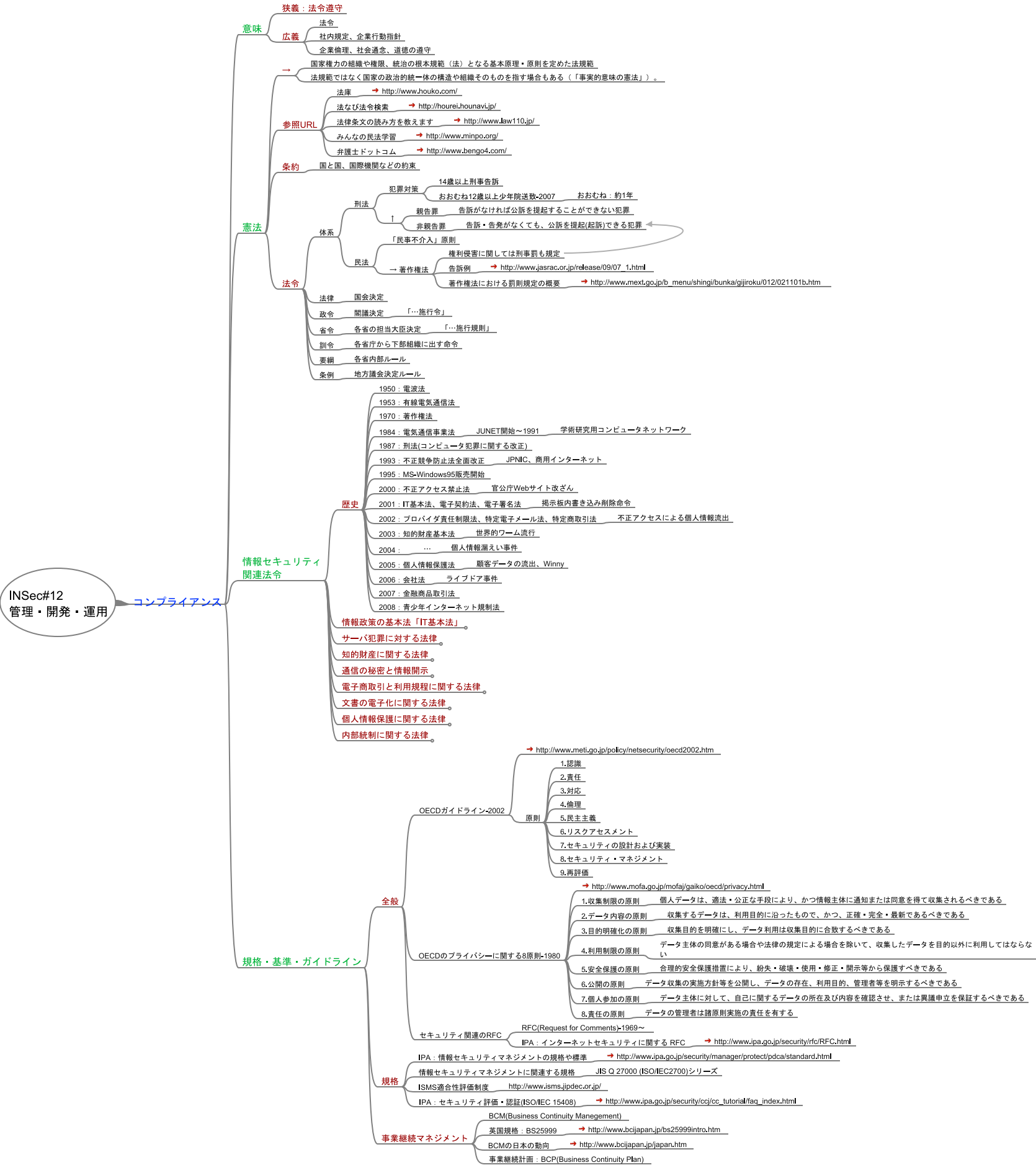
INSec#12
管理・開発・運用
コンプライアンス
意味
狭義：法令遵守
広義
法令
社内規定、企業行動指針
企業倫理、社会通念、道徳の遵守
→
国家権力の組織や権限、統治の根本規範（法）となる基本原理・原則を定めた法規範
法規範ではなく国家の政治的統一体の構造や組織そのものを指す場合もある（「事実的意味の憲法」）。
参照URL
法庫
→ http://www.houko.com/
法なび法令検索
→ http://hourei.hounavi.jp/
法律条文の読み方を教えます
→ http://www.law110.jp/
みんなの民法学習
→ http://www.minpo.org/
弁護士ドットコム
→ http://www.bengo4.com/
条約
国と国、国際機関などの約束
憲法
法令
体系
刑法
犯罪対策
14歳以上刑事告訴
おおむね12歳以上少年院送致-2007
おおむね：約1年
↑
親告罪
告訴がなければ公訴を提起することができない犯罪
非親告罪
告訴・告発がなくても、公訴を提起(起訴)できる犯罪
民法
「民事不介入」原則
→ 著作権法
権利侵害に関しては刑事罰も規定
告訴例
→ http://www.jasrac.or.jp/release/09/07_1.html
著作権法における罰則規定の概要
→ http://www.mext.go.jp/b_menu/shingi/bunka/gijiroku/012/021101b.htm
法律
国会決定
政令
閣議決定
「…施行令」
省令
各省の担当大臣決定
「…施行規則」
訓令
各省庁から下部組織に出す命令
要綱
各省内部ルール
条例
地方議会決定ルール
情報セキュリティ関連法令
歴史
1950：電波法
1953：有線電気通信法
1970：著作権法
1984：電気通信事業法
JUNET開始～1991
学術研究用コンピュータネットワーク
1987：刑法(コンピュータ犯罪に関する改正)
1993：不正競争防止法全面改正
JPNIC、商用インターネット
1995：MS-Windows95販売開始
2000：不正アクセス禁止法
官公庁Webサイト改ざん
2001：IT基本法、電子契約法、電子署名法
掲示板内書き込み削除命令
2002：プロバイダ責任制限法、特定電子メール法、特定商取引法
不正アクセスによる個人情報流出
2003：知的財産基本法
世界的ワーム流行
2004：…
個人情報漏えい事件
2005：個人情報保護法
顧客データの流出、Winny
2006：会社法
ライブドア事件
2007：金融商品取引法
2008：青少年インターネット規制法
情報政策の基本法「IT基本法」
サーバ犯罪に対する法律
知的財産に関する法律
通信の秘密と情報開示
電子商取引と利用規程に関する法律
文書の電子化に関する法律
個人情報保護に関する法律
