資料6－5

次世代情報セキュリティ政策研究会資料

T-ISAC-Jモデル(事業者間連携スキーム)2.0
官民連携スキーム2.0
に関する考察

2008.4.3

(財)日本データ通信協会
Telecom-ISAC Japan　企画調整部
有村　浩一

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

テレコム・アイザック・ジャパン

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

大規模なサイバー脅威に共同で立ち向かう「互助会型モデル」の成功事例

●2002年に日本で最初のISACとして発足
●商用サービスの安全かつ安心な運用の確立を目的に、テレコム通信事業者を含む会員が関連情報を共有分析し、タイムリーな対策をとる場を提供

会員

- 連携活動・情報共有はWorking groupを核におこなう。
- WGにT-ISAC-Jの活動のカラーが反映される。

緑文字はISP、通信事業者を示す。

会長　：KDDI株式会社
副会長　：NTTコミュニケーションズ株式会社、ニフティ株式会社
委員　：日本電気株式会社、株式会社インターネットイニシアティブ、株式会社日立製作所、松下電器産業株式会社、沖電気工業株式会社、ソフトバンクBB株式会社、横河電機株式会社、松下電工株式会社、東日本電信電話株式会社、西日本電信電話株式会社、エヌ・ティ・ティ・ビジュアル通信株式会社、日本電信電話株式会社、株式会社KDDI研究所、NECビッグローブ株式会社、富士通株式会社
アライアンスメンバー：株式会社ラック、インテック・ネットコア株式会社、トレンドマイクロ株式会社、インターネット セキュリティ システムズ株式会社
オブザーバー：総務省、独立行政法人情報通信研究機構　他

