CPSEC-WP-2019001

サプライチェーンにおける信頼構築に向けて
－ 第 1 報　信頼を損なう事故事例の分析と信頼構築の基本的考え方 －

2019 年 10 月

国立研究開発法人産業技術総合研究所
サイバーフィジカルセキュリティ研究センター

[概要]製品・サービスのためのサプライチェーンにおいて、製品・サービスに対する信頼を損なうような事故事例（セキュリティ事故を含む）が発生している。いくつかの事故事例を紹介し、その原因を分析する。原因分析すると、これらの事例では、事故は製造から運用までのライフサイクル全般に渡っており、事故の発生原因はライフサイクルの各段階で守るべき業務規程の不備と違反の2つに大別されることがわかる。サプライチェーンに参加する各企業が業務規程の不備と違反を防止して事故を減らすことが、サプライチェーン全体の信頼を構築することになる。サプライチェーンがサイバーフィジカル空間に大きくシフトする現在、サイバーフィジカル空間の利点を駆使して、信頼を構築する機会が到来している。

1.　はじめに

私たちの日常生活は、他者が作った商品やサービスを使わずには成り立たない。それらの商品やサービスを私たちは対価を払って購入する。その対価は、商品やサービスへの期待の表現でもある。すなわち、大きな対価を支払うことは、大きな期待の表れである。しかし、対価が小さくても、商品やサービスが備えるべき条件がないわけではない。例えば、いくら安い食品であっても、私たちの健康を害するものではないことは暗黙の了解があるであろう。暗黙の信頼関係を前提にして、私たちの消費生活は成り立っている、と信じて来た。しかし、もはやそうした暗黙の信頼関係は存在しないことを示すような事例が、最近発生している。

こうした変化の背景には、サプライチェーンの複雑化とグローバル化がある。取引に関与する企業や人の数が増えた分、信頼及び信頼を支える責任に対する考え方のばらつきが大きくなる。納品された製品が要求仕様を完全に満たし信頼に足るかは、受入れ期間にわかるものとそうでないものがある。わからない部分は信頼したこととして製品を使うしかないが、そうした根拠を欠く信頼の蓄積が信頼を崩す結果になっているのであろう。また、サプライチェーンにおける情報の交換のかなりの部分がサイバー空間に移行しているので、サイバー空間で情報の改ざんや漏洩があっても、サプライチェーンの信頼は損なわれる。サイバー空間を構成する IT 機器を狙った攻撃方法の増加・多様化によって、アタックサーフェス（攻撃の標的となり得る対象の全体）も増大し、サプライチェーンにおける信頼が損なわれる機会も増大している。発生する事故や問題は、企業統治のあり方が透明性を重視するようになったことで、より顕在化している面もあろう。しかし、このように

揺らいでいる信頼を再構築していかない限り、サイバー空間と現実の物理空間が融合するサイバーフィジカル空間の上に構築されたサプライチェーンは成立し得ない。信頼の再構築を考えるためには、先ず問題分析が必要である。問題となる事例を、IT に関するものから、いくつか見てみよう。

2. 事故事例と分析

サーバマザーボードへの攻撃用チップ組込み報道[1]

事例概要:

時期	2018 年 10 月
場所	米国（事件発生）
業種/分野	IT
損なわれた信頼	製品による秘密情報保持

ある報道機関が、ある国が米国企業 30 社のサーバコンピュータを改ざんしたと発表した。本発表によれば、世界最大級のサーバマザーボードのサプライヤが当該国の請負業者に製造委託したマザーボードに、当該国軍関係者によって超小型の攻撃用チップが製造工程で組み込まれた。その結果、運用中の OS にバックドアが開けられ、秘密情報が漏洩したとされる。サーバコンピュータを改ざんされたとされる企業のうち 2 社は、この報道を否定した。

事例分析:

