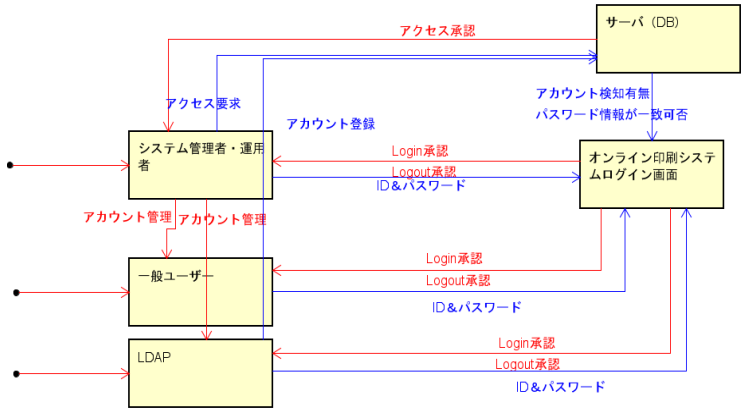
付録1: 事例3「STAMP/STPAによるWebアプリケーションリスク分析」
～Webアプリケーション情報資産のリスク分析～

1. 適用した事例

Webアプリケーションのセキュリティを脅かす脆弱性のうち,情報漏洩の防止を着目し,システムにある重要資産となるDB及びサーバに対するSTAMP WorkBenchを用いた分析を試みた.

2. Step0

Step0では, STAMP/STPAの手法に沿って一般的なWebアプリケーションシステムをベースにし,運用を前提としてシステムのアーキテクチャなどを設定した.アクシデント・ハザード（運用上望ましくない事情）・安全制約を識別し,登場人物を抽出した.
コントロールアクションの定義を元に,CS図を自動に生成された.STAMP手法はコントロールと被コントロールの相互作用を着目している手法となり,STAMP Workbenchで関係性の整理と構成の可視化を自動に実施された. 以下が例の一部である.



3. Step 1（UCAの抽出）

Step 1 では, CS図からCAを識別し，4つのガイドワードを適用しハザードにつながる非安全なUCAを抽出した．(図は省略)

4. Step 2（HCFの特定及び対策検討）

抽出したUCAに対してUCAごとにSTRIDE手法を適用して,攻撃者の意図をとらえるためのヒントワードとしてリスクの洗い出しを行い,HCF表を作った. STRIDE手法では６つ分類でセキュリティ対策につなげやすいと感じた. また，これらのリスクへの対策の検討については，分析にて洗い出されたHCFを元に脅威緩和策の対策表を立案した.以下が例の一部である.

対策表 / 対策表

HCFID	HCF	対策ID	対策	UCA	対策対象コンポーネント
HCF5-P-1-1	（なりすまし）LDAPインジェクション攻撃でシステムを登録できた。	M7	入力された文字列（パラメータ）に含まれるメタ文字をエスケープする	(UCA5-P-1) 登録していないLDAPユーザーがIDとパスワードを入力する時に、Loginが実施された。[SC1][SC2]	LDAP オンライン印刷システムログイン画面 サーバ（DB）
HCF10-T-1-1	ログアウト時間が明確に設定していない	M8	セッション識別子はログアウトした際、一定期間アクセスが無い場合、タイムアウト時間を経過した場合には無効にする	(UCA10-T-1) ログアウト処理が遅くなる場合は、認証したユーザー以外に登録無しの人が登録したユーザーのアカウントが利用される[SC1]	オンライン印刷システムログイン画面 サーバ（DB） システム管理者・運用者 一般ユーザー
HCF5-P-1-2	（改ざん）潜入したマルウェアにより改ざんされたことで、ログイン無しでも登録できた。	M9	マルウェア対策	(UCA5-P-1) 登録していないLDAPユーザーがIDとパスワードを入力する時に、Loginが実施された。[SC1][SC2]	オンライン印刷システムログイン画面 サーバ（DB）
HCF5-P-1-2	（改ざん）潜入したマルウェアにより改ざんされたことで、ログイン無しでも登録できた。	M5	アクセス権の管理	(UCA5-P-1) 登録していないLDAPユーザーがIDとパスワードを入力する時に、Loginが実施された。[SC1][SC2]	オンライン印刷システムログイン画面 サーバ（DB）
HCF5-P-1-3	（情報の暴露）LDAP登録情報が盗難された。	M10	データの暗号化	(UCA5-P-1) 登録していないLDAPユーザーがIDとパスワードを入力する時に、Loginが実施された。[SC1][SC2]	LDAP サーバ（DB）
HCF5-P-1-3	（情報の暴露）LDAP登録情報が盗難された。	M1	アクセスログ管理	(UCA5-P-1) 登録していないLDAPユーザーがIDとパスワードを入力する時に、Loginが実施された。[SC1][SC2]	システム管理者・運用者
HCF11-P-1-2	（改ざん）潜入したマルウェアにより改ざんされたことで、ログイン無しでも登録できた。	M5	アクセス権の管理	(UCA11-P-1) 管理者以外のユーザーがDBアクセスできる[SC4]	オンライン印刷システムログイン画面 サーバ（DB）

5. おわりに

一般的なWebアプリケーションシステムに対する,STAMP/STPAによる脅威分析/リスク分析を実施することで，情報漏洩の誘発要因を洗い出して，対策を立てることができた．システムのモデリングについて要素間のコントロール相関作用があるシステムに対するSTAMP/STPAが有効であると考え,STAMP WorkBenchツールはリスク分析に利用しやすいと感じた.

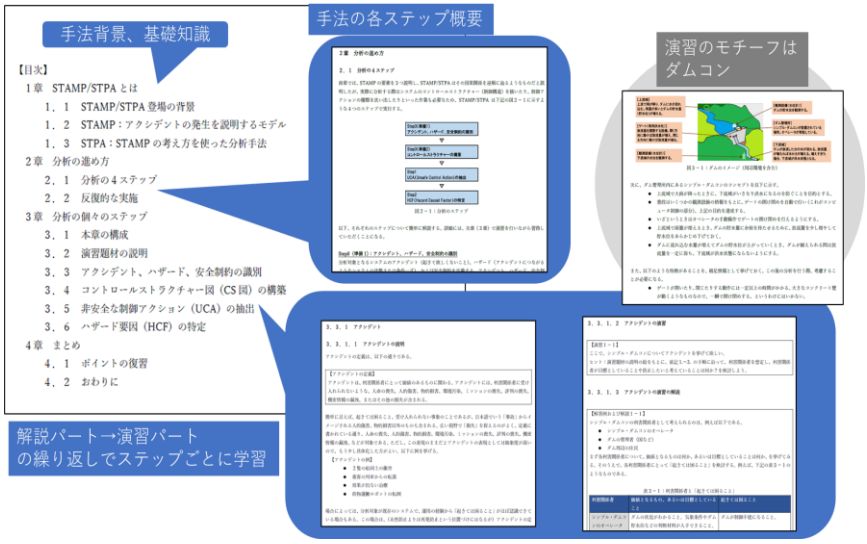
付録2: 事例4「STAMP/STPA教育コンテンツの作成」

1. 適用した事例

STAMP/STPAの社内標準化を推進するため，作成した2つの教育コンテンツ（チュートリアル、座学教育（テキスト））について、分科会メンバからのフィードバックを反映することでブラッシュアップを図った。

