

情報セキュリティポリシーにおける例外措置

村崎 康博^{1,a)} 原田 要之助¹

受付日 2017年3月13日, 採録日 2017年9月5日

概要: 情報セキュリティポリシーの策定・実施は, すべての組織 (企業や官公庁など) において必須施策の1つであり, 想定外の事象にも対応できるように“例外措置”を策定している組織もある, この例外措置の策定状況についてアンケート調査したところ, 組織ごとの策定・運用実態や, ポリシーからの逸脱程度と例外措置の傾向が明らかになった. 内閣サイバーセキュリティセンターが提供している情報セキュリティ対策のための統一管理基準を広く活用していくために, 効率的な例外措置の活用を今後検討すべきであると考ええる.

キーワード: 情報セキュリティポリシー, 例外措置, 政府統一基準群

Exception Rules Concerning the Information Security Policy

YASUHIRO MURASAKI^{1,a)} YONOSUKE HARADA¹

Received: March 13, 2017, Accepted: September 5, 2017

Abstract: Implementation of information security rules is one of mandatory measures for all of enterprises, incl. government. Those rules have been designed from historical security incidents. On the other hand, those cannot cover unexpected incidents and new requirements. Therefore, some of enterprises have implemented “exception rule for exceptional case”. Nowadays, scope of escape from rigid rule might be dependent on individual organizational matters. In addition, it is unclear that those rules have been written based on proper recognition on security risk under unexpected situation. This study surveys and analyzes present situation of “exception rules” and application of the rules, and the benefit from the viewpoint of organizational governance.

Keywords: Information security management, exception rule, exception measure, deviation

1. はじめに

我々は日常業務や学業, そして私生活において, ルールやマナー, あるいは規律・規範を守っている. これらには一般に分かりやすさの観点から, 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慣習的に多い.

しかしルールなどにすべての措置を盛り込むのは難しいため, 潜在的に例外が存在する. したがって実際には原則と例外が存在することが多く, 例外を適切に措置することで, 我々は日常業務や学業, そして私生活を維持している. 一方, 組織において情報セキュリティを維持・活用する

場合についても, 原則と例外は存在する. そもそも組織は情報セキュリティポリシー (以下, ポリシー) において, 起こりうるすべてのセキュリティインシデントやリスクを事前に把握し, それに対応する措置をあらかじめ策定したうえで, 運用することは困難である. そのため, 例外措置を講じる必要が出てくる.

さらに情報セキュリティにおいて例外措置は, 災害やセキュリティ攻撃のような非常事態における措置だけではない. ICTの著しい技術進歩や一般社会への急速な普及などの影響に対して円滑に仕事を進めるための対策としても例外措置は必要と考えられる [1], [2].

実際, 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) [3], [4], [5] や, 金融機関などのポ

¹ 情報セキュリティ大学院大学
Institute of Information Security, Yokohama, Kanagawa
221-0835, Japan

^{a)} mgs148503@iisec.ac.jp

リシーにおいても、例外措置が明記されている [6], [7], [8]. これにともない官公庁や金融機関, さらには外資系企業などでも例外措置の取扱いが広まっており, 今後一般企業にも広がるものと考えられる。

2. 例外措置の定義と範囲

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, 本稿での例外の定義と範囲を以下に述べる。

まず日常業務において, 定常的にリスクを低減させるために実施されている措置は, 原則, ポリシーに網羅されているものとする。この場合, 一般にポリシーから外れる事象や措置は「逸脱」とすることが多い。

しかしながら本稿では1章でも触れたように, 従来「逸脱」とされたものから一部を「例外措置」として区別する。具体的には, 承認権限者によって逸脱の内容・範囲を厳密に評価され, ポリシーと同程度のリスク低減効果があると許された措置を「例外措置」として定義する。そしてポリシーおよび追加した例外措置からも外れた事象や措置を改めて「逸脱」とする。

2.2 ポリシーにおける例外措置

ポリシーの基本構造は, 図1の内側の三角形に示すとおり三層構造で解説されている [9], [10], [11], [12]. 例外措置の実施範囲は, 図1において内側のポリシー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る。なお逸脱領域と例外措置の規定との境界については, 4章で述べる。

まず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」である。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全体的に統一された内容となっている。

基本方針に関係する例外措置としては, たとえば「CISOなど責任者による例外措置の許可権限」や「非常時での緊急対策本部の設置・指示命令系の統一」などであり, 経営方針に関わる, 包括的なものになっている。

次に, この基本方針に基づき, すべ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。対策基準には, 基本方針を実行に移すための具体的な対策を記述する。

対策基準での例外措置は, 組織全体に共通したものである必要はなく, 対象部門ごとに策定・実施してもよい。個別具体的に例外措置を実施することで, 部門ごとの日常業務に沿ってセキュリティリスクを低減させたり, リスクレベルを維持させたりするための, 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つねに行う [7], [9].

