Japan Information Security
Management Systems User Group

サイバーセキュリティインシデント発生時の対応とISMS 管理策

インシデント対応にISMS管理策は役立つか？

鈴木　拓也

Fsas Technologies Inc.

自己紹介

鈴木 拓也

JNSA標準化部会 日本ISMSユーザグループ
インプリメンテーション研究会
CISSP, 情報処理安全確保支援士

所属：

エフサステクノロジーズ株式会社
CSIRT室

略歴：

- 1993 富士通株式会社入社
- 2013 サイバー攻撃の検知技術の研究開発
- 2017 セキュリティ標準・規格担当
  ISO/IEC, ITU-Tの標準化, NIST, GDPRなどの調査・対応を担当
- 2019 クラウドサービスの安全性評価に関する検討会
  管理基準ワーキンググループ専門委員
- 2022 ~ 富士通エフサス（現エフサステクノロジーズ）
  CSIRT室長、グループの情報管理統括およびインシデント対応

所属会社 概要：

会社名 (英語表記)	エフサステクノロジーズ株式会社 (Fsas Technologies Inc.)
設立	2024年4月1日
事業内容	• サーバ・ストレージの開発・製造・販売・保守 • ネットワーク製品の販売・保守 • 法人向けPCの販売 (直接販売のみ)
所在地	本店: 神奈川県川崎市中原区中丸子13-2 (フロンティア武蔵小杉) 本社事務所: 神奈川県川崎市幸区大宮町1-5 (JR川崎タワー)

4,845億円
売上規模
(国内・連結24年度実績)

約6,800名
従業員
(連結)

約140拠点
拠点数
(連結製販・保守全拠点)

■ 製造拠点 伊達工場 (福島県)
- サーバ、ストレージの製造拠点
- FTIは日本唯一の国産サーバー製造ベンダー

はじめに

あなたの組織で「**ランサムウェアに感染しました**」という報告が
上がってきたらどう対応しますか？

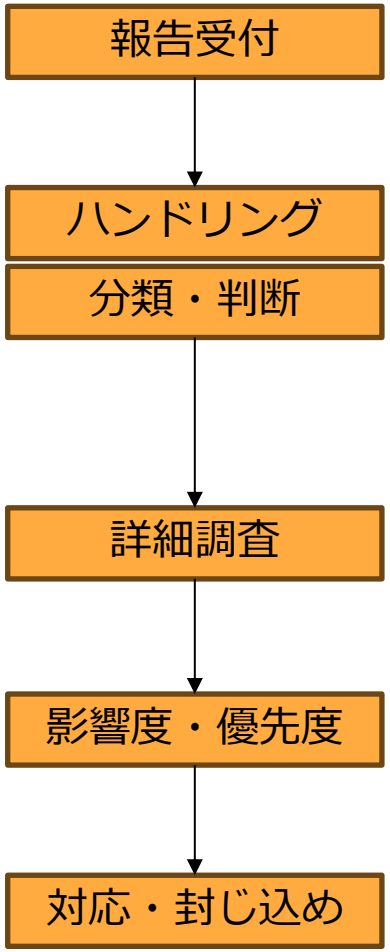
ある朝「社員のパソコンで**身代金を要求するポップアップ**が表示されました…」と連絡が来ました。
その社員は上司に報告し、上司の指示でパソコンをネットワークから切り離しました。電源は入れっぱなしで、ポップアップのスクリーンショットは撮っているとのことです。
あなたは、**社内ネットワークへの感染**、**業務停止**や**取引先への影響**など頭に浮かびます。**まずは話を聞く**ため関係者に連絡します。
ここから**インシデント対応が始まります**。

皆さんの組織では、サイバーセキュリティインシデントが発生したとき、**インシデントに対応する人**と、普段、**情報セキュリティマネジメントを運営している人**はどのように**連携**していますか。

