

SIP 信用でつなぐネットワーク

2021.6.17

富士通株式会社

プリンシパル アーキテクト 天満 尚二

※本研究の一部は、内閣府が進める戦略的イノベーション創造プログラム（SIP）「IoT社会に対応したサイバー・フィジカル・セキュリティ」（管理法人：NEDO）によって実施されています。

研究開発の背景・目的

サプライヤーとの契約プロセスの現状

- 部品のサプライヤーとの契約に際しては、企業の経営状況、製造実行能力(製造能力、技術力、品質など)をドキュメントや面談、現地視察などを交え、企業の信用度を検証
- 契約後も面談などによる定期監査等を行い、継続的に信用度の検証により関係を強化

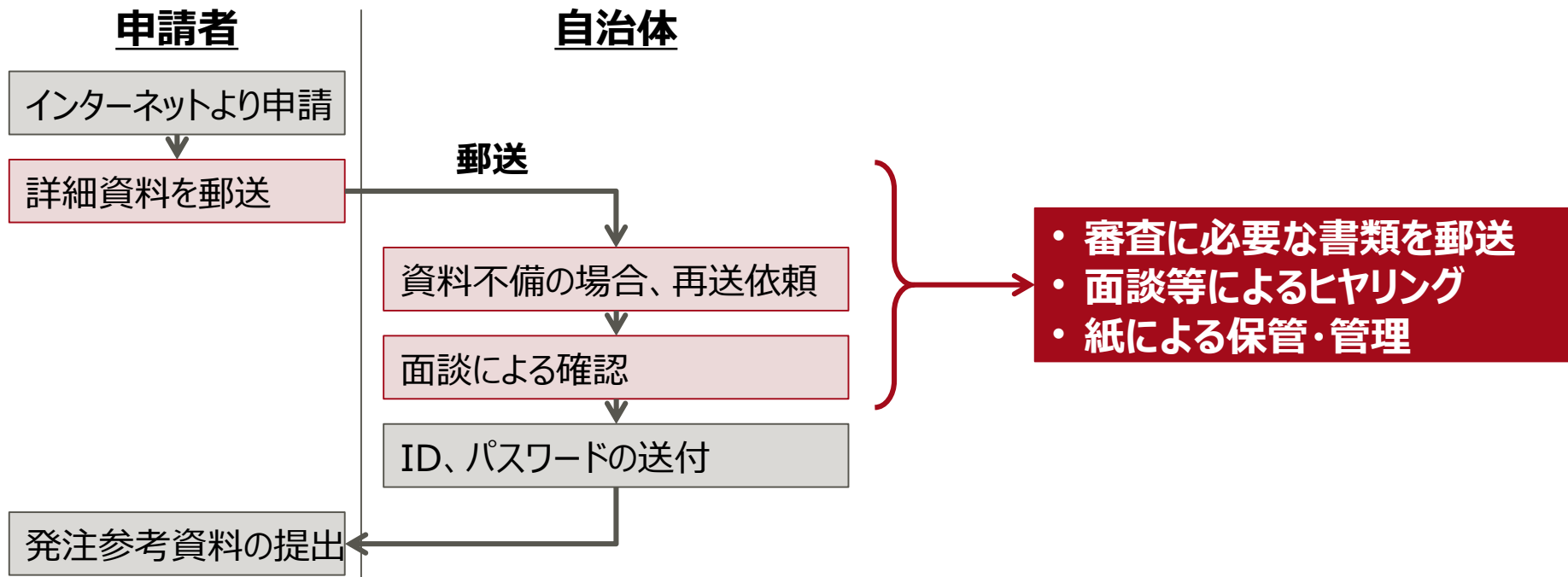


サプライヤーとの契約に際しては、契約前に、段階的にサプライヤーの信用度を検証し、信用関係を構築

契約後も、定期監査等により、契約の実行状況を監視し、信用関係を強化

自治体業務 (入札資格申請)の現状

- 審査請求や発注参考資料の提出は、インターネットで可能であるが、審査(能力、技術力、品質など)に必要な資料提出は郵送、その後、面談等によるヒヤリングなどにより、企業の信用度を検証、審査を実施



■ 製造業:

- ・ 契約前に、面談・会議などによる契約先の信用度を確認し、十分な信用度を持つ相手と契約
- ・ 契約後も、実施状況を面談、会議により定期監査を行い、信用度を継続して検証

■ 自治体:

- ・ 申請作業などのデジタル化は進むものの、実業務は依然としてアナログ
- ・ 提出資料の電子化等、自治体業務の負担が増加

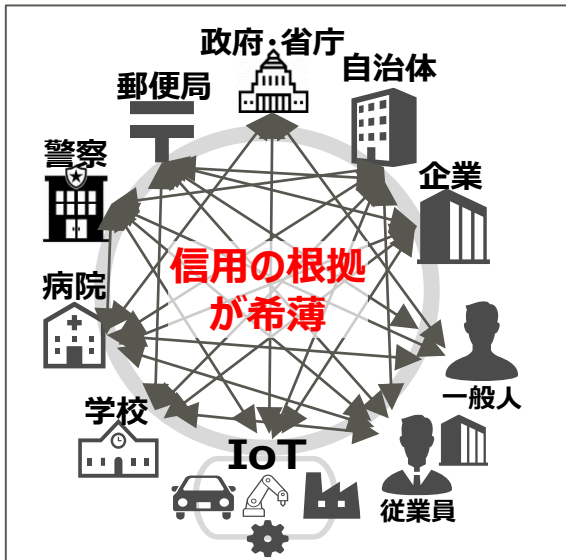


上記課題は、リアルの世界で行っている契約先等の検証が
サイバー空間で実現できていないことが原因

サイバー空間において相互に信用を検証・確認した上で
組織内、組織間でデータを安心して流通する「信用できる場」が必要

目標：研究開発が目指す社会像

■ 「信用できる場」：つながる相手/データを保証する新たな社会基盤



■ 信用できる場の要件

- (1) システム間が安全につながる仕組み
 - ・ 情報を民主的に共有
 - ・ 対等・公平な協議・合意形成
 - ・ システム全体のセキュリティ対策自動化
- (2) データの真正性保証
 - ・ eSignature
 - ・ eSeal
 - ・ eTimestamp、等
- (3) 人・組織の真正性の確保
 - ・ Proofing(法人の個人、本人確認)
 - ・ Authentication(認証)
 - ・ 認証連携、等

【現在】

- ✓ 送られてきたメールやデータは正しいのか？
- ✓ 相手は信頼できる人か？

【今後】

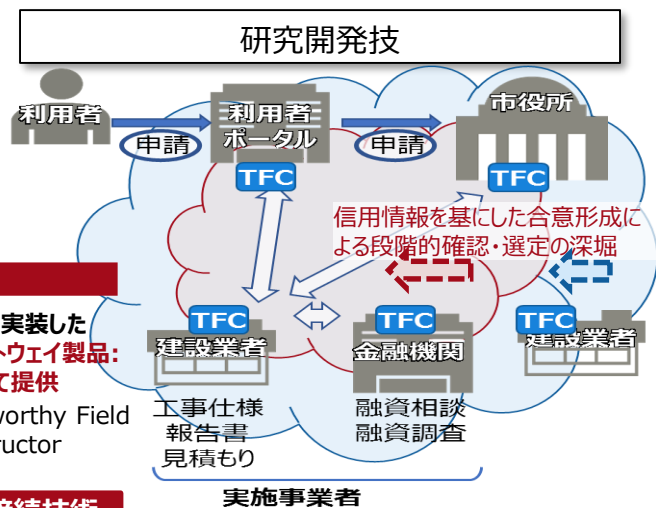
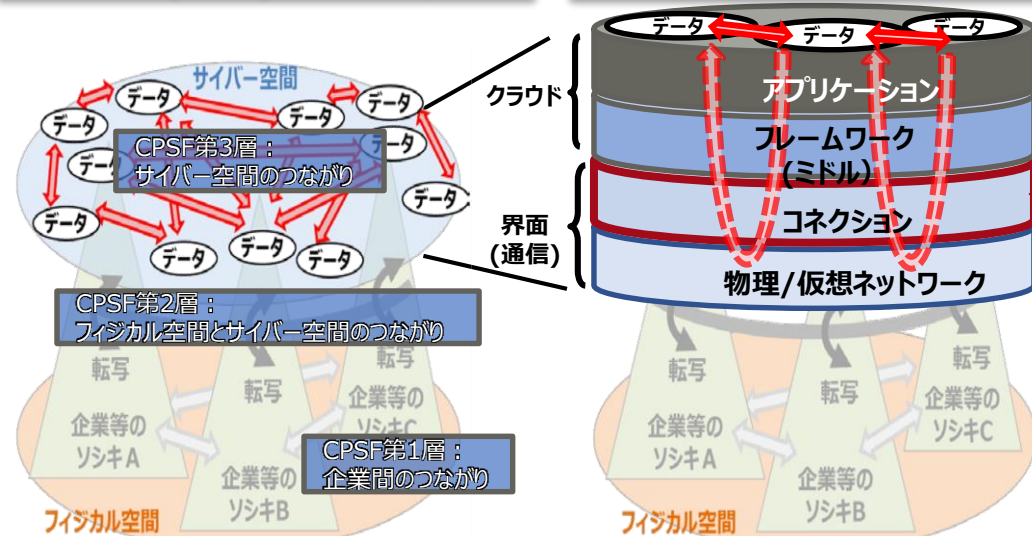
安全、かつシンプルな繋がり
(人/組織/クラウド間等)を実現

