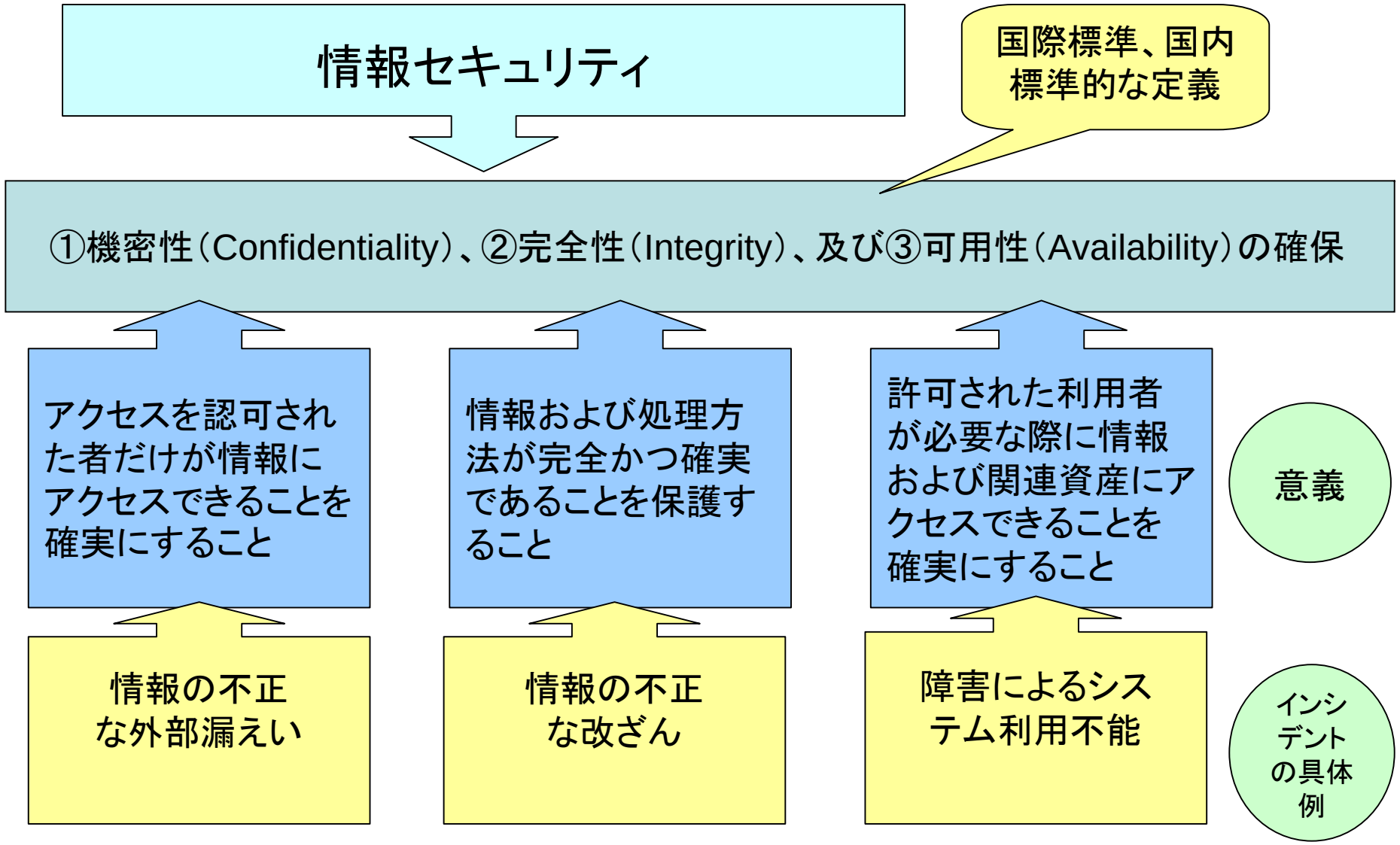
情報セキュリティと法制度

弁護士　国立情報学研究所客員教授
岡村　久道



CIA概念確立に至る経緯（時間順）

1992年のOECD情報セキュリティガイドライン（2002年改訂）
CIA概念初登場

1997年のOECD暗号政策ガイドライン
CIA概念承継

1998年のBS 7799 Part.1
英国規格

2000年のISO/IEC 17799
国際規格化

2001年のJIS X 5080
国内規格化

2001年の欧州評議会閣僚委員会サイバー犯罪条約
（わが国は2004年4月21日に国会で承認し、同年7月1日に効力発生）
第2章第1節第1款を「コンピュータデータ及びコンピュータシステムの機密性、完全性及び利用可能性に対する犯罪」と題して、各種犯罪類型を定める等。

