[Ⓡ 研究論文]

例外措置を活用した情報セキュリティポリシーの柔軟な運用に関する提案～中小企業に着目して～

Proposal on Flexible Management of Information Security Policy Utilizing Exceptional Rules
～ Focusing on Small and Medium-sized Enterprises ～

村﨑　康博　Yasuhiro Murasaki
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

情報セキュリティマネジメント体制の確立は、官公庁や大企業だけでなく中小企業においても必須の課題である。サイバー攻撃など情報セキュリティに関わるリスクへの対応等のため、各企業では情報セキュリティポリシー（以下、ポリシー）を策定し、ポリシーに則った原則規定に従って日常業務を管理・運用してきている。

昨今、社会情勢や技術革新に伴い、時々刻々と変化するリスクや新規デバイスに対応していくなか、原則規定やそれに関わる管理基準・運用手順に基づいた措置も、迅速かつ柔軟に変更していく対応が求められている。しかしながら予め原則規定にはない措置への一律的な管理策はなく、逸脱した措置への解釈・対応には日常業務へのリスクが存在すると考える。

本稿では、ポリシーに例外措置を策定することで、原則規定からの逸脱によるリスク回避や、ポリシー維持につながることを紹介し、さらには、比較的企業規模が小さい企業にとって、例外措置を活用することが、ポリシーを経営戦略に柔軟に適合させ、新たなビジネスチャンスにつなげていく効果が期待できることを述べる。

キーワード：例外措置、情報セキュリティポリシー、中小企業

1．はじめに

今や情報セキュリティポリシー（以下、ポリシー）の策定・実施は、企業規模の大小に関係なく全ての組織（企業や官公庁など）において必須施策のひとつであり、中小企業でも例外ではない。

このポリシーを運用管理する上で、「例外措置」を策定・運用し、想定外の事象にも対応できるようにすることが、これまでにも推奨されてきており[17][20]、例外措置の策定状況についてのアンケート調査結果を分析した結果[22]では、中小企業も含む一部の企業でも実際に策定していることが明らかになった。一方で例外措置の運用実態については、具体的な事象への措置に対して通常規定としているか、あるいは例外として措置しているか、といった傾向も明らかになった。

本稿では、中小企業でポリシーをより柔軟に維持・運用していくための例外措置の活用と効果について述べる。

2．ポリシーにおける例外措置

2.1　情報セキュリティの維持と例外措置

我々は日常業務において、ルールやマナー、あるいは規律・規範を守っている。これらには一般にわかりやすさの観点から、慣習的に詳細に限定するのではなく、原則についてのみ示すことが多い。しかしルールなどに全ての措置を取り上げるのは難しいため、例外が存在する。したがってルールなどでは原則と例外が存在することが多く、例外を適切に規定し実施することで、我々は日常業務を維持している[21]。

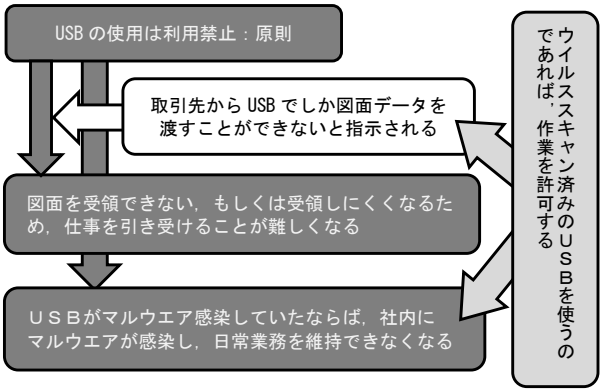
投稿受理日	2017 年 3 月 30 日
再投稿受理日	2017 年 8 月 31 日
査読完了日	2017 年 10 月 6 日

今日の情報セキュリティへの対策においても、社内ルールには「原則と例外」が存在するものと考える。しかし、企業で情報セキュリティを維持・活用する場合に例外を取り扱うときは、日常生活のルールやマナーで例外を取り扱う以上に、「原則と例外」の使い分けを意識しなければならない。これについては、内閣サイバーセキュリティセンター（以下､NISC）からの「政府機関の情報セキュリティ対策のための統一基準群」[1][2][3]や、金融機関などにおけるセキュリティポリシー策定においても示されている[13][14][15]。なお、一般にこれらは官公庁や金融機関・外資系企業向けに策定されてはいるが、例外措置の策定の考え方などは、企業規模に関わらず、中小企業にも活用できるものと考える。

2.2　例外のふるまい

ここで情報セキュリティにおける例外の基本的なふるまいについて、企業における USB フラッシュメモリー（以下、USB）などの利用制限を例として取り上げる。

昨今の個人情報・秘密情報漏えいに関する事件・事故の要因に、当該情報の入った USB を社外へ持ち出すことが挙げられている。そこで企業では、対策として社内ルールに USB の持ち出しについて、USB の全面禁止や利用制限を規定することが多い[16]。その一方で、企業の中には、取引先から図面データの受け渡しにおいて USB によるデータ交換が要請されることが多い。このケースを例に考える（図 1 参照）。



