博 士 論 文

「情報セキュリティポリシーに関わる例外規程の必要性と限界」

Yasuhiro MURASAKI
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
情報セキュリティ専攻

2019 年 9 月

目次

初出一覧

【学会査読論文】

(1) 村﨑康博, 原田要之助, “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)

(2) 村﨑康博, 原田要之助, “情報セキュリティポリシーにおける例外措置”, 情処論文誌, Vol.58, No.12, pp,1856-1862(2017)

(3) 村﨑康博, 原田要之助, “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～”, システム監査, Vol.31, No.1, pp140-149 (2018)

(4) Murasaki , Y. , Harada , Y. , “Exceptional Rules Concerning the Information Security Policy”, Twenty-Second Pacific Asia Conference on Information Systems(PACIS2018), Doctoral Consortium, pp101-107 (2018)

【学会研究会発表論文】

(5) 村﨑康博, 原田要之助, “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)

(6) 村﨑康博, 原田要之助, “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)

(7) 村﨑康博, 原田要之助, “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)

(8) 村﨑康博, 原田要之助, “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)

(9) 村﨑康博, 稲葉緑, 原田要之助, “情報セキュリティポリシーにおける例外措置の利用者による実施阻害要因および対応に関する一考察”, 情報処理学会研究報告, Vol.2018-SPT-30, No.1 (2018)

【学会研究大会予稿】

(10) 村﨑康博, 原田要之助, “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”, 電子情報通信学会総合大会, A-12-3 (2016)
(11) 村﨑康博, 松井俊浩, 原田要之助, “情報セキュリティポリシーにおける例外措置の技術的対策との関わり”, 電子情報通信学会総合大会, (2019)
(12) 村﨑康博, “情報セキュリティポリシーに関わる例外規程の必要性と限界”, 第 18 回情報科学技術フォーラム講演予稿集, N-014 (2019) <FIT2019 奨励賞受賞>

1. 研究の背景・動機・目的

本論文の第 1 章として，まず情報セキュリティポリシーに関わる例外規程の研究をはじめた時代背景と個人的動機，ならびに研究の目的について述べる．

本テーマの研究を始める以前は，例外措置はいわば「良薬」だと認識していた（例外措置の定義は 2.1 節参照）．例外は都合のよいものである．原則に当てはまらない事象に対して，兎にも角にも例外として一時措置を講じる．それで結果として業務が継続できたのであれば，例外はまさに良薬であった．

しかし諺にもあるように，良薬であるならば口に苦い．実際，例外にはそれを承認する者（当時の筆者）にとっても，申請する者（現在の筆者）にとっても，より多くのリスクを受容しなくてはならず，承認事由を上長に説明する際になんとも言えないほろ苦さを実感していた．そもそもどうして例外が存在して，それが必要なのか？その一方でなぜ例外は面倒なのか？そもそも例外とは何なのか？

ともかくいずれにせよ情報セキュリティに携わる業務には例外を取り扱うことが求められる．故に例外について正しく理解する必要があると実感した．

本論文の冒頭にあたり，まず例外そのものについて述べる．

1.1　時代背景と「例外」の必要性

そもそも情報セキュリティの業務において例外は必要なのだろうか．例外の必要性は，実は，現代の複層的な業務改革・組織運営が直面している「不確実性」[1)]に深く関わっている．

本論文の執筆を始めた 2018 年は，安倍内閣が目玉政策の一つとして「働き方改革」を掲げ，ワーク・ライフ・バランスの見直し，特に総労働時間の短縮と，それを可能にする仕事の効率化が注目された年であった[2)]．この取り組みは，中央官庁や自治体はもとより，一般の民間企業にも浸透し，根本的な業務内容の見直しや意識改革がせまられている．

報道などでは「（医療や介護現場の）働き過ぎ」や「ブラック企業」などの負の面が注目されがちであるが，本来の目的は後段の「効率化」の方であり，しかも

1) 経営学が「不確実性」に初めて正面から向き合ったのは，1977 年にガルブレイスが BBC の番組と書籍で公表した “The Age of Uncertainty” であったと思われる．他方，経済学では早くも 1921 年にナイトが risk と uncertainty を明確に区分し，前者を予測可能なもの，後者を不可能なものとして上で，現代企業の利益は前者ではなく後者から生まれるとした（Frank H. Knight(1921) “Risk, Uncertainty and Profit”, Houghton Mifflin Company）．

2) 厚生労働省“「働き方改革」の実現に向けて”, 2018, (オンライン). (オンライン). https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000148322.html. (アクセス日: 2019 年 6 月 10 日).

「省力化」よりも「創造的なイノベーション」が期待されている. これをなくして政府が同時に提唱する「Society 5.0」という, 欧米や中国に対峙できる技術力の確保と, それによる優位なビジネス展開はあり得ない.「イノベーション」はもはや企業や官庁を問わずあらゆる組織の責任者に求められているのである[3] .

その一方で人がコントロールできない事象が存在し, その発生確率さえ予測できないため[4], このような環境でビジネスを展開せざるを得ないならば, 予め立てる計画も事象の変化に柔軟に対応できるものでなければならない. そのためこれまでの常識にとらわれない仕事の進め方や, ものの考え方が求められる[5]. これは社会が要請する「働き方改革」である.

この「不確実性」を伴う環境の一つの例が, 情報セキュリティやサイバーセキュリティと呼ばれる領域である. 昨今のマルウエアやサイバー攻撃は, 従来の想定を超えるものであり, これに対応する対策も技術と運用の両面で広がらざるを得ない.

現代の組織は, より複雑性を増し, 過去の知識で対応できないような不確実性が増大しているといえる. したがってより複雑性の増した現代の組織では, 過去の知見にとらわれない, よりフレキシブルな対応が出来るような仕組みが求められている. これの 1 つに「例外」があると考える. 特に情報セキュリティ施策は不確実性を伴うものであるため, 想定が難しい問題や事象に対しては「例外」を考えざるを得ない. すなわち例外が必要なのである.

1.2 例外の煩雑性

次に, 例外の取り扱いは少なからず煩雑である. それはなぜか.

一般的に, 例外に対して何らかの措置[6]をする場合は, 事象の一つ一つに対

3) 内閣府,“Society5.0”,内閣府, (オンライン).https://www8.cao.go.jp/cstp/society5_0/index.html. (アクセス日: 2019 年 6 月 10 日).

4) なお最近の経営学の書物では, 東日本大震災の影響を受けたためか, “Unexpected”(想定外)と同一視するものもある

5) 沼上幹,“組織戦略の考え方ー 企業経営の健全性のためにー”,ちくま新書, 2003 年.

6) 「措置」については, 広辞苑(第七版)では「とりはからって始末をつけること。処置。」, 大辞林(第三版)では「うまくとりはからって始末すること。処置。」とされている. さらに法律用語での「措置」と「処置」の違いについては, 法律用語辞典(第4版, 有斐閣)や法令用語辞典(第 10 次改訂版, 学陽書房)などから「ある問題に対する対策, 施策等その問題を処理するためにとられるもろもろの手段をまとめていう場合が多い.「処置」が個々の事項の始末について用いられるのに対し,「措置」は, これを総体として表示し, 又はその結末よりも手続きの面に着眼して用いられることが多い」とされている. web 上での解説によると, 物事を完結させるかどうか, 事前に対処するかどうかにあるとされる. 措置は必要な手続きにより物事を始めから最後まで手続きを行い, また事前に対処するのに対し, 処置はその場の状況や判断で対処し, 物事が起こってから対処するのに使われるとされる. (“Investigate Blog”, https://g2015graman.top/archives/2856.html あるいは“国語力アップで人生豊かに”, https://kokugoryokuup.com/measure-treatment/) 本論文では用語の統一するため, これより「措置」という用語をもって, 後に述べる組織内においての不確実性を伴う情報セキュリティ分野への施策を考え

して異なる対応を考えなくてはならないため，「判断」という作業が伴う．ここで，企業や役所などを例に考えてみる．「判断」の出発点は，例外の申請を受け付ける窓口担当者にあるが，決定にあたって通常は上司の承認が必要になる．場合によっては，「判断」が，さらに上位者の承認というヒエラルキーを上っていくことになる．したがって「例外」が頻発すれば，中間管理者や経営層の業務を圧迫することになりかねない．

そこで，この例外にかかる措置を，ある程度ルール化することが有効となる．すなわち経営層にまで上がる例外の承認要件と手続きの多くを，明文化・体系化して権限を中間管理者に委譲し，中間管理者で対応を完結させればよい．判断を要する例外に限って，前述のヒエラルキーを上がって経営層が承認することにする．また，類似の事例が多発するようなら，それらの措置もまた明文化して，ルーチン業務として処理できるようにする．こうした組織設計により，経営層の負担を軽減するとともに，判断ミスを減らすこともできる．さらには例外に関わる措置の一部を汎用的にルール化し，明文化することで例外に関わる措置への承認・実施への効率化が期待できる．

なお，情報セキュリティが経営上の重要事項となった現代では，組織において実施する情報セキュリティ対策の指針を，全組織的に「情報セキュリティポリシー」[7]として策定し，内部規程としても活用するのが一般的とされている．したがって，情報セキュリティポリシーにおいても例外に関する規程を設けることが避けられない．

しかし他方で，「例外はあくまでも例外である」のが一般的だと考える．前述のように例外が頻発して原則に取って代わることがあることは否定できないが，それが定常化すれば原則の妥当性そのものが疑われることになる．したがって例外には何らかの限界があり，安易に内部規程と同等にルール化することは避けるべきでもある．故に判断を伴う点，原則と例外を区別して取り扱わなくてならない点などが，例外を扱う上で煩雑にしている原因であると推定する．

1.3 「例外」という概念

では，そもそも例外とは何なのか．

ていきたい．

7) 情報セキュリティポリシーとは，例えば，総務省「情報セキュリティポリシーの概要と目的」によれば，企業や組織において実施する情報セキュリティ対策の方針や行動指針のことを指す．
「情報セキュリティポリシーには，社内規定といった組織全体のルールから，どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方，情報セキュリティを確保するための体制，運用規定，基本方針，対策基準などを具体的に記載するのが一般的です」．

本論文で使用する例外に関わる用語や概念の定義は次章で行なうこととして，ここでは「例外」という一般的な概念について，基本的な意味を述べておく．

「例外」という言葉は，広辞苑（第七版）によれば「通例の原則にあてはまっていないこと，または一般の原則の適用を受けないこと」である．また大辞林（第三版）では「普通の例からはずれていること．原則にあてはまらないこと．また，そういうもの」とされ，いずれも「原則」という言葉と対で表されることが多い．また我々が「原則として」という語を付してルールや規程を伝える場合は，相手に対して「例外がある」ということを暗に伝えていることにもなる．すなわち「例外がある」ということは，言い換えると「原則から逸脱する」と解釈できる．

通常我々は，仕事や学業，そしてプライベートにおいて，ルールやマナーを守って生活している．ルールには一般に原則と例外が存在するので，例外に対して適切に対応し措置することで，原則による規律を維持している．これを原則と例外の相互補完という．しかしながら世の中の事象には，予め原則として措置できないものの例外としてなら措置できるもの，あるいは想定外の事象のため例外としても予め措置できないものとがある．前者では原則を継続して維持することができるが，後者ではルールや規程そのものを抜本的に見直すことの契機となり，原則と例外が逆転する場合さえもある．これを原則と例外の代替関係という．

すなわち例外というものは，相互補完および代替関係といった原則と相互に関係しながら，セットで作用することがわかる．

例えば，予め例外に関する規程が策定されている場合には，例外申請を審査する側としてそれに沿って申請を処理し，適切に手続きを進めることで，業務を遂行することが可能であると考える．一方，例外が定められていない場合には，どのように措置すべきか，あるいは申請そのものを却下すべきか（取り下げてもらうべきか）を即座に判断できず，日常業務に支障をきたすおそれがある．

情報セキュリティポリシーの策定と実施においては，日常業務のルールやマナーの場合以上に，例外をなるべく広範囲に取り込んでいかざるを得ない．なぜなら，情報セキュリティポリシーに基づく組織の業務は汎用的にルール化されたものであり，かつ即応性が求められることから，それに付随する例外の適用範囲も，情報セキュリティポリシーを網羅するように広くとる必要があるからである．

また情報セキュリティの場合には，災害やセキュリティ攻撃といった非常時における例外の適用だけでなく，情報技術の著しい技術進歩や一般への急速な普及などにより，平常時における例外の適用が不可欠となっている．しかし起こり得るすべての情報セキュリティインシデント（以下，インシデント）やリスクを事前に把握し，それに対する措置を事前に策定し実施することは不可能である．

また前述のとおり例外がもともと原則に対する逸脱であることは避けられない．そこで内部規程から逸脱している行動に関して，どの程度まで容認し，またそれを容認することで新たに生ずるリスクが，容認するメリットを上回らないか，という判断が求められてくるのである．

1.4　例外に関する基本例

例外について論じていくに当たり，具体的なイメージを想起しやすいよう，その基本例（プロトタイプ）を提示する．ここでは組織における USB フラッシュメモリー（以下，USB メモリ）等可搬型メディアの業務利用と，第三者認証のない外部クラウドの利用との二つのケースについて管理策と例外の必要性を取り上げる．

1.4.1 ケース1：USB メモリ管理策

昨今の個人情報・秘密情報漏えいに関する事件・事故の主要な原因に，当該情報の入った USB メモリを社外へ持ち出すことが挙げられている[8]．そこで組織では，対策として組織内ルールに USB メモリの持ち出しについて，USB メモリの全面禁止や利用制限を策定することが多い[9]．その一方で，組織の中には，取引先から図面データの受け渡しにおいて USB メモリによるデータ交換が要請されることも多い．このケースを例に考える（図 1-1 参照）．

ある組織で「USB メモリは全面使用禁止」を内部規程として策定していたとする．これが原則に該当する．この場合，組織が自社の規則通り USB メモリ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る．あるいは取引先にて印刷したものを受け取って，自組織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．一方，無条件で USB メモリ利用の規則を破ってデータを受領した場合，この USB メモリがマルウエアに感染していたならば，組織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 メモリ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 メモリの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 USB メモリ」を使用するといった要件が，内部規程から逸脱している事象に対して，例外を規程として策定する場合の許容要件（つまり許容範囲）となる．

---

8) 情報処理推進機構, “内部不正による情報セキュリティインシデント実態調査”, (オンライン). https://www.ipa.go.jp/files/000051140.pdf. (アクセス日: 2019 年 6 月 10 日).

9) 日経 NETWORK, “企業セキュリティ調査 Part2USB メモリ編”, 日経 NETWORK, 第 7 月号, pp. pp.42-44, 2012

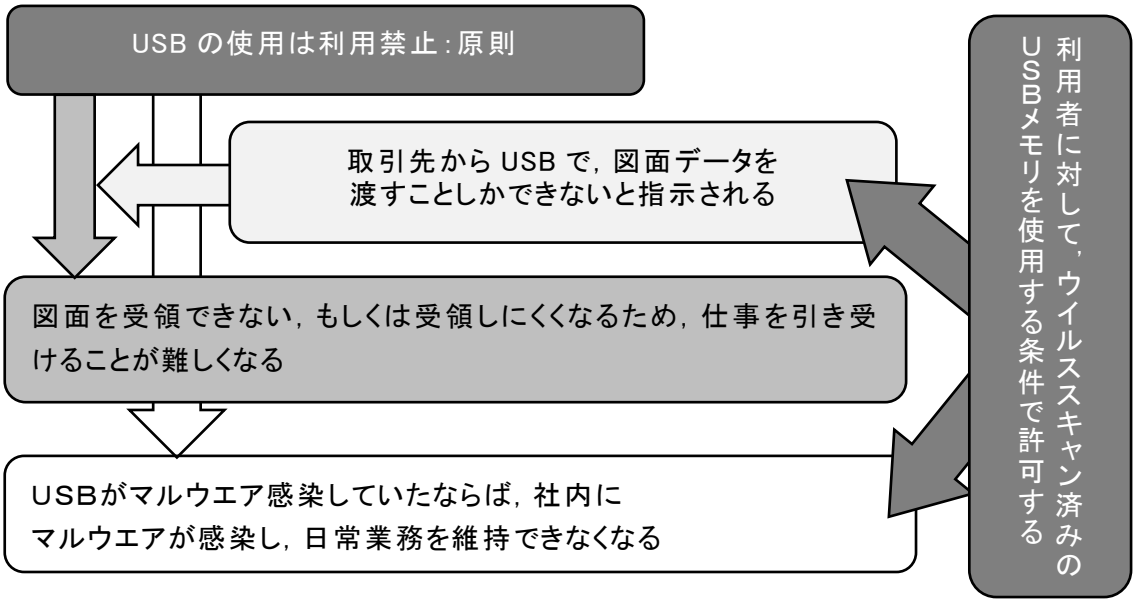

図 1-1 USB メモリ管理策における例外の基本例

なお上記で述べた例外の適用においては，USB メモリの利用者に関する要件のみを紹介したが，システム管理者に対しては「対象システムを特別の監視対象として運用する」といった要件が加味されることになる．

1.4.2 ケース2：第三者認証のない外部クラウドの利用への管理策

次に第三者認証のない外部クラウドの利用について取り上げる．クラウドサービス事業者のセキュリティの現状を評価する手段としては，利用組織が事業者に対して直接監査を実施することは，クラウドサービス事業者のポリシーや利用者側の費用的・時間的面から難しい[10]．そのため一般的にはクラウドサービス事業者のセキュリティ対策の確認方法として第三者認証が活用されており[11]，これに対応して，多くのクラウドサービス事業者が第三者認証を取得している[12]．

しかしながら，外部クラウドサービス事業者の特定サービスを利用するに当たり，当該事業者が第三者認証を取得していないケースがあることも否定できない．そのため，当該サービスを利用する場合は，例外の適用が考えられる．

10) 栗田 克己，樋口 清秀，“クラウド・コンピューティングにおける非対称情報の解消について”，情報通信学会誌，2012 年 30 巻 1 号 p. 1_15-1_26
11) 佐藤栄城，原田要之助，“クラウドサービス利用における第三者認証制度の考察”，情報処理学会研究報告，Vol.2013-EIP-59，No.1(2013)
12) ビジネス on IT，“クラウド環境における第 3 者認証制度”，2019-2-8， https://www.business-on-it.com/1002-cloud-security-3rd-pty-certification/

このケースを例に考えると，ある組織で「第三者認証のない外部クラウドの利用は禁止」を内部規程として策定していたとする．これが原則に該当する．しかしながらその組織が目指す新規業務開拓には，第三者認証のされていない外部クラウドサービスが提供する特定サービスの利用が不可欠だとする．この場合，第三者認証のない外部クラウドの利用禁止を貫くならば，当該クラウドのみが提供する特定サービスを利用しての新規業務開拓ができなくなる．その結果，自組織でサービスを設計・開発しなくてはならなくなり，手間（時間）と経費がかかる．また，当該クラウドへの内部規程を無条件で破ってサービスを利用した場合，このクラウドが突然停止したりマルウエア攻撃を受けたりすると新規業務に影響が生じ，これにより日常業務も維持できなくなる．

上記のようなケースにおいて，「あらかじめ組織内イントラネットと切り離し，クラウド業者に対し最大限の管理・運用の徹底と早期の第三者認証の申請を条件として，一時的に利用を承認する」，すなわち例外として条件付きでクラウド利用を承認することで，新規業務への機会を得ることが可能となる．ここで述べた措置が例外の適用であり，「あらかじめ組織内イントラネットと切り離し，クラウド業者に対し最大限の管理・運用の徹底と早期の第三者認証の申請を条件とする」といった要件が，内部規程から逸脱している事象に対しての例外の策定許容要件（つまり許容範囲）となる．

なお上記で述べた例外の適用のケースにおいては，利用者に関する要件のみを紹介しているが，システム管理者に対しては「対象システムを特別の監視対象として運用する」といった要件が加味されることになる．

1.5　本研究の目的と本論文の構成

本研究は，情報セキュリティの業務を遂行する上で，例外というものを認識し，例外への許容範囲がどこまで認められ，かつどのように措置されるべきか，またその例外の限界はどこか，といったプリミティブな疑問に答えようと出発した．その上で，本論文では，例外を適用することによってもたらされるであろう，業務の効率化を探求することを主目的とし，組織における情報セキュリティポリシーの例外の策定の必要性・可能性，そしてその運用の必要性と限界について論じる．

具体的には，例外を規程として策定するという管理・運用方法は，例外の申請者もしくは申請部門（利用部門）や承認者もしくは承認部門（主に管理部門）さらには，組織経営全体にとって有効であることを論じる．これは特に，不確実性の高い情報セキュリティ分野において，組織ごとに情報セキュリティポリシーを策定し，同時にその例外をも規程として策定することは，今日の組織において喫緊

の課題であるとともに，そこに優位な意義を見出せるものと考える．

そして例外を規程として策定する意義を補足するために，例外の適用をどのように判断し，また規程をどのように策定・運用するべきかについて探求する．このことは，迅速な例外の適用によって組織の日常業務に負担軽減が期待できるかを明らかにするほか，情報セキュリティポリシーからど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の適用を認め，業務の継続ができるのかを知る手がかりとなる．

本論文の章構成は次の通りである．

まず本論文で用いる「例外措置」と「例外規程」をはじめとする用語の定義と研究対象となる範囲を第 2 章で定めた後，「例外」の必要性と限界について整理する．第 3 章では，国内外の例外に関わる先行事例を調査し，例外の活用の傾向と課題について考察する．

次に第 4 章では，第 3 章の先行事例で把握できなかった例外の活用の実態についてアンケート調査を行い，例外の取り扱いや効果などを分析したことを述べる．これらの結果から，具体的な管理策における原則と例外との比率を求め，その傾向についても考察する．

第 3 章と第 4 章の結果・考察を受けて第 5 章では，例外規程（定義は 2.1 節参照）の活用に向けての対策について述べる．具体的には，組織内での策定主体と注意点，例外規程にすべきかどうかへの考え方，および利用者への対策について言及する．最後の第 6 章では例外規程の普及に向けての提言と今後の期待について論じる．

なお本論文は，これまでの筆者の研究を総括するものであるため，「初出一覧」に記載した諸論文を見直し，再整理している．そのため，用語の定義も再考し，さらに次章で述べるように統一を図っているため，初出の用語と本論文の用語が一致しない場合は，本論文の用語が優先するものと考えていただきたい．

1.6　例外を組織内で管理・運用する主体

前節では，例外を適用するにあたっての基本例を示した．実際に例外を組織内で取り扱っていくためには，例外をマネジメントサイクル化すなわち PDCA サイクル（Plan-Do-Check-Act cycle）によって管理・運用していく体制を構築していくことが求められる．これは例外をただ単に活用するだけでなく，情報セキュリティマネジメントとして，規程の策定，措置の実施および管理・運用が明確にできるからである．

通常，情報セキュリティポリシーについては，組織の管理部門が専門的に立案・策定し，それに沿った措置を利用部門が実施し，実施結果を評価・改善していく．そのため例外においても，管理部門が主体となったトップダウンでの管理策が考えられる．一方で例外の策定を考慮した場合，利用部門が求める例外の適用を利用部門自身がボトムアップ的に立案し，管理部門への上申などを極力減らし，利用部門が主体となって管理・運用することも考えられる．

こうした例外の特徴から，本論文では，組織における例外の適用への管理・運用には体系的に大きく「管理部門主導タイプ」と「利用部門主導タイプ」の 2 つの主体のタイプにまず区別する．これを表 1-1 のように特徴づけることができる．2 つのタイプのどちらを使っているかを知ることは，管理部門・利用部門のどちらが主体となって例外を策定しているかなど，その組織の例外適用における管理・運用の姿勢が把握できることになる．

なお本論文では，4 章のアンケート調査を経て，管理部門主導タイプと利用部門主導タイプの両方の長所をバランスさせて，柔軟な運用を提案する（詳細は 5.2.1 項を参照）．

表 1-1 例外を組織内で管理・運用する主体

	主体のタイプ	特徴
1	管理部門主導タイプ（トップダウンタイプ）	経営側，組織全体の統一規程・基準・ガイドラインにおいて例外を策定．経営側で管理．改定は数年程度の間隔で定期的に実施する．
2	利用部門主導タイプ（ボトムアップタイプ）	現場側，事業所や職場ごとの基準やガイドライン，手引きなどにおいて例外を策定．各現場で管理．直接運用に関わることが多いため改定はその都度柔軟に対応する．

1.7　研究の直接的動機

最後に本研究の直接的動機を述べて本章の結びとする.

筆者は 2014 年 6 月から 2017 年 6 月にかけて, 組織の情報システム部門に在籍し, IT ユーザ部門から外部クラウドや管理外 PC の使用などの例外措置に関する各種申請・相談窓口業務を担当していた. そこでは, 情報システムに関する例外申請の承認業務も含まれていた(この間の経緯は, 初出一覧(5)に詳しく述べている).

一般に, 原則的な措置に関しては, 情報セキュリティポリシーに則って内部規程等で詳細に記載されているが, 例外的な措置に関しては大まかな措置方法のみが記されていることが多い. 詳細な措置方法については, 与えられた権限のもとで個人の判断に委ねられ, それを上長が承認するという過程だけが決められている. これはもともと申請内容を内部規程に予め記述することが難しく, ケース・バイ・ケースであるという,「例外」の性質上やむを得ないことではあろう.

しかし当の担当者にしてみれば, これは困惑するものであった. 個々の申請内容と自らの内部規程の意味解釈と業務経験とを照らし合わせつつ判断するしかなかった. 上長決済への対応も考え合わせると, 労力と時間を要することが多い反面, 例外の申請は急を要し, 迅速に措置を実施することが求められるので, 苦労が絶えなかった.

このような経験から, 例外規程(用語の定義は 2.1.4 項参照)の利点(規程に明記された事象にはもちろん, 明記されていない事象にも準用できる)を実感するとともに, その限界にも関心を持つようになった. 例外申請を効率よく審査・承認するために, 何らかの統一的なルールの存在, また, 他の組織ではそれをどのように策定し運用しているのか, さらには仮に統一的なルールがあるとすれば, どのように普及させていくべきなのか, という点に関心を持つようになった.

そこで例外を研究テーマとして, 2014 年 10 月に当大学院博士前期課程に入学した後, おおむね 2015 年 3 月頃から先行事例やアンケート調査を通じて, 本研究に取り組むことになった次第である.

小括

本章では，まず研究をはじめた時代背景と，個人的動機について述べた．

2014 年から 2017 年にかけて情報システム部門に在籍していた筆者は，例外措置に関する申請窓口で「例外」を運用することになったのがきっかけとなり，例外の存在意義，必要性，煩雑性，運用の在り方について興味と疑問を持つに至った．

情報セキュリティ施策はその性質上不確実性が伴うため，想定が難しい問題や事象に対しては「例外」を考えざるを得ない．これが例外の必要性である．また例外に対して何らかの措置をする場合，それぞれの事象に対して個別事情を考慮した対応を考えなくてはならないため，「判断」という作業が伴う．これが例外の煩雑性につながる．したがって例外にかかる措置を例外規程として策定することで，一般化と個別事情への配慮という，相反する目的間のバランスをとることが有効と考える．

また例外は，常に原則と密接に関係して考える必要がある．例外はあくまでも例外であり，例外は原則に対する逸脱であることは避けられない．そこで情報セキュリティポリシーから逸脱している行為に関して，それを例外としてどの程度まで容認するのか，またそれを容認することによって新たに生ずるリスクが容認するメリットを上回らないか（効用対リスク効果），という判断が求められる．

さらに例外の適用には「管理部門主導タイプ」と「利用部門主導タイプ」の 2 種類あり，組織がそのどちらを使うかにより，組織の運用姿勢が把握できるものと考える．

2. 例外の定義と研究対象，必要性と限界

第1章では情報セキュリティの業務における例外の必要性と煩雑性について述べた.「例外」という用語そのもの，あるいはそれに関連する考察は広範囲の内容を含んでいることから，これから本論文で例外について論じるにあたり，まずは本章にて用語の定義を示し，併せて本研究の研究対象の範囲を明確にする.その上で，例外の必要性と限界について述べる. なお付録 A6 にて本論文で用いる重要な用語をまとめている. 合わせて参照されたい.

2.1　例外・例外措置・例外規程の定義

本節では，原則規程，通常措置および逸脱を述べた上で例外について説明し，その上で例外の中から例外措置および例外規程の定義と範囲（内包と外延）について述べる.

2.1.1 原則規程，通常措置及び逸脱

情報セキュリティに関する組織全体の方針は，情報セキュリティポリシーに定められている. そこでは，組織全体のルールとして「どのような情報を，どのような脅威から，どのように守るのか」といった基本方針とともに，情報セキュリティを守るための体制，運用規程・対策基準などが具体的に記載されている[13]. これらの規程は，日常業務において定常的に実施されるべきリスク低減措置としてまとめられたものであり，関係者が合意して策定したものでもあるため，原則として遵守しなければならないものである. これを本論文では「原則規程」と定める. そして原則規程（即ち，元を辿れば情報セキュリティポリシーに則って）の管理策[14]それぞれに対し，日常業務において定常的に実施されている措置を，本論文では「通常措置」と定義する. すなわち通常措置は原則規程によって明文化・ルール化された措置である.

したがって通常措置を破る行為は，「逸脱」行為・措置となり，是正あるいは非難の対象になる. なお本論文では逸脱について，特に「情報セキュリティポリシーからの逸脱」と記述する場合を除き「原則規程からの逸脱」に便宜上表記する.

---

13) 総務省，“情報セキュリティポリシーの概要と目的”, (オンライン). http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/04-2.html. (アクセス日: 2019 年 6 月 10 日).

14) JIS Q 27000:2014 では，管理策（control）は，「リスクを修正（modifying）する対策」と定義されている. また注釈として「管理策には，リスクを修正するためのあらゆるプロセス，方針，仕掛け，実務及びその他の処置を含む」とする一方，「常に意図又は想定した修正効果を発揮するとは限らない」と留意を付加している.

2.1.2 例外（本論文における）

しかし同じ「逸脱」の中には，「原則に対する例外」として組織で認めたものや，予め求められていなくても緊急避難的に実施した方が良いもの，これまで検討されてこなかったが原則よりもリスク低減効果が高いと思われるもの，などが存在し得る．これらは本来「逸脱」であるが，原則を補完するために「例外」として認知されたり（相互補完），場合によって原則に取って代わったり（代替関係）するなどの有効性が認められるもの，いわば「原則の予備軍」である．このことから，この両者を総称して「例外」と考える．

本論文における「例外」とは，1.3 節における広辞苑の定義を情報セキュリティに当てはめたものである．特に，情報セキュリティを守るための管理手順が定められていることを前提に，原則とは違った手続きが必要な場合の要件を定めた規則，あるいは定められた手続きそのものを指す．

2.1.3 例外措置

原則に対する逸脱において，その逸脱の内容・範囲を把握し，原則規程もしくは通常措置と同程度の効用対リスク効果が期待できるとして，承認権限者から許可を得た措置を，本論文では「例外措置」と定義する[15)]．

例外措置は，原則規程をすぐに改定できず，通常措置として対応しきれない状態もしくは通常措置そのものがない状態において，利用部門が業務やビジネスにおいて活用するための措置のうち，利用部門の判断や管理部門での承認に基づいて一時的に実施される措置である．

これには次のことが考えられるからである．原則規程に予め策定されていない場合や原則規程から逸脱した事象・行為は逸脱領域にあたる．そのため，逸脱行為は即禁止され罰則の適用が検討されることがある．また原則規程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措置（当該事象への対策）を原則規程に盛り込む改定は困難である．

このような事態を避けるため，例外措置を原則規程の改定までの当該事象のリスクに対応する一時的な措置とする．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でき，原則規程からの逸脱を防ぐことになる．

この原則規程からの逸脱に基づく例外措置には以下の要素が全て求められる．

15) H24 政府統一管理基準では，利用者がその実施に責任を持つ原則規程を遵守することが困難な状況で，業務の適正な遂行を継続するため，遵守事項とは異なる代替の方法を採用し，又は遵守事項を実施しないことについて合理的理由がある場合に，そのことについて申請し許可を得た上で適用する行為として定義している

(1) 計画準備段階で対策手順を予め策定し，実際に事象が発生した場合は，手順に従って例外措置を実施する．
(2) 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準備する．
(3) 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の実施を可能にする（実施したときには，実施内容を報告する）．
(4) 実施した例外措置を管理する．
(5) 例外措置と罰則（措置から逸脱したときのため）をセットにする．

これら 5 項目は組織全体で統一した内容とするのではなく，それぞれの部門で様々な管理策において例外措置を実施するものと考える．これは部門によって管理する情報やリスクが異なるため，部門毎に実務に沿った例外が必要となる．なお(5)については，罰則の意義についてより深い理解が必要なため，5.4.3 項にて改めて論じることにする．

なお例外措置は第 3 章の先行事例や第 4 章のアンケート調査の結果からも，今日の組織において活用されてきていることが明らかになっている．

なお例外措置は事前承認が原則だが，事後承認も例外として認めることも考えらえる．しかし事前に組織が把握していない措置であるため，措置を実施した時点で逸脱行為の区別がつかないというリスクが伴う．これを避けるために次項のとおり例外規程を予め策定し，事後承認に関わるルールとして設定しておくべきである．

2.1.4 例外規程

組織が例外措置を管理・運用していくためには，措置の申請，承認・許可，実施，報告，さらには見直し等といった手続きやその内容について明確にルール化し，記録保存する必要がある．したがって原則規程によって管理・運用されている通常措置の取り扱いと同等に，例外措置を規程として汎用的にルール化していくことによって，より効率的に管理・運用できるものと考える．本論文では，この例外措置の根拠規程を「例外規程」と定義する．すなわち同一もしくは類似する例外措置の適用が多い状況において，当該例外措置を（代替手段の導入も含め）ルール化し，規程として策定したものを例外規程とする．例外規程には，例外措置の策定手続き，あるいは例外措置を策定した規範が含まれる．

例外措置を汎用的にルール化することで承認・許可作業を可能な限り簡便化・省力化でき，業務の効率化が図れる．また規程として明文化することで管理・運用の可視化が期待できる．

なお，例外規程として改めて策定しなくても，原則規程を利用部門にてカスタマイズすればよいという考えがある．これは，本研究を始めた当初から議論されてきている点である．しかし規程策定へのマンパワーやスキルが乏しい傾向にあると考えられる利用部門で，管理部門や経営層への説明や承認も含め，組織横断で原則規程を改定することは難しい．また例外規程で取り扱う例外措置は，原則規程で定められた通常措置とは異なる管理・運用がされるべきである．これは例外措置として承認され，実施しているという意識を利用部門に与え，例外措置の頻発を抑える必要性による．したがって例外規程は原則規程と切り離して取り扱うべきと考える．

以降，本論文では「例外」の表記には，例外規程および例外措置を含めて述べていく．また「例外規程」または「例外措置」それぞれについて述べる場合は，区別して表記し論じていくこととする．なお，本論文では，原則規程や例外規程を内部規程などに明文化してルール化することを，「規程を策定する」「規程策定」と表現する．また，原則規程に則り措置をすることを「通常措置を実施する」，例外規程の有無に関わらず例外措置をとることを「例外措置を実施する」と，原則，表記する．

また，本論文では「例外」の英語表記を，“exception”，「例外措置」を“exceptional measure”，そして「例外規程」を“exceptional rule”で用いている．これは，第 3 章の先行事例で取り上げる，政府機関の情報セキュリティ対策のための統一基準群の英訳版（Common Standards for Information Security Measures for Government Agencies）で“exceptional measure”という語が用いられていること参考にしている[16]．なお “measure”は，措置を実施する具体的措置を意味するのに対して，措置の要件を定める規則は“rule”と表記し，後者が本研究の主たる検討対象である[17]．

16) The Cybersecurity Strategic Headquarters, “Common Standards for Information Security Measures for Government Agencies (FY2016)”, 2016.
17) Oxford English Dictionary によれば，exception は “A person or thing that is excluded from a general statement or does not follow a rule.”と説明されている．すなわち，通常のステートメント（表明文，宣言書，報告書など）から除外された，あるいはルールに従わない人や物を指し，本論文での原則の規程から除外もしくは従わない措置を例外措置として扱うことと一致する．

2.2　本研究における例外

前節では，例外そのものの意味は広範囲であることから，本論文で述べていく上で文言の定義づけをした．さらに本研究を進める上で，例外を取り扱う研究対象を定義しなくてはならない．本節では例外について 2 つの区別を取り上げ，その上で本論文における例外の研究対象範囲を述べる．

2.2.1 情報セキュリティポリシーにおける例外

まず例外の範囲を，原則規程のおおもととなる情報セキュリティポリシーに基づいて定義する．この情報セキュリティ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）から成り立っている[18)19)20)21)]．例外はこの三層のそれぞれに対応し，その範囲は逸脱領域（2.1.3 項参照）との間にあると考える．以下，「基本方針」「対策基準」および「実施手順」について述べる．なおこれらの三層構造は情報セキュリティポリシーに基づいて策定されている原則規程にも当てはまるものとみなし，以下原則規程における三層構造に置き換えて述べていくことにする．

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 2-1 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規程としては，例えば「CISO（Chief Information Security Officer；最高情報セキュリティ責任者）など責任者による例外措置の許可権限」や「非常時での非常対策本部（もしくは緊急対策本部）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，全ての組織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」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．対策基準での例外規程は，組織全

18) 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”, 内閣サイバーセキュリティセンター, (オンライン). http://www.nisc.go.jp/active/sisaku/2002_1128/ISP_Guideline_20021128.html. (アクセス日 : 2019 年 6 月 10 日).

19) 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). http://www.soumu.go.jp/main_content/000348656.pdf.

20) 総務省, “情報セキュリティポリシーの内容”, 総務省ホームページ, (オンライン). http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/04-3.html. (アクセス日 : 2019 年 6 月 10 日).

21) 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).http://www.ipa.go.jp/security/manager/protect/pdca/policy.html. (アクセス日 : 2019 年 6 月 10 日).

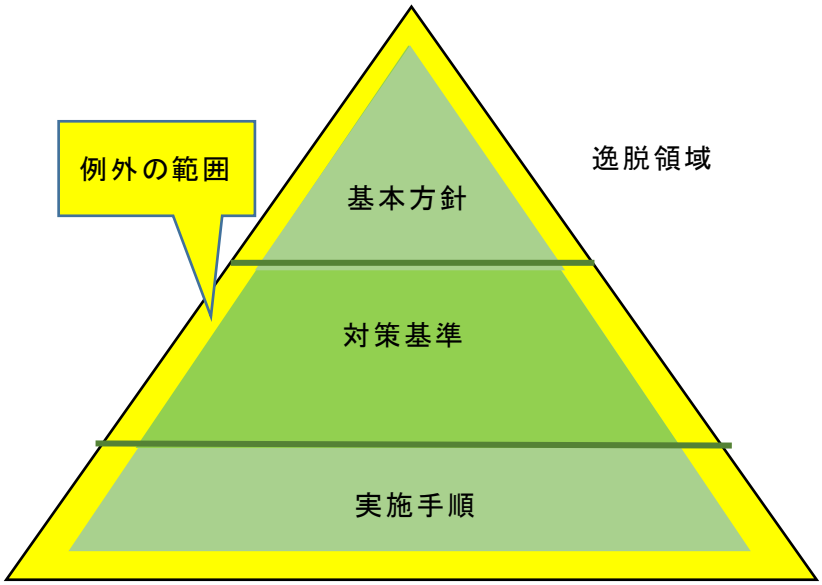

図 2-1 情報セキュリティポリシー（原則規程）基本構造と例外

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．これは一般にリスクは部門・部署ごとに異なるため，適用する対策基準も変わるためである．個別具体的に例外措置を実施することで，部門・部署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常に行う[22]．

さらに「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，最下層の「実施手順」である．

例外は「基本方針」，「対策基準」および「実施手順」それぞれに適用することによって，業務効率の向上が期待できると考える．一方で，例外規程の策定および例外措置の実施内容については，それぞれの層で異なる形式になるとも考えられる．本論文では三層のうち「基本方針」と「対策基準」での例外規程について述べる．これは「実施手順」は上位二つの層に拘束されるため，上位層での例外規程の策定および管理・運用から直接結びつけられると考えられるからである[23]．

22) 金融情報システムセンター，“金融情報システムセンターガイドライン検索システム”，(オンライン). https://www.fisc.or.jp/guideline/. (アクセス日：2019 年 6 月 10 日).

23) 文献によっては，基本方針と対策基準のみを情報セキュリティポリシーとして整理し，実施手順は細則として個別対策などを盛り込んで肉付けする形が一般的とする事例もある．（サイバーセキュリティ.com，「情報セキュリティポリシー策定のポイントとサンプル例文集と策定しないリスクとは？」，https://cybersecurity-jp.com/security-measures/22421（アクセス日：2019 年 6 月 11 日）など）

まず基本方針における例外規程の策定および例外措置の実施について述べる. 基本方針は, 組織の情報セキュリティについて, 組織の理念や運用方針を表明するものであり, 組織に属する構成員(従業員や派遣社員, 協力会社の出向社員等)を対象に全体的に統一された内容となっていることが一般的である[24].

そのため基本方針での例外規程は, 例外措置の容認の可否や, 非常時での非常対策本部の設置・指示命令系統の統一などといった, 大筋の方針を定める. 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なくてはならない.

なお基本方針は頻繁にかつ定期的に見直されるものではないため, 例外規程についても同様である. したがって基本方針における例外規程は, 以下の事象が起きた場合に策定を検討することになる.

(1) 事故・事件等により大きな脅威や脆弱性が発見された場合
(2) 新たな事業展開や法制度の変更に伴うセキュリティ要件が変わる場合
(3) NISC (National center of Incident readiness and Strategy for Cybersecurity, 内閣サイバーセキュリティセンター)や外部監査機関等から見直しの勧告を受けた場合

など.

(1)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. (2)の新たな事業展開については, 例えば「外部クラウドサービスの組織内への導入決定」, 法制度の変更については, 例えば「個人情報保護法の改正に伴う個人情報の管理厳格化」などに対するセキュリティ要件の変更があげられる. また(3)については, 勧告の内容をもとに担当部門において「基本方針への見直しに関する検討会の設置」「基本方針の変更とそれに伴う各部門への対策基準・実施手順の見直しの指示」などがあげられる. すなわち基本方針では, 非常時・改変時での非常対策本部の設置・指示命令系統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.

さらに例外規程は, 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門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考えられる.

24) 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.

次に，対策基準での例外規程の策定および例外措置の実施について述べる．対策基準は，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，標準，スタンダートやガイドラインと呼ばれるものである．対策基準では基本方針とは異なり，各現場レベル・部門ごとでの状況の変化に適切に対応するために，原則規程の見直しや例外措置の追加策定が求められる．

対策基準においては，セキュリティレベル（リスクのレベル）を安全とみなせるレベルに維持することが求められる．そのため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必要がある．

また基本方針での例外規程と異なり，対策基準での例外規程は個別具体的に策定することになる．すなわち当該事象に対応する例外規程は，原則規程を見直して盛り込まれるまでの，もしくは全く暫定的なものとしての，一時的な例外措置として実施されるものとなる．

一般的には日常業務で想定できるものであったとしても，例えば BYOD（Bring your own device：私物端末の業務利用）のケースでは，例外措置の煩雑さや実効性の難しさなどから，例外規程を策定していない組織が多い[25]．このようにあえて規程として明文化しない場合，「想定外の事象」が起こりうることを抽象的なイメージで「想定内」として意識し続けなければならない．これはリスクを認識していながら対策せずに放置したことと等価である．

そこで私物端末を業務用として一時的に利用を許可する場合，具体的に，使用期間や目的，理由を明記した申請書の提出を義務付けるなどの実施手順を定めた例外規程があることで，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．

なお対策基準では，各部門おいて具体的な管理策ごとに例外規程が必要であり，当該例外措置を実施するための実施手順（図 2-1 の最下層）の作成が求められる．

2.2.2 緊急時・非常時・平常時における例外

規程を策定し例外措置が実施されるケースとして，緊急時・非常時・平常時の 3 つのケースが想定される．そのため，これらと例外との区分について明らかにし，本論文での例外の範囲を明確にする必要がある．

緊急時（あるいは緊急事態）とは，戦争やテロ，大規模災害などの非常事態に対処するため，「一時的に政府に強い権限を与える法的な根拠」を示す概念である．国際的には国家の最高法規（一般的には憲法あるいは基本法と呼ばれ

25) 平木健士,原田要之助, “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 年 6 月 7 日

るもの）にこうした条項（緊急事態条項）を持つのが普通で，具体的には行政の長が緊急事態を宣言すれば，行政が法律と同じ効力を持つ政令を定めたり，地方自治体の首長に必要な指示をしたりすることができ，国民の順守義務もそれに含まれている．

日本国憲法では緊急事態が定められていないため注目されていないが，災害対策基本法には「災害緊急事態」（同法 105 条），原子力災害対策特別措置法には「原子力緊急事態」（同法 15 条）の定めがあり，平成 23（2011）年 3 月 11 日に発生した東日本大震災に当たって後者が発動されたが，前者は発動されなかった．災害緊急事態は，かつては災害対策本部の設置の前提であったが，阪神淡路大震災（平成 7（1995）年 1 月 17 日発生）の教訓から，要件から除かれたからである[26]．

いずれにせよ，日本は世界でも稀な「憲法に緊急事態条項を含まない国」である．その影響からか，武力攻撃事態対処法ができてもなお，「緊急事態」という概念が憲法論においても定着していない．ましてや災害対策や情報セキュリティ対策において，「緊急事態」を想定することは忌避されている．したがって本論文でも，緊急時という分類は見送り，「非常時」と「平常時」の 2 区分について取り上げる[27]．

「非常時」における例外措置は，想定外のインシデントや事件・事故などに対するもので，対応策がリソース的・時間的な制約などにより実施できない場合がある．想定外の事象への対策は，必ずしも情報セキュリティ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予め策定されていなかったり，もしくは不十分であったりするためである．このような場合，計画段階で想定した範囲内だけで実施すると，かえって柔軟に対応できなくなるおそれがあることから，例外規程を用意して非常時に備え，自由度を確保するねらいもある[28]．

また非常時における例外措置は，即時対応が求められる措置であるため，主に BCP（Business Continuity Planning；事業継続計画）で策定すべき一時的な措置と重なる．すなわち，インシデント対応や BCP といった，組織の大方針に従うため，当該措置を内部規程に盛り込む場合では，原則規程にこだわらない例

26) 従って新法においては，内閣総理大臣が単独で設置を決定できる「非常災害対策本部」（同法 24 条）と，閣議にかけなければ設置できない「緊急災害対策本部」（同法 28 条の 2）の両者があることになる．なお前者が存在する中で後者が設置された場合は，後者が前者の事務を承継することになる（同条 3 項）．

27) 本研究では従来「緊急時例外措置」と表記していたが，本論文では災害対策基本法改正の経緯等も勘案して再考し「非常時」と表記する．これにより「緊急災害」に達しなくとも「平常時」ではない事象においても，例外措置を取り扱う必要性を述べる．

28) 内閣官房情報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」”，(オンライン)．
http://www.nisc.go.jp/active/general/pdf/K304-111C.pdf. (アクセス日：2019 年 6 月 10 日)．

外規程として取り扱われることになる. しかし長期間継続させるものではなく, 可及的速やかに「原則」に戻さなくてはならない.

一方,「平常時」における例外措置は, 重大かつ緊急を要するものではないものの, 原則規程では取り扱えない事象を対象とする. そのため予め例外規程として策定され, ある程度の期間にわたって例外措置が実施される.

例外措置が実施できない場合, 原則規程から逸脱した事象や行為はすべて認められなくなる. また原則規程の改定にはリスク分析や評価, 対応等の検討が必要で時間がかかるため, リスクが高まった時点ですぐには対応できない. こうしたリスク対応がとれない事態を避けるため, 組織において例外措置を実施することが考えられる. そして例外規程を予め策定しておくことで, 迅速に例外措置が実施でき, リスク対応がとれるものと期待できる.

2.2.3 本論文での例外の研究対象

これまで本論文での例外の研究対象を決める上で, 情報セキュリティポリシー(原則規程)の基本構造, ならびに非常時・平常時での区別について述べた. 本論文では主に「平常時」における「対策基準」の例外を研究対象とする.

研究の対象を対策基準とした理由は, 基本方針と比べ日常業務に直結し, 組織のリスクの変化などに柔軟かつ定期的に対応しなければならないと考えたからである. また平常時とした理由は, 非常時の例外規程に比べ頻度が高く, また長期間運用されることから, 原則規程からの逸脱程度の判断や評価が定期的に管理され, 定式化するための対策を探ることが研究に結びつくと判断したためである.

本論文では, 以降,「平常時」における「対策基準」について論じていく. その上で, 組織での例外措置の実施, および例外規程の策定による例外措置の管理・運用, それらを手掛ける組織内での体制, さらには例外適用への判断や評価などといった観点で調べていく.

