Vol.2020-EIP-87 No.5
2020/2/14

情報資産の廃棄問題におけるセキュリティ管理と法的課題について

原田要之助[†1] 板倉陽一郎[†2]

概要 自治体からリースバックされたサーバのハードディスクが廃棄業者から盗み出されてオークションで販売されるという事件が発生した．ハードディスクは，自治体が管理している企業の納税情報や住民及び自治体職員の個人情報などを取り扱う情報システムで使われていた．自治体は簡易な初期化をして，リース会社に廃棄を依頼した．リース会社は専門の廃棄業者に再委託した．この再委託先から盗まれた．この自治体，廃棄業者は，重要な情報が流出したとして会見を行い謝罪した．本稿では，この問題を取り上げ，情報セキュリティのマネジメント及び法的な観点からそれぞれ問題点を提起する．

キーワード：情報セキュリティマネジメント，情報資産の廃棄，外部委託管理

A study on the disposal of secured asset from security managment and regal aspect

Harada Yonosuke[†1], Itakura Yoichiro[†2]

1. はじめに

2019 年に富士通リース株式会社（以下では，富士通リースという）が神奈川県庁にリースしているサーバに利用されているハードディスク装置（以下では，HDD という）が利用期限となったため，自社にリースバックした．神奈川県では，HDD に簡易な初期化を実施して引き渡した．富士通リースは，その後，HDD の内部のデータの破棄を株式会社ブロードリンク（以下では，ブロードリンクという）に委託した．ブロードリンクの社員が不正にこの HDD を盗み出してオークションサイトに出品した．オークションで入手した人が，HDD を調べたところ，神奈川県の公文書が復元できたことから朝日新聞社に情報提供した．

この事件については，現在，情報化を進めている自治体や企業にとって，情報のライフサイクル，情報セキュリティ管理や法的な問題について様々な問題を提起している．事件は 2020 年 1 月の執筆時点における公開情報をもとに学術的な観点から，課題について述べる．

2. 事件について

2.1 概要

2019 年 12 月 6 日に朝日新聞で事件が報道され事件が発覚した，（図 1 に示す）．

納税などに関する大量の個人情報や秘密情報を含む神奈川県庁の行政文書が蓄積されたハードディスク（HDD）が，ネットオークションを通じて転売され，流出していたことが朝日新聞の取材で分かった．県のサーバーから取り外された HDD のデータ消去が不十分なまま，中古品として出回っていた．県によると，データの消去から廃棄までを請け負った業者の社員が，転売に関与したことを認めているという．

流出した HDD は，本来は復元できないように業者が破壊処理するはずだったものだ．行政が保管する膨大な個人情報が流出するという，ずさんな情報管理の実態が明らかになった．

転売された HDD は縦約 15 センチ，横約 10 センチ，厚さ約 2.5 センチ．少なくとも 9 個あり，この中に保存されたデータの容量は 27 テラバイトに上る．仮に画像を添付したメール 1 通を 3 メガバイトとすると，900 万通に相当する．神奈川県が調査を続けているが，情報流出の事案としては世界でもまれな規模に上る可能性がある．

県が確認したところ，HDD は県庁内の各部局の情報を蓄積する共有サーバに使われていた．中には，法人名が記載された税務調査後の通知や，個人名や住所が記載された自動車税の納税記録，企業の提出書類，県職員の業務記録や名簿類などが含まれていた．

県によると，転売されていた HDD は，県が富士通リース（東京都千代田区）から借りたサーバに使われたもので，今春に交換時期を迎え，サーバから取り外された．富士通リースは県との契約に基づき，データを復元不可能な状態にする作業を，情報機器の再生事業を手がけるブロードリンク（同中央区）に委託．同社に対し富士通リースは，破壊して作動しないようにしてから廃棄するか，データを完全に消去するよう指示していた．

県からブロードリンクに引き渡された時点で，HDD には簡易なデータ消去（初期化）が施されていた．HDD は都内にあるブロードリンクの施設で保管されていたが，データの消去作業の担当者が一部を持ち出し，オークションサイトに出品したという．

出品されていた HDD 9 個を，IT 企業経営の男性が仕事に使おうと落札．使用前に安全性を確かめるため男性が中身を確認したところ，データの存在に気づいた．復元ソフトを使うと，神奈川県の公文書とみられる大量のファイルが保存されていたという．