「**あらかじめウイルススキャン済み**」を施すといった要件が，
逸脱に対する許容要件（つまり許容範囲）となる．

図 1　例外のふるまい（USB を例に）

ある中小企業で「USB は全面使用禁止」を社内ルールとして策定していたとする。この場合、中小企業が自社の規則通り USB の使用禁止を貫くならば、図面を受け取れないことで仕事が受注できなくなったり、取引先にて印刷したものを受け取って、自社でスキャンし電子データにして利用したりするなど、手間（時間）と経費がかかる。また、無条件で USB 利用の規則を破ってデータを受領した場合、この USB がマルウエアに感染していたならば、社内にマルウエア感染が拡散し、日常業務が維持できなくなる。

上記のようなケースにおいて、「あらかじめ取引先でウイルススキャン済みの USB を受領するのであれば作業を許可する」、すなわち、例外として条件付きで USB 利用を許可することで、日常業務の中で対応が可能となる。ここで述べた措置が「例外」の適用であり、「あらかじめウイルススキャン済み」を施すといった要件が、内部規定からの逸脱に対する許容要件（つまり許容範囲）となる（図 1 参照）。

3．例外措置の定義とポイント

3.1　本稿での用語の定義

「例外」という用語は広範囲の内容を含んでいるため、定義と範囲を以下に示す。

ポリシーの基本構造は、図 2-1 の内側の三角形に示す通り三層構造（基本方針・対策基準・実施手順）で解説されている[2][9][10][12]。そこで日常業務で定常的に実施されている措置のうち、ポリシーに明記されている規定を「原則規定」とする。この場合、一般的にはこの原則規定から外れることを「逸脱」とすることが多い。

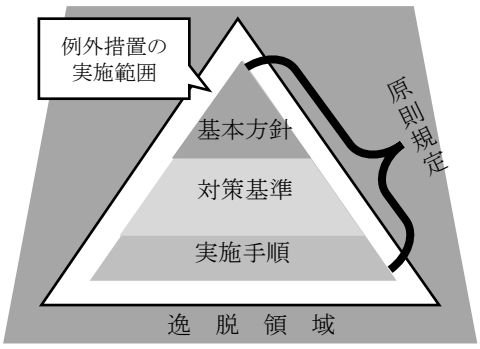


図 2-1　情報セキュリティポリシー基本構造と例外措置

しかしながら本稿では、逸脱の内容・範囲のリスクを厳密に評価して例外と逸脱を区別する。すなわち、リスク低減効果があるとして、承認権限者によって逸脱と区別されて許可される管理策を「例外」とし､実施した行為を「例外措置」とする。例外措置の実施範囲は、図 2-1 において内側の原

則規定の三角形と外側の逸脱領域に挟まれた範囲と位置づけられ、図１の「例外措置の実施範囲」がこれにあてはまる。そして原則規定、および追加した例外措置から外れた事象や措置を、本稿では改めて「逸脱」とする。図 2-1 の三角形外縁内はポリシーであり、そこから外の灰色部分は逸脱領域を指す。

3.2 例外措置のポイント

2.1 節で述べた「例外措置」を策定する場合のポイントについては文献 [17] に詳しく述べられている。本稿ではこの中から中小企業に適した項目を以下に要約する。

- 計画準備段階で対策手順を策定し、実際に事象が発生した場合は、手順に従って例外措置を行う
- 計画準備段階での手順が事象に対する措置の実情に沿わないときには、手順以外の方法で対応できるようにするための手続きを予め準備する
- 担当者の判断で、事前に定められた措置とは異なる例外措置を可能にする（実施したときには、実施を報告する）
- 実施した例外措置をも管理する
- 例外措置と罰則とをセットにする（例外措置と逸脱を区別するため、逸脱についての罰則を用意する）

なお、例外措置からのさらなる例外は避けるべきである。これは、既に例外を認めているため、利用部門側（被管理側）の心理的抵抗感が減少していることから、図に乗って要求を高めてくることが考えられる。このように管理側にとって、「例外からの例外」を認めることは、業務遂行上リスクを高めることにつながるものであり避けなければならない。

3.3 例外措置の適用への判断

一般的には、企業の多くはリスク分析をもとにして策定した管理策の実施状況から、原則規定からの逸脱に対する許容範囲を判断し、例外措置を策定して活用している [20][23][24]。

このような場合には、「企業の目的が設定されてはじめて、リスクが識別されるものである」という前提が求められる。すなわち原則規定においても、元々残余リスクが含まれており、このことから原則規定を策定する段階においては、リスク分析を行い、リスクが残ったとしてもその内容や対処を十分理解してうえで策定するべきである。

また、逸脱した事象に対しての措置を、原則規定には明記されていない別の代替方法により、原則と同程度のリスク軽減が期待できると判断したならば、例外措置として許可すればよいとする。こうすることで、例外措置が持つ、リスクの程度を予め理解して例外措置として策定することができる（図 2-2 の右の吹きだしが示す円内と三角形の内側とが交わる領域）。

原則規定は企業ごとの判断により例外措置と組み合わせることで、柔軟な運用が可能となると考えられる。

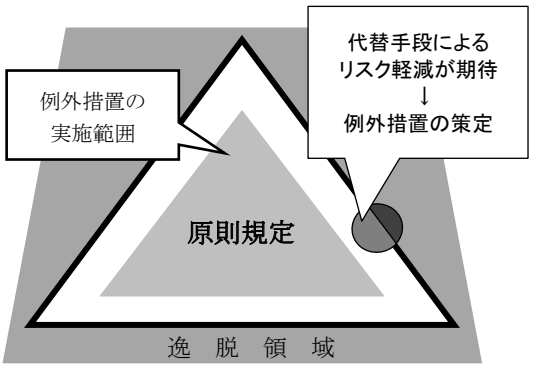


図 2-2 代替手段による例外措置の策定範囲の確立

4. アンケート調査による例外措置の実態分析

ここで、中小企業における例外措置の策定状況、ならびに原則規定と例外措置の策定との関連性を把握するために、アンケート調査による実態調査結果を分析した。本章ではアンケート調査結果と分析結果について述べる。