2.3　例外の必要性

ここまで，本論文にて例外を論じる上で必要となる定義と研究対象範囲について述べた．例外規程および例外措置は既に定義づけたので，本節では平常時での対策基準における例外の必要性について述べる．

2.3.1 業務効率の向上

まず，例外措置を例外規程によって汎用的にルール化することで，承認作業を可能な限り簡便化でき，業務効率が図れる．規程として明文化することで管理・運用の可視化が期待できる．

これは筆者の経験であるが，例えば自組織が管理していない外部業者の PC を，原則規程上禁止しているイントラネットへの接続を希望する例外申請が出された場合，自組織と同一のセキュリティ管理ソフトが導入済みであることと，指定したプロキシ設定が実施されていることを条件に，申請・誓約書のみの形式審査で承認する例外規程が存在していた．これにより申請者・承認者ともに負荷がほとんどかからず，効率化が図られていることは自明である．一方で，当該例外規程に該当しない例外申請がされた場合，例えば，PC の動作機能上セキュリティ管理ソフトがインストールされていない場合では，例外措置として承認するかの審査処理が伴う．したがって当該申請には申請者・承認者双方に労力も時間もかかることになる．

2.3.2 いわゆるシャドーIT の未然防止

例外の適用は，管理部門におけるリスク対策においても極めて重要であり，安心安全な業務運用に役立つものと考える．なぜなら例外措置がない場合，利用者は原則規程に該当しないものは実施できないし，実施した場合は規程違反として罰則の対象となる場合があるからである．いずれにしても健全な業務遂行ができなくなる．そこで原則規程を無視して，管理部門から管理されないように水面下で原則規程に該当しない逸脱行為を実施されてしまうことが考えられる．

例えば私物スマートフォンの業務利用を取り上げてみる．これらは近年 IoT（Internet of Things：もののインターネット）や BYOD への対応が普及しつつあるものの，依然多くの組織では原則禁止にしているものと推定する．また現場（利用部門）からの要望がなければ，管理部門から私物スマートフォンの利用を検討するとは経験上考えにくい．したがって当該利用については現場からの要請が主であると考える．

まとめると，業務で私物スマートフォンを利用した方が，仕事をしやすいと判断したときに，利用部門は以下のような行為を実施するものと考える[29]．

(1)管理部門に見つからないようにだまって利用する．場合によってはグループぐるみで実施することも否定できない．

(2)管理部門と相談し，業務として利用できるように働きかける

（1）はいわゆる「シャドーIT」と呼ばれるものである[30]．（2）は「利用部門主導タイプ」の例外措置に対応する．

他方，情報セキュリティ管理者としては申請を受けた時に，①承認しない，②無条件で承認する，③条件付きで承認する，3 つの選択肢が考えられる．ここで例外措置が実施できなければ，①しか選択できない．一方例外措置が実施できるのであれば③になる．もともと②であれば，例外措置ではなく通常措置として実施されているはずである．

また時間的・労力的に余裕があるならば，（事象が発生した時点では）例外措置がなくとも，検討・審議・経営許可を得た上で，②か③の措置をとることも考えられる．つまり当該事象をきっかけにして，例外措置を実施することとなる．しかし，時間的に余裕がなく喫緊の対応を要する場合において，例外措置がないときは，現場担当者の判断でまず一時的措置をとり，後ほど承認のため周辺や上層へのエスカレーションすることも考えられる．

次に利用者側の心理面から考えたとき，原則だけでなく例外があると，一種の緊急退避術と考えられ，安堵感につながる効果が考えられる．一方で管理部門としては，利用部門に例外措置の実施を承認したことで，セキュリティ上完全に問題がないか，または責任が重くなりはしないか，などと言う不安感が出てくることも否めない．なぜなら管理部門が例外措置を認めたことは，利用部門としては「お墨付き」を得たわけであり，リスク対策と同時に責任も管理部門側にあると転嫁することも可能だからである．したがって例外を承認した管理部門としてはさらに重い責任を負うことになる．管理部者の判断・承認が確立していない，もしくは承認の裁量でブレが生じるようなときには，情報セキュリティへの確保が難しく，管理部門の精神的な負担も大きくなる可能性がある．

---

29) 内閣サイバーセキュリティセンター，“スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書”，2015 月 5 月 21 日．
(オンライン).http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf. (アクセス日：2019 年 6 月 10 日).

30) 遠藤宗正，“シャドーIT とはこれでおさらば!? 企業をむしばむ無断使用ツールを「断捨離」する 3 つのステップ，“シャドーIT”との向き合い方”，IT Media ニュース，2015. (オンライン).
http://www.itmedia.co.jp/news/articles/1501/27/news045.html. [アクセス日：2018 年 12 月 21].

しかしながら，原則のみの場合だと違反して即罰則の対象となったり[31)]，水面下で無断に使用されたりすることを考えれば，情報セキュリティのリスク管理においては，内部規程に「原則」と「例外」があることが望ましい．内部規程に盛り込まれていない事象に対して，どのように明記しているかで，上記の対応に差がつくことは容易に想像できる．

2.3.3 技術進歩への柔軟な対応

例外が原則の補完として柔軟に効果を発揮できることを説明するために，技術進歩と例外との関係性を考えてみる．筆者が着目したのは，組織活動において，組織の情報インフラ[32)]整備における技術進歩と原則規程とは整合性が取れない（合致しない）ことが起こる，という現象である．この現象には，(1)原則規程が技術進歩に追いつかない場合，(2)技術進歩が原則規程に対し十分でない場合，(3)技術進歩が逸脱領域に達する場合，の 3 つのケースが考えられる．本項ではこのうち(1)の原則規程が技術進歩に追いつかないケースに着目し，情報セキュリティポリシーにおける原則規程と法律，そして技術進歩との関係について述べる．

例外措置を用いない場合，原則規程の外側の周りは逸脱領域である．原則規程の境界は，それと境界を一にする逸脱領域の範囲の内側の境界である．そして逸脱領域はそれと境界を一にする法令違反領域の内側の領域を範囲とする．そこで逸脱領域の限度域と法令違反領域の間にある境界を，ここでは「法定境界線」と定義する．例外措置を伴わない逸脱行為のうち，法定境界線を超えるものは法令違反の対象となる．したがって法定境界線は逸脱領域の内側にある原則規程における法律上の限界を表すこととなる．すなわち逸脱領域に存在する例外措置もまた，法定境界線が限界となることを示すことになる．

---

31) 佐藤慶浩，“政府機関の情報セキュリティ対策のための統一基準”，(オンライン)．
http://yosihiro.com/speech/presenter/2006-08-02/index.html (アクセス日：2019 年 6 月 10 日).なお佐藤氏へのインタビューの際「例外措置を設けることによって，責任が明確となることで故意と過失の間のグレーゾーンがなくなり，組織のガバナンスの観点からは情報セキュリティ管理としては，むしろ効果的であり，また例外措置の記録は，以後のマネジメントサイクルでのリスクの見直しに役立てることができるようになる」というコメントがあった．前者についてはいささか断定的な見解であるが，後者は ISMS（3.3.1 項参照）など管理策にも通じる概念と思われる．

32) なお本論文での情報インフラは組織が業務上保有している情報システム機器やデバイス，使用するクラウドも指すものとする．
参考：品質マネジメントシステム（Quality Management System ; QMS）の国際規格である，ISO9001:2015 の「7.1.3 インフラストラクチャ」において「組織は、プロセスの運用に必要なインフラストラクチャ、並びに製品及びサービスの適合を達成するための必要なインフラストラクチャを明確にし、提供し、維持しなければならない。」の記載がある．さらに同項の注記には「インフラストラクチャとしては次を含めることができる。 a)建物及び関連するユーティリティ b)設備。これにはハードウエア及びソフトウエアを含む c)輸送のために資源 d)情報通信技術」の記述がある．b)および d)の記載は，本論文の情報インフラの定義に参考となるものと考える．

次に情報を取り扱う組織は情報インフラを保有しているのが一般的であり，これら情報インフラが持つ機能を有効活用するためには，その活用範囲についてリスク分析を行い，その結果に基づいて原則規程を策定しておくことが求められる．これにより原則規程に基づく通常措置として，組織は情報インフラを十分に活用することができる．その上で組織は，技術進歩に伴う情報インフラを整備することによって生じる高い経済性や利便性を求めることが可能となる．

例えば組織が保有する情報インフラの一つに「ファイル共有システム」がある．このファイル共有システムは組織の保有する情報を組織内あるいは外部業者と共有するために用いられる基幹システムである．このファイル共有システムを組織が有効活用していくためには，予め運用規則などを原則規程に明記し管理・運用していくことが求められる．

ところで組織が発展していくためには，組織をめぐる新しい環境に適応し，先進の情報インフラを取り入れていかなければならない．そのため技術進歩に伴い情報インフラの活用範囲が，従来のものから新しいものへと変化していく（一般的には機能拡張を目指すわけであるから，本論文では拡張する方向へ変化するものと解釈し表現する）．一方で情報インフラを管理・運用する範囲を策定していた原則規程も，新しい情報インフラの活用範囲の拡張に伴い改定していく必要がある．これは活用範囲が変更された，新しい情報インフラの管理運用が従来の原則規程では網羅しきれなくなり，逸脱になることを防ぐためである．

ファイル共有システムは従来，組織内でオンプレミスサーバを構築し運用されてきた．一般的にみて原則規程においても，ファイル共有システム内での情報の取り扱いについては，機密情報や個人情報については社外秘扱いとし，厳重に管理されてきた．それが近年利便性や経済性の向上から外部クラウドが広く利用されてきたことにより，組織は外部クラウドを利用したファイル共有システムを運用できるようになった．外部クラウドを利用する場合，組織はまず外部クラウド利用に対するリスク分析を行い，その上で従来のオンプレミスサーバにはなかった機能の拡張部分に対して，情報セキュリティポリシーに則り，現行の原則規程で措置できるのか，新たに原則規程の改定が必要なのか，または例外措置を施すのか，といったことを判断する必要がある．

しかしながら，原則規程を改定するには時間を要する．原則規程は組織の文化や組織のリスク受容に裏付けられたものであり，すぐには変えられないからである．そのため原則規程の改定作業が，情報インフラの技術進歩による活用範囲の変化の速度についていけないことが起こる．それが(1)の「原則規程が技術進歩に追いつかない場合」である．

そこで原則規程の改定が完了するまでの間，例外措置の実施により一時的に，その間隙を補完するわけである．これにより情報インフラの技術進歩を，例外措置で管理運用することが可能となる．その上で例外措置の実施を，例外規程の策定によってさらに管理運用することが望ましいと考える．

当該ファイル共有システムにおいても，クラウド化の機能を網羅できる原則規程をすぐに改定できないため，改定されるまでの間の一時措置として，例外措置を実施し，システムの運用を図ることになる．例えば，組織がいずれ改定する原則規程として外部クラウドに預ける情報を社外秘以外の一般情報のみとし，個人情報は従来通りオンプレミスサーバに保管させる．機密情報に関しては，例外措置扱いとして外部クラウドに保管すると判断したならば，原則規程が改定されるまでの間，3 つのケースの例外措置（A，B および C）が考えられる．

例外措置ケース A は新しい情報インフラの活用範囲を，いずれ改定される原則規程の範囲内で使用する場合であり，ファイル共有システムでは一般情報を外部クラウドに預けるケースが該当する．これは原則規程が改定されれば例外措置ではなくなる．

例外措置ケースB は新しい情報インフラの活用範囲を例外措置によって最大限に使用する場合であり，ファイル共有システムでは機密情報を外部クラウドに預けるケースが該当する．改定される原則規程をもってしてもその上限を超えるところがあり，法令違反では無いものの，上限を超える措置の部分については個別に例外措置の対応とする．

例外措置ケースC は新しい情報インフラを目一杯使い法令違反となる場合であり，ファイル共有システムでは組織が承認していなかった個人情報を外部クラウドに預けるケースが該当する（この場合，個人情報を利用者の第三者提供の同意なしに外部委託すると個人情報保護法違反となる）．改定後の原則規程，それに対する例外措置の両方をもってしても，法令違反となり，社会通念上認められるものではない．

以上，例外措置ケース A から例外措置ケース C についてまとめたものを表 2-1 に示す．

表 2-1 情報インフラの技術進歩における例外措置ケース

例外措置ケース	(例)ファイル共有システム	補足説明
A: (情報インフラの)活用範囲を改定後の原則規程の範囲内で使用する.	一般情報を外部クラウドに預ける. 改訂後の原則規程の範囲内である.	・ いずれ改定される原則規程の範囲内での措置を想定したもの ・ 原則規程が改定されれば例外措置ではなくなる
B: 活用範囲を最大限に使用するため, 改定後の原則規程の範囲を超える場合は例外措置によって補完する.	機密情報を外部クラウドに預ける. 改定後の原則規程では一般情報に限定しているため, 例外措置によって使用することになる.	・ 改定される原則規程においてもその上限を超えるところがある ・ 法令違反では無いものの, 上限を超える措置の部分については個別に例外措置の対応とする.
C: 活用範囲を目一杯使ったことで, 法定境界線を超え, 法令違反の対象となる.	組織が承認していない個人情報を外部クラウドに預ける(なお, この場合個人情報を利用者の第三者提供の同意なしに外部委託すると個人情報保護法違反となる).	・ 改定後の原則規程, それに対する例外措置の両方をもってしても, 法令違反となる ・ 社会通念上認められない

以上, 技術進歩と原則規程とは整合性が取れない関係性について, (1)原則規程が技術進歩に追いつかない場合を例に, 例外が原則の補完として柔軟に効果を発揮できることを述べた. なお本論文では取り上げなかった, (2)技術進歩が原則規程に対し十分でない場合, および(3)技術進歩が逸脱領域に達する場合においても, 改定に時間を要する原則規程の維持を図る上で, 例外措置の実施および例外規程の策定の必要性があると考える.

2.4　例外が持つ限界

前節では例外の必要性について述べた. 例外を組織の管理・運用に適用することで, 管理部門が把握できない利用部門でのシャドーIT の未然の防止や, 技術進歩への柔軟な対応が期待できるものと考える. その一方で, 例外は原則を補完する役割がある(原則と例外の相互補完)ことを意識しなくてはならない. 例外が原則に取って替わる(原則と例外の代替関係)のは稀であるし, また稀であるべきである.

本節では組織が例外を適用することを考えていくにあたって, 相互補完への意識および代替関係の回避といった, 例外がもつ限界ともいえる留意点への基本的な考えを補足する.

リスクは組織の目的が設定されてはじめて識別される. 一般的に組織の多くは, 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, 原則規程からの逸脱に対する許容範囲を判断して例外措置を実施している. この場合, 原則規程には残余リスクがもともと含まれており, 内容や対処を十分理解しておかなくてはならない. さらに原則規程を補完する例外規程もまた, 残余リスクが含まれていることを認識して策定するべきである.

そもそも残余リスクという考え方自体が, 将来の不測事態をすべて予見したり, 最適な行動を計算に入れたりすることは出来ないという, 人間の知的能力の限界を考慮した「限定合理性」[33)]を前提にしたものである(5.5 節でも取り上げる).

即ち, 経済主体の行動として極限までの合理性を前提とせず(つまり知り得る限りの諸条件を全て充足すること＝satisfy を求めず), あらかじめ定めた限られた範囲での次善的な最適化に止めるしかない(satisfice しかできない)という発想である. したがって, 残余リスクの取り扱いについては,「対応を拒否する／諦める」, あるいは「一時的に対応を保留する」ことにより, 業務継続の維持が可能となるのである.

このような発想に立てば, 逸脱した事象に対する措置も, 原則措置と同程度の効用対リスク効果が見込まれると判断できた場合, 原則規程には明記されていない別の代替方法により, 例外措置として実施を許可すれば良いことになる. さらに例外措置のリスク程度をあらかじめ理解し, 例外規程の策定に反映することができる（図 2-2 の右の吹きだしが示す円内と例外の実施範囲の三角形の内側とが交わる赤色で示した領域).

33) Simon の考え方に準拠している. H.A.Simon",意思決定と合理性",ちくま学芸文庫,2016

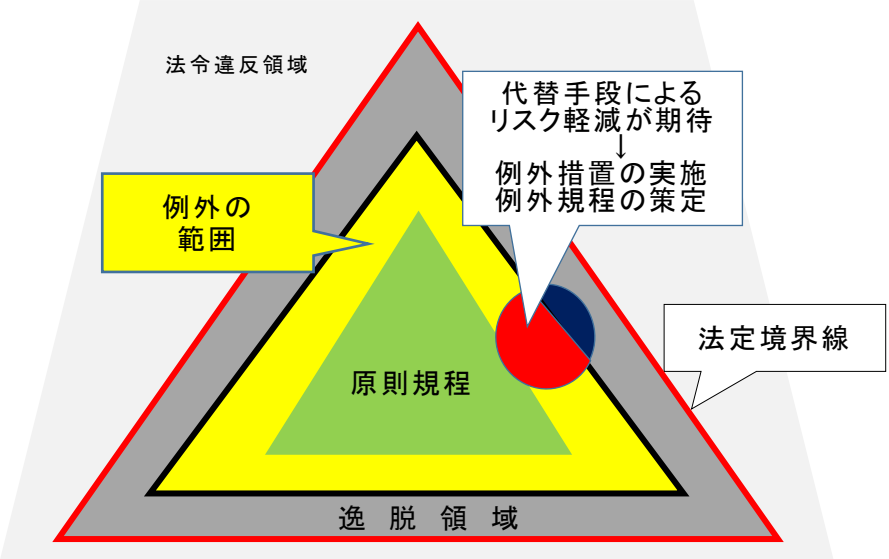

図　2-2　代替手段による例外範囲の確立

しかし，既に例外を認められている利用部門は，例外に対する心理的抵抗感が減少しており，過信してさらに例外措置を求めてくることが考えられる．これは組織の情報セキュリティ管理側にとって，「例外からの例外」を認めることで，業務遂行上の管理リスクを高めることにつながり，避けなければならない[34]．

そのための方策として，「厳罰化」と「組織性逸脱化への防止」の 2 つが考えられる．前者は法学者が好むもので，一般的に法の実効性はその強制力にあるとされるから，罰則が整備され現実に発動されることは望ましいとも考えられる．しかし，制定法の領域にあっても，罰則がかなり厳格に適用されるのは刑法・知的財産法などに限られるのが現状である．

また，本来情報セキュリティにおいては，実行行為者，被害の特定，因果関係の立証などを特定することが難しい（帰属（attribution）問題）という難問があり，その特定には多大な費用がかかる事は言うまでもない．組織内部の情報セキュリティ問題において，組織が罰則の実行者の場合，制定法の場合ほど多くの選択肢は用意されていない．せいぜい就業規則違反に基づく懲戒処分程度であり，この行使においてハードルが高い．日本の法制では懲戒処分として最強の「解雇」の要件が，他の先進国に比べて，著しく厳格である．

34) 何が原則で何が例外であるかは，基準点の取り方如何で変化し得る．知的財産権のうちでも著作権に例を取り，「情報の自由利用」という原点から出発すれば，「著作権という排他権の設定」自体が，例外となる．その例外，つまり「例外の例外」となるのが「公正利用」の概念である．この場合は「例外の例外」は，「原則に帰る」ことと同じになるので，法律にも明記され許容されているが，すべての事象がこのような関係になる訳ではない．

そのためむしろ注意を払うべきところは，逸脱行為が蔓延し，組織の秩序が乱れるほどになる状態をいかに回避するか，と言う点に絞られるものと考える．産業心理学あるいは組織心理学の研究者の間では，「組織性逸脱」という語が共有されているが，このような無秩序に近い状態を生じさせない点に，最大の注意が払われるべきであると考える（5.4.3 項で取り上げる）．

そもそも例外措置は，原則規程からの逸脱に対して，即罰則とすることを避ける作用もある（2.1.3 項参照）が故に，当該例外措置からの更なる逸脱行為は認めるべきではない．また，逸脱の防止策として罰則のみに頼るのではなく，各種の手段を組み合わせるべきである．日本では稀な「バウンティ（bounty）」という報奨制度（ペナルティというマイナスを与えるのではなく，バウンティという褒美を与える制度．例：バグバウンティ）の導入も考えられる．

小括

本章では，本論文における例外の用語と研究対象について定義し，例外の必要性と限界の基本的な考えを述べた．

例外措置とは，原則に対する逸脱において，その逸脱の内容・範囲を把握し，原則規程もしくは通常措置と同程度の効用対リスク効果が期待できるとして，承認権限者から許可を得た措置であると定義する．実務的にいえば，例外措置は，原則規程をすぐに改定できず，通常措置として対応しきれない状態もしくは通常措置そのものがない状態において，利用部門の判断や管理部門での承認に基づいて一時的に実施される措置である．

例外規程は例外措置の根拠規程として，同一もしくは類似する例外措置の適用が多い状況において，代替手段の導入も含め，例外措置の根拠を規程として策定したものとして定義する．言い換えれば例外措置を管理・運用していくための，措置の申請，承認・許可，実施，報告，さらには見直し等といった手続きやその内容について明確に策定した根拠規程であり，組織はこれらを記録し保存していく．これは業務の効率化に直結することから，例外措置をできる限り例外規程として策定し管理・運用していくよう，組織は努めるべきである．

本論文では，「平常時」のもので，情報セキュリティポリシーの 3 層構造のうち「対策基準」における例外規程及び例外措置に絞って研究を行った．これは対策基準が基本方針と比べ日常業務に直結し，組織のリスク対策の変化などに柔軟かつ定期的に対応しなければならないことや，平常時は非常時と比べ見直し頻度が高く，かつ長期間運用され，管理部門により原則規程からの逸脱程度の判断や評価が定期的に管理されるため，定式化しやすいと考えたからである．

例外には業務の効率化が図れるなどの効果が期待できる一方で，例外がもつ残余リスクや，利用部門における心理的作用などに起因する行為や措置などへの留意点も考慮しなくてはならない．これらを理解したうえで例外を適用することが望ましい．

第 3 章では，第 2 章で定めた例外が，社会でどの程度普及しているのかについて，まずは先行事例を調査する．

3. 例外の先行事例

2 章では例外に係る定義と範囲，さらには必要性と限界について述べた．3 章および 4 章では組織での例外措置の実施および例外規程の策定の実態について具体的に探っていく．まず本章では，現在の国内外の例外に関わる先行事例を調査し，その傾向と課題について述べる．

3.1　例外の先行事例を調査するにあたって

今日の情報セキュリティ対策は，技術的・システム的な対策や人材育成・確保や啓発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の一部としての組織的な対応が求められている．その中で情報セキュリティポリシーに則った原則規程を策定し，通常措置の実施に備えることは，どの組織においても必須施策の一つと考える．

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措置を実施し，これを実施することで継続的な業務管理の維持に努め始めている．なお，情報セキュリティポリシーに例外措置を実施することの必要性については，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管理基準（以下，統一管理基準と表す）の推進や[35]，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である[36][37]．

ところで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各種報告書（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 36 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，2018 年度には 290 程度の企業が登録されている[38]．しかしながらセキュリティポリシーに関わる具体的な規程策定や措置の記載について報告されることは少ない．そのため情報セキュリティポリシーに関わる内部規程や情報セキュリティポリシーに記載される例外について，上記報告書等では一般公開されていない．

35) 情報セキュリティ政策会議，“政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）”，平成 26 年 5 月 19 日．(オンライン)．http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf. (アクセス日：2019 年 6 月 10 日)．

36) 日立グループ，“情報セキュリティ報告書 2018”，2018 年 9 月．(オンライン)．http://www.hitachi.co.jp/sustainability/download/pdf/securityreport.pdf. (アクセス日：2019 年 6 月 10 日)

37) 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．

38) 経済産業省，“平成 28 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)．　https://www.meti.go.jp/policy/netsecurity/is-kansa/. (アクセス日：2019 年 6 月 10 日)．

したがって本研究開始当初，第 2 章で定めた研究対象である平常時の対策基準における例外に関する公開文書や報告などは稀有であった．まして「例外規程」そのものをテーマにした先行研究は，本研究で調査した限りでは当初見当たらなかった[39]．おそらく例外に関する取扱いが組織において企業秘密情報であるのではないかと推定され，このことが本研究での調査活動を難しくするものであった．

しかしながら本研究では，第 2 章で定義した用語（例外，例外措置および例外規程）と研究対象（平常時の対策基準）をもとに，情報セキュリティポリシーからの逸脱とそれに対する例外への適用に関する先行事例調査を試みた．具体的には，2.2.3 項で述べた通り，組織での例外措置の実施，および例外規程の策定による例外措置の管理・運用，それらを手掛ける組織内での主体のパターン，さらには例外適用への判断や評価などといった観点で事例を追ってみた．これらの調査の結果に基づき，本章では例外への取り組みを明確に示していると推定した組織や国際規格の事例について紹介する．

ここで，先行事例の内容への理解を補足するために，本研究においての前提事例とした，A 社の例外措置窓口担当者の日常業務をモデル化したものを紹介する．なお，当事例は 2015 年時点のものである[40]．

当該担当者は当時組織の情報システム部門に従事し，IT ユーザ部門からの各種申請・相談窓口を担当していた．窓口は，例外申請やそれに関する事前相談を受けたとき，まず内部規程や実施基準，ガイドラインなどの原則に当てはまるかどうか確認する．次に原則で承認できないと判断した場合，例外措置が事前に明記されているかどうかを調べる．一連の業務フロー例としては図 3-1 のとおりである．

また例外申請の主な相談内容例は以下の通りである．なお本事例は必ずしも実務と合致した事例ではないことを断っておく．

(1) Windows PC のみ接続を認めているイントラネットに，映像加工のための Mac を接続したい．
(2) 特定の外部クラウドサービスの導入を検討しているが，当該クラウドが未だ第三者認証を得ていない．しかし〇〇機能を利用するには他に選択肢がない．

39) この実態から，初出一覧にあるとおり，本研究において精力的に学会発表を行い，自らを先行研究として進めてきた．
40) 当該担当者は筆者自身である．詳細については，初出一覧(5)を参照されたい．なお図 3-1 は図 3-2 を参考に 2015 年に作成しているが，現在（2019 年）も同様の運用であるとは限らない．

(3) USB メモリは原則使用禁止になっているが，○○システムの設計上，外部業者とのデータの受け渡しに使わざるを得ない．

これらの事例に対し，例外規程がない場合には，即時判断できないため業務が滞る事態になる．特に以下の条件のもとでは対応が難しいことが多い．

①承認時間が限られている

②他に選択肢がない

③既に利用している，契約済みである

④承認しなければ現場の実務・サービスが滞ってしまう

当該承認担当者が経験した例外措置へのケースでは，直前での申請・相談を受けることもあり，迅速に内部規程へのあてはめ，上長への報告と承認処理への対応が求められる．類似の例外措置の申請があった場合，その措置に関わる過去の事例を集計・分析しておけば，直前での申請にも迅速な対応が可能ではなかったかと経験上感知していた．しかし当時は過去の対応に基づいてその都度処理し，例外措置をもとに汎用的にルール化を進めることはなかった．

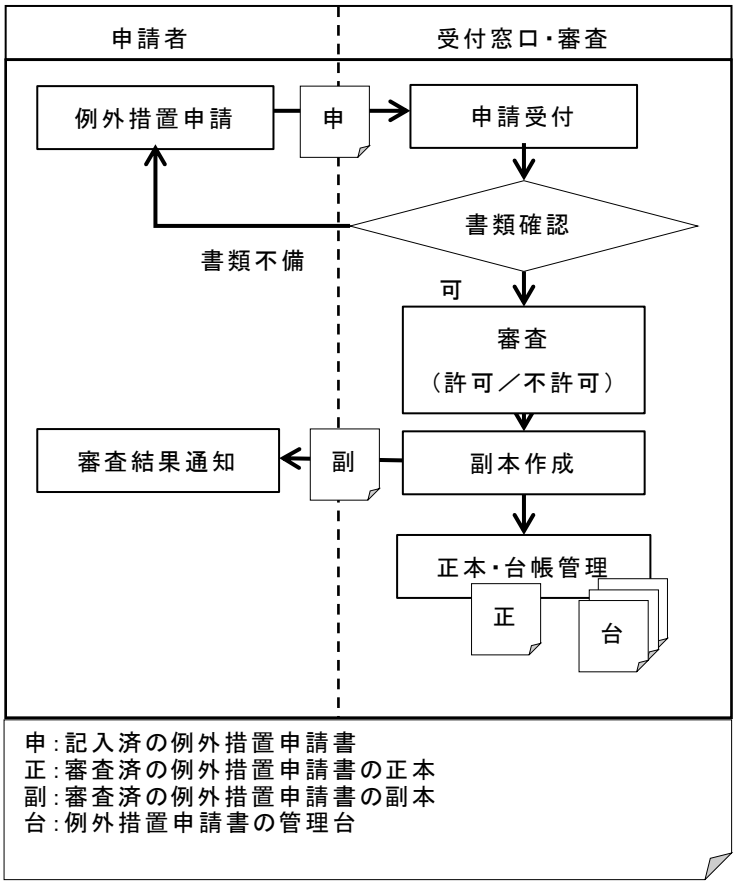

図 3-1 A 社の例外措置の業務フロー例

本事例については，例外措置を実施しているが十分な例外規程を策定しているわけではない．また当該例外措置は平常時の対策基準でのものであり，「例外措置」の管理・運用および策定主体は当該部門である．上記(1)から(3)については例外措置として取り扱っている．

3.2 国内事例

3.2.1 官公庁

例外措置の事例として本論文において最も参考としたのが，官公庁や一部の組織において策定・実施が進められている，NISC の統一管理基準である．

この統一管理基準での例外措置は，NISC が策定するにあたって開催した有識者会議に参画し，情報セキュリティ個人情報保護の担当であった佐藤慶浩氏（当時は日本ヒューレットパッカード株式会社に所属）が，インシデントなどにおける例外措置を中心となって検討し取りまとめた．

以下はこの統一管理基準における例外措置の在り方について示した，佐藤氏の資料の引用とヒアリング（2015 年 8 月実施）から一部加筆したものである[41)]．

「情報セキュリティに対するインシデントに対しては，特に対応手順や体制を整備することが求められている．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いても，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ことに遅れてしまうと，結果的に対応が遅れてしまうことになる．

インシデントへの対応が遅れないようにするためには事後のことばかりではなく，インシデントが発生する前の事象にも広く注意をする必要がある．即ちインシデントの管理の際には，インシデントから始めるのでは不十分な管理策となってしまう．

そこで，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及び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り，インシデントの管理では，インシデントになる前の事象も対象とする管理策を講じなければならない．

41) 佐藤慶浩，“企業における情報セキュリティ対策の実務”， (オンライン). http://yosihiro.com/speech/present-er/2014-11-29b/data/resources/2014-11-29b-enPit.pdf. (アクセス日：2019 年 6 月 10 日).

ここ（統一管理基準）では，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を基本にしている．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．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である．

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，事前に定められた措置とは異なる例外措置ができるようにすることも必要である．統一管理基準ではそのような例外措置についても管理策を講じることについて述べている．」

佐藤氏の知見はインシデント対応を想定しており，本研究においては非常時例外措置への考え方を示している．しかし本研究における平常時例外措置にも転用できるものと考える．

なおNISCは例外措置の手続きの流れ（図 3-2 参照）や様式も定めている[42]．図 3-2 は図 3-1 をさらに詳細に業務フローを定めていることがわかる．特に，管理台帳は許可権限者（管理部門）ではなく，CISO すなわち経営側が担っている点と，審査の際は申請者（利用部門）から疑義・意見のできる機会を与えている点は特徴的である．これは，例外措置が利用部門で実施されることから，現場の業務に適した内容で例外措置が見直される仕組みになっていることと，経営側にも例外措置の実施状況が報告されることで，組織全体として例外措置を管理・運用できる体制になっていることを推定できる．

ところで統一管理基準には例外措置が明記されているものの，例外規程の文言はない．したがって，例外措置の実施は積極的に推進しているものの，例外規程として管理・運用していないものと考える[43]．これはすなわち原則規程そのものに例外措置を策定しているものであり，本論文で述べているように区別した管理体制ではない．なお例外として区別された管理策については，統一管理基準及び統一技術基準などで掲載されている．また管理・運用主体は管理部門であると推定できるものの，部門ごとにカスタマイズを推奨していることから，利用

42) 内閣官房情報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”，内閣サイバーセキュリティセンター，2011 年 4 月．(オンライン)．
https://www.nisc.go.jp/active/general/kijun_man_index.htm. (アクセス日：2019 年 6 月 10 日)．

43) なお，当時の担当者からのヒアリングによれば，「例外措置については、かつては『必要に応じ，○○しても良い』といった抽象的委任が多かったため，自分が担当して時には，『必要に応じ』は認めず，『△△や××の場合等』と必ず例示せよ．その上で『等』を入れるのがやむを得ない場合は許す」という方針を徹底されていたようである．説明責任を明確に求めていたことが推定できる．

部門でも策定・管理・運用している可能性はある. さらに例外措置の実施については, 実際には監査方針とも密接な関係がでてくるため, 政府の監査方針についても対策を講じる必要があると推定する.

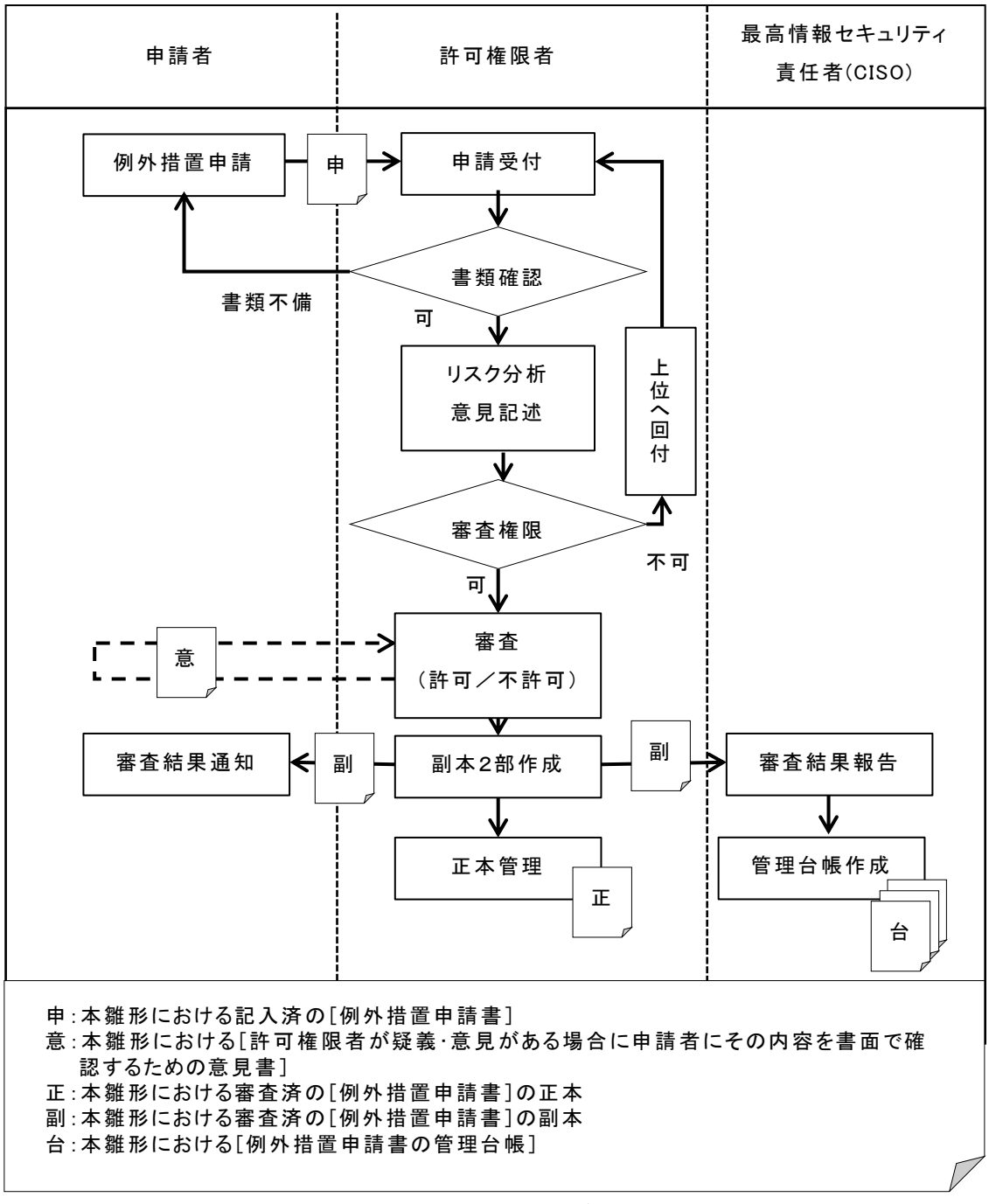

図 3-2 例外措置業務フロー

なお本研究では，4 章以降の 2015 年度アンケート調査での表記の都合上，「統一管理基準」は平成 24 年度版（2012 年）を指すこととする．例外措置に関する策定については，2019 年 9 月 12 日現在，平成 30 年度が最新版である．さらに統一管理基準は，平成 26 年度版（2014 年）以降は統一基準に集約されている[44)45)]．

3.2.2 民間組織

次に国内民間組織についてであるが，佐藤氏からのヒアリングによれば，官公庁以外での例外措置の導入は複数のグローバル IT 企業の日本法人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模様である（2015 年現在）．さらに，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」も当該基準を参考にしているため，金融機関については日本銀行を含め，ほぼすべてにおいて例外措置を導入しているものと考える．

本論文では先行事例調査の段階で，個別に具体的な調査・ヒアリングは実施していない．これは 3.1 節でも述べたようにセキュリティポリシーに関わる具体的な規程策定や措置の記載について報告されることが少なく，例外措置については上記報告書などでは一般公開されていないことから，3.1 節で述べたように企業秘密情報にもつながるものと判断したためである．

しかしながら，上記の組織が政府の統一管理基準に準拠しているならば，例外措置は実施されているものと推定する．一方で例外規程の策定の有無は不明である．仮に例外規程が策定されているならば，その管理・運用は管理部門が担っている可能性がある．また例外として区別する判断については不明である．

44) サイバーセキュリティ戦略本部，“政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）”，平成 28 年 8 月 31 日．(オンライン).https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf. (アクセス日：2019 年 6 月 10 日).

45) サイバーセキュリティ戦略本部，“政府機関の情報セキュリティ対策のための統一基準（平成 30 年度版）”，平成 30 年 7 月 25 日．(オンライン).
https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf. (アクセス日：2019 年 6 月 10 日).

3.3 国際規格・ガイドライン事例

3.3.1 ISMS

ISMS（Information Security Management System：情報セキュリティマネジメントシステム）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について，第三者が審査することを目的とする[46)47)48)49)].

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 [50)51)]. 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が定められている. その中の「12.1 運用の手順及び責任」で「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 操作手順」「12.1.2 変更管理」が記載されている. これら操作手順の e) f)，ならびに変更管理の g) h)に例外措置への対応についての記載がある. これによれば例外措置を認める場合は，例外措置として明確に規程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ことが示されている. すなわち 2013 年度の ISO/IEC27002(2013)にもとづく ISMS への新規の認証審査もしくは更新審査を希望する組織は，例外規程の策定・例外措置の実施が求められることと推定する.

46) ISO/IEC JTC, “ISO/IEC27001:2013”
47) ISO/IEC JTC, “ISO/IEC27002:2013”
48) 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.
49) 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.
50) 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.
51) 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.

「12.1.1 **操作手順書**」（抜粋）

管理策:

操作手順は，文書化し，必要とする全ての利用者に対して利用可能とすることが望ましい

実施の手引き：

情報処理設備及び通信設備に関連する操作（例えば，コンピュータの起動・停止の手順，バックアップ，装置の保守，媒体の取扱い，コンピュータ室及びメールの取扱いの管理・安全）の手順書を作成することが望ましい．

操作手順には，次の事項を含む，操作上の指示を明記することが望ましい．

e) **作業中に発生し得る，誤り又はその他の例外状況の処理についての指示．これには，システムユーティリティの利用の制限を含む．**

f) **操作上又は技術上の不測の問題が発生した場合の，外部のサポート用連絡先を含む，サポート用及び段階的取扱い（escalation）用の連絡先**

システムの管理活動のための操作手順及び文書化手順は，正式な文書として取り扱い，その手順書の変更は，管理層によって認可されることが望ましい．技術的に可能であれば，情報システムは，同一の手順，ツール及びユーティリティを用いて，首尾一貫した管理を行うことが望ましい．

「12.1.2 **変更管理**」（抜粋）

管理策：

情報セキュリティに影響を与える，組織，業務プロセス，情報処理設備及びシステムの変更は，管理することが望ましい

実施の手引き：

この管理策の実施については，特に，次の事項を考慮することが望ましい．

g) **うまくいかない変更及びこれに伴う予期できない事象を取り消し，これらから回復する手順及び責任を含む，代替手順**

h) **インシデントの解決のために必要な変更を，迅速にかつ管理して実施できるようにするための，非常時の変更プロセスの提供（16.1 参照）**

あらゆる変更の十分な管理を確実にするためには，正式な責任体制及び手順を備えていることが望ましい．変更がなされたときには，変更に関わる全ての関連情報を含んだ監査ログを保持することが望ましい．

関連情報：

情報処理設備及びシステムの変更に対する不十分な管理は，システム又はセキュリティ不具合の一般的な原因となる．特に，システムを開発ステージから運用ステージに移す段階では，運用環境の変更は，アプリケーションの信頼性に影響を及ぼすことがある

しかし一方で ISMS では積極的に例外措置による運用を奨励しているわけではない. 2013 年版では当該記載自体が実は「例外」として残されたものとされている. すなわち ISMS においては, 原則規程によってできる限り事前にあらゆる事象を想定して運用し, 例外措置はなるべく少なくすることが望ましいと考えられている. そして例外措置をむやみに認めることは運用範囲が曖昧になり, セキュリティ確保が難しくなるおそれがあるとされている.

したがって ISO/IEC27002:2013 では個別具体的な「実施の手引き」や関連情報に例示を記載しているわけではない. すなわち, より具体的な規程策定や措置手順については各組織に委ねられていると考える.

ちなみに 2002 年版（ISO/IEC17799:2000）においては, 上記該当箇所である 10 章「システムの開発及び保守」にて 10.1 節「システムのセキュリティ要求事項」の 10.1.1 項「セキュリティ要件事項の分析及び明示」では, 例外措置を明確に取り扱う管理施策ではなかったことがわかっている. その後, ISMS の世界的な展開などの経緯をふまえて 2013 年版に改訂されていることに鑑みると, 欧米諸国においても, 例外措置を用いた管理基準の策定・運用が必要になったと推定することができる.

したがって ISMS 準拠の組織であれば例外措置は実施されており, 例外規程の策定も一部で見られる可能性はある. 管理・運用主体は管理部門であると推定する. 通常措置と例外措置の区別については, 例外規程が策定されているならば明記されている可能性はある.

2002 年改訂版（ISO/IEC17799:2000）
10 章「システムの開発及び保守」
10.1 節「システムのセキュリティ要求事項」
10.1.1 項「セキュリティ要件事項の分析及び明示」（抜粋）

「（前略）セキュリティが確保できなった場合，又はセキュリティが確保されていない場合に起こると思われる業務上の損害の可能性もその要求事項及び管理策に反映されることが望ましい．セキュリティ要求事項を分析し，この溶融事項を満たすための管理策を明確にするための枠組みが，リスクアセスメント及びリスクマネジメントである．（後略）」

3.3.2 米国 NIST

NIST （National Institute of Standards and Technology，米国国立標準技術研究所）は米国規格であるが，日本をはじめ諸外国の組織における情報セキュリティポリシーの策定や情報セキュリティ監査基準等でも参照されていることから，本研究では国際規格に準ずる規格として取り上げる．

NIST は”Guide for Security Focused Configuration Management of Information Systems”にて，情報セキュリティには，組織の全体的な CM（Configuration Management：構成管理）が不可欠であり，CM の情報システムのセキュリティ面を実装した，SecCM（Security-focused Configuration Management：セキュリティ構成管理）を提唱し，情報セキュリティの集中管理を主張している[52)53)54)55)56)]．

SecCM はセキュリティを実現するための情報システムの構成の管理と制御として定義され，「IT ビジネスアプリケーションの機能」と「セキュリティに重点を置いた訓練」の両方を単一のプロセスとして統合することが期待されている．この SecCM 訓練に例外措置が明記されている．

SecCM ではまずセキュリティで保護された構成設定を確立するための基本として，一般的なセキュリティ構成を検討する．構成設定に関してはナショナルチェックリストプログラム (http://checklists.nist.gov) を参照する．これらのチェックリストは，幅広い商用製品を網羅しており，SCAP (Security Content Automation Protocol)対応ツールによる自動評価を容易にするために標準化された形式で書かれている．

次にセキュリティで保護された構成を開発し，組織全体の一貫性を確保するためのトップダウンアプローチで実装することで，確立されたドメイン全体にわたって，安全な構成ポリシーを一元的に配布できるようにする．一方で，ローカルの制約や要件をサポートするために特定の情報システムの構成を調整するために，組織ごとの情報セキュリティポリシーの例外を必要とする場合があることを策定している．この例外措置は必ず文書化し，その情報システムのベースライン構成の一部として承認することを求めている．

このように，NIST が提供する情報セキュリティに関する規格の一部にも，例外

52) NIST, “SP800・FIPS”, (オンライン). http://csrc.nist.gov/publications/PubsSPs.html. (アクセス日：2019 年 6 月 10 日).
53) NIST, “Information Security Handbook: A Guide for Managers”, NIST Special Publication 800-100, 2006.
54) NIST, “Information Security Guide For Government Executives”, NISTIR 7359, 2007.
55) NIST, “Guide for Security-Focused Configuration Management of Information Systems”, NIST Special Publication 800-128, 2011.
56) NIST, “Guide to General Server Security”, NIST Special Publication 800-123, 2008.

措置に関わる申請・承認手続きが付加されていることが分かる．また文書化を求めていることから，一部は例外規程として策定されている可能性がある．非常時のみならず平常時の対策基準でも適用されているものと考えられるため，例外措置も当該基準に適用されているものと推定する．例外措置の管理・運用は，ローカルでの制約などを考慮していることから，管理部門・利用部門それぞれで担っている可能性がある．仮に例外規程があるならば，その策定についても管理部門・利用部門それぞれで担っていると考えられ，原則規程と区別しているものと推定する．

3.4　海外事例

3.4.1 日本企業海外法人

本研究では日本企業のある米国法人での例として,「例外処理におけるガイドラインと手順（Exception Handling Guidelines and Procedures）」[57]の考え方を紹介する. なお本事例についても一般に公開されていないため, ヒアリング（2015 年実施）によって得た法人の考え方を紹介する.

各項目と主な内容を表 3-1 に示す. 統一管理基準と同様, 原則規程では対処が難しい事象に対して例外を適用しているが, 特徴として 2 点あげられる.

一つは原則規程からのコンプライアンス違反について「逸脱（deviation）」を定義し, その逸脱の範囲を厳密に選定したうえで, 例外規程を策定している点である. これにより例外措置が与えるリスクをできる限り把握する仕組みができていると考える.

もう一つは例外規程を策定するにあたり, 原則規程から逸脱しなくてはならない事由を必ず提出させている点である. 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）」の考えに帰するものである. 例外措置の適用を申請するのであれば, 申請部門に対して説明責任を負わせる. これにより例外措置によって起こりうるリスクを理解させ, 情報セキュリティの確保を図っていく.

なお, この「Comply or Explain」の考えについては, 日本社会においても通用・活用されてきている. 例えば, 金融庁及び東京証券取引所を共同事務局とする「コーポレートガバナンス・コードの策定に関する有識者会議」では, 上場企業がそれぞれ実現を目指す企業統治のあり方を, 当該会議が提案しているコーポレートガバナンス・コードに照合する際に,「Comply or Explain」の導入を提案している[58].

本事例は, 数少ない例外規程を例示できたものである. 例外規程を策定した上で平常時の対策基準での例外措置として実施されている. 管理・運用は管理部門が担うが, 様々な利用部門に柔軟に対応できるよう協調して策定している傾向にもあるという. 内容については企業秘密であり示されていないが, 例外として区別する判断についても組織内でなされているものと推定する.

57) 実際の規程名称のため「例外処理～」とそのまま掲載している
58) 山内達夫, “コーポレートガバナンス・コードの基本的な考え方（案）の解説”, テクニカルセンター 会計情報, vol.463, 2015.

表 3-1 例外処理におけるガイドラインと手順（抜粋）

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。

3.4.2 欧州医薬品庁

欧州医薬品庁(EMA, European Medicines Agency)は 1995 年に設立され, EU 内の既存医薬品規制当局における業務の協調を目的に, EU と製薬業界からの資金提供と加盟国からの間接的な補助金で設立された(本部ロンドン).

この欧州医薬品庁における標準的な操作手順書において,「例外および法令順守非適用事象への要求と記録」に関する手引きがある[59]. この中で, 例外と違反を以下のように定義している. なお原文は英語で表記されており筆者が和訳している.

> 例外：
> 確立された手順（確立された手順の 1 つまたは複数のステップを別の手段に置換または手段を省略する行為）または制御のオーバーライド（以前の制御結果に反する行為）からの逸脱であるが, 規制または契約上の規程（例：欧州医薬品庁外の事業体との契約）が遵守されており, 既存の手順では予見できず, 措置が講じられる前に責任者が事前承認するもの.
> 違反：
> 確立された手順からの逸脱, または既存の規制における制御の差し替え, 契約上の規程に違反する可能性があって, 行為が取られた後に検出されるもの. ここでいう手順とは, 例えば内部実装ルール, マニュアル, ガイドラインなどを指す.

