東工大キャリアアップMOTプログラム
サイバーセキュリティ経営戦略コース
（2023年度） 説明会

2023年＠Zoom収録によるweb配信

（前半）コースコーディネーター三笠、CUMOT古俣

〇ご挨拶

〇急速に変化していくサイバーセキュリティ人材の役割

〇目指すべき姿　ー戦略マネジメント層とは？

〇コースの目的と特徴

〇カリキュラム・講師紹介（担当予定）

（後半） CUMOT古俣

〇CUMOTとは

〇受講形態（Zoomによるオンライン受講）

〇実施概要/募集要項

〇受講実績と受講イメージ　ご紹介

〇FAQ／アンケートのお願い

サイバーセキュリティ経営戦略コース
コーディネーター　ご紹介とご挨拶

三笠　武則（みかさ　たけのり）
株式会社NTTデータ経営研究所
エグゼクティブスペシャリスト
兼　営業秘密保護推進研究会 事務局長
兼　一般社団法人日本クラウド産業協会 理事

小野 浩司（おの こうじ）
ALSOK
商品サービス戦略部
情報セキュリティサービス推進室長

急速に変化していく
サイバーセキュリティ人材の役割

サイバーセキュリティを担う人材が背負う役割はどんどんと重くなってきていて、企業価値を左右してしまうところまできています。

1. **企業は今生き残るために・・・**
   標的型攻撃／ランサムウェア、サプライチェーン攻撃等の課題に対処することに加えて、
   インシデント対応に日頃から着実に備え、
   経験のない危機的事態に直面しても事業を継続する力が必要に。

2. **そして、企業経営は今生き残ることから、将来を生き抜くことへ！**
   戦略的な知財・ノウハウ活用と**保護を実現するガバナンス構築**が浸透中。

3. **さらに、企業の競争力を守ることから、国家の競争力を守ることへ！**
   ゼロデイ攻撃が持つ意味や背景とは？　・・・実は、10億円規模の裏ビジネス。
   国家的なスパイ／サイバー攻撃に晒され、**経済安全保障やセキュリティクリアランスにも力を注ぐことが不可欠**に・・・

これからの時代は、**経営層と現場の両方に寄り添い**、経営層のリーダーシップと
ガバナンス構築を導くことができるサイバーセキュリティ人材が益々重要になります。

目指すべき姿
戦略マネジメント層とは？

戦略マネジメント層とは、内閣サイバーセキュリティセンターが提唱した新しい高度サイバーセキュリティ人材像であり、国が率先して育成に取り組んでいます。

戦略マネジメント層は、

1.サイバー脅威に対する企業・組織のリスクマネジメント、インシデント対応及び事業継続力の充実
2.知的財産権の戦略的活用と相俟って、戦略的な知財・ノウハウ秘匿（情報漏えい防止）のガバナンス構築
3.急速に対応が進み始めた、経済安全保障への組織的対応　等

を推進します。

本コースが育成を目指すのは、戦略マネジメント層の人材です。

サイバーセキュリティ経営戦略コース
～コーディネーターが期待する受講者像～

サイバーセキュリティの経験が豊富でさらに知見を深めたい方に加えて、**経営企画部門のセキュリティ企画担当、知財部門の知財保護担当で情報漏えい対策に関心がある方、事業部門でサイバーセキュリティ対策を担う方などに受講していただきたい**と考えています。

（コーディネータが期待する受講生像）

- サイバーセキュリティ経営の導入・促進に取り組む（取り組みたい）経営企画部門等の方
- CISOまたはその補佐役（戦略マネジメント層）の即戦力を目指す方
- 情報システム/セキュリティ部門の一担当者から、企業・組織のサイバーセキュリティ経営を担う戦略的人材へのステップアップを目指す方
- 事業部門の事業経営／事業戦略に、サイバーセキュリティ経営の手法を取り入れたい方
- その他、サイバーセキュリティ経営のエッセンスを体系的に学びたい方等

サイバーセキュリティ経営戦略コース
特徴

- 充実の講師陣：我が国をリードする産官学の実務経験豊富な外部講師陣が講義を担当
- サイバーセキュリティ経営のエッセンスを体系的にカバーする希少なカリキュラム
- 座学だけでなく、受講生同士による議論やワークショップによって理解を深める実践的な講義スタイル
- 演習形式の講義も行うことで、「何を」だけでなく「どうやって」まで学べる機会を提供

サイバーセキュリティ経営戦略コース
学ぶ内容

前半の展開：サイバーセキュリティ経営の全貌を知り、土地勘を養う

- めざすべきアウトカム
- 企業価値を向上させるには
- 経営層との関わり方
- 経営戦略としての思考法
- リスクマネジメントのポイント
- 関連法令

ワークショップ1：実際の事件における危機的経験に基づく「危機管理のポイント」のディスカッション

後半の展開：サイバーセキュリティ経営戦略の実践に資する専門的知識を学ぶ

- 国家が関与するサイバー攻撃のインパクト
- サプライチェーンセキュリティと経済安全保障
- コミュニケーションの重要性

ワークショップ2：実際の事件における組織的対応の失敗経験に基づく「サイバーセキュリティ経営のポイント」のディスカッション
机上演習　サイバー攻撃リスクの特定と望ましい対応のシミュレーション

