暗号資産に関する全世界における サイバーインシデントの 調査とリスクの考察

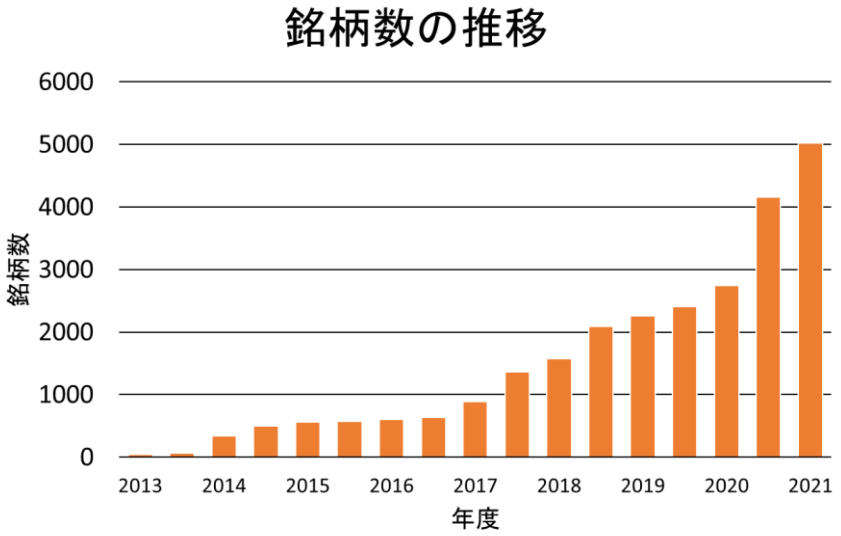
4班
班員：伊藤奎政　岸淵涼平　曹彦　都築祐人
アドバイザー：矢田昇平　面和成

背景

・近年、暗号資産が注目されている

暗号資産（仮想通貨）：ブロックチェーンと呼ばれる暗号技術を用いた電子的資産の一つ
例）ビットコイン、イーサリアム

https://coinmarketcap.com/ja/currencies/bitcoin/



・コロナ禍における外出機会の減少、オンライン化

▼

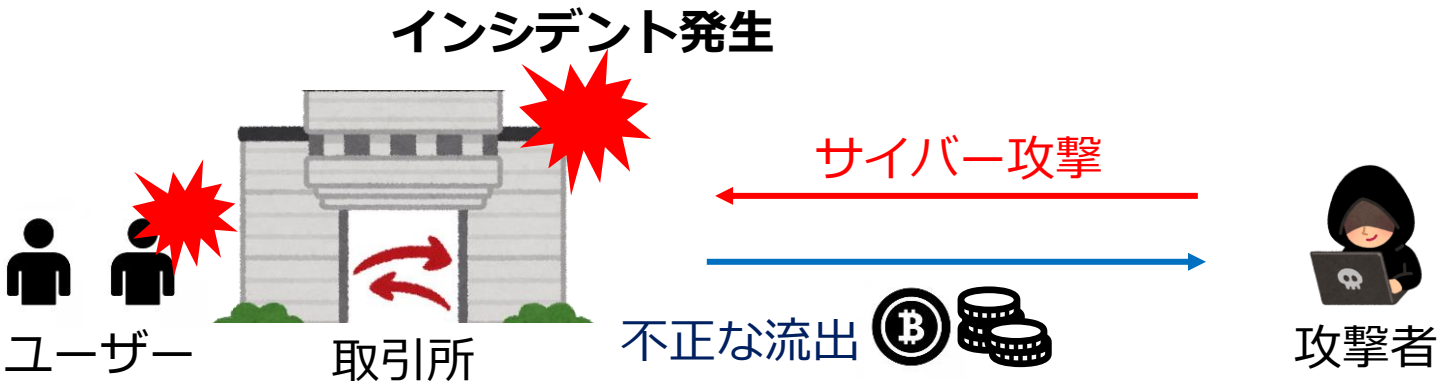
決済手段などの利用も進む暗号資産への期待が高まる

暗号資産のサイバー攻撃リスク

- 暗号資産は独自のメリットがある一方で、多様なサイバー攻撃にさらされるリスクも存在
  - 従来のサイバー攻撃から、ブロックチェーンや取引システムの脆弱性をついた暗号資産独自の攻撃
  - 対象は各ユーザーから暗号資産取引所、暗号資産自体などさまざま
  - 暗号資産の価値上昇に伴い、攻撃のメリットも増加

