Vol.2016-EIP-71 No.6
2016/2/19

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

村﨑康博[†1]　　原田要之助[†1]

内閣サイバーセキュリティセンター(NISC)から発表されている「政府機関の情報セキュリティ対策のための統一基準群」の規定には，情報セキュリティに関わる内部規定として「例外措置」の申請・審査・承認のための手順と担当者を含めるよう定めている．一方，民間組織において使用される規定では，例外措置が規定され適用されているかは不明である．さらに官公庁でも例外措置条項をそのまま適用しているのかは明確でない．

本稿では各組織における例外措置の策定状況と認知度についてアンケートによる調査を実施し，その発見事項から今後の研究課題を考察した．

Survey on Exception Measures of Information Security policy in Organization.

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

The Rule of "Management Standards for Information Security Measures for the Central Government Computer Systems" announced by the National Information Security Center (NISC)" included a procedure and person in charge for application, examination, the approval of "exception measures" as an internal rule about information security. On the other hand, in the rule to be used in private organization, whether exception measures are prescribed or applied are unknown. Furthermore, even in the government offices, the clause of “exception measures”has been applied is not clear.

In this study, a survey by the questionnaire about the development situation and the recognition of the “exception measures” in each organization is carried out, and considered the finding issues for a future research theme

1. はじめに

今日の情報セキュリティ対策においては，技術的・システム的な対策や人材育成・確保や啓もう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などの組織的な対応が求められている．

その中で，情報セキュリティインシデント(以下，インシデント)に備え，事前に規定を策定し迅速な措置の実施に備えることは，どの企業や官公庁など(以下，組織と表す)においても必須施策のひとつと考えられる．

また，一部の組織では，想定できなかった状況にも対応できるように事前に“例外規定”を策定し，例外措置を実施することで継続的な業務管理を維持しようとしている．

各組織における例外措置の策定状況と認知度の実態を把握することは，情報セキュリティ対策を考える上で重要な要素の1つである．そこで，本稿では，現状を確認するためにアンケートによる調査を実施し，結果分析を行った．さらに，得られた結果から，今後の課題について考察する[1][2].

2. 情報セキュリティポリシーにおける例外規定

2.1 例外規定を策定する意義

情報セキュリティの組織的な対策の１つに，内部規定等による業務管理・運用体制の構築があげられる．これは，情報セキュリティポリシー（基本方針）を策定し，それに基づいてスタンダード（対策基準）として規定・ルールを策定し，さらに具体的に運用していくためのプロシージャー（実施手順）を設定していくものである．

対策をとるべき事象が法的にある程度決められている場合，通常規定から逸脱する行為については事前に想定できるため，業務の継続化を維持するための例外措置は，事前に例外規定に策定することができる．

例えば，特許出願の場合には，いち早く研究成果を学会発表するために，出願手続きが遅延することがあらかじめ“想定”される．したがって特許法では「発明の新

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

規性喪失の例外規定の適用（３０条)」，により例外措置の事後対応を事前計画で想定した範囲内だけで実施できる．したがって通常・例外のいずれからも逸脱した措置について，法的には認められず却下されることになる．

一方，情報セキュリティの場合においては，情報セキュリティインシデントが予測不可能な状況となることもあるので，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，想定外の状況への柔軟な対応を難しくする場合がある．

したがって，情報セキュリティの場合の例外規定には以下の要素が求められる [3].

- 原則は，計画準備段階で策定した手順に従い，実際のインシデント発生時に対応する
- 計画準備段階での手順がインシデントの実情に沿わないときには，手順以外の方法で対応できるための手続きを予め準備する
- また，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を可能にする
- これらの例外処置をも管理する対象に含める
- 例外措置と罰則とを事前に対応づけている

例外措置を設けることによって，実際には違反の結果，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，ガバナンス構築としては，むしろ効果的と考えられている．また例外措置の記録は，以後のリスク管理での見直しに役立てることができるようになる [4].

