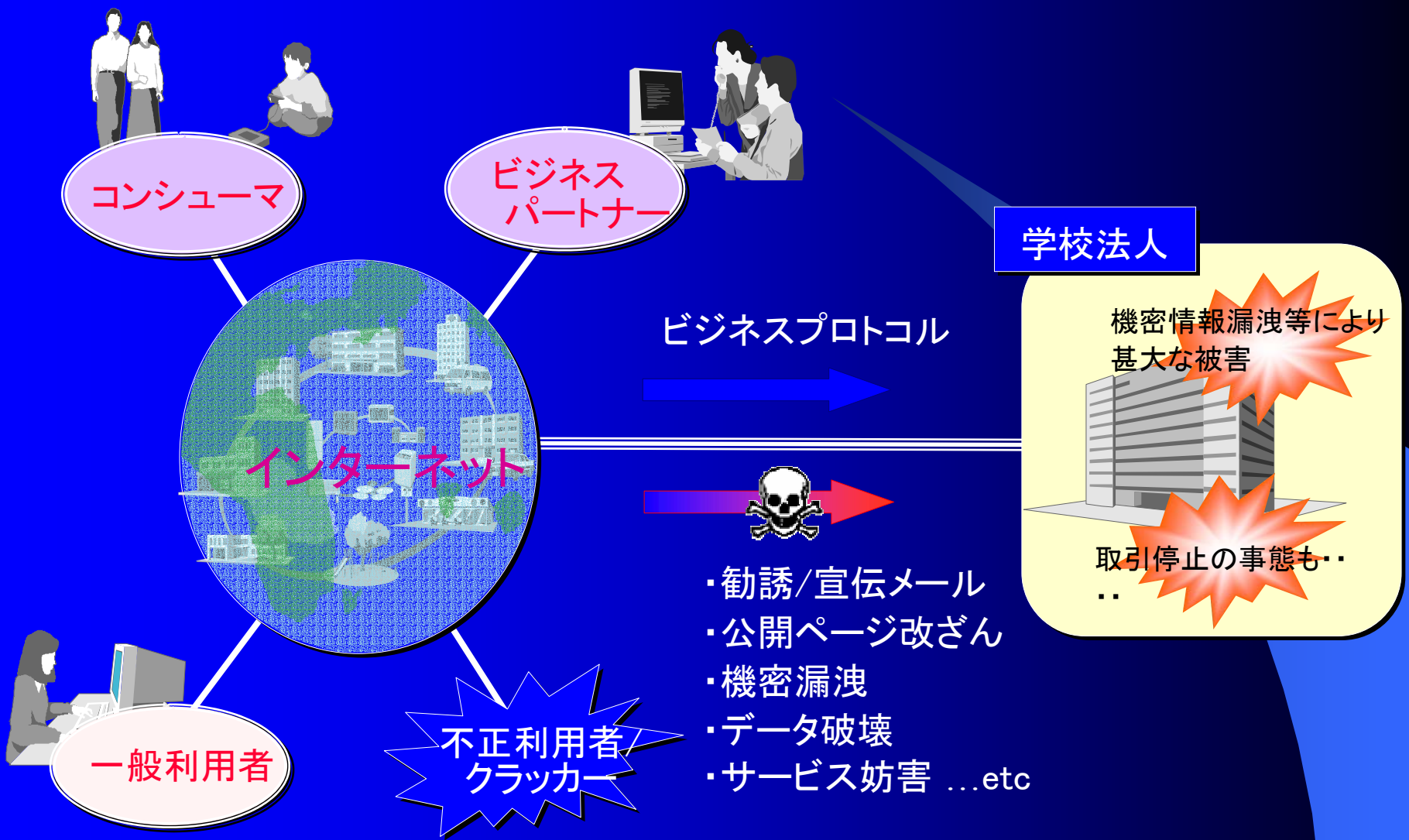
学校法人の個人情報リスク

個人情報保護法からみた
学校現場のリーガルリスク

主催：21世紀大学経営協会
ガバナンス委員会第１回セミナー
2004年12月22日

NIS　田淵義朗
tabu@gincorp.co.jp

ビジネスと犯罪者が混在するインターネット



