LAC
ともに、イキル

セキュリティ業務に必要な倫理とその教育

2019年10月24日(木)

株式会社ラック

プロフィール：長谷川　長一

CISSP®

株式会社ラック　サイバー・グリッド・ジャパン　理事
NPO 日本ネットワークセキュリティ協会(JNSA) 教育部会WGリーダー

■ソフトバンク、日本ユニシスを経て、現職。情報セキュリティコンサルティング、情報セキュリティ監査業務を経て、現在は主にセキュリティ教育、組織・人材交流業務を担当。

■主な担当講師業務
- □(ISC)2 CISSPレビュートレーニングセミナー認定主任講師
- □東京電機大学 国際化サイバーセキュリティ学特別コース(CySec) 講師

■最近の主な活動
- □ 総務省 サイバーセキュリティタスクフォース人材育成分科会構成員(2018年度～)
- □ IPA 情報処理安全確保支援士講習統括委員会委員（2017年度～）
- □ 情報危機管理コンテスト 運営スタッフ（2017年度～）

ほか

■主な著書等
「IT現場のセキュリティ対策完全ガイド」（日経BP社）
「情報セキュリティプロフェッショナル教科書」(アスキーメディアワークス、共著）、
「ネットワークセキュリティ」（オーム社、共著）等。

URL : http://www.lac.co.jp/
E-mail : choichi.hasegawa@lac.co.jp　http://www.facebook.com/choichi.hasegawa

株式会社ラック

蛇口をひねれば飲み水が出る当り前を、高度情報社会でも実現します。

株式会社ラックは1986年に設立されました。”Little eArth Corporation”という社名には、ICTの進展で地球が相対的に小さくなっていく中で、ICTを基盤に国や企業の発展を支えていこうという理念がこめられています。JSOC、サイバー・グリッド・ジャパン、サイバー救急センター等の業務をしています。

商　号	株式会社ラック LAC：Little eArth Corporation Co., Ltd.
設　立	1986年(昭和61年)9月
資本金	10億円
代　表	代表取締役社長　　西本　逸郎
従業員数	2,220名（2019年4月1日現在）
売上高	384億円(連結：2018年3月期)
決算期	3月末日
認定資格	経済産業省情報セキュリティ監査企業登録 情報セキュリティマネジメントシステム (ISO/IEC 27001)認証取得(JSOC) プライバシーマーク認定取得

- ✓ http://www.lac.co.jp/
- ✓ sales@lac.co.jp
- ✓ Twitter　@lac_security
- ✓ YouTube　laccotv
- ✓ Facebook　Little.eArth.Corp

・本社
〒102-0093　東京都千代田区平河町 2-16-1
平河町森タワー
03-6757-0111(代表)
03-6757-0113 (営業窓口)

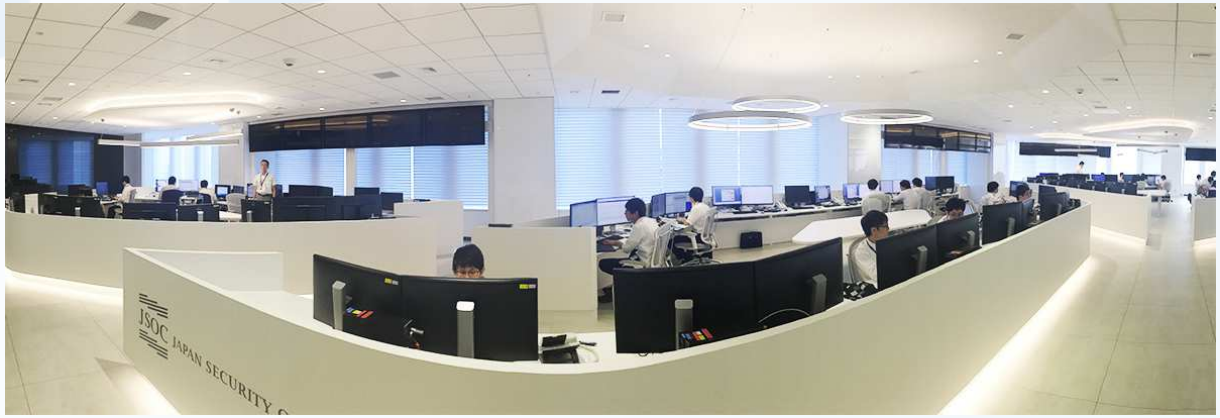
・名古屋オフィス
・福岡オフィス
・アクシス事業所（福島県喜多方市）

・テクノセンター北九州
(2019年4月開設)
・東陽町オフィス
(2019年5月開設)

・シンガポール支店
・韓国ソウル 子会社 CSLAC
Cyber Security LAC Co.,Ltd.

