明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

資料52-6

深刻化・増大・加速するサイバーリスク対応に必要なサイバー攻撃対処能力の向上（国産化）

情報セキュリティ大学院大学

Institute of Information Security

後藤　厚宏

GOTO, Atsuhiro

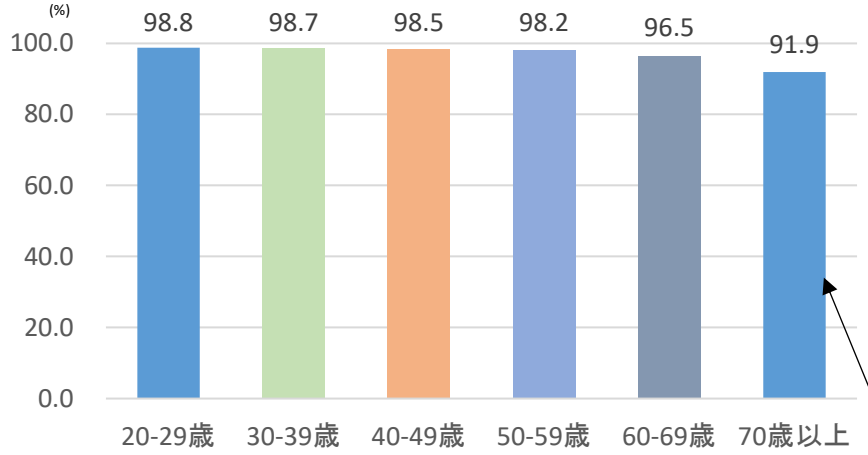
- 社会経済活動全体が情報通信（デジタル）に依存
- すべての国民の生活や仕事に広がるサイバー攻撃リスク
- 国内外での深刻なサイバー事案と脅威の増大