▼

これまでに多くのサイバーインシデントが発生



暗号資産インシデントの例

- 2016/8/2　暗号資産取引所「Bitfinex」で約7000万ドルのBitcoinがハッキング被害
  →このインシデントの影響により一時Bitcoinの価格が下落

インシデント発生

→価格変動リスク
安定した運用に弊害

当時のBitcoinの時価 https://coinmarketcap.com/ja/currencies/bitcoin/

▼

インシデントの対策が重要

暗号資産に関する先行研究

暗号資産のリスクに関する研究

・Li et al.（2020）[1]やWang et al.（2020）[2]

ー ブロックチェーンの主要なリスクや攻撃手法をまとめた研究

▼

実際のインシデント事例に関してはほとんど整理されていない

暗号資産のインシデント事例をまとめた研究

・Grobys et al.（2019）[3]や Biais et al.（2018）[4]

ー 暗号資産の価格変動に対する主要なインシデントの影響を調査

▼

インシデント自体の分析や対策には言及していない

まとめられたインシデントも一部のみ

研究目的

問題意識

・暗号資産の運用のためにインシデントへの対策が必須
・個々のインシデント事例を整理・分析した研究があまり見られない

▼

研究目的

過去に発生したインシデント事例を一つ一つ調査・整理
インシデントの攻撃手法や原因から傾向などを分析

⬇

変化するインシデントリスクを明らかにする

研究手法・流れ

・**2009年から2020年までに実際に発生したインシデントを調査**
ー 2009年：ビットコイン（暗号資産）の始まり
ー インシデント事例は実際に金銭被害が報告されているものを対象
ー 暗号資産取引所の公式サイトや海外のニュース記事を参照

