[Ⓡ 研究論文]

大規模な個人情報漏えい事故に対する事業継続計画の監査に関する一考察

A Study on Audit of Business Continuity Plan for Large-scale Personal Information Leakage

鈴木　宏幸　Hiroyuki Suzuki
原田　要之助　Yonosuke Harada
情報セキュリティ大学院大学
Institute of Information Security

概　要

筆者らは学会誌「システム監査」第 29 巻第 1 号 [1] において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事業継続計画 (Business Continuity Plan：以降「BCP」と言う) 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。本論文ではシステム監査の手法を用いて大規模な個人情報漏えいに対するの有効性の評価を行なう事について考察する。

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

JNSA（Japan Network Security Association：NPO 日本ネットワークセキュリティ協会）より「情報セキュリティインシデントに関する調査報告書」[2] が発行されている。2015 年の調査報告では、インシデント発生件数は 2013 年の 1388 件から 799 件と減少している。しかし、想定損害賠償総額については前回調査の 1438 億 7184 万円から 2541 億 3663 万円へと大幅に増加している。すなわち、インシデント 1 件当たりの及ぼす影響度は増加しており、個人情報漏えい事故の発生が事業継続の阻害要因となってきている。本稿では大規模個人情報漏えい事故の特徴と事故発生時の BCP の必要性、及び BCP の有効性評価について文献 [1] をもとに、システム監査の役割について考察する。

2．個人情報漏えい事故の特性

個人情報漏えい事故に対する対策は日々進化しており、2015 年の調査報告では発生件数は減少しているが事故は継続して発生し続けている。筆者らはこれをべき乗則に当てはめて考察している。

個人情報漏えい事故の発生件数と個人情報の漏えい件数は、発生頻度の低い要素の合計が全体に対して無視できない割合を占め、べき乗則のロングテールの法則に当たる。

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。べき乗則の特徴は以下の通り。

（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テール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 [1] が知られている。地震の発生回数 [2] 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

投稿受理日	2017 年 3 月 29 日
再投稿受理日	2017 年 8 月 17 日
再々投稿受理日	2017 年 10 月 30 日
査読完了日	2017 年 11 月 15 日

でいえば僅かな回数である。

（3）情報漏えい事故の分布

個人情報漏えい事件の件数と規模についてJNSAの2011年の調査結果[2]を対数軸で表現した結果、べき乗則となる事が判明した。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件の全体を対象に分析した結果を図1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フリーの特性が確認できる。

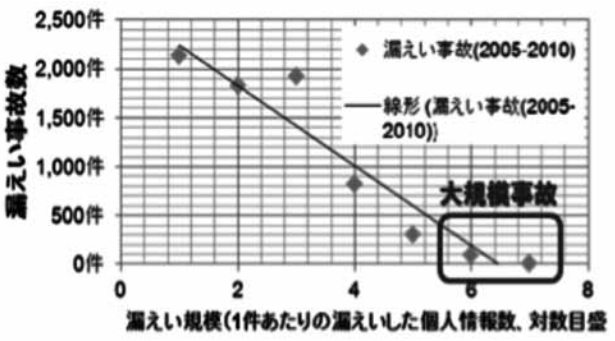

図1　2005～2010年の調査結果を対数軸で分析

2-2　情報漏えい事故での個人情報の流出経路

個人情報が紙媒体、電子媒体、ネットワーク経由等どの経路から流出したかを調査し、個人情報の漏えい経路別に事故一件当りの漏えい人数について箱髭図[3]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2は個人情報漏えい事故一件当たりの漏えい経路の箱髭図である。本図は筆者らが作成しJNSA発行の「情報セキュリティインシデントに関する調査報告書」に掲載している。

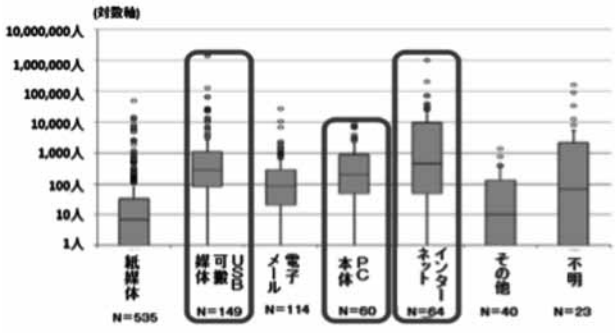

図2　個人情報漏えい経路別の漏えい人数

「USB可搬媒体」「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サービスを経路として多く発生していることがわかる。

一方紙媒体による個人情報漏えい事故は件数こそ多くなっているが1件の事故毎の漏えい件数は少ない傾向にある。

3．大規模な個人情報漏えい事故の影響と分析

筆者ら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」と定義した。

3-1　事業に与える影響

大規模個人情報漏えい事故は、漏えい件数のみならず情報の重要度が事業に与える影響に大きく係わってくる。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。筆者らは、これをJNSAが提唱するEP図を用いた分析及びENISA（European Network and Information Security Agency：欧州ネットワーク情報セキュリティ庁）の情報漏えい事故の評価指標をもとに評価する手法について以下に検討した。