情報犯罪の種類

- 不正なリソースの使用
- 不正な情報の取得
- 情報改ざん
- システム破壊

被害の影響

学内資源の損害
- システム機能停止
- 貴重なデータの損失
- 機密の漏洩

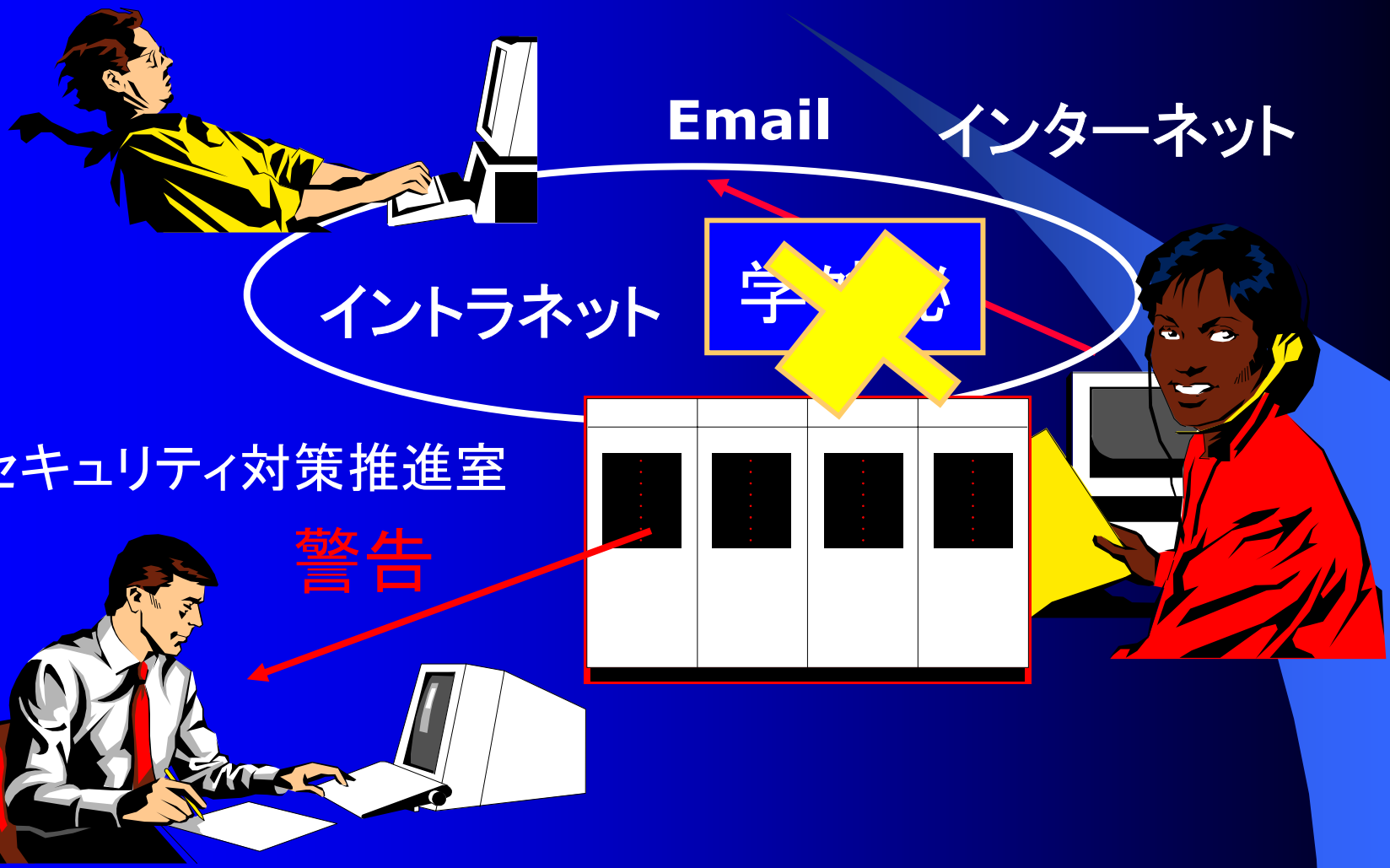
第3者への間接的影響
- 個人情報の流出
- 成りすましによる詐欺
- データの悪用