▼

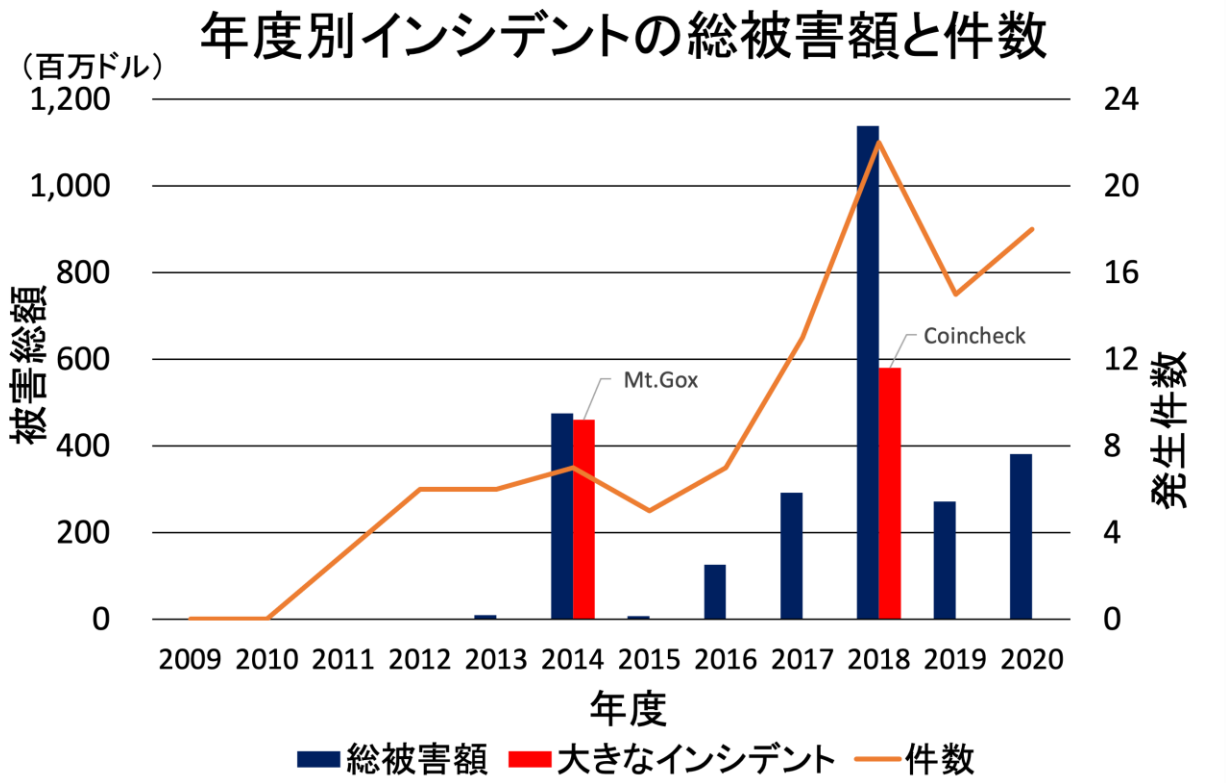
・**インシデント事例を「被害対象」や「被害原因」により分類**

▼

・**インシデントの全体的な特徴や時系列的な傾向を把握**
インシデントリスクの変化や原因を考察

結果：インシデント被害額と件数

・総件数：102件、総被害額：＄26.9億

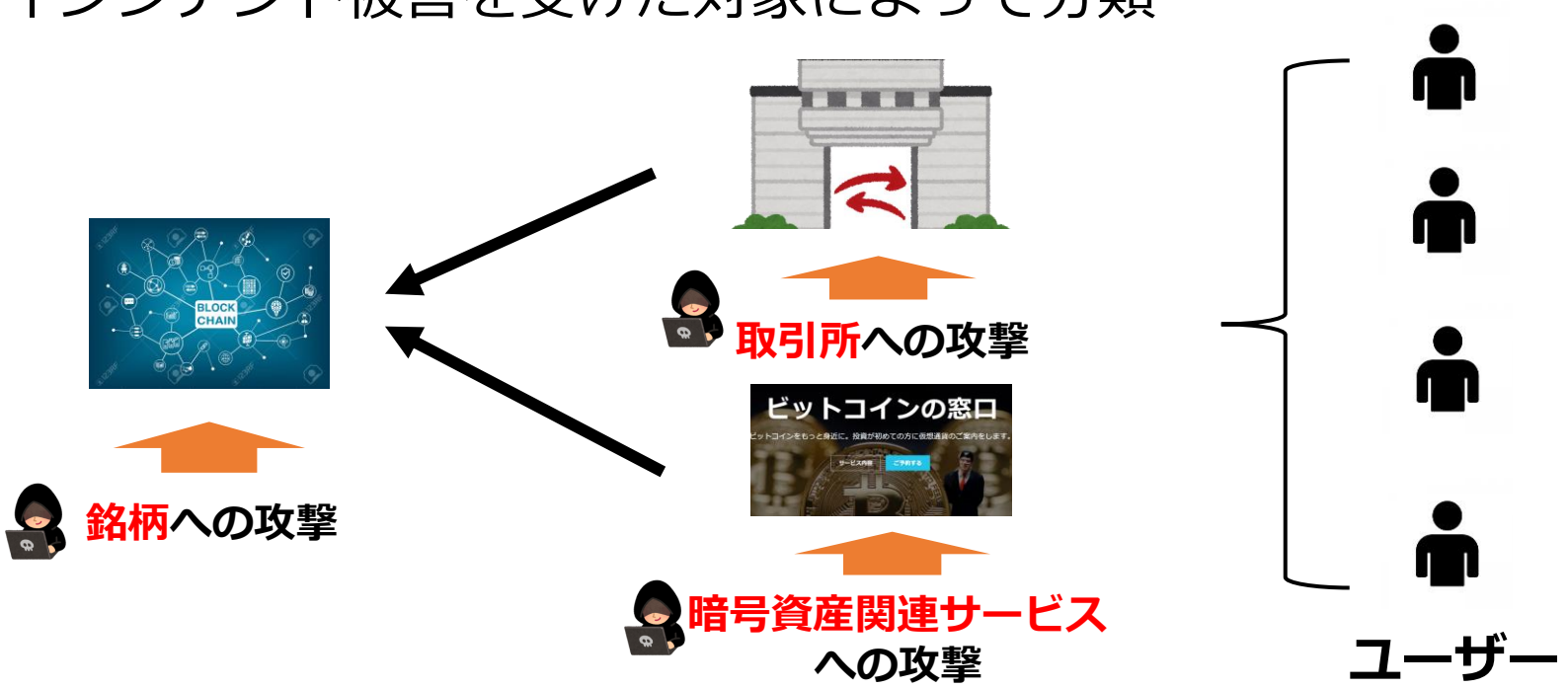


・2014年、2018年は大きなインシデントが発生したことにより被害総額が突出

・被害額と件数は年々増加傾向（大きなインシデントは例外）
→暗号資産の価値や注目度の増加が影響

被害対象による分類

・インシデント被害を受けた対象によって分類