個人情報の価値を分類する方法としてJNSAは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EP図を公表している[3]。図3にEP図を例示する。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EP図による各個人情報のレベルは以下のようになる。

図3　個人情報の価値を分類したEP図

・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

個人情報の属性の重み付けには統一基準が設けられていないため、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より、社内・組織内での基準を定めておく。

ENISA は事業に与える影響の観点から情報漏えい事故の評価指標を公開している [4]。

この評価指標を表 1 に示す。しかし、筆者らの検討では表 1 のはこのまま自組織で利用するのは難しく、適用するためには評点を定めるプロセスが必要となる。漏えいした情報の種類、件数と影響度を勘案し、大規模個人情報漏えい事故の独自基準を策定する事が重要である。

すなわち、企業は一般的に、経営に影響するような事故が発生した場合には、その対応について一般的には BCP を用いる。しかし、多くの企業では、BCP を自然災害やパンデミックなどの物理的な事故への対応に止めていることが多く、大規模な個人情報漏えい事故を BCP の対象にしていない。そのため筆者らは BCP の対象に個人情報漏えい事故を加えた。企業内で、大規模個人情報漏えい事故を BCP の対象としての基準を取り決めて、BCP と同じ基準で個人情報漏えい事故の影響を算定し比較することを提案する。

表 1　ENISA の個人情報漏えい事故のレベル指標
（筆者らにて邦訳）

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）

3-2　新たな視点での BCP に対する分析

個人情報漏えいの際にも、事故・事件の影響分析の手法としては、BIA（Business Impact Analysis: ビジネス影響分析) の実施が有効である。本論文の BIA の定義は経済産業省事業継続計画策定ガイドライン [5] に基づいている。

大規模自然災害を対象とする BIA では主に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主に、保有する情報に着目する点ことが重要であり、特性が違うことを指摘した。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ず事後対応による事業の中断、対応リソース要求、お詫び金の発生、再発防止処置等においてリソース不足が発生して事業に影響を与える。

また、大規模個人情報漏えい事故では、事故の影響がすぐには特定できず、のちに被害の規模が拡大することもあることや二次的な被害もあり、自然災害の場合のように直線的に復旧は進まない。被害を正確に把握するためには、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要素となる。

以上の検討の結果として、自然災害を対象とした既存の BCP に加えて、人間系のミス、不正行為によって発生する事故についても BCP に追加することが必要となる。

4．大規模な個人情報漏えい事故に対する BCP

筆者らは学会誌「システム監査」第 29 巻第 1 号 [1] において大規模個人情報漏えいに対する BCP の策定から運用のプロセスについて考察した。本章では前述の論文の内容 [1] を引用し、大規模な個人情報漏えい事故に対する BCP について紹介する。

4-1　BCP の対象範囲

大規模個人情報漏えい事故が発生した場合、事後対策が組織の保有する IT サービス [4] の中断や停止を伴うと事業継続に与える影響が特に高くなる。一方、PC、外部記録媒体の紛失・盗難が発生した場合、IT サービスを構成しているネットワーク、サーバ等のプラットフォーム、業務システム等への物理的な影響は小さい。例えば、e コマース（電子化された商取引）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じることが多い。この場合、

IT サービスを構成しているネットワーク、業務システムが稼動しているサーバーなどのプラットフォーム、データベースなどは物理的な被害を受けておらず、e コマースを簡単に再開できる。しかし原因が不明なままサービスを再開すると、再び攻撃を受けてより深刻な事態となるため、事業を停止することが多い。中断期間には e コマースの売上が途絶えるため事業に与える影響も大きい。このことから、大規模な個人情報漏えいの場合には、IT サービスを構成する組織、業務システム、プラットフォーム、ネットワーク BCP の対象範囲とすることが必要である。本論文では、この対象範囲における影響を自然災害の場合の事故とのアナロジーから、IT サービス操業度という考え方を用いて考察を行なう。

4-2 IT サービス操業度について

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。

IT サービス操業度とは IT サービス停止から IT サービス再開までのサービス停止の影響を図る値と考える。IT サービスが正常稼動している状態を 100 とし、IT サービスが停止した場合、操業の落込み度 × 時間を減産して算出する。

IT サービスを全面的に停止し対策を行う場合の IT サービス操業度は図 4 のように表せる。

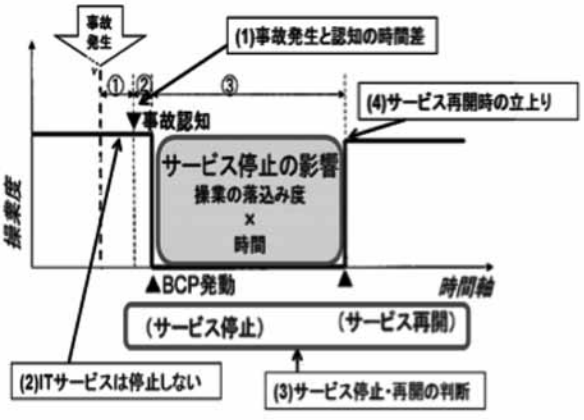

図 4 大規模個人情報漏えい事故発生時の IT サービス操業度 [1]

