Vol.2016-IOT-35 No.5
Vol.2016-SPT-20 No.5
2016/9/23

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

村﨑康博[†1]　　原田要之助[†1]

情報セキュリティに関する規定の策定・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と考えられる．さらに一部の組織では，想定外の状況にも対応できるように“例外規定”を策定し，実際に“例外措置”を実施してきている．
本研究ではこれまでに，組織ガバナンスの観点から“例外規定の策定”と“例外措置”の実態を調査し分析してきた．さらに例外措置として認めるべき原則規定からの逸脱範囲について，管理策の具体的事例を基に分析し，さらに例外規定が有効か否かの主観評価を実施した．
本稿では，これらの結果や考察を基に，例外規定の策定普及に向けてのいくつかの対策を考察する．

A Study of towards the popularization for Exception Rules of Information Security Policy

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

Implementation of information security rules, for example policy and standard, is considered as one of measures for all of enterprises. And some organization has implemented “exception rules” which means “escape rules for exceptional case or incident”, and has deployed ‘exception handling measures’.
In this study, present situation of “exception rules” and “exception handling measures” are researched and analyzed from the viewpoint of organizational governance and management. In addition, allowance of deviation from the principle rules, which is accepted as exception handling measures, has been analyzed by using practical cases, and then, a subjectivity evaluation whether “exception rules” was effective or not has been carried out.
In this paper, some measures to deploy exception rules are considered based on the analytic results and considerations.

1. はじめに

ICT を取り扱う組織は，情報セキュリティポリシーにおいて，予め例外規定を策定し例外措置を講じることが必要である[1][2]．しかし調査結果では例外規定の普及は道半ばであり，策定・未策定の組織が２極化しており，さらには例外規定が，主に情報システム系部門が策定・管理・運用していることが明らかになっている[2]．

一方で例外規定を策定するにあたり，情報セキュリティポリシーからの逸脱程度をどこまで例外措置として許容するべきかどうかが，管理策ごとに異なった傾向がみられる．さらには，例外規定が有効であることを分かりやすくするために評価指標を設定することが必要であることを示してきた[4]．

本稿では，組織ごとの情報セキュリティポリシーにおいて例外規定を普及させていくための課題を整理し，普及の方法などについて考察する．

2. 例外規定の定義と範囲

2.1 原則規定と例外規定

“例外”という用語は広範囲の内容を含んでいるため，はじめに本稿での例外規定の定義と範囲を示す．

まず日常業務において定常的に実施されている措置が，情報セキュリティポリシーに明記されている規定を「原則規定」とする．原則規定から外れることを「逸脱」とし，その内容・範囲を厳密に評価して，権限者によって承認した逸脱を「例外」として定義する．また情報セキュリティポリシーへの文面化の有無を問わず例外を実施した行為を「例外措置」とし，例外措置が文面化されている規定を「例外規定」と定義する[4]．

表１　緊急時例外措置と平常時例外措置
（参考文献 5 より作成）

	特徴	基本方針（2.3.1 項参照）	対策基準（2.3.2 項参照）
緊急時例外措置（2.2.1 項参照）	・一時的な措置 ・規定されていない／規定が不十分の場合あり	・事故・事件等で安全対策上大きな脆弱性が発見される事象等	日常業務に大きな影響を及ぼす事象等
平常時例外措置（2.2.2 項参照）	・比較的長期間継続する措置（再利用がある） ・予め規定されることが望ましい	・新規事業や法改正に伴うセキュリティ要件が変わる事象 ・NISC や外部監査機関等から見直しの勧告を受けた事象等	日常業務に大きく影響を与えないものの，原則規定では対応できない事象等

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

Vol.2016-IOT-35 No.5
Vol.2016-SPT-20 No.5
2016/9/23

2.2 緊急時例外措置と平常時例外措置

例外措置を時間的な制約や規定などへの明文化により，「緊急時例外措置」と「平常時例外措置」の２つを定義する．それぞれの措置の特徴を表１に示す．

2.2.1 緊急時例外措置

緊急時例外措置は，大災害やインシデントなど，想定外の事象で必ずしも規定が策定されておらず，もしくは不十分なため，その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の事象が対象となる．即時対応が求められる例外措置であり，主に BCP に規定すべき一時的な措置である．

