

公認内部監査人



Certified
Internal
Auditor



公認内部監査人(CIA) Part III／第6回

Abitus

※アビタスCIA本講座講義資料のため、MUFG CIA受験対策講座の実施回と異なります。

9-9 不測事態対応計画

事業継続計画、不測事態対応計画の構築

ビジネスの中断は自然災害、事故または意図的な犯罪行為によって発生する。ビジネスの中断は重大な財務上および業務上の損害をもたらすことがある。ビジネスの成功にITの活用が不可欠な今日、コンピュータ・システムの中断についても十分な準備が必要である。

論点

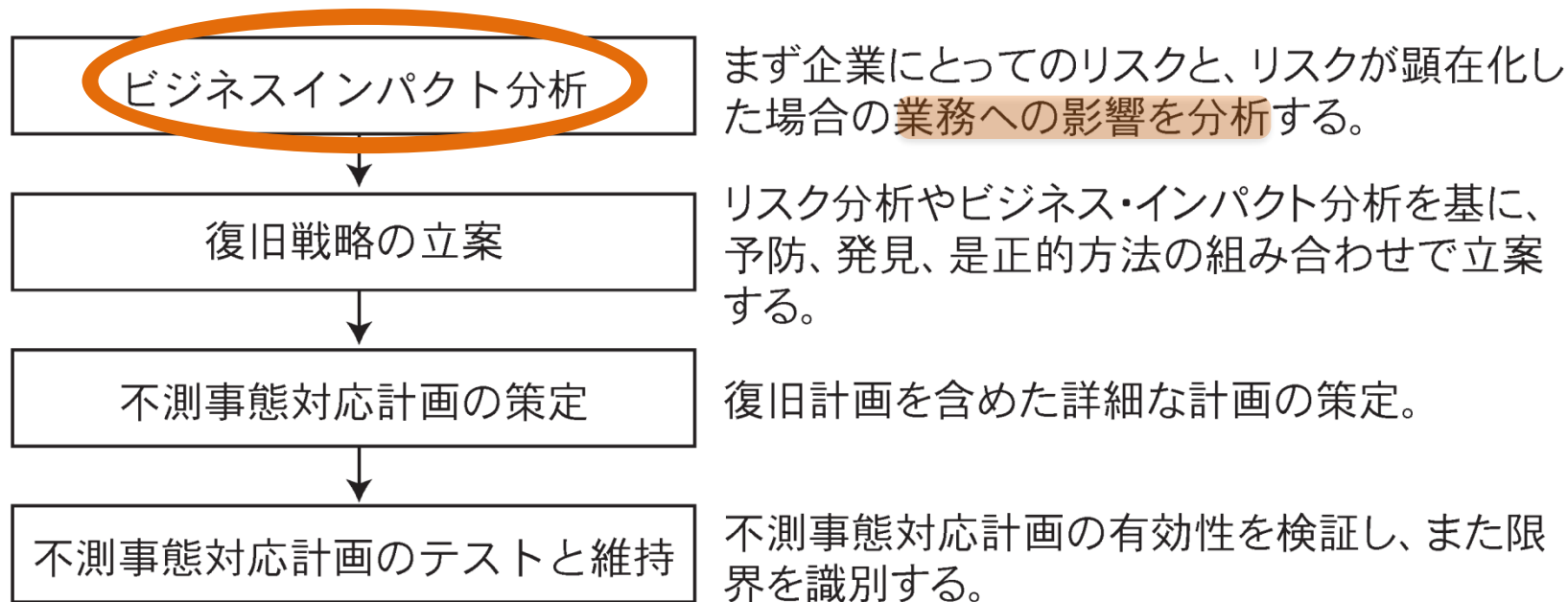
ITに関わる不測事態対応計画

ITに関わる不測事態対応計画(contingency planning)とは、自然災害等により組織体にとって重要な機能を持つコンピュータ・システムや通信サービスが遮断された場合、どのように復旧するか計画立案を含め、業務リスクを軽減させるように設計されたプロセスである。

BCP=CP

災害、テロなどの緊急事態に遭遇した場合、
事業継続のための方法、手段などを取り決めておく計画

a) 不測事態対応計画の一連の流れは以下の通り。



ビジネスインパクト分析(BIA)によって以下の点が明らかになる。

- 事業継続計画の対象となる重要業務の特定
- 業務継続・復旧の優先順位付け
- 目標復旧時間と目標復旧ポイントの設定

ビジネスインパクト分析を行うことの主目的は、有事の際に復旧を優先する業務の選定とその目標復旧時間の決定にある。

まず優先的に復旧させる業務の選定は、「有事」を想定することから始まる。まず環境面からの分析として、対象業務に関係する建物や電気・ガス・水道といった社会インフラにおける被害想定と業務への影響を検討する。

