＜研究論文＞

急激に変化する環境に対応した情報セキュリティへのアプローチ

A New Approach to Information Security in Rapidly Changing Environment

内藤　裕之　Hiroyuki Naitoh　ブリーズ・コンサルティングオフィス
植野　俊雄　Toshio Ueno　ISU
齋藤　敏雄　Toshio Saito　日本大学

概要

ICT の急速な発展により、人々の生活や企業の活動は大きく変化した。このような状況を情報セキュリティの観点から眺めると、組織および組織構成員による ICT の利用環境には質的な変化が生じており、その結果個人および組織は、今までに直面したことのない新たな脅威に身をさらす可能性が高まっている。

本研究の目的は、昨今の ICT の急速な発展に伴う利用環境の変化、それに伴う新たな脅威の顕在化とその特徴を明らかにし、それらに対応した情報セキュリティ確保のための新たなアプローチの方向性と基本的考え方を提案することである。本論文で提案する新たなアプローチ（本研究ではオブジェクトアプローチと呼ぶ。）とは、どのような組織にも普遍的に適用できる考え方で、利用環境の変化に不変な要素、すなわちデータに着目し、データの守るべき特性を維持する方策を最優先することを基本とするものである。

キーワード：情報セキュリティ、ICT 利用環境の変化、オブジェクトアプローチ

1　はじめに

ICT の急速な発展により、人々の生活や企業の活動は、大きく変化した。人々は誰でも、スマートフォンなどのモバイル端末を利用して世界中から様々な情報をいつでも手に入れることが可能になり、同時に自己の思いや行動を世界に対して自由に発信できるようになった。さらにツイッターやフェイスブックのようなソーシャルメディアは、人々のコミュニケーションの仕方に大きな影響を及ぼしている。一方、企業における情報システムでは、サーバがオンプレミスからクラウドへと移行しつつあり、クライアントはパソコンからタブレットなどのモバイル端末へと変わり始めている。

今日の組織が直面するこのような状況を、情報セキュリティの観点から眺めると、組織および組織構成員による ICT 利用の環境が、従来とは質的に大きく変化しつつあり、結果として、組織を取り巻く脅威もまた、内容および顕在化の仕方の両面において、複雑化し続けていることが分かる。変化を続ける ICT 利用環境の下で活動している組織が情報セキュリティを確保するためには、既存の管理策を今までと同じやり方で適用することで果たして十分であろうか。従来のアプローチに代わる、あるいはそれを補完する別の考え方に沿った新たなアプローチが求められるのではないのか。このような問題意識の共有が本研究の出発点である。

本研究の目的は、昨今の ICT の急速な発展に伴う利用環境の変化、それに伴う新たな脅威の顕在化とその特徴を明らかにし、それらに対応した情報セキュリティ確保のための新たなアプローチの方向性と基本的考え方を提案することである。本論文で提案する新たなアプローチとは、どのよう

2014/4/2 受付　2014/9/16 受理

な組織にも普遍的に適用できる考え方で、利用環境の変化に不変な要素、すなわちデータに着目し、データの守るべき特性を維持する方策を最優先することである。

本論文は、以下のように構成される。２章では、情報セキュリティを取り巻く環境の変化をICTの急速な発展を軸に概観する。３章では、利用環境の変化にともなう新たな脅威の顕在化とその特徴を明らかにする。４章では、既存の管理策を用いてなされる従来のアプローチを適用した場合の問題点とその限界を議論する。５章では、従来のアプローチとは異なる新たなアプローチを提案し、その基本的考え方を示す。最後に６章では、まとめと今後の課題を示す。

2 情報セキュリティを取り巻く環境の変化[1),2)]

2.1 ICTの急速な発展に伴う利用(できる)環境の多様化

インターネットは、今日では、人々の生活および企業活動にとって必要欠くべからざる社会インフラの一つである。人々の消費行動や企業による様々な活動は、日々大量のデータを生み出しているが、これらのデータは、インターネットあるいは企業独自の通信回線に繋がれた各種の情報システムを介して、リアルタイムに記録、蓄積、そして交換され、時には国境を越えて遠く離れた場所に保管されている。一方、こうして獲得されたデータは、日常生活における利便性を高めるために、あるいは組織活動のさまざまな局面で直面する課題を解決するために、有効に活用される時代になりつつある。こうしたICTの急激な展開は、以下に示すような利用環境の多様性を生み出している。

(1) クラウドサービスの進歩

インターネットの主要技術は、オープンソースとして広がってきたために、インフラやデータの互換性が高い。したがって、ベンダーによる囲い込みが困難なため、ネットワークを介してストレージ空間や処理環境といった各種のサービスを提供する形態が増えてきた。近年、このいわゆるクラウドサービスが、ネットワークや仮想化技術の進化によって多様化、低価格化してきている。総務省の通信利用動向調査[3)]によると、クラウドサービスを利用している企業は2010年の13.8%から2012年では28.3%へと倍増しており、クラウドサービスに対する敷居が低くなってきたことが分かる。