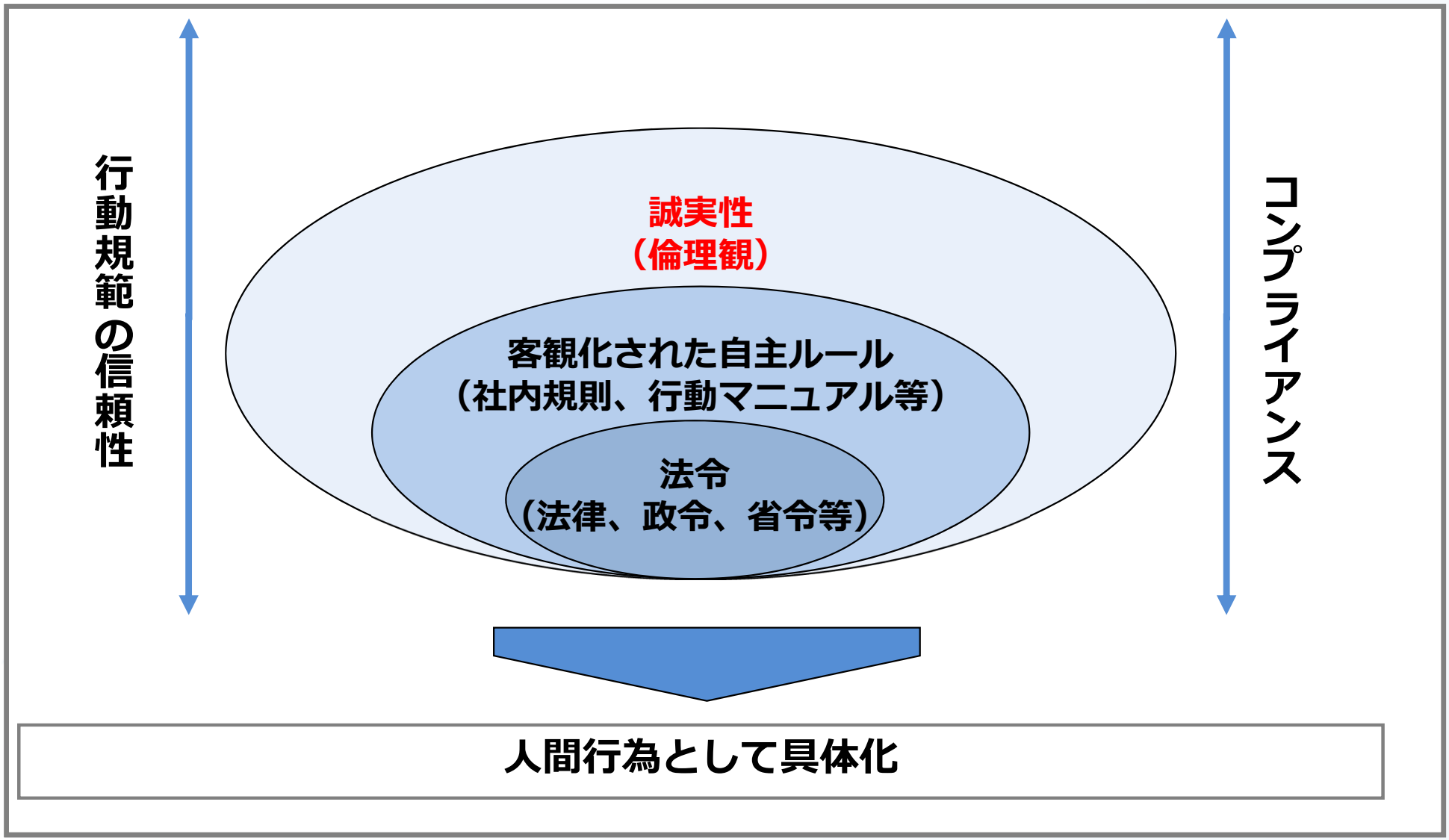
■ JSOC (Japan Security Operation Center)

