Vol.2018-IOT-43 No.1
Vol.2018-SPT-30 No.1
2018/9/27

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

村﨑康博[†1]　稲葉緑[†1]　原田要之助[†1]

概要：情報セキュリティポリシーの策定・実施は，全ての組織（企業や官公庁など）において必須施策のひとつであり，想定外の事象にも対応できるように“例外措置”の策定が推奨されてきている．例外措置の普及をはかる上で，利用者が例外措置を実施する上で障害となる要因が挙げられてきている．これらの阻害要因を調べることにより，個人および組織における対応案について考察し提案する．

A Study on Response to Users' Inhibitory Factors in Exceptional Rules of Information Security Policy

YASUHIRO MURASAKI[†1]　MIDORI INABA[†1]
YONOSUKE HARADA[†1]

The formulation and implementation of the information security policy is one of the essential measures in all organizations (private companies and government offices), and it has been recommended to formulate "exceptional rules" to be able to cope with unexpected events, in the dissemination of exception measures. In the dissemination of the exceptional rules, it has been mentioned that the user becomes a failure to implement the exceptional rules. By examining these inhibition factors, we discuss and propose countermeasures for individuals and organizations.

1. はじめに

1.1 例外措置の研究の動機

情報セキュリティポリシーの策定と運用においては，ポリシーをもとに策定される内部規定などの原則規定のほか，緊急時の想定されない事象や，日常業務が著しく困難になるほどではないものの通常時とは異なる処理を必要とする事象に対して，例外措置を予め策定し運用することが効果的である[1].

文献 1 で筆者は，本研究を始めた動機について，例外措置を承認する立場にあった過去の業務経験から由来すると記載した．一般に情報セキュリティポリシーに則って詳細に記載されている内部規範等に対し，例外措置は大まかな方針のみ示される．詳細な対応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，その結果を上長が承認するといった過程を示されることが多い．これは申請内容がもともと内部規範に予め記述することが難しく，ケースバイケースであることが多いこと等が要因として挙げられる．

そのため筆者の場合も，個々の申請内容を自らの内部規範の意味解釈と業務経験とで照らし合わせ，判断することが多かった．上長決済も合わせると労力と時間を要することが多い反面，例外措置の申請は急を要し，迅速に即決することが求められたことも少なくない．

このことから，例外措置に統一的なルールがそもそも存在するのか，他組織ではどのように処理を進めているのかを調査し,今後の対策について研究する必要性が出てきた．

1.2 これまでの例外措置の研究についての概要

情報セキュリティポリシーにおける例外措置の研究については，これまでも文献 1 および 2 などで論じてきた．その概要について述べる．

例外措置は従来の内部規範（原則規定）から逸脱した事象に対し，即違反や罰則を適用するのではなく，同等のリスク軽減が期待できる対策を事前に申請し承認を受けることで回避させ，業務の継続・維持を図る役割がある．

例外措置を導入し，従来の内部規範（原則規定）とセットで運用することで，緊急時のみならず通常時においても想定外の事象がある場合に，迅速に対策をとることが可能である．

ここで例外措置は情報セキュリティマネジメントや組織のガバナンスを維持するために，予め策定・明文化することで措置そのものの管理を明確にすることが求められる．そのためには，例外措置を管理部門のみならず利用部門でもその業務内容にあった例外措置を策定することが効果的である．さらに例外措置が原則規定からの一時的な措置であると考えるならば，定期的に見直しをマネジメントの一環として行う必要がある．

1.3 本稿の目的

しかしその一方で，筆者は例外措置を策定しても実際に利用部門で活用されていないこともあると報告している[2]．そこで文献 2 では，例外措置を普及させるための施策として 3 つ取り上げている．「例外措置の策定方法」「例外措置の実施方法」そして「利用者の阻害要因への対応方法」

†1 情報セキュリティ大学院大学
Institute of Information Security

である．詳細については 3 章で述べるが，このうち「利用者の阻害要因への対応方法」においては，さらに 3 つの従業員のタイプを取り上げた．これは例外措置において「そのものの存在が知らない」，「知っていても内容を十分理解していない」，さらには「理解していても守らない」とすることがあげられる．

