ビットコインシステム
導入に対する
システムアシュアランス

奈良先端技術大学院大学
氏名：井上　万実

全体概要

シチュエーション設定

・企業が決済手段にビットコインを導入することを仮定
・財務経理部門の責任者が経営者へビットコインが安全であることを説得するためにD-Caseを用いることを想定

全体の流れ

- ビットコインシステムの概要
- ユースケースを用いたシステム定義
- PHAによる初期リスク分析
- ミスユースケースによるリスク対策検討
- D-Caseによる論証の構築

ビットコインシステムとは

- オープンソースのソフトウェアによって作られた決済システム
- P2Pネットワークを用いて、データの透明性を確保
- 決済の処理を分散して行う
- 匿名性のある仮想通貨

ビットコインシステムの安全性

- いくつかのトランザクションが集まってブロックをなす
- ブロックの鎖をブロックチェーンと言う
- ネットワーク上で全トランザクション履歴を含むブロックチェーンを共有する
  - 各参加者が同一のブロックチェーンを持つ
- ブロックチェーンの書き換えは容易ではない

BlockChain

トランザクションの具体例

トランザクション例:

0100000001<u>4b17cb55adb9b8d96c052ae241597088a5f32aa2e82a8b8e13340c4f3328485</u>0000000008b48304502206
d8a91ef254961eaa8b5591f13ca821d23a81e6567e67527062984c5f1bb53c6022100d722cc03229fefd82f28856ca84b
4301fa01dd1d82120269a96d1d0e5e7056e8014104e8414348a7d1cbe57e99353b50bcd22c047d6a83bb7e182592c55
e473454a21ff64dd20ddfb820a922c9bb23638f7b840e430b5531d744d9e6b0a4ae8b69cca5ffffffff02bbb64d57030000
0019<u>76a914a54badcbf7723ad8e9f4a48bc171631ad52eb3e188ac</u>$_A$c0ea2101000000001976<u>a91415250f1b438ce0271e
aac8edff508de7ba4001ad88ac</u>$_B$00000000

前のトランザクションハッシュ（4b17cb55…f33284850）から
アドレスA、Bへの送信であると分かる。

※トランザクションハッシュは前のトランザクションデータ（01000…000）と
SHA暗号化を用いてSHA(SHA(01000…000))で計算される。
緑の部分に下線を引いてAとBと書いて、AとBへの送信であると分かる

ビットコインシステムの処理フロー

- 利用者は送信先アドレス、金額を指定したトランザクションを生成し暗号化する

- トランザクションをビットコインネットワークにブロードキャスト

- 各マイナー（採掘者）が複数のトランザクションをまとめてブロックを生成及びブロードキャストを試みる

- マイナーが新規ブロックを取引履歴の集合に追加

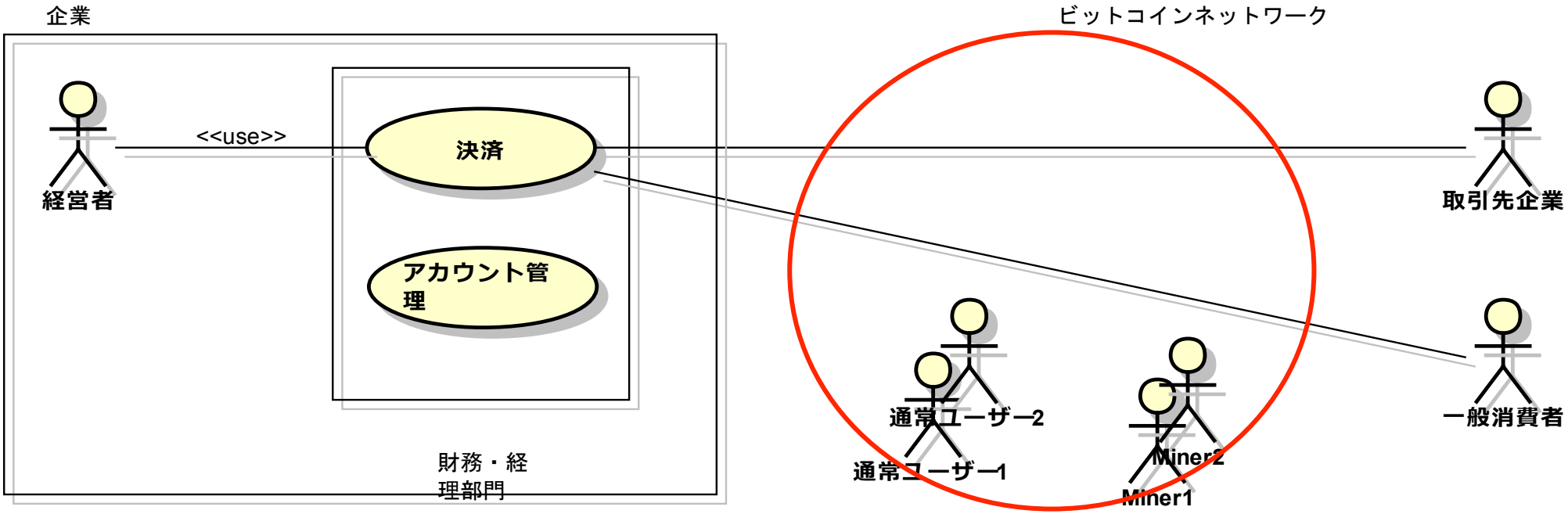
ットコインシステムの必要性(利点＆欠点)

