大規模な情報漏えい事件の特性と対策の考え方

原田要之助[1]

概要

情報セキュリティインシデントに関する共同研究の調査[1] , [2]を分析したところ, 情報漏えい事故件数と1件あたりで漏えいした個人情報の数の分布は裾が長く, べき乗則に従うことが分かった[3], [4]. べき乗則は, 地震の規模と件数に見られるグーテンベルグ・リヒター則[5]として知られている. このべき乗則は近年研究が進み, 同様な現象が様々な分野でみられることが指摘されている[6].

本稿では, 情報セキュリティインシデント調査をベースにして, べき乗分布となる背景を検討し, 企業においては, 大規模な情報漏えいが起きることを想定する必要があること, これに対応するには, 情報漏えいを想定したBCP/BCMが対策として重要であることを述べる.

1 はじめに

日本では，プライバシーマーク制度が1998年に実施され，1999年にはJIS Q.15001が制定され，また，2003年には個人情報保護法が制定された．このような法制度や個人情報を管理する仕組みが導入され，個人情報漏洩事件は減少すると考えられた．しかし，法律施行以後も，ダイレクトメールや振り込め詐欺などが減らず，厳密化されたはずの個人情報の収集や無断使用が減らず，法制度の実効性が十分ではない．これは，JNSA（NPO日本ネットワークセキュリティ協会）が定点観測している情報セキュリティインシデント調査[1] [2]でも明らかとなっている．これを図１に示す．図１が興味深いのは，個人情報保護法が完全施行された2005年から3年間は情報漏えい事故の件数が減少していることである．しかし，情報漏えいに対する個人情報保護法による主務大臣への報告や罰則の適用などが一巡した2008年からは急に増大している[2].

これの理由としては, 個人情報を扱う企業や組織が増大していることとこれらの企業では多くの場合パソコンやサーバが用いれ, インターネットにも接続されている. また, 昨今では，メモリ素子の大規模化と低廉化により，大規模なデータを小型のUSBメモリ

1 情報セキュリティ研究科　教授

2 個別の原因としては，2008 年には教育・学習支援業，金融・保険業．サービス業，運輸業などの業種で漏えい件数が増加したことや地方自治体が積極的に漏えい事故について情報開示したことなどが述べられている．

やパソコンなどで企業外部に持ち出す機会が増加したことがあげられる[4].

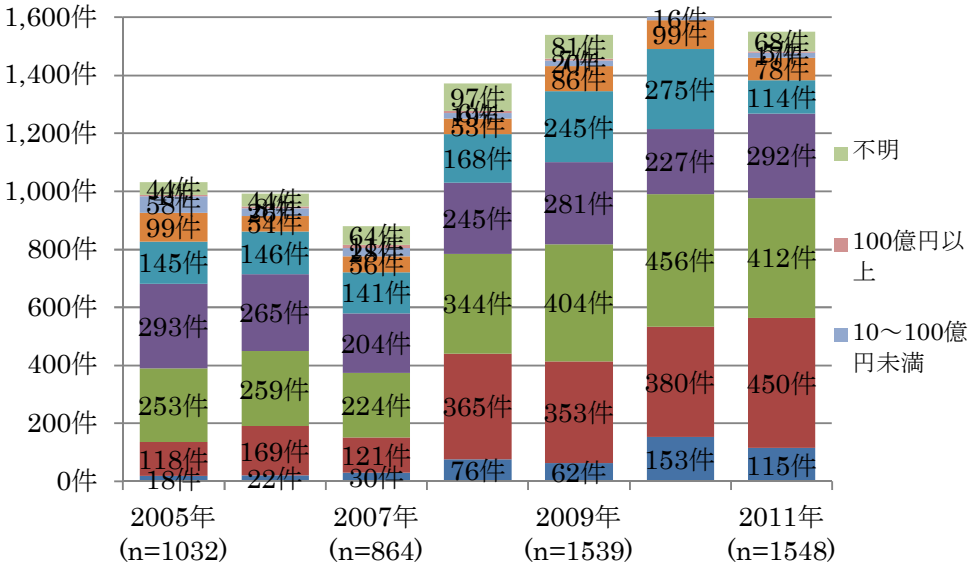

図1　2005年～2011年までのインシデント調査[1]より

2 インシデント調査における事故件数の分布

2.1 べき乗分布について

地震のエネルギーを示すマグニチュード（リヒタースケール）と頻度の関係がグーテンベルグ･リヒター則と呼ばれる対数の関係にあることが知られている[5]. これを図2に示す.

