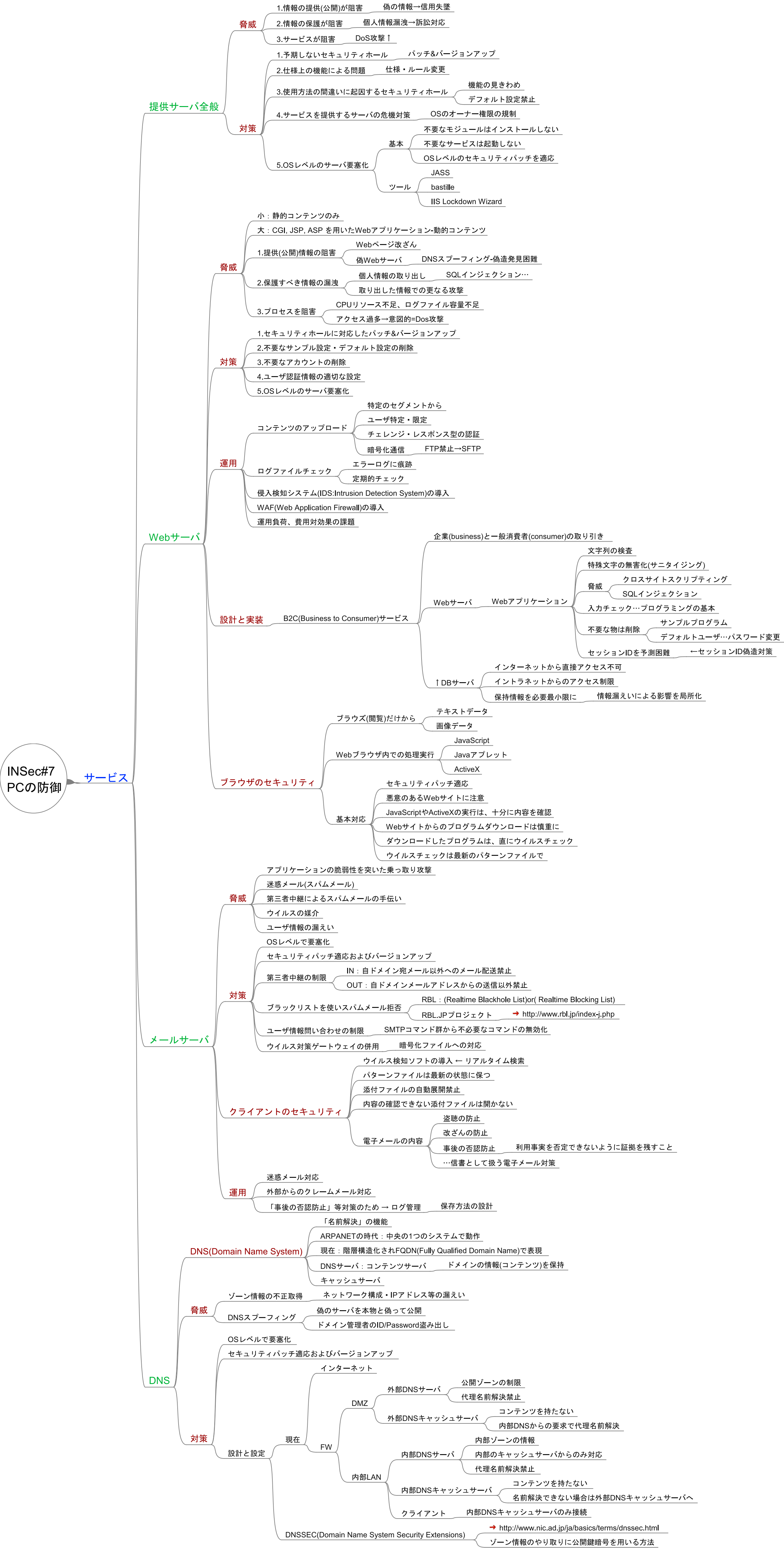
INSec#7
PCの防御
サービス
提供サーバ全般
脅威
1.情報の提供(公開)が阻害
偽の情報→信用失墜
2.情報の保護が阻害
個人情報漏洩→訴訟対応
3.サービスが阻害
DoS攻撃↑
対策
1.予期しないセキュリティホール
パッチ&バージョンアップ
2.仕様上の機能による問題
仕様・ルール変更
3.使用方法の間違いに起因するセキュリティホール
機能の見きわめ
デフォルト設定禁止
4.サービスを提供するサーバの危機対策
OSのオーナー権限の規制
5.OSレベルのサーバ要塞化
基本
不要なモジュールはインストールしない
不要なサービスは起動しない
OSレベルのセキュリティパッチを適応
ツール
JASS
bastille
IIS Lockdown Wizard
Webサーバ
脅威
小：静的コンテンツのみ
大：CGI, JSP, ASP を用いたWebアプリケーション-動的コンテンツ
1.提供(公開)情報の阻害
Webページ改ざん
偽Webサーバ
DNSスプーフィング-偽造発見困難
2.保護すべき情報の漏洩
個人情報の取り出し
SQLインジェクション…
取り出した情報での更なる攻撃
3.プロセスを阻害
CPUリソース不足、ログファイル容量不足
アクセス過多→意図的=Dos攻撃
対策
1.セキュリティホールに対応したパッチ&バージョンアップ
2.不要なサンプル設定・デフォルト設定の削除
3.不要なアカウントの削除
4.ユーザ認証情報の適切な設定
5.OSレベルのサーバ要塞化
運用
コンテンツのアップロード
特定のセグメントから
ユーザ特定・限定
チェレンジ・レスポンス型の認証
暗号化通信
FTP禁止→SFTP
ログファイルチェック
エラーログに痕跡
定期的チェック
侵入検知システム(IDS:Intrusion Detection System)の導入
WAF(Web Application Firewall)の導入
運用負荷、費用対効果の課題
設計と実装
B2C(Business to Consumer)サービス
企業(business)と一般消費者(consumer)の取り引き
Webサーバ
Webアプリケーション
文字列の検査
特殊文字の無害化(サニタイジング)
脅威
クロスサイトスクリプティング
SQLインジェクション
入力チェック…プログラミングの基本
不要な物は削除
サンプルプログラム
デフォルトユーザ…パスワード変更
セッションIDを予測困難
←セッションID偽造対策
↑DBサーバ
インターネットから直接アクセス不可
イントラネットからのアクセス制限
保持情報を必要最小限に
情報漏えいによる影響を局所化
ブラウザのセキュリティ
ブラウズ(閲覧)だけから
テキストデータ
画像データ
Webブラウザ内での処理実行
JavaScript
Javaアプレット
ActiveX
基本対応
セキュリティパッチ適応
悪意のあるWebサイトに注意
