



より安全なシステム構築のために
～CC-Case_iによるセキュリティ要件の見える化

2016.4.22

金子 朋子（株式会社NTTデータ）

NTT DATA

金子朋子

博士（情報学）

(株)NTTデータ品質保証部所属.

入社以来航空機データ通信システム、遊技系システム等のシステム開発に従事. 情報セキュリティの社会問題化したプロジェクトも経験. 社内在宅勤務制度の設立時WGメンバー.

2013年情報セキュリティ大学院大学博士後期課程修了.

同大学院客員研究員.

文部科学省認定プログラム・サーティフィケート取得者

(情報セキュリティスペシャリスト, ソフトウェアスペシャリスト)

2015年 日本ネットワークセキュリティ協会(JNSA)

学術論文部門 優秀賞受賞

研究テーマ：セキュア開発方法論、品質保証



- 1.はじめに
- 2.関連要素技術（コモンクライテリア、アシュアランスケース）
- 3.CC-CaseのCC認証を伴わないセキュリティ要求分析への適用方法
 - CC-Caseインシデント対応版提案の背景
 - CC-Case_iの定義と目的・構造・適用対象・モデル
 - セキュリティインシデントとそのプロセス
 - セキュリティインシデント解決方法の妥当性
4. CC-Case_iのメリット
 - 見える化の特長
 - 使い方の工夫

本発表でお伝えしたいこと

- ① CC-Case_i とは何か？
- ② セキュリティインシデントに対して
どのように使うのか？
- ③ CC-Case_iのメリットは何か？

CC-Case_i の関連要素技術

1. CC

(Common Criteria)

2. アシユアランス・ケース

- CC（Common Criteria : ISO/IEC15408）＝ITセキュリティ評価基準（国際規格）
- CCは開発者が主張するセキュリティ保証の信頼性に関する評価の枠組みを規定

＊「セキュリティ保証」＝セキュリティ機能が間違いなく動作することの確からしさ

＊「ITセキュリティ評価」＝「セキュリティ保証」を確認すること

- 国家レベルで、第三者による確認の制度と確認結果を国際的に認め合う相互承認制度も確立されている。



認証書受入国：8カ国

＊シンガポールは6月19日に加盟を自主的に取り止め。

◆ CCパート1 概説と一般モデル

セキュリティ目標 (Security Target : S T)

ST概説

適合性主張

セキュリティ課題定義

脅威 組織のセキュリティ方針 前提条件

セキュリティ対策方針

TOEのセキュリティ対策方針

運用環境のセキュリティ対策方針 セキュリティ対策

拡張コンポーネント定義

セキュリティ要件

セキュリティ機能要件 セキュリティ要件根拠

セキュリティ保証要件

TOE要約仕様

プロテクションプロファイル (P P)