2.2 本稿での例外規定の定義

一方、情報セキュリティにおける例外規定は，最初から全ての事象に網羅的に対処できる措置手順を準備した上で運用をはじめるわけではない．そしてそれは甚大災害やサイバーテロなどの非常時での事象ばかりでなく，日常業務に支障がないものの通常ルールから逸脱した想定外の新たな事象に対しても例外措置を講じることが起こりうる．

日常業務においても”想定外の事象が起こりうる”ことを“想定内”として意識し，非常時・通常時問わず，逸脱する運用をせざるを得ない事象に対して例外規定を用いて措置を講じ、措置の時点で規定がない場合は事後に規定策定への手続きを進めるべきであると考える．

2.3 例外規定策定の事例と動向

情報セキュリティ分野における国内の外規定の策定を明確に示しているのが，内閣サイバーセキュリティセンター（以下，NISC）の「政府機関の情報セキュリティ対策のための統一基準群（以下，統一基準群）」である[5]. これは官公庁向けに，情報セキュリティに関わる内部規定において「例外措置」の申請・審査・承認のための手順と担当者を含めている．例外措置の手続きの流れを図１に示す．さらに，このための様式も定められている[6].

また，ISMS[7][8]においては，ISO/IEC27002:2013 の１２章「運用のセキュリティ」において，情報処理設備の運用における管理目的及び管理策操作手順に，例外への対応についての記載がある[9][10]．具体的には，例外措置を認める場合には，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述べている．すなわち，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・実施が求められていると言えよう．

また，民間組織においては，金融機関など一部の組織では統一基準群を参考にしているものの[11][12]，例外規定についてどの程度普及しているかはこれまで不明であった. さらに，官公庁においても，統一基準群の例外規定をどのように適用しているのかについても不明であった．

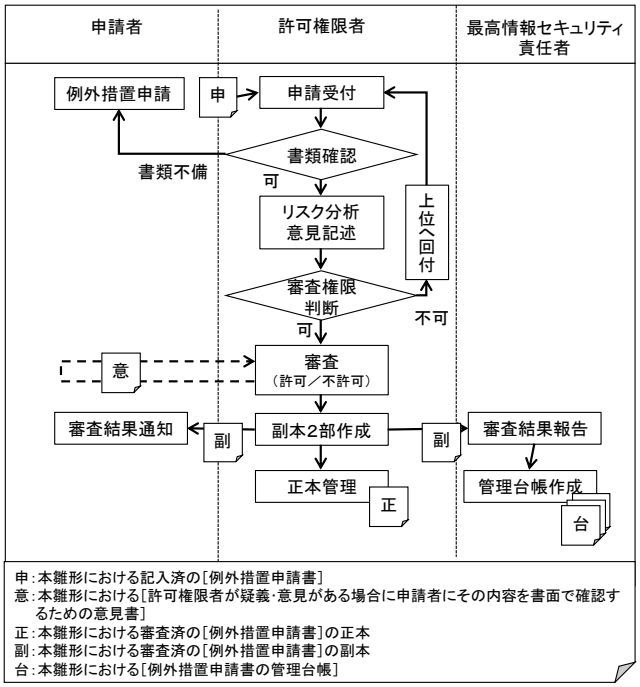

図 1 政府機関等での例外措置業務フロー

3. 例外規定のアンケート調査に向けて

そこで前述の通り，例外規定の策定状況の実態を把握するために，官公庁（政府機関・自治体など），企業，大学などの組織に対してアンケートによる調査を実施した[1].

3.1 仮定の設定

まず，アンケート調査を実施する上で，組織における例外規定の普及に向けた取組みへの理想と実際から，仮定をたてた．これを表１に示す．

表１　組織の例外規定に関する仮定

（仮定 1）	例外規定の普及は分野ごとにばらつきがあるが，少なくとも官公庁では，実際に業務として例外措置を行っている.
（仮定 2）	内部規定にない例外措置をとるとき，緊急性を要する場合は，直接経営判断を優先するだけでなく，現場責任者の判断でも措置ができるようになっている.

（仮定 3）	新規に例外規定を策定する場合，これまでの事例や外部からのものを参考にしている．
（仮定 4）	例外規定の策定は，情報システム部門など中央で統括しながら作成するのか，あるいは各組織の権限内で作成するのかは，組織によって違いがある．
（仮定 5）	例外規定の業務内容の見直しは短い期間で定期的に行われる．
（仮定 6）	例外規定では例外措置のための実施手順を記載し，特に罰則とセットにしている．

3.2 アンケート設問作成においての事前準備

当該アンケートで設問をたてるにあたって，仮定をもとに，回答者が経営側・現場側どちらでも回答できるよう配慮した．具体的には，トップダウン型の包括的な設問，ボトムアップ型の具体事例に関する設問を盛り込む工夫をした．

4. アンケート調査の実施

4.1 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「例外規定」の実態を把握するために，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したアンケートの一部（第 3 章）として，例外規定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[1][2].

