資料2－2

総務省 公衆無線LAN
セキュリティ分科会

公衆無線LANセキュリティ課題の論点整理

～公衆無線LANの活用と2020大会成功へ向けて～

2017年12月1日

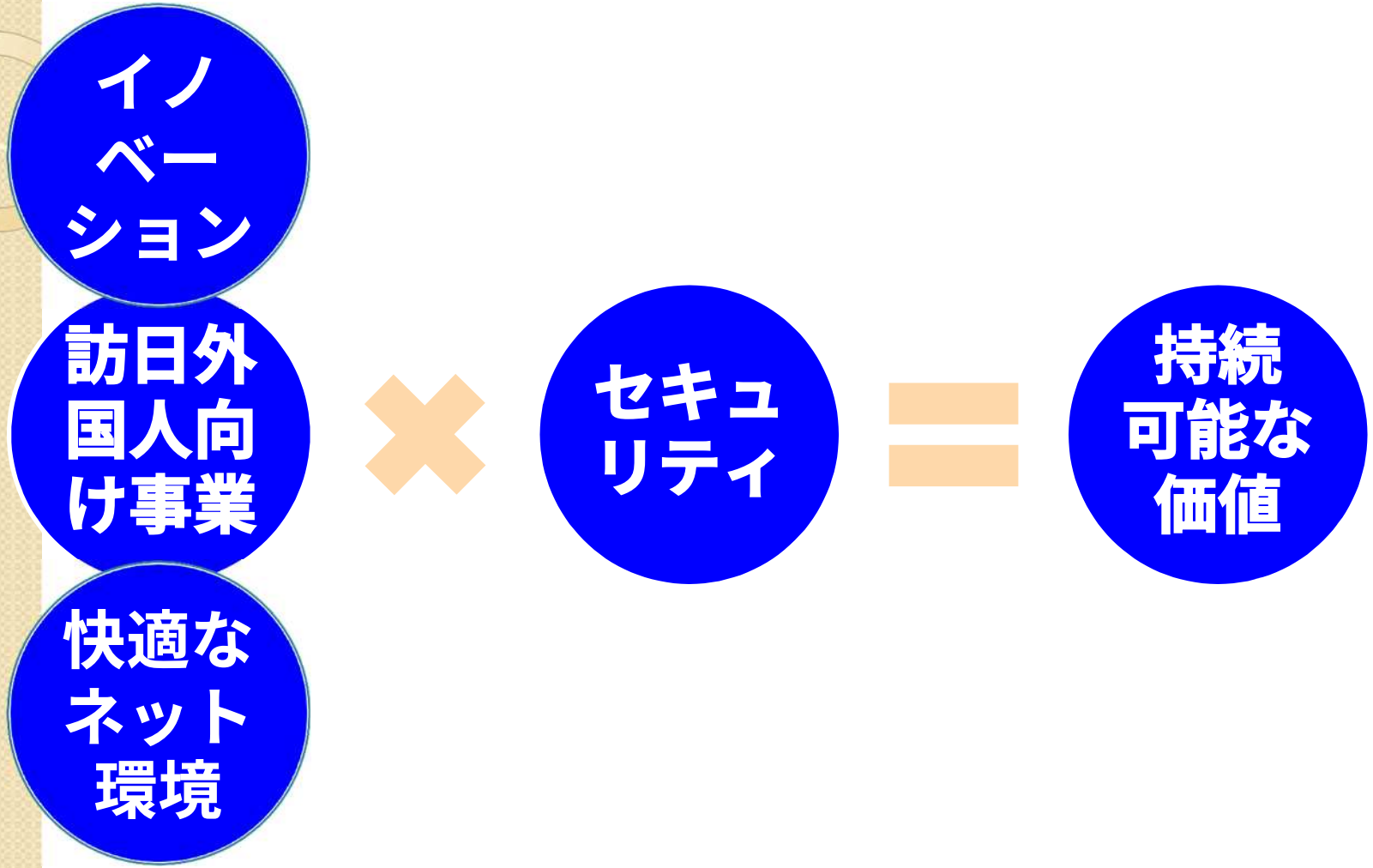
【本日のポイント】
①考え方
②ステークホルダーモデル化
③マトリクス型論点整理

