Vol.2017-EIP-75 No.12
2017/2/17

サプライチェーンと情報セキュリティ

金子啓子[†1]

概要：本稿では、サプライチェーンと情報セキュリティという古くて新しい問題を俯瞰して整理し、実務上の課題について検討する。調達・委託先における情報管理としての情報セキュリティについては、調達・委託先に情報セキュリティを要請する必要性と制度上の取組を紹介し、情報セキュリティ事故発生時の調達・委託先への損害賠償や求償の課題と製造物責任に示唆を得た解決方法の提案を行う。製品セキュリティについては、品質レベルの考え方についての課題を整理し、契約上、要請すべき内部管理を検討する。

キーワード：情報セキュリティ，サプライチェーン、損害賠償、製品セキュリティ、ＩＴセキュリティ

Supply-Chain and Information Security

KEIKO KANEKO[†1]

Abstract: This manuscript shows the overview of “supply-chain and information security”, which is old and new issue, and discuss practical challenges. With regard to information security as information management at the supplier of goods or services, this explains the necessity of requiring information security to the supplier and related social system or governmental action, and make some proposal on the reimbursement of the damages to the supplier hinted with product liability practice. As for information security of product/system, this discusses the measure to decide what the required quality should be, and internal control to be required by the agreement.

Keywords: information security, supply-chain, reimbursement of damages, security of products/service, IT security

1. はじめに：サプライチェーンと情報セキュリティのパターン

近年、サプライチェーンにおける情報セキュリティが議論されている。サプライチェーンにおける情報セキュリティには、大きく分けて、2 種類ある。一つは、仕入先・委託先における情報管理としての情報セキュリティであり、もう一つは、調達するシステムや部品、プログラムのセキュリティ（いわゆる製品セキュリティ）である。

例えば、架空のメーカーA 社を例にとると、下記のような場面で情報セキュリティが関係してくる。

⑴　部品の調達先 B 社に対して、自ら開発した技術ノウハウを開示して部品の製造を委託したり、部品メーカーと共同開発をする場合、部品メーカーから技術ノウハウが流出しないよう、また、流用されないよう、部品メーカーに対し情報管理を求める。

⑵　メーカーA が会員制のサービスを行うにあたり、消費者から個人情報を登録いただくが、

⑵－１　その登録や取扱、システム運用を C 社に委託する。C 社から情報漏えいがないよう、C 社における情報セキュリティを求める。

⑵－２　自社でシステムを保有するのではなく、ホスティングを含め、D 社のクラウドサービスを利用する。その際、D 社に情報漏えいがないよう、D 社のサービスに一定の情報セキュリティレベルを求めたい。

⑵－３　Web サイトなどのシステムを E 社に委託して開発してもらうに際し、一定のセキュリティレベルを要請する。

⑶　メーカーA が販売する PC やネットワークにつながる製品やシステムに、マルウエアやバックドアが仕込まれていたり、脆弱性が放置されていたりといった、情報セキュリティ上の問題がないよう、PC や製品の部品やソフトウエアのベンダ F 社に、その納品物に一定の製品セキュリティ品質を求める。

⑴、⑵－１、２は、調達先における情報管理を求めるものであり、⑵－３、⑶は、納入される製品の製品セキュリティである。

これらは、古くからある問題ではあるが、近年、国家間でサイバー空間を通じた情報窃取や攻撃が激しくなる中、製品セキュリティは特に重要になっており、政府調達においては、かなりスクリーニングが厳しくなっているa。

この論文では、この古くて新しい問題を俯瞰して整理し、実務上の課題について検討する。

それぞれの場合に、実務上は、①契約上の手当、②実務上、

†1 情報セキュリティ大学院大学
Institute of Information Security

a 「必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を府省庁が確認できることを加えること」が要求されている。サイバーセキュリティ戦略本部「政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）」（2016 年 8 月 31 日）5.1.2　29 頁

求めるレベルをどうするか、③情報セキュリティレベルの確認・監査、④情報セキュリティ事故発生時の対応と損害賠償、の問題がある。

2. 調達・委託先における情報管理としての情報セキュリティ

2.1 調達先への情報セキュリティの要請

⑴のような、調達先との取引においては、機密性について、古くから開発契約や購買契約に機密保持条項を入れてきた。通常、機密保持条項では、機密保持、目的外利用の禁止が定められ、この目的のために、情報を善良な管理者の注意を以て管理することb、従業員や委託先に対しても同様の義務を課し、これを遵守することを保証すること、程度が定められる場合が多かったが、「善良な管理者の注意をもった管理」の内容はあまり具体的に踏み込まなかった。多少、踏み込んだ条文でも、アクセス権者の限定やそのリストの維持、複製の禁止や分解・リバースエンジニアリングの禁止、程度が定められている程度だった。

この段階では、自らの秘密管理性を保持することと、開示の相手方の会社の故意か重過失による自社製品への流用や、第三者への開示をけん制することが主な目的だった。機密保持義務違反による損害賠償は立証が難しいので、予定損害賠償額を定めることが時々あるが、このような目的だったので、1 億円など、高額の金額を入れて牽制する例が多く、受ける方も、交渉してはみるものの、自分さえ気を付けておけばよいので、甘受することが多かった。

高度成長期までは、日本は欧米から技術を輸入する立場であり、契約には入れていても、どちらかというと性善説で臨み、あまり厳しくチェックして来なかった。逆に、欧米の企業が日本企業に生産委託をするためにトレードシークレットを開示する取引では、かなり厳しく制限され実施を監査されたと聞く。

しかし、1990 年代後半から、周辺諸国のコンペティタから技術を狙われる立場になった。急激に技術的に追い上げられると同時に、様々な手口で技術情報が盗まれたと思われる状況が発見された。1991 年、WTO の TRIPS 協定に先取りして対応するために、民事的保護だけができた営業秘密の保護は、このような背景から、2003 年の不正競争防止法改正で、中国・韓国より遅れたが刑事罰が導入され、以降、５回の改正で、強化されてきた。

