Vol.2016-DPS-168 No.11
Vol.2016-SPT-21 No.11
Vol.2016-EIP-74 No.11
2016/11/18

組織の情報セキュリティ向上の取組みについて -CSIRT と ISMS の類似と相違に着目した考察-

副島恵子[†1]　原田要之助[†1]

概要：大規模な個人情報漏洩事件などが頻発する昨今，情報セキュリティインシデント（以下，インシデントという）対応を行う CSIRT（Computer Security Incident Response Team）が注目を集めている．本研究では，CSIRT 活動と情報セキュリティマネジメントとの関係を明らかにし，組織の情報セキュリティ向上に寄与する CSIRT 活動のあり方について考察する．

キーワード：インシデント対応，CSIRT，ISMS，PDCA，OODA

Efforts of information security improvement of the organization -A study on the similarity and difference of CSIRT and ISMS-

KEIKO SOEJIMA[†1]　YONOSUKE HARADA[†1]

Abstract: CSIRT (Computer Security Incident Response Team) has attracted attention, as large-scale personal information leakage incidents occur frequently these days. In this study, clarify the relationship between the CSIRT activities and information security management, and consider the role of CSIRT activities to improve the information security of the organization.

Keywords: Incident Response, CSIRT, ISMS, PDCA, OODA

1. はじめに

情報システムが組織の事業活動に不可欠なものとなり，コンピュータやインターネットは我々の生活に密接に関わっている．近年では，ビッグデータ，IoT，クラウドなどによって，あらゆる情報が今までと異なる方法で扱われるようになった．個人情報に代表される機密性の高い情報が，膨大に扱われるようになり，これらを狙ったサイバー攻撃も増大・悪質化している．

サイバー攻撃の悪質化とともに，インシデントの発生がもたらす被害は，甚大化している．インシデントが組織の事業活動や社会に与えるインパクトは以前にも増して大きくなっているが，大規模なインシデントは後を絶たない．

インシデントの発生は，業務の中断や顧客離れなど組織経営に重大な影響を及ぼす．一方で IT 技術や攻撃手法の高度化によって，インシデントの対応は複雑化している．

本研究では，インシデントの対応に着目し，定常的な情報セキュリティマネジメント活動と緊急時対応型の CSIRT 活動を関連付けた統合型セキュリティマネジメントについて考察する．また，CSIRT 活動を組織の情報セキュリティ向上に繋げるしくみについて検討する．なお，本稿でのインシデントとは，内部不正による情報漏洩やサイバー攻撃による被害などを指す．

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

2. インシデントに対する組織の取り組み

2.1 インシデントの影響

インシデントの発生は，事業の停止などの直接的な影響だけにとどまらない．その影響が経営的な問題となり，顧客離れや株価の下落など大きなビジネスリスクにつながることがある．

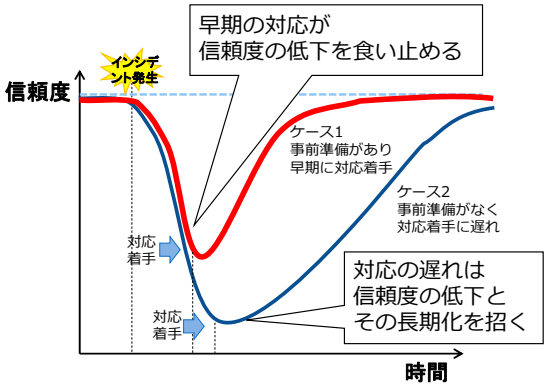

図 1　信頼度低下の時間経過のイメージ

インシデントによる組織の信頼度の低下と対応の実施タイミングの関係を図 1 に示す．図 1 は，インシデントの発生後，最初は緩やかな信頼度の低下が，事件が報道されるにつれて急激にすすむ様子を表している．信頼度の低下が緩やかにすすんでいる早期の段階で適切な対応を行えば，信頼度の低下を止められる．対応が遅くなると，事業活動にとって致命的な信頼度低下や長期にわたる信頼度低下に

Vol.2016-DPS-168 No.11
Vol.2016-SPT-21 No.11
Vol.2016-EIP-74 No.11
2016/11/18

つながる.