◆ CCパート2 機能コンポーネント

◆ CCパート3 保証コンポーネント

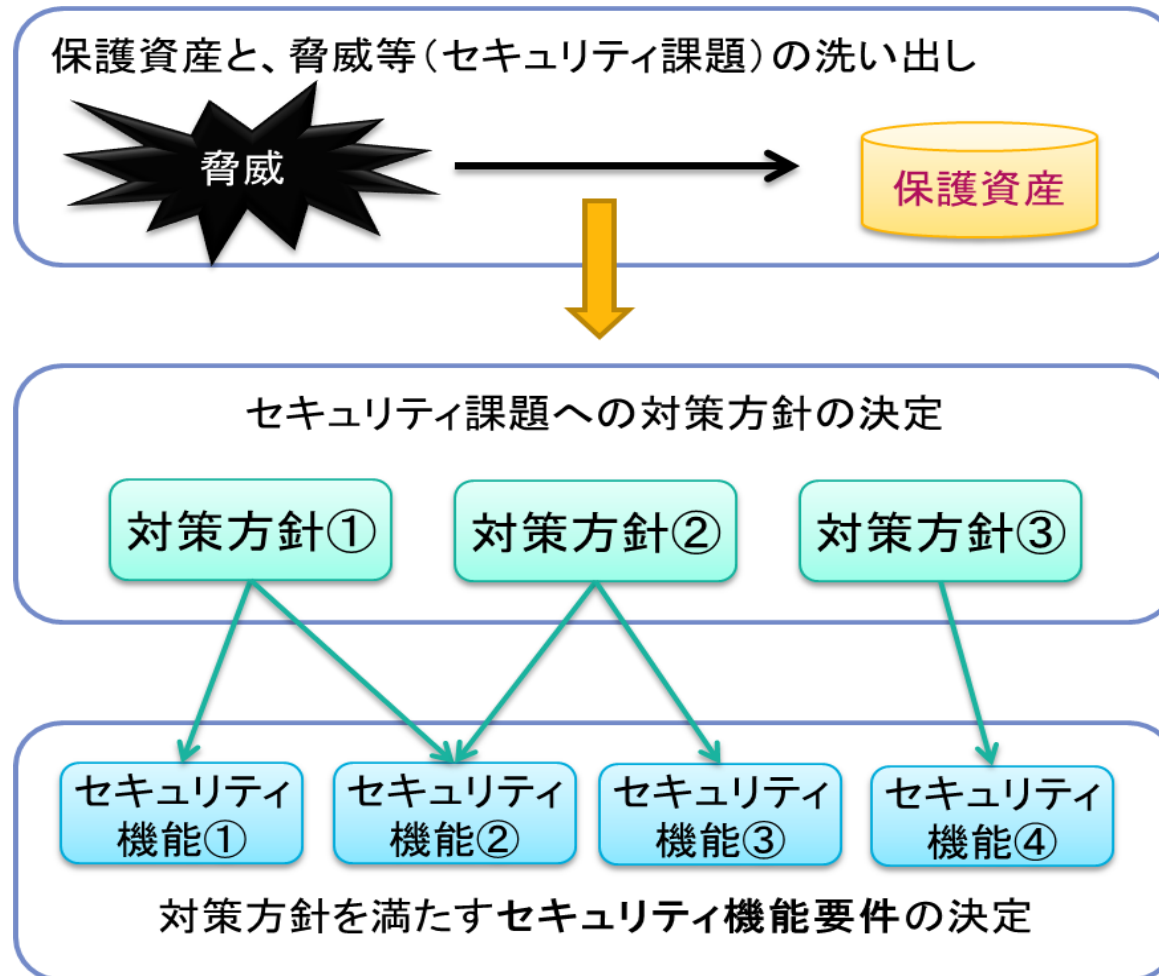
◆ C E M 情報セキュリティ評価方法

CCパート2
(セキュリティ
機能要件)

CCパート3
(E A L 保
証要件)

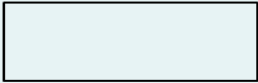
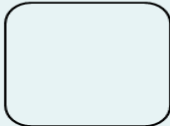
STはセキュリティ保証の目標を規定した文書

- 評価対象のシステムが装備するセキュリティ機能を定義
- 必須のセキュリティ評価対象



テスト結果や検証結果を**エビデンス**としそれらを根拠にシステムの安全性・信頼性を**議論**し、システム認証者や利用者などに**保証**する、あるいは確信させるためのドキュメント

GSNの構成要素

名称	図式要素	説明
ゴール(主張)		システムが達成すべき性質を示す。下位の主張や説明に分かれる
戦略(説明)		主張の達成を導くために必要となる説明を示す。下位の主張や説明に分解される
コンテキスト(前提)		主張や説明が必要となる理由としての外部情報を示す
未定義要素		まだ具体化できていない主張や説明であることを示す
証跡		主張や説明が達成できることを示す証拠

アシュアランスケースの構造と内容の要求事項（最低限）

- ・ システムや製品の性質に対する**主張**(claim)
- ・ 主張に対する系統的な**議論**(argumentation)
- ・ この議論を裏付ける**証跡**(evidence)
- ・ 明示的な**前提**(explicit assumption)
- ・ 議論の途中で補助的な主張を用いることにより、最上位の主張に対して、証跡や前提を**階層的に結び付ける**ことができる

