

データサイエンティストに対する サイバーセキュリティ教育の重要性

ワークショップ「データサイエンスにおけるサイバーセキュリティ教育事例」

2024/03/22

Kei Harada

• 原田 慧(はらだ けい)

➤D×2プログラム所属の教授

✓デザイン思考・データサイエンスでD×2

➤実務家教員

✓京都大学→名古屋大学(数理学博士)

→データサイエンティスト(12年)

✓23年3月まで普通に企業で働いていました

➤Kaggle Master

✓Kaggle: データサイエンスの競技会場

✓最適化関連が得意

✓AtCoder青色(max黄)

今日は実務家の立場からお話します



アカデミアを
離れてみたら
博士、道なき道をゆく

岩波書店編集部 編

岩波書店

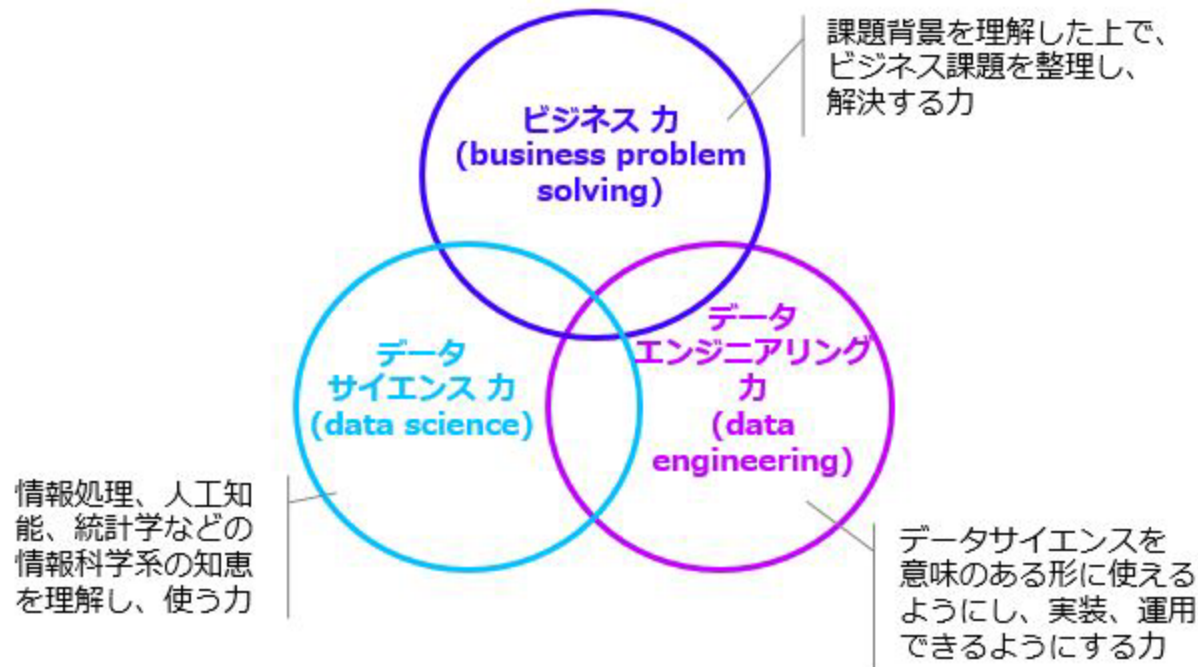
<https://www.amazon.co.jp/dp/4000614835>

- データサイエンティストのあり方の変化
 - 最近のトピック: オーナー不在
- セキュリティとデータサイエンティスト
 - なぜデータサイエンティストが怒られるのか
 - 怒られ事例1
 - 怒られ事例2
- まとめ
 - 優秀なデータサイエンティストほどプロジェクトの開始を任される
 - ✓ セキュリティのスペシャリストは後からやってくる。いつ巻き込めばいいのかわからない
 - ✓ (セキュリティの人には優しくしてほしい)
 - セキュリティの勘所がわかると嬉しい

データサイエンティストのあり方の変化

- 大きく3種類のスキルが必要とされている
 - 2014年にデータサイエンティスト協会が発表した有名な図

データサイエンティストに求められるスキルセット



<https://prt看es.jp/main/html/rd/p/000000005.000007312.html>

- 約10年で起きたこと(私見)