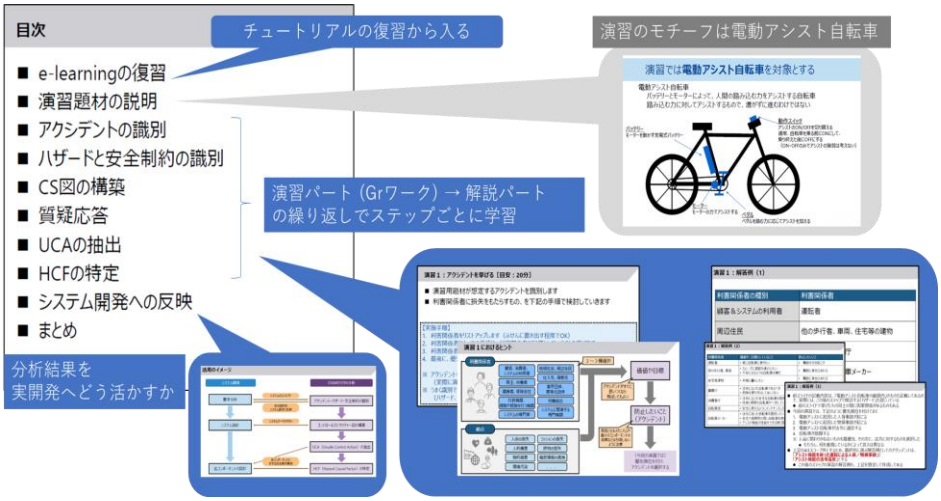
2. チュートリアル

チュートリアルは、背景となる考え方および、基礎知識を説明した上で、手法の各ステップに従って解説パートと演習パートを繰り返すことで学習する。



3. 座学教育

座学教育は、教師対面型となり、チュートリアルの復習から入り、手法の各ステップに従って受講者のグループワーク演習と教師の解説パートを繰り返すことで学習する。最後に分析結果を実際の開発へどのように活かすかについても触れる。



4. 分科会からのフィードバック結果

各コンテンツについて理解度、有益度の両面で4段階評価のうち分科会メンバの75%以上の方が上位2段階評価を付けた。自由記述のコメントから具体事例を使って演習をする形式が学習効果を高めやすくなっている点が確認できた。座学教育は、テキストのみの確認となり、教師からの説明による補足を前提としている部分があることからチュートリアルに比べて評価が低くなった。座学教育で演習モチーフに選択した電動アシスト自転車に対し、チュートリアルではダム管理用制御処理設備（ダムコン）を選択したが、むしろ身近でないダムコンの方が進めやすかったというコメントが複数あった。新規開発のような場面でもSTAMP/STPAが有効活用できるという感触が得られた。

5. おわりに

分科会メンバから得たフィードバックから記載した受講目的の明確化、手法の一般定義との整合強化、演習の説明と回答例の粒度統一を実施し、教育コンテンツのブラッシュアップを図ることができた。今後教育コンテンツを社内公開し、STAMP/STPAの社内標準化推進に活用していく。

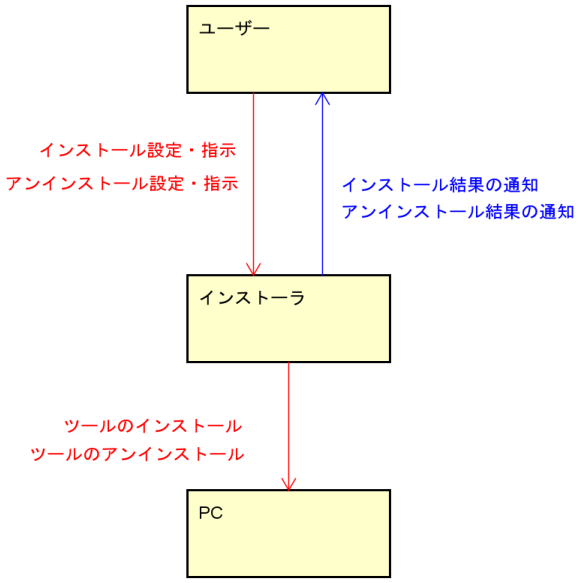
付録3:事例5 「STAMP/STPAによる不具合分析となぜなぜ分析の比較」

1. 適用した事例

設計ツールのインストーラが原因で発生した過去流出不具合に対して、STAMP/STPAを用いて安全分析を実施する。また、STAMP/STPAの分析結果となぜなぜ分析結果を比較することで、分析結果を評価する。

2. 分析結果

コントロールストラクチャー図、UCAの抽出結果を以下に示す。



From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
ユーザー	インストーラ		インストール未実施	(UCA1-P-1) 誤った設定でインストールを実施 [SC1]		
ユーザー	インストーラ		アンインストール未実施	(UCA2-P-1) 誤った設定でアンインストールを実施 [SC3]		
インストーラ	PC		インストーラを実行したが、インストールされない	(UCA3-P-1) インストーラが、ツールが使用する領域外にデータを書き込む [SC2]		書き込み中にタイムアウトと判定され、インストール前の状態に復帰 (UCA3-D-1) 書き込み中にタイムアウトと判定され、処理を中断
インストーラ	PC		アンインストーラを実行したが、アンインストールされない	(UCA4-P-1) アンインストーラが、インストールした領域外のデータを削除する [SC4]		削除中にタイムアウトと判定され、アンインストール前の状態に復帰 (UCA4-D-1) 削除中にタイムアウトと判定され、処理を中断

抽出したUCAは、インストーラの不具合によってデータを破壊するケースと考えられる。この結果を別途実施したなぜなぜ分析結果と比較した。

3. 感想・考察

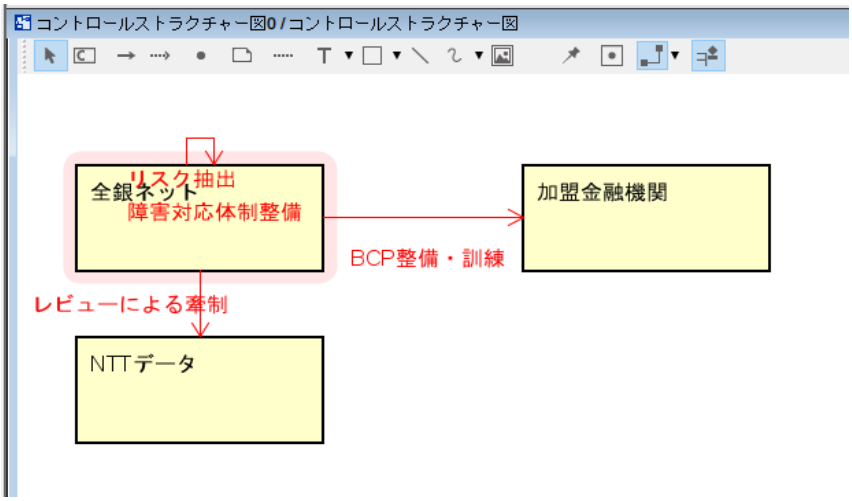
STAMP/STPAを用いた安全分析を実施することで、インストーラによってデータを破壊するケースに、インストール時とアンインストール時があることが導けた。一方、なぜなぜ分析は、アンインストール時に不具合が発生したという事実から分析をスタートしているため、インストール時という観点は表れなかった。様々な観点を広く抽出したい場合に、STAMP/STPAは有効であると感じた。
しかし、STAMP/STPAで抽出したシナリオは抽象度が高く、具体化して対策を立てるには経験・能力が必要と感じた。この点は、具体的なシナリオを抽出できるなぜなぜ分析の方が有効であると感じた。

付録4: 事例6「STAMP/STPAによる障害分析」

1. 適用した事例

2023年12月01日付 全国銀行資金決済ネットワークとNTTデータ連名のプレスリリース「全国銀行データ通信システムの障害について」および関連の報道記事を元にSTAMP WorkBenchを用いた分析を試みた。

2. Step0



手法に沿ってアクシデント・ハザード・安全制約を識別し、登場人物を抽出した。

コントロールアクションの定義を元に、自動生成されたコントロールストラクチャー図を右に示す。

プレスリリースを元にしたため、**システム構造の記述や組織の内部構造(品質保証部門の存在等)の記述ではなく、会社単位の荒い記述しか抽出できなかった。**

3. Step 1

同じく手法に沿ってUCA(Unsafe Control Action)を抽出したが、Not Providing以外のUCAが抽出できなかった(図は省略)。

これは、**コントロールアクションが荒いものになっていたため、処理のタイミングに起因するUCA等の抽出に至らなかった**ものと考える。

4. Step 2

HCF表を作成した。ヒントワードとして「(1)Not Providing(指示が出ない)」など、**「IPA-(組織)対(組織)」を用いたことで、機会の欠陥と違い組織の問題のヒントとして使いやすかった。**