これらをもとに, 所定の申請書によって例外申請を受け付ける手順となっている.

なお, 例外措置の申請・承認手続きを運用している組織は他にもみられる. (本研究で調べた限りでは, 例えば, 米国アトランタ州 Children's Healthcare of Atlanta 社[60], 米国ミシガン州 INFORSEC INSTITUTE[61], 英国 Birmingham and Solihull Mental Health NHS Foundation Trust[62]など)

上記機関を調査した限りでは, 例外措置の実施は認められるものの例外規程

59) European Medicines Agency, "Requesting and recording of exceptions and non-compliance events, Standard", European Medicines Agency Standard operation procedure, 2018.
60) Children's Healthcare of Atlanta, "Information Management, Administrative and Operational Policies and Procedures", (オンライン). https://www.choa.org/~/media/files/Childrens/research/it-technology-acceptable-use-form.pdf?la=en/ (アクセス日: 2019 年 6 月 10 日).
61) Inforsec Institute, "Exception Management - InfoSec Resources" - (オンライン). https://resources.infosecinstitute.com/exception-management/#gref. (アクセス日: 2019 年 6 月 10 日).
62) Birmingham and Solihull Mental Health NHS Foundation Trust, "information systems security policy (issp)". (オンライン). https://www.bsmhft.nhs.uk/EasysiteWeb/getresource.axd?AssetID=4448&type=full&servicetype=Attachment. (アクセス日: 2019 年 6 月 10 日).

を策定しているかどうかは不明であった. 管理・運用主体は管理部門のみであると考える. また例外として区別する判断については明らかではないが, 申請書から推定するに, 自組織管理のシステムやサービスにおいて, 通常と異なる運用をする場合や, 自組織管理外のシステムを自組織内で利用する場合において, 例外措置の対象とするものと考えられる.

3.5　海外の大学での先行事例

海外事例を調査するに従い，海外の大学での事例がある程度占めたことから，本節では大学の事例として分けて，例外措置の運用について紹介する．大学では，一つの大きい組織として統一的な方針を立てて，情報セキュリティに対応しているが，研究内容によって変更しなければならない．そのため例外措置を設けているところが多い．以下にその例を示す．

3.5.1 米国　ジョージア工科大学

米国ジョージア工科大学（Georgia Institute of Technology）では，予め大学における情報セキュリティポリシーが，申請する項目ごと（例えば，コンピュータネットワークセキュリティ手順，データアクセスポリシー等）に閲覧できるようになっている．その上で希望する項目での例外を申請するために，以下の項目を所定の申請書に明確に記載した上で，所定の電子メールアドレスに送信する手順となっている[63)]．

例外適用申請情報
- 例外適用を要求する理由を明記する．
- 例外措置が適用されるシステムまたはネットワークの一覧を明記する．マシン名と IP アドレスの一覧も記載する．
- 機密性の高いまたはビジネスクリティカルなデータが含まれる場合は列挙する．
- 潜在的なリスクを軽減するために，全て緩和策を記載する．

なお例外措置の有効期間は最初の例外承認日から最大 12 か月とされ，更新または終了を希望する場合は，承認決定を受けるためのレビューが必須となっている．このように例外措置の申請にあたっては，その理由を示し，実施内容と不具合時への対処方法の明記が，予め求められていることがわかる．

なお例外規程を策定しているかどうかは不明である．管理・運用主体は管理部門のみと推定する．例外として区別する判断については明らかではないが，申請情報の記載項目から，大学管理のシステムやサービスにおいて，通常と異なる運用をする場合に例外措置の対象とするものと考える．

63) Georgia Institute of Technology, “Policy Exceptions”, (オンライン). https://policylibrary.gatech.edu/information-technology/policy-exceptions. (アクセス日：2019 年 6 月 10 日).

3.5.2 米国　ルイビル大学

米国ケンタッキー州のルイビル大学（University of Louisville）では，情報セキュリティを専門に取り扱う事務局が，大学の情報資産にかかる C.I.A.（Confidentiality；秘匿性，Integrity；完全性，Availability；可用性）を管理・運用する目的で，学生・教職員向けに下記の項目で構成された情報セキュリティプログラムを提供し公開している．

- 情報セキュリティのポリシー，基準，ガイドラインの開発とコミュニケーション
- 情報セキュリティの意識向上とトレーニング
- 情報セキュリティのインシデント対応
- 識別，評価，情報セキュリティ上のリスクの軽減
- 大学のコンプライアンスへの取り組みや情報セキュリティ関連プログラムのサポート

この中の情報セキュリティポリシーおよび基準において，例外措置の申請規則が明記しており，これに基づいて申請者が例外申請を行う手続きとなっている．当該規則の概要は以下の通りである[64]．

「規制，コンプライアンス，C.I.A.要件など情報セキュリティに関する事項は，大学が一元的にサポートまたは推奨する規程に基づくのが望ましいが，全ての学部や研究室等において常に適用できないことは理解している．したがって原則的には，一元的にサポートあるいは推奨された技術手法からの逸脱は認めない．しかし正当なビジネス目的や研究目的がある場合において，適切な代替技術手段を実施し，管理維持でき，既存の大学の運営方針と標準に相当するのであれば，例外を考慮することがある．」

この内容は，他の事例と同様に，例外措置の承認には，原則規程と同等のリスク軽減が代替手段によって期待できることを条件の一つにしている．また例外措置のプロセスを遵守するよう厳格に定められていることから，例外措置からの逸脱は認めないことが明らかである．以下は例外措置の申請プロセスである．

64) University of Louisville, “Policy Exception Process”, (オンライン).https://louisville.edu/security/policies/policy-exception-process. (アクセス日：2019 年 6 月 10 日).

実施基準:

情報セキュリティポリシーや基準に準拠できない学校，部署，または他の団体は，セキュリティ上の例外を提出する必要がある．簡易的な例外申請を除き，申請時において代替手段または技術的にかかる直接的／間接的な費用を提示する必要がある．「情報セキュリティポリシー例外リクエストテンプレート」(以下を参照)を利用し，法律，規制，大学政策，想定されるリスク，規制環境に合致する技術的，物理的および行政上の要件を記載すること．

申請・承認の流れ：

1. 予備審査：
   例外申請書を完成させる前に，申請書の初期書式をもとにオンライン伺いを送信し，事前審査を受ける．

2. 例外申請書の提出
   受容可能な潜在的なリスクレベルであり，大学管理の適切なレベルであることが承認の条件であり，（責任者の）サインの記載が必要

   ビジネスおよび/または研究内容：
   - （標準・応用）技術およびプロセス，該当するポリシー番号など．
   - サポートされている，または推奨されている技術手法または標準が，IT を含む申請要件を満たさない事由．
   - 管理センターが管理制御するための手段
   - 実施に必要なライセンスのコスト，ハードウェア，ソフトウエア，インフラ，トレーニングや手続き文書，行政およびサポート担当者，一時的なコンサルタント，災害復旧，バックアップ，ビジネス継続性，およびサポートするための資金調達を含む実装方法やメンテナンスに係るコストを予測する技術的手法

   データ評価：
   - データの定義
   - 希望するユーザ（教員，職員，研究員，学生，臨床技師など）のデータ
   - 法律/規制（HIPAA，FERPA，PCI，NIH の要件，その他の法律や規制など），一般的なプライバシーまたは知的財産等に関する懸念事項，大学の方針及び/又は慎重な実践によるデータアクセス制限要件．
   - このデータとアクセスを管理し，オペレーティングシステム，データベース，アプリケーションおよびその他の手段によるハードウェアおよびその他の関連インフラストラクチャの物理的なセキュリティを含む論理セキュリティを含むセキュリティ方法論．

   実施計画
   - プロジェクト実施計画とリソース，実施に向けたタイムライン．

   保全計画
   - 継続的な保守，管理，ユーザートレーニング，偶発事象に特化した計画とリソース．

3. 申請書は審査委員会での審査
委員会には，情報セキュリティ責任者（ISO）および情報技術（IT）の代表者ならびにアドバイザリー能力のある監査サービスが含まれること．
- リスク受諾書
- 委員会は，担当エンティティのリスク受諾書を完成させる．この文書は，実施者が想定しているリスクを特定するものである．この書式は，当該提案が実施のために承認されている場合には，委員会の文書の評価（上記のとおり）に基づいて文書化される．
- リスク受諾書，受け入れ承認と署名は副学長が行う．この承認は，管理者がプロジェクトとシステムに内在するリスクを認識し，それを受け入れ，エンティティリソースを使用してシステムを維持し，発生するリスクイベントを軽減することが文書化されている．

特別な状況を除き，徹底して完全な提案があれば，審査委員会は受領後 30 日以内に提案書を審査し承認する．
承認された場合，申請者は実施を続行する．IT のサブジェクトマターエキスパート（SME）は，計画または適切な変更の遵守の実施状況を監視する．実装が計画通りに進めば，技術またはプロセスは生産に移行することができる．
注： SME はプロジェクトマネージャーではないこと．
例外の申請が却下された場合，または計画どおりに実施できない場合，申請者は修正するか，代替ソリューションを探すことができる．

4. 今後のレビューまたは監査
監査サービス，情報セキュリティ，組織のコンプライアンス，IT または大学のマネジメントについては，計画，セキュリティなどが継続的に遵守されているかどうか技術的審査を行うことがある．

実施責任：

政策当局/施行：大学の情報セキュリティ責任者（ISO）は，これらの方針と基準の開発，公表，変更，監督を担当する．ISO は，大学のリーダーシップ，情報技術，監査サービスなどと連携して，これらのポリシーと標準の開発，監視，実施を行う．
ポリシーの遵守：これらのポリシー，基準，および/または関連する情報セキュリティポリシー，標準または手続きを遵守しないと，地方自治体の条例，州法または連邦法に従い，雇用，サービスまたは大学との関係の終了を含む懲戒処分が発生する可能性がある．

例外措置の申請プロセスを見る限り，当該大学の事例は例外規程を策定しているのと同等であると考える．また管理・運用主体は管理部門のみと推定する．なお例外として区別する判断については明らかではない．

3.5.3 英国 ノッティンガム大学

ノッティンガム大学（University of Nottingham）は，英国ノッティンガム市にキャンパスを置く，1881 年設立の大規模研究型大学である．設立当初はロンドン大学のカレッジであったが，1948 年にノッティンガム大学として独立．アジア・パシフィック地域との連携強化のため，マレーシア・中国にもキャンパスを開校し，イギリスの中でもグローバル度の高い大学とされている．

当大学でのセキュリティポリシーは，情報システムおよびその運用，インフラ，あるいは大学の評判に影響を及ぼす可能性のある情報など，セキュリティ問題から大学を守ることを目的としている．さらに大学のすべてのメンバーに情報セキ

ュリティ問題への意識を高めることも掲げている.

情報セキュリティポリシーは下記の項目ごとにそれぞれ定義, 策定されている.

情報セキュリティポリシー定義項目
- アンチウイルス対策
- 情報資産運用管理
- 監査
- PC, モバイル機器
- ダイアルアウト
- 電子メール
- 暗号化
- ネットワークモニタリング
  （ネットワーク制御・接続, パスワード, 物理的セキュリティ, リモートアクセス, サーバセキュリティ, サードパーティのリモートアクセス）

この情報セキュリティポリシーにおけるいくつかの項目に例外措置が明記されている. 例えば, 個人利用の PC やサーバへのセキュリティパッチ, 大学キャンパスからのダイアルアウトアクセス, ワイアレスアクセスポイントへの接続, サードパーティのリモートアクセスサービスなどがある[65].

例外申請への承認には, CIO (Chief Information Officer;最高情報責任者)あるいは CIO などが指名した人, もしくは UEB (大学執行委員会)の判断による事前承認が必要となっている.

例外規程を策定しているかどうかは不明である. 管理・運用主体は管理部門のみであると考える. また例外として区別する判断については, 内容は明らかではないが, 上記ポリシーにて明記されているものと推定する.

なお, 例外措置の申請・承認手続きを運用している組織は他にもみられる. （本研究で調べた限りでは, 例えば, 米国オハイオ州 Youngstown state university[66], フィンランド VAMK(University of applied sciences)[67]など）

いずれも他大学と同様の傾向にあると推定している.

65) The University of Nottingham, “Information Security Policy 2015/16”, (オンライン) .https://www.nottingham.ac.uk/legalservices/documents/information-security-policy.pdf. (アクセス日: 2019 年 6 月 10 日).
66) Youngstown state university, “Overview of IT Security Waivers and Exceptions”, (オンライン).https://cms.ysu.edu/administrative-offices/it-security-services/overview-it-security-waivers-and-exceptions. (アクセス日: 2019 年 6 月 10 日).
67) VAMK(University of applied sciences), “Information Security Policy”, (オンライン). http://www.puv.fi/en/study/it-basics/rules/policy/. (アクセス日: 2019 年 6 月 10 日).

3.6　先行事例・調査からの考察

例外措置に関する国内外の先行事例を調査した結果，以下の点が明らかになった．

まず国内では，政府が統一管理基準によって例外措置への対応を明記しており，情報セキュリティ対策での例外措置の必要性を示している．さらには申請・承認における過程を図示し，各省庁で導入しやすいように工夫している．この統一管理基準をもとに省庁や関連組織だけでなく，金融など民間企業の一部でも例外措置が実施されていることがわかった．

しかしながら，政府統一管理基準では例外規程の記載がなく，例外規程として策定しているのかどうかは本調査だけでは明らかにはならなかった．例外規程については，組織の情報セキュリティポリシーが盛り込まれた内部規程が非公開であることが多いことから，先行事例が少ないものと推定する．

次に国際規格・ガイドラインでは，ISMS に例外措置の管理・運用が含められていることから，ISMS の認定を受けている（受けようとしている）組織であれば，例外措置の活用は必要であると考える．さらには 2013 年の ISO/IEC27002 改正に際して例外事項が残されたことは，欧米諸国にも情報セキュリティにおける例外措置の必要性があるものと推定できる．おそらく例外規程としては明記せず，原則規程を改定する中で例外措置として実施し，例外規程の概念を取り入れている事例が存在するのではないかと考える．

一方，欧米での民間組織や大学の一部でも，例外措置への申請・承認・運用の事例が見られた．このことから海外の事例においても，例外規程として予め策定しているとみなせるところが一部あるものと推定する．例えば例外規程を策定する際には，予め原則規程からの逸脱を把握し，管理部門が利用部門に対し「Comply or Explain」を求める事例がみられた．あるいは承認された例外措置範囲から逸脱する行為は違反の対象となることを，管理部門から利用部門に示すことで，事後の利用者側の責任所在を明確に与える事例もあった．

しかしながら，本論文での先行事例調査の範囲では，多くの組織が例外規程を策定して例外措置を実施しているかどうかを判定することはできなかった．また調査した全ての組織が，非常時のみならず平常時の対策基準での例外措置を実施していることはわかったものの，管理・運用の主体部門については，管理部門が多いものと推定するに留まった．さらに通常措置と例外措置の区別については，多くの組織が不明であった．

本考察をさらに第 2 章の用語，さらには必要性と限界での観点で再考してみる．例外措置という用語は利用されているが，例外規程（英単語では

exceptional rules あるは exception(al) regulation ほか近似ワードなど）は明確に見当たらなかった. 3.4.1 項の事例では「例外規定」とされているが, これは本論文での「例外規程」とみなせば, 本論文での唯一の活用例ではないかと考える. また調査した全ての組織が, 平常時の対策基準での例外措置を実施していることはわかった.

例外の必要性については, どの先行事例においても具体的に記述されてはいなかった. しかし例外規程を策定していた組織の事例（3.4.1 項, あるいは 3.5.2 項も含まれる可能性あり）では, 業務効率を図る目的で例外規程への必要性があるのではないかと推定する. さらに例外が持つ限界への取り組みとしては, 事前の例外申請がない逸脱行為は違反と断定され, 罰則の対象と明記している組織が多い（3.4.1 項, 3.5.1 項, 3.5.3 項）. これは厳罰化への具体的な取り組みを示す上で興味深い結果である. さらに利用部門での例外からの逸脱も認めない事例（3.5.2 項）も見られた. これらの知見により, 本調査において例外の必要性や限界に関わる先行事例が最低限得られたものと考える.

小括

本章では，例外の実態を把握するために，研究対象である「平常時の対策基準における例外」に関する先行事例（国内事例，国際規格事例，海外事例）の調査結果を紹介した．

本論文において最も参考としたのが例外措置を体系的に記述している NISC の統一管理基準である．これをもとに日本では省庁や関連組織だけでなく，金融機関等の民間企業の一部で例外措置が実施されていることがわかった．また ISMS 認定を受けている組織であれば，例外措置の導入が不可欠であると考える．さらに国際規格や海外の企業の事例では，一部の組織がすでに例外規程を導入し，例外措置の申請・承認・運用がなされている．さらに事前の例外申請がない逸脱行為は違反と認定され罰則の対象と明記している組織が多いことも興味深い．

しかし，先行事例の多くは申請手続きに関するものが多く，組織が例外規程を策定して例外措置を実施しているかどうかについては判定することはできなかった．また管理・運用の主体部門については，管理部門が多いと推定できないものの断定はできなかった．さらにどのような原則規程からの逸脱行為が例外措置とされているかについては，多くの組織が不明であった．例外規程や例外措置の実態に関する包括的な統計資料を取り扱った文献もなかった．

先行事例調査から，例外措置を実施しているだけでなく，例外規程によって管理・運用している組織では，業務の効率化が図られているものと推定する．しかし直接的に公表されているわけではないことから明確に判定することはできなかった．

そこで本研究では，直接組織に例外措置の実施及び例外規程の策定における実態について回答を求めるために，第4章のアンケート調査の実施につなげていくことにした．

4. 例外の実態の把握

第 3 章の先行事例調査では，原則規程からの逸脱に対し，例外措置の適用と違反とを区別している組織，また例外措置の申請・承認・運用手順を活用している複数の組織について把握することができた．一方で，組織が例外規程を策定して例外措置を実施しているかどうかを判定することはできなかった．また調査した全ての組織が，非常時のみならず平常時の対策基準での例外措置を実施していることがわかったものの，管理・運用の主体部門については，管理部門が多いと推定するに留まった．

本章では，第 3 章の結果を受けて，例外措置の実態を把握するために実施したアンケート調査について述べ，調査結果から課題と対策に向けて述べる．

4.1　アンケート調査における例外に関する「想定」

本研究では，組織における例外規程および例外措置の実態と効果を把握するために，第 2 章の用語の定義と研究対象をもとに，3.6 節の考察から表 4-1 に示す例外に関する 8 つの「想定」[68]をたてた．

表 4-1 例外に関する想定

（想定 1）	例外規程はある程度普及している
（想定 2）	内部規程にない例外措置は，経営判断だけでなく，現場判断でも実施できる
（想定 3）	例外規程の策定時は，他の先行事例等を参考にしている
（想定 4）	例外規程は，現場組織によって異なっている
（想定 5）	例外規程は定期的に見直されている
（想定 6）	例外措置の実施手順を明記し，特に罰則とセットにしている
（想定 7）	原則規程か例外規程かのどちらを策定するかの傾向がわかる
（想定 8）	例外規程への評価を定量的に明示化でき，セキュリティ上の満足度が分かりやすくなる

「想定」は第 2 章及び 3.6 節の考察から，次のような根拠をもとに設定している．まず例外規程の策定実態を把握するために，例外規程がある程度普及して

68) 本研究での「想定」については，いわゆる自然科学で取り扱われる「仮説」の設定で求められる厳密な検証・検定を要しているものではないとする

いるとして,「想定 1」を設定した. 次に例外規程を策定, 管理・運用する組織の主体部門を調べるため, 例外措置は部門ごとでも実施しており(想定 2), その上で規程を策定する際は, 他の先行事例を参考にしながら(想定 3), 部門ごと(設問では現場組織)に異なったものを策定する(想定 4)ものとして設定した.

次に, 例外は原則の補完であり, 一時的な規程・措置であることから, 例外規程は定期的に見直されているとして「想定 5」を設定した. さらに, 例外の限界による厳罰化への留意点から, 例外規程には罰則をセットにしているとして「想定 6」を設定した.

そして組織における管理策において, そもそも原則規程としているのか例外規程としているのかをたずねることで, 例外規程を策定する傾向を知ることができるとして「想定 7」を設定した. 最後に, 例外規程の効用であり業務効率の向上を知る一つの手段として, 例外規程への評価を定量的に明示化でき, セキュリティ上の満足度が分かりやすくなるとして「想定 8」を設定した.

なお, このうち想定 1 から想定 6 については, 例外の実態に関する「想定」とし, NISC の統一管理基準も参考にして設定した. これは, 統一管理基準が例外措置を具体的に実施するための手順やひな形を提供している点, 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. これらが組織によって実施されているか調査することは, 統一管理基準の必要性が明らかになることにつながるとも考える. また想定 7 及び想定 8 は, 例外規程に関する評価について「想定」としたものである. なお「想定」を設定するにあたっては, これまでの筆者の実務経験も考慮している.

本研究では,「想定」を検証する手段として 4.2 節以降に述べるアンケート調査を利用している. 想定 1 から想定 7 については本章, そして想定 8 については付録第 A1 章でそれぞれ分析・考察している.

4.2　2015 年度アンケート調査

4.1 節で設定した「想定」をもとに例外措置の実態を把握するためにアンケート調査を実施した[69].

4.2.1 アンケート調査実施内容（全体）

各組織で情報セキュリティに関わる例外措置および例外規程の実態を把握するために, 2015 年度の情報セキュリティ大学院大学原田研究室で実施したアンケートの一部（第 3 章）として, 例外措置に関連する設問を盛り込んだ.

当研究室では 2015 年 8 月に「情報セキュリティ調査」アンケートを郵送にて実施した. 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, 官公庁, 教育機関などから選んだ 4,500 組織（送達確認できたのは 4,373 組織）である. その結果 352 件（8.0%）の回答が得られた. なお, 本調査においては回答の未記入および択一問題における重複回答等の無効回答は, 無回答として計上している[70]

表 4-2 アンケート設問（要約. 参考文献 69 より一部加筆）

[設問 14]	例外規程の有無
[設問 15]	例外規程にない例外措置の承認手段
[設問 16]	具体的な業務上の事象において, 例外措置の有無
[設問 17]	内部規程に例外措置がない事象への一時的措置として最初にとる手段
[設問 18]	例外規程の新規策定時の参考元
[設問 19]	例外規程の策定部門
[設問 20]	例外規程は, 組織全体での統一規程か, 現場組織ごとの規程か
[設問 21]	例外措置の実施手順の記載の有無
[設問 22]	例外規程の見直し頻度
[設問 23]	例外規程による効果への主観的評価

69) 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” , (オンライン). http://lab.iisec.ac.jp/~harada_lab/survey/2015.html.
70) 村﨑康博ほか, “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, 2016

4.2.2 アンケート設問

表 4-1 の想定に基づいて作成したアンケートの設問を表 4-2 に示す. 本研究では全アンケート設問のうち「設問 14」から「設問 23」までが例外規程に関する設問である.

アンケートではまず例外についての用語解説を冒頭に明記した[71]. 次に経営側・現場側どちらの立場から回答されるかを把握しつつ, 特に利用部門(現場側)でもボトムアップ的な例外措置の取扱いの有無が得られるよう, 具体的な管理策を提示し, それに対する措置としてイメージしてもらえるよう工夫した.

以下, 本節ではアンケート調査の結果のうち, 例外規程の実態を示す想定 1 から想定 6 について示す. 想定 7 については 4.6 節で, 想定 8 については付録 A1 章にて述べる.

71) 本アンケート票の用語説明においては, 例外措置を「情報セキュリティ関連規定に基づいて業務を遂行するにあたり、当該規定へ適用させることが適正な業務遂行を著しく妨げる等の理由により、当該規定とは異なる代替の方法を採用すること又は規定を実施しないことを認めざるを得ない場合にとる手続きをさす。」と定義している. さらに「例外措置が当該関連規定に記載されている箇所」を例外規定(当初の用語)と説明した上で回答してもらった.

4.2.3 調査結果 1:例外規程の有無(想定1, 設問 14)

想定1では「例外規程はある程度普及している」に基づいて設問 14 を設定し, 質問した.

設問 14 の結果を図 4-1 に示す. 本設問では内部規程全般において「例外規程」の項目の有無についてたずねている. 結果は, 青色系の「すべて/一部例外措置に内部規程にある」割合と, 赤色の「内部規程にない」割合が同じ(42%)であった.

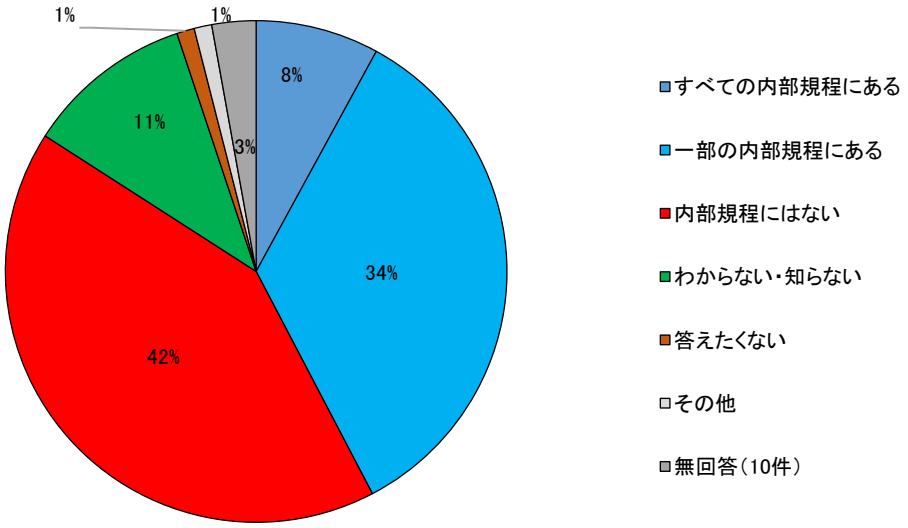

図 4-1 情報セキュリティに関わる内部規程全般において「例外規程」の有無
(択一, N=352)

次に業種別にクロス分析し, 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 4-2 に示す. 図 4-2 より「情報通信業」と「サービス業」では 50%が, 「すべての内部規程にある」もしくは「一部の内部規程にある」ことが分かる.

一方「公務(政府・自治体)」の場合は「内部規程にはない」が 24%あり, 「大学」では半数以上(53%)に及んでいる.

これらの結果から, 公務・大学における想定 1 については, 例外規程について策定の有無が同程度であることから, 例外規程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, これらの業界では情報技術の依存度が高く技術進歩の影響を受けるため, 例外規程が他の業界と比べて必要となっていると考える.

一方，政府・自治体では，統一管理基準によって例外規程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進んでいるものと推定する．

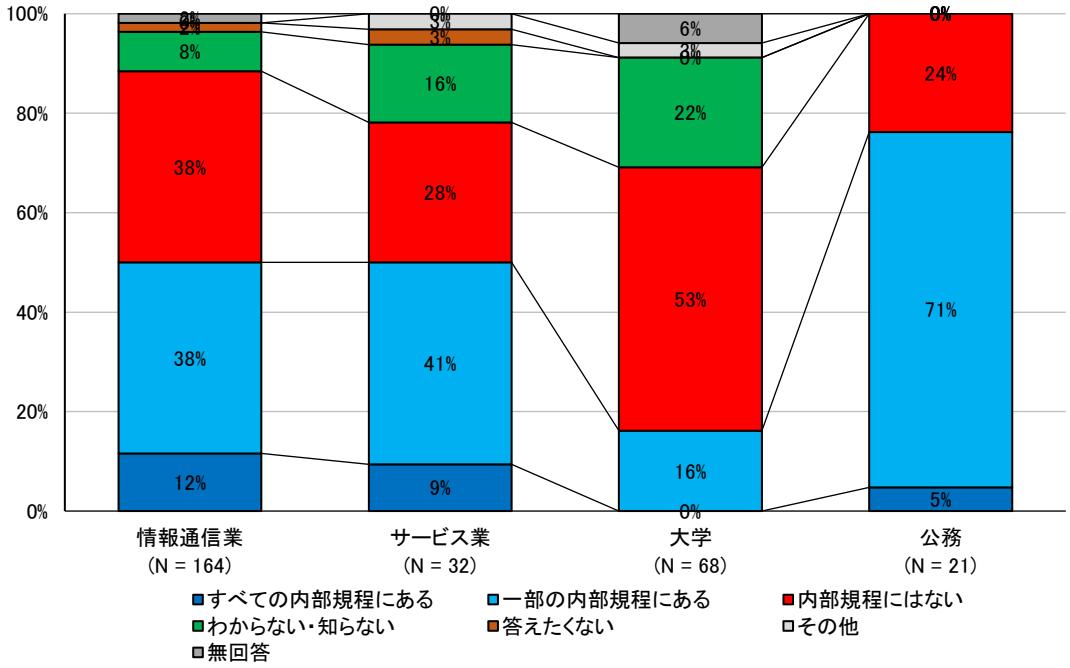

図 4-2 情報セキュリティに関わる内部規程全般での「例外規程」の項目の有無（業種別，択一）

4.2.4 調査結果 2：例外規程にない例外措置の承認手段（想定2，設問 15，17）

想定 2 では「内部規程にない例外措置は，経営判断だけでなく，現場判断でも実施できる」に基づいて設問 15 及び設問 17 を設定し，質問した．

まず，設問 15 の結果を図 4-3 に示す．設問 15 では例外規程に明記されていない事象（障害、事故・事件、災害等）に対する一時的な例外措置の実施の経験の有無についてたずねている．

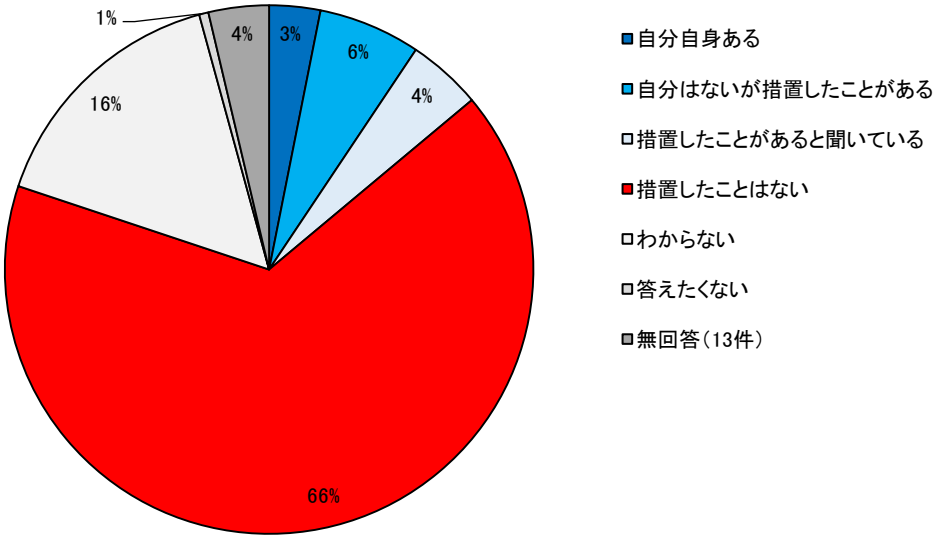

図 4-3 例外規程に明記されていない事象に対して，
一時的に例外措置した経験の有無（択一，N=352

図 4-3 から実際に例外措置を実施した総数（「自分自身ある（3%）」「自分はないが措置したことがある（6%）」「措置したことがあると聞いている（4%）」の和）は 13%にとどまり，7 割近くは「措置したことがない」ことがわかった．「わからない」「無回答」の占める割合も考慮すると，この結果から例外措置の実施が実際に普及していない傾向にあることを示すものと推定する．

なお例外措置は各組織で実際に規程を策定して措置を経験し，自組織での事例を増やし，組織学習をしていかなければ，当該組織に適応する例外措置の獲得とその効果を得ることは難しいと考える．

次に設問 17 の結果を図 4-4 に示す. 本設問は, 内部規程に例外規程がない事象に対し一時的に例外措置をとる場合, 「最初」にどのような手段をとるか(とると想定するか)をたずねた. 図 4-4 からは, 最初の措置判断は, 赤色の「CISO 等経営責任者に直接判断を受ける」組織は 23%にとどまり, 青色の「(利用部門の)情報セキュリティ責任者による現場判断を受ける」が半数を占めることがわかる.

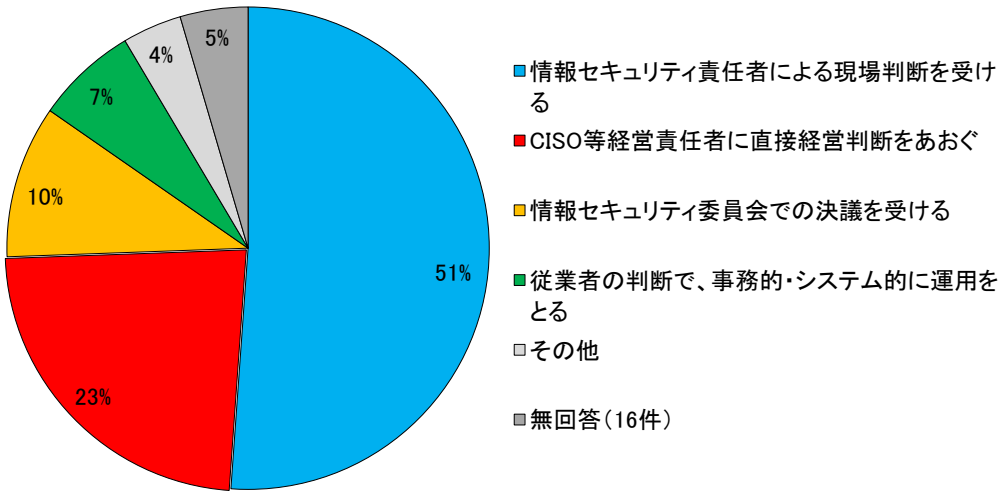

図 4-4 例外規程にない例外措置をとる場合に「最初」にとる手段(択一, N=352)

以上からは, 想定 2 に対する結果として, 一時的に例外措置を実施する際は, 画一的に管理部門主導タイプばかりだけではなく, まずは「現場組織の判断」が優先される利用部門主導タイプで実施されている組織が多い.

4.2.5 調 査 結 果 3：例 外 規 程 の 新 規 策 定 時 の 参 考 元（想定3，設問 18）

想定 3 では「例外規程の策定時は，他の先行事例等を参考にしている」に基づいて設問 18 を設定し，質問した．設問 18 の結果を図 4-5 に示す．

本設問は，内部規程に新規の例外規程を策定する場合，何を参考にするか（すると想定するか）をたずねた．同図からは，例外規程は赤色の「他社事例」や「政府官庁の統一管理基準」をもとに策定されることが多い．

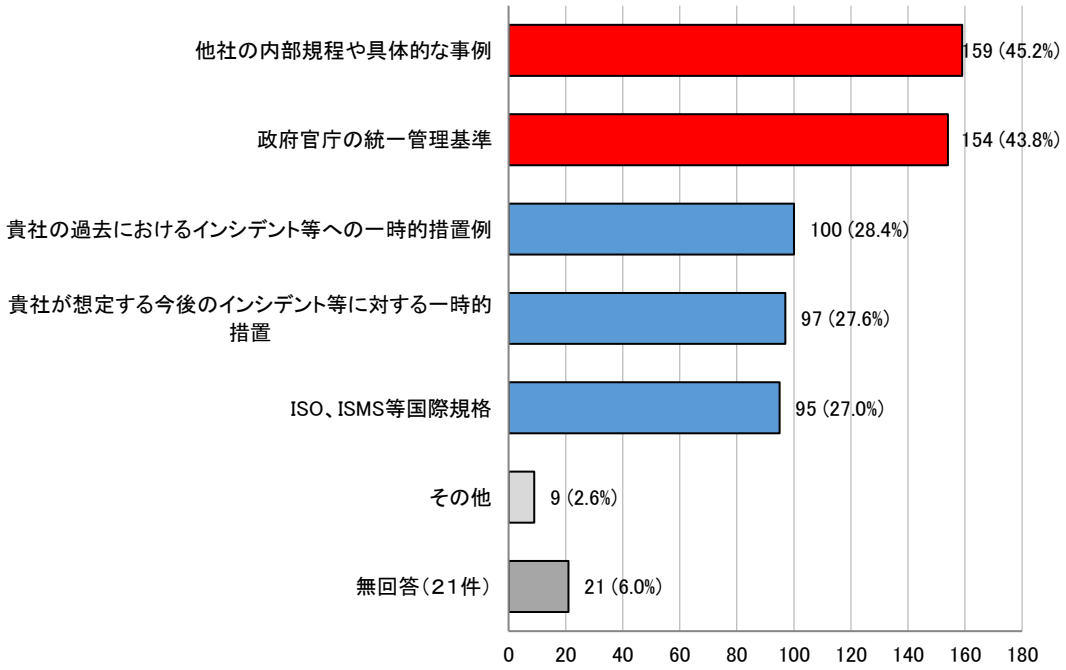

図 4-5 内部規程に新規の例外規程を策定する場合の参考元
（複数選択，N=352）

さらに公務（政府・自治体）についての内訳を図 4-6 に示す．なお件数が少ないため参考情報とする．同図から赤色の「政府・官公庁の統一管理基準」が他に比べ多く，統一管理基準を基に例外規程が策定され，比較的普及しているものとみられる．

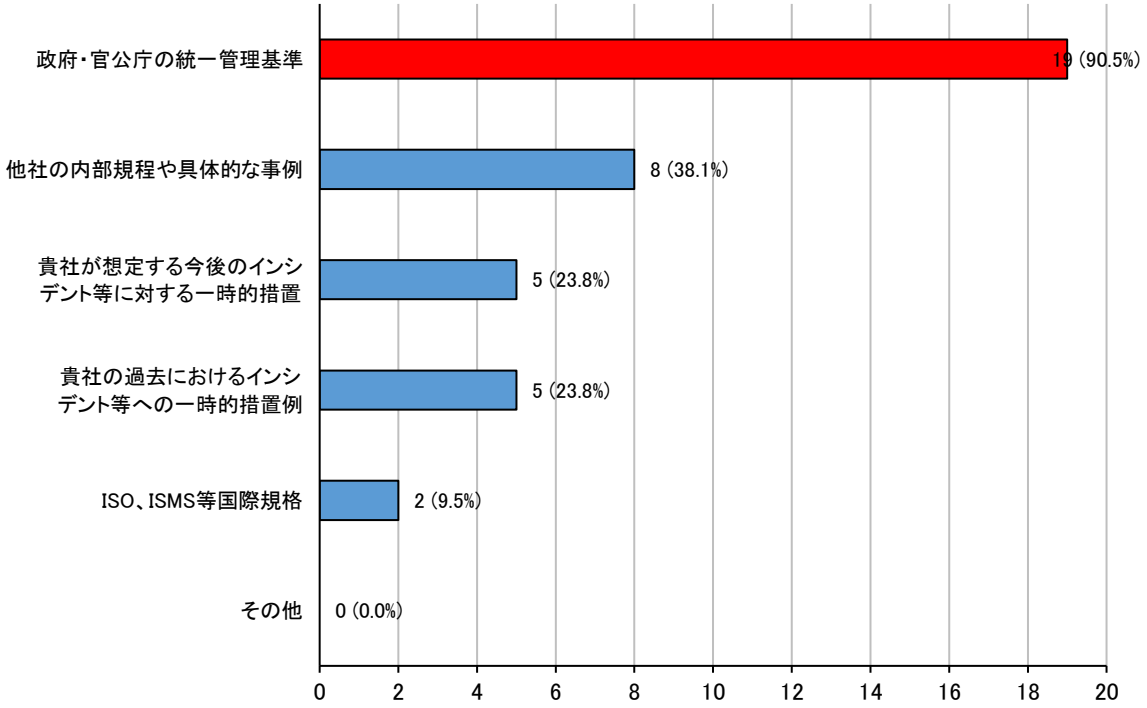

図 4-6 内部規程に新規の例外規程を策定する場合の参考元
（政府・自治体,N=21）

これらにより，想定 3 に対する結果として，例外規程を策定する場合，外部からの事例を参考にする組織が多い傾向にあることが分かる．また統一管理基準を参考にする組織も多く，新規に例外規程を策定する際の参考にしていることが分かる．

4.2.6 調査結果 4:例外規程の策定部門(想定4, 設問 19,20)

想定 4 では「例外規程は, 現場組織によって異なっている」に基づいて設問 19 及び設問 20 を設定し, 質問した.

先に, 設問 20 の結果を図 4-7 に示す. 本設問は, 例外規程は組織全体での統一された内部規程のみか, それとも現場組織ごとにも策定されているかをたずねた. 同図から, 例外規程は青色の「統一基準のみ」が半数を越え(55%), 赤色の「現場組織ごと」緑色の「両方」と現場組織を考慮している割合(13%)と大きく差があることが分かった.

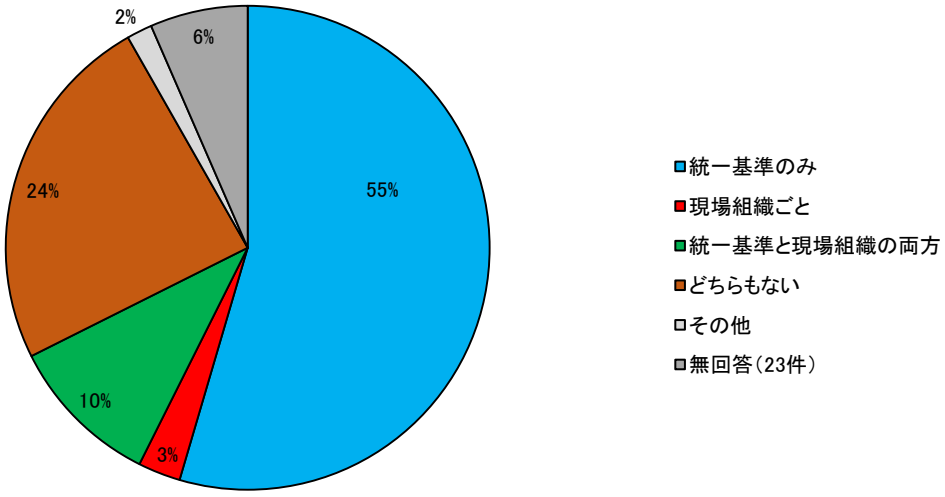

図 4-7 例外規程は組織全体で統一されたものか, 現場組織ごとにも策定されたものか
(択一, N=352)

次に，設問 19 の結果を図 4-8 に示す．本設問は，例外規程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かをたずねている．同図からは，例外規程を策定する組織は赤色系の「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．

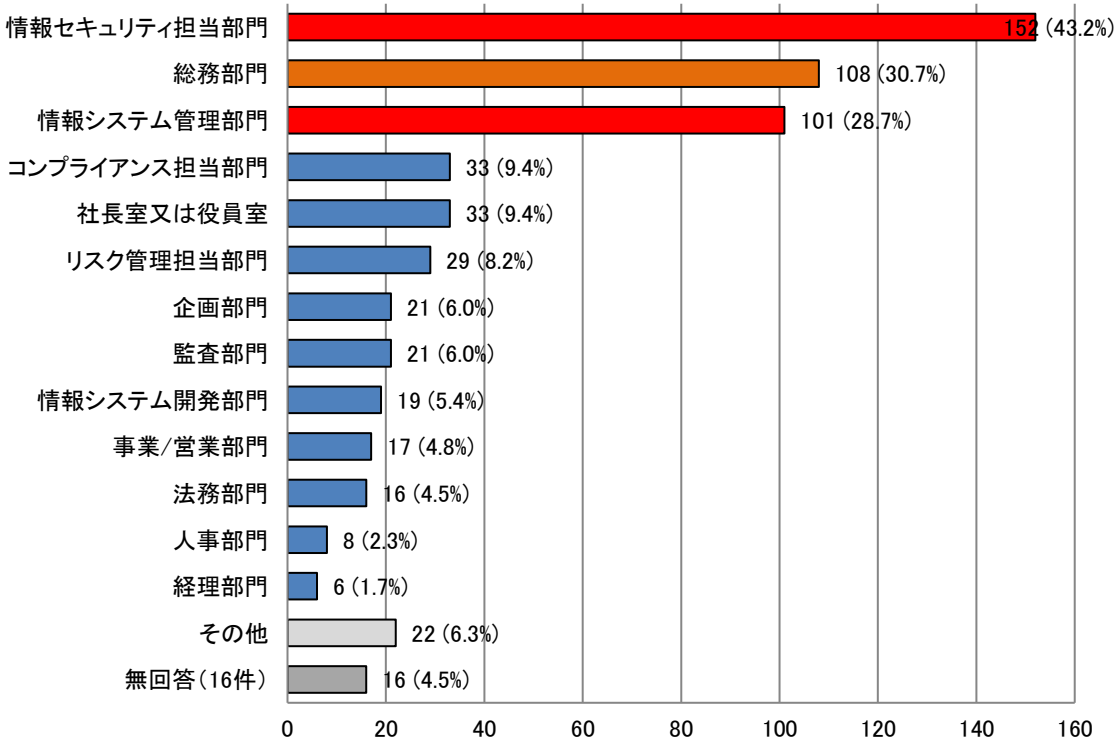

図 4-8 例外措置を実施するにあたり，
例外規程の策定と管理の事務処理をする主体部門
（択一，N=352，グラフ内の数値は回答数）

すなわち，想定 4 に対応する「設問 20」ならびに「設問 19」，さらに想定 2 における「設問 17」からは，多くの組織が例外規程を含まない統一基準のみで策定・運用していることがわかる．例外規程については，策定や運用にあたって専門的知識や経験などを要すると考えれば，情報セキュリティ担当部門や情報システム管理部門など情報系部門が策定し，管理・運用まで担当せざるを得ないのが現状であると考える．

4.2.7 調査結果 5:例外規程の見直し頻度(想定5, 設問 22)

想定 5 では「例外規程は定期的に見直されている」に基づいて設問 22 を設定し, 質問した.「設問 22」の結果を図 4-9 に示す.

本設問は, 例外規程の見直しの頻度についてたずねている. 同図からは, 例外規程の見直し頻度は, 青色の「随時」見直ししている組織が 40%と多い. また赤色の「1 年以内(14%)」緑色「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.

想定 5 に対する結果として, 組織は例外規程について, 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. なお, その他や未回答が多いことから,見直しをしていない組織も多いのではないかとも考えられる.

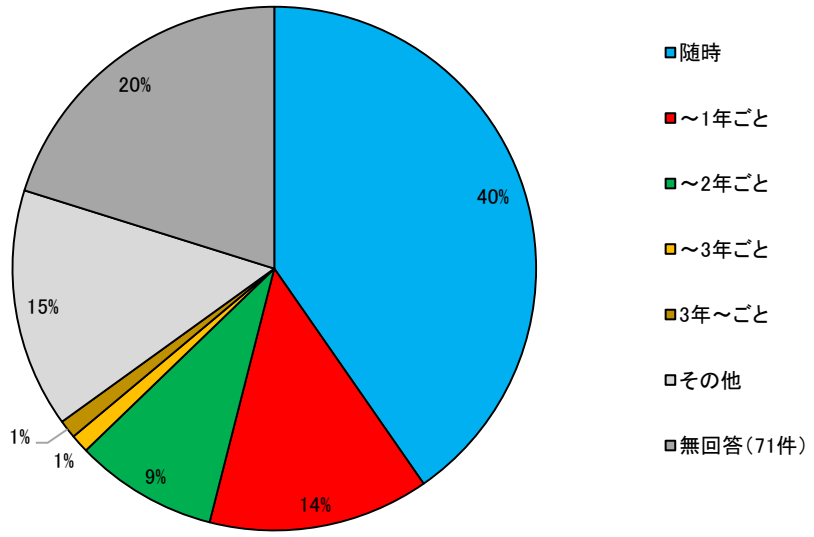

図 4-9 例外規程の見直し頻度(択一, N=352)

4.2.8 調査結果 6：例外措置の実施手順の記載の有無（想定6，設問 21）

想定 6 では「例外措置の実施手順を明記し，特に罰則とセットにしている」に基づいて設問 21 を設定し，質問した．設問 21 の結果を図 4-10 に示す．

本設問は，例外措置の業務にはどのような手続きが盛り込まれているかをたずねた．同図からは，赤色の「指定書式の申請書」，「管理・運用指導（実施・終了）」，「審査（稟議・通知）」が手続きとして盛り込まれている一方，黄色の「罰則の適用」や「措置手順の見直し」が比較的少ないことが分かった．

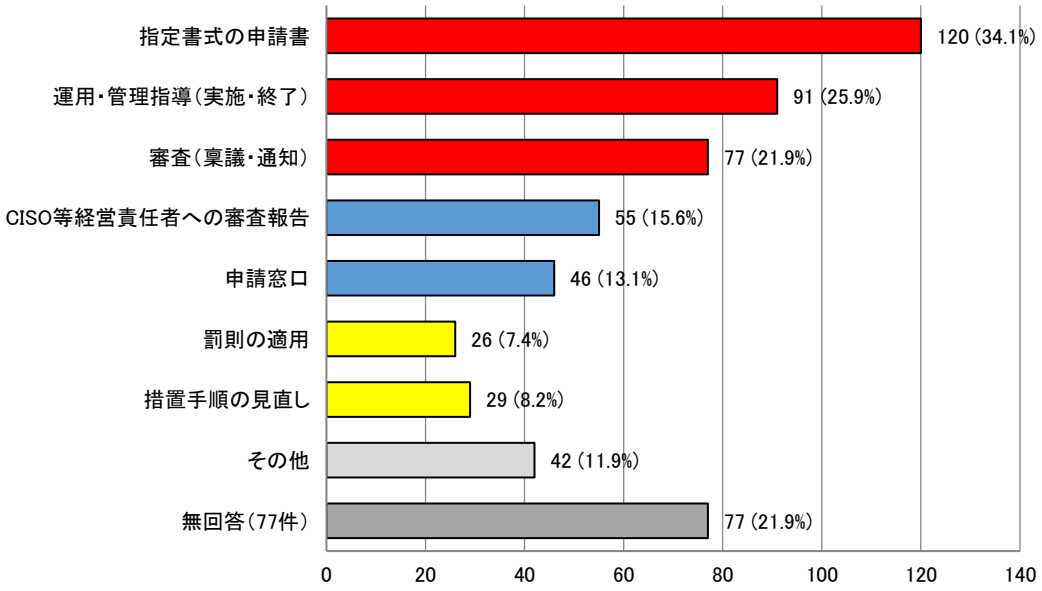

図 4-10 例外措置の業務に盛り込まれる手続き（複数選択，N=352）

想定 6 に対する結果から，統一管理基準で推奨している例外措置から逸脱した場合の罰則の適用が少ないことがわかる．したがって仮に例外措置から逸脱しても抑止できる効果が例外規程に明記されていない組織が多いと推定できる．一方で例外規程を策定している組織では図 3-2 のような業務フローが整備されているものと考えられる．すなわち例外規程の有無から，組織において手続きの体系化がなされているか判断できる．

4.3　2015 年度アンケート調査結果からの考察

以上 2015 年度アンケート調査について各想定に対する結果を表 4-3 に示す.

