

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 －例外措置の主観評価と規定逸脱からの許容程度について－

村崎康博^{†1} 原田要之助^{†1}

情報セキュリティポリシーにおける例外規定は、通常規定からの逸脱程度が許容できると判断した上で策定することが望ましい。したがって逸脱に対する許容範囲を調査・分析することは、例外規定に沿った措置を実施する際のリスク回避に効果があると考えられる。

本稿では例外規定の効果を調べるために、まず例外規定の満足度について主観評価を行い、その上で、通常規定との逸脱程度と例外措置との関係について分析を行った。

A Study on the Effect of Exception Measures of Information Security Policy in Organization

- Regarding the Subjective Evaluation and the Tolerance Level of Exception Measures -

YASUHIRO MURASAKI^{†1} YONOSUKE HARADA^{†1}

It would be necessary to establish exception rules of Information Security policy based on consideration about allowance level deviated from regular procedures. Therefore, it is considered that survey and analysis of the acceptable range for deviations would be effective to avoid risk in execution of exception rules.

In this paper, in order to investigate the benefit of exception rules, satisfaction of exception rules is subjectively assessed at first. Then, relationship between level of deviation from normal regulation and exception measures is analyzed.

1. はじめに

昨今の情報セキュリティ対策においては、技術的・システムの対策や人材育成・確保や啓もう活動などの人的対策に合わせ、法的措置も含めた組織ガバナンスなどの組織的な対策が求められている。

その中で、情報セキュリティインシデント（以下、インシデント）に備え、事前に規定の策定し迅速な措置の実施につなげることは、どの企業や官公庁など（以下、組織と表す）において必須施策のひとつと考えられる。

また一部の組織では、事前に想定できなかった状況にも対応できるように例外規定を策定し、例外措置を実施することで継続的な業務管理の維持に努めは始めている。すなわち各組織における例外措置の策定状況と認知度について把握するは、情報セキュリティ対策の重要な要素の1つであると考えられる^{[1][2]}。

情報セキュリティポリシーに例外規定を策定することの重要性については、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」（以下、統一基準群）の推進や^{[1][3][4][5]}金融機関等におけるセキュリティポリシー策定においても明らかになっている^{[6][7][8]}。

一方で例外規定をどのように評価し、具体的にはどのように策定するべきかについては、これまで2つの課題をとりあげてきた^[9]。1つは、例外規定があることで迅

速に例外措置を実施し、通常業務に大きく負担が軽減できるものと期待できるのか、もう1つは、通常規定からの程度の逸脱した事象（もしくは行為）なら、許容範囲として例外措置をとり、業務を継続していくことができるのかである。

本稿では、まず2章において広範囲の内容を含む“例外”を情報セキュリティポリシーにおいて整理し、用語の定義と範囲を述べる。

次に例外措置の許容について検証を進めるにあたり、4章で例外規定に対する効果への満足度について、主観評価を用いて数値化（定量化）した。この分析から具体的な事象に対して、例外措置としての対応をどうするかを考察する。

さらに5章では、具体的な事象に対して、対処する措置内容を明文化した規定の有無ならびに規定がある場合での通常規定と例外規定（2.1 節で定義）との比率について調査した。この分析から例外措置の項目を分類し、分類ごとの傾向について考察する。

2. 例外規定の定義と範囲

2.1 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、はじめに本稿での例外規定の定義と範囲を示す。

まず日常業務において定常的に実施されている措置が、情報セキュリティポリシーに明記されている規定を

^{†1} 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

「通常規定」とする。通常規定から外れることを「逸脱」とし、その内容・範囲を厳密に評価して、権限者によって承認した逸脱を「例外」として定義する。また情報セキュリティポリシーへの文面化の有無を問わず例外を実施した行為を「例外措置」とし、例外措置が文面化されている規定を「例外規定」と定義する。

組織における情報セキュリティにおける例外規定は、策定時に全ての事象を網羅的に対処する措置を準備して運用をはじめるわけではない。すなわち、想定できて準備されている事象と想定できない事象が存在する^[1]。

つまり、非常時・通常時を問わず、規定から逸脱する運用をせざるを得ない事象に対しては、例外規定に定めた例外措置を実施する。一方、措置の時点で例外規定がなく、発生したリスクが受容できないレベルのときには、事後に規定を追加もしくは新規に規定を策定することで、想定外の事象への対応として再現しないようにすることが必要となる。

2.2 情報セキュリティポリシーにおける例外規定

例外規定は、組織の内部規定等で通常規定と共に用いられる情報セキュリティポリシーに盛り込まれるが、情報セキュリティポリシーの基本構造は、図1に示す通り三層構造で解説されている^{[10][11][12][13]}。なお図中における例外規定の範囲としては、この基本構造の外枠に位置づけられる。

