RN-003

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
A Study on the Exceptional Rules Concerning the Information Security Policy

村﨑 康博† 原田 要之助†
YASUHIRO MURASAKI† YONOSUKE HARADA†

1. はじめに

1.1. 背景（例外と情報セキュリティポリシー）

我々は通常仕事や学業，そしてプライベートの生活において，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．しかしルール等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．したがってルール等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，我々は業務活動や私生活を維持している．

情報セキュリティポリシーを策定・運用する場合においても，日常生活のルールやマナーと同様に例外措置を適切に実施することは必要である．情報セキュリティの場合には，例外規定は現場での業務遂行において，規定等への逸脱が適切とされると判断した事象に対して，例外措置を策定することになる．

一方，情報セキュリティポリシーは起こりうる全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，予め通常規定として策定した上で運用することは困難である．この点は日常生活のルールなどと異なる．情報セキュリティの場合には，災害やセキュリティ攻撃のような非常事態における例外措置だけでなく，ＩＣＴの著しい技術進歩や一般への急速な普及などにより，通常業務において円滑に仕事を進めるためには，例外規定が必要となる．

しかし，ある時点で通常規定から逸脱した事象に対して例外規定を策定するにあたり，どの程度までの逸脱を容認して措置するのか，容認することで起こりうるリスクや不安を克服・回避できるのかを判断することは難しい．

この例外規定を適切にどこまで認めるべきかについては，組織毎の判断に委ねられているため，各組織がインシデントやリスクを正しく評価しているか明らかではない．

本稿では，例外規定の策定と例外措置の取り扱いや効果などを分析し，アンケート調査を用いて社会全体の動向を調べた．その結果，組織にとっては例外規定が必要であることを明らかにする．さらに例外規定の期待効果についての検証について述べる．

1.2. 事前考察

情報セキュリティに関する内部規定を自組織で策定する場合では，例外に関する取り扱いは，インシデントでの緊急対応やリスク回避のために重要とされている[1][2]．

情報セキュリティポリシーについては，規定に「通常（原則）」と「例外」があることが望ましい．しかし，規定に例外措置がなく原則のみの場合，通常規定に規定されていないものは実施できないし，実施した場合は規定違反となり罰則が伴う[3]．いずれにしても業務遂行が困難になる．また 2.1 節で述べるが，通常規定を無視して組織に知られず水面下で実施されてしまう可能性がある．このような場合に不測の事象が起きたとき，例外規定の有無で対応に差がつくことになる．

2. 例外規定の先行事例

2.1. 先行事例からの分析

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はじめとして報告書（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）で公開されるようになった（例えば，文献[4]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，平成 27 年度には 260 を超える企業が登録されている[5]．しかしセキュリティポリシーに関わる具体的な規定策定や措置の記載については報告されることが少ない．そのため情報セキュリティポリシーやポリシーに記載される例外規定については，上記報告書などでは一般公開されていない．

そこでいくつかの先行事例を調査・ヒアリングした結果，例外規定への適用には具体的な事象によっても対応が変わることがわかった．さらに組織が抱える目標・目的，業種，人員，資本金などの特徴によっても変わると報告されている．[6]

例えば可搬型メディアの外部持ち出し，ＢＹＯＤの許可，外部クラウドの活用などの具体事例では，実際に通常規定・例外規定がされている組織がある一方で，全く規定を策定しない組織もあることが分かっている[7]．策定していない組織においては，あえて規定を作らないことで利用する現場に責任転嫁しており，管理・経営側への上申ルートを作らず組織としての責任を放棄している．

すなわち，新規のデバイスやサービス，想定されなかったインシデントやリスクへの対応においては，事前にリスクを評価して規定を策定する必要があるものの，実際には策定できていない．しかし昨今の情報漏えいに関する事件・事故などから，内閣サイバーセキュリティセンター（以下，NISC）の政策方針（2.2 節参照）や情報セキュリティに係る組織ガバナンス・マネジメントが重要となっている．本稿では，以上の実態を前提として，組織に必要となる例

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

外規定を調査した．その事例を以下に示す．

2.2. 官公庁の例外規定

例外規定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・実施を進めている「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[8][9]．

この統一基準群では，NISC が規定を策定するにあたった有識者会議では，インシデントへの対応で必要となる例外規定について検討している[3]．ここでは，「事前想定」と「想定外対応」が取り上げられている．すなわち，インシデントなど事前の想定が不可能な事象については，事後対応を事前計画で想定した範囲内だけで実施すると，かえって想定外の状況に柔軟に対応できなくなると述べている．