プロセス	製造
規程に	違反

この事例は、製品の改変がなされた事例である。攻撃用チップの埋込みは、規程から逸脱し、規程の及ばない力によって故意になされたものだから、製造企業内で防ぎようがない。当該サーバコンピュータを購入した組織は、購入した製品が自組織の秘密情報を流出するとは想定しないであろう。そうした前提が成立しないことを示す事例である。購入組織がこの事件の発生を未然に防止するには、使用前に個々の購入製品の筐体を開けて、攻撃用チップが埋め込まれていないことを確認しなければならかったのだろうか。そうではなく、製品製造企業が、製品を安心して使ってもらうために製品に問題ないことを示すべきである。また、仮にこの報道が事実でなかったとしても、サーバコンピュータ製造企業の信頼は大きく傷つけられたであろう。企業は、信頼に対する疑義に対しても対抗できることが望ましい。

ルータへのバックドアツールの追加疑惑[2]

事例概要:

時期	2015 年 4 月
場所	世界の数ヶ国（事件発生の可能性）
業種/分野	IT
損なわれた信頼	製品による秘密情報保持

ある国家機関の元職員が、その著作を通じて、当該国家機関によるネットワーク機器に対する改ざん疑惑を告発した。それによれば、当該国家機関は、国外に輸出されるルータを配送ルートから入手し、バックドアを埋め込み、再梱包して配送ルートに戻していた。その結果、それらネットワーク機器が処理する通信トラフィックが傍受され、当該国家機関に情報が漏洩したとされる。ネットワーク機器を製造した企業は、「政府と協力して自社製品を意図的に脆弱にすることはない」とコメントした。

事例分析:

プロセス	流通
規程に	不備

この事例も、製品の改変である。サプライチェーンは、参加する製造企業だけでなく流通経路も信頼できるものでないと、全体の信頼は存在しない。すなわち、流通経路も含めたサプライチェーン全体が信頼できるかが問われる。流通経路の出荷から入荷までの間に製品が開梱されていないことを確認するための仕組みは存在するが、この事例ではそうした対策が不十分だったのだろう。

WannaCry によるチップ製造ライン停止[3]

事例概要:

時期	2018 年 8 月
場所	アジア
業種/分野	半導体製造
損なわれた信頼	企業の情報セキュリティ対策

世界最大手の企業が、複数の工場がランサムウェア"WannaCry"に感染し、コンピュータシステムと製造設備に影響があったと発表した。具体的には、マルウェアに汚染されたツールソフトウェアをウィルスチェックしないでインストールしたことから、社内ネットワークに接続された 1 万台以上の Windows PC に被害が拡大した。マルウェア感染が最終的な問題ではあるが、根本的な発生原因はサプライヤの作業誤りだった。2018 年第 3 四半期の売上高は、出荷遅延や対策費用により、約 3%減少すると推定されている。

事例分析:

プロセス	製造
規程に	違反

この事例では、業務の継続性が阻害されている。企業の内部問題でしかないように見えるが、間接的には、納期遅れなどによって、製品購入企業の活動が遅延するなどの被害が発生しているかも知れない。もし同様の事故が多発すれば、社会全体の生産性は低下する。そのような状況になった場合には、製品自体の信頼でなく、取引先企業のプロセスの信頼が今まで以上に問われることになるであろう。

信頼はセキュリティの重要な概念として取り扱われて来た。しかし、信頼はセキュリティの実現だ

けで達成されるものではない。サプライチェーンにおいては、セキュリティだけではなく、いろいろな意味での信頼が損なわれる事例が報告されている。次に、安全性が関係する分野での信頼に関わる事例を見てみよう。

新幹線車両台車枠の仕様外製品の納入[4]

事例概要:

