



JNSA 2021年度活動報告会

日本ISMSユーザグループ 成果報告

**「ISO27002改訂に伴う意見提言と
現場で実践出来る効果的なセキュリティ教育」**

**標準化部会 日本ISMSユーザグループ
リーダー
魚脇 雅晴**

1. 日本ISMSユーザグループとは？
2. 2020年の活動紹介
 - ・ 27002規格改定に対する提案活動
 - ・ 実践かつ効果的なセキュリティ教育
3. 2021年の活動紹介
 - ・ ISMSとゼロトラストセキュリティについての考察（仮）
4. インプリメンテーション研究会へのお誘い

日本ISMSユーザグループとは？

標準化動向

標準化の活用&定着

ISMSの普及・促進

情報セキュリティセミナー

標準化動向
の情報発信

リエゾン参加

SC 27/WG1 小委員会
アドホック会議

貢献

標準化

連携

構築・運用

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

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・・・

2020年の活動紹介

日本ISMSユーザグループの活動紹介 2020年



ISMSの普及・促進

貢献

標準化 連携 構築・運用

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**

■ 27002規格改定に対する提案活動

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

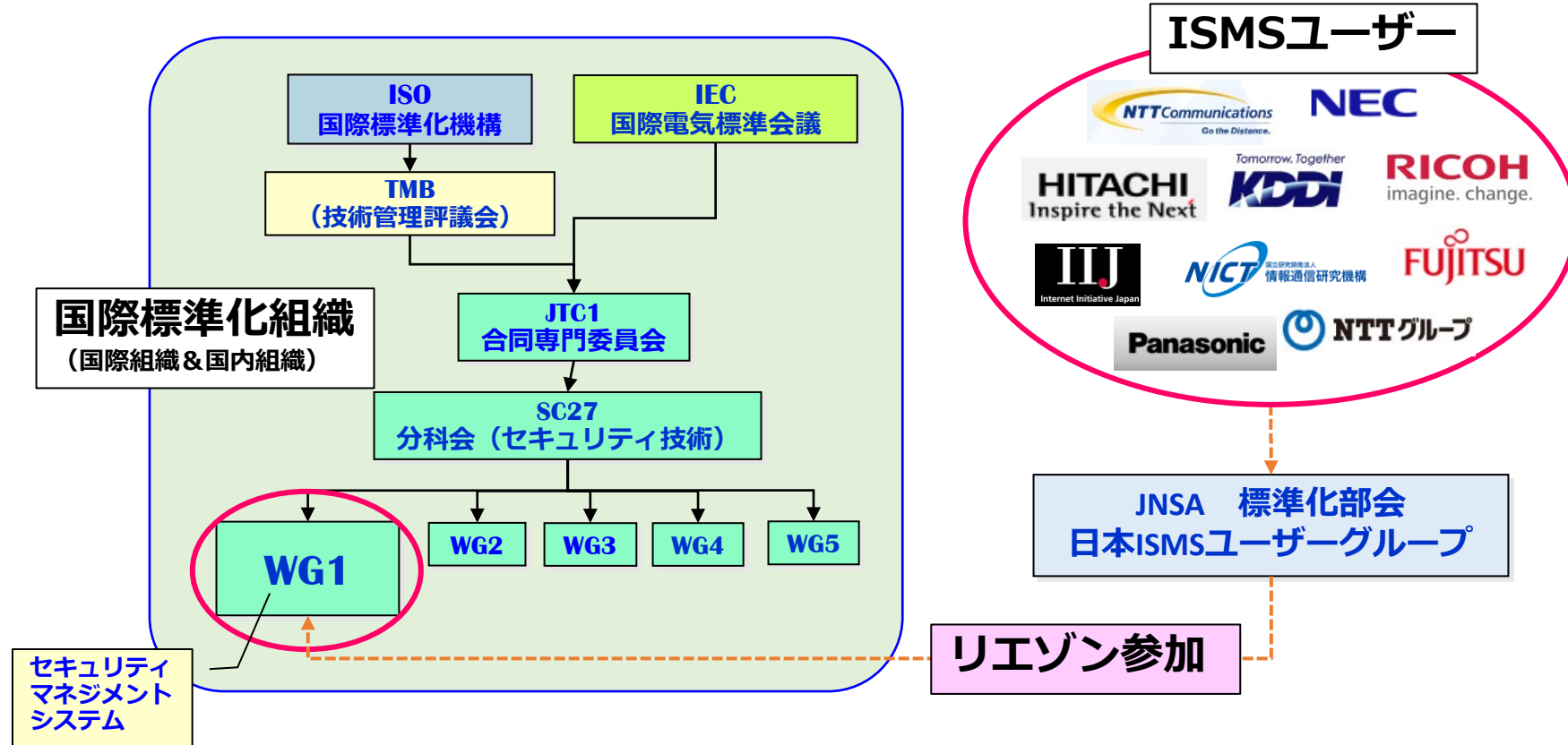
■ 実践かつ効果的なセキュリティ教育

**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・・・**

27002規格改定に対する提案活動

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の提言

日本ISMSユーザーグループと国際標準化組織



従来の活動

リエゾン参加と日本国内
向けの情報発信

2020年の活動

「規格を利用するユーザーの声
を規格の策定や改定に反映」

ISMS-UGのメンバー組織の事例収集

情報セキュリティリスク対策の採用時に

- ①規格要求事項との紐付けに悩む
- ②27002の実施の手引を見ても該当するガイダンスが見つからない



インプリメンテーション研究会での討議

情報セキュリティリスク対策の採用時に

- ①具体的なシチュエーションでの必要性の可視化
- ②標準化（共通化）としての整理

提案



国際標準化組織

前提条件：管理策レベルは国際会議の改定案を採用する
（ISMS-UGの組織で追加の管理策の採用はない）

管理策			提案概要	国内	国際
#1	9.2.4	利用者の秘密認証情報の管理	シングルサインオン（SSO）の導入によるパスワード漏洩リスクの低減	－	－
#2	9.4.1	情報へのアクセス制限	社外ネットワークからのアクセスで同一IDで異なる端末からのアクセスを制限	○	×
#3	9.4.2	セキュリティに配慮したログオン手順	①システムの初期画面に過去のログイン履歴を表示することによって、なりすましによる不正利用を発見する。 ②生体認証を利用する場合には、パスワード等の登録内容を変更できる認証手段と組み合わせた多要素認証とする	×	－
#4	11.2.4	装置の保守	機密データの格納されたICT設備や媒体を障害対応等のために組織外に持ち出す場合及び持出後に廃棄する場合のルールを策定する	○	○
#5	12.3.1	情報のバックアップ	クラウドサービスを利用する場合、利用者の操作ミスによるデータ修復や障害時の復旧を確実にするため、どのようなバックアップサービスが提供されるのかを確認し、必要なバックアップができるようにする	○	○
#6	13.1.1	ネットワーク管理策	認可されない機器の接続防止のために、MACアドレス、機器認証、電子証明書等を利用し排他や検知を実施する	○	○

