実践的SOC/CSIRT人材の育成

2017年6月9日(金)

株式会社ラック　長谷川 長一

長谷川　長一（はせがわ　ちょういち）

CISSP®

株式会社ラック　事業企画推進室　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 高度ICT利活用人材育成会議 委員（2011~2013年度）
- □ 経済産業省 情報セキュリティ人材の育成指標等の作成事業 WG委員(2012年度)
- □ 文部科学省 中核的専門人材養成の戦略的推進事業 委員（2012年度～）

■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

SOCとCSIRT関連の業務
～ラックのサービスの場合～

LAC監視センター 「JSOC」

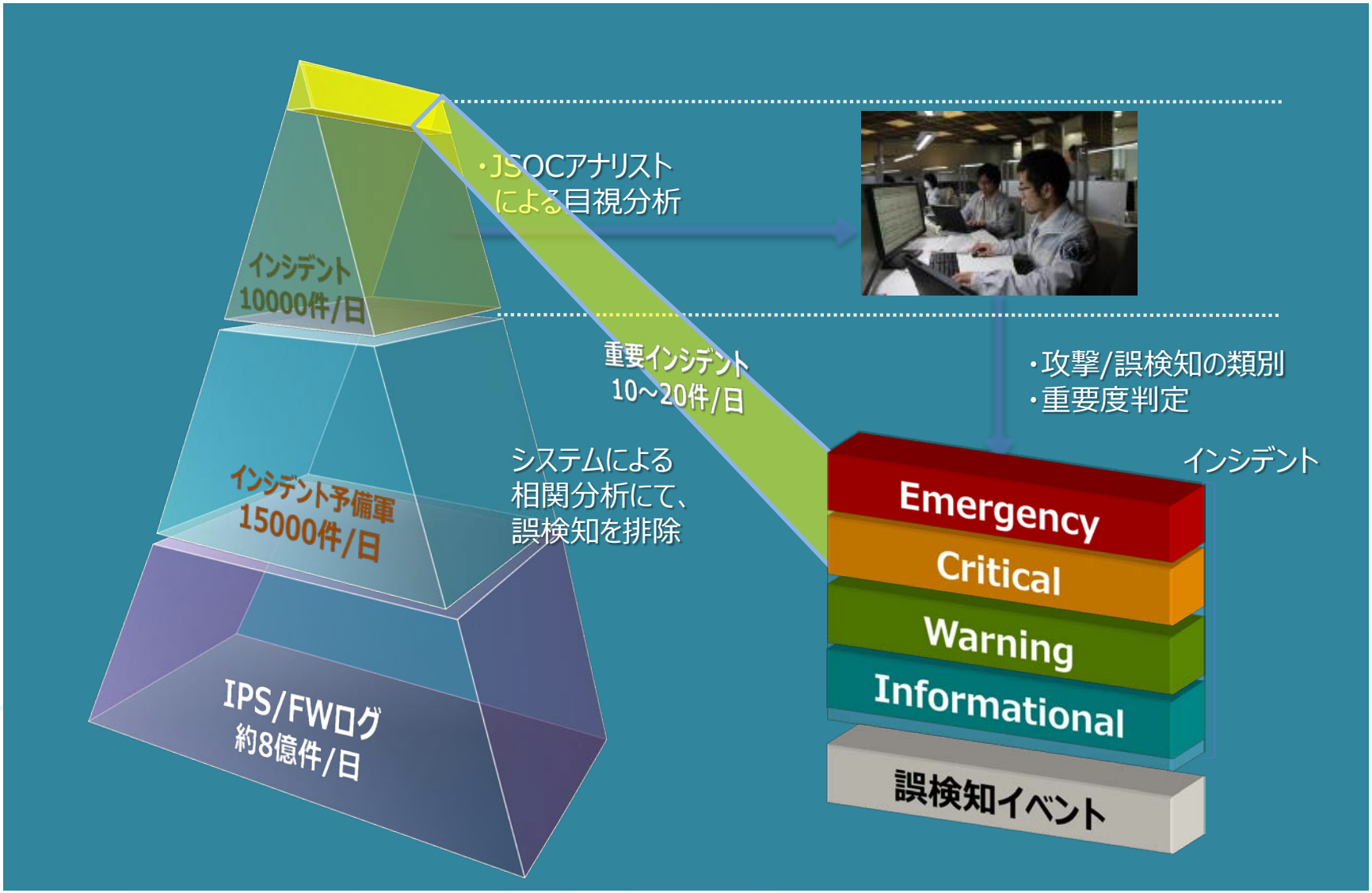
LAC監視センター 「JSOC」とは

JSOC（ジェイソック）は、英語名Japan Security Operation Centerの頭文字を取り組織名とした、セキュリティ監視・運用サービスの拠点です。JSOCは2002年に東京・虎ノ門に開設されましたが、そのルーツは2000年に東京・お台場に設立されたセキュリティ監視センターです。同年開催された「九州・沖縄サミット」の公式サイトにおける不正アクセス監視・対応を支援したことから、セキュリティ監視サービスは通常の運用を開始しました。そして2010年6月に平河町に移転し、今後に備え監視システムや設備を一新しました。

多くのお客様からの信頼をいただき、JSOCで監視・分析の対象となる機器（監視センサー）の数は増加し続けています。現在では850団体以上、1,500センサー以上（※1）となり、国内最大規模を誇るに至っています。