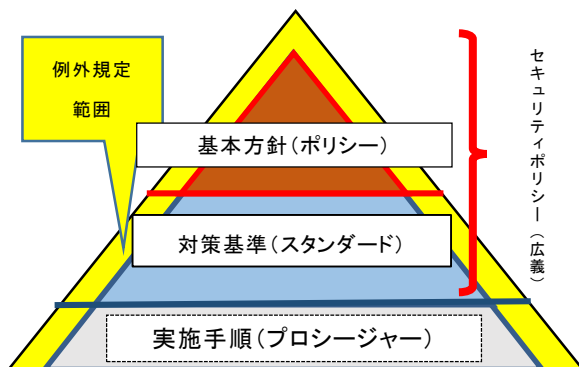


図1 情報セキュリティポリシー基本構造
(参考文献10乃至13より筆者加筆)

情報セキュリティ対策における基本的な考え方を定めるものが、図1の最上層にある「基本方針(狭義の情報セキュリティポリシー)」である。

この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めるのが、2層目の「対策基準(情報セキュリティスタンダード)」である。前述した「(広義の)情報セキュリティポリシー」はこの「基本方針」と「対策基準」を総称することがあり^[11]、本稿でも同様に定義し、以下「ポリシー」と記述する。

この「対策基準」を、具体的なシステムや手順、手続

に展開して個別の実施事項を定めるものが「実施手順(情報セキュリティプロシージャー)」である^[10]。

例外規定はこの3層それぞれに盛り込むことによって業務効率の向上が期待できるが、策定の内容についてはそれぞれ異なる形式になると考える。以下、ポリシーにおける基本方針と対策基準の観点での例外規定について述べる。

2.3 基本方針での例外規定

基本方針は、組織の経営・運用方針について表明するものであり、組織に属する構成員を対象に統一された内容となっていることが一般的である^[7]。したがってどの構成員にも理解できるよう平易で簡潔に記述されており、経営側の意思を表明したり、構成員の義務を明記したりして、形骸化を防ぐ内容となっている。また基本方針は経営方針や組織内風土を反映したものではなくてはならない。

したがって基本方針における例外規定の策定は、以下の事象が起きた時に策定を検討することになる。なお基本方針は頻繁にかつ定期的に見直しをされるものではないため、例外規定においても同様とみなされる。

- (1) 新たな事業展開や法制度の変更にとまなうセキュリティ要件が変わる事象
 - (2) 事故・事件等により安全対策上の大きな脆弱性が発見される事象
 - (3) NISCや外部監査機関などから見直しの勧告を受けた事象
- など。

(1)については、例えば「パブリッククラウドを積極的に利用する」、「情報漏えいの対策としてUSBメモリの利用は全面的に禁止」するかどうかに対する運用方針の決定がある。また(2)については、災害時やインシデント発生時において、「非常事態の宣言と業務移行命令」、「対策本部の設置」、「審議・連絡体制への移行」、「例外措置の実施」などへの対策基準項目の採択の決定などがあげられる。

すなわち基本方針では、例外規定の容認の可否や、非常時での緊急対策本部の設置・指示命令系の統一などといった大筋の方針を定めた策定にとどまる。

さらに例外規定の策定は、基本方針の見直しにつながるため、経営層の承認が必要であり、具体的な策定においてはセキュリティ管理部门が担当業務として担うか、新たに検討委員会などのタスクフォースを編成して行うことが見られる。

2.4 対策基準での例外規定

対策基準では、基本方針を実行に移すための具体的な対策を記述したものであり、スタンダードやガイドライ

ンと呼ばれるものである^[7]。具体的対策を記述するため、組織全体共通にする必要はなく、対象部門別に策定してもよい。一方で、セキュリティレベルを安全とみなせるレベルに維持するために、常にセキュリティ上の見落としや脆弱性がないかのチェックを行う。また基本方針とは異なり、各現場レベルでの状況の変化に適切に対応するために、通常規定の見直しや例外規定の策定求められる。

例外規定は、通常規定に規定されていない事象に対して措置をとるときに必要となる。また基本方針での例外規定と異なり、個別具体的に例外措置を規定する。すなわち当該事象に対応する措置は、通常規定を見直して盛り込まれるまでの、もしくは全くの一時的な対応としての、暫定措置として実施される。

なお対策基準における例外規定については、以下の2つの規模の異なる事象に対して、策定方法が変わるものと考えられる。

1つは大災害など経営に直接影響するほどではないが、日常業務に大きな影響を及ぼす事象への例外規定が求められる時である。一例として大手ソフトウェア会社のOSのサポート期限切れに伴う、基幹システムのソフトウェア更新への対応がある。基幹システムにおいて当初の想定をこえるインシデント対策が求められ、OSに依存していたインタフェースの改修を実施したり、OS自体の延命措置を依頼したりするなど、日常業務においても暫定措置を強いられた組織もあった。

