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。

Part 3 コースシラバス

			ページ
第1回	Chapter 1	戦略	1 〜 44
第2回	Chapter 2 Chapter 3	業績測定方法 組織行動	45 〜 90
第3回	Chapter 4 Chapter 5	リーダーシップ 組織構造とビジネス・プロセス	91 〜 142
第4回	Chapter 6 Chapter 7	データアナリティクス アプリケーションおよびシステム・ソフトウェア	143 〜 195

Part 3 コースシラバス

			ページ
第5回	Chapter 8 Chapter 9-1 ～ 9-8	ITインフラストラクチャー ITコントロール・フレームワーク、災害復旧	2 ～ 41
第6回	Chapter 9-9 ～ 9-10 Chapter 10	ITコントロール・フレームワーク、災害復旧 情報セキュリティ	42 ～ 78
第7回	Chapter 11-1 ～ 11-11	財務会計	79 ～ 103
第8回	Chapter 11-12 ～ 11-16 Chapter 12-1 ～ 12-4	財務会計 財務(ファイナンス)	104 ～ 150
第9回	Chapter 12-5 ～ 12-12	財務(ファイナンス)	151 ～ 182
第10回	Chapter 13-1 ～ 13-8	管理会計	183 ～ 204
第11回	Chapter 13-9 ～ 13-18	管理会計	205 ～ 227

9-9　不測事態対応計画

事業継続計画と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

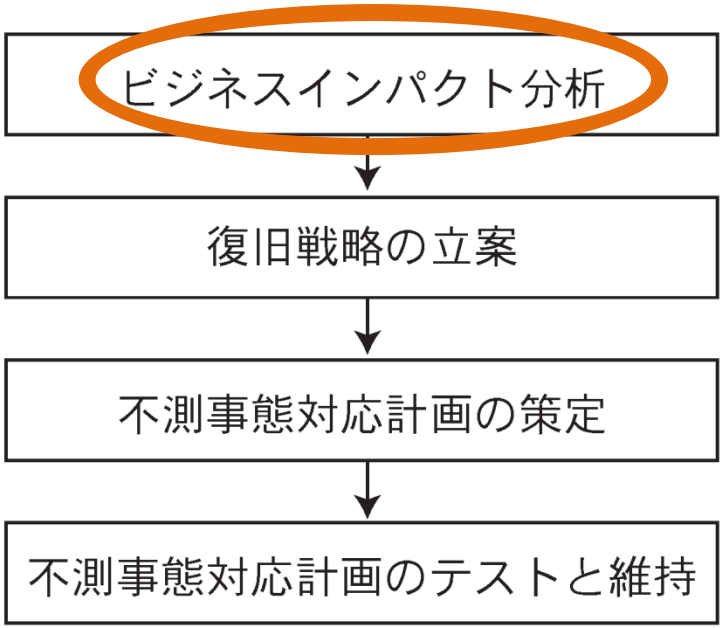
ITに関わる不測事態対応計画(contingency planning)とは、自然災害等により組織体にとって重要な機能を持つコンピュータ・システムや通信サービスが遮断された場合、どのように復旧するかの計画立案を含め、業務リスクを軽減させるように設計されたプロセスである。

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。



まず企業にとってのリスクと、リスクが顕在化した場合の業務への影響を分析する。

リスク分析やビジネス・インパクト分析を基に、予防、発見、是正的方法の組み合わせで立案する。

復旧計画を含めた詳細な計画の策定。

不測事態対応計画の有効性を検証し、また限界を識別する。

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%

b） 耐故障コンピュータ・システム、可用性コンピュータ

耐故障コンピュータ・システムとは、継続して中断されないサービスを提供するために、ハードウェア、ソフトウェア、及び電源装置の構成要素を重複して搭載しているコンピュータ・システムである。オンライン取引処理を必要とする航空会社や金融機関等は、100％の稼働率を確保するために伝統的に耐故障コンピュータ・システムを利用してきた。

可用性コンピュータも、耐故障コンピュータ・システム同様、バックアップのハードウェア資源を搭載しており、アプリケーションとシステムの可用性を最大化するように設計されている。ただ、可用性コンピュータは、障害が発生した際に即座に回復するためのシステムである一方で、耐故障コンピュータ・システムが利用可能な状態を継続するシステムであり、“回復させる時間”という概念がないという点において異なる。

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

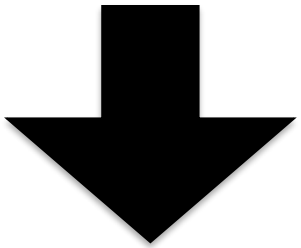
ミラーリングにおけるデメリットは以下のどちらか？

- コストがかかる ○
- 情報の保管に混乱が起きる ×

Key Point

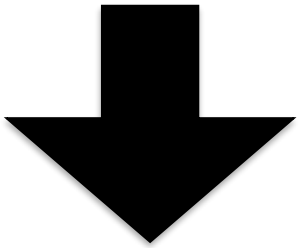
RPOとコストの関係性の問題

RPOが長い



コストが低い

RPO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。

10-1 ITに係るリスク

IT に係るリスクの定義

国際標準化機構(ISO)が発行する「IT セキュリティの管理に対するガイドライン」では、リスクを以下のように定義する。IT 業界では、この定義が通説となっている。

