

2018

インシデント対応 ワークショップ

インシデントで検証する自組織のセキュリティ対策

Version 0.1 2018 年 3 月 30 日

JNSA CISO 支援ワーキンググループ

目次

はじめに	2
インシデント対応の基本	2
ワークショップの進め方	4
ワークショップ環境の設定	6
インシデント事例	6
システム環境	7
ステークホルダー	10
第一インシデント	12
インシデントの選択	12
初期対応シートの作成	12
インシデント対応表とインシデント報告書の作成	12
インシデント発表（記者会見シミュレーション）	12
改善点の検討	13
第二インシデント	13
ラップアップ	13
次のステップ	14
参考文献	15
標準的なインシデント対応	15
セキュリティ事件の例	15
マイクロソフト「セキュリティガイドブック」	15
日本年金機構	15

はじめに

セキュリティ事故が社会的な問題として報道されるようになっていきます。事故が起きた際の影響は、平均で4億円を超えているにもかかわらず、セキュリティ事件が後を絶ちません。セキュリティ対策が進まない要因に、「経営レベルでのセキュリティを捉える」ことが出来ていない点や、有効性が低くなったにもかかわらず、「境界領域防御とツールに頼った対策」を基本的な対策としている点が挙げられています。

「経営レベルでのセキュリティを捉える」ための取り組みとして、経済産業省から「サイバーセキュリティ経営ガイドライン」が公表されています。経営にセキュリティ対策を組み込むことが大きな課題になっていますが、セキュリティ・IT 担当者が、経営者を含めた他部門の責任者と具体的なセキュリティ施策について議論する機会は殆どありません。唯一の機会はセキュリティ侵害が発生したときだけかもしれませんが、セキュリティ侵害発生時に初めて緊急対応をするのでは、適切な対応を期待することができません。

このワークショップでは、報道されたセキュリティ事件が、自組織に発生することを想定し、セキュリティポリシーや事故対応ポリシーなどに則って外部に対する報告書の作成を行います。この作業を通じて、事故対応における組織面での課題を検証し、報告書の作成や状況の判断のために必要な情報(ログなど)が揃っていることを検証します。また、再発防止策の策定を通じて、現在のセキュリティ対策の問題点を洗い出し、強化すべきポイントを明らかにしていきます。

インシデント対応の基本

セキュリティにかかわる事象は、イベント、インシデント、アクシデント(セキュリティ侵害)と分類されます。アクシデントに至らない重要な事象をインシデントすることが一般的ですが、アクシデントとインシデントは結果的に区分されるものであり、対応を行う時点では必ずしも区別が出来ないため、本ワークショップではアクシデントも含めてインシデントと呼称します。

また、IT システムは、情報系だけではなく、ビジネスの基盤としても位置付けられています。このためインシデントの影響は、IT 部門やセキュリティ部門の視点だけではなく、ビジネスに対する影響について評価する必要があります。例えば、飛行中の飛行機の制御装置、手術中の電子医療機器、稼働中の原子力発電所の制御装置、交通管制システムなどは、システムの停止が生命に影響を与える可能性があるため、容易に停止させることはできません。このため、インシデント対応は、事業部門、法務部門、経営陣などを交えた判断を速やかに行い、遅滞なく対応することが求められます。このため、事前に「インシデント対応手順」を策定すること推奨されています。

本ワークショップでは、「インシデント対応手順」の策定を通じて、組織のセキュリティ在り方やステークホルダーを明らかにすることが期待できます。しかし、事故が発生した際に初めて

「インシデント対応手順」に基づいた緊急対応を行う場合、迅速な対応ができないばかりか、対応手順の適切性が担保できません。当ワークショップでは、インシデント対応の机上演習を実施することで、インシデント対応手順の内容と適切性を検証し、必要に応じてセキュリティ施策の見直しを行うこと、事故が発生した際には、手順に従ったインシデント対応を適切かつ遅滞なく実施できることを目指すものです。

ワークショップの進め方

ワークショップを効果的に進めるために、実際の環境や組織構成を簡素化し、「想定 IT システム環境」と、「ステークホルダーリスト」で構成する「ワークショップ環境」を作成します。参加者は、事前に実際の規定などを調べていただき、「ワークショップ環境」と実際の規定（以下：インシデント対応計画）を使って、ワークショップを進めます。