次に業務面からの分析として、業務を行う際の最低条件を整理し、想定被害下における停止業務を洗い出す。このうち、業績に与える影響やCSR等の観点から優先順位付けを行い、優先的に復旧させる業務を選定していくことになる。

また、洗い出された業務について目標復旧時間と目標復旧ポイントを定め、これを達成できるように対策(予防・代替手段など)を検討していくことになる。

〈システムに関する不測事態対応計画時の指標〉

目標復旧時間(RTO)	事前に定めたレベルにシステムが復旧するまでの時間。 業務の重要度に応じて設定する。
目標復旧時点(RPO)	データの復旧を保証する時点。RPOが1時間であれば、 システム停止の1時間前までのデータが復旧される。
目標復旧レベル(RLO)	目標復旧時間の経過後に、システムが復旧するレベル。

許容される中断期間の例

	目標復旧時間(RTO)	目標復旧時点(RPO)	目標復旧レベル(RLO)
レベル	目標時間	目標時点	目標水準
1	1時間以内	停止直前	平常時と同水準
2	6 時間以内	6時間前	平常時の70%
3	24時間以内	1日前	平常時の50%

c) 障害回復計画に使われる技術

1) フェイルソフト(fail soft)

システムの一部に障害が発生した際に、故障した箇所を破棄、切り離すなどして障害の影響が他に及ぶのを防ぎ、最低限のシステムの稼動を続けるための技術。

2) ミラーリング(mirroring)

サーバーの全てのプロセス及び取引をバックアップサーバーへ複製しておき、主たるサーバーの機能障害が起きた際に、バックアップサーバーが引き継ぐ。

d) 不測事態対応計画に対応する設備
不測事態に対応する設備体制には以下がある。

1) ホット・サイト

障害が発生した場合に、適合性のあるコンピュータ機器があり、瞬時にもしくは数時間以内に業務が再開できる体制のことである。

2) コールド・サイト

障害が発生した場合に、コンピュータを設置する場所のみ確保されているが、実際にコンピュータ等は運びこむ必要がある。

3) ウォーム・サイト

ホット・サイトとコールド・サイトの中間に位置する。基礎的なインフラは提供されているが、通常はコンピュータ設備を欠く。ウォーム・サイトは、緊急導入のためのコンピュータがすぐに取り得できることを前提としているが、他の設備をそろえるには、数日あるいは数週間かかる場合がある。

4) 相互援助協定

同等の装置あるいはアプリケーションを保持する2つ以上の組織間で結ばれる協定であり、参加者は災害等が発生した場合に、互いにコンピュータを使用する時間を提供することを約束する。低コストであるが、装置構成の差により、効果的に運用するためには頻繁なプログラム変更が必要となる。

Key Point

ミラーリングにおけるデメリットは以下のどちらか？

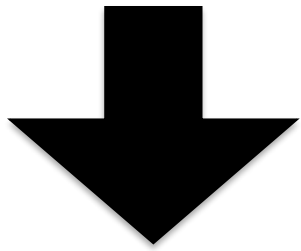


- コストがかかる ○
- 情報の保管に混乱が起きる ✕

Key Point

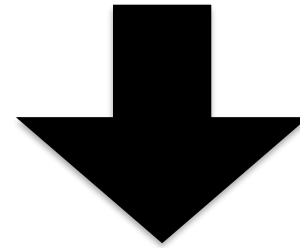
R_{P0}とコストの関係性の問題

RP0が長い



コストが低い

RP0が短い



コストが高い

不測事態対応計画の内部監査

不測事態対応計画の実効性を検証するための内部監査手続として以下の方法が考えられる。

- a) 不測事態対応計画の内容を、定期的に机上レビューしていることを確認する。
- b) 不測事態対応計画の内容を理解していることを確認すべく、担当者にインタビューする。

上記手続からもわかるように、システムを完全に復旧できなかった場合のことや、一時的に業務が停止することへの影響を勘案して、実際にシステムを停止させて計画通りに復旧できるかどうかを検証するような手続は通常行わない。

9-10 バックアップ

人的ミスを含む様々なトラブルからデータやプログラムを守るために、定期的にバックアップを取得することが有効である。なおバックアップ媒体は本番環境とは別の媒体を使用するが、安価な磁気テープが採用されることが多い。

