情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

人・組織・情報の関係から考える情報セキュリティ

日本オラクル株式会社
テクノロジー製品事業統括本部
担当ディレクター

情報セキュリティ大学院大学
セキュアシステム研究所　客員研究員
北野晴人 ,CISSP,JGISP

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

自己紹介

北野晴人（きたの　はると） 1964年東京生まれ

- 2種通信事業者、外資系通信機器ベンダーなどを経て、2001年日本オラクル入社。データベース、アイデンティティ管理を中心にオラクル製品のセキュリティと販売戦略・ビジネス開発などを担当中
- 情報セキュリティ大学院大学博士前期課程修了（情報学）・2010年からセキュアシステム研究所客員研究員
- CISSP、JGISP　アジアパシフィック・アドバイザリーボートメンバー
- 著書
  - 2004年「ひとごとではないデータベース情報の漏洩防止」（技術評論社）
  - 2009年「Oracle Database 11gセキュリティガイド」（共著・アスキー）
  - その他雑誌・Web記事など
- セキュリティを仕事にしたきっかけはL3スイッチの「認証VLAN」でした

はじめに（本日頂いていたテーマ）

2010年は特に政府機関などでも
内部関係者による情報漏洩が問題に
なった。もちろん企業でもあいかわらず
事故は多い。
日本と海外とで情報管理のやりかたや
実情はどれくらい違うのだろうか？外資
系に勤めている人ならよく知っているの
ではないか？
・・・そんなわけで基調講演ヨロシク！

じ、自信ない
けど頑張って
みます・・・

そんなわけで考えてみました・・・
（本講演の内容は所属組織等の見解を表すものではありません。）

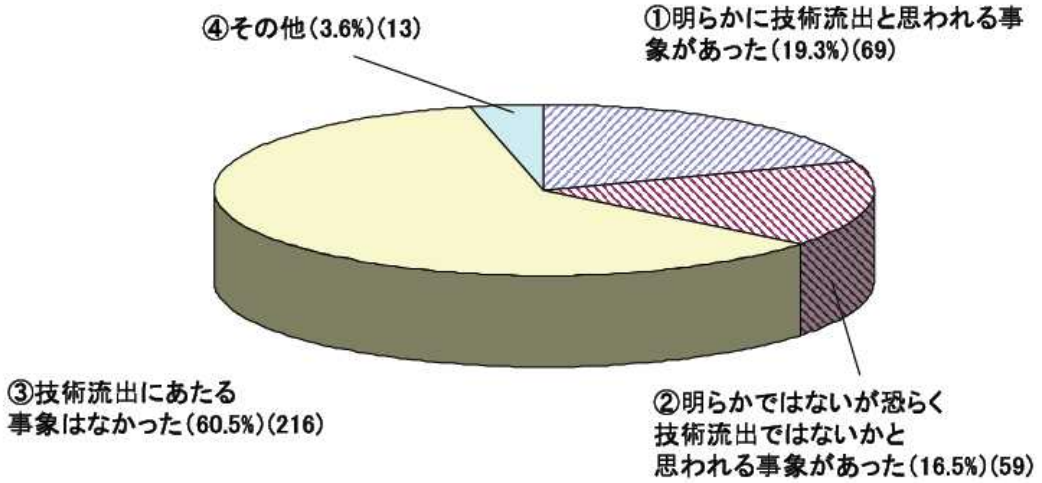
日本と欧米、そんなに差がある？

日本でも米国でも起きた内部からの情報流出

- 日本でも米国でも「最も機密保護が厳格に行われている」と思われる政府機関から情報流出が起きている。
- 米軍や米政府の情報セキュリティは最高のレベルではなかったのか？
- 日本でも米国・欧州でも同じように自動車メーカーの機密情報が盗まれた。
- 製造業における知的財産保護は米国のほうがずっと先進しているのではなかったのか？

働く人の意識に日米で差はあるか？

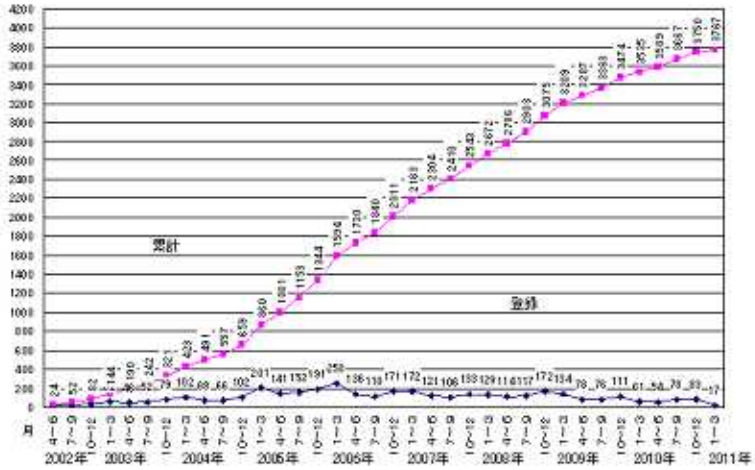
- 日本でも海外でも、調査をすると「転職時、解雇時には会社の機密情報を持ち出す」または「持ち出した」と回答する人が相当数存在する。
  - 米国：シマンテックの調査（2008年）
  - 日本：トレンドマイクロの調査（2009年）
- 実際に日本でも米国でも、製造業の知的財産流出については「退職者が持ち出した」ケースが発生している。