(2) PCからモバイルデバイスへ

スマートフォンやタブレットPCといった携帯可能で高機能なモバイル端末が普及し、子供から老人まで誰もが日常的に利用するようになってきた。このことは、高速で安価もしくは無料の無線LAN（WiFi）接続インフラの普及とあいまって、情報の表示や処理ができる環境が、企業の情報システム部門の管理範囲外に大きく広がっていることを意味する。昨今では、経費節減、業務の効率化を目的として、従業者が自らの私有端末を業務利用に使う、いわゆるBYOD（Bring Your Own Device）の形態を許容する企業およびそれを支援する技術も現れている。

(3) 新たなコミュニケーションサービス(SNSなど)の展開と利用者の低年齢化

フェイスブックやツイッターといった、いわゆるソーシャルネットワーキングサービス（SNS）は、メールに代表される従来のコミュニケーション方法と異なり、クラウド上にデータを保持しながら、個人においては友人間での情報交換、企業においては広報や広告宣伝などのさまざまな利用を生み出している。特に、若年層によるスマートフォンを経由したサービス利用が急増している。

(4) 制御系システムや社会インフラのコントロール

家電製品などをネットワークに接続して外部からコントロールすることや、スマートシティ構想、車両運行制御等に見るように、ICTを利用して社会インフラをきめ細かにコントロールすることが始まっている。これらのネットワークは、独自のインフラでセキュリティを確保しているものもあれば、インターネットを利用するものもある。生活者の利便性を高めるサービスとして、家庭内のPCからインターネット経由で接続できるものが増えている。

2.2 情報処理形態および業務スタイルの変化

前節で述べたICTの利用環境の多様化によって、企業や組織における情報処理の仕組み、人々の働くスタイル、そして組織の在り方は、大きく変化してきている。以下では、主要な変化を３点あげる。

(1) オンプレミスからクラウドへ

自社施設で、自社所有のコンピュータ（ハード、ソフト）を用い、自社専用のネットワーク（LANや専用線）を使って自社の要員のみで情報処理を

行う形態、つまり完全なるオンプレミスともいえる環境は、今ではレガシーなどと呼ばれることも多いが、金融機関など高い機密性、安全性を求められる業種の基幹システムではまだまだ主流である。しかし他の大多数の業種や情報系、顧客サービス系システムではインターネットを利用したクラウド化が進行中であり、セキュリティおよびパフォーマンスとコストの関係で、一定部分はオンプレミスに残し、残りは外部で行う形態が、現在の主流であると思われる。

Webやメールサーバで外部のホスティングサービスを利用したり、ファイルサーバを共有のデータセンタに置いたりすることなどが一般的であるが、アプリケーション単位でクラウドサービスを利用するケースも増えてきている。さらに進んだ例では、社内リソースをほとんど使用せず、IT系の業務はほぼすべて外部に依存するという形態もみられる。すなわち、インフラは外部のホスティングやクラウドサービスを利用し、端末は個人所有のPCやスマートデバイスを用いた自前のモバイル環境下で、SNSやWebメールを用いてコミュニケーションを行うというような業務スタイルである。この場合、利用するICTについて、自社でコントロール可能な部分はきわめて少ない。

(2) 業務組織と働き方の多様化、複雑化

組織的、人的な面でいうと、企業が正社員のみでシステムの開発、運用を行っていたのは過去の話であり、大半の技術者を外注に依存するか、あるいは丸投げすることも多くなっている。これらのアウトソーシングにもいくつかのタイプがある。孫請け、ひ孫請けのように組織的に階層化が深まり複雑化することもあれば、最近のWeb系ベンチャー企業のように、独立した個人単位でプロジェクトに参加し業務を役割分担したりするようなことも増えている。したがって、雇用形態も流動的になり、作業を行う勤務場所も所属企業内に用意されるとは限らず、開発・運用拠点などの外部に用意された場所や個人宅などに分散化が進み、プロジェクト要員の管理は一層複雑かつ困難になってきている。

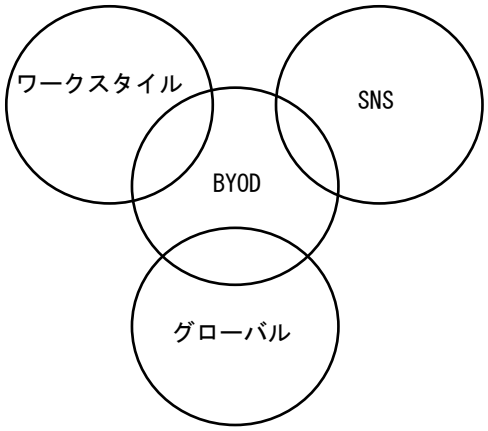
(3) 禁止から活用へ

2005年に個人情報保護法が施行されて以来、企業や自治体においては、情報、特に一般消費者の個人情報の利用や提供に関して、非常に保守的かつ神経質な姿勢が見られるようになり、緊急時に必要な情報が提供されないなどの弊害も現れていた。大災害のたびにこれら弊害が議論され、緊急時の利用方法についての合意形成の在り方に対する検討が進んでいる。