IT サービス操業度の特徴について以下に示す。

（1）事故の発生から事故の認知までの時間差

BCP の場合は、情報漏えい事故の発生から認知までの時間差が問題となっている。情報漏えい事故の場合は、この点が顕著である。例えば、情報漏えい事故については大小にかかわらず情報システムからはもたらされる事が少ない。多くの事故事例では、漏えいした個人からの通報や問い合わせ、ホームページなどの書き込みなどで事故が判明している。

BCP での時間差は、事故直後では無く、ある一定の時刻経過後に起きることから、事前に予想できて被害をコントロールすることができる。しかし、個人情報の漏えいの場合には、時間差をコントロールすることはできない。

（2）大規模個人情報漏えい事故が発生しても 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があっても、IT サービスは自ら停止しないし、自動で停止することができない。組織の判断で、被害の拡大防止、ソフトウエア製品のセキュリティ上の問題点対応、情報漏えい事故の原因追求等のため、停止させることになる。

（3）IT サービスの停止および再開は経営判断に委ねられる

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変わる。自然災害 BCP の場合と同様に、IT サービスの停止は業務を中断させ、復旧コストを発生させ経営に直結する。IT サービス停止及び再開判断のは、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。

（4）IT サービスの再開に係る操業度

図 4 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は直角に立ち上がる。これは、通常の BCP の場合には、RTO(Recovery Time Objective: 現時点での実際の事故発生時に目標とする実現可能な復旧時間) と RLO(Recovery Level Objective: 業務が中断することにより落ち込んでしまった水準を復旧させる程度) をベースに IT サービスの再開を経営判断して決めるが、個人情報漏えいの場合の復旧には、時間差がない。IT サービスの物理的なリソース（電力、サーバー等のプラットフォーム、ネットワーク等）は被害を受けていないので直線的な立ち上がりとなる。マルウェア感染による個人情報漏えい事故の場合には、セキュリティパッチの

適用、アプリケーションの修正など全ての対策が行なわれた時点で復旧完了となる。

4-3 IT サービス利用度の考察

消費者や住民を対象とした IT サービスでは、企業の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。消費者は信用や安全性の懸念等から利用を控えるからである。有償の IT サービス提供であれば事業が復旧しても収入源が激減して、結果として事業が継続できない事態となることも想定される。そこで筆者らは、IT サービスの操業度とは別の指標として IT サービス利用度という考え方を用いて考察を行なう。

IT サービス利用度とは、IT サービスが稼動している時間当たりの利用件数と考えられる。
時間当たりの利用件数が高い程 IT サービスの利用度は高いと言える。

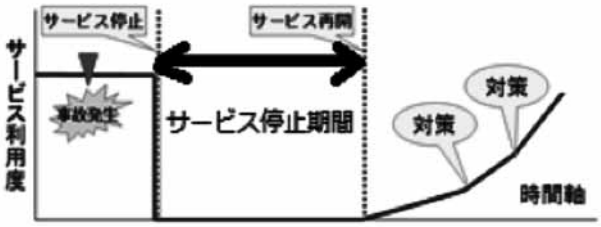

図５ IT サービス利用度 [1]

図５では、情報漏えい事故発生後に IT サービス全面停止を想定した場合のサービス利用度を表すために筆者らが作成した。IT サービス停止期間が過ぎてもサービス利用度は自動的には元の段階まで上がらない。この観点からは、個人情報漏えい事故に対する BCP には、IT サービス利用度を考慮した複数の対策が必要である。

4-4 BCP の対象組織

大規模個人情報漏えい事故の多くは、その原因が IT サービスによるため、BCP の対象組織には IT サービスを導入、運用している運用部門がまず考えられる。そして IT サービスの利用部門の参画が必須である。また、大規模個人情報漏えい事故の場合には利用者に対する説明責任や組織としての対策など経営判断が求められるため、経営層の関与が必要となる。そして情報発信を行なう広報部門、さらに事故対応時の訴訟リスクに備えて法務部門の関与も必要となる。大規模個人情報漏えい事故にはこれらの組織が連携して BCP を発動し、タイムリーな対応策を遂行できるように、個々の役割分担を BCP に明記することが必要となる。

4-5 BCP の策定

大規模個人情報漏えいの BCP を策定する場合には予防と復旧の２つの特性を取り込むことが必要である。大規模個人情報漏えい事故の発生を可能な限り抑止する予防の段階、それでもべき乗則によって発生する事故の復旧の段階の両方を BCP に組み込み有効性を高める事が必要である

5. BCP の有効性について

大規模な個人情報漏えいに対応した BCP を実効性のあるものにするために、被害の予防のプロセス、被害の復旧のプロセスにおいて有効性を測定する事が重要である。以下に有効性を測定する上で必要な事項について検討する。

5-1 被害の予防のプロセス

このプロセスでは、リスクに対する対応策を立案し実施する。大規模な個人情報漏えい事故が組織に与える影響度を分析、現状とのギャップ分析を実施し、予防策を立案する。

① BIA からの有効性測定

プロセスの有効性の測定には、大規模個人情報漏えい事故が組織に与える影響度を測った BIA の結果が活用できる。BIA からの有効性について以下の点を測定する。

（1）BIA の実施時期

個人情報漏えいはいつおきるか分からないため、不定期に実施すべき BIA とそのトリガーの例を以下に示す。

・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
・個人情報漏えいの通報

リスクが変化したタイミングで BIA が確実に実施されている事が BIA 実施時期の有効性評価指標となる。変化したリスクに対応して BIA を実施していれば BIA の実施時期は適切であると言える。

