

一般社員向けセキュリティ教育コンテンツご紹介

情報セキュリティの基礎からサイバー脅威対策まで
組織の教育課題に対応するeラーニング研修

株式会社ラック
セキュリティアカデミー



Agenda

1. サービス概要
2. 各コース詳細
3. お問い合わせ・トライアル

セキュリティ教育の課題と、ラックだからできる解決

多くの組織が抱える課題

教育を
やりっぱなし
になっている

最新脅威に
追いつけない

組織全体に
浸透しない



セキュリティ担当者

リソース不足で
十分に手が回らない…



ラックのeラーニングで解決

- ✓ 現場での知見をもとに、実務に活かせる理解を促進
- ✓ 最新の脅威・攻撃動向に対応した実践的なコンテンツ
- ✓ 管理機能により組織全体の受講状況・理解度を可視化



セキュリティサービスで培った知見
を教育に還元

ラックセキュリティアカデミーのeラーニングの特長



短時間で無理なく受講可能



新入社員から管理職まで
体系的にカバー



理解度テストで定着を支援



管理者による進捗・結果の
一元管理

「知識」だけでなく、「対応できる人材」の育成を支援します

目的別に選べるコースラインナップ

ニーズやレベルに応じて体系的にコースをご用意しています

基礎教育 P.6

- ロボタと挑戦！セキュリティチャレンジ【日常編】
- 情報セキュリティ講座【社員の意識編】
- 情報セキュリティ講座【テレワーク編】

新入社員向け P.10

- 新入社員向け 情報セキュリティ研修

管理職向け P.11

- 管理職向け 情報セキュリティ講座

サイバー脅威対策 P.12

- 情報セキュリティ講座【サイバー攻撃編】
- 情報セキュリティ研修【標的型攻撃メール対策編】
- サポート詐欺の実態
- 「だます技術」～増加する金融犯罪・詐欺から身を守る～

応用・セキュリティ強化 P.16

- インシデントレスポンス概論
- プラス・セキュリティ人材育成講座
セキュリティの基礎

教育課題別おすすめコース

- 全社員向けの年次教育を実施したい

情報セキュリティ講座【社員の意識編】
- 流行りのランサムウェアを学ばせたい

情報セキュリティ講座【サイバー攻撃編】
- 万が一に備え事故対応を学びたい

インシデントレスポンス概論

目的・課題に応じて、最適なコースをお選びいただけます

価格

1コース **110,000円**(税込) / 50名まで
※50名を超える場合、1名追加につき2,200円

受講期間

30日間

視聴時間

約**10～60分**
※コースにより異なります

Agenda

1. サービス概要
- 2. 各コース詳細**
3. お問い合わせ・トライアル

ロボタと挑戦！セキュリティチャレンジ【日常編】(1)

日常業務で起こりがちなセキュリティリスクを題材に、基本的な対策を楽しく身につけます

コースの特長

- ✓ パスワード管理や情報管理など、身近なテーマを学べる
- ✓ テーマごとにシーンとアンケートによる回答、解説を組み合わせた構成

主なコース内容

- パスワード管理
- 情報管理
- PCの安全管理
- 不審なメールにご用心
- もしもの時の対応



おすすめの対象者



全社員

視聴時間



約60分

ロボタと挑戦！セキュリティチャレンジ【日常編】(2)

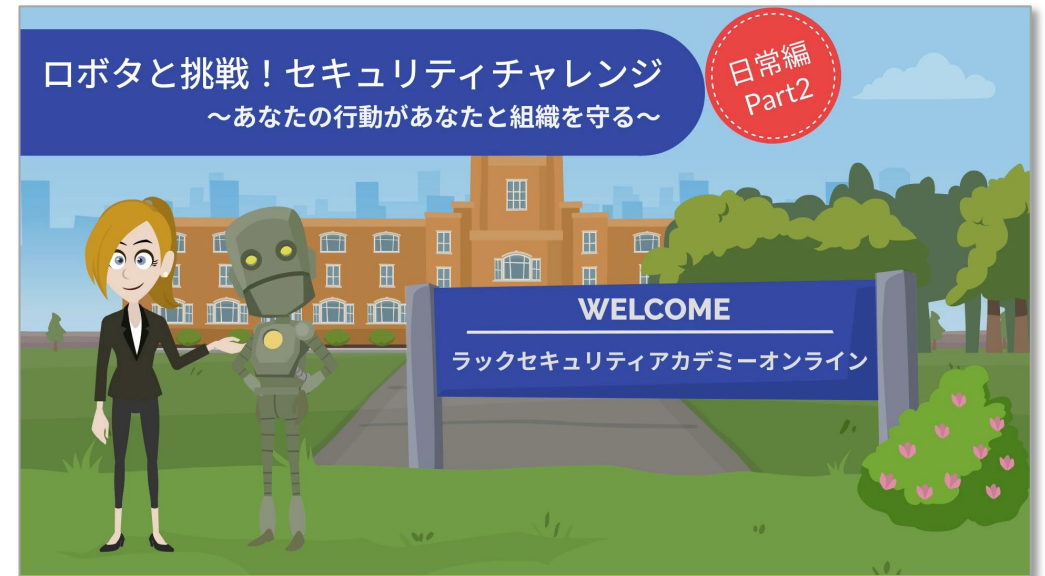
SNSやクラウド利用など、見落としがちなりスクに気づき、適切な対応方法を学びます