最近では更に、個人の行動履歴なども含むビッグデータの活用を、社会として推進しようという動きも現れ、関連する技術の進歩も手伝って新たな情報の積極的活用についての議論が始まっている。

2.3 複数の利用環境が交差する複合的ICT利用環境の出現

ICTの利用環境の多様化とそれに付随して生じてきた仕事のスタイル、情報処理の仕組み、そして組織の在り方の変化によって、今日では、個人および組織による情報処理の多くは、複数の利用環境が互いに交差する複合的ICT利用環境の下で行われるようになっている（図表1）。



図表1　BYODを中心としたICT利用環境の組み合わせ例

図表1で示すように、グローバル環境下で利用されているモバイル端末、個人所有のスマートフォンによるソーシャルネットワークサービスの利用、インターネットを介した在宅での仕事など、多くの複合的ICT利用環境の例を挙げることができる。

3　新たな脅威の顕在化とその特徴[1),2)]

3.1 従来になかった脅威の発生

前章で挙げたような新たな利用環境の出現は、情報利用の利便性を向上させると同時に、以下のような新たな脅威も生み出している。

(1) インターネット利用に伴う脅威

インターネットの利用は、データの交換と蓄積

の行われる空間が、必ずしも国内に留まることなく国境を越えた全世界に広がることを意味する。したがって、国によって異なる法令の下では、対象となるデータにどの国の法令が適用されるかによって、様々な問題が発生する。例えば、クラウドサービスのデータ保管サーバに関連して、所在場所の相手国の法的紛争でサーバが差し押さえられたり、共用している無関係の他企業への強制捜査のためにデータを開示させられたりするリスクなどが発生しうる。

(2) 雇用形態の変化に伴う脅威

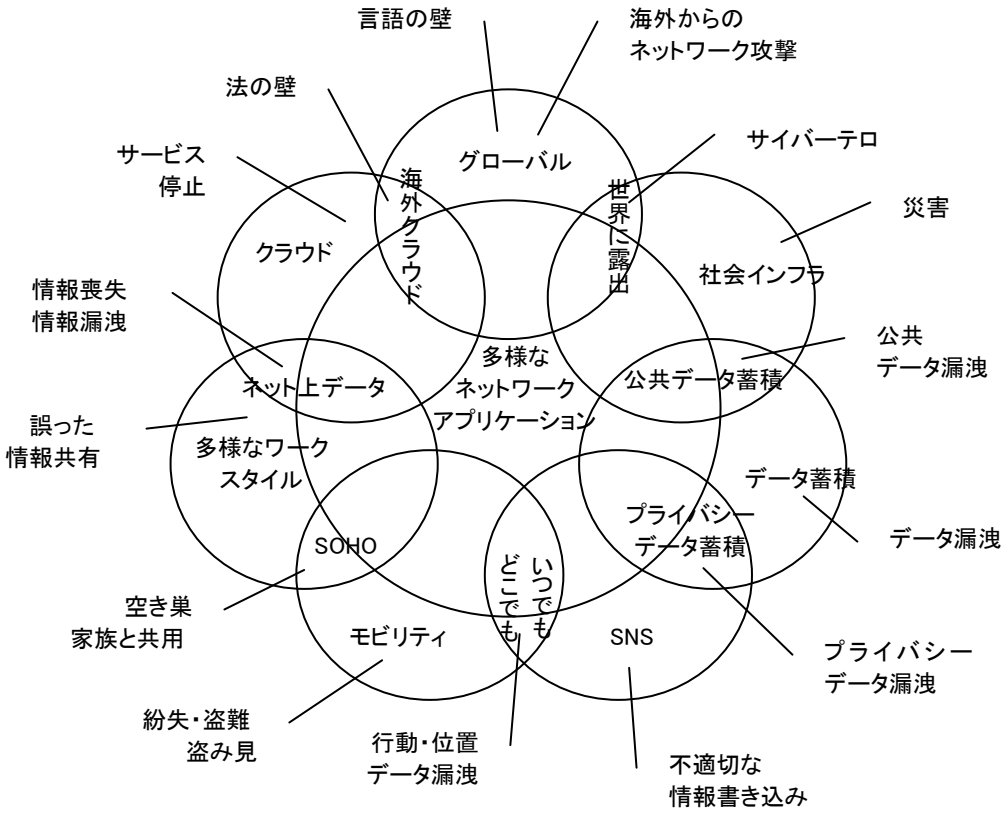
雇用形態の流動化に伴い、プロジェクトや業務への参画者が社外へ広がっていき、守秘義務の範囲や有効期間、著作権やライセンスに対する管理が、運営面で困難になる。こうした環境下では形式化した誓約書やチェックリストだけが最終的な拠り所となるが、これらは参画者の善意に期待することを前提としたものであり、初めから悪意を持って参画した者や組織に不満を抱いた者による故意の不正行為を排除できないため、それだけでは有効なコントロールにならない。

