Microsoft

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

Microsoft Security Forum 2020

～変化に備える、2020 年のセキュリティ対策～

Microsoft
DIGITAL TRUST SECURITY

Microsoft
Security Forum 2020

河野 省二
Shoji Kawano

日本マイクロソフト株式会社
Chief Security Officer

Microsoft

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

2020 年からのセキュリティ

~マイクロソフトの考えるデータファースト、デジタルガバメント~

日本マイクロソフト株式会社
技術統括室 チーフ セキュリティ オフィサー
河野 省二

新型コロナウイルス影響下のマイクロソフトの取り組み

マイクロソフト全体の取組み

- 在宅勤務の活用を強く推奨

日本マイクロソフトの取組み

- 「小・中・高等学校、特別支援学校の臨時休業」を受けて、ファミリーケア休暇（年間 5 日付与）の利用範囲を拡大

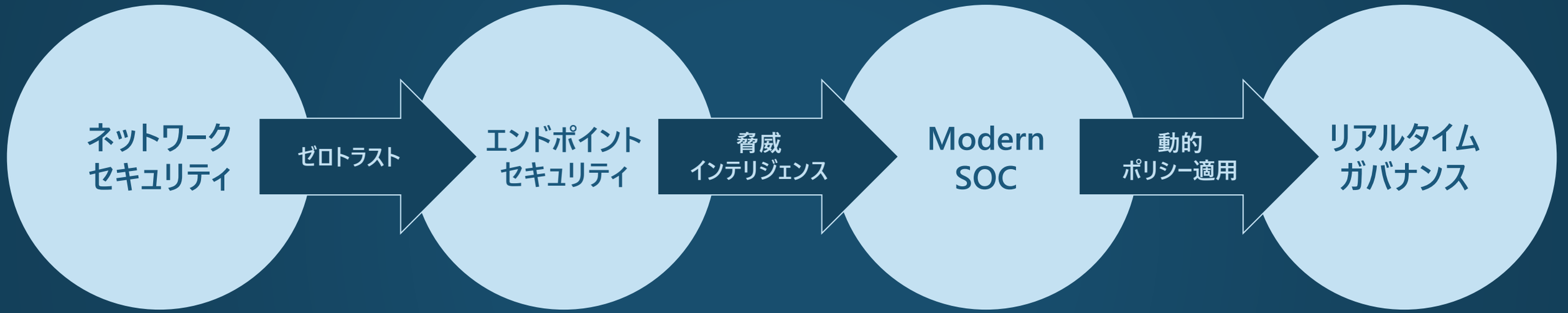
DIGITAL TRUST

Business Sustainability

社会の持続性のためにも、ビジネスの持続性を忘れてはいけない

DIGITAL TRUST

セキュリティの変化とこれから



Self-healingによる、レジリエンスの実現

OSやアプリの進化、クラウド利用の推進によって、動的にガバナンスを構築でき、
動的ポリシー適用によって業務を止めることなく脆弱性対策を実行できるようになった

DIGITAL TRUST


DIGITAL
TRUST

Microsoft

DIGITAL TRUST SECURITY

Microsoft Security Forum 2020

NISC

内閣官房
内閣サイバー セキュリティ センター
副センター長 内閣審議官

山内 智生様

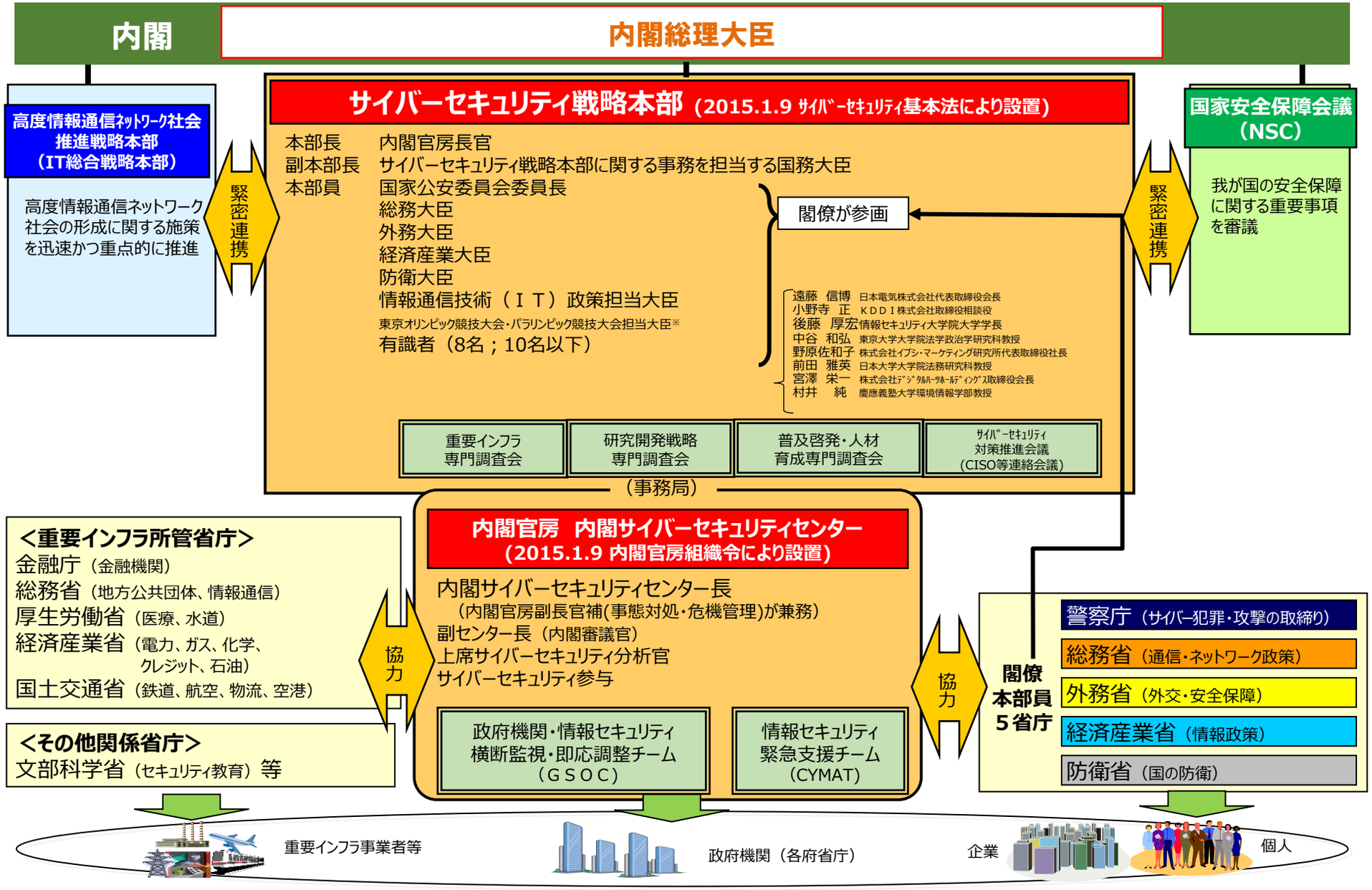
Society 5.0 に向け取り組むべき サイバー セキュリティ対策

内閣官房
内閣サイバーセキュリティセンター
副センター長　　山　内　　智　生

我が国のサイバーセキュリティ政策

～全体像と人材育成・普及啓発関係の取組み～

サイバーセキュリティ政策の推進体制



サイバーセキュリティ戦略

（平成30年７月27日　閣議決定）

◆ この戦略は、サイバーセキュリティ基本法に基づく２回目の「サイバーセキュリティに関する基本的な計画」。2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後３年間（2018年～2021年）の諸施策の目標及び実施方針を国内外に示すもの

＜全体構成＞

1　策定の趣旨・背景

- サイバー空間がもたらす人類が経験したことのないパラダイムシフト（Society5.0）
- サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会を見据えた新たな戦略の必要性

2　サイバー空間に係る認識

- 人工知能（AI）、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- 技術・サービスを制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

3　本戦略の目的

- 基本的な立場の堅持（基本法の目的、基本的な理念（自由、公正かつ安全なサイバー空間）及び基本原則）
- 目指すサイバーセキュリティの基本的な在り方：持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進。　３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進

4　目的達成のための施策

経済社会の活力の向上及び持続的発展

～新たな価値創出を支える サイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 多様なつながりから価値を生み出すサプライチェーンの実現
- 安全なIoTシステムの構築

国民が安全で安心して暮らせる社会の実現

～国民・社会を守る任務を保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与

～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

横断的施策

- 人材育成・確保
- 研究開発の推進
- 全員参加による協働

5　推進体制

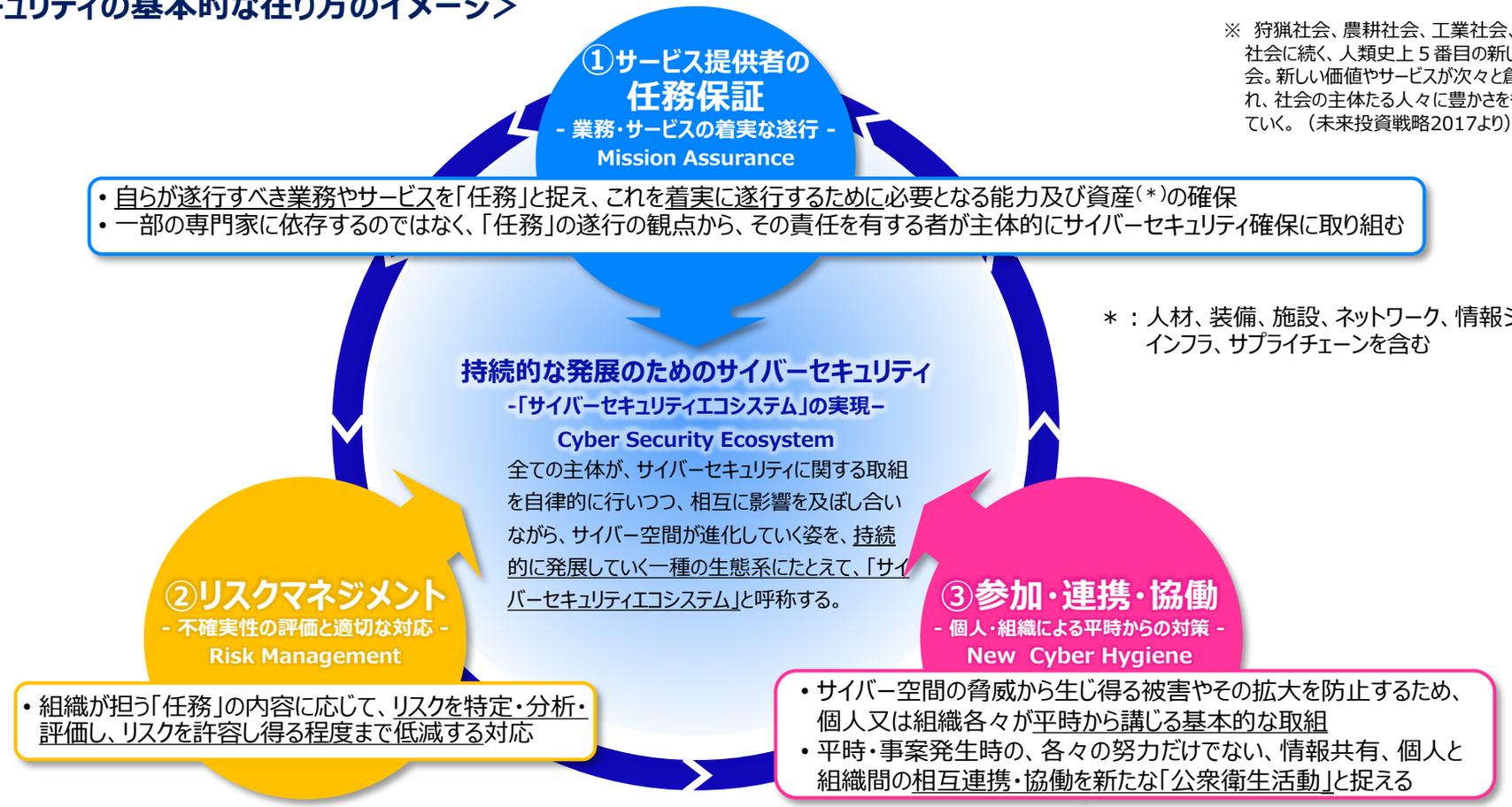
内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが調整・連携の主導的役割を担う。

目指す姿 （持続的な発展のためのサイバーセキュリティ　–「サイバーセキュリティエコシステム」の実現- ）

○　新しい価値やサービスが次々と創出されて人々に豊かさをもたらす社会（Society5.0※）の実現に寄与するため、実空間との一体化が進展しているサイバー空間の持続的な発展を目指す（「サイバーセキュリティエコシステム」の実現）。

○　このため、これまでの基本的な立場を堅持しつつ、３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）から、官民のサイバーセキュリティに関する取組を推進していく。

＜サイバーセキュリティの基本的な在り方のイメージ＞



※　狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（未来投資戦略2017より）

＊：人材、装備、施設、ネットワーク、情報システム、インフラ、サプライチェーンを含む

サイバーセキュリティ人材育成取組方針
～事業継続と価値創出に向けた産学官連携の推進～（概要）

	経営層	戦略マネジメント層	実務者層・技術者層
役割	● ビジネスやサービスの着実な遂行（任務保証）が重要 ● 事業継続と価値創出のためのリスクマネジメントの一環として、対策を推進	●事業継続と価値創出に係るリスクマネジメントを中心となって支える役割 ●経営層の方針を踏まえた対策立案、実務者・技術者の指揮	●方針を踏まえたセキュリティ対策の企画・構築・実施
課題	◆リスクマネジメントに向けた、経営層の理解と意識改革の推進 ◆業種・業態の違いを踏まえた、サイバーセキュリティの位置付けの明確化とリスクマネジメントの浸透 ◆取組に対する経営上のインセンティブ付与	◆マネジメント機能の中でサイバーセキュリティリスクを考慮する必要 ◆戦略マネジメント層向けの適切な教材やプログラムが存在しない	◆経営層・戦略マネジメント層を支え、他の専門人材とチームの一員として対処できる人材の育成 ◆新たな技術やシステム開発手法の知識・スキルの育成
		人材規模・キャリアパス（需要）と、人材育成施策（供給）の好循環	
今後の施策の方向性（産学官の連携）	**○経営層の理解と意識改革の推進** ✓経営層が果たすべき役割、認識の共有 ✓経営層向けのツールの検討 ✓経営層向け伝道師の発掘・派遣 ✓「経団連サイバーセキュリティ経営宣言」の普及 **○業種・業態別の差異を踏まえた基盤の整備** ✓業種・業態別に対策レベルを示すツールの整備 ✓企業関係法制度の整理に向けた検討 **○サイバーセキュリティ投資のためのインセンティブ** ✓情報開示の推進（ガイドラインの策定等） ✓税制優遇の執行やサイバー保険活用の検討	**○組織における戦略マネジメント層の定着** ✓戦略マネジメント層の意義に対する経営層の理解の推進 ✓戦略マネジメント層の機能の明確化 ✓戦略マネジメントとセキュリティ対策が調和した指針の整備 **○カリキュラム・教材開発と学び直しの推進**	**○経営層・戦略マネジメント層を支える人材育成** ✓産学官連携によるカリキュラムの検討・実施 **○クラウドや先端技術等の利用に係る人材育成** ✓先端技術等の利用に関わるセキュリティの知識・スキル育成
	○サイバーセキュリティ人材育成施策の充実・強化と施策間連携の推進 **○人材育成の「見える化」の推進** ✓ 米国の取組等を参考にしつつ、産学官連携により需要と供給の「見える化」を推進 [例] 人材規模・キャリアパスの明確化、カリキュラム・教材等が一覧になったポータルサイトの整備、育成プログラムの適切な評価基準の策定等		

若年層における教育の充実
＜課題＞ ICTの基本的な原理・仕組みなどを理解し、論理的思考力を育てるとともに、情報モラル教育も重要
＜施策＞ 初等中等教育段階での教育課程内の取組に加え、地域や企業等で、自由に機器・ツールを用いて学べる機会を創出

