セキュリティマネジメント実践により**組織の活性化**を図る！

富士通株式会社
サイバーセキュリティ事業戦略本部
丹野　隆志

目　次

0.はじめに

0.はじめに

ある偉人の言葉

愚者は過去を語り、
賢者は現在を語り、
狂者は未来を語る。

0.はじめに

約200年前

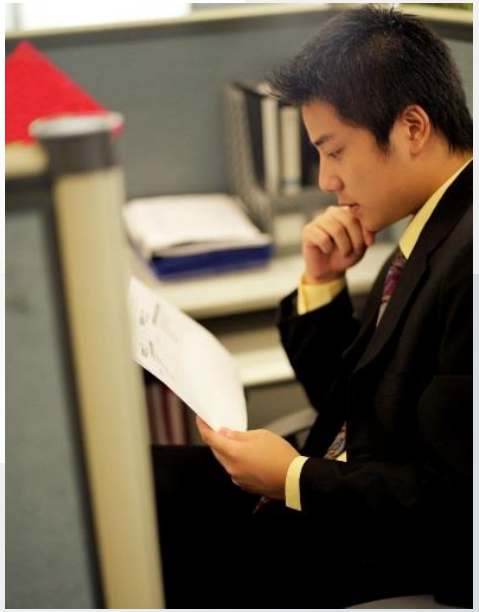
ナポレオン・ボナパルト

1769年8月15日 ～ 1821年5月5日

0.はじめに

現代

そして、今、現代の組織では・・・。



0.はじめに

現代

情報セキュリティマネジメントには

過去を振り返り、

現在を洞察し、

未来を築く

仕組みが求められている

0.はじめに

現代

この仕組みには、
①**マネジメントプロセス**
②**組織構成員**
が**両輪**となることが
求められる。

0.はじめに

現代

さて、多くの組織では・・・。

0.はじめに

現代

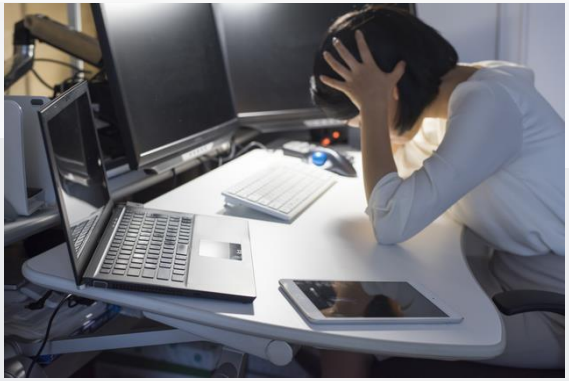
仕組みの両輪となる

組織構成員は**ヒト・・**。

0.はじめに

現代

最近の**組織構成員**は
セキュリティマネジメントで
疲弊してはいないだろうか？



0.はじめに

現代

既に多くの**組織構成員**は
日常業務で**疲弊**している

成果評価制度
コンピテンシー評価制度
終身雇用制度の崩壊

0.はじめに

現代

日常のセキュリティマネジメント
対応について多くの組織は
業務評価指標としていない

1.サイバーセキュリティの現状

1.サイバーセキュリティの現状

最近のサイバーセキュリティの現状の一部について整理してみると・・・

1.サイバーセキュリティの現状

■「情報セキュリティ10大脅威 2017」

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル欠如に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT機器の不適切な管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

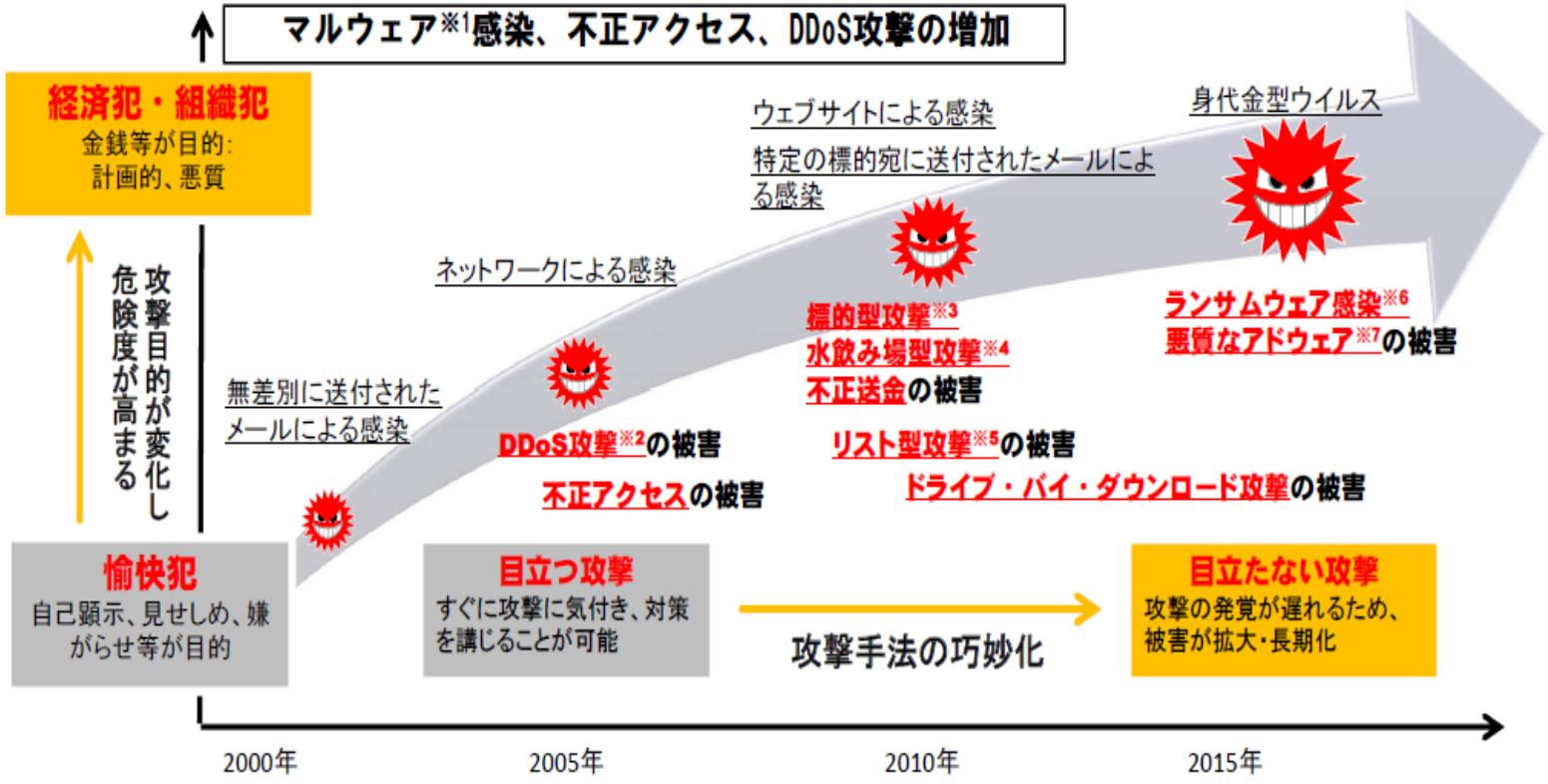
出典元：情報処理推進機構(IPA)サイトより

1.サイバーセキュリティの現状

サイバーセキュリティ上の脅威の増大

1

インターネット等の情報通信技術は社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、サイバーセキュリティ上の脅威が悪質化・巧妙化し、その被害が深刻化。



