C6：あつまれ！セキュリティ運用ピーポー

あつまる！シーサートピーポー
～訓練演習、教育ノウハウを共有してよかった話～

一般社団法人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
インシデント対応演習訓練WG主査　井出雄介
セキュリティ教育検討WG主査　渡辺文恵

自己紹介　井出 雄介

お客様と一緒に。CSIRT構築や教育・訓練をご支援します。

経歴

2001年から国内大手製造業にて製造ラインプロセス改善業務、情報システムインフラの企画、設計、構築、運用業務に従事。
2014年から同社情報システム部門にて情報セキュリティ専門組織の体制構築、運用業務、グループ会社・海外拠点を含むグループセキュリティガバナンス向上、インシデント対応業務に従事した経験を活かし、2019年から現職にてCSIRT構築・運用支援、セキュリティポリシー策定支援、インシデントハンドリング支援、役員および従業員への訓練・教育支援など、緊急時のインシデント対応支援および平時のサイバーセキュリティに関するお客様プロジェクトの推進支援に従事。
また、日本シーサート協議会インシデント対応訓練ワーキンググループに参加し、主査として国内CSIRTの演習・訓練実施に関する啓発活動を行っている。

資格など

- 日本シーサート協議会 インシデント対応演習訓練WG 主査
- 日本シーサート協議会 運営委員
- CSIRT 対応能力向上トレーニング TRANSITS Workshop 講師
- Certified SIM3 Auditor
- 情報処理安全確保支援士(第009459号)

