資料２－２

Fast, Frank, and Friendly
Financials ISAC Japan

金融ISACの協働活動について

一般社団法人 金融ISAC

<https://www.f-isac.jp>

組織概要

名称	一般社団法人 金融ISAC			
設立	2014年8月			
会員数 (2024年7月末時点)	正会員	434社		
		内訳	銀行・信金信組・労金	255社
			証券	56社
			生損保	60社
			クレジット	14社
			金融持株会社等	49社
	トライアル会員	7社		
	アフィリエイト会員	28社		
	賛助会員	2社 (JPCERT/CC 殿、生命保険協会 殿)		
構成	理事 4名 (常勤 3)、監事 1名、事務局員 5名			
沿革	2012年　前身となるコミュニティ (CISS) を設立 2014年4月　設立準備会を設置 2014年8月　一般社団法人 金融ISAC設立 2015年4月　米国FS-ISACとアフィリエイト合意			

金融ISAC

Fast, Frank, and Friendly
Financials ISAC Japan

■**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**を実現するための組織です

[三助]

自助

自分たちで
自分たちの身を助ける
(自社の取組み)

共助

共に助け合う
(金融ISAC等、
相互扶助の枠組み)

公助

自助・共助ではできないことを
公的な組織が助ける
(金融庁等、公的な組織との連携)

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
✓ SIGNAL・WGでの情報共有　など

ISACの基盤

✓ 成果物の共同開発
✓ 共同演習の実施　など

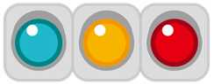
SIGNAL

コレクティブ インテリジェンス | リソース シェアリング

- **SIGNAL**は、インシデントや脆弱性等に関するタイムリーな情報を共有するためのポータルサイトです
- **TLP**に従って情報共有の範囲・対象をコントロールしています

[SIGNAL]

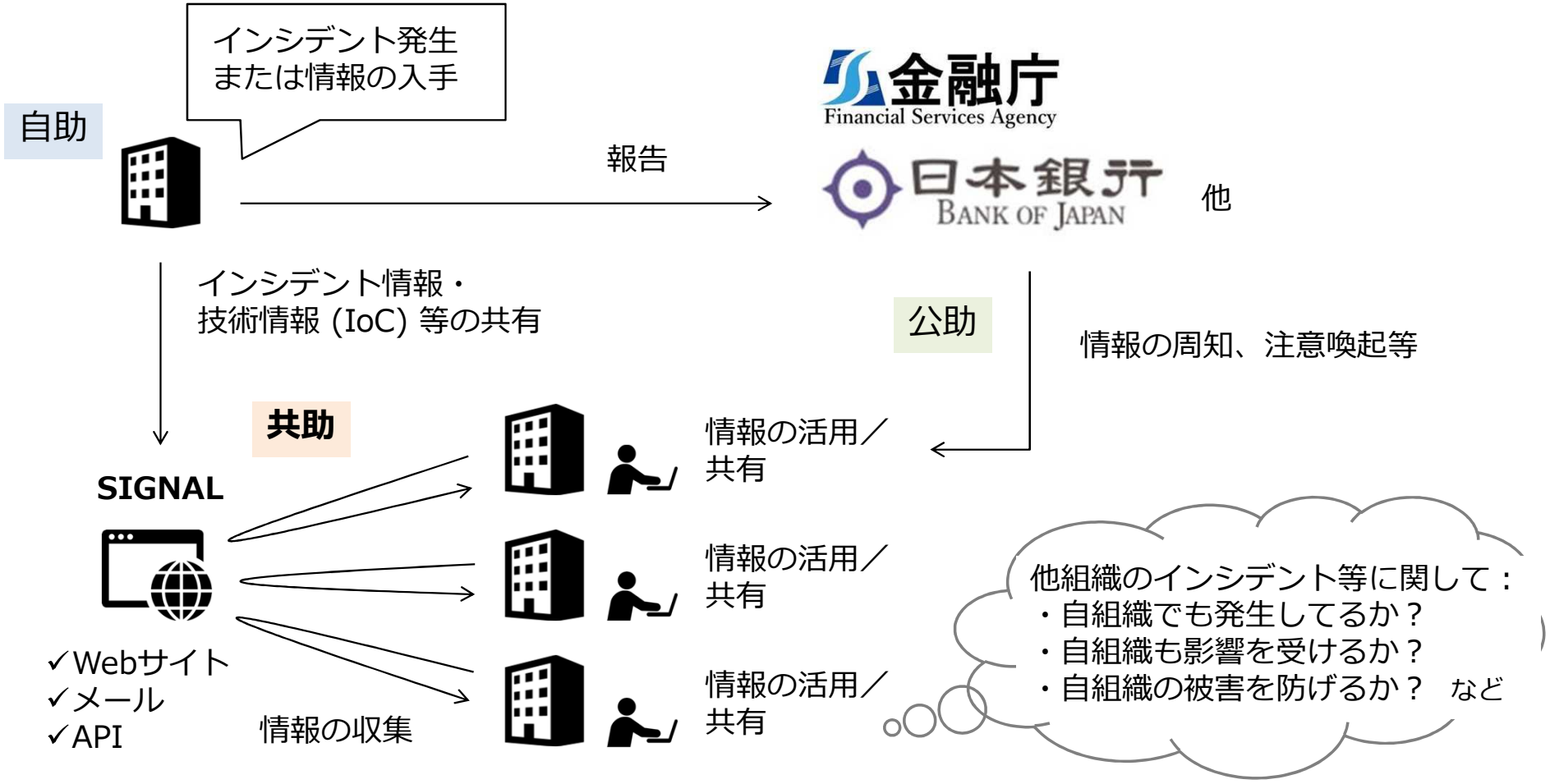
[TLP: Traffic Light Protocol]