中小企業関連の取組
＜課題＞ 知識・スキルが十分ではなく、セキュリティ対策への投資が困難。踏み台となった場合、社会への影響が大きい。
＜施策＞ 業種毎のアプローチ、セキュアモデル（クラウド活用等）と一体の対策集の策定・普及、インセンティブの仕組（税制優遇等）の検討

「サイバーセキュリティ意識・行動強化プログラム」（概要）

2019年（平成31年）１月24日
サイバーセキュリティ戦略本部決定

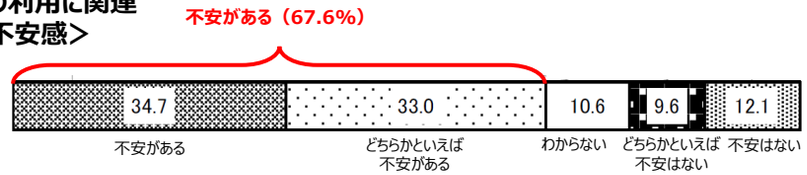
1　はじめに

「サイバーセキュリティ戦略」(2018年7月閣議決定)に基づき、普及啓発について、2020年東京オリンピック・パラリンピック競技大会を見据えつつ、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、本プログラムを策定。

2　現状

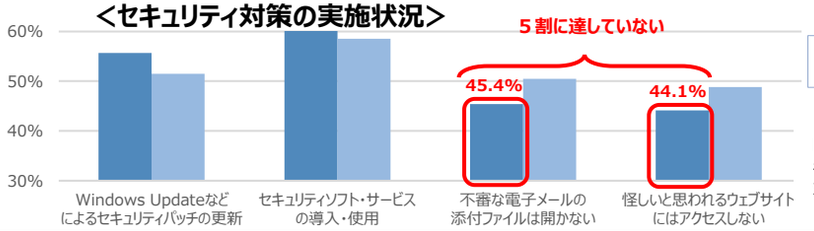
①個人：**AIやIoTの「生活」への浸透**に伴い、インターネット利用への**不安感が拡大。**一方、**具体的な対策の実施に十分に結びついていない。**
②企業：**中小企業では、特に規模の小さい企業ほど**担当者が置かれない場合も多いなど、**取組が遅れている。**

＜インターネットの利用に関連するトラブルへの不安感＞



（出典）インターネットの安全・安心に関する世論調査（内閣府、2018年11月）

＜セキュリティ対策の実施状況＞



「2018年度情報セキュリティの脅威に対する意識調査」（IPA）を元に作成

3　今後の取組の基本的な考え方

・対策に関する情報が国民一人一人や中小企業に必ずしも行き届いていない、いわば「**サイバーセキュリティのラストワンマイル**」の状況。
・「３つの視点」から取組を推進：①**継続的な実施**、②対象に合わせた**適切なツール・コンテンツの提供**、③**関係者間の連携**の促進

4　具体的取組の推進

(1) 基本的な対策の徹底

・個人や企業が**取組の必要性を自覚し、当たり前のこととして取組を講じる**状態を目指し、**必要な対策を継続的に伝える**

（取組の一例）
「インターネットを安全に利用するための情報セキュリティ対策９か条」（2015年2月 NISC・IPA）の各種取組への浸透

(2) 重点的な対象とその内容

・**様々な対象に幅広く実施することを前提**としつつ、以下の対象について、**重点的に取組を実施**

①**中小企業**　中小企業のトラブル対応を支援する「サイバーセキュリティお助け隊」の地域実証、「SECURITY ACTION」活用の促進、中小企業支援ネットワークによる啓発等

②**若年層**　無自覚なまま加害者になることを防ぐためのリテラシー向上の取組、先端的人材育成施策の推進

③**地域における取組の支援**　産学官連携型の取組の活性化、高専学生によるボランティア活動等

高専学生によるボランティア活動（提供：警察庁）

(3) 情報発信・相談窓口の充実

・**最新の脅威の情報・対策の適時かつ迅速な発信**や**相談できる窓口の確保**等、自ら取り組むための環境を整備

（取組の一例）NISCにおけるSNSによる情報発信

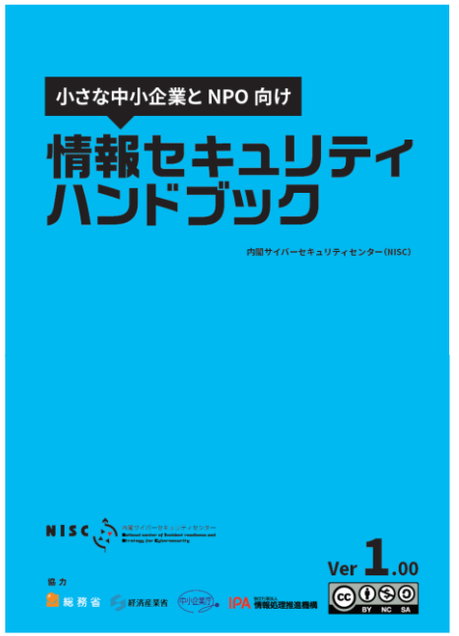
5　連携体制の強化

・**NISCをはじめとした関係機関が連携**し、ラストワンマイルに情報が行き着くよう配慮しつつ取組を推進
①**ポータルサイトによる取組の見える化・連携推進**　②ツール・コンテンツの共有　③サイバーセキュリティ月間の推進　④国際的連携の強化、⑤**ＰＤＣＡによる継続的改善**
・**官民の様々な取組を集約するポータルサイト**を構築し、**対象となる層や伝達手法の見える化及び連携を推進**
・個別施策の実施状況に加え、**個人や企業の対策の実施状況**等を分析し、本プログラムの**内容・効果の定期的な評価、見直しを実施**

「小さな中小企業とＮＰＯ向け　情報セキュリティハンドブック」（NISC）

- 特に小規模な事業者や、セキュリティ担当者を置くことが難しい企業及びＮＰＯ(特定非営利法人)に向けて、サイバーセキュリティをわかりやすく解説した、「小さな中小企業とＮＰＯ向け情報セキュリティハンドブック」を、関係機関の協力を得てＮＩＳＣで作成し、平成３１年４月に公表。
- サイバーセキュリティに関する必要性は感じていても、どこから取り組んで良いか分からないという方々に、広く活用いただけるよう、NISCウェブページにおいて公開。

目次



https://nisc.go.jp/security-site/blue_handbook/index.html

みんなで使おう　サイバーセキュリティ・ポータルサイト (NISC)

1．経緯

官民で様々な人材層を対象とした多様な普及啓発・人材育成施策を講じているが、これらを横断的に整理し必要な施策へのアクセスを可能とするような媒体が存在しないため、国民が自らのレベルに応じた適切な施策にアクセスできるようになることを目的とし、本サイトを構築・運用していく。

2．特徴

サイトを訪問した方が、適切な施策を見つけられるようにするため、①通常の網羅的な施策一覧だけではなく、②自らのニーズからアクセスできるような工夫を行う。

①網羅的な施策一覧からアクセス

自身の属性を「若年層」「社会人以上」「中小企業」「大企業」「自治体・教育機関」の５つから選択し、それに適したレベル別の施策を情報提供。

②自らのニーズからアクセス

以下の５つの事例を設定し、それに適した施策を情報提供。

- 「サイバーセキュリティの基本的なところから知りたい」
- 「少しわかってきたけどもっと詳しく知りたい」
- 「自社社員のセキュリティレベルを上げてもらいたい」
- 「経営とセキュリティの両方の観点から学びたい」
- 「地域で開催されているイベントを知りたい」

⇒　3/11　より仮運用開始

サイトイメージ

②自らのニーズからアクセス

①網羅的な施策一覧

「サイバーセキュリティ関係法令Q&Aハンドブック」（NISC）

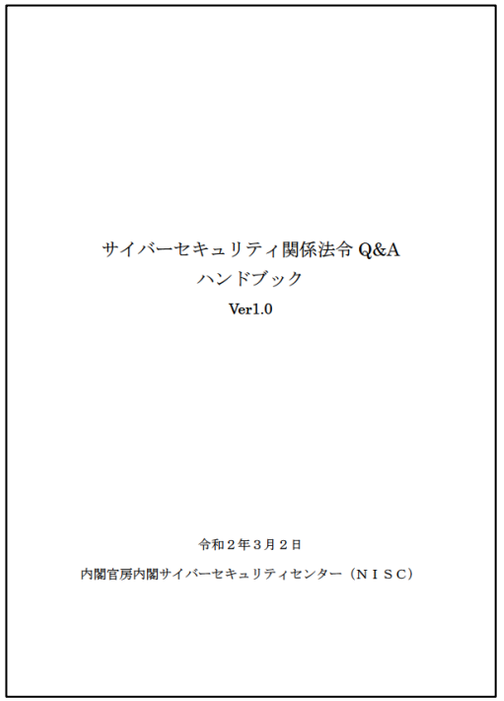
NISCは、令和２年３月２日、サイバーセキュリティ対策において参照すべき関係法令をQ&A形式で解説する「サイバーセキュリティ関係法令Q&Aハンドブック Ver1.0」を作成・公開。
企業における平時のサイバーセキュリティ対策及びインシデント発生時の対応に関する法令上の事項に加え、情報の取扱いに関する法令や、情勢の変化等に伴い生じる法的課題等を可能な限り平易な表記で記述。

サブWG・タスクフォース会合合同開催

タスクフォースからサブWGへのドラフト提出

Q&Aで取り上げている主なトピックス

1. **サイバーセキュリティ基本法関連**
2. **会社法関連**（内部統制システム等）
3. **個人情報保護法関連**
4. **不正競争防止法関連**
5. **労働法関連**（秘密保持・競業避止等）
6. **情報通信ネットワーク関連**（IoT関連を含む）
7. **契約関連**（電子署名、システム開発、クラウド等）
8. **資格等**（情報処理安全確保支援士等）
9. **その他各論**（リバースエンジニアリング、暗号、情報共有等）
10. **インシデント対応関連**（デジタルフォレンジックを含む）
11. **民事訴訟手続**
12. **刑事実体法**（サイバー犯罪等）
13. **海外法令**（GDPR等）



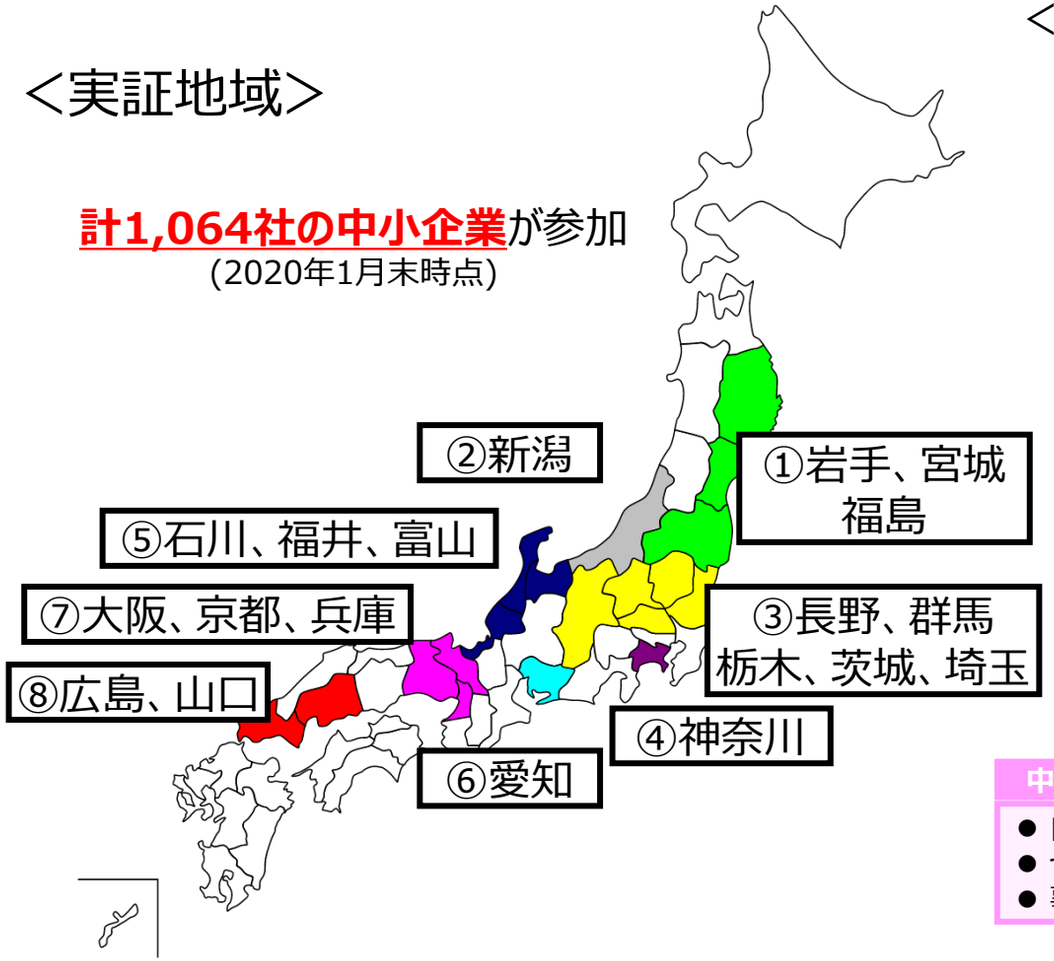
【経緯】
- 平成30年10月10日、サイバーセキュリティ戦略本部普及啓発・人材育成専門調査会は、サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ（以下「サブWG」という。）を設置。
- 経済産業省が平成21年に作成した「情報セキュリティ関連法令の要求事項集」をベースとし、サブWGの下部に設置したタスクフォースを中心としてドラフトを起草、令和２年２月18日にサブWGへ提出し、サブWGにおいてとりまとめ。

サイバーセキュリティお助け隊実証事業（経済産業省：事後対策支援）

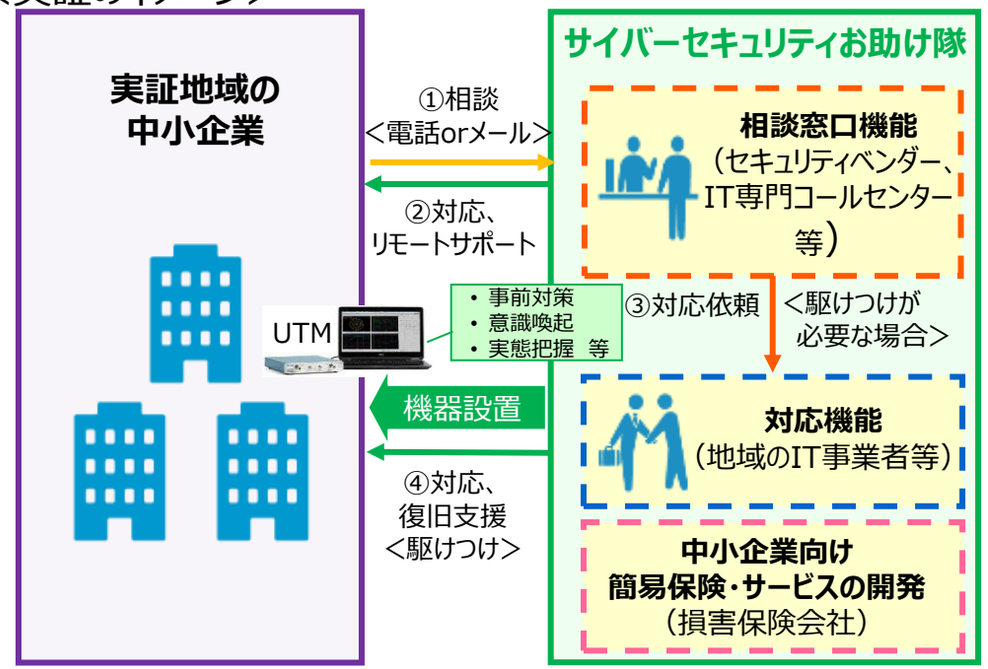
- 全国**8地域**において、地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした**実証事業**を実施。
- 中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティ簡易保険サービスの実現を目指す**。

＜実証地域＞

計1,064社の中小企業が参加
(2020年1月末時点)



＜実証のイメージ＞



実証結果

中小企業　側
- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

保険会社、セキュリティベンダー　側
- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

公衆無線LAN（Wi-Fi）関係ガイドラインの改定（総務省）

- 公衆無線LANの提供者・利用者向けにガイドラインを作成しており、周知啓発に活用。
- 現行版と比べ、WPA3等の新技術も出てきていることから、現在、内容の見直しを実施中。
- 改定版ができた場合、Wi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に改めて周知予定。

