一般財団法人 日本科学技術連盟
第39年度(2023年度)ソフトウェア品質管理研究会成果発表会
演習コースⅣセーフティ＆セキュリティ
2024年 3月 8日(金)

Webシステムのセキュリティ要件分析、および機器撤去作業時のリスク抽出事例の報告

「演習コースⅣ：セーフティ＆セキュリティ」活動報告

メンバー
安樂 啓之（インフォテック）
杜 馨瓏（コニカミノルタ）
水野 浩之（東芝）
草彅 明彦（ダイニチ工業）
伊達 大輝（オムロン）
倉田 優輝
(日立ソリューションズ・クリエイト)
堤 智也（TIS）
浜田 泰之（TIS）
大谷 雅和（デンソークリエイト）

主 査 金子 朋子 （創価大学）
副 主 査 髙橋 雄志 （日本AIシステムサービス）
アドバイザー 佐々木 良一（東京電機大学）

今日ご説明する内容

- **「演習コースⅣ：セーフティ＆セキュリティ」活動概要**
- **分析事例のご紹介**
  - STAMP/STPAについての概要説明
  - 事例１
    Webシステムのセキュリティ要件分析
  - 事例２
    ネットワーク機器撤去時の作業リスク抽出
- **各メンバー、及び分析事例のご紹介**

「演習コースⅣ：セーフティ＆セキュリティ」活動概要

2023/5　6　7　8　9　10

セキュリティ分析手法についての学習

★セーフティ＆セキュリティ
統合アプローチSTAMPの
安全分析手法STPA

★事故分析手法CAST

ソフトウェア品質
シンポジウム

★各種分析手法と標準STAMPS&S
機械学習システムと安全、
セキュリティ・バイ・デザイン

レジリエンスエンジニアリング★
とFRAM

机上での学びだけでは身につかない経験を身につけるために各人が取り組み

各人の利用・評価

「演習コースⅣ：セーフティ＆セキュリティ」活動概要

2023/11	12	2024/1	2	3

セキュリティ分析手法についての学習

★AIとセキュリティ

AI/IoTシステム安全性シンポジウム
STAMP/FRAMワークショップ

3日間にわたってSTAMP/STPA, CAST, FRAM等の事例発表などがありました。

メンバーで持ち寄った分析などの結果を共有し、活動報告内容を検討

★各人の利用評価の共有（コンペ）

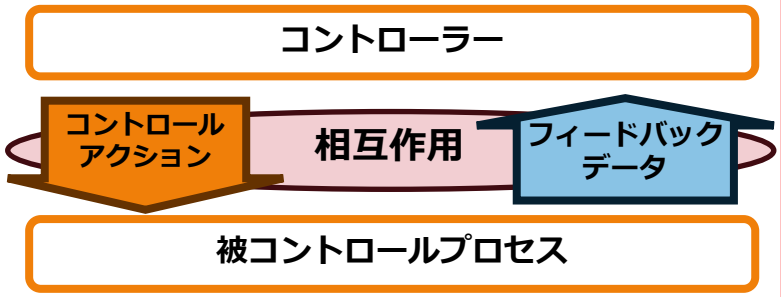
活動報告

各人の利用・評価 → 報告のまとめなど

本コースの学習内容（概要）

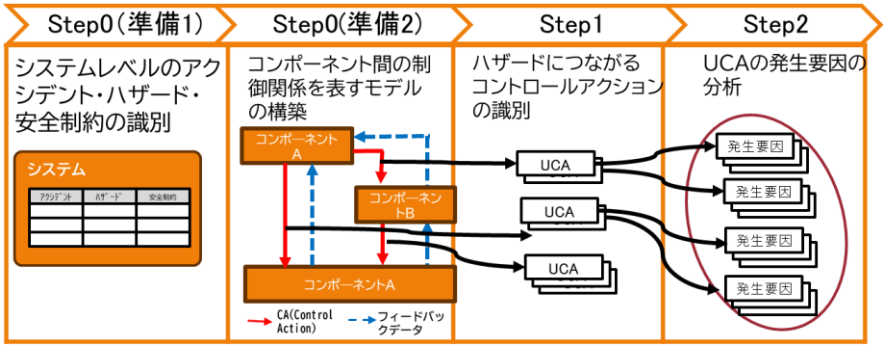
STAMP

「制御要素（コントローラー）」と「被制御要素（被コントロールプロセス）」の「相互作用」に着目したメカニズム



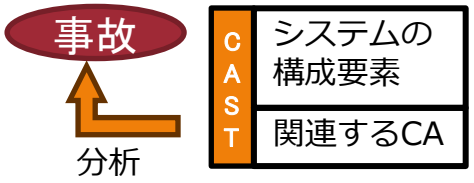
STPA

STAMP アクシデントモデルを前提として、システムのハザード要因を分析する新しい安全解析手法



CAST

STAMP事故モデルの考え方に基づいた事後分析手法

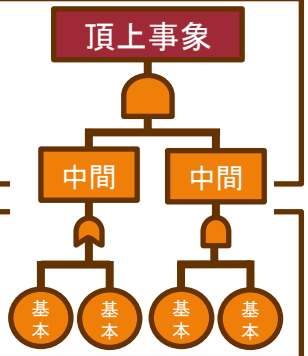


FTA

頂上事象の発生頻度分析のために故障原因を論理的にたどる手法

ATA

FTAと同様の木形式で攻撃手段を論理的にたどる手法

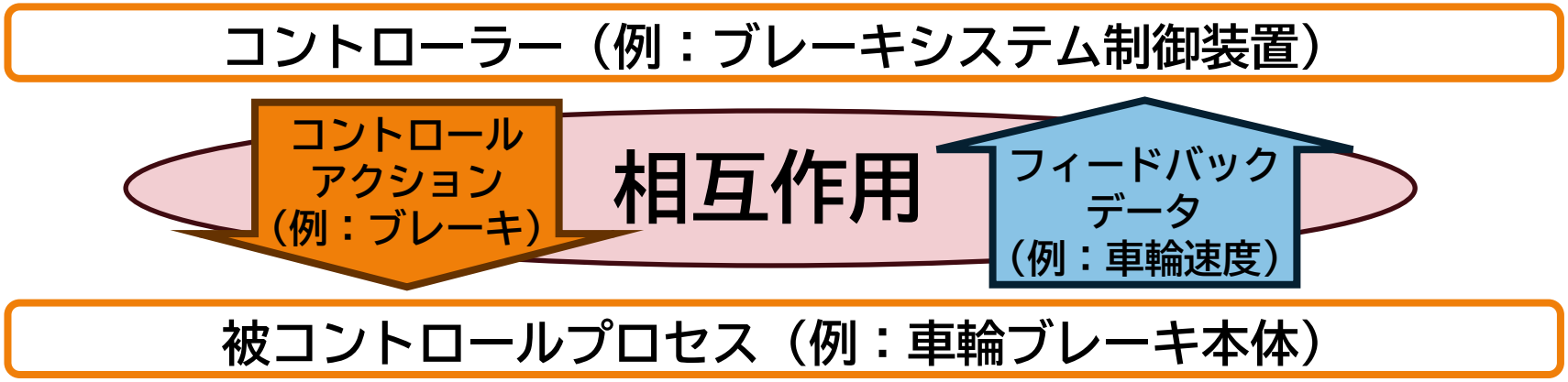


その他

- ETA
- CDM
- FRAM …

STAMP/STPAの概要説明

- **STAMP (System-Theoretic Accident Model and Processes: システム理論に基づく事故モデル)**
  - システムの事故の多くは構成要素の故障ではなくシステムの中で制御を行うコントローラーと被コントロールプロセスの相互作用が適切に働かないことによっておきているという前提
  - 「制御要素（コントローラー）」と「被制御要素（被コントロールプロセス）」の「相互作用」に着目したメカニズムを説明
  - 「アクションが働かない原因」＝「相互作用の不適切な作用」という視点を持つことで原因を具現化するアプローチ

