オープンデータを用いたサプライヤーのセキュリティ評価手法

森 拓海[1]　藤田 真浩[1]　山中 忠和[1]

概要：サプライチェーン攻撃の増加によって，サプライチェーンを形成する複数のサプライヤーのすべてが適切なセキュリティ水準を達成することが求められている．従来，サプライヤーのセキュリティ水準の評価は，過去の取引実績や知名度などの主観に頼ることが多く，セキュリティ水準の低いサプライヤーが選択され，サイバー攻撃の対象となっていた．本稿では，複数の情報源から収集したオープンデータを活用し，セキュリティ水準を数値化するサプライヤーのセキュリティ評価手法を提案する．本方式では，情報源を評価項目に応じて分類，重み付けを行った上でリポジトリ化し，発注元(バイヤー)の要求に応じてセキュリティ水準を数値化することで，サプライヤーのセキュリティリスクの可視化と共通認識を促進する．また，NIST SP800-53,SP800-161 といったセキュリティ管理基準と照らし合わせ，サプライヤーが公開すべき情報と，その公開方法について評価し，本方式の有効性を確認した．

キーワード：サプライチェーンセキュリティ，オープンデータ，セキュリティ評価手法

Security Rating Method using Open Data for Suppliers in Supply Chain

Takumi Mori[1]　Masahiro Fujita[1]　Tadakazu Yamanaka[1]

Abstract: With the increase of supply chain attacks, all the suppliers in the supply chain must achieve the appropriate security level to protect the attacks. The suppliers' security levels have been evaluated subjectively by checking transaction histories and/or a company's name. It leads that a low security level supplier is selected, and then it may be targeted for cyber attacks. In this paper, we propose a supplier security rating method that quantifies the security level by using open data collected from multiple information sources. The collected data are classified, weighted based on security rating items, and stored to a repository. The security levels are evaluated objectively by referring to the repository and based on a request of buyers. The security risks of the suppliers can be visualized and make common view of security between the buyers and suppliers. In addition, we evaluated the information that suppliers should disclose and the method of disclosure using security management standards such as NIST SP 800-53 and SP 800-161, and verified the effectiveness of our method.

Keywords: Supply chain security, Open data, Security rating method

1. はじめに

1.1 背景

IoT の普及により，１つの製品・サービスを開発するには，サプライヤーの協力が不可欠であり，安全・安心なサプライチェーンの形成が求められる．カスペルスキーは，2017 年に発表した脅威予測レポート[1]の中で，「サプライチェーン攻撃」の増加を指摘し，ソフトウェア製品の正規のアップデートに ShadowPad, ExPetr/NotPetya といったマルウェアが組み込まれた事例を紹介している．いずれの事例も，アップデートサーバにアクセスするための認証情報が漏洩したことが原因であった．これらは，サプライチェーン上のセキュリティ水準の低い組織を狙って攻撃したものであり，カスペルスキーは 2018 年度の脅威予測レポート[2]で，サプライチェーン攻撃への対策の難しさを指摘している．

サプライチェーンにおいて，発注元(バイヤー)と(複数の)サプライヤーの情報セキュリティリスクの認識に齟齬が発生することで，一部のサプライヤーの脆弱性が原因でサプライチェーン全体が機能停止してしまう．これを防ぐために，米国連邦情報システムを対象としたセキュリティ管理策の基準である NIST SP800-53[3](民間企業向けには SP800-171[4])でもサプライチェーンのセキュリティについて言及している．また，サプライチェーンセキュリティに特化した SP800-161[5]も策定されており，サプライチェーンのセキュリティの重要性は，今後も増していくと考えられる．

1.2 関連研究

サプライチェーンにおける情報セキュリティの取り組みとして[6][7]がある．久保ら[6]は，日本企業を対象に，サプライチェーンにおける情報セキュリティ管理について，アンケート調査や公開情報(有価証券報告書, CSR 報告書な

1三菱電機株式会社 情報技術総合研究所 〒247-8501 神奈川県鎌倉市大船 5-1-1.
Mitsubishi Electric Corporation,Information Technology R & D Center,5-1-1
Ofuna Kamakura, Kanagawa, 247-8501, Japan.