○＝採用、×＝不採用、－＝提案事由解消（又は国際会議へ提出せず）

NO	管理策	追加案	理由/背景
9.4.2	セキュリティに配慮したログオン手順	生体認証を外部（公衆ネットワーク等）からのアクセスに対する認証手段とする場合には、パスワード等の登録内容を変更できる認証手段と組み合わせた多要素認証とすることが望ましい。	パスワード漏洩（盗難や推測により）した場合、速やかに変更することが被害を防止する手段となるが、生体認証は変更することができない。
13.1.1	ネットワーク管理策	認可されない機器の接続を防止するため、MACアドレス、機器認証、電子証明書等を利用し排他や検知を実施する。	ISO/IEC 27001 : 2005では「A.11.4.3 ネットワークにおける装置の識別」という管理策があったが、ISO/IEC 27001 : 2013ではA.13.1.1に統合されている。しかし、27002 : 2013の実施の手引きにはそれが反映されていない。認可されない機器の接続は防止されなければならないが、現在の規格・実施の手引ではそのコントロールが示されていない。

2020年ISO/IEC 27002規格改定提案研究結果

27002実施の手引改定（追加）検討件数 9件

※内2件は改定27002では
解決する見込み

27002Ad hoc会議への提案は 7件

27002Ad hoc会議への提案結果：採用 6件

国際会議による検討の結果、採用 5件

実践かつ効果的なセキュリティ教育

ベストプラクティクスを検討&提供
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・・・

各企業で長年実施してきているセキュリティ教育ですが、日本ISMSユーザグループメンバー含めて以外と悩みや課題を抱えていることがわかりました。

誰もが抱えている共通的な悩みであるセキュリティ教育について、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**実践かつ効果的なセキュリティ教育**について掘り下げます。

本来はどうあるべきか
規格要求事項を紐解く

+

各社の実践事例から
学ぶ

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

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

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

力量の分類

ビジネススキル

セキュリティスキル

- ・ 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

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・・・

力量設定&有効性評価

役割毎に力量を設定&教育を
実施し、有効性評価

正しく認識させる

正しい認識、
正しい行動（期待値）



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

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

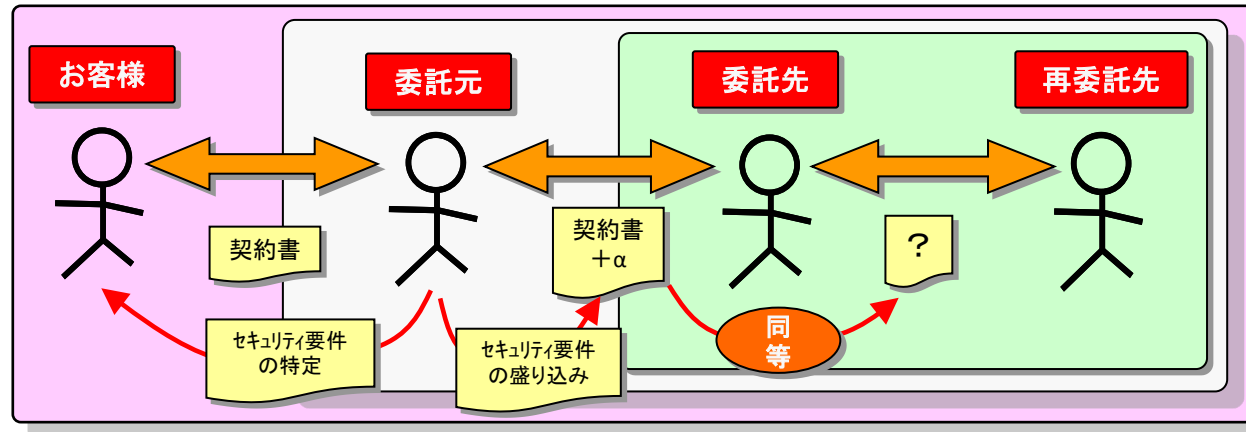
結果に応じたペナルティ

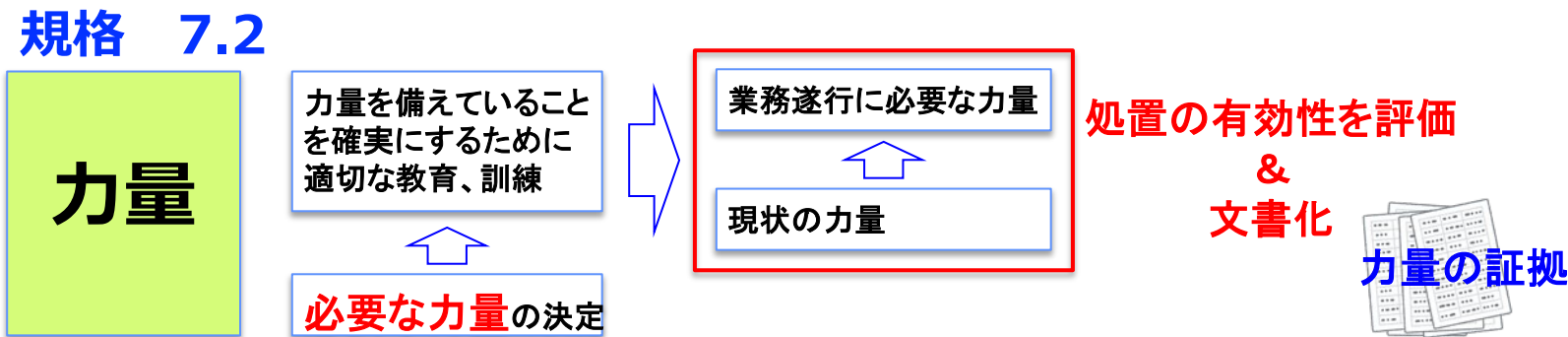


- ・お客様SI案件のPM
- ・唯我独尊

事例④ 従業員の役割、契約相手の認識に対する期待

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等への書き込み禁止など	・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)





一般社員向けの業務スキルとセキュリティスキル

力量の設定 & 教育/訓練			力量の評価
力量の分類	○ ビジネス を推進する業務スキル	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	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