取引所：暗号資産を売買することができるサービス
大量の資金とユーザデータが保存されている

暗号資産関連サービス：取引所を除く暗号資産に関連するサービス
ウォレットサービス、DeFi、ICO
(Initial Coin Offering）など

銘柄：BTC、ETHをはじめとした暗号資産自体

被害原因による分類

・インシデント被害の発生した原因によって分類

インシデントの被害原因

人による脆弱性

セキュリティ情報が外部に漏れたり、内部不正アクセスなどによる被害

取引所サーバの脆弱性

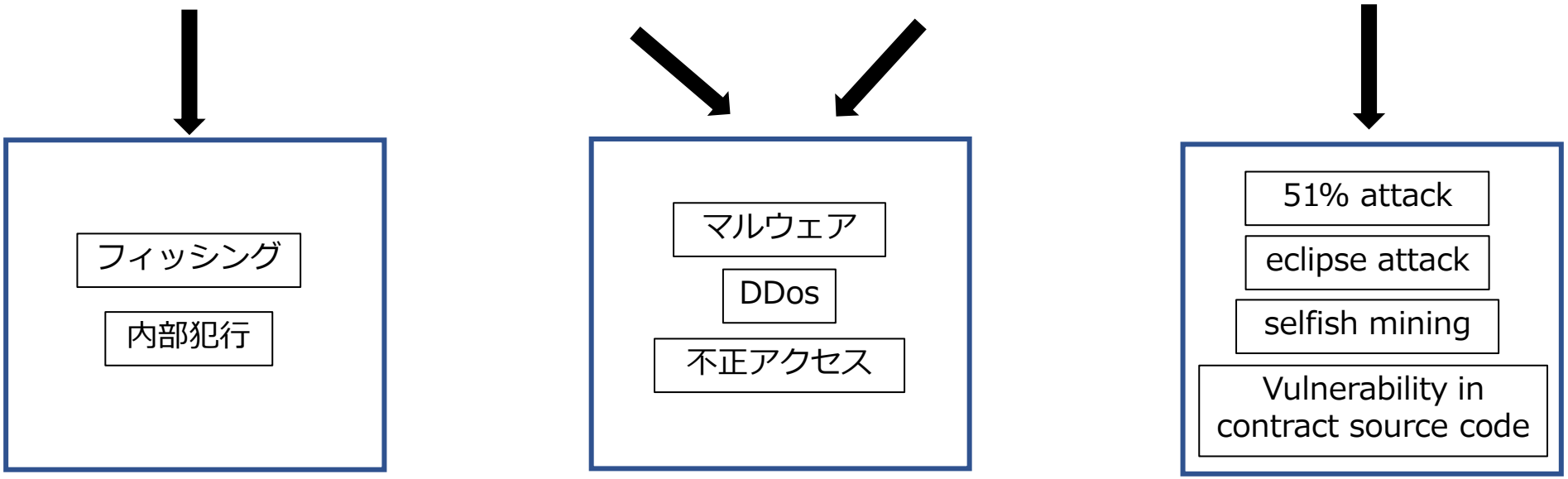
取引所のサービスシステムに対する攻撃、不正アクセスや営業妨害による被害