本来、営業秘密保護は、英米法で発達した unfair competition の一種である。事業競争の中で、事業者は、技術や顧客情報、商品戦略、価格戦略、等々、コンペティタに知られると、自らは投下してきた投資を相手が省けたり、裏をかいたりして、競争優位を失うような情報を外部に漏れないようにする。逆に激しい競争の中で、コンペティタが次に何をやろうとしているのか、自社がうまく作れないものをどのように作っているのか、等を、合法な範囲で情報収集しようとすることcは健全な競争の一環である。しかし、秘密として管理しているのに、それを不正な手段で入手したりその介在を知って入手、使用したり、さらに提供する行為を不正な競争の類型としてけん制するのが、営業秘密保護であるd。結果として知的財産権に類似する効果があるが、物権的性質ではなく、あくまでも不法行為のような行為規制の性質のものである。従って、秘密として管理しているかどうかの判断は、入手手段の不正性、悪質性によって変わってもおかしくないと考える。

現に、かつては小規模なかつらの事業者が、表紙にマル秘の印を押し、支店のカウンター内側の顧客からは見えない場所に保管していたことでも秘密管理性は認められたeように、各社の状況にあった守り方をすればよかった。しかし、経済産業省は、法律上の評価とは別に、情報セキュリティ管理を普及させる目的もあり、実際に、どのように隙なく守るかを啓発的に示すため、2003 年、ISO/IEC27002 ベースの営業秘密管理指針を発行fした。

また、民間でも、本来、法律の要件を満たすための秘密管理性の確保であれば、業務上知る必要のある人だけがアクセスできる Need to know ベースの管理策でよかったはずだが、狙われていると思われる事業については、産業スパイの被害にあった経験をもとに、アクセス権者に対するけん制や、社外の故意に情報を盗もうとする者から守るための対策も打たなければならなくなった。そこで、情報管理、情報セキュリティの社内基準を整備し、情報の重要性に応じて、これらの管理策を義務付ける会社がでて来た。

情報を入手する立場からは、守りの堅い本丸に忍び込むようなリスクの高いことはやらず、情報が渡されていそうな、最もガードが弱そうなところを狙う。従って、守る側とすれば、自社だけでなく、営業秘密を開示、共有している調達先にも、自社の社内基準に準じた、具体的な管理策を要請する必要が出てきた。

ある企業は、調達先に求める情報セキュリティレベルを公開し、調達基準に入れたg。優越的地位の濫用、下請法違反にならないように配慮しつつも、狙われている事業に関連する調達先については、一定のセキュリティレベルを要請せざるを得ない。実効性を高めるために定期的に監査も実施して確認している。高度な情報セキュリティを要求し

b 「自らの保有する同じ重要性のある情報と同じレベル、しかし、善良な管理者の注意義務を下回らない」という定め方をしたものもある。

c 例えば、外部から見えるものから推測したり、商品を購入して分析するなど。

d しかし、2009 年の不正競争防止法の法律改正で、図利加害に目的拡大

e大阪地方裁判所平成８年４月１６日判決、裁判所ホームページ参照

f 営業秘密として保護されるための要件と誤解され、2015 年改訂。

g http://www.panasonic.com/jp/corporate/management/procurement/for-suppliers.html

ているわけではないが、小規模な町工場にはそのままでは実施が難しいこともある。そのような場合は、現地に出向き、リスクベースで規模と重要性から判断して、その管理策が対策しようとしている脅威への代替策を共に考えるようなことも行っている。

しかし、一般的には、より高い情報セキュリティを要求することは、時として調達先でのコストがアップし、調達品の購入価格アップの要請を招くことにつながるというジレンマがある。結局、元々きっちり情報管理がなされているところを調達先に選ぶことにもなるが、情報セキュリティができている会社が評価される、という意味では、情報セキュリティも競争力や信用の一つの要素といえる。中小企業の社長から、ISMS の認証を取ったお蔭で他の会社からも受注が増えた、という声も聴いたことがある。市場の力で規範が普及していく良い事例かもしれない。

事故発生時の対応としては、不審なコンタクトがあった、サンプルが行方不明になった、など、情報が狙われている兆候と疑われる事があったときにすぐに連絡してもらうことが重要になる。本当に狙われていることが確認でき、対策を強化することができるからである。例えば、メーカーA を騙って問い合わせの電話があったことや、信用して話してしまった、などということは、追及して損害賠償を請求するより誤報でもよいのですぐに報告してもらうことの方が重要である。

2.2 個人情報取扱の委託先への情報セキュリティの要請

個人情報保護法第 22 条では、安全管理措置の重要な要素として、委託先の監督義務が定められており、契約上、委託先に、機密保持義務を課すことはもちろん、一定の情報セキュリティを求めることは、当たり前のこととなっている。経産省の個人情報保護ガイドラインの第 22 条の解説によれば、委託先の監督には、委託先を適切に選定すること、委託先に法第２０条に基づく安全管理措置を遵守させるために必要な契約を締結すること、委託先における委託された個人データの取扱状況を把握することが含まれる、とされているh。更に、委託先による再委託についても、2014 年 12 月の改正以前は「注意を要する」にとどまっていたがi、改正後のガイドラインjでは、再委託先での流出事故でも同様の責任があるため、委託元は、かなり踏み込んで、契約や管理方法の事前承認や、実態把握まで踏込むことを「望ましい」とし、その後の再委託のサプライチェーンについても、同様とする、としている。まさに、法律上、サプライチェーンでの情報セキュリティを（望ましい、という形ではあるが）求めたものと言える。

求める情報セキュリティレベルについては、漏えい防止のためには、少なくとも自社で定めるレベルと同等であることが必要となるk。かたや、委託元が優越的地位にあるl場合は、委託元は、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課してはいけないのmで、実際の対応は難しい。結局、調達先の場合と同様、情報セキュリティができているところに委託する、ということになる。経済産業省のガイドラインも、2014 年 12 月改正で委託先管理を強化しているが、第 20 条で要求するような具体的な管理策は委託先の選定のところにリストし、これを示唆しているように思われる。

このように、法律上の委託先の監督義務から委託先での情報セキュリティ状況の把握が義務とされていることだけでなく、プライバシーマークの認証取得にあたっての審査内容でも JISQ15000 の 4.4.3.4 項に基づく監督が要請されていることから、個人情報の委託先への監査は一般的に行われている。

