教育教材（概要）

育成対象：**技術者層（鉄道：電気部門、航空：システム維持管理部門）**

対応	担当部署		サイバー攻撃の際の役割
	鉄道	航空	
システム異常の検知・通報	司令所/指令所	システム運用部門（オペレーター）	**異常の原因としてサイバー攻撃があるという意義をもち、適切に連絡ができる能力**
システム障害対応	電気部門（外部委託先を含む）	システム維持管理部門（外部委託先を含む）	**サイバー攻撃に備えた準備、インシデント発生時の対応、サイバー攻撃対策などの一連の活動に「対応」*1)できる能力**
サイバー攻撃のインシデント対応立案、実行	セキュリティ担当部門 CSIRT・情報システム部門 セキュリティベンダー等		**サイバー攻撃に備えた準備、インシデント対応、サイバー攻撃対策などの一連の活動を立案、実行できる能力**

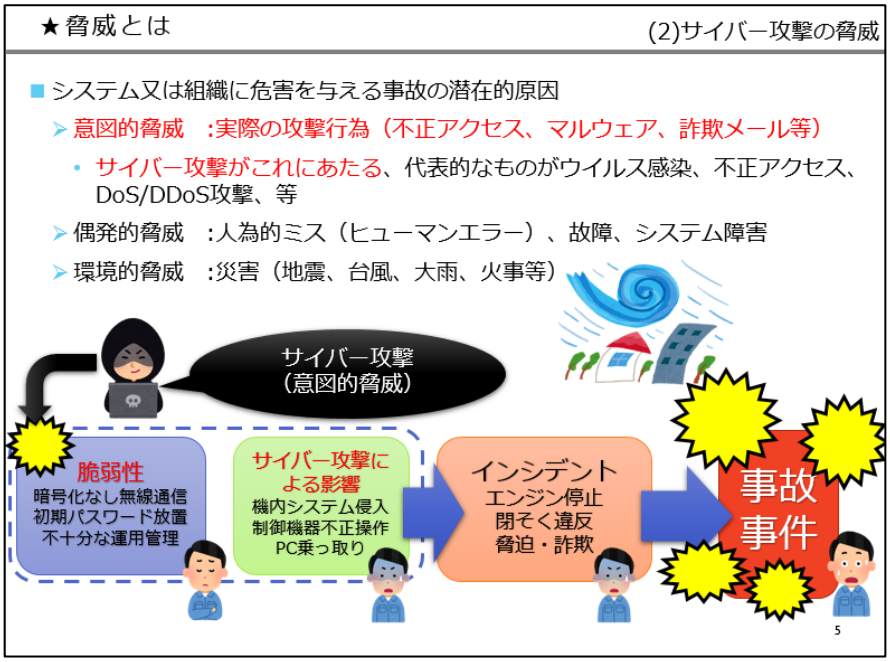
*1)「対応」とは、対象となるシステムを維持管理する人材が、サイバーに対処（原因究明、復旧など）する専門機関の助言を受けて、システムの復旧につなげる活動などにあたる他、システムを熟知する立場から、サイバーに対処（原因究明、復旧など）する専門機関と連携して、システムに関する助言や援助を行うことを指す。

カリキュラム

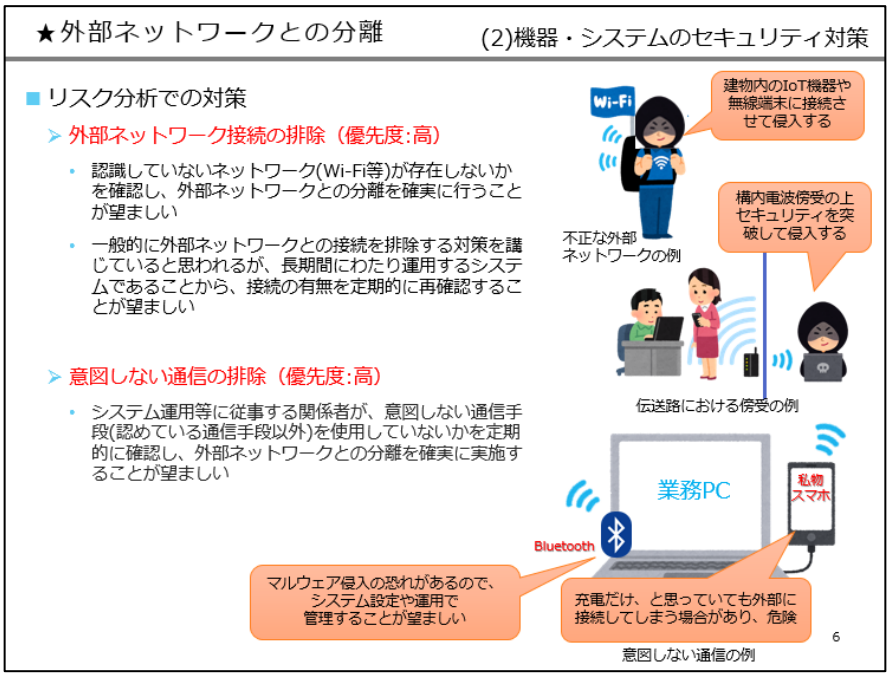
講座名	学習内容	
第1回サイバー攻撃の現状	(1)サイバーセキュリティに関する動向 (2)脅威とインシデント (3)想定される攻撃手法 (4)セキュリティ確保への取り組みの状況	サイバー攻撃により、業務に関わるシステムの停止や誤作動が生じると、社会的混乱や人的被害をもたらす可能性があり、その対策が急務であることを認識する。
第2回サイバー攻撃の手法と脆弱性	(1)サイバー攻撃の脅威 (2)脆弱性	鉄道分野及び航空分野において発生する可能性のあるサイバー攻撃の手法と脆弱性を理解する。
第3回サイバーセキュリティ基礎	(1)セキュリティマネジメント (2)資産管理の重要性 (3)リスク評価の重要性	サイバーセキュリティ対応の基礎となる考え方や手法の概要とその重要性を理解する。
第4回ネットワーク基礎	(1)ネットワークとプロトコル (2)TCP/IP の概要 (3)ネットワーク接続機器	サイバー攻撃の概要を把握するため、また、サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携し、対応（支援）するために必要となるネットワークの知識を学習する。
第5回セキュリティ技術	(1)対策技術の用語と概要 (2)多層防御 (3)フォレンジックの概要	サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携し、対応（支援）するために必要となるセキュリティ技術の用語と概要を学習する。
第6回サイバー攻撃対策	(1)設備・システムのセキュリティ対策 (2)運用・管理のセキュリティ対策	主なセキュリティ対策の概要を学習する。
第7回サプライチェーンのセキュリティ対策	(1)サプライチェーンのセキュリティ対策の重要性 (2)外部委託範囲の特定と管理 (3)情報の入手とその有効活用	サプライチェーンのセキュリティ対策の重要性とインシデント対応に備えるための重要なポイントを学習する。
第8回インシデント対応	(1)インシデント発生時の対応手順 (2)インシデント対応体制 (3)初動対応のポイント	インシデント発生の際、その原因がサイバー攻撃である疑いを考慮し、迅速かつ適切に対応（支援）するためのポイントを学習する。
第9回学習の振り返り	(1)コースのまとめと振り返り (2)質疑応答	学習の振り返りを通して本カリキュラムを総括する。

教材の一例

教材とりよせ申請はこちらをクリックしてください



第2回：サイバー攻撃の手法と脆弱性より



第6回：サイバー攻撃対策より