情報システム運用管理哲学再考――「コンピュータの人支配」の視点から

(2) セキュリティ主義，法令遵守主義，ネットワーク支配

A Review of the Philosophy of Information System Management/Administration from the Viewpoint of '*Computer-Dominated Organization*'

(2) Security-ism, Compliance-ism and Center-dominated Network

宮下英明
北海道教育大学岩見沢校
Hideaki Miyashita
Hokkaido University of Education, Iwamizawa Campus

要旨

「セキュリティ」を担当すると，セキュリティ一辺倒になり，セキュリティと他とのトレードオフを考えなくなる――セキュリティ主義の本末転倒。セキュリティ主義は，「無菌」パラダイムに立つ。「無菌」は無理なスタンスであり，この無理を通そうとすることで管理主義の本末転倒に進む。「無菌」パラダイムは「健康」パラダイムへシフトされねばならない。

セキュリティ主義と同様なものに，法令遵守主義がある。「法令遵守（コンプライアンス）」を担当すると，「法令遵守」を程度問題で考えず，「法令遵守」に生活を従わせるという本末転倒をやる。

「コンピュータの人支配」は，人の心的傾向性がつくってしまうものであり，そこにはむしろ各種「善意」が見える。 そしてこのようなものとして，「大学執行部のネットワーク支配――言論・情報の統制」が主題化されることになる。この場合の「善意」は，「前衛主義・中央指導」のエリート主義の善意（独善）である。

Abstract : When one takes charge of 'secury'-management, s/he tends to be totally committed to 'security', rarely think of the trade-off between securty and the others, and do such things as 'putting the cart before the horse'. It is the 'security-ism'. Security-ism stands on the paradigm of 'germ-free'. This paradigm is impossible, and therefore it leads people to 'put the cart before the horse'. It must be switched to the paradigm of 'health'.

We should recognize the compliance-ism as the same kind of security-ism. It means the excessive reaction to rules, that is, 'putting the life before the rule'.

'Computer-dominated' results from human disposition. And there we rather recognize 'goodwill'. And, in this sense, 'domination of network by organization executives' becomes a related subject to be considered. The 'goodwill' in this case is the self-righteousness of the elitism, which is avant-gardism/centralism.

Key words : Security, Compliance, Center-dominated

はじめに

本論校の (1) では，情報システム運用管理に関係する「コンピュータの人支配」の構造を，国立大学の方法論・哲学と照らしつつ，論じた。この (2) では，情報システム運用管理の本末転倒を導いている要因の大きなものとして，「セキュリティ主義と法令遵守主義を特に論ずる。また，「ネットワーク支配」を主題化し考察する。

5 セキュリティ主義

5.1. セキュリティ主義

5.1.0 要旨

「セキュリティ」を担当すると，自ずと「セキュリティ」一辺倒になり，セキュリティと他とのトレードオフを考えなくなる。しかもいまは，「セキュリティ」バブルが，この心理傾向の環境になっている。結果は，セキュリティ主義――「セキュリティ」を絶対（正義）にしてしまう精神構造。

セキュリティ主義は，「セキュリティ」に「生活」を従わせる本末転倒をやる。セキュリティ主義を前にして，ネットワークの思想・理念は萎んで消える。そしていまは，このセキュリティ主義で「セキュリティ・ポリシー」がつくられ・進められようとする状況にある。これは，「ネットワーク支配」がまさに起ころうとしている危険な状況である。

5.1.1 セキュリティ主義

5.1.1.1 セキュリティ主義

「セキュリティ」を担当すると，「セキュリティ」にのめり込む。周りを見なくなり，「セキュリティ」一辺倒になる。他とのト

レードオフを考えなくなる。「セキュリティ」を「ゼロかイチか」の問題にしてしまい，「イチでなければならない」の潔癖症を身につける。——これをここでは「セキュリティ主義」と呼ぶことにする。

セキュリティ主義は他とのトレードオフを考えないので，本末転倒をやる。すなわち，「セキュリティ」に「生活」を従わせようとする。——生活において「セキュリティ」は程度問題なのだが，「イチでなければならない」の潔癖症は（値がイチではない「不潔な」）現実の生活を許さない。セキュリティ主義は，批判の対象とし，そして退けねばならない。

5.1.1.2「セキュリティ」バブル

「バブル」という＜集団心理＞現象がある。バブルが終わってバブル期を振り返り，社会全体が舞い上がっていたことに呆れる。しかし，バブルの最中には，それぞれが自分は合理的に思考し行動していると思っている。バブルと「合理的な思考・行動」は，矛盾しない。「合理的な思考・行動」は，時間スパン依存であるからだ。自分 / 社会の一生を今日 1 日のように考えるのか，それともこれから先ずっとのように考えるのかで，「合理的な思考・行動」が違ってくる。バブルとは，自分 / 社会の一生を今日 1 日とするような思考・行動の仕方を人がとるようになる現象である。「ＩＴ」が，バブルになった。そしていまは，「セキュリティ」がバブルになっている。

バブルは，短期利益回収型のビジネスが触媒になる。特に，ベンチャー型ビジネスが，バブルの雰囲気形成に一役買う。「セキュリティ」バブルでは，セキュリティビジネスがバブルの雰囲気形成の中心にいる。

「セキュリティ」バブルの渦中にいる者は，「セキュリティ」に対する自分の考え方（「合理的な思考・行動」）を疑っていない。しかしそれは，自分 / 社会の一生を今日 1 日とするような思考・行動の仕方をとっているということである。よって，失敗する。ゆえにバブル期にこそ，「いま」を長期スパンで（すなわち，「いま」を未来像と重ねて）思考しようとするインテリジェンスが必要になる。

「セキュリティ」のいまのパラダイムは「虫を自分に寄せ付けない」である。しかし，これはもう無理になってきている。すなわち，このパラダイムは，(1) 手間暇と経費に関してひどくハイコストになってきた。（よって，セキュリティビジネスが成り立つ。）そして，(2) 実効しているのかどうかが，現実にわからなくなりつつある。

これは，システムが拡大し複雑系になるときの，システムの宿命である。大きなシステムは，「虫」を呼び込む。見方を変えれば，大きなシステムは，「虫（小さき者・卑しき者）」をたくさん養う役割を担う。一本の大木は，無数の虫を自分に棲まわせる一つの生態系である。ほ乳動物は，自分の腸にびっしり隙間無く寄生虫を棲まわせる。そして，「虫」が己の要素になっていく。

いま，ネットワークは，犯罪や病毒を棲まわせるシステムに成長した。すなわち，「機能的不具合・トラブルに対して強くなる」という形とともに，「犯罪や病毒に対して強くなる」という形で，進化している。実際，いま急に犯罪や病毒が無くなったときには無用になってしまう機能・装置を，既に数多く内装している。つまり，ネットワークは，現実に，犯罪や病毒と共にあるべきカラダに変わってきている。

「虫を自分に寄せ付けない」パラダイムは，もう無理になってきており，早晩破綻する。一方，「セキュリティ」バブルは，人にこの破綻を見させないように働く。そして，無理な方向に進ませる。無理は，システムをいびつにする。いびつなシステムとは？それは，内部統制，使用制限，thin client，認証，障壁，機能削除，アップデート等々を錦の御旗に掲げる「セキュリティ至上」のシステムである。そして「セキュリティ」バブル期には，これは「いびつ」と思われない。

5.1.1.3 インターネットの理念実現仕様が裏目に

インターネットが大学に入ってきたときのそれの思想・理念は，「自由と進歩」「貢献」「共有・互恵」「ユーザ本位」にあった。

システムには，「共有・互恵」「ユーザ本位」の機能が盛り込まれた。個が欲することの実現のためにインターネット全体が協力する——そのような考え方である。例えば，あるサーバへのアクセスでは，他のサーバに途中の足場になってもらえる。メールサーバは，郵便ポストと同じに，だれでもメール送信のために使える。自分のサーバを，できるだけ多くの人に使ってもらえるようにする。

その後，インターネットは，経済インフラ，そして生活インフラへと「成長」した。そしてこれに伴い，ネットワークの悪用とそれに対するセキュリティが，問題になってくる。アンセキュアなシステムは悪用の踏み台にされることから，そのようなシステムを運用している個人・組織の社会的責任が厳しく問われるようになる。ここに，インターネットの「自由と進歩」「貢献」「共有・互恵」「ユーザ本位」の思想・理念を実現するためのシステム仕様は，完全に裏目に出てしまうことになった。

5.1.1.4 インターネットの理念の棄損

大学のネットワークは，大学の各部局それぞれでネットワークの可能性，活用方法，管理運用方法を，手探りする形から始まった。そこでは，いろいろなことが指向され，実験された。

その当時のネットワークの思想・理念は，「自由と進歩」「貢献」「共有・互恵」「ユーザ本位」にあった。システムには，「共有・互恵」「ユーザ本位」の機能が盛り込まれた。

その後，インターネットは経済インフラ・生活インフラに「成長」し，これに伴いセキュリティーが課題になってくる。セキュリティとは，自分の家に鍵をかけ，外から侵入されたり・盗まれたり・覗かれたりがないようにすること。ここに，インターネットの理念（「共有・互恵」「ユーザ本位」）の実現としてつくられてきたシステムの仕様が，完全に裏目に出てしまうことになる。（§5.1.1.3 インターネットの理念実現仕様が裏目に）

そして，ネットワークの「自由と進歩」「貢献」「共有･互恵」「ユーザ本位」の思想･理念は，捨てられる。 ――インターネットの思想・理念に疎い者は，簡単に捨てる。それらを知っている者も,諦めて捨てる。システムに盛り込んできた「共有･互恵」「ユーザ本位」の機能は，すべて封印される。そのような機能を生かしたままにしているシステム管理者は,「犯罪的」ということになる。

5.1.1.5「セキュリティ」ビジネス

ＩＴ企業は,「セキュリティ」バブルにビジネスチャンスを見る。「セキュリティ」商品をつくり商売しようとする。そしてこの関係において,「セキュリティ」ビジネスは「セキュリティ」バブルを演出していることにもなる。

「セキュリティ」ビジネスは，セキュリティが実現・達成しないことで成り立つビジネスである。セキュリティは着実に高まっていくが，このことに対し彼らは,

「*依然危ない*」「*新たな危険が発生している*」

を言い続けねばならない。よって，消費者の方は,「セキュリティ」ビジネスが言ってくることを,

「*ビジネスとして言っているのだ*」「*程度問題・トレードオフを無視した言い方をしているのだ*」

と受けとめるのが正しい。

この構造の理解は重要である。「この分野だから，消費者は企業を 100%信用してかかってよい」というものはない。「ウィルス対策ソフト」も例外ではない。

確認： 危険が言われるとき，つぎの２通りの警戒がある：

A. 言われている危険に対する警戒

B. 危険を言っている者に対する警戒

5.1.2「セキュリティ・ポリシー」の危険性

5.1.2.1「セキュリティ・ポリシー」の危険性

いまは，セキュリティ主義で「セキュリティ・ポリシー」がつくられ･進められようとする状況にある。これは,「ネットワーク支配」がいつでも起ころうする危険な状況である。

セキュリティを言い出せば，何でもありになる。「安全第一」であるからだ。実際，セキュリティを理由にしたネットワーク使用の自由制約に際し，異論を述べようとする者は，まずほとんどいない。一般ユーザなら，セキュリティを言われると,「定めし事情があるのだろう」「自分独りが勝手を言うことはできない」になってしまう。

セキュリティを理由にした自由制約に対する異論は，つぎの形になる：

「*セキュリティより自由が大事*」

「*セキュリティを理由にした自由制約は，本末転倒*」

そして，つぎの思考法を用いる：

「安全」を程度問題・確率の問題としてとらえ・考え，

そして「自由」とのトレードオフを考える。

この異論を立てることは，ひじょうに面倒であり，成功させることも簡単でない。つまり，異論を立てるのはコスト（労力と時間）がかかる。異論の構想をもてる者も，このコストがひどいのを見て，無抵抗を選ぶ。

一般に，自由の保守は，ひたすら面倒に耐えるということである。降りかかってくる火の粉に逐一リアクションすること。このリアクションを面倒がって，一つに妥協すると，後はずっと妥協をつづけねばならなくなる。 ――＜しがらみ＞の醸成。

セキュリティを理由にした自由制約に対して異論をつくるのはたいへんだが，セキュリティを言う側は簡単に自由制約を言う。実際, セキュリティのための自由制約を伝える事務連絡は，ありふれている。なぜ，セキュリティを言う方は簡単か？異論に出会わないからである。出会うことがないので，異論があり得るということに想いが至らない。そして，最大正義を述べているつもりで，セキュリティを言う。