このうち, 想定 2, 3 及び 6 については, 概ね実施されていることがわかった. その一方で想定 1, 4 及び 5 の 3 つについては, 例外の活用に向けての課題であると考える. そこで本論文ではこの想定 1, 4 及び 5 についてさらに取り上げる.

表 4-3　2015 年度調査における想定と結果

想定(表 4-1 から要約)	結果
想定 1:例外規程はある程度普及している	・策定している組織と未策定の組織とで両極化している.
想定 2:内部規程にない例外措置は, 経営判断だけでなく, 現場判断でも実施できる	・例外措置は, 画一的な管理部門主導タイプばかりだけではなく,「現場組織の判断」が優勢される利用部門主導タイプで実施されることもある.
想定 3:例外規程時, 他の先行事例等を参考にしている	・外部事例を参考にする組織が多く, 特に政府統一管理基準を参考にする組織も多い.
想定 4:例外規程は, 組織によって異なっている	・部門ごとにカスタマイズして策定しているものは少ない. ・多くは専門部門において組織の統一管理基準で策定している.
想定 5:例外規程は定期的に見直されている	・事象が起きたその都度例外措置を実施している. ・必要に応じてその後規程として策定／見直す.
想定 6:例外措置の実施手順を明記し, 特に罰則とセットにしている	・例外規程を策定している組織では業務フローが整備されている. ・罰則の適用が少ないことから, 原則規程や例外措置への違反に抑止力が乏しい.

ここで, この結果を 2.2.3 項で上げた観点に照らし合わせてみる.

組織で例外措置を実施しているかについては, 本調査では直接的に確認することはできなかったものの, 想定 1(設問 14)の結果から少なくとも 42%の組織は例外措置を実施していることがわかる. 例外規程を策定した上での管理・運用については, 想定 1 の結果のとおり策定している組織と未策定の組織とで両極化している. 組織において例外を管理・運用している主体については, 想定 2 の結果より, 例外措置が画一的に管理部門主導タイプばかりだけではなく, 現場組織の判断が優先される利用部門主導タイプでも実施されることもあることがわかった.

4.3.1 策定／未策定の両極化（調査結果 1 より）

調査結果 1 から，情報セキュリティポリシーに対して，例外規程がある組織とない組織とで両極化していることが明らかになった．例外規程がない理由としては例外規程に対する認知が薄いか，もともと例外規程が必要と認識していない可能性がある．このことから今後，例外規程がない組織に対して普及を図ることが必要と考える．

例外規程がなく情報セキュリティポリシーが原則規程のみの場合，組織の現場など利用部門がビジネスで必要と自己判断し，原則規程を無視して管理部門に知られないように水面下で原則規程（つまり情報セキュリティポリシー）から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，このような逸脱を全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．

そこである事象に対して，原則規程として情報セキュリティポリシーに盛り込むのか，例外規程として一時的に例外措置をとるのか，あるいは例外措置もしないのか，といった対策が選択肢として考えられる．

4.3.2 専門部門への集中（調査結果 4 より）

調査結果 4 から，部門ごとに例外規程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管理基準で例外規程が策定されている．また，例外規程・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，利用部門では少ない．

例外規程の管理・運用主体については体系的に「管理部門主導タイプ」と「利用部門主導タイプ」の 2 つに分けられると述べた（表 2-1）．アンケート調査の結果からも，多くの組織において情報系部門からの管理部門主導タイプの規程策定がされていることがわかる．

すなわち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，多くは組織の統一基準で例外規程の策定・例外措置の実施がされている．また，例外規程の管理は，情報セキュリティや情報システムに関わる部門が多く，現場からの策定は少ないことからも，同じく管理部門主導タイプの策定・管理・運用となっていると考える．

例外規程の策定には，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．管理部門と利用部門が協調する組織体制の構築などが求められると考える（5.2.1 項参照）．

また，情報セキュリティポリシーは，組織の運営方針，組織風土及び情報セキ

ュリティの特殊性を反映する必要がある. しかしながら情報セキュリティ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」とみなして, 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[72].

従って情報セキュリティポリシーに付随する例外規程についても, 組織ごとに異なるものではなく, 情報セキュリティ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, 組織に必要な例外規程とはなっていないものと考えられる.

4.3.3 必要に応じた都度ごとの見直し(調査結果 5 より)

調査結果 5 からは「随時」見直ししている組織が多い一方,「実際に例外措置をすることが少ない(図 4-1)」,「見直し頻度もその都度(図 4-9)」,「例外規程の策定はないが一時的に例外措置を実施した(後述 4.6.1 項の図 4-15)」の特徴を持つ組織が多くみられることもわかった. 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都度ごとに対応し, その後, 必要に応じて規程として策定・見直ししているものと考える.

都度の対応では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程として汎用的にルール化していないため, 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.

例外措置は, 原則規程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, もともとの情報セキュリティポリシーに当該例外措置を原則規程として新たに盛り込むのか, その事象のみに限定して引き続き例外措置を実施(望ましくは例外規程として策定)するのかなど, 見直す必要があると考える.

72) 宇崎俊介, “第 1 回:情報セキュリティポリシーの現状,【特集】スローポリシーのススメ, atmarkIT”, 2002/7/26. (オンライン). http://www.atmarkit.co.jp/fsecurity/special/27spolicy/spolicy01.html. (アクセス日: 2019 年 6 月 10 日).

4.4　2018 年度アンケート調査

本研究では, 2015 年度のアンケート調査結果に基づき, 4.3 節で取り上げた想定 1, 想定 4 および想定 5 での考察から, 4.6 節で取り上げる想定 7 も含め, 例外措置の実態と効果について 2018 年度に改めて調査を実施した[73].

4.4.1 アンケート調査実施内容（全体）

2018 年度のアンケート調査は, 2018 年 8 月に当研究室から「情報セキュリティ調査」アンケート用紙を郵送して実施した. 対象は, 2015 年度とほぼ同様, 日本国内のプライバシーマーク（以下, P マーク）取得組織, ISMS 認証取得組織, CSMS 認証取得組織, 官公庁, 教育機関などから選んだ 4,500 組織(送達確認できたのは 4,233 組織)である. その結果 402 件（9.5%）の回答が得られた. なお, 本調査においては回答の未記入及び択一問題における重複回答等の無効回答は, 無回答として計上している[74]. 「例外規程」にかかわる設問は当該アンケートの第 6 章として盛り込んでいる.

4.4.2 アンケート設問

調査結果 1,4 および 5 に基づいて作成したアンケートの設問を表 4-4 に示す. 本研究では全アンケート設問のうち「設問 34」から「設問 39」までが例外規程に関する設問である. なお, 設問 38 及び設問 39 については, 4.6 節で取り上げる.

73) 情報セキュリティ大学院大学原田研究室, “2018 年度情報セキュリティ調査”, (オンライン). http://lab.iisec.ac.jp/~harada_lab/survey.html. (アクセス日 : 2019 年 6 月 10 日).

74) 李哲ほか, “2018 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”, 2019 年 暗号と情報セキュリティシンポジウム講演予稿集, 2019

表 4-4 アンケート設問（要約．参考文献 73 より一部加筆）

[設問 34] （想定 1）	情報セキュリティに関わる内部規程全般において「例外措置」の項目の有無
[設問 35] （想定 4）	例外規程は，組織全体での統一規程か，現場組織ごとの規程か
[設問 36] （想定 4）	例外規程と管理の事務処理する主体部門
[設問 37] （想定 5）	例外規程の見直し頻度
[設問 38] （想定 7）	具体的な業務上の事象において，例外規程の有無
[設問 39] （想定 7）	具体的な業務上の事象において，原則規程か例外規程か

4.4.3 調査結果 1:例外規程の有無(想定1, 設問 34)

想定 1「例外規程の導入」についてアンケート調査の結果を図 4-11 に示す. 設問 34 では内部規程全般において「例外規程」の項目の有無をたずねた.

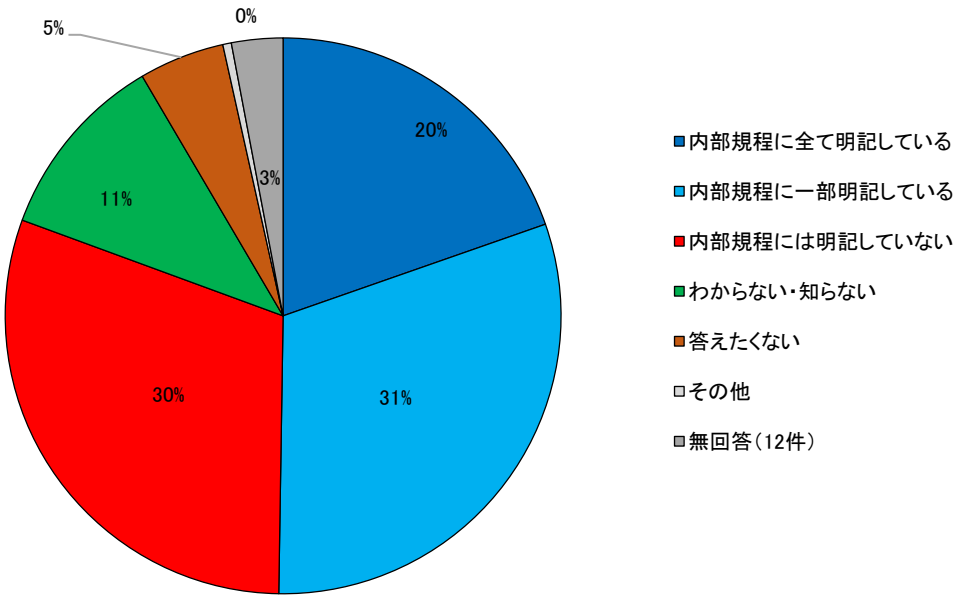

図 4-11 情報セキュリティに関わる内部規程全般において「例外規程」の有無
(択一, N=402)

図 4-11 から, 例外規程が「内部規程に全て(79 件)もしくは一部(123 件)に明記されている」割合(51%)は半数を超え,「明記されていない(122 件)」割合(30%)より 21 ポイント高い回答となっていることがわかる.

4.4.4 調査結果 2:例外規程の策定部門(想定4, 設問 35,36)

想定 4「例外規程」についてアンケート調査の結果を図 4-12 示す. まず設問 35 で, 例外規程が全体で統一された内部規程のみか現場組織ごとにも策定されているかをたずねた.

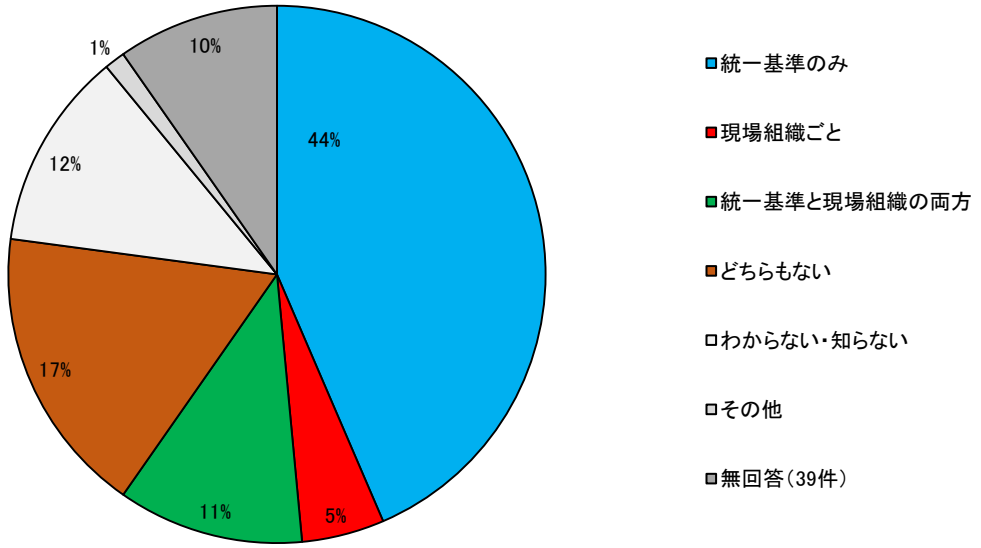

図 4-12 例外規程は組織全体で統一されたものか, 現場組織ごとにも策定されたものか(択一, N=402)

図 4-12 から, 例外規程は「統一基準のみ(175 件)」策定されている組織が 4 割を超え(44%), 現場組織での策定(「現場組織ごと(20 件, 5%)」「統一基準と現場組織の両方(45 件, 11%)」)は合わせても 1 割程度(16%)にとどまっていることがわかる.

次に，設問 36 の結果を図 4-13 に示す．本設問は，例外規程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ている．

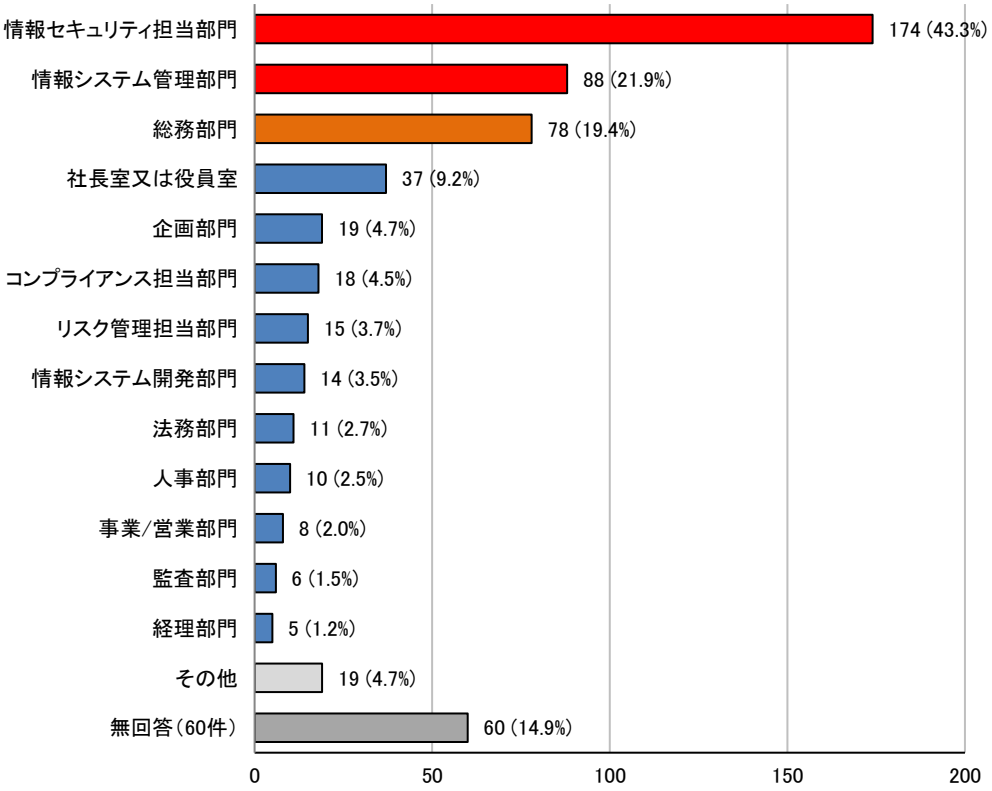

図 4-13 例外措置を実施するにあたり，例外規程と管理の事務処理をする主体部門（択一，N=402，グラフ内の数値は回答数）

図 4-13 から，例外規程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への設問に対しては，例外規程を策定する部門は赤色系の主に情報系部門（「情報セキュリティ担当部門（174 件，43.3%）」「情報システム管理部門（88 件，21.9%）」「総務部門（77 件，19.2%）」）を取扱う部門で他部門と比べ多いことがわかる．これは 2015 年度調査と同等の結果となった．

4.4.5 調査結果 3:例外規程の見直し頻度(想定5, 設問 37)

想定 5「例外規程の見直し」についてアンケート結果を図 4-14 に示す. 設問 37 では, 例外規程の見直しの頻度についてたずねた.

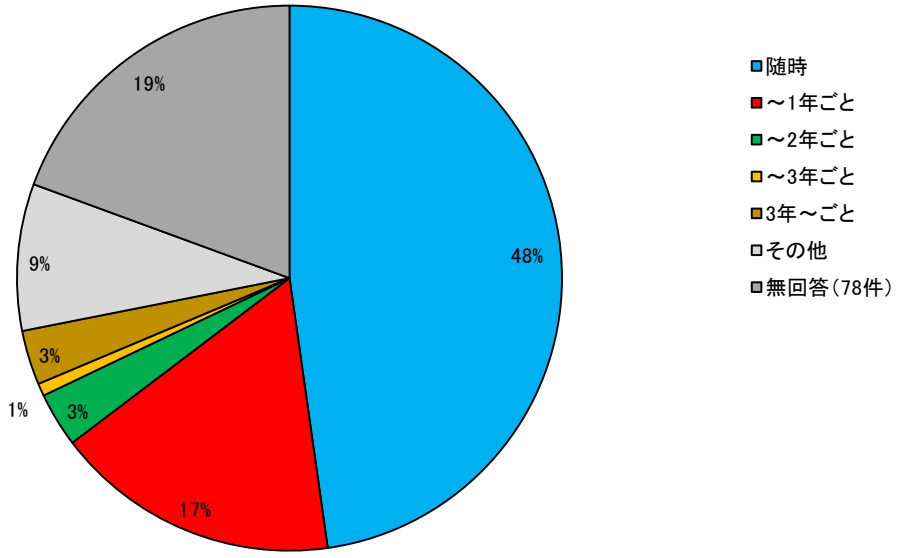

図 4-14 例外規程の見直し頻度(択一, N=402)

図 4-14 から,「随時(192 件, 48%)」が半数近くを占め, 例外規程の見直し頻度は, 特に定期的に実施しておらず, 案件が発生し実施した後に見直している組織が多いことがわかる.

4.5　2 つのアンケート調査結果の比較

以上, 2018 年度調査の結果を受けて, 想定 1, 想定 4 および想定 5 について 2015 年度調査結果と比較して考察する.

4.5.1 例外規程の有無（想定 1）

2015 年度調査（4.2.3 項）の図 4-1 と 2018 年度調査（4.4.3 項）の図 4-11 とを比較する.

2015 年度調査では「すべての内部規程にある（8%）」「一部の内部規程にある（34%）」の合計が 42%と,「内部規程にない」の 42%と同数で両極化していると述べた. 一方で 2018 年度調査ではそれぞれ, 20%＋31%＝51%と 30%と 21 ポイント増加している. 更に「すべての内部規程にある」については, 12 ポイント増加している. このことからこの 3 年間で例外規程の策定が進んでいることが推定できる.

4.5.2 例外規程の策定部門（想定 4）

まず, 2015 年度調査（4.2.6 項）の図 4-7 と, 2018 年度調査（4.4.4 項）の図 4-12 とを比較する.

2015 年度調査での「統一基準のみ」が 55%であったのに対し, 2018 年度調査では 44%と 11 ポイント減少している. 一方で,「現場組織ごと」「統一基準と現場組織の両方」については, それぞれ, 3%＋10%＝13%と 5%＋11%＝16%で変化が少ない. さらに, 2015 年度調査の「どちらもない」は 24%, 2018 年度調査の「どちらもない（17%）」と「わからない・知らない（12%）」の合計 29%と, こちらも変化が少ない. このことから, 統一基準のみの例外規程の策定が減少しているものの, 現場組織での例外規程の策定が進んでいないこと, さらに例外規程の管理自体も進んでいないことが推定できる.

次に, 2015 年度調査結果の図 4-8 と 2018 年度調査の図 4-13 とを比較する.

2015 年度調査での策定・管理する部門の上位3つは「情報セキュリティ部門（152 件, 43.2%）」「総務部門（108 件, 30.7%）」「情報システム部門（101 件, 28.7%）」であり, 他の部門と比べて多いことがわかる. 一方で 2018 年度調査ではそれぞれ,（174 件, 43.3%）,（77 件, 19.2%）,（88 件, 21.9%）であった. いずれの年度も上位3部門が他の部門よりも多い傾向は変わらず, 例外規程や管理においては専門的な知識や経験が必要と考える. これは「総務部門」が 11.5 ポイント減少していることから, 情報セキュリティポリシーに関わる管理・運用は専門部門が担うようになってきていることが推定できる.

4.5.3 例外規程の見直し頻度（想定 5）

2015 年度調査（4.2.7 項）の図 4-9 と 2018 年度調査（4.4.5 項）の図 4-14 とを比較する.

2015 年度調査での「随時」が 40％であったのに対し, 2018 年度調査では 48％と微増している. また, 1 年までの見直しが 14％から 17％, 2 年までが 9％から 3％となっており, 大きな変化はない. したがって, 定期的な見直しが望ましいとする例外規程の運用が進んでいないものと推定する.

4.5.4 2 つのアンケート調査の比較から

以上, 4.5.1 項から 4.5.3 項の結果をまとめる.

例外規程の策定（4.5.1 項参照）については, 策定／未策定の割合が均衡からやや策定に進んでいる傾向が見られた. このことは例外規程の普及を検討する上で, 活用に向けての対策を促していけば, さらに活用が進むのではないかと期待できる. 一方で, 例外規程の策定部門（4.5.2 項参照）は管理部門が主体であることや, 見直し頻度（4.5.3 項参照）はその都度行われているという実態に関しては大きな変化は見られず, 活用に向けての課題と考える. すなわち例外規程の策定には, 例外措置を実際に実施する利用部門への関わりは必要である. また, 例外措置を一時しのぎで実施するのではなく, 例外規程の策定によって管理・運用し, 定期的に見直しをすることが求められる.

4.6　例外規程と原則規程の策定状況

本節ではアンケート調査のうち，具体的な管理策の事例に対して規程（原則・例外）の有無や例外措置への策定傾向についてを，「想定 7」に基づいて述べる．ある管理策への措置（通常措置か例外措置のいずれか）が，原則規程もしくは例外規程のいずれを策定するかを調べることは，組織がどの程度例外を許容しているかを知る手掛かりとなり，例外措置を実施させるかどうかの判断につながる．

例えば，1.4.1 項で取り上げた USB メモリの管理策事例において，例外措置として USB メモリを使用する場合は，あらかじめウイルススキャン済みであることを条件の一つとすることが考えられる．この場合，利用者に対し「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．またシステム管理者に対しては，「対象システムを特別の監視対象として運用する」といった要件が，例外措置の対象となる．

組織においては，この許容範囲を「原則規程に盛り込む」のか，「例外規程として策定する」のか，あるいは「全く指定しない」のかについて，業種や組織，規模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，すなわち例外規程を策定しない事例に限れば，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程を策定しないのかの2つに分けられるものと考える．

4.6.1 アンケート調査実施内容（想定 7）

情報セキュリティポリシーからの逸脱と例外規程との関連性について，まず 2015 年度調査の想定 7「原則規程か例外規程かのどちらを策定するかの傾向がわかる」に対応するアンケート設問 16 を用いて分析した．設問 16 では，2015 年度調査内で使用した具体的な管理策の事例をもとに，表 4-5 に示すとおり 14 の例外措置の具体的な管理策を事例として設定した．

表 4-5 設問 16 で設定した具体的な管理策事例

(1)	ウイルス対策ソフトウエアを導入していない PC を利用する
(2)	サポート切れのソフトウエアを 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(スマートフォン・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)	日本国内法非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

この表 5-1 において, (5) (6) (9) (10) (13)は 2018 年度調査の設問 38 に, また(2) (3) (7) (8) (11) (12)は同調査設問 39 でも実施している.

そして各具体事例への回答用に表 4-6 に示す選択肢を設定した. 選択肢は「原則規程を策定」「例外規程を策定」「例外規程は未策定」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 4-6 設問 16 における選択肢一覧(一部, 加筆修正)

規程別	選択肢	
原則規程を策定	(1)	元来, 通常措置としている
	(2)	例外措置から変更した
例外規程を策定	(3)	例外規程に従い, 例外措置をしている
	(4)	例外措置をしたことがない
例外規程は未策定	(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

アンケート回答した単純集計結果を図 4-15 に示す. なお図 4-15 は表 4-6 の「原則規程に策定」「例外規程を策定」の合計の高い順に管理策を並べている. また図 4-15 中の事例の記載は表 4-5 から一部省略している.

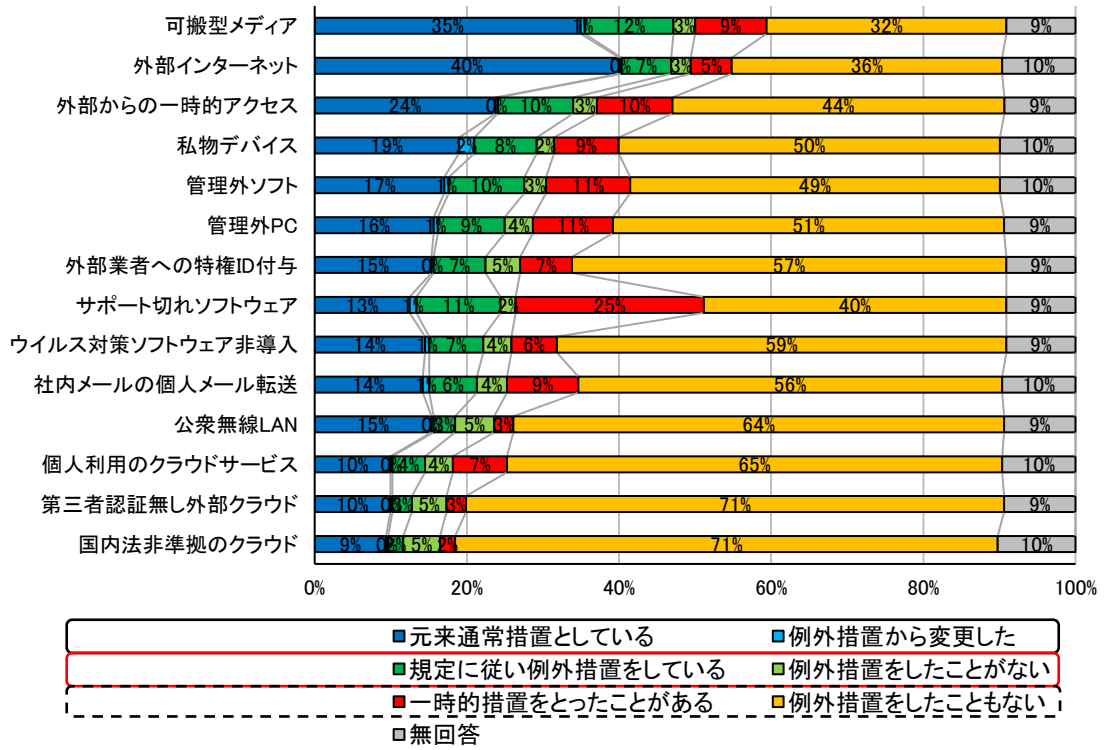

図 4-15 具体的な管理策における例外規程の有無

（択一，N=352）

図 4-15 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，表 4-6 に示す「原則規程を策定」「例外規程を策定」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」「日本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 割以上において例外規程がなく，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 5-1 からは，クラウドの利用については規程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．一つは全くクラウドを利用していない組織であること．もう一つは，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，すなわち規程が伴わない現場判断での利用であること，である．なお後者は 2.3.2 項で述べた BYOD のケースと同様に，利用現場に管理・運用をまかせ，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，クラウド以外の管理策については，何らかの規程が策定済みであり，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，原則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ものと考える．

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程があれば申請・承認手続きをとるようにしていることが分かる．なお業種別で回答の多かった「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 4-16 に示す．

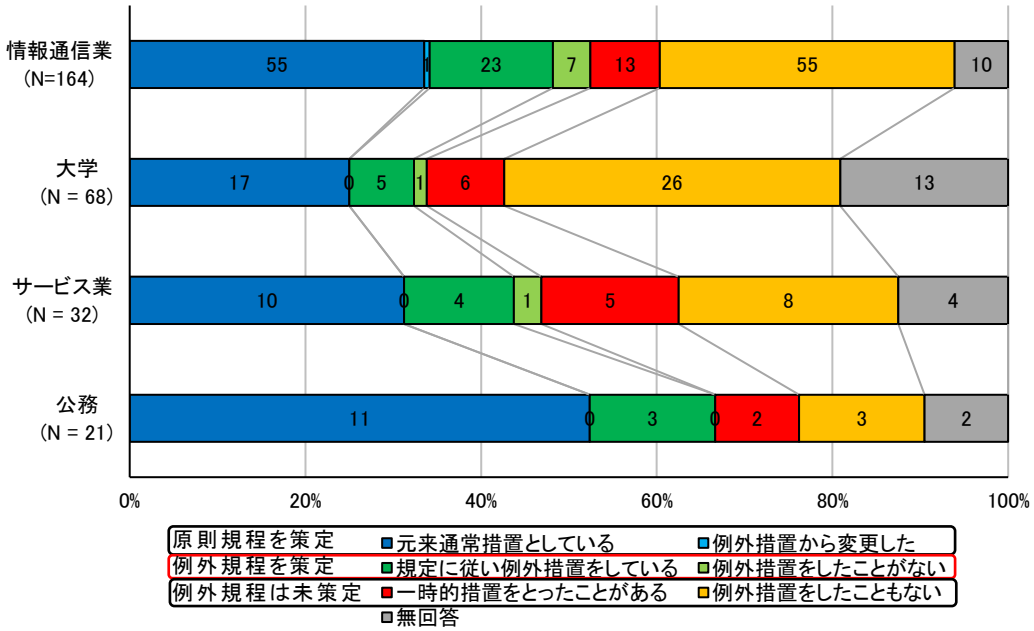

図 4-16 業種別での具体的な業務上の事象における例外規程の有無
（択一，グラフ中の数値は回答数）

公務では 68%，情報通信業では 53%が「原則規程を策定」「例外規程を策定」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具体事例では，概ね 30～40%の割合で原則規程あるいは例外規程が策定されている．すなわち，具体的な管理策それぞれに事前に規程がある組織については，組織ガバナンス・セキュリティマネジメントに活用しているものと推定する．

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管理策と異なり特殊性が見られた．原則規程あるいは例外規程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，他の管理策と比べ極端に多い．これは大手ソフトウエア会社の OS（Operating System）のサポート期限への対応が当該アンケート調査の回答時期（2015 年）と重なったことで，今

回だけの特殊性と推定する. しかし各組織が今後も起こりうる OS サポート切れへの措置には, 例外規程あるいは原則規程として策定していくことが望ましいと考える.

次に 2018 年度調査の結果を図 4-17 に示す.

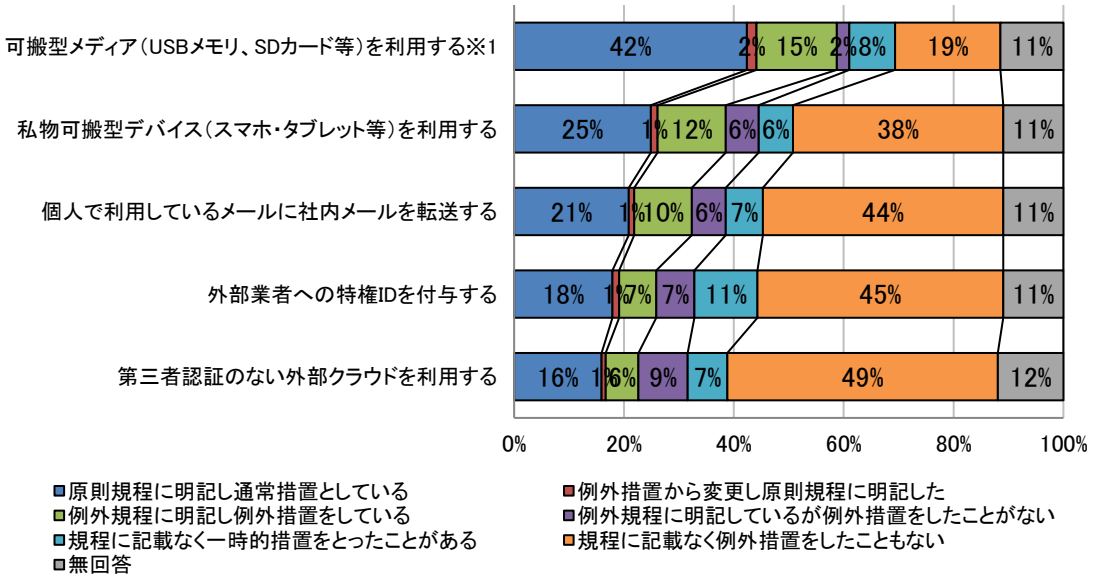

図 4-17 具体的な管理策における例外規程の有無
（択一, ※1 : N=349〔可搬型メディア～〕, その他の項目は N=402）

図 4-17 から,「可搬型メディアの利用（合計 213 件, 61%）」においては, 原則規程による措置が 42%と他の管理策事例と比べて差がある事がわかる. USB メモリの取り扱いにおいては1章でも述べたように事前に規程を策定しておく必要があることが実態として現れている. また例外措置としてではなく, 原則規程で管理・運用する背景には, 日常業務において USB メモリの取り扱いが通常措置として普及していることがわかる.

またその他の項目については,「規程になく例外措置をしたことがない」と回答したものが多いものの, 2015 年度の結果から比較すると 30 ポイント程度減少し 5 割以下となっている. 情報セキュリティポリシーにおいて管理策への取り組みが進んでいるものと考える.

4.6.2 原則規程と例外規程の策定状況の比較

図 4-15 の単純集計結果から原則規程と例外規程状況のみを抽出し，原則規程の比率が高い順に示したものを図 4-18 に示す．

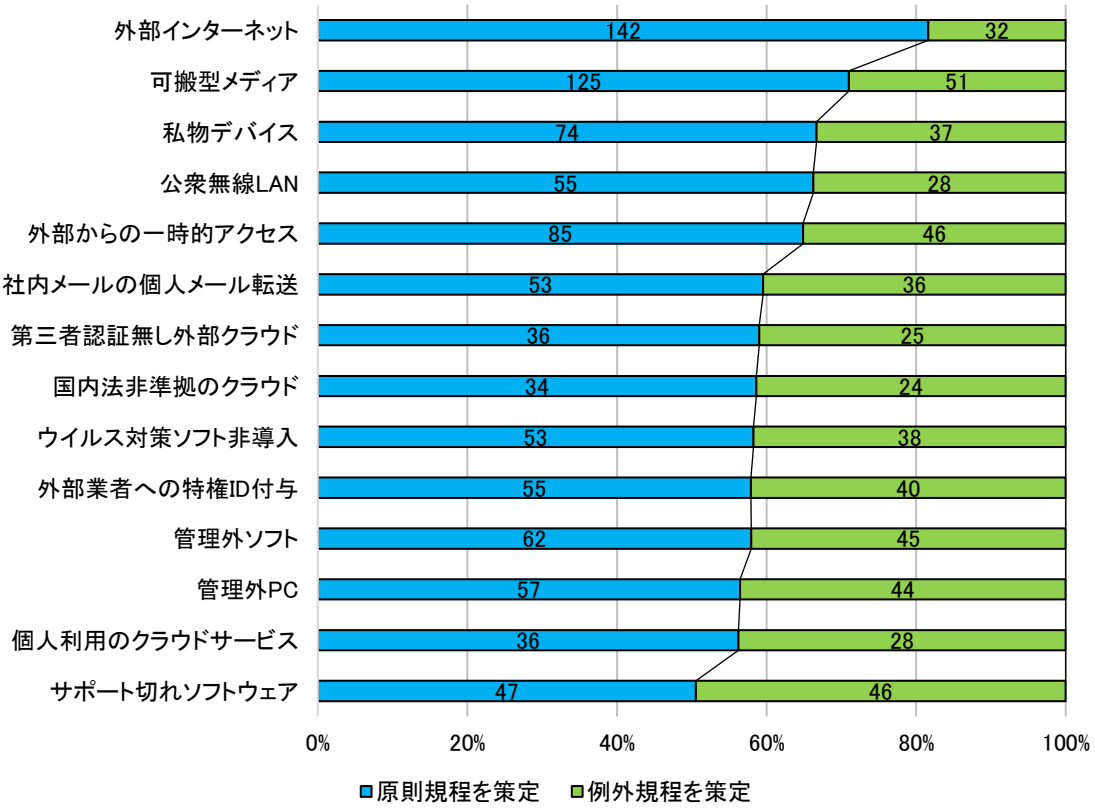

図 4-18 原則規程と例外規程との比率（2015 年度調査）
（択一，グラフ内の数値は回答数）

図 4-18 より以下のことが考えられる．なおここでは管理策それぞれに対して，原則規程・例外規程を問わず，規程が策定されていることを前提にしている．

4.6.1 項で述べたとおり「可搬型メディア」「外部インターネット」の利用については規程の策定が進んでおり，ほぼ原則規程として策定されていることがわかる．その他の管理策については，原則規程への策定が進んでいるものの，例外規程との差が少ない．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，当該管理策は例外規程として策定される傾向にあることがわかる．

次に 2018 年度調査結果を図 4-19 に示す．

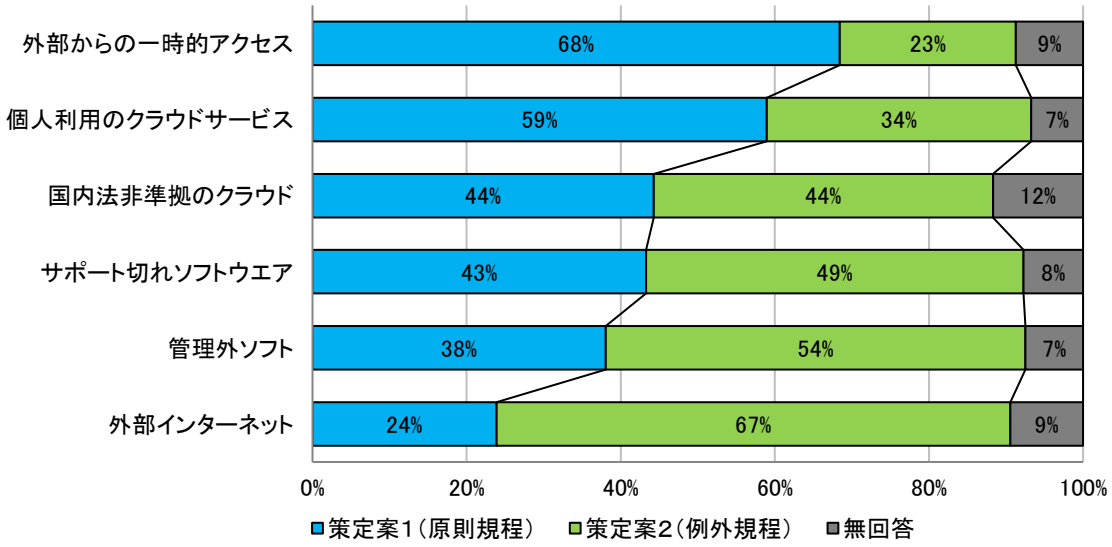

図 4-19 具体的な管理策における原則規程か例外措置かの選択
（2018 年度調査）（択一，N=402）

本設問は管理策それぞれに具体的な原則規程例と例外規程例を選択肢として用意し，二者択一で回答してもらった．その結果，原則規程で策定されている割合が高かったのは「プログラム保守のための外部からの一時的アクセス（275 件，68%）」と「個人で利用しているクラウドサービスの利用（237 件，59%）」であった．一方で，例外規程で策定されている割合が高かったのは「外部インターネットの使用（268 件，67%）」「自社が管理していないソフトウエアの使用（219 件，54%）」であった．

当該調査において具体的に原則規程例，例外規程例で回答してもらうと，通常措置で実施するもの，例外措置で実施するもの，あるいは双方均衡しているものなど，個々の管理策において特徴をみることができた．

なお設問方式が 2015 年度調査と 2018 年度調査で異なるため，図 5-4 との単純比較は難しいことは認識している．その上で，業務上での「外部インターネットの使用」に関しては，2015 年度調査では原則規程，2018 年度調査は例外規程がそれぞれ上位を占めるといった，相反する結果を得た．具体的な管理策へは，原則規程よりも柔軟に変更できる例外規程で対応する組織が増えているとも考えられる．

4.6.3 原則規程か例外規程かどちらを策定するかの考察

以上の調査結果・分析より，例外規程を活用する組織は，個々の管理策において，原則規程に基づく通常措置を実施するか，例外措置を実施するかをまず判断する．そのうえで例外措置を実施するのであれば，例外規程を策定するで管理・運用するものと考える．さらに例外規程を策定する場合は，自組織における原則規程からの逸脱に対する許容範囲を判断しているものと推定する．

しかし図 4-15 に示すとおり，個々の具体的な管理策において例外措置の実施が異なるため，例外規程の活用状況については全体としては不十分であると考える．特にクラウド利用等では例外規程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等に対して利用方法がまだ定まっていない組織は，リスクが明確に把握できていないことから，管理策として例外規程を策定してもリスクが低減できるかは不明である．

そこで組織は，リスク分析の結果からリスク対策が必要な管理策については，それらに対応する措置をはっきりと情報セキュリティポリシーに盛り込むことが求められる．その一方でリスクが比較的大きくない管理策については例外規程で対応するといった運用を行う．このように情報セキュリティポリシーにおいて原則規程と例外規程とを使い分けることで，現時点ではリスク分析が不明の事象や新技術への導入，早急に対応が求められる事象等にも即応し，組織の情報セキュリティ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る．

4.7　例外規程に関する想定と結論

以上，本章のまとめとして，例外規程に関する想定 1 から想定 7 までについて，アンケート調査結果に基づき表 4-7 でまとめる．また想定 8 については付録 A1 章を参照されたい．

表 4-7 例外規程に関する想定と結果（表 4-3 に加筆）

想定	結果
想定1：例外規程はある程度普及している	・策定している組織と未策定の組織とで両極化している ・策定が進んでいる傾向も見られる
想定2：内部規程にない例外措置は，経営判断だけでなく，現場判断でも実施できる	・例外措置は，画一的に管理部門主導タイプばかりだけではなく，「現場組織の判断」が優先される利用部門主導タイプで実施されることもある
想定3：例外規程の策定時は，他の先行事例等を参考にしている	・外部事例を参考にする組織が多く，特に政府統一管理基準を参考にする組織も多い
想定4：例外規程は，組織によって異なっている	・部門ごとにカスタマイズして策定しているものは少ない ・多くは専門部門において組織の統一基準で策定
想定5：例外規程は定期的に見直されている	・事象が起きたその都度例外措置を実施している ・必要に応じてその後規程として策定／見直ししている
想定6：例外措置の実施手順を明記し，特に罰則とセットにしている	・例外規程を策定している組織では業務フローが整備されている ・罰則の適用が少ないことから，原則規程や例外規程への違反に抑止力が乏しい
想定7：原則規程か例外規程かのどちらを策定するかの傾向がわかる	・組織の多くは管理策の実施状況をもとに，原則規程からの逸脱に対する許容範囲を判断している ・組織はリスク分析がはっきりとされている措置から原則規程とする ・原則規程と例外措置と使い分けることで，柔軟な運用が可能である

以下，各想定に対する結果について説明する．

想定 1 の「例外規程はある程度普及している」に対する結果として「策定している組織と未策定の組織とで両極化している」とした．これは 4.5.1 項でも述べた通り，2015 年度調査では両極化していた一方で，2018 年度調査ではやや策定が進んでいることが考えられる．この傾向が進んでいくことに期待したい．

想定 2 の「非常時は，経営判断だけでなく，現場判断でも例外措置ができる」に対する結果として「緊急性を要する例外措置は，画一的に管理部門主導タイプばかりだけではなく，現場組織の判断が優先される利用部門主導タイプで実施されることもある」とした．例外措置の実施に留まらず，利用部門でも例外規程の策定まで担っていくことが望まれる．

想定 3 の「例外規程時，他の先行事例等を参考にする」に対する結果として「外部事例を参考にする組織が多く，特に政府統一管理基準を参考にする組織も多い」とした．他組織での例外規程の事例が増えることは，未策定である組織において例外規程を初めから策定するといった負担の軽減につながるものと考える．更に 3.2 節で取り上げた政府統一基準群をもとに，自組織に適した例外規程にカスタマイズできる環境になることが望ましい．

その一方で，想定 4 の「例外規程は，組織によって異なる」に対する結果として「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で策定している」とした．これは 4.5.2 項でも述べた通り，統一基準のみの例外規程の策定が減少しているものの，現場組織での例外規程の策定が進んでおらず，さらに例外規程の管理自体も進んでいないことからわかる．また，管理部門に集中する傾向があることがわかったことは，例外規程の策定には専門知識が必要と考える裏付けになった．そのため，想定 2 でも触れたが，利用部門でも例外規程が策定できる人材育成・組織作りが求められる．

想定 5 について「例外措置は定期的に見直されている」に対する結果として「事象が起きたその都度例外措置を実施し，必要に応じてその後規程として策定／見直ししている」とした．2.4 節でも述べたが，例外規程は原則規程を補完するのが主たる役割であるため，常に原則規程と照らし合わせて運用しなくてはならない．定常化する例外規程であるならば，原則規程に盛り込むのか，あるいは削除するのかを定期的に見直すことが求められる．

想定 6 について「例外措置の実施手順を明記し，特に罰則とセットにしている」に対する結果として「例外規程を策定している組織では業務フローが整備されている．その一方で，罰則の適用が少ないことから，原則規程や例外規程への違反に抑止力が乏しい」とした．例外措置の申請・承認手続きについては，3 章の

国内外の先行事例でも例外措置を実施している組織では普及していることがわかっており，本アンケート調査でもその裏付けとなったと考える．一方で例外規程において罰則の導入の明記が比較的少なかった．このことから，例外規程からの逸脱に対して罰則が抑止力となる有効手段であると認識するものの，2.4 節及び 5.4.3 項で述べたとおり，必ずしも罰則ありきでの例外規程ではなく，罰則の適用を事前に防ぐ仕組みも必要であると考える．

最後に想定 7 について「原則規程か例外規程かのどちらを策定するかの傾向がわかる」に対する結果として「組織の多くは管理策の実施状況をもとに，原則規程からの逸脱に対する許容範囲を判断し，リスク分析がはっきりとされている措置から原則規程に盛り込んでいる．そして，原則規程に盛り込まれない措置の一部においては例外措置として実施できるように，原則規程と例外規程とを使い分けることで，柔軟な運用が可能である」とした．例外規程を活用することにより，現時点ではリスク分析が不明の事象や新技術への導入，早急に対応が求められる事象等に即応し，組織の情報セキュリティ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る．

小括

本章では，第 3 章の間隙を埋めるため，日本の組織を対象にアンケート調査を実施し，その結果を分析した．

組織において例外措置を実施しているかについては，本調査では直接的に設問していないものの，例外規程を策定している組織が約 4 割程度あり，少なくとも当該組織は例外措置を実施していることがわかった．また組織において例外規程を管理・運用している主体については，画一的な管理部門主導タイプばかりではなく，現場組織の判断が優先される利用部門主導タイプでも例外措置が実施されていることがわかった．

さらにアンケート調査の結果から次の 3 つを課題として見出した．①例外規程を持つ組織と持たない組織とが概ね同数で両極化している．②管理部門の統一的な基準を元に策定され，現場向けにカスタマイズしている例は少ない．③見直しは定期的ではなく必要に応じて実施されている．これらの結果から例外規程は十分に普及していないものと判断せざるを得ない．

また同じアンケート調査で，原則規程と例外規程の策定状況について集計・分析した．その結果，管理策によっては「原則規程のみを策定し通常措置を実施している」もの，「例外規程を策定し例外措置を実施している」もの，さらには「原則規程も例外規程も策定していない」ものがみられるなど，一律でないことが分かった．具体的な管理策においては，例えば「可搬型メディアの使用」や「外部インターネットの使用」については，原則規程として策定しているという回答が多い．一方で，「サポート切れのソフトウエアの使用」では例外規程として運用しているものが比較的多い．しかし「日本国内法非準拠のクラウドの使用」や「第三者認証の無い外部クラウドの使用」などについては，多くの管理策において，原則規程，例外規程ともに策定されていないことが明らかになった．

本アンケート調査の集計・分析の結果から，例外規程を策定している組織においては業務の効率化が図られていると推定する[75]．しかし上述の 3 つの課題から，必ずしも利用部門においての例外措置の実施が，現状に沿った例外規程の策定および管理・運用となっているとは限らないことがわかった．

本章と第 3 章の先行事例調査の結果から，例外規程のさらなる活用に向けての対策を検討する必要がある．次章では例外規程の活用に向けての対策を例外規程適用の限界も含め述べていく．

---

75) なお，付録 A1で想定 8 に対する分析の結果では，例外規程を策定していることに安心・満足している組織は約 8 割になると推測している．満足・安心への回答からは，業務の効率化の対する満足度も含まれるものと考える．

5. 例外規程の活用に向けての対策

本章では，これまで本論文で述べてきたことを受けて，例外規程の活用を考える上でのポイントを整理し，それぞれについての見解を述べる．ポイントとしては，例外規程の策定主体と注意点，例外規程にすべきかどうかの考え方，利用部門で実際に活用できうる例外規程の捉え方の3点を取り上げる．さらに例外規程を適用しても越えられない限界について述べ，例外規程を活用する上での留意点として取り上げる．

5.1　例外規程を活用する意義

例外措置の実施が必要不可欠であることは，これまで述べてきたが，先行事例調査やアンケートの結果からは，組織などでは例外の実施について，規程とまで明確かつ体系的に考えず場当たり的に必要なもののみ「例外」としての措置を個別に扱ってきたことが見て取れる．企業は例外を多数扱う中で，体系的に扱う必要性を感じて，例外規程を策定するようになると考えられる．そこで，この実態を踏まえて，例外規程に基づいて例外措置を管理・運用していく意義を以下に示す．

2.3 節でも触れたように，例外措置を例外規程によって汎用的にルール化することで，承認作業を可能な限り簡便化・省力化できる．さらに例外規程を情報セキュリティポリシーの基本構造に則って原則規程および例外領域などとともに体系化・モデル化（図 2-1 および図 2-2 参照）することにより，管理・運用の可視化が期待できる．これらが例外措置を管理・運用していく上で，例外規程を策定する意義と考える．したがって，例外措置を講ずるための例外をいかに例外規程として策定するかがポイントとなる．

そこで本論文では第 4 章の結果も参考にして，以下の 3 つについて，例外規程の活用に向けて論じていく．

・ 例外規程の策定主体と注意点（5.2 節）
・ 例外規程にすべきかどうかの考え方（5.3 節）
・ 利用者がもつ例外措置への阻害要因（5.4 節及び付録 A3 章）

なお例外の取り扱いについては，例外規程を策定・承認・管理する管理部門側と，実際に例外措置を実施する利用部門側とでそれぞれ分けることが考えられ，本論文では管理部門側を主として取り上げる．これはこれまでの研究調査の結果により，組織ガバナンスを中心に扱うのは管理部門側だからである[76)]．

一方で，体系的に管理部門がルール化するのは負担が大きい．そのため利用部門においても，情報セキュリティ対策などにおいては例外措置を相談するなどしてルール化を担ってきた．利用部門が携わっていくについては，単独で実施するよりも管理部門と相談することが慣習的と考えられる．したがって日本の組織においては，どちらかが一方的にすすめるよりも協調してすすめるのが望ましいと考えられる．

76) しかしながら，管理部門での取り組みを知ることは，利用部門においても参考になると考える．これは 5.2.1 項でも触れるが，例外規程の策定については，管理部門のみならず利用部門にも適用できる内容であるからである．

5.2　例外規程の策定主体と注意点

例外規程の普及を図るためには，例外規程そのものが作りやすく，かつ利用部門が利用しやすいものにする必要がある．本節では組織において実際に例外規程を取り扱う主体部門（1.5 節参照）に着目し，策定する上での組織体制の考え方について述べる．さらに例外規程を策定する上での注意点として，強行法規との関係について触れる．

5.2.1 例外規程を取り扱う主体

例外規程はヒエラルキー（1.2 節参照）と利用部門への適用との特徴から，1.4 節にて，取り扱う主体部門によって，体系的に 2 つのタイプに分けられることを述べてきた．なお 5.1 節で述べた通り，例外の取り扱いについては，例外規程を策定・承認・管理する管理部門側と，実際に例外措置を実施する利用部門側とにそれぞれ分けていることから，例外規程の策定を担う主体部門も管理部門を前提とする．これは想定 4 での調査結果（4.3 節参照）から明らかである．したがって規程を策定する権限はもともと管理部門が持っているものと推定する．

(1) 管理部門主導タイプ（トップダウンタイプ）

管理部門主導タイプは，まず管理部門において，その組織の持つ情報セキュリティポリシーに則り，例外への対策基準や管理策を明示し，経営側にそれらを承認させた上で，例外規程を策定する．その後，定期的に例外規程の改定を実施するタイプである．そのためトップダウンともいえる．

管理部門は情報セキュリティポリシーの策定や例外規程策定を取り扱う専門部門であることから，この分野においては精通していると推定する．管理部門主導タイプにおいて，例外規程を策定し管理する主体は管理部門である．

(2) 利用部門主導タイプ（ボトムアップタイプ）

利用部門主導タイプの主体は利用部門である各現場である．個々の現場で用いられている，もしくは個々の現場独自の基準やガイドラインから例外規程を策定し，おのおの現場で管理する．これは現場である利用部門の方が管理部門より実情を直に把握しており，例外規程策定，承認，運用または改定についても，それを反映しやすい．また反映することによりその現場に応じた例外規程が運用できる．これは(1)と逆の流れとなっており，ボトムアップといえる．

なお ISO では「マネジメントシステムを共通に構築して，分野ごとに必要な差分を追加する」というアプローチがあり，これに準じて考えることができる．さらにマネジメントシステム共通の構造が，ISO Directive ANNEX SL で規格化され

ている[77]. これを分野が異なる利用部門ごとの例外規程の策定に適用するのである.

