

情報セキュリティセミナー

情報セキュリティ・マネジメント概論

v. 1.1

2001.10.24



情報処理振興事業協会
セキュリティセンター

概要

各組織体において情報セキュリティ対策を実践するにあたって、上級経営管理者層の支持を得る必要がある事項があります。例えば、セキュリティポリシーの立案と、その定期的な見直しの必要性を説明しなければならないことがあるでしょう。情報セキュリティ対策の実践においては、このように事前に定めるべき事項や、あらかじめ資源を確保しておかなければならない事項があります。

情報セキュリティの技術的事項をマネジメントの中に位置付けて理解し、技術的知識を有するとは限らない上級経営管理者層の人と上手にコミュニケーションをとることができるようにします。

受講後の目標

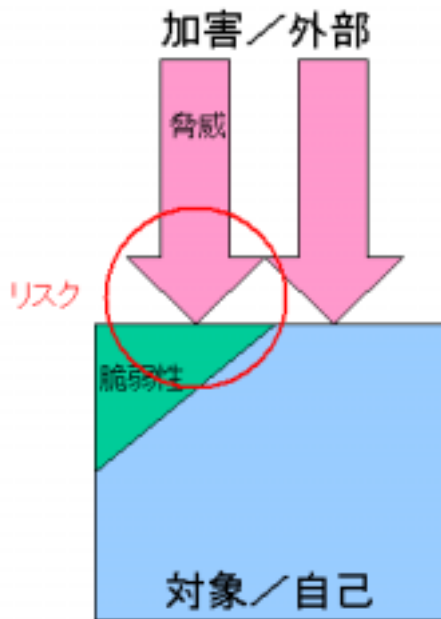
技術的な知識を有しない上位経営管理層に、セキュリティポリシーの立案・見直しの必要性や、情報セキュリティ対策は製品の導入ではなくプロセスであることなどを説明できるようになることを目標にします。

目次

1. 情報セキュリティの用語と概念.....	3
2. 情報セキュリティマネジメント	7
2.1. セキュリティポリシーの必要性.....	7
2.2. 情報セキュリティ・マネジメントのサイクル	9
3. 復習問題.....	10
A. 参考資料	10

1. 情報セキュリティの用語と概念

脅威 + (脆弱性 + 露出) リスク
インシデント： リスクが実現した状態



脅威 (Threats):

情報システムに対する加害。意図的な加害以外に、過失による情報セキュリティ侵害の驚異もあるでしょう。侵入者 (intruder) は、世界中におり、侵入/サービス妨害攻撃の脅威があります。また脅威は攻撃者に限られません。ワームの伝搬やウイルスの感染も身近な脅威です。今日のインターネットに常時接続されている環境においては、常に外部からの脅威が存在しているといえるでしょう。また、内部の従業員等も情報システムを攻撃する可能性をもっています。

脆弱性 (Vulnerabilities):

保有する情報システムに存在する弱点 (広義)。ソフトウェアの脆弱性について、いわゆる脆弱性の中を整理して厳密に理解しようとする見解があり、この場合、脆弱性 (狭義) と露出に分けます。ここでは、この見解に従って整理を試みます。:

- ◇ 脆弱性 (狭義): 予定されているセキュリティを満たさない欠陥。
- ◇ 露出 (Exposures): そもそもセキュリティが存在しない仕様。

この他に設定ミスや弱いパスワードなどもソフトウェア自体の欠陥ではありません。

情報セキュリティリスク (Risks):

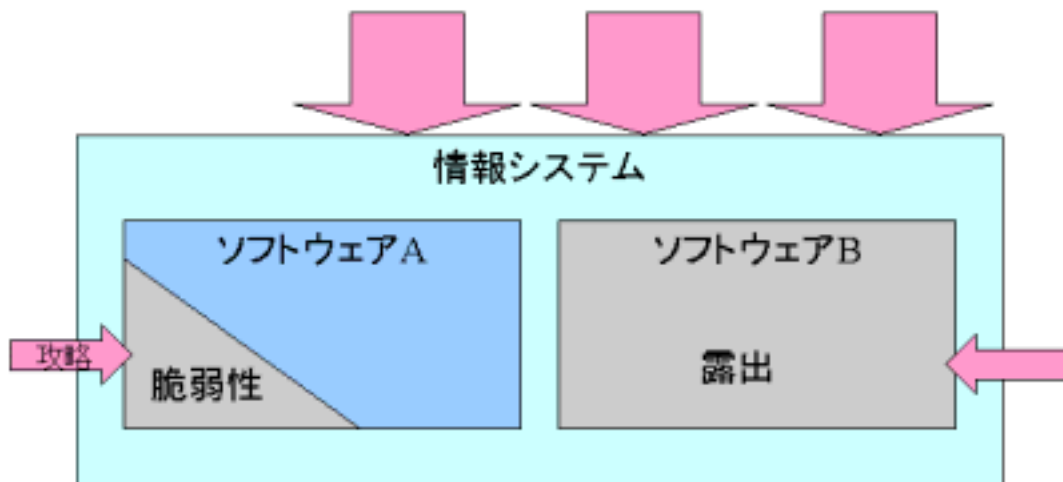
周知の脆弱性や露出が存在していたり、本人認証が確かなものでなかったりすれば、その状況はリスクが発生しているといえます。このリスクを低減させたり、回避したりするために対策を行います。