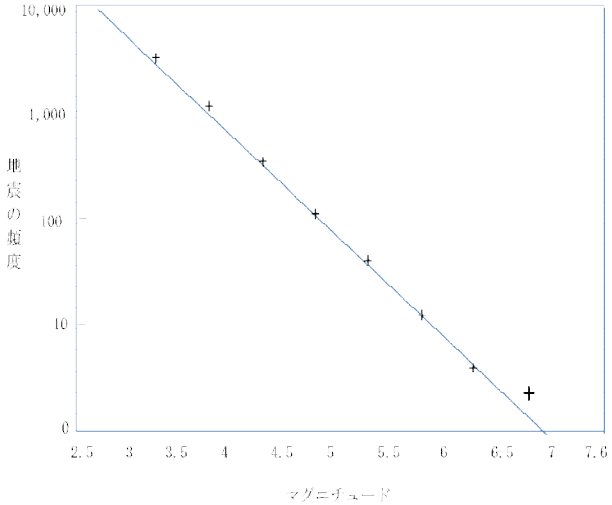

図2　グーテンベルグ･リヒター則はべき乗分布の例[5]

マーク・ブキャナンは，地震のエネルギーを示すマグニチュード（リヒタースケール）

と頻度のグーテンベルグ･リヒター則はべき乗則でありことを図2を例示して，さまざまな自然界の分布にこのべき乗則があてはまることを述べている[6]．これらの例として，山火事や凍ったジャガイモの破片の大きさの分布，フラクタルなどをあげている．さらに，マーク・ブキャナンは，べき乗則が自然界だけでなく，都市の大きさや戦争の規模といった人間の活動に関する事項にもべき乗則が当てはまることを示している．

次に，マーク・ブキャナンはべき乗則となる理由として，臨界状態を必要条件としてあげている．臨海状態にある場合には，次に起きる多数の事象は，単なる小さい規模の事象である場合も，全体を崩壊させるような大規模な事象にもなりうる．そして，それを予測するのは困難であると指摘している．例えば，地震については，臨界状態にあるプレートでは常に何らかの局所的な崩壊が多数起きている．その中には，プレート全体を破壊させるような東日本大震災のような規模の巨大な地震も起きうるとことになる．

2.2 ネットワークに多く見られるべき乗則について

ネットワークの分野では，会田らによって，いろいろな通信ネットワークでべき乗則が見られること[7]や湯田らによってソーシャルネットワークサービスにおけるべき乗則に関する研究[8]が行われている，また，WWW のハイパーリンクの大きさや論文の引用数などのさまざまなネットワークの構造に同様なべき乗則が成り立つことが研究されている[9]．

ネットワーク構造の場合，ノードの次数分布がべき法則に従う場合にはスケールフリーという性質[10]を持つことが指摘されている．これらの特性は，ネットワークの外部性が持つ特徴によって発現されると考えられる．ネットワークの外部性をもつものは，ランダムな関係ではなく，ネットワークを構成するノード間の関係がべき乗則に従うことが知られており，理論的に解明されつつある．また，辰巳は，金融分野においてもべき乗則が成り立つこと，これがネットワークの外部性と関係することを示唆している[10]．

2.3 情報漏えいに見られるべき乗則について

情報セキュリティ大学院大学では，2011年度よりJNSAと共同で情報セキュリティインシデント調査[1]を実施して，2011年度の個人情報漏えい事件の件数と漏えい規模（漏えいした個人情報の件数）を分析して，べき乗則の関係があることを示した[3]．これを図3に示す．さらに，同様の調査をJNSAの2005年からの調査結果を用いて検証した．2010年についての分析結果を図4に示す．図3と図4は，個人情報漏えい事件の件数と漏えい規模がべき乗則に従うことを示している．次に，2005-2011年の全体の個人情報漏洩事件の全体を対象に分析した．その結果を図5に示す．図5も図3，図4と同様なべき乗則に従うことが分かり，このことからスケールフリーの特性が確かめることができる．