2.2 インシデントへの対応と CSIRT

インシデントへの対応を適切に行うために，組織が取り組むべき事項を CSIRT（Computer Security Incident Response Team）の活動を一例として考える.

CSIRT がインシデントに対して行う活動全般は，「インシデントマネジメント」と呼ばれる [1]. インシデントマネジメントの要素を図 2 に示す. 図 2 のインシデントマネジメントの要素は,「インシデントハンドリング」,「脆弱性対応」,「事象分析」,「普及啓発」,「注意喚起」,「その他の関連業務」に分けられる. インシデントの発生から解決までの一連の処置にあたるインシデントハンドリング機能を図 2 の左側に示す. 図 2 のインシデントハンドリングの機能は,「検知・連絡受付」,「トリアージ」,「インシデントレスポンス」,「報告・情報公開」から成り立っている.

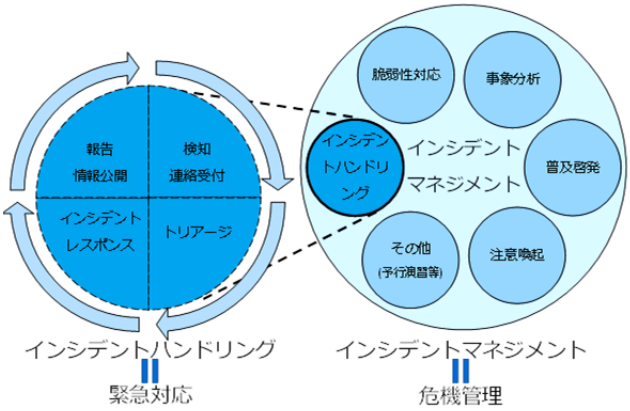

図 2　インシデントマネジメントと
インシデントハンドリング a)

2.3 CSIRT の役割と活動

インシデントが頻発・大規模化する中で，インシデントの影響を最小限に抑えるための組織・機能が CSIRT である. CSIRT は，インシデントの対応を行う専門チームで，その役割はしばしば「消防」にたとえられる.

インシデント時のインシデントハンドリングの流れを図 3 に示す. 図 3 の「検知・連絡受付」では，インシデントに関して社内やお客さまなどの社外から寄せられた情報を CSIRT が一元的に集約する. 図 3 の「トリアージ」では，集められた情報について対応の優先順位付けや対応方針の策定を CSIRT が行う. 図 3 の「インシデントレスポンス」では， CSIRT はトリアージの結果に基づいて，対応実施部門への指示や支援を行う. 実際の対応を CSIRT 自身が行う場合や，対応実施部門に対して助言等の支援を CSIRT が行う場合など，様々なケースがある.

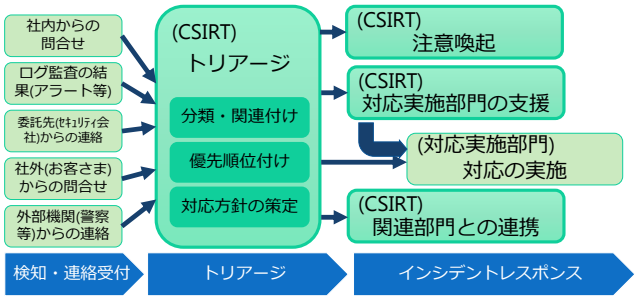

図 3　インシデントハンドリングの流れb)

図 3 からは，インシデントの対応が多岐にわたる複雑な取り組みであることがわかる. また，検知・連絡フェーズやインシデントレスポンスフェーズにみられるように，インシデントの対応は，社内外の多くの組織と連携して行われている.

インシデンへの対応は，複雑で多岐にわたっている. CSIRT が司令塔となって動くことで，インシデントへの迅速かつ適切な対応が可能になる.

3. 組織の情報セキュリティの体制

本章では，組織の情報セキュリティの体制について考察する.