出典：平成19年経済産業省「我が国における技術流出及び管理の実態について」

個人的な実感値としてはどうだろうか？

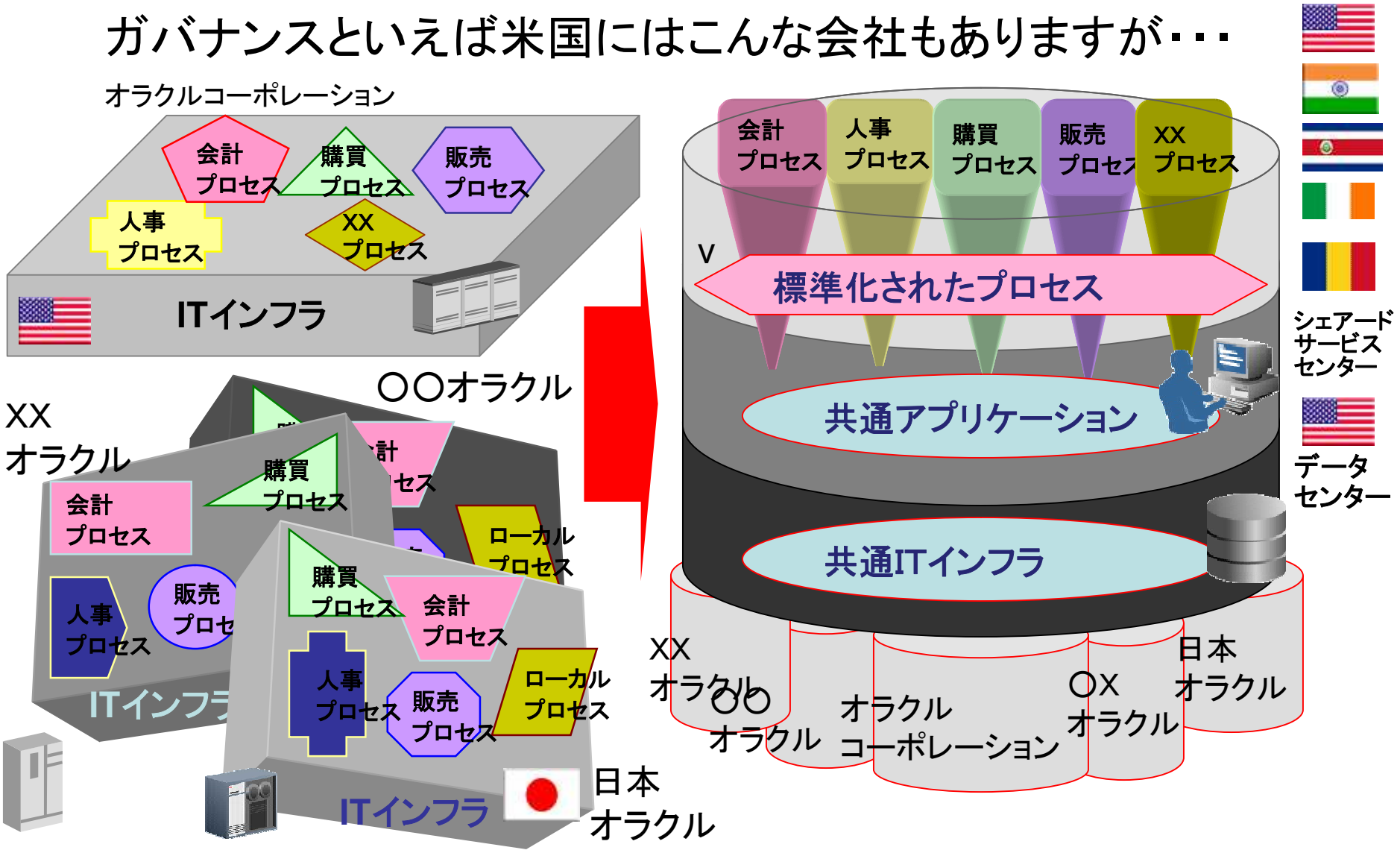
- 日本企業の情報セキュリティ・ポリシーと技術的対策はとても厳格になってきている。
  - 持ち出しPCの制限、暗号化
  - USBメモリの禁止、暗号化
  - 作業場所への入退室、監視カメラ・・・
  - Webは「ほとんどのサイトが閲覧不能」（？）
  - むしろISMS認証取得組織数では日本はダントツ世界一である。（2011年2月18日現在3767）
- 外資系社員としての実感値は・・・
  - 差があるとすれば「トップダウンのガバナンス」



ISMS認証取得組織数推移
（出典：JIPDEC　http://www.isms.jipdec.jp/lst/ind/suii.html　）

実は情報管理の実態も、内部不正による事件・事故の発生も、日本と欧米で大きな差はないように見える。
あえて差があるとすれば「トップダウンのガバナンス」であるが、これは情報セキュリティの分野に限ったことではない。

ガバナンスといえば米国にはこんな会社もありますが・・・



Global Single Instance（GSI：グローバルシングルインスタンス）

なぜ「大きな差がある」ような気がするのか？

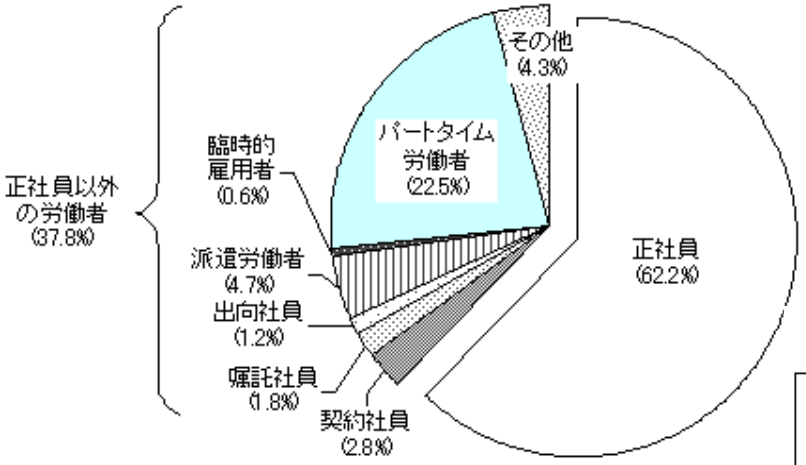
- 「米国は企業も政府機関も“性悪説”を前提として厳格にセキュリティ対策を行っている。それに比べて日本はまだ立ち後れている」という**“イメージ”**があるのはなぜか？
  - 欧米式の優れたところだけが輸入されているが、必ずしも全てが優れているわけではない。
  - セキュリティ・ポリシーには少し差があるが、大きな差はなさそう。
  - 技術的対策もさほど劣ってはいない。技術力の差ではなく普及方法。
- 差があるとすれば、それは**「人と組織の関係」**ではないだろうか？
  - なぜならガバナンスは最終的に「人」を統治するものだから。
  - それぞれの国が持つ文化的・歴史的背景が関わってくるから。

