



組織におけるルール作りと 情報セキュリティ対策

2015年12月1日

株式会社 日本HP

個人情報保護対策室長

佐藤慶浩

自己紹介

佐藤 慶浩(さとう よしひろ)

株式会社 日本HP 個人情報保護対策室長

元 内閣参事官補佐・情報セキュリティ指導専門官(民間併任)

(内閣官房 情報セキュリティセンター)

【社外の活動】

IT総合戦略本部 パーソナルデータ検討会技術検討ワーキンググループ 構成員

経済産業省 個人情報保護ガイドライン検討委員会 委員

厚生労働省医療等分野における番号制度の活用等に関する研究会 構成員

杉並区 住基ネット運用監視委員会 委員長

世田谷区 情報公開・個人情報保護審議会 構成員

経済産業省 IT融合フォーラム パーソナルデータワーキンググループ 元構成員

JIPDEC プライバシーマーク運営要領改正委員会 元委員

JIPDEC ISMS適合性評価制度技術専門部会 委員

ISO/IEC JTC1/SC27 WG5 プライバシー小委員会 元主査、現エキスパート

情報ネットワーク法学会 元・副理事長

デジタル・フォレンジック研究会 理事

【その他】

<http://yoshihiro.com/profile/>

ルール作りとルール運用の基本

社員・職員を信じること

※企業以外の組織の場合、社員は職員と読み替えてください。

全員に当事者意識を持ってもらう

ルール遵守対象者全員の当事者意識が大切
対象者であれば正社員・正職員に限らず大切

日頃のコミュニケーションを大切にする

全員のコミュニケーションが大切
気づいたことを互いに声かけあえることが大切

目次

ルール作りと運用



大きな事故を防ぐためのアイデア
ルール作りの基本的考え方
ルールを守る環境作り

大きな事故を防ぐためのアイデア 社内情報セキュリティ対策への応用

参考

政府が情報セキュリティ対策統一基準を発行したときに、
用いたスローガン

情報セキュリティ対策は、
誰かがいつかどこかでやってくれることではなく、
全員がいつも各自の職場でやることです。

大きな事故を防ぐためのアイデア 街の治安：凶悪犯罪を防ぐための試み

(参考)

ブローケン・ウィンドウズ理論

Broken Windows Theory

March 1982, Atlantic Online

※一例であり、これを画一的に、あるいは一意に推奨するという
ことではありません。

(参考)

ブローケン・ウィンドウズ理論

第1段階

落書きが放置されていると罪悪感が薄れやすくなる

第2段階

軽犯罪が多発し治安が悪くなる

第3段階

警察の監視がないと判断され、より凶悪な犯罪者が寄り付く

第4段階

犯罪がエスカレートし凶悪犯罪が発生する

対策

(1)落書きを徹底的に消す

→警察や住民の監視があるというメッセージ

→軽い気持ちで罪を犯す人が減少する

(2)軽犯罪の取締りを強化する

→小さな犯罪も許さないという姿勢をアピール

→犯罪を起こそうと思う人間は近づかない

→凶悪犯罪は低減する

March 1982

Broken Windows

The police and neighborhood safety

by James Q. Wilson and George L. Kelling

In the mid-1970s The State of New Jersey announced a "Safe and Clean Neighborhoods Program," designed to improve the quality of community life in twenty-eight cities. As part of that program, the state provided money to help cities take police officers out of their patrol cars and assign them to walking beats. The governor and other state officials were enthusiastic about using foot patrol as a way of cutting crime, but many police chiefs were skeptical. Foot patrol, in their eyes, had been pretty much discredited. It reduced the mobility of the police, who thus had difficulty responding to citizen calls for service, and it weakened headquarters control over patrol officers.

