Vol.2017-EIP-75 No.15
2017/2/17

環境変化に対応できる情報セキュリティ組織の機能と構造 -CSIRT に着目した考察-

副島恵子[†1]　原田要之助[†1]

概要：ISMS ベースで行われる組織の情報セキュリティ活動は，PDCA サイクルによるトップダウン型の取り組みである．標的型攻撃などサイバー攻撃が多様化・巧妙化する中，情報セキュリティインシデントなどの環境変化に速やかに対応できることが組織の情報セキュリティ活動に求められている．一方，情報セキュリティインシデント対応を行う専門部隊として CSIRT が注目されている．

本研究では CSIRT の機能に着目し，CSIRT の活動が組織の情報セキュリティの活動を活性化するための組織構造や機能分担について考察を行った．

キーワード：インシデント対応，CSIRT，ISMS，PDCA，OODA，トップダウン，ボトムアップ

The function and structure on information security organization that respond to environmental change -A study focused on the CSIRT-

KEIKO SOEJIMA[†1]　YONOSUKE HARADA[†1]

Abstract: The information security activities of the organization based on ISMS is a top-down approach based on the PDCA cycle. While cyber attacks such as APTs (Advanced Persistent Threats) are diversifying and sophisticated, the organization is required to respond promptly to environmental changes such as information security incidents. On the other hand, CSIRT has attracted attention, as a specialized unit handling information security incidents.

In this study, focusing on the function of CSIRT, the function and structure on information security organization are examined to activate the information security activities of the organization.

Keywords: Incident Response, CSIRT, ISMS, PDCA, OODA, Top-down, Bottom-up

1. はじめに

IT 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，クラウドなどにより，組織内の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や営業機能が，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・巧妙化している．そのため，サイバー攻撃に起因した情報セキュリティインシデントa（以下，インシデントという）が組織の事業活動や社会に与える影響は，以前にも増して大きくなってきている．

大規模な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．一方で攻撃者の組織化や新たな技術の利用など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，企業における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を実施する組織の機能と構造について考察する．また，CSIRT 活動を緊急時対応だけでなく企業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．

2. インシデントに対する組織の取り組み

2.1 インシデント対応における組織の問題

2014 年以降，大規模な個人情報漏洩事件が繰り返し発生している．これらの個人情報漏洩事件のインシデント対応では，表 1 に示すいくつかの組織的な問題が見られた．表 1 の（1）は，組織全体と経営層の問題である．（2）は組織の情報セキュリティ部門の問題である．（3）は現場の問題である．なお，本稿における「情報セキュリティ部門」とは，組織の情報セキュリティの取り組みを統括する部門と定義する．また，「現場」は，情報セキュリティ部門の指示のもとで情報セキュリティに取り組む組織内の各部門で，情報セキュリティや情報システム関連以外の業務を主とする実務担当者と定義する．

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

a本稿でのインシデントとは，内部不正による情報漏洩や，サイバー攻撃がもたらす企業の情報や活動への被害を指す

表 1　インシデント対応における組織的な問題

No	問題
(1)	・ インシデントを想定した組織体制が不足(a) ・ 組織全体の対応ルールが不備，判断が遅延(b) ・ 組織全体の情報共有の不足，役員への報告が遅延(b)(c)
(2)	・ インシデントの発見の遅延(a)(c) ・ インシデントへの対応策の周知不足(b) ・ 担当者ベースでの対応，対応の遅延(b)(c)
(3)	・ インシデントの発生や兆候を見逃し(a)(c) ・ インシデントへの対応策が機能しない(b) ・ セキュリティ対策に生じた不備を見逃し(a)

(a)：2014 年 ベネッセホールディングスで 4858 万人の個人情報漏洩[1]

(b)：2015 年 日本年金機構で 101 万人の個人情報漏洩[2]

(c)：2016 年 株式会社ジェイティービーで 790 万人の個人情報漏洩の可能性[3]

表 1 の（1）の組織全体と経営層の問題は，インシデントへの対応が可能な組織体制ができておらず下部組織からの報告や事件発生後の経営判断が遅れたことである．インシデントの対応では，情報共有を図り適切なタイミングで対応策を判断することが必要であるが，これができていなかった．インシデント対応を前提とした情報セキュリティの取り組みが不足していたと考えられる．

