

研究会 1
2020に備えたサイバー対処
サイバー攻撃におけるヒューマンファクター

第16回 デジタル・フォレンジック・
コミュニティ2019 in TOKYO
2019年12月9日(月)

山口 孝夫
有人宇宙システム株式会社

サイバー攻撃とヒューマンファクターの関連性

1. サイバー攻撃に関係するのは、

みんな人間である

攻撃する者

攻撃を受ける者

攻撃に対応する者

被害を受ける者

2. 情報漏洩の原因に特徴的なのは、

誤操作

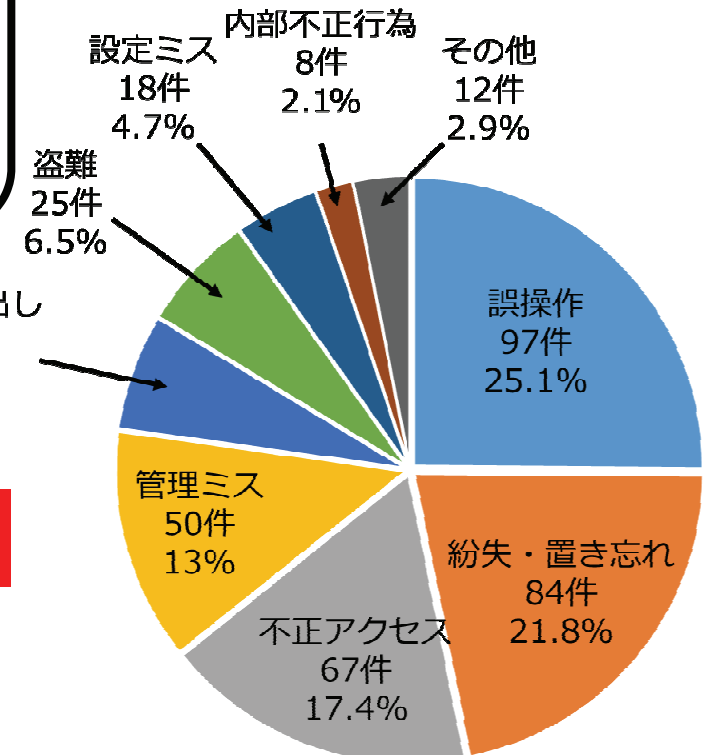
紛失・置き忘れ

管理ミス

設定ミス

ヒューマンエラー

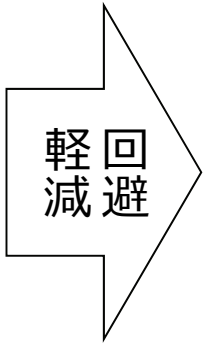
65%



出典：NPO日本ネットワークセキュリティ調査報告書（2017年）をもとに作図

ヒューマンエラー対策（航空宇宙分野）

事故原因の徹底究明
↓
ヒューマンエラー：約70%



5つの基本スキルの強化

ノンテクニカルスキル
または
(クルーリソースマネジメントスキル)

