＜研究論文＞

大規模個人情報漏えい事故の特性を考慮した事業継続対策

Issue of the business continuation measure which considered the specific characteristic of the large-scale personal information leakage

鈴木　宏幸　Hiroyuki Suzuki
新原　功一　Koichi Niihara
原田　要之助　Yonosuke Harada
情報セキュリティ大学院大学　情報セキュリティ研究科

要　約

筆者らはNPO日本ネットワークセキュリティ協会(以下JNSA)と情報セキュリティ大学院大学(以下IISEC)が協力して2011年から2014年まで実施したインシデント調査に参加し、個人情報漏えい事故の規模と頻度がべき乗則に従う事を発表した[1][2]。べき乗則に従う代表例には、地震の規模と頻度がある[3]。地震では事象が起きたことを想定した対策が取られている。一方、情報漏えい事故の場合、情報漏えいの発生を防ぐための対策を充実させ漏えいリスクを受容できるレベルまで下げるという考え方が主流である。しかし、べき乗則で発生する情報漏えい事故に対しては事前対策のみでなく、事後対策を踏まえたBCP(Business Continuity Plan: 事業継続計画)の策定を行うべきである。

本稿では大規模個人情報漏えい事故の発生傾向を把握し、事業に与える影響分析の考え方、対策の必要性について分析を行い、BCPの策定とその作成ポイント、有効性評価に対する考察を実施した。

キーワード：個人情報漏えい事故、リスク分析、情報セキュリティ対策、事業継続計画、システム監査

1．はじめに

IISECとJNSAでは、新聞やインターネットニュースなどで報道された個人情報漏えい事故の情報を集計し､分析した結果を「情報セキュリティインシデントに関する調査報告書」として公開している[4]。個人情報漏えい事故は毎年発生し続けており、一度に大量の個人情報が漏えいする事故も毎年発生している。本稿では個人情報漏えい事故の調査結果からその法則性を見出し、個人情報漏えい事故の事業継続対策について考察する。

2．個人情報漏えい事故の発生

毎年数件、一回当たり大量の個人情報が漏えいする事故が発生している。これは個人情報漏えい対策が進む中で防げなかった事故と考えられ、以下で述べるべき乗則のロングテールの法則に当てはまる。

2-1 べき乗則

べき乗則は、近年複雑系の中で研究がなされ様々な事例が判明している。べき乗則では以下の特徴がある。

(1) ロングテール

べき乗則は正規分布のように平均付近に集中せず分布のすそが長く続くのが特徴である。

(2) スケール不変性

スケール不変性とはどの尺度で拡大しても、同じような特徴が出現することである。これは大きな出来事も小さな出来事も同じメカニズムのもとで生成されており、大きな出来事が何か特別な理由によるものではない事を意味する。

べき乗則に従う代表例として、地震の頻度と地震の規模を示すグーテンベルグ・リヒター則が知られている。地震の発生回数は非常に多いが、社会生活に重大な影響を与える大地震は発生回数でいえば僅かな回数である。

2014/3/24受付　2015/12/14受理

(3) 個人情報漏えい事故の件数・規模分布

個人情報漏えい事故の件数と規模についてJNSAの2011年の調査結果を対数軸で表現した結果、べき乗則となる事が分かった。これを図1に示す。同様に2010年の分析結果を図2に示す。また、2005年から2010年の全体の個人情報漏えい事故の全体を対象に分析した結果を図3に示す。どの分析結果も同様にべき乗則に従う事を示しておりスケール普遍性の特性が確認できる。