5.1.2.2「セキュリティ・ポリシー」の沿革

国立の機関に対して「セキュリティ・ポリシー」が明示的に示されたのは,『情報セキュリティポリシーに関するガイドライン』(情報セキュリティ対策推進会議 / 官邸 , 2000-07-18) ([1]) を以てする：

> 各省庁はこのガイドラインを踏まえ、平成 12 年 12 月までに情報セキュリティポリシーを策定し、これに基づく総合的・体系的な情報セキュリティ対策を図ること‥‥
> これらの情報に関して利用者個人の裁量で、その扱いが判断されることのないよう、組織として意思統一され、明文化された文書である情報セキュリティポリシーを策定することが必要である。(II.1.(1))
>
> 情報セキュリティポリシーの中には、継続的な情報収集及びセキュリティ確保の体制を構築しておくこと、また「いかに破られないか」のみならず「破られたときどうするか」についての対策も適切に規定し、当該規定に基づいた対策を十分に構築しておくことが重要である。(II.1.(2))
>
> 情報セキュリティポリシー［とは,］各省庁が所有する情報資産の情報セキュリティ対策について、各省庁が総合的･体系的かつ具体的にとりまとめたもの。
> どのような情報資産をどのような脅威から、どのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定。情報セキュリティ基本方針及び情報セキュリティ対策基準からなる。(II.3)
>
> すべての情報は、その重要度に応じて適切に分類された上で、その分類毎の適切な対策を講じていく必要がある。(II.4)
>
> ポリシーは、平成 15 年度にその基盤が構築される電子政府の実現のための情報セキュリティの十分な確保を当面の目標として策定していくものである (II.6.(2))

リスク分析［において］重要性の分類を行い、この結果に基づき、要求されるセキュリティの水準を定める。

脅威の例
物理的脅威：侵入、破壊、故障、停電、災害等
技術的脅威:不正アクセス、盗聴、コンピュータウイルス、改ざん・消去、DoS 攻撃、なりすまし等
人的脅威　：誤操作、持ち出し、不正行為、パスワードの不適切管理等
(III.2.(4),(4),(a))

5.1.2.3「セキュリティ・ポリシー」の方法論

1.「セキュリティ・ポリシー」は,「ネットワークは破られてはならないもの」から出発する。この立場は,「ネットワークは破られるもの」の立場を退ける。

「破られてはならないもの」「破られるもの」の選択肢の意味は何か？一つに，コストである (コストの内容は，管理労働と経費)。セキュリティは, コストとのトレードオフで考えられる。ハイ・セキュリティを求めれば，ハイ・コストになる。

また，この選択肢には,「共生」の考え方の違いがある。「破られてはならない」を立場とする者は,「破られてはならない」を他にも及ぼす。このことで，迷惑な存在になる。一方,「破られるもの」は,「共生」の敷居が低いことを望む立場である。

2.「セキュリティポリシー」は,「規則遵守」をセキュリティが実現されている形とする立場である。「セキュリティポリシー」作成の後には,「遵守義務」がくる。

「規則」の立場は,「良識 (不文律)」の立場を退ける。「規則」「良識」の選択肢の意味は何か？「良識」が採られるのは，自由・融通を保つためである。「良識」は信用ならない (性悪説) となるとき，自由・融通は「悪さをする」の意味になる。そこで，統制のための「規則」に向かう。

3.「セキュリティポリシー」は，ネットワーク管理者を「人を管理・統制する者」にする。この立場は,「ネットワーク管理者＝ユーザの利便性を考える者」の立場を退ける。特徴的なことに，組織執行部は「情報セキュリティ委員会」を人の管理組織として用い, そしてこの中にネットワーク管理者を取り込む。

「セキュリティ」を名分とする「人の管理・統制」は，通りやすい。感覚麻痺して,「何でもあり」になる。例えば，個人の PC にインストールされているソフトウェアは,「情報セキュリティ委員会が関知すべきでない情報資産」である。しかし，不用意でいると簡単に「関知すべき」に転じる。

4.「セキュリティポリシー」は,「失敗忌避」の立場になる。失敗は，コンプライアンスだの失敗の報告義務だのと，ただ形式的に大騒ぎされる。大騒ぎは,「失敗＝罪」の雰囲気を醸成する。そして，失敗しそうなことを封じる管理・統制，失敗に対する臆病が，進行する。

5.「セキュリティポリシー」は,「マニュアルで処理」の立場である。実際のところ，ひとはマニュアルをつくることはできるが，マニュアルを読まない・読むことができない。マニュアルをつくる側は，マニュアルをつくったことで問題が解決したつもりなる。「セキュリティポリシー」の効用は，ポッカリ大きな穴をあけるだけというネガティブなものである。

5.1.2.4 thin クライアント

「セキュリティ」の主題を自ら理論化できていない組織 / 機関は，セキュリティの問題に対しては最も安全な (すなわち責任問題化を最も免れ得る) スタンスを選ぼうとする。その結果, バランスを欠いたやたら高いプライオリティを，セキュリティにおく。

「thin クライアント」という概念がある。ネットワーク端末 (コンピュータおよび使用主体) の機能をできるだけ絞る / 低くする，という意味だ。これのもともと発想は：

> *多くのそして雑多な端末の管理の煩雑を減じるために, 端末を一つの規格にし,「アプリケーションはサーバが提供する」という形で端末の機能をできるだけ減らす。*

しかし今日,「thin クライアント」が「セキュリティ」の関連で言われるようになっている。すなわち：*ネットワーク端末で悪さをさせない / 事件を起こさせないために，ネットワーク端末を「thin クライアント」にする。*

ＩＴ産業は「thin クライアント」をビジネスにしようとして,「セキュリティ」の不安をあおる。セキュリティに漠然とした不安を抱く組織 / 機関は,「thin クライアント」を趨勢と受け取って,「thin クライアント」の導入を考える。しかしこのとき，組織 / 機関は「セキュリティと人的資源 / 組織活力のトレードオフ」の意味を十分理解する必要がある。

「thin クライアント」で thin にされているのは，ネットワーク端末の機器である以上に, それを活用する組織構成員である。「thin クライアント」は，人的資源のポテンシャルを自ら下げる行為。よって，ネットワーク端末が「*組織構成員が，多様な個として，多様な情報力を発揮するための装置*」になっている組織 / 機関では,「thin クライアント」は自殺行為になる。

> 註：管理主義が風土の組織 / 機関では，セキュリティが人的資源 / 組織活力と簡単にトレードオフされる。 なぜなら，管理主義は，責任を問われる立場に就いた者に，組織よりも自分の免責を考えよう仕向けるからだ。

5.2「無菌」パラダイム

5.2.0 要旨

ネットワーク管理の立場からのセキュリティ対策は，管理主義の本末転倒――「システムによる人支配」――としてのセキュリティ主義に転じやすい。このセキュリティ主義は,「無菌」パラダイムに立つ。「無菌」は無理なスタンスである。この無理を通そうとすることで，管理主義の本末転倒に進む。

「無菌」パラダイムは，「健康」パラダイムへシフトされねばならない。「健康」パラダイムの要諦は，保菌・脆弱性持ち・感染症既往歴有りを普通態と見なすことである。

5.2.1「無菌」パラダイムの無理を知る

5.2.1.1 ネットワークの進化とセキュリティ

ネットワーク / インターネットは，いま，完全に社会の基本インフラになっている。社会はネットワークの上に基幹要素をシフトし，ネットワークがトラブルを起こしたときには社会全体が麻痺してしまう構造をつくった。

これは，わずか十数年の間の出来事である。そして，この事態の急展開に，ネットワークの精神文化が追いついていない。

インターネットは，現在のものとはまったく違うスタンス・形で始まった。日本の国立大学がインターネットでつながった 1990 年代初めの頃は，イノベーション・篤志・連帯がインターネットの文化だった。そして，社会全体がインターネットに参入してきた。インターネットは，社会の構造をそのまま取り込んだ社会インフラになった。商業主義や犯罪もそっくりここに棲む。

ネットワーク管理・運用の方法論も，この事態の推移に応じて変化してきた。大学インターネットの時代は，サービスを広く共有するという思想に立っていた。ネットワーク管理・運用の方法論は，「門戸・サービスを外に開く」だった。商業主義や犯罪の棲むいまのネットワークの管理・運用の方法論は，セキュリティ――すなわち，各戸がしっかり施錠するというもの。

さらに，セキュリティは，《事件 → 責任追及》のいまの社会風潮とマッチして，いまやネットワークの第一等の「精神文化」になった。セキュリティを信用問題に位置づけるようになった組織・機関は，セキュリティ対策（免責対策を含め）に余念がない。ハードウェア，ソフトウェアのビジネスが一段落し新しい市場を模索していた IT ビジネス界は，セキュリティに大きな市場を見て，セキュリティ・ビジネスを展開している。

しかし，システム一般に言えることとして，システムは無菌・無垢のままで大きくはなれない。システムの進化は汚染とのトレードオフである。実際，システムの汚染に対して再構築が方法となり得るのは，システムが小さくて単純な場合だ。大きなシステムが汚染したときには，その汚染との共存を考えるしかない。このとき，システムに関する「セキュリティ」問題は，「健康」問題に変わる。

> 註：わたしたちの身心の健康は，体に取り込んだ菌や寄生生物との共存を要素にしている。 寄生は共生へと変わる。わたしたちの身心は，体に取り込んだ菌や寄生生物と共にある。これらの菌や寄生生物を排除したならば，人は病気になる。

ネットワークは，日々急速に拡大し続け，複雑の度を増し，まさに「セキュリティ」から「健康」へのパラダイムシフトが必要になるシステムへと進化している。

5.2.1.2「無菌」パラダイムの無効化

ネットワークを使った不正・犯罪行為は，つねに試みられる。膨大な数にのぼりそして不可視のこれらに対し「無菌」パラダイムで臨むことは，不可能になっていく。

実際，何を対策しても，「完全はない」が言われる。「あらゆることに危険がある」が言われる。しかし，細かいことにいちいち神経を使って対応していたら，身が保たない。そんな暇もない。知識・技術・能力の面でも，とてもついていけるものではない。そして，果たしていま自分が無菌でいるのかどうかも，わからない。

「注意喚起」も，意味をもてなくなる。――「注意喚起」は，ユーザにとってとんでもなく曖昧で，内容的に大変そうで，結局対応のしようがないことを，言うだけになる：

○ *パソコン及び外部記録媒体等の適正な管理をお願いします。*

何をやれば「適正な管理」ということになるのか‥‥

○ *パソコンや外部記録媒体（新規に購入したものを含む）におけるウイルス感染の有無，OS やアプリケーションの脆弱性への対応状況，不要なアプリケーションや機能の導入・使用状況，ウイルス対策ソフトにおけるパターンファイルの適用状況を確認するなどして，情報漏えい事案の発生防止及び発生時の被害拡大防止に努めてください。*

何を言っているのかわからない。 何をどうすればいいのか，わからない。ウィルス対策ソフトが汚染されるということはないのか？ どこまでが信用してよいことなのか，さっぱりわからない。結局，注意されても，どうしようもない。

○ *安易に不審なメール・添付ファイル及び Web ページを開くことがないようにしてください。*

「安易・安易でない」の基準・理屈がわからない‥‥
「不審なら開かない」では，仕事はできない。

○ *関係者を編ってウイルスを含んだ電子メールが送られることもあります。*

開くことになるだろう‥‥

○ *電子メールは送信者を偽ることが容易です。メールに含まれるウェブサイトのリンクを，安易にクリックしないこと。*

クレジットカードの「今月の使用状況」がウェブページにあることを知らせるメールが来た。リンクボタンをクリックしてもよいのか？アップデートされたソフトのダウンロードサイトを知らせるメールが届いた。ウェブサイトのリンクボタンをクリックしてもよいのか？（関連して：コンピュータ画面で，アップデートされたソフトがダウンロードできるというメッセージのウィンドウが開いた。信用していいのか？）

○ *フィッシング詐欺に注意しましょう。*

オンラインショッピングはどんな場合にだいじょうぶなのか？これはよい・これはだめは，どうしたらわかるのか？

○ *大手企業や官公庁のウェブサイトも，ウィルスを埋め込まれてしまっていることがあります。そのようなサイトにアクセスすると感染することになります。*

ウェブを使わないという選択はできない。
結局，注意されてもどうしようもない。

5.2.1.3「病気にかかったらゼロから作り直す」は無理

コンピュータのウィルス感染や不正侵入では，不正プログラムの埋め込みやファイルの改竄が行われる。このことを，埋め込まれた不正プログラムや不正コードを「病原体」と見立てて，「コンピュータが病気にかかる」と言い表すことにする。