（2）情報資産に着目した BIA

BIA を実施する際に、業務毎の情報資産とその価値、個人情報が漏えいした場合の経営に与える重大性（例えば、想定される被害額など）が分析されている事を確認する。これらの観点から分析されている事が BIA の有効性評価の指標となる。情報資産各々の資産価値と情報漏えい時の影響度が分析され、リスクが明確になっていれば情報資産に着目した BIA は有効と言える。

（3）IT サービス操業度と IT サービス利用度から見た RTG、RLO の設定

BIA にて IT サービス操業度と IT サービス利用度の双方について適切な RTG(Recovery Time Goal: 現状では達成が難しくとも改善活動で目指すべき最大許容停止時間) と RLO が設定されている事が評価指標となる。

大規模個人情報漏えい事故に対しての IT サービスの停止判断は経営面の判断にてに意図的に行なわれ、また復旧についても同様である。すなわち、IT サービス操業度の RLO は IT サービス停止前と同等となる。

一方､IT サービスを復旧させただけでは IT サービス利用度は大規模個人情報漏えい事故発生前には戻らない。経営面からの対策を実施して組織やブランドの安全性を上げて初めて利用度は上がって来る。従って、経営面から実施する施策時点における RTG、RLO が、施策と整合性をもち妥当なレベルに設定されていれば有効と言える。

（4）前回 BIA との比較

複数回実施した BIA の結果の比較検討は有効性を評価する大きな指標となる。比較対象は BIA 中の RTO、RTG の数値の変化だけではなく、リスクパターンが業務と対応して洗い出されているか、対象業務が細分化されているかなど BIA 対象業務の詳細化の度合いも重要な有効性評価の指標となる。これらが前回の BIA と比較して詳細化され、精度が上がっていれば BIA は有効と言える。

BIA は実施して終わりではない。環境の変化に合わせ都度、BIA が最新の状態に更新されている事が重要である。

②脆弱性課題とリスク対策からの有効性測定

BCP では BIA で洗い出した対象業務のリスクパターンについて脆弱性課題を抽出し、リスク対応計画を立案し実施する。この部分は被害の予防プロセスの中心となる。

脆弱性とはソフトウエア製品やアプリケーション等におけるセキュリティ上の問題箇所でありコンピュータ不正アクセスやコンピュータウイルス等により、この問題の箇所が攻撃されることで、ソフトウエア製品やアプリケーションの本来の機能や性能を損なう原因となり得るものを示す。

（1）脆弱性課題の抽出

脆弱性についてはメーカー・ベンダー、JPCERT/CC(Japan Computer Emergency Response Team Coordination Center:

一般社団法人 JPCERT コーディネーションセンター) などが常時、脆弱性情報を更新している。これらの情報を入手し、OS、アプリケーションをアップデートする必要があるが、これらは情報セキュリティ対策のルーチンとして常時行なうべき事項であり BCP とは異なる。ただし、課題を BCP に（バックアップなどを含めて）反映させることが必要である。

BCP で対策すべきの脆弱性課題の例を以下に示す。

・OS のサポート停止
・機器の旧式化
・複数コンピュータシステム間の不整合
・アプリケーションの方式の陳腐化により安全性が確保できない

近年、内部犯行による大規模情報漏えい事故が発生し、内部犯行の防止が大きな課題となっている。そこで、独立行政法人情報処理推進機構では「組織における内部不正防止ガイドライン」[8] を発行、改版しているので内容を組織の状況に合わせてチェックし、対応できていない部分を抽出し、脆弱性課題と合わせて管理、対策する事が必要である。

日常的に脆弱性課題を抽出して、情報を活用して BCP に反映していることが有効性評価の指標となる。

（2）リスク対応計画

脆弱性課題については、どの脆弱性課題を、いつまでに、どの程度の費用を掛けて対策を行なうかを計画し実施する。リスク対応計画においては実現可能性が大きな要素となる。個々の脆弱性課題を細分化し実際に対策できるレベルの施策まで落とし込む事が重要である。また、リスク対応計画では対応期限を定めることは必須であるが、計画の進捗確認、進捗ポイントを予め設定しておく事が計画の実現に向けた大きな要素である。このうち、必要な項目については BCP に反映させる

必要がある。BCP に反映させている頻度が有効性の指標となる。

（3）リスク対応計画の結果の振り返り

リスク対応計画では定期的に対策の進捗状況、対応結果の振り返りを実施し、その成果、課題の確認を行なう。残課題がある場合は原因を明確にして次回策定のリスク対応計画に引継ぎ、未対応項目を残さない事が重要である。課題の確認が有効性評価の指標となる。