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，例外規定を用意して緊急時に備え，自由度を確保するねらいもある[8][7]．

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，当該措置を内部規定に盛り込む場合では，原則規定にこだわらない例外規定として取り扱われる[2][3]．

2.2.2 平常時例外措置

一方，平常時例外措置は重大かつ緊急を要するものではないものの，原則規定では措置できない事象に対して講じる例外措置である．そのため予め例外規定として策定され，ある程度の期間にわたって例外規定が利用される．

当該措置が規定されていない場合，原則規定から逸脱した事象や行為は逸脱領域にあたるため，逸脱とみなされる．また原則規定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対応できない．この対応できなくなる事態を避けるため，多くの組織では当該措置に例外規定を盛り込んでいる．

2.3 情報セキュリティポリシーにおける例外規定

例外規定は，組織の内部規定等で原則規定と共に用いられる情報セキュリティポリシーに盛り込まれる．情報セキュリティポリシーの基本構造は，図１に示す通り三層構造で解説されている[10][11][12][13]．なお，図中における例外規定の範囲としては，この基本構造の外枠に位置づけられる．

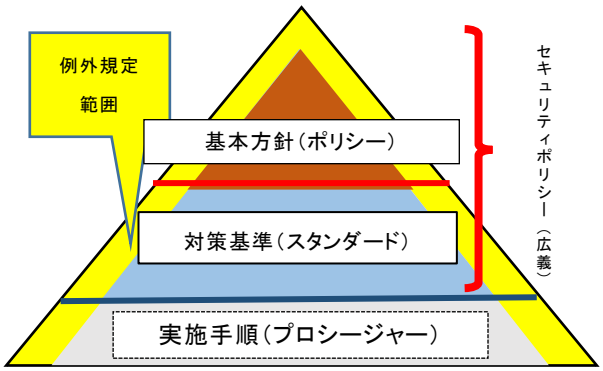

図１　情報セキュリティポリシー基本構造
（参考文献 14 から 17 より筆者加筆）

情報セキュリティ対策における基本的な考え方を定めるものが，図１の最上層にある「基本方針（狭義の情報セキュリティポリシー）」である．

この基本方針に基づき，全ての情報システムに共通の情報セキュリティ対策の基準を定めるのが，２層目の「対策基準（情報セキュリティスタンダート）」である．

前述した「（広義の）情報セキュリティポリシー」はこの「基本方針」と「対策基準」を総称することがあり[7]，本稿でも同様に定義し，以下「ポリシー」と呼ぶ．

2.3.1 情報セキュリティ基本方針での例外規定

基本方針は，組織の情報セキュリティについて，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（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[14]．

基本方針では，例外規定の容認の可否や，非常時での緊急対策本部の設置・指示命令系の統一などといった，大筋の方針を定めている．そのため頻繁にかつ定期的に見直しされるものではなく，基本方針における例外規定についても同様となる．

したがって基本方針における例外規定の策定は，以下の事象が起きた時に策定を検討することになる．

緊急時例外措置

- 事故・事件等により安全対策上の大きな脆弱性が発見される事象など，現方針では対応できないとき

  例えば，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．

平常時例外措置

- 新たな事業展開や法律・法制度の変更にともなうセキュリティ要件が変わるとき
- ＮＩＳＣや外部監査機関などから見直しの勧告を受けたとき

  例えば「パブリッククラウドを積極的に利用する」，「情報漏えいの対策として USB メモリの利用は全面的に禁止」するかどうかに対する運用方針の決定がある．

2.3.2 情報セキュリティ対策基準での例外規定

対策基準では，情報セキュリティについて基本方針を実行に移すための具体的な対策が記述され[14]，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してもよい．一方で，セキュリティレベルを安全とみなせるレベルに維持するために，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．基本方針とは異なり，各現場レベルでの状況の変化に適切に対応するために，原則規定の見直しや例外規定の追加策定が求められる．

対策基準での例外規定は，基本方針とは異なり，個別具体的に例外措置を規定する．すなわち当該事象に対応する措置は，現在の規定を見直して盛り込まれるまでの間，暫定措置として実施される．