「人と組織の関係」に着目して、
内部不正の発生要因を考えてみる

人と組織の関係の変化

「人と組織の関係」の変化 ①

- 既に民間企業の就業者の約1/3は社員ではなく、転職希望が増加傾向
- 従業者の組織に対する帰属意識の変化（会社が潰れても「他人事」）



厚労省：
平成19年就業形態の多様化に関する総合実態調査結果の概況

表１　転職希望者数及び割合（雇用者：15～34歳）－平成19年

（千人，%）

現職の就業形態	希望する仕事の就業形態	総数	うち転職希望者		正規就業を希望		非正規就業を希望	
		実数	実数	割合	実数	転職希望者を100とする構成比※	実数	転職希望者を100とする構成比※
男	正規就業者	7,902	1,224	15.5	1,022	83.5	67	5.5
	非正規就業者	2,377	790	33.2	561	71.0	162	20.6
女	正規就業者	4,474	753	16.8	576	76.6	140	18.5
	非正規就業者	3,892	967	24.8	589	61.0	336	34.7

※ 転職希望者総数と希望する仕事の就業形態の内訳の合計とは，総数に「自営業を希望」，「不詳」等を含むことから一致しない。

厚労省：「平成19年就業構造基本調査」による転職希望者数及び割合

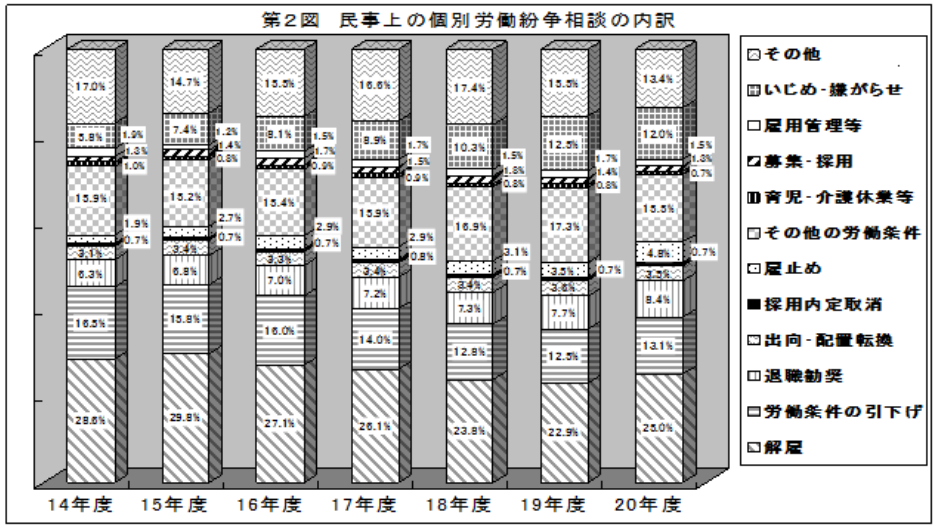
「人と組織の関係」の変化　②

- 「うつ」などストレスに起因する変化（50%を越えるメンタルヘルスの増加）
- 職場におけるいじめの増加（6年間で2倍以上）

—%—

区　分		全産業 規模計	全産業 1,000人以上	全産業 300～999人	全産業 300人未満	製造業	非製造業
合　計		248社	89社	82社	77社	117社	131社
		100.0	100.0	100.0	100.0	100.0	100.0
増加している		**55.2**	**70.8**	**59.8**	**32.5**	**53.8**	**56.5**
横ばい		24.6	24.7	22.0	27.3	29.9	19.8
減少している		2.8		2.4	6.5	3.4	2.3
その他		3.2	1.1		9.1	1.7	4.6
分からない		14.1	3.4	15.9	24.7	11.1	16.8
「増加している」場合，特に増加が目立つ年代層（複数回答）	小　計	131社	60社	48社	23社	59社	72社
		100.0	100.0	100.0	100.0	100.0	100.0
	20代	41.2	38.3	45.8	39.1	30.5	**50.0**
	30代	**51.9**	**53.3**	**47.9**	**56.5**	**59.3**	45.8
	40代	19.1	21.7	12.5	26.1	32.2	8.3
	50代	0.8	1.7				1.4
	年代に関係なく増加	25.2	23.3	35.4	8.7	27.1	23.6

2008年　財団法人 労務行政研究所「「企業におけるメンタルヘルスの実態と対策」



厚生労働省「平成20年度個別労働紛争解決制度施行状況」

「人と組織の関係」における日本的経営の変化　①

- かつての「日本的経営」
  - 三種の神器は「終身雇用」「年功序列賃金」「労働組合」だった。
  - 終戦後～高度成長期の大きな目的は「生活保障」であった。
    - 福利厚生・社会保障の充実
  - 日本の企業は「共同体」であり、ある種のコミュニティであった。
  - 職場の非公式組織が社会統制機能を持っていた。
  - ずっと働き続けるからこそ組織は大事であり、不正を行うことは考えなかった。

コンピュータが発達しはじめた1980年代には、まだ日本的経営が大きな成功をおさめていた。そのため情報もコンピュータシステムも「みんなで共有、みんなで使う」ことを前提として構築され、運用されていた。