Red/赤	情報を直接共有した範囲に厳密に限定される
Amber+ STRICT/黄	情報を共有した特定のグループ (会議参加者等) 内に情報を留め、特定グループ外への情報の持ち出しは不可 (所属組織内でも共有不可)
Amber/黄	情報を必要とする先に対して、守秘を管理できる範囲でのみ共有を可とする (会員のシステム・サービスを守ること以外を目的とした使用は不可)
Green/緑	情報を必要とする先に対して、共有を可とする
Clear/白	公知の情報として扱う

情報の収集と活用

コレクティブ インテリジェンス | リソース シェアリング



情報の収集と活用：事例

コレクティブ インテリジェンス | リソース シェアリング

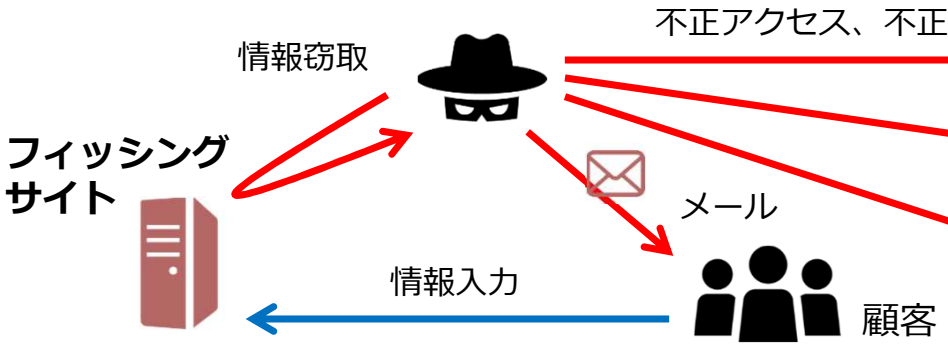
■DDoS事案に関する情報共有

Fast, Frank, and Friendly
Financials ISAC Japan

会員企業間での情報共有：
- 事案に関する情報共有
- 攻撃手口に関する情報共有
- 対応に関する相談・情報共有

など

■フィッシング事案や対策に関する情報共有



Fast, Frank, and Friendly
Financials ISAC Japan

会員企業間での情報共有：
- 事案に関する情報共有
- 対応に関する相談・事例共有
- 対策に関する相談・情報共有

など

カンファレンス

コレクティブ インテリジェンス | リソース シェアリング

■年に2回実施する大規模カンファレンスを通じて、会員間で「**互いに顔の見える信頼関係**」の構築・醸成を目指しています

#	時期	場所	主な内容
アニュアル カンファレンス	5～6月頃	東京	✓ WG活動等に関する年次報告
フォール カンファレンス	10～11月頃	地域	✓ WG活動等に関するアップデート ✓ WGの出張ワークショップ

ワーキンググループ (WG)