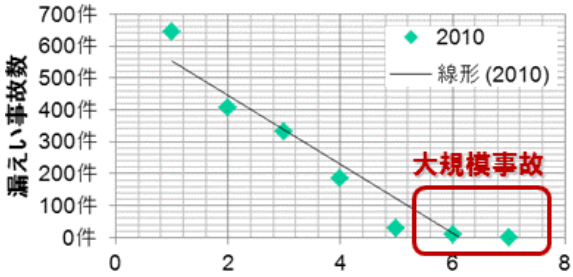


図1　2010年の調査結果を対数軸で分析

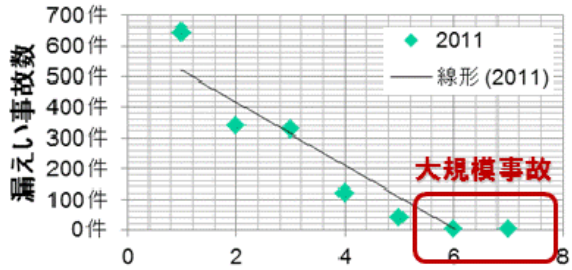


図2　2011年の調査結果を対数軸で分析

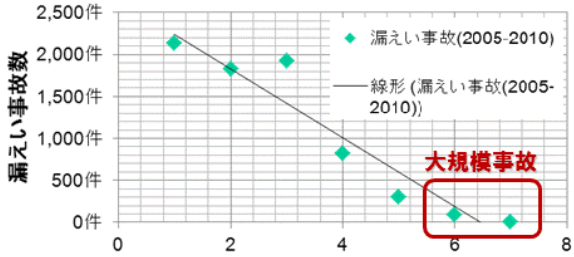


図3　2005～2010年の調査結果を対数軸で分析

2-2　個人情報漏えい事故での個人情報の流出経路

個人情報漏えい事故の個人情報流出経路について紙媒体、電子媒体、ネットワーク経由等流出経路別調査の調査を行い、事故一件当りの個人情報の漏えい人数について箱髭図を用いて分析した。箱髭図を用いて分析する事により例外的な事故の値を除外し、傾向を分かり易く把握する事ができる。図4は個人情報漏えい事故一件当たりの漏えい経路別の漏えい件数の箱髭図である。図4から「USB等可搬記録媒体」「PC本体」「インターネット」は他の項目と比べて箱髭図の箱の部分が図の上部にあり、被害人数が大きい。このことから被害人数の大きい個人情報漏えい事故はITを経路として多く発生していることがわかる。

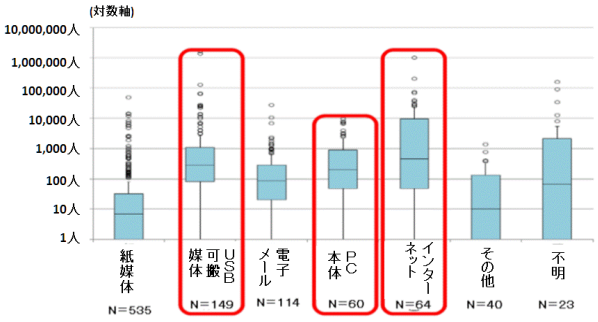


図4　個人情報漏えい経路別の漏えい人数

2-3 大規模個人情報漏えい事故の定義

本稿では大規模個人情報漏えい事故を「企業の存続に重大な影響を及ぼし、個人情報の当事者を含むステークホルダの利益を大きく損なう恐れがあると評価された個人情報漏えい事故」と定義する。また、大規模個人情報漏えい事故は企業の経営の影響が大きいためBCPの対象とすることが考えられる。BCPの対象範囲をITサービスの継続を脅かす可能性がある大規模個人情報漏えい事故とする。なお本稿でのITサービスの継続の定義は、経済産業省ITサービス継続ガイドライン改訂版の「ITサービス継続とは、事業継続の一部であり、ITサービスの中断・停止による事業継続に与える影響を求められるサービスレベルに応じて最適化するための取り組みである」[5]によるものとする。

2-4 事業に与える影響

個人情報漏えい事故では一般的に「漏えい日時(期間)」、「漏えいした個人情報の種類」、「漏えい件数」、「漏えい経路」が個人情報漏えい事故の発生組織よりステークホルダーに報告される。個人情報漏えい件数が大量になる場合、多くのメディアにて事故が報道される。一方、個人情報の漏えい人数の絶対値のみだけでは情報漏えい事故を起こした組織の事業に与える影響を決定できない。

これは漏えい件数は同じでも漏えいした個人情報の内容、重要度によって与える影響は変化するからである。

ENISA（European Network and Information Security Agency）では事業に与える影響の観点から情報漏えい事故の評点を公開している。[6]

この評点を表 1 に示す。この評点に対して漏えい対象情報の種類、件数と影響度を勘案し、大規模個人情報漏えい事故の基準とする事が考えられる。

評点	レベル	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害。
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	回復不可能な極めて深刻な事象の発生。 （たと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）

表 1　ENISA の情報漏えい事故の評点レベル [6]
指標を筆者らにて邦訳 [2]

BCP は経営に影響する事故毎に作成される。大地震、パンデミック等の BCP は作成済みの企業が多くなってきている。大規模な個人情報漏えい事故を BCP の対象にするためには新たな定義が必要になる。すなわち組織内で大規模個人情報漏えい事故の基準を取り決め、個人情報漏えい事故の影響を他と同じ基準で算出し比較できる事が重要である。

3．大規模個人情報漏えい事故に対する BCP の必要性と対象範囲

企業組織の活動においては、大地震を代表とする自然災害、パンデミック、製品事故に伴う巨額損害賠償等を継続的な事業継続の阻害要因として想定して、事業活動継続に対するリスクとして捉え、事前対策としてリスク分析を実施し、万一の事故発生後の危機管理対策を策定している。同様に大規模個人情報漏えい事故についても 2-1 節に述べたように一定の割合で必ず発生し、活動の阻害要因となるため、企業の BCP の対象に含める必要がある。

3-1 BCP で想定される脅威

IISEC 原田研究室では 2013 年 7 月から 8 月にかけて P マーク取得企業、ISMS 認証取得企業、官公庁、教育機関など 4,500 組織の情報セキュリティ・システム担当者に対してアンケート調査を行い 367 件の回答を得た [7]。本調査では BCP の策定状況について設問し回答を得た。BCP 策定済の回答が 41%、今後策定する予定 / 検討を含めると 88% の組織が BCP を意識した活動を実施している。BCP が想定する脅威に対する回答を図 5 に示す。図 5 からは、地震、津波、洪水、竜巻、台風などの気象災害（124 件）、火事（111 件）、パンデミック（102 件）に続き、個人情報漏えい事故（サイバー攻撃以外）（90 件）が 5 番目になっている。さらに、この個人情報漏えい事故は、サイバー攻撃（55 件）より上位となっていることから、個人情報漏えい事故の方が脅威が高いとする組織が多いことが分かる。すなわち、個人情報漏えい事故が組織の活動を阻害する大きな脅威と認識されている。また、調査結果からは個人情報漏えい事故の主要な対策である IT-BCP（Information Technology- Business Continuity Plan: IT サービスにおける事業継続計画）を策定済の組織が 25%、今後策定する予定、検討中を含めると 64% の組織が IT-BCP を意識しているとの結果となった。IT-BCP の対象については IT サービスの停止（33%）に対し、個人情報の漏えい（64%）が倍近い値となっている。IT-BCP を策定するにあたっては個人情報の漏えいを多くの組織がより重要と認識している。

