デジタルトラストとゼロトラストネットワーク

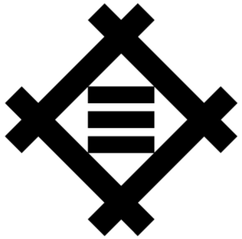
PKI & TRUST Days online 2021 - デジタル社会におけるトラスト

2021/04/15

所属先紹介 & 自己紹介

- 鈴木研吾 (@ken5scal)
- 所属:
  - LayerX株式会社 CTO室
  - 三井物産デジタル・アセットマネジメント 業務部
- O'Reilly「Zero Trust Network」監訳

LayerX



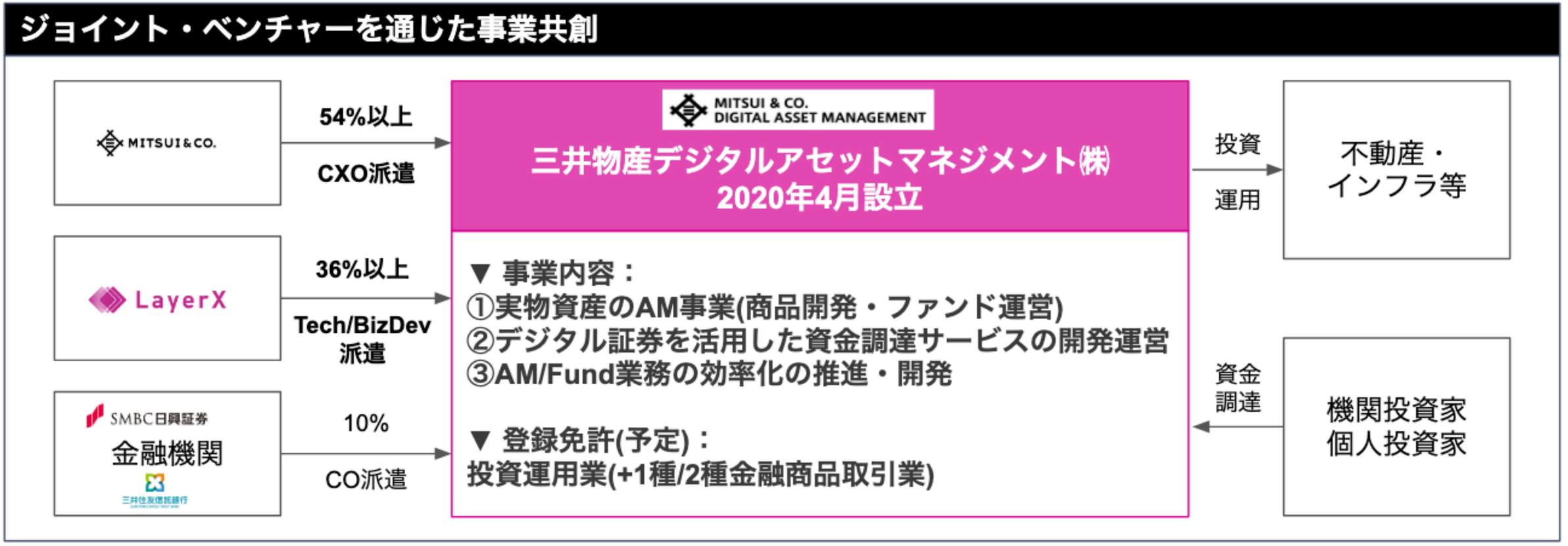
MITSUI & CO.
DIGITAL ASSET
MANAGEMENT

取組事例: 三井物産とアセットマネジメント領域で協業

JVを設立、共同事業として証券発行プロセスやファンド期中管理のDXを推進

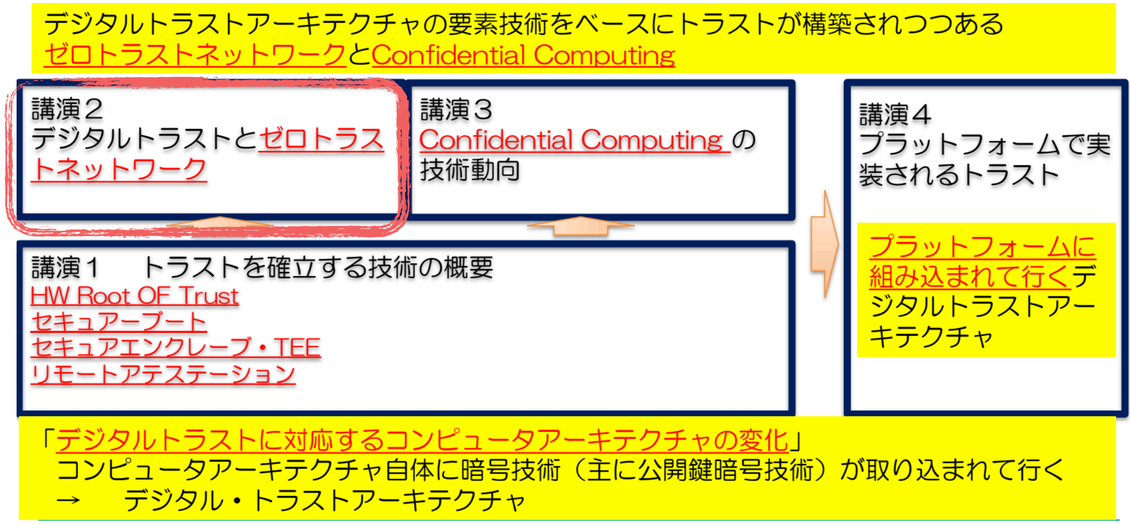
- アセットマネジメント領域にデジタル技術をフル活用
- 紙とFAXがはこびるファンド商品組成・資金調達・運用プロセスを効率化し、商品の収益性を向上
- デジタル証券を活用し、今まで証券化されなかった新たな投資商品を創造する

ジョイント・ベンチャーを通じた事業共創



今日のゴール

- Computing/Platform利用者側におけるトラスト
- 次セッションのディスカッションにおける情報整理



今日のアウトライン

- 今日のゴール
- 自己紹介
- デジタル社会とトラスト
- 自組織のトラスト

デジタル社会とトラスト
- サービスプロバイダがトラスト
してもらうには

信頼（Trust）とは

- 相手が利益を発生させる、しかし確実に行為することが確実ではないが、それでもその行為することを前提とした自分の行為
  - 「信頼」ニコラス・ルーマン
- 社会システム存続のための「複雑性の縮減」
  - 「信頼」ニコラス・ルーマン
- サービスの提供が第三者によるということから生じる 不確実性を解消するための要素
  - 「電子署名法の数奇な運命」
- 事実の確認をしない状態で、相手先が期待したとおりに振る舞うと信じる度合い
  - by Trusted Web推進協議会

