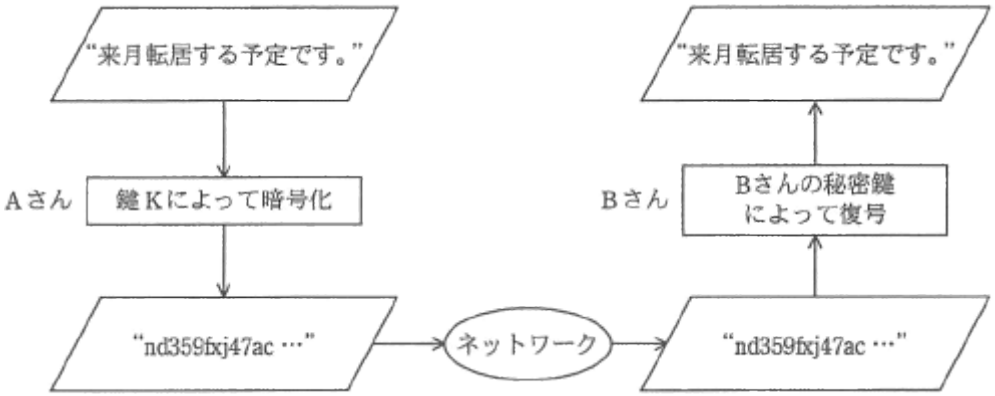
基本情報講座　　2013/6/26
分野：セキュリティー

例題１
公開鍵暗号方式を用いて，図のようにＡさんからＢさんへ，他人に秘密にしておきたい文章を送るとき，暗号化に用いる鍵 Ｋとして，適切なものはどれか。



Ａさんの公開鍵　ア、　　Ａさんの秘密鍵　イ、
Ｂさんの公開鍵　ウ、　　共通の秘密鍵　エ

正解ウ

解説
公開鍵暗号方式は、暗号化して送信することは誰でもできるが、暗号化された内容を復号できるのは正規の受信者だけという特徴をもつ暗号方式です。

この問題の場合、受信者はＢさんなので、Ａさんは Ｂさんの公開鍵で文章の内容を暗号化し、Ｂさんは自身の秘密鍵で復号をするという流れになります。したがって暗号化に用いる鍵は「Ｂさんの公開鍵」になります。

例題２
リスク移転を説明したものはどれか。
損失の発生率を低下させること　　ア
保険に加入するなど資金面での対策を講じること　　イ
リスクの原因を除去すること　　ウ
リスクを扱いやすい単位に分解するか集約すること　　エ

正解　　イ

解説
リスク対応には、リスクコントロールとリスクファイナンスの考え方があります。その双方にリスク移転という対応がありますが、
選択肢の中では「イ」がリスクファイナンスのリスク移転に該当します。保険に加入し他社に金銭的なリスクを移転する対策です。
ちなみにリスクコントロールのリスク移転とは、リスクのある業務をアウトソーシングするなどリスクを他者に移転する対策です。

損失の発生率を低下させること：リスク最適化の説明です。
保険に加入するなど資金面での対策を講じること：正しい。リスク移転の説明です。
リスクの原因を除去すること：リスク回避の説明です。
リスクを扱いやすい単位に分解するか集約すること：リスク最適化の手法の説明です。

例題３
SQL インジェクション攻撃を防ぐ方法はどれか。

入力中の文字がデータベースへの問合せや操作において，特別な意味をもつ文字として解釈されないようにする。　ア

入力に HTML タグが含まれていたら, HTML タグとして解釈されない他の文字列に置き換える。　イ

入力に，上位ディレクトリを指定する文字(../)を含むときは受け付けない。　ウ

入力の全体の長さが制限を越えているときは受け付けない。　エ

正解　ア

解説
SQL インジェクション攻撃は、データベースを扱うアプリケーションのセキュリティ上の不備を悪用して、データベースシステムを不正に操作する SQL 文を発行させる攻撃手法です。これを防ぐにはユーザの入力値の中で、SQL において特別な意味を持つ文字(単一引用符「'」やバックスラッシュ「＼」など)を、無効化してから SQL 文に組み込むことが重要かつ効果的な対策となります。

入力中の文字がデータベースへの問合せや操作において，特別な意味をもつ文字として解釈されないようにする：正しい。SQL インジェクション攻撃を防ぐ方法です。

入力に HTML タグが含まれていたら, HTML タグとして解釈されない他の文字列に置き換える：クロスサイトスクリプティング(XSS)を防ぐ方法です。

入力に，上位ディレクトリを指定する文字(../)を含むときは受け付けない：ディレクトリラバーサル攻撃を防ぐ方法です。

入力の全体の長さが制限を越えているときは受け付けない：バッファオーバフロー攻撃を防ぐ方法です。

小テスト

問題 1

X さんは，Y さんにインターネットを使って電子メールを送ろうとしている。電子メールの内容を秘密にする必要があるので，公開鍵暗号方式を使って暗号化して送信したい。電子メールの内容を暗号化するのに使用する鍵はどれか。

