Japan Information Security
Management Systems User Group

テーマ１

実践かつ効果的なセキュリティ教育

JNSA 標準化部会

日本ISMSユーザグループ　リーダー

インプリメンテーション研究会　主査

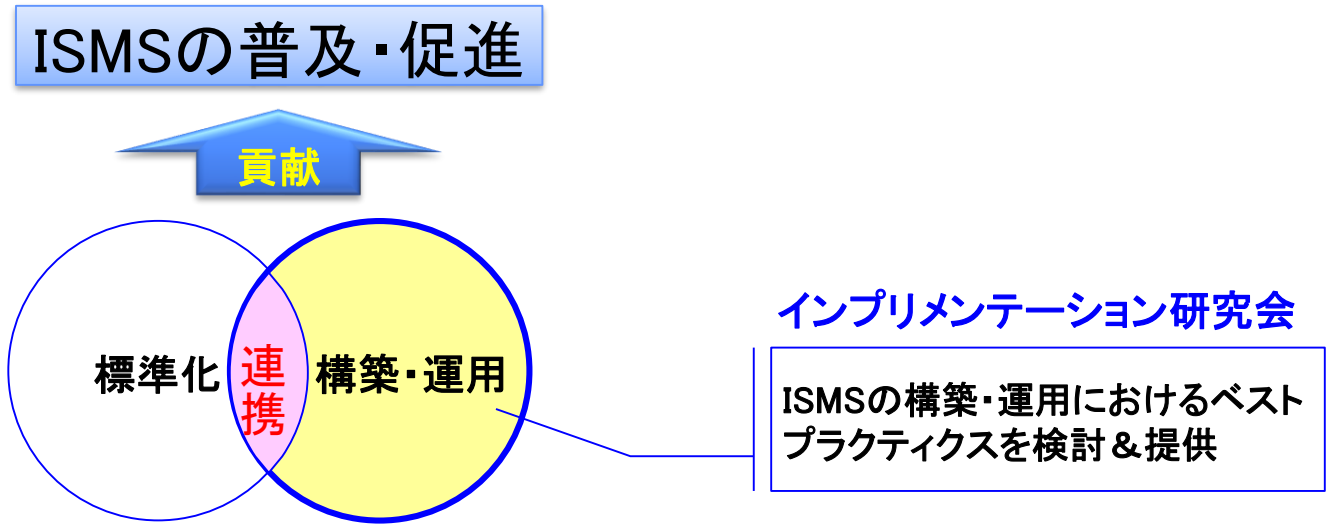
2020年12月18日

魚脇　雅晴

日本ISMSユーザグループの活動紹介

■活動目的と活動概要

日本ISMSユーザグループではISMSを構築・運用する上で規格をどう読み解いて、企業活動にISMSを積極的に実践活用する方法を検討、研究し、国内外へ発信します。具体的にはISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることで**ISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における健全かつ効果的なISMS普及・促進に貢献する活動**を行っています。



インプリメンテーションWGの活動テーマ

活動テーマのご紹介　（2006～2012）

年度	インプリメンテーションWG	メジャメントWG
2006	■本WGの活動紹介＆ISMS導入に関する課題の事例紹介	■有効性測定の基本的な考え方＆取り組み事例紹介
2007	■情報セキュリティ研修・啓発 ■効率的リスクアセスメント	■有効性測定の基本的な考え方＆新たな取り組み事例紹介（進捗状況含む）
2008	■ISMS構築事例に見る有効性測定構築の傾向 ■業務委託先のセキュリティ評価	■有効性測定の基本的な考え方＆共通フレームワーク案（進捗状況含む）
2009	■標準的なリスク分類と具体的な管理策の対応のモデル化 ■管理策の有効性評価を効果的に行うモニタリング手法のモデル化	■ISO/IEC27001における「有効性測定」
2010	■標準的なリスク分類と具体的な管理策の対応のモデル化 ■管理策の有効性評価を効果的に行うモニタリング手法のモデル化	■ISO/IEC27001における「有効性測定」
2011	■可視化手法を用いたリスク対策モデル ■ISMS全体の有効性評価手法	■管理策の有効性測定
2012	■可視化手法を用いたリスク対策モデルとその実践的応用 ■ISMS実践手法　BCPのモデル化の検討	■管理策の有効性測定

インプリメンテーションWGの活動状況テーマ

活動テーマのご紹介　（2013～2020）

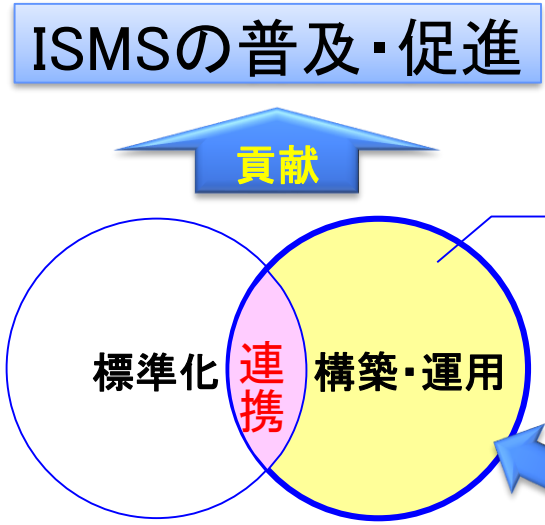
年度	インプリメンテーションWG	メジャメントWG
2013	■ISMS推進事務局の悩みと解決策 ■有効性評価に基づくISMS実践活用	メジャメントWGは有効性評価に関する成果を持って活動を休止。インプリメンテーション研究会に一本化して活動。
2014	■ISMS推進事務局の悩みと解決策 ■ISMS規格改訂にともなう実装方法の検討	
2015	■ISMSを成功させる理想的なCISOの条件 ■減らないインシデントの特効薬	
2016	■サイバー攻撃を事例としたリスクマネジメントの実践 ■運用フェーズにおける有効性の評価	
2017	■現場と連携したリスクアセスメント手法の実践活用 ■内部監査を有効に運用するための手法の考察	
2018	■ISMS規格要求事項から紐解く最新のビジネス環境リスク ■働き方改革における情報セキュリティ	
2019	■最新の環境変化に伴うISMSの実装検討 ■各社の事例から学ぶISMSの実装について	
2020	**■実践かつ効果的なセキュリティ教育** **■規格の解釈（ISO/IEC27002の改定）に伴う対応についての取り組み**	

インプリメンテーション研究会のメンバー

中村　昌登	アイレット(株)
松原　勝美	(株)インターネットイニシアティブ
大月　あゆみ	SBテクノロジー（株）
森　親章	NECソリューションイノベータ(株)
大熊　信也	NECソリューションイノベータ(株)
大平　泰寛	NECソリューションイノベータ(株)
秋山　健一	NECプラットフォームズ(株)
松居　隼司	NECプラットフォームズ(株)
安田　次郎	NECプラットフォームズ(株)
早川　宏	エヌ・ティ・ティ・コミュニケーションズ(株)
魚脇　雅晴	NTTコム ソリューションズ(株)
村山　尚	NTTコム ソリューションズ(株)
原　路子	NTTコム ソリューションズ(株)
広田　正毅	NTTコム ソリューションズ(株)
梅　文夫	NTTコム ソリューションズ(株)
中谷　勝彦	NTTコム ソリューションズ(株)
徳永　安芸	NTTコム ソリューションズ(株)
前田　佳子	NTTコム ソリューションズ(株)
河本　敏宏	(株)エヌ・ティ・ティ・データ
和田　義毅	(株)エヌ・ティ・ティ・データ
今野　尚昭	エヌ・ティ・ティ・データ先端技術(株)
小澤　隆一	エヌ・ティ・ティ・データ先端技術(株)
鍋島　聡臣	エヌ・ティ・ティ・データ先端技術(株)
帯刀　静夫	(株)NTT ファシリティーズ エンジニアリング
宮本　俊之	(株)NTT ファシリティーズ エンジニアリング

水本　政宏	ＫＤＤＩ(株)
橋本　秀行	ＫＤＤＩ(株)
奥田晃典	(株)JSOL
武井　正好	(株)大和総研ビジネス・イノベーション
間形　文彦	日本電信電話(株)
岡野　裕樹	日本電信電話(株)
相羽　律子	(株) 日立製作所
上村　竜也	(株)VSN
増田　浩次	富士通(株)
阿部　正峰	富士通(株)
新井　雅	富士通(株)
槇谷　努	富士通(株)
宮本　豊	(株)ラック
小梁　康志	リコージャパン(株)
羽田　卓郎	リコージャパン(株)
矢島　大	リコージャパン(株)
置田　健児	リコージャパン(株)
常川　直樹	パナソニック（株）
葛西　章広	個人（(一財）高度映像情報センター（AVCC)）
冨田　吉弘	個人（元・富士通）
小野　等	個人（ICMS、元・リコージャパン）
野代　安紀	個人（元・富士通）
尾崎　幸彦	個人（JACO：日本環境認証機構）
杉山英夫	個人（日本メックス株式会社）

今年のインプリメンテーション研究会のテーマ



インプリメンテーション研究会

ISMSの構築・運用におけるベストプラクティクスを検討＆提供

ベストプラクティクスを検討＆提供

事例研究として、下記のテーマ深掘り

■実践かつ効果的なセキュリティ教育

標準化されたものをどのようにビジネスの世界に反映＆定着させるか・・・

アドフォック会議にリエゾンとして参加

ユーザー目線で「現場で理解し、使いこなせること」を意識したISO27002の規格の改正に関する方向性について意見を提言

■規格の解釈（ISO/IEC27002の改定）に伴う対応についての取り組み

活動テーマ(案)の選定理由

メンバーの一番関心があり、切実な問題をテーマに選定

m.uowaki uowakiさんが、投票を開始しました
05 Feb, 02:26 PM

インプリ研のテーマについて簡単な投票を実施します。
取り組みたいテーマについて投票願います。

○ 案１：最新の環境変化に伴うISMSの実装検討　・・・　継続テーマ	1
○ 案２：ISMSの管理策の実装　「oooについての考察」昨年はログ　・・・継続テーマ	2
○ 案３：サイバーセキュリティ（一人から始めるCSIRT・・・）	2
○ 案４：規格の解釈（ISO/IEC27002の改定）に伴う対応についての取り組み	5
○ 案５：内部監査の品質向上、有効性評価	0
○ 案６：経営層とのコミュニケーション（特にリスク）	1
◉ 案７：実践かつ効果的なセキュリティ研修	8

CSV形式でダウンロード・投票数： 19

テーマ1

実践かつ効果的なセキュリティ教育

ストーリー・テラー・・・

セキュリティ教育に悩んでいるあなた
あなたの抱えている悩みは誰もが抱えている共通的な悩みでもあり、
本質的なものです
教育は組織文化の醸成の有効な手段となるはず！

本テーマではセキュリティ教育にフォーカスをあてて、組織の抱えている
課題や規格要求事項から具体的な管理策やプロセスに落とし込むこと
で**現実的かつ効果的なセキュリティ教育**について掘り下げます