世代管理

バックアップ媒体を複数本用意することで世代管理を行うことができる。例えば週次でフルバックアップ、日次で差分バックアップを取得している場合、1週間分のバックアップ媒体を3セット用意することで、3世代管理(本番環境を含めると4世代管理)が可能となる。

世代管理を行うことで、復元できるデータが直前だけでなく、世代数分まで戻ることが可能となる。

バックアップ媒体は本番環境がある場所と同じ場所に保管しておく、火災や地震などが発生した場合、本番データとバックアップデータの両方を喪失してしまうリスクがある。このため、バックアップ媒体は地理的遠隔地に保管することが推奨される。これを**オフサイト保管**という。多くの場合、1世代を直近世代用、1世代をオフサイト保管用、1世代をオフサイト保管地との輸送に充てたテープローテーションを行うことが多い。

データ廃棄時の留意点

データセキュリティの重要な側面として、削除したデータが完全に消去され、第三者によって復元ができないようになっているかを確認することがある。特に機密情報については、特別なファイル消去ソフトウェアや消磁、物理的破壊等の方法を取ることが検討されるべきである。

10-1 ITに係るリスク

10-2 情報セキュリティとサイバー・セキュリティ

対象となる情報は、電子的な形態で存在するものに 限られない

情報セキュリティ

組織体が保管するデータは、組織体の最も重要な資産の一つであり、情報資産に係るリスク管理は非常に重要である。情報資産に対するセキュリティについても、コンピュータ・システムのセキュリティ同様、物理的統制と論理的統制が有効である。

サイバー・セキュリティ

サイバー・セキュリティとは、主にネットワークを経由して実施されるサイバー攻撃に対して、適切なセキュリティ対策を実施することである。

近年、インターネット上でサーバーがサイバー攻撃を受けて個人情報流出するなどの事件が増えており、企業が事後対応等に追われるなど経済的損失を被ることが多い。このような事態を事前に予防し、かつ、事態が発生した場合でも早期終息ができるようにすべく、サイバー・セキュリティ対策が重要視されている。

情報セキュリティのC.I.A.

機密性(Confidentiality)、インテグリティ(Integrity)、可用性(Availability)のそれぞれのイニシャルを取って情報セキュリティのC.I.A.と呼ばれる。

情報セキュリティ対策に際しては、一般にこの3つの要素を維持することが求められる。

機密性	機密性とは、所定の情報資産に対するアクセス権限を持つ者と権限を持たない者を明確に区別することで、情報が権限の無い者に漏れないようにすることである。
インテグリティ	インテグリティ(完全性)とは、情報の改竄が無くかつ整合性の取れた正確な状態であることをいう。システムに完全性が確保されていないと、処理結果に矛盾や異常などが発生しシステム自体が成り立たなくなるため、あらゆる情報システムにおいて必須の要素となる。
可用性	可用性とは、アクセス権限を持つ使用者が、必要なときにいつでも情報にアクセスができることである。

10-3 全般統制 物理的コントロール

物理的コントロール

物理的コントロールは、物理的アクセス・コントロール、環境の危険に対するコントロール、及び自然災害からの保護を含む。

物理的アクセス・コントロール

アクセス・コントロールの観点から情報資産を大別すると、物理的アクセス・コントロール(施設の施錠管理など、物理的な管理でコントロールする方法)が対象とする情報資産と論理的アクセス・コントロール(システム上のアクセス権限をコントロールする方法)が対象とする情報資産に分類される。

建物内への侵入の回避

このうち物理的アクセス・コントロールは、コンピュータ機器、ファイル、書類のある施設には権限のある者以外のアクセスを禁止する。警備員の採用や、写真入のIDカードの携帯を義務付けるほか、カードキー等の方法がある。

物理的アクセス・コントロールの例

a) カード

特定のIDカードの保有者を入室権限者とみなす方法。IDカードを紛失しても当該IDカードの失効手続を行うことでカードリーダ自体の更新は不要であるため、後述の「鍵」より優れている。

b) 鍵

鍵の保有者を入室権限者とみなす方法。鍵を紛失した際は、ドアの鍵を更新する必要があるため、紛失時の経済的損害が大きい。

c) 生体認証 **バイオメトリクス(Biometrics)認証**

静脈や指紋などを利用して、入室権限者を識別する方法。静脈や指紋などは変わることのない情報であるため、個人の特定が絶対的である。しかし静脈情報や指紋情報は最上位の個人情報であり、これらのデータが流出すると回復できないというデメリットがあるため、強固なセキュリティ対策の実施が必須となる。

d) キーパッド(コード入力)