コレクティブ インテリジェンス | **リソース シェアリング**

■ 「**各社の共通課題**」に対応するWG、および業態別コミュニティ

インシデント対応 WG	共同演習 WG	不正送金対策 WG	グローバル 情報連携 WG
スキルアップ WG	インテリジェンス WG	ベスト プラクティス WG	脆弱性対応 WG
FinTech セキュリティ WG	AKC WG (Active Knowledge Center)	セキュリティ オペレーション 高度化WG	Next Generation WG
内部監査 WG			

＋ 業態別コミュニティ
(地銀、信金、証券、生保他)

WGの主な活動

コレクティブ インテリジェンス | **リソース シェアリング**

① **会議体**の開催

✓ 企画の進捗状況の共有
✓ WGのテーマに関連する勉強会　など


② SIGNAL等での**情報共有**

✓ WGメンバー間の情報共有、お悩み相談　など


③ **成果物**の作成、**イベント**の開催

✓ WGメンバー有志による企画・開発活動　など


原則、正会員は
自由に参照可能

[主な成果物]

- インシデント対応マニュアル
- 脆弱性対応マニュアル
- サイバー攻撃対策
  ベストプラクティスガイド　など

[主なイベント]

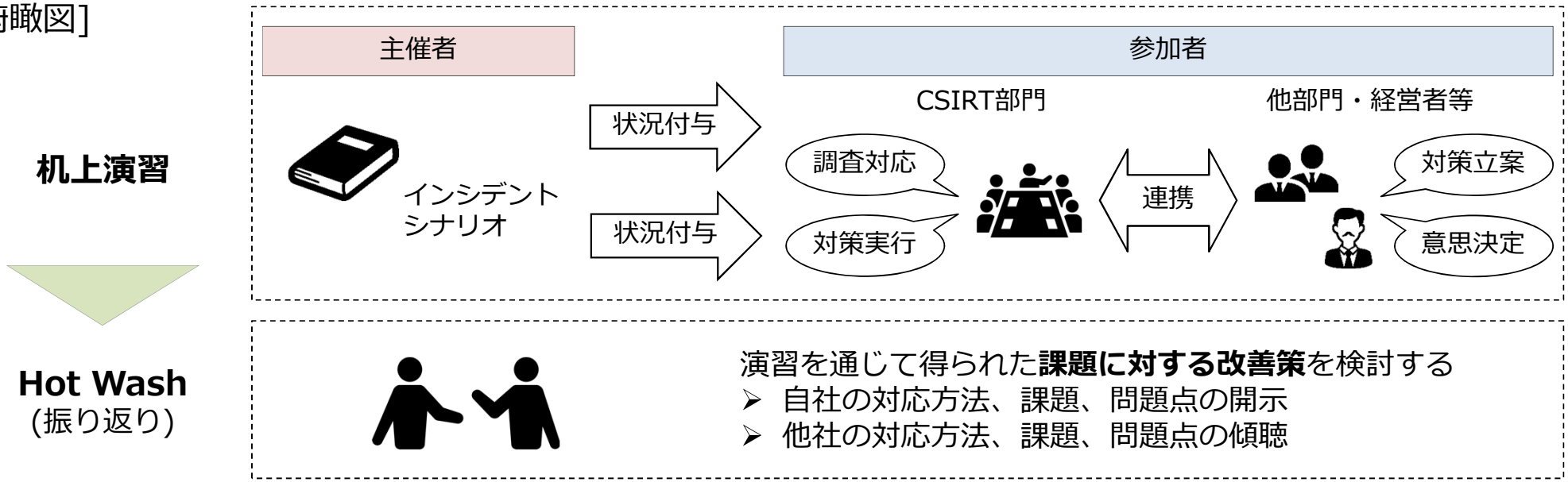
- 共同演習
- ワークショップ
- 勉強会　など

例：組織のスキルアップ

コレクティブ インテリジェンス | **リソース シェアリング**

■法人向け共同演習「FIRE」

[俯瞰図]



