組織リスク動的判断モデル作業部会

報告書

平成 22 年 3 月

目次

0. 調査の目的と背景

情報セキュリティ分野は、対応すべき脅威や関連する技術など、様々な側面において環境の変化が早い。また、近年の攻撃手法の高度化やそれに対応する対策の深化に伴い、情報セキュリティに係る専門分化や分業化が生じつつある。刻々と変化する状況を適時適切に把握し、新たに生起する課題に対して的確な対応を行うためには、関係する専門分野の知見を有する各主体が、情報を共有し、かつ連携して対処していくことが重要である。

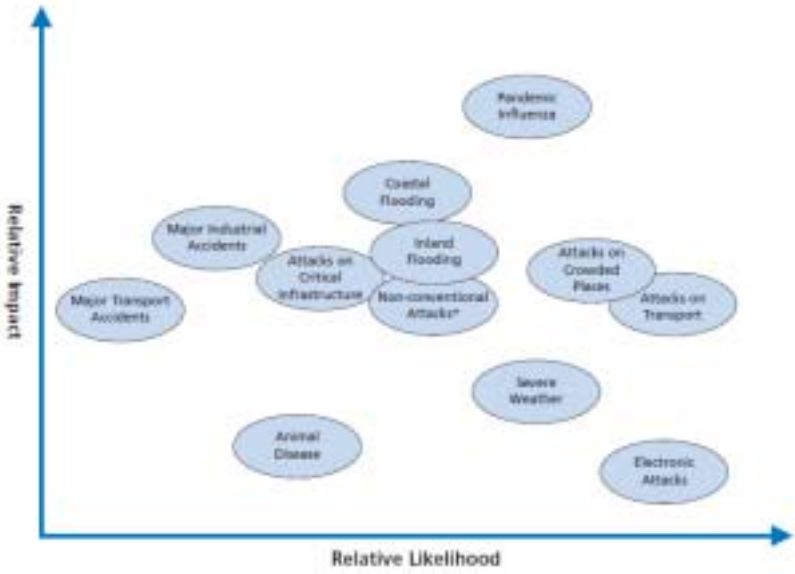
このため、「セキュア・ジャパン 2009」(平成 21 年 6 月 22 日情報セキュリティ政策会議決定)に基づき、内閣官房情報セキュリティセンター(以下、「NISC」)において、システム設計分野、ウイルス解析分野、技術分野、ISP 分野等の各専門分野の情報共有スキームの役割と連携性を整理し、それぞれの目的・機能に応じた情報連携と情報交換モデルの検討を行い、この一環として組織リスク動的判断モデルに関するチャート等を作成する。

1. 組織とインシデント対応を巡る現状

1.1. 背景

1.1.1. 脅威の変化に伴って生じた諸課題

ITに対する脅威は、従来、組織への影響が比較的低いとみなされていた。たとえば英国内閣府では、「Electronic Attacks」（電子的攻撃）は発生頻度が高いが影響は低い脅威と位置づけられている。しかし、攻撃側のビジネスモデルの確立を背景とした標的型攻撃の台頭や攻撃基盤の成長といった脅威の変化に伴い、企業等の組織に与える影響は急速に拡大していると考えられる。



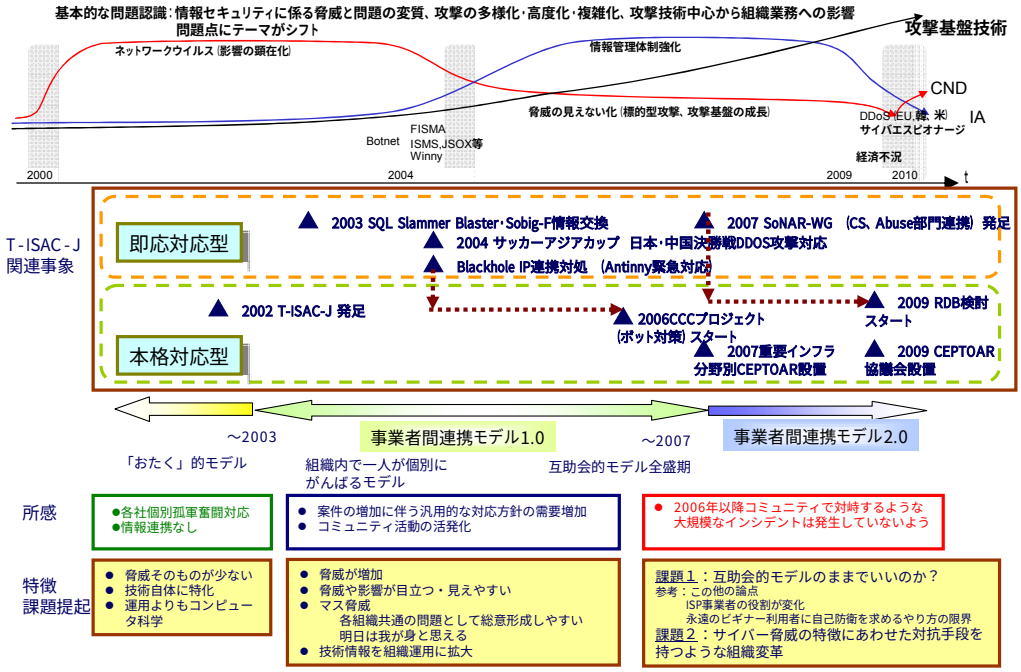
資料：長岡技術科学大学・渡辺准教授[1]

図 1-1 英国内閣府によるリスクマップ（例示）

時間的経緯を踏まえると、まず、2000 年頃からネットワークウイルスによる影響の顕在化が進んできた。しかし、2004 年頃から、攻撃の悪質化・複雑化が進み、特定のターゲットを狙った標的型攻撃や攻撃基盤の成長が進展し、脅威の見えない化が進むこととなった。一方、ISMS、個人情報保護法の施行、J-SOX 等、組織における情報管理体制強化の動きもあり、攻撃技術への対応から、組織業務への影響を考慮する必要性が高まってきた。

このような脅威の変化に伴い、発生した事象に対する即応対応型ではなく、本格対応が求められるようになっており、それに伴い対応組織の変化も迫られている。特に、社会を席巻するような大規模インシデント、いわゆる「マス脅威」が見られなくなった現在、問題の共有が困難であるため、互助会的モデルで形成された事業者間連携は、一つの転機を迎えているという見方もある。図 1-2 に脅威の変化と組織モデルの関連を示す。

[1] 第 3 回 DM-WG 渡辺主査資料(P5)

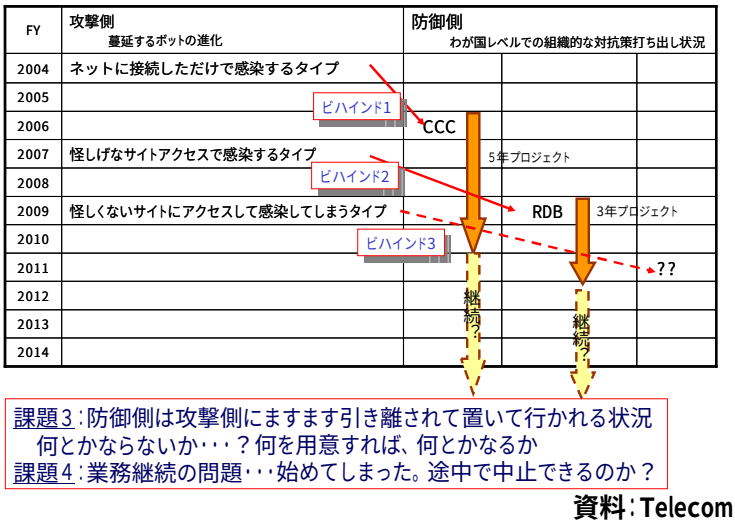


資料：Telecom-ISAC Japan[2]

図 1-2 脅威の変化と組織モデル

しかし、脅威の変化に対応していくことは容易ではない。図 1-3、表 1-2 の通り、ボットを例とした攻撃側の進化と比較し、防御側の組織的な対応に関しては遅れがちになる。脅威を理解し、それに対応するための体制を整えるのに時間を要し、プロジェクトとして動きだした頃には、脅威が進化している。

今後の組織モデル整備検討では、脅威の変化に追随する為の動勢分析機能を重視する事が必要である。



課題3：防御側は攻撃側にますます引き離されて置いて行かれる状況
何とかならないか・・・？何を用意すれば、何とかなるか
課題4：業務継続の問題・・・始めてしまった。途中で中止できるのか？

資料：Telecom-ISAC Japan[3]

[2] 第 1 回 DM-WG 有村構成員資料 (P5)

図 1-3 攻撃側と防御側の変化

表 1-1 攻撃の変化

時期	2004年	2007年	2009年	
CCCプロジェクト年表	CCCスタート前	スタートから3年	スタートから5年後	
攻撃ポイント	脆弱性攻撃型のタイプ 【例：ネットワーク感染型ボット】	怪しげなサイトアクセスで感染するタイプ 【例：SQLインジェクション、MPack/IcePack、Mal/IFrame】	怪しくないサイトにアクセスして感染してしまうタイプ 【例:Gumblerウイルス】	〔抽象化〕 多様化・高度化・複雑化により困難がもたらされる項目
攻撃の検知（入り口）	受動型待ち受け	能動型	能動型	発見
一次攻撃	NW脆弱性攻撃	裏口、壁穴狙い 例：SQLインジェクション	正面玄関狙い 短期更新 例：アカウントクラック	発見
2次攻撃（中間サーバー、DLサーバー）	1段、ただし 海外サーバー、野良サーバー	多段化、プログラム的動作（まりも記述可能）、短期引っ越し	同じ挙動をしない	追跡
攻撃対象の分散	端末	端末＋webサーバ	端末＋webサーバ	対策指示の複雑化 （異なる対策の同時実施）
被害者（数・質）	多数、ただし均一的	多様化	さらなる多様化	利害関係者数
感染拡大の輪の分断	数量的な広がり ボットプログラム入手は可能 実験室でのボットネット再現は可能	空間的広がり 水面下、分業化	時間的変動要素 時間的な分断化・時間差（ほとぼりをさましてから使用）	全体像解明
感染拡大防止対策 ＜＝ 解決策の展開機能＋ 解決策の創出機能 ＋				これらの項目に備える・耐える機能

資料：Telecom-ISAC Japan[4]

1.1.2. 組織の変化～インシデント対応の事例より

脅威の変化に伴い、対応組織側にもの変化が求められる。ここでは委託先社員より個人情報を含むデータが流出した企業における対応事例について、技術部門と組織管理部門の関わりという観点から分析する。

(1) 事象の概要

IT サービスを行う某企業 A の委託先社員の自宅より、Winny を通じて A 企業の顧客が保有する個人情報を含む過去プロジェクトのデータが万単位の規模で漏洩した。その後、漏洩した情報を入手し事実を把握した第三者が、匿名掲示板への投稿、マスメディアへの通報・リーク、share ネットワークへの情報の再放流等を行ったため、事態が大きくなり、企業 A においては、対策のための人件費、お詫び状送付費用、相談窓口設置関連費用、Winny/Share 上での情報拡散防止費用、弁護士費用等、その対応のために多くの期間と莫大なコストを要した。