出展元：サイバーセキュリティの現状と総務省の対応について　平成29年1月

1.サイバーセキュリティの現状

出典元：情報処理推進機構(IPA)サイトより

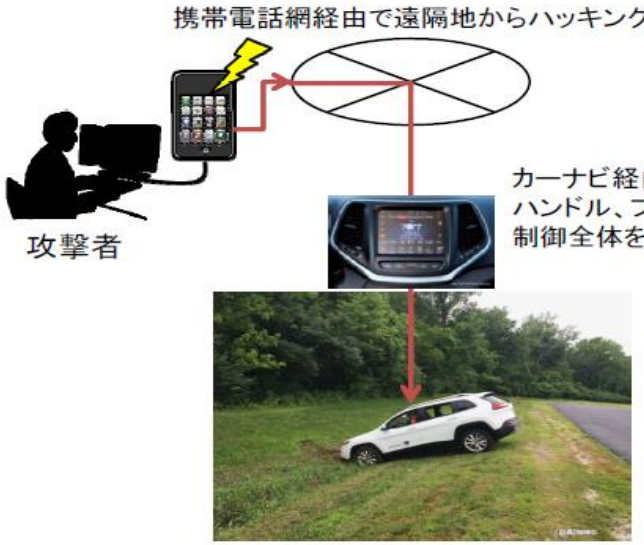
1.サイバーセキュリティの現状

IoTセキュリティ対策の必要性について

6

IoTでは、これまで接続されていなかった自動車やカメラなどの機器が、WiFiや携帯電話網などを介してインターネットに接続されることにより、新たな脅威が発生し、それに対するセキュリティ対策が必要となった。

自動車へのハッキングによる遠隔操作



人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

監視カメラの映像がインターネット上に公開

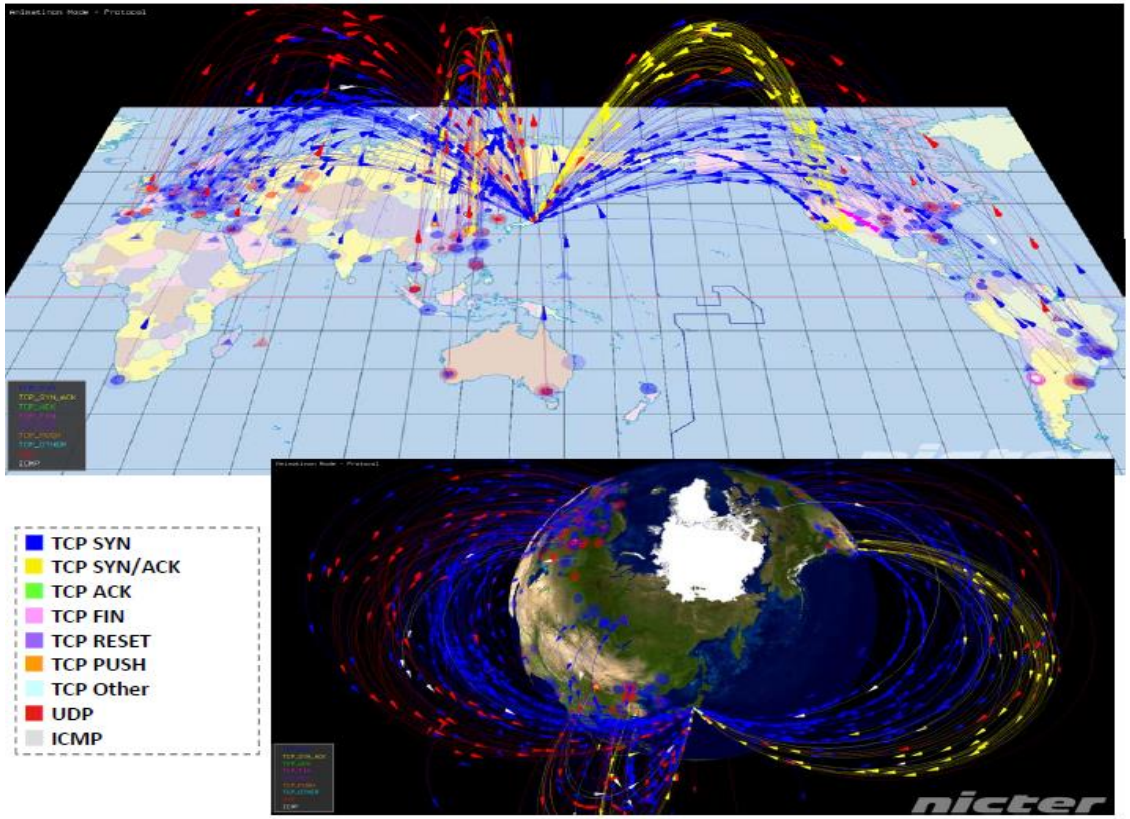
セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**。
（ID, パスワードなどの初期設定が必要）

出展元：サイバーセキュリティの現状と総務省の対応について　平成29年1月

1.サイバーセキュリティの現状

サイバー攻撃の状況 （NICTERによる観測）

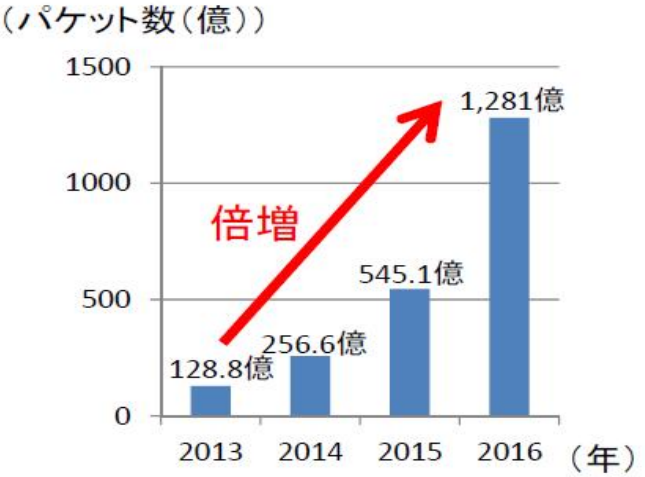
➢ 国立研究開発法人 情報通信研究機構（NICT）では、未使用のIPアドレスブロック30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測。