ビットコインシステムには利点と欠点がそれぞれ存在する。

Pros	Cons
• 特定の機関･組織に依存しない • 国を跨ぐような遠隔決済を安価にすることができる • 使用者の機密性がVISA等と比べて高い	• 中央銀行を持たないため、価値の変動が激しい • ビットコインを用いた取引の完了には時間がかかる

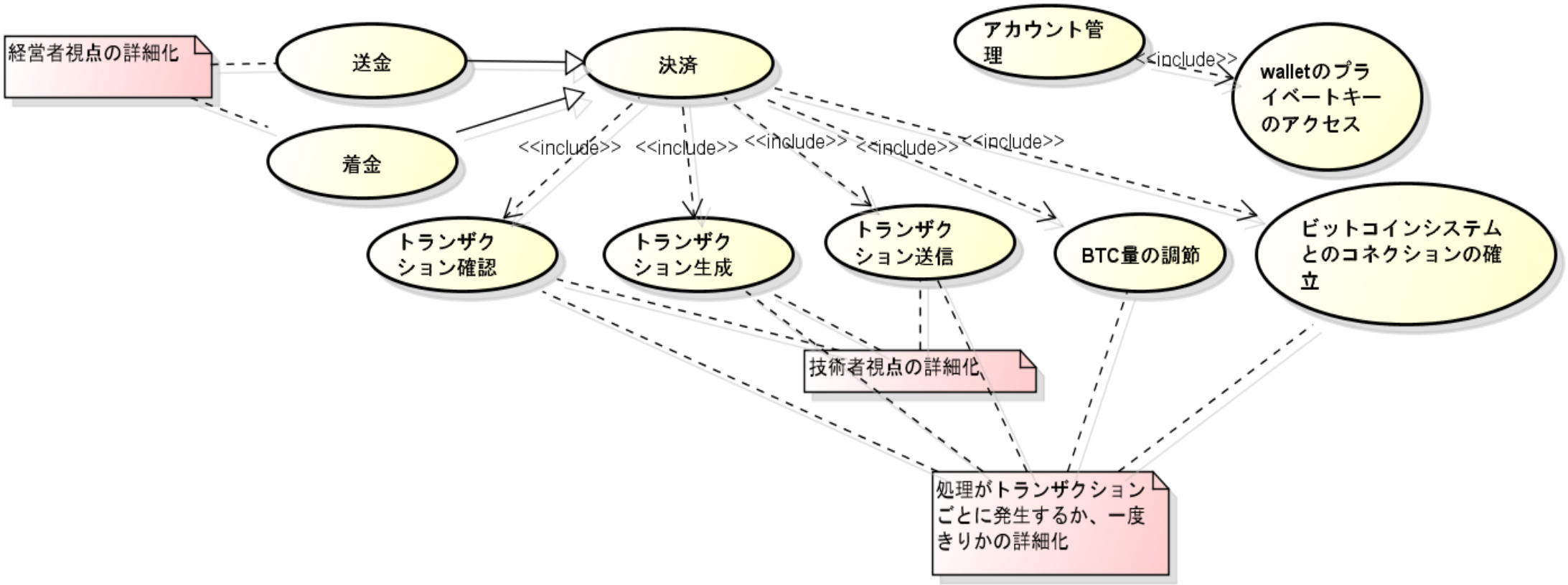
システムの全体像:全体ユースケース図

対象:ビットコインの導入を考えている企業の財務経理部門

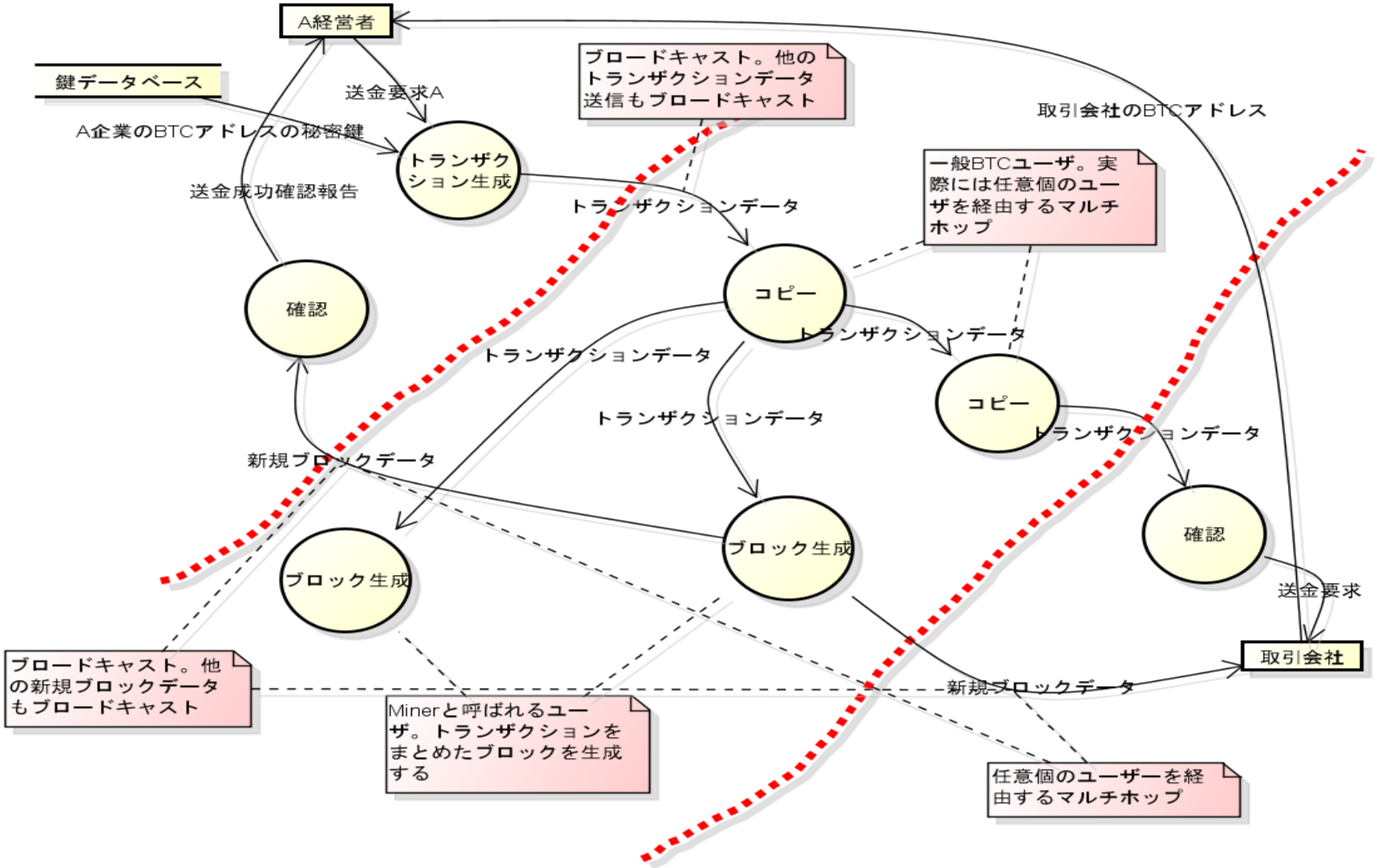


分析の準備：決済ユースケースの詳細化

決済機能の洗い出し



分析の準備:データフロー図



分析の準備：扱うデーター覧

秘密鍵
- ランダムな256bitの値 : int

送金要求
- 送金金額 : int
- 送信先 : String

トランザクションデータ
- version : int
- 入力元walletの数 : int
- 前回のトランザクションのハッシュ : String
- 出力先walletの数 : int
- BTC額 : int
- 公開鍵 : String
- Scriptsignature : String