提供者向け

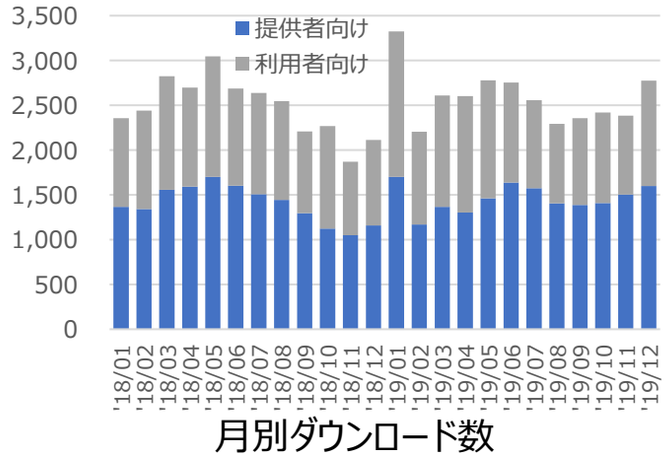
利用者向け

「Wi-Fi提供者向け セキュリティ対策の手引き」の見直し

現行版（2016年８月版）について、次の観点から見直しを実施中

- ✓新技術動向（WPA3、Enhanced Open、Wi-Fi 6等）を反映
- ✓対象者の明確化（自店利用者のみへの提供も対象）
- ✓偽アクセスポイント対策について追記
- ✓提供環境に応じたセキュリティ対策が必要であることを明示
- ✓セキュリティ対策状況の利用者への周知が必要であることを明確化

年間約３万件のWeb閲覧数



月別ダウンロード数

「Wi-Fi利用者向け 簡易マニュアル」の見直し

現行版（2015年３月版）について、次の観点から見直しを実施中

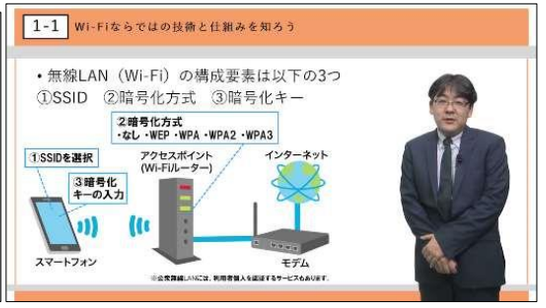
- ✓新技術動向（WPA3、Enhanced Open、Wi-Fi 6等）を反映
- ✓「公衆利用」と、限定的な「家庭・職場利用」の差異を明確化
- ✓TLS(SSL)による上位レイヤーでの暗号化について追記
- ✓無線LANルータ等の管理用ID・パスワードの設定変更について追記

公衆無線LAN（Wi-Fi）の利用に関する周知啓発（総務省）

- 公衆無線LANの利用者のセキュリティ対策に関する周知啓発を目的として、**オンライン動画講座**を開講。（2020年２月10日～3月23日）
- 無線LANのセキュリティ対策に関する**ショートムービー**を作成し**SNSを通じて周知**予定（本年３月）。

オンライン動画講座

- ✓有識者が、公衆無線LAN利用時のリスクや、適切なセキュリティ対策を動画(全10回)により紹介
- ✓オンライン講座プラットフォーム「gacco」にて配信
  https://gacco.org/wifi-security/
  （2020年２月10日～３月23日）



第１回：もっとつながる・使える公衆無線LAN ＜Wi-Fiの技術＞
第２回：とっても危険！「野良Wi-Fi」
第３回：そのWi-Fi、本物ですか？
第４回：さまざまな公衆無線LANサービスを知ろう
第５回：Wi-Fiの接続と暗号化の仕組み
第６回：安全なWeb利用の方法
第７回：自分で重要な通信内容を守る
第８回：より安全・安心にWi-Fiを使うために
第９回(追加講義)：Wi-Fi規格の最新動向
第10回(追加講義)：自宅や外出先で行う最新のセキュリティ対策とは

SNSを用いた周知啓発

- ✓無線LANのセキュリティ対策に関し、20秒程度の動画コンテンツを作成（全３種）
- ✓若年層を含む利用者への周知のため、SNSを通じて作成動画を周知
- ✓動画から上記オンライン動画講座にリンクを張ることで相乗効果を期待

＜動画① 知らない接続先を使わない＞

その他、「動画② HTTPSの利用・確認」「動画③ 管理用パスワード等の適切な設定」を作成中

２０２０年東京大会に向けた取組状況

大会の運営に大きな影響を及ぼし得る重要サービス事業者等を対象とした**リスクマネジメントの促進**や、関係府省庁、大会組織委員会、東京都等を含めた関係組織と、サイバーセキュリティに係る脅威・事案情報の共有等を担う中核的組織としてのサイバーセキュリティ対処調整センターの構築等、**対処態勢の整備**を推進中。これらの仕組み、運用経験及びノウハウは、東京大会のみならず、我が国の持続的なサイバーセキュリティの強化のために活用。

リスクマネジメントの促進

○ **取組状況**

手順書を作成するとともに、東京大会において開催・運営に影響を与える重要サービス事業者等を選定し、リスクの低減と最新のリスクへの対応のため、**リスクアセスメント**の実施を依頼。2016年度から2020年６月末まで計６回を予定。実施結果について横断的に分析し各事業者等にフィードバック。現在、第5回目を実施中。

また、競技会場に提供されるサービスの重要度に応じて対象事業者等を選定の上、サイバーセキュリティ対策の実施状況をNISCが検証する**横断的リスク評価**を2020年３月末までに計３回実施。現在、第2、3回目を実施中。

○ **今後の取組**

リスクアセスメントの取組については、引き続き、重要サービス事業者等のリスクアセスメントにおいて、情報資産、リスクの洗い出しの網羅性及び要対応リスクに対する対策の網羅的な検討を促進するとともに、残存リスクが顕在化した場合の対応体制の強化を促進。

横断的リスク評価の取組については、引き続き、重要サービス事業者等（競技会場(レガシー部分)を含む。）を対象として検証を実施するとともに、競技会場のオーバーレイ部分の対策の整備状況及び監督状況について東京大会組織委員会を対象として検証を実施。

対処態勢の整備（サイバーセキュリティ対処調整センターの構築等）

○ **取組状況**

情報共有システムの構築が完了し、2019年４月に設置した**サイバーセキュリティ対処調整センター**を大会までの大規模イベント（G20大阪サミット等関係閣僚会合、ラグビーワールドカップ等）において運用、ラグビーワールドカップ組織委員会、会合の現地事務局等に連絡要員を派遣するとともに、サイバーセキュリティ対処調整センターの情報共有システムを使用した関係組織・機関への迅速な情報提供を実施したほか、情報共有及びインシデント発生時の対処に係る訓練・演習を重ねている。情報共有・事案発生時の態勢について関係府省庁、大会組織委員会、東京都等と協議して決定した**対応手順等**について逐次改善を実施中。また、サイバー脅威情報の提供について4社から協力を受けることを決定した。

○ **今後の取組**

重要サービス事業者等も参加する情報共有及びインシデント発生時の対処支援調整等の**訓練・演習**を実施し、大会関係組織間で緊密に連絡調整を図るための態勢を整備する。ラグビーワールドカップ等の大規模イベントにおける情報共有及びインシデント発生時の対処に係る運用の実施結果や訓練・演習を通じて関係職員の練度向上及び対応手順等の改善を行い、大会に向けて万全の対処態勢の整備を目指す。

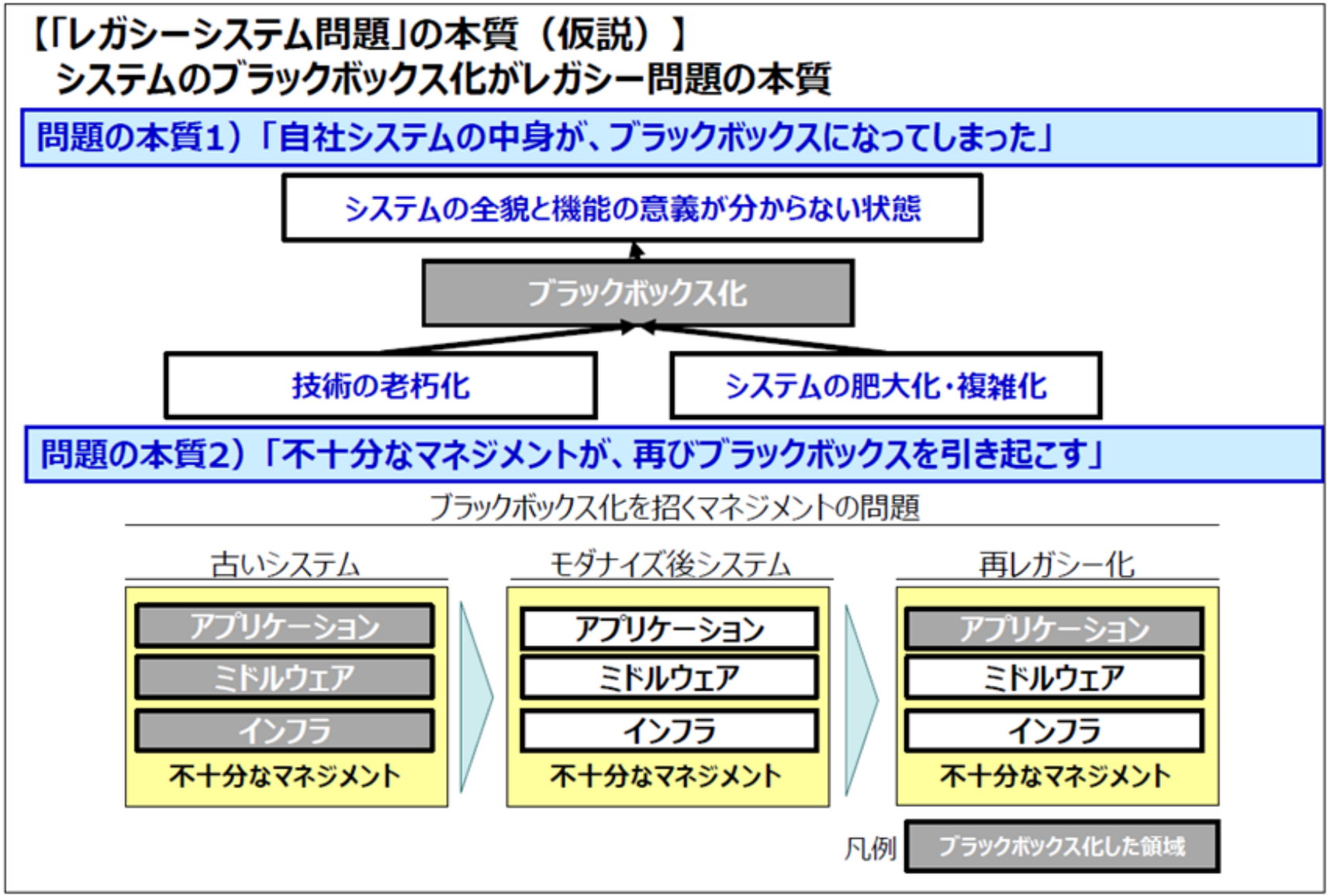
サイバーセキュリティとDX

※本内容には発表者の私見が含まれます

ありがちなサイバーセキュリティの姿

- 経営層は、デジタル化とサイバーセキュリティの確保を担当の仕事だと思っているし、そもそもサイバーセキュリティをなぜ行うのか公式文書のどこにも記載がない
- 経営企画部門は、デジタル化とサイバーセキュリティを効率化と防護のため（だけ）と思っているし、セキュリティ監査と具体的な対策・投資がバラバラ
  （場当たり的にセキュリティ対策をしている）
- 担当者は、システムの運用・保守とセキュリティ対策に追われる毎日、事故がなくて当たり前、何か起こると怒られる
- セキュリティポリシーは策定したが、現実に即しておらず利用者もその内容を理解していない
- BCPを策定したが、IT・サイバーセキュリティ部門と他の部門の連携は検証していない

既存システムの問題点



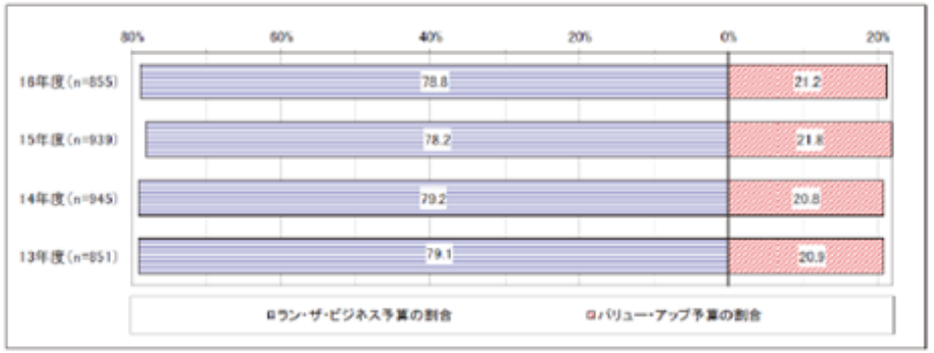
（出典）DXに向けた研究会　一般社団法人日本情報システム・ユーザー協会説明資料より

⇒　**セキュリティ対策でも同様の問題が生じているのでは？**

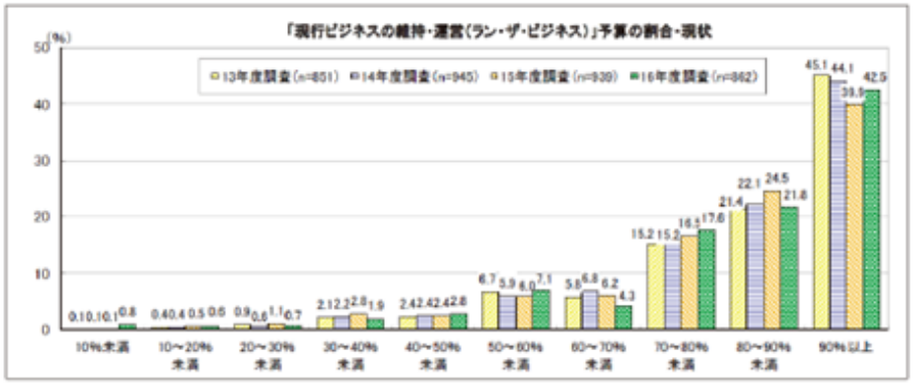
既存システムの運用・保守に割かれてしまう資金・人材

- **IT関連費用の８０%は現行ビジネスの維持・運営（ラン・ザ・ビジネス）**に割り当てられている。この結果、**戦略的なIT投資に資金・人材を振り向けられていない**。

ラン・ザ・ビジネスとバリューアップのIT予算比は80:20

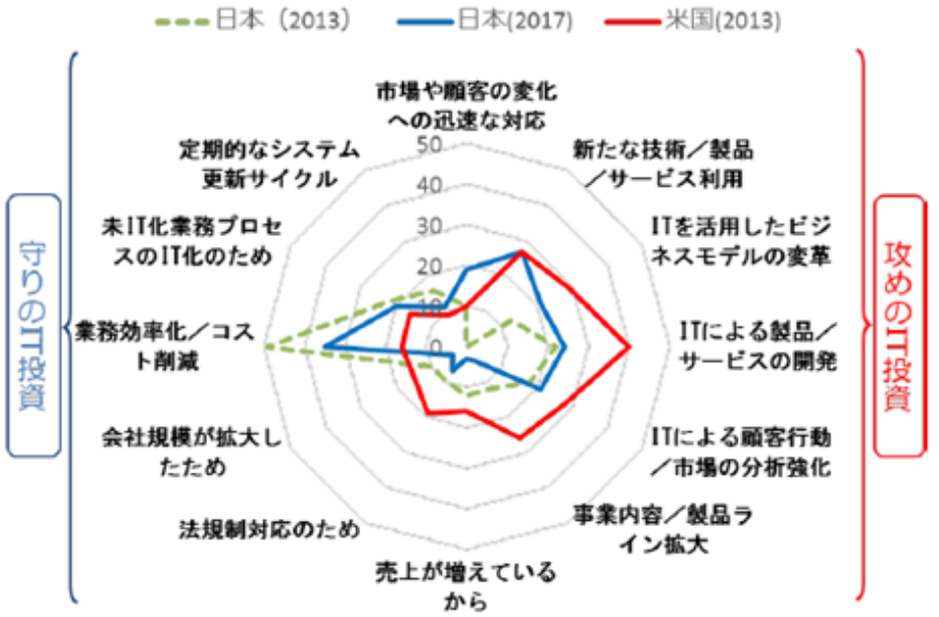


ラン・ザ・ビジネス予算90%以上の企業が約40%で大多数



（出典）一般社団法人日本情報システム・ユーザー協会「企業IT動向調査報告書 2017」より

IT投資における日米比較



（出典）一般社団法人電子情報技術産業協会「2017年国内企業の「IT経営」に関する調査」（2018年１月）より

５つの対応策

1 「DX推進システムガイドライン」の策定

- 既存システムの刷新や新たなデジタル技術を活用するに当たっての「体制のあり方」、「実行プロセス」等を提示
- 経営者、取締役会、株主等のチェック・リストとして活用