なお対策基準は，2.2 節で述べた「緊急時例外措置」と「平常時例外措置」ではそれぞれに異なる運用となる．

緊急時例外措置

緊急時例外措置では，日常業務に大きな影響を及ぼす事象への措置が求められる．例えば，OS のサポート期限切れに伴う，基幹システムのソフトウエア更新への対応がある．OS 更新に伴うソフトウエア改修が困難であったり，当初の想定をこえるコストがかかったりしたことなどから，サポート切れの OS 自体の延命措置の依頼など，日常業務に暫定措置が必要となった組織もあったと考えられる[2]

平常時例外措置

日常業務に大きく影響を与えないものの，原則規定とは異なる措置をとる必要がある．日常業務で想定できるものであったとしても，例えば BYOD のケースで

Vol.2016-IOT-35 No.5
Vol.2016-SPT-20 No.5
2016/9/23

は，措置の煩雑さなどから，規定していない組織が多い[6]．このようにあえて規定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とになる．

したがって対策基準では具体的な例外規定の策定が必要であり，それに基づく例外措置を具体的に実施するための実施手順（図１の最下層）の作成が必要になる．

2.4 本稿での例外規定の範囲

以上，例外規定における定義とポリシーとの関連性について述べたが，本稿では主に対策基準における「平常時例外措置」を研究対象範囲として，例外規定の策定と例外措置の実施について述べる．

対策基準を対象とした理由は，まず 2.3 節で述べた通り，基本方針に比べ対策基準におけるポリシーの見直しが，日常業務に直結し，柔軟かつ定期的に行わなければならないからである．

また平常時の例外措置を対象としたのは，緊急時の例外措置に比べ長期間運用されることから，原則規定からの逸脱程度の判断や評価が，定期的に管理される必要があるためでもある．

平常時の例外措置を規定するには，当該措置によるリスク低減が情報セキュリティ管理策基準の求めるリスク低減と同程度であることが求められる．

表 2　例外規定策定に関する仮定と結果
［参考文献 6 から著者加筆］*脚注

仮定	結果
仮定１：多くは専門部門において組織の統一基準群で策定	・事象が起きたその都度例外措置を実施 ・必要に応じてその後規定として策定／見直ししている．
仮定２：例外規定の策定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二極化している．
仮定３：規定の策定は，組織によって異なる	・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群で策定
仮定４：原則規定からの逸脱程度から，例外規定策定の傾向がわかる	・組織の多くは管理策の実施状況をもとに，原則規定からの逸脱に対する許容範囲を判断 ・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定とする ・原則規定と例外規定と組み合わせることで，柔軟な運用が可能
仮定５：例外措置の定量的評価ができ，規定策定へのヒントにすることができる	・主観評価実験の結果から，各管理策への満足度・安全度を高めるような例外規定を具体的に策定することで，例外規定全体の許容限が上がる． ・満足・安全な管理策に基づく例外措置を実施することにつながる

3. 例外規定への仮定の設定とアンケート調査結果

組織における例外規定の実態と効果を把握するために仮定をたて，アンケート調査を行った．その結果を表 2 に示す[15]．

本稿では，先行事例調査とアンケート調査を通じ，例外措置の状況から組織の情報セキュリティの管理状況が分かることを示す.これは管理面における組織の情報セキュリティガバナンスの把握につながると考えられるからである．

仮定１の結果から，例外規定の策定が，組織によって導入程度が異なっており，仮定２の結果から，全体では例外規定の策定状況は策定済と未策定の二極化状態にあり，組織によっては例外措置を活用できているとはいえないことが分かる．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，例外措置が半数の組織に活用されていること，また官公庁や自治体では統一基準群の例外規定を推進している[1][2]ことから，例外規定を策定する組織が増えると考えられる．

さらに仮定３の結果から，組織において例外規定を実際に策定し，具体的な例外措置を実施・管理しているのは，情報システム・情報セキュリティを専門とする情報系部門に集中していることも明らかになった．したがって情報セキュリティに関する規定が，全ての組織における必須施策の１つとなっている昨今，各組織ではそれぞれに適した例外規定と措置の導入への検討をしていく必要がある[2]．