***GSNは代表的なアシュアランスケース手法**

① CC-Case_i とは何か？

CCの課題

複雑

一般的なセキュリティ
要求分析にはあまり
利用されていない

デジタル複合機などの特定のセキュリ
ティ機能のハードウェア製品や政府調
達対象案件に利用が限られる

CC-Case

認証を取るための開発を想定していた

インシデントのニーズが高いことがわかった！！

セキュリティインシデント後の本格対処で利用を検討

<理由>

セキュリティは非機能要件であり、当初のシステム設計時には機能要件として挙がらないが、その後のインシデント発生により、システム改修が必要となる事例が多いため

CC-Caseの定義

セキュリティ要求分析と保証
の統合開発方法論

CC-Caseの目的

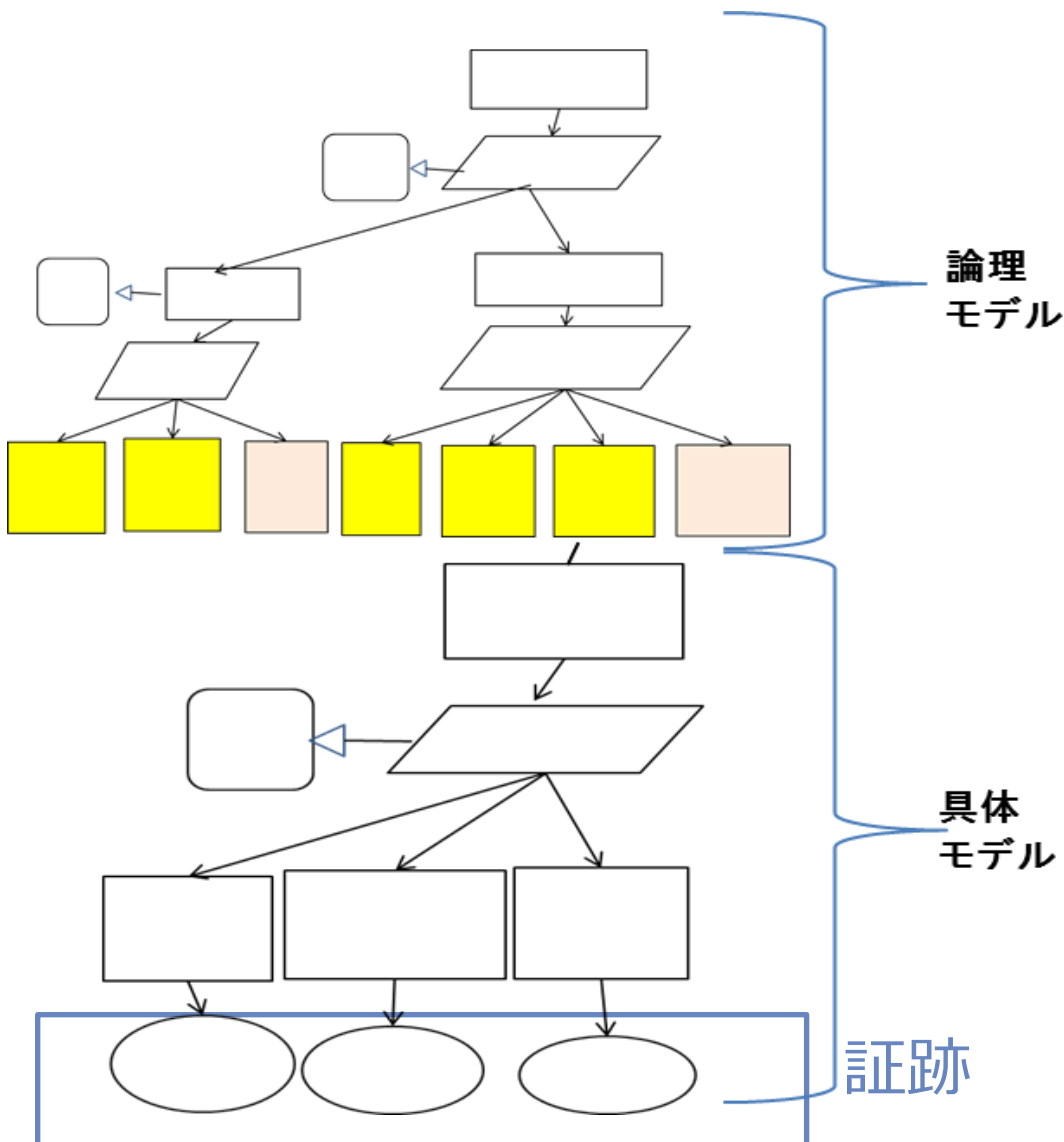
開発のセキュリティ上の課題を解決するため、セキュアなシステム開発への対応を実施すること