補足ではあるが, このタイプは利用部門内で例外規程を完結できる為, 管理部門は原則規程のみの管理・運用となる.

これまで(1)管理部門主導タイプと(2)利用部門主導タイプの 2 つのタイプを紹介してきた. しかし本研究では, 不確実性のある想定外の事象を扱うには, それらだけではなく, 2 つのタイプを交えた施策も必要と思われる. 例えば, 例外規程策定は個々の現場である利用部門が主体として担い, 運用する. その例外規程策定に対する承認権限は管理部門が主体として担い, 例外措置実施後にはその運用報告を利用部門に課して, 蓄積, 分析し, 例外規程の策定から例外措置の実施, 改定までを管理部門が一限管理する(図 5-1 参照). このように(1), (2)の 2 つのタイプを程よく融合し, 柔軟にそれらを活用することも, 敢えて必要ではないかと考える.

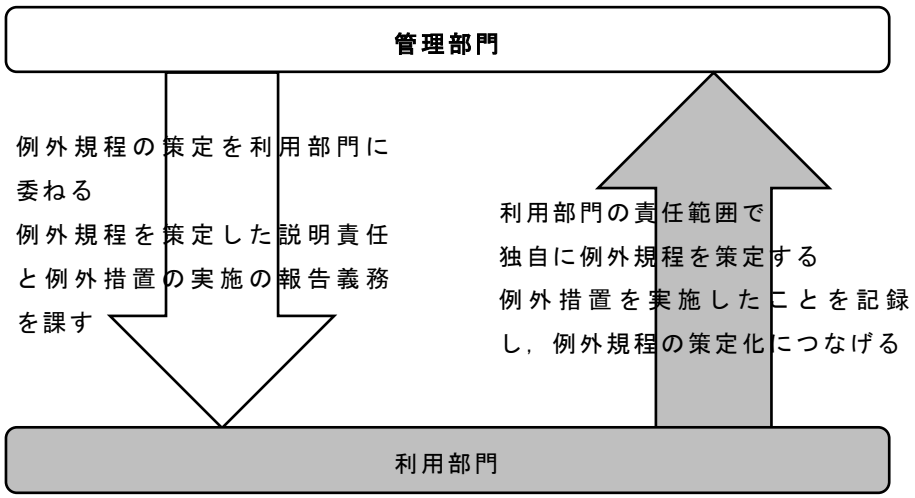

図 5-1 管理部門・利用部門協調による例外規程の策定への体系化

これは従来管理部門で策定される傾向にあった例外規程を利用部門でも手掛けることにより, 双方で例外規程を評価するといった PDCA の実現が可能と考えたからである. また 4.2.6 項の結果から, 例外規程の策定は管理部門主導タイプである一方で, 4.2.4 項の結果により承認手段としては利用部門主導タイプで対応しているということからも推定できるからである.

また組織全体に共通する規程の策定には, 管理部門主導タイプを適用し, 策

77) 原田要之助, “ITシステムのリスクマネジメントの全体像”, 著: 佐々木良一編「ITリスク学」, pp. pp122-138.

定することが望ましい. 一方で個々の利用部門に即した措置を必要とする規程については, その利用部門が主体となる利用部門主導タイプが望ましいと考える.

現在は技術革新により, 企業組織のあり方や働き方に変革が起きている. このような時代においては, 例外措置が適用される事象が起こりやすくなると考えられる. この状況をサポートするためにも例外規程の策定と管理・運用を滞りなく行い, 情報セキュリティ対策を柔軟に対応させることが組織としては望ましい. これは例外措置を適用するなかで, 管理部門と利用部門が互いに手を携え協調しながら, リスクの増大の抑制とその利用の最大効果の恩恵を得ることにつながるからである[78].

なお管理部門・利用部門が協調して実施するためには, 利用部門において課題があると考える. ひとつは利用部門の方が管理を担う責任が重くなると考えられる点である. もうひとつは利用部門が管理部門と比べ, 情報セキュリティポリシーの策定や例外規程策定を取り扱う専門知識は乏しいと考えられる点である. これらの課題に対処していくには, 管理部門が利用部門を支援して, 利用部門が例外規程策定の主体部門を担えるように導くことが必要と考える[79].

5.2.2 強行法規への注意点

次に例外規程を策定する上での注意点として, 強行法規との関連について述べる. 2 章で述べたが, 例外規程と逸脱領域の境界線においては, 法令や条例等で罰則が設定されている法定境界線(図 5-2 中の赤線)を決して超えてはならないと考える. そのため強行法規が例外規程の策定および例外措置の実施の上限である.

例外規程及び例外措置の上限が強行法規であることは, 情報セキュリティポリシーに関するガイドラインのいくつかにおいて, 個人情報保護法や不正アクセス禁止法への法令遵守が記載されていることからも明らかである[80][81].

本来超えるべきではない法定境界線を越えて例外措置を実施することは避けるべきである. これは例外規程の限界の一つとみなせるが, この限界は組織が安心安全にビジネスを拡張・継続していくための必須条件と考える[82].

---

78) 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.
79) 管理部門主導タイプと利用部門主導タイプが融合したパターンは例外規程の策定と管理に関する主体部門が利用部門となるため, 前提である「例外規程の策定を担う主体部門は管理部門」と異なってくる. 本章では以降も管理部門向けの対策を主として取り上げていくため, 管理部門が例外規程の策定主体として述べていく.
80) 情報セキュリティ対策推進会議, "情報セキュリティポリシーに関するガイドライン", 首相官邸, 2000
81) 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, 2015
82) 飯田によれば,「ルールはときに benevolence(著者は「温情」に近いと解釈)と対立する. ルールをそ

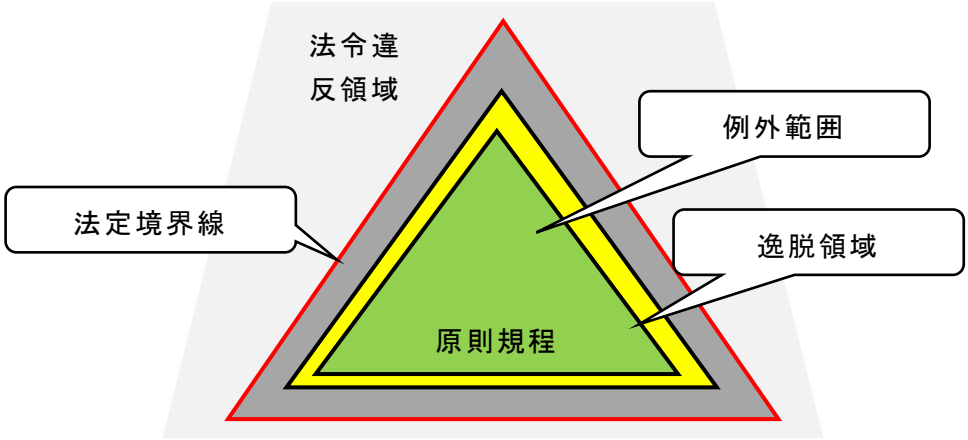

図 5-2 原則規程と例外範囲，逸脱領域及び法定境界線構成図

のまま適用すると妥当と思えない結論が導かれる場合，私たちはルールに反した判断をすることがある．もしルールを破ることが benovolence に基づいているのであれば，ルールを適用した際の違和感を正面から検討したり明示的に考慮要素として取り組んだりすることがルールの発展に資するだろう．」（飯田高，“リーガル・ラディカリズム連載第 1 回　ルールを破って育てる”，Quarterly Jurist 2018 Autumn Norbember 27, pp100-107）

現場が，組織の業務効率を図ることを目的に，あえて原則規程から逸脱する措置を実施しようとした場合，その考えや行為は必ずしも不自然なものではなく，原則規程をよりよくするために検討した結果であるべきとも捉えられる．

一方で次のように追記している．「ただし，（中略）ルール破りは予想もしていなかった結論を招く危険性もある．（中略）そのため，ルールを構造化するための理論が必要となり，それを通じてルールは発展していく．そして，ルールの再構造化は社会集団の再構造化でもあり，ルールを破ることは，守ることと同じく，長期的には社会集団を変化させる触媒として働くかもしれない．」

すなわち例外規程を策定し原則規程を併用することで，業務効率化を図るために原則規程を逸脱せざるを得なかった措置を，例外規程によって補完する．この構造が，結果として情報セキュリティポリシーの発展につながることと考えるにあたり，この論説は一助となる．

5.3　例外規程にすべきかどうかの考え方

次に具体的な管理策において，原則規程とするのか，例外規程とするのかといった，実際に例外規程を運用していくための方法について考える．なお本節では，例外申請をする者およびその部門を，申請者および申請部門とし，例外申請に対し承認する者およびその部門を承認者および承認部門と呼ぶことにする．一般には，申請者および申請部門は利用者および利用部門，承認者および承認部門は管理者および管理部門であると考えられる．

例外措置の運用には通常，申請者あるいは申請部門から提出された例外申請の内容を，承認者あるいは承認部門が既存の原則規程もしくは例外規程によって速やかに承認もしくは却下の「判断」ができるかにかかっている．判断できない場合は組織にとって「想定外」の申請となり，さらに新たな例外措置の実施を検討しなくてはならなくなる．承認部門が新規の例外措置の実施を承認するには，既存の原則規程と同程度の効用対リスク効果が期待できると「判断」できるかに求められる．

そこでそのような判断をするためには，組織毎のリスク分析が必要となる（4.6.3項参照）．新規の例外措置の実施を承認するかにおいて，リスク分析の結果から，リスクは比較的大きくないと「判断」した場合は，例外措置の実施内容および適用範囲を指示した上で実施を承認する．さらにその実施内容および適用範囲がルール化できるものであれば例外規程として策定し，管理・運用する．一方リスク分析の結果から，リスクは比較的大きいと「判断」し，リスク対策が必要だと「判断」した場合は，もはや旧来の原則規程と同程度の効用対リスク効果が期待できないため，例外措置として扱うことは難しいと考える．そのため原則規程を改定し通常措置として実施を承認するか，あるいは却下するかの「判断」が求められる．

この「判断」は当該組織のリスク対策に基づくものであり，組織の目的によって異なってくる．したがって組織毎のリスク対策への判断結果が例外措置の判断基準となり，すなわち例外規程策定の判断基準へとつながるものと考える．

以下，本節では4章のアンケート結果に基づき，図4-18における，2位の「可搬型メディア」，3位の「私物デバイス」，4位の「公衆無線LAN」及び8位の「国内法非準拠のクラウド」の 4 つを例に，具体的な管理策での例外規程策定への判断基準を考える．なおこれらは一例であり「リスク対策の内容」，および「例外措置の実施内容および適用範囲」は一意でなく，様々なケースが想定できる．組織に適用できる例外措置および例外規程を得るには，例外措置を実施し，そ

の実施内容をルール化することで例外規程を策定し，その例外規程をもとに例外措置の実施を管理・運用していくという経験を，組織が蓄積していかなければならないと考える．

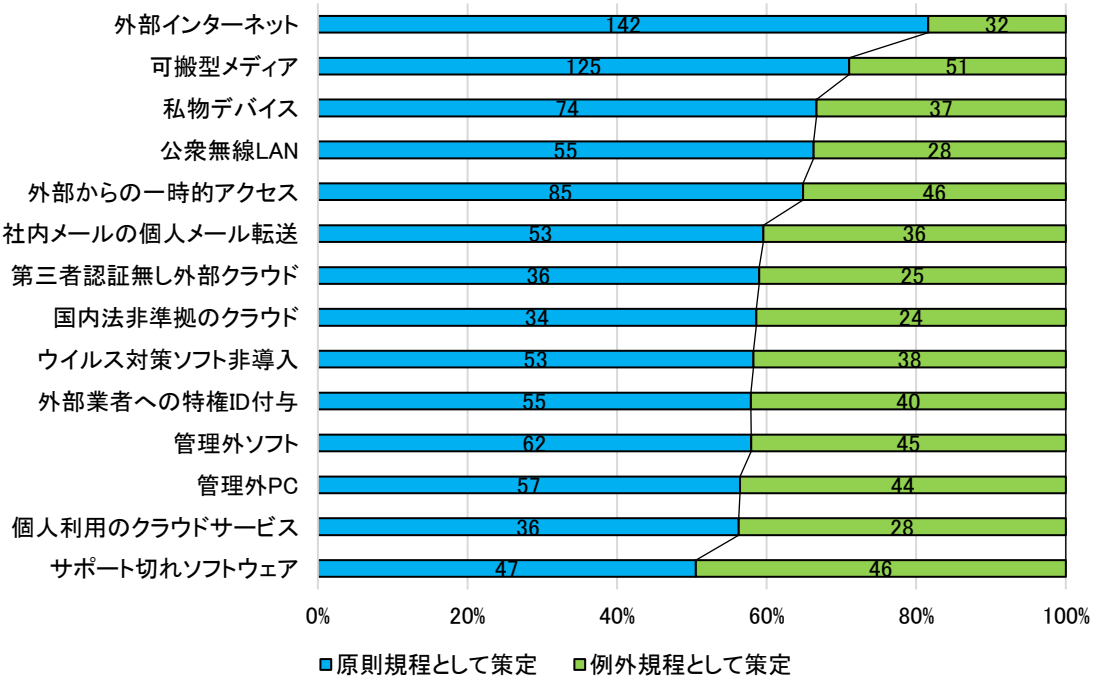

図 4-18　原則規程と例外規程との比率（択一，グラフ内の数値は件数）（再掲）

5.3.1 可搬型メディア

可搬型メディア（USB メモリーや SD カード等）の利用に対する管理策は，図 4-18 の結果から原則規程の方が例外規程よりも多いことがわかる．ただし USB メモリに対する利用制限があるものの，完全に禁止している組織が少ない．小中高学校や教育機関，研究施設，個人情報・秘密情報を扱う機関においては，禁止もしくは組織から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事例もある[83)]．

そこで管理策としての例外規程は，「業務上取引先からの指示等やむを得ない場合は，予めウイルススキャン済みのものであれば使用許可する」とする．これにより外部への機密情報の流出や漏洩を防ぐことができ，かつ，業務効率の低下やウイルス感染の防止も計れ，日常業務としての対応が可能となる．

例外規程策定の主体のタイプは管理部門主導タイプと利用部門主導タイプが程よく融合したパターンを活用することにしたい．可搬型メディア使用は，全組織一律ではなく部門ごとに使用状況が違うため，管理部門と利用部門が協調して策定するのがよいと考えたためである．また例外規程策定の意義においては，原則規程で使用が禁止されているメディアであっても例外規程を策定しておけば，速やかにその使用が可能となり，日常業務が維持できるという点である．

83) 文部科学省初等中等教育局児童生徒課，“学校における携帯電話の取扱い等について（通知）”，文部科学省，平成 21 年 1 月 30 日． (オンライン).
http://www.mext.go.jp/b_menu/hakusho/nc/1234695.htm. (アクセス日：2019 年 6 月 10 日).

5.3.2 私物デバイス

私物デバイス(スマートフォンやタブレット等)の使用については，組織が調達に係る費用対効果を考慮しなくてはならない．そのため組織貸与より私物デバイスの使用を認めるといった方向に進むものと推定する[84]．

そこで管理策としての例外規程は，「私物デバイスの登録，指定アプリのインストール，業務使用手引きの励行及び誓約書の提出による許可とする」とする．それにより管理部門が私物デバイスの業務使用への教育を施し，私物デバイスでも管理可能となり，私物デバイスの業務使用が可能となる．そのことにより，シャドーIT の問題，ウイルス感染防止及び調達コスト削減等のメリットが期待できるものと考える．

例外規程策定の主体のタイプとしては，管理部門主導タイプと利用部門主導タイプが程よく融合したパターンを活用するのが望ましいとする．私物デバイスは個人の所有によるところが大きいので，申請部門，承認部門双方で協調し運用するのが望ましいと考える．例外規程策定の意義については，原則規程で使用が禁止されている私物デバイスも例外規程策定により，措置として迅速に運用が可能となり，業務効率の向上につながると期待できる．

なお私物デバイスについては，個々の組織の状況により原則規程とするか例外規程とするかの判断が異なってくると考える．組織全体で恒常的に私物デバイスを使用していくのであれば，導入にあたりリスク分析を実施した上で原則規程として策定すべきである[85]．一方，一部の組織で一時的に使用するのであれば，デバイスの組織貸与と同等のリスク低減が期待できるよう対策を講じた上で，例外措置を実施し例外規程として管理運用していくのが望ましい．

私物デバイスの業務使用を禁止する選択肢もあるが，その結果として安全性が担保されないまま隠れて使用され続けることが否定できない．すなわちリスクが可視化されないまま，より高いリスクにつながる可能性もあることを管理部門は考慮すべきであると考える[86]．

---

84) いわゆる BYOD の運用に関わってくる

85) 私物デバイスを使用する際のリスクとしては，利用者および組織の機密情報の漏えい，業務上の通信費用に対する不正課金，攻撃者によって踏み台とされ，第三者を攻撃してしまうなど，ほとんどはアプリの導入・利用に起因するとした報告がある(KDDI 文献)

86) 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).
http://itpro.nikkeibp.co.jp/article/COLUMN/20120920/423888/.

5.3.3 公衆無線 LAN

職場を離れ出張・外勤先からインターネットを通じて自組織の基幹システムにアクセスし，データの授受が可能となることは，5.3.2 項の私物デバイスと同様に業務活動の幅が広がり，業務効率の向上が期待できる．特に無線 LAN は携帯回線通信よりも大容量伝送が可能であり，2020 年のオリンピック・パラリンピックを控え，市街地の施設や街頭で急速に利用が広まっている．しかしながら無線 LAN，特に公衆無線 LAN の多くは不特定多数の人々が容易に情報収集できるようパスワードフリーで設定しているものがあり，情報セキュリティ上業務として使用するには安全とはいえない．そこでこの場合の管理策としての例外規程は設けない．したがって例外措置もない．

公衆無線 LAN 使用に関しては，その性質上サイバー攻撃の標的や踏み台となりやすく，自組織の情報インフラに深刻な影響の出るリスクがある．そこで，公衆無線 LAN 使用については原則規程のみの策定とし，その管理･運用を徹底する．通常，無線 LAN 使用については，多くの組織が原則規程として使用を禁止しているところが多いと思われる．しかしながら旧来の原則規程のままでは，昨今の業務活動の広がりに対処できず，業務の向上が図られない．その場合，原則規程の改定を行うことが考えられる．

原則規程の改定とは 2.1.3 項で述べた通りである．改定後の新原則規程とは，この場合，技術的には「あらかじめ管理部門に VPN 接続申請の承認を受け，TSL や VPN 等暗号化した通信を行うのであれば作業許可する」，運用的には，「公共の場ではファイル共有機能を解除する，公衆無線 LAN サービスのログイン画面に電子証明書エラーが表示されたら接続しない」などであり，技術面，運用面の両方から現況に沿って入念に策定する[87]．このような改定を施すことにより，日常業務の安全な維持が保たれ，業務向上に貢献できると考える．

これら原則規程の管理主体のタイプは管理部門主導タイプが望ましいと考える．特に，そのリスクにおいては影響が組織全体に及ぶ場合があるため，管理部門が一元的に受け持ち，その策定，運用，蓄積，分析，改定までを管理することが望ましい．

総務省では組織等が安心して無線 LAN を導入・運用するための手引きを提供しており[88]，導入に関しては，原則規程として細かく例示している．例えば，「原則禁止」としているのは「アドホックモードの制限」など極少数で，利用してい

87) 総務省，“一般利用者が安心して無線 LAN を利用するために”, 2012 年 11 月 2 日． (オンライン). http://www.soumu.go.jp/main_content/000183224.pdf. (アクセス日: 2019 年 6 月 10 日).
88) 総務省，“企業等が安心して 無線LANを導入・運用するために”, 2013 年 1 月 30 日． (オンライン). http://www.soumu.go.jp/main_content/000199320.pdf.

る場合は，厳密に説明（Comply or Explain）が求められるものと考える．

5.3.4 国内法非準拠のクラウド

本研究を始めた2015年当初，組織が業務として外部クラウドを利用する場合，利用契約が国内非準拠である海外企業のクラウドサービスが回避され，もっぱら国内法準拠のクラウドサービスが利用されていた．これはクラウドベンダー保有のデータセンターが海外の非公開の場所に設置されており[89]，万が一，法的対応をとる場合国内法で対処することが難しく，また解決には費用と時間がかかるというリスクがあったためであった．そのため国内法非準拠のクラウドサービスは，機密情報等重要なデータの保管や基幹システムとしての導入は避けられ，日本国内での普及は進まなかった．

しかし現在では，海外のクラウドベンダーでもデータセンターを日本国内に設置するようになり，それに合わせて利用契約も国内法準拠で対応できるようになってきている．また組織がグローバル企業であるならば，あえて国内法非準拠であっても契約を締結することも推定できる．現在の社会市場の傾向から鑑みると，クラウドの利用は一般的になりつつあり，経営層もクラウドに対する信頼性・利便性，さらにはリスクも認識するようになってきている．すなわちクラウドサービスの導入に関しては経営層の抵抗感も以前と比べれば減ってきているものと考える[90]．

そこで管理策としての例外規程は「あらかじめクラウドベンダーもしくは当該クラウドの仲介業者と個別に国内法準拠の利用契約を締結すれば利用許可する」とする．なおクラウドサービスの利用については，基幹システムとして常時使用するのか，または一部の利用部門が一時的に利用するかにより，管理策が異なると考える．組織全体で常時使用するのであれば原則規程に盛り込むことが肝要であり，一時的なものであれば例外規程を策定して措置することが望ましい．また策定主体のタイプも組織全体での常時使用であれば，管理部門がクラウド業者と包括契約を結び，原則規程として明確に運用する．一部の一時的な，いわば個別利用であれば，管理部門主導タイプと利用部門主導タイプが程よく融合したパターンを活用するのが望ましいと考える．その意義（5.1節参照）としては，原則規程を改定するほどではないが，例外規程を策定することにより国内法非準拠クラウドへの承認が迅速に実施でき，業務上の利用を促進することで業務効率の向上が期待できると考える．

89) 例えばgoogle map を利用したアプリケーションを作成しようとした場合，このままでは入力した地名や住所などキーワードがどの国のサーバで管理されるかは明らかでないものと推定する
90) 総務省，平成27年度版情報通信白書，2016.

5.3.5 例外規程にすべきかどうかの考え方への考察

以上，4 つの管理策での策定例について例外規程にすべきかどうかを述べた．なお，参考として管理策項目ごとに，情報セキュリティポリシーにおける原則規程と例外規程例を表 5-1 に示す．また付録 A5 に補足資料を付加している．もともと表 5-1 は中小企業向けに例外措置の普及に向けての研究調査において提案してきたが（初出一覧（3）及び付録 A2 章参照），組織の規模に関わらず適用できるものと考える．また表中の管理策の一部については，2018 年度調査の設問に使用し，原則規程もしくは例外規程への適用について調査している（図 4-17，図 4-19 参照）．

調査結果からは管理策によっては原則規程が多数を占めているもの，例外規程が比較的策定されているものとあった．このことより原則規程，例外規程それぞれに適性があるものと推定でき，それに応じて例外措置の承認基準や手順をカスタマイズすることが望ましいと考える．なお，例外措置が比較的策定されている管理策は，利用するデバイス・サービスが自組織の所有ではなく，管理対象外であるものが多くみられる．これは従来，これらが組織の原則規程の適用を受けないことから起因するものと推定する．

表 5-1 各管理策における原則規程例と例外規程例対比表

管理策	原則規程例	例外規程例
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承認する
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のものであれば使用を承認する
サポート切れの OS やソフトウエア	サポート切れのOSやソフトウエアの使用は全面禁止である	完全に外部ネットに接続しないレガシーシステムについては承認することもある
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	一時的措置が必要と経営層が判断した場合は事後申請で構わない
私物デバイス（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	私物デバイスの登録，指定アプリのインストール，業務使用手引きの励行および誓約書の提出により承認
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，持ち込みを承認する
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，利用を承認する
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承認することもある
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	一時的措置が必要であると経営層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に社内メールを転送	原則禁止	業務上理由がある場合は，申請の上，転送を承認する
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，一時的に利用を承認することもある
国内法非準拠のクラウドを利用する	クラウドの利用契約は国内法準拠とする	クラウドベンダーもしくは当該クラウドの仲介業者と個別に国内法準拠の利用契約を締結すれば承認する
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，一時的に利用を承認することもある

5.4　利用者がもつ例外措置への阻害要因

例外規程を策定し，例外措置を実施するにあたり，そもそも例外措置の適用を受けようとする（あるいは受けようとしない）利用者がもつ例外措置への阻害要因を把握した上で，それらに対する対策を検討する必要がある．本節では，利用部門・利用者側の立場で例外措置への阻害要因を明らかにし，阻害要因への対応策をもとに例外規程を提言する．

5.4.1 例外措置の実施を阻害する3つの要因

原則規程から逸脱したもののうち，組織が「例外措置」として認定した措置であっても，利用者がそれを守らないことが考えられる．利用者が例外措置を遵守することへの阻害要因としては以下の 3 つが挙げられる．（参考文献91に筆者加筆）

（1） 例外措置の存在自体を知らない

まず決められた例外措置を遵守するためには，これから行おうとしている行動が，原則規程はもちろん，例外措置の範囲内でもあるかどうかを知っているということが大前提である．これは，もし利用者が例外措置の存在を知らなければ，自分が行おうとしている行動が原則規程から逸脱しているという認識があったとしても，それが例外措置の適用範囲からも逸脱するおそれがある「不安全行動」であるのかどうかまで認識することができないからである．すなわち，利用者は逸脱した行動であるという自覚がなく，例外措置によって救済されるものかどうかも知らないことになる．

（2） 例外措置が存在することは知っているが，正確に理解していない

例外措置が存在することを知っていても，その背景について正しく理解していなければならない．その例外措置がなぜ策定されているのか，またその例外措置にはどういう意味があるのか，等である．もしこのような背景についての知識がなければ，例外措置の重要性についての認識を見誤り，規程違反を犯しやすくなる．

（3） 例外措置が存在することは正確に理解もしているが，守らない

実務経験が豊富なベテラン担当者は，技術も知識も十分に備わっているはずである．にもかかわらずリスクを十分に判断できずに（あるいは判断せずに）実際には規程違反を犯してしまう場合がある．規程や例外について熟知しているがゆえに，自分勝手な作業をし，結果的にリスクを招いてしまう．

このうち（1）及び（2）は，行為者（利用者）の例外措置についての知識不足が，

91) 岡部康成，事故や災害を防止するために,リスク・マネジメントの心理学，新曜社,pp.245-270, 2003.

規程違反を犯す原因となっていることが分かる. 知識不足が原因である規程違反であれば, これまでの知識教育を中心とした安全教育によって防止することができる. 特にこれらの規程違反の防止には, 徹底した「ノウ・ホワイ(Know why)教育」, つまり, ものごとの原理原則・根拠・背景などを理解し, 本質的な問題点を見抜き解決する力を養うことを目指し, 体験学習や実習・演習・訓練を多く取り入れるものが挙げられる[92].

しかし(3)は, 知識教育を中心として行ってきた安全教育では十分に防止することができない. また, 例外措置をよく理解して例外措置を守らないという場合には, 例外措置からの逸脱行動がリスクをともなっていることを認識した上で, あえて危険な行動を選択しているのである. 心理学でいう, リスク・テイキングである[93]. 人間がリスク・テイキングしやすくなる状況として以下が挙げられる.

- リスクに気が付かないか, 主観的にリスクが小さいとき
- リスクを犯してでも, 得られる目標の価値が大きいとき
- デメリットが大きいと分かっていても, どうしてもリスクを取らざるを得ない場合

なお, 上記の行動は人間行動だけでなく組織行動にも当てはまる. 即ち, 現場担当者だけでなく, 知識が十分にある現場管理者や, 組織全体の経営に携わる経営者も陥る可能性のある「結果としての逸脱」であることは, 人間本来の行動から来るものである. これは心理学では古くから指摘されている. リスクは目的・目標があってはじめて定義されるため, 目標達成のためにリスクをあえてとる基本方針をとるならば, おのずと例外措置の幅も広げざるを得ないものと考える.

5.4.2 守らない利用部門における組織性逸脱との関連性

前項でも触れた「組織行動」における逸脱については, 法定境界線を越え, それでも法を犯してでも行われてしまう組織不正もみられる. 昨今の組織不正(表 5-2 参照)は, 組織が法定境界線を越えた結果であると考える. 組織の非常事態への回避のため, 不正と知りつつ組織維持のために逸脱行為をし, その場をしのぐことができれば, 根本的な解決を先送りにして, その後も例外措置として継続していく. しかしその例外措置が新たな事態に対応しきれなくなり, やがては不正行為が明るみに出る. 例外措置が法定境界線を超えているため, 捜査当局によって明らかになったのち, 罰則を受けることにつながっていく.

92) 赤崎貫志, 新林栄一, “ヒューマンファクターの現状とヒューマンエラーのゼロ化を目指してⅢ 化学プラントのヒューマンファクターと安全教育”, 電気学会論文誌 D,vol.117, No.6, pp671-672, 1997.
93) 芳賀繁, 違反と不安全行動, 失敗のメカニズム, 角川ソフィア文庫, pp.147-166, 2003 年 7 月 25 日.

この要因としては，本間氏らの「組織性逸脱行為」理論が参考となる[94]．組織性逸脱行為とは「集団的効果を目的として，集団内メンバーにより感知され，違反の実行者を含む複数の直接的・間接的関与者によって生じる一般社会に照らして逸脱した行為であり，当該集団の外の人々に何らかの悪影響をもたらす集団行為」である．従来，組織体犯罪・組織体違反行為・ホワイトカラー犯罪などと呼ばれてきた[95]．

表 5-2 平成以降の主な大企業による組織不正の一例[96]

年	事件
平成 9(1997)年	山一証券損失隠し隠ぺい
平成12(2000)年	雪印乳業食中毒事件
平成16(2004)年	三菱自動車リコール隠し
平成23(2011)年	オリンパス損失隠し
平成27(2015)年	東芝不正決算
平成30(2018)年	神戸製鋼検査データ改ざん
平成30(2018)年	スルガ銀行不正融資

組織の不正行為の特徴としては，主に次の 4 つを掲げている．

- 複数の成員（組織の構成員）が集団効果として組織利益または組織存続を求めて行為に及ぶ．すなわち，組織内では成員は組織目標に向かっての協働作業に従事するため，組織目標へ向かう行為は賞賛され，それを拒む行為は抑制され非難される傾向にある．
- 不正行為に関与する成員は，実行犯としての直接関与者ばかりでなく，直接は関わらないが不正を容認する間接的関与者が存在する．

94) 本間道子編著，“組織性逸脱行為過程”，多賀出版(2007)

95) この理論の目的は，社会心理学的視点から不正行為がなぜ生じるかを組織の要因から解明することにある．そもそも違法行為を起こした当事者は，従来社会のルールに従い，よき社会人であり，往々にして仕事熱心で仕事仲間の評価も良い社員であった．本間らは，不正行為は，個人の資質やパーソナリティなど個人特性ではなく，むしろ状況・組織環境などの影響があるのではないか，と指摘する．そこで，集団あるいは組織体という社会的構造・社会関係性がこのような逸脱の生起を生じ易くさせたり，不正を促していたりしているのではないかとする仮説をたて，組織・集団心理学に立脚した組織犯罪のメカニズムを分析した
なお，組織性逸脱行為と職務犯罪との違いについては，以下の3点を挙げている．
・平常時目的が個人利益ではなく，組織利益（集合効果）である．
・複数の多様な関わり方による関与者で成り立つ．
・間接関与者の方が，逸脱行為に心理的影響を及ぼす．
組織性逸脱行為がいかに悪質であるか，さらに深刻な損害をもたらすことになるかが推察できる．

96) NHK スペシャル，“平成史スクープドキュメント第2回　バブル終わらない清算　～山一証券破綻の深層～”，日本放送協会，(オンライン).
http://www6.nhk.or.jp/special/detail/index.html?aid=20181202. (アクセス日：2019 年 6 月 10 日).

・ 不正行為がいったん発生すると，それは当該組織ばかりでなく，一般社会に甚大な被害をもたらす可能性が高い．
・ 通常の個人犯罪と比べて不可視性が高く，加害者と被害者の関係が明確にならず，その特定化も難しい．

これらのことから，情報セキュリティ施策においては，組織不正が本来の原則規程の枠組みを超え，原則規程と法定境界線の間の逸脱領域において行われていることが推定できる．

したがって組織内の逸脱行為が法的逸脱に及ばないために，例外措置を実施することが求められ，さらに当該例外措置の管理・運用の可視化を図るために，例外規程を策定する必要がある．これにより例外措置への申請手順を明確にし，組織内で周知徹底させることが予防の一効果につながるものと考える．換言すれば，たとえ例外規程を策定したとしても，組織内で活用できなければ，組織を不正行為から防ぐことはできない．このことは例外規程を運用していく上での留意点となる．

5.4.3 組織の不正行為に関する先行研究から得られる考察

情報セキュリティポリシーを知っていても守らない組織の構成員や組織自体に対し，逸脱行為を阻止する対策については，これまでいくつか先行研究が報告されている．

ある事例では，逸脱防止への組織での対策として，情報セキュリティ業務の可視化を進めることで，構成員にとって分かりやすくし啓発を促せるとしている．別の事例では従業員の情報セキュリティへの取り組みへのモチベーションを上げることで，逸脱への対策が心理的に受容されやすくなると考えている．さらに，情報システムが持つ安全性を示すことで構成員の業務に対して情報セキュリティポリシーからの逸脱即罰則とならない安心感を与えるといった事例や，逸脱には罰則が伴うことを周知・教育することで，逸脱行為ではなく例外措置を実施させ，逸脱行為による罰則適用から萎縮効果が期待できるとした報告がある．

その上で，最終手段として，佐藤氏（3.2.1 項参照）が推奨している，例外措置と罰則をセットとし，「罰則を伴う逸脱」と「罰則を免除する例外規程」との境界を明確にすることは，一つの対応策の原点になると考える．

なお先行研究に関する詳細は事例については，付録 A3 もしくは初出一覧（8）及び（9）を参照されたい．

5.5　例外規程適用の限界への見解

以上，本章では例外規程の活用について，活用する意義，例外規程の策定主体と注意点，例外規程にすべきかどうかの考え方，さらには利用者が持つ例外措置への阻害要因の捉え方について述べてきた．これらをもとに例外規程を策定し管理・運用していけば，例外規程の持つ効用を得ることが期待できる．すなわち業務の効率化が期待できる．

その一方で，これらを講じて例外規程を活用したとしても，その適用には限界もあると考える．これは 2.4 節で述べたように，例外が本来持っている限界があり，それを認識したうえで例外措置の実施さらには例外規程の策定に結びついていることから明らかである．本節では例外規程への活用を図っていく上での限界について考察する．

5.5.1 例外規程策定への限界（残余リスクとの関係）

まず例外規程を策定する上での限界について，例外が本来持つ残余リスクとの関係をもとに述べる．

特に天変地異の多い日本では，原則規程は基準ではなく標準とみなされ，絶対的なルールではない．そのため根本から揺らぎがある状態の原則規程と例外規程の運用には難しい面がある．これは例外規程及び例外措置がもともと原則規程にもとづいて策定・実施されているためである．例外措置をどこまで認めるべきかの限界については，特に例外措置の範囲やリスクを判断する管理部門側のスキルや経験などに左右される．

このように例外規程の管理・運用の徹底を図る必要性としては，例外措置がもつ残余リスクへの解釈に曖昧さがあり，それを考慮することに帰する．本来，情報セキュリティポリシーが原則規程のみ（つまり，完全合理性）での管理・運用であれば，「残余リスク」は明確に把握することができる．しかしながら本研究では，情報セキュリティポリシーを原則規程のみで管理・運用することは困難であると述べてきた．そこで例外措置を実施することにより，柔軟に業務を維持することができるとも述べてきた．ただし不明瞭な例外措置の適用で管理・運用を緩和しすぎてしまうと，どこまでが残余リスクなのか把握できない状態に陥る可能性がある．

一方，2.4 節でも述べた Simon の限定合理性によれば，人間には，将来の不測事態をすべて予見したり，最適な行動を計算に入れたりすることは出来ないという，知的能力の限界があることを指摘している．そして経済主体の行動として生涯効用の最大化といった極限までの合理性を前提とせず，あらかじめ定めた限られた範囲での次善的な最適化に止めるべきと提言している．

このことから，例外規程自体も人間が作り出す規範であることから，同じく限定合理性に留意し，できる限り残余リスクに対する一時退避を考慮した例外規程の策定が求められることになる．すなわち，情報セキュリティポリシーが原則規程と例外規程とを併せ持ったとしても，限定合理性にもとづく残余リスクに対する限界があることを留意する必要がある．

5.5.2 例外規程運用への限界（技術進歩とのバランス等の配慮）

次に例外規程を管理・運用していく上での限界について，2.3.3 項で触れた技術進歩と例外との関係について述べる．

組織活動において，組織の情報インフラ整備における技術進歩と原則規程とは整合性が取れない（合致しない）ことから，原則規程のみでの管理・運用していくには限界がある．そこで例外規程を策定しそれに基づいた例外措置を実施することで，技術進歩との整合性が難しい原則規程を補完し，組織の運営に情報インフラを十分に利用できると考える．

しかしながら 5.4.3 項の組織性逸脱への関連性にも触れたが，組織内で能動的に運用できる例外規程でなければ，技術進歩とうまく整合できず，かえって組織運営の弊害になる可能性も否定できない．このことが例外規程の管理・運用における限界の一つであると考える．

5.5.3 例外規程がもたらす業務効率化への限界（想定外などの概念との関係）

最後に，例外規程そのものの意義にもあたる「業務効率化」への限界と情報セキュリティ業務で遭遇する想定外の事象に対する管理策について述べる．

5.5.1 項で述べた限定合理性にかかる解釈は，例外規程に限らず，情報セキュリティポリシー全体にも及ぶものと考える．つまり 1.1 節で述べてきた不確実性（あるいは想定外）のマネジメントにも限界があると解釈する．

すなわち，情報セキュリティポリシーそのものに不確実性・想定外への対策が必要とされているのであれば，それに基づいて策定される原則規程と例外規程においても，不確実性・想定外への対策が当然求められる．しかしながら，特に例外規程において，これらに留意して策定する事は容易ではない．これを実現するためには，原則規程と例外規程の策定にかかる専門知識が必携となる．また組織そのものの業務意識改善も要するものであると考える．

一方，業務意識改善において，Weick は「マインドフルネスな組織づくり」[97]を

97) 佐藤（3.2.1 項参照）は，K.E.Weick の日本語版著書「不確実性のマネジメント」への書評において，

提唱し，マインドフルネスな組織化を実現するための要件を以下に掲げている．

・現状の予想に対する反復的チェック
・最新の経験に基づく予想の絶え間ない精緻化と差異化
・前例のない出来事を意味づけるような新たな予想を生み出す意志と能力
・状況の示す意味合いとそれへの対処法に対する繊細な評価
・洞察力や従来の機能の改善につながるような新たな意味合いの発見

しかしながらこれらを習得するにおいても，まずは業務上において相当な訓練と，経験に裏付けられた知識の獲得と意識改革が要求されることは推定できる．

Weick はさらにこれらを意識した上で，さらに不測の事態を予測し，「失敗にこだわる」「単純化を避ける」「オペレーションに敏感になる」の 3 点を認識することが望ましいと述べている．また不測の事態を抑制するために「レジリエンスを決意する」「専門知を重んじる」をさらに意識（あるいは決心）するべきと提言している．なお最後の専門知においては，5.2.1 項で述べたように管理部門・利用部門が程よく融合し柔軟に協調する体制により，各部門にて専門知識の獲得が期待できると考える．

このように不確実性を伴う，想定外な事象への対策に例外規程が適用できるかどうかは，それを策定・運用していく組織の業務意識にも深く関わることが考えられる．言い換えれば，例外規程の効用が組織の意識内にとどまってしまうことが，例外規程の限界の一つであるとも考える．

次のように不確実性のもとでの組織のマネジメントについて論じている．
「確かに昨今の企業が取り組む課題には，予想不可能なことが多くなっている．それが予想できないことにより，自信を失うこともあるのではないだろうか．しかし，そもそも予想できないものは仕方ないという姿勢で取り組む場合もある．不確実な事象をマネジメントするために確実なものにするという発想ではなく，それらを不確実なままでマネジメントしようという観点が求められる．計画的な手順の大切さとともに，本来，それとは矛盾する計画外の事象への取り組み方との関係を整理していく．これら2つの位置づけを理解して設計することで，それぞれの効果が最大化することの意味を知ることができる」．

小括

本章では，第 3 章および第 4 章までの調査分析を受けて，例外規程の活用に向けての対策を述べた．

例外規程を適用する意義は，例外措置を汎用的にルール化することで，承認作業を可能な限り簡便化・省力化でき，業務効率が図れることにある．さらに例外規程を体系化・モデル化することにより，管理・運用の可視化が期待できることにある．

例外規程の活用を考えるポイントは，例外規程を策定する主体部門の在り方，原則規程からの逸脱行為のうちどのような態様のものを例外規程にすべきかどうかの判断基準，そして利用者がもつ例外措置への阻害要因の 3 点がある．例外規程の策定主体については，策定自体は利用部門が担い，策定に対する承認権限は管理部門が担うとした，管理部門主導タイプと利用部門主導タイプとを程よく融合し柔軟に活用することを提案する．例外規程にすべきかどうかについては，新規の例外措置の実施によるリスクが比較的大きくないと判断し，その実施内容および適用範囲がルール化できるものであれば例外規程として策定する．さらに利用部門が持つ例外措置への阻害要因を把握し，それらに対する対応措置を考える必要がある．

さらにこの章では，例外規程を適用しても超えられない限界についても述べ，例外規程を活用する上での留意点とした．

例外規程策定については，出来る限り残余リスクに対する一時退避を考慮した例外規程の策定に努力する必要がある．また組織内で活用できうる例外規程でなければ，かえって阻害要因となる可能性も否定できない．さらに不確実性・想定外への対策が求められるため，原則規程と例外規程の策定にかかる専門知識と，組織の業務改善への意識が必要となる．

次章では結言として，例外規程を活用していく上での提言とビジネス展開への期待について述べる．

6. 結言

以上，本論文では，例外措置を実施し，例外規程を策定することで管理・運用することが日常業務への負担軽減につながり，結果として業務の効率化が図れるのか，また原則規程からど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の適用を認め，業務を継続していくことができるのか，という疑問について探求してきた．そして内外の先行事例調査及びアンケート調査を通じて分析・考察を重ねることで例外の必要性と限界について認識し，例外規程の活用に向けての対策を論じてきた．

本章では結言として，例外規程の策定及び例外措置の実施に向けたポイントを示し，普及に向けての提言及び今後の展望について述べていく．

6.1　これまでの各章のまとめ

まず，これまで第 1 章から第 6 章までで述べてきた内容をまとめてみる．

第 1 章「研究の背景・動機・目的」では，まず研究をはじめた時代背景と，個人的動機について述べた．

2014 年から 2017 年にかけて情報システム部門に在籍していた筆者は，例外措置に関する申請窓口で「例外」を運用することになったのがきっかけとなり，例外の存在意義，必要性，煩雑性，運用の在り方について興味と疑問を持つに至った．

情報セキュリティ施策はその性質上不確実性が伴うため，想定が難しい問題や事象に対しては「例外」を考えざるを得ない．これが例外の必要性である．また例外に対して何らかの措置をする場合，それぞれの事象に対して個別事情を考慮した対応を考えなくてはならないため，「判断」という作業が伴う．これが例外の煩雑性につながる．したがって例外にかかる措置を例外規程として策定することで，一般化と個別事情への配慮という，相反する目的間のバランスをとることができると考える．

また例外は，常に原則と密接に関係して考える必要がある．例外はあくまでも例外であり，例外は原則に対する逸脱であることは避けられない．そこで情報セキュリティポリシーから逸脱している行為に関して，それを例外としてどの程度まで容認するのか，またそれを容認することによって新たに生ずるリスクが容認するメリットを上回らないか（効用対リスク効果），という判断が求められる．

さらに例外の適用には「管理部門主導タイプ」と「利用部門主導タイプ」の 2 種類あり，組織がそのどちらを使うかにより，組織の運用姿勢が把握できるものと考

える.