なお「対策基準」を, 具体的なシステムや手順, 手続に

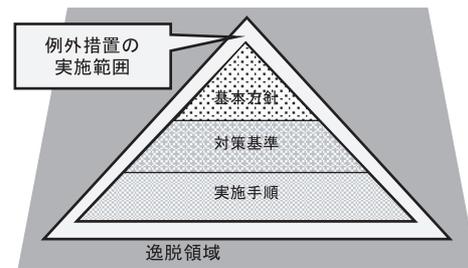


図1 情報セキュリティポリシー基本構造

Fig. 1 Basic structure of information security policy.

展開して個別の実施事項を定めるものが, 最下層の「実施手順 (情報セキュリティプロシージャ)」である。

2.3 例外措置の特徴

災害やセキュリティインシデントのような想定外の事象に対しては, 必ずしも当該事象がポリシーの対象になっていなかったり, 必要な対策基準や実施手順があらかじめ策定されてなかったり, もしくは不十分であったりする。このため事前計画で想定したポリシーの範囲内だけで実施すると, リソースや時間がかかって手順の一部が実施できなくなったり, あるいは措置そのものができなくなったりするなど, かえって柔軟に対応できなくなるおそれがある。

さらに例外措置があらかじめ策定されていない場合, 2.1節で述べたようにポリシーから逸脱した事象や行為は逸脱領域にあたるため, 即禁止や規制, 罰則の措置がとられる。またポリシーの改定そのものにも時間がかかるため, 事象のリスクが変わった時点ですぐに当該事象への措置がとれない。

このような事態を避けるため, 当該事象に対応する例外措置は, ポリシーを見直して盛り込まれるまでの暫定措置として実施される [1]. すなわち例外措置によって想定外の事象への対応をカバーすることにより, ポリシーからの逸脱を防ぐことが期待できる [2].

3. 例外措置の先行事例

組織の情報セキュリティの取り組みについては, 上場企業や政府機関を中心に, 報告書 (有価証券報告書, 情報セキュリティ報告書, 年次レポートなど) によって公開されるようになった (たとえば, 文献 [6] など). また, 経済産業省では情報セキュリティ監査制度をもとに「情報セキュリティ監査企業台帳」を公開し, 2016年度には300近くの企業がそこに登録されている [13].

しかしポリシーに関わる規定の策定や措置の記載についての具体的な報告は少ない。そのためポリシーは上記報告書などでは一般公開されておらず, 例外措置についても詳細に知ることは難しい。

本稿では, このような実態があるなかで, 実際の組織においてどのようなポリシーや例外措置が決められているか

について調査した。その事例を以下に示す。

3.1 官公庁での例外措置

例外措置の事例として最も参考となるのは、官公庁や一部の企業において策定・実施を進められている、NISC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)である [3], [4]。

この統一基準群が策定される際の有識者会議において、インシデント対応で必要となる例外措置の規定について検討がされている [2]。ここでは、例外措置についてインシデントなど事前の想定が不可能な事象の場合、事後対応を事前計画で想定した範囲内だけで実施すると、かえって想定外の状況に柔軟に対応できなくなることが指摘されている。そして、そのために例外措置をあらかじめ想定しておくことが必要であると述べている。

なおNISCでは、例外措置を効率良く進めるために手続きの流れや様式も定めている [5]。

3.2 ISMSでの例外措置

情報セキュリティマネジメントシステム (Information Security Management System 以下、ISMS) は、組織の意思決定に必要な管理体制 (マネジメントの仕組み) が導入されていること、および情報セキュリティのリスクを低減させるための管理策が適切に維持・運用されていることを目的に策定されている [14], [15]。

ISMSに必要な管理策についての詳細なガイドとして、ISO/IEC27002:2013がある [16], [17]。この中の12章「運用のセキュリティ」では、情報処理設備の運用における管理目的および管理策が定められている。

