど）。

安全分析者
- それに伴う損失（商談機会の喪失、賠償、信用失墜、盗難被害拡大）を提示。
- 「インターネット接続が長時間停止し、商談の機会を失った」などの損失定義は抽象的で、具体的な業務形態が示されていないため理解しづらい。
- 「契約している警備システムの遠隔監視・緊急対処サービスが使用できなくなる」などは、盗難という損失が明確で理解しやすい。このような損失定義により具体的な対策が導き出せる。
- 損失を明確にすることで、ネットワークシステム以外の業務全体に関わる対策も検討可能になる。商談、賠償、信用などの損失も、具体的なビジネス文脈で考える必要がある。
- この議論は STPA の導入段階として非常に重要であり、有意義で面白い議論になっているとの評価。教育用コンテンツとしての整理の重要性を指摘。

有識者
- 分析範囲を「ルーターとルーター管理者」に限定する方針に立ち返ることを説明。
- 分析の目的と損失の定義の整合性について再確認し、分析範囲外の損失は除外したいと表明。
- 上司からの「インターネット接続維持」の指示に対し、管理ミスで長時間接続が切断された場合は「ミッション失敗」として損失としたい。
- 分析範囲が狭いため、得られる対策が一般的なものにとどまる可能性があるが、それでも試験的な分析として成立させたい。

安全分析者
- ルーター管理の失敗を例に、分析の出発点として損失を明確に定義することが重要。
- 損失を防ぐための制御構造図とコントロールアクション(CA)の設計を優先し、ハザードや安全制約はあとから考えてもよいと助言。
- CA が失敗した場合に、どのような損失が発生するかを考えることが、分析の本質である。
- 分析の継続を激励。

有識者
- UCA 分析と並行して、システムと関係者を含む「ポンチ絵」の作成を提案。
- ポンチ絵の作成を了承。

安全分析者
- 分析の進捗があれば再度共有する旨を伝える。

■レビュー時の議論内容の主な論点と学び

論点	内容
損失の定義	「インターネット停止」ではなく、それによって生じる「商談機会の喪失」「信用失墜」などを明確にする必要がある。
アクシデントの整理	原因と結果を混同せず、アクシデントは「防ぎたい損失」に焦点を当てる。
分析範囲の明確化	分析対象を「ルーターとその管理者」に限定し、範囲外の損失は除外。
教育的価値	STAMP の考え方（安全制御）を伝える教材として、損失の具体化と論理的思考が重要。

■有識者が指摘する要点

有識者が最も重要だと考えているのは、**「損失を具体的に定義すること」**でした。

●その理由と背景

有識者は一貫して、STAMP/STPA 解析において「イベント」や「状態」ではなく、「損失」に焦点を当てるべきだと強調しています。

1. **損失を明確に定義することで、制御構造や対策が導きやすくなる**
    - 例:「インターネット接続が停止する」ではなく、「商談の機会を失う」「顧客の信用を失う」など、**業務やビジネスに直結する損失**を明示することが重要。
2. **抽象的な損失ではなく、具体的な業務やサービスに基づいた損失を考える**
    - たとえば、Teams やメール、IP 電話などの停止がどのような影響を及ぼすかを具体的に想定することで、**現実的なリスクと対策**が見えてくる。
3. **「安全を制御する」という STAMP の考え方へのパラダイムシフト**
    - 従来の「信頼性を向上させる」ではなく、「本当に防ぐべき損失は何か」を起点に考えることが、STAMP の本質であると指摘しています。

●代表的な発言からの引用（要約）

「損失を具体的に定義すれば、その原因から損失に至るシナリオも考えやすくなりますし、損失を防ぐための制御構造図も考えやすくなると思います。」

「『ネットワークの停止を防止する』という従来の分析目標から、『本当に大事な損失を防ぐ』というパラダイムシフトが必要です。」

●結論

有識者が最も重視しているのは、**「損失の具体化を通じて、現実的かつ有効な安全対策を導くこと」**です。これは STAMP/STPA の教育的意義にもつながると考えています。