また例外規定の策定と例外措置の実施の効果を，仮定４にもとづく原則規定からの逸脱程度の許容範囲と例外措置との観点と，仮定５にもとづく例外規定策定への主観評価実験による定量的評価の観点から分析している．これらにより例外規定は，原則規定からの逸脱に対する許容範囲を明確に判断し，原則規定の定期的な見直しとともに策定することが必要と述べられている[3]．

4. 例外規定策定普及に向けての考察

本章では，これまで本稿で述べてきたことを受けて，適切な例外措置の普及をはかり，例外規定の策定に向けての考察を述べる．

4.1 概要

例外規定を策定・管理する管理者側と実際に例外措置を実施する利用者側に分けられるが，本稿では主に管理者側を中心に取り上げる．これは，これまでの研究調査の結果から鑑み，組織ガバナンスを中心に担うのは管理者側であること，両者を比較すると例外措置を承認する側である管理者側の負担が大きいこと，さらには，例外規定を普及させるためには，管理者側からの働きかけが重要であると考えられる．

そこで本章では，以下の項目にわけて考察する．

- 例外規定の策定方法（4.2 節）
- 例外措置の実施方法－３つの具体例をもとに－（4.3 節）
- 利用者側の阻害要因への対応方法－教育，監査・評価，罰則をもとに－（4.4 節）

4.2 例外規定の策定方法

例外規定の策定に向けて，策定の方法には３つある[1]．

4.2.1 トップダウン方法

まず管理部門で例外措置の管理策・対策基準を取り決め，具体的には実施手順を明記して規定する．

* 脚注：もともと文献 6 での仮定は８個設定しており，本稿での仮定１～５はそれぞれ，引用文献での仮定５・１・４・７・８にあたる．

経営側，組織全体の統一規定・基準・ガイドラインにおいて例外規定を策定．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．

4.2.2 ボトムアップ方法

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規定を策定．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．

利用部門から申請時に，実施手順を添えた管理策・対策基準案を提案・提出させ，管理部門が審査・承認・許可する．

4.2.3 ハイブリッド方法

4.2.1 と 4.2.2 の両項のトップダウンとボトムアップを混合する．管理部門は利用部門の管理責任者に対して，例外規定の策定に関わる権限を付与する旨の例外規定を策定するだけにとどめ，説明責任と報告義務を課すものである．一方，利用部門の管理責任者が利用部門の責任範囲で，独自に例外規定を策定して，例外措置を実施するか，例外措置を実施したのちに，例外規定を策定するかのどちらも実行できるようにする．

4.2.4 例外規定の策定方法への考察

本稿では，4.2.3 項のハイブリッド方法を提案する．

これは，共通する規定策定は，基本方針にてトップダウン方式を取り，個別具体的な規定策定は，対策基準にてボトムアップ方式を採用する際に有効な手段であると考えるからである．例えば ISO における「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の共通な構造が，ISO Directive ANNEX SL で規格化されている[16]．これを例外規定に適用するわけである．

また，ある特定の事象に対する措置においても，分野ごと組織ごと部門ごとそれぞれに特色のあると考えられる．例えば，USB メモリの使用も，情報通信業では，禁止とする規定や例外規定として規制がある一方で，大学等教育機関などでは，緩和されているなど異なる措置を取られていることが分かっている[5]．

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，平常的なもの主に取り扱うのかで，異なってくる．即ち組織ごとに例外規定を策定させるには，現場責任者への権限，例外規定の教育が伴うものと考えられる．

一方で，一般社会の市場動向や組織の経営方針，今後の IoT 等技術の進歩に伴い，例外措置が適用される事象が起こりやすくなるのであれば，例外措置・例外規定を柔軟に変化させることが望ましい．

これは例外措置の関わる事象が起こりやすくなることは，リスクも起こりやすくなることにつながるためである．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[17]．

また，例外措置は「緊急時であれば即時性，平常時で長期間運用」と仮に運用したとしても，見直すまでは一時的な措置であるととらえるならば，恒常的な原則規定でない限り，措置も変化し，見直しを経て，例外規定も変化するものと考えられる．

さらには，例外規定からのさらなる例外は避けるべきである．既に例外を認めているため，利用部門側（被管理側）の心理的抵抗感が減少しているため，図に乗って要求してくることが考えられる．しかし管理側にとって，“例外からの例外”を認めることは，業務遂行上リスク要因を増やすことにつながるものであると考える．