対策表 / 対策表

HCFID	HCF	対策ID	対策	UCA	対策対象コンポーネ...
HCF1-N-1-1	基準が曖昧で指示出さない	M1	ベンダーマネジメント力の向上	(UCA1-N-1) レビュー不足により欠陥仕様が除去されない	全銀ネット
HCF1-N-1-1	基準が曖昧で指示出さない	M2	移行方法・リスク洗い出し方法・優先順位・復旧策・タイムマネジメントのマニュアル化	(UCA1-N-1) レビュー不足により欠陥仕様が除去されない	全銀ネット
HCF2-N-1-1	リスク対応が必要という認識の欠如	M3	障害発生時のマニュアル化	(UCA2-N-1) リスク認識が不充分で体制が取られていない	NTTデータ 全銀ネット
HCF2-N-1-1	リスク対応が必要という認識の欠如	M4	実践的な訓練の実施	(UCA2-N-1) リスク認識が不充分で体制が取られていない	NTTデータ 全銀ネット
HCF4-N-1-1	責任者/担当者スキル不足で放置	M5	コンチプラン・代替手段を想定したBCPの策定	(UCA4-N-1) 障害発生時に取りうるBCPが検討されていない	NTTデータ 全銀ネット 加盟金融機関
HCF4-N-1-1	責任者/担当者スキル不足で放置	M6	訓練の実施とBCP運用ルール強化	(UCA4-N-1) 障害発生時に取りうるBCPが検討されていない	NTTデータ 全銀ネット 加盟金融機関

HCFを元に対策表を作成し、プレスリリースに記載されていた「対策」をマッピングした(この過程でHCFが新たに洗い出されたものがある)。

また、同じHCFに複数の対策が当てはまるが、記載が重複しているものがあり、**STAMP Workbenchで流れを整理してみると対策の整合性や抜け漏れが可視化しやすいと感じた。**

5. おわりに

プレスリリースの情報を元に、技術解説記事の情報を織り込んで分析するつもりだったが、プレスリリースを軸にすると技術論やその対策が登場しないためうまく織り込めなかった(C言語のlong長が変わったため確保メモリ領域からインデックステーブルが溢れたことでデータ破壊が発生した件)。

技術解説記事や事故報告書の内容を分析したほうがSTAMP Workbenchの特性を活かせた可能性がある。

実業務に直結する障害情報を元にした分析ができなかったため業務活用性の評価はできなかったが、**障害報告書を読み解く際に情報を整理する**ことにも一定程度使えると感じた。

参考文献: 「全国銀行データ通信システムの障害について」 全国銀行資金決済ネットワーク、NTT データ 2023年12月01日
https://www.zengin-net.jp/announcement/pdf/announcement_20231201.pdf

付録5：事例7「過去発生障害に対するCASTを用いた分析」

1. 適用した事例
過去に発生した障害を題材としてCASTを用いた分析を試みた。
分析については以下のCAST分析プロセスにて実施した。

2. STEP１．基本情報の把握（基本情報の収集）

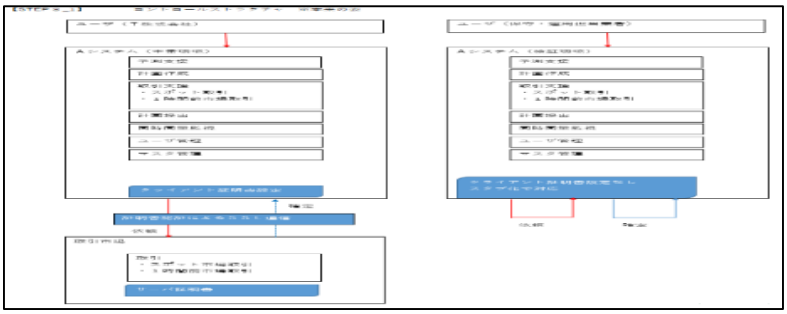
障害が発生したシステムの情報収集と分析を実施する範囲を定義し、識別したハザードからハザードを防止するために必要なシステムレベルの安全制約を特定した。
※特定したのは「アクシデント」、「ハザード」、「安全制約」の3点。
＜分析対象障害＞
障害発生後、暫定対応テストにおいて検証環境から本番環境に誤って接続を行いテストデータを投入するインシデントが発生。
※作業時の工夫としては、CAST分析で分析で使用している用語が分かりづらい為、用語の再定義を行い分析作業がスムーズに実施出来るようにした。
・アクシデント：望んでもいないし計画もしていない、損失につながるようなイベント
　→「重大障害／回避すべき損失」と定義ロ
・ハザード：システムを取り巻く環境が最悪な条件と重なることで、アクシデントにつながる状態
　→「システムにとって危険な状態」と定義

3. STEP２．具体的事象（物理モデルの分析）

STEP１で特定した3点（アクシデント、ハザード、安全制約）を基に具体的なコンポーネントに対して安全上の責務（責任）、非安全なコントロールアクション、プロセス／メンタルモデルの欠如、意思決定された状況・背景に置き換えて分析を行った。

4. STEP３．安全コントロールストラクチャの作成

対象システムにおけるコントロールストラクチャを記述した。



5. STEP４．抽象事象（論理モデルの分析）

コンポーネント単体ではなく、複数のコンポーネントが関わり合って発生した事象を抽象的事象と捉え「STEP２.」で実施した具体的なコンポーネントでの分析と同様に分析を実施した。

6. STEP5．システム全体の整合（欠陥特定）

「具体的コンポーネントレベルでの分析」、「抽象的コンポーネントレベルでの分析」結果から今回の障害事例の特徴と分析から見える弱点を分析し改善案を検討した。

7. おわりに

自社では「なせなせ分析」による障害分析が主流となっているが本分析手法も障害分析手法の1つとして実施可能なことが実践を通して実感できた。
今回のCAST分析実施によりCASTに対する理解は深まった。今後は実践を多く積む事で「なぜなぜ分析」と使い分けを行いたい。

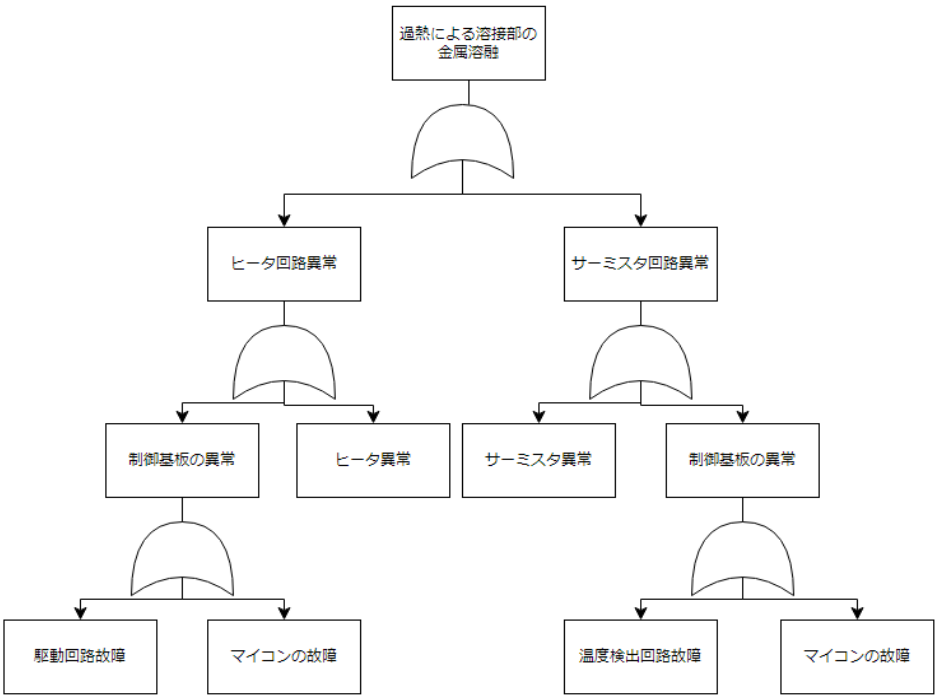
付録6：事例8「FTAを用いた製品安全に関する脅威の可視化」

1. 適用した事例

第三者認証機関に対し、製品安全に関する規格適合性の認証試験を依頼した。
試験にあたり製品の危険と、その危険に対しどういった対策を打ったのか示す必要がある。
本事例ではFTAを用いてそれらを可視化した。