4.2 アンケート設問

3.1 節の表 1 の仮定に基づいて作成したアンケートの設問を表 2 に示す．本稿では全アンケート設問のうち「設問 1 4」から「設問 2 3」までが対象となる．なお，本稿ではこのうちの「設問 1 4」および「設問 1 7」から「設問 2 2」までを分析に使用している[1].

5 章では，表 1 の仮定の順に関連する設問について分析して考察する．

表 2　アンケート設問

［設問 14］	情報セキュリティに関わる内部規定全般において「例外規定」の項目の有無
［設問 15］	例外規定が明記されていない事象（障害，事故・事件，災害など）に対して，一時的に例外措置した経験の有無
［設問 16］	具体的な業務上の事象において，例外規定の有無
［設問 17］	内部規定に例外規定がない事象で緊急を要する事態での一時的措置に，最初にとる手段
［設問 18］	新規の例外規定を策定する場合の参考元
［設問 19］	例外規定の策定と管理の事務処理する主体部署
［設問 20］	例外規定が，組織全体での統一規定か，現場組織ごとの規定か
［設問 21］	例外規定に記載された例外措置の手続き内容
［設問 22］	例外規定の見直し頻度
［設問 23］	具体的な効果についての主観的評価

5. アンケート分析結果

5.1 仮定１：

「例外規定の普及は分野ごとにばらつきがあるが，少なくとも官公庁では，実際に業務として例外措置を行っている．」

設問１４の結果を図２に示す．本設問では内部規定全般において「例外規定」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／一部例外規定に内部規定にある」割合と，赤色の「内部規定にない」割合が同じ（４２%）であった．

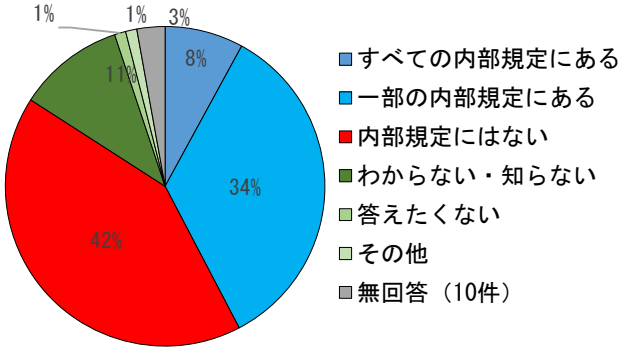

図２　情報セキュリティに関わる内部規定全般において「例外規定」の項目の有無（択一）

また，業種別 [1][2]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）」それぞれのクロス分析の結果を図３に示す．同図より「情報通信業」と「サービス業」では５０%が，青色系の「すべて／一部例外規定に内部規定にある」ことが分かる．

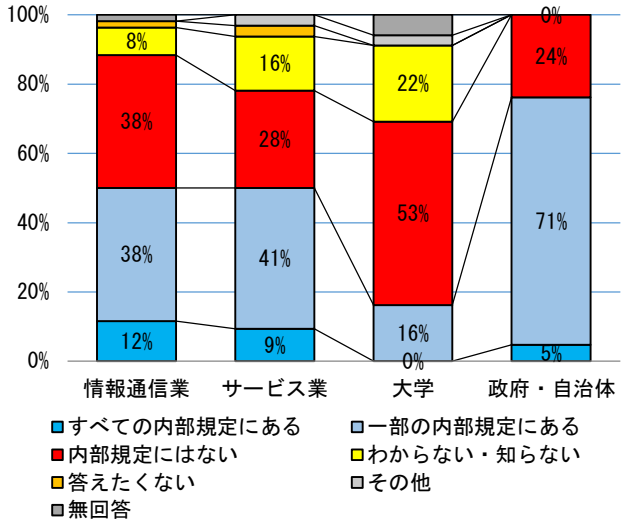

図３　情報セキュリティに関わる内部規定全般での「例外規定」の項目の有無（業種別，択一）

一方，公務（政府・自治体）では赤色の「内部規定にはない」が２４％あり，「大学」では半数以上（５３％）におよんでいる．

これらから，仮定１については，例外規定について策定の有無が同程度であることから，十分に普及しているものとは言えない．しかし「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る．公務においても，政府・官庁では統一基準群によって例外規定を策定して普及していることを考慮すれば，自治体への普及が今後の課題になると考えられる．

