MWS/CWS合同企画セッション in SCIS2019

製品セキュリティと研究活動
～脆弱性発見者と対応者、それぞれの視点からの取組みを知ろう～

脆弱性ハンドリング

日本コンピュータセキュリティ
インシデント対応チーム協議会
運営委員長　寺田真敏
2019年01月24日

日本シーサート協議会とは

- 設立
  - 2007年3月
- 名称
  - 名称：日本コンピュータセキュリティインシデント対応チーム協議会
  - 略称：日本シーサート協議会
- 使命
  - 本協議会の全会員による緊密な連携体制等の実現を追及することにより、会員間に共通する課題の解決を目指す
  - 社会全体のセキュリティ向上に必要な仕組みづくりの促進を図る
- 加盟数
  - 327チーム(2019年1月16日時点)

CSIRT
日本シーサート協議会

日本シーサート協議会とは

- 活動
  - {組織間の協力 x (事前対処＋事後対処)}に向けた場の提供
    - 分野横断的な場の提供
    - セキュリティ業界のパイプ役
    - 地区毎で顔の見える活動の場(シーサートワークショップ等)の提供
  - {組織間の協力 x (事前対処＋事後対処)}に向けた場の整備
    - アドレス帳(日本シーサート協議会加盟組織一覧)の整備
    - シーサート活動の暗黙知(慣習)の明文化
    - 地区毎で顔の見える活動の場(シーサートワークショップ等)の整備

国内のシーサートコミュニティが、いざというときに協力して活動できるための場の提供と整備

シーサートワークショップ(CWS)とは

- 日本シーサート協議会のシーサートワークショップ
  チャタムハウスルールの下で、実事例を中心に、情報交換や連携をする実務の場として広げたい
  ⇒ 実務の場のシーサートワークショップ

その一方で、上記だけでは解決できない課題も、、

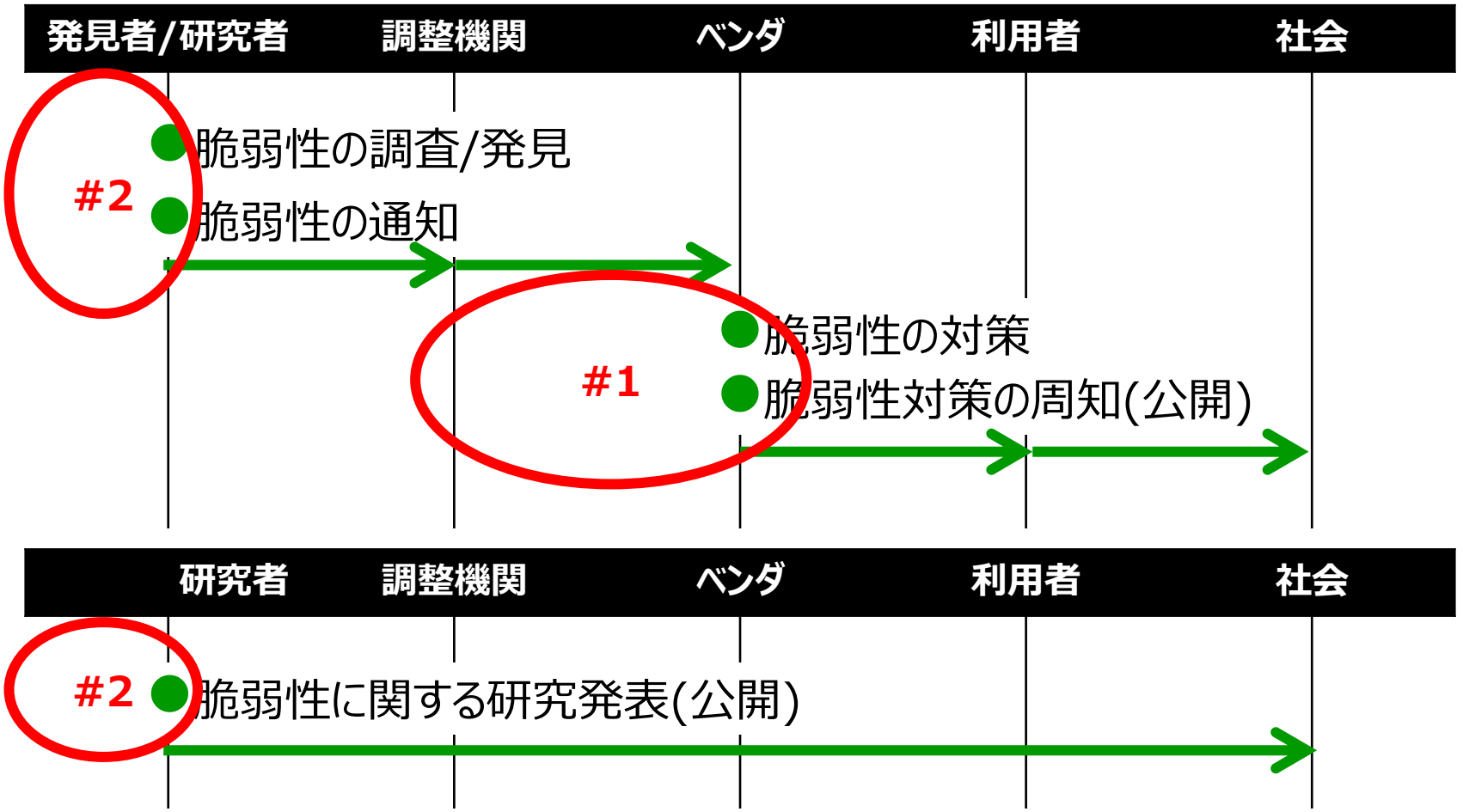
- 学術系のシーサートの方へ：学位取得につなげてもらおう
- 企業系のシーサートの方へ：学会という場での発表方法を学んでもらおう