・ダークネットに飛来するパケットの送信元アドレスから緯度・経度を推定し、世界地図上で可視化

・色：パケットごとにプロトコル等を表現

１年間で観測されたサイバー攻撃回数



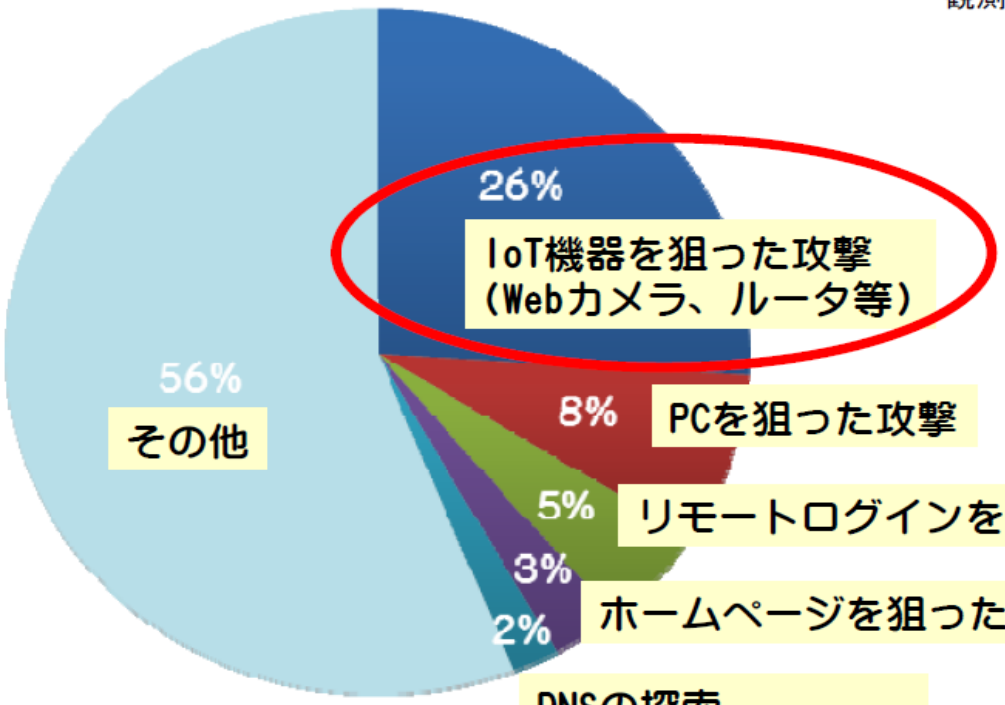
出展元：サイバーセキュリティの現状と総務省の対応について　平成29年1月

1.サイバーセキュリティの現状

NICTで観測されたサイバー攻撃の対象

4

観測したサイバー攻撃の内訳（2015年）

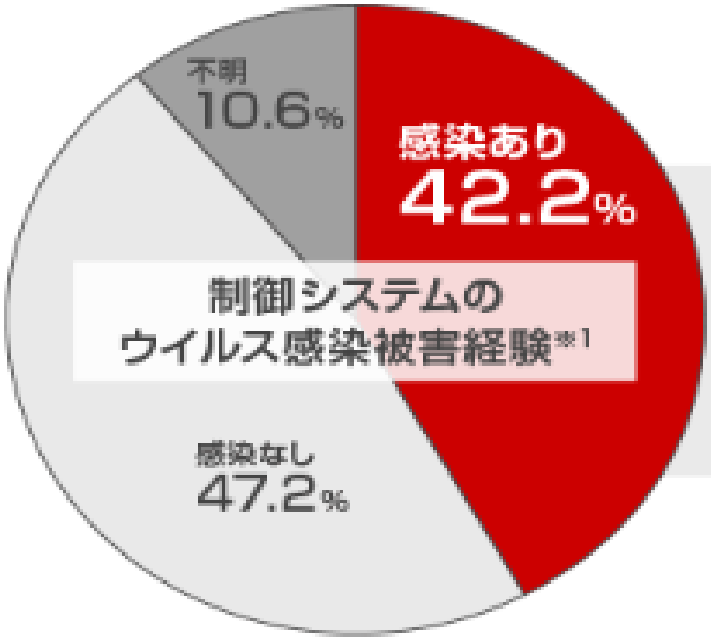


観測された全サイバー攻撃545.1億パケットのうち、

1/4がIoTを狙っている！

出展元：サイバーセキュリティの現状と総務省の対応について　平成29年1月

1.サイバーセキュリティの現状



ウイルス感染経験者の

55.4% 稼働停止※2

停止期間6日以上のケースも

出典：2014年9月 トレンドマイクロ調べ

FA/PA系制御システムの管理に関わりのある人218名にインターネット調査を実施

※1 設問：お勤め先において、あなたが管理するFA/PA系産業制御システムがコンピュータウイルス感染の被害にあった事はありますか？(N=218)

※2 設問：その被害の結果として、あなたが管理するFA/PA系産業制御システムが稼働停止に至ったことはありますか？稼働停止に至ったことがある場合、その期間についてお答えください。(N=92)

日本における制御システムの被害実態（図１）

出展元： trendmicroサイトより

1.サイバーセキュリティの現状

これらは、サイバーセキュリティにおける現状の一例にしか過ぎない

1.サイバーセキュリティの現状

そして・・・
セキュリティリスクの範囲拡大に関わらず、組織構成員の業務負担は
変化しないか**増大**している

1.サイバーセキュリティの現状

終身雇用制度の崩壊
成果評価制度
コンピテンシー評価制度
IT化に伴う効率化等・・・

1.サイバーセキュリティの現状

組織で生き残るためには
目標達成が最優先・・・

1.サイバーセキュリティの現状

直接、業務成果として
評価されないセキュリティ
マネジメントは、**ストレス**
以外の何者でもない。

1.サイバーセキュリティの現状

・・・・と、感じている組織構成員は少なくないのではないだろうか？

2.情報セキュリティインシデント傾向

2.情報セキュリティインシデント傾向

表 4-2：インシデント・トップ 10

No.	漏えい人数	業種	原因
1	679 万人	生活関連サービス業，娯楽業	ワーム・ウイルス
2	98 万人	情報通信業	不正アクセス
3	81 万人	電気・ガス・熱供給・水道業	紛失・置忘れ
4	64 万人	情報通信業	不正アクセス
5	58 万 9463 人	情報通信業	不正アクセス
6	42 万 8138 人	情報通信業	不正アクセス
7	42 万 1313 人	卸売業，小売業	不正アクセス
8	35 万人	生活関連サービス業，娯楽業	不正アクセス
9	21 万 9025 人	卸売業，小売業	不正アクセス
10	21 万人	電気・ガス・熱供給・水道業	管理ミス