サイバーセキュリティ経営戦略
カリキュラムとスケジュール

木曜19～21時　開催@Zoomオンライン講義

月曜開催で、Zoomでのオンライン受講の方法やグループ課題の進め方等を説明

回	日程	科目	担当	所属・役職等
–	1/13（月）	受講ガイダンス、グループ課題説明	古俣升雄 三笠武則	東京工業大学 環境・社会理工学院 株式会社 NTT データ経営研究所
1	11/16	サイバーセキュリティ経営の導入・目指すべきアウトカム	三角育生	東海大学情報通信学部長 教授
2	11/30	サイバーセキュリティを通じた企業価値向上のポイント	梶浦敏範	日本サイバーセキュリティ・イノベーション委員会代表理事
3	12/7	経営層と戦略マネジメント層の望ましい関わり	外村慶	PwC Japan, Chief Security and Trust Officer, Chief Data Officer
4	12/14	企業のDX戦略から学ぶサイバーセキュリティ戦略の着眼点	三谷慶一郎	株式会社 NTT データ経営研究所 執行役員 エグゼクティブ・コンサルタント
5	12/21	サイバーセキュリティにおけるリスクマネジメントのポイント	野口和彦	NPO 法人リスク共生社会推進センター理事長
6	1/11	サイバーセキュリティの関連法令	蔦大輔	森・濱田松本法律事務所　弁護士
7	1/18	ワークショップ1：WannaCry事件に基づくディスカッション	村山厚	株式会社日立製作所 情報セキュリティリスク統括本部 情報セキュリティ戦略企画本部 本部長
–	1/25	グループ課題中間発表	コース担当教員・コースコーディネータ	
8	2/1	国際政治はサイバー攻撃能力をどう変えたか	小宮山功一朗	JPCERT/CC 国際部部長
9	2/8	サプライチェーンのセキュリティと経済安全保障	石原修	株式会社日立製作所セキュリティ事業統括本部セキュリティイノベーション推進本部長
10	2/15	サイバーセキュリティ経営におけるコミュニケーションの重要性	鎌田敬介	金融 ISAC　専務理事 / 株式会社 Armoris 取締役専務
11	2/22	ワークショップ2：日本年金機構の事件に基づくディスカッション	三角育生	東海大学情報通信学部長 教授
12	2/29	机上演習：事業経営の観点から、サイバーセキュリティリスクの特定と対応戦略をシミュレーションしてみよう！	大野博堂	株式会社 NTT データ経営研究所パートナー金融政策コンサルティングユニット長
13	3/9（土）	特別講義	調整中	※受講生のご希望に従って講義内容／講師をアレンジ
14		グループ課題最終発表	コース担当教員・コースコーディネータ	

土曜開催で、特別講義とグループ課題発表

サイバーセキュリティ経営戦略コース

講義スタイル　～3つの育成手法～

① レクチャー＆ディスカッション
② ワークショップ・演習形式
③ グループ課題発表

受講生5名前後が一組になり、コース期間（約5ヶ月間）でグループ課題に取り組んでいただきます。テーマは、サイバーセキュリティに関連する企業、団体等の課題などを想定しています。

・1月25日（木）にグループ課題の中間発表とフォロー
・3月9日（土）にグループ課題最終成果発表会
※グループ課題の取組みについては、講義直後（21時～）及び講義日以外に、**任意参加の**グループ活動が発生します。

2021年度のグループ課題の例

※2023年度はテーマや設定を変更する場合があります

【ケース】

1．大手インフラサービス企業が二重脅迫型ランサムウェアの攻撃を受け、重要データ窃取後に暗号化が行われ、多額の身代金を支払わなければ盗み出されたデータを公開すると脅迫を受けました。CISOを補佐する立場として、CISOにどのような進言をするかを、対象とする局面・対応段階を選んでまとめてください。

参考例：2021年5月に米国の大手石油パイプライン企業が「DarkSide」と呼ばれるランサムウェア／犯罪グループから二重脅迫型ランサムウェアの攻撃を受けて数日間操業停止に追い込まれた件

2．大手交通機関への風評被害を狙った悪意の投稿が行われ、その中には、チケット予約サービス利用者の個人情報を大量に窃取したという脅しと、それと思われる情報の一部が含まれていました。現時点で、どのような攻撃を受けたかはまだ分かりません。CISOを補佐する立場として、CISOにどのような進言をするかを、対象とする局面・対応段階を選んでまとめてください。

【中間報告での報告内容】

それまでに受けた授業の内容を踏まえて、次の点を整理して発表してください。中間報告ですので、十分に練られていなくても大丈夫です。

◆対象企業の設定と理由
◆グループ内でのメンバー間の役割分担
◆重大危機に対し、必要な緊急対応を列挙し、これに優先順位を付けること
◆どのような法令が関係するかを調べること
◆社内・社外のステークホルダーを列挙すること
◆最終報告に向けての今後の検討方針