筆者はそれぞれのタイプに対する対策を提案したが，特に「例外措置を理解していても守らない」従業員に対しては，罰則の適用の利用を対策案として提案した（3.3 節参照）．これは，罰則に対する従業員が抱く嫌悪感を抑制力となり，罰則を回避させることで例外措置の利用につながることを述べた．また一方で，単に罰則による影響から適用するだけでなく，利用部門・従業員自身の遵法・倫理意識への向上につながるものであることが前提であるべきと提言している．

しかしながら，罰則の適用はそもそも従業員である人そのものがどのように逸脱と向き合うのかを考慮した上で検討するべきではないかと再考する．すなわち組織の形態や風土も様々であるため，逸脱の実態を把握したうえで，罰則も含め対策の手法を調べる必要がある．

そこで本稿では，例外措置の普及を図るうえで従業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，特に例外措置を意図的に実施しない／できない要因について，先行事例調査をもとに探索し，そこからセキュリティポリシーを遵守するための例外措置の策定方法について提案を行うことを目的とした．

こうした利用部門および利用者側の立場にたって，例外措置への阻害要因を明らかにし，阻害要因への対応を考慮した例外措置への普及について述べる．

2. 情報セキュリティポリシーと例外措置

1.2 節で概要を述べたが，本稿で示す例外措置とは，図 1 に示すようなポリシーの基本構造と逸脱領域の間に挟まれた範囲と位置付けている．

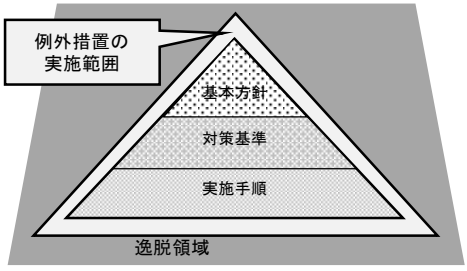

図 1　情報セキュリティポリシー基本構造[3][4]
Fig.1 Basic Structure of Information Security Policy

例外措置は，基本構造を構成する基本方針，対策基準およ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措置は，組織全体に共通したものである必要はなく，対象部門ごとに策定・実施してもよい．個別具体的に例外措置を実施することで，部門ごとの日常業務に沿ってセキュリティリスクを低減させたり，リスクレベルを維持させたりするための，セキュリティ上の見落としや脆弱性がないかのチェックを常に行う [3] [4] ．

2.1 例外措置の必要性と重要性

例外措置には，以下のとおり例外措置をとることの必要性と重要性があると考える[2].

必要性と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があるゆえに，自由度がある例外措置により許容範囲をもつことができることに由来する．

一方，重要性とは，原則規定と例外措置との調和をとって業務を遂行していくことに由来する．結果として例外が日常業務に組み込まれるため，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．

効果としては，まず例外措置への実行処理速度を早くしたりして，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，より客観的に冷静に判断・審査・決定を進めることができる．さらには罰則と組み合わせることとで，責任範囲を明確にすることなどが考えられる．

以上，例外措置はポリシーを見直して盛り込まれるまでの暫定措置として実施される[5]．すなわち例外措置によって想定外の事象への対応をカバーすることにより，ポリシーからの逸脱を防ぐことが期待できる[6].

