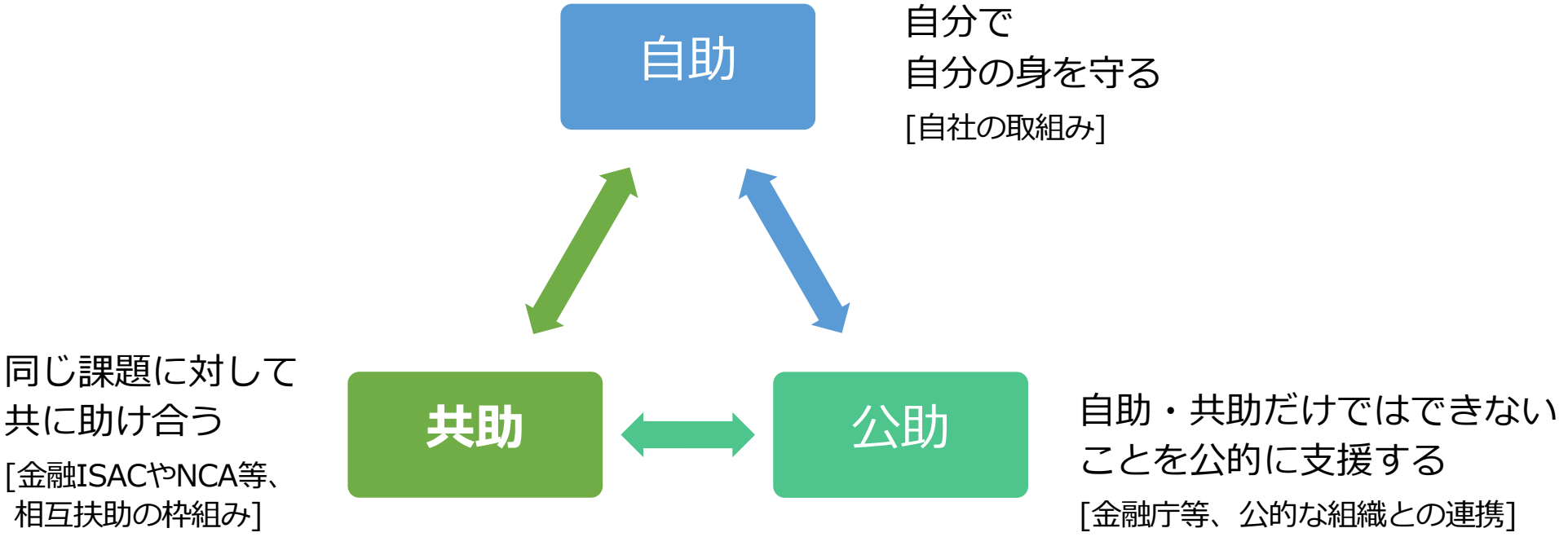
Fast, Frank, and Friendly
Financials ISAC Japan

OSSのセキュリティ
～金融業界の視点から～

一般社団法人 金融ISAC
鎌田敬介
kamata@f-isac.jp

金融ISACとは

- **金融ISAC**は、金融業界のサイバーセキュリティ分野における「**共助**」を実現するための一般社団法人です。銀行、保険、証券などを中心に約430社が会員



活動の柱

- サイバーセキュリティに係る脅威に対する防衛力を向上・維持するために、**2つの活動の柱**のもとで日々活動しています

コレクティブ インテリジェンス

◇ 各社で検知したインシデント、脆弱性情報等を共有する
◇ より多くのより正確な情報が互いを強固にする

リソースシェアリング

◇ ワーキンググループ活動を通じ、共通の課題への対応・対策の検討を進める
◇ 共に取組むことで、限られたリソースを有効活用する

✓ カンファレンス
✓ 情報共有　など

ISACの基盤

✓ 成果物の共同開発
✓ 共同演習の実施　など

金融業界にとってのOSSのセキュリティ？

- OSSに特化して何かしているか、というと、そうではない？
- ユーザ企業におけるOSSの位置づけとは？
- OSSが話題に出てくる場面は？

脆弱性対応の難しさ

- 脆弱性情報が公表された際にリスクや脅威度をどう判定するか？
- コレクティブインテリジェンスとして、多角的な分析情報を共有
- CVSSの値に頼っていいのか？
- 技術的に理解することが最善ではあるが…
- 脆弱性単体のリスク＋環境要因
  - ＋サプライチェーン

OSSに特化した脆弱性対応のいくつかの観点

- ソースコードが公開されているので脆弱性に関する詳細情報が大量に出てくることがある
- 脆弱性の実証コードや攻撃コードが出やすい
- あるOSSに脆弱性が出た場合、そのOSSが組み込まれた製品も影響を受けるが、ベンダの対応にタイムラグが発生する
- 著名OSSの深刻な脆弱性が一度見つかると同じソフトウエアの脆弱性が繰り返し発見される（？）
- ソースが公開されているのでその気になれば自分で直せる！が、一般的には難しい（出来る人にとっては簡単）

海外の金融機関の事例

- 自社で使っている著名OSSの開発者を雇う
- ↑により脆弱性が出たときに迅速に対応できる
- そういう人は優秀なITエンジニアでもある
- OSS開発の推進を間接的に支援（社会貢献になる）
- ある金融機関のペンテストチームはOSSツールしか使っていない

OSSのセキュリティ（再）

- OSSに特化して何か、はしてはいない。そもそも特にOSSであるかどうかについて特別に意識していない？

- 「OSSの思想」と「企業ITの姿勢」の乖離

- OSSに特化してユーザー企業が考えるべきセキュリティは脆弱性対応だけなのか？

- SBOMの先にありそうなもの

Fast, Frank, and Friendly

Financials ISAC Japan