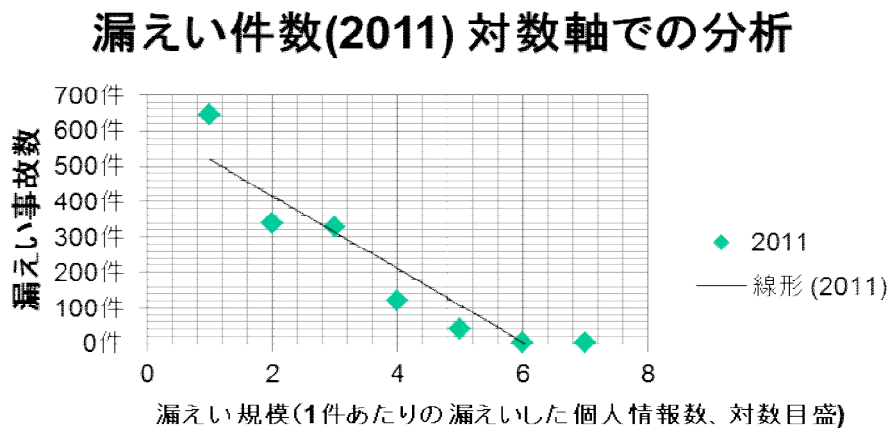

図3　2011年のインシデント調査結果がべき乗則となる例[1]より

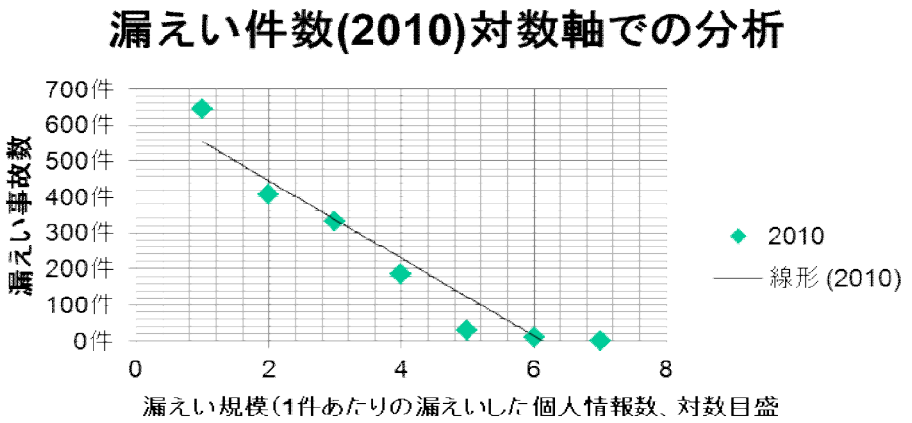

図4　2010年のインシデント調査結果がべき乗則となる例

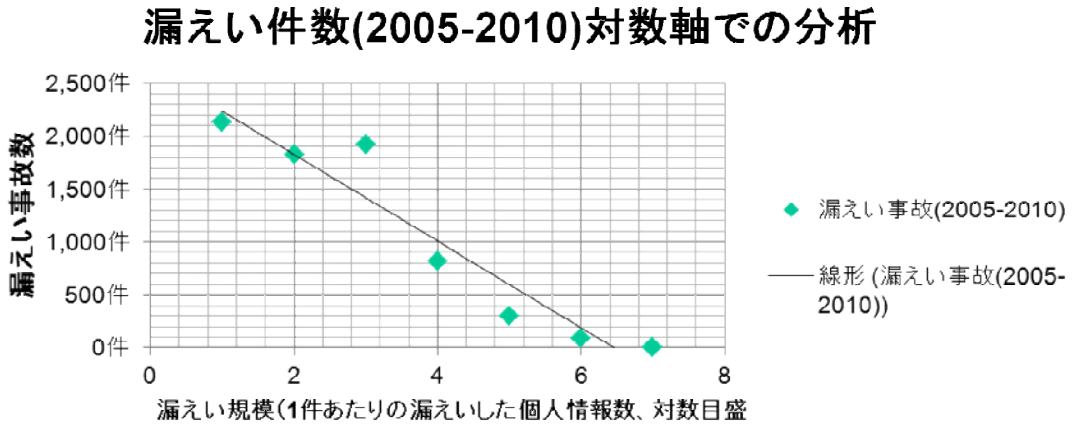

図5　2005～2010年のインシデント調査結果がべき乗則となる例

なお，図5の分布の裾を見たときに，べき乗則の線より下回っていることが分かる．これについては，小規模の情報漏洩事象では，漏洩した場合の情報漏洩の件数がべき乗則に比べて少ないことの研究がなされ，小規模であることから公表されていないものが多数存在することにより，報告される件数が実際よりも少なくとなっていることが分析されている[12]．すなわち，情報漏洩の規模と件数の分布がべき乗則になることがより強く支持されている．