(3) SNS 利用に伴う脅威

SNS での関係者の不用意な書き込みを発端として、サイトの炎上や風評被害、コンプライアンス違反の露見などにより、業務停止や廃業を余儀なくされる事例が散見されている。また、サービス条件や規約の理解不足により、誤った公開範囲で情報が開示されたり、不適切なアプリケーションの連携による情報や ID の流出も起きている。こうした SNS 特有のリスクを把握し予見することは困難であり、組織としての管理には限界がある。

3.2 複合的利用環境において顕在化する脅威

2.3 節で述べたように、新たな利用環境が複合的に混じり合う ICT の利用環境においては、複数の利用環境が相互に関連しあうことで、個々の利用環境下では生起しなかった新たな脅威が顕在化すると考えられる。以下の図表 2 は、そのような脅威の例である。



図表２　複合的 ICT 利用環境において顕在化する脅威の例

3.3 新たな脅威の特徴

個別の ICT 利用環境において予想される脅威に比べ、複数の利用環境が交差する複合的 ICT 利用環境において予想される脅威は、より複雑であり、顕在化の予想は一層難しいものとなる。複合的 ICT 利用環境における新たな脅威の基本的特徴を抽象的に表現すれば、次の３つを挙げることができる。

(1) 脅威が顕在化するプロセスの中身を知ることが一層困難

複数の要因が複雑に作用し合うため、脅威が顕在化する因果連鎖の把握が困難である。関係するシステム全体を把握し統制できる要員を、組織的に確保することは難しく、一定部分はブラックボックスとして扱わざるを得ないことになり、プロセス全体をコントロールすることが非常に困難である。

(2) 脅威の存在範囲が閉鎖空間から開放空間へと拡大

インターネット利用の日常化とグローバル化により、ネットワークを介したデータ交換の物理的境界はなくなり、また地理的距離の意味が喪失する。したがって、物理的な境界はもちろんのこと、ネットワークにおいても内側と外側という概念が不明瞭となり、仮想化技術も加わってますますセキュリティ境界の設定が難しくなっている。

(3) 脅威の顕在化の時期が不連続から連続へと変化

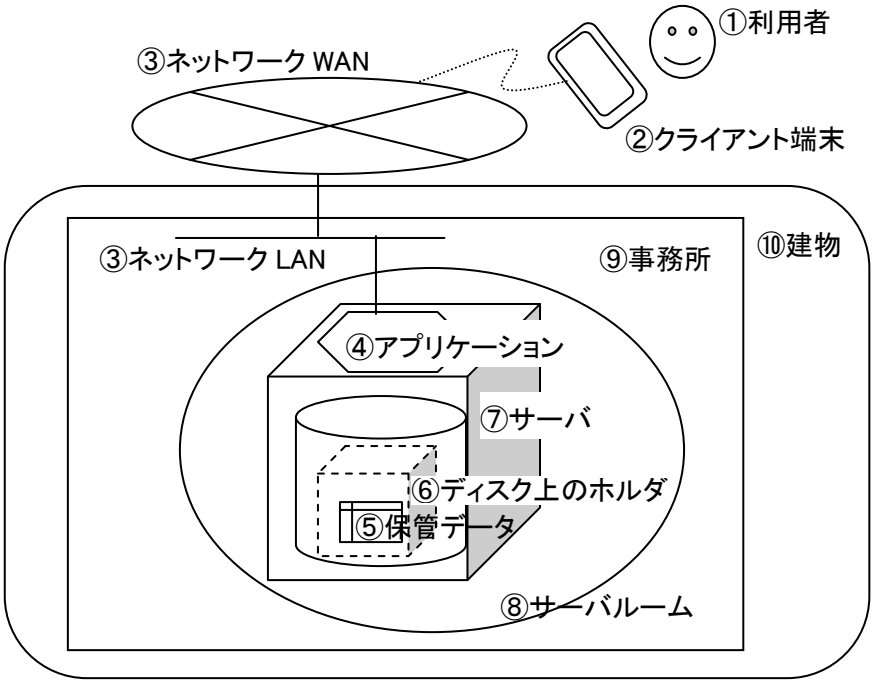
モバイル端末の携行やネットワークサービスのグローバル化は、システムへのアクセスがいつでもどこでもできるということを意味するので、一般的な就業時間は意味を持たなくなってくる。そうなると多国籍企業でなくても、24 時間、業務が止まる時間はなくなるといってよい。脅威はいつでも切れ目なく顕在化すると考えることが必要になる。

4　従来型アプローチの限界

4.1 従来型アプローチの考え方

従来のアプローチでは、情報システムを、利用者を含めて情報システムに関連するすべてから構成される全体と捉え、その構成要素であるノードやアプリケーション（これらには、媒体、機器、設備、ソフトウェア、人を含む）に対し、情報セキュリティを確保するための管理策を個別に策定し運用することを主眼としてきた。図表３は、情報システムを構成する各要素を示している。

システムがオンプレミスで、企業が情報システムを主体的にコントロールでき、かつデータが静的に存在している間は、このようなやり方がデータを保護する有効な対策であった。