などなど、、、

学問として、シーサートを支える場を作っておきたい
⇒ 学術の場のシーサートワークショップ
(実務と学術の協働の場)

脆弱性ハンドリング

- 脆弱性の発見、通知、対策、周知(公開)までの一連のプロセス



脆弱性ハンドリング [#1]

【脆弱性ハンドリング事例】Windows環境におけるDLL問題

- アプリケーションが本来読み込むべきではないDLL/EXEファイルを読み込んでしまう状況が発生することに起因
  - **2010年に報告されたDLL問題・・・カレントディレクトリ型**
    データファイルと同一のディレクトリに置かれた(偽の)DLLファイルを、システムディレクトリにある(正規の)DLLファイルよりも優先して読み込んでしまう問題
  - **2016年以降に報告されたDLL問題・・・アプリケーションディレクトリ型**
    アプリケーション起動時にアプリケーションと同一のディレクトリに置かれた(偽の)DLLファイルを、システムディレクトリにある(正規の)DLLファイルよりも優先して読み込んでしまう問題

年	2018	2017	2016	2015	2014	2013	2012	2011	2010
JVN登録	28	71	7	3	1	0	2	4	6

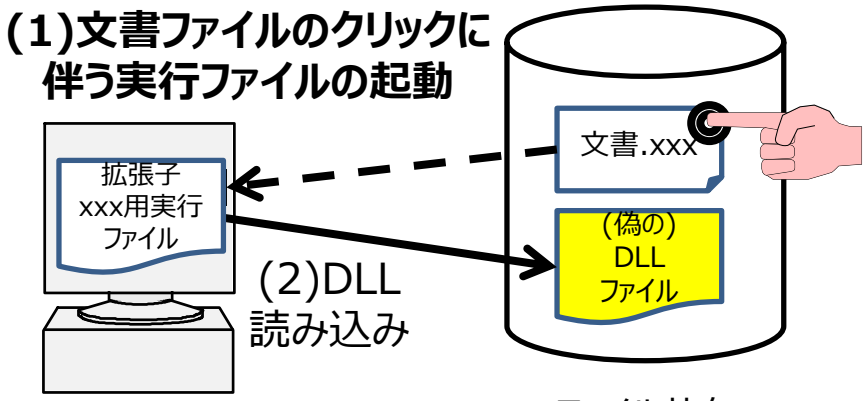
アプリケーションディレクトリ型DLL問題

カレントディレクトリ型DLL問題

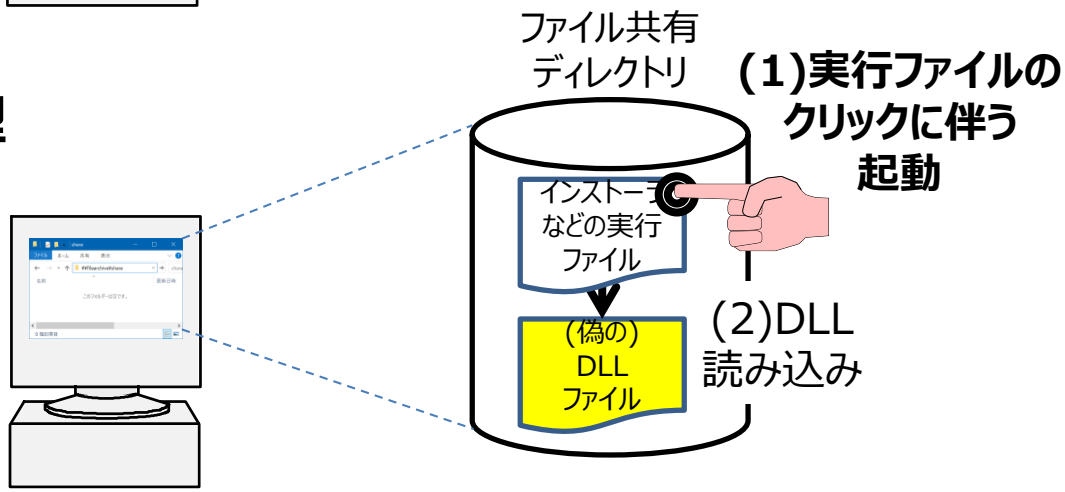
脆弱性ハンドリング［#1］

【脆弱性ハンドリング事例】脆弱性の概要

- **カレントディレクトリ型**
  データファイルと同一の
  ディレクトリに置かれた
  (偽の)DLLファイルを
  読み込んでしまう



- **アプリケーションディレクトリ型**
  アプリケーション起動時に
  アプリケーションと同一の
  ディレクトリに置かれた
  (偽の)DLLファイルを
  読み込んでしまう



脆弱性ハンドリング [#1]

【脆弱性ハンドリング事例】対応経緯

日付	イベント
2017年5月26日	調整機関(JPCERT/CC)から自社製品が該当するとの通知を受信
2017年6月上旬	開発部門との検討の結果、脆弱性につながる原因が複数あること、影響が広範囲に渡ること、原因の中にはユーザによる対処のみが対策となる場合もあることを認識
2017年6月26日	IPA、JPCERT/CCと、課題共有の打合せを依頼し、実施
2017年7月31日	意見交換のための国内ベンダ会合開催をJPCERT/CCに依頼し、実施 その後、問題と原因、対処方法に関する作成資料をJPCERT/CC経由で国内ベンダに展開
2017年9月27日	「HIRT-PUB17011：DLL読み込み問題」を公開
2017年9月28日	JPCERT/CC：「JVNTA#91240916 Windows アプリケーションによる DLL 読み込みやコマンド実行に関する問題」の[参考情報]にリンクを追加
	IPA：「【注意喚起】Windowsアプリケーションの利用における注意」を発信