(2) 事後対応

企業 A においては、情報漏洩を防止するための仕組みや規定はあったが、機能していない点があった。そのため、以下の対策を改めて実施し、各種技術的な対策も再度徹底させた。

- トップダウンにより、個人情報流出の影響の大きさを全員に理解させる
- 自社だけでなく、委託先も含めて考える

---

[3] 第 1 回 DM-WG 有村構成員資料（P6）
[4] 第 1 回 DM-WG 有村構成員資料（P7）

・ 過去持ち帰った個人情報、機密情報の消去、返却を徹底する
・ 個人情報や機密情報の保存状況を調査し、情報の削除や暗号化を徹底する

(3) インシデント対応における課題と有効な対策

本事例においてインシデント対応が困難だった点は、

・ 技術的内容が複雑であり容易に理解できない
・ 組織の分業化によって個別対処となり全体を取りまとめることが難しい
・ 真実の追究によって責任の所在が明確化できるかわからない

という点が挙げられる。

しかし、本事例では、情報が流出した企業 A の顧客が被害者に丁寧に対応し、企業 A は IT に関わる技術面でのサポートに注力した。最終的に、企業 A は顧客に対し損害賠償を支払ったが、事後対応が有効であったこともあり、早期に合意するに至った。

また、企業 A において、平時は CISO (Chief Information Security Officer：情報セキュリティ最高責任者) をトップとした情報セキュリティを推進組織の中に、セキュリティ技術専門部隊が存在しているが、本事例では、図 1-4 の通り、社内組織を取りまとめる役割を果たすために、情報セキュリティ専門部門が事象対応における主たる組織である意志決定会議と連携し、全体取りまとめにおいて重要な役割を果たした。

さらに、企業 A の本社は米国にあるが、日本の事例に対しても協力的だった点は、トップダウンで対応を進める上で非常に有効であった。企業 A のポリシーとして社会貢献が大前提としてあるため、漏洩した情報の再放流者への毅然とした対応によって日本の winny 等を通じた漏洩情報の拡散に関わる状況の変革を期待した点があったという。関係組織において、インシデント対応のインセンティブとなる理由が双方で一致しなくとも、win-win 関係が構築できるケースもある。

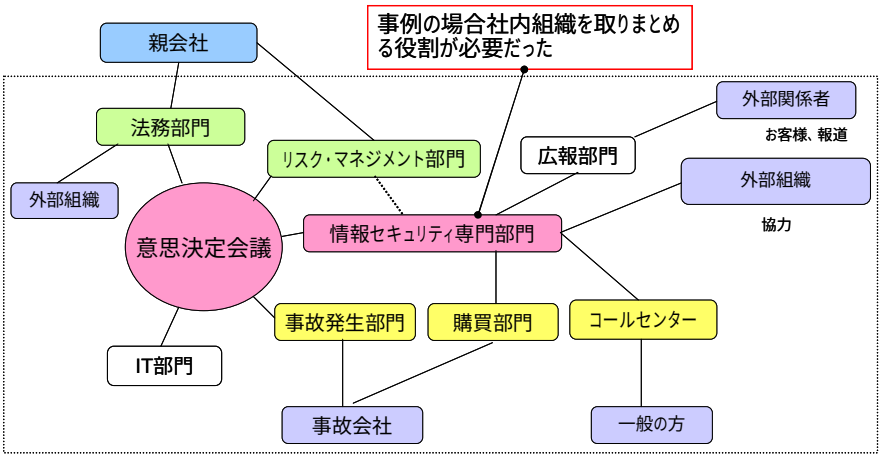


図 1-4 某インシデント事例における関係組織の全体像

1.2. 技術専門部署における課題

1.2.1. 技術専門部署の役割変化

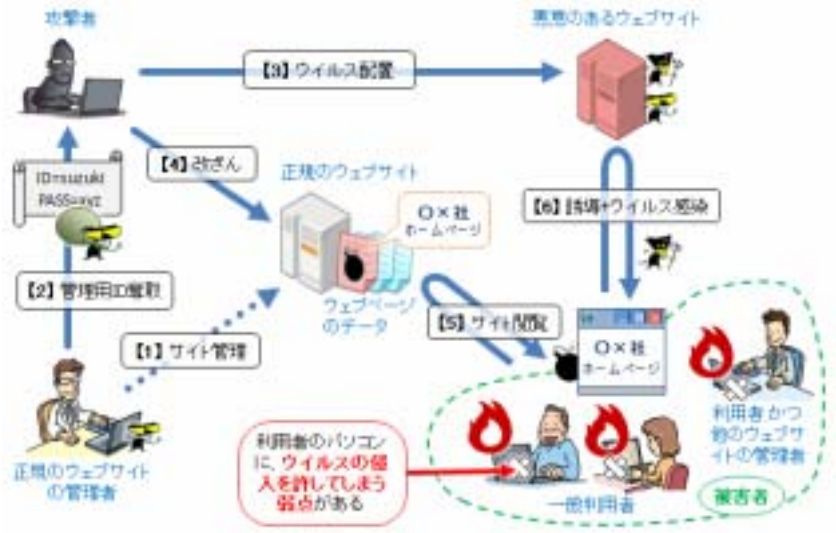
技術専門部署の役割について、Gumblar によるインシデント対応の問題を基に検証する。

Gumblar とは、特定のウイルスを指すものではなく、攻撃者が複数の攻撃手段を併用し、多数のパソコンに様々なウイルスを感染させようとするために使う一連の手口のことである。株式会社ラックの発表[5]では、2009 年は年間を通じて Web サイトの改ざんを狙った攻撃が多く発生しており、上半期は SQL インジェクションなどの外部から直接 Web サイトを改ざんする攻撃が多く検知されたが、下半期は Conficker や Gumblar 等、Web サイト管理者の FTP アカウントを窃取する被害が増えており、特に下半期は Gumblar による複数企業の Web サイト改ざんの被害が報告されている。

Gumblar は次の点でこれまでのインシデントとは異なる問題を提示した。

- Web サイトのコンテンツ管理に用いる FTP 等のサービス基盤が脅威の拡大や伝搬に利用された。
- Web サイトの管理体制が多様化しており、複数の部署や委託先に権限や責任がまたがっていたため、対処や原因究明が非常に難しい。

こうした基盤が今後攻撃そのものに悪用される可能性についても十分警戒する必要がある。



資料：情報処理推進機構「コンピュータウイルス・不正アクセスの届出状況[1 月分]について」[6]

図 1-5 Gumblar の全体図

[5] http://www.lac.co.jp/news/press20100317.html

[6] http://www.ipa.go.jp/security/txt/2010/02outline.html

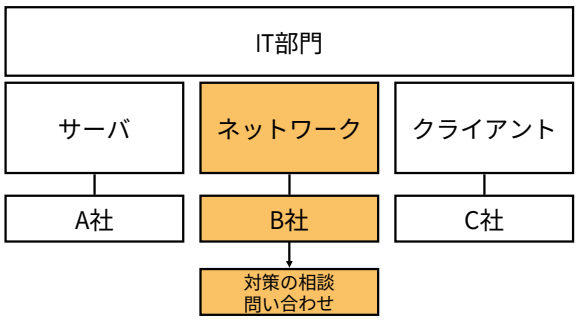
Gumblar については、それぞれ攻撃に利用する脆弱性やサイト構成が異なるため、対応が非常に困難である。対策が困難点については、以下が挙げられる。[7]

a) クライアントアプリのアップデート
- 使用しているソフトウェアが脆弱性問題に対応したものをリリースしていない
- アップデート方法がわかりにくい
- 業務アプリケーションとの関係でアップデートができない
- ウイルス対策ソフトのみに依存している

b) 予防策と事後策への対応
- メーカは「やられないため」の対策を提供
- 「やられたこと」を発見する対策は自己否定に繋がる可能性
- 事後策はシステムのみで対応しにくく、製品に実装しにくい

> ○メーカ：脆弱性ごとに対応するシグネチャを開発
> (例) MS の脆弱性への攻撃、Apache の脆弱性への攻撃 → 予防策
> ○JSOC：起きうるインシデントごとに対応するシグネチャを開発
> (例) ボット感染通信、攻撃が成功した通信 → 事後策

c) 対策ポイントの偏り
- 担当メーカにセキュリティ対策を任せた場合、対策に偏りができる
- IT 部門をスリム化しすぎて、全体のバランスを考えられる人がいない
- その結果、各ベンダが提案するものをそのまま実施することになる
- 本来は全体のバランスを考えて対策を打たなければならない



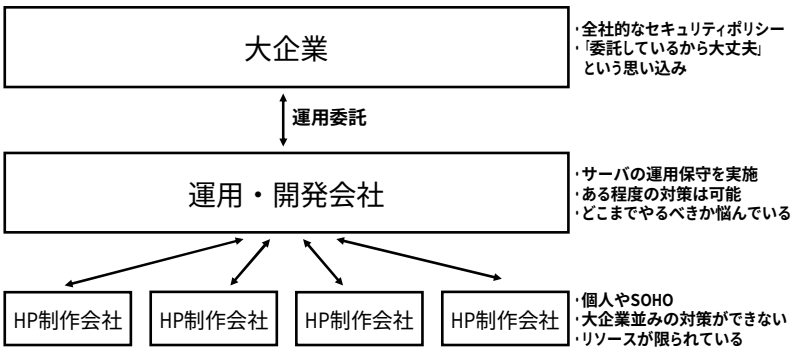
資料：株式会社ラック

図 1-6 Gumblar 対策における組織の切り分け

[7] 第 2 回 DM-WG 株式会社ラック・川口洋氏資料 (P11-15)

d) セキュリティ対策のコストと企業の体力

- HP 制作会社に大企業の求める対策を実施できる体力があるとは限らない
- それでも求められた場合、「やっている」と言わざるを得ない
- 「建前」だけで形骸化している企業でインシデントが発生