新規ブロック情報
- Hash値 : String
- バージョン番号 : int
- 前のブロックのHash値 : String
- 生成時間 : int
- bit長 : int
- トランザクション数 : int
- ブロックサイズ : int
- ブロックインデックス : int
- ブロック高 : int
- 個々のトランザクションデータ : List of トランザクションデータ

取引会社のBTCアドレス
- BTCアドレス : String

wallet
- アドレス : String

実施した初期リスク分析

PHA（Preliminary Hazard Analysis）

:サブシステムごとにハザード及び脅威を洗い出す手法（ハザードを構成する三要素として、ソース、メカニズム、アウトカムが必要）

No.	システム	サブシステム	ハザード	原因	影響	初期リスク			リスク低減案	推定残存リスク			属性	分類
						発生頻度	重大性	リスク評価		発生頻度	重大性	リスク評価		
破局的な														

※三菱総合研究所　石原先生の講義に基づく

今回はサブシステムとしてアクター及びユースケースを用いた

PHAによるリスク分析

PHA ワークシート

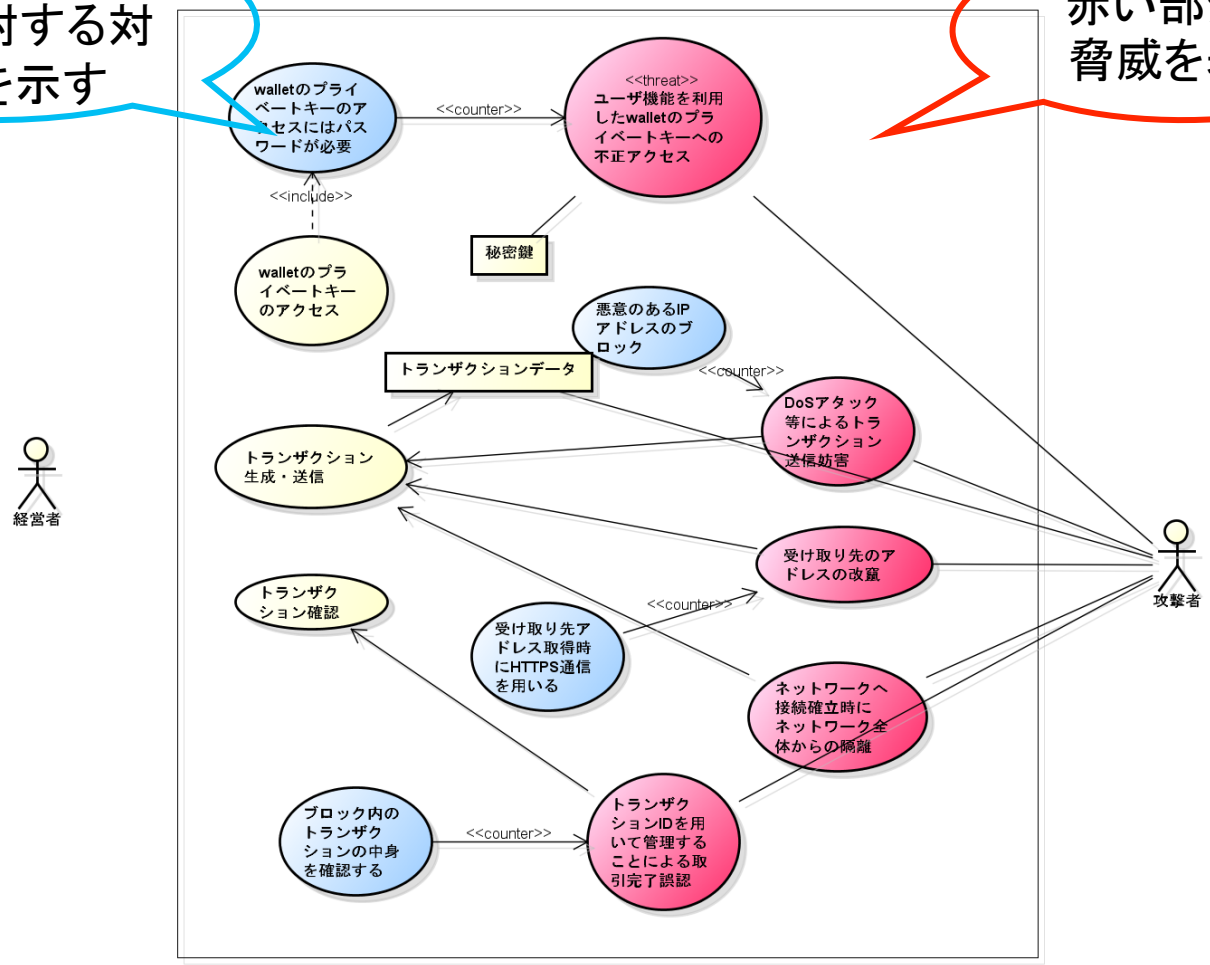
No.	システム	サブシステム	ハザード	原因	影響	初期リスク			リスク低減案	推定残存リスク			属性	分類
						発生頻度	重大性	リスク評価		発生頻度	重大性	リスク評価		
破局的な														
001	ビットコインシステム	ビットコインシステム	SHA-256 暗号、楕円曲線暗号の解読によるブロック化の困難さの消失	システム内脆弱性	ビットコインシステムの破綻	小	大	大	代替的な一方向関数を用いた暗号化手法の準備	極小	大	大	a,b	β2