信頼（Trust）の種類

- 慣れ親しみ、人格的信頼
- **システム信頼**
  - 特定の機能システムにおける行為同士を仲介するメディア
  - 「信頼の飛躍」のための媒介
  - 例
    - 経済（決済）システム: 貨幣
    - 経済（市場）システム: 金融商品

社会の複雑性は増えている

- 2014年: 第四次スタートアップブーム
  - 規制産業に参入するスタートアップの増加
  - 大手企業のオープンイノベーション追求とスタートアップ連携
  - 例:
    - 金融のアンバンドリング、Embedded Finance
- コロナによる強制テレワーク化
- 改正個人情報保護法

デジタル化とは

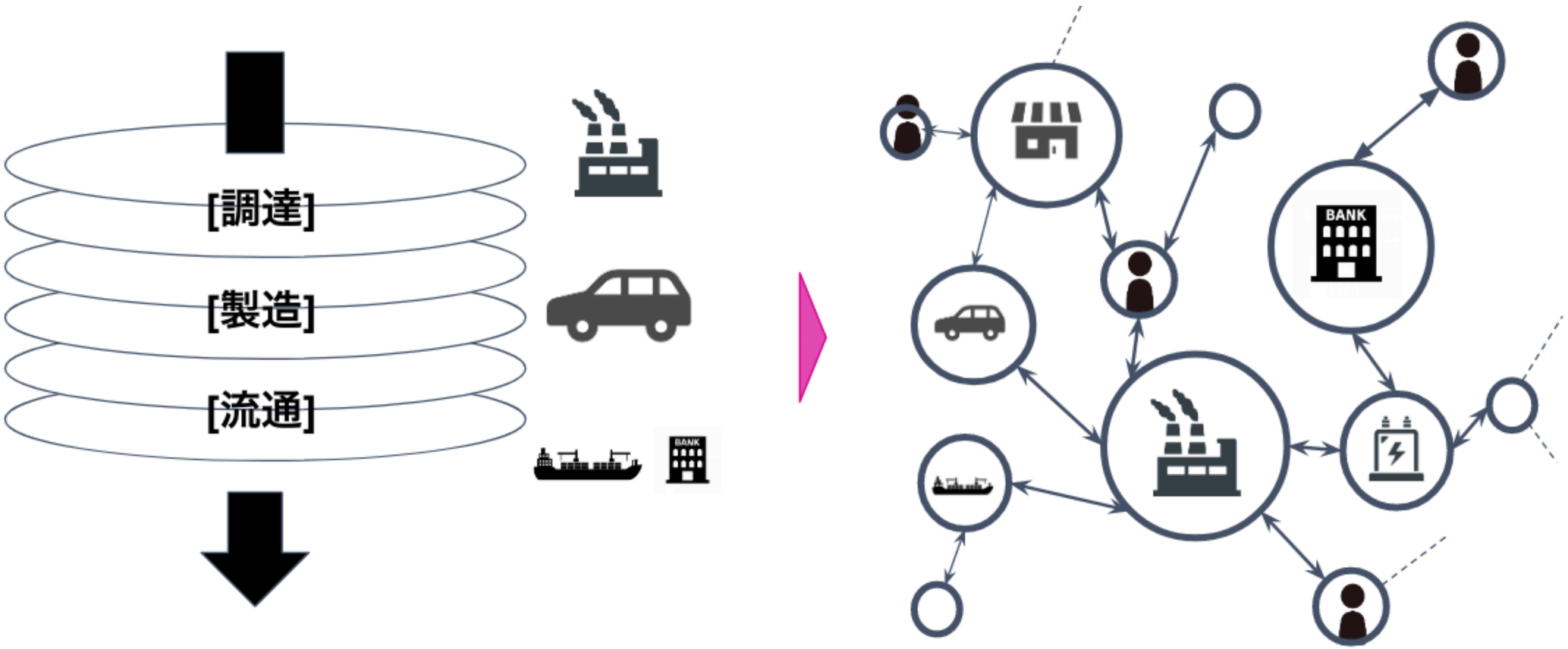
LayerXが定義する「DX」

一般定義	「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、**製品やサービス、ビジネスモデルを変革**するとともに、**業務そのものや、組織、プロセス、企業文化・風土を変革**し、競争上の優位性を確立すること。」

LayerXのパートナー

既存レガシーが重く、バリューチェーンが複雑な企業・産業	「既存業務を、**ソフトウェア的パーツの集合に再定義**すること。バリューチェーンの複雑さ故の煩雑な**業務を人手から開放し、単一事業のコスト削減**を行う。またソフトウェア的パーツに再定義することで接続性や利用性を向上させ、予期せぬ**バリューチェーン参加者へのエコシステム開放で新たな収益源**を作る。」

デジタル化と複雑性



デジタル化と複雑性と信頼

- “従来の社会と同じものを構築するに足る信頼（Trust）を担保する仕組み” = **システム信頼**が必要
  - 「デジタル社会のTrustの構築とインセンティブデザイン〜2020年を振り返って〜」https://media.dglab.com/2020/12/25-trust-1/
- 人格的信頼に比べると、人物ごとに信頼を確認する必要がないので、学習しやすい
- 一方、より強いResiliencyが必要
  - 信頼問題にとって警鐘を鳴らすような出来事、特別な防御策を促すような出来事を、システムの動作にもたせなければならないため、コントロールは遥かに難しくなった
  - 維持と破棄を同時に実現する必要性によって、システム信頼が高まり、一方リスクも高まった

P92

システム信頼を構築するものは？

原動力は「信頼」です。

360°
business
innovation.

With Integrity

三井物産グループ行動指針

MITSUI&CO.

三井物産グループ行動指針

[問い合わせ先] 法務部コンプライアンス室
mbkhotline@mitsui.com
03-3285-7789

行動指針本文の
内容は、こちらから

講演１　13：45-14：20

「トラストを確立する技術の概要 〜 どのような技術がなぜ作られてきたのか 〜」

宮澤 慎一 氏（セコム株式会社 IS研究所 主務研究員）

＜概要＞
IoT機器、スマートフォン、PC、サーバーなど、小規模な機器から大規模な機器まで、Secure BootやAttestationなど「トラストを確立する技術」が適用されるようになってきました。これらの技術を組み合わせることによって、どんな人間に渡った後でもどんなネットワーク越しでも「接続対象のハードウェアが想定した機器なのか」「その上で動作しているソフトウェアが想定したソフトウェアなのか」を確認し確実にすることが可能となります。これらの技術は、いつごろ、なぜ登場してきたのでしょうか？本講演では、歴史を振り返りつつ技術の概要を紹介します。

- **Trustを実現するものとは、Integrity**
- **Integrity** = Tamper Proof + Isolation

Integrity

Integrityとは何か

- Integer: In(否定)-Tangere(触れる)　から Integrityへ
- 触れられてない状態、かけてない状態　から　正直、誠実、高潔、首尾一貫性
- 自分自身の原則と行動を調和させようと努力する人であり、自己の内部の一貫性を維持するよう懸命に努力している状態

論　文

日本経営倫理学会誌
第26号（２０１９年）

インテグリティとは何か

What is Integrity?

