【 世界の金融市場に視る、サイバーセキュリティ防災訓練とは？】

～ NUARI　DECIDE®platformのご紹介 ～

2018年6月

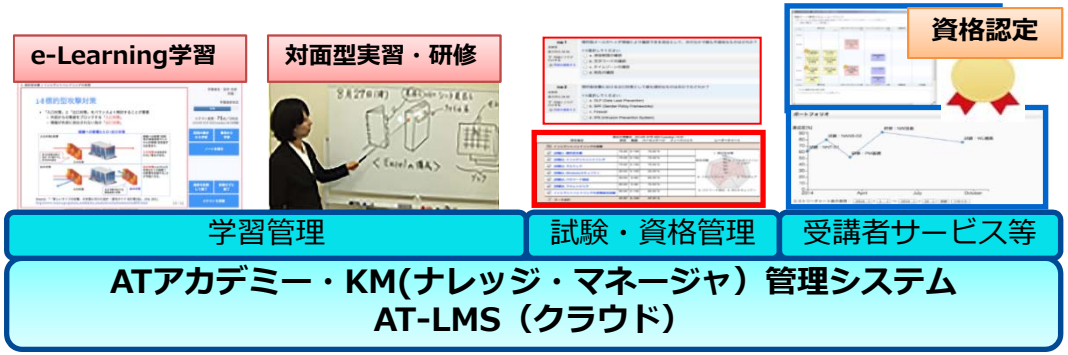
アライドテレシスアカデミー株式会社

Allied Telesis Academy Inc.

会社概要

アライドテレシスアカデミー株式会社

代表取締役	小林　忍
設立	2006年11月
本社場所	〒141-0031 東京都品川区西五反田7-21-11　第2TOCビル TEL 03-5437-6066 FAX 03-5437-6062
業務内容	◆ ITのネットワーク分野から始め、ITの各分野における、スキル指標を公開した資格制度をATアカデミー資格として、設立・実施・運営 ◆ ATアカデミーに関する教育ソリューション（資格・研修・e-Learning等）を、大学・外郭団体・SIerに紹介・販売



サイバーセキュリティをめぐる最新事情

■「情報セキュリティ10大脅威 2017」

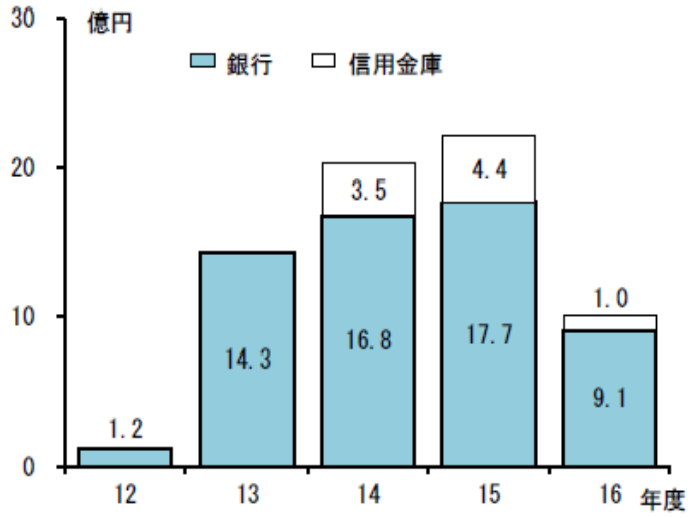
昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル欠如に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT機器の不適切な管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