時期	2018 年 2 月
場所	日本
業種/分野	車両製造
損なわれた信頼	仕様準拠による製品の安全

N700 系新幹線車両台車枠に関して、製造における不備によってき裂が発生したと、当該台車枠を製造した企業が発表した。具体的には、台車枠部材の製造工程で、作業指導票の規定が徹底されず、溶接施工を含めた何らかの原因によって生じた割れが存在し、それを起点にき裂に至ったと推定されている。発生原因としては、作業指示文書が粗いこと、その補完作業に対する指導や教育が現場作業者に任され、その実施・確認を追跡する記録がなかったことが挙げられている。また、き裂が発生した箇所の板厚確認は品質管理項目にも検査項目にも含まれていなかった。再発防止策として、図面指示通りでない製品が出荷されない仕組みの確立、工程内のプロセス確認、作業指導票を含めた書類監査、作業者の教育内容を刷新が挙げられている。

事例分析:

プロセス	製造
規程に	不備

この事例では、規程の不備を現場の判断で補おうとしたが、妥当に判断できなかったことが問題の本質である。現場の判断の質は、その現場に依存する。そのような依存性を解消するために業務規程は存在しているのに、業務規程の存在する意味を否定する結果になっている。

産業用ゴム製品の検査不正[5]

事例概要:

時期	2017 年 3 月
場所	日本
業種/分野	産業用部品製造
損なわれた信頼	基準に則った検査実施、製品の仕様準拠による安全

産業用ゴム製品(タンカーなどの輸送配管の弁を受ける弁座(シートリング))の検査で、本来、当該企業と納入先の間で 5 個につき 1 個の抜取り検査(寸法計測、硬度測定)をすることが取り決めになっていたにも関わらず、10 個または 20 個に 1 個しか抜取り検査が実施されていなかった。企業の報道発表によると、検査員の個人的怠慢、不正を行なってはならないという規範意識の鈍磨、管理・監督の不徹底、監視し辛い検査環境などが問題だったとしている。これに対して再発防止

策も提示されており、意識向上や企業風土の改善だけでなく、可能な限りの自動化、ビデオ監視カメラの導入にも言及しており、人間系の対策だけでなく、技術的な対策が含まれている。

事例分析:

プロセス	試験
規程に	違反

この事例では、規程は、存在しているが、個人的な怠慢が原因で正しく実行されていない。個人の規範意識のばらつきを抑えることが、企業の責任であり、製品ひいては企業の信頼を高めることになる。従業員の規範意識を高めるには管理・監督の徹底が必要だが、人間の力だけに頼ることには限界がある。

ディーゼル車排気ガス不正[6]

事例概要:

時期	2015 年 9 月
場所	ドイツ
業種/分野	自動車製造
損なわれた信頼	製品の環境基準への適合、基準に則った検査実施

米国環境保護庁(EPA)は、ドイツの自動車メーカーに対して大気汚染防止法違反を通告し、同社が EPA 排出基準を回避するソフトウェアを車両にインストールしたことを明らかにした。これを受けて当該自動車メーカーは 4 日後、ディーゼルエンジンのソフトウェアの排気ガスベンチテスト結果と実際の道路上使用時の測定値との大きな相違を解明中であり、世界で 1,100 万台がこの問題に関係することを発表した。その後カリフォルニア州は、当該自動車メーカーが車両に不正なソフトウェアを搭載し、検査中なのか実際の道路を走行しているかを見分けて、検査中にのみ排気ガス規制を満たす不正操作が行われたこと、この不正によって排出基準で許容されるよりも最大 40 倍多くの汚染物質を排出していたことを突き止めた。

事例分析:

プロセス	設計・製造・試験
規程に	違反

この事例は、法的規制を逸脱するための不正機能を、製造者自身が設計して製品に搭載した事例である。規制当局は、本事例のような複雑かつ巧妙な規制逃れの試みを完全に取り締まることは技術的に困難である。なぜなら、製品・サービスの設計から運用までの全ライフサイクルに渡って、規制当局や消費者が規制順守の完全性を監視することが必要になり、現実的ではないからである。

製造業は、衣食住などのわれわれの日常生活とも密接に関わっており、一般消費者も巻き込むような問題に発展する可能性もある。そうした事例をいくつか見てみよう。

「ハラール認証製品」のハラール不適合問題[7]