https://www.lac.co.jp/corporate/unit/jsoc.html

JSOCにおける分析の流れ



緊急対応サービス「サイバー119」

https://www.lac.co.jp/service/consulting/cyber119.html

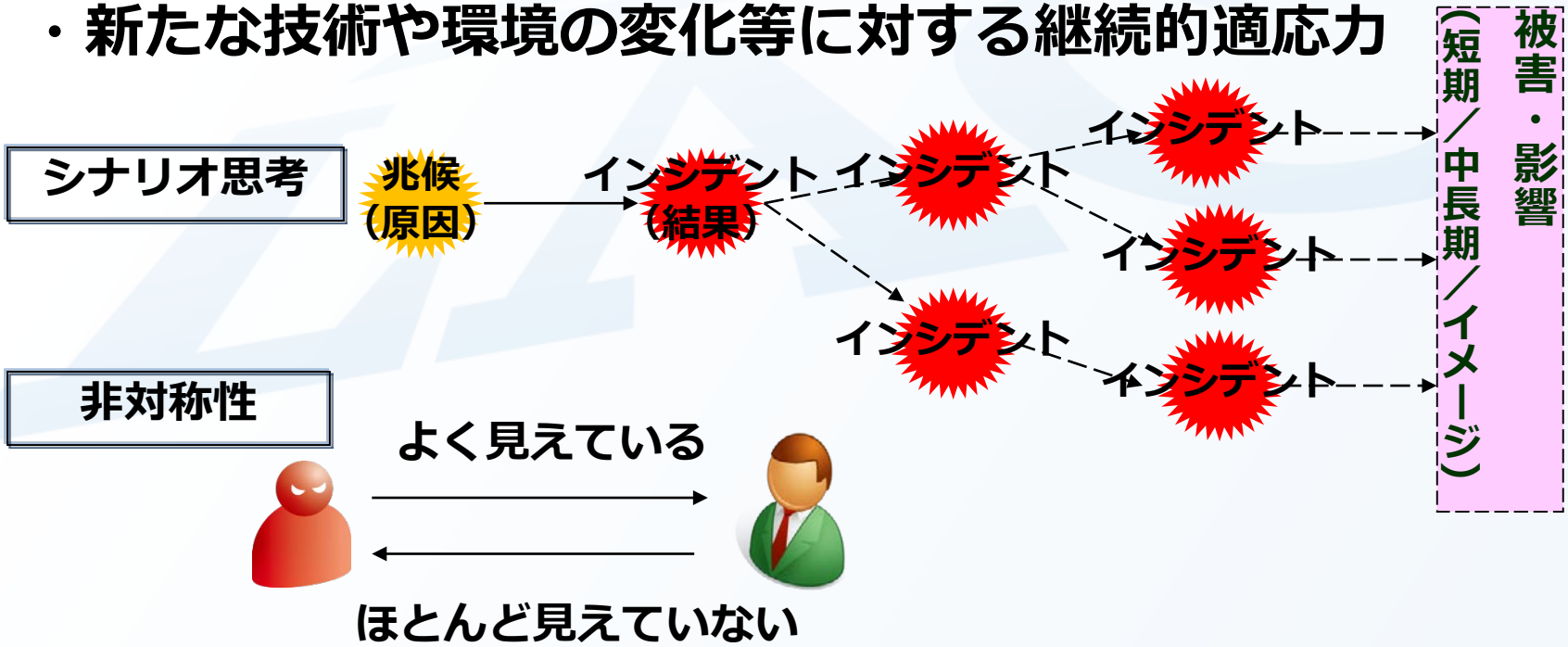
緊急対応サービスの概要

事件・事故	具体例
誤操作、不注意、過失など	Winnyなどのファイル共有ソフトを自宅やオフィスで使用、パソコンやメディアの紛失、メールの誤送信など
外部からの犯行（Webサイト侵入・バックドアなど）	SQLインジェクションによるデータベースへの侵入、外部から出入りできる秘密の扉を設置、クレジットカード情報の漏えい
内部犯行（踏み台・ボット・金銭目的ほか）	ボットなどによるパソコンの乗っ取り、アカウント・個人情報・クレジットカード情報・機密情報の漏えい
関係者犯行（金銭目的）	アカウント・個人情報・クレジットカード情報・営業機密・大企業や官公庁の機密情報の漏えい、内部と元関係者の関与の可能性
関係者犯行（恨み・自爆犯行）	情報漏えいそのものが目的ではないWinnyによる漏えい偽装、ストーカー的犯行

https://www.lac.co.jp/service/consulting/cyber119.html

＜参考＞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）
- 倫理観、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