出典：IPA「情報セキュリティ10大脅威2017」
https://www.ipa.go.jp/security/vuln/10threats2017.html

近年のセキュリティの事例は標的型攻撃やランサムウェアなどどんどん巧妙な手口、組織的な犯罪となっている。

金融機関のセキュリティに関する取組み

インターネット・バンキングによる
預金などの不正引き出し金額の推移



（資料）全国銀行協会、全国信用金庫協会

＊Financial System Report-Annex 2017年10月発行より引用

サイバー攻撃に起因した国内の大規模な
情報漏えい事例

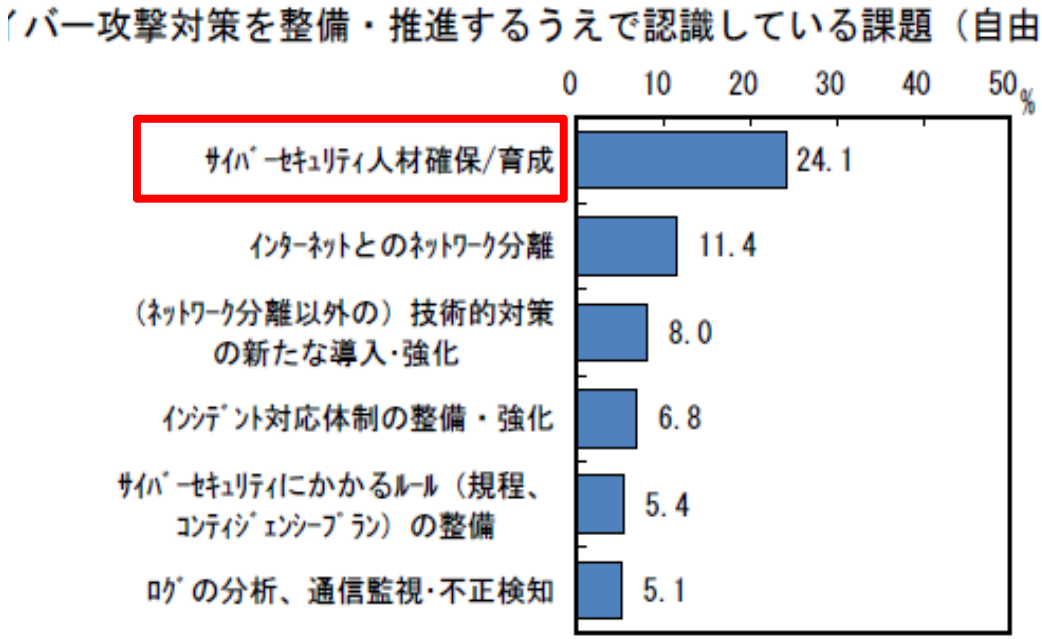
時期	内容
2013年	不正アクセスによって最大2,200万件の顧客ID情報と100万人強の暗号化されたパスワードが流出した可能性。
2015年	標的型メールによるサイバー攻撃を受け、システムに格納していた100万件強の個人情報が流出。
2016年	子会社職員が、取引先を装った標的型メールの添付ファイルを開きマルウェア感染。不正アクセスにより800万人弱の個人情報が流出した可能性。
2017年	クレジットカードによる支払サイトに不正アクセスが発生し、利用者のクレジットカード情報70万件弱が流出。
2017年	オンラインストアに対して脆弱性を悪用した不正アクセスが発生。100万件超の顧客情報が流出。
2017年	チケットサイトに不正アクセスがあり、個人情報約15万件（うちクレジットカード情報約3万件）が流出。カード不正利用による被害も一部判明。

（資料）各種公表情報

金融機関が昨今の環境変化に対応し、付加価値の高いサービスを創出していくうえでは、外部などからの 攻撃に対する情報の安全管理およびコンピュータシステム・通信ネットワークの安全性や信頼性の確保、すなわち**サイバーセキュリティの確保が不可欠**である。
2018年にはコインチェック株式会社のネム流出金額、580億円

サイバー攻撃に対する課題

- 日本銀行「Financial System Report-Annex]2017年秋、報告書



バー攻撃対策を整備・推進するうえで認識している課題（自由記述、上位 6 位）

＊Financial System Report-Annex
2017年10月発行より引用

サイバーセキュリティ対策を担う専門人材は質・量ともに不足している。経済産業省の「IT人材の最新動向と将来推計に関する調査結果」によると、IT企業及びユーザー企業の情報セキュリティ人材は、**2020年に約 19.3 万人が不足**すると推計されている。

出典：経団連「Society 5.0 実現に向けたサイバーセキュリティの強化を求める」
https://www.keidanren.or.jp/policy/2017/103_honbun.pdf

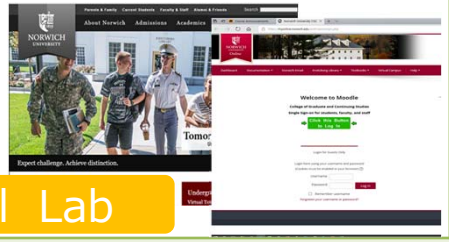
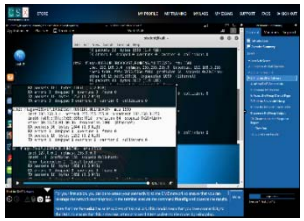
人材育成が急務