③組織・体制面の有効性測定

組織・体制面での有効性指標を以下にブレークダウンする。大規模個人情報漏えい事故に対する BCP では、利用部門や IT 関連部門のみでは対応できず関連部門を取り込んだ事業継続体制を構築することが重要となる。有効性測定では体制が大規模個人情報漏えい事故に対して発生時にタイムリーに対応できること、事後対策が実施できることなど組織的な観点から有効性を評価することになる。これには、個人情報漏えい保険などの対策も含まれる。

（1）関連部門のアサインメント

大規模個人情報漏えい事故発生時には各関連部門が連携し対応を行なう事となる。

BCP に必要な部門と役割を以下に列挙する。なお、部門の名称は組織毎に異なるので役割から読み替える事が必要である。

・IT サービス導入・運用部門

情報システム部など IT サービスの導入、運用を担当する。大規模情報漏えい事故発生時は IT サービスの停止、再開のオペレーション、情報漏えい経路の特定、原因の究明、IT サービスを構築しているネットワーク、アプリケーション、プラットフォームの脆弱性対応などを担当する。

・IT サービス利用部門

IT サービスを利用して業務を行なっている部門では事故発生時 IT サービス停止状況での代替業務の計画、漏えいした情報の重要度、業務への影響判定等を実施する。

・経営陣

大規模個人情報漏えい事故発生時には、IT サービス停止による業務中断、ひいては業務中断による収益現象、事故対応体制、費用の準備、費用また個人情報が漏えいした被害者に対するお詫び金の発生、脆弱性対応のための新たな設備投資、会見での説明等経営層の関与なしには対応できない。

・広報部門

広報等組織外へ情報発信を行なう部門においては会見の実施、事故の対外発表、組織外との窓口対応等を実施する。

・法務部門

大規模個人情報漏えい事故発生時の訴訟リスク対応など各種法務関連業務を担当する。

・CSIRT

近年 CSIRT(Computer Security Incident Response Team) を構築する組織が増加している。上記部門と連携して実効性の高いチームを構築していくことが望まれる。

・その他

大規模な個人情報漏えいは、株価にも影響を与える可能性があり、企業内部の経営陣の発表や対応などインサイダー情報となるものもあるので、企業の情報管理体制も重要となる。

これらの体制が事故に対して機能するのかが有効性評価の指標となる。BCP のレビュー、対策訓練等を通じ各部門から過不足の無い事が確認できれば有効であると言える。

（2）コミュニケーション体制の確立

事故に対して企業内部のコミュニケーション体制が有効性の指標となる。

事業継続に必要な関連部門に対して、内部の連絡体制が確立できていること、事故発生時に確実に連絡できること、必要な情報を共有できることが重要である。以下に要点を列挙する。

・各部門のキーマンの取り込み

各部門の連絡先担当者は、単なる窓口では有効に機能しない。実際に動けるキーマンを取り込んだ連絡体制を確立する。

・副担当のアサイン

主担当に連絡できない場合もあり、迅速に連絡、対応するために必ず副担当をアサインする。

・複数の連絡方法の組み込み

事故発生時の連絡方法は部門の固定電話のみではなく、携帯電話、ｅメール、グループウェア等複数の連絡手段を組み込む。

BCP のレビュー、対策訓練等を通じコミュニケーション体制の関連メンバより過不足の無い事が確認できれば有効であると言える。

④周知徹底

大規模個人情報漏えい事故は、地震等の自然災害と異なり組織内の誰もが一斉に検知できるものではない。従って大規模個人情報漏えいの特性、対応方針が組織内に周知徹底できていないと事故発生後の対応が取れない事態となる。組織により定めた大規模情報漏えい事故の定義と対応方針、方法を確実に周知徹底する事が有効性の指標となる。事前の通知がなされており BCP 関連の全員に周知徹底されていれば有効であると言える。

（1）基本方針の徹底

基本方針は組織の経営者が宣言する。個人情報保護方針に経営者が署名し公開する。組織にとって何が大規模個人情報漏えい事故に当たるかを明確にし、事故を起こさないために何が必要かを規定し、その上で対象範囲、責任者を明確にする。また、必要に応じ業界標準、該当する法令、各種基準を追記する。事前にどの程度の方針が策定されているかが有効性評価の指標となる。基本方針のレビューにおいて基本方針が承認され周知徹底が行なわれている事が確認できれば有効であると言える。

（2）教育の実施

基本方針の徹底のみではなく、事故の予防プロセス、事故発生時の復旧プロセスについて組織内各部門の一般構成員、事業継続計画遂行メンバに対して役割毎に見合った教育を実施する。基本的には全員向けの基礎教育と事業継続計画遂行メンバに対する専門教育を分けて実施する。教育は予め計画した定期開催の教育と新たな脅威、対策に対応する臨時開催のものがある。教育の頻度やその内容が有効性評価の指標となる。BCP 推進メンバが教育の頻度や内容について適正と判断できれば教育は有効であると言える。

（3）ドキュメントの整備

BCP を遂行する上で必要なドキュメントを整備する。ドキュメントは BCP 策定時に新たに作成するものと各種既存ドキュメントを BCP に取り込んで活用するものがある。