CC-Case_iの定義

CC認証を伴わないセキュリティインシデントの本格対処に適した「セキュリティ要求分析と保証」をサポートするプロセスと記法の統合手法

CC-Case_iの目的

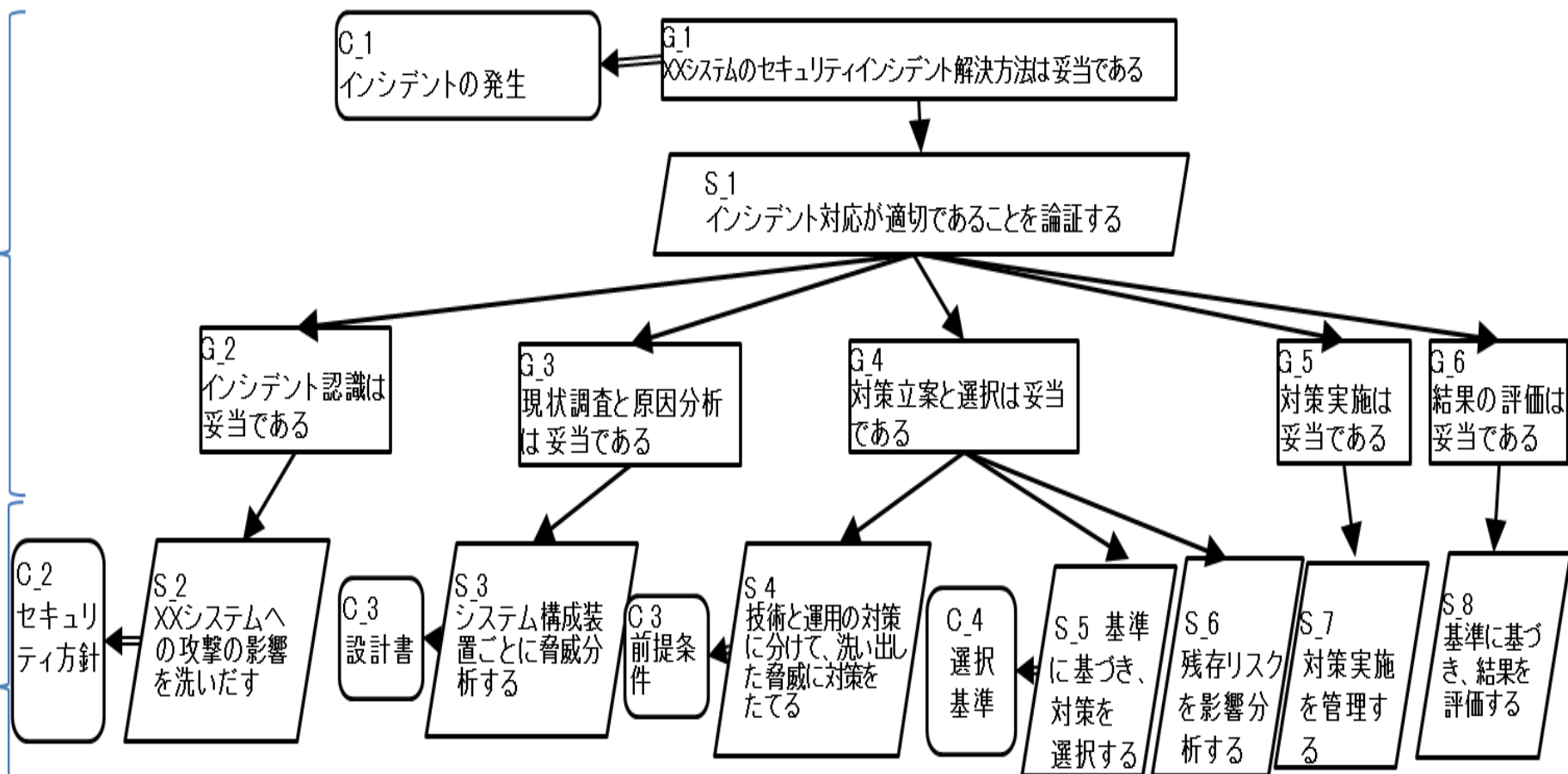
インシデントの本格対応も含め、CC認証を伴わない一般的な開発におけるセキュリティ上の課題解決に役立てること



