事業継続マネジメントにおけるインシデント・マネジメントの考え方 [1]

日本ヒューレット・パッカード株式会社
佐藤　慶浩

１．はじめに

事業継続に関してのインシデント・マネジメントの法的要件やコンプライアンスにおける位置づけについては、情報ネットワーク法学会として、研究を取りまとめるには至っていない。
ここでは、国際規格を引用しながら、インシデント・マネジメントとして必要なことについて紹介する。

２．インシデント・マネジメントの基本的な考え方

２．１　イベント（事象）とインシデント

国際規格に関連して、ISO/IEC 18044 情報セキュリティ・インシデント・マネジメントという技術文書がある。この文書単体は国内であまり知られていないが、情報セキュリティのマネジメントシステム認証の国際規格である ISO/IEC 27001 がインシデント・マネジメントの管理策として参照している文書である。この ISO/IEC 18044 は、これまでの技術文書から国際標準にするべく ISO/IEC 27035 として作成中である。現時点では、27035 は審議中で内容が公表されていないので、ここでの紹介は、18044 を引用する
BCP(Business continuity planning)についての定義は図１のとおりである。なお、これは今回の他の報告にあるような事業継続の全体枠組みにおける定義ではなく、情報セキュリティ対策の観点での BCP の定義ということになる。

[1] 本稿は、「情報セキュリティ総合的普及啓発シンポジウム（2009 年 1 月 28 日開催）」の講演内容を文章にしたものです。http://yosihiro.com/speech/index.html#2009-01-28

3.1 Business continuity planning

Business continuity planning is the process to ensure that recovery of operations will be assured should any unexpected or unwanted incident occur that is capable of negatively impacting the continuity of essential business functions and supporting elements. The process should also ensure that recovery is achieved in the required priorities and timescales, and subsequently all business functions and supporting elements will be recovered back to normal.

The key elements of this process need to ensure that the necessary plans and facilities are put in place, and tested, and that they encompass information, business processes, information systems and services, voice and data communications, people and physical facilities.

出典：ISO/IEC TR 18044 Information Security Incident Management

図 1

この後に説明する情報セキュリティ・インシデント・マネジメントの考え方では、情報セキュリティ・イベント（information security event）と情報セキュリティ・インシデント（information security incident）という２つの重要な用語がある。それぞれの定義を図２に示す。（18044 は現時点で JIS 化や邦訳の予定はないので、定義文について英文のまま引用するが、これらの定義は、27001 で参照されているため、邦訳については、JIS Q 27001 を参照するとよい。）

3.2 Information security event

An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

3.3 Information security incident

An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

出典：ISO/IEC TR 18044 Information Security Incident Management

図 2

情報セキュリティ・イベントは定義にあるとおり、情報セキュリティの侵害の可能性又はセキュリティに関連する未知の状況が見出されることである。

２つの用語は information security という接頭辞があるが、18044 で述べているものは必ずしも情報セキュリティに特化しているものではないので、それぞれ接頭辞をあまり意識せずに、イベントとインシデントとして読むことができる。

イベントの邦訳は事象と考えることができる。インシデントの邦訳は、事故と考えることもできるが、インシデントの方が日本語の事故よりも若干広義と考えられるため、ここではインシデントのまま説明する。

インシデントの定義内容の特徴を紹介する。

定義では、インシデントを unwanted or unexpected な事象群と表している。unwanted は望んでいないという意味なので組織が望んでいない事象ということである。それによって組織に被害をもたらせば、それをインシデントとして対応するのは当然のことであり、特に説明を補足するまでのことはない。一方、unexpected は予期していなかったという意味だが、予期せずに悪いことが起きれば、それは unwanted とほぼ同義である。ここで、unexpected をあえて追加しているのは、結果的に被害を及ぼさない事象であっても、その結果が予想に反しているならば、それをインシデントとして取り扱うということである。

たとえば、原因となる何かがあって、それに対する対策を何も講じていなかったため、本来は被害が出ても当然なのに、なぜか、被害には至らなかったという場合である。その場合には、それはインシデントではないと考えるのか、たまたま運がよくて被害にはならなかったが、インシデントの兆候と捕らえて、それについて対応するのかという違いがある。18044 では、インシデント・マネジメントとして後者の対応を推奨する意味で、unexpected をあえて追加しているのである。

