令和4年度「専修学校による地域産業中核的人材養成事業」

■航空機設計・製造分野におけるDX人材養成事業■

令和4年度プロト教材資料

本プロト教材資料は、文部科学省の教育政策推進事業委託費による委託事業として、日本航空大学校が実施した令和4年度「専修学校による地域産業中核的人材養成事業」の成果物です。

日本航空大学校

情報リテラシー学習領域
情報セキュリティ倫理

第1回

情報セキュリティ
マネジメントシステム

情報セキュリティマネジメントシステム
ISMS

ISO/IEC 27001は、情報セキュリティマネジメントシステム（ISMS）に関する国際規格

□情報セキュリティーマネージメントとは

企業情報の漏洩リスクを事前に予防し対処し対策する事が重要

どのようなリスクが想定され、どのような対策を行うのかを
計画P、実行Dし、問題点をチェックCして、改善Aする…
その仕組みを「情報セキュリティマネジメントシステム」と言います

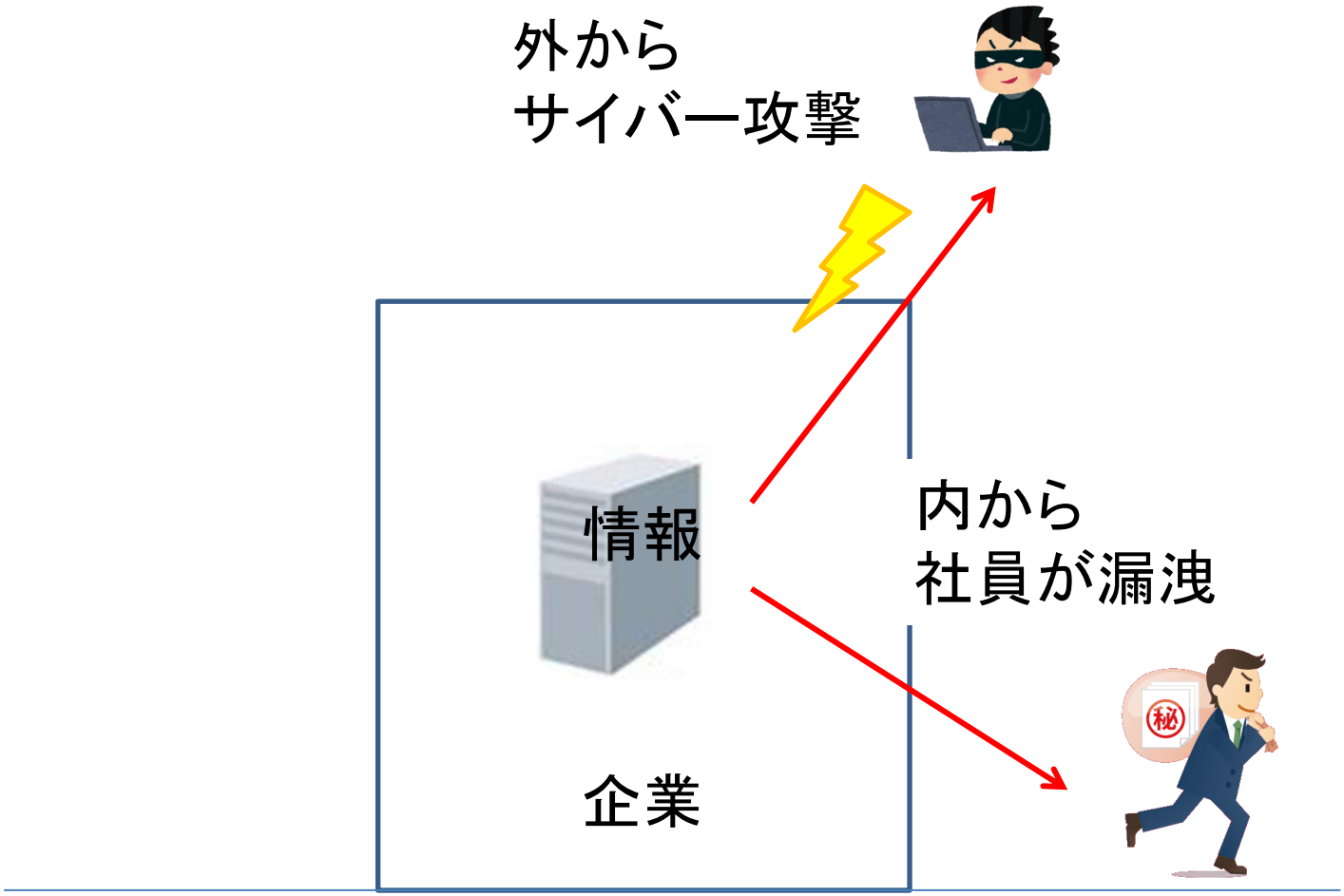
情報セキュリティーマネージメントシステム

Information Security Management Systems　ISMS

ISO27001は、このシステムを構築するための一つの枠組みです

ISO27001を取得することは、情報社会を取り巻く問題に大いに関心
を持って取り組んでいるという、社内外への表明となります

口情報を盗られる2つのルート



□企業の情報資産

公開する情報	守る情報
販売している商品のこと、広告	新製品の計画情報、開発データ、設計図
会社の考え、姿勢、環境、CSR	経営計画、秘密
会社の経営状態、売上、利益	お客様の個人情報
⇩	⇩
広報部門の活動	情報セキュリティー部門の活動

□情報資産への脅威

脅威

権限のない人間が
情報にアクセスできる

情報の**管理**方法が不明瞭、
破壊・改ざん・消去もできる

必要な者が必要な時に
必要な情報にアクセス
できない状態

企業の
情報セキュリティー
脆弱

問題

機密情報漏洩

データ改ざん

企業活動停止

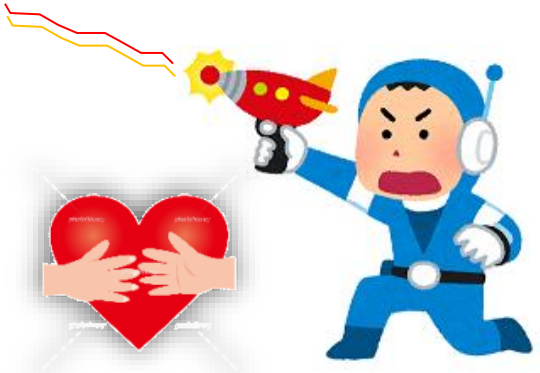
□情報のセキュリティーのために

外部からのサイバー攻撃、内部からの情報漏洩、といった

情報犯罪のリスクから情報資産を守るためには、何が必要でしょうか

・セキュリティに正面から取り組む組織体制、トップの姿勢、	仕組みつくり
・セキュリティーポリシー、運用規程、基準、	守るルール
・最新技術のシステム機器、対策ソフト、	戦う手段
・従業員の情報モラルの向上、ルール教育、	倫理感

これらが企業のセキュリティ水準を高めるために必須です



□情報セキュリティの３目標　C.I.A

機密性（Confidential）、完全性（Integrity）、可用性（Availability）

機密性(Confidentiality)とは、
権限を持つ者だけが、その情報にアクセスが出来る仕組みを作り
許可のない人間が情報にアクセスするのを防止すること

完全性(Integrity)とは、
情報の**管理**・保護方法が確実な仕組みを作り、
情報が破壊・改ざん・消去されていない状態をつくること

可用性(Availability)とは、
決められた条件のもとで情報を利用できるシステムを作り、
必要な者が必要な時に必要な情報にアクセス**利用**できる状態を作ること

□情報セキュリティの３目標　C.I.A

機密性（Confidential）

機密性(Confidentiality)とは、
権限を持つ者だけが、その情報にアクセスが出来る仕組みを作り
許可のない人間が情報にアクセスするのを防止すること

・パスワードを知る利用者のみがアクセスでき、知らないものはアクセスできない

・システム内に保管されているデータを不正に持ち出せない

・社内ネットワークの通信内容が盗聴されない

情報セキュリティの３目標　C.I.A

、完全性（Integrity）、

完全性(Integrity)とは、
情報の**管理**・保護方法が確実な仕組みを作り、
情報が破壊・改ざん・消去されていない状態をつくること

・サーバーデータが改ざんされていない

・webページが改ざんされていない

情報セキュリティの３目標　C.I.A

可用性（Availability）

・サイバー攻撃を受けシステム停止に至っても、バックアップデータが保管されている

・地震、停電等でシステム障害が発生しても、引き続きバックアップで利用可能である

可用性(Availability)とは、
決められた条件のもとで情報を利用できるシステムを作り、
必要な者が必要な時に必要な情報にアクセス**利用**できる状態を作ること

□ISMSの目指す姿

情報の機密性・完全性・可用性の3つをよくマネジメントし、
企業活動に有効活用するためのガイドラインです

企業の情報セキュリティー体制

機密性
Confidentiality

完全性
Integrity

可用性
Availability

ISO 27001
INFORMATION SECURITY
MANAGEMENT SYSTEM

□ISO 27001　導入の狙う効果

1）情報セキュリティリスクの低減を行う

マネジメントシステムを構築することで、リスクを業務ベースで全社的に捉え、必要な対策を行い、上手く機能しているのか判定し、反映するというPDCAサイクルで計画的に展開することができる

2）従業員のセキュリティー意識向上・モラル向上が実現できる

従業員の情報セキュリティに対する意識、気の緩み、悪意などについて改善できる

3）社外に対して、信頼感や安心感をアピールできる。

展開実績をHPに公開して、広報や営業の訴求ポイントとして利用できる
外部者へ防衛力を知らせることができる

組織名称	株式会社IHI
組織部門名称	高度情報マネジメント統括本部
所在地	東京都江東区豊洲3-1-1 豊洲IHIビル（本社）
認証基準	JIS Q 27001:2014(ISO/IEC 27001:2013)
認証登録番号	JUSE-IR-094
登録範囲	高度情報マネジメント統括の企画業務・構築業務・運用業務・業務評価の主要プロセスおよびプロセスで活用する情報資産、およびセキュリティ事業関連製品の営業、開発、調達、製造、修理およびサービスに関する情報資産 適用宣言書：2021年11月17日
初回登録日	2007年5月28日
有効期限	2025年5月27日
認証機関（認定番号）	一般財団法人日本科学技術連盟　ISO審査登録センター(ISR005)

動画視聴　IPAあなたの会社のセキュリティー女医　1分から6分30秒

IPA

Information-technology　Promotion Agency

情報処理推進機構

経産省、IPA　主催検定

情報セキュリティーマネージメント試験

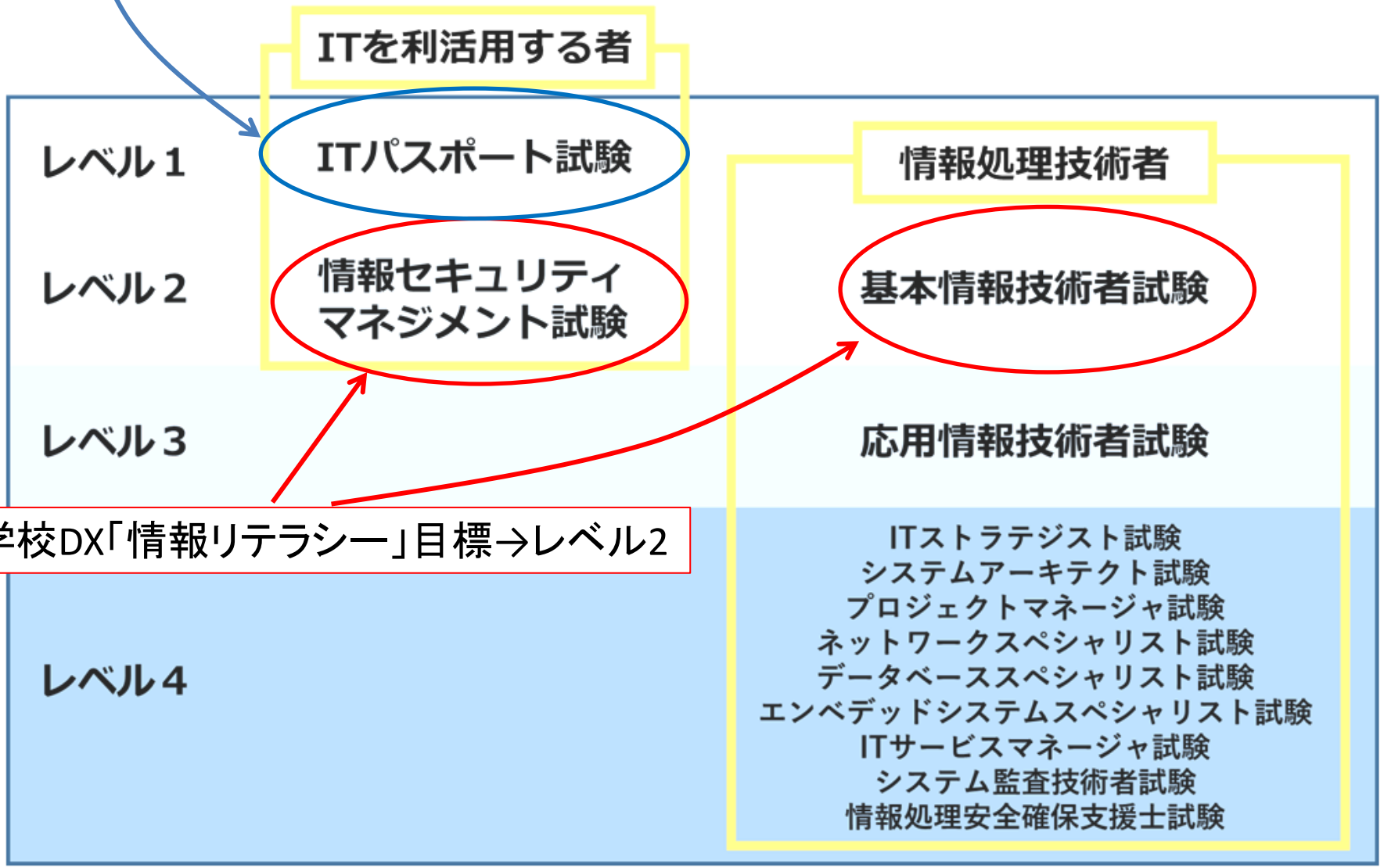
大学校DX「情報リテラシー」 目標→レベル2

高校「情報I」 目標　→レベル1

高校「情報I」目標→レベル1

経産省、IPA　主催検定

情報処理技術者試験の種類



大学校DX「情報リテラシー」目標→レベル2

IPA

ITパスポート試験

あなたのＩＴ力を証明する国家試験

ITパスポート公式キャラクター
上峰亜衣（うえみねあい）

【プロフィール：マンガ】 https://www3.jitec.ipa.go.jp/JitesCbt/html/uemine/profile.html

「iパス」は、ITを利活用するすべての社会人・学生が備えておくべき
ITに関する基礎的な知識が証明できる国家試験です。

あなたのIT力を証明する

国家試験

日本の元気を
iパスで!!

iパス公式キャラクター

パス

上峰 亜衣（うえみね あい）

PROFILE

社会人2年目、23歳。大手商社の経営企画部門に所属。業務に必要なITと経営に関する基礎知識を得るため、iパスに挑戦。2回目で合格（750点）。iパスで得た幅広い知識を活かして、日々、奮闘中。

IPA Better Life with IT

独立行政法人 情報処理推進機構

アンケート回答　2022年5月
三菱重工IT系部門エンジニア様

三菱重工

IT知識が広く浅く学べる。	5) 学生時代に取得を勧められる情報系資格について、項目に○をご記入ください (○) IT パスポート試験、　( ) 情報検定(J 検) (○) 基本情報技術者試験　( ) 日商プログラミング検定 ( ) Python 3 エンジニア認定基礎試験 ( ) C 言語プログラミング能力認定試験 ( ) Microsoft 認定資格　( ) 統計検定 その他 ( )

第2回

サイバー攻撃の問題事例

サイバーについて

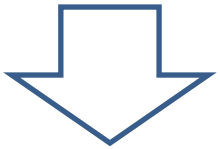
cyber は「サイバネティックス」(cybernetics)に由来する語

生物を自らを制御する機械システムととらえ

機械システム工学　～　人間の脳神経生理学　～　社会学

の相互関係（コミュニケーション）を統一的に扱うことを意図して発展した

学際領域



今では「コンピュータの」「電脳の」という意味の
形容詞や接頭語として広く使われる

ウィーナー

サイバネティックス

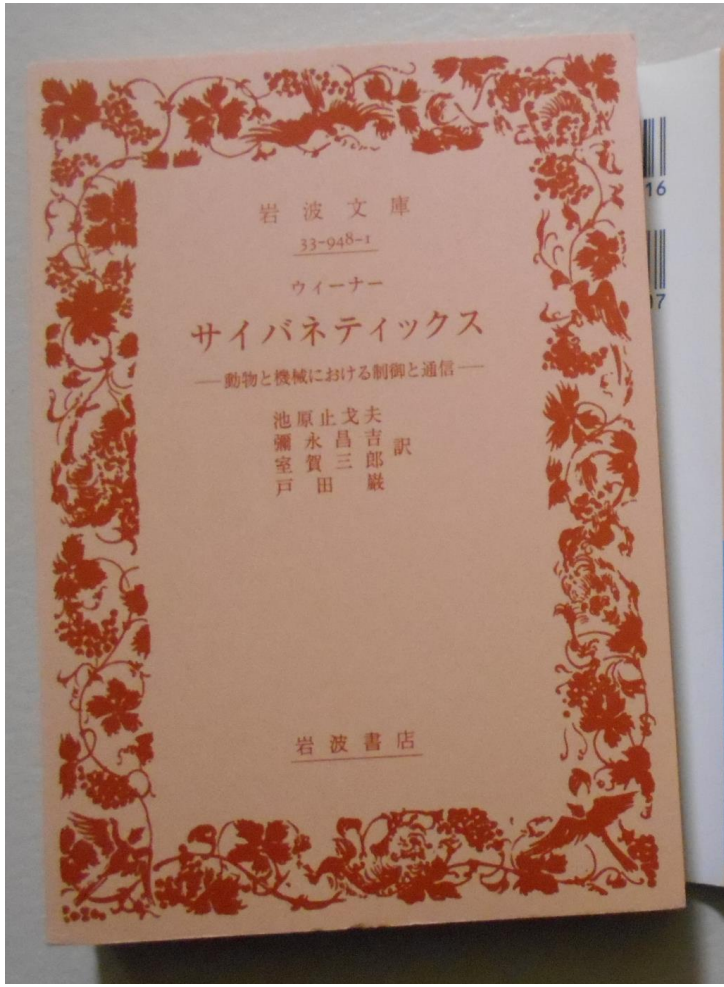
動物と機械における制御と通信

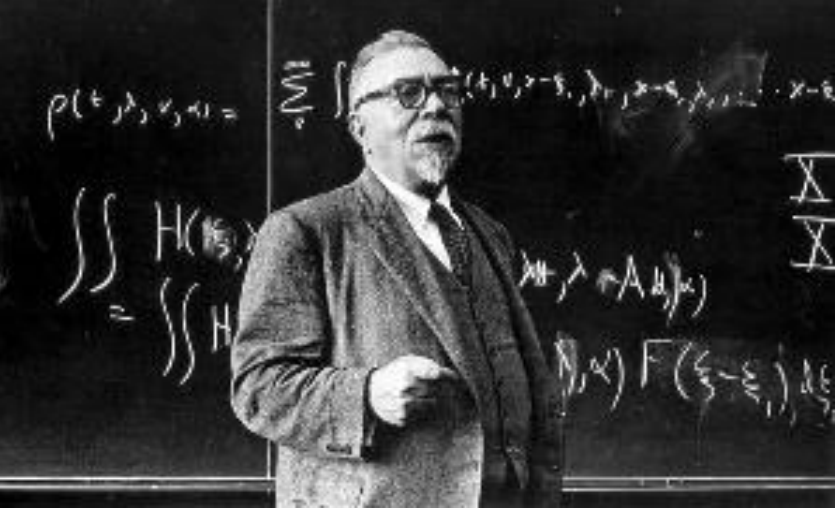
池原止戈夫・彌永昌吉
室賀三郎・戸田 巌訳

心の働きから生命や社会までをダイナミックな制御システムとして捉えようとした先駆的な書。本書の書名そのものが新しい学問領域を創成し、自然科学分野のみならず、社会科学の分野にも多大な影響を与えた。現在でも、人工知能や認知科学、カオスや自己組織化といった非線形現象一般を解析する研究の方法論の基礎となっている。（解説＝大澤真幸）