目標：研究開発が目指す適用領域

■ 不特定多数の組織からビジネスなどで協働するパートナーを精選し接続する「**精選接続技術**」を開発し、経済産業省サイバーセキュリティ対策フレームワーク第3層におけるコネクション制御レイヤーに適用

サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)における三層モデル

本研究開発により、コネクション層における安心・安全を確保



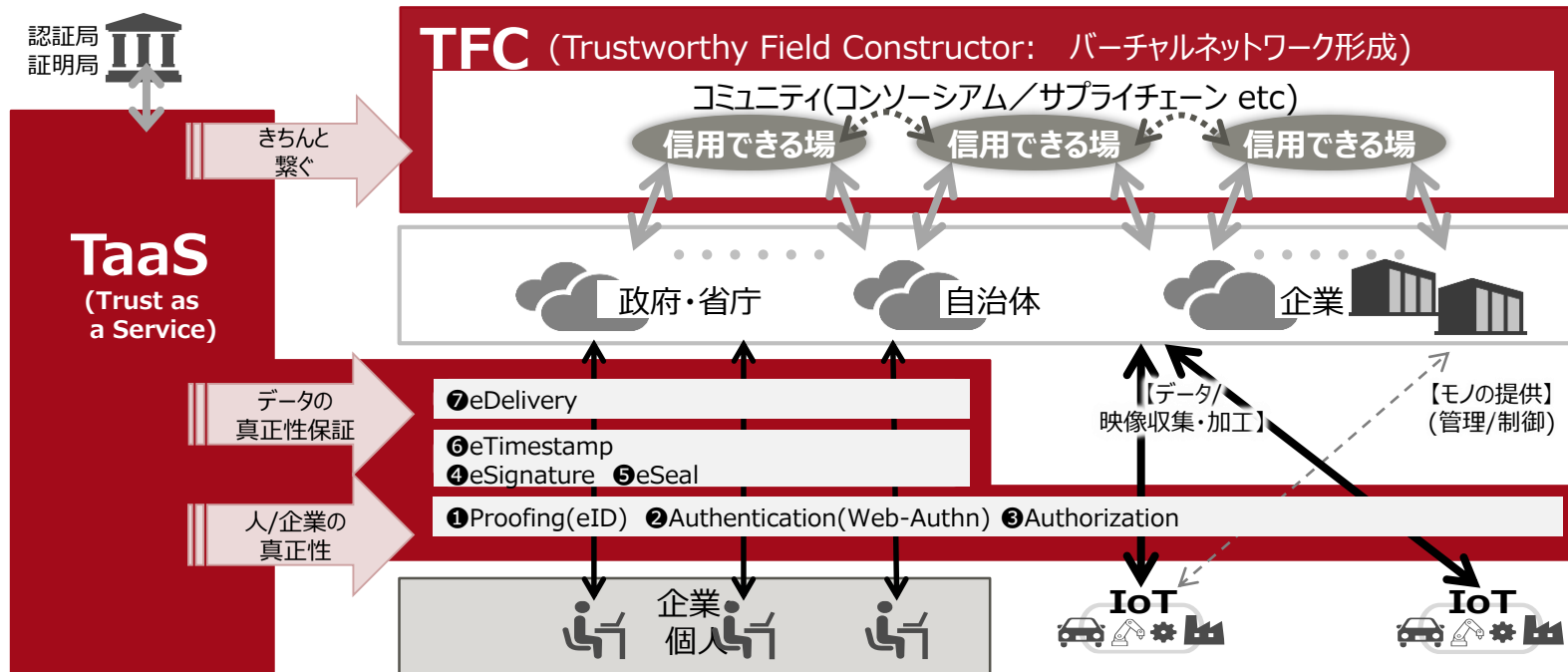
精選接続技術を実装したソフトウェアゲートウェイ製品: TFC(仮称)として提供
※TFC: Trustworthy Field Constructor

精選接続技術
サイバー空間において、組織間で相互提供した信用情報(※)を基にした組織間の合意形成による接続組織の信用性確認・選定を段階的に繰り返し、接続相手を決定し、接続

目標：研究開発の位置づけ

■ クラウドシステム(PaaS)等のネットワーク機能層と位置づけ

- クラウド内・外の目的を同じくする企業、行政システム等を接続する「信用できる場」を構成
- 企業情報や関連する属性情報を相互に共有し、参加者の合意形成により安全なネットワークを構築



※TaaS: データや接続先の真正性を検証・保証するサービス

研究開発技術詳細

信頼チェーンに関わる情報の安全な流通技術の研究開発 FUJITSU

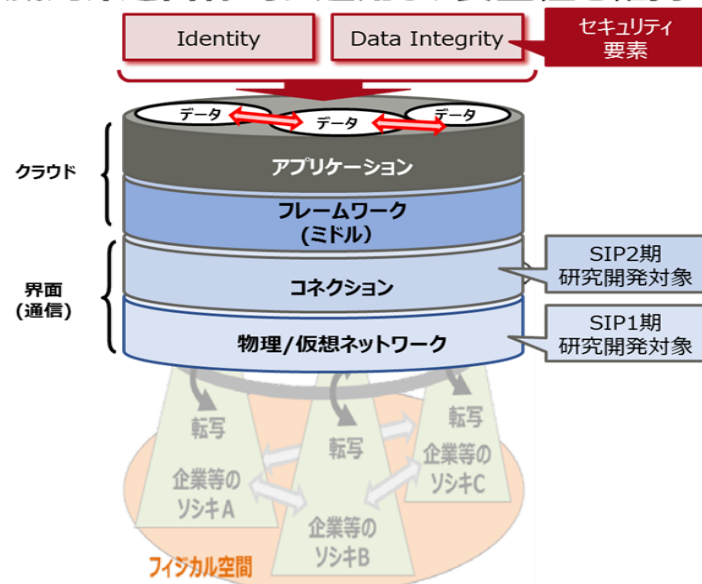
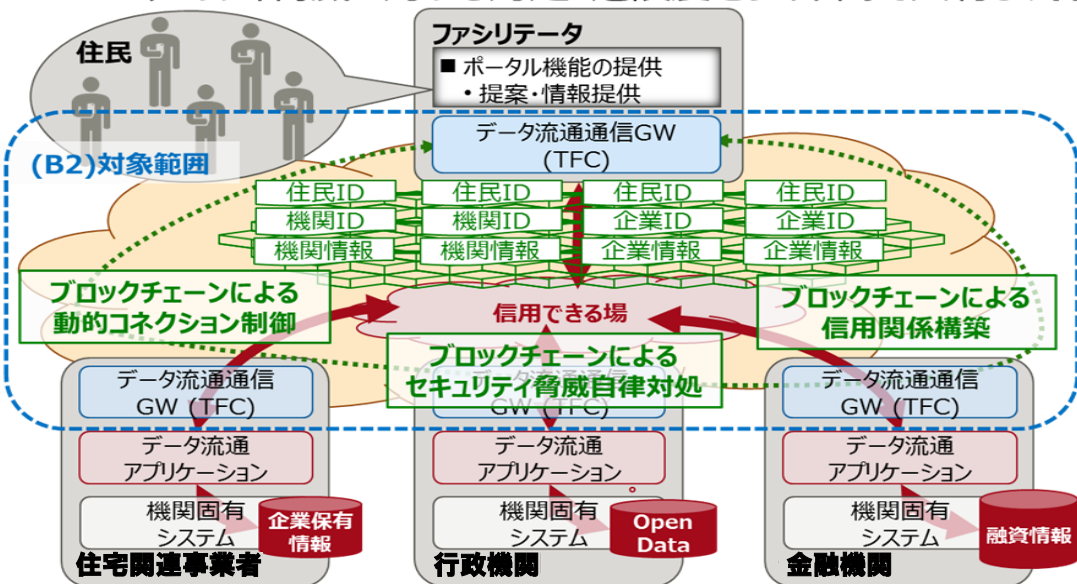
信用できる法人・組織のみが参加し、セキュリティ脅威対策を自律適用するデータ流通環境を提供、
 専門スキルや複雑な操作なしに、法人・組織の安全なデータ流通を実現