2.3 政府や制度上の取組

個人情報保護法の制定を後押しすることになった個人情報漏えい事故nでも、委託先のアルバイト学生による犯行であったことから、前述のとおり、個人情報保護法では委託先の監督が盛り込まれた。以降、2.1 で述べたような営業秘密保護においても同様のニーズが出てきた。そもそも、情報システム業界は、多段のアウトソーシングで成り立っている業界であり、厳しいコスト競争の中では、海外へのアウトソースも含め、どうしても外注することが多くなる。

政府もアウトソーシング先の情報セキュリティのリスクに対応し、経済産業省は、情報セキュリティガバナンスoの一環として、2009 年、「アウトソーシングに関する情報

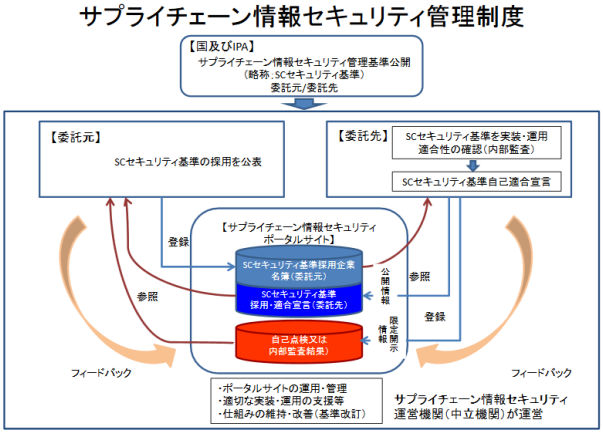
h　個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
(平成２６年１２月１２日厚生労働省・経済産業省告示第４号)　41 頁
i　個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
(平成２１年１０月９日厚生労働省・経済産業省告示第２号) 39 頁
j「このため、委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、委託先から事前報告又は承認を求める、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施する等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が法第２０条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。」前掲注 h　42 頁
k 委託先の選定に関する説明だが、「委託先の安全管理措置が、少なくとも法第２０条で求められるものと同等であることを確認するため、以下の項目が、委託する業務内容に沿って、確実に実施されることについて、委託先の社内体制、規程等の確認、必要に応じて、実地検査等を行」うことを推奨している。　前掲注 h　41 頁
l 優越的地位にあるかどうかは、取引依存度、委託元の市場における地位、委託先にとっての取引先変更の可能性、委託元と取引することの必要性を示す具体的事実等を総合的に考慮して判断される。公正取引委員会　『優越的地位の濫用に関する独占禁止法の考え方ガイドブック　優越的地位の濫用　知っておきたい取引ルール』　2015 年 7 月
m 「なお、優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。」前掲注 h　41 頁
n 1999 年宇治市住民情報流出事件
o　http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html　（最終閲覧　2017 年 1 月 1 日）

セキュリティ対策ガイダンス」pを発行した。そこでは、そもそもアウトソースする目的とリスクを認識して、アウトソース先の選定や、そもそもアウトソースする部分を良く見極めること、特に、海外へのアウトソースでの留意点の追加、アウトソース先との契約に盛りこむべきことや状況確認の必要性など留意点、そして、それが企業集団として実施されるような社内行政が望まれることなどが啓発的に書かれている。

同じく、経済産業省は、情報セキュリティガバナンスの一環として、2009 年、「情報セキュリティ格付を実施する各種機関の運営に関する一般要求事項」qを発行した。

実は、格付け制度の提案は、2007 年、民間の情報セキュリティを重要視する会社数社ではじめられた。その理由の一つにサプライチェーンの情報セキュリティ問題がある。委託先選定にあたり、その情報セキュリティの状況を確認することが望ましいとされているが、初めから監査のようなことはなかなか難しい。外形的にわかるものとしては、プライバシーマークや ISMS などの外部機関による認証を受けているかどうかがある。確かに、これらは、企業の情報セキュリティや個人情報保護に取組む姿勢を示すものではあるが､情報セキュリティのレベルを示すものではなく、社内で行うリスク評価に基づくマネージメントシステムが回っているかどうか、を確認するものである。従ってこれとは別に､委託先がどのレベルで情報を守ってくれるのか、を知るニーズがある。また、委託先にとっても、様々な委託元企業から様々な情報セキュリティを要求されることや、各社からの監査に都度対応することも負担が大きい。そこで、情報セキュリティレベルを客観的に証明する格付けがあれば､それを示すことで監査も不要となるのではないか、という観点から、情報セキュリティ格付けが提案された。情報セキュリティができていることが企業の信用につながる、という観点からも､「格付け」に期待が寄せられた。そこで、2008 年、株式会社アイ・エス・レーティングが設立され、情報セキュリティの格付けを行っているr。

また、2003 年からスタートしている情報セキュリティ監査制度においても、2010 年、日本セキュリティ監査協会がサプライチェーンの情報セキュリティ管理モデルを提案、2012 年、「サプライチェーンの情報セキュリティの管理基準」を策定したs。そこでは、一定の価値のある情報を想定して、わかりやすい情報セキュリティ管理基準を定め、委託先企業がそれに適合していることを自己宣言することで、多段のアウトソースがあっても均一的な情報セキュリティが確保できる制度を提案している。



更に、国際標準では、ISO/IEC27036（Information technology — Security techniques — Information security for supplier relationships）で、サプライチェーンの情報セキュリティを取り上げている。そこでは、委託先における情報管理としての情報セキュリティだけでなく、調達した ICT 機器やシステムの製品セキュリティ問題や、クラウドサービス利用における情報セキュリティもカバーされている。

過去、海外の委託先に対し、一定の情報セキュリティ管理策の実施、監査受入、再委託先への同様の管理などを要請する際に説得が難しい時もあったが、国際標準化されることで説得もしやすくなる。更に、ISO/IEC27001 に基づく認証の対象にもできるので、再(々)委託先にも情報セキュリティを徹底させる事業者として信頼向上につなげることができる。

これらの努力により､サプライチェーンでの具体的な管理レベルや管理策が明確になり、委託先への要請も、やりやすくなった。2.1 で指摘したように、委託先に情報セキュリティを管理させることによる委託先でのコストアップや契約価格への反映をどう評価するかは、情報セキュリティ事故発生のリスクとのバランスで評価可能である。情報の内容によって委託先を使い分けることにより、バランスを取ることができる。