なおOSのサポート期限切れは今後数年後に定期的に起こりうる想定できるため、通常規定にはない例外規定として策定していくのか、一時的に措置だけするかでは、今後の対策基準とし大きく影響していくものと考えられる。

もう1つとしては、日常業務に大きく影響を与えないものの、通常規定とは異なる措置をとる必要がある場合である。すなわち、日常業務で想定できるものであったとしても、BYODのケースのように^[7]、措置の大きさなどで規定しないという“想定外の事象”が起こりうることを“想定内”として意識しなければならないこともある。

さらには私物端末を業務として一時的に利用を許可する例外措置の場合、具体的に、使用期間や目的、理由を目意識した申請書の提出を義務付けるなどの実施手順を定める規定があることで、利用開始時期や審議・決定する時間を短縮できる効果が期待できる。

したがって対策基準では具体的な例外規定の策定が必要であり、当該例外規定にもとづく例外措置を実施するための実施手順の作成が求められる。

2.5 本稿での例外規定の範囲

以上、例外規定における定義とポリシーとの関連性について述べた。なお本稿では、日常業務に直結し、より柔軟に定期的もしくは即時に見直しが求められる対策基準における例外規定について主に取り上げ、これを適用範囲とする。以降適用範囲における日常業務での例外規定の策定と例外措置の実施について述べる。

3. 例外規定への仮定の設定とアンケート調査

3.1 例外規定の調査のための仮定の設定

組織における例外規定の実態と効果を把握するために2章の定義と範囲をもとに、表1に示す2つの仮定をたてた。なお表1に記載のない仮定1乃至仮定6は例外規定の実態について設定しており、詳細については別途報告している^[9]。また本稿では仮定を検証する手段として、3.2節のアンケート調査を利用している。

表1 組織の例外規定に関する仮定

(仮定7)	通常規定との逸脱程度と、例外措置の規定策定との間には、何らかの関係がある
(仮定8)	例外規定の策定に伴う例外措置への定量的評価ができ、評価基準ができるのではない

3.2 アンケート調査実施概要

例外規定の策定状況の実態を把握するために、公務(政府・自治体)、企業、大学などの組織に対してアンケートによる調査を実施した^[9]。

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、例年「情報セキュリティ調査」を実施している。平成27年度の調査項目の一部に、本稿のテーマである例外規定に関連する設問を盛り込んだ。

アンケート調査は2015年8月に郵送にて実施した。対象は、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、教育機関などから選んだ4,500組織(送達確認:4,373組織)である。その結果352件(8.0%)の回答が得られた^{[15][16]}。

3.3 アンケート設問

3.1節の表1の仮定に基づいて設問16と設問23を作成し(表2参照)、設問16は仮定7に対する分析(5章)に、設問23は仮定8に対応する分析(4章)に用いた。なお設問14、設問15および設問17乃至設問22については、3.1節で触れた仮定1から仮定6にかかる単純集計(一部クロス分析)用を使用している^[15]。

表2 アンケート設問一覧

[設問16]	具体的な業務上の事象において、例外規定の有無
[設問23]	具体的な効果についての主観的評価

4. 例外措置に対する主観評価の試み

本章では、例外措置の許容について検証を進めるにあたり、例外規定に対する効果への満足度について、主観評価を用いて述べる。

4.1 概要

表1の仮定8「例外規定の策定に伴う例外措置への定量的評価ができ、評価基準ができるのではないか」に対応するアンケート設問 23 の「具体的な目的や効果に対してどのような効果があると、主観的に感じているか」について、アンケート項目に答える形態での主観評価実験を実施した。

設問は、過去のアンケート調査^[15]で使用した設問肢や2章の先行事例をもとに、9つの例外措置の具体事例(迅速な業務手続きができることで業務停止を防ぐ等)を設問肢とし(表3参照)、それぞれに対して主観的に満足・安心かどうかといった、6段階の回答選択肢を選んでもらう形式とし(表4参照)、その結果を評価とした^[17]。

表3 設問23における設問肢一覧

(1)	迅速な業務手続きで業務停止を防ぐ
(2)	通常手続きに係る時間・コストが節約でき、機会損失・被害を未然に防ぐ
(3)	現時点では想定外で、通常手続きに書いていない事象にも、予め審議体制を確立できている
(4)	規定違反として罰則適用を未然に防ぐ
(5)	次期規定策定への参考、事例となる
(6)	内部・外部監査への適用しやすくなる
(7)	経営ガバナンスに貢献できる
(8)	ISMS 等第三者認証の更新が容易になる
(9)	情報セキュリティ関連規定全体に効果がある