図表３　情報システムの全体

4.2 従来型アプローチの問題点

本論文が対象としている新しい環境下では、すなわち複合的ICT利用環境の下では、情報（データ）を扱う媒体や機器を個別独立したものとして扱うことはできず、したがって単一の管理策では対応しきれなくなってくる。例えば、サーバをどんなに守っても、クライアントとモバイル機器を通じて同期しているクラウド上のストレージ経由で、情報が漏えいすることを考慮しなくてはならない。また、情報、媒体、デバイス、あるいは業務において、企業（組織）と個人の境目がボーダレスになってきたため、管理方針を徹底しづらくなってきている。

4.3 従来型アプローチの限界

複合的なICT利用環境下では、すでに見たように、既存の管理策では限界がある。その理由は主に2つある。一つは、既存の管理策は、4.1節で示したように、自社のオフィス内、あるいはサーバ室といったように、個別の利用環境を想定したものが多いことである。そのため、社外利用、あるいはクラウドアプリケーションの利用などの複合的なICT利用環境の下では、十分カバーしきれなくなっている。クラウド環境下では、ノードやアプリケーションの仮想化が図られているので、物理的なノードやアプリケーションを前提とした従来の管理策では有効な対策にならない。

もう一つの理由は、既存の管理策は、オンプレミスのような環境を基に経験的に積み上げられたノウハウを集大成して策定されており、比較的安定した利用環境を想定していることである。既存の管理策、あるいはその延長上で見直しを図り改善した管理策では、今日のように急速に変化する環境への対応は困難となっている。

従来の想定では対処できない複雑な状況が生じているといえる。

5 新しいアプローチの考え方とその方法

5.1 環境変化に影響を受けない不変なものに着目する方法

(1) 守るべきものは何か

利用環境が変わっても不変なのは、データの機密性や完全性といった守るべき特性である。したがって利用環境がどのように変化しても、これらを維持する方策を考えるのが、まずは究極的な対策となるはずである。

データの守るべき特性を維持するための方策として、今まではデータを格納する“入れ物”の対策に依存してきた。例えば、フォルダのアクセス制御、ネットワークアクセス時の認証、Windowsなどのログインパスワード、サーバ室の施錠、オフィスの入退管理、ビルの機械警備などである。しかし、それならば素直にデータそのものに対策を施した方がよいのではないか、という結論に至るのが自然な成り行きではなかろうか。データそのものの守るべき特性を維持するための対策が施されれば、データの入れ物に対策を施す必要性は減少し、入れ物を限定することなくデータを利用できる。つまり、クラウドであろうが個人所有のデバイスであろうが、データの保存場所や媒体を気にすることなく、自由なシステム構成を活用することができることになる。

そこで、対象とするデータに対して、はじめに情報セキュリティの観点からデータの特性を明らかにし、次にその特性を維持するための方策を検討し、最後にそのための具体的管理策を作成することで、道筋が見えてくると思われる。

(2) データの分類

データの守るべき特性を明確にするために、組織における情報セキュリティの観点からデータを整理し分類してみる。

以下では、いくつかの基準に沿って分類を試みる。

①データの存在場所に関して

データがある場所はどこか。

国内あるいは国外。国内ならば、個人の情報機器内、組織内、あるいは組織外。組織外としては、元従業者、情報窃盗者、流出情報取引組織、スパイなども含まれる。

②データ存在の認知に関して

データの利用者が、データの存在を認知しているか否か。

存在を認知されたデータ、未認知のデータ

③データ内容の認知に関して

データの利用者が、データの内容を認知しているか否か。

内容が認知されたデータ、未認知のデータ

④データの内容に関して

データの主な内容は何か。

人、モノ、カネ、技術

⑤人に関するデータの内容に関して

組織との関係は何か。

組織内（従業員、役員、非正規雇用者）、組織外（顧客、その他一般人）

⑥データの発生源に関して
データの発生源はどこか。
組織内（部門、業務、作成者は誰か）、組織外

⑦データの所有に関して
データの所有者は誰か。
個人所有、組織共有、外部組織所有

⑧データの著作権に関して
データの著作権は誰のものか。
原著作権者、譲渡を受けた著作権者、著作権非所有者

⑨データ所有者からの利用の許諾方法に関して
許諾された利用範囲の種類は何か。
参照、印刷、記憶媒体への保存、改変、引用転載、再配布、

⑩データ利用についての法律との関係
データの利用が法律で許容されているか否か。
利用が許容されるデータ、利用禁止データ

(3) 個人情報の分類によるデータ特性

個人情報を対象データとして、データの特性を考察してみる。例えば、先に挙げた分類基準の中から、データ内容の認知に関する基準を取り上げ適用すれば、個人情報に関するデータは、情報提供者である個人がデータ内容を知っているか否かと、情報取得者である組織がデータ内容を知っているか否かの２つの基準の組み合わせから、次の４つのタイプに分けられる。

①個人と組織が共に知っている
具体例：
個人が組織へ提供した個人データ
組織が外部へ公開しているデータ

②個人は知らないが、組織は知っている
具体例：
個人が提供したデータを組織が加工し、組織が活用するデータ
利用システムの利用範囲などの組織が決めた設定データ
アクセスログなどの監視データ