JSOCは、ラックが運営する情報セキュリティに関するオペレーションセンターです。24時間365日運営。高度な分析官とインシデント対応技術者を配置しています。2000年の九州・沖縄サミットの運用・監視を皮切りに、日本の各分野でのトップ企業など高レベルのセキュリティが要求されるお客様に、高品質なサービスを提供しています。



なぜ「倫理」が必要か

「倫理」と「コンプライアンス」の概念



情報分野で「倫理」が求められる背景

□情報処理技術者を取り巻く環境の変化

・**技術的な環境の変化**：

情報処理技術が**社会的に大きい影響力を持つアプリケーション**を数多く産み出しつつある

・**社会的な環境の変化**：

情報処理技術者は**自己の行動に対する責任を持たなければならない**という考え方が生じてきた

→ **専門家の独善を防ぐ**ことと、自律的な行為規範が必要。

「倫理綱領」～情報処理学会　https://www.ipsj.or.jp/ipsjcode.html

情報処理学会 倫理綱領

1.社会人として
- 1.1　他者の生命、安全、財産を侵害しない。
- 1.2　他者の人格とプライバシーを尊重する。
- 1.3　他者の知的財産権と知的成果を尊重する。
- 1.4　情報システムや通信ネットワークの運用規則を遵守する。
- 1.5　社会における文化の多様性に配慮する。

2.専門家として
- 2.1　たえず専門能力の向上に努め、業務においては最善を尽くす。
- 2.2　事実やデータを尊重する。
- 2.3　情報処理技術がもたらす社会やユーザへの影響とリスクについて配慮する。
- 2.4　依頼者との契約や合意を尊重し、依頼者の秘匿情報を守る。

3.組織責任者として
- 3.1　情報システムの開発と運用によって影響を受けるすべての人々の要求に応じ、その尊厳を損なわないように配慮する。
- 3.2　情報システムの相互接続について、管理方針の異なる情報システムの存在することを認め、その接続がいかなる人々の人格をも侵害しないように配慮する。
- 3.3　情報システムの開発と運用について、資源の正当かつ適切な利用のための規則を作成し、その実施に責任を持つ。
- 3.4　情報処理技術の原則、制約、リスクについて、自己が属する組織の構成員が学ぶ機会を設ける。

「倫理綱領」～情報処理学会　https://www.ipsj.or.jp/ipsjcode.html

「OECD情報セキュリティガイドライン」

(1) 認識（Awareness）
参加者は、情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分達にできることについて認識すべきである。

(2) 責任（Responsibility）
すべての参加者は、情報システム及びネットワークのセキュリティに責任を負う。

(3) 対応（Response）
参加者は、セキュリティの事件・事故に対する予防、検出及び対応のために、時宜を得たかつ協力的な方法で行動すべきである。

(4) 倫理（Ethics）
参加者は、他者の正当な利益を尊重するべきである。

(5) 民主主義（Democracy）
情報システム及びネットワーク[illegible]リティは、民主主義社会の本質的な価値に適合すべきである。

(6) リスクアセスメン[illegible]
参加者は、リスクア[illegible]

(7) セキュリティの設[illegible]
参加者は、情報システ[illegible]ある。

(8) セキュリティマネ[illegible]
参加者は、セキュリテ[illegible]

(9) 再評価（Reasses[illegible]
参加者は、情報システム及びネットワークのセキュリティのレビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。

情報システム及びネットワークが我々の社会に普及していることから、参加者は自らの作為又は不作為が、他者に損害を与えるおそれがあることを認識する必要がある。
それゆえ、倫理的な行動が極めて重要であり、参加者は、ベストプラクティスの形成及び採用に努め、かつセキュリティの必要性を認識し他者の正当な利益を尊重する行動を促進することに努めるべきである。

https://www.mofa.go.jp/mofaj/gaiko/oecd/security_gl_a.html

「RFC1087 倫理とインターネット」

インターネットへのアクセスおよびその利用は、ある種の特権であり、すべての利用者によってそのように取り扱われなければなりません。インターネットを利用する上では、次のような目的でなされるいかなる行為も、反倫理的で許容できないものです。