表4 回答選択肢

規定別	選択肢
満足・安全圏	(1) とても満足・安全
	(2) 満足・安全
	(3) どちらかといえば満足・安全
不満・不安圏	(4) どちらかといえば不満・不安
	(5) 不満・不安
	(6) とても不満・不安
その他	(7) 一時的措置をとったことがある

単純集計結果を図2に示す。なお設問肢は表4に示す「満足・安全圏」の合計の多い順に並べている。

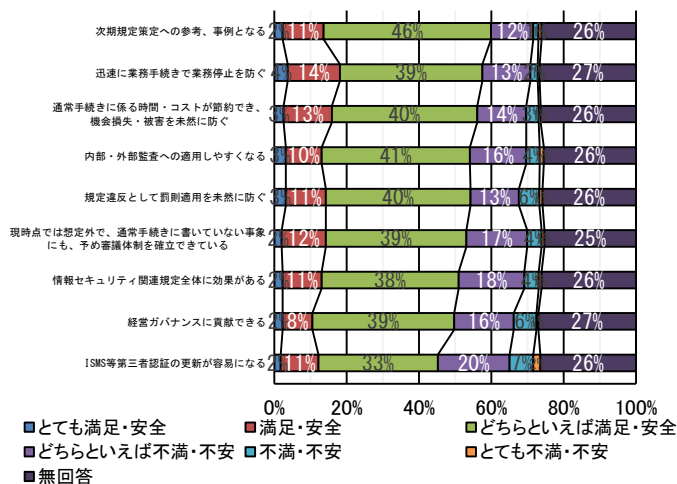


図2 具体的な目的や効果に対する主観的評価
(択一、N=352)

図2からは、9つの例外措置のうち、「次期規定の見直し」「手続きの迅速化」「時間・コスト削減への効果」において満足・安心圏が50%から60%の範囲であることが分かる。

また無回答を除き、単純に満足・安全圏と不満・不安圏とで分けしものを図3に示す。図3からは、すべての設問肢において、満足・安全圏が不満・不安圏を上回ることがわかった。

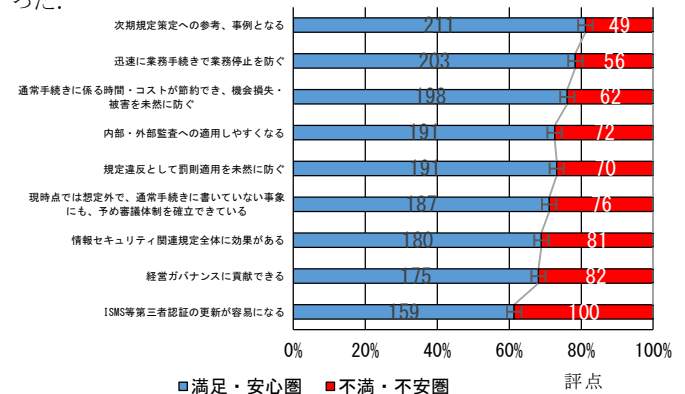


図3 満足・安心圏ー不満・不安圏別グラフ
(択一、グラフ内の数値は回答数)

4.2 二重刺激劣化尺度法による主観評価分析

図3の示すように、満足・安心圏が不満・不安圏を上回った点をさらに詳細に分析するために、図2の結果をもとに二重刺激劣化尺度法(以下、分析法)^[18]を用いて主観評価分析を行った^[17]。この分析法は主に画質・音質劣化の主観評価に利用する。本稿ではこの分析法により、例外規定の有無によるポリシーなどへの満足度を評価した。

まずアンケート設問 23 の6段階回答選択肢と分析法の5段階評価点との互換性をとり(表5参照)、設問肢ごとの累積評点を求めた上で分析を行った(図4参照)。なお互換性をとるにあたり、アンケート回答選択肢の「とても満足・安全」と「満足・安全」を、分析法の評点5「気に入らない」にまとめている。