富士通株式会社
サイバーセキュリティ事業戦略本部
セキュリティマイスター
佳山こうせつ

目次

- 考え方
- ステークホルダー整理モデル化
- マトリクス型整理

日本全体のセキュリティ意識をレガシーへ

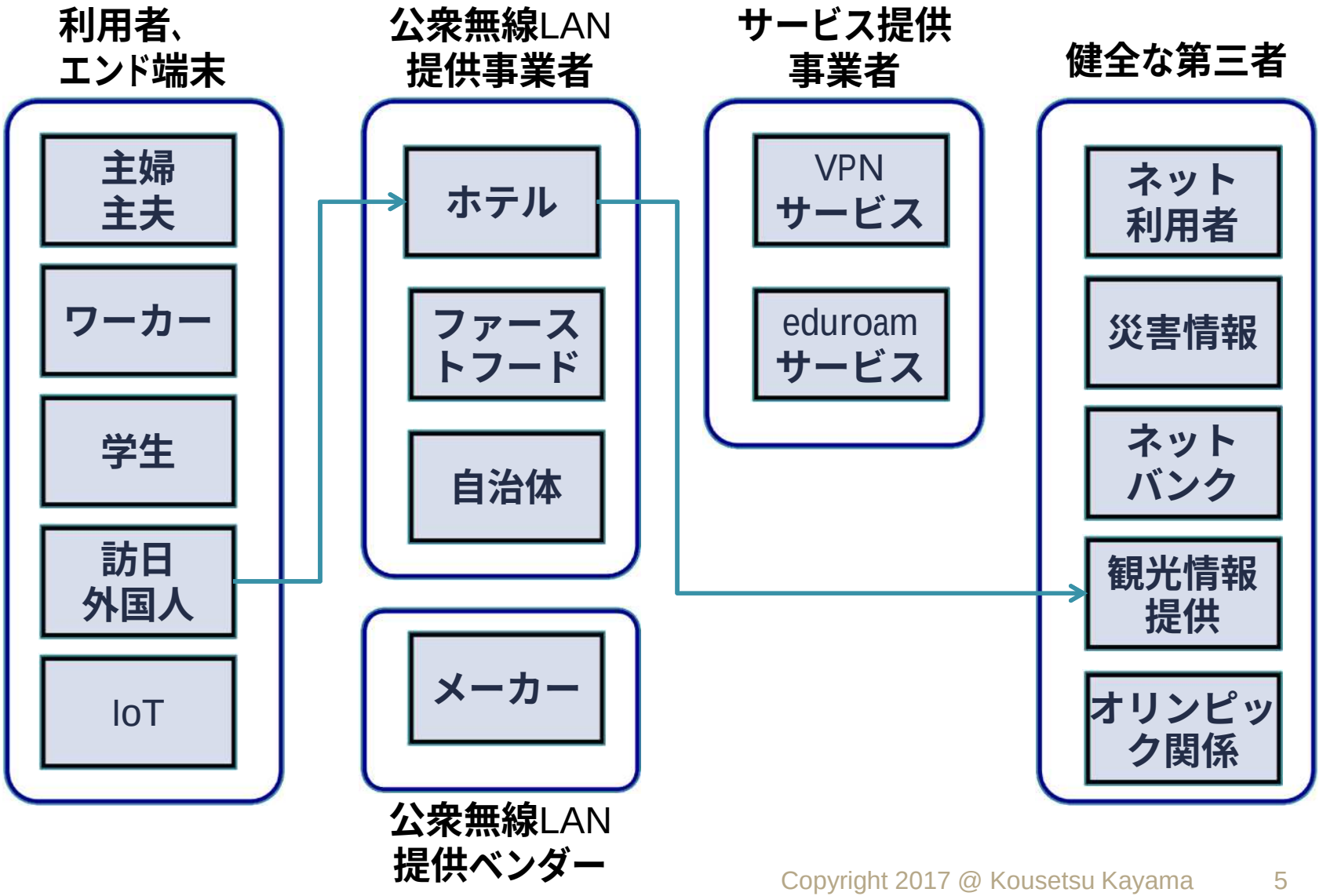


何かのためにセキュリティがあるという意識を産官学横断で醸成し脅威を正しく怖がる