主要なWG

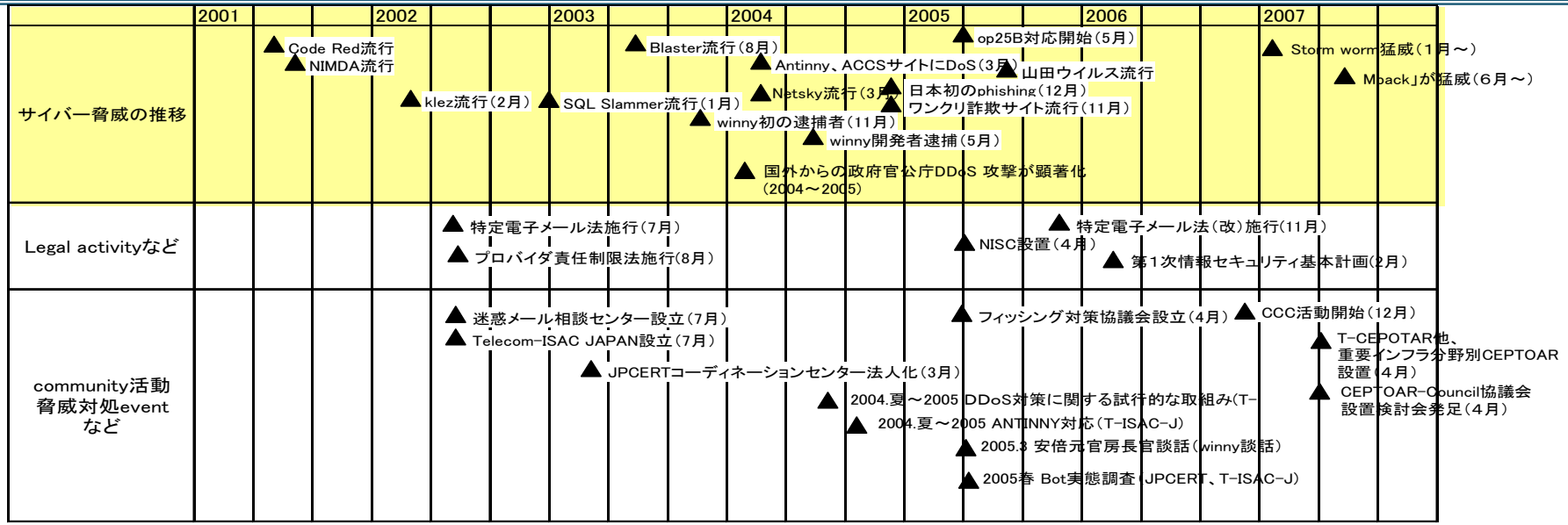
Cyber Clean Center

- DDoS攻撃対応　WG
- nicter支援 WG
- BGP経路情報監視 WG
- ACCESS-WG
- SoNAR-WG（Abuse部門、CS部門連携）
- サイバークリーンセンター運用業務
- 日中韓コーディネーション機能　　etc

連携活動心得

- 会員は"Our security depends on your security"を信じ、win-winの関係構築に貢献する意図をもつこと。
- 1事業者では手に負えない大規模な脅威に一致団結して対処すること
- 情報共有のための連携するのではなく、連携のための情報共有を行うこと

１社対応を超える大規模インシデント発生は過去のもの？



- ●各社個別孤軍奮闘対応
- ●情報連携なし

- ● 案件の増加に伴う汎用的な対応方針の需要増加
- ● コミュニティ活動の活発化

- ● 2006年以降コミュニティで対峙するような大規模なインシデントは発生していないよう

- ● 2004年を境に、ワームやウイルスの大きな拡散は見られず、マルウエアの活動は過去のもののように思える。
- ● サイバークリーンセンターでは、脅威となる手法は巧妙化され、水面下で拡大して、むしろ危険性が増していることを示唆するデータを観測している。