井出 雄介, CISSP
チーフコンサルタント

自己紹介　渡辺 文恵

◆所属

株式会社ディー・エヌ・エー
技術統括部 セキュリティ部／ DeNA CERT

◆職歴

営業→CS→マーケ→品質管理→セキュリティ

◆セキュリティのお仕事・・・

- セキュリティポリシーの策定や監査
- インシデント管理
- 社内相談窓口の開設・運用
- 事業部や子会社のセキュリティ支援
- 社内教育・啓発←いまここ

◆日本シーサート協議会（NCA）での活動

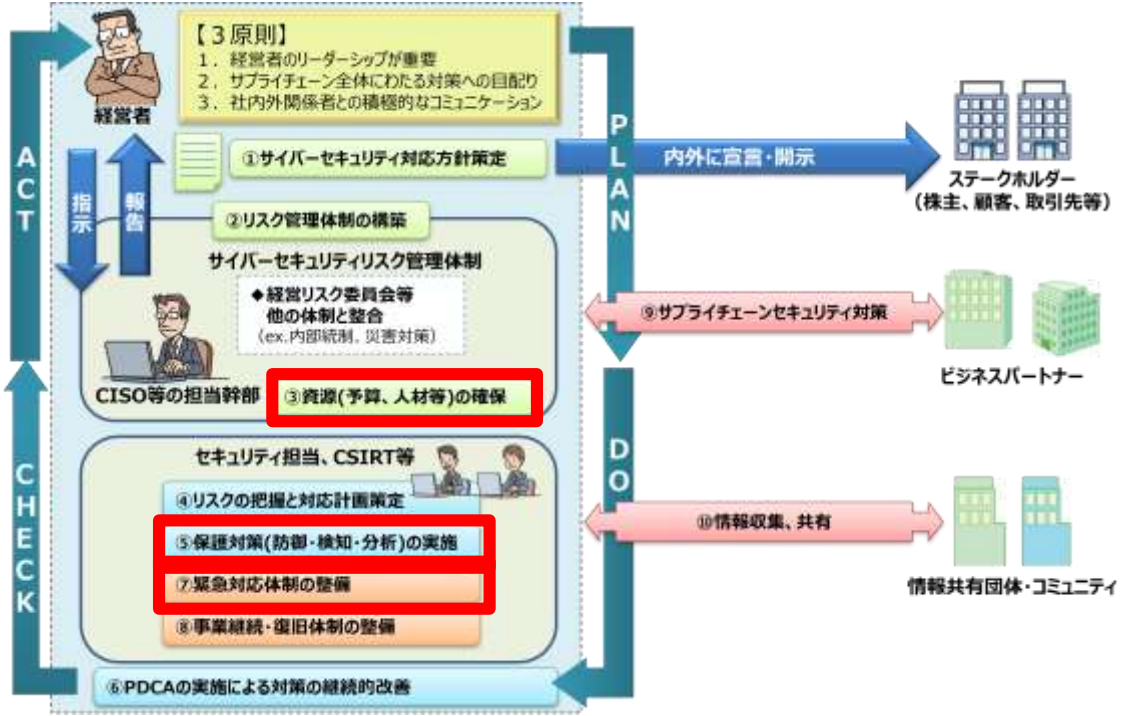
- 地区活動委員会
- チームトレーニング委員会
- セキュリティ教育検討WG

◆資格

- CISM
- 産業カウンセラー
- キャリアコンサルタント

日本シーサート協議会
公式Youtube

必要性が示されている訓練演習、教育



出典：サイバーセキュリティ経営ガイドラインと支援ツール (経済産業省)
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

サイバーセキュリティ経営ガイドライン Ver 3.0

指示③(対策例)
従業員向けやセキュリティ担当者向けなどの研修等のための予算を確保し、**継続的に役割に応じたセキュリティ教育を実施**する。

指示⑤(対策例)
従業員に対する教育を定期的に行い、適切な対応が行えるよう日頃から備える。

指示⑦
インシデント発生時の対応について、**適宜実践的な演習を実施**させる。

工数削減してうまくやりたい？
工数かけてうまくやりたい？

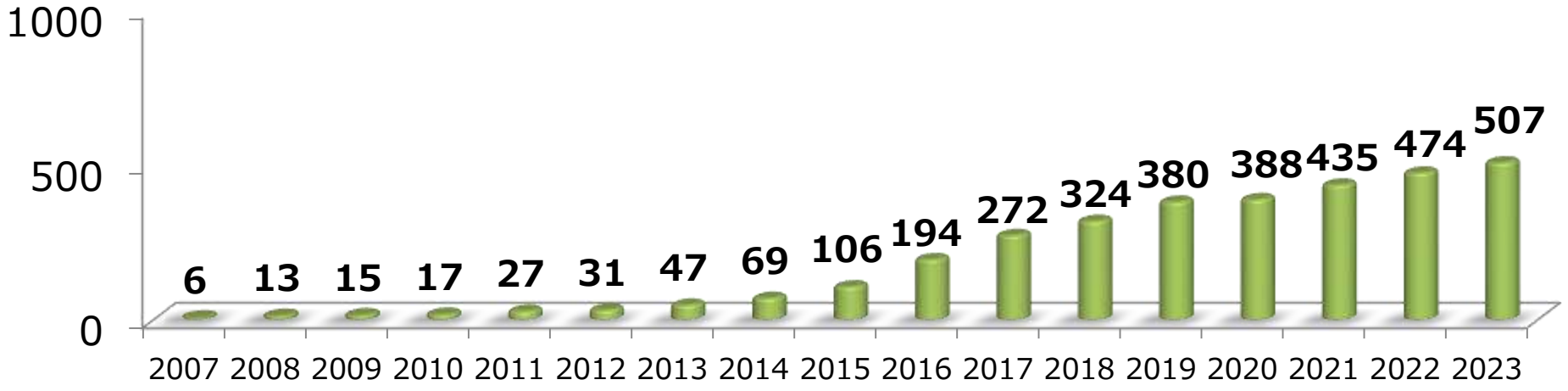
簡単に日本シーサート協議会を紹介します

- 設立
  - 2007年3月（2020年4月より一般社団法人として活動開始）
- 名称
  - 正式名称：一般社団法人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
  - 英語名：NIPPON CSIRT ASSOCIATION
  - ウェブ： https://www.nca.gr.jp/
- 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

CSIRT
日本シーサート協議会

ありがとうございます！

- 日本シーサート協議会の加盟チーム数も順調に伸び、累積で507チームとなりました(2023年10月現在)



活動概要

- シーサート同士の出会いと情報交換の場としていろいろやってます

テーマごとの会合

地区ごとの会合

期間ごとの会合

ワーキンググループ(WG)

- **問題提起と解決のための活動としてワーキンググループを立ち上げ、**
  会員ならびに協議会外部の協力者と共に、問題解決を図っていきます。
  https://www.nca.gr.jp/activity/index.html