4.3 例外措置の実施方法（３つの具体例をもとに）

本節では，例外措置の実施方法について，原則規定からの逸脱と例外規定との関連性にかかるアンケート調査の結果のうち，図２で上位を占めた「外部クラウド」「可搬型メディア」「公衆無線 LAN」の３つの具体的な管理策をもとに考察する[4]．

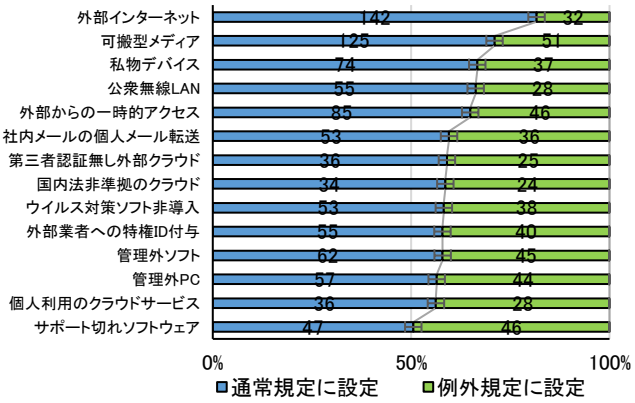

図２ 原則規定と例外規定との比率[4]
（択一，グラフ内の数値は回答数）

4.3.1 クラウド事業者のサービス

クラウドサービスの利用については，まず一時的に利用するのか，基幹システムの一部として常時使用するかで，管理策が異なる．そのため基本方針との関連性が強く，例外規定を策定するかどうかは，すなわち経営層の判断がまず重要となる．

経営の基本方針でクラウドファーストと経営判断したのであれば，例外規定を策定する必要はない．管理部門がクラウド事業者と統括契約して利用することで，運用することになる．

一方で，必ずしもクラウドを組織で全面に利用するのではなく，あくまでも一部のビジネスで一時的に使用する場合であれば，例外規定を策定すれば十分である．

しかし，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，さらにはリスクがあることも認識するようになってきている．すなわちクラウド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[22]．

よって今後，クラウドに対する例外規定は，規定に盛り込むことが望ましく，急ぐ場合には例外規定を利用するようになるものと考えられる．

4.3.2 可搬型メディア（管理外 PC，スマホ，USB メモリなど）

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組織は少ない．一方で，小中高学校や教育機関[23]，研究施設，個人情報・秘密情報を扱う機関[9]においては，禁止もしくは組織からの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．

USB は使用禁止，PC は組織が貸与するといった原則規定の策定を前提とし，必要に応じて，例外措置の一部を緩和する例外規定を策定する方法が考えられる．

一方，スマートフォンの貸与については組織における費用対効果の考慮から，使用禁止でも組織貸与のいずれでものなく，私物スマートフォンの使用を認める BYOD

の方向に進むものと考える．したがって，BYOD の例外措置は必要とされており，例外規定の策定は必要であると考える．方策案としては，まずスマートフォンなどの私物端末の業務での利用を許可することになる．

そのうえで管理部門は「接続してもよいクラウドやネットワーク，そこで管理してよいデータは何か」といった詳細な例外について明確に例示するなどして，従業員への周知徹底と，「どういった使い方をすると危険なのか」などの教育を強化することが必要となる．

BYOD を禁止する選択肢もあるが,その結果として現在のように安全性が担保されていない BYOD が隠れて使われ続けることになる．すなわちリスクが隠れてより高いリスクにつながることを管理部門は肝に命じるべきである．[24]

4.3.3 公衆無線 LAN

日常業務において，公衆無線 LAN のうち特に SSL 等暗号化されていないものへの利用は禁止するか，一部制限を設けて例外措置として利用させる方向である．例えば，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，など一般利用者でも対策が求められるルールの順守を徹底させた上で利用を認めることが考えられる[25]．