2.4 情報セキュリティ事故による損害賠償

実務的に難しいのは､事故発生時の損害賠償やそれを規定した契約である。

委託先での情報セキュリティ管理に「問題」があったため、情報が漏えいした場合、営業秘密であれば、委託元の事業が競争力を失うし、個人情報であれば、委託元が「お詫びの印」を配布したり、本人たちから損害賠償を請求されたり、といった損害が委託元に発生する。これを委託先

p http://www.meti.go.jp/policy/netsecurity/downloadfiles/outsourcing_guidelines.pdf
(最終閲覧　2017 年 1 月 1 日)
q http://www.meti.go.jp/policy/netsecurity/downloadfiles/kakuduke_youkyuujikou.pdf
(最終閲覧　2017 年 1 月 1 日)
r 情報セキュリティ格付けの内容については、
http://www.israting.com/rating/index.html
(最終閲覧　2017 年 1 月 1 日)
s http://www.jasa.jp/information/sec_supplychain.html　（最終閲覧　2017 年 1 月 1 日）

に求償できるか、という問題がある。元々、システム業界では、システムの開発契約や運用契約に損害賠償額の上限を設けることが多かったため、同様の上限をかけてくることも多く、この上限を巡って交渉が難航することは多い。逆に、中小の事業者であれば、契約では上限のない損害賠償を約束していても、いざ事故が起こるとそれだけの資力はなく、損害賠償できないことになる。委託元がある程度の大企業であれば、損害賠償請求自体が下請けいじめとして社会的非難を受けることも考えねばならないt。

まず、責任分界点の問題がある。

委託元の方が情報システムや情報セキュリティに精通し、具体的な管理策を要請して監査もする場合、具体的に要請されたことができていなければ、もちろん委託先の過失となるだろうが、要請されたことだけをやっていては防げなかった場合、委託先の過失と言えるか、が問題になりうる。契約上、「委託先は善良な管理者の注意義務を持って管理する」ことと定めている場合も多いだろうし、仮に定めていない場合でも、要請されたことだけをやる、ということが明確でない場合は、受託者として、善管注意義務はあるだろう。とはいえ、委託先が中小企業で情報セキュリティの専門性を期待しづらい企業で委託元の方が専門性もあり、委託先の状況を委託元が監査などで知り黙認していたような場合、契約上期待された情報セキュリティレベルは実施していた、として契約の不履行として求償できない場合もあろう。そう考えると、この観点からは、委託先の状況を把握することが得策かどうか、という議論も出てくるかもしれない。

逆に、システム会社ではない企業がシステム会社に委託する場合など、委託先の方が情報セキュリティのスキルがある場合は、委託先の責任が認められる場合が多いだろうu。信用を得るために外部認証を取る、情報セキュリティ格付けを受ける、ことが逆に法律上の言明責任を負わされることになることも考えられる。しかし、そのような法務的な心配をしてアピールを避けていれば、競争に負けるだけではなく、社会的にも評価されない。現実に情報セキュリティにしっかり取り組み、それをアピールしつつ、そのうえで保証の限界をきっちり契約に書くアプローチにすべきである。法的な責任移転に拘泥するよりも、世の中の情報セキュリティレベルを上げることの方が重要で、責任移転の議論ではそれを促進するように展開すべきである。この点は、後述する。

次に、委託先の帰責事由を考えるとき、故意については、組織の故意か、内部の個人の故意か、過失については、ミスか、より高い対策を打つべきだったか、を分けて考えた方がわかりやすい。委託先がコンペティタに情報を売ったり、自らのビジネスに委託元の情報を無断で使用したような、故意・重過失によるものは、現実の回収可能性は別にして、損害賠償請求はできるだろう。委託先が、誤って誤送信した、暗号化していないパソコンを電車に置き忘れた、という委託先のミスによるものでも、委託先としても責任を問われてもやむを得ない、と考えるだろう。メンテナンスを容易にするためにインターネット上にアクセスコントロールすらなくリンクを張らずに個人情報を置いていた、という事故も１０年以上前まではあったが、このレベルでも求償可能だろう。

しかし、防御レベルの不足については、まさに、「善良な管理者の注意義務」を以て管理するとすれば、何をやるべきだったか、の判断になる。というのは、機密性にかかわる情報セキュリティ管理策は、社外や社内からの（計画的か出来心か興味本位か偶然かは別にして）故意の行動（情報にアクセスする、持ち出す）、という脅威に対しての対策だからである。故意に対する完璧な防御はない。管理の裏をかいて情報を窃取するからである。「悪いことをする人はいない」「狙われるはずがない」という単純な性善説による防御レベル不足は論外だろう。しかし、技術の進歩も速く、高度な攻撃方法がブラックマーケットなどを通じて普及し、脅威と防御の鼬ごっこが続く中で、一般的には通常の情報システム部門の人間には具体的な情報は入りにくく、また、一旦入れたシステムなどの改修もそう頻繁にできるわけではない。実際にそこまでして狙われる可能性がどの程度なのか、も読めない中で、コストや現場への負担のかかる対策も難しい、ということもある。だからこそ、ISO/IEC27001でも、情報資産の価値の評価やリスク分析のうえ、リスク判断をして管理策を決める、という抽象的な表現にならざるを得ない。この状況で、一定の情報セキュリティ対策をしている企業が更にどこまでの備えをするのが善良な管理者の注意義務を尽くしたことになるのかの判断は、かなり難しい。しかし、一旦、自社で事故が起こると、真面目な事業者なら原因を分析し、何をやっていれば防げたのか、を分析し、改善策を計画し実施する。この時の分析は、かならずしも善管注意義務のレベルを示したものとは限らない。後知恵で、こうしていれば防げたのではないか、と、考えたものである。このような状況で、委託先に帰責事由があったといえるかどうか、疑問な場合もあろう。

リスク分析をしてリスク判断をして管理策を決める際、その脅威の発生確率が読めないこととコストから、リスクを受容することもよく行われる。これが過失認定において、不利に働かないか、も気になるところである。つまり、そんな脅威があることを認識していたのに対策をしなかった、という使われ方をするかもしれない(米国においては、懲罰的賠償の根拠にも使われ得る。)また、リスク対応計画をマネージメントレビューで担当取締役や社長が承認したことが、株主代表訴訟で不利に使われるかもしれない。これら

t 経済産業省のガイドラインでも、注意すべき点として、指摘している。前掲注 m
u東京地裁　平成 26 年 1 月 23 日　判時 2221 号 71 頁

を考え合わせると、もしかしたら、ある程度のレベルで対策してきた事業者にとって、情報セキュリティ事故の責任は、事実上、無過失責任、結果責任になりつつあるのかもしれない。