アライドテレシスグループが提供する研修

Level	内容	対象部署・対象者
Level5	CSIRTハンズオン研修　実践演習 （IPA：情報セキュリティ安全支援士試験対策対応）	**CSIRTメンバー（候補含む）、SOCメンバー 法務・総務部・広報部**
	各業種に渡るサイバー演習支援・管理ツール（DECIDE Platform)を利用した本格的な実践演習	
Level4	サイバーセキュリティのフォレンジック手法や各種セキュリティ・インシデントの特徴および対策を学習	**CSIRTメンバー（候補含む）、SOCメンバー 法務・総務部・広報部**
Level3	IT専門分野（外部資格）のサーバー構築資格（MCTS・LPIC/LinuC）、NW資格（Allied-CAP・CPE / CCNP)・プログラミング（LPIC/LinuC・Sea-J）との連携	**IS部・SE部・開発部**
Level2	人事/教育部門/IS部門でのハンドリング研修実施 (国民のための情報セキュリティサイト「社員・職員＆組織幹部＆情報管理担当の情報セキュリティ対策研修」)	**全社員**
Level1	社会人としてのセキュリティに関する基本コンピテンシー(国民のための情報セキュリティサイト「基礎知識＆一般利用者 研修」)	**新入社員・入社前研修**

※学生・新人からCSIRTメンバーになる道筋（キャリアパス）を、ご提案いたします

アライドテレシスアカデミーの提供する研修コンテンツ

Level	学習ソリューション			
Level5	各業種におけるサイバー攻撃に対する実戦さながらの演習			
	サイバー防災訓練ツール NUARI DECIDE®Platform.com 		情報処理安全確保 支援士CSIRT サイバー演習  	
Level4	CSIRTを実施する上で必要不可欠な知識および実践能力の習得			
	Norwich 大学大学院生向け e-Learning  NU Virtual Lab		CSX Practitioner   	
Level3	IT専門分野（外部資格との連携）			
	サーバー構築 MCP・LPIC/LinuC	プログラミング Oracle Java	NW構築 **ATACD認定制度** NW上級コース	情報セキュリティ Norwich大学 大学生向けe-Learning
Level2	サイバーセキュリティ初級 国民のための情報セキュリティサイト 対策編		2018年8月リリース予定	
Level1	サイバーセキュリティ入門 国民のための情報セキュリティサイト 基礎知識			