インシデント (Incidents):

実際にリスクを攻撃するイベントが発生した場合、インシデントとして認識されます。リスクが実現している状態にあるといえます。

適用 1 : 情報システムへの適用

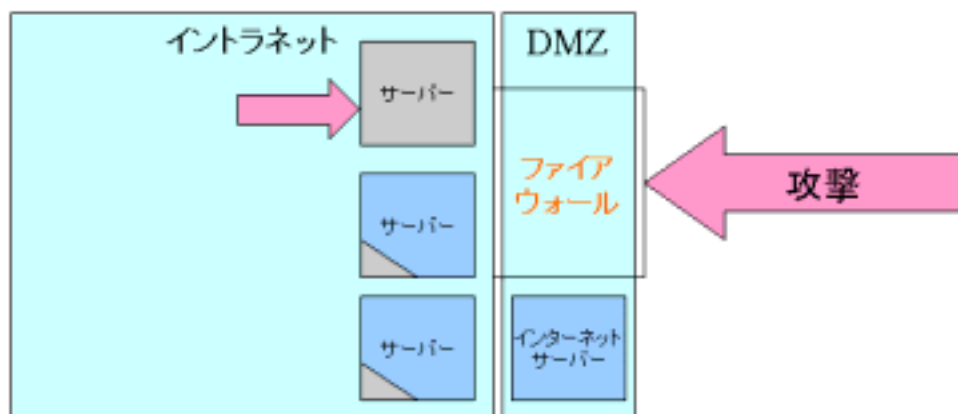
適用1: 情報システム



Copyright 2001 IPA. All rights reserved

情報システムは常に脅威にさらされています。この情報システムを構成するソフトウェア A に脆弱性が発見されたとします。その脆弱性を攻略する攻撃者が現れるかもしれません。ソフトウェア B は、そもそもセキュリティ機能を持たない仕様であるかもしれません。

適用2: 組織体のネットワーク



Copyright 2001 IPA, All rights reserved

経営管理者はファイアウォールを「物」のように考える傾向があるようです。ファイアウォールはネットワークセグメントを守る「考え方」です。防火壁よりは城壁の方が、そのイメージは近いかもしれませんが、よいインターネットファイアウォールは単純な外部 / 内部の考え方ではありません。インターネットサーバーは、内部のネットワークでも外部のネットワークでもないネットワークに配置するので、2重の城壁があるイメージです。

ファイアウォールの考え方は、フェイルセーフの考え方です。DMZ(Demilitarized Zone) と呼ばれる緩衝部分がまず攻撃にさらされますが、たとえこのセグメントにあるサーバーが侵入されてもなお内部のネットワークへのアクセスから守ろうという考え方です。

攻撃にさらされるインターネットサーバーへのアクセスも制限しますが、当然ながらこれらのサーバー自体のセキュリティが求められます。そのため、セキュリティを確保すべく、不要なサービスが提供されない専用のサーバーとし、修正プログラムがある場合には即座に適用します。このような活動は「要塞化する」と呼ばれ、これらのサーバーは要塞ホスト (Bastion Host) と呼ばれるわけです。

内部ネットワーク (イントラネット) 中のサーバーに脆弱性があるかもしれません。あるいはセキュリティを持たない仕様のサービスを提供しているかもしれません。ファイアウォールは、たとえ内部ネットワークに脆弱性があるうとも、それに対する外部からのア

アクセスを制限する役割を果たします。いわば柔らかいものを包む硬い殻のような役割です。

インターネットファイアウォールによる内部ネットワークの防護には限界があります。まず内部からの攻撃に対する防護にはなっていません。また、すべてのアクセスがファイアウォールを通過するという前提が成り立たない状況においては、他の経路からのアクセスについてもセキュリティ対策を施す必要があります。リモートアクセス手段を提供する際には、そのセキュリティを検討する必要があります。

インターネットファイアウォールは、インターネットサーバーについても防護します。しかしその防護にも限界があります。通常、インターネットサーバーが提供するサービス以外のサービスに相当するポート番号の通過について制限します。一方、インターネットサーバーが提供するサービスに相当するポート番号の通過は許可するので、Web サーバーやメールの SMTP 中継サーバー等へは到達可能です。よって web サーバー自体に脆弱性がある場合には、その脆弱性を解消する必要がありますし、メールの添付ファイルとして送られてくる悪意あるプログラムを防ぐためには別の手段の導入が必要です。

ファイアウォールは「物」ではありません。考え方です。ファイアウォールの考え方は、今日のインターネットセキュリティ対策において重要で不可欠な考え方です。しかし、ファイアウォールの考え方だけでは限界があります。最悪の場合をよく考えておく必要があります。

