

【サイバーセキュリティ人材の育成に関する施策間連携WG】

私企業におけるセキュリティ人材 を取り巻く現状と課題

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。

2017年 9月 14日

丸山司郎

Benesse InfoShell

企業の目的とセキュリティ

ドロッカー

□ 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」

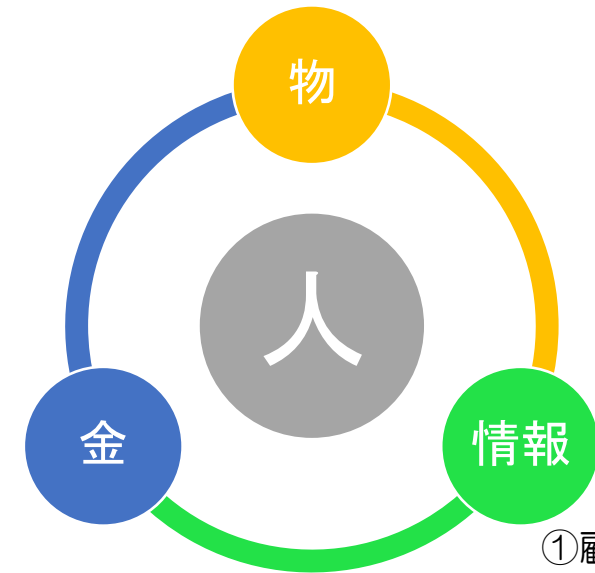


私の考え