航空・宇宙分野のノンテクニカルスキル

訓練で徹底的に強化



情報漏洩における3つの不足・欠如

知識不足

守るべきルールを知らない

技量不足

知っていたが実行できない

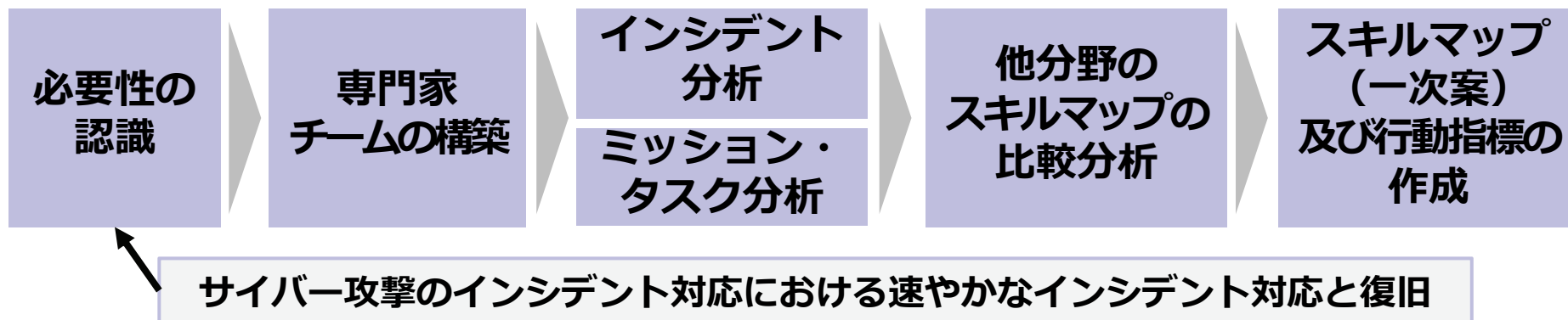
倫理感欠如

ルールを守ることができない

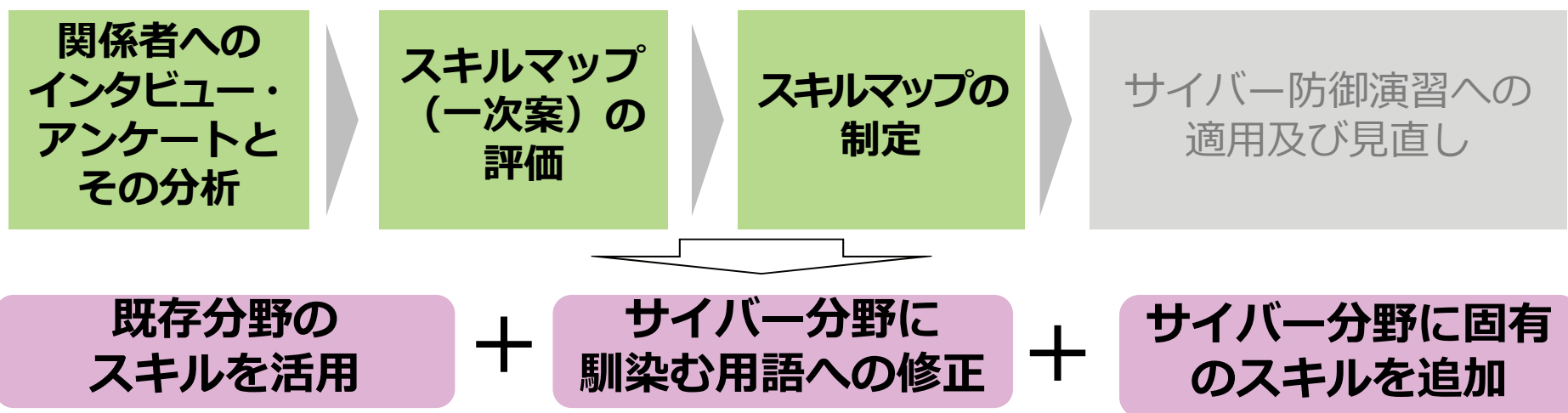
航空・宇宙分野ではありえない要因

サイバー攻撃固有のノンテクニカルスキルが必要

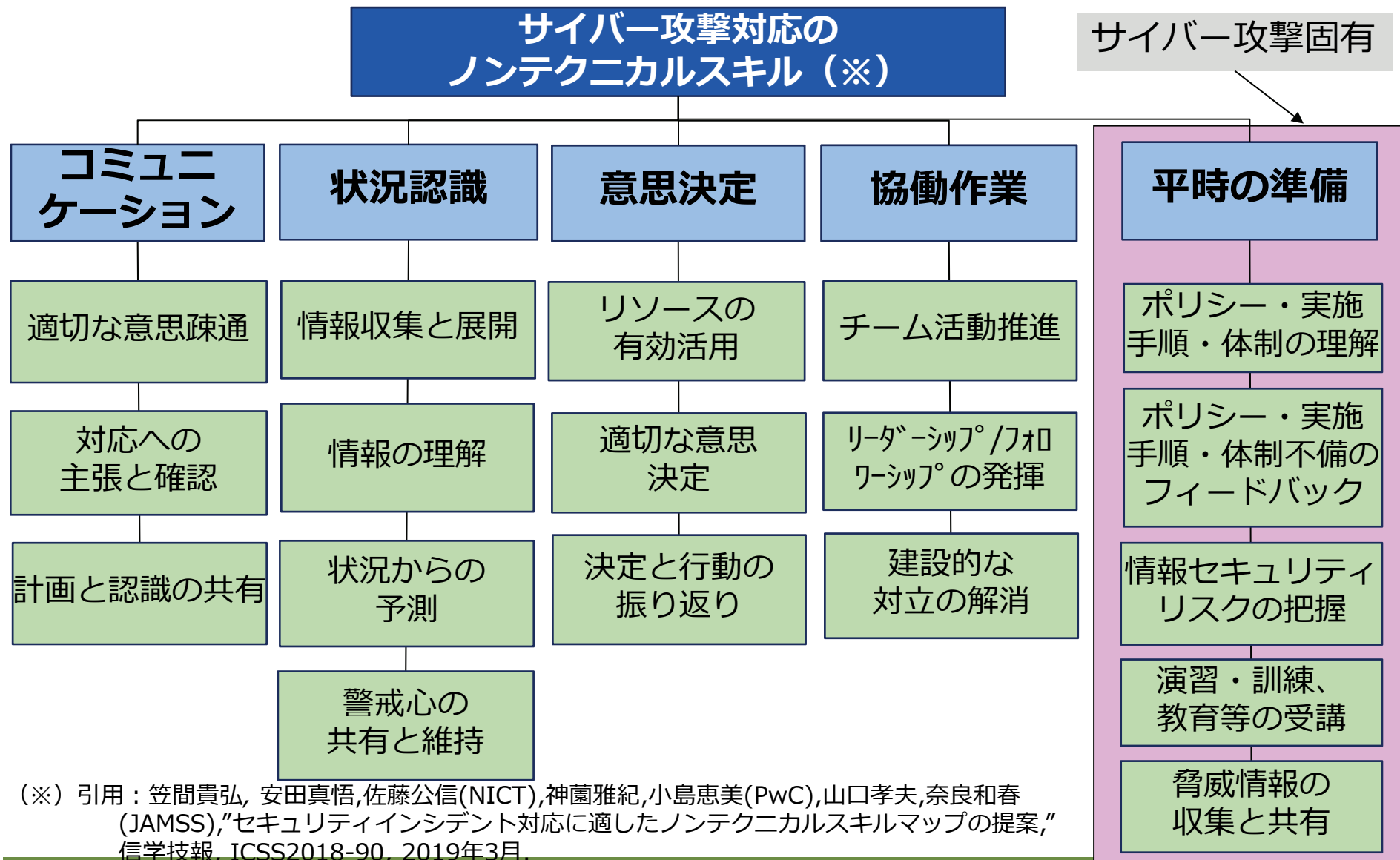
1 調査・分析段階



2 妥当性評価段階

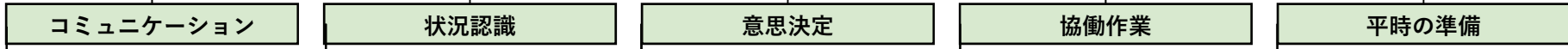


サイバー攻撃対応のノンテクニカルスキル

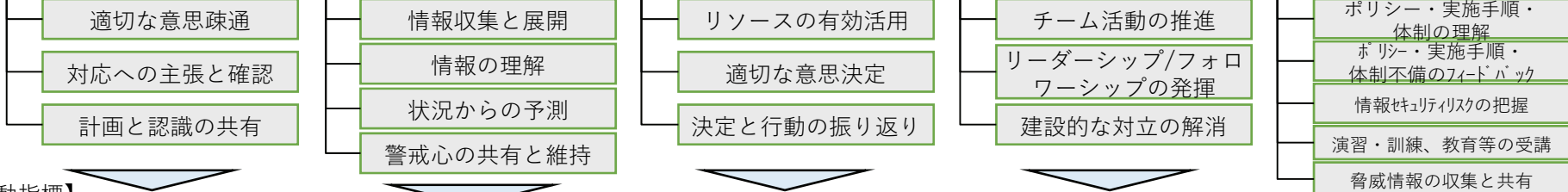


サイバー攻撃におけるインシデント対応に求められるノンテクニカルスキル

【スキル分類】



【スキル構成要素】



【行動指標】

<p>適切な意思疎通</p> <ul style="list-style-type: none"> 自分（発信者）のメッセージを、相手（受信者）が正しく理解したことを確認している。 相手（発信者）のメッセージを、自分（受信者）が理解したことを相手に伝えている。 自分のメッセージは、相手に期待するアクションを起こさせるような手段、内容で伝えている。 <p>対応への主張と確認</p> <ul style="list-style-type: none"> 主張と確認は、相手及び自分の立場や考えの両方を考慮して行っている。 危険な状況を察知した場合は、曖昧な言い方はせず、明確な言葉で、かつ適切な声量で主張及び質問している。 <p>計画と認識の共有</p> <ul style="list-style-type: none"> 5W1H「いつ、どこで、だれが、なにを、なぜ、どのように」の情報を関係者と共有している。 説明している。先々の計画や見込方針を適切に 	<p>情報収集と展開</p> <ul style="list-style-type: none"> 状況を正確に把握するため、適切な方法・手段で、または適切な担当者から、速やかに十分な情報を収集している。 収集した情報を必要な人に、適切なタイミングで、必要な情報を相互に交換している。 