資料：株式会社ラック

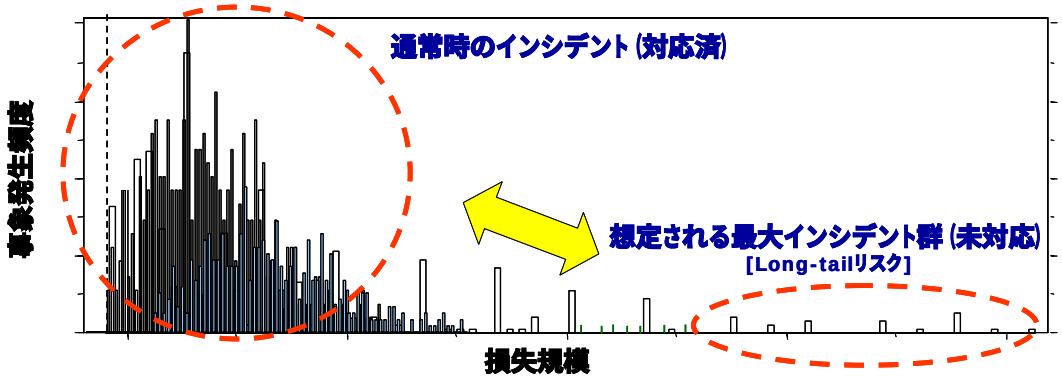
図 1-7 Gumblar 被害を受けた企業の構造

Gumblar 被害においては、関連する組織が企業内外で複数に分かれることから、原因究明が非常に難しい。多くの組織において、システム開発形態はマルチベンダとなっており、効率化やコスト最適化の観点からマルチベンダ自体には問題はないが、インシデントの発生時、どこに問題があるか、対策をどうするか等、全体を考えられる人がいないことが問題である。経営者なり CISO なりが自社の Gumblar 対策状況について確認しようにも、情報システム部門の人員が少なく多忙のため、関係組織からの「大丈夫である」という報告だけ受けて終わっているのが多くの実態であるという。これらの問題に関して、情報システム部門が対応するのか、あるいは組織における戦力の再配分が必要なのかは、企業の状況次第で異なるが、組織として対応策を検討する必要がある。

また、このような事象発生時の技術専門部署の課題としては、リスクの高い事件事故に協力を得ることが難しい、その事象に対して対応を実施した後の再発防止に設備にかける資金がない、すなわち 2 度と事故は起こらないという前提になっていることが挙げられる。また、非常時に技術専門部署が組織間のコーディネーションを行う機能を果たす場合は、事務局としての役割が多く、技術的な対応である解析等にかける時間の確保が難しいということもある。

これまで深刻な情報セキュリティインシデントへの対応が十分でなかったことから、技術専門部署の必要性が顕在化した。しかし、そうした大規模な事象は頻発するものではないため、そのためだけに存在する組織は成立しにくいという問題もある。

機器の故障やシステム不調など、通常のITトラブルについては既存のサポート部署が対応しており、技術専門部署との関係について柔軟に考える必要がある。



資料:第 3 回 DM-WG　渡辺主査資料(P14)

図 1-8　インシデントの分布

1.2.2. インシデントの予兆に関する変化

技術専門部署における課題として、新たな脅威によるインシデント対応事例をもとに、予兆把握の必要性について述べる。

[Gumblar の事例[8]]

(a)　対応経緯

■注意喚起:社内向け(注意喚起メール)

- 2009 年 05 月 27 日　Gumblar / Martuz / Geno / JSRedir-R attack
- 2009 年 06 月 11 日　Gumblar / Martuz / Geno / JSRedir-R に関する(再)注意喚起
- 2009 年 10 月 27 日　Gumblar 亜種の活動に関する注意喚起
- 2009 年 10 月 29 日　マルウェア Win32/Daonol ならびにその亜種に関する注意喚起
- 2009 年 11 月 30 日　Gumblar 亜種の活動に関する注意喚起
- 2010 年 01 月 12 日　マルウェア Gumblar 感染拡大に関する注意喚起

■注意喚起:インターネット向け(社外向け Web サイト掲載)

- 2009 年 10 月 29 日　マルウェア Win32/Daonol ならびにその亜種に関する注意喚起
- 2010 年 01 月 12 日　Gumblar 感染拡大に関する注意喚起

(b)　課題

- 社内環境(安全)とインターネット環境(危険)のギャップ
- 管理下でのインシデント事例なし
- 報道の過熱化
- 外注／委託先への徹底方法(Winny 対策≠Gumblar 対策)

[8] 第 1 回 DM-WG　寺田構成員資料(P5)

【SSL を使用した DDoS 攻撃の事例[9]】

(a) 対応経緯

■2010 年 2 月 3 日　ポート 443/TCP に対し、不正形式の SSL 接続が大量に発生

- 約 2 万の接続が常時発生
- SSL 接続でネゴシエーションエラーで切断
- http はサービス継続可、https はサービス継続不可
- 攻撃の形態から「Pushdo による SSL を使用した DDoS 攻撃」と判断

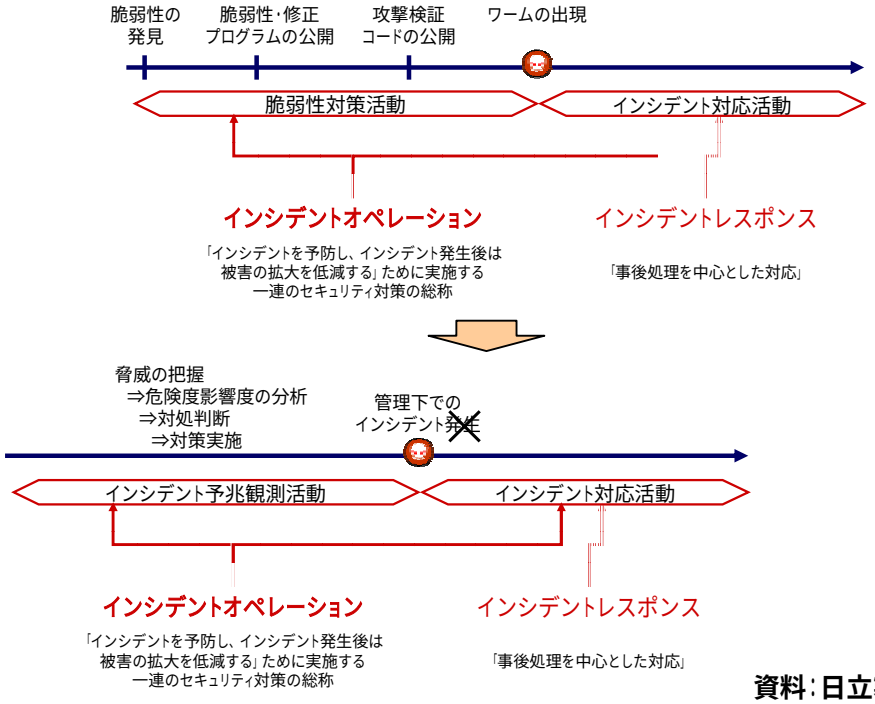
■2010 年 2 月 5 日

- 1 万 6 千程度の接続にまで低下

(b) 課題

- 注意喚起を出したいが、不確定要素が多いことから、現時点ではペンディング状態
- 「注意喚起」の意味や効果が昔と違っており、受け取る側のニーズも変わって来ている。

このように、インシデントレスポンスとは事後処理を中心とした対応となるが、事前予防活動としてのインシデントオペレーションをみると、従来のワーム世代では、インシデントの予兆は脆弱性発見であり、修正プログラムや攻撃検証コードの公開であった。しかし、新たな脅威に対しては、インシデントは局地的なインシデント発生から、脅威を把握し、危険度影響度の分析や対処判断、対策実施によってインシデントを予兆し、未然にインシデント発生を防ぐことが必要になっている。



資料：日立製作所[10]

図 1-9 インシデント(事故)の予兆に関する変化

[9] 第 1 回 DM-WG　寺田構成員資料 (P7)

[10] 第 1 回 DM-WG　寺田構成員資料 (P3-4)

1.2.3. 情報セキュリティのモチベーション構造

寺田らの研究[11]によると、情報セキュリティのモチベーションを構成する諸要因は以下のように定義できる。[12]

■動機要因 (6 因子)

- リスク管理：セキュリティリスクの管理
- 内部統制：内部犯行の防止や社員の被害からの保護
- 改善：監査指摘の改善、事故再発防止
- 取引先の要求：調達や取引先の要求
- 社会的責任：法令順守、社会的責任
- 競争優位：他社との差別化、対外的アピール、利害関係者の評価

■阻害要因 (5 因子)

- 技術・ノウハウ：情報セキュリティ対策に関する技術やノウハウ
- 手間・効率：業務効率低下や作業負荷
- 組織運営：経営者の関心のなさや業績向上への貢献
- コスト：予算確保の難しさや予算がないこと
- 理解・協力：社員への教育やルール順守の難しさ

たとえば、多数報道され注目されたケース（Gumbler 攻撃）とあまり注目されなかったケース（SSL を使用した DDoS 攻撃）でこれらを比較すると表 1-2 のようになる。

表 1-2 動機要因と阻害要因

分類	項目	注目された事例 （Gumblar攻撃）	注目されなかった事例 （SSLを使用したDDoS攻撃）
動機要因	リスク管理	サーバ、クライアント	サーバ
	内部統制		
	改善	管理下でのインシデント事例なし	管理下でのインシデント事例あり
	取引先の要求		
	社会的責任	報道の過熱化	
	競争優位		
阻害要因	技術・ノウハウ	対策あり	有効な施策不明
	手間・効率	外注／委託先への徹底方法	
	組織運営		
	コスト		
	理解・協力	社内とインターネット環境のギャップ	

資料：日立製作所

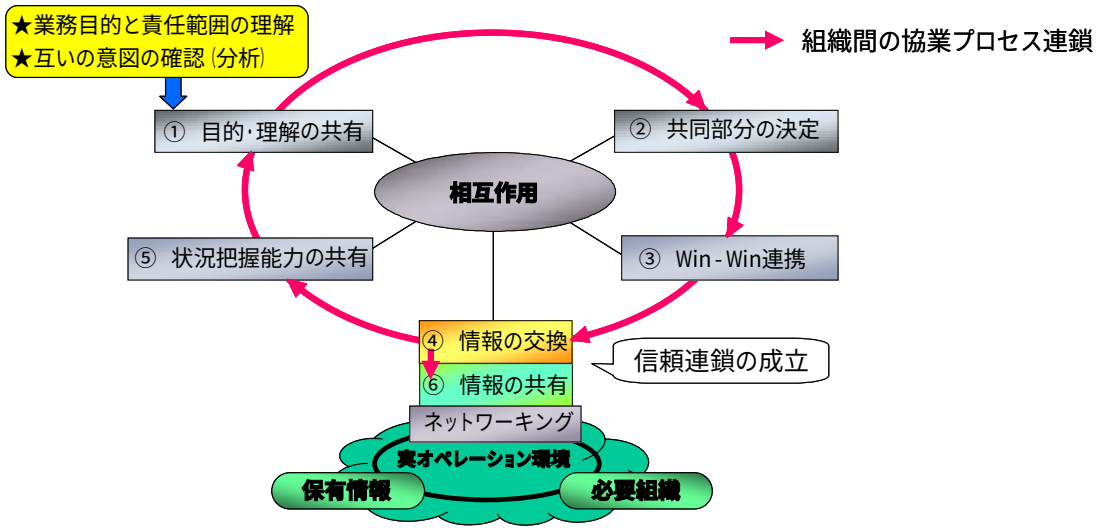
[11] 菅野泰子，寺田真敏，山田安秀，鎌倉稔成，土居範久："情報セキュリティ対策におけるモチベーションの構造に関する研究"，情報処理学会 コンピュータセキュリティ シンポジウム 2008, (Oct.8-10, 2008)