一般的なインシデント対応の流れ

JNSA 日本セキュリティオペレーション事業協会（ISOG-J）の「セキュリティ対応組織の教科書 第3.2版」を参照にすると、一般的なインシデント対応フローは以下のようになります。

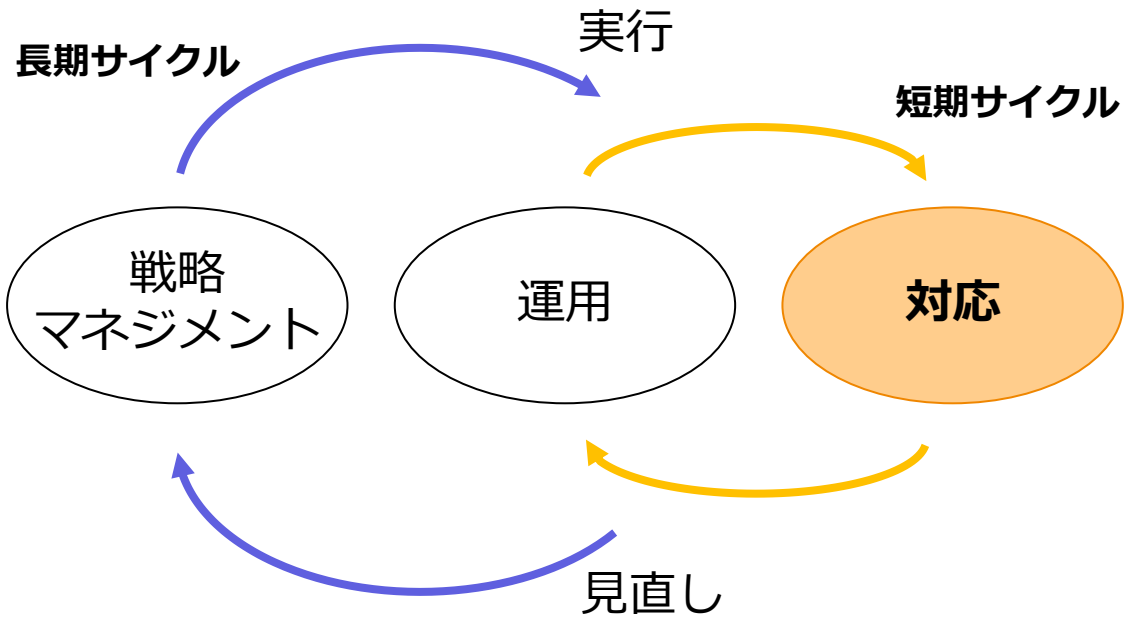
1. イベントをトリガーに**インシデント対応をスタート**する
   この事例では感染の連絡がイベント
2. 対応を要する**インシデントであるかを判断**する
   サポート詐欺のように脅しだけのケースもあり見極めが必要、
   感染の場合は経営層を含め社内にリスク報告
3. インシデント情報を**詳細に調査**する
   ランサムウェアの特定や動作等の情報収集、侵害状況や被害把握のため調査、封じ込めと影響範囲も特定
4. インシデントの**影響度および優先度を判断**する
   調査結果を基に業務や取引先への影響および関係機関への通報要否など判断、アクションアイテム化
5. インシデント**収束に向けた対処**を行う
6. 収束に伴いインシデント対応の**収束を宣言**する



今回のお話のスコープ

ISMSとインシデント対応は時間軸が合わない？
いえいえ、サイバーセキュリティ対応でも、ISMSのような**長期サイクル**とインシデント対応のような**短期サイクル**が存在します。

セキュリティ対応実行サイクル



「セキュリティ対応組織（SOC/CSIRT）の教科書
~ X.1060フレームワークの活用~ 第3.2版」JNSA/ISOG-J より

カテゴリー
A. 戦略マネジメント
B. 即時分析
C. 深掘分析
D. インシデント対応
E. 診断と評価
F. 脅威情報の収集及び分析と評価
G. プラットフォームの開発・保守
H. 内部不正対応支援
I. 外部組織との積極的連携