002	ビットコインシステム	ビットコインシステム	悪意のあるユーザによる 50%以上のハッシュパワーの掌握	システム内脆弱性	ビットコインシステムの破綻	極小	大	大	マイニンググループの分散	極小	大	大	b	β2
重大な														
003	ビットコインシステム	取引先企業	サーバーアタックによる取引妨害	悪意のあるユーザ	決済を行うことが困難になる	大	大	大	悪意のあるユーザのアドレスのアクセスをブロックする	大	小	小	a,b	β1
004	ビットコインシステム	取引先企業	ビットコインの急激な下落	市況の変化	金銭的損失	大	大	大	社内の BTC 量を管理する	大	小	小	a	γ
005	ビットコインシステム	通信経路	P2P ネットワーク参加時に、悪意のあるユーザからのネットワークからの隔離	悪意のあるユーザ	決済を行うことが困難になる	小	大	大	特定のサーバーをビットコインネットワークにアクセスさせ続ける。	小	小	小	a,b	β1
006	ビットコインシステム	通信経路	HTTP 通信を用いることにより送り先の書き換え	悪意のあるユーザ	BTC の喪失	大	大	大	HTTPS 通信を用いる	小	大	大	a,b	β1
007	ビットコインシステム	通信経路	ネットワークの負荷増大による取引遅延	悪意のあるユーザ	決済を行うことが困難になる	大	大	大	Peer 間の送信条件によって対処	小	大	大	a,b	β1
008	ビットコインシステム	アカウント管理	ハッキングによる BTC の喪失	悪意のあるユーザ	BTC の喪失	小	大	大	ウイルス対策ソフトウェアの導入	小	小	小	a,b	β1

										小	大	大	a	γ
										する	小	大	大	a,b	β1
										ブロックす	小	大	大	a,b	β1
										力を定める	小	大	大	a	γ
013	ビットコインシステム	マイナー	ブロックチェーンの分断	システムエラー	決済に遅延が発生する	大	大	大	なし	大	大	大		α