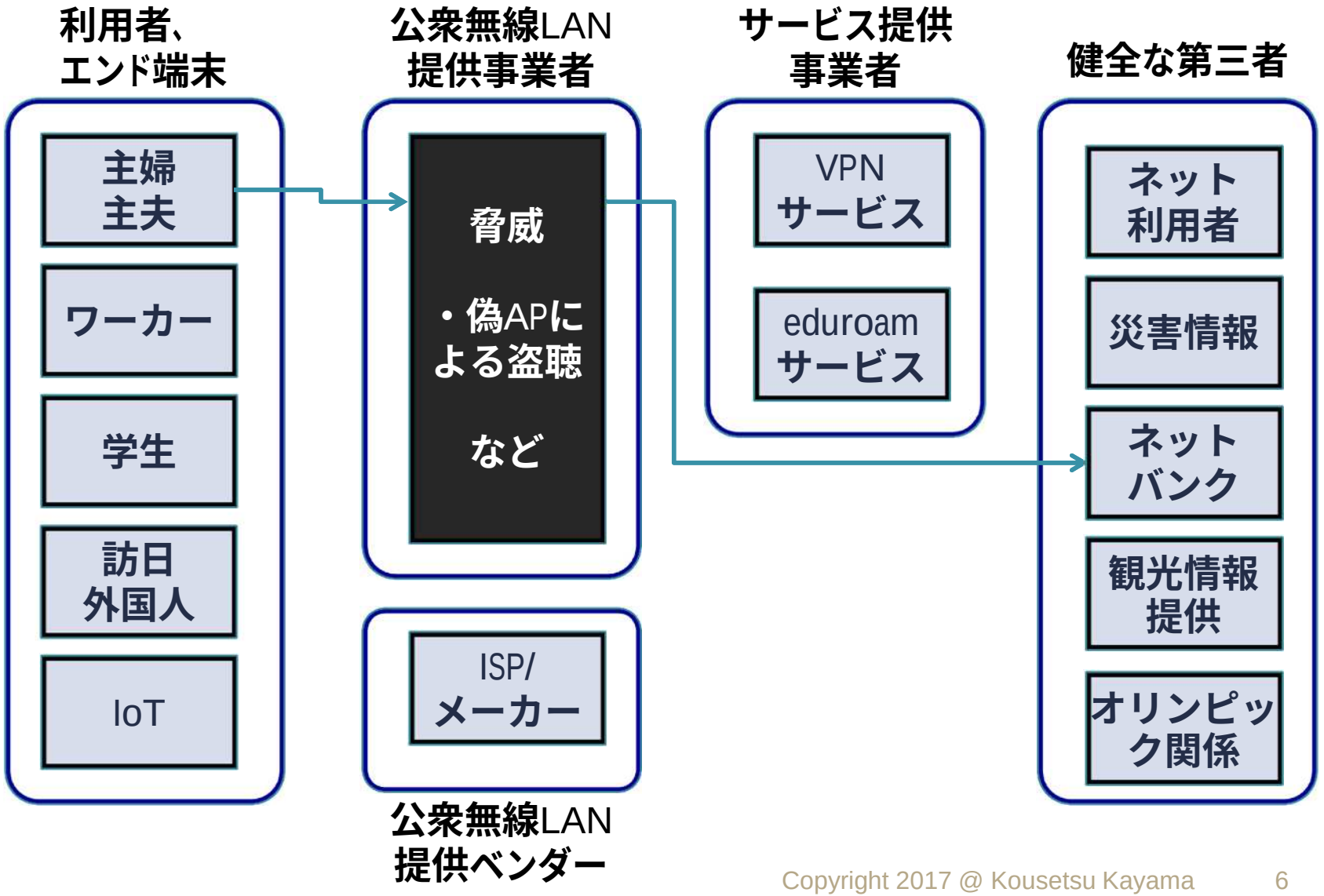
目次

- 考え方
- ステークホルダーモデル化
- マトリクス型整理

ステークホルダーモデル化



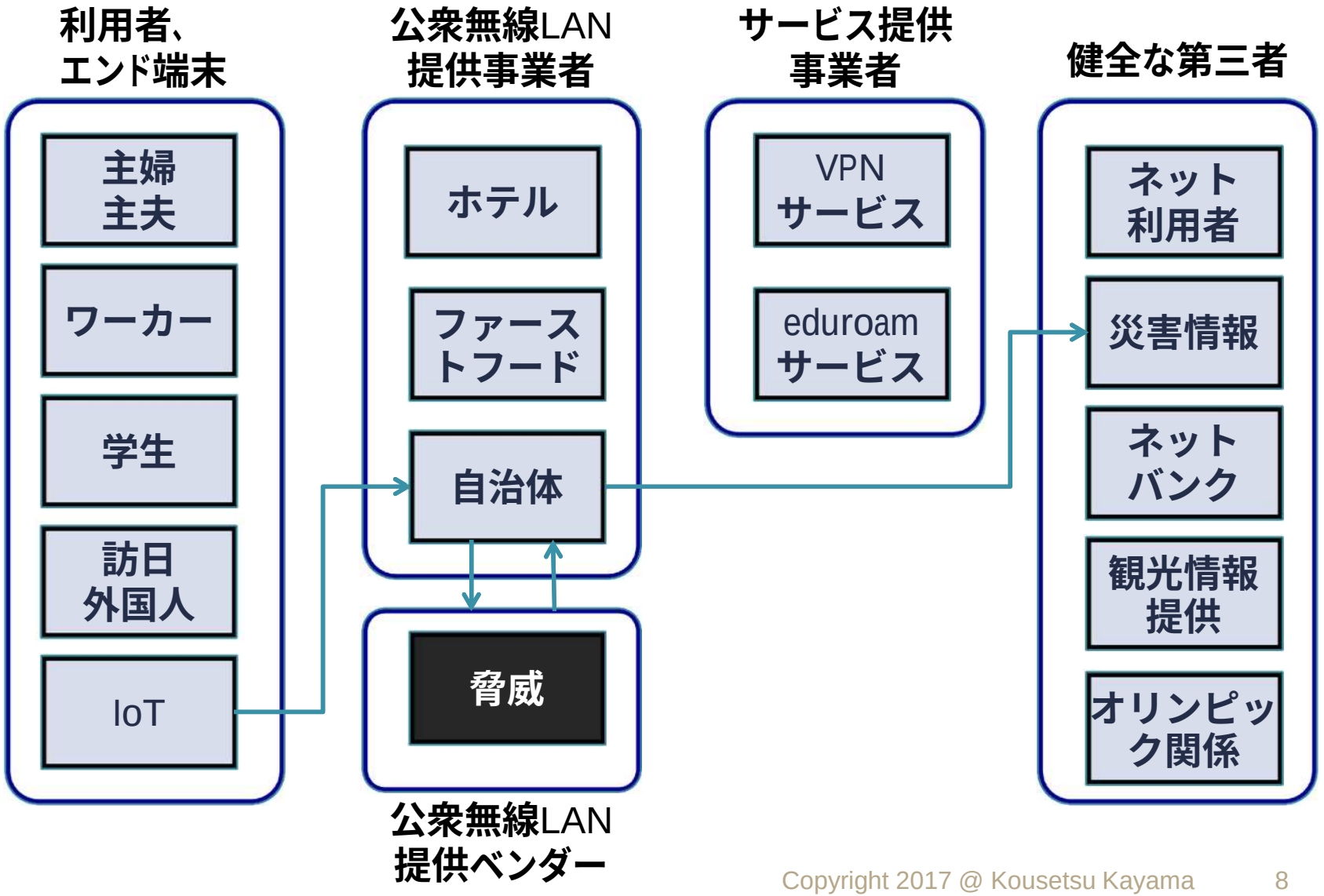
ステークホルダーモデル化
ケーススタディ①：公衆無線LAN提供事業者に脅威



ステークホルダーモデル化
ケーススタディ①：公衆無線LAN提供事業者に脅威

対象	**利用者、 エンド端末**	**提供事業者**
想定被害	**金銭的被害 のっとり 誘導**	**風評被害**
発展被害	**攻撃への加担**	**脅迫**
対策	**脅威把握し、 安全な利用形態を促進**	**脅威把握し安全な利用形態を仕様化**