[12] 第 1 回 DM-WG 寺田構成員資料（P8-9）

1.2.4. 外部組織との接点

脅威の変化に伴い、単独組織としての対応だけではなく、外部組織との連携を踏まえての対応がより効果的なケースが増加しつつある。外部組織とのコラボレーションにおいては、**図 1-10** に示すように、双方の利害が一致すること、責任範囲を明確化できることを前提として、「目的･理解の共有」「共同部分の決定」「Win-Win 連携」「情報の交換」「状況把握能力の共有」を連鎖として回していくことが有効である。

サイバーセキュリティ分野においては、機密情報を扱う機会も多いため、円滑な情報共有の推進については課題となるケースが多い。情報共有のためには、組織としての連携に関して情報の取り扱いに関わる規則や手順等を定める必要があるのは当然のことながら、まず双方の利害が一致することが重要となる。もちろん、組織連携ありきではなく、外部組織との情報共有を手段とした効果的なインシデント対応の実現が目的であることは留意しなければならない。



資料：DM-WG 事務局

図 1-10 コラボレーション･プロセスの基本概念

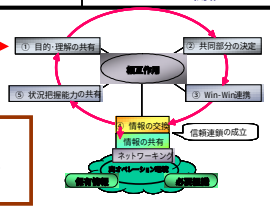
また、外部組織との連携が有効であることは間違いないが、現実には難しいことが多い。この問題の解決のためには、コラボレーションをする目的･理解を共有するための初期時点で、相手の出方がわかっていることが必要である。例えば、民間分野については、**表 1-3** のように、CCC ボット対策プロジェクトや Gumblar 対応等において ISP の連携事例がある。このときの複数 ISP の共通の目的は、前者では「ボットによる攻撃からの設備保護」、後者では「苦情申告の急増や ftp アカウントの ISP 管理サーバからの流出疑惑」であり、これらが共有できたために、競合会社であっても ISP としてのコラボレーションができたと考えられる。民間分野の競合他社間における連携は、一般的には難しいが利害の一致や双方の責任範囲が明確化できれば連携も可能であるし、逆に、重要インフラ分野等、類似技術利用業界であっても、異業種では連携が難しいと言える。

表 1-3 Telecom-ISAC Japan のコラボレーション・プロセス

T-ISAC-J 活動事例	コラボレーション・プロセスのステップ				
	① 目的・理解の共有	② 共同部分の決定	③ Win-Win連携	④ 情報の交換	⑤ 状況把握能力の共有
DDoS攻撃緊急対処のためのブラックホール共同設定	DDoS攻撃への緊急対処	攻撃データ廃棄の共同実施 通信データ廃棄対象のアドレス情報	緊急避難的実施にあたっての監督官庁との調整（お墨付き確保） 対処要請受領に合わせた共同作業	攻撃状況と効果	共同連携スキームの整備
CCCボット対策プロジェクト	ボットによる攻撃からの設備保護	ボット感染状況実態調査 ボット駆除方法の検討	共同注意喚起	ハニーポット攻撃状況 注意喚起効果 問題点・改善案 感染ユーザ対応ノウハウ	ボット感染状況
BGP経路ハイジャック監視	事象発生の速やかな発見、速やかな対処をしたい （特に）某社がよくハイジャックされていた。ある時、ハイジャックを受けていなかった別の事業者が受けて対策に手間取った。	ハイジャックは外から見ていないと分かりづらいことに気づいた。 BGP経路運用上の問題解決	外部に（共有の）経路監視システムを作ろう	経路情報・ハイジャック事象の共同蓄積	ハイジャック件数・状況の共有、ハイジャック発生時のアラーム通知、復旧連携
Gumbler対応	苦情申告の急増 ftpアカウントのISP管理サーバからの流出疑惑	ftp送信元状況の分析	疑惑のftp送信元IPアドレスリスト提供	改ざんスクリプト アクセス状況 海外アドレス／国内アドレス区分 アドレスブロック対処効果	Web改ざん抑止効果 アカウントクラック問題への注目 包括的な感染防止策検討の機運醸成 ラウンドテーブル開催

①の起動スイッチがありそう
①の初期時点で相手の出方がわかっていることが必要らしい

①の起動スイッチ



民間分野については
だから、競合会社であっても同業業界だからできた。
だから、類似技術利用業界であっても異業種では連携が難しい

組み合わせ論的には
政府分野と民間分野のコラボについても同様か？

資料：Telecom-ISAC Japan[13]

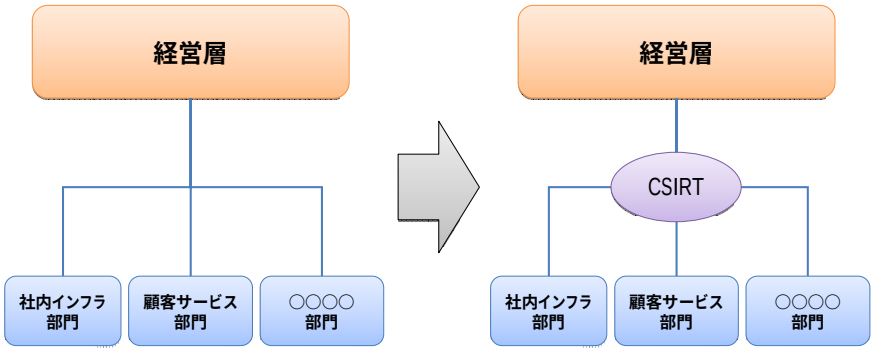
官民連携についても、同様の考え方で連携を推進できる可能性がある。外部組織においては、各目的特性が存在するため、連携の相手によって、連携のあり方が異なってくることが考えられる。例えば、CND の観点で守るべきものはどんな対象にとっても情報資産であるが、リソース・スキルレベルからみて自衛的に自己を守りきれない個人・中小企業は、ISP にとって事業継続上の脅威である。情報セキュリティに係る脅威と問題の変質に伴い、これらの対象に対して継続的に対策を行うため、継続的活動を担保する組織構築が必要となる。継続的組織の維持には、活動に要する資金の継続的な調達・リソース確保が担保されることが必要となるが、経済活動基づく場合、そ景気に左右されるなどして、継続が確約出来ない場合がある。資金を含む継続的なリソース確保のためには、このような対策の実施根拠に非競争領域分野的発想・準公共財的発想を政策戦略的に導入することが今後必要になってくるかもしれない。

[13] 第 1 回 DM-WG 有村構成員資料（P9）

日本の風土に合った技術専門部署の概念

組織において、サイバーセキュリティに関わるインシデントが発生した際に技術的な対応を行う代表的な技術専門部署は CSIRT（Computer Security Incindet Response Team：コンピュータセキュリティ緊急対応体制）がある。CSIRT の一般的な定義としては、コンピュータセキュリティインシデントの情報収集、調査、対応を行うサービス組織とされている。

日本企業における CSIRT 構築のメリットとして、たとえば経営層に対するコンピュータセキュリティに関わる窓口を一本化できると見方があった。図 1-11 のように、各部署が別々に行っていたインシデント対応を CSIRT に一本化することで対応の効率化が図られ、経営層に報告する情報の集中管理を行うというイメージである。



資料：サイバーディフェンス研究所[14]

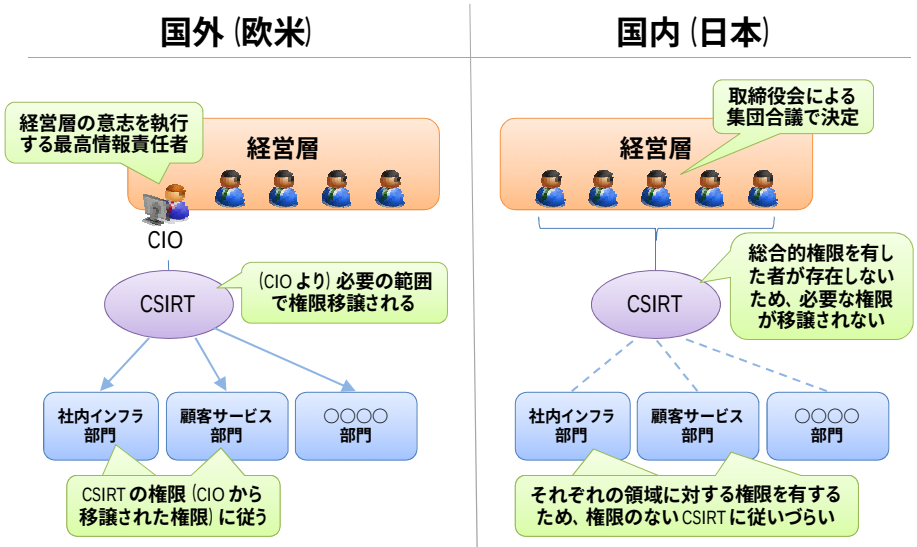
図 1-11 CSIRT 構築の概念

日本では、1996 年の JPCERT/CC 設立以来、2010 年 3 月時点で 15 の CISRT が日本シーサート協議会に加盟しているが、現在、いくつかの問題が指摘されている。具体的には、実際には CSIRT が米国から来た概念であるため、日本の組織においては、CSIRT が本来の設立目的を果たし、効果的に活動することが難しい点、経営層からの理解を得るのが難しい点、また、既存の IT 関連部門との業務の役割と責任の切り分けが難しいという点が挙げられる。

米国では、経営層の意志を執行する CIO から必要な範囲で権限委譲された CSIRT が、その委託権限によって各部門を動かすことが可能だが、日本では CSIRT に総合的権限を有した者が存在せず、各部門もそれぞれの領域において権限を有するため、権限のない CSIRT には従いづらい。

また、ホストコンピュータ～クラサバ時代は、日本企業にも社内に IT 専門家がいて、情報システム部門が企業内の情報システムの設計・製造を行っていたが、設計・製造・運用が一体化してから、情報システム部門は具材調達の一部門の要素が大きくなってきた。分割発注によるノウハウの外部移行による結果の組織特性の問題もあり、各部門の取りまとめをする部分の機能が失われているという事情もある。