1992年のOECD情報セキュリティガイドラインと法制度

- 法制度との関連を射程に入れたもの。
- 「実施」部分において、「このガイドラインに示される目的の達成及び原則の実施にあたり、政府及び公共部門、民間部門には、情報システムのセキュリティのため、適切な、法律、行政、自主規範その他対策及び実践、手続き、規則の確立及び確立の推進・支援が求められる。」として、法律等に言及。さらに、「規定がまだ策定されていない場合、以下のことをなすべきである。」として、いくつかの点に言及しており、そのなかで法制度と関連する箇所あり。
- もっとも、もともとOECD理事会勧告は法的拘束力を有する性格のものではない。
- そのため、同ガイドラインにかかるOECD理事会勧告も、「政府及び公共部門、民間部門は、……努力すべきである。」とするにとどまり、情報セキュリティのための法整備を加盟国等に対して義務づけるまでには至っていない。
- 同ガイドラインを2002年に改訂した「情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて」にかかるOECD理事会勧告も、「規定されたセキュリティ文化を取り入れ、普及させることによって、このガイドラインを反映し、かつ考慮した政策、実践、手段及び手続を新たに確立し、又は、既存のものを改正すること。」「この勧告の付属文書に規定される『情報システム及びネットワークのセキュリティのためのガイドライン：セキュリティ文化の普及に向けて』は強制的なものではなく、国家の主権に影響を及ぼさないことを認識し……推奨する。」とするにとどまる。

サイバー犯罪条約と法制度

- 機密性、完全性及び可用性に向けられた行為の抑止に必要な条約として位置付けられる。
- 「国内法レベルでとるべき措置」のうち、機密性、完全性及び可用性を侵害する犯罪行為として、次の条項を置いている。
  - 「違法な傍受」（第3条）
  - 「データの妨害」（第4条）
  - 「システムの妨害」（第5条）
  - 「装置の濫用」（第6条）
- これらの行為を自国の国内法上の犯罪とするため、必要な立法その他の措置をとるべきものとして、これを義務づける。
- これに対応するための刑事法改正案が提出されたが、現時点では未成立。

具体例一（不正指令電磁的記録作成等）
第百六十八条の二　人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。
一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録
二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録
2　前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。
3　前項の罪の未遂は、罰する。
（不正指令電磁的記録取得等）
第百六十八条の三　前条第一項の目的で、同項各号に掲げる電磁的記録その他の記録を取得し、又は保管した者は、二年以下の懲役又は三十万円以下の罰金に処する。
第百七十五条中「図画」の下に「、電磁的記録に係る記録媒体」を加え、「、販売し」を削り、「又は二百五十万円以下の罰金若しくは科料に処する」を「若しくは二百五十万円以下の罰金若しくは科料に処し、又は懲役及び罰金を併科する」に改め、同条後段を次のように改める。
電気通信の送信によりわいせつな電磁的記録その他の記録を頒布した者も、同様とする。
第百七十五条に次の一項を加える。
2　有償で頒布する目的で、前項の物を所持し、又は同項の電磁的記録を保管した者も、同項と同様とする。
第二百三十四条の二に次の一項を加える。
2　前項の罪の未遂は、罰する。