この1年間研究会のメンバーで議論を重ねてきて、各組織が抱えて
いる課題の解決の糸口になるように検討＆整理してきました

本成果が皆様の組織においてセキュリティ教育の振り返りや抱えている
課題解決の一助となれば幸いです

理想の世界を想像してみると・・・

理想郷としての組織

力量	認識＆行動

知る → 理解 → 出来る能力 → 正しく行動

- 正しい行動
- 間違った行動

全員がルールを理解

指導出来るレベルの社員が大半

標的型攻撃メールを開く人間は一人もいない

各組織で抱える課題

現状把握

現状の課題把握（研究会メンバーへのアンケート）

現状の課題・欲求

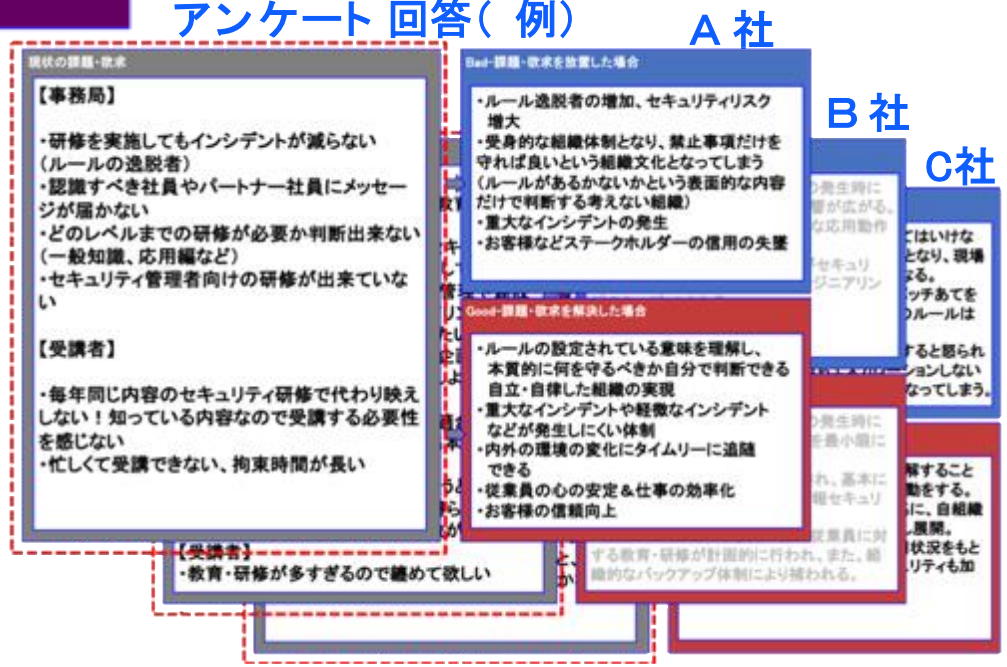
Bad-課題・欲求を放置した場合

Good-課題・欲求を解決した場合

Bad→Goodへ向かう方策は？

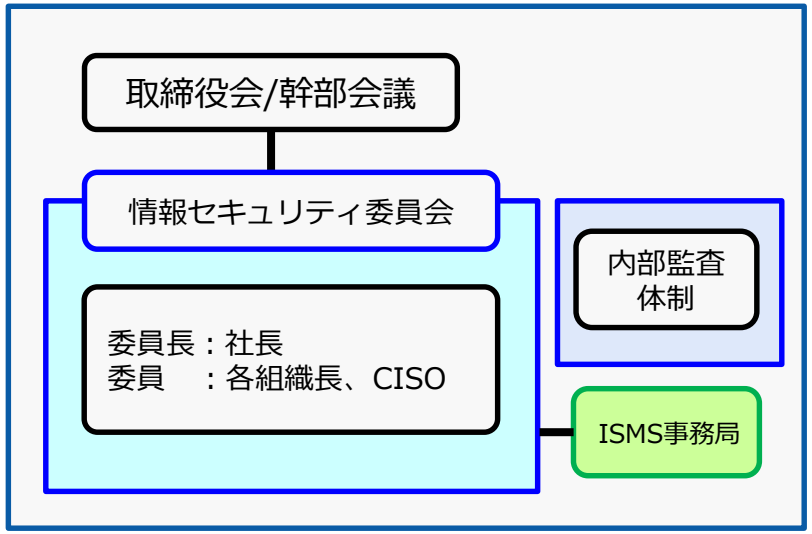
Value-ISMS-UGが提案する方策（方向性）は？・・・一文で表現

アンケート 回答（ 例）

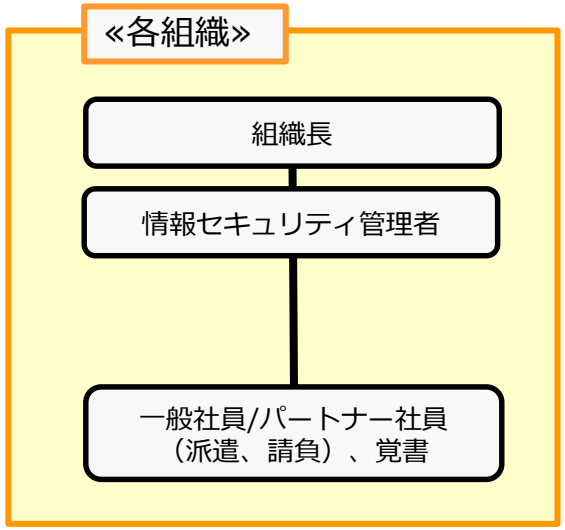


現状の課題把握（組織体制の例示）

組織体制



・ISMS事務局員
・規則　守（45歳）
男性、既婚



・お客様SI案件のPM
・唯我独尊（32歳）
男性、未婚

現場サイド（唯我独尊さん）の心の声

毎年同じ内容のセキュリティ研修で
代わり映えしない！
知っている内容なので受講する必要性を
感じない

忙しくて受講できない、拘束時間が長い

Web教育なので、**テスト、アンケートだけ受けて終わり**にする・・・

教育・研修が多すぎるので
まとめて欲しい

・お客様SI案件のPM
・唯我独尊（32歳）
男性、未婚

（常に意識している）**教える側と、**
（一時だけ研修を）**受ける側との温度差**がある

研修内容が実務と乖離し、また
専門用語が解らず、**自分事として腑に落ちない**（理解度低下）

事務局（規則 守さん）の心の声

認識すべき社員やパートナー社員にメッセージが届かない

受講者の理解を深められるような、実務で役立つ研修ができていない

研修を実施してもインシデントが減らない（ルールの逸脱者）

体制が脆弱なためルールを周知されずインシデントを起こす業務委託先等もある

・ISMS事務局員
・規則　守（45歳）
男性、既婚

セキュリティ管理者向けの研修が出来ていない

セキュリティ管理者に必要な力量設定＆教育が出来ていない

研修は**全社の教育・研修担当にてとりまとめて実施して欲しい**
（コンプラ、CSR、輸出管理、GDPR、セキュリティ）

教育教材の作成に稼働が掛かる

現場サイドと事務局の葛藤

教えたつもり・・・

100%

・お客様SI案件のPM
・唯我独尊（32歳）
男性、未婚

・ISMS事務局員
・規則　守（45歳）
男性、既婚

レスポンス・・・

（常に意識している）**教える側と**、
（一時だけ研修を）**受ける側**
との温度差がある

現場の声を事務局目線で課題化（受講者目線）

	現場の声	課題化した項目
受講者	毎年同じ内容のセキュリティ研修で代わり映えしない！知っている内容なので受講する必要性を感じない	**マンネリ化（受講意欲がわかない）** →（常に意識している） **教える側と、受ける側との温度差**
	Web教育なので、テスト、アンケートだけ受けて終わりにする（受講完了すれOK！）	
	研修内容が実務と乖離 専門用語で分かりずらい （理解度低下）	ISMSの要求事項などの用語をそのまま使った教材や研修内容 **本業の業務とリンクが出来なくて、他人事** （として捉えている） →結果的に理解度向上に繋がらない
	忙しくて受講できない、 拘束時間が長い	**本業に追われて研修にまとまった時間が取れない** また、他の研修（コンプライアンス、CSRなど）も同時期（年度末）に実施されていて、イジメのような構図だ！ →他の分野の研修含めて開催日程の調整や実施方法について検討の余地あり

事務局目線で課題の深掘り（事務局目線）

	現状の課題	課題の深堀
事務局	研修を実施してもインシデントが減らない（ルールの逸脱者）	**受講済み≠理解** （全員受講済みでも理解不足によるインシデントが減らない） **→100%受講で有効性評価OKではない！** **→問題行動をとる人の行動分析**
	認識すべき社員やパートナー社員にメッセージが届かない	ルールから逸脱しやすい受講者は仕事をしながら受講するので理解出来ていない （まじめに受講している割合は？） **→ネガティブ従業員との戦い**
	どのレベルまでの研修が必要か判断出来ない（一般知識、応用編など）	どのレベルの研修が必要か**明確な判断基準がない** （現状はセキュリティルール、組織が直面している脅威、インシデント発生時の行動規範などを題材）
	セキュリティ管理者向けの研修が出来ていない	**役割に応じた力量設定** が出来ていない。

課題のキーワードと解決のアプローチ

課題のキーワード

- マンネリ化
- 積極的な受講意欲がわかない
- 教える側と受ける側との温度差
- 本業の業務とリンクが出来なくて、他人事
- 本業に追われて研修のまとまった時間を取れない、取りにくい
- 全員受講済みでも理解不足によるインシデントが減らない
- 受講者は仕事をしながら受講
- 研修レベルの明確な判断基準がない
- 役割に応じた力量設定

解決へのアプローチ

〇規格要求事項からセキュリティ教育において考慮すべき事項を可視化

〇各社の実践事例の分析＆まとめ

→セキュリティ教育の全体像を整理

→ベストプラクティスとして整理

規格要求事項から導かれる管理策の要件整理

初心に立ち戻って振り返り・・・

本来、組織の全ての従業員、契約相手に**役割に応じた力量、認識**を設定し、職務に関連する組織の方針及び手順について**適切な、意識向上のための教育及び訓練**を受けなければならず、また、定めに従ってその更新を受けなければならないが、実態は乖離している

ルールの理解、セキュリティマインドの醸成は年1回のセキュリティ研修で理解し、身につくものではなく様々な形態での意識付けを実施する必要がある

本来はどうあるべきか規格要求事項を振り返る・・・

A.7.2.2 情報セキュリティの意識向上、教育及訓練
7.2 力量
7.3 認識

A.7.2.2 情報セキュリティの意識向上、教育及訓練

管理策

組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、**適切な、意識向上のための教育及び訓練**を受けなければならず、また、**定めに従ってその更新**を受けなければならない

27002実施の手引きでは・・・

規格要求事項　　27002実施の手引き

情報セキュリティの意識向上プログラムは、

①情報セキュリティに関する**各自の責任及びその責任を果たす方法について、認識**させてることを狙いとする

②**保護すべき組織の情報及び情報を保護するために実施されている管理策を考慮**に入れて、組織の情報セキュリティのための方針群及び関連する手順に沿って確立する

③**キャンペーン（情報セキュリティの日など）、及びパンフレットまたは会報**の発行のような、複数の意識向上の活動を含める

④**従業員の役割、契約相手の認識に対する組織の期待**を考慮に入れる

⑤長期にわたり、できれば**定期的に計画**される
→活動が繰り返され、**新しい従業員及び契約相手も対象**となる

⑥**定期的に更新**して組織の方針及び手順に沿うようにする

⑦必要とされた場合に実施する
→教室での訓練、通信教育、インターネットを利用した訓練、自己学習その他**多様な手段**

7.2 力量

管理策　組織は下記の事項を行わなければならない

a） 組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に**必要な力量を決定**する

b） **適切な教育、訓練又は経験に基づいて**、それらの人々が**力量を備えていることを確実**にする

c） 該当する場合には、必ず、**必要な力量を身に付けるための処置**をとり、とった**処置の有効性を評価**する

d） **力量の証拠として、適切な文書化**された情報を保持する力

注記　適用される処置には、例えば、現在雇用している人々に対する、教育訓練の提供、指導の実施、配置転換の実施などがあり、また、力量を備えた人々の雇用、そうした人々との契約締結などもある

JISQ 27000:2014
2.11　力量（competence）
意図した結果を達成するために、知識及び技能を適用する能力

7.3 認識

管理策　組織の管理下で働く人々は、次の事項に関して認識をもたなければならない

a） **情報セキュリティ方針**
b） 情報セキュリティパフォーマンスの向上によって得られる便益を含む、**ISMSの有効性に対する自らの貢献**
c） ISMS **要求事項に適合しないことの意味**

認識は、教育・訓練やISMS活動を通じて醸成されるものであり、また
日常の業務における問題意識、危機意識の育成に繋がる
ひいてはISMSに携わる人々の力量の向上にもつながる

規格要求事項から導かれる管理策の要件整理

規格A.7.2.2

情報セキュリティの**意識向上**、**教育**及**訓練**

組織の全ての従業員、関係する契約者

適切な、**意識向上**のための**教育及び訓練**

27002実施の手引き

規格　7.2

力量

力量を備えていることを確実にするために適切な教育、訓練

必要な力量の決定

業務遂行に必要な力量

現状の力量

処置の有効性を評価
&
文書化

力量の証拠

力量の分類

ビジネスを推進するスキル
セキュリティスキル

規格　7.3

認識

組織の全ての従業員、関係する契約者

必要な認識

- 情報セキュリティ方針
- ISMSの有効性に対する自らの貢献
- 要求事項に適合しないことの意味

規格要求事項から導かれる管理策の要件整理

27002実施の手引き

情報セキュリティの意識向上プログラムは、

①情報セキュリティに関する**各自の責任及びその責任を果たす方法について、認識**させてることを狙いとする

②**保護すべき組織の情報及び情報を保護するために実施されている管理策を考慮**に入れて、組織の情報セキュリティのための方針群及び関連する手順に沿って確立する

③**キャンペーン（情報セキュリティの日など）、及びパンフレットまたは会報**の発行のような、複数の意識向上の活動を含める

④**従業員の役割、契約相手の認識に対する組織の期待**を考慮に入れる

⑤長期にわたり、できれば**定期的に計画**される
→活動が繰り返され、**新しい従業員及び契約相手も対象**となる

⑥**定期的に更新**して組織の方針及び手順に沿うようにする

⑦必要とされた場合に実施する
→教室での訓練、通信教育、インターネットを利用した訓練、自己学習その他**多様な手段**

管理策の具体的要件として盛り込む

規格要求事項から考慮すべき要件一覧（7点）

考慮すべき要件	具体的にはどうするか？	備考
①各自の責任及びその責任を果たす方法について認識	→自身が行動したこと及び行動しなかったことに対する個人の責任	事例①
②保護すべき組織の情報及び保護する管理策を考慮	組織で保有する重要度の高い情報資産とそれを守るために実施している管理策（ルール）認識させる	事例②
③キャンペーン、及びパンフレットまたは会報	・年末年始、GWや大型連休前の注意喚起 ・ルールブックなどの理解しやすいルールの棚卸し	事例③
④従業員の役割、契約相手の認識に対する組織の期待	情報セキュリティに関する基本的な手順（例：インシデント報告）及び基本的な管理策（例：パスワード設定、マルウェア対応）	事例④
⑤定期的に計画、新しい従業員及び契約相手も対象	年一回の全体研修だけでなく、人事異動や採用に伴う新メンバーへの研修などの対応	事例⑤
⑥定期的に更新	コンテンツはルールの新規、変更に応じて最新化する（法令や内部の方針変更など）	事例⑥
⑦多様な手段	状況に応じ、最適な手段を選択 大規模な組織ではオンライン研修が多い	事例⑦

事例① セキュリティに関する責任と行動要件（案）

具体的な行動要件	具体的な事例	備考
自身が行動したことに対する個人の責任	SNSに会社情報やお客さまなどの機密情報をアップするなどによる情報漏洩に対するビジネスインパクトと個人の責任について明示する	行動したことによるペナルティとして懲罰対応 （ビジネスインパクトに応じた量刑）
自身が行動しなかったことに対する個人の責任	標的型攻撃メールを誤って開いてしまった場合に下記の緊急対応が求められる ・NWからの遮断（拡散防止のため） ・報連相（開いてしまったマルウェアの影響度の把握と注意喚起の水平展開のため）	行動しなかったことによるペナルティとして懲罰対応 （ビジネスインパクトに応じた量刑）

行動した結果責任 → 禁止行為の実行

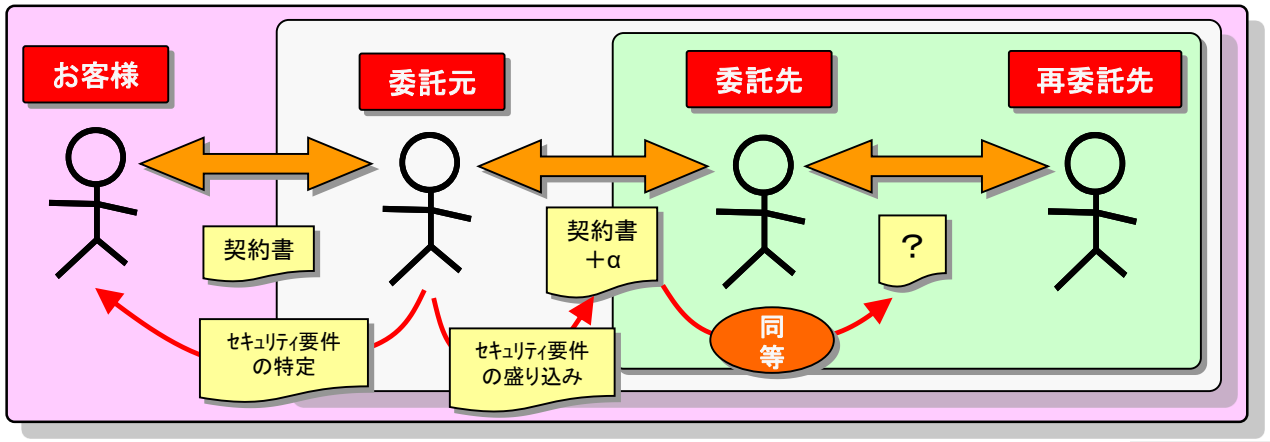
行動しなかった結果責任 → 義務行為の履行違反

結果に応じたペナルティ

・お客様SI案件のPM
・唯我独尊（32歳）
男性、未婚

事例④　従業員の役割、契約相手の認識に対する期待（案）

具体的な行動要件	具体的な事例	備考
情報セキュリティに関する基本的な手順 （例：インシデント報告）及び基本的な管理策（例：パスワードのセキュリティ、マルウェア対応、クリアデスク）	従業員として基本的に遵守すべきセキュリティルールの行動指針に従った対応を期待している 例） インシデント報告、PWD管理、マルウェア対応、クリアデスク/クリアスクリーン、SNS等への書込み禁止など	・全社員向けのセキュリティ研修のコンテンツ ・セキュリティハンドブック ・社内ポータルなどへの情報掲載 ※：委託元としての行動規範（委託先管理含め）
	委託先には業務委託仕様書等にセキュリティ要件を明示し、契約での縛りで実行性について担保する	委託元→委託先の現場管理者→業務従事者への意識付け（伝言ゲームの様相）