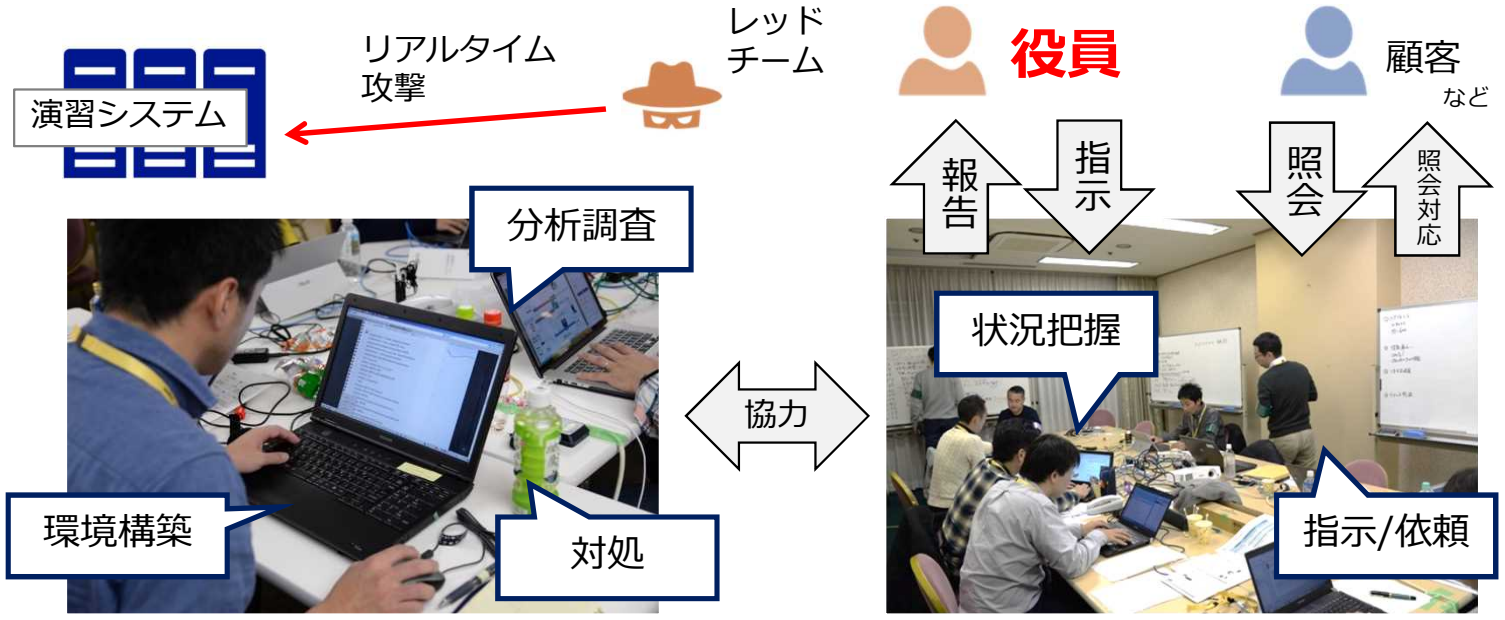
[過去の実施実績]

- ✓ FIRE (毎年8月頃実施)
- ✓ FIRE CowN (NISC分野横断的演習と同時開催)
- ✓ Delta Wallシナリオ解説会 (2023年～)
  in 東京・京都・名古屋・金沢・岡山・北九州
- ✓ 地域演習 in Osaka (2019年1月25日)
- ✓ ミニ地域演習 in Nagoya (2018年2月15日)
- ✓ 地域演習 in Toyama (2017年2月24日)
- ✓ 地域演習 in Kochi (2017年12月1日)