4.1 アンケートの概要

情報セキュリティ大学院大学原田研究室では、各組織の情報セキュリティに関わる実態を把握するために、毎年「情報セキュリティ調査」を実施している。

本稿におけるアンケート調査は 2015 年 8 月に、日本国内のプライバシーマーク取得組織、ISMS 認証取得組織、BCMS 認証取得組織、政府・自治体、教育機関など 4,500 件から回答を得た 352 件 (全体の 8.0％) を対象に調査・分析されている（詳細な内容については文献 [25] を参照）。

このアンケート調査の項目の一部に、本稿のテーマである例外措置に関連する設問を盛り込んだ。

4.2　例外措置の実態

この調査では、例外措置を実施する際の判断・決定において、原則規定からの逸脱の程度が「例外措置としてどの程度許容されるものであるか」を調べている。具体的には、個々の管理策に対し「原則規定に策定」「例外措置を策定」あるいは「例外措置が未策定」の何れかを尋ね、その結果を発表している[20]。

本稿では、中小企業に関わる例外措置の実態について分析を行った。その結果を図３に示す。なお本稿では、中小企業を従業員数300人以下の組織とみなした[8]。

図３からは、「可搬型メディアの利用」（太枠）項目に対し、「原則規定に策定」「例外措置を策定」（凡例中の実線枠）の回答が多い。すなわち、「可搬型メディア」の利用については、2.2節で述べたように昨今の情報セキュリティに関わる事件・事故を受けて、業務上での利用を禁止・制限する動きがある一方で、使用を許可する例外措置を策定して、リスクを認識させて使用させるという「例外措置」がとられていることが分かる。

なお「可搬型メディアの利用」項目については業種別に分析を行い、このうち回答数が比較的多い「情報通信業」「サービス業」を図４に示す（業種別に関する詳細な内容については文献[25]を参照）。