5.2 仮定２：

「内部規定にない例外措置をとるとき，緊急性を要する場合は，直接経営判断を優先するだけでなく，現場責任者の判断でも措置ができるようになっている．」

仮定２に対応する設問１７の結果を図４に示す．本設問は，内部規定に例外規定がない事象で緊急を要する事態において一時的措置をとる場合，「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．同図からは，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「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．

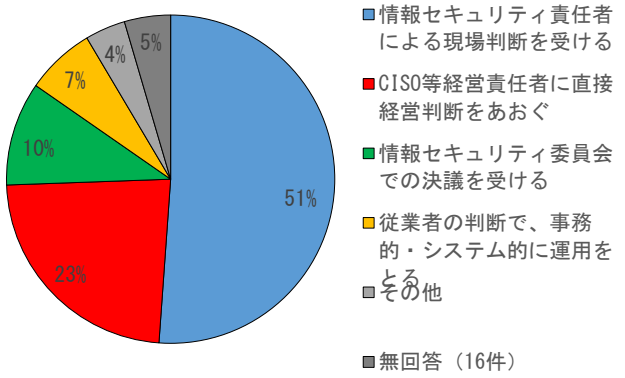

図４　内部規定に例外規定がない事象で緊急を要する事態において一時的措置をとる場合，「最初」にとる手段

以上からは，仮定２に対する結果として，緊急性を要する例外措置は，画一的にトップダウン型ばかりだけではなく，まずは「現場組織の判断」が優勢されるボトムアップ型で実施されている組織が多いこと分かる．

5.3 仮定３：

「新規に例外規定を策定する場合，これまでの事例や外部からのものを参考にしている．」

仮定３に対応する設問１８の結果を図５に示す．本設問は，内部規定に新規の例外規定を策定する場合，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，例外規定は赤色の「他社事例」や「政府官庁の管理基準」をもとに策定されることが多いことが分かる．

さらに公務（政府・自治体）についての内訳を図６に示す．同図から赤色の「政府・官公庁の管理基準」が他に比べ多く，統一基準群を基に例外規定が策定され，比較的普及しているものとみられる．

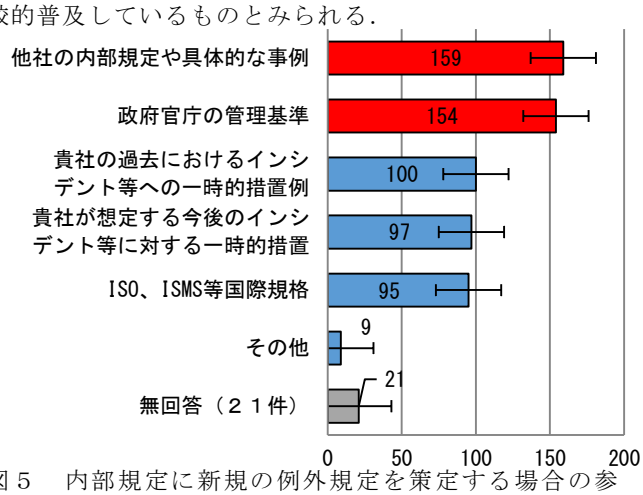

図５　内部規定に新規の例外規定を策定する場合の参考元（複数選択）

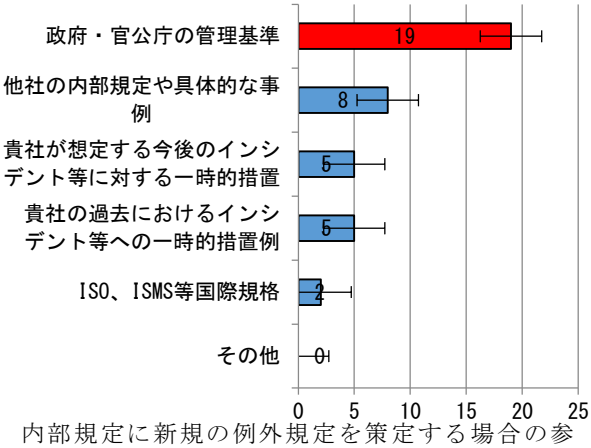

図６　内部規定に新規の例外規定を策定する場合の参考元（政府・自治体）

これらにより，仮定３に対する結果として，例外規定を作成する場合，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．また統一基準群を参考にする組織も多く，例外規定を新規策定する際での参考となっていることが分かる．