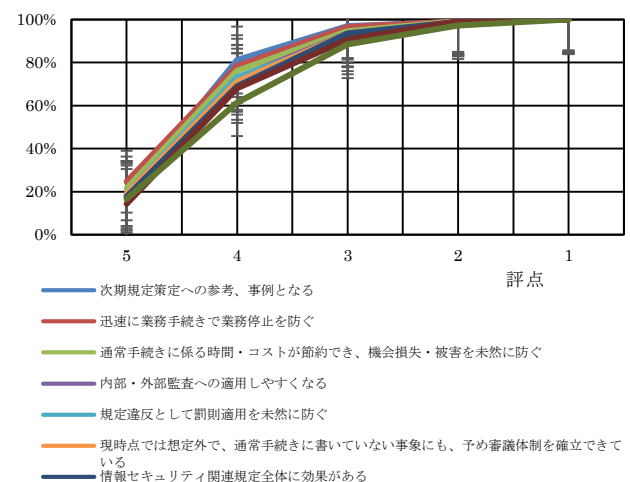


図4 設問肢別累積評点

表5 主観評価点の互換一覧

評点	5	4	3	2	1
アンケート回答選択肢	とても満足・安全／満足・安全	どちらかといえば満足・安全	どちらかといえば不満・不安	不満・不安	とても不満・不安
二重刺激劣化尺度法回答選択肢	気にならない	どちらかといえば気にならない	どちらかといえば気になる	気になる	とても気になる

図4をもとに評点別累積値を設問肢間の相関を分析し、その結果を表6に示す。表6からは設問肢間の相関が強く、それぞれの傾向に依存性があることがわかった。

表6 評点別累積値を設問肢間の相関
(小数点2桁以下四捨五入、表中の「問」は文中の「設問」を指す)

相関	問1	問2	問3	問4	問5	問6	問7	問8	設9
問1	1.00								
問2	0.99	1.00							
問3	0.99	0.99	1.00						
問4	0.99	0.99	0.99	1.00					
問5	0.99	0.99	0.99	0.99	1.00				
問6	0.99	0.99	0.99	0.99	0.99	1.00			
問7	0.98	0.99	0.99	0.99	0.99	0.99	1.00		
問8	0.98	0.99	0.99	0.99	0.99	0.99	0.99	1.00	
問9	0.97	0.98	0.98	0.99	0.99	0.99	0.99	0.99	1.00

そこで図4の各設問肢の平均値を利用して許容限を求めることにした。その結果をグラフにしたものを図5に示す。

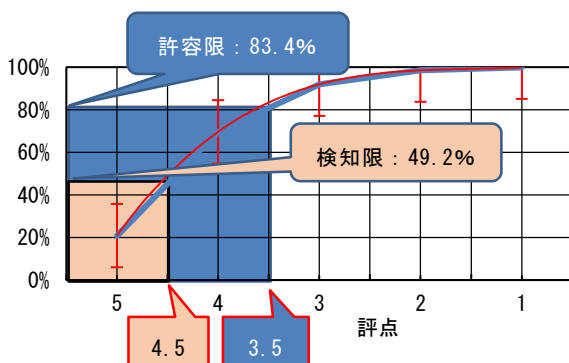


図5 主観評価分析結果

図5中の平均値から近似式を求めた結果、評点 3.5 における許容限は 83.4(単位%)、ならびに 4.5 における検知限は 49.2 となった。この結果から8割以上が自組織のポリシーにおける例外規定に対して、「満足・安心」できると回答したものと解釈できる。

以上、主観評価を用い組織の満足度を数値化(定量化)することは、例外措置の効果を知る手掛かりの1つになるものとする。例外規定を設定するにあわせて満足度を評価することで、その項目への(例外措置としての)対応をどうするかを目安にできると期待できる。

4.3 主観評価分析結果へのヒアリング調査

なお上述の許容限 83.4 について、直観的な感想や意見を求めるために学内でヒアリング調査を試みた。

本調査は、平成 28 年2月 26 日に開催された 2015 年度 ISS Square (<http://iss.iisec.ac.jp/>)シンポジウムでのポスター発表(内容は非公開)会場にて口頭により実施した。

ヒアリングは、まず本節の手法を説明した後で、

“自組織の情報セキュリティポリシーにおける
例外規定の「満足・安心」度は約 80%です”

と報告を受けたと想定したときに、直観的に、

「安心を感じる／安全と思う」か、

「不安を感じる／危険と思う」か、

のいずれであるかをたずねてみた。その結果を図6に示す。

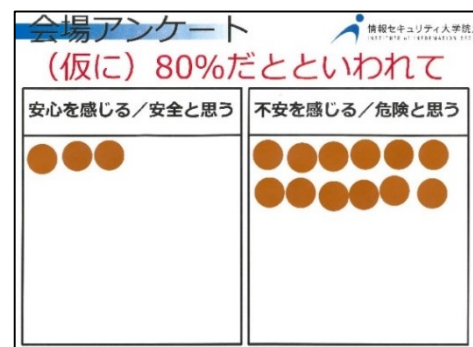


図6 許容限に対するアンケート結果(択一、N=15)

回答者は学内の教官、連携教官ならびに学生・卒業生の 15名で、サンプル数が少なく、情報セキュリティを専門とする者からの回答であったため、図6の結果を単純に一般社会への評価に転用することは難しい。