“コンピュータのパスワードはみんなが知ってないと、誰かが休んだ時に困るじゃないか”というのが普通の環境だった。

「人と組織の関係」における日本的経営の変化　②

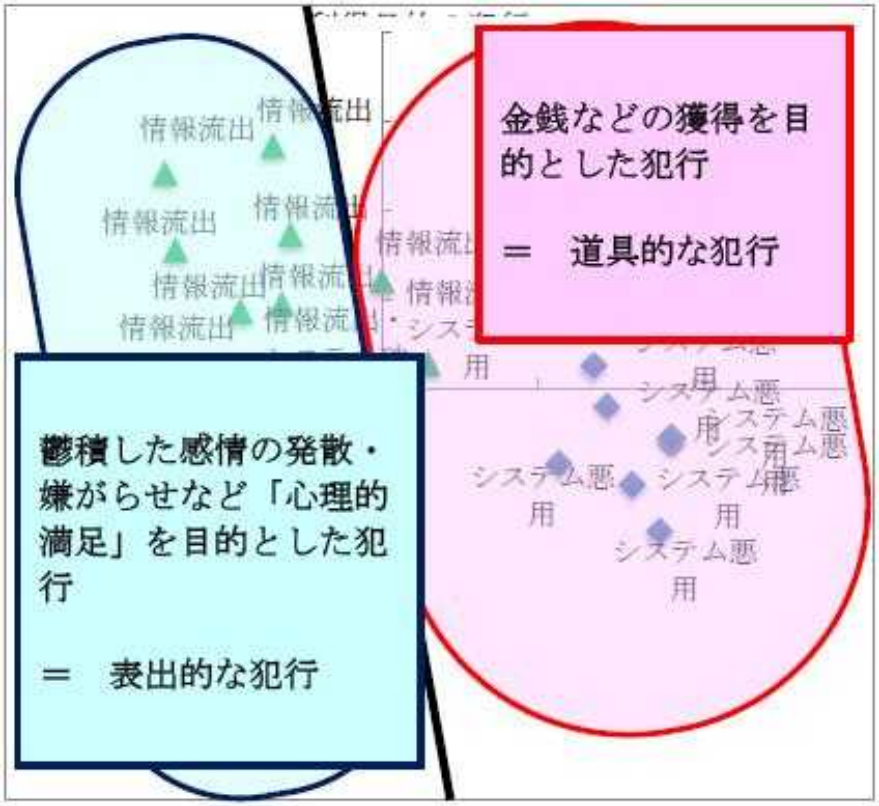
- グローバリゼーションという名の欧米化
  - 日本型経営には合議制、責任の不明確化、意思決定のスピードなどの課題があったため、迅速な意思決定と経営のスピード向上を求めた。
  - 企業が欧米型「機能体」としての組織に変化する。
  - 成果主義・目標管理制度による給与格差と「相対的剥奪」が生まれた。
  - 「職務記述書（Job Description）」と“It is NOT my job!”な世界
  - 雇用の流動・構造の変化を生み出し、人と組織の関係を希薄にした。

グローバリゼーションは必ずしも成功しているわけではない。しかし人と組織の関係は確実に変化し、それに伴って「情報にかかわるリスク」も欧米化した。特に今世紀に入ってからそれが加速している。

その一方で、ITやシステムの構築・運用の現場はこの変化の速度に追いついていないのではないか？（例：アクセスコントロールの難しさ）

人と組織の関係から生まれる内部不正の動機

内部不正の類型を考える



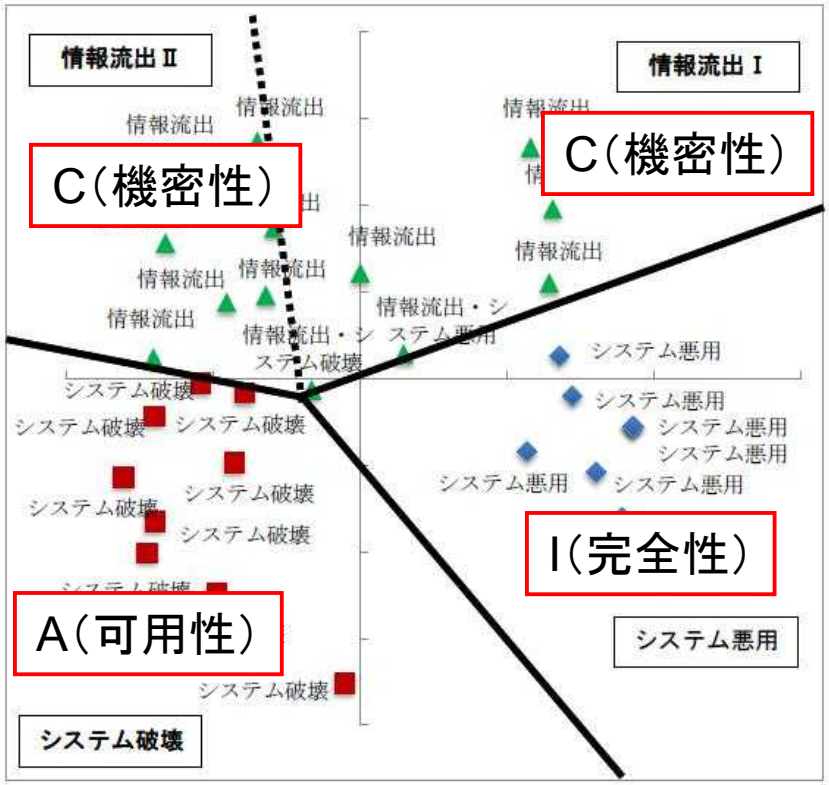
内部犯行者による情報セキュリティ事案の4分類

（出典：財団法人 社会安全研究財団 情報セキュリティにおける人的脅威対策に関する調査研究委員会(辻井重男,江口有隣,他)「情報セキュリティにおける人的脅威対策に関する調査研究報告書」

内部犯行者による情報セキュリティ事案 4分類の実際の事故事例

- システム破壊
  - 2008年7月　銀行
    元派遣社員によるネットワークへの不正侵入により、ファイルの削除が行われたことで社員向けホームページが停止された
- システム悪用
  - 2009年5月 出版社
    元社員による会社の銀行預金口座からキャッシュカードを利用して不正に現金を引き出していた
- 情報流出Ⅰ(道具的な犯行)
  - 2009年9月　証券会社
    金銭に困った社員が無断で情報を持ち出し、その個人情報を転売した
- 情報流出Ⅱ(表出的な犯行)
  - 2011年1月　中古パチンコ販売会社
    この会社社長が会長に対し恨みがあり、困らせてやりたくて営業秘密を不正に取得し、情報流出させた