第 2 章「例外の定義と研究対象，必要性と限界」では，本論文における例外の用語と研究対象について定義し，例外の必要性と限界の基本的な考えを述べた.

例外措置とは，原則に対する逸脱において，その逸脱の内容・範囲を把握し，原則規程もしくは通常措置と同程度の効用対リスク効果が期待できるとして，承認権限者から許可を得た措置であると定義する. 実務的にいえば，例外措置は，原則規程をすぐに改定できず，通常措置として対応しきれない状態もしくは通常措置そのものがない状態において，利用部門の判断や管理部門での承認に基づいて一時的に実施される措置である.

例外規程は例外措置の根拠規程として，同一もしくは類似する例外措置の適用が多い状況において，代替手段の導入も含め，例外措置の根拠を規程として策定したものとして定義する. 言い換えれば例外措置を管理・運用していくための，措置の申請，承認・許可，実施，報告，さらには見直し等といった手続きやその内容について明確に策定した根拠規程であり，組織はこれらを記録し保存していく. これは業務の効率化に直結することから，例外措置をできる限り例外規程として策定し管理・運用していくよう，組織は努めるべきである.

本論文では，「平常時」のもので，情報セキュリティポリシーの 3 層構造のうち「対策基準」における例外規程及び例外措置に絞って研究を行った. これは対策基準が基本方針と比べ日常業務に直結し，組織のリスク対策の変化などに柔軟かつ定期的に対応しなければならないことや，平常時は非常時と比べ見直し頻度が高く，かつ長期間運用され，管理部門により原則規程からの逸脱程度の判断や評価が定期的に管理されるため，定式化しやすいと考えたからである.

例外には業務の効率化が図れるなどの効果が期待できる一方で，例外がもつ残余リスクや，利用部門における心理的作用などに起因する行為や措置などへの留意点も考慮しなくてはならない. これらを理解したうえで例外を適用することが望ましい.

第 3 章「例外の先行事例」では，例外の実態を把握するために，研究対象である「平常時の対策基準における例外」に関する先行事例（国内事例，国際規格事例，海外事例）の調査結果を紹介した.

本論文において最も参考としたのが例外措置を体系的に記述している NISC の統一管理基準である. これをもとに日本では省庁や関連組織だけでなく，金

融機関等の民間企業の一部で例外措置が実施されていることがわかった. また ISMS 認定を受けている組織であれば, 例外措置の導入が不可欠であると考える. さらに国際規格や海外の企業の事例では, 一部の組織がすでに例外規程を導入し, 例外措置の申請・承認・運用がなされている. さらに事前の例外申請がない逸脱行為は違反と認定され罰則の対象と明記している組織が多いことも興味深い.

しかし, 先行事例の多くは申請手続きに関するものが多く, 組織が例外規程を策定して例外措置を実施しているかどうかについては判定することはできなかった. また管理・運用の主体部門については, 管理部門が多いと推定できないものの断定はできなかった. さらにどのような原則規程からの逸脱行為が例外措置とされているかについては, 多くの組織が不明であった. 例外規程や例外措置の実態に関する包括的な統計資料を取り扱った文献もなかった.

先行事例調査から, 例外措置を実施しているだけでなく, 例外規程によって管理・運用している組織では, 業務の効率化が図られているものと推定する. しかし直接的に公表されているわけではないことから明確に判定することはできなかった.

第 4 章「例外措置の実態の把握」では, 第 3 章の間隙を埋めるため, 日本の組織を対象にアンケート調査を実施し, その結果を分析した.

組織において例外措置を実施しているかについては, 本調査では直接的に設問していないものの, 例外規程を策定している組織が約 4 割程度あり, 少なくとも当該組織は例外措置を実施していることがわかった. また組織において例外規程を管理・運用している主体については, 画一的な管理部門主導タイプばかりではなく, 現場組織の判断が優先される利用部門主導タイプでも例外措置が実施されていることがわかった.

さらにアンケート調査の結果から次の 3 つを課題として見出した. ①例外規程を持つ組織と持たない組織とが概ね同数で両極化している. ②管理部門の統一的な基準を元に策定され, 現場向けにカスタマイズしている例は少ない. ③見直しは定期的ではなく必要に応じて実施されている. これらの結果から例外規程は十分に普及していないものと判断せざるを得ない.

また同じアンケート調査で, 原則規程と例外規程の策定状況について集計・分析した. その結果, 管理策によっては「原則規程のみを策定し通常措置を実施している」もの, 「例外規程を策定し例外措置を実施している」もの, さらには「原則規程も例外規程も策定していない」ものがみられるなど, 一律でないことが

分かった. 具体的な管理策においては, 例えば「可搬型メディアの使用」や「外部インターネットの使用」については, 原則規程として策定しているという回答が多い. 一方で,「サポート切れのソフトウエアの使用」では例外規程として運用しているものが比較的多い. しかし「日本国内法非準拠のクラウドの使用」や「第三者認証の無い外部クラウドの使用」などについては, 多くの管理策において, 原則規程, 例外規程ともに策定されていないことが明らかになった.

本アンケート調査の集計・分析の結果から, 例外規程を策定している組織においては業務の効率化が図られていると推定する. しかし上述の 3 つの課題から, 必ずしも利用部門においての例外措置の実施が, 現状に沿った例外規程の策定および管理・運用となっているとは限らないことがわかった.

第 5 章「例外規程の活用に向けての対策」では, 第 3 章および第 4 章までの調査分析を受けて, 例外規程の活用に向けての対策を述べた.

例外規程を適用する意義は, 例外措置を汎用的にルール化することで, 承認作業を可能な限り簡便化・省力化でき, 業務効率が図れることにある. さらに例外規程を体系化・モデル化することにより, 管理・運用の可視化が期待できることにある.

例外規程の活用を考えるポイントは, 例外規程を策定する主体部門の在り方, 原則規程からの逸脱行為のうちどのような態様のものを例外規程にすべきかどうかの判断基準, そして利用者がもつ例外措置への阻害要因の 3 点がある. 例外規程の策定主体については, 策定自体は利用部門が担い, 策定に対する承認権限は管理部門が担うとした, 管理部門主導タイプと利用部門主導タイプとを程よく融合し柔軟に活用することを提案する. 例外規程にすべきかどうかについては, 新規の例外措置の実施によるリスクが比較的大きくないと判断し, その実施内容および適用範囲がルール化できるものであれば例外規程として策定する. さらに利用部門が持つ例外措置への阻害要因を把握し, それらに対する対応措置を考える必要がある.

さらにこの章では, 例外規程を適用しても超えられない限界についても述べ, 例外規程を活用する上での留意点とした.

例外規程策定については, 出来る限り残余リスクに対する一時退避を考慮した例外規程の策定に努力する必要がある. また組織内で活用できうる例外規程でなければ, かえって阻害要因となる可能性も否定できない. さらに不確実性・想定外への対策が求められるため, 原則規程と例外規程の策定にかかる専門知識と, 組織の業務改善への意識が必要となる.

本章「結言」では，第 1 章から第 5 章までの議論を総括した上で，例外規程の普及に向けての提言，および可能性について述べる．

6.2　例外規程の普及に向けての提言

本節では，5 章での例外規程の活用に向けての対策をもとに，例外規程の策定及び例外措置の実施に向けたポイントをまとめながら，本論文としての例外規程の普及に向けての提言を述べる.

6.2.1 情報セキュリティポリシー基本構造ごとに例外規程を策定する

例外規程は，情報セキュリティポリシーの基本構造を構成する基本方針，対策基準，及び実施手順それぞれに策定されているのが望ましい. 特に対策基準での例外規程は，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. 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に，日常業務に沿った部門ごとの例外措置を実施して，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常に行うべきである.

6.2.2 例外規程を予め策定する

情報セキュリティポリシーが完全に確定した段階で情報セキュリティ業務を運用することは難しい. そこで情報セキュリティポリシーに基づく原則規程が維持できないときに用いる例外措置は，業務継続のためのバッファのようなものである.

例外規程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に移行できる利点がある.

本学原田研究室での 2015 年度のアンケート調査の結果では，例外規程は組織によって導入程度が異なっており，全体で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を示した. その一方で，情報技術への依存度の高い情報通信業やサービス業ではそれら半数に活用され，また政府や自治体では統一管理基準の例外措置を推進してきた. さらに 2018 年度アンケート調査結果でも，徐々に例外措置を活用する組織が増えてきていることが窺われる.

一方で例外規程に予め策定しておくことで，情報セキュリティポリシーの維持にどの程度貢献できているのかを知る必要がある. 具体的には，例外を可視化できなくては，規程策定に向けての事務手続・承認・運用が普及することは難しい. すなわち，例外規程があることで，セキュリティ上どの程度，安心・満足できるのかについて数値化して示すことができれば至便である.

本研究では，例外規程と例外措置の実施の効果を，原則規程との逸脱程度と例外措置との関係（想定 7，第 4 章参照），及び例外規程に伴う例外措置への評価基準（想定 8，付録 A1 参照）を用いて検証している. その結果，原則規

程と例外規程とのバランスや定量的評価の提示が重要であると考える.

6.2.3 例外措置の許容範囲を決めておく

例外措置は, 原則規程から逸脱した事象をすぐに違反として懲罰するのではなく, 日常業務を運用するに許容できる範囲及び条件に当てはまると承認者が判断できるならば, 一時的に原則とは異なる措置を承認することができる. これにより, 業務の停滞や停止を迅速に回避する効用が期待できる.

そのため例外規程は, 情報セキュリティポリシーからの逸脱に対する許容範囲を明確に判断し, 情報セキュリティポリシーの定期的な見直しとともに策定することが求められる. 本来これらは, 各組織で実際にリスク分析して管理策を情報セキュリティ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重要である.

例外措置は原則規程と同等のリスク低減を備え, 原則規程では逸脱する事象に対して即座に対応できる効果が求められるだけでなく, 利用者にとって使いやすい効果も求められる. アンケート調査からは例外措置を必要としていなかったり, 知らなかったりしている可能性もあることが分かっている. これらのことから, 例外措置をどの程度, どのくらいの頻度で講じるべきか, また例外規程をどの範囲内で策定するべきかについては, 重要な要素である.

さらには, 的確に例外措置を実施できるだけの素質(6.2.5 項参照)が利用者および利用部門に求められる. 申請内容と素質を照らし合わせて, 例外措置の承認にランク付けする仕組みが必要と考える.

6.2.4 例外規程の策定には例外措置の信頼性を求める

例外措置があることで, 情報セキュリティポリシーやそれに基づいて策定される原則は例外の相互補完によって, それ自身変更の少ない運用が期待できる. そのためには, 例外措置に対する信頼性が求められる. 具体的には, 例外規程を策定することが有効であるかどうかの評価を定量的に明示化することで, セキュリティ上, どの程度安心・満足できるが分かりやすくなると考える(付録 A1 参照). これによって例外措置の効果を可視化し, 常に見直しの参考にすることにもつながるものと考える. また利用者側が本来抱いている例外措置への阻害要因への対策(5.4 節参照)についても, 分析して対処していく必要がある.

今後, 例外措置の蓄積による多様化も踏まえ, 6.2.5 項のレベル別例外措置を取り入れた例外規程により, 利用者あるいは利用部門のスキル等でランク付けされた例外規程で, 管理部門による例外措置への承認および利用部門での実施が有効であると考える.

6.2.5 申請者の資質でレベル別に例外措置を承認する

5.4 節(併せて付録 A3 参照)では, これまでの先行事例をもとに逸脱行為への対策について, 罰則の適用も含め述べた. 本節では申請者(利用者)もしくは申請部門(利用部門)のスキルや経験に応じてレベル別に例外措置を承認する考え方を述べる.

承認可否の判断の時間短縮を目的に, 従来の手順を省略する例外措置を認めるためには, 過去の例外措置への実績と, 例外措置を実施できるだけのスキルを持ち合わせているかが問われる. この点を例外措置適用への承認判断に利用する. すなわち例外措置を, 申請者あるいは申請部門のスキルや経験, また例外措置それ自体が持つリスクにそれぞれ条件化し, それら条件に見合ったレベルの例外措置を適用させるという, いわば「レベル別例外措置」の活用を検討課題として提議する.

このレベル別例外措置の導入は, 例外措置と申請者あるいは申請部門の持つ適性度を示すことにつながり, 例外措置の承認判断の基盤となって, 判定基準(バロメーターあるいは目安)となる. 例えば「可搬型メディア使用への対策」と「国内法非準拠のクラウド使用への対策」とでは, 例外措置申請の対象媒体が全く違い, それぞれの環境で, もとは原則規程として策定されていたものなのか, それとも例外規程を策定して対策したいものなのか, また各々の利用頻度やセキュリティ対策等においても, 適性度が異なるものと考える. さらには申請者や申請部門によっても, それらが持つ「スキル(作業処理能力)」,「経験」,「資格」および「権限」により, 適性度は異なってくるものと考えられる.

そしてそれら資質と例外措置においてのリスク回避の難易度とを組み合わせることでレベル別例外措置とし, 迅速で的確な判定を促し, 業務効率の向上につながるものと考える. したがって例外措置は, 画一的に実施するのではなく, 各々の適性を鑑みた上で例外規程を策定・管理し, 措置を行うことが必須であると考える.

例として 5.3.1 項の「可搬型メディア」での USB メモリの使用を取り上げる. USB メモリのリスクとしては「外部への機密情報の流出や漏洩」があり, 例外措置として「あらかじめ取引先でウイルススキャン済みの USB メモリを受領するのであれば作業許可する」とする. これにより申請者は USB メモリに機密情報を格納した業務で使用することが可能となる. ここで「レベル別例外措置」の活用した場合, IPA の情報処理技術者の資格の有無や高度情報処理技術者レベルの保有スキルによって, USB の種類や格納する情報の制限を設定することができる. すなわち申請者もしくは申請部門の責任者が無資格者であれば 300 ギガバイト

までの容量で機密情報の格納は不可とし，基本情報処理者であれば 1 テラバイトまでの容量で機密情報の格納は可能とし，情報処理安全確保支援士など高度情報処理技術者レベルであれば容量及び情報の種類は無制限とする，というようなレベル別もしくはスキルに見合った例外措置が可能となると考える．

このようにレベル別例外措置を導入することで，承認者は客観的に申請者が例外措置を実施するに十分な資質を有すると判断できる．それと同時に，実施そのものに対する権利と義務を付与することで，「例外措置があるとわかっているのに守らない」利用者への管理が可能となる．

6.2.6 例外規程を管理部門と利用部門が協調して策定・運用する

例外措置は各組織で実際に実施して経験を積まなければ，その効果の程度をはかることは難しい．一方，例外規程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．情報セキュリティに関する規程が全ての組織において必須施策の一つである昨今では，各組織それぞれに適応した例外措置の導入も検討していく必要がある．

しかしながら例外規程の実態を見る限り，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る．また，個々の組織において個別に情報セキュリティポリシーや例外規程を策定することは難しいのが現状である．

そこで，NISC の統一管理基準が広く活用されているように，まずは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全ての組織で活用できるような体制作りなどを検討していく必要があると考える．

そして 5.2.1 項で述べたように，例外規程の策定主体は，管理部門主導タイプと利用部門主導タイプを程よく融合し，それらを柔軟に活用することで，例外を取り扱っていくことが期待できる．

6.3　例外規程によるビジネス展開の期待

原則規程は，原則であるゆえに保守的な規程にならざるを得ない．一方組織によっては，基本方針での原則規程の範囲を狭くし，ビジネス展開を狙う目標・目的をもつために，例外規程を広げて例外措置を位置付けることもできる．

つまり例外措置により，リスクに対して積極的にリスク・テイキングする業務を遂行することもできる．この場合，基本方針にて例外措置を承認し，例外措置が持つリスクをしっかり受け止めて，業務拡大を進めることも可能と考える．例えば，新規デバイスの導入を積極的に実施していくといった内容の例外規程を予め策定し，それに基づいた例外措置を実施していく．

一方，日本社会においては，契約書に明記されていない事項については双方紳士的に話し合いで解決することが慣習的である[98)]．転じて，決められていないことは，その場で関係者が集まり，とにかく一時措置を決めて実施する．あるいは責任者の判断で実施する．規程の策定はその後で決めることが一般的に行われている．この慣習を，例外規程を策定する機会をとらえ，「決められていない」一時措置をできる限り例外措置に転用できるかどうかの調整の場として活用していくことが求められる．

なおビジネス展開においては，付録 A2 章では，ケーススタディとして中小企業を取り上げた．中小企業こそ例外規程を活用することでビジネス展開が図れる可能性があるものと考える．

さらに例外措置の活用においては，情報セキュリティポリシーに直接的あるいは間接的に関連する他の分野でも期待できる．例えば，情報セキュリティシステムへのアジャイル開発[99)100)]や，人工知能（AI）・ロボット開発[101)]において，開発設計段階で想定できない開発要素・工程への修正対策などを，例外措置を用いて柔軟に対応することが期待できる．

98) 明確に例外規程を策定しなくても明示的に例外を許容でき，罰則の適用を避け，説明責任も明確にできる．あえて例外を特別視しなくても，何とか業務を継続することができていたことが，例外措置策定の普及を難しくしているのではないかとも考えられる．

99) James R. Fitzer, “Agile Information Security”, BookBaby, 2015

100) 情報処理推進機構, “アジャイル開発の進め方”, 2018 年 4 月．(オンライン). https://www.ipa.go.jp/files/000065606.pdf. (アクセス日: 2019 年 6 月 10 日).

101) 村﨑ほか, “テレビを一緒に視聴するロボットの開発ガイドライン策定に向けての一考察”, 情報処理学会研究報告,vol.2017-EIP-78, No.14, 2017.

6.4　おわりに

博士前期課程修了後の 2017 年 6 月，筆者は組織内定期異動のため，情報システム部門から研究開発部門に移った．情報セキュリティポリシーを策定・管理する立場から，利用・遵守する立場に変わった．そして担当していた業務から離れて，今度は例外申請をすることになった．

利用・遵守する立場で例外措置を扱ってみて，例外規程の策定をより客観的にみることができるようになった．例えば，外部クラウドの例外申請については，管理部門の立場ではクラウドベンダーへの調査依頼や運用マニュアルの作成，上長への承認印の受領などを当たり前のように指示していた．しかしながらこれらの申請書類の提出が実に煩雑なものであると実感した．一方，例外規程があることで，例外申請への審査に必要な事務処理における，申請者との個別面談や上司への相談が簡便化・省力化できていた．これはすなわち業務効率があったものだと感じている．

さらに，技術進歩により原則規程の適用が困難になり，例外規程の適用を実体験できた．USB メモリである．USB メモリは情報システム部門在籍中では全面禁止とされ例外措置は認めてこなかった．それが可搬型媒体を管理できるシステムを導入したことで，USB メモリのシステム管理が可能となり，例外措置として使用が認められることになった．この情報インフラ整備では，逆のケースもある．例えば IBM では当該企業管理下のファイル共有システムを導入したことで，原則許可されていた USB メモリの全面禁止に踏み切ったという報告がある[102)]．このように，進化する情報インフラは，本論文に述べているとおり，組織の規程の見直し（技術進歩を取り入れるための原則規程との整合）が必要となることが確認できた．

また，管理部門の申請窓口業務で経験したことを振り返ってみると，例外措置の取り扱いは，例外規程がないのとあるのとでは承認作業の時間と手間に，第1章でも述べたとおり大きな差がある．すなわち，もともと例外措置の承認作業に例外規程がなければ，管理部門においてはかなりの業務負担につながる．現場の立場からは，個々の審査・承認あるいは上長へのエスカレーションの利用は避けたい．そもそも原則規程が厳密であれば，認めないと明確に指示できる．原則規程が曖昧で都度例外措置を実施するようになると，管理業務は承認行為が増えて煩雑となり，水面下での逸脱が起きることにもつながり，組織のガバナンスにも影響が出る可能性もある．

---

102) IBM の記事については例えば，Tech Target Japan の 2018/11/7 の記事：(オンライン).
https://techtarget.itmedia.co.jp/tt/news/1811/07/news04.html (アクセス日：2019 年 6 月 10 日).

では，例外規程・例外措置は利用部門には有用であり，結局のところ管理部門には有用ではないと断定できるものか？筆者は否と考える．それは，例外措置が多かれ少なかれ情報セキュリティポリシーにおいて対応せざるを得ない実態であることを，本研究で明らかにしたからである．どれだけ情報セキュリティポリシーとそれに基づく原則規程を確立しようとしても，技術進歩，法改正への対応，働き方改革などによる仕事環境や仕事のやり方の変化などから，業務・ビジネスでのリスクが大きく変化するため整合できなくなる．したがって原則規程に明記していない事象への対応が余儀なくされる．ここにおいて，例外措置（あるいは例外措置とは呼称しないまでも，本論文で述べた例外措置の概念に基づいて実施される行為）を実施することにつながる．例外措置は管理部門では承認・管理せざるを得ない業務実態であるならば，あらかじめ例外規程を策定しておくことは，有用であると考える．

次に組織経営の面から考えてみる．例外措置（あるいは例外措置の概念に準じた措置）は，情報セキュリティポリシーを策定している組織であれば，必須の措置と考えるが，その一方で，例外措置を明文化するかどうか，すなわち例外規程を策定するべきかどうかは組織の判断に委ねられている．むしろ政府統一管理基準によって官公庁等が導入を義務付けていないのであれば，例外規程の導入は自由である．あるいは「例外規程」という名称でなくとも，部門毎で策定している規程等において例外措置を明記している事例もあろう[103)]．いずれもしても，これからの組織運営には例外措置に関して，なんらかの規程が事前に導入されており，常に見直しを行うことが求められる．

筆者は，例外規程と運用が，組織での情報セキュリティの方針を示す情報セキュリティポリシーに基づいていることから，この例外措置の実施状況を把握することは，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一つになると考える．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，経営層に対して例外の必要性を知らせる必要がある．なぜなら経営層が関わることについては，NISC の統一管理基準で例外措置の管理台帳を CISO が担っている事例（3.2.1 項参照）があることからも明らかである．例外の必要性については 2.3 節でも述べたが，さらには，情報セキュリティポリシーがもつ逸脱領域との境目のゆらぎを，自由度がある例外により許容範囲として

103) 初出一覧にて議論となってきた，例外規程も明文化されればそれは規程であるから原則規程ではないか？と寄せられた指摘の根本的な理由である．本研究では本論文で述べてきたとおり，例外はあくまで例外であって原則でなりえない．この概念のもと，それぞれ明文化されているとはいえ，措置の実施内容と承認・管理手続き等，さらに心理的影響への観点から，原則と例外とで区別するべきと主張してきている．勿論，組織それぞれの仕組みや方針，観点等から今後も議論すべき論点であるとも認識している．

カバーできる点，さらに原則規程と例外規程との調和をとることで業務を遂行していくことができる点が考えられる．例外措置が日常業務に組み込まれることで業務継続が容易となり，いわゆる事業継続にも貢献できるようになる．これらの効果としては，まず例外措置への実行処理速度を早くすることが，結果的にコスト削減につながる可能性がある．また措置内容に属人的な判断が少なくなり，より客観的に判断・審査・承認を進めることができる．

繰り返しになるが，例外措置は各組織で実際に規程を策定して措置を経験し，自組織での事例を増やし，組織学習をしていかなければ，当該組織に適応する例外措置の獲得とその効果を得ることは難しい．社会全体や業種ごとにおける具体的な例外措置の共有化など，全ての組織で例外措置の活用を見据えた体制作りなど，今後検討していく必要があると考える．

最後に，当初，本研究テーマを半信半疑で指導教官はじめ何人かの先生方やゼミ内で相談したことの印象を今でも忘れない．それは，筆者自身，「例外」が研究テーマとして受理されるとは，「想定外」であったからである．しかし相談を受けていただいた先生方・学生・客員研究員からは，ほぼ肯定的な意見を頂いた．とても意外であった．しかも情報セキュリティマネジメントの初心者であった筆者に，先生方から研究方針や方法を懇切にご助言していただき，とても励みになったことを覚えている．

その一方で，「例外規程」の在り方を学内外で広め，認知していくことは相当難しいということもわかり，これは現在に至っている．初出文献での査読論文をはじめ，これまでも様々な専門家や先達の方々からご意見・ご助言を頂き，時には議論してきた．それだけ情報セキュリティマネジメントにおいて「例外」を研究することは新奇性があり，あるいは「例外」「想定外」だったのもしれない．

本研究に従事し，本論文を執筆するにあたって，「例外」といえども曖昧・適当に扱うことは，情報セキュリティマネジメントにのみならず，どの分野においても許されない時代になってきていると実感する．そして例外につながる考え方やその規程の策定，それに基づく例外措置の実施がその補完手段の一つであると筆者は考える．

例外を研究・探求してきたことが，組織や人々の活動への一助になれば幸いである．

（付録）

A1 例外規程策定への定量的評価の試み

例外規程を予め策定し，例外措置を実施することが有効かどうかを判断するためには，なんらかの指標により評価する必要がある．そこで，本研究では例外措置の許容範囲を検証するにあたり，例外規程の策定に対する効果への満足度を評価する試みを行った．

本章では 2015 年度アンケート調査の結果から，主観評価実験手法に基づく定量的評価を用いて述べる．なお本章の内容は，初出一覧（10）の学会発表予稿をもとにしている．

A1.1 例外規程における具体的効果に関する調査（想定 8）

本調査では 4.1 節の想定 8「例外規程への評価を定量的に明示化でき，セキュリティ上の満足度が分かりやすくなる」に基づいて設問 23 を設定し質問した．

設問 23 は例外規程による効果に対して，主観的にどの程度満足・安全に感じているかをたずねている（表 4-2 参照）．具体的には表 A1-1 に示す設問肢それぞれに対して「とても満足・安心」から「とても不満・不安」までの6段階評価で回答を求めた（表 A1-2 参照）．なお例外規程による具体的効果についての設問肢は，他の設問で使用した設問肢や 3 章の先行事例のなかから，を列挙した．

表 A1-1 設問 23 における設問肢一覧（例外規程による具体的効果）

(1)	迅速に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)	規程違反として罰則適用を未然に防ぐ
(5)	次期規程策定への参考，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程全体に効果がある

表 A1-2 回答選択肢

規程別	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

設問 23 における単純集計結果を図 A1-1 に示す. なお設問肢は表 A1-2 に示す「満足・安全圏」の合計の多い順に並べている. 図 A1-1 からは, 9 つの例外規程の具体的効果のうち,「次期規程の見直し」「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.

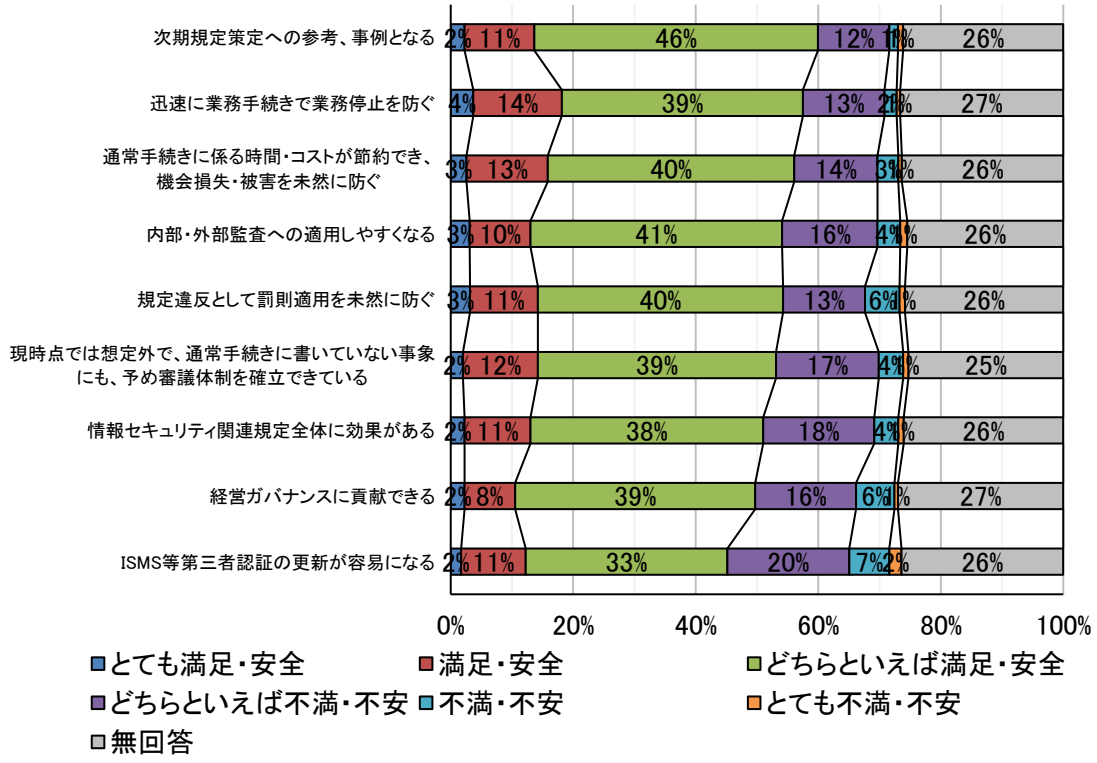

図 A1-1 具体的な目的や効果に対する主観的評価

（択一, N=352）

また無回答を除き，単純に「満足・安全圏」と「不満・不安圏」とで区分けしたものを図 A1-2 に示す．図 A1-2 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．

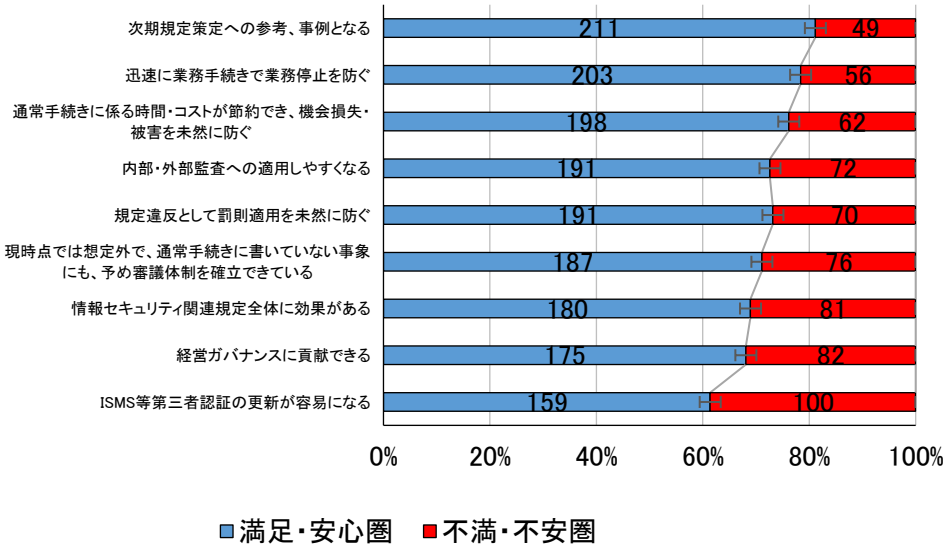

図 A1-2 満足・安心圏－不満・不安圏別グラフ
（択一，グラフ内の数値は回答数）

A1.2 二重刺激劣化尺度法による主観評価分析

図 A1-2 の示すように，満足・安心圏が不満・不満圏を上回った点をさらに分析するために，図 A1-2 の結果を二重刺激劣化尺度法（以下，分析法）[104]を用いた主観評価分析を行った．この分析法は主に画質・音質劣化の主観評価に利用されており，本研究ではこれにより，例外規程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．

まずデータの前処理として，アンケート設問 23 中の 6 段階回答選択肢と，分析法の 5 段階評価点との互換をとった（表 A1-3 参照）．具体的にはアンケート回答選択肢の「とても満足・安全」と「満足・安全」は，分析法の評点 5「気にならない」に属するものとみなして互換を図った．

前処理で回答選択肢と評価点との互換をとった上で，設問肢ごとの累積評点を求め（図 A1-3 参照），さらに設問肢間での累積評点の相関を分析した（表 A1-4）．表 A1-4 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．

104) ITU-R, “ITU-R 勧告”,Methodology for the subjective assessment of the quality of television pictures”, BT500-11”, 2006

表 A1-3 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

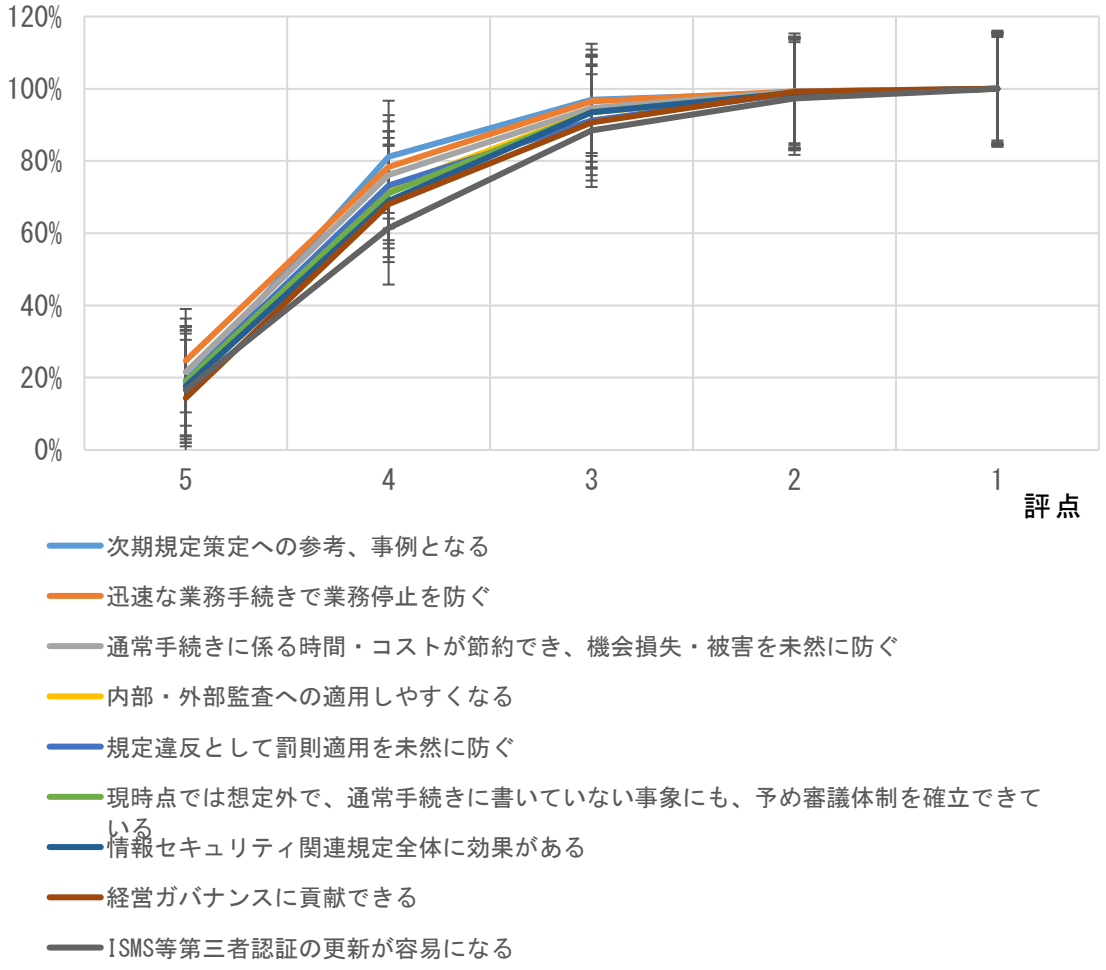

図 A1-3 設問肢別累積評点

表 A1-4 設問肢間での累積評点の相関
（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

次に図 A1-3 の設問肢ごとの累積評点の平均から許容限を求めた．その結果を図 A1-4 に示す．図 A1-4 中の平均値から近似式を求めた結果，評点 3.5 で求める許容限は 83.4（単位％），ならびに 4.5 で求める検知限は 49.2 となった．このことから回答者の 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程に対して「満足・安心」していることが推定できる．すなわち当該主観評価手法を用いることで，組織の満足度を数値化（定量化）して理解する手がかりの一つになると考える．

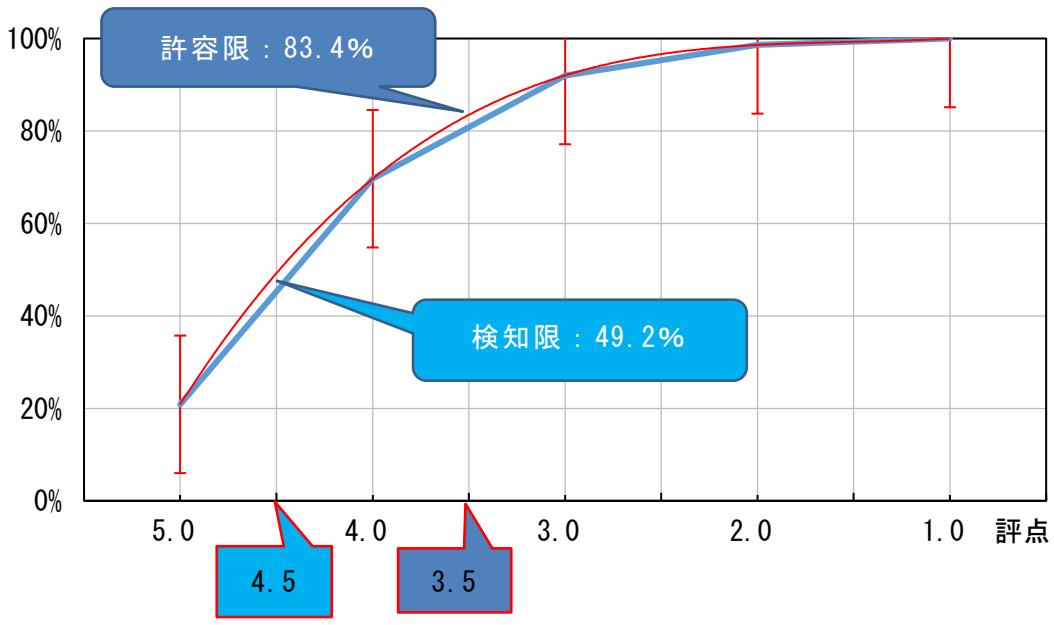

図 A1-4 主観評価分析結果

A1.3 主観評価分析結果へのヒアリング調査

本研究ではさらに，上述の許容限 83.4 について直観的な感想や意見を得るために，情報セキュリティ大学院大学内でヒアリング調査を試みた．

本調査は，2016 年2月 26 日に開催された 2015 年度 ISS Square シンポジウム (http://iss.iisec.ac.jp/)でのポスター発表（内容は非公開）の会場で，口頭で行った．ヒアリング内容については，「自組織の情報セキュリティポリシーにおける例外規程の「満足・安心」度は 80%である」ことを想定してもらい，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た．

その結果を図 A1-5 に示す．なお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 A1-5 の結果を単純に一般社会への評価にすることは難しい．

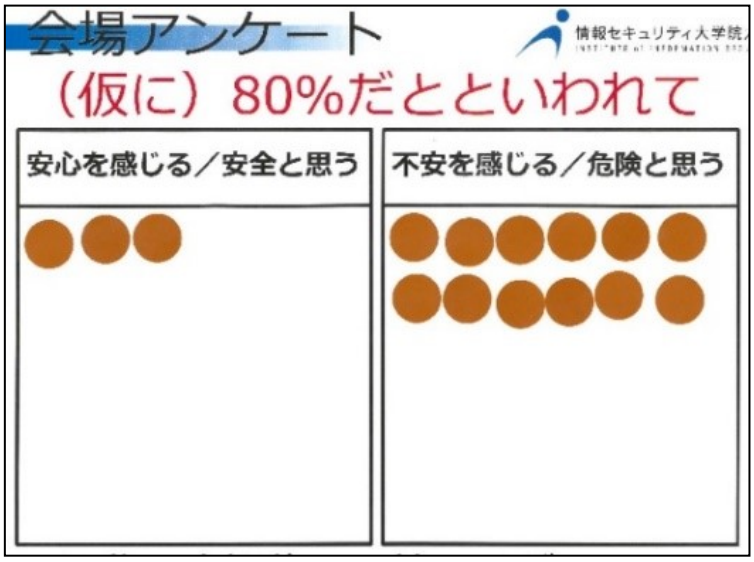

図 A1-5 許容限（%）に対するアンケート結果（択一，N=15）

しかしながら，12 名（80%）が「不安を感じる／危険と思う」と回答した．その主な理由として，「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．

このヒアリング調査は，さらに 2018 年 12 月 19 日で発表した博士研究発表会において，同様の質問を聴講生にも行った．その結果を図 A1-6 に示す．

「安心を感じる／安全と思う」への回答が 8 件，「不安を感じる／危険を感じる」への回答が 9 件と，ほぼ同数であった．このことから情報セキュリティポリシーにおける例外規程の満足度が約 80%というのは楽観的であるともいえないことがわかった．

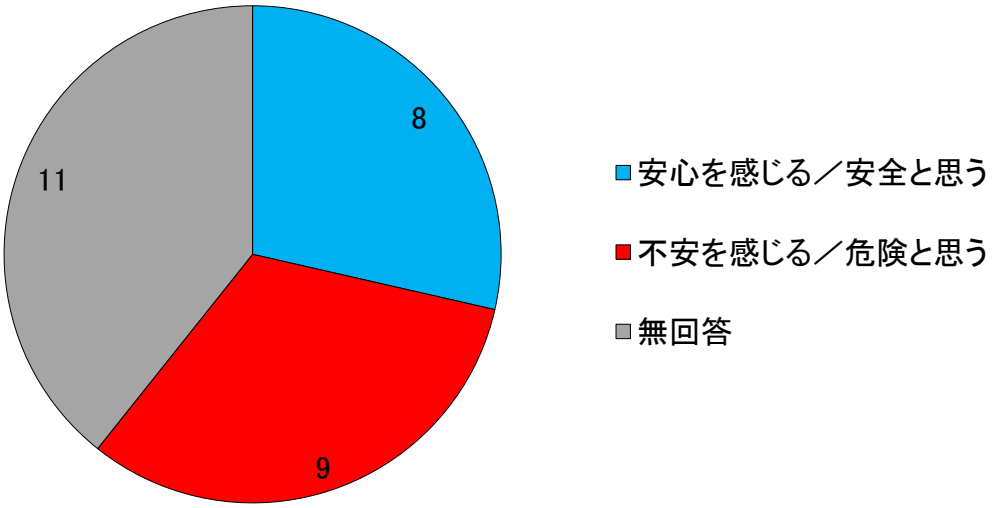

図 A1-6　許容限（%）に対するアンケート結果（択一，N=28）

これらのヒアリング調査は，サンプル数が少ないことから参考情報程度にとどまったものの，情報セキュリティへの満足度について議論する機会となった．

A1.4 例外規程策定済組織における例外規程の定量評価

続いて本研究では，実際に例外規程を策定している組織が，例外規程を満足しているかどうかを分析した．本節では，表 4-2 の設問 16 の結果を示す図 4-15 において，表 4-6 の「例外規程を策定」（「(3)例外規程に従い，例外措置をしている」と「(4)例外措置をしたことがない」を合わせたもの）の割合の高かった「可搬型メディア」（11.6%+2.8%=14.4%）と，低かった「日本国内法非準拠のクラウド」（2.0%+4.8%=6.8%）を取り上げる．それぞれ図 A1-7 及び図 A1-8 に設問 23 の各項目の満足度（図 A1-2 での満足・安心圏）を分析した結果を示す．

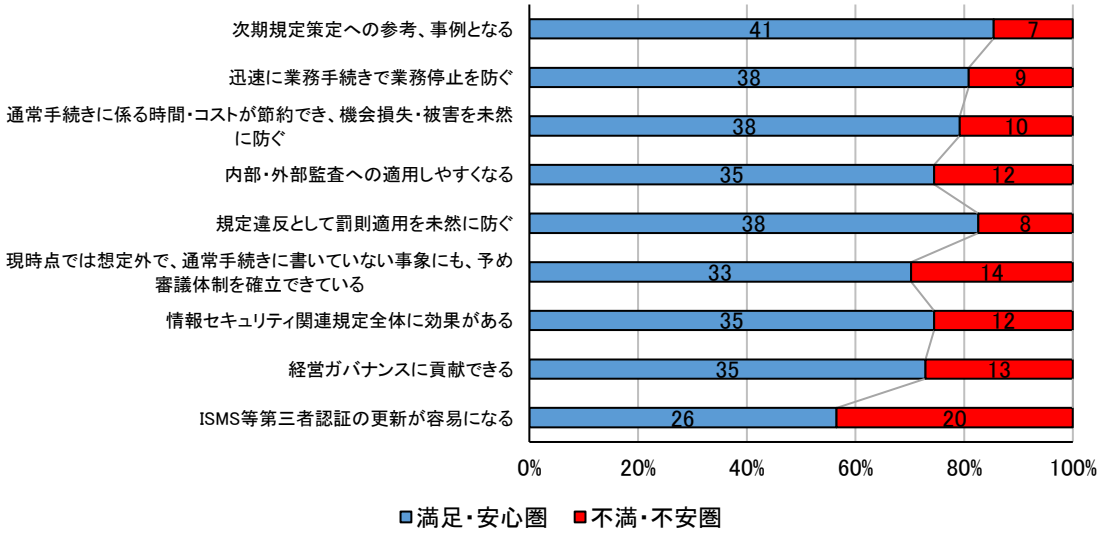

図　A1-7　例外措置を実施している組織における満足度
（可搬型メディアを利用する，グラフ内の数値は回答数）

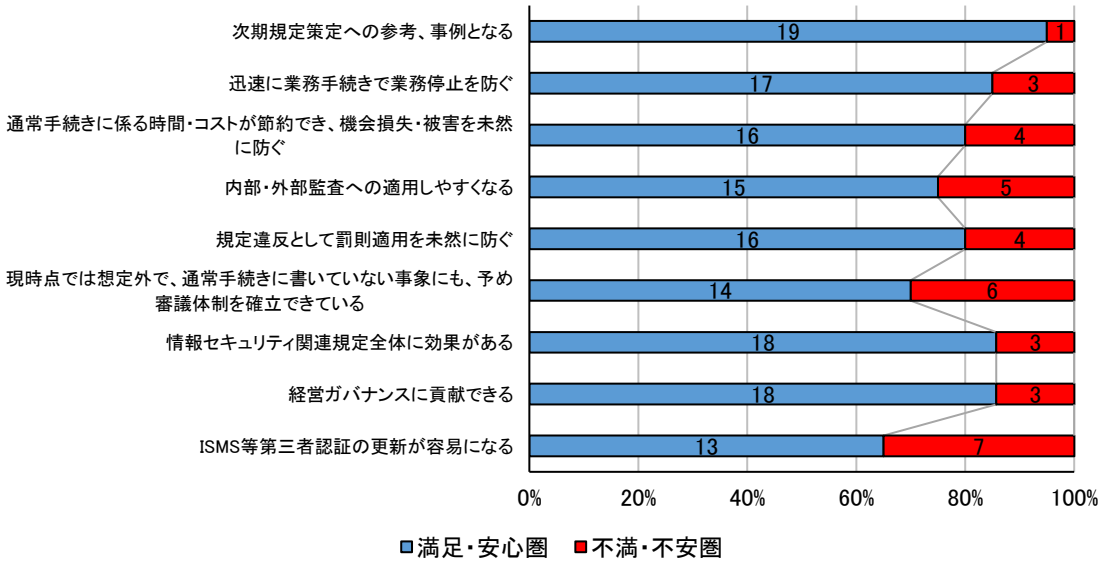

図　A1-8　例外措置を実施している組織における満足度
（日本国内法非準拠のクラウドを利用する，グラフ内の数値は回答数）

各項目でばらつきはあるものの，いずれも満足度（満足・安心圏）が 50%を超えていることがわかる．したがって例外規程を実際に策定している組織では，例外規程を策定する目的・効果それぞれに対して満足・安心に感じていると推定する．多かった項目としては「次期規程策定への参考，事例となる」「迅速に業

務手続きで業務停止を防ぐ」があげられ，例外規程がもつ特徴に対して評価が高いものと考える．一方「ISMS 等第三者認証の更新が容易になる」については他の項目と比べて低くなっている．ISMS（3.3.1 項参照）では例外措置が明記されているものの，実際には満足・安心と感じられるには至っていないということがわかった．

小括

以上，本章では，例外規程の策定における具体的効果への評価を定量的に明示し，その満足度について分析した．

アンケート紙面上で主観評価実験を行い，単純集計結果から二重刺激劣化尺度法を応用し，許容限を求めた結果，アンケート回答者の 8 割程度が例外規程に満足であると試算した．さらにこの試算結果を情報セキュリティに精通した者からヒアリングした結果，当該許容限の結果では満足できるものでないとする j 評価を得ることができた．

また実際に例外規程を策定している組織から，例外規程への満足・安心度が高いことも明らかになった．このことから組織では，例外規程の効果を理解したうえで例外措置を実施しているものと推定する．

A2 例外措置の普及に向けての実践と拡張

本章では例外措置の普及に向けて，中小企業を例にケーススタディを述べる．

情報セキュリティマネジメント体制の確立は，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対応のため，中小企業でも情報セキュリティポリシーを策定し，それに則った原則規程に従って，日常業務を管理・運用している．

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で，原則規程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程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．

本論文では，比較的規模が小さい企業が例外措置を活用することで，情報セキュリティ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という効果が期待できることを述べる．

なお本章の内容については，初出一覧(3)の学会査読論文をもとにしている．

A2.1 中小企業における例外措置

中小企業においても，情報セキュリティポリシーを管理・運用する上で例外規程を策定し，想定外の事象にも対応できるようにすることが望ましい．このことは2015 年度及び 2018 年度アンケート調査結果を分析した結果からも，中小企業を含む一部の組織が例外規程を実際に策定していることが明らかになった．

A2.2 例外措置の実態

アンケート調査では，例外措置を実施する際の判断・決定において，原則規程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「原則規程を策定」「例外規程を策定」あるいは「例外規程は未策定」の何れかを尋ね，その結果を公表している．

本節では，さらに中小企業における例外措置の実態について分析した．その結果を図 A2-1 に示す．なお本研究では，中小企業を従業員数 300 人以下の組織とみなした[105)]．

105) 中小企業庁, “中小企業・小規模企業者の定義”, 中小企業庁, (オンライン). http://www.chusho.meti.go.jp/soshiki/teigi.html. (アクセス日: 2019 年 6 月 10 日).