莫大なる金銭的損害

対外的信用の失墜

セキュリティ対策の重要性増大
インターネット使用の条件・義務的要素に

電子メール監視体制の強化



URLフィルタリング

セキュリティ対策

忙しい・・忙しい
見積書を昼までに・・と

実際は・・・

必要ないカテゴリーのHPを閲覧出来ない様に規制をかける
ソフトウェア＝**URL**フィルタリング製品の導入

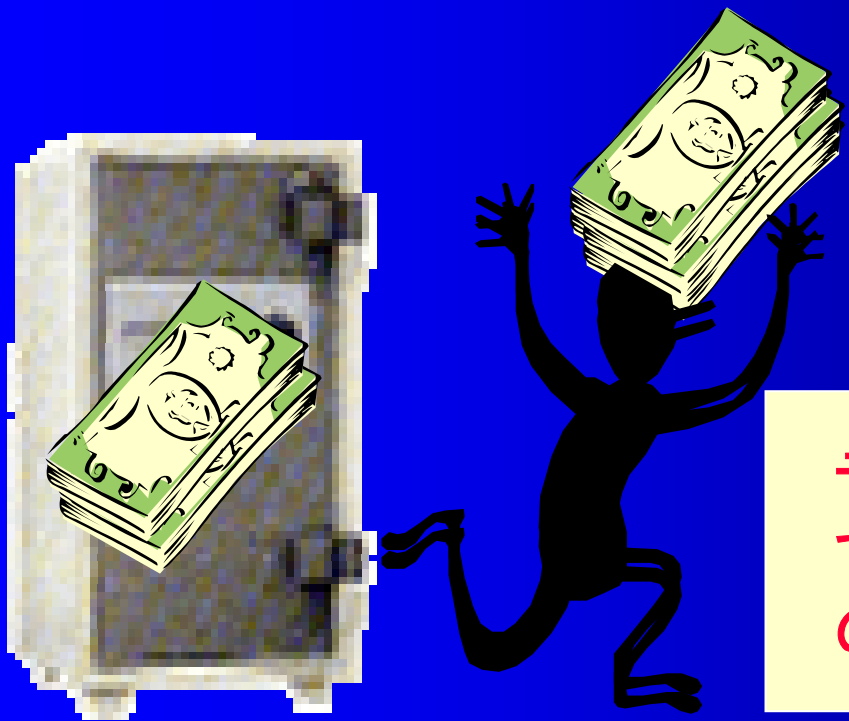
相次ぐ個人情報漏洩事件

（2004年5月13日経ビジネスより）

社名	公表時期	規模
ローソン	2003年6月	56万件
アプラス	8月	7万9000件
ファミリーマート	10月	18万件
NTTデータ	12月	4312件
東武鉄道	12月	13万件
三洋信販	2004年1月	120万件
ソフトバンクBB	1月	445万件
ジャパネットたかた	3月	66万件
サントリー	3月	7万5000件
アッカ・ネットワークス	3月	最大110万件
コスモ石油	4月	最大220万件
日本信販	4月	最大10万件

学生情報の漏洩
教職員情報の漏洩

やっかいなのは、漏れた事に気づかない



お金や物は持ち去られると
物理的に見て分かる

データはコピーして持ち去られ
ても、サーバから消えていない
ので気づかない

1．情報漏洩事件の原因

- 組織全体の無知・認識不足
- 教職員（学生も）の無知・認識不足
- 取扱い不注意・過失
- 検査体制（外注業者監督）のずさん
- 日常の情報管理不十分
- システム会社への丸投げ
- ウイルス対策不十分
- HP、掲示板への対策不十分
- 内部犯罪の対策不十分
- 経営トップの認識不十分