出展元： JNSA 2016年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～より

2.情報セキュリティインシデント傾向

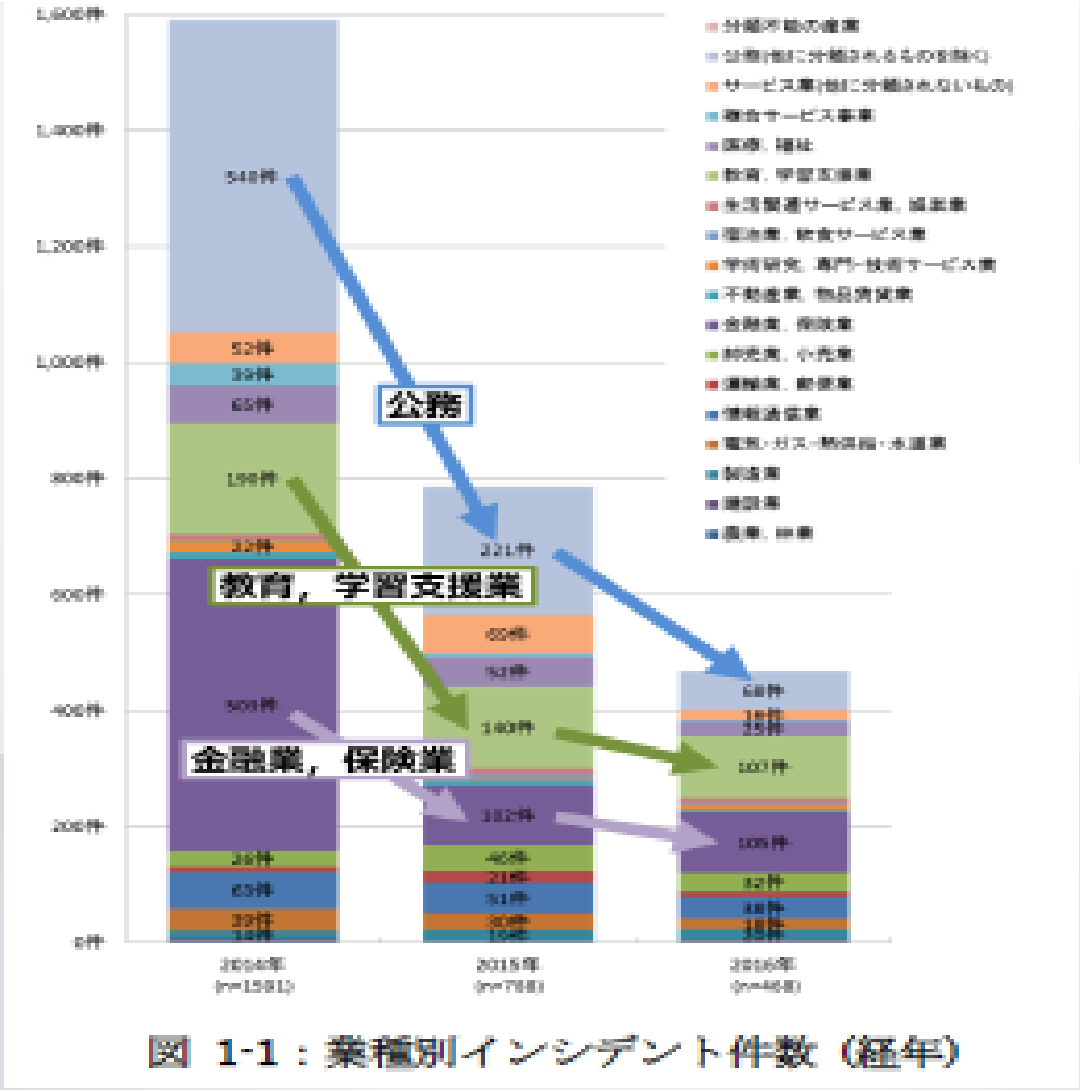


図 1-1：業種別インシデント件数（経年）

出展元： JNSA 2016年 情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編～より

2.情報セキュリティインシデント傾向

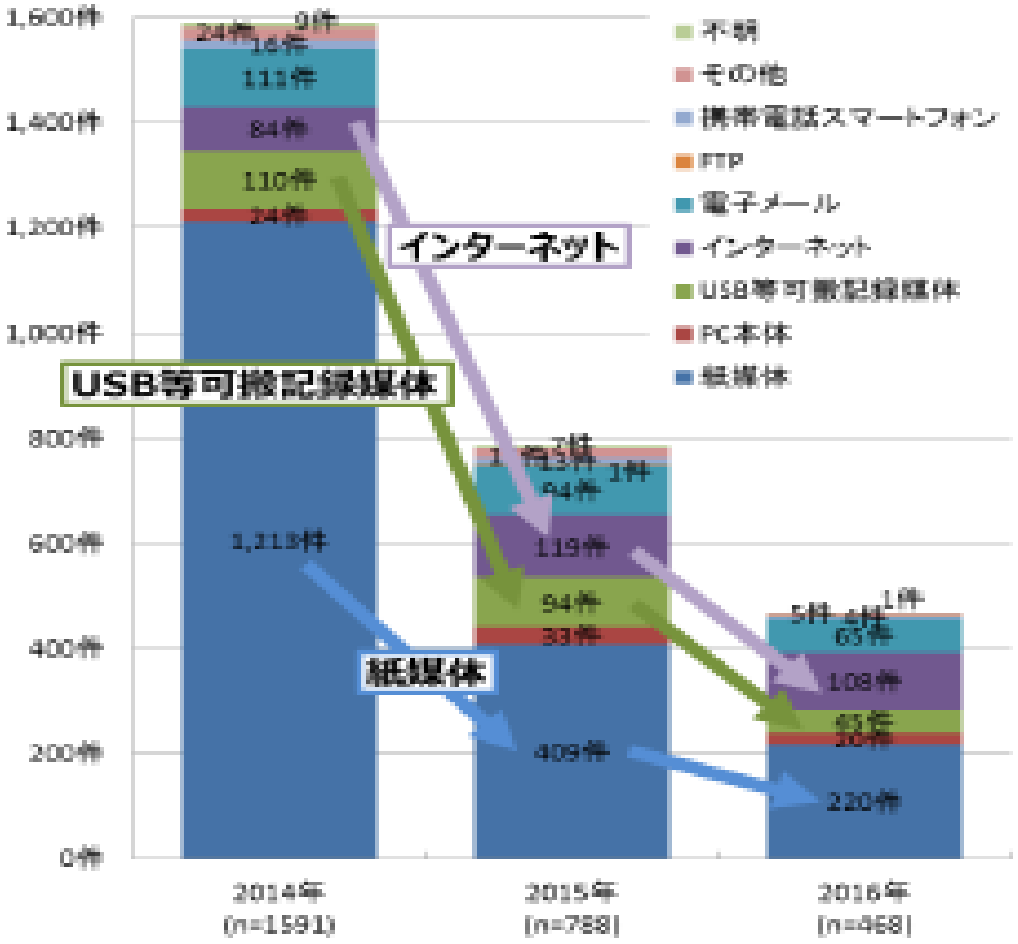


図 1-2：漏えい経路別インシデント件数（経年）

出展元： JNSA 2016年 情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編～より

2.情報セキュリティインシデント傾向

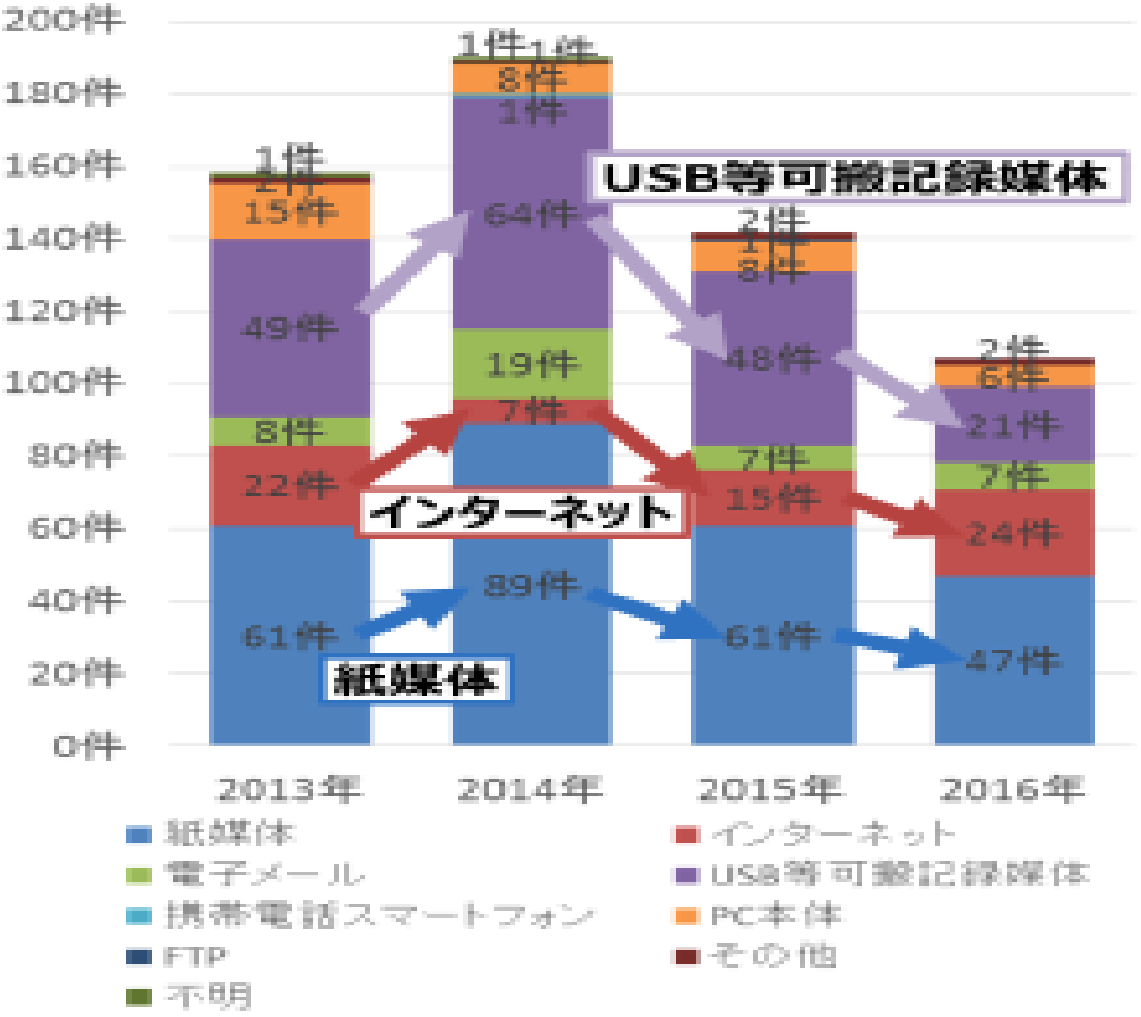


図 1-3：教育，学習支援業の漏えい経路(経年)