セキュリティの教科書には，病気にかかったコンピュータはゼロから作り直すとある。なぜなら，病原体は巧妙に身を隠している。それを見つけ出し駆除することにしても，全部を見つけ駆除できたかどうかはわからない。したがって，ゼロから作り直すしかないというわけだ。

では，どうやってゼロから作り直す？問題は，これまでユーザが蓄積してきたデータファイルである。直近のバックアップを用いてよいか？ ——しかし，その時にはクリーンであったという保証はない。疑うほどに遡らねばならないが，データは気前よくバッサリ捨てられるものではない。1 日分といえども，取り返しが利かないものであれば，保たねばならない。

よって，「ゼロから作り直す」は，現実にはあり得ない。病原体を見つけ出し駆除することに手を尽くす。そして「これでまだ残っていたら，もうしようがない」というところまで行って，「復旧した」ことにする。以降このコンピュータは，「病気にかかったことがある・病気を持っているかも知れない」ものとして生きる。

5.2.2 ネットワーク「感染症」の実際を知る

5.2.2.1 ネットワークの「感染症」

「ネットワーク･セキュリティ」（ここでは,「ネットワーク」のことばを「ネットワークないしその中のコンピュータ」の意味で用いる）の中身は,「ネットワーク悪用の試みからネットワークを守る」対策である。ネットワークを悪用しようとする者は，いろいろな方法を講じてくる。しかし，主要な方法はつぎのものである：

ネットワークに虫を寄生させ，
それを使ってネットワークを悪用する。

ここで謂う「虫」は，プログラムである。ネットワークに寄生した虫は，ネットワークの内部に悪用可能な状態をつくる。また，ネットワーク悪用の主体を兼ねるものもある。

一般に，寄生虫に棲まわれカラダを蝕まれることは，病気の一つとされる。実際,「感染症」がこの病気の名である。

ネットワークの「感染症」の場合,「感染」にはつぎの２タイプがある：

1. 寄生虫が潜む誘いの餌を，食べてしまう
2. 知らずに寄生虫を注射される (自然感染)

ここで「知らずに寄生虫を注射される (自然感染)」とは, クラッキング (攻撃 / 侵入) の自動プログラムにやられてしまう結果として，寄生虫を体内に棲まわせられる場合を謂う。

1, 2 を人体の感染性で喩えると：

1. 大腸菌のついた野菜を食べる
2. マラリア原虫を持つ蚊に刺されて，マラリア原虫が内に入る

ネットワークの中に寄生虫を放つ目的には，つぎの２通りがある：

A. ネットワーク悪用のエージェントとして使う
B. テロ (愉快犯)

A の場合は，寄生虫を放った者は同時に「虫使い」である。B の場合は，寄生虫を放ってそれで終わり。(Winny を使って個人のコンピュータの内容をインターネット上に流すウィルスは，B タイプである。)

タイプＡの場合，寄生虫の行う仕事にはおよそつぎの３タイプがある：

a. バックドア (主人が入って来れるように，内側からドアを開ける)
b. 盗み見エージェント (ネットワーク内の情報を盗み見て，主人に知らせる)
c. 兵隊ロボット (主人の命令が来たら，グローバルネットワークに散在している同類と同時一斉に，命令されたことを行う)

なお, ネットワークの「感染症」は, 多くの場合伝染病である。すなわち寄生虫は，ネット上に他の宿主を求め，自分のコピーを送り込もうとする。

5.2.2.2「感染症」と犯罪性の関係

ネットワークの「感染症」はつぎのようにカテゴライズできる (§5.2.1 ネットワークの「感染症」)：

<table>
<tr><th colspan="2">寄生虫の仕事</th><th>感染の仕方</th><th>伝染性</th></tr>
<tr><td>ネット悪用
エージェント</td><td>a. バックドア
b. 盗み見
c. 兵隊ロボット</td><td rowspan="2">つぎの2通り：
誘いの餌
注射</td><td rowspan="2">寄生虫の多くは，
自分で宿主を開拓
するタイプ</td></tr>
<tr><td colspan="2">テロ</td></tr>
</table>

「ネット悪用エージェント」と「テロ」の違い

「ネット悪用エージェント」によるネットワーク悪用は，ビジネスである。自分のためであり, 計算的である。一方「テロ」は，ただ「世の中や権力を引っかき回したい」(「世の中をよくしたい」も含めて)。自分にとっての利得は考えの中になく，このテロで世の中がどうなるかについても計算しているわけで

はない。

テロの例：

コンピュータの中のファイルを，消去する。

コンピュータの中のファイルを，インターネットに流す。

公的機関や企業の公式ホームページを改竄する。

「誘いの餌」と「注射」の違い

両者の違いは，魚を捕るのにつり糸を使うか銛を使うかの違いと同型。――「つり糸を使う」では，魚が自分の方に寄ってくる。「銛を使う」では，自分が魚の方に寄っていく。

前者と比べて後者では，労力，身に降りかかる危険，そして必要な技能の度合いが格段に高まる。よってこの場合は，労力・危険度・技能に見合う成果をもたらすような獲物に狙いを定める。「誘いの餌」の被害者は狙われた者ではないが，「注射」の被害者は狙われた者である。

註：ネット端末でいうと，「誘いの餌」では PC を獲物にする。「注射」では，PC およびサーバマシンを獲物にする。注射攻撃に対して脆弱な部分を探しだし，そこから攻撃する。――これらのことを行うのも，コンピュータプログラムである。(人がマニュアルで行うのではない。)

5.2.2.3 寄生虫感染のりくつを知る

寄生虫は目に見えないので，人類は病気の不安にただ怯え，病気の迷信をさまざまにつくった。ネットワークの感染症の場合も，事情が似ている。

一般ユーザは，「○○をしてはならない」「△△をしなければならない」を指示される。一方，「○○をしないことの意味は？するとどうなるか？」「△△をすることの意味は？しないとどうなるか？」の学習機会をもたない。そこで，りくつを知らずにただ不安を抱くという状態になる。

りくつを知らずにただ不安を抱くという状態は，何をまねくか？迷信商売に騙される。衆愚政治に利用される。

ここで，寄生虫感染のりくつを，つぎの２つのタイプそれぞれについて，簡単に (一般者の理解形として) 押さえておく：

A. 知らずに寄生虫を注射される (自然感染)

B. 寄生虫が潜む誘いの餌を，食べてしまう

A. 知らずに寄生虫を注射される (自然感染)

1.「コンピュータをネットワークにつなぐ」の意味には，「不特定多数のコンピュータからアクセスを受ける」が含まれる。「アクセスを受ける」の実体は，「通信パケットの形になったコードを受ける」である。

2. 通信パケットには種類が定められている。コンピュータは，通信パケットの受け口 (ポート) を複数装備している。そして，「通信パケットの種類毎に受け口を配分」という形でこれらを使う。「受け口を配分」の意味には，「ある種類の通信パケットに対しては受け口を用意しない」(通信制限) も含まれる。

3. 受信を許可している種類の通信パケットが届くと，その内容 (コード) を処理するプログラムが起動する。そのプログラムの作成者 (プログラマー) は，「処理するコードはこんなものである」と想定してプログラムをつくっている。しかし，プログラマーの想定は，プログラムにとっては知ったことでない。プログラムは，プログラマーの想定外のコードに対しても，律儀に処理をする。

4. このしくみを利用して，つぎのことが可能になる場合がある：

プログラムがあるコードを律儀に処理した結果が「寄生虫を棲まわせる」になる。

これが可能になるとき，つぎのような言い回しがされる：

「そのプログラムには脆弱性がある」

「可能なら，脆弱性が修正されるまで，そのプログラムが使う受信ポートを閉じた方がよい」

5.「寄生虫を棲まわせる」ことを目的にした危険なコードは，コンピュータに頻繁に届いている。危険なコードを発信しているのは，プログラムである。(インターネット上の膨大な数のコンピュータを獲物として狙うことは人間業ではないが，プログラムならできる。) そのプログラムを動かしているのは，人であるとは限らない。 実際，多くの場合，危険なコードの発信は自動プログラムによる。

6. 危険なコードがコンピュータに届くこと自体は，事件ではない。(普通の風景であり，恐れることではない。) そのコードを受け口から内部へ通すことも，事件ではない。(普通の風景であり，恐れることではない。) 事件は，つぎの場合である：

受信コードを処理するプログラムの律儀な処理が，「寄生虫を棲まわせる」を結果するようなものになっている。

7.「そのプログラムには脆弱性がある」「可能なら，脆弱性が修正されるまで，そのプログラムが使う受信ポートを閉じた方がよい」の情報は，本来，そのプログラムのベンダーがユーザに伝えることになる。この種の情報は，第三者機関によっても提供されている。しかし，このような情報に付き合う面倒を一般ユーザの義務のようにすることは，現実的でない。「自然感染しないようにする」は，無理なスタンスである。一般ユーザは，つぎのスタンスでよい：

(1) ソフトのアップデート (アップデータのダウンロードと自動インストール) がベンダーからアナウンスされたら，これに応ずる。

(2) ウィルスチェックソフトを自分のコンピュータにインストールする。ウィルスチェックソフトが何かを指示してきたら，それに従う。

(3) これらをしてなお自然感染してしまったら，しようがないと諦める。

(4) 併せて，寄生虫感染に続く犯罪のタイプ (特に，盗み見，ファイル流出) を考慮して，コンピュータ内のファイルを「被害を小さくする」よう整備することに努める。

8.「寄生虫の自然感染ないしそれによる被害発生」の場合,「責任問題」はどのようになるか？これは，ユーザ個々の自己責任である。インターネットは,「寄生虫の自然感染ないしそれによる被害発生」が自分の身の上にも起こり得る世界である。「寄生虫の自然感染ないしそれによる被害発生」が絶対嫌なら, インターネットにコンピュータにつながないことだ。つなぐなら,「寄生虫の自然感染ないしそれによる被害発生」を覚悟し，セキュリティ対策も自分で責任をもたねらばならない，となる。

B. 寄生虫が潜む誘いの餌を食べてしまう

このタイプの感染には，つぎのものがある：

(1) あるファイルをダウンロードして開き，感染する
(2) メールないしそれに添付のファイルを開いて，感染する
(3) あるウェブサイトにアクセスして，感染する

(1) あるファイルをダウンロードして開き，感染する

このファイルには，つぎの２通りがある：

(1a) 実行ファイル (→ 寄生虫をインストールする)
(1b) 文書ファイル (通常使っているプログラムで開かれる)

(1a) の場合の寄生虫生成は，自明。

(1b) の場合の寄生虫生成は，つぎのようになる。

ファイルを開くとは，あるプログラムが起動してそのファイルに書かれているコードを処理をすることである。そのプログラムの作成者 (プログラマー) は,「処理するコードはこんなものである」と想定してプログラムをつくっている。しかし，プログラマーの想定は，プログラムにとっては知ったことでない。 プログラムは，プログラマーの想定外のコードに対しても，律儀に処理をする。このしくみを利用して，つぎのことが可能になる場合がある：

プログラムがあるコードを律儀に処理した結果が
「寄生虫を棲まわせる」になる。

そして，実際これを利用する者がいる。

註 : (1b) の場合の寄生虫生成は，しくみとしては「自然感染」の場合と同じである。

(2) メールないしそれに添付のファイルを開いて感染

「メールないしそれに添付のファイルを開く」は ,「あるファイルをダウンロードし開く」の一つの形である。「メールを開くだけで感染」は，(1b) のケース。「添付ファイルを開くことで感染」は，つぎのように場合が分かれる：

・メールソフト経由で開くときは，(1b) のケース。
・一旦ファイルとして保存してから開くときは，(1a) と (1b) の２通りがある。

(3) ウェブサイトにアクセスして感染

ウェブサイトにアクセスするとは，そのサイトからウェブページのソースファイルを自分のコンピュータにダウンロードし，そのファイルをブラウザで開くことである。「ファイルをダウンロードし開く」の一つとして，(1b) のケースになる。

ここで,「脆弱性」とは：

(1) 通常使っているプログラムが,
あるコードを律儀に処理した結果が「寄生虫を棲まわせる」になる

具合になっているとき，つぎのような言い回しがされる：

「そのプログラムには脆弱性がある」

「脆弱性修正のアップデータが既にあるときは, アップデートする」

「脆弱性修正のアップデータがまだできていないときは, 可能なら，アップデータができるまでそのプログラムを使わない」

(2)「プログラムの脆弱性」の情報につねにアンテナを張っていることを一般ユーザに求めるのは，現実的でない。一般ユーザは，つぎを実行していればそれでよしとされねばならない：

