

Trusted Web ホワイトペーパー

Ver2.0

付録

2022 年 7 月 25 日

Trusted Web 推進協議会

目次

付録 A. TRUSTED WEB ユースケース	1
(1) ユースケースのタイトル	1
(2) 背景	1
(3) 現状とその問題点	1
① 本ユースケースに登場するステークホルダー	1
② 実際のやりとりのイメージ例	2
③ やり取りされる情報	2
④ 本ユースケースにおける特異な点	2
⑤ ステークホルダー毎のペインポイント	2
⑥ ペインポイントの整理	3
(4) Trusted Web 技術の適用	4
① 効果を期待できるポイント	4
② 適用方針	4
③ 関与するデータ	5
④ エンティティ間のやりとり	5
⑤ 証明書とトラストヒエラルキ	6
⑥ VC/証明書の発行者とトラストヒエラルキ	6
(5) 議論	7
① 検討外とした事項	7
② Trusted Web モデル適用の有効性	7
③ 脅威モデルと分析	7
④ セキュリティ視点での考察	7
⑤ プライバシー視点での考察	7
⑥ 他分野への応用可能性	7
⑦ その他の議論	7
(6) 関連文書等	エラー! ブックマークが定義されていません。
(7) 付録: 用語	7
(8) 付録: VC のサンプル	8
① 本人確認 VC	8
② 在籍確認 VC	9
③ リファレンス VC	10
付録 B. TRUSTED WEB ユースケース 2	12
(1) タイトル	12
(2) 背景	12
(3) 記法についての留意点	12
(4) 議論するペインポイント	13
(5) 効果を期待できるポイント	13

(6) 本ユースケースにおける特異な点	13
(7) 本文書における「確認」の定義	13
(8) 現状	15
① エンティティ	15
② 関与する情報	15
③ 事業再構築補助金申請における情報の流れ	18
④ 事業再構築補助金申請の手順	18
⑤ 今回の議論から除外した事項・今後議論が必要な事項	19
(9) 現状の問題点	21
① 申請者が作成する書類の内容の正しさに関する問題	21
② 他の組織によって作成された書類の正しさに関する問題	21
③ 提出された書類一揃い全体に対する正しさに関する問題	21
④ 申請者が作成する書類の形式についての問題	21
(10) Trusted Web 技術の適用	22
① 方針	22
② 適用する技術	22
③ 追加されるエンティティと情報	23
④ エンティティ	23
⑤ 関与する情報	23
⑥ デジタル署名をするエンティティ	24
⑦ 情報の流れ	25
⑧ Trusted Web を適用した場合の手順	26
⑨ トラストフレームワークとトラストヒエラルキ	27
(11) 関連文書等	エラー! ブックマークが定義されていません。
(12) 付録 A. Verifiable Credentials の例	28
① 法人 Wallet 内にストアされる G ビズ ID 依拠の VC 例 (G ビズ ID の鍵で署名した JWS を想定)	28
② G ビズ ID が発行する法人に関する検証済みクレーム例	29
③ 税理士の署名がされた Verifiable Presentation	31
(13) 今回用いなかったテキスト	32
① 交付申請に纏わる部分の議論	32
付録 C. TRUSTED WEB ユースケース 3	33
(1) 背景	33
(2) 現状と想定されるシナリオ	33
① エンティティ	33
② 管理対象化学物質を含む製品例	34
③ シナリオ	35
(3) 現状の課題と議論するペインポイント	37

① 営業秘密の保持	37
② 開示範囲の制御	38
③ 既存規制・新規制への対応	38
④ 製造現場の 4M 変更への追従	38
⑤ 企業・データの ID 管理	39
⑥ データの信頼性の担保	39
⑦ 中小企業のフォロー	40
⑧ 規制当局への報告	40
⑨ プロセスで使用される化学物質の管理	40
⑩ 化学反応により伝達されたものから変化する化学物質の管理	40
⑪ 販売後の問い合わせ対応	41
⑫ 製造販売終了後の対応	41
(4) 効果を期待できるポイント	41
(5) 本ユースケースにおける特異な点	42
(6) 要求事項	42
① データ加工・開示・流通・通信に対する要求	42
② 規制・工程変更等に対する要求	43
③ データ管理・検証への要求	44
④ アーキテクチャ・プラットフォームへの要求	44
(7) Trusted Web 技術の適用	44
① 方針	44
② Identifier の目的	44
③ Trustable Communication が求められるシーン	46
④ Dynamic Consent が活かせるシーン	46
⑤ Trace 機能が必要とされるシーン	46
⑥ Trusted Web 技術の適用における検討事項	47
⑦ Trusted Web 機能との関係	47
(8) 議論	48
(9) まとめ	49
(10) 関連文書等	エラー! ブックマークが定義されていません。
付録 D. シーケンス図	51
(1 / 4)	51
(2 / 4)	52
(3 / 4)	53
(4 / 4)	54

個人

(1) ユースケースのタイトル

個人の就業等における属性情報の管理・証明

(2) 背景

昨今のデジタル化の進展や COVID-19 の影響により、企業の採用プロセスのデジタル化が急速に進展している。こうした中で、就職・転職活動を行う個人にとっては、自らの機微な属性情報の取扱いに対する懸念やリスクが高まっている。

一方、人口減少や人材需給逼迫の下、採用難が広がる中、採用企業にとっては、採用時のミスマッチを回避すべく、信頼できる情報を得るニーズが高まっている。このような中、人材を採用する際に、採用企業は応募者本人が作成する履歴書や職務経歴書の内容の確認に加え、応募者の現職または前職の同僚や上司に対し、応募者本人の実績や勤務状況に偽りがないうかの確認を行うリファレンスチェックを実施するケースも増えてきている。しかしながら、採用企業からすると、応募者本人やリファレンス提供者について、本人確認や、現職・前職企業の在籍確認などを行うにはハードルが高く、確認手法の信頼性の担保には課題がある。また、応募者やリファレンス提供者の機微な属性情報については、採用企業にとっても、その取扱いに対する信頼性を高め、これら関係者が安心して自らの情報を提供できる環境を整えることが求められている。

本ユースケースでは、応募者、リファレンス提供者、採用企業が「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」に足りる情報のやりとりの可能性を検討する。

検討と平行して、検討結果の一部を具現化したプロトタイプを開発した。なお、プロトタイプで実装したのは検討結果の一部であるため、たとえば、全てのペインポイントを解決した形にはなっていない。プロトタイプ実装についての議論は後半のセクションを参照のこと。

(3) 現状とその問題点

① 本ユースケースに登場するステークホルダー

ステークホルダーとして登場するのは、大きく分けて、人と組織である

1. 人
 - a) 応募者
 - b) リファレンス提供者
 - c) 転職先企業の担当者
2. 組織
 - a) 転職先企業
 - b) 応募者の所属企業、あるいは、かつての所属企業

注：本ユースケースにおいては、上記に挙げた人と組織の間での情報のやりとりを検討するが、現実的な現場においては、人材仲介業者などが応募者や転職先企業との橋渡しをしたりマッチングをしたりする業者が介在する可能性がある。

② 実際のやりとりのイメージ例

以下にやり取りのイメージ例を示す。

1. 転職先企業が、応募サイトを公開する。
2. 応募者が転職先企業に応募に必要な情報を登録する。
3. 転職先企業が応募者に対してリファレンスを要求する。
4. 応募者はリファレンス提供者にリファレンス提供のための情報を提供する。
5. リファレンス提供者はリファレンス提供する。
6. リファレンス提供者はリファレンス提供したことを応募者に伝える。

③ やり取りされる情報

1. 応募者本人の応募（本人確認）情報
 - a) 転職先企業に開示
2. 応募者本人がどこに転職しようとしているかの企業の情報
 - a) リファレンス提供者に本人が開示
3. 応募者本人の在籍証明情報
 - a) 転職先企業に開示
4. リファレンス提供者の本人確認情報
 - a) 転職先企業に開示（応募者本人は参照できない）
5. リファレンス提供者の在籍証明情報
 - a) 転職先企業に開示（応募者本人は参照できない）
6. リファレンス情報
 - a) 転職先企業に開示（応募者本人は参照できない）

④ 本ユースケースにおける特異な点

応募者とリファレンス提供者のプライバシーを保ちつつ、企業への十分かつ検証可能な情報提供が困難である点が特異である。本人、転職先企業、リファレンス提供者のそれぞれが必要かつ十分な情報のやりとりをする必要があり、それぞれのエンティティが、どの情報を誰に見せるかを厳密にコントロールできる必要がある。また、本人確認情報に加え、現・前職における在籍確認の証明も必要となるが本人のプライバシーを確保した方法が必要である。

⑤ ステークホルダー毎のペインポイント

ステークホルダー毎の視点でペインポイントをまとめると、以下の通りになる

1. 転職先企業側
 - a) 応募者、リファレンス提供者が本人であることの確認が容易ではない。
 - b) 応募者、リファレンス提供者が現・前職企業に在籍していること・いたことの確認が難しい。
 - c) 応募書類やリファレンス内容が改ざんされていないかの検証ができない。
 - d) 応募者の意図しない情報を受け取ってしまうかもしれない。
 - e) 応募者やリファレンス提供者から、属性情報の取扱いについて不安を持たれている懸念がある。
2. 応募者側
 - a) 本人確認のために、応募とは直接関係の無い情報を開示する必要がある。
 - b) 応募書類やリファレンス内容が改ざんされていないか確認ができない。
 - c) 応募者本人が自らの情報の開示内容、開示先がコントロールできない。

- d) 応募書類やリファレンス内容を誰がいつ参照したかを確かめられない。
 - e) 応募時に提供したデータの撤回ができない。
 - f) 情報が目的外利用や意図しない第三者に提供される可能性がある。
3. リファレンス提供者側
- a) リファレンスの内容が応募者本人や転職先企業以外に知られてしまうかもしれない。
 - b) リファレンス内容を誰がいつ参照したかを確かめられない。

⑥ ペインポイントの整理

ペインポイントを、整理・集約すると、以下のようになる

1. 全ての参加者の視点
 - a) 情報をやりとりする相手が、主張する通りのアイデンティティに結びつく本人であるかを確認できない
 - b) 相手が示した属性情報が正しいのか
 - c) 相手が所属（現在あるいは過去）を主張している企業への在籍の事実があるか
 - d) やりとりする情報が改ざんされているかどうか検証できない
2. 情報の提供側の視点
 - a) 提供する情報が正しく管理されていることを知り得ない
 - b) 提供する情報が不正に開示されるリスクがある
 - c) 目的外利用や第三者提供のリスク
 - d) 提供する必要がない情報を開示する必要がある場合がある
 - e) 提供した情報を撤回できない
3. 情報の受け取り側の視点
 - a) 受け取った情報が正しく管理されていることを情報提供側に示すことができない
 - b) 不必要な情報を受け取るリスクがある

(4) Trusted Web 技術の適用

本節では、情報の検証可能な範囲を広げる Trusted Web 技術がどのように適用出来るかについて議論する。

① 効果を期待できるポイント

本人確認情報や在籍確認情報などを検証可能な情報として渡すことで、転職先企業側の関係者が本人であることや在籍を現実的なコストで確認可能になることが期待できる。応募者本人やリファレンス提供者が転職先企業に対して、必要な情報のみ転職先企業にのみ開示する形で提供することとし、検証可能な情報への一次アクセスを制御できるようにすることで応募者本人は、開示先をコントロールし参照履歴も確認することができる。また、採用企業において、例えば情報を取得する際の同意や、取得した情報を目的外利用していないことの証明・担保が容易になることにより、情報の取扱いに対する信頼性を高め、これら関係者が安心して自らの情報を提供できる環境を整えることができる。

ここで述べたように、情報をやり取りする相手の確証が持て、個人のスキルや実績等のデータを各個人が開示範囲のコントロールしつつ、情報自身の確からしさを確保しつつ伝達することが一般にできる。このような個人の情報の制御下におけるやり取りが実現することにより、①個人にとっては、自らが活躍し、自己実現できる機会を広げることができ、②採用企業にとっては、コロナ後や DX に伴う社会の変革の中で、効率的・効果的な採用を実現でき、③社会全体にとっては、人口減の中で、社会全体として人材リソース配分の最適化を図ることができる。

② 適用方針

1. Verifiable Credentials と証明書

本ユースケースでは、W3C 標準である Verifiable Credentials[VC]¹(以下、VC) の適用を想定して議論する。加えて、トラストヒエラルキ確保における必要に応じて、X.509 PKI²を適用する。

2. 関係者それぞれの本人確認

本ユースケースにおいては、なんらかの方法で本人に到達可能なアイデンティティを示す VC を入手する必要がある。たとえば、Identity Provider (IdP) を合わせて提供しているようなメールサービスを起点として、本人への到達性が確認されているメールアドレスを示す VC を発行できる。一方、本人を示す VC とそのアイデンティティに結びつけられたアイデンティティアシュアランスの程度 (IAL) の必要性については議論が必要である。

¹ 出典 : W3C Verifiable Credentials Data Model 1.0
<https://www.w3.org/TR/vc-data-model/>

² 出典 : RFC5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
<https://www.rfc-editor.org/rfc/rfc5280>
IPA による和訳:
<https://www.ipa.go.jp/security/rfc/RFC5280-00JA.html>

