情報セキュリティセミナー
インシデントマネジメント

v.1.0

情報処理振興事業協会
セキュリティセンター

概要

情報セキュリティインシデントへの一連の対応プロセスを説明し、その中で平時における事前準備の重要性を強調します。ここでは「インシデント対応」とは表現せず、一連のマネジメントプロセスとして論じます。

平時においてインシデントに対応するための事前準備をする際には、上級経営管理層の参画も必要です。それは方針を支持していただき、必要な資源を確保する必要があるからです。

目標

- ✧ 効果的なインシデント対応を行うためには、平時における事前の準備が必要であることを理解する。
- ✧ 上記の事前準備が必要であることを、上級経営管理者層に説明できること。

目次

1. 平時におけるインシデント対応の準備

1.1. セキュリティポリシー等の中で明記

管理・運用の方針がなければ組織体のメンバーは秩序をもって動くことができません。セキュリティポリシー（もしくは防災計画）の中で、インシデント対応に対応することと、関連する責任の所在が明記される必要があります。そのためには、経営管理者にこのことの必要性を説明し、参画を得るようにする必要があります。

残念ながらインシデント対応の活動は、組織体に収益をもたらす活動ではありません。しかし、組織体が情報システムを利用し、インターネットに接続する限り、常に情報セキュリティ上の脅威は存在しています。潜在的に必然的に将来、インシデントに対応しなければならない状況にあります。

インシデント対応は、収益を生まない活動であるからこそ、効果的／効率的に行われる必要があるのです。場当たり的な対応では、五月雨的にコストが発生し続けてしまうこともあるでしょう。また、不適切なインシデント対応を行うと、企業の事業活動に重要な影響を与える可能性もあるでしょう。

1.2. 平時に行われていなければならないこと

以下に、インシデント対応を行う際には前提となる平時に行われていなければならない事項を掲げます。

(1) 定期的バックアップ

システムの設定情報やデータをバックアップしておかなければ、以前の状態に復旧することができません。

(2) システムの通常状態の把握

システム管理者／ネットワーク管理者がシステムの通常の状態を把握していなければ、情報セキュリティの侵害を認識することができません。

(3) 外部情報収集と修正プログラムの適用

ソフトウェアの脆弱性に関する情報の中に、自らのシステムが利用しているものの該当がないか、日常的にチェックしておく必要があります。該当する脆弱性情報が報告されていながら修正プログラムを適用することなどの対策を施していない場合、システムをリスクがある状態に放置していることになります。

(4) 予行演習

インシデント対応の手順は、人が行う行為の連続です。手順に不備があれば、適宜修正しておく必要があります。ただし、実際のインシデントへの対応は、なかなか予行演習のようにはいかないのも事実です。

1.3. 技術的手段の準備

技術的手段が整っていなければ、平時に行っておくべきことを行うことができません。

- 情報セキュリティ侵害を検知することを支援するツール
- バックアップの資源

2. 情報セキュリティ侵害を検出する

検出・認識の方法 **　自主的な検出** **　他者からの連絡** **ツールの利用** **次に何をすべきか？**

2.1. 検出・認識の方法

**　自主的な検出方法には２つあります。:**

1. **ミスユース検出**

既知の侵害パターンに基づく情報とのマッチングにより､該当侵害の存在を検出する方式。
Signature recognition **（シグネチャ認識）ともいいます。**

2. **アノマリー検出**

通常ではない変則・異常なイベント、統計的に稀なイベントを検出する方式です。セキュリティ侵害行為を意味するイベントは通常ではないイベントに含まれるはずであると仮定されています。

**　いずれも事前の準備がなければ、迅速に検出・通知することができません。日頃から流行している攻撃やウイルスについて情報を知っておきましょう。**
システム管理の日誌を通常のノートのようなオフラインなものに書いて大事に保管することをお薦めします。システムに適用したパッチや、ツールのシグネチャの情報などを正確に書き留めておくと、インシデント発生時には役立ちます。
**　この他、他者からの連絡によってインシデント発生を知らされることもあるでしょう。この場合においても、自らその情報の真偽を確認すべきでしょう。また、インシデント以外にも対応せざるを得ないことがあるでしょう。いわゆる** spam **についての苦情がエンドユーザから集まることがあります。また、デマのコンピュータウイルスのチェーンメール等、まぎらわしい事象もあります。**

2.2. ツールの利用

インシデントマネジメントは人が行うプロセスですが、自動化することができることは自動化し、効率よく作業します。 例えば、各種設定ファイルを対象にして、それらに変更がないかを検出するために、Tripwire のようなツールを利用することができます。

事前にファイルの状態を、ハッシュ関数を通して得られるデータとして記録しておきます。検査時には再度、該当ファイルについてハッシュ関数を通じて得られるデータを再作成し、当初のものと比較する仕組みです。