サイバーセキュリティ事業での海外との提携

アライドテレシス

ユーザー様

サイバーセキュリティサービス

日本の市場に合った研修

外部団体
共同研究

大学＋高等専門学校＋SI
＋各種セキュリティメーカー様

日本市場

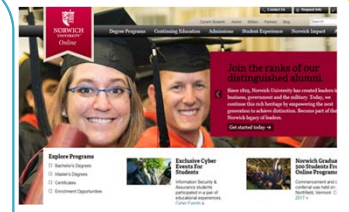
コンテンツの流通

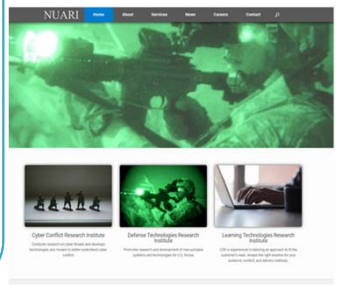
Webinar訓練
DECIDE®Platform

CSX (ISACA)
CYBERSECURITY NEXUS

Norwich Univ.
＋
NUARI
＋
ATI

NORWICH UNIVERSITY Online





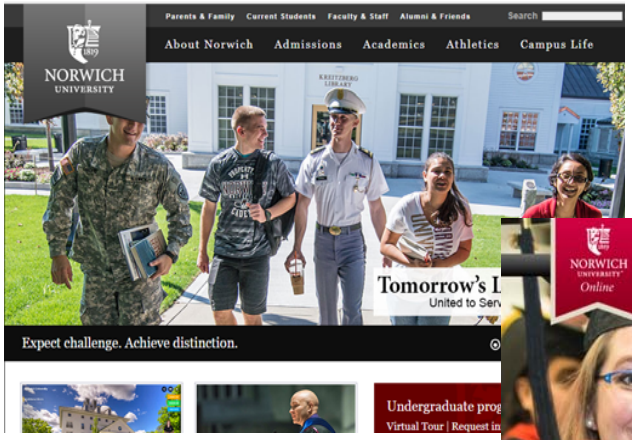
NUARI：Virtual・Incident・Exercise

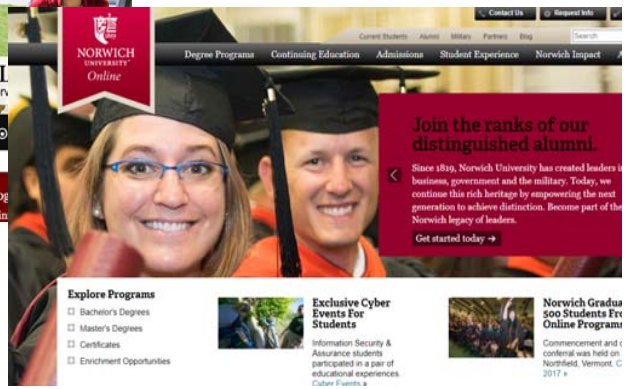
ISACA Osaka Chapter

US/EU

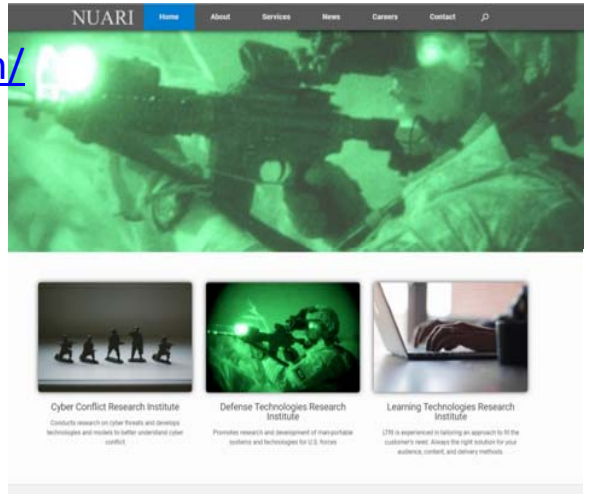
Norwich大学･NUARIとは

- Norwich大学の卒業生は、米国防衛省・国土安全保障省で就業するための権利を習得できる大学です。（日本：防衛大学）
  国家安全保障局（NSA）と国土安全保障省（DHS）にから、サイバー防衛教育のアカデミックエクセレンスセンター（CAE-CDE）に指定されました。学科の特徴としては、サイバー防衛とデジタルフォレンジックにあり、Defense Cyber Crime Center（DC3）はNational Forensic Academic Excellence（CDFAE）の国立センターとして認定されました。
- Norwich大学の応用研究機関企業（NUARI：Norwich University Applied Research Institutes）は、2002年にパトリック・リーヒー上院議員の下で立法化され、国土安全保障省と国防総省からの資金も投入され設立されたNPOです。NUARIは、サイバーインシデント管理の課題に取り組む国立センターであり、サイバー戦争ゲーム、分散学習技術、分散シミュレーション技術、重要なインフラストラクチャー訓練を通じ、人財を育成いたします。