例：個人のスキルアップ

コレクティブ インテリジェンス | **リソース シェアリング**

■総合危機管理演習「サイバークエスト」



技術チーム（システム部門相当）　　**管理チーム**（CSIRT相当）

- ✓ 架空の金融機関の一員としてインシデントに対処する、**1泊2日の実機演習**
- ✓ 技術的な対応だけでなく、顧客対応や経営、関連機関への連絡等を体験する
- ✓ **実際にサイバー攻撃を受けたらどうなるか**、身を持って体験することができる
- ✓ 演習用の即席チームを組成し、**他社の参加者との交流**も図る

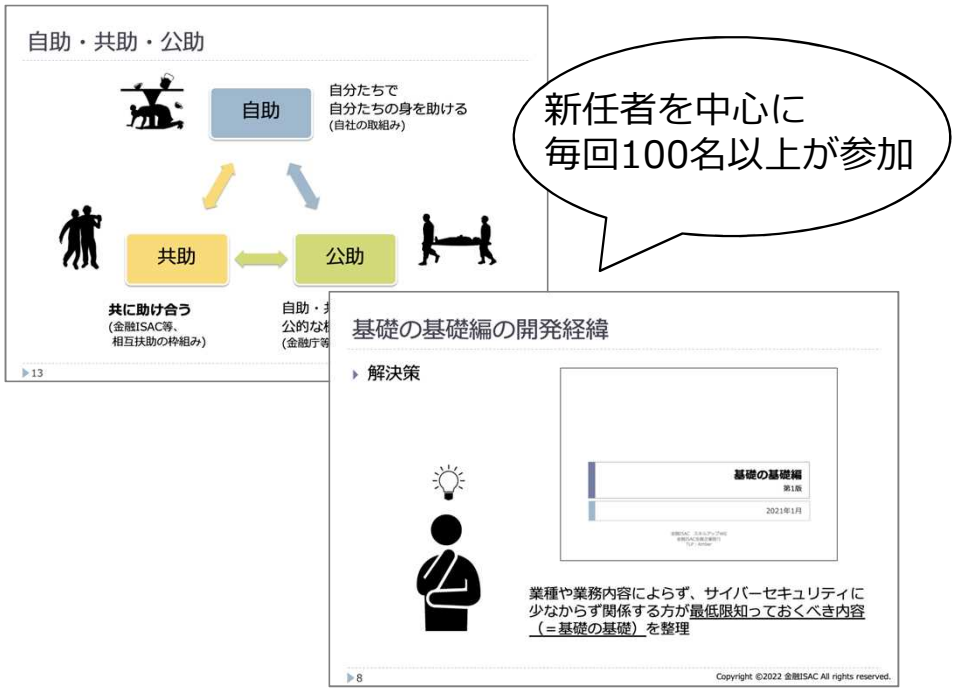
例：新任者のスキルアップ

コレクティブ インテリジェンス

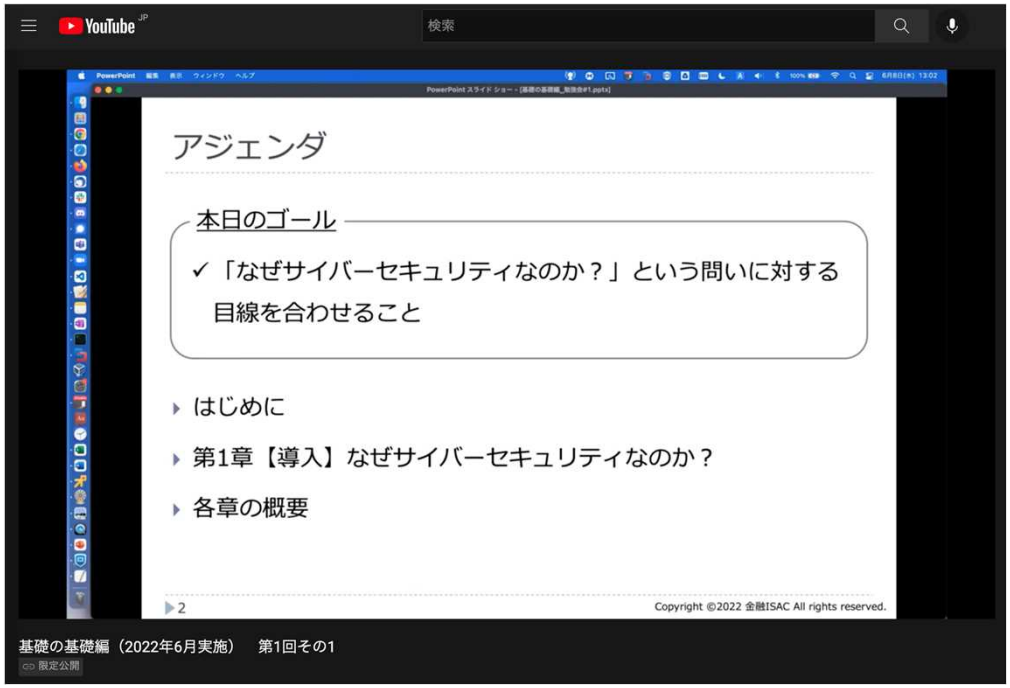
リソース シェアリング

■初任者向け教材「基礎の基礎編」

[教材を活用した勉強会]

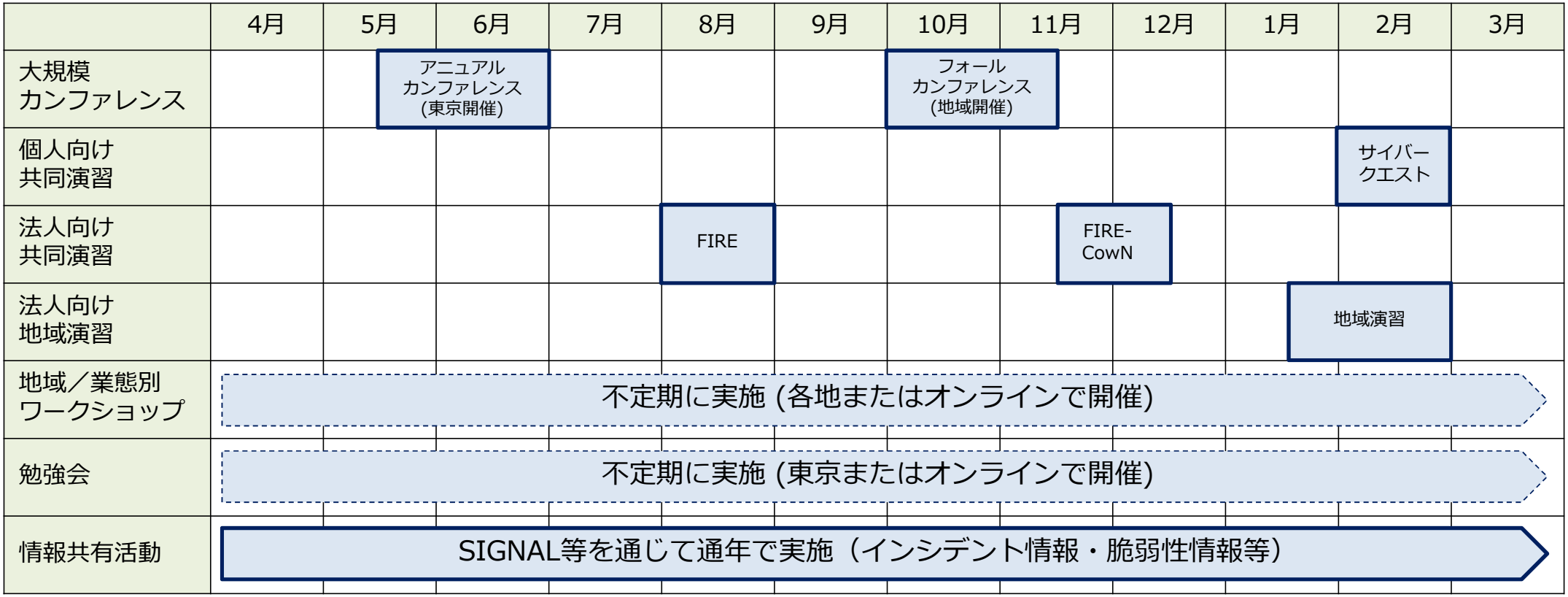


[動画配信]