CC-Case_iは
CC-Caseと論理構造は
同じ！！

論理モデルと具体モデルに分類される

- CC-Case_iの適用対象はシステムまたは製品。仕様を決める際に承認を取る特定の顧客がない場合は要件を決めるうえでの関係者と読み替える。



**CC基準から、
インシデント対応用のプロセスに変えた！！**

② セキュリティインシデントに対して どのように使うのか？

セキュリティインシデント：事業運営に影響を与えたり、情報セキュリティを脅かしたりする事件や事故のこと

セキュリティインシデント対応

「1. 平時におけるインシデント対応の準備」

- ・ インシデントに対応する際の目的と目標事項，通知体制の確立が必要
→セキュリティポリシーに記載すべき事項

「2. 情報セキュリティ侵害を検出」

- ・ インシデントであることと，その重要性に対するインシデントの識別が必要

「3. 情報セキュリティインシデント対応」

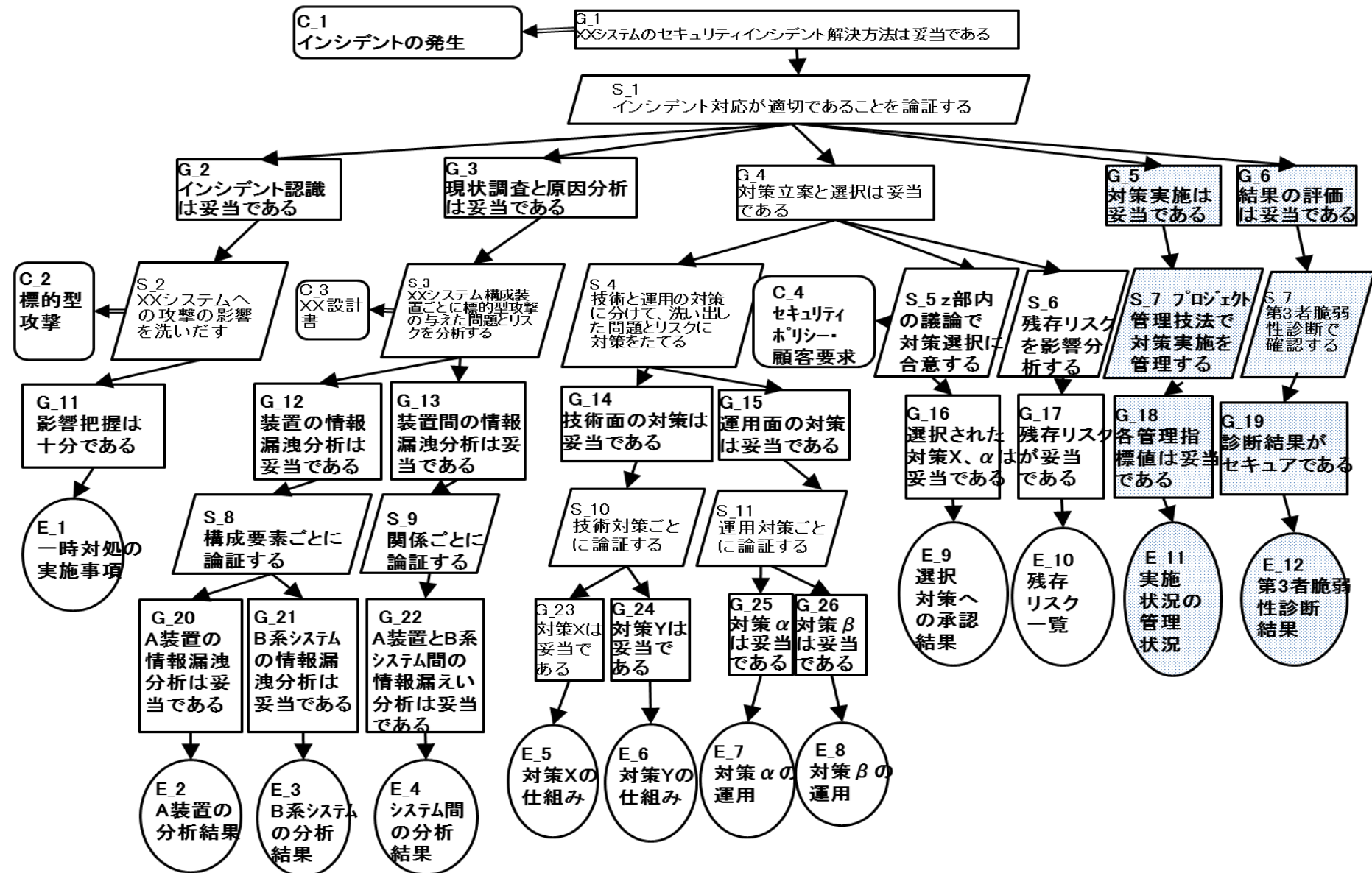
- ・ 暫定的対応

- ・ 本格的対処

→システムの改修や運用方法の変更を伴うことも多い。

CC-Case_iのプロセス

段階	ゴール	目的	入力	手続き	出力	出力に対する確認
G-1	XXシステムのセキュリティインシデント解決方法は妥当である	セキュリティインシデントの解決方法の妥当性を確認する	・インシデントの発生	G-2からG-6までのゴールがすべて満たされていることを確認する	・インシデント解決の評価	妥当性確認