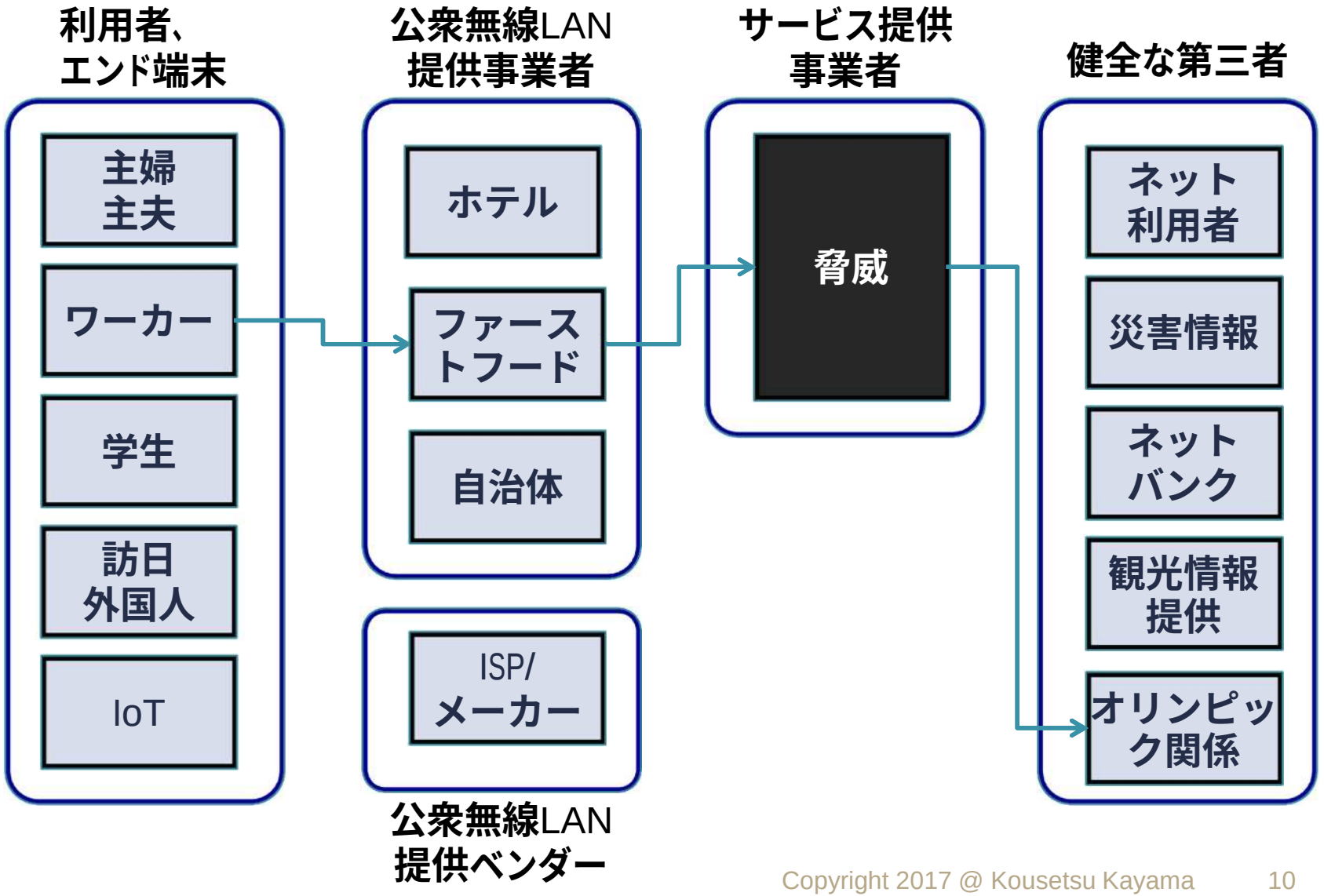
ステークホルダーモデル化
ケーススタディ②：公衆無線LAN提供ベンダーに脅威



ステークホルダーモデル化
ケーススタディ②：公衆無線LAN提供ベンダーに脅威

対象	**利用者、エンド端末**
想定被害	**金銭的被害** **のっとり** **誘導**
発展被害	**脅迫** **攻撃への加担**
対策	**脅威把握** **VPN利用の促進**