事例概要:

時期	2000 年 9 月
場所	インドネシア
業種/分野	食品製造
損なわれた信頼	食品の宗教戒律への適合

日本の食品会社がインドネシアのハラール認証更新時に、豚由来の酵素を調味料の製造過程で使っているとの指摘を受けた。食品会社は、調味料の主原料及び副原料にはハラール違反になるような物質は一切使用しておらず、豚由来の酵素は製造に使用される発酵菌の保存用培地の一部として使用され、製造過程における触媒と位置付けている。なお、当該酵素は、外部から調達した製品である。インドネシア食品医薬局も最終製品には豚由来の物質は含まれていないとの声明を発表したが、ハラール委員会が当該物質はハラール上不適切と判断したため、食品医薬局から製品の回収指示が出て、食品会社は従った。その年の 11 月に豆を原料とする酵素に切り替え、ハラール委員会から問題ないとの見解を受けた。

事例分析:

プロセス	設計
規程に	不備

この事例では、規程が網羅性を欠いていたのだろう。企業のグローバル化においては、市場国の文化・価値観に適応しなければならず、自国での企業活動では想定し得ない問題が潜在している場合もある。現代では、消費者に製品やサービスを提供する企業は、より複雑で長くなったサプライチェーンの末端に位置し、サプライチェーンの中で提供された全ての原材料や部品に由来する事故の一次的な責任を取ることになるリスクを抱えている。上記事例では、道義的な責任は問われなかったかも知れないが、製品回収で事業上の責任を取った。そうした影響を未然に防ぐには、食品会社のハラール認証時の査察と同様の厳格な現場視察を、酵素の仕入れ先企業に対してもしておくべきだったのであろう。

航空機副操縦士の乗務前過剰飲酒[8], [9]

事例概要:

時期	2018 年 11、2003 年 8 月
場所	英国、日本
業種/分野	旅客輸送
損なわれた信頼	旅客の安全

乗務前の副操縦士が、乗務 50 分前の呼気検査で現地基準の 9 倍超のアルコールが検出されたことによって逮捕され、禁錮 10 カ月の実刑判決を言い渡され、翌日懲戒解雇された。副操縦士は、逮捕前、社内の呼気検査を不正にすり抜けていた。共に乗務予定だった機長 2 人からは距離をとっていたため、機長らは見過ごしたとみられる。航空会社は、事故の半年前、海外の空港で新型

の呼気アルコール感知器を導入すると発表していた。
同様の事件が国内の路線高速バスでも起きている。バス運転手は深夜から翌朝未明にかけて飲酒してから就寝し、午前 7 時頃、補助運行管理者から点呼を受けた。補助運行管理者は二日酔いかもしれないと思いながらも、交替運転手の手配が面倒でそのまま乗務させた。警察は、会社の責任を問い、会社を送検した。
事例分析:

プロセス	運用
規程に	違反

いずれの場合も、安全に旅客を輸送するための規程は存在し、当日の乗務員の状態が任務に支障がないことの確認も実施されている。副操縦士・運転手らの、責任意識の欠如、精神的な弱さが、企業が設けた確認の仕組みをなきものにしてしまっている。破ろうと思えば破れるような規程もあり、その場合、破るか破らないかは個人に依存する。対外的な信頼を得るためには、企業は、穴がないだけでなく、穴をこじ開けられないような規程や仕組みを作らなければならない。しかし、それは人間系だけでの解決は難しい。

コンピュータ制御交通システムの逆走[10]
事例概要:

時期	2019 年 6 月
場所	日本
業種/分野	旅客輸送
損なわれた信頼	安全な運行

コンピュータ制御の無人自動運転車両が逆走し車止めに衝突して、14 人が重軽傷を負う事故が起きた。運営会社が発表した事故原因は断線だった。100 本超の回路の 1 本が断線した結果、進行方向の切替え指示が全体に伝わらず、逆走した可能性がある。断線を感知できる仕組みはなく、異常時に列車を停止する装置は断線で作動しなかったとみられ、運営会社はシステム上の欠陥と認めた。車両制御の専門家は、「断線を検知するすべは、必ず用意しておくべきだった」としている。
事例分析:

プロセス	設計
規程に	不備

この事件は、断線検知機能を組み込まなかった設計不備の問題である。事故の責任はシステムを保有する運営会社にあるのだろうが、システムを設計し構築した企業にも責任の一端はあるであろう。この事例も、サプライチェーンの信頼の問題である。既に述べたように、サプライチェーンを経て届けられる製品やサービスの一次的な責任はサプライチェーンの末端にある企業が負うことになる。よって、この事例の場合も末端の運営会社が事故の責任を負う形になっている。

3.　分析のまとめ

以上の事例から、信頼を損なう原因は、製品・システム・サービスのライフサイクルの中の種々のプロセスで発生していることがわかる。事例をプロセス毎に整理すると、以下のようになる。

<table>
<tr><td colspan="2"></td><td colspan="2">事例</td></tr>
<tr><td rowspan="5">プロセス</td><td>設計</td><td>ハラール不適合問題、コンピュータ制御交通システムの逆走</td><td rowspan="3">ディーゼル車排気ガス不正</td></tr>
<tr><td>製造</td><td>サーバマザーボードへの攻撃用チップ組込み、チップ製造ライン停止、新幹線車両台車枠の仕様外製品の納入</td></tr>
<tr><td>試験</td><td>産業用ゴム製品の検査不正</td></tr>
<tr><td>（流通）</td><td colspan="2">ルータへのバックドアツールの追加疑惑</td></tr>
<tr><td>運用</td><td colspan="2">乗務前過剰飲酒</td></tr>
</table>

また、当該プロセスを実行するための規程が企業には存在しているが、規程の不備・違反のどちらに起因しているかに、信頼構築のための方策は依存するであろう。事例をこの観点で整理すると、以下のようになる。

<table>
<tr><td colspan="2"></td><td>事例</td></tr>
<tr><td rowspan="2">規程</td><td>不備</td><td>ルータへのバックドアツールの追加疑惑*、新幹線車両台車枠の仕様外製品の納入、ハラール不適合問題、コンピュータ制御交通システムの逆走</td></tr>
<tr><td>違反</td><td>サーバマザーボードへの攻撃用チップ組込み*、チップ製造ライン停止、産業用ゴム製品の検査不正、ディーゼル車排気ガス不正、乗務前過剰飲酒</td></tr>
</table>

なお、上の表で＊を付けたものは、攻撃によるものである。攻撃は攻撃された組織の信頼を損なわせる場合もある。

事例を見てわかるとおり、信頼を損なう原因を作り込むプロセスと問題が発生するプロセスは必ずしも同じではない。また、原因を作り込んだ企業で問題が発生するとは限らない。例えば、コンピュータ制御交通システムの逆走では、交通システムを開発した企業における設計不備が、交通システムを運営する企業での事故として現れている。

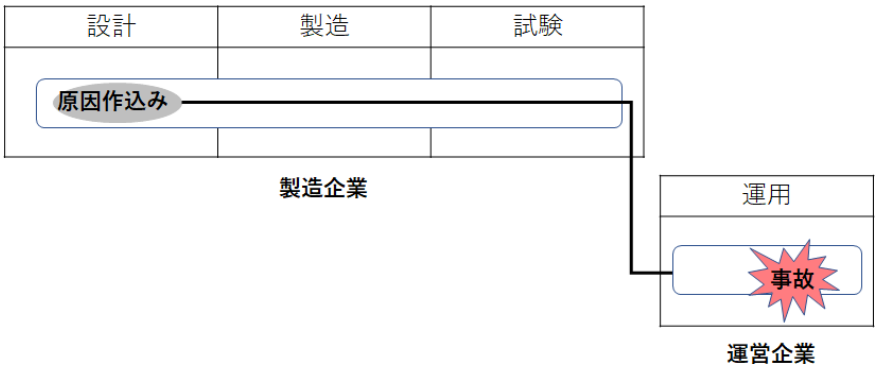

図 1　事故の原因作り込みと発生がプロセスをまたがる事例

また、問題が自組織で発生した場合でも、提供先でより大きな問題を発生させ、信頼をより大きく損なう可能性があったことに注意しなければならない。例えば、産業用ゴム製品の検査不正の問題ではタンカー事故の可能性を、潜在させている。