事例⑥　定期的更新

具体的な行動要件	具体的な事例	備考
コンテンツはルールの新規、変更に応じて最新化する（法令や内部の方針変更など）	法改正やガイドラインやセキュリティルールの変更に速やかに対応しないと法律違反や不適合となることから、必要に応じて随時周知徹底する 事例： 改正個人情報対応など規程類の改定や業務マニュアルの見直しなどを実施すると共に社内ポータル等に掲示することで意識付けを実施する必要がある	年1回 上期/下期にイベント設定（四半期毎）

法改正・ガイドライン

法改正やガイドラインの変更等については施行までに一定の猶予期間があるので、関連組織やセキュリティ団体のサイトを**定期的にモニタリングする（半期毎、年次）**

社会的に影響のあるセキュリティインシデント

ニュースをモニタリングすると共にセキュリティ団体のサイトを**定期的に確認する（随時）**

7.2 力量について

規格要求事項から導かれる管理策の要件整理（一般社員）

規格　7.2

力量

力量を備えていることを確実にするために適切な教育、訓練

必要な力量の決定

業務遂行に必要な力量

現状の力量

処置の有効性を評価
&
文書化

力量の証拠

一般社員向けの業務スキルとセキュリティスキル

力量の分類	力量の設定＆教育/訓練		力量の評価
ビジネスを推進する業務スキル	○ビジネスを推進する業務スキル ＜事例＞営業職 ・ヒアリング能力、交渉・提案力、課題発見力、事務処理など	現場サイドを中心に教育/訓練を実施	社内の評価指標に基づく社内指導者による力量把握など
セキュリティを遵守するスキル	○セキュリティを遵守するスキル ・ISMS/PMSの規程 ・セキュリティー般知識 ・インシデント対応力など	事務局を中心に全社員研修などを実施	研修後の効果測定や標的型攻撃メール訓練での対応のモニタリングなど

規格要求事項から導かれる力量の決定＆評価について

規格　7.2

力量

力量を備えていることを確実にするために適切な教育、訓練

必要な力量の決定

業務遂行に必要な力量

現状の力量

処置の有効性を評価
＆
文書化

力量の証拠

知る　理解　出来る能力

力量

業務	タスク	教育	力量の証拠	
		研修・OJT	評価者	資格取得
○○業務	タスクＡ	受講済み	○	ベンダ資格 社内資格
	タスクＢ	受講済み	○	
	タスクＣ	受講済み	△	
	タスクＤ	未受講	×	

力量の決定　教育、訓練　力量の評価・証拠

一般社員
の
力量設定

事例： 力量設定について

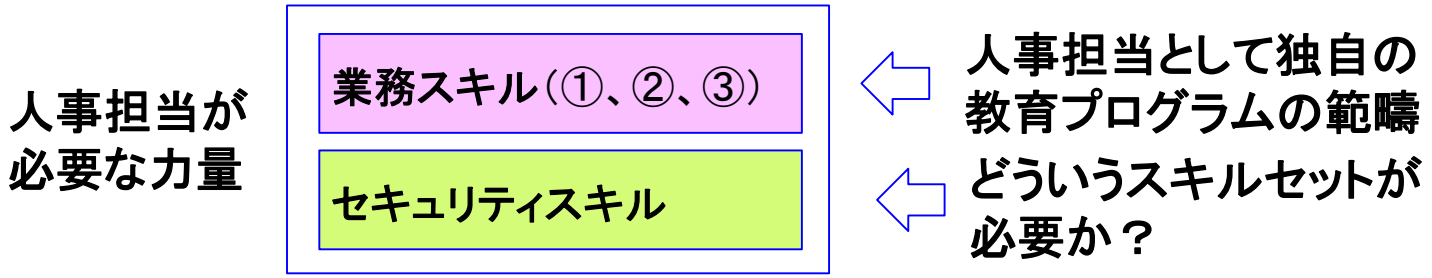
力量設定についての考え方について人事担当をユースケースに事例化

〇人事担当のスキルセット

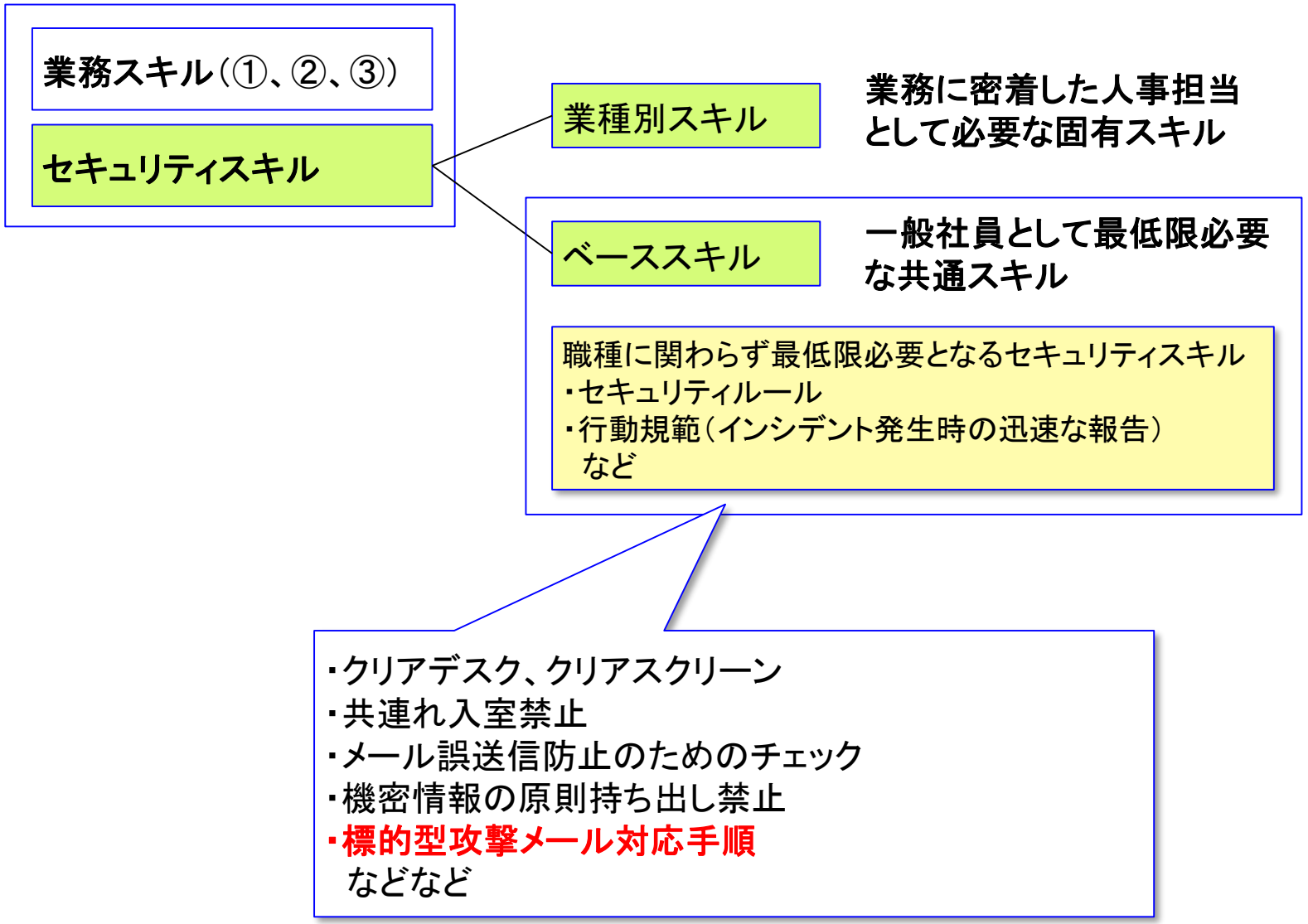
①法律関係の知識
労働基準法や労働安全衛生法、社会保険、雇用保険、個人情報保護法等を熟知

②コミュニケーション能力
人間関係調整能力と問題解決能力です。人事は様々な社員と折衝

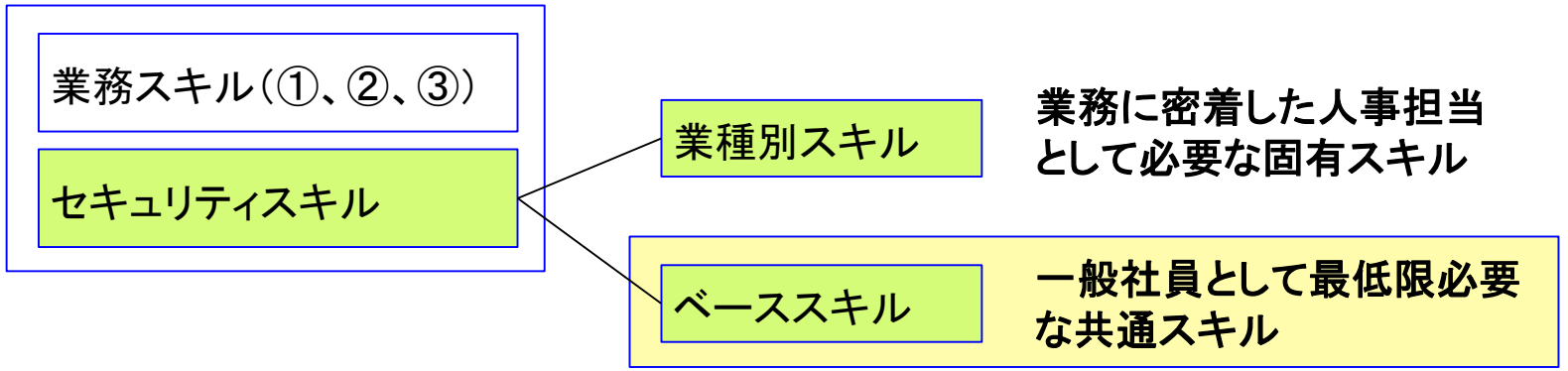
③モラル（守秘義務など）
秘密情報を扱うことが多い人事担当は守秘義務遵守はもちろんのこと
情報の漏洩等がおこらないように細心の注意が必要



人事担当が必要な力量 （ベーススキル）



人事担当が必要な力量 （ベーススキル）

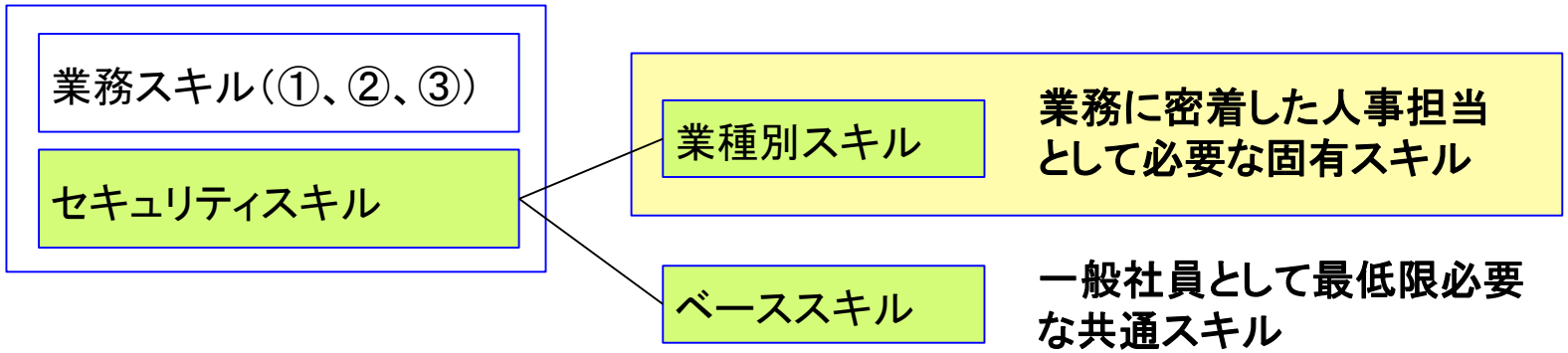


事例：**標的型攻撃メール対応手順**

標的型攻撃メールに対して理解するだけでなく、適切な対応が実践出来るスキルと意識づけ

①標的型攻撃メールについての全体概要
②標的型攻撃メールのリスクについて理解
③標的型攻撃メールを識別して開かない
④誤って開いた時の基本行動が実践出来る
- NWからの遮断
- 当該PCの隔離
- 報連相

人事担当が必要な力量 （業種別スキル）



事例：

個人情報を常に取り扱う人事担当としては**個人情報保護法やガイドラインを理解**して行動することが求められる
人事業務に従事する前に必要なスキルをすべて習得することが理想であるが、実際には人事異動や派遣社員の交代等でスキルGAPのある従業員が従事するケースは現実問題としてあり得る

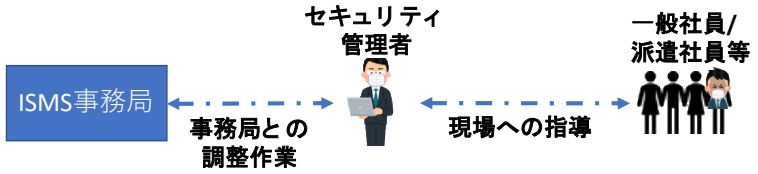
→**業務プロセスへのセキュリティの組み込み**が必要

例）障がい者枠での採用時に**障がい者手帳などの要配慮個人情報の収集**に該当するが収集にあたり**当事者に承諾を得るなどの管理プロセスを構築**することで新規業務従事者でも一定のレベルの業務遂行が実施出来るようにすることが望ましい

セキュリティ管理者
の
力量設定

事例： セキュリティ管理者の力量設定について（案）

名称	役割	主な業務
情報セキュリティ 管理者	セキュリティ 施策の実施＆指導等の管理	自部門におけるセキュリティ ガバナンスの維持・ 向上 ・ 全社セキュリティ 施策の現場展開（ 外部媒体調査、自己点検、など） ・ リスクアセスメント 支援 ・ インシデント 対応支援 担当内におけるインシデント 発生時の全般的な対応（ エスカレーション、調査・ 対処・ 再発防止策検討・ 実施、担当内注意喚起、情報セキュリティ 事故報告書作成からCISO説明及び承認受領の調整など）