具体的には12.1節「運用の手順及び責任」では、「情報処理設備の正確かつセキュリティを保った運用を確実にすること」が記述されており、さらに12.1.1項「操作手順書」および12.1.2項「変更管理」において、それぞれの実施手順が記載されている。

なお、これら操作手順の「実施の手引き e) および f)」、ならびに変更管理の「実施の手引き g) および h)」において、例外措置の記載がある。ここでは例外措置を認める場合、明確に例外措置として運用することを定めるとともに、例外措置に関わる変更管理を徹底するとしている。

3.3 海外での例外措置

海外事例として本稿では、日本企業の米国法人での例外措置の定義について述べる。なお本事例はヒアリング調査によるものである。

ヒアリングした組織では、例外措置におけるガイドラインと手順 (Exception Handling Guidelines and Procedures) を規定している。このガイドラインでは、3.1節に述べた統一基準群と同様、ポリシーでは対応が難しい事象に対して

例外措置を許可 (定義) している。この特徴を2点述べる。

1つは、逸脱と例外措置を明確に区別して定義している点である。これによりポリシーから逸脱した事象が、例外措置を実施することによって、ポリシーと同等の効果が確保できる。その結果として、ポリシー違反による事象・事件を防げるかどうか判断できるものと考ええる。

もう1つは、例外措置を実施するにあたり、例外措置をとらなくてはならない事由を必ず提出させて説明責任を問うている点である。これは「Comply or Explain (原則を実施するか、実施しない場合はその理由を説明するか)」の考えに基づいている。すなわち例外措置を実施するのであれば、申請した部門や個人に対して、その説明責任を負わせ、そして例外措置によって起こりうるリスクを理解させる。これにより、リスクの発生を未然に防ぎ情報セキュリティの確保を図る。

3.4 民間組織での例外措置

官公庁以外では外資系企業や日本の大手企業の約20社がNISCの統一基準群における例外措置を採用している [18]。

また、金融情報システムセンター (FISC: The Center for Financial Industry Information Systems) 発行の金融機関などにおけるセキュリティポリシー策定のための手引書 [7], [8] にも同様の例外措置が明記されている。したがって、日本銀行を含め国内の金融機関が例外措置を導入しているものと考えられる。

4. 例外措置の課題

3章では先行事例の調査やヒアリングを通じて、官公庁や企業では、例外措置をあらかじめ策定することで組織の意思決定やマネジメントに役立てていることが分かった。一方で少なくとも以下のような課題があると考ええる。

4.1 課題1: 例外措置の導入

例外措置がなくポリシーのみの場合、企業の現場など利用部門がビジネスで必要と自己判断し、ポリシーを無視して管理部門に知られないように水面下でポリシーを逸脱するおそれもある。管理部門側も全面禁止として例外を認めない場合は、このような逸脱をまったく想定していないか、もしくは逸脱を黙認しているか、のいずれかが考えられる [19]。

そこである事象に対して、措置をポリシーとして盛り込むのか、一時的に例外として措置をとるのか、あるいは措置をしないのか、といった対策が候補として考えられる。

4.2 課題2: 例外措置の策定

ポリシーは、組織の運営方針、組織風土および情報セキュリティの特殊性を反映する必要がある。しかしながらポリシーの策定にあたって「自社のリスクは他社と共通で

ある」と見なして、外部の雛形を安易にそのまま導入するにとどまり、画一的なものになっているのではないかとする課題もある [20].

したがって、ポリシーに付随する例外措置についても、組織ごとに異なるものではなく、ポリシー同様に画一的なものになっている可能性があるため、組織に必要な例外措置とはなっていないことが考えられる。

4.3 課題3：例外措置の見直し

例外措置は、ポリシーから逸脱した事象が起きたときへの一時的な措置であり、措置の実施後も同様の逸脱が想定できる場合には、ポリシーに新たに盛り込むのか、その事象のみとして一時しのぎの措置とするのかなど、見直す必要があると考える。

なお、実際に見直しを実行しているかどうか、実態が明らかになっているわけではない。

4.4 課題4：ポリシーからの逸脱の程度と例外措置

3章の先行事例では、ポリシーからどの程度までの逸脱を例外措置の規定として許容しているか具体的には分からなかった。これはポリシーをあらかじめ明確に策定したうえで例外措置が運用されるわけではない(1章参照)ことも原因である [2], [19]. したがって図1に示すとおり、ポリシーと例外措置の実施範囲をどのように線引きするのか、さらには逸脱領域に対する明確な例外措置の境界線をどこまで拡張できるのか明らかではない。

昨今の情報漏えいに関する事件・事故などから考えると、今後組織においては、事前にリスクを評価して、ポリシーと逸脱の範囲を求め、間を埋める例外措置を活用することが必要であると考えられる。

5. 例外措置の現状

4章の課題に対して、組織における例外措置の規定の実態と効果を把握するために、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 [18].