仮に前者のように、結果的に被害がなければインシデントとしないということでは、同じ原因が発生したときに、次は被害になるかもしれない。被害に至らない事象に対しても対応をしておけば、同じ原因が将来発生した場合に、被害を未然に防ぎやすくなるはずであるということだ。それによって、予期していなかった事象については、被害の有無を問わず、インシデントとして対応して再発防止策についても必要に応じて検討するのがよいということを意図している。

以上のように用語を定義した上で、以下のことを 18044 では示唆している。
組織では、インシデントへの対応手順や体制を整備しなければならない。しかし、インシデントを迅速に対応できる体制が確立しても、日常的に発生している多くの事象を、現場の当事者がインシデントとして認識するのが遅れると、結果的に対応が遅れてしまう。
消防署が１１９番で連絡を受けてからの対応が迅速にできるような準備をいくらしても、１１９番への通報が遅れれば、結果的に火災発生から消防車の現場到着までの時間を短縮できないようなものだ。
事業継続マネジメントにおけるＩＴに関するインシデントの種類を区分する観点はいくつかある。たとえば、災害と機器障害を分けるなどが考えられる。しかし、事象をインシデントと認識する主体的な者の違いという観点も考えられる。すなわち、事象がインシデントであることを現場でなければ気づけないことか、現場以外も気づけるかという違いである。現場以外でも気づける例としては、地震のような災害がある。地震については、現場からの報告を受けずとも、地震の発生に気づくことができ、それはすぐさまインシデントとして対応することができる。一方で、ある社員のパソコンが不自然な動作をしているとき、それが単なるソフトウェアの不具合なのか、ウイルス感染による被害なのかというような事象は、その社員からの報告でしか、インシデントとして対応することができない。このとき、ウイルス感染であったのに、単純な不具合だと見逃して、インシデント対応チームへの連絡が遅れれば、その間にウイルスが社内に感染し、さらには社外にも感染させてしまってから、チームが知るところとなったならば、入念なインシデント対応手順が後手になってしまう。このことは、先例の地震に気づいて対応をすることとは、出発点で異なっている。

そのようにならないためには、インシデントと認識された以後のことばかりではなく、それ以前の事象にも広く注意をする必要がある。つまり、インシデントの管理をする際に、インシデントから始まる一連の措置だけを範囲とするのでは不十分な管理策ということだ。
これは重要なことであるが解決策は簡単ではない。なぜなら、現場からあらゆる事象をインシデント対応チームに報告されても困るかもしれないからだ。すべてのことをチームで仕分けるので些細なことでも遠慮なく報告せよとするのか、何らかの基準を示して仕分けてから報告させるかのトレードオフは意外と大変なことである。
先の１１９番通報の喩えで言うならば、煙を見たらすぐ通報するのか、それが火災かを煙の元まで行って確認してから通報するのかの違いということになる。

18044 では、これについてはガイドするには至っていない。27035 では、categorization として類型化についてのガイドを加えることを試みる予定だが、審議は始まったばかりで、まだ具体的な解説には至っていないので、今後の動向をご確認いただきたい。

いずれにせよ、インシデントとなる可能性や未知の状況を示している事象が、事業運営を危うくする確率（18044 では情報セキュリティを脅かす確率）が高くなることでインシデントに変遷するという考え方をすることが重要である。このとき、事象そのものが変化するわけではなく、組織としてのその事象の捉え方が変わるだけであるという点に注意が必要である。煙という事象が、焚き火によるものなら単なる事象であり、火災によるものならばインシデントになるということである。
見え方が変わるのではなく、見方を変える必要があるということだ。そのように、インシデントの管理では、インシデントとして認識する前の事象も対象とする管理策を講じる必要がある。