男性からの情報提供を受け，朝日新聞が 11 月 27 日に県に情報流出の可能性を指摘．HDD に記されていた製品番号から，県のサーバーに使われていた実物と分かった．

図 1 朝日新聞から([1]より)

†1 情報セキュリティ大学院大学客員教授, Institute of Information Security
†2 ひかり総合法律事務所 Hikari Sogoh Law Offices

また,事件について日経新聞では，図 2 に示すように述べている．日経新聞では，ブロードリンクから持ち出された HDD が神奈川県の案件のみならず，多数の官公庁からの廃棄が委託されているとしており，この事件が特殊な事例ではないことを示唆している．

個人情報を含む神奈川県の大量の行政データが蓄積されたハードディスク（HDD）が転売され，外部に流出する恐れのあることが 6 日分かった．県のサーバーを更新した際，取り外された HDD の廃棄を委託された事業者の社員がデータ消去の不十分な状態で一部を持ち出し，ネットオークションで販売した．データ量は最大 54 テラバイトに上る可能性があるという．
富士通リースは「現時点でコメントできることはない」としている．ブロードリンクの幹部は取材に対し，流出があったことを認めた上で「現時点では詳細を説明できない」と話した．
ブロードリンクのウェブサイトには「主要取引先」として，複数のメガバンクや大手電力会社の社名のほか最高裁，防衛省などが挙げられている．

図 2 日経新聞から([2]より)

2.2 神奈川県の対応

神奈川県では，2014 年に富士通リースとリースを契約し当該ファイルサーバで HDD の利用を開始した．県の発表によると，県庁の物理的セキュリティが施されたところに設置しており，庁内で利用するものであることや，様々な分野のデータを扱うため，暗号化せずに利用してきた[3]．
2019 年 2 月にリース契約が終了したことから，神奈川県はファイルサーバをリプレースすることを決め，富士通リースにリースバックした．その際に，ファイルサーバのファイルをすべて削除した[3]．なお，この処理は通常のものであり，復元ソフトにより復元が可能である．
オークションサイドから HDD を落札した人が HDD に残存データを確認して，復元して，神奈川県庁の情報ではないかと疑い，12 月 5 日に新聞社に情報提供するとともに，県庁に届けた．これを受けて，2019 年 12 月 6 日に朝日新聞が報道，神奈川県が公表した．以降の神奈川県庁からの情報をもとに経過を図３に示す．

12 月 6 日（発表）：リース契約満了により返却した HDD の盗難について
12 月 7 日（発表）：盗難された 18 本以外の HDD は，溶解処理や解体処理されており，外部に持ち出されていない
12 月 12 日 県民からの「お問い合わせ専用ダイヤル」の設置
12 月 16 日（知事会見）事件の概要と再発防止策について
12 月 20 日（発表）所在不明の HDD の一部回収について
12 月 21 日（発表）：所在不明の HDD の 18 台全体の回収について
12 月 24 日（知事会見）：県のデータが入った HDD の盗難
12 月 27 日（発表）：HDD から復元されたデータの消去等について
2 年 1 月 6 日（発表）：新たな被害は確認されていない

図 3 神奈川県の公式発表から(県庁 web サイト[3]による)

神奈川県は，今回の事件に関しては，自分たちの情報セキュリティ管理が甘かったことについては初期の段階で反省の意を示しており，HDD を回収できたこと，HDD の内容の漏えいが確認できないことから事件の早期の幕引きを図っている．

2.3 富士通リースの対応

富士通リースは神奈川県のリースが終了したファイルサーバについては HDD を廃棄するようブロードリンクに依頼した[1]．リース契約には，データが完全に消去されたことを示す証明書を県に提出する内容も含まれている[1]が，富士通リースは HDD の廃棄を依頼しているが，証明書の発行をブロードリンクに依頼していなかったとみられる．富士通リースは，情報処理設備のリースをしているだけで，設備がどのような目的で利用されるか，また，情報のライフサイクルには関与しない．また，リース期間が終了するときには，資産の管理者として設備をリースバックする．この際には情報などが残っていることはありえない，すなわち，リース設備を利用する方の責任で確実な消去をする必要がある．しかし，今回は神奈川県から HDD の廃棄を依頼されたとされている．オプションとしてリース契約にデータ消去が追加されているのであれば，契約の履行という観点での HDD に関する責任があると考える．