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。2015年度の調査項目の一部に、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。

アンケート調査は2015年8月に郵送で実施した。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 [21].

以下、アンケート調査の結果と考察について、4章に述べた課題1から3については本章で、課題4については6

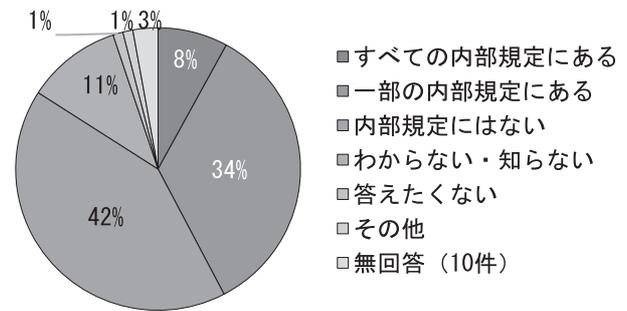


図2 情報セキュリティに関わる内部規定全般において「例外措置」の有無(択一, N=352)

Fig. 2 Presence or absence of “exceptions” in the internal regulations related to information security.

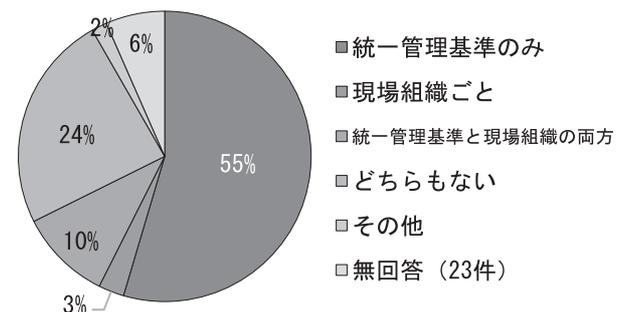


図3 例外措置は組織全体で統一されたものか、現場組織ごとにも規定されたものか(択一, N=352)

Fig. 3 Exception rules which was unified in the entire organization, whether that is also specified for each site organization.

章で述べる。なお、課題1から3へのアンケート調査については3.1節のNISCの統一基準群での例外措置のポイントも参考にした。

5.1 例外措置の規定の有無

課題1「例外措置の導入」についてアンケート調査の結果を図2に示す。本設問では内部規定全般において「例外措置の規定」の項目の有無をたずねた。なおここでの内部規定は本稿でのポリシーと見なして説明する。

結果は、例外措置は「すべての内部規定にある」「一部の内部規定にある」割合と、「内部規定にはない」割合が同じ(42%)であった。

5.2 例外措置の規定の策定部門

課題2「例外措置の策定」についてアンケート調査の結果を示す。まず“例外措置は組織全体での統一されたもののみか、それとも現場組織ごとにもあるのか”をたずねた結果を図3に示す。

図3から、例外措置の策定は「統一管理基準のみ」が半数を超え(55%)、「現場組織ごと」と「統一基準群と現場組織の両方」を合わせた割合(13%)と大きく差があることが分かった。

次に“例外措置を実施するにあたり、例外措置の策定と

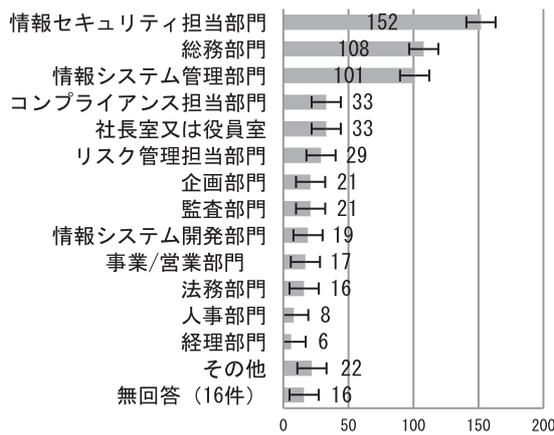


図 4 例外措置を実施するにあたり、例外措置の策定と管理の事務処理をする主体部門 (択一、グラフ内の数値は回答数)

Fig. 4 Subject department to the business processing of formulation of regulations and management upon developing the exception.