麗澤大学大学院経済研究科　博士課程　大　塚　祐　一
Reitaku University, Graduate School of Economics and Business Administration　Yuichi Otsuka

ABSTRACT

The notion of integrity, one of the central concepts in business ethics, has been perceived as a virtue of character and recognized as an essential quality that manager and leader should hold. Every time corporate scandals and corporate unethical behavior come into the open, we repeatedly hear the word. However, despite the common sense that integrity is important, there is no common definition or understanding because of its ambiguity. In this paper, as a first step of understanding of integrity, I will roughly describe the outline of integrity. In that work, I will classify the previous studies on integrity into broad sense and narrow sense and then try to give integrated interpretation of integrity.

キーワード
狭義のインテグリティ、広義のインテグリティ、首尾一貫性

Integrityの対象 in デジタル社会

- 自分自身の原則と行動を調和させようと努力する人であり、自己の内部の一貫性を維持するよう懸命に努力している状態
  - Digital Identity GuidelineやISO 24760でいうとEntity
- Q: デジタル社会において”既存業務をソフトウェア化”した場合、このEntityは何があたるのか

Integrityの対象 in デジタル社会

- 自分自身の原則と行動を調和させようと努力する人であり、自己の内部の一貫性を維持するよう懸命に努力している状態
  - Digital Identity GuidelineやISO 24760でいうとEntity
- Q: デジタル社会において”既存業務をソフトウェア化”した場合、このEntityは何があたるのか
  - **A: デバイス**

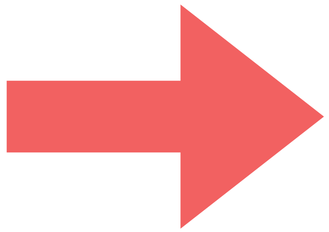
Devices as an Entity

- “The next decade promises the universal democratization of connectivity to every device.”
  - 「The Severn Properties of Highly Secure Devices」https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf
- 単純な入出力装置から、人間のデジタル活動を代理とするAgent
  - ブラウザ、ブラウザエクステンション、バイナリ、デスクトップアプリというUser-Agentの元締め



Integrity of the Device

自分自身の原則と行動を調和させようと努力する人であり、自己の内部の一貫性を維持するよう懸命に努力している状態



自分自身に課せられたポリシーに準拠しようと努力するデバイスであり、ポリシーとの一貫性を維持するよう懸命に連携している状態

デジタル化

全体としてのDevice Integrity

CAPCOM

2021年4月13日

大阪市中央区内平野町三丁目1番3号
株式会社カプコン
代表取締役社長 辻本 春弘
(コード番号：9697 東証第1部)

不正アクセスに関する調査結果のご報告【第4報】

株式会社カプコンは、第三者による不正アクセス攻撃を受け、当社グループが保有する個人情報が流出しま
したこと（以下「本インシデント」といいます。）を2020年11月4日から2021年1月12日にかけて公表いた
しました（以下「既報」といいます。）。
この度、外部の専門企業の協力のもと進めてまいりました本インシデントに関する調査が完了し、報告書
を受領しましたので、当該調査結果および再発防止に向けた取り組みにつきましてご報告申しあげます。
なお、当社グループのシステムは現時点でほぼ復旧しており、新設の「セキュリティ監督委員会」と連携
し、今後も継続的にセキュリティ、個人情報保護の強化を図ってまいります。
お客様はじめ多くのご関係先にご心配とご迷惑をおかけいたしましたことを、深くお詫び申しあげます。
また、お客様はじめ関係各位のご支援に深く感謝申しあげます。

2020年10月、当社の北米現地法人（Capcom U.S.A., Inc.）が保有していた予備の旧型VPN（Virtual Private Network）装置に対するサイバー攻撃を受け、社内ネットワークへ不正侵入されたものと調査により判断されています。当時、同現地法人を含め当社グループでは既に別型の新たなVPN装置を導入済でしたが、同社所在地であるカリフォルニア州における新型コロナウイルス感染急拡大に起因するネットワーク負荷の増大に伴い、通信障害等が発生した際の緊急避難用として同現地法人においてのみ当該旧型VPN装置1台が残存しており、サイバー攻撃の対象となりました。なお、現時点で当該装置は既に廃棄済みです。

その後、かかる北米現地法人の当該旧型VPN装置を経由して米国および国内拠点における一部の機器に対する乗っ取り行為が実施され、情報が窃取されるに至ったと判断されています。従来より境界型※1のセキュリティ対策は敷いており、また、後述するSOC※2サービスやEDR※3といった防御策の導入にも着手しておりましたところ、新型コロナウイルス感染拡大に伴いインフラ整備を優先せざるを得なかった結果、本件発生時は検証の途上（未済）でした。

