Vol.2015-DPS-164 No.7
Vol.2015-EIP-69 No.7
2015/9/11

情報セキュリティにおける例外措置に関する考察

村﨑康博[†1]　　原田要之助[†1]

今や情報セキュリティに関する規定の策定・実施は，どの組織（企業や官公庁など）においても必須施策のひとつと考えられる．これらの規定は従来のインシデント事例をもとに作成されている.また一部の組織では，想定外の状況にも対応できるように“例外規定”を策定している．

しかし“例外措置”をどの対象範囲まで認めるべきかについては，組織毎の判断に委ねられている可能性がある．また不測の事態にリスクを正しく認識した上で，例外措置を講じているかどうかも明らかではない．

本研究では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取扱いやその効果などを調査する．加えて，社会全体や分野毎に統一基準が必要かどうか，その期待効果について検証を進めていく．

A Study on the Exceptional Rules Concerning the Information Security Policy & Standard

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

Nowadays, Develop and promote of official rules about the information security is one of mandatory measures for every enterprise. Those rules are designed based on existing incidents. Some of enterprises implement "rule for exceptional case" in order to respond to unexpected situation.

However, definition of exceptional case such as acceptable inside a range might be dependent on decision of individual organization. It is not obvious that they assess security risk of unexpected situation definitely, whether having taken exception measures either.

In this study, actual conditions of "the exceptional rules" and exception measures, and the benefit of enforcement are surveyed from the viewpoint of organizational governance. In addition, the necessity of standards across society or industry wise, and its expected effectiveness will be investigated.

1. はじめに

「例外」という言葉は，広辞苑によれば例外とは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とされている．一方「例外」は「原則」という言葉と対で表現されることも多い．たとえば文章で「原則～とする」と表現されると，行間に「例外」の存在があり，ある程度許容されていることを読み取ることができる．即ち我々は「原則として」とルールや規定を伝える場合，相手に対して「例外がある」ということも暗に伝えることが多い．

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を営んでいる．ルールには一般に原則と例外が存在することが多く，例外を適切に規定し実施することで，我々は原則による規律を維持できるものとしている．

しかしながら事象には，あらかじめ原則には措置できないものの，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，後者はルールや規定を見直すために規律を維持できなくなるおそれがあり，仕事や家庭生活が一時中断する可能性もある．

予め例外規定がある場合には，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継続することが可能である．一方例外規定がない場合には，どのように処理すべきか，あるいは申請そのものを却下もしくは取り下げてもらうべきかを即座に判断できず，通常業務に支障をきたすことがある．案件が「情報セキュリティ」に関わるものであれば，判断と実施，指示を早急に進めなければ，深刻な影響を受けることにつながるおそれもある．

一方で，例外規定を策定する場合には，例外をどのように認めるのかについての規定が必要となる。そのためには規定に関する文面などの検討も必要である．

そこで本稿では，まず例外規定の必要性について，実在する事業体（以下，仮にＮ社）の実務事例をもとに他の事例をも含めて，必要性の高いことを確認する．次に，これらの実態から想定される問題点を取り上げる．例外については，あまり先行研究がないことからアンケート調査により，実態を確認する予定である．これらについて説明する．なお本事例については一般に公開されていないため，考え

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

方を紹介していく．

2. 情報セキュリティにおける例外規定の事例

まず本稿では，本研究テーマの大前提になっている，N社の窓口担当者の日常業務について紹介する．

当該担当者は企業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るが，通常申請や相談を受けたとき，まず規定や基準，ガイドラインの原則に当てはまるかどうか確認する．また通常の手続きで処理できないと判断した場合は，当該規定等において，例外規定があるかどうかを調べることが多い．業務フロー例としては図１のとおりである．

また例外申請の主な相談内容例は次の通りである．なお必ずしも実務と合致した事例ではないことを断わっておく．

- WindowsPC のみ接続を認めていないイントラネットに，生放送でリアルタイム作画をするための Mac を接続したい．
- 特定の外部クラウドサービスの導入を検討しているが未だ第３者認証を得ていない．しかし○○機能を利用するには他に選択肢がない．
- 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のため使わざるを得ない．