事実と想定を明確にして、正確に情報展開している。 <p>情報の理解</p> <ul style="list-style-type: none"> 提供された/収集した情報を正しく理解している。 提供された/収集した情報に基づき当該リスクの全体像を正しく理解している。 <p>状況からの予測</p> <ul style="list-style-type: none"> 収集及び理解した情報から、今後の状況がどうなるかを予測している。 <p>警戒心の共有と維持</p> <ul style="list-style-type: none"> インシデント発生時の警戒心と、状況予測からの危機感を関係者と共有する。 一点集中や思い込みをせず、常に周囲の状況、情報に注意を向けて、明らかになっていないインシデントの有無を意識して情報収集に努めている。 	<p>リソースの有効活用</p> <ul style="list-style-type: none"> 関係者が意思決定の場に参加して、意見や解決策を提案している。 自分または自チームで判断・対応が難しいと判断した場合、然るべき人員・組織・外部の専門家等のリソースを有効に活用している。 <p>適切な意思決定</p> <ul style="list-style-type: none"> 意思決定を行ううえでの前提条件（時間的制約、Go/No_Goの判断基準、重要度、リスク）を特定している。 不測の事態/緊急事態を想定して、代替案を考慮のうえ意思決定をしている。 意思決定に基づく行動を起こす前に、現在の状況を再確認している。 <p>決定と行動の振り返り</p> <ul style="list-style-type: none"> 意思決定に則した行動を行い、その結果の適否を確認している。 意思決定と決定根拠、そして行動結果の適否を関係者で共有している。 	<p>チーム活動の推進</p> <ul style="list-style-type: none"> チーム活動促進のため、発言しやすい、意見を言いやすい、聞きやすい、そして活動に参加しやすい雰囲気・環境作りを行っている。 関係者が与えられた役割に応じて、主体性と責任をもって行動している。 <p>リーダーシップ/フォローアップの発揮</p> <ul style="list-style-type: none"> リーダーとして、関係者に対してインシデントの収束に向けた動機付けや行動の方向付けを行っている。 