https://www.capcom.co.jp/ir/news/html/210413.html

ゼロトラスト

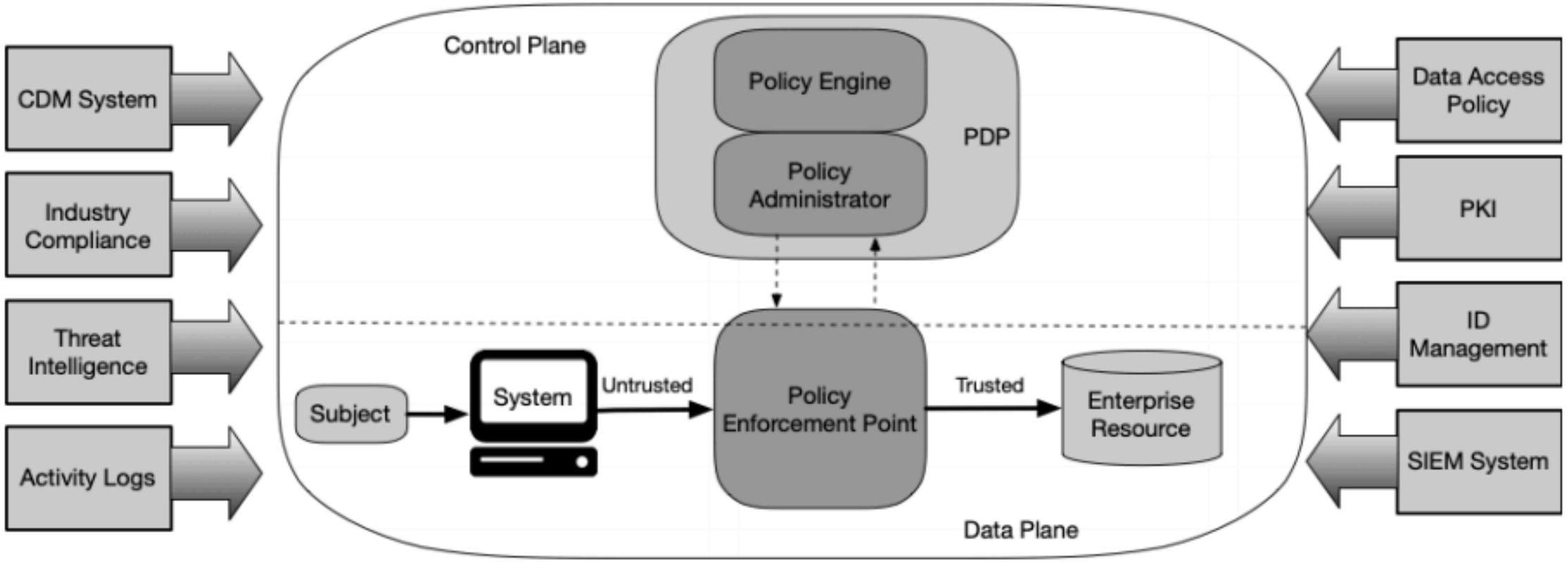
ゼロトラストに関する全般知識

ユーザー企業における情報システムとセキュリティ - 全体像編

2019/08/10 By @ken5scal

https://speakerdeck.com/ken5scal/yuzaqi-ye-niokeruqing-bao-sisutemutosekiyuritei-number-seccamp2019

トラストの基点を多様化させたゼロトラスト



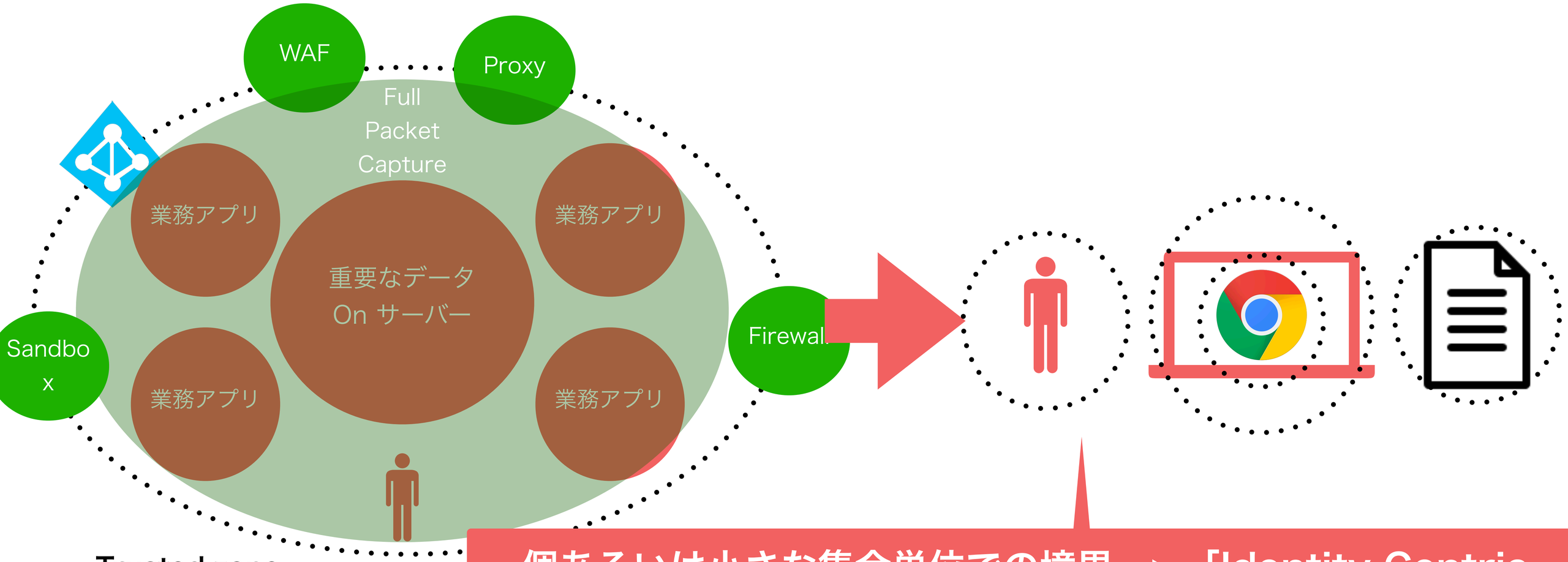
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf

ゼロトラストが求められる背景

- 業務環境の離散と多様化
  - スマートデバイスとテレワーク
  - 基幹システムおよびユーザー向け基盤のクラウド化
- 変わらないセキュリティ要件と脅威
  - 複数組織間でのデータのやり取り（例: 銀行API）
  - サプライチェーンが広がる中、従来の脅威をMitigate