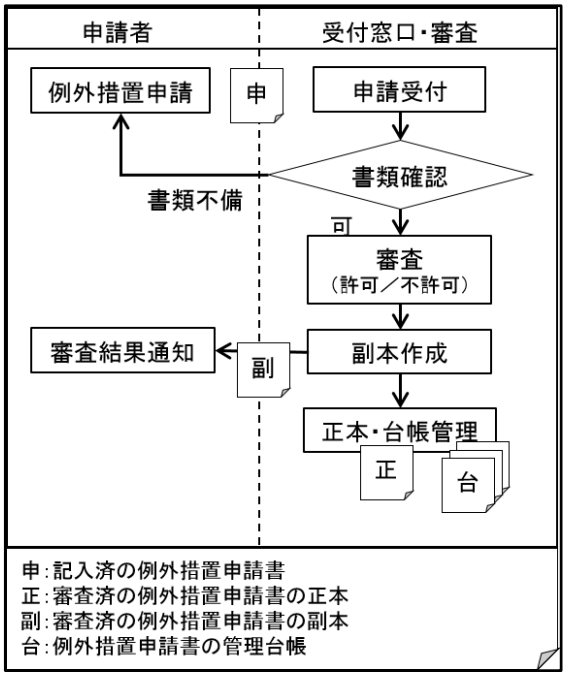

図 1　N社の例外措置の業務フロー例
Figure 1　A flow example of exceptional rules.(N CORP.)

これらの事例に対し，例外規定がない場合には，即時判断できないため処理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．

- 承認時間が限られている
- 他に選択肢がない
- 既に利用している，契約済みである
- 承認しなければ現場の実務・サービスが滞ってしまう

当該担当者の経験した例外規定をあてはめたケースでは，総じていつも直前になって相談してくる場合が多く，常に，迅速な対応が求められる．多くの場合，事実上認めざるを得ないと判断した場合でも，受付窓口の担当者としては，セキュリティインシデントへの不安感が残る．

では例外規定や措置の業務フローの見直しを検討するにあたり，他に参考になる事例があるのかどうか．その手掛かりを探るべく，まず情報システムを取り扱う組織が広く認証取得を受けている（あるいは試みている）ISMS での該当箇所について調べた．

2.1 ISMS(情報セキュリティマネジメントシステム)での例外規定

ISMS は，組織の意志決定に必要な管理体制（マネジメントの仕組み）が導入されていること，及び情報セキュリティのリスクを低減するためのコントロール（管理策）が適切に維持・管理されていることを目的とする[1][5].

ISMS を実践するための管理策に関する詳細なガイドとして，ISO/IEC27002:2013 がある．この中の１２章「運用のセキュリティ」では，情報処理設備の運用における管理目的及び管理策を定めている．さらに「12.1 運用の手順及び責任」に「情報処理設備の正確かつセキュリティを保った運用を確実にすること」を記述しており，「12.1.1」「12.1.2」ではそれぞれ操作手順・変更管理が記載されている．

操作手順の e) f)，ならびに変更管理の g) h)に例外への対応についての記載がある[3][4]．これによれば例外措置を認める場合は，例外規定として明確に規定等に定めるとともに，運用を変更する場合には変更管理を徹底することを示している．すなわち今回改正された ISO/IEC27002(2013)にもとづき ISMS 認証への新規もしくは更新認定を希望する組織は，例外規定の策定・実施が求められることにつながる．

しかし一方で ISMS では積極的に例外規定による運用を奨励しているわけではない．2013 年改訂では当該記載自体が実は“例外”として残されたものとされている．できる限り事前にあらゆる事象を想定して規定したうえで運用し，できる限り例外規定は少なくすることが望ましい．例外規定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 では個別具体的な指示や例示を記載しているわけではない．転じて，より具体的な規定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られる．

Vol.2015-DPS-164 No.7
Vol.2015-EIP-69 No.7
2015/9/11

「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，緊急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

2.2 官公庁での情報セキュリティ例外規定

そこで具体的な規定策定の事例として，官公庁や一部の企業で策定・実施を進めている「政府機関の情報セキュリティ対策のための統一管理基準」をとりあげる[7].