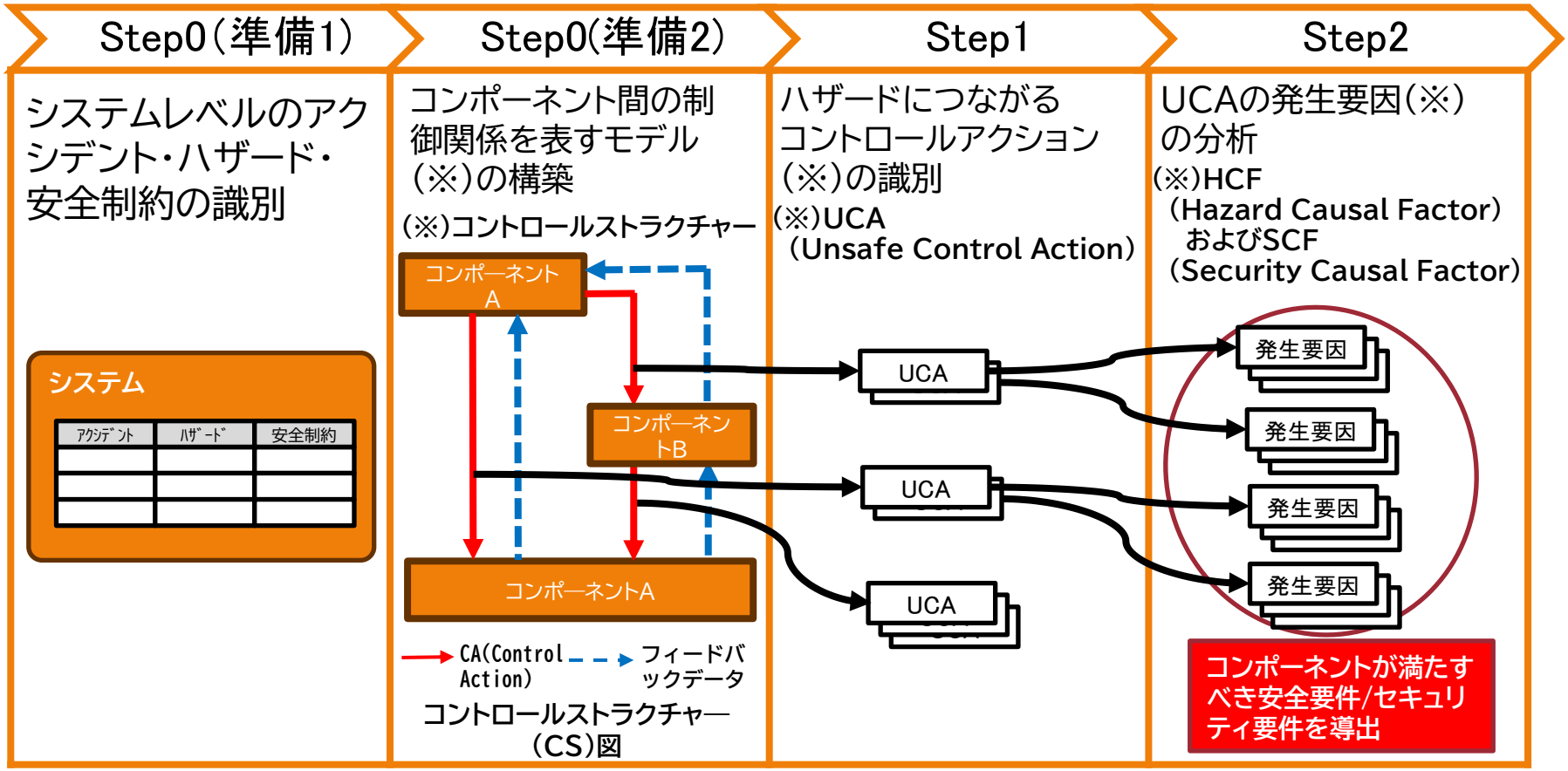


システム理論に基づく事故モデルSTAMP

「STAMPガイドブック ～システム思考による安全分析～ 2019年3月公開」

STAMP/STPAの概要説明

- **STPA（System-Theoretic Process Analysys）**
  - STAMP アクシデントモデルを前提としてシステムのハザード要因を分析する新しい安全解析手法



STPAによる分析の進め方

「STAMPガイドブック ～システム思考による安全分析～ 2019年3月公開」

分析事例のご紹介

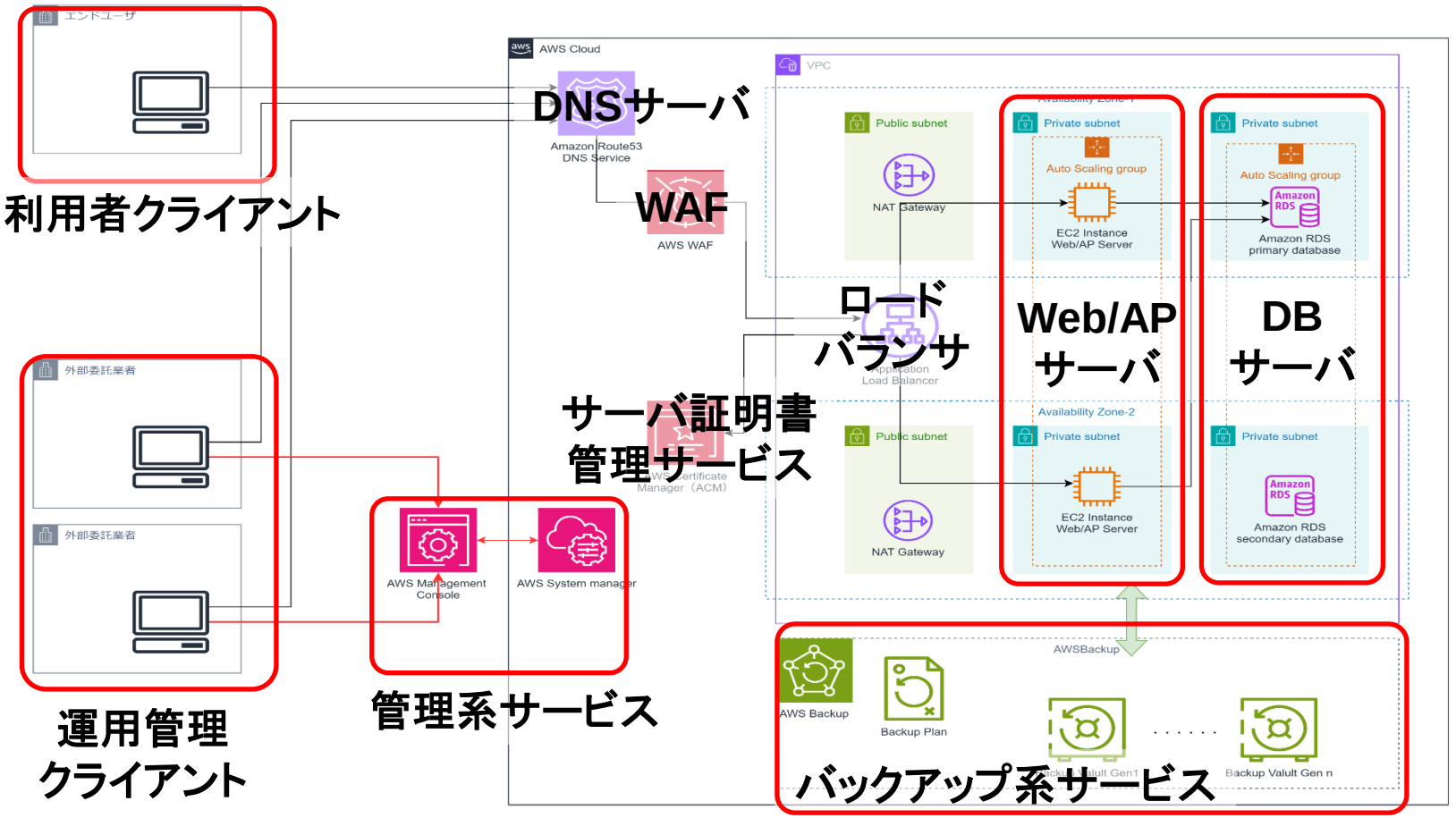
本日ご説明する内容

No	事例概要	使用/関連手法
1	Webシステムのセキュリティ要件分析	STAMP/STPA
2	ネットワーク機器撤去時の作業リスク抽出	STAMP/STPA
3	STAMP/STPAによるWebアプリケーションソフトウェアのリスク分析	STAMP/STPA
4	STAMP/STPA教育コンテンツの作成	STAMP/STPA
5	STAMP/STPAによる不具合分析となぜなぜ分析の比較	STAMP/STPA
6	STAMP/STPAによる障害分析	STAMP/STPA
7	CASTによる障害分析	CAST
8	FTAを用いた製品安全に関する脅威の可視化	FTA
9	ATAを用いた所定作業におけるサーバへの攻撃構造の可視化	ATA