シーサート構築前 → **シーサート構築後(協議会加盟後)**

【オブザーバ参加可】

オブザーバ参加可と指定したWGやワークショップ等(シーサートWG、シーサートワークショップなど)

【会員、専門委員のみ参加可】

CSIRT課題検討WG
CSIRT人材WG
脅威情報共有WG
 -システム連携推進 サブWG
インシデント事例分析WG
インシデント対応演習訓練WG
- 机上演習手法検討サブWG
- メール訓練手法検討サブWG

セキュリティレポーティングWG
サイバーセキュリティ研究動向WG
ログ分析WG
CSIRT評価モデル検討WG
法制度研究WG
ツール共有WG
工場セキュリティWG
脆弱性管理WG
セキュリティ教育検討WG
PSIRT WG

本日お話するWG

名称	主査	活動内容
インシデント対応演習訓練WG 主にCSIRTを対象	井出　雄介 (PIRATES)	インシデント対応訓練を効率的・効果的に実施するための手順・ノウハウについて、加盟チームでの実施事例を共有すると共に、机上演習ガイドの具体化や模擬机上演習を通じてインシデント対応訓練の実施を促進する。
セキュリティ教育検討WG 主に組織の従業員が対象	渡辺 文恵 (DeNA CERT)	組織内の従業者向けセキュリティ教育に関する情報共有や課題解決のためのディスカッションを実施し、各組織の教育担当者が活用できる教育コンテンツをまとめたドキュメント類の検討も行います。そして多くのCSIRTで、より効果的で効率的なセキュリティ教育・啓発ができるようになることを目指します。

工数削減してうまくやりたい話

問題意識：演習(訓練)について

- **いざというときの備えとして**
  インシデント発生時の訓練や演習を実施したいけど
  実施のハードルが高く、実現に至っていない・・・

  - **関係者、参加してほしいプレイヤーの勧誘に手間がかかる**
    ✓ 「必要性の理解」「目的の設定」「日程調整」
  - **訓練や演習の準備に工数がかかりすぎる**
    ✓ 「シナリオ作成」「会場の準備」「配布物準備」「事前説明」
  - **訓練や演習実施中の差配できる人がいない**
    ✓ 「司会進行技術」「ディスカッションの活性化」

訓練WGから（まとめ）

- **関係者、参加してほしいプレイヤーの勧誘に手間がかかる**
  - ✓ 「必要性の理解」「目的の設定」「日程調整」
- **訓練や演習の準備に工数がかかりすぎる**
  - ✓ 「シナリオ作成」「会場の準備」「配布物準備」「事前説明」

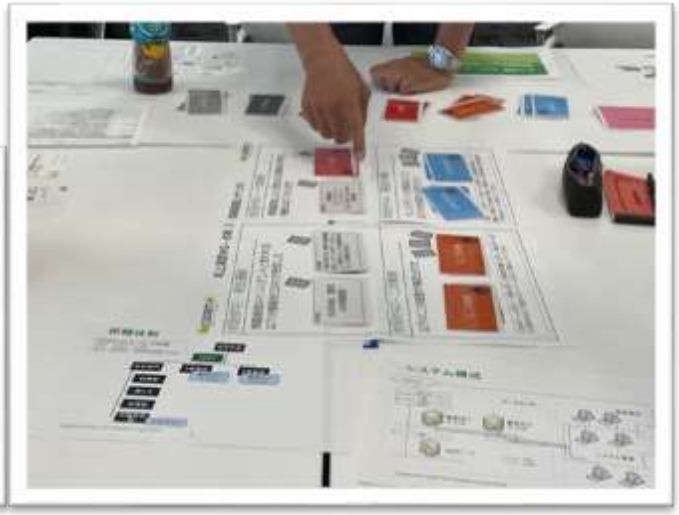
▶ **担当者たちの知恵(ノウハウ)を文書化したマニュアルに沿ってスモールスタートでやってみることができる**

- **訓練や演習実施中の差配できる人がいない**
  - ✓ 「司会進行技術」「ディスカッションの活性化」

▶ WGに参加して
できている組織に直接聞くことができる
できる人のやり方を直接見ることができる

訓練WGから (1：未経験者歓迎)