3. 所属の確認

確認の対象者が当該組織に所属していることを示すことができる VC を用意し用いる。確認の対象者のアイデンティティに、当該在籍組織の所属について証明する情報が紐付いていれば用いることが出来る。単純に在籍を示すだけであれば、「デジタル名刺」相当の VC があれば、流用可能である。一方、本ユースケースにおいては、在籍確認がなされたことを在籍先に知られたくない、というプライバシー上の要件がある。証明書発行者は基本的に在籍している組織であるので、証明書発行者に何らかの問い合わせをするような VC (【家に電話をかける】タイプ) は適用できないが、デジタル名刺における有効性確認をある程度妥協することで流用は可能と言える。

③ 関与するデータ

1. 人のアイデンティティにまつわる情報
 - a) 応募者
 - b) リファレンス提供者
 - c) 転職先企業の担当者
2. 組織（法人）のアイデンティティにまつわる情報
 - a) 転職先企業
 - b) 応募者の所属企業、あるいは、かつての所属企業
 - c) 特定の者の特定の組織への在籍確認情報
 - d) 応募者の在籍確認情報
 - e) リファレンス提供者の在籍確認情報
3. 応募者が記述した応募に関する情報
4. リファレンス情報

④ エンティティ間のやりとり

1. 転職先企業が、応募サイトを公開する。
2. 応募者が応募の意思を表示し、以下の情報を転職先企業だけが復号できるように暗号化し、ストレージにアップロードする。
 - a) 発行されている本人確認 VC
 - b) 現・前職企業から発行されている在籍確認 VC
3. 応募者が転職先企業に応募に必要な情報を送付する。
 - a) 本人確認 VC、在籍確認 VC のダウンロード URL
 - b) 連絡に必要なメールアドレス
4. 転職先企業が本人確認 VC、在籍確認 VC をダウンロードし復号化、検証する。
 - a) このときにダウンロードの履歴が残る
5. 転職先企業が応募者に対してリファレンスを要求する。
6. 応募者はリファレンス提供者に以下の情報とともにリファレンスへの回答を要求する。
 - a) 転職先企業 DID³（または公開鍵）
7. 応募者はリファレンスに回答し VC を作成する。
8. 応募者は以下の情報を転職先企業だけが復号できるように暗号化し、応募者のストレージにアップロードする。

³ 出典：W3C Decentralized Identifiers (DIDs) v1.0
<https://www.w3.org/TR/did-core/>

- a) 発行されている本人確認 VC
- b) 現・前職企業から発行されている在籍確認 VC
- c) リファレンス回答 VC
- 9. リファレンス提供者はリファレンス回答したこと、アップロードしたことを応募者に伝える。
- 10. 応募者はリファレンスに関する情報をダウンロードする URL を転職先企業に伝える。
- 11. 転職先企業がリファレンス提供者の本人確認 VC、在籍確認 VC、リファレンス回答 VC をダウンロードし復号化、検証する。
 - a) このときにダウンロードの履歴が残る

⑤ 証明書とトラストヒエラルキ

1. 用いられる VC/証明書

- 1. 組織を示すもの
 - a) 転職先の企業を示すもの
 - b) 転職元の企業を示すもの
- 2. 関係者・担当者を示すもの
 - a) 応募者本人の本人確認情報
 - b) リファレンス提供者の本人確認情報
- 3. 特定の者の特定の組織への在籍確認情報
 - a) 本人の在籍証明情報
 - b) リファレンス提供者の在籍証明情報
- 4. 本人の記述した応募に関する情報
 - a) 本人が応募のために用意した情報
- 5. リファレンス情報
 - a) リファレンス対象と、リファレンスを記述した者と、記述内容をデジタル署名されたデータとして示す VC

⑥ VC/証明書の発行者とトラストヒエラルキ

- 1. 組織を示すもの
組織を示す VC/証明書についての議論は、法人ユースケースの議論を参照のこと。
- 2. 関係者・担当者を示すもの
関係者、担当者は、組織によって発行された在籍証明を用いるのが適切であり、組織が用いている証明書あるいは VC に紐付いた公開鍵を用いる。
- 3. 特定の者の特定の組織への在籍確認情報
関係者、担当者は、組織によって発行された在籍証明を用いるのが適切である。
- 4. 本人の記述した応募に関する情報
本人を示す証明書に紐付いた公開鍵、あるいは、本人が用いている事を証明できる、対象毎に用意した公開鍵を用いて署名する。
- 5. リファレンス情報
リファレンス提供者を示す証明書に紐付いた公開鍵、あるいは、本人が用いている事を証明できる、対象毎に用意した公開鍵を用いて署名する。

(5) 議論

① 検討外とした事項

一度ダウンロードされ復号化された情報については応募者本人がコントロールできないため、本ユースケースでは対象外とした。

② Trusted Web モデル適用の有効性

③ 脅威モデルと分析

④ セキュリティ視点での考察

⑤ プライバシー視点での考察

⑥ 他分野への応用可能性

⑦ その他の議論

(6) 付録：用語

1. 属性情報

2. Verifiable Credentials (VC) [VC]

① 本人確認 VC

8

② 在籍確認 VC

```
{
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://github.com/DataSignInc/trusted-web-  
vocab/blob/f0780b88084cfbae3b119473362b2d1e1c807ab9/schema.jsonld"
    ],
    "type": [
      "VerifiableCredential",
      "EmployeeCredential"
    ],
    "credentialSubject": {
      "worksFor": "did:ion:EiBoZxu209mxIv-fAYJU6b3ekH-6qYWWIBPQJBvyNTxggQ",
      "memberOf": {
        "id": "https://example.com/dummy-id",
        "type": [
          "Organization"
        ],
        "name": "技術部",
        "parentOrganization": "did:ion:EiBoZxu209mxIv-fAYJU6b3ekH-  
6qYWWIBPQJBvyNTxggQ"
      },
      "jobTitle": "シニアコンサルタント"
    }
  },
  "sub": "did:ion:EiBwmsE3SVMSqNDgoUtRbtP0BYZFdnELOGkBybEOEo3QDQ:eyJkZWx0YSI6eyJwYXRjaGVzIjpbeyJhY3Rpb24iOiJyZXBsYWNIIEwiZG9jdW1lbnQiOnsicHVibGljS2V5cyI6W3siaWQiOiJrZXktMSIsInB1YmtpY0tleUp3ayI6eyJjcniOiJzZWwmbU2azEiLCJrdHkiOiJFQyIsIngiaWJOWFhrSTVVcy1jR1k3WHBNalUzUW5NT01uUS1PbWIYQmsxMORic2txZC1nIiwieSI6IiJBMMFFb2IQTXZpbE1wNk1hZ1NTV1RJQ3BCYWR2ZmFURGOxTIV2X0h4emsifSwichHVycG9zZXMiOisiYXVOaGVudGljYXRpb24iLCJrZXIBZ3JlZW1lbnQiXSwidHIwZSI6IkVpZzd4amIraGhcnhuSG5aY2Foaw9uS2V5MjAxOSJ9XX19XSwidXBkYXRlIQ29tbWlObWVudCI6IkVpZzd4amIraGhcnhuSG5aATIQMNWNYROIeVdPZ1FPdlRMjlPngROVGJnc3cifSwic3VmZml4RGFOYSI6eyJkZWx0YUhhc2giOiJFaURidHE1MOthRUlka01UcG53SXkxYzNQVmxvS0lvZUI0SHkyZTU3ejllSm9RIiwicmVjb3ZlcnlDb21taXRtZW50IjoirWIDV21mN21NYkpvdMDhpRzFBbkhhOVJUSUFRS3F2WFIiU19EZDIanZkzUTB1dyJ9fQ",
  "nbf": 1646126857,
  "iss": "did:ion:EiBoZxu209mxIv-fAYJU6b3ekH-6qYWWIBPQJBvyNTxggQ"
}
```

③ リファレンス VC

```
{  
    "vc": {  
        "@context": [  
            "https://www.w3.org/2018/credentials/v1",  
            "https://github.com/DataSignInc/trusted-web-  
vocab/blob/f0780b88084cfbae3b119473362b2d1e1c807ab9/schema.jsonld"  
        ],  
        "type": [  
            "VerifiableCredential",  
            "ReferenceCredential"  
        ],  
        "credentialSubject": {  
            "relationship": "boss",  
            "communicationAbility": "円滑に会議を進行していた。",  
            "achievement": "プロジェクトリーダーとしてプロジェクトを成功に導いた。  
",  
            "author": "  
did:ion:EiBWmsE3SVMSqNDgoUtrBtp0BYZfDneLOGkByBE0Eo3QDDQ:eyJkZWx0YSI6eyJwYXRjaGVzIjpbeyJhY3Rpb24iOiJyZXBsYWNIIEwiZG9jdW1lbnQiOnsicHVibGljS2V5cyI6W3siaWQiOiJRZXktMSIsInB1YmxpY0tleUp3ayI6eyJjcniYoiOjZzZWNoMjU2azElLCJrdHkiOiJFQyIsIngiaWVudCI6ImNmbmFFb2ltXZpbE1wNmhhbmVudCmlleVdpZ1FPdlIRmjlpNGROVGJnc3cifSwic3VmZml4RGFOYSI6eyJkZWx0YUhhc2giOiJFaURidHE1MDthRUlkao1UCg53SXkxYZnNQVMxvSOlvZUIrSHkyZTUzejlISm9RIiwicmVjb3ZlcnlDb21taXRtZW50IjoirWDV21mN21NYkpvdMDhpRZFBBkhhoVJSUFRS3F2WiFiU19EZDIanZkdUTBDydj9fQ","  
answerDate": "2022-03-01T09:27:37.580Z"  
}  
},  
    "sub": "  
did:ion:EiBWmsE3SVMSqNDgoUtrBtp0BYZfDneLOGkByBE0Eo3QDDQ:eyJkZWx0YSI6eyJwYXRjaGVzIjpbeyJhY3Rpb24iOiJyZXBsYWNIIEwiZG9jdW1lbnQiOnsicHVibGljS2V5cyI6W3siaWQiOiJRZXktMSIsInB1YmxpY0tleUp3ayI6eyJjcniYoiOjZzZWNoMjU2azElLCJrdHkiOiJFQyIsIngiaWVudCI6ImNmbmFFb2ltXZpbE1wNmhhbmVudCmlleVdpZ1FPdlIRmjlpNGROVGJnc3cifSwic3VmZml4RGFOYSI6eyJkZWx0YUhhc2giOiJFaURidHE1MDthRUlkao1UCg53SXkxYZnNQVMxvSOlvZUIrSHkyZTUzejlISm9RIiwicmVjb3ZlcnlDb21taXRtZW50IjoirWDV21mN21NYkpvdMDhpRZFBBkhhoVJSUFRS3F2WiFiU19EZDIanZkdUTBDydj9fQ",  
nbf": 1646126857,  
iss": "  
did:ion:EiBWmsE3SVMSqNDgoUtrBtp0BYZfDneLOGkByBE0Eo3QDDQ:eyJkZWx0YSI6eyJwYXRjaGVzIjpbeyJhY3Rpb24iOiJyZXBsYWNIIEwiZG9jdW1lbnQiOnsicHVibGljS2V5cyI6W3siaWQi
```

0iJrZXktMSIsInB1YmXPY0tleUp3ayI6eyJjcnYi0iJzZWNwMjU2azEiLCJrdHki0iJFQyIsIngi
0iJOWFhrSTVVcy1jR1k3WHBNaIUzUW5NT01uUS1PbWlYQmsxMORlc2txZC1nIiwieSI6IiJBMmFF
b2lQTXZpbE1wNk1hZ1NTV1RjQ3BCYWR2ZmFURG0xTV2X0h4emsifSwicHVycG9zZXMi0lSiYXV0
aGVudGljYXRpb24iLCJrZXlBZ3JlZW1lbnQiXSwidHlwZSI6IkvjZHNhU2VjcDI1NmsxVmVyaWZp
Y2F0aW9uS2V5MjAxOSJ9XX19XSwidXBkYXRlQ29tbWl0bWVudCI6IkVpQzd4amlraGhHcnhuSG5a
aTlQMWNyR0lieVdPZ1FPdlIRMjlpNGROVGJnc3cifSwic3VmZml4RGFOYSI6eyJkZWx0YUhhc2gi
0iJFaURidHE1M0thRUlka01UcG53SXkxYzNQVmxvS0lvZU1DSHkyZTU3ejl1Sm9RIiwicmVjb3Zl
cnlDb21taXRtZW50IjoirWlDV21mN21NYkpvMDhpRzFBbkhh0VJUSUFRS3F2WIFIU19EZDlaNzkz
UTB1dyJ9fQ”
}

法人

(1) タイトル

法人と補助金

(2) 背景

中小企業等が補助金等を行政に対し申請する際、申請書とともに様々な提出書類を提出する。申請書は企業が用意するが、提出書類として国や中小企業支援機関によって一定のお墨付きを与えられた書類を用意し申請書とともに提出する。現状では、申請書自体の形式が補助金によって異なるので、それに合わせて手作業により情報を入力するか他の文書から文字情報としてコピーする必要がある。ここには間違いが入り込む余地があると同時に、手間がかかる⁴。提出書類については、確からしさを容易に確認できない場合があり、類似事例として、実際に確定申告書に対する収受印を偽造した不正給金申請の事例報告等がある。

本ユースケースでは、令和4年度1月20日募集を開始した、[事業再構築補助金]⁵の第5回公募の情報を元に、法人が通常枠での補助金額3,000万円を越える申請を行う場合に限定して議論する。

(3) 記法についての留意点

本文書では、「文書」と「情報」を書き分けているが、「情報」と読み替えても正しく読めるはずである。ただし、「文書」と記述しないと不自然であるところは「文書」としている。