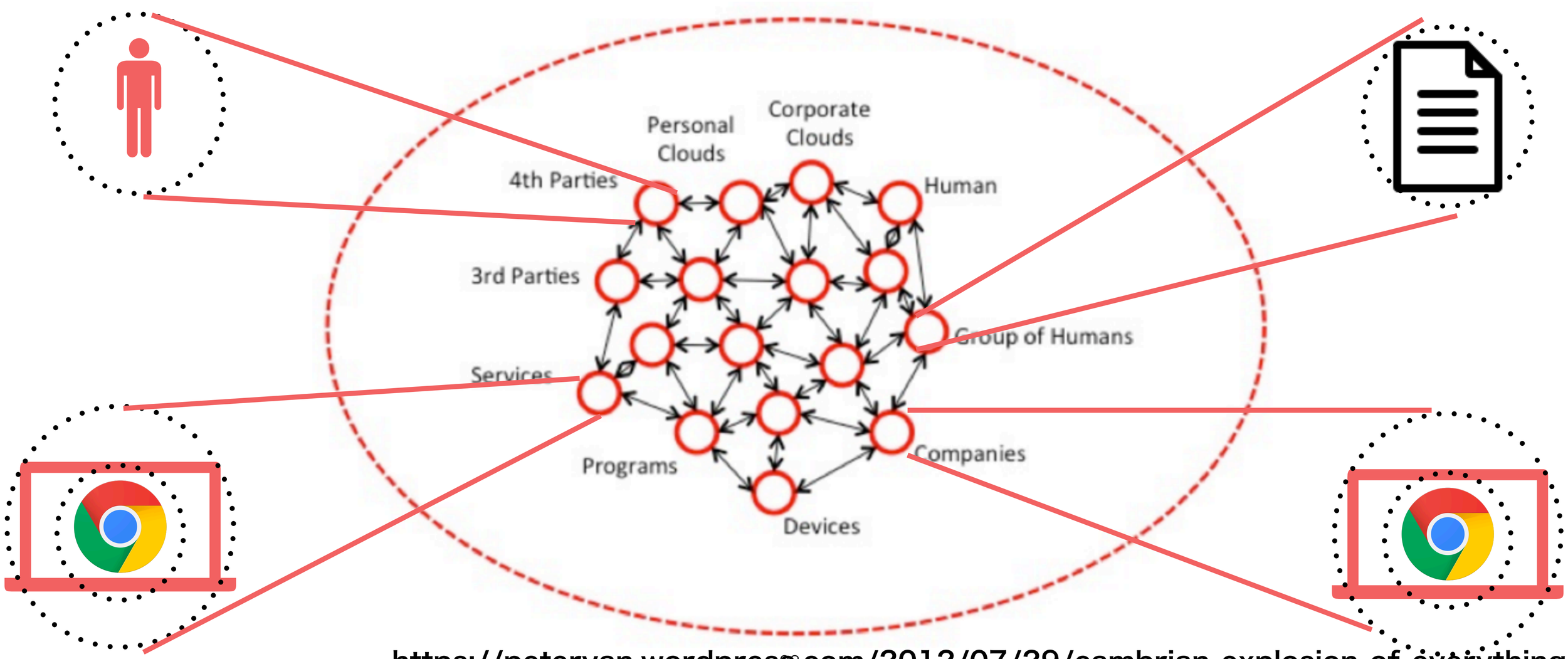
上記に応える柔軟で堅牢な実装を可能にする
設計思想および全体設計がゼロトラスト

その結果起こること: Trusted Zoneのマイクロ化



- 個あるいは小さな集合単位での境界 => 「Identity Centric」
- 場所や時間を問わない検証 =>「Always Verify」

同時にDevice郡（Fleet）のIntegrityが外せない



https://petervan.wordpress.com/2012/07/29/cambrian-explosion-of-everything/

Beyond Corp - Building a Healthy Fleet

- Control（対策?管理?）的観点からのHealthy Fleetの定義付け
- Controlが一貫して且つ包括的に計測・適用された状態
- 計測(measurement）によってControlの継続的に改善できる状態

Hunter King is an Engineer on the Security Operations team at Google. Currently, he focuses on endpoint integrity and identity. Hunter has also been a Lead Engineer in the BeyondCorp effort for the last seven years. Prior to Google, he was a Security Researcher at SecureWorks. He enjoys hiking, tinkering, and making lights blink. Hunter holds a bachelor's degree in computer science from Colgate University. hunterking@google.com

Michael Janosko is a Security Engineer Manager in Google's Enterprise Infrastructure Protection group, where he helps secure the way Google works. On weekends, he enjoys a good cup of coffee while building forts with his son. janosko@google.com

Betsy Beyer is a Technical Writer for Google Site Reliability Engineering in NYC, and the editor of *Site Reliability Engineering: How Google Runs Production Systems* and the forthcoming *Site Reliability Workbook*. She has previously written documentation for Google Datacenter and Hardware Operations teams. bbeyer@google.com

Max Saltonstall is a Technical Director in the Google Cloud Office of the CTO in New York. Since joining Google in 2011, he has worked on video products, internal change management, IT externalization, and coding puzzles. He has a degree in computer science and psychology from Yale. maxsaltonstall@google.com

Any security capability is inherently only as secure as the other systems it trusts. The BeyondCorp project helped Google clearly define and make access decisions around the platforms we trust, shifting our security strategy from protecting services to protecting trusted platforms. Previous BeyondCorp articles discussed the tooling Google uses to confidently ascertain the provenance of a device, but we have not yet covered the mechanics behind how we trust these devices.

Our focus on platform security is supported by a wealth of evidence [1] in the industry that end users are the number one target of a wide range of attacks that also vary in sophistication. Attackers can devise quite advanced social engineering attacks as mechanisms to deliver malicious code onto devices, where they can then exploit the large attack surface of modern operating systems. Advanced attackers aim to reuse trust inherent in the device, the credentials on the device, or the trust granted to the user to further exploit systems.

To successfully prevent compromise in environments with a constant mix of trusted (enterprise web apps, corporate credentials) and untrusted content (external software repos, social media, personal email, etc.), the platforms themselves must have a layered and consistent set of controls. As a result, the platforms that make up the fleet are the new perimeter.

Building upon Previous Work

The work we describe in this article builds upon the work described in the white paper "Fleet Management at Scale" [2] and the previous five BeyondCorp articles [3]. Building on this foundation, our team aimed to further strengthen the BeyondCorp model by:

1. Defining what a healthy fleet looks like from a common control perspective
2. Ensuring that these controls are consistently and comprehensively applied, measured, and enforced
3. Using these measurements to drive continuous improvement in our control set

Defining the Threats against Your Environment

As with any defensive security effort, it's important to first define the threats against the environment you're trying to protect. When creating this list of threats, it's helpful to think of classes of attacks instead of all the variants of a single attack. Attackers are constantly discovering new variants of attacks, which makes defining the entire tactical threat environment impossible. However, if you successfully mitigate a class of attacks, then variants within that class should be less concerning [4].