①全社セキュリティ 施策の現場展開
②リスクアセスメント
③インシデント 対応支援
④内部監査/外部審査対応
などなど・・・

説明省略

セキュリティ 管理者の力量レベル設定（ 案）

	事務局		セキュリティ管理者		現場
	◎	＞	○	＞	△
	◎	＞	○	＞	△
	△	＜	◎	≧	○

	作業分類	作業項目	作業内容	
定期	ISMS/PMS審査対応	情報資産台帳の棚卸＆リスクアセスメント	組織として守るべき情報 卸＆再評価	
		内部監査対応（被監査組織）	内部監査受審のための資料の ＆監査対応	
		内部監査対応（監査チーム）	内部監査業務従事	
		外部審査対応（被審査組織）	外部審査受診のための資料の準備	ISMSは毎年 PMSは隔年
	外部記録媒体管理状況報告	機密情報が書込み可能な媒体の棚卸＆管理状況の報告	ハードウェア管理簿、貸出管理簿等の管理状況の確認＆報告書の提出	実施内容を内部で調整が必要
	自己点検	自組織内のセキュリティの遵守状況の確認	居室、プロジェクトルーム等のクリアデスク、クリアスクリーン、ロッカー/書庫の施錠状況などの確認＆報告	

	作業分類	作業項目	作業内容	備考
不定期	規程やルール変更時の周知	セキュリティ規則の現場への展開	セキュリティ規則（新規、変更など）の現場への周知＆意識付け	
	リスクアセスメント対応	自組織内で発生しうるリスク源を特定し、ビジネスへの影響を受容可能なレベルにコントロールする	下記のイベント毎にリスクアセスメントを実施 ア）情報資産や業務プロセスの見直し イ）内部監査、外部審査時の指摘事項対応 ウ）環境の変化 エ）インシデントの発生に伴う要因分析	
	インシデント対応	自組織内で発生したインシデント対応支援やヒヤリハットなどの再発防止対応	インシデント対応支援 担当内におけるインシデント発生時の全般的な対応（エスカレーション、調査・対処・再発防止策検討・実施、担当内注意喚起、情報セキュリティインシデント報告書作成からCISO説明及び承認受領の調整など）	

7.3 認識について

認識とは？

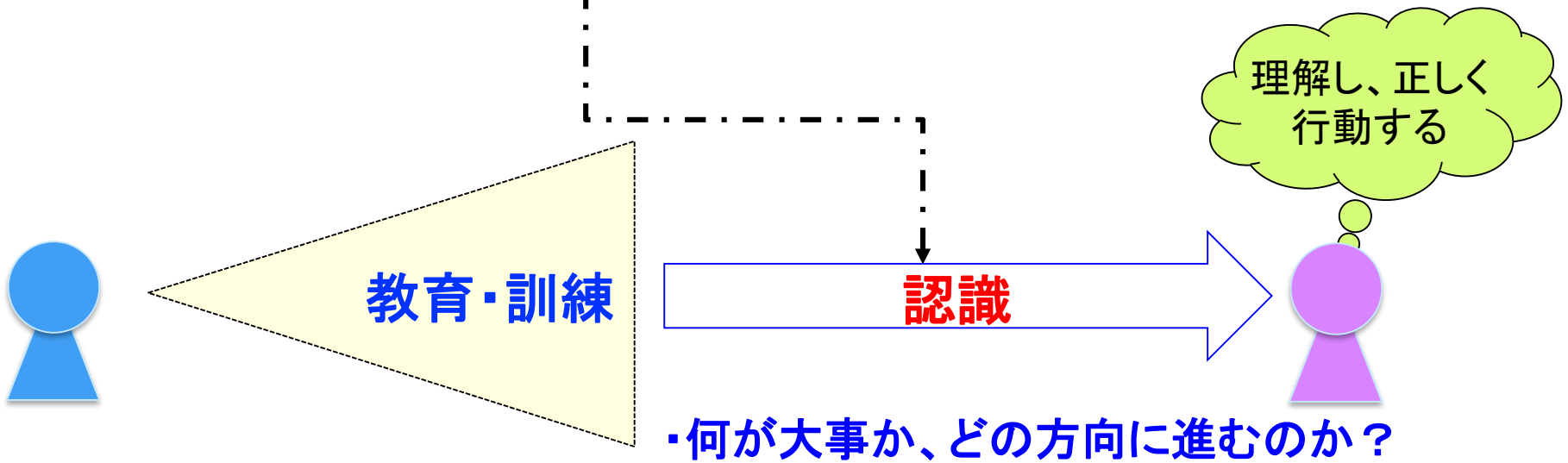
規格　7.3

認識

組織の全ての従業員、関係する契約者

必要な認識

- 情報セキュリティ方針
- ISMSの有効性に対する自らの貢献
- 要求事項に適合しないことの意味



- 何が大事か、どの方向に進むのか？
- 自らの役割や求められる行動
- 行動しなかった影響など（リスク、ビジネスインパクト）

認識とは？

100%　理解

必要スキル習得100%

認識

知る　理解　出来る能力　正しく行動

力量

スキルレベル

- 人に指導できる 
- 一人で実施できる 
- 指導されながらできる

十分な力量

認識あり	正しく行動（期待通り）
認識不足など	行動しない、誤った行動（リスクが発生）

効果的に認識させる方法論

日常の業務における問題意識、危機意識の育成

教育・訓練やISMS活動を通じて醸成

a）情報セキュリティ方針
b）ISMSの有効性に対する自らの貢献
c）要求事項に適合しないことの意味

認識を高めるための活動

- 意識づけのリマインドメールなど
- アンケート＆フィードバック
- KY−mtgによるディスカッション
- 同業他社のインシデント事例の共有

- 全社セキュリティ研修
- 内部監査/外部審査対応
- 案件毎のリスクアセスメントなど

効果的に認識させる方法論

真に認識してもらうためには・・・

ルールは組織を守るため
だけでなく、
従業員を守るためにある

a）情報セキュリティ方針
b）ISMSの有効性に対する
　自らの貢献
c）要求事項に適合しない
　ことの意味

教育・訓練やISMS活動を通じて醸成

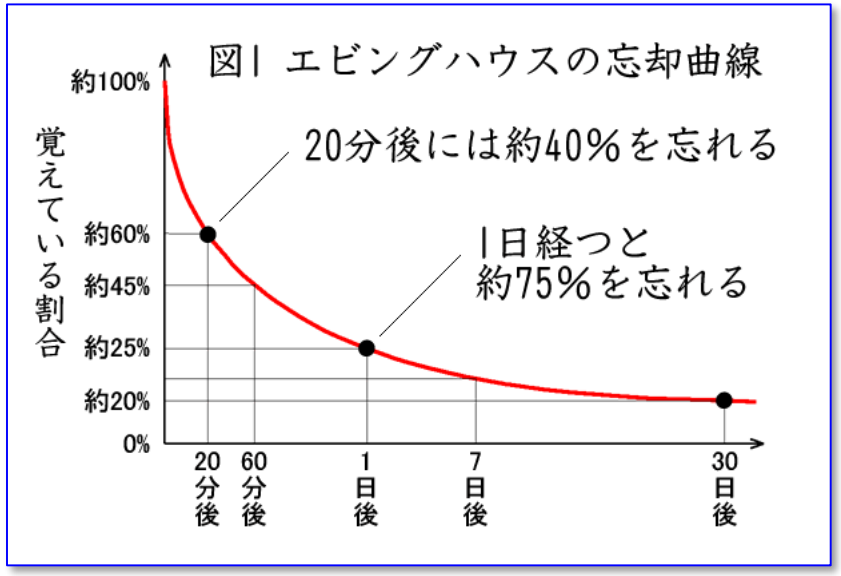
日常の業務における問題意識、危機意識の育成

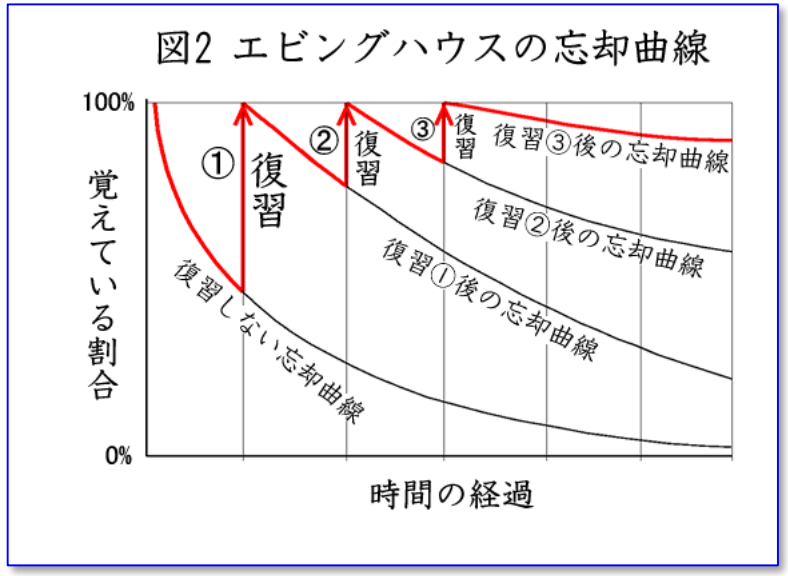
各社の実践事例に学ぶ

忘却曲線
との戦い

忘却曲線との戦い・・・

一度だけの教育・訓練だとすぐに忘れてしまうので、復習を繰り返すことで必要な力量や認識を身につけることができるはず・・・





https://www.jikuukan.ac/web/guide/aex1.php

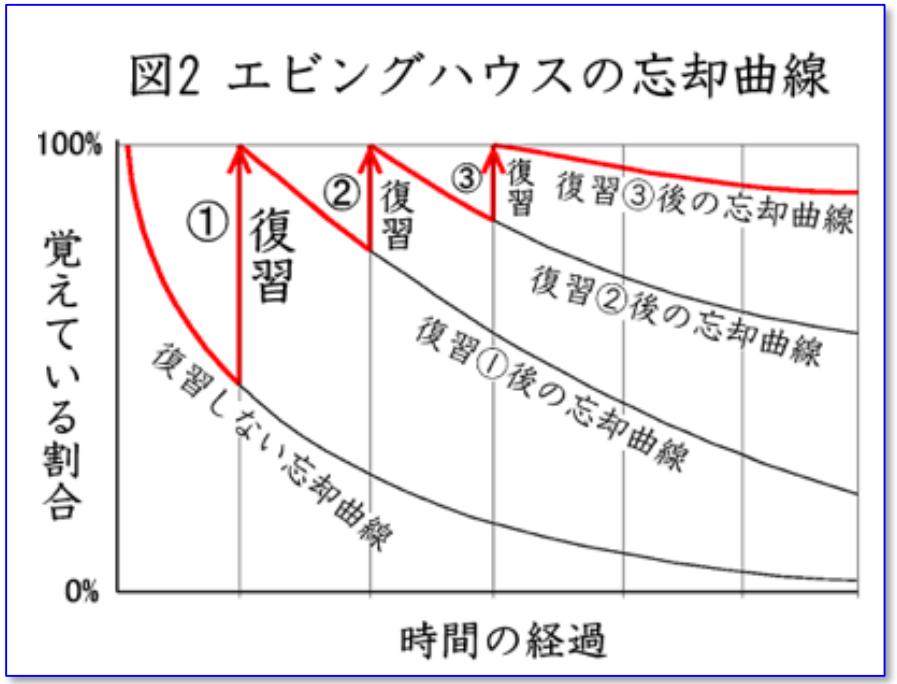
忘却曲線との戦い・・・どうするか？

1．忘却曲線とどう戦うか？（方法論）

・業務に密着した研修ならば**OJTにて繰り返し**身に着ける

・業務に密着していない研修ならば**事後課題**を設定

必ず忘れるという前提条件で研修メニューの設定が必要



忘却曲線との戦い・・・どうするか？

2. 具体的にはどうする？（具体論）

・研修後何もしないとすぐに忘れてしまう

・復習としてテキストを読み返すだけではすぐに忘却・・・

①研修＋事後課題の提出

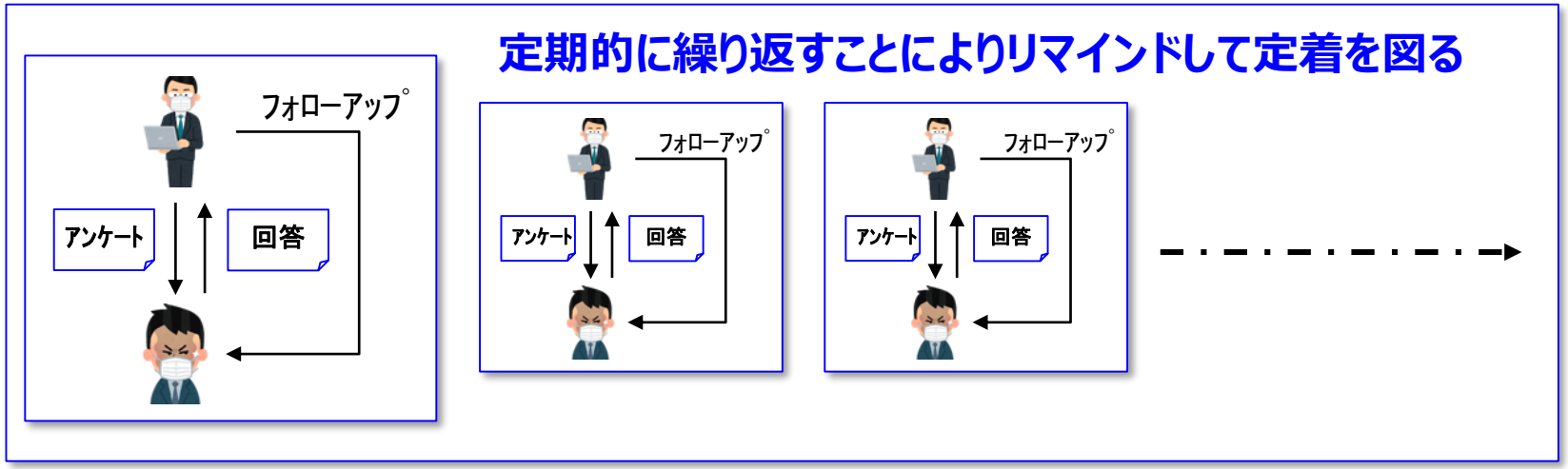
→事後課題で振り返り（考える）が発生することで再学習効果が期待
→単純な復習だけではなく考えて答えを導くことで身に付く（忘れにくくなる）