[14] 第 2 回 DM-WG 名和構成員資料（P2）



資料：サイバーディフェンス研究所資料[15]（一部 MRI 修正）

図 1-12 構築された CSIRT の権限の違い

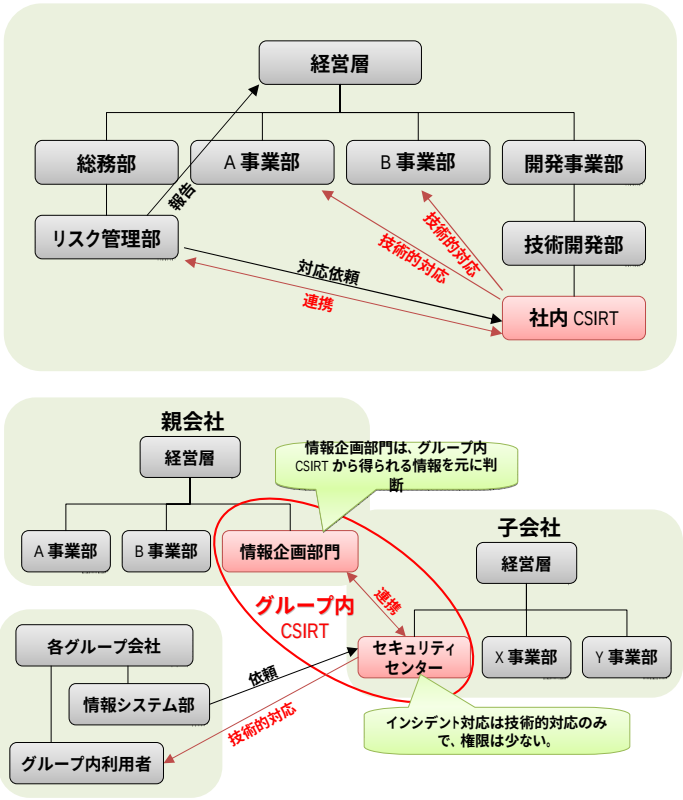
一方、国内においては、災害大国と言われるほど自然災害に対する緊急対応の経験が豊かであり、多くの企業は独自のノウハウや、社内における非常時の対応にかかる仕組みや体制を有している事が少なくない。また、日本における企業内の部署は、それぞれの領域において一定レベルの権限を有し、発生したインシデントに対して、自助努力で解決しようとする姿勢を持っている。このことは、インシデント対応を円滑かつ有効に実施する上で大きな強みとなっている。

しかし、最近はインシデントの高度化・複雑化がさらに進んでおり、企業において技術的な対応に関する支援が必要になってきている。

そのため、CSIRT は、社内において非常時の対応にかかる仕組みに組み込まれた一つの機能として、技術的面に特化したサービスを提供する部署や体制の形で構築されることが多くなっている。

このように、日本における CSIRT は、海外における CSIRT 概念とは毛色が異なる独特の特徴を持つことに留意しなければならない。20 年前、米国から輸入した CSIRT の概念をそのまま適用しようとして、無理が生じているのが現状である。

[15] 第 2 回 DM-WG 名和構成員資料（P3）



資料：サイバーディフェンス研究所[16]

図 1-13 最近、国内で多く見られる CSIRT

現実的にインシデント対応を行うためには、CSIRT が問題定義をしっかりしないと各組織からの協力が得づらい。CSIRT が問題を問題として認識できるように定義する必要がある。その上で、組織全体を動かすために、利害が一致すること、責任範囲を明確化できることを前提として、共通の目的や目標を作ること、そして各部署が自身のリスクを認識し排除していくこと、外部の協力を得る必要があるかどうか検討することが重要である。

また、技術専門部署の組織体制は情報システム部門でも CSIRT でも構わないが、平時から何らかの役割を果たしていかないと、組織として成り立たない。その結果、日常的なトラブルに対応するサポートセンターと情報セキュリティインシデントに対応する CSIRT の境界が曖昧になってきている。いずれにせよ、平時のトラブルにも想定外の事件事故の場合にも柔軟に対応できる組織を構築していくことが必要である。

日本における主な特徴・特性における技術専門部署の分類を以下に示す。

【タイプ 1：限定的な技術情報提供組織】

全社的なインシデント対応は、経営層や総務部門、非常時にアドホックに構築されるリスク対応

[16] 第 2 回 DM-WG 名和構成員資料 (P4-5)

組織が主体となって行い、情報システム部門の一部もしくは情報システム部門と連携することで、インシデントの原因究明、復旧、再発防止策等に関するコンピュータセキュリティに係わる技術的な情報を経営層や主たるインシデント対応組織に報告する組織体系。IT を本業としない企業。

【タイプ 2：統合的な情報管理組織】

全社的なインシデント対応は、総務部門や非常時にアドホックに構築されるリスク対応組織が主体となって行うが、組織の各部署で保有するインシデントの原因究明、復旧、再発防止策等に関するコンピュータセキュリティに係わる技術的情報を一括して取りまとめ、主たるインシデント対応組織に報告する組織体系。技術専門部署と各部署との連携関係を日常から構築しており、IT や IT に関わる製品・サービス提供が本業、もしくは業務と情報システムの関係が深い企業。

【タイプ 3：グループ横断的対応組織】

脅威情報や脆弱性情報、対応に関わる情報など、様々なコンピュータセキュリティに関する情報をグループ全体として取得し、必要に応じて各グループ企業に情報提供を行う組織体系。インシデント発生時は、インシデントの影響範囲に応じて、関連する各企業への情報提供のほか、実際のインシデント対応に関しても各企業の担当部署と連携しながら行う。IT や IT に関わる製品・サービス提供が本業であり、一定程度のグループ規模を持つ企業。

【タイプ 4：外部連携重視組織】

自組織だけでは対応できないインシデントに対して、国内外の技術専門部署組織と連携を行うことが重視される組織体系。ISP や通信事業者等、限定された業種。

留意すべきは、技術専門組織ありきではなく、既存の組織体系やビジネスの特性、企業文化を踏まえ、組織全体のリスクコントロールが目的である点である。いずれの組織体系であろうと、技術専門部署構築のメリットとして主に以下の点が挙げられるため、動的判断モデルチャートの例を基に、これらのメリットを享受するための組織体制及び手順を構築することが望ましい。

＜主な技術専門部署構築のメリット＞

- 情報セキュリティにかかるグループ企業の統制
- ビジネス展開の足がかり（特に海外向け展開）
- 顧客に対する「情報セキュリティの安心・安全」のメッセージ
- 組織内の横断モデル及びエスカレーションの実現
  （組織の横串的調整能力の基盤整備）
- 関係機関に向けた情報セキュリティの取り組みに関するアピール
- 他社との共通問題の解決、コミュニティへの参加
  （事実上の外部との情報体制が実現）

・　同じ悩みを抱える担当者間の情報交流

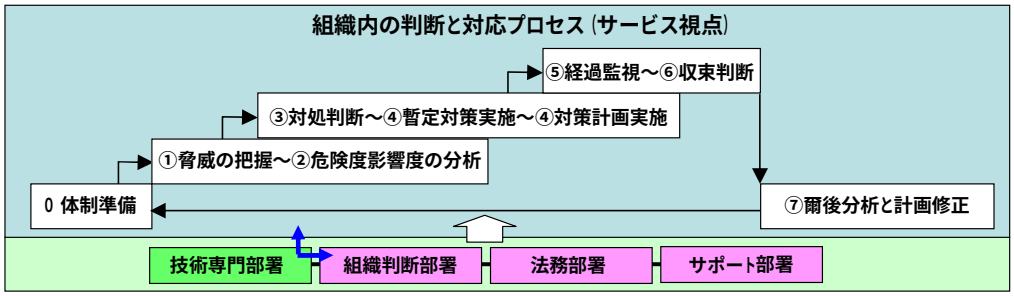
ただし、このような技術専門部署が有効に機能している組織においては、実態として、際立った能力を持つ専門家、すなわち、セキュリティに関わる技術的な知識を熟知している、もしくは知識に対するインデックスを持つ人材が、並外れた馬力で支えているケースが少なくない。技術専門部署の取り扱う領域が広い場合や、サイバーセキュリティの要素がビジネスにおいて非常に大きい企業においては、特定の人材に依存することによるリスクにも配慮する必要がある。半面、個性的な人材を際立たせることで、経営層から見えやすくする効果も期待できる。日本独特の企業における組織体制と企業文化を踏まえた機能分解を行い、日本流の技術専門部署のあり方についてさらに検討する必要がある。

2. 組織対応のセオリー

2.1. 組織の対応モデル

2.1.1. 動的判断モデル

サイバーセキュリティに係わるインシデント対応体制や技術専門組織の位置付け・役割については、ビジネスにおけるサイバーセキュリティに係わるリスクの大きさ、業務における情報システムへの依存度、情報システムやサイバーセキュリティ関連人材の保有状況、既存のリスク管理体制の成熟度等によって異なる。このような技術専門部署における役割を、インシデント発生時の組織内の判断と対応プロセスをサービス視点から整理すると、図 2-1 **エラー! 参照元が見つかりません。**となる。



資料：DM-WG 事務局

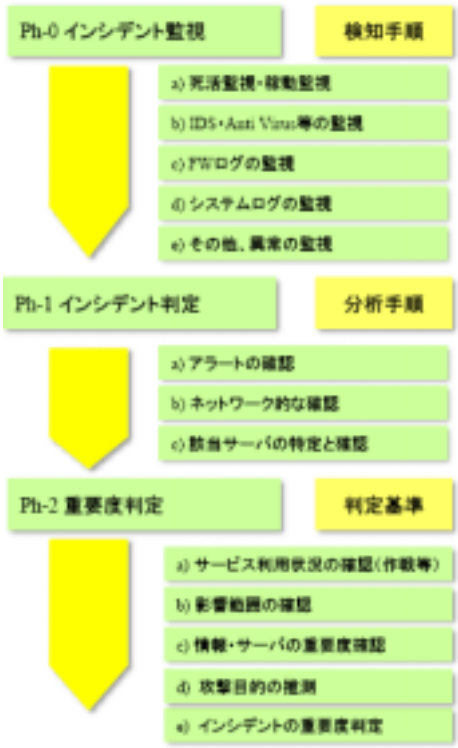
図 2-1 組織内の判断と対応プロセス

一般に、インシデントの対処は、通常の監視業務を通じてインシデントを検出し、重要度を判定する「監視フェーズ」、暫定的な対処や被害状況の分析、再発防止策の立案を行う「一次対応フェーズ」、被害を受けたシステム等の復旧を行う「二次対応フェーズ」の3つのフェーズに分かれる。

(1) 監視フェーズ

監視フェーズでは、稼働状況やシステムログ、ウイルス・不正アクセスの侵入等を日常的に監視する監視業務を実施していることが前提となる。この監視業務を通じて、セキュリティイベントが検出される。 イベントが検出された場合、それが誤検知でないか（実際にインシデントが発生しているのか）をアラートの内容から判定する。

インシデントと判定された場合、そのインシデントの重要度を算定する。重要度の算定にあたっては、影響範囲や、攻撃の目的等を基本として算定する。



資料：マイクロソフト

図 2-2 監視フェーズのフロー[17]

(2) 一次対応フェーズ

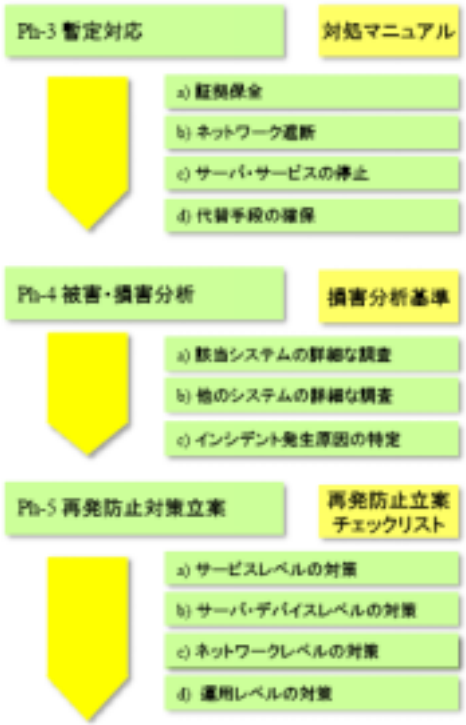
一次対応フェーズでは、対処マニュアルに基づく暫定対応、被害・損害の分析、再発防止策の立案を行う。