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

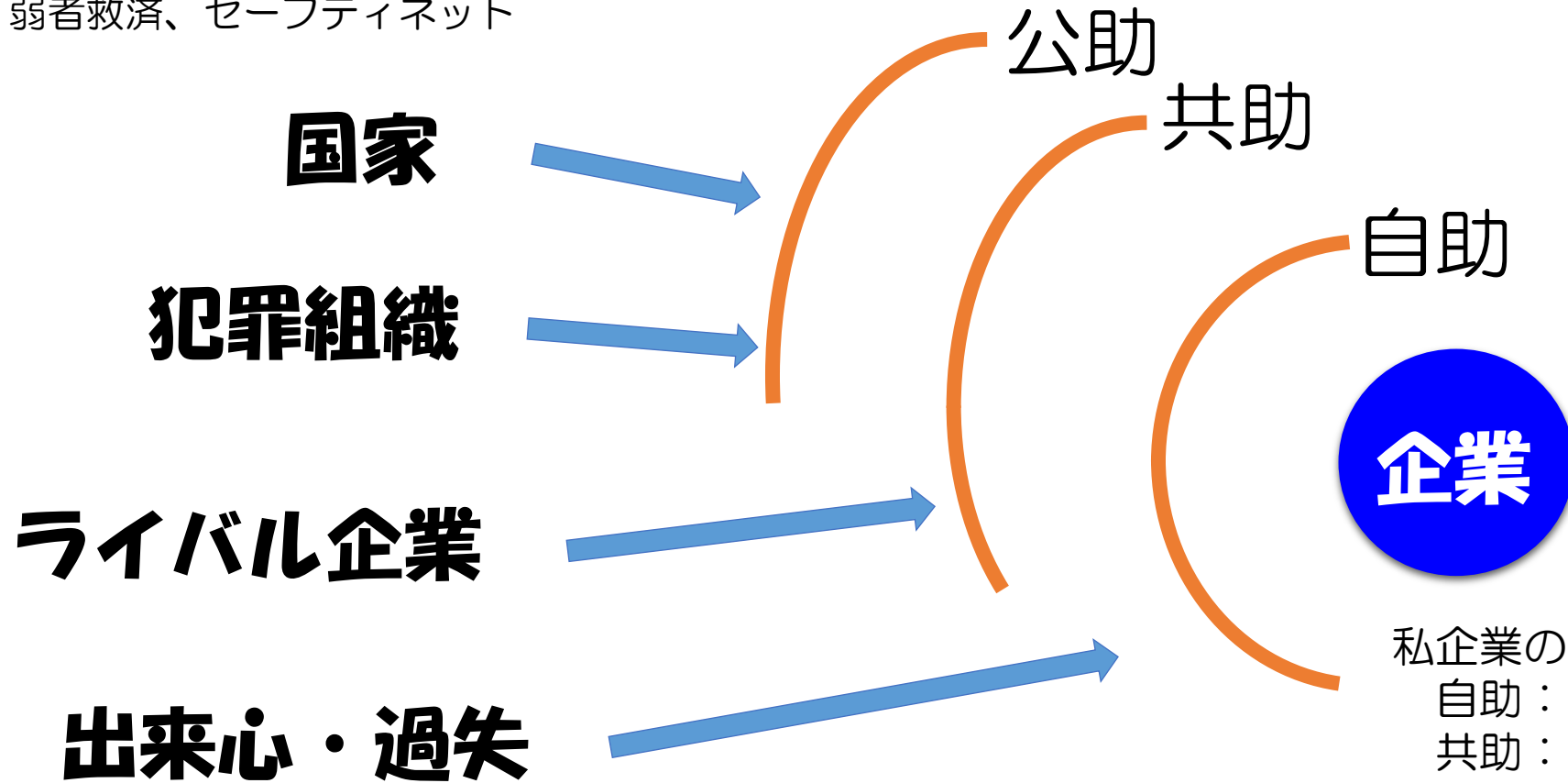
企業として何をどこまでやればいいのか？

国からの視点

公助：国防、安保、国際ルール締結

共助：相互扶助、情報共有

自助：弱者救済、セーフティネット



私企業の視点

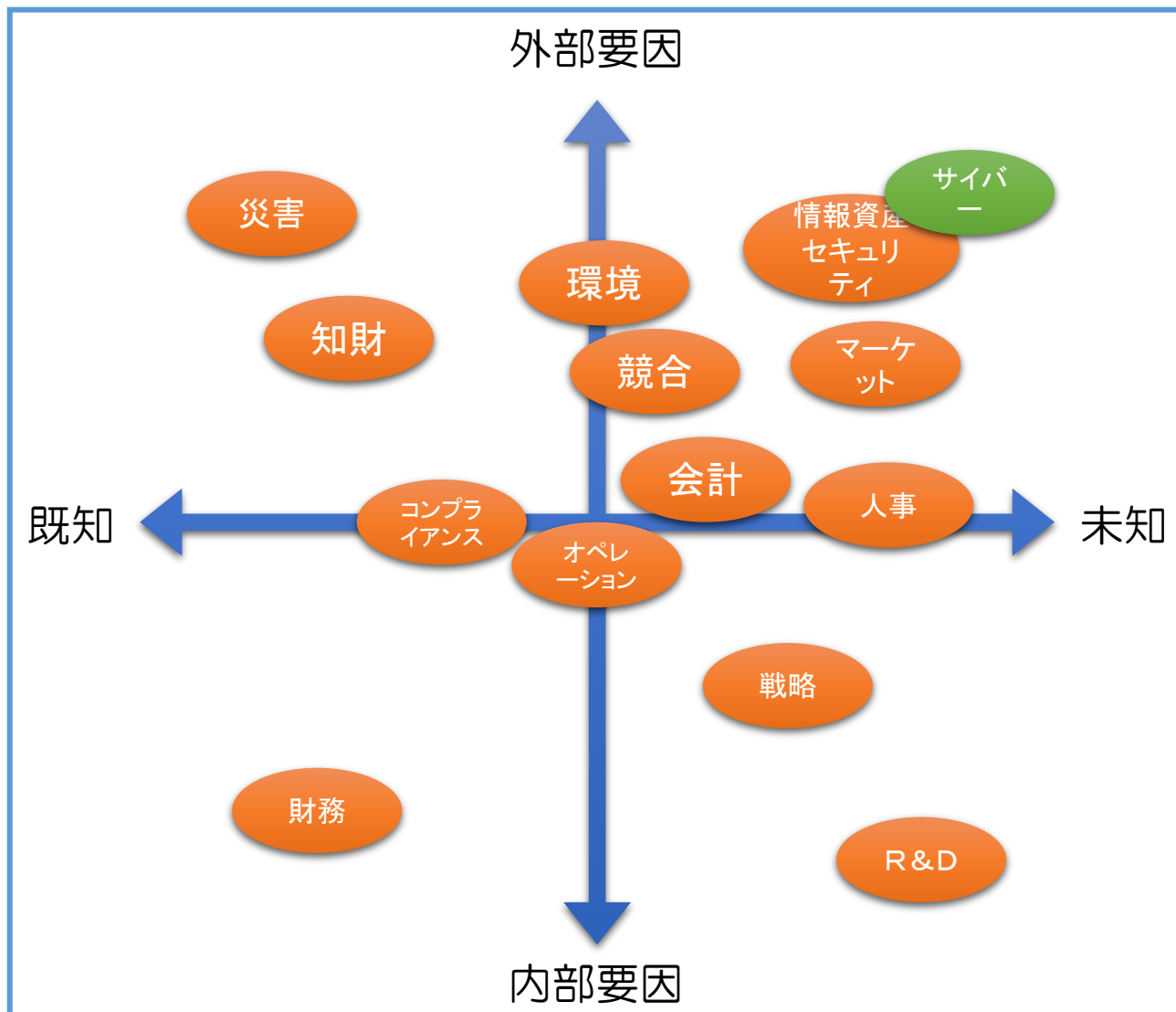
自助：自分の身は自分で守る

共助：同業とは仲良く

公助：人に迷惑をかけない