演習は2回に分けて行います。まず、演習1として「ワークショップ環境」と「インシデント対応規定」を使って、想定インシデントの対応を行います。そして、演習1の対応をレビューし、必要に応じて「ワークショップ環境」と「インシデント対応計画」の見直しを行い、演習2では、見直しを行った「ワークショップ環境」と「インシデント対応計画」を使って、想定インシデント対応を行います。なお、演習2では、インシデント対応規定を適用するためには工夫が必要な、「インシデント付加要因」を加えます。

- ワークショップ環境

- システム環境

実際の環境に基づいて、一般化・簡素化した IT システム環境（想定 IT システム環境）を定義します。

管理状況や運用状況を、「想定 IT システム環境ファクトシート」に基づいて作成して下さい。

- ステークホルダー

当ワークショップでは、実際の組織構成に基づいて一般化したステークホルダーを、「ステークホルダーリスト」として作成し、これを参加者に割り当てるようにします。

- ワークショップの流れ

- 事前準備（主催者）

ワークショップ開催の事前ミーティングを行います。

事前ミーティングでは、組織の IT 環境と、組織構成に基づいて、ワークショップで使用する「想定 IT 環境」と、ステークホルダーリストを作成します。

- 事前準備（参加者）

インシデントハンドリングに必要な社内の規定や手続きなど（以下、インシデント対応規定）を確認して、「インシデント対応ポリシー」に記載してください。

当日は、これらの書類を持参ください。電子媒体でも構いませんが、紙媒体を要することをお勧めします。

- イン트로ダクション
- 第一インシデント
 - ✧ インシデントの選択
 - ✧ 初期対応シートの作成
 - ✧ インシデント対応表の作成
 - ✧ インシデント報告書の作成
 - ✧ インシデント発表（記者会見シミュレーション）
- 改善点の検討
 - ✧ インシデント対応規定の見直し
 - ✧ ワークショップ環境の見直し
- 第二インシデント
 - ✧ インシデントの選択
 - ✧ 初期対応シートの作成
 - ✧ インシデント対応表の作成
 - ✧ インシデント報告書の作成
 - ✧ インシデント発表（記者会見シミュレーション）
- ラップアップ

ワークショップ環境の設定

「想定 IT 環境」、「ステークホルダー」を定義するにあたり、ワークショップで実施するインシデント事例を選択します。その上で、インシデント事例に基づいて「想定 IT 環境」、「ステークホルダー」を定義していきます。

インシデント事例

典型的なインシデント事例を以下に記載します。

表 1 典型的なインシデントの例

	インシデント	情報元	受付部門	状況など
1	標的型攻撃で機密情報が漏れた可能性があることが、外部からの連絡で判明した	JPCERT/CC	CSIRT	顧客情報、クレジットカード有無 (件数、50, 500, 5,000, 50,000, 500,000) 営業情報、設計情報、
2	ハッカーの侵入を受けて、すべてのメールがインターネットに公開されたと連絡が入った	メディア	広報	
3	WEB ページから顧客情報が閲覧可能な状態にあると連絡	個人 (匿名)	広報	クレジットカード有無 (件数、50, 500, 5,000, 50,000, 500,000)
4	弊社にしか登録をしていない「メールアドレスに広告が入った」とのクレームが、今日になって入った	顧客	サポート	1 件、5 件、50 件、500 件、50000 件
5	顧客から、弊社にしか登録をしていない「クレジットカードが勝手に使われた」とのクレームが入った	顧客	サポート	1 件、5 件、50 件、500 件、50000 件
6	インターネット上の掲示板に弊社の顧客情報を含むドキュメントが掲載されている	取引先	担当営業	
7	弊社が所有する IP アドレスから攻撃を受けているとのクレームが入った	取引のない海外企業	サポート	1 件、5 件、50 件、500 件、50000 件
8	弊社のメールアドレスを使った、標的メールが取引先に送信された	官公庁	大代表 → 広報	1 件、5 件、50 件、

システム環境

次に、想定 IT 環境ファクトシートを作成します。

例えば、インシデントとして「1. 標的型攻撃で機密情報が漏れた可能性があることが、外部からの連絡で判明した」を選択した場合、以下の IT 関連システムについて定義が必要になります。