2. Step0(危険の可視化)

製品の危険源をFTAを用いて可視化した。以下が機密に関する情報を除いた例の一部である。



3. Step 1(対策の可視化)

step0で可視化した故障に対し、
・どういった故障モードがあるか
・各故障モードでの製品の挙動
・製品として打った対策
以上3点を表形式でまとめた。以下が機密に関する情報を除いた表の一部である。

◆安全機能による異常検知

			単一故障時の挙動	危険事象	安全機能による異常検知	判定
ポート保護抵抗故障(R48)	短絡故障	→	問題なく動作	危険とならない	なし	○
	開放故障	→	ヒータ常時OFF	危険とならない	GAS01、GAS02	○
フォトカプラ(発光側)(PT1)	短絡故障	→	問題なく動作	危険とならない	なし	○
	開放故障	→	問題なく動作	危険とならない	なし	○
トランジスタ故障(QR3)	E-C間短絡故障	→	ヒータ常時全波通電	過熱	VAP01	○
	E-B間短絡故障	→	ヒータ常時OFF	危険とならない	GAS01、GAS02	○
	C-B間短絡故障	→	ヒータ常時OFF	危険とならない	VAP01	○
	開放故障	→	ヒータ常時OFF	危険とならない	GAS01、GAS02	○

4. おわりに

本事例で作成したFTA図を用いて、規格適合性の試験を合格することができた。
脅威とその対策の表現手法としてFTAが有効であると示せたと考える。

付録7：事例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」

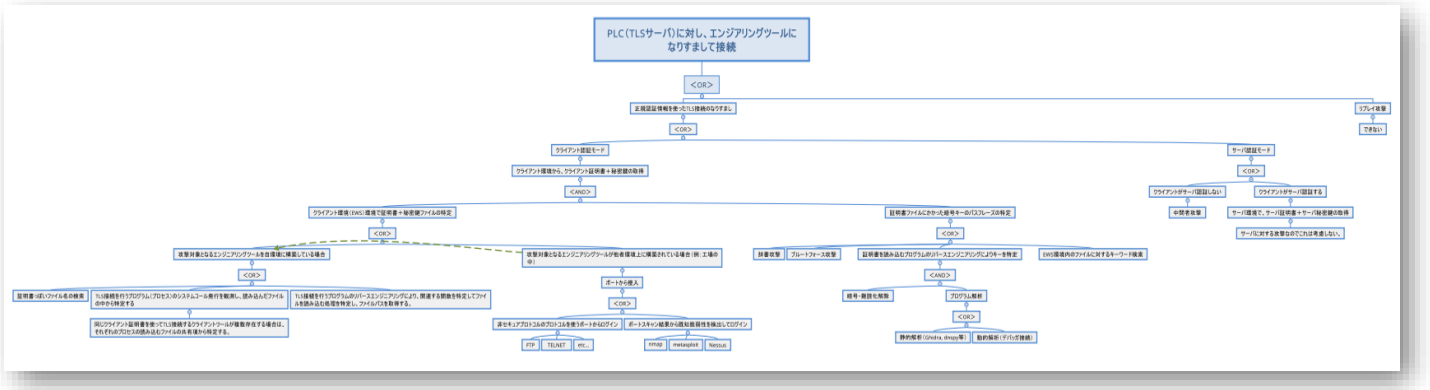
1. 適用した事例

組織内部のネットワークでサーバ/クライアントモデルのソフトウェアサービスを攻撃対象とし、サーバに対して正規クライアントをなりすますことを攻撃目標と置いた。
この場合における攻撃構造について、ATAを用いて分析し、可視化した。

前提：
- ・サーバ/クライアントは同一サブネットに存在し、TLSプロトコルで通信している。
- ・攻撃者は、ユーザ環境のサーバ/クライアントと同一サブネット上の別マシンからネットワーク経由で攻撃を行う。
- ・攻撃者は、同様のサービスを自ら購入し、同様の実行環境を自身が管理マシン上で実行可能である。（サービスの共通機能に対する解析が可能）

2. 実施結果

対象サービスに対して考えられる攻撃をATAを用いて可視化した。下記は、作成したATAの全体図である。



3. 所感

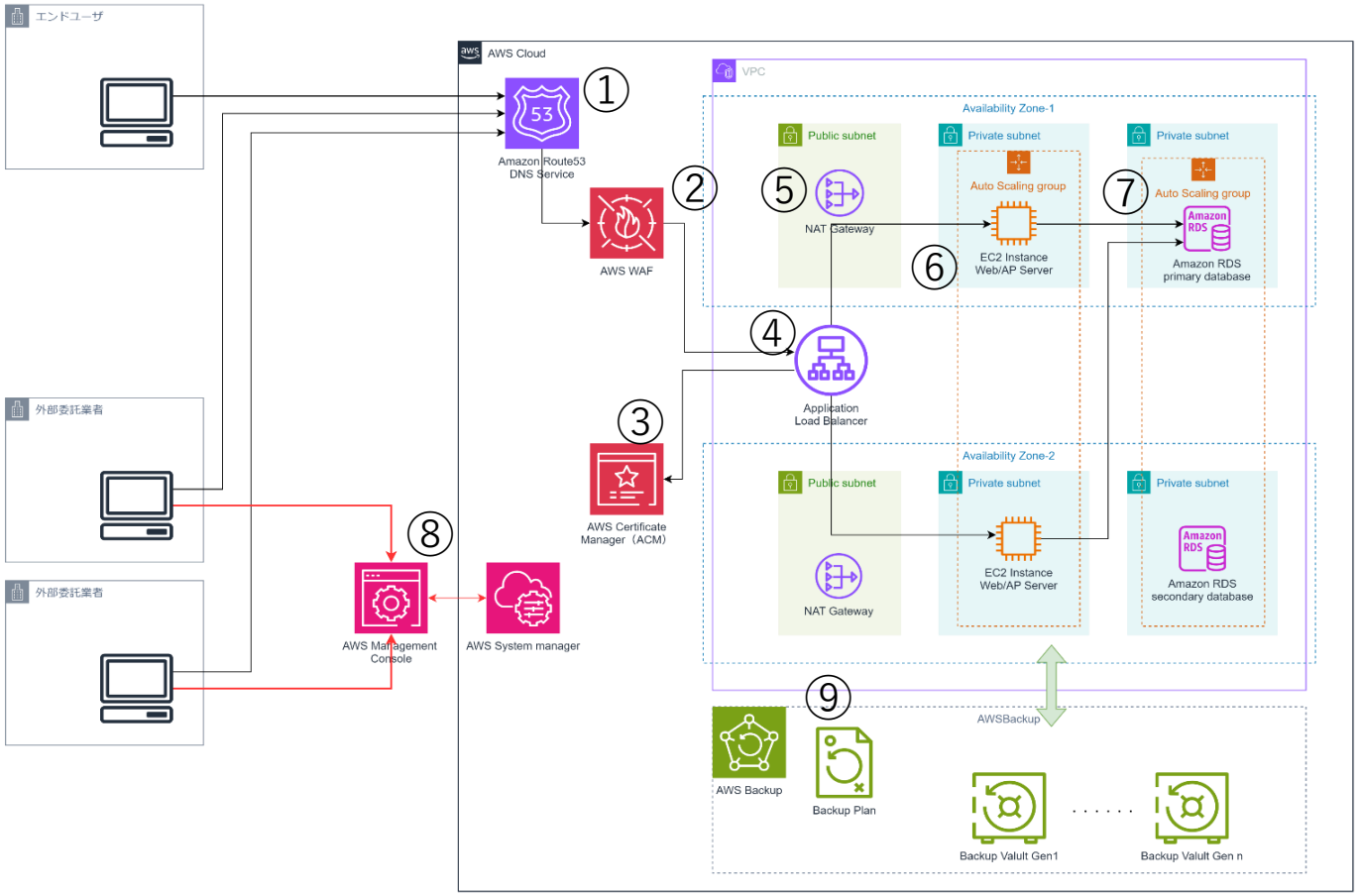
<メリット>
1つの具体的な攻撃に対し、その構造を木構造で可視化でき、攻撃の構造を整理できた。
期の作成過程において、記入中の木を俯瞰し、不足する攻撃ルートに気づくことができたため、全貌がわかっていない攻撃に対してその構造を検討する際にも有用であることを実感できた。
ANDとORの攻撃要素間の関係性を記載するため、最終的に攻撃を達成するために必要な条件を整理することもできた。このため、対策を考える際、必要箇所を絞って対策することを検討しやすくなったと感じた。