2.3. 統一基準群の例外規定のポイント

以下では統一基準群の例外規定のポイントについて述べる[3]．

- 原則は計画準備段階で策定した手順に従い，実際のインシデント発生時に対応する
- 計画準備段階での手順がインシデントの実情に沿わないときには，手順以外の方法で対応できるための手続きを予め準備し講じる
- また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
- これらの例外処置をも管理する策を講じる
- 例外措置と罰則とをセットにする

なお NISC では，例外措置を効率よく進めるために手続きの流れ（図１参照）や様式も定めている[10]．

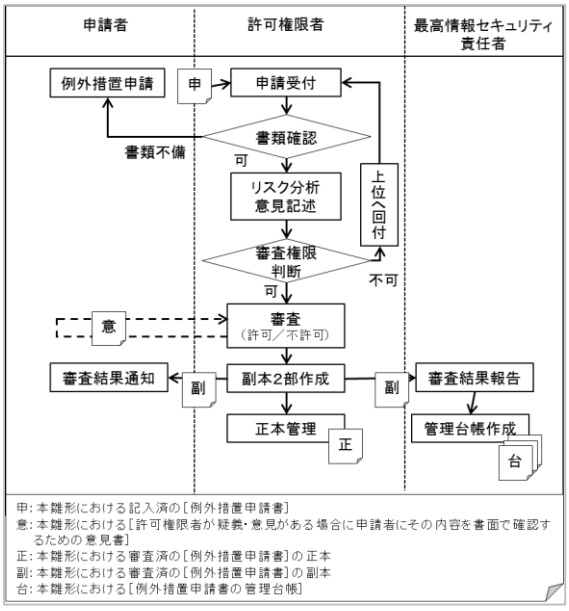

図1 例外措置業務フロー[10]

2.4. ＩＳＭＳ(Information Security Management System)での例外規定

情報セキュリティマネジメントシステム（以下，ISMS）は，組織の意志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，及び情報セキュリティのリスクを低減するためのコントロール（管理策）が適切に維持・管理されていることを目的とする[11][12]．

ISMS を実践するための管理策に関する詳細なガイドとして，ISO/IEC27002:2013 がある．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及び管理策を定めている[11]．さらに「12.1 運用の手順及び責任」に「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」を記述しており，「12.1.1」「12.1.2」ではそれぞれ操作手順・変更管理が記載されている[12]．

操作手順の e）f），ならびに変更管理の g）h）に例外への対応について例外規定の記載がある[13][14]．例外措置を認める場合は，例外規定として明確に規定等に定めるとともに，運用を変更する場合には変更管理を徹底するとしている．すなわち，今回改正された ISO/IEC27002:2013 にもとづき ISMS 認証への新規もしくは更新認定を希望する組織は，必要があるときには例外規定の策定・実施が求められていることになる．

一方，ISMS の管理策は必須ではないことから，ISMS では積極的に例外規定による運用を奨励しているわけではない．2013 年改訂では当該記載自体が，実は“例外的”な内容として残されたものである[14]．

なお，ISO/IEC27002:2013 では個別具体的な指示や例示を記載しているわけではない．より具体的な規定策定や措置手順については各組織の判断に委ねられている．これらの規定でカバーできない場合のインシデント・リスクなどについてのみ例外を実施する．したがって，組織が例外規定を策定する場合には，組織の説明責任が問われていることになる．

2.5. 海外での例外規定

海外における例外処理について日本企業の米国法人での例を述べる．なお本事例については一般に公開されないため，考え方についてヒアリング調査を実施した．その内容を紹介する．

ヒアリングした組織では，例外処理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．その主な項目と概要を例として表１に示す．表１からは，2.3 節に述べた統一基準群と同様，通常規定では対処が難しい事象に対して例外規定を策定していることが分かる．この特徴を２点述べる．

１つは，逸脱と例外規定を明確に区別して定義している点である．これにより例外規定によって発生するリスクを把握することができる．

もう１つは，例外規定を策定するにあたり，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いている点である．ここでは「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）」の考えによる．すなわち例外規定を適用するのであれば，申請した部門や個人に対して説明責任を負わせることで，例外措置によって起こりうるリスクを理解させ，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．