暗号資産関連サービスの脆弱性

ウォレットシステムなど他社が開発するシステムに対する攻撃による被害

ブロックチェーン・スマコン脆弱性

暗号資産の基幹技術ブロックチェーンを悪用、攻撃などによる被害



各被害原因における攻撃の例

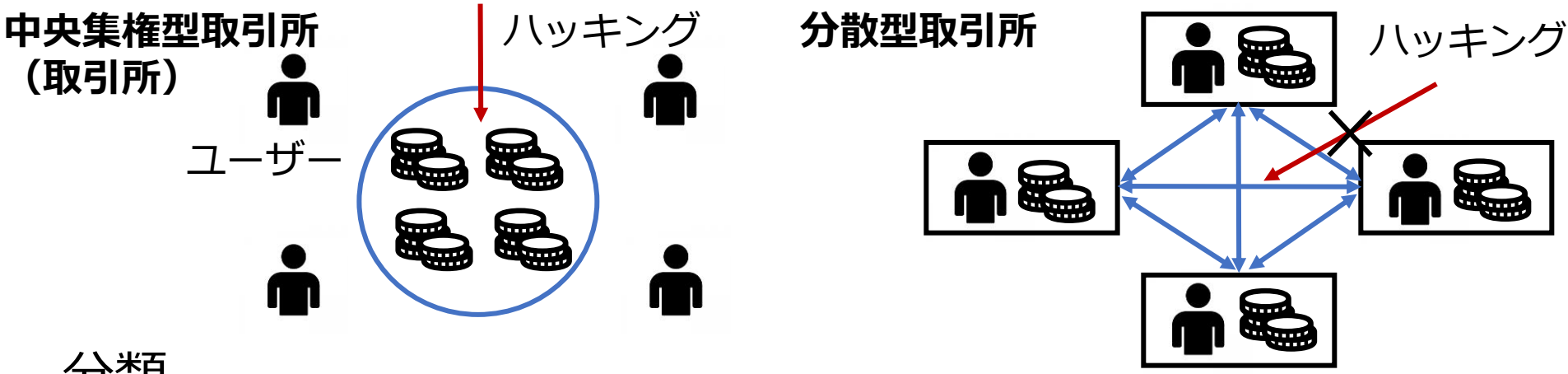
インシデントの分類例

分散型取引所の場合

・**<u>分散型取引所</u>**：管理者なしで暗号資産の取引が可能な取引所

▼

取引は全てブロックチェーン上で自動的に行われる



分類

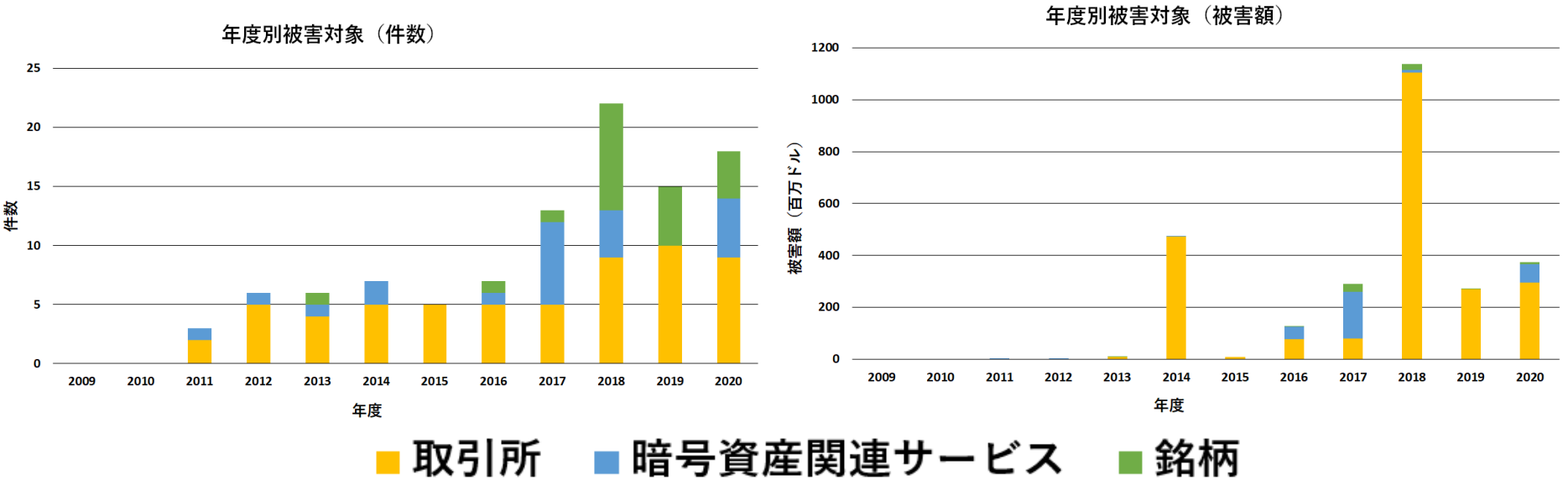
・**被害対象**⇒**取引所**に分類