ど)の調査をもとに，日本のサプライチェーンの情報セキュリティ管理の課題をまとめ，それを解決するリスク管理のPDCA サイクルを提案している．原田ら[7]は，サプライチェーンにおけるバイヤーが，複数のサプライヤーをモニタリングする方法として，サプライチェーン全体の IT ガバナンスを調整し，統合する方法を提案している．

これらの研究では，ガバナンスの統制方法の検討を通じて，サプライチェーン全体の信頼性確保のために，情報の可視化と統制が必要であることを示唆している．そこで，本稿では，以下を課題とする．

① サプライチェーン上のサプライヤーに関する情報セキュリティリスクの客観的指標の確立

② 複数のサプライヤーのリスクの共通認識の促進

これらの課題について，オープンデータを用いたサプライヤーのセキュリティ評価手法を提案する．

1.3 本稿の貢献

オープンデータを利用し，セキュリティ水準(セキュリティポリシーの内容，サプライヤーの属性確認，調達品の原産国，輸送経路など)を数値化することによって，サプライチェーン上のバイヤーと複数のサプライヤー間のセキュリティ水準の齟齬を解消する．

本稿では，セキュリティの評価に関連する複数のオープンデータの情報源に重み付けし，検証対象のセキュリティ項目に応じて情報源を特定し，重みと評価項目によってセキュリティ水準を数値化する方式を提案する．この方式に対し，NIST SP800-53,SP800-161 といったセキュリティ管理基準と照らし合わせ，サプライヤーが公開すべき情報と，その公開方法についての方針を示す．

2. 提案方式：オープンデータを用いたサプライヤーのセキュリティ評価手法

2.1 アプローチ

サプライチェーンのセキュリティは SCRM(Supply Chain Risk Management)の枠組みで進める．青地ら([8])の提案スキームでは，以下の 5 つステップから構成される．

STEP1. 基本方針の策定

STEP2. 現状分析

STEP3. リスク戦略の策定

STEP4. 監視・検知・対応計画

STEP5. 実施・運用・改善

このうち，STEP2～4 でリスクの把握，分析，対応を行う上で，サプライチェーン上の脆弱な箇所を特定し，それらに絞って対策を実施するために，リスクの可視化が必要となる．まず，サプライヤーのセキュリティリスクとなり得る事項(評価項目)を検討し，リスクの判断基準となる情報を明らかにする．次に，判断基準となる情報源の種類を分類する．分類した情報源の特性に応じて，情報源を重み付けし，リポジトリ化する．最後に，評価項目と情報源の重さに応じて，サプライヤーのセキュリティ水準を 0～100 点で点数化する．

2.2 Linked Open Data (LOD)

本方式では，インターネット上に公開されたオープンデータを活用する．オープンデータを公開・共有するための技術として Linked Open Data (LOD)[9]がある．この技術は，構造化されたデータ同士をリンクさせてグラフ構造を形成し，リンクをたどってデータを検索可能とする点が特徴である．HTML 文書間のハイパーリンクと類似しているが，よりコンピュータ処理に特化したインタフェースを持つ．REST API や SPARQL API に準拠したエンドポイントにクエリを発行する事で LOD を利用できる．LOD の仕組みを活用したアプリケーションの多くは，発展途上にあり，慶應義塾大学などが協力する LOD チャレンジ実行委員会が主催する Linked Open Data Challenge(2011 年～)が開催されるなどして，その活用が期待されている．

2.3 方式の説明

サプライヤーの情報セキュリティに関するオープンデータを，評価するセキュリティ項目に応じて収集，リポジトリ化し，バイヤーのセキュリティ評価要求に応じて数値を算出する．オープンデータを活用することで，第三者視点が確保でき，共通のリスク認識を促すことができる．以降に方式の詳細手順を示す．