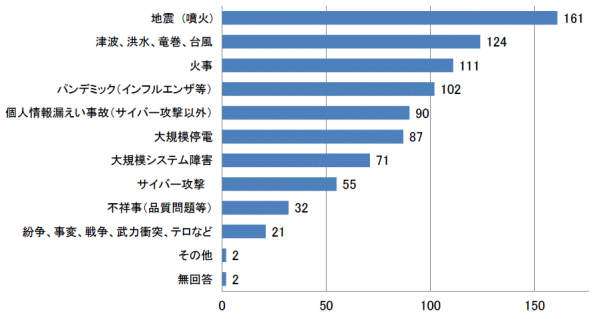


図 5　事業継続で想定されている脅威

3-2 事故前提の対策の必要性

従来の個人情報漏えい事故対策は事前対策が主であり、情報漏えいのリスクを下げる活動（JIS

Q 15001:2006、ISO/IEC27002 等の管理策導入による事故防止）が中心であった[8]。

2-1 節に述べたように、2005 年度から 2011 年度までの「情報セキュリティインシデントに関する調査報告書」では 1 回当たり 10 万件以上の個人情報が漏えいする事故が毎年度発生しており、大規模個人情報漏えい事故がべき乗則分布に従って一定の割合で発生している。この事実からは、個人情報漏えい事故が発生することを前提として、事故後の影響を最小限に下げるという事後対策もふまえた対策が必要である。以下では、事故後をふまえた BCP 対策について検討する。

3-3 BCP の対象

2-2 節では、IT を漏えい経路とした漏えい人数が比較的多いことを述べたが、当該事故の事後対策が組織の保有する IT サービスの中断や停止を伴う場合、事業に与える影響が特に高くなる。一方、PC や、USB 可搬媒体の紛失・盗難が発生した場合、漏えい自体の対応の必要があるが、IT を構成している各システムへの影響は小さい。一方、e コマース等を提供するウェブサイトがサイバー攻撃により情報漏えいした場合、原因究明までの期間は当該サイトを中断して解析や再発防止策を講ずる必要がある。この場合、中断期間は e コマースの売上が途絶えるため事業に与える影響が大きい。

すなわち、情報漏えい事故が事業に与える観点からは、IT-BCP の対象となる。

4. 個人情報漏えい事故が事業に与える影響分析

個人情報漏えい事故が事業へ与える影響は当該組織の事業形態や規模、個人情報の保有件数等により異なる。影響分析の手法として BCP の策定における手法の一つである BIA（Business Impact Analysis: ビジネス影響分析）の実施が有効である。本稿における BIA は経済産業省事業継続計画策定ガイドライン[9]の「組織における重要な事業・業務（基幹事業・業務）、プロセス、それに関連するリソースを特定し、事業継続が及ぼす影響の分析を行う」に基づく。

また、本稿では、影響分析の対象範囲としては組織の事業継続の観点から組織自体に係る影響を対象とする。

組織は IT サービスを提供する情報システムに脆弱性が確認された場合、脆弱性の内容に応じた BIA の実施基準が必要となる。システムの脆弱性に関する情報として、例えば独立行政法人情報処理推進機構（以下では IPA: Information-technology Promotion Agency, Japan）の「重要なセキュリティ情報」に該当する製品の情報が掲載されたときや、ベンダから導入した製品やシステムの脆弱性に関する通知が利用できる。これをタイムリーに実施するには、組織内で BIA を実施する基準と BIA 責任者を定めておく事が重要である。

4-1 保有情報・業務・システムに着目した分析

大規模自然災害を対象とした BIA では主に組織とインフラ関連のリソース損失の影響を分析する。一方、大規模個人情報漏えい事故の場合には保有する情報に着目することが必要となる。すなわち、大規模個人情報漏えい事故の場合、事故が発生した時点ではリソース自体の損失は起こらないが、その後に発生する事後対応による事業の中断、対応リソース要求、お詫び金の支払いや問い合わせ対応、再発防止の対策実施等においてリソース不足が発生して、事業に大きな影響を与える。

また、大規模個人情報漏えい事故では、流出した個人情報の件数、個人情報の重要度、個人情報を使用している業務に対する組織の依存割合、個人情報を取り扱うシステムの数、重要度などが事業に大きく影響を与えるため、これらに着目した BIA を実施することになる。BIA を行うには事業の現状把握、リソース分析を行うための対象となる事業概要、業務フロー、ステークホルダー一覧、想定リスクパターンが必要となる。これらに加えて大規模個人情報漏えい事故に特有なインプットとして以下の情報が必要となる。