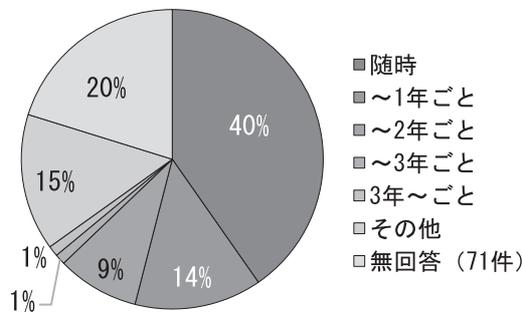


図 5 例外措置の見直し頻度 (択一、N=352)

Fig. 5 Review the frequency of exceptions.

管理の事務処理する主体部門はどこであるか”をたずねた結果を図 4 に示す。図 4 からは、例外措置を策定する組織は「情報セキュリティ担当部門」、「総務部門」、「情報システム管理部門」の順で多いことが分かる。さらに「総務部門」が情報システム業務を担当している組織もあることや「情報システム開発部門」の回答も含めると、例外措置の策定と管理については、情報系部門がほぼ主体となって担っているものと解釈できる。

5.3 例外措置の業務の見直し期間

課題 3「例外措置の見直し」についてアンケート結果を図 5 に示す。本設問は、例外措置の見直しの頻度についてたずねた。図 5 からは、例外措置の見直し頻度は、「随時」と回答した組織が 40%と最も多い。

さらに「1年以内 (14%)」「2年以内 (9%)」と続き、比較的短い期間で見直しをしていることが分かった。一方で「その他」が 15%、「無回答」が 20%とあることから、見直しをしていない組織も多いと解釈することができる。

5.4 例外措置の現状からの考察

以上、課題 1 から 3 についてのアンケート調査の結果か

ら以下のことが考えられる。

5.4.1 策定/未策定の二極化

5.1 節の結果からは、ポリシーに対して、例外措置がある組織とない組織とで二極化している。ない理由としては例外措置に対する認知が薄いのか、もともと例外措置を必要と認識していない可能性がある (5.4.3 項参照)。このことから今後、例外措置がない組織に対しては、普及を図ることが必要と考えられる。

5.4.2 専門部門への集中

5.2 節の結果から、部門ごとに例外措置を策定して実施しているものは少なく、多くは専門部門において組織の統一基準群で例外措置が規定されている。また、例外措置の策定・管理は、情報セキュリティや情報システムに関わる専門的知識のある情報系部門が多く、「経理部門」などの利用部門では少ない。

例外措置には、専門的な知識や経験などに基づく判断が必要であり、利用部門で策定するのは難しい。情報系部門と利用部門で協議する組織体制の構築などが求められると考える。

5.4.3 例外措置体制がとれない組織

5.3 節の結果からは、「随時」見直ししている組織が多い一方、文献 [1] による詳細な分析から、“実際に例外措置をすることが少ない”、“見直し頻度もそのつど”、“例外措置の規定はないが一時的に例外措置を実施した”の特徴を持つ組織が多くみられることも分かった。すなわち、多くの組織では、例外措置について事象が起きたそのつどに対応し、その後、必要に応じて規定として策定・見直ししていると考えられる。

つどの対応では、緊急性も求められることから、一時しのぎで例外措置を行うことになる。同じ事象が起きても組織が規定として学習していないため、将来、同様な事件や事故が発生すると、再度、同様な一時しのぎの例外措置を繰り返す可能性が懸念される。

以上により、例外措置の実施状況の把握が、組織の情報セキュリティマネジメントに対する経営側の考え方を知る手がかりの 1 つになることが分かった。ただし、例外措置を実施しているのは一部の組織にとどまっていることから、経営者に対して例外措置の効用を知らせる必要があると考える。