→**コーポレートガバナンス**のガイダンスや**「攻めのIT経営銘柄」**とも連動

2 「見える化」指標、中立的な診断スキームの構築

経営者自らが、ITシステムの現状と問題点を把握し、適切にガバナンスできるよう、

- **「見える化」指標**の策定
  - 技術的負債の度合い、データ活用のしやすさ等の情報資産の現状
  - システム刷新のための体制や実行プロセスの現状
- 中立的で簡易な診断スキームの構築

3 DX実現に向けたITシステム構築におけるコスト・リスク低減のための対応策

- 刷新後のシステムが実現すべきゴールイメージ（変化に迅速に追従できるシステムに）の共有（ガイドラインでチェック）
- 不要なシステムは廃棄し、刷新前に軽量化（ガイドラインでチェック）
- 刷新におけるマイクロサービス等の活用を実証（細分化により大規模・長期に伴うリスクを回避）
- **協調領域における共通プラットフォームの構築**（割り勘効果）（実証）
- コネクテッド・インダストリーズ税制（2020年度まで）

4 ユーザ企業・ベンダー企業間の新たな関係

- システム再構築やアジャイル開発に適した契約ガイドラインの見直し
- 技術研究組合の活用検討（アプリケーション提供型への活用など）
- モデル契約にトラブル後の対応としてADRの活用を促進

5 DX人材の育成・確保

- レガシーシステムの維持・保守業務から解放し、DX分野に人材をシフト
- アジャイル開発の実践による事業部門人材のIT人材化
- スキル標準、講座認定制度による人材育成

（出典：経済産業省「デジタルトランスフォーメションに向けた研究会」報告書（2018年9月））

目指したいサイバーセキュリティの姿

- 経営層は、デジタル化計画が業務フロント・バックオフィス双方に及ぼす影響とサイバーリスクの概要を知っていて、自社の経営計画にもサイバーセキュリティ対策を行う目的が記載されている
- 経営企画部門は、自社のシステムに障害が出たり、情報流出が生じた場合に、　どの程度の損失につながるかを把握しており、情報資産の管理とセキュリティ監査が連動することで、具体的な対策・投資の優先順位を決めている
- 担当者は、リスク分析の結果を知っており、どこに障害が生じると重大事であるか認識している
- 会社全体として、現場が理解できるDXに適応したセキュリティポリシーを策定しており、DXによる利点とセキュリティの確保が両立しているとともに、策定したBCPが実働するかどうかIT・サイバーセキュリティ部門と他部門が連携して検証している

システム・機械に任せられるものは任せ、知的集約的な業務に
人的資源を投入することがDXの趣旨にも叶うのでは？

サイバーリスクハンドブック（経団連）

- 本ハンドブックは、経団連会員企業の全ての取締役の方々にご一読頂き、サイバーリスクをどう認識していくか、更に、どう対処していくかを考え、行動に移していって頂くようお願いする目的で・・・

（序文　中西経団連会長）

まずはできることから始めては如何でしょう？

例えば・・・

- どんなシステム・情報資産を保有し、そのシステムが止まると業務にどのような支障が生じるのか、保有個人情報や機密情報が漏えいするとどのような損害が生じるか、またどの程度の頻度で監査を受けているかを調査
  ⇒　資源配分の優先度合い、効率化の度合いと改善の目途
- 適切な人材育成と管理
  ⇒　評価軸、キャリア・パスの設定、“IT畜”・“セキュリティ畜”からの脱却

- システムの運用状況、セキュリティ対策の状況を把握
  ⇒　リスク分析と残留リスク（サプライチェーンリスク／外部委託対策を含む）の把握
- 誰とどのような情報共有をしているか
  ⇒　適切なアクセス管理の設定
- 適切なセキュリティポリシーになっているか
  ⇒　社員への研修、フィードバック（現実離れしていないか双方向で運用）

最後に

- 現場に任せるだけではDXの全体像がつかめないので、是非、戦略・企画部門の方に”DX with Cybersecurity”を考えていただきたい
- リスク管理の一環にサイバーセキュリティがあるはずなので、「サイバー」だからといって難しく考える必要はないと思います
- 最終的に目指す目標と当座の（現実的な）目標は分けて立てては如何でしょうか

・・・

是非、社内の人材育成、普及啓発を含め必要な資源配分をお願いいたします

ご清聴ありがとうございました

https://www.nisc.go.jp


DIGITAL
TRUST

Microsoft
DIGITAL TRUST SECURITY

Microsoft Security Forum 2020

株式会社資生堂
情報セキュリティ部長 (CISO)

斉藤 宗一郎 様

情報セキュリティが健全に機能するために必要なこと

2020/3/12

(株)資生堂　CISO 斉藤宗一郎

SHISEIDO

SECURITY

AGENDA

1 情報セキュリティはリスク管理である

2 3 LINES OF DEFENSE

3 課題

SECURITY

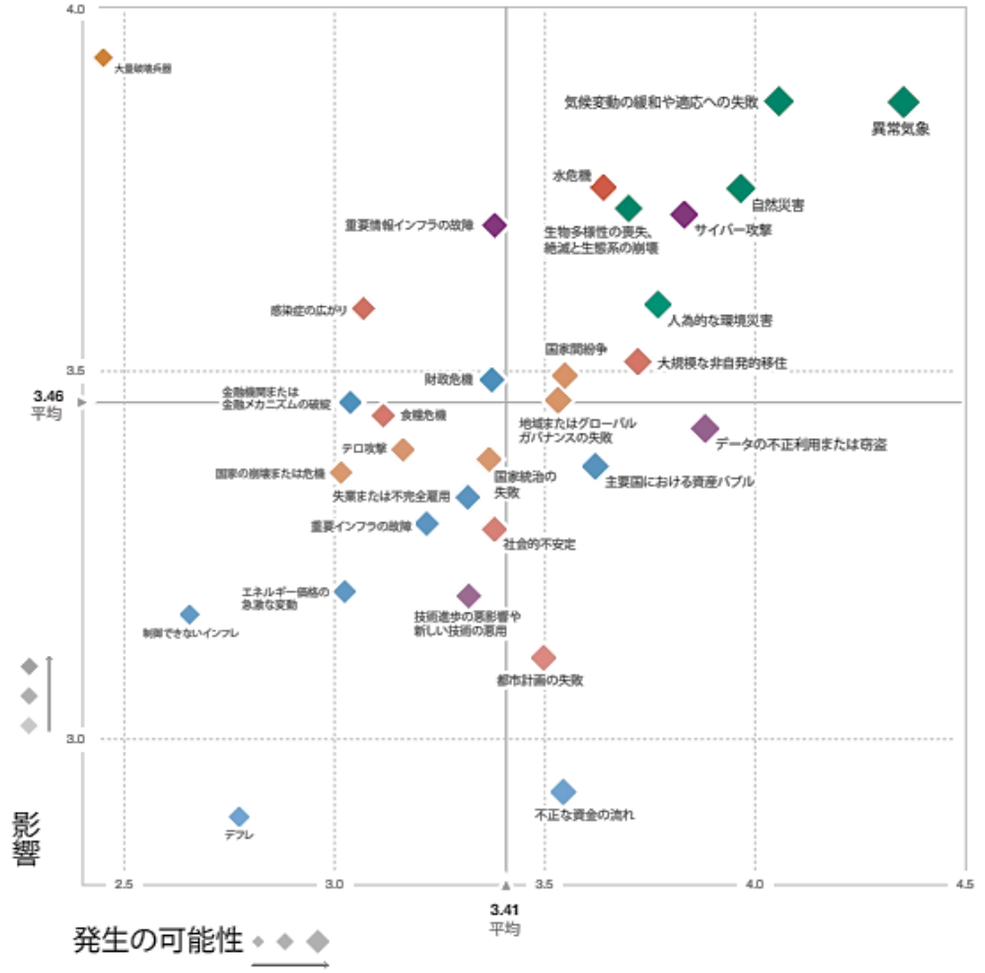
AGENDA

1 情報セキュリティはリスク管理である

2 3 LINES OF DEFENSE

3 課題

1. 情報セキュリティはリスク管理である　–　World Economic Forum



発生可能性が高いリスク 10 位
1. 異常気象
2. 気候変動の緩和や適応への失敗
3. 自然災害
4. データの不正利用
5. サイバー攻撃
6. 人為的な環境災害
7. 大規模な非自発的移住
8. 生物多様性の喪失、絶滅と生態系の崩壊
9. 水危機
10. 主要国における資産バブル

資生堂：リスクのトップ 5 として認識

1. 情報セキュリティはリスク管理である　－　データ主権と規制　(個人情報)

技術対策だけではない

- ✓ 情報セキュリティとしては各国の法規制も注視していく必要がある
- ✓ GDPR, CCPA, PDAP, CSLなど

データそのものを守る

- ✓ DX 時代ではデータは自社 DC だけでなく、クラウドや
  ビジネスパートナー間で共有され所在の把握が難しくなる
- ✓ ネットワークやシステムの脆弱性に加え、
  データそのものを守るという意識が大事

個人情報の取り扱い

- ✓ お客さまの価値観の変化
- ✓ 収集した個人情報は企業資産ではない
- ✓ マーケティングや研究部門などデータを活用する人の意識変革

1. 情報セキュリティはリスク管理である　－　投資家・経営者の眼

投資家が見るのは

- ✓ 投資家は企業の財務状態に加え、SDGs やサイバーリスクについても注視してきている
- ✓ 合併・買収時にもITデューデリジェンスが必要

サイバー保険

- ✓ サイバー保険が急伸しているがリスク・レーティングの確立が急がれている
- ✓ ネットワークやシステムの脆弱性に加え、データそのものを守るという意識が大事

資生堂：サイバーリスク･レーティングを意識しKPIに、同時にPMLに着手

SECURITY

AGENDA

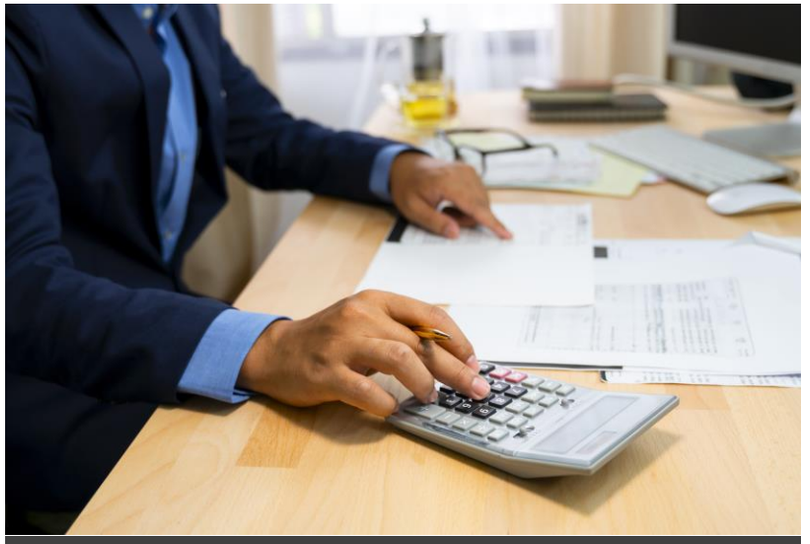
1 情報セキュリティはリスク管理である

2 3 LINES OF DEFENSE

3 課題

2. リスク管理に必要な “3 Lines of Defense” の考え方

健全なリスク管理：『現業部門・管理部門・内部監査部門が連携しリスク管理を行い、
組織全体の内部統率を実行する』（※Committee of Sponsoring Organizations of the Treadway Commission：トレッドウェイ委員会支援組織委員会）

第1のディフェンスライン（Business Owner/System Owner）	第2のディフェンスライン（Standard Settler）	第3のディフェンスライン（Assurance Provider）
		
リスクオーナーとして リスクコントロールを行う	リスクに対する監視を行う	合理的な保証を提供する

SECURITY

AGENDA

1 情報セキュリティはリスク管理である

2 3 LINES OF DEFENSE

3 課題

3. 課題

- **社内での関心を高める**
  - ✓全体（特に非IT部門）のIT/デジタル・リテラシーを如何に高めるか
- **ポリシーガイドライン策定時の工夫**
  - ✓規程を作成する人はルールや規制へのMECEと運用現場に対する洞察が必要
- **規程類の形骸化させないために**
  - ✓策定した規程類の研修や掲示板などでの周知には限界がある

※詳しくは「資生堂が目指す情報分類・活用・監視のガバナンス」にて

資生堂：グローバルに社内で様々な部署を巻き込んでの活動


SHISEIDO


DIGITAL
TRUST

Microsoft

DIGITAL TRUST SECURITY

Microsoft Security Forum 2020

Keidanren

Policy & Action

日本経済団体連合会
デジタルエコノミー推進委員会
企画部会長

浦川 伸一 様

Microsoft Security Forum 2020

SOMPO ホールディングス
安心・安全・健康のテーマパーク

基調講演２

DX時代における DX-Ready の考え方と Security-Ready に向けた取り組み

2020年3月12日

経団連 デジタルエコノミー推進委員会 企画部会長
損保ジャパン日本興亜 取締役常務執行役員 CIO
浦川　伸一

自己紹介

浦川　伸一

略歴

1984年 外資系IT企業入社　金融機関担当部門でSE、PM等を歴任

2013年 損保ジャパン / 日本興亜損保 執行役員

2014年 SOMPOシステムズ 代表取締役社長（現職）

2015年 SOMPOシステムイノベーションズ 代表取締役社長

2016年 SOMPOホールディングス 常務執行役員 グループCIO

損保ジャパン日本興亜 取締役常務執行役員 CIO（現職）

2020年 損保ジャパン 取締役専務執行役員 CIO（4月～）

その他の主な職務（いずれも現職）

経団連: デジタルエコノミー推進委員会 企画部会長、デジタルトランスフォーメーション会議 タスクフォース座長

経済産業省: Society5.0時代のデジタルガバナンス検討会 委員

内閣府: 人間中心のAI社会原則検討会議 構成員　NEDO: 技術委員（AI系）

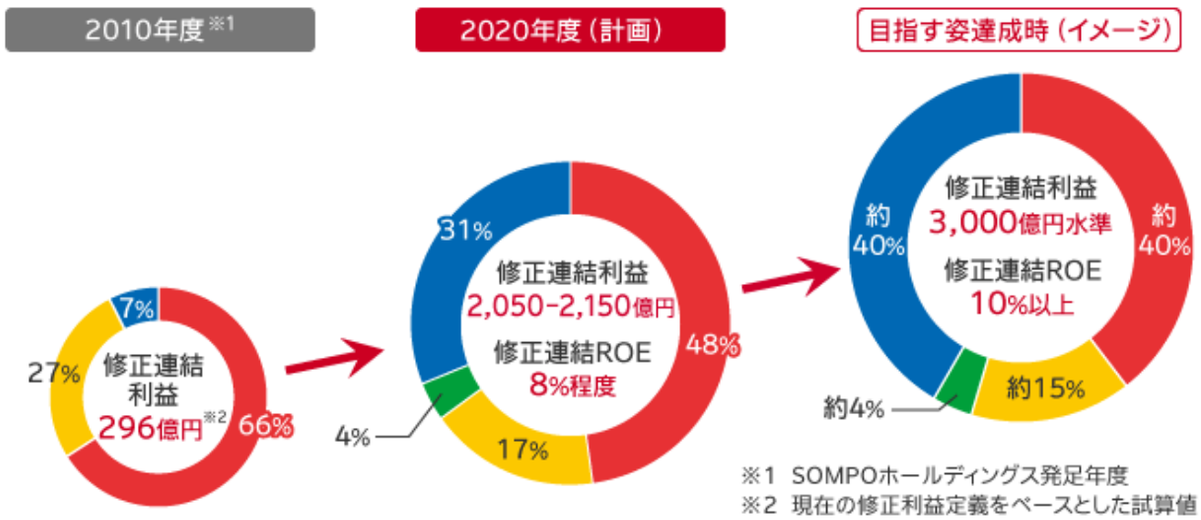
PM学会: 監事　CSA-J: 理事　ISO/TC258(国際PM標準): エキスパート