・**被害原因**⇒ブロックチェーンの取引システムが原因の場合

ブロックチェーン・スマコン脆弱性に分類

結果：被害対象による分類

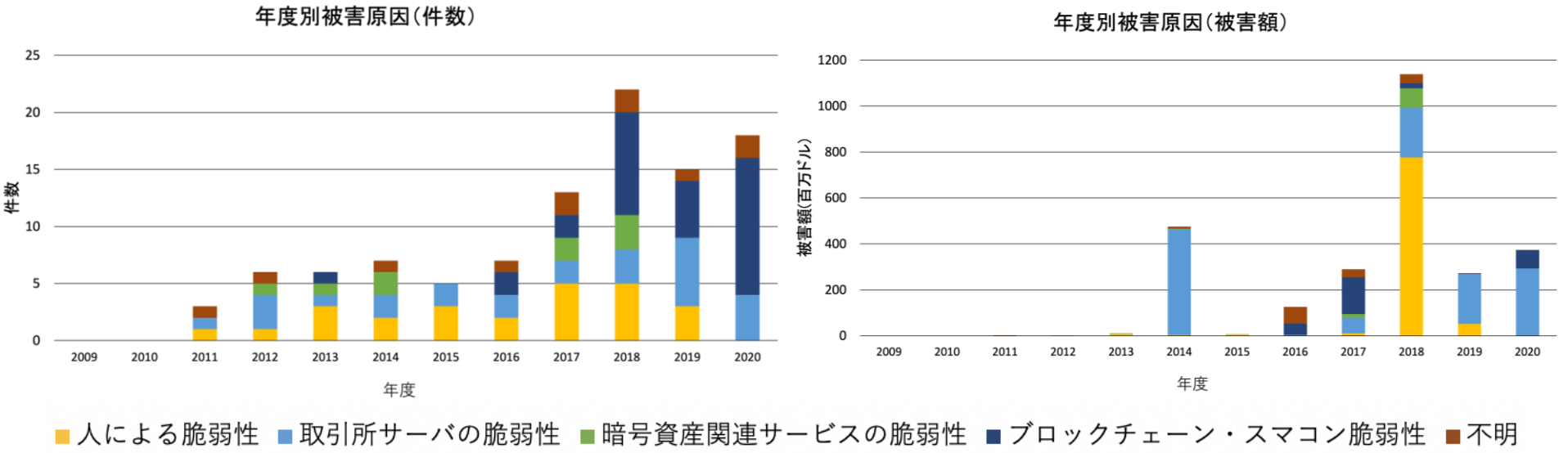
被害対象によりインシデントを分類



- 被害件数は取引所が最も多く、暗号資産関連サービスと銘柄がほぼ同等
- 被害額は取引所に対するインシデントが圧倒的に多い
  →取引所は多くのユーザーのウォレットを管理しているため、
  被害が大きくなりやすい
- 2017年頃から暗号資産関連サービス、2018年頃から銘柄の件数が増加傾向
  →DeFiやICOなどのスマートコントラクト関連の暗号資産サービスの増加、
  アルトコインの増加が原因