内部不正の類型を考える



内部犯行者による情報セキュリティ事案の4分類

(出典:財団法人 社会安全研究財団 情報セキュリティにおける人的脅威対策に関する調査研究委員会(辻井重男,江口有隣,他)「情報セキュリティにおける人的脅威対策に関する調査研究報告書」

内部犯行者による情報セキュリティ事案 4分類の実際の事故事例

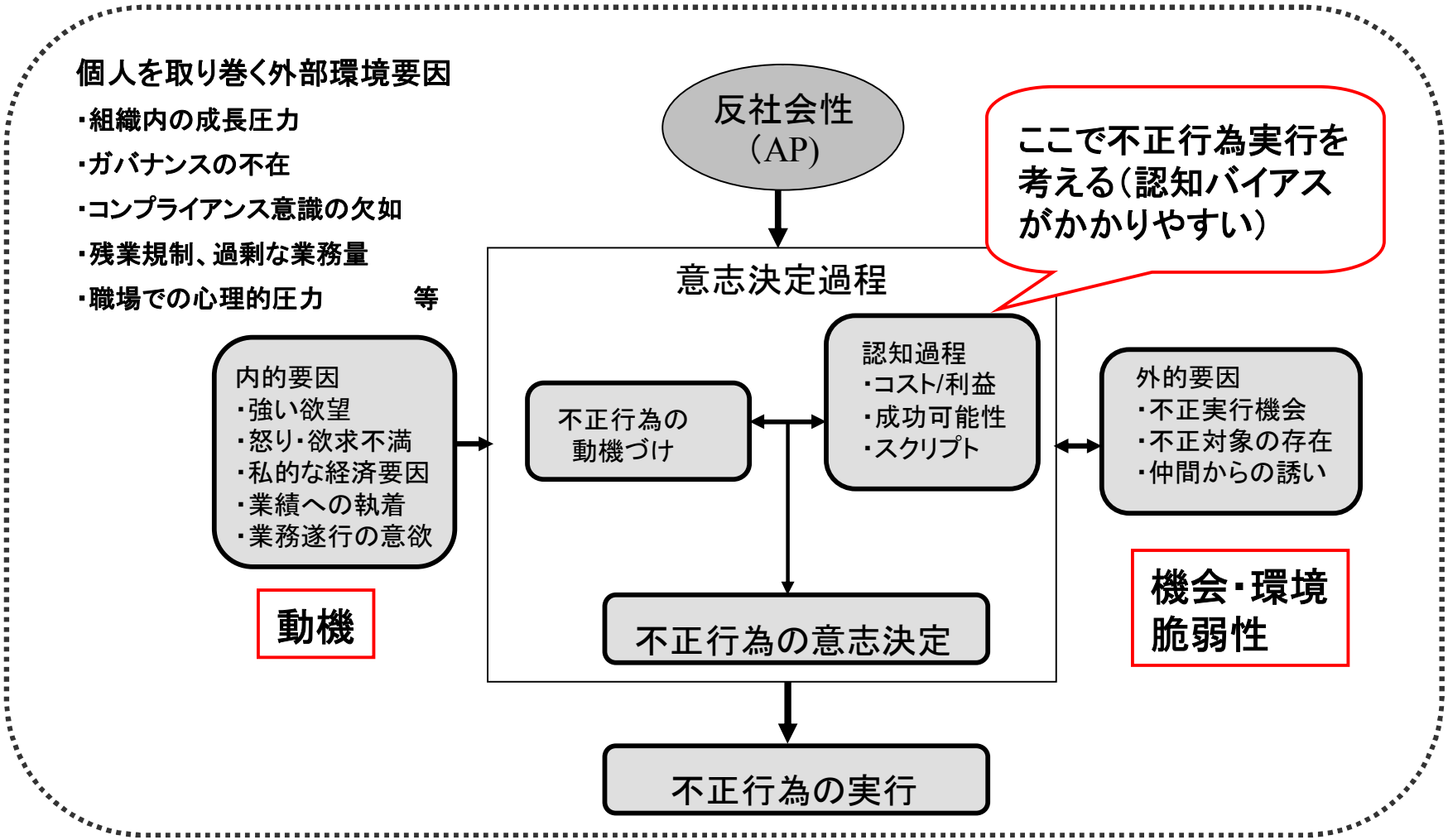
- システム破壊
  - 2008年7月　銀行
    元派遣社員によるネットワークへの不正侵入により、ファイルの削除が行われたことで社員向けホームページが停止された
- システム悪用
  - 2009年5月 出版社
    元社員による会社の銀行預金口座からキャッシュカードを利用して不正に現金を引き出していた
- 情報流出Ⅰ(道具的な犯行)
  - 2009年9月　証券会社
    金銭に困った社員が無断で情報を持ち出し、その個人情報を転売した
- 情報流出Ⅱ(表出的な犯行)
  - 2011年1月　中古パチンコ販売会社
    この会社社長が会長に対し恨みがあり、困らせてやりたくて営業秘密を不正に取得し、情報流出させた

性善説と性悪説（よくある話ですが・・・）

- 性善説（孟子）
  - 人間は善を行うべき道徳的本性を先天的に具有しており、悪の行為はその本性を汚損・隠蔽することから起こるとする説。正統的儒学の人間観。（Yahoo「大辞林 」）
  - 「人は本質として善だから、放っておいても悪事は行わないとする楽天主義」ではない。
- 性悪説（荀子）
  - 人間の本性を利己的欲望とみて、善の行為は後天的習得によってのみ可能とする説。孟子の性善説に対立。（Yahoo「大辞林 」）
  - 「人間の本性が悪だから、人間は悪事を行うのが当然である」という人間不信的な主義ではない。

つまりどちらの説をとっても「人は善行も悪行も行う可能性がある。だから一定のルールと教育（＝セキュリティ・ポリシーと従業員教育）が大事であると言っている。

どのように不正行為の意思決定を行うのか



ファーリントン「統合的認知的反社会的傾向（ICAP）理論」を情報セキュリティむけに修正

人と組織の関係から生まれる内部不正の動機　①

フレデリック・ハーズバーグの「動機付け－衛生理論」

1959年にハーズバーグとピッツバーグ心理学研究所が行った調査における分析結果から導き出された「動機付け－衛生理論」。約200人のエンジニアと経理担当事務員に対して、「仕事上どんなことによって幸福と感じ、また満足に感じたか」「どんなことによって不幸や不満を感じたか」という質問を行い、分析したもの。