3. 例外措置の実施を阻害する３つの要因

2 章では例外措置の適用範囲とその必要性・重要性について述べた．しかしながら原則規定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次の 3 つが考えられる．（参考文献 7 に筆者加筆）

3.1 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，原則規定はもちろん，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．

もし例外措置の存在を知らなければ，利用者が行おうとしている行動が，原則規定から逸脱しているという認識があるとしても，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」であるのかどうかという認識はないと考える．

結果として，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．

3.2 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

次に，例外措置の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，規定違反を犯しやすくなる．

3.3 例外措置が存在することも正確に理解もしているが，守らない

そして，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）実際には規定違反を犯してしまう場合がある．

規定や例外について熟知しているがゆえに，途中の作業を省略するために，結果的にリスクを招いてしまう．

リスクを考えず，自分のやりやすい方法に内在するリスクを知らずに，勝手に規定を解釈して結果として逸脱につながる作業を実施する．

3.4 3 つの要因に対する課題

3.1 節および 3.2 節は，行為者（利用者）の例外措置についての知識不足が，規定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定違反であれば，これまでの知識教育を中心として安全教育によって防止することができる．特にこれらの規定違反の防止には，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[8].

しかし 3.3 節は，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[9]. 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．

1. リスクに気が付かないか，主観的にリスクが小さいとき
2. リスクを犯してでも，得られる目標の価値が大きいとき
3. リスクを避けた場合の，デメリットが大きいとき

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られる．

では，逸脱行為に対して利用者（人間）はどのような背景と傾向があるのか．このことについて先行事例をもとに 4 章で取り上げる．

4. 利用者における逸脱行為の傾向

4.1 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[10]. 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，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/管理者から指示を受けていないため, セキュリティへの対策労力は無駄であると認識している．
3. 利用者は，オフライン業務・オンライン業務それぞれでの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があり，BYOD 等の使用は特に影響を与える．

4.2 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[11][12][13]．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．

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を導く可能性がある．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く評価されることがある．すなわち小さいベネフィットを先に経験すると，次に大きなベネフィットが伴う場合，リスク・テイキングをとりやすくなる．

そのため次第に大きいベネフィットをより受容する傾向があり，ベネフィットの物理量の単純な増加のみではなく，損失を回避することでリスク予防への留意がさらに高まったとみなす可能性がある．したがって日常的に状況に応じてリスクを敢行する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．

これはコストが大きい状況にて予防への留意がされなくなっていく可能性を示唆し，さらに大きなコストを先に経験することで損失回避が機能しなくなる傾向がある．

すなわちリスクを伴う意思決定に損失回避が反映されにくくなることで，後続に小さいコストが伴った場合でも，同等の敢行を行い，同様のベネフィットを優先してしまう結果となる．

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，違反を抑制するにおいて重要である．

4.3 利用者における時間リスクと逸脱（いかに時間を節約するかがポイント）

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り，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．したがって特に業務優先等のためにセキュリティルールを故意に違反し，本人の意図に反して情報漏えいにつながってしまう[14].

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．情報漏えいの原因となる違反行為の１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といった，根本的な原因として考えられる．

なお文献 14 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．研修等の教育に頼る形だけでは防ぎきれないものの，持出行動が原因で引き起こされた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求められているとしている．

4.4 利用者における IT 被害傾向

逆に，IT 被害経験を 4 種類（ウイルス感染，不正利用被害，プライバシ漏えい，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[15].

文献 15 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るが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ことがわかっている．

一方で，コスト認知の低い・ベネフィット認知が高い場合，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．

5. 逸脱に関わる社会・組織との関係

4 章では主に利用者（人間）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」傾向にある利用者は，利用者個人に起因する面もありつつ，利用者が所属する組織，さらには生活している社会全般においても起因することが知られている．そこで 5 章では逸脱に関わる組織および社会における関係について先行事例調査により述べる．

5.1 社会規範のコスト

一般に「規範」というものには「社会規範」と「市場規範」の２種類があり，このうち，社会規範を以下に維持して組織内の信頼性・連携を維持することが重要であるといわれている[16].

文献 16 によれば，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，市場規範へ逸脱してしまうと，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．

文献 16 にも述べられているが，客観的なビジネスライクを考えれば，市場規範が優先するように思えるが，社会規範は会社への忠誠心を与える役割もあると筆者も考える．

5.2 個人重視と組織重視～協働して行う不正行為

さらに，会社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[17].

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も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文献 17 では述べられている．

また通常の人でもわずかな不正行為を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損害が大きい．

文献 17 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ものとされる．

5.3 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，対策実行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[18].