5.4 仮定４：

「例外規定の策定は，情報システム部門など中央で統括しながら作成するのか，あるいは各組織の権限内で作成するのかは，組織によって違いがある．」

仮定４に対応する設問２０の結果を図７に示す．本設問は，例外規定は組織全体での統一された内部規定のみか，それとも現場組織ごとにも規定されているかをたずねた．同図から，例外規定は青色の「統一管理基準のみ」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．

次に，設問１９の結果を図８に示す．本設問は，例外規定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署はどこであるかをたずねている．同図からは，例外規定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．

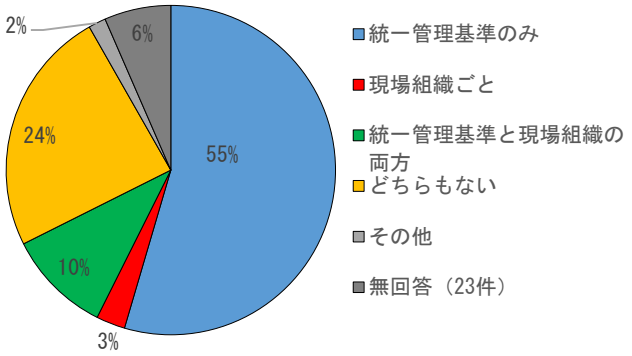

図７　例外規定は組織全体で統一されたものか，現場組織ごとにも規定されたものか（択一）

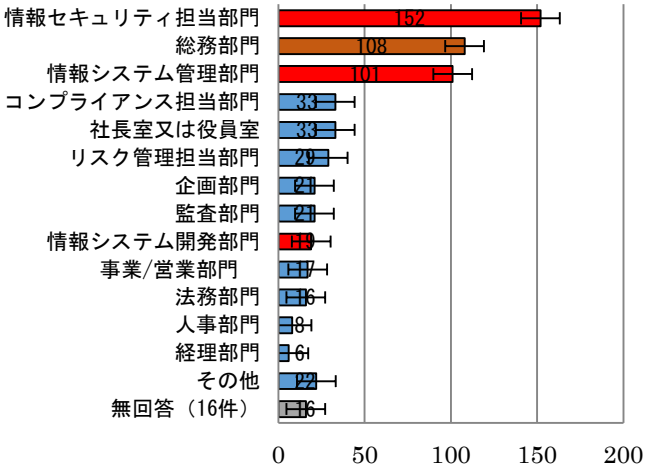

図８　例外規定を策定するにあたり，規程の策定と管理の事務処理をする主体部署

すなわち，仮定４に対応する「設問２０」ならびに「設問１７」「設問１９」からは，多くの組織が例外規定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．例外規定については，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，情報セキュリティや情報システムなどの IT 関連部局で策定し，運用・管理まで手掛けざるを得ない現状であると考えられる．

5.5 仮定５：

「例外規定の業務内容の見直しは短い期間で定期的に行われる．」

仮定５に対応する「設問２２」の結果を図９に示す．本設問は，例外規定の見直しの頻度についてたずねている．同図からは，例外規定の見直し頻度は，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．

仮定５に対する結果として，組織は例外規定について，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ことが分かる．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．

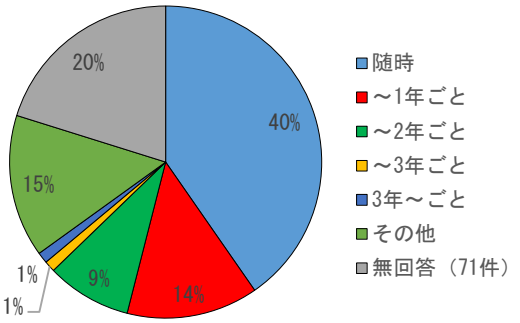

図９　例外規定の見直し頻度（択一）

5.6 仮定６

「例外規定では例外措置のための実施手順を記載し，特に罰則とセットにしている．」

仮定６に対応する設問２１の結果を図１０に示す．本設問は，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るかをたずねた．同図からは，赤色の「指定書式の申請書」，「運用・管理指導（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」比較的少ないことが分かった．