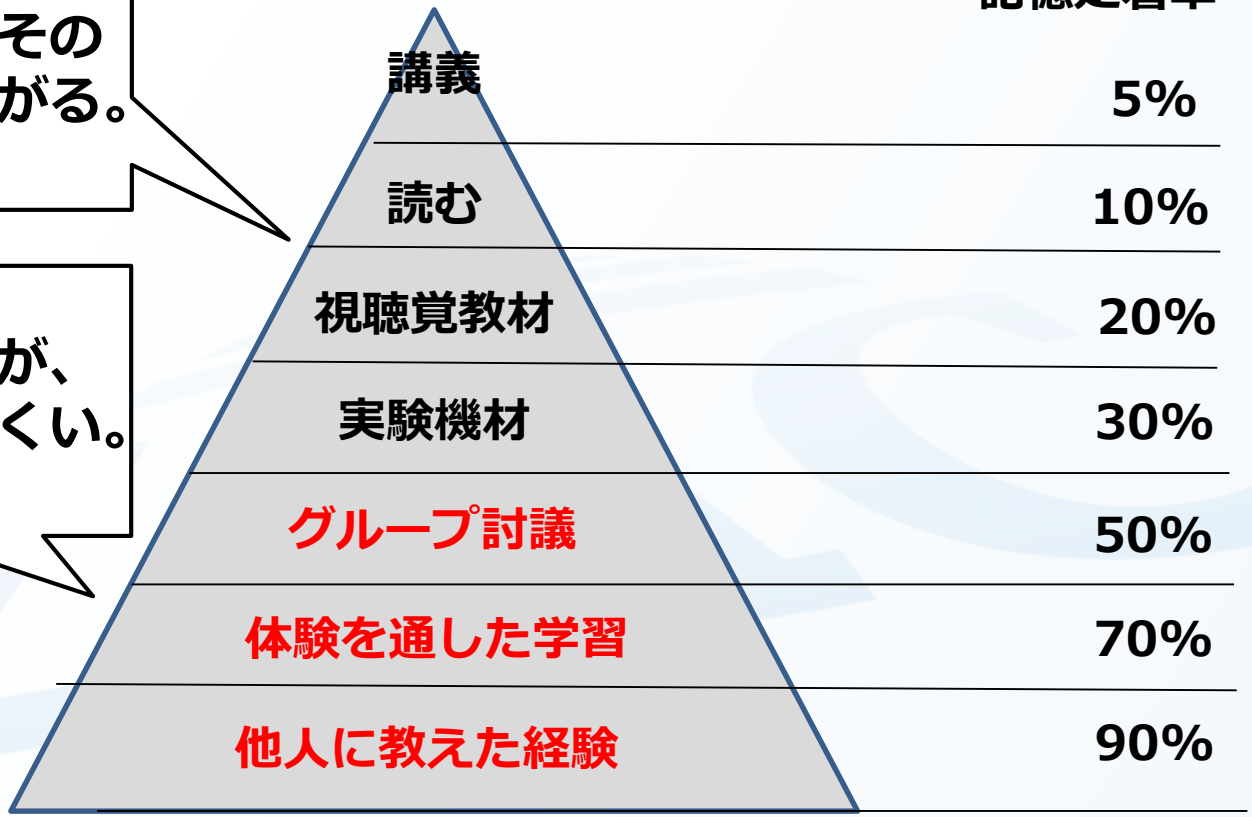


実践的教育・訓練の取り組み事例

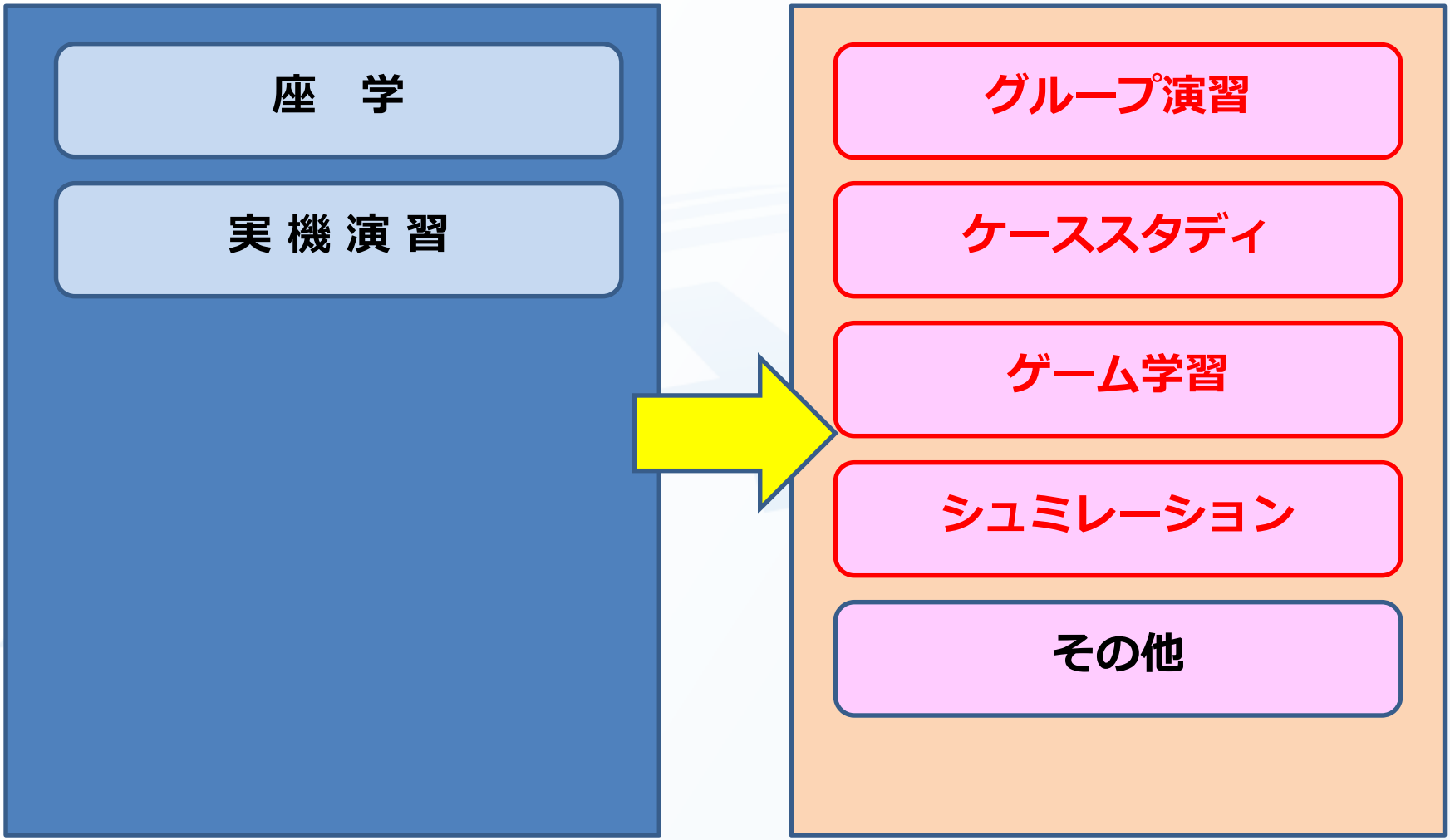
＜参考＞「ラーニング・ピラミッド」

教えることで、その人のスキルも上がる。

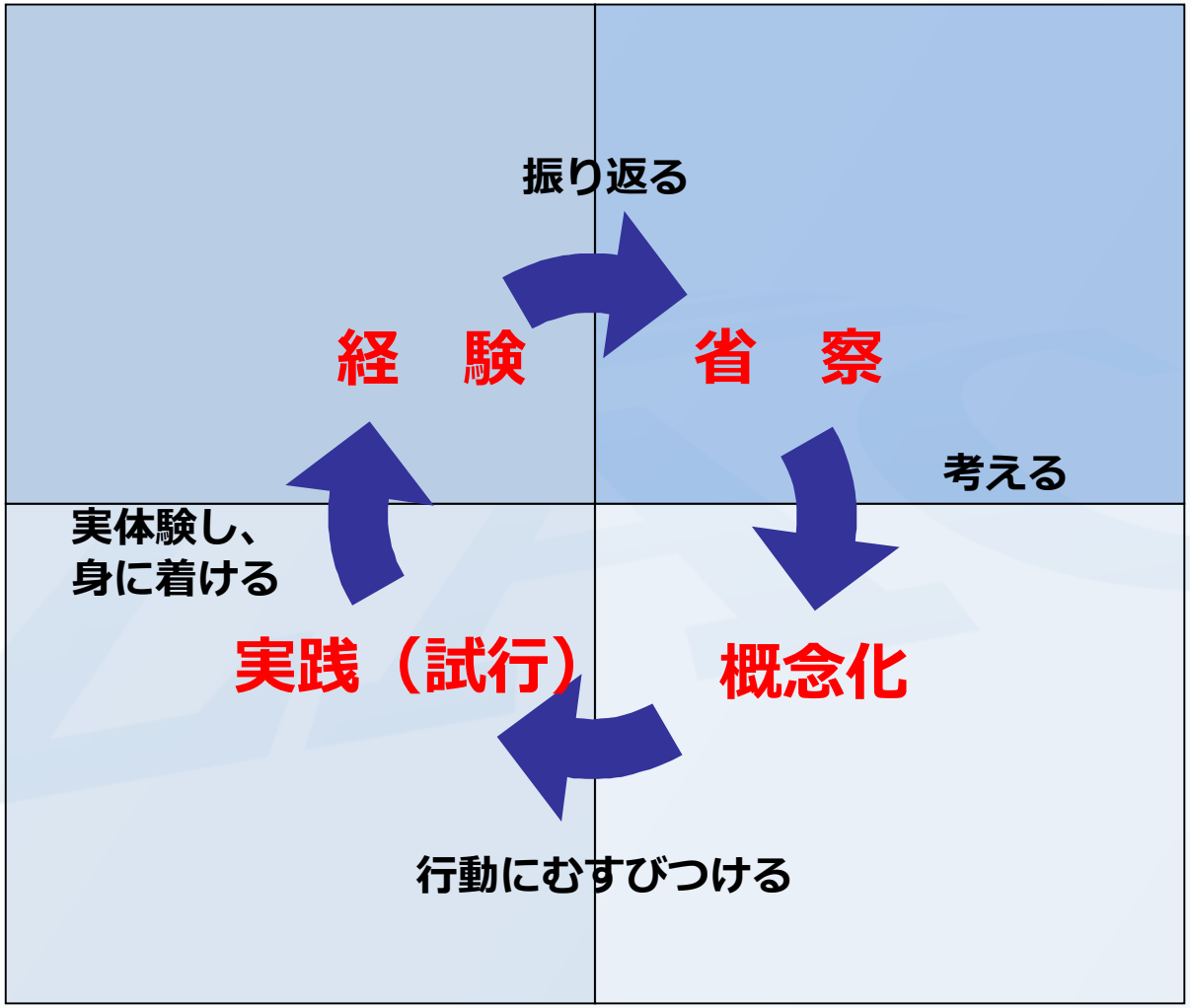
ここができる人が、少ない。育てにくい。



実践的人材をつくるための教育・訓練