事例１：Webシステムのセキュリティ要件分析

概要

一般的なWebアプリケーションをベースにSTAMP/STPAを利用したセキュリティ要件分析



事例1で分析対象とした一般的な2層のWebシステムの構成

事例１：Webシステムのセキュリティ要件分析

Step0（準備1） Step0(準備2) Step1 Step2

Step0（準備1）
- システムレベルのアクシデント、ハザード、安全制約の識別

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	システムが異常をきたし運用不可能な状態となる	H1	システムを構成するサーバが暗号化される	SC1	サーバ上では不正なアプリケーションが動作してはならない
A1	システムが異常をきたし運用不可能な状態となる	H2	システムの環境の変更について、誰が、いつ、何をしたかについて検知できない	SC2	システムの環境の変更について、誰が、いつ、何をしたか、検知出来る必要がある
A1	システムが異常をきたし運用不可能な状態となる	H3	システムを構成するサーバが不正に削除・変更される	SC3	システムを構成するサーバは正規の手順で削除、変更できること
A2	アプリケーションが正常に動作できず、運用不可能になる	H4	アプリケーションの構築・変更マスタが不正に削除、変更される	SC4	アプリケーションの変更は許可されたものによる操作によって行われること
A3	システムを取り巻く環境に問題があり、運用不可能になる	H5	システムがインターネットを利用できなくなる	SC5	システムは運用時間はインターネットとのアクセスが利用できること
A3	システムを取り巻く環境に問題があり、運用不可能になる	H6	クラウドサービスが利用不可能になる	SC6	システムは運用時間の間、サービス利用が出来ること
A4	システム上で管理する情報が漏えいする	H7	アプリケーションのユーザからの不正操作によりデータが漏えいする	SC7	アプリケーションは許可されたもの以外は利用しないこと
A4	システム上で管理する情報が漏えいする	H8	クラウドサービスのストレージ上のデータの盗難によりシステム上のデータが漏えいする	SC8	クラウド上のストレージ上のデータは許可されたもの以外は利用できないこと
A4	システム上で管理する情報が漏えいする	H9	バックアップデータの盗難により、システム上の管理データが漏えいする	SC9	バックアップデータへのアクセスは、許可されたもの以外できないこと
A5	システム運用に必要なアカウント情報が漏えいする	H10	AWS利用のためのルート、およびIAMアカウントのIDやパスワードが漏えいする	SC10	ルートユーザ、およびIAMユーザのアカウントのパスワードは盗難や類推などにより漏えいすることがないこと
A5	システム運用に必要なアカウント情報が漏えいする	H11	AWS利用のためのルート、およびIAMアカウントのID、パスワードを解読、利用される	SC11	ルートユーザ、およびIAMユーザは、多要素認証にて認証を行うこと
A6	情報漏えい事故によりエンドユーザからの信用が失墜する	H12	攻撃者が盗んだ個人情報を不正に利用される	SC12	システムが保持する個人情報が外部に漏えいしないこと
A6	情報漏えい事故によりエンドユーザからの信用が失墜する	H13	システムが保持する個人情報へのアクセスの検知が出来ない	SC13	システムが保持する個人情報へのアクセスは監視され、問題発生時は異常検知できること

運用不能になり、復旧が必要な事象

情報漏えいが発生し、対応が必要な事象

事例１：Webシステムのセキュリティ要件分析

Step0（準備1） Step0(準備2) Step1 Step2

Step0（準備1）

- システムレベルのアクシデント、ハザード、安全制約の識別

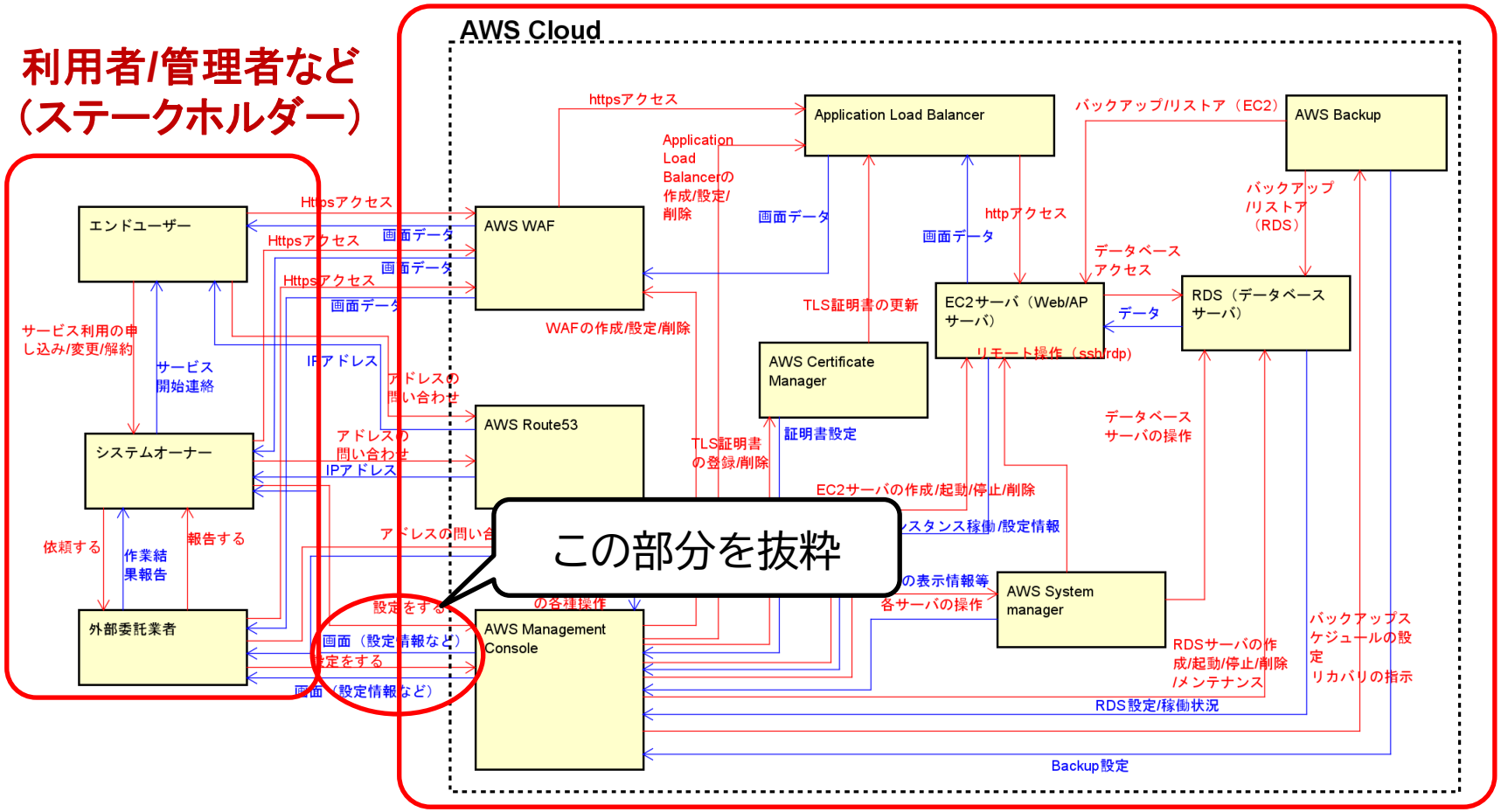
アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	システムが異常をきたし運用不可能な状態となる	H1	システムを構成するサーバが暗号化される	SC1	サーバ上では不正なアプリケーションが動作してはならない
A1	システムが異常をきたし運用不可能な状態となる	H2	システムの環境の変更について、誰が、いつ、何をしたかについて検知できない	SC2	システムの環境の変更について、誰が、いつ、何をしたか、検知出来る必要がある
A1	システムが異常をきたし運用不可能な状態となる	H3	システムを構成するサーバが不正に削除・変更される	SC3	システムを構成するサーバは正規の手順で削除、変更できる必要がある
A2	アプリケーションが保有するデータが利用できなくなり、運用不可能になる	H4	アプリケーションの稼働に必要なマスタが不正に削除、変更される	SC4	アプリケーションマスタの変更は許可されたものによる操作によって行われること
A3	システムを取り巻く環境に問題があり、運用不可能になる	H5	システムがインターネットを利用できなくなる	SC5	システムは運用時間はインターネットとのアクセスが利用できること
A3	システムを取り巻く環境に問題があり、運用不可能になる	H6	クラウドサービスが利用不可能になる	SC6	システムは運用時間の間、サービス利用が出来ること
A4	システム上で管理する情報が漏えいする	H7	アプリケーションのユーザからの不正操作によりデータが漏えいする	SC7	アプリケーションは許可されたもの以外は利用しないこと
A4	システム上で管理する情報が漏えいする	H8	クラウドサービスのストレージ上のデータの盗難によりシステム上のデータが漏えいする	SC8	クラウド上のストレージ上のデータは許可されたもの以外は利用できないこと
A4	システム上で管理する情報が漏えいする	H9	バックアップデータの盗難により、システム上の管理データが漏えいする	SC9	バックアップデータへのアクセスは、許可されたもの以外は利用できないこと
A5	システム運用に必要なアカウント情報が漏えいする	H10	AWS利用のためのルート、およびIAMアカウントのID、パスワードが漏えいする	SC10	ルートユーザ、およびIAMユーザのアカウントのパスワードは盗難や類推などにより漏えいすることがないこと
A5	システム運用に必要なアカウント情報が漏えいする	H11	AWS利用のためのルート、およびIAMアカウントのID、パスワードを解読、利用される	SC11	ルートユーザ、おおびIAMユーザは、多要素認証にて認証を行うこと
A6	情報漏えい事故によりエンドユーザからの信用が失墜する	H12	攻撃者が盗んだ個人情報を不正に利用される	SC12	システムが保持する個人情報が外部に漏えいしないこと
A6	情報漏えい事故によりエンドユーザからの信用が失墜する	H13	システムが保持する個人情報へのアクセスの検知が出来ない	SC13	システムが保持する個人情報へのアクセスは監視され、問題発生時は異常検知できること