サイバー攻撃等の見え方が変わってきた。
今はちょうど、サイバー攻撃やボット攻撃の様相が変わる変化点にあるではないのか？

T-ISAC-J会員の共通成功体験

① 事業者連携、関連異業種横断連携の成功事例を体験

脅威へのフォローアップには異業種の知恵を横断的に結集することが有効

例、DDoS攻撃共同対処連携、CCCプロジェクト他

② 観測データの収集とそれを会員と共有することの重要性を理解

例、BGP経路奉行システムのデータ、CCCボット攻撃観測データ

③ 一部の分野では日本をほぼ覆い尽くすカバレッジを達成。そのカバレッジを活かした目線で連携に関する具体的議論ができる

例、BGP-WGやACCESS-WG参加企業

確信： 事業者連携スキームの育成・普及は継続的に必要！

サイバー脅威対処モデルの変化【～2007】

サイバー脅威の特徴にあわせた対抗手段を持つような組織変革

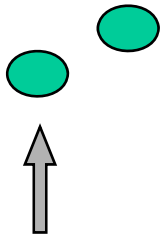
●各社個別孤軍奮闘対応
●情報連携なし

● 案件の増加に伴う汎用的な対応方針の需要増加
● コミュニティ活動の活発化

● 2006年以降コミュニティで対峙するような大規模なインシデントは発生していないよう

２００３以前

「おたく」的モデル



● 脅威そのものが少ない
● 技術自体に特化
● 運用よりもコンピュータ科学

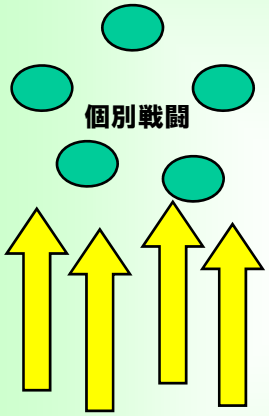
事業者間連携モデル1.0

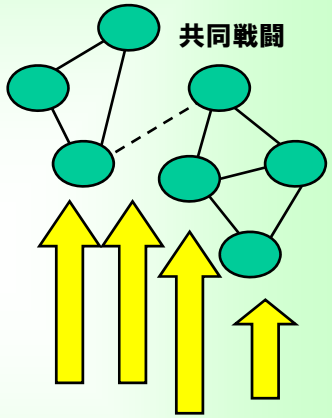
２００３～

組織内で一人が個別にがんばるモデル

互助会的モデル全盛期

（例、Telecom-ISAC Japanなど）





● 脅威が増加
● 脅威や影響が目立つ・見えやすい
● マス脅威
　各組織共通の問題として総意形成しやすい
　明日は我が身と思える
● 技術情報を組織運用に拡大

現在（～今後）

これまでの脅威には事業者横断の協調・連携によって対処できた。

脅威の質がこれまでとは変わったとしたら、

互助会的モデルのままでいいのか？

参考：この他の論点
　ISP事業者の役割が変化
　永遠のビギナー利用者に自己防衛を求めるやり方の限界

事業者間連携モデル2.0

変わった脅威に対応するための新たな事業者連携モデル

サイバー脅威の質の変化の方向は？

いまどきのボット　【各種収集情報から】

1．動機のプロフェッショナル化
- 金銭目的、趣味を卒業し、ビジネスモデルの下でおこわなれる各種行為
- ソーシャルエンジニアリング駆使のターゲットアタック・スピアメール型

2．サイバー脅威の複雑化・高度化
- ソーシャルエンジニアリングの駆使
- web感染型増加の予兆
- 多段・多重マルウエアDL型ボット
- 防衛線の延伸

  狙われ始めたMS製品以外の脆弱性（利用される脆弱性の多様化）
  国ごとに著名なソフトウエアをねらう。

4．サイバー脅威の局在化
- ボットは特定の地域、国にあわせて作成されている
- 標的型攻撃
- その地域の特色にあわせて繁殖している悪意あるコードのタイプも変わる

5．サイバー脅威の潜在化
- 最新版駆除ツールが効かない方向に攻撃技術は動く
- 解析に時間と手間が係る方向に製造技術は動く（難読化）

脅威の質の変化が互助会的モデルにもたらすもの

サイバー脅威の局在化、潜在化、高度化・複雑化は何をもたらすのか？

高度化・複雑化：１事業者では手に負えない個別で高度な脅威
局在化・潜在化：インシデントの見えない化
各組織個別の問題へ、同業他社の当事者意識の低下
組織間連携の意義の希薄化

１．（外見的には）
2003年当初の「組織内で個別にがんばるモデル」への逆戻り
インシデント対応当事者の単独組織力では手に負えない事態を対応当事者１組織で対応する事態

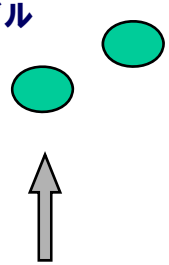
２．互助会的モデルの発展的変革
（参考）互助会的モデル・・・事業会社の壁を越えた問題意識の共有ならびに、人ごとは思えない危機感の共有から始まるサイバー脅威への共同対処活動