インシデントにより作戦指示やその他の運用に支障が出ている場合、暫定対応として、被害の拡大を抑止するための対策や代替手段の確保を行う。インシデントの重要度によっては、機能回復を優先させるなど、トリアージ（選別）を行い、対処の優先度を設定する必要がある。

被害・損害の分析では、該当システム、周辺のシステム、同様の構成を持ったシステムについて詳細な調査を行い、発生原因の特定と、影響範囲の特定を行う。

さらに、上記分析結果に基づき、再発防止策を立案する。技術的な対策が行えない場合、運用を含めて再発の防止または、再発の際に被害を最小限にとどめるための対策を立案する。

[17] 第 1 回 MAP-WG 高橋構成員資料（P24）



資料：マイクロソフト

図 2-3 一次対応フェーズのフロー[18]

(3) 二次対応フェーズ

二次対応フェーズでは、復旧作業、再発防止策の実施および事後処理を行う。

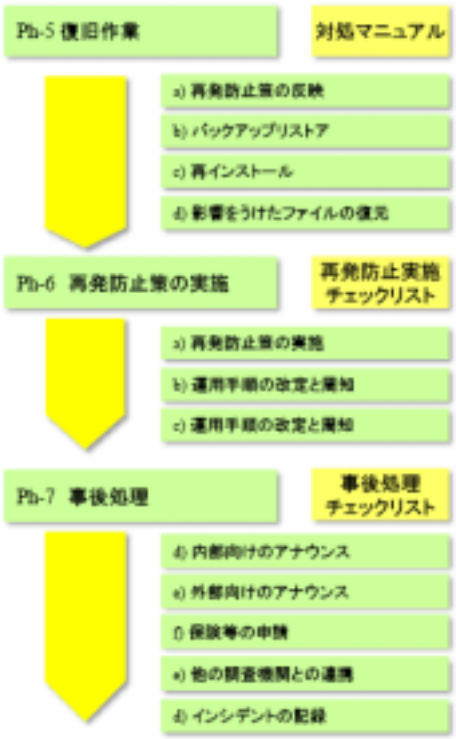
まず、分析内容に基づき、復旧作業を行う。明確に影響がない場合を除き、システムの再インストールを行う。また、影響を受けたファイルは、最新のバックアップデータに基づき復元する。

被害を受けたシステムの復旧にとどまらず、立案した再発防止策を迅速に実装する。

さらに、技術的・運用的な復旧に加えて、内部・外部の利用者へのアナウンス、ベンダとの連絡、保険等の処理を実施する。状況により、他の組織と連携が必要な場合もこの対処を行う。

インシデント対応に係る一連の作業や指示、その結果は、確実に記録として残し、蓄積する。

[18]第 1 回 MAP-WG 高橋構成員資料（P25）



資料：マイクロソフト

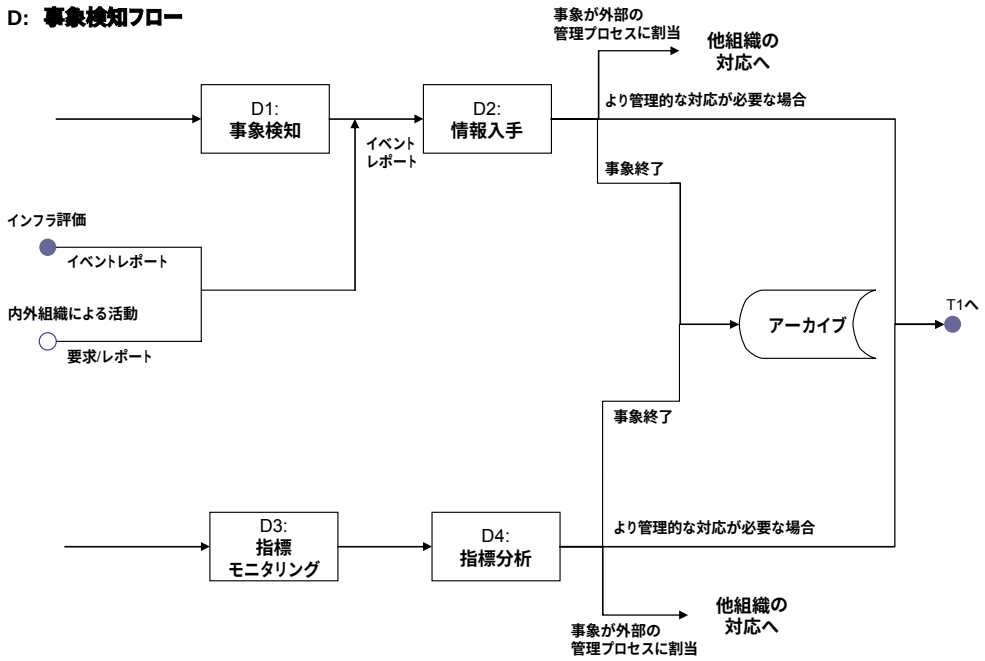
図 2-4 二次対応フェーズのフロー[19]

以下に、上記のモデルを前提とした、組織における動的判断モデルの詳細例として、米国型 CSIRT のモデルに基づく「事象検知」「トリアージ」「対応」「技術的対応」のチャートを示す。

【事象検知フロー】

疑わしい、あるいは非日常的な動きが検知された場合、または、アドバイザリやアラート等が上がった際の対応が事象検知フローである。この場合、技術専門部署や技術専門部署関係者のミッションに関連する非日常的な動きを特定し、時間的制約の中、適切な機密管理の下、対応を行うことが重要である。

[19]第 1 回 MAP-WG 高橋構成員資料（P26）

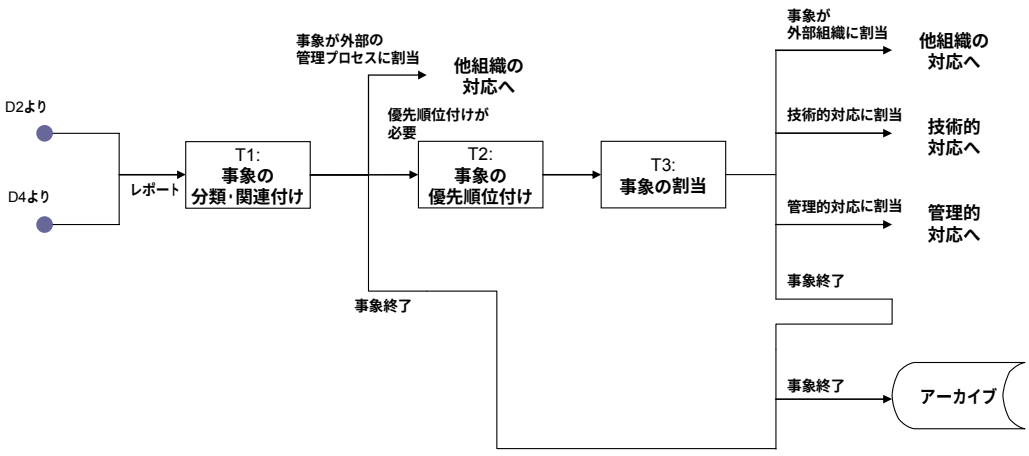


資料：CMU-SEI-2004-TR-015 を基に MRI 作成

図 2-1 動的判断モデルチャートの例：事象検知フロー

【トリアージフロー】

イベント情報の到着がトリガーとなり、イベント情報を分類し、適切な人間に割り当てるのがトリアージフローである。この場合、時間的制約の中、適切な機密管理の下、適切な書式により対応を行うことが重要である。



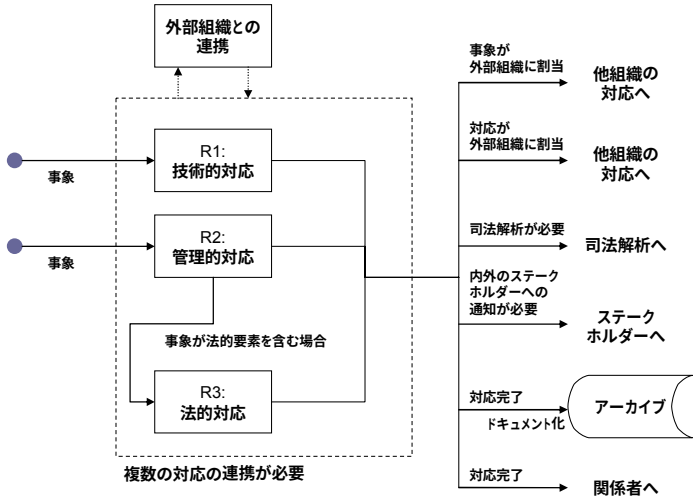
資料：CMU-SEI-2004-TR-015 を基に MRI 作成

図 2-2 動的判断モデルチャートの例：トリアージフロー

【対応フロー】

各自に割り当てられたイベントが到着した場合の対応が対応フローである。この場合、時間的制約の中、セキュリティ面や法的･捜査的な観点から適切な情報管理の下、規定されたポリシーや手順、品質要求に基づいた対応を行うことが重要である。

R: 対応フロー

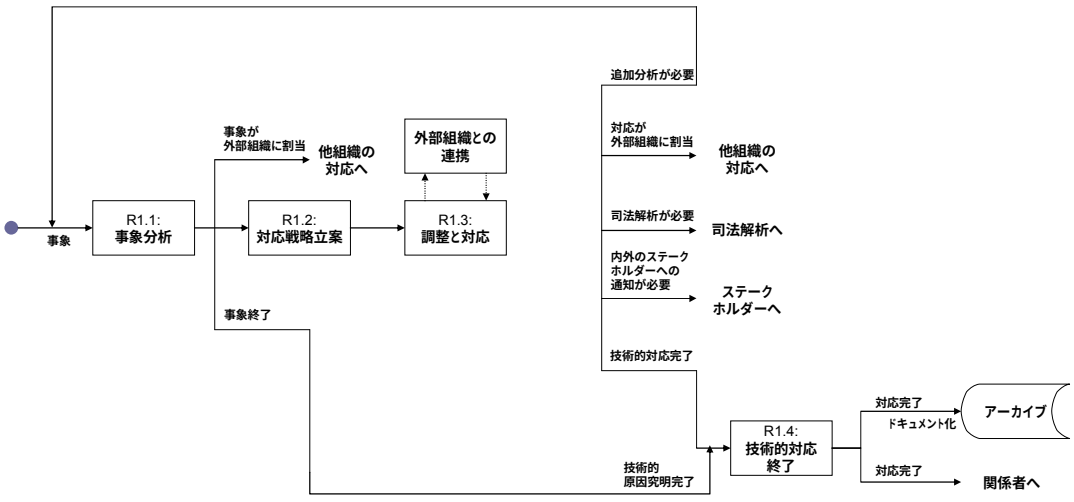


資料：CMU-SEI-2004-TR-015 を基に MRI 作成

図 2-3 動的判断モデルチャートの例：対応フロー

対応フローには、対応内容によって、技術的対応、組織管理的対応、法的対応等がある。技術的対応の際には、 指定された担当者が各イベントについて適切に計画･分析し、関係サイトやその他の関係者間の調整の下、適切な技術的対応を行う。