表 1　例外処理におけるガイドラインと手順（例）

1	序論	省略
2	目的	「セキュリティ方針または標準」（以下、規定等）からの逸脱程度を例外規定として策定 例外措置を承認するための上申手続きの策定
3	範囲	社内全体のおける規定等へのコンプライアンス違反事象
4	定義	「逸脱」「例外」「申請者」「欠陥行為を補完するコントロール」を定義 このうち、「逸脱」「例外」は次の通り 逸脱：規定等の中の特定コントロールに対するコンプライアンス違反の例。 それは情報資産への通常リスクより高い事が想定される。 例外：適切な承認を受けて規定化された逸脱を言う。 通常ならば規定等に対する違反行為だが、 特別のアクティビティまたはプロセスが許可される。
5	ガイドライン	例外は設備面・運用面において事前に規定・承認が必要 例外は社内全組織に効力 例外は現場からの要請を基に規定・承認される 例外は定期的はレビューが必要 例外は常に参照できるよう管理 例外の運用は現場に責任の役割を担う
6	責任	リスク分析は、情報セキュリティ部門が担う。 情報セキュリティ部門はリスクを適切に識別し、例外規定に必要な条件をリスト化する。 例外規定の今後の可否や拡張への検討にはレビューが必要。 例外規定が拡張される場合は、当該規定を策定した担当者の承認が必要。
7	参照（逸脱の処理）	情報セキュリティの例外規定には逸脱とリスクに関して明記しなくてはならない。 申請者は現場での職務を遂行するために要求する逸脱を明記しなくてはならない。 申請者はそれをもとに例外措置を要求できる。 逸脱に関する情報は、以下を明記しなければならない: ・逸脱の内容説明 ・逸脱が関連する規程等の参照箇所 ・施設、人員またはシステム等で確認されるリスクの直接的な影響 ・現場で逸脱が適切とされる理由 ・逸脱と関連してリスクを制限する補償コントロールまたは要因 ・逸脱を報告する者の名前
8	例外管理プロセス	・逸脱内容の明文化 ・リスクを最小化するための必要な補償コントロール等の識別 ・認可プロセスを調整する ・例外規定の周期的なレビュー　など
9	エスカレーション	現場での業務遂行において、規定等への逸脱が適切とされるならば、例外規定を策定しなければならない。 現場を横断的に確認されたリスクに対する例外規定を策定する場合は、必要に応じてリスクの影響を受ける現場からの認可を得る。 責任者は少なくとも例外措置による危険性を詳細に現場に伝達しし、リスクの影響を受ける現場から、例外規定の承認を得る。

2.6.　民間組織における現状

NISC の統一基準群における例外規定は，官公庁以外では外資系企業や日本の大手企業の約 20 社に同じモデルを導入しているとされている[6].

また，金融情報システムセンター（FISC：The Center for Financial Industry Information Systems）発行の金融機関等におけるセキュリティポリシー策定のための手引書[15][16]も同様のため，一部の金融機関については日本銀行を含め導入しているものと考えられる.

2.7.　先行事例調査からの考察

本章では，いくつかの先行事例を通じて，情報セキュリティポリシーに盛り込まれるべき，情報セキュリティにかかる例外規定について考察した.

いずれにおいても，例外規定を予め設定することで，組織ガバナンス・マネジメントに役立つということが分かった．一方で，具体的にどの程度まで例外規定が普及しているかについては不明な点も多い．特に民間組織において金融機関など一部では統一基準群を参考にしているものの，どの程度規定され実施しているかはこれまで不明であった．官公庁・自治体においても政府機関向けに作られた統一基準群を，どのように適用しているのかについて調査が必要である.

例外規定の普及の実態と，具体的な例外措置の効果を調べる手段を探るべく，いくつかの仮定を設定し調査することにした.

3.　例外規定を分析するにあたっての仮定

3.1.　例外規定の定義と範囲

“例外”という用語は広範囲の内容を含んでいるので，本稿での例外規定の定義と範囲を以下に述べる.

通常規定から外れることを「逸脱（deviation）」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（exceptional rules）」として定義する.

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[3].

また，日常業務で想定できるものであったとしても，2.1 節で述べたＢＹＯＤのケースのように[7]，措置の大変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．すなわち，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，例外規定を用いて措置を講じることになる．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.

本稿での例外規定を適用する範囲は，日常業務における例外規定の策定と例外措置の運用を主として取り扱うことにする.

3.2.　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 3.1 節の定義と範囲をもとに，表２に示す８つの仮定をたてた.

このうち，仮定１から仮定６については，例外規定の実態について，2.3 節の“例外規定のポイント”をもとに設定した．具体的には NISC の統一基準群をもとにして設定した．これは，統一基準群が例外措置を具体的に実施するための手順やひな形が提供している点，組織ごとにカスタマイズすることを指示している点，ならびに罰則がセットされている点による．またこれらの点が組織によって実施されているか調査することで，統一基準群の必要性が明らかになるからである（図１および文献４参照）.