脅威の質が変わった・・・

個別の脅威課題時代の事業者連携モデルをどう考えるか？

２００３以前

「おたく」的モデル

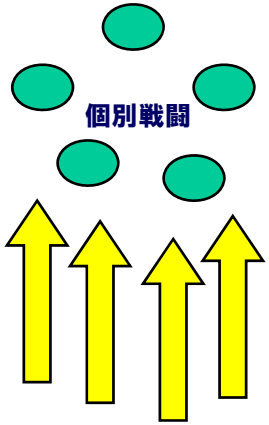


脅威そのものが少ない

Computer Science、
技術自体に特化

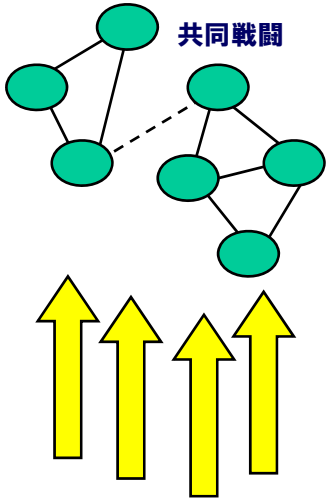
２００３～
事業者間連携モデル1.0

組織内で一人が個別にがんばるモデル



互助会モデル全盛期

（例、Telecom-ISAC Japanなど）



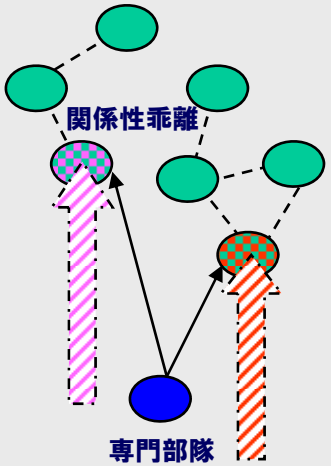
マス脅威（各組織共通の問題）

脅威や影響が判りやすい

技術情報を組織運用に拡大

現在（～今後）
事業者間連携モデル2.0

個別Win-Win専門特化モデル？



個別で高度な脅威（各組織個別の問題）

脅威の存在が潜在化（当事者意識低下）

組織間連携の意義が薄れる