青 948-1
岩波文庫

ノーバート・ウィーナー
「サイバネティックス」
―動物と機械における制御と通信―
(岩波文庫) 1948年



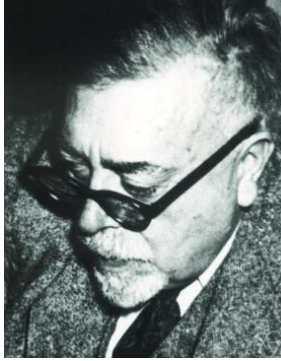


ノーバート・ウィナー（Norbert Wiener）

1894年11月26日 - 1964年3月18日
アメリカ合衆国の数学者

サイバネティクス理論の提唱者
渡り鳥の飛行を観察して「通信とフィードバック制御」という歴史に残る論文を発表、
その中で「サイバネティクス理論」を発表した。

第二次世界大戦中の射撃制御装置に関する研究は
通信理論への関心を総合し、サイバネティックスを
定式化することへ彼を促した。
戦後、彼は自身の影響力を行使し、人工知能、
計算機科学、神経心理学の分野における当時最も
優れた研究者をMITに招き研究をおこなった。



1948年　　動物と機械　における　制御　と　通信

コンピューター（電脳）技術の発明・発展

50年後

- ロボット工学
- プログラム制御
- インターネット

機械と人間の融合物を意味する「サイボーグ」もしばしば使われる

宮城県石巻市にある、石ノ森マンガ館

企業のｻｰﾊﾞｰへの
サイバー攻撃事例

事例1：ホンダ　サイバー攻撃　2020年6月8日

・社内ネットワークが使えなくなった

・社員のパソコンが感染し、使えなくなった

・海外の9つの工場で生産が一時停止になった

事象

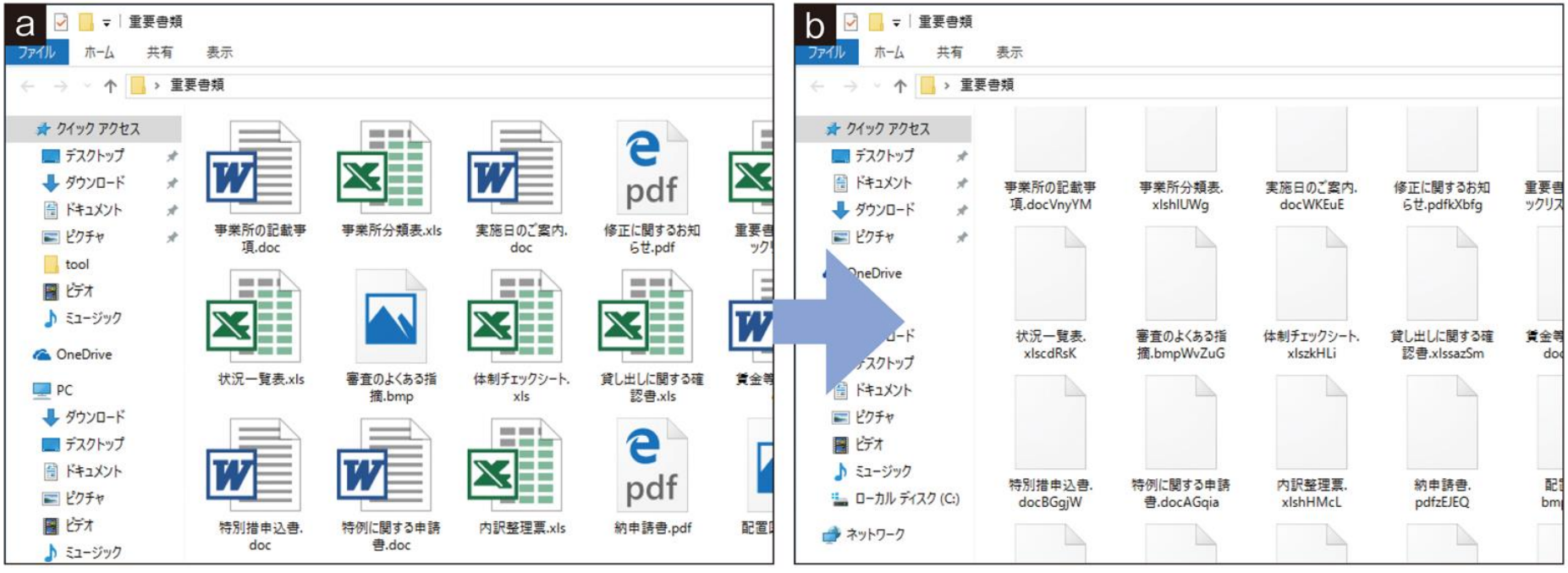
・外部からのサイバー攻撃の影響で8日の午前9時ごろから社内のネットワークを通じたメールのやり取りなどができなくなり、ウイルスに感染したとみられるパソコンの画面が真っ暗になるといった異常が出た

・災害の際に利用する緊急連絡網を通じて、業務用や私用のスマホなどにメールや自動音声で連絡した

・原因を調べるために、全社員のパソコン使用、社内のネットワークへのアクセスを制限し、有給休暇を取るよう勧めた

・社内のサーバーに外部から侵入されてウイルスが拡散していたことが判明した
パソコンのデータをハッカーが暗号化し、解除のために金銭を要求する「ランサムウェア（身代金ウイルス）」が全社的に広がったものとみられる。

こうなっちゃう


a
重要書類
ファイル
ホーム
共有
表示
重要書類
クイック アクセス
デスクトップ
ダウンロード
ドキュメント
ピクチャ
tool
ビデオ
ミュージック
OneDrive
PC
ダウンロード
デスクトップ
ドキュメント
ピクチャ
ビデオ
ミュージック
事業所の記載事項.doc
事業所分類表.xls
実施日のご案内.doc
修正に関するお知らせ.pdf
状況一覧表.xls
審査のよくある指摘.bmp
体制チェックシート.xls
貸し出しに関する確認書.xls
特別措申込書.doc
特例に関する申請書.doc
内訳整理票.xls
納申請書.pdf
b
重要書類
ファイル
ホーム
共有
表示
重要書類
クイック アクセス
デスクトップ
ドキュメント
ダウンロード
ピクチャ
ビデオ
ミュージック
ローカル ディスク (C:)
ネットワーク
事業所の記載事項.docVnyYM
事業所分類表.xlshIUWg
実施日のご案内.docWKEuE
修正に関するお知らせ.pdfkXbfg
状況一覧表.xlscdRsK
審査のよくある指摘.bmpWvZuG
体制チェックシート.xlszkHLi
貸し出しに関する確認書.xlssazSm
特別措申込書.docBGgjW
特例に関する申請書.docAGqia
内訳整理票.xlshHMcL
納申請書.pdfzEJEQ

被害の大きさ

・自動車を生産するUSAの全5工場とトルコの1工場など計9工場、
二輪車を生産するインドとブラジルの各1工場
において生産できなくなった。
自動車工場は全世界に約30カ所あり、3割ほどが止まったことになる。

・USAオハイオ工場では、生産ラインを管理するシステムにも障害が起きてた
コールセンターの受付やリース契約の業務もできなくなった。

国内では
・自動車や二輪車をつくる4工場で「完成車検査システム」が動かず、一時出荷を見合わせた

事例:トヨタ　サイバー攻撃　2022年2月26日

・部品メーカーの受注発注システムが使えなくなった

・社内サーバーを全て停止した

・国内全14工場で生産が停止となり、13000台の生産が滞った

トヨタ本体ではなく、サプライチェーンのセキュリティー対策の脆弱な企業をついての攻撃が発生した

経緯

小島プレスの子会社の通信用機器にウィルスが侵入

⇩

生産活動に必要な取引先様との受発注データを担うシステムの
サーバーが被害を受けた、部品生産ができなくなった

⇩

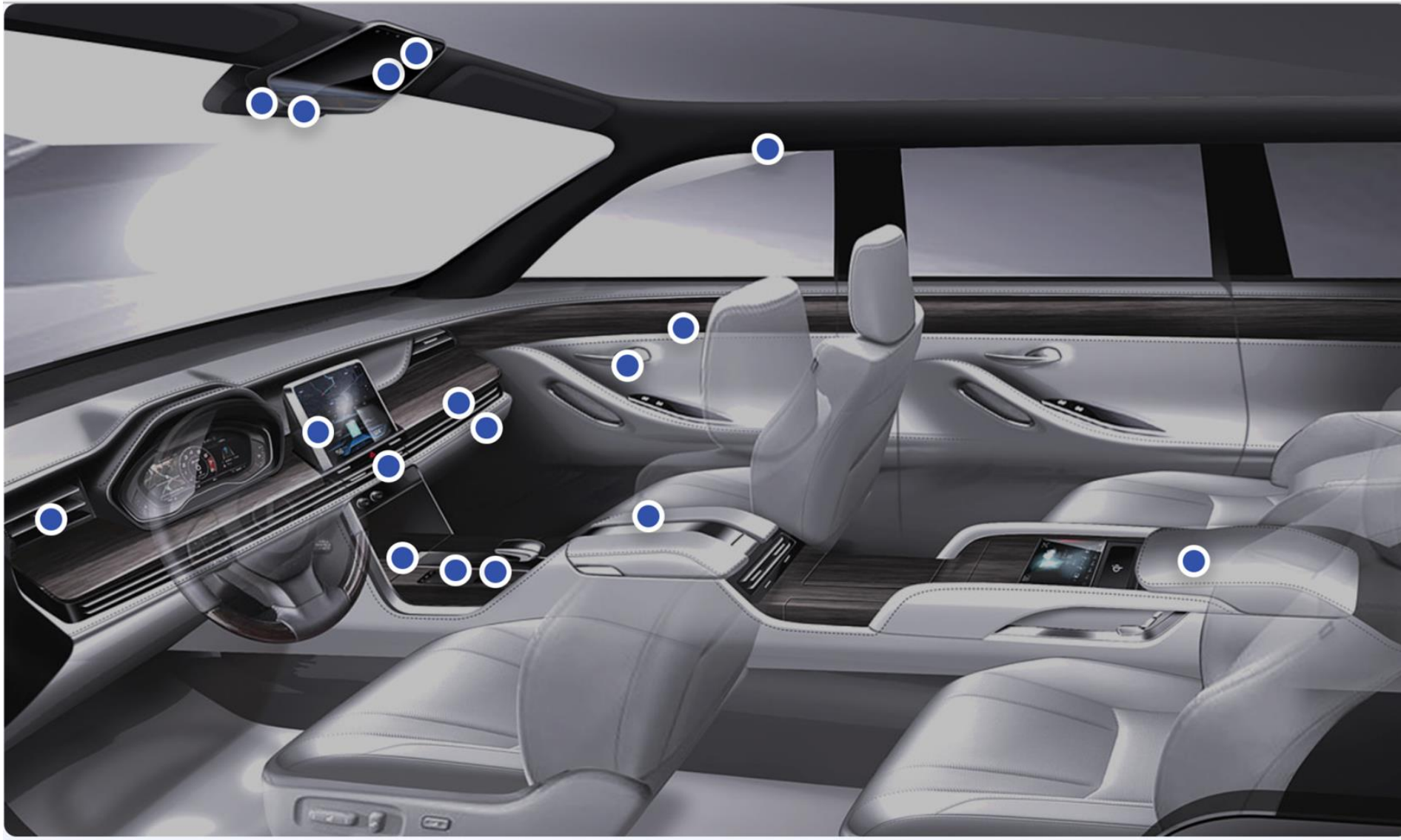
2月26日、トヨタは部品の供給が受けられず、全工場を止めた
影響範囲の特定などのため、社内サーバーを一旦全て停止した

⇩

この影響からグループの日野自動車、ダイハツ工業も26日、
一部生産を見合わせた

ランサムウエア（身代金要求型ウイルス）に感染し、被害を受けた可能性が高い

小島プレス社の部品



小島プレス株式会社

資本金
4億5000万円
売上高
1,790億円（2021年）
社員数
1,650名（2022年1月付）
所在地
愛知県豊田市下市場町3丁目30番地

主要取引先
トヨタ自動車、トヨタ車体、トヨタ紡織、林テレンプ、トヨタ自動車東日本、
豊田自動織機、日野自動車、プライムアースEVエナジー、
ダイハツ工業、豊田通商、デンソー、アイシン、ジェイテクト、スバル、
プライム プラネット エナジー&ソリューションズ

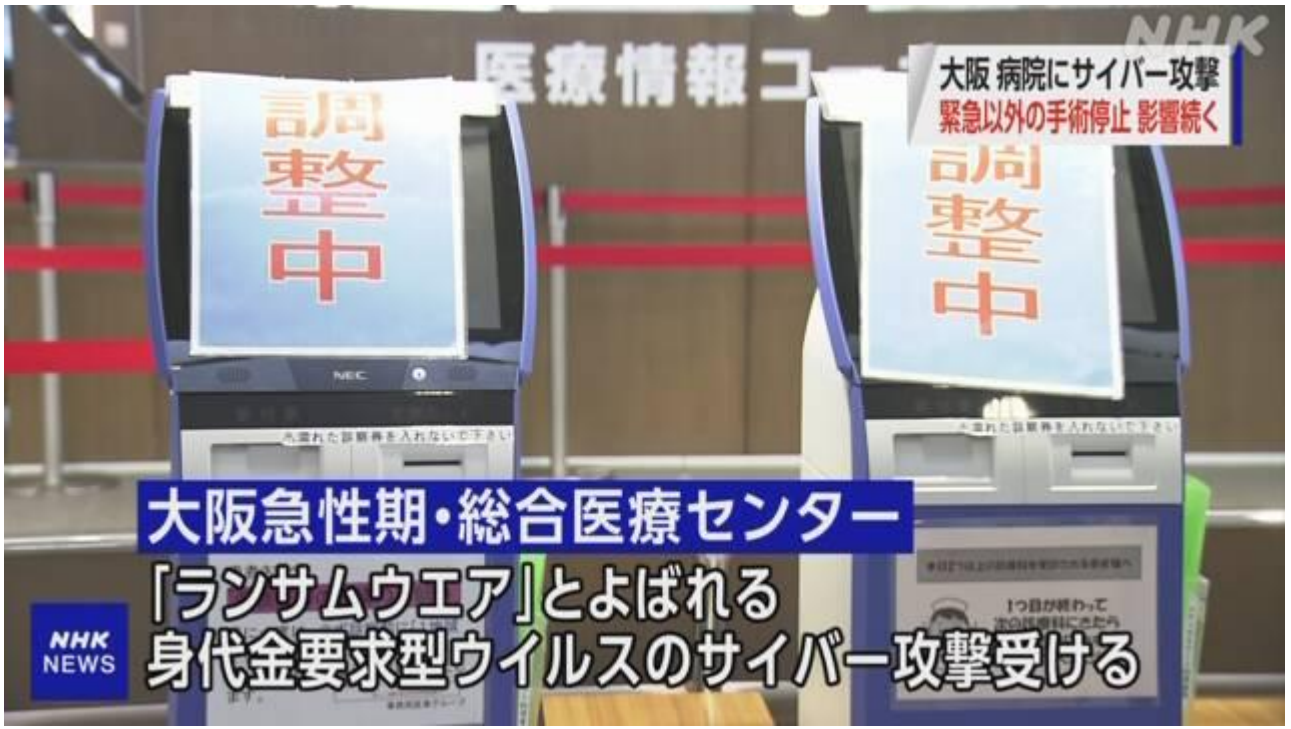
その後の調査で、ウイルスの侵入口は、小島プレスの子会社の通信用機器だった（VPN？）ことが判明。機器には、攻撃を受けやすい 脆弱ぜいじゃく 性があった。トヨタの供給網は6万社に上る。そのうち1社のセキュリティーが破られるだけで、全体がマヒする危うさを示した

事例：病院 サイバー攻撃

大阪急性期・総合医療センター
2022年10月31日

事象

・電子カルテなどのシステムに障害が発生,、閲覧できなくなった
・外来診療や緊急以外の手術を停止、救急患者の受け入れもできない
・会計、薬処方のシステムも稼働できなくなった



ルート

患者の給食を納入している事業者からウイルスが侵入した可能性が高い

堺市の事業者から病院のサーバーへの不正なアクセスが大量に確認された

この事業者のデータセンターも病院と同じ「ランサムウエア」に感染していた

事業者のデータセンターのセキュリティーは古いバージョンのままだった

メールに乗ってきたのではなさそう

サイバー被害を受けた医療機関の主な事例

平成30年10月	宇陀市立病院（奈良県）	電子カルテなど医療情報システムがコンピュータウイルスに感染。一部データが暗号化され、カルテが閲覧できない状態に
令和3年5月	市立東大阪医療センター（大阪府）	医用画像参照システムに不正アクセスがあり、システムが利用不可に
10月	つるぎ町立半田病院（徳島県）	電子カルテの端末やサーバーのデータが暗号化され、使用不能に
	富士病院（静岡県）	不正アクセスでシステム障害が発生
4年1月	春日井リハビリテーション病院（愛知県）	電子カルテシステムに障害。不正アクセスの疑い
4月	青山病院（大阪府）	不正アクセスでシステム障害発生。病院内のカルテが使用不可に
10月	大阪急性期・総合医療センター（大阪府）	電子カルテシステムで障害が発生。通常診療の停止が続いている

ハッカーが病院を狙う意味

1.新型コロナ感染拡大で医療が逼迫している

2.医療機関は重要な個人情報を多く扱っている

3.医療機関はシステム停止が人命に関わるため即時の復旧が必要

4.医療機関はセキュリティ対策が他の業種に比較して脆弱である

早急にシステム復旧のための身代金要求に応じなければならない弱みにつけ込む

ここで動画視聴　TVニュース

第3回

サイバー攻撃の構造と対策

情報セキュリティ10大脅威 2022」

IPA

順位	「組織」向け脅威	昨年順位
1位	標的型攻撃による被害	1位
2位	ビジネスメール詐欺による被害	3位
3位	ランサムウェアによる被害	2位
4位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW※
5位	内部不正による情報漏えい	8位
6位	サービス妨害攻撃によるサービスの停止	9位
7位	インターネットサービスからの個人情報の窃取	6位
8位	IoT機器の脆弱性の顕在化	7位
9位	脆弱性対策情報の公開に伴う悪用増加	4位
10位	不注意による情報漏えい	12位

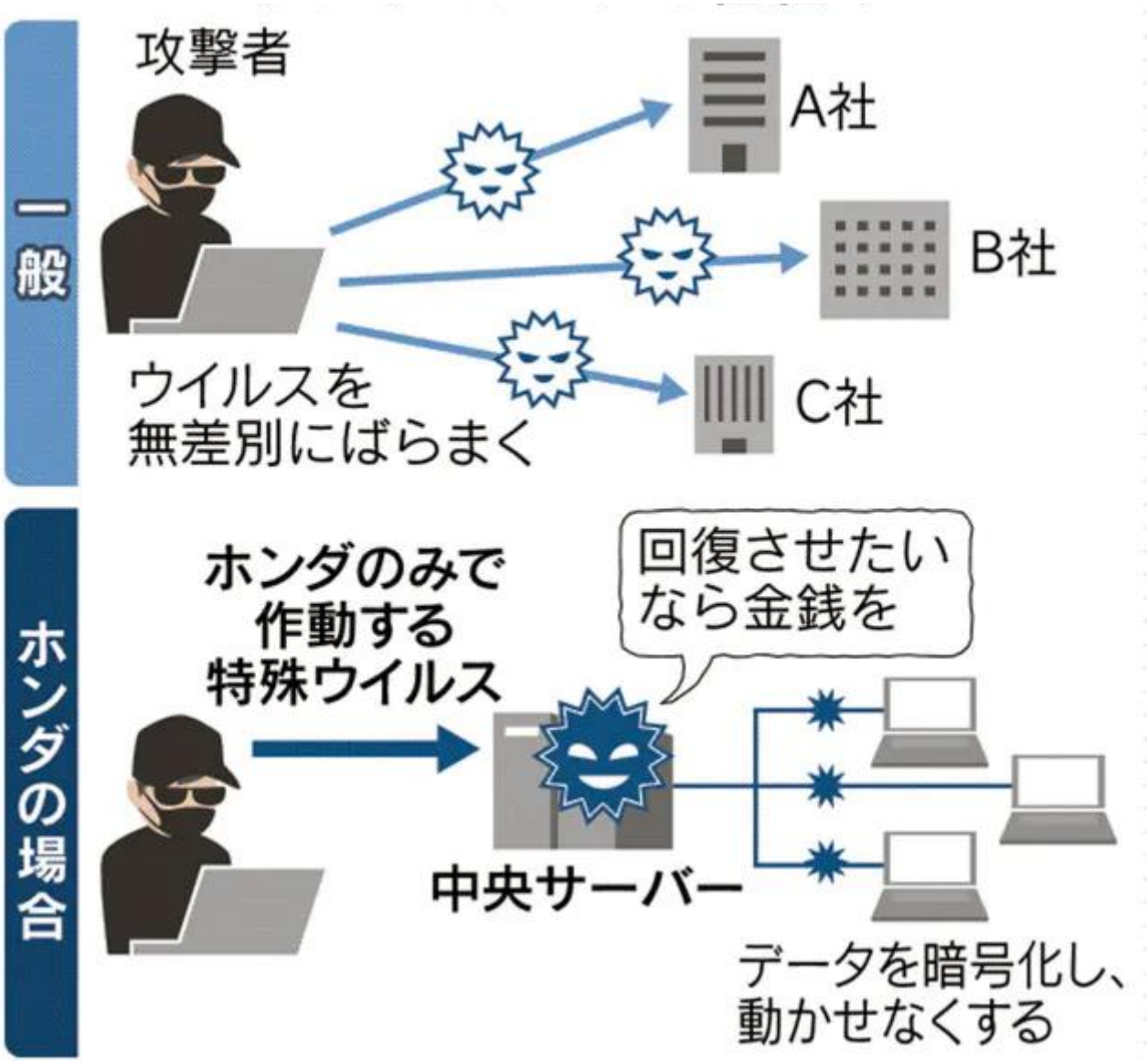
標的型企業攻撃の手口

標的型サイバー攻撃

事業規模が大きく重要なデータを多く有している製造業は、
IoTの推進により外部ネットワークとの接続点が増加したことも相まって、
標的型攻撃の対象となりやすい

特定の企業に狙いを定め、端末をマルウェアに感染させることで、
内部へ潜入します。
感染した端末を起点として組織内部のネットワークやサーバーを探索し、
侵害範囲を拡大していきます