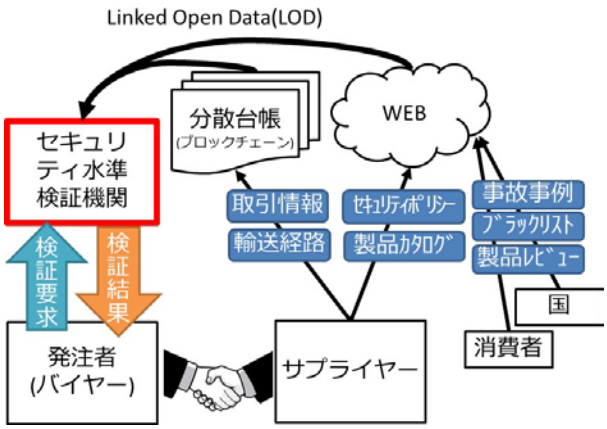

図 1 提案方式の構成

図 1 は，本方式の構成図である．図中のセキュリティ水準検証機関が，本方式を用いてセキュリティ水準の評価を行うエンティティである．セキュリティ標準検証機関は，バイヤーから，サプライヤーに関するセキュリティ検証要求に応じて，WEB や分散台帳などから LOD の仕組みを利用して公開情報を収集し，検証結果を数値化してバイヤーに返却する．公開情報は，サプライヤー自身が公開する取引情報，製品の輸送経路情報，製品カタログ，セキュリテ

ィポリシーなどのほか，国や消費者が公開する製品の事故事例や製品レビュー，禁輸国などのブラックリスト情報をその特性に応じて WEB か分散台帳に蓄積することを想定する．以降で方式の動作を説明する．

2.3.1 オープンデータの蓄積

公開情報が取引情報や輸送経路情報など，トランザクションデータの場合は，LOD に対応した分散台帳に書き込む．ブロックチェーンを応用した分散台帳であれば，データの完全性が保証されるため，セキュリティ評価のためのデータとして信頼性を担保することができる．トランザクションデータ以外の場合は，LOD に対応した WEB サイトやデータベースに蓄積する．

2.3.2 リポジトリの作成

セキュリティ水準検証機関は，検索エンジンやクローラを使い，LOD に対応した情報源を検索する．検索により発見された情報源を，セキュリティの評価項目ごとに分類する．例えば，取引情報，輸送経路，セキュリティポリシー，組織情報，製品カタログ，事故事例，禁輸国，取引禁止企業，法律・規制，製品レビューなどである．

情報源には，重みづけを実施する．例えば，表 1 のように情報の信頼性に応じて重み付けを設定する．

表 1 情報源の重み付けの例

重さ	情報源の種類	情報源の例
1	一般的な公開情報	製品カタログ，製品レビュー，セキュリティポリシー，組織情報
2	準公的機関の情報	取引情報，輸送経路
3	公的機関の情報	法人情報，事故事例，禁輸国，取引禁止企業，法律・規制

最後に，情報源の名称，情報源の種類，重さ，URI をエントリとして，リポジトリを作成する．

2.3.3 セキュリティ水準の検証

セキュリティ水準検証機関は，バイヤーから受信したサプライヤーの検証要求に対し，サプライヤーのセキュリティ水準の評価結果を返却する．検証要求は，サプライヤーに関するセキュリティポリシーの存在，属性確認，調達品の原産国，輸送経路など，セキュリティに関する評価対象を指定する．

検証要求に対して，情報源の種類を特定する．検証要求に対応する情報源の種類は，表 2 のように予め定義する．

次に，セキュリティ水準の数値化を行う．検証要求に対する情報源が存在しない場合は，セキュリティに関するサプライヤーの情報が公開されていないことを意味し，信頼できないと判断し，点数を 0 とする．情報源が見つかった場合，検証要求に対して予め定義した評価項目で以下のように数値化する．