金融ISACの一年

■会員である**金融機関に特化した各種イベント**を開催しています



金融ISAC活動のメリット

① 有事および平時のサイバーセキュリティ対策・対応の高度化

日々進化する攻撃手法を把握し**適切な対策・対応を講じる**ための**ヒントや答え**が得られる

サイバーセキュリティで相対するのは「お客さま」ではなく「攻撃者」なので攻撃動向に合わせた対策・対応が必要不可欠であり、金融ISAC活動が効果的です

自社の対策・対応を検討する上で**陥りがちなバイアス (先入観) を回避**できる

組織を跨った情報共有により、陥りがちなバイアス (大したことはない、関係ない) を排除でき、より客観的な検討が可能になります

他組織の知見を活用し、**自組織のレベルアップに役立たせる**ことができる

金融ISACの膨大な情報や成果物を活用することで、追加の費用発生なく金融業界の他組織の知見を取り入れることができます

② 他組織との関係構築・連携強化

他組織の事例・実態を把握できたり**共に助け合う業界内の仲間**ができる

情報を積極的に共有・交換することで他組織の取組事例や生の情報が得られる可能性があります

金融業界の仲間ができるのも金融ISACだからこそです

③ 知識とスキルの習得・向上

挑戦と失敗が許される場所で多くの経験が得られる

自組織の営利に直接関係しない場だからこそ、挑戦と失敗の繰り返しによる成長が可能です

同業者との会話や連携は大きな刺激になります

下記について、**原則として会費の範囲内で自由にご参加・ご利用**いただけます
(交通費・宿泊費等は除く)

- ✓ 各種情報
- ✓ イベント (カンファレンス、勉強会等)
- ✓ 各種ガイド・マニュアル
- ✓ 教育教材
- ✓ 演習　など

有識者会議へのコメント

- **重要インフラ事業者等の対策強化**
  - ✓ 金融では大手向のFFIEC（米国連邦金融機関審査委員会）のCybersecurity Assessment Tool、CRI(Cyber Risk Institute)のThe Profile、中小向では金融庁のサイバーセキュリティ・アセスメント・ツールといった金融に合わせたツールがあり、グローバルなスタンダート化も進行している状況。

  - ✓ レポーティングについてもFSB（金融安定理事会。主要国金融当局により構成される）でFormat for Incident Reporting Exchangeの議論が進んでいる。

  - ✓ ISACは業界毎であるが故に、より効率的で適切な共有が可能になっていると考えている。

  - ✓ ISACはクリントン政権下の大統領令で作られたものであるが、最も有名なFS-ISACは2012年の#OP Ababilを契機に競争相手の垣根を越えて情報共有を行う機運が当事者の間で高まり、今の活動が本格的にスタートしたと言われている。価値のある情報共有は自律的な発言の安全が守られたコミュニティに存在する精神のもと、共有活動は会員（民間）の間のみに厳しく制限している。（TLP(Traffic Light Protocol）でコントロールされている）

有識者会議へのコメント

✓ US金融の主な官民連携
- FS-ISACとは別にFSSCC（民、米国金融サービスセクター連携協議会）とFBIIC（官、米国金融銀行情報インフラ委員会）の協働。
（UKはCMORG（Cross Market Operational Resilience Group））
- DHS（米国国土安全保障省）からのアドバイザリー
- CISOから現場担当者に至るまで、軍・法執行機関関係者が多く、重要な人材輩出元となっている。

✓ 日本の金融の官民連携
- サイバーセキュリティ対策関係者連携会議にて、金融庁・日銀、金融協会、FISC（財団法人金融情報システムセンター）、JPX（日本取引所グループ）、金融ISAC間で情報共有を実施している。
- 金融庁・日銀・金融ISACで脆弱性情報（dailyの脆弱性、KEV（Known Exploited Vulnerabilities））の共有を行っている。
- G-7CEG（サイバーエキスパートグループ、G7及びEUの金融当局により構成される。各国から民間代表も参加）や個別の協議を通じて、認識の共有を図っている。