3.1 ISMS によるマネジメントシステム

ISO/IEC 27001:2005 では，表 1 に示す「Plan（計画）」,「Do（実行）」,「Check（点検）」,「Act（処置）」のプロセスを繰り返すことで情報セキュリティの確立・維持・向上を目指す PDCA サイクルのモデルが採用された. PDCA サイクルは, アメリカの統計数学者 Edwards Deming が品質管理の手法として提唱し，今ではマネジメントシステムとして広く定着している.

表 1　PDCA サイクルの各プロセス

Plan	目標を立て，達成のための計画を立てる
Do	計画にもとづいて業務を実行する
Check	目標が達成されているか業務を確認・評価する
Act	確認・評価結果をもとに業務を改善する

マネジメントシステムとは，方針，目的及びその目的を達成するためのプロセスを確立するための相互に関連・作用する一連の要素と JIS Q 27000:2014 で定義されている. ISMS は，情報セキュリティを確保・維持するための組織的・体系的な取り組みである. 組織的，技術的，物理的，人的な対策を組み合わせて情報セキュリティを実現し，継続的な改善によって向上していく.

ISMS での情報セキュリティの取り組みの実施事項には，図 4 のように管理面の実施事項と現場の実施事項がある

a) JPCERT/CC の図[1]をもとに一部修正

b) JPCERT/CC の図[1]をもとに加筆・修正

Vol.2016-DPS-168 No.11
Vol.2016-SPT-21 No.11
Vol.2016-EIP-74 No.11
2016/11/18

と考えられる．

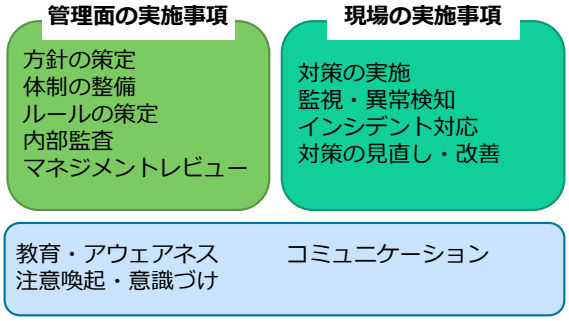

図 4　ISMS の取り組みの実施事項

管理面の実施事項は，現場の業務と異なる ISMS 特有のものが多い．組織が ISMS ベースで情報セキュリティに取り組む場合，ISMS 特有の実施事項を既存の会議体などを活用せずに新たな仕組みによって実現する傾向にあるように思われる．結果として，情報セキュリティの取り組みは管理面重視となる．そのため，現場の業務と直結しない仕組みが ISMS によって作られたと従業員に受け取られることが少なくない．情報セキュリティは，業務量の増加を招く大変な取り組みであるという負担感が生じ，現場が情報セキュリティの実施に抵抗感を抱く一因になっていると考えられる．ISMS ベースの取り組みでは，現場との距離感が問題である．

3.2 CSIRT の活動と OODA ループ

サイバー攻撃の巧妙化を背景に「総務省における情報セキュリティ政策の推進に関する提言」が 2013 年に公表された．この提言では，変化の激しいサイバーリスクに対して従来の PDCA 的アプローチでは対応に遅れが出ることが指摘され，図 5 に示す OODA ループによる動的防御プロセス連携が推奨されている．

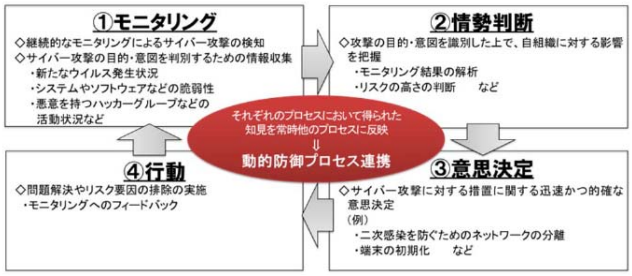

図 5　動的防御プロセス連携[2]