・インターネット上のリソースに対して権限のないアクセスを獲得しようとすること

・インターネットの本来の利用を妨害すること

・これらの行為によって、リソース（人的資源、処理能力、コンピュータ）を浪費すること

・コンピュータで処理される情報の完全性を毀損すること

・利用者のプライバシーを侵害すること

https://www.ipa.go.jp/security/rfc/RFC1087JA.html

情報セキュリティの倫理

「情報処理安全確保支援士 倫理綱領」

１．公正と誠実

　情報処理安全確保支援士は、業務上の判断を行うにあたり、先入観をもたず、他者かの不当な影響を受けず、常に公正な立場を堅持し、公正・誠実に業務を遂行しなければならない。

２．秘密保持

　情報処理安全確保支援士は、正当な理由がなく、その業務に関して知り得た秘密を漏らし、又は盗用してはならない。

３．法令等の遵守

　情報処理安全確保支援士は、法令等や専門職としての倫理を遵守しなければならない。

４．信用保持

　情報処理安全確保支援士は、専門家としての自覚をもち、信用を失墜する行為をしてはならない。

５．自己研鑽

　情報処理安全確保支援士は、専門家としての能力を必要とされる水準に維持し、かつ自らの知識・技能を高めなければならない。

https://www.ipa.go.jp/files/000073810.pdf

倫理的な判断と行動(1)～(ISC)2倫理規約

- **社会、一般大衆の福利、およびインフラを保護する**
  - –情報システムにおける世間の信頼性を高め、それを維持する。
  - –万全な情報セキュリティ対策についての理解を促し、その必要性を認識させる。
  - –公共インフラの保全性を維持し、強化する。
  - –安全性に問題のある慣習をやめさせる。
- **法律に違わず、公正かつ誠実に責任を持って行動する**
  - –真実を告げ、あらゆる利害関係者に自分の行動を逐次報告する。
  - –明示的、暗黙的にかかわらず、すべての契約および提携の取り決め事項を順守する。
  - – すべての関係者を公平に扱う。矛盾を解決するときは、公共の安全性の検討、当事者、個々人、セキュリティ専門家に対する義務をこの順序で考慮する。
  - –助言や忠告は慎重に行う。不必要な不安を煽ったり、軽々しく保証したりしない。自分の権限内で、慎重かつ客観的に真実を報告する。
  - –管轄区域によって法律が異なる場合は、サービス対象である管轄の法律を優先する。

https://www.ipa.go.jp/security/rfc/RFC1087JA.html

倫理的な判断と行動(2)～(ISC)2倫理規約

- **当事者に対して、十分かつ適切なサービスを提供する**
  - –対象システム、アプリケーション、および情報の価値を維持する。
  - –自分に対する信頼に応え、与えられた権限を尊重する。
  - –利害の衝突、または利害が衝突しているかのように見える行動を避ける。
  - –十分な能力とその資格のあるサービスのみを提供する。
- **セキュリティ専門家としての知識を向上し、保護する**
  - –最も適した人物に対して専門知識の促進を支援する。その他すべての条件が同じ場合、適任と認められ、これらの規律に従う人物や団体を選定する。日頃の行動や評判が、セキュリティ専門家としての信頼を損なう可能性のある人物とはかかわらないようにする
  - –悪意ある行為や不注意な行動によって、他のセキュリティ専門家の評判を傷付けないようにする。
  - –自分自身のスキルを向上し、常に最先端の知識を習得する。時間と知識を惜しまずに他者のトレーニングにあたる。

https://www.ipa.go.jp/security/rfc/RFC1087JA.html

サイバーセキュリティ業務における倫理行動宣言

□ 行動規範

サイバーセキュリティ事業に携わる者は、情報社会、セキュリティ製品やサービスを利用するお客様、そして事業者自身を守るために、以下の行動規範に則って事業を遂行します。

1. 情報社会の安全を向上させ、安心の醸成に努めます。
2. 法令等の正しい理解に努め、これを遵守します。
3. 高度化する脅威に備え、技術の向上に努めます。
4. 自らの製品およびサービスの安全確保に努めます。
5. 倫理観を持ち、正当な目的のために業務を遂行します。