以上より，以下のことが分かる．

①2010年，2011年の情報漏洩の規模と件数の分布は，べき乗則に従う．

②2005-2011年の全体情報漏洩の規模と件数の分布についても，べき乗則に従う

③分布の裾，とくに，小規模の情報漏洩事象では，公表されていないものを補正することで，分布の小さい部分もべき乗則に従う

以上のことからは，情報漏洩の規模と件数の分布がべき乗則に従い，スケールフリーとなっていることが結論づけられる．

3 べき乗則の背景にあるもの

3.1 個人情報の特性について

2.3節で述べた情報漏洩の規模と件数の分布がべき乗則に従う理由について検討する．

① 個人情報とITの関係

個人情報のIT化について検討する．個人情報は，ITが普及する前からビジネスの有効なツールであった．しかし，個人情報の活用が脚光をあびるようになったのは，ITが利用されるようになった1970年代以降である．さらに，1990年代には，パソコンの能力向上とコスト低下にともなって，より広くビジネスにITが利用されるようになった．そのため，ビジネスでは，ITを利用した個人情報の集積が進み，広く利用されるようになった．

② 個人情報のデータベース化

次に，個人情報がITを利用してデータベース化される誘因について考えてみる．個人情報をビジネスで利用するのは，主に顧客へのプロモーションとアフターサービスである．プロモーションの場合には顧客に関する属性情報をもとに売り込む商品を決めたり，新しい商品のコンセプトに合う顧客を検索したりする．紙ベースで顧客情報を管理している場合と比べると，効果が高い．一方，アフターサービスでは，顧客からの問い合わせに対してタイムリーに対応することで顧客満足度を高め，顧客を囲い込むことができる．具体的には，顧客に販売した製品が何で，いつ販売したのか，その履歴はどうなのかなどが個人情報と併せてデータベース化されるようになっている．また，販売した後にも，顧客に問いかけて製品の状況や不満などを聞くことができる．すなわち，個人情報の活用がビジネスの鍵であり，顧客の個人情報をITで管理

できることで，顧客を囲い込むツールがより強化される点が大きな誘因となる．すなわち，個人情報のデータベース化は，ビジネスの観点からみると大規模化に向かうと考えられる．

③　個人情報の漏えいの管理

個人情報は，①に述べたようにビジネスの有用なツールであるため，利用される頻度が高い．また，個人の情報は時間とともに変化するため，個人情報保護法への準拠のため，事業者は常にデータベースのアップデートが必要である．また，同意を得て関連会社などに利用させるようなケースもあり，管理が十分出ないケースも起きる．

さらに，②に述べたように，データベース化されていると，利用価値が高まるが，管理面でこの違いを認識できず，従来通りの管理にとどまることが多い．しかし，競争環境下では，競合相手にとっても大きな価値を持っているため，個人情報自体が価値を持ち，ブラックマーケットでは，高く販売される．そのため，個人情報の管理者がモラルハザードをおこすと犯罪につながるケースが増えると考えられる．

以上により，個人情報がIT化され，さらには，データベース化されるという特性は，カーツワイルの述べる収穫加速の法則に従う[3]といえる．すなわち，データベースは，高度化され，大規模化するほどその効用が増す．その反面として，個人情報が集積されて大規模化することで，個人情報を集めたデータベースの相対的な価値が高まり，大規模な個人情報の漏えいのリスクも高まる．

3.2 IT化された個人情報の持つネットワークの外部性について

2.2節では，ネットワークの特性を持つ場合，べき乗則に従う例が述べられている．個人情報がIT化された場合には，3.1節に述べたように，収穫加速の法則に従って，「多くの個人情報が集まるほどその効用が高まる」．これについて，以下に考察する．

①　ITの利便性の向上

個人情報は，収穫加速の法則にしたがって，一般的にデータが多く集まるほど利便性が高まる．そのため，競争状態にあるサービス業では，ある事業者が情報システムを利用して個人情報をデータベース化すると，その利便性が高まり，他の競争業者に対して競争優位に立つ．このことから，データベース化が競争の重要な要素として，競争時強者間に広がる．そのため，業界として見た場合の個人情報のデータベース化がより広がっていくことになる．これは，IT化によるネットワークの外部性と呼べるであろう．