<デメリット（難しかった点）>
どのような攻撃が考えられるかわかり切っていない場合、攻撃の時系列（流れ）を考える方が攻撃を想像しやすいことがあった。
しかし、ATAは時系列を表現することをフレームワークとして担保しているわけではないため、時系列で考えた方がわかりやすいことと達成条件(AND, OR)で整理した方がわかりやすいことの共存して表現することが難しかった（今回はできなかった）。
両者を同時に表現できると、より攻撃構造をわかりやすく表現できるのではないかと感じた。

4. おわりに

ATAを用いて、サーバ/クライアントモデルのソフトウェアサービスに対する攻撃構造の分析、および可視化を行った。
要素的な攻撃行動のどれが成立した際に攻撃が有効となるか整理できる一方、攻撃行動の時系列の表現には作成者の工夫が必要であり、木の作成過程において整理に混乱する場面があった。
条件と時系列で図を分けた場合、図の間の対応関係を保つコストが発生するため、1度に表現可能な図があると現場で更に有用であると感じた。

付録８：事例１「STAMP/STPA を用いたWeb システムのセキュリティ要件分析」
分析対象となるWebアプリケーションのアーキテクチャ



① Route53を使って静的・動的なWeb クライアントからのリクエストのルーティング を行います。

② AWS WAFのようなアプリケーションファイア ウォールによって一般的なWeb脆弱性攻撃 からWebアプリケーションを守ります。

③ ACMにより、TLS証明書をシンプルに管理 します。

④ インターネットに面したアプリケーションロード バランサーはWebトラフィックと複数のAZに 割り振ります。

⑤⑥ パブリックサブネットに配置されたNATゲート ウェイはプライベートサブネットにあるEC2イン スタンスにインターネットからのアクセスを中継 します。

⑦ DB層はAmazon RDSによるシンプルな DB管理により行います。

⑧ 開発時のサーバの保守や資産の導入/各種 設定などは、AWS Management Console から作業を行います。

⑨ バックアップについては、Backup Planに従い、 データが保存されます。（左図のBackup Valut が該当）

付録9：事例１「STAMP/STPA を用いたWeb システムのセキュリティ要件分析」

UCA表（抜粋）

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	サービス利用の申し込み/変更/解約	エンドユーザー	システムオーナー	エンドユーザによるサービス申し込み時	(UCA1-N-1) サービス変更/解約が届かない [SC7] サービス申し込みが届かない	(UCA1-P-1) サービス申し込みがの内容が誤っている [SC7]	(UCA1-T-1) サービス変更/解約の通知が届くのが遅延し、無効/不正なアカウントでアクセス可能 [SC7] 利用申し込み手続きの遅延	(UCA1-D-1) サービス変更/解約に時間がかかり、無効なアカウントでのアクセスが可能 [SC7] サービス利用申し込みの承認が遅延しサービスが利用開始が遅延
2	アドレスの問い合わせ	エンドユーザー	AWS Route53	エンドユーザによるシステムに対するアクセス時	(UCA2-N-1) DNSによるアドレス解決が出来ない [SC6]	(UCA2-P-1) DNSから誤ったアドレスが与えられる [SC6]	(UCA2-T-1) DNSの応答が遅すぎる [SC6]	-
3	Httpsアクセス	エンドユーザー	AWS WAF	システムに対するWebアクセス時	(UCA3-N-1) WAFが停止する [SC6]	(UCA3-P-1) WAFが正常な通信を異常と誤検知 [SC6] (UCA3-P-2) 不正な入力(SQL入りの入力データなど)が検知されない [SC12][SC13]	(UCA3-T-1) WAFの応答が遅すぎる [SC6]	-
4	報告する	外部委託業者	システムオーナー	外部委託業者によるオーナーへの報告時	(UCA4-N-1) 問題や各種報告がなされないことによって、発生した問題を認識することが出来ない [SC13][SC2]	(UCA4-P-1) 誤った報告により、問題を誤認する [SC13][SC2]	(UCA4-T-1) 遅すぎる報告により、問題の認識も遅れ、問題の影響を大きくしてしまう [SC13][SC2]	-
5	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	(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]	(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]	(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]	-
6	アドレスの問い合わせ	外部委託業者	AWS Route53	外部委託業者によるシステムに対するアクセス時(動作確認、テスト実施など)	(UCA6-N-1) DNSによるアドレス解決が出来ない [SC6]	(UCA6-P-1) DNSにより、誤ったアドレスが与えられる [SC6]	(UCA6-T-1) DNSからの応答に時間がかかりすぎてエラーになる [SC6]	-
7	Httpsアクセス	外部委託業者	AWS WAF	外部委託業者によるWebアクセス時(動作確認、テスト実施など)	(UCA7-N-1) WAFが応答しない [SC6] (UCA7-N-2) WAFの誤検知により、正常な通信が拒否される。 [SC6]	-	(UCA7-T-1) WAFの応答が長すぎてタイムアウト [SC6]	-
8	依頼する	システムオーナー	外部委託業者	システムの修正、仕様変更依頼時	(UCA8-N-1) 作業依頼が業者に届かない [SC3][SC4]	(UCA8-P-1) 誤った作業依頼が連絡される。 [SC3] (UCA8-P-2) 正規の権限を持たない人から指示が行われる。(統制の不備、内部犯、あるいはなりすましによる問題) [SC3]	(UCA8-T-1) 作業準備に十分な余裕のないタイミングでシステム停止を伴う依頼が届く(運用時間における即時依頼等) [SC6]	(UCA8-D-1) 保守の時間内に作業できるタイミングでシステム停止を伴う作業依頼が確認されない/受理されない [SC6]
9	設定をする	システムオーナー	AWS Management Console	システムオーナーによるシステム操作者(外部委託業者、システムオーナー)のユーザーメンテナンス、権限設定等を行う場合	(UCA9-N-1) システムオーナーが離職者や、離任者などのユーザ削除しない。 [SC3][SC4][SC8][SC9] (UCA9-N-2) システムオーナーによる利用者の権限設定が行われない。 [SC3][SC4][SC8][SC9]	(UCA9-P-1) システムオーナーが利用者のメンテナンスを誤ってしまう。(追加、削除、変更) [SC3][SC4][SC8][SC9] (UCA9-P-2) システムオーナーが利用者の権限設定を誤ってしまう。 [SC3][SC4][SC8][SC9] (UCA9-P-3) 内部犯によるによる不正アクセス [SC12][SC13][SC8][SC9]	(UCA9-T-1) システムオーナーによる利用者のメンテナンスが、変更日よりも早い/遅い [SC3][SC4][SC8][SC9]	-
10	アドレスの問い合わせ	システムオーナー	AWS Route53	システムオーナーによるシステムに対するアクセス時(オーナーによる受け入れのための動作確認時)	(UCA10-N-1) DNSによるアドレス解決が出来ない [SC6]	(UCA10-P-1) DNSから誤ったアドレスが与えられる [SC6]	(UCA10-T-1) DNSの応答が遅すぎる [SC6]	-
11	Httpsアクセス	システムオーナー	AWS WAF	システムオーナーによるWebアクセス時(オーナーによる受け入れのための動作確認時)	(UCA11-N-1) WAFが応答しない [SC6] (UCA11-N-2) WAFの誤検知により、正常な通信が拒否される。 [SC6]	-	(UCA11-T-1) WAFの応答が長すぎてタイムアウト [SC6]	-