X さんの公開鍵　ア、　　X さんの秘密鍵　　イ
Y さんの公開鍵　ウ、　　Y さんの秘密鍵　　エ

正解　ウ

解説

公開鍵暗号方式は、受信者の鍵を使って暗号化・復号化をする暗号化通信方式です。
送信者は、受信者の公開鍵を使って暗号化したデータを送信し受信者は自分の秘密鍵を使ってデータを復号します。考え方としては暗号化は誰でもできるが復号できるのは、受信者だけということです。データが途中で傍受されても復号はできませんので安全性が確保されます。通信相手が複数いても必要となる鍵の数は 1 つだけでよく、共通鍵暗号方式で問題のあった事前の鍵送付・鍵の数の多さを克服した暗号方式です。
ただし暗号化・復号化するのにかかる時間は共通鍵暗号方式に比べて長いので、インターネット通信に使われる SSL では、両方を組み合わせたハイブリッド方式が用いられています。

問題の場合､X さんが Y さんに電子メールを送ろうとしているので暗号化に使用する鍵は、受信者 Y さんの公開鍵になります。

問題２
リスク移転に該当するものはどれか。

損失の発生率を低下させること　ア、
保険に加入するなどで他者と損失の負担を分担すること　イ、
リスクの原因を除去すること　ウ、
リスクを扱いやすい単位に分解するか集約すること　エ

正解　イ

解説
リスク移転とは、保険をかけたり契約を結ぶことでリスクに関する損失の負担を他者と分担する戦略です。
リスクが顕在化した場合の損失被害額と同額の保険をかけることは、保険会社にそのリスクを移転することになります。

損失の発生率を低下させること：リスク低減に該当します。
保険に加入するなどで他者と損失の負担を分担すること：リスク移転に該当します。
リスクの原因を除去すること：　リスク回避に該当します。
リスクを扱いやすい単位に分解するか集約すること：リスク分解・リスク集約に該当します。

問題３
SQL インジェクションの説明はどれか。

Web アプリケーションに問題があるとき，データベースに悪意のある問合せや操作を行う命令文を入力して，データベースのデータを改ざんしたり不正に取得したりする攻撃
ア

悪意のあるスクリプトを埋め込んだ Web ページを訪問者に閲覧させて, 別の Web サイトで, その訪問者が意図しない操作を行わせる攻撃
イ

市販されているDBMSの脆弱性を利用することによって，宿主となるデータベーサーバを探して自己伝染を繰り返し，インターネットのトラフイツクを急増させる攻撃
ウ

訪問者の入力データをそのまま画面に表示するWebサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送ることによって，訪問者のブラウザで実行させる攻撃
エ

正解　ア

解説
SQLインジェクション(SQL Injection)は、入力データとしてデータベースへの命令文を構成するデータを入力し、Webアプリケーションが想定しない想定外のSQL文を意図的に実行させることでデータベースを攻撃する行為です。
入力値の中でSQLとして特別な意味を持つ文字を適切にエスケープすることで防ぐことができます。DBMSやライブラリによってはエスケープ処理が自動化されているものもあり有用です。

Webアプリケーションに問題があるとき，データベースに悪意のある問合せや操作を行う命令文を入力して，データベースのデータを改ざんしたり不正に取得したりする攻撃：
正しい。SQLインジェクションの説明です。

悪意のあるスクリプトを埋め込んだWebページを訪問者に閲覧させて,別のWebサイトで,その訪問者が意図しない操作を行わせる攻撃：クロスサイトリクエストフォージェリの説明です。

市販されているDBMSの脆弱性を利用することによって，宿主となるデータベーサーバを探して自己伝染を繰り返し，インターネットのトラフイツクを急増させる攻撃：
SQL Slammerなどのセキュリティホールを付いて感染を広げるタイプのワームの説明です。
訪問者の入力データをそのまま画面に表示するWebサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送ることによって，訪問者のブラウザで実行させる攻撃：
クロスサイトスクリプティングの説明です。

問題４

データの破壊，改ざんなどの不正な機能をプログラムの一部に組み込んだものを送ってインストールさせ，実行させるものはどれか。
DoS 攻撃　ア、　　辞書攻撃　イ、
トロイの木馬　ウ、　　バッファオーバフロー攻撃　エ、