2.5 製造物責任からの示唆と提案

無過失責任や後知恵での非難、というと、製造物責任と似たところがあるように思われる。テレビセットからの出火、という、明らかな欠陥はともかく、米国の PL 訴訟では、機器に関連して怪我をすると、後知恵で欠陥の主張がなされることも多いし、陪審たちは、被害者への同情から欠陥認定をすることも多い[v]。その意味では、状況としては類似点がある。生命身体財産に直接被害を及ぼしてしまうため、無過失責任で賠償責任を負わせ、弱い消費者と強い(?)メーカーとの間で損害の負担のバランスを取り、また、経済的圧力により安全性の改善を促す製造物責任と、一般的にはそこまでの被害には至らない情報セキュリティ事故とは、規範としては同等とすべきとは考えられない。しかし、過失があったと非難されることなく何らかの是正に向かわせる制度としては参考になる部分があると考えられる。

責任認定の観点と、サプライチェーン内での責任の負担、という観点から検討する。

2.5.1 責任認定の観点

責任認定に製造物責任の概念は参考として使えるだろうか？

製造物責任では、「本質安全設計」の努力をしても解決できないものを使用上の警告として製品や取扱説明書に書くことによって責任を免れることもできる。情報セキュリティにおいては、むしろ、低いセキュリティレベルしかないことを書いて、サービスの選定時に考慮してもらうことはできるかもしれない。コンピュータやネットワークのビジネスであれば、それは可能だが、特に消費者の個人情報を扱うビジネスでは現実的ではない。

欠陥認定に関し、日本の製造物責任法では、開発危険の抗弁があり、当該製造物をその製造業者等が引き渡した時における科学又は技術に関する知見によっては、当該製造物にその欠陥があることを認識することができなかった場合には、製造物責任はないとされている。開発、提供時の品質については、同様の議論は当てはまる。しかし、引渡しによって供給者の手が届かなくなった製品と、システムを手元におきつつサービスを提供している場合とは同じともいえないであろう。システムをアップデートすることによって、情報セキュリティレベルをあげることは可能だからであるが、一定のリードタイムは認められるべきであろう。科学又は技術に関する最先端の研究者の知見だけでなく、そのような攻撃方法やセキュリティホールの存在、活用の容易さの変化、具体的攻撃の発生頻度などが、一般の情報システム部門の情報セキュリティにかかわる人にも知られるようになることを基準とすると、情報セキュリティにおいても使えるかもしれない[w]。これを前提とすると、無過失責任ではなくなるのかもしれないが。

また、アメリカの PL 訴訟では、事故後、製品を改善したことを欠陥があったことの証拠としては使えないという判例が活きている。もしそれを証拠とできるなら、メーカーは改善をためらい、結果として、安全な社会を作るという製造物責任の目的が損なわれるからである。この点も、情報セキュリティ事故発生後の後知恵での反省を責任論に使うべきかどうかに参考になるだろう。

2.5.2 サプライチェーン内での責任の負担の観点

サプライチェーン内での損害賠償はどうだろうか？

日本の製造物責任法では、第 4 条第 2 項で、「当該製造物が他の製造物の部品又は原材料として使用された場合において、その欠陥が専ら当該他の製造物の一製造業者が行った設計に関する指示に従ったことにより生じ、かつ、その欠陥が生じたことにつき過失がない」場合には、製造物責任はない、とされている。これは、前述の、委託元から要請された管理策を実施していても情報セキュリティ事故が発生した場合の責任に参考になるかもしれない。しかし、情報セキュリティ管理策の知識が普及してくると、よほどの小さな企業でない限り、言われていないからやらなかった、ということが通じないことも多いだろう。結局、「専ら」の認定での調整になるのだろう。

アメリカの PL 訴訟においては、完成品について PL 訴訟が提起されたとき、完成品の「製造業者等[x]」は、OEM 製品の供給者はもちろん、原因がどこにあるかわからない段階でも、すぐに上流工程の部品の供給者に通知をし、共同で防禦できるようにすることが多い。契約上も、直ちに通知しなければ、部品業者の防禦機会を失わせることになるので、求償できない、という規定をおくことが多い。この規定と共に、供給者は契約で定められた額以上の PL 保険を付保し製造業者等を被保険者とする義務なども定めら

[v] 例えば、ガスコンロにつながる配管を子供が足で押したため上に乗っていた鍋がひっくり返って子供がやけどをした場合、五徳の足の数が 3 本だったのが欠陥、と主張され、そのような使用環境が通常の使用か、それを予測すべきだったか、が争われたが、子供の火傷の写真が出されるとわかると、陪審の反応が予測され、高額で和解するなど。

[w] 欠陥認定に使われる、製品の有する効用と危険を比較して後者が前者を上回れば欠陥ありとする「危険効用基準」も、効用はインターネットを通じて便益を享受できる、という点であり、かならずしも情報セキュリティリスクとオフセットのものではない。ましてや、「消費者期待基準」は、情報セキュリティ事故がないことが消費者期待ということになろう。

[x] ここでは、日本の製造物責任法における「製造業者等」の概念と同じ者として使う。
一　当該製造物を業として製造、加工又は輸入した者（以下単に「製造業者」という。）
二　自ら当該製造物の製造業者として当該製造物にその氏名、商号、商標その他の表示（以下「氏名等の表示」という。）をした者又は当該製造物にその製造業者と誤認させるような氏名等の表示をした者
三　前号に掲げる者のほか、当該製造物の製造、加工、輸入又は販売に係る形態その他の事情からみて、当該製造物にその実質的な製造業者と認めることができる氏名等の表示をした者

れることが多く、OEM 製品のようなサプライチェーン内での責任の切り分けが不要なものでは、製造業者等に代わって訴訟を遂行し製造業者等を防禦する義務まで定められていることも多い。結局のところ、被害者への損害賠償をサプライチェーン内で求償するというより、被害者との訴訟で必要となる訴訟費用や調査費用を、サプライチェーン内の誰の保険でカバーするかの問題に帰着させ、まずは被害者との訴訟に注力し内輪もめにあまり労力をかけない仕組みである。もちろん、保険を使うことで以降の保険料が上がるといった経済的影響は考えられるし、保険会社間での求償問題もありうるが、貸し借りのある保険会社のプロの間の求償は、内輪もめに多大な労力を割かない、合理的な方法ともいえる。