① 安心・安全なデータ流通環境の構築

- 信用情報（組織確認情報）を複数の参加組織の合意・承認により、**フィジカル空間とサイバー空間の登録組織・法人の一意性を保証し**、連携すべき組織のみが参加するデータ流通環境を構築

② データ流通環境の安全性の維持

- セキュリティ脅威に対する対処・危険度をサイト間で共有し、**脅威対策を自律的に適用し**、安全性を維持



- 精選接続技術: 属性情報の共有・相互確認により、接続先の一意性を確保する技術
 - 信用形成3層モデル
 - 実世界における信用形成プロセスを3段階(事前審査、認定、取引・監査)に分け、段階毎に共有する属性情報(信用情報)をモデル化
 - 信用形成段階毎に情報流通範囲を統制する情報交換の「場」を構成
 - マルチステークホルダによる合意形成
 - 「場」の参加者全員による「場」のアクションの合意形成方式
 - 「起案」、「審議」、「結審」のプロセス標準化
 - ネットワークセキュリティ脅威に対する自律適用
 - 発生したネットワークセキュリティ インシデントの脅威ランク付けによる見える化、対策の自動適用
 - ネットワークセキュリティ インシデント対策の「場」への自動展開
- 既存技術の活用
 - ブロックチェーン: 属性情報共有における参加者の主権確保、改ざん防止
 - IDルーティング・メッセージ: 企業IDで通信先を確認し、暗号メッセージを送受

① 安心・安全なデータ流通環境の構築

①安心・安全なデータ流通環境の構築【考え方】

① 信用形成段階毎に情報流通範囲を統制する情報交換の「場」を構築

- サイバー空間上に企業のデジタルツインを構成するTFC(Trustworthy Field Constructor)を配備し登録企業IDと契約企業の同一性を確保
- 信用形成段階を3層にモデル化(事前審査、認定、取引・監査)し、各層の目的毎に以下を持つ情報流通のための閉域空間「場」を設け、構築・維持情報(信用情報)の流通を統制することにより、信用情報の漏洩・改竄を防止
 - 各層、各場よりにアクセス制御された分散台帳による信用情報流通(共有範囲制限、改竄防止)
 - 企業IDルーティングによりネットワークアドレスを隠蔽した暗号メッセージ通信(情報漏洩防止)
- マルチステークホルダ・プロセスに基づく合意形成により信用情報を相互確認し、信用情報の完全性、真正性を確保。

さらに、地域性の高い問題、各企業を起点とした問題提起、合議による解決により、中央集権型がカバーできていない適時性を確保

第1層: データ流通機構 [事前審査]

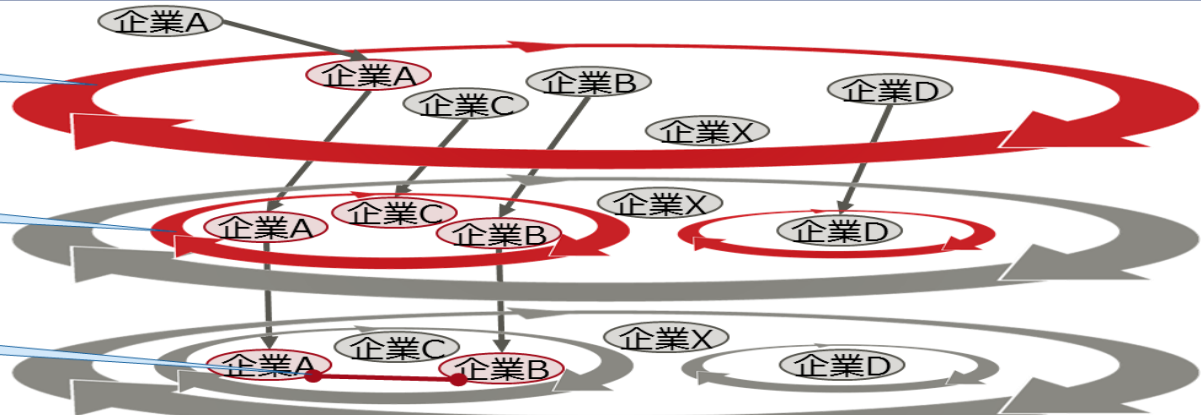
・何らかのサプライチェーンに参加したい企業群

第2層: 信用できる場 [認定]

・特定のビジネス目的を持った企業群
ex. 工作機械製造・販売・保守

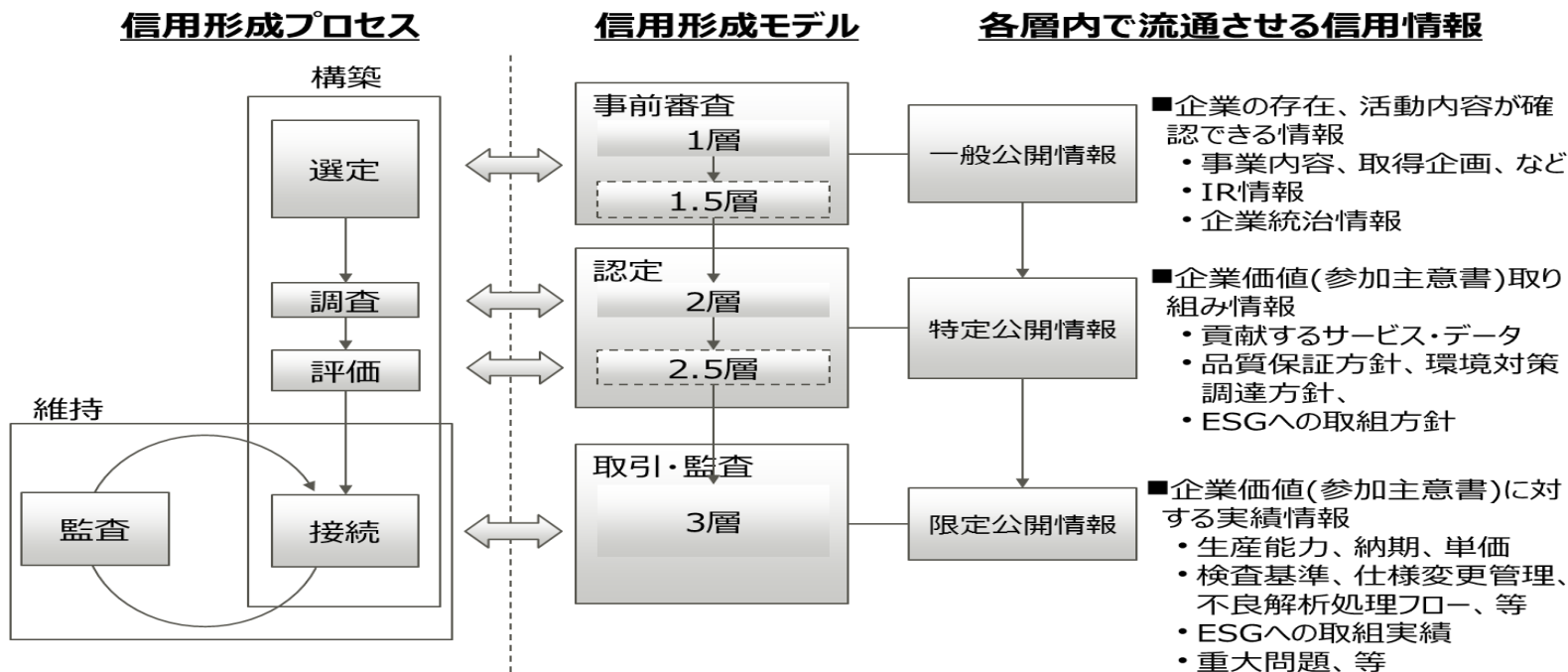
第3層: サプライチェーン [取引・監査]