2. 情報漏洩事件の内容（一例）

- 組織全体の無知・認識不足
  予備校へ合格者名を本人の承諾なしに提供する
- 教職員の無知・認識不足
  電子メール誤配信（BCC→CC）
- 取扱い不注意・過失
  顧客情報の入ったノートPCの置き忘れ、盗難
- 検査体制のずさん
  記録媒体の受け渡し中の紛失、監査不実行

2. 情報漏洩事件の内容（続き）

- 日常の情報管理不十分
  パスワードの公然性、使いまわし、不正アクセス誘発
- システム会社への丸投げ
  ネット上で個人情報の丸見え、閲覧可能な設計
- ウイルス対策不十分
  感染したPCからファイルの一部からメールに添付され個人情報が流出

2. 情報漏洩事件の内容（続き）

- HP、掲示板への対策不十分
  - 卒業生の個人情報をHPに掲載
- 内部犯罪の対策不十分
  - 社外への持ち出しから情報流失、脅迫
- 経営トップの認識不十分
  - 事件として露出しない情報漏洩（多数）

個人情報とは（定義）

★個人情報保護法での定義（第2条第1項）
「生存する個人に関する情報であって、特定の個人を識別することができるもの」

◆（広義）個人の属性に関する情報のすべて
（公知・非公知、記名・無記名、事実・評価、財産的価値の有無、センシティブか否か、など関係ない）

◆（狭義）プライバシー（みだりに公にされたくない私的な事項）に関わる情報

個人情報の種類

◆基本情報

住所、氏名、年齢、連絡先などの個人属性情報など（基本4情報）

◆センシティブ情報　[sensitive―]

取り扱いに特に注意を要する情報．個人の思想や信条，国家の機密のような，ひとつ扱いを間違えると大きな問題が生じかねない情報

（１）個人信用情報（金融・資産関連など）、身体特性、学歴、趣味・嗜好、結婚歴など（やや人に知られたくない情報）

（２）人種および民族、門地および本籍地（所在都道府県に関する情報を除く）、思想、宗教、信条、政治的見解、犯罪歴、保健医療（個人健康情報）、労働組合への加入、ならびに性生活など（人に知られたくない情報）

個人情報漏洩のリーガルリスク①

民事責任

■被害者からの損害賠償請求
（債務不履行、不法行為）
（１人あたり１万円の損害賠償）
※最低額（最高裁判例に準拠）

※委託先や行為者への責任追及（被害者として）

個人情報漏洩による法的責任

損害賠償責任について

①漏洩による具体的な被害がなくても、漏洩させた事実のみで慰謝料が発生する

宇治市の事件では、「（自分のデータを）不特定の者にいつ購入されていかなる目的でそれが利用されるかわからないという不安感」についてプライバシー侵害を認定し、1人あたり1万円の慰謝料

②教職員、委託先の行為による漏洩についても、自社が被害者に対して直接責任を負う（使用者責任）

守秘義務契約があっても、被害者との関係では企業の免責にはならない

個人情報漏洩のリーガルリスク②

刑事責任

- 窃盗罪（情報に付随したハードウエアで犯罪構成）
- 情報窃盗（刑法改正の方向）
- 不正競争防止法違反（刑罰が重くなる方向）
  ※コンタミネーション

個人情報漏洩のリーガルリスク③

行政責任

■監督官庁による業務改善命令、許認可の取消・更新不可

■個人情報保護法による主務大臣の勧告、命令

◆（命令に違反したとき）6月以下の懲役又は30万円以下の罰金（第56条）

◆法人と行為者個人（代表者や従業員）の両罰規定

リーガル以外のリスク（USR／SR）

①ブランドイメージダウン（社会的信用喪失）
②在校生やその父兄に信頼喪失
③志望者減少
④経営幹部の辞任、懲戒、報酬減額
⑤事故発生後の対処
⑥データベース再構築のため時間ロスと
　新たな費用発生
⑦教職員のモチベーション低下