なお本稿では，仮定を検証する手段として，後述のアンケート調査を利用している.

表２　組織の例外規定に関する仮定

（仮定 1）	例外規定の普及は分野ごとにばらつきがあるが，少なくとも官公庁では，実際に業務として例外措置を行っている
（仮定 2）	内部規定にない例外措置をとるとき，緊急性を要する場合は，直接経営判断を優先するだけでなく，現場責任者の判断でも措置ができるようになっている
（仮定 3）	新規に例外規定を策定する場合，これまでの事例や外部からのものを参考にしている
（仮定 4）	例外規定の策定は，情報システム部門など中央で統括しながら作成するのか，あるいは各組織の権限内で作成するのかは，組織によって違いがある
（仮定 5）	例外規定の業務内容の見直しは短い期間で定期的に行われる
（仮定 6）	例外規定では例外措置のための実施手順を記載し，特に罰則とセットにしている
（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か

4.　アンケート調査について

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[6]．

4.1. アンケート調査実施内容（全体）

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[17][18]．

4.2. アンケート設問

3.1 節の表 1 の仮定に基づいて設問 14 から設問 23 を作成した．これを表 3 に示す．なお，設問 16 は仮定 7 に対する分析（7 章），また設問 23 は仮定 8 に対応する分析（6 章）に用い，それ以外の設問は仮定 1 から仮定 6 にかかる単純集計（一部クロス分析）用に使用している[17]．

表 3　アンケート設問一覧

[設問 14]	情報セキュリティに関わる内部規定全般において「例外規定」の項目の有無
[設問 15]	例外規定が明記されていない事象（障害，事故・事件，災害など）に対して，一時的に例外措置した経験の有無
[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 17]	内部規定に例外規定がない事象で緊急を要する事態での一時的措置に，最初にとる手段
[設問 18]	新規の例外規定を策定する場合の参考元
[設問 19]	例外規定の策定と管理の事務処理する主体部門
[設問 20]	例外規定が，組織全体での統一規定か，現場組織ごとの規定か
[設問 21]	例外規定に記載された例外措置の手続き内容
[設問 22]	例外規定の見直し頻度
[設問 23]	具体的な効果についての主観的評価

5. 例外規定策定の現状

5.1. アンケート調査の結果

本章では，例外規定策定と例外措置実施の現状について，特に特徴がみられた仮定 1，仮定 4 および仮定 5 を取り上げ，アンケート調査の結果を示す．なお，全ての仮定に対する分析や考察は文献[1]に述べている．

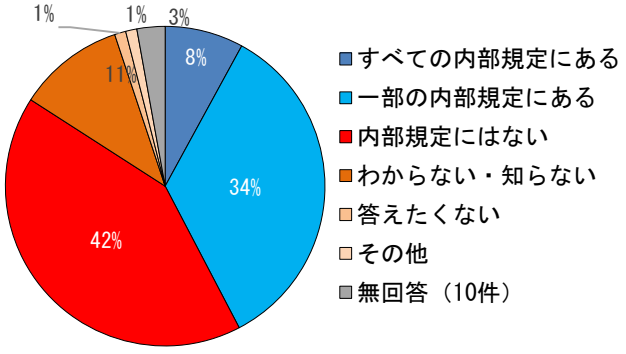

図 2　情報セキュリティに関わる内部規定全般において「例外規定」の項目の有無（択一，N=352）

5.1.1. 例外規定の有無（仮定 1）

本項では，仮定 1「例外規定の普及は分野ごとにばらつきがあるが，少なくとも官公庁では，実際に業務として例外措置を行っている」について考察する．

設問 14 の単純集計結果を図 2 に示す．本設問では内部規定全般において「例外規定」の項目の有無をたずねた．結果は，「すべて例外規定に内部規定にある」「一部例外規定に内部規定にある」割合と，「内部規定にない」割合が同じ（42%）であった．

次に，業種別[17][18]にクロス分析し，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）」の結果を図 3 に示す．図 3 より「情報通信業」と「サービス業」では 50%が，「すべての内部規定にある」もしくは「一部の例外規定に内部規定にある」ことが分かる．