Many police officers also disliked foot patrol, but for different reasons: it was hard work, it kept them outside on cold, rainy nights, and it reduced their chances for making a "good pinch." In some departments, assigning officers to foot patrol had been used as a form of punishment. And academic experts on policing doubted that foot patrol would have any impact on crime rates; it was, in the opinion of most, little more than a sop to public opinion. But since the state was paying for it, the local authorities were willing to go along

Five years after the program started, the Police

凶悪犯罪を未然に防止 することはできるか？

軽犯罪の取り締まりを強 化することで、結果的に、 凶悪犯罪の発生率が下 がる傾向になる。

情報セキュリティの大事 故を防ぐには、日々の軽 微な対策を全員が実施 することが必要。

大きな事故を防ぐためのアイデア 社内情報セキュリティ対策への応用

情報セキュリティに関する軽微なルール遵守を徹底する。

例)

社員証をいつも見えるように携帯・掲示する

機密文書にはすべて「機密」の明記をする

パソコンから離席時は短時間でも画面をロックする

など

→対策は毎日・全員で漏れなくやることだという意識

→対策に会社(全員)が注力しているのだという意識

目次

ルール作りと運用

大きな事故を防ぐためのアイデア



ルール作りの基本的考え方

ルールを守る環境作り

ルールとその運用： ガバナンス構築

達成目標の合意形成としての定義(HP社の参考事例)

1. 遵守事項(すべきこととしてはならないこと)を、会社がルールとして定めていること
2. 遵守事項を、会社が社員に対して教育していること
3. 遵守事項を、社員が理解していること
4. 遵守事項を遵守することについて、社員が同意していること
5. 社員による同意状況を、会社が把握していること

このとき、会社において、対象とする社員の範囲で、遵守事項のガバナンスが構築されている。

参考：遵守事項策定の際は、それが計測可能であることを原則としている。

→「達成目標の合意形成」は、「動機付けの交渉」(宍戸善一著「動機付けの仕組としての企業」より)に相当

ルール(規程)の策定

理解の促進→用語と文体

用語などの定義

組織内で通常用いている用語を使う

組織内で従来使っていない用語を安易に使わない

(法令順守や認証取得のために定義された用語に対応する必要があるならば、それらと組織内用語の対応表で対外的説明責任を果たすのがよい。それを逆向きにしない。)

主語の明確化

誰が実施することかを具体的に明記する

受動態の文章で書かない

日本語での留意事項

カタカナの使用の最小化

→避けられないカタカナ用語は丁寧に解説する

→専門用語を組織内教育でドヤ顔で説明するのは注意信号

ルール(規程)の策定

理解の促進→何を統一的に定めるか

文の種類の前定義

定義事項の文

遵守事項の文

必須行為 (employee Must Do: ~しなければならない)

推奨行為 (employee Should Do: ~することが望ましい)

禁止行為 (employee Must Not Do: ~してはならない)

許諾行為 (employee May Do: ~することができる)

支援義務 (company Must Do: ~する)

権限留保 (company May Do: ~する場合がある)

権限放棄 (company Never Do: ~することはない)



行為の限定
ではなく
理解の促進

決意表明と
事前通知

何を定める？ 最低水準 (baseline) と / か適正水準 (just enough)

ルール(規程)の策定

責任者の決定→逸脱手続き(WHO)

***ビジネスの例外を前提にする**

ビジネスの例外→情報システム使用の例外→情報セキュリティの例外

企業の場合の例)

初期値は、代表取締役社長＝経営的・法的な最高責任者

~~「例外を認めない」~~



「社長決裁をしなければならない」

責務の委任

経営資産＝人、物、金、情報

ルール(規程)の策定

ルールの個々の条項に記載すること

WHAT(,WHEN,WHERE):

何をすべきか(してはならないか)
(対策の手段の例示)

WHY:

なぜ、それをすべきか(してはならないか)
(受け入れられないリスクの考察)

WHO:

誰がそれをすべきか(してはならないか)
(受け入れるリスクの考察)

ルールの個々の条項で考えておくべきこと

HOW: その遵守状況の確認方法と確認基準

ルール(規程)の見直し

参考: 政府機関統一基準見直しの考え方

➤ 基準外要因の確認 (リスク分析をする。必要なら、対応として許容リスクも見直す。)

A. 政府内要件の変化への対応

- 情報セキュリティ対策に係る行政事務要件について、その目標達成のために統一基準改訂の必要があれば、改訂方法を決定する

B. 政府外環境の変化への対応

- 世の中で起きた事件事故についての検証 (政府機関内で発生したと仮定して以下の検証をする)
 - 原因が基準違反とならなければ改訂必要
 - 原因が基準違反となるならば改訂不要 (ただし、「遵守事項や解説見直し」の材料とする。)
- 周知された注意喚起についての検証
 - 基準で対応していない潜在的脅威について、顕在化の可能性が高まっていればリスク対応する