２．２　事前想定と想定外対応

18044 が示唆していることで特徴的なことは、もうひとつある。
インシデント対応としては、計画準備段階として事前計画に基づく対応手順を充実させて、実際のインシデント発生時に、手順に従って対応することが基本である。しかし、その一方で、計画準備段階に用意した手順がインシデントの実情に沿わないときには、手順以外の方法による対応をするための手続きが必要であることを指摘している。なぜなら、インシデントとは、予測不可能な状況となることもあり、その場合には、事後対応を事前計画で想定した範囲内だけで実施することは、むしろ想定外の状況に柔軟に対応をできなくなる場合があるからだ。そのため、想定外の状況に遭遇した場合には、実際の担当者の判断で、事前に定められた処置とは異なる例外処置をできるようにすることも必要となる。そのような例外処置についても管理するような管理策を講じることについて述べている。
このとき、例外処置という語感からは、それが希少のように思ってしまうかもしれないが、実は意外にそうでもない。事前計画に基づく対応手順とは、何らかのインシデントを想定して用意していることから、その想定に基づく予防や防止策を講じることが考えられる。その結果、想定しているようなインシデントについては未然に防ぐ努力がなされており、むしろインシデントとして発見されるものは、想定外のことになる割合は少なくないと考えることができる。
特に事業継続に悪影響を与えるようなインシデントについては、予め想定されていることであれば、そのリスクを残存させるよりは、軽減、回避しているはずであり、そのようなインシデントは、まったく想定していないようなことも起こり得ると考える方が自然であると言える。
以上のように例外処置を希少なものと考えずに、その発生を前提として、例外が発生した場合の手続きを整備することが重要となる。手続きの最初となるのは、事前に準備した標準手順の遵守から、場合によってはそれから逸脱することも含めた例外処置で対応することに切り替える判断

と承認の手続きである。この逸脱について正式に許可されなければ、標準手順だけの遵守が逆効果になってしまうことがあるかもしれない。この許可を誰がいつするのか？その者と連絡が取れなければどうするのか？連絡がとれない状態が一定時間経過したら、事後承認が必ず与えられるのか？その判断の結果について責任所在はどうなるのか？などを、予め明確にしておく必要がある。
それが明確でないということは、担当者がよかれと思って対処したことが、後になって標準手順違反として処分されるかもしれないということになる。それでは、担当者は、組織の事業継続の維持と、自身の責任問題との究極の選択が迫られてしまう。そのとき、保身を選択した人を責めるのは筋違いである。逆に、無心で事業継続の維持にまい進する人は、言い過ぎかもしれないが、実のところリスク管理能力がないかもしれない。
標準手順では役割分担して全員が連携することが基本であり、例外処置では全員が通常の役割を排除して被害拡大防止として考えられることを、できる人が個別判断でやるということが許されなければならない。個別判断は情報共有がある程度必要となるが、通常の連携とは異なる連携をしてもよいということである。そのために、標準手順から例外対処に切り替えることになった場合には、全関係者が一斉にそれに切り替えなければならない。ある人は標準手順だけで、別の人は例外処置だけでというのが混在した場合にはどちらもうまく機能しなくなるからである。
例外処置として全員が役割分担から離れてしまうことでは収拾がつかなくなるのではないかと思われるかもしれないが、必ずしもそうではないということについての良書として、「不確実性のマネジメントーManaging Unexpected」（カール E.　ワイク著、ダイヤモンド社出版）がある。同書では、想定外のことが起きても安全性を維持することが求められるＨＲＯ（高信頼性組織）の紹介と、事象をインシデントの兆候として注意深く確認するための姿勢をマインドフルとして紹介している。ここではその詳細について紹介しないが、それらについては同書を参考にされたい。

例外処置をいささか強調したが、想定範囲内であれば、標準手順の遵守は絶対であることは言うまでもなく、予め想定することや標準手順の整備を軽んじることがあってはならない。
想定外のことが発生するということを想定するのは、自然なことでありインシデント・マネジメントにおいて大切なことなのである。

３．事業継続マネジメントにおけるインシデント・マネジメント

３．１　ワンストップ

先述のとおり、インシデント・マネジメントは事象を見落とさないようにすることが、すべての基本でありそこから始まる。そして、事象を発見した人が、インシデント対応をする人に遅滞なく連絡する体制が必要である。発見してから連絡先を調べるというのではなく、そのことを予め周知しておくことが遅延をなくすことになる。１１９番を誰もが知っているように、社内での１

１９番に相当する連絡先の周知が必要である。このとき、インシデントについて最終的に対応する側の立場で考えると、事象の種類ごとに受付窓口を分けたくなるのはわかるが、それでは発見者が事象ではなく、インシデントの切り分けをしてからでないと連絡できないことになる。そのため、インシデント対応の連絡先は、その種類が多すぎてはならない。なるべくワンストップにするのがよいが、事象だけから分担が明確になるのであれば、複数あってもよい。たとえば、１１０番と１１９番のようにである。