脆弱性ハンドリング［#1］

【脆弱性ハンドリング事例】原因と対処

分類	概要	対策1		対策2		対策3
		アプリケーション側の対策				ユーザ側の対策
		アプリケーション起動時にSetDefaultDllDirectories関数やLoadLibraryEx関数、DLL遅延読み込みなどを使用する。		アプリケーション起動時に実行ファイルを新規に作成したフォルダにコピーしてから実行する。		実行ファイルについては、安全な形で実行する。例：ユーザ自身が、新規に作成したフォルダに実行ファイルを移動してから実行する。不審なDLLファイルなどがないことを確認後、実行する。
		インストール型	左記以外	インストール型	左記以外	
#1	直接的に相対パスでリンクしているDLLの読み込み	○	○	○	N/A	◎
#2	間接的に相対パスでリンクしているDLLの読み込み	○	○	○		
#3	DLLフォワーディングによるDLLの読み込み	△				
#4	独自方式でのDLLの読み込み	×				
#5	アプリケーション互換性機能によるDLLの読み込み	○				
#6	動作監視ソフトによるDLLの読み込み	×				
#7	OS互換性機能によるDLLの読み込み	×				

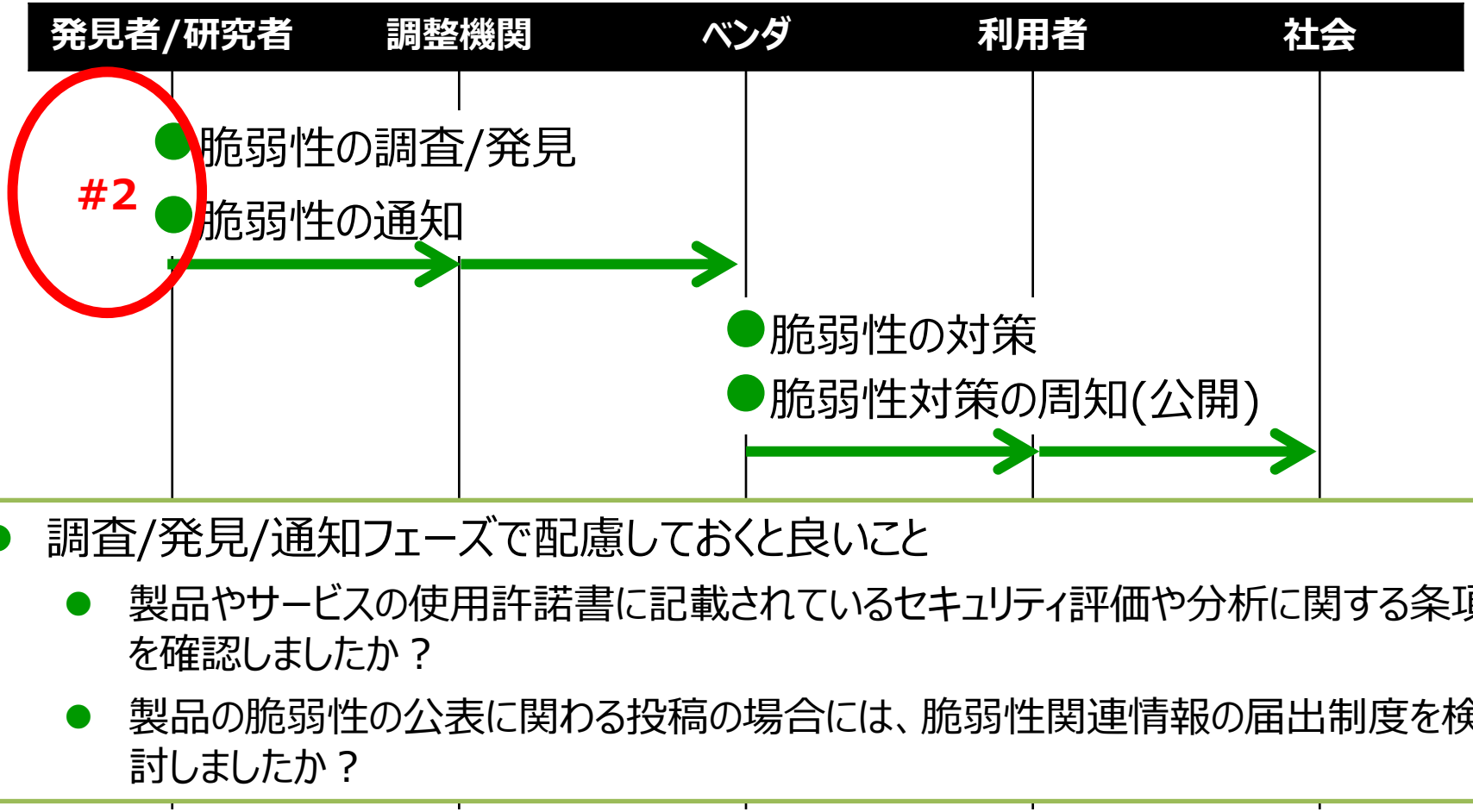
←発見者/研究者からの指摘

←原因調査の過程で明らかになった問題

本脆弱性ハンドリングは、原因調査の過程で、脆弱性問題の影響範囲が広いことがわかり、調整機関と協力して対処を実施した事例

脆弱性ハンドリング [#2]