しかしながら、12名(80%)が「不安を感じる／危険と思う」と回答し、主な理由として、“情報セキュリティポリシーの重要性を認識している立場では、8割程度の満足・安全度では納得できず、楽観的な傾向が見られる”などの意見が多く寄せられた。その一方で、「安心を感じる／安全と思う」と回答した理由としては、“より客観的に考えれば8割強の評価は十分な結果ではないか”とする意見が少数だが寄せられた。

5. 通常規定からの逸脱と例外規定について

本章では、4章に引き続き例外措置の許容について検証を進めるにあたり、具体的な事象に対して、規定(通常・例外)の有無・例外規定への策定傾向について述べる。

5.1 概要

通常規定からの逸脱の程度が、“例外規定としてどの程度許容されるものであるか”は例外措置を実施する際の判断・決定に重要な要素であると考えられる。

例えば、USBメモリを全面使用禁止している組織があるとする。当該組織が保有する基幹系機器(例えばサーバー)のメンテナンスを請け負う事業者が、USBメ

メモリでしか、作業ファイルを更新できないようなシステムである場合、通常規定のみであれば、作業できないため通常業務を維持することができなくなる。一方、USBがマルウェアを保持していたならば、一時的にUSBメモリを使用許可したために、組織のイントラネットにマルウェアに感染することになり、これもまた通常業務が維持できなくなる。したがってあらかじめウイルススキャン済みのUSBを使うのであれば、USBメモリによる作業を許可することで、メンテナンス作業も通常業務も継続することが可能となる。この場合、「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。

組織においては、この許容範囲を通常規定に盛り込むのか、例外規定として策定するか、あるいは全く指定しないのかは、業種や規模、組織によっても異なってくるものと思われる。さらには、逸脱への許容範囲を策定しない、すなわち例外規定を策定しない事例を考えてみれば、逸脱する事例を全く想定していないのか、もしくはあえて逸脱に対して規定を策定しないのかの2つに分けられるものと考えられる。

そこで表1の仮定7「通常規定との逸脱程度と、例外措置の規定策定との間には、何らかの関係がある」に対応するアンケート設問14を用いて分析した。設問14では、過去のアンケート調査^[15]で使用した設問肢や先行事例^{[9][17]}をもとに、14個の例外措置の具体事例を表7に示す設問肢として設定した。

表7 設問16における設問肢一覧

(1)	ウイルス対策ソフトウェアを導入していないPCを利用する
(2)	サポート切れのOSやソフトウェアをPCで利用する
(3)	貴社管理外ソフトを利用する
(4)	貴社管理外のPCを利用する
(5)	私物可搬型デバイス(スマホ・タブレット等)を利用する
(6)	可搬型メディア(USBメモリ、SDカード等)を利用する
(7)	外部インターネットを利用する
(8)	プログラム保守のため外部からの一時的アクセスを許可する
(9)	外部業者への特権IDを付与する
(10)	第三者認証のない外部クラウドを利用する
(11)	非日本国内法準拠のクラウドを利用する
(12)	個人で利用しているクラウドサービスを利用する
(13)	個人で利用しているメールに社内メールを転送する
(14)	公衆無線LAN(暗号無し)を利用する

そして各設問肢への回答用に表8に示す選択肢を設定した。選択肢は「通常規定に設定」「例外規定に設定」「規定がない」の3パターンにそれぞれに具体的な措置の実施をたずねた。

表8 設問16における選択肢一覧

規定別	選択肢
通常規定に設定	(1) 元来、通常措置としている
	(2) 例外措置から変更した
例外規定に設定	(3) 規定に従い、例外措置をしている
	(4) 例外措置をしたことがない
規定がない	(5) 一時的措置をとったことがある
	(6) 例外措置をしたことがない

設問肢・選択肢を設定しアンケート回答した単純集計結果を図7に示す^{[15][16]}。なお図7は表7の「通常規定に設定」「例外規定に設定」の合計の高い順に設問肢を並べている。また図7中の設問肢の記載は表7から一部省略している。