②　ITのハードウェアの進歩

[3]　カーツワイルは，IT の変革を収穫加速の法則としてとらえ，「広義の有用な情報量である秩序とカオスと時間の関係の一般法則の下位法則」として位置づけている．[12]

ITのハードウェアの進歩により，情報のCPUがムーアの法則に従い，ほぼ2.5年に能力が2倍となっていることが知られている[4]．また，同様に，蓄積メディアの大容量化についても，同様な傾向にあることが知られている．とくに，データベースの処理では，蓄積メディアによる蓄積量とこれを検索するときの情報処理の能力が大きく影響する．この両者に通信ネットワークの容量増加とコスト低下が加重する．事業者においては，個人情報については，競争面，コスト面から，ITで管理するようになる．

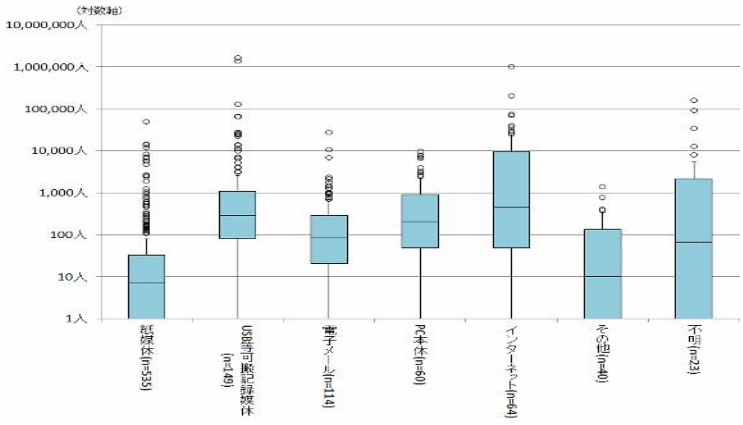

図6　漏えい経路の漏えい人数（箱ひげ図）{1}より

図6に媒体別の情報漏えいの箱ひげ図を示す．どのメディアも，漏えい人数の多い裾が長い分布を示していることが分かる[5]．とくに，可搬型メディア（左から2番目）とインターネット（左から5番目）の２つの分布の裾が長いことが分かる．これは，可搬型メディアの蓄積容量が向上しており，一度，漏えいすると大規模な漏えい事故となる．

③　顧客環境の変化

顧客においても，同様なIT化が進んでいる．すなわち，利用できるパソコンやスマートフォンなどの能力向上とコストの相対的な低下により，データをパソコンなどで扱うケースが増大している．また，インターネットの規模と通信速度が飛躍的に高まっている．そのため，インターネットで個人情報を利用するケースが増大している．これらに相まって，IT化が進んでいる．

以上の①～③による環境変化に伴う特性と，人間は情報処理に関する管理ミスや事

4 ムーアの法則については，学者の中でも見解が分かれている．技術的な限界から外れてきているというものと，巨視的な視点で見れば，他の技術がカバーして相対的には法則が維持されているという観点である．本稿では，文献[10]の立場にたち，今後もムーアの法則は継続するという立場をとる．

5 サンプル数の関係でべき乗となるかは今後の課題である．

故を確率的に起こすという習性を考慮すると，今後も，企業や組織においてデータベース化が進み，図1に示すように情報漏えい件数が今後も増大していく考えられる．ところが，①～③の特性は，指数的な増加であり，このことが，情報漏洩の規模と件数がべき乗則につながると一因と考えられる．

3.3 個人情報の持つネットワークの外部性

2.2節では，ネットワークの外部性を持つ場合に，その分布がべき乗となることを述べた．3.2節で述べたように，個人情報の場合も，データの利用にネットワークの外部性が見られることからもべき乗則に従うことが想定される．したがって，情報漏洩事故がネットワークの外部性を持つことにつながる．ただし，ネットワークの外部性をもつ場合，べき乗分布に従うことが，述べられている[13] [14]ように，今後，モデルなどでの検証が必要である．