個人情報保護法の定義

◎定義（第2条）

◆個人情報とは・・・

生存する個人に関する情報で、特定の個人を識別できるもの

◆個人情報データベース等とは・・・

個人情報を含む情報の集合物であって、検索できるように体系的に構成したもの（コンピュータ処理情報＋マニュアル処理情報）

◆個人情報取扱事業者とは・・・

個人情報データベース等を事業の用に供している者

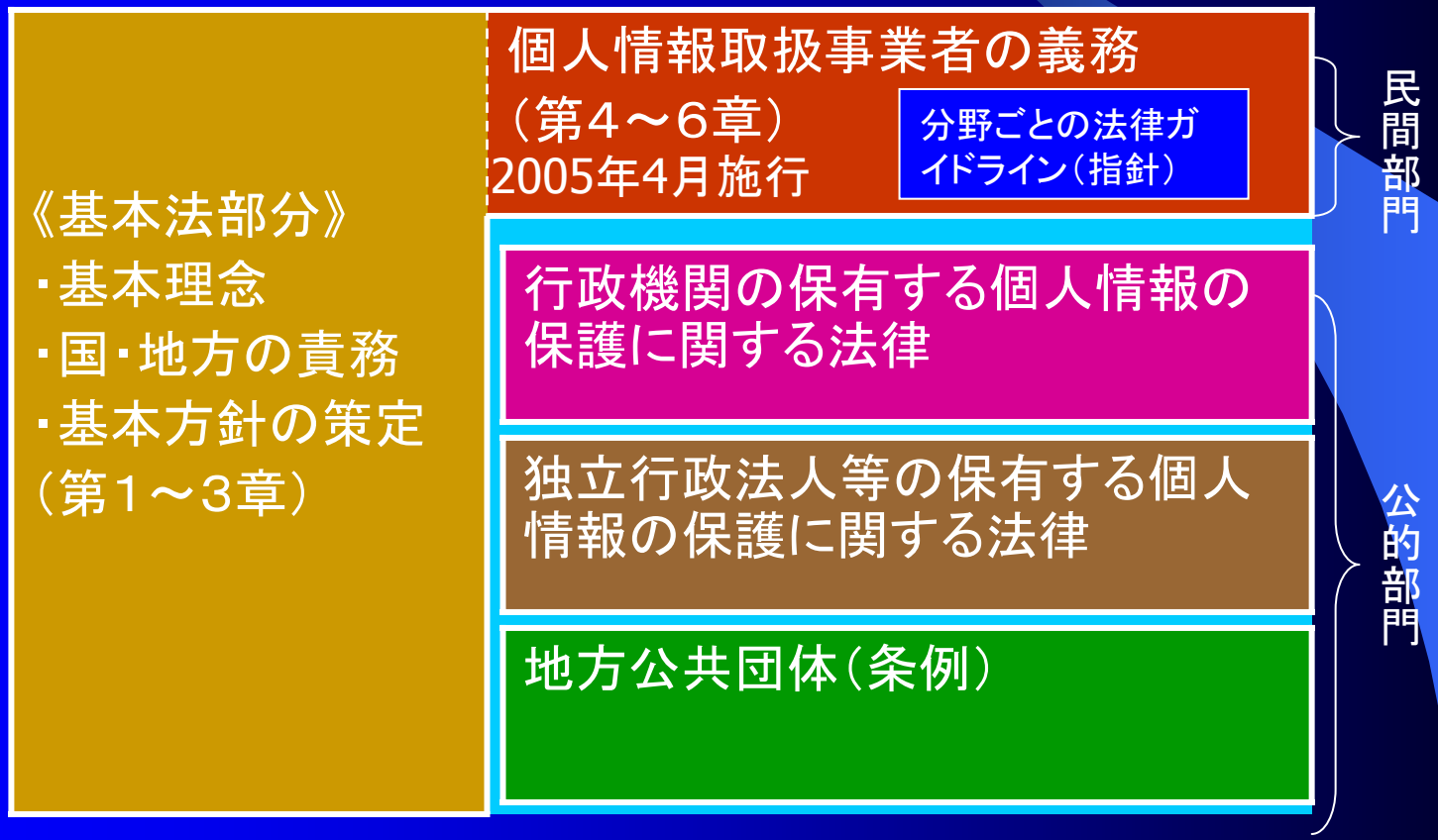
（適用除外）

・過去6カ月以内のいずれの日においても5000人分を超えない者

個人情報保護法の法制

個人情報の保護に関する法律

（総務省サイト資料）