表 2 検証要求と情報源の対応

検証要求	情報源の種類
セキュリティポリシーの存在	セキュリティポリシー，組織情報，法律・規制
属性確認	組織情報, 禁輸国, 取引禁止企業，法人情報
調達品の原産国	製品カタログ, 取引情報, 輸送経路
輸送経路	輸送経路, 禁輸国, 取引禁止企業

① 情報源 Si の評価項目に応じた点数付け
評価項目の点数 P_{si} ，評価項目の回答(x_{si})の最大値 $x_{si}^{max}=1$ ，情報源の重み w_{si} ($1 \leqq i \leqq n$) : n は参照した情報源の数

$$P_{si} = x_{si}^{max} \times w_{si} \quad (1)$$

② 評価項目の点数の重みの計算(評価項目ごとの点数の割合を計算)
$P_s : P_{si}$ の合計値 とし，評価項目点数の重み P_{wi} を以下のように求める．

$$P_{wi} = P_{si} / P_s \quad (2)$$

③ 点数の計算(評価項目の点数を 100 点満点で点数化)
評価項目の回答 x_{si}
検証内容の点数 P は，以下で求める．

$$P = \sum_{i=1}^{n} (X_{si} \times P_{wi}) \times 100 \quad (3)$$

以上の手順で，検証要求に対して 0～100 点で評価した結果をバイヤーに返却する．

3. 評価結果

本方式の評価として，認証要求として「セキュリティポリシーの存在」を例に，セキュリティ水準の数値化の具体例を示す. また, 本方式実用性を検討するため, NIST SP800-53 および SP800-161 のサプライヤー評価に関する要件に対し，提案手法でどのように対応可能かを検討する．

3.1 セキュリティ水準の評価例

3.1.1 前提条件

(1) 評価項目

「セキュリティポリシーの存在」を検証するための評価項目として，以下 3 つを定義する．

評価項目 1：セキュリティポリシーの情報源に，該当するサプライヤー企業にセキュリティポリシーが存在するか

評価項目 2：セキュリティポリシーに関連する組織情報が存在するか

評価項目 3：セキュリティポリシーで，セキュリティに関連する法律・規制を遵守する旨の記述が存在するか

(2) 情報源のリポジトリ

情報源の重み付けは表 1 とし，各情報源はリポジトリに登録されているものとする．

(3) 検証要求と情報源の対応

表 2 に示した定義とする．

3.1.2 セキュリティ水準の数値化

検証要求「セキュリティポリシーの存在」に関するセキュリティ水準の数値化を 2.3.3 節の手順に沿って行う．

① 情報源 Si の評価項目に応じた点数付け

情報源は以下とする．

S_1：セキュリティポリシー

S_2：組織情報

S_3：法律・規制

それぞれの情報源の重さは以下のとおり．

w_{s1} =1

w_{s2} =1

w_{s3} =3

x_{si}^{max}=1 のため，P_{si}= w_{si} (1 ≦ i ≦ 3)である．

よって，評価項目は以下のようになる．

評価項目 1：セキュリティポリシーの情報源(w_{s1} =1)に，該当するサプライヤー企業にセキュリティポリシーが存在するか

評価項目 2：セキュリティポリシーに関連する組織情報(w_{s2} =1)が存在するか

評価項目 3：セキュリティポリシーで，セキュリティに関連する法律・規制(w_{s3} =3)を遵守する旨の記述が存在するか

評価項目に対し，存在する場合は x_{si} =1，存在しない場合は x_{si} =0　とする．

② 評価項目の重みの計算

評価項目点数の合計値(P_s)は評価項目 1(1 点)＋評価項目 2(1 点)＋評価項目 3(3 点) = 5 点である．よって，各評価項目点数の重み(P_{wi})は以下のようになる．