表 1 の（2）の情報セキュリティ部門の問題は，現場に対する対応策の周知が不十分であったことである．日本年金機構の個人情報漏洩事件では，情報セキュリティ部門から不審メールへの注意喚起が行われていた．しかし，この注意喚起には添付ファイルを開封した場合の対処や連絡先が含まれていなかった．一方で現場では，注意喚起後にも不審メールを開封しており，適切な対応を行ったとは言いがたい．情報セキュリティ部門のもう一つの問題は，担当者だけで初動対応が行われ，結果的に必要な組織的な対応をとるのが遅延したことである．インシデントの対応では，異なる組織間や同じ組織内の部門間で連携して組織的に対応にあたることが必要である．

表 1 の（3）の現場の問題は，情報セキュリティ対策にあった不備に気付いていなかったこと，または不備のために対策が有効でなくリスクが発現したことに気づかなかったことである．情報セキュリティ部門との連携不足もあり，（決められた事をやりさえすればよいという）現場が情報セキュリティ対策に主体性を持って取り組んでいなかったことがうかがえる．情報セキュリティが一部の専門家のものとなり，現場の情報セキュリティに対する当事者意識が欠落していたと考える．インシデントへの耐性がある組織とするために，現場の意識を変革する必要がある．

このほかに，現場と情報セキュリティ部門に共通する問題として，インシデントの兆候の見逃しと発見の遅れがある．

2.2 インシデント対応と CSIRT

インシデントが頻発・大規模化する中で，情報セキュリティインシデントの影響を最小限に抑えるための組織・機能として注目されているのが CSIRT（Computer Security Incident Response Team）である．CSIRT は，情報セキュリティインシデントの対応を専門に行うチームで，その役割はしばしば「消防」にたとえられる．

CSIRT の機能は，緊急時の対応であるインシデントハンドリングのほか，平常時の脆弱性対応，事象分析，普及啓発，注意喚起など多岐にわたっている．[4]

CSIRT は，組織内外の関連する部門や関連機関と連携してインシデント対応にあたる．図 1 は，インシデント対応の各フェーズにおける対応者と実施事項である．図 1 の「発見」から「初動対応」のフェーズでは，現場と CSIRT が協力してインシデント対応が行われる．図 1 の「初動対応」から「復旧」のフェーズは，現場と CSIRT に加え関係箇所が連携してインシデント対応が行われる．関係箇所には，コンピュータやネットワークのセキュリティを担当する情報システム部門，機密文書の取り扱いや入退室管理を定める総務部門，従業員の懲罰を扱う人事部門などのほか，顧客への説明を行う営業部門，プレスリリースなどを担当する広報部門等がある．社会的影響が大きなインシデントや，業務の中断を伴うシステムやネットワークの停止を必要とするインシデント対応の場合は，経営者との連携も必要となる．

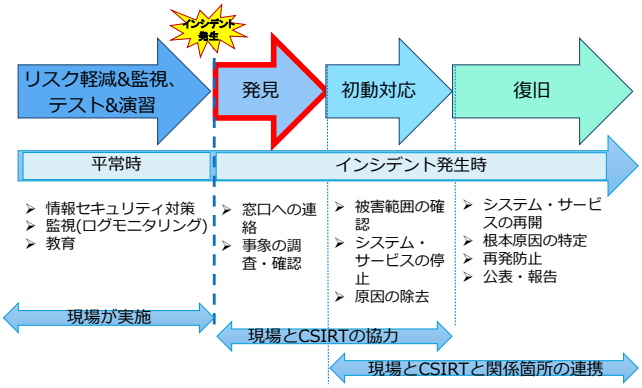

図 1　インシデント対応の各フェーズの対応者と実施事項b

2.3 インシデント対応における PDCA サイクルの限界

ISO/IEC 27001:2005 では，表 2 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．

b ISO/IEC 27031:2011 の図をもとに加筆して作成

表 2　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

情報セキュリティの取り組みの考え方として主流となっている PDCA サイクルであるが，次々と登場する攻撃など組織を取り巻く環境がめまぐるしく変化する中で，限界が見えている．小室は，PDCA サイクルの限界の要因をいくつか指摘している．ひとつは，オープンシステムで捉える必要がある情報セキュリティに対して，PDCA サイクルでは組織をクローズドシステムとして捉えていることである．また，トップダウンの命令系統である PDCA サイクルではトップの策定した計画が絶対とされるが，インシデント対応のように変化する状況の中では，計画をベーすにすることが常に最適な方法とは限らないということである．さらに，企業の存続に関わるようなインシデント対応ではトップの関与が必要となるが，PDCA サイクルでは計画と執行が分離されていることを挙げている [5].