数字の組み合わせなどのパスコードを知っている者を入室権限者とみなす方法。入室権限者の変更があればパスコードを変更する必要があるため、入室権限者の変動が激しい場合は適用に向かない。

環境的コントロール

コンピュータ・システムが安定的に稼働し続けるためには、コンピュータルームの管理も重要である。

a) 温度・湿度管理

コンピュータルームには多くのサーバーが設置されるため高温になりやすい。またコンピュータは湿度に弱いため、一般的にコンピュータ室には能力の高いエアコンを設置する。なおサーバールーム内の温度を一定にするために大型扇風機を設置する例もある。

b) 電源管理

コンピュータは電気で動く。通常、電源は停電の一種である瞬断が発生する。また停電発生時においてもシステムを正常終了させるためには一定期間システムの稼働を支える電源が必要である。これらの対応策として、無停電電源装置(UPS)を設置する。

また長期的な停電が発生しても稼働が求められるコンピュータ・システムがある場合は、自家発電装置の設置が必要となる。

c) 消火設備

サーバーは発熱するため、温度管理が適切でないと発火する可能性がある。また災害等によりサーバールームが被災し、消火を必要とする場合も考えられる。このような事態に備えて消火器が設置されるが、消火器は通常の粉末消火器ではコンピュータ・システムに粉末が詰まり使用できなくなるため、二酸化炭素消火器の設置が必要である。なお当然であるが、コンピュータルームにはスプリンクラーの設置は厳禁である。

10-4 全般統制 論理的コントロール

論理的コントロール

論理的コントロールは、ソフトウェアを利用して論理的な規則によってアクセス等の検討をする。

論理的アクセス・コントロール

システムへの侵入の回避

論理的アクセス・コントロールは、アクセス権限のある利用者を識別するシステムである。論理的アクセス・コントロールでは、無権限者のアクセスを回避し、承認された者に対してシステムを利用できる権限の範囲を与える。

組織体にとって最も重要な資産の一つであるデータへの効果的なセキュリティ・システムは以下のような保証を提供する。

- a) 権限のある利用者のみデータへアクセスできること
- b) アクセスのレベルはその必要性に応じていること
- c) データの修正には完全な監査証跡が残ること
- d) 未承認のアクセスは拒絶され、アクセスを試みたことが報告されること

論理的アクセス・コントロールの例

a) ユーザー認証

1) パスワード認証

ユーザー IDなどの識別情報とパスワードの組み合わせが一致する場合に、アクセスしようとしている者を正当な本人であると見なす方法である。パスワードにはユーザーが文字列を指定している場合もあれば、トークンなどで自動生成したコードを利用する場合もある。パスワードは秘匿性を高める必要があるため、ユーザーが文字列を指定する場合は、他人に推測されにくいパスワードにすることやパスワードを解析されにくいように一定以上の桁数や英数字混在などの複雑なパスワードにすることが推奨される。

3) 2段階認証

上述のパスワードは複数の認証場面で使いまわされることにより、1つが漏えいすると芋づる式に他の認証も突破されてしまう脆弱性を持っていた。このためパスワード単独での認証では限界があることから、パスワード認証に加えて、セキュリティコードなどによる認証を行う2段階認証が誕生した。

たとえば、システムにアクセスする時にパスワードだけでなく、メールで送られた数字を入力させることで、正当な本人であることを確認する。

b) ユーザー ID 管理

1) ユーザー ID の棚卸

ユーザー ID などの識別情報は常に最新の状態になっている必要がある。どれほど強固な認証の仕組みを実装していても、かつて権限者であった者が異動や退職などで無権限者になったにもかかわらず、ユーザー ID が付与されたままであれば十分なアクセス・コントロールが実現できているとは限らない。このためセキュリティ担当者を採用し、常にユーザー ID が最新化されている状況を担保することが望まれる。

c) 事後監視・その他

1) アクセス・コントロール・ソフトウェア

機密データの不正な改竄などを防止する機能を含むソフトウェア。ユーザー識別および認証の適用やログの記録を含む。

2) 監査ロギング

アクセス履歴

全てのアクセス試行を、その成功失敗にかかわらず記録しセキュリティ管理者に報告する機能(アクセス・コントロール・ソフトウェアの機能にも含まれる)。

3) 自動ログオフ機能設定

一定の時間操作をしないと自動的に接続が切られるという設定。

10-5 インターネットセキュリティ

インターネットセキュリティ

多くの組織のネットワーク(イントラネット)はインターネットと接続している。このため、インターネット経由でイントラネットにアクセスことが可能となり、場所を選ばずに仕事をすることが可能となるなど、利便性の向上が図られている。