サイバー空間の環境変化とリスク

サイバー空間の「公共空間化」が一層進展
⇒社会経済活動全体が情報通信（デジタル）に依存

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

年齢別スマートフォン保有率

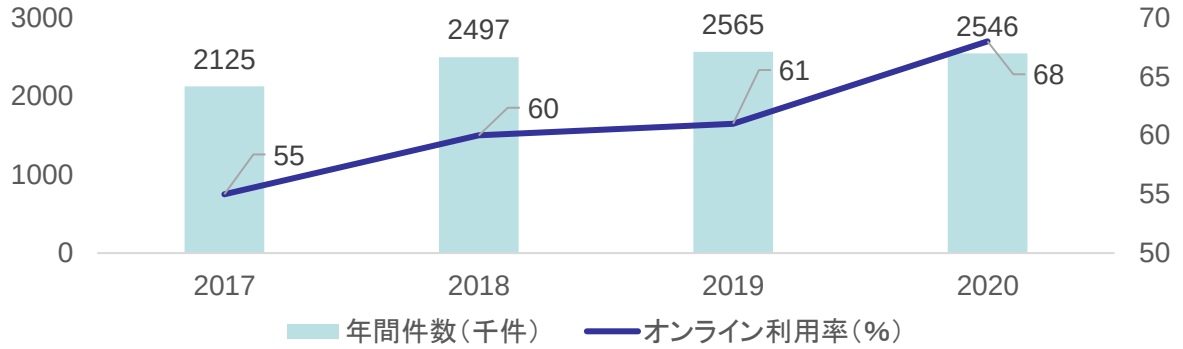


出典：NTTドコモ　モバイル社会研究所 「2024年調査」

オンライン行政手続件数と利用率

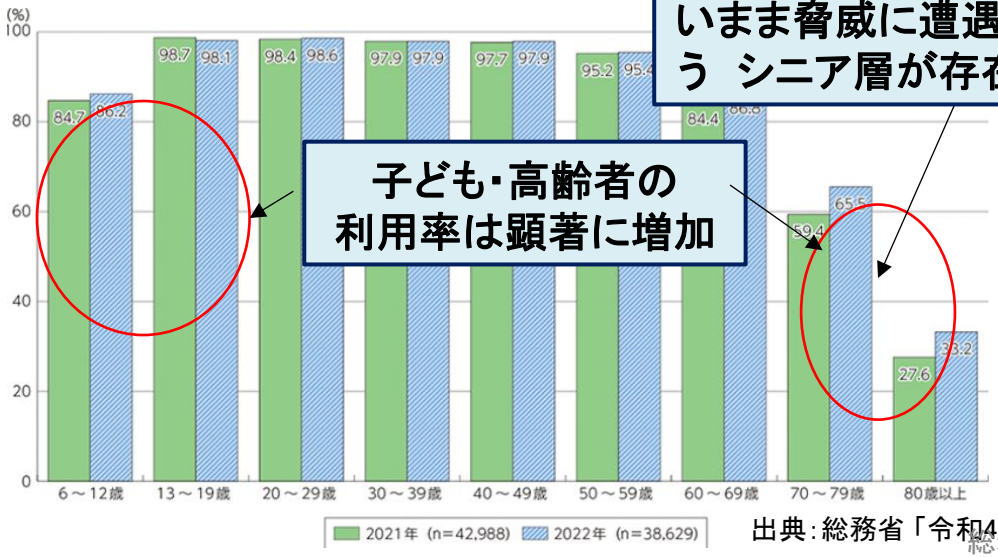
※2025年までに約2万2千の行政手続のオンライン化98%超を目標
（2021年6月 政府規制改革推進会議）