NPO日本ネットワーク セキュリティ協会(JNSA)　倫理行動宣言
https://www.jnsa.org/cybersecurity_ethics/

＜参考＞ラック教育コースの注意書き

本コースは、『ネットワーク社会の安全・安心・信頼の確立に貢献できる情報セキュリティプロフェショナルの育成』を目的としています。

情報セキュリティプロフェッショナルに求められる知識・技能を修得するためには、効果的なセキュリティコントロールを導き出すための手法はもちろんのこと、人・組織・システムの弱点を把握し、セキュリティを突破するための手法についても学ぶ必要があります。このため、情報セキュリティプロフェッショナルには、自らの持つ知識・技能を正しく活用し、行動できる倫理観が求められます。

情報セキュリティプロフェッショナルに求められる一般的な倫理規範（※「RFC1087 インターネットと倫理」）を以下に示します。なお、**本コースで習得した知識・技能を悪用した場合、刑法又は民法により処罰されることがあります。**

倫理教育の問題点とその解決方法

セキュリティ業務で求められる「倫理観」

・事実を見極め、それをもとに考える。
　→「職業的懐疑心」

・注意深く、誠実に業務を行う。
　→「注意義務」「誠実(忠実)義務」

・自分の役割・権限・責任、能力を十分に認識し、それを全うする。
　→ 自分の使命(ミッション)は何？

倫理観のために：信頼できるデータや証拠とは？

信頼できるデータとは？

信頼できるログ管理とは？

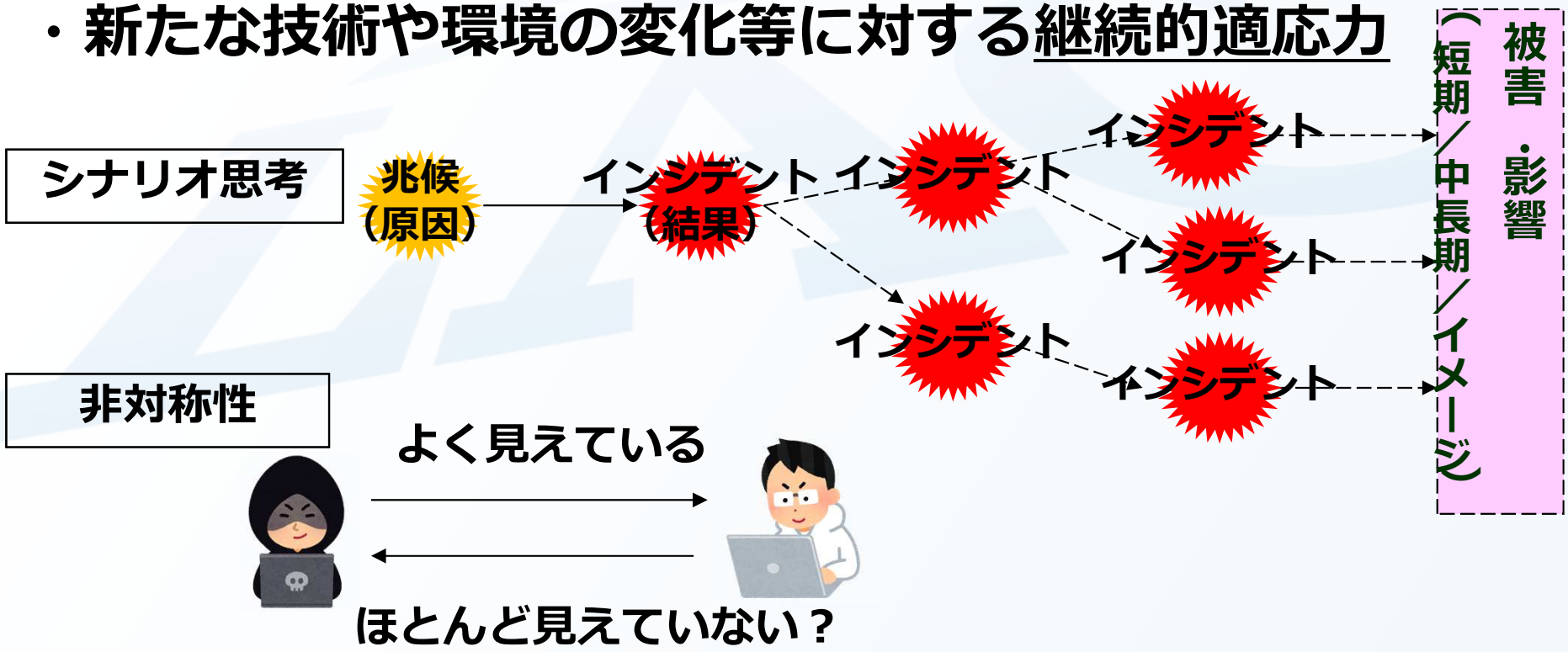
信頼できるメディアとは？

信頼できるログ解析と証拠は？

信頼できるログとは？

必要とされる実践的なスキルの例

- 事実を尺度にした思考と判断（特に、緊急時）
- 倫理的行動（注意義務や誠実義務）の遂行
- シナリオ思考（多くの不確実性要素のある中でも、予測し、対応する能力）
- 非対称性（不正／攻撃をする側との見え方の違い）への適応
- 新たな技術や環境の変化等に対する継続的適応力