ドキュメントについてはポリシー、スタンダード、プロシージャの３階層に分けて構成する【図6】。

・ポリシーでは上記の基本方針を中心として、なぜ個人情報を守るかという Why の部分についてのドキュメントを取りまとめる。
・スタンダードでは基本方針を受けて何を行なうか What の部分を取りまとめる。個人情報を保護するための対策基準がこれに当たり、各種ガイドラインを適用する。適用範囲や対象者を明確にして取りまとめる。
・プロシージャでは実際に対策を行なう際にどうやって行なうか How の部分のドキュメントを取りまとめる。各種のマニュアルがこれに当たり詳細な手順を記載する。

図６　ドキュメント構成の３階層

作成したドキュメントは文書番号を採番してインデックスを作成し、管理する。ドキュメントが改版された場合はインデックスをただちに修正して最新版が識別できるようにするとともに関係者に通知する。

ドキュメントの格納場所についても考慮し、必要とするメンバが必要な時に取り出せる所に格納する。

近年ペーパーレス化で電子化した文書をグループウェアで管理する事が増えているが、個人情報漏えい事故発生時に文書管理サーバーが利用できなくなる事態も考慮し、ローカル PC へのバックアップ、紙ドキュメントの利用も検討しておく。これらのドキュメントの有無と管理状況が有効性の評価指標となる。適切に管理できていればドキュメントの整備は有効に行なわれていると言える。

5-2　被害の復旧プロセス

被害の復旧プロセスにおいては、有効性を測定するために実際の事故を発生させる事は出来ないため、訓練を中心に以下の復旧プロセスの有効性を確認する。

BCP を実際の事故発生時に、確実に遂行するために訓練を定期的に実施している事を確認する。訓練内容、訓練対象を役割レベルに応じて取り決

め、適任者をアサインして実施する事がBCPの有効性を高める事となる。

（1）事象の発見

本論文では事象を大規模個人情報漏えい事故に至る可能性のある事態と定義する。具体的には不正アクセス、ウィルス感染、インターネットからの攻撃などITサービスに直接影響を与えるもの、またITサービス以外にも電話、メール、掲示板、各種SNSへの個人情報の書き込みなどがこれに当たる。

大規模個人情報漏えい事故の兆候は検知の仕組みがなければ検知することができない。検知の仕組みはITサービスを構成している各システムに組み込む事は必須であるが、事象はITサービスのみならず多方面から挙げられる事となる。

事象の発見の訓練では事象のケースを想定して事象毎の訓練を実施する。

事象ごとのケースの例

[特定のサーバーに対して過度のアクセス集中]
情報システム部門にてアクセス元とアクセスデータの特定

[匿名での電話]
業務部門にて内容の聞き取りと関係部門への連絡、事実確認。

事象ごとの訓練において予定した訓練結果が出ていればBCPは有効と言える。

訓練の結果自組織のみでの事象の発見、事故発生の確認が難しいと判断した場合は外部組織の活用も視野に入れる。

（2）エスカレーション

事象を受け、大規模個人情報漏えいの可能性が考えられる場合、エスカレーション(escalation：段階的な上位への報告)を実施する。エスカレーションの訓練においては最終報告まで所要時間の測定が訓練指標として必須である。また、伝達される内容の正確さの確認、キーマン不在の際のエスカレーション方法などを組み込む。

（3）事故の公表

大規模個人情報漏えい事故が実際に発生した場合の事故の公表についても訓練実施を検討する。経営者による会見の訓練の実施は実際には難しいと思われるので会見のシナリオを関係者にてレビューし問題点を挙げていくことがが考えられる。

（4）リアルタイムBIA

情報漏えいの事故となる事象を検知し、それが大規模個人情報漏えい事故と判断した場合、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。

状況の変化に応じ対応変えていく必要があるが、この影響を分析する。事故発生前のBIA結果を基にしリアルタイムで新しい情報を加味したBIAを実施する。

このリアルタイムBIAの訓練を実施した場合、BCPの遂行に大きな効果が期待される。

リアルタイムBIAの訓練方法として、いくつかの事象やイベントを予め定義し、BCP遂行メンバが集まりBIAを実施して結果を確認するケーススタディの方法が考えられる。

近年、OODAループ[5]によるマネジメントがクローズアップされてきているが、刻々と状況が変わる事故対応においては定型的なPDCAサイクルに比べ、より実用的な対応が行なえると考えられる、リアルタイムBIAのOODAループの適合については今後考察して行きたい。

リアルタイムでどの程度の対応がとれるかは有効性評価の指標となる。

訓練シナリオを作成し、訓練実施した結果が予想した訓練内容となっていればリアルタイムBIAは有効であると言える。

（5）法対応

事故対応の際の訴訟リスクについて、判例などをふまえたシミュレーションを行い自組織において対応が出来るかを確認する。もし、シミュレーションにおいて自組織のみで対応が難しいと判断した場合は外部組織の活用も考慮に入れる必要がある。

6．BCPの監査の実施による有効性測定

①BCPの監査の位置付け

情報セキュリティ大学院大学原田研究室にて2016年12月に発表した2016年情報セキュリティアンケート調査結果[9]において、管理策の新規導入、見直しの理由として事業継続計画(BCP/BCM)と緊急時対応を挙げた組織が501組織中52組織と約一割存在する。