At a very high level, some classes of threats to consider aga inst your platforms include:

1. **Unknown devices**: sensitive systems accessed by unknown or unmanaged devices
2. **Platform compromise**: exploitation of a misconfigured operating system or software on the platform

Healthy Fleetを毀損しうる脅威

- Unknown Devices
- Platform Compromise
- Security Control Bypass
- Privilege Escalation
- SW Compromise
- Attack Persistence
- Authentication Bypass
- Data Compromise
- Attack Concealment
- Attack Repudiation

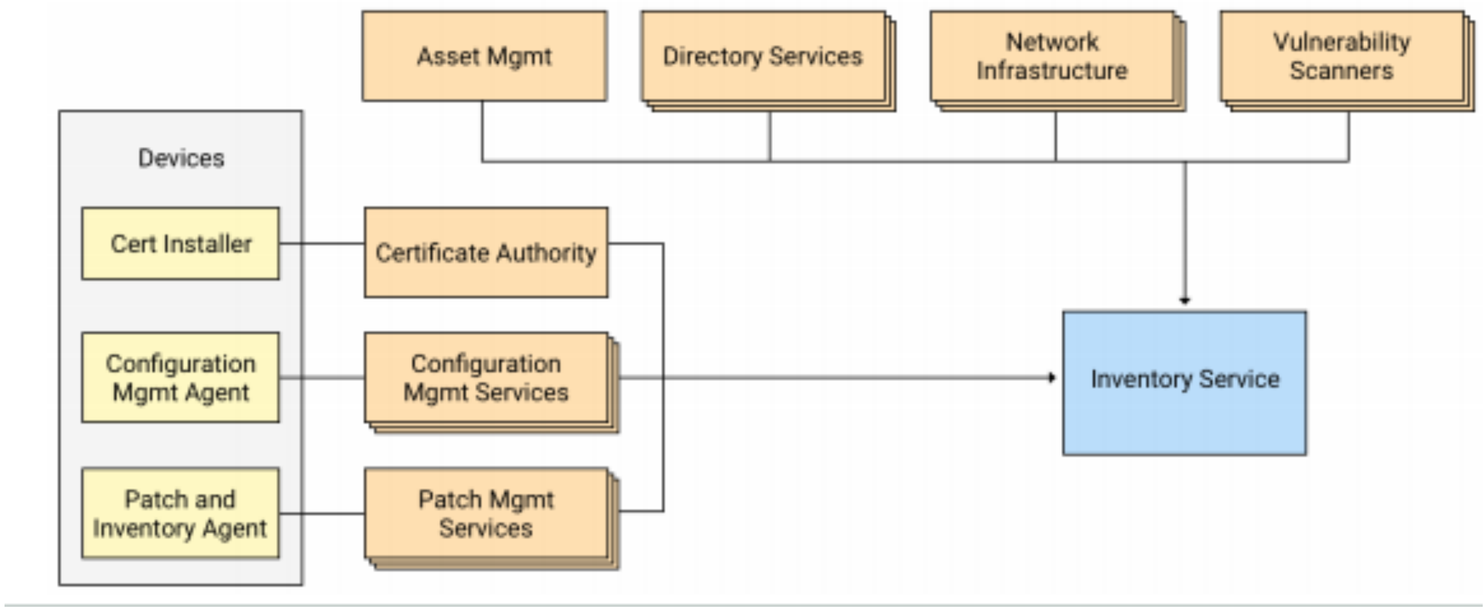
Healthy Fleet関連の脅威への対策

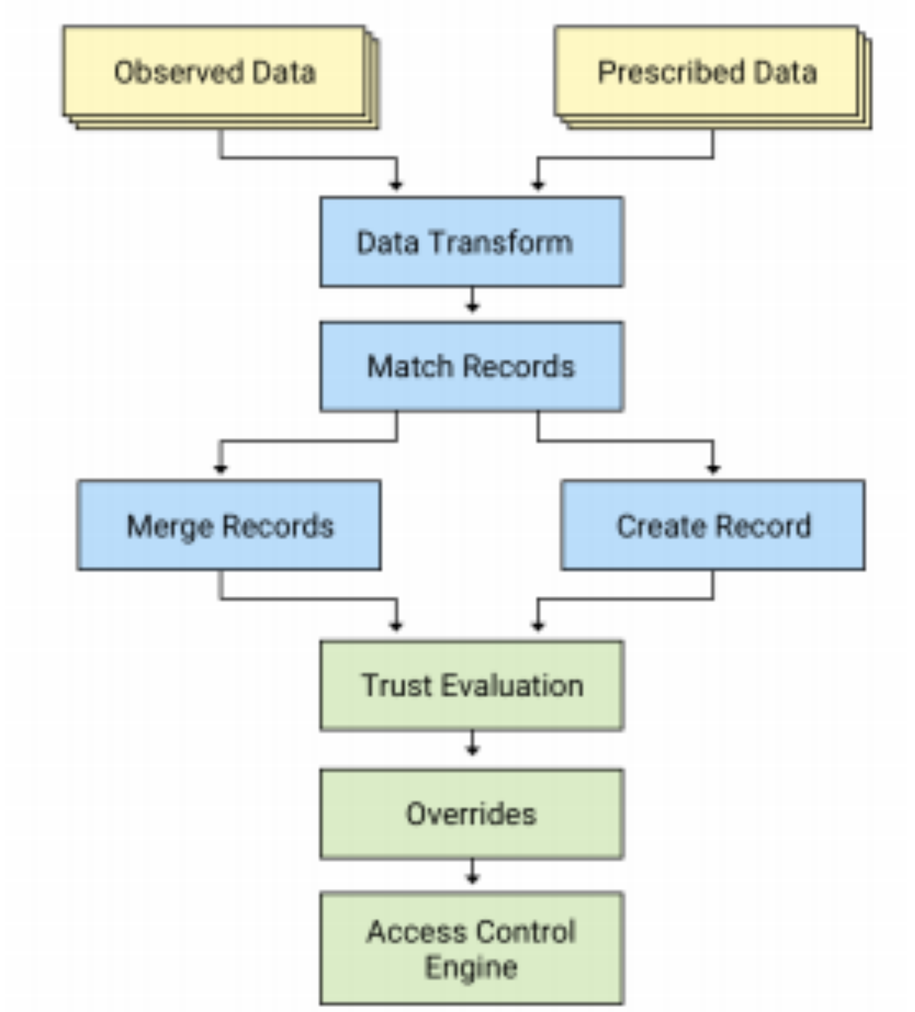
- Fleet inventory and asset mgt
- OS & base sw config mgt
- Security Policy mgt and Enforcement
- Resilience against system takeover & persistence
- SW Integrity and Control
- Remotely verifiable platform state
- Robust authn platform and user
- Data Protection
- Logging and Log Collection fro Detection Capability
- Resource capability on platform/Detection Response