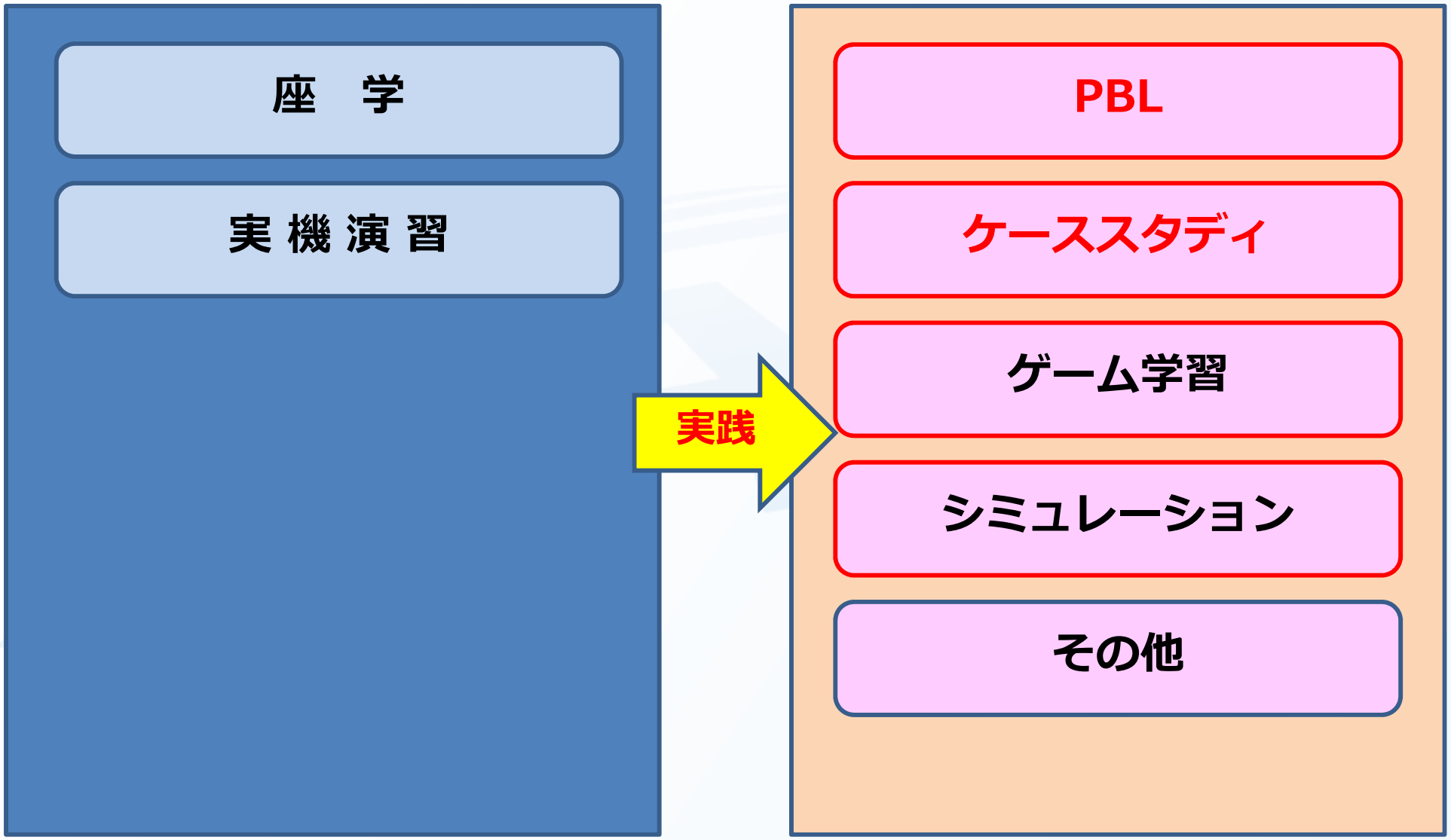
「倫理」は、何をどうやって教えるのか

「やってはダメ」なことを教えて、評価や管理するのではない。
（動機付けも測定・評価も困難）

規範的な行為＝「やるべきこと」を教えなければならない。

実務の中でできるようにするためには、**「実践的教育」**でなければならない。
（「一般論」や「抽象論」で具体的な行動に結びつけることも困難）

実践的人材をつくるための教育・訓練



実践教育：「特性」を磨き、「倫理観」をつける

・人材によって、「特性」は異なる。
・職種や役割によっても、必要とされる「特性」も「倫理」も異なる。

これらを見い出し（気づき）、「スキル」となるよう磨くには「演習」「訓練」をするしかない。

「演習」「訓練」は、シナリオで繰り返し行われなければならない。

＜参考＞教育設計の指針

「IDの第一原理」～M.D.メリル

要　素	概　要
問題 (Problem)	現実に起こりそうな**問題に挑戦**する
活性化 (Activation)	すでに知っている**知識を動員**する
例示 (Demonstration)	**例示**がある(“Tell me“ でなく “Show me“)
応用 (Application)	**応用**するチャンスがある(“Let me”)
統合 (Integration)	**現場で活用**し、**振り返る**チャンスがある

【ケーススタディ事例(1)】経歴の詐称

・あるところでいっしょに仕事をした、セキュリティ技術者Aさんが、過去の経歴を偽っていたことが判明しました。

　それに対し、Bさんは「経歴を詐称したが、業務はまじめにやっていたので問題はない」と言い、Cさんは「経歴の詐称は、IT技術者としても問題だし、セキュリティ技術者であればなお問題だ。まじめに業務をしていたかどうかの問題ではない」と言っています。

　これに対し、あなたはどう考えますか。その理由も述べてください。

【ケーススタディ事例(2)】担当者の運用・設定ミス発覚