出展元： JNSA 2016年 情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編～より

2.情報セキュリティインシデント傾向

(1) 単年分析(件数)

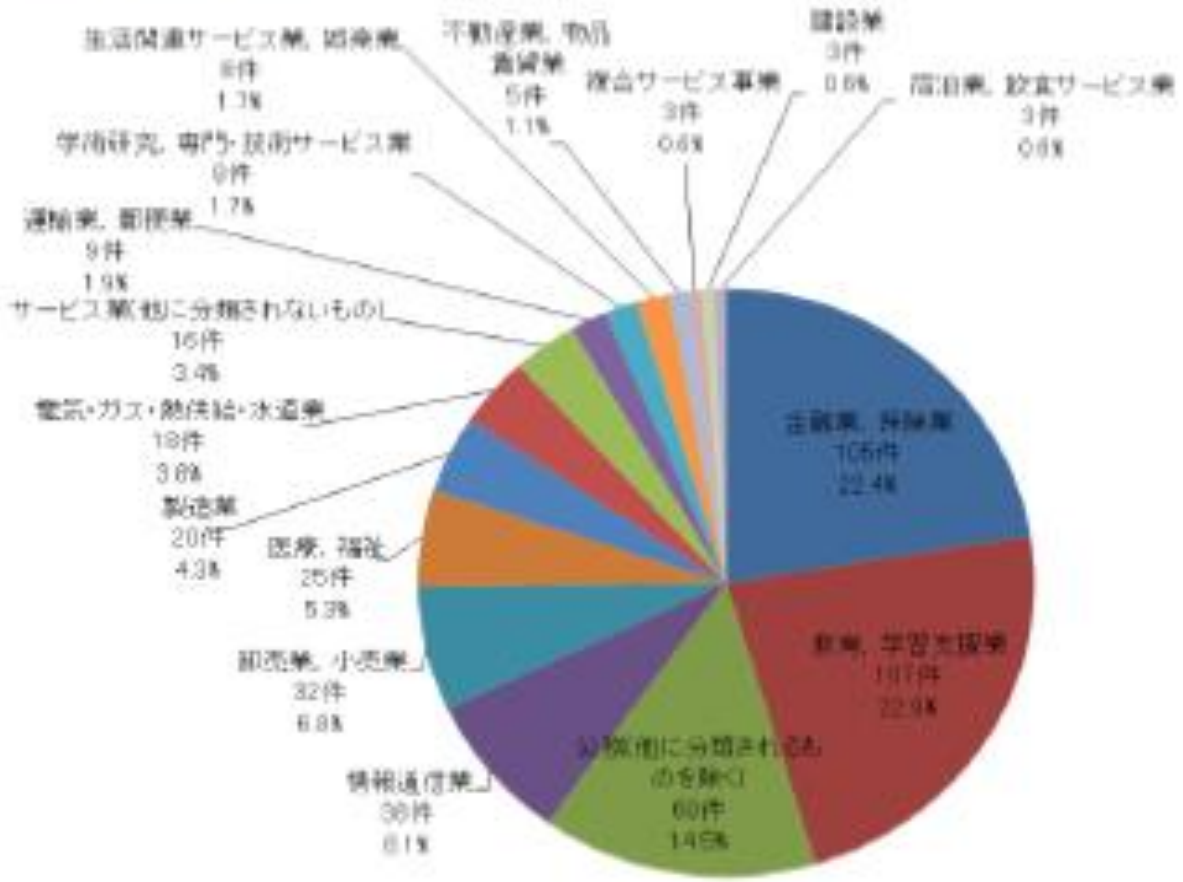


図 4-1：業種別比率（件数）

出展元： JNSA 2016年 情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編～より

2.情報セキュリティインシデント傾向

(1)　単年分析(件数)

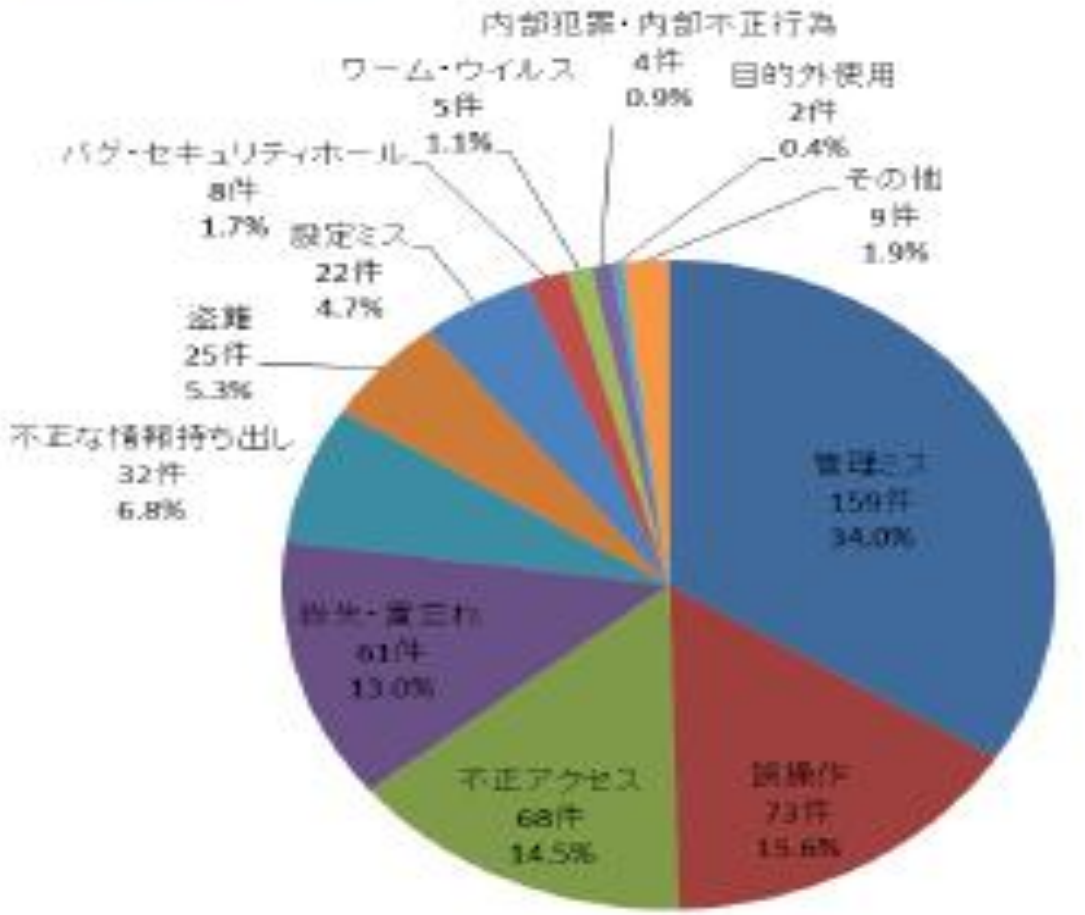


図 4-8：漏えい原因比率（件数）

出展元： JNSA 2016年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～より

2.情報セキュリティインシデント傾向

(3)　単年分析(人数)