2022年度のグループ課題の例

※2023年度はテーマや設定を変更する場合があります

【ケース】

【ケース1】食品製造大手企業がサイバー攻撃により本体だけでなくグループ企業も利用しているシステムが暗号化の被害を受けた。オンラインバックアップも被害に遭い、システム障害のBCPを策定していたが機能せず、サーバーの早期復旧が困難。決算報告にも影響しそうである。CISOを補佐する立場として、CISOにどのような進言をするかをまとめてください。

【ケース2】モバイル通信キャリアが、スマートフォンを活用して前払い式口座を開設し、銀行口座と連携させることで、オンライン決済や口座からの入出金、ユーザー間での送金ができるサービスを開始したところ、不正な前払い口座を開設して他人の銀行口座と紐付け、不正にオンライン決済を行なったり、銀行預金を勝手に引き下ろしてマネーロンダリング等に悪用したりする事件が多数発生していることが発覚しました。また、ダークウェブで売買されている漏洩した被害者の個人情報がこの不正に悪用されていることもわかりました。次の2つのタイミングで、経営層やCISOにどのような進言をするかを取りまとめてください。

① 事件が発覚し、詳しい調査に着手する段階
② 調査が終了し、問題となった前払い口座サービスの継続可否を決定する段階

東工大キャリアアップMOTプログラム
サイバーセキュリティ経営戦略コース
（2023年度） 説明会（後半）

2023年＠Zoom収録によるweb配信

（後半） CUMOT担当　古俣

〇CUMOTとは

〇受講形態（Zoomによるオンライン受講）

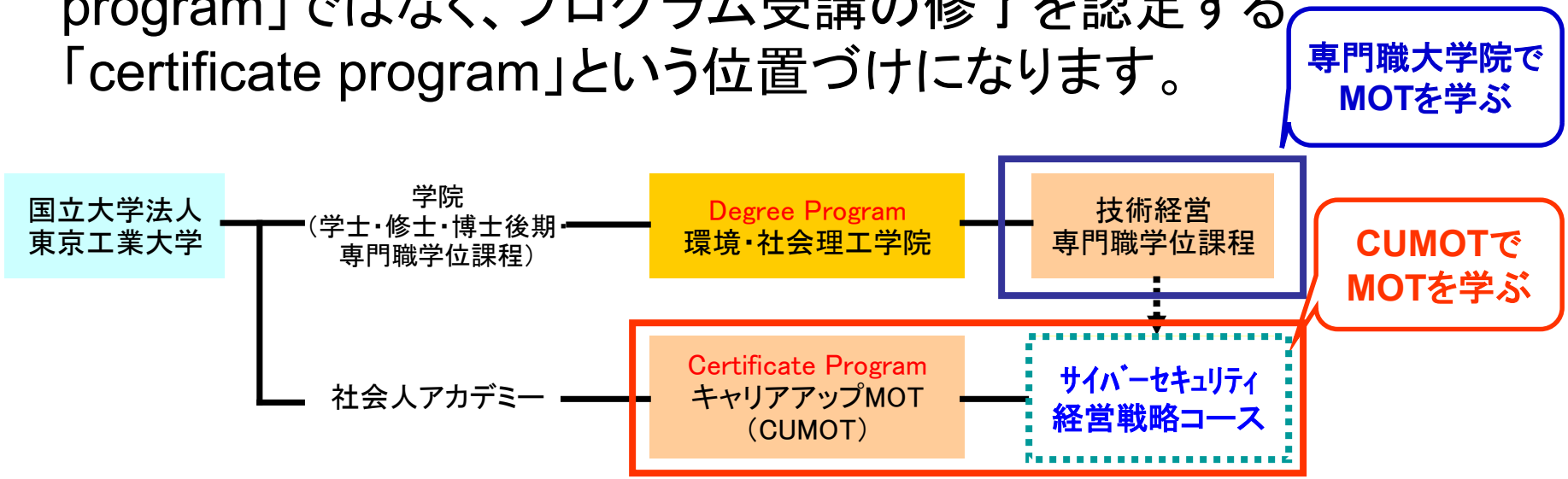
〇実施概要/募集要項

〇受講実績と受講イメージ　ご紹介

〇FAQ／アンケートのお願い

キャリアアップMOTとは？

CUMOT(キューモット)は、“Career Up　MOT”の略称です。社会人の方が働きながらMOT（ Management of Technology：技術経営）の学びを通じて、キャリアアップを図ることを支援します。
本学の「社会人アカデミー」のプログラムの1つとして位置付けられ、環境・社会理工学院（技術経営専門職学位課程）が事業主体となり実施しております。学位等を認定する「degree program」ではなく、プログラム受講の修了を認定する「certificate program」という位置づけになります。



受講形態

・Zoomを使ったオンライン配信での受講形態で開講します（オンライン講義の受講に必要な通信環境は受講者にてご用意いただきます）

・Zoomを使って受講（視聴）いただきますが、欠席や通信状況の不具合などオンラインでの視聴環境が整わなかった方には、録画をして補講用のeラーニングをご用意する予定です（録画について講師の了解を得た場合に限ります）