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



- 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。
- 日本特有の文化で、やられたものはたたかれる

サイバーセキュリティは経営者の責任である？

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

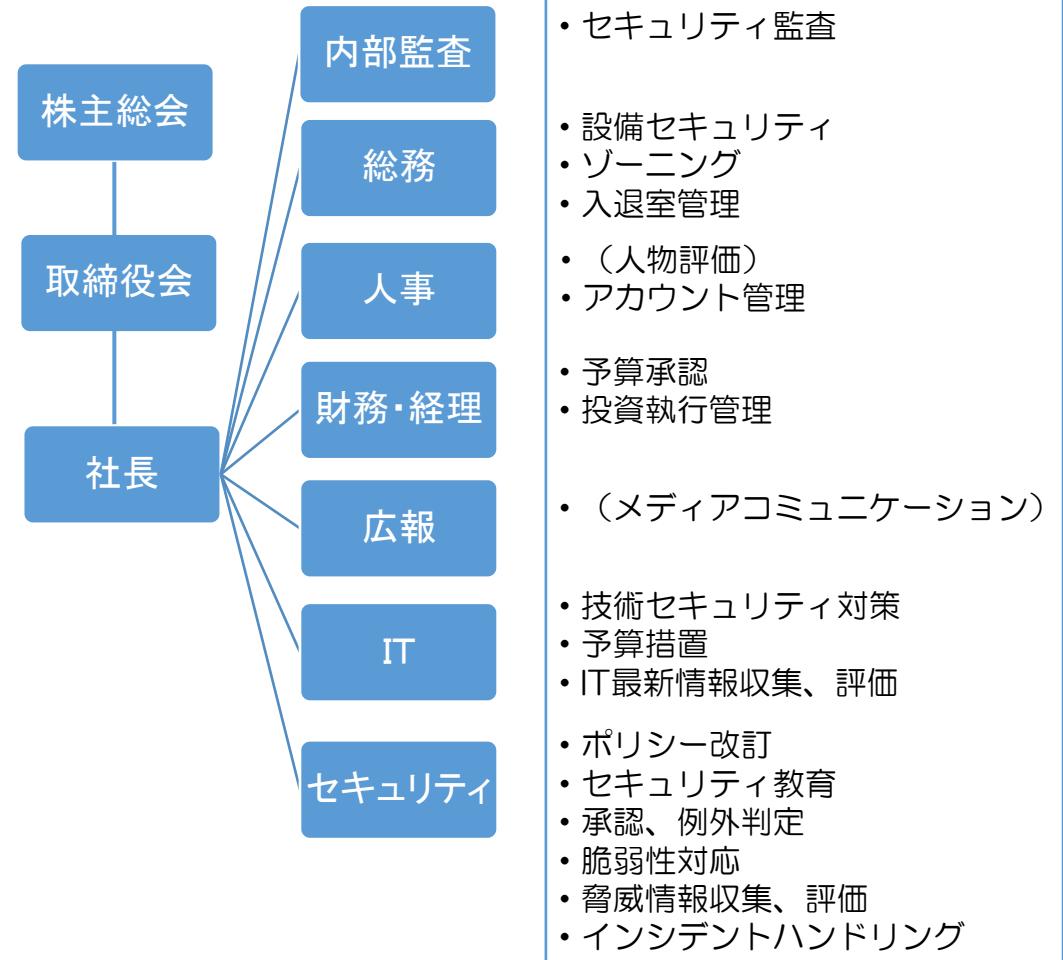
組織は目的を達成するための手段であるため、組織は戦略に従い、戦略は産業構造に従う。