- 発表当初まで(～2014年ごろ)

- ✓ 全部できる人を普通の給料で雇おうとする無謀な企業
 - ✓ 「そんな超人いるわけないだろ」というプレイヤーの冷ややかな声
 - ✓ 自称なんでもできる人(意識高い系)の出現

- スキル定義・レベルが普及した数年後(2015年ごろ～)

- ✓ 「全部できる超人はいないから協力しよう」という動き
 - ✓ 個人プレーからチームプレーに
 - ✓ スキルの具体化、サイエンスのスペシャリストの増加
 - ✓ 新卒社員のレベル向上(←教育の充実)

- ここ最近(2020年～)

- ✓ 新しい職種の定着、細分化
 - ✓ 「リーダー不在」という課題の顕在化

「データサイエンティスト」の多様化

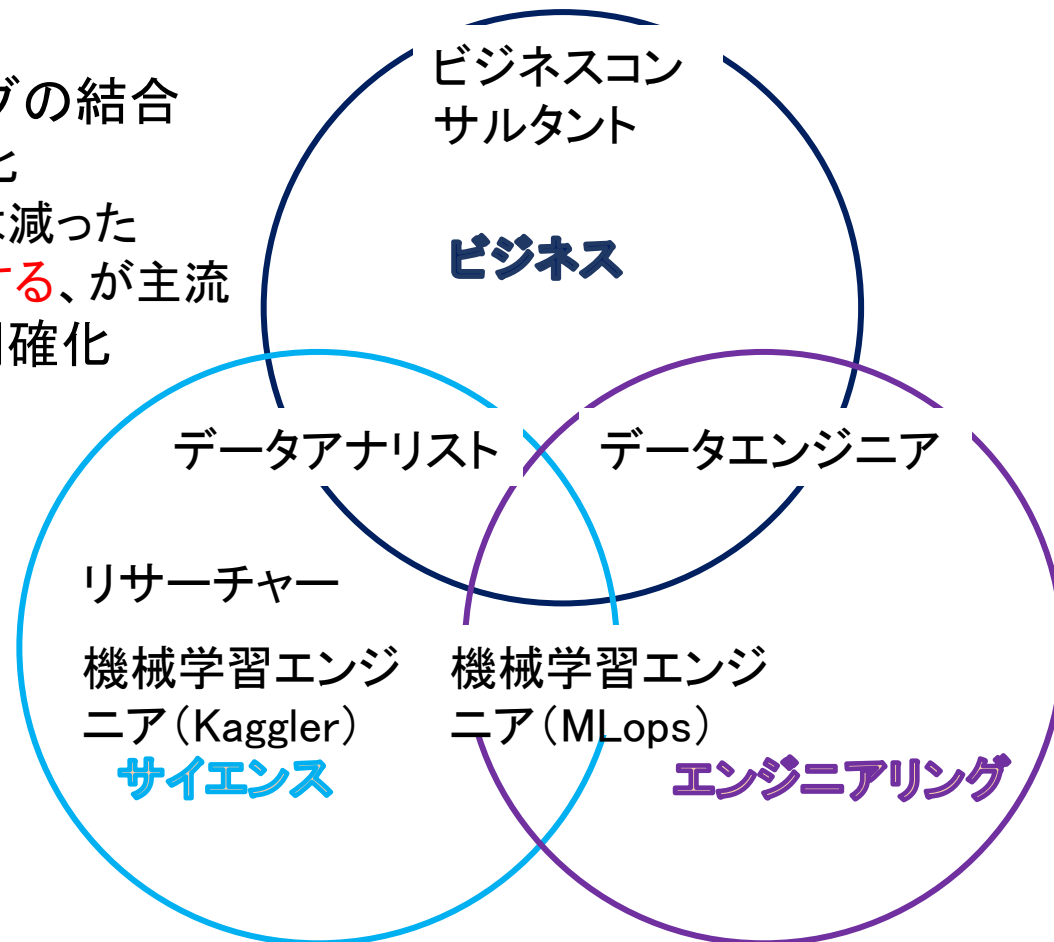
- DS職種マップ

- 会社により呼称は様々

- 最近の変化