正解　ウ

解説
トロイの木馬は、実行形式のプログラム(.exe)を被害者が実行することで動作を開始し、一見通常の動作をしているように見せかけておいて、裏では OS の設定変更，パスワードの窃盗，外部からの遠隔操作の踏み台になるなどの悪意のある動作を秘密裏に行うウィルスです。

DoS 攻撃(Denial of Service)は、通常ではありえない数のリクエストをサーバに送信 することでサーバを過負荷状態にし、サーバのシステムダウンや応答停止などの障害を引き起こさせる攻撃手法です。

辞書攻撃は、パスワードとして利用されそうな単語を網羅した辞書データを用いて，パスワード解読を試みる攻撃手法です。

トロイの木馬
正しい。

バッファオーバフロー攻撃は、プログラム中に潜むバグを悪用し、入力データを受け取るバッファ領域の内外を上書きすることで誤動作を引き起こさせる攻撃手法です。

問題 5
DNS キャッシュポイズニングに分類される攻撃内容はどれか。

DNS サーバのソフトウェアのバージョン情報を入手して, DNS サーバのセキュリティホールを特定する。　ア

PC が参照する DNS サーバに誤ったドメイン情報を注入して，偽装された Web サーバに PC の利用者を誘導する。　イ

攻撃対象のサービスを妨害するために，攻撃者が DNS サーバを踏み台に利用して再帰的な問合せを大量に行う。　ウ

内部情報を入手するために，DNS サーバが保存するゾーン情報をまとめて転送させる。エ
正解　イ

解説
DNS キャッシュポイズニングは、DNS サーバからの名前解決要求があった場合に正常な応答に加えて偽の名前解決情報を付加して送信することで、そのサーバのキャッシュに偽の情報を登録させるという攻撃手法です。
この汚染された DNS サーバを利用したユーザが、偽のキャッシュ情報をもとに悪意のあるサイトに誘導され、機密情報を盗まれるなどの被害が発生する可能性があります。

DNS サーバのソフトウェアのバージョン情報を入手して, DNS サーバのセキュリティホールを特定する：ポートスキャンの説明です。

PC が参照する DNS サーバに誤ったドメイン情報を注入して，偽装された Web サーバに PC の利用者を誘導する：DNS キャッシュポイズニングの説明です。

攻撃対象のサービスを妨害するために，攻撃者が DNS サーバを踏み台に利用して再帰的な問合せを大量に行う。DRDoS 攻撃※の一種である DNS リフレクション攻撃の説明です。

内部情報を入手するために，DNS サーバが保存するゾーン情報をまとめて転送させる：
ゾーン転送要求を使用したターゲットサイトの情報収集行為の説明です。

DRDoS 攻撃※Distributed Reflection DoS の略。TCP，UDP，ICMP など TCP/IP の基本的な通信手順やアプリケーション仕様において発生する応答パケットを大量に発生させることでターゲットの帯域をあふれさせる反射型の DoS 攻撃。

問題 6
手順に示すセキュリティ攻撃はどれか。

〔手順〕攻撃者が金融機関の偽の Web サイトを用意する。
金融機関の社員を装って，偽の Web サイトへ誘導する URL を本文中に含めた電子メールを送信する。
電子メールの受信者が，その電子メールを信用して本文中の URL をクリックすると，偽の

Web サイトに誘導される。
偽の Web サイトと気付かずに認証情報を入力すると，その情報が攻撃者に渡る。

DDoS 攻撃　ア、　　フィッシング　イ、
ボット　　ウ、　　メールヘッダインジェクション　　エ

正解　イ

解説
フィッシング(phishing)は、銀行やクレジットカード会社、ショッピングサイトなどの有名企業を装ったメールを送付し、メール本文内のハイパーリンクをクリックさせることで、本物そっくりな偽の Web サイトに誘導し、設置してある入力フォームに入力した情報などの個人情報を不正に搾取する行為です。

DDoS 攻撃：
DDoS(Distributed Denial of Service)攻撃は、ネットワークを介して不特定多数のコンピュータをウィルスに感染させ、感染したコンピュータを遠隔操作することで標的のサーバへ一斉攻撃を仕掛けさせる攻撃をいいます。

フィッシング：
正しい。電子メールを使って偽の Web サイトに誘導するという流れからフィッシングとわかります。

ボット：
ボットは、感染したコンピュータを外部から遠隔操作できる状態にすることを目的に作られた悪性のプログラムです。

メールヘッダインジェクション：
メールヘッダインジェクションは、宛先(To)や件名(Subject)などのメールヘッダを入力フォームなどの外部から指定できる場合に、改行文字を使ってメールヘッダや本文を追加・変更する手法です。