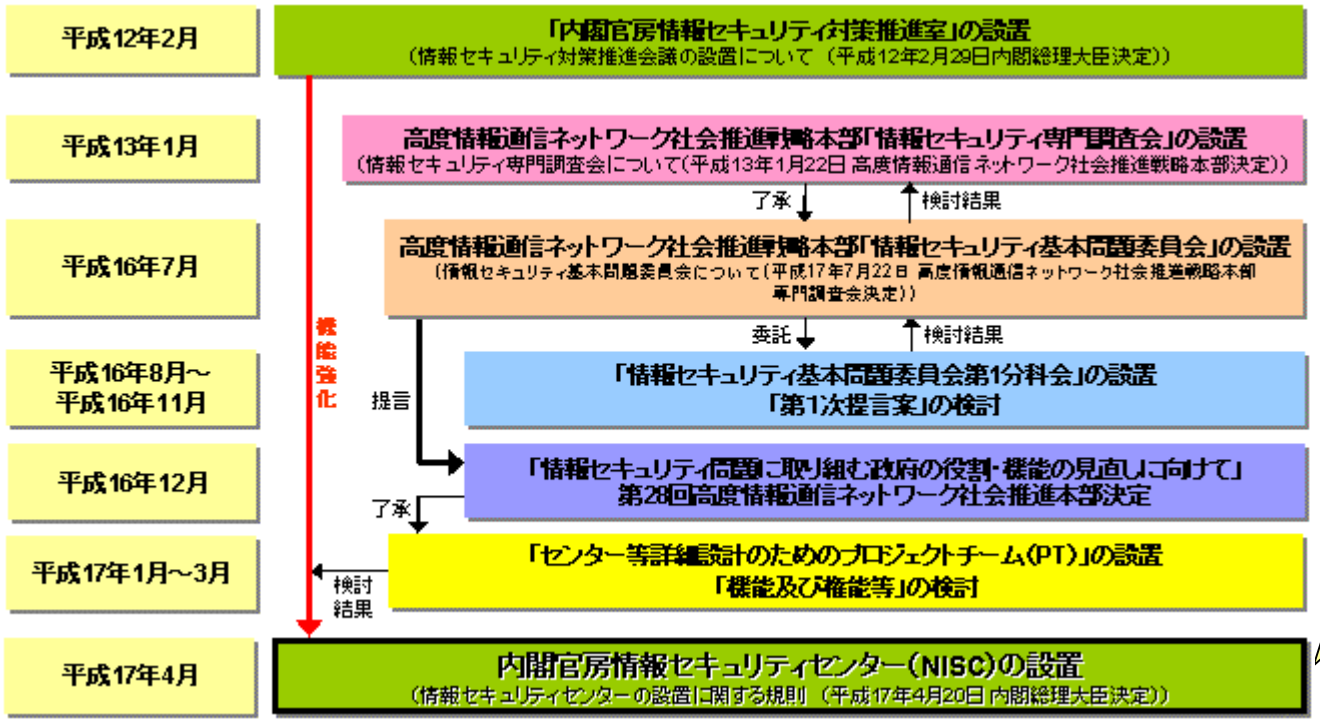
わが国の法制度と情報セキュリティ

- 情報セキュリティ全体を包括的に保護するための法令は現時点では不存在。
- 情報セキュリティという用語自体も、法律や政令には登場せず、いくつかの省令に登場する程度。
  - 現行法令中には、「プログラム」「インターネット」「ネットワーク」等の用語が用いられているものがある。これに加えて、後述のとおり、おおむねコンピュータを表す用語として「電子計算機」が、情報処理システムを表す用語として「電子情報処理組織」が、電子データに対応する用語として「電磁的記録」が登場。
- 「安全」「安心」といった用語がIT関連の法令を中心に散在している程度であり、そこでも「CIA」に対応した体系化はなされていない。
- 個々の現行法中には、「情報の漏えい、滅失又はき損の防止その他の情報の安全管理（適切な管理）のために必要かつ適切な措置」を講じるべきことを定めているものが少なくない。
  - 不動産登記法第123条第1項、個人情報保護法第20条から第22条まで、行政機関個人情報保護法第6条第1項・第9条、独立行政法人等個人情報保護法第7条第1項・第10条、電子署名に係る地方公共団体の認証業務に関する法律第4条、住民基本台帳法第30条の29第1項・第30条の33第1項・第36条の2第1項など
- 「情報の安全管理（適切な管理）のために必要かつ適切な措置」とは、「CIA」の3要素すべてを実質的に含んだ概念
  - 「その他の情報の安全管理（適切な管理）」のとおり、「漏えい、滅失又はき損」は例示にすぎないが、少なくとも漏えいが発生すれば機密性が損なわれ、滅失又はき損が、一部について発生すれば完全性が、相当部分以上について発生すれば可用性が損なわれる。