この統一基準は，内閣サイバーセキュリティセンター（NISC)が策定するにあたって開催した有識者会議に参画した，日本ヒューレットパッカード株式会社個人情報保護対策室長の佐藤慶浩氏がインシデントなどにおける例外規定を検討した．以下はこの統一基準における例外規定の在り方について示した，佐藤の資料の引用から一部加筆したものである[9].

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を遅れてしまうと，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．

ここでは，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ことも指摘している．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，事前に定められた処置とは異なる例外処置ができるようにすることも必要である．統一基準ではそのような例外処置についても管理策を講じることについて述べている[9].

さらに，政府においては，例外措置の手続きの流れ（図２に示す）や様式も定めている[8]．ここでのポイントは，例外措置は違反と抱き合わせた建てつけとなっていることである．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，ガバナンス構築としては，むしろ効果的である．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ようになる．

例外規定の策定は，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．

佐藤によれば，官公庁以外での「例外の想定」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．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[13][14]も同様に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，ほぼすべて導入しているものと考えられる．

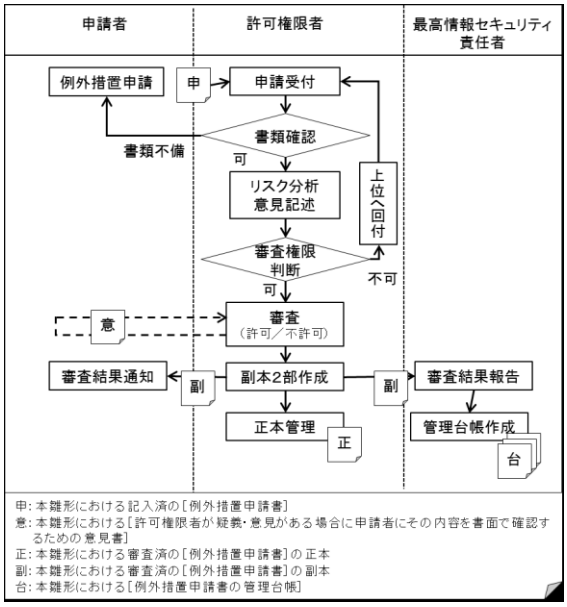

図 2　政府機関等での例外措置業務フロー[8]
Figure 2　A flow example of exceptional rules.(Govt)

なお佐藤はこの例外規定について，他に参照して提案・策定してきたわけではないとのことである．したがって先行事例など参考となる事例について，今後さらに調査していく必要がある．

2.3 海外での例外規定の事例

本稿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）」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，考え方を紹介する．

各項目と主な内容を表 1 に示す. 前項の統一基準と同様，通常規定では対処が難しい事象に対して例外規定を策定しているが，特徴として２点あげられる．

１つは通常規定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，例外規定を策定している点である．これにより例外規定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られる．

もう１つは例外規定を策定するにあたり，通常規定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[6]．例外規定の適用を申請するのであれば，申請した部署に対して説明責任を負わせることで，例外措置によって起こりうるリスクを理解させ，情報セキュリティの確保を図るものである．

さらに米国が政府向けに策定したガイドラインに，NIST SP 800 シリーズがある[11]．膨大な資料のためまだ十分に内容を把握しできていないが，今後調査を進めていく予定である．

表 1　例外処理におけるガイドラインと手順（抜粋）
Table 1　A Guideline and procedure in exceptional rules

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. 考察

２章の事例紹介でも触れているが，実際に情報セキュリティに関する内部規定を自社で策定する場合にあたり，この例外の取り扱いはリスク回避の意味も含め極めて重要と考える．