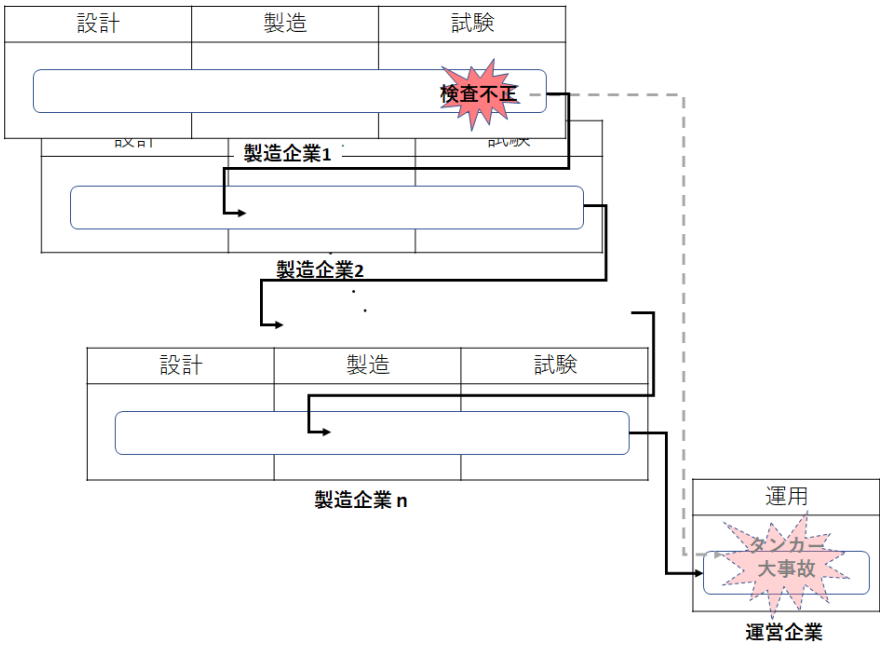

図 2　事故原因作り込みの後で複数の企業を経てから事故が発生する事例

4.　サイバーフィジカル空間での信頼の構築へ

このように、サプライチェーン上の企業は、その企業に至るまでの企業の責任も負うことになる可能性がある。サプライチェーンの終点に近づけば近づくほど、責任は大きくなり、問題もより重大になる場合もあり、事業のリスクは大きくなる。リスク低減のためには、ひとつの企業の努力だけでは解決できず、サプライチェーン全体での取組みが必要である。サプライチェーンを構成する企業が、サプライチェーン全体としての信頼を増大させることに参加して、リスクを低減させるのである。企業間の信頼は、具体的には、発注側企業が機能だけでなく信頼に関する要求も含めた明

確な要求を受注側企業に提示すること、要求を提示された受注側企業は自社のプロセスが要求に足ることの証拠を、必要に応じて、データをもって発注側企業に示すことで形成される。こうした企業間の信頼で企業をつないで行くことによって、サプライチェーンの信頼の連鎖が形成されるのであろう。