事例１：Webシステムのセキュリティ要件分析

Step0（準備1） | Step0(準備2) | Step1 | Step2

Step0（準備2）

- コントロールストラクチャーの構築



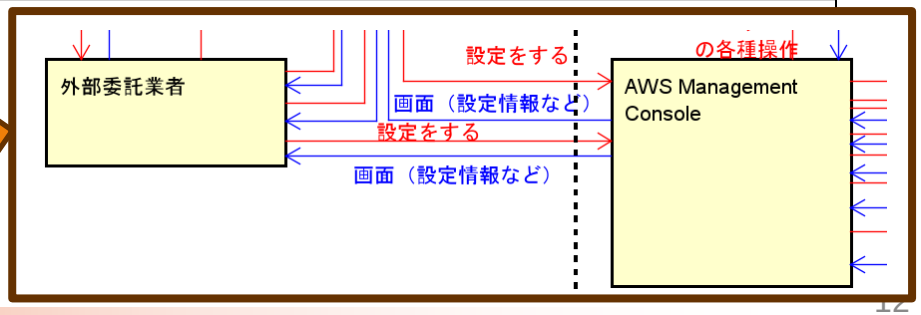
事例１：Webシステムのセキュリティ要件分析

Step0（準備1） Step0(準備2) **Step1** Step2

Step1
- ハザードに繋がるコントロールアクション(UCA)の分析

UCAの識別（外部委託業者によるシステムメンテナンス時の設定）

CA/ From/ To	CA提供条件	Type	Description
設定をする/ 外部委託業者 / AWS Management Console	システムのメンテナンス操作時	Not Providing	(UCA5-N-1) システムのメンテナンスに関する機能を操作することが出来ないため適切な保守が実施出来ない /[SC11][SC3][SC6][SC8][SC9]
		Providing causes hazard	(UCA5-P-1) 操作を誤ることによって誤ったアプリケーションを配布・動作させてしまう/ [SC1] (UCA5-P-2) 要件を満たさないパスワードの設定が行われる。/ [SC10] (UCA5-P-3) 誤操作により、システムが保有する情報が外部からアクセス可能になる / [SC12] (UCA5-P-4) 誤操作により、誤った検知設定が行われる / [SC13] (UCA5-P-5) 誤操作により、操作履歴（ログなど）が消えてしまう / [SC2] (UCA5-P-6) アクセス権の設定を間違える / [SC3][SC6][SC8][SC9] (UCA5-P-7) 通信許可の設定を誤ることで通信による操作、利用などが出来なくなる / [SC3][SC4][SC5][SC6][SC7][SC8][SC9] (UCA5-P-8) クラウド上のバックアップを誤って削除する / [SC9]
		Too early / Too late	(UCA5-T-1) 不正アクセス監視の問題発生～検知に時間がかかりすぎる / [SC13]
		Stop too soon / Applying too long	



事例１：Webシステムのセキュリティ要件分析

Step0（準備1） Step0(準備2) Step1 Step2

Step1
- ハザードに繋がるコントロールアクション(UCA)の分析

UCAの識別（外部委託業者によるシステムメンテナンス時の設定）

CA/ From/ To	CA提供条件	Type	Description
		Not Providing	(UCA5-N-1) システムのメンテナンスに関する機能を操作することが出来ないため適切な保守が実施出来ない /[SC11][SC3][SC6][SC8][SC9]
る/ 外部委託業者 /	システ	Providing causes hazard	1) 操作を誤ることによって誤ったアプリケーションを配布・動作させてしまう/ [SC1] 2) 要件を満たさないパスワードの設定が行われる。/ [SC10] 3) 誤操作により、システムが保有する情報が外部からアクセス可能になる / [SC12] (UCA5-P-4) 誤操作により、誤った検知設定が行われる / [SC13] (UCA5-P-5) 誤操作により[…]が消えてしまう / [SC2] (UCA5-P-6) アクセス権の設[…]SC3][SC4][SC9] -7) 通信許可の設定を誤ることで通信による操作、利用などが出来なくなる / C4][SC5][SC6][SC7][SC8][SC9] -8) クラウド上のバックアップを誤って削除する / [SC9]
geme nt Conso le	作時	Too early / Too late	(UCA5-T-1) 不正アクセス監視の問題発生～検知に時間がかかりすぎる / [SC13]
		Stop too soon / Applying too long	

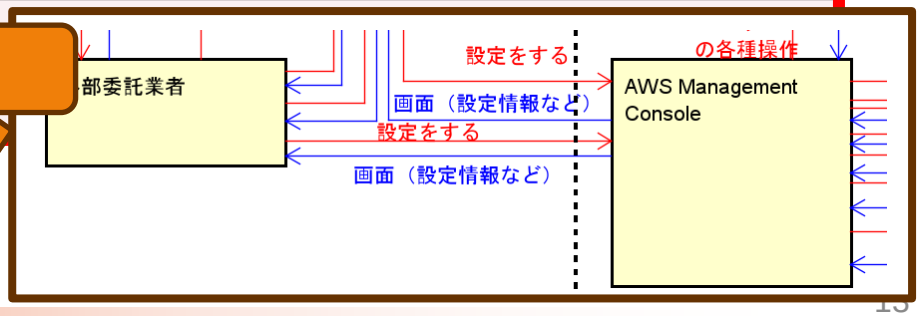
与えられないとハザード

与えられるとハザード

洗い出したUCA

遅すぎ・早すぎ

遅すぎる停止・早すぎる適用



事例１：Webシステムのセキュリティ要件分析

Step0（準備1） Step0(準備2) Step1 Step2

Step2
- UCA発生要因(HCF/SCF)の分析/対策の検討

特定する手順
(1) UCAごとにヒントワード（後述）をあてはめハザードとなりうるかを検討する。
(2) ハザード事象が発生する条件(HCF/SCF)とアクシデントにつながるまでのシナリオを作成する。