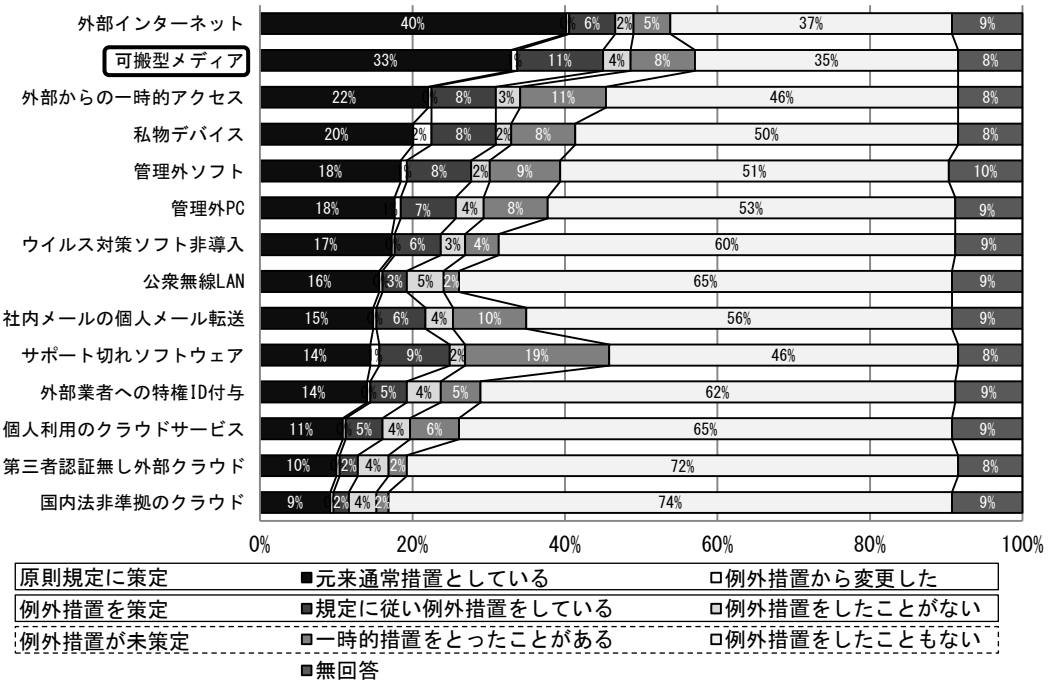


図３　中小企業における具体的な業務上の事象における例外措置の策定の有無（択一、N=249）

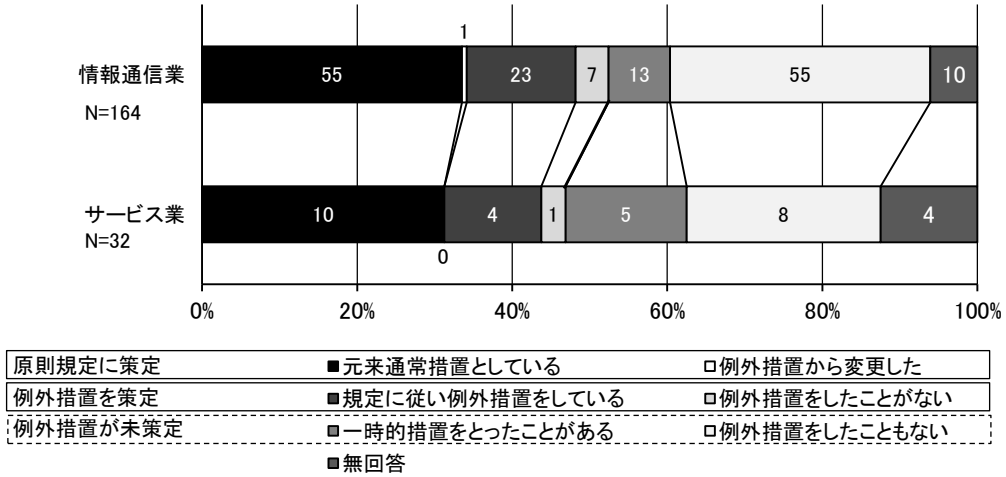


図４　業種別での可搬型メディアに対する例外措置の有無（択一、グラフ中の数値は回答数）

図４からは、情報通信業では「通常措置に設定」と「例外措置を策定」の合計が 52%（55+1+23+7=86 件）と、「例外措置が未策定」の 42％（13+55=68 件）より 10 ポイント程度多い。一方で、サービス業においてはそれぞれ 42%（15 件）、40％（13 件）とほぼ同様な結果となっている。この結果からは USB の利用制限が規定として徹底されている企業とそうでない企業に両極化されていることがわかる [20][22][24]。

4.3 原則規定と例外措置の策定との関連性

図３の単純集計結果から原則規定と例外措置の策定状況のみを抽出し、原則規定の比率が高い順に示したものを図５に示す [20][23][24]。各管理策に対して、原則規定・例外措置の策定を問わず、規定が策定されている中小企業については次のことが考えられる。

まず、例外措置の各管理策について、例外措置を策定しているものが最も多いものでも 50％を超えていない。このことから、例外措置を規定しない理由としては、例外措置そのものを必要としていない、あるいはポリシーや管理策の策定において、例外を規定することに思い至っていないようにも考えられる。これは、中小企業のポリシーの策定にあたって、NISC のガイドラインを参照することもなく、また、中小企業向けのガイドラインに例外措置への規定が記載されていないことなどが考えられる。

個別にみると「外部インターネット」「可搬型メディア」の利用については、多くの企業でほぼ原則規定が策定され通常の措置として運用されている。一方で、その他の管理策については、原則規定で対応する企業が多いものの、例外措置を策定している企業との差が少ない。これは企業において原則規定と例外措置の策定とを組み合わせて、ポリシーの維持管理・運用を進めているためと考えられる。

さらには例外措置の策定を適用する際には、具体的な事象によって対応が変わることも考えられる。例えば、USB の外部持ち出し、BYOD の許可、外部クラウドの活用などの具体事例 [16] では、実際に原則規定・例外措置の策定がされている企業がある一方で、全く規定を策定しない企業もある [19]。

以上、アンケート結果をまとめると次のとおりとなる。

- 例外措置は、策定している中小企業と、していない中小企業とで両極化している。
- 同じ例外措置でも、業種によって策定していたり、策定していなかったりしている。
- 中小企業によっては例外措置を不要もしくは例外措置を想定していない可能性もある。
- 原則規定と例外措置の策定とを組み合わせて、ポリシーの維持管理・運用を進めている中小企業もあると考えられる。