システムイノベーションセンター(SIC): 理事　JPドメイン名諮問委員会: 委員

日立製作所: ITユーザー会会長　日本IBM: IBM Services Client Advisory Board Member

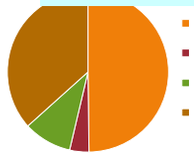
事業ポートフォリオの推移

国内損保事業　海外保険事業　国内生保事業　介護・ヘルスケア事業等



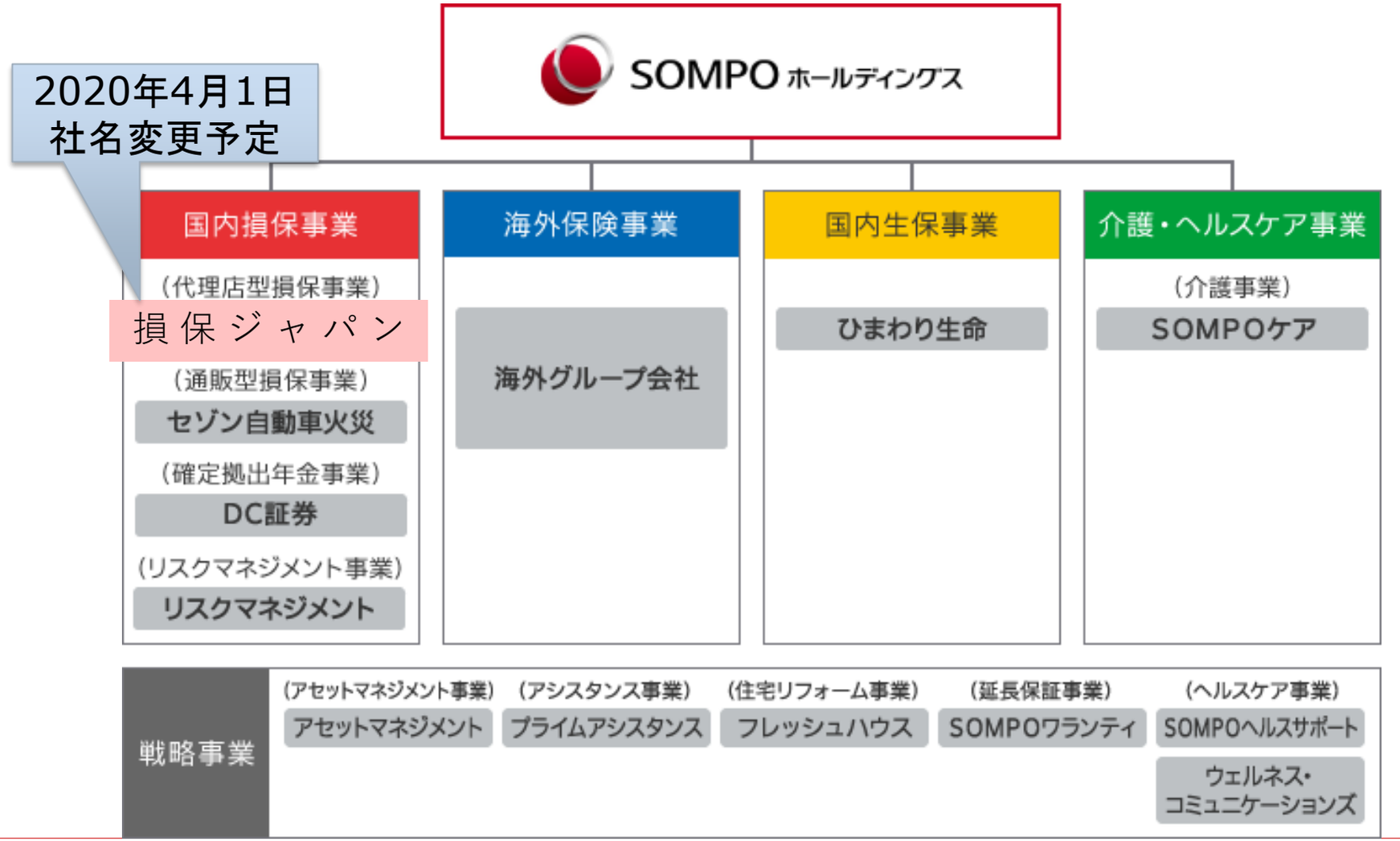
※1　SOMPOホールディングス発足年度
※2　現在の修正利益定義をベースとした試算値

従業員:約80,000人



SOMPOグループストラクチャー

「安心・安全・健康」に生活いただくための幅広い商品・サービスを提供



経団連サイバーセキュリティ経営宣言

経済界は、全員参加でサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献する。サイバー攻撃が激化する2020年の東京オリンピック・パラリンピック競技大会までを重点取り組み期間として、左記の事項の実践に努めることを宣言する。

2018年3月 経団連

1 経営課題としての認識

■経営者自らが最新情勢への理解を深めることを怠らず、サイバーセキュリティを投資と位置づけて積極的な経営に取り組む。
■経営者自らが現実を直視してリスクと向き合い、経営の重要課題として認識し、経営者としてのリーダーシップを発揮しつつ、自らの責任で対策に取り組む。

2 経営方針の策定と意思表明

■特定・防御だけでなく、検知・対応・復旧も重視した上で、経営方針やインシデントからの早期回復に向けたBCP(事業継続計画)の策定を行う。
■経営者が率先して社内外のステークホルダーに意思表明を行うとともに、認識するリスクとそれに応じた取り組みを各種報告書に自主的に記載するなど開示に努める。

3 社内外体制の構築・対策の実施

■予算・人員等のリソースを十分に確保するとともに、社内体制を整え、人的・技術的・物理的等の必要な対策を講じる。
■経営・企画管理・技術者・従業員の各層における人材育成と必要な教育を行う。
■取引先や委託先、海外も含めたサプライチェーン対策に努める。

4 対策を講じた製品・システムやサービスの社会への普及

■製品・システムやサービスの開発・設計・製造・提供をはじめとするさまざまな事業活動において、サイバーセキュリティ対策に努める。

5 安心・安全なエコシステムの構築への貢献

■関係官庁・組織・団体等との連携のもと、各自の積極的な情報提供による情報共有や国内外における対話、人的ネットワーク構築を図る。
■各種情報を踏まえた対策に関して注意喚起することによって、社会全体のサイバーセキュリティ強化に寄与する。

DXの時代？

極端に分業化された日本のビジネス&IT

ビジネス部門とIT部門の役割が明確に分かれた状態でDXができるか

文理分断

ダブルorトリプルメジャーな人材を輩出する必要性

Diversity & Inclusion 思考の欠如

多様性を当たり前にチーム化できる人材

フラット社会（突出人材が出にくい）

機会の平等を推進し、AIなどの突出した技術者が育つ環境を

リカレント教育不足

中高年であっても知識や価値観のアップデートは必須の時代

日本の欠点ばかりに着眼して改善策を見出すようなアプローチのみでは、DXに馴染まないと考える

「令和維新」に必須の経営の理解

DXを理解している企業とは？

① 社長が「イノベーションの源泉がソフトウエアにある」と理解している
② 経営幹部が発表資料を作成している
③ 情報システム部長がソフトウエアを書ける
④ 外部から中途入社の経営幹部がいる
⑤ サブスクリプション型のビジネスモデルを実施している
⑥ マーケティング、開発、運用が一体化した組織がある
⑦ 企業投資・買収部門がある

出典：日経電子版 2020/1/8 大阪大学 栄藤稔教授

要するに、外部から幹部人材を採用し、既存ビジネスを根底から見直し、デジタル技術を駆使した上で、M&Aや企業間のエコ化を前提にビジネスモデルの刷新を推進できる体制を作っているか、ということと理解した

日本発DX「令和維新」

人と組織

経営層（CxO）の深い理解

経営層が、DXの本質を理解し、経営戦略を考え、攻めのIT投資に継続的にコミットしているか

IT部門の確実な改革

IT部門が、管理者層含め最新技術を常にアップデートし、ベンダー任せにせずシステム構築する能力を有するか

全社ITリテラシーの改革

ビジネス部門が、デジタル技術利用によるビジネス変革を考案、市場投入しビジネス変革を実践しているか

ビジョンと戦略

協創前提のDX構想

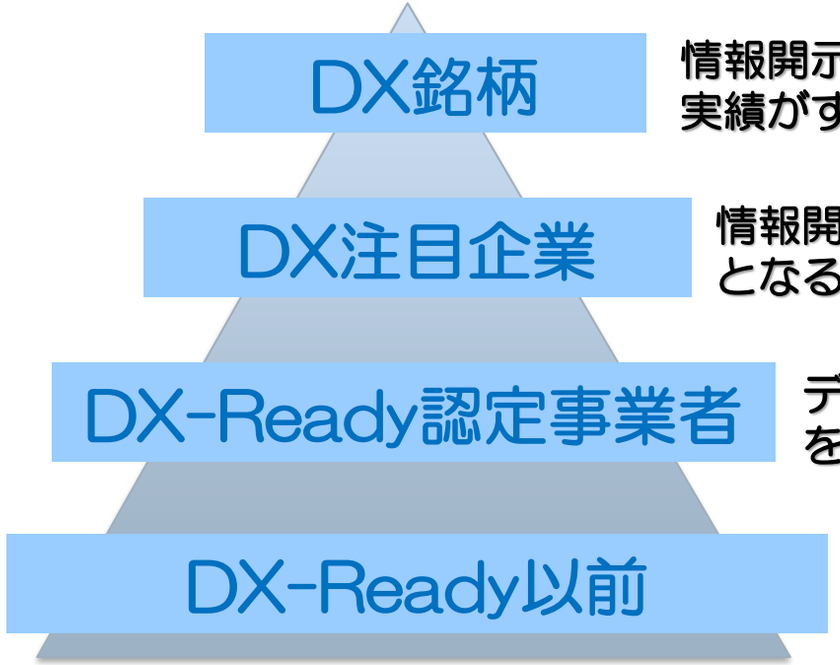
日本のDXの真髄である協創を具現化し、自社の強みをさらに増幅できているか

中長期的なLX・DX実施

LXの計画的遂行によりコスト効率化を実現し、DX-Readyな企業にシフトできているか

経済産業省がリードするDX推進

商務情報局 「Society5.0時代のデジタル・ガバナンス検討会」で、2020年5月に認定制度などを立ち上げる想定



情報開示を積極的に行い、優れたデジタル活用実績がすでに現れている企業

情報開示を積極的に行い、優れたプラクティスとなる企業

デジタル変革を進め、デジタルガバナンスを向上する準備が整っている企業

行動原則
デジタルガバナンスコード

原則1：ビジョン構築
原則2：デジタル戦略策定
原則3：体制構築と関係者との協業
原則4：デジタル経営資源の適正配分
原則5：デジタル戦略の実行と評価

当職も委員として参加、企業側目線でDXの普及に必要と思われる視点で議論を実施中

ユーザー企業回帰の勧め

IT開発を取り巻く新潮流

1. Security-Native化

2. AI-Native化

3. Cloud-Native化

4. Agility-Native化

ユーザー企業IT部門の実力回帰が急務

1. Security-Native化	情報セキュリティ・サーバーセキュリティ徹底の常識化
2. AI-Ready化	AI機能を当たり前のように情報システムへ組み込み化
3. Cloud-Native化	SaaS/PaaSかつマルチクラウドベースで対応速度改善を
4. Agility-Native化	開発スタイルの改革の断行

これらのトレンドは、いずれもIT人材の過半数がユーザー企業に所属する欧米諸国発のトレンドであり、ベンダー依存体質の強い我が国では、推進の足かせになっている

日本も、IT技術力・デジタル技術力をIT企業から取り戻さねば、DXのスピード感に追いつけない時代

IT部門上層部のテクノロジー課題

最新技術・手法を探求していないIT部門のマネジメント層がボトルネックになっている

最近当職にあった相談	理解しておくべき技術領域例
パブリッククラウドで開発をしたいがコンテナ技術を選択すべき？	クラウド技術
AIプロジェクトで学習済モデルの品質が高まらないが本稼働していいか	データ×AI
アジャイル開発のスプリント後半で画面標準の手戻りが多発したが全て修正すべきか	オープン技術
バッチ業務をマイクロサービスを意識しrestAPIで疎結合化したが、パフォーマンスが出ない	アジャイル
	マイクロサービス

90年代のオープン系シフト、その後のインターネット技術への進化の時とは比較にならないくらいキャッチアップ遅れが深刻化している

Security-NativeなOpen環境がもたらす次世代課題例

SaaS/PaaSのクラウド環境とK8s　開発課題

クラウドは、生産性や基盤運用負荷の容易さから、今後はIaaSよりもSaaS/PaaS主流の時代と考えているが、セキュリティポリシーの徹底が大前提

マイクロサービス化とAPIマネジメント　デザイン課題

マイクロサービス化とAPI管理は、今後の主流と捉えているが、並行して脆弱性による脅威も飛躍的に増すことが想定される

CI/CDとDevOpsの実用化　運用課題

業務サイクルの高速化、ソフトウエアの脆弱性対応から、CI/CDサイクルの迅速化が大きな課題。DevOpsを加速させ、圧倒的なスピードでDXを進める運用部門改革が急務

Security感応度の醸成　人材課題

IT部門の各層（トップ層、管理者層、担当層）、各部門（アプリ、基盤、運用）でのセキュリティ意識の醸成は今や死活問題

DX-Readyと
Security-Ready

DX-Ready

企業としてDXを推進するために、テクノロジー観点では以下の４つのReadyが前提条件になるのではないか

DX-Ready

① AI-Ready
経営・ビジネス・IT部門それぞれがAIを理解し、DXのエンジンに

② Agile-Ready
IT部門・ビジネス部門共に、アジャイルを当たり前の文化に

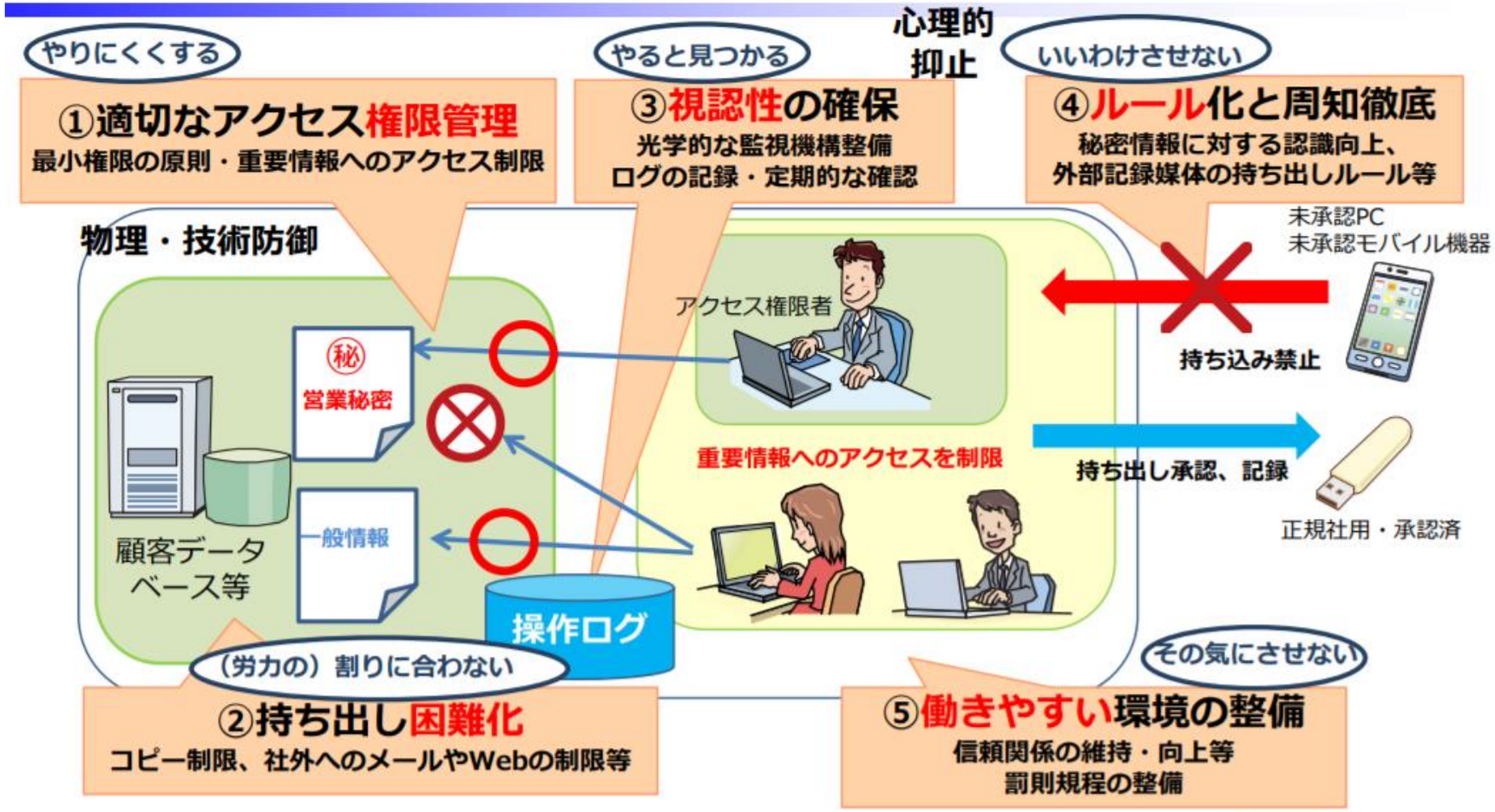
③ Cloud-Ready
オンプレミス環境であっても、段階的にクラウド移行可能な状態に