学校法人としてやるべきこと（基本）

「個人情報の保護に関する基本方針」

（平成16年4月2日閣議決定）

個人情報取扱事業者が講ずべき措置

①事業者が行う措置の対外的明確化

事業者の個人情報保護方針（いわゆるプライバシーポリシー、プライバシーステートメント）の策定・公表

個人情報漏えい事案の発生時には、事実関係等を公表

②責任体制の確保

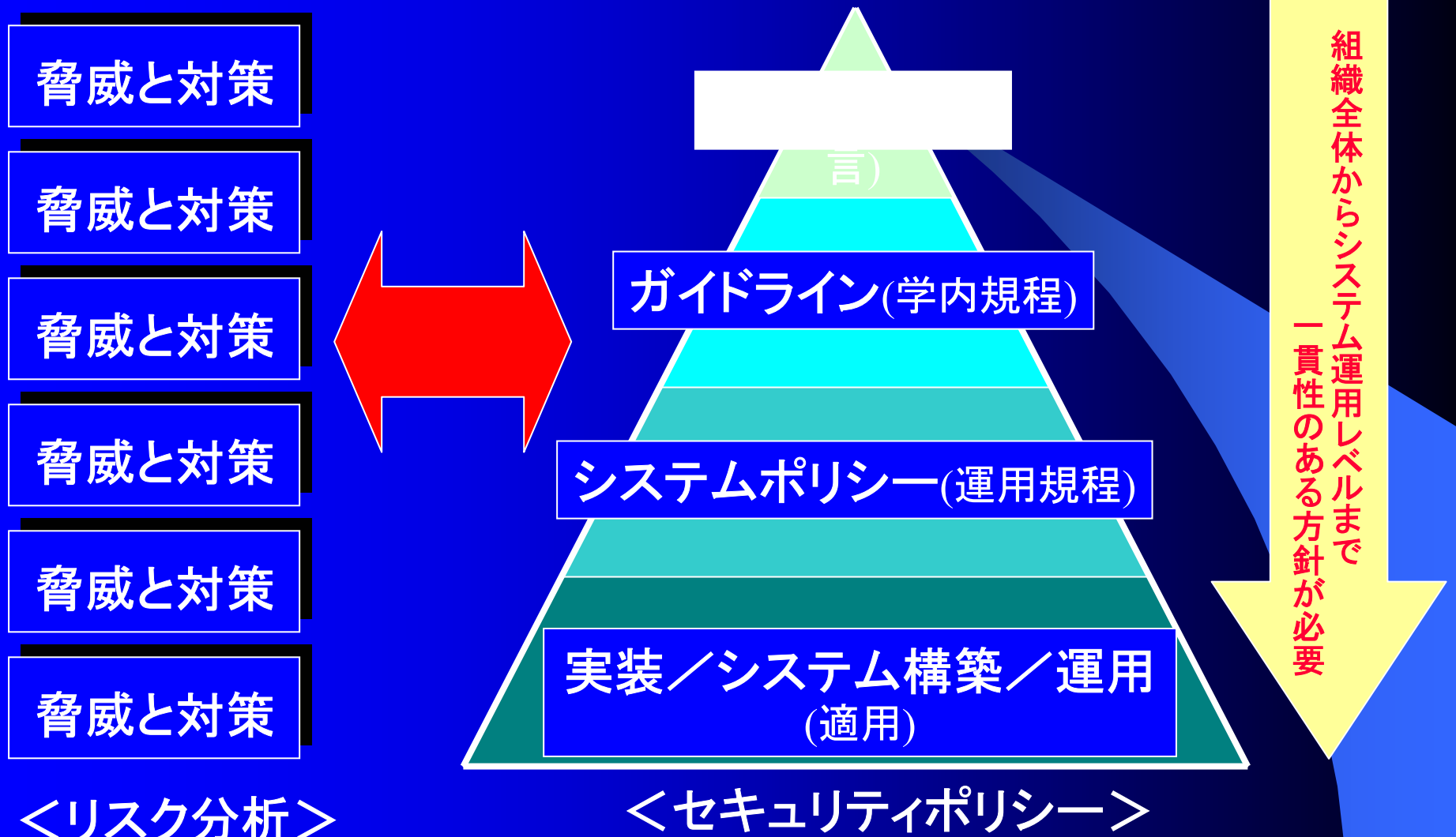
外部からの不正アクセスの防御対策、個人情報保護管理者の設置、内部関係者のアクセス管理や持ち出し防止策等、個人情報の安全管理について、社内の責任体制を整備