何が脅威か判りにくい
特化専門能力の組織運用化

組織が個別にがんばる2003年以前モデルに戻るのか、互助会モデルとは違う別のあらたな組織間連携モデルが必要か

（専門組織との個別対応組織が自律的に必要に応じて有機的に緩くつながる）

事業者間連携モデル2.0への挑戦

事業者間連携の関係が希薄化するなかであっても
脅威が個別化するなかであっても

「いまどきのボットやサイバー脅威」への対処行為（下記、①②③ぐらいについては）に合わせた事業者横断連携に発展すべき

連携モチベーションの基本
- 彼を知り己を知れば百戦殆うからず。（孫子、謀攻篇）
- 事業者横断の協調・連携によって脅威に対処してきた実績

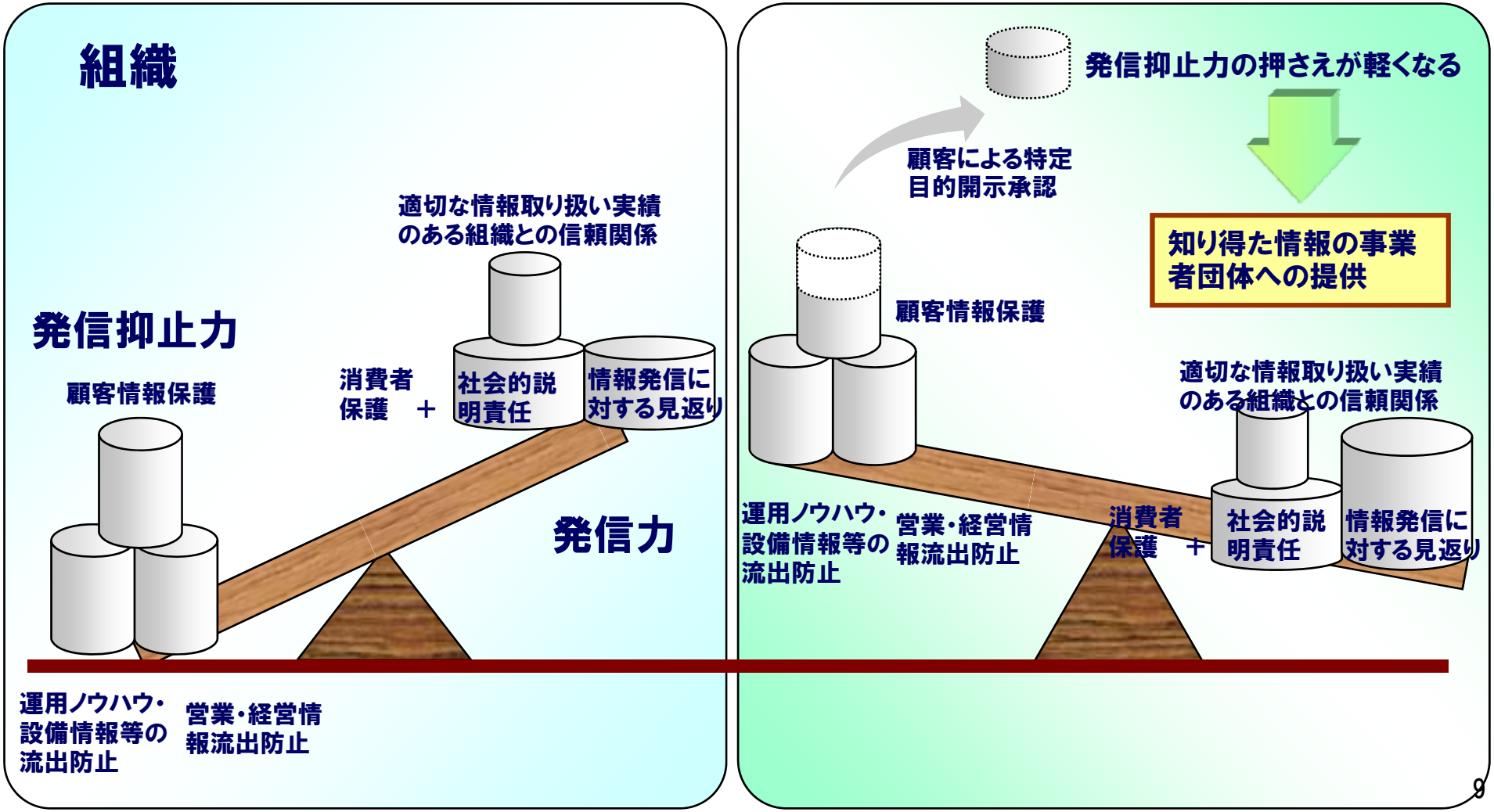
参考　サイバー脅威への対処行為の例
- ①　攻撃の発生の検知
- ②　攻撃事例の収集
- ③　攻撃方法の分析
- ④　防御・対策の案出
- ⑤　上記の獲得情報・知識の共有
- ⑥　仲間を増やす（問題意識の共有）