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

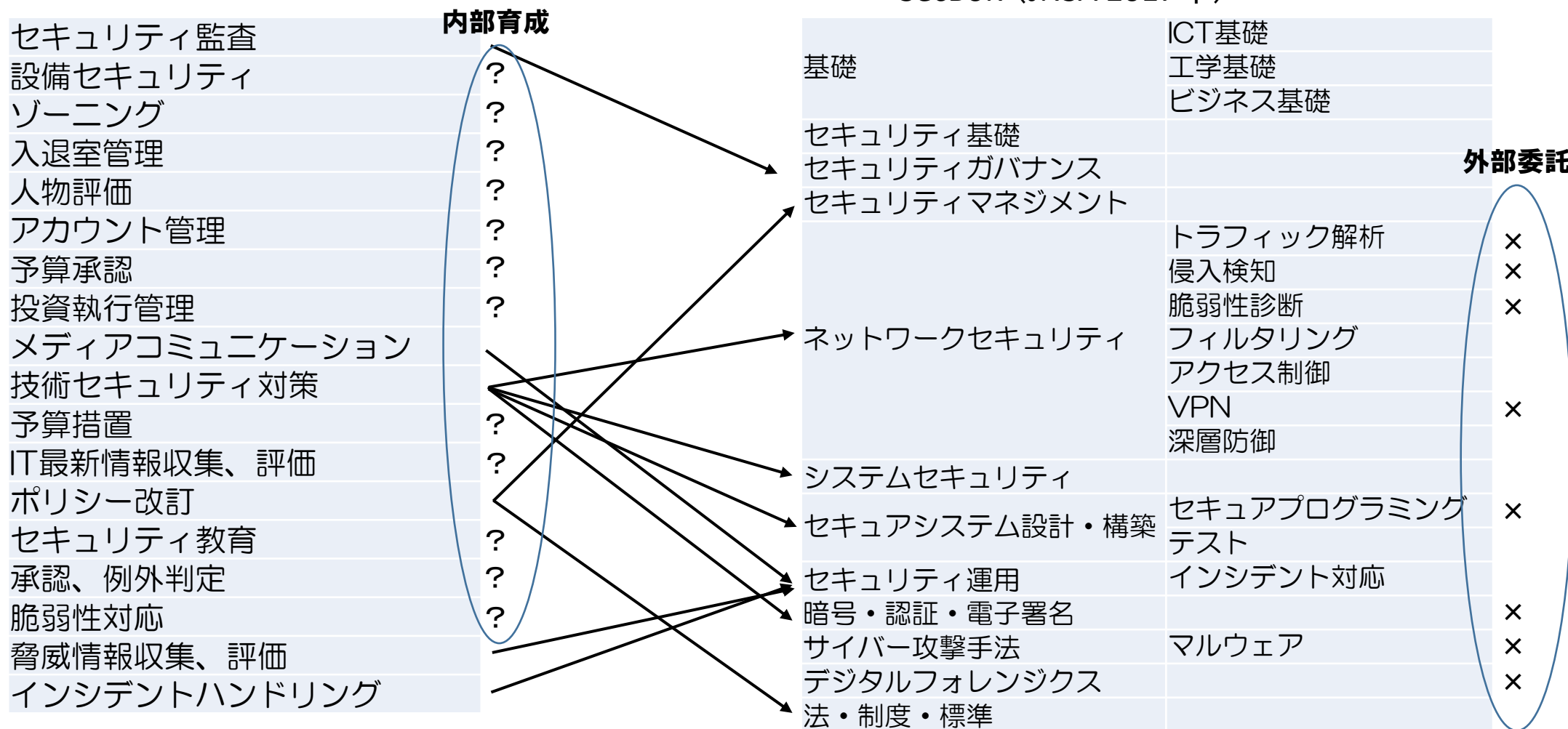
限りある経営資源に応じた戦略でないと、机上の空論。競争優位性のあるコアコンピタンスに注力すべき。 **実組織の役割**