・あなたは、D社のネットワーク及びシステムの検査業務を請け負いました。あなたが普段から懇意にしている窓口の担当者Eさんはこの検査にとても協力的なこともあり、業務は順調に進んでいました。しかし、あるサーバーを調べていたところ、いくつかの運用ミスや設定ミスを検出しました。このサーバーの管理者は、Eさんでした。

　これを知ったEさんは、「あとから設定などはし直すので、このことは検査報告しないで欲しい」と言っています。

　これに対し、あなたはどう対応しますか。その理由も述べてください。

【ケーススタディ事例(3)】内部犯行の可能性

・あなたは、情報流出事件が起こったF社から調査を請け負いました。

　調べたところ、内部の人間しか利用できない特権アカウントにより、業務時間外である早朝の情報のコピーや外部への送信・アップロードが確認されました。

　これをF社のCIOであるG取締役に話したところ「社員Hの内部犯行に間違いないので、Hの通信や行動をネットワークで24時間監視して欲しい」と依頼を受けました。

　これに対し、あなたはどう対応しますか。その理由も述べてください。

まとめ

- **IT技術者、特にセキュリティ業務に関わる技術者には必須の知識と「行為規範」です。**

- **要領や規約、ガイドライン等を暗記させるのではなく、行動の規範として理解させ、普段から実践させることを習慣にしましょう。**

- **そのためには、推進する体制や教育のためのケース（事例の収集と活用）や評価の枠組みが必要。**

LAC
ともに、イキル

Thank you. Any Questions ?

※ この講演における発言、及び資料の内容は、個人の見解であり、所属する企業や団体を代表するものではありません。

株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1
平河町森タワー
Tel 03-6757-0113　Fax 03-6757-0193
www.lac.co.jp