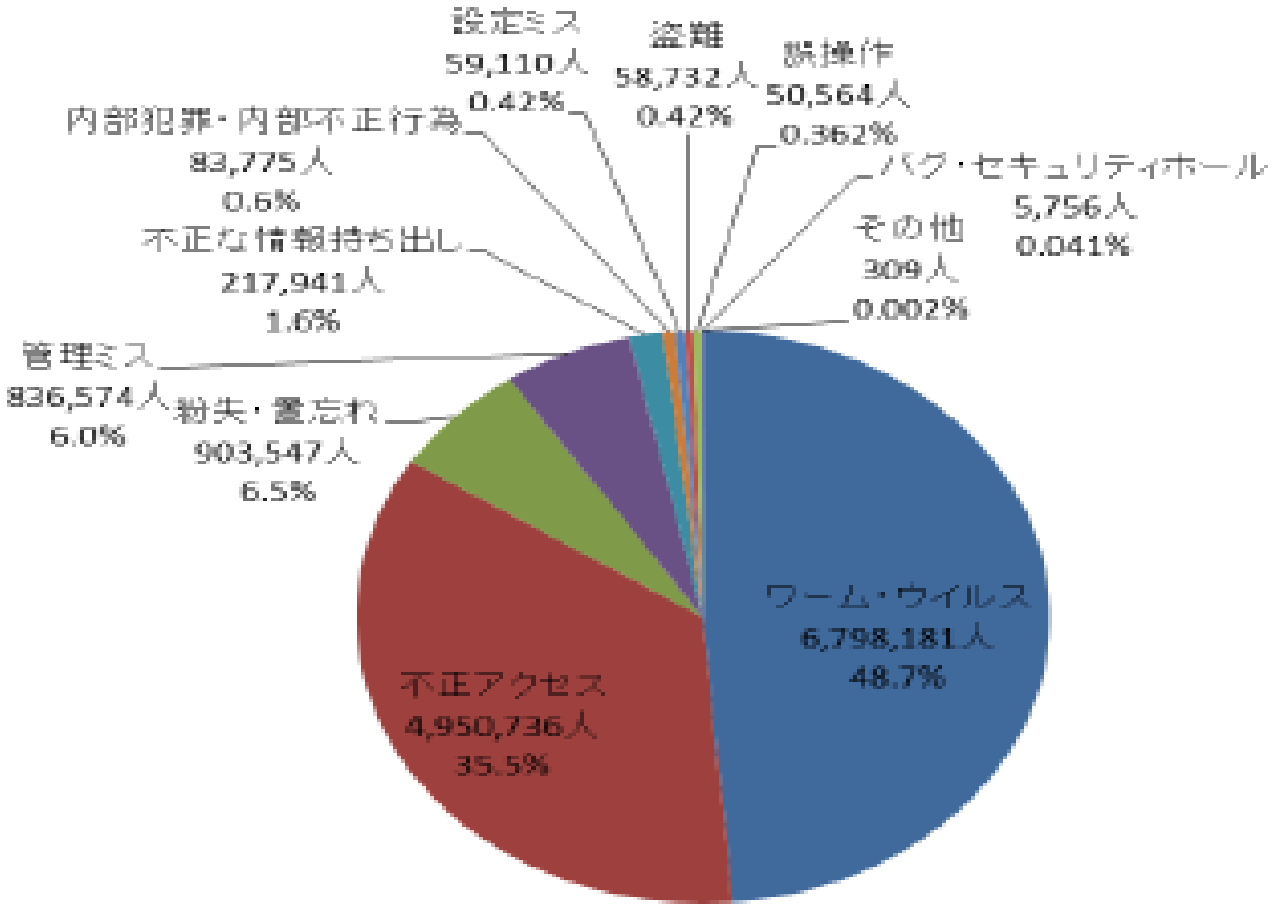


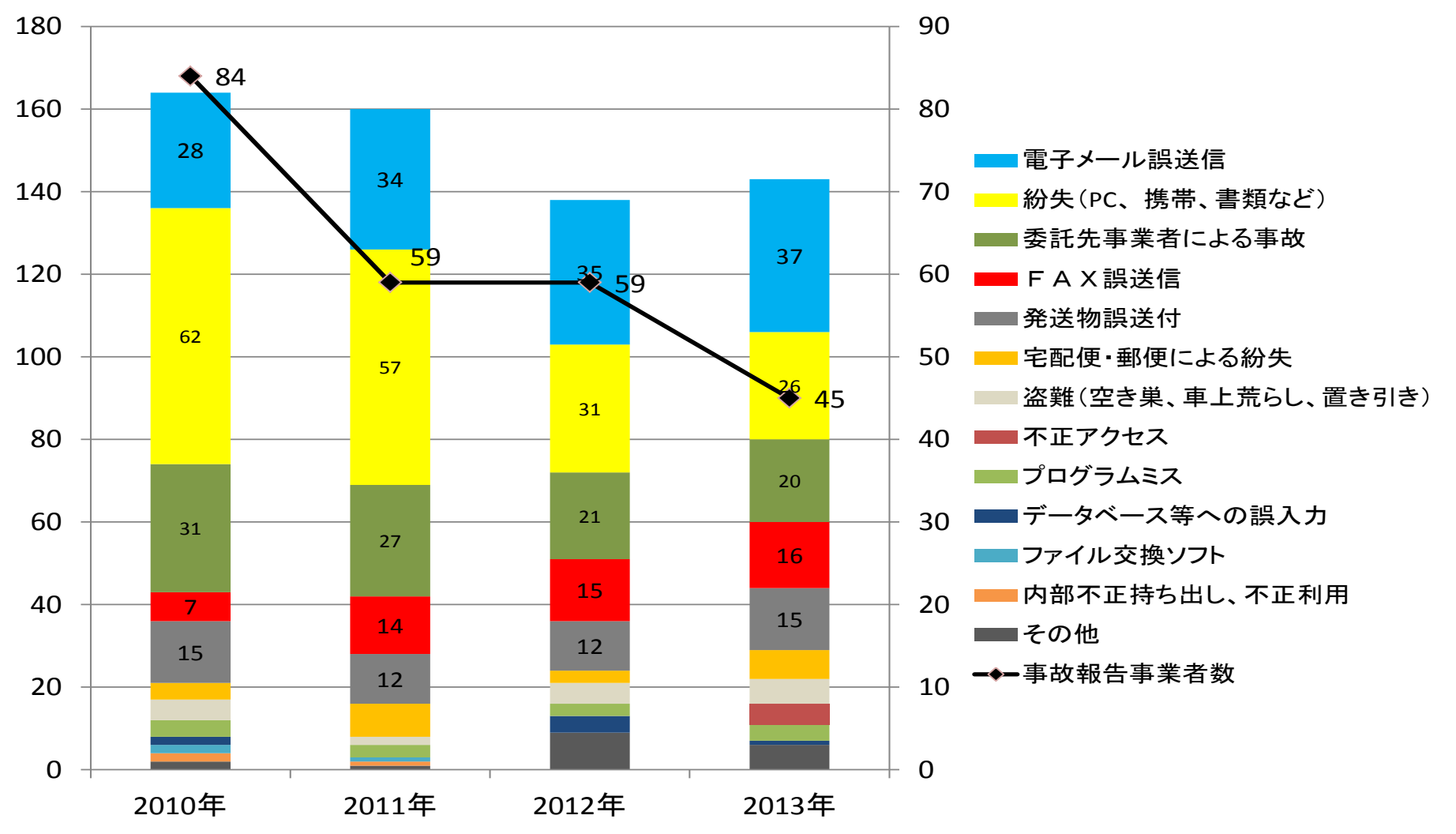
図 4-10：漏えい原因比率（人数）

出展元： JNSA 2016年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～より

３.セキュリティ事故は何故起こるのか？

3.セキュリティ事故は何故起こるのか？

個人情報取り扱い事故状況（2010～2013）

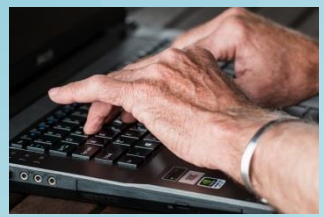


情報サービス産業協会報告書より

３.セキュリティ事故は何故起こるのか？

個人情報取り扱い事故状況（2010～2013）

１位	電子メールの誤送信
２位	紛失（PC、携帯電話、書類等）
３位	委託先事業者による事故
４位	ＦＡＸの誤送信
５位	発送物の誤送付・誤封入



情報サービス産業協会報告書より

3.セキュリティ事故は何故起こるのか？

人間は、そもそも、**ミスをする生き物**

1. 人間は気まぐれである
2. 人間はなまけものである
3. 人間は不注意である
4. 人間は根気がない
5. 人間は単調を嫌う
6. 人間はのろまである
7. 人間は論理的思考力が弱い
8. 人間は何をするかわかならい