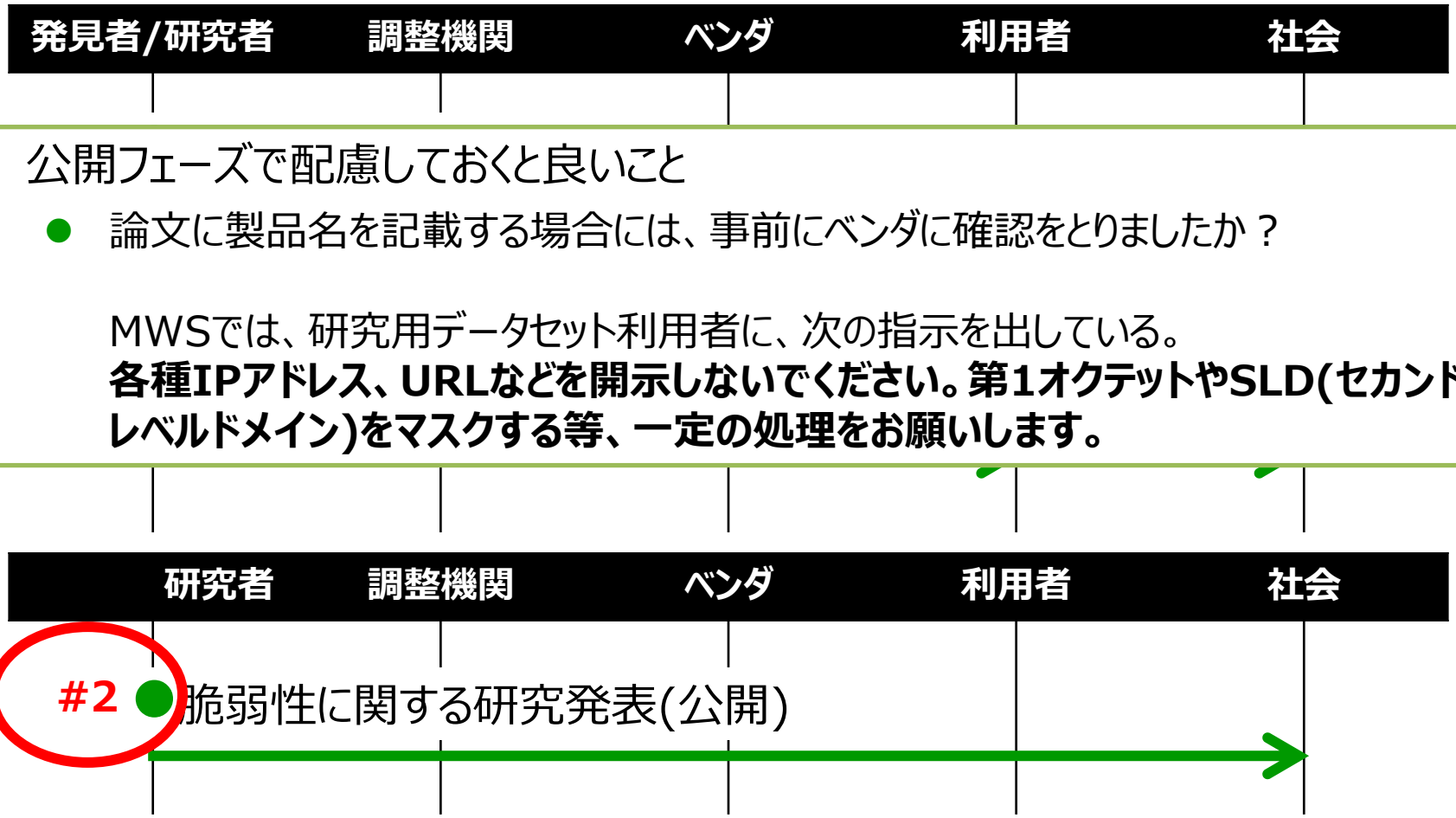
- 脆弱性の発見、通知、対策、周知(公開)までの一連のプロセス



- 調査/発見/通知フェーズで配慮しておくと良いこと
  - 製品やサービスの使用許諾書に記載されているセキュリティ評価や分析に関する条項を確認しましたか？
  - 製品の脆弱性の公表に関わる投稿の場合には、脆弱性関連情報の届出制度を検討しましたか？

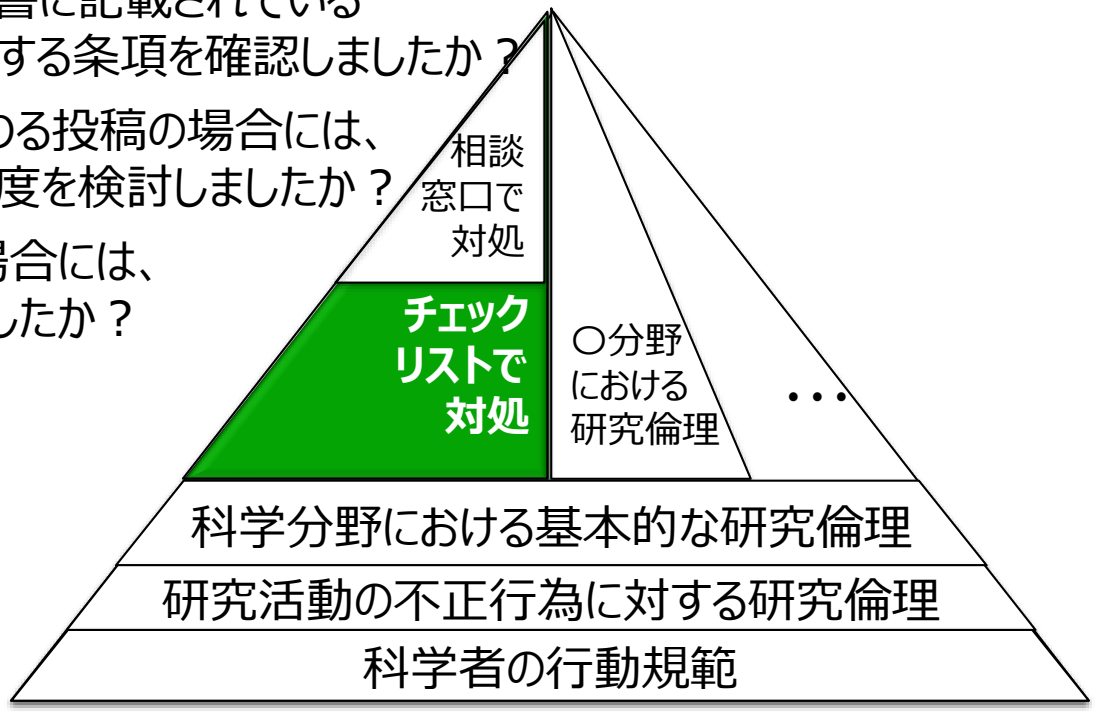
脆弱性ハンドリング [#2]