- 満足を促すもの　⇒「動機付け要因」(motivator)
- 不満足を回避するもの ⇒「衛生要因」(hygiene factors)

主な衛生要因(不満足という回答を導いた要因・上から多い順):

- ·会社の方針と管理
- ·監督
- ·監督者との関係
- ·労働条件
- ·給与

これらは内部不正の動機を生み出す？

人と組織の関係から生まれる内部不正の動機　②

「情報セキュリティにおける人的脅威対策に関する調査研究報告書」の調査結果と
ハーズバーグの衛生要因との照合表

分類	システム悪用	システム破壊	情報流出 I （道具的）	情報流出 II （表出的）
職場への不満	上司の態度や経営への不満	納得のいかない解雇や評価への不満	納得のいかない業務や上司への不満	上司や会社、評価への不満
衛生要因	•会社の方針と管理 •監督者との関係	•会社の方針と管理 •労働条件 •給与	•会社の方針と管理 •監督者との関係 •給与	•会社の方針と管理 •監督者との関係 •労働条件 •給与
動機	金銭の困窮や職場環境への不満	解雇されたことや上司、会社等への不満	金銭の困窮や評価を得るため	上司や会社への恨み
衛生要因	•監督者との関係 •給与	•会社の方針と管理 •労働条件 •給与 •身分 •保障	•会社の方針と管理 •監督者との関係 •給与	•会社の方針と管理 •監督者との関係 •労働条件

照合した結果より、調査結果はハーズバーグの動機付け
ー衛生理論と符合する

人と組織の関係から生まれる内部不正の動機　③

従業員満足と情報セキュリティに関する内容について、Webアンケートを実施

（情報セキュリティ大学院大学・遠藤による調査・2011年1月実施）

アンケートの概要

- アンケート対象者：一般企業に勤めている人

役職	経営者	取締役	管理職	一般社員
人数	1	0	8	21

- 人数　：30人

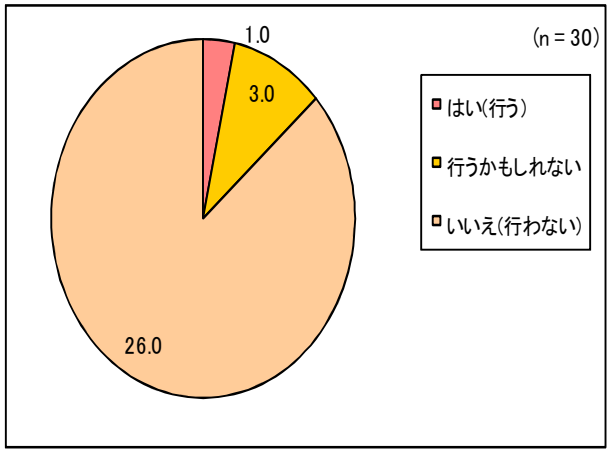
性別	男性	女性
人数	21	9

- 年代：20代～50代

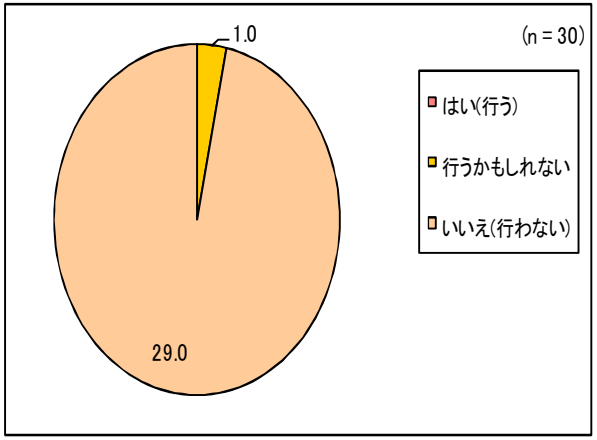
年代	10代	20代	30代	40代	50代	60代以上
人数	0	1	21	5	3	0

人と組織の関係から生まれる内部不正の動機　④

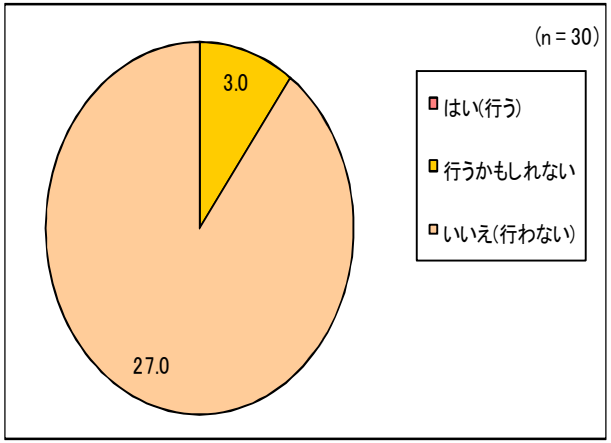
■ Q6-1.もしもあなたが職場で虐め(上司や同僚から)受けていたら、システムの悪用をして虐めた相手のメールを盗み見するかもしれない



■ Q6-2.もしもあなたが緊急にお金が必要となったら、情報を持ち出すかもしれない



■ Q6-3.もしもあなたが不当に解雇されたら、解雇された会社のシステムやホームページを攻撃するかもしれない



人と組織の関係から生まれる内部不正の動機　⑤

Q6を中心としたクロス集計の結果

質問番号	選んだ回答	「そう思わない」「ややそう思わない」を選んだ質問番号	対応する衛生要因の項目（不満を感じている項目）
Q6-1	はい(行う)	・Q1全て ・Q2(Q2-1除く) ・Q3(Q3-1,Q3-3除く) ・Q4全て	・会社の方針と管理 ・監督 ・給与 ・身分 ・保障 ・個人生活 ・労働条件 ・監督者との関係 ・同僚との関係 ・対人関係
	行うかもしれない	・Q1全て ・Q2(Q2-2除く) ・Q3(Q3-3,Q3-5除く) ・Q4(Q4-1,Q4-5除く)	・会社の方針と管理 ・監督 ・労働条件 ・監督者との関係 ・給与 ・保障