G-2	インシデント認識は妥当である	インシデントを認識し、一時対処が妥当であることを確認する	・セキュリティ方針	基準に基づき、結果を評価する	・一時対処の実施結果	妥当性確認
G-3	現状調査と原因分析は妥当である	本格対処に必要な現状調査・分析を行う	・設計書 ・保護資産	・システム構成装置や機能等に分けて脅威分析する	・システムとシステム間の脅威分析結果	妥当性確認
G-4	対策立案と選択は妥当である	最適な対策を選択する	・前提条件	・技術と運用の対策に分けて、洗い出した脅威に対策をたてる ・基準に基づき、対策を選択する	・対策選択根拠 ・選択対策への承認結果 ・残存リスク	妥当性確認
G-5	対策実施は妥当である	対策を着実に実行する	・選択した対策	実施状況を管理し、対策を実施する	・実施結果	妥当性確認
G-6	結果の評価は妥当である	実施結果を評価し、次の改善につなげる	・実施結果	基準に基づき、結果を評価する	・実施状況の評価結果	妥当性確認



- セキュリティインシデントの本質的原因は？ → いろいろあり

脅威分析・システム
リスク評価が不十分

各フェーズ間のセキュ
リティに関する分析の
一貫性欠如

セキュリティ対策の検
証方法のあいまいさ

設計・実装時のレビュー
が不十分でシステムバグ
を見つけ切れていない

...