しかしイントラネットへのアクセスを無制限に認めると機密情報の漏えいや組織内にある情報資産の破壊の恐れがあるため、一定のセキュリティ対策が必要となる。

b) ファイアウォール

ファイアウォールは、組織体内部のネットワークと外部のネットワークの間に設置され、組織体内のネットワークを外部から保護するためのセキュリティ・システムである。

ファイアウォールは、主に以下のようなことを可能とする。

- インターネット上における特定のサイトに対するアクセス防止
- 特定のユーザーによる、特定のサーバーやサービスへのアクセス防止
- 組織体の内部ネットワークと外部ネットワーク間の通信のモニタリング(監視)

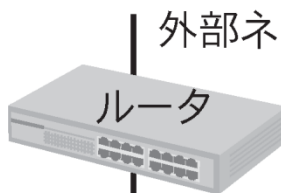
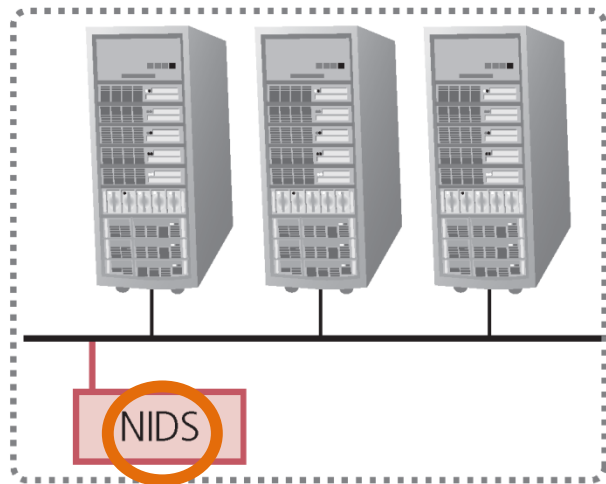
d) 侵入検知システム (Intrusion Detection System; IDS)

ネットワークの保護においてファイアウォールを補足するものに侵入検知システムがある。IDSはネットワークを使用する上での異常を監視することにより、不正アクセスの証拠を収集する。

ネットワーク上のIDS(NIDS)は、ネットワーク上を流れるパケットを監視し、不正アクセスを検知する。

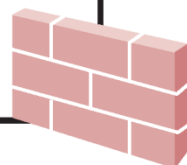
イントラネット

内部ネットワーク

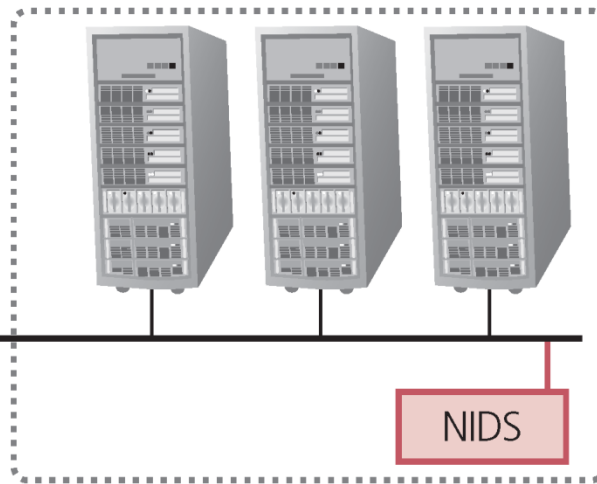


外部ネットワーク

インターネット



ファイア・ウォール



10-6 データの保存に係るセキュリティ

10-7 情報の保護

マルウェア(Malware)

マルウェアはシステムの破壊目的よりも金銭的利益を目的とするものが多い。コンピュータ・システムへ侵入し、パスワードや財務データを収集するなどの犯罪が増加し続けている。マルウェアには以下のようなものがある。

複製機能がある

ワーム
(worm programs)

利用者のディスクの空き容量やメモリがなくなるまで、自己増殖により破壊活動を行う。インターネットが普及するにつれ、電子メールなどを介して高速で自己増殖するものが出現している。

トロイの木馬 (Trojan horse)	正当なプログラムのコピー等外側からは他のもののように見えるが、無害なプログラムと利用者を信じ込ませてコンピュータへ侵入し、攻撃的手段によって、データ消去やファイルの外部流出などの破壊活動を行うプログラムのことである。トロイの木馬は単独の複製能力は持たないが、実行されるとより悪質なソフトウェアのインストールを可能にする等の影響がある。
論理爆弾 (logic bomb)	プログラムに特定の条件(特定の日、システム操作等)がそろった場合不正プログラムが作動する仕組みで、システム攻撃を開始する。
バックドア (back door)	通常の認証を回避し、不正侵入をするための裏口。(Wormによってもインストールされ得る。)