このように，PDCA サイクルには，サイバー攻撃のように動的に変化するリスクに対抗しきれないという問題があることから，PDCA サイクルによらない仕組みを考える必要がある．

3. 緊急対応可能な組織に求められる取り組み

3.1 OODA ループによる取り組み

高度化するサイバー攻撃に迅速かつ的確に対応することを目的として,「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 2 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[6].

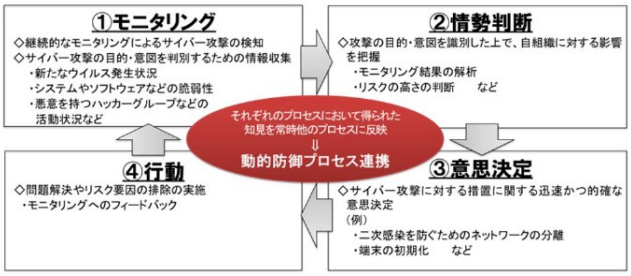

図 2　動的防御プロセス連携[6]

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インシデント対応の活動に適していると考えられる．

3.2 情報セキュリティの取り組みへの現場の参加

多くの企業で ISMS（Information Security Management System）に基づいた情報セキュリティの取り組みが行われている．企業における ISMS の取り組みの実施事項は，図 3 のように管理面の実施事項 cと現場の実施事項に分けられる．管理面の実施事項はマネジメントレビューや内部監査など現場の業務と異なる ISMS 特有のものが多い．また，情報セキュリティ対策は，現場が関与しない状態で，全社的にリスクアセスメントを通じて決定されることがある．情報セキュリティ部門によって行われるリスクアセスメントでは，企業全体で洗い出されたリスクについて統一的に分析・評価され，情報セキュリティ対策が決定される．そのため，現場が直面するリスクと実施される情報セキュリティ対策に乖離が生まれる．これらが引き金となって，ISMS ベースの取り組みでは，現場との距離感が生まれ，現場が情報セキュリティに主体的に取り組まなくなることがあると考えられる．

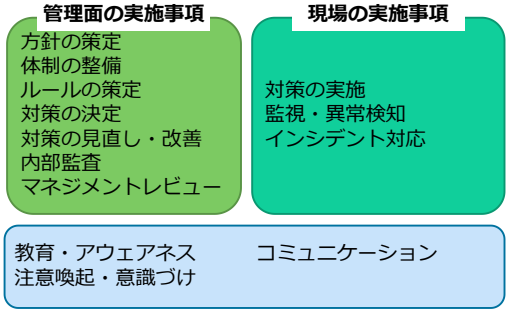

図 3　ISMS の取り組みの実施事項

ISMS のもうひとつの問題は，静的リスクを主に扱い，あらかじめリスクを分析・評価することでリスクを削減するという考え方にある．実際にはインシデントの発生はあとを絶たず，予測とは異なる事象が発生する．そのため，リスクの削減には限界がある．インシデントが発生することを前提として，予測ができないサイバー攻撃などの動的リスクを扱える仕組みが求められている．

予測が困難な災害などの危機対応の考え方に ICS（Incident Command System）がある．ICS は，リスクが発現する現場に権限を集中させて，発見と対策の意思決定を素早く行うことで，被害を最小限にするという考え方である [7]．インシデント対応においても，ICS と同様に，現場に権限を持たせるボトムアップの取り組みが必要と考えることができる．

c管理面の実施事項は，組織全体で情報セキュリティに取り組むための実施事項である．

3.3 ボトムアップによる情報セキュリティの取り組み

全社を攻撃対象とするような予測ができないインシデントに対する対策は，短期間に全社に展開する必要がある．インシデント対応は，予測できないこと，素早い対応が必要なことから OODA ループで扱うのが望ましいと考えられる．OODA ループがサイバー攻撃などの急激な変化への対応に適するのに比べ，PDCA サイクルは長期スパンの体系的な取り組みであり，計画をベースとするため，予測できない急激な変化には対応できないと考えられる．

小室によると，PDCA サイクルは，組織の上層部が「日常的執行業務に埋没せずに，長期的な展望や抜本的な変革を考えるなどの計画業務に注力できる」ことに意義がある．そのためには，現場に自由度と権限を認め，リスク対応の経験をつませる必要がある．一方で，企業の存続に関わるような問題にはトップの関与が不可欠であるという．

沼上によると，環境の不確実性が高まる中，頻発する多数の例外的な事象への対応を強いられる組織では，事業部制によってトップが長期的な展望の策定や成長戦略に注力できると述べている．また，事業部制では日常的に生じる問題を自分たちで解決できるよう資源や権限が各事業部に与えられているが，そのことが組織の階層構造と官僚制を否定しているわけではないという[8]．これは，ボトムアップの取り組みとトップダウンの取り組みが，両立できることを示していると考えられる．