標的型サイバー攻撃


一般
攻撃者
A社
B社
C社
ウイルスを
無差別にばらまく
ホンダの場合
ホンダのみで
作動する
特殊ウイルス
回復させたい
なら金銭を
中央サーバー
データを暗号化し、
動かせなくする

感染経路

○経路1　電子メール開封感染

× 添付ファイルによる感染

メールに添付したファイルを実行させることで、ランサムウェアに感染させる

メールの差出人や件名、本文をなりすまして標的型攻撃を仕掛ける手法と、

「請求書」、「問い合わせ」といった件名と内容でばら撒き型の攻撃を仕掛ける

手法がある

× 本文のURLリンク先クリックによる感染

メールの本文にあるURLをクリックさせることで、ランサムウェアをダウンロード

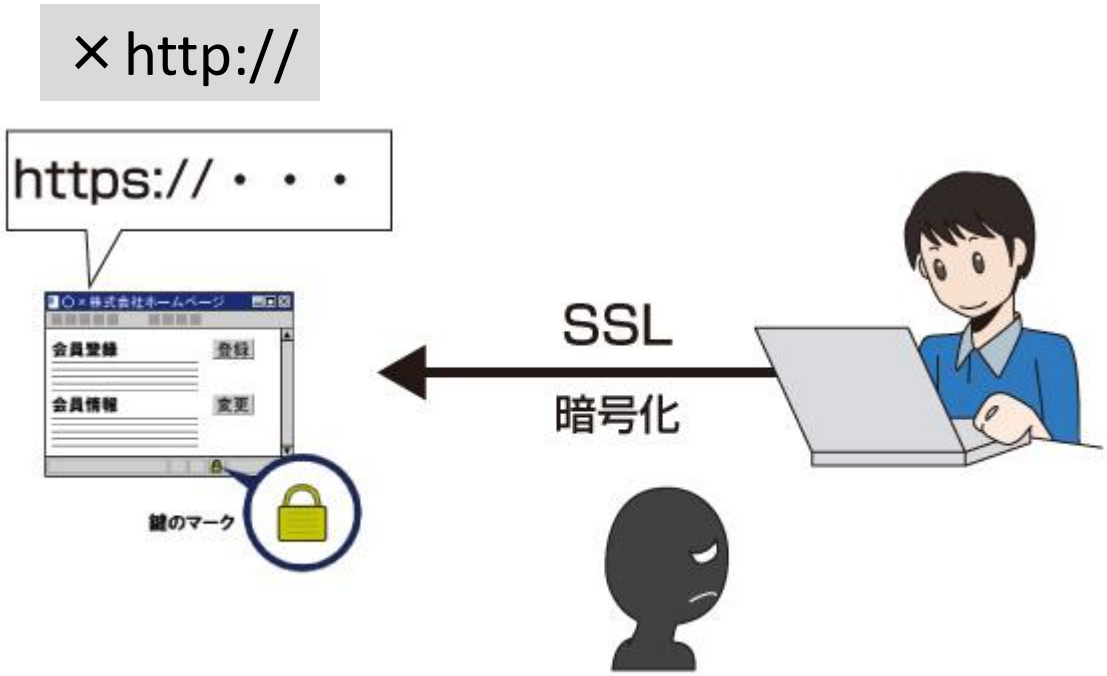
させて感染させる手法だ。メールの件名や本文、URLのリンク先を巧妙に作り

こんでおり、思わずクリックしてしまう危険性がある

○経路2　Webブラウザのホームページ接続感染

ブラウザーのホームページを閲覧

アプリのダウンロードしインストール



○経路3 リモート接続VPNから侵入

最近目立っているのが、新型コロナウイルスの影響でテレワーク利用されている、
「VPN」などのリモート接続を狙った手口です。
外部からの接続をするネットワーク機器にみつかったぜい弱ポイントを突いたり、
社内サーバーへ接続するための認証PW/IDを何らかの手段で入手して、
社内ネットワークに侵入し感染させるケースです。

手口A:
電子メール攻撃

手口A：なりすましメールによる侵入

不審なE-mail が届く

実在の個人名、取引会社名　を語る

請求書、製品の問い合わせ、取材依頼

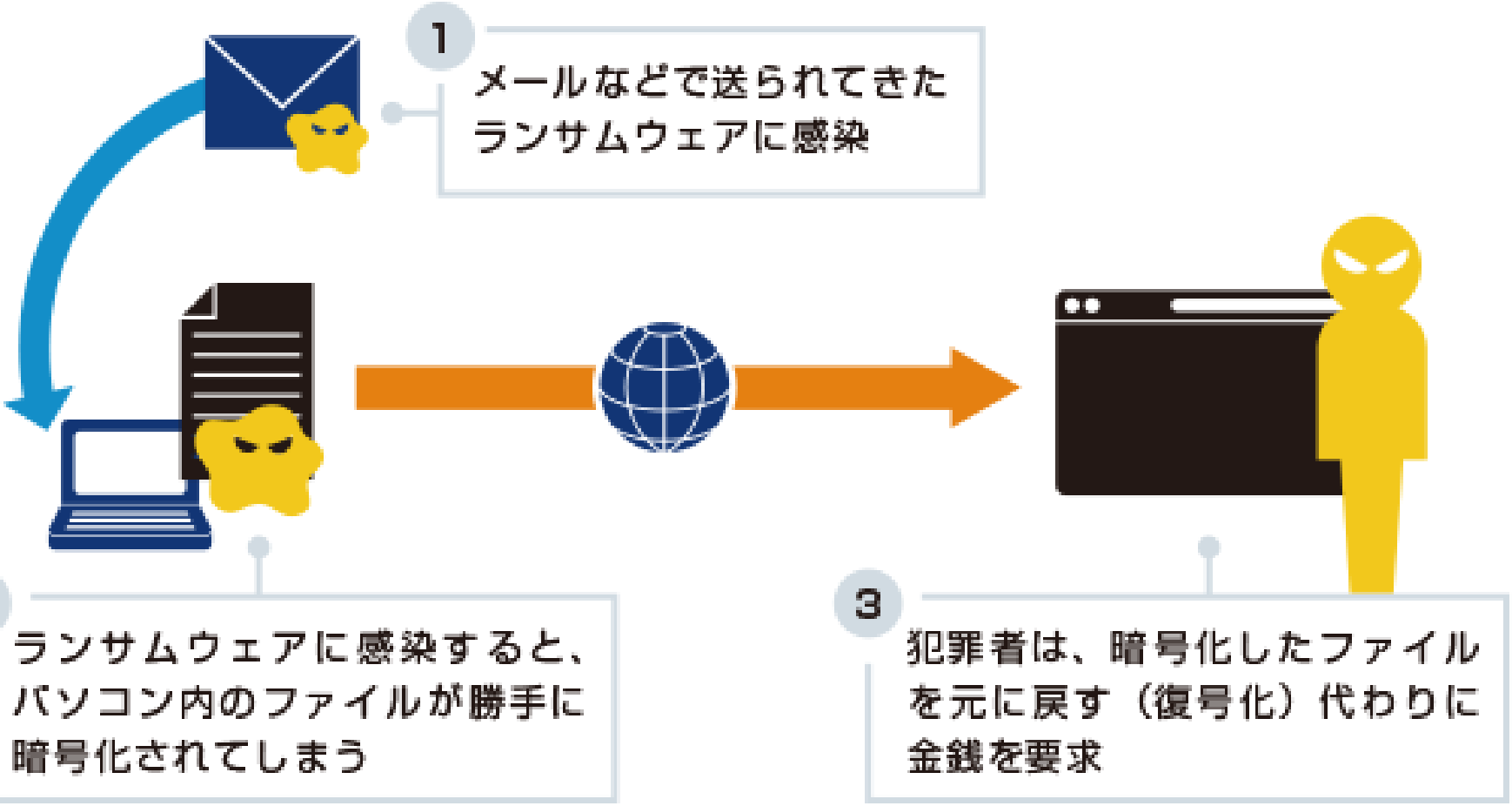
添付ファイルを開ける、実行ファイル .exe

PCにウィルスがはいりこむ

社内ネットワークやサーバーにウィルスがばらまかれる

社内システムの機能を不全化、会社活動を妨害

HP、機密文書、個人情報にたどり着き、暗号化、改ざんする


1
メールなどで送られてきた
ランサムウェアに感染
2
ランサムウェアに感染すると、
パソコン内のファイルが勝手に
暗号化されてしまう
3
犯罪者は、暗号化したファイル
を元に戻す（復号化）代わりに
金銭を要求

電子メール攻撃対策

メール対策　・不審メールに気付く、開けない
・社員教育訓練

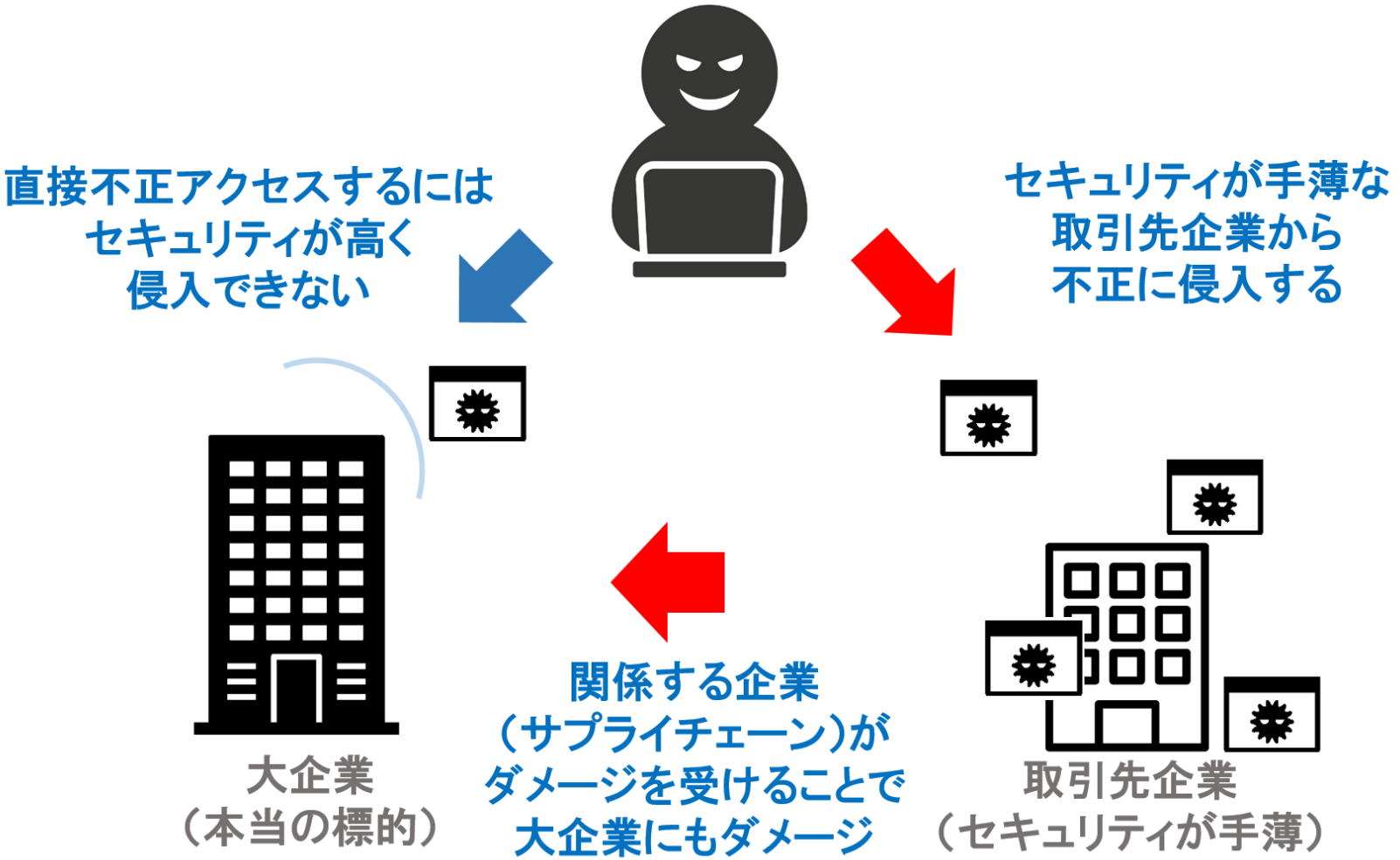
不用意にメールの添付ファイルを開かないよう、従業員教育を徹底する

基本OA対策　・ウイルス対策ソフトの導入と定期的な更新
・OSやソフトウエアの管理とアップデート
・不審なメール・ウェブサイトへのアクセス制御
・外部ネットワークと社内ネットワークの分離
・ID・パスワードや二段階認証によるIT制御

手口B:
弱い企業を突く

手口B：サプライチェーン攻撃

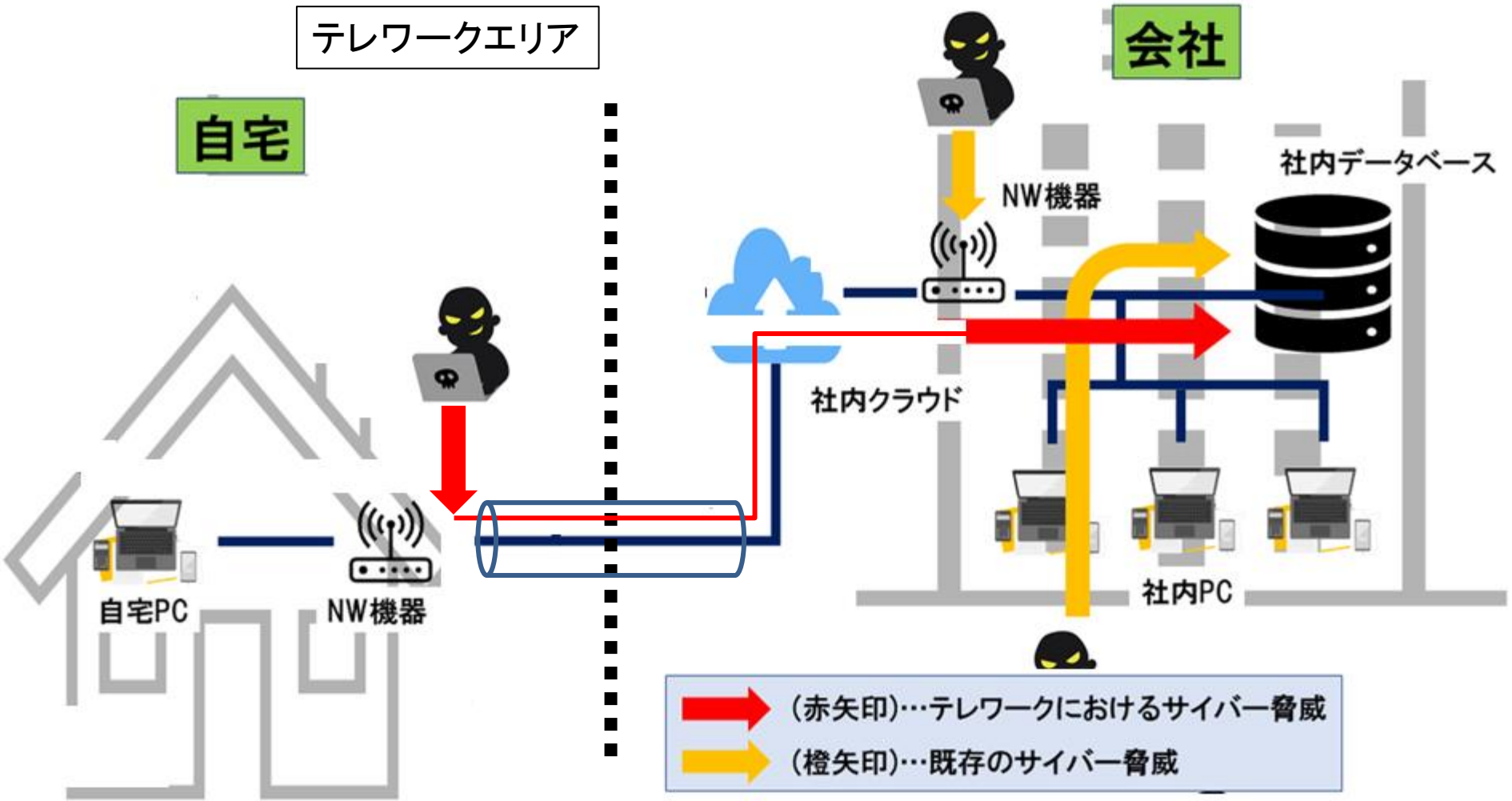
標的となる企業に直接攻撃するのではなく、セキュリティの手薄な
関連会社や取引先企業を通じて侵入する



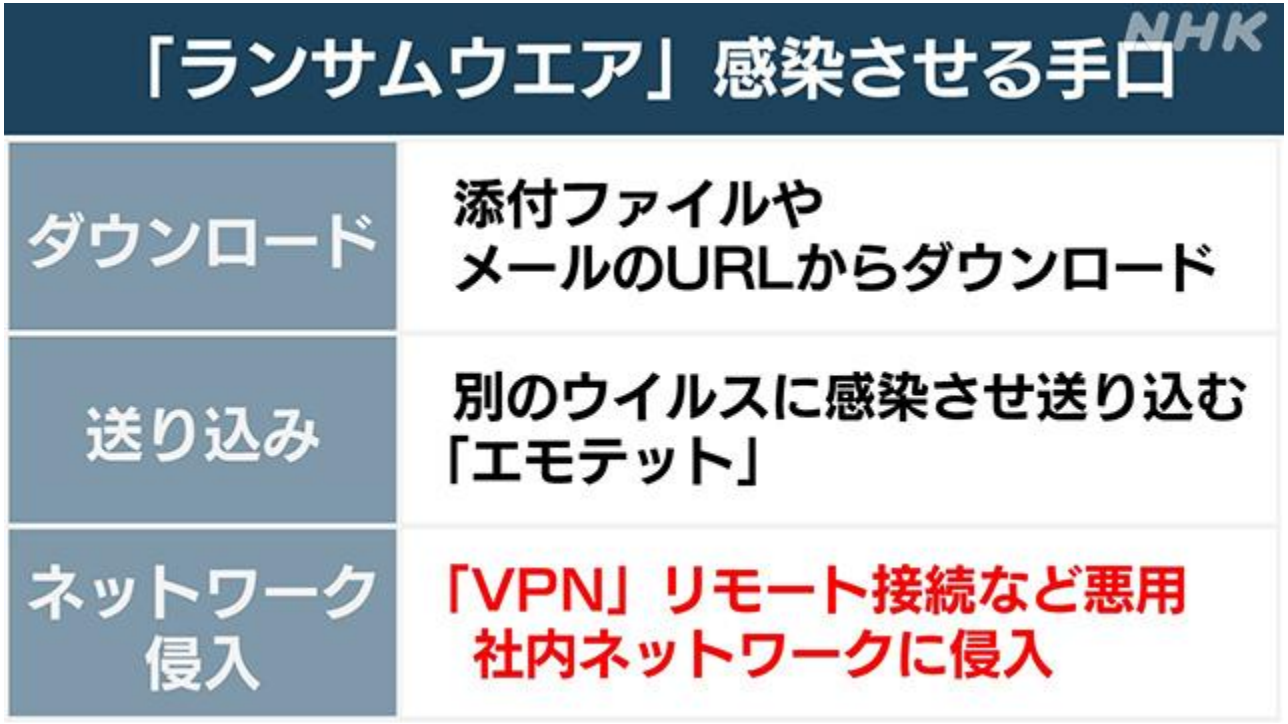
リモートワークで情報セキュリティーはどうやっているのだろう

手口C:
テレワークのセキュリティー盲点

VPN接続機器の脆弱性によるリスク



Secure Mobile Access（SMA）100


「ランサムウエア」感染させる手口
NHK
ダウンロード
添付ファイルや
メールのURLからダウンロード
送り込み
別のウイルスに感染させ送り込む
「エモテット」
ネットワーク
侵入
「VPN」リモート接続など悪用
社内ネットワークに侵入

