サイバー情報共有イニシアティブ（J-CSIP）の活動

J-CSIP: initiative for Cyber Security Information sharing Partnership of Japan

IPA

資料６

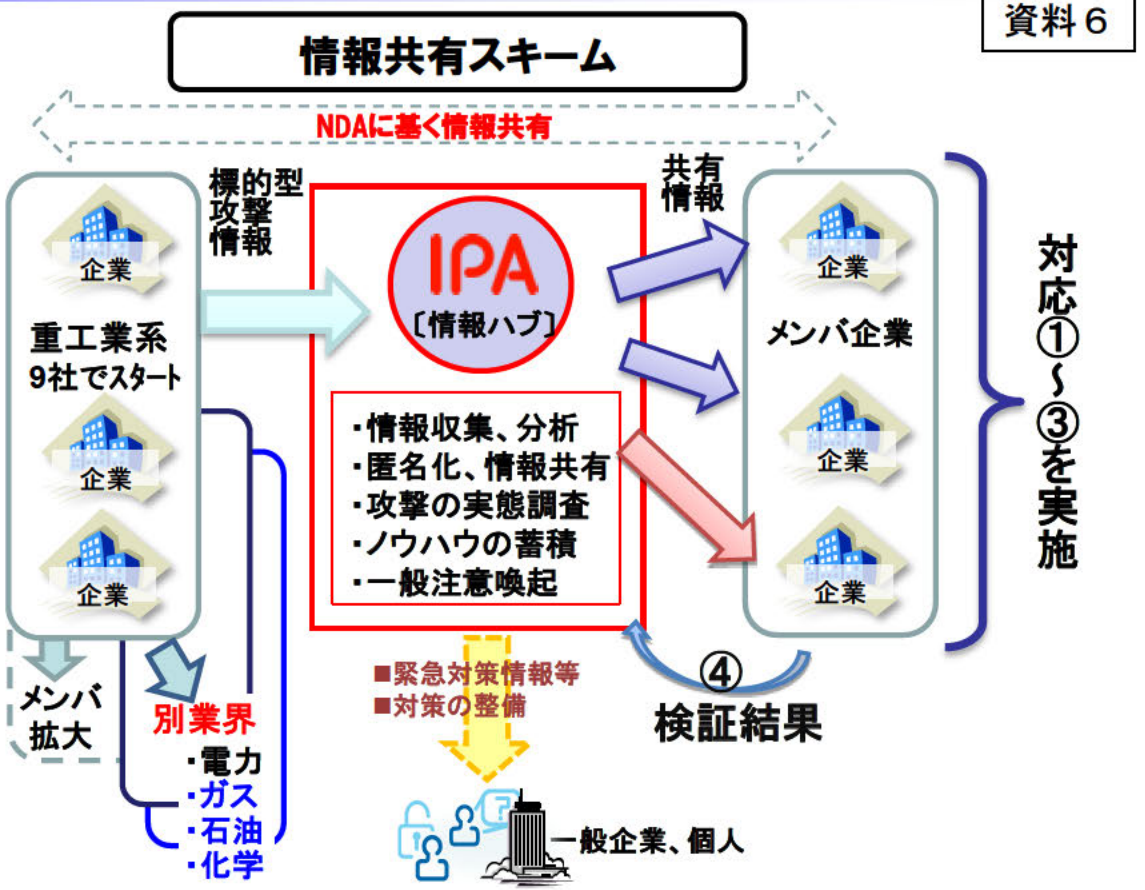
J-CSIPメンバ企業実施項目

標的型攻撃メールからスタート

① 組織内への注意喚起・初動対策
⇒ メール開封を回避
②メールサーバのアーカイブの検証
⇒ 攻撃痕跡検証
③防御対策
⇒メールフィルタのチューニング、
FWパラメータ設定等

④ 検証結果のフィードバック ⇒ 再度の情報共有
- ✔ 該当メール、類似メールの検出有無
- ✔ 開封の有無
- ✔ 被害の有無

情報共有スキーム



解析協議会に対するIPAの貢献(1) および 期待する事項(2,3)

1. J-CSIPメンバーの許可の下に、重要組織に対する最新の攻撃情報の知見の共有、およびマルウェア検体の提供
2. 迅速な解析、より広く深い解析による、情報共有内容および対策対応の高度化
3. 今後想定される攻撃に対する事前対応、システム対策など組織的セキュリティ力の向上