http://www.norwich.edu/
https://nuari.net/
https://decideplatform.com/



NUARIが提供するDECIDE®platform

～　米国金融市場で使用されている
サイバー防災訓練ツール　～

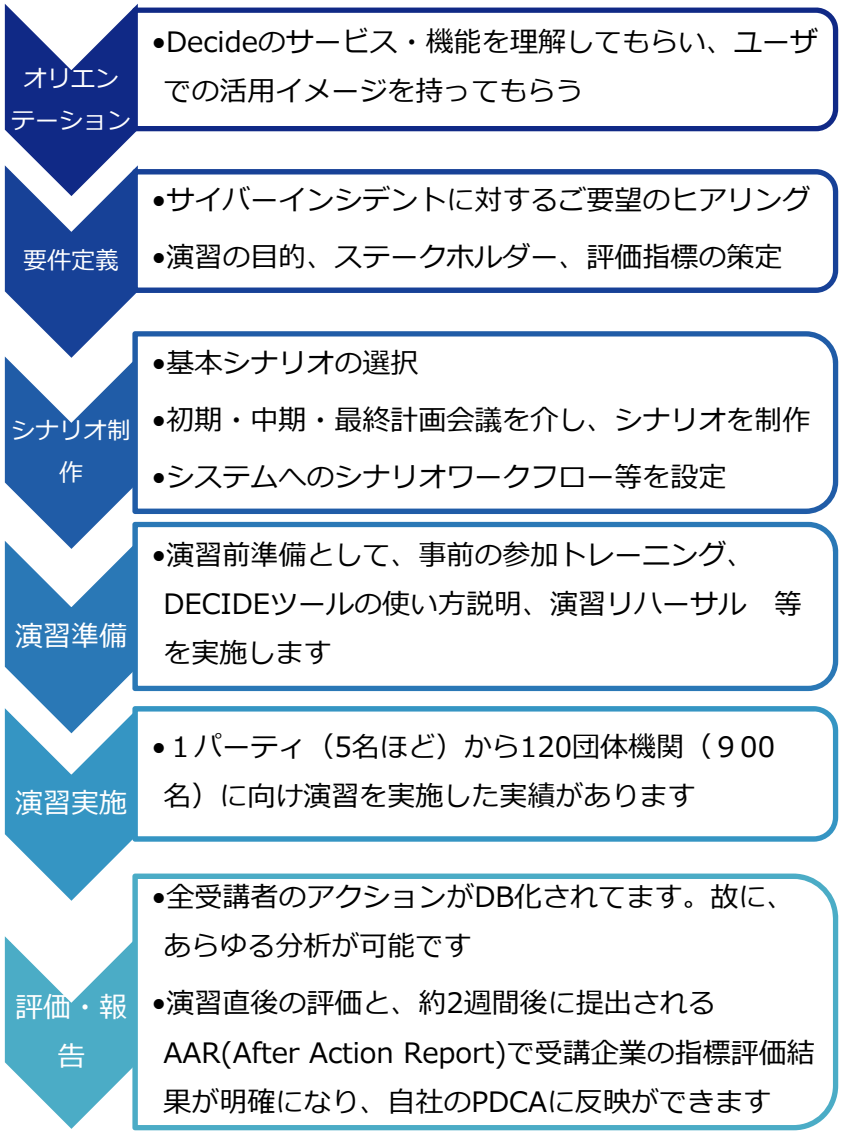
サイバー防災訓練ツール　DECIDE®platform

Webカンファレンスツール（ウェビナー）を使用したサイバーインシデントに対応するため防災訓練ツール。
（金融インシデントを含む、各業種に向けた15種類以上のシナリオを備えております。）

— DECIDE®platformは、「ワークフローアプリ＋Webiner 」

- インシデント通知：　メール/ファシリテーターによる起動
- アクション選択により、シナリオが自動的に変動します
- アクション選択の判断材料として、「国の指針」、「他社の対応事例」等参考情報が自動的に表記されます
- 対象　　企業の経営陣および、幹部の方々
  — CISO、広報、総務、法務、…

【DECIDE®platformの実施工程】



DECIDE Platform　動作概要

【質問と決定パネル】
　複数の選択肢からインシデント状況にあったアクションを選択するパネル。

選択された項目に準じた、Work Flowで次のアクションが指示されます。質問もチャットで行うことが可能です。

【情報タイル】
　ここに表示される内容は、現行発生しているインシデントの情報サイトです。　他のCSIRTメンバーが類似の事象が発生した際にどう対応したか、また、他の報告書等をチェックすることで、自分たちの次アクションを判断するための情報がここにあります。

【 受信inbox】
システムから送られてくるメールが、 メインコミュニケーションパネルとなります。 演習を通じて更新情報と重要な情報を表示していきます。 メッセージの送信や他の参加者への情報の転送が可能です。

- 事例ユーザー　　金融、製造業、IT会社、エネルギー会社　等
  （15種類以上のシナリオあり）

Quantum DawnとDECIDE Platform

Quantum Dawnとは：

Quantum Dawnという名を冠した演習は、2011年、2013年、2015年、そして2017年と過去４回、2年おきに実施。

初回のQuantum Dawnでは13の金融機関や関係組織が参加する規模で米国の株式市場がサイバー攻撃により混乱することを想定した演習が実施された。演習は回を重ねるごとに、その演習規模（参加組織や参加国）は拡大している。