・具体的なビジネスを目的とした企業群
ex. A社工作機械の製造・販売・保守



①安心・安全なデータ流通環境の構築【信用情報】

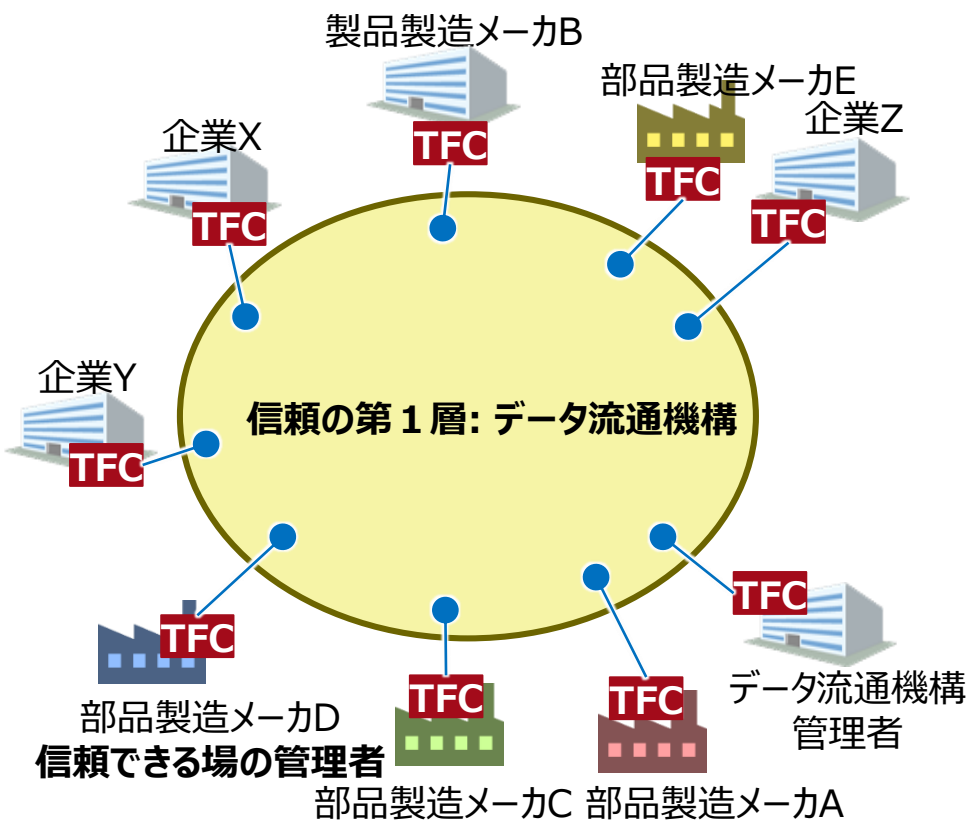
- 信用情報：企業等、信用できる場の参加者を示す企業情報、関連する属性情報の集合
 - 信用形成を3段階のプロセスでモデル化、各段階で共有する属性情報を定義し、信用情報として参加者間の信用形成情報として共有



①安心・安全なデータ流通環境の構築 - 動作概要

① 安心・安全なデータ流通環境の構築

【信用の第1層: データ流通機構への参加(導入)】



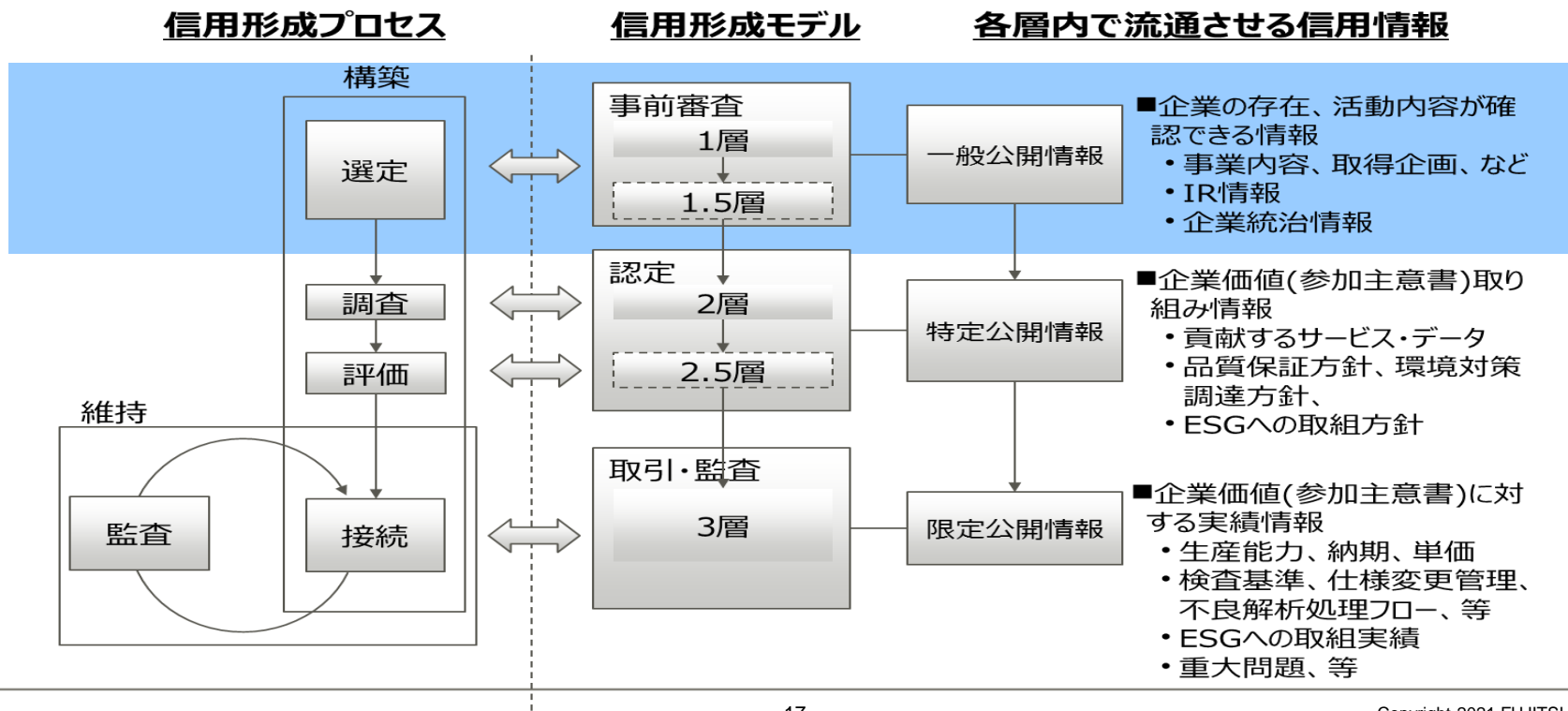
- サービス事業者が、信用の第1層: データ流通機構を開設
 - 新たなビジネス創造、新たなパートナーを求める企業など、データのサプライチェーンの構築を考える企業を勧誘
- ↓
- 利用企業は、TFCの配布を受け、信用の第1層: データ流通機構に参加
 - データ流通機構事業者が参加者の現存を確認
 - 利用契約後、信用情報を設定し、TFCを配布
 - 利用企業が持つインターネット回線にTFCを接続し、第1層に参加