＜参考＞経験学習のためのモデル



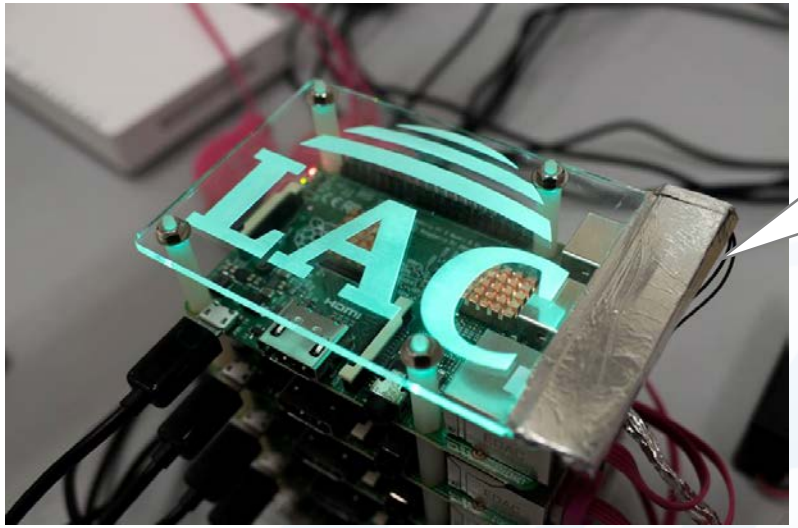
「経験学習モデル」～デビット・コルブ

「経験学習」と「振り返り学習」

種　類	知識伝達学習	経験学習	振り返り学習
概要	正しい知識を持った人が、持っていない人に転移させて学ばせる	自らの体験や考察、他人の観察をもとに問題を解決しながら学ぶ	自らを振り返る（省察）することで、これから何をすべきかを学ぶ
メリット	・必要な知識を効率的に伝達できる。 ・多くの人を一度に学習させることができる。 ・未経験者や知識の少ない初心者にも教えることができる。	・自分の知識や経験が学習に生かしやすい。 ・受講者が主体的に学習できる。 ・具体的な「行動変容」に結びつけしやすい。	・受講者個々に合った「深い学習」が可能になる。 ・参加者同士の「学び合い」ができる。
デメリット	・内容が一律になりやすく、経験や知識のある者にとっては内容的に物足りなくなる。 ・講師主導のため、受講者の主体性が失われやすい。	・知識や経験の少ない人は学習しにくい。 ・一度に多くの知識やスキルを学ぶことができない。 ・過去の知識や経験から抜け出せないことがある。	・(講師など)外からの視点が入らないと、学びが広がりにくい。 ・学習の時間がかかり、効率が悪い。 ・受講者によって、差が出やすい。
学習形式	座学（スクール形式）	協働(ワークショップ形式)	協働(ディスカッション形式)