ビジネスを推進する業務スキル

セキュリティを遵守するスキル

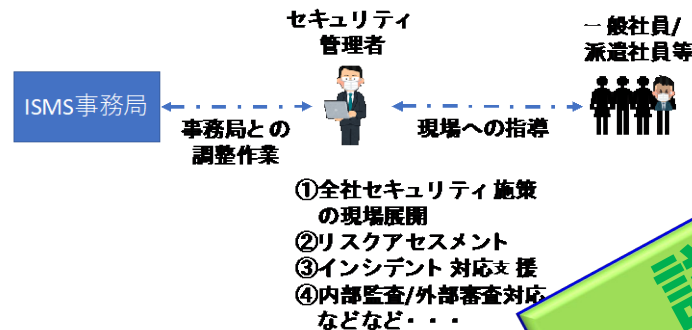
＜事例＞営業職

- ・ヒアリング能力、交渉・提案力、課題発見力、事務処理など

- ・ISMS/PMSの規程
- ・セキュリティ一般知識
- ・インシデント対応力など

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）



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
◎	>	○	>
◎	>	○	>
△	<	◎	≧

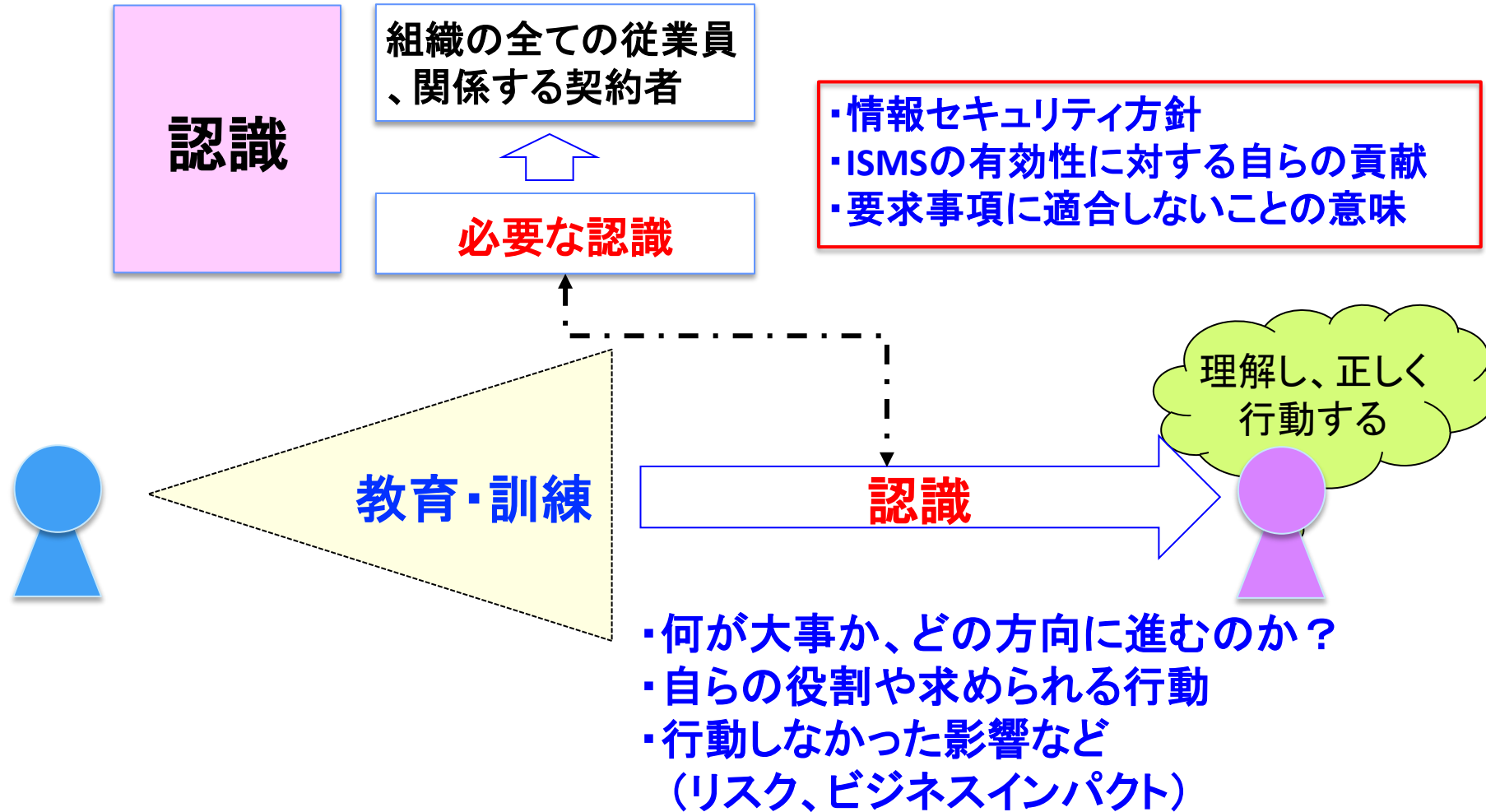
詳細な説明省略

	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の棚卸&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準備&監査対応
		内部監査対応（監査チーム）	内部監査業務従事
	外部記録媒体管理状況報告	外部審査対応（被審査組織）	外部審査受審のための資料の準備
		自己点検	自組織内のセキュリティの遵守状況の確認

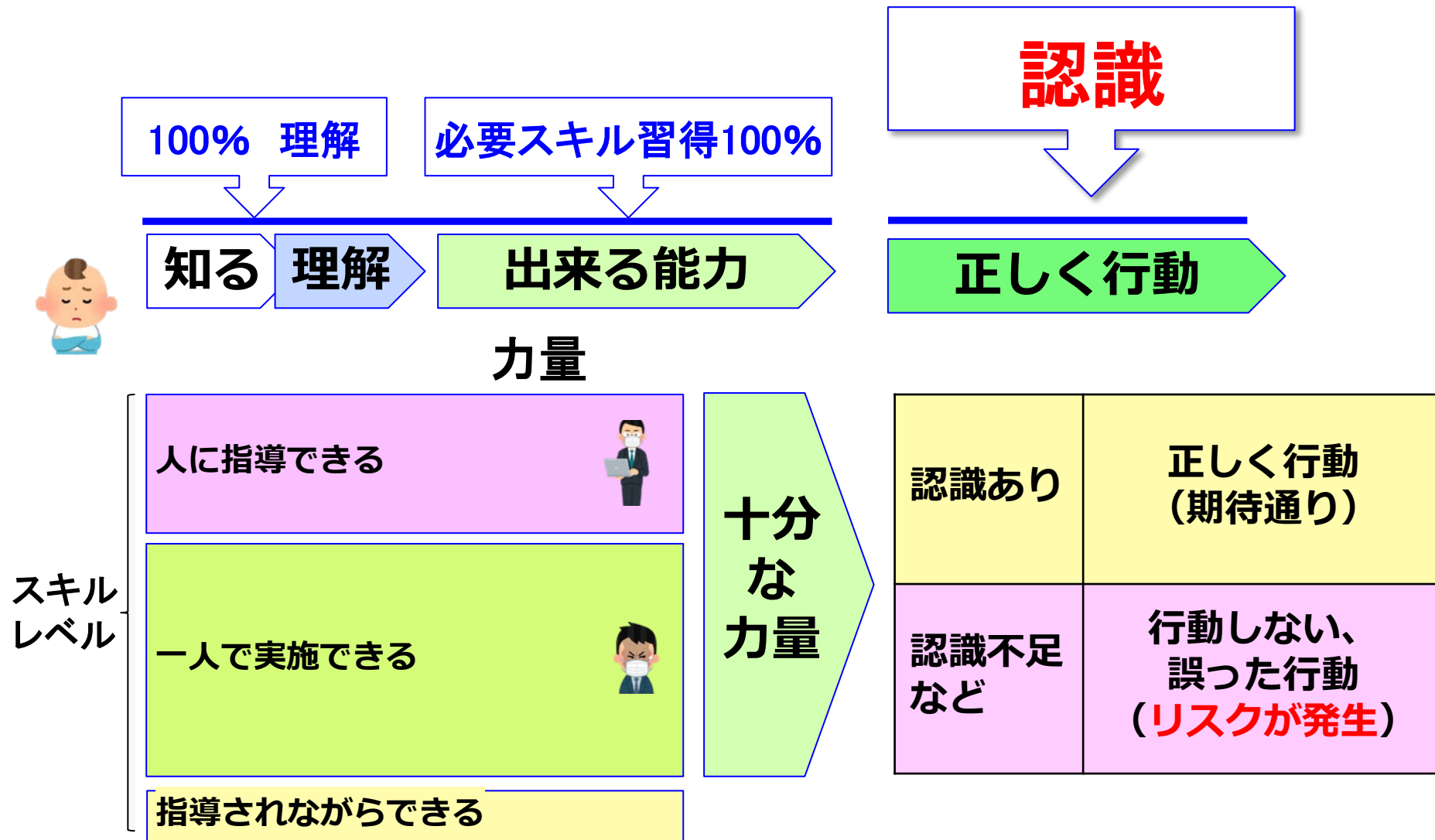
	作業分類	作業項目	作業内容	備考
不定期	規程やルール変更時の周知	セキュリティ規則の現場への展開	セキュリティ規則（新規、変更など）の現場への周知&意識付け	
	リスクアセスメント対応	自組織内で発生するリスク源を特定し、ビジネスへの影響を容可能なレベルにコントロールする	下記のイベント毎にリスクアセスメントを実施 ア) 情報資産や業務プロセスの見直し イ) 内部監査、外部審査時の指摘事項対応 ウ) 環境の変化 エ) インシデントの発生に伴う要因分析	
	インシデント対応	自組織内で発生したインシデント対応支援やヒヤリハットなどの再発防止対応	インシデント対応支援 担当内におけるインシデン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）	