インシデント対応とISMS管理策とのつながり

よく聞くのが「インシデントが起きたとき、**CSIRTが火を消し**に走ります。
ISMSは“なぜ火が出たのか”を仕組みから見直します。」

ISMS担当者の役割（例）：

インシデントの最中には、個人情報保護委員会への報告など**一部の役割**を担います。
インシデントが収まってから、再発防止や水平展開、対応の評価と**マネジメントの見直し**などを担当します。

直接関係する管理策として以下のものがあります。

- 情報セキュリティインシデント**管理の計画策定と準備（5.24）**
- 情報セキュリティインシデントへの**対応（5.26）**
- 情報セキュリティインシデントからの**学習（5.27）**

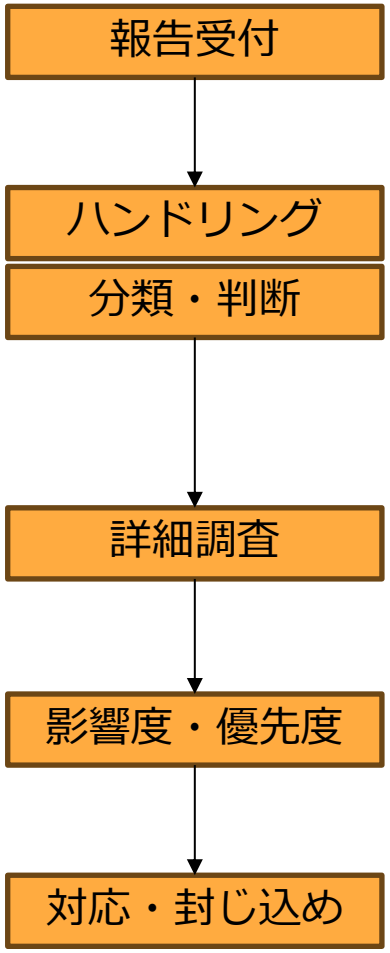
※（）内はJIS Q.27001 附属書Aの番号を示す

長期サイクルの観点が中心

でもインシデント対応の最中に、**実施している管理策の情報を最大限に活用**することで**対応を効率化**できないでしょうか。

インシデント対応に活かせるISMS管理策（実は重要！）　その1

詳細調査フェーズで役に立つ情報



例えば、

暗号化されたサーバーに保存されていた情報は何か？どんな影響があるのか？

情報のリストと分類（個人情報、機密情報、お客様の情報など）

- 情報及びその他関連資産の目録（5.9）、情報の分類（5.12）と情報のラベル付け（5.13）

暗号化されていて対象が確認できない！

対象情報のバックアップ有無、復元可否

- 情報のバックアップ（8.13）

よくある課題

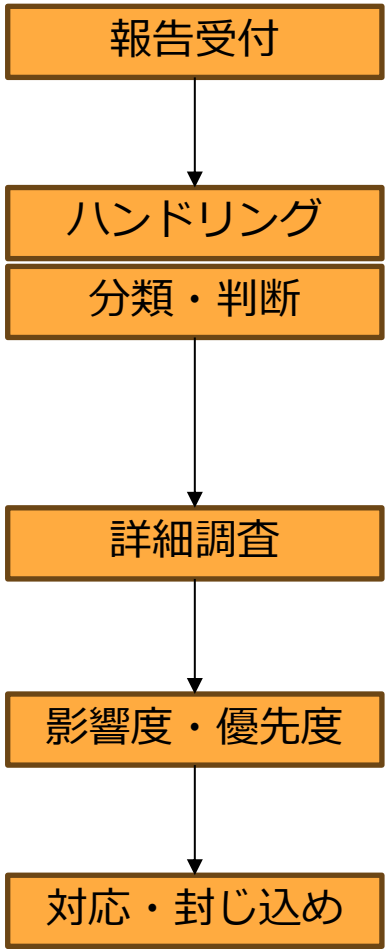
管理策が**短期サイクルを考慮していない**

半年前のリストで対応には使えない

復元に時間がかかる

インシデント対応に活かせるISMS管理策（実は重要！）　その2

詳細調査フェーズで役に立つ情報



例えば、

どこから入られたのか？ランサムウェアはどんな動作をするのか？どんな被害が想定されるのか？

利用される情報システムの脆弱性情報、技術的特徴を含む特定の攻撃に関する詳細な情報

- 脅威インテリジェンス（5.7）
- 技術的ぜい弱性の管理（8.8）

よくある課題

対応に役立つ情報が収集、整理できていない

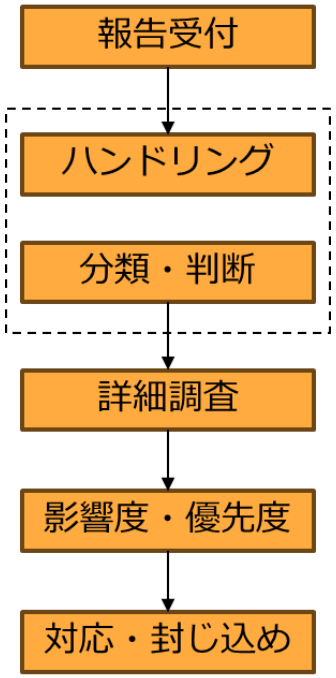
脅威の対応や分析には情報が不足

対応組織間で情報が共有できていない