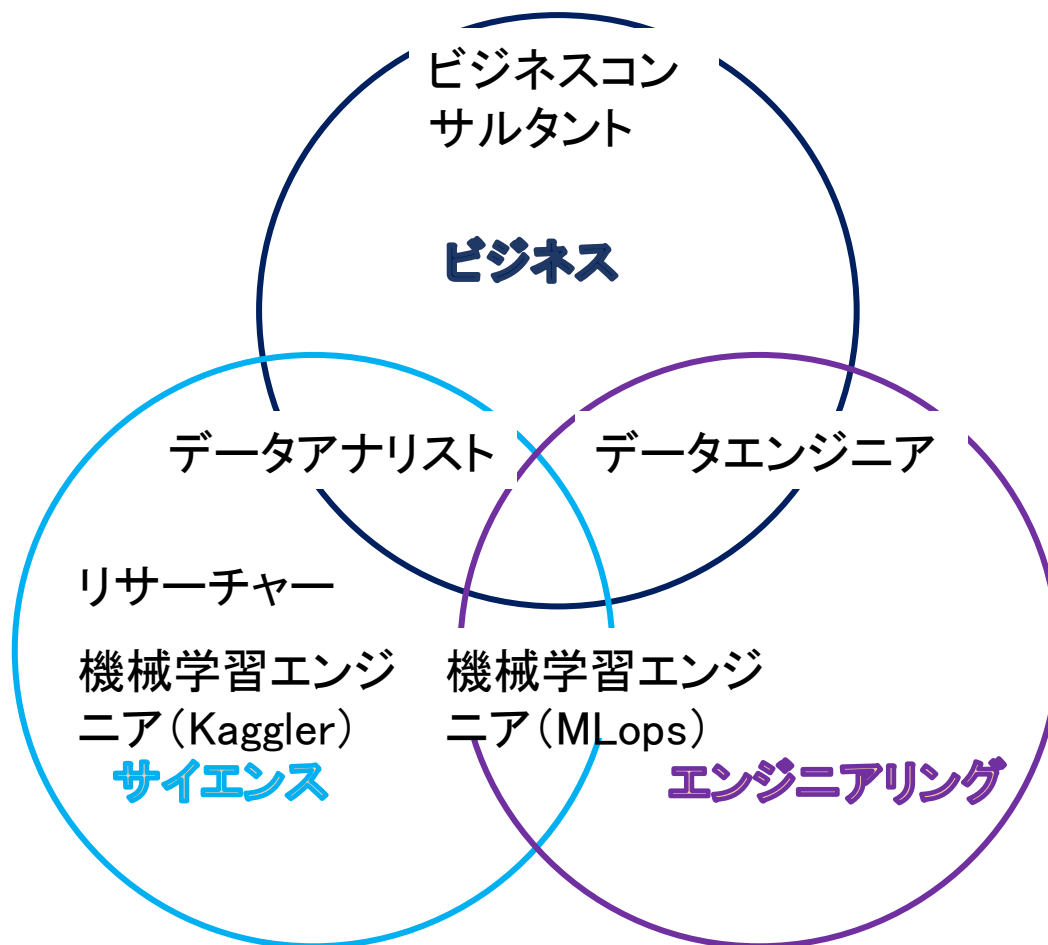
- サイエンスとエンジニアリングの結合
 - ✓ 人々の努力とツールの進化
 - ✓ サイエンスのみの働き方は減った
 - ✓ ある程度まで自分で実装する、が主流
 - ビジネスに寄り添う職種の明確化

- 細分化の結果
リーダーの不在が問題に



サイバーセキュリティとデータサイエンティスト

- 前の図にいないことから分かるように少し遠い



セキュリティの
エンジニア
(専門職)

- 両者が関わる時は大抵データサイエンティストが(やんわり)セキュリティの担当者に怒られるとき
 - DSはセキュリティの重要性を認識していないわけではない
 - 「セキュリティについては素人が判断するな、必ず専門家と相談しろ」と(まともな会社なら)新人研修で必ず教えられる
 - 前例があるプロジェクトなら簡単、ない場合が大変