2.4 ブロードリンクの対応

ブロードリンクは 2019 年春に，富士通リースからファイルサーバを引きとった．廃棄する他の HDD と併せて廃棄処理待ちとした[4]．
今回，ブロードリンクの社員が廃棄処理待ちとなっている多数の HDD から抜き取って詐取していた．神奈川県の HDD も持ち出されてオークションサイトに出品されて販売された．ブロードリンクでは，この社員が入社してからオークションで落札された 3904 個を追跡して情報補漏えいを調査した．12 月 9 日には,神奈川県の HDD からの情報の流出はないとした．12 月 20 日には，持ち出しのないような個別の廃棄処理待ち HDD の管理方法，廃棄作業の可視化，破壊の作業の確認，作業工程の管理，作業員の持ち物に検査などの具体的な改善策を発表している[5]．
フロードリンクは従業員に不正を働かれた被害者ではあるが，一方，情報セキュリティ管理の観点からは従業員に対する管理や情報資産の管理面での責任がある．これについては，次章で分析する．

12 月 6 日（発表）：ブロードリンクが会見を開き謝罪．
12 月 9 日（発表）：現時点で神奈川以外に情報流出確認されず
12 月 20 日（発表）：再発防止実施内容について発表[5]

図4 ブロードリンクの発表から([5]より)

2.5 監督機関の対応

総務省は，この事件が表面化した 12 月 6 日に，本事案にかかる「情報システム機器の廃棄等時におけるセキュリティの確保について」(12 月 6 日付け事務連絡) を全国の全国自治体に通知した．この内容を図 4 に示す．

・物理的な破壊，または磁気を用いたデータの消去
・処理作業完了まで職員の立会

図 4　令和元年 12 月 6 日付け総務省自治税務局電子化推進室事務連絡より（抜粋）

総務省のこの異例に素早い対応は，この問題が神奈川県にとどまるものではなく全国の自治体の共通の問題と捉えた対応と見られる．

2.6 ISMS の認証について

今回の事件の関係者である神奈川県，富士通リース，ブロードリンクともに ISMS 認証を受けている．なお，ISMS は事業所の情報セキュリティマネジメントの状態について評価するものであり，マネジメントが不十分なことから問題が発生したときには処分が下される．2020 年 1 月中旬時点ではブロードリンクのみが停止処分となっている．

2019 年 12 月 6 日に報道された「株式会社ブロードリンクにおける従業員の不正行為による個人情報流出」の不祥事に関する報道内容につきまして，BSI グループジャパン株式会社の ISO 27001 の認証取得企業である株式会社ブロードリンクに対して 2019 年 12 月 24 ?に臨時審査を?いました結果，マネジメントシステムの不適合の是正処置とその有効性が確認できるまで，ISO 27001 の認証を一時停止することを 2019 年 12 月 25 日に決定しました

図 5 BSI の発表から（web サイトによる）

3. ISMS の管理策からの問題点について

3.1 関連する管理策について

ここでは，JIS Q.27002 の管理策から今回の問題に関連するものを抽出して，観点について述べる．

6.2.1 情報の分類
管理策
情報は，法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類することが望ましい．
実施の手引
情報の分類及び関連する保護管理策では，情報を共有又は制限する業務上の要求，及び法的要求事項を考慮することが望ましい．情報以外の資産も，その資産に保管される情報，処理される情報，又は他の形で取り扱われる若しくは保護される情報の分類に従って分類することができる．

6.2.2 情報のラベル付け
管理策
情報のラベル付けに関する適切な一連の手順は，組織が採用した情報分類体系に従って策定し，実施することが望ましい．
実施の手引
情報のラベル付けに関する手順は，物理的形式及び電子的形式の情報及び関連する資産に適用できる必要がある．ラベル付けは，分類体系を反映していることが望ましい．・・手順では，媒体の種類に応じて，情報がどのようにアクセスされるか又は資産がどのように取り扱われるかを考慮して，ラベルを添付する場所及びその添付方法に関する手引を示すことが望ましい．・・従業員及び契約相手に，ラベル付けに関する手順を認識させることが望ましい．
取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には，適切な分類ラベルを付けることが望ましい．

6.2.3 資産の取扱い
管理策
資産の取扱いに関する手順は，組織が採用した情報分類体系に従って策定し，実施することが望ましい．
実施の手引
情報を分類（8.2.1 参照）に従って取り扱い，処理し，保管し，伝達するための手順を作成することが望ましい．
この場合，次の事項を考慮することが望ましい．
a) 各レベルの分類に応じた保護の要求事項に対応するアクセス制限をする．
b) 資産の認可された受領者について，正式な記録を維持する．
（略）