質問番号	選んだ回答	「そう思わない」「ややそう思わない」を選んだ質問番号	対応する衛生要因の項目（不満を感じている項目）
Q6-2	行うかもしれない	・Q1-4 ・Q2(Q2-1除く) ・Q3-2	・会社の方針と管理 ・労働条件 ・監督者との関係

質問番号	選んだ回答	「そう思わない」「ややそう思わない」を選んだ質問番号	対応する衛生要因の項目（不満を感じている項目）
Q6-3	行うかもしれない	・Q2-3,Q2-4 ・Q3-2	・労働条件 ・監督者との関係

現実には誰もがリスクを背負っている

- 結局のところ、誰でも不正を行う危険は潜在的に持っている。性善説でも性悪説でもなく、人がいればそこにはリスクがあると考えるべき。
- 職場、仕事に何らかの不満があると、セキュリティリスクは増大する。
- 職場に不満はなくても、企業側の努力でどうにもならない事情は起こる可能性はある。
  - 家族の事情で借金？
  - 恋愛模様でお酒？
- かつての日本的経営では企業が共同体・コミュニティとしても機能していたので、職場にある程度の心理的セーフネットがあった。日本企業が欧米型の機能体組織に変わろうとする中で、こういったものは失われつつあるのかも知れない。
- それに代わる新たなセーフネットが技術的対策であるはずだが、「人と組織の関係」が変化するスピードに追いつけていない。

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

人と組織の関係とこれからの情報セキュリティ

マグレガーのX理論・Y理論による経営の人間観

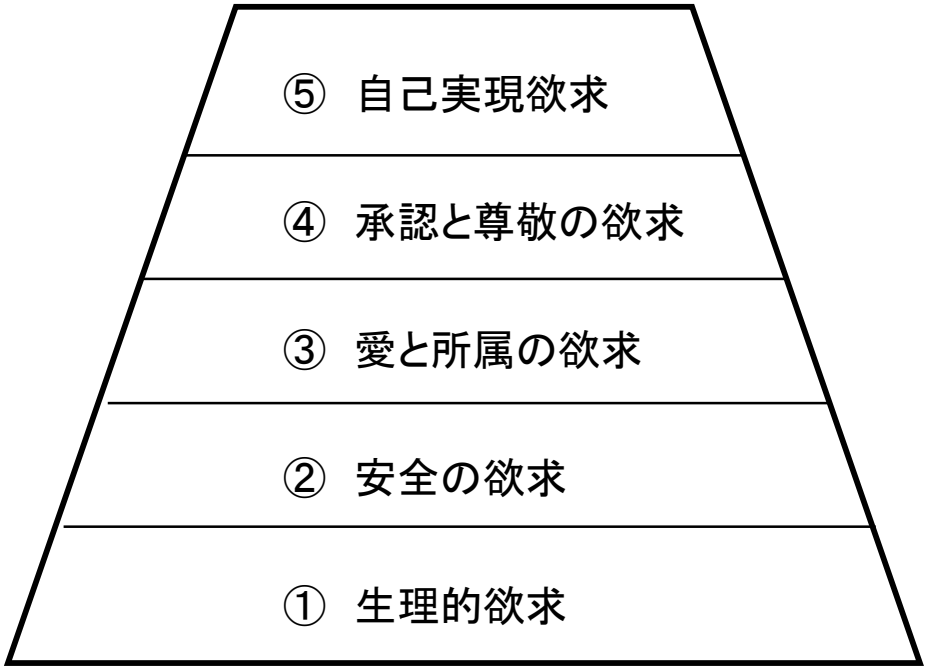
- X理論の前提
  - 人間は生来仕事がきらいで、なろうことなら仕事はしたくないと思っている。
  - 人間は強制されたり、統制されたり、命令されたり、処罰するぞとおどされたりしなければ、じゅうぶんな力を出さない。
  - 普通の人間は命令されるほうが好きで、責任を回避したがり、あまり野心をもたず、なによりもまず安全を望んでいる。
- Y理論の前提
  - 仕事で心身を使うのはごくあたりまえのことであり、遊びや休憩の場合と変わりはない。
  - 人は自分が進んで身を委ねた目標のためには自ら自分にムチ打って働くものである。
  - 献身的に目標達成につくすかどうかは、それを達成して得る報酬次第である。
  - 普通の人間は、条件次第では責任を引き受けるばかりか、自らすすんで責任をとろうとする。
  - 企業内の問題を解決しようと比較的高度の想像力を駆使し、手練をつくし、創意工夫をこらす能力は、たいていの人に備わっている。
  - 現代の企業においては、日常、従業員の知的能力はほんの一部だけしか生かされていない。

出典:「企業の人間的側面」(ダグラス・マグレガー)

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

人間の欲求とモチベーションを考える

・ マズローの5段階欲求説（ある欲求が満たされると次の段階の欲求が生まれる）



情報セキュリティマネジメントをより高品質に向上させることに有効な高次欲求と社会的インセンティブ
・経営への参画を実感できる
・自らの創造性を活かした仕事

情報セキュリティリスクを低減するために有効な欲求とインセンティブ
・上司との関係
・職場の人間関係
・給料
・労働環境
・生命・身体の安全

・ より前向きに情報セキュリティに取り組むモチベーションを引き出すためには、業務に対するモチベーションを高めることが必要。経営者は④～⑤の欲求を満足させるためのインセンティブと施策を考える必要がある。