R1: 技術的対応フロー



資料：CMU-SEI-2004-TR-015 を基に MRI 作成

図 2-4 動的判断モデルチャートの例：技術的対応フロー

2.1.2. 動的判断モデルに基づく運用の成否の要件分析

組織リスクに関する動的判断を下す際、単純に情報システムのダメージだけで判断していては、組織としての被害を抑制することに寄与できない可能性がある。そこで、動的判断の指標として、経営への影響を採り上げる考え方がある。表 2-1 に、組織としての被害規模の段階的な目安の例を示す。

表 2-1 組織リスクに関する動的判断の際の指標イメージの例[20]

資料：津森信也、大石正明「経営者のためのトータルリスク管理」 中央経済社

また、動的判断モデルチャートが有効に機能するためには、インシデント発生時に何が起きているのか、何を守らなければならないか、何を判断しなければならないか、何の情報をどう使うのかについて、各部門が共有していることが重要である。インシデント対応時の各部門の目的と必要な情報の一例を、表 2-2 に示す。

表 2-2 インシデント対応時の各部門の協力体制と必要な情報

組織	個別の目的	協力阻害要因	必要な情報
本社	信頼の回復	高コスト	何が問題なのか
法務部門	信頼の回復	高コスト	証拠となる事実・情報
ﾘｽｸﾏﾈｼﾞﾒﾝﾄ部門	再発防止	情報セキュリティ部門との重複	発生原因
広報部門	適切な情報公開	知らない人に知らせること	対応の進捗
情報セキュリティ部門	根本原因と真実の追究	真実を認めない	調査の技術
事故発生部門	お客様との関係修復	お客様の不利益	対応の進捗
購買部門	―	契約書変更など	具体的な内容
コールセンター	―	判断を伴う対応	技術のサポート 情報の伝え方
IT部門	効果的なシステムの導入	作業の発生	発生原因

資料：IBM 資料[21] (一部 MRI 変更)

[20] 第一回 MAP-WG 高橋構成員資料(P21)

2.2. 技術専門部署の役割と提供情報

2.2.1. 事業継続におけるサイバーセキュリティの考え方

日本企業ではサイバーセキュリティに関する脅威より自然災害等に関わる脅威に対するリスクマネジメント体制が発達していたことから、企業におけるリスク管理体制は、経営層・総務部門・法務部門・広報部門・情報システム部門等、各関係部署間で既に構築された手順・体制が存在するケースがほとんどである。

BCP（Business Continuity Plan：事業継続計画）においては、自然災害・新型インフルエンザ・IT障害、脅威の種類に寄らず、非常時は業務の継続について重要業務に集中することが重要となる。通常業務のうち重要業務を選定し、その他を一部縮小業務、休止業務に選別する。また、インシデント発生によって、インシデント対応や行政・取引先・マスコミ等との連絡調整など、新たに発生する業務もある。重要と選定された通常業務の一部と、新たに発生する業務を合わせて「重要業務」とする。

本社で重要業務に選定される可能性が高い業務の一例としては、支払・決済、決算、物流、受発注、従業員への給与支払い、関係会社への融資、資産運用業務、与信管理、システム継続等が挙げられる。業務への影響は経営層の判断であり、被害規模に応じて柔軟に対応を変えていく必要がある。重要か否かの判断は、例えば年度末では決算業務が重要になる等、時期や曜日、日時によって重要業務が異なる場合もある。また、事業をいつ再開すべきかという問題についても、経営層がきちんと認識していく必要がある。

企業存続を揺るがすような事例では、組織体制や BCM（Business Continuity Managemnet：事業継続管理）の取り組みにおいて、一般的な災害とサイバーセキュリティで共通項があるため、BCP の考え方はそのままサイバーセキュリティに関わるインシデント対応を検討する上でも適用可能である。ただし、例えば情報漏洩では、流出データが本業に近いと事業への影響がわかりやすいが、そうでない場合は事業への影響がわかりづらい。特に、サイバーセキュリティに係わる CND の場合には、インプットされるイベントと結果の関係がわかりにくい点が課題である。

2.2.2. 技術専門部署において必要な情報

(1) 重要業務の検討

BCP の観点では、経済産業省「事業継続計画策定ガイドライン」において、BCP が発動された場合の各フェーズの実施項目として

[21] 第 2 回 DM-WG 徳田構成員資料（P8）

表 2-3 の項目が推奨されている。

これらの推奨項目は一例であるが、BCP 発動時の全社的な対応事項、そして各関係部署の役割を認識しておくことは、技術専門部署として、関係部署や経営層等の主たる対応組織、あるいは外部に対して適切な情報提供を行うにあたり、適切かつ効率的な判断を実施することが可能となる。

表 2-3 BCP の各フェーズにおける実施項目

BCP 発動フェーズ	・発生事象の確認 ・対策本部設置 ・各対策チーム（部門）の設置 ・安全確保、安否確認 ・要員の配置 ・被害状況の確認 ・業務影響の確認 ・基本方針の決定 ・対応の優先順位の決定 ・復旧目標の決定 ・初期対応の実施 ・リスクコミュニケーションの実施
業務再開フェーズ	・人的資源の確保 ・物的資源の確保 ・代替オフィスの確保 ・業務再開範囲の確認 ・代替運用の開始 ・復旧作業の実施 ・復旧目処の確認 ・運用上の留意事項 ・リスクコミュニケーションの実施
業務回復フェーズ	・業務継続の影響確認 ・復旧状況の確認 ・追加資源投入の検討、実施 ・更なる業務縮退の検討、実施 ・継続業務の拡大の検討、実施 ・復旧作業の実施 ・復旧目処の確認 ・全面復旧のタイミングの決定 ・復旧に向けた資源再配置の計画 ・復旧後の制限の確認 ・リスクコミュニケーションの実施
全面復旧フェーズ	・復旧手順の確認 ・全面復旧の実施 ・資源の再配置 ・業務制限への対応 ・代替運用の本格的縮退 ・総括（被害状況のまとめ、利害関係者への影響のまとめ、再発防止策の検討、BCP の見直しの実施、サービスレベルアグリーメントの見直し、利害関係者への事後処理の実施、業績への影響の見極め） ・経営計画の見直し ・リスクコミュニケーションの実施

資料：経済産業省「事業継続計画策定ガイドライン」（2005 年 3 月）

また、同じ経済産業省のガイドラインでは、システム対策チームの役割として、表 2-4 に挙げた項目が推奨されている。コンピュータセキュリティに係わる技術専門部署の役割と、例示したシステム対策チームの役割は必ずしも一致するものではないが、情報システム部門との連携、もしくは単独で活動する技術専門組織として参考になる点も多い。

表 2-4 BCP のフェーズ毎のシステム対策チームの役割

BCP 発動フェーズ	・ 対策チームの立ち上げ ・ 連絡窓口の立ち上げ ・ システム被害状況調査 ・ 復旧目処の確認 ・ 業務への影響範囲の想定と特定 ・ 運用体制の確認 ・ バックアップ切り替え要否判断のためのその他の情報収集 ・ 初期のシステム保全対応・復旧対応指示
業務再開フェーズ	・ 代替手段によるシステム運用の指揮 ・ 問題点の把握、対応、報告 ・ システム被害状況調査（継続） ・ 復旧目処の確認（継続） ・ 業務への影響範囲の確認（継続） ・ 運用体制の確認（継続） ・ システム保全対応・復旧対応指揮（継続）
業務回復フェーズ	・ 代替運用の状況把握 ・ 全面復旧時期の設定 ・ 全面復旧に向けた手順の策定 ・ 復旧目処の確認（継続） ・ 業務への影響範囲の確認（継続） ・ システム保全対応・復旧対応指揮（継続） ・ 代替手段によるシステム運用の指揮（継続） ・ 問題点の把握、対応、報告（継続）
全面復旧フェーズ	・ 代替運用の状況把握 ・ 手作業分データの反映 ・ 平常運用のテスト・検証 ・ 本番機への移行対応指揮 ・ 運用記録の整備・保管 ・ 代替機縮退対応指揮 ・ 被害状況の総括 ・ 業務への影響範囲の確認（継続） ・ 問題点の把握、対応、報告（継続）

資料：経済産業省「事業継続計画策定ガイドライン」（2005 年 3 月）

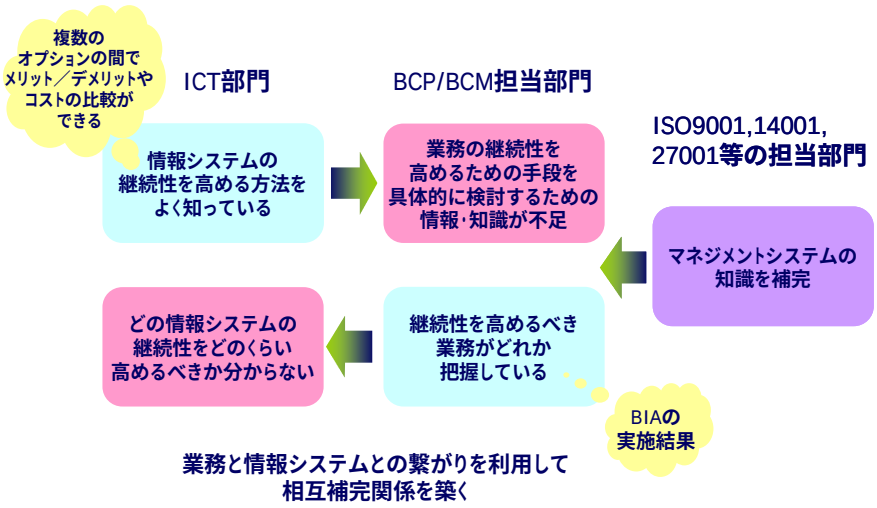
重要業務の検討時には、一般的な日本企業では、担当部門が重要業務を見て、経営層が各部門との関係性を検討し、全体バランスを見るという形が一般的である。しかし、現実には、IT-BCP の検討時点から、どの事業を優先させるかが全社の意識で統一されておらず、IT 部門としても何を優先していいのかわからないことが多いという問題がある。BCP 策定時から優先業務に関する意識を各部門で共有し、インシデント発生時には経営層の的確な指示により、迅速かつ効率的に各部門が対応できる体制を構築することが望ましい。