個人情報がネットワークの外部性を持つことから，企業の経営やマネジメントは，以下のような観点が必要となろう．

データベースの規模が大きくなるほど，漏えいのリスクが高まると想定して，対応策を検討する必要がある．これは，データベースが管理するデータが2倍になったときに，そのデータベースの持つ効用は2倍以上となる．そのため，リスクは，この効用に比例するので，データベースが大規模になればなるほど，リスク対策をきちんとする必要がある．

4 情報漏えい対策としてのBCM/BCP

4.1 既存の個人情報漏えい対策

多くの企業や組織では，情報セキュリティのマネジメントを導入している．これらの最も広く利用されているISMS[15]，[16]をベースに議論する．ISMSを実施する場合には，個人情報などの情報資産を特定して，リスク分析を実施する．リスク分析の結果，このリスクを低減するために情報セキュリティ対策として管理策を実施する．

ただし，ISMSなどの情報セキュリティで用いるリスク分析では，多くの場合，「ある事象の結果とその発生の起こりやすさとの組合せとして表現される」ことが多い[17]．これは，大規模な情報セキュリティ事故の発生確率は小さく，ほどんど無視できることによる．しかし，2章で述べたように，情報漏えいの事故は正規分布に従うのではなく，より，裾の長い分布であることが分かっている．したがって，大規模な情報漏えいが必然的に起きるという前提を仮定する必要があり，大規模な情報漏えいを無視することはできない．

また，大規模な情報漏えいについては，経済産業書が，ITサービス継続ガイドラインを改訂して，「これらのケースには，大規模な自然災害によるもの，標的型攻撃やサイバー攻撃によりIT サービスが中断するもの，個人情報などが持出などによって外部に流

出してビジネスが停止されたもの，IT の部分的な機器故障が波及してビジネスやサービスが継続できなるものなどがある．」[18]と述べている．すなわち，大規模な個人情報の漏えい事件については，ISMSなどの定常な状態を対象とした対策ではなく，緊急時を対象とした対応が必要としている．しかし，ITサービス継続ガイドライン（改訂版）では，東日本大震災への対応の改訂が喫緊の課題であり，ほとんど自然災害からの回復について述べているだけである[18]．

そこで，[3]や [4]では，大規模な個人情報漏えい事故を定義して，その対応策としてのBCP/BCMが検討されている．

4.2 大規模な個人情報漏えいの定義

2章の分析は，あくまでも，大規模な個人情報の漏えいが発生するというマクロのレベルの概念であり，個々の企業や組織に大規模な個人情報漏えいが発生するというものではない．企業や組織の規模はさまざまであり，取り扱っている情報量も異なる．したがって，大規模な情報漏えいが起きるとしても，企業によって異なる．そこで，BCP/BCMによる対策を検討する場合，企業にとって必要な「大規模な個人情報漏えい」を定義する必要がある．

そこで，[3]や [4]では，BCP/BCMを考える際の考え方として，事故の評価尺度を被害人数の絶対量ではなく，自組織の情報漏えい事故が引き起こす結果のインパクトの観点から検討すべきとしている．ENISAでは，個人情報の漏えいの事業インパクトの観点からの情報漏えい事故の評価指標を提案している[19]．このうち，評点6 に該当するものを大規模な個人情報漏えい事故と考えるのが適切とした[3]．

ただし，この定義ではビジネスの回復不能と定義しており，ビジネスを回復させる形でのBCPの対策がとれるかは別である．これは，個人情報漏えいの場合，漏えいした情報を現状回復できない場合も想定する必要があるからであろう．

表 1 情報漏えい事故の評価指標[19]（邦訳は[3]による）

評価スケール		
評点	レート	引き起こす結果
1	低い／僅か	無いか、無視できる。
2-3	中間	深刻ではない。克服できる経済的損失。
4-5	高い	やや重要な経済的損失や社会的評価の低下が発生するが克服できる。
6	非常に高い	回復不能な極めて深刻な事象の発生。（例えば関係者の健康的被害、重度の経済的損失、社会的評価の低下）

4.3 情報漏えいへのBCP/BCMの適用

情報漏えい対策として，BCPのモデルを適用する場合には，自然災害など物理的な被害がある場合と分けて考える必要がある[18]．これは，個人情報漏えい事故では，物理的な被害を受けることは少なく，すぐに判明しない場合もある．とくに，個人情報のデータベースのコピーが密かに持ち出された場合には，検出が難しい．インシデント調査の多くの事例では，企業が管理している顧客情報が不正に利用されて，顧客に被害がでて初めて事故が判明するケースが多い．事件が発覚したときには，企業のIT機器には何らの物理的な損傷もなく，ビジネスは継続している．ただし，経営判断で，ビジネスを中断する場合が多い．自然災害の場合には，BIAは想定した災害をベースに実施すればよいか，個人情報漏えいのケースでは，BIAを事件の検出時に実施することが求められる[3]．