リスク低減案の分析:ミスユースケース図

青い部分は
脅威に対する対
抗策を示す

赤い部分が
脅威を表す



※みずほ情報総研の金子先生の講義による

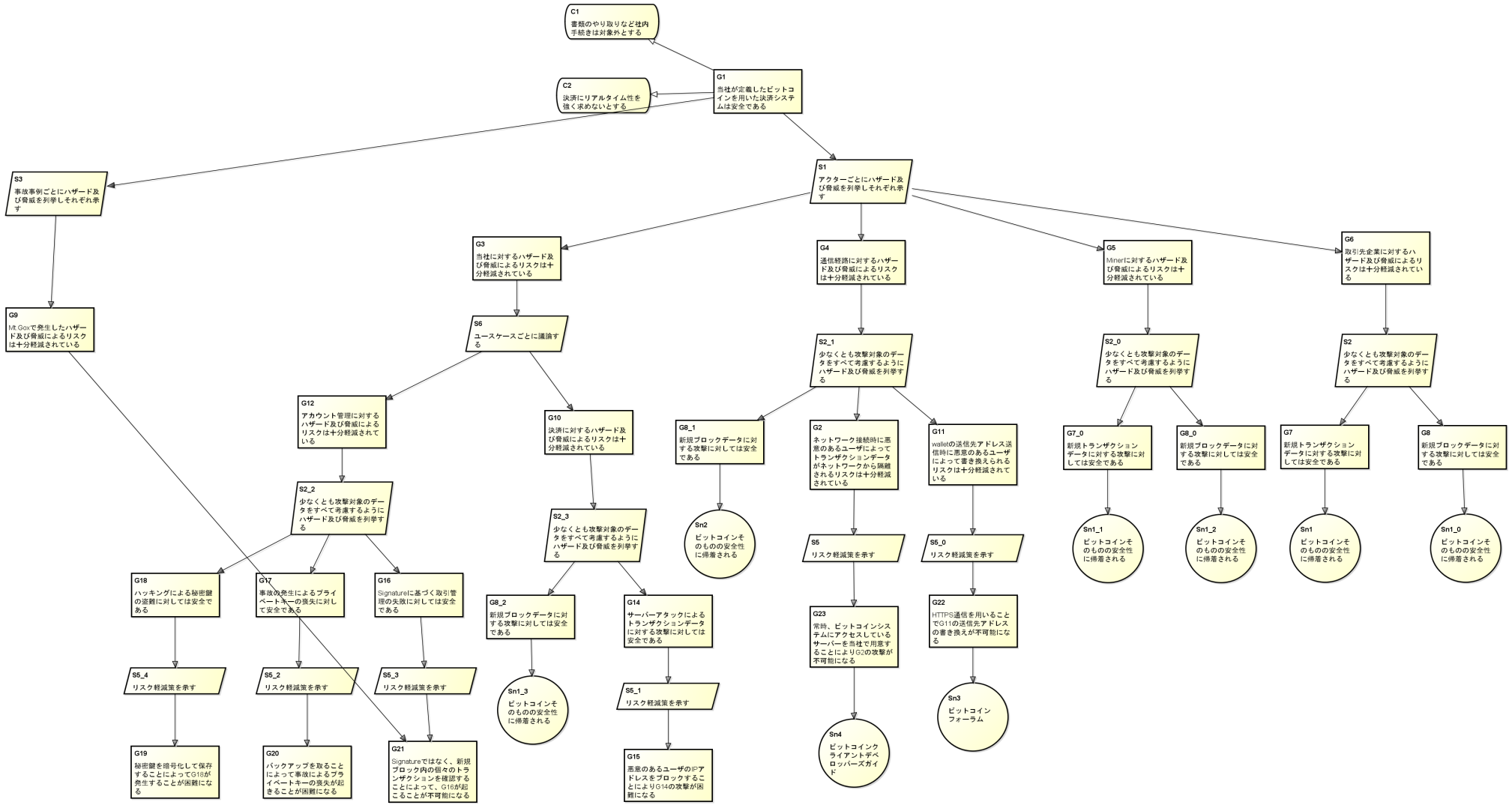
アシュアランスケースによる分析

アシュアランスケースの戦略

1. 図的なアシュアランスケースの表現であるGSN(Goal Structuring Notation)を用いた　※
2. トップゴール：導入企業のビットコインを用いた決済システムの安全性
3. 戦略：経営者視点と技術者視点から議論
   - ➢技術者視点：
     - ❑ユースケースのアクターに基づく
     - ❑さらに、データフロー図で用いたデータを基に分析
   - ➢経営者視点：事故事例に基づく