データサイエンティスト



セキュリティ担当のエンジニア



「DX推進スキル標準」の人材類型

- 理想状態はこれらの類型・その下位区分のロールが(多少の兼務はあっても)埋まっていること

理想:

何がなんでもこれを作る！
予算はある、最終責任は私が取る！



DXの取組みにおいて、ビジネスや業務の変革を通じて実現したいこと(=目的)を設定したうえで、関係者をコーディネートし関係者間の協働関係の構築をリードしながら、目的実現に向けたプロセスの一貫した推進を通じて、目的を実現する人材

ビジネスの視点、顧客・ユーザーの視点等を総合的にとらえ、製品・サービスの方針や開発のプロセスを策定し、それらに沿った製品・サービスのありかたのデザインを担う人材



デザイナー

DXの推進において、データを活用した業務変革や新規ビジネスの実現に向けて、データを収集・解析する仕組みの設計・実装・運用を担う人材



データ
サイエンティスト

DXの推進において、デジタル技術を活用した製品・サービスを提供するためのシステムやソフトウェアの設計・実装・運用を担う人材



ソフトウェアエンジニア

業務プロセスを支えるデジタル環境におけるサイバーセキュリティリスクの影響を抑制する対策を担う人材



サイバーセキュリティ

データやデジタル
技術を活用した
製品・サービスや
業務などの変革

https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/main.html

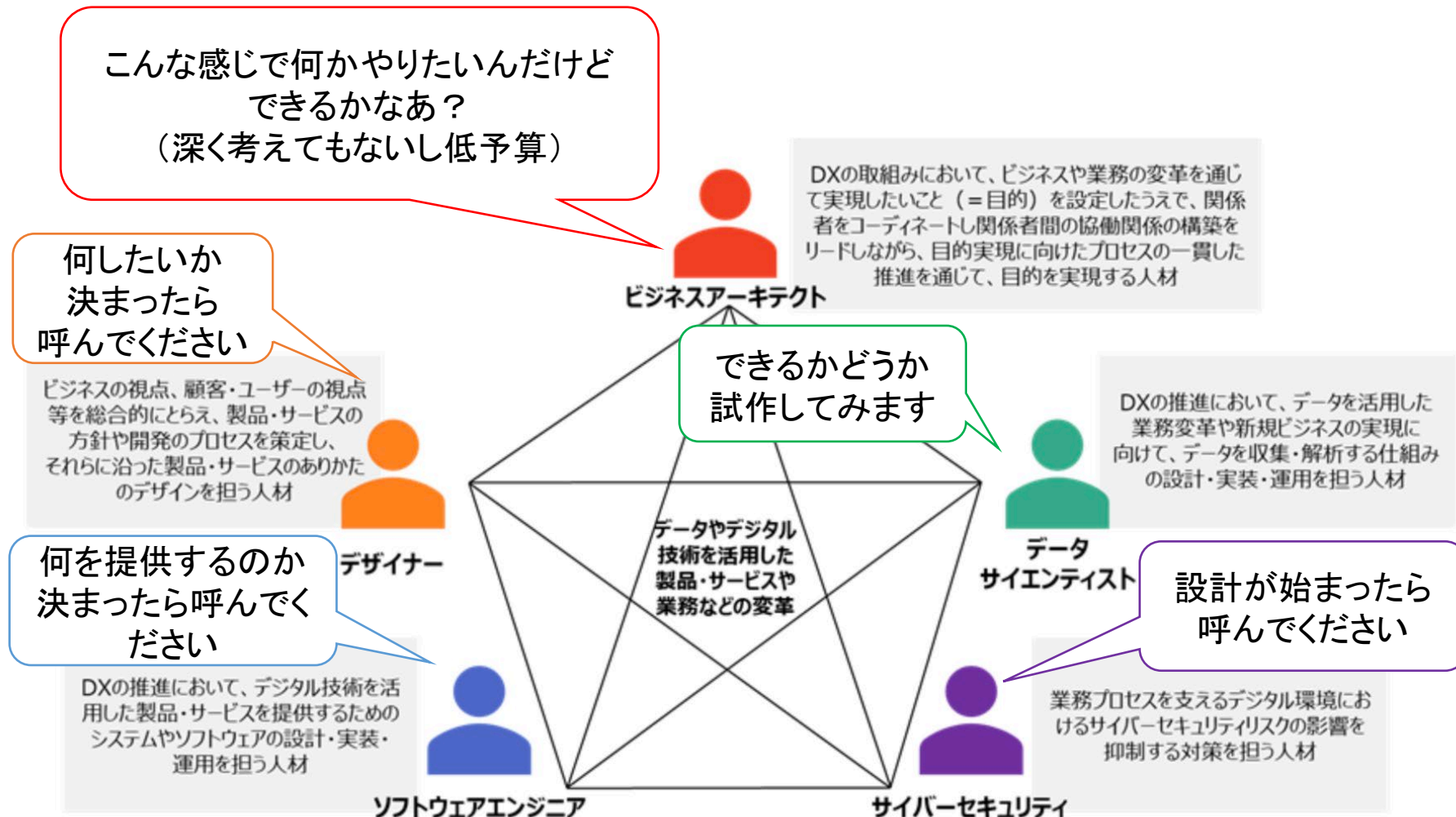
「DX推進スキル標準」の人材類型

- ビジネスアーキテクトへの要求レベルが高い
 - 技術的にできるかどうかもリスクの中で投資を受ける、起業と同じレベル
 - 大抵の人は大きい絵は描けない