3.4 トップダウンとボトムアップの融合

組織において，情報セキュリティの取り組みは現場からのボトムアップだけでは不十分であり，情報セキュリティポリシーを統一的に実施するなどのトップダウンと融合した取り組みが必要とされていると考えられる．また，トップダウンとボトムアップの融合は可能である．

OODA ループは 2 つの「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不向きである．そこで，ボトムアップの OODA ループとトップダウンの PDCA サイクルが合わさった仕組みで，組織の情報セキュリティの取り組みを行うことを提案する．

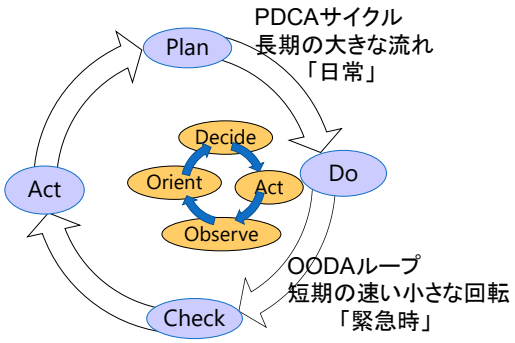

図 4　PDCA サイクルと OODA ループ

OODA ループとマネジメントシステムの PDCA サイクルの関係は，図 4 のように，日常を扱う長期の流れを PDCA サイクル，緊急時の短期の速い回転を OODA ループとして捉えることができる．OODA ループと PDCA サイクルを組み合わせることで，情報セキュリティの取り組みの迅速性と網羅性の両立が可能になると考える．

4. 現場主体の情報セキュリティの取り組みの提案

4.1 現場主体型の情報セキュリティの取り組み

インシデントなどの環境変化に対応可能な組織とするために，現場が短期間のループを繰り返すことで情報セキュリティの強化を図るモデルを提案する．従来の ISMS での情報セキュリティの取り組み（以下，従来型）は，情報セキュリティ部門がルールの策定と対策の決定を行い，現場にルールと対策の遵守を指導するトップダウンの取り組みである．これに対し，現場である業務部門を主体とした取り組み（以下，現場主体型という）は，対策の見直しや改善を現場で行うボトムアップの取り組みである．

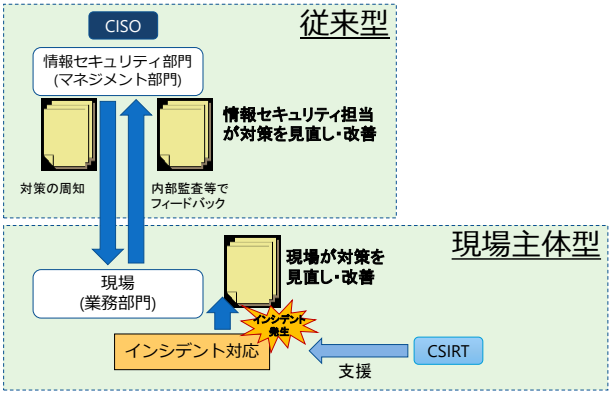

図 5　従来型と現場主体型の概念

従来型と現場主体型の概念を図 5 に示す．従来型では経営層（図 5 では CISO として表現）からの指示を受けた情報セキュリティ部門が対策を決定し，現場からの意見を取り入れ，対策の見直しや改善を行う．従来型では ISMS の規格である ISO/IEC 27001:2013 の管理策をベースとして，体系的かつ網羅的に情報セキュリティの対策を策定できる．しかし対策の見直しや改善は，内部監査の結果を利用して組織全体で行われるため，数か月から 1 年間隔という比較的長い時間が必要となる．一方，現場主体型では，インシデント対応と連動して，現場が対策の見直しや改善をリアルタイムで行う．

本稿におけるルールと対策は，表 3 のように定義する．表 3 では，ルールと対策は役割や性質が異なるものと捉えられるが，ルールと対策を一体のものとして情報セキュリティ部門において一元的に扱っている企業が多いと考えられる．本稿ではルールと対策の策定または決定と見直しの取り扱い部門を分けて考える．

表 3　ルールと対策の定義

ルール	対策
・ 基本となるきまり ・ 組織全体の情報セキュリティの取り組みを異なる現場で統一性のあるものにするためのもの ・ 組織が共通認識をもって情報セキュリティに取り組めるようにするためのもの ・ 対策の指針・原則にあたるもの	・ 情報セキュリティを実現するための手段や手続 ・ 技術, 文書などのツールを使って実施・実行されるもの ・ 具体的な手順，行動を指す