このようなBCPのモデルには，図7のように事件が発生しても影響がすぐに出ないタイプ[20]となり，事件の早期の発見が必要となる．とくに，影響が大きいケースは，例えば，多数の顧客のクレジットカード情報が漏えいするような場合には，その時点で，ビジネス全面的な停止が必要となルようなケースであり，ビジネスの再開までには時間がかかることになる．とくに，大規模な情報漏えいの場合には，機会損失にも考慮しなければならない．

図7　事件の影響がすぐに現れない場合（文献[21]より）

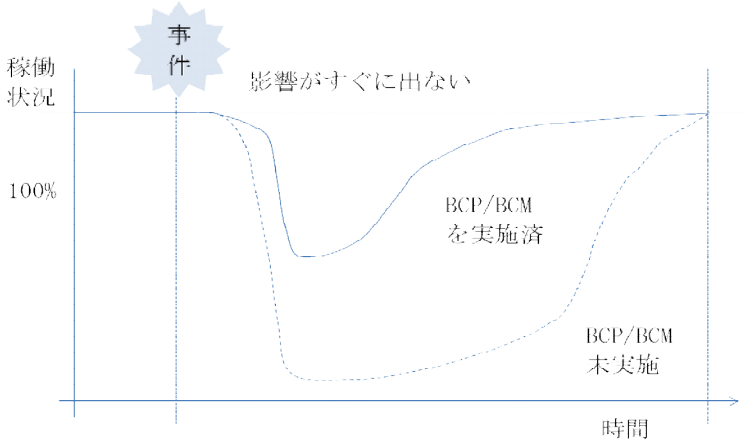

図７の場合には，事件がいつ検出されても対応できるような事前の対策が重要となる，ただし，情報漏えい事件では，従来のBCP/BCMの多くがビジネスの機器の復旧を前提として設備の回復・再稼働をベースに全体像を計画して整備している[22]ため，そのままの適用は難しい．

4.4 企業経営の視点からの情報漏えい対策

企業や組織では，東日本大震災を契機に内閣府のガイドライン[23]をベースに

BCP/BCMの整備が進みつつある．

大規模な個人情報漏えいを想定したBCP/BCMについては，個人情報の漏えいという特性を生かした対応策が望まれる．これには，次の６つのステップが必要となる[4]．

① 事前対策

個人情報の漏えいという特性を考慮したBIAを実施する．

② 検出

事件をいち早く検出することが重要である．IT機器のモニタリングのみならず，インターネットなどの情報や金融機関・カード会社などとの連携を図り，疑わしい情報を素早く入手できる仕組みを構築する．

③ リアルタイムBIA

検出されたときに素早く判断して対応できるための事前対策が重要であるとともに，事故に対応して，ビジネスをどのように継続・再開するかを検討する．この場合，検討している時点での被害状況，利用できるリソース，対応策などを再検討し，実施の優先度を決める必要がある．これは，事前には全て想定しきれないので，検出後に速やかに実施することが求められる．

④ ビジネスの制限やフォレンジクス

ビジネスの停止も含めたビジネスの制限（縮退）を実施する．とくに，二次被害を防止する事や情報システムなどのフォレンジック調査等による原因調査の観点からビジネス制限することが求められる．

⑤ ビジネス再開

停止したビジネスは，二次被害の発生や世論の動向などを見極めながら再開する．

⑥ PDCAの維持と監査

気象や組織ではビジネスが再開したあと，得た教訓をきちんと文書にして残しておくとともに問題点を洗い出すために監査を実施することが望まれる．監査のあと，ビジネスの観点からBIAを見直すことも重要である．

まとめ

情報セキュリティインシデントに関する共同研究の調査の結果を分析して，個人情報漏えい件数の分布は裾が長く，べき乗則に従うことが分かった．このべき乗則については，近年研究が進み，スケールフリーの特性や大規模な事件や事故が実際に起きることが知られている．