https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/main.html

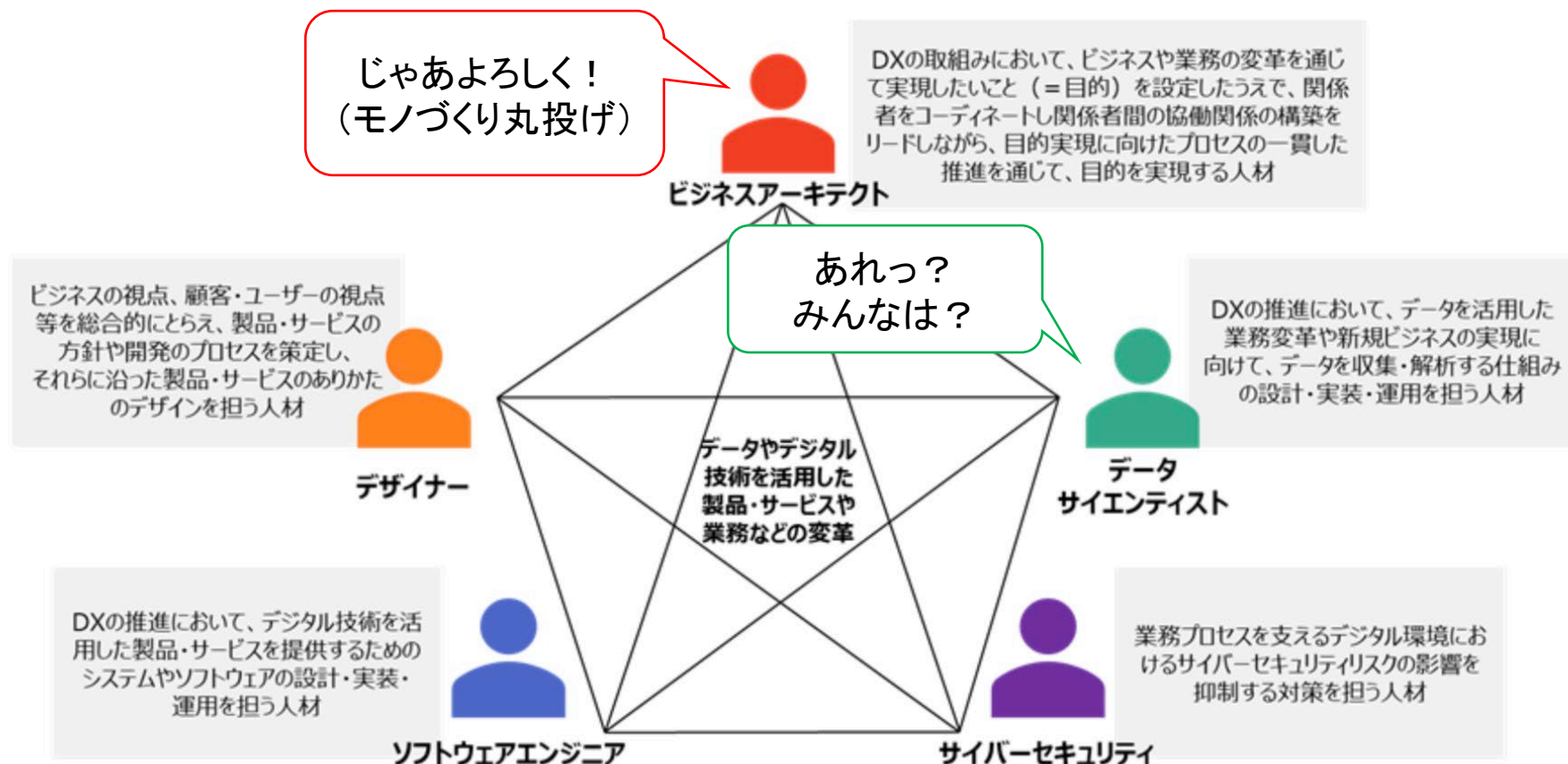
「DX推進スキル標準」の人材類型



https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/main.html

「DX推進スキル標準」の人材類型

- 現実にはデータサイエンティストが小さく始める、になりがち
 - 小さく実現可能性の検証となると動けるのはデータサイエンティスト



https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/main.html

- 微妙な試作品ができた状態で関係者集合
 - データサイエンティストがスキル違いで作ったので微妙なのは当然
 - ✓ セキュリティだけでなくソフトウェア、デザイン面でも微妙
 - しかし最初に案件に参画したデータサイエンティストに一日の長があつて、最も要件を理解している
 - 後から参画した人にとっては他人の作ったものを直すというつまらない仕事に

データサイエンティスト
(モノづくりチーム代表)



セキュリティ担当の
エンジニア 他



- 試作品を作って顧客(or ユーザー部門)と同意した、
だがその設計はセキュリティ上ダメ
 - 最初は何を作るか決まっていないし、何かを作るかも決まっていない
 - ✓ 顧客側としては試作品がないとわからないことが多い
 - ✓ 作るものが決まっていないので最初は低予算プロジェクトで色々試行錯誤する
 - 少人数のアジャイル開発とセキュリティは相性が悪い？

データサイエンティスト



なんで要件が決まった段階で相談
しないんですか！？

要件は先週決まったんです...

じゃあ何を作るか検討する段階から