図 6 は，情報セキュリティのルール・手順書類の文書体系について，従来型と現場主体型の違いを示しているd．従来型では，第 1 層の基本方針と第 2 層の対策基準は情報セキュリティ部門が策定と見直しを行うが，現場主体型では，第 2 層の決定・見直しは現場が行う．現場主体型では，組織全体の情報セキュリティを統制し組織内の共通認識を培う第 1 層のルールについて，情報セキュリティ部門が策定と見直しを行う．実際の情報セキュリティ対策である第 2 層の対策は，現場が決定し見直しする．

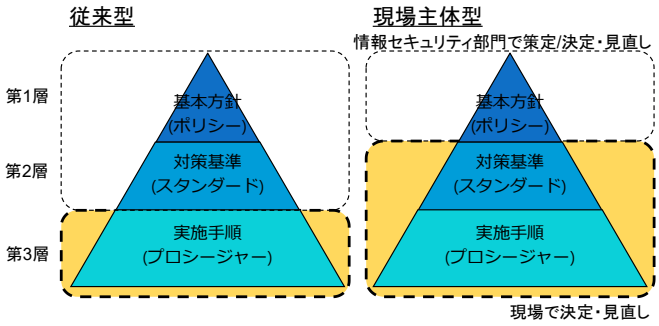

図 6　従来型と現場主体型による違い

現場主体型は，次の特徴を有する．

- 対策の決定，見直し・改善を現場が行う
- リアルタイムで対策を見直し・改善

村﨑は，想定に基づいて事前に定めたルール（従来型に相当すると考えられる）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．そこで，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もあると述べている[9][10]．現場主体型は，予測不可能で動的に変化するリスクに対応可能な情報セキュリティの取り組みである．

現場が決定する情報セキュリティ対策は，図 7 のように中心に情報セキュリティ部門が決定した原理・原則が核として存在する細胞のような形になると考えられる．図 7 で核の外側にある現場が決定する具体的な対策内容は，環境変化によって見直し・改善が行われる部分である．柔軟さをもったこの構造によって，インシデントへの迅速な対応が可能となると考えられる．

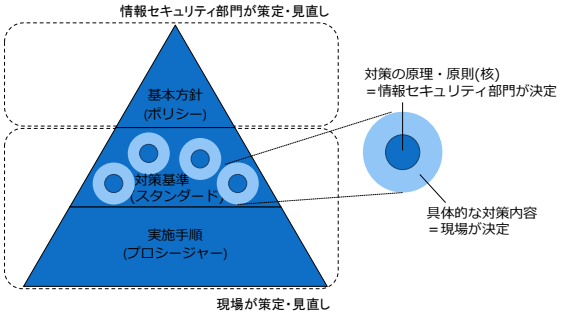

図 7　情報セキュリティ対策のイメージ

4.2 現場主体型の実施事項

図 3 で示した ISMS の取り組みの実施事項の内容を表 4 に示す．

表 4　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 ルールの策定	・組織の方向付け，目的の明確化 ・責任・権限の割り当て ・情報セキュリティ対策の指針の明確化
対策の決定	・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

表 4 の実施事項について，従来型と現場主体型における実施部門を表 5 及び表 6 に示す．

表 5 及び表 6 の網掛け部は，従来型と現場主体型で実施部門が異なる部分を示している．従来型で情報セキュリティ部門が実施していた対策の決定と対策の見直し･改善は，現場主体型では現場の実施事項となる．また，従来型で情報セキュリティ部門が指示を行い主導していた監視・異常検知は，現場主体型では現場が主体となって実施する．同様にインシデント対応についても情報セキュリティ部門ではなく現場が実施する．

d図 6 の上から第 1 層，第 2 層，第 3 層とする

表 5　従来型の実施事項

実施事項 / 実施部門	方針の策定 体制の整備 ルールの策定	対策の決定	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
情報セキュリティ部門	○	○		指示	○	○	○	○	○
現場			○	○	連携				

表 6　現場主体型の実施事項

実施事項 / 実施部門	方針の策定 体制の整備 ルールの策定	対策の決定	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
情報セキュリティ部門	○			支援	連携		○	○	○
現場		○	○	○	○	○			

5. 現場主体型の実現に向けて

5.1 現場主体型における CSIRT の役割

現場主体型には，現場が情報セキュリティに自主的に取り組む風土があることが必要である．この現場主体型における課題は，現場が情報セキュリティに積極的に関与するためにどうするか，情報セキュリティ対策のレベルをどのようにして保証するかである．