①安心・安全なデータ流通環境の構築

【信用の第1層:データ流通機構の信用情報】

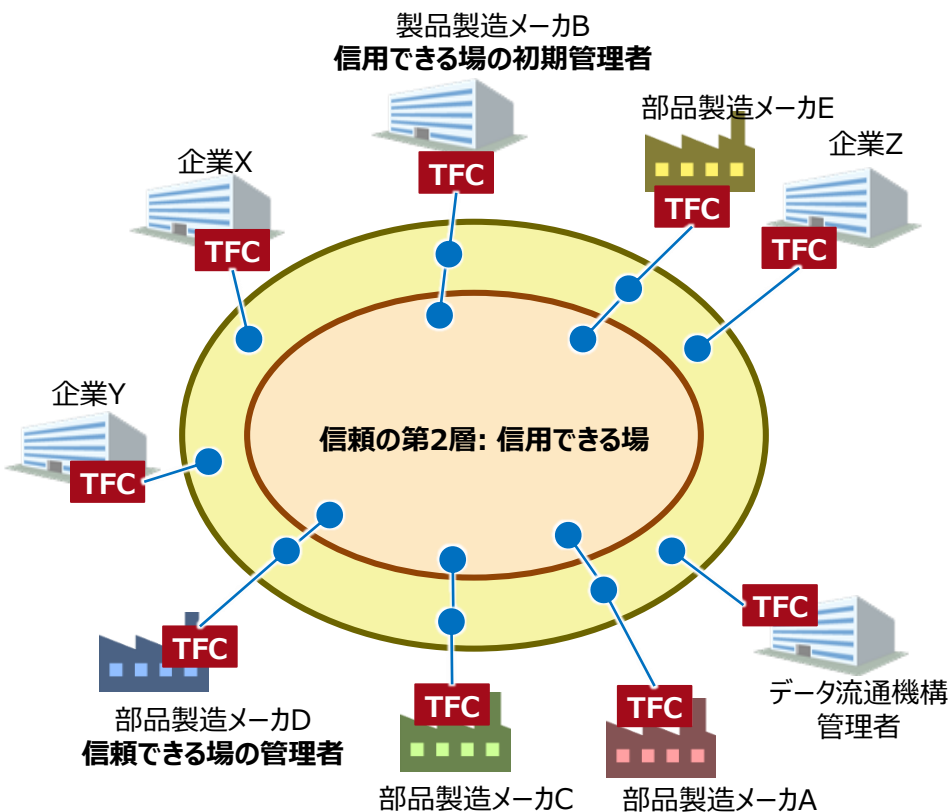
■ 信用の第1層: データ流通機構で共有される信用情報

- 現存確認された企業の事業内容、IR情報、企業統治情報など、企業かを示す属性情報を共有



①安心・安全なデータ流通環境の構築

【信用の第2層：信用できる場の創設】



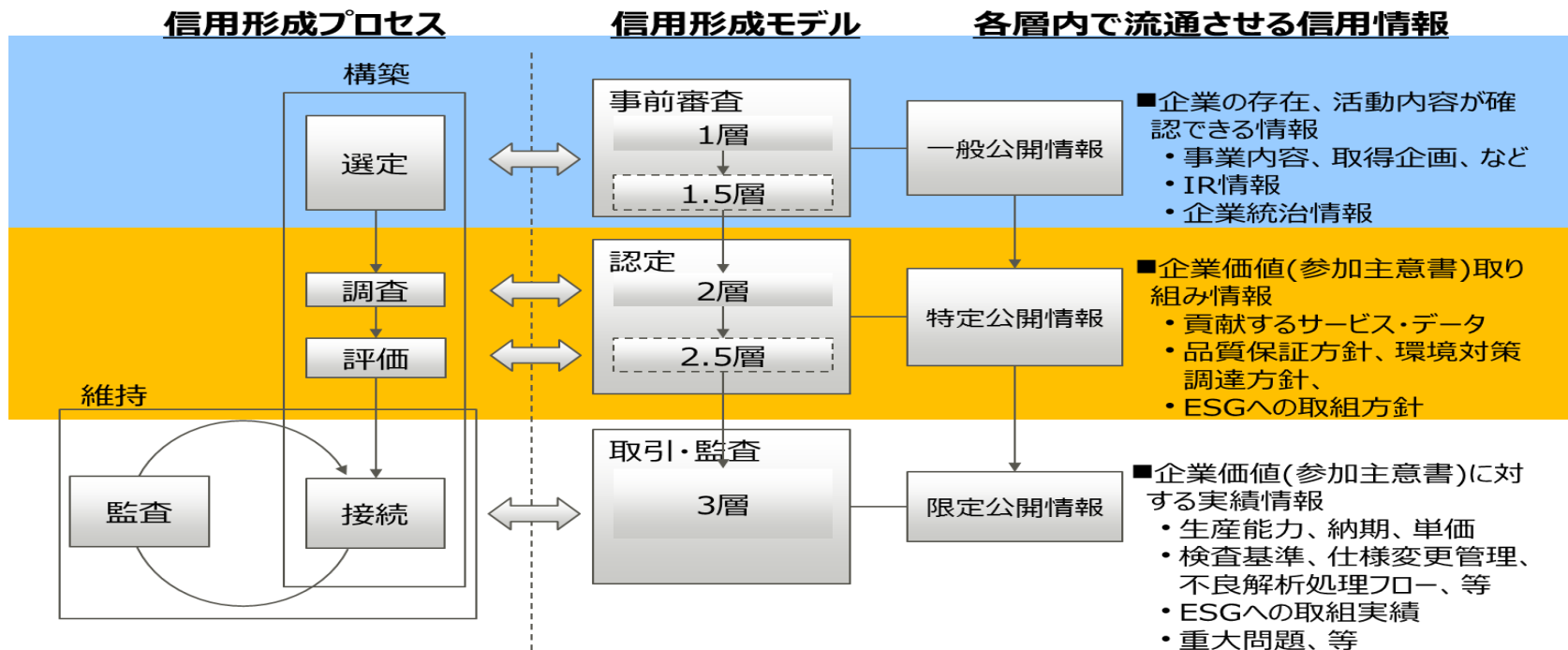
- 新たにビジネスを始めたい企業がパートナーを集めるために、「信用の第2層：信用できる場」を創設
- 参加企業が「信用の第2層：信用できる場」を創設
 - 参加企業がビジネス共創の目的・目標を明示し、「第2層：信用できる場」の創設を起案し、創設審議の参加企業を募集
 - 参加表明企業と「信用の第1層：データ流通機構」で公開されている信用情報をもとに「信用の第2層：信頼できる場」における以下を審議・決定
 - ✓ 場の創設
 - ✓ 場への参加者
 - ✓ 管理者(場のファシリテータ)