結果：被害原因による分類

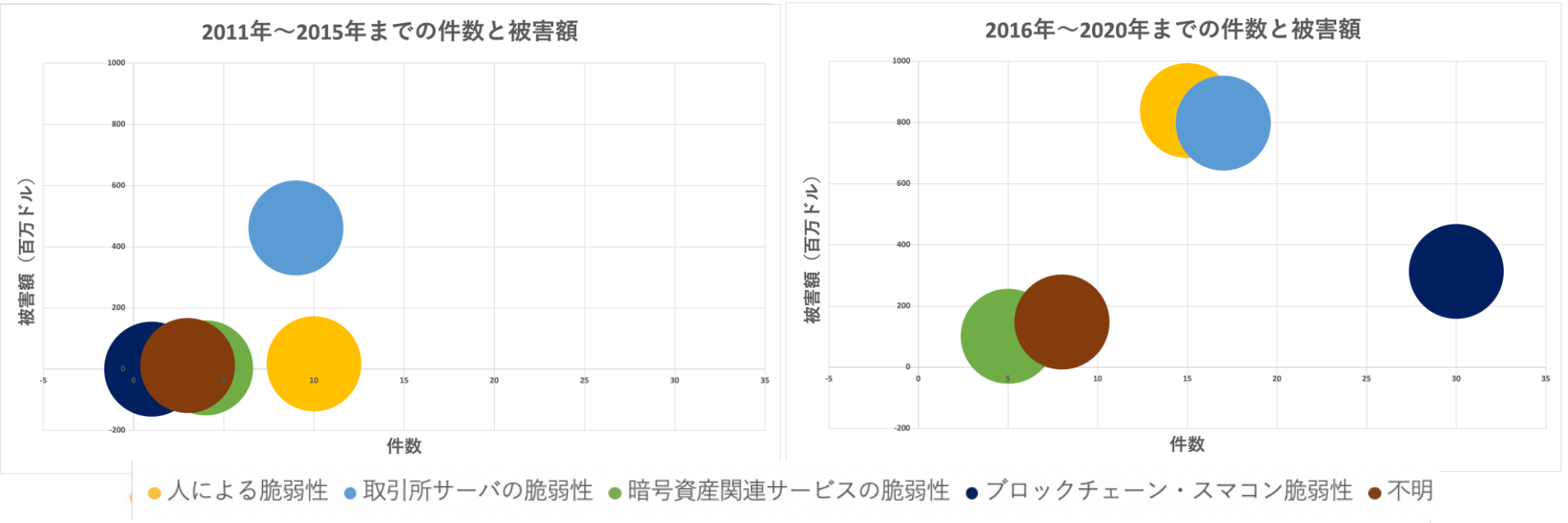
被害原因によりインシデントを分類



- **ブロックチェーン・スマコン脆弱性**によるインシデント件数が増加
  →アルトコインの増加、スマートコントラクトを用いたサービスや取引所の増加
- **取引所サーバの脆弱性**を原因としたインシデントは毎年発生しており被害額も他の原因より比較的多い
- 人による脆弱性のインシデントも、ほぼ毎年発生
  →近年、暗号資産関連サービスを利用した詐欺も発生

結果：被害原因による分類

5年毎（2011~2015 & 2016~2020）の被害原因の傾向



- 人による脆弱性のインシデントは常に件数が多く、被害額が大きく増加
  場合によっては一つのインシデントで巨額な被害額となるときがある
  →暗号資産を扱う上では、ユーザーも含め情報リテラシーを高く持つ必要
- ブロックチェーン・スマコン脆弱性の件数は増えているが被害額はさほど増えていない
- 取引所サーバの脆弱性は件数も被害額も増加
  比較的、件数＋被害額が他の被害原因より大きくなっている

結果のまとめと考察

・インシデント件数＋被害額の増加
　ー 暗号資産の価値・注目の高まりに応じてリスクも多様化

・**取引所**を対象＋原因としたインシデントが多数
　ー 多額の暗号資産を管理しているため、成功すれば大きな
　　利益・被害
　ー 取引所のリスク対策が重要

・**ブロックチェーン・スマコン**に関するインシデントも近年増加
　ー 新規のコインやスマコンを用いたサービスの増加
　　→セキュリティリスクが高い
　ー 分散型取引所も多くが被害の対象に

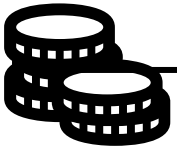
・人が持つ情報に対する知識や理解の不足が常に課題
　ー 暗号資産を扱う上では、ユーザーも含め情報リテラシーを
　　高く持つ必要

提言

ユーザー側

▶取引所や暗号資産関連サービスなどのリスクをよく理解

▶投資先を分散させる、新規サービスにむやみに手を出さないなど暗号資産と慎重に付き合う



サービス提供側

▶サービスを提供する上での統一的なセキュリティ基準などを定めるべき（例：日本のICOにおける被害は規制とともに減少）

▶ブロックチェーンに関するリスクだけでなく、暗号資産を扱うサービスのリスクについても注視・研究をするべき

参考文献

[1] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen：A survey on the security of blockchain systems, Future Generation Computer Systems, Vol. 107, pp. 841-853, 2020.

[2] Wang Zeli, Jin Hai, Dai Weiqi, Choo Kim-Kwang Raymond, Zou Deqing：Ethereum smart contract security research: survey and future research opportunities, Frontiers of Computer Science, Vol. 15, 152802, 2020.

[3] Grobys Klaus, Sapkota Niranjan：Contagion of Uncertainty: Transmission of Risk from the Cryptocurrency Market to the Foreign Exchange Market, SSRN Electronic Journal, 2019.

[4] Biais Bruno, Bisiere Christophe, Bouvard Matthieu, Casamatta Catherine, Menkveld Albert J：Equilibrium Bitcoin Pricing, SSRN Electronic Journal, 2018.