- 2020年(コロナ禍)のWG内アンケートにて、35%のシーサートが演習・訓練を定期的に実施していると回答した
  - ベテラン、未経験者まざって、一緒に体験できる場
  - 演習キット

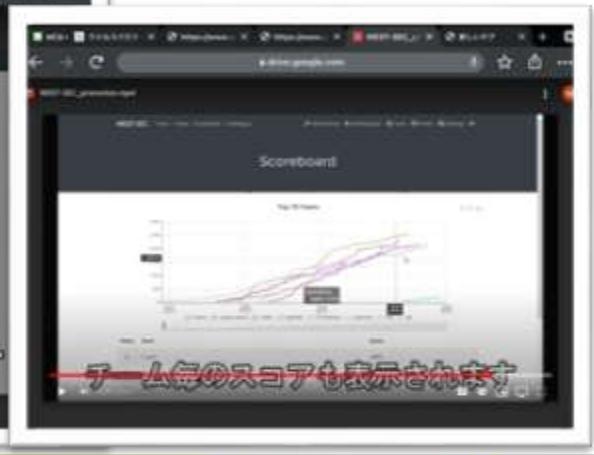


訓練WGから (2：オンラインによる演習)

- コロナ禍により、オンラインによるインシデント対応も実際ある
  - 有志が集まってガイドを作成 (2021年オンライン演習ベストプラクティス集)
  - Webでの演習キットを作成＆もちろん体験 (2020年CTFd)


NCA机上演習
オンラインベストプラクティス集

目次



訓練WGから (3：活動はNCAの枠を超え)

- **2019年 FIRSTにてワークショップ開催**
- **2023年 CAPJの演習体験**

30th Annual FIRSTCON2018 (WGメンバー撮影)



23件 15ヶ国

31th Annual FIRSTCON2019
(WGメンバー撮影)


訓練WGから (4：活動を通じた成果)

- **6年間の様々なノウハウを文書化**
  - スムーズな訓練運営をするためのガイドが欲しい
  - スキマ時間や朝会で実施がしたい
  - 他組織の訓練を聞きたい

分類	ドキュメント名	概要	開示範囲
演習 (訓練)	**サイバー攻撃演習訓練実施マニュアル_Ver.1.2**	**サイバー攻撃演習/訓練実施手法を整理、自組織での演習/訓練運営のための手引き資料**	**一般公開**
	インシデント机上演習ガイド第1版	Red vs Blue 机上演習キット インシデント対応机上訓練ガイド_第1版	WG外秘
	201912_机上演習sWG	sWGの概要説明、新演習案02と、**15分演習**の説明	WG外秘
	新演習案02-20181202-v2.0	新演習案02の実施案とシナリオ	WG外秘
	オンラインベストプラクティス_20211117	オンラインベストプラクティス集	WG外秘
事例共有	発表要旨	WGにて**事例紹介**の発表内容の骨子を抜き出し、共通様式でA5 1枚程度にまとめたもの	WG外秘
メール訓練	**メール訓練手引書__第3版**	**メール訓練担当者向け実施手引書**	**一般公開**

マニュアルを活用して工数削減

- サイバー攻撃演習訓練実施マニュアルを用いると
  - **サイバー攻撃演習/訓練実施の実施手法、検討ポイントがわかる**
  - **目的を設定し、どのようなタイプの手法を選択すればよいかわかる**
  - **演習/訓練を難易度で分類し、成熟度に沿った指針を立てられる**

第2章　サイバー攻撃演習/訓練実施のためのSTEP

- STEP1：プロジェクトの構築
- STEP2：情報収集
- STEP3：計画の作成
- STEP4：シナリオ検討
- STEP5：実施準備・実施
- STEP6：実施後対応