文献 18 におけるこの理論は，多くの人が集団的にセキュリティ対策を実行することで脅威を低減できると説得効果を説明する理論である．この理論に基づき，8 つの規定要因（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）から構成されており，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．

結果によると対策実行意思には，8 つの規定要因のうち，「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，個人や組織がセキュリティ対策への実施が促される可能性があることを示している．

5.4 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，ポリシーが守りやすいような運営を行うと同時に，画一化できない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．

このセキュリティ対策はどのような組織でも同じような画一的なルールを遵守するべきでないとし，以下 3 つの仮説をたてて，集団主義におけるポリシーからの逸脱を報告した事例がある[19].

1. 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. 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った形式化できない組織的な要因に影響を受ける．
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．

文献 19 では，これらについてアンケート調査によるデータ分析により，いずれも仮説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．

5.5 情報漏えいにつながる行動に関して

また，個人が組織において「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分かっている[20]．一方で，「低い情報リテラシ」「ルールの不認知」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されている．

これらを受けて文献 20 では，職場環境の改善とともに従業員満足度の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．

6. 逸脱行為への対策案

これまで，ポリシーを知っていても守らない個人や組織の実態について述べてきた．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取り上げる．

6.1 従業員のリスク行動に対する企業の取り組みモデル

組織的違反においては，従業員は個人よりも組織を優先するという善意のもとでは，違反に対する罪悪感が薄れてしまうことが考えられる．これはすなわち，組織の従業員が，自分の意識に基づいて規則に反するようなリスク行動をとる傾向にあることを表す．

そこで従業員のリスク行動に対する企業の取り組むためのモデルを提案されている[21]．このモデルの柱は 3 つあり，「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」である．これらを連携することで相乗的なメリットがあるとしている．

文献 21 においてはアンケート分析の結果をもとに，違反と組織風土に関する共分散構造分析を示している．その中では「個人的違反の要因」および「組織的違反の要因」を紹介している．

6.2 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

利用者にとって，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，対策に対する動機付け（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，製造業等で導入されてきている．この手法を情報セキュリティ分野にも取り入れることを提案されている[22]. これを実践することにより，インセンティブを感じさせることが難しい取り組みについて，実施へのヒントを含むものと考えている．

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，ポリシーやルールおよび操作手順の策定，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るため，利用者に対してモチベーションを与えることで管理する当該手法へ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）での運用管理において，通常であれば，ルーティン業務と捉えられている項目を他の項目とあわせもつことで「クリエイティブ業務」へと進化させ，クリエイティブ思考よりモチベーションを持たせるといった対策が挙げられている．これにより，ルーティン業務に伴うやらされ感から由来するミスを減らし，それによって引き起こされるインシデント発生への低減も狙う. さらには「自律」「熟達」「目的」それぞれのポイント毎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っている．

こうして，セキュリティ対策への実態を知る利用者がモチベーションを得ることにより，自らセキュリティ対策を立案することで, より実効性ある対策が組むことができる．仮に実態に合わなくなったルールがあれば，自分らの権限ですばやく修正できるといったメリットがあるとされてい

る．

6.3 情報セキュリティに関する知識のない利用者への安定感の提供

利用者の中には，情報セキュリティへの知識がない上にあえてポリシーを逸脱する者もいるものと考えられる．こうした場合，利用者に対し，情報セキュリティ対策は安全目的だけでなく，安心も提供できるシステムを検討する目的があることを伝える必要があるとされる[23].

文献 23 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がない利用者がもと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」「親切さ」「親しみ」「知名度」の 4 つにまとめている．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を，事業者やシステムが持っていると判断すると“安心”できる」重要な要因として解釈している．

このような知見に基づけば，組織が情報セキュリティにできる限り対応しきれるインフラやシステムを保有していることにより，利用者は安心して安全な日常業務ができると実感でき，これによりあえてリスクをもって逸脱する行為が防げるのではないかと考える．

6.4 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，利用部門が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定を適用することが考えられる[1].