図 A2-1 からは,「可搬型メディアの利用」項目に対し,「原則規程に設定」「例外規程に設定」(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, 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. その一方で, 使用を許可する例外規程を策定して, 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も分かる.

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 A2-2 に示す.

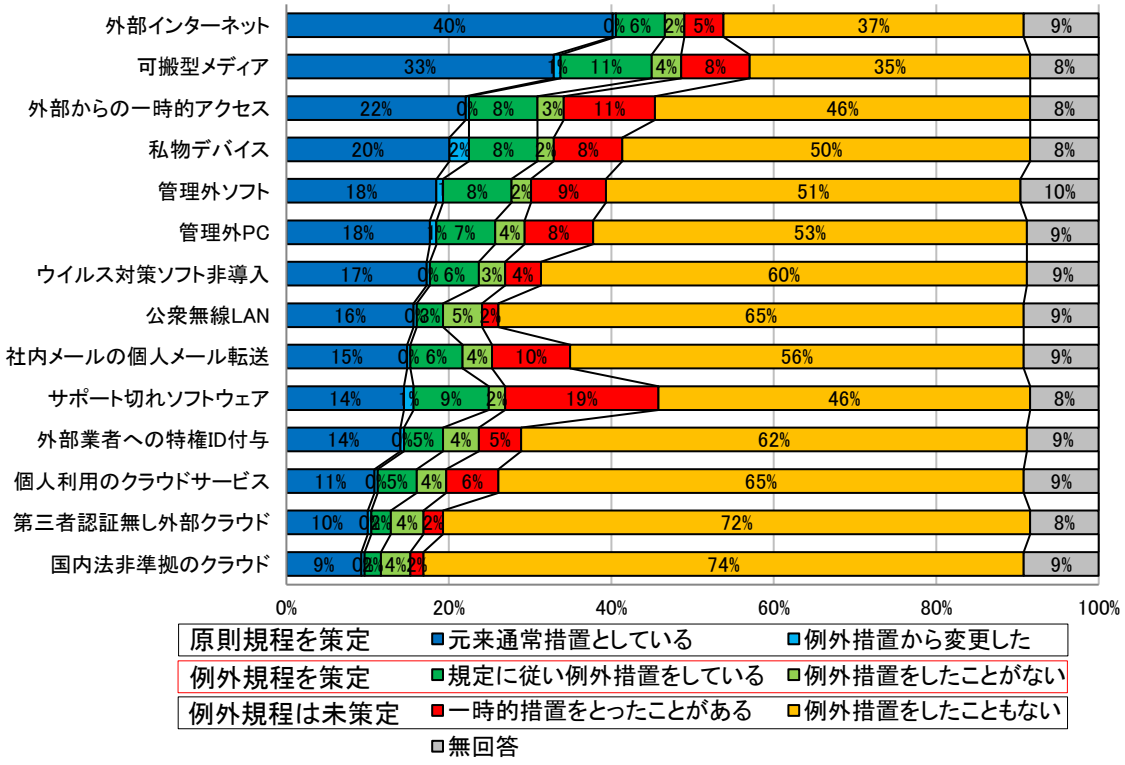

図 A2-1 中小企業における具体的な業務上の事象における例外規程の有無 (択一, N=249)

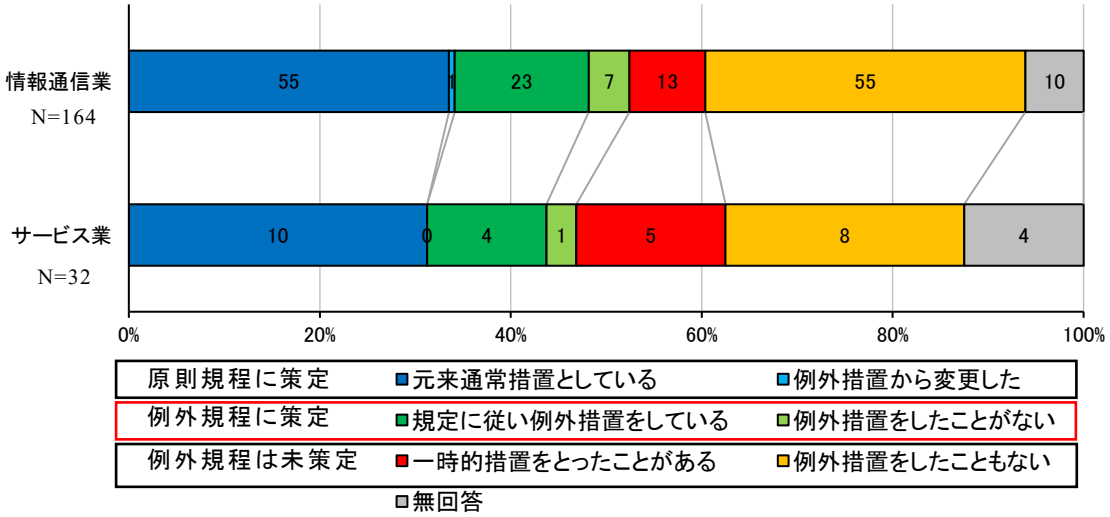

図 A2-2 業種別での可搬型メディアに対する例外措置の有無
（択一，グラフ中の数値は回答数）

図 A2-2 からは，情報通信業では「原則規程に設定」と「例外規程に設定」の合計が 52%（55+1+23+7=86 件）と，「例外規程が未策定」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．この結果から可搬型メディアの利用制限が原則規程もしくは例外規程として徹底されている中小企業とそうでない中小企業とで両極化されていることがわかる．

A2.3 原則規程と例外規程との関連性

図 A2-1 の単純集計結果から原則規程と例外規程状況のみを抽出し，原則規程の比率が高い順に示したものを図 A2-3 に示す．各管理策に対して原則規程もしくは例外規程が策定されている中小企業について以下のことが考えられる．

まず，具体的な管理策それぞれについて，例外規程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．このことから例外規程があまり活用されていないことがわかる．例外規程を策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，あるいは情報セキュリティポリシーや原則規程の策定において，例外の策定が想起されていないようにも考えられる．これは，中小企業が情報セキュリティポリシーを策定するにあたり，NISC のガイドラインを活用していなかったり，また，中小企業向けのガイドラインには例外規程の策定が記載されていないことなどが理由として考えられる．

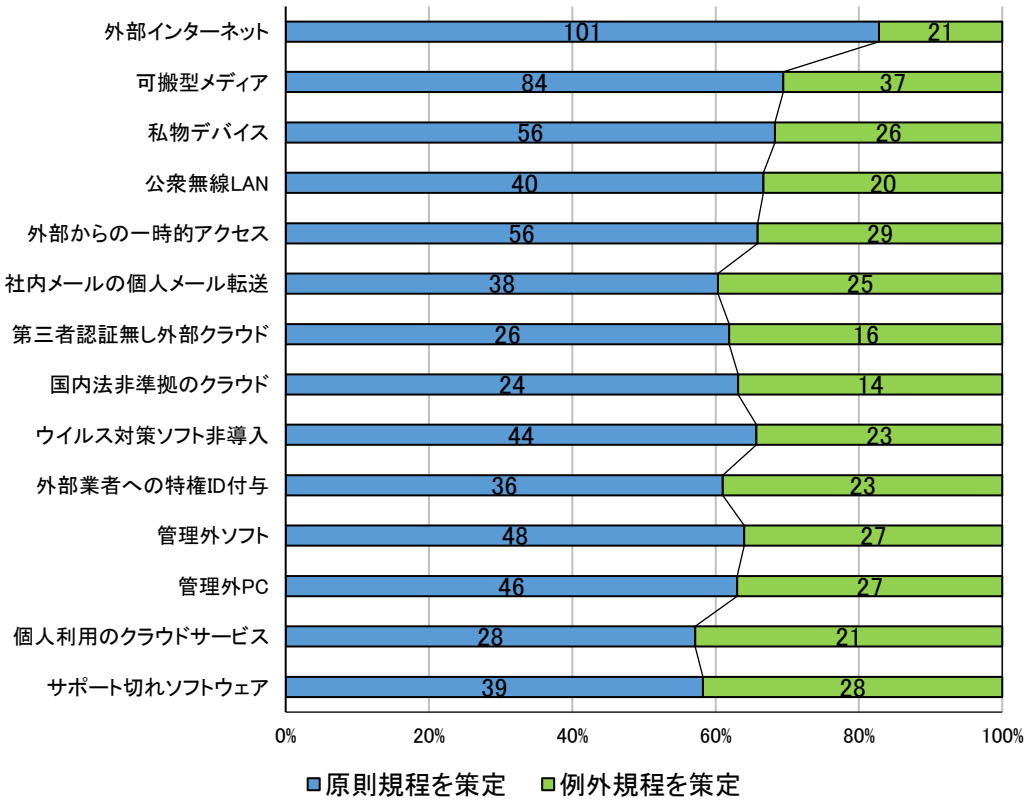

図　A2-3　中小企業における原則規程と例外規程との比率
（択一，グラフ内の数値は件数）

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，多くの中小企業でほぼ原則規程が策定され通常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，原則規程で対応する中小企業が多いものの，例外規程を策定している中小企業との差が少ない．これは中小企業において原則規程と例外規程とを組み合わせて，情報セキュリティポリシーの維持管理・運用を進めているためと考える．

さらには例外規程を適用する際には，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 メモリの外部持ち出し，BYOD の許可，外部クラウドの活用などの具体事例では，実際に原則規程もしくは例外規程がされている中小企業がある一方で，全く規程を策定しない中小企業もある．

以上，アンケート結果をまとめると以下のとおりとなる．

・例外規程は，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．
・同じ管理策への対応でも，業種によって例外規程を策定していたり，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.
- 原則規程と例外規程と区別して, 情報セキュリティ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る.

A2.4 中小企業における例外措置の限界

A2.3 節では中小企業における例外措置の実態と, 原則規程と例外規程との関連性について考察した. この中小企業について, 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[106)107)], 昨今の中小企業は, 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」[108)]では, 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とも報告している.

本節では, 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限界について述べる.

A2.4.1 例外を認める判断と適切な措置・リスク対応への限界

例外措置の適用については, まず例外をどの程度まで認めるのかについての「判断」が必要である. 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, この判断は中小企業ごとに経営者が決めなければならない.

一方で IPA の調査結果(文献 107)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

106) 情報処理推進機構, "中小企業の情報セキュリティ対策ガイドライン", 情報処理推進機構セキュリティセンター, (オンライン). http://www.ipa.go.jp/files/000014017.pdf. (アクセス日: 2019 年 6 月 10 日).

107) 情報処理推進機構, "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). http:/ww.ipa.go.jp/files/000014023.pdf. (アクセス日: 2019 年 6 月 10 日).

108) 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). https:/ww.ipa.go.jp/security/fy28/reports/sme/index.html. (アクセス日: 2019 年 6 月 10 日).

実施されていない中小企業も多い」「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」などが挙げられている．すなわち一般に，中小企業では人的なリソースの不足から，情報セキュリティポリシーにもとづく原則規程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である．その結果として原則規程が厳しいものになることが多いと考える．

これは原則規程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人的なリソースの不足から困難であると想定する．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がとれるように，例外措置におけるリスク判断や残余リスクの受容を柔軟に判断できるような体制を整備する必要がある．

A2.4.2 措置が持つ緊急性の判断への限界

USB メモリの例は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程よりも優先される．一方，平常時であれば，原則規程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程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，後者はルールや規程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滞りなく継続することが重要であると考える．

A2.5 中小企業の例外措置の活用に向けて

A2.4 節を受け，本節では中小企業を対象に，例外措置の活用とその対策について述べる．

A2.5.1 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，業種ごと・組織ごと・部門ごとに，それぞれリスクが異なる．例えば可搬型メディアの使用についても，情報通信業では，禁止とする規程や例外規程として規制がある一方で，サービス業では，使用が緩和されているなど異なる措置が取られている（図 A2-2 参照）．

中小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，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．即ち中小企業ごとに例外規程を策定させるには，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中小企業の経営方針，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・対応させることがより必要になると考える．

これは例外措置に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．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，定常的な原則規程でない限り，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る．

中小企業の場合，リスクが発現した場合においても，その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．

また規模が比較的小さいことで，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中小企業に適合しないと判断したときには，直ぐに当該例外措置を見直すこともできる．

これは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．

A2.5.2 競争優位に繋がる例外措置の可能性

一部の中小企業は，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程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策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，中小企業では以下の施策が考えられる．

まず類似の規程をもとに例外規程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，動きに時間がかかる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，中小企業を競争優位に繋げることが期待できる．しかし，例外措置の経験の少ない中小企業が，例外措置を実施する際は，間違った運用（逸脱）とならないよう気を付けなくてはならない．

A2.5.3 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，中小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，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．また中小企業は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をしていると主張できる．

A2.6 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，中小企業に適した情報セキュリティポリシーについて提案し，一例として，図 A2-1 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情報セキュリティポリシーについて述べる．

管理外 PC，スマートフォン，USB メモリに対する利用制限はあるものの，完全に禁止している中小企業では少ない．一方で，特に教育機関や研究施設，個人情報・秘密情報を扱う中小企業においては，禁止もしくはその企業から支給された可搬型メディアによる使用に限定されている．

これらから見て取れるのは，USB メモリは原則使用禁止，PC は中小企業が貸与するといった原則規程の策定を前提とし，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ているということである．

一方，IPA の調査結果などから，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 の例外措置は中小企業の多くが必要としており，例外規程は必須の施策であると考える．

具体的な案としては以下のとおりである．

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の種類」といった例外規程を策定し，これと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．

また利用が増えてきた場合は，例外措置ではなく原則規程とするべきか検討を始める．

この場合 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「シャドーIT」が蔓延してしまうおそれがある．その結果，リスクが見えにくく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，インシデント発生にも対応しやすいものと期待できる．監査の場合にも，管理部門が例外措置の実施状況という形でリスクの程度を確認できる効果も期待できる．

さらに BYOD の禁止は従業員への監視を強化することなどが必要となり，より管理部門の負担が増えることにつながる．中小企業の情報セキュリティポリシーについては，例外措置を含んだ柔軟な形で規則を策定することが，より現実的と考える．

なお管理策項目ごとに，情報セキュリティポリシーにおける原則規程と例外規程例の表 A2-1 を再掲する．中小企業では，これを利用して具体的な例外規程を策定すればよいと考える．なお管理策項目は 2015 年度アンケートの設問 16 を参照している．さらに表 A2-1 の一部を 2018 年度アンケートの設問 38 及び設問 39 に用いて調査した．その結果から中小企業を抽出したものを図 A2-4 及び図 A2-5 に示す．アンケート調査で集計したところ，図 A2-4 の傾向は組織全体を示す図 A2-1 と同様であると推定できる．

図 A2-4 の結果では，「可搬型メディアの利用（「原則規程に策定」と「例外規程に策定」合計 127 件，62％）」が他の項目と比べて差がある．その他の項目については，「規程に記載なく例外措置をしたことがない」と回答したものが多い．

図 A2-5 の結果では，「プログラム保守のための外部からの一時的アクセス（158 件，66％）」や，「個人で利用しているクラウドサービスの利用（139 件，58％）」である．一方で，例外措置で策定されている割合が高いのは「外部インターネットの使用（162 件，67％）」「自社が管理していないソフトウエアの使用（131 件，54％）」であった．

中小企業においても，原則規程で通常措置を実施するもの，例外規程で例外措置を実施するもの，あるいは双方区別して実施しているものなど，個々の具体的な管理策において特徴が表れている（A2.3 節参照）．

表 A2-1 情報セキュリティポリシーと例外措置対比表（例）（表 5-1 再掲）

管理策	原則規程例	例外規程例
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承認する
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のものであれば使用を承認する
サポート切れの OS やソフトウエア	サポート切れのOSやソフトウエアの使用は全面禁止である	完全に外部ネットに接続しないレガシーシステムについては承認することもある
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	一時的措置が必要と経営層が判断した場合は事後申請で構わない
私物デバイス（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	私物デバイスの登録，指定アプリのインストール，業務使用手引きの励行および誓約書の提出により承認
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，持ち込みを承認する
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，利用を承認する
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承認することもある
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	一時的措置が必要であると経営層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に社内メールを転送	原則禁止	業務上理由がある場合は，申請の上，転送を承認する
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，一時的に利用を承認することもある
国内法非準拠のクラウドを利用する	クラウドの利用契約は国内法準拠とする	クラウドベンダーもしくは当該クラウドの仲介業者と個別に国内法準拠の利用契約を締結すれば承認する
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，一時的に利用を承認することもある

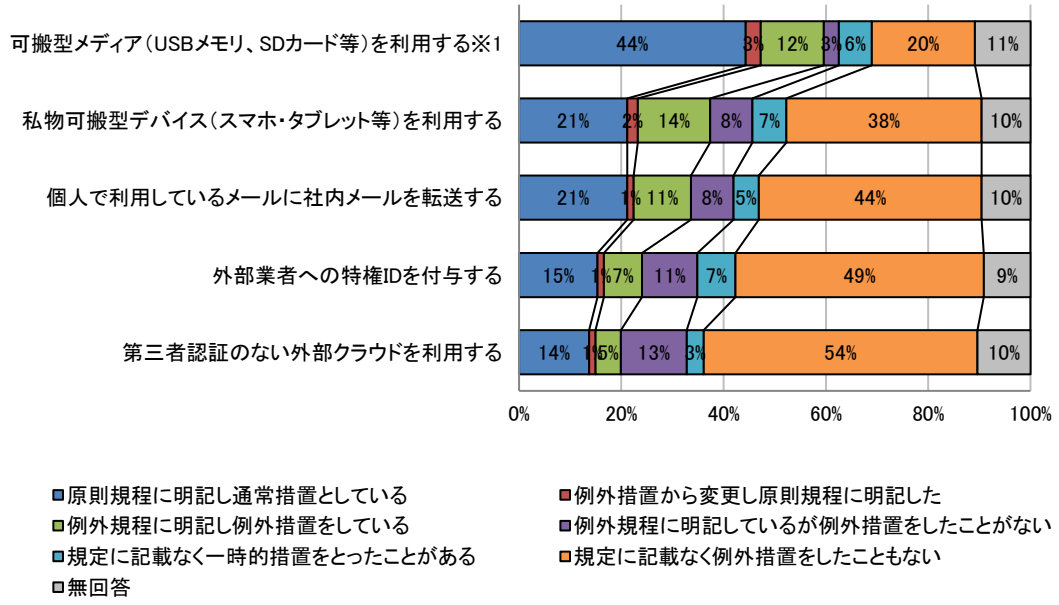

図　A2-4　具体的な管理策における例外措置の有無（図 4-17 参照）
（択一，N=203〔可搬型メディア～〕，その他の項目は 241）

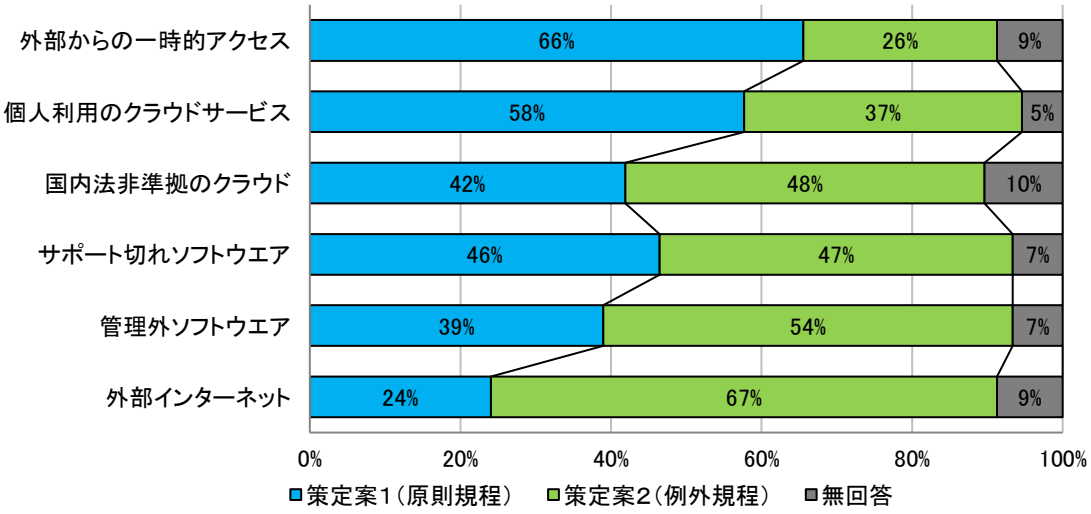

図　A2-5　具体的な管理策における原則規程か例外規程かの選択
（図 4-19 参照）（択一，N=241）

小括

本章では，例外措置の普及に向けてのケーススタディとして，中小企業における例外措置の導入を提案した．人的資金的にリソース不足である中小企業が大企業と対峙していくための方法の一つとして，例外措置の特徴を有効に生かし，ダイナミックにビジネス展開する手法が挙げられる．

また具体的な管理策において，原則規程例と例外規程例を例示し，2018 年度アンケート調査で集計した，「プログラム保守のための外部からの一時的アクセス」「個人利用のクラウドサービスの業務使用」においては原則規程で策定されている割合が高いことがわかった．一方で「外部インターネットの使用」「自社が管理していないソフトウエアの使用」では例外規程が策定されている割合が高いこともわかった．通常措置で実施するもの，例外措置で実施するもの，あるいは双方区別して実施するものなど，個々の具体的な管理策において特徴が表れている．

リスクが様々に変化する中で，組織にとって，情報セキュリティ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，中小企業も含め組織の一部では，アンケート調査にもあるとおり，原則規程及びリスクに対応して例外規程に基づいた措置を講じてきている．

一方，例外規程は，情報セキュリティポリシーに基づく原則規程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．すなわち例外規程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，頻繁に原則規程を見直すことは難しく，そのため例外規程を用いて柔軟に例外措置を実施するほうが効果的である．

中小企業では，人的リソースが不足しており，情報セキュリティポリシーや原則規程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．すなわち中小企業においては，リスクに対してきめ細かく情報セキュリティ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例外規程を策定し，例外措置によっていち早くそれらを利用することで，大企業に対して差別化をする．中小企業がこの機会をとらえ，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していく．最終的には，これを情報セキュリティ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．こうして中小企業では，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いえよう.

A3 例外措置の利用者側による実施阻害要因及び対応

本章では，5.4.3 項の補足として，例外措置の普及を図るうえで組織の構成員や組織自体における意識や行動に要因があることに注目し，特に例外措置の利用者である構成員における逸脱行為の傾向と，逸脱に関わる社会・組織との関係，さらにはこれらの逸脱行為への対策案について先行研究を調査した．対策案については，罰則の適用への利用と照らし合わせて紹介する．

なお本章の内容については，初出一覧(8)及び(9)の学会研究会発表論文をもとにしている．

A3.1 利用者における逸脱行為の傾向

逸脱行為に対して利用者はどのような背景と傾向があるのか．本節ではこれについての先行研究を取り上げる．

A3.1.1 利用者のセキュリティ対策におけるレベルの違い

利用者のセキュリティ対策は，そのセキュリティ知識とこれまでの経験に大きく影響を受けているとされており，また個人と仕事との責任分界への認識が対策にも影響があるという報告がある[109)]．これらの相互作用は，利用者がセキュリティ対策に関与する程度にも影響し，以下のとおり異なるレベルでの対策につながっていることが明らかになっている．

(1) 様々なセキュリティ対策が，様々な要因・程度で動機付けされるため，情報セキュリティポリシーへのコンプライアンスが複雑化している．
(2) 利用者は，セキュリティ対策が自分たちの仕事の環境を維持するために，職務の一環として強化していると，組織/管理者から知らされていないため，セキュリティへの対策労力は不要であると認識している．
(3) 同じオフライン業務・オンライン業務であっても，利用者それぞれセキュリティに対する脅威を受け止める感受性が異なる．
(4) 利用者がセキュリティタスクの責任を認識し，そのうちのいくつかは責任を受け入れ，他は組織に分散させる，リスク・テイキングへの理解が足りない．
(5) 利用者の個人と仕事との責任分界のあいまいさが職場での脆弱性につな

109) J. Blythe, L. Coverntry , L. Little, “Unpacking security policy compliance”, The motivators and barriers of employees' security behaviors, 2015 Symposium on Usable Privacy and Security, pp.103-122, 2015.

がる. 特に BYOD 等の使用については影響を受けやすい.

A3.1.2 リスクとベネフィットとの関係

リスク・テイキングは不安全行動の一種として, リスクの認知やベネフィットの認知からの影響を単独もしくは相互連動して影響を受ける[110)111)112)]. なお, ここでのベネフィットとはメリット(利点)によりもたらされる利益・利得を指す.

森泉氏らの研究によれば,「リスク受容においてこのベネフィットを主体に意思決定を行うことは, リスクレベルに関わらず, 非合理的なリスク受容判断につながる可能性がある. ベネフィットの大きさと敢行傾向は比例関係にあるが, 状況によってはベネフィットの物理量が小さくとも高い認知が得られることがある. すなわち小さいベネフィットを得ることに慣れ, それを行い続けると, さらに大きなベネフィットが期待できる場合には, リスク・テイキングしやすくなる. そのため次第に大きいベネフィットを受容する傾向にあり, ベネフィットの物理量の単純な増加のみでなく損失を回避することで, リスクに対する弁明ができると考えてしまう. したがって状況に応じてしばしばリスクを冒す傾向にある利用者は, 違反を敢行しやすいことが明らかになっている.」としている.

これをコスト面から考えてみると, この研究からベネフィットを得るためにかかるコストが大きい状況にも関わらず, リスク予防が留意されなくなることが示唆され, さらに大きなコストがかかる状況を経験すればするほど, リスク回避が機能しなくなる傾向にあると推定できる. すなわちリスクを伴う意思決定においてリスク回避が反映されにくくなるため, ベネフィットを得るためのコストが小さい場合でも, 大きいコストと同等のリスク選考を行ってしまい, 絶えずベネフィットを優先してしまうものと考える.

そのため, リスクを実際に被る可能性があること自体を行為者に知覚させることが, 違反を抑制することにおいて役立つ.

A3.1.3 利用者における時間リスクと逸脱

前項において, ベネフィットを得るためのコストが特に時間的コスト(待機時間)を伴う場合, すなわち必要な手続きを行うのに時間的負担が大きいと, 個人のリスクへの認知が低くなる. これは手続きに関する問い合わせ先を認識していない／しないなど逸脱を抑止できない原因になる. したがって業務優先等のためにセ

110) 森泉慎吾 , 臼井伸之介, "リスク傾向が違反敢行に及ぼす影響", 日本心理学会第 75 回大会, 2011.
111) 森泉慎吾, "リスク受容に伴うベネフィットがリスク受容判断の合理性に及ぼす影響", 産業・組織心理学会第 32 回大会発表論文集, 193-196, 2016.
112) 森泉慎吾 , 臼井伸之介, "時間的コスト認知とリスク受容に関する心理的要因の関係", 産業・組織心理学会第 33 回大会発表論文集, 2017.

キュリティルールを逸脱し，本人の意図に反して情報漏えいにつながってしまう[113].

さらには組織における情報漏えいは内部者に起因するものが多い[114]. 情報漏えいの原因となる違反行為の一つとされる「職場からの許可のない情報持出行為」については，例えば「早急に対応する必要がある」などの時間的なプレッシャーに曝されることにより，逸脱行為につながることが，根本的な原因となると考える.

なお岡野氏の研究（文献 113）によれば，「時間的リスクに伴う逸脱行為を行う人は，自分の人事評価を気にする人ほど起こしやすく，情報セキュリティに関わる知識が高いほど起こしにくい」ことがわかっている. そのため研修等の教育に頼るだけでは防ぎきれはしないものの，持出行動が原因で引き起こされる漏えい事故によって，どのような損害が組織に及ぶかを認知させることが重要と考える.

A3.1.4 利用者における情報セキュリティ被害傾向

逆に，情報セキュリティ被害の経験を 4 種類（ウイルス感染，不正利用被害，プライバシー漏えい，詐欺被害）に分け，それぞれに属する質問の影響度などを分析することで，セキュリティ対策への許容の度合いをみた報告がある[115].

寺田氏らの研究によると，「セキュリティ対策への心理負担の度合いが多いほど被害が少ない. セキュリティ対策は面倒であり負担に感じつつあるものの，対策を実施することで被害を少なくする傾向がある」ということがわかっている. 利用者が例外措置を実施する際に，例外措置から逸脱したと管理部門が判断した場合は，利用者に対し罰則を適用する. これにより，例外措置を承認されたことで心理的負担が軽減された利用者に対し，管理部門が改めて心理的負荷が加わることで，利用者自身が情報セキュリティ意識が再認識され，被害を受けることを抑える効果が期待できる.

一方で，セキュリティ対策へのコスト認知が低く，かつ，ベネフィット認知が高い場合には，対策費用をかけて情報インフラ整備や利用者教育を充実させることで，おおむねセキュリティ被害を減らす方向に作用しているものとみられる.

---

113) 岡野裕樹 ，奥山浩伸，“セキュリティルール違反行動の抑止に関する一考察”，情報処理学会論文誌 Vol.58, No.1, pp,258-268, 2017.

114) NPO 日本ネットワークセキュリティ協会，“2017 年 情報セキュリティインシデントに関する調査報告書【速報版】”， (オンライン). https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf. (アクセス日：2019 年 6 月 10 日).

115) 寺田剛陽，津田宏，片山佳則 ，鳥居悟，“IT被害に遭いやすい心理的・行動的特性に関する調査”，マルチメディア，分散，協調とモバイル（DISCOMO2014）シンポジウム，2014.

A3.2 逸脱に関わる社会・組織との関係

A3.1 節では主に利用者が逸脱行為を起こすための背景と傾向について述べた. 一方で利用者, 特に「例外措置を知っていても守らない」傾向にある利用者の逸脱行為は, 利用者個人に起因する面もありつつ, 利用者が構成員として所属する組織, さらには生活している社会全般の環境においても起因することが知られている. そこで本節では逸脱に関わる組織及び社会における関係について先行事例・先行研究を述べる.

A3.2.1 社会規範と市場規範

一般に「規範」というものには「社会規範」と「市場規範」の2種類があるといわれているが, このうち社会規範は組織内の信頼性および連携を維持することが重要であるといわれている.

これは Ariely の文献116,117において,「双方は織り交ぜて扱うべきではなく, 別々に取り扱うべきとしている. 社会規範から一旦, 市場規範へ変更してしまうと, 二度と社会規範に戻るどころか, 社会規範で維持していたルールや秩序からさらに悪くなる傾向にある」と記述されている. このことから規範を考えていくにあたり, 客観的でビジネスライクな行動をとるときは, 市場規範が優先しているように思えるが, 一方で組織への忠誠心を与える役割は社会規範にあるものと考える.

A3.2.2 個人重視と組織重視

さらに Ariely の文献118,119では,「組織のように集団で仕事をすることは, 協働で経済行動や意思決定をすすめることにつながる. プロジェクトを組んで大きな仕事を達成するためには不可欠である」としている.

しかし一方で,「個人の利益だけでなく, パートナーやグループ全体の利益につながるのであれば, いささかの不正行為をしてしまう傾向がある. 特にパートナーと親しい付き合いをしているかどうかで, その傾向は全く異なる実験結果もある」とも述べている. 通常の生活の中でも人はわずかな不正行為を気づかずにしてしまう傾向があり, それは全体の大勢を占めるため, 大きな不正を犯す少数派よりも累計すると損害が大きくなることもある.

Ariely によれば,「対策については集団内での監視体制　の強化が挙げられているが, 集団内での親密性がここにも影響が出てくる」としている. このことか

116) D. Ariely, A Taste of Irrationality, HarperCollins e-books, 2010.
117) ダン・アリエリー, 予想どおり不合理, 早川書房, 2010.
118) D. Ariely, The Honest Truth About Dishonesty, Harper; Reprint, 2013.
119) ダン・アリエリー, ずる, 早川書房, 2014.

ら，個人重視より組織重視に組織経営が委ねられ，それは組織の決定を掌握する経営者の意向に基づいて構成員が逸脱行動を起こしやすいものと考える．

A3.2.3 集団的防護動機理論

一方，情報セキュリティ対策行為に導くために，対策を実行する意思に影響を与える要因を，集団的防衛動機理論というものに基づいて検討した事例もある[120)]．

浜津氏らによるこの理論は，多くの人が集団的にセキュリティ対策を実施することで脅威を低減できるとした理論である．この理論では，8 つの規程要因（深刻さ認知，生起確率認知，コスト認知，実行能力認知，効果性認知，責任認知，実行者割合認知，規範認知）と，これに 3 つの潜在変数（ウイルス感染経験，IT 知識，IT スキル）を階層的に組み合わせた「対策実行意思モデル」を考案し，Web アンケート調査と，仮想的なウイルス感染を体験できる評価実験の両方により調査している．

評価実験の結果から，対策を実行する意思には，8 つの規程要因のうち，「深刻さ認知」，「効果性認知」，「生起確率認知」が影響していることがわかり，特に「深刻さ認知」は，「ウイルス感染の恐怖」「感染による被害の深刻さ」「不実施リスクを考慮した対策行動への実行」への理解が高いことが報告されている．

つまり深刻さを強調することにより，組織の構成員や組織自体がセキュリティ対策への実施を促される可能性があることを示している．

A3.2.4 組織文化・風土との関係

情報セキュリティ対策の実効性を高めるためには，画一化された対策だけではなく，情報セキュリティポリシーが守られやすいような運営を行うと同時に，様々な組織風土や組織文化を考慮し，それに合った対策を実施する必要がある．

どのような組織においても画一的なルールを策定し遵守するのではなく，以下 3 つの想定をたてて，集団主義における情報セキュリティポリシーからの逸脱を報告した事例がある[121)]．

（1）情報セキュリティポリシーへの逸脱行為の程度は，情報セキュリティに関する画一的な対策が実施されているかに影響を受ける．

（2）情報セキュリティポリシーへの逸脱行為の程度は，画一的な対策だけでなく，上司の態度や職場の雰囲気といった形式化できない組織的な要因

120) 浜津翔，栗野俊一 ，吉開範章，“集団的防護動機理論に基づく情報セキュリティ対策実行意思モデルの提案とその活用”，情報処理学会論文誌 Vol.56, No.12, pp,2200-2209, 2015.

121) 浜屋敏 ，山本哲寛，“日本企業における情報セキュリティ逸脱行為と組織文化・風土との関係”，富士通総研研究レポート，No.373, 2011.

に影響を受ける.

(3) 組織的な要因は「集団主義」に代表される組織文化・組織風土に影響を受ける.

浜屋氏の研究では, これらについてのアンケート調査によるデータ分析を行い, いずれの想定も成り立つことを証明している. すなわち, 情報セキュリティ対策は, 画一的な情報セキュリティポリシーの策定だけではなく, 組織文化・組織風土にあった対策を柔軟に行う必要があるとしている. この考えは, 例外規程を管理部門のみに策定・管理させるだけでなく, 利用部門でも可能にするための組織づくりの根幹になると考える.

A3.2.5 情報漏えいにつながる行動に関して

実は組織の構成員が「情報漏えいにつながる行動」を起こす原因として「不正容認風土」が最も大きな直接的な影響を与えることが明らかになっている[122].

竹村氏の研究では, その中で「低い情報リテラシー」「ルールの不認知」については, 「不正容認風土」「抵抗感のなさ」と比べるとそれほど大きな影響を与えないことも確認している. そこでこれらから情報漏えい防止には, 職場環境の改善とともに従業員の満足度向上策の実施や, コンプライアンス教育の実施が求められると述べている.

このことは情報セキュリティポリシーからの逸脱行為にも影響があると考える. 組織における情報セキュリティを維持する上でも, 例外措置を用いることで, 逸脱行為を抑制することが期待できる.

A3.3 逸脱行為への対策案

これまで, 情報セキュリティポリシーを知っていても守らない組織の構成員や組織自体の実態について述べてきた. 本節ではこれらを踏まえて, 個人もしくは組織が逸脱行為を阻止する対策について述べる.

A3.3.1 構成員のリスク行動に対する組織の取り組みモデル

組織的違反は, 構成員は個人よりも組織を優先するという善意のもとにおいて, 違反に対する罪悪感が薄れてしまうことが考えられる. すなわち, 組織の構成員が, 自分の意志に基づいて組織のためにあえて規則に反するようなリスク行動をとってしまう傾向がある.

122) 竹村敏彦, 三好祐輔 , 花村憲一, "情報漏えいにつながる行動に関する実証分析", 情報処理学会論文誌 Vol.56, No.12, pp,2191-2199, 2015.

これについて構成員のリスク行動に対する組織の取り組みモデルが提案されている[123]. 大和田氏らの研究では「教育を中心としたリスク認知能力の向上施策」,「情報セキュリティマップの作成」そして「リスク顕在化を想定した未然防止策」の 3 つモデルをあげている. そしてこれらの対策を連携することで, リスク行動に対する相乗的な効果があるとしている.

情報セキュリティマップの作成は, 情報セキュリティポリシーの可視化にも通じるものと考える. 例外措置が必要なのかどうかなど俯瞰的かつ客観的にとらえることが可能となる. 例外規程を予め策定する際などに利用できると考える.

A3.3.2 モチベーションマネジメントの適用

組織の構成員にとっては, 情報セキュリティ対策は「やらされ感」を感じやすいことから, 管理部門が情報セキュリティ対策への動機付け(モチベーション)を与えることで, 自発的な行動を活性化させようとする考え方がある. これは「モチベーションマネジメント」と呼ばれており, 従来, 製造業等に導入されてきているものである. この手法を情報セキュリティ分野に取り入れることが提案されている[124].

頼永氏による研究では,「情報セキュリティ対策においてシステム化で対応できるもの以外については, 情報セキュリティポリシーやルール及び操作手順の策定, 過去の失敗事例の精査, 罰則の付加が対策として挙げられる. しかしながらこれらを社員教育によって対策するには限界があり, そのため構成員に対してモチベーションが与えられるようなマネジメント手法の導入が考えられる. 一例として情報セキュリティマネジメントシステム(ISMS)での管理・運用をあげる. 通常であればルーチン業務と捉えられている項目を, 他の項目と合わせもつことで「クリエイティブ業務」へと進化させる. これによって, 構成員に情報セキュリティ対策へのモチベーションを持たせ, ルーチン業務に伴いがちな「やらされ感」から由来するミスを減らし, 引き起こされるインシデント発生の低減を図ることができる. また「自律」「熟達」「目的」それぞれのポイントごとにモチベーションを管理することにより,「やらされ感」の低減を図ることができる. さらにはセキュリティ対策の実態を知る構成員がモチベーションを持つことにより, 自発的にセキュリティ対策に取り組むことも期待できる. これは実態に合わなくなったルールがあれば, 自らの権限ですばやく修正できるといった効果につながるものと考える.」

この先行研究からは, 構成員にインセンティブを感じさせることが, 煩雑に感じる情報セキュリティ対策を前向きにとらえることができるとし, これにより構成員お

123) 大和田竜児 , 内田勝也, "従業員のリスク行動に対する企業の取り組みモデルの提案", 情報処理学会研究報告, Vol.2010-CSEC-48, No.52, pp.1-6, 2010.
124) 頼永忍, "モチベーションマネジメントの情報セキュリティマネジメント分野への適用の提案", 情報処理学会研究報告, Vol.2010-CSEC-51, No.7, pp.1-6, 2010.

よび組織による逸脱行為を防ぐ働きにつながるものと考えられる.

A3.3.3 構成員への安心感の提供

構成員の中には, 情報セキュリティへの知識がない上に, 情報セキュリティポリシーを逸脱する者も存在すると考える. こうした場合, 情報セキュリティ対策は構成員に対し, 安全目的だけでなく, 安心も提供する目的をもって情報インフラを提供する必要があるとされる[125]. 西岡氏らの研究では, アンケート調査結果の因子分析を通じて, 情報セキュリティに関する知識のない構成員が求める安心感の要因を抽出することを検討している.

安心感の因子としては,「認知的トラストにおけるコンピテンス(有能感)」「親切さ」「親しみ」「知名度」の 4 つにまとめられている. このうち認知トラストとはコンピテンス, 誠実, 善意を含み, 特にコンピテンスについて「ユーザが個人情報などを漏えいされない能力. このコンピテンスを事業者やシステムが持っていると構成員が判断できれば, "安心する"」重要な要因として解釈している.

この知見に基づくのであれば, 組織が情報セキュリティ対策に対応できる十分な情報インフラや情報システムを保有することで, 構成員は安全な日常業務ができると実感でき, あえてリスクをもって逸脱するような行為も防げるのではないかと考える.

A3.3.4 罰則の適用の利用

さらには,「例外措置を理解していても守らない」阻害要因への対策としては, 利用部門における例外措置から逸脱した行為に対し, 管理部門によって罰則規程を適用することが考えられる.

逸脱・違反を防止するには, 例外措置を逸脱し危険行動を行った場合に, 危険行動の経験を, 不快な出来事として記憶させることが必要である. しかし, そのために事件・事故を起こさせるということは避けなくてはならない. そこで不快な出来事として記憶させるためにも, 例外措置違反に対しては罰則を設け, 時として実際に罰を与えることも必要とする考えである.

なお統一管理基準では, 例外措置が罰則規程と合わせて記載されている. 違反は事象の一つであるが, その結果責任が明確になることが重要である. しかし, 実務上は悪意のない違反などについて責任があいまいになることがある. そこで例外規程を策定して事前に例外措置の承認を得ることで, 同じ逸脱行為で

125) 西岡大, 藤原康宏 , 村山優子, "情報セキュリティに関する知識のないユーザを対象とした安定感の要因抽出のための Web 調査の実施", マルチメディア, 分散, 協調とモバイル(DICOMO2011)シンポジウム, pp151-160, 2011.

あっても申請していた者としなかった者との間で逸脱に対する責任が切り分けられ，むしろマネジメントの観点からは，効果的な面もあると考える．また例外措置の記録は，リスク管理と見直しの観点からも，現状把握に役立てることができる．例外措置の有無により違反であるか否かが明確になるため，例外措置の手順に則っていれば故意の違反・逸脱ではないことが立証できる．

一方で，罰則を伴う規程は，例外規程策定時より事前に策定しなければならない．これは，法制度が参考となる，刑法の前提となる「罪刑法定主義」が貫かれ，規程がないままに処罰が科されてはならない大原則に基づくためである[126)]．罰則を伴う規程を策定するにおいても，必ず事前に根拠を示し，周知することが求められる．すなわち例外措置を逸脱することは社会規範から外れた危険行為であり，それに対する制裁・罰則を事前に作っておくことが不可欠である．さらに事前に罰則の規程範囲を明確にすることで，例えば例外申請をせずに利用部門が行った逸脱行為の責任を管理部門は負わない，など管理部門における例外措置への有効性が担保できる．

近藤氏らの研究によれば，具体的な罰則規程の策定については，各組織の就業規則や服務規律に準拠し，その内容を懲戒処分の規程などとして具体的に盛り込む必要があるとしている．したがって，情報系部門のみならず，法務部門や総務部門，さらには外部の弁護士などと連携した規程づくりが必要と考える．

罰則を実際に適用することの意味と効果については，情報セキュリティポリシー及び組織の綱紀の維持，セキュリティ確保への手段のほか，利用部門への教育・啓蒙への効果も期待できる．したがって，単に組織に対する影響から罰則を適用するだけでなく，利用部門・利用者自身の遵法・倫理意識への向上につながるものであることが望ましいと考える．

126) 近藤佐保子ほか，“ネットワーク利用に関する学内罰則規程のあり方”，電子情報通信学会技術研究報告，FACE99-38,pp.17-22, 1999.

小括

本章では，5.4.3 項の補足として，例外の普及を図るうえで構成員や組織における意識や行動に要因があることに注目し，特に利用者（構成員）における逸脱行為の傾向と，逸脱に関わる社会・組織との関係，さらにはこれらの逸脱行為への対策案について先行研究を調査した．本調査を通じて，情報セキュリティポリシーにおける例外について，その普及への課題のひとつと考えられる利用者側の阻害要因に対応するための手法がいくつか提案されてきていることがわかった．情報セキュリティポリシーや原則規程をあえて逸脱しようとする個人や組織の実態やその対策を知ることは，例外措置を実施していくうえで参考になると考える．

A4 「例外規程」と法律の「例外規定」との関連

本章では例外規程の説明を補足するために，法律で用いられる例外規定[127]について取り上げ，情報セキュリティポリシーの例外規程との関連性について述べる[128]．法律が定める例外規定の例として，特許法第 30 条を本章では取り上げる[129]．なお同条は筆者が以前所属していた知財部門で扱っていた，特許法の重要な条文の一つであると考える．

A4.1 特許法の例外規定

特許法第 30 条は，発明の新規性喪失の例外規定について定めている．日本の特許制度では，特許出願より前に公開された発明は原則として特許を受けることはできない．しかし特許庁は，刊行物への論文発表等によって自らの発明を公開した後に，その発明について特許出願をしても特許を受けることができないことは，発明者にとって酷な場合もあり，また産業の発達への寄与という点でも特許法の趣旨にもそぐわないと考える[130]．

この観点から特許法では，「特定の条件の下で発明を公開した後に特許出願した場合には，先の公開によってその発明の新規性が喪失しないものとして取り扱う」として，発明の新規性喪失の例外を設けている．これが特許法における「例外規定」である．

この発明の新規性喪失の例外の適用を受けるための条件は，

（1） 発明の公開日から 1 年以内に特許出願すること．

（2） 特許出願と同時に，発明の新規性喪失の例外規程の適用を受けようとする旨を記載した書面を提出する．

（3） 特許出願から 30 日以内に，発明の新規性喪失の例外規程の適用の要件を満たすことを証明する書面を提出する．

証明する書面：「公開の事実」及び「特許を受ける権利の承継等の事実」

127) 組織が個々に定める「例外規程」よりも，法律の「例外規定」の方が，強制力が強いと考える．

128) 企業などの組織は，内部規程を策定して事業を円滑に実施する自由がある（私的自治の原則）が，日本国で事業活動を行う場合は日本法が適用される．情報セキュリティも例外ではなく，情報セキュリティポリシー策定の自由があるからといって，その内容が日本法の法規に（少なくとも強行法規に当たる部分では）反することはできない．その意味では情報セキュリティポリシーに関する例外規程も，法律の定めの範囲内でなければならない．

129) なお知的財産制度は，「発明」や「創作」といった知的生産物に有体物の所有権に類似の排他性を政策的に付与するものであるから，原則と例外の関係が分かり易い．注 25)で述べた著作権のケースも併せて参照されたい．

130) 特許庁，“平成 30 年改正法対応・発明の新規性喪失の例外規程の適用を受けるための出願人の手引き”，平成 30 年 6 月．(オンライン)．
http://www.jpo.go.jp/shiryou/kijun/kijun2/files/hatumei_reigai/h30_tebiki.pdf. (アクセス日：2019 年 6 月 10 日)．

とある[131]. すなわち例外規程の条件が法律によって確定されていることを示している. 具体的には, 申請手続きに関する条件において, 公開した方法(学会発表, Web 公開, 集会, 展示や販売等)を明記した「証明する書面」の提出などが義務付けられている.

この申請過程や申請書類の内容についての例外は認められない. さらに, この例外規定にも残余リスクがあり, 猶予期間内でも同内容を独自に第三者が発明し出願した場合は例外規定の適用はなくなる.