③従業者の啓発

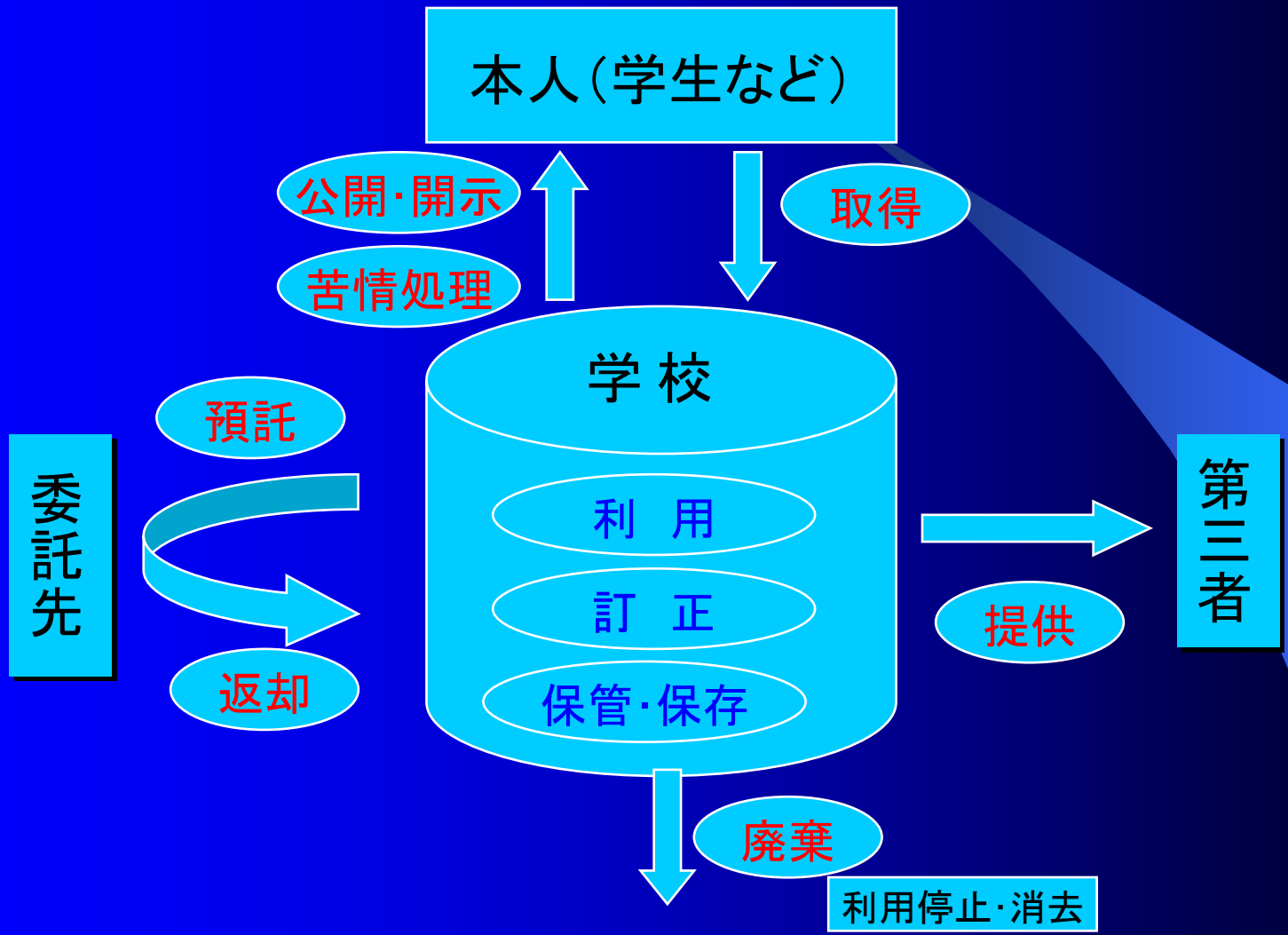
教育研修の実施等により、現場の従業者の啓発、個人情報保護意識を徹底

セキュリティポリシーの位置付け（参考）

リスク分析とセキュリティポリシーの関係



学校法人における個人情報保護の体系



■事例（Q＆A）

Q1．卒業生の在職者調査について

　3･4年生の就職活動に役立てるために、企業宛に卒業生の在職者を調査する目的で在職名簿の一覧を送付しておりますが、これは保護法に抵触しますか？
　また、企業からこの一覧表を加除していただき返送していただいております。返送する企業も保護法に抵触しますか。？

■事例（Q＆A）

Q2．求人企業宛に送付する大学案内を作成しておりますが、ここに学生の顔写真、学部・学科、氏名、就職内定先などを掲載しておりますが、保護法に抵触しますでしょうか。？
　勿論学生には掲載することの同意を取り付けております。

■事例（Q＆A）

Q3．教職員組合の代表を選出する際、非常勤、アルバイト研究員まで含めて選挙を実施し、その過半数をもって正式な地位を得るとなっております。

　そこで、組合から旧職員の個人情報を求められた場合、データを学校として渡していいでしょうか？

　組合は元来データを持っておりません。

■事例（Q＆A）

Q4．大学生協は学生の住居（下宿先）の紹介・斡旋を行っています。
　過去、大学生協から学生の個人情報を求められた場合、出してきました。
　今後どのような手順を踏む必要があるのか、それともないのか、どうすればよいでしょうか？

■事例（Q＆A）