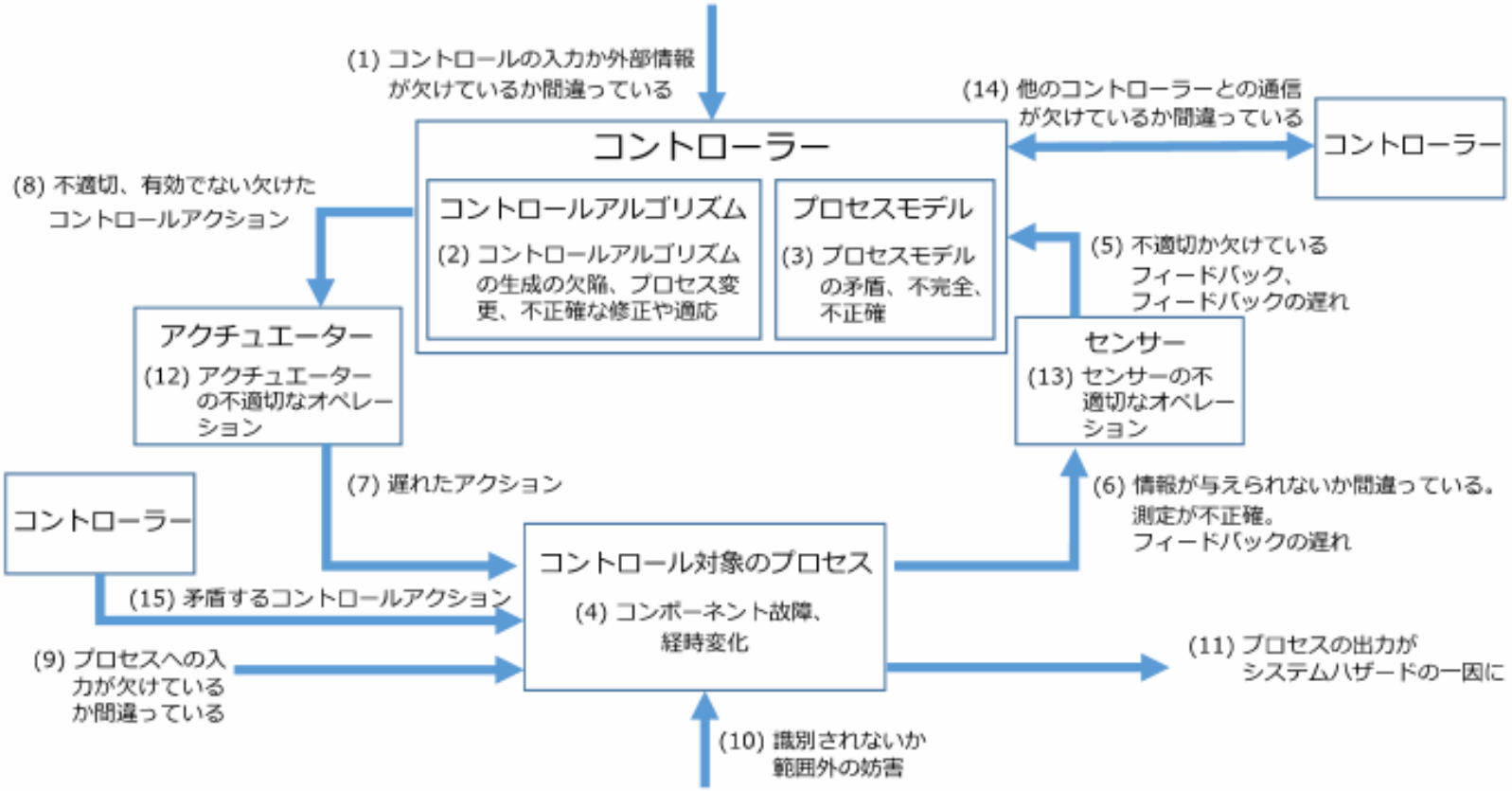
UCA	システムのメンテナンスに関する機能を操作することが出来ないため適切な保守が実施出来ない
ヒントワード	（11）プロセスの出力がシステムハザードの一因に
HCF/SCF	初回ログイン時にパスワード変更権限がないので変更に失敗したのち操作不能

シナリオ	プロセス
	保守作業者(外部委託業者、あるいはシステムオーナー)がAWS Management Consoleのログイン画面を表示
	保守作業者はログインのためにアカウントID･ユーザID･パスワード(初期パスワード)を入力
	AWSのログインに成功した後にパスワードの変更を促すメッセージを表示
	保守作業者によるパスワード更新をおこなうもののそのユーザにパスワード変更権限がないのでパスワード更新に失敗して操作不能になる

事例１：Webシステムのセキュリティ要件分析

Step0(準備1) → Step0(準備2) → Step1 → Step2

Step2
- UCA発生要因(HCF/SCF)の分析/対策の検討



HCFの抽出時に使ったヒントワード

「セーフティ＆セキュリティ入門 AI,IoT時代のシステム安全 2021年10月26日」

事例１：Webシステムのセキュリティ要件分析

Step0（準備1） Step0(準備2) Step1 Step2

Step2
- UCA発生要因(HCF/SCF)の分析/対策の検討

SCF抽出時に利用したヒントワード（STRIDE）

脅威	説明
Spoofing identity	他のユーザになりすます
Tampering	データの意図的な操作、改ざんをする
Repudiation	ユーザアクションを否認する
Information Disclousure	アクセス権のない相手に情報を公開する
Denial of Service	攻撃により正規利用者のサービス中断をする
Elevation of Privilege	悪用可能な不正アクセス権限を得る

事例１：Webシステムのセキュリティ要件分析

Step0（準備1） Step0(準備2) Step1 Step2

Step2
- UCA発生要因(HCF/SCF)の分析/対策の検討

HCF/SCFの特定と、シナリオ（抜粋）

ID	HCF/SCF	ヒントワード	シナリオ
HCF5-N-1-3	初回ログイン時にパスワードの変更を求められるが、パスワード変更権限の割当がないことから、パスワードの変更が出来ず、ログインすることが出来ない	(11) プロセスの出力がシステムハザードの一因に	保守作業者（外部委託業者、あるいはシステムオーナー）がAWS Management Consoleのログイン画面を表示する 保守作業者は、ログインはアカウントID、ユーザID、パスワード（初期パスワード）を入力する AWSのログインに成功するが、ログイン時にパスワードの変更が必要なため、変更を促すメッセージが表示される。 保守さ業者は新しいパスワードを入力するが、そのユーザにパスワード変更権限がないことからパスワードの変更に失敗し、ログイン後の操作が出来ない
HCF5-N-1-4	ルートユーザでログインしようとしたところ、別のユーザがパスワードを変更してしまいログインが出来ない	(2) コントロールアルゴリズムの生成の欠陥、プロセス変更、不正確な修正や適応	守作業者A（外部委託業者、あるいはシステムオーナー）がAWS Management Consoleのルートユーザのログイン画面を表示する 保守作業者Aがログイン後、何らかの理由（パスワードの有効期限切れなど）によりパスワードを変更した 保守作業者Aがパスワード変更に関する内容についての引継ぎを失念した、あるいは保守作業者Bの引継ぎ確認漏れ等の理由により情報 保守作業者Aがログイン画面を表示する 保守作業者Aがルートユーザでログインすることが出来ない。
HCF5-N-1-5	しまい、正規の利用者（保守作業者）がログイン出来ない	(16) Spoofing Identify	攻撃者がパスワードアタック（辞書によるパスワード推測、あるいは総当たり攻撃）によりルートユーザアカウントのID、およびパスワードを入手する 攻撃者はルートユーザによるログインに成功する 攻撃者はルートユーザのパスワードを変更する。 のアカウントをロックアウト、あるいはパスワードを変更を変更し、ログインをできはシステムオーナー）がルートユーザー、あるいはIAMユーザでログインを試みるが