Healthy Fleetを毀損しうる脅威と対策

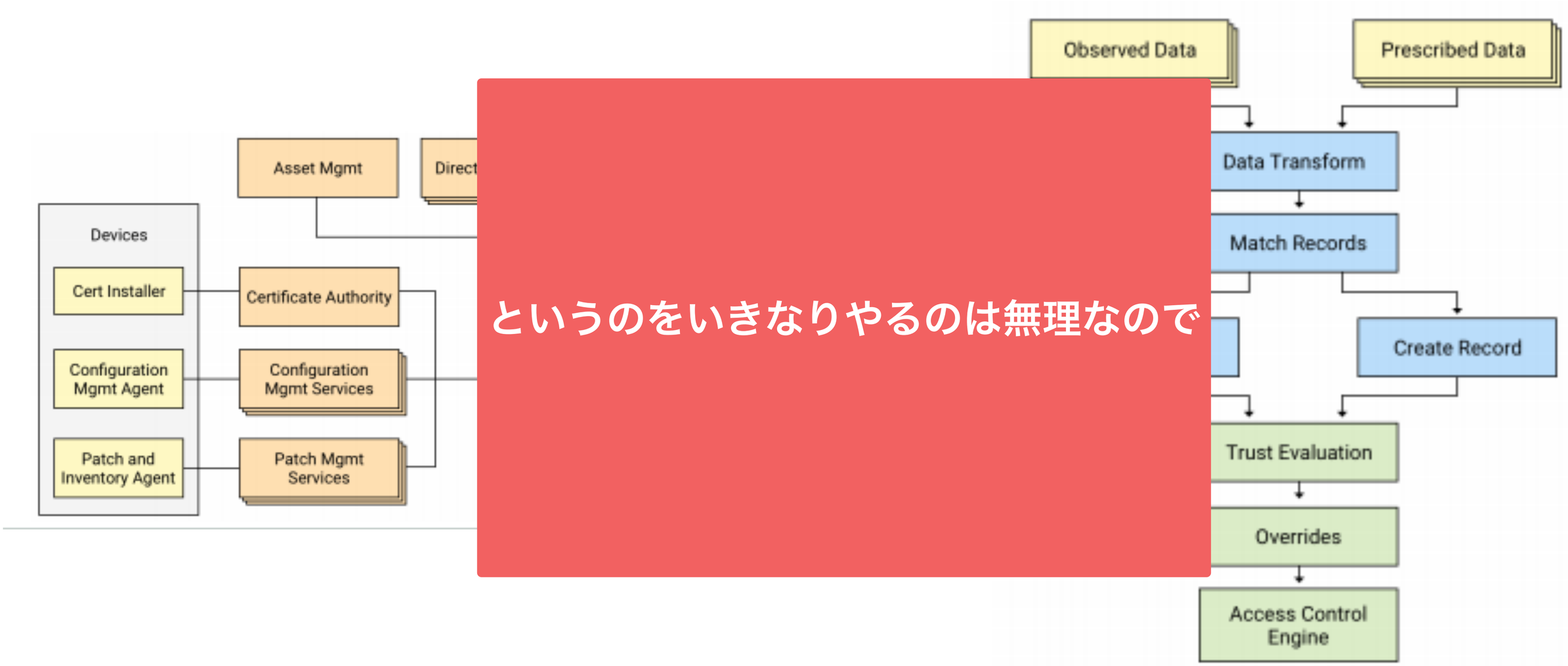
Threats	Control
Unknown Devices	Fleet Inventory and Asset Management
Platform Compromise	OS & Base Software Configuration Management
Security Control Bypass	Security Policy Management & Enforcement
Privilege Escalation	Resilience Against System Takeover & Persistence
Software Compromise	Software Control and Anti-Malware
Attack Persistence	Remotely Verifiable Platform and User
Authentication Bypass	Robust authentication of platform and User
Data Compromise	Data Protection
Attack Concealment	Logging and Log collection for detection capability
Attack Repudiation	Response capability on platform/detection & response

Healthy FleetのTrustブートストラップ





Healthy FleetのTrustブートストラップ



というのをいきなりやるのは無理なので

Healthy FleetのTrustブートストラップ

- トラスト状態のレベル訳
  - Untrusted, Identified, Trusted
- デバイスの数に応じてスケールさせる
  - インベントリシステムとアクセス制御への組み込み
  - デバイスの状態と周辺情報の収集
  - パッチや構成管理
  - 継続的なデバイス評価
  - HealthyでないDeviceの検知
- 柔軟なポリシー運用
- 予防によるシグナル化

現実世界の運用

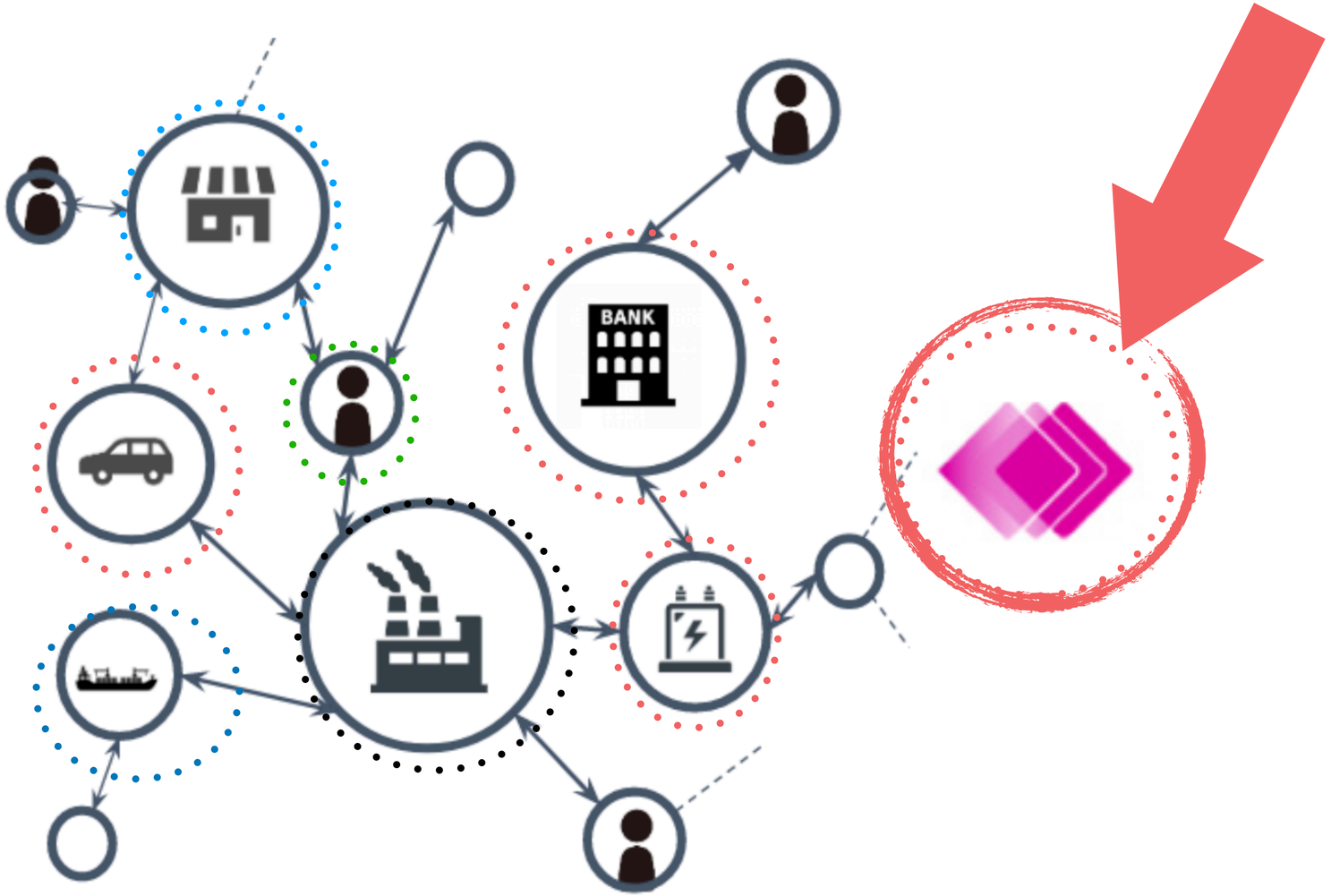
- Platformは信頼できるのか？
  - Intel T2チップのMacだとApple Storeの店員はFirmware Passwordをバイパスして修理できる
- 計測したログ配送を含めた外部サービス利用時のクレデンシャル管理
  - 71389　??　S　　0:00.00 sh -c PATH=$PATH:/usr/local/jamf/bin; '/Library/Application Support/JAMF/tmp/{POLICY}' '/' '{DEVICE}' '{USER}' '{ARG}' " " " " " " " " >& '/Library/Application Support/JAMF/tmp/71324.tmp’
- 開発者が開発時に使いたいroot権限と、管理者が管理のために使いたいroot権限が密結合
- 優先順位としてのDevice Fleet