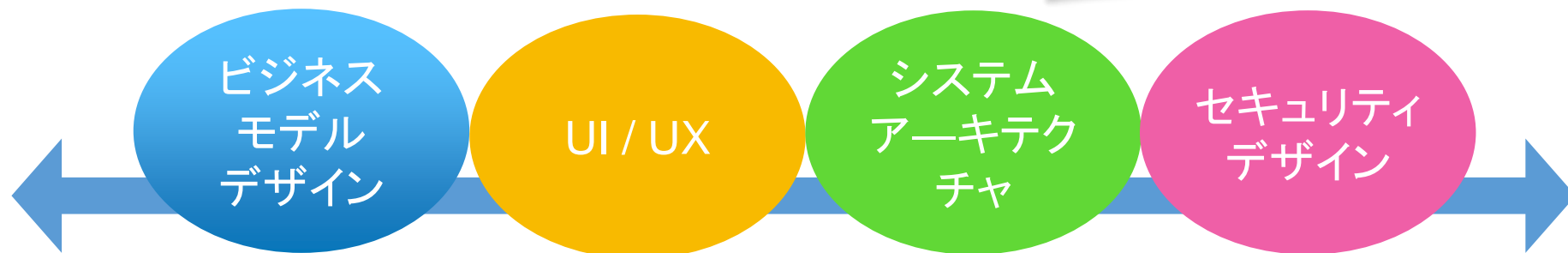
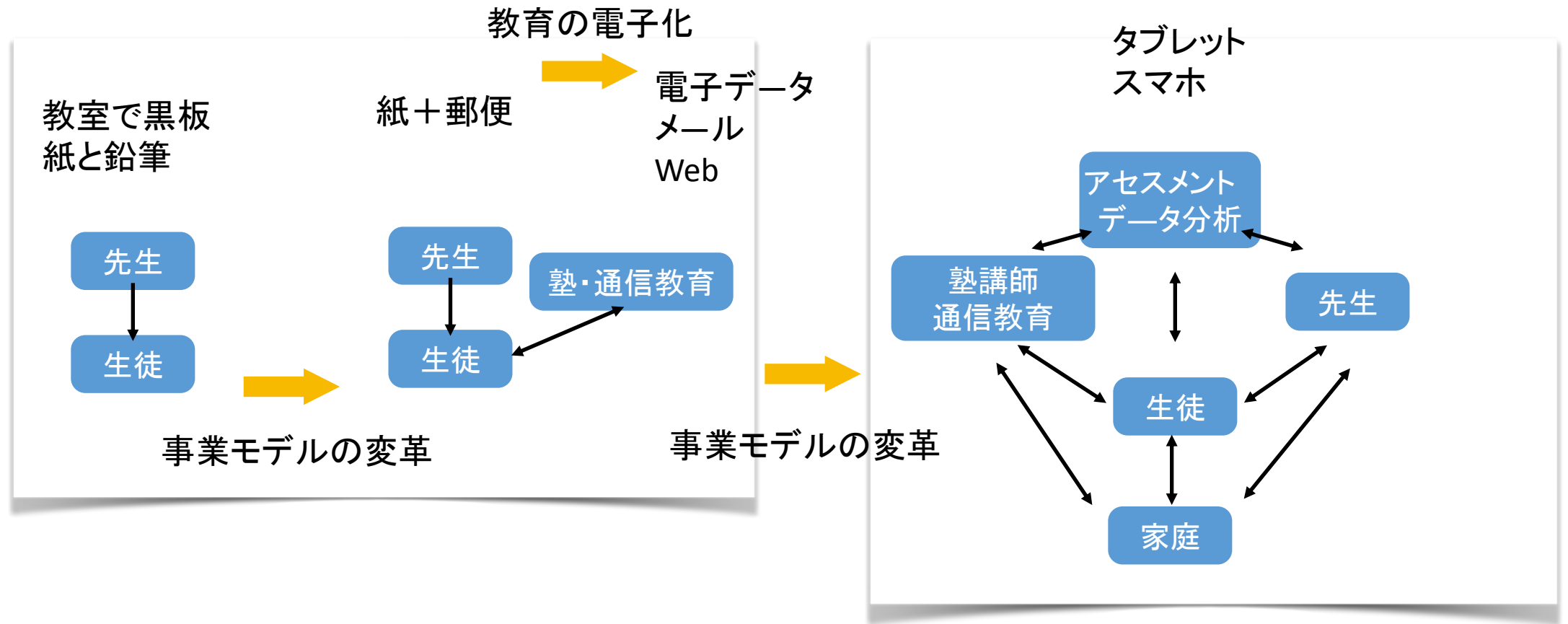
必要機能とセキュリティ人材とのギャップ