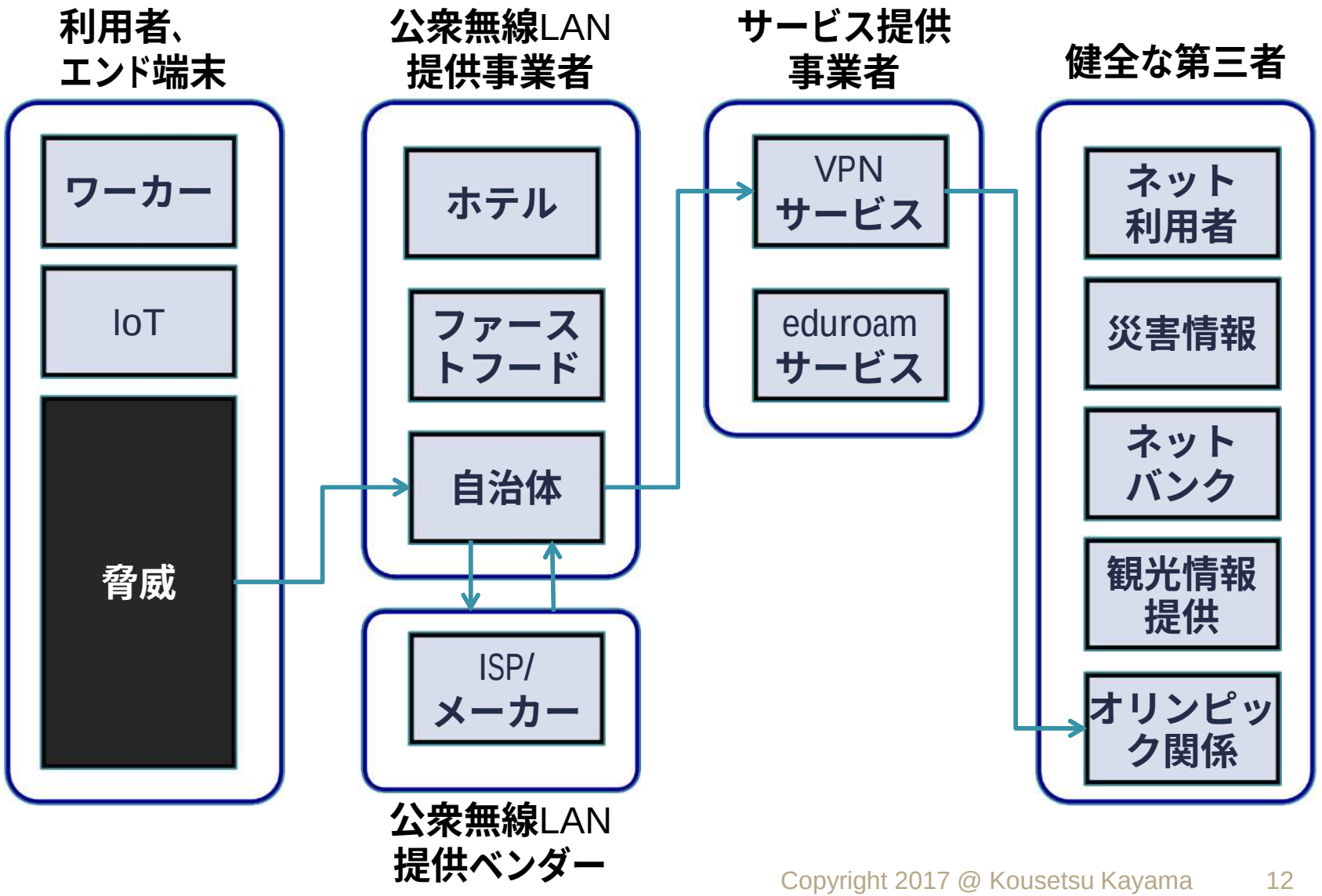
ステークホルダーモデル化
ケーススタディ③：サービス提供事業者に脅威



ステークホルダーモデル化
ケーススタディ③：サービス提供事業者に脅威

対象	利用者、エンド端末
想定被害	金銭的被害 のっとり 誘導
発展被害	脅迫 攻撃への加担
対策	脅威把握 有料で優良なVPN利用促進 国や業界団体がお墨付き

ステークホルダーモデル化
ケーススタディ④：利用者に脅威



ステークホルダーモデル化
ケーススタディ④：利用者に脅威

対象	利用者、 エンド端末	公衆無線LAN 提供事業者	公衆無線LAN 提供ベンダー	サービス 提供事業者	健全な 第三者
想定 被害	同一AP内の 盗聴やウイ ルス感染	風評被害	風評被害	風評被害	事業の継続 性損害
発展 被害	誤認逮捕	脅迫、捜査 協力コスト	脅迫、捜査協 力コスト	脅迫、捜査 協力コスト	組織的疲弊
対策	VPN利用	悪用防止、 本人確認を サービスとし て提供	悪用防止、トレーサビリティに必要な機能の提供	悪用防止、 本人確認と ローミング サービスな どを提供	レスポンス 体制の整備
	脅威把握 事後追跡性 定期的な統合訓練				

目次

- 考え方
- ステークホルダー整理モデル化
- マトリクス型整理

ステークホルダーを軸にまとめ

～今後の論点を整理～

	利用者、エンド端末	公衆無線LAN提供事業者	公衆無線LAN提供ベンダー	サービス提供事業者	健全な第三者
モチベーション	快適なネット環境で情報入手	お客様の誘致	需要の獲得	新たなサービスの開拓	憂いなくデータ利活用や本業を推進
対策	脅威把握し安全な利用を促進	脅威把握し安全な利用形態を仕様化	トレーサビリティに必要な機能の提供	本人確認やローミングサービスなどを提供	レスポンス体制の整備
考えるべき課題例	促進方法、リテラシ教育	指導方法、体制支援と優遇制度	トレーサビリティなど必要な機能と設計手法の提示	国や業界団体のお墨付きプロセス	事態対処訓練

Innovation Centric Security

守るセキュリティからつなげるセキュリティを
産官学横断で実現