5．中小企業における例外措置の課題

４章では中小企業における例外措置の実態と原則規定と例外措置の策定との関連性について考察した。

この中小企業について、情報処理推進機構 (以下、IPA) の「中小企業の情報セキュリティ対策ガイドライン」等によれば [4][5]、昨今の中小企業は、

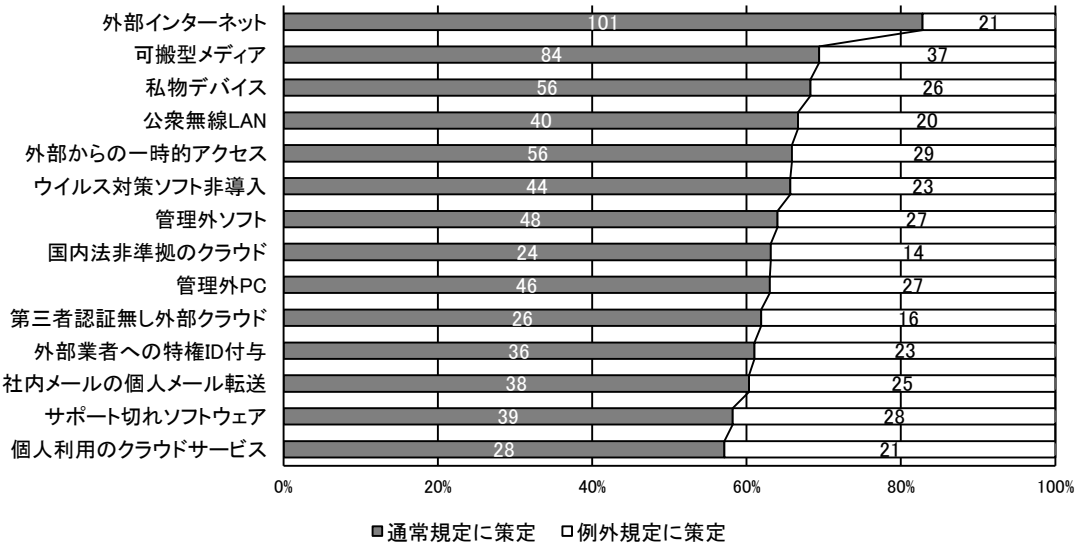


図５ 中小企業における原則規定と例外措置の策定との比率（択一、グラフ内の数値は回答数）

取引先からISMSやPマークの取得などの第三者認証の取得を要請されたりするなど、情報セキュリティ対策が必須となっている傾向がみられる。

しかし、同じくIPAの「2016年度中小企業における情報セキュリティ対策の実態調査報告書」[6]で報告されているように、中小企業では大企業に比べて担当者が少ないことから、本来業務と兼務で担当していることも多いと考えられ、リスクの変化を捉えてきめ細かな情報セキュリティ対策を実施するのが難しい。

本章では、このような中小企業における、例外の措置を実施する場合での課題について述べる。

5.1　例外を認めるべき範囲の判断と適切な措置・リスク対応への課題

3.3節で例外措置の適用への判断について述べたが、まず、例外措置を策定する場合には、例外をどのように認めるのかについての「方針」が必要となる。そしてそのためには例外をどの程度まで許可するかなど「判断」に関するルールも必要である。

しかしながらある時点で逸脱した事象に対して、「具体的にどの範囲までの逸脱を容認して例外措置とするのか」あるいは「(一般的には、リスク分析を行わずにリスク増加を受容することはできないが) 例外措置を容認することで起こりうるリスクを受容できるのか」を判断することは難しい。そして、この判断は企業毎に経営者が決めなければならない。

一方でIPAの調査結果[6]から、「企業規模が小さいほど情報セキュリティ対策の専門部署を設置できておらず、また、組織的なセキュリティ対策が実施されていない企業も多い」「情報セキュリティ担当者の設置やセキュリティポリシーの策定は実施率が低い」ことが挙げられ、一般に、中小企業では人的なリソースの不足から、ポリシーにもとづく原則規定自体が管理面でのリスクに対して、より保守的になりがちとなり、その結果として原則規定が厳しいものになることが多いと考えられる。

これは原則規定からの逸脱について、特に中小企業の場合、インシデントやリスクを正しく評価することが困難であるからである。さらには、例外を認めたことで管理側の責任も発生するため、どうしても保守的になり、リスクを高く評価しがちになる。その結果、例外措置についても厳しいものとなり、担当者の要望と乖離する事が考えられる。

したがって、中小企業が例外措置を考える場合、経営者は情報セキュリティの管理部門が保守的にならずに例外措置をとれるように、例外措置におけるリスク判断や残余リスクの受容をタイムリーに判断できるような体制を整備する必要がある。

5.2　措置が持つ緊急性の判断への課題

2.2節のUSBの例は、図面のデータ利用が緊急性を伴うのであれば、時間制約を理由に例外措置が原則規定よりも優先される。一方、平常時であれば、原則規定に従って例外措置がとられる。このように対応する事象の特殊性に応じて例外措置を適切に実施・管理しなくてはならない。

事象には予め原則規定では措置できないもののうち、例外として措置する（できる）ものと、想定外のため措置されない（できない）ものがある。そして前者は継続して規律を維持することができるが、後者はルールや規定を見直すために規律を維持できないおそれもある。規律を維持できない後者の場合においては、日常業務に影響がでる可能性もある。

すなわち、予め例外措置をする（できる）ようにし、それに沿って申請を受理し適切に手続きを進めることで業務を継続することが必要であると考える。

6．中小企業の例外措置の活用に向けて

5章の課題を受けて、本章では中小企業を対象にポリシーでの例外措置の活用に向けての対策について述べる。

6.1　企業規模の違いにおける例外措置の考え方

ある特定の事象に対する措置においても、業種毎･企業毎･部門毎に、それぞれにリスクが異なる。例えばUSBの使用についても、情報通信業では、禁止とする規定や例外措置の策定として規制がある一方で、サービス業では、緩和されているなど異なる措置が取られている（図4参照）。

企業ではそれぞれの業務において、主に緊急性を要する事象を取り扱うのか、主に平常的なものとして取り扱うのかで例外措置が異なってくる。即ち企業ごとに例外措置を策定させるには、現場責任者への権限委譲、例外措置についての教育が必要となる。一方で、一般社会における市場動向

や企業の経営方針、今後のIoT等技術の進歩に伴い、例外措置が適用される事態が起こりやすくなると考えられ、例外措置を柔軟に変化させることがより必要となると考える。

これは例外措置の関わる事象が起こりやすくなるということが、リスクも起こりやすくなるということと同じであることを表す。そしてリスクは、それが起こりうる事象とその結果、またはそれらの組み合わせにより特徴づけられる[11]。したがって、例外措置は、見直すまでは一時的な措置であり、恒常的な原則規定でない限り、措置も変化し、見直しを経て、例外措置も変化する必要があると考えられる。