VPN
Virtual Private Network
仮想専用線

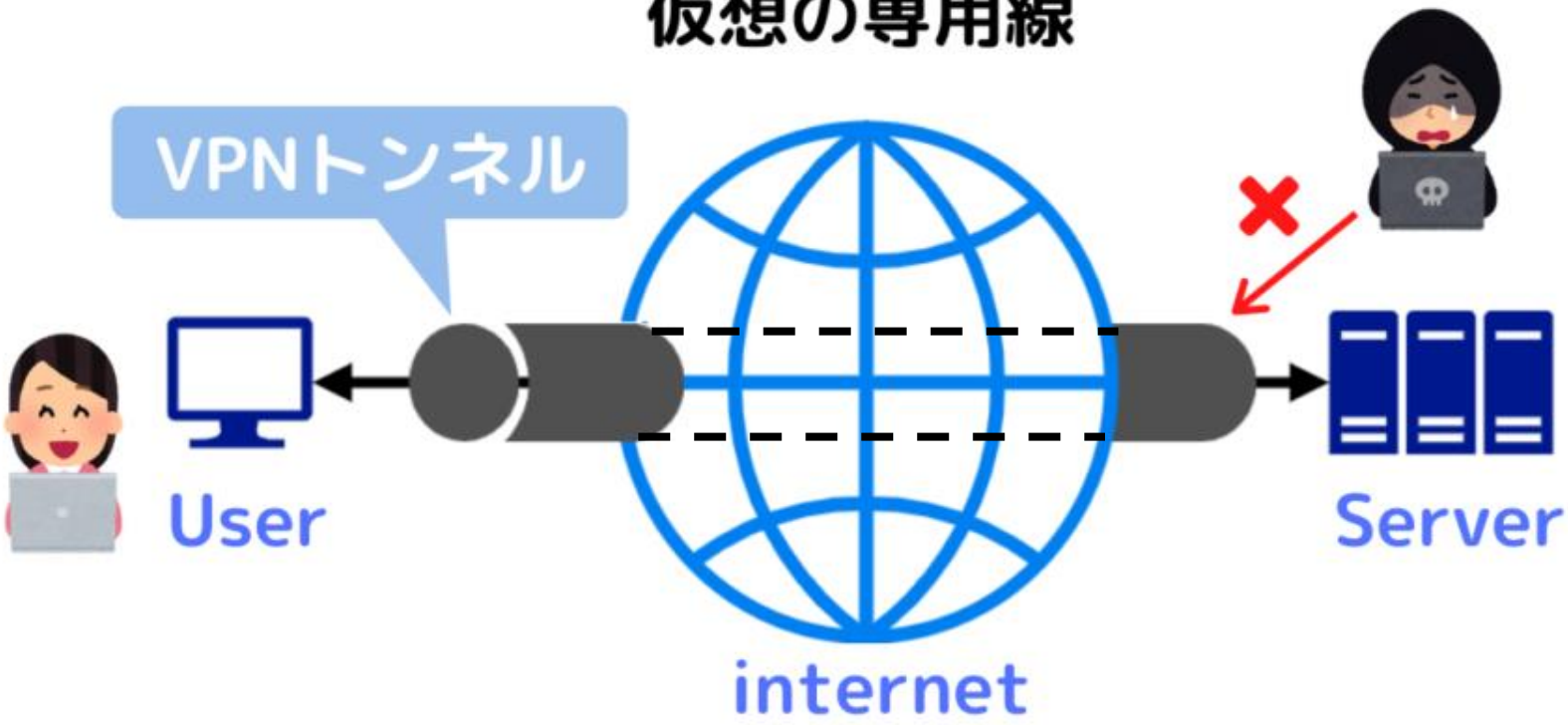
VPNはVirtual Private Networkの略称で仮想専用線とは？

インターネット上でデータを安全にやり取りするためには、Webベースの暗号化接続方式であるSSL通信や物理的な専用線の構築が使われてきました。
しかしSSL通信には通信品質の確保や、なりすましによる通信の改ざんリスク、物理的な専用線には敷設・管理コストが非常に高価という課題がありました。
それに対してVPNは一定の通信品質を確保しつつ、通信傍受や盗聴のリスクを避けることができる技術として、世の中に広く普及しています

送信側、受信側にそれぞれに設置した機器で「カプセル化」と呼ばれる処理を行うことで、第三者には見えない仮想的なトンネルを形成して通信する仕組みです（トンネリング）

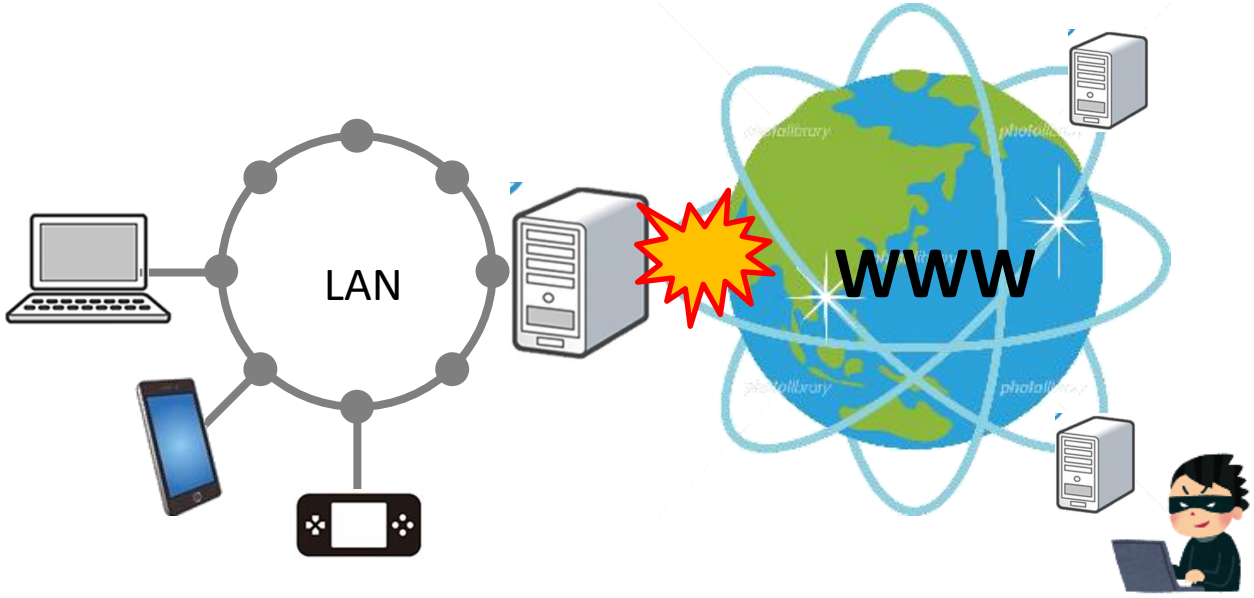
VPN = Virtual Private Network

仮想の専用線



リスク対策

ネット接続のリスクを認識する



①OS，ソフトウェア　は常に最新の状態にしよう

②ウィルス対策ソフトを導入しよう

③パスワードを強化しよう

④怪しいHPには接続しない

⑤不審なメールを見極める力をつけよう

①OS、ソフトウェアを最新に保つ

ソフトウェアには、時間の経過とともに、セキュリティーホール（脆弱性）と呼ばれる不具合個所が発見されます。

脆弱性は、プログラムの仕様要件や設計ミスに起因する品質問題です。

発見されるたびに、それを修正するための修正プログラムがアップデートされて配布されています

②ウィルス対策ソフトを導入

ウイルス対策ソフトを導入すれば万全ということではありませんが。

ウイルスも日々進化しており、対策ソフトのアップデートが間に合わないことも少なくありません。対策ソフトは手段のひとつでしかありません

③パスワードPWを強化する

危険なパスワード

(1) 8文字以下

(1) 自分の名前
Yamada、taro、（名前）
Ishikawa wajima（住所）
Taro （ペットの名前）

(2) 一般的な英単語
password、baseball、

(3) わかりやすい並び
0000 （同じ文字の組み合わせ）
123456、（安易な数字や英文字の並び）
asdf、qwerty（キーボードの配列）

(4)生年月日、社員コード

安全なパスワード

・10桁以上、14桁以上望ましい

・大文字＋小文字＋数字＋特殊記号　の組合せ

&, @, “,?, ^, -, %, !, #, $, *

ReyNum@2300%Turb!

・ﾊﾟｽﾜｰﾄﾞを使いまわさない

・ﾊﾟｽﾜｰﾄﾞ生成ﾂｰﾙ、管理ﾂｰﾙをつかう

④怪しいホームページにはアクセスしない

・http で始まるURLサイトは危険

× http　暗号化されない、個人情報は素通り
〇 https　暗号化される

鍵のアイコンで確認できる

・怪しいネットショップ　ある商品が激安、お得感満載
クレジットカード決済ができない
@gmail.com、@yahoo.co.jp、などのフリーメールを使っている
日本語が不自然

・偽サイト×　amazon-co-jp.pw
〇　amazon.co.jp

・アダルト系、出会い系

闇サイト、怖い宗教団体

⑤メール添付ファイルからウィルス感染対策

受信側としての注意

・不審メールに気付く、開けない

・添付ファイルのあるメールには厳重注意

・メールのやり取りのある発信元、実在の会社組織名からのメールも疑ってかかる

A社様からのメール
この添付ファイル
何だろう？

発信側としての注意

・メール本文で済ませる、添付文はつけない

情報セキュリティー〇カ条

①OS，ソフトウェア　は常に最新の状態にしよう

②ウィルス対策ソフトを導入しよう

③パスワードを強化しよう

④怪しいHPには接続しない

⑤不審なメールを見極める力をつけよう

社員のセキュリティリテラシーが最後の砦になる

動画視聴　IPAあなたの会社のセキュリティー女医　6分30秒以降

ソフトウェアの品質

ISO25000
ソフトウェア製品の品質要求と評価

品質以前の商品性問題

IoT（Internet of Things）における品質課題

SEC
Software Reliability Enhancement Center

想定する利用者と、製品が必要とする初期設定や操作の難易度が合っていない

開発時には想定されなかった使い方をされ不具合が発生する

通信路上の対策が不十分なため、情報が盗まれる、個人情報が漏えいする、第三者からシステムが乗っ取られる可能性がある

他の事業者が提供するサービスと同一環境で共存できない

新しい使い方に対する利用者のニーズがつかみきれず、想定する利用者にとって実用的で満足できるサービスになっていない

デバイスの種類が多く、動作プラットフォームとして指定した組み合わせの全てを検証できない

利用者の身近で動作する製品の不具合で、身体的、金銭的な危害を及ぼす事故の可能性がある

市場適合性の検証ができないまま商品化している現状

ISO/IEC 25000シリーズ、JIS X 25000シリーズ （SQuaRE）

SEC Software Reliability Enhancement Center

- 名称：ソフトウェア製品の品質要求及び評価
  Systems and software Quality Requirements and Evaluation
- 組織：ISO/IEC JTC1 SC7/WG6
- 概要：システム及びソフトウェアの多岐にわたるステークホルダ（利用者、発注者、開発者など）が持つ多様な品質要求を定義し、その実装を評価するための共通の考え方を示す国際規格

SQuaREの構造

SQuaRE活用のポイント

SEC
Software Reliability Enhancement Center

- **品質要件の明確化**
  - 品質は高ければよいというものではない（適正品質の確保）
  - 品質モデルを使って網羅性を考慮しつつ、細分化することで管理が容易になる
- **品質計画の明確化**
  - 定量的な目標設定と評価計画
  - どの開発工程でどの品質をどれだけ作り込むか
- **重要な品質特性（副特性）を選択**
  - 想定利用者や製品戦略等に従い優先順位をつける
- **標準的なモデルを利用することで再利用を可能に**
  - 開発手法の普及、定量的品質管理などを組織的な取り組みに

リスク危機感、責任感が感じられない

IPA／SECの取り組み

SEC
Software Reliability Enhancement Center

品質説明のステップ

- 品質要求の定義
- 設計、製造
- 検証（エビデンス収集）
- 第三者による評価（認証）
- 利用者への説明

「つながる世界のソフトウェア品質ガイド」（2015年6月書籍発行済み）

製品・サービスを提供する事業者が理解しておくべき品質に関する基本的な知識と、国際規格SQuaREの活用についてわかりやすく解説

「ソフトウェア品質説明のための制度ガイドライン」（平成25年6月公開済み）

第三者が品質を評価する制度の設計において考慮すべき事項を記載（43項目）

認証制度が作れるのか
MRJでは完成できなかった

IPA
情報処理推進機構

IPA

Information-technology　Promotion Agency

情報処理推進機構

情報処理の促進に関する法律に基づき、IT社会推進のための技術や人材についての振興を行うために

1970年10月に特別認可法人情報処理振興事業協会として創立された

2004年に独立行政法人（経済産業省所管）として、現在の形に改組された

主な事業は

①IT分野の技術開発の支援、

②IT人材の育成、検定制度の運営

③情報セキュリティについての調査・研究や情報発信

②人材育成分野では、国家試験の「情報処理技術者試験」を実施している

・天才プログラマの発掘を目指す「未踏ソフトウェア創造事業」、

「未踏ユース」（若年層対象）、

・「セキュリティ・キャンプ」学生対象のセキュリティ教育合宿

なども行っている。

③情報セキュリティ関連では、

セキュリティセンター（ISEC）、産業サイバーセキュリティセンター(ICSCoE）などの部局を抱え、

・セキュリティ知識の啓発活動、「情報セキュリティー白書」「DX白書」の発行

・「情報処理安全確保支援士試験」の実施、

・ソフトウェア脆弱性データベースの「JVN」（Japan Vulnerability Notes）の運営、

・サイバー情報共有イニシアティブ（J-CSIP）の主催、

・ITセキュリティ評価及び認証制度（JISEC）の運営などを行っている

2021年刊行

DX白書2021
日米比較調査にみるDXの戦略、人材、技術

2021年12月1日　印刷書籍版 第1版発行

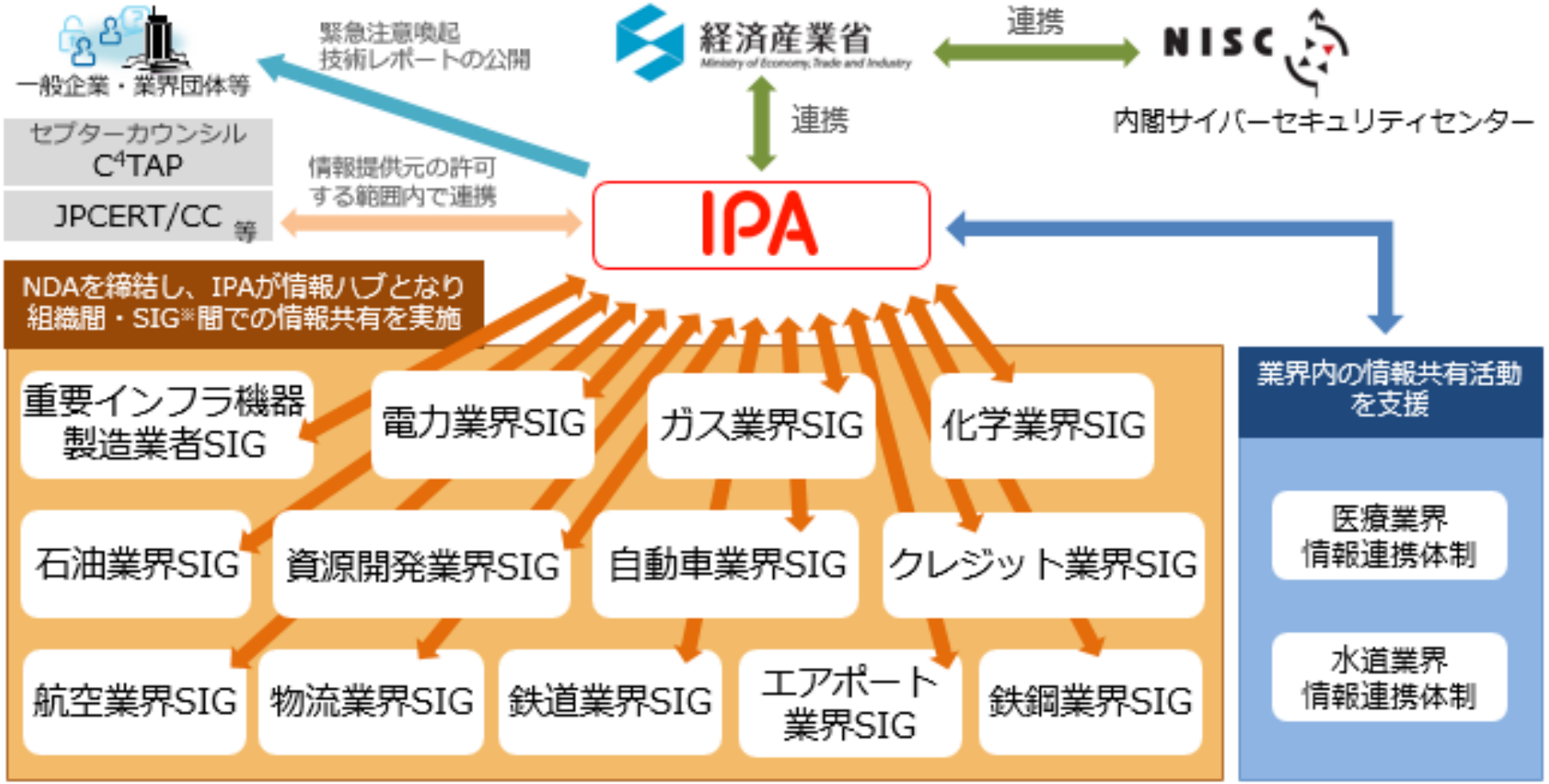
企画・著作・制作・発行

独立行政法人情報処理推進機構（IPA）

〒113－6591 東京都文京区本駒込2-28-8
文京グリーンコートセンターオフィス 16階
https://www.ipa.go.jp/

サイバー情報共有イニシアティブ J-CSIP

J-CSIP（ジェイシップ）は、IPAを情報ハブ（集約点）として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく取り組みです。
IPAと各参加組織、業界団体間での秘密保持契約（NDA）の締結等により、参加組織およびそのグループ企業において検知されたサイバー攻撃等の情報をIPAに集約し、参加組織間での情報共有を行っています。