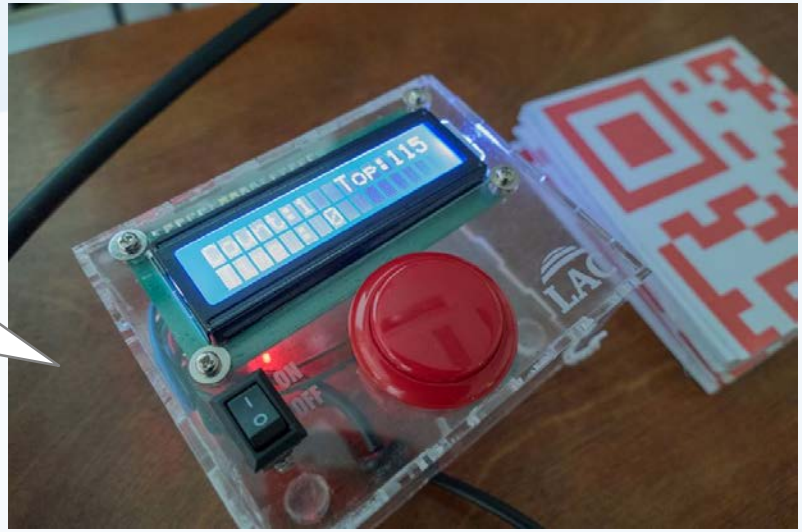
＜事例＞CTF(Catch the Flag)

学習した知識・技術を、CTFで確認する学習。



ラズベリーパイ5段重ねのCTF用サーバー。
（中身：問題サーバー、得点サーバー等）

ラック特製の小道具。
連打ボタン、QRコードパズル等



＜事例＞「LACサバイバルチャレンジ」

ニュース　日経NETWORK

ラック、社員が攻撃を体験するサイバー防災訓練を実施

2014/06/02
山田 剛良＝日経NETWORK （筆者執筆記事一覧）

記事一覧へ >>

シェア　ツイート　B! ブックマーク

セキュリティ大手のラックは2014年6月1日、サイバー攻撃を実際に体験する演習「LACサバイバルチャレンジ」を社員研修として実施した。社員と協力企業の技術者計46人が参加し、1チーム5～6人の9チームに分かれ、架空のネット通販企業のサイトを運営。主催者が仕掛けるサイバー攻撃から防御するシステム運用技術を丸1日で競った（写真1）。自分が運用するシステムがサイバー攻撃を実際に受け体験を通じて技術者の意識を高め、サービス品質を高める狙い。将来的には研修サービスとして事業化も視野に入れる。

LAC社内実施の**実践的シナリオ演習。**
本人の自由意思による参加。

最新のサイバー攻撃を体感し、現状のスキルを、実業務に生かせるスキルにする目的。

緊急時において、今までの知識や技術を生かして適切かつ迅速に判断・対応できるのか。

チャレンジできる場を与え、スキル維持・向上を支援する。

～日経ITpro
http://itpro.nikkeibp.co.jp/article/NEWS/20140602/560762/

＜事例＞ LAC「サイバーセキュリティボード」

2～3名のグループ戦。
(組織横断的なグループ編成が可能)
会社を経営しながら、発生するインシデントに対応します。

もっとも多くの売り上げを上げたチームが勝ち！

弊社若手社員の発案。

迅速かつ適切な対応のために

多くは、セキュリティ機関や捜査機関からの連絡から

(1) 感染等(攻撃・犯罪)の疑い → 多くはここ。
(2) 実被害発生の疑い → いきなり、この連絡が来ることもある。
⇒ 想定は難しくないが、**事前に準備していないと判断も行動もできない。**
予め組織としての対応方針や手順を決めておかなければならない。

→ 理解するだけではなく、訓練が必要！

「演習」「訓練」を
通して、緊急時の対応
を可能に!!

そして、育成する側がすべきこと

- 育成する人材の育成と維持。現役かつ現場を知っている者しかできない実践教育。

- 育成した人材の活用のための環境や体制の構築と維持。(組織内の研修だけでなく、外部での活動に参加させる)

- チャレンジできる場(機会) 、失敗できる場の提供。

- 欠点を見つけ修正する教育ではなく、長所を見つけ伸ばしていく教育。

組織的、かつ継続的な支援が必要

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、個人の見解を含んでいます。それらは、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