【JSSM公開討論会】

（私見）情報セキュリティの課題

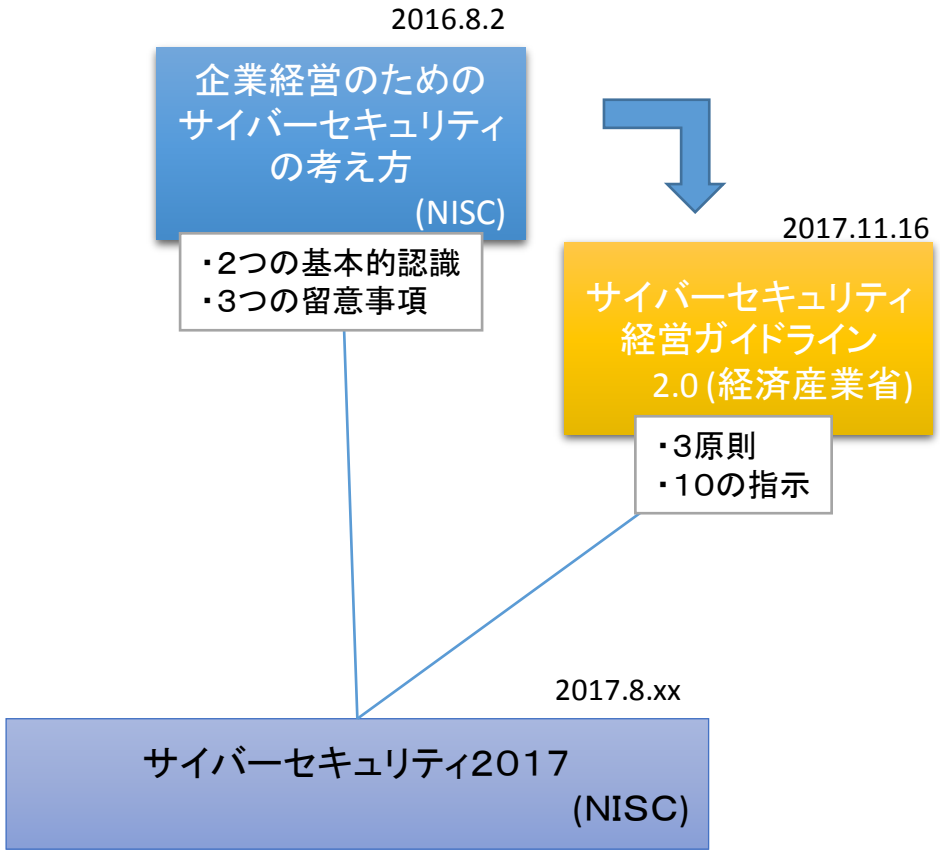
注）
当資料は、あくまで私個人の見解であり、私の所属する会社や、企業グループの見解ではございませんこと、ご了承ください。

2018年 3月 17日

丸山司郎

Benesse InfoShell

サイバーセキュリティ経営ガイドライン



改定の目的

- NISTがフレームワークを改定した
- 1.0ができて2年が経ち、課長が変わった
- SBT辻さんが作った付録Cを公表したかった

2016.12.8
サイバーセキュリティ
経営ガイドライン
解説書
(IPA)

2017.4.13
企業のCISOやCSI
RTに関する実態調
査
(IPA)