① 安心・安全なデータ流通環境の構築

【信用の第2層:信用できる場の信用情報】

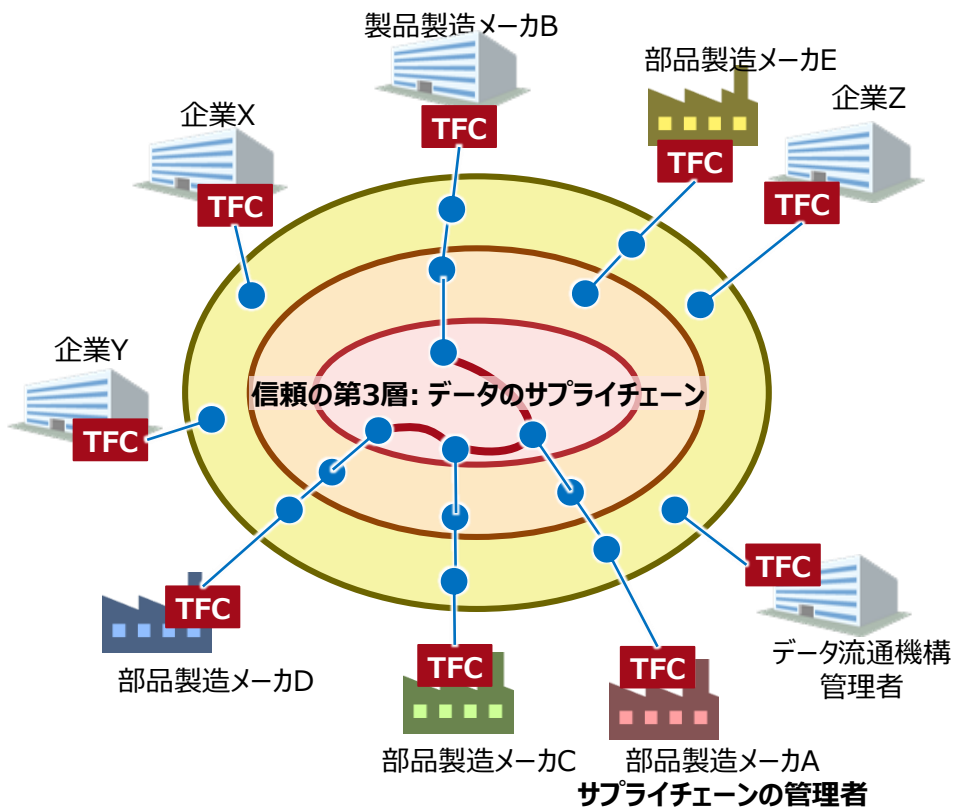
■ 信用の第2層: 信用できる場で共有される信用情報

- 企業が提供するサービス・製品、品質方針、調達方針、環境対策、ESG取り組み方針など、企業価値を示す属性情報を共有



①安心・安全なデータ流通環境の構築

【第3層: データ・サプライチェーン創設】



■ 実ビジネスを行うパートナーを集めるために、「信用の第3層: データ・サプライチェーン」を創設

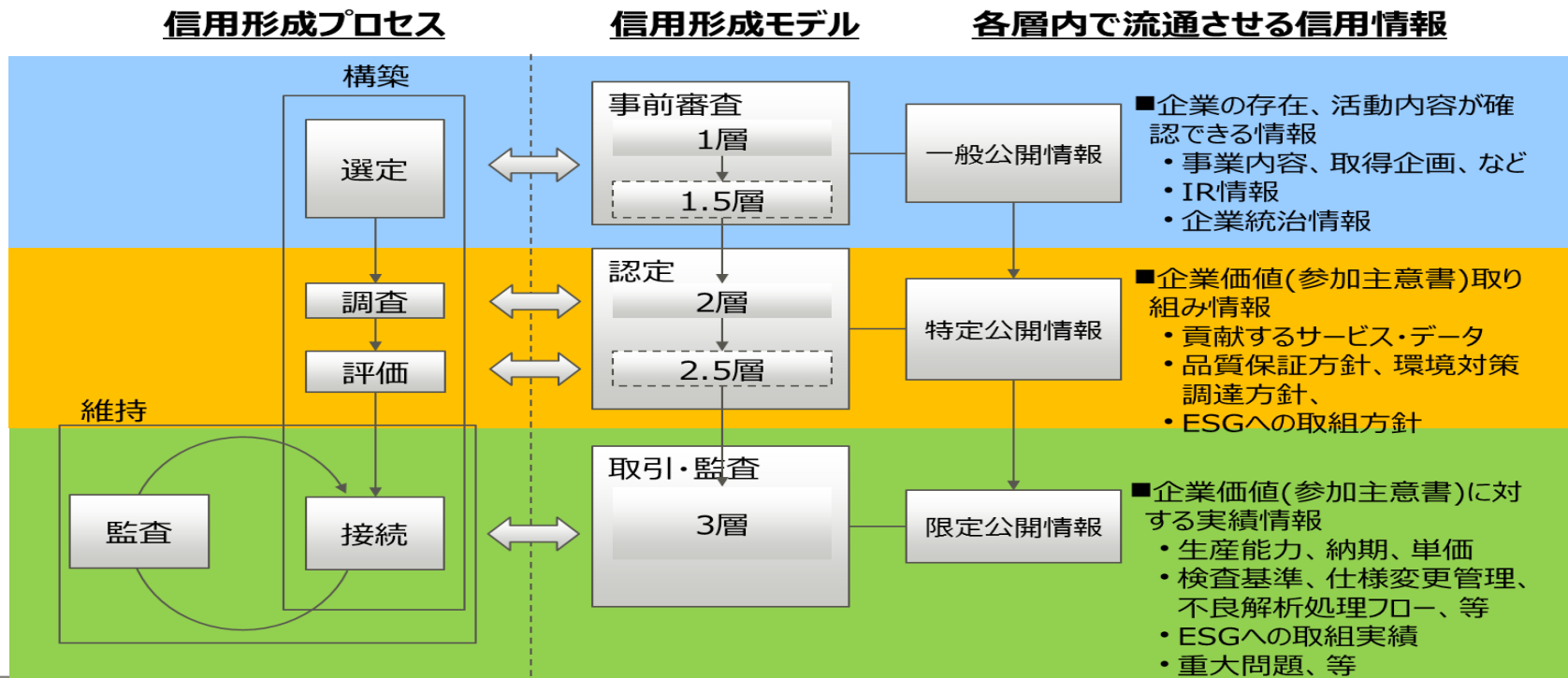
■ 第2層参加企業が「信用の第3層: データ・サプライチェーン」を創設

- 参加企業がビジネス共創の目的・目標を明示し「第3層: データ・サプライチェーン」の創設を起案、創設審議の参加企業を募集
- 参加表明企業と「信用の第1層: データ流通機構」、「信用の第2層: 信用できる場」で公開されている信用情報をもとに「第3層: データ・サプライチェーン」における以下を審議・決定
 - ✓ 創設
 - ✓ 参加者
 - ✓ 管理者(場のファシリテータ)