例外がない場合，通常規定に該当しないものは実施できないし，実施した場合は規定違反として罰則が伴う．いずれにしても健全な業務遂行ができなくなる．また通常規定を無視して，水面下で実施することも考えられる[12].
例えば私物スマホの業務利用を取り上げているが，これらは近年 IoT（Internet of Things：もののインターネット）や BYOD（Bring your own device：私的デバイス活用）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考えられる．また現場からのニーズがなければ（後述のボトムアップ型），経営側（後述のトップダウン型）から私物スマホの利用を検討するとは経験上考えにくいため，利用については現場からの要請が主であると考える．

この場合利用者側の立場で，業務でも私物スマホを利用した方が，仕事がしやすいと思ったとき，以下のような行動をとると考える[2].

(1)　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.

Vol.2015-DPS-164 No.7
Vol.2015-EIP-69 No.7
2015/9/11

(2) 関連する規定を管理している部門に相談し，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[12]. (2)は後述定義する「ボトムアップ型」例外申請と扱うことができる.

他方，申請窓口・承認者側としては申請を受けた時に，次の選択肢が考えられる.

① 拒否するか
② 無条件で許可するか
③ 条件付きで許可するか

ここで当該措置ができる例外規定がなければ，①しか選択できない．一方例外規定があるならば③になる．もともと②であれば，例外規定ではなく通常規定になっているはずである.

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）例外規定がなくとも，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例外規定もしくは通常規定を策定するといった具合である.

しかし時間に余裕がなく，喫緊の対応が要する場合において例外規定がないときは，現場担当者の判断でまず一時的措置をとり，後ほど周辺や上層へのエスカレーションする手続きになるものと考えられる.

次に心理面から考えたとき，原則と例外があると，利用者側としては逃げ道があるかもしれないといった一種の安心感がもたせる効果が考えられる．半面，承認者側としては，本当に認めてセキュリティ上に問題がないか，あるいは認めたことへの責任が重くなりはしないかといった不安感がでてくることも否定できない．なぜなら承認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を承認側に押し付けることが可能だからである．したがって例外を承認した側としては監査における“二重責任”に近い責任を負うことになる．承認側の判断が確立していない，もしくは承認者の裁量でブレが生じるようなことでは，情報セキュリティへの確保が難しく，承認者の精神的な負担も大きくなる可能性がある.

情報セキュリティのリスク管理については，規定に「通常（原則)」と「例外」があることが望ましく，原則のみの場合だと違反して罰則の対象となったり，水面下で無断に使用されたりすることが考える．また規定に盛り込まれていない，不測の事象に対してどのように規定で明記しているかで，上記の対応に差がつくことは容易に想定できるものと考えられる.

4. 例外規定の調査に向けて

そこで各組織で情報セキュリティに関わる「例外規定」の実態を収集するために，平成 27 年度の情報セキュリティ大学院大学原田研究室で実施するアンケートに本稿で述べた例外規定に関連する設問を盛り込む予定である．当研究室では例年日本国内のプライバシーマーク取得企業，ISMS 認証取得企業，BCMS 認証取得企業,官公庁，教育機関などから，ランダムに選んだ約 4,500 の情報セキュリティシステム担当者を対象とした「情報セキュリティ調査」を実施しているが今年度も 7 月配布・8 月回収を行い，10 月をめどに分析していく予定である.

当該アンケートで設問をたてるにあたり，例外規定については大きく「トップダウン的な例外規定」と「ボトムアップ的な例外規定」の２つに分けて定義した.

(1) トップダウン型例外規定：
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.

(2) ボトムアップ型例外規定：
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.

アンケートでは経営側・現場側どちらの立場から回答されるかを把握しつつ，特に現場側でボトムアップ的な例外規定の取扱いがなされているかどうかを，具体的な事象ごとに回答してもらえるよう工夫した.
設定した設問の主旨を以下に示す.