(1) 保有している個人情報の一覧

組織が保有している個人情報の一覧である。個人情報について属性、件数、入手元とともに保管先（社内､社外（データセンター等））形態（紙、電子媒体、データベース）について一覧化しておく。また、顧客を特定するための ID やパスワード等も BIA の際に分析・評価の対象となる。

(2) 情報と業務の関連図、業務と業務の関連図

組織における個人情報の業務利用のドキュメントを用意する。情報と業務の流れを示した DFD (Data Flow Diagram: データフロー図)を用意し、DFD を階層別にたどる事により業務と業務の関係、個人情報を含む情報の業務間の流れを確認す

る。

(3) データベース一覧

個人情報を取り扱うシステムでは各情報システムが使用しているデータベースのテーブルレベルの一覧が必要である。

(4) 個人情報のデータライフサイクルを把握できる資料

データベース一覧ではデータベース内のテーブル毎に個人情報の格納場所等のスタティックな把握は可能である。しかし、個人情報の作成、登録、活用、消去のデータライフサイクルについては確認できない、これを把握するためには CRUD 図（Create Read Update Delete 図）等データライフサイクルを記した資料を用意する。これらの資料はシステムの拡張、更新に合わせて最新の状況にしておく事が必要である。

4-2 被害額の算出手法

BIA ではまず対象業務に対して事業継続・復旧の優先順位付けを実施するが、大規模個人情報漏えい事故の場合では事故発生の場合に蒙る被害が大きい業務を優先する。被害の大きさを計る尺度としては漏えいした個人情報の件数だけでは不十分であり、被害の金額等を評価尺度とする。

情報セキュリティ事故における被害額の算出手法として IPA が「被害額算出モデル」を発表している。当該モデルは情報漏えい事故により発生する損害の費用を積み上げ、事故 1 件当たりの被害額を算出する。具体的には費用を以下の 4 つの被害分類として明細を積み上げて算出する [9]。

- 表面的被害（顧客対応費用、システム復旧費用、逸失利益等、直接現れてくる被害）
- 潜在的被害（システム停止期間中の業務効率低下等、潜在的な被害）
- 対外対応費用（損害賠償、お詫び金、広告等に費やした費用）
- 新規情報セキュリティ投資（事故を機に新たに導入する機器、システム監査、教育等の投資）

当該モデルにより組織は人件費、設備費用、想定損害賠償額、お詫び金などの詳細金額が算出でき、分析結果はより具体的なものとなる。なお、当該モデルにて抽出した項目の一部（例えば、広報宣伝活動費用、新規情報セキュリティ投資費用など）は情報漏えい事故発生時の対応そのものであり、必要に応じて BCP に取り込む事が可能である。図 6 に被害額算出モデルによる算出例を示す。

費用項目			
大分類	中分類	項目	損失額明細
対外対応費用			
	損害賠償請求への対応費用		
		カード不正利用に関しての補填額	2,400,000
		人件費（調査・手続き等）@6.5万 / 2日 × 2人	130,000
	お詫び金支払い対応費用		
		（お詫び金なし）	
	広告宣伝活動に要した費用		
		謝罪会見（準備含む）	
		人件費 @6.5万 / 日 × 8人	520,000
		新聞に謝罪広告掲載	4,000,000
		WEBに謝罪ページの掲載	600,000
		被害者への連絡通信費用	2,150,000
		24,322名へ個別に説明文書を送付	
		24,322 × 68（通信費+印刷費）	
	問い合わせ窓口の設置（設置期間二ヶ月） フロアは社内に確保		
		窓口人件費	
		総括社員 @6.5万 × / 日 × 60日 × 2人	7,800,000
		臨時オペレータ @2万 × / 日 × 60日 × 2人	3,500,000
		通信費	
		@2万 × 60日	1,200,000

図 6　被害額算出モデルによる算出例（一部）

4-3 個人情報の価値算出

被害額の算出に当たっての大きな課題に、個人情報の価値の算出がある。個人情報の属性によって流出した場合の影響度は大きく変動する。例えば、メールアドレスのみが流出した場合と、クレジットカード番号が流出した場合では、後者の方が遥かに影響は大きい。

個人情報の価値を分析する方法として情報を経済的損失レベルと精神的苦痛レベルを各 3 段階に分けた S-EP 図（Simple-EconomicPrivacy 図）が挙げられる [10]。図 7 に S-EP 図を例示する。S-EP 図では個人情報の属性を 9 つの領域に分類し、各領域の重み付けを行う。例えば、S-EP 図による各個人情報のレベルは以下のようになる。

- 氏名のみ流出
  経済的損失 Lv：1　精神的苦痛 Lv：1
- 年収情報が流出
  経済的損失 Lv；2、精神的苦痛 Lv：2
- カルテ情報が流出
  経済的損失 Lv；1、精神的苦痛 Lv：3

なお、個人情報の属性の重み付けには過去の事例や公表された個人情報漏えい事故でのお詫び金の情報等により社内・組織内で事前に基準を定めておく。

また、個人情報の価値設定について櫻井は消費者の立場で個人情報が漏えいした際に支払って欲しい金額をアンケート形式で収集、分析し、個人情報の内容によって価値が異なることを示している [11]。