2016.11.5
中小企業の情報セ
キュリティ対策ガイド
ライン
(IPA)
・3原則
・7つの取り組み

問題点

- 善管注意義務の判断基準となりうる指針がない
- なぜサイバーだけ？
- 余計なお世話

3原則（意訳）

1．経営者はセキュリティ投資を実施せよ

2．パートナーや委託先も含めたサプライチェーンに対する対策をせよ

3．リスクや対策に係る情報を開示せよ

やらない経営者は、善管注意義務違反！

企業の目的とセキュリティ

ドラッカー

□ 企業の存在意義とは

「顧客を創造することである」

□ 組織マネジメントの役割とは

①「自らの組織に特有の使命を果たす」

②「仕事を通じて働く人たちを生かす」

③「社会の問題について貢献する」

私の考え

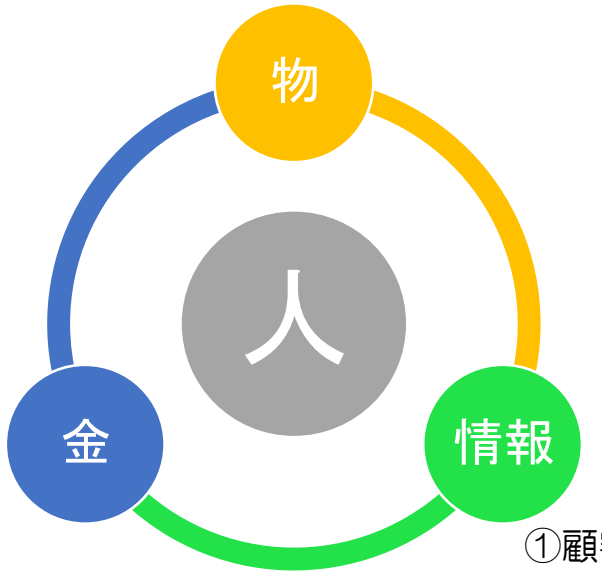
我が社が情報セキュリティ対策をする理由

① 顧客から預託された情報資産を守る

② 自社の事業推進に対するリスクを減らす

③ インシデントによって、他社に迷惑をかけない

企業が守る経営資産



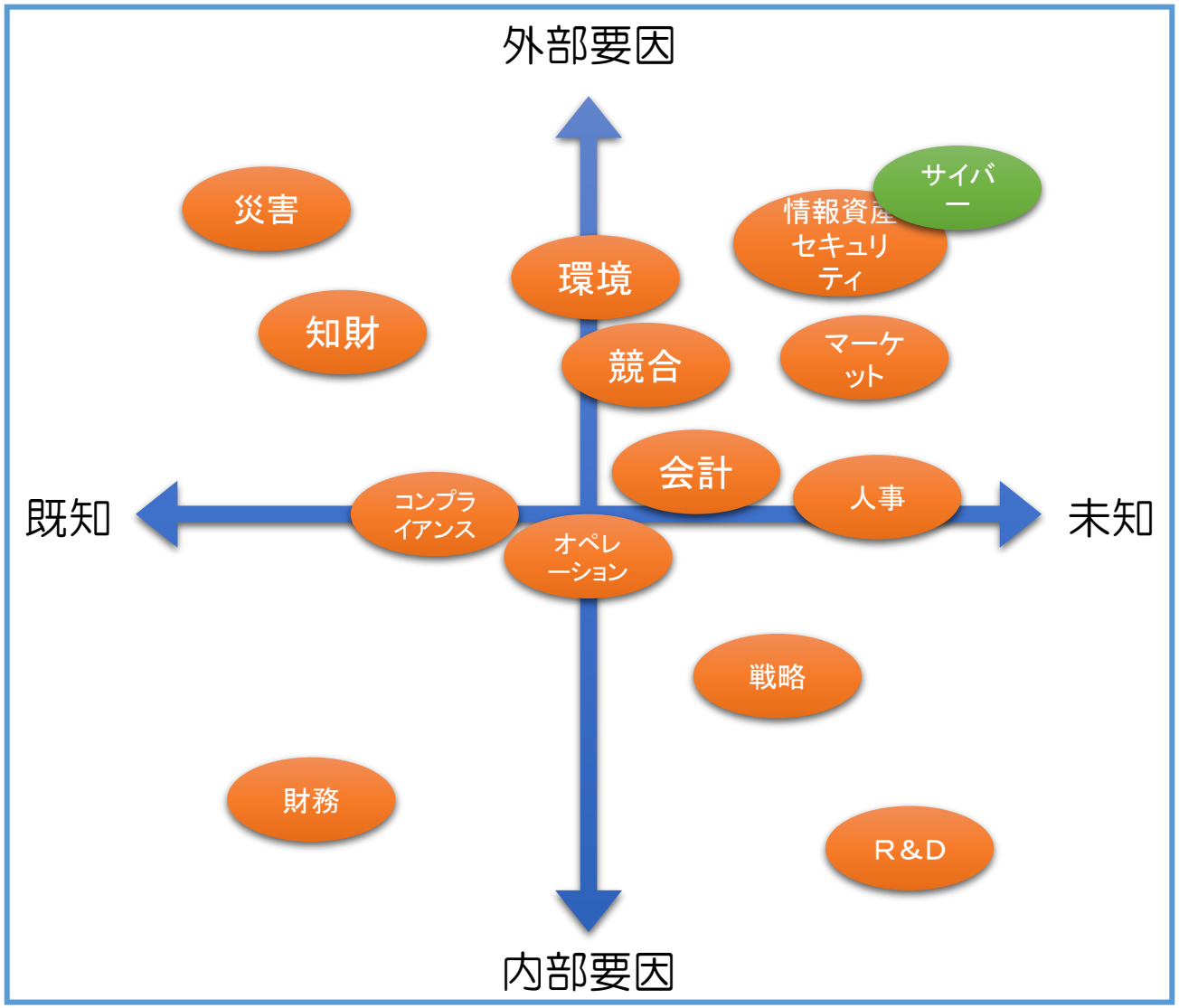
①顧客からの預り情報

②顧客個人情報

③営業機密

サイバー セキュリティ リスクの理解

企業をとりまくリスク概念



ＩＴ革命という激変の中、サイバーセキュリティは攻守のバランスがとれていない。

私の考える事業リスクの順位

1．ＩＴ革命による事業環境変化
2．日本市場の縮小