有識者会議へのコメント

✓ 官民連携の在り方

- 同種のサービス、システムを保有するため、同じような脆弱性や攻撃リスクを抱える組織間で競合の壁を越えて相互扶助の**共助**を行っているが、シェアリングされた知見をもとに自らの手で自らのサービス、システムを守る**自助**を前提としている。
- 要求される事項は高度化の一途をたどっているが、各々の時点でのベースライン的なものはあり、お客さま、マーケット更には社会一般への説明責任を果たすために**公助**によるレギュレーション、監督、指導は重要である。真の相手は攻撃者であり、捉えがたく時々刻々と変化していくため、官民での連携でより適切な方向を向き、**３つの助を最大化**することは社会インフラの担い手としての責務と認識している。
- 一方で、民間の立場としての活動は限りがあり、**官によるプロアクティブな情報収集、解析、そして防御への期待は高い**。
- 官で得たインテリジェンスを的確に共有していくオペレーションは機密性等を考慮するとハンドリングが難しいと考えられるが、範囲を絞った特定の分野への情報であれば、当該業態の窓口を経由し、緊急を要する脆弱性であれば、同種のサービス・システムを保有する業態の中で、**より具体的な対応策を導きだすことが可能なISACの活用は有用と考えられる**。（NISC経由の重大な脆弱性情報の供給で既に恩恵を得ています）
- 組織の規模によって情報を活かす能力は異なるため、**ISACによるトリクルダウン的な機能**も対応を全体に浸透させていくための一助になると考えられる。

有識者会議へのコメント

- **民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有**
  - ✓ 繰り返しになるが、**シェアリングとレポーティングは根本的に性格が異なる**。前者がボランタリーベースであるのに対し、後者はマンデイトリー。監視がなされている環境下でのボランタリーなシェアリングは極めて難しい。
  - ✓ 現状、金融では不正送金といった顧客をターゲットとしたクライム系のインシデントが太宗を占めるため、レポーティングを求めるのであれば、自システム・サービスが直接のターゲットなるものと、その顧客がターゲットとなるものを分けて考えることも必要ではないか。（金融分野では既に分かれてレポートされている）
  - ✓ **レポーティングは対応中の組織に相応のリソースを強いる**こととなり、相応の考慮が必要。

  - ✓ その他、レポーティングの在り方については金融業界では課題のひとつで、インシデント対応のリソースを消化してしまう要因として認識されている。

  - ✓ レポーティングやシェアリングの自動化は内容によるが、重大な情報であればあるほど、情報元や内容そのものの確認が重要となり、オペレータの介入が必要の認識。

有識者会議へのコメント

- **業種横断的な情報連携の重要性について**
  - ✓ サイバー攻撃は多様であり、業種をまたいだ連携や認識共有、更には産業全体のボトムアップは重要と考えられる。
  - ✓ 一方で、ISACが業種毎に組成されているのは、情報共有を効率的かつ効果的に行う目的とtrusted circleの運営の難しさに理由があり、業種内と業種横断の重要性は意味合いが大きく異なるものと認識している。
  - ✓ 自律・主体的に運営されているISAC間の連携は可能であり、ICT、電力、Auto、交通、ソフトウェア、貿易、金融のISAC間でのコミュニティが存在する。

- **他業態とのベストプラクティスの横展開の重要性について**
  - ✓ 内容により、必要に応じて行うべきものだと考えられる。
  - ✓ 各ISACの情報や知見は原則、限定されたコミュニティの中で共有されることを前提としている。

- **クリアランス制度を活用した情報連携の重要性について**
  - ✓ 現状、当ISAC内でクリアランス制度がないことによる支障は認識していない。
  - ✓ 民間セクターとしては、どのような新たな情報や知見がクリアランス制度の前提となるのかを注視しており、US等でなされているようなハイレベルなインテリジェンス情報が政府側から共有される時、与えられた情報を効率的・効果的に展開していくため、情報が一般に公開される前に信頼されたグループの中で咀嚼が進んでいく仕組みが出来ればよりよい方向に向かうと考えている。

Fast, Frank, and Friendly

Financials ISAC Japan