内部統制に関する法律
規格・基準・ガイドライン
全般
OECDガイドライン-2002
→ http://www.meti.go.jp/policy/netsecurity/oecd2002.htm
原則
1.認識
2.責任
3.対応
4.倫理
5.民主主義
6.リスクアセスメント
7.セキュリティの設計および実装
8.セキュリティ・マネジメント
9.再評価
OECDのプライバシーに関する8原則-1980
→ http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html
1.収集制限の原則
個人データは、適法・公正な手段により、かつ情報主体に通知または同意を得て収集されるべきである
2.データ内容の原則
収集するデータは、利用目的に沿ったもので、かつ、正確・完全・最新であるべきである
3.目的明確化の原則
収集目的を明確にし、データ利用は収集目的に合致するべきである
4.利用制限の原則
データ主体の同意がある場合や法律の規定による場合を除いて、収集したデータを目的以外に利用してはならない
5.安全保護の原則
合理的安全保護措置により、紛失・破壊・使用・修正・開示等から保護すべきである
6.公開の原則
データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべきである
7.個人参加の原則
データ主体に対して、自己に関するデータの所在及び内容を確認させ、または異議申立を保証するべきである
8.責任の原則
データの管理者は諸原則実施の責任を有する
セキュリティ関連のRFC
RFC(Request for Comments)-1969～
IPA：インターネットセキュリティに関する RFC
→ http://www.ipa.go.jp/security/rfc/RFC.html
規格
IPA：情報セキュリティマネジメントの規格や標準
→ http://www.ipa.go.jp/security/manager/protect/pdca/standard.html
情報セキュリティマネジメントに関連する規格
JIS Q 27000 (ISO/IEC2700)シリーズ
ISMS適合性評価制度
http://www.isms.jipdec.or.jp/
IPA：セキュリティ評価・認証(ISO/IEC 15408)
→ http://www.ipa.go.jp/security/ccj/cc_tutorial/faq_index.html
事業継続マネジメント
BCM(Business Continuity Management)
英国規格：BS25999
→ http://www.bcijapan.jp/bs25999intro.htm
BCMの日本の動向
→ http://www.bcijapan.jp/japan.htm
事業継続計画：BCP(Business Continuity Plan)