3．ワークライフバランス
4．労働力不足（人数、能力）
5．国際競争力低下
6．情報資産リスク（含サイバー）

情報資産セキュリティの現状

サイバー脅威の現実

- 犯罪者は最もクリエイティブな存在である。
- 脅威のレンジは世界規模である
  （高校生から、ＮＳＡ又はロシアマフィアまで）
- ＩＴの進歩と同じ速さで脅威が増大する
- 犯罪者を取り締まる有効な手段はない

守る側の現実

- 見つかってすぐの脆弱性にやられても仕方ない
- 攻撃側が本気だったら、一企業じゃ守れない
- あんな高度な手口でやられたから仕方ない
- 犯罪者が悪いのであって、守れなかった者が悪いわけではない

実際の課題

・罰則はあるが、免責となる基準がない

・対策強度の評価指標や評価手段がない

・採用時にセキュリティ人物評価ができない。

・終身雇用で怪しい奴でも辞めさせられない。

・日本特有の文化で、やられたものが叩かれる。

採用時に聞いてはいけない質問

a. 本人に責任のない事項の把握
- **本籍・出生地**
- **家族（職業、続柄、健康、地位、学歴、収入、資産など）**
- 住宅状況（間取り、部屋数、住宅の種類など）
- **生活環境・家庭環境など**

b. 本来自由であるべき事項
- **宗教**
- 支持政党
- **人生観、生活信条**
- **尊敬する人物**
- **思想**
- 労働組合に関する情報（加入状況や活動歴など）
- **学生運動など社会運動**
- 購読新聞・雑誌・愛読書など