一方で，組織内での無線 LAN の使用については，組織によって利用状況が異なることは考えられるものの，高速化や利便性に伴い今後は無線LAN利用がより進む可能性が高いと考える．しかし暗号化技術の進歩があるものの有線と比べれば，無線というメディアの特性からくる情報漏えいのリスクが高いままである．したがって管理部門が全体管理できる無線 LAN システムを構築する場合，設置・設定・運用については厳密に規定しなくてはならない．このため，一部の利用部門で例外措置としての無線 LAN の利用は減り，原則規定による策定が進むものと考える．総務省では企業等が安心して 無線 LAN を導入・運用するための手引きを提供しており[26]，導入に関しては，ほとんど原則規定として細かく例示している．例えば，例外規定が導入されると考えられるのは“原則禁止”としている「アドホックモードの制限」など極少数で，かつ利用していれば，厳密に説明（Comply or Explain）が求められるものと考える．

4.4 利用者側の阻害要因への対応方法（教育，監査・評価，罰則をもとに）

本節では，利用部門すなわち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，阻害要因への対応策をもとに例外規定の策定を提言する．

4.4.1 例外措置の実施を阻害する３つの要因

まず原則規定から逸脱し，例外規定に適用しうる措置の実施を阻害する要因は次の３つが考えられる．（参考文献 18 に筆者加筆）

(1) 例外規定の存在自体を知らない

・決められた例外規定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，例外規定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．
・もし例外規定の存在を知らなければ，現場担当者が行おうとしている行動が，例外規定からも逸脱している「不安全行動」であるという認識すらない．
・結果として例外規定から逸脱した行動になってしまうということも知らない．

(2) 例外規定が存在することは知っているが，正確に理解していない

・例外規定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．
・その例外規定がなぜ策定されているのか，またその例外規定にはどういう意味があるのか，もしこのような背景についての知識がなければ例外規定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) 例外規定が存在することも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．

(1)と(2)は，行為者（利用者）の例外規定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[19]．

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，(3)については，例外規定をよく理解して例外規定を守らないという場合には，例外規定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[20]．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，おのずと例外規定の幅も広げざるを得ないものと考えられる．

以上を踏まえ，利用部門側の阻害要因に対して克服すべく，管理部門が実施する方法として 4.4.2 項で考察する．

4.4.2 「政府統一基準群の標準化」をもとにした「教育・研修・訓練」

「(1)例外規定があることを知らない」阻害要因への対策としては,NISC の政府統一基準群は手順やひな形も用意されていることから最も参考となるものであり，これを利用して，例外規定の整備，普及をはかることが望

ましい.

利用部門（現場）が，例外規定そのものの存在を知らない場合には，組織全体や部門ごとに正しく周知・普及していないおそれがある．そのため，まず管理部門側の体制強化（原則規定および例外規定の存在の周知徹底）が求められる．ここでは，内部規定に例外規定を盛り込めるような管理者が求められ，例外規定の見直し，特に逸脱程度とリスクを判断（評価）して例外を許可できる体制や承認責任者の選出が必要と考える．

なお，これらの担当者は，管理部門だけでなく，利用部門（現場）の責任者にも求められると考えられることから，組織全体の全ての中間管理者にも例外規定に関する知識を与える必要あり．当該者向けに教育・研修・訓練などの対策・実施が必要と考える．例えば，ケーススタディによる机上での実習，あるいは，OJT など管理部門が現地利用部門の責任者と連携して部門内の例外規定を策定する実務を行い，原則規定と例外規定との関係や例外措置によるリスクなどについて理解を深め，普及を図るべきである．

前述のとおり，政府統一基準群では例外措置の業務フローにおいて，例外措置を認めるための，上申書：誓約書の稟議がある．例外措置が企業間のサプライチェーンに及ぶ場合に関しては特に，書類のみで例外措置におけるリスクを完全に担保することは難しいと考えるが，「Comply or Explain」を実際に適用していくことで効果は期待できると考える．

4.4.3 外部認証制度・情報セキュリティ監査の利用

「(2)例外規定を正確に理解していない」阻害要因への対策としては，4.4.1 項で述べたように，まずは例外規定のリスクを認知させ，「Comply or Explain」を徹底させることが求められる．しかしリスクについて不明あるいは意見が一致しない場合は，外部認証制度を利用したり，情報セキュリティ監査を受けたりすることで，統一見解を持つことが望ましい．

例えば，ISMS や SOC2 Type2 の認証取得など，第 3 者評価や外部認証を利用する方法について述べる．本方法においては例えば，ISMS 取得を目指す組織であれば，情報セキュリティポリシーの策定・整備が当然求められるものであり，「ISMS 適合性評価制度」において用いられる適合性評価の尺度と整合できる利点がある．特に，認証を既に受けている組織であれば，更新や定期的な検査において，例外規定の策定と適切な例外措置のリスクを評価できる．いずれにしても，経営側が，「監査から指摘される／認証を受ける」ことを意識して，例外規定を策定・運用・管理していくことが望ましい．

次に情報セキュリティ監査による例外規定への強制的な理解獲得を図ることが考えられる．

情報セキュリティ監査では，例外規定が正しく規定されているか，あるいは例外措置が適切に運用されているかなどを評価することが可能であり，組織全体の例外規定の平準化への効果も期待できる．組織の情報セキュリティ担当部門とは独立した監査部門の立場から，例外規定の有無や例外措置の適切な措置，原則規定からの逸脱程度などを，内部監査や外部監査によって客観的に指摘されることが期待できる．「改善勧告」があった場合などについては，管理部門が指摘事項に基づいて規定を見直し，例外措置の運用を監視する仕組みが要請される．

なお，経済産業省では「情報セキュリティ管理基準／監査基準」を策定し，監査人が原則として監査上の判断の尺度として用いるべき基準を提供している．

いずれにしても，例外規定の管理・運用における PDCA の「C:チェック」機能として，外部認証制度や監査を活用することができる．これらの結果により，情報セキュリティ管理基準の見直しにつながり，情報セキュリティポリシーにおいて例外規定の策定・普及が果たせるものと考える．

4.4.4 罰則の適用の利用

「(3)例外規定を理解していても守らない」阻害要因への対策としては，利用部門が例外規定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．

違反を防止するには，例外規定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，例外規定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[20]．

なお政府統一基準群によれば，例外措置は違反と抱き合わせた建てつけとなっている点が参考になる．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．

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．例外規定の有無により違反であるかどうかが明確になるため，例外規定に則っていれば，故意の違反・逸脱ではないことが立証できる[8]．

一方で，罰則を伴う場合は，例外規定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．

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規定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て措置がされた後で，結果責任を甘受することを防ぐ必要がある[21]．

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．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．

5. むすび

以上，本稿では，組織のポリシーにおける例外措置について，主に対策基準での平常時例外措置を中心に取り上げ，当該措置の必要性と例外規定を策定し措置を具体化することの必要性を論じた．

5.1 総合考察

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の運用業務を開始することは難しい．例外措置は，情報セキュリティポリシーに基づく原則規定が維持できないときの，日常業務が継続できるバッファのようなものである．措置を講じながらその効果を検証していくものでないといけない．

その例外措置を予め例外規定として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を移行できるメリットがある．

上述の通り例外措置は，原則規定から逸脱した事象をすぐに違反・罰則措置をとるのでなく，通常業務の運用で許容できる範囲・条件であれば，暫定的に一時的に通常とは異なる措置を承認・許可する．これにより，即座に業務を中断させることを回避できる．

さらには，例外規定があることで，情報セキュリティポリシーの変更の少ない運用に貢献できる．具体的には，例外規定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．今後，例外規定の効果を可視化することについても考えていきたい．

5.2 例外が持つ可能性について

原則規定は，原則であるゆえに保守的な規定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定の範囲を狭くし，ビジネス展開を狙う目標・目的をもつために，例外規定を広げて例外措置を位置付けることもできる．

つまり例外規定により，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，基本方針にて例外規定を承認し，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なると考える．例えば対策基準において例外規定を策定し，新規デバイスの導入を積極的に実施することもできる．

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．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．ルール化はその後で決めることが一般的に行われている．

明確に例外規定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，例外規定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．

5.3 今後の展望

最後に．例外規定には，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．

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，自由度がある例外規定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，原則規定と例外規定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．

例外措置は各組織で実際に規定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規定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規定・例外措置の共有化など，全ての組織で例外規定を利活用できるような体制作りなどを，今後検討していく必要があると考える．