- 脆弱性の発見、通知、対策、周知(公開)までの一連のプロセス



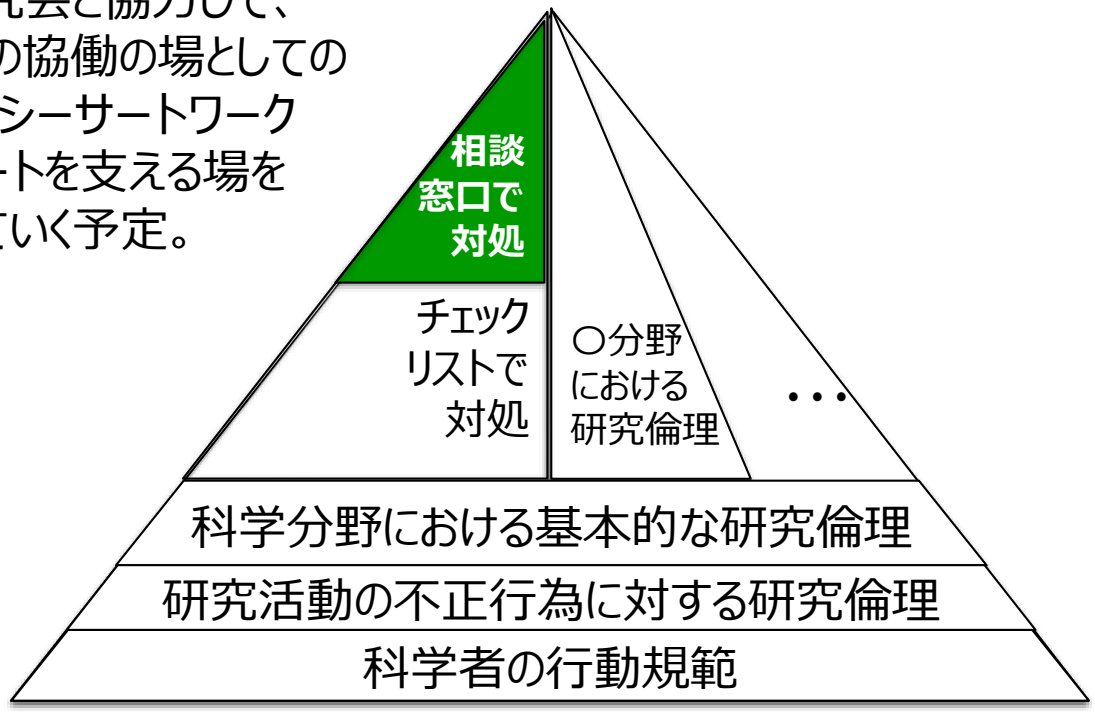
脆弱性ハンドリング [まとめ]

- サイバーセキュリティ研究における倫理的な研究プロセスの普及啓発
  投稿論文の書き方で解決できる問題
  ⇒論文投稿時に参照する「チェックリスト」の作成
- チェックリストの項目として、配慮しておくと良いことを取り込んで頂きたい。
  - 製品やサービスの使用許諾書に記載されている
    セキュリティ評価や分析に関する条項を確認しましたか？
  - 製品の脆弱性の公表に関わる投稿の場合には、
    脆弱性関連情報の届出制度を検討しましたか？
  - 論文に製品名を記載する場合には、
    事前にベンダに確認をとりましたか？



