N-014

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

A Study on Necessity and Limitation of Exceptional Rules Concerning the Information Security Policy

村﨑 康博†

Yasuhiro Murasaki†

1. はじめに

1.1 情報セキュリティポリシーでの例外

昨今のマルウエアやサイバー攻撃は，従来の想定内に収まることはなく，これに対処する対策も技術と運用の両面で広がりをみせている．こうした中，不確実性を伴う情報セキュリティ施策は，想定が難しい問題や事象に対して「例外」を考えざるを得ない．ここでの「例外」とは，特に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としたうえで，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．本稿では，前者を「例外規程」，後者を「例外措置」と示す．

1.2 原則と例外の両立

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おり，その基本構造は図 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[1][2][3][4]．例外はこの三層のそれぞれに対応し，例外規程を盛り込むことによって，業務効率の向上が期待できると考える．

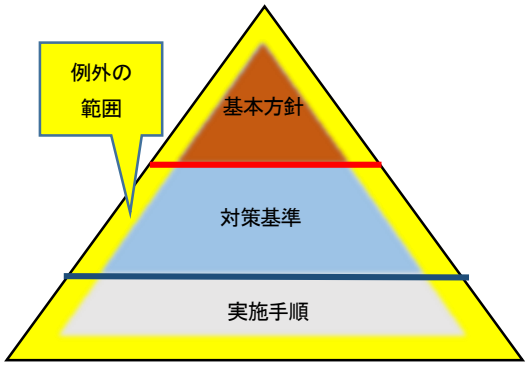

図 1 情報セキュリティポリシーの基本構造

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が伴う場合がある．いずれにしても健全な業務運営をできなくなる．利用者によっては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において無断で実施されてしまうことも考えられる．したがって例外措置は，組織経営の面でリスク回避の意味も含め，極めて重要であり，安心安全な業務運営において役立つものと考える．

また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．一方で管理者側としては，利用者に例外運用を承認したことで，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．なぜなら管理者が例外運用を認めたことは，利用者としては「お墨付き」を貰ったわけであり，リスク回避と同時に責任も管理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者としてはさらに重い責任を負うことになる．管理者の承認・判断が確立していない，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，管理者の精神的な負担も大きくなる可能性がある．

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[5]，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不測の事象に対して，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定できる．

2. 例外の必要性

例外に対して何らかの措置をする場合は，事象の 1 つ 1 つに対して異なる対応を考えなくてはならないため，「判断」という作業を伴う．「判断」の出発点は組織の構成員である個人にあるが，通常は上司の承認が必要になり，場合によってはさらに上位ポスト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考えられる．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（プログラム化）して権限を委譲し，中間管理者で対応を完結させるのである．当該要件に該当しな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・ワーク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．例外措置の一部を例外規程として明文化することで例外措置への承認・実施への効率化が期待できる．

3. 例外規程を策定する意義

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

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

てきたが，先行事例調査やアンケート調査の結果からは，例外措置そのものの運用管理については，必ずしも例外規程として明確に体系化されてきたとは考えられない[6]．そこであらためて，例外規程を策定し，例外規程に基づいて例外措置を厳密に管理運用していく意義を以下に示す．

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・許可作業を可能な限り簡便化・省力化でき，業務効率が図れる．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 1 参照）することにより，管理運用の可視化が期待できる．これが例外規程を策定する意義と考える．

4. 例外規程適用の限界

例外規程を利活用したとしても，その適用には限界もあると考える．例外には限界があり，それを認識した上で例外規定の策定，および措置の実施につながっていくのである．本節では例外規程への利活用を図っていく上での限界について考察する．

4.1 例外規程策定への限界

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．例外措置を実施することで柔軟に業務を維持することができるとも述べてきた．しかしながら，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，Simon の限定合理性[7]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．

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リスク軽減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え方法により，例外措置として許可すれば良いことになる．こうすることでリスク程度をあらかじめ理解し，例外規程として策定することができる（図 2 の右の吹きだしが示す円内と例外措置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）．