出所：高橋秀俊，ヒューマン・ファクターと信頼度，コンピュータにおけるヒューマン・インターフェース
http://ylab.sfc.keio.ac.jp/lecture/2008/interfacedesign/lib/pdf/interface2008-handout2.pdf

3.セキュリティ事故は何故起こるのか？

では、私たちはこのまま<u>セキュリティ事故</u>を防ぐことが出来ないのでしょうか？

3.セキュリティ事故は何故起こるのか？

2015年・・・。2年前に
私は、ある仮説を立てました。
さて、その仮説とは・・・。

3.セキュリティ事故は何故起こるのか？

組織構成員の思考力が
低下、若しくは**停止**し、
主体性が失われている・・・

3.セキュリティ事故は何故起こるのか？

『**アイヒマン症候群**』という言葉を
あなたは聞いたことがありますか？

3.セキュリティ事故は何故起こるのか？

アドルフ・アイヒマンが残した言葉

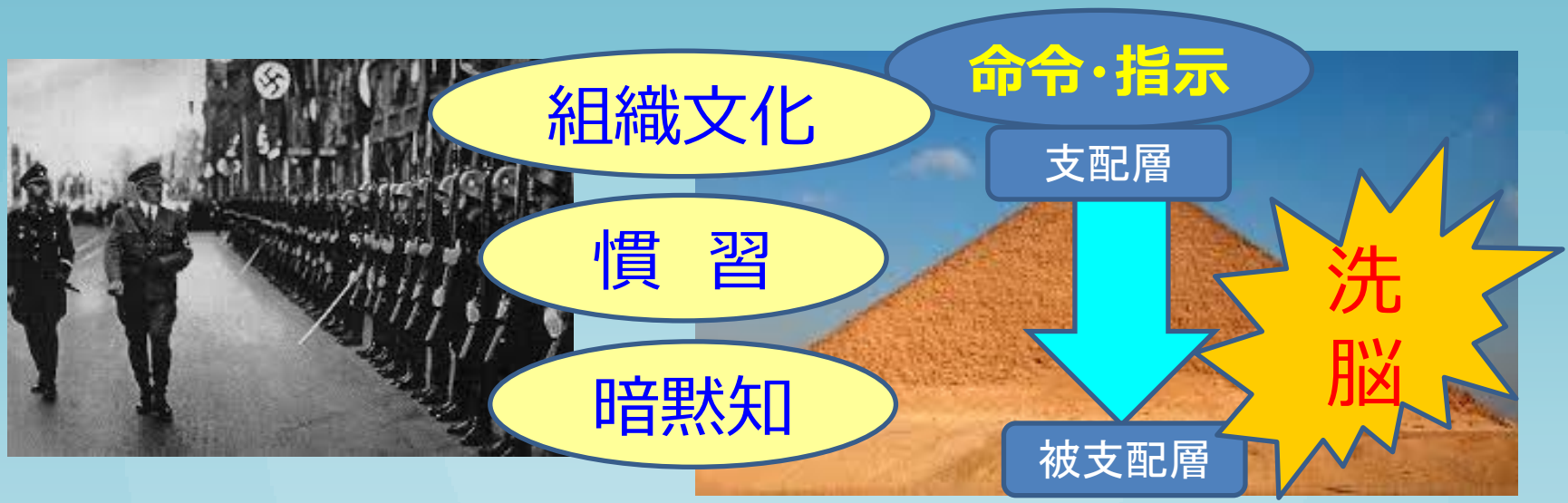
「一人の死は**悲劇**だが、集団の死は**統計上の数字**に過ぎない」

「**組織の命令**に従っただけです」

3.セキュリティ事故は何故起こるのか？

アイヒマン症候群とは

人間は、例え矛盾を感じていても、組織から命令され続けると、**罪悪感を抱くことなしに命令通りに動く習性を持つ生き物**です。
この習性はアイヒマン実験で検証されています。



3.セキュリティ事故は何故起こるのか？

上が決めたことは、絶対服従。
それが組織というものだ！
お前たちは、何も疑わず、指示通りに動いていればいいんだ！

疑問は残るが
まーいいか

勿論です。A部長・・・。
仰せの通りに対応します。

3.セキュリティ事故は何故起こるのか？

大きな組織構成員ほど、**アイヒマン症候群**になる可能性が高く、この症候群に陥る構成員には、この自覚症状がないのが特徴です。

矛盾、可能性に目をつぶり、
思考停止状態に陥っている。

3.セキュリティ事故は何故起こるのか？

組織構成員のセキュリティリスクへの
対応力が低下している。
そして・・・セキュリティインシデント
発生確率が高まる結果につながる

3.セキュリティ事故は何故起こるのか？

さて・・・**自主性**と**主体性**・・・。
この違いは一体？

3.セキュリティ事故は何故起こるのか？

自主性とは、組織が決めたことを
上から言われる前に、自分から
進んで行うというもの。

3.セキュリティ事故は何故起こるのか？

組織構成員には
主体的に行動する姿勢
が求められています。

3.セキュリティ事故は何故起こるのか？

アイヒマン症候群に陥らないためには・・・

①主体的に、物事を考える。
②矛盾に対して、極度に自分を押し殺さない。
③組織の誤った判断に、見て見ぬ振りをしない！
④自分の頭で思考し、判断することを常に忘れない。

ひとつでも良いので、
チャレンジしてみましょう！

4.組織の活性化を図る

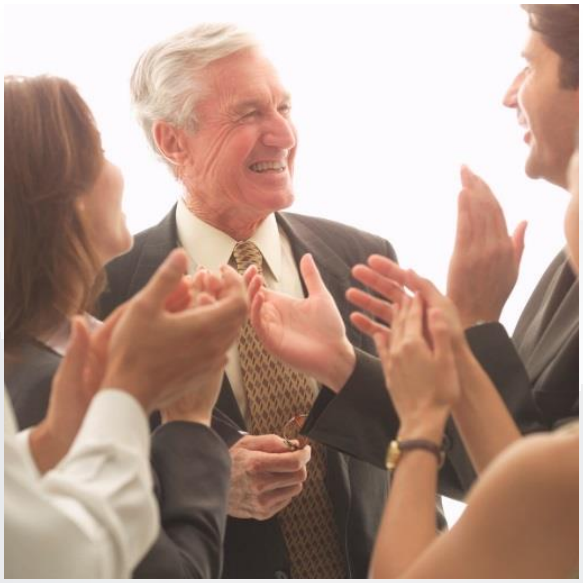
４.組織の活性化を図る

one for all　all for one

一人は皆のために　皆は一人のために

4.組織の活性化を図る

グローバル人材は、
リスクに強い！



４.組織の活性化を図る

この二人に共通するものは何か？

４.組織の活性化を図る

共通キーワード

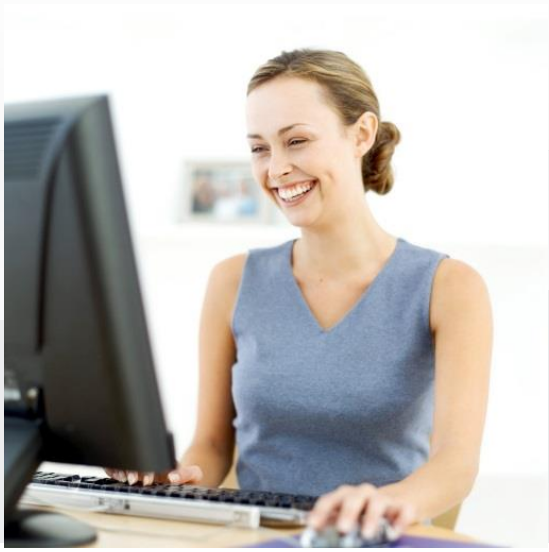
それは・・・

ピンチこそチャンス！

４.組織の活性化を図る

行動こそ主役

やる気は脇役



４.組織の活性化を図る

目標設定の最大の目的は目標を実現することではない。

４.組織の活性化を図る

人のモチベーション
を最高レベルに
引き上げることである

４.組織の活性化を図る

モチベーションアップ3効果

(1)サンクス効果
(2)スポットライト効果
(3)ピグマリオン効果

４.組織の活性化を図る

6.1 リスク及び機会への取り組み：(6.1.1 a), b), c)、6.1.2 a), a) 2)、6.1.3 c)が新規、それ以外は改訂)