マルウェアに対するコントロール

マルウェアに対してはアンチウイルスソフトウェアによる検知、修復を通じて、感染前の状態に戻すことができる。ただし毎日のように新しいウイルスが誕生している現在においては、常に最新のウイルス定義にアップデートしておかなければマルウェアに対するコントロールとしては不十分である。

また、アンチウイルスソフトウェアは感染直前・又は感染後のコントロールとして有効であるが、そもそも感染させない、すなわち事前のコントロールを具備することも重要である。

事前のコントロールには、差出人不明の電子メールの添付ファイルを開かない等の利用者教育のほかに、組織が承認していないソフトウェアのインストール制限やウイルスの感染経路の一つであるUSBメモリなどを系統的に使用不可能にするなどが挙げられる。

様々な攻撃

現在のコンピュータ・システムは不正アクセスやコンピュータ・ウイルスなどの脅威にさらされている。悪意を持って他人のコンピュータのデータやプログラムを盗聴、改ざん、破壊などをするクラッカーと呼ばれる者が、インターネットなどのネットワークを通じて外部から様々な攻撃を仕掛けてくる。なおハッカーとはコンピュータに精通した人々に対する尊称であり、クラッカーとは区別される。

a)

Key Point: パスワードなどの情報を、IT技術を使わずに盗み取る行為（ex: 電話、肩越しに見る、ゴミ箱をあさる）

b) ソーシャルエンジニアリング(Social engineering)

権限のある利用者などから心理的な策略によってパスワードなどのセキュリティ上重要な情報を入手することである。例えば、IDカードを忘れたと偽って借りること、役職を偽って(他人になりすまして)アクセス方法を聞きだすこと等がある。

c) フィッシング(phishing)

正規のWebサイトや電子メールを装って、ユーザーからパスワードなどの情報を入手する手口。銀行のネットバンキングなどは金銭に直結するWebサイトであるため、フィッシングの標的になりやすい。

d) DoS 攻撃(Denial of Service attack)

DDOS

サービスの可用性を侵害することを目的とした攻撃である。一斉にデータを送信することによりネットワーク上のトラフィックを増大させ、一時的にサービスのレスポンスを著しく悪化させる攻撃である

Key Point



参 考

サイバー・セキュリティ関連用語

APT 攻撃 (Advanced Persistent Threat)	特定の相手に狙いを定め、その相手に適合した方法・手段を適宜用いて侵入・潜伏し、数か月から数年にわたって継続するサイバー攻撃。
アドウェア (Adware)	無料で使える代わりに広告を表示するソフトウェア。アドウェアがマルウェアのような動きをする場合がある
ブートセクタ感染型 ウイルス (Boot virus)	ブートとはコンピュータを起動し利用可能にするプロセスである。ブート領域に感染することによりコンピュータを起動不能に追い込むウイルスである
ボットネット (Botnet)	サイバー攻撃により乗っ取った多数のコンピュータで構成されるネットワークのこと

クリックジャッキング (Clickjacking)	ソーシャルメディア上の「いいね!」ボタンなどのクリック可能なコンテンツの下にハイパーリンクを隠し、クリックするとマルウェアのダウンロードや他のウェブサイトへ個人情報の送信などが実行されるサイバー攻撃。
クリプトジャッキング (Cryptojacking)	携帯端末やコンピュータを乗っ取り、ビットコインなどの暗号通貨のマイニング(発掘)行為に加担させるサイバー攻撃。 暗号通貨にはマイニングと呼ばれる次のチェーンを計算することで入手可能なものがあるが、計算には多くのCPUなどのITリソースを必要とすることから、近年増加傾向にある。
DDoS 攻撃 (Designated denial-of-service attack)	多量のマシンから1つのサービスに、一斉にDoS 攻撃を仕掛けること
マクロウイルス (Macro virus)	Microsoft Officeのマクロ機能を悪用したコンピュータ・ウイルス