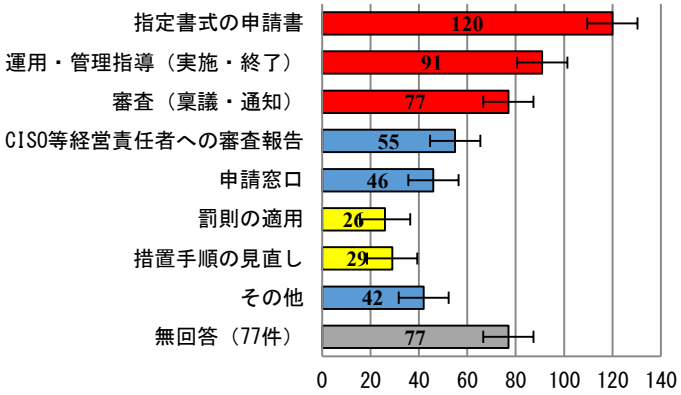

図１０例外規定における例外措置の業務に盛り込まれる手続き（複数選択可）

仮定６に対する結果については，統一基準群で推奨している罰則の適用が少ないことから，通常規定や例外規定への違反に抑止力が乏しく，情報セキュリティへの管理体制に影響がでるおそれがあることが分かった．また例外規定を策定している組織では図１のような業務フローが整備されていると考えられる．

6. 考察

各仮定に対する考察を受けて，本稿では，以下の点が考えられる．

まず，例外規定については体系的に「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

分けられると考える（表３）.

表３　例外規定のタイプ

	タイプ	特徴
1	トップダウン型	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	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.

本アンケートの「設問１７」と「設問２０」の結果から，多くの組織においてトップダウン型の規定策定がされている. すなわち部署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策定・措置されている．また，例外措置の策定・管理は，情報セキュリティや情報システムに関わる部署が多く，現場からの策定は少ないことからも，同じくトップダウン型の策定・運用・管理となっていると考えられる.

次に，

“実際に措置をすることが少ない”

“見直し頻度もその都度”

“例外規定はないが一時的に例外措置を実施した”

組織が多いことから，例外措置は事象が起きたその都度に対応し，その後必要に応じて規定として策定・見直ししているとみられる．したがって一時しのぎで，まず例外措置を行い，次回同じ事象や全く異なる事象が起きた時の例外措置をとれない組織が残されていると考えられる.

そして，情報セキュリティに関する内部規定への例外措置の規定化については，策定している組織と未策定の組織とで二極化しており，今後，例外措置を策定していない組織への，普及への働きかけが求められるものと考えられる.

7. まとめと今後に向けて

本稿では主に統一基準群を参考に，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取扱いやその効果などを調査するために，アンケート調査を実施し分析を進めた.

本アンケートを通じて，例外規定策定の現状を知ることは，情報セキュリティにおける組織ガバナンスの実態の一部を得ることにつながるものと考える.

この例外措置の規定策定は政府期間のみならず，情報を扱う全ての組織で必須であると考える. 一方で，その策定への普及は十分に進んでおらず，組織は，どのように盛り込んでいくべきか，試行錯誤している様子がうかがえる.

そして今後，重要な要素となるのは，“通常基準との逸脱程度と例外措置との関係”および“例外規定の策定に伴う例外措置への評価基準”と考える. 今回のアンケート結果を踏まえ，今後はこの2つの要素について別途仮定をたてて，アンケートの詳細な分析を進めていく予定である. そして社会全体や分野ごと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.

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] 情報セキュリティ大学院大学原田研究室ホームページ http://lab.iisec.ac.jp/~harada_lab/survey.html
[2] 村崎ほか,“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，2B3-3.
[3] 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
[4] 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　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
[5] 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） http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf
[6] 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
[7] 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
[8] 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)
[9] ISO/IEC27002:2013
[10] 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)
[11] 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/
[12] 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