②研修＋OJT＋OJT・・・OJT

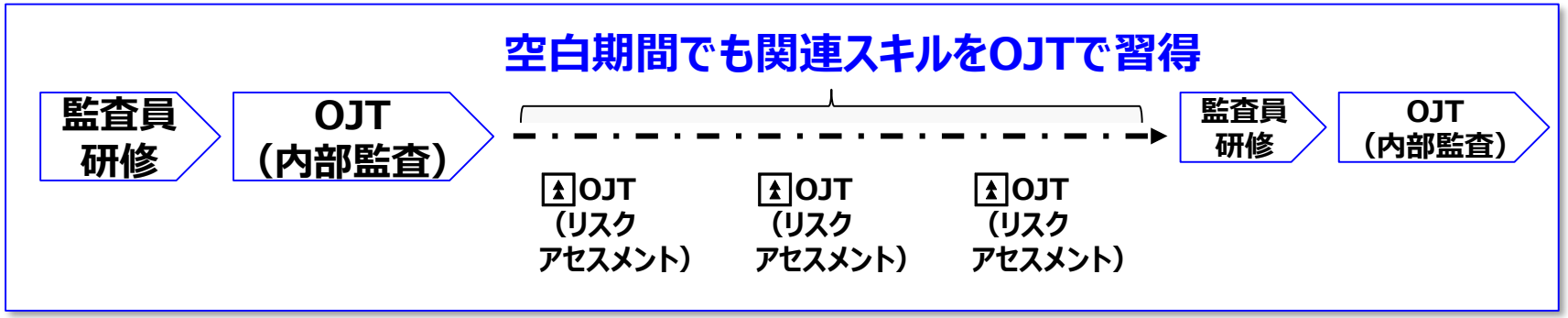
→直接関係しないが関連する業務や要素となる業務に従事

忘却曲線との戦い・・・どうするか？

事例1：毎月のセキュリティアンケート&フォローアップの実施



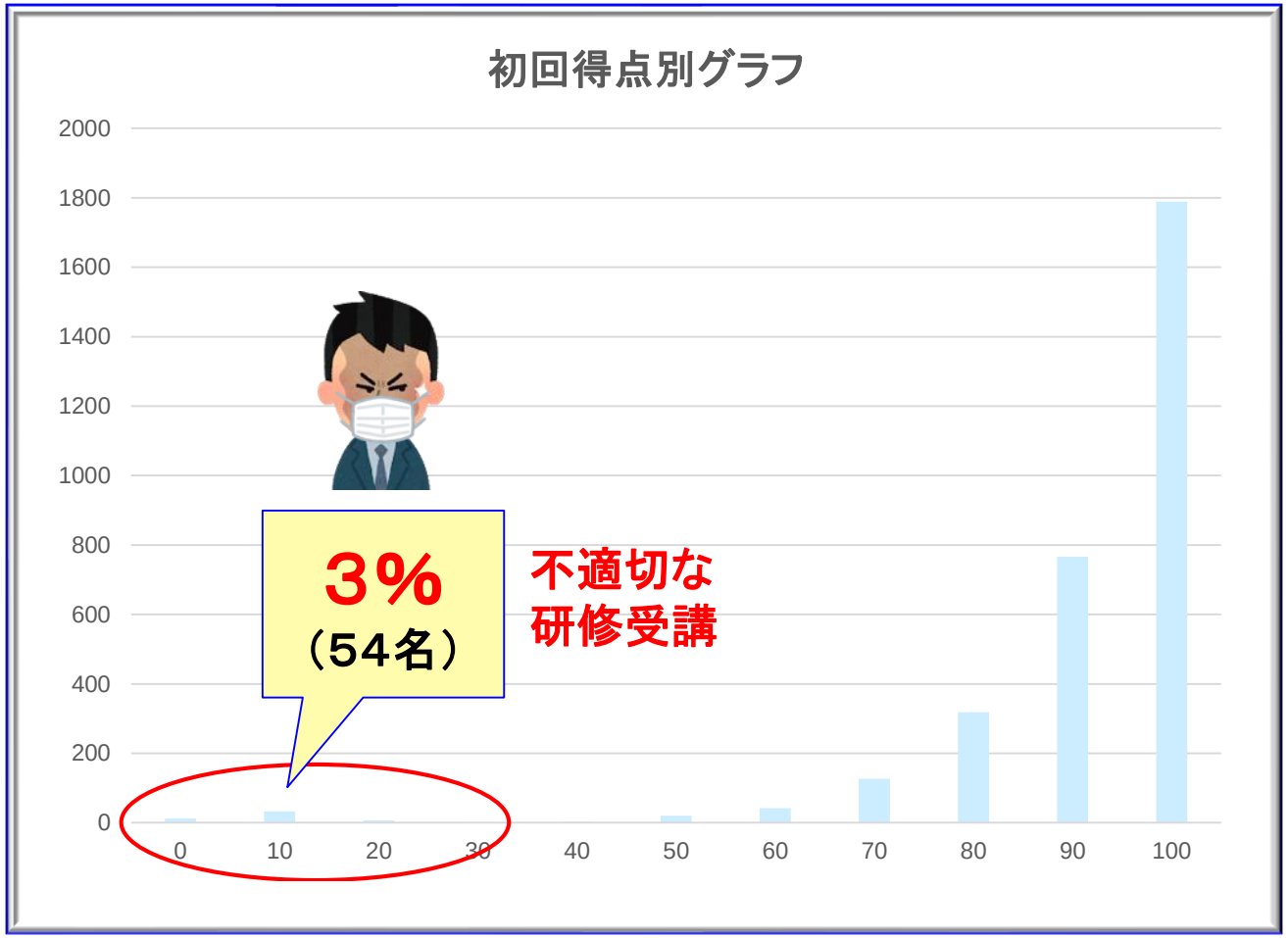
事例2：内部監査員



ネガティブ従業員との戦い

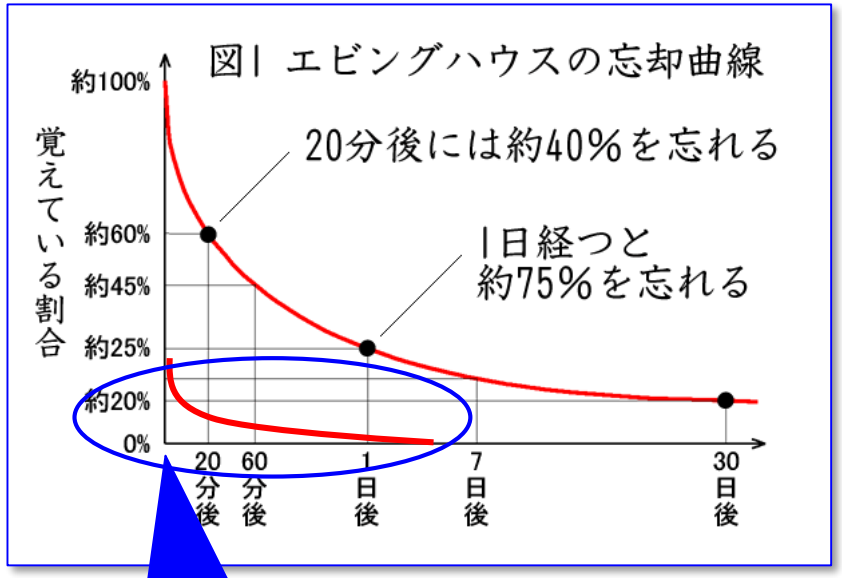
ネガティブ従業員の存在に対してどうするか？

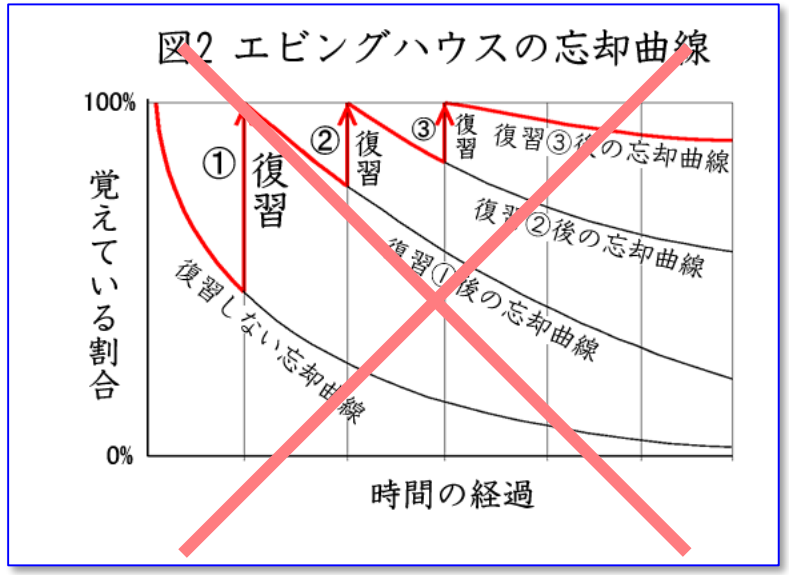
合格（100点）まで何度も受講するシステムとなっているA社の事例だが、データを分析すると**初回時に何も考えずに回答して、以降間違ったところだけ総当たりで回答するという行動パターン**が一定数見受けられる