アクシデントに至るまでのシナリオを検討

UCAの発生要因

UCAとHCF/SCFを関連付けたヒントワード

事例１：Webシステムのセキュリティ要件分析

Step0（準備1） Step0(準備2) Step1 **Step2**

Step2
- UCA発生要因(HCF/SCF)の分析/対策の検討

UCA	対策対象コンポーネント	HCF/SCF	方針	エラー着想手順	対策
(UCA5-N-1) システムのメンテナンスに関する機能を操作することが出来ないため適切な保守が実施出来ない [SC11][SC3][SC6][SC8][SC9]	システムオーナー 外部委託業者	IAMユーザのパスワードを忘れてしまう等によって、AWS Management Consoleにログインすることが出来ない	回避	④ やりやすくする	IDaaSやパスワードマネージャの利用によって、パスワードの管理をする
(UCA5-N-1) システムのメンテナンスに関する機能を操作することが出来ないため適切な保守が実施出来ない [SC11][SC3][SC6][SC8][SC9]	システムオーナー	…を紛失、あるいは破損してしまい、…ことが出来ない	軽減	⑪ 被害に備える	(IAMユーザの場合)MFAトークン紛失時のリセット、および再設定の手順をあらかじめ用意しておき、保守ユーザ内へ周知する。
			軽減	⑪ 被害に備える	(ルートユーザの場合)MFAトークンを2つ登録し、1つが紛失、あるい破損した場合は予備によるログインができるようにする。
(UCA5-N-1) システムのメンテナンスに関する機能を操作することが出来ないため適切な保守が実施出来ない [SC11][SC3][SC6][SC8][SC9]	システムオーナー 外部委託業者	初回ログイン時…が、	軽減	③ わかりやすくする	ユーザアカウント発行の手順をツール化し、必要な権限をプリセットするようにCLIにて設定する。
			軽減	⑨ 自…	ユーザ登録手順のチェックリストを作成し、確実な登録を確認する手順とする
(UCA5-N-1) システムのメンテナンスに関する機能を操作することが出来ないため適切な保守が実施出来ない [SC11][SC3][SC6][SC8][SC9]	システムオーナー 外部委託業者				ルートユーザのパスワード変更を監視対象とし、何かの操作が行われた…、運用担当者へメールで通…くように設定をする。
	システムオーナー 外部委託業者				…ユーザのパスワード紛失時に…、アカウント回復手順のため…の質問を設定し、問題発生時の復旧手順を用意する。

HCF/SCFに対する方針を(回避,軽減,共有/転嫁,受容)から選択

4STEP/Mからリスクへの対策方針を選択

選択した方針に従い、具体化した内容を記述

事例１：Webシステムのセキュリティ要件分析

Step0（準備1） Step0(準備2) Step1 **Step2**

Step2
- UCA発生要因(HCF/SCF)の分析/対策の検討

4STEP/M(※1)による問題への対策

No	ステップ	対策	説明
1	(1)機会最小	やめる(なくす)	作業を見直してやめることを検討。
2	(2) 最小確率	出来ないようにする	仕組み、制約を変えてできない形にする
3		分かりやすくする	色や表示等を工夫しわかりやすくする
4		やりやすくする	操作性を見直すなどしてやりやすくする
5		知覚能力を持たせる	知覚能力を維持する(睡眠、健康、加齢等を認識し、パフォーマンスを維持するように心がける)
6		認知・予測させる	危険、間違え探しなどのトレーニング
7		安全を優先させる	安全を優先する価値観づくり、実践など
8		できる能力を持たせる	機械等の品質保証、人間の品質保証(操作者の健康、心身状態のチェック、訓練など)
9	(3) 多重検出	自分で気づかせる	リチェック、指差呼称などの実施
10		検出する	チェックリストなどにより間違いを検出する
11	(4) 被害局限	備える	問題発生に備えておく(失敗の影響を減らす対策や、コンティジェンシープランの準備、保険、リスクマネジメント等)

(※1)Strategic approach To Error Prevention & Mitigation by 4Ms の略

事例１：Webシステムのセキュリティ要件分析

Step0（準備1） → Step0(準備2) → Step1 → Step2

Step2
- UCA発生要因(HCF/SCF)の分析/対策の検討

4STEP/M(※1)による問題への対策

No	ステップ	対策	説明
1	(1)機会最小		してやめることを検討。
2	(2) 最小確率		的を変えてできない形にする
3		分	を工夫しわかりやすくする
4		やりやすくする	操作性を見直すなどしてやりやすくする
5		知覚能力を持たせる	知覚能力を維持する(睡眠、健康、加齢等を認識し、パフォーマンスを維持するように心がける)
6		認知・予測させる	危険、間違え探しなどのトレーニング
7		安全を優先させる	安全を優先する価値観づくり、実践など
8		できる能力を持たせる	機械等の品質保証、人間の品質保証(操作者の健康、心身状態のチェック、訓練など)
9	(3) 多重検出		指差呼称などの実施
10		検出する	トなどにより間違いを検出する
11	(4) 被害局限	備	備えておく(失敗の影響を減らす対策や、コンティジェンの準備、保険、リスクマネジメント等)

Minimum encounter

Minimum probability

Multiple detection

Minimum damage

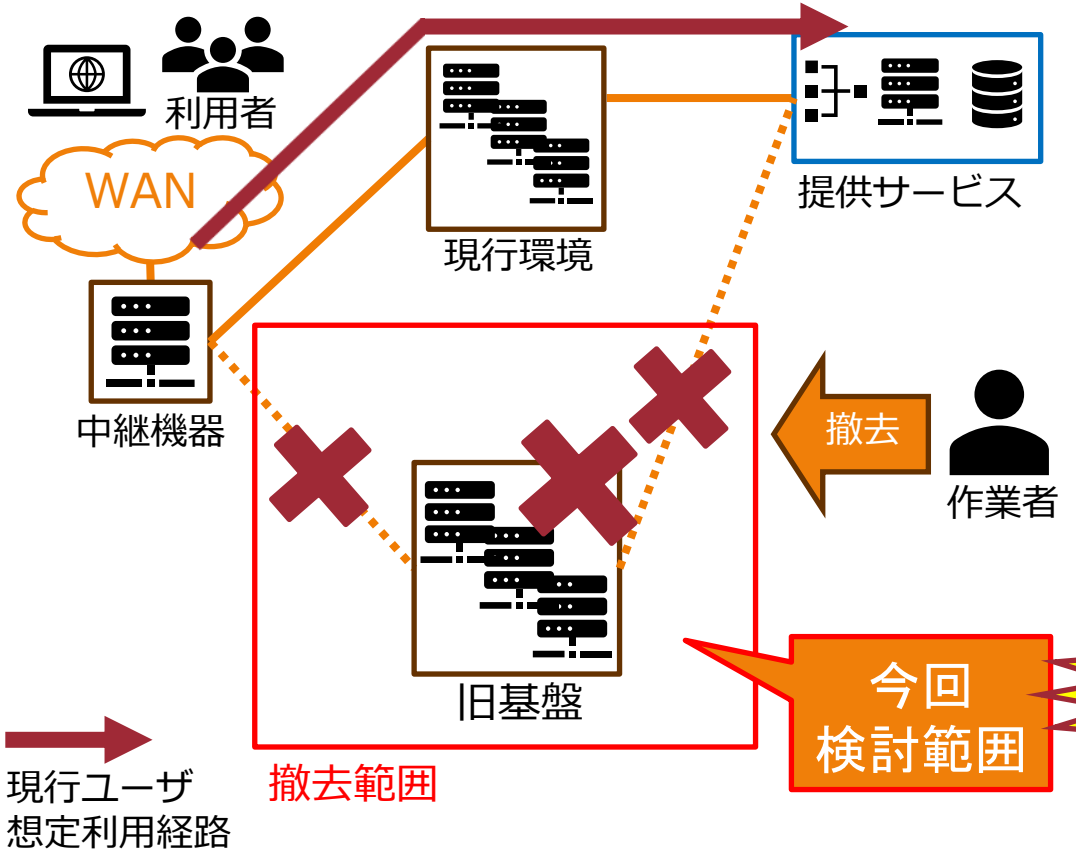
(※1)Strategic approach To Error Prevention & Mitigation by 4Ms の略

- **STAMP/STPAによる分析を行った考察**
  - STAMP/STPAのモデルを作る**前提条件が必要**
    - 最初はSTAMP Workbenchに向かってモデルづくりを試行錯誤しようとしたが全く先に進めることが出来なかった。
  - 分析はウォーターフォールのようにステップを踏むのではなく、**インクリメンタルに実施するほうがよい**
    - 一度にすべてを洗い出してから先へ進もうとすると、検討すべき対象がおおいので、複雑に感じた。
    - フロントローディング一部について先行させることで、得た気づきや知見を他に展開できる。また分析の複雑さがコントロールできる。
  - **４STEP/M**による対策案の作成は、**STAMP/STPAと相性がよい**
    - STAMP/STPAにおけるUCAの識別、HCF/SCFの特定と、４STEP/Mによる対策の検討のアプローチは似ているので、違和感がなかった。