⁴ 申請書作成については gBizID の利用により緩和できている部分がある

⁵ 事業再構築補助金 ウェブサイト

<https://jigyousaikouchiku.go.jp/>

(4) 議論するペインポイント

- 補助金の募集及び受付をする受付機関、申請者、申請に関係した情報を扱う業者等のステークホルダー間でやりとりされる情報の形式が、補助金毎に必要な情報が異なることで提出機会毎に異なることが多々あり、結果、複数の補助金申請をする場合、情報を揃えて提出する側に大きな痛みがある。デジタル技術を活用することによって、提出された書類の内容の正しさを、紙ベースの書類より少ない手数で確認することができるのではないかと期待される。

(5) 効果を期待できるポイント

「信頼できる情報」を組み合わせる事によって、情報が発信者から発信された時の状態から改変されていないこと、さらに発信者が一定の確認をしたことを示すことができる（「確認」の程度の定義は(7)参照）。これらの事実に頼ることで、法人等の法人の補助金申請における申請者と補助金受付組織の負担を軽減でき、不正補助金申請の削減が見込まれる。

(6) 本ユースケースにおける特異な点

- 申請手続きが、申請者の営業についての情報に關与するエンティティとの連携によって実現されている
- 申請手続きにおいて、gBizID、jGrants等の既存の事業者のためのサービスが適用可能である

(7) 本文書における「確認」の定義

本文書で「情報を確認した」と記述される行為の意味を書き分けるため、確認の段階を定義する必要がある、ここで整理する。

仮に、情報Dを確認の対象として、A（情報の作成者）、B（確認をするもの）が関与するとする。複数の情報を揃えて提出することになるので、情報が複数である場合についても考慮する。ここで「情報Dの内容を確認する」あるいは「情報一揃いを確認する」という行為には、いくつかの段階がある。なお、以下に記す「指定された基準」とは、申請書作成の指示で示されている事項とする。

1. 外形的な確認の段階
(外形的とは、書き込む欄が揃っている、と解釈されたい)
 - a) 情報が存在する
 - b) 情報が存在し、かつ、指定された外形通り整っている
2. 単一の情報としての内容の確認の段階
 - a) 外形が整っており(上記1.を満たす)、かつ、必要な項目が記載されている。
 - b) 上記に加え、それぞれの必要な記載項目が、指定された基準に従って記載されている
3. 情報の集まりとしての確認の段階
 - a) それぞれの情報の内容を(上記2.を満たすことで)確認でき、提出情報の組み合わせと数において指定された基準に合致していること
 - b) b) 上記に加え、提出された情報間に齟齬が無い事。

さらに、情報についてはそれぞれの情報の作成者が、情報の集まりについては情報の取りまとめをするもの（申請者）が確認し、署名することができる。

以下の説明では、【形式確認済み】という表現を、上記 1. の確認をしたことを示すこととし、【内容確認済み】という表現を、情報を対象とした場合は 2. の確認をしたことを、情報の集まりを対象とした場合は 3. の確認をしたこととする。

なお、今回議論しているユースケースにおいて署名をすることの意味は、下記の例外を除き、上記における確認 2b あるいは 確認 3b 相当を作成者あるいは申請者が署名時に行ったということを示すに過ぎないとする。例外は、以下の二点である

1. 本ユースケースで対象としている事業再構築補助金における「確認書」の発行者が、「確認書」提出に当たって求められている通りに実際に【確認】したことを示す
 2. 書類に宣誓事項が含まれる場合は、その宣誓を含意する
- 上記二点については電子署名法による解釈が必要である。

(8) 現状

事業再構築補助金申請における現状を整理する

① エンティティ

詳細については〔公募要領〕⁶ 参照。

- 受付機関（経済産業省から基金設置法人経由で委託を受けた事業実施事務局）
- 申請者：補助金を申請する事業者（説明文書中では「補助事業者」）
- 税務署（国税庁）
- 認定経営革新等支援機関
- 金融機関
- gBizID サービス
- jGrants サービス
- ミラサポplus サービス

② 関与する情報

詳細については〔公募要領〕参照。

1. 事業再構築補助金特設応募サイトで電子申請時に入力する情報
1. 事業計画書
 - a) 売り上げ減少を示すための資料（比較できる2期分）
 - b) 確定申告書の場合：確定申告書の一部
 - 1) 確定申告書第一表の控え
 - 2) 法人事業概況説明書の控え
 - 3) 上記は、收受日押印済のもの、または申告に対するe-Tax受信通知
 - c) 確定申告の基礎となる書類（試算表、帳面、その他）
2. 決算書等
3. 事業財務情報
4. 労働者名簿
5. 事業計画の内容が精査し妥当と認められたことを示す情報
 - a) 認定経営革新等支援機関による事業計画の確認証
 - b) 金融機関による事業計画の確認証

提出される情報の確認は情報により異なる。それぞれの情報の作成者、確認者、関係性を以下に示す。

⁶ 令和二年度第三次補正 事業再構築補助金 公募要領（第5回）
<https://jigyousaikouchiku.go.jp/pdf/koubo005.pdf>

表 1. 事業再構築補助金申請時の添付書類（法人・通常枠のみ・申請額 3000 万超の場合を抜粋）

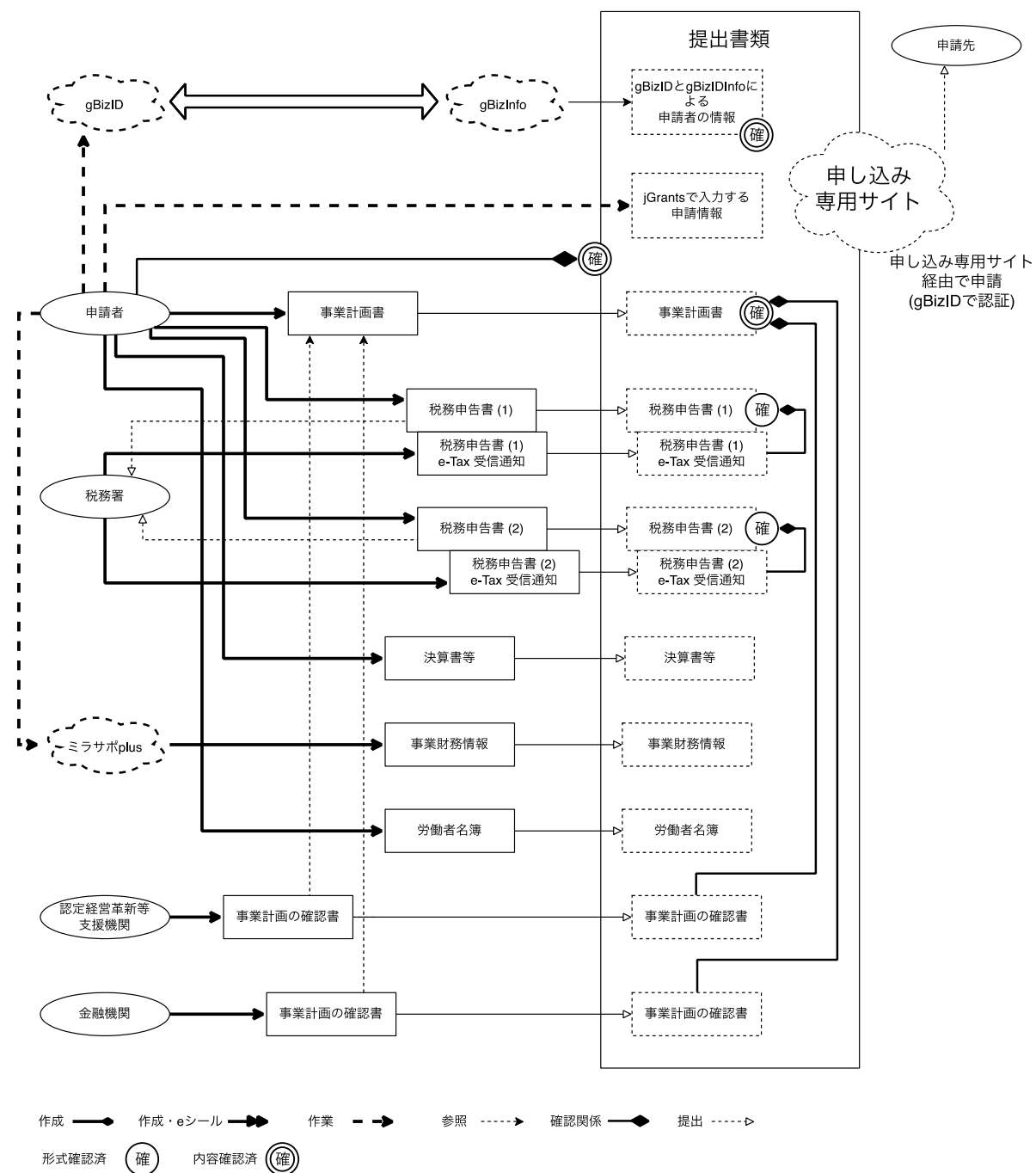
項目	対象情報	確認対象の情報	作成者	提出された書類の形式 の確認者（作成者を除く）	内容の確認者 （作成者を除く）
電子申請時に入力する事項	事業再構築補助金特設応募サイトで入力（参考資料として電子申請入力項目準備用のファイルあり）	入力された情報	申請者	事業再構築補助金特設応募サイト	－
事業計画書	・ 事業計画書	－	申請者	－	認定経営革新等支援機関および金融機関
認定経営革新等支援機関による確認書	・ 認定経営革新等支援機関による確認書（様式 1-1） ⁷	事業計画書	認定経営革新等支援機関	認定経営革新等支援機関	－
金融機関による確認書（補助金額 3,000 万円を超える事業の場合）	・ 金融機関による確認書（様式 1-2）	事業計画書	金融機関	金融機関	－
コロナ以前に比べて売上高が減少したことを示す書類 又は コロナ以前に比べて付加価値額が減少したことを示す書類 ※コロナ以前とコロナ以降の両方が必要	（法人の場合）売り上げ減少を示すための比較対象の 2 期分の確定申告書の一部 － 確定申告書第一表の控え － 法人事業概況説明書の控え 及び収受日押印済の控えまたは e-Tax 受信通知あるいは確定申告の基礎となる書類（試算表、帳面、その他）	－	申請者	税務署	－

⁷ 「認定経営革新等支援機関 ID 番号」を記載する必要がある

項目	対象情報	確認対象の情報	作成者	提出された書類の形式 の確認者（作成者を除く）	内容の確認者 （作成者を除く）
電子申請時に入力する事項	事業再構築補助金特設応募サイトで入力（参考資料として電子申請入力項目準備用のファイルあり）	入力された情報	申請者	事業再構築補助金特設応募サイト	－
決算書等	・ 決算書（貸借対照表、損益計算書、製造原価報告書、販売管理費明細、個別注記表）	－	申請者	－	－
経済産業省ミラサポplus 「電子申請サポート」により作成した事業財務情報	・ 事業財務情報	ミラサポplusで作成した事業財務情報	申請者	ミラサポplus	－
労働者名簿	・ 労働者名簿の写し	労働者名簿	申請者	－	－

③ 事業再構築補助金申請における情報の流れ

以下の図で事業再構築補助金におけるエンティティ、関与する情報と提出における手順について整理する



注:

- 形式確認済: 対象情報を形式の点で確認したことを示す
- 内容確認済: 形式に加え内容についても確認していることを示す

④ 事業再構築補助金申請の手順

1. 前提および事前準備

1. 申請者は以下の事前準備を済ませている前提とする。
 - a) gBizID プライムのアカウント作成
 - b) ミラサポ plus のアカウント作成 (gBizID アカウントが必要)

2. 申請における流れ

1. 補助金に関する制度説明資料、申請に関する資料、添付書類および参考資料等がウェブサイトで公開される。事業再構築補助金については[事業再構築補助金]で公開された
2. 申請者は電子申請時に入力する項目を用意する（[事業再構築補助金電子申請入力項目]⁸⁾）
3. 申請者は以下の添付書類を用意する
 - a) 確定申告書 2 期分の以下の部分
 - 1) 確定申告書第一表の控え
 - 2) 法人事業概況説明書の控え
 - b) 上記の收受日押印済の控え、あるいは、e-Tax 受信通知。收受印の無い場合は納税証明書で代替する。
 - c) 決算書写し
 - d) 労働者名簿の写し
 - e) 事業財務情報（ミラサポ plus サイトで作成）
4. 申請者は事業計画書（15 ページ以内のフリーフォーマット。内容については[事業再構築補助金電子申請入力項目]に指示あり）を認定経営革新等支援機関や金融機関とやりとりしながら、必要に応じて上記添付情報を提示しつつ作成する。
5. 認定経営革新等支援機関と金融機関は事業計画書の実現性を確認した後に、確認書類を作成する。
6. 申請者は 事業再構築補助金特設応募サイトにて申請準備を行う。この際に上記「電子申請時に入力する項目」にて用意した情報を入力する。
7. 申請者は 事業再構築補助金特設応募サイト経由で事業計画書と添付書類一式を提出する
8. 受付機関が受け取り、申請書受理票を発行
9. 受付機関は審査を実施
10. 審査には採択審査委員会が関与
11. 受付機関が申請者に採択結果を通知

⑤ 今回の議論から除外した事項・今後議論が必要な事項

- 採択結果通知後の手続きについては、今回は議論を省く。
 - 申請書類が受理されたことは確認できるため問題がないが、書類が受理された後の処理の進行状況の随時確認におけるペインがあることが理解されている。一方、ただし、補助金申請の受理までの流れにおいてはこの点の痛みは少ないという判断で、議論からは除外した。
 - 一方、採択結果通知後の交付申請処理については、進行状況について知りたいという要望があると理解している。
- ☐ なお、補助金と異なり、給付金の場合は申請から給付が直結しているので、処理の進行状況には強い関心があるという意見がある。