(2) 技術専門組織が保有する事業継続性に必要な情報

全社的な BCP 対応における情報システム部門の役割を考える上で、情報システム部門が保有する情報をいかに効果的に業務の継続性に結び付けるために提供するかが重要なポイントとなる。通常、情報システム部門は、情報システムの継続性を高める方法をよく知っているが、どの情報システムの継続性をどのくらい高めるべきかは分からない。一方、主たるインシデント対応組織

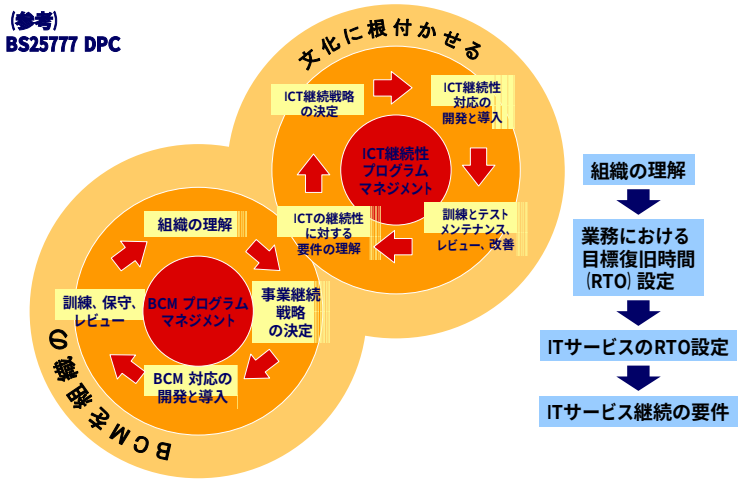
である組織は、BIA の結果、継続性を高めるべき業務がどれか把握しているが、業務の継続性を高めるための手段を具体的に検討するための情報･知識が不足している。

これを補完するのが、ISO9001,14001,27001 等の担当部門によるマネジメントシステムの知識である。



資料：インターリスク総研[22]

図 2-5　BCP 社内体制 ～ ICT 部門と BCP/BCM 担当部門との相互補完



資料：インターリスク総研[23]

図 2-6　IT サービス継続マネジメントと BCM

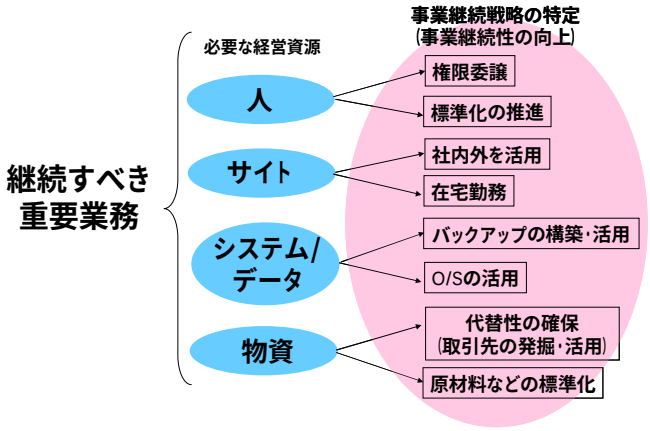
マネジメントシステムの知識も活用しつつ、情報システム部門あるいはサイバーセキュリティに

[22] 第 3 回 DM-WG　篠原構成員資料 (P11)
[23] 第 3 回 DM-WG　篠原構成員資料 (P12)

関わる技術専門部署が、各部署において必要な情報を見極め提供する、もしくはそのために必要な情報の提供を要求することが重要である。

(3) 対応時の経営資源

重要業務を継続するために必要な経営資源は、人（権限委譲や標準化の推進）、サイト（社内外を活用、在宅勤務）、システム/データ（バックアップの構築・活用、O/S の活用）、物資（代替性の確保、原材料などの標準化）等である。



資料：インターリスク総研[24]

図 2-7 重要業務を継続するための対策

経営資産分配の点では、部門内から見えるインパクトと同時に全社的な観点で見たコスト負担の問題がある。対策への投資という点でトータルコストへの結び付け方を考えないと、技術専門部署が行う対応は、その場凌ぎ的な問題対応や単なるレスポンスから抜けきらなくなってしまう。現実的には、コストが BCM プロジェクトの中で認められる場合や、各部門で認められる場合のいずれもがあるが、BCM プロジェクトとして経営層に具申していくと経営層にとっては分かりやすいが、各部門からバラバラに具申されると、経営層もリスクや予算分配がわからない。

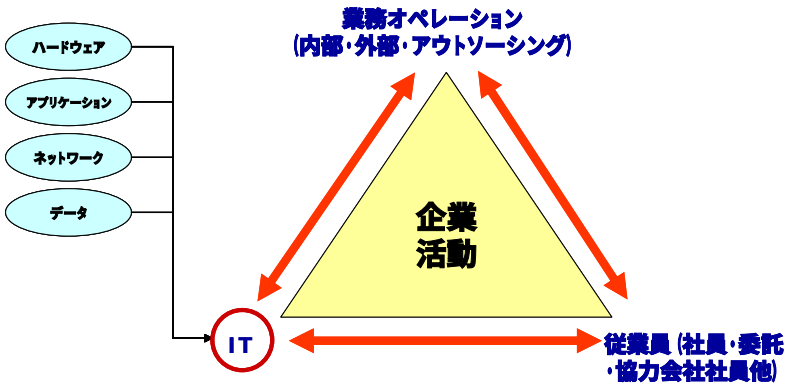
以上のような状況を踏まえると、技術専門部隊には、事後対処から事前予防へ期待が移っているのではないか。ROI/SROI の価値は本来事前対処にあり、その確率を下げるところにあるはず。平時は情報セキュリティ推進という立場で、社内の情報セキュリティの完成度を高める。平常時に問題がないところでどうするかは検討の余地がある。

2.2.3. 企業経営における動的リスクマネジメント

企業活動を支える 3 つの要素＝事業継続性確保に必要な観点は、業務オペレーション（内部・

[24] 第 3 回 DM-WG 篠原構成員資料（P11）

外部･アウトソーシング）、従業員（社員･委託･協力会社社員他）、IT である。



資料：長岡技術科学大学･渡辺准教授[25]

図 2-8 組織のリスクマネジメントの対象となる要素

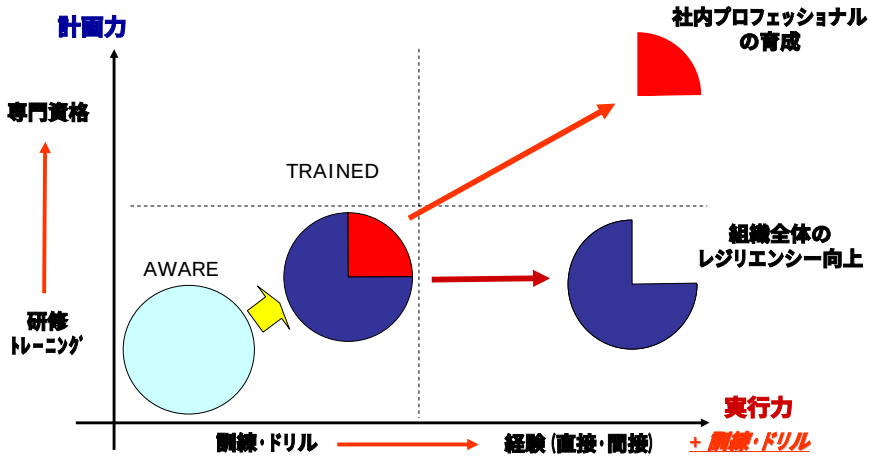
事業継続を検討する上では、BIA（Business impact analysis）が重要である。BIA におけるポイントは、重要業務プロセスの継続に必要な重要文書･データ、重要システムの特定･抽出、RTO、RPO、情報通信技術や媒体に関する要求仕様やコストの検討である。

従来型のリスクマネジメントには限界が来ており、事前対応から事故前提へのシフトが必要である。状況情報の統合による意志決定とコミュニケーション”connect the dots”が必要である。

また、DRM 体制として社内プロフェッショナルの育成と組織全体のレジリエンシー向上が重要である。リスクマネジメントの上でトレーニングが大事だが実際にやることは難しい。水面下を捉えるために、小さなインシデントを集めるというアプローチも含まれる。また、シミュレータのようなもので、現象を見せることも1つの方法である。航空業界に見られるように、事故について正直に報告しても、責任を問われない文化の下、積極的に事故報告を行い、その情報を共有することで大事故を防ぐ仕掛けは、万国共通で長期間に渡って築いている。

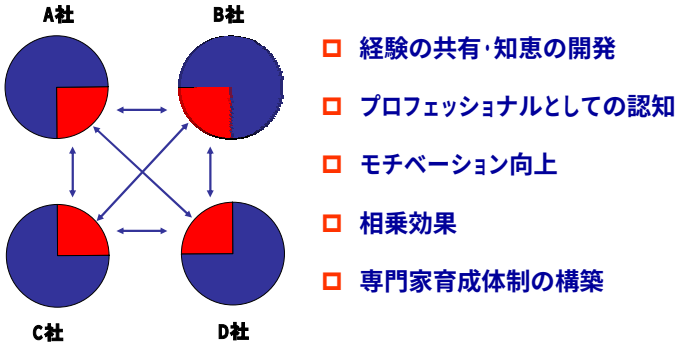
プロフェッショナルの評価、教育制度についても検討の必要がある。プロフェッショナルの意味合いも時代と共に変化することに留意しなければならない。各自は本業を持った上で、非常時に集まって対応するという方法も考えられる。

[25] 第 3 回 DM-WG 渡辺主査資料



資料：長岡技術科学大学・渡辺准教授[26]

図 2-9　DRM 体制の構築



資料：長岡技術科学大学・渡辺准教授[27]

図 2-10　プロフェッショナル人材間の情報・経験共有

[26] 第 3 回 DM-WG　渡辺主査資料
[27] 第 3 回 DM-WG　渡辺主査資料

3. まとめ

3.1. 総括

本調査においては、情報システムとビジネス環境の整理を基に、サイバーセキュリティに関わるインシデント発生時の技術専門部署の課題について明確化し、日本の企業形態に即した望ましいインシデント対応のあり方について検討を行った。また、サイバーセキュリティに関わるインシデントの発生時の動的判断について、各主体が状況に応じて最適な判断を行うためにの動的判断モデルチャートを作成し、効果的に運用するための条件について整理した。

3.2. 今後の方向性

情報システムがビジネス継続のための重要な基盤となるに伴い、新たに発生するサイバーセキュリティ上の脅威の質が変化している。企業においてはビジネス継続の観点から、インシデント発生時の技術専門部署に求める役割が変化してきており、技術専門部署においても、従来の業務や役割の枠組みに留まっていては、企業として効果的な対応を行うことが難しくなっている。

今後は、企業における事業継続マネジメントの考え方を踏まえ、平時の事前予防の活動も踏まえつつ、効果的な事後対応体制・手順を整備していく必要がある。そのために、企業内外における各部門・組織の効果的な情報共有・連携対処の方法を、継続的に検討しなければならない。