12	httpsアクセス	AWS WAF	Application Load Balancer	エンドユーザ/システムオーナー/外部委託業者などによるWebアクセス時(WAFを通過後)	(UCA12-N-1) ALBが応答しない [SC6]	(UCA12-P-1) ALB上のTLS証明書が期限切れなので、クライアントブラウザでエラー表示 [SC6] (UCA12-P-2) ALBのTLS暗号スイートが脆弱なものを含んでおり、解読可能 [SC12][SC13]	(UCA12-T-1) ALBの応答が長すぎてタイムアウト [SC6]	-
13	各サーバの操作	AWS Management Console	AWS System manager	DBやWebサーバなどのメンテナンスの為のリモート操作時	(UCA13-N-1) System Managerが応答しない [SC6]	-	(UCA13-T-1) System Managerの応答が長すぎて、タイムアウト [SC6]	-
14	DNSサーバの各種操作	AWS Management Console	AWS Route53	システムのFQDNと関連する属性情報(IPアドレス、TLS証明書設定字のシステム保有認証をするためのTXTレコードなど)を設定する時	(UCA14-N-1) DNSレコードのメンテナンスが出来ない [SC3][SC5][SC6]	(UCA14-P-1) DNSレコードの設定を誤ってしまう。 [SC12][SC13][SC3][SC4][SC5][SC6][SC7][SC8][SC9]	-	(UCA14-D-1) DNSの反映が間に合わずアクセスに失敗する [SC6] (UCA14-D-2) DNSの反映が間に合わず、誤った接続先に接続される [SC12][SC13][SC6]
15	WAFの作成/設定/削除	AWS Management Console	AWS WAF	WAFに対するメンテナンス(作成、検知ルールの設定など)時	(UCA15-N-1) メンテナンスが行われないことによる不適切な動作(誤検知、あるいは検知失敗) [SC12][SC13][SC6][SC7]	(UCA15-P-1) メンテナンスの間違いに伴う不適切な動作(誤検知、あるいは検知失敗) [SC12][SC13][SC6][SC7]	-	-
16	Application Load Balancerの作成/設定/削除	AWS Management Console	Application Load Balancer	システムを構成する複数のWebサーバのアドレス情報のメンテナンス時	(UCA16-N-1) ALBの操作に失敗する。 [SC6]	(UCA16-P-1) ALBの操作を誤る [SC6]	-	-
17	TLS証明書の登録/削除	AWS Management Console	AWS Certificate Manager	ステージング環境用のTLS証明書(DV)の作成時	(UCA17-N-1) DVの設定が出来ない(=テストによる確認が出来ない) [SC3][SC6]	(UCA17-P-1) DVに関する設定の誤り [SC3][SC6]	(UCA17-T-1) DV証明書の適用が遅延し、証明書が失効する [SC3][SC6]	-
18	EC2サーバの作成/起動/停止/削除	AWS Management Console	EC2サーバ(Web/APサーバ)	Webサーバの起動、停止、作成、削除のメンテナンス時	(UCA18-N-1) EC2サーバの操作が出来ない [SC3][SC6]	(UCA18-P-1) 誤ってEC2サーバを削除してしまう。 [SC6]	-	-
19	RDSサーバの作成/起動/停止/削除/メンテナンス	AWS Management Console	RDS(データベースサーバ)	DBサーバの起動、停止、作成、削除、スナップショットへの復元などのメンテナンス時	(UCA19-N-1) RDSサーバの操作が出来ない [SC3][SC6]	(UCA19-P-1) RDSサーバを誤って削除してしまう [SC3][SC6]	-	-
20	バックアップスケジュールの設定	AWS Management Console	AWS Backup	バックアップの世代数、ルール等の設定時	(UCA20-N-1) バックアップスケジュールが設定出来ない [SC3][SC9]	(UCA20-P-1) バックアップ設定を誤ってしまう。 [SC3][SC9]	-	-
21	リカバリの指示	AWS Management Console	AWS Backup	バックアップからシステムを復元する時	(UCA21-N-1) リカバリ操作が出来ない [SC12][SC3][SC6]	(UCA21-P-1) 誤ったバックアップデータによりサーバが復元される [SC3][SC6] (UCA21-P-2) バックアップデータが不正に削除される。 [SC3][SC6] (UCA21-P-3) 不正アクセスによるバックアップデータの漏えい [SC9]	(UCA21-T-1) リストアに時間がかかりすぎてしまいサービスが復旧しない [SC6]	
22	httpアクセス	Application Load Balancer	EC2サーバ(Web/APサーバ)	エンドユーザ/システムオーナー/外部委託業者などによるWebアクセス時(ALBを通過後)	(UCA22-N-1) WebAPサーバが応答しない [SC6]	-	-	-
23	TLS証明書の更新	AWS Certificate Manager	Application Load Balancer	ステージング環境用のTLS証明書(DV)の有効期限切れに伴う更新時	(UCA23-N-1) ALBが証明書の変更を受け付けないため、証明書が失効する [SC2][SC6]	-	-	-
24	リモート操作(ssh/rdp)	AWS System manager	EC2サーバ(Web/APサーバ)	外部委託業者等によるシステム保守/運用のためのサーバ操作時	(UCA24-N-1) EC2サーバがリモート保守を受け付けない [SC4][SC6][SC7]	(UCA24-P-1) 不正アクセスによりログなどが持ち去られる。 [SC10][SC8]	-	-
25	データベースサーバの操作	AWS System manager	RDS(データベースサーバ)	外部委託業者等によるシステム保守/運用のためのDBサーバ操作(マスタメンテナンス、保守作業など)時	(UCA25-N-1) RDSが応答しない [SC3][SC6]	(UCA25-P-1) RDSの脆弱性悪用などによる不正アクセス [SC12]	-	-
26	データベースアクセス	EC2サーバ(Web/APサーバ)	RDS(データベースサーバ)	Webアクセス時のデータ参照/更新時	(UCA26-N-1) DBサーバが応答しない [SC6]	-	-	-
27	バックアップ/リストア(EC2)	AWS Backup	EC2サーバ(Web/APサーバ)	バックアップスケジュールに基づいたWebサーバのバックアップおよびリストア操作時	(UCA27-N-1) バックアップが行われない [SC6]	(UCA27-P-1) リストアに失敗する [SC3][SC6] (UCA27-P-2) RPO以降のデータ(ログ等を含む)の喪失 [SC3][SC6][SC9]	(UCA27-T-1) リストアに時間がかかりすぎてしまい、オンラインサービスが再開できない。 [SC6]	-
28	バックアップ/リストア(RDS)	AWS Backup	RDS(データベースサーバ)	バックアップスケジュールに基づいたDBサーバのバックアップおよびリストア操作時	(UCA28-N-1) バックアップが行われない [SC6]	(UCA28-P-1) リストアに失敗する [SC3][SC6] (UCA28-P-2) RPO以降のデータ(ログ等を含む)の喪失 [SC4][SC6][SC9]	(UCA28-T-1) リストアに時間がかかりすぎてしまい、オンラインサービスが再開できない [SC6]	