6. ポリシーからの逸脱と例外措置

本章では、ポリシーからの逸脱と例外措置との関連性について、課題 4 に基づくアンケート調査の結果を示す。

6.1 アンケート調査の分析

例外措置を実施する際の判断・決定において、ポリシーからの逸脱の程度が“例外措置の規定としてどの程度許容されるものであるか”を把握することは、3 章の先行事例で

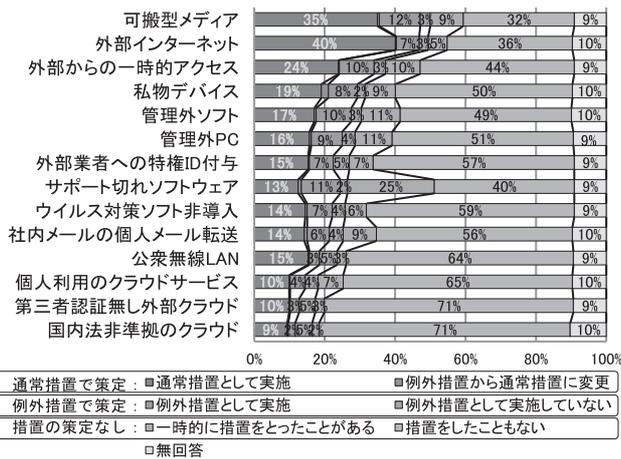


図 6 具体的な管理策における例外措置の有無 (択一, N = 352)
 Fig. 6 Presence or absence of the exception rules in the event on the specific business.

述べたとおり、重要な要素であると考えられる。そこで課題 4「ポリシーからの逸脱の程度と例外措置」について、対応するアンケート設問を用いて分析した。設問では対策基準での具体的な管理策に対し「通常措置で策定」「例外措置で策定」して実施しているか、あるいは「措置として策定していない」か、をたずねた。なおここでの通常措置とは、ポリシーに準じて通常（原則）として措置することを指す。集計結果を図 6 に示す [19]。

図 6 からは、「可搬型メディアの利用」「外部インターネットの利用」項目に対し、「通常措置としている」「例外措置をしている」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」については、ともに 7 割以上は例外措置もとったことがないという結果になった。さらに図 6 からは、クラウドの利用については多くの組織に例外措置がないことも分かった。

6.2 ポリシーと例外措置の策定状況

図 6 の単純集計結果から通常措置と例外措置の策定状況のみを抽出し、ポリシーの比率が高い順に示したものを図 7 に示す。

各管理策に対して、通常措置・例外措置を問わず、規定が策定されていることを前提にすると、図 7 より「外部インターネット」「可搬型メディア」の利用については、多くの組織で通常措置、すなわちポリシーで規定された通常の措置として実施されていることが分かる。

また、その他の管理策については、通常措置で実施する組織の数は多いものの、例外措置として実施する組織と比べると数の差は小さい。これは例外措置に順応性のある組織が、通常措置と例外措置とを組み合わせ、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。

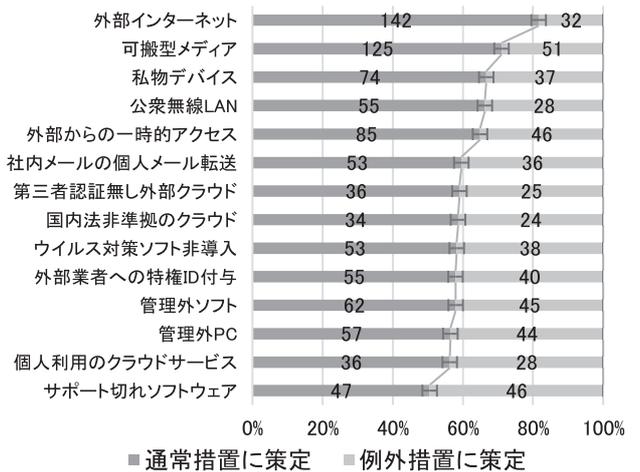


図 7 通常措置と例外措置との比率 (択一, グラフ内の数値は回答数)
 Fig. 7 Ratio of principle regulations and exceptions.

6.3 ポリシーからの逸脱と例外措置に関する考察

以上のことから、例外措置に順応性のある組織であれば、管理策の実施状況をもとにポリシーからの逸脱に対する許容範囲 (図 1 の例外措置の実施範囲に相当) を判断し、例外措置を策定して活用しているものと考えられる。

しかし、その活用状況については図 6 に示すとおり個々の管理策においても例外措置の実施が異なり、特にクラウド利用などでは例外措置が十分に活用されていないことが分かった。さらに、可搬型メディアなど、まだ利用方法が定まっていないものについては、リスクが明確に分かっていないことから、現時点で管理策に例外措置を導入しても、組織のリスクが低減できるかが不明であると考えられる。

すなわち組織は、リスク分析の結果からリスク対策が必要な事象については、それらに対応する措置をはっきりとポリシーに盛り込む。その一方でリスクが比較的大きくない事象については例外措置で対応するといった運用が見られる。