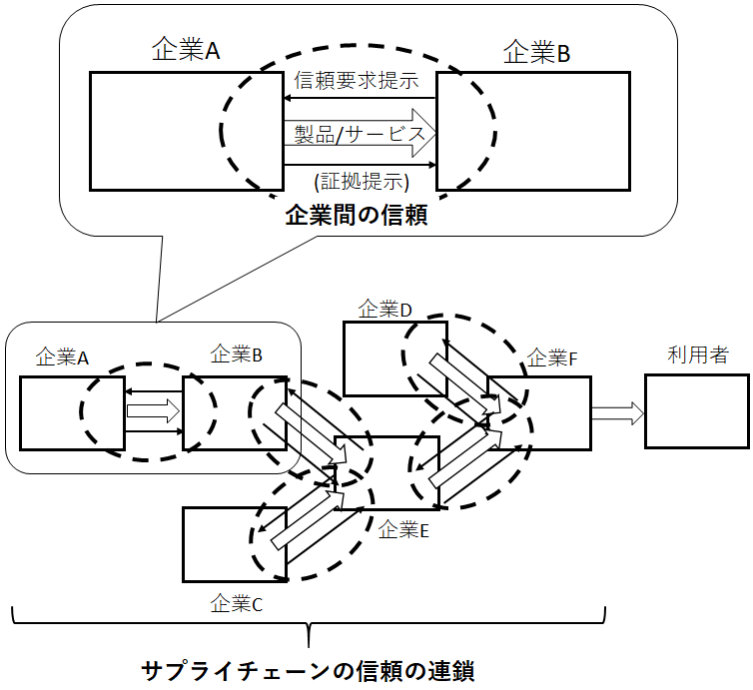

図 3 サプライチェーンにおける信頼の連鎖

注）信頼要求とは、機能だけでなく信頼に関する要求も含めた明確な要求を指す。

企業間の信頼の前提は、自社内において、社内規程を順守して各プロセスを実施し、規程が適用できないとわかった場合は全社での対応判断がなされることである。この前提を基にサプライチェーン全体で企業間の信頼を形成するには、少し時間がかかるかも知れない。よって、信頼の連鎖は全てが同時に解決されるわけではなく、構築が可能な部分から一歩一歩進めていくしかない。アタックサーフェスの増大傾向を考慮すれば、取組みへの着手を遅らせることはできない。

サプライチェーンが複雑になればなるほど、信頼を連鎖させるためのコストは増加し、実現も難しいと考えられるかも知れない。それでも、現在出現しつつあるサイバーフィジカル空間は、サプライチェーンを取り込んで、信頼を構築するための好適な場になるであろう。サイバーフィジカル空間では、それぞれのプロセスにおいて、フィジカル空間の状態を適切なセンサーで収集・デジタル化しサイバー空間へ移行させて処理できる。これには初期コストはかかるが、人がやっていた作業をサイバー空間へ自動的に移行させて処理させることで、長期的にはコスト低減につなげられるであろう。規程順守の判定やその記録も、サイバーフィジカル空間での実現は容易である。規程が適用できない場合には、判断すべき人たちがサイバー空間上で決裁できる。信頼の連鎖に

必要な要求事項も証拠も、サイバーフィジカル空間では自動収集し記録できる。そうしたデータは、必要に応じて、適切な範囲で開示することで信頼を連鎖させることができるであろう。サイバーフィジカル空間上に構築されるサプライチェーンの信頼の連鎖は、従来とは異なる新たな信頼を産み出し、それによって、事故の発生は抑制され、社会全体のコスト低減につながるであろう。

5. 謝辞

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。

参考文献

[1]https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
[2] https://www.itmedia.co.jp/news/articles/1405/15/news096.html
[3]https://www.vice.com/en_us/article/3ky75b/windows-malware-wannacry-new-iphone-delays
[4] https://www.khi.co.jp/news/C3180228-1_2.pdf
[5] https://www.toyotires.co.jp/uploads/2017/03/20170324.pdf
[6]https://www.epa.gov/sites/production/files/2015-10/documents/vw-nov-caa-09-18-15.pdf
[7] https://www.ajinomoto.com/jp/presscenter/press/detail/2001_01_06.html
[8] https://www.bbc.com/japanese/46395567
[9] https://response.jp/article/2003/09/26/54177.html
[10] https://www.itmedia.co.jp/news/articles/1906/10/news049.html