ネガティブ従業員との戦い・・・

ネガティブ従業員は100%スタートではなく、20～25%スタートとなることから復習の繰り返しは効果的ではない・・・

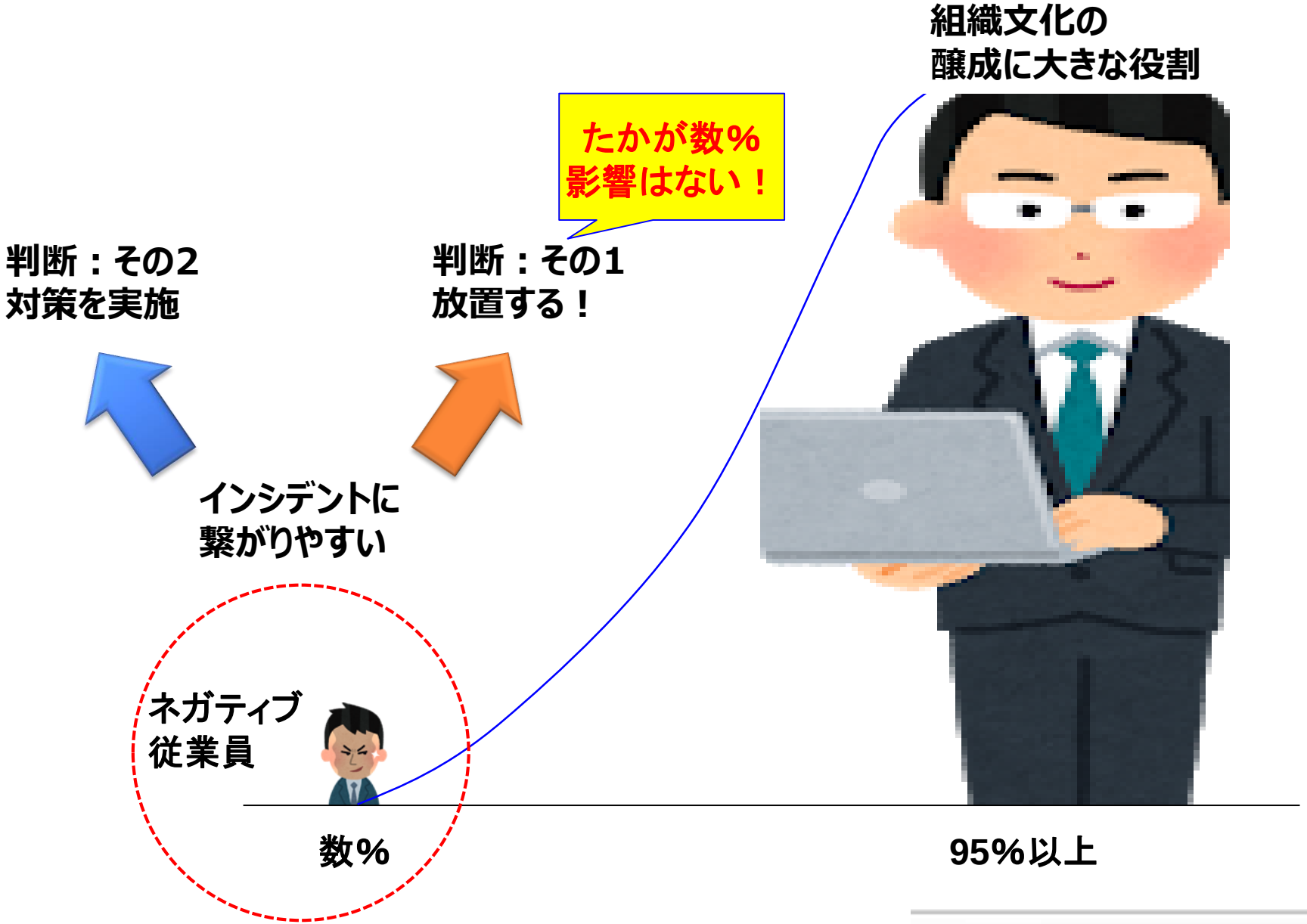




ネガティブ従業員のスタートライン

https://www.jikuukan.ac/web/guide/aex1.php

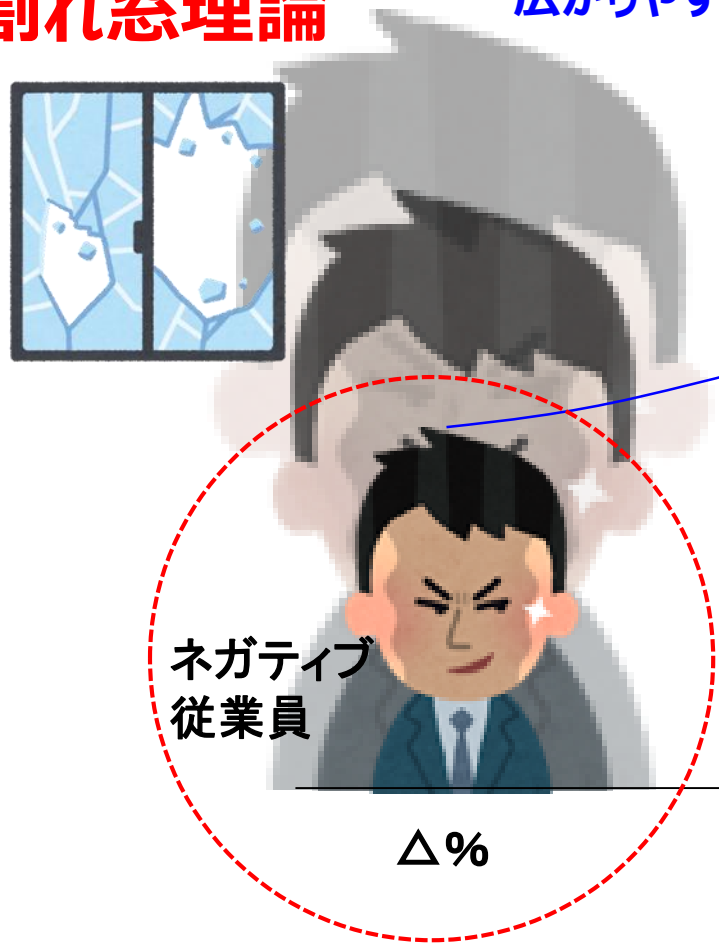
ネガティブ従業員との戦い・・・



ネガティブ従業員との戦い・・・　放置した結果（想像）

割れ窓理論

悪い影響ほど
広がりやすい



ネガティブ
従業員

△%

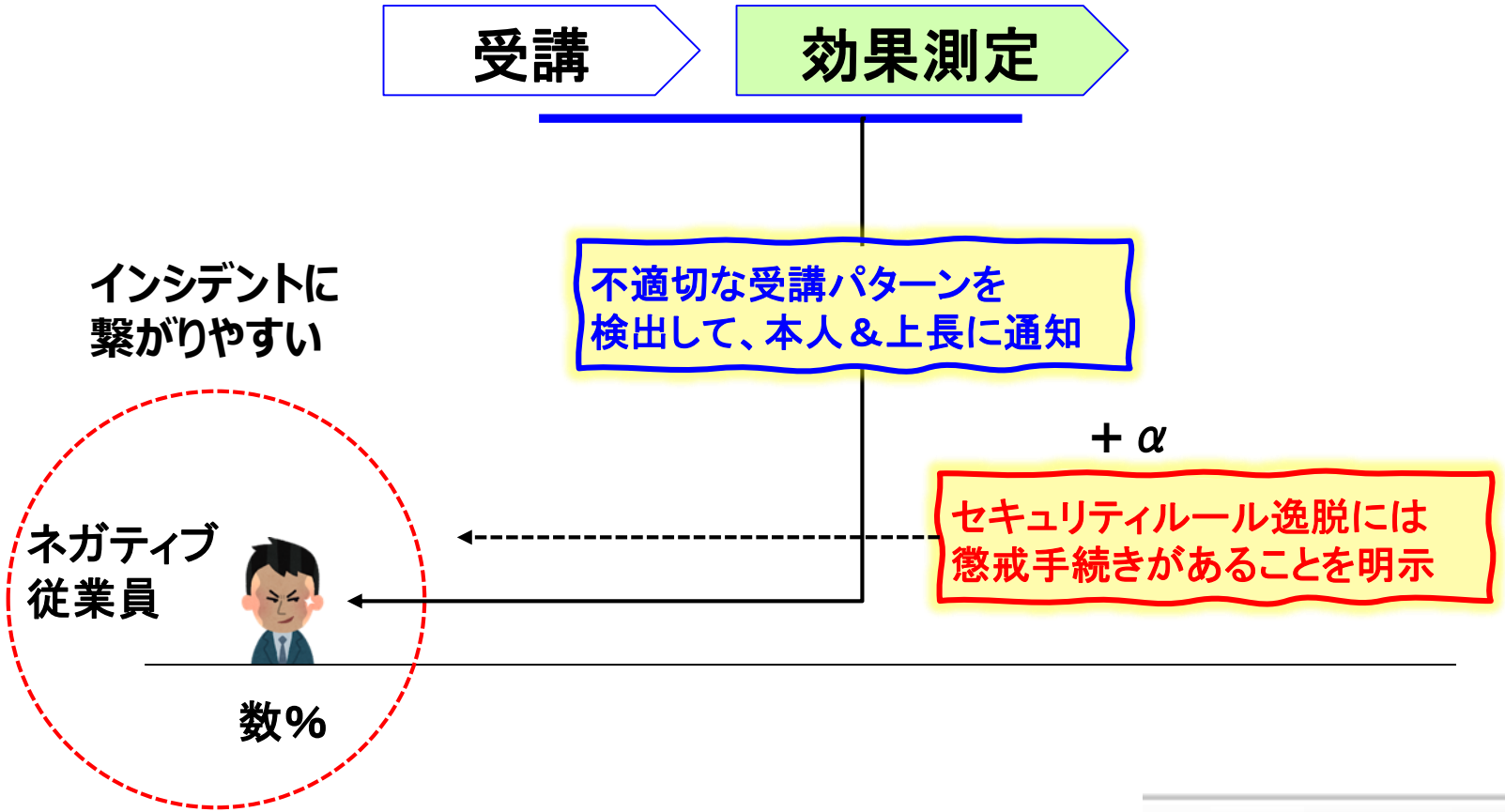
組織全体のセキュリティ
ガバナンスの低下

〇%以上

ネガティブ従業員との戦い・・・　対策案

○太陽　→ 魅力あるコンテンツの提供

○北風　→ 受講状況をモニタリング＆通知＆指導
→ 懲戒手続きの明示



適切な行動、不適切な行動の背景・・・ネガティブ従業員

A：理想的な従業員（十分な力量＆正しい認識）が適切な行動

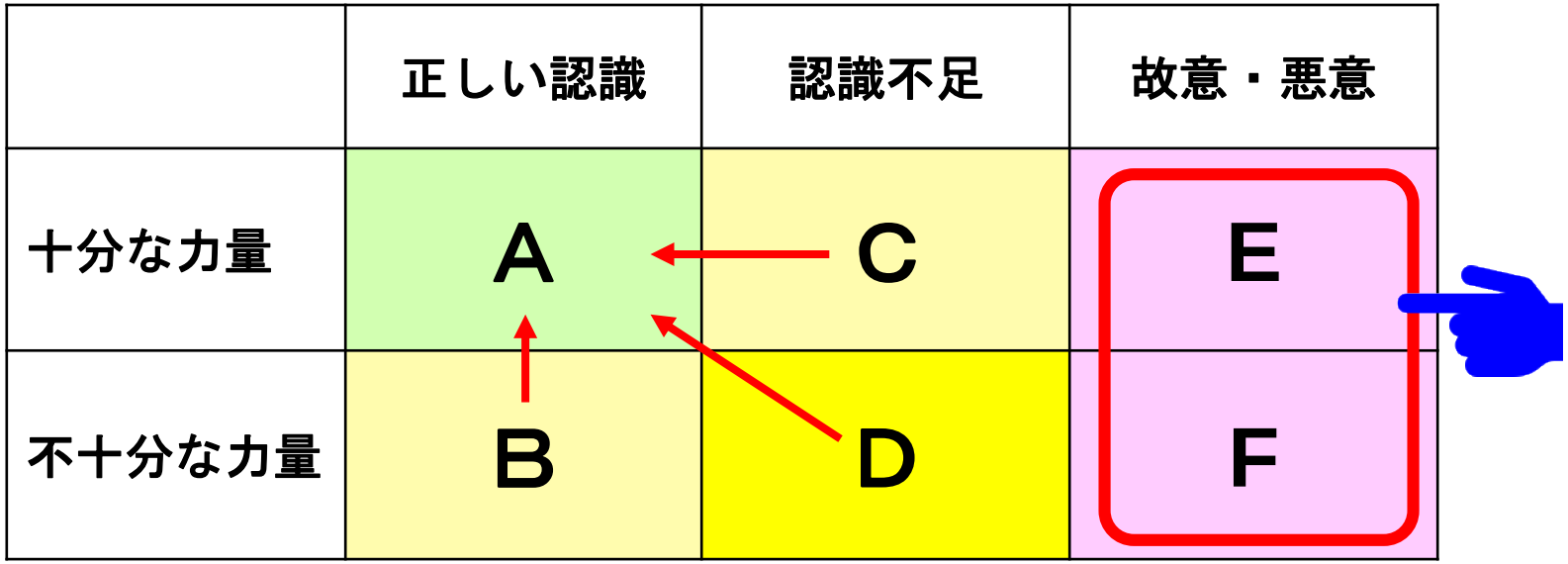
B：力量は不十分だが、正しい認識を持って行動

C：十分な力量を持っているが、認識不足で不適切な行動

D：力量不足・認識不足で不適切行動

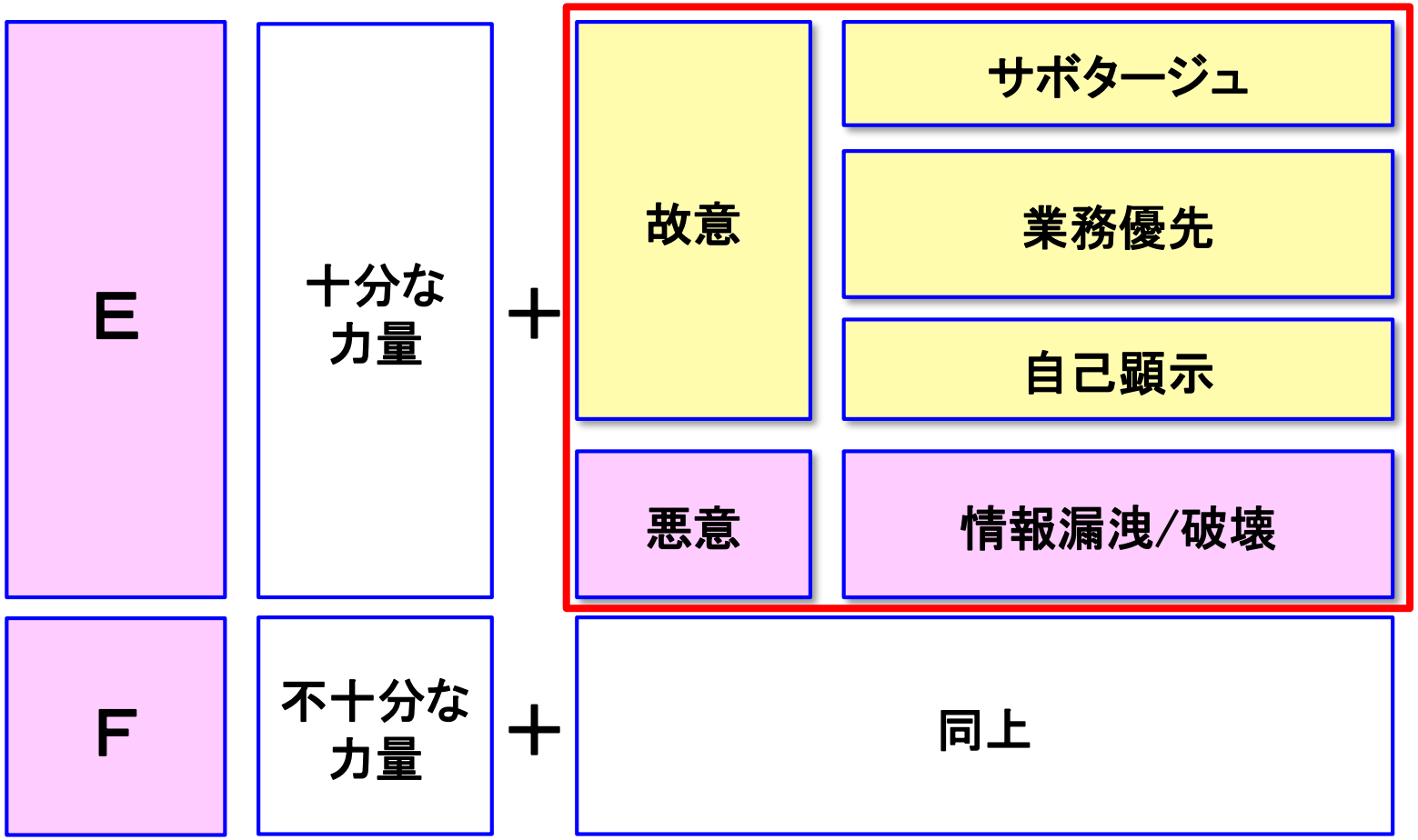
E：十分な力量を持っているが、故意・悪意を持って不適切な行動

F：不十分な力量だが、故意・悪意を持って不適切な行動



適切な行動、不適切な行動の背景・・・ネガティブ従業員

E＆F：　故意・悪意を持って行動するパターン



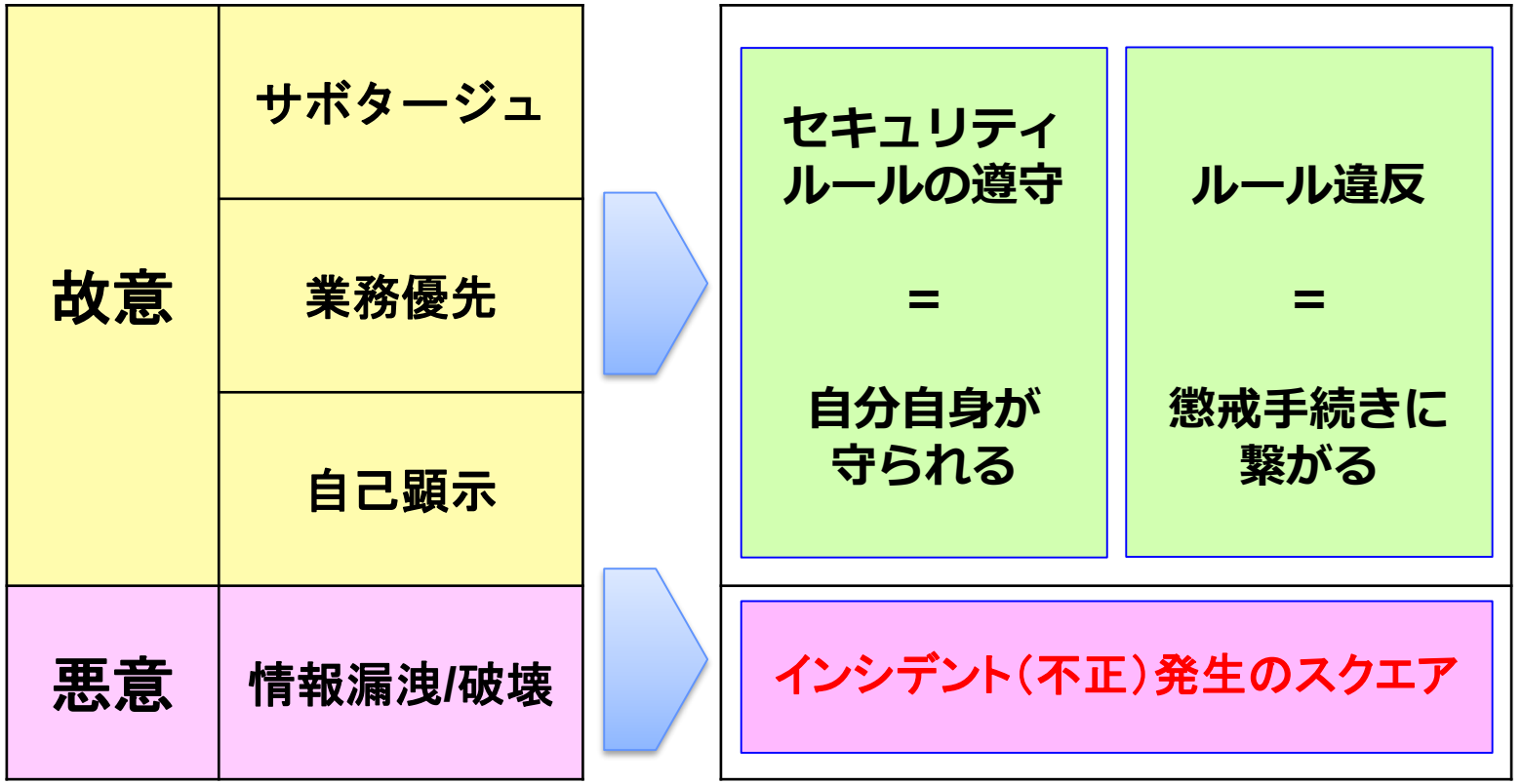
適切な行動、不適切な行動の背景・・・ネガティブ従業員

E&F:　故意・悪意を持って行動するパターン

故意	サボタージュ	・マルウェア感染などのインシデント報告など ・機密情報などの持ち出し申請漏れ
	業務優先	・リスクアセスメントを実施しないで、新サービスを開始する ・脆弱性診断をしないでシステムのサービスを開始する ・未許可のBYOD
	自己顕示	・セキュリティ制限の抜け道を探して実行 →ユーザ権限から管理者権限に昇格など
悪意	情報漏洩/破壊	・金銭目的で機密情報にアクセスして盗む ・業務妨害として情報を破壊する →逆恨みや愉快犯