現実世界の運用

- Platformは信頼できるのか？
  - Intel T2チップのMacだとApple Storeの店員はFirmware Passwordをバイパスして修理できる
- 計測したログ配送を含めた外部サービス利用時のク
  - 71389 ?? S 0:00.00 sh -c PATH=$PAT Application Support/JAMF/tmp/{POLICY}' " " >& '/Library/Application Support/JAMF
- 開発者が開発時に使いたいroot権限と、管理者が管
- 優先順位としてのDevice Fleet

クライアントサイドのTEEに期待？

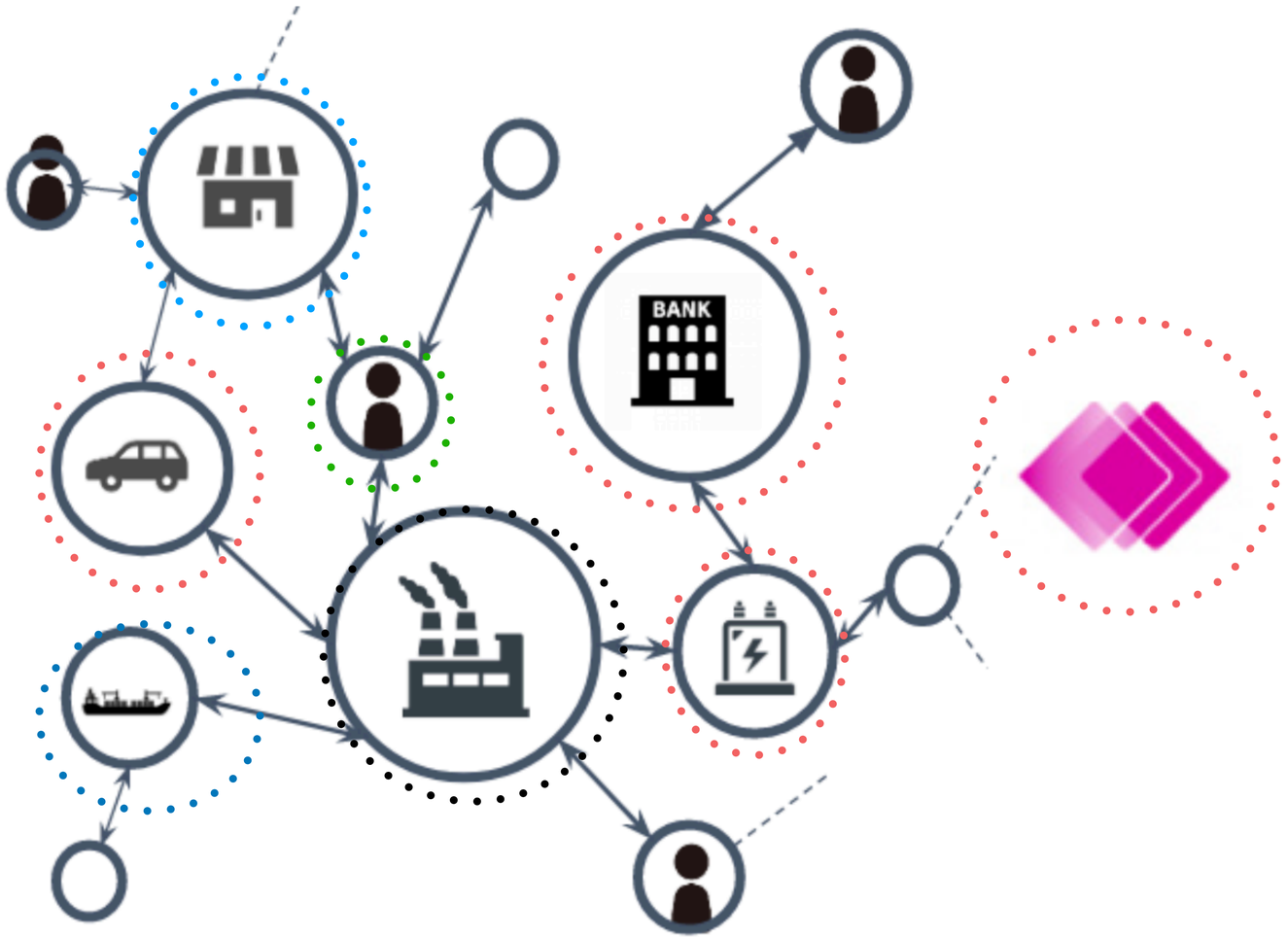
Zero Trustがカバーしている範囲



エンドユーザーにとってはーつのサービス

系全体でのTrustをする時代へ

エンドユーザー



Thank you!