2. 情報セキュリティマネジメント

2.1. セキュリティポリシーの必要性

本質的なこと：

- ◇ 組織体の意思として何を守るか
- ◇ 誰が責任者であるか

本質的でないこと：

- ◇ 文書のタイトル
- ◇ 文書の厚さ

定められていることが望ましいこと：

- ◇ インシデント発生時の対処方針

セキュリティポリシーの必要性と、それに基づく手順（**procedure**）の整備の必要性についてお話しします。

(1) 組織体の活動における方針の設定

セキュリティポリシーは、基本的には「何を守るのか?」、「そのための体制は?」についての組織体の意思としての方針・目標です。ブームではなく必然的なものです。組織体の意思として確立すべき事項があり、それを文書化する必要もあるのです。ただし、セキュリティポリシーという表紙がついている文書がセキュリティポリシーというわけではではありませんし、その厚さが重要というわけでもありません。

実際に確立されるセキュリティポリシーを前提に組織体が動くことが重要です。

What? : 何を守るのか?

守るべき情報資産等を識別する必要があります。公開情報が改ざんされてはならないでしょうし、機密情報が漏洩してはならないことでしょう。情報資産自体を守ることに加えて、社会的信用も重要でしょう。

Who? : 誰が責任者であるか?

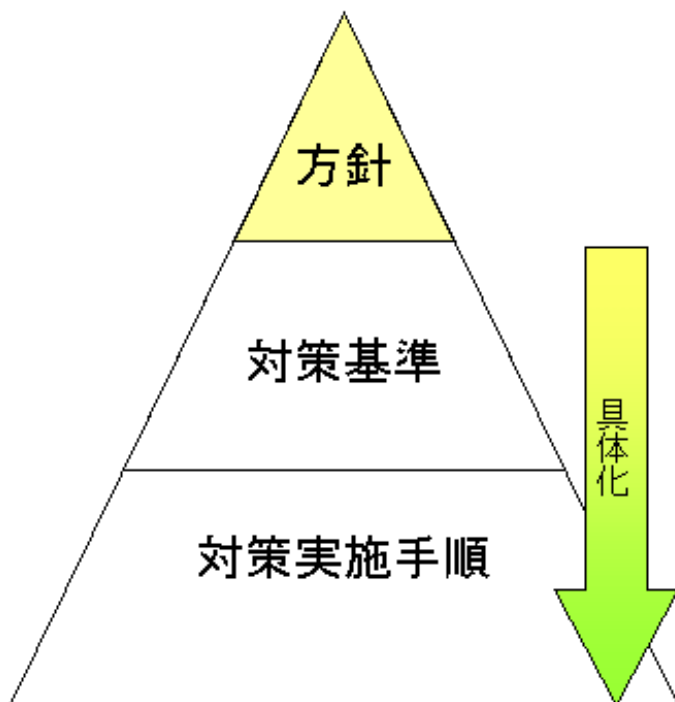
誰が守るべき情報資産等に責任を負うかを定める必要があります。情報システム部門のほかに、内部監査部門や、調達部門も関連する可能性があるでしょう。情報セキ

セキュリティ対策は製品ではありません。プロセスであり人が主役です。

(2) 手順書の整備の必要性

セキュリティポリシーの核として「何を守るのか？」と「誰が責任者であるか？」が定められたとします。これに向けて組織体の活動を動かしたいところですが、抽象的な方針だけでは、組織体のメンバーは動くことができません。そこで、より具体的な手順も定めておく必要があります。実働的であることを確保するためには、しばしば改訂されることあるでしょう。そこでバージョンや日付を付しておき、メンバーが現行版を認識・入手できるようにしておく必要があります。

図：セキュリティポリシーの階層



(3) インシデント対応のポリシー

インシデント発生時にも効果的に対応できるように方針を定めておくことが望まれます。Who? :「誰が？」に関して連絡先 (Point Of Contact) となるかを定めておくことが重要です。また、限られた時間的制約の中で動くこととなりますので、対応手順の整備も重要となります。

2.2. 情報セキュリティ・マネジメントのサイクル

情報セキュリティマネジメントのサイクル



セキュリティポリシーに基づいて、情報システムがマネジメント（管理）される必要があります。情報セキュリティ対策は人が行うプロセスであり、製品ではありません。そのマネジメントのプロセスは一連のサイクルです。よりよいセキュリティ実践を導入しつつ改善するプロセスなのです。

- ◇ 計画（**Planning**）: 対策実施手順作成
- ◇ 実施（**Implement**）: 構築・実装・運用 / 教育
- ◇ 検査・監査（**Assurance & Audit**）: 対策実施手順評価

3. 復習問題

うまく説明できますか？

- ◇ ファイアウォール製品を買って設置さえすればよいというわけではないこと
- ◇ フェイルセーフの考え方
- ◇ セキュリティポリシーという文書があればよいというわけではないこと
- ◇ 情報セキュリティ対策は終わりなきプロセスであること

A. 参考資料

情報セキュリティの用語と概念関連

IPA/ISEC ネットワークセキュリティ関連用語集

セキュリティポリシー関連

IPA/ISEC 情報システム部門責任者向けのページ

「情報システム部門責任者向け 情報セキュリティブックレット」

IETF RFC 2196 サイトセキュリティハンドブック