事例２：ネットワーク機器撤去時の作業リスク抽出

■概要

旧基盤老朽化に伴うネットワーク機器撤去時の作業リスクを
STAMP/STPAで分析し抽出



■想定環境 / 前提条件
- 旧基盤関連機器のみ対象
- 稼働状況に影響があるリスクのみ抽出
  ※体調不良、災害…は対象外

事例２：ネットワーク機器撤去時の作業リスク抽出

Step0（準備1） Step0(準備2) Step1 Step2

Step0（準備1）
- システムレベルのアクシデント、ハザード、安全制約の識別

アクシデント	ハザード	安全制約
新基盤から機器を撤去してしまいサービスが利用できる	作業者が撤去対象機器を誤る	作業時に再監者が1手順ごとに作業者の作業の正当性を確認し保証する
	撤去対象機器が新基盤と旧基盤両方で利用されている	撤去対象機器の状態を確認し撤去可能であることまたは撤去対象箇所を確定する
		撤去対象機器が接続されている機器を事前に洗い出し、撤去しても問題ないことを確認する
旧基盤機器撤去時サービスが停止する	ユーザが旧基盤経由でサービスを利用している	撤去対象機器の状態を確認し撤去可能であることまたは撤去対象箇所を確定する
		撤去対象機器が接続されている機器を事前に洗い出し、撤去しても問題ないことを確認する
	旧基盤から新基盤を経由する想定外の通信経路が存在する	撤去対象機器の状態を確認し撤去可能であることまたは撤去対象箇所を確定する
		撤去対象機器が接続されている機器を事前に洗い出し、撤去しても問題ないことを確認する

新基盤から誤って撤去してしまうケース

旧基盤から撤去する際にサービス停止してしまうケース

事例２：ネットワーク機器撤去時の作業リスク抽出

Step0（準備1） Step0（準備2） Step1 Step2

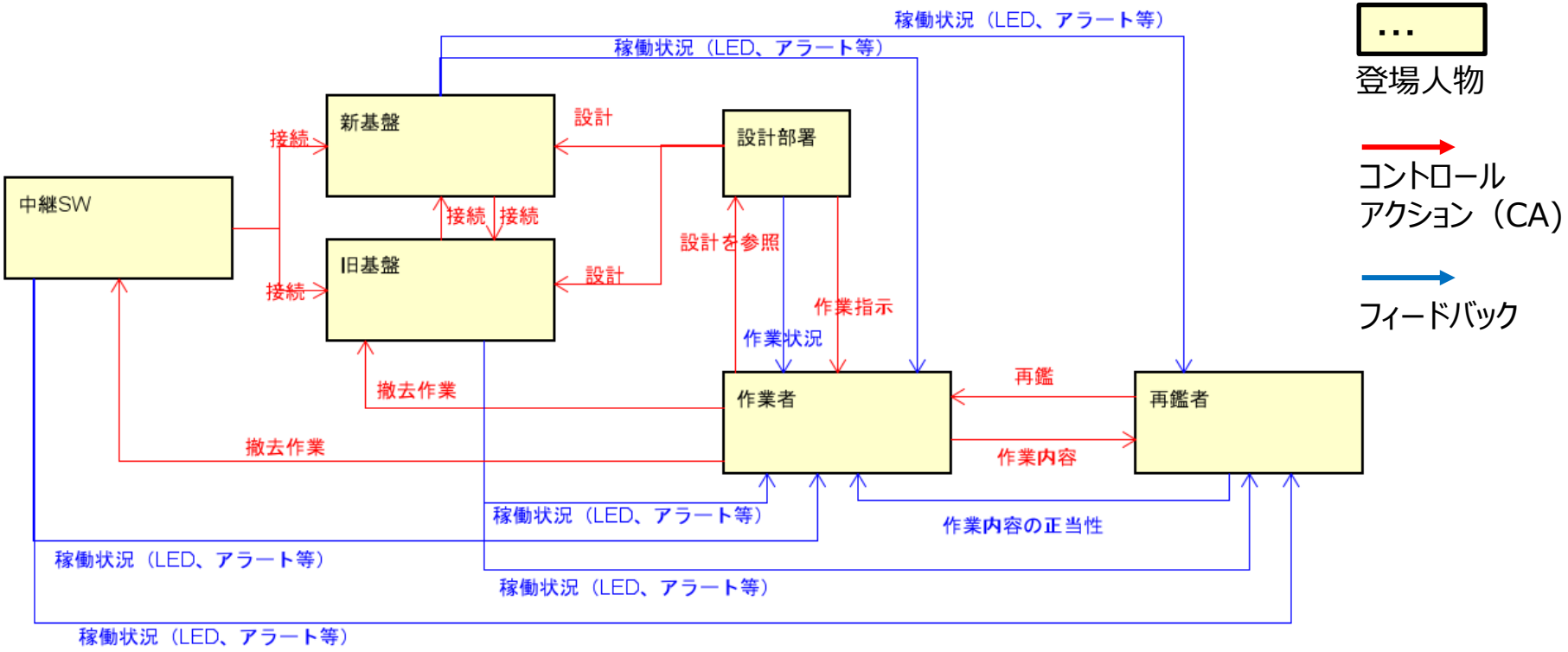
Step0（準備1）
- システムレベルのアクシデント、ハザード、安全制約の識別

アクシデント	ハザード	安全制約
新基盤から機器を撤去してしまいサービスが利用不可になる	作業者が撤去対象機器を誤る	作業時に再監者が1手順ごとに作業者の作業の正当性を確認し保証する
	撤去対象機器が新基盤と旧基盤両方で利用されている	撤去対象機器の状態を確認し撤去可能であることまたは撤去対象箇所を確定する
		撤去対象機器が接続されている機器を事前に洗い出し、撤去しても問題ないことを確認する
旧基盤機器撤去時にサービスが停止する	ユーザが旧基盤経由でサービスを利用している	撤去対象機器の状態を確認し撤去可能であることまたは撤去対象箇所を確定する
		撤去対象機器が接続されている機器を事前に洗い出し、撤去しても問題ないことを確認する
	旧基盤から新基盤を経由する想定外の通信経路が存在する	撤去対象機器の状態を確認し撤去可能であることまたは撤去対象箇所を確定する
		撤去対象機器が接続されている機器を事前に洗い出し、撤去しても問題ないことを確認する

事例２：ネットワーク機器撤去時の作業リスク抽出

Step0（準備1） | Step0(準備2) | Step1 | Step2

Step0（準備2)
- コントロールストラクチャーの構築

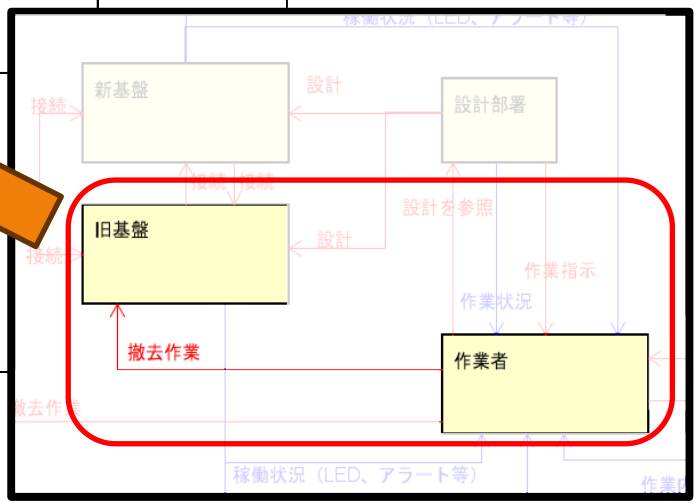


事例２：ネットワーク機器撤去時の作業リスク抽出

Step0（準備1） → Step0(準備2) → Step1 → Step2

Step1
- ハザードに繋がるコントロールアクション(UCA)の分析

No	CA	From	To	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	撤去作業	作業者	旧基盤		(UCA1-P-1) 撤去予定ではない機器が撤去される		
2	撤去作業	作業者	中継SW		(UCA2-P-1) ユーザが利用しているNW機器・経路が撤去さ		
3	再鑑	再鑑者	作業者	(UCA3-N-1) 不正な作業手順が実行される [SC1]			
4	設計	設計部署	旧基盤	(UCA4-N-1) 意図しない通信経路や機器が存在する [SC3]	(UCA4-P-1) 設計時の思想とは異なる経路を作成する		
⋮							