(1) マネジメントシステム規格の**リスクマネジメント規格は、ISO31000**を決定。

(2) リスクの定義が「目的に対する不確かさの影響」に変更された。従って、評価可能な目的の設定が求められる。「不確かさ」は、プラスもあればマイナスもある。その他に、新しい概念として、「リスク機会」、「リスク基準」、「情報 を実施するための基準」、「リスク所有者」、「リスクのレベル」、「リスクの優先順位」などがある。

(3) また、リスク対応もこれまで「低減（管理策の適用）、受容、移転、回避」の4つであったが、「ISO 31000 リスクマネジメント」との整合化を図ったことにより、「リスクの回避、リスク機会の追求、リスク源の除去、起こりやすさを変える、結果を変える、リスク共有、リスク保有」の7つに変更された。

出展元：JNSA　ISO/IEC27001＆27002の改版概要と最新情報より

４.組織の活性化を図る

ISO27001 2013に
リスクには、機会（プラス）がある
という新しい概念が取り込まれた

４.組織の活性化を図る

セキュリティリスクは、
守りではなく攻めも大事！

5.最後に

5.最後に

社内だけでなく
社会全体の動きを
ウオッチしよう

４.最後に

情報セキュリティ白書2017

広がる利用、見えてきた脅威：つながる社会へ着実な備えを

概要説明資料

2017年8月1日

独立行政法人情報処理推進機構
技術本部セキュリティセンター
情報セキュリティ分析ラボラトリー

5.最後に

情報セキュリティ白書2017
広がる利用、見えてきた脅威：つながる社会へ着実な備えを

情報セキュリティの動向を広くカバーした一冊

■2016年度に情報セキュリティの分野で起きた
注目すべき出来事を分かりやすく解説

■国内外における情報セキュリティインシデントの状況や事例、攻撃の手口や脆弱性の動向、企業や政府等における情報セキュリティ対策の状況を掲載

■情報セキュリティを支える基盤の動向として、
国内外における情報セキュリティ政策や関連法の整備状況、情報セキュリティ人材の現状、
組織の情報セキュリティマネジメントの状況、
国際標準化活動の動向を掲載

■制御システム、IoT、スマートデバイス、Fintech、
オリンピックなど、2016年に注目された出来事、
分野の情報セキュリティについて解説

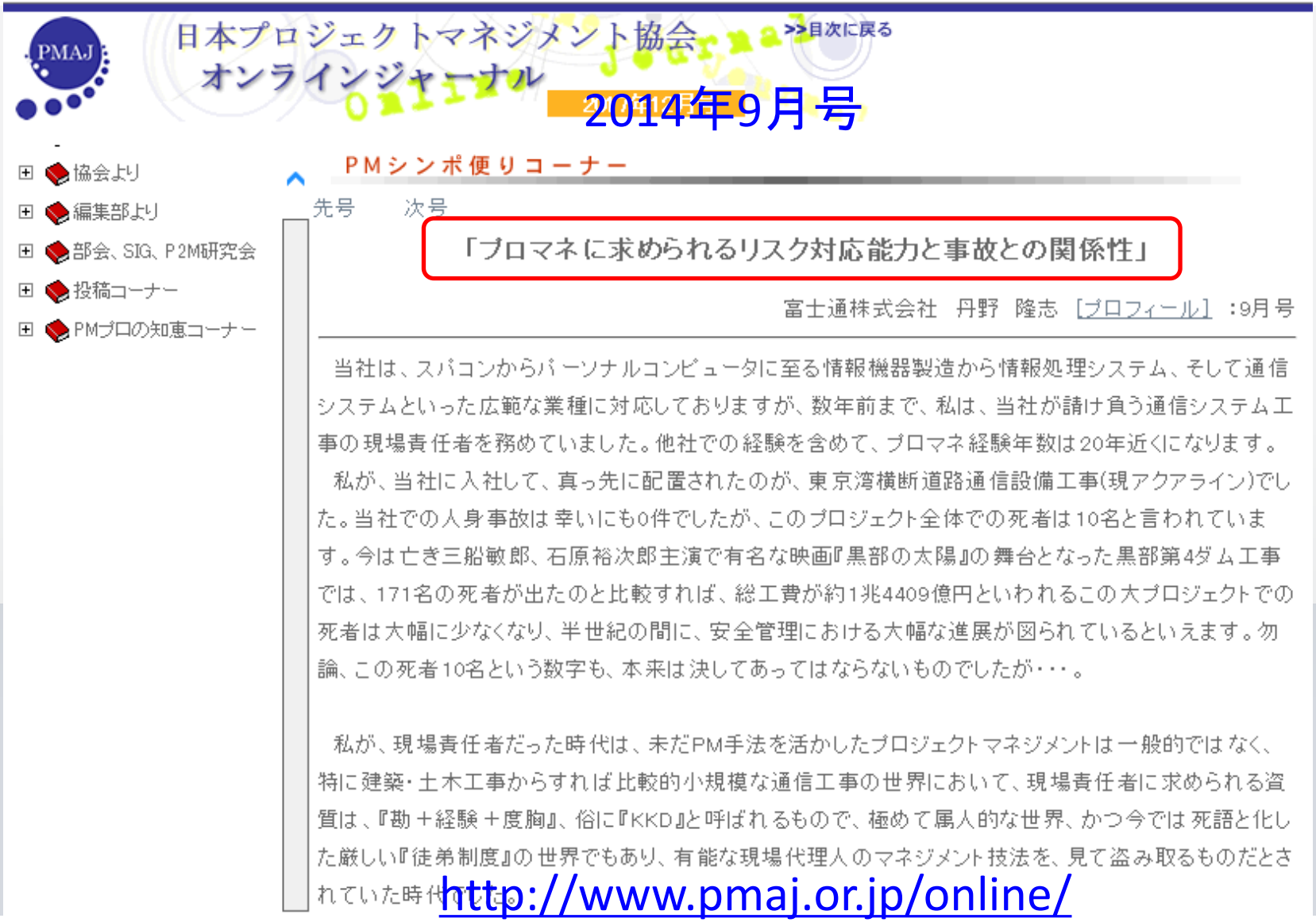
◆入手先：Amazon
全国官報販売組合
IPA　※全国の書店からも購入できます
電子書籍版は2017年8月、Amazon Kindleストア、
楽天Kobo等より発売

2017年7月1日発売

発行：IPA
ISBN：978-4-905318-53-8
ソフトカバー / A4判
定価　2,000円（税別）
電子書籍版　定価1,600円（税別）

1

5.最後に



http://www.pmaj.or.jp/online/

5.最後に

効果的なセキュリティマネジメントを実践して組織の活性化を図ろう！

to be continued