c. 採用選考の方法
- **身元調査などの実施**

私の考える情報資産セキュリティ対策

組織（人）は戦略に従う

組織は目的を達成するための手段であるため、
組織は戦略に従い、戦略は産業構造に従う。

経営資産の保護と活用

① 人的資産

信用できる人を採用し、安心して働ける環境を提供する。

② 物的資産

災害、犯罪、棄損などから物理資産を守り、労働生産性の向上に寄与する設備を構築・維持する。

③ 資金

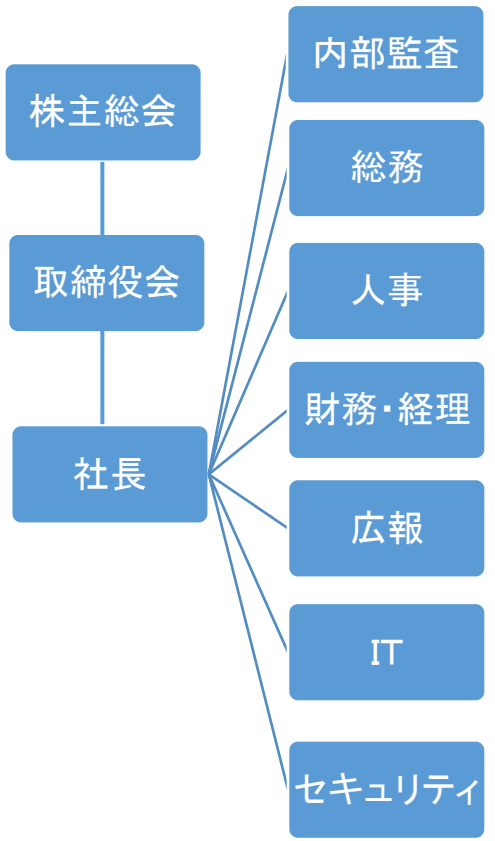
犯罪や内部不正、金融リスクから資金を守り、より有効な事業投資につなげる

④ 情報資産セキュリティ

競争優位性のあるデータを大量に収集し、漏えい、改ざん、棄損から保護しつつ、分析・解析し事業拡大に役立てる。

戦略は組織（人）に従う

限りある経営資源に応じた戦略でないと、机上の空論。
競争優位性のあるコアコンピタンスに注力すべき。



実組織の役割

- セキュリティ監査

- 設備セキュリティ
- ゾーニング
- 入退室管理

- （人物評価）
- アカウント管理

- 予算承認
- 投資執行管理

- （メディアコミュニケーション）

- 技術セキュリティ対策
- 予算措置
- IT最新情報収集、評価

- ポリシー改訂
- セキュリティ教育
- 承認、例外判定
- 脆弱性対応
- 脅威情報収集、評価
- インシデントハンドリング

必要機能とセキュリティ人材とのギャップ

我が社が必要とするセキュリティ機能

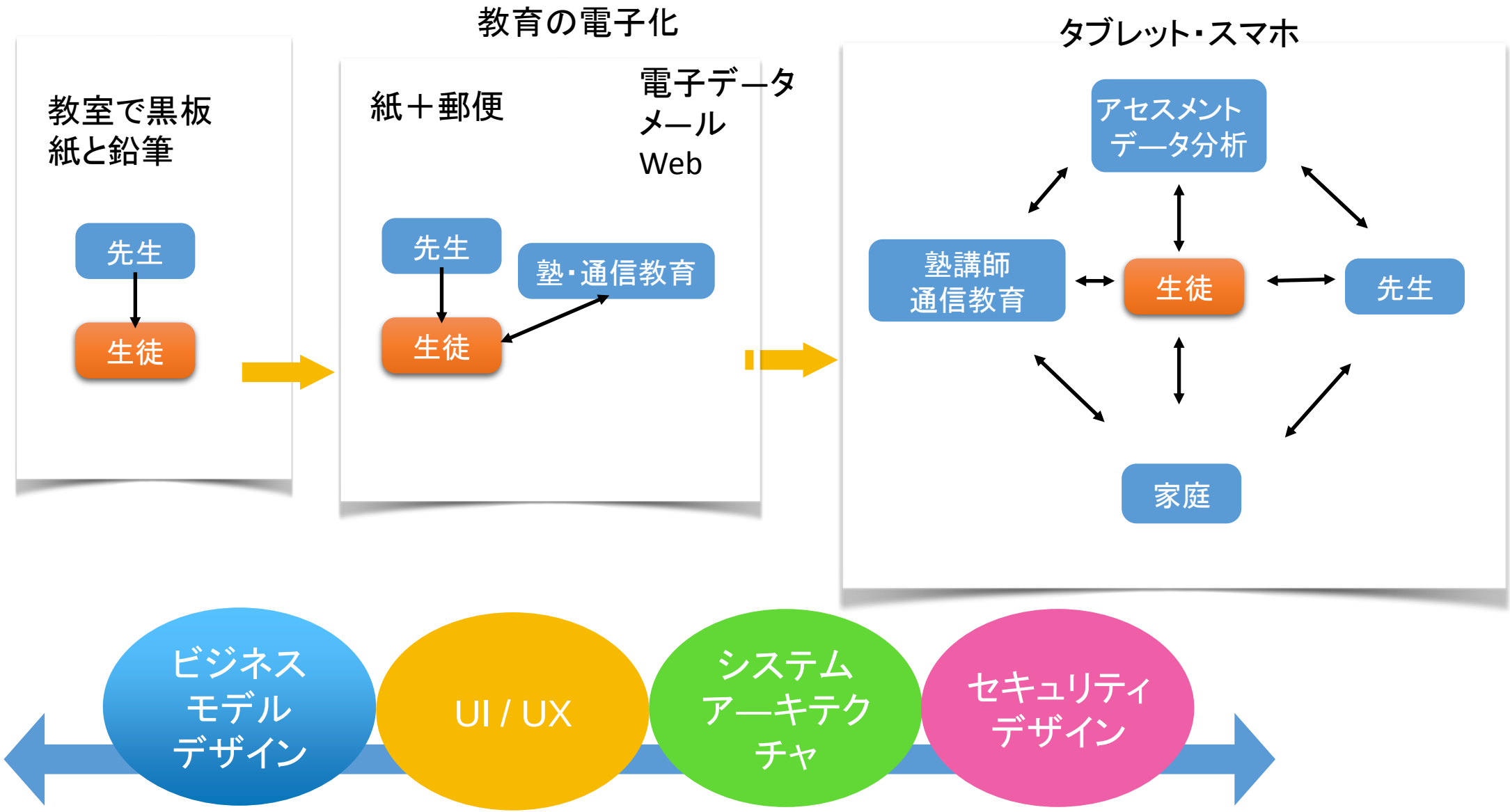
内部育成

セキュリティ監査	
設備セキュリティ	?
ゾーニング	?
入退室管理	?
人物評価	?
アカウント管理	?
予算承認	?
投資執行管理	?
メディアコミュニケーション	
技術セキュリティ対策	
予算措置	?
IT最新情報収集、評価	?
ポリシー改訂	
セキュリティ教育	?
承認、例外判定	?
脆弱性対応	?