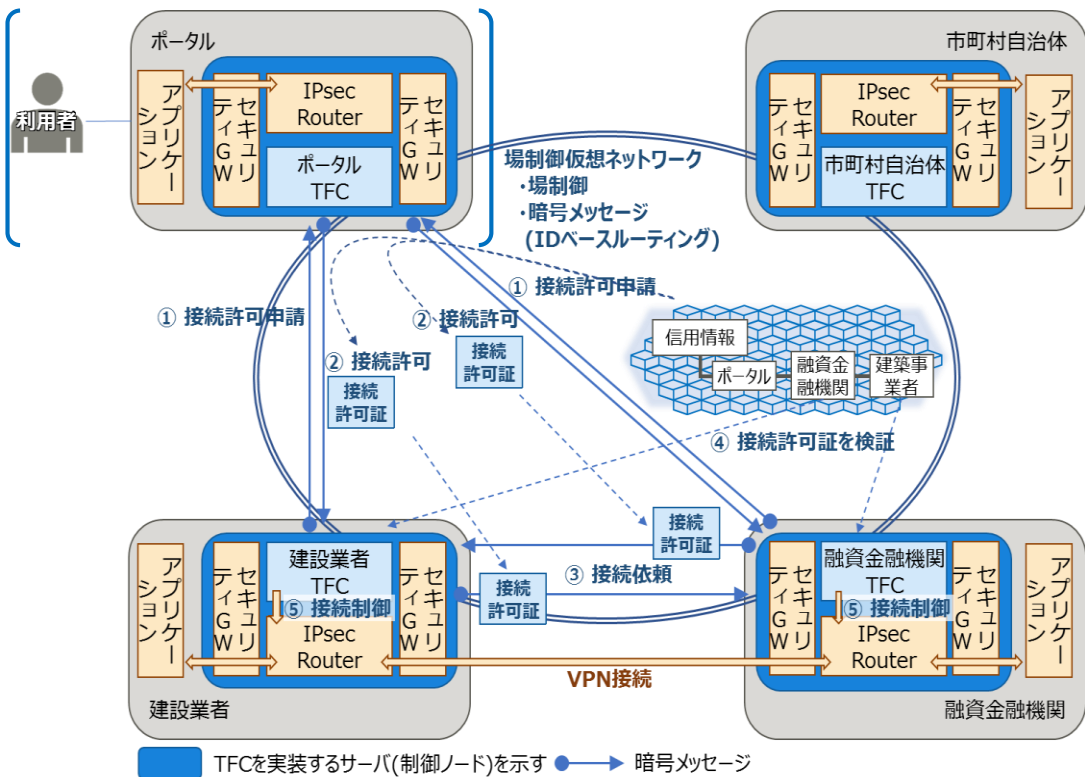
①安心・安全なデータ流通環境の構築

【信用の第3層:データ・サプライチェーンの信用情報】

- 信用の第2層: 信用できる場で共有される信用情報
 - 提供するサービス・製品、品質実績、生産能力、検査基準など、企業実力・実績を示す情報を共有



①安心・安全なデータ流通環境の構築【回線接続】



■ 参加者間のアプリケーション間回線接続

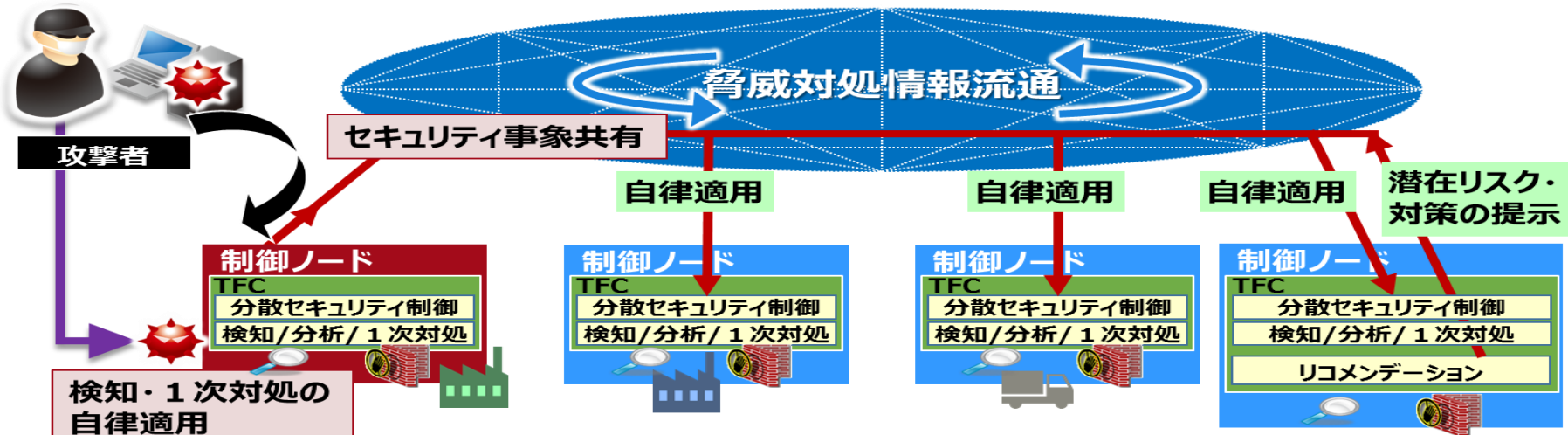
- 信用情報をもとに、信用の第3層: データ・サプライチェーンにけるメッセージ交換先範囲を限定
- 信用の第3層: データ・サプライチェーンにおける信用情報を含む接続先許可証を相互交換し、アプリケーションの接続経路を開設

②データ流通環境の安全性の維持

②データ流通環境の安全性の維持【考え方】

② TFCによる「場」のセキュリティ脅威監視、1次対策のサプライチェーン全体への自律適用

- TFCに同じ外部・内部脅威対策を統一配備し、「場」毎に脅威を監視
- 分散セキュリティ制御技術により脅威対策をサプライチェーン全体に自律適用
 - 脅威発生時の外部・内部脅威対策のログ分析、トラフィック分析から、危険度を算出することにより脅威影響を全TFCの共通指標として可視化
 - 脅威対処情報流通を介して全TFCに対処・危険度を共有・展開。危険度に合わせて各TFCで事前設定された脅威対策(設定変更など)を**自律適用**し、影響を極小化
- 脅威対処情報流通で共有される情報を元に、発生頻度、発生から対処までの時間、未解決件数などの解析から、信用できる場に対する潜在的リスク・対策などを提言 (リコメンデーション)