Key Point

マルバタイジング (Malvertising)	不正広告とも呼ばれ、Web 広告からのマルウェア感染のこと
メモリ常駐型ウイルス (Memory-resident virus)	主にメインメモリに感染するウイルス。メインメモリ上に感染することによりアンチウイルスソフトウェアでの駆除が困難になる
パッチ (Patch)	バグ修正や機能変更を目的として既存プログラムを修正するプログラムのこと
ペネトレーションテスト (Penetration test)	検証対象のシステムに対して、想定される攻撃シナリオを複数用意し、実際に攻撃を行い、侵入または検証対象のデータの奪取ができるかどうかを検証するテスト。

ファームिंग (Pharming)	不正なスクリプトによってインターネットの閲覧者を偽のWebサイトに誘導し、不正に個人情報を得るフィッシング詐欺の類似手法
セッションハイジャック (Session hijacking)	通信を乗っ取り、本人に代わって「なりすまし」ログインを行うサイバー攻撃。本人変わってログインすることで、ログイン先の機密情報などを盗んだり、不正送金などを行う。
スパム (Spam)	一斉にばらまかれる迷惑メール
スプーフィング (Spoofing)	インターネット上で他人になりすまし、情報盗用などを行うこと。スプーフィング(なりすまし)には、メールの発信元のアドレスや名前を偽装するメールスプーフィング、偽のIPアドレスを用いてサーバーに侵入を試みるIPスプーフィング等がある。

スパイウェア (Spyware)	ユーザーに知られることなく情報収集することを目的とした不正なプログラム
デマウイルス (Virus hoax)	存在しないウイルスを存在するかのよう装う詐欺
ゼロデイ攻撃 (Zero-day attack)	システムに脆弱性が見つかり、修正プログラムが適用される日(これをOne Dayと呼ぶ)よりも前の攻撃のこと

10-8 データ保護法令

Fair Information Practices; FIP

Fair Information Practices(FIP)とは、連邦取引委員会(FTC)によって策定された個人情報取り扱いに関する原則的な運用についての原則であり、広く受け入れられているガイドラインである。連邦取引委員会は、1998年に報告書“Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress”を発行し、主に以下の4つの原則を列挙している。

a) 通知

個人情報を集める者は、事前に情報の取り扱いについて個人情報を持つ当事者に開示をすること

b) 選択

個人情報を収集してもよいかどうか、および収集する場合はその使用方法について、当事者に選択権を与えること

c) アクセス

収集した個人情報を当事者が参照及び訂正することが可能なこと

d) セキュリティ

情報の不正利用に対して妥当な手段を図ること

なお、FIPは米国プライバシー法およびEUデータ保護条令に採用されている。

EU一般データ保護規則(General Data Protection Regulation; GDPR)

EU一般データ保護規則(GDPR)は、EU加盟国における個人情報保護を目的とした管理規則であり、個人データの移転と処理について法的要件が定められている。

個人情報に関する規制は、EUの各加盟国法に委ねられていたため、各国間で差異があり、ビジネス上の障害となるケースがあった。この状況を改善すべく各加盟国法の個人情報保護に関する規制を廃止し、統一ルールを導入をするべく、EU一般データ保護規則が策定され、2018年5月より適用された。

EU一般データ保護規則で保護対象となる個人情報は、EU内に所在する個人のデータが対象となる。また個人のデータには以下が含まれている。

- 氏名
- 識別番号
- 所在地データ
- メールアドレス
- オンライン識別子(IP アドレス、クッキー)
- クレジットカード情報
- パスポート情報
- 身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関する要因

マネジメントと内部監査人の個人情報保護に関する役割

個人情報の漏えい事件が発生すると、企業の社会的信用が低下する。またお詫び料や損害賠償などの経済的損失だけでなく、個人情報を提供した会員の脱退などによる業績への影響などがある。このような損失から組織を守るための第一義的な役割・責任はマネジメントにある。このため、マネジメントには個人情報を適切に集めて、適切に使い、個人の権利利益を保護するために、PDCAサイクルを基本としたマネジメントシステムを構築する責任がある。

一方、内部監査人には、マネジメントが導入したPDCAサイクルが継続して運用されていることについて、内部監査を通じて担保することが求められる。具体的には、個人情報に関する関連法令に準拠していること、個人の権利保護や個人情報の安全管理措置の有効性と効率性を評価することになる。

10-9 最新のテクノロジーとセキュリティへの影響

Key Point

BYOD(Bring your own device)

私的デバイスの業務利用のこと。従来は情報漏洩リスクを危惧して私的デバイスの業務利用を禁止する企業が多かった。しかしながら、スマートフォンをはじめとした携帯端末の高性能化によりセキュリティ強化が可能になったことを背景に、常に持ち運んで使い慣れた私的デバイスを業務利用した方が効率的であることが増えたため、BYODを導入する企業が増えた。