コースの特長

- ✓ 業務とプライベートにまたがる利用シーンを扱う
- ✓ 具体的なケースをもとに判断のポイントを紹介

主なコース内容

- 社外での言動・行動に注意
- SNSの利用
- クラウドサービスの利用
- もしもの時の対応



おすすめの対象者



全社員

視聴時間



約45分

情報セキュリティ講座【社員の意識編】

セキュリティルールの必要性を理解し、組織の一員として適切に行動できる意識を醸成します

コースの特長

- ✓ セキュリティの基本的な考え方やルールを整理
- ✓ 身近なリスクを自分ごととして捉え直すことができる

主なコース内容

- 情報セキュリティとは
- 情報の価値と性質
- 主な人的リスク
- ビジネスメール詐欺による金銭被害
- 不注意による情報漏えい等の被害
- 身近に起こる脅威と対策
- セキュリティ事故に遭遇した際の報告手順

情報セキュリティ講座

おすすめの対象者



全社員

視聴時間



約20分

情報セキュリティ研修【テレワーク編】

テレワーク環境におけるリスクを理解し、安全に業務を行うための対策を学びます

コースの特長

✓ 端末やネットワーク利用時の注意点を解説

✓ アニメ形式で継続的に学習しやすい

主なコース内容

- 持ち出す情報の注意
- 持ち出し端末のセキュリティ対策
- 仕事をする場所や環境に注意
- 無線LAN利用時の注意
- クラウドサービス利用の注意
- 偽メールに注意
- もしもの時に備えて



おすすめの対象者



全社員

視聴時間





約40分

新入社員向け 情報セキュリティ研修

新入社員が陥りやすい事故事例をもとに、社会人として必要なセキュリティ基礎を習得します

コースの特長

- 
社会人として必要なセキュリティ基礎を体系的に習得
- 
事故事例からミス傾向を理解し、適切な行動への意識を高める

主なコース内容

- 情報セキュリティとは
- 情報の取り扱い
- アカウント管理
- インターネットの利用
- SNSの利用
- 電子メールの利用 (送信・受信時)
- もしもの時に備えて



The screenshot shows a presentation slide with the LAC logo and tagline 'LAC supports your Business' at the top. Below the logo, it lists services: CYBER - EDUCATION - PENTEST - JSOC - 119 - CONSULTING. The main title of the slide is '新入社員向け 情報セキュリティ研修'. At the bottom right, there is a logo for 'LAC Security Academy' with the tagline 'ともに、イキル'.

おすすめの対象者



**新入社員
初学者**

視聴時間





約40分




管理職向け 情報セキュリティ講座(1)

管理職として求められる役割を理解し、セキュリティ推進に必要な考え方を学びます

コースの特長

- 
管理職としての役割や責任を整理
- 
やるべきことや注意点を具体的に解説

主なコース内容

- 
 管理職・リーダーが
「知っておくべきこと」
- 
 管理職・リーダーが
「やるべきこと」
- 
 管理職・リーダーが
「やってはいけないこと」

LAC
 supports your Business
 CYBER - EDUCATION - PENTEST - JSOC - IIR - CONSULTING



管理職向けセキュリティ講座 1

「管理職・リーダーに求められる役割」編

組織において、管理職や現場のリーダーに求められる役割について、解説します。



おすすめの対象者



管理職

視聴時間



約25分

情報セキュリティ講座【サイバー攻撃編】

最新のサイバー攻撃の手口を理解し、被害を防ぐための基礎知識を学びます

コースの特長

- ✓ ランサムウェアやフィッシングなど主要な攻撃を解説
- ✓ 攻撃の理解 + 対応のポイントを紹介

主なコース内容

- What's IPA?
- サプライチェーン攻撃
- ランサムウェア攻撃
- フィッシング
- 報告手順
- 報告のポイント
- 報告の注意点



おすすめの対象者



全社員

視聴時間





約20分

情報セキュリティ研修【標的型攻撃メール対策編】

巧妙化する標的型攻撃メールの見極め方と、被害を防ぐための対応力を習得します

コースの特長

-  よくある攻撃パターンや見極めのポイントを紹介
-  基本的な対策から開封時対応まで一連の行動を習得

主なコース内容

- 標的型攻撃とは
 その他の攻撃の手口
- 標的型攻撃によるウイルス感染の手口
 基本的な対策と開封時の対応
- 標的型攻撃メールの難易度と見極めポイント

LAC supports your Business

CYBER - EDUCATION - PENTEST - JSOC - 119 - CONSULTING

We provide IT total solutions for you.