ご参考）インシデント対応に活かせるISMS管理策全体像

ISO/IEC 27002:2022 を参考に作成

対応フロー



ISO/IEC27002 手引き (Guidance) より	5.24	5.26	5.27
連絡先を含む、情報セキュリティ事象を報告するための共通の方法	6.8		
必要な力量を持つ指定されたチーム		5.24	
情報セキュリティインシデントに関する基準 - 情報セキュリティ事象及び 情報セキュリティ インシデントの監視、検知、分類、分析及び報告	8.15, 8.16, 5.25,5.7, 8.8		
証拠の取扱い	5.28	5.28	
危機管理活動及び場合によっては事業継続計画の発動を含む段階的取扱い		5.29, 5.30	
関係当局、外部の利益団体及び会議、供給 並びに顧客など、内部及び外部の利害関係者との調整	5.5, 5.6		
インシデント後の分析 利用者の意識向上及び訓練		5.27	6.3

箇条	管理策
5.5	関係当局との連絡
5.6	専門組織との連絡
5.7	脅威インテリジェンス
5.25	情報セキュリティ事象の評価及び決定

箇条	管理策
5.28	証拠の収集
5.29	事業の中断・阻害時の情報セキュリティ
5.30	事業継続のためのICTの備え
6.3	情報セキュリティの意識向上，教育及び訓練

箇条	管理策
6.8	情報セキュリティ事象の報告
8.8	技術的ぜい弱性の管理
8.15	ログ取得
8.16	監視活動

ISMS管理策は、インシデント対応の『武器』となる

サイバーセキュリティの視点で**管理策の実装を見直し**、ISMS管理策を**短期サイクルで運用**することで、インシデント発生時に迅速な判断と対応が可能となり、**組織の被害を最小化**できます。

インシデント発生時の対応	武器となるISMS管理策と実装
インシデントの**「分析・判断」** • 実際に情報は漏洩したのか • どんな影響があるのか • これから何が起こるのか	**判断出来る情報**を集めておく • **脅威インテリジェンス**で外部の脅威情報を積極的に収集 • インシデント対応チームと共有し分析
組織の**「状況把握」** • どんな情報が漏洩した恐れがあるのか	**短いサイクル**で情報を取得し、最新情報を**横断的に素早く検索**できる仕組みを構築 • 情報資産目録、分類とラベル付け • 構成情報や技術的ぜい弱性の管理状況
迅速な**「初動対応」** • 発生した事象の報告要否	組織全体で**緊急時の対応**を整理・共有 • 関係当局、専門組織との連絡 • 法令、規制及び契約上の要求事項