定義 脅威が起こる可能性は、資産の損失の原因となる単一または集合体としての複数の資産に内在する脆弱性にある。リスクの影響あるいはそれに関連する重大な問題は、営業価値の損失及び脅威の発生に対する予測頻度に比例する。

a） 脅威とは、情報資産に有害な状況をもたらす状況、事象である。脅威は情報資産の使用に関連した脆弱性により生じる。

b） 脆弱性は情報資産の特性であり、脅威を助長する。

> より具体的には、ITに係る脆弱性とは、情報資産、又はITプロセスにおいて、ビジネス・リスクやセキュリティ・リスクへと発展するかもしれない弱点や脅威にさらされることである。

c)　脅威の発生による結果を影響度とよび、損失を導く可能性がある。

d)　リスクは、影響度(損失)と脅威の発生頻度により計算され、分析される。

ITに係るリスクの分類

a） IT関連リスクは、以下の２つのグループに分類することができる。

天災、第三者不正アクセス

1） 全般的リスク	特定のシステムやプロセスに限定されることなく、企業全体に影響を与え得るリスク
（例）	インターネットを利用しているある企業のネットワーク・システムに、ファイアウォールが設定されていない場合、またはデータセンターの消火設備の動作確認が定期的になされていない場合等、関連するリスクは企業全体に影響を与え得る。
2） 特定のリスク	特定のプロセスや勘定残高に直接的に影響を与えるリスク
（例）	注文システムの不具合がもたらすリスク等

b） 内部監査人が、リスク・ベースの監査計画を策定するためにITリスクを評価する場合は、静的リスクおよび動的リスクについて考慮に入れる必要がある。

1） 静的リスク	組織体が業務を行う業界において典型的に引き起こされるリスクで、年によって変化をすることのないもの
（例）	オンラインで書籍を販売している企業にとって、オンラインの注文システムを搭載しているWebサーバーに関連するリスクが伴う。仮に、Webサーバーが停止した場合、直接売上に影響を与える
2） 動的リスク	常に変化し続けるリスクであり、技術の革新などによって引き起こされるもの
（例）	Windowsに代表されるOSにおける重大な欠陥の発覚

Windows 7 サポート終了、新しい法規制

1） 静的リスクは、多くの場合、質問とインタビューによる評価で十分であり、各評価についても毎年変更が少ない。

2） 動的リスクは、前年度そのリスクが存在しないため、前年のアップデートだけでは不十分である。リスク評価に際しては、インタビューにのみ頼るのではなく、パッチ管理等のその他の発見技法を用いる必要がある。また、発見後適切な分析が求められる。

動的リスクには、ITに関連する新しい法規制も含まれる。例えばプライバシーに関する法規制の違反リスクに対しては、情報の保管管理のための方針と手続の調査等が必要になる。

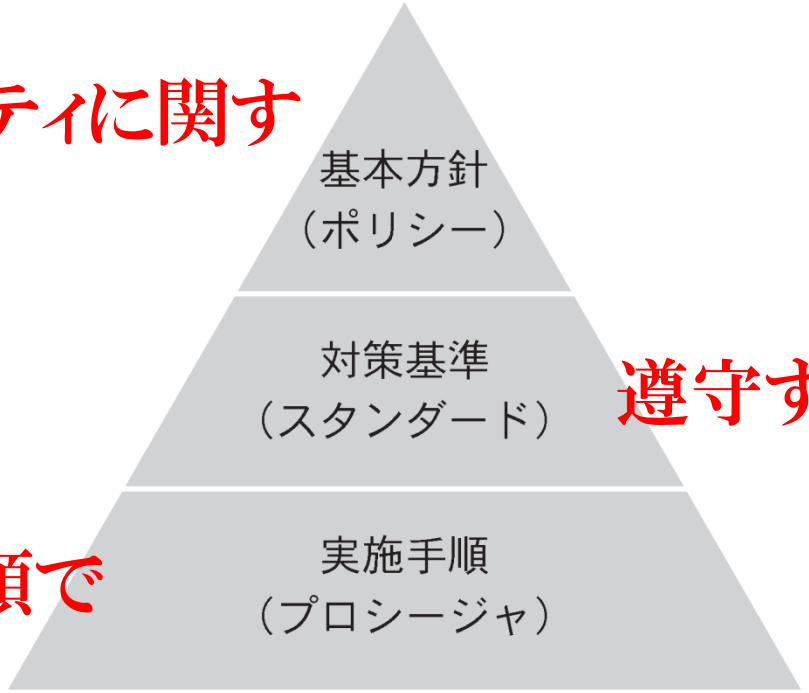
Key Point

情報セキュリティポリシー

ISMSに基づいて、情報セキュリティに関する組織内の取り組みを規定した文書を情報セキュリティポリシーという。

情報セキュリティポリシーは３階層の文書で構成されている。

情報セキュリティに関する基本方針



遵守すべき行為

どのような手順で実施するか

ポリシー

主旨、適用範囲、適用者、各人の責任

スタンダード

アップデートやライセンスのルール、パスワードの変更ルール

プロシージャ

パスワードの変更手順、操作方法

基本方針(ポリシー)は、情報セキュリティの必要性、目的、あるべき姿といった根本的な原則を定めるものである。基本方針は基本理念であるため、一度制定すると、原則として変更しない。ポリシーは各組織の状況や体制及び考え方に応じて策定するため、ポリシーにスタンダード(対策基準)が含まれる場合もある。