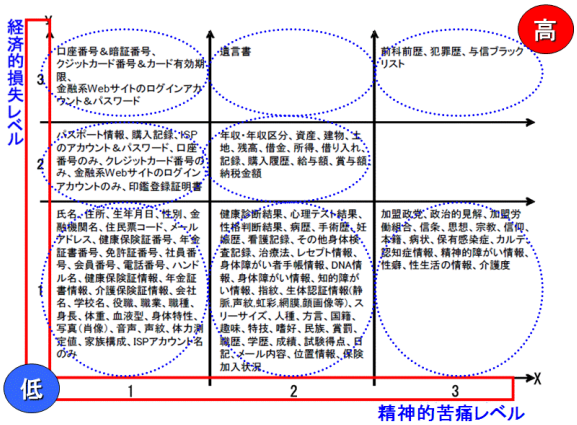


図 7 情報の価値基準の検討（S-EP 図）

4-4 IT サービス操業度の考察

情報漏えい発生から検知までの時間、情報漏えいの検知からそれが大規模個人情報漏えい事故と判断し BCP 発動までの時間、IT サービス業務復旧対応時間を短縮し被害や影響を最小限にする事が大規模個人情報漏えい事故に対する IT-BCP のポイントである [12]。

大規模な個人情報漏えい事故の発生の場合、IT サービスを全面的に停止し対策を行うことが多い。この場合の IT サービスの操業度を図式化すると図 8 のようになる。

図 8 には 4 つの大きな特徴があり、以下に示す。

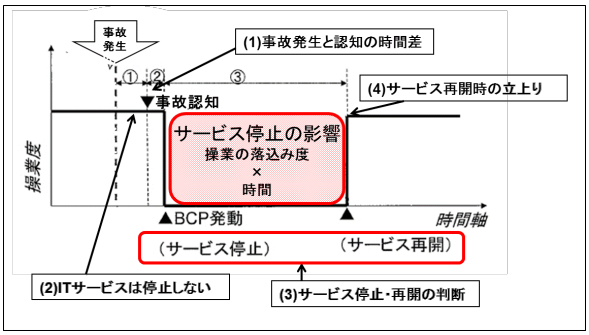


図 8　大規模個人情報漏えい事故発生時の
IT サービス操業度曲線

(1) 事故発生と認知の時間差

大規模個人情報漏えい事故が大規模自然災害と大きく異なる点は、IT サービス利用者はサービスの停止や異常等が無ければ個人情報の漏えいの発生を認知する事が難しい点にある。これは企業が IT サービス提供状況の監視や被害者からの問い合わせ・通報等から事故の事象を知り検証を行って確認して大規模個人情報漏えい事故として認知するためである。そのために、事故の発生と認知の時間差が発生する。

(2) IT サービスは停止しない

大規模個人情報漏えい事故の発生時、IT サービスは自動で停止しない。被害の拡大防止、脆弱性への対応、原因追求等のため、組織の情報システムの判断で IT サービスを停止させている。IT サービスの停止では、サービスの全面停止、サービスの部分停止、サービスの全面続行の 3 パターンがある。これらを選択するためには、IT サービスを提供している情報システムが保有、利用している他のサービスなどの運用などを考慮して、全面停止が必須か、サブシステムまでの部分停止に留めるか判断する。例えば、別のサブシステムが個人情報データベースを参照している場合にはそれらサブシステムの全サービスの停止も必要になる。

(3) IT サービスの停止・再開の判断

IT サービス停止の影響を考えた場合、IT サービスの利用範囲に対応して停止の影響が大きくなり IT サービスの停止が経営を圧迫する事態となることが想定される。したがって、IT サービス停止の判断は、個人情報の担当部門だけでは行うことができず経営判断となる。経営判断をスムーズに行うには、判断基準が事前に整備され、必要な情報がタイムリーに経営者に提供されることが重要となる。

(4) サービスの再開時の立上り

IT サービスの操業度をシステム単位に評価した場合、図 8 の（4）サービス再開時の立ち上がりに示す様にサービスが復旧した時点で操業度曲線は直角に立ち上がる。大地震等からの復旧の操業度曲線は緩やかに立ち上がる [2]。これに比べ大規模情報漏えい事故の場合 IT サービスのリソース（電力、サーバー等の IT 資産、ネットワーク等）は物理的に被害を受けていないので直線的な立ち上がりとなる。

4-5 IT サービス利用度の考察

個人情報漏えい事故が発生し、被害の拡大防止、原因究明のため IT サービスを停止し、復旧した場合、操業度は前述の様に IT サービス停止前と同様のレベルまで復旧し利用可能な状態となる。しかし、事業継続を考えた場合 IT サービスの操業度とは別の指標として、IT サービス利用度が挙げられる。個人情報漏えい事故に対する対応、対策が施され、IT サービスを事故前と同じレベルま

で復旧しても IT サービスが利用されない可能性がある。特に、消費者や住民を対象としたサービスではブランド価値の低下、安全性の懸念等から利用者がすぐに戻らない可能性が高い。有償の IT サービス提供であれば事業の収入源が激減して、事業が継続できない事態となることも想定される。このため IT サービスの利用度合いを平常時から把握しておくことが必要となる。