- 解決方法は？ → 様々なケースがある

運用で
カバー

同様なインシデント
を防ぐ仕組みの確
立が必要

システム自体の大
規模な技術的改
修が必要

インシデントが起きた
装置・システムだけ
でなく他装置への影響
検討が必要

単なる問題解決だ
けでなく今後のリス
ク対処が必要

...

原因も解決方法も多様なため、インシデントの解決は難しい。
では解決方法が妥当であることを示すために大事なことは？

インシデント解決の
プロセス

+

議論による
「レビューの強化」

③ CC-Case_iのメリットは何か？

CC-Case_iは3つの見える化の特長をもつ。

1.主張と証跡の見える化：

ゴールとしての主張とその主張の正しさを裏付ける証跡が存在すること

- GSNはトップゴールの主張を満たすことを可視化できる手法だから

2.論理の見える化：

前提条件、戦略、ゴールの関係性の明示により、トップの主張から証跡までの論理が明確化されること

- GSNは図の最下層に主張が正しいことを示す証跡を記述するから
- 更にインシデントの本格対応に適したモデルとしてCC-Case_iを提案

3.保証ストーリーの見える化：

プロセスと実施事項の明確化によりインシデント全体の解決ストーリーの可視化

- CC-Case_iは管理プロセスと各インシデントへの対処がつながる統合方法論
- プロセスアプローチによるインシデント抽出、分析、管理は定性的にも定量的にも適用可能であり、インシデント解決の適切性を保証できる

CC-Case_iの使い方の3つの工夫

「議論のツール」:

- ステークホルダ間の認識の食い違いを防ぐ
- できる限り1枚の図で論理の全体像を表記し、インシデント解決ストーリーをステークホルダで共通認識ができるようにする。（実用性にこだわりあり。）

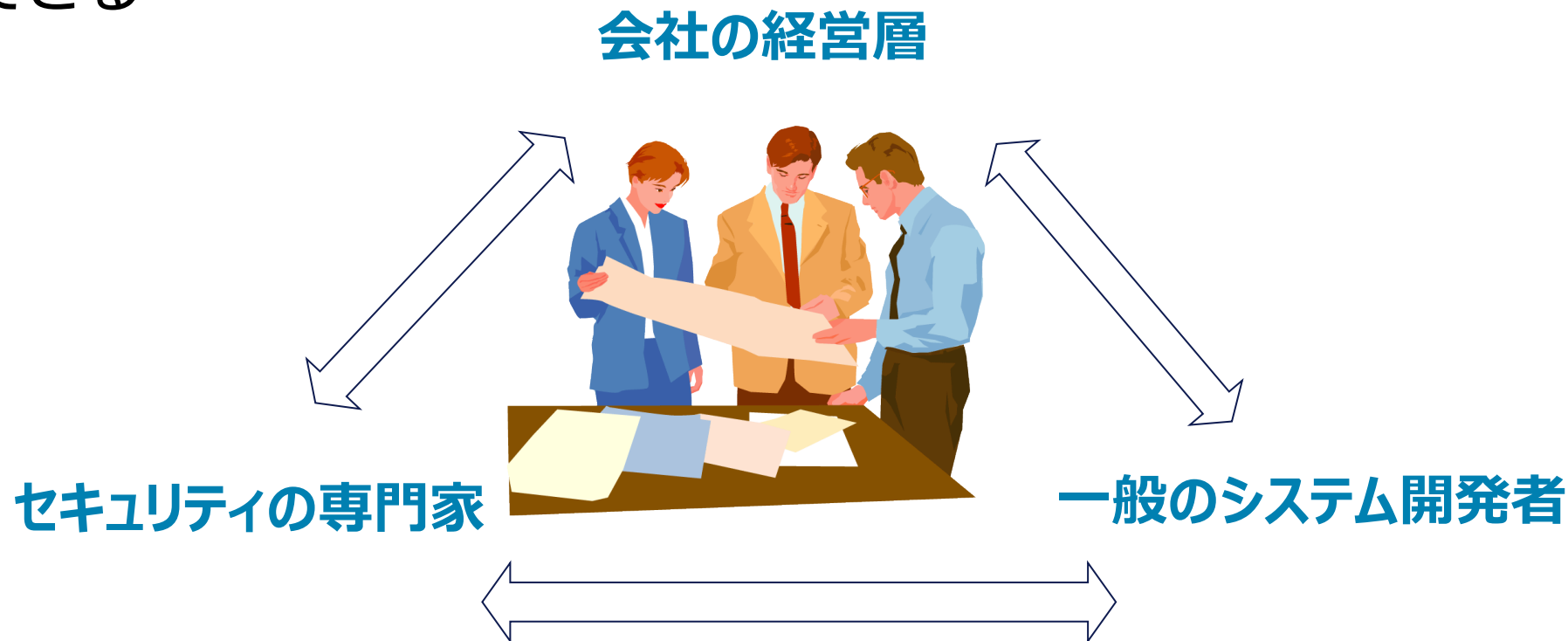
「セキュリティ保証のツール」:

- インシデント解決の妥当性確認の一連のプロセスと結果が要件を満たすことを確認するツールである。
- 単に要件に対する検証を実施するだけでなく、ステークホルダ間の議論による妥当性確認が可能である。

「脅威と対策の資産化ツール」:

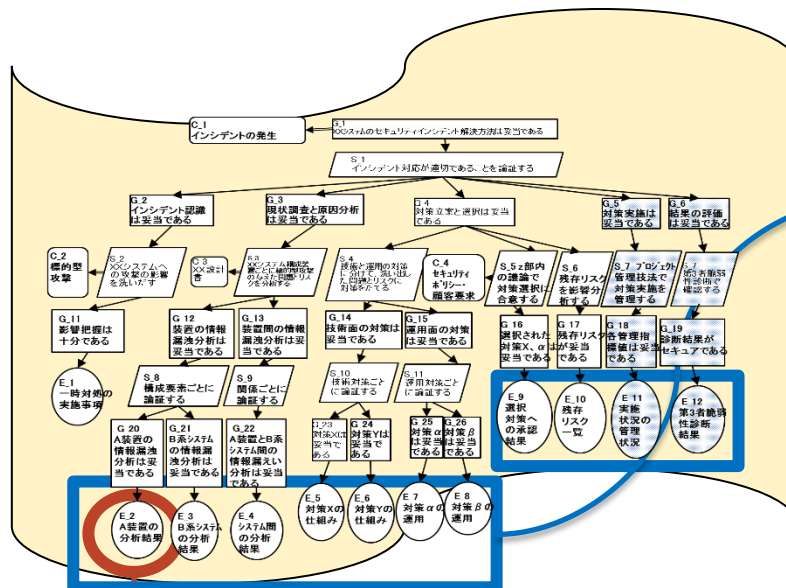
- 証跡単位でDB化して脅威と対策のノウハウを資産化できる。
（CC-Caseは一連のプロセスを形式化しているため）
- 利用者が自社等のシステムにおいて資産化を進めることにより、将来的に自社システムにおけるプロアクティブな対処につなげられる可能性がある

インシデント解決ストーリーをステークホルダで共通認識ができる



異なるバックグラウンドをもつステークホルダ間で理解の壁をなくし、互いのもつ見識を活かしたインシデント解決を図る！！

① 1枚の図で論理の全体像を表記



④ 証跡単位でDB
化して脅威と対策の
ノウハウを資産化で
きる。



プロアクティブな対応

② 各項目の詳細
内容にはリンクを
張って参照できる

リンク

XXXXXXXX
1.XXXX
2.XXXX

③ 進捗段階に応じ、妥当
性確認を完了した決定事
項と計画段階の未決定段
階を区別。内容を書き換え
ていく。

ご清聴ありがとうございました!!