→講師の了解を得た場合、振り返り用にレコーディング動画を期間限定（1週間等）で共有する場合があります

・グループ課題の取り組みは、後述のGMSSを活用していただきます

・講義資料はPDFデータで配布予定です

・Zoomでの視聴方法については、別途、事務局から事前にご案内します

サイバーセキュリティ経営戦略コース
募集要項

受講期間

2023年11月13日～2024年3月9日　毎週木曜19時~21時開催（全14回）
※受講ガイダンス（11/13）は月曜（19~21時）、特別講義/グループ課題最終発表会（3/9）は土曜日に実施します（13時30分開始予定）

受講対象者

サイバーセキュリティ経営の企画、サイバーセキュリティ経営の主力としての活動、現場の情報システム/セキュリティ担当からのステップアップ、事業部の経営戦略へのサイバーセキュリティ経営の取り込み等に取り組む方、など。

受講場所

Zoomを用いたオンライン受講です。
※オンライン講義の受講に必要な通信環境は受講者にてご用意ください

募集人数

24名　（＊最小開催人数12名）

受講料

198,000円（消費税込）
※お支払方法はお振込みにて受講前に手続きについてご案内します（10月下旬予定）。お振込み後の受講料の返還はいたしませんので、ご了承ください

申込期間

2023年8月1日（火）～2023年10月6日（金）（締切日必着）
※定員に達し次第、応募は締め切りますのでご注意ください。
※企業派遣など上記期間での対応が難しい場合はメールまたはお問い合わせフォームよりご相談ください。

申込方法

願書に必要事項をご記入のうえ、下記の住所までお送りください（締切日必着）。※PDFファイル等、電子ファイルでのご提出も受け付けます（cumot-info@mot.titech.ac.jp）。メールの送受信をもって押印・署名扱いとさせていただきます。
申込用紙は専用webサイトからダウンロードできます。
〒108-0023　東京都港区芝浦3-3-6　CIC910　CUMOT事務局
サイバーセキュリティ経営戦略コース　受講申込担当

受講審査・受講通知

願書をお送りいただいた後、志望理由書等にもとづく書類審査をいたします（申込順審査）。受講通知についてはメールにてご連絡いたします（受講許可の案内を通知）。
専用 Web サイト：https://www.academy.titech.ac.jp/cumot/cy

お問い合わせ

東京工業大学　CUMOT事務局
問い合わせ先E-mail：cumot-info@mot.titech.ac.jp
※受講についてお問合せがある場合は、メール等にて個別相談にも応じます。