（1）資産の分類とラベル付け

資産の取扱いの手順については，分類とラベル付けをベースにした情報のライフサイクル全ての段階を対象に手順が策定されている(6.2.1，6.2.2)．これをベースに情報分類体系を策定して運用し記録を維持するとなっている(6.2.3)．

8.3.1 取外し可能な媒体の管理
管理策
組織が採用した分類体系に従って，取外し可能な媒体の管理のための手順を実施することが望ましい．
実施の手引
取外し可能な媒体の管理のために，次の事項を考慮することが望ましい．
a) 再利用可能な媒体を組織から移動する場合に，その内容が以後不要であるならば，これを復元不能とする．
b) 必要かつ実際的な場合には，組織から移動する媒体について，認可を要求する．また，そのような移動について，監査証跡の維持のために記録を保管する．
c) 全ての媒体は，製造業者の仕様に従って，安全でセキュリティが保たれた環境に保管する．
d) データの機密性又は完全性が重要な考慮事項である場合は，取外し可能な媒体上のデータを保護するために，暗号技術を用いる．
（略）

11.2.5 資産の移動
管理策
装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出さないことが望ましい．
実施の手引
この管理策の実施については，次の事項を考慮することが望ましい．
a) 資産を構外に持ち出すことを許す権限をもつ従業員及び外部の利用者を特定する．
b) 資産の持出し期限を設定し，また，返却がそのとおりであったか検証する．
c) 必要かつ適切な場合は，資産が構外に持ち出されていることを記録し，また，返却時に記録する．
（略）

（2）資産のライフサイクル管理

資産の取得から利用，不要になった 際の資産の廃棄について資産のリスクに合わせた管理が求められる．資産を取得し た場合には，情報の分類とラベル付けが求められる．しかし，HDD はシステムの一部であり，個別に管理されてはいない．しかし，システムから取り外した場合には，その媒体に含まれている情報に合わせた管理や保管，監査証跡が必要(8.3.1)となる．なお，資産を取り外す場合には，再利用の有無で異なる．再利用可能な媒体の場合には，その

内容が以 後不要であるならば，これを復元不能とする(8.3.1)となっており，神奈川県の初期化だけでは不十分である．また，システムからHDDを取り外す場合には，資産を事前の認可なしでは，構外に持ち 出さないことが望ましい，持ち出す場合には，権限をもつ従業員及び外部の利用者を特定する(11.2.5)となっている．

8.3.2 媒体の処分
管理策
媒体が不要になった場合は，正式な手順を用いて，セキュリティを保って処分することが望ましい．
実施の手引
認可されていない者に秘密情報が漏えいするリスクを最小化するために，媒体のセキュリティを保った処分のための正式な手順を確立することが望ましい．秘密情報を格納した媒体の，セキュリティを保った処分の手順は，その情報の取扱いに慎重を要する度合いに応じたものであることが望ましい．この管理策の実施については，次の事項を考慮することが望ましい．
a) 秘密情報を格納した媒体は，セキュリティを保って，保管し，処分する（例えば，焼却，シュレッダーの利用，組織内の他のアプリケーションでの利用のためのデータ消去）．
b) セキュリティを保った処分を必要とする品目を特定するために，手順が備わっている．
c) 取扱いに慎重を要する媒体類を選び出そうとするよりも，全ての媒体類を集めて，セキュリティを保ち処分するほうが簡単な場合もある．
d) 多くの業者が，媒体の収集及び処分のサービスを提供している．十分な管理策及び経験をもつ適切な外部関係者を選定することに，注意を払う．
e) 監査証跡を維持するために，取扱いに慎重を要する品目の処分を記録しておく．

処分のために媒体を集める場合，集積することによる影響に配慮することが望ましい．取扱いに慎重を要する情報ではない情報でも，その量が集まると，取扱いに慎重を要する情報に変わる場合がある．

（3）媒体の処分

再利用を前提としない媒体が不要となった場合には，廃棄の管理策を適用することになる．媒体のセキュリティを保った処分のための正式な手順を確立することが望ましい．とくに，秘密情報を格納した媒体の，セキュリティを保った処分の手順は，その情報の取扱いに慎重を要する度合いに応じたものであることが望ましい(8.3.2)と，明示的な手順を要求している．神奈川県，富士通リース，ブロードリングの3社とも，取り外し資産の管理について，保存されている情報の重要性から見ると資産の移動に伴って，利用者の権限や特定や期限，記録が求められている．