※SIG: Special Interest Group の略

動画視聴　町田啓太サイバー攻撃　5分

第4回

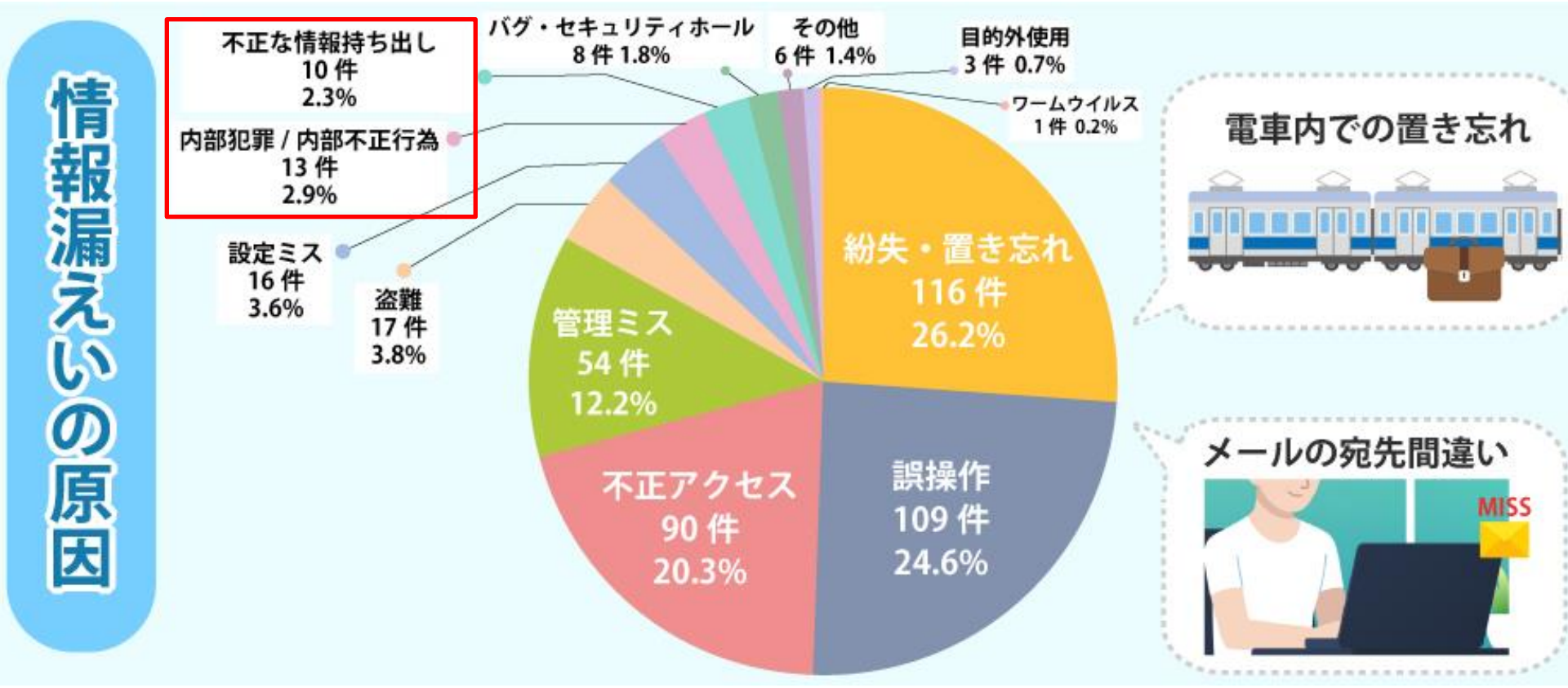
内部不正問題

内部不正の問題

情報漏えいの原因、6割は従業員のうっかりミス

基本的な心得の徹底が重要

5%



参照：2018年 情報セキュリティインシデントに関する調査報告書 | JNSA（日本ネットワークセキュリティ協会）

社員の情報セキュリティ意識
組織内部の不正

動画視聴　IPA新入社員3つのかばん　　前半2分まで

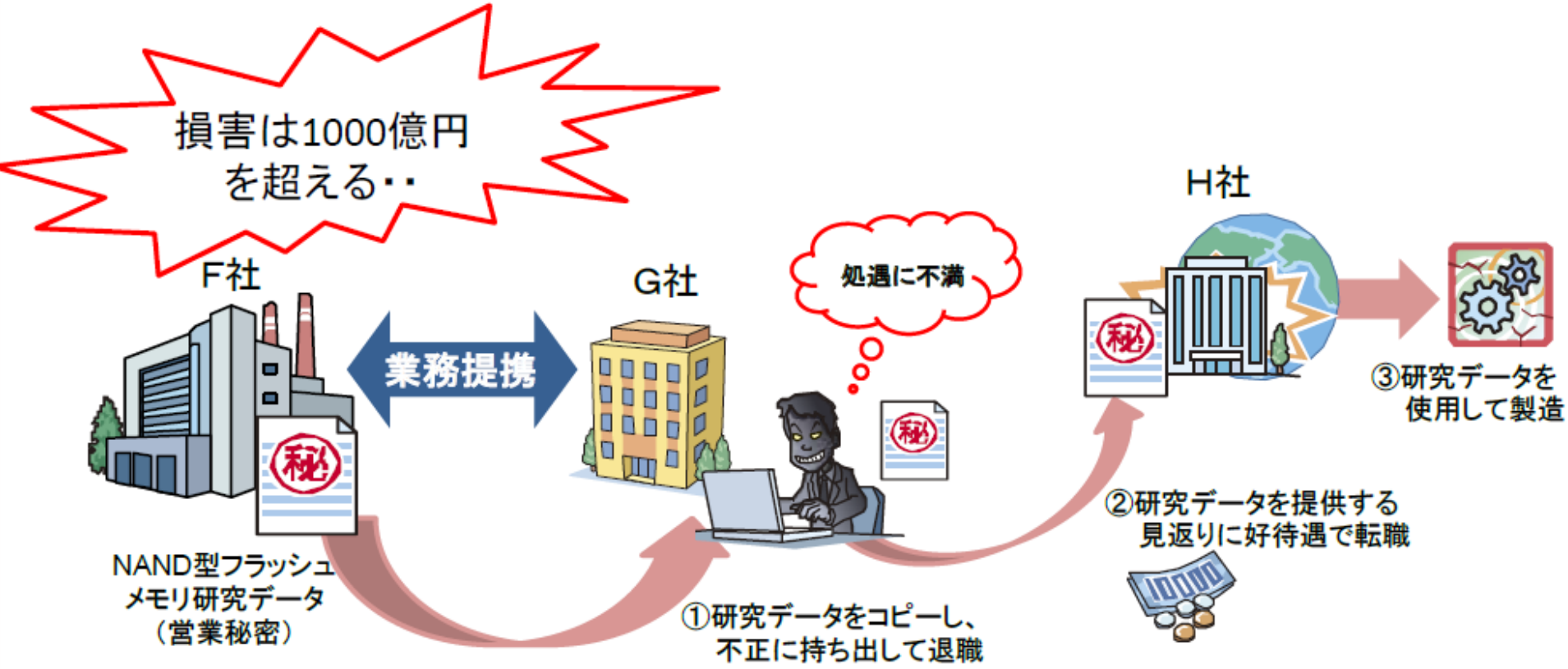
退職・転社社員による
情報持ち出し

機密

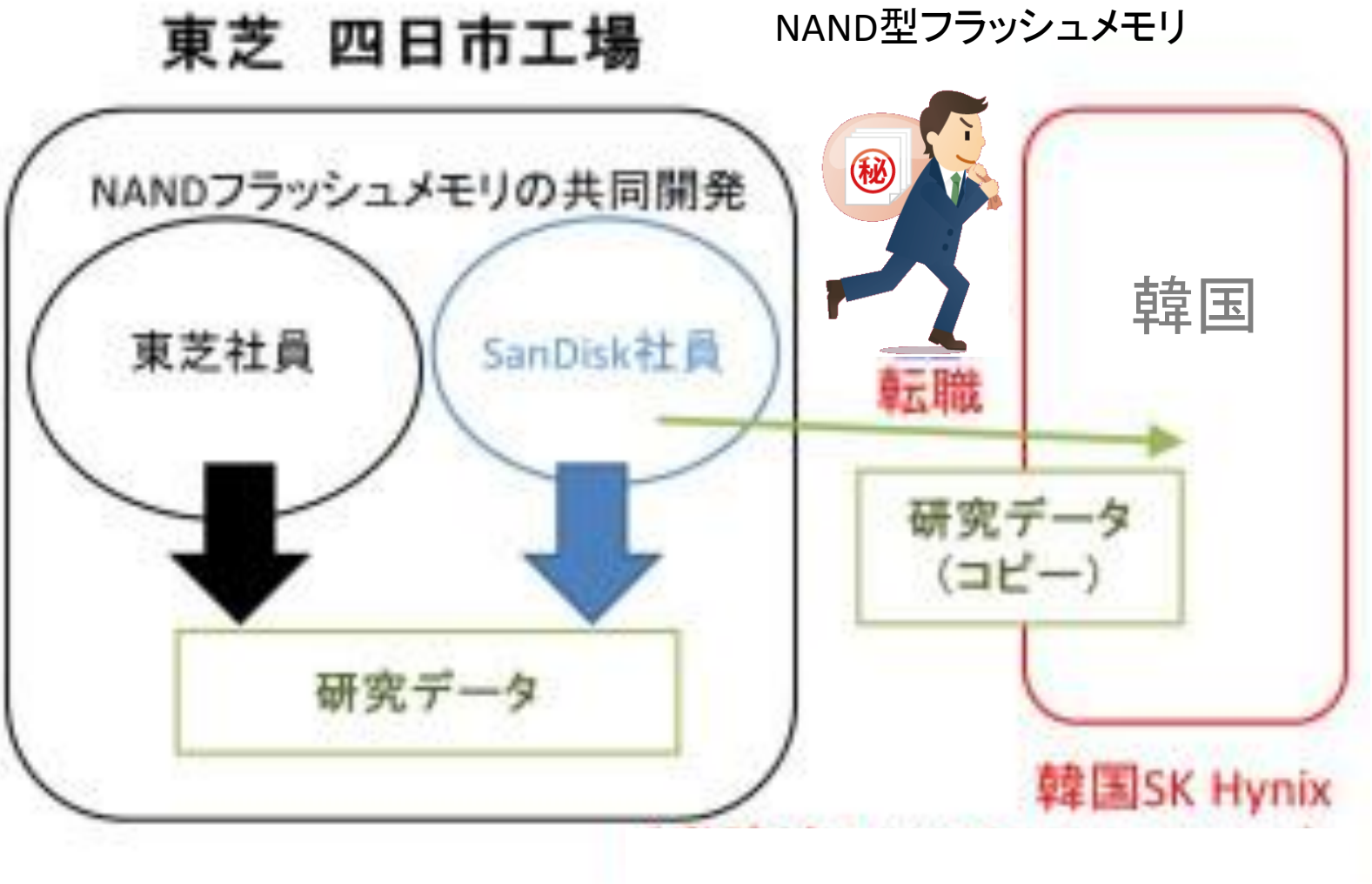
事例1

エンジニア転社　機密持ち出し

2014年3月、F社のフラッシュメモリーの研究データを不正に持ち出し、転職先である韓国の半導体大手H社に提供したとして、F社と業務提携していた半導体メーカー G社の元技術者が、不正競争防止法違反（営業秘密開示）容疑で逮捕された。

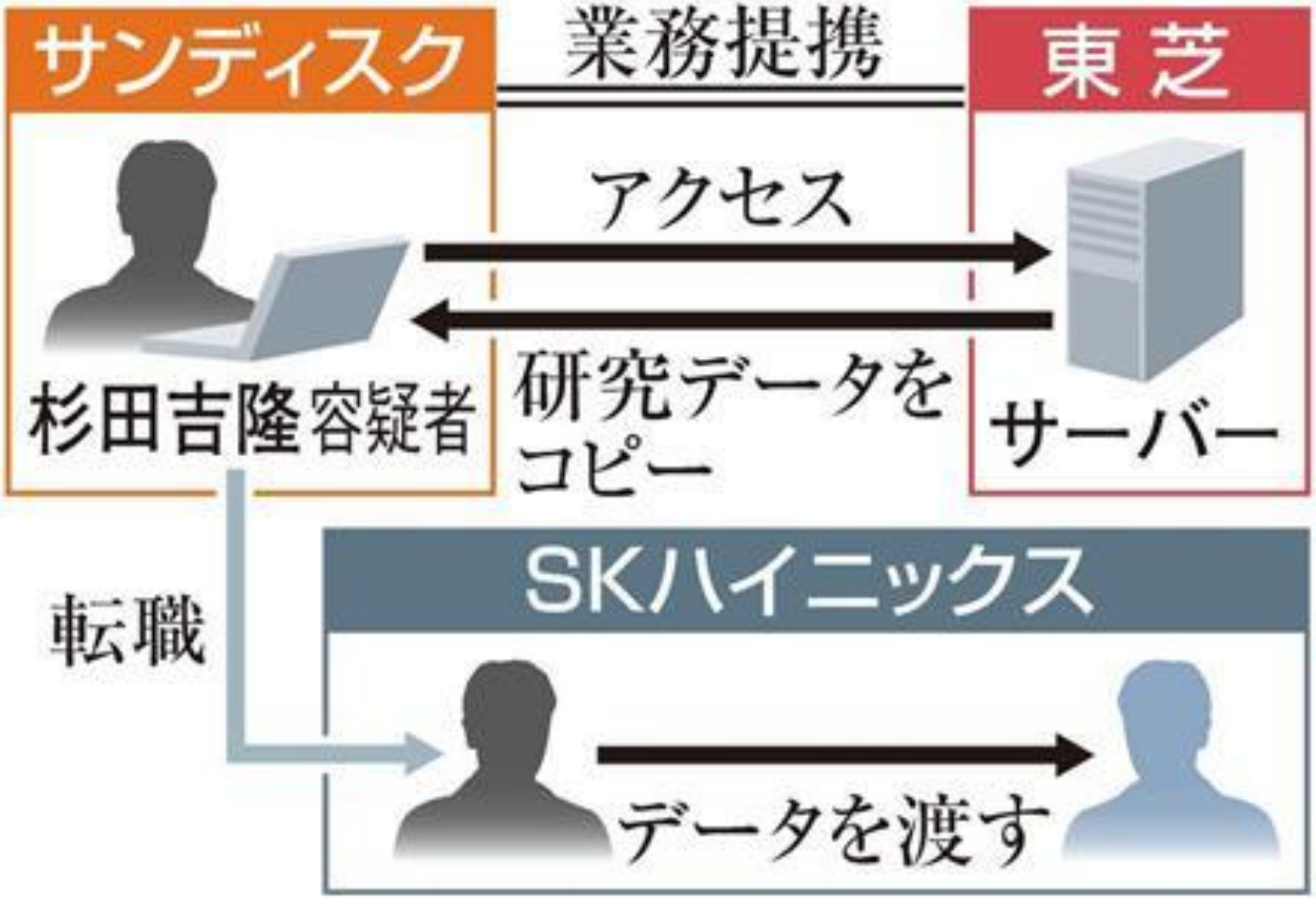


エンジニア転社　機密持ち出し



https://pc.watch.impress.co.jp/docs/column/semicon/640888.html

研究データ漏洩事件の構図



エンジニア転社　機密持ち出し

東芝は2014年3月13日、NAND型フラッシュメモリの技術に関する機密情報について、韓国のSKハイニックスを提訴した。不正競争防止法に基づき損害賠償等を求める民事訴訟を東京地方裁判所に提起した。

2008年当時、彼はサンディスクの従業員として東芝の四日市工場内で共同開発に従事していた。退職する際、機密情報を不正に持出し、SKハイニックス社に転社した。その情報がSKハイニックス社で使用されていたとして、不正競争防止法違反の容疑で逮捕された事実を受けて提訴したもの。

東芝とSKハイニックスは、現在提携・取引関係にある一方で、NAND型フラッシュメモリの分野では互いに競争関係にあり、NAND型フラッシュメモリに関わる機密情報が漏洩した疑義が生じ、調査を進めていた過程から発覚したとしている。

2014年3月14日にNHKニュースは、東芝から不正に持ち出されたのは絶縁膜の材料に関するデータだと報じた。NANDフラッシュメモリの絶縁膜材料に関するデータは製造ノウハウ(特に信頼性)に直結しており、きわめて重要な技術である。例えば、ゲート絶縁膜(トンネル絶縁膜)、インターポリ絶縁膜(浮遊ゲートと制御ゲートの間にある絶縁膜)、素子分離絶縁膜(隣接するメモリセルを電気的に分離する絶縁膜)の品質は、メモリの性能を大きく左右する。SK Hynixがこれらのデータに高値を付けたとしても、不思議ではない。

東芝は、NANDフラッシュメモリー技術に関する機密情報を韓国SK Hynix社が不正に取得・使用したとして東京地方裁判所に提起していた民事訴訟について、2014年12月19日に同社との和解に合意した。この合意に基づき、東芝はSK Hynix社から和解金2億7800万米ドル（約330億円）を受け取る。

事例2　元ソフトバンク社員の転社時機密情報持ち出し

2020年
転社

SoftBank

楽天モバイル

コロナテレワークの当時

動画視聴　TVニュース

当社元社員の逮捕について

2020年1月25日
ソフトバンク株式会社
SoftBank

本日、当社の元社員が、警視庁に不正競争防止法違反の容疑で逮捕されました。

このような事件が発生し、お客さま、株主の皆さま、ならびに当社に関係する全ての方々に多大なるご心配とご迷惑をおかけしましたことを深くお詫び申し上げます。

当社が現在認識している事柄は以下の通りです。

- 当該元社員が、当社の作業文書等を無断で社外に持ち出していたこと
- 持ち出された文書は機密性が低く、機密性の高い情報（お客さまの個人情報、通信の秘密に関わる情報、当社の取引先に関する情報等）は一切含まれていないこと
- 当該元社員は、上記の機密性の高い情報へのアクセス権限を保持していなかったこと

また、社内で検証した結果、当社のシステムやネットワークに対する外部からの不正アクセスの形跡や、不正プログラムなどの検知はありませんでした。

2021年2月22日
元ソフトバンク社員の機密情報持ち出し、内部不正

被告はソフトバンク社では携帯電話基地局の設置工事業務などに従事していた。
警視庁は、楽天モバイル側から容疑者に対してスムーズな転職条件として営業秘密の不正持ち出しの指示があり、計画的に営業秘密の持ち出しが行われたと見ている。

容疑者から押収したPCを解析し、約170のファイルを30回にわたり持ち出されて痕跡が確認されています
退職当日にも容疑者の自宅からソフトバンク社のテレワーク用のシステムを通じてクラウドサービスに接続し、営業秘密を含むファイルを自分のフリーメールアドレス宛に添付し送信を行い情報の持ち出しを行っている。
退職に際し集中的に特定の情報を収集しており計画的であると言わざるをえません

持ち出された情報
4G/5Gの基地局（マンション・私有地など）の設置場所
伝送網構築の工期短縮、設計コスト削減に関わる資料
NTT設置の光ファイバー回線網

ソフトバンクでは社員の入社時に秘密保持の誓約書を取得しており、そこには退職後を含めて「業務上の機密事項およびソフトバンクや取引先にとって不利益となる事項を漏洩しないこと」「ソフトバンクの組織上・企画上・営業上・技術上の情報について、事前の書面による許可なく、いかなる方法をもってしても開示、漏洩もしくは使用しないこと」などが明記してあり、被告の元社員も署名・なつ印のうえ、提出していた。
退職後にも機密情報を第三者に開示、漏洩しないことなどを誓約させていた

東京地方裁判所は、「携帯電話通信事業者にとって喫緊の課題となっていた5G化対応の計画など重要な情報が詰まった営業秘密を持ち出した悪質な犯行で、転職先での仕事に役立てようという動機も身勝手だ」として、懲役2年、執行猶予4年、罰金100万円の有罪判決を言い渡しました

事例3

かっぱ寿司事件

転社

国内の回転ずし事業の売り上げは、

▽最大手の「スシロー」を運営する「あきんどスシロー」が2132億円

▽2位の「くら寿司」が1315億円

▽3位の「ゼンショーホールディングス」の傘下にある「はま寿司」が1300億円

▽4位が「かっぱ寿司」を運営する「カッパ・クリエイト」で、529億円

かっぱ寿司運営会社社長ら逮捕 不正競争防止法違反容疑

2022年9月30日

田邊社長は、2020年11月に、役員を務めていた「はま寿司」の親会社からカッパ・クリエイトの顧問に転職し、副社長を経て2021年、社長に就任していた。

2020年9月から12月にかけて「はま寿司」の仕入れに関するデータをコピーして不正に持ち出し、自社のデータと比較して使用したなどとして、不正競争防止法違反の疑いが持たれています

不正競争防止法の「営業秘密」について

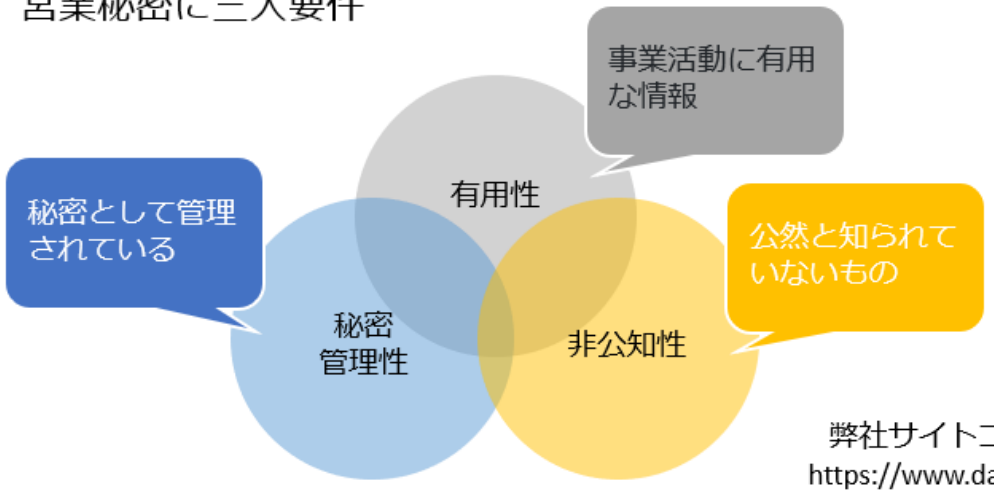
不正競争防止法とは

市場における競争の公平性を維持するため、競争の不正行為を禁止する法律
具体的に、風評や商品の模倣の禁止、営業秘密の保護などについて定められている
違反時は、差し止めや損害賠償請求を求めることができる

営業秘密とは

技術情報などの知的財産や営業情報など、社外に公開しない秘伝の機密情報

営業秘密に三大要件



「秘密管理性」の認定に厳しい傾向があり、過去の裁判でも認められないケースがあります。
秘密管理性を満たすためには、秘密としてその他の情報とは区別して、アクセス制限などを設けて管理する必要があります。

弊社サイトコラム：「特許」「営業秘密」による知的財産の保護について
https://www.dataclasys.com/column/intellectual_property_protection_20201228/

内部不正の原因分析

不具合事例

会社のメールアドレスから個人のメールアドレスに送ったり、クラウドストレージにアップロードしたりすることで、ソフトバンク社の5Gネットワーク情報が含まれた多数の電子ファイルなどを持ち出し、楽天モバイル社への転職に至った。
ソフトバンク社に大きな損害を与えた