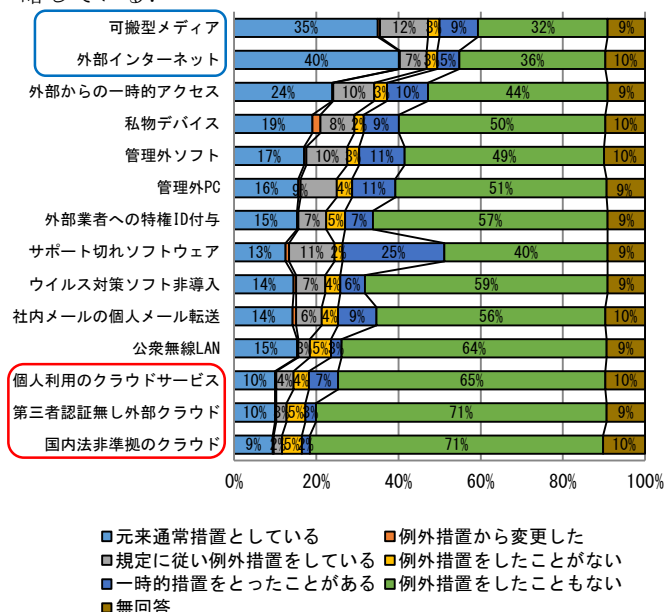


図7 具体的な業務上の事象における例外規定の有無(択一、N=352)

図7からは、「可搬型メディア」「外部インターネット」項目に対し、表8に示す「通常措置に設定」「例外規定に設定」への回答が多かった。

一方で、「個人利用のクラウドサービス」「第三者認証無しの外部クラウド」「国内法非準拠のクラウド」について回答を求めたところ、ともに7割以上が例外規定がなく、例外措置もとったことがないという結果になった。すなわち図7からは、クラウドの利用については規定がない組織が多いことがわかった。

これについては以下の2点が考えられる。1つは全くクラウドを利用していない組織であること。もう1つは、情報システム部門や情報セキュリティ部門への申請・上申なしで現場組織がクラウドを利用している。すなわち規定が伴わない現場判断での利用である。2.4節で述べたBYODのケースと同様^[14]に、利用現場に運用・管理をまかせ、管理組織が知らない形をとっているとも考えられる。

一方、クラウド以外の設問肢については、何らかの規定が策定済みであり、例外措置も実施されている可能性が高い。例えば「外部インターネット」の利用については、通常業務上不必要なサイトへの閲覧を禁止する上で、申請・上申があれば、例外的に閲覧を許可している。

また「可搬型メディア」の利用については、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、使用を許可する旨の例外規定があれば、手続きをとった上で例外措置をとるようにしていることが分かる。

なお業種別^{[9][17]}で回答の多かった「情報通信業」「サービス業」「大学」「公務（政府・自治体）」それぞれにクロス分析した結果を図8に示す。

公務では68%、情報通信業では53%が「通常措置に設定」「例外規定に設定」と回答したのに対し、大学では33%と差があることがわかった。これは公務ではUSBメモリを利用制限が徹底されている反面、大学においては制限が少ない傾向にあると考えられる。

その他イントラネット接続管理外や外部アクセスに関わる設問肢では、概ね30～40%の割合で通常規定あるいは例外規定が策定されている。すなわち、設問肢それぞれに事前に規定があることで、組織ガバナンス・マネジメントに有効となっている。

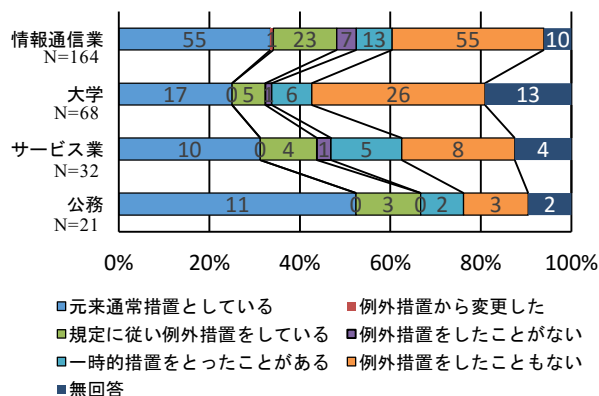


図8 業種別での具体的な業務上の事象における例外規定の有無（択一、グラフ中の数値は回答数）

なお「サポート切れのソフトウェアの利用」に対する回答については他の項目と異なり特殊性が見られた。通常規定もしくは例外規定が策定されていないものの、実際に例外措置を一時的に実施した回答が25%と、他の設問肢と比べ極端に多い。これは大手ソフトウェア会社のOSのサポート期限に対する対応が、本アンケート調査の回答時期と重なったことで今回だけの特殊性と考える。しかし2.4節で述べたとおり、各組織が今後も起こりうるOSサポート切れへの措置に、例外規定あるいは通常規定として規定していくのか、今後の動向を注視し

ていく必要がある。

5.2 通常規定と例外規定との策定状況における考察

図7の単純集計結果から通常規定と例外規定の策定状況のみを抽出し、通常規定の比率が高い順に示したものを図9に示す。なおここでは各設問肢に対して、通常規定・例外規定を問わず、規定が策定されていることを前提にしている。