我が社が必要とするセキュリティ機能

セキュリティ人材スキルマップ SecBoK (JNSA 2017年)



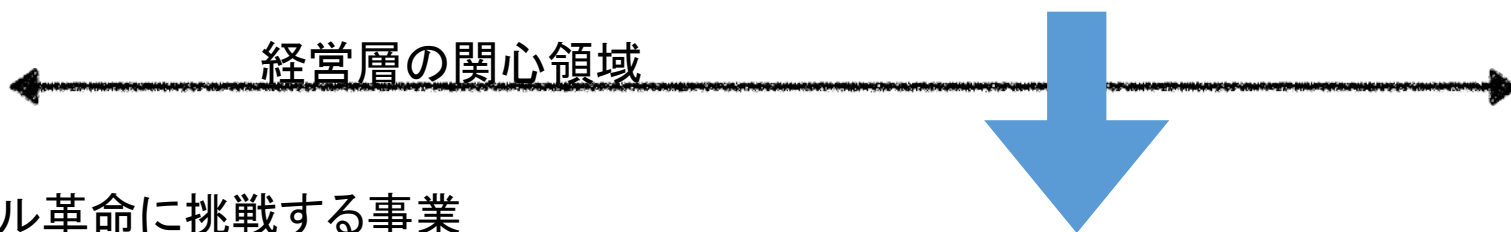
デジタル革命に挑む事業部門の情報セキュリティ



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 学習習慣 成績向上	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			
		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	—	—	—	—	—	—	—	—	○	—	—	—	—	—	—	○	—	○	○	—	—	○	○	



デジタル革命に挑戦する事業

	教育効果 学習習慣 成績向上	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			
		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	—	—	○	○	—	—	○	—	○	—	—	○	○	—	—	◎	◎	○	○	◎	○	○	○	