適切な行動、不適切な行動の背景・・・ネガティブ従業員

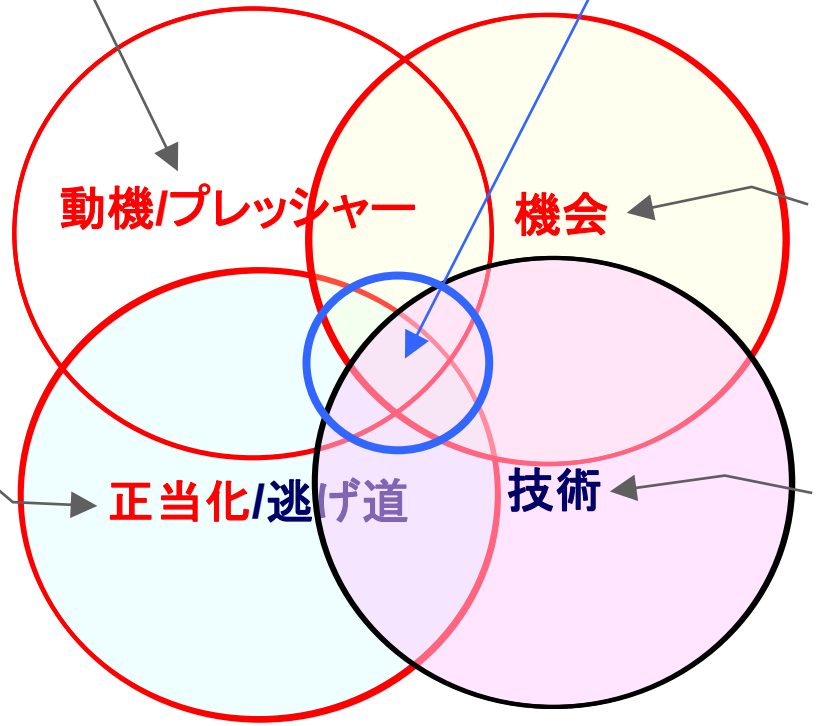
E&F:　故意・悪意を持って行動するパターン



要因分析のツール： インシデント（不正）発生のスクエア

動機がなければ考えない（不満、不安、金銭的悩み、欲望、利益（見返り）、など、動機となる原因を調査し、観察する）

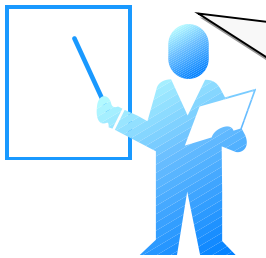
四要素が重なっている部分で問題が発生し易い。



機会がなければ実行できない（機会を与えない）

自己正当化と逃げ道がなければ実行し難い（監視、検知の仕組みと、記録、報告の徹底を行う）

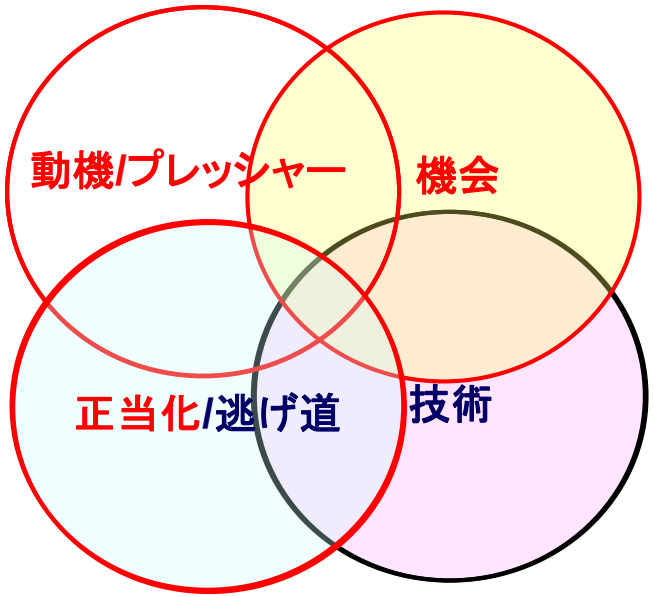
技術がなければ実行できない（高度な技術で防御するか、管理者以外には変更できない仕組みとする）



不正のトライアングル（赤〇の項目）は、米国の犯罪学者であるD.R.クレッシーが、人間（犯罪者）の心理面を研究して導き出した理論ですが、情報セキュリティの面からみると、トライアングル理論に、「技術」や「逃げ道」などを追加することで、より効果的にインシデントを防止できる可能性があります。

必要な力量があっても不適切行動した要因は？

唯我独尊さんの深層心理



・お客様SI案件のPM
・唯我独尊（32歳）
男性、未婚

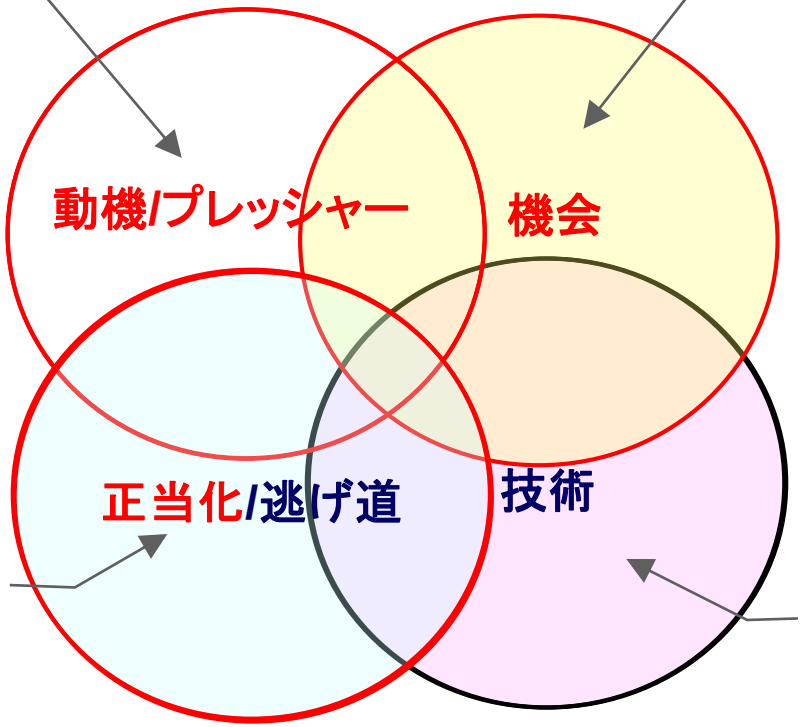
WHY３・・・

必要な力量があっても不適切行動した要因は？

唯我独尊さんの深層心理

・セキュリティルールを守ると効率が悪い
・納期が迫っている

・承認機能が働かない
手続きのプロセス不明
・チェック機能が働かない
（手続きしなくてもばれない）



・ルール設定に穴がある
（抜け道）
・自分だけは大丈夫という過信
・

・技術があり、制限を回避して実行出来てしまう

・ルールの軽視
・ばれない
・本来の意味の理解不足

レセプターを
開く

レセプター [receptor]とは？

生物学用語で、細胞が情報を受信する器官のことを言う。受容体、受容器。

人間の細胞はお互いにコミュニケーションを交わしている。コミュニケーションを交わすためには、他の細胞から発信された情報を受信する器官が必要になる。この受信する器官をレセプターと呼ぶ。

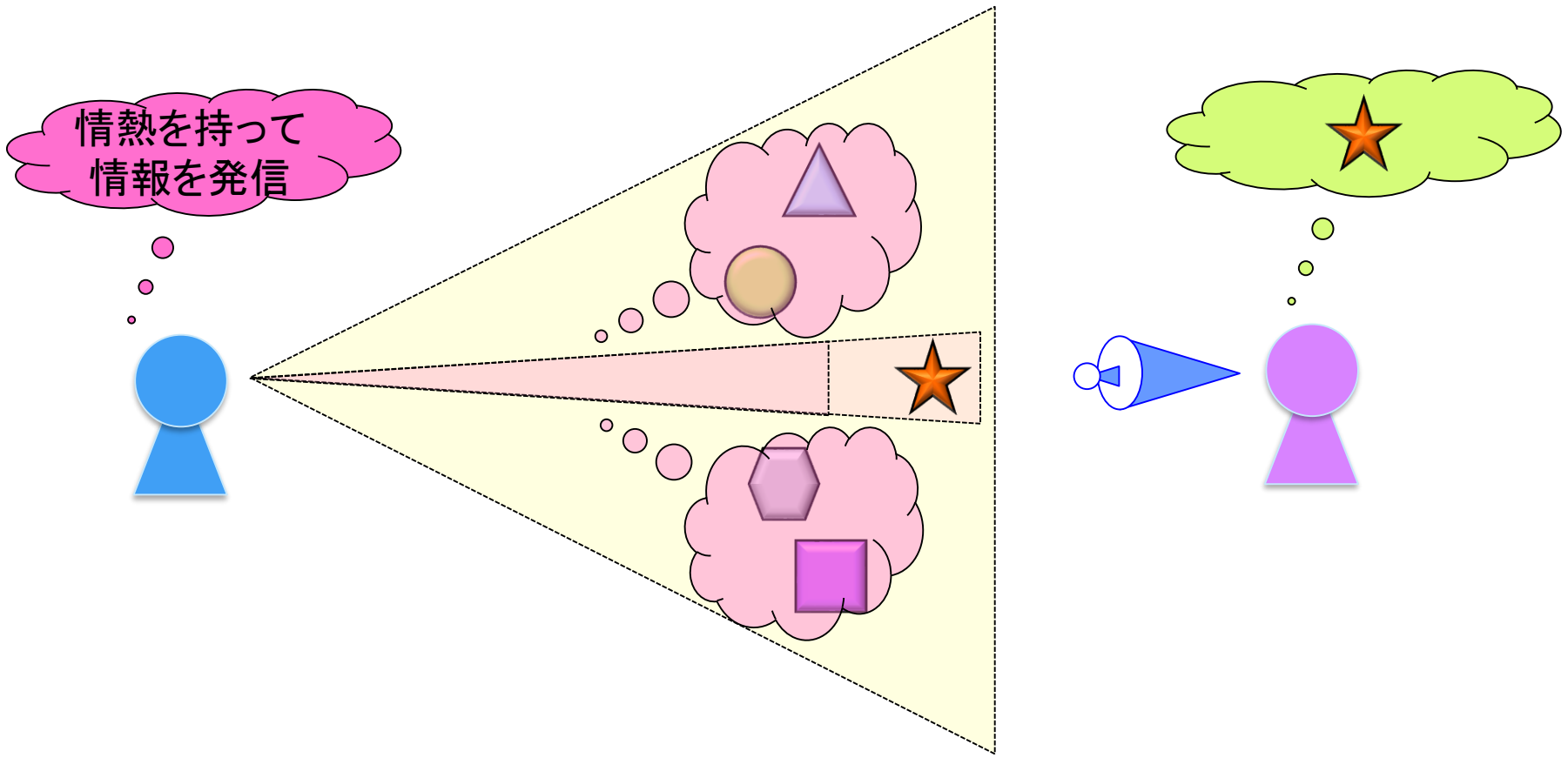
レセプターの特徴は、ただ単にやってくる情報を受け取っているのではなく、**受け取ると決めた情報だけを受け入れる**こと。

人間同士のコミュニケーションにも同じことが言え、**きちんと情報を伝えるには、そのことについて相手がレセプターをもっているかどうかを確かめる必要がある**。

引用：レセプター [receptor]:コーチング用語集
https://coach.co.jp/30/-receptor-20160830.html

情報の共有（･･･伝えたつもり）の誤解

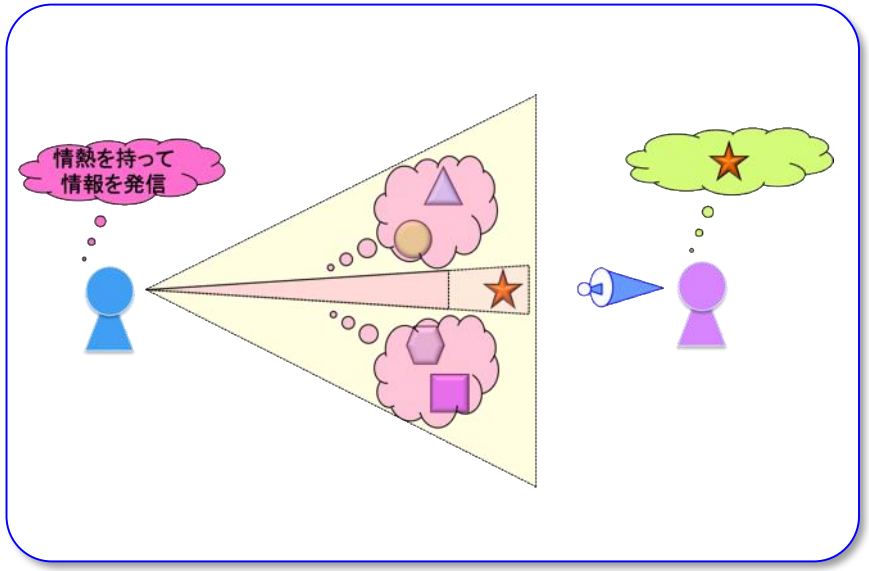
一方的に情報発信しても受け取り側でレセプターが閉じていると
断片的な情報だけしか伝わらない！