突然ですが、参加いただいている皆様にアンケートを取らせていただきたいと思います。

これからいくつか組織に関するご質問を表示させていただきます。
Zoomウェビナーの投票機能によりご回答ください。

この質問を通じて、皆さんの組織の現状を共有し、
課題を浮き彫りにしたいと考えています

質問1

あなたの関わっている組織では、サイバーセキュリティインシデントに対応する組織と情報セキュリティマネジメントを担当している組織は別ですか、それとも一緒ですか？

（1）一緒の組織だ
（2）別の組織だ
（3）決まっていない
（4）その他

質問2

あなたの関わっている組織で、サイバーセキュリティインシデントに対応する際、関連する組織同士で連携がうまくいかずに混乱したことはありますか？
関連する組織とは、サイバーセキュリティインシデント対応組織、ISMS担当組織の他にも、リスクマネジメント担当組織や法務、事業継続担当組織などがあります。

（1）混乱したことはない
（2）混乱したことがあった
（3）サイバーセキュリティインシデント対応の経験がない
（4）その他

質問3

あなたの関わっている組織で、「管理策の実装が短期的なサイクルを意識していない」「管理策がセグメント化されている」という状況はありますか。

（1）そんなことはない
（2）そういう面もある
（3）まさにその通りだ
（4）その他

この問いでは、ISMS管理策をインシデント対応に活用する際に障害となる事象をお聞きしたいと思います。

質問に記載した状況の補足です

- 「管理策の実装が短期的なサイクルを意識していない」
  例えば、ISMSに関する記録やログは、リアルタイムではなく、四半期、半年、1年ごとに見直しているため、インシデントが発生した場合の調査には使えない。
- 「管理策がセグメント化されている」
  例えば、小さい単位で管理方法を決めているため、組織横断で影響調査をする場合に、組織ごとの差分を確認しながら調査を進める必要がある。

まとめ

本日は、サイバーセキュリティインシデント対応の視点を考慮してセキュリティ管理策の実装を見直すことで、もっと効率的にインシデント対応できる可能性がある、ということを課題提起させていただきました。

本日、参加いただいている組織の状況を見てみたいと思います。

各質問の回答分布：

Q1. サイバーセキュリティインシデント対応と情報セキュリティマネジメント担当は別組織？

一緒の組織だ	５３％
別の組織だ	３３％
決まっていない	９％
その他	５％

Q2. 関連する組織間で連携がうまくいかずに混乱したことは？

混乱したことはない	３２％
混乱したことがあった	２３％
インシデント対応の経験がない	３６％
その他	９％

Q3. サイバーセキュリティインシデント対応におけるISMS管理策の課題、共感できる？

そんなことはない	１９％
そういう面もある	５９％
まさにその通りだ	１１％
その他	１１％

今後の取り組み

インシデント対応と情報セキュリティマネジメントが効率的に連携するために、
ガイドラインや国際標準などをさらに調査したいと思います。

参考情報：
情報セキュリティインシデントマネジメントに関する国際標準（ISO/IEC）

ISO/IEC 27035シリーズ **(現時点では英語版のみの発行)**
Information technology -- Information security incident management
情報セキュリティインシデントマネジメント

ISO/IEC 27035-1:2023
Part 1: Principles and process/第1部：原則とプロセス
ISO/IEC 27035-2:2023
Part 2: Guidelines to plan and prepare for incident response/第2部：インシデント対応を計画および準備するためのガイドライン
ISO/IEC 27035-3:2020
Part 3: Guidelines for ICT incident response operations/第3部：ICTインシデント対応運用のガイドライン
ISO/IEC 27035-4:2024
Part 4: Coordination/第4部：調整

ご清聴ありがとうございました。

鈴木 拓也（エフサステクノロジーズ）　suzuki.takuya@fujitsu.com