一方，「公務（政府・自治体）」の場合は「内部規定にはない」が 24%あり，「大学」では半数以上（53%）におよんでいる．

これらの結果から，仮定 1 については，例外規定について策定の有無が同程度であることから，例外規定が一般的な方策となっているとは考えられない．一方「情報通信業」・「サービス業」では半数程度が策定している傾向にあり，これらの業界ではＩＣＴの依存度が高く技術進歩の影響をうけるため，例外規定が他の業界と比べて必要となっていると考えられる．

一方，政府・自治体では，統一基準群によって例外規定の策定を推進していることから，政府・自治体及び関連組織への普及が今後の課題になる．

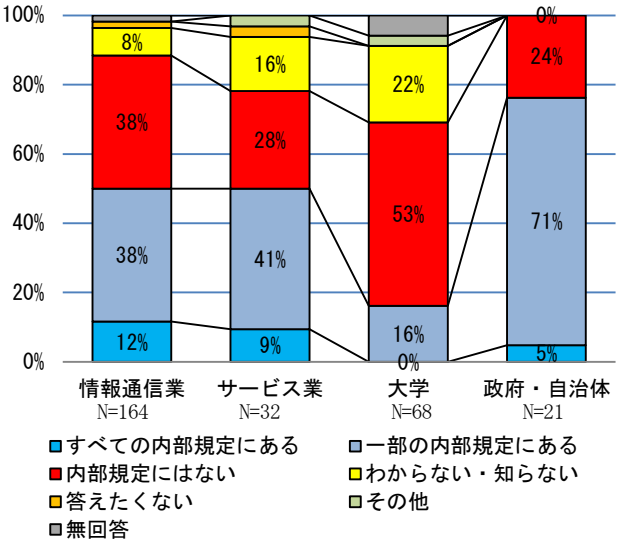

図 3　情報セキュリティに関わる内部規定全般での「例外規定」の項目の有無（業種別，択一）

5.1.2. 例外規定の策定部門（仮定 4）

本項では仮定 4「例外規定の策定は，情報システム部門など中央で統括しながら作成するのか，あるいは各組織の権限内で作成するのかは，組織によって違いがある」について考察する．

仮定 4 に対応する設問 20 の結果を図 4 に示す．本設問は，例外規定は組織全体での統一された内部規定のみか，それとも現場組織ごとにも規定されているかをたずねた．

図４から，例外規定は「統一管理基準のみ」が半数を越え（55%），「現場組織ごと」と「統一基準群と現場組織の両方」とを合わせた割合（13%）と大きく差があることが分かった．

次に，設問 19 の結果を図５に示す．本設問は，例外規定を策定するにあたり，規程の策定と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．図５からは，例外規定を策定する組織は「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」の順で多く，「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」も含めると，情報系部門が圧倒的に占めていることがわかる．

すなわち，仮定４に対応する「設問 20」ならびに「設問 19」からは，多くの組織が例外規定を統一管理基準のみで策定・運用していることがわかる．例外規定については，策定や運用にあたって専門的知識や経験などを要するので，情報セキュリティや情報システムなどの専門部門で策定し，運用・管理まで手掛けざるを得ない現状であることがわかる．

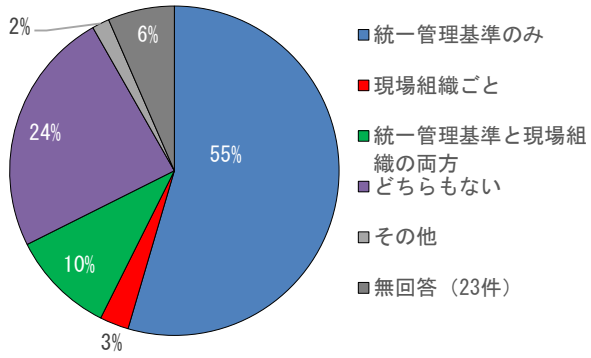

図４　例外規定は組織全体で統一されたものか，現場組織ごとにも規定されたものか（択一，N=352）

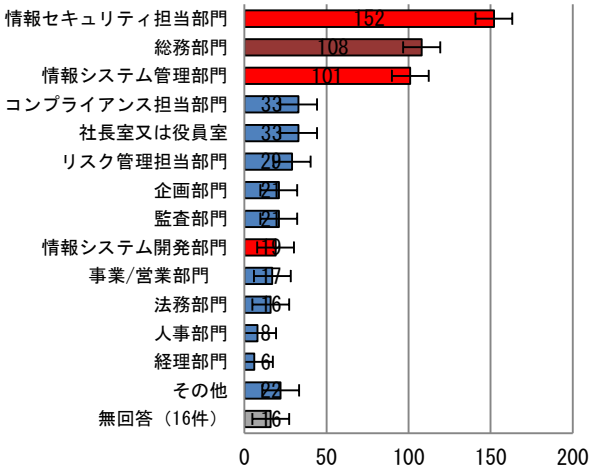

図５　例外規定を策定するにあたり，規程の策定と管理の事務処理をする主体部門
(択一，グラフ内の数値は回答数)