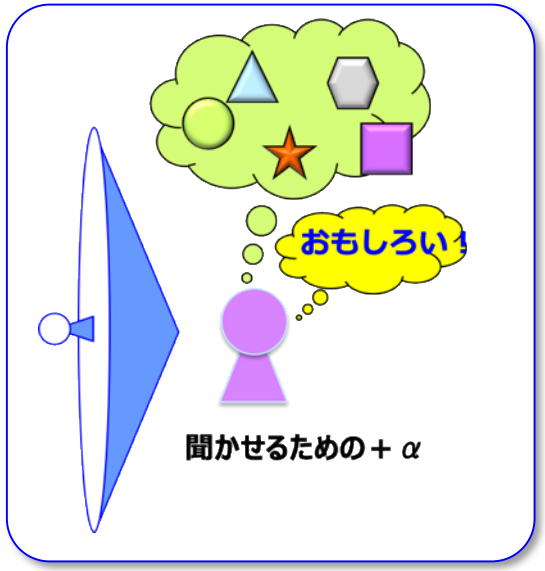
：レセプター

レセプターを開かせるにはどうする？

BADな状態



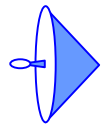
GOODな状態



〇北風
- 研修状況が個人毎に分析していることを認識させる
- 懲戒手続きを認識させる

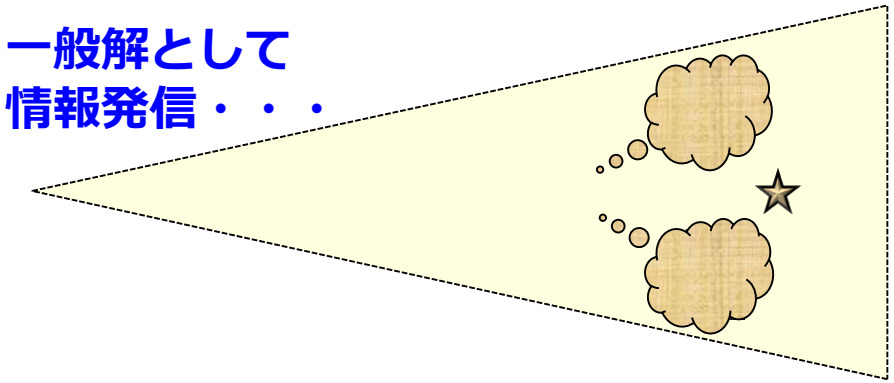
→自分の不利益になること（自分自身に損害が発生する）を明確に認識させる
会社のダメージだけでなく、自分自身が大変な目に遭う

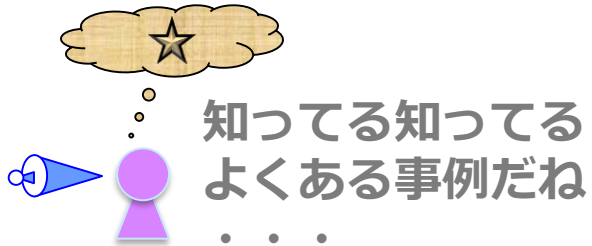
〇太陽
- 出来るだけ身近な事例を引用することで興味を持たせる


：レセプター

事例：レセプターを開かせる・・・

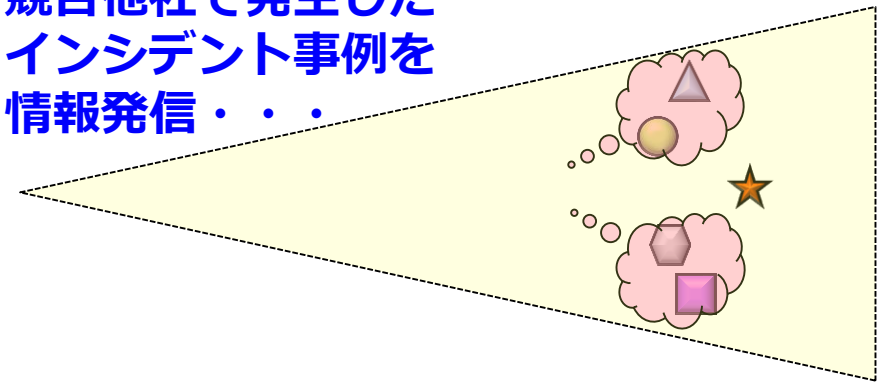
一般解として
情報発信・・・





具体的かつ身近な事例

競合他社で発生した
インシデント事例を
情報発信・・・



まとめ

規格要求事項から紐解く　＆　各社の事例から学ぶ

規格要求事項から紐解く

規格A.7.2.2

情報セキュリティの**意識向上**、**教育及訓練**

組織の全ての従業員、関係する契約者

適切な、**意識向上**のための**教育及び訓練**

27002実施の手引き

規格　7.2

力量

力量を備えていることを確実にするために適切な教育、訓練

必要な力量の決定

業務遂行に必要な力量

現状の力量

処置の有効性を評価
＆
文書化
力量の証拠

力量の分類

- ビジネススキル
- セキュリティスキル

規格　7.3

認識

組織の全ての従業員、関係する契約者

必要な認識

- 情報セキュリティ方針
- ISMSの有効性に対する自らの貢献
- 要求事項に適合しないことの意味

各社の事例から学ぶ

事例①：忘却曲線との戦い

事例②：ネガティブ従業員との戦い

事例③：レセプターを開く

セキュリティ教育の全体像

有効性評価　　業務遂行に必要な　　ほとんどの従業員が

AsIs　全社員受講率100%　→　力量100%　→　正しく行動〇〇%以上　ToBe

力量　　認識＆行動

知る　理解　出来る能力　　正しく行動

人に指導できる

一人で実施できる

指導されながらできる

スキル
レベル

正しい行動

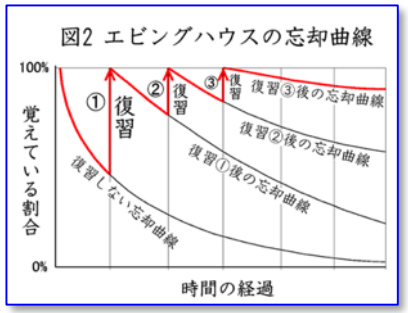
間違った行動

セキュリティ研修
（座学）

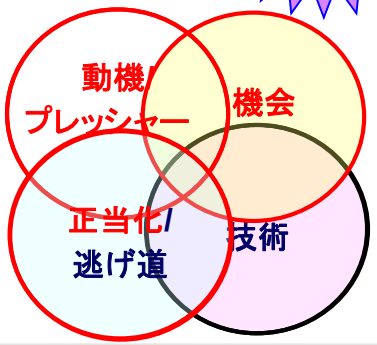
OJT
（実習、業務）

レセプター
を開く

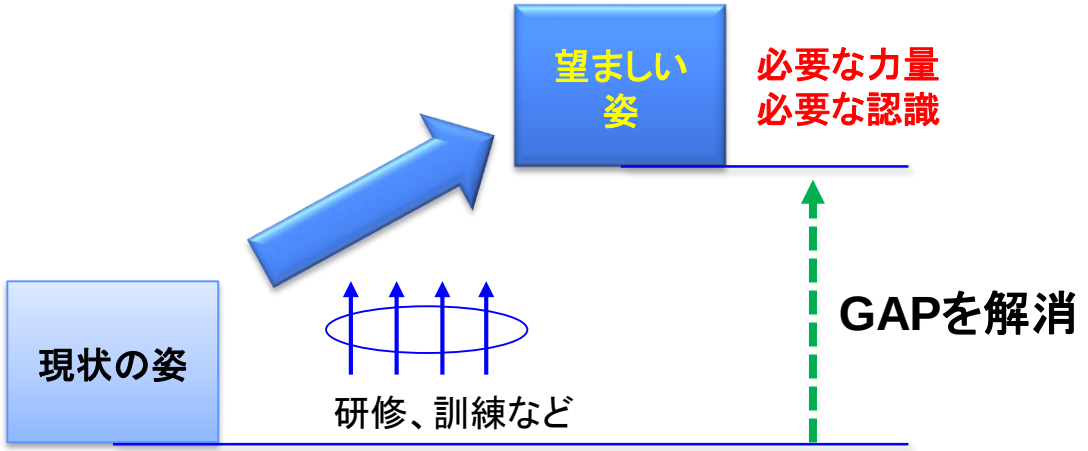
忘却曲線



ネガティブ
従業員
との戦い



参考：多様なセキュリティ教育、訓練



下記の研修、アンケート、訓練などを
年次、四半期、月次、随時等に分類する

①研修（全社セキュリティ研修、監査員研修、技術向上、など）
②訓練（標的型攻撃メール対応、BCP、〇 〇）
③周知メール＆掲示板掲載（新規ルール＆変更、長期休み前の注意喚起）
④アンケート（意識調査＆GAP分析）
⑤職場での小集団mtg（KY-mtgなど）
⑥職場点件（自己点検*1）

*1：Self Check

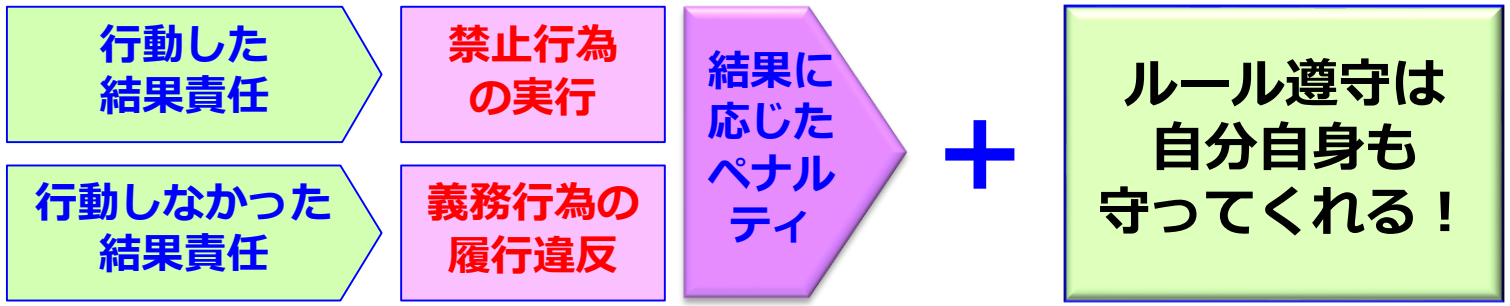
まとめ（伝えたいこと）

○旧来のマンネリ研修＆教育からの脱却について

セキュリティ教育コンテンツにひと工夫

→レセプターを開く
→忘却曲線を意識したリマインド
→北風と太陽

○正しく行動していれば自分も守られる



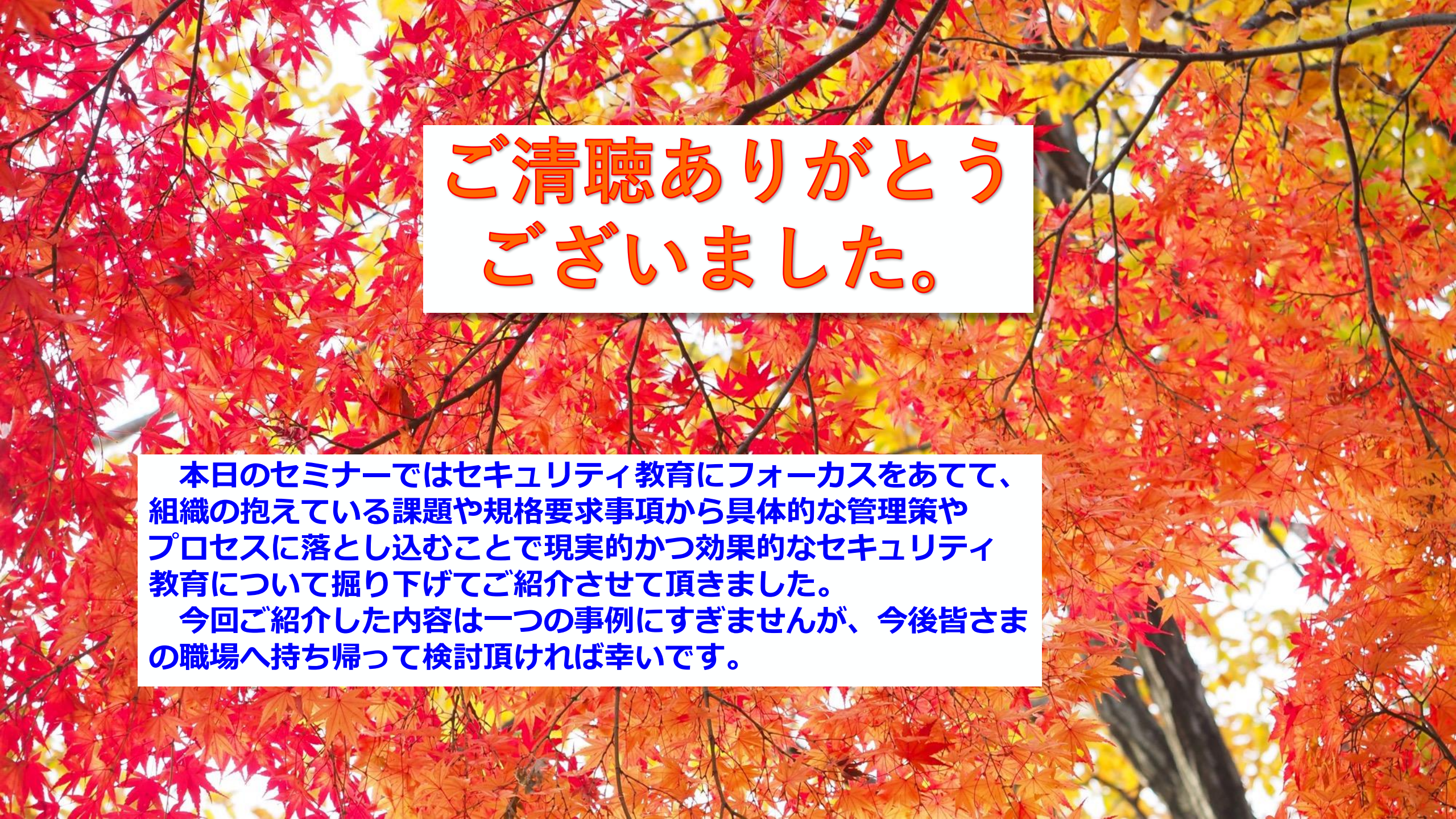
最後に活動の紹介（インプリ研）

皆さんも是非ご参加ください

〇毎月最終木曜日に定例開催（18:00～21:00）
〇前半テーマ1、後半テーマ2を集中討議
〇研究会のテーマだけでなく、各社の疑問や悩みも解決
　（コンサル目線ではなく、実践経験に基づく回答・・・）
〇会員でなくともオブザーバー制度でお試し参加可能

参加のご連絡はJNSA事務局まで・・・

インプリメンテーション研究会（討議模様）



ご清聴ありがとうございました。

本日のセミナーではセキュリティ教育にフォーカスをあてて、組織の抱えている課題や規格要求事項から具体的な管理策やプロセスに落とし込むことで現実的かつ効果的なセキュリティ教育について掘り下げてご紹介させて頂きました。

今回ご紹介した内容は一つの事例にすぎませんが、今後皆さまの職場へ持ち帰って検討頂ければ幸いです。