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，危険行動の経験が，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，例外措置違反の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がある[2].

なお政府統一基準群では，例外措置が違反と抱き合わせた建てつけとなっており，この点が参考になる．違反は事象の 1 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．例外措置を設けると，実際には違反の結果責任が明確となって故意と過失の間のグレーゾーンがなくなり，ガバナンスの観点からは，むしろ効果的と考える[24].

また例外措置の記録は，リスク管理と見直しについても，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どうかが明確になるため，例外措置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[24].

一方で，罰則を伴う場合は，例外措置策定時において事前に規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，規定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[25].

罰則を科すからには，必ず事前に根拠を規定し周知することが求められる，さらに想定外への事象にも措置がとれる例外措置の有効性を担保するために，事前に違反に対するサンクション，すなわち社会的規範からはずれた行為に対して加えられる懲罰的な振舞い，社会的制裁を作っておくことが不可欠である．即ち想定外への事象に対し措置がされた後，結果責任を甘受することを防ぐ必要がある．

文献 25 では，具体的な罰則規定の策定については，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定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，情報システム系専門部門のみならず，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定づくりが必要となる．

罰則を実際に適用することの意味と効果については，ポリシーおよび組織ガバナンスの維持，セキュリティ確保への手段である一方，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られる．

6.5 従来の先行事例における対策に関する考察

本章では，ポリシーを知っていても守らない個人や組織に対し，逸脱行為を阻止する対策についてのこれまでに先行事例を取り上げた．組織の対策についてモデル化すなわち見える化を進めることで，従業員にとって分かりやすくし啓発を促したり，従業員のモチベーションを挙げることで，意識を変えさせたりするなど，対策が心理的に受け入れやすくさせることを重要視してきている．また，情報システムが持つ安全性を示すことや，逸脱には罰則が伴うことを示すことで，従業員の業務に対する安心感を与える施策も考えられている．

罰則を伴う逸脱と罰則を免除する例外措置との境界を明確にすることは，1 つの対応策の原点になると考える．例外措置を様々な事象で対応付けていくための手法について，次章で提案する．

7. 段階的例外措置への適用

6 章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．最後に本稿では利用者の能力別・経験別に応じて段階的に例外措置の承認する手法を提案する．

4.2 節にあるとおり，時間短縮を目的に，従来の工程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利用者のスキルや経験と，例外措置自体が持つリスクの程度に沿って，数段階の「マチュリティモデルでの多段化例外措置」を提案する．

このマチョリティモデルの導入は，例外措置のもつ成熟度を示すことにもつながる．例えば USB メモリ使用への対策と海外プライベートクラウド使用に関わる対策とでは，例外措置を策定して対策するのか，もともと原則規定として規定されているのかなど，それぞれの利用頻度やセキュリティ対策において「成熟度」が異なるものと思われる[5]．さらには利用部門毎によっても彼らのスキルや経験によって「成熟度」が異なる可能性がある．

したがって 5.4 節にもあるとおり，例外措置においても画一的に実施・管理するのではなく，それぞれの成熟度に合わせて策定・管理する必要がある．そこで利用者が例外措置を申請するにあたり，個人の資質として予め求められるものとして，「スキル・作業処理能力」，「経験・体験」，「資格・レベル」および「権限」の 4 つが挙げられると考える．これに，例外措置が本来持つ成熟度と照合したうえで，申請内容を申請者の資質と照合して承認／却下の目安とするルールを予め設定する．

これにより，ある利用者もしくは利用部門が，ある例外措置を申請するにあたり，承認者がより早く例外措置への判断ができるようになる．

本稿で提案するマチュリティモデルを図 2 に示す．原則規定と逸脱領域の間にある例外措置の領域を階層化し，上述にレベルに応じて実行できる例外措置の領域をマネジメントする考えである．例外措置の領域内に設定する階層については組織毎に設定するが，事前に決して逸脱を許さない境界線を明示しておくことが重要である．これが例外措置と逸脱領域の境界線に該当し，決して法令が設定されている境界線（図中の破線）を超えることは無いと考える．