5.1.3.　例外規定の業務の見直し期間（仮定５）

本項では仮定５「例外規定の業務内容の見直しは短い期間で定期的に行われる」について考察する．

仮定５に対応する「設問 22」の結果を図６に示す．本設問は，例外規定の見直しの頻度についてたずねた．図６からは，例外規定の見直し頻度は，「随時」見直ししている組織が 40%と多い．

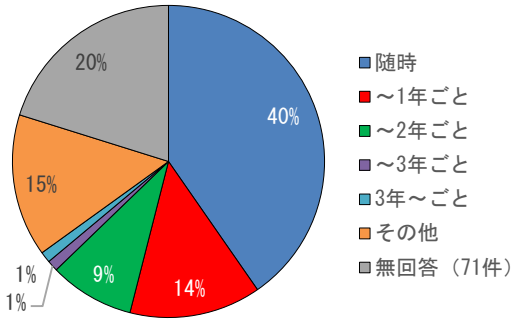

図６　例外規定の見直し頻度（択一，N=352）

また，「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．

以上のことから，仮定５に対して，組織は例外規定について，見直しは随時行うものの，定期的ではなく必要に応じて対処しているところが多いことが分かる．

一方その他（15%）や未回答（20%）と多いことから，見直しをしていない組織が多いと解釈することができる．

5.2.　例外規定策定の現状からの考察

以上，5.1 節のアンケート分析の考察から組織の特徴は以下のようにまとめられる．

5.2.1.　専門部門への集中

5.1.2 項の結果から，部門ごとにカスタマイズして策定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策定・措置がなされている．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な部門が多く，現場の策定が少ないことからも，策定・運用・管理が専門部門に集中している．

5.2.2.　例外措置体制がとれない組織

5.1.3 項の結果からは，

“実際に例外措置をすることが少ない”

“見直し頻度もその都度”

“例外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[1]．

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都度対応し，その後，必要に応じて規定として策定・見直ししている．

都度の対応では，緊急性も求められ，一時しのぎで例外措置を行うことになる．将来，同じ事象が起きても組織が学習していないため，同様な事件や事故が発生すると，再度一時しのぎの例外措置を繰り返すことになる．

5.2.3.　策定／未策定の二極化

5.1.1 項の結果からは，情報セキュリティに関する内部規定への例外措置の規定化については，策定している組織と未策定の組織とで二極化している．このことから今後，例外措置を策定していない組織に対して，例外規定の普及が必要と考える．

以上，例外規定が，組織の内部規定等での情報セキュリティポリシーに規定され，NISC の統一基準群にて普及推進されていることから，例外措置の実施状況は，組織の情報セキュリティのガバナンス及びマネジメントの実態を知る手がかりの１つになることが分かった．ただし，例外規定の策定が一部の組織にとどまっており，ガバナンスやマネジメントが十分でない組織が多いことも確認できた．

6. 例外規定への主観評価

6.1. 概要

本章では，例外措置が組織に与える具体的な効果について述べる．表２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．

設問では，過去のアンケート調査[17]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（迅速に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，それぞれに対して主観的に満足・安心かどうかを６段階の回答選択肢として評価する形式とした（図７凡例参照）[2]．

単純集計結果を図７に示す．図７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“とても満足・安全”・“満足・安全”ならびに“どちらかといえば満足・安全”の３つの合計が 50%から 60%の範囲であることが分かる．