高度情報通信ネットワーク社会形成基本法（IT基本法）

- 第2条
  - 「高度情報通信ネットワーク社会」を「インターネットその他の高度情報通信ネットワークを通じて自由かつ安全に多様な情報又は知識を世界的規模で入手し、共有し、又は発信することにより、あらゆる分野における創造的かつ活力ある発展が可能となる社会」と位置づけて「安全」に言及。
- 第22条
  - 「高度情報通信ネットワークの安全性の確保等」の表題の下に「国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない。」と規定して「安心」に言及。
- 情報セキュリティという用語そのものは登場していないが、前記各条項には情報セキュリティが含まれているものと考えることができる 。
  - 法律案が衆議院内閣委員会において審議された際、政府側答弁において「安全でそして信頼の置ける高度情報通信ネットワーク社会を構築していく上で、情報セキュリティの確保ということが大変大切な基盤である」という認識が示されている 。さらに、この法律案が参議院交通・情報通信委員会において2000年11月28日に可決された際にも、「高度情報通信ネットワークの安全性及び信頼性を確保するため、ネットワークの脆弱性の解消、不正アクセスの防止、個人情報の保護等の情報セキュリティ対策を一層強化すること。」とする附帯決議が行われている。
- 同法は高度情報通信ネットワークのみを対象とするものであって、情報システム全体を対象とするものではない。しかし、2002年のOECD情報セキュリティガイドラインや2003年の国際連合総会決議（57/239）にも示されているとおり、今日において情報セキュリティの中心は情報ネットワーク関連であり、わが国において他に情報セキュリティに関し政府の責務を定めた法令が存在していないこと等の事情もあり、実際にはこの法律に基づき政府の情報セキュリティ政策が推進。

政府の情報セキュリティ対策推進体制



セキュリティ文化専門委員会等を開催して、民間部門を含めたセキュリティ文化の醸成につき調査検討
2002年のOECD情報セキュリティガイドラインの「セキュリティ文化」に対応

出典・内閣官房情報セキュリティセンター「内閣官房情報セキュリティセンター（NISC）設置までの経緯」

個人情報保護法と情報セキュリティ

- 個人情報保護法は、対象を個人データに限定しつつ、CIA全体を保護。
- 不正行為者の責任追及よりも、管理する側に責任を持たせる。
- 個人情報漏えい事故などでは、純然たる外部者の不正行為よりも、従業員など純然たる内部者、もしくは委託先によるケースが大半を占めていることを踏まえ、第21条（従業者に対する監督）および第22条（委託先に対する監督）が置かれた。
- 個人情報保護法の実効性担保は、主として主務大臣の関与による。
- すでに金融庁が漏えい事件につき、全面施行後初の勧告を行っている。
- 現行法は管理する側に責任を持たせるが、不正漏えい行為に対する直罰規定の導入に向けた法改正を検討中。

同法を軸に、情報セキュリティ策の整備が進行中。内容を具体化するための各省庁ガイドライン策定済み。

第20条（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人 データの安全管理のために必要かつ適切な措置を講じなければならない。

第21条（従業者の監督）

個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

第22条（委託先の監督）

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

機密性（Confidentiality）と法律　―刑事責任

- アクセスを認可された者だけが情報にアクセスできることを確実にすることを意味。
- 現在のわが国には情報の機密性全般を包括的に対象とする法律は不存在。
- 刑法
  - 情報が媒体その他の有体物の上に載せられている場合には、当該有体物は刑法によって保護され、当該有体物を不正に持ち出すなどして侵害する行為は窃盗罪・業務上横領罪等により処罰対象となりうる。その結果、有体物に載せられた情報も保護されうるが、それはあくまでも有体物が保護されることの反射的効果にすぎず、情報自体を保護しているわけではない。これに対し、情報だけが持ち出されるなどして、有体物と切り離された形で情報が侵害された場合は、刑法では原則として処罰の対象とはならない。
  - コンピュータ犯罪処罰規定を新設した1987年刑法一部改正でも機密性への対応は図られず。
- 個別分野に限定して機密性を保護する役割を営む規定
  - 資格等との関係で情報の保有主体を限定した処罰規定が存在。医師、弁護士、公務員など特定の職業に就いている者に対し、職務上知り得た情報について罰則付きで守秘義務を負わせる。
  - 客体となる情報の種類を限定して保護するための規定。通信の秘密、個人情報、営業秘密が、その具体例。
  - 特定の不正な手段による機密性侵害を禁止する法律も存在。不正アクセス禁止法など。
- 処罰規定は故意犯に限定され、過失による侵害事例の責任は民事責任・行政処分に委ねられている。