④ Security-Ready
情報セキュリティ・サイバーセキュリティを徹底し、DXに専念できる状態に

Security-Ready

情報セキュリティは、どこからでも攻撃を受ける環境にあることを認識し、網羅的な対策を施すことが求められている

Security-Ready：情報セキュリティ対策の継続改善



出典：IPA 情報セキュリティHP

サイバー攻撃手法

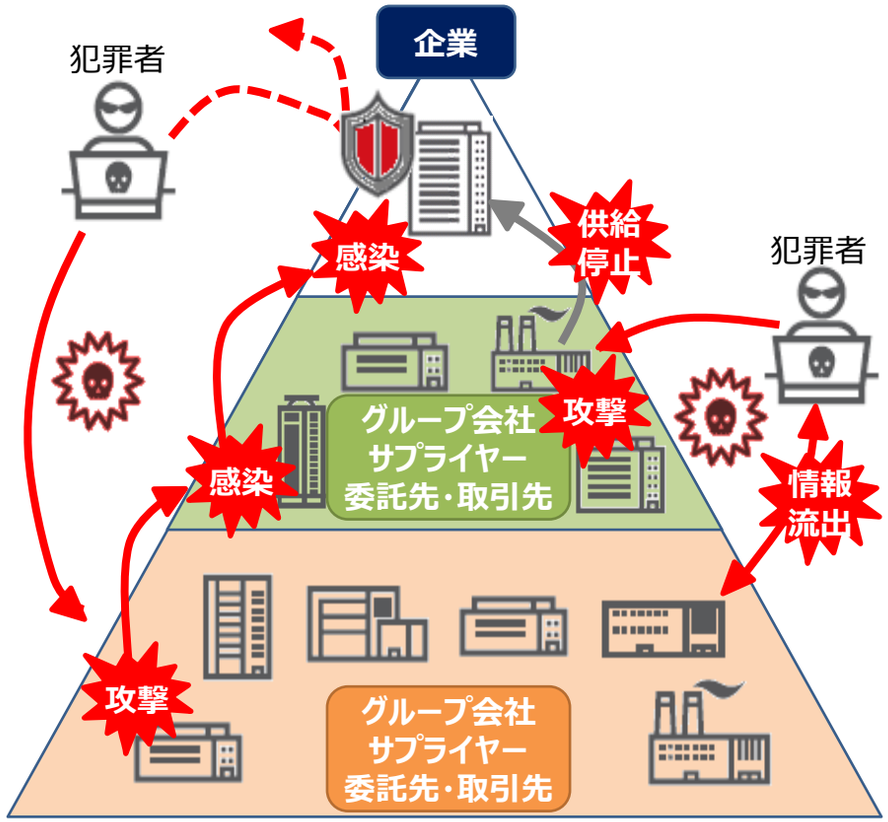
近年のサイバー攻撃の多くは、「システムの脆弱性」を狙った侵入

2020順位	昨年順位	内容
1	1	標的型攻撃による被害
2	5	内部不正による情報漏洩
3	2	ビジネスメール詐欺による被害
4	4	サプライチェーンの弱点を悪用した攻撃の高まり
5	3	ランサムウエアによる被害
6	16	予期せぬIT基盤の障害に伴う業務停止
7	10	不注意による情報漏洩
8	7	インターネットサービスからの個人情報の窃取
9	8	IOT機器の脆弱性の顕在化
10	6	サービス妨害攻撃によるサービスの停止

出典：IPA「情報セキュリティ10大脅威 2020」

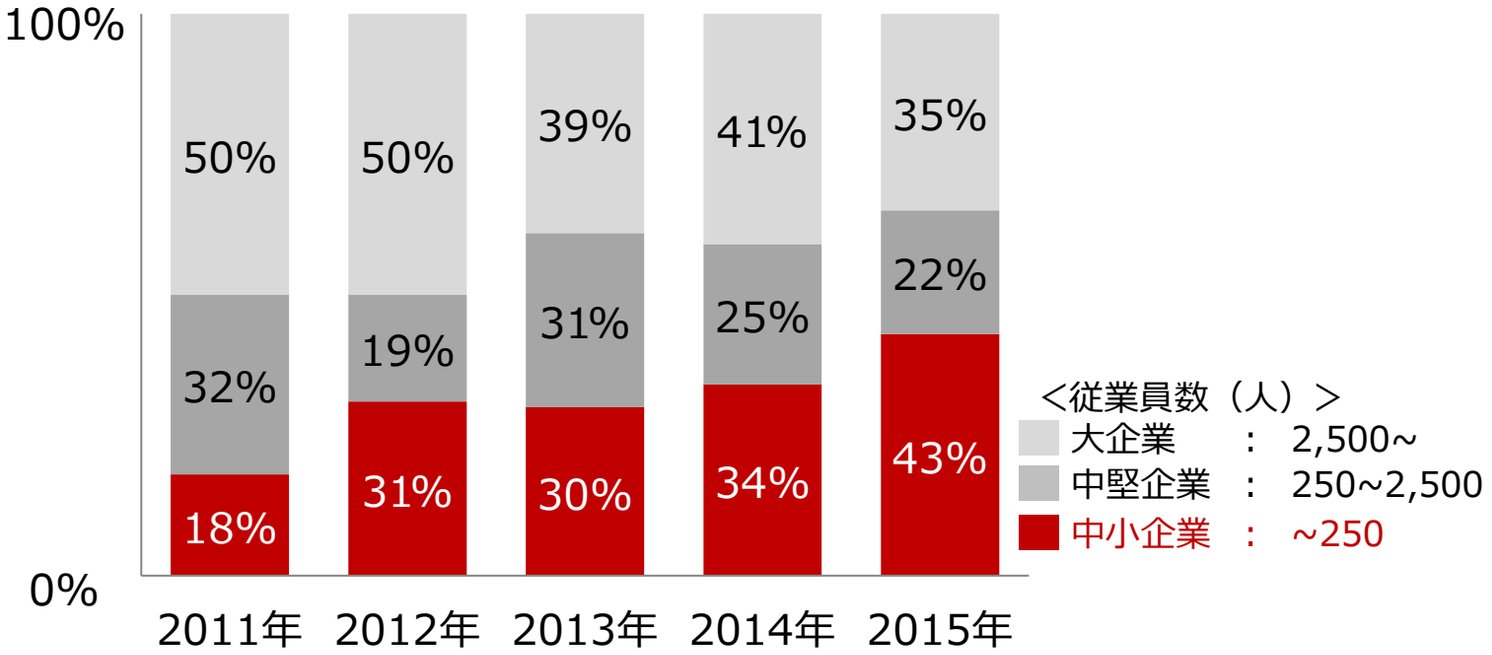
サプライチェーン攻撃手法

✓ **自社のサプライヤー等のセキュリティ対策状況も管理することが重要**



✓ **サプライチェーンの中小企業のセキュリティ対策は必要不可欠**

■スピアフィッシング攻撃の標的となった企業の規模別割合[1)]

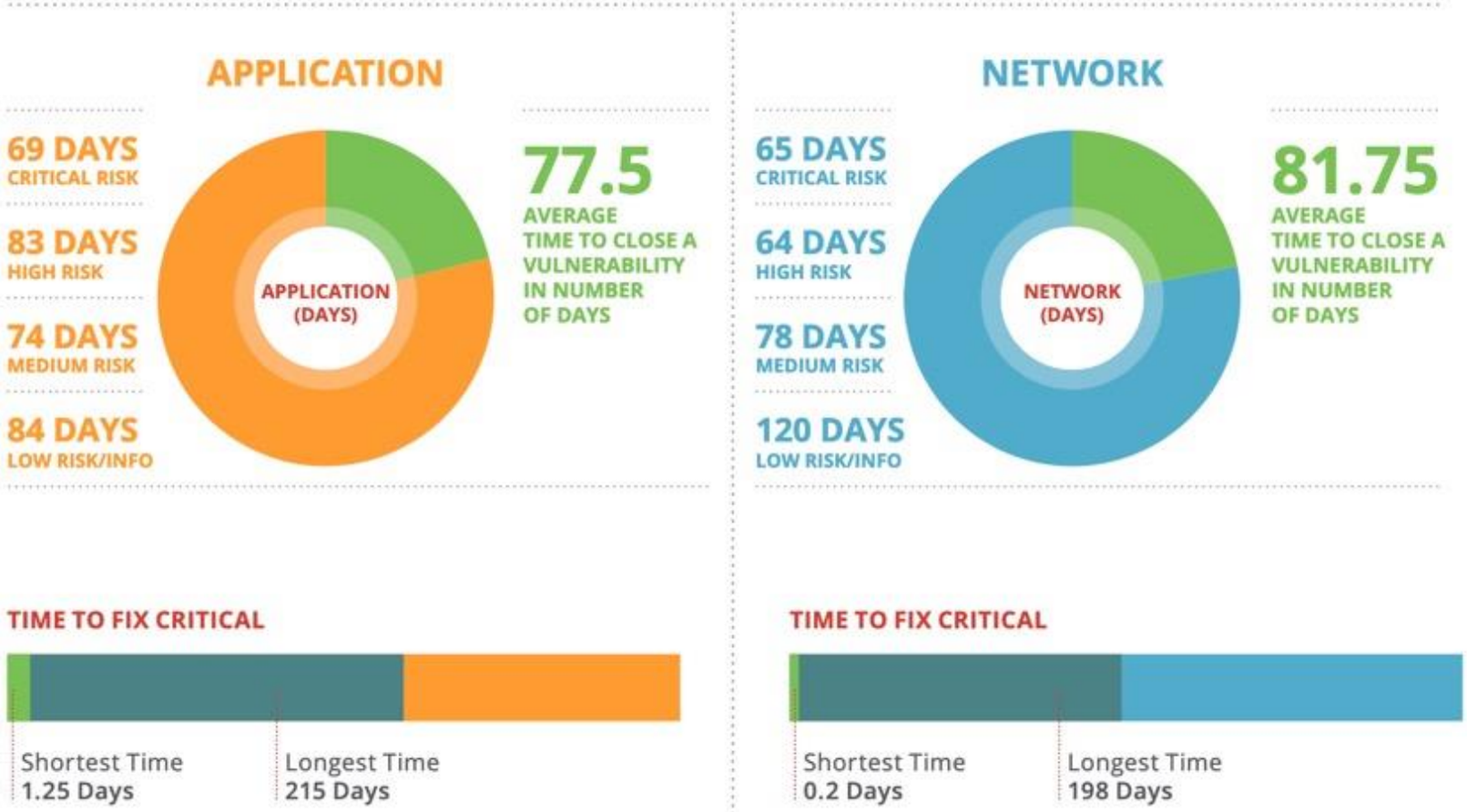


スピアフィッシングとは？？
通常のフィッシングと違い、「特定の企業」の「特定の人物や社員」を標的にする

出典：Internet Security Threat Report, Symantec, 2018

基幹系のオープンシステム化に伴う脆弱性リスク

意外と知られていないが、商用ソフトウエアではオープンソースが多用されており、脆弱性リスクが飛躍的に高まっている



❶ 膨大な脆弱性

左図の通り、脆弱性の適用サイクルは短期化しており、運用は容易ではない

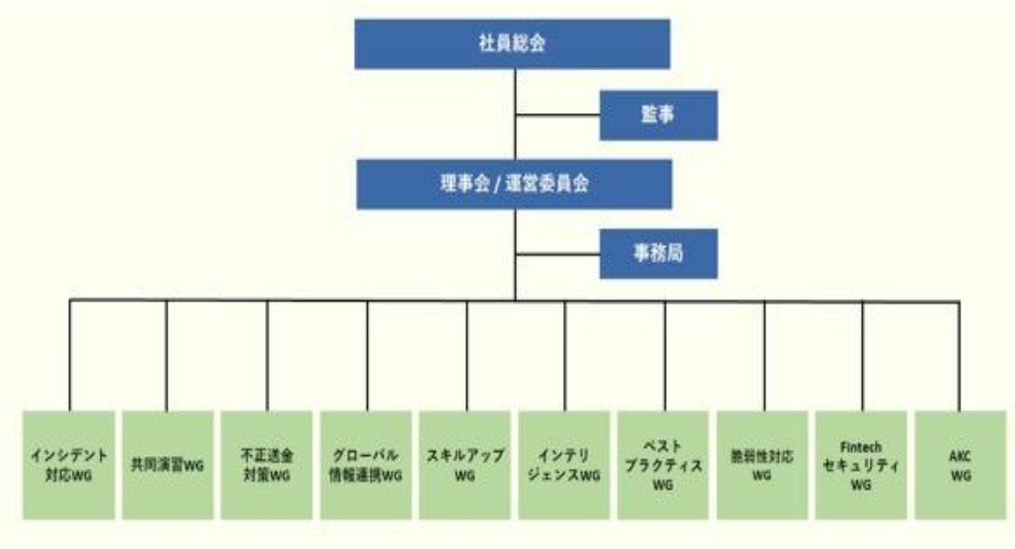
❷ 容易ではないマッチング

ソフトウエア資産情報と脆弱性情報をマッチングしたり、脆弱性スキャンによるトリアージを実施するも、チケット管理は容易ではない

出典：https://landing.edgescan.com/vulnerability-stats

金融ISACの取り組み

業界毎のISAC組織に積極関与し、情報連携、ノウハウ蓄積などの取り組みを、より積極的に行うべき時代



出典：金融ISAC HP

インシデント対応WG
従来は危機管理対応やBCPの一環として行っていたインシデント対応をサイバーセキュリティ特有のインシデントという観点から見直し、基本手順の検討やマニュアルの作成について議論し、成果物を会員間で共有していきます。

共同演習WG
会員各社が連携して行う「共同サイバー演習」の企画・運営をするとともに、国内外で行われているサイバー演習の事例やノウハウの収集と共有を推進していきます。

不正送金対策WG
主にバンキングマルウェアによる攻撃の最新手口とその対策の収集と共有を行いながら、不正送金対策のベストプラクティスを検討していきます。

グローバル情報連携WG
米国FS-ISACとの情報共有範囲の拡大を図り、共有可能な各種情報のローカライズ（日本語化）を行うなどの活動を実施していきます。

スキルアップWG
金融機関のセキュリティ担当として必要な知識やスキル、金融ISACにおいて共有された情報を活用するスキルの確保・向上に取り組み、各種勉強会などを企画・実施していきます。