リーダーとして、インシデントの収束に向けて、フォロワーに業務指示、アドバイス、及び結果に対するフィードバックを行っている。 フォロワーとして、インシデントの収束に向けて、リーダーの業務指示やアドバイスに従って行動し、行動後はリーダーに状況を報告している。 <p>建設的な対立の解消</p> <ul style="list-style-type: none"> 関係者の意見の対立や、認識の齟齬がある場合、感情の対立に発展させずに、論理的・客観的に対立の原因究明と解決策を見出している。 	<p>ポリシー・実施手順・体制の理解</p> <ul style="list-style-type: none"> インシデント対応に必要なポリシー、対策基準、具体的な実施手順などを理解している。 ポリシー、対策基準、実施手順を適切に運用している。 <p>ポリシー・実施手順・体制不備のフィードバック</p> <ul style="list-style-type: none"> ポリシー・実施手順などに不備がある（ある）あった場合は、然るべき人員・組織に報告する。 インシデント発生時にインシデントレスポンスが適切に機能する体制で（ない）なかった場合は、然るべき人員・組織に報告する。 <p>情報セキュリティリスクの把握</p> <ul style="list-style-type: none"> サイバー攻撃による潜在的なセキュリティリスクを理解している。 <p>演習・訓練、教育等の受講</p> <ul style="list-style-type: none"> サイバー攻撃によるインシデント発生時に備え、演習や訓練等の教育を定期的に受講し、その効果を確認している。 <p>脅威情報の収集と共有</p> <ul style="list-style-type: none"> 日々巧妙化しているサイバー攻撃等の脅威情報や、インシデント対応に関連する情報を日ごろから収集し、関係者と共有している。
---	--	--	--	--

(※) 引用：笠間貴弘, 安田真悟, 佐藤公信(NICT), 神園雅紀, 小島恵美(PwC), 山口孝夫, 奈良和春(JAMSS), “セキュリティインシデント対応に適したノンテクニカルスキルマップの提案,” 信学技報, ICSS2018-90, 2019年3月.