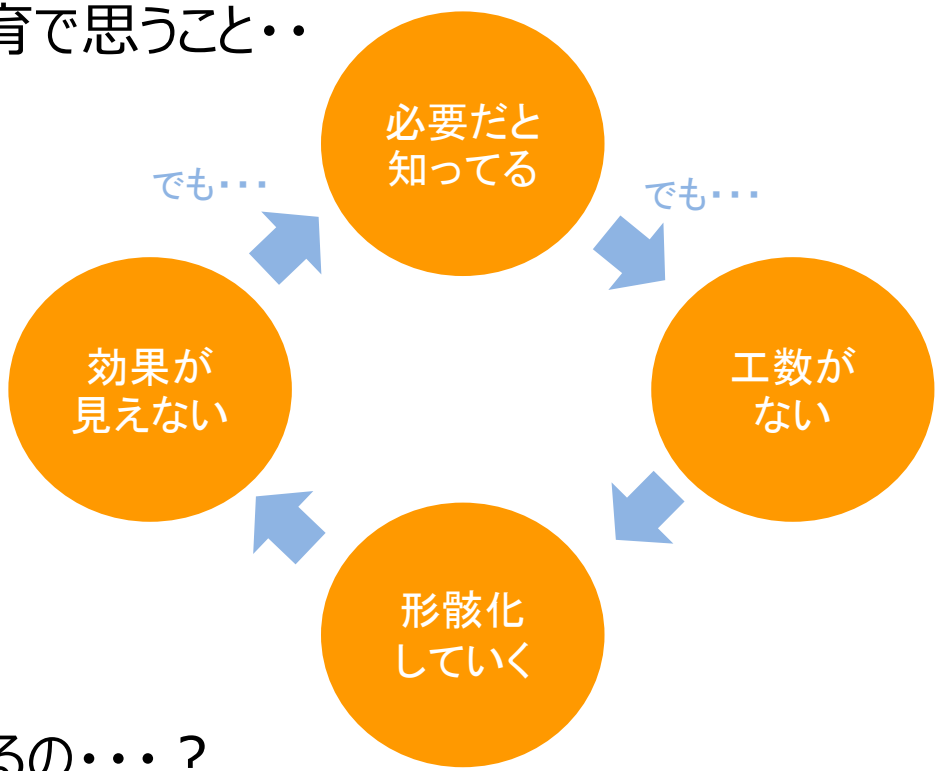
目的例：

- インシデント対応フローの検証
- インシデント対応フローの習得
- サイバー攻撃における、事業継続計画(BCP)の検証
- CSIRTのインシデント対応能力の向上
- インシデント対応時の自組織内の情報連携の検証
- インシデント対応時の組織外情報連携の検証
- インシデント対応時のリソースの検証
- インシデント対応時のコミュニケーションツールの検証
- インシデント対応時のコミュニケーションツールの習得
- 自組織内への啓発活動/意識向上/役割理解促進
- テクニカルスキルの習得　etc.

工数かけてうまくやりたい話

問題意識：社内セキュリティ教育について

セキュリティ教育で思うこと・・



みんなどうしてるの・・・？

セキュリティ教育検討WG　～やってみた～

セキュリティ教育検討WG　2022年10月設立
2023年11月現在　137組織311名が登録
検討する教育の対象は、組織の従業者

これまで事例共有、発表していただいた皆さん(敬称略)
・事例共有会
DeNA / サイボウズ / インテック / ワコール / 小林製薬/小田急電鉄 /
東京海上ディーアール / ANAシステムズ /
・LT大会
Sansan / MICIN / KINTOテクノロジーズ/ マイナビ / NTT-CERT/
サイボウズ / DeNA / 東京海上ディーアール /日本たばこ産業 / 小林製薬

ありがとうございます！

セキュリティ教育検討WG～やってよかった～

事例共有で得られた知見

- 親近感を持たせる・興味をひくコンテンツ
  - ボードゲーム、4コマ漫画、イベント、CTF
- 教材作成に使えるコンテンツやツール
  - 無料教材、無料イラスト、音声ソフト
- 組織体制、役割に合わせたプログラムラインナップ
  - マネージャー向け、事業ラインの窓口担当者向け
- 各社の教材の完成度、工夫
- 実はインターネット基礎の基礎が必要だった・・

など

セキュリティ教育検討WG～やってよかった～

質疑応答やアンケートから見えてきた、尽きないお悩み

- どのくらい工数かけてますか？
- うちには指標がない
- 効果測定やってますか？どうすれば？
- 対象者のリテラシーに合わせたコンテンツを作りたいけど工数が・・
- 経営層向けにやってますか？委託先はどうしてますか？
- テストの難易度は・・？ ？
- リアル講義がいい？録画でいい？