付録10：事例１「STAMP/STPA を用いたWeb システムのセキュリティ要件分析」

HCF/SCF表（UCA5-N-1対応箇所）

ID	HCF	ヒントワード	シナリオ
HCF5-N-1-1	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	(9) プロセスへの入力が欠けているか間違っている	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、アカウントのID,ユーザID,あるいはユーザパスワードを失念し、ログインが出来ない
HCF5-N-1-2	AWS Management Consoleにログインするために必要なトークンを紛失、あるいは破損してしまい、ログインすることが出来ない	(9) プロセスへの入力が欠けているか間違っている	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,パスワードを入力する 保守作業者は、ワンタイムパスワードを入力しようとするが、MFAトークンが壊れた、あるいは紛失した等により、入力が出来ず、ログイン出来ない。
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	保守作業者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はログイン後、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は、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の共有がなかった。 保守作業者B（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Bは、変更後のパスワードをしらないので、AWS Management Consoleにログインすることが出来ない。
HCF5-N-1-5	成りすましによって、アカウントが乗っ取られてしまい、正規の利用者（保守作業者）がログイン出来ない	(16) Spoofing Identify ：なりすまし	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。 攻撃者は管理権限を持つIAMユーザ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、ログインをできなくする 保守作業者（外部委託業者、あるい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パスワードの変更、あるいはアカウントロックアウトによりログインに失敗する
HCF5-N-1-6	保守作業者（外部板城業者、あるいはシステムオーナー）の環境から通信が出来ないことによってログイン画面を行うことが出来ない	(8) 不適切、有効でない欠けたコントロールアクション	保守作業者（外部板城業者、あるいはシステムオーナー）がAWS Management Consoleのログイン画面へ接続を試みるネットワーク障害、通信機器故障等の原因により、AWSに接続が出来ず、ログインに失敗する

付録11：事例１「STAMP/STPA を用いたWeb システムのセキュリティ要件分析」

対策表（抜粋）

HCFID	HCF/SCF	方針	エラー着想手順	対策	UCA	対策対象コンポーネント
HCF2-T-1-1	DNSサーバに対してDoS/DDoS等による不正なアクセスが集中し、応答が遅延する	共有	② できないようにする	AWS ShieldによるDoS/DDoS対策をベースとすることとする。	(UCA2-T-1) DNSの応答が遅すぎる [SC6]	AWS Internet Gateway
HCF1-N-1-1	エンドユーザの利用者アカウントのメンテナンス依頼が漏れる	軽減	③ わかりやすくする	マニュアルに、主要ユースケースに基づく操作内容などを示し、確実な操作ができるように促す	(UCA1-N-1) サービス変更/解約が届かない [SC7]	システムオーナー 外部委託業者
HCF1-D-1-1	一時期に大量の利用契約の申し込みや解約などの依頼が来たことにより、メンテナンスが遅延し、アカウントの解約が遅延する	軽減	① やめる	利用申し込みに関する変更/解約を自動化し、人手での作業をなくすことによって遅延を防ぐ	(UCA1-D-1) サービス変更/解約に時間がかかり、無効なアカウントでのアクセスが可能 [SC7]	システムオーナー 外部委託業者
		軽減	③ わかりやすくする	受け付けたアカウントによる操作を自動的に監視対象に追加し、アクションがあった場合は通知が出るようにする。		システムオーナー 外部委託業者
		軽減	④ やりやすくする	アカウントの削除の前にロックアウトをするまでは利用者にやってもらうことで不正なシステムアクセスが出にくくする。		エンドユーザー
		軽減	⑪ 被害に備える	SIEMなどにより不正アクセスの有無、操作内容を後で確認できる仕組みづくり		システムオーナー 外部委託業者
HCF1-D-1-2	変更/解約などに関する届け出書類が誤っており、受理に時間がかかってしまう。	軽減	③ わかりやすくする	変更、解約をオンライン化し、エラーチェックを行うことで誤った届け出が出にくくする。	(UCA1-D-1) サービス変更/解約に時間がかかり、無効なアカウントでのアクセスが可能 [SC7]	システムオーナー 外部委託業者
HCF5-N-1-1	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 外部委託業者
HCF5-N-1-2	AWS Management Consoleにログインするために必要なトークンを紛失、あるいは破損してしまい、ログインすることが出来ない	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。	(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
		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、あるいは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。		システムオーナー
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	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。	(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
		軽減	⑨ 自分で気づかせる	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		システムオーナー 外部委託業者
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	軽減	⑩ エラーを検出する	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場合は、運用担当者へメールで通知がいくように設定をする。	(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 外部委託業者
		軽減	⑪ 被害に備える	ルートユーザのパスワード紛失時に備えて、アカウント回復手順のための秘密の質問を設定し、問題発生時の復旧手順を用意する。		システムオーナー 外部委託業者
HCF5-N-1-5	成りすましによって、アカウントが乗っ取られてしまい、正規の利用者(保守作業者)がログイン出来ない	軽減	② できないようにする	パスワードのポリシー(文字数、文字種、世代数など)を設定し、安易に解読されない程度にパスワードを難解なものとするように強制する。	(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]	AWS IAM
		軽減	② できないようにする	IAMユーザ、ルートユーザのログインの接続元IPアドレスを設定し、特定の場所以外からのログインを許可しない運用にする。		AWS IAM
		軽減	⑩ エラーを検出する	IAMユーザ、ルートユーザのMFA未設定ログインを監視し、問題のあるログインを検知した場合は、MFA登録をするように促す運用をする。		AWS IAM
HCF5-N-1-6	保守作業者(外部板城業者、あるいはシステムオーナー)の環境から通信が出来ないことによってログイン画面を行うことが出来ない	軽減	⑪ 被害に備える	ネットワーク障害時に備えた復旧に備えた連絡先の整備(通信業者やNW機器の保守業者の連絡先リスト)、および復旧マニュアルを用意する。	(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
HCF5-P-1-1	保守作業者(外部委託業者)が開発したアプリケーションの欠陥が含まれている事に気づかずにアプリケーションのデプロイを行ってしまう。	軽減	③ わかりやすくする	資源(リリースの手順を整備し、テストについてのレビューやリリースの為の判定等を行うことを確実にし、品質を保証する。	(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]	外部委託業者
		軽減	⑪ 被害に備える	リリースについては、夜間などシステム利用者が少ないタイミングにシステムを停止して実施することとし、問題発生時の被害を最小限にする。		外部委託業者
		軽減	⑪ 被害に備える	問題発生時の切り戻し手順を準備し、リリースしたモジュールに問題があるとわかった場合は切り戻せるようにする。		外部委託業者
HCF5-P-2-1	パスワードを解析され、不正アクセスを許してしまう。	軽減	② できないようにする	パスワードのポリシー(文字数、文字種、世代数など)を設定し、安易に解読されない程度にパスワードを難解なものとするように強制する。	(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]	AWS IAM
		軽減	② できないようにする	IAMユーザ、ルートユーザのMFA未設定ログインを監視し、問題のあるログインを検知した場合は、MFA登録をするように促す運用をする。		AWS IAM
HCF5-P-3-1	システムのメンテナンス時にアクセス制限の設定を誤り、外部からの不正なアクセスを許してしまう。	軽減	⑩ エラーを検出する	AWS Configにより変更箇所を通知させることとして、適用後にチェックリストに基づいた確認を行う。	(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]	AWS Config
HCF5-P-4-1	メンテナンス時の誤操作により、監視設定を誤ってしまい検知すべき事象を検知できない。	軽減	⑩ エラーを検出する	AWS Configにより変更箇所を通知させることとして、適用後にチェックリストに基づいた確認を行う。	(UCA5-P-4) 誤操作により、誤った検知設定が行われる [SC13]	AWS Config
HCF5-P-5-1	メンテナンス時の誤操作によって、ログを消去してしまう。	軽減	⑪ 被害に備える	S3にログを随時転送することによって、ログを別に保管する。	(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]	S3
HCF5-P-5-2	メンテナンス時に誤ってリストアをする行ってしまい、Webサーバ上のRPO以降のログが消去される	軽減	⑪ 被害に備える	S3にログを随時転送することによって、ログを別に保管する。	(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]	S3
HCF5-P-6-1	利用者のメンテナンス時にアクセス権設定を誤ってしまい、許可されない利用者に強力な権限を与えてしまう。	軽減	⑩ エラーを検出する	AWS Configにより変更箇所を通知させることとして、適用後にチェックリストに基づいた確認を行う。	(UCA5-P-6) アクセス権の設定を間違える [SC3][SC6][SC8][SC9]	AWS Config
HCF5-P-7-1	メンテナンス時にセキュリティグループの設定を誤ってしまい外部からのアクセスが出来なくなる。	軽減	⑩ エラーを検出する	AWS Configにより変更箇所を通知させることとして、適用後にチェックリストに基づいた確認を行う。	(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]	AWS Config
		軽減	⑪ 被害に備える	ログインできない場合に備えて、AWS向けの修正依頼の為に必要な手順を確認しておく。		AWS Support
HCF5-P-7-2	メンテナンス時にネットワークACLの設定を誤ってしまい、外部からのアクセスが出来なくなる。	軽減	⑩ エラーを検出する	AWS Configにより変更箇所を通知させることとして、適用後にチェックリストに基づいた確認を行う。	(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]	AWS Config
		軽減	⑪ 被害に備える	ログインできない場合に備えて、AWS向けの修正依頼の為に必要な手順を確認しておく。		AWS Support
HCF5-P-7-3	メンテナンス時にネットワークACLの設定を誤ってしまい、監視が出来なくなる	軽減	⑩ エラーを検出する	AWS Configにより変更箇所を通知させることとして、適用後にチェックリストに基づいた確認を行う。	(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]	AWS Config
		軽減	⑪ 被害に備える	ログインできない場合に備えて、AWS向けの修正依頼の為に必要な手順を確認しておく。		AWS Support
HCF5-P-7-4	メンテナンスにより、IAMの接続元IPアドレス設定を誤り、外部からのメンテナンスを受け付けなくなる。	軽減	⑩ エラーを検出する	AWS Configにより変更箇所を通知させることとして、適用後にチェックリストに基づいた確認を行う。	(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]	AWS Config
		軽減	⑪ 被害に備える	ログインできない場合に備えて、AWS向けの修正依頼の為に必要な手順を確認しておく。		AWS Support

