サイバー攻撃の被害者予測システムと攻撃利得低減方式の構築-

大阪大学　　宮地充子

超スマート社会の「悪」の研究（セコム科学技術振興財団）

https://www.secomzaidan.jp/tokutei.html

重要なのが，新しい社会でどのような「悪」が企てられているのか，そのありかや動機や目的を探り，来たるべき攻撃を予知することです．これによって，どのような攻撃が誰に対していつ仕掛けられるのかが高い蓋然性をもって予測でき、防御や回復のための手段を講じることができるようになります．そこから先は、技術と法律の世界になるわけです．

本研究では，文理融合によって、超スマート社会の安全・安心を飛躍的に高める研究を目指します．また，研究の中で， 近未来に企てられるであろう攻撃を検討した上で具体的に設定し、これの対策となる技術やマネジメント法をパイロットシステムとして示すことを目標とします．

背景とプロジェクトの目的

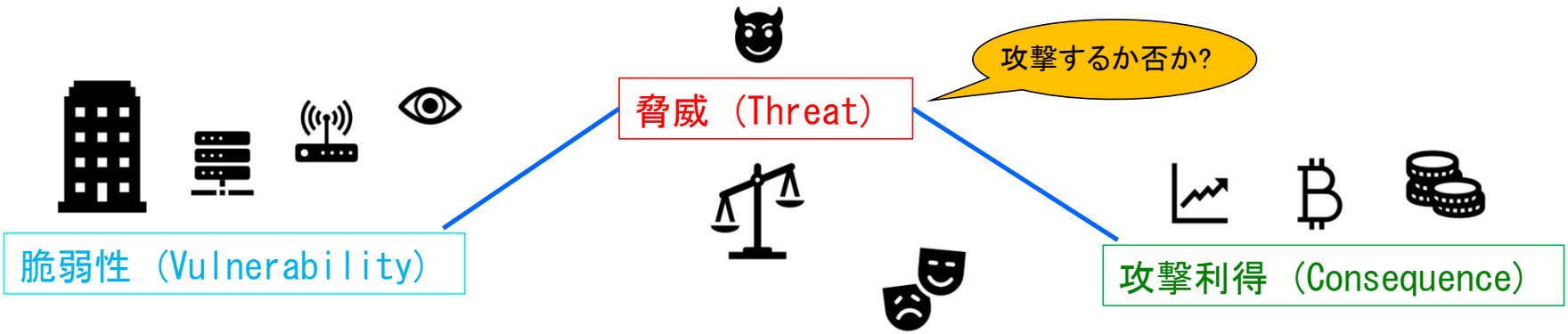
背景

近年，サイバー攻撃の目的が愉快犯から金銭目的，さらには国家支援の目的など，移行している．コロナ禍における，医療・製薬業界へのサイバー攻撃の急激な増加は創薬にかかわる機械学習の手法などの知的財産や詳細な個人情報を含む患者記録などの高価な情報の存在も重要な要素と考えられる．また，サイバー攻撃による医療機関の業務停止はサイバー攻撃が国民生活に直結することの現れともいえる．

一方，医療・製薬業界の全企業が攻撃被害を受けたわけではなく，攻撃者は攻撃対象を選択しているとも考えられる．つまり，近未来に企てられる攻撃への対策には，サイバー攻撃の予知とともに，攻撃対象から外されるような仕組みの構築が必要である．