認識とは？

規格 7.3

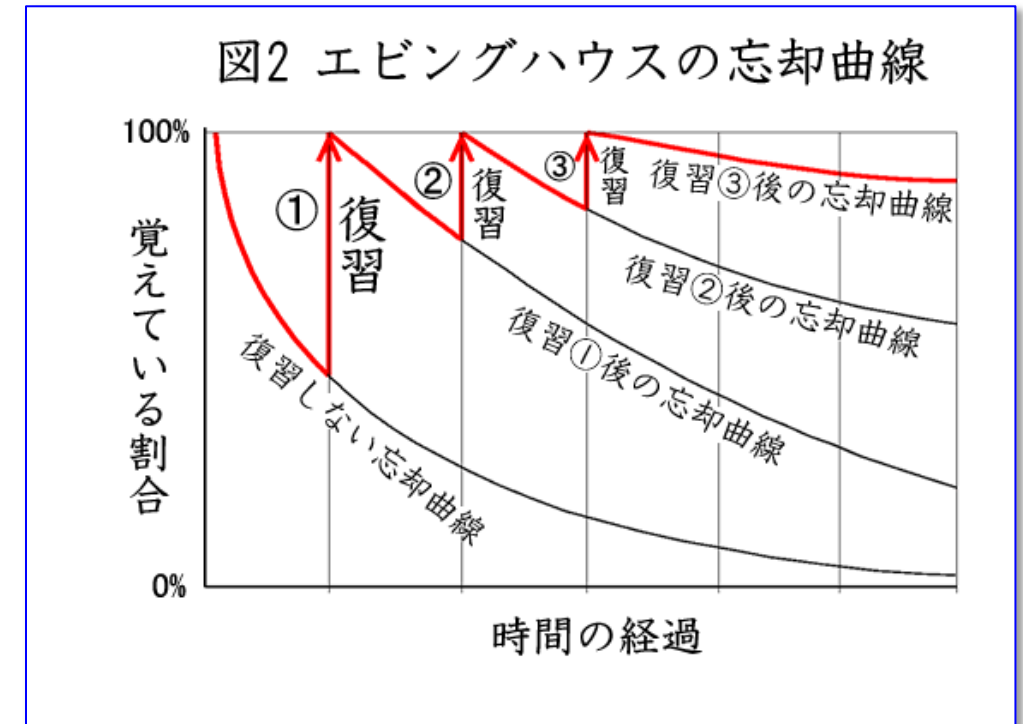
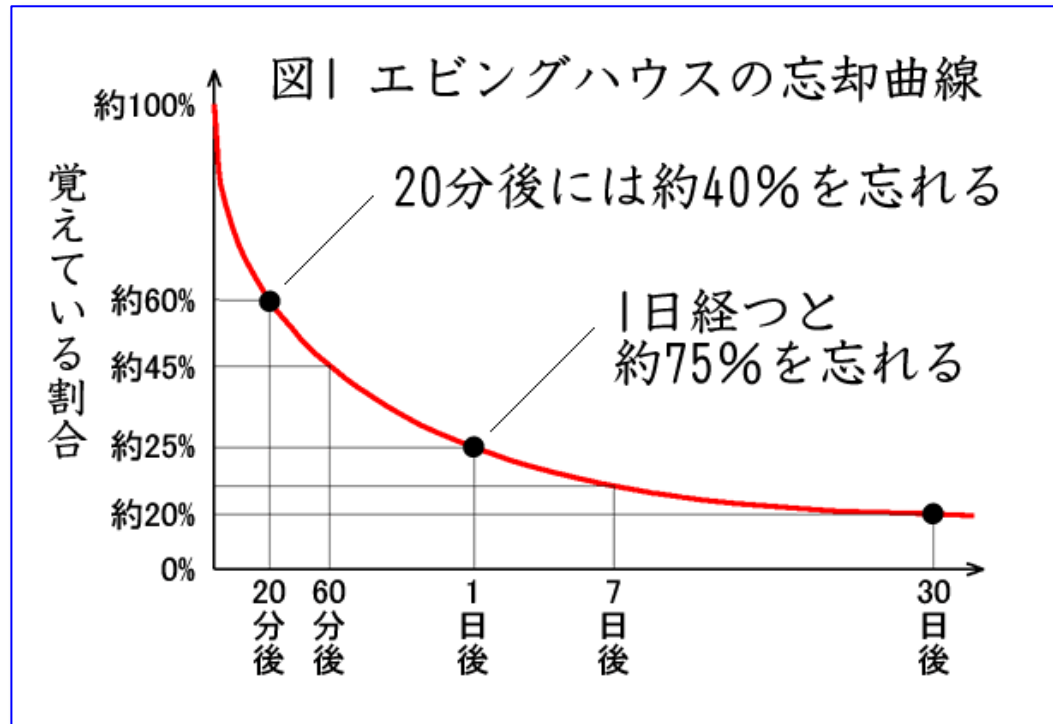


認識とは？



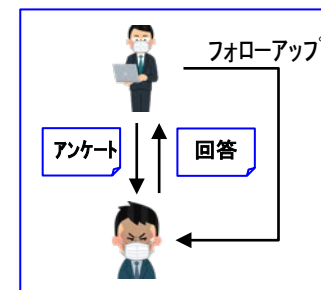
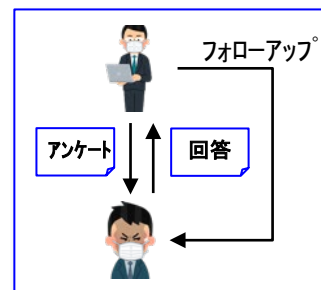
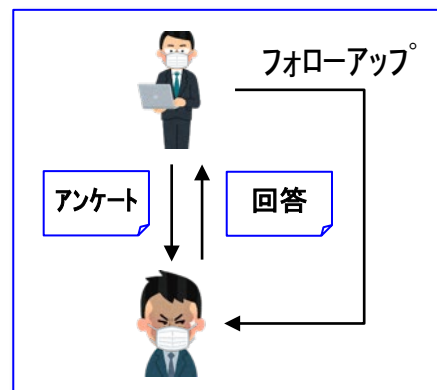
各社の実践事例 に学ぶ