➤ 基準におけるすべての内容確認 (改訂で許容リスクを変化させないことを原則とする。)

C. 実務に則した遵守事項の見直し

- 運用に障害又は困難をきたす部分があれば、それを解消・軽減するための修正をする
 - 遵守事項の達成目標を変えずに表現(主語・述語・客体、条件等)を変更する
 - 遵守事項の達成目標を変える

D. 運用改善のための適用範囲・解説等の見直し

- 誤解のない表現の追加・修正

E. 文言の改善

- 表現漏れ、誤字脱字の修正

ルール(規程)の見直し

参考: 政府機関統一基準見直しの考え方

B. 政府外環境の変化への対応

- 世の中で起きた事件事故についての検証（政府機関内で発生したと仮定して以下の検証をする）
 - 原因が基準違反とならなければ改訂必要
 - 原因が基準違反となるならば改訂不要
(ただし、「遵守事項や解説見直し」の材料とする。)

ルール違反への対処

違反者には、謝罪させるのではなく、理由を説明してもらおう。

ガバナンスとしては、原因の特定を最優先する

特定した原因に基く再発防止策の検討

再発防止のための対策実施(周知・徹底以外に最低1つ)

HPにおける監査方針

違反については(始末書ではなく)理由書の提出

監査者は被監査者と絶対に敵対してはならない

監査者は支援者・助言者と認識されなければならない

ルール違反の発生は、ルール見直しの機会と考える。

ブロークンウィンドウズ理論からの教訓

軽微な違反の予防と再発防止を徹底する

ルール(規程)作りの基本的考え方

策定時の注意点:

- 社内用語を使うこと、慣れない用語・カタカナ用語を最少化すること
- 主語(誰が実施するのか)を明確にすること
- 述語(どの程度実施するのか)を明確にすること
- 例外発生を想定すること
- 実施可能なことに限ること → 事前合意が前提
- 性善説を前提とすること
- リスク許容レベル及び範囲の拡大傾向を想定すること

運用時の注意点:

- 実施状況の確認指標を明確にすること

見直し時の注意点:

- 見直し作業方針をあらかじめ定めること(方針も随時見直してもよい)

目次

ルール作りと運用

大きな事故を防ぐためのアイデア

ルール作りの基本的考え方



ルールを守る環境作り

ルールを守る環境作り 4つのチェックポイント

- ①性悪説だけでは組織は成り立たない
- ②性善説を前提とした対策
- ③権限を悪用できる機会を減らす
- ④善人を増やし、悪人を減らす環境

ルールを守る環境作り ①

性悪説だけでは組織は成り立たない

- ・ 性善説を前提にして、
- ・ 性悪説を想定する

※政府の情報セキュリティ政策会議のいう「事故前提社会」とは、「事故発生を想定」又は「事故対応を前提」の意で、「事故発生を前提」ではない。。。

ルールを守る環境作り ②

性善説を前提とした対策とは・・・

先に述べたガバナンスの構築が必要

1. 遵守事項(すべきこととしてはならないこと)を、会社がルールとして定めていること
2. 遵守事項を、会社が社員に対して教育していること
3. 遵守事項を、社員が理解していること
4. 遵守事項を遵守することについて、社員が同意していること
5. 社員による同意状況を、会社が把握していること