⁸ 令和二年度第三次補正 事業再構築補助金 ウェブサイト / 資料ダウンロード
電子申請入力項目 (Word)
<https://jigyousaikaouchiku.go.jp/pdf/denshi.docx>

- 全体のプロセスの確からしさについても Trusted Web の議論の対象であるが、今回の議論からは除外した。
- 今回は、gBizID、jGrants、ミラサポ plus 等の既存のサービスをそのまま適用する形で示したが、このやり方が長期的な最適解であるかどうかについては議論の余地がある
- 議論を単純化させるため、銀行や、認定経営革新等支援機関等、補助金申請組織以外の関係者も、gBizID を持っているとは仮定している。実際には、領域に応じた Identity Provider (IdP) を適用する、あるいは、認定経営革新等支援機関の証明書を保持するなどといった設計が取り得る。

(9) 現状の問題点

ここで、現状の問題を、提出される書類のタイプによって整理する。一部の事例は、事業再構築補助金で確認されている申請の不備の例⁹を例としてあげた。

① 申請者が作成する書類の内容の正しさに関する問題

申請者によって作成された書類に含まれる情報が、求められている情報に合致した正しい情報であるかどうかの確認が難しい。事業再構築補助金申請で確認されている不備の例を以下に示す。

1. 「認定経営革新等支援機関による確認書」に記載された法人名等が申請者と異なる。
2. 認定経営革新等支援機関ではなく、申請者名で「認定経営革新等支援機関による確認書」が作成されている

② 他の組織によって作成された書類の正しさに関する問題

他の組織によって作成または確認された書類を添付する場合があるが、それらの書類が作成も元、あるいは確認者によって確認された後に、意図的に改変されるリスクがあり、その検知に向けた工数がかかっている。

③ 提出された書類一揃い全体に対する正しさに関する問題

用意された書類や添付書類がそろっていても、申請書類全体として正しく揃えられているかどうかという問題がある。事業再構築補助金申請で確認されている不備の例を以下に示す。

1. 月別売上高が証明する書類が添付されていない（形式の不備）
2. 選択された年月とは異なる年月の書類が添付されている（内容の不備）
3. ミラサポ plus からの「事業財務情報」が添付されていない（形式の不備）

④ 申請者が作成する書類の形式についての問題

デジタル化が全く進んでいない支援事業は多数あり、それらについては、提出者自身が作成する書類が支援事業によってまちまちであり、毎回形式を合わせて入力する必要がある。

なお、事業再構築補助金の場合は、専用サイトから申し込む形になっているため、手入力をする必要があるものの、複数の書類に同一事項を書き込むなどといった、従来の紙による申請と比べ痛みは少ない¹⁰

⁹ https://jigyousaikouchiku.go.jp/pdf/shinsei_fubi.pdf

¹⁰ ただし、項目によってはコピー＆ペーストさえ出来ないという指摘がある

(10) Trusted Web 技術の適用

① 方針

1. 対象となる情報を完全性と情報の出所をともに確かめられるようにすることにより、Trust できる範囲を拡大する。このことにより、情報の出所まで遡るような確認の繰り返しを避けることができる。これを実現するために、デジタル署名¹¹を活用する。情報の出所でデジタル署名し、かつ、デジタル署名をするのに用いた公開鍵を示すために必要に応じて公開鍵証明書を組み合わせる。本質的には e シールを活用する¹²。なお、プロセスの正しさについては、本ユースケースではアウトオブスコープである。
 - a) 【形式確認済み】【(形式及び)内容確認済み】とされている情報がそれぞれの確認後に改ざんされていないこと、そして確認者が誰であるかを e シールで確認できる
 - 1) 形式確認 e シール: 対象情報を形式の点で確認したことを示す e シール
 - 2) 内容確認 e シール: 形式に加え内容についても確認していることを示す e シール
 - 3) 電子帳簿保存法対応の税務・会計システムを用い、電子帳簿保存法に則った形で発行された試算表などのレポート機能を活用し、内容確認 e シール付きの文書として参照できるようにする
2. エンティティに関連するエンティティ自体の開示可能な属性情報を整理し、属性情報の証明書を発行し用いる
 - a) gBizID 経由で属性情報証明書を発行する
 - b) デジタル名刺的に、各エンティティの担当者の所属や連絡先などの情報が確認可能となる
 - c) 認定経営革新等支援機関の認定経営革新等支援機関 ID 付きの情報を添付できる

② 適用する技術

公開鍵暗号技術を適用し、対象となる情報を完全性と情報の出所と共に確かめられるようにする。そのようにして確認された情報を組み合わせ、できる限り広範囲に適用することで、「検証可能な領域を広げることで Trust を高める」Trusted Web の効果を得る。この実現のためには、公開鍵暗号アルゴリズムだけでは実現できない。具体的には、以下の 4 つの標準あるいは技術の選択で決定される:

1. 対象となる情報の塊への参照(あるいは同梱)方法、または、シリアルライゼーションの方法
2. 対象となる情報の塊への公開鍵暗号によるデジタル署名におけるアルゴリズム選択(実際は暗号アルゴリズムとハッシュアルゴリズムの組み合わせ)
3. デジタル署名に用いられた公開鍵暗号鍵の出所を示す情報。一般には公開鍵証明書
4. 上記 1. ~3. を全てあるいは個別にパッケージング(シリアルライゼーション)する方式

¹¹ 電子署名とデジタル署名は区別する。法人における電子署名は代表者個人による意思表示が目的(電子署名法に基づく)

¹² e シールは、e シールの対象となる情報の完全性(integrity)確認と発行元証明が目的

いわゆる X.509 PKI で決まっているのは 3. と 3. のための 4. のみであり、上記 4 点を全てカバーするためには、X.509 PKI で決められていることだけでは不十分である。たとえば、e-Tax においては、1, 2 に相当する情報が別途規定されている[e-Tax 仕様書一覧]¹³。

現時点では、上記全てに対応する方式として、Verifiable Credentials に基づく方法を用いるのがフレキシビリティの点で適切と考えられる。VC を用いつつ、信頼の起点 (root of trust) として GPKI、Web Trust を組み合わせることができる。実際にこの方式に用いている方式の例としては、国内向けのコロナワクチン接種証明書 (国内用の Smart Healthcard 準拠版) があげられる。

一方、3. の内容によらず、4. が、「Trusted Web エコシステム」全体で同一形式であることが、広範囲での運用の点では望ましいが、現時点では Verifiable Credential に準拠する方式として、JSON + JWT と JSON-LD + Linked Data Proof の二つが存在する。

なお、交換される文書へ付与される情報改ざん検知と出所確認情報は「e シール」として整理するのが妥当と考える。ただし、現時点では e シールの日本国内における定義は無く、議論が進められていると認識している。そのため、将来、今回ユースケースで使うのに過不足ない形で定義されるということを前提で、e シールとして整理することにした。

③ 追加されるエンティティと情報

1. 電子帳簿保存法対応の税務・会計システム

a) 以下のようなレポートを想定

- 1) 会計帳簿における月次推移
- 2) 会計帳簿における試算表
- 3) 収益レポート

④ エンティティ

1. 受付機関 (経済産業省から基金設置法人経由で委託を受けた事業実施事務局)
2. 申請者: 補助金を申請する事業者 (説明文書中では「補助事業者」)
3. 税務署 (国税庁)
4. 認定経営革新等支援機関
5. 金融機関
6. gBizID サービス
7. 事業再構築補助金特設応募サイト
8. ミラサポ plus サービス
9. 電子帳簿保存法対応の税務・会計システム
10. クラウド人事労務サービス提供者

⑤ 関与する情報

1. 事業計画書
2. 事業再構築補助金特設応募サイトする申請情報¹⁴
3. 電子帳簿保存法対応の税務・会計システムで管理されている以下の情報
 - a) 元帳

¹³ e-Tax 仕様書一覧

<https://www.e-tax.nta.go.jp/shiyo/shiyo3.htm>

¹⁴ 誓約事項があり。この部分は電子署名法上の考慮が必要

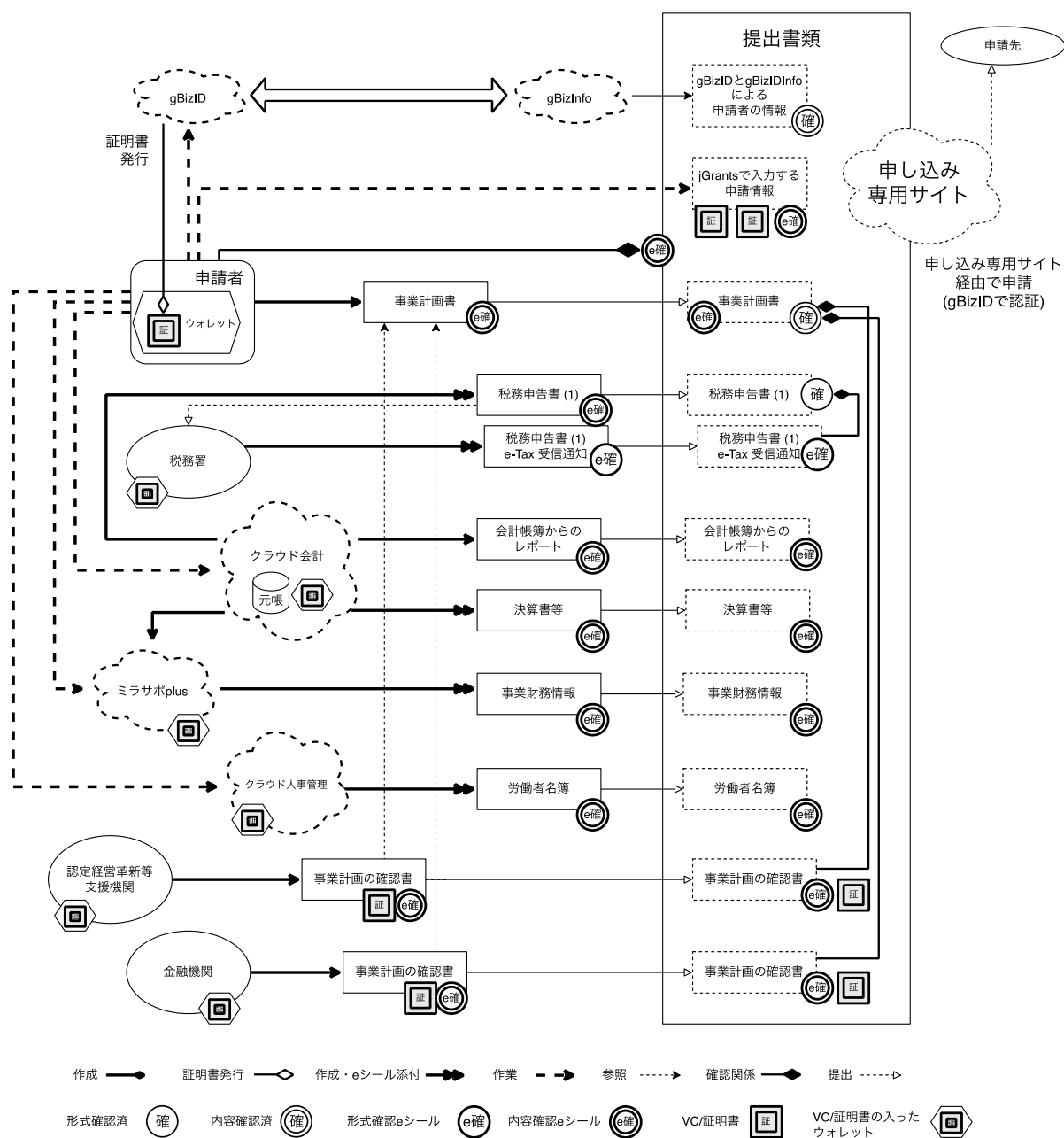
- b) 売り上げ減少を示すための資料（比較できる 2 期分）
 - 1) 確定申告書の場合：確定申告書の一部
 - i) 確定申告書第一表の控え
 - ii) 法人事業概況説明書の控え
 - 2) 確定申告の基礎となる書類
 - 会計帳簿における月次推移、会計帳簿における試算表、収益レポート等
- c) 決算書等
- d) 事業財務情報（ミラサポ plus 経由で形式を整える）
- 4. クラウド人事管理システムで管理されている以下の情報
- 5. 労働者名簿
- 6. 認定経営革新等支援機関による事業計画の確認証
- 7. 金融機関による事業計画の確認証

⑥ デジタル署名をするエンティティ

- 1. 関係者・担当者
- 2. 申請者の代表者（gBizID プライム想定）
- 3. 申請担当者（gBizID メンバー想定）
- 4. 事業実施場所担当者（gBizID メンバー想定）
- 5. 認定経営革新等支援機関担当者（gBizID メンバー想定）
- 6. 金融機関（銀行名のみ）（gBizID メンバー想定）
- 7. 民間クラウドサービス
- 8. 電子帳簿保存法対応の税務・会計システム
- 9. クラウド人事管理システム
- 10. 国の提供するクラウドサービス
- 11. gBizID
- 12. ミラサポ plus
- 13. 事業再構築補助金特設応募サイト
- 14. 税務署
 - 税務署の收受担当

⑦ 情報の流れ

Trusted Web 技術を適用した場合の情報の流れを以下に示す



注:

- 形式確認 e シール: 形式を確認したことを示す e シール
- 内容確認 e シール: 内容を確認したことを示す e シール
- VC/証明書: 所属証明書、または、官籍証明書、または、サービス証明書 (サービスプロバイダの提供するサービス)
- ウォレット: VC/証明書情報とともに対応する秘密鍵を保持し公開鍵暗号によってデジタル署名をするための機構。情報を与えることで、情報に結びついた e シールを発行できる。

⑧ Trusted Web を適用した場合の手順

1. 前提および事前準備

1. 申請者は以下を事前に行っていることとする
 - a) gBizID プライムのアカウント作成
 - b) ミラサポ plus のアカウント作成 (gBizID アカウントが必要)
 - c) 電子帳簿保存法対応の税務・会計システムを用いて電子帳簿法に則った形で元帳を管理する。
2. クラウド人事労務システムを用いて人事労務管理を行う。
3. それぞれのエンティティは、VC/証明書を入しウォレットに格納しておく（発行主体との対応関係は 7.7 参照）

2. 申請における流れ

1. 補助金に関する制度説明資料、申請に関する資料、添付書類および参考資料等がウェブサイトで公開される。事業再構築補助金については[事業再構築補助金]で公開された
2. 申請者は電子申請時に入力する項目を用意する（[事業再構築補助金電子申請入力項目]を参照）
3. 申請者は以下の添付書類を電子帳簿保存法対応の税務・会計システムを用いて用意する
 - a) 確定申告書 1 期分の以下の部分
 - 1) 確定申告書第一表の控え {内容確認 e シール付与}
 - 2) 法人事業概況説明書の控え {内容確認 e シール付与}
 - b) 上記の e-Tax 受信通知 {形式確認 e シール付与}
 - c) 決算書写し
 - d) 事業財務情報（ミラサポ plus サイト経由で作成）
4. 申請者は以下の添付書類をクラウド人事労務システムを用いて用意する
 - a) 労働者名簿 {内容確認 e シール付与}
5. 申請者は事業計画書（15 ページ以内のフリーフォーマット。内容については[事業再構築補助金電子申請入力項目]に指示あり）を認定経営革新等支援機関や金融機関とやりとりしながら、必要に応じて上記添付文書を提示しつつ作成する。
6. 認定経営革新等支援機関と金融機関は、それぞれの事業計画書の「内容は経済産業省が定める事業再構築指針に沿った取組であり、成果目標の達成が見込まれることを確認」し、確認書類を{内容確認 e シール付与}にて作成する。認定経営革新等支援機関担当者と金融機関の VC を付与する
7. 申請者は事業計画書に{内容確認 e シール}を付与する。文言は確認書テンプレートより引用。
8. 申請者は jGrants にて申請する。
 - a) 上記「電子申請時に入力する項目」にて用意した情報を入力する。
 - b) 事業計画書と添付文書一式をアップロードする
 - c) 申請する法人と申請する法人における担当者の VC を添付する
 - 1) 申請者の代表者情報
 - 2) 申請担当者
 - 3) 事業実施場所担当者
 - d) jGrants で用いられている gBizID に紐付いている法人登記情報が添付される
 - e) 提出書類全体に対して {内容確認 e シール} を付与する

- f) 提出する
- 9. 受付機関が受け取り、申請書受理票を発行
- 10. 受付機関は審査を実施
- 11. 審査には採択審査委員会が関与
- 12. 受付機関が申請者に採択結果を通知

⑨ トラストフレームワークとトラストヒエラルキ

1. 用いられる VC/証明書

1. 関係者・担当者を示すもの

以下のエンティティの VC を gBizID から発行しウォレットに収めて用いる。前提として、gBizID を Identity Provider (IdP) として VC を発行する形で整理した¹⁵。なお、議論を単純化させるため、申請担当者以外も gBizID を持っているとは仮定している

- a) 申請者の代表者情報
- b) 申請担当者
- c) 事業実施場所担当者
- d) 認定経営革新等支援機関担当者
- e) 金融機関（銀行名のみ？）

2. 民間クラウドサービス

以下のエンティティは、いわゆる Web PKI における X.509 PKI ベースの証明書を活用する（市販されている OS のトラストストアに含まれる root CA の子にあたる CA から販売・発行されているもの）

- a) 電子帳簿保存法対応の税務・会計システム
- b) クラウド人事管理システム

3. 国が提供するクラウドサービス

以下のエンティティは、GPKI トラストヒエラルキに基づいた X.509 証明書を発行し、用いる

- a) gBizID
- b) ミラサポ plus
- c) jGrants

4. 税務署

以下のエンティティは、GPKI トラストヒエラルキに基づいた X.509 官職証明書を発行し、用いる

- a) 税務署の収受担当

¹⁵ gBizID については、個人事業者を扱わなくするという議論があるが、法人も個人事業者を区別して議論していない

(11) 付録 A. Verifiable Credentials の例

特定技術を推奨するわけではないが JWT 形式の Verifiable Credentials で表現すると以下の形となる

- ① 法人 Wallet 内にストアされる G ビズ ID 依拠の VC 例 (G ビズ ID の鍵で署名した JWS を想定)

```
{
  "@context": [
    "https://www.w3c.org/2018/credentials/v1",
    "https://gbiz-id.go.jp/2021/credentials/prime/v1"
  ],
  "id": "http://gbiz-id.go.jp/credentials/prime/1242",
  "type": ["VerifiableCredential", "GBizIDPrimeCredential"],
  "issuer": "https://gbiz-id.go.jp/issuers/xxxx",
  "issuanceDate": "2022-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:ion:xxxxxxxx",
    "given_name": "〇 〇 ",
    "family_name": "〇 〇 ",
    "given_name": "タ ロウ",
    "family_name": "ヤマダ",
    "birthdate": "1980-01-01",
    "address": {
      "region": "13",
      "locality": "〇 〇 ",
      "street_address": "〇 〇 〇 〇 〇 〇 〇 〇 ",
      "postal_code": "0000000"
    },
    "phone_number": "111111111111",
    "email": "yamada.tarou@example.co.jp",
    "authority": {
      "name": "aaa 〇 〇 〇 〇 ",
      "registrationNumber": "27101007182XX",
      "registeredAddress": {
        "region": "13",
        "locality": "〇 〇 ",
        "street_address": "〇 〇 〇 〇 〇 〇 〇 〇 ",
        "postal_code": "0000000"
      }
    }
  }
}
```



```

    },
    "permission": [ {
      "role": "□ □ ",
      "validity": [ {
        "start": "2018-03-02T10:00Z"
      }
    ]
  }
],
},
}
}

```

② G ビズ ID が発行する法人に関する検証済みクレーム例

```

{
  "sub": "1242",
  "email": "yamada.tarou@example.co.jp",
  "verified_claims": {
    "verification": {
      "trust_framework": "ja_digital_agency",
      "time": "2020-04-23T18:25Z",
      "verification_process": "f24c6f-6d3f-4ec5-973e-b0d8506f3bc7",
      "assurance_level": "ial2",
      "evidence": [
        {
          "type": "document",
          "validation_method": {
            "type": "Commercial registration",
            "policy": "Commercial Registration Act.",
            "procedure": "submitted on the gbiz id registration web"
          },
          "document_details": {
            "type": "ja_commercial_register",
            "document_number": "99999",
            "serial_number": "ア 123456",
            "date_of_issuance": "2021-01-01",
            "date_of_expiry": "2030-12-31",
            "issuer": {
              "name": "XX □ □ □ ",
              "country": "JA",
              "jurisdiction": "JA"
            }
          }
        }
      ]
    }
  }
}

```

```

    }
  }
}
],
},
"claims": {
  "given_name": "□ □ ",
  "family_name": "□ □ ",
  "given_name": "タロウ",
  "family_name": "ヤマダ",
  "birthdate": "1980-01-01",
  "address": {
    "region": "13",
    "locality": "□ □ ",
    "street_address": "□ □ □ □ □ □ □ □ ",
    "postal_code": "0000000"
  },
  "phone_number": "11111111111",
  "authority": [ {
    "applies_to": {
      "organization_name#": "aaa □ □ □ □ ",
      "organization_name": "aaa corporation",
      "registration_number": "27101007182XX",
      "registered_address": {
        "region": "13",
        "locality": "□ □ ",
        "street_address": "□ □ □ □ □ □ □ □ ",
        "postal_code": "0000000"
      },
      "registered_jurisdiction": "?????"
    },
    "permission": [ {
      "role": "President",
      "validity": [ {
        "start": "2018-03-02T10:00Z"
      } ]
    } ],
    "granted_by": {
      "method": "pipp",

```

```

        "granting_body": "The Ministry of Justice",
        "reason": "registered as a commercial company"
    }
  ]
}
}
}

```

③ 税理士の署名がされた Verifiable Presentation

```

{
  "@context": [
    "https://www.w3c.org/2018/credentials/v1",
    "https://xxx/credentials/financialStatements/v1"
  ],
  "type": "VerifiablePresentation",
  "verifiableCredential": [{
    "@context": [
      "https://www.w3c.org/2018/credentials/v1",
      "https://xxx/credentials/financialStatements/v1"
    ],
    "id": "http://xxx/credentials/financialStatements/xxx",
    "type": ["VerifiableCredential", "financialStatements"],
    "issuer": "https://xxx/issuers/xxx", ← □ □ ソフト ?
    "issuanceDate": "2022-01-01T00:00:00Z",
    "credentialSubject": {
      "id": "did:ion:xxxxx",
      "name": "aaa □ □ □ □ ",
      "statements": {
        // □ □ □ □
      }
    }
  }
}

```

(12) 今回用いなかったテキスト

① 交付申請に纏わる部分の議論

以下の議論は、交付決定後のやりとりに関する部分のため、今回の申請までのフローに入らないので、削除した

事業再構築補助金のよくある交付申請の不備の例¹⁶

1. 相見積書の提出がない（形式の不備）
2. 見積書には、〇〇工事 とあるが、相見積書には、△△工事とある（内容の不備）
3. 提出される見積書と経費明細表が一致していない（内容の不備）
4. 経費明細表の積算基礎に「名称、単価、数量」が記載されていない（内容の不備）
5. 経費明細表の数字を修正したが、4. 事業概要（5）「本事業で取得する主な資産」が修正されていない（内容の不備）

¹⁶ https://jigyousaikouchiku.go.jp/pdf/documents/kofu_shinsei_fubi.pdf

サプライチェーンにおける化学物質管理

(1) 背景

各国・地域において、製品に含有される有害性の高い物質（例えば、REACH（Registration, Evaluation, Authorization and Restriction of Chemicals）規則で言えば、高懸念物質（SVHC: Substances of Very High Concerns）として規制）等の化学物質の製造・輸入や使用等に関する法規制がある。我が国においても、化学物質の審査及び製造等の規制に関する法律（昭和四十八年法律第百十七号、以下、化審法という。）により、化学物質の製造、輸入、使用等を規制している。また、環境の保全上の支障を未然に防ぐために、特定化学物質の環境への排出量の把握等及び管理の改善の促進に関する法律（平成十一年法律第八十六号、以下、化管法という。）により、事業者による化学物質の自主管理の改善を促している。欧州では、REACH 規則により化学物質の登録、評価、許認可、制限、情報伝達等を規制している。また、電気・電子機器については特に RoHS（Restriction of Hazardous Substances Directive）指令により特定有害物質の使用等を制限している。

本ユースケースでは、これらの規制への対応のためにサプライチェーンにおける化学物質の含有量の管理についての 4 つのシナリオとそのペインポイント、要求事項、Trusted Web 技術の適用可能性を議論する。

(2) 現状と想定されるシナリオ

現状のサプライチェーンにおける化学物質管理方法として、我が国の電気・電子機器の製造において広く利用されている chemSHERPA¹⁷ を利用した情報共有を元に議論する。

① エンティティ

本ユースケースにおけるエンティティは以下のとおりである。

- 川上企業（原材料（化学品等）メーカー等）
- 川中企業（部品、中間製品メーカー等）
- 川下企業（最終セットメーカー等）
- 化学物質管理規制当局（日本、諸外国・地域）
- 各業界の業界団体
- 国際標準化団体等
- コンサルタント（調査受託会社等）
- ソフトウェアプロバイダ
- ユーザー（事業者、消費者等）
- リサイクラー（リサイクル、廃棄業者等）
- 分析業者

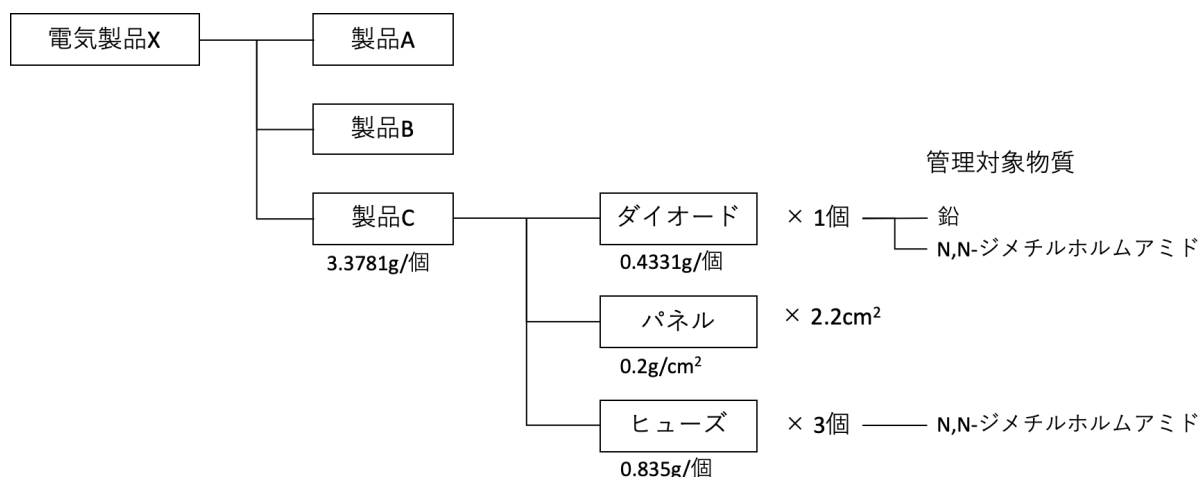
サプライチェーンにおいては、上流にある原材料（化学品等）メーカー等の川上企業、原材料や部品から部品や中間製品を製造する企業や商社（注：商品の受け渡しのみを手伝う場合