<Quantum Dawn演習の軌跡>

演習プラットフォームとして
“DECIDE”が採用

① Quantum Dawn　2011年9月　－１部屋　13 団体にて実施

② Quantum Dawn2　2013年9月　－２か国　50団体にて実施

③ Quantum Dawn3　2015年9月　－４か国　72団体＋8政府機関にて実施（FBI, Department of Homeland等）

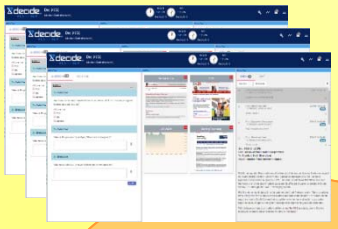
④ Quantum Dawn4　2017年11月　–全世界エリア (North America, South America, Asia, Europe, Africa)
120団体＋8政府機関にて実施

※Quantum Dawn3以降は、金融機関情報共有分析センター（FS-ISAC）や他の重要な政府パートナー金融機関主要機関が相互に情報交換し、システム攻撃に対する株式市場の運営を維持する対応プロセスを実践した。

DECIDE Platform演習　鳥瞰図

NUAR Iコントロール

ファシリテイター



ファシリテイター

団体

受講団体 *A*

DECIDE F.S.

オブサーバー機関

FBI

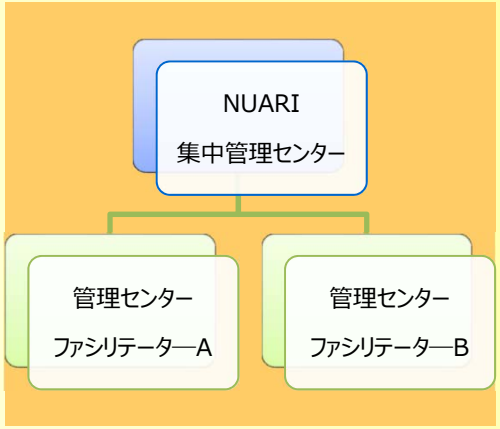
Treasury

DHS

ISAC

企業