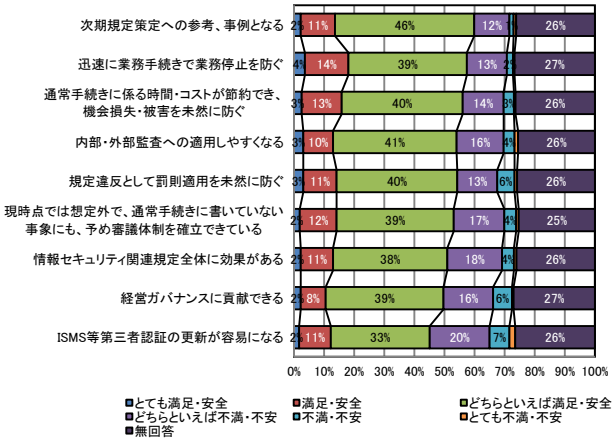

図７　具体的な目的や効果に対する主観的評価
（択一，N=352）

6.2. 二重刺激劣化尺度法による主観評価分析

図７の結果をもとに二重刺激劣化尺度法[19]を用いて主観評価分析を行った[2]．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情報セキュリティポリシーなどへの満足度を評価した．なおアンケート設問 23 の６段階回答選択肢と二重刺激劣化尺度法の５段階評価点との互換性をとり（表４参照），設問肢ごとの累積評点を求めた上で分析を行った（図８参照）．

表４　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

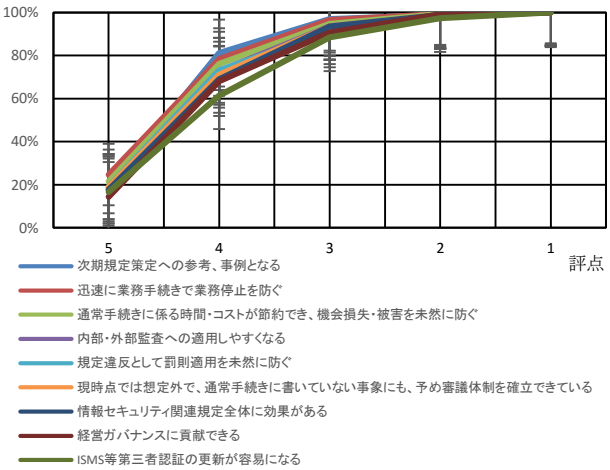

図８　設問肢別累積評点

図８をもとに評点別累積値を設問肢ごとに分析した結果，設問肢間の相関が強く，それぞれの傾向に差がないことがわかった．そこで図８の設問肢の平均を用いて許容限を求めた．その結果をグラフにしたものを図９に示す．

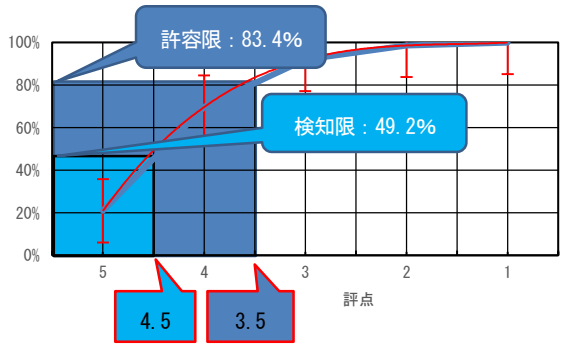

図９　主観評価分析結果

図９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．

これからは，８割以上が自組織の情報セキュリティポリシーにおける例外規定に対して「満足・安心」とできると答えている．

以上，主観評価を用い数値化（定量化）することで，組織の満足度を知ることができる．例外規定を設定するとき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）対応をどうするかの目安にできる．

7. 通常規定からの逸脱と例外規定について

7.1. 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，２章の事例で紹介したとおり，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．そこで表２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 では例外措置の具体事例を設問肢とし，それぞれに対し「通常規定に策定」「例外規定に策定」あるいは「規定せずに違反行為」として措置しているかについてたずねた．単純集計結果を図 10 に示す[2]．

図 10 からは，「外部インターネットの利用」「可搬型メディアの利用」項目に対し，「通常措置としている」「例外規定に従い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 10 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．

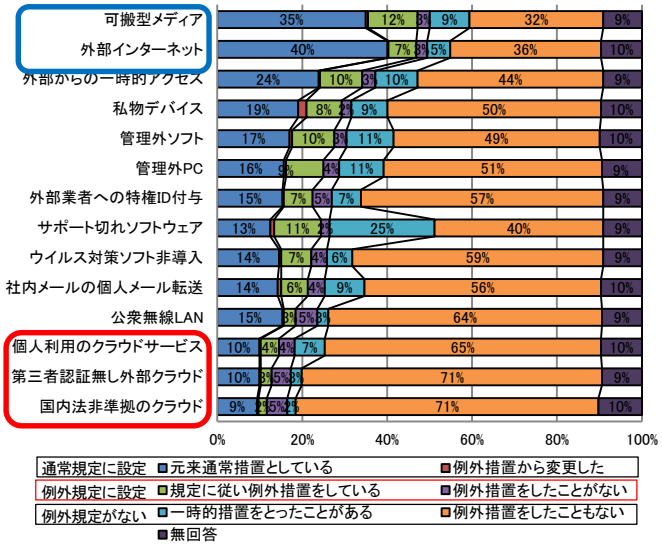

図 10　具体的な業務上の事象における例外規定の有無（択一，N=352）

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点．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点．すなわち規定が伴わない現場判断での利用である．2.1 節で述べたＢＹＯＤのケースと同様[7]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している上で，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，措置手続きをとるようにしていることが分かる．