このような保険による解決は、前述した様々な課題への示唆にもなる。

前述のように、システム契約からの伝統の、損害賠償額の上限設定も、一旦事故が起こると大きな損害となるから考えられたものであるが、保険料であれば、ある程度負担できるだろう。また、中小企業への求償が社会的に非難される懸念についても、保険間の問題で会社が潰れる心配がない、という前提ができれば、社会的なコンセンサスが得られるのではないか。委託先の管理状況の把握が委託先への責任転嫁の支障になるかもしれない、という懸念も、把握し本当に長年黙認していたのであれば元々そのリスクは委託先に移転していないといえるし、そうでなければ、万一の場合の責任移転ができないことを恐れて把握しないよりも、双方の保険で処理すると割り切って、把握し改善を促すことを促進するほうが、サプライチェーン全体の情報セキュリティレベルを上げ、リスクを減らすことにつながると思われる。

また、委託先が、認証取得や情報セキュリティ格付けをアピールすることによる言明責任の懸念も、むしろ、契約の中で、保証の限界を決めることで解決すべきである。保険により大きな損害賠償の懸念を払しょくし、安心して、情報セキュリティに真摯に取組んでいることを競争力の一つとできるようにすることが、世の中の情報セキュリティレベルをあげる上げることにつながると思われる。

勿論、保険にも限界はあるし、保険に甘えて情報セキュリティ強化を怠るようでは本末転倒である。現在も行われているように、保険会社は、その会社の情報セキュリティの取組を審査し、よく取組む事業者は保険料が下がり、怠る事業者は保険料が上がる仕組みを持たねばならない。あくまでも、あたかも無過失責任に近い状況への対応からの提案である。

3. 製品セキュリティ

冒頭の事例の、⑵－３、⑶のような、納入される製品の製品セキュリティは、取引の観点からは、基本的には品質保証の問題である。例えば、インターネットカメラに DDoS 攻撃の踏み台にされるような脆弱性があるようなケースであるy。しかし、故意にバックドアが埋め込まれていた場合などは、影響が非常に大きいため、注目されている。

中国、米国、ロシアなどが国家間の諜報にサイバー上のハッキングを使っているという報道があるz。また、2015 年 2 月、ロシアのセキュリティ会社であるカスペルスキーは、米系のシーゲートやウェスタンデジタル、記事によっては東芝の、HDD のファームウエアに、某国の機関（同社は米国の NSA を示唆）がアクセスできるバックドアが埋め込まれている、と公表したaaが、2012 年には、中国の華為技術と中興通訊のネットワーク機器は中国政府が米国の通信に対するスパイ行為やサイバー戦争を行うために利用される懸念があるという報告書を米下院情報特別委員会が出しているbb。

中国政府は 2009 年、CCC という同国の安全基準・認証制度の対象に IT セキュリティ製品を加え、少なくとも政府調達については、ソースコードの開示を求める対策ccを取っているが、米国でも、日本でも、政府調達については、その上流も含め、このような問題がないかを保証させるような動きが出ている。日本においては、2015 年 5 月、NISC が「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を策定ddしている。

製品セキュリティにおいても、実務上は、①契約上の手当、②実務上、求めるレベルをどうするか、③情報セキュリティレベルの確認・監査、④情報セキュリティ事故発生時の対応と損害賠償、の問題がある。また、責任を考える際、（契約で求められる）品質レベルをどう考えるか、と、帰責事由を分けて検討した方が、わかりやすいと思う。帰責事由も、情報管理の場合と同様、故意については、組織の故意か、内部の個人の故意か、過失については、ミスか、より高い対策を打つべきだったか、を分けて考えた方がわ

y 「大規模 DDoS 攻撃は防犯カメラが踏み台に、中国メーカーがリコール表明」IT メディアエンタープライズ 2016 年 10 月 25 日 http://www.itmedia.co.jp/enterprise/articles/1610/25/news059.html （最終閲覧 2017 年 1 月 18 日）

z 例えば、ロシア政府が米大統領選に干渉するためサイバー攻撃を仕掛けたとして、米国駐在のロシア外交官 35 人が国外退去を命じられた。日本経済新聞 2016 年 12 月 30 日 http://www.nikkei.com/article/DGXLAS0040001_Q6A231C1000000/ （最終閲覧 2017 年 1 月 18 日）

aa http://www.gizmodo.jp/2015/02/nsa_9.html （最終閲覧 2017 年 1 月 4 日） https://www.techpowerup.com/209925/nsa-hides-spying-backdoors-into-hard-drive-firmware （最終閲覧 2017 年 1 月 4 日）

bb 「Report: Chinese Tech Firms Should Be Viewed With Suspicion, Barred From U.S. Networks」WIRED 2012 年 10 月 8 日 https://www.wired.com/2012/10/chinese-telecoms-suspicious/ （最終閲覧 2017 年 1 月 18 日）

cc 突然提案された当初の案では、すべてのセキュリティ製品を対象としていたが、先進工業国は知的財産権侵害として反対し、最終的には政府調達のものに限定された。読みようによっては、ネットワークにつながるすべての製品、と解釈し得る点にも懸念があった。

dd http://www.nisc.go.jp/active/general/sbd_sakutei.html （最終閲覧 2017 年 1 月 4 日）

かりやすい。

3.1 品質レベルの考え方

契約上、仕様書などで具体的な要求品質を定める、検査仕様を定めるような場合は､品質レベルに迷うことはない。また、業界や IPA などが様々な具体的な基準を定めるようになるとあまり争いはないだろう。これらがない場合、また、それほど詳細に定めていない場合、何が求められる品質レベルかが問題になる｡1 対 1 の場合もさることながら、特に、個別の契約が成立しにくい大衆向けの製品で、より判断が難しくなる。