③個人は知っているが、組織は知らない
具体例：
個人が組織に提供しないデータ
パスワードとして設定する文字列（本人が変更したもの）

④個人と組織が共に知らない
具体例：
無断ダウンロード、漏えい等により第三者に渡ったデータ

組織が保護管理すべきデータはもちろん、タイプ①と②である。特にタイプ②のデータは、データの所有権、データの利用権などとの関連で、特に慎重な取り扱いが要求される。また、タイプ④の、ひとたび漏えいして第三者によって保管されているデータを、認知し管理することは、所有権を持つ正規な個人または組織にとって不可能である。データの存在を認知している個人または組織であるからこそ、当該データを思うように管理できるのである。

このように、先の（２）データ分類を用いて、保護対象データと保護管理責任の所在を具体的に明らかにすることで、より一層確実に、データそのものの守るべき特性を維持する方策を見出し、有効な管理策を作成することができる。

5.2 データそのものを守る方式　― オブジェクトアプローチ ―

本節では、守るべきデータの特性として、堅牢性、復元性、そして自立性を取り上げ、これらを維持するための方策の基本的な考え方を述べ、さらに、具体的管理策を挙げる。ただし、以下で示すように、データの堅牢性とは、データの存在場所に関わりなく、データの機密性と完全性を確保できるという概念であり、データの復元性とは、データの可用性の確保に対応した概念である。そしてデータの自立性とは、データの利用に関連する全情報を属性として常時保持し、これを基にデータの利用者を制限することで、機密性と完全性を確保できるという概念である。

(1) データの堅牢性

データの堅牢性を維持するとは、データの置かれた場所や保存された媒体に関わりなく、そのデータにアクセスを許可された者以外には、参照および変更ができない形態でデータを保管し、伝送することである。

管理策の例としては、データの暗号化と認証によるファイル属性設定がある。フォルダの暗号化やパスワード設定したファイル圧縮などは、復号化したデータの堅牢性が十分とは言えないが、汎用性がありコストもかからないので一定の効果は期待できる。

(2) データの復元性

データの復元性を維持するとは、一つまたは二

つのノードでデータの使用がアクセス不可や誤修正、滅失等によって利用不可能となっても、別のノードに保管された同一データの利用が可能な状態にあり、かつ使用不可能であったノードも速やかに回復されることである。

情報システムでは、使用可能性のことを一般に「可用性」という言い方をするが、データについては同じ時点の内容でなければならないので、「可用性」でなく「復元性」という用語をあえて使用することにした。

管理策の例としては、データレプリケーション（データの複製の複数場所への保管）やスナップショットによるバックアップなどがある。

(3) データの自立性

データの自立性を維持するとは、データの利用、操作、履歴などに関する管理情報などを属性として付加した形態でデータを保管し維持することで、属性で規定された以外のデータの利用は不可能にすることである。

管理策の例としては、Information Rights Management（IRM）、Rights Management Services（RMS）がある。これらの説明は、次節でする。

(4) クライアントの安全性

クライアントはデータの特性とは直接関係するものではないが、クライアントではデータを参照したり入力したりするので、一時的にはディスプレイ上やキーボード上で保護されない状態でデータが保持される。クライアントの安全性を維持するとは、クライアントの認証は、許可された利用者だけが行い、それが維持されているときだけアクセス情報が表示され、表示は他の者からもまたプログラムからもキャプチャされないように保護することや、クライアント自身にデータを保存させないことである。

管理策の例としては、シンクライアントやMDMの利用がある。

データの分類から得られるデータ特性との関連を含めて、オブジェクトアプローチのイメージを概念図として示したものが、図表４である。

5.3 現存のソリューション例とオブジェクトアプローチとの関係

本節では、現在ベンダーによって提供されているソリューションの例を挙げて、はじめにその特徴を説明し、次に、オブジェクトアプローチの観点から、問題点を明らかにする。

(1) DLP ソリューション[4),5),6)]

機密データが組織の管理領域から不正に流出するのを防止する対策としては、DLP（data loss/leak prevention：情報漏えい対策）ソリューションが知られている。