対象	PC 環境	管理状況	ログ
○	OS	Windows 7 が中心 ただし、Windows XP も一部に残っている ドメインアカウント使用率は 50%	特に統制はしていない
	パッチ	利用者の裁量に任せている	特に記録はしていない
○	セキュリティ対策ソフト	XX 社の xxx を標準 AV として利用している。 パターンファイルの更新は自動で行われるので、特に統制はしていない。	xxx 管理サーバーに検知状況などが集約される。保存期間は特に決めていない
○	管理手法・状況	AD は、LDAP として使用。 グループポリシーの適用などは行っていない	
○	ブラウザ	特に制限はしていない	
○	オフィス	Office 2016 が利用可能だが、リボンインタフェースが苦手なことから、Office 2003 を使用する従業員も少なくない	

	ネットワーク環境	管理状況	ログ
○	ファイアウォール	インターネットからインバウンドは、メールと、DMZ の公開サーバーのみ許可をしている アウトバウンドは、Web(HTTP, HTTPS)、DNS,だけを許可	ログが膨大になるため、特に制限を設けず、上書をするようにしている。 ログは、Deny のみ、Allow は記録していない
○	プロキシ	プロキシを用意しているが、強制をすると動かないソフトがあるため、強制はしていない。	初期設定のまま、利用している。
	IDS 等（インターネット）		
	IDS 等（DMZ）		
	IDS 等（イントラネット）		

	業務サーバー	管理状況	ログ
○	AD (DC)/LDAP 等	OS パッチ適用状況 インターネットアクセスの有無 特権ユーザー(DomainAdmin 等) x x 名	収集しているログの種類 収集の方法 ログの保存期間 分析等の実施状況
△	SV1:	OS パッチ適用状況 特権ユーザー キitting	収集しているログの種類 収集の方法 ログの保存期間
	SV2～n		
	IDS 等		

	メールサーバー	管理状況	ログ
○	メールサーバー	メールシステム OS パッチ適用状況 特権ユーザー SPF/DKIM	収集しているログの種類 収集の方法 ログの保存期間
○	スパム対策	システム名 OS パッチ適用状況 特権ユーザー 更新方法 更新状況	収集しているログの種類 収集の方法 ログの保存期間
○	ウイルス対策	システム名 OS パッチ適用状況	収集しているログの種類 収集の方法

		特権ユーザー 更新方法 更新状況	ログの保存期間

	公開サーバー		
△	DNS	システム名 (BIND x.x 等) OS パッチ適用状況 特権ユーザー	収集しているログの種類 収集の方法 ログの保存期間
△	Web：ホームページ	システム名 OS パッチ適用状況 特権ユーザー	収集しているログの種類 収集の方法 ログの保存期間
△	Web：CDS	システム名 OS パッチ適用状況 特権ユーザー	収集しているログの種類 収集の方法 ログの保存期間
△	Web：顧客向け業務ページ	システム名 OS パッチ適用状況 特権ユーザー	収集しているログの種類 収集の方法 ログの保存期間
△	Web:DataBase	システム名 OS パッチ適用状況 特権ユーザー	収集しているログの種類 収集の方法 ログの保存期間

△	Web: x x x x		
△	Web: x x x x		
△	Web: x x x x		
△			

ステークホルダー

ステークホルダーを定義します。できる限り、「インシデント対応計画」と、実際の業務を意識して作成をしてください。

表 2 社内のステークホルダー

名称	実務での役割	備考
CSIRT		ワークショップのファシリテーター
広報		監督官庁対応も兼ねるか、別途割り当てる
経営者・事業責任者		
CIO		
CFO		
法務部門		
サポート部門		
当該システムの開発者		
当該システムの運用者		
法人系の営業 (営業企画)		
(ベンダー)		とりあえず、想定しない。 想定する場合は、報告を持ってくるような設定にする

表 3 社外のステークホルダー

名称	実務での役割	備考
監督官庁		
親会社		
関連会社		
取引先		
顧客		
メディア		
SNS・BLOG		

第一インシデント

インシデントの選択

あらかじめ、主催者が設定をしたインシデントの中から、対応するインシデントを選択します。

初期対応シートの作成

「インシデント対応シート」に、インシデントの重要度と、判断の根拠を記載してください。
また、このインシデントにグループ内での名称をつけてください(例えば、標的型攻撃事案 2015-05#1 等)

時間軸の表に対して、対処すべき事柄を記載してください。

インシデント対応表とインシデント報告書の作成

事前に調べた「インシデント対応ポリシー」に基づいて、「インシデント対応表」に必要事項を記載してください。「インシデント報告書」も記載します。「インシデント対応表」と並行して記載していただいて構いません。