・ウィルスチェックソフトをインストールする。
・ベンダーからアップデートの催促が届いたときには，これに応ずる。
・つぎのことを (一応頭の中では) 心掛けている：
1. 怪しいファイルは，ダウンロードしない。
既にダウンロードしていたら，開かない。
2. 怪しいメールないし添付ファイルは開かない。
3. 怪しいウェブサイトにはアクセスしない。

註 :「(一応頭の中では)」としているのは，実際問題として「怪しい」は不明であるし,「怪しいを言っていたら仕事 / 生活にならない」だってあるからである。

5.2.2.4「感染症」対策とこれの限界

ネットワークの「感染症」の対策は，つぎの２段階で考えられることになる：

1. 虫に寄生されないようにする。
2. 虫に寄生されたことがわかったときは，これを駆除する。

1.「虫に寄生されないようにする」

感染の仕方には,「誘いの餌」と「注射」の２通りがある (§5.2.2.1 ネットワークの「感染症」)。

「誘いの餌」の場合は，つぎのことが対策になる：

・「誘いの餌」についての知識を持ち,「誘いの餌」に誘われないよう心掛ける。
・「誘いの餌」が自分に届かないようにする (「ファイアウォール」)
・餌を食べてしまったときは，入り口で虫を殺す (「ウィルスチェック」)

そして,「注射」の場合は，つぎのことが対策になる：

・「注射」を打たれてしまうような隙を，つくらない。
　例えば,「注射」を打たれそうな場所を固く閉じる。
・「注射」を打たれていなかどうかを,つねにチェックする。

しかし，以上の対策には自ずから限界がある。先ず，ネットワークは,「不自由のない通信･すべての者に開かれている通信」を本位とする。一方,「感染症」予防の方法は通信制限である。「感染症」予防は，通信そのものを不自由にする。(確認：最強のセキュリティ対策は，ネットワークを使わないことである。)

実際，ひとは安全と不自由のトレードオフを考える方に向かう。 ――「安全か不自由か」ではなく，安全と不自由の間に折り合いをつけることを考える。

つぎに,「寄生虫を入り口で阻止」の対策は，人の行うこととしては無理である。ウィルスチェック・ソフトは，ウィルスの多様化・新登場に追いつかなくなる。そもそも，本当に機能しているのかどうか，ユーザにはわからない。 ――実際，ウィルスチェック･ソフトは,これに対するユーザの「信用」で保っているに過ぎない。「注射」を打たれていないかどうかのチェックも，実際作業としてはできることではない。

註「すべき」と「できる」は違う。国は外国人に不法侵入させないことになっているが，不法侵入はふつうに起こっている。 不法侵入阻止が実際作業としてできることではないからだ。

2.「虫に寄生されたことがわかったときは，これを駆除する」

いろいろ工夫し，ツールも用いたりして，寄生虫を見つけ出し駆除しようとする。しかし，寄生虫は巧妙に隠れている。寄生虫を見つけ出しこれを潰しても，これで本当にクリーンにできたのかどうかはわからない。実際，本当の寄生虫を隠すために，わざと囮の寄生虫が見つけ出されるようにしているのかも知れない。そこで，セキュリティの教科書ならば,

「虫に寄生されたことがわかったときは,
すみやかに患者を隔離し，カラダをゼロから作り直す」

と書くことになる。しかし，実際問題として，これはできることではない。現実には,「これ以上やるのは無理」といったところまで寄生虫の駆除をやって,それでよしとすることになる。(§5.2.1.3「病気にかかったらゼロから作り直す」は無理)。

5.2.2.5 感染症患者

寄生虫は，環境変化によって活動できなくなることが考えられる。コンピュータの場合，ＯＳの変更がこの「環境変化」になり得る。また，寄生虫が外部記憶メディアに棲んでいる場合は，コンピュータ本体の変更がこの「環境変化」になり得る。

寄生虫の主人が存在しなくなることも考えられる。実際,「虫使い」の立場に立ってみればわかるように,「虫使い」はラクに続けていかれる仕事ではない。

こういうわけで，つぎからつぎと新しい虫に寄生されるというのでなければ，感染症はやがて消えていくと考えるのが自然である。感染症の既往歴のあるコンピュータのうち現在発症中 (実働的) であるものは，割合的には，おそらくかなり少ないだろう。

5.2.3「ネットワーク犯罪」の実態を知る

5.2.3.1 悪い虫・善い虫

社会を律しているのは，先ず，不文律としての倫理である。そして，法律がこれを補う。ネットワークも同様。ネットワーク犯罪を考えるためには，本来，先ず倫理 (不文律) のとらえができていなければならない。

実際，ネットワークには，犯罪のためにつくられた虫 (悪い虫) の他にも，虫 (善い虫) が棲む：

1. アプリケーションソフトのインストールでは，ＰＣをソフトのベンダーと通信させる虫 (スパイウェア) が同時にインストールされる。
2. ネットワーク管理者は,「虫使い」である。

機能的には，悪い虫と善い虫を区別するものはない。 ――実際，善い虫は悪い虫に転じる。虫の悪い・善いは，虫使いの悪い・善いのことである。しかし，虫使いの「善い」は,「信用されている」である。そして，この信用には何の根拠もない。――虫使いの悪い・善いも，つきつめると自己撞着に陥る：

1. アプリケーションソフトのインストールで起こる「寄生虫感染」が「犯罪」とされないのは，単にユーザがベンダー (「虫使い」) を信用しているからである。 そして，この信用には何の根拠もない。
2. ネットワークにおけるいちばん怪しい「虫使い」は,ネットワーク管理者自身である。

そしてさらには，虫使いの存在さえも立てられなくなる。

註：「ネットワークを寄生虫感染させる」をネットワークへの攻撃 / 侵入 (「クラッキング」) によって行えば，これは不正アクセス禁止法が規定するところの犯罪行為になる。クラッキング罪は住居侵入罪に相当させたものであるが，住居侵入罪は住居侵入するのが人だから成り立っている。一方，クラッキングはプログラムの行うことである。＜プログラム - 対 - これを動かす者＞の対応は，つねにつくれるのか？ 否。伝染性の自動プログラムのすることであれば，それはできない。

5.2.3.2「ネットワーク犯罪」の内容

「ネットワークの寄生虫感染」と「寄生虫感染したネットワークに対する / を使った犯罪」(ここでは,「ネットワーク」のことばを「ネットワークないしその中のコンピュータ」の意味で用いる)は,区別して考える必要がある。実際,「寄生虫感染」の議論で盛り上がってしまう結果，これに続く「犯罪」の方が思考停止される現状がある。

「感染する・しない」を決定的なポイントとする考え方は，間違いである。実際，「感染する・しない」を決定的なポイントとする考え方に立てば，感染したら一巻の終わりである。しかし，セキュリティビジネスが商品とする「万全の措置」にお金をきちんきちんと払っていても，感染するときは感染する。

註：「万全の措置」は，守備していない寄生虫感染に対しては無効である。特に，新種の寄生虫感染の出現では，「万全の措置」がこれに追いつくまでの期間は，感染を避けられない期間になる。

正しい考え方は，つぎのようになる：

1. 感染の仕方とそれにつづく犯罪の内容を理解する
2. 各局面で適切に対応できるようにする。特に，「感染している状態にあって，犯罪に対応する」術を知り，実践する。

以下，「ネットワークの寄生虫感染」と「寄生虫感染したネットワークに対する / を使ったビジネスタイプの犯罪 (すなわち，テロタイプではない犯罪)」について，これの内容 (ただし可能性も含め) を簡単に確認しておく。

1. 個人 A の PC を寄生虫感染させる場合
   a. 寄生虫＝バックドア
      (PC を，不正アクセスの踏み台に使う)
      ○ 不正アクセスの足跡を消す

   b. 寄生虫＝盗み見
      ○ A の個人情報を，虫使い宛に知らせる
      (情報は，なりすまし犯罪に使う)
      個人情報： ID/ パスワード，クレジットカード番号等
      なりすまし犯罪： ネット上売買等
      ○ その他犯罪に使える情報を，虫使いに知らせる
      (情報は，犯罪に使う)
      例えば，A が勤務する組織 B に属するファイルを，つぎのような理由・目的から，取得しようとする (ただし，B に属するファイルを，A が自分の PC に入れている場合)：
      自分にとって価値，裏マーケットで売買，
      漏洩事件として暴露し B を困らせる，等

   c. 寄生虫＝兵隊ロボット
      (PC を，犯罪に使う兵隊部隊の一員にする)
      ○ 誹謗・中傷メール，スパムメール，ウィルスメール等を発信・中継させる
      ○ DoS 攻撃に参加させる

2. サーバ機を寄生虫感染させる場合
   a. 寄生虫＝バックドア
      ○ このサーバ機を，不正アクセスの踏み台に使う
      ● 不正アクセスの足跡を消す
      ○ 犯罪に使う隠れサイトを，このサーバ機の中に構築
      ● 有害・違法な情報 / コンテンツを提供・取り引きするサイト
      ● フィッシングの導き先のウェブサイト
      ――つぎのように使う：
      ・現存する会社のサイトになりすまし，これにアクセスしてきた者の個人情報を取得
      ・寄生虫感染させる
      ● 詐欺行為をするためのウェブサイト

   b. 寄生虫＝盗み見
      ○ ログイン時の入力内容等を，虫使いに知らせる

5.2.3.3「犯罪」の程度を測り，相応に対する

寄生虫感染したネットワークに対する / を使ったビジネスタイプの犯罪 (すなわち，テロタイプではない犯罪) は，つぎのようになる (§5.2.3.2「ネットワーク犯罪」の内容)：

感染対象	寄生虫タイプ	犯　　罪
PC	バックドア	PC を不正アクセスの踏み台として使う
	兵隊ロボット	スパムメール，ウィルスメールを発信・中継 DoS 攻撃に参加
	盗み見	ユーザの個人情報を，虫使いに知らせる (情報は，なりすまし犯罪に使う) その他犯罪に使える情報を虫使いに知らせる (情報は，犯罪に使う)
サーバ機	バックドア	サーバ機を不正アクセスの踏み台として使う サーバ機の中に犯罪に使う隠れサイトを構築
	盗み見	ログイン時の入力内容等を，虫使いに知らせる

ここで，「犯罪被害はどの程度のものか？」と考えてみよう。

註：寄生虫に棲まわれると，システムに負荷が加わる。また，寄生虫のプログラムが拙いものであれば，システムのバグになったりする。よって，寄生虫に棲まわれることによりシステムに不具合が起こるということはある。ここでは，このような被害は考慮外とする。

1. PC の場合

(1) 兵隊ロボット

この場合は，「周りに迷惑をかけている」という道義的問題 / 環境問題になる。自分に直接被害が及ぶという意味の「恐れなければならない」というタイプの問題にはならない。――つぎは，Sophos が発表している「スパムメール・リレー ワースト国 12」([2]) であるが，これは，兵隊ロボットタイプの寄生虫の生息状況を示すデータになる：

1. 米国	28.4%	7. ドイツ	3.4%
2. 韓国	5.2%	8. トルコ	3.2%
3. 中国	4.9%	9. ポーランド	2.7%
4. ロシア	4.4%	10. 英国	2.4%
5. ブラジル	3.7%	11. ルーマニア	2.3%
6. フランス	3.6%	12. メキシコ	1.9%

(2) 盗み見

虫使いの側に立って考えるとわかるように，なりすまし犯罪につかえる有用な個人情報を盗み見で得ることは，たとえピンポイントで個人を狙うにしても，簡単ではない。ほんとうに割に合うというのでなければ，やれることではない。PC の所有者の方も，なりすまし犯罪につかわれるような情報の入ったファイルについては，それの扱いを注意すればよい。

現実として，一般ユーザの PC を使うスタンスは「風邪を気にしていては生活できない」である。そして，スタンスはこれでよい。なぜなら，システムの脆弱性は，全体的には着実に埋められていくことになるからである。セキュリティビジネスは，ビジネスの都合から，このようなことは言わない。 ネットワーク管理者も，立場の都合上，このようなことは言わない。しかし，「風邪を気にしていては生活できない」が＜見識＞である。

2. サーバ機の場合

○ 不正アクセスの踏み台として使われる

まことしやかにつぎのように言われるのを見ることがある：「*踏み台にされたサーバは，被害者であると同時に加害者である。このサーバが踏み台になって攻撃されたところから，損害賠償を求められることがあり得る。*」このような損害賠償はあり得ない。「風邪をうつされた者が，風邪をうつした者に損害賠償を求める」があり得ないのと，同じである。風邪をうつされた者が風邪をうつした者に損害賠償を求めるということはない。なぜか？「風邪をうつされるのは，自己責任」というようになっているからだ。「風邪をうつされるのがいやなら，うつされる可能性のある場所からは自ら身を退け！」となる。