実際の事件では、むしろ紛失、気の緩みによる盗難被害の事例が多く、故意犯のケースは少ない。

機密性（Confidentiality）と法律　ー民事責任

- 不法行為責任においては、民法第709条の文言の抽象性ゆえに、情報セキュリティ関連の事件に対しても、支障なく適用することができる。しかも過失による場合であっても責任の追及が可能。
- 情報を漏えいすることによって損害を与えた場合に、漏えいによってプライバシーの権利を侵害されたとして不法行為に基づき損害賠償の対象となった事件は少なくない。
  - 宇治市住民基本台帳データ流出事件
  - 北海道警察江別署捜査情報漏えい事件
- 他に不正競争防止法に基づく営業秘密関連事件が多い。
  - 「秘密管理性」の要件との関係で、情報セキュリティ管理策を講じていなければ保護されないことに注意。
- 漏えいと懲戒処分との関係で訴訟になるケースも存在
  - 前橋信金事件

宇治市住民基本台帳データ流出事件

- 事　案
  - 京都府宇治市の住民基本台帳データ約22万人分が不正流出した事実が判明。市がメンテナンスを委託していた電算業者（A社）の下請（B社）に児童検診用データを預けていたところ、B社のアルバイト大学生が自分で持参した光磁気ディスク（MO）にコピーして持ち出し名簿業者に無断売却、インターネット上で販売されていた事案で、住民3名から市への損害賠償請求事件。
- 第一審（京都地判平成13年2月24日）
  - 請求一部認容（弁護士費用を含め総額計45000円の支払を命じた）
- 控訴審（大阪高判平成13年12月25日）
  - 市の控訴を棄却
  - 「控訴人は、A社がB社に再委託することを承認し･･･、控訴人の担当職員は、乳幼児検診システムの開発業務について、現にC社の代表取締役であるAや従業員であるBと打ち合わせを行い、従業員Tも、この打ち合わせに参加し･･･Bと従業員Tは、当初、控訴人の庁舎内で乳幼児検診システムの開発業務を行って」おり、「本件データを庁舎外に持ち出すことについても控訴人の承諾を求めたのである。これらの事実に照らすと、控訴人と従業員Tとの間には、実質的な指揮･監督関係があったと認め」られるので、市は使用者責任を負う。
- 上告審（最決平成14年7月11日）
  - 市の上告を棄却
- ポイント
  - 不正行為者本人ではなく、情報管理者側が民法上の使用者責任により責任を負う。使用者責任は実質的な無過失責任。