LAC
ともに、イキル

情報セキュリティ研修

標的型攻撃メール対策 編



LAC Security Academy

おすすめの対象者



全社員

視聴時間



約35分

サポート詐欺の実態

実際の詐欺手口を通じて、被害を防ぐための知識と対応方法を学習します

コースの特長

- ✓ デモ動画によりリアルな詐欺の流れを紹介
- ✓ サポート詐欺を専門とするアナリスト監修のもと、対処方法や注意点を解説

主なコース内容

突然の出会い編

- サポート詐欺デモ動画
- サポート詐欺とは
- サポート詐欺の特徴

安全への第一歩編

- 電話をかけると何が起こる？
- サポート詐欺の被害
- サポート詐欺における重要なポイント



おすすめの対象者



全社員

視聴時間





約10分

「だます技術」～増加する金融犯罪・詐欺から身を守る～

詐欺の仕組みと人がだまされる心理を理解し、「だまされない力」を身につけます

コースの特長

- 
 ラックのFC3が出版した書籍を教材に、実際の事例をもとに手口を解説
- 
 個人のリテラシー向上を通じて組織全体のリスク低減に貢献

主なコース内容

手口編


- 本物と錯覚させる
- 美味しい話で惹きつける
- 話術と仕掛けで信用させる
- 考えられない状況に陥れる


対策編

- メッセージはまず疑う
- オフィシャル情報を確認する
- 電話番号をチェックする
- 「相談は恥」と思わない

金融犯罪対策センター監修
「だます技術」
～増加する金融犯罪・詐欺から身を守る～

手口編





金融犯罪対策センター
FC3 - Financial Crime Control Center

© LAC Co., Ltd.

おすすめの対象者



全社員

視聴時間





約15分

インシデントレスポンス概論

セキュリティ事故発生時に、組織として適切に対応するための基本手順を体系的に学びます

コースの特長

- 
事故発生から復旧までの流れを一貫して理解
- 
CSIRTや外部連携など、実務に必要な観点も学習可能

主なコース内容

- インシデントレスポンス手順書
 原因と被害状況の調査
- CSIRT
 再発防止策の検討と振り返り
- イベントの検知
 インシデントレスポンス対応のポイント
- 被害拡大の防止



おすすめの対象者



全社員
情報セキュリティ
担当者

視聴時間





約60分

プラス・セキュリティ人材育成講座 セキュリティの基礎

DX推進に必要なセキュリティの基本知識を、広く体系的に理解します

コースの特長

- 
暗号や認証、サイバー脅威など技術基礎をコンパクトに整理
- 
ビジネスとセキュリティの関係性を理解できる構成

主なコース内容

- | | |
|---|---|
| <ul style="list-style-type: none"> □ DXとは □ 情報セキュリティの三要素 □ 暗号 □ デジタル証明書 | <ul style="list-style-type: none"> □ 主なマルウェアの種類 □ パスワードクラッキング □ セキュリティ・バイ・デザイン □ 多要素認証の活用 |
|---|---|



おすすめの対象者



**全社員
管理職**

視聴時間



約25分

Agenda

1. サービス概要
2. 各コース詳細
3. お問い合わせ・トライアル

セキュリティ対策を「理解」から「行動」へ



教育を効率化



対応できる人材を育成



行動を組織に定着

無料トライアル実施中

まずは実際のコンテンツをご体験ください



1コースにつき

- ✓ 人数：最大2名
- ✓ 期間：1週間
- ✓ 費用：無料

※人数・期間につきまして、ご要望がございましたらご相談ください

お問い合わせ

トライアル受講やサービスに関するご相談などがございましたら、お気軽にお問い合わせください

お問い合わせフォームはこちら

https://cp.lac.co.jp/lachp/security_education_contact

✉ ola-info@lac.co.jp

YouTubeチャンネル



T3 with セキュリティ教育を含むコンテンツのサンプル動画を公開しています！

[ラックセキュリティアカデミーオンライン](#)

※T3 with セキュリティ教育=メール訓練+eラーニングの教育サービス



※本資料は作成時点の情報に基づいており、記載内容は予告なく変更される場合があります。

※本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。

※本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。

※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。