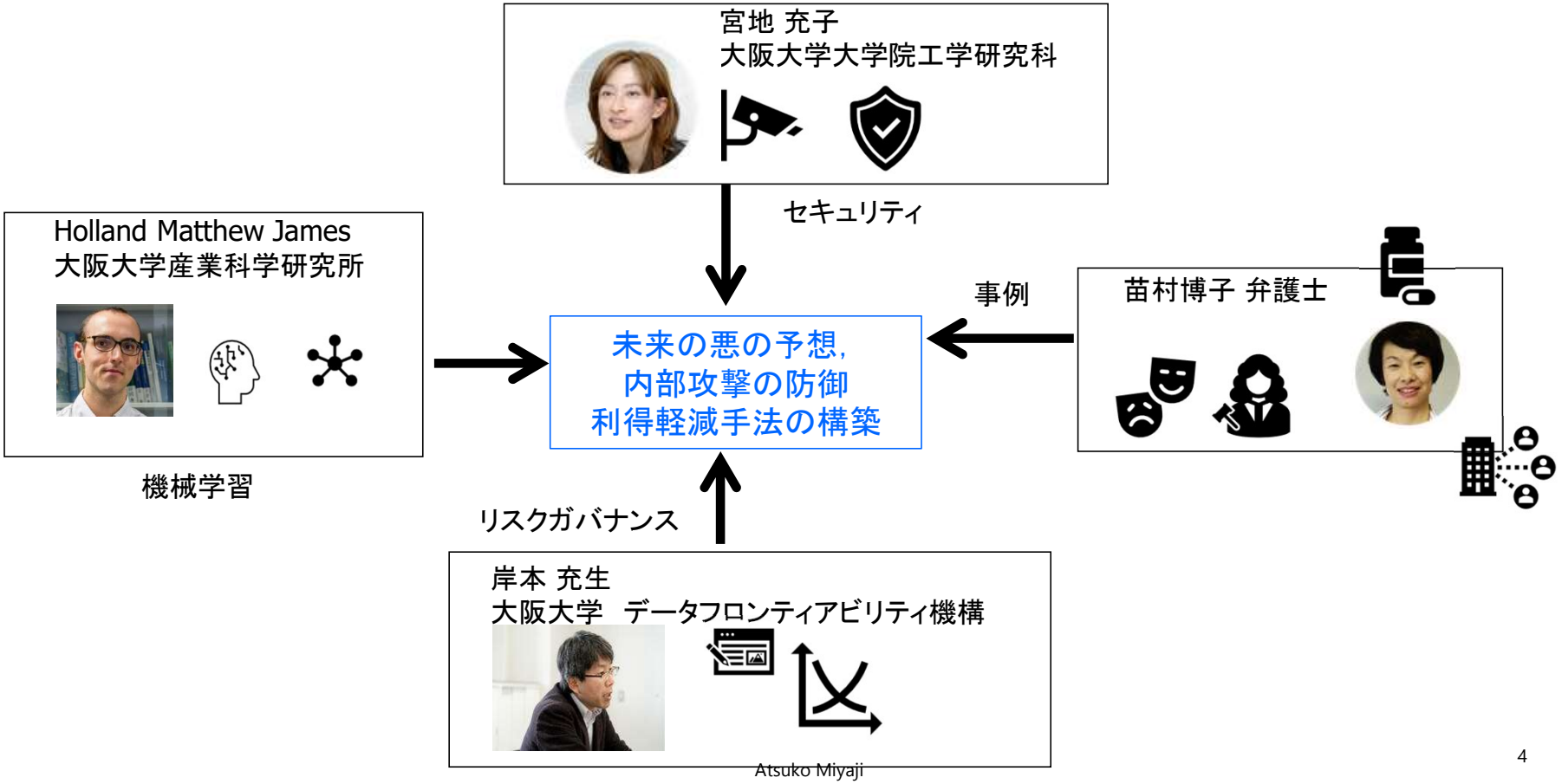
研究課題

研究課題1．脅威予測シミュレーションの構築
攻撃の動機や目的を探り，脆弱性と攻撃利得による脅威分析を実施し，近未来の攻撃の予知シミュレーションを構築．
研究課題2．攻撃利得軽減枠組みの構築
主観的攻撃利得を劣化させるデータ保管技術の構築