サイバーセキュリティ経営戦略コース
受講実績と受講イメージ　ご紹介

- シラバス（例）
- 教材レジュメ
- 受講生の声
- Zoomによる遠隔受講
- 学習支援システム（GMSS）

シラバス

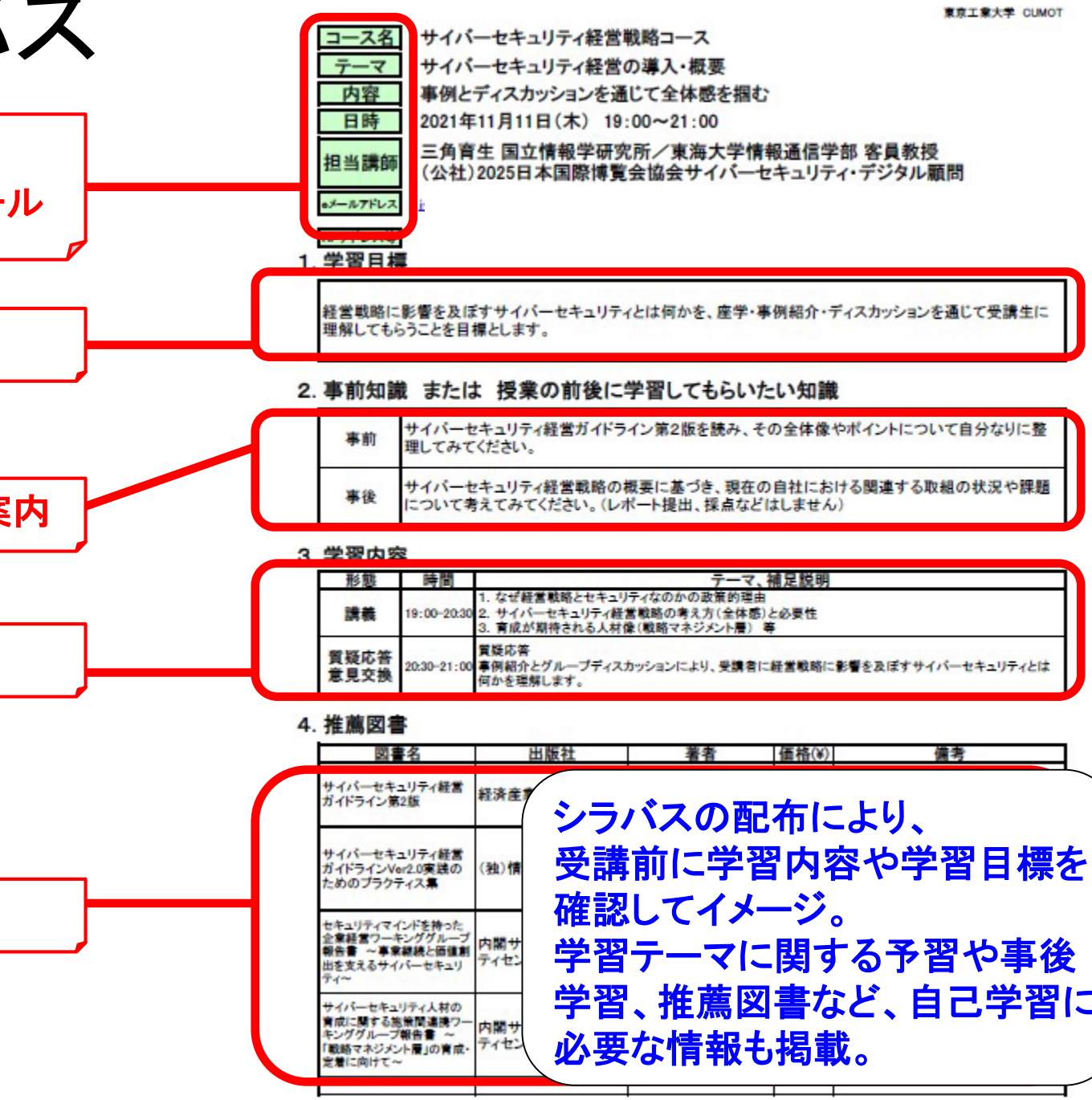
科目名と
担当講師プロフィール

学習目標

事前・事後の学習案内

学習内容の詳細

推薦図書



東京工業大学 CLMOT

コース名	サイバーセキュリティ経営戦略コース
テーマ	サイバーセキュリティ経営の導入・概要
内容	事例とディスカッションを通じて全体感を掴む
日時	2021年11月11日(木) 19:00～21:00
担当講師	三角育生 国立情報学研究所／東海大学情報通信学部 客員教授 (公社)2025日本国際博覧会協会サイバーセキュリティ・デジタル顧問
eメールアドレス	

1. 学習目標

経営戦略に影響を及ぼすサイバーセキュリティとは何かを、座学・事例紹介・ディスカッションを通じて受講生に理解してもらうことを目標とします。

2. 事前知識 または 授業の前後に学習してもらいたい知識

事前	サイバーセキュリティ経営ガイドライン第2版を読み、その全体像やポイントについて自分なりに整理してみてください。
事後	サイバーセキュリティ経営戦略の概要に基づき、現在の自社における関連する取組の状況や課題について考えてみてください。(レポート提出、採点などはしません)

3. 学習内容

形態	時間	テーマ、補足説明
講義	19:00-20:30	1. なぜ経営戦略とセキュリティなのかの政策的理由 2. サイバーセキュリティ経営戦略の考え方(全体感)と必要性 3. 育成が期待される人材像(戦略マネジメント層) 等
質疑応答 意見交換	20:30-21:00	質疑応答 事例紹介とグループディスカッションにより、受講者に経営戦略に影響を及ぼすサイバーセキュリティとは何かを理解します。

4. 推薦図書

図書名	出版社	著者	価格(¥)	備考
サイバーセキュリティ経営ガイドライン第2版	経済産			
サイバーセキュリティ経営ガイドラインVer2.0実践のためのプラクティス集	(独)情			
セキュリティマインドを持った企業経営ワーキンググループ報告書 ～事業継続と価値創出を支えるサイバーセキュリティ～	内閣サティセン			
サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ報告書 ～「戦略マネジメント層」の育成・定着に向けて～	内閣サティセン			

シラバスの配布により、
受講前に学習内容や学習目標を確認してイメージ。
学習テーマに関する予習や事後学習、推薦図書など、自己学習に必要な情報も掲載。

教材・レジュメ

教材例

PDFファイルにて事前に資料を配布

サイバーセキュリティ経営に関する豊富な実務経験と理論にもとづくプレゼン資料を配布

受講生の評価

プログラム受講者へのアンケート

※5段階評価　平均

【受講満足度】

Q 「サイバーセキュリティ経営戦略コース」授業の総合的な満足度は？

⇒平均4.6（非常に満足5⇔1満足していない）

【授業内容の評価】

Q 授業で学んだことが今後自分の業務に役立つと考えますか？

⇒平均4.8（非常に役立つだろうと考えている 5⇔1役立たないだろうと考えている ）

Q サイバーセキュリティ経営戦略コースの受講を知り合いにも勧めたいと思いますか

⇒平均4.7（そう思う5⇔1そう思わない） 全ての受講生が肯定的（そう思う、どちらかといえばそう思う）

【過去の参加者の所属先の例】

株式会社日本総合研究所、東日本電信電話株式会社、日本放送協会、株式会社サイバーディフェンス研究所、沖電気工業株式会社、株式会社JSOL、株式会社NTTデータ経営研究所、日本電気株式会社、三菱電機株式会社、株式会社ジュピターテレコム、第一三共株式会社、株式会社デンソー、防衛省、社団法人共同通信社、公益財団法人　金融情報システムセンター、株式会社肥後銀行、等