さらに 6.2 節のとおり、ポリシーに例外措置を組み合わせることで、現時点ではリスク分析が不明の事象や新技術への導入、緊急性のある事案などに即応し、組織のポリシーの維持管理・運用に柔軟に活用できるものと考えられる。

7. まとめ

本稿では、組織のポリシーにおける例外措置について、その必要性和活用に向けた具体化について論じた。

例外措置は、ポリシーからの逸脱に対する許容範囲を明確に判断し (6.3 節参照)、ポリシーの定期的な見直しとともに策定する (2.2 節参照) ことが求められる。本来これらは、各組織で実際にリスク分析して管理策をポリシーとして策定するか、例外措置を実施して、組織内での適用事例を増やしていくことが必要である。

しかしながら 5 章の例外措置の現状を見る限り、当該組織のリスクに適応する例外措置の獲得とその効果を得るこ

とは十分に進んでいないと考えられる。また、個々の組織において個別にポリシーや例外措置を作ることは難しいのが実態である。

そこで、NISCの政府統一基準が広く活用されているように、社会全体や業界ごとで統一的に使える例外措置を盛り込んだ基準が必要と考えられる。個々の組織は、この基準を参考にして、個別の具体的な例外措置を構築することで適切な対応をとることができるものと期待される。さらに、例外措置については組織を超えてすべての組織で活用できるような体制作りなどを、今後検討していく必要があると考える。

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いただきました企業や団体、組織の皆様へ感謝します。

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。

さらにご指導いただいた本学諸先生、在学生・客員研究員各位、本学事務局、ならびに派遣元である日本放送協会情報システム局の皆様へ感謝いたします。

参考文献

[1] 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)。
 [2] 佐藤慶浩：企業における情報セキュリティ対策の実務，入手先 (http://yoshihiro.com/speech/presenter/2014-11-29b/data/resources/2014-11-29b-enPit.pdf) (参照 2017-01-11)。
 [3] 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解説書「1.2.1.3 違反と例外措置」，入手先 (http://www.nisc.go.jp/active/general/pdf/K304-111C.pdf) (参照 2017-06-23)。
 [4] 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），入手先 (http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf) (参照 2017-06-23)。
 [5] 政府機関統一基準適用個別マニュアル群 DM2-04 2011 年 4 月，入手先 (http://www.nisc.go.jp/active/general/kijun_man_index.htm) (参照 2017-06-23)。
 [6] 日立グループ：情報セキュリティ報告書，日立製作所 (2016)。
 [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ア・ヒント集 (V1.0)，東京海上リスクコンサルティング (2014)。
 [9] 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，入手先 (http://www.nisc.go.jp/active/sisaku/2002.1128/ISP_Guideline_20021128.html) (参照 2017-06-23)。
 [10] 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），入手先 (http://www.

soumu.go.jp/main_content/000348656.pdf) (参照 2017-06-23)。
 [11] 情報セキュリティポリシーの内容 (2013 年)，入手先 (http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/04-3.html) (参照 2017-06-23)。
 [12] 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)，入手先 (http://www.ipa.go.jp/security/manager/protect/pdca/policy.html) (参照 2017-06-23)。
 [13] 平成 28 年度情報セキュリティ監査企業台帳，入手先 (http://www.meti.go.jp/policy/netsecurity/is-kansa/) (参照 2017-06-23)。
 [14] 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)。
 [15] 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)。
 [16] 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)。
 [17] 中尾康二（編）：ISO/IEC27002, 2013 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 (2015)。
 [18] 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)。
 [19] 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)。
 [20] 情報セキュリティポリシーの現状，入手先 (http://www.atmarkit.co.jp/fsecurity/special/27spolicy/spolicy01.html) (参照 2017-06-23)。
 [21] 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)。



村崎 康博 (正会員)

情報セキュリティ大学院大学。1992 年日本放送協会入局。2016 年情報セキュリティ大学院大学情報セキュリティ専攻博士前期課程修了。同年より情報セキュリティ大学院大学客員研究員として情報セキュリティマネジメント

トの研究等に従事。



原田 要之助 (正会員)

情報セキュリティ大学院大学。1979 年京都大学大学院工学研究科数理工学専攻を修了，電信電話公社（現，NTT）の研究所を経て，2010 年から情報セキュリティ大学院大学教授。リスクマ

ネジメントを担当。