現場主体型はインシデントの発生を対策の見直し・改善のきっかけとしているが，致命的なダメージを受ける前の予兆の段階で現場が対策を見直すことも重要となる．現場は，どのような行為や状態がインシデントにつながる可能性があるのかを認識できなくてはならない．また，新たなリスクに対する危機意識を持つこと，新たなリスクの情報を知得し，その対応を経験して体得することも現場に求められる．この活動については，現場だけでは実施が難しい．インシデントの分析や対応については，専門家である CSIRT が協力しながら実施することが求められる．

すなわち，CSIRT がインシデント時に行う注意喚起や平常時の普及啓発活動は，現場に情報セキュリティを意識させ，情報セキュリティに対するモチベーションを高めると考えられる．また，現場は対策の見直し・改善に必要となる情報セキュリティの専門知識や技術を十分持つとは限らないが，CSIRT によるインシデント対応の支援が現場の知識や技術を補完すると期待される．

5.2 情報セキュリティ部門，CSIRT，現場の機能分担

現場主体型では，図 8 のように情報セキュリティ部門，CSIRT，現場が相互に連携する構造をとると考えられる．情報セキュリティ部門は，基本方針やルールの策定・見直しを行い，企業全体の情報セキュリティの取り組みを統制する．また，予算や要員などについて CSIRT 及び現場と経営層の仲介を行う．インシデント対応は，社内外の多くの組織と連携して行われるが，情報セキュリティ部門が窓口や調整役を担うことで，確実で迅速な対応が可能となる．

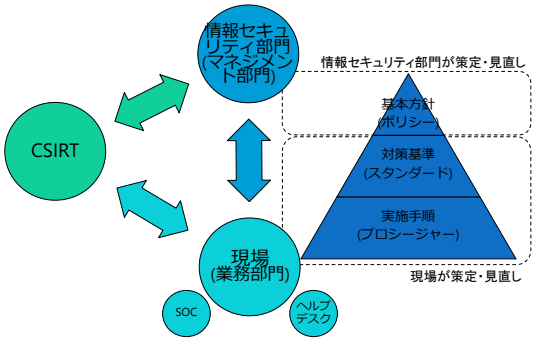

図 8　情報セキュリティ部門，CSIRT，現場の役割

現場主体型では，各部門がそれぞれに情報セキュリティへの取り組みを分担する．すなわち，ISMS で必要とされる情報セキュリティ対策の主管部門は，入退室管理であれば総務部門，PC のウイルス対策であれば情報システム部門といったように機能分担する．このとき情報セキュリティ部門には，組織全体の情報セキュリティのバランスを保つため，各部門の調整を行う役割が求められると考える．情報セキュリティ部門が，重複する機能や対策の交通整理を行い，欠落する機能や対策がある場合には主管部門を決めるよう社内に働きかける．また，各部門で決定した情報セキュリティ対策のレベルが全社としての基準をクリアしているかどうか，部門間で対策に重複や不整合がないかなどのチェックを情報セキュリティ部門が行う．情報セキュリティ部門が各部門の情報セキュリティ対策を横通しでチェックすることで，現場主体型においても統制の取れた情報セキュリティの取り組みが実現可能となる．

5.3 CSIRT の役割・機能と位置づけの考察

企業内での CSIRT の機能と位置づけは企業規模，業種，構造によって異なり，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．現場主体型における現場，CSIRT，情報セキュリティ部門の役割と機能の関係について，どのような形が望ましいのかを図 9 の想定される 4 つの形態で考察を行う．

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[11]．企業において，情報セキュリティと情報システムは一体視される傾向にあり，情報システム部門が情報セキュリティ部門の役割を担うこともある．同様に情報セキュリティのインシデント対応の専門部隊である CSIRT を情報システム部門内に置くケースも想定される．情報セキュリティを専門に扱う部門と，他の業務を主として扱いながら情報セキュリティに取り組む部門では取り組みに違いがあると考えるため，本節では，情報システム部門を現場として扱う．