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・・・



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

定期的に繰り返すことによりリマインドして定着を図る

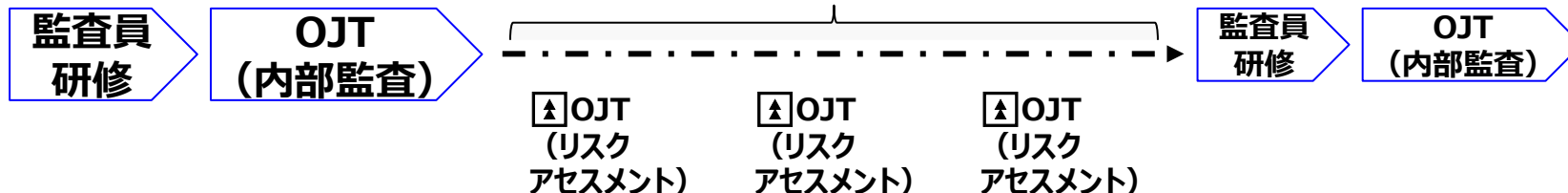


必ず忘れるという
前提条件で研修
メニューの設定が
必要

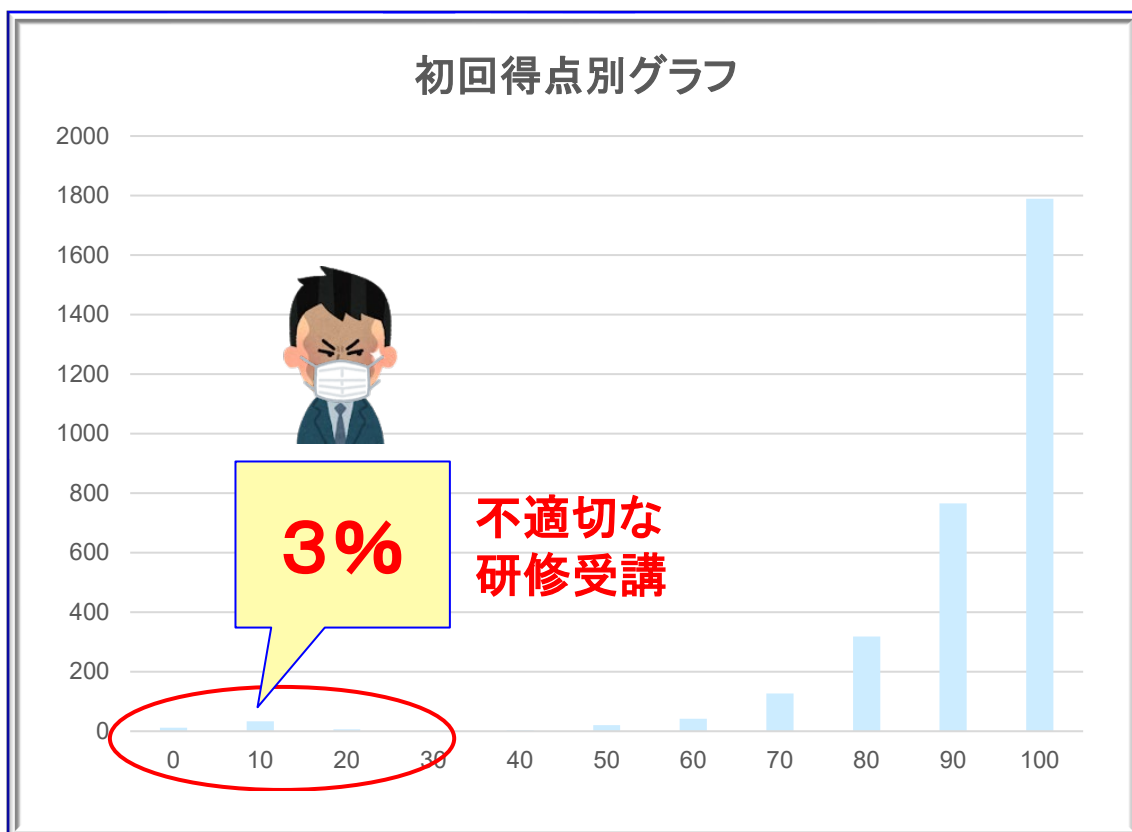


事例2：内部監査員

空白期間でも関連スキルをOJTで習得

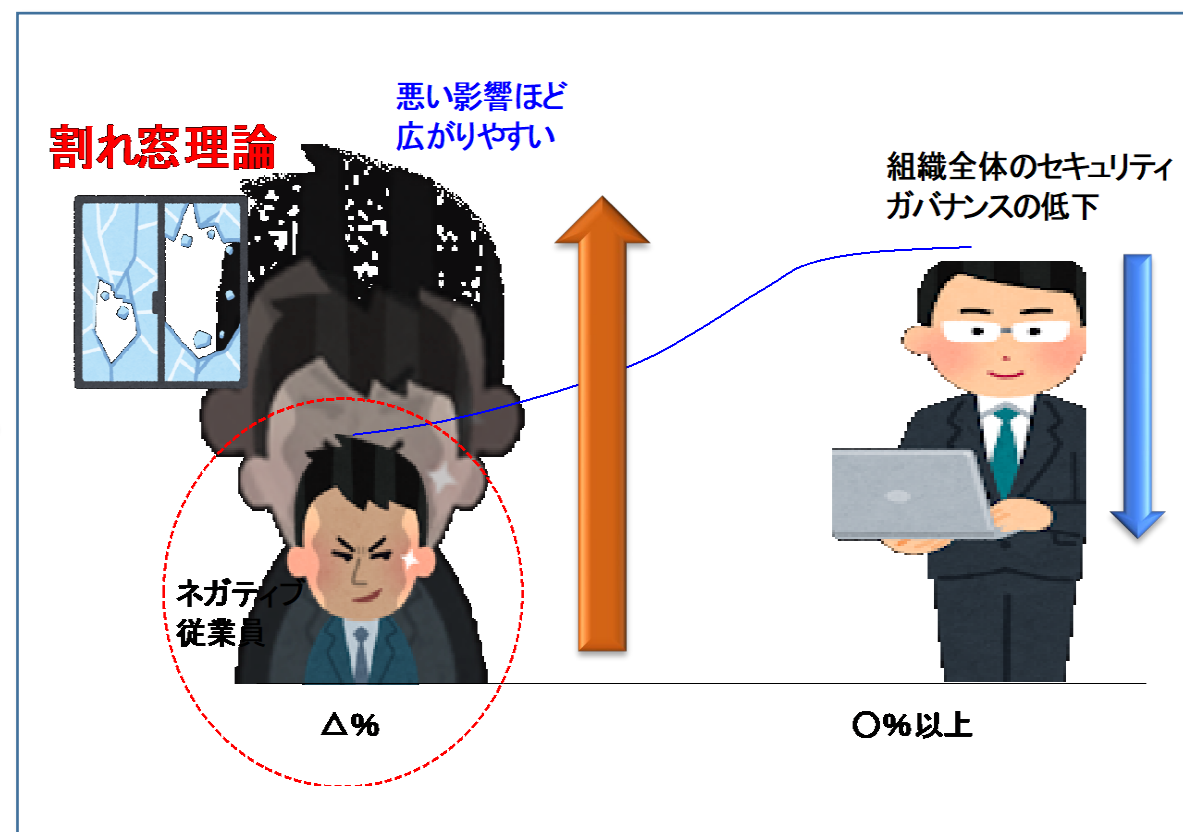


合格（100点）まで何度も受講するシステムとなっているA社の事例だが、データを分析すると**初回時に何も考えずに回答して、以降間違ったところだけ総当たりで回答するという行動パターン**が一定数見受けられる