インターネットは，寄生虫感染症が原因のさまざまな被害が自分の身の上にも起こり得る世界である。被害遭遇が絶対嫌なら，インターネットにコンピュータにつながないことだ。つなぐ以上は，被害遭遇を自己責任として覚悟し，セキュリティ対策も自分で責任をもたねらばならない。——踏み台にされたサーバから攻撃を受けた者は，サーバの管理者にサーバが攻撃している事実を「教えてやる」べきである。同時に，「教えてやる」が限度である。これからさらに進んで「損害賠償」を求めるようなことはできない。

5.2.3.4「犯罪との消極的共存」の思想へ

犯罪が存在するのは，定めし存在する理由があるからだろう。すなわち，犯罪の存在否定は，人の社会が拠って立つある複雑系の否定になるのだろう。

ネットワーク管理では，ネットワーク犯罪は否定的な存在として扱われる。しかし，ともかく存在しそして無くなるとは考えられない以上，その存在は認めねばならない。実際，ネットワークの文化には，文化一般と同じく，「犯罪がせっせと文化にインテリジェンスを与え，文化を育ててきた」面がある。

あるインテリジェンスは，それによって自分の存在を危うくされる / 自分の生活を不具合にされる者にとっては，犯罪である。ただそれだけのことである。インテリジェンスの本質的なところでは，犯罪性はわからなくなる：

1. スパムメールをやるために「虫使い」をやれば，犯罪になる。マイクロソフトがユーザ同報のために行う「虫使い」は，犯罪にならない。
2. インターネットという出来事自体，ある見方に立てば「犯罪」になる。

5.2.4「無菌」パラダイムを支えているものをとらえる

5.2.4.1「セキュリティ」ビジネス

「セキュリティ」は，ここしばらく，ＩＴ業界にとってビッグなマーケットになっている。そしてこの関係において，「セキュリティ」ビジネスは「セキュリティ」バブルを演出している。 (§5.1.1.5 セキュリティ主義と「セキュリティ」ビジネス)

セキュリティ・ビジネスは，「無菌」パラダイムを掲げる。実際，「無菌」が，セキュリティ・ビジネスのためのセキュリティ・パラダイムになる。 ——なぜなら，セキュリティ・ビジネスはセキュリティが実現・達成しないことで成り立つビジネスであるが，「無菌」は実現・達成されないからである。感染症を程度問題にしてしまったら，セキュリティ・ビジネスはひどく成り立ちにくくなる。

5.2.4.2 個人情報保護主義

「無菌」をパラダイムとするセキュリティ主義にとって，個人情報保護主義は強力な味方になる。

個人情報保護主義は，つぎの形で「ネットワークの感染症」の問題と関わってくる：

> コンピュータに寄生する虫の一種に，Winny を使ってファイルをインターネット上に流すものがある。流出するファイルが個人情報であるとき，これは「個人情報保護」の問題になる。

個人情報保護主義は，「ゼロかイチか」の立場である。生徒の名前が書かれた紙が路上に落ちていれば，個人情報流出の責任問題が立てられ，マスコミの取り上げるところとなる。個人情報保護主義を前にしては，「そんなことはたいしたことではない」を言い出すような良識論は完全に封殺される。この「ゼロかイチか」が，「ゼロかイチか」をスタンスとする「セキュリティ主義」とぴったり合い，ネットワーク感染症問題のところでは「無菌」パラダイムとぴったり合う。

Winny を使ってファイルを流出させる寄生虫への対策は，「Winny を使いたいなら，それ専用のコンピュータを用意せよ」が本来のものである。ところが，ファイル流出のりくつの話が面倒なものになるので，ファイルの一斉・一律管理の方向に論が進められる。

個人情報流出には，盗み見タイプの寄生虫によるものも，可能性として考えられる。しかし，ここまで考えると，ネットに繋がったコンピュータでは仕事ができなくなる。

良識論が興らねばならない。すなわち，個人情報保護主義を退け，個人情報保護を程度問題として論じる良識論。そして，問題をつぎの形に替える良識論である：「インターネットに繋がったコンピュータに入れてよいファイルと入れてはならないファイルの区別」「制限されたネットワーク (VPN) の導入」

5.2.4.3 失敗断罪・責任追及主義

「失敗＝隠蔽するもの」とする体質が，人にも組織にもある。失敗隠蔽は社会被害・犯罪性を大きくしていく。そして，ついに犯罪として摘発され，責任が厳しく追及される。

失敗隠蔽の断罪は，失敗断罪に短絡していく。「失敗にはたいてい隠蔽が伴っている」という現実が，この短絡を合理化する。失敗断罪・責任追及主義社会の成立である。

失敗すれば断罪・責任追及がくるので，「絶対失敗を起こさない」が当事者のスタンスになる。「ゼロかイチか」のスタンスである。「この失敗はたいしてことではない / あたりまえ / ありがたい」を言う良識論は封殺される。

自分のネットワークの中で事件が起きたら失敗断罪がまっているとなれば，「ネットワーク管理＝事件を絶対に起こさないための管理」になってしまう。そしてその方法は，事件の因になりそうな＜菌＞ (特に，感染症の菌) の徹底排除である。

一方，当事者には ,「事件を絶対に起こさない」「事件の因になりそうな＜菌＞の徹底排除」が無理なスタンスであることもわかっている。このとき，ネットワーク運用はつぎに向かう：

・事なかれ主義の安全主義
・通達主義の責任回避主義

ここで「事なかれ主義の安全主義」とは，「＜菌＞の出現機会を減らす･無くす」を方法にすることである。そしてこれは，ネットワークを不自由にすることと同じ。(＜菌＞の出現機会を減らす・無くすやり方の最高のものは，「ネットワークを使えなくする」である。)

5.2.4.4「管理 / セキュリティ」パラダイムの未熟

情報システム管理担当者が「事件が発生したら即懲罰」を条件付けられたら，彼らは事件が絶対起こらないシステム運用を行う。それは，情報システムを使えなくすることである。

> 註：情報システムの管理事務の都合とユーザの都合は，異なる。事務は，事件が発生して責任問題が自分にくるのを嫌う。 そこで，情報コンセントに鍵をかけたり，IP の発行を申請制度にしたりする。一方，ユーザは，情報コンセントを自由に使いたい。 そしてこれができるためには，IP が DHCP で自動発行されるようになっていなければならない。

情報システムが使えるようになっているとは，事件も当然起こるようになっているということである。情報システムを使えるようにしようと思うなら，情報システム管理担当者は事件に対しては免責としなければならない。

現在は，事件発生を情報システム管理担当者の責任問題にする雰囲気ができ上がっている。これは，一種の集団心理 / 集団ヒステリー (行政から各機関末端までの全体を含む集団の，集団心理 / 集団ヒステリー) である。どうしてこうなるかというと，「情報化」の歴史がまだ浅いからである。ひとは，「情報システム管理」をどう扱ってよいかまだわかっていない状態にある。情報システム管理のパラダイムが定まっていないのである。

情報システム管理のパラダイムが定まるためには，たくさん修行を積まねばならない。いまは未熟なので，とりあえず「無菌」を情報システム管理のパラダイムにしている。

> 註：「無菌」は，ひとが選ぶパラダイムとしては，もっとも幼稚なものである。菌は世界の要素である。 そして，自分は世界内存在である。 世界を否定しては自分の存在は立てられない。 よって，菌との共生を否定しては自分の存在は立てられない。

修行が積まれ，世界が見えてくることにより，「無菌」パラダイムは「健康」パラダイムにシフトしていく。(§5.2.5.2「無菌」から「健康」へのパラダイムシフト)「無菌」パラダイムでは，菌の侵入を許した管理者はそのことで罪になる (謝罪しなければならない)。よって, 管理者は「無菌」を絶対にする。「健康」パラダイムでは，菌との共生にバランスをとることが管理の意味になる。管理者は，菌の侵入をもって罪になることはない。

要点：「無菌」パラダイムを絶対のものとしてはならない。このパラダイムは，組織 (の思想) の未熟を表しているに過ぎない。「無菌」パラダイムは，事件を起こさないために情報システムを使えなくする。これは，本末転倒である。

5.2.5「健康」パラダイムにシフト――「生活」の思想へ

5.2.5.1「健康づくり」の形

「コンピュータによる人支配」は，「管理主義の本末転倒」の一つである。本章では，「コンピュータによる人支配」の一つとして，セキュリティ主義 (セキュアであることを自己目的化する立場) を問題にしてきた。

ネット犯罪は多様であるが，最も情報ネットワークに特徴的な犯罪は「寄生虫感染症」の形をとる犯罪である。そこで,「感染症に強くなる健康づくり」が主題になる。

感染には，ユーザの行動に原因するものと，カラダの脆弱性に原因するものの２通りがある。このうち「健康づくり」で主題になるのは，カラダの脆弱性に原因する感染の方であり，そしてこの感染は，「プログラムの脆弱性がつけ込まれる」というものである。 (§5.2.2.3 寄生虫感染のりくつを知る)

よって,「感染症に強くなる健康づくり」の内容は ,「プログラムの脆弱な部分を直す」。そしてこれは，プログラムの開発元 (ベンダー) の仕事である。

よく「セキュリティ技術向上と犯罪技術向上のいたちごっこ」ということが言われるが,「プログラムの脆弱な部分を直す」は確実に進んでいく。「寄生虫感染症」タイプの犯罪は，「ユー

ザを騙して，寄生虫感染する行動をとらせる」の方に益々シフトせざるを得なくなる。

なお，「騙されて，寄生虫感染する行動をする」への対策は，寄生虫感染させるコードを，入り口でストップできるようにすること；中に入れてしまい寄生虫が発生しても，駆除できるようにすること。そしてこれをつくるのは，システムソフトウェアの開発元のサービス，あるいはユーザによる「ウィルスチェック・駆除ソフトのインストール」である。

5.2.5.2「無菌」から「健康」へのパラダイムシフト

システムのセキュリティ問題は，システムの出発とともには起こらない。システムが汚染されたところから始まる。

システムが成長し，犯罪の旨味が見えてきたところで，犯罪の標的になり，そしてセキュリティが問題化されるようになる。セキュリティが問題化されたときには，システムには既に犯罪が棲んでいる。すなわち，システムは汚染されている。

システムが単純で小さければ「システムの再構築」を汚染除去の方法とすることができるが，システムが大きくなると「システムの再構築」はあり得ないものになる。また，システムが大きくなれば，巧妙化する犯罪からそれを守ることは，ますます至難になる。結局，大きなシステムは汚染を抱え，汚染との共存を考えるものになる。セキュリティ対策は，「システムの汚染をいま以上にひどくしない」ないし「被害を治癒する」というようになる。また，前線を後退させて，より小さくより中心的な部分の防衛に目標を変える。システムの進化は汚染とのトレードオフである。システム一般に言えることとして，システムは無菌・無垢のままで大きくはなれない。(例：わたしたちの棲む社会——犯罪との共棲)

しかし，ここが重要な点であるが，このことは汚染に対するシステムの敗北/屈服を意味しない。システムは，汚染を自分の要素とするようになる。「汚染を取り除くと病気になってしまう」体に変わる。そのような形に＜進化＞する。

例 1: わたしたちの体 (菌や寄生生物との共棲) ——寄生は共生へと変わる＝菌や寄生生物を排除したら病気になる (例：アレルギー症)

例 2: わたしたちの棲む社会 (犯罪との共棲) ——犯罪の経済効果

そしてこのとき，システムに関する「セキュリティ＝無菌」問題は，「健康」問題に変わる。「無菌」のパラダイムは，「汚染・犯罪からの防衛」。「健康」のパラダイムは，「汚染・犯罪を自分の体内に取り込みそれと共生することで，かえって自分の生命力が改善される」というもの。

5.2.5.3「生活」の思想へ

生活は，便利とリスクのトレードオフであり，そしてパフォーマンスとコストのトレードオフである。安全は欲しいが，コストがかかる。ほどほどの安全で手を打って，後はリスクが来ないことを願う (運を天にまかせる)。