P_{w1} = 1/5 = 0.2

P_{w2} = 1/5 = 0.2

P_{w3} = 3/5 = 0.6

③ 実際の点数の計算

評価項目 1 が「存在する(x_{s1}=1)」とし，

(1 * 0.2) *100 = 20 点

評価項目 2 が「存在しない(x_{s2}=0) 」とし，

(0 * 0.2) *100 = 0 点

評価項目 3 が「存在する(x_{s3}=1) 」とし，

(1 * 0.6) *100 = 60 点

すなわち，検証内容の点数は 80 点となる．

3.2 NIST SP800-53 および SP800-161 との対応

情報セキュリティにおける管理策は，組織，システム／サービス，機器などの対象に応じて多岐にわたる．この情報セキュリティの管理策のカタログとして，米国連邦情報システムを対象とした NIST SP800-53(Rev. 4 が最新，Rev.5 は策定中)がある．SP800-53 は，政府の機密情報(CI：Classified Information)以外の重要情報(CUI ： Controlled Unclassified Information)を扱う民間企業向けには SP800-171 もあるが，管理策は SP800-53 のサブセットである．

SP800-53 は適用範囲が広く，粒度の細かいセキュリティ管理策が定義されており，ISO/IEC 27001 や ISO/IEC15408 といったセキュリティの国際標準との対応も取られている．そのため，近年では米国はもとより日本でも参照する動きが広がっている．

また，サプライチェーンのリスク管理に特化した SP800-161 も存在する．SP800-161 は，連邦政府システムおよび組織のための ICT サプライチェーンのリスク管理(ICT SCRM)を支援するための指針を示すものである．この文書で示される ICT SCRM 制御フォーマットは，SP 800-53 Rev. 4 のコントロールまたはコントロール強化にリンクする形で示される(SP800-53 にリンクされていない独自の管理策も含まれる).

SP800-53 および，SP800-161 で独自に定義される管理策のうち，サプライチェーンにおける他組織のセキュリティ評価に関するものをまとめ，本方式で対応可能かを評価した．

SP800-53 および SP800-161 のサプライチェーンにおける他組織(サプライヤー)のセキュリティ評価に関連する管理策に対する本方式での対応を表 3 に示した．

各管理策に対し，大部分は参照する情報源が存在すれば本方式で対応することが可能である．

表 3 NIST SP800-53,161 のサプライヤー評価項目との対応

管理策番号	管理策名	提案方式での対応
SA-9	外部情報システムサービス	情報源として以下を活用 ・法律・規則
SA-9(1)	リスクアセスメント/組織による承認	本方式で実施するセキュリティ水準評価そのもの
SA-9(2)	機能/ポート/プロトコル/サービスを明確にする	情報源として以下を活用 ・製品カタログ
SA-12(1)	調達戦略/ツール/方法	情報源として以下を活用 ・調達経路
SA-12(2)	供給業者に対するレビュー	本方式で実施するセキュリティ水準評価そのもの
SA-12(7)	選択/受け入れ/アップデートに先立つアセスメント	本方式で実施するセキュリティ評価そのもの
SA-12(8)	あらゆる情報源からの情報の利用	複数のオープンデータを活用
SA-12(10)	本物であることと，改変されてないことを確認する	情報源として以下を活用 ・調達経路 ・輸管の履歴(情物一致)
SA-12(11)	エレメント，プロセス，および関係者の侵入テスト/分析	情報源として以下を利用 ・セキュリティ認証 (EDSA，SSA)
PS-7	第三者職員によるセキュリティ	情報源として以下を利用 ・セキュリティ認証 (ISMS,CSMS)
PV-1※	起源 (provenance) の方針と手順	情報源として以下を利用 ・調達経路
PV-2※	起源の追跡とベースラインの開発	情報源として以下を利用 ・製品の在庫状況 ・製品のサポート期限
PV-3※	起源に関する監査ロール	ブロックチェーンを使い，監査記録を保護する.
SA-18(3)※	タンパー抵抗と検出|返品規則	情報源として以下を利用 ・製品の事故事例 ・リコール情報