米空軍のパイロットであった John Boyd によって提唱された OODA ループは，「Observe（観測）」，「Orient（情勢判断）」，「Decide（意思決定）」，「Act（行動）」の素早い繰り返しによる意思決定によって生存率があがるという考え方である．OODA ループの考え方は，サイバー攻撃に対抗し迅速かつ的確な判断が求められる CSIRT の活動に適している．一方，OODA ループは「O」にコストがかかるため，すべての情報セキュリティ対策を網羅的に対応するのには適していない．

インシデントへの対応の各フェーズにおける実施事項と対応者を図 6 に示す．

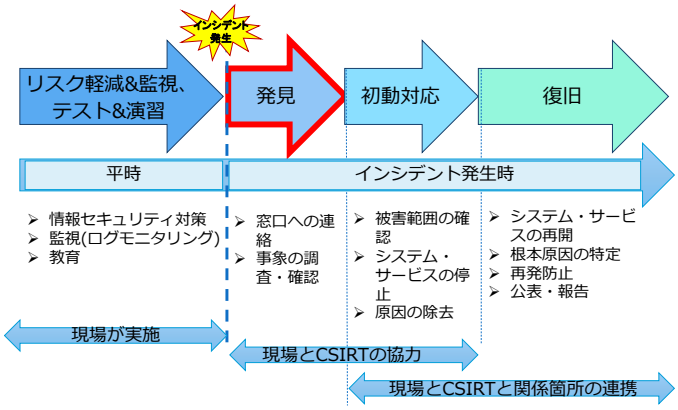

図 6　各フェーズの対応者と実施事項c)

図 6 に示すとおり，現場では平時から情報セキュリティ対策を実施し，インシデントの兆候を発見するための監視などを実施している．現場は，発見した事象を CSIRT に報告する．初動対応フェーズにおける被害範囲の確認や原因除去，復旧フェーズにおける根本原因の特定や再発防止など，現場と CSIRT が協力してインシデントへの対応にあたる．以下，発見から再発防止までの一連の対応をインシデント対応とよぶ．

このように CSIRT の活動は，3.1 節で述べた情報セキュリティの取り組みにおける現場の実施事項と密接にかかわっている．インシデント対応をきっかけとした全社を攻撃対象とするような脅威に対する対策は，短期間に全社に展開する必要がある．現場の実施事項は，CSIRT 活動とともに OODA ループで扱うのが望ましいと考えられる．

OODA ループとマネジメントシステムの PDCA サイクルの関係をみると，図 7 のように，日常を扱う長期の流れが PDCA サイクルであり，緊急時の短期の速い回転が OODA ループと考えることができる．CSIRT と現場における OODA ループの繰り返しによって，組織全体の情報セキュリティが向上することが期待される．

c) ISO/IEC 27031:2011 の図をもとに加筆・修正

Vol.2016-DPS-168 No.11
Vol.2016-SPT-21 No.11
Vol.2016-EIP-74 No.11
2016/11/18

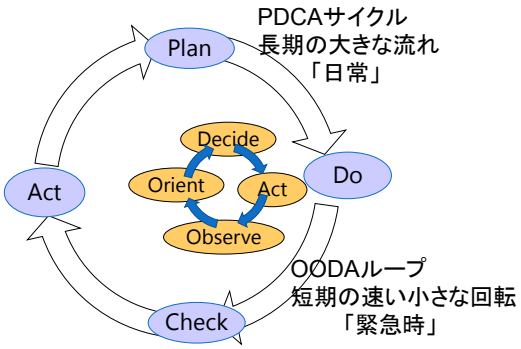

図 7　PDCA サイクルと OODA ループ

4. 組織の情報セキュリティの取り組みの今後

ISMS での情報セキュリティの取り組みは，基本方針の策定，リスクアセスメントによる情報セキュリティ対策の決定など理論的で長期的な取り組みのため，捉えづらい側面がある．特にこれから情報セキュリティに本格的に取り組もうとする組織にとって，ISMS での取り組みはハードルが高いと思われる．一方，CSIRT の整備から始める OODA ループによる現場の情報セキュリティ強化は，短期間のループであることから比較的取り組みやすいと考えられる．