オンライン利用率は着実に増加



出典：内閣官房IT総合戦略室・総務省「行政手続等の棚卸結果等の概要」

年齢別インターネット利用率



出典：総務省「令和4年通信利用動向調査」

サイバー空間利用の自覚のないまま脅威に遭遇し、被害に遭う　シニア層が存在する可能性

子ども・高齢者の利用率は顕著に増加

勤務先のテレワーク実施率

5類移行で一段落 制度としては定着か

リスクの拡大：すべての国民の生活や仕事に広がる

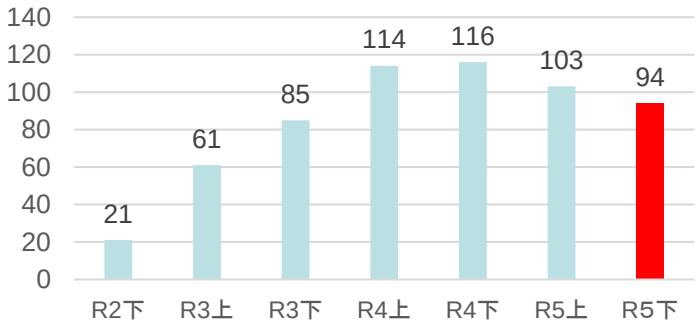
フィッシング詐欺

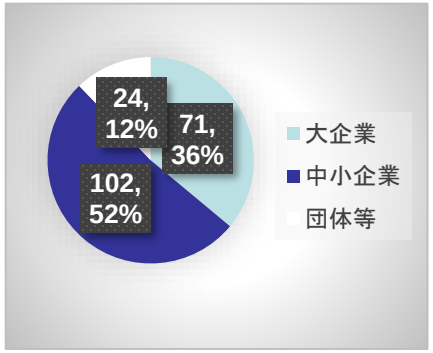
報告・出現サイト数ともに2年前から倍増

（データ出所）フィッシング対策協議会月次報告書「2024年3月 フィッシング報告状況」

ランサムウェア被害の報告件数・被害組織の規模別報告状況

企業・団体等におけるランサムウェア被害は高止まり
中小企業・組織からの被害報告が過半数

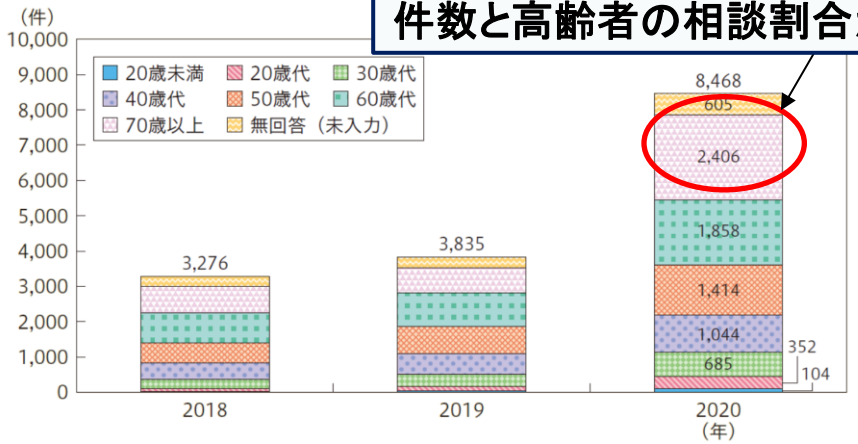




出典：「令和5年におけるサイバー空間をめぐる脅威の情勢等について」(警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

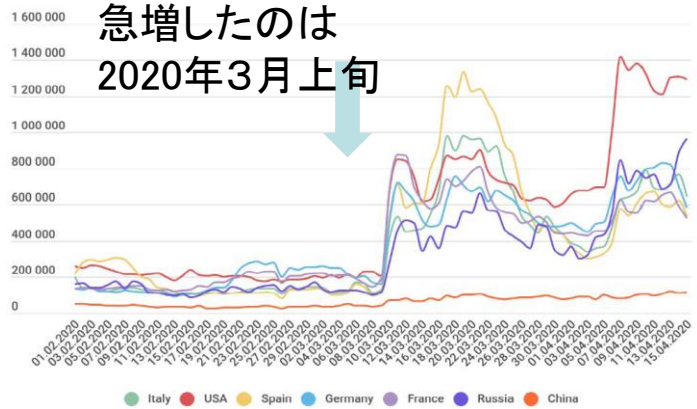
「不在通知の偽SMS」に関する消費生活相談件数

件数と高齢者の相談割合が顕著に増加



出典：「令和3年版 消費者白書」(消費者庁)
https://www.caa.go.jp/policies/policy/consumer_research/white_paper/assets/2021_whitepaper_all.pdf

リモートデスクトップを狙った攻撃件数の推移



管理者・利用者の目の届きづらい攻撃が増加

[出典]Kaspersky「Remote spring: the rise of RDP bruteforce attacks(2020/4/29)」
https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/

世界における主な「大規模」サイバー攻撃等

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

海外のみならず、近年我が国でも深刻なサイバー事案が発生

2019年3月　ノルウェーの世界最大のアルミ製造大手のNorsk Hydroに対するランサムウエア攻撃、復旧に数か月を要し、70億円以上

2022年1月～　ウクライナの政府機関、金融機関等に対し、Web サイトの改ざんやDDoS攻撃、破壊型マルウエアなどによるサイバー攻撃が相次ぎ発生

2020年12月　SolarWinds製品の正規のアップデートを通じた、米国の政府機関や大手IT企業に対するサイバー攻撃

2021年2月　米国フロリダ州オールズマー市水道局に対するサイバー攻撃、使用する薬剤の濃度を一時人体に影響を与える値に変更される

2021年5月　米国の食肉加工事業者JBS USAに対するランサムウエア攻撃、12億円相当の身代金支払い、10以上の工場が操業停止

2021年5月　米国石油パイプライン企業　米国東海岸の45%の燃料輸送を担うコロニアルパイプラインに対するランサムウエア攻撃、5日間の操業停止を引き起こし、5億円相当の身代金支払い