脅威情報収集、評価	
インシデントハンドリング	

セキュリティ人材スキルマップ
SecBoK（JNSA 2017年）

		外部委託
基礎	ICT基礎	
	工学基礎	
	ビジネス基礎	
セキュリティ基礎		
セキュリティガバナンス		
セキュリティマネジメント		
ネットワークセキュリティ	トラフィック解析	×
	侵入検知	×
	脆弱性診断	×
	フィルタリング	
	アクセス制御	
	VPN	×
	深層防御	
システムセキュリティ		
セキュアシステム設計・構築	セキュアプログラミング	×
	テスト	
セキュリティ運用	インシデント対応	
暗号・認証・電子署名		×
サイバー攻撃手法	マルウェア	×
デジタルフォレンジクス		×
法・制度・標準		

デジタル革命に挑む事業部門の情報セキュリティ



デジタル革命により広がる情報セキュリティの責任

最低限のシステム利用レベルの事業（メール、Web、専用システム程度）

	教育効果	メディアミックス				コンテンツ		コスト		新技術				利用者リテラシー			システム運用				セキュリティ			
	学習習慣成績向上	紙通販	デバイス	親スマホLINE	学校、塾	質	更新頻度	デバイス	コンテンツ	MVCバランス	パフォーマンス	通信環境4G、wifi	AI、IoT、BigData	入力I/F	デバイスの普及度	使い勝手	アクセス制御	端末ライフサイクル	障害・インシデント対応	脆弱性対応	暗号化	端末プラットフォーム	Webセキュリティ	個人情報保護
ビジネスモデルデザイン	◎	◎	—	—	◎	○		—	◎		○		—	—	—			—	○			—		◎
UI/UX		○	—	—	○	◎	—			○	○	—		—	—	—	○							
システムアーキテクチャ			—	—			—	—		◎	◎	—	—	—	—		◎	—	◎	◎	◎	—	◎	○
セキュリティデザイン			—	—				—		○			—	—			○	—	○	○		—	○	○