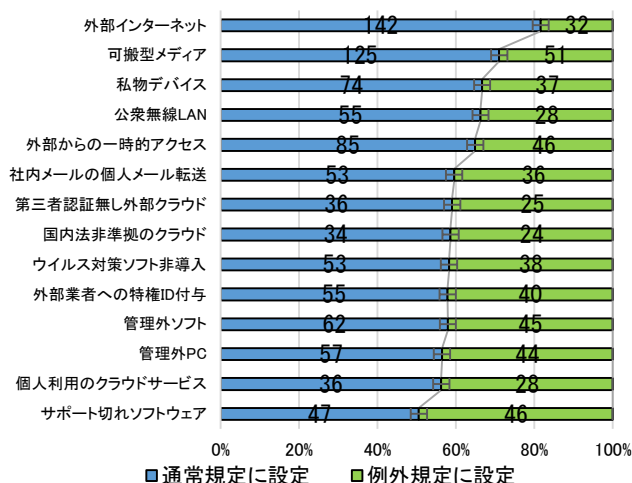


図9 通常規定と例外規定との比率（択一、グラフ内の数値は回答数）

図9から「可搬型メディア」「外部インターネット」の利用については、5.1節で述べたとおり規定策定が進んでおり、ほぼ通常規定として策定され通常措置として運用されていることがわかる。

その他の設問肢については、通常規定への策定が進んでいるものの、例外規定との差が少ない。これは組織が双方をうまく使い分けて、管理・運用しているためと考えられる。特に「サポート切れのソフトウェアの利用」については同程度の比率であり、5.1節で述べたように例外規定・通常規定の使い分けが進んでいることがわかる。

6. まとめ

本稿では、情報セキュリティポリシーにおける例外措置への主観評価、ならびに通常規定からの逸脱と例外措置と許容程度の関係について述べた。

まず「例外」について定義と範囲を整理し、基本方針・対策基準ごとの例外規定の策定の特徴について述べた。

次に、例外規定の策定と例外措置の実施の効果を、通常規定との逸脱程度と例外措置との関係（仮定7）、および例外規定の策定に伴う例外措置への評価基準（仮定8）を用いて検証し、通常規定と例外規定とのバランスや定量的評価の提示していく重要性を述べた。

事前に例外規定を策定し例外措置を実施することで、不測の事象に備えることは、日常業務の維持もしくは最低限の業務量の低下に結びつくと考え。

今後は、例外規定の策定実態と傾向ならびに例外措置の効果に関する知見を取りまとめ、普及に向けた提言していきたいと考える。

謝辞 本調査を実施するにあたり、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原田研究室各位ならびに本学事務局の皆様には感謝致します。

参考文献

- [1] 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://yoshihiro.com/speech/presenter/2014-11-29b/data/resources/2014-11-29-b-enPit.pdf>>，
- [2] 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
- [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(オンライン)，入手先<<http://www.nisc.go.jp/active/general/pdf/K304-111C.pdf>>
- [4] 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(オンライン)，入手先<<http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf>>
- [5] 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(オンライン)，入手先<http://www.nisc.go.jp/active/general/kijun_man_index.htm>
- [6] 日立グループ：情報セキュリティ報告書，日立製作所，2014
- [7] 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
- [8] 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
- [9] 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
- [10] 総務省：地方公共団体における情報セキュリティポリシーに関するガイドライン(平成27年3月版)，総務省ホームページ(オンライン)，入手先<http://www.soumu.go.jp/main_content/000348656.pdf>
- [11] 内閣サイバーセキュリティセンター：政府の情報セキュリティの基本的な考え方，情報セキュリティポリシーに関するガイドライン H14（オンライン），入手先<http://www.nisc.go.jp/active/sisaku/2002_1128/ISP_Guideline_20021128.html>
- [12] 総務省：情報セキュリティポリシーの内容（2013年），総務省ホームページ(オンライン)，入手先<http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/04-3.html>
- [13] 情報処理推進機構：情報セキュリティポリシーの策定，情報セキュリティマネジメントとPDCAサイクル(2016)（オンライン），入手先<<http://www.ipa.go.jp/security/manager/protect/pdca/policy.html>>
- [14] 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
- [15] 村崎康博ほか：“2015年情報セキュリティ調査から見える企業・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
- [16] 情報セキュリティ大学院大学原田研究室：2015年度情報セキュリティ調査，情報セキュリティ大学院大学原田研究室ホームページ(オンライン)，入手先<http://lab.iisec.ac.jp/~harada_lab/survey.html>
- [17] 村崎康博ほか：“情報セキュリティポリシーの例外措置における主観評価に関する一検討”，信学総大，A-12-3，2016
- [18] ITU-R 勧告，“Methodology for the subjective assessment of the quality of television pictures”，BT500-11,2006
（以上，オンライン入手先の参照日時は2016-04-08）