ルールを守る環境作り ②

性善説を前提とした対策・・・

守れるルールだけが、守られる。

実施できるルールだけを設けて、「ルールはすべて守るものである」という意識を定着させることが、結果的にルール遵守を定着させることができる。

できることの他に、できれば望ましいようなルールを混在させて、「必ずしも守らなくてもよいルールもある」という意識を持たれることは好ましくない。

遵守するための具体的な実施方法が明確になっていないルールを設けることは避ける。

**情報利活用の要求に即して保護との両立ができる
ルールを設けることが重要。**

ルールを守る環境作り ②

性善説を前提とした対策・・・

性善説を前提にして性悪説も想定する

性善説を前提とする。その上で、性悪説についても想定すると考えることが重要。

性善説であれば、「ルールは守られる」というところから検討し始めることができる。

ルールが破られるという性悪説への対策は、ルールを守っている性善説の人達によって実施するしかないことを忘れてはいけない。

ルールを守る環境作り ②

性善説を前提とした対策に、

性悪説を想定した対策を上乗せする。

- ・ 性善説を前提とした対策を実施している人達に担ってもらおう。
- ・ いかなる規則や教育も悪人には効果がない。
- ・ 悪人向け対策を担ってもらおう善人が不可欠。
- ・ 性善説を前提としない組織に非標準手順業務のリスク対応策の展開はあり得ない。