今後，現場の実施事項を中心とした情報セキュリティの取り組みが増加するとして，どのような課題があるか考察する．

4.1 CSIRT の役割・機能

CSIRT の活動には教育・啓蒙活動も含まれている．実際にインシデントの対応にあたっている CSIRT による教育・啓蒙活動は，従来からあるテキストベースのセキュリティ教育と比べ，より身近で現実感のあるものとして受け止められる可能性が高い．現場を中心とした情報セキュリティの取り組みは，わかりやすく，説得力があり，素早い改善が可能になる．このようにみていくと ISMS なしでも組織の情報セキュリティが十分確保できるように思われる．

しかし，情報セキュリティに対する組織の考え方や方向性を示した基本方針の策定は，組織として取り組むべき事項であり現場での実施は適当とは言えない．また，内部監査やマネジメントレビューなどは，情報セキュリティの取り組み全般を見渡して組織全体で長期的に改善しながら取り組むべき事項である．

では，これらの役割・機能を CSIRT が担うことができるかであるが，それには以下のような問題があると想定される．CSIRT の役割・機能は，これらの問題を考慮した上で決定すべきである．

- 管理面の実施事項と現場の実施事項は要求されるスピード感など特性が異なっている
- CSIRT の役割・機能が肥大化すると，業務量が必要以上に増加する
- CSIRT は緊急性の高い業務に追われており，定常的な日常の業務に手が回らない

4.2 従業員との関係

従業員からの情報は，図 6 の発見フェーズにおいて CSIRT がインシデントの兆候をつかみ適切な対応を行うために，非常に重要である．特にファイアウォールや IDS など既存のセキュリティ機器で検知や防御ができなかった攻撃の場合，従業員が異常に気づき CSIRT に報告することが発見の第一歩になる．

従業員が気づいた異常を速やかに CSIRT に報告するにあたっての，心理的ハードルについて考える．

従来の ISMS での管理は，策定されたルールに基づいた静的な情報セキュリティ対策の実施であることから，ルールの違反や逸脱を許さない風潮がある．背景として，品質管理の手法として生まれた PDCA サイクルの適用方法に誤解があったのではないかと考える．「C」がルール違反のあぶり出しや違反の原因調査中心となり，ルール重視で現場の業務に対する自由度がない仕組みに陥っていた恐れがある．その結果，ISMS による管理に対して警戒心を抱く従業員が少なくない状態となっている．

従業員の心理的ハードルを解消し，気づいた異常が報告されるようにするために，従業員が相談しやすい空気を作ることが CSIRT に求められる．異常の検知時やインシデント発生時には，問題の解消や被害の最小化に努め，原因調査や犯人探しを優先しすぎないことが重要である．また，普段から従業員と CSIRT の間でコミュニケーションのパイプをもち，信頼関係を築くことも大事である．

5. 情報セキュリティの取り組みパターンの提案

現場の実施事項を中心とした情報セキュリティの取り組みのパターンを検討する．パターンでは，対策を実施する「現場」を情報システム部門とし，マネジメント部門，情報システム部門，CSIRT の役割を以下のように想定する．

- マネジメント部門：基本方針の策定，体制の整備，内部監査，マネジメントレビューなどを行う．
- 情報システム部門：社内の情報システムの導入・運用を行い，対策を実施する．ITIL（Information Technology Infrastructure Library）のサービスマネジメントの活動全般を扱う．
- CSIRT：インシデント対応を行い，対策の見直し・改善を支援する．

5.1 従来型と現場主体型のモデル

従来の ISMS に基づいた組織の情報セキュリティの取り組み（以下，従来型）のパターンを表 2 に示す．表 2 では，マネジメント部門が策定したルールに基づき，情報システム部門が対策を実施している．従来型では対策の見直し・改善は，マネジメント部門が内部監査の結果を利用して行う．そのため，対策の見直し・改善はリアルタイムでなく，数か月から 1 年間隔で行われることになる．