：CA

事例２：ネットワーク機器撤去時の作業リスク抽出

Step0（準備1） Step0(準備2) Step1 Step2

Step1
- ハザードに繋がるコントロールアクション(UCA)の分析

No	CA	From	To	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	撤去作業	作業者	旧基盤		(UCA1-P-1) 撤去予定ではない機器が撤去される		
2	撤去作業	作業者	中継SW		(UCA2-P-1) ユーザが利用しているNW機器・経路が撤去される		
3	再鑑	再鑑者	作業者	(UCA3-N-1) 不正な作業手順が実行される [SC1]			
4	設計	設計部署	旧基盤	(UCA4-N-1) 意図しない通信経路や機器が存在する [SC3]	(UCA4-P-1) 設計時の思想とは異なる経路を作成する		
⋮							

ガイドワードを元にUCAを分析

与えられないとハザード

与えられるとハザード

早すぎ 遅すぎ

早すぎる停止 遅すぎる適用

事例２：ネットワーク機器撤去時の作業リスク抽出

Step0（準備1） → Step0(準備2) → Step1 → Step2

Step2
- UCA発生要因(HCF)の分析/対策の検討

UCA	HCF	対策	対策対象 登場人物
撤去予定ではない機器が撤去される	撤去対象機器として事前に確認した機器に誤りがある	作業前に現地調査および設計書との突き合わせを実施し相違がないかを確認する	作業者 設計部署
	作業対象機器を手と声 とは異なる機器 う☒	再鑑者が作業者 る	
不正な作業手順が実行される	作業者が作業手順書に存在しない手順を実施する	再鑑者が作業者の作業 る	
意図しない通信経路や機器が存在する	作業前に現地調査を実施していない	作業前に現地調査おとの突き合わせを実施ないかを確認する	
	ケーブルタグ等現地機器の記載情報が古い		
⋮			

Not Providing	Providing causes hazard	Too earl late
	(UCA1-P-1) 撤去予定ではない機器が撤去される	
	(UCA2-P-1) ユーザが利用しているNW機器・経路が撤去される	
(UCA3-N-1) 不正		

事例２：ネットワーク機器撤去時の作業リスク抽出

Step0（準備1） → Step0(準備2) → Step1 → Step2

Step2
- UCA発生要因(HCF)の分析/対策の検討

UCA	HCF	対策	対策対象
撤去予定ではない機器が撤去される	撤去対象機器として事前に確認した機器に誤りがある	作業前に現地調査および設計書との突き合わせを実施し相違がないかを確認する	作業者 設計部署
	作業者の不注意で撤去対象機器とは異なる機器を撤去してしまう☒	作業対象機器を手と声を出して確認する	作業者 再監者
		再鑑者が作業者の作業を確認する	再監者
不正な作業手順が実行される	作業者が作業手順書に存在しない手順を実施する	再鑑者が作業者の作業を確認する	再監者
意図しない通信経路や機器が存在する	作業前に現地調査を実施していない	作業前に現地調査および設計書との突き合わせを実施し相違がないかを確認する	作業者 設計部署
	ケーブルタグ等現地機器の記載情報が古い		
⋮			

HCF・対策を検討
↓
実際の運用と比較

事例２：ネットワーク機器撤去時の作業リスク抽出

■感想

- アクシデント、ハザード、対策を体系的かつ網羅的に抽出
  - 実際の運用と同等の対策を抽出

- ただし、
  アクシデントやハザード、登場人物の整理・設定が難しい
  - 対象システムへの理解、想定リスクの範囲、対策の妥当性…

- **妥当なハザードは？**
- **登場人物間の関連？**
- **UCAの分析方法？UCAはどう発生する？**
- **対策は妥当？　…など**

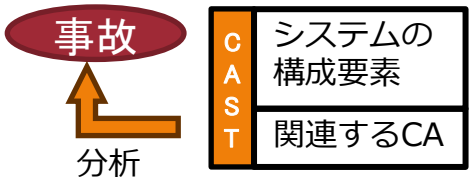
★実際に活用するには、
・手法の反復練習や実務経験を通じたシステム理解・スキル向上が必須
・アクシデントやリスク大小による適用要否判断も必要

その他事例一覧

■その他　安心安全に関わる様々なテーマと実際の事例分析

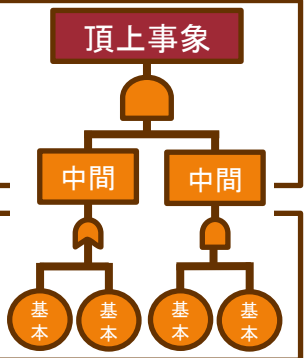
CAST

STAMP事故モデルの考え方に基づいた事後分析手法



FTA

頂上事象の発生頻度分析のために故障原因を論理的にたどる手法



ATA

FTAと同様の木形式で攻撃手段を論理的にたどる手法

その他
- ETA
- CDM
- FRAM　…

様々な手法を学習

No	事例概要	使用/関連手法
3	STAMP/STPAによるWebアプリケーションソフトウェアのリスク分析	STAMP/STPA
4	STAMP/STPA教育コンテンツの作成	STAMP/STPA
5	STAMP/STPAによる不具合分析となぜなぜ分析の比較	STAMP/STPA
6	STAMP/STPAによる障害分析	STAMP/STPA
7	CASTによる障害分析	CAST
8	FTAを用いた製品安全に関する脅威の可視化	FTA
9	ATAを用いた所定作業におけるサーバへの攻撃構造の可視化	ATA

コースの感想

No	事例概要
1	機能要件のデザインとセキュリティ要件のデザインのアプローチの違いがつかめてきたのがとても良かったです。今後、業務で活用していきこうと思います。
2	様々な事例を通じて安心安全に関わる手法を学習でき、実務でも使用するイメージが湧いてきましたが、実際に活用するためには業務上の経験がまだまだ必要だとも感じました。
3	色々な事例を通じてリスク・事故分析の技術と手法を学習できるのがとてもよかったです。今後の業務で手法を活用して経験を積んでいきたいと思っています。
4	分科会メンバからのフィードバックにより、コンテンツ自体のリファインだけでなく、手法に対する新たな気づきも得られ有意義でした。グループ内への手法推進に活用していきます。
5	事例に適用することで、STAMP/STPAによる分析となぜなぜ分析の違いを実感することができてよかった。
6	具体的な事例に適用することでSTAMP Workbenchによる可視化効果を実感できた。 今後、業務での活用を検討したい。
7	他の事例を通じて、色々な事例へ分析手法を適用できることがわかった。今後の業務で分析手法を適用して行きたいと思う。
8	自社内での障害分析は「なぜなぜ分析」の適用が多いが、本分科会にてCAST分析を知り、実際の事例に適用して分析を行うことができた。今後は事例により使い分けを行いたい。
9	他の方の事例を通して、自身が実施していない手法の理解も得られた点が有意義でした。また、セキュリティ対策の課題感が共有できたことも、モチベーションとなりました。

ご指導を頂きました
金子主査、髙橋副主査、佐々木特別講師、野本特別講師
ならびに特別講義の講師の方々、
ご協力頂いた研究員の皆様、事務局の皆様に
心から御礼申し上げます。

ご清聴ありがとうございました

演習コースIV　セーフティ＆セキュリティー同

参考資料

- STAMPガイドブック ～システム思考による安全分析～ 2019年3月公開, https://www.ipa.go.jp/digital/stamp/about.html ,2024/02/12参照
- 金子 朋子ら,セーフティ＆セキュリティ入門 AI、IoT時代のシステム安全,日科技連, 2021
- 河野龍太郎，医療におけるヒューマンエラー 第2版 なぜ間違える どう防ぐ，医学書院p.72，2004