３．２　インシデント対応チーム

事象がインシデントとして認識されたならば、対応をしなければならないが、対応に必要な作業をいくつかのチームに分けるのがよい。暫定対応チーム、恒久対応チームと渉外対応チーム、管理と判断のチームの４つのチームで分担することが考えられる。

暫定対応チームは、インシデントによる被害の拡大防止に必要な実務的な作業を担当する。それは暫定的な措置でもよく、緊急にすべきことを優先する。

恒久対応チームは、原因調査や再発防止など、当面の拡大防止措置の後に必要となる作業を担当する。このチームは、まずは、暫定対応チームとして作業して、恒久対応が必要となった時点で、必要となった範囲のことを実施するのでも構わない。ただし、メンバーは、暫定対応なのか恒久対応なのかを意識して実施するのがよい。

渉外対応チームは、そのインシデントについての組織外との対応についての作業を担当する。インシデントが顧客に影響するなら、社内のコールセンター（電話対応窓口）などの協力が必要となる。マスコミに関することは、広報部などが直接担当するなどが考えられる。大切な点は、これらの対応が暫定対応チームに及ばないようにして、彼らの暫定対応作業が阻害されないようにすることである。

管理と判断チームは、対応作業の進捗管理と判断に特化する。このチームは他のチームが実施するような実務的な作業は行わず、常に冷静に進捗の管理と、暫定対応チームなどの他のチームが自身で判断できないことを判断することに特化する。逆に暫定対応チームは判断に悩むようなことがあれば、それはこのチームに判断を委ねて、判断を必要としない他の暫定対応作業を優先的に継続するのがよい。このチームの作業負荷が高くない状態があるかもしれないが、そのときにも、原則として他のチームの作業を引き受けない方がよい。それを引き受けている間に、緊急の判断事項があった場合に、その判断が遅れてしまいかねないからである。

３．３　ノンストップ

ワンストップにすることやインシデント対応チームで述べたことは、インシデントへの対応についてなるべく無駄な待機時間をなくすことである。すなわち、それをノンストップにするということである。

連絡や判断といった人と人とのコミュニケーションに関係することについて、特に見落とさないように立案する必要がある。インシデント対応の際には、これらの待機時間は、被害の拡大になったり、社外への説明で通常では問題とならないことが大きな問題として受け取られたりしてしまう。
対応フローを整備する際に、待機時間がゼロになるか、時間切れによる事後承認など、タイムアウトを必ず設けて、待機でデッドロックすることがないようにしなければならない。

３．４　解決策は問題の中にはない

事業継続を阻害するようなインシデントが発生した場合の、暫定措置は、インシデントの原因となっている箇所についての、インシデント前への復旧には限らない。それは恒久対応として復旧すべきことである。暫定措置では、平常時の手段とは異なる手段を用いてでも、事業を継続する必要がある。目的達成のために手段を選ばないと言うことができる。特にＩＴに係るインシデントでは、ＩＴの復旧を試みることの他に、ＩＴ以外の方法による代替策で事業を継続するための事前準備を用意周到にすることが重要である。

４．　今後の課題

27035 では、インシデントの類型化のガイドを試みようとしていることを述べたが、その他に、インシデント・マネジメントそのものの改善をどのように実施するのかについても考える必要がある。
これについては、27004 として管理策の有効性評価の議論もされているところであるが、計測できないことの改善が困難であることから、インシデント・マネジメントをどのように評価するのかについても今後検討していく必要があると思われる。

現時点で言えることは、インシデントの発生回数は、インシデント防止対策の評価指標となり得るが、インシデント・マネジメントの評価指標ではない。まだ、国際規格としての議論は進んでいないが、事象を社内の誰かが発見してから、インシデント対応に着手するまでの時間などは、インシデント・マネジメントの評価指標になり得るものと考えられるであろう。そのように測定可能な時間であれば、それを短縮するという改善計画を作成することができるようになる。その他にも評価指標についての検討を継続していく必要があるものと考えている。

（本稿は、http://yosihiro.com/speech/index.html#2009-01-28 からダウンロードできます。）