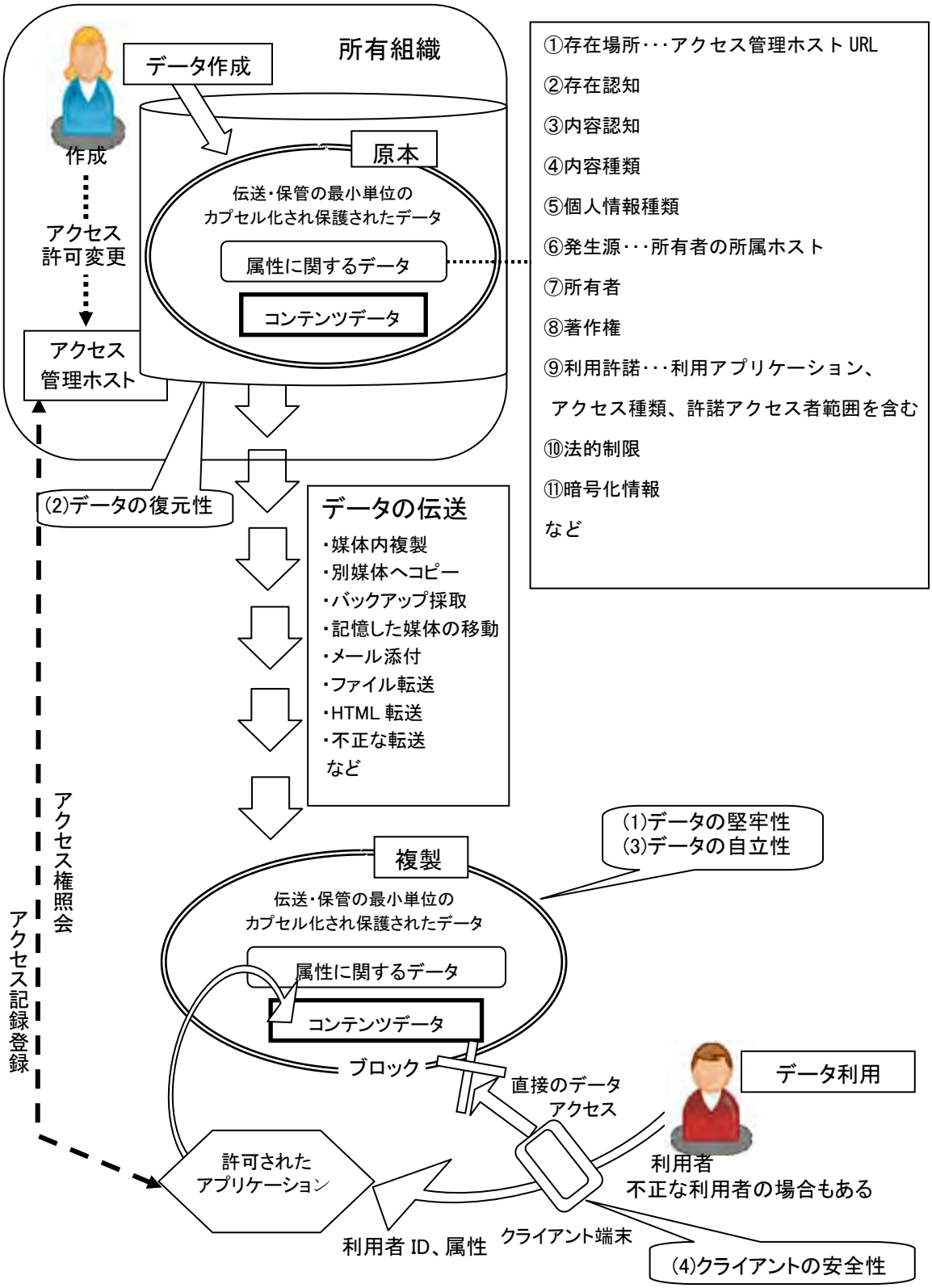
DLP ソリューションは、隔離空間におけるデータ監視方式を採用している。すなわち、隔離空間の中でファイル検閲を実行し、データ流出防止を行うことを主要な技術としている。具体的には、ファイル（又はファイルの一部）からデータが機密データであるかどうかを判別し、隔離空間の中にあるストレージ、端末、ネットワークを監視して機密データの漏洩防止を自動的に実行するものである。また、セキュリティポリシーの適用を自動化し、禁止されている行動をリアルタイムにブロックすることによって、アクセス制御だけでは実現できない情報漏えい防止を実現している。昨今流行している「標的型攻撃による情報流出」の防止にも対応している。

問題点は、データが隔離空間にあるうちは良いが、一旦隔離空間の外部へ出たあとは何ら制御することはできないことである。例えば、データのアクセス許可を得た上で業務委託先がデータをダウンロードした場合、また顧客等に提出するためにデータを持出した場合、さらに出張先などでDLP ツールが設定されていないパソコンに格納した場合などのケースでは、それ以降についてはデータに対する取り扱い制限が効かなくなる。すなわち、管理領域外でのデータの堅牢性、自立性は保証されない。

(2) Information Rights Management（IRM）および Rights Management Services（RMS）[7),8),9),10)]

Information Rights Management（IRM）は、ドキュメントを開けるユーザを指定し、受信者によるドキュメントの開封、変更、印刷、転送またはその他の操作を実行できる権限の設定によって使用方法を指定することで、永続的なファイルレベルの情報保護を実現する働きをする。

Rights Management Services（RMS）は、RMS と RMS 対応のアプリケーション（Word や PDF reader）との連動によって、オンラインやオフライン、およびファイアウォールの内側と外側を問わず、ファイルが無断で使用されないよう保護す



図表４　オブジェクトアプローチの概念

る機能をもつ。具体的には、次のような機能を実現できる。作成者または所有者がファイルにポリシーを適用した後は、ファイルが企業ネットワークの外側に移動しても、ポリシーはファイルに残る。ファイルのアクセス状況を追跡および監査するために、RMS によりログ記録が行える。解雇した従業員や取引が終了した第三者などに既に渡してあるファイルや情報漏えいして所在が分からないファイルに対して、アクセス権限を無効にすることで、参照禁止が行える。