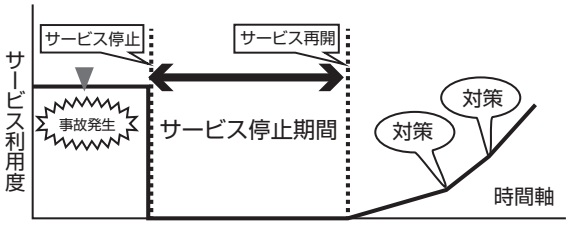


図 9　IT サービス停止と利用度

図 9 に個人情報漏えい事故発生の対処として IT サービス全面停止のケースを想定したサービス利用度の推移を示す。図中の矢印の期間が長い程、IT サービス復旧後のサービス利用度は元に戻りにくいことを示している。サービス復旧直後のサービス利用度はゼロに近く、顧客やユーザへのお詫び、再発防止策の公表、広報／宣伝活動等の対策を実施しない限り、サービスの利用度は事故発生前のレベルまで戻らないと考えられる。すなわち、安全性に対する懸念の払拭など複数の対策を BCP に組み込み対処することが必要と考えられる。

これらの対策はシステム部門のみで実施することは困難であり、全社的な対応が必要となる。人的側面、費用的側面からの影響度を BIA に含めておくべきである。

5．大規模個人情報漏えい事故 BCP の策定

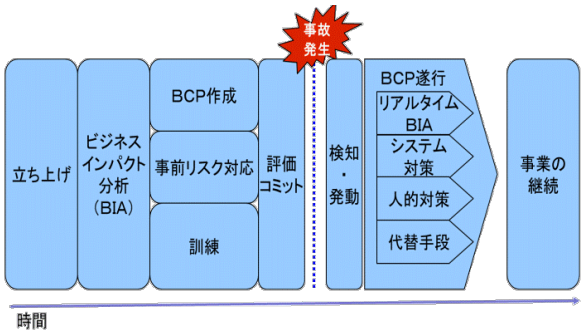
5-1 BCP 策定のプロセス

一般社団法人電子情報技術産業協会、一般社団法人情報通信ネットワーク産業協会発行の「BCP 策定・BCM 導入のポイント」[13] では BCP のプロセスを 2 つに分類している。

・被害の予防／防止
　被害や影響を最小限にする事前対策 / 計画
・重要業務が中断した場合は早期に復旧
　可能な限り早期に再開させる復旧対策

図 10 に大規模個人情報漏えい事故対応の BCP のプロセスを記載する。図 10 の各プロセスの中で大規模個人情報漏えい事故の特性を取り込む事が有効性の高い BCP 策定のポイントになる。

図 10　大規模個人情報漏えい事故対応



BCP のプロセス

5-2 BIA の実施頻度

BCMS（Business Continuity Management System: 事業継続マネジメントシステム）で大規模個人情報漏えい事故を考える場合には、当該マネジメントシステムの運用の中で BIA を実施することになる。一方、IT 分野では技術進歩、利用機器の変化が激しく、常に新しい脅威、脆弱性が発生しており、実施していた対策が一日にして無効になることがある。すなわち、BIA を実施する頻度は一年に一回では不十分であり、BIA を実施するトリガーの基準を制定することが求められる。これを以下に示す。

・組織の大幅な変更
・システムの大幅な追加、変更
・システム基盤に重大な脆弱性が発覚
・システムのアプリケーションに重大な脆弱性が発覚
・重大事象の通報

5-3 個人情報漏えい発生検知の仕組み作り

個人情報漏えいの検知の仕組みを適切に設けない限り、情報漏えい事故発生の検知は偶然頼みとなる。例えば、組織がインターネットに公開する WEB サイトが不正アクセスにより個人情報を奪取された場合、攻撃者が犯行の痕跡を削除し、かつ入手した個人情報を一切悪用しない（又は悪用が気づかれない手段で利用する）ことが考えられる。このような場合、組織がその犯行に気付くことは困難である。

したがって、個人情報漏えいを検知する仕組みを導入し、検知した事象を元に大規模個人情報漏えい事故の発生を判断することが重要となる。検知の仕組みには、トラフィック監視、アクセス監

視、ログ監視などのITサービスからの事象報告に加えて、相談窓口情報（利用者報告、通報など）からの事象報告、ソーシャルメディアの書き込み監視などが必要である。これらの事象を収集し、個人情報漏えいを検知して、経営陣の素早い判断に繋げるための組織対応が必要となる。大規模個人情報漏えい事故発生の検知では、対策チームの体制構築、日常の運用体制が課題である。さらに、検知のための監視業務を自組織で対応できない場合には、セキュリティ監視サービスの活用が候補となる。

6．大規模個人情報漏えい事故BCPに組み込むべき対策

6-1 危機管理／緊急対応体制の確立

JPCERT/CC（Japan Computer Emergency Response Team Coordination Center）では「事故前提」の考え方に基づき、インシデント対応に重点に置いた事中、事後対策のためCSIRT（Computer Security Incident Response Team:緊急対応体制）の必要性を述べている。情報セキュリティの危機管理体制では脆弱性対応、緊急対応、事象分析、普及啓発、対応計画の予行演習等の機能が必要となる。組織内にCSIRTを設置して、大規模情報漏えいを含むインシデント報告を集める窓口を一本化し、部門間調整を行い対策を一元化する。CSIRTは大規模情報漏えい事故が発生してからの立ち上げではなく事前に組織し事故対応の事前準備、組織内外との連携、情報収集を行う。本節ではCSIRTが、大規模漏えい事故に関して実施する機能について述べる。