Vol.2017-EIP-75 No.15
2017/2/17

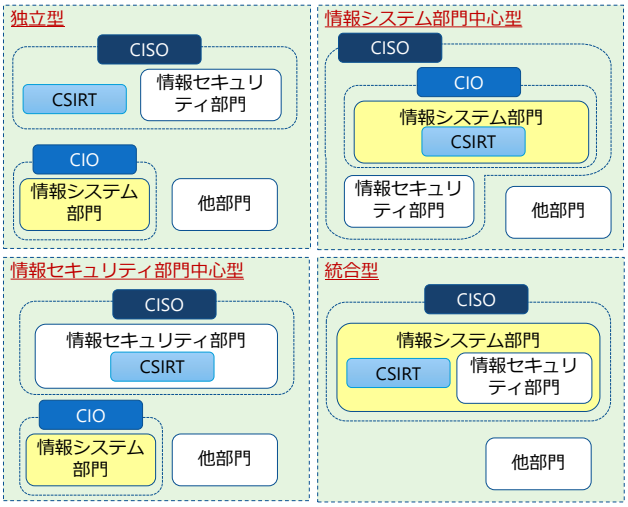

図 9　CSIRT と情報システム部門，情報セキュリティ部門の機能と役割の形態

図 9 に示す独立型，情報システム部門中心型，情報セキュリティ部門中心型，統合型の 4 つの形態について，表 4 の実施事項をどの部門が担当するのかを考える．

表 7 は情報セキュリティ部門，情報システム部門，CSIRT がそれぞれ異なる組織である独立型における実施事項の形態である．表 8 は，情報システム部門と CSIRT が同一組織で，情報セキュリティ部門が独立している情報システム部門中心型における実施事項のパターンである．表 9 は，情報セキュリティ部門と CSIRT が同一組織で情報システム部門が独立している情報セキュリティ部門中心型における実施事項の形態である．表 7 から表 9 の塗りつぶし部は，各形態で実施部門に違いがある実施項目を示す．表 7 の独立型では，CSIRT が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．役割・機能を分担するため，要員の確保が可能な規模の大きな企業向きの形態と考えられる．

表 8 の情報システム部門中心型では，CSIRT の役割・機能と情報システム部門の業務のすみ分けが不十分な状態である．そのため，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緊急時のインシデント対応も行うことになる．インシデント対応と日常的な業務の両立が課題となる．統合型においても同様に両立が課題となる．

表 9 の情報セキュリティ部門中心型では，緊急時のインシデント対応と内部監査等との両立が課題となる．しかし，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り，少ない要員で効率的に情報セキュリティに取り組める形態と考えられる．

以上のように，4 つの形態それぞれに対して企業規模，現場の状況，ISMS 導入状況などによって適した形態が異なると考えられる．

表 7　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	対策の決定	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
情報セキュリティ部門	○						○	○	○
情報システム部門		○	○	○	連携	○			
CSIRT					○	支援			○

表 8　情報システム部門中心型

実施事項 / 実施部門	方針の策定，体制の整備，ルールの策定	対策の決定	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
情報セキュリティ部門	○						○	○	○
情報システム部門／CSIRT		○	○	○	○	○			○

表 9　情報セキュリティ部門中心型

実施事項 / 実施部門	方針の策定，体制の整備，ルールの策定	対策の決定	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
情報セキュリティ部門／CSIRT	○				○	支援	○	○	○
情報システム部門		○	○	○	連携	○			

5.4　情報システム部門と情報セキュリティ部門の機能の分離

情報セキュリティ大学院大学原田研究室では，2016 年 8 月 10 日から 10 月 31 日にかけて，「2016 年情報セキュリティ調査」を実施した．調査対象は，日本国内のプライバシーマーク（以下，P マーク）取得組織，ISMS 認証取得組織，官公庁，教育機関などから選んだ 4,800 組織の情報セキュリティ担当者である[12].

回答者の所属は，「総務部門」26%，「情報システム管理部門」23%，「情報セキュリティ担当部門」22%となっており，多くの企業で情報システム部門が情報セキュリティを担当していることが分かる．回答者を「情報セキュリティ担当部門」，「情報システム部門（情報システム管理部門と情報システム開発部門の合計）」，「その他」に分け，情報セキュリティ対策を推進する上での難しさとのクロス集計を行った．

図 10 は，回答者の所属別にみた情報セキュリティ対策を推進する組織が内部から評価を得ることの難しさである．図 10 では，「情報システム部門」において「難しい（「とても難しい」から「どちらかといえば難しい」の総和）」とする割合が高くなっていることが分かる．カイ 2 乗値は 0.000 であり統計的に優位な関連があることが確認できた．情報システム部門で「難しい」の割合が高くなるこの傾向は，

体制整備・運営の難しさ，人材確保の難しさにおいても同様であった．この結果から，情報システム部門が情報セキュリティを担当する場合，体制整備・運営，人材確保，組織内からの評価において，組織的な運営の難しさが現れるといえる．