Q5．卒業生のデータ管理は校友会で行っております。

　校友会は大学の組織に位置づけられており、学生課が所有している学生データを移管する形でデータを受け渡しています。

　これとは別に卒業生の会があり、これは任意団体で卒業生のOBが中心になって運営されています。もちろん学外組織であり、学生のデータは持っていませんので、卒業生のデータを求められます。求めがあれば出すことをどう考えればいいでしょうか？

■事例（Q＆A）

Q6．5の場合と同様、在学生の父母の会があります。
　こちらも学外組織であり、父母によって独立して会計があり、運営されています。
　学生課に対してデータをもとめられた場合、どのように対応を考えればよいのでしょうか？

■事例（Q＆A）

Q7．旧国立大学、公立大学、私立大学でそれぞれ監督官庁はどこになりますか？

行政指導はどこが行うのですか？

文部科学省は個人情報保護法に関して、問題が生じた場合、どのような関わりが生じますか？

■本日の講師
■田淵義朗（ＮＩＳ会長・オープンラーニング㈱専務取締役・東洋学園大学）
■連絡先　　tabu@gincorp.co.jp

ＮＩＳ（ネット情報セキュリティ研究会）

http://www.e-secure.jp

■会員数　　正会員（１８０名）準会員（５５０名）

■研究内容

ネット社会に流布する情報に対して、組織のリスク管理者の取るべき態度とその処方箋の研究。内容は、ネットクレームやブログ・掲示板での誹謗･中傷、ネット告発、情報漏洩など、起こる原因とリスクの認識および発見した場合の対策について、具体的な相談事例を通して検証する。