受講生の声　その1

【受講者の声】

●サイバーセキュリティは危機管理の一環であり、危機管理全般に通じて言えることだが、経営層の意識改革が最も重要だと改めて感じた。CIOなど専門領域も理解しながらも経営全般にどう寄与できるかという経営層としての意識も持った人材を育てることが急務だと思われる。日本の現状を見ると、IT化、国際化が進んでいるのに、経営層にサイバーに関する危機管理意識が不十分な人が多いように思われる。経営層の人材育成が伴わないと実効は上がらない。その意味でサイバーセキュリティの意識を持った経営層を育てる本コースの意義は重要だと思う。今後の発展を期待している。

●DXやデータドリブン経営が叫ばれる中、ITへの依存度が飛躍的にあがることで、サイバーセキュリティに対する企業の姿勢が経営課題に直結することが理解できた。企業がサイバーセキュリティに対応するためには、現場と経営層の意向を整理し、さらなる企業価値向上を推進できるバイプレイヤーの存在が不可欠であることを学んだ。

●経営者目線、現場目線とは違ったリスクへの関心・判断を学べた。

受講生の声　その2

【受講者の声】

●講義の中で、講師の先生のご苦労された点等も垣間みれ、貴重なお話を沢山聞くことができ、現在の仕事はもちろん、今後のキャリアの方向性を考えるうえで大変参考になりました。後半の机上訓練の講義は実践的で良かったです。さらに多くのケーススタディによる様々なシチュエーションを擬似的に体験することができると受講生の学びが実践へと結びつくように思いました。

●当初期待していた通り、体系立ててサイバーセキュリティについて学習することができました。

●サイバーセキュリティはIT部門だけの問題ではなく、経営課題であり、経営層がリーダーシップを発揮して、スピーディーに意思決定していく必要があることを学んだ。経営判断の材料となる情報を経営層へ適切なタイミングでエスカレーションするのが戦略層の重要な役割となる。そのためには事業部門や経営層との日頃からのコミュニケーションが重要であり、組織の中で自分の味方になってくれる人を見つけ、セキュリティ対策・維持を円滑に推進していく必要があると思った。

Zoomによる遠隔受講

➢ 遠隔（Zoom）受講ガイド

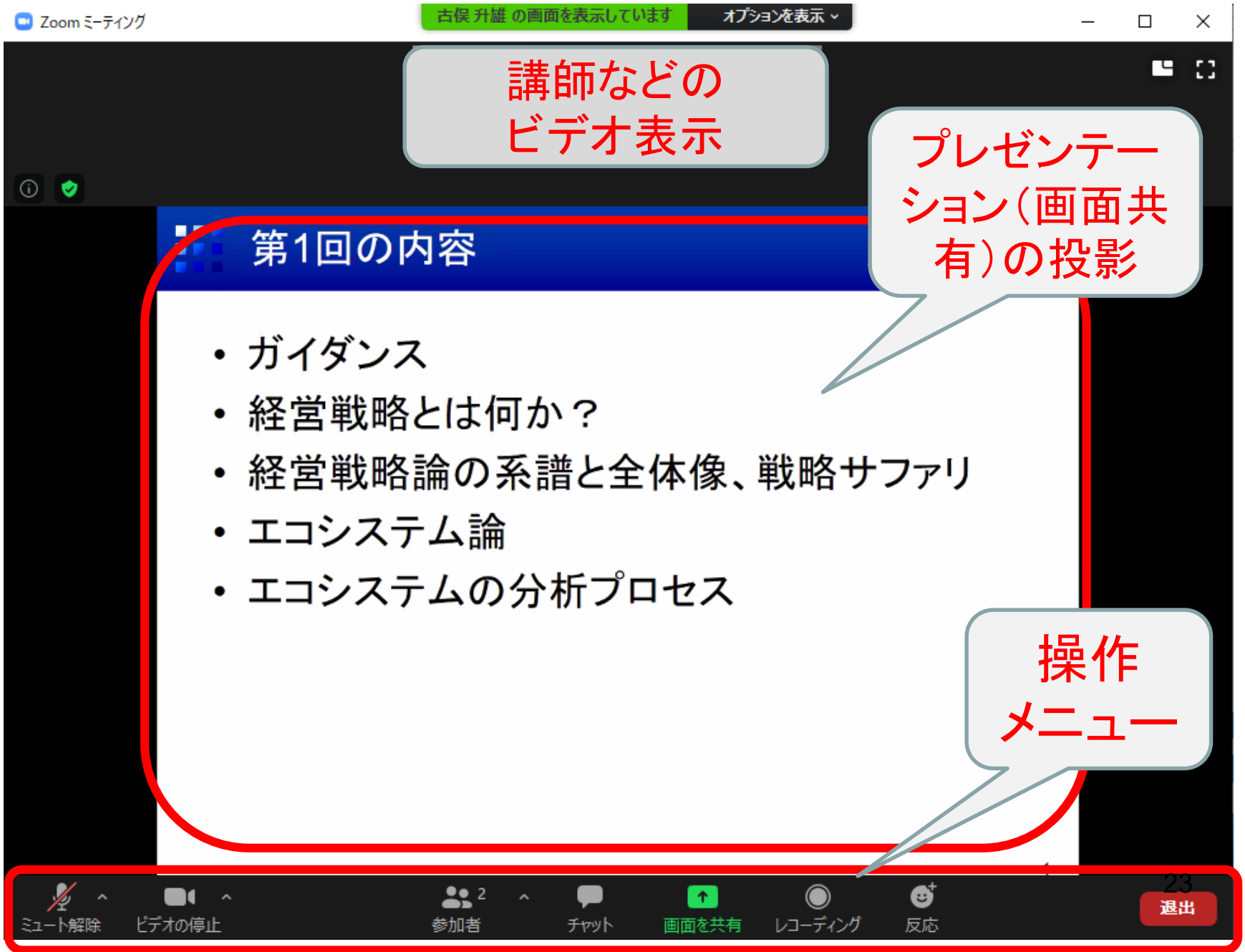
・Zoomでの受講にあたって必要な環境、操作方法、受講時の基本仕様、グループディスカッションの方法、など運用に関するガイドを事前に配布します。受講ガイダンスでは実際にお試しで操作や簡単な演習もします。