[Q1] 自社の情報セキュリティに関わる内部規定において「例外規定」（１頁用語参照）の項目がありますか.
[Q2] 例外規定は，自社全体での統一された内部規定のみですか，それとも現場組織ごとにも規定されていますか
[Q3] 例外規定を策定するにあたり，規定の策定と管理の事務処理をする部門は主にどこですか（複数回答可）
[Q4] 例外規定における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ますか（複数回答可）
[Q5] 内部規定に新規の例外規定を策定する場合，何を参考にしますか（すると想定していますか）
[Q6] 以下の具体的な業務上の事象において，例外規定はありますか
[Q7] 内部規定に例外規定がない事象で，数日中での一時的措置をとるとした場合，「最初」にどのような手段をとりますか（とると想定していますか）

[Q8] 例外規定の見直し頻度をお教えください.
[Q9] 具体的な目的・狙いにたいしてどのような効果があると，主観的に感じていますか

今後アンケートの結果を集計・分析することにより，組織が情報セキュリティの例外規定をどのように活用しているかを求めていく予定である.

5. まとめと今後について

本稿では，情報セキュリティにおける例外規定について実務や他の事例を挙げて，例外規定の必要性について述べてきた．そしてこれらの事例をもとに考察し，実際に現状を把握するために今後行うアンケート調査について説明した.

例外規定を策定する際には，予め通常規定からの逸脱を把握し，説明責任を課す事例がある一方，例外措置を実施する際は，違反と抱き合わせることで事後の責任所在を明確に与える事例もあった．政府機関統一基準における例外の取り扱いについては，実施例はあるものの，具体的にどのように機能しているのか，あるいは他の業種にも実際に導入しやすいものかどうか調査していく必要はあるのではないかと考える.

さらには 2013 年の ISMS 改正に例外事項が残されたことは，それぞれに情報セキュリティにおける例外規定・例外措置の必要性があるものと推定できる．ISMS の認定を受けている（受けようとしている）組織が例外規定をどの程度まで策定しているのかについても調べる価値があると考える.

今回アンケート項目を作成するにあたっては，これまでの実務経験を考慮して設問を設定しているが，アンケート調査・分析を進め,仮説の裏付けや見直しを早期に調整し，例外規定の統一的な策定の必要性や効果について探っていく予定である.

総じて，例外規定・例外措置が情報セキュリティマネジメントにどのように有効に活用していくべきかを今後も検討していきたいと考える.

謝辞 本調査を実施するにあたり，アンケートの封入，データ入力に多大な協力を頂いた，複数の神奈川県下の養護学校・支援学校の皆様に感謝します．さらに温かい指導を頂いた情報セキュリティ大学院の教授の皆様，議論頂いた原田研究室の研究員皆様，郵便の事務にご協力頂いた大学事務の皆様に感謝します.

参考文献

1) ISO/IEC27001:2013（JIS Q 27001:2014）,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
2) 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)
3) ISO/IEC27002:2013
4) 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)
5) 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)
6) 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.463/2015.3
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」,
http://www.nisc.go.jp/active/general/pdf/K304-111C.pdf
8) 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,
http://www.nisc.go.jp/active/general/kijun_man_index.htm
9) 佐藤慶浩: 企業における情報セキュリティ対策の実務, 情報セキュリティ大学院大学講義資料,
http://yosihiro.com/speech/presenter/2014-11-29b/data/resources/2014-11-29b-enPit.pdf
10) 内閣サイバーセキュリティセンター: 政府機関の情報セキュリティ対策のための統一管理基準（平成 26 年度版）解説書「1.2.1.3 違反と例外措置」,
http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf
11) NIST SP800・FIPS,
http://csrc.nist.gov/publications/PubsSPs.html
http://csrc.nist.gov/publications/PubsFIPS.html
12) 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, , IT Media ニュース“シャドーIT”との向き合い方 2015.1,
http://www.itmedia.co.jp/news/articles/1501/27/news045.html
13) 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, https://www.fisc.or.jp/guideline/
14) 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）(2014),
http://www.tokiorisk.co.jp/risk_info/up_file/200402041.pdf