緊急対応は４つの機能で構成される。

(1) モニタリング（事象の検知、報告受付）

収集可能な情報、今後必要とされる情報、情報を保有している組織を把握しタイムリーに情報収集するための機能。

(2) トリアージ（事実確認、対応の判断）

大規模情報漏えい事故で入ってくる様々な事象に対しての事実確認、事象の重み付け、対応の判断及び優先順位の設定。

(3) インシデントレスポンス（分析、対処、エスカレーション、連携）

組織間の情報共有、情報分析、組織内/外へのエスカレーション、組織を跨ぎ連携した対応。

(4) リスクコミュニケーション（報告、情報公開）

大規模個人情報漏えい事故対応では関係機関への連絡、事故の公表など多様なコミュニケーションが必要となる。自組織においてガイドラインで推奨されるコミュニケーションの検証を行う。コミュニケーションを取るべき対象組織（マスメディアを含む）の数、手段、タイミング等の要素が複雑に絡む為事前のコミュニケーション計画が重要である。

6-2 対応手順の整備

IPAは情報漏えいを７つのケースに分類してケース毎の対応手順等を示している。IISECでは情報セキュリティインシデントの対応フローやチェックリストを公開している。またENISAもRecommendations on technical implementation guidelines of Article 4にてインシデント発生時の対応フローを公開している。これらを有効に活用して組織に合った対応手順を整備することが必要である[6] [14]。

6-3 漏えいルートの調査・分析

個人情報漏えい事故が発生した場合、一刻も早い情報漏えいのルートの特定が必要とされる。経済産業省「事業継続計画策定ガイドライン」は、BCPのケーススタディとして情報漏えいデータ改ざんへの対応を示している[5]。情報漏えいの原因調査は5W1Hであらゆる業務形態、漏えいルートを調査・分析を必要としている。また、調査分析に当たって社内・組織内での対応、外部への委託条件を明確にしておく。

6-4 リアルタイムBIA

情報漏えいの事象を検知し、それが大規模個人情報漏えいと判断した場合、被害拡大を防ぐためにシステムやサービスの縮退運転、代替手段の提供を早急に行なうケースが存在する。すなわち、状況の変化に応じて対応を変えていく必要がある。大規模個人情報漏えい事故発生前のBIAを元にし、リアルタイムで、新たに新しい情報を加味したBIAを行う必要がある。リアルタイムBIAは新たなイベントの発生や新たな事実の判明などイベントドリブンで行なう。特に、リアルタイムBIAの実施方法、実施メンバ、結果のエスカレーションルート等を事前に定めておくことが重要である。

7．大規模個人情報漏えい事故BCPの有効性について

7-1 システム監査の実施による有効性測定

前章まで大規模個人情報漏えい事故 BCP 策定の必要性および策定における留意点について述べた。本章では策定した大規模個人情報漏えい事故 BCP の有効性について考察を行う。

BCP は大きくは被害の予防／防止と復旧のプロセスに分けられるとした。前者においては施策の実施の進行状況、再度リスクアセスメントを実施してのリスクの削減状況が有効性を評価する指標として利用できる。後者においては BCP の総合訓練が該当するが大規模個人情報漏えい事故は IT サービスと密接に関連していて実際にサービスを停止させる程の事故の訓練実施は事業に影響を与える。発災の検知及び情報共有の仕組みを構築して、その運用を訓練すべきである。

大規模個人情報漏えい事故に対する BCP の有効性評価を実施する場合、個々の管理策を個別に評価するのではなく、評価指標をまとめ、組織全体として事業全体の観点から対策を評価する必要がある。この様な評価には全体最適の視点があるシステム監査が役立つ。

7-2 システム監査の位置付け

大規模個人情報漏えい事故 BCP のシステム監査を実施するには、まず BCP が適切に構築され、その一要素として IT-BCP が存在し、更にその中に大規模個人情報漏えい事故 BCP が存在することが必要となる。

IT-BCP のガイドラインは、2011 年に国際標準として ISO/IEC27031 が策定され、国内では経済産業省が「IT サービス継続ガイドライン」を 2011 年に改訂した。これらは IT-BCP に特化したガイドラインであるため、ISO22301 等による事業継続マネジメントシステムを補完する位置付けとなる。IT-BCP のシステム監査は、ISO22301 及び先述の IT-BCP のガイドラインを元に行うことが望ましい。[15]

その中で、IT-BCP のシステム監査の一つの要素として、大規模個人情報漏えいの BCP を確認する。システム監査の際は、４章で述べた特性を考慮しているか確認する事が重要となる。

7-3「IT サービス継続ガイドライン」を参考としたシステム監査のポイント

(1) 計画（文書）の策定

大規模個人情報漏えい事故の発生以降の事後対策に限定せず、事前対策である個人情報漏えい防止のための物理的対策、教育に加えて BCP 自体を改善していくための維持改善計画が明確に文書化されている事を確認する。また、個人情報漏えいに対する想定外の脆弱性、脅威の発生に対する BCP の改善計画についても確認する。