➢ Zoomについて

インターネット環境（+マイク、ビデオ）があれば受講ができます。CUMOTの講義は一方向のセミナーと違い、受講生が主体的に学んでいただく学習形態（クラスディスカッション）ですので、発言のために「マイク」のご用意（ノートパソコンやタブレット等であれば備え付けのもので十分）を推奨します。

➢ 通信環境の不具合について

本プログラムでは、通信環境の不具合や欠席時のフォロー用に独自の動画配信システム（後述）でフォローをします。


Zoom ミーティング
古俣 升雄 の画面を表示しています
オプションを表示
講師などの
ビデオ表示
プレゼンテーション（画面共有）の投影
第1回の内容
• ガイダンス
• 経営戦略とは何か？
• 経営戦略論の系譜と全体像、戦略サファリ
• エコシステム論
• エコシステムの分析プロセス
操作
メニュー
ミュート解除
ビデオの停止
参加者
2
チャット
画面を共有
レコーディング
反応
退出

学習支援システム（GMSS）の導入

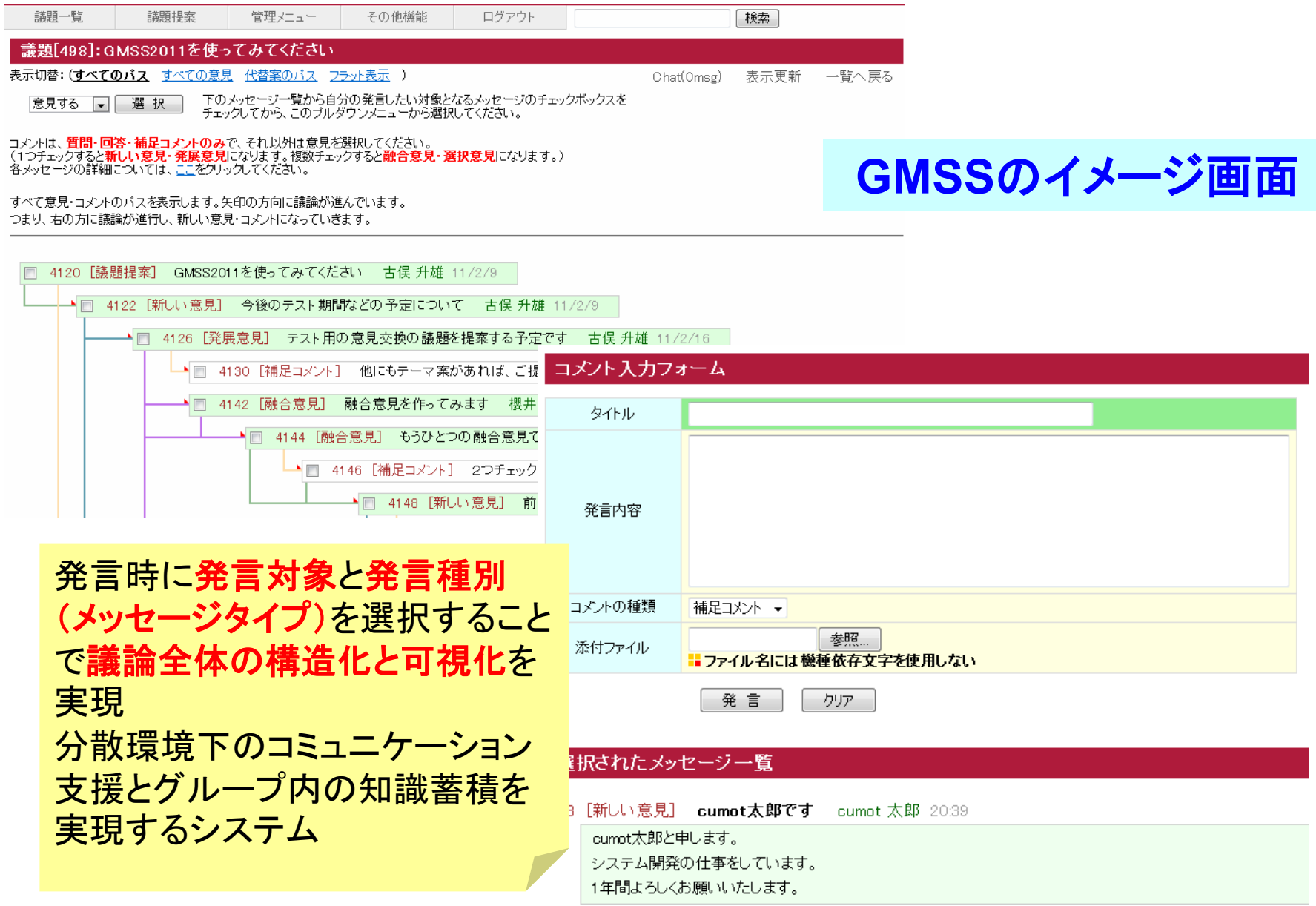
プログラムに参加する社会人の学習環境

- ■異なる企業に属する
- ■勤務先や住居の場所も異なる
- ■顔をあわせた議論の場は週に1度の講義の日のみ
- ■発表などグループワークの課題がある
- ■時間を合わせてグループワークを行うには制約がある
- ■講義終了後の対応では時間も限られる

→ **グループ内で意見交換やコミュニケーションを行う機会が少ないと、グループワークによる学習効果も期待できない**

Web上でディスカッションや意見交換ができる GMSS(ｸﾞﾙｰﾌﾟﾒﾓﾘｰｻﾎﾟｰﾄｼｽﾃﾑ)を導入し、学習利便性を向上

GMSSのイメージ画面



発言時に**発言対象**と**発言種別(メッセージタイプ)**を選択することで**議論全体の構造化と可視化**を実現

分散環境下のコミュニケーション支援とグループ内の知識蓄積を実現するシステム

【補講用eラーニング】
講師の了解をいただいた科目/学習テーマにおいては、欠席者用にwebでみられる補講用のeラーニングをご用意しています。

よくある質問①

◆セキュリティの担当ではないが、自分は受講対象者なのか？

対象領域についてですが、セキュリティをどのようにとらえて考えるか、がポイントになると思います。webサイトにある「このような方に受講をお勧めします」でご紹介しておりますとおり、部門担当者でなくても、経営やマネジメントの視点からセキュリティを戦略的に取り組む必要がある方など、対象領域は広くとらえていただいて大丈夫です。

◆サイバーセキュリティについて初学ですが、どの程度の事前知識が必要か？