Vol.2016-DPS-168 No.11
Vol.2016-SPT-21 No.11
Vol.2016-EIP-74 No.11
2016/11/18

表 2　従来型

実施事項 / 実施部門	方針の策定 体制の整備	ルールの策定	対策の実施	監視 異常検知	インシデント対応	対策の見直し・改善	内部監査	マネジメントレビュー	教育・アウェアネス 注意喚起・意識づけ
マネジメント部門	○	○				○	○	○	○
情報システム部門			○	○	○				

表 2 の実施事項は，図 4 の実施事項と対応している．各実施事項の内容を表 3 に示す．

表 3　実施事項の内容

実施事項	主な内容
方針の策定 体制の整備	・組織の方向付け，目的の明確化 ・責任・権限の割り当て
ルールの策定	・情報セキュリティ対策の明確化 (書類の持ち出し管理，情報システムのウイルス対策など)
対策の実施	・情報セキュリティ対策の実施 (書類の持ち出し管理，情報システムのウイルス対策など)
監視 異常検知	・ログのモニタリング ・定常監視
インシデント対応	・事象の把握 ・状況判断(トリアージ) ・対応支援
対策の見直し・改善	・情報セキュリティ対策の見直し・変更・強化
内部監査	・対策の実施状況確認 ・仕組み全体のチェック
マネジメントレビュー	・目的の達成状況評価 ・方針・目的の見直し
教育・アウェアネス 注意喚起・意識づけ	・従業員の教育・訓練 ・啓蒙活動

現場主体の情報セキュリティの取り組み（以下，現場主体型）を表 4 に示す．表 2 及び表 4 の網掛け部は，両者で異なる部分を示す．表 4 では，情報システム部門がルールの策定，対策の実施等を行い，インシデント対応の結果を反映して対策の見直し・改善を行っている．現場主体型では対策の見直し・改善は，インシデント対応と連動してリアルタイムで行われることになる．

表 4　現場主体型

実施事項 / 実施部門	方針の策定 体制の整備	ルールの策定	対策の実施	監視 異常検知	インシデント対応	対策の見直し・改善	内部監査	マネジメントレビュー	教育・アウェアネス 注意喚起・意識づけ
マネジメント部門	○						○	○	○
情報システム部門		○	○	○	○	○			

村﨑は，想定に基づいて事前に定めたルールでは，インシデントなど予測不可能な状況への柔軟な対応が困難であることを指摘した．インシデントなどの環境変化に対応するために，現場が例外規定の策定に参加する必要があると述べている [3]，[4]．

5.2 組織内での CSIRT の位置づけによる取り組みの違い

現場主体型における CSIRT の関わりを考える．組織内での CSIRT の位置づけによって，関わり方が異なり，情報セキュリティの取り組みにも違いが生まれると考えられる．

JPCERT/CC が 2015 年に実施した調査では，「情報システム管理部門系」や「セキュリティ対策部門系」が CSIRT 構築に関わっていることがわかる [5]．CSIRT と現場の実施事項を担当する情報システム部門，管理面の実施事項を担当するマネジメント部門の関係には，いくつかのパターンがあると想定される．CSIRT が独立しているケース，マネジメント部門や情報システム部門内に CSIRT があるケースなど，想定されるパターンの例を図 8 に示す．図 8 では，独立型，情報システム部門主導型，マネジメント部門主導型，統合型の 4 パターンに分けた．