経営層の関心領域

デジタル革命に挑戦する事業

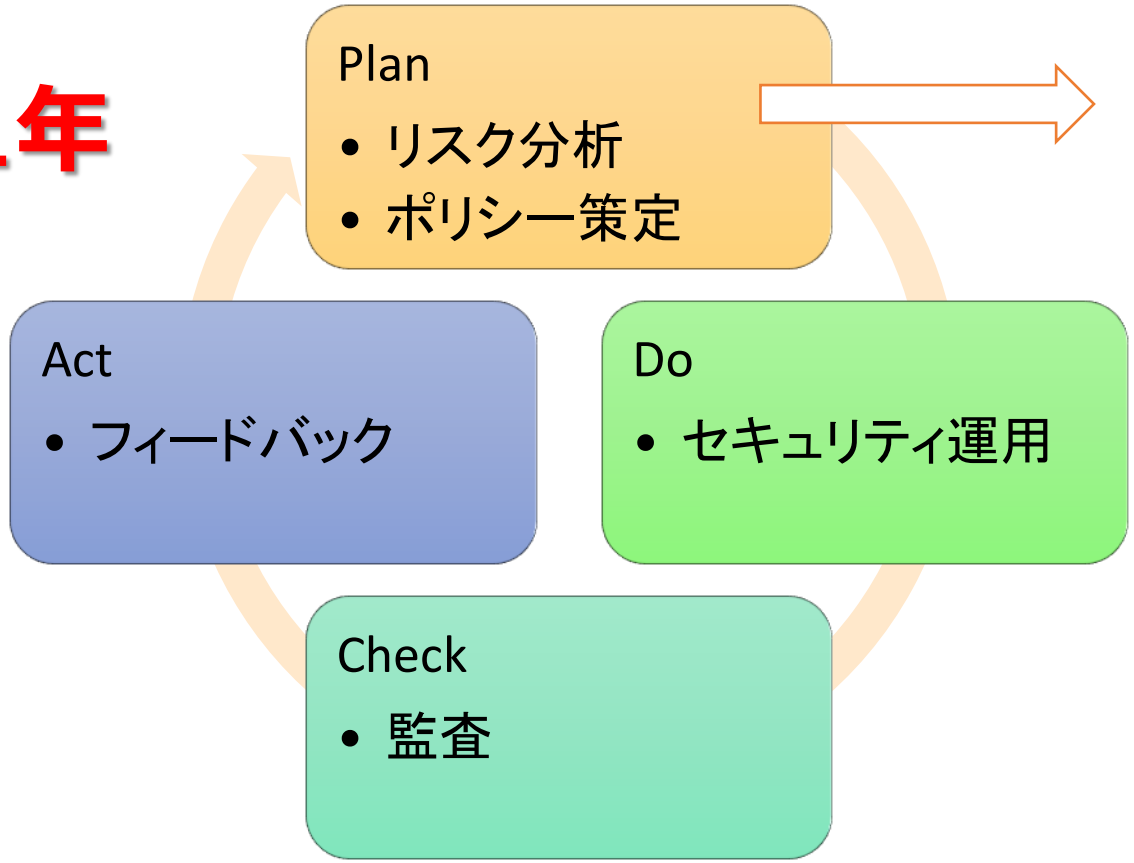
Security Everywhere

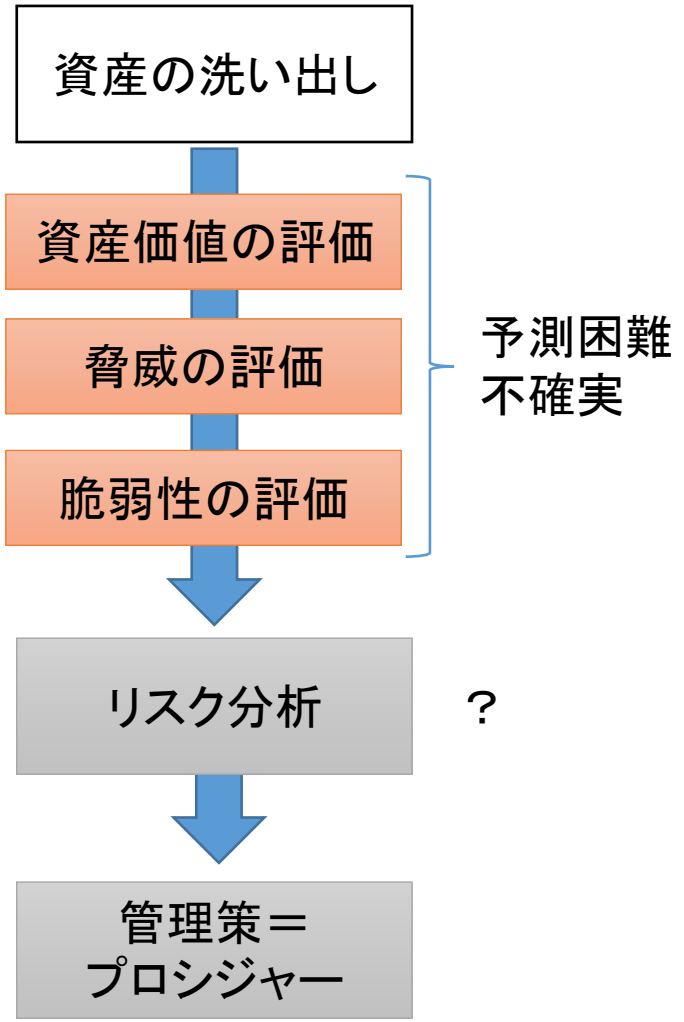
	教育効果	メディアミックス				コンテンツ		コスト		新技術				利用者リテラシー			システム運用				セキュリティ			
	学習習慣成績向上	紙通販	デバイス	親スマホLINE	学校、塾	質	更新頻度	デバイス	コンテンツ	MVCバランス	パフォーマンス	通信環境4G、wifi	AI、IoT、BigData	入力I/F	デバイスの普及度	使い勝手	アクセス制御	端末ライフサイクル	障害・インシデント対応	脆弱性対応	暗号化	端末プラットフォーム	Webセキュリティ	個人情報保護
ビジネスモデルデザイン	◎	◎	○	○	◎	○		○	◎		○		◎	○	◎			○	○			○		◎
UI/UX		○	◎	◎	○	◎	○			○	○	○		◎	○	◎	○							
システムアーキテクチャ			○	○			◎	◎		◎	◎	◎	○	○	○		○	○	◎	◎	○	◎	◎	○
セキュリティデザイン			○	○				○		○			○	○			◎	◎	○	○	◎	○	○	○