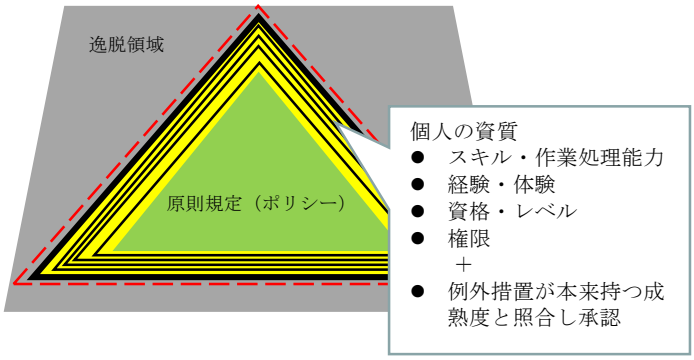

図 2　例外措置におけるマチュリティモデル案
Fig.2 Draft Maturity Model in Exception Rules

マチョリティモデルを導入することにより，利用者が客観的に例外処理を実施するに十分なスキルや資格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ても守らない」利用者への救済あるいは管理が可能となる．

8. まとめ

本稿では，情報セキュリティポリシーにおける例外措置において，例外措置の普及への課題の 1 つと考えられる利用者側の阻害要因について先行事例を中心に述べ，それらに対応するための手法について考察・提案してきた．特に例外措置をはじめポリシーや原則規定そのものから，あえて逸脱しようとする個人や組織の実態や対策を中心にとりあげた．

例外措置は原則規定を同等のリスク低減を備え，原則規定では逸脱する事象に対して迅速に対応できる効果が求められるだけでなく，5.4 節などでも取り上げたように，利用者にとって利用しやすい，承認判断が迅速であるなどの効果も求められる．さらには的確に例外措置を実施できるだけの素質が利用者・利用部門に求められる．最終的には申請内容と素質に応じて段階的に例外措置を認める仕組みが必要と考える．

今後，例外措置のマチュリティモデルによる多段化について調査研究を継続するとともに，効果的な例外措置の各組織への普及方法について引き続き考察していきたい．

参考文献

[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，情処論文誌 Vol.58, No.12, pp,1856-1862(2017)
[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規定の普及に向けての一考察，情処学会研究報告,Vol.2016-SPT-20 No.5(2016)
[3]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)
[4]政府の情報セキュリティの基本的な考え方,情報セキュリティポリシーに関するガイドライン H14,入手先 <http://www.nisc.go.jp/active/sisaku/2002_1128/ISP_Guideline_20021128.html> (参照 2018-07-11)
[5]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)
[6]村崎康博,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]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)
[8]赤崎貫志ほか：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,電学論 D,vol.117, No.6(1997)
[9]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)
[10] Blythe,J.M. Coverntry,L. Little,L.：Unpacking security policy compliance: The motivators and barriers of employees' security behaviors, 2015 Symposium on Usable Privacy and Security, pp.103-122(2015)
[11]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,日心第 75 回大会（2011）
[12]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)
[13]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)
[14]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,情処論文誌 Vol.58, No.1, pp,258-268(2017)
[15]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)
[16]ダン・アリエリー：予想どおりに不合理,早川書房(2010)
[17]ダン・アリエリー：ずる,早川書房(2014)
[18]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,情処論文誌 Vol.56, No.12, pp,2200-2209(2015)
[19]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)
[20] 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,情処論文誌 Vol.56, No.12, pp,2191-2199(2015)
[21]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)
[22]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)
[23]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)
[24]佐藤慶浩：企業における情報セキュリティ対策の実務，佐藤慶浩ホームページ(オンライン)，入手先 <http://yosihiro.com/speech/presenter/2014-11-29b/data (参照 2018-07-11）
[25]近藤佐保子ほか：ネットワーク利用に関する学内罰則規定のあり方」，信学技報，FACE99-38,pp.17-22(1999)