しかし，リスクをいつも考えていると，リスクに対しだんだん神経質になり，リスク回避 (安全) を最優先事項とするようになる。そして，生活を自ら不自由にしていく。

ネットワーク・セキュリティの方法は，「使用形態の限定」である。「使用形態の限定」は，ネットワークの自由な・創造的な使用をできなくするということである。

大学は，自由・創造本位でやってきた。自由・創造は，事故に対する隙が多い。このことに対し，「事故は自由・創造のコスト」と達観してきた。しかし，この達観の文化が，大学からいま急速に失われている/既に消えてしまった。「時代の流れ」を言い訳にする一方で「グローバル・スタンダード」で合理化を図る，コセコセした事なかれ主義の場になった。ネットワークのセキュリティ対策「使用形態の限定」は，この風潮と重なる。

> 註：一般に，事なかれ主義に対しては，これがつぎに「組織内部的にも性悪説の適用をする」へ発展することを警戒しなければならない。性善説 - 対 - 性悪説は，自由 - 対 - 統制のことである。「*ここは性悪説でやるしかない*」を簡単に言う風潮があるが，これは簡単に言わせてよいことばではない。

「ネットワーク・セキュリティ」は，何よりも先ず「哲学」の問題である。——それからずっと下って，技術の問題である。

大学は，インターネット黎明期の「自由・創造の気風」の記憶を持っている。この記憶をいま改めて呼び起こす必要がある。

5.2.6 一般ユーザ向け教材

「*ネットに接続するだけでウィルス感染*」と脅され，ウィルスチェックソフトを購入してコンピュータにインストール。基本ソフトにおいて，セキュリティ対策したバージョンへのアップデートを促すメッセージが突然コンピュータ画面に現れ，素直に「実行」をクリック。この辺りのりくつがわからないので，「セキュリティ」に関してはいつも宙ぶらりんな気持：

1. 「ネットでウィルス感染」とはどういうこと？
2. ロボットがする悪さとは？
3. ウィルス感染対策とは？
4. 自分のコンピュータがウィルス感染すると，被害は？
5. ウィルス感染はどの程度？

これが一般ユーザのいまの境遇であり，これでは不安ビジネスの言いなり (思うつぼ) になってしまう。よって「ネット接続でウィルス感染」のりくつのインストラクションが必要になる。

6 法令遵守主義

6.0 要旨

「法令遵守 (コンプライアンス)」を担当すると，「法令遵守」にのめり込む。周りを見なくなり，「法令遵守」一辺倒になる。他とのトレードオフを考えなくなる。「法令遵守」を「ゼロか

イチか」の問題にしてしまい，「イチでなければならない」の潔癖症を身につける。——これをここでは「法令遵守主義」と呼ぶことにする。

法令遵守主義は他とのトレードオフを考えないので，本末転倒をやる。すなわち，「法令遵守」に「生活」を従わせようとする。——生活において「法令遵守」は程度問題なのだが，「イチでなければならない」の潔癖症は (値がイチではない「不潔な」) 現実の生活を許さない。

法令遵守主義は，批判の対象とし，そして退けねばならない。

6.1 法令遵守主義の構造

6.1.1「法令遵守 / 説明責任」の理解・適用の混乱

「法令遵守 / 説明責任」は，どこから出てきたか？それは，「組織ぐるみ犯罪」から出てきた。1990 年代のアメリカで企業犯罪が相次ぐ状況があり，これをどうするかが問題になった。企業経営学はこの主題で盛り上がる。『OECD Principles of Corporate Governance』([3]) などが著される。そして，「法令遵守 / 説明責任」をビジネスにする企業も現れてくる。

この問題構造を正しく理解しないと，「法令遵守 / 説明責任」を組織の＜内部統制＞に使う間違いをやってしまう。特に，「法人化」の国立大学は，これに進む危険性が高い：

> *いま，時代の先端は「コーポレート・ガバナンス」だ！*
> *コーポレートたる国立大学法人は，これを取り入れるぞ！*
> *"compliance", "accountability", "disclosure", "risk-management" に，網羅的に取り組むのだ！*

組織における「不正 / 犯罪」は一様ではない。このことを理解していないと，「法令遵守 / 説明責任」の適用を誤ることになる。そこで，組織における「不正 / 犯罪」をカテゴリー分けして考える必要がある。あわせて，「不正 / 犯罪」と「失敗」を区別する必要がある。

このとき，つぎのようなカテゴリーが導かれる：

	犯罪	失敗
組織ぐるみ (上意下達)	上下—犯罪	上下—失敗
複数の者が，互いに独立あるいは集団心理でする (→ 組織風土が問われる)	風土—犯罪	風土—失敗
グループがする	グループ—犯罪	グループ—失敗
個人がする	個人—犯罪	個人—失敗

例 1. 記録管理の国際標準 ISO15489 は，「失敗」が適用対象である (「犯罪」ではない)。

例 2. 新潟大学・岡山大学の「ソフトウェアの大量不正コピー」は，「風土—犯罪」のカテゴリーに入る。

「グループ—犯罪」「個人—犯罪」は，組織の＜不運＞の問題である。この犯罪は，確率的に存在する。これには，処分 (あるいはさらに，矯正) で対処する。この犯罪を起こさないために＜内部統制＞的な措置を講ずるといったことは，やってはならない。——＜内部統制＞は，本末転倒である。

「風土—犯罪」には，処罰とモラル涵養 (啓蒙・教育) で対する。この場合も，犯罪を起こさないために＜内部統制＞的な措置を講ずるといったことは，やってはならない。——＜内部統制＞は，本末転倒である。管理の示威は，モラル涵養に逆行する。モラル涵養には，時間のかかるものもある。そして，時間がかかるものに対しては，必要な時間をかけるしかない。

「法令遵守・説明責任」は，「上下—犯罪」が適用対象である。また，「法令遵守・説明責任」は「上下—失敗」にも適用される。

「上下—犯罪」への対策が「法令遵守・説明責任」であるのは，なぜか？それは，ひとは「上意」と「一致団結」に抗えないからだ。「法令遵守・説明責任」は，組織のトップに照準が向けられている。この点を間違えてはならない。

重要：「法令遵守・説明責任」を＜内部統制＞の理由・方法として使うのは，論理として間違いである。

6.1.2 横並びが「内部統制」を競う形に

「法人化」の国立大学は，コーポレートの素人として，「先ずは形から入る」みたいに企業経営を真似し始めた。国立大学と営利企業の違いをきちんと考えることをやらねばならないのだが，営利企業がどんなのかそもそもよくわからないので，これはパスしてしまう。そして，この流れを固定化する要素の一つに，国立大学の横並びがある。(§4.1.2 横並び)

横並びでいま国立大学がのめり込んでいるものの一つに，「内部統制」がある。——これに至る過程は，つぎのようになる：

1. ある国立大学で，ある不正・犯罪が起こる。
2. 文科省が，各国立大学に「あなたのところも注意しなさい」の通達をする。
3. 別の国立大学が，(ほめられることをするつもりで，あるいは何か働きかけを受けて) 内部統制の規程を自分のところで制定する。
4. これを見たさらに別の国立大学が (自分もほめられることをしなければと思い) これを真似る。
5. (「*取り残されたらまずい*」の思いから) 真似の連鎖が起こって，すべての国立大学が内部統制の規程制定で横並びする。

例：ソフトウェアの中央管理 (「管理台帳」) 問題 (§4.4.3)

6.2 個人情報保護主義

6.2.0 要旨

個人情報保護法の成立後，これの遵守として生活の一部様式を 180 度転換することが起こっている。特徴的なものの一例は，使い物にならない「職員名簿」。住所・電話番号がないので，使い物にならない。しかしこんなものでも，個人情報保護法に従い，「取り扱い注意」となる。

「*以前の様式は大間違いだった。われわれはひどく愚かだっ*

た。」の総括があっての 180 度転換ではない。実際,「以前と今のどちらがまともか？」と問われたときのひとの答えは「以前」になる。しかし同時に，ひとは個人情報保護法遵守として以前の様式を 180 度転換することに躊躇しない。マスコミは個人情報保護失敗の摘発の先兵をやる。これは一体どういうことか？

これは，集団ヒステリーである。ひとはこの手のことをよくやる。これに対しては,「またやってるよ」くらいの感覚で応じておけばよいのだが，この集団ヒステリーがネットワーク管理をも取り込もうとする。

6.2.1『個人情報保護法』が独り歩きする土壌

2003 年 5 月 30 日に『個人情報保護法』([4]) が制定された。これの案が出てきたのは 2001 年だが，この法に言論の自由の危機を見た者たちが反対行動を起こした。城山三郎ががんばったこと，マスコミが概して後ろ向きであったことが，よく知られている。そのときは反対が効を奏して法案が引っ込んだように見えたが，再び現れて法になってしまった。

『個人情報保護法』の当初の理由づけ (建て前) は,「個人情報が無軌道に使われるのを防ぐ」。これに対しては，ある有力者や政治家を週刊誌ネタから守るためだろうと当時は言われた。そして，法の成立からしばらく経った今日，心配されていた悪用や弊害が拡がっている。法は独り歩きする。だから怖い。政治家や有力者を週刊誌ネタから守るみたいな乗りでやったことが, とんでもないことに及ぶ。これを城山らは警告したのだ。

ここで興味深いのは，トップが何かを言うより先に，ボトムの側で法遵守のポーズを勝手に競い合うということだ。例えば，名簿廃止や名簿を使い物にならない内容につくりかえることを，あちこちでやりはじめた。それをすることがいかにも進歩的あるという風に, 自慢気にこれを行う。学校現場だったら, イデオロギー的な閉鎖主義とマッチする。

よくよく認識しておかねばならないことは，日本が「言論の自由」「情報」の哲学の後進国であるということ。ことば狩りのように個人情報漏洩狩り (「個人情報保護」の意味拡大) が正義感・使命感をもって進められる，そんな精神風土なのだ。

しかもいまは,「理不尽な○○」「モンスター○○」の世の中。なんでもかんでも「個人情報漏洩」の言いがかりを受ける可能性がある。哲学のない学校だったら，試験の成績リストなんかも自ら引っ込めるだろう (しかも，いいことをしているつもりで)。

参考：北海道教育大学 ,『ホームページにおける保有個人情報の適切な取扱いについて (通知)』(2007-08-21) ([5])

6.2.2「個人情報保護」集団ヒステリーの内容

人の集団に関する事実として，集団的な「合理に対する思考停止と斉一行動」がある。これの説明概念として「集団心理 / 集団ヒステリー」が用いられる。 (§4.1.5 集団心理による斉一行動)

日本はいま,「個人情報保護」の集団ヒステリーに嵌っている。この場合の「合理に対する思考停止」は,「個人情報」を内容的に考えないということである。 ――「ゼロかイチか」にする。

新聞は，どうってことのない「個人情報」がどこかに流れたことも，鬼の首でもとったように報道する。「個人情報保護」は魔女狩りの集団ヒステリーと化し，どうってことのないものに対して「どうってことはない」とは，だれも言えない。 ――そんなことを言ったら，袋だたきに遭うという思いで，互いにすくみ合う。

各機関は,「個人情報保護」で失敗し新聞に書かれることに怯え,「*わたしのところは個人情報保護にこんなに熱心だ*」を表すことと,「個人情報」をガチガチに閉じこめること (＝情報として使い物にならなくすること) に腐心する。

使えない名簿，連絡網をやめたため緊急時に困る，不埒な人間の保護に使われる，といった不具合を見せつけられても，この集団ヒステリーは改まる気配がない。

情報システム管理にとっては,「個人情報保護」で失敗することよりも，この集団ヒステリーに嵌ることの方が，はるかに問題である。国立大学の場合であれば，先ず文科省が「個人情報保護」を国立大学に通達して, 自分のアリバイづくりをする。つぎにこれを受けた国立大学の中央部署が，下の部署に通達を回して，自分のアリバイづくりをする。情報システム管理の部署も，各機関および教職員個人に通達を出して，自分のアリバイづくりをする。この流れでは，一貫して,「個人情報」を内容的に考えることがされていない。関心は,「自分の立場の安全――責任問題を背負い込まない」の方にある。

このとき，つぎのことが危ぶまれてくる：

> それぞれの場所で，ガチガチに強固な防壁構築をする。
> この結果として, 情報システムが (ユーザ本位ではなく)
> 管理者本位のものになっていく。

教育には，評価の通知のように,「個人情報の共有」がある。共有の一員が，これを他に見せれば，これは「個人情報が外に流れた」になる。そして「個人情報保護」集団ヒステリーのもとでは，これは個人情報漏洩事件ということになり，当該教員の責任問題 / 処分問題になる。特に，教育に「web-based」を活用している場合などは，個人情報漏洩事件にされるかされないかは，偶然 (「運」) の問題である。

6.2.3 情報統制につながる危険

情報の扱いには危険が伴う。したがって，情報を扱うには哲学が要る。 (「勇気 / 蛮勇」ではなく「哲学」である。)