BYODを導入する際、企業は以下のことを検討する必要がある。

- a) 私的デバイスを使用する際の基本的なルールの制定
- b) 私的デバイス自体のセキュリティ対策
- c) 紛失・盗難時の対応
- d) 退職時のデータの削除方法

検知システムを入れる

リモートワイプ

携帯端末を紛失した際、遠隔操作により全てのデータを削除(破壊)することで携帯端末から情報を抜き取ることを防止する技術のこと。BYODが広がった背景にはリモートワイプ技術の発展がある。

リモートワイプは遠隔操作によるデータの削除技術であって、工場出荷状態に戻すといった初期化の技術ではない。最近では特定のデータのみを削除することも可能になってきている。

スマート・デバイス(Smart Device)

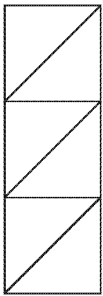
あらゆる用途に使用可能な情報機器の総称。スマートフォンやタブレットに限らず、個人の健康関連データを測定するウェアラブル機器やネットワーク接続された家電なども含む。スマート・デバイスは一つのOS上で様々なアプリケーションソフトウェアが稼働し、ネットワークとも常時接続していることが多いため、端末単体のセキュリティ対策として、認証やウイルス対策、暗号化、紛失・盗難対策などの実施が必要となる。

Key Point

MC 9–10–5

会社の中古パソコンを外部団体へ販売する際の方針を監査人がレビューする場合、次のどれが最大の関心事となるか。

- a. 消去したハードディスク上のファイルが、完全に削除されているかどうか。
- b. そのコンピュータがウイルスを持つかどうか。
- c. そのコンピュータで使用している全ソフトウェアは適切にライセンスを取得しているか。
- d. そのコンピュータに端末エミュレーションソフトウェアがあるかどうか。



コンピュータの譲渡に関する問題。

ほとんどの削除プログラムは、ファイルポインターを削除し、書き込まれているデータを消さない。会社は、そのデータを完全に消す特別のユーティリティソフトウェアを活用すべきである。これは、パソコン上に機密データが入っている可能性がある場合に重要なことである。

従って、正解はa。

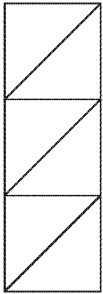
b, c, dは誤り。これらのデータを含めて全て削除されるべきである。

Key Point

MC10-3-2

データセンターの物理的セキュリティの設計において、考慮するのが適切でないのは次のどれか。

- a. 鉄道路線および高速道路の潜在リスクの評価
- b. バイオメトリックス・アクセス・システムの採用
- c. オペレーティング・システムに対するアクセス承認テーブルの設計
- d. 無停電電力供給システムと対雷防御を含めること



物理的コントロールに関する問題。

オペレーティング・システムに対するアクセス承認テーブルの設計は、論理的アクセス統制である。

従って、正解はc。

本問は、適切でないものを選択させる問題である。

a, b, dは選択されない。いずれも物理的セキュリティにかかるものである。

本日の論点

- ◆ 不測事態対応計画
- ◆ ITリスクとIT統制

Chapter 10

◎ 3, 4, 5, 7, 9

ジェイルブレイク(Jail break)・ルート化(Rooting)

スマホやタブレット、家庭用ゲーム機などの情報機器で、開発元がソフトウェアの実行環境に施している制限を非正規な方法で撤廃し、自由にソフトウェアを導入・実行できるようにすること。

主にI phoneに対してはジェイルブレイク、Androidに対してはルート化と言う。

ホット・サイト

本運用とほぼ同じシステムや設備を導入し、ミラーリングも行い、稼働状態で待機している

コールド・サイト

障害が発生した後に、機材の搬入、設定作業、バックアップデータ導入などを行う

ウォーム・サイト

ある程度の設備を揃え、非稼働状態で待機している

Key Point

顧客が要求した場合に、通信会社が要求に応じる義務が生じる可能性があるものは？

- A:** 現在の顧客から個人情報の利用方法について開示するように求められた
- B: 元顧客から過去10年間の通信利用に関する情報の提供を求められた

Key Point

あなたが持っている認証は？

- ① What you have
- ② What you know
- ③ What you are

- ① 本人しか持っていない認証を相手に提示できるか
(例：IDカード、メールで通知されるパスコード)
- ② 本人しか知らないはずの知識を相手に提示できるか
(例：パスワード、秘密の質問)
- ③ 本人の身体的特徴を照合する
(例：指紋、静脈、顔認証)