故意にバックドアを作る、マルウエアを埋め込む、ということは、明らかに契約上の求める品質レベルを満たしていないが、脆弱性があるのかないのか、については判断が難しい。攻撃のレベルが上がり、また、解析技術が上がると、従来は脆弱性でなかったものが脆弱性になるからである。これを契約上求める品質レベルを満たさない、とすると不可能を要求することになる。求められる最も高い品質レベルとしては、使われ方を想定しながらリスク分析し、そのリスク分析に基づいた機能要件を満たし、IPA などで警鐘がならされているものはもちろん、JPCERT やメーカーなどにより公開されている脆弱性は対応しており、市場に頒布された後も（完成品メーカーが配信環境を整えることが前提だが）脆弱性が発見されたときに契約で定める期間、アップデートをする、ということだろう。

特に、ネットワークにつながる家電など、従来の「システム」でない製品の場合、アップデートの期間が問題となる。情報システムの場合、昔から、バグのないソフトウエアはない、とされ、サポートは有料か、普及型の PC の OS やアプリなどでは、その製品の販売終了から長くて 5 年ほどで終了する。後は、ユーザーは、業務で使用するか、消費者であってもある程度情報リテラシーのある人が前提であり、その拘束力についていろいろ議論はあるものの、利用開始時に免責条項の入った利用契約に合意しており、ユーザーの自己責任、という文化もできている。PC はユーザーから見てもソフトウエアが製品と分けられるので、製造物責任はあまり心配ない。家電の場合、ユーザーから見て機器とソフトウエアとは一体であり、メーカー保証は 1 年でも､製品事故が起これば引渡しから 10 年間は製造物責任が問われることになる。システムと違って自己責任の文化はなく、むしろ、ユーザーが子供からお年寄りまでの「弱き消費者」であるため、メーカー責任の文化がある。ディスプレイのあるネット家電なら、初期設定に利用契約を出すことは可能だが、電気屋さんがセットしてしまう場合も多く、ディスプレイのないものも多い。結局、契約での免責と言っても取扱説明書や同梱の契約でシュリンクラップ契約的な契約にならざるをえない。

この違いの中、新たに発見された脆弱性は、製造物責任法上[ee]は開発危険の抗弁が可能かもしれないが、企業にとってお客様対応から考えると、対応するか、接続機能を止めて安全側に倒すか、契約前にかなり大きな警告を書いて認知させるか、しかない。今後、車をはじめ IoT の消費者による利用が進んでいく中、ますますそのような物が出てくると思われる。

また、ホワイトハッカーに脆弱性を指摘された場合、対応するのかどうかの判断も難しい。ある程度条件が重なったときに脆弱性が突かれるとか、突かれたとしても今の使用法なら被害は大きくない、というときには対応をしないこともある。しかし、それが後日、問題になると、脆弱性を知っていて放置した、という判断になることも考えられる。従って、対応しないという判断をするときは、実務としては、それなりのリスク分析の根拠を残して置くべきであり、用途・環境の変化でリスクが変化して、損害が大きくならないか等のリスクの変化モニタリングの継続が必要となると考える。

3.2 契約と品質管理・内部管理

製品セキュリティ確保のためには、契約上、納入される製品に求める品質だけを義務付けるのでは不足となる。というのは、受入検査で製品セキュリティ上の問題がないことをチェックするのは容易ではないからである。

マルウエア解析と同様、検査には、動的分析（ブラックボックステスト）と､静的分析（ホワイトボックステスト）があるが、動的分析では完全に脆弱性を把握できず、特に故意に埋め込まれたものは、サンドボックスでは動かない対策もされているものは見つけるのが困難である。静的分析にはかなりの工数がかかり、あまり現実的ではない[ff]。

そうなると、調達先に内部管理や開発（再）委託先への同様の内部管理を求め、更なる再委託先にも同様に義務付け、その後も同様とする、ということが必要になる。調達先が更に調達するソフトウエアやデバイス、更には開発ツールについても、製品セキュリティ上の問題のないことの保証を要求することになるとも考えられ､同様の理由から、結果としての製品の保証だけでなく、内部管理も求めることになり、その再調達先にも同様の保証を求めることを要求することになる。ちょうど、RoHS 規制や CSR 調達[gg]と同様の規定となると考えられる。ただし、直接品質に影響するところが、異なる。

では、どのような内部管理が必要となるか。これを、前

---

ee もちろん、それにより生命身体財産に損害があった場合、だが。そもそも、脆弱性が事故につながるのは、攻撃者という第三者が介在する場合であり、守りが弱い、ということが欠陥なのかという議論は、日本ではあるだろう。アメリカではすべて判例法なので、当然原告弁護士はそう主張し、それが法律問題とされれば裁判官が判断するが、事実問題とされれば陪審が原告を勝たせたいと思えば欠陥になってしまう。

ff 解析ツールはあるものの研究段階である。

gg 例えば電気・電子業界では、EICC（電子業界行動規範： Electric Industry Code of Conduct）などがある。

述の帰責事由の分類毎に検討する。

ソフトウエアやソフトウエアの入った部品の調達先が故意にマルウエアを仕込む場合は、帰責事由があることは明確だが、立証に困難を伴うだろう。結局、調達先を選ぶ段階から注意せよ、ということかもしれない。昔、某宗教団体の運営するシステム開発会社に警察も含め官公庁や企業等から、約 160 のシステム開発を受注していたことが問題となったhhが、前述の NISC の手引書では中立的客観的な記述に留めているii。

最もあり得るパターンとして、調達先の従業員、派遣社員などの故意による場合が想定される。それに対しては、身元確認の他、複数担当者による相互監視、操作ログの確認、などの内部者牽制を含む管理jjを求めることになる。身元確認問題は、ISO/IEC27002 などでも求められるもので、欧米では人権に配慮しつつも合理的なものと捉えられているようだが、日本では、人権とのバランスが物議をかもすため、実効的ではない。民間企業が行う場合は、私人間の憲法上の権利のバランスであり、政府調達品、特に国防、国家機密、社会安全、社会インフラに関するもの、それらに採用され得る汎用品、広く社会に普及する汎用品については、認められるべきであろう。もちろん、その手法と判断において不当な差別とならないような注意は必要だろうkk。

調達先のミスによるものは、当然、情報セキュリティやシステム品質確保体制の要請が必要だが、前節冒頭に述べたように、求める品質が何かを具体的に詳細に合意しておかなかった場合には過失を問えるかどうかが問題になろう。