ネガティブ従業員との戦い・・・

放置した結果（想像）



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

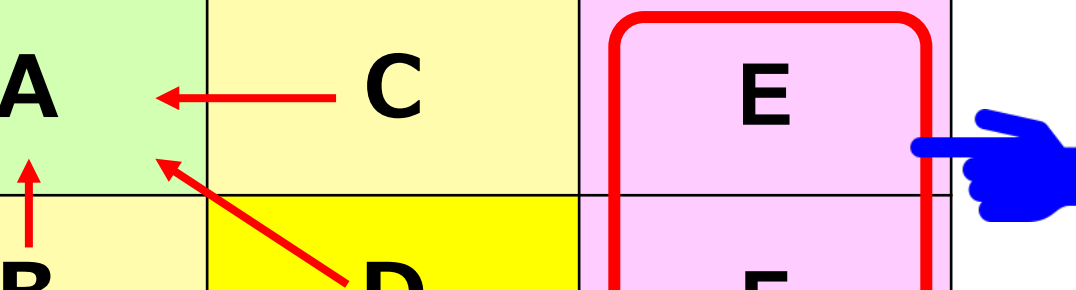
C：十分な力量を持っているが、認識不足で不適切な行動

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

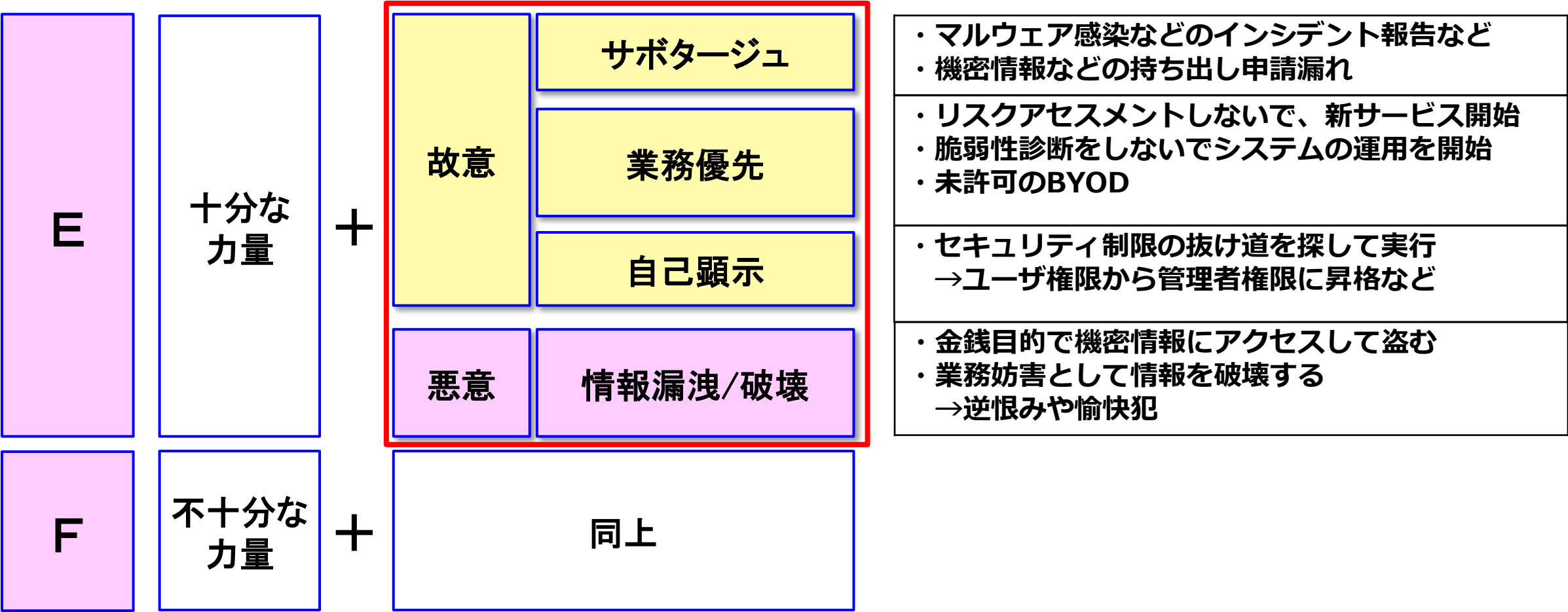
F：不十分な力量だが、故意・悪意を持って不適切な行動

	正しい認識	認識不足	故意・悪意
十分な力量	A	C	E
不十分な力量	B	D	F

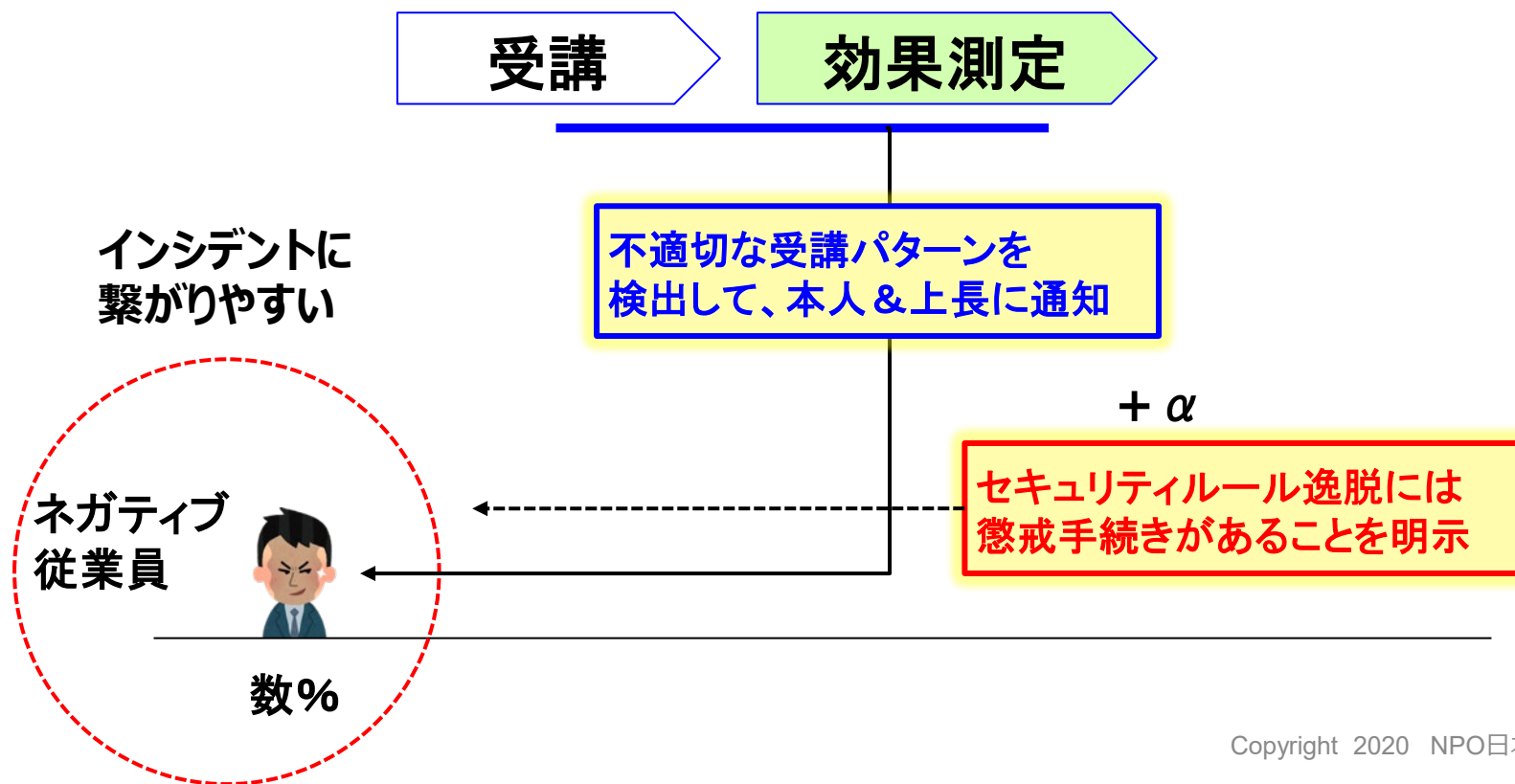


E & F : 故意・悪意を持って行動するパターン

【具体的な行動事例】



- 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



2020年の取り組み

■ 情報セキュリティマネジメントセミナー



■ 情報セキュリティマネジメントセミナー2020

【基調講演】

- ・ 「サイバーセキュリティにおけるISMSの役割 」

【標準化動向】

- ・ 「ISO/IEC 27000ファミリー規格の最新動向」

【研究会成果報告】

- ・ 「実践かつ効果的なセキュリティ教育」
- ・ 「規格（ISO/IEC27002）改定に対するISMSユーザー意見反映の取り組み」

参考：セミナー開催情報