謝辞 本調査を実施するにあたり，アンケートへの回答にご協力を頂きました企業や団体，組織の皆様に感謝します．

またアンケートの封入，データ入力に多大な協力をいただいた，神奈川県立麻生養護学校元石川分教室，神奈川県立高津養護学校川崎北分教室，神奈川県立鶴見養護学校岸根分教室，神奈川県立みどり養護学校新栄分教室，川崎市立中央支援学校（五十音順），外 1 校の神奈川県内の特別支援学校に感謝します．さらに御指導頂いた本学原田研究室各位ならびに本学事務局の皆様に感謝致します．

参考文献

[1] 村崎康博ほか：情報セキュリティ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
[2] 村崎康博ほか："情報セキュリティ調査で分かった組織における情報セキュリティポリシーの"例外措置"について", 情報処理学会研究報告, vol.2016-EIP-71, No.6, 2016
[3] 村崎康博ほか："情報セキュリティポリシーの例外措置における主観評価に関する一検討", 信学総大, A-12-3, 2016
[4] 村崎康博ほか："情報セキュリティポリシーにおける例外措置の効果への一検討", 情報処理学会研究報告, vol.2016-EIP-72, No.2, 2016
[5] 村崎康博ほか："情報セキュリティポリシーにおける例外措置に関する一考察",第 15 回情報科学技術フォーラム講演予稿集, 3P-RN003, 2016
[6] 平木健士ほか：業務利用のスマートデバイスのマネジメントについて，システム監査学会 2013 年度第 27 回研究大会, 2013
[7] 内閣サイバーセキュリティセンター：政府機関の情報セキュリティ対策のための統一管理基準（平成 24 年度版）解説書「1.2.1.3 違反と例外措置」, 内閣サイバーセキュリティセンター(オンライン), 入手先< http//www. nisc.go.jp/active/general/pdf/K304-111C.pdf>(参照 2016-08-02）
[8] 佐藤慶浩：企業における情報セキュリティ対策の実務, 佐藤慶浩ホームページ(オンライン), 入手先 <http://yosihiro.com/speech/presenter/2014-11-29b/data/resources/2014-11-29 b-enPit.pdf>, (参照 2016-08-02）
[9] 「企業セキュリティ調査　Part2 USB メモリー編」日経 NETWORK 2012 年 7 月号 pp.42-44,2012
[10] 内閣サイバーセキュリティセンター：政府機関統一基準適用個別マニュアル群 DM2-04 2011 年 4 月，内閣サイバーセキュリティセンター(オンライン), 入手先 <http://www. nisc.go.jp/active/general/kijun_man_index.

htm>(参照 2016-08-02)
[11] 日本規格協会：JIS Q 27001,2014（ISO/IEC27001,2013）情報技術―セキュリティ技術―情報セキュリティマネジメントシステムー要求事項,日本規格協会，2014
[12] 中尾康二編：ISO/IEC27001,2013 情報セキュリティマネジメントシステム要求事項の解説，日本規格協会，2014
[13] 日本規格協会：JIS Q 27002,2014（ISO/IEC27002,2013），情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範,日本規格協会，2014
[14] 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
[15] 情報セキュリティ大学院大学原田研究室：2015 年度情報セキュリティ調査, 情報セキュリティ大学院大学原田研究室ホームページ（オンライン），入手先<http//lab.iisec.ac.jp/~harada_lab/survey.html>(参照 2016-08-02)
[16] 原田要之助, ＩＴシステムのリスクマネジメントの全体像，佐々木良一編「ＩＴリスク学」，pp122-138
[17] 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
[18] 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)
[19] 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.
[20] 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)
[21] 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)
[22] 総務省,「平成２７年度版情報通信白書」，2016
[23] 文部科学省,「学校における携帯電話の取扱い等について（通知）」平成 21 年 1 月 30 日（オンライン），入手先<http://www.mext.go.jp/b_menu/hakusho/nc/1234695.htm>(参照 2016-08-02)
[24] 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），入手先<http://itpro.nikkeibp.co.jp/article/COLUMN/20120920/423888/>(参照 2016-08-02)
[25] 総務省,「一般利用者が安心して無線 LAN を利用するために」，2012/11/2（オンライン），入手先<http://www.soumu.go.jp/main_content/000183224.pdf>(参照 2016-08-02)
[26] 総務省,「企業等が安心して 無線ＬＡＮを導入・運用するために」，2013/1/30（オンライン），入手先<http://www.soumu.go.jp/main_content/000199320.pdf>(参照 2016-08-02)