事象を分解する

- システム上の不具合
  - ユーザ側
    - ・メールでデータを外部に送信することが出来たこと
    - ・自宅PCから営業機密情報へアクセスすることが出来たこと
  - 管理側
    - ・退職日までパスワードが変更されずにサーバーにアクセスが可能であったこと
    - ・適切なログ管理がなされていなかったこと
- 人事労務上の不具合
  - ・機密保持契約書の内容が遵守されなかった事
  - ・競合他社への転社が可能であった事
  - ・退職の目論見を確認できていなかった事

【技術的要因】

①不正を起こすことが技術的に可能、セキュリティが構築できていない

・権限を持たない従業員、派遣社員、委託社員が重要な情報に簡単にアクセスできてしまう状況はリスクが高いと言えます

②内部不正をしても見つからない、隠すことができる環境の存在

・エラーが表示されてもログなどが記録されておらず追跡できないといった状況

従業員に認知された場合、内部不正が起こるリスクが高まります

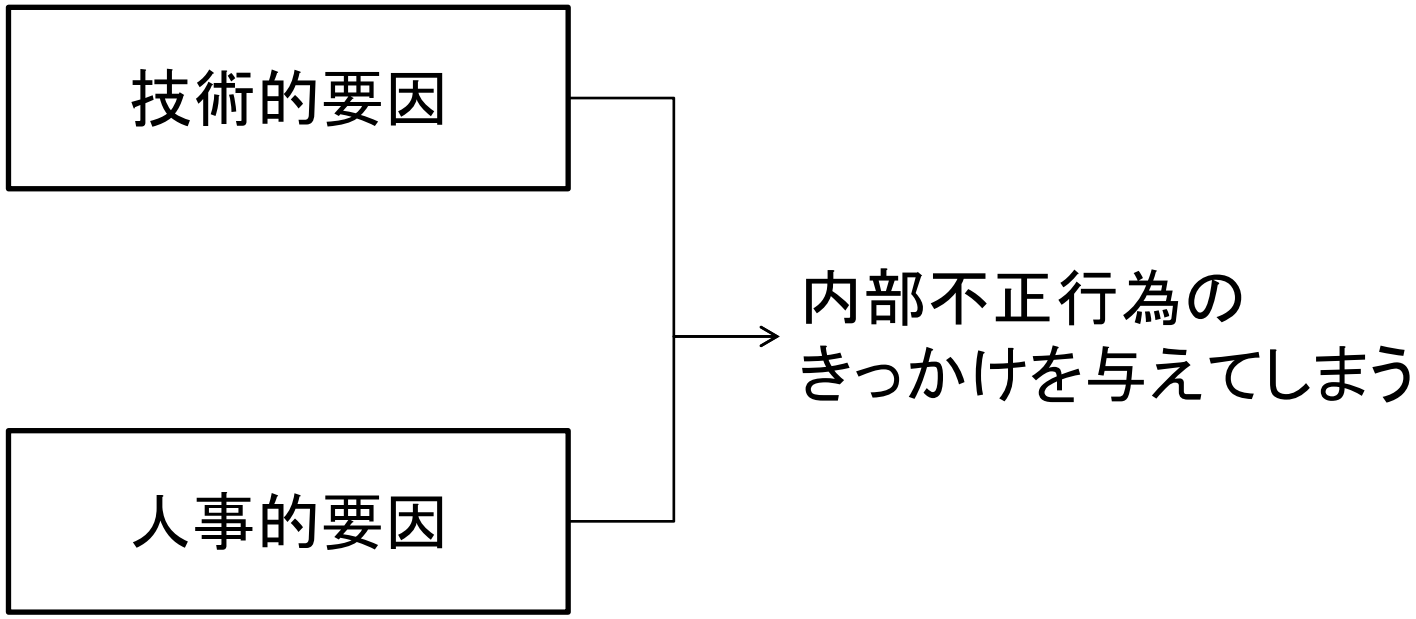
【人事的要因】

③組織体制や人事評価に対する従業員の不満、過剰なノルマへのプレッシャー等

内部不正を行う動機や、不正を正当化する理由が顕在化している

不満が社内から聞こえてくる場合、内部不正が起こりやすくなっていると言えます。

復讐・逆恨み的な内部不正が発生しやすくなります


技術的要因
人事的要因
内部不正行為の
きっかけを与えてしまう

IPA（独立行政法人情報処理推進）が2015年に行った調査

内部不正のきっかけを作ってしまう要因として、

「不当だと思う解雇通告を受けた」34.2%、

「給与や賞与に不満がある」23.2%、

「社内の人事評価に不満がある」22.7%

処遇や人事評価に関する項目ほど回答数が高い傾向がみられた

□会社としての意識改革を

退職者の管理不備を改める

情報セキュリティーに関するシステムマネージメントISMSを発展させる

企業の体質改革、従業員がより働きやすい環境を作る

第5回

内部不正対策

内部不正の特徴

1、社外からの攻撃よりも被害額が大きくなりやすいこと

ビジネスにおける直接的な損失や、信頼低下、売り上げ低下、内部不正に関わる調査費用なども含まれます。

2、表に出てこない内部不正事例も多数存在すると推測されること

IPAの調査によると、内部不正を行った者に対して「懲戒処分や起訴はしなかった」と回答した割合は、30.9%に上りました。内部不正をしていた事実が会社のイメージダウンにつながることを懸念することが大きな要因です。

3、故意ではない内部不正も多いこと

IPAの調査によると、内部不正を行った理由のうち、故意ではない「うっかり違反」が40.5%、「ルールを知らなかった」が17.5%、合計58.3%と半数以上を占めます。

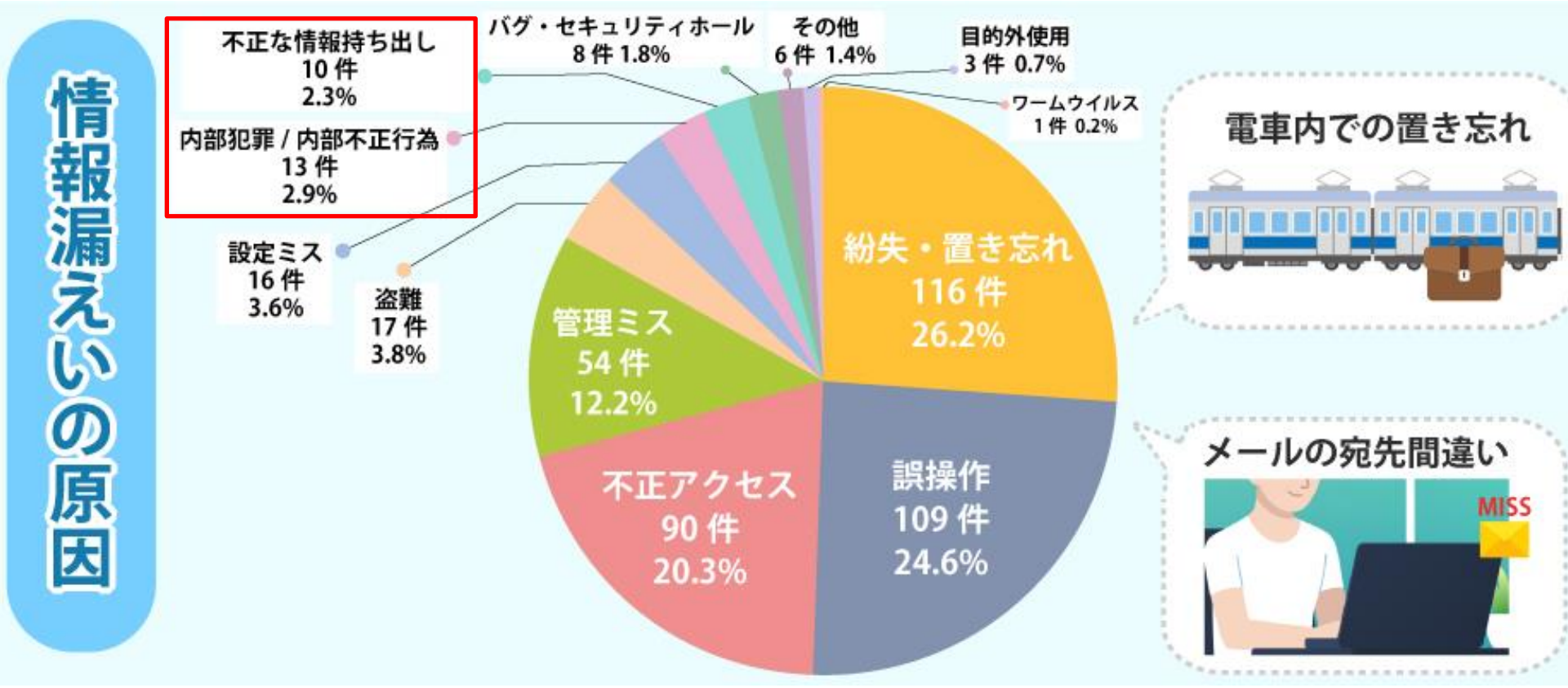
参考：組織における内部不正とその対策　情報処理推進機構

企業の内部不正対策

情報漏えいの原因、TOP5のうち4つは従業員のうっかりミス

基本的な心得の徹底が重要

5%



参照：2018年 情報セキュリティインシデントに関する調査報告書 | JNSA（日本ネットワークセキュリティ協会）

機密情報保持契約

Non Disclosure Agreement

機密保持、守秘義務　　契約書サンプル

1．従業員等の入社時

秘密保持に関する誓約書

この度、私は、貴社に採用されるにあたり、下記事項を遵守することを誓約いたします。

記

第１条（在職時の秘密保持）
貴社就業規則及び貴社情報管理規程を遵守し、次に示される貴社の秘密情報（＊１）について、貴社の許可なく、不正に開示又は不正に使用しないことを約束いたします。
①　製品開発に関する技術資料、製造原価及び販売における価格決定等の貴社製品に関する情報
②　（以下略）

第２条（退職後の秘密保持）
前条各号の秘密情報については、貴社を退職した後においても、不正に開示又は不正に使用しないことを約束いたします。退職時に、貴社との間で秘密保持契約を締結することに同意いたします。

第３条（損害賠償）
前二条に違反して、第一条各号の秘密情報を不正に開示又は不正に使用した場合、法的な責任を負担するものであることを確認し、これにより貴社が被った一切の被害を賠償することを約束いたします。

第４条（第三者の秘密情報）（＊２）

１．第三者の秘密情報を含んだ媒体（文書、図画、写真、ＵＳＢメモリ、ＤＶＤ、ハードディスクドライブその他情報を記載又は記録するものをいう。）を一切保有しておらず、また今後も保有しないことを約束いたします。

２．貴社の業務に従事するにあたり、第三者が保有するあらゆる秘密情報を、当該第三者の事前の書面による承諾なくして貴社に開示し、又は使用若しくは出願（以下「使用等」という。）させない、貴社が使用等するように仕向けない、又は貴社が使用等しているとみなされるような行為を貴社にとらせないことを約束いたします。

第５条（第三者に対する守秘義務等の遵守）（＊２）

貴社に入社する前に第三者に対して守秘義務又は競業避止義務を負っている場合は、必要な都度その旨を上司に報告し、当該守秘義務及び競業避止義務を守ることを約束いたします。

（＊３）

以上

平成　　年　　月　　日

株式会社＿＿＿＿＿＿＿＿

代表取締役社長＿＿＿＿＿＿＿＿殿

住　所　＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿

氏　名　＿＿＿＿＿＿＿＿＿＿＿＿　印

秘密保持に関する誓約書（プロジェクト参加従業員用）

株式会社

代表取締役　　殿

私はこの度、貴社　　プロジェクト（以下「本件プロジェクト」という）の担当者として参画するにあたり、私が貴社入社時にお約束した秘密保持に関する誓約書を厳守するとともに、下記事項を誓約致します。

第１条（秘密保持の誓約）

私は貴社の許可なくして、社外はもちろん貴社従業員で本件プロジェクトに直接関与していない者に対しても、次の事項の秘密情報（以下「秘密情報」という）を開示、漏洩し、もしくは自ら使用しないことを約束致します。

①貴社において本件プロジェクトが遂行されている事実

②本件プロジェクト参加により知り得た別紙記載の一切の情報

③以上の他、貴社が特に本件プロジェクト秘密保持対象として指定した情報

第２条（公表後の秘密保持）

私は本件プロジェクトの結果が公表された後といえども、未公開の部分については前条記載の秘密情報を、貴社の許可なく、社外はもちろん貴社従業員で本件プロジェクトに直接関与していない者に対しても、開示・漏洩し、もしくは自ら使用しないことを約束致します。

第３条（秘密の譲渡）

第１条記載の秘密情報については、私がその秘密の形成、創出に関わった場合であっても貴社業務上作成したものであることを確認し、当該秘密に関する一切の権利が貴社にあることを確認致します。また当該秘密に関し私に帰属する一切の権利を貴社に譲渡し、貴社に対し当該秘密が私に属する旨の主張を致しません。

第４条（資料の返還等）

私は、前各条を厳守するため、本件プロジェクト参加の過程で、貴社により、保管を許された資料一切の保管を厳重に行うことを約束し、貴社により返還を要求された場合、または私が本件プロジェクトからその理由を問わず離脱した場合は、これらの資料及びそのコピー並びにそれらに関する資料の一切を直ちに返還することを約束致します。また本件プロジェクト離脱後も、第１条記載の秘密情報を開示、漏洩もしくは使用しないことを約束致します。