2023年9月　米国のホテル・カジノ運営大手Caesars and MGMに対するランサムウエア攻撃、復旧に15億円、合計の損害額は150億円

2018年～　日本の複数の医療機関に対するランサムウエア攻撃、一部の病院では、事象発生から約5ヶ月後、暗号化されたデータを復元

2022年3月　自動車部品製造企業がサイバー攻撃を受け、当該部品納入先であるメーカーの国内全工場が稼働停止

2022年9月　e-Govほか、一部の政府機関、団体、企業等のWebサイトが一時閲覧停止。ハッカー集団が犯行を暗示

2023年7月　港湾ターミナルシステムがサイバー攻撃を受け、貨物の積卸作業が2日半にわたり停止

2024年2月　スーパーマーケット運営企業がランサムウェア攻撃を受け、基幹システムが停止。有価証券報告書提出を2ヶ月延期。

2024年6月 動画配信サイトを運営する企業グループがランサムウェアを含む大規模なサイバー攻撃を受け、1ヶ月以上の配信停止に加え、関係組織の個人情報も漏洩

2022年5月 コスタリカ政府は、複数の政府機関がランサムウエアによる攻撃を受け、国家非常事態宣言を発出

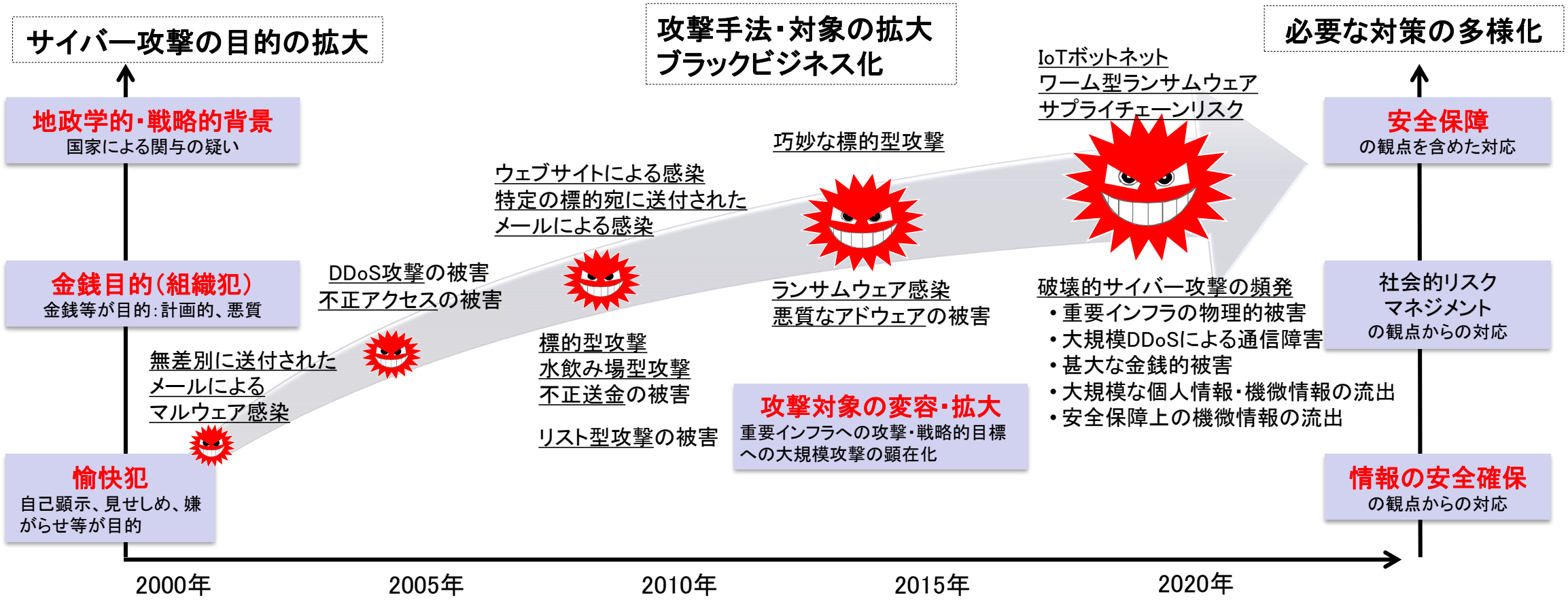
2020年8月　ニュージーランド証券取引所に対するDDoS攻撃、4日連続で取引停止

2020年11月　ブラジルの上級司法裁判所に対するランサムウエア攻撃、1週間の業務停止

2022年2月　米国の衛星通信企業 Viasatがサイバー攻撃を受け、欧州や中東地域で数時間の通信障害が発生、完全に回復するまでに数日を要し、ドイツの風力発電所が停止する等の影響

サイバーセキュリティ上の脅威の増大

✓ サイバー攻撃の目的の変化や攻撃手法・対象の拡大など、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。