特許法第 30 条

（発明の新規性の喪失の例外）
第三十条　特許を受ける権利を有する者の意に反して第二十九条第一項各号のいずれかに該当するに至つた発明は, その該当するに至つた日から一年以内にその者がした特許出願に係る発明についての同項及び同条第二項の規程の適用については, 同条第一項各号のいずれかに該当するに至らなかつたものとみなす.
2　特許を受ける権利を有する者の行為に起因して第二十九条第一項各号のいずれかに該当するに至つた発明（発明, 実用新案, 意匠又は商標に関する公報に掲載されたことにより同項各号のいずれかに該当するに至つたものを除く.）も, その該当するに至つた日から一年以内にその者がした特許出願に係る発明についての同項及び同条第二項の規程の適用については, 前項と同様とする.
3　前項の規程の適用を受けようとする者は, その旨を記載した書面を特許出願と同時に特許庁長官に提出し, かつ, 第二十九条第一項各号のいずれかに該当するに至つた発明が前項の規程の適用を受けることができる発明であることを証明する書面（次項において「証明書」という.）を特許出願の日から三十日以内に特許庁長官に提出しなければならない.
4　証明書を提出する者がその責めに帰することができない理由により前項に規定する期間内に証明書を提出することができないときは, 同項の規程にかかわらず, その理由がなくなつた日から十四日（在外者にあつては, 二月）以内でその期間の経過後六月以内にその証明書を特許庁長官に提出することができる.

131) 平成 30 年の特許法改正によって発明の新規性喪失の例外期間が 6 か月から 1 年に延長された. 原則として, 出願日が平成 30 年 6 月 9 日以降である特許出願が, 平成 30 年改正後の特許法第 30 条の適用対象となる.

A4.2 例外規程と例外規定との関連性

前節の特許法での例外規定をふまえ，本節では情報セキュリティポリシーでの例外規程との関連性について述べる．

特許法第 30 条では，特許法の適用範囲と例外適用範囲との境界は，立法によって明確に定められている．したがって特許法の例外適用は，どの組織でも共通であり，法改正されない限り変更されない．また法改正は頻繁にされることがないため，例外規定を改定することは難しい．

一方で情報セキュリティポリシーでは，組織における原則規程と例外規程との境界，すなわち原則規程とすべきか例外規程とすべきかは，情報セキュリティポリシーにおける例外措置の程度や頻度によって，組織ごとの判断となる．したがって例外規程は社会全体で法律のように一律ではなく，組織ごとに異なっている．さらには組織の情報セキュリティ対策の変化に応じて，例外規程も柔軟に見直されなくてはならない．これはサイバー攻撃の深化や新規デバイスの導入等のよるリスクの変化に対応するためである．したがって原則規程の改定を待たずに例外措置を柔軟に実施するのが望ましい．すなわち例外規程は時間的にも一律ではなく変化するものと考える．

これらを図 A4-2 で示す．図中左側の特許法では特許法適用範囲と例外適用範囲との境界が明確である一方，右側の情報セキュリティポリシーの原則規程と例外規程との境界は組織ごと・時間ごとに柔軟に変化するため，確定されているわけではない．この点が法律である特許法の例外規定と異なるところである．

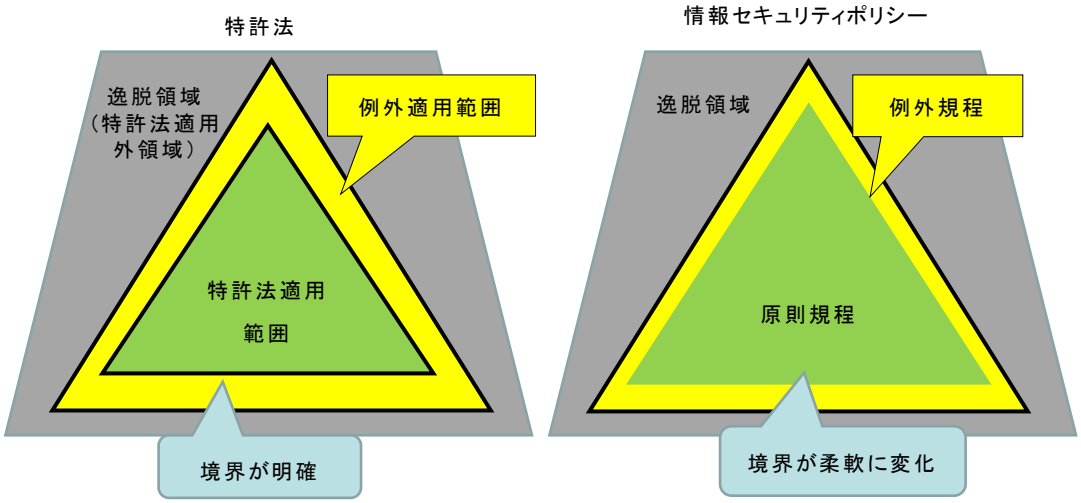

図 A4-2 特許法と情報セキュリティポリシーにおける例外領域の比較

小括

以上，本章では例外規程の説明を補足するために，法律で用いられる例外規定について取り上げ，情報セキュリティポリシーの例外規程との関連性について述べた．

特許法も情報セキュリティポリシーも双方とも原則からの逸脱に対し，一部を例外によって取り扱う点で類似している．このことから情報セキュリティポリシーにおける例外規程を策定していく上では，法律上の解釈や形式が参考になると考える．したがって例外規程を策定・運用する部門は情報系部門のみならず法務部門とも連携して策定していくことが望ましい．

A5 各管理策における原則規程と例外規程（解説）

外部インターネットの組織内利用

通常，従業員が組織内でインターネット利用する場合は，組織内イントラネットを経由してインターネットに接続するのが一般的である．この場合，組織でのインターネット利用ガイドライン等の原則規程が策定されており，従業員はそれに則って利用する．組織内での機密保持及び，社内環境の保護，情報資源の有効活用を目的に，インターネットの利用と管理を行うわけである．

しかしながら，情報収集やネットワーク上の実験，公衆向けサービスへの展開などの業務上の理由から，外部インターネットの利用を求める場合がある．その場合は原則規程に則り，当該情報インフラと切り離して，外部インターネットを利用しなければならない．

この場合業務上の情報であれば，外部インターネット上で取り扱うものであったとしても，組織内イントラネットで取り扱うものと同様に，組織のインターネット利用ガイドライン等の原則規程に則る必要がある．しかし厳密には，外部インターネットにおける利用ガイドラインが必ずしも策定しているわけではない．

したがって外部インターネットを利用する場合は，取り扱う情報を自組織内での取り扱いと同等にすることによって，原則規程と同程度の効用対リスク効果が期待できる例外措置によって利用することが可能となる．

策定の一例	
原則	許可なく外部インターネットの利用は禁止する．
例外	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．

参考文献

（「インターネット利用に関する標準 0.9 版」日本ネットワーク・セキュリティ協会（JNSA）,2001 年）

２章「外部ネットワーク接続セキュリティ方針」，４章「インターネット利用に関する標準」

可搬型メディア（USB メモリ，SD カード等）の業務利用

可搬型メディアは低価格化と大容量化に伴い，情報を取り扱う上での利便性の高いデバイスである．その一方，容易に組織外に情報を持ち出すことも可能となり，取り扱いを厳格にしなければ情報漏えいにつながることは，近年の事件・事故において明確である．さらには USB メモリによってマルウエア感染につながる事例も見られる．

そのため，管理のための技術進歩やクラウドによる情報運搬の代替手法により，業務での USB メモリの使用を禁止する組織も現れた．しかしながらこうした対策を持たない組織において，USB を例外措置なしで全面禁止するのは難しいと思われる．

Sky 株式会社のホームページからの抜粋によると，「ただ，いきなり USB メモリを一律に使用禁止にすると，業務に大きな影響が出ることも考慮する必要があります．また，私物の使用禁止など一部の禁止であっても，それまでは問題なく使えていた物が使えなくなると，正しいことだと理解していても心理的な反発が生まれ，運用がうまくいかないことも多いと言われます．適切な利用を定着するためには，利用者自身が，USB メモリ本体の物質的価値ではなく，その中に保存されている情報の価値や重要性を認識することが大切です．しかし，わかってはいるけれど「今回だけは―」「このくらいなら―」という気持ちもあり，利用者の情報セキュリティ意識はすぐに変えられるわけではありません．適切に扱うための利用ルールを定めて周知徹底すると同時に，必要に応じて管理ツールなどを活用して制御することも有効です．」とされている．

管理策を柔軟に策定して管理・運用の面で工夫する必要があると提案している（1.4.1 項参照）．

策定の一例	
原則	USB メモリの使用は原則禁止とする
例外	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のものであれば使用を承認する

参考文献

「利便性を犠牲にしない USB メモリの管理方法とは」SKYSEA Client View ホームページ，https://www.skyseaclientview.net/column/device/usb01/

サポート切れの OS やソフトウエアの利用

サポート切れの OS やソフトウエアを業務で利用することは，セキュリティ確保の面で，禁止とするのが原則である．
キャノン IT ソリューションでは，サポート切れの OS 利用は延命措置としての例外措置であるとし，下記のように述べている．

「やむを得ない事情で「延長サポート」終了時に移行が間に合わないこともあります．その場合はセキュリティ対策ソフトを利用したり，脆弱性攻撃を防ぐ「仮想パッチ技術」を活用したりすることで，被害を少しでも抑えるようにします．ただし，これらの対策は一時的な延命措置に過ぎません．速やかに新 OS へ移行することを強く推奨します．」

一方で，トレンドマイクロによれば，「サポート終了を迎えた OS の継続利用停止には長時間を要することが あるため，移行完了までの全対象期間を計画に含める必要があります．公式のサポート終了から 9 カ月近く経過しても，多くのサーバは引き続き稼働しており，移行が完了するまで，まだしばらく時間を要することが 最近の業界調査で明らかになっています．」と述べている．

このことから財政的・技術的な制約によって，サポート切れの OS やソフトウエアを引き続き利用する組織が多いことが問題となっている．

策定の一例	
原則	サポート切れの OS やソフトウエアの使用は全面禁止である．
例外	完全に外部ネットに接続しないレガシーシステムについては承認することもある．

参考文献
「SECURITY Q&A」，マルウエア情報局，キャノン IT ソリューションズホームページ，https://eset-info.canon-its.jp/malware_info/qa/detail/150416_1.html
「サポート期間が終了するソフトウエアに注意」，総務省ホームページ，総務省 安心してインターネットを使うための国民のための情報セキュリティサイト
「サポート終了後の OS やソフトを使い続けてはいけない 2 つの理由」2014/03/14,インターネットセキュリティナレッジ，トレンドマイクロホームページ，https://is702.jp/column/1537/

プログラム保守のための外部からの一時的アクセスの許可

組織のオンプレミス環境にあるサーバの保守は，保守契約に基づく請負業者のプログラム保守を目的とした，外部からの一時アクセス（リモートアクセス）の承認が必要となる．

リモートアクセスについては，IPA が手引きを発行しており，接続に必要な技術的基礎知識や環境整備について提言している．請負業者による一時的なアクセスの場合は，例外規程によって運用することが考えられる．

策定の一例	
原則	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．
例外	一時的措置が必要と経営層が判断した場合は事後申請で構わない．

参考文献

「リモートアクセス環境におけるセキュリティ」平成19年11月，独立行政法人情報処理推進機構

私物デバイス（スマートフォン・タブレット等）の使用

「可搬型メディア」に類似する管理策であるが，USB メモリと異なり，BYOD が普及しつつあるなかで，私物デバイスの業務利用が常態化に向けて整備されてきている．またセキュリティ対策も MDM の普及によって，デバイスの盗難紛失や OS・アプリケーションのバージョン管理など，利用リスクを低減することが可能となってきた．

またスマートフォンやタブレットは通信連絡手段を有していることから，組織によっては全従業員を対象に利用を促すこともある．この場合は原則規程にて管理・運用されるべきである．一方で，対象者を限定するのであれば，例外規程として利用することが望ましいと考える．

策定の一例	
原則	業務上必要がない場合は，原則使用を禁止
例外	私物デバイスの登録，指定アプリのインストール，業務使用手引きの励行および誓約書の提出により承認

参考文献
「BYOD (私物端末の業務利用) 最新事情とセキュリティ対策」, グローバルサインブログ, GMO インターネットグループホームページ,
https://jp.globalsign.com/blog/articles/byod_181128.html

自社が管理していない PC の組織内利用

「私物可搬型デバイス」と異なり, PC は組織が従業員に貸与していることが多いほか, 管理方法についてもウイルス管理ソフトウエアなど技術的に進化・普及していることから, 組織外で利用することが多くなっていると考える. 一方で, 自社が管理していない, 従業員の私物 PC や外部業者の PC をそれぞれ持ち込んで組織のイントラネットに接続する場合もある.

この場合, 組織がガイドラインに則って導入している管理用ソフトウエアが予め導入されているとは限らないため, 組織内利用については例外措置が必要と考える.

策定の一例	
原則	自社以外のPCの持ち込みは原則禁止
例外	業務上理由がある場合は, 申請の上, 持ち込みを承認する

自社が管理していないソフトウエアの利用

基本的には「自社が管理していない PC」と同等の管理策になるが, 加えて, 無償でダウンロード可能な, フリーソフトウエアのインストールへの対策が求められる.

インストールできる権限の付与を従業員に対して与えるかどうかにも関わるが, 権限を従業員に付与する場合は, 自社が保有するソフトウエアライセンスに限定して許可する必要がある.

策定の一例	
原則	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
例外	業務上理由がある場合は, 申請の上, 利用を承認する

ウイルス対策ソフトウエアを導入していない PC の利用

今や，業務においてウイルス対策ソフトの導入は必須条件である．したがって多くの組織は原則規程として当該ソフトのインストールは必須としており，導入していない PC をイントラネットに接続させることは認めないとしている．

その一方で制御系システムの PC ではレガシーシステムが導入されている事例も少なくない．これらにウイルス対策ソフトをインストールすることで，従来のパフォーマンスが得られない場合は，当該ソフト導入を見送ることも考えられる．したがってこのような場合は，当該 PC を全く外部ネットに接続させないなど，例外措置によって代替手段を用いることが望ましい．

策定の一例	
原則	利用禁止
例外	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承認することもある

外部業者への特権 ID を付与する

特権 ID とは，組織内のオンプレミスでも外部クラウドでも，システム管理上必要となる強力な権限を持つ，管理者向けのアカウント ID である．システムそのものの起動や停止のほか，アプリケーションのインストールや削除もでき，システムを管理・運用していくうえでは必ず必要となる．一方，大きな権限を持つがゆえにシステムの改変や機密情報の持ち出し，不正なアカウントの登録といった不正行為も容易である．

多くの組織では規模の大小に関係なく，特権 ID の管理の難しさから，適切な管理が課題とされている．一方でシステム管理にはメンテナンスに関わる作業量の多いく専門知識を要することから，外部委託によって作業者を確保するケースも多い．こうした外部業者が作業するにあたっては，組織の管理者と同等の特権 ID を予め付与する必要がある．したがって外部業者への特権 ID を付与する場合は，例外規程ではなく原則規程として厳格に管理することが望ましい．当然，作業内容や作業する日時も異なるため権限に応じた期限付きの特権 ID を個別に付与するべきである．

しかしながら，突発的な故障などで，早急のシステムメンテナンスが必要となった場合も想定できる．したがって，非常措置が必要であると経営者が判断した場合の例外申請は事後報告で構わないとする例外規程も必要と考える．

策定の一例	
原則	保守による外部業者への付与は事前承認を要する
例外	非常措置が必要であると経営層が判断した場合は事後申請で構わない

参考文献
「特権 ID の適切な管理方法について」, マルウエア情報局, キャノン IT ソリューションズホームページ,
https://eset-info.canon-its.jp/malware_info/special/detail/190205.html , 2019.2.5

個人で利用しているメールに社内メールを転送する

社内メールには, 組織の機密情報などが含まれることがあり, そのまま個人用メール（社外メール）に転送するのは, 情報の持ち出しにつながる場合がある. 個人用メールアカウントは, 組織の管理下にないため, セキュリティ保護やガバナンスの対象からも外れているため, 業務利用はコンプライアンス規程違反と解釈されることが多い. また個人用アカウントのメールが組織内サーバ上に格納されていないためリスクにさらされることにもなる. その一方で, 外部からのメール閲覧を希望したり, BYOD の普及で個人用メールでの利用を求めたりするケースもある. したがって組織は, 外部でのメール閲覧ができる情報インフラ整備が必要となる一方で, それまでの過渡期において, 一切禁止とするか, 転送もやむを得ないとの判断が必要となる.

策定の一例	
原則	原則禁止
例外	業務上理由がある場合は, 申請の上, 転送を承認する

参考文献
「個人用メールアカウントを業務利用することのリスク」2015-3-6, バラクーダホームページ, https://www.barracuda.co.jp/column/detail/402
「Gmail を仕事で使っても大丈夫？」2013-4-30, Kaspersky ホームページ, https://blog.kaspersky.co.jp/is-gmail-safe-for-work/739/

公衆無線 LAN（暗号無し）の業務利用

総務省は「無線 LAN ビジネスガイドライン（第 2 版）」を2016年に発行し，その中で，適切な情報セキュリティ対策として，暗号化及び認証の情報セキュリティ方式に対応したアクセスポイントの設置を指導している．このことから，暗号化や VPN 接続ができない公衆無線 LAN の業務利用は厳格に禁止するべきと判断する．

策定の一例	
原則	禁止
例外	例外無し

参考文献
「無線 LAN ビジネスガイドライン（第 2 版）」2016-9-23，総務省，http://www.soumu.go.jp/main_content/000444788.pdf

個人で利用しているクラウドサービス（Dropbox 等）を利用する

「個人で利用しているメールに社内メールを転送する」と同等の管理策と考える．スターティアホールディングス株式会社による「業務におけるオンラインストレージの利用実態調査第 4 弾（2018 年版）」の結果によると，業務上で利用される個人契約のオンラインス トレージの利用者が存在することが見て取れる．

クラウドストレージは，取引先と大容量の業務データを円滑にやり取りしたいときなどに役立つ．このようなクラウドサービスはクラウドベンダー側でセキュリティ対策が取られてはいるものの，利用者が取り扱い操作を誤る事により、外部への情報漏えいにつながりやすい恐れがある．組織において法人契約のクラウドサービスを利用するのか否か，の判断により，個人契約のクラウドサービスの業務利用が可能かを考える必要がある．そして利用する場合は例外措置が望ましい．

策定の一例	
原則	原則禁止とし，企業が契約するクラウドを利用する
例外	取引先からの指示などやむを得ない場合は，申請の上，一時的に利用を承認することもある

参考文献
「業務におけるオンラインストレージの利用実態調査第 4 弾（2018 年版）」2018-11-28, スターティアホールディングス株式会社, https://www.startiaholdings.com/dcms_media/other/2018_onlinestorage_release.pdf
「私用のクラウドサービスを勝手に業務で利用してはいけません」2017-11-16, トレンドマイクロホームページ, https://www.is702.jp/manga/2236/

日本国内法非準拠のクラウドを利用する

以前は, 大手の外部クラウド（AWS, MS Azure, Google Cloud）のデータセンターは国外に設置されており, 準拠法も日本国内法ではないこともあり, これらに不安を持つ組織においては利用を見送るケースがあった. 近年はデータセンターを日本国内に設置し, 日本国内法準拠に応じる外部クラウドが増えたことで, 利用へのハードルが低くなったと考える.

一方で, GDPR や個人情報保護法への対応に伴い, 外部クラウドを利用した組織への個人情報・機密情報の取り扱い厳格化が進む中, あらためてデータセンターの所在や国内法準拠の有無の確認など, 利用時の原則規程の策定が求められる. そして国内法非準拠クラウドを利用する場合は, クラウドベンダーもしくは当該クラウドの仲介業者と個別に国内法準拠の利用契約を締結するとした例外措置により, 承認することが望ましい.

策定の一例	
原則	クラウドの利用契約は国内法準拠とする
例外	クラウドベンダーもしくは当該クラウドの仲介業者と個別に国内法準拠の利用契約を締結すれば承認する

参考文献
「GDPR, 個人情報保護法…クラウドサービスを取り巻く国内外の法規制とリスク対応」2018-7-31, EnterpriseZone ホームページ, https://enterprisezine.jp/article/detail/10993

第三者認証のない外部クラウドを利用する

クラウドサービス事業者のセキュリティ対策の現状を評価する手段として，その利用組織が直接監査を実施することは，費用・時間の面において無理がある．そのためクラウドサービス事業者のセキュリティ対策の確認手段として，第三者認証が一般的には活用されており，多くのクラウドサービス事業者が第三者認証を取得している．利用者は外部クラウドを選定する際は，クラウドサービス事業者が第三者認証を取得しているか否かを確認し，第三者認証を受けていない外部クラウドの利用は原則禁止することが望ましいと考える．

しかしながら，利用したい外部クラウドサービス事業者が第三者認証を取得していないケースも考えられる．その場合は例外措置を用いる必要があると考える．（1.4.2 項参照）

策定の一例	
原則	原則禁止
例外	取引先からの指示などやむを得ない場合は，申請の上，一時的に利用を承認することもある

参考文献
「クラウドサービス利用における第三者認証制度の考察」，佐藤栄城，原田要之助，情報処理学会研究報告，Vol.2013-EIP-59，No.1(2013)
「クラウド・コンピューティングにおける非対称情報の解消について」，栗田 克己，樋口 清秀，情報通信学会誌，2012 年 30 巻 1 号 p. 1_15-1_26
「クラウド環境における第 3 者認証制度」2019-2-8，ビジネス on IT，https://www.business-on-it.com/1002-cloud-security-3rd-pty-certification/

A6 用語集

【あ】

逸脱

本研究では，原則規程（通常措置）を破る行為や措置を指す．

- 逸脱の範囲は，原則規程の限度域との境界から法令違反領域との境界までの間の領域とする．
- 是正あるいは非難の対象になり得る．

【か】

原則規程

組織が定めた情報セキュリティポリシーに基づき，情報セキュリティに向けた体制，運用規程・対策基準などを具体的に記載された内部規程．

日常業務において定常的に実施されるべきリスク低減措置としてまとめられ，関係者が合意して策定する．（参考：通常措置）

原則と例外の相互補完

予め原則として措置できない事象への対策を，例外として措置できることにより，例外が原則を補うことによって，組織の情報セキュリティ対策を維持していること．

原則と例外の代替関係

原則では措置できない事象への対策を，例外としてルールや規程そのものを抜本的に見直すことによって，組織の情報セキュリティ対策を維持すること．

【さ】

残余リスク

組織において内部統制を整備・運用しても依然として残されるリスク．

- 原則規程においても，元々残余リスクが含まれていることから，原則規程を策定する段階においてリスク分析を行い，対応後の残余リスクの内容や対処を十分理解しておく.
- 残余リスクという考え方自体が，将来の不測事態をすべて予見したり，最適な行動を計算に入れたりすることは出来ないという，人間の知的能力の限界を考慮した「限定合理性」を前提にしている

情報インフラ

本論文で情報インフラは組織が業務上保有している情報システム機器やデバイスを指す.

- 参考：品質マネジメントシステム（Quality Management System ; QMS）の国際規格である，ISO9001:2015 の「7.1.3 インフラストラクチャ」において「組織は、プロセスの運用に必要なインフラストラクチャ、並びに製品及びサービスの適合を達成するための必要なインフラストラクチャを明確にし、提供し、維持しなければならない。」の記載がある.
- さらに同項の注記には「インフラストラクチャとしては次を含めることができる a)建物及び関連するユーティリティ b)設備。これにはハードウエア及びソフトウエアを含む c)輸送のために資源 d)情報通信技術」の記述がある.
- b)および d)の記載は，本論文の情報インフラの定義に参考になるものと考える.

情報セキュリティポリシー

企業などの組織が取り扱う情報やコンピュータシステムを安全に保つための基本方針や対策基準などを定めたもの．広義には、具体的な規約や実施手順、管理規定などを含む場合がある.

- 組織のセキュリティ対策を効率よく、効果的に行うための指針であり、恒久的にセキュリティを維持するための仕組み.
- 情報セキュリティポリシーには，情報セキュリティに関する組織全体の方針が定められている.
- 組織全体のルールとして「どのような情報を，どのような脅威から，どのように守るのか」といった基本方針とともに，情報セキュリティを守るための体制，運用規程・対策基準などが具体的に記載されている.

組織性逸脱

集団的効果を目的として，集団内メンバーにより感知され，違反の実行者を含む複数の直接的・間接的関与者によって生じる一般社会に照らして逸脱した行為（参考：逸脱）．

- 当該集団の外の人々に何らかの悪影響をもたらす集団行為．
- 従来，組織体犯罪・組織体違反行為・ホワイトカラー犯罪などと呼ばれてきた．

【た】

通常措置

原則規程（即ち情報セキュリティポリシー）に則って，管理策それぞれに対し，日常業務において定常的に実施されている措置．

- 通常措置は原則規程によって明文化・可視化された措置．

統一管理基準

各府省庁の情報セキュリティ対策内容の整合化・共通化を促進するために，各府省庁がとるべき情報セキュリティ対策を NISC によって定めたもの．

【な】

【は】

法定境界線

逸脱領域の限度域と法令違反領域の間にある境界

- 例外措置を伴わない逸脱行為のうち，法定境界線を超えるものは法令違反の対象となる．
- 逸脱領域の内側にある原則規程における法律上の限界を表す．
- 逸脱領域に存在する例外措置も法定境界線が限界となることを示す．

【ま】

【や】

【ら】

例外

逸脱のうち，通常措置からの逸脱程度が小さく，組織からの承認・許可が許容される可能性のある行為や措置．

- （参考：広辞苑）通例の原則にあてはまっていないこと。一般の原則の適用を受けないこと．
- 情報セキュリティを守るための管理手順が定められていることを前提に，原則とは違った手続きが必要な場合の要件を定めた規則，あるいは定められた手続きそのものを指す．
- 原則を補完するために「例外」として認知されたり（相互補完），場合によって原則に取って代わったり（代替関係）するなどの有効性が認められるもの，いわば「原則の予備軍」である．

例外規程

例外措置の根拠規程．同一もしくは類似する例外措置の適用が多い状況において，代替手段の導入も含め，例外措置の根拠を規程として策定したもの

- 例外措置を管理・運用していくための，措置の申請，承認・許可，実施，報告，さらには見直し等といった手続きやその内容について明確に策定した根拠規程．

例外措置

原則規程に対する逸脱行為において，その逸脱の内容・範囲が，原則規程もしくは通常措置と同程度の効用対リスク効果が期待できると組織が判断した措置．

- 実務的にいえば，例外措置は，原則規程をすぐに改定できず，通常措置として対応しきれない状態もしくは通常措置そのものがない状態において，利用部門の判断や管理部門での承認に基づいて一時的に実施される措置である．
- （参考：H24 政府統一管理基準から加筆）利用者がその実施に責任を

持つ原則規程を遵守することが困難な状況で，業務の適正な遂行を継続するため，遵守事項とは異なる代替の方法を採用し，又は遵守事項を実施しないことについて合理的理由がある場合に，そのことについて申請し許可を得た上で適用する行為

レベル別例外措置

申請者あるいは申請部門のスキルや経験，また例外措置それ自体が持つリスクにそれぞれ条件化し，それら条件に見合ったレベルに適用させる例外措置．

【わ】

参考文献（文中より）

2) 厚生労働省“「働き方改革」の実現に向けて”, 2018, (オンライン). (オンライン). https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000148322.html. (アクセス日: 2019 年 6 月 10 日).

3) 内閣府,“Society5.0”,内閣府, (オンライン).https://www8.cao.go.jp/cstp/society5_0/index.html. (アクセス日: 2019 年 6 月 10 日).

5) 沼上幹, “組織戦略の考え方ー 企業経営の健全性のためにー”,ちくま新書, 2003 年.

8) 情報処理推進機構, “内部不正による情報セキュリティインシデント実態調査”, (オンライン). https://www.ipa.go.jp/files/000051140.pdf. (アクセス日: 2019 年 6 月 10 日).

9) 日経 NETWORK, “企業セキュリティ調査 Part2USB メモリ編”, 日経 NETWORK, 第 7 月号, pp. pp.42-44, 2012

10) 栗田 克己, 樋口 清秀, “クラウド・コンピューティングにおける非対称情報の解消について”, 情報通信学会誌, 2012 年 30 巻 1 号 p. 1_15-1_26

11) 佐藤栄城, 原田要之助, “クラウドサービス利用における第三者認証制度の考察”, 情報処理学会研究報告, Vol.2013-EIP-59, No.1(2013)

12) ビジネス on IT, “クラウド環境における第 3 者認証制度”, 2019-2-8, https://www.business-on-it.com/1002-cloud-security-3rd-pty-certification/

13) 総務省, “情報セキュリティポリシーの概要と目的”, (オンライン). http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/04-2.html. (アクセス日: 2019 年 6 月 10 日).

16) The Cybersecurity Strategic Headquarters, “Common Standards for Information Security Measures for Government Agencies (FY2016)”, 2016.

18) 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”, 内閣サイバーセキュリティセンター, (オンライン). http://www.nisc.go.jp/active/sisaku/2002_1128/ISP_Guideline_20021128.html. (アクセス日: 2019 年 6 月 10 日).

19) 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). http://www.soumu.go.jp/main_content/000348656.pdf.

20) 総務省, “情報セキュリティポリシーの内容”, 総務省ホームページ, (オンライン). http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/04-3.html. (アクセス日: 2019 年 6 月 10 日).

21) 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).http://www.ipa.go.jp/security/manager/protect/pdca/policy.html. (アクセス日: 2019 年 6 月 10 日).

22) 金融情報システムセンター, “金融情報システムセンターガイドライン検索システム”, (オンライン).

24) 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.https://www.fisc.or.jp/guideline/. (アクセス日: 2019 年 6 月 10 日).

25) 平木健士,原田要之助, “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 年 6 月 7 日

28) 内閣官房情報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」”, (オンライン). http://www.nisc.go.jp/active/general/pdf/K304-111C.pdf. (アクセス日: 2019 年 6 月 10 日).

29) 内閣サイバーセキュリティセンター, “スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書”, 2015 月 5 月 21 日. (オンライン).http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf. (アクセス日: 2019 年 6 月 10 日).
30) 遠藤宗正, “シャドーIT とはこれでおさらば!? 企業をむしばむ無断使用ツールを「断捨離」する 3 つのステップ, “シャドーIT”との向き合い方”, IT Media ニュース, 2015. (オンライン). http://www.itmedia.co.jp/news/articles/1501/27/news045.html. [アクセス日: 2018 年 12 月 21].
31) 佐藤慶浩, “政府機関の情報セキュリティ対策のための統一基準”, (オンライン).http://yosihiro.com/speech/presenter/2006-08-02/index.html (アクセス日: 2019 年 6 月 10 日).
33) H.A.Simon”,意思決定と合理性”,ちくま学芸文庫,2016
35) 情報セキュリティ政策会議, “政府機関の情報セキュリティ対策のための統一基準（平成 26 年度版）”, 平成 26 年 5 月 19 日. (オンライン). http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf. (アクセス日: 2019 年 6 月 10 日).
36) 日立グループ, “情報セキュリティ報告書 2018”, 2018 年 9 月. (オンライン). http://www.hitachi.co.jp/sustainability/download/pdf/securityreport.pdf. (アクセス日: 2019 年 6 月 10 日)
37) 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.
38) 経済産業省, “平成 28 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). https://www.meti.go.jp/policy/netsecurity/is-kansa/. (アクセス日: 2019 年 6 月 10 日).
41) 佐藤慶浩, “企業における情報セキュリティ対策の実務”, (オンライン). http://yosihiro.com/speech/present-er/2014-11-29b/data/resources/2014-11-29b-enPit.pdf. (アクセス日: 2019 年 6 月 10 日).
42) 内閣官房情報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”, 内閣サイバーセキュリティセンター, 2011 年 4 月. (オンライン). https://www.nisc.go.jp/active/general/kijun_man_index.htm. (アクセス日: 2019 年 6 月 10 日).
44) サイバーセキュリティ戦略本部, “政府機関の情報セキュリティ対策のための統一基準（平成 28 年度版）”, 平成 28 年 8 月 31 日. (オンライン).https://www.nisc.go.jp/active/general/pdf/kijyun28.pdf. (アクセス日: 2019 年 6 月 10 日).
45) サイバーセキュリティ戦略本部, “政府機関の情報セキュリティ対策のための統一基準（平成 30 年度版）”, 平成 30 年 7 月 25 日. (オンライン). https://www.nisc.go.jp/active/general/pdf/kijyun30.pdf. (アクセス日: 2019 年 6 月 10 日).
46) ISO/IEC JTC, “ISO/IEC27001:2013”
47) ISO/IEC JTC, “ISO/IEC27002:2013”
48) 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.
49) 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.
50) 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.
51) 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.

52) NIST,“SP800・FIPS”, (オンライン). http://csrc.nist.gov/publications/PubsSPs.html. (アクセス日: 2019 年 6 月 10 日).
53) NIST, “Information Security Handbook: A Guide for Managers”, NIST Special Publication 800-100, 2006.
54) NIST, “Information Security Guide For Government Executives”, NISTIR 7359, 2007.
55) NIST, “Guide for Security-Focused Configuration Management of Information Systems”, NIST Special Publication 800-128, 2011.
56) NIST, “Guide to General Server Security”, NIST Special Publication 800-123, 2008.
58) 山内達夫,“コーポレートガバナンス・コードの基本的な考え方(案)の解説”, テクニカルセンター 会計情報, vol.463, 2015.
59) European Medicines Agency, “Requesting and recording of exceptions and non-compliance events, Standard”, European Medicines Agency Standard operation procedure, 2018.
60) Children’s Healthcare of Atlanta,“Information Management, Administrative and Operational Policies and Procedures”, (オンライン). https://www.choa.org/~/media/files/Childrens/research/it-technology-acceptable-use-form.pdf?la=en/ (アクセス日: 2019 年 6 月 10 日).
61) Inforsec Institute,“Exception Management - InfoSec Resources” - (オンライン). https://resources.infosecinstitute.com/exception-management/#gref. (アクセス日: 2019 年 6 月 10 日).
62) Birmingham and Solihull Mental Health NHS Foundation Trust,“information systems security policy (issp)”. (オンライン). https://www.bsmhft.nhs.uk/EasysiteWeb/getresource.axd?AssetID=4448&type=full&servicetype=Attachment. (アクセス日: 2019 年 6 月 10 日).
63) Georgia Institute of Technology,“Policy Exceptions”, (オンライン). https://policylibrary.gatech.edu/information-technology/policy-exceptions. (アクセス日: 2019 年 6 月 10 日).
64) University of Louisville,“Policy Exception Process”, (オンライン).https://louisville.edu/security/policies/policy-exception-process. (アクセス日: 2019 年 6 月 10 日).
65) The University of Nottingham,“Information Security Policy 2015/16”, (オンライン).https://www.nottingham.ac.uk/legalservices/documents/information-security-policy.pdf. (アクセス日: 2019 年 6 月 10 日).
66) Youngstown state university,“Overview of IT Security Waivers and Exceptions”, (オンライン).https://cms.ysu.edu/administrative-offices/it-security-services/overview-it-security-waivers-and-exceptions. (アクセス日: 2019 年 6 月 10 日).
67) VAMK(University of applied sciences),“Information Security Policy”, (オンライン). http://www.puv.fi/en/study/it-basics/rules/policy/. (アクセス日: 2019 年 6 月 10 日).
69) 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”, (オンライン). http://lab.iisec.ac.jp/~harada_lab/survey/2015.html.
70) 村﨑康博ほか,“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, 2016
72) 宇崎俊介,“第 1 回:情報セキュリティポリシーの現状,【特集】スローポリシーのススメ, atmarkIT”, 2002/7/26. (オンライン). http://www.atmarkit.co.jp/fsecurity/special/27spolicy/spolicy01.html. (アクセス日: 2019 年 6 月 10 日).
73) 情報セキュリティ大学院大学原田研究室,“2018 年度情報セキュリティ調査”, (オンライン). http://lab.iisec.ac.jp/~harada_lab/survey.html. (アクセス日: 2019 年 6 月 10 日).

74) 李哲ほか, “2018 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”, 2019 年 暗号と情報セキュリティシンポジウム講演予稿集, 2019
77) 原田要之助, “ITシステムのリスクマネジメントの全体像”, 著: 佐々木良一編「ITリスク学」, pp. pp122-138.
78) 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.
80) 情報セキュリティ対策推進会議, “情報セキュリティポリシーに関するガイドライン”, 首相官邸, 2000
81) 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, 2015
83) 文部科学省初等中等教育局児童生徒課, “学校における携帯電話の取扱い等について（通知）”, 文部科学省, 平成 21 年 1 月 30 日. (オンライン). http://www.mext.go.jp/b_menu/hakusho/nc/1234695.htm. (アクセス日: 2019 年 6 月 10 日).
86) 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). http://itpro.nikkeibp.co.jp/article/COLUMN/20120920/423888/.
87) 総務省, “一般利用者が安心して無線 LAN を利用するために”, 2012 年 11 月 2 日. (オンライン). http://www.soumu.go.jp/main_content/000183224.pdf. (アクセス日: 2019 年 6 月 10 日).
88) 総務省, “企業等が安心して 無線LANを導入・運用するために”, 2013 年 1 月 30 日. (オンライン). http://www.soumu.go.jp/main_content/000199320.pdf.
90) 総務省, 平成27年度版情報通信白書, 2016.
91) 岡部康成, 事故や災害を防止するために,リスク・マネジメントの心理学, 新曜社,pp.245-270, 2003.
92) 赤崎貫志, 新林栄一, “ヒューマンファクターの現状とヒューマンエラーのゼロ化を目指してⅢ 化学プラントのヒューマンファクターと安全教育”, 電気学会論文誌 D,vol.117, No.6, pp671-672, 1997.
93) 芳賀繁, 違反と不安全行動, 失敗のメカニズム, 角川ソフィア文庫, pp.147-166, 2003 年 7 月 25 日.
94) 本間道子編著, “組織性逸脱行為過程”, 多賀出版(2007)
96) NHK スペシャル, “平成史スクープドキュメント第2回 バブル終わらない清算 ～山一証券破綻の深層～”, 日本放送協会, (オンライン). http://www6.nhk.or.jp/special/detail/index.html?aid=20181202. (アクセス日: 2019 年 6 月 10 日).
99) James R. Fitzer, “Agile Information Security”, BookBaby, 2015
100) 情報処理推進機構, “アジャイル開発の進め方”, 2018 年 4 月. (オンライン). https://www.ipa.go.jp/files/000065606.pdf. (アクセス日: 2019 年 6 月 10 日).
101) 村﨑ほか, “テレビを一緒に視聴するロボットの開発ガイドライン策定に向けての一考察”, 情報処理学会研究報告,vol.2017-EIP-78, No.14, 2017.
102) Tech Target Japan の 2018/11/7 の記事:(オンライン). https://techtarget.itmedia.co.jp/tt/news/1811/07/news04.html (アクセス日: 2019 年 6 月 10 日).
104) ITU-R, “ITU-R 勧告”,Methodology for the subjective assessment of the quality of television pictures”, BT500-11”, 2006
105) 中小企業庁, “中小企業・小規模企業者の定義”, 中小企業庁, (オンライン). http://www.chusho.meti.go.jp/soshiki/teigi.html. (アクセス日: 2019 年 6 月 10 日).
106) 情報処理推進機構, “中小企業の情報セキュリティ対策ガイドライン”, 情報処理推進機構セキュリティセンター, (オンライン). http://www.ipa.go.jp/files/000014017.pdf. (アクセス日: 2019 年 6 月 10 日).
107) 情報処理推進機構, “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). http:/ww.ipa.go.jp/files/000014023.pdf. (アクセス日: 2019 年 6 月 10 日).
108) 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). https:/ww.ipa.go.jp/security/fy28/reports/sme/index.html. (アクセス日: 2019 年 6 月 10 日).
109) J. Blythe, L. Coverntry , L. Little, “Unpacking security policy compliance”, The motivators and barriers of employees' security behaviors, 2015 Symposium on Usable Privacy and Security, pp.103-122, 2015.
110) 森泉慎吾 , 臼井伸之介, “リスク傾向が違反敢行に及ぼす影響”, 日本心理学会第 75 回大会, 2011.
111) 森泉慎吾, “リスク受容に伴うベネフィットがリスク受容判断の合理性に及ぼす影響”, 産業・組織心理学会第 32 回大会発表論文集, 193-196, 2016.
112) 森泉慎吾 , 臼井伸之介, “時間的コスト認知とリスク受容に関する心理的要因の関係”, 産業・組織心理学会第 33 回大会発表論文集, 2017.
113) 岡野裕樹 , 奥山浩伸, “セキュリティルール違反行動の抑止に関する一考察”, 情報処理学会論文誌 Vol.58, No.1, pp,258-268, 2017.
114) NPO 日本ネットワークセキュリティ協会, “2017 年 情報セキュリティインシデントに関する調査報告書【速報版】”, (オンライン). https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf. (アクセス日: 2019 年 6 月 10 日).
115) 寺田剛陽, 津田宏, 片山佳則 , 鳥居悟, “IT被害に遭いやすい心理的・行動的特性に関する調査”, マルチメディア, 分散, 協調とモバイル (DISCOMO2014)シンポジウム, 2014.
116) D. Ariely, A Taste of Irrationality, HarperCollins e-books, 2010.
117) ダン・アリエリー, 予想どおり不合理, 早川書房, 2010.
118) D. Ariely, The Honest Truth About Dishonesty, Harper; Reprint, 2013.
119) ダン・アリエリー, ずる, 早川書房, 2014.
120) 浜津翔, 栗野俊一 , 吉開範章, “集団的防護動機理論に基づく情報セキュリティ対策実行意思モデルの提案とその活用”, 情報処理学会論文誌 Vol.56, No.12, pp,2200-2209, 2015.
121) 浜屋敏 , 山本哲寛, “日本企業における情報セキュリティ逸脱行為と組織文化・風土との関係”, 富士通総研研究レポート, No.373, 2011.
122) 竹村敏彦, 三好祐輔 , 花村憲一, “情報漏えいにつながる行動に関する実証分析”, 情報処理学会論文誌 Vol.56, No.12, pp,2191-2199, 2015.
123) 大和田竜児 , 内田勝也, “従業員のリスク行動に対する企業の取り組みモデルの提案”, 情報処理学会研究報告, Vol.2010-CSEC-48, No.52, pp.1-6, 2010.
124) 頼永忍, “モチベーションマネジメントの情報セキュリティマネジメント分野への適用の提案”, 情報処理学会研究報告, Vol.2010-CSEC-51, No.7, pp.1-6, 2010.
125) 西岡大, 藤原康宏 , 村山優子, “情報セキュリティに関する知識のないユーザを対象とした安定感の要因抽出のための Web 調査の実施”, マルチメディア, 分散, 協調とモバイル(DICOMO2011)シンポジウム, pp151-160, 2011.
126) 近藤佐保子ほか, “ネットワーク利用に関する学内罰則規程のあり方”, 電子情報通信学会技術研究報告, FACE99-38,pp.17-22, 1999.
130) 特許庁, “平成 30 年改正法対応・発明の新規性喪失の例外規程の適用を受けるための出願人の手引き”, 平成 30 年 6 月. (オンライン). http://www.jpo.go.jp/shiryou/kijun/kijun2/files/hatumei_reigai/h30_tebiki.pdf. (アクセス日: 2019 年 6 月 10 日).

謝辞

本研究を進めるにあたり，研究の方向性や内容，論文執筆の基本に至るまで，終始温かいご指導と励ましを賜りました，情報セキュリティ大学院大学の原田要之助名誉教授に心から感謝の意を表します．原田先生は，筆者が 2014 年 10 月の博士前期課程入学から 2016 年 9 月の修了まで，および 2018 年 4 月の博士後期課程入学から定年退官された 2019 年 3 月までの指導教官として，情報セキュリティマネジメントについて全くの初学者だった筆者を，情報セキュリティ監査人補の資格取得や博士号取得までに導いてくださいました．また「例外」を研究テーマに決めた際も，先生には一番にご理解いただき，また後押しいただきました．旧原田研究室で数多く学外発表ができたことも，ひとえに原田先生のご指導によるものです．

林紘一郎元学長には，2018 年度の本論文の主査として，また 2019 年度上期の副査としてご指導とご鞭撻を賜りました．林先生からはセキュリティマネジメントの観点から執筆してきた本論文を，法学・経済学・経営学の観点から広くご助言を頂き，社会科学分野での博士論文の執筆方法や表現の工夫等をご教授頂きました．

後藤厚宏学長には，2018 年度の本論文の副査として，また 2019 年度からは本論文の主査ならびに指導教官としてご指導とご鞭撻を賜りました．後藤先生からは自然科学の観点から多々ご助言頂き，また他分野の専門家に理解してもらうことの重要性を教えていただきました．第 18 回情報科学技術フォーラム（FIT2019）への投稿（初出一覧(12)）を承認頂き，その結果学会発表で初めて FIT 奨励賞を受賞できたことは，後藤先生のおかげであります．

また副査として審査いただきました湯淺懇道教授・学長補佐には，日頃より情報セキュリティに関する情報を交換させて頂き，本研究に限らず，幅広く有益なご助言を賜りました．さらに松井俊浩教授並びに稲葉緑准教授には博士演習セミナーを通じて本研究をさらに深めるための手法をご教授いただき，電子情報通信学会総合大会（初出一覧(11)），情報処理学会セキュリティ心理学とトラスト研究会（初出一覧(9)）で報告する機会を得ることができました．厚く御礼申し上げます．

また本研究において，直接の動機となりました本学講義「企業における情報セキュリティ対策の実務(2014 年 11 月 29 日開催)」で登壇されました佐藤慶浩氏に厚く御礼申し上げます．この講義で政府の統一管理基準並びに例外措置について受講していなければ，当時筆者が業務で取り扱っていた「例外」を本研究

のテーマにする事は到底思いつかなかったことと考えます.

さらに原田先生から学術交流の場として推薦して頂き, 発表・参加をして参りました, 情報処理学会電子化知的財産・社会基盤研究会並びにセキュリティ心理学とトラスト研究会, 電子情報通信学会技術と社会倫理研究会, システム監査学会に御礼申し上げます. 学会活動を通じて日本大学危機管理学部小向太郎先生, 同じく日本大学商学部堀江正之先生, 名古屋市立大学金子格先生, 佛教大学社会学部吉見憲二先生, 徳島文理大学総合政策学部橋本誠志先生, 新潟大学法学部須川賢洋先生他多数の先生方と本研究について議論をさせて頂いたことは望外の喜びでした. また東京電機大学の猪俣敦夫先生には, 博士後期課程入学のきっかけの一つを与えて頂きました. 御礼申し上げます. 先生より情報処理学会への論文投稿(初出一覧(2))を勧めて頂かなければ, 当該論文の採録もなく, 原田先生より博士後期課程入学を勧めていただくことも, あるいはなかったかと思います. 加えて情報セキュリティ大学院大学の教授各位, 在学生・客員研究員各位とは輪講発表やゼミでの議論を通じて, 研究のヒントとなる助言・提案をいただくことができました. 特に旧原田研究室で客員研究員として在籍されていた久保知裕氏, 根岸秀忠氏には, 博士前期課程から英訳支援を通じ, 研究テーマについて助言をいただきました. 御礼申し上げます. さらには本学事務局の皆様にも, 書類手続きや機材設営など様々な件でお世話になりました. 感謝致します.

あわせて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, 外1校(以上, 2015 年度協力)及び, 神奈川県立みどり養護学校新栄分教室, 神奈川県立麻生養護学校元石川分教室, 外 1 校(以上, 2018 年度協力)(五十音順)の皆様に感謝します.

また情報セキュリティ分野での人材育成・確保を主な目的に, 2014 年に本学博士前期課程への国内派遣の機会を与えてくださった日本放送協会情報システム局在籍当時の上司, 小林和正氏, 長村中氏, 山本秀人氏, 浅川玲氏, 土生尚氏, 増子明洋氏, 中島陽一郎氏, 新見琢司氏, 熱海徹氏, 有馬伸一郎氏, 宮崎洋光氏, 六山浩一氏, 赤木慎司氏, 池田有里氏(以上,

当時および現在の所属・役職を省略）ほか関係者各位，並びに 2018 年，個人として入学した博士後期課程における，勤務外での研究活動・論文執筆に対するご配慮をいただきました，同協会放送技術研究所ネットサービス基盤研究部の中川俊夫部長（現デジタルセンター専任部長），石川清彦部長，山本正男上級研究員，大竹剛副部長，上原道宏上級研究員（現 情報システム局），藤井亜里砂上級研究員，金子豊主任研究員，小川一人上級研究員及び関係各位に厚く御礼を申し上げます．

そして最後に，学業を本当に支えてくれた家族に深謝します．特に，日頃から筆者を心身ともに支援し続け，さらに博士請求論文審査に向けて本論文への加筆・修正作業が山場を迎えた 2019 年の夏は，本研究への予備知識を持つ余裕のない状態で，かつ自身の余暇や睡眠を割いてまで，本論文の校正作業に適切かつ熱心に支援してくれた，図書館司書でもある妻 村﨑亜希世に深く感謝します．