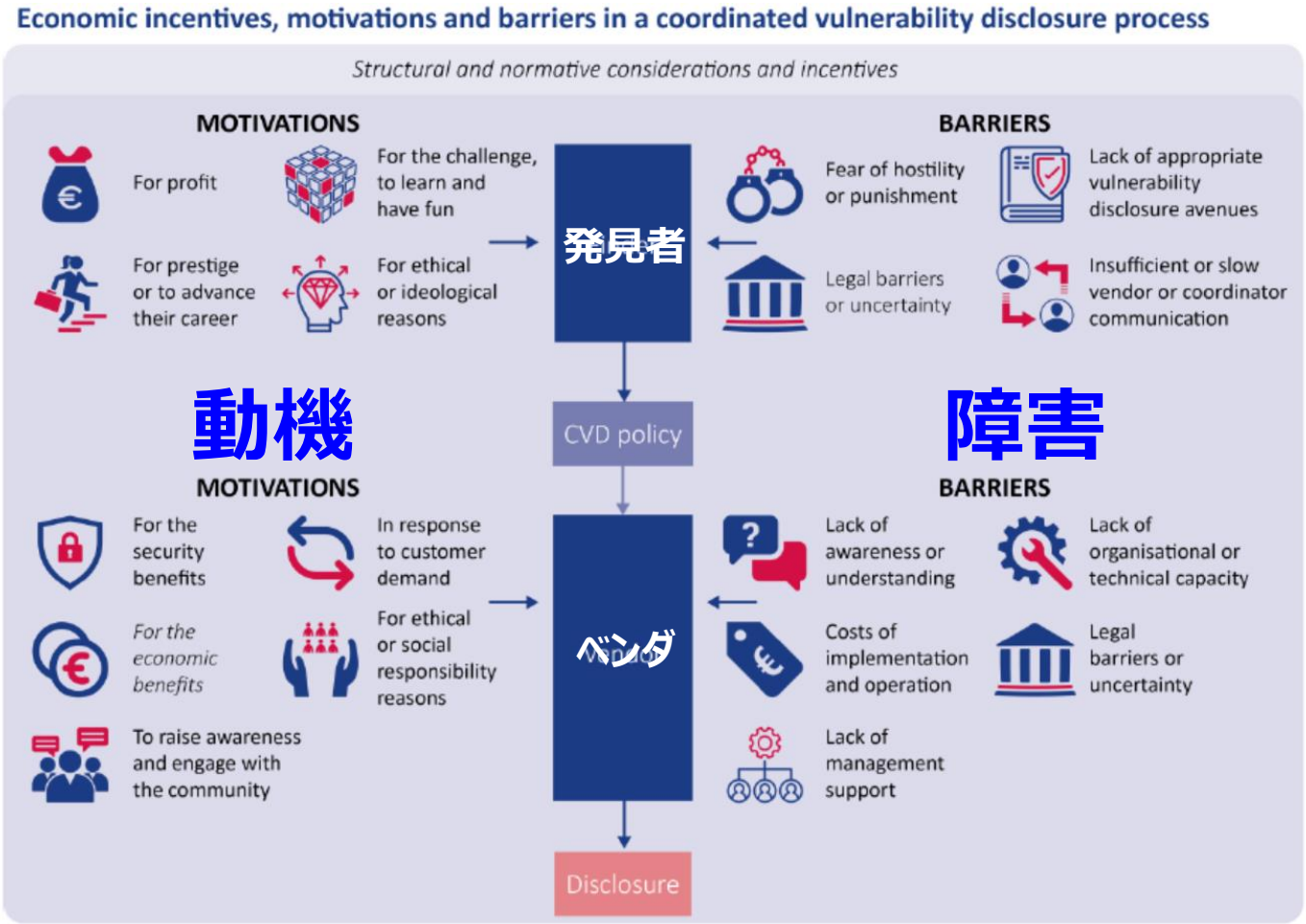
脆弱性ハンドリング [まとめ]

- サイバーセキュリティ研究における倫理的な研究プロセスの普及啓発
  研究そのもののアプローチの検証を通して解決できる問題
  ⇒研究会/シンポジウムに研究倫理に関する相談窓口の設置
- シーサートを事前の相談窓口として活用することも検討して頂きたい。
  - 協議会としては、学術の研究会と協力して、シーサート実務者と研究者の協働の場としての活用されるよう『学術の場のシーサートワークショップ(学問として、シーサートを支える場を作っておきたい) 』を整備していく予定。



脆弱性ハンドリング [参考]

- ENISA：Economics of vulnerability disclosure (2018年12月)



シーサート実務者と研究者の協働の場の整備
活用を通して、より良いセキュリティ対応を考え、
そして、実現していきます。

CSIRT
日本シーサート協議会

http://www.nca.gr.jp/