<https://www.jnsa.org/seminar/2020/index.html>



本日の資料のフルセット版
が掲載されています！

2021年の活動紹介

ISMSとゼロトラストセキュリティについての考察（仮）

組織を取り巻く内外の環境の変化とゼロトラスト

2004年 2010年 2017年

2020年

2021年

昔からあるゼロトラストの概念

Jericho Forum (ジェリコ・フォーラム)
を正式に設立「非境界化」問題の解決に
注力する議論が開始

Forrester Research, Inc のJohn Kindervag
(ジョンキンダーバグ) 氏よりインフラから
信頼を取り除くことを前提とした考え方である
「ゼロトラスト」というコンセプトが提唱

People, Workloads, Data, の主要軸を追加し、
自動化&オーケストレーション と 可視化&分析
を構成要素全体に関連付けカニンガム博士により
Zero Trust eXtended (ZTX) として再定義

ゼロトラストというキーワードが頻繁

組織を取り巻く環境の変化

- ・ クラウドファースト時代
(機密情報の社外保管急増)
→ SaaS利用の拡大でさらに加速
- ・ サイバー攻撃の多発&多様化
- ・ コロナ禍におけるテレワーク増大
- ・ 内部不正
- ・ DXの加速&普及

ニーズ
の
高まり

ゼロトラスト対応のセキュリティ
プロダクトの相次ぐ発表

技術の
追隨

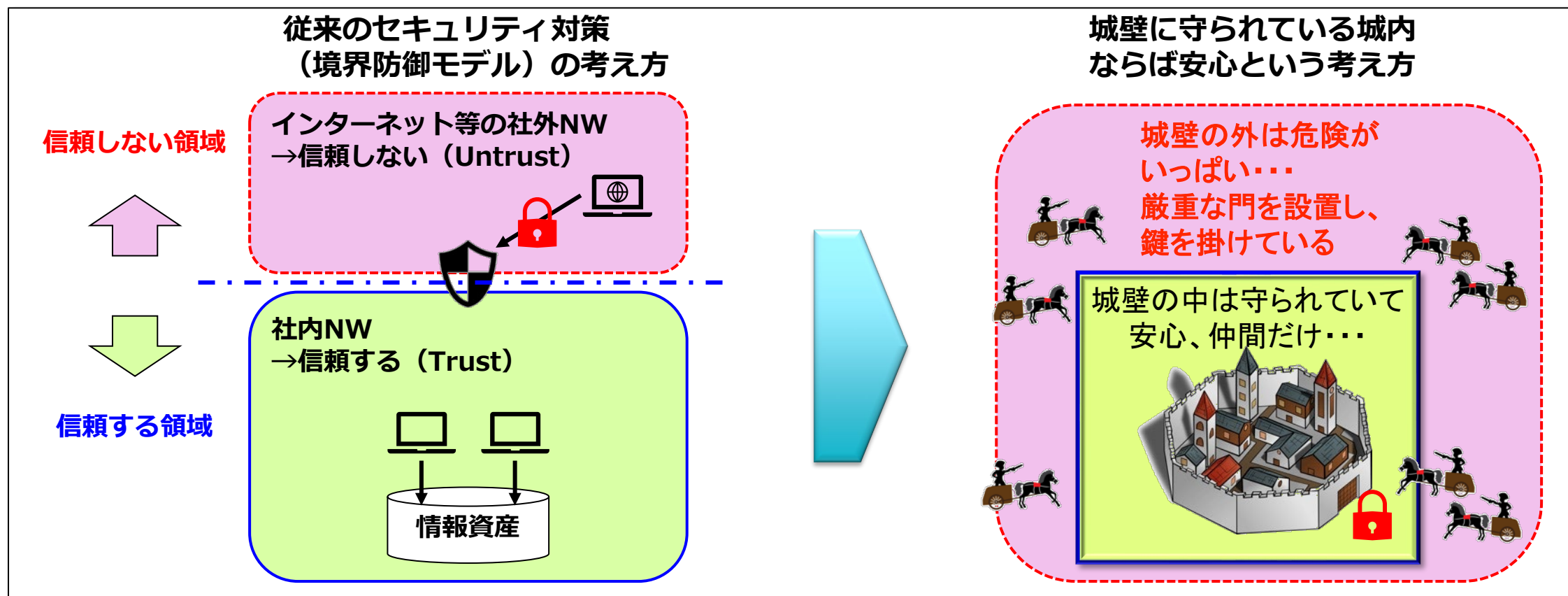
NISTのゼロトラストアーキテクチャー
(SP 800-207, ドラフト版)