インテリジェンスWG
様々な情報ソースから攻撃傾向や近い将来に発生が想定される攻撃、攻撃手法等を類推・予測することを試み、加えて効果的な防御体制の準備・構築についても検討・議論していきます。

ベストプラクティスWG
金融機関におけるサイバーセキュリティ対策として、会員各社のノウハウ・知見に基づいた、「実践力のある、生きた取り組み」をベストプラクティスとしてとりまとめます。

脆弱性対応WG
製品プログラム・システム物理機器に焦点をあて、脆弱性対応の方法を検討します。また、脆弱性に関する会員間の情報共有・連携の方法についても検討し、とりまとめます。

FinTechセキュリティWG
新しい技術及びその利用方法を表す用語として広がっているFinTechについて、セキュリティ上のリスクと強化について検討します。また、関連諸団体、FinTech企業との連携を図ります。

AKC （Active Knowledge Center）WG
サイバーセキュリティ対策について、どのように進めればよいか分からないという悩みを持つ会員企業に対し、各々の身の丈に合った施策が実行できるよう、各地域に出向きつつ、機動的かつ具体的なサポートを実現していきます。

Cyber Week @Tel Aviv

日本でのサイバーセキュリティに関する取り組みや、イスラエルのスタートアップ企業への期待などについて、SOMPO HDとしてパネル講演を実施

Special Response Unit for Tokyo2020

SOMPOの取り組みとして、特別体制を配備。インシデントレスポンスに加え、平時はダークウェブ等から攻撃の予兆を調査し、脅威分析に活用する

SOMPO-HD CSIRT

Special Response Unit for 2020

グループ各社

SOMPO CYBER SECURITY
powered by SOMPO RISK MANAGEMENT

オリパラ開催中は国内に**常駐（1~2名）**
5日間のRed Team演習も実施予定

リモートで**常時スタンバイ（24/365）**
（複数名）

超高度技術者

テクニカルメンバー
【元CSIRTマネージャー】

Cyber Researcher
【元IDF8200部隊出身】

CYE

Incident Response

イスラエル国防軍8200部隊等で経験を積んだ実績豊富な専門家が、国家レベルの方法論と技術を駆使したフォレンジックにより、被害範囲を評価・脅威を特定して攻撃を封じ込め、コア資産への損害を防止

SOMPOグループに関連する脅威情報を
ダークウェブ等から収集、提供

SenseCy
A VERINT Company

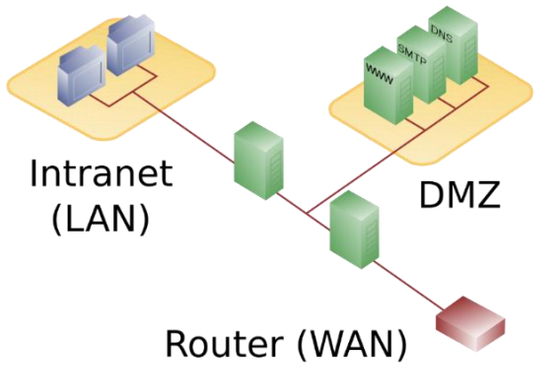
Threat Intelligence

ダークウェブを含めたサイバー空間に漏洩している情報（ブランド名、役員の氏名、ドメイン名、IPアドレス等）や攻撃キャンペーン情報を独自のツールを使って集約・蓄積・分析し、早期警戒情報と実用的な知見を提供

Security-Readyに向けて

セキュリティ管理や重要な判断を下すために、以下を理解し、徹底することが重要。

- **自社・自組織のシステムの全貌と運用実態**
- **問題となっている攻撃手法**
- **発動の影響範囲**



経営層・管理者層は、DXの推進には積極的だが、自社のビジネスを適応・変革させることを優先し、サイバーセキュリティは後回しになりがち

まとめ

DX-Ready推進のKSF

1.　日本発DXの理解

制度・業界・企業の壁が日本では、自律分散型で段階的に接続しながらDXを実現出来るインフラ整備が一つのヒント

2.　ユーザーIT部門の復権

4つのIT新潮流により、ユーザー企業側が一定レベル復権していかないと、日本発DXは進まないと危惧

3. DX-Ready(Security-Ready)の理解

Security-Readyを軸に、DX-Readyな企業が増えれば、DXを基軸とした協創が進み出し、日本独自のDX環境が醸成されていくと確信している


ご清聴ありがとう
ございました！


DIGITAL
TRUST

Microsoft

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

データ駆動型社会（Data Driven Society）
パーソナルデータの保護と利活用
～ トラストの実現に向けて ～

Panelists

石井　夏生利様

中央大学
国際情報学部教授

志済　聡子様

中外製薬株式会社
執行役員
デジタル・IT統括部門長

片山 建

日本マイクロソフト株式会社
政策渉外・法務本部
デジタル政策部長

Kaori Ishii

Satoko Shisai

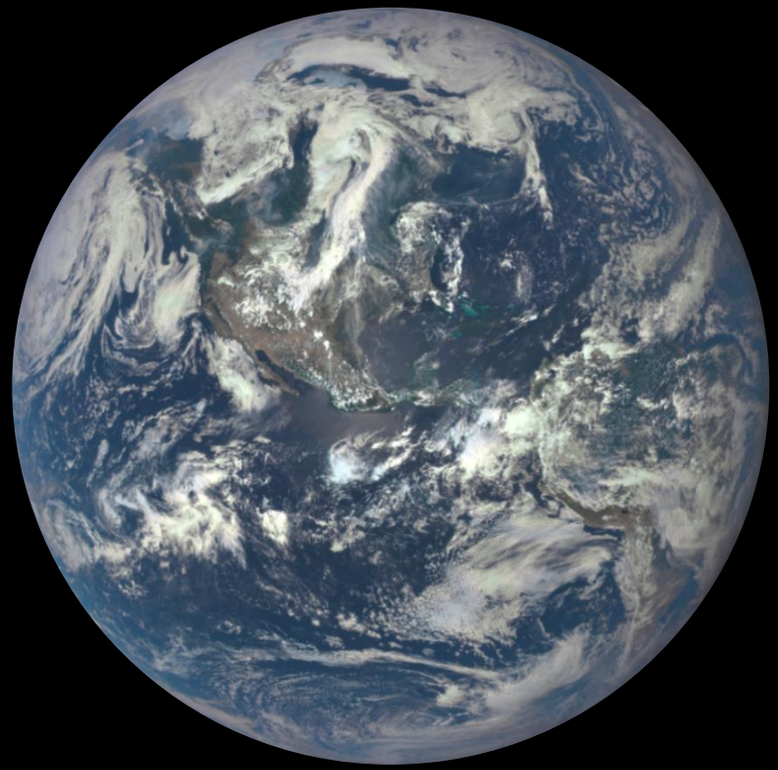
プライバシー：

利活用と保護のバランス

プライバシーは基本的な人権です

Microsoft mission

Empower every person and every organization on the planet to achieve more

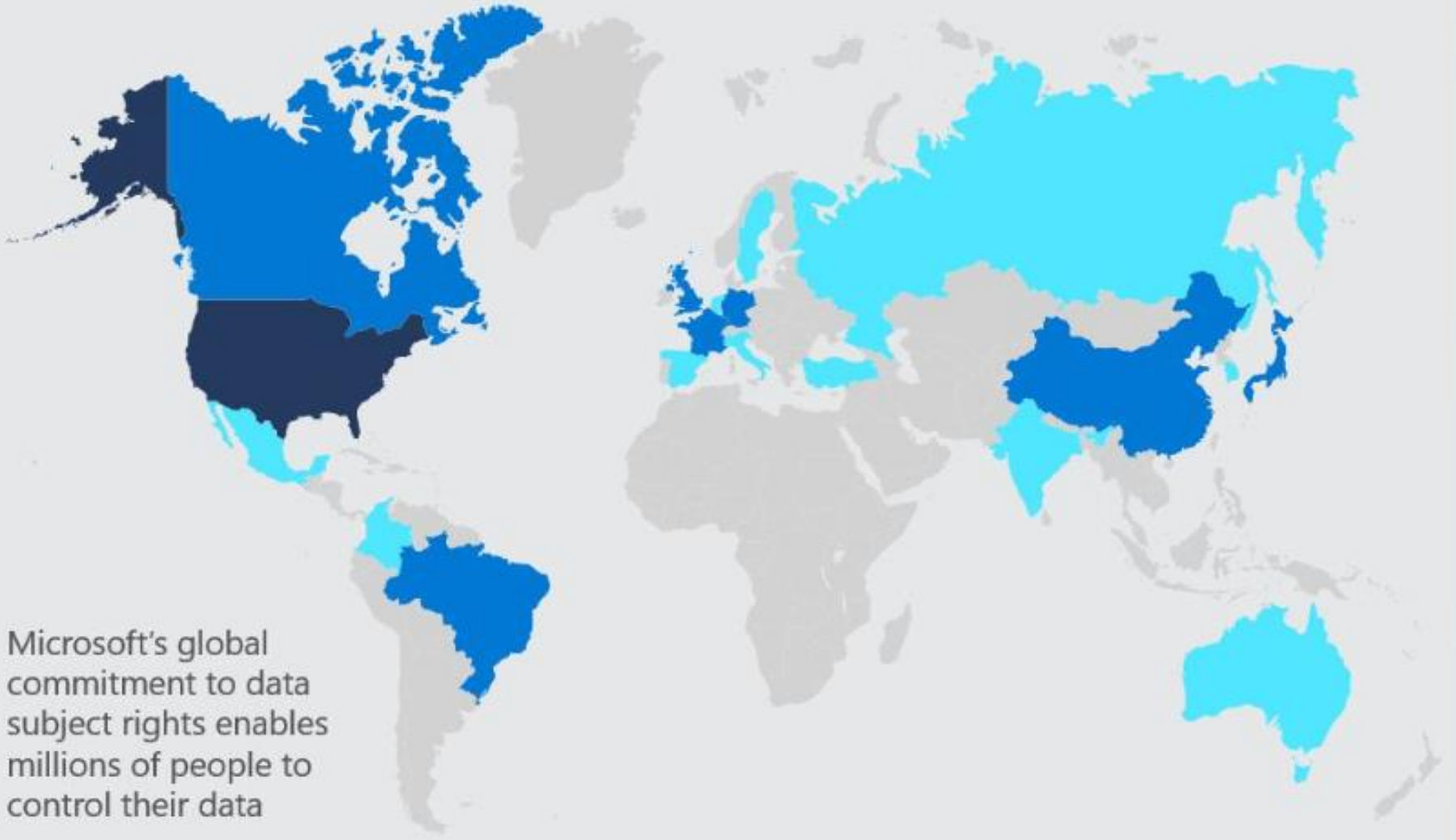


“地球上のすべての個人とすべての組織がより多くのことを達成できるようにする”

Microsoft

GDPR

18 Million People Around the World Use Microsoft's Dashboard to Interact with their Data in the First Year of GDPR

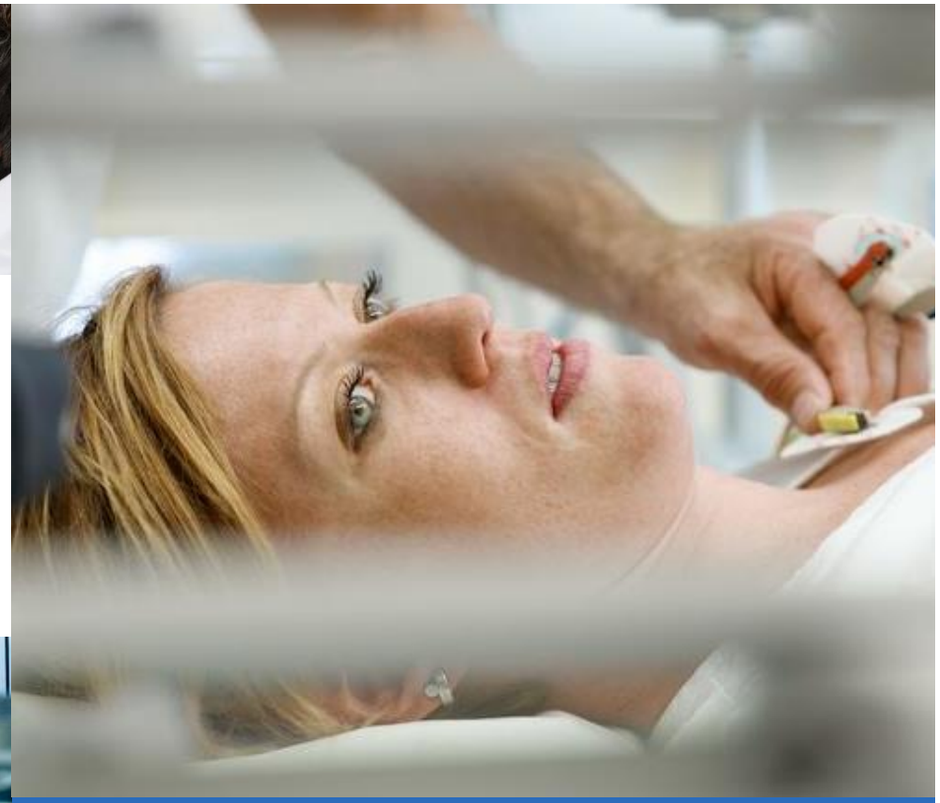


Microsoft's global commitment to data subject rights enables millions of people to control their data

Top 20 Countries

Countries	Number of users
United States	6.7 million
Japan	1.4 million
United Kingdom	1.3 million
France	807,000
Canada	726,000
Brazil	673,000
Germany	615,000
China	435,000
Mexico	384,000
Australia	378,000
Italy	315,000
Spain	292,000
Netherlands	271,000
India	269,000
South Korea	217,000
Turkey	188,000
Russia	172,000
Belgium	163,000
Colombia	145,000
Sweden	135,000

中外製薬について



Roche

CHUGAI 中外製薬

Roche ロシュ グループ

医療用医薬品の研究開発・製造・販売

がん領域11年連続国内トップシェア

バイオ・抗体医薬品で革新的創薬

2002　ロシュと戦略的パートナーシップ締結

中外製薬のGDPRへの対応

・2017「個人情報保護に関するポリシー」制定
　グループ間での標準契約条項に基づく契約締結
・海外子会社へのローカル・ガイドライン整備及び
　報告体制整備
・ロシュとの標準契約条項に基づく契約締結