付録12：事例２「STAMP/STPAを用いたネットワーク機器撤去時の作業リスク抽出」

前提条件一覧

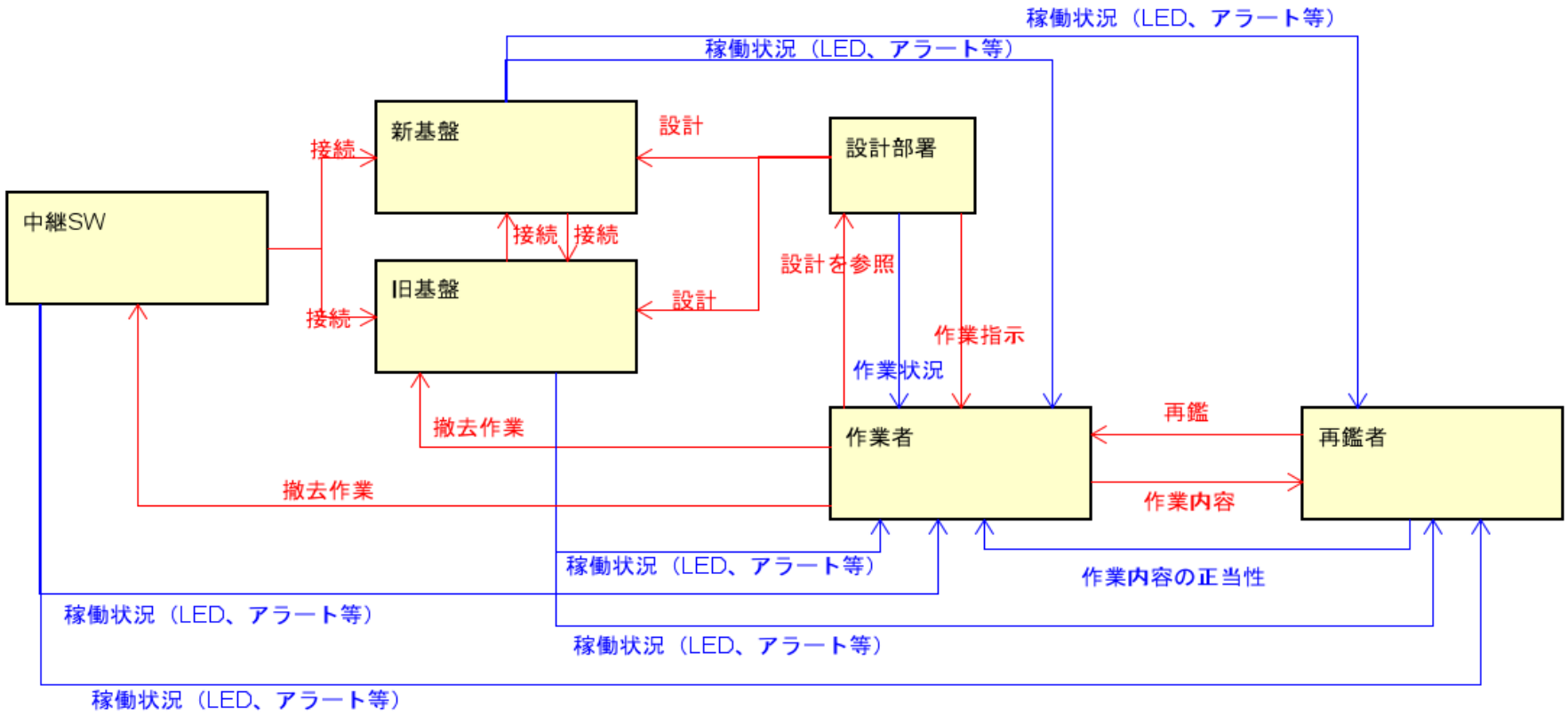
No	名前
1	データセンタ内には現在稼働中の新基盤と、原価低減のため撤去対象である旧基盤の2つの基盤が存在する。 今回は基盤提供時やサービス稼働時全体のSTPA分析ではなく、旧基盤から新基盤への稼働切り替え後の及び機器撤去作業時について分析する
2	エンドユーザはWAN経由で新基盤・旧基盤へアクセスしサービスを利用する
3	作業者の体調不良や他作業都合などの機器撤去できなかった場合などの、稼働状況には影響しない事象は対象外とする

付録13：事例２「STAMP/STPAを用いたネットワーク機器撤去時の作業リスク抽出」
アクシデント・ハザード・安全制約の一覧

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

付録14：事例２「STAMP/STPAを用いたネットワーク機器撤去時の作業リスク抽出」

CS図



付録15：事例２「STAMP/STPAを用いたネットワーク機器撤去時の作業リスク抽出」

UCAの抽出，HCFの特定，および対策検討

HCF	UCA	対策	対策対象 登場人物
撤去対象機器として事前に確認した機器に誤りがある	撤去予定ではない機器が撤去される	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 再鑑者
		再鑑者が作業者の作業を確認する	再鑑者
作業者が作業手順書に存在しない手順を実施する	不正な作業手順が実行される	再鑑者が作業者の作業を確認する	再鑑者
作業前に現地調査を実施していない	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			
設計書に記載された情報が古い			
設計当初の意図を確認せず設計する	設計時の思想とは異なる経路を作成する	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
作業前の影響調査時に確認する設計書が異なる	誤った設計書を参照し誤った機器が撤去される	設計内で影響調査、資材作成に使用した資材を確認する	作業者 再鑑者 設計部署
ユーザが利用している機器・経路かどうかの確認をせずに撤去する	ユーザが利用しているネットワーク機器・経路が撤去される	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
		撤去前に機器の状態が抜線可能かどうかを確認する・確認する手順にする	作業者 再鑑者 設計部署