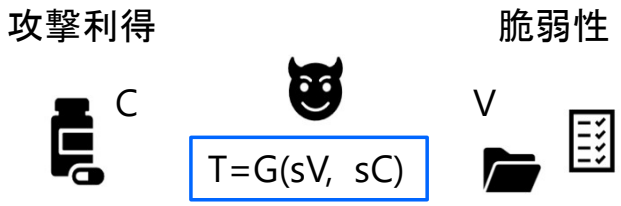
研究実施体制

悪と内部攻撃防御の必要因子 → リスクガバナンスと事例分析 → セキュリティと機械学習 解決プロトタイプ構築



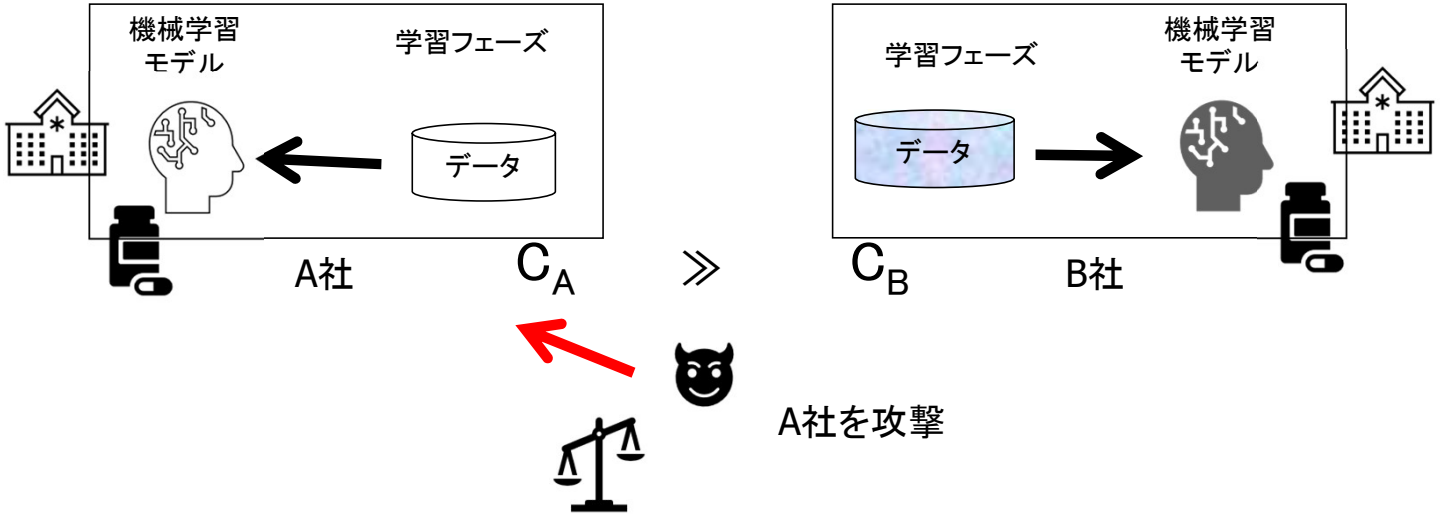
（研究課題1） 攻撃利得と脆弱性を用いた攻撃予測シミュレーション

・攻撃利得と脆弱性を鑑みて，脅威は決定する．
・脆弱性，攻撃利得を現状の分析により再構築．
・次に，脅威を再定義された脆弱性，攻撃利得から再構築．
　脅威= G((新）脆弱性，(新) 攻撃利得）



(研究課題2)攻撃利得軽減枠組みの構築

・攻撃利得軽減データの枠組みと機械学習の効果のバイデザインの構築.
・絶対なる安全はないという前提で, 攻撃利得を下げるアプローチ.



近未来の攻撃–サプライチェーン型攻撃への適応

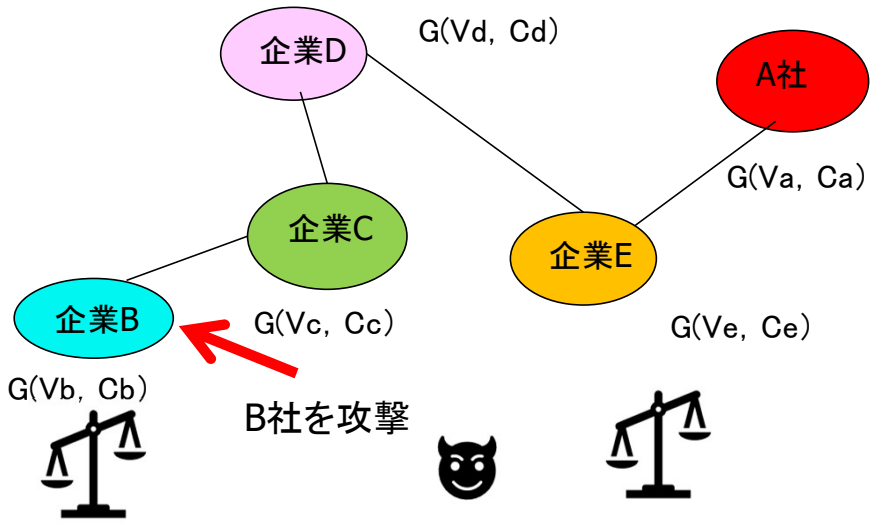
背景

サプライチェーンとは，製品の原材料・部品の調達から販売に至るまでの一連の流れを指します．企業間の繋がりは，製造現場だけではありません．地方公共団体，総合病院なども様々な業種が互いに関連して事業を継続しています．
昨今，世界中でサプライチェーン攻撃による被害が発生しています．サプライチェーン攻撃とは，組織間の業務上の繋がりを悪用し，比較的セキュリティレベルの低い取引先や子会社などを経由することで，ターゲット組織へ侵入します．
最終標的の組織は，子会社の侵入のため，侵入に気づかない間に攻撃を受ける危険性があります．

研究課題

研究課題1の脅威予測シミュレーションおよび，研究課題2の主観的攻撃利得劣化技術を適用することで，近未来のサプライチェーン攻撃を回避します．

サプライチェーン型



サプライチェーン型