記載するにあたっては、「インシデント報告書」に記載する内容も考慮しながら記載してください。また、具体的な規定がない場合は、判断の根拠、判断の責任者、対応の責任者、対応上の考慮点などを、別途記載してください。

インシデント発表（記者会見シミュレーション）

記者会見を想定して、「式次第（アジェンダ）」を記載してください。

- 式次第（アジェンダ）の送付先
- 会見の名称
- 会見の概要
- 登壇者（役職、氏名、内部情報として会見での役割）

「式次第（アジェンダ）」に基づいて、「インシデント報告書」に記載した内容を発表してください。ワークショップ講師および、他の参加者がメディアとして、会見に参加します。難しい質問が出るかもしれませんが、記者会見を想定して、できるだけ適切にコメントするようにしてください。

改善点の検討

ここまでの作業を振り返り、「インシデント対応手順」、「インシデント対応ポリシー」、「想定 IT 環境ファクトシート」、「ステークホルダーリスト」、「初期対応」、「インシデント対応表」、「インシデント報告」、「式次第（アジェンダ）」等を修正します。修正に当たっては、変更理由を明記し、履歴がわかるようにしてください。

第二インシデント

第二インシデントを選択するとともに、付加要因を設定します。典型的な付加要因として、以下のような事例を挙げる可以做到。

- 社長や CIO が倒れた、または、出張中で連絡がつかない
- とめどなく、被害が広がっていった
- 記者会見で失敗した
- ジャーナリストに注目された（厳しく報道された）
- 暗号化されているはずなのに、暗号化されていなかった

これらの条件の設定を終えたら、第一インシデントと同様の手順で演習を行います。

ラップアップ

ワークショップを振り返り、講師が講評を行います。また、受講者との Q&A 等を通じて、効果的なセキュリティ対策の実施に向けたディスカッションを行います。

次のステップ

本ワークショップを一度でも実施することは、組織の危機対応能力を格段に高める効果があることは間違いのないことだと思います。しかし、日々の環境は刻々と変化しており、人間の記憶も不確かであるため、一度ワークショップを実施しただけでは、いざ緊急対応が必要になった際には、適切な対応ができないことも少なくありません。

緊急対応には限りませんが、セキュリティ対策には二つのアプローチがあると考えています。ひとつは、実績のあるフレームワークに従って構築を進めるという考え方で、フレームワークを上手に使うことで、合理的で効率的な対策を構築することができます。一方で、フレームワークに従うだけでは実効性のある対策にはなりません。緊急対応の実践を重ねる中で、対応手順を組織の状況に合わせてメンテナンスし、すべてのステークホルダーが訓練された状態を維持することも重要です。このためには、日常的に発生するイベントや、比較的小さなインシデントに対して、緊急対応手順に沿ったハンドリングを行い、常に緊急対応が動いている状況を維持することが効果的です。

本ワークショップは、組織におけるセキュリティ対策の実務的な評価も目的としています。ネットワークやサービスの停止などの影響の大きい判断を行うための手順と責任者を確認し、連絡手段とともに、連絡が取れないケースの対処も明らかにすべきです。特に経営陣、事業責任者、広報、人事などの重要なステークホルダーとの連携に気を配ってください。起点となった従業員などに対する処罰の確認も重要な要素です。また、判断を行うために必要な設計資料、インベントリ、ログを速やかに取得し利用できるか、証拠保全の手順は適切に組み込まれ、速やかな実施が可能か、という視点も重要なポイントです。

参考文献

標準的なインシデント対応

NIST SP800-1 「コンピューターセキュリティインシデント対応ガイド」(IPA)

<http://www.ipa.go.jp/security/publications/nist/> (関連ドキュメントを含む)

JPCERT/CC 「インシデントハンドリングマニュアル」

https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20151126.pdf

CSIRT 協議会「CSIRT スタータキット」

<http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf>

セキュリティ事件の例

マイクロソフト「セキュリティガイドブック」

https://www.microsoft.com/japan/msbc/Express/contents/enterprise_security/

- ケース 1 : 社内情報の持ち出しによる情報漏えい
- ケース 2 : ウイルス感染による情報漏えい
- ケース 3 : 事故による経営陣の退任

日本年金機構

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結果報告」

<https://www.nenkin.go.jp/info/index.html>

NISC : 「日本年金機構における個人情報流出事案に関する原因究明調査結果」

http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf

厚生労働省（日本年金機構における不正アクセスによる情報流出事案検証委員会）
検証報告書

http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150821-02.pdf