ゼロトラストとは？ . . . 従来のセキュリティ対策との違い

ゼロトラストとは「**何も信頼しない**」を前提に対策を講じるセキュリティの考え方

従来のセキュリティ対策（境界防御モデル）

→ 信頼できる「内側」と信頼できない「外側」にネットワークを分け、その境界線で対策を講じる

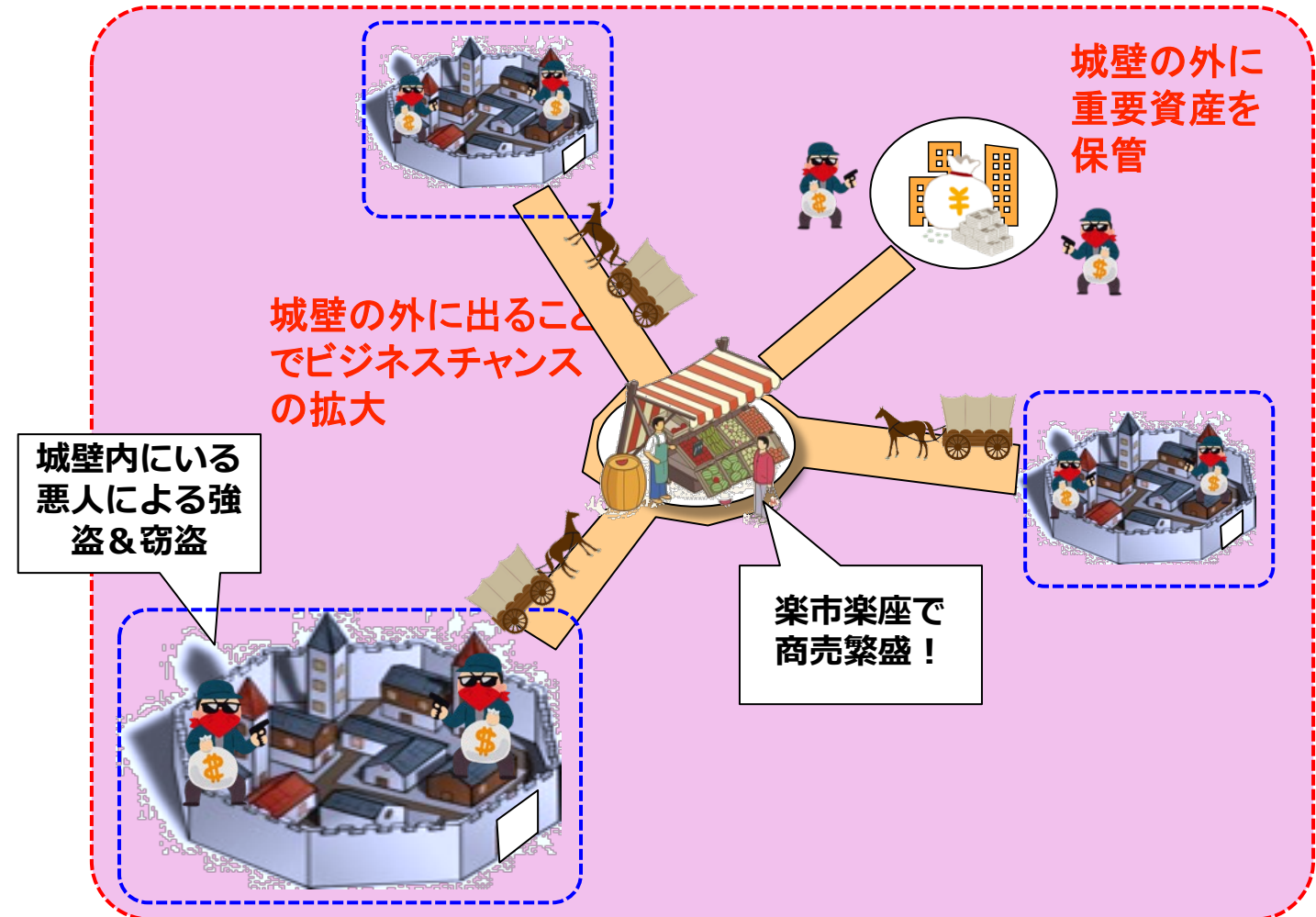
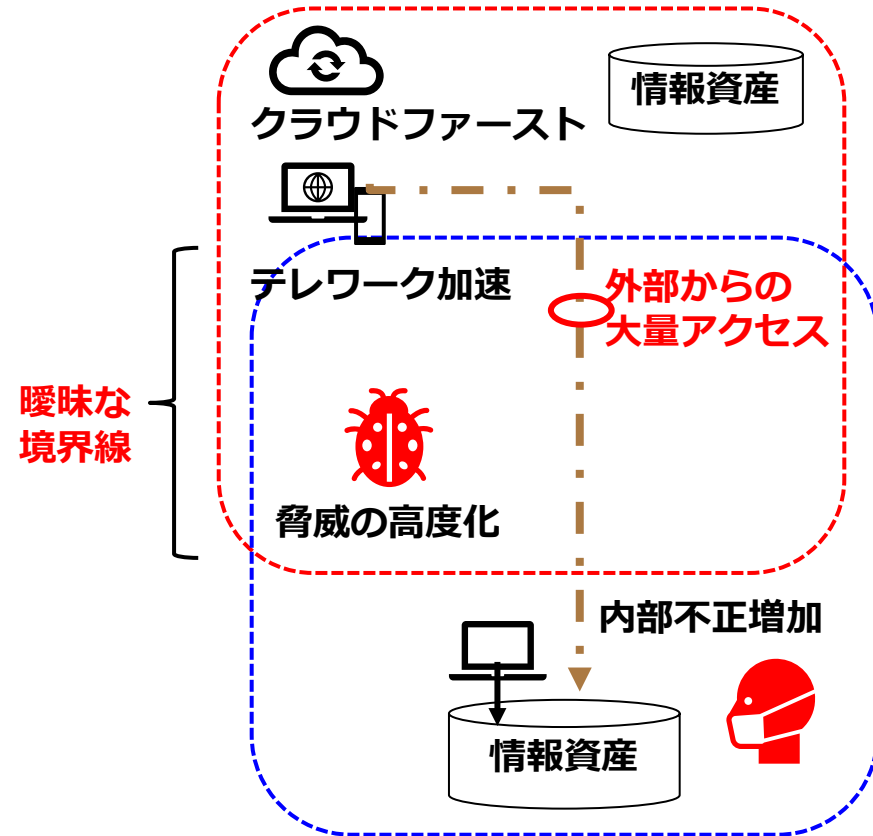


ゼロトラストとは？ . . . 境界防御モデルの限界

境界防御モデルの限界

→ 信頼できる「内側」と信頼できない「外側」の線引きが曖昧となり境界防御の前提条件が崩れた . . .

境界防御モデルの限界



ゼロトラストモデル（全て信頼しない、常に検証）

- 信頼しない（Untrust）とは？
- 常に検証（Always Verify）とは？

具体的な実装にはゼロトラストセキュリティ製品の導入が前提条件となっている

もし、経営者からゼロトラストセキュリティの導入を指示されたら・・・

- 自らの言葉で経営者に説明したい（リスクコミュニケーション）
- 技術に詳しくないが、情シスと連携してセキュリティ要件をまとめたい

日本ISMSユーザグループとしては製品導入ありきの前に本質について検討したい・・・

信頼しない、常に検証についてどういうことが判り易く解説すると共にISMSとの関係を整理することで自社にあったゼロトラストセキュリティの要求条件を整理できるはず・・・

続きは12月に開催予定の情報セキュリティマネジメントセミナーにて

2021年の取り組み

■インプリメンテーション研究会へのお誘い

2021年は下記の2テーマに取り組んでいます。

毎年、**組織を取り巻く環境の変化に対応したテーマに挑戦**しています。

ご興味のある方は一緒に検討に参加頂ければ幸いです。

冷やかしも大歓迎ですので、気軽に事務局へご連絡ください。

テーマ1: ISMSとゼロトラストセキュリティについての考察

テーマ2: ISMS要求事項対応事例(箇条4)の考察

現在、Web会議 (zoom)
で討議しています！

毎月最終木曜日18:00～21:00