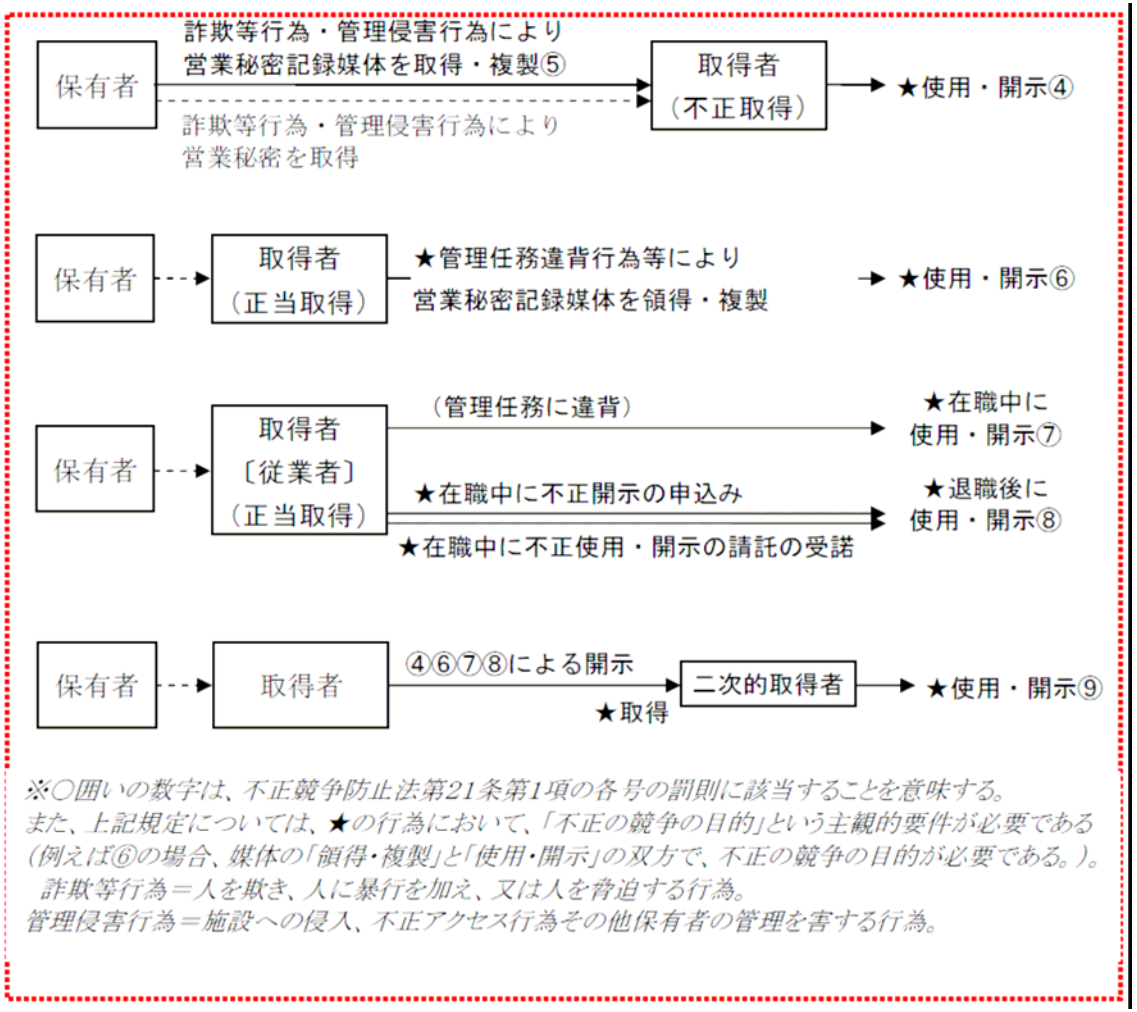
北海道警察江別署捜査情報漏えい事件

- 事案
  - 道交法違反容疑で逮捕、不起訴となった江別市の男性会社員（原告）を被疑者とする捜査関係文書が、北海道江別署の男性巡査の私有パソコンからインターネットを通じて外部に流出したとして、原告の被った精神的損害の賠償200万円を北海道（被告）に請求した訴訟。ファイル交換ソフト「Winny」を私有パソコンにインストールしており、パソコンがアンティニーウイルスに汚染されていることを知らずに、私的な目的でWinnyを起動させインターネットに接続した結果、パソコンのデスクトップ画面上に保存されていた捜査関係文書がアンティニーによってパソコンの公開用フォルダに複写され、他のWinny利用者に閲覧可能な状態となり、そのことがインターネット利用者の情報交換を目的とするホームページに掲載されたこともあって、捜査情報が不特定多数のWinny利用者によって閲覧され、ダウンロードされるに至った。
- 第一審（札幌地判平成17年4月28日）
  - 巡査がパソコンを使用して本件捜査関係文書を作成した際に作成途中の同文書をハードディスクに保存した行為は職務行為そのものであり、また、同巡査が上記文書をパソコン内に保存したままパソコンを自宅に持ち帰り、インターネットに接続させた行為は、作成途中の本件捜査関係文書の保存、管理という点において捜査関係文書の作成という職務行為と関連して一体不可分のものというべきであるから、巡査の上記原因行為は「職務を行う」についてのものということができるとして、慰謝料40万円の支払を北海道に命じた。
- 控訴審（札幌高判平成17年11月11日）
  - 原判決を取り消し、請求棄却。報道によれば、自宅でネット接続した行為を「職務とは無関係の行為」と判断。道警の管理責任については「当時、このウイルスは広く知られておらず、流出の予見可能性はなかった」とした。

不正競争防止法による営業秘密の保護

- 民事的保護と刑事的保護あり。
- この法律では、①秘密管理性、②有用性及び③非公知性という3要件をすべて満たす必要がある。
- 要件①の判断基準として次の点を掲げる判例が多い。
  - (1)当該情報にアクセスした者に当該情報が営業秘密であることを認識できるようにしていること(客観的認識可能性)
  - (2)当該情報にアクセスできる者が制限されていること(アクセス制限)
- さらに具体的な認定要素として、コンピュータ処理用顧客データ社外持ち出し事案の判例では、パスワード等によるデータへのアクセス・閲覧制限、データのコピー・出力等の規制、保管場所の施錠・入退室制限、就業規則等による機密保持義務条項、社内教育・指導による周知徹底等の有無が総合的に判断される傾向にある