中外製薬の海外拠点　　ロシュ本社

GDPR

- 標準契約条項　SCC

GDPR

- 十分性　Adequacy
- 2019年1月23日

GDPRの透明性

CHUO UNIVERSITY
FACULTY OF
GLOBAL INFORMATICS

<u>データ主体(本人)の権利(第12条～第14条)</u>

- 簡潔かつ透明で、分かりやすい情報提供
- 本人から情報を収集する場合に提供すべき情報
- 本人以外から情報を収集する場合に提供すべき情報

アカウンタビリティの重要性

アカウンタビリティ

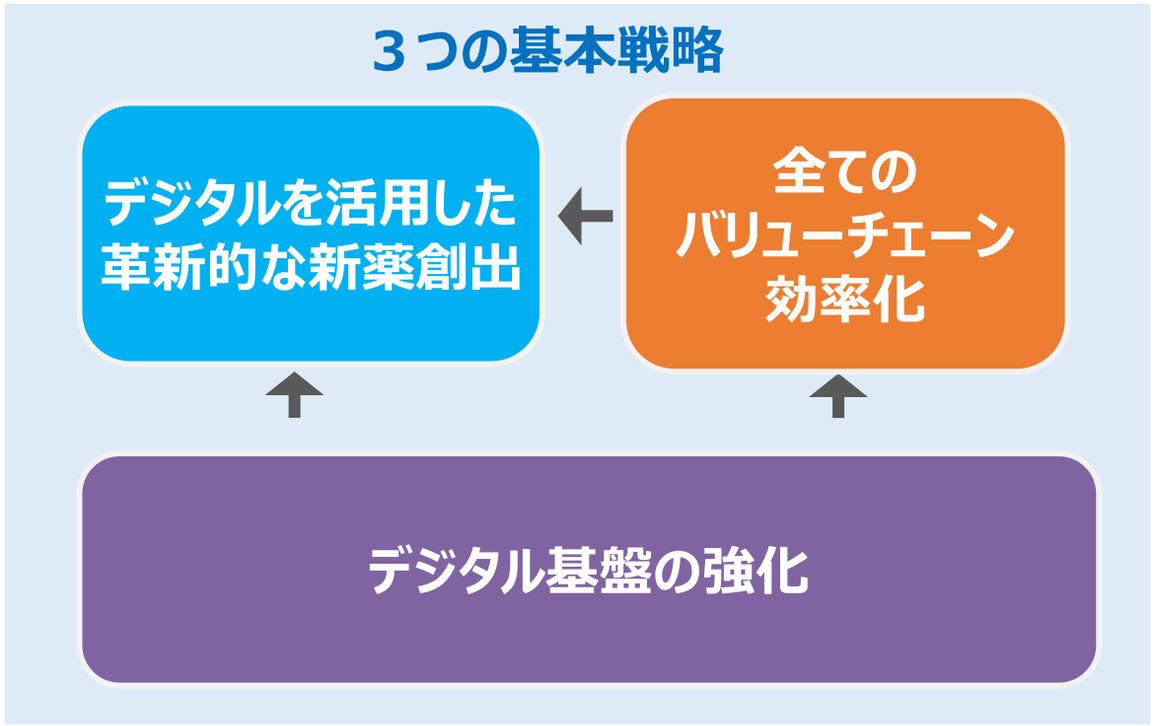
Accountability

中外製薬のデジタルビジョンと戦略

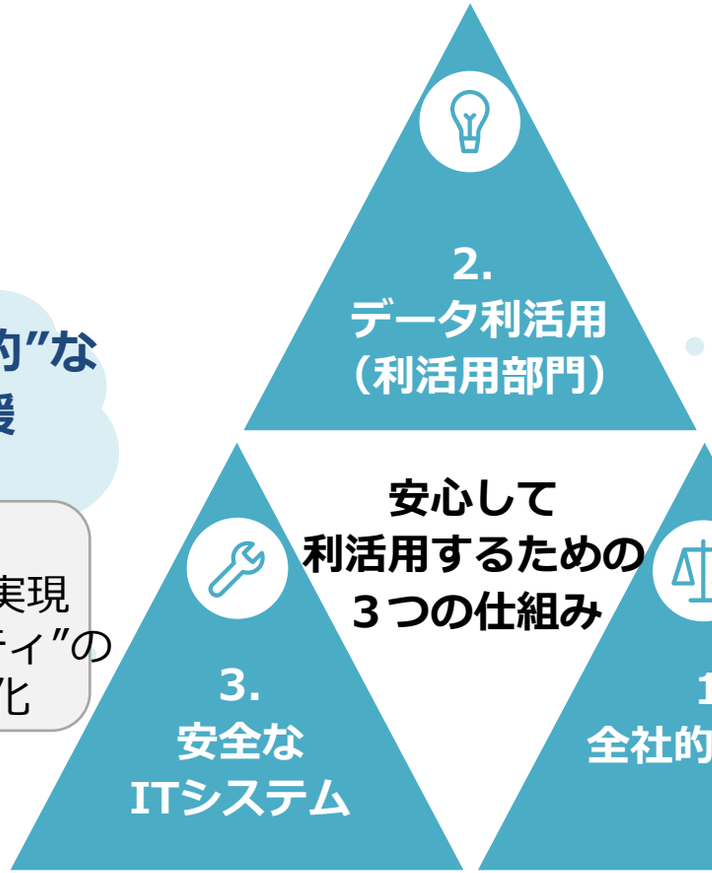
CHUGAI DIGITAL

CHUGAI DIGITAL VISION 2030

デジタル技術によって中外製薬のビジネスを革新し、
社会を変えるヘルスケアソリューションを提供する
トップイノベーターになる



中外製薬のデジタルコンプライアンス活動



デジタルコンプライアンスに関する社員のリテラシー向上

主要課題
- 継続的な教育の仕組整備

“セキュア x 効率的”な基盤整備の支援

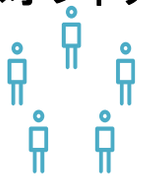
主要課題
- 環境評価の“保証“の実現
- ”デジタルセキュリティ”の定義と機能・体制強化

先進的取り組みを支える全社方針/仕組みの提供

主要課題
- 足元の機能・体制強化
- デジタル戦略推進との連携
- ”デジタルコンプライアンス”の再定義と機能・体制強化

デジタルコンプライアンス委員会

ヒト由来データの利活用に関する利活用部門からの相談事項及び
全社デジタルコンプライアンス方針について検討・決定する

	構成員	役割
委員長 	• 担当部長	• 委員会検討結果の承認・回答書への署名 • 基本方針に関する事項は更にエスカレーション
委員 **（デジタルコンプライアンスオフィサー）** 	• 利活用部門から選出されたデジタルコンプライアンスオフィサー	• 利活用部門からの個別相談事項の討議と対応策の決定 • 全社デジタルコンプライアンス方針の検討 委員は個別案件および方針策定において利活用部門視点での意見を提供する
事務局	• 担当部内の担当グループ	• 付議者からの相談事項の整理 • 委員会の運営

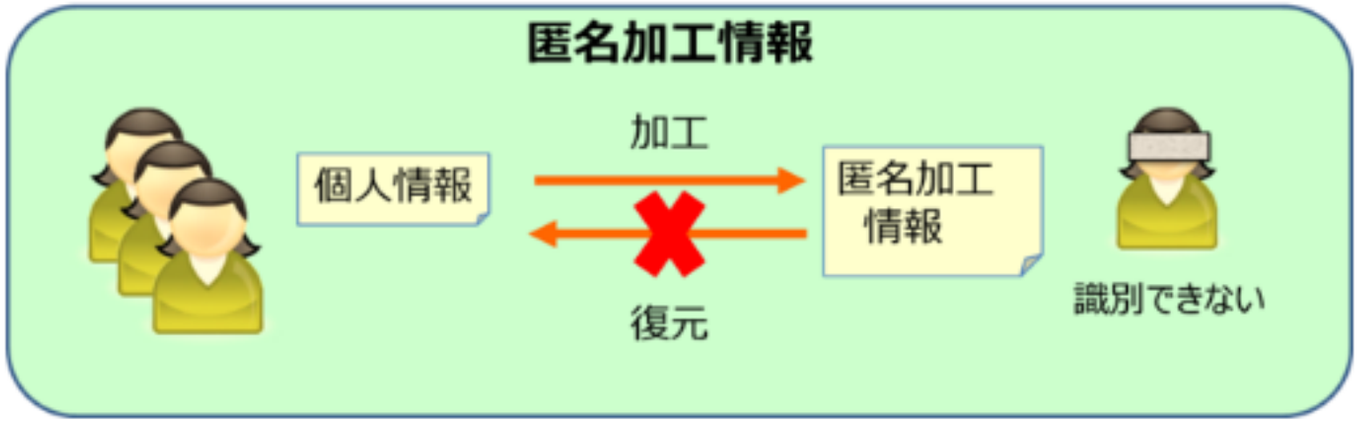
国際標準の重要性

- ISO/IEC 27701
- Data Protection Mapping Project

匿名加工情報とは

匿名加工情報とは、特定の個人を識別することができないように個人情報を加工し、当該個人情報を復元できないようにした情報のことをいいます。

また、匿名加工情報は、一定のルールの下で、本人同意を得ることなく、事業者間におけるデータ取引やデータ連携を含むパーソナルデータの利活用を促進することを目的に個人情報保護法の改正により新たに導入されました。

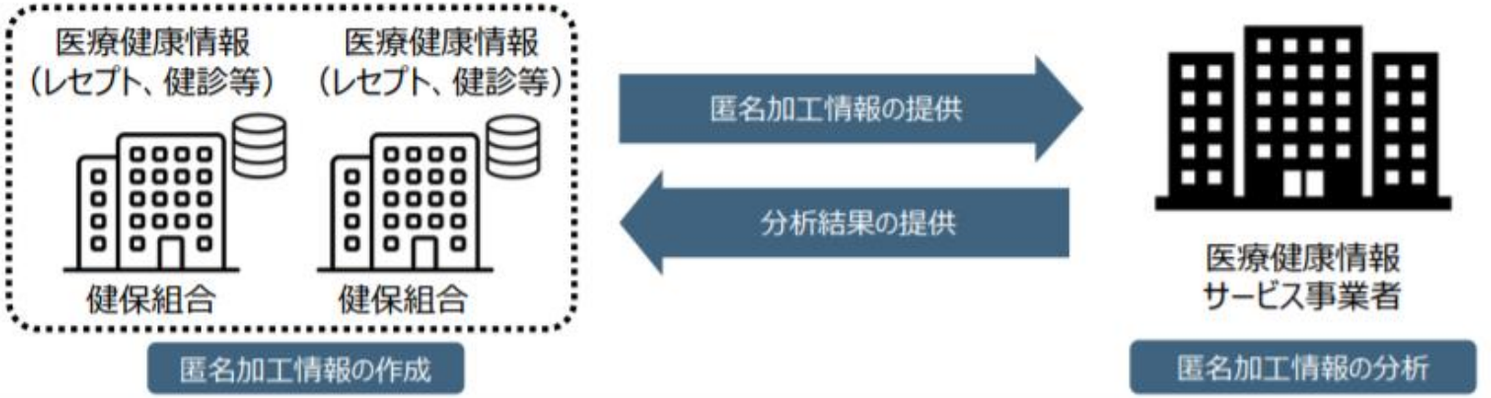


クレジットカード情報、物流ドライバーの運行、健康診断情報、Wi-Fi位置情報、医療健康情報、観光客情報など

個人情報保護委員会「匿名加工情報制度について」(https://www.ppc.go.jp/personalinfo/tokumeikakouInfo/)

事例５　医療健康情報の利活用

- 本事例では、健康保険組合が保有する組合員の医療健康情報について匿名加工情報の作成を行い、匿名加工後の情報を医療健康情報サービス事業者へ第三者提供を行うものである。
- 匿名加工情報の提供先である医療健康情報サービス事業者では、匿名加工情報を使った各種分析を行っている。



匿名加工の対象となる個人情報		適用情報、レセプト情報、健診結果情報
匿名加工情報の利活用目的		健保組合では、組合員個人の各種医療健康情報を保有しており、独自にデータの分析等を行っているが、個人情報を含むデータなので、そのまま取り扱うことには様々な制約がある。そのため、保有しているデータを匿名加工して専門的な分析機関に提供することで、よりスムーズにデータ分析を行うこととした。将来的にはAI等も活用し、組合員の生活習慣の改善につながる、企業の健康経営に向けた様々なサービスの材料としていくことを見据えている
匿名加工に用いた手法	適用情報	氏名、住所、生年月日、保険者番号、保険証記号・番号、加入日・脱退日、個人識別キーは削除。制度区分、性別、続柄はk-匿名化をベースとした加工
	レセプト情報	個人識別キー、レセプトキー、医療機関は削除。診療年月は個人の生年月からの月数に置換え。傷病名は削除して傷病コードを掲載。診療行為コードは特異な診療行為を除外。医薬品情報は特異な医薬品情報を除外
	健診結果情報	個人識別キーは削除。健診受診年月日は個人の生年月からの月数に置換え。検査値は外れ値を処理（トップコーディング、ボトムコーディング）。問診項目は加工なし
匿名加工情報の提供方法		対象データ群を暗号化した上で外部記録媒体（DVD-ROM等）に保存し手交する

野村総合研究所「パーソナルデータの適正な利活用の在り方に関する動向調査」事例集サマリ(平成31年3月)(https://www.ppc.go.jp/files/pdf/jireisyu_summary_201903.pdf)6頁

仮名加工情報の創設

CHUO UNIVERSITY
FACULTY OF
GLOBAL INFORMATICS

- 2020年3月10日閣議決定
- 「仮名加工情報」：個人情報に含まれる記述等の削除等により他の情報と照合しない限り特定の個人を識別することができないように加工した情報。
- イノベーションを促進する観点から、氏名等を削除した「仮名加工情報」を創設 し、内部分析に限定する等を条件に、開示・利用停止請求への対応等の義務を緩和する。

個人情報保護委員会「「個人情報の保護に関する法律等の一部を改正する法律案」の閣議決定について」(2020年3月10日)(https://www.ppc.go.jp/news/press/2019/20200310/)より

公益性

CHUO UNIVERSITY
FACULTY OF
GLOBAL INFORMATICS

- 「個人情報」に処理を施すアプローチ
  - ✓匿名加工情報、仮名化
- 個人情報の「取扱い」に着目するアプローチ
  - ✓公益性
    - ➢学術研究、社会福祉、青少年保護、文化の発展、教育の振興、環境保全、犯罪の抑止、高齢者の雇用安定、障害者支援、スポーツ振興、貧困の解消、動物愛護など


がんではない。
ひとりを見つめるのだ。
私は何と闘っているのだろう
がん細胞？
いや　向き合うべき相手は
ひとりの人間ではないのか
ひとつとして同じ遺伝子はない
つまり　同じ答えはない
一人ひとりの遺伝子変異に基づく
がん医療に貢献しています。
創造で、想像を超える。
すべての革新は患者さんのために
CHUGAI
中外製薬
Roche
ロシュ グループ

Microsoft
Security Forum 2020

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

まとめ

Microsoft

アカウンタビリティ

Accountability

公的部門の電子化

CHUO UNIVERSITY
FACULTY OF
GLOBAL INFORMATICS

- データ駆動型社会はプラットフォーマーやグローバル事業者のみの議論ではない。
- 公的部門のデジタル(行政の電子化)を含めた一体的なデジタルトランフォーメーション

デジタル手続法の概要（令和元年12月施行）

デジタル技術を活用し、行政手続等の**利便性の向上**や**行政運営の簡素化・効率化**を図るため、
行政のデジタル化に関する基本原則及び行政手続の原則オンライン化のために必要な事項等を定める。

○行政手続オンライン化法の改正

デジタル技術を活用した行政の推進の基本原則

①**デジタルファースト**：個々の手続・サービスが一貫してデジタルで完結する
②**ワンスオンリー**：一度提出した情報は、二度提出することを不要とする
③**コネクテッド・ワンストップ**：民間サービスを含め、複数の手続・サービスをワンストップで実現する

行政手続のデジタル化のために必要な事項

行政手続におけるデジタル技術の活用

行政手続のオンライン原則

- 国の行政手続（申請及び申請に基づく処分通知）について、**オンライン化実施を原則化**
（地方公共団体等は努力義務）
- **本人確認**や**手数料納付**も**オンラインで実施**
（電子署名等、電子納付）

添付書類の省略

- **行政機関間の情報連携**等によって入手・参照できる情報に係る添付書類について、**添付を不要とする規定を整備**
（登記事項証明書（令和２年度情報連携開始予定）や住民票の写しなどの本人確認書類等）

デジタル化を実現するための情報システム整備計画

- オンライン化、添付書類の省略、**情報システムの共用化、データの標準化、APIの整備、情報セキュリティ対策、BPR等**

デジタルデバイドの是正

- デジタル技術の利用のための能力等の格差の是正
（高齢者等に対する相談、助言その他の援助）

民間手続におけるデジタル技術の活用の促進

- 行政手続に関連する民間手続のワンストップ化
- 法令に基づく民間手続について、支障がないと認める場合に、デジタル化を可能とする法制上の措置を実施

首相官邸「デジタル手続法」(kantei.go.jp/jp/singi/it2/hourei/pdf/digital_gaiyo.pdf)


DIGITAL
TRUST

お客様へのご支援

リモートワークに取り組む組織に向けて、無料相談窓口を開設

セキュア リモートワーク相談窓口（無料）
お電話でのご相談は 0120-167-400 まで
Web からのご相談こちら >

無償ライセンス・サービスを提供

法人向け

- Office 365 E1 ライセンスの 6 ヶ月無償提供
- Microsoft Teams トレーニングの無償提供
- Microsoft Teams Live Event サービスの実施支援

教育機関向け

- Office 365 A1 ライセンスの無償提供
- オンラインイベント配信用機材として、Surface を無償貸与
- Minecraft: Education Editionを無償提供（A1アカウントが必要）

DIGITAL TRUST Summit 2019

次のセッションのご紹介

特別セッション:
WVD で在宅勤務応援キャンペーン開始!
WVD だから実現できる早急なリモートワーク環境構築

DIGITAL TRUST

Microsoft

Microsoft
DIGITAL TRUST
SECURITY

#digitaltrust