第５条（退職後の秘密保持）

貴社を退職した後といえども、第１条記載の秘密情報を開示、漏洩もしくは使用しないことを約束致します。

年　　月　　日

住所

氏名

動画視聴　IPAあなたの会社のセキュリティー女医　6分30秒以降

IPA Better Life with IT 情報処理推進機構

「企業における営業秘密管理に関する実態調査2020」報告書について

https://www.ipa.go.jp/files/000089191.pdf

調査概要

(1) 調査期間：2020年10月12日～11月27日
(2) 企業への郵送アンケート実施：調査票数 16,000件　回収数 2,175件

	製造業	非製造業
大規模企業（従業員301名以上）	304社	438社
中小規模企業（従業員300名以下）	583社	785社

独立行政法人情報処理推進機構（IPA）が発表した

「企業における営業秘密管理に関する実態調査2020」報告書によると、

情報漏えいで最も多いルートは

「中途退職者による漏えい」

「現職従業員などの誤操作・誤認識等による漏えい」

といった内部不正に関するものでした。

実態把握

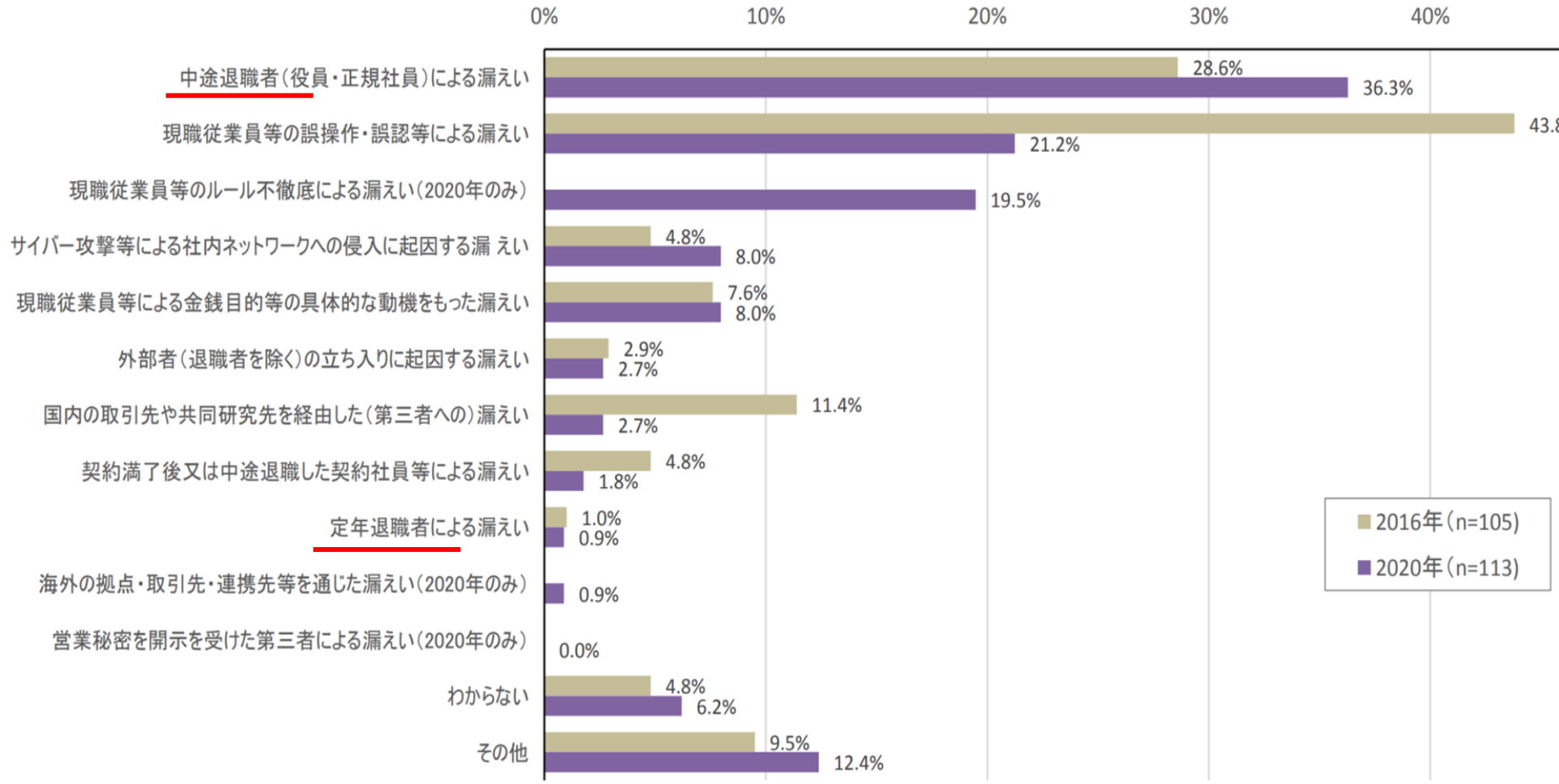


図 2.2-26　営業秘密の漏えいルート（経年比較）

中途退職者による漏えい　36%

課題認識

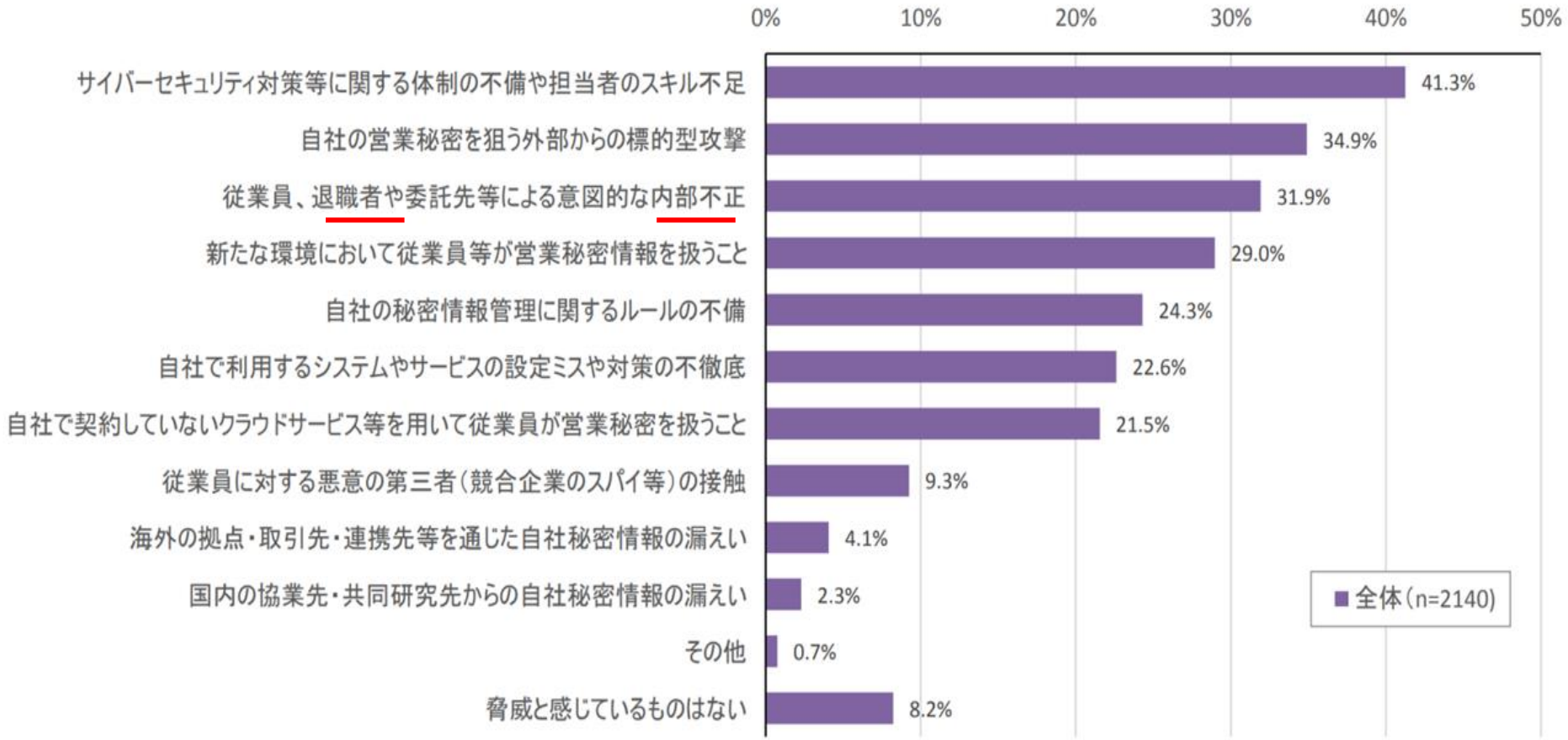


図 2.2-32　営業秘密の漏えいに関して、現在脅威と感じ、対策が必要と考えているもの

従業員、退職者、委託先による意図的な内部不正　31%

実施対策

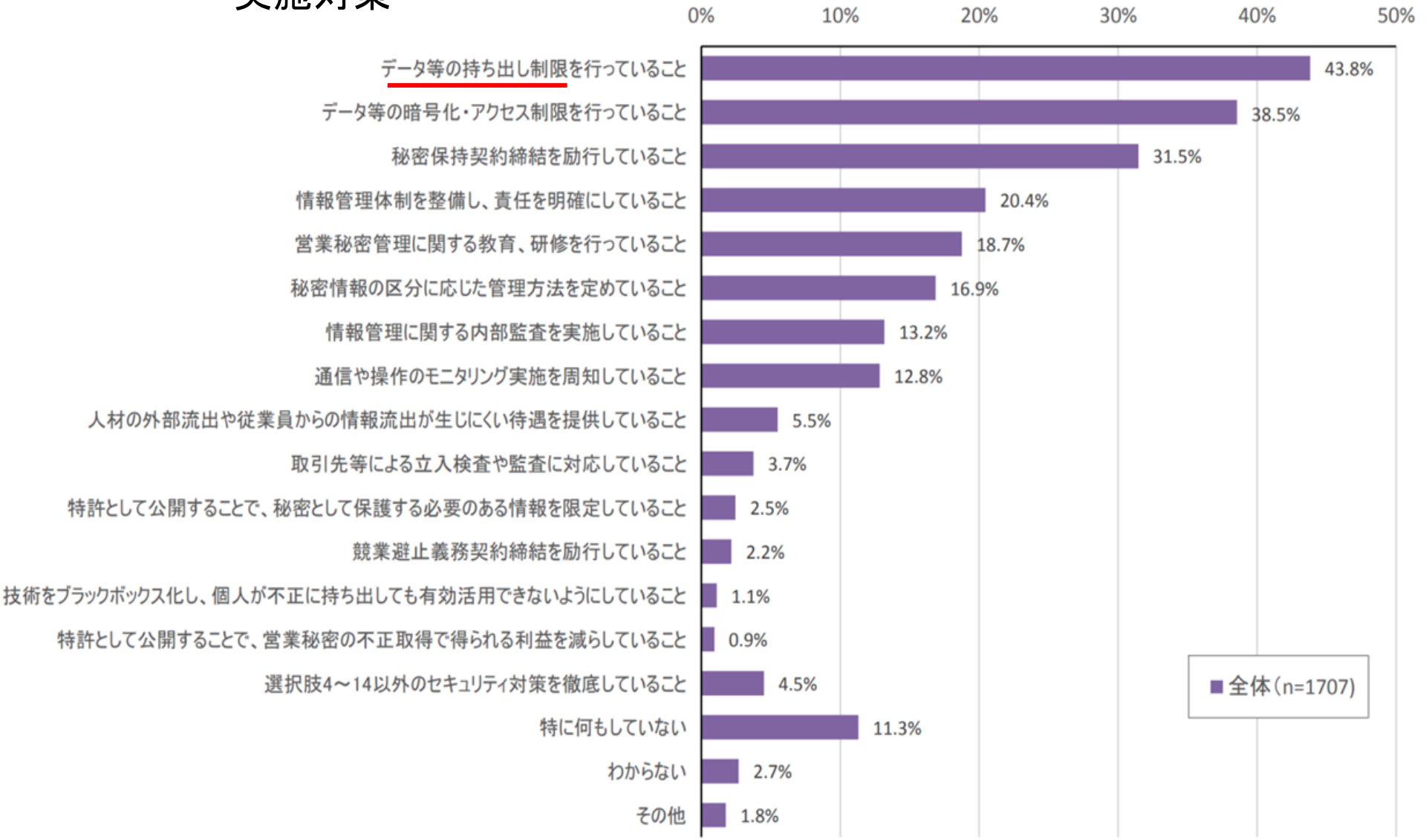


図 2.2-3(**ﾃﾞｰﾀの持出し制限　43%** ない要因

機密書類からの情報漏えいを防ぐために

以前は紙が危なかった

1. 印刷したらすぐに回収

2. 廃棄時はシュレッダーで

現在はUSBメモリーが危ない

企業の
情報セキュリティーポリシー

情報セキュリティポリシーとは、企業のセキュリティーに関する基本方針

策定の目的

①サイバー攻撃、情報漏えい、といったリスクから守るためです。

被害から守れるように、十分な設備やルールを整える必要があります。

②情報セキュリティポリシーの策定は、従業員の意識を高めることにもつながります

情報漏えい事件の多くは内部の人為的なミスが原因

「どのような情報を」「どのような理由で」「どのようにして」守らないといけないのか、

自分たちで考えて決めることで、セキュリティに対する意識自体が高まります

ISO27001の取得を目指すことも目標となります

安全対策と同じスタンス

情報セキュリティポリシーの内容は、「基本方針」「対策基準」「実施手順」
3階層に分かれる

・基本方針
“ポリシー”と呼ばれ「Why」にあたる内容。なぜ情報セキュリティ対策が必要なのか、どのような方針で取り組むのかといった内容であり、経営者の目的、目標から導き出されます。情報セキュリティポリシー全体の根幹になります。

・対策基準
“スタンダード”と呼ばれ「What」にあたる部分。どんな対策を実施するのか、
遵守すべき項目等、情報セキュリティ対策を行うためのルール集となります。
入退出の管理基準、セキュリティ教育基準、社内ネットワーク利用基準などです。

・実施手順
“プロシージャー”と呼ばれ「How」にあたる部分。個別の項目について具体的に実施する手順を記述します。マニュアルとなります。
入退出管理マニュアル、ウイルス対策ソフト導入手順、ネットワーク設定マニュアルなどです。

会社の理念、フィロソフィー

情報セキュリティポリシー

基本方針

対策基準

実施手順

IHI 社の
情報セキュリティー対策

組織名称	株式会社IHI
組織部門名称	高度情報マネジメント統括本部
所在地	東京都江東区豊洲3-1-1 豊洲IHIビル（本社）
認証基準	JIS Q 27001:2014(ISO/IEC 27001:2013)
認証登録番号	JUSE-IR-094
登録範囲	高度情報マネジメント統括の企画業務・構築業務・運用業務・業務評価の主要プロセスおよびプロセスで活用する情報資産、およびセキュリティ事業関連製品の営業、開発、調達、製造、修理およびサービスに関する情報資産 適用宣言書：2021年11月17日
初回登録日	2007年5月28日
有効期限	2025年5月27日
認証機関（認定番号）	一般財団法人日本科学技術連盟　ISO審査登録センター(ISR005)

IHIグループ情報セキュリティポリシー

方針

IHIグループは，お客さまやお取引先の機密情報，会社の経営情報や技術情報などを確実に保護するために「IHIグループ情報セキュリティポリシー」を定め，情報の適正な管理と情報セキュリティの維持・向上に取り組んでいます。

IHIグループ情報セキュリティポリシー

IHIグループが保有する情報資産の安全性を確保し，お客さまおよびユーザや社会との信頼関係を一層ゆるぎないものにするため，ここにIHIグループ情報セキュリティポリシーを定める。

（活動の基本）

1. IHIグループは，漏洩，盗難，紛失，破壊，不正な侵入，障害および災害等から情報資産を保護し，維持するために，適切な人的・組織的・技術的諸対策を講じる。
   万一情報資産にセキュリティ上の問題が発生した場合は，その原因を迅速に究明し，その被害を最小限に止めるように努める。

（情報資産）

2. 情報資産とは，媒体を問わずIHIグループが事業の活動の中で扱う情報，および情報を扱うために必要な装置･施設･サービスをいう。

（適用範囲）

3. IHIグループ各社の役員，従業員のほか，派遣社員等，IHIグループの情報資産を利用する者に対し本ポリシーを適用する。

（法令等の遵守）

4. IHIグループは，情報資産に関する法令，規範およびお客さまとのセキュリティに関する契約上の要求事項･義務を遵守する。

（教育）

5. IHIグループ各社は，IHIグループの情報資産を利用する者に対し，必要なセキュリティの教育を行ない，セキュリティ意識の向上および維持を図る。

（運用体制等）

6. IHIグループ各社は，情報セキュリティに関する規定を定め，情報管理の責任者を置く等，情報セキュリティの運用管理の仕組みを確立し，維持および改善を含めた活動を継続的に実施する。

（経営幹部の責任）

7. 経営幹部は，率先垂範して本ポリシーを実践するものとする。本ポリシーに反するような事態が発生したときには，自ら解決に当たり，原因究明，再発防止に努め，権限と責任を明確にしたうえで，適正に対処する。

（処分）

8. 情報セキュリティに関する規定に違反する事例が生じた場合には，IHIグループ各社の就業規則等により処分する。

（公表）

9. 本ポリシーは，IHIグループの情報資産を利用する者に対して公表･通知するとともに，一般にも公表する。

IHIグループ情報セキュリティポリシー

IHIグループが保有する情報資産の安全性を確保し，お客さまおよびユーザや社会との信頼関係を一層ゆるぎないものにするため，ここにIHIグループ情報セキュリティポリシーを定める。

（活動の基本）

IHIグループは，漏洩，盗難，紛失，破壊，不正な侵入，障害および災害等から情報資産を保護し，維持するために，適切な人的・組織的・技術的諸対策を講じる。万一情報資産にセキュリティ上の問題が発生した場合は，その原因を迅速に究明し，その被害を最小限に止めるように努める。

（情報資産）

情報資産とは，媒体を問わずIHIグループが事業の活動の中で扱う情報，および情報を扱うために必要な装置・施設・サービスをいう。

（適用範囲）

IHIグループ各社の役員，従業員のほか，派遣社員等，IHIグループの情報資産を利用する者に対し本ポリシーを適用する。

（法令等の遵守）

IHIグループは，情報資産に関する法令，規範およびお客さまとのセキュリティに関する契約上の要求事項・義務を遵守する。

（教育）
IHIグループ各社は，IHIグループの情報資産を利用する者に対し，必要なセキュリティの教育を行ない，セキュリティ意識の向上および維持を図る。

（運用体制等）
IHIグループ各社は，情報セキュリティに関する規定を定め，情報管理の責任者を置く等，情報セキュリティの運用管理の仕組みを確立し，維持および改善を含めた活動を継続的に実施する。

（経営幹部の責任）
経営幹部は，率先垂範して本ポリシーを実践するものとする。本ポリシーに反するような事態が発生したときには，自ら解決に当たり，原因究明，再発防止に努め，権限と責任を明確にしたうえで，適正に対処する。

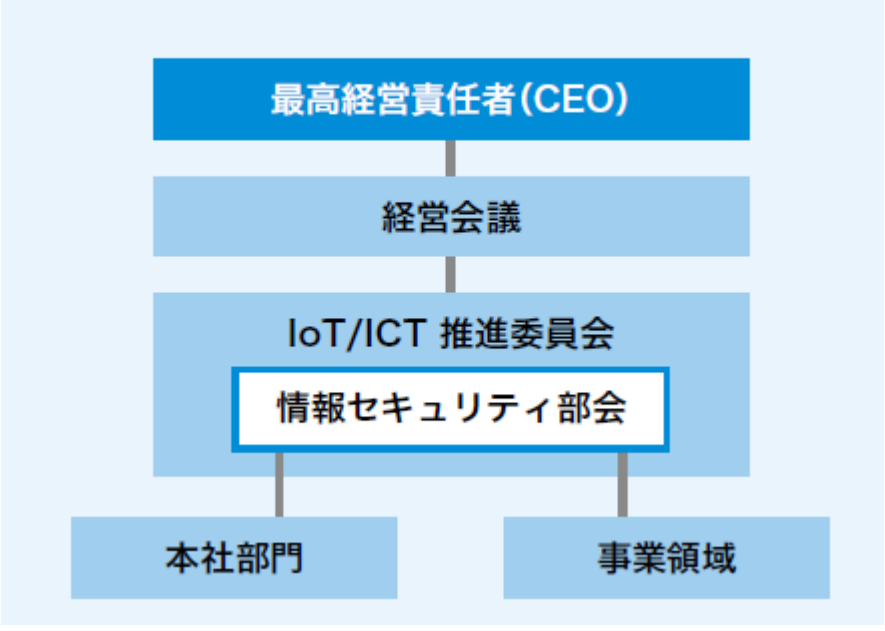
（処分）
情報セキュリティに関する規定に違反する事例が生じた場合には，IHIグループ各社の就業規則等により処分する。

（公表）
本ポリシーは，IHIグループの情報資産を利用する者に対して公表・通知するとともに，一般にも公表する。

体制

IHIグループでは，情報マネジメント関連事項担当役員を最高責任者とした情報セキュリティ推進体制を構築しています。IoT／ICT推進委員会に置いた情報セキュリティ部会を取りまとめ機関とし，IHIの本社部門・事業領域・SBUおよび関係会社ごとに統括管理責任者をおいて，情報セキュリティ活動に取り組んでいます。

情報セキュリティ活動推進体制図



実績

情報セキュリティ対策

IHIグループは，情報セキュリティのリスクに対してルール・ツール・教育の3つの側面から対策を実施しています。

ルール面では，「IHIグループ情報セキュリティポリシー」「情報セキュリティ対策基準」「情報システム利用者規程」などの諸規定を定めています。ツール面では，ウイルス対策ソフトウェアなどのセキュリティツールを導入し，適宜最新機種に更新しています。

情報セキュリティマネジメントシステム

IHIグループは，IHIの主要部門と主要なグループ会社で構成する情報セキュリティ部会を年3回開催し，情報セキュリティ対策の計画・実施・点検を1年サイクルで実施しています。

2019年度以降，PDCAにおける「C（Check）」機能の強化として，自組織・事業領域・コーポレート部門による3段階の情報セキュリティ監査体制を構築しています。自組織（IHIの各部門および関係会社）における内部監査，コーポレート部門による文書監査，主管部門である事業領域による監査をそれぞれ実施しています。2020年度の事業領域による監査では，SBU・関係会社10組織を監査し，発見された不備に対して事業領域が改善を指導しました。

IHIグループの中でも国の重要な業務に携わる部署およびグループ会社では，社外の専門機関による情報セキュリティの国際規格ISO27001の認証審査を毎年受け，高いセキュリティレベルの維持に努めています。

教育・浸透

従業員への教育

IHIグループは，情報セキュリティのルールやツールに対する従業員の理解を深めるためのe-ラーニングを毎年実施し，セキュリティ意識の維持・向上を図っています。

e-ラーニング受講率

（単位：%，対象：IHI）

項目	2017年度	2018年度	2019年度	2020年度
e-ラーニング受講率	98.0	96.8	83.0	96.0

在宅勤務における情報漏えい対策

2020年度は，新型コロナウイルス感染拡大防止対策としてIHIグループ全体で在宅勤務を開始しました。これまでのオフィスでの業務に比べてリモートワークが増え，働き方や働く環境の変化をねらったサイバー攻撃が増加しています。社外での業務におけるセキュリティ遵守事項について，e-ラーニングや社内報で，従業員への注意喚起を行なっています。具体的には，パソコンの私的利用の禁止や本人や家族が共有する情報機器（私有情報機器）への業務情報保存の禁止などが遵守事項となります。

IHIグループでは，従来から，業務データが保存されていない持ち出し専用のパソコンを用意し，社外での業務は原則的にこれを用いることとしています。在宅勤務時に持ち出し専用パソコンを使用することで，紛失・盗難による情報漏えいリスクを低減しています。

アンケート調査別紙（１／３）

平成２５年度卒業生　株式会社ＩＨＩ　勅使川原 祐二

IHI

＞＞道徳

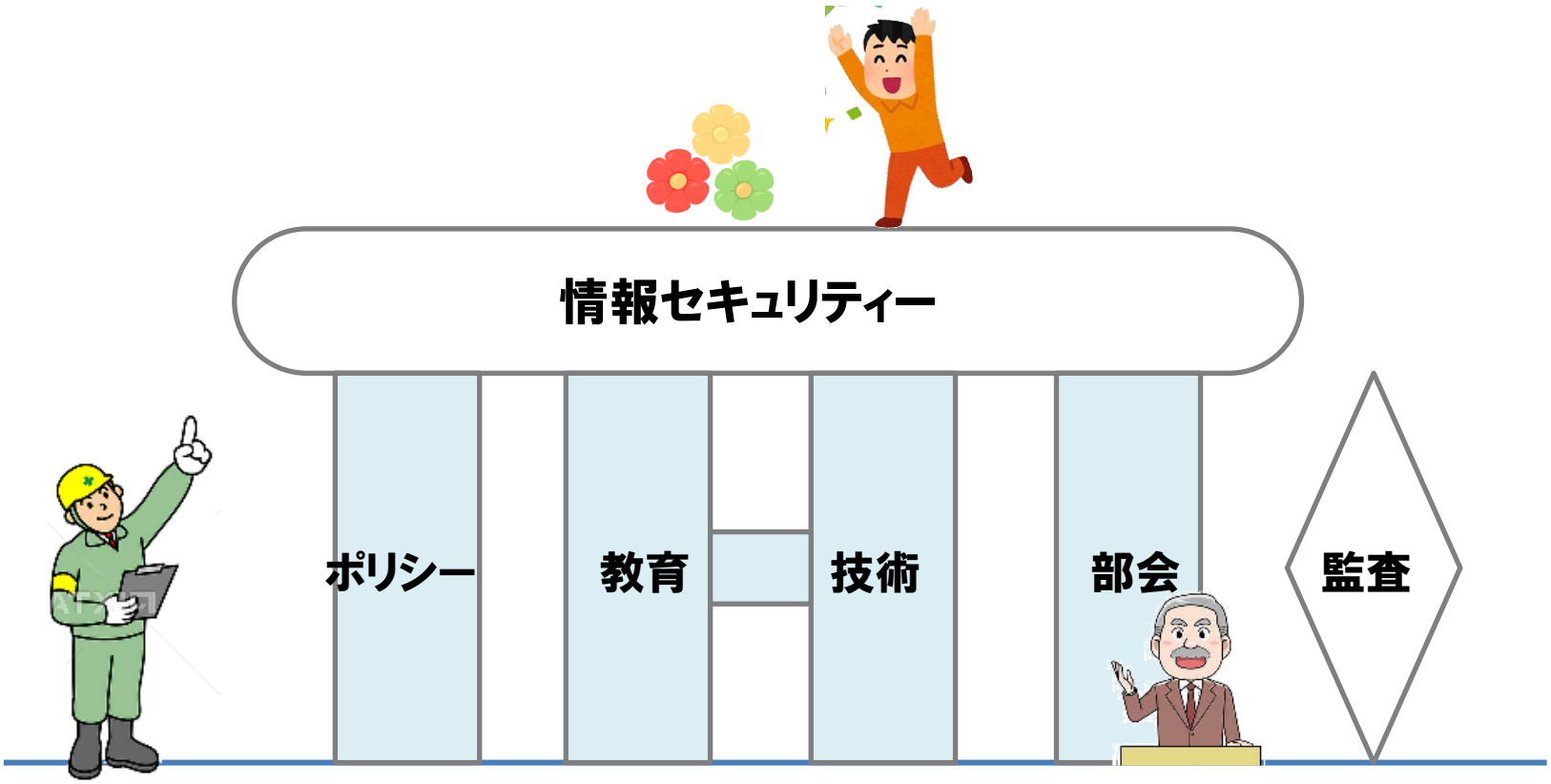
ご存じのことと思いますが、弊社は数年前に航空エンジン整備事業において不適切な検査行為を行いました（不適切事案の詳細は弊社ホームページのプレスリリース等をご確認下さい）。当時、弊社以外の自動車メーカや金属材料メーカも、同様の不適切な検査行為が散見される状況でした。不適切行為は“ルールを守る”という社会通念上当たり前の判断力を欠けていただけでなく、モノづくり企業に勤める技術者としての倫理観の欠如と言わざるを得ません。