IRM と RMS の両方式ともに、データの自立性を維持する方式を採用しており、基本的には 5.2 節の方式を実現するための基本機能を提供している。ただし、現状では、限られたベンダーの限られたアプリケーション環境で、かつ限られたファイル形式のものが、実用として提供されているに留まっており、環境およびファイル形式共に利用可能範囲が拡大され、かつ利用ユーザの費用負担の軽減又は無料化が、今後の課題である。

(3) MDM(Mobile Device Management)[11),12),13),14)]

クライアント端末の保護策として、以下のような機能を持つモバイル機器管理機能がいろいろと提供されている。

①紛失・盗難による情報漏えい防止
パスワードロックの強制化、デバイス位置の把握、遠隔ロック、遠隔消去など。

②不正利用による情報漏えい防止
カメラ、Bluetooth、無線 LAN、SD カード等を無効化するデバイス機能制限、ホワイトリストやブラックリストによるアプリの利用制限、定期的な監視による利用状況の収集や違反アプリの強制削除など。

③資産管理の徹底
端末ID、OSバージョン、アプリ、セキュリティポリシー適用状況などの構成情報の収集と一元管理、業務アプリやパッチ等の配信とインストールなど。

④セキュリティポリシーの強制
ウィルス対策、更新したポリシーの遠隔適用、部署や役職等に応じたポリシー管理など。

クライアントの安全性を支援する機能群が提供されつつあるが、まだまだ基本的な機能のレベルと言える。今後はさらに、クライアントでデータを参照したり入力したりする際に、平文状態で表示されたデータ内容のキャプチャや入力内容の盗聴などを防止する機能などの整備が必要で、さらなる改善が望まれる。

6 おわりに

本研究では、はじめに情報セキュリティを取り巻く環境の急激な変化を概観した上で、ICT 利用環境の変化に伴う新たな脅威の顕在化とその特徴を明らかにした。次に既存の管理策を用いた従来のアプローチを適用した場合の問題点と限界を浮き彫りにし、最後に利用環境の変化に不変な特性に着目した新しいアプローチ（オブジェクトアプローチ）の方向性と考え方を示した。

本研究で示した考え方を実現する具体的方法についての検討は、まだまだ不十分であり今後の課題である。

参考文献

1) 2012 年版 10 大脅威、独立行政法人情報処理推進機構、2012.
2) 2013 年版 10 大脅威、独立行政法人情報処理推進機構、2013.
3) 通信利用動向調査 企業編
http://www.soumu.go.jp/johotsusintokei/statistics/statistics05b2.html
4) 前場宏之、情報漏えい対策ソリューション DLP とは、@IT、トレンドマイクロ株式会社、2009/9/7
http://www.atmarkit.co.jp/fsecurity/special/150dlp/dlp01.html
5) 山本秀宣、情報漏えいを防ぐ DLP テクノロジーとは、Think IT、株式会社シマンテック、2009/11/13
http://thinkit.co.jp/article/1070/1
6) McAfee Data Loss Prevention、2007/11
http://ad.impress.co.jp/special/mcafee0711/
7) Office 2013 で Information Rights Management を計画する、Microsoft Corporation、2013-12-18
http://technet.microsoft.com/ja-jp/library/cc179103（v=office.15）.aspx
8) NAVIstaff ドキュメント統制システム、日立ソリューションズ
http://www.hitachi-solutions.co.jp/katsubun/sp/navistaff/?cid=yjl_0022271
9) 佐藤義昭、Microsoft® Active Directory Rights Management サービスと HP IceWall SSO との連携効果、日本 HP、2010/4/16
http://h50146.www5.hp.com/products/

software/security/icewall/iwsoftware/report/ms_rms.html
10) Rights Management Services 構築サービス，日立ソリューションズ
http://www.hitachi-solutions.co.jp/rms/
11）坪田弘樹、基礎から学ぶ「MDM（モバイルデバイス管理）ツール」の選び方、月刊テレコミュニケーション 2011 年 9 月号から再編集のうえ転載、
http://businessnetwork.jp/Detail/tabid/65/artid/1674/Default.aspx
12）MDM（モバイル端末管理）の製品一覧、IT トレンド
http://it-trend.jp/mdm?r=ov&utm_source=yahoo&utm_medium=cpc&utm_campaign=yahoo_listing_camp
13）MDM（モバイルデバイス管理）の導入状況 (2012 年 3 月アンケート実施結果)、キーマンズネット
http://www.keyman.or.jp/at/pcmob/mobile/30004609/
14）太田智晴、ワークスタイル変革 Day 企業モバイル活用フォーラム 2013 レポート レコモット東郷氏「BYOD に MDM は必須ではないと断言させていただく」、ビジネスネットワーク、2013/10/24
http://businessnetwork.jp/Detail/tabid/65/artid/3073/Default.aspx