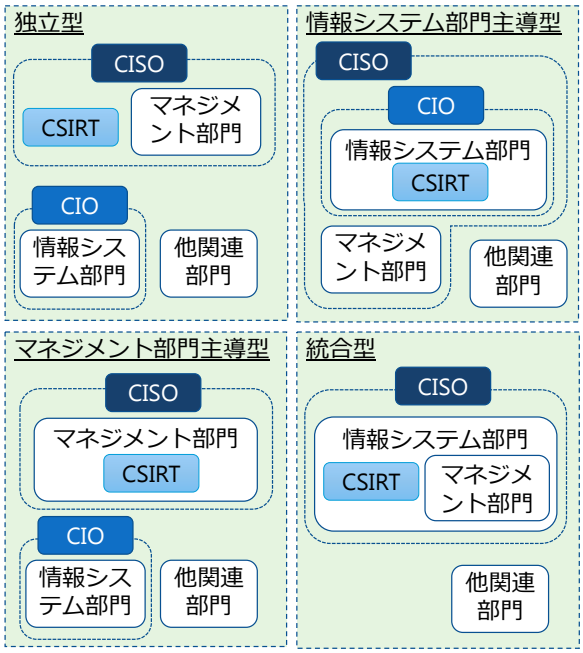

図 8　CSIRT と情報システム部門，マネジメント部門の関係のパターン

(1) 独立型

マネジメント部門，情報システム部門，CSIRT がそれぞれ異なる組織の場合の情報セキュリティの取り組みパターンである．これを表 5 に表す．表 5 から表 8 の網掛け部は各パターンで異なる部分を示す．表 5 では，インシデント対応は CSIRT が情報システム部門と連携して行い，インシデント対応の結果を反映して情報システム部門が対策の見直し・改善を行っている．独立型では，CSIRT はインシデント対応に集中することができるため，少人数で多くのインシデント対応を行うケースなどに向くと考えられる．以下に独立型の特徴を挙げる．

- CSIRT がインシデント対応に集中できる

Vol.2016-DPS-168 No.11
Vol.2016-SPT-21 No.11
Vol.2016-EIP-74 No.11
2016/11/18

- インシデントの発生が多い規模の大きな組織に適する
- 役割・機能の分担が可能な規模の大きな組織に適する
- 規模の小さな組織は，インシデントの発生が少なく，要員も限られるので独立型にこだわる必要はない

表 5　独立型

実施事項 / 実施部門	方針の策定体制の整備	ルールの策定	対策の実施	監視異常検知	インシデント対応	対策の見直し・改善	内部監査	マネジメントレビュー	教育・アウェアネス注意喚起・意識づけ
マネジメント部門	○						○	○	○
情報システム部門		○	○	○	連携	○			
CSIRT					○	支援			○

(2) 情報システム部門主導型

情報システム部門と CSIRT が同一組織で，マネジメント部門が独立している場合の情報セキュリティの取り組みパターンである．これを表 6 に表す．表 6 では，CSIRT を含んだ情報システム部門がルールの策定，対策の実施等を行い，インシデント対応の結果を反映して対策の見直し・改善を行っている．情報システム部門内で CSIRT の役割・機能のすみ分けができていないため，CSIRT は対策実施やモニタリングなどの日常的な業務をこなしながらインシデント対応も行うことになる．インシデント対応が頻繁に発生しない規模が小さな組織であれば問題ないが，多くのインシデント対応を行う組織では，緊急時の対応に追われ対策の見直し・改善などが遅れる恐れがある．以下に情報システム部門主導型の特徴を挙げる．

- 情報セキュリティの発生が少ない規模の小さな組織に適する
- 少ない要員で効率的に情報セキュリティに取り組める
- インシデント対応と現場の実施事項の両立が課題となる

表 6　情報システム部門主導型

実施事項 / 実施部門	方針の策定体制の整備	ルールの策定	対策の実施	監視異常検知	インシデント対応	対策の見直し・改善	内部監査	マネジメントレビュー	教育・アウェアネス注意喚起・意識づけ
マネジメント部門	○						○	○	○
情報システム部門 CSIRT		○	○	○	○	○			○

(3) マネジメント部門主導型

マネジメント部門と CSIRT が同一組織で情報システム部門が独立している場合の情報セキュリティの取り組みのパターンである．これを表 7 に表す．表 7 では，CSIRT を含んだマネジメント部門が方針の策定，内部監査等とともにインシデント対応を行っている．情報システム部門がルールの策定，対策の実施等を行い，インシデント対応の結果を反映して対策の見直し・改善を行う．情報システム部門主導型と同様に緊急時の対応に追われ，内部監査等に支障が出る可能性があるが，対策の見直し・改善は独立型と同様に情報システム部門において速やかに実施可能である．以下にマネジメント部門主導型の特徴を挙げる．