2.3. 次に何をすべきか？

発生したインシデントの状態を、できるかぎり完全な形で保存する必要があります。基本的にはバックアップの手段を利用して、各種設定ファイルを必須の対象とします。リムーバルなメディアにフルコピーを複数とります。インシデントの技術的問題を分析する対象となるとともに、証拠資料となる可能性があります。

進行中のインシデントの場合、バックアップ手段ではとれない情報を控えておくのがよいでしょう。例えば、ネットワークの接続状況、ログインユーザー、すべてのプロセス等です。

該当インシデントに関する外部の情報が公表されていないかを調べます。情報源として IPA/ISEC や JPCERT/CC が web で提供している情報をご利用ください。

本当にインシデントか？を確認します。例えば indent について、インシデントと紛らわしい事象もあります。

時系列の記録をオフラインで記述し始めます。

3. 情報セキュリティインシデントに対応する

インシデント対応手順の確認

報告する
(1) 組織体内部のコミュニケーション
(2) 関連組織とのコミュニケーション

暫定的対応と本格的対応

3.1. インシデント対応手順の確認

定められたインシデント対応手順を確認し、作業もれや混乱がないようにします。

3.2. 報告する

(1) 組織体内部のコミュニケーション

情報セキュリティ侵害は、システム管理者に対する個人的な挑戦ではありませんので、組織体の一員として行動する必要があります。まず、セキュリティポリシーと手順に従って組織体内部の責任者に報告します。このときマネジメントや広報の技術的に詳しくない人間とコミュニケートする必要があります。そのためには簡潔に説明する必要があります。

(2) 関連組織とのコミュニケーション

外部関連組織とのコミュニケーションは別の作業です。JPCERT/CC のような CSIRT を通じてコミュニケーションをとることも有効です。

参考資料：JPCERT/CC 技術メモ 関係サイトとの情報交換

3.3. 暫定的対応と本格的対応

暫定的対応として行うべきことと、本格的対応として行うべきことの内容は異なります。サーバーへの侵入のインシデントが発生し、その攻撃者がシステム特権を得ている場合には、システム全体が侵される可能性があります。攻撃者によってバックドアが仕掛けられている可能性があります。このような場合、本格的対応として、クリーンなシステムから再構築することをお薦めします。暫定的な対応を行わずに、このような本格的対応を行うことはできません。

(1) 暫定的対応

ネットワーク接続の切断、サービスの停止は、ビジネスの観点から抵抗がある作業です。上級経営管理者には、サービスを停止する必要がある場合もあることを事前に認識しておいてもらい、迅速な承認を得ることができるようにしておく必要があります。

(2) 本格的対応

攻撃者にシステム特権を奪われてしまったときには、原則としてクリーンなシステムから再構築する必要があります。今日のコンピュータシステムは、まさに複雑なシステムであり、悪意あるプログラムをしかけられていないことを検出し、それが存在しないことを保証することは不可能に近い困難です。再度、クリーンなシステムを再構築するしかありません。

(2-1) オペレーティングシステムの再インストール

信頼できるメディアからクリーンなシステムを再インストールします。アプリケーションも再インストールします。

(2-2) 修正プログラムの適用

利用しているシステムについて修正プログラムが提供されている場合、それらを適用します。以前のシステムに適用していたとしても、システムを以前と同じメディアから再インストールしたのであれば修正は適用されていませんので、再度適用しなおす必要があります。

しばしば、修正プログラムの適用は、アプリケーションとの相性等の不具合を生じることがあります。また、バージョンアップされたシステムを、いきなり本番のインターネットサーバーで試すのは失敗する可能性があります。本番サーバーと同等の実験環境においてパッチの適用や、新しいバージョンのシステムを試すことが望ましいといえます。

(2-3) 復旧

設定ファイルの情報やデータをバックアップから復旧します。バックアップが採られていない場合、これらを復旧できません。

4. 改善する

時系列の記録を整理しておくのが有用です。事後反省会を開催し、良かった点と改善すべき点をリストし、経営管理者に報告するべきでしょう。

公式文書としてのセキュリティポリシーや手順書類に、改善点を反映・集約することが必要です。 技術的準備の改善、組織間コミュニケーションの改善もはかりましょう。

参考資料

JPCERT/CC **技術メモ**

コンピュータセキュリティインシデントへの対応

http://www.jpcert.or.jp/ed/2000/ed000007.txt

関係サイトとの情報交換

http://www.jpcert.or.jp/ed/2000/ed000006.txt

CERT Guide to System and Network Security Practice
Julia H.Allen
ISBN 0-201-73723-X
ADDISON-WESLEY

Incident Response
Kenneth R.van Wyk & Richard Forno
ISBN 0-59600-130-4
O'REILLY