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．

なお「サポート切れのソフトウエアの利用」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．通常規定あるい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エア会社の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によるもので，今回だけの特殊性と考える．しかし今後もＯＳサポート切れへの対応は数年おきに起こりうるため，5.1.3 項に述べたように，各組織が今後の対応を例外規定とするべきか，あるいは通常規定とするべきか，今後の動向を注視していく必要がある．

7.2. 通常規定と例外規定との策定状況における考察

図 10 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 11 に示す．

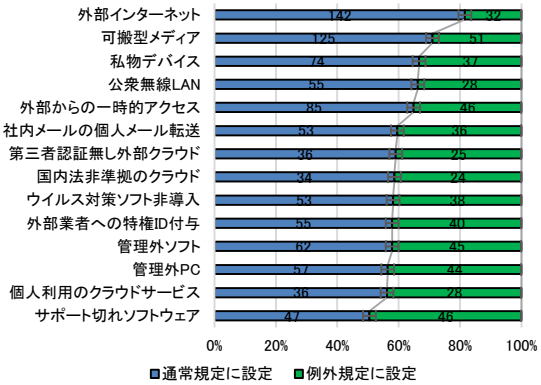

図 11　通常規定と例外規定との比率（択一，グラフ内の数値は回答数）

図 11 より以下のことが考えられる．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．

7.2 節で述べたとおり「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エアの利用」については同程度の比率であり，7.1 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．

8. まとめ

本稿では主に組織ガバナンスとマネジメントの観点から,例外規定の策定と例外措置の取扱いやその効果についてを,アンケート調査を実施し,その分析結果から実態を明らかにした.

アンケート調査を通じて,組織における例外規定策定の現状から,情報セキュリティにおける組織ガバナンスの実態を知ることができることを示した.

例外規定の策定は,組織によって導入程度が異なっており,全体では例外規定の策定は十分に進んでおらず,例外措置が活用されているとはいえないことも示した.一方で,ＩＣＴへの依存度の高い情報通信業やサービス業では半数に活用され,また政府や自治体では統一基準群の例外規定を推進していることから,今後例外規定を策定する組織が増えていくことが分かった.

さらに例外規定を策定し管理しているのは,情報システム・情報セキュリティを専門とする情報系部門に集中していることも明らかになった.したがって情報セキュリティに関する規定が全ての組織において必須施策のひとつである昨今では,各組織それぞれに適用した例外規定の導入に向けて検討していく必要がある.

また,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の重要性を述べた.

なお残された課題として,

- 統一基準群を例に,社会全体や分野毎における例外規定の具体的な措置内容の共有化
- 例外規定の期待効果を明確に示すことができる指標など,定量評価の提示とその検証方法の発掘
- 例外規定の策定普及に向けた,提言の取りまとめ

などがあげられる.

例外措置は各組織で実際に運用しなければ,その効果の程度をはかることは難しい.例外措置が全ての組織で利活用できるようにするためには,上記の課題への十分な検討が今後必要であり,例外規定が盛り込まれた情報セキュリティポリシーの普及を図っていくことが求められる.

謝辞

本稿を執筆するのあたり,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] 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] 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

[3] 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/2014-11-29 b-enPit.pdf>, (参照 2016-04-08)

[4] 日立グループ:情報セキュリティ報告書, 日立製作所,2014 csr/csr_images/securityreport.pdf〉(参照 2016-04-08)

[5] 経済産業省：平成 27 年度情報セキュリティ監査企業台帳,経済産業省ホームページ（オンライン）, 入手先< http//www.meti.go.jp/policy/netsecurity/ is-kansa/)（参照 2016-04-08)

[6] 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

[7] 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

[8] 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〉(参照 2016-04-08)

[9] 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〉(参照 2016-04-08)

[10] 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〉(参照 2016-04-08)

[11] 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

[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

[14] 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

[15] 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

[16] 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

[17] 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

[18] 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〉(参照 2016-04-08)

[19] ITU-R 勧告,”Methodology for the subjective assessment of the quality of television pictures”, BT500-11, 2006