本稿では，情報漏えいの分布がべき乗分布となる背景を検討し，企業における個人情報の情報処理がIT化され，大規模に管理されるようになったことの負の側面であることを示した．企業や組織にとって，IT化による高度化は避けられないものであり，漏えいした際の対策が必要となることを示した．

さらに，本稿では，大規模な情報漏えいが起きることを想定する場合の対策には，情報漏えいを想定したBCP/BCMが利用できることを述べた．さらに，この場合のBCMの問題点は，自然災害の場合とは異なって事件の検出が困難なことである．ただし，検出できなければ，BCP/BCMを発動することができない．そこで，事件が検出されたあと，早期の復旧をするために，再度，BIAを実施する考え方を示した．

なお，本稿では概念を示しただけであり，今後，実際の企業や組織を対象にしてより具体化することが必要である．

謝辞

本稿をまとめるにあたって，情報セキュリティ大学院大学の教員，研究室の学生や研究生から得られた温かい助言や調査への協力に感謝する．

参考文献

［１］NPO日本ネットワークセキュリティ協会，情報セキュリティ大学院大学，2011年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～，2012年9月

［２］NPO日本ネットワークセキュリティ協会，2010年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～，2011年年8月

［３］菅原尚志，新原功一，小倉久宜，鈴木宏幸，原田要之助，大規模な個人情報漏えいの特性を考慮した対策について，システム監査学会第26回研究大会，2012年6月

［４］鈴木宏幸，新原功一，小倉久宜，根岸秀忠，原田要之助，大規模な個人情報漏えいの特性を考慮した事業継続対策について，システム監査学会第25回公開進歩シンポジューム，2012年11月予定

［５］Richter, Charles F.，”An instrumental earthquake magnitude scale，” Bulletin of the Seismological Society of America』, 1935年1月

［６］マーク・ブキャナン，歴史は「べき乗則」で動く，ハヤカワ文庫，2009年

［７］会田雅樹，物理の現象論に学ぶ-通信ネットワークに現れるべき乗則を利用した社会ネットワーク構造の解明，電子情報通信学会 vol.91，No.10，2008年

［８］湯田聰夫，小野直亮，藤原義久，ソーシャル・ネットワーキング・サービスにおける人的ネットワークの構造，情報処理学会論文誌　vol.47，No.3，2006年

［９］Réka Albert and Albert-László Barabási, Statistical mechanics of complex networks, Rev. Mod. Phys. 74, 47-97 (2002)

［10］アルバート・ラズロ・バラバシ，新ネットワーク思考—世界のしくみを読み解く:訳青木 薫，NHK出版，2002年

［11］辰巳憲一，金融活動における情報ネットワークと金融仲介業，学習院大学　経済論集

第47巻　第1号，2010年4月
［12］NPO日本ネットワークセキュリティ協会，情報セキュリティインシデントに関する調査報告書～発生確率編～，2011年4月
［13］レイモンド・カーツワイル，スピリチュアル・マシーン　コンピューターに魂が宿るとき：;田中三彦・田中茂彦訳，翔泳社，2001年
［14］レイモンド・カーツワイル（Raymond Kurzweil），ポスト・ヒューマン誕生 コンピューターが人類の知性を超えるとき：井上健監訳他，NHK出版，2007年
［15］日本規格協会，JIS Q27001:2006（情報技術―情報セキュリティマネジメントシステム―要求事項），2006 年
［16］日本規格協会，JIS Q27002:2006（情報技術―情報セキュリティマネジメントの実践のための規範），2006年
［17］ISO，ISO31000:2009，Risk Managemeent - Principles and guidelines，2009
［18］経済産業省，IT サービス継続ガイドライン改訂版，2005 年 3 月
［19］ENISA，Recommendations on technical，implementation guidelines of Article 4，2012
［20］ISO/IEC，ISO/IEC27031，Information technology -- Security techniques -- Guidelines for ICT readiness for business continuity，2011 年 3 月
［21］原田要之助，東日本大震災に学ぶ事業継続計画と IT の在り方:組織における IT リスク管理，情報セキュリティ総合科学（紀要）vol.3，2011 年
［22］経済産業省，事業継続計画策定ガイドライン（企業における情報セキュリティガバナンスのあり方に関する研究会報告書・参考資料），2005 年 3 月
［23］内閣府，事業継続ガイドライン 第二版― わが国企業の減災と災害対応の向上のために ―，2009 年 11 月