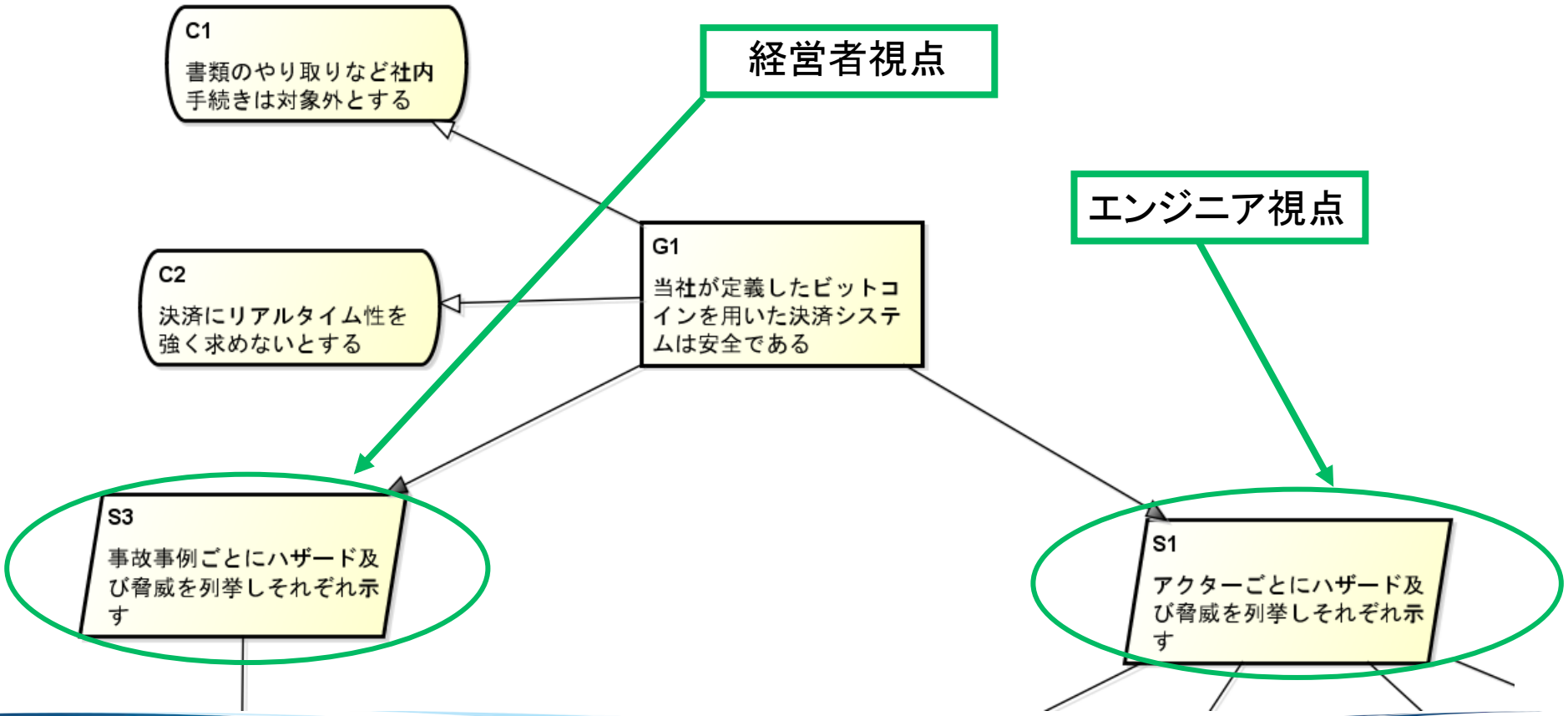
※富士ゼロックス　上野先生の講義による

アシュアランスケース作成結果



アシュアランスケース詳細

説明対象者に基づいてストラテジーの分割を実行した。
経営者視点では説得力を、エンジニア視点では網羅性を軸にリスクの洗い出しを行った



まとめ

今回行ったこと:

- ユースケース、PHA等を用いてリスクを列挙し、アシュアランスケースを作成した

今後の課題:

- PHAでのリスク列挙が網羅的かどうかに関して、確証がないので、なんとかしたい
- リスクの発生確率の見積もりが主観に基づいて行われたので、もっと客観性を持つ形で見積もりをしたい
- アシュアランスケースを書くのは面倒なので自動化したい(コードジェネレーターを作りたい)

ご清聴ありがとうございました。