ＩＳＭＳの課題

デジタル革命には通用しない。
・リスクが読めない
・遅い
・子ども扱い（ルールを守ればOK)

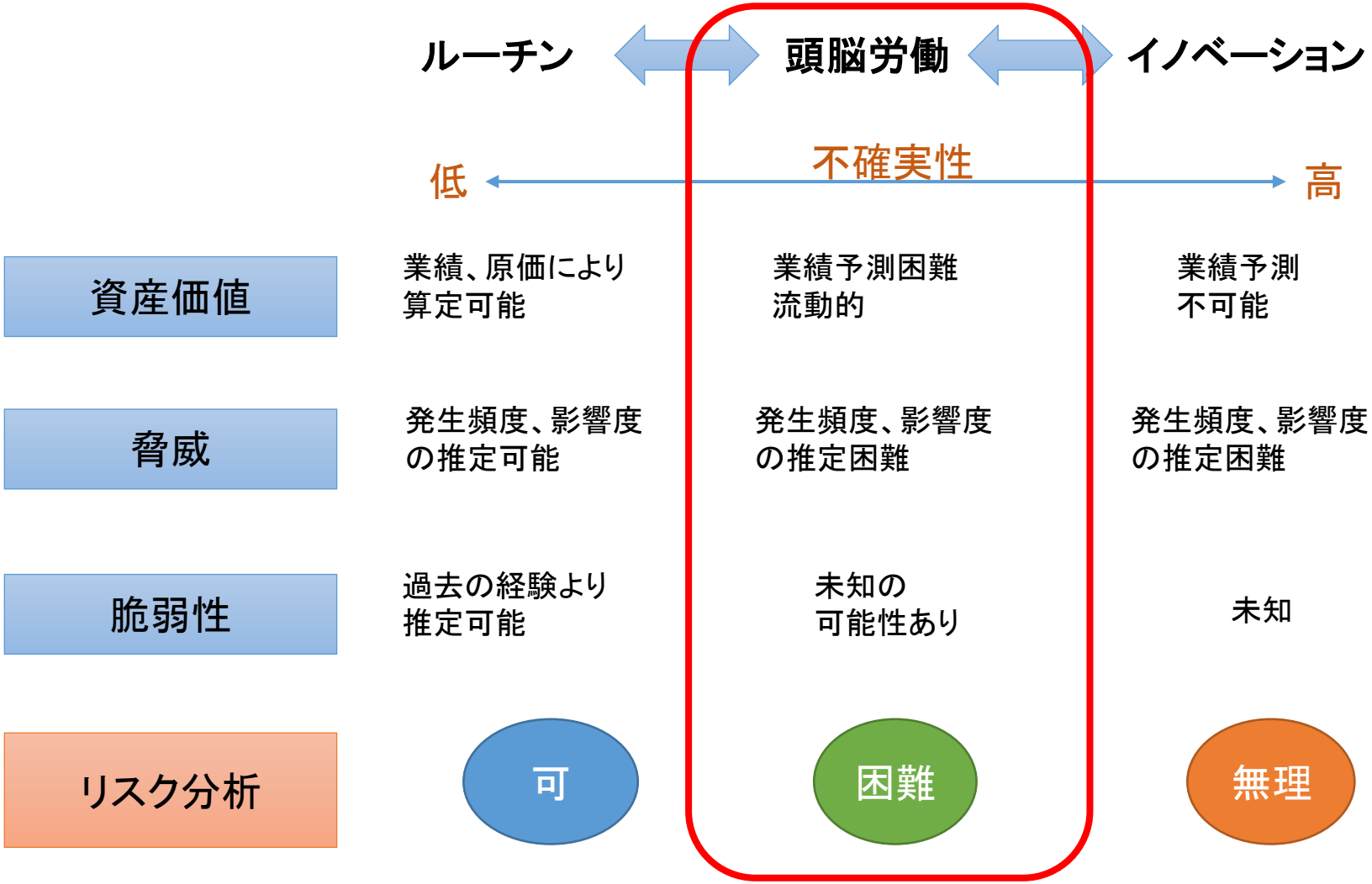
1年



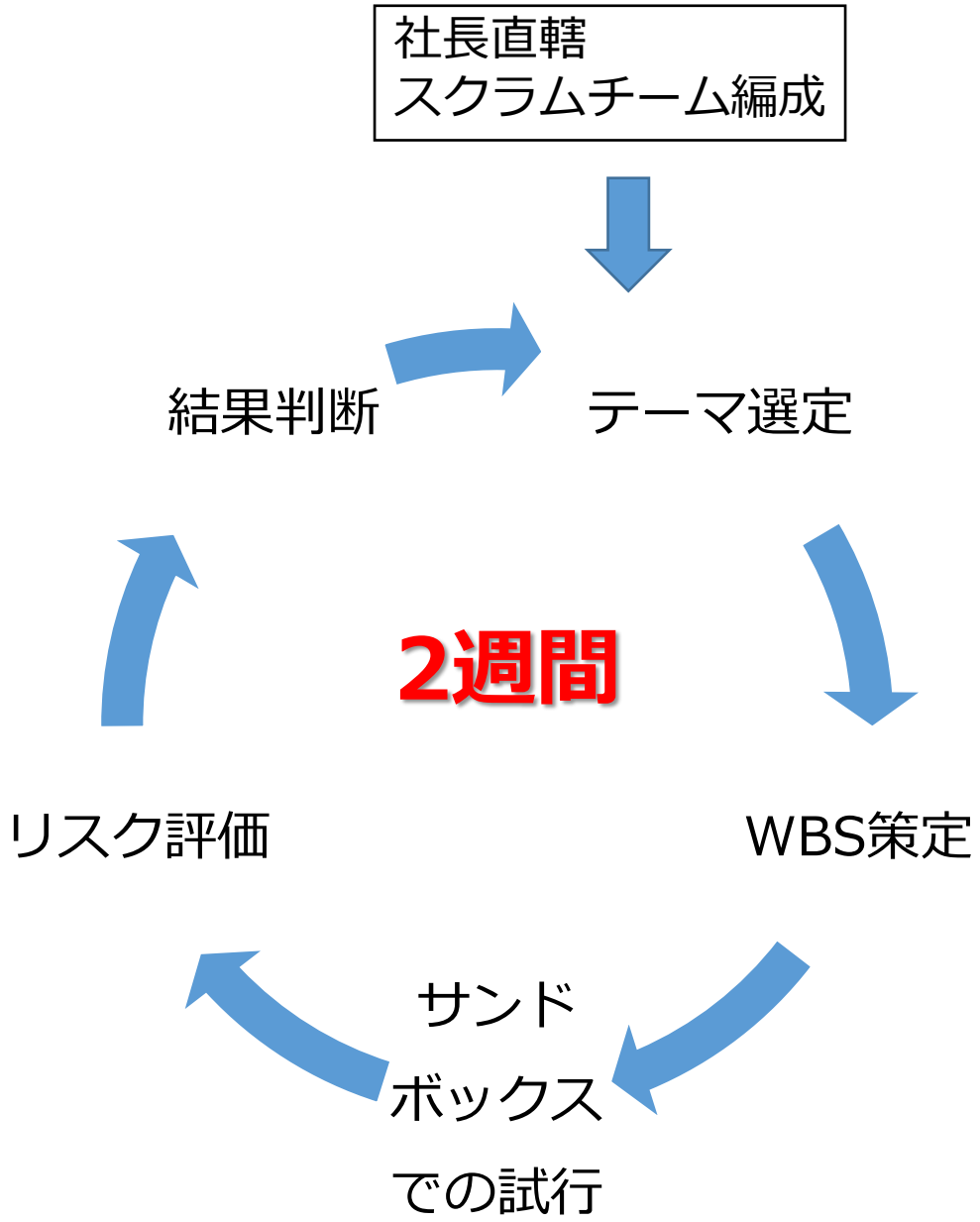


ＩＳＭＳの課題

デジタル革命により、リスク分析ロジックの妥当性が薄れた



スクラム的リスク評価　（お試し中）



ポイント
1．業務現場とルール担当と技術担当でチームを作り、工程を省く
2．セーフティとセキュリティを分ける
3．ショートサイクル（2週間）で、準備・試行・省察を回す
4．リアルタイムの意見交換
5．最小単位（サンドボックス）で初め、失敗を受け入れる
6．うまく行ったら展開する
7．ルールは最後に変更する