11.2.7 装置のセキュリティを保った処分又は再利用
管理策
記憶媒体を内蔵した全ての装置は，処分又は再利用する前に，全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること，又はセキュリティを保って上書きしていることを確実にするために，検証することが望ましい．
実施の手引
（略）
秘密情報又は著作権のある情報を格納した記憶媒体は，物理的に破壊することが望ましく，又はその情報を破壊，消去若しくは上書きすることが望ましい．消去又は上書きには，標準的な消去又は初期化の機能を利用するよりも，元の情報を媒体から取り出せなくする技術を利用することが望ましい．

（4）装置のセキュリティ管理

装置のセキュリティの管理策では，記録媒体について物理的に破壊することや上書きを進めており，初期化では十分でないとしている．

15.1.1 供給者関係のための情報セキュリティの方針
管理策
組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化することが望ましい．
実施の手引
組織は，供給者による組織の情報へのアクセスに具体的に対処するため，方針において情報セキュリティ管理策を特定し，これを義務付けることが望ましい．これらの管理策では，次の事項を含む，組織が実施するプロセス及び手順，並びに組織が供給者に対して実施するよう要求することが望ましいプロセス及び手順を取り扱うことが望ましい．
（以下，抜粋）
c) 様々な供給者に許可される情報へのアクセスの種類の定義，並びにそのアクセスの監視及び管理
d) 情報の種類及びアクセスの種類ごとの最低限の情報セキュリティ要求事項で，組織の事業上のニーズ及び要求事項並びに組織のリスクプロファイルに基づく供給者との個々の合意の基礎となるもの
g) 組織の情報を保護するために供給者に適用する義務の種類
h) 供給者によるアクセスに伴うインシデント及び不測の事態への対処．これには，組織及び供給者の責任も含める．
l) 情報セキュリティに関する要求事項及び管理策を，両当事者が署名する合意書の中に記載する条件
m) 情報，情報処理施設及び移動が必要なその他のものの移行の管理，並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化．

15.1.2 供給者との合意におけるセキュリティの取扱い
管理策
関連する全ての情報セキュリティ要求事項を確立し，組織の情報に対して，アクセス，処理，保存若しくは通信を行う，又は組織の情報のためのIT基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意することが望ましい．
実施の手引
関連する情報セキュリティ要求事項を満たすという両当事者の義務に関し，組織と供給者との間に誤解が生じないことを確実にするために，供給者との合意を確立し，これを文書化することが望ましい．
特定された情報セキュリティ要求事項を満たすために，合意には，次の事項を含めることを考慮することが望ましい．組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化することが望ましい．
（以下，抜粋）
a) 提供し又はアクセスされる情報の記載，及び提供方法又はアクセス方法の記載
b) 組織の分類体系に従った情報の分類（8.2参照）．必要な場合，組織の分類体系と供給者の分類体系との間の対応付け．
d) 契約の各当事者に対する，合意した一連の管理策（アクセス制御，パフォーマンスのレビュー，監視，報告及び監査を含む．）の実施の義務
g) それぞれの契約に関連する情報セキュリティのための方針群
h) インシデント管理の要求事項及び手順（特に，インシデントからの回復中の通知及び協力）
k) 情報セキュリティに関する連絡先担当者も含む，合意における相手方の担当者．
m) 供給者が実施する，合意に関わるプロセス及び管理策を監査する権利
n) 合意上の問題点の解決及び紛争解決のプロセス

p) 組織のセキュリティ要求事項を順守するという供給者の義務

（5）供給者のセキュリティと ICT のサプライチェーン

次に，事業者と供給者との関係で見ていく必要がある．供給者関係の管理策としては，以下が述べられている．ここで述べられている管理策は，供給者との関係における方針や契約，管理面などのについてであり包括的なものとなっている．

供給者のセキュリティと ICT のサプライチェーン 事業者と供給者との関係で見ていく必要がある．

15.1.3 ICT サプライチェーン
管理策
供給者との合意には，情報通信技術（以下，ICT という．）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めることが望ましい．
実施の手引
サプライチェーンのセキュリティについては，供給者との合意に次の事項を含めることを考慮することが望ましい．
（以下，抜粋）
f) 重要な構成要素及びその供給元が，サプライチェーン全体を通じて追跡可能であるという保証を得る．
h) サプライチェーンについての情報，並びに組織と供給者との間で生じる可能性のある問題及び妥協についての情報を共有するための規則を定める．