巻き込んでくださいよ～

(モノづくりするかも決まってい
ないのにそんな予算はないです...)

セキュリティ担当の
エンジニア



注：理解のある人限定

怒られ事例あるある2

- お堅い会社のDX推進案件。順調に進んでいたが、いざ実装検討となったら出てきた先方のセキュリティ担当がお堅い

→炎上案件に

データサイエンティスト



セキュリティ担当(自社)



当社の常識にとらわれずに
新しいことをやっていきましょう！

その前に御社は初めてですのでベン
ダーチェックリスト(数百項目ある)を埋め
てください。×がついてもいいですが、そ
れぞれに代替の対策を記入してください。
それから外部と接続するとのことですが、
決裁が必要です、オンプレでの実装含め
た妥当性について再検討を...

ちょっと何言ってるかわからない。
セキュリティ部門さん助けて。

とてもつらい

DX推進者(顧客)



セキュリティ担当(顧客)



• 望ましいセキュリティとの関係

➤ デジタルスキル標準:

- ✓ 「データ管理やプライバシー保護 に関するポリシーの検討」がサイバーセキュリティとデータサイエンティストの連携らしい
- ✓ 実際にはそんな狭い範囲では済まなくて、設計者としてDSが全般を背負ってしまいがち

➤ 新しいものを作るときには特に大変で、データサイエンティストはセキュリティの問題で苦勞する

何を作るか決まってないのにセキュリティの話はできない

VS

何を作るか決まった時点で試作品があって、既にセキュリティの問題がある

➤ 勉強すれば勘所がわかるようになりそう

- ✓ ただし勉強したところで素人判断は本当に危険
- ✓ セキュリティを蔑ろにする意思は誰も持っていない、特に商用(数千万～)のものを作るならサイバーセキュリティのスペシャリストは絶対に必要
- ✓ とりあえず仲良くなる方法から？？？