この組織が対象とする事業継続の阻害要因として情報漏えいを対象としているかまでは調査していないが事業継続を意識した組織が存在している。

ISMS(Information Security Management

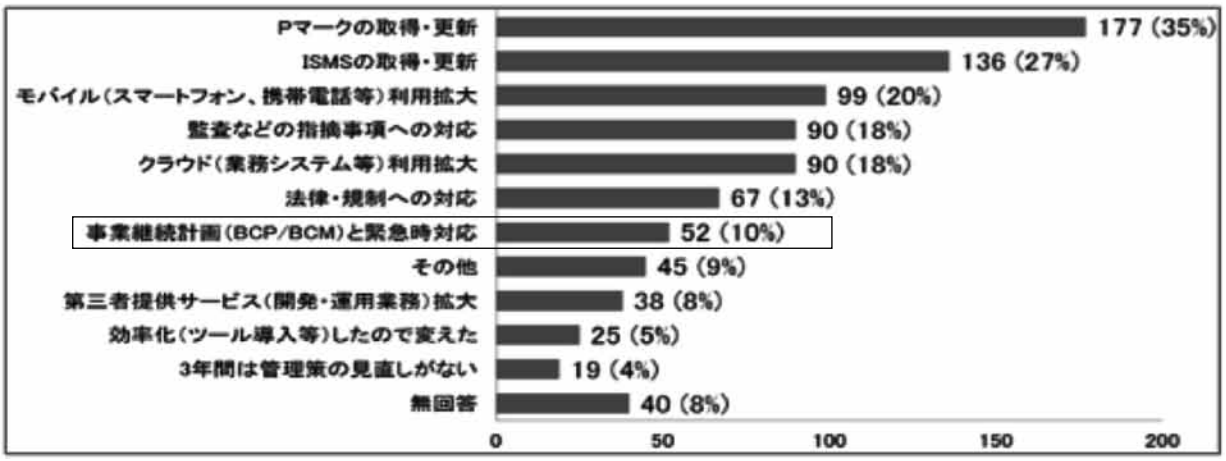

図７　管理策を新規導入、見直しした理由

System: 情報セキュリティマネジメントシステム)、P マークの認証取得においては規格、要求事項に従って監査手続きを実施した範囲において適切であることを保証する保証型監査が実施されている。また、BCP についても ISO22301 認証に伴う保証型監査が実施されている。大規模個人情報漏えい事故に対する BCP の有効性を計るために双方の規格、要求事項を満たしている事を確認する保証型監査を行なう事は、組織においては要求事項、監査項目が多岐に渡り負担が大きくなる。本論文では BCP の有効性を監査によって測る事を目的としているので保証型監査の実施までは必要としていない。

監査形態としては監査対象の組織体の事業継続に関するマネジメントやコントロールの改善を目的として、BCP の問題点を検出し必要に応じて監査での検出項目に対応した改善提案を行なう「助言型監査」を行なう事が実態に即している。

（1）情報セキュリティ監査と BCP の監査

情報セキュリティ監査については前述の 2016 年情報セキュリティアンケート調査結果において過去 1 年間に監査を行なった組織が調査対象の 80% という結果が出ており、監査は組織における情報セキュリティ対策実行上重要なツールとなっていると言える。

情報セキュリティ監査と同様に大規模個人情報漏えい事故に対する BCP の監査により BCP の完成度を高め、実効性のあるものとするための重要な施策となる。

①監査の基準

BCP の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に対する BCP が存在することが必要となる。

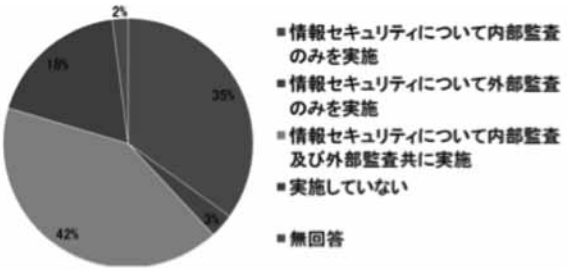

図８　情報セキュリティ監査の実施状況

IT-BCP のガイドラインは 2011 年に 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 [10] が 2011 年に改訂されている。これらは IT-BCP に特化したガイドラインであるため、ISO22301 などにより事業継続マネジメントに関する補完が必要である。BCP の監査は IT-BCP のガイドラインと ISO22301 の監査項目を対象の IT サービスに合わせ取捨選択して行なう事が望ましい。監査項目のイメージを下図に示す。

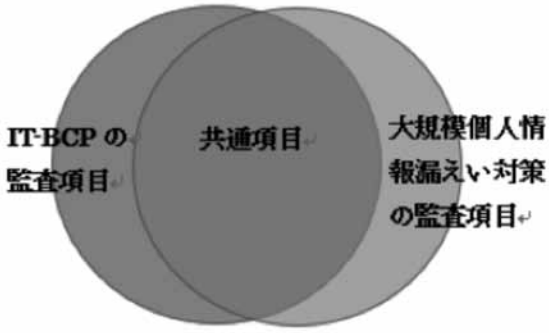

図９　監査項目のイメージ

BCP の監査項目の設定にあたっては５章で述べた有効性の評価ポイントを組み込む事により実態に即した監査となる。

②監査の実施

BCP の監査に当たっては、大規模個人情報漏えい事故が組織の事業継続上の大きなリスクとして認識されており、方針、施策がある程度組織内に浸透していることが前提となる。実際に監査を行なうことを想定し、必要な要素を例として列挙する。