調達先が、どこまでの高い対策を打つべきか、は、品質レベルの合意をしっかりしておけば、開発プロセスについては、前述の内部・外部の故意の犯行がありうる、という点以外は、ソフトウエアの品質管理の問題と同じではないかと考える。

前述のとおり、品質レベルとしては、①リスク分析し機能要件化する、②その機能要件を満たし、③わかっている脆弱性には対応し、④セキュアコーディングの注意点には対応し、⑤市場に頒布された後に脆弱性が発見されたときにアップデートできる、ということになると思われる。⑤は基本的には下流行程との契約によることになるだろうが、②、③、④は、品質管理の問題に帰着できる。

①については、ISO/IEC15408 のセキュリティ機能要件や政府調達における情報セキュリティ要件設定マニュアルの付録 A、IPA の開発者のための解説書シリーズなど、様々な手引きがあり、下流行程とは無関係に対応すべきものも多いとは思われる。しかし、ISO/IEC15408 のセキュリティターゲット策定と同様、下流行程のなかでの使われ方で決めていくべきものもある。例えば、①には、

ｉ）例えば初期パスワードを同一にするかどうかなど、使われ方に余り左右されないもの、

ii) 初期パスワードを変更しなければ危ないことを知っているかどうかなど、調達者を含む下流行程の利用者の知識がなければ脆弱となるもの、

iii) 下流行程のシステムや最終ユーザーの使われ方を想定すると脆弱となるもの

が考えられ、ii)iii)は当然下流行程（調達者）との関係で情報セキュリティ要件（汎用品ならどのような情報セキュリティ仕様のものを選択してもらうか）を詰めなければならないが、i)についても対応すればコストが上がるため、結局、調達者にレベルを説明して選択してもらうことが必要となる場合もある。こうすることによって、ベンダと調達者の間の責任分界点を明確にすることもできる。

とはいえ、契約で対応するとしても、実際に事故が起こるのは、ベンダ側から見れば想定していない使われ方によることが多く、製造物責任における部品供給者と製品製造者のような問題やその解決手法などが参考になるだろう。ただ、ソフトウエア（製品）については、元々バグのないソフトはない、という論法で伝統的に品質保証を避けてきており、部品供給のような緊張関係はないかもしれない。それだけに、調達する側が、しっかりとした要求仕様を提示する必要がある。

内部、外部からの故意の犯行を想定した内部管理、という意味では、ISO/IEC27001 で完全性と機密性の観点からプロセスのリスク分析をして、内部管理の内容を検討するアプローチが良いのではないか。また、事故発生時の対応において最も大事なことは、サプライチェーン内でのトレーサビリティである。その不正プログラムがどのソフトに入っていたのか、どこで混入したのか、誰が開発や試験に従事していたのか、を突き止められるような記録と管理体制が重要である。不正プログラムでなくても、例えばあるミドルウエアに脆弱性が発見されたとき、それを自社製品で

---

hh http://www.npsc.go.jp/info/3_16.html（最終閲覧　2017年1月14日）

http://www.asyura2.com/sora/bd5/msg/696.html　（最終閲覧　2017年1月14日）

ii 開発の外部委託についてだが、選定にあたっては、下記を考慮
①サプライチェーン全般における機能的な管理体制、管理プロセスが委託元に対して透明化・可視化されている委託先を選定する。
② 委託元において、サプライチェーン・リスクを増大させる要因となる脆弱性の有無等を確認するために必要な、委託先及び再委託先で委託事業に従事する者の身元や専門性等の情報を提供することができる委託先を選定する。
③ 委託先を選定するに当たり、組織における人の権利、義務、業務内容等、業務を進める上での手順、情報セキュリティに対する組織文化に関する過去の実績を考慮する。
④ 再委託先を管理するための手順が明らかであり、当該手順により再委託先を管理する能力を有すると認められる事業者を選定する。
⑤ 委託事業の実施において、情報セキュリティインシデントが発生した場合、情報セキュリティ監査を受け入れることが可能な事業者であって、委託元からインシデント対応結果や再発防止策の実施等を求められた際に、必要な情報を提供可能な事業者を選定する。
内閣サイバーセキュリティセンター（NISC）「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」８頁（2016 年 10 月 25 日）

jj NISC 前掲注 ii）12 頁

kk 人選時だけでなく、その後も、ギャンブルにおぼれている、借金がある、急に金回りが良くなる、などの兆候に注意することなども、よく指摘されている。

使っているかがすぐにわかり、すぐに供給元に対応を要請することができなければ、結局、ユーザーが情報セキュリティ上のリスクに晒され被害を受ける。これらができるような管理を調達先に要請する必要がある。

多くの調達先に対し個別に確認することが難しい、調達先にとっても複数の提供先からバラバラと監査に来られるのは困る、という観点からは、情報管理の場合と同様、外部認証や格付け的なものが有効と考えられる。ISO/IEC15408 外部認証は、上述のセキュリティ機能要件関連も開発プロセスの監査もあり、有益と思われる。なお、政府調達においても、ISO/IEC15408 を取得している製品の優遇を選定基準にすることが有益、とされているll。

勿論、これらの確保はコストにも跳ね返るが、リスクとのバランスを考えて判断することになる。また、認証取得製品が増えると、その間での競争も促進されるので全体的なコストも下がるはずで、長い目で見れば世の中がセキュアになることにつながる。

4. 最後に

サプライチェーンと情報セキュリティについては、この他にもクラウドサービスの利用や、約款による外部サービスの利用など、論点は様々にある。クラウドサービスの情報セキュリティについては、ISO/IEC27017 ができており、ベンダに要求するだけでなく、約款により、個別の交渉が難しいことを前提として、セキュリティレベルを見て選択することによるセキュリティ確保も、手法として示されている。

情報セキュリティの規範を一般的に強制するのは難しい中、契約や取引を通じた規範の強制と確認の連鎖により安心できるシステムやサービスが提供され、正しく対応している事業者が選ばれることで安心が促進される。そのためにも、サプライチェーンの参加者に合理的な責任分界と保険を活用した合理的な責任負担方法が定着することが望まれる。

謝辞 ご多忙の中ご指導いただいた演習指導の原田教授、及び後方支援頂いた研究室の湯淺教授に感謝申し上げます。

ll内閣官房 内閣サイバーセキュリティセンター「府省庁対策基準策定のためのガイドライン（平成 28 年度版）」127 頁、142 頁