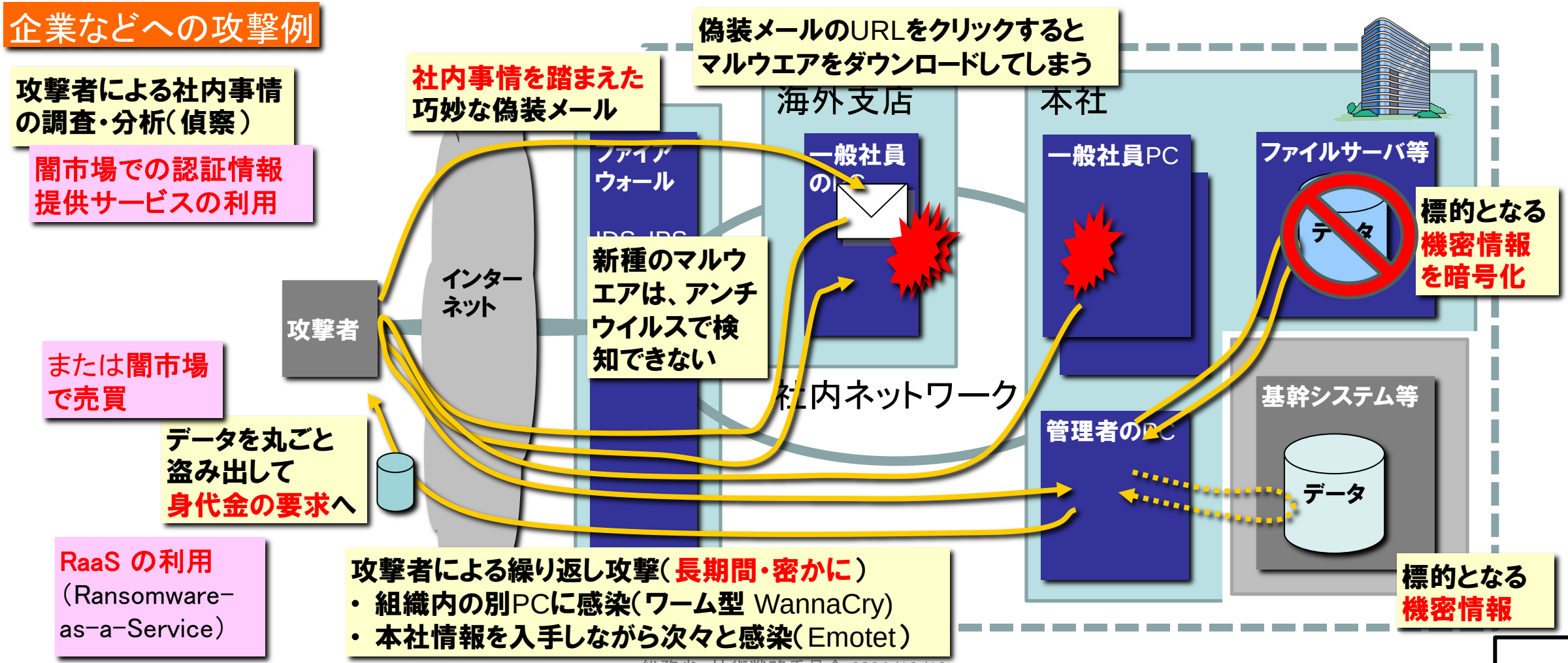
- 極めて高い技術力と裏ビジネス化
- 攻撃被害の広範かつ深刻な影響

深刻化・増大・加速するサイバーリスクに必要な取組み

高度な攻撃ツールの組合せによる執拗なランサムウェア攻撃

- ✓ 企業や政府機関を狙うサイバー攻撃は、攻撃対象に関する情報収集（偵察）、防御が弱い部署（海外支店やサプライチェーン）への攻撃から始まり、高度な攻撃ツールを組合せながら執拗に実行される。
- ✓ 利用される攻撃ツールや関連情報を闇市場を介して流通・売買される。

企業などへの攻撃例



極めて高い技術力と裏ビジネス化への対応が必要に

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