哲学のない者は，情報の扱いに対し事なかれ主義や「臭い物に蓋」のスタンスをとる。そして，これを偉いことのように勘違いして, このスタンスの指導に及ぶ。哲学の希薄な組織では, この指導に「右へ倣い」する。情報の扱いにビクつき，閉鎖主義に逃げ込む。

「個人情報保護」は，組織の統制につながる / 利用される危

険がある。情報の扱いには危険が伴う。失敗は必ず起こる。(ひとは，失敗を百パーセント防ぐようにコストをかけることは，しない / できない。) このとき，その失敗を理由にして，言論差し止めの処分をする，あるいは身分上の処分をするということが起こり得る。

もっとも，組織の長は，いちばんハラハラしていなければならない立場である。自分の失敗でなくとも，最終責任は自分にくる。この意味では最も気の毒な立場にいるわけだが，しかしそれゆえにこそ，人一倍「言論の自由」「情報」の哲学 (リスク管理の経営学ではない) を強固にしていなければならない立場でもある。

6.2.4「姑息」に流れることへの警戒

「個人情報保護」の問題は, 内容的に (すなわち, ケース・バイ・ケースで) 扱うことが必要である。しかし，いまの風潮は「ゼロかイチか」である。

自ら「ゼロかイチか」にして,「個人情報」の扱いにビクビクする。及び腰になる。そして,「全部保管庫に入れて鍵をかける」みたいな，おかしな方向に進む。あるいは,「扱いにくい形にする」という, 本質的でないやり方 (「姑息」) に流れる。

「姑息」とは，ウェブページでのレコード表示を例にすると，つぎのようなのを謂う：

- 100 個のレコードを表示する場合， 1 頁に全部を表示するとすぐにコピーされるので， 1 頁につき 10 個だけ表示する。(コピーに手間がかかることを見せて，コピーを諦めさせる。)
- 技術的に，コピー (テクストの取り出し) を困難にする。

これを,「合理的」と言わず，なぜ「姑息」と言うか？本来の目的である利便性をわざわざ壊す，という本末転倒をやっているからだ。 ——実際，ユーザ全体が不便を被る一方で，コピーしようとする者はどうあろうとコピーする。

世の中のことを見渡せば,「ゼロかイチか」の方が普通でないことがわかる。「ゼロかイチか」でやると, 全体が不便を被る。そこで,「＜けしからん＞は確率的に必ずある」から出発する。そして,「＜けしからん＞を無くす」ではなく,「＜けしからん＞が現れるその都度，それを叩く」を方法にする。——「＜けしからん＞は無くならないが，個別的に叩くことがこれを抑えるやり方になる」というスタンスである。

情報システム管理の主題になる「個人情報保護」にしても，これを方法にするしかない。

7 ネットワーク支配——言論・情報の統制

7.0 要旨

本論考の主題「コンピュータの人支配」の趣旨は，つぎのものである：

> 人の傾向性 (本質) が「コンピュータの人支配」をつくってしまう。 特に,「コンピュータの人支配」をつくるのは, 人の悪意ではなく，むしろ善意である。

本章では,「大学執行部のネットワーク支配——言論・情報の統制」を,「悪意ではなくむしろ善意」の視点で考察する。これは, 大学執行部のインテリジェンスが確かであるときには, 無用の論となる。そうでないときは，必要な論である。そして少なくとも，将来の心配に備えて用意しておくべき論である。

「大学執行部のネットワーク支配」の場合の「善意」は,「前衛主義・中央指導」のエリート主義の善意 (「独善」) である：

> 大学のネットワークを執行部に対する批判のメディアに使う者は，組織にとって有害である。このような者からネットワークを取り上げねばならない。よって，執行部がネットワークを支配する。

大学執行部のネットワーク支配は,「組織の中のコミュニケーションは，トリー型でなければならない」とする論によって合理化される：

> 大学のネットワークを使った組織横断的なコミュニケーションは，組織の秩序を破壊する。 組織内コミュニケーションは，上から下，下から上へと，トリー型に構成されたノードを伝って行わねばならない。 実際，これが無視されると，中央指導が成り立たなくなる。コミュニケーションのルールを無視する者から，ネットワークを取り上げねばならない。よって，執行部がネットワークを支配する。

また，大学執行部のネットワーク支配は,「大学のネットワークは民間の企業ネットワークと同じであり，大学執行部が経営戦略の立場からこれの意味・位置づけをあたえる」とする論によって合理化される：

> 大学のネットワークを執行部方針批判のメディアに使う者は, 自分の組織の「国益」を台無しにする者であり「非国民」である。このような者からネットワークを取り上げねばならない。よって，執行部がネットワークを支配する。

7.1「ネットワーク支配」

7.1.1「ネットワーク支配」とは何か？

「ネットワーク支配」とは，ネットワークの運用に「デモクラシー」がなくなることである。だれか独りの思いでネットーワークの運用が行われることである。そのだれかを,「支配者」と呼ぶ。

デモクラシーの存在しない体制では，組織がうまく保たれるか酷くなるかが，支配者の資質頼みになる。古代中国の正史の方法論 (「易姓革命」) では，よい支配者を「君主」，その資質を「徳」と謂う。

デモクラシー / 自由主義は,「独善」を科学することにより,

「君主の徳」の概念を退け，「支配者」を認めない。

国立大学でのネットワーク開始時・幼年期には，「情報」のことに比較的詳しい・関心の強い教員が，ネットワーク管理を担当した。この時期は，「ネットワークとは何ものか？」「ネットワークで何ができるか？」の問題意識がネットワーク運用を導く。ネットワークの試行錯誤的活用が奨励される。世の中はまだ，コンピュータを使わないと思えば使わないで済む時代である。よって，「支配」は問題にならない。

その後，ネットワークの使用が一般的になり，ネットワークが仕事のインフラになる。ネットワークは「管理」されるものになる。そして，「管理が支配に転じる」が，問題になってくる。実際，この期のネットワーク管理は，ネットワーク管理者兼務教員の「徳」を頼みにするものになっている。そしてこれは，既に「ネットワーク管理者のネットワーク支配」である。

「ネットワーク管理者兼務教員のネットワーク支配」の状況は，「大学執行部のネットワーク支配」へほんの一歩という危うい状況である。例えばつぎのことで，この「一歩」はすぐに実現する：

・教員がネットワーク管理者兼務から撤退
・ネットワーク管理のアウトソーシング

そこで，つぎの問題意識となる：

> 「ネットワーク管理者兼務教員のネットワーク支配」の時期のうちに，「デモクラシー」をつくらねばならない。この時期に「デモクラシー」をつくらねば，手遅れになる。

ここで誤解してならないのは，「デモクラシー」は＜規則＞ではないということだ。ものごとをよく知らない者は，規則や制度がソルーションだと思う。 そして，軽薄に考えた規則や制度で，組織をダメにする。

デモクラシーは＜カラダ＞である。この意味を理解するために，「教育」を考えてみるとよい。教育は，＜カラダ＞づくりとして社会成員をつくる。＜規則＞で「社会成員」を定めることが社会成員をつくる方法になるか？——ならない。

この＜カラダ＞はどのようにしてつくる？ ひとりひとりが努めてつぎのことを実践すること：

A.「直接制のネットワーク」

B.「ネット活用の利便」を考え，要求し，これに貢献する。

これが方法である。地味だが，これ以外にない。——ソルーションはつねに地味である。これがわからない者 / これにがまんできない者が，「改革」(規則づくり・制度替え) に走る。

7.1.2「ネットワーク支配」の判定項目

「ネットワーク支配」は，ネットワーク運用に関するデモクラシーの貫徹度で測られるところのものである。では，「デモクラシーの貫徹度」はどのようにとらえられるのか？

「デモクラシーの貫徹度」を考えるときは，形式に対し実質を区別する必要がある。例えば，「委員会運営になっている」は形式の話。「委員会運営だからデモクラシーだ」とはならない。実質とは，「運用」の中身のこと。

デモクラシーは，自由主義，科学と組みの概念である。＜不自由＞は＜自由制約＞であるから，デモクラシーに問題はないか？と考えを進める。しかもこのとき，＜自由制約＞の場合には，科学レベルの理由付けがなければならない，と考える。そこで，＜自由制約＞とその理由付けの現状が，「デモクラシー貫徹度」の実質の基準 (criteria) になる。

科学的理由付けでは，「ネットワークの意義」が要素になる。通常，＜自由制約＞は「ネットワークの意義」と「ネットワークの安全」の間のトレードオフという形で理由づけられる。——ここで，「ネットワークの意義」は，組織依存である。

以上のように概念枠組を設定したところで，「*国立大学を場とするネットワーク使用の＜自由制約＞と理由付けの現状*」の主題化へと進む。このとき，基準 (criteria) としてチェックしていくことになる＜自由制約＞には，可能性として，つぎのようなものがある：

・校内の情報コンセントが，鍵管理されている。
・講義室の情報システムが，鍵管理されている。
・IP アドレス取得が申告制であり，飛び入りで使えない。
・ソフトウェア使用が報告制になっている。中央管理される。
・ローカルサーバの導入が認可制であり，ハードルが高い。
・トラブルの受付窓口が不明。対応が不十分・不親切。
・情報システムの使用に関わる情報の提供が乏しい。説明不足。内容がユーザフレンドリーでない。ウェブベースになっていない。
・情報システムの運用・管理に関する情報の提供が乏しい。説明不足。内容がユーザフレンドリーでない。ウェブベースになっていない。

(以下は，民間の営利企業では「セキュリティ・ポリシー」の形でスタンダードになっているもの：)

・thin client (PC の仕様が特定の業務でしか使えないようになっている)
・アクセス制限がかけられている。
・アクセス履歴が検閲される。
・メールが検閲される。
・通信が検閲 (盗聴) される。

以上の項目を見てよくよく理解すべきは，「*ネットワーク管理を用いた＜言論・情報の統制＞は，いとも簡単*」ということである。 ——ゆえに，「ネットワーク管理」をつねに警戒的・批判的に主題化していかねばならないわけである。

7.2「大学執行部のネットワーク支配」

7.2.1「善意」のネットワーク支配

「コンピュータの人支配」を考察する本論考の趣旨は，「*統制の体制に向かわせるのは，人の悪意ではなくむしろ善意*」にある。そして「大学執行部のネットワーク支配」も，「人の悪意

ではなくむしろ善意が行う」ととらえるものになる。

それはどのような「善意」か？このときの「善意」は，エリート主義の善意（「独善」）である。実際，大学執行部に加わろうとするほどの者は，自分をエリートと見なしているわけなので，エリート主義の独善に嵌りやすい。しかも，国立大学には，伝統的に，前衛主義・中央指導のイデオロギーが色濃くあった。このイデオロギーにつく大学執行部が「法人化」の国立大学の執行部にそのままスライドすれば，「学長の強いリーダシップ」に前衛主義・中央指導がピッタリはまったトップダウン体制ができあがる。

一般論として，前衛主義・中央指導は，「大衆＝愚民」思想（「大衆は，中央が指導し従わせるべきもの」）であるので，一般組織員が指導部に向けて意味のある批判をすることはあり得ないものになる。一般組織員が中央を批判することは体制にとって有害であり，これは取り締まりの対象としなければならない。言論の抑圧へ。言論抑圧の最も効果的で直接的な方法は，言論メディアの支配である。——こうして，前衛主義・中央指導体制は，自ずと言論メディア支配に向かう。

この一般論を，いまの「法人化」の国立大学にあてはめてみる。前衛主義・中央指導体制にとって，自分を脅かす＜言論の自由＞の最も強力なメディアはネットワークである。これを支配すれば，批判は個人レベルで封じ込める。

「＜言論の自由＞のメディアとしてのネットワーク」というコンセプトは，国立大学に特徴的なものである。実際，民間の営利企業をはじめほとんどの機関のネットワークは，このコンセプトと無縁である（§1.1.1 国立大学と営利企業で「ネットワーク」の意義は異なる）。

なぜ国立大学では「言論の自由」なのか？それは大学が，自分が社会的価値をアウトプットする方法論を「自由」（「個の多様性，価値の多様性の解発 (release)」）に定めているからだ。

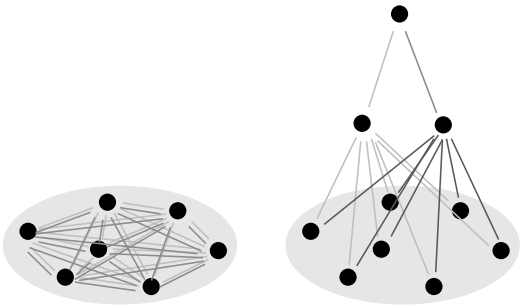
前衛主義・中央指導は，確信的に反自由主義である。そこで，「前衛主義・中央指導を体質とする大学執行部が起こり，ネットワーク支配に進む」事態を，警戒的・批判的に主題化することが必要になるわけである。