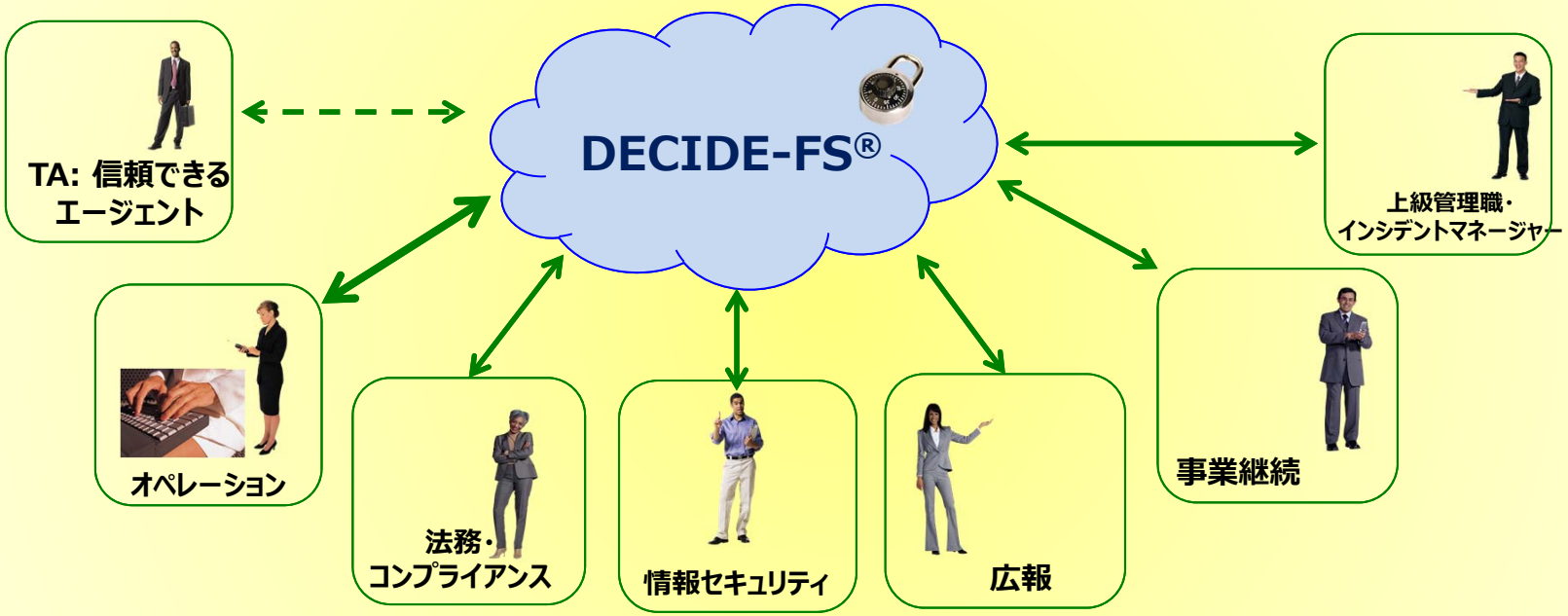
受講企業 *B*



DHS ： United States Department of Homeland Security　アメリカ合衆国・国土安全保障省
Treasury ： 国家財政委員会　　ISAC: Information Sharing and Analysis Center

DECIDE Platform演習　団体・企業の参加者役割

・団体・企業のキーパーソンが参加



・サイバーインシデントへの対応能力を評価すると同時に、課題を洗い出し、
今後のアクションに反映していきます

DECIDE Platform実際の演習スケジュール（QDⅢ）

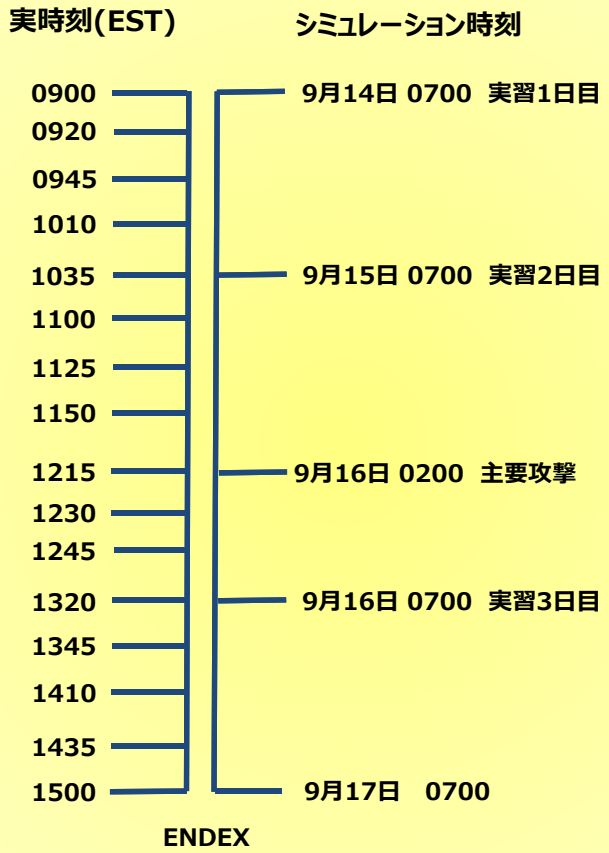
分岐点（BP)注記

1. 16 分岐点（設問）

2. 設問後休憩: 5分間

3.平均事象演習時間: 25分間 (5分間の休憩を含む)

4. 主要攻撃: 60 分間 で2回の小規模な分岐点を含む



予定表

1. 実時間 (EST): 6 時間

2. 実習は全3日で、それぞれ 清算および決済を含む完全な取引サイクルを包括する

3. 五つの攻撃シナリオ
   - DNS乗っ取り
   - DDoS
   - 外部への個人情報（PII）漏えい
   - 内部の可用性損失(DDoS)
   - 決済システムセキュティ侵害