[提案] コンピテンシーによる人事評価

- 「高い業績をコンスタントに示している人の行動の仕方などに見られる行動特性」のこと
  - 1970年代にハーバード大の教授であったマクレランドが、「学歴や知能レベルが同等の外交官が、開発途上国駐在期間に業績格差がつくのはなぜか？」という依頼を受け、調査・研究を行った結果「学歴や知能は業績の高さとさほど相関はなく、高業績者には幾つかの共通の行動特性がある」ことが判明したことから、米国を中心として人事評価のための手法として利用されている。
  - 日本でも導入が進んでいる。これを使って情報セキュリティを人事評価に取り込めないだろうか？

(%)

制度の有無等 / 企業規模	制度がある	人事考課の手法					制度がない	不明
		目標管理	コンピテンシー	情意	その他	不明		
規模計	81.7	(79.0)	(19.6)	(34.3)	(9.1)	(1.2)	17.9	0.4
1,000人以上	95.7	(90.1)	(30.1)	(32.3)	(9.2)	(0.2)	4.1	0.3
500人以上1,000人未満	90.2	(82.7)	(23.3)	(32.9)	(12.3)	(0.5)	8.7	1.1
500人未満	79.3	(77.2)	(17.9)	(34.8)	(8.6)	(1.4)	20.4	0.3

複数回答

(注) ( ) 内は、制度がある企業を１００とした割合。

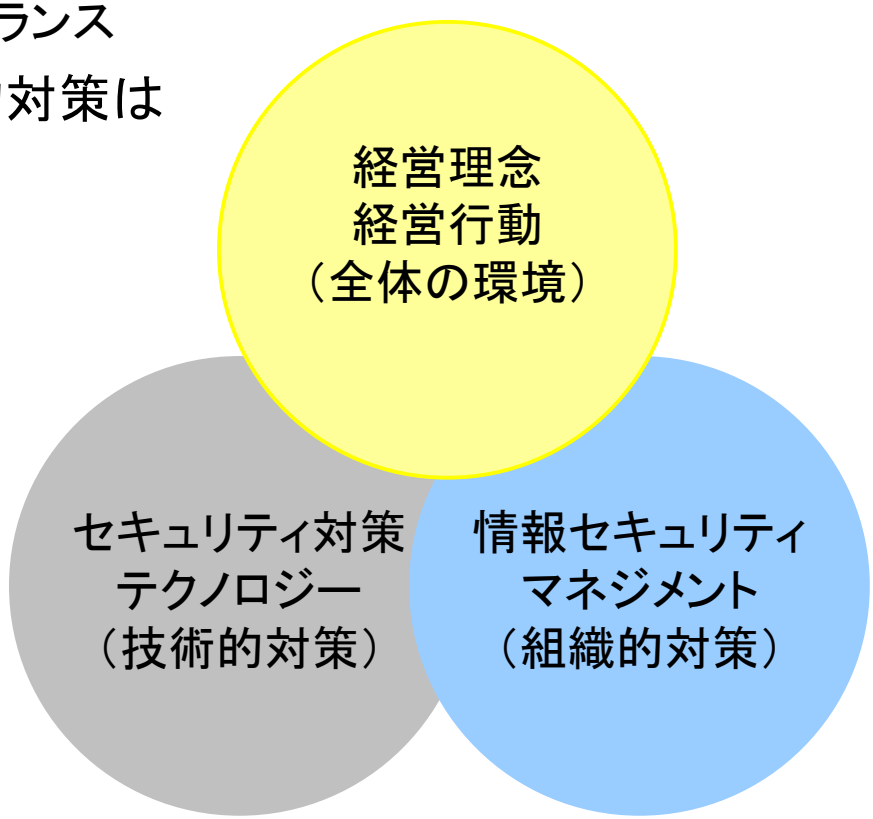
国内企業における目標管理とコンピテンシーの導入状況

[提案] コンピテンシーによる評価のイメージ試作

行動指標	評価		
	自己	上司	総合
· 作成したドキュメントには全てルールに基づいた機密性ラベル（社外秘・部外秘等）をつける。			
· ドキュメント類を社外に送付・開示する際は社外秘情報が含まれていないか確実に最終チェックを行っておく。			
· 社外または他の部署、部門等から入手した情報を自分が社外（情報の提供元とは異なる社外）に送付・開示する際、機密性の度合いが不明な時は必ず情報の入手元に確認を行う。			
· 機密保持契約等にもとづいて機密情報を社外に送付する場合はメールの誤送信防止、暗号やパスワードの利用などを行い慎重に行う。			
· 社内で機密情報を保管する場合は「だれにアクセス権が必要か」を常に考えて適切なアクセスコントロールを行う。			
· 個人情報を取り扱う場合は、当該情報主体に許可を受けていない第三者提供や目的外利用を行わないように留意する。			
· 決められたセキュリティ・ポリシーがある場合はそれを遵守し、不都合や問題がある場合にはセキュリティ部門、システム部門、法務部門等適切な部門と確認・調整を行ったうえで対処する。			

経営と情報セキュリティ

- 近年日本企業は欧米型の機能体組織に変わりつつあるが、何でも米国型にすれば良いわけではない。
- 日本の文化・歴史的背景をふまえたある種のカスタマイズが必要。
  - X理論/Y理論の和風組み合わせバランス
- 最後のセーフティネットとして技術的対策は確実に実装しておく必要がある。



おわりに（経営者の方へのお願い）

- 経営戦略、人事施策などの基本的な経営行動による従業者のモチベーションは生産性や業績に影響するだけではなく、情報セキュリティ関連リスクにも影響を及ぼすことを明確に理解して頂きたい。
- 良くないのは「性善説でやっていました」という言葉が「対策を怠っていました」という意味の言い訳に使われることである。性善説でも性悪説でもなく、人はあやまちをおかすものなので、ルールと教育、技術的対策への投資は不可欠と考えて頂きたい。
- 技術的対策への投資は会社を守るためだけではなく、社員一人一人を守るためのセーフネットであると理解して頂きたい。
- 情報保護のために努力する従業者が適正に評価され、相応のインセンティブを得られるしくみを構築するべきである。これによってゼロかマイナスの情報セキュリティではなく、価値を作り出すプラスの情報セキュリティを実現して頂きたい。

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

ご静聴ありがとうございました。

Mail:haruhito.kitano@iisec.ac.jp
Twitter:@HarutoJ