（1）監査の形態

BCP の監査の形態は助言型監査とし組織における現状の確認、改善事項を抽出し改善に繋げる事を主目的とし、被監査人に趣旨を理解させ、ありのままの状態を監査する。監査項目が固まっていない事を見越して内部監査とし、BCP に関連する部門において内部監査として組織内で実施する。

（2）監査項目

BCP の監査の観点として、BCP の観点と IT ガバナンス、IT 戦略の視点が必要である。双方の要素を取り込み大規模個人情報漏えい事故対策に特化した監査チェックリストを作成し監査項目とする。

（3）監査人

監査人は大規模個人情報漏えい事故と BCP の知見を持った要員を BCP 要員外からアサインし、BCP の監査の中立性を担保する。適切な監査人が社内でアサインできない場合は、外部の監査人の活用を検討する。

（4）被監査人

被監査人は BCP に組み込まれた各部門の長、事業継続計画遂行メンバ、組織の一般構成員を対象とする。被監査人に対し監査人は施策の実施状況の確認を行おこなう。監査結果に不適合項目、改善項目がある場合は被監査人は監査指摘事項の改善を行なう。

（5）監査方法

BCP の監査方法としては監査チェックリストを各部門に記入させ内容を確認する書類監査、実際に現地に出向いてヒアリング、エビデンスの確認を行なう実地監査を組み合わせて実施する。可能であれば、実際に個人情報漏えいをシミュレートした訓練状況を評価することも必要であろう。

BCP の監査において明確となった検出項目（ポリシー違反や規定違反を含む）、未適用項目については、その原因について部門固有の問題か、BCP 全体の問題かを切り分ける必要がある。

（6）評価

個々の評価項目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の観点から対策の状況を総合的に評価する必要がある。評価項目ごとの有効性の度合いとともに BCP 活動が組織に与えた影響についても評価することが望ましい。

なお、BCP の監査が終了したあと、有効性の評価に用いた項目自体が適切であったかについて被監査部門にヒアリングして適切性などを見直し、次回以降の BCP の監査での監査項目として設定し監査を行なう。

（7）報告

BCP の監査結果はサマライズして経営陣に報告を行い、問題点の重大性や逼迫性に応じて対策や今後の方針及び、必要な対策を立てる際の重要な参考とする。

7．おわりに

筆者らは、大規模個人情報漏えい事故については BCP の枠組みに組み込んで影響分析、事前対策、事後対策の計画策定を実施することを提言した[1]。本論文では、大規模個人情報漏えいを想定した BCP を具体化するためには、対策の有効性を担保することが必要であること監査が役立つことを示した。さらに、有効性評価の項目について検討し、監査に当たっての基本的な要素について考察を行なった。

なお、文中でも述べているが、BCP の監査基準として評価ポイントを取りまとめた監査チェックリストの作成、標準化が急務と考えている。

参考文献

[1] 鈴木宏幸、新原幸一、原田要之助、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、学会誌システム監査第 29 巻 1 号 (2016)

[2] NPO 日本ネットワークセキュリティ協会、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)

[3] 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)

[4] ENISA、Recommendations on technicalimplementation guidelines of

Article 4、2010(2010)
[5] 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 "BCP 策定ガイドライン"(2005)
[6] 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)
[7]（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)
[8] 組織における内部不正防止ガイドライン、情報処理推進機構 (2107)
[9] 2016 年情報セキュリティアンケート調査結果、情報セキュリティ大学院大学原田研究室 (2016)
[10] 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)

注

1) グーテンベルグ・リヒター則
ドイツの地震学者ベノー・グーテンベルグとアメリカ合衆国の地震学者チャールズ・リヒターが見出した、地震の発生頻度と規模の関係を表す法則である。片対数グラフで表すと直線関係になる。
2) 地震の発生回数
マグニチュードが 1 大きくなるごとに地震の回数は約 10 分の 1 となる
3) 箱髭図
箱髭図はばらつきのあるデータをわかりやすく表現するための統計学的グラフである。重要な要約統計量である第一四分位数、中央値、第三四分位数で長方形を構成する。また長方形の上辺及び下辺から伸びる線の先端より小さい丸印は外れ値であり、正規分布でいう 3Σ に相当する。
4) IT サービス
顧客のニーズにあわせ IT 技術を組み合わせ適切なサービスを提供すること。
5) OODA ループ
OODA ループは、朝鮮戦争の航空戦についての洞察を基盤にして、指揮官のあるべき意思決定プロセスを分かりやすく理論化したものである。すなわち、監視（Observe）- 情勢判断（Orient）- 意思決定（Decide）- 行動（Act）のサイクルを繰り返すことによって、健全な意思決定を実現する。計画中心の PDCA サイクルに比べ、より臨機応変な状況対応が取れるとされている。

鈴木　宏幸　情報セキュリティ大学院大学
情報セキュリティ研究科