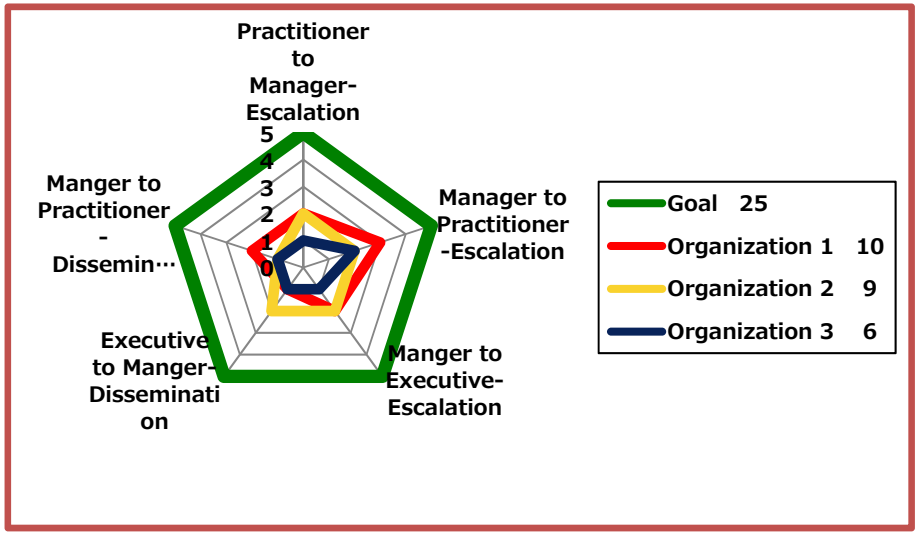
- インシデント発生の事象をシミュレーションすることで、6時間の演習で、4日間の対策演習カリキュラムを実施した
- 各分岐点で質疑応答が設定されており、回答データも全てDB化されます
- シナリオは選定項目により動的に変更されていきます　→　受講団体・企業の背の丈に合ったシナリオ構成となります

DECIDE Platform　評価・報告

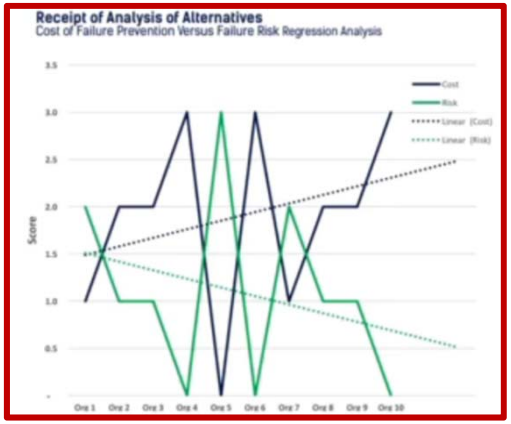
- ブレークポイント毎に設定された質疑応答結果
  - 各参加者が選択した、入力したデータの分析
- AAR(After Action Report)
  - 包括的な分析データ、PDCAに反映情報として活用してください
  - 通常、演習後約2週間で報告書を発行いたします

【ブレークポイント62の設問群での、各受講者の回答一覧】

【チームで比較したコミュニケーション評価一覧】



【RISKと投資との相関表】



DECIDE Platform　特徴

- シナリオがワークフローに従い動的に変更されるため、固定化されたシナリオよりも、受講者の特質を反映した有益な訓練を行うことができます

  ― 現在、日本での大規模なサイバー演習となると、同じ業種でも規模が異なる企業群が同時に同じシナリオで訓練している。 すると、規模、および業務目的の差異から身の丈から外れた演習となり、大規模サイバー訓練の課題であった。

  ― Quantum DawnⅣでは、世界の金融市場に位置する120団体＋8政府機関を対象に1日で実施している。同じ業種・規模の団体は、シナリオ経由ルートが略一致し、他社との比較も分析がしやすく、問題分析もより具体的に顕著化しやすい。 動的シナリオを使用することで、より高い訓練効果を得ることができる

- 評価分析報告もシステム化（一部）

  ― ブレークポイントでの質疑応答結果、フロー経路等、すべてデータベース化が図られ主だった分析内容は、システム基本機能として提示される
    - アンケート集計等の手作業等は不要

  ― 多々実施された訓練を基に、強味弱みの分析が実施され対応アクションが明確に提示される

「教育」でつなぐ、人と未来。アライドテレシスアカデミー

お問い合わせメールアドレス：　sales@at-academy.co.jp