供給者関係の管理策としては，以下が述べられている．ここで述べられている管理策は，供給者との関係における方針や契約，管理面などのについてであり包括的なものである．しかし，情報セキュリティ要求事項について，供給者と情報の種類及びアクセスの種類ごとの最低限の情報セキュリティ要求事項の合意をする．(15.1.1)この中には，当然，委託する資産の管理，組織の分類体系に従った情報の分類，必要な場合， 組織の分類体系と供給者の分類体系との間の対応付け(15.1.2)が含まれると考えられる．またこの要求条件は ICT のサプライチェーンにも継承される(15.1.3)．

管理策からは，今回の事件の当事者間の契約は，情報セキュリティ管理の観点からは不十分であったと結論づけられる．

7.2.2 情報セキュリティの意識向上，教育及び訓練
管理策
組織の全ての従業員，及び関係する場合には契約相手は，職務に関連する組織の方針及び手順についての，適切な，意識向上のための教育及び訓練を受け，また，定めに従ってその更新を受けることが望ましい．

7.2.3 懲戒手続
管理策
情報セキュリティ違反を犯した従業員に対して処置をとるための，正式かつ周知された懲戒手続を備えることが望ましい．

（6）事業者の人的な管理

HDD を詐取していたブロードリンクの元社員は窃盗で逮捕されている．情報セキュリティ管理では，従業員への意識向上，教育・訓練について述べている．また，懲戒手続についても述べている．しかし，これだけでは従業員の犯罪対策としては十分ではない．これには， IPA の不正対策ガイドラインが役立つ．

3.2 神奈川県と富士通リースに求められる管理策

神奈川県に求められるのは，情報の管理元として，情報の管理をきちんとしておけば，リースバックに際して，今回のように安易な引き渡すことはなかったと考える．とくに管理策**「11.2.7 装置のセキュリティを保った処分又は再利用」**を適用して，記録媒体の破壊，消去若しくは上書きを実施すべきであった．富士通リースは，神奈川県への供給者としての立場での情報管理が求められる．サーバ機器のリースといっても，神奈川県の重要情報の処理に用いられることは自明であり，知らないという言い訳は通用しない．神奈川県から HDD の廃棄を委託されたのであれば，ISMS の認証企業としては，当然に重要情報が残存しているとして HDD の完全な廃棄までの管理をすべきであったと考える．

3.3 ブロードリンクに求められる管理策

ブロードリンク社は，HDD の廃棄を委託されたが，契約した通りの情報管理がなされておらず，盗難されて販売されても気付けなかったのは ISMS 認証事業者としてはあまりにも管理が不十分であったと言えよう．

まとめ

2019 年 12 月に起きた「機密情報の処理に用いられていた HDD が十分に管理されずに外部に流出した問題」を取り上げて，セキュリティの管理の側面と法的な観点での問題点について論じた．現時点では，まだ，進行中の部分もあり，今後の展開を見ていく必要がある．しかし，明らかになったのは，サプライチェーンの中で情報の管理が変わっていくことである．元の情報資産の分類や扱いが継承されることが基本であるが，情報の廃棄の場合には，情報資産としての管理が継承されなかったことが一番の問題と考えられる．

謝辞

本研究にさまざまなコメントや意見をいただいた関係者に感謝します．

参考文献

[1] 朝日新聞デジタル,行政文書が大量流出　納税記録などのＨＤＤ転売,
https://digital.asahi.com/articles/ASMD57WSXMD5UTIL065.html（アクセス，2020 年 1 月 10 日）
[2] 朝日新聞デジタル,神奈川県文書，大規模流出　個人の納税情報など　廃棄業者社員，ＨＤＤ転売,
https://digital.asahi.com/articles/DA3S14284382.html，（アクセス，2019 年 1 月 10 日）

[3] 朝日新聞デジタル,神奈川県情報流出　容疑者が在籍する会社は防衛省，最高裁判所なども顧客
https://dot.asahi.com/wa/2019120800003.html?page=1
[4] 神奈川県，行政情報に大量流出懸念　廃棄機器転売され，日経新聞 2019/12/6（アクセス，2019 年 12 月 30 日）
日本規格協会，JIS Q.27002:2014
[5] ブロードリンク，『情報機器盗難・流出』関連の更新情報，https://www.broadlink.co.jp/progress-report/