などなど・・・

事例共有やディスカッションはまだまだ続く！

セキュリティ教育検討WG～これから～

評価モデルの例
カークパトリックの4段階評価法

Level 4	• Results（成果）	成果の達成度…職場の業務向上、業績貢献
Level 3	• Behavior（行動）	職場での応用度…インタビューや他者評価など
Level 2	• Learning（学習）	学習の達成度…理解度テストやレポートなど
Level 1	• Reaction（反応）	学習の満足度…アンケート調査など

【参考】https://www.kirkpatrickpartners.com/the-kirkpatrick-model/

セキュリティ教育検討WG～これから～

事例共有・ディスカッションに加えて分科会

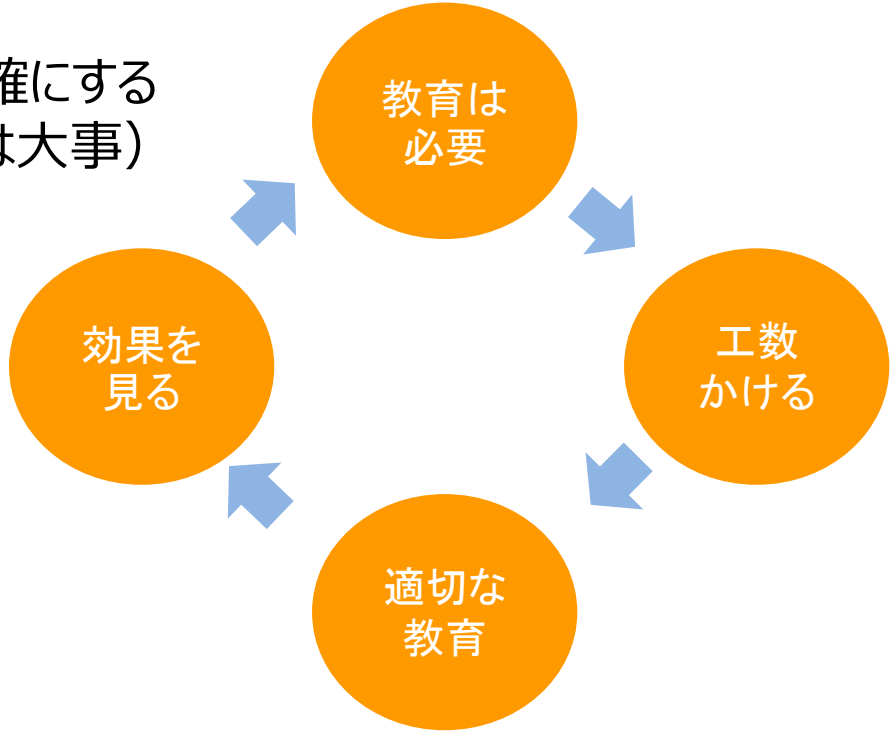
- **セキュリティ教育動向調査（仮）**
  組織内セキュリティ教育の動向、傾向などをまとめ各社の参考にしてもらう
  ・社内教育に関するアンケートをとってデータ集計する
  ・集計・分析結果をまとめてNCA内に公開する

- **サンプル教材作成（仮）**
  各社での教材作成を効率化する
  ・自社の研修資料を持ち寄って、よき研修資料のサンプルを作る
  例）テキスト、テスト問題、アンケートなど
  ・WG内（もしくはNCA内）に共有して活用してもらう

セキュリティ教育検討WG～まとめ～

セキュリティ教育で思うこと

- まずは自組織の教育の目的を明確にする
- ちゃんと手間ひまかける（仕込みは大事）
- 効果を見逃さない



WGに思うこと

- もっと共有、もっとディスカッション
- やがてアウトプット
- 越境学習

まとめ

- 訓練・演習、教育ともに効率化と改善を継続的に実施
- 小さく始めて育てればいい
- 目的を明確に
- 効果を測って次につなげよう
- 仲間の知恵を借りてうまくやろう

コミュニティをぜひ活用してください

知恵共有
運用よくなりゃ
皆ハッピー

ちょっと宣伝：Annual Conference 2023

シーサートに限定しないセキュリティトピックが満載
コミュニティを知る　コミュニティに参加する
一般参加可能　無料

https://annualconf.nca.gr.jp/

ありがとうございました

CSIRT同士の積極的なコミュニケーションを図ることによって、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

https://www.nca.gr.jp/