ルールを守る環境作り ③

権限を悪用できる機会を減らす：不正行為の類型

許可されていない者による不正行為（通称：外部犯）

・ 無許可の行為

悪意あり

— 技術面：アクセス制御による防御・多重の防御

許可された者による不正行為（通称：内部犯）

・ 誤操作・過失

悪意なし

— 誤操作を軽減する設計

— 啓発、教育、訓練

・ 権限の悪用

悪意なし

悪意あり

— 運用面：許可する権限の最少化

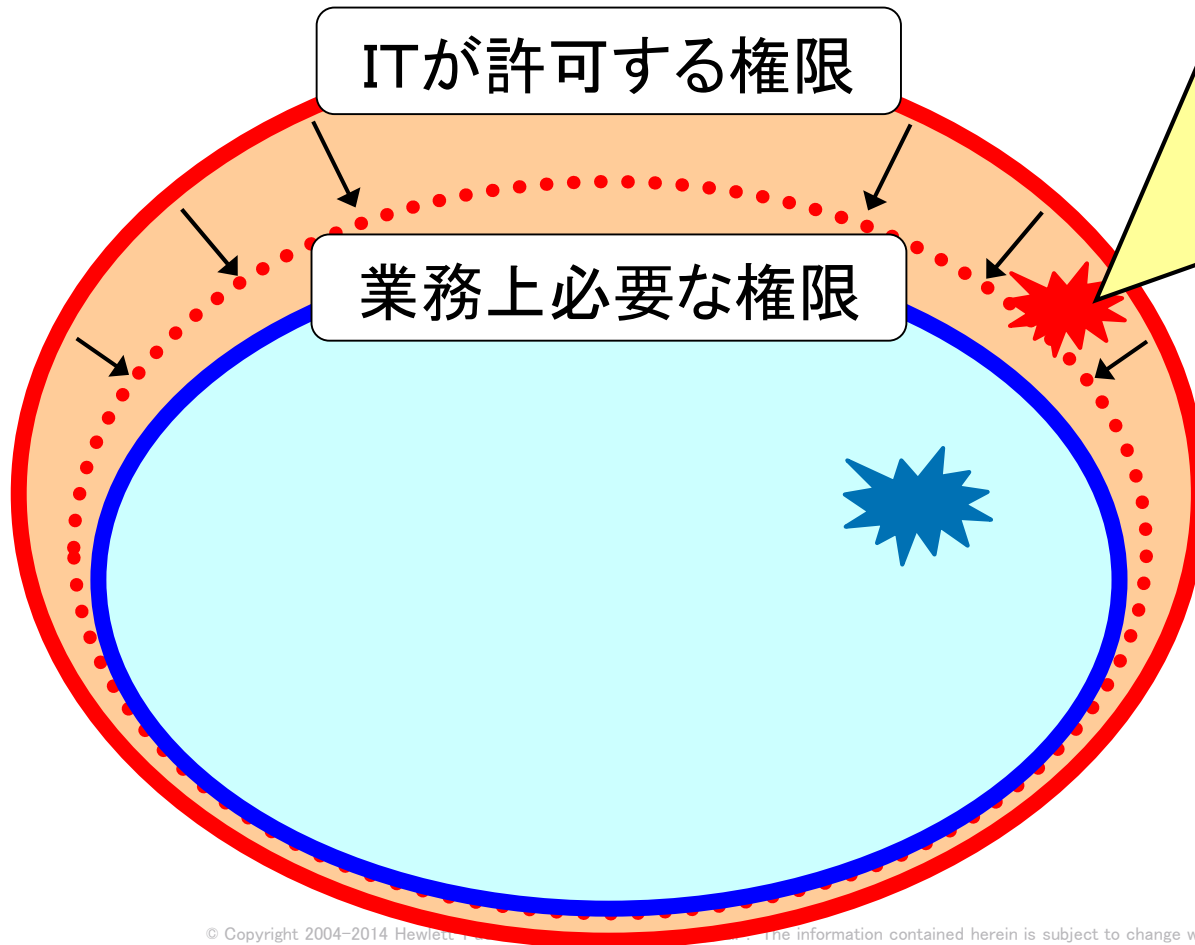
— 技術面：監視による抑止効果

27 — 技術面：アノマリ・アクセス（非通常行動）の検出



ルールを守る環境作り ③ 権限を悪用できる機会を減らす

許可する権限の最小化



不必要な権限
を最小化する



5W1Hの観点

で検証:

誰が?

何を?

いつ?

どこで?

どんな目的で?

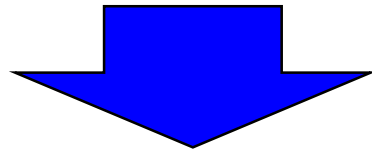
どういう方法

で?