※は NIST SP800-161 独自の管理策

4. 考察

本章では，1.2 節で挙げた課題に対する考察を述べる．

課題①に対しては，3.1 節で示したように，サプライヤーのセキュリティ水準を数値化して評価することが可能であることを確認した．数値化したセキュリティ水準は，オープンデータを根拠とするため，客観性がある．

課題②については，リスクを 1～100 点に点数化した数値で示すことにより，複数のサプライヤー間で共通のリスク認識が促進されるといえる．

本方式を活用することによって，発注者にとってはサプライヤー選定時に，サプライヤーにとっては受注のために対策強化のモチベーションアップにつなげることができる．

新たな課題として，オープンデータとして公開すべき情報や公開方法について考察する. 3.2 節で, NIST SP800-53, SP800-161 との対応を確認した．その際，必要とされる情報源について，現時点で利用可能なものを表 4 にまとめた．

表 4　NIST SP800-53,161 の要件に対応する情報源の例

求められる情報源	利用可能な情報源の例
法律・規則	(一財) 安全保障貿易情報センター(CISTEC)：総合データベース(有料) 国内法令コーナー http://www.cistec.or.jp/dlaw/index.html
製品カタログ	製品のメーカーWeb ページで公開.
調達経路	ほとんど非公開
輸管の履歴 (情物一致)	(一財) 安全保障貿易情報センター(CISTEC)：公表リスト(有料) https://www.cistec.or.jp/klk/ (リスト規制に該当しないと判定した集積回路のリスト)
セキュリティ認証 (EDSA，SSA)	ISASecure： ISASecure Certified Devices https://www.isasecure.org/en-US/End-Users/ISASecure-Certified-Devices
セキュリティ認証 (ISMS,CSMS)	(一社)情報マネジメントシステム認定センター(ISMS-AC)： ISMS 認証取得組織 https://isms.jp/lst/ind/index.html
製品の在庫状況	製品によっては Web ページで公開.
製品のサポート期限	各製品のサポート Web ページにて公開. マイクロソフト製品の例： https://support.microsoft.com/ja-jp/lifecycle/search
事故事例	(独)製品評価技術基盤機構: 製品事故情報 DB, http://www.jiko.nite.go.jp/php/jiko/search/index.php
リコール情報	(独)製品評価技術基盤機構: 社告・リコール情報 DB, http://www.jiko.nite.go.jp/php/shakoku/search/index.php

見つかった情報源で LOD に対応しているものはなかった．また，CISTEC のデータベースのように，公開はされているが，有料のものもある．また，製品カタログや，在庫状況は，メーカーごとに公開され，情報の取得のインタフェースが統合されていない．さらに，調達経路のように，ほとんど公開されていない情報もあった．

現在公開されている情報源を利用する場合，LOD の API をほとんど利用できないため，実装が難しくなる可能性がある．しかし，インタフェースの整備は，LOD の需要の高まりにより，いずれ解消すると考えられる．

有料の情報や，非公開の情報の利用については，適切なアクセス制御が必要になる．特に，公的な取引情報は法人インフォなどで公開されるが，企業間のビジネスに関する情報は非公開であることが多い．オープンデータの公開基盤としての信頼性・可用性の向上と，情報開示の制御(機密性の担保)は，トレードオフの関係にある．例えば，プライベート型ブロックチェーンを用いて取引履歴の管理を行えば, 参加者の信頼性(書き込まれる情報の信頼性)は高め, 非参加者から情報を秘匿することはできる．しかし，合意形成において厳格な承認が無くても良いため，取引履歴が改ざんされる可能性は残る．また，ブロックチェーンに参加さえすれば情報はすべて閲覧可能なため，参加者間での情報の開示制御は難しい．

この課題に対し，機密情報はブロックチェーンに記憶せず, 暗号化した機密情報のハッシュ値(機密情報へのポインタ)のみをブロックチェーンに記録する方式[10]や，アクセス制御機能を持つ暗号方式である関数型暗号で暗号化したうえでブロックチェーン上に機密情報を保存する方式[11]が提案されている．このような方式と組み合わせることにより，アクセス制御が必要なオープンデータをサプライヤーのセキュリティ水準評価に利用することが可能と考えられる．