¹⁷ chemSHERPA by JAMP ウェブサイト
<https://chemsherpa.net>

がほとんどであるが、稀にサプライヤーを秘匿し、商社名で製品・部品を提供することもある。) 等の川中企業、これらの部品や中間製品から最終製品を製造する川下企業が中心的なエンティティとなる。また、化学物質の規制を行う化学物質安全管理規制当局や、各規制から業界に関連する化学物質リストを管理する各業界の業界団体や国際標準化団体もエンティティである。また、規制対象の化学物質の調査等を委託するコンサルタントや、これらの管理ソフトウェアを提供するソフトウェアプロバイダがサプライチェーンの各企業に関係する。製品上市後、消費者の手に渡った製品については、そのユーザーやリサイクラーがエンティティとなりうる。また、規制当局の検査やリサイクル時に含有化学物質を分析する業者も本ユースケースに関係するエンティティである。

② 管理対象化学物質を含む製品例

以下の図はユースケースの説明のために単純化した電気製品 X の構成である。なお、本製品例は、chemSHERPA で用いられているものである。ここでは、管理対象物質としては、鉛と N, N-ジメチルホルムアミドを対象とする。



ダイオード、パネル、ヒューズの部品は川上企業から提供された原材料に基づき、川中企業が製造する。さらに次の川中企業はダイオード 1 個、パネル 2.2cm²、ヒューズ 3 個から構成される製品 C を製造する。製品 A、B は川中企業が製造するが、ここでは管理対象化学物質を含まないとする。川下企業はこれらの製品 A、B、C から最終セットアップを行い、電気製品 X を製造する。

このとき、ダイオードは、1 個あたり最大 96%の鉛を含む含鉛はんだを 0.05g、1 個あたり最大 23%の N, N-ジメチルホルムアミドを含む PA（ポリアミド、ナイロン樹脂）を 3.08mg 使用している。また、ヒューズは、1 個あたり最大 0.11%の N, N-ジメチルホルムアミドを含むエポキシ樹脂を 20mg 使用している。つまり、原部品については、ダイオードは鉛を 11%（原部品重量 0.4331g に対して 0.05 × 0.95 [g] の鉛）、N, N-ジメチルホルムアミドを 0.16%（原部品重量 0.4331g に対して 3.08 × 0.23 [mg] の N, N-ジメチルホルムアミド）を含み、ヒューズは N, N-ジメチルホルムアミドを 0.002%（原部品重量 0.835g に対して 20 × 0.0011 [mg]）含む。REACH 規則では、管理対象物質が部品の重量比で 0.1%を超えた場合に伝達しなければならないことになっており、この場合、ダイオードの鉛および N, N-ジメチルホルムアミドは REACH 規則における情報伝達の義務があるが、ヒューズの N, N-ジメチルホルムアミドは Not-Relevant（SVHC 規制対象外）となり、この情報の伝達は REACH 規則においては義務ではない。

③ シナリオ

本ユースケースでは、以下の4つのシナリオを対象としてサプライチェーンにおける化学物質管理の課題およびペインポイント並びに Trusted Web 技術の適用について議論する。

1. 川下企業が製品上市前に管理対象物質の使用状況を川上、川中企業に確認する場合
2. 製品上市後に規制当局が新たに管理対象物質を規定する場合
3. 製品上市後、サプライチェーンにおいて製造方法や原材料等の変更があった場合
4. 購入者・リサイクル業者から問い合わせを受けた際に、規制に適合していることや管理対象物質の内容を回答する場合

シナリオ1は製品を新しく製造・上市する際に一般的に行われている手続きである。シナリオ2および3は、製品上市後に規制または製品に含有する化学物質の含有量に変更があった場合の手続きである。シナリオ4は、製品が消費者に渡った後の手続きである。シナリオ4については現状の規制では画一的な手続きはないが、将来の循環型社会においてはより重要性を増すシナリオであると考ええる。

1. シナリオ1

本シナリオでは、川下企業が製品上市前に管理対象物質の使用状況を確認し、保存、管理、規制当局への提出を行う場合を考える。本シナリオは、現状、以下の手順により化学物質の管理を実現している。

1. 川下企業が川上、川中企業に管理対象物質のデータを要求する。
2. 川上企業が川中企業にデータを送る。
3. 川中企業が様々な川上企業から集まるデータを足し合わせて一つのユニットにして川下企業にデータを送る。
4. 川下企業が様々な川中企業から集まるデータを足し合わせて一つのユニットにして保存、管理する（規制当局に提出する）。

つまり、本シナリオでは、川下企業から川上、川中企業に管理対象物質のデータを要求し、取得する Pull 型・Request&Reply 型のモデルである。また、サプライチェーンにおける製品・部品の流れとデータの流れは原則として一致する。

前述の製品例を用いて説明すると、以下のような手順となる。

1. 電気製品 X の上市において、川下企業が製品 A、B、C を製造する川中企業に管理対象物質のデータを要求する。製品 C を製造する川中企業はこの要求を受けて、構成する部品であるダイオード、パネル、ヒューズを製造するための原材料を提供している川上企業に管理対象物質のデータを要求する。なお、川下企業が川中企業の製品設計を行っている場合は、川中企業に代わり、川下企業が川上企業に管理対象物質のデータを要求することもある。
2. ダイオード、パネル、ヒューズを製造するための原材料を提供しているそれぞれの川上企業は、含有する管理対象物質のデータを川中企業に送る。本製品例では、ダイオードは鉛を 11%（原部品重量 0.4331g に対して 0.05×0.95 [g] の鉛）、N,N-ジメチルホルムアミドを 0.16%（原部品重量 0.4331g に対して 3.08×0.23 [mg] の N,N-ジメチルホルムアミド）含むことを伝達する。ヒューズについては、N,N-ジメチルホルムアミドを 0.002%（原部品重量 0.835g に対して 20×0.0011 [mg]）含有するが、

先述のとおり、例えば REACH 規則では規制対象外であるため、この情報を川中企業に提供するかは、川上企業・川中企業間の契約等に依存する。このように、各川上企業は管理対象物質のデータを製品 C を製造する川中企業に提供する。

3. 製品 C を製造する川中企業は、製品 C はダイオード 1 個、パネル 2.2cm²、ヒューズ 3 個から構成されるため、これらを足し合わせて集計したデータを川下企業に提供する。
4. 川下企業はそれぞれの川中企業から提供されたデータを足し合わせる。本製品例では、製品 A、B は管理対象物質を含有していないため、製品 C のデータを元に最終製品 X に含まれる管理対象物質の含有量を集計し、保存、管理する。また、必要に応じて規制当局に提出する。

なお、現状、管理対象物質のデータ提供は売買契約等の契約に基づき行われており、データの信頼性も契約に基づくものである。また、chemSHERPA では、管理対象物質のデータについて、会社名、事業所名に加えて、入力者名と確認者名を記入する形になっている。

2. シナリオ 2

本シナリオでは、製品上市後に規制当局が管理対象物質を規定する場合を考える。製品上市後に新たに管理対象物質が規定された場合は、生産中であればシナリオ 1 と同様の手順で川下企業が川上、川中企業に確認する。最終製品または一部の製品・部品が生産終了後で川下企業により管理対象物質のデータを確認できない場合は、分析業者が対象の製品に含有される管理対象物質量を分析することになる。

上記製品例において、電気製品 X または製品 A、B、C、ダイオード、パネル、ヒューズ等の部品の生産終了後にここで対象としている化学物質が管理対象物質に規定された場合は、分析業者が電気製品 X を分析し、生産終了によりデータを得られない構成部品であるダイオード、パネル、ヒューズ等に含まれる化学物質量を計測する。

本シナリオもシナリオ 1 と同様に川下企業側からの要求に基づく Pull 型のモデルであり、サプライチェーンにおける製品・部品の流れとデータの流れが原則として一致する。しかし、生産終了によりデータを得られない場合は、第三者の分析業者による分析結果によりデータが作成されるため、サプライチェーンにおける製品・部品の流れとデータの流れが一致しないモデルも考えられる。

3. シナリオ 3

本シナリオでは、製品上市後、サプライチェーンにおいて製造方法や原材料等の変更により管理対象物質の含有量に変更があった場合を考える。川上企業において管理対象物質のデータに変更があった場合、そのデータを川中企業に提供し、さらにそのデータを反映したデータを川下企業に提供する。川中企業において管理対象物質のデータに変更があった場合は、そのデータを川下企業に提供する。川下企業は提供されたデータを足し合わせて一つのユニットにして保存、管理する（規制当局に提出する）。

本シナリオは、シナリオ 1 および 2 とは異なり、川下企業側からの要求に基づかない、Push 型のモデルである。また、サプライチェーンにおける製品・部品の流れとデータの流れは原則として一致する。

4. シナリオ 4

本シナリオでは、購入者・リサイクル業者から問い合わせを受けた際に、規制に適合していることや管理対象物質の内容を回答する場合を考える。欧州の REACH 規則では、SVHC が含有されている場合には、消費者から問い合わせを受けたら回答をしないといけない規則となっており、製品ごとの SVHC 含有量を登録する SCiP (Substances of Concern In articles as such or in complex objects (Products)) データベース¹⁸も整備されている。

本シナリオでは、川下企業は、消費者からの問い合わせに対して、シナリオ 1 から 3 で保存、管理されている情報に基づき、規制への適合状況や管理対象物質の内容を回答する。SCiP データベースのように中央集権的なデータベースが存在する場合は、それを参照することもある。

上記製品例について考えると、消費者から電気製品 X の SVHC 含有量について問い合わせを受けた場合には、シナリオ 1 から 3 で保存、管理した SVHC 含有量を消費者に回答する。

(3) 現状の課題と議論するペインポイント

上述した化学物質管理の現状と想定されるシナリオにおける課題と議論するペインポイントを以下のとおりまとめ、各課題・ペインポイントについて詳説する。

- 営業秘密の保持
- 開示範囲の制御
- 既存規制・新規制への対応
- 製造現場の 4M 変更への追従
- 企業・データの ID 管理
- データの信頼性の担保
- 中小企業のフォロー
- 規制当局への報告
- プロセスで使用する化学物質の管理
- 化学反応により伝達されたものから変化する化学物質の管理
- 販売後の問い合わせ対応
- 販売終了後の対応

① 営業秘密の保持

製品に含有する化学物質の情報は、各社の秘伝のノウハウや営業秘密など秘匿性が極めて高い情報も含まれる。そのため、一元化された円滑な情報伝達が困難である。例えば、サプライヤーは社名を明らかにしないのが一般的であり、サプライチェーンにおいて管理対象物質のデータを提供する場合もシナリオ 1 の川中企業の製品 C で示したように集計した形で提供している。

また、この営業秘密の保持のため、中央集権的なデータベースで各製品・部品に含有する化学物質情報を管理することには注意が必要である。

¹⁸ European Chemical Agency ウェブサイト SCiP データベース
<https://echa.europa.eu/scip>

② 開示範囲の制御

上述の営業秘密の保持と関連して、サプライチェーンにおける化学物質管理の現状では、企業間の契約がある前提となっている。シナリオ1で説明したように、chemSHERPAを用いた例でも、メールによる川上、川中企業のデータ提供依頼に応じて逐次データを送ることにより、開示範囲をコントロールしていることが多い。

また、管理対象物質のデータについては、足し合わされた形で提供しており、一次サプライヤーとは直接やりとりをするが、その先のサプライヤーについては開示されないことが一般である。そのため、一次サプライヤーより先から提供されたデータに基づき集計されたデータの信頼性については、一次サプライヤーとの契約により担保する方法に依らざるを得ない。

③ 既存規制・新規制への対応

化学物質の管理については国内外で様々な関連規制があり、またこれらの規制は定期的に変更されている。そのため、既存規制への対応に加えて、変更された新規制にも対応する必要がある。

前述のシナリオ1から3で川上企業から川中企業、川中企業から川下企業に提供される管理対象物質のデータは、法律等による規制対象であるため、売買契約等に当該データの提供が含まれ、それにより開示されている。一方で、法規制外の化学物質の開示は任意であり、必要最小限の情報だけ提供するのが通常であり、多くの場合はこれらのデータについては開示されない。また、もし開示された場合も、データを受け取り集計する側はこれらの非開示の情報を含むためデータの一貫性が担保できない。そのため、一部開示されている化学物質が新たに規制された場合にも、結局問い合わせが必要となる。つまり、現状は規制の変更への対応コストが大きくなってしまいうという課題がある。

また、既存規制、変更された新規制に対する調査対象・範囲の判断が困難であるという課題がある。調査対象・範囲が広すぎるとすべての川上、川中企業が調査対象となるなど、調査にかかるコストが高くなり、調査対象・範囲を狭めすぎると調査漏れが生じてしまう。そのため、適切な調査対象・範囲を判断するために、コンサルタントに調査を委託することもある。