製造業には“技術者倫理”と呼ばれる徳育に近い、倫理観があります。貴校は多くの人材を製造業界に輩出しており、E・M・K 科の学生には一般的な道徳教育のほかに技術者倫理は欠かすことのできない知識であると考えています。

＞＞ネットセキュリティー

報道でも話題になりますが、日本の企業はサイバー攻撃の対象となっています。不審なメールは開かない、OSやソフトウェアは適切にアップデートするなど、当たり前の行動が重要です。また、ウイルスを招き入れてしまったときの損害や社会責任の大きさも認識しておく必要があります。

当方、部内でOA キーマンと呼ばれる役割を担当していますが、残念ながら上述の意識が希薄な者が部内にも少なからずいます。社会人になる前からことの重大さを認識し、当たり前のことは当たり前にするための、ISMS教育が必要と痛感しています。


情報セキュリティー
ポリシー
教育
技術
部会
監査

日産様の社員教育

こんご、日産　からご提示いただく

動画視聴　IPA新入社員3つのかばん　　後半10分

第6回

情報技術者倫理

社員のコンプライアンス違反

不正のトライアングル

アメリカの組織犯罪研究者であるドナルド・R・クレッシー（Donald Ray Cressey）が提唱した、

動機

誘惑や欲求、仕事のストレスや不満、不安

正当化

仕事のためには仕方ない
少しだけならば皆していると肯定する

機会

可能性がある状況、機密情報にアクセス権限

事例2　元ソフトバンク社員の転職時機密情報持ち出し

楽天モバイル側からスムーズな転職の条件暗示？
転職先での仕事に役立てようという勝手な動機

機会
退職日までサーバーにアクセスが可能であること
メールでデータを外部に持ち出すことが出来ること
自宅PCからアクセスすることが出来ること
退職申請したにもファイルのパスワードが変更されていなかったこと
適切なログ管理がなされていないこと

正当化

退職時にも機密情報を第三者に開示、漏洩しないことなどを誓約していたものの、、、

3要素の中でも、正当化は心の問題、

闇の中、報道からは分からない

最後に、
心に踏み込む対策が必要

コンプライアンス違反を引き起こす3つのステップ

正当化

自分ではない、会社が悪いからだ

機会

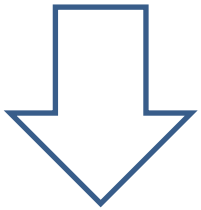
機密情報に触れる業務権限

動機

仕事のストレスや会社への不満

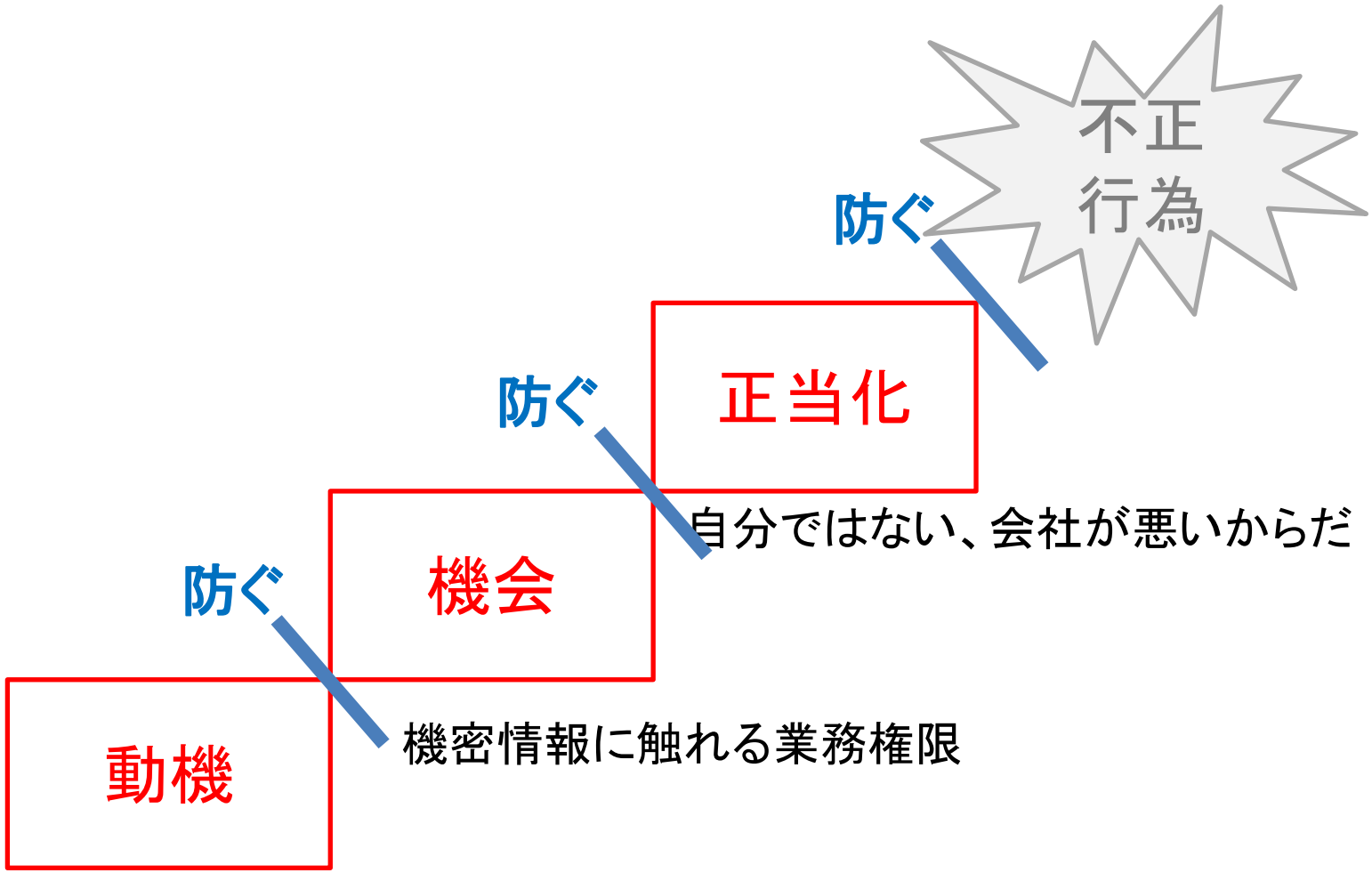
企業として組織的に予防に取り組めるのは「機会」、
システムやルールを整備して不正を行う機会をできる限り排除する

しかし、不正のトライアングルの「動機」と「正当化」がある限り、
完全にｾﾞﾛにすることは事実上困難



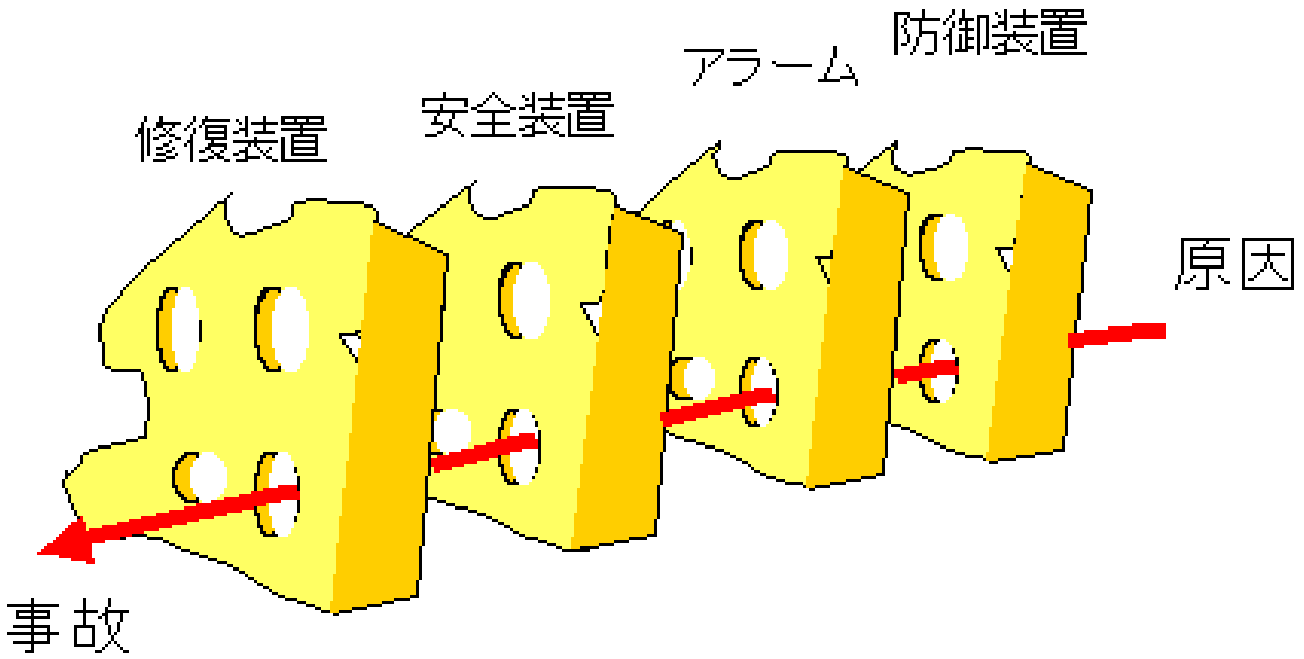
技術者の**倫理感**の醸成

コンプライアンス違反の階段を上らないように



スイスチーズモデル

スイスチーズモデル



事故を起こす原因が発生しても、どこかの防御機構に止められる場合には、事故は発生しない。
しかし、いずれの防御機構にもどこか穴があり、穴は時々刻々と変化し、たまたま穴の位置が重なると事故発生まで到達してしまう。

技術偉人との禅問答に学ぶ

正当化心理への禅問答

稲盛和夫さん

働き方、考え方、生き方

正当化心理への禅問答

訴え：自分ではない、会社が悪いからだ

検査データを少しごまかしたら、
上司からこっぴどく叱られた
忙しい時は、皆やっている
検査員を増やさない会社が悪いのであって、私に無理を押しつける会社が間違っている
SNSに大げさに書いて陥れてやる

答え：感謝の心からプラスの行動が

良い心からプラスの考え方が生まれる
考え方が生きる行動姿勢となる
考え方次第で人生や仕事の結果は180度変わるもの

良い心は感謝の心から
恩を受けた人の顔を思いだすこと

人生・仕事の結果
＝
考え方×熱意×能力

稲盛和夫

人生や仕事の結果は、考え方と熱意と能力の3つの要素の掛け算で決まります。

このうち能力と熱意は、それぞれ0点から100点まであり、これが積で掛かるので、能力を鼻にかけ努力を怠った人よりは、自分には普通の能力しかないと思って誰よりも努力した人の方が、はるかにすばらしい結果を残すことができます。

これに考え方が掛かります。考え方とは生きる姿勢でありマイナス100点からプラス100点まであります。考え方次第で人生や仕事の結果は180度変わってくるのです。

そこで能力や熱意とともに、人間としての正しい考え方をもつことが何より大切になるのです。

考え方とは良い心。

良い心：常に明るく前向きに、肯定的、建設的、協調的

（プラス）善意、思いやり、優しさ、真面目、正直、謙虚、努力
利己的でない、強欲でなく足るを知っていること、感謝の心

悪い心：後ろ向き、否定的、非協調的、暗い、悪意、意地悪

（マイナス）他人を陥れる、不真面目、嘘つき、傲慢、怠け者、利己的
強欲、不平不満、人を恨み妬む

□プラスの考え方を持つとは

考え方とは良い心。

良 い 心：常に明るく前向きに、肯定的、建設的、協調的

（プ ラ ス）善意、思いやり、優しさ、真面目、正直、謙虚、努力

利己的でない、強欲でなく足るを知っていること、感謝の心

悪 い 心：後ろ向き、否定的、非協調的、暗い、悪意、意地悪

（マイナス）他人を陥れる、不真面目、嘘つき、傲慢、怠け者、利己的

強欲、不平不満、人を恨み妬む

どれも、そうできれば苦労しない、といったものであるが、

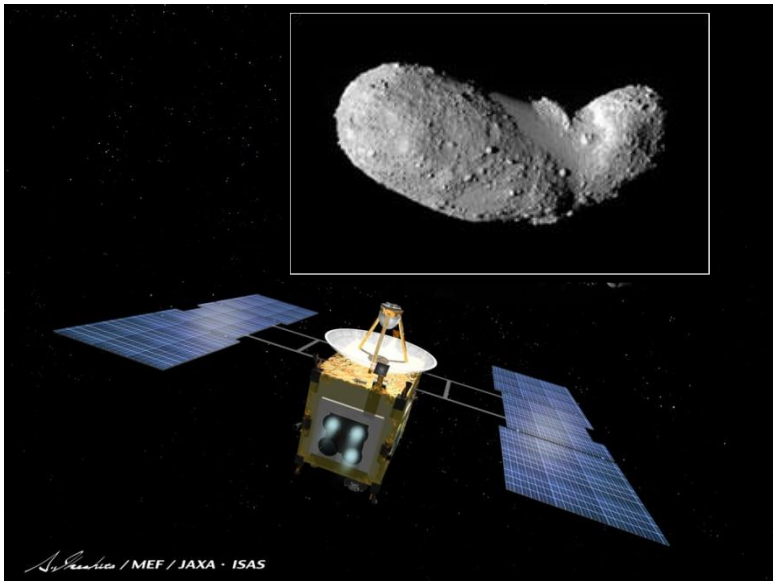
感謝する心

これならできるだろう、恩を受けた人の顔を思いだすようにしてほしい

会社がいつも正しいわけではない

機会心理への禅問答

糸川英夫さん



はやぶさ設計者
東大ロケット開発
「逆転の発想」
組織工学研究所
友人を持て
バレー、楽器

機会心理への禅問答

訴え：機会へのストレス

会社で人事に所属していますが
人事データを扱う仕事がイヤです
上司も仕事も好きになれません
上司は冷徹に社員の事を簡単にリストラします。
会社に真の友人はなく孤独です
リモートで人事機密データを全部消去して無くしてしまいたいです

組織の中の人
友人、師

答え：組織のなかで

仕事の時間と別に生きがいの時間を

1日3分楽しい時を持つ

友人はタイプの異なる友人を持つ

師は勝手に選び師から勝手に学ぶ

人生、何歳になろうと
一日に二四時間しかない
というか
二四時間もあるというか
その中の何時間か何分かで
新しいことを学び、知り、
新しい人を友にもち、
たとえ三分でも
楽しいときをもてれば
やはり生きてよかったのでしょう。

糸川　英夫

← 1日　24時間法 →

生活の時間	仕事の時間	生きがいの時間
睡眠をとったり、食事をしたり、入浴をしたりする時間で、生存に必要とする基本的な行為に費やす	基本的に戸主が会社にいって仕事をする時間で、生活費を稼ぐことに費やす。主婦の家事労働、子供の勉強も含まれる	たとえばライフワークや趣味など、生きがいや意欲を感じることに費やす。仕事と生きがいが一致すれば一番よい

バレーを踊る姿

会社と自分は切り離す
会社の中で友人を持つ

□　友人、パートナーを持つ

人生に友人、
仕事にパートナー（相方）を持て

自分と異なるタイプの人間を

同類だと、新しい着想や刺激を受けることがない
広がらない

デ・センター手法　相手に合わせて、中心を変化させる

1.自分の考えを相手に合わせてみる

2.外してみる、否定、反論

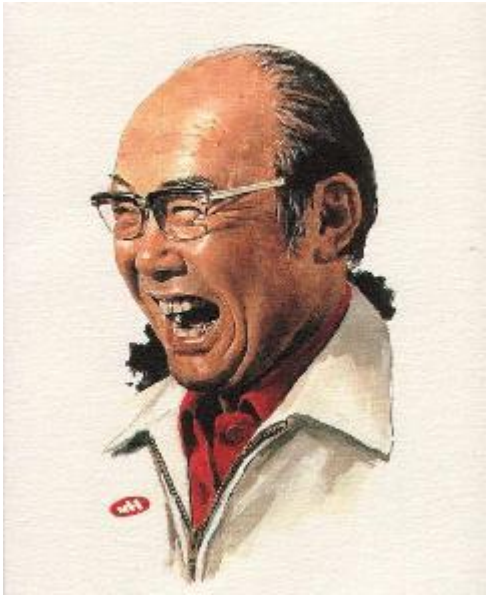
□　師匠、尊敬する先輩

黙って待っていても見つからない

師から何を学ぶかは、弟子の勝手
　　師の責任ではない

出身大学、肩書き
　　自分も師もランキングしない

動機心理への禅問答



本田宗一郎さん

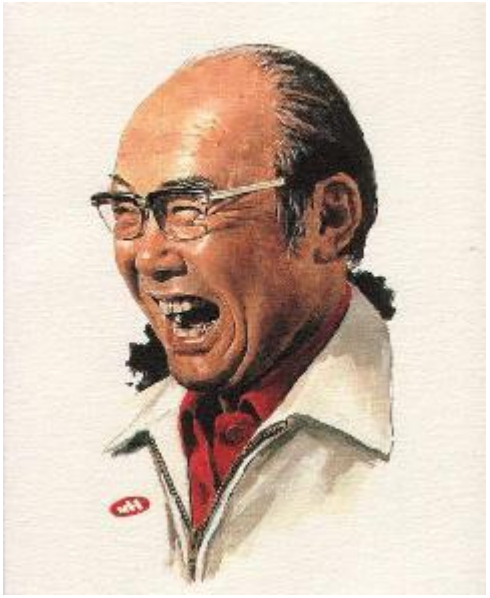
自分のために働け

技術の前では平等

動機心理への禅問答

訴え：会社への不満

会社では営業成績の競争でくたびれはてました。会社に行きたくありません。給料もよくありません。会社への忠誠心なんか出てきません。
顧客データをUSBにコピーして競争会社へ転社してやりたいです。彼らがあわてている姿を想像するだけで愉快でスカッとします。



答え：会社へ求めない

愛社精神よりも、自分のために働け
不平不満いうより、改革をしなさい
プライドは要らない
人生は長いマラソン
貧乏は大いに結構

Stay foolish, stay hungry.

「本田宗一郎からの手紙」　片山　修

新入社員のきみへ

入社おめでとう。
非常に希望を大きくもつて進んでおられる諸君に何か話せということなんで、まあ、今日はひとつ、いろいろな文句をいいたいと思う。
だいたい、どこの会社へ入っても、ほとんどの社長が愛社精神ということをいうだろう。
しかし……愛社精神なんていうことよりも、まず第一に自分のために働けということを申し上げたい。ひとのために働くなんていうのは嘘なんだよ。
そんなきれいごとでは絶対に働けないということなんです。

×愛社精神　　〇自分

動画視聴　自分のために働くということ本田宗一郎

だいたい、みんなも入社するにあたって、あれこれと自分なりに考えて入ってきただろう。みんな自分のためを思って会社を選び、会社に入ってくる。それを途中で愛社精神に切り替えて、モデルチェンジするなんてことは卑怯だぞ。
だから私は、君たちに対しても絶対に愛社精神を叩きこむようなことはしない。愛社精神というものは、きみたちが自分を磨いて一所懸命に生きていくうちに、自然に発生してくるものと信じているんです。

×愛社精神

諸君が、これから進んでいくコースには、いろいろな困難もあることだろう。自分の思うとおりには、なかなかいかないのが世の中というものなんだ。そのときに、不平不満だけでは解決できないんです。
この会社にしても、良い点もあり悪い点もある。だから悪い点は悪いで、はっきりと見きわめ、どんどん改革して前進していく、これがきみたちにいちばん期待することなんだ。この会社に新しい思想、新しい風を入れるのがきみたちの役目なんです。

×不平不満より改革

「会社のために働くな」　本田　宗一郎

人生は長いマラソン

僕はいつもうちの若い大学出の技術屋やデザイナーたちにいっている。君らは、ひとかどの専門家だと思っているかも知れないが、それじゃ聞くが大学は何年だ。四年だというが、正月の休みが一カ月、春休み二カ月、夏休み二カ月を引くと半年しか勉強していないわけだ。その半年も休講があったり、サボッたり、一般教養科目があったりで、本当に得意というか専門科目は四年間にどのくらいになるというのか。一日七時間労働に割ってみるとおそらく四年間学校に通っても三カ月そこそこだろう。それぽっち勉強して俺は技術家だとかデザイナーだと得意になるのはまだ早いぞといってやった。

貧乏はすべきである

僕は、僕なりに生きていくことへの大きな自信をもっている。どうしてこういう自信が生まれてきたかと聞かれれば、やはり貧乏な家に生まれたからだというほかはない。貧乏だと自分以外に頼るものがないのだから、独立心は当然盛んになるわけだ。

だから、貧乏でも決して悲観することはない。貧乏をしてひねくれてしまっては困るが、貧乏をプラスに変えることができるなら、貧乏はすべきである。

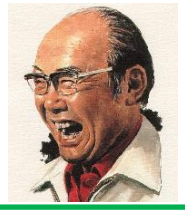
正しい
行い

正当化

恩人へ感謝

組織

友人、師を持つ



動機

自分のために働く