- 情報セキュリティの発生が少ない規模の小さな組織に適する
- 少ない要員で効率的に情報セキュリティに取り組める
- インシデント対応と現場の実施事項を異なる組織で行うため，情報システム部門主導型よりも両立が容易である

表 7　マネジメント部門主導型

実施事項 / 実施部門	方針の策定体制の整備	ルールの策定	対策の実施	監視異常検知	インシデント対応	対策の見直し・改善	内部監査	マネジメントレビュー	教育・アウェアネス注意喚起・意識づけ
マネジメント部門 CSIRT	○				○	支援	○	○	○
情報システム部門		○	○	○	連携	○			

(4) 統合型

マネジメント部門，情報システム部門，CSIRT がすべて同一組織の場合の情報セキュリティの取り組みパターンである．これを表 8 に表す．表 8 では，すべてを同じ組織で実施しており表 2 の従来型に近く，対策の見直し・改善などが遅くなる恐れがある．以下に統合型の特徴を挙げる．

- インシデントの発生が少ない規模の小さな組織に適する
- すべての実施事項を扱うため，特に管理面の実施事項について実施の有無や度合いなどが課題となる

表 8　統合型

実施事項 / 実施部門	方針の策定体制の整備	ルールの策定	対策の実施	監視異常検知	インシデント対応	対策の見直し・改善	内部監査	マネジメントレビュー	教育・アウェアネス注意喚起・意識づけ
マネジメント部門 情報システム部門 CSIRT	○	○	○	○	○	○	○	○	○

Vol.2016-DPS-168 No.11
Vol.2016-SPT-21 No.11
Vol.2016-EIP-74 No.11
2016/11/18

6. おわりに

従来の ISMS の取り組みは，現場の業務と乖離した形式的な管理面の実施事項が多く，現場にとってわかりづらいものだった．想定される脅威の増加とともに対策も即応性が求めれるようになったが，従来の ISMS は 1 年をサイクルとした取り組みであるため，十分に対応できない．これを補うものとして，今後，CSIRT を中心とした現場主体の情報セキュリティの取り組みが増加すると考える．一方，CSIRT は消防的な対応を行うため，長期的に組織全体で取り組む基本方針の策定などの対応は難しい．

5.2 節では CSIRT の組織内での位置づけの違いによる情報セキュリティの取り組みの違いを 4 つのパターンで比較検討した．検討の結果では，インシデント対応と現場の実施事項は，異なる組織で実施するのが望ましいのではないかと考える．

今後，以下の点について検討を進めていく予定である．

- 各パターンでのメリット・デメリットの掘り下げ
- 業種・業態による最適なパターン
- 組織の規模とパターンの関係（特に中小企業）
- CSIRT の提供サービスによる最適なパターン
- 4.1 節で述べた問題, 4.2 節で述べた心理的ハードルを考慮した最適なモデル
- 管理面の実施事項の要否・実施の度合い

謝辞

本論文の作成にあたり，ご指導いただいた情報セキュリティ大学院大学の教授陣，また多くの助言をいただいた原田研究室の客員研究員及びメンバーに，謹んで感謝の意を表する．

参考文献

[1] JPCERT/CC. CSIRT ガイド Ver.1.0. https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf, (2016 年 8 月 24 日参照). 2015

[2] 総務省. 総務省における情報セキュリティ政策の推進に関する提言. http://www.soumu.go.jp/main_content/000217000.pdf, (2016 年 10 月 4 日参照). 2013

[3] 村﨑康博ほか. 情報セキュリティ調査でわ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書, vol.2016-EIP-71, No.6. 2016

[4] 村﨑康博ほか. 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 -例外措置の主観評価と規定逸脱からの許容程度について-. 情報処理学会研究報告書, vol.2016-EIP-72, No.2. 2016

[5] JPCERT/CC. 2015 年度 CSIRT 構築および運用における実態調査. https://www.jpcert.or.jp/research/20160629_CSIRT-survey.pdf, (2016 年 9 月 8 日参照). 2016