情報セキュリティ管理策を講じていなければ保護されないことに注意



出典・経済産業省「営業秘密管理指針改訂版」

労働法関係　一前橋信金事件

- 漏えいと懲戒処分
  - 企業が自社の保管する顧客名簿を従業員に持ち出されて漏えいしたような場合、社内規程で懲戒の対象として規定されていることを前提条件として、社内で懲戒処分の対象となりうる。こうした懲戒処分の効力が争われたケースとして、前橋信金事件がある。
- 事　案
  - 信用金庫（被告）の労働組合が事実上分裂し、組合代表者たる職員（原告）が、他の職員に被告のオンライン端末機を正規の手続を経由せず無断で操作させて、同信金従業員組合会計名義の預金残高を確認したところ、就業規則違反に該当するとして被告から懲戒処分を受けた。これを不服とした原告が被告を相手取って懲戒処分の効力を争った。
- 第一審（前橋地判昭和61年5月20日）
  - 被告が定めたオンライン事務取扱要領が、全職員に配布されず、端末機の操作に関し現実には被告が想定していた取扱要領に反する運用がなされていた点などを重視して、前記懲戒処分を無効とした。
- 控訴審（東京高判昭和62年8月31日）
  - 取扱要領に反する運用の実状であったので，被告は運用・管理に関する文書を各店長宛に交付し、説明会を開くなどして取扱要領に従い端末機の扱いを周知徹底させるべく努力していたことなどを認定して、前記懲戒処分を有効とした。
- ポイント
  - 適正な情報セキュリティ・マネジメントを講じていなければ、法的保護を受けることができないおそれがあるという事実が示されている半面、適正な情報セキュリティ技術を講じておれば法律によって保護されるという意味で、両者間に協力・補完関係が存在。

完全性（Integrity）

- 情報および処理方法が完全かつ確実であることを保護することを意味。
- 紛争の典型例は、情報の不正な改ざん行為
- わが国の判例上では金融機関におけるオンライン詐欺の事案が多い。
  - 三和銀行事件の大阪地判昭和57年7月27日
  - 第一勧銀事件の大阪地判昭和63年10月７日
  - その他
  - 電子計算機使用詐欺罪によって処罰
- 金融機関以外における故意によって完全性が侵害された事例
  - 朝日放送クラッキング事件の大阪地判平成9年10月3日
  - 霞ヶ関中央省庁連続クラッキング事件（2000年1月発生）
  - ニフティ電子掲示板詐欺事件の京都地判平成9年5月9日
  - パチンコ遊技台裏ロム事件の福岡高判平成12年9月21日
- 過失による完全性の侵害事例の典型例はコンピュータの誤操作事案
  - 日本相互銀行コンピュータ誤操作事件の福岡地判昭和53年４月
  - 三和銀行コンピュータ誤操作事件の札幌高判昭和55年6月
  - 預金者名コンピュータ誤入力事件の東京地判平成10年7月14日

偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律（平成17年法律第94号）

- 平成17年 8月 3日成立、平成17年 8月10日公布。
- 偽造・盗難カード等を用いて行われる不正な払い戻し等により預金者に生じた損害について、原則として金融機関に補償を義務づける。
  - 偽造カード等を用いて行われた払い戻し等による損害については、簡単に偽造されてしまうような脆弱なシステムを使っている金融機関の責任が重いことから、預金者に重大な過失がない限り、金融機関がその損害の全額を負担。
  - 次に、盗難カード等を用いて行われた払い戻し等による預金者の損害については、預金者に重大な過失がある場合を除き、原則として金融機関がその損害の全額を補てんするものとしているが、脆弱なシステムを提供している金融機関の責任と、不正な払い戻しが行われるに至った預金者側の事情を考慮して、預金者に重大な過失以外の過失があることが金融機関により証明された場合には、損害の4分の3を補てん。
  - 預金者の過失については立証責任の転換を図り、預金者に過失があることの立証責任は金融機関にあることとした。
- 偽造・盗難カード等を用いた不正な払い戻し等が行われないようにして、預金者がその預金を安心して預けられるよう、金融機関に対し、預金者の利便性を損なうことなく、現在の我が国の脆弱なATMシステムを改め、安全性の高い、世界に冠たるATMシステムの再構築を行うために必要な措置について規定。