5. まとめ

サプライチェーンにおけるサプライヤーのセキュリティを評価するために，セキュリティに関連する複数のオープンデータの情報源をリポジトリ化し，セキュリティ水準を数値化する手法を提案した．

従来はサプライヤーのセキュリティ評価はバイヤーが，過去の取引実績やサプライヤーの知名度など，主観的に実施している場合が多かった．セキュリティ水準の評価にオープンデータを用いることで，評価に客観性を持たせることができ，数値化することにより複数のサプライヤーに関するリスクの共通認識を促進する．

一方で，セキュリティ水準の評価に使用する情報源については，適切なアクセス制御が必要な場合もある．本方式で情報源として例示しているブロックチェーンの場合，記録される情報の完全性は担保されるが, 秘匿性を持たない．そこで，暗号技術と組み合わせた方法でオープンデータを蓄積・公開する方法もあることがわかった．

また，本方式ではサプライヤーのセキュリティの評価項目は，単一の情報源により評価を実施している．公的機関の情報のように情報源の信頼性が担保されている場合を除き，評価結果の真偽を単一の情報源に頼ることは適切ではない．そこで，評価項目の回答の信頼度に情報源の数や種類の多さを追加することを今後の検討課題とする．

サプライチェーンにおけるバイヤーのセキュリティの要求や，サプライヤーのセキュリティ水準は変化していくものである．本方式のように，日々蓄積されるオープンデータを活用し，セキュリティ水準の再評価を効率化することで，より安心・安全なサプライチェーンの構築が可能になるだろう．

参考文献

[1] KASPWRSKY:2018 年サイバー脅威の予測, KASPERSKY(online), available from <https://media.kaspersky.com/jp/pdf/pr/Kaspersky_KSB2017_Predictions-PR-1043.pdf>(accessed 2019-3-28).

[2] KASPWRSKY:2019 年サイバー脅威の予測, KASPERSKY(online), available from <https://media.kaspersky.com/jp/pdf/pr/Kaspersky_KSB2018_Predictions-PR-1047.pdf>(accessed 2019-3-28).

[3] NIST: SP800-53 Rev.4 Security and Privacy Controls for Federal Information Systems and Organizations, NIST(online), available from <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final >(accessed 2019-3-28).

[4] NIST: SP800-171 Rev.1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST(online), available from <https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final> (accessed 2019-3-28).

[5] NIST: SP800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations, NIST(online), available from <https://csrc.nist.gov/publications/detail/sp/800-161/final >(accessed 2019-3-28).

[6] 久保知裕, 原田要之助: サプライチェーンにおける情報セキュリティの研究,情報処理学会研究報告, Vol.2014-EIP-65, No.3, pp.1-8(2014).

[7] 原田要之助, 久保知裕: 複数企業にまたがった IT サービスのサプライチェーンにおける IT ガバナンスの課題について, 情報処理学会研究報告, Vol.2015-EIP-67, No.3, 1-8(2015).

[8] 青地忠浩: サプライチェーンリスクマネジメントのフレームワークと実例, 日本 LCA 学会誌, Vol.14, No.4, pp.256-266(2018).

[9] Bizer, C., Heath, T., Berners-Lee, T. : Linked data – the story so far, International Journal On Semantic Web and Information Systems 5(3), pp.1–22(2009).

[10] Zyskind,G. Nathan,O. and Pentland,A. : Decentralizing Privacy: Using Blockchain to Protect Personal Data, 2015 IEEE Security and Privacy Workshops, IEEE, pp.180-184(2015).

[11] 柴田 陽一,小関 義博,川合 豊ほか:関数型暗号とブロックチェーンの組合せによる秘匿分散記録システムの試作, DICOMO2018 論文集, pp.1879-1882(2018).