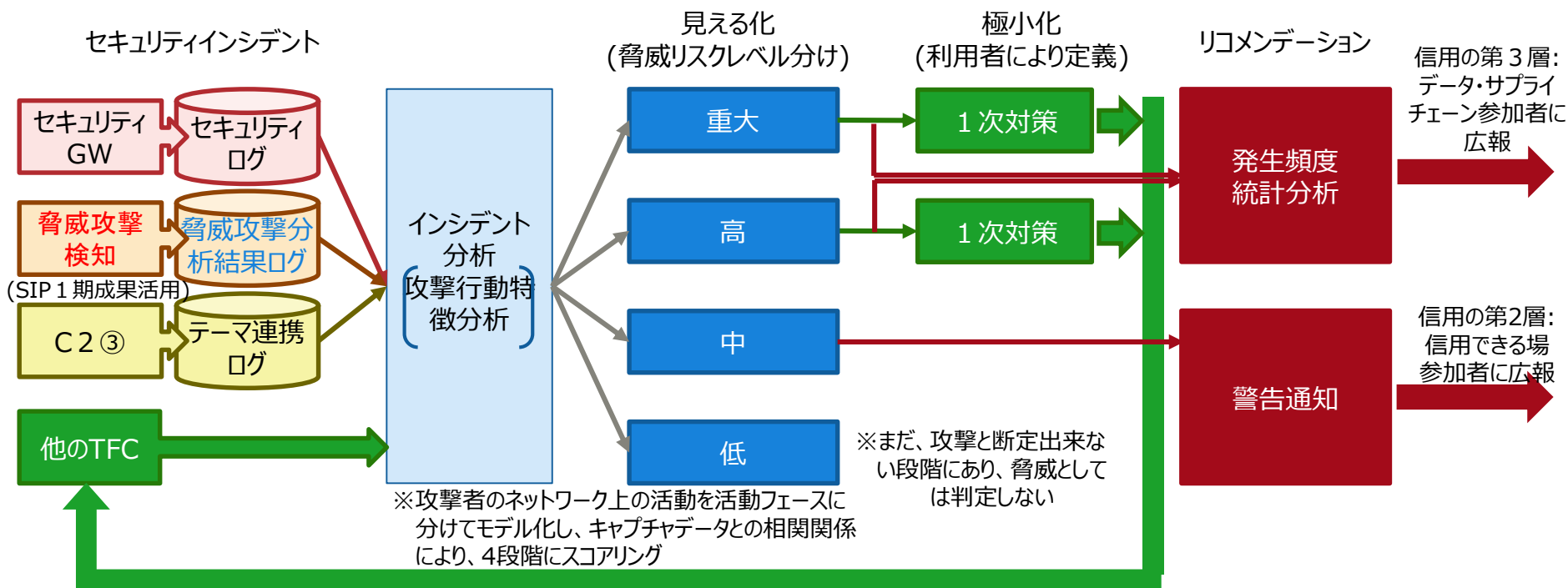


※制御ノード：TFC、その他関連モジュール(セキュリティGW、ルーターなど)を搭載したサーバ

②データ流通環境の安全性の維持

【見える化・極小化、リコメンデーション】

■ セキュリティ脅威分析から1次対策の実施、関係者へのリコメンデーションまでの一連の処置を自律的に実行

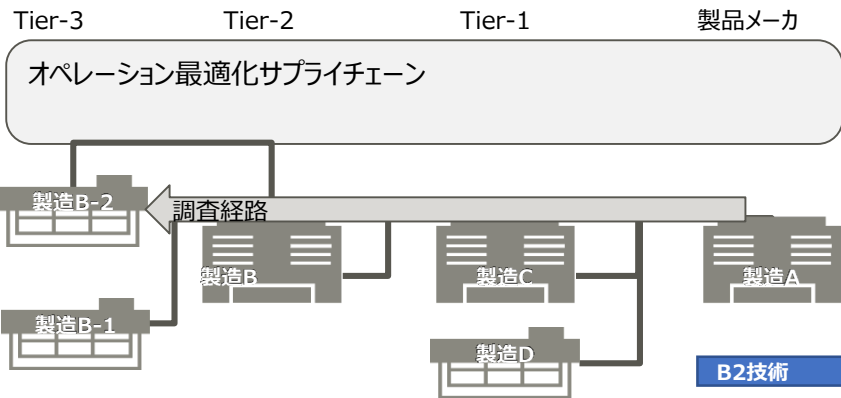


適用例・効果

応用例：製造サプライチェーンへの適用

■ サプライチェーンの運営・管理への活用例

- Tier-1～Tier-3まで信用できる場に收容。
- Tier-3企業が重大問題の発生を信用できる場に展開、関係者の合議により対策を立案
⇒ 従来、約1か月以上かかった問題発生から検知・調査期間を数日に

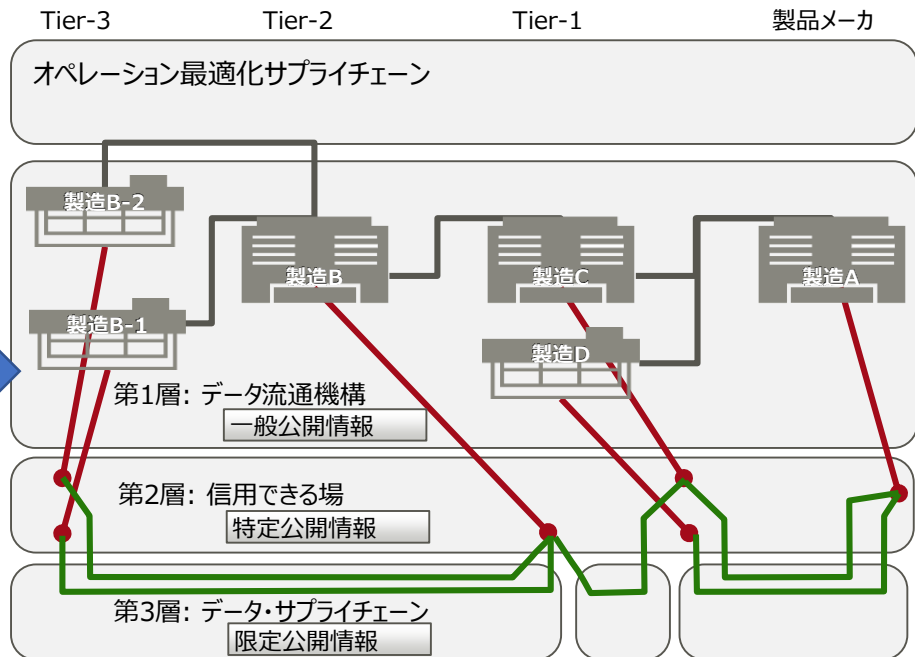


現状のサプライチェーンでは、通常、製品メーカーはTier-1しか把握できておらず、電話等による中間企業を経由した調査に1か月以上かかっている

- ・検知契機: Tier-1の納期遅延
- ・調査経路: Tier-1 ⇒ Tier-1 ⇒ Tier-1/Tier-2
 經由 Tier-2 經由 Tier-3

・調査期間: 約1か月以上

※3.11時の当社実績、コロナ禍における某社ヒヤリング



応用例：自治体への適用(1)

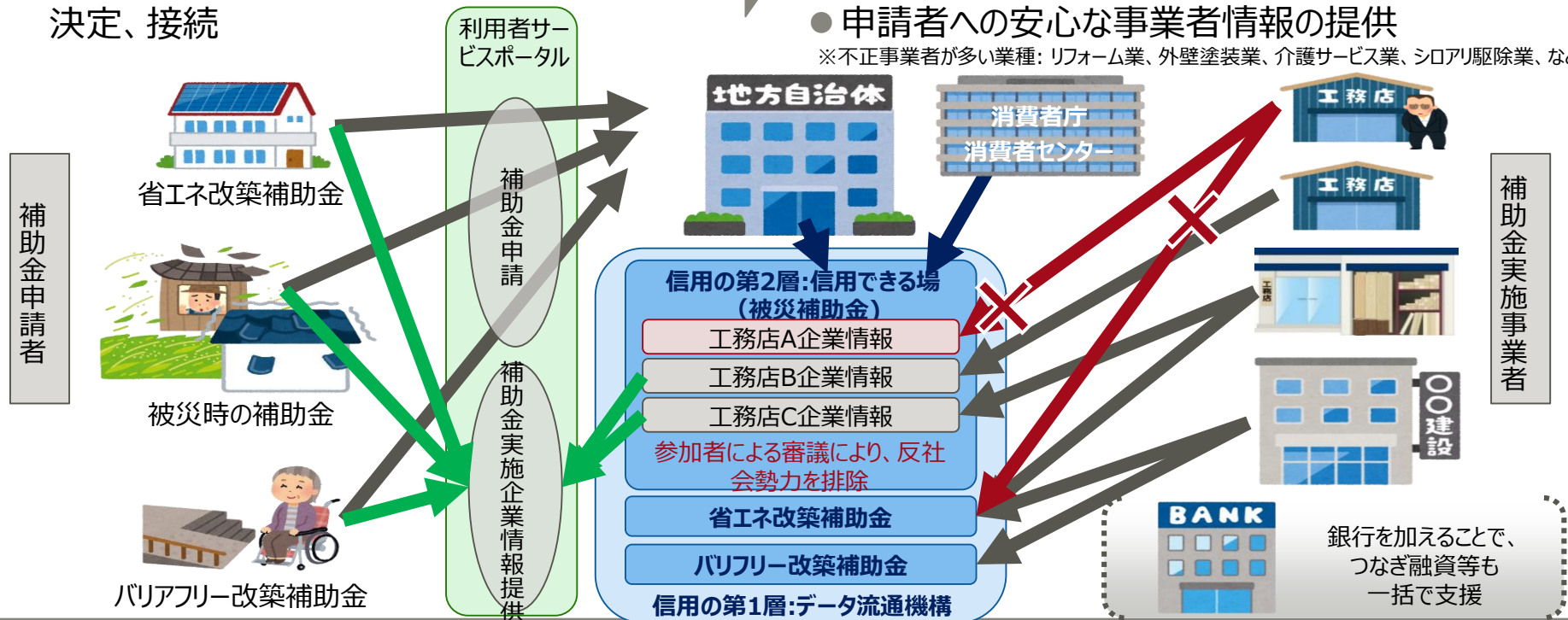
■精選接続技術の適用

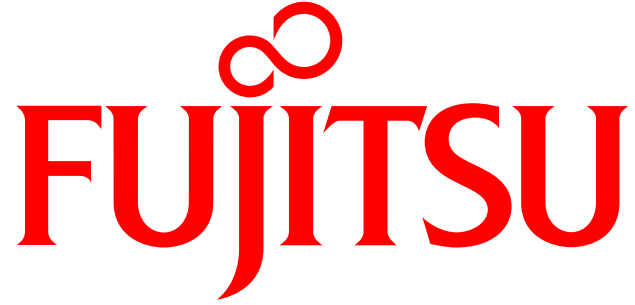
- 審査に必要な情報を信用情報として共有参加可否を参加法人＋自治体にて審議し、参加を決定、接続

■効果

- 参加者による反社会勢力、不適正事業者の排除
- 参加者による実施者の適正審査の常態化
- 申請者への安心な事業者情報の提供

※不正事業者が多い業種：リフォーム業、外壁塗装業、介護サービス業、シロアリ駆除業、など





shaping tomorrow with you