サイバーセキュリティと経営戦略のかかわり（マネジメント）を学ぶコースですので、高度なセキュリティーの知識や技術は必要ありません。学習経験が無い方でも、これから当該分野を担う可能性がある方なども受講対象となっています。一方で、インターネット、ITシステム、LANなどについての概念的な理解を、ある程度お持ちである方が良いです。また、サイバー脅威との関わりはなくても、事業リスク管理・事業継続等についての業務経験・知識をお持ちであれば、受講に大いに役立つはずです。
本コースでは学習経験が無い方は、事前に資料や参考文献などで予習し、講義で学んだことをしっかりと復習していただき、グループディスカッションやグループ課題、実務を通じてアウトプットしていただくことで、学んだことを習得いただけると思います。

よくある質問②

◆学割等はあるか？

CUMOTは公開講座にあたるため、受講者の身分は学生ではありません。
そのため学割はありません。

◆受講前に、事前に必要な知識はあるのか？

学習テーマによっては、事前にケース教材や本を読んでいてくださいというものもあります。ただ、事前に知識を増やすよりも、その場でしっかり学習して受講後にも学習を継続していただきたいと考えています。

◆サイバーセキュリティ経営戦略コース以外について教えてください（2023　実績・予定）。

エッセンシャルMOTコース（1年コース、4月～翌年2月）
エッセンシャルMOT夏季集中（4ヶ月コース、6～9月）
エッセンシャルMOT秋季（半年コース、10月～翌年3月）
知的財産戦略コース（5ヶ月コース、5～9月）
標準化戦略実践コース（5ヶ月コース、5～9月）
CUMOT×STAMP連携プログラム（4ヶ月コース、11～2月）
サービスイノベーション集中（1ヶ月、2～3月）

よくある質問③

◆個人で会社をやっているが、受講しても大丈夫か？

大丈夫です。いままでの受講生にもいらっしゃいます。

◆志望理由書で選考するのか？

ご経歴や志望動機に基づいて、プログラムの趣旨とあっているかを審査させていただきます。審査は落とすためのものではなく、あくまでもプログラムの趣旨との整合があるかを確認するために、ご提出いただいております。

◆年齢制限はないのか？

同コースにおいては、受講対象として年齢制限は設けておりません。
志望理由とプログラムの趣旨が一致していれば問題ございません。

◆出張などで講義に出席できないとき、eラーニングなどで講義内容を補完するものがあるか？

Zoomでのオンライン講義形式の場合、講師の了解を得た実施回については後日、
CUMOT専用の動画配信システムで欠席者フォロー用のeラーニングをご案内します。

最後までご視聴いただき、ありがとうございました。ご質問等がありましたら、eメールまたはお問い合わせフォームよりご連絡ください。

【Mail】 cumot-info@mot.titech.ac.jp

【問い合わせフォーム】

https://www.academy.titech.ac.jp/cumot/faq_index.html