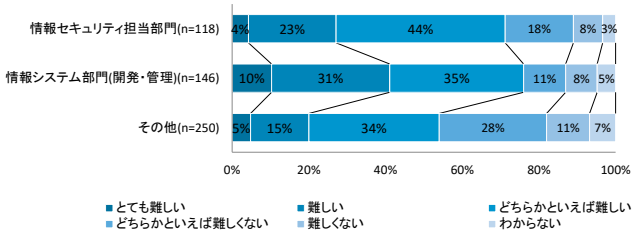

図 10　情報セキュリティ対策を推進する組織が内部から評価を得ることの難しさ

図 10 のように，情報システム部門が情報セキュリティを担当する場合，組織内からの評価は得にくくなっている．このことから，インシデント対応のような組織内の関連部門との連携が必要となる取り組みは，情報システム部門以外が主導することが望ましいと考えられる．今後，CSIRT の機能や役割などをうまく活用して，企業の組織的な課題を克服することが望まれる．

6. おわりに

従来の PDCA サイクルに基づいた情報セキュリティの取り組みは，予測できるリスクに対する対策が中心であった．手法や攻撃対象が変化し高度化するサイバー攻撃などは予測が困難であるため，PDCA モデルでは対応できない．そのため，多くの企業では，複雑化するインシデント対応を的確かつ迅速に行うため，CSIRT を整備する動きが広がっている．情報セキュリティの取り組みは今後，これまでの ISMS に基づいたトップダウンの取り組みから CSIRT と現場を中心としたボトムアップの取り組みに変化する必要があると考えられる．そこで，本稿ではこのボトムアップのアプローチとして現場が主体となって情報セキュリティ対策の決定・実施・改善を行う現場主体型の取り組みを提案した．現場主体型では，CSIRT が現場の情報セキュリティ意識の向上を助け，現場に不足する知識を補完し，現場を教育することが望まれる．

インシデント対応における組織的な問題として，組織内の連携不足や現場の情報セキュリティに対する当事者意識の欠落がある．この問題は，従来の情報セキュリティの取り組みが情報セキュリティ部門を中心として進められていたことに起因することを指摘した．現場が情報セキュリティに積極的に関与する現場主体型ではこの問題が解消すると期待される．すなわち，現場主体型によってインシデントなどの環境変化に対応可能な情報セキュリティ組織が実現できると考える．

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．あわせて，情報セキュリティ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，調査票の封入，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，神奈川県立相模原養護学校，神奈川県立相模原養護学校橋本分教室，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，神奈川県立中原養護学校，神奈川県立みどり養護学校新栄分教室，川崎市立田島支援学校（五十音順）に感謝します．さらに，本学事務局の皆様に感謝致します．

参考文献

[1] ベネッセホールディングス．個人情報漏えい事故調査委員会による調査報告について．http://blog.benesse.ne.jp/bh/ja/news/m/2014/09/25/docs/20140925%E3%83%AA%E3%83%AA%E3%83%BC%E3%82%B9.pdf, (2016 年 7 月 16 日参照). 2014
[2] 日本年金機構不正アクセスによる情報流出事案に関する調査委員会．不正アクセスによる情報流出事案に関する調査結果報告. https://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf. (2016 年 7 月 16 日参照). 2015
[3] 第 2 回 観光庁・旅行業界情報共有会議．旅行業界情報流出事案検討会 中間とりまとめ ～旅行業情報セキュリティ向上のため早急に構ずべき対策～．http://www.mlit.go.jp/kankocho/topics06_000080.html, (2016 年 9 月 6 日参照). 2016
[4] 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
[5] 小室達章．リスクマネジメントシステムと PDCA サイクル．金城学院大学論集，社会科学編, 6(1), p.1-12. 2009
[6] 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
[7] 一般財団法人 日本科学技術連盟．危機管理体制のあるべき姿．日科技連ニュース No.115, 2013 年 6 月号. https://www.juse-iso.jp/cms_file/cms.cms,resource./2784/resource/, (2016 年 12 月 19 日参照). 2013
[8] 沼上幹．組織戦略の考え方．ちくま新書, p.28-39. 2003
[9] 村崎康博ほか．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
[10] 村崎康博ほか．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．情報処理学会研究報告書, vol.2016-SPT-20, No.5. 2016
[11] 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
[12] 副島恵子ほか，“2016 年情報セキュリティ調査から見えてくる組織（民間企業・官公庁・教育機関）における現状”，2017 年 暗号と情報セキュリティシンポジウム講演予稿集, 2A2-3. 2017