中小企業の場合、リスクが発現した場合においても、小回りのきく体制、すなわち小規模な経営体制が持つ、敏捷性のある意思決定により、直ぐにリスク対応を行うことで、被害を最小にすることも可能である。

また規模が小さいことで、経営者を含め“従業員の顔が見える”環境にあり、経営者から従業員に例外措置を直接、迅速に伝えて実施するだけでなく、従業員からもまた、経営者に対し現場で即座に必要とされる例外措置を直接提案することができる。仮に、策定した例外措置がその企業に適合しないと判断したときには、直ぐに当該例外規定を見直すこともできる[4]。

これは、5章の課題である、例外措置を適切に判断する体制づくりや緊急性を要する例外措置について、「企業規模が小さいことが有利に働く」可能性があることを示すものと考える。

6.2 競争優位に繋がる例外措置の可能性

一部の企業は、他社と差別化を図るために、いち早く新規のデバイスやサービスを導入し事業を効率的に進めようといった戦略的な経営を進めている。ここでは、これらのデバイスやサービスがもたらす、想定されなかったインシデントやリスクについて、事前にリスク評価して規定を策定する必要がある。そしてその結果を反映したセキュリティ対策を規定することが原則である。

これらについて大企業などでは、十分に検討して対策を実施している。そのため、セキュリティ対策を厳しくするあまり、デバイスを持ち出せない、あるいはBYODを禁止することにつながる。

一方、中小企業では次の施策が考えられる。

まず類似の規定をもとに例外措置を策定してデバイスなどを使ってみる。併せて、例外措置を運用しながらリスクや追加が必要な管理策についての経験を積み重ねる。この過程で、どの程度・どの頻度で例外措置を講じるべきか、その範囲をどうするべきかの経験を積んでいく。

その結果として、迅速に行動し、素早くフィードバックすることで、新しいセキュリティデバイスやサービスなどにおいて、動きの遅い大企業に対して競争優位に立つことが可能となる。

このように例外措置を活用することで、中小企業の競争優位に繋げることが期待できる。しかし、経験の少ない中小企業で、例外措置を実施したときには、これが本格的な逸脱にならないようにチェックすることが必要である。

6.3 例外措置と監査・外部認証

企業規模が小さい場合、例外措置が影響する範囲も限定されるので、例外措置が逸脱にならないための最低限の仕組みが必要となる。これには、幾つか種類があるが、既に企業内部にある監査などの仕組みを利活用するのがよいと考える。具体的には、リスクの高い分野に絞り込んで重点的に実施するのがよいと考える。内部の監査であれば、企業の特殊性やどの領域が逸脱になるかについても理解できているので、問題が起きたときに適切に対応できると考えられる。

このような柔軟な体制と管理の仕組みを構築して管理できれば、5章でも触れたが、将来的にISMSやPマークの外部認証への対応も可能になるものと考える。

また当該企業が取引している業者に対しても、例外措置の運用も含めた監査を定期的に受けていることで、「例外措置はいい加減なルール」と思われないような運用と管理がなされていることを主張できる。

6.4 例外措置を前提としたセキュリティポリシーの提案

本節では、中小企業に適したポリシーについて提案し、一例として、図3で上位にあった「可搬型メディア」とBYODの具体的な管理策をもとに、例外措置を前提としたポリシーについて述べる。

2.2節でも述べたが、管理外PC、スマートフォン、USBに対する利用制限はあるものの、完全に禁止している企業は中小企業では少ない。一方で、特に教育機関[7]や研究施設、個人情報・秘密情報

を扱う企業[16]においては、禁止もしくは企業からの支給された可搬型メディアによる使用に制限されている。

これらから見て取れるのは、USBは原則使用禁止、PCは企業が貸与するといった原則規定の策定を前提とし、必要に応じて、例外措置として、一部を緩和する方法が考えられるということである。

一方、IPAの調査結果[6]などから、スマートフォンの貸与については中小企業における費用対効果の考慮から、使用禁止でも企業貸与のいずれでもなく、私物スマートフォンの使用を認めるBYODの方向に進む可能性が高いと考える。したがって、BYODの例外措置は企業の多くが必要としており、例外措置の策定は必須であると考える。

具体的な案としては次のとおりである。

まずスマートフォンなどの私物端末の業務利用は現時点では原則禁止であることを周知する。

そのうえで管理部門は、希望する利用部門や利用者からその事由や利用方法についてヒアリング等を行い、「接続してもよいクラウドやネットワーク、利用できるデータや業務は何か」といった例外措置を策定し、これに遵守できる利用申請について認めることにする。

さらに従業員に対し例外措置を例示するなどして明確に周知徹底を図り、例えば「どういった使い方をすると危険なのか（リスクに繋がるのか）」などについての教育を受けさせる。

利用部門が増えてきた場合は、例外措置ではなく原則規定とするべきか検討を始める。

この場合、文献[18]に述べられているように、BYODを禁止する選択肢もあるが、その結果として管理部門が把握できない部分でBYODが蔓延化してしまうおそれがある。その結果、よりリスクが見えなくなり潜在化することで、より高いリスクにつながり、インシデント対応が難しくなる。一方、例外措置でむしろBYODのリスクを顕在化させておくことでリスクが可視化でき、インシデントの際にも対応しやすい効果が期待できる。監査の場合にも、例外措置の実施状況という形でリスクの程度をチェックできる効果も期待できる。