さらに、個社ごとに情報管理をしているため、新規制に対応するための問い合わせにおいても、例えば chemSHERPA ではメールが使われることが多く、情報伝達に人的工数がかかってしまうという課題がある。

④ 製造現場の 4M 変更への追従

製造現場においては、4M（Man：人、Machine：機械、Method：方法、Material：材料）の変更が常に行われている。これらの 4M 変更により、管理対象物質の含有量が変わることがあるが、前述のシナリオ3のサプライチェーンにおける変更によるデータ提供が行われないことがある。この原因として、サプライヤー自身が変更を認識していないこともあり、また検知も困難である（サイレントチェンジ）ため、4M 変更による管理対象物質の変化を追従することが困難となっている。

また、初回に調査をした情報から、実際はモノとしては何も変わっていないのに、変更デー

たを流通しなければいけない局面もある。管理対象物質の追加、途中のメーカーによる設計変更、作り方の変更などにより変更情報を伝達してもらわなければいけない場合にも、川下企業から新たな問い合わせをしないと変更情報を出してくれないメーカーもあり、川下企業において過大な負担になっているという課題がある。

⑤ 企業・データの ID 管理

企業や製品・部品、化学物質の ID 管理は各企業の内部的な独自 ID（製品番号・部番等）を採用していることもあり統一的な管理方法がない。また、採用している管理ソフトウェアのソフトウェアプロバイダに依存する面もある。

企業 ID については、D-U-N-S(R) (The Data Universal Numbering System) Number¹⁹と呼ばれる R&B 社の企業コードデータベースがあるため、これを使うこともある。chemSHERPA では D-U-N-S(R) コードも使用可能となっている。しかし、各企業や管理ソフトウェアによっては別の ID 体系を採用することもあり、統一されているわけではない。

製品・部品の ID は、シナリオ 1 の手順を鑑み、川下企業が部番のデータベースを作成し、サプライヤーにその部番を示してデータを要求することが多い。サプライヤー側も独自の番号を持っており、示された部番からの変換が必要である。

化学物質の ID は標準化団体・業界団体で規制に従い策定されている。そのため、規制外・管理外の物質は ID が振られていないこともある。また、規制対象となる化学物質データは業界ごとに使用する化学物質が異なり、また法規制の変更によっても規制対象が変化するため、複数の規制リストとバージョンにより管理する必要がある。例えば、chemSHERPA では 8 つの規制に加え、自動車業界の規制リストである GADSL (Global Automotive Declarable Substance List)²⁰および電気・電子機器の規制リストである IEC 62474 (Material Declaration for Products of and for the Electrotechnical Industry)²¹を含めたデータベースを作成しており、リスト、バージョン、リスト内の化学物質 ID で管理対象物質を管理、情報提供するようになっている。

⑥ データの信頼性の担保

chemSHERPA の運用では、データの信頼性は契約または不使用証明書などの提出に依存しており、システムの・機械的に担保されているわけではない。chemSHERPA においては、データ提供者の記入者、承認者の名前を記入することになっており、記入者、承認者がサプライヤーの従業員であることが分かればそのデータは正しいと考えている。そのため、仮にデータの集計を間違えたり、改ざんがあった場合にも検証できない。なお、抜き打ち検査で検証することもある。

また、複社購入（複数の企業から同種の製品・部品を調達すること）を行っている場合もあ

¹⁹ Dun & Bradstreet ウェブサイト D-U-N-S(R) Number
<https://www.dnb.com/duns-number.html>

²⁰ Global Automotive Declarable Substance List (GADSL) ウェブサイト
<https://www.gadsl.org>

²¹ IEC 62474 – Material Declaration for Products of and for the Electrotechnical Industry
<https://std.iec.ch/iec62474>

り、部品の調達元ごとに管理対象物質を管理しきれない場合、それらの最大量を取るなどして、規制の目的を満たす最悪値判断をしている場合もある。このため、規制は満たすものの情報としては正確性に欠くという問題もある。

⑦ 中小企業のフォロー

川中企業には中小企業も多く、シナリオ1および2に従い、情報提供を依頼してもなかなか提供されないことも多い。川下企業が川中企業の製品の設計に関与している場合は、川下企業が素材も把握しているため、川下企業が川上企業の手先に情報提供を求めて、中小企業である川中企業のデータを補完する情報として使うなど、運用面でカバーしていることも多い。また、高コストなシステム導入は中小企業にとって困難なことも多く、中小企業でも容易に導入、運用できる仕組みが課題となっている。

⑧ 規制当局への報告

規制当局への報告は、各規制に制度が異なるため、報告義務（例えば、REACH 規則では年間1t以上上市した法人のみに報告義務）等に対する製品管理・基準判断ミスによる報告漏れなどが発生するおそれがある。そのため、各規制に対応した適切な製品管理・基準判断が求められる。

また、保存・保管義務（証拠の保存）のために各製品に関する情報を管理する必要がある。この管理について事業者によっては内部システムを構築して一元的に管理していることも多いと思われ、それほど負担にはなっていない可能性も考えられるが、異なる目的の法令に対応するために、規制当局への報告が求められた場合は、これらの管理された情報から適切な情報を出力して提供する必要がある。

⑨ プロセスで使用する化学物質の管理

洗剤等の製造プロセスで使用する化学物質については、製品に含有されず、規制が異なる。そのため、chemSHERPA ではこれらを対象外としている。他方、税務管理（米国の Ozone Depleting Chemicals (ODC) Excise Tax 等）や化審法対応のために製造プロセスで使用する化学物質の管理は必要とされているが、サプライチェーンや製品に紐付く形では管理はしていない。

一方で、環境負荷に関する情報を消費者に提供する目的や、バージン材・リサイクル材の区分けが必要という IEC/ISO における議論にもあるように、原材料に関する情報や製造プロセスにおいて使用される化学物質・環境負荷の管理に対する要求はある。

⑩ 化学反応により伝達されたものから変化する化学物質の管理

製造過程において、化学反応等でサプライヤーから伝達されたものと違う形に変化してしまう化学物質についても管理する必要がある。例えば、そのまま原材料に含まれる化学品の化学物質が伝達せずに、その化学品の状態が揮発してなくなってしまうたり、他の化学物質との化学変化をして別の新たな物質になったりといった変化を伴う製造過程もある。この原部品に対して化学変化を起こして固形化（変化）・揮発・残留するなどの製造過程については、人が介在したり、温度条件などで変化するため一律に計算式で計算できないことも多い。そのため、その変化・条件を想定して管理対象物質についてのデータの集計と情報伝達を行う必要がある。場合に依っては、バージョン・リビジョンやロットごとで管理する必要

もあると考えられる。

また、この製造過程は属人化することが多く、営業秘密の保持の観点からも、必要最低限の情報のみを開示することが多い。そのため、製品化するとき情報の関係性が途切れてしまい、情報の関係性を辿ることが困難である。

⑪ 販売後の問い合わせ対応

ユーザーやリサイクル業者の保護のために、販売後の製品に含有される管理対象物質についても顧客からの問い合わせへの対応が義務づけられていることがある。例えば、REACH 規則では、年間 1t 以上上市した法人のみに規制当局への報告義務があるが、この報告義務がない製品についても顧客からの SVHC 含有量についての問い合わせには対応する義務がある。

この問い合わせ対応については、標準的な回答フォーマットが規定されておらず、川下企業に委ねられている。

また、中央集権的な SCiP データベースと呼ばれる製品名に対する SVHC 含有量のデータベースがあり、これへの登録が義務づけられている場合があるが、SCiP データベースに登録する製品名は、実際に販売されている製品名とは別の識別子・名前で登録することも多く、データベースを参照してもマッチングが取れないという課題もある。これにより、この問い合わせ対応の目的のひとつである、リサイクル業者が危険物質を含む製品を認識・識別することが達成できていない。

⑫ 製造販売終了後の対応

製造販売終了後はサプライヤーとの契約も終了しており、新たな規制に対する問い合わせ等が困難である。例えば、20 年後といった場合、製造販売した企業が存在せずにトレースできないことも考えられる。この点については、管理対象物質が製品に含有され流通しているにも関わらず、それに関する情報が一緒に流通していないことが根本的な原因のひとつであると考えられる。

(4) 効果を期待できるポイント

目的を達成するにはデータの信頼性が重要である。現状のワークフローでは、契約により一定のデータの信頼性を確保している（債務不履行や不法行為による損害賠償請求権などによりデータの改ざんをけん制している）が、ミスや 4M 変更による報告漏れなどが発生しうる状況となっている。一方で、すべての情報を開示することは、製造方法や調達情報等の営業秘密の保持の観点から許容できない。

そこで、「営業秘密の保持」や「開示範囲の制御」を実現しながら、「データの信頼性」を担保出来る仕組みが実現できれば、このような 4M 変更への追従や規制当局への報告、さらには販売後の問い合わせ対応、販売終了後の対応も実現可能となりうる。

現在は多くの過程で人手による作業が発生しているが、これらが実現できることで機械的に対応できる範囲が増えると考えられる。これにより、化学物質管理の工程を迅速に行うことができ、新規制への対応のみに留まらず、迅速性を活かした調達先の検討やサプライチェーンにおけるリスク管理等にも有用となりうると考えられる。

(5) 本ユースケースにおける特異な点

- 営業秘密を取り扱うため、開示内容・開示範囲の制御が必要である点
 - ② データの中身だけでなく、流通過程（サプライヤー情報など）も秘匿する必要がある
- データの信頼性を担保するために検証可能である点
 - ② データの流通過程を秘匿しながら、検証のための情報（信頼）を伝搬する必要がある

(6) 要求事項

上記課題やペインポイントを解決すべく、本ユースケースに求められる要求事項をまとめる。

① データ加工・開示・流通・通信に対する要求

1. 営業秘密の保持と開示範囲の制御

- 各社のデータの秘匿性を保ちつつ、適切な条件で迅速に情報を流通させる仕組み
- 事前にできる限りの化学物質を管理しておき、規制が変更された場合に必要な情報を動的に開示・取得できる仕組み（規制当局からの規制をベースとしていれば自動で開示する）
 - ② 中央集権的だと出さないが各社管理しているという状況だと協力してもらえるのか？→ 法律で規定された場合は対応するしかない。
 - ② 規制前から管理するインセンティブは？ → 原材料メーカーであればそもそも管理はしている（品質管理）。どこまで出すかの問題。
- 会社対会社の場合、会社と従業員の関係を明確にし、開示範囲を詳細に制御可能にする仕組み
- コンサルタントのような第三者から情報の開示を受ける場合は、コンサルタントが集めたサプライヤーからの情報を他の川下企業に流すときに正しく同意を取る仕組み

2. データの信頼性の担保

- 会社と従業員の関係を明確にし、記入者、承認者など、データの提供者情報の信頼性を検証可能にする仕組み
- コンサルタントのようなサプライチェーンに直接関与しない第三者からデータ提供を受ける場合、現状では規制に関する責任は川下企業が取るとなっているため、そのデータの信頼性を担保・検証をする仕組み（現状売買契約が前提となっているため、このような仕組みがあると、サプライヤーの新規開拓が容易になる可能性がある。）
- 自己適合宣言に対してエビデンスを規制当局に（必要に応じて）動的に提出（IEC 63000）するなど、信頼性の担保と開示範囲の制御をする仕組み
 - ② 現状、規制当局の判断には、複合的なエビデンス（分析（次のロットで同じとは限らない）、chemSHERPA 情報、売買契約など）が用いられている。
 - ② UAE・サウジアラビア・ロシア（今後）など、自己適合宣言の書類を事前に出して許可番号を事前に取り必要のある国・地域もある。
 - ② 提出したものと確認・審査したことを分離できるとよい（トレース機能？）

3. プロセスで使用される化学物質

- 営業秘密を保護する仕組み
 - ② 含有量 0 も営業秘密にあたる可能性がある。
- 使用していないことの証明をする仕組み
- プロセスのみで使用して、製品に残っていないことを証明する仕組み

4. 化学反応により伝達されたものから変化する化学物質

- 消えてしまう情報を流通・検証する仕組み
 - ② 含有される化学物質以外で注目を浴びているのは CO₂ (Net 0 を目指す社会) であり、これが価値となる可能性があるため、これに対応できると社会的影響が大きいと考えられる。例えば、使った電気 (RE100) などの記録がある。
- 地政学的に偏在している Critical Raw Material (CRM、レアメタル) の情報があるとサプライチェーンリスクの評価などにも応用可能である (例: コバルト@コンゴ 8 割)。

② 規制・工程変更等に対する要求

1. 既存規制・新規制への対応

- 規制 (管理対象物質) の一覧・データベースが必要
- Global で統一された化学物質リスト (自動車は GADSL、電気電子では IEC 62474) が必要
 - ② 現状は、規制から業界標準・国際標準が絞り込みを行い、各社がリストを作成している。
 - ② 部品メーカーは電気電子にも自動車にも提供しているので、広い管理対象物質リストを作っている (規制、業界標準を見比べて作っている)。
 - ② RoHS では鉛、鉛化合物が規制対象であるが、chemSHERPA では鉛化合物をリスト化・定義し、鉛化合物の分子式から鉛の量 (規制対象) を計算している。ただし、このリストから通常使用されないような鉛化合物が漏れる可能性はある。
 - ② 無機物・有機物ともに化合物で指定されている場合もある。特に、有機物で指定されている場合 (e. g., フタル酸エステル) は化学変化する可能性が高いため、そのデータ化が困難である。
- 規制変更に従うための通知の仕組み
 - ② 規制が緩和されることはまずないため、規制強化への対応が必要である。
 - ② 規制の時期によっては対象が変わるため、バージョン管理が必要である。