事業者横断情報共有・連携活動を阻む高い壁
知り得ていても、お客様の許可がない限り有益情報が出せないモデル

このモデルが突破できないか？
この障壁の高さを低くできないか？
個別脅威には観測点増加とカバレッジ増加で対処するため

事業者間情報共有天秤（イメージ）

- 知り得ていても、お客様の許可がない限り有益情報が出せないモデル
- 共益目的のためにお客様に関する情報の開示承認を取り付けるための組織内調整・顧客調整は大変。

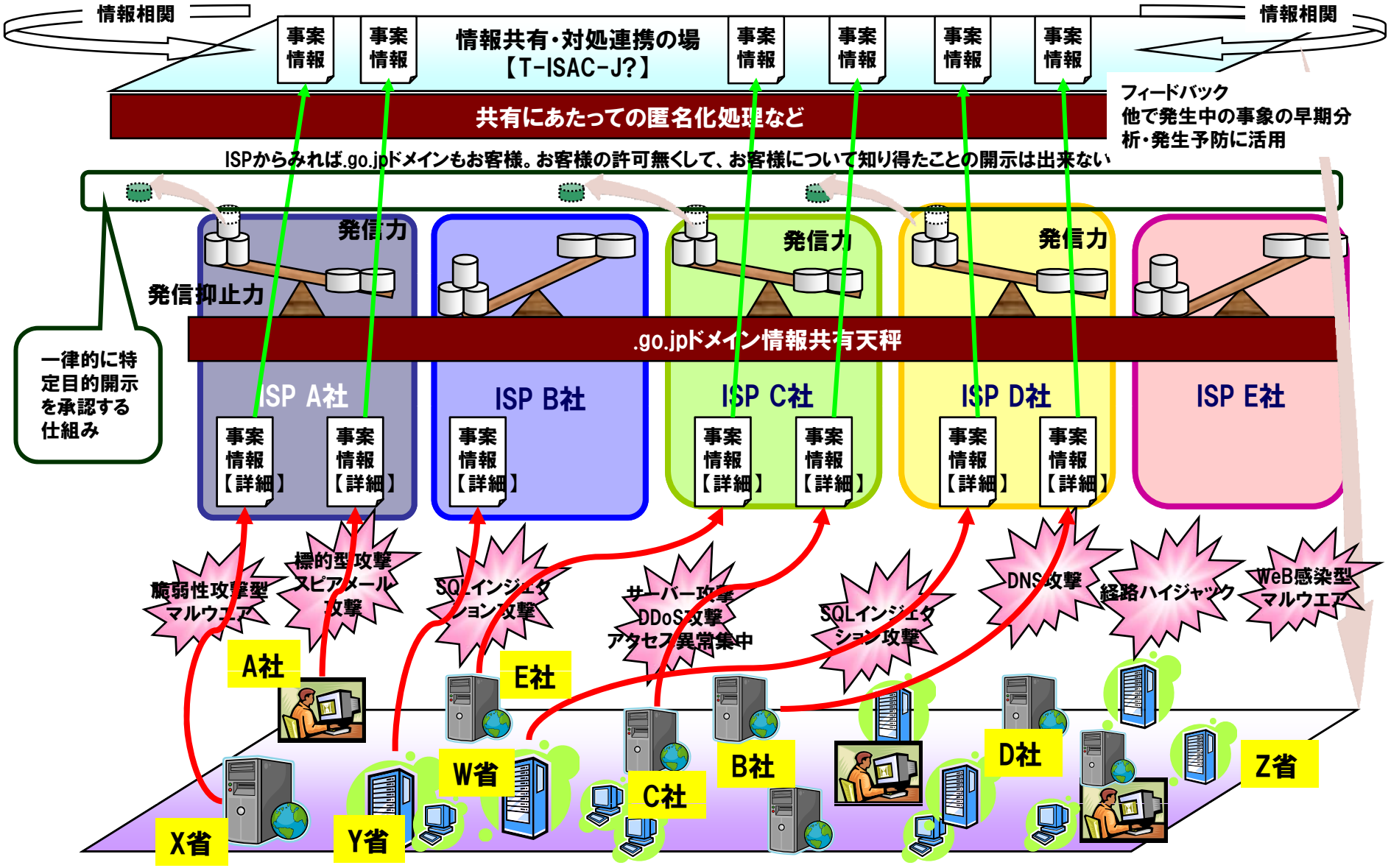


天秤を発信力側に傾ける・・・

- 事件は現場で起きている。.co.jpドメイン、.comドメイン・・・でいろいろ発生
- .go.jpドメインユーザも被害者になるとの視点を！
- .go.jpドメインユーザも民間事業者も被害にあった場合の対処活動はほぼ一緒
- ISPからみれば.go.jpドメインユーザも、民間企業もお客様
- お客様の許可無くして、ISP、SOC事業者がお客様について知り得たことの開示は出来ない。
- お客様の許可があれば出しようはある。（期待）

いまこそ情報共有・提供における雰囲気醸成と英断を！
（官民連携スキーム2.0）

多くの天秤が発信力側に傾くと



まとめ

① ISAC設立から６年、事業者間連携の成功事例【BGP-WG、DDoS攻撃共同対処、CCC他など】
② １事業者では手に負えない大規模な脅威に共同で立ち向かう「互助会型モデル」は成功
③ 今後、同様な脅威発生のときには協調・連携経験が生きるであろう。
④ これまでのものは違う「いまどきの攻撃」はT-ISAC-Jモデルの変革を迫る

攻撃は高度、範囲は限定的　⇒　複数事業者にまたがらない　⇒

他人事化　⇒　事業者間連携の希薄化

⑤ 「いまどきの攻撃」への対処を目指す事業者間連携モデル2.0を考察

1. 事業者間連携モデル2.0
   これまでの事業者間連携スキームを「いまどきのボットやサイバー脅威」に脅威に対抗するためへの進化
2. 官民連携スキーム2.0
   いまこそ、.go.jpドメイン、.co.jp/.comドメインユーザが情報共有・提供する雰囲気醸成との情報連携促進を