さらにBYODを禁止することは、実効性を高めるために従業員を監視するなどが必要となり、より管理部門の負担が増えることにつながる。人的なリソースが厳しい中小企業においては、ポリシーについては、厳しい規制を前提にするよりも、例外措置を含んだ形で規則を策定することがより、現実的と考えられる。

参考として図5の管理策項目ごとに、ポリシーにおける原則規定と例外措置の策定例を対比した表を付録として添付した。中小企業では、これを利用して具体的な例外措置を策定すればよいと考える。

7. おわりに

リスクが時々刻々と変化する中で、組織にとって、ポリシーを完全に確定した状態で情報セキュリティマネジメント体制を確立することは難しい。そのため、中小企業も含め企業の一部では、4章のアンケート調査にもあるとおり、原則規定およびリスクに対応して例外措置に基づいた措置を講じてきている。

例外措置は、ポリシーに基づく原則規定が維持できないときに、日常業務を継続するためのバッファのようなものである。すなわち、例外措置を予め策定しておくことは、例外措置が必要と思われる事象が起きた時に、迅速かつ客観的に措置を移行できるメリットがある。リスク変化の激しい環境では、頻繁に規定を見直すことは難しく、そのため例外措置を用いて柔軟に運用する方が効果的である。

中小企業では、人的リソースが不足しており、ポリシーや原則規定を頻繁に見直すことが難しい。一方、新しいデバイスなどの影響については、規模が小さいが故に限定的であることから、例外措置についても容易に扱える。すなわち、中小企業ではリスクに対してきめ細かくポリシーを見直すことよりも、新しいデバイスなどを戦略的に利用できるように例外措置を整備し、いち早く利用することで、大企業に対して差別化を図れる。この機会をとらえ、例外措置に基づき新しいデバイスを先行的に利用することで、リスクや問題点の経験や知識を素早く入手できる。

最終的には、これをポリシーに反映することで、リスクを的確にコントロールしていく。すなわち、中小企業では、例外措置を活用することで、現実的に可能な情報セキュリティマネジメントの運用が可能となり、結果として適切な情報セキュリティ対策を実施できると言えよう。

謝辞　本稿を執筆するにあたり、調査研究のため情報セキュリティに関するアンケートへの回答にご協力を頂きました企業や団体、組織の皆様に

感謝します。

また、アンケートの封入、データ入力に多大な協力をいただいた、神奈川県立麻生養護学校元石川分教室、神奈川県立高津養護学校川崎北分教室、神奈川県立鶴見養護学校岸根分教室、神奈川県立みどり養護学校新栄分教室、川崎市立中央支援学校(五十音順)、外1校の神奈川県内の特別支援学校に感謝します。

さらに御指導頂いた本学諸先生、在学生・客員研究員各位、ならびに本学事務局の皆様に感謝致します。

参考文献

[1] 内閣サイバーセキュリティセンター;「政府機関の情報セキュリティ対策のための統一管理基準(平成24年度版)解説書「1.2.1.3 違反と例外措置」」、内閣サイバーセキュリティセンターホームページ(オンライン)、入手先< http//www.nisc.go.jp/active/general/pdf/K304-111C.pdf>(参照 2017-08-31)

[2] 内閣サイバーセキュリティセンター;「政府機関統一基準適用個別マニュアル群 DM2-04 2011年4月」、内閣サイバーセキュリティセンターホームページ(オンライン)、入手先 <http://www. nisc.go.jp/active/general/kijun_man_index.htm> (参照 2017-08-31)

[3] 内閣サイバーセキュリティセンター;「政府機関の情報セキュリティ対策のための統一管理基準(平成26年度版)」、内閣サイバーセキュリティセンターホームページ(オンライン)、入手先 <http//www.nisc.go.jp/active/general/pdf/kijyun26.pdf>(参照 2017-08-31)

[4] 独立行政法人情報処理推進機構セキュリティセンター;「中小企業の情報セキュリティ対策ガイドライン」、独立行政法人情報処理推進機構セキュリティセンターホームページ(オンライン)、入手先< http://www.ipa.go.jp/files/000014017.pdf> (参照 2017-08-31)

[5] 独立行政法人情報処理推進機構セキュリティセンター;「中小企業における組織的な情報セキュリティ対策ガイドライン」、独立行政法人情報処理推進機構セキュリティセンターホームページ(オンライン)、入手先< http://www.ipa.go.jp/files/000014023.pdf> (参照 2017-08-31)

[6] 独立行政法人情報処理推進機構;「2016年度中小企業における情報セキュリティ対策の実態調査報告書」、独立行政法人情報処理推進機構セキュリティセンターホームページ(オンライン)、入手先< https://www.ipa.go.jp/security/fy28/reports/sme/index.html> (参照 2017-08-31)

[7] 文部科学省;「学校における携帯電話の取扱い等について(通知)、平成21年1月30日」、文部科学省ホームページ(オンライン)、入手先<http://www.mext.go.jp/b_menu/hakusho/nc/1234695.htm> (参照 2017-08-31)

[8] 中小企業庁;「中小企業・小規模企業者の定義」、中小企業庁ホームページ(オンライン)、入手先< http://www.chusho.meti.go.jp/soshiki/teigi.html>

[9] 日本規格協会;「JIS Q 27001:2014(ISO/IEC27001:2013)情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」、日本規格協会(2014)