2. 製造現場の 4M 変更への追従

- 管理ガイドラインを策定するなど、管理プロセスを正常に動かす仕組み
 - ② 生産工程を変えたとき (例えばラインを変えたときに鉛が混入するなど) の確認
 - ② サプライヤー監査
- 新たな化学物質であったり、生産工程の変更に対して手軽に (知識をあまり持たないでも使え、営業秘密が守られる) 規制と見比べる仕組み
 - ② これがあると、中小企業でも Push 型で通知できると考えられる。
 - ② なお、現状でも 1 年に 1 回変更がないかをサプライヤーに確認している企業もある。

③ データ管理・検証への要求

1. 規制当局への報告

- 信頼性/自己適合宣言の例と同じくエビデンスを取れる状態・トレース出来る状態にする仕組み

2. 製造販売終了後の対応

- データの保存・保管をする仕組み
- （会社がなくなるときなど）データを委譲する仕組み

3. 販売後の問い合わせ対応

- ユーザー、リサイクル業者まで考えたデータの流通・検証の仕組み

④ アーキテクチャ・プラットフォームへの要求

- 企業・データの ID 管理
- 営業秘密の保持・開示範囲の制御
- プラットフォーム上に乗る他のシステムとの関連性
 - ② プラットフォームの管理者・コスト構造
 - ② プラットフォーム上のシステムの管理者
- 中小企業のフォロー（UI/UX、導入コストを含む）

(7) Trusted Web 技術の適用

① 方針

上述の課題・ペインポイントを解決し、要求事項を満たすためには、現在の Trusted Web 技術では議論が不足しているものもある。一方で、Trusted Web の 4 つの機能として挙げられた Identifier 管理機能、Trustable Communication 機能、Dynamic Consent 機能、Trace 機能については、本ユースケースにおいても核となりうる重要な機能である。これらの機能をより具体的に議論するために、ここでは本ユースケースにおける Identifier の目的と Trustable Communication、Dynamic Consent および Trace 機能が関係するシーンをそれぞれまとめる。

② Identifier の目的

現在 chemSHERPA 等で使用されている Identifier とその目的等をまとめる。

- 製品・部品（階層構造（含まれる部品リスト）あり）
 - ② 製品番号（製造側）
 - ◇ 目的：製品を特定するため
 - ② 部番（受け取る側）
 - ◇ 目的：物を特定するため
- 材料（部品の中に含まれる材料）
 - ② 材料リストのバージョン

- ② 材料番号（国際的に unique なものはない。chemSHERPA や IMDS（自動車）などで独自採番）
- ② マテリアルクラス（材料のカテゴリ）
 - ◇ 化学物質と同じ
- 化学物質（材料に含まれる化学物質）
 - ② リストのバージョン
 - ◇ 目的：いつの法規制（EU リーチ・化審法など）に対応するか特定するため
 - ② 化学物質そのものの番号（通常は CAS 番号）
 - ◇ 目的：含有する化学物質を特定するため
 - ② 化学物質の物質群
 - ◇ RoHS では規制が鉛および「化合物」となっているので群として扱う。例えば、クロム酸鉛だと 1:n（六価クロム・鉛の両方のカテゴリ）。
- 国・地域（ISO の国・地域コードを使っている）
 - ② 生産国・地域
 - ◇ 目的：あまりない？
 - ② 上市の際
 - ◇ 目的：法規制との照合のため
- 事業者
 - ② 会社名
 - ◇ 目的：企業間の関係（契約等）、供給者を特定するため
 - ② 事業所
 - ◇ 目的：作っている場所を特定するため（別の場所で作る場合は、chemSHERPA データ取り直し）
 - ② データ入力者
 - ◇ 目的：入力者を特定するため
 - ② データ確認者
 - ◇ 目的：確認者を特定するため
- 契約
 - ② 目的：契約内容を照会するため
- データ
 - ② シート（製品・材料・化学物質の ID は上記）
 - ◇ 目的：バージョン管理
 - ◇ 目的：誰にいつどのシートを渡したか管理するため
- 法律の Exemption（適用除外）：条件の定義
 - ② 用途
 - ◇ 回避する技術がない（エッセンシャルユース）場合は除外規定ができる
 - 例）医療機器 → 最終製品カテゴリに ID がつく
 - 例）高温はんだ → 高温はんだ（材料）に ID がつく（はんだ自体が材料。化学物質は鉛・すず → 高温はんだなら鉛 OK by RoHS）
 - ◇ 研究開発用途（リストなし・ID は付与されない）
 - ◇ その他
 - 例）子供の玩具は規制の閾値が厳しいが、サーバ製品ではそれよりも緩いなど → 最終製品
 - ② 期限
 - ◇ 技術の進歩等を想定して適用除外の期限も定められているので期限も管理する必要がある
 - 期限：上市の段階
 - 期限は延長される場合がある

- ② そのまま延長される場合は同じ ID
- ② さらに細分化して一部だけ延長するとなると ID 振り直し

③ Trustable Communication が求められるシーン

- サプライヤーから提出されたデータが正しいかを判断する
 - ② データの正しさを示す根拠が紐付いていると良い
 - ◇ 現状は契約で縛っている
 - ◇ 現状は、過去にもらったデータと見比べて遜色がないのか見ている
- 自社が提出したデータがどこに改ざんされずに流通していることを担保したい
- 部品が最川下のどこに行ったのかを知りたい（トレース機能も関係するが、Communication のモデルとしても検討が必要である。）
 - ② 自動車メーカーに行くのであれば自動車の規制に合った情報を出せるのにわからないと出せない
- 将来は情報を追えるようにした方がいい（ref. 営業秘密・機密）
 - ② どこから流れてきたか
 - ② どこへ流れていったか w
- 部品の階層構造・調達情報・商流などを追えないようにしたい（ref. 営業秘密・機密）
- 時間的な制約と「トラスト」の関係を記述する
 - ② 生産確認判断（開発後、生産するまでに行う必要がある）がスケジュール的な区切り

④ Dynamic Consent が活かせるシーン

- 新しく規制対象の化学物質が規定された場合に速やかに流通する機能（規制をトリガーとした合意形成）
 - ② Full declaration → 情報を出す
- サプライヤーが変わったときに速やかに情報が更新される
 - ② 契約上は変更通知書を受け取っているが時間がかかる
 - ② サイレントチェンジがあるのでは？
- サプライチェーンの動きが常に分かると管理上うれしい
- 生産終了・廃業時にデータをどこかに残して、動的に問い合わせできる状態だと生産後の対応ができる
 - ② Full declaration → 情報を出す
- 自己適合宣言に対してエビデンスを当局に提出する

⑤ Trace 機能が必要とされるシーン

- Dynamic Consent でデータが流通した先をトレース・監査
- データ自体の流通をトレース（営業秘密とのトレードオフあり）
- 過去の規制・状態との照合 → Trusted Web を設計する上で必要
 - ② （最近はないけれど過去にはあったかもしれない）
 - ② Smart Contract は例えば 1 年前の条件（スナップショット）でどういう動きをするのか検証するのが結構大変
 - ② ブロックチェーンの場合は、スナップショットを取り出せない

- 10 年前に出荷した機械 (=10 年前の規制でチェック・情報を保存) に対して、保守パーツが最新の規制で保存しないといけないことがある→トレースとログとスナップショット？
- データの作られた時間・位置

⑥ Trusted Web 技術の適用における検討事項

- 中小企業のフォロー (UI/UX、導入コストを含む)
- 情報伝達が切れてしまった場合にもトラストがつながるようにする
- システムやツールを作ったときのコスト負担 (永遠の課題)
サプライチェーンはグローバルなのでより難しい
- ② データを使う側：川下
- ② スペック：川上・川中

⑦ Trusted Web 機能との関係

上記で本ユースケースにおける Identifier の意味と Trustable Communication、Dynamic Consent および Trace 機能が関係するシーンをまとめた。このように、Trusted Web との機能により、サプライチェーンにおける化学物質管理において、データの流通を促進し、信頼性を担保することが可能になると考えられる。

一方で、本ユースケースの核となる特異な点は、営業秘密の保持や開示範囲の制御を実現しながら信頼性を担保するという点である。この実現には現在議論されている Trusted Web の機能だけでは不十分であると考えられ、その実現のためにアーキテクチャと実装技術、運用技術についてより深く議論および検討をする必要がある。

本ユースケースに対して Trusted Web 技術に求められる技術については、次章にて議論する。

(8) 議論

上記の効果を期待できる点、本ユースケースにおける特異な点および要求事項でまとめたとおり、サプライチェーンにおける化学物質管理において、営業秘密の保持や開示範囲の選択といった情報を保護する仕組みが必要とされる一方で、川上企業から川中、川下企業、ユーザーやリサイクラー、規制当局へとデータが流通する中でデータの信頼性を担保する仕組みも必要となる。ここでは、これらの点に着目して Trusted Web 技術との関係について議論する。

まず、Trusted Web における信頼の担保は、データの流通等を記録することで検証可能にすることを前提としているが、本ユースケースでは、営業秘密の保持の観点から、データ自体の関連性を直接記録したり、データの提供者や発行者、検証者等のエンティティを直接記録し、開示することは好ましくない。そのため、データの流通を単純に記録することで検証可能とする技術は適用できない。このことは個人情報の選択的開示に近い部分もあるが、データの提供者や発行者、検証者等のエンティティも秘匿する必要があるなどと言った点で、選択的開示よりも紐付けられる情報が限定されることが考えられる。

これを実現するためには、データ自体は連鎖させずに、信頼（トラスト）にあたる部分のみ連鎖させ、生データは流通しなくても Trustable な状態を提供・流通する仕組みが必要とされる。また、この Trustable な状態を生データに依らず検証する仕組みも必要である。これには、証憑（エビデンス）に基づくものであることを記録する一方で、その証憑自体は開示しない仕組みが必要となる。

一方で、開示範囲の選択においては、データ自体の連鎖が途切れることで、川上企業にとってデータ開示の根拠が不明瞭となり、例えば、川下企業が自動車業界であり、規制に対応するために必要な情報であるということであれば川中企業を通じて情報を提供できるにもかかわらず、川中企業によりデータの連鎖が途切れるため、開示できないというようなことも発生しうる。そのため、川上企業の提供するデータの中に動的な合意形成のために必要な情報を埋め込むことで、川中企業には開示せずに、川上企業と川下企業の間で情報提供の仕組みがあると良いと考える。これを実現するには、川中企業にはデータを開示せずに川上企業からのデータを集計できる秘密計算などの技術のほかに、川下企業に提供される動的な合意形成のために必要な情報から川上企業を特定できないようにするなど、川中企業の営業秘密を保護する技術などが必要となる。

また、開示したデータについて、データを作成した人・会社がデータの流通後にも管理できる仕組みがあることが好ましい。これは、データの流通後に流通先を辿ることは、川中・川下企業の営業秘密の保持のため困難であると考えられる。一方で、データの流通先で合意された目的にのみ利用されていることを確認でき、合意された目的外での利用に関してはデータの削除や流通を停止するような監査の仕組みも必要となってくると考えられる。特に、企業活動においては、ノウハウやその他の営業秘密の漏洩は企業活動を継続できなくなるほどの大きな損失を生じる可能性がある。そのため、このような監査の仕組みや高度なセキュリティを担保する仕組みも基盤として求められる。

特に、法規制以上のデータの開示については、川下企業の調達仕様書などにより、その根拠が示されることもあるが、データの開示がこのような根拠に基づき動的な合意形成により実現でき、データの開示側にそのデータの制御ができれば、データのオープン化により、サプライヤー側の技術力のアピールの機会増大や、調達側の迅速性を活かした調達先の検討やサプライチェーンにおけるリスク管理等にも有用となりうると考えられる。

上記のように本ユースケースへの Trusted Web 技術の適用においては、信頼性を担保するだけでなく、営業秘密の保持や開示範囲の制御も必要である。これを分散型のアーキテクチャである Trusted Web で実現するためには、分散型を前提とした社会の仕組みも検討する必要があると考えられる。一方で、ワークフローが異なると使えなくなるようなものは基盤たりえないので、Trusted Web には様々なワークフローやアプリケーションに対応するための柔軟性・拡張性を担保したエコシステムづくりも必要であると考ええる。

(9) まとめ

本ユースケースでは、各国・地域における製品に含有される有害性の高い物質等の化学物質の製造・輸入や使用等に関する法規制への対応のために、サプライチェーンにおける化学物質の含有量の管理についての4つのシナリオと課題およびペインポイント、要求事項、Trusted Web 技術の適用可能性を議論した。本ユースケースでは、特異な点として、データの内容や流通・通信についての信頼性の担保が必要とされる一方で、データ自体に含まれる営業秘密の保持やデータの開示範囲の制御が非常に重要である点が挙げられた。これらの実現のためには、データを単純に関連付けずに検証する仕組みが必要とされる。一部は情報の選択的開示に近い概念ではあるが、8章で議論したように、データの持ち主や生成者、検証者などといった情報ですら秘匿すべ

き情報であり、これを実現する基盤を設計するには、アーキテクチャや実装技術、運用技術についての議論と推敲が必要であると考えられる。

本ユースケースは、複雑な事例を扱っているものの、基盤技術として必要な要件を深く議論できたと考える。よって、今後は、本ユースケースを含め、その他のユースケースからの要件や課題等を議論しながら、Trusted Web の 4 つの機能の抽象化および実装技術・運用技術の検討が必要であると考ええる。

付録 D. シーケンス図
(1 / 4)