ルールを守る環境作り ④ 善人を増やし、悪人を減らす環境

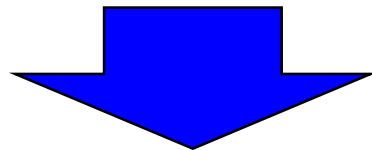
性悪説だけでは組織は成り立たない

- ・ 性善説を前提にして、
- ・ 性悪説を想定する



悪人を減らし、善人を増やす環境

- ・ 基本は「正直者がバカをみない」環境



善人が増えれば・・・権限委譲できる

ルールを守る環境作り 4つのチェックポイント

- ①性悪説だけでは組織は成り立たない
- ②性善説を前提とした対策
- ③権限を悪用できる機会を減らす
- ④善人を増やし、悪人を減らす環境

「正直者がバカをみない」環境

参考書籍

「不確実性のマネジメント」

Managing Unexpected

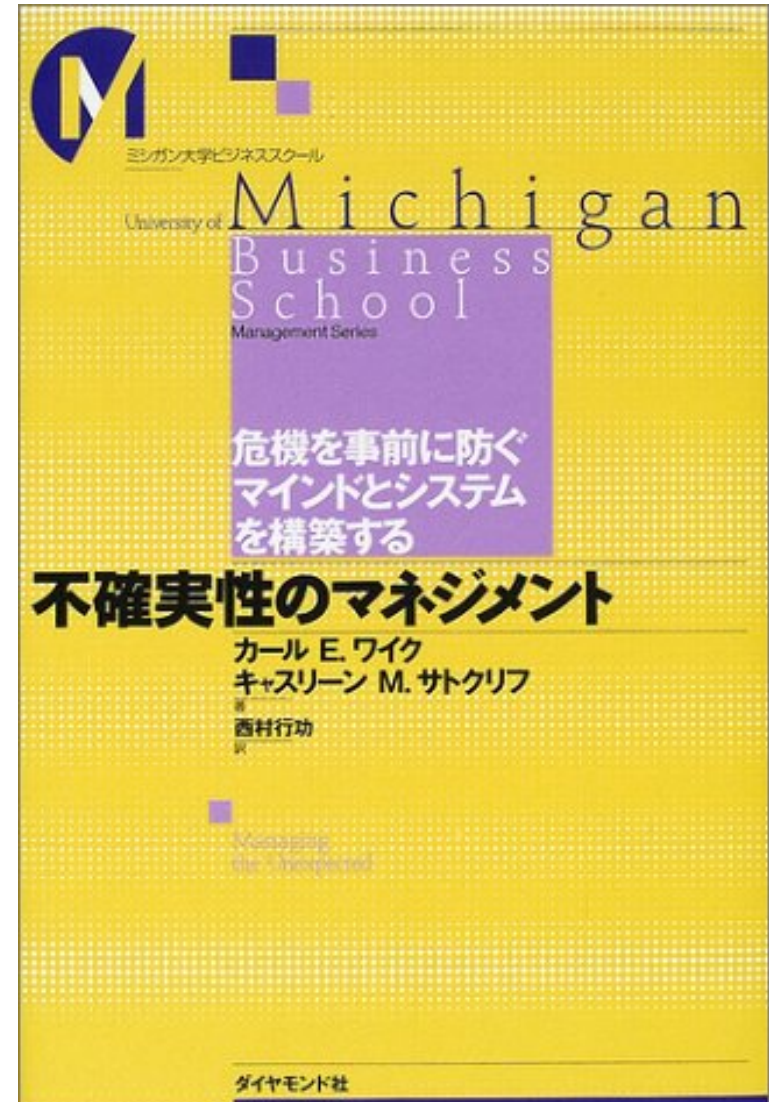
カール E. ワイク著

キーワード:

・HRO (High Reliability Organization)

高信頼性組織

・マインドフル



(参考)

ITアーキテクトによるセキュリティ設計



Security & Trust

<http://www.atmarkit.co.jp/fsecurity/special/48arc/arc01.html>

【特集】 つぎはぎシステムを防ぐセキュリティアーキテクチャ

- SLAに見るセキュリティの位置付け
- セキュリティ要件の5つのA（真正確認、アクセス制御、権限管理、監査、保証）
- アイデンティティ・マネジメント
- プロビジョニング

※経済産業省個人情報保護法ガイドライン第20条の補足説明としても有用な解説になっています。

(参考)

営業秘密 ～営業秘密を守り活用する～

経済産業省 <http://www.meti.go.jp/>

不正競争防止法

営業秘密管理指針

－参考資料 1：営業秘密管理チェックシート

トップページ > 政策別に探す > 経済産業 > 知的財産の適切な保護 >
知的財産政策／不正競争防止

<http://www.meti.go.jp/policy/economy/chizai/chiteki/index.html>

> 主要施策 | 営業秘密

(参考)

中小企業向け情報セキュリティ対策

IPA(情報処理推進機構)<http://www.ipa.go.jp/>

- 5分でできる！ 自社診断パンフレット

- 5分でできる！ 自社診断シート

<http://www.ipa.go.jp/security/manager/know/sme-guide/index.html>

(参考)

コストをかけずにできるセキュリティ対策

常識として知っておきたい個人情報保護法

第5回:コストをかけずにできるセキュリティ対策

<http://thinkit.co.jp/free/article/0606/1/5/>

政府:内閣官房情報セキュリティセンター

政府機関の情報セキュリティ対策のための統一基準

<http://www.nisc.go.jp/active/general/kijun01.html>

政府機関統一基準適用個別マニュアル群

DM6-05:府省庁支給以外の情報システムによる情報処理の手

順書 PC編 策定手引書

<http://www.nisc.go.jp/active/general/pdf/dm6-05->

101_manual.pdf



目次

ルール作りと運用

大きな事故を防ぐためのアイデア

ルール作りの基本的考え方

ルールを守る環境作り

リスクの傾向

回避しないリスクは減らない

性善説を前提にして、性悪説を想定する。

- × 事故前提
- 事故想定 又は 事故対応前提

悪いことができないようにする。→しかし、完全に防ぐことはできない。

悪いことができないように努める。

加えて、以下のことを予防する。

「悪いことだと知らなかった。」を防ぐ。→禁止事項

「悪いことだと思わなかった。」を防ぐ。→禁止目的

「悪いことだと知っていたが、ばれるとは思わなかった。」→記録保全

悪いことをすればできるが、やったらばれる仕組み作り。

総じて、周知・教育・訓練が重要。

ルール作りとルール運用の基本

社員・職員を信じること

※企業以外の組織の場合、社員は職員と読み替えてください。

全員に当事者意識を持ってもらう

ルール遵守対象者全員の当事者意識が大切
対象者であれば正社員・正職員に限らず大切

日頃のコミュニケーションを大切にする

全員のコミュニケーションが大切
気づいたことを互いに声かけあえることが大切



発表の録音と資料のダウンロード

<http://よしひろ.com/>



お問い合わせ

[http:// **twitter**com/4416sato](http://twitter.com/4416sato)