基準(スタンダード)には、ポリシーを実現するために組織が守るべき基本的なルールが記載される。また全プロシージャに共通のルールとしての位置づけもある。IT技術の発展や社内環境の変化に応じて改訂する。ISO/IEC 27002にてひな形が提供されている。

実施手順(プロシージャ)には、具体的な実施手順が記載される。セキュリティに関するマニュアルや標準業務手続書(SOP)が実施手順に該当する。

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が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。

論点　パスワード認証のセキュリティ強化

パスワード認証のセキュリティ強化のために以下のような機能が実装されることがある。

1）　一定回数以上パスワードを間違えるとアクセスできない。

2）　過去に使用したパスワードは利用できない。

アカウントの乗っ取りは、マシンによるパスワードの総当たり試行が多いことから、上記 1)の機能は、セキュリティ強化に特に有用である。

2） 端末認証

特定の端末のみにアクセスを限定することで、端末からのアクセスは正当なアクセスであるとみなす方法である。端末の利用者が正当な本人であるかどうかは端末への物理的・論理的なアクセス・コントロールで担保される。

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。

4)　コールバック

社外からのコンピュータへのアクセスを承認された従業員のみに制限する方法である。まず、従業員が会社のコンピュータ・システムを電話で呼びだし、ユーザー名、パスワードを入力する。システムは一度遮断され、その従業員がアクセスを許可された者であることが識別されると、システムが自動で利用者へ通信を行う。

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。

Key Point

ユーザー頼みとなり、脆弱性のあるコントロールは以下のどれか？

A: パスワード認証
B: パスワードの定期的変更
C: パスワードのロックアウト
D: 自動ログオフ

10-7 情報の保護

情報の保護

情報の重要性が高まれば高まるほど、機密性は高まる。

情報セキュリティ対策を実施する際に維持することが求められる要素の１つに機密性が含まれているように、情報が権限のない者に漏れないようにすることは、情報セキュリティを考える第一歩と言える。

eSACモデルによるITビジネスアシュアランス目標

eSACとはIIAが、eビジネスに関わるシステムの管理環境を評価するための枠組みとして作成したガイドラインである。

eSACではITビジネスアシュアランスの目標として、以下の5つが挙げられており、そのうちの1つに情報の保護に関する事項が含まれている。

可用性 （Availability）	情報、プロセス、サービスが必要な時に利用可能であることを保証すること
能力 （Capability）	システム処理が確実にかつ適正な時間で完了する能力を保有していること
機能性 （Functionality）	ユーザーのニーズを満たす機能、応答性、使いやすさを備えていること
保護性 （Protectability）	不正なアクセスや使用から、ハードウェアやソフトウェア、データが保護されていること
説明性 （Accountability）	システム処理が正確に完了したこと保証するために、個人の役割、行動、責任が明確にされていること

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メモリなどをシステム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）

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

不正コピー

コンピュータ・システムの領域において複製は容易に実行可能である。ソフトウェアも同様に複製が可能であり、ソフトウェアの製造元が了解していない複製は不正コピーと呼ばれ、使用許諾契約（ソフトウェアのライセンス契約）上の違反行為となる。

ソフトウェアのライセンス契約は、組織体とソフトウェアの製造元との間での契約であり、多くの場合、ソースコードのライセンスを組織体が購入しない限り、ソースコードを解明するためにソフトウェアの逆コンパイルあるいは逆行分析（リバース・エンジニアリング）を行うことを明確に禁止している。

なお、バックアップ対象にプログラムが含まれていることが多い今日においては、障害回復のためにバックアップとしてソフトウェアのプログラムをコピーすることの合意が使用許諾契約上に明記されていることが望ましい。

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。

ファーミング (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に装う詐欺
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

10-9 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。

Key Point

MC10-3-2

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

△ 8

Key Point

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。

アンチウイルスソフトなどの限界

既存のウイルスに対しては有効。新しいウイルスに対しては、更新が必要。

Key Point

企業への抗議活動としてサイバー攻撃をするとすれば、以下のどれを行うのが最も有効か？

A: ハッキング
B: フィッシング
C: 海賊行為
D: 改ざん

また一般に、ハッキングにはWebサイトの改竄行為も含まれると考えられます。
https://blogs.mcafee.jp/waht-is-hacking-and-prevention