7.2.2 中央指導デモクラット

一般論として，中央指導の体制においては，トリー型指令系統を逸脱・無視するコミュニケーションは敵になる。それは，中央指導の秩序を乱し，体制破壊につながる。よって，共産主義国家が好例になるように，中央指導体制は自ずと系統逸脱的なコミュニケーションの排除に進む。この排除は，メディア管理と個別摘発の２面で行われる。

中央指導が嫌うのは，「直接制のネットワーク」。そして，中央指導が「かくあるべし」としているのは，「トリー・ネットワーク」。

中央指導を退けようとするものが，デモクラシーである。しかし，中央指導体制には，「学長の強力なリーダシップ」のトップダウン体制を実現した国立大学が例になるが，自分をデモクラシーに立つ者とみなすタイプのものがある。



直接制のネットワーク　　トリー・ネットワーク

このとき鍵になっているのが，「代議制」である。デモクラシーは，中央指導を退ける装置として，代議制を用いる。しかし，代議制も，「トリー・ネットワーク」を用いる。代議制のトリーと中央指導のトリーの違いは，僅かに意味付けの違いだ——ボトムアップとトップダウン。構造的に同じなので，ボトムアップは容易にトップダウンに変えられる。

このように，代議制というのはひじょうに危ういシステムなので，代議制を中央指導からガードするには，さらに装置が必要になる。これが，「直接制のネットワーク」だ。

件（くだん）の中央指導は，デモクラシーから「代議制」を形としてとり，デモクラシーのもう一つの要素の「直接制のネットワーク」を退ける。しかし，「代議制」をとっていることを以て，自分のことを「デモクラシーに付いている」とする。「直接制のネットワーク」を重要としないのは，彼らの前衛主義・エリート主義による：

「*正しく考えることのできる者が，代議員に選ばれてくる。*」
「*正しく考えることができれば，自分たちと同じになる（自分たちと同じでないのは，正しく考えることができないからである）。*」
「*正しいことを知りたければ，われわれに尋ねればよい。われわれがそれを教えてやろう。*」

この精神構造を，ここでは「中央指導デモクラット」と呼ぶことにする。

註：デモクラシーは，つぎの哲学を以て中央指導 / 執行部指導（前衛主義）を退けるところのものである：
「知は多数多様の個に存する。少数は，個の知（それが集まって形成する複雑系の知）を拾えない。よってつねに誤る（例：共産主義国家の計画経済）。」

中央指導デモクラットは，「組織秩序」の言い方で，「直接制のネットワーク」を排除しようとする。（中央指導の安定は，直接制の排除にかかっている！）

「直接制のネットワーク」排斥のメディア管理は，メディアが貧しい段階では成功する。しかし，今日，個人がコスト・レスでグローバルなコミュニケーションを展開できるメディアが，一般のものになってしまった。インターネットである。

「直接制のネットワーク」の立場では，インターネットが自由主義・デモクラシーを実現するためのインフラとしてことのほか重要なものになる。——実際，インターネットの登場で，反照的に，自由主義・デモクラシーがこれまで自身を実現するインフラを実は持っていなかったことがわかった。

こういうわけで，中央指導デモクラットによる「直接制のネットワーク」排除の行動は，自ずと「中央によるネットワーク支配」に進む。

以上の一般論は，「学長の強力なリーダシップ」のトップダウン体制を実現した国立大学にもあてはまる。 ——少なくとも，「あてはまる」を，警戒的・批判的に主題にする必要がある。

7.2.3「企業益・営業妨害」

営利企業では，内部から公然と経営陣批判が出てくることはない。（出てくることが許されるのは，匿名の内部告発。）経営陣批判は，つぎのようにリアクションされるものになる：

> 「*会社の長を批判して自分の会社を貶めること・自分の会社の営業を妨害することは，身内の者の行為として，あり得ない！*」

国の場合は，内部から公然と政権批判が出てくる。政権批判は，つぎのようにリアクションされるものとはならない：

> 「*国の長を批判して自分の国を貶めること・国益を損することは，国民の行為として，あり得ない！*」

この違いは何か？ 企業は，オーナーが提案するゲームである。ゲームの内容を承知して，このゲームに参加する。オーナーは，つぎのように言える：

> 「*気に入らないなら参加するな！ 他のところでゲームをさがせ！*」

国の場合，オーナーはいない。政権はオーナーではない。ゲームの一局を提案する役を委された者である。政権は，「気に入らないなら参加するな！ 他のところでゲームをさがせ！」は言えない。

政権の提案してくることは，危なっかしくてしょうがいない。政権も自分自身不安でしようがない。そこで，＜公然と行われる政権批判＞が求められる。

> 註：政権は「国益」ということばを使うが，本気で使っているとすれば，＜学問＞がないことになる。 実際，＜学問＞のある者は，「複雑」とか「塞翁が馬」というものを知っているので，ゲームの一局のことで「国益」ということばは使えない。

国の機関（含：国立大学）は，国と同じである。国の機関は，＜公然と行われる執行部批判＞を己の要件とする。

翻って，「大学執行部のネットワーク支配」が起こるときは，大学からこの見識が失せてしまっているときである。

7.3 教員が管理者を担うことの意義

7.3.1 教員兼管理者の意義

大学の精神的インフラは「自由主義」である。表向きの善悪論やイデオロギーから超然たろうとする自由主義である。

自由は，絶えず脅かされる。油断したり遠慮したりすると，たちまち自由の抑圧・蹂躙が起こる。

自由の抑圧・蹂躙は，＜善人＞が行うので始末が悪い。＜悪人＞が相手ならば反対するが，＜善人＞が行うので，遠慮・気遣いから自由の抑圧・蹂躙を容認することになる。自由抑圧の貌は，たいていつぎのものである：「組織の利益のため」

たいていの組織は，構成員が自分の組織を公然と批判することを，あり得ないものとする。せいぜい，「批判は，内に納めて外には出さないもの」と思い込んでいる。こうして，「組織の利益のため」が，自由を封じる。これを「全体主義」という。

こういうわけで，自由の保守は「全体主義」と闘うこととほぼ重なる。言論を封じようとする独裁者と闘うのではなく，「組織の利益のため」と闘うわけだ。

大学ネットワーク（情報システム）の管理の第一義は，情報的活動の自由（特に，言論の自由）の保守である。この意義がなければ，管理はだれにやらせてもよい。この意義があるから，管理者が問題になる。

大学ネットワークの管理をだれでもよいことにすると，大学執行部はネットワーク管理者を自分の系列に置いて，大学ネットワークを「組織の利益のため」のネットワークにしようとする。すなわち，ネットワーク上の情報的活動の自由を封じようとする。

> 註：「組織の利益のため」の名分に降った情報システムは，広報のシステムになる。

情報的活動の自由を封じるのは造作もないことで，単にネットワークを使い勝手の悪いものにすればよい。そして，現場を知らない / 現場から離れた者がネットワーク管理に就けば，ネットワークは使い勝手の悪いものになる。よって，ネットワーク上の情報的活動の自由を封じるには，事務局にネットワーク管理事務をおき，そしてそれがネットワーク管理をアウトソーシングすればよい。

＜自由＞は空気みたいなもので，それが手近にあるときは，それを保守している装置の存在に気づかない。失われるときに，それを保守していた装置があったことに気づく。——大学ネットワーク管理とは，このようなものだ。

大学ネットワークは，（特に国立大学の場合は）教員が管理者になって管理してきた。これには，自由の保守という意義がある。——そしてこれが「教員がネットワーク管理者」の最も大きな意義である。

大学ネットワークの管理は，「三権分立」的な意味合いから，大学執行部と分かれている必要がある。「三権分立」を崩そうとするのは＜悪人＞ではなく「組織の利益のため」を唱える＜善人＞であるということに，よくよく留意しよう。「うちは善人ばかりだから，大学ネットワークを執行部に委ねよう」をやっ

たら，たちまちにネットワークに自由がなくなる。

大学において，大学執行部に対し大学ネットワークを分権できる立場の者は，教員しかいない。教員兼ネットワーク管理者は，労働過重が問題にされるが，かといって現状では取り替えが効かない。

註１：「教員がネットワーク管理者」の意義には，もう一つ重要なものとして，「ネットワークの使用形態を知る者が担当」がある。 一般に，組織の業態を知らない者は，その組織のネットワーク管理者にはなれない。

註２：「ネットワーク管理者＝教員」は，人件費がケチられたことの犠牲者ではない。 多くの場合が，ボランティアである。

7.3.2 アウトソーシングは適さない

ネットワーク管理者教員の過重労働は，たいていつぎのような形で問題にされる：

「ネットワーク運用・管理のアウトソーシングがこれの解決策であり，そしてこの解決をはばんでいるのが人件費惜しみ」

しかし，ネットワーク（情報システム）運用･管理のアウトソーシングは，大学という組織には適さない。そして，アウトソーシングはネットワーク管理者教員を無くすものにもならない。なぜ？

ここしばらく，「人材の有効配置」の視点から，ネットワーク運用・管理のアウトソーシングが謳われてきた。しかし最近になって，アウトソーシングからの撤退の動きが，企業において顕著になってきた。つぎのことが，企業にわかってきた：

「アウトソーシングは，ネットワーク運用・管理を自分が行うことに代わるものではない」

実際，ネットワークの運用・管理は，システム（ハードウェアとソフトウェア）管理以上に，ユーザ（人）に対するサービスである。そして，その組織における＜サービス＞が何であるかは，その組織の者でなければわからない。

アウトソーシングでは，このサービスが失われる。また，外部者には，システム（ハードウェアとソフトウェア）の使い勝手がその組織においてどうであるかがわからない。そこで，たいてい，使い勝手の悪いシステムがトップダウンで降りてくる。

そして，サービスを失った組織はどうするか？身内の中にサービスを担当する者を改めてつくりはじめる。すなわち，コンピュータやネットワーク導入の時期に起こったことが，再現される：

コンピュータやネットワークを割と得意とする者に助力を求める；
彼らに助力を求めることが常習化する；
彼らにに親しい・疎いでサービスの違いが組織構成員の中に現れてくる；
サービスを公平にそして機械化するために，サービス部隊が望まれ結成される。

これが「アウトソーシング」というものの含意である。

おわりに

情報システム運用管理は，管理・統制の独り歩きに進む。管理･統制の独り歩きは，「コンピュータの人支配」をつくる。「コンピュータの人支配」は，人が自分の便利のためにつくった道具に支配される現象である。それは，「本末転倒・倒錯」の相で現れる。

「コンピュータの人支配」は，人の傾向性および組織の力学の自発運動である。人の傾向性および組織の力学の自発運動であるということは，各種「善意」がそれを進めているということである。「善意」が進めることなので，抵抗が起こりにくく，また起こしにくい。

「コンピュータの人支配」は，そうならないのがあたりまえというものではなく，そうなってしまうことが自然なのである。このような「コンピュータの人支配」を招かないためには，「コンピュータの人支配」を構造的に理解する必要がある。そして，「コンピュータの人支配」をさせない主体として立つための哲学を持つ必要がある。

この哲学の構想は，反照的に，「国立大学」という存在を立てている哲学を主題化する。その哲学は「自由」の哲学である。

本論考は，以上のことを主題化して，研究スキームの作成を試行した。これに続く課題は，実際にシステムに「自由」をデザインするという実践的課題である。そこでつぎは，「自由」をどのようにデザインするか / できるかの論考・試験研究を行う。

引用 / 参考文献

[1] 情報セキュリティ対策推進会議 / 官邸 , 2000-07-18 : 情報セキュリティポリシーに関するガイドライン , http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html

[2] Sophos, 2007-10 : "Dirty dozen" spam-relaying countries for Q3 2007, http://www.sophos.com/pressoffice/news/articles/2007/10/dirtydozoct07.html

[3] OECD, 1999 : OECD Principles of Corporate Governance, http://www.oecd.org/dataoecd/32/18/31557724.pdf (2004 edition)

[4] 2003-05-30 : 個人情報保護法 , http://www5.cao.go.jp/seikatsu/kojin/houritsu/

[5] 北海道教育大学 , 2007-08-21 : ホームページにおける保有個人情報の適切な取扱いについて（通知）, http://justice.iwa.hokkyodai.ac.jp/data/2007/08/21/