JavaScriptやActiveXの実行は、十分に内容を確認
Webサイトからのプログラムダウンロードは慎重に
ダウンロードしたプログラムは、直にウイルスチェック
ウイルスチェックは最新のパターンファイルで
メールサーバ
脅威
アプリケーションの脆弱性を突いた乗っ取り攻撃
迷惑メール(スパムメール)
第三者中継によるスパムメールの手伝い
ウイルスの媒介
ユーザ情報の漏えい
対策
OSレベルで要塞化
セキュリティパッチ適応およびバージョンアップ
第三者中継の制限
IN：自ドメイン宛メール以外へのメール配送禁止
OUT：自ドメインメールアドレスからの送信以外禁止
ブラックリストを使いスパムメール拒否
RBL：(Realtime Blackhole List)or(Realtime Blocking List)
RBL.JPプロジェクト
➜ http://www.rbl.jp/index-j.php
ユーザ情報問い合わせの制限
SMTPコマンド群から不必要なコマンドの無効化
ウイルス対策ゲートウェイの併用
暗号化ファイルへの対応
クライアントのセキュリティ
ウイルス検知ソフトの導入 ← リアルタイム検索
パターンファイルは最新の状態に保つ
添付ファイルの自動展開禁止
内容の確認できない添付ファイルは開かない
電子メールの内容
盗聴の防止
改ざんの防止
事後の否認防止
利用事実を否定できないように証拠を残すこと
…信書として扱う電子メール対策
運用
迷惑メール対応
外部からのクレームメール対応
「事後の否認防止」等対策のため → ログ管理
保存方法の設計
DNS
DNS(Domain Name System)
「名前解決」の機能
ARPANETの時代：中央の1つのシステムで動作
現在：階層構造化されFQDN(Fully Qualified Domain Name)で表現
DNSサーバ：コンテンツサーバ
ドメインの情報(コンテンツ)を保持
キャッシュサーバ
脅威
ゾーン情報の不正取得
ネットワーク構成・IPアドレス等の漏えい
DNSスプーフィング
偽のサーバを本物と偽って公開
ドメイン管理者のID/Password盗み出し
対策
OSレベルで要塞化
セキュリティパッチ適応およびバージョンアップ
設計と設定
現在
インターネット
FW
DMZ
外部DNSサーバ
公開ゾーンの制限
代理名前解決禁止
外部DNSキャッシュサーバ
コンテンツを持たない
内部DNSからの要求で代理名前解決
内部LAN
内部DNSサーバ
内部ゾーンの情報
内部のキャッシュサーバからのみ対応
代理名前解決禁止
内部DNSキャッシュサーバ
コンテンツを持たない
名前解決できない場合は外部DNSキャッシュサーバへ
クライアント
内部DNSキャッシュサーバのみ接続
DNSSEC(Domain Name System Security Extensions)
➜ http://www.nic.ad.jp/ja/basics/terms/dnssec.html
ゾーン情報のやり取りに公開鍵暗号を用いる方法