[10] 日本規格協会;「JIS Q 27002、2014(ISO/IEC27002:2013)、情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範」、日本規格協会(2014)

[11] 日本規格協会;「JIS Q 31000:2010 リスクマネジメント―原則及び指針」、日本規格協会(2010)

[12] 中尾康二編;「ISO/IEC27001:2013 情報セキュリティマネジメントシステム要求事項の解説」、日本規格協会(2014)

[13] 日立グループ;「情報セキュリティ報告書」、日立製作所(2014)

[14] 金融情報システムセンター;「金融機関等におけるセキュリティポリシー策定のための手引書(第2版)」、金融情報システムセンター(2008)

[15] 東京海上リスクコンサルティング;「金融機関の情報セキュリティポリシー策定のためのアイディア・ヒント集(V1.0)」、東京海上リスクコンサルティング(2014)

[16] 日経NETWORK;「企業セキュリティ調査 Part2 USB編」、日経NETWORK 2012年7月号 pp.42-44(2012)

[17] 佐藤慶浩;「企業における情報セキュリティ対策の実務」、佐藤慶浩ホームページ(オンライン)、入手先 <http://yosihiro.com/speech/presenter/2014-11-29b/data/resources/2014-11-29b-enPit.pdf>、(参照 2017-08-31)

[18] 高槻 芳；「公私混同のススメ ～ 今どきのBYOD、クラウドが生むBYOD新潮流」、日経コンピュータホームページ2012/09/24（オンライン）、入手先 <http://itpro.nikkeibp.co.jp/article/COLUMN/20120920/423888/>(参照2017-08-31)
[19] 平木健士ほか；「業務利用のスマートデバイスのマネジメントについて」、システム監査学会2013年度第27回研究大会（2013）
[20] 村崎康博ほか；「情報セキュリティポリシーにおける例外措置に関する一考察」、第15回情報科学技術フォーラム講演予稿集、3P-RN003（2016）
[21] 村崎康博ほか；「情報セキュリティにおける例外措置に関する考察」、情報処理学会研究報告、Vol.2015-EIP-69、No.7（2015）
[22] 村崎康博ほか；「情報セキュリティ調査で分かった組織における情報セキュリティポリシーの " 例外措置 " について」、情報処理学会研究報告、Vol.2016-EIP-71、No.6（2016）
[23] 村崎康博ほか；「情報セキュリティポリシーにおける例外措置の効果への一検討」、情報処理学会研究報告、Vol.2016-EIP-72、No.2（2016）
[24] 村崎康博ほか；「情報セキュリティポリシーにおける例外規定の普及に向けての一考察」、情報処理学会研究報告、Vol.2016-SPT-20（2016）
[25] 村崎康博ほか；「2015年情報セキュリティ調査から見えてくる企業・組織における現状」、2016年 暗号と情報セキュリティシンポジウム講演予稿集、2B3-3（2016）

付録

付録 A.1 情報セキュリティポリシーにおける原則規定と例外措置の策定対比表（例）
（図５の各管理策項目にもとづく）

管理策	原則規定例	例外措置の策定例
外部インターネット	許可なく外部インターネットの利用は禁止する	業務上理由がある場合は、申請の上、外部インターネットの利用を許可する
可搬型メディア（USBメモリ、SDカード等）	ＵＳＢメモリの使用は原則禁止とする	取引先からの指示などやむを得ない場合は、予めウイルススキャン済みであれば使用を許可する
サポート切れのOSやソフトウエア	サポート切れのＯＳはソフトウエアの使用は全面禁止である	全く外部ネットに接続しないレガシーシステムについては許可することもある
プログラム保守のための外部からの一時的アクセス	プログラム保守による外部からのアクセスは事前承認を要する	緊急措置が必要であると経営者が判断した場合は事後申請で構わない
私物可搬型デバイス(スマホ・タブレット等)	業務上必要がない場合は、原則使用を禁止	ウイルス対策や盗難時データ処理を設定した上で許可する
自社が管理していないPC	自社以外のＰＣの持ち込みは原則禁止	業務上理由がある場合は、申請の上、持ち込みを許可する
自社が管理していないソフトウエア	自社保有ライセンス以外のソフトウエアの利用は原則禁止	業務上理由がある場合は、申請の上、利用を許可する
ウイルス対策ソフトウエアを導入していないPC	利用禁止	業務上理由があり、全く外部ネットに接続しないレガシーシステムについては許可することもある
外部業者への特権IDを付与	保守による外部業者への付与は事前承認を要する	緊急措置が必要であると経営者が判断した場合は事後申請で構わない
個人で利用しているメールを社内メールに転送	原則禁止	業務上理由がある場合は、申請の上、転送を許可する
公衆無線LAN（暗号無し）の利用	禁止	例外無し
個人で利用しているクラウドサービス（Dropbox等）を利用する	原則禁止とし、企業が契約するクラウドを利用する	取引先からの指示などやむを得ない場合は、申請の上、一時的に利用を許可することもある
非日本国内法準拠のクラウドを利用する	社内審査の許可があれば、企業が契約するクラウドを利用する	取引先からの指示などやむを得ない場合は、申請の上、一時的に利用を許可することもある
第三者認証のない外部クラウドを利用する	原則禁止	取引先からの指示などやむを得ない場合は、申請の上、一時的に利用を許可することもある

村﨑　康博　　情報セキュリティ大学院大学　情報セキュリティ研究科