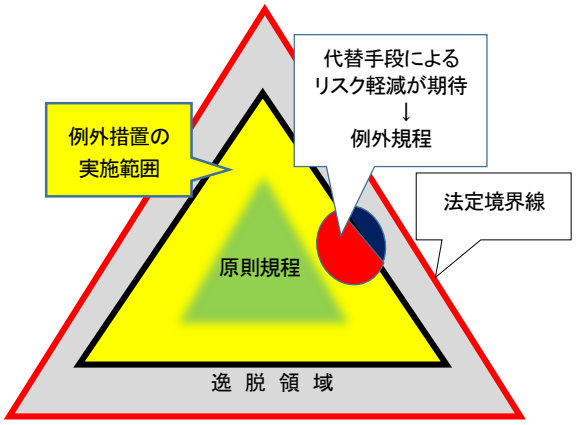

図 2　代替手段による例外規程範囲の確立

しかし，既に例外を認められている利用者側（被管理者側）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．　そのための方策として，「厳罰化」と「組織性逸脱化」という閾値を設ける方法の 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，実行行為者を特定することが難しい（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．また組織が罰則の実行者だとすれば，制定法の場合ほど多くの選択肢は用意されていない．せいぜい就業規則に基づく懲戒処分である．日本の法制では懲戒処分として最強の「解雇」の要件が，先進国に比べて，著しく厳格である．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．

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，擦り合わせ，リエゾン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理解する

必要がある.

4.2 インフラ整備における例外規程運用への限界

次に例外規程を管理運用していく上での限界について，インフラ整備と例外との関係について述べる.

組織活動において，情報セキュリティポリシーと組織が持つ情報システムやインフラ整備などの運用範囲との整合性が取れない（合致しない）ことが起こることについて，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，インフラ整備との整合性が難しい原則規程を補完し，組織の運営にインフラ整備を十分に利用できると考える.

しかしながら組織内で能動的に運用できる例外規程でなければ，インフラ整備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 1 つであると考えられる.

4.3 例外規程がもたらす業務効率化への限界

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.

限定合理性にかかる解釈においては，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できるのである.

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」）を提唱し，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[8].

- 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ものと考える.

不確実性を伴う，想定外な事象への対策として，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である. すなわち例外規程の効力が，組織の意識内にとどまってしまう点が例外規程のもう一つの限界であるとも考えられる.

5. 例外規程の普及に向けての提言

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た上で，本論文として例外規程の普及に向けての提言を述べる.

5.1 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. 例外措置は，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の，業務継続のためのバッファのようなものである. そのため措置を講じながらその効果を検証していくものと考える.

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，ICT 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.

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. 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，例外を明示化・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，及び例外規程に伴う例外措置への評価基準を用いて検証し，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.

5.2 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.

5.3 例外規程を管理部門と利用部門で策定・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ひとつである昨今では，各組織それぞれに適用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られる．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，内閣サイバーセキュリティセンター（NISC）の統一管理基準[9]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られる．個々の組織は，この基準を参考にして，個別の具体的な例外措置を構築することで適切な対応をとることができるものと期待される．さらに，例外措置については組織を超えて全ての組織で利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．

5.4 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，原則業務を運用するに許容できる範囲及び条件であれば，暫定的にもしくは一時的に，原則とは異なる措置を承認・許可する機能がある．これにより，即座に業務を停止させることを回避できるという特徴がある．

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た．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が利用部門・利用者に求められる．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．

5.5 例外措置として実施していく

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規程は，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．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も効果的である．さらには，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についても，分析して対処していく必要がある[10]．

今後，例外措置の蓄積による多様化も踏まえ，利用者のスキル等でランク付けされた例外規程によって，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. まとめ

例外はあくまでも「例外」であって，原則を補完するのが主たる役割である（原則と例外の補完関係）．それが原則に取って代わる（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．

また情報セキュリティポリシーに基づく原則規程からの逸脱に対し，即罰則を用いることのないようにするための例外措置でもあるので，当該例外措置からのさらなる逸脱は認められないと考える．

情報セキュリティにおいて例外措置は欠かせない手段である．この措置を効果的に管理運用する上でも，官民挙げての例外規程の策定が望まれるものと考える．

参考文献

[1] 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 1 日).

[2] 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. (アクセス日: 2019 年 6 月 1 日).

[3] 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 1 日).

[4] 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 1 日).

[5] 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 1 日).

[6] 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)

[7] 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)

[8] K.E.Weick，“不確実性のマネジメント”，ダイヤモンド社，(2002)

[9] 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).

[10] 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)