可用性（Availability）

- 許可された利用者が、必要な際に情報および関連資産にアクセスできることを確実にすること
- みずほフィナンシャルグループ大規模システム障害発生事件
- 世田谷ケーブル火災事件の東京高判平成2年7月12日
- ハードディスク・データ消失事件の広島地判平成11年2年24日
  - 原告がパソコン内蔵ハードディスク容量を増大させるために新たなハードディスクを購入し、販売店（被告）に旧ディスクから新ディスクへの交換を依頼したところ、被告の従業員が誤って旧ディスクを初期化したので、旧ディスク内に記録されていた原告の業務上不可欠な多量のデータがすべて消去された事案で、被告に損害賠償責任が認められた。
- レンタルサーバ・データ消滅事件の東京地判平成13年9月28日
  - 納入した製品が可用性を欠くとして取引先から訴えられた事案であり、インターネット接続プロバイダ（被告）のレンタルサーバ内に保管されていた原告の電子商取引サイト用コンテンツデータを、システム変更の際に被告が誤って消滅させたことを理由とする損害賠償請求を一部認容した。
- 東京電送センター事件の東京地判平成8年7月11日
  - コンピュータ機器の売買契約で、買主が機器に瑕疵を発見したときは直ちに売主に内容を通知すべき約定がある場合、通知を受ける都度、売主が機器を調査して代替品との交換又は修理等の必要な措置を行い、瑕疵ある状態を解消すれば、売主は債務不履行責任を負わないとした。

企業会計審「財務報告に係る内部統制の評価及び監査の基準（公開草案）」（2005年7月13日）

- 企業会計審「内部統制監査」では、ITの利用による業務の効率化は内部統制の要素。
- 内部統制とは、企業等の4つの目的（①業務の有効性及び効率性、②財務報告の信頼性、③事業活動に関わる法令等の遵守、④資産の保全）の達成のために企業内のすべての者によって遂行されるプロセスであり、次の6つの基本的要素から構成。

①統制環境
②リスクの評価と対応
③統制活動
④情報と伝達
⑤モニタリング
⑥ITの利用

情報セキュリティと内部統制とは関連性を有する

- 参考－大和銀行株主代表訴訟第一審判決（大阪地判平成12年9月20日）
  - さまざまなリスクに対する企業の対応について、「健全な会社経営を行うためには、目的とする事業の種類、性質等に応じて生じる各種のリスク‥‥の状況を正確に把握し、適切に制御すること、すなわちリスク管理が欠かせず、会社が営む事業の規模、特性等に応じたリスク管理体制（いわゆる内部統制システム）を整備することを要する。そして重要な業務執行については、取締役会が決定することを要するから（商法260条2項）、会社経営の根幹に係わるリスク管理体制の大綱については、取締役会で決定することを要し、業務執行を担当する代表取締役及び業務担当取締役は、大綱を踏まえ、担当する部門におけるリスク管理体制を具体的に決定するべき職務を負う。」と判示して、これを怠った当時の経営陣に対し、当時の為替レートで約計830億円もの支払いを命じた。

新会社法と内部統制

- 348条3項4 号
  - 取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備
- 362条4項
  - 大会社においては、取締役は、前項第4号に掲げる事項を決定しなければならない。

- 362条4項6号
  - 取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備
- 362条5項
  - 大会社である取締役会設置会社においては、取締役会は、前項第6号に掲げる事項を決定しなければならない。

- 416条1項1号ホ
  - 取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備
- 362条2項
  - 委員会設置会社の取締役会は、前項第1号イからホまでに掲げる事項を決定しなければならない。

商法施行規則193条6号
執行役の職務の執行が法令及び定款に適合し、かつ、効率的に行われることを確保するための体制に関するその他の事項

委任禁止

その他の問題

- 無線タグ・生体認証
  - 個人情報保護法とガイドラインで対応
- 無権限アクセスでの侵入行為
  - 無権限での侵入行為は不正アクセス禁止法で禁止。書き換え等を伴う場合やDdos攻撃は刑法の電算機損壊等業務妨害罪の対象。
- ウイルス
  - 配布行為は刑法の電算機損壊等業務妨害罪の対象
  - 処罰範囲拡張に向けて、現在、国会で刑法改正審議中
- 迷惑メール
  - 特定電子メール送信適正化法、特定商取引法等で規制
- ワン切り
  - 有線電気通信法で規制
- 架空請求メール、ワンクリック詐欺、振り込め詐欺
  - 刑法の詐欺罪、本人確認法等で対処
- フィッシング（Phishing）詐欺
  - 著作権法違反で摘発
- 残された課題
  - ゾンビPC、ボットネット、スパイウェア等の規制