(2) 情報資産に着目した BIA

組織が保有する個人情報に着目した BIA の実施を確認する。BIA の結果の確認だけではなく、BIA を行う上で収集したドキュメントについても確認を行う。また、顕在化した個人情報漏えいリスクと BIA の間の整合について確認する。個人情報の属性と利用範囲により個人情報の保有リスクは異なるため業務毎にリスクと影響分析の結果について詳細に確認する。

(3) 組織・体制

大規模個人情報漏えいの事前・事後対策を遂行する組織・体制について確認する。IT サービス継続計画の主体は情報システム部門と事業部門システム担当となる事が想定される一方、大規模個人情報漏えいの場合、影響が広範囲に渡り、経営、業務、事業部門、場合によっては社外の対応が不可欠となる。すなわち大規模個人情報漏えい事故 BCP では横断的な組織対応のための網羅性、機能分担を確認する必要がある。

機能分担については最適化も考慮することになる。個人情報漏えいのリスクに対する全ての対策を BCP に取り込むと規模が大きくなり実現性に欠けるため、セキュリティパッチの適用の基準等 IT サービス継続に特化したものは IT サービス継続計画の中で取り組むなど最適化され、実際に運用できる計画となっている事も確認する。

(4) 検知

大規模個人情報漏えい事故の発生の検知について確認する。情報漏えいの検知方法が IT サービス経由の情報に偏重していないか、IT サービス以外から報告される事象の対応部門の確認、社内・組織内のみでの検知の可能性、想定される事象への対応方法、複数の事象の整合について確認する。

(5) コミュニケーション

個人情報漏えい事故の事後対応計画の確認の中でコミュニケーション遂行方法を確認する。大規模情報漏えい事故が発生した場合、ステークホルダーが多岐に渡り、コミュニケーションを取る際に相応の労力を要する。すなわち、自組織内以外

の外部組織、顧客とのコミュニケーション計画が確立されている事を確認する。コミュニケーション計画ではコミュニケーションの緊急度、コミュニケーションメディア（口頭、電話、書面、メール、公式発表など）、コミュニケーション障壁が網羅されている事を確認する。また、コミュニケーションに要するコストが見積もられている事も重要である。

8．おわりに

本稿は情報セキュリティ大学院大学がシステム監査学会第第 26 回研究大会、第 25 回公開シンポジウム、第 27 回研究大会、第 26 回公開シンポジウムの 4 回に渡って発表した大規模個人情報漏えい事故に対する BCP に対する考察を再編成したものである。今回、2013 年に IISEC で実施した情報セキュリティアンケートの結果を踏まえても、大規模個人情報漏えい事故は重大な業務阻害要因であるとの認識が広まっている事を確認できた。今後、大規模個人情報漏えい事故に対する BCP を策定しようとする組織、BCP の有効性を測定する段階に入った組織において参考となれば幸いである。

謝辞

本研究を進めるにあたり、研究の方向性、内容について積極的な議論をいただいた情報セキュリティ大学院大学の教授、原田研究室の先輩・後輩、個人情報漏えい事故のデータを長期継続して収集分析している NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループのメンバ、及びシステム監査学会のシンポジウム、研究発表大会にて聴講、アドバイス頂いた皆様に感謝します。

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（2012）

[2] 菅原尚志、新原功一、小倉久宣、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）

[3] 原田要之助 大規模な情報漏えい事故の特性と対策の考え方 情報セキュリティ大学院大学情報セキュリティ総合科学第 4 号（2012）

[4]NPO 日本ネットワークセキュリティ協会 2012 年 情報セキュリティインシデントに関する調査報告書【上半期 速報版】（調査研究部会 セキュリティ被害調査 WG）（2012）

[5] サービス継続検討ワーキンググループ,"IT サービス継続ガイドライン改定版 ", 経済産業省 , (2011)

[6]ENISA、Recommendations on technicalimplementation guidelines of Article 4、2010（2010）

[7] 情報セキュリティ大学院大学原田研究室 2013 年 情報セキュリティ アンケート調査結果 http://lab.iisec.ac.jp/~harada_lab/survey/2013/2013_questionnaire_result.pdf

[8]ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security management

[9] 独立行政法人情報処理推進機構、"2005 年企業における情報セキュリティ事象被害額調査 "（2006）

[10] 特定非営利活動法人日本ネットワークセキュリティ協会、情報漏えいの分析 https://www.ipa.go.jp/files/000013364.pdf

[11] 櫻井直子 ," 情報セキュリティの価値と評価―消費者が考える個人情報の値段 ", 文眞堂 , (2012)

[12]（社）電子情報技術産業協会、情報通信ネットワーク産業協会 ," 電機・電子・情報通信産業ＢＣＰ策定・ＢＣＭ導入のポイント～取り組み事例と課題～ ",（社）電子情報技術産業協会情報通信ネットワーク産業協会 ,（2008）

[13]ISO22301 事業継続のマネジメントシステム（2012）

[14] 情報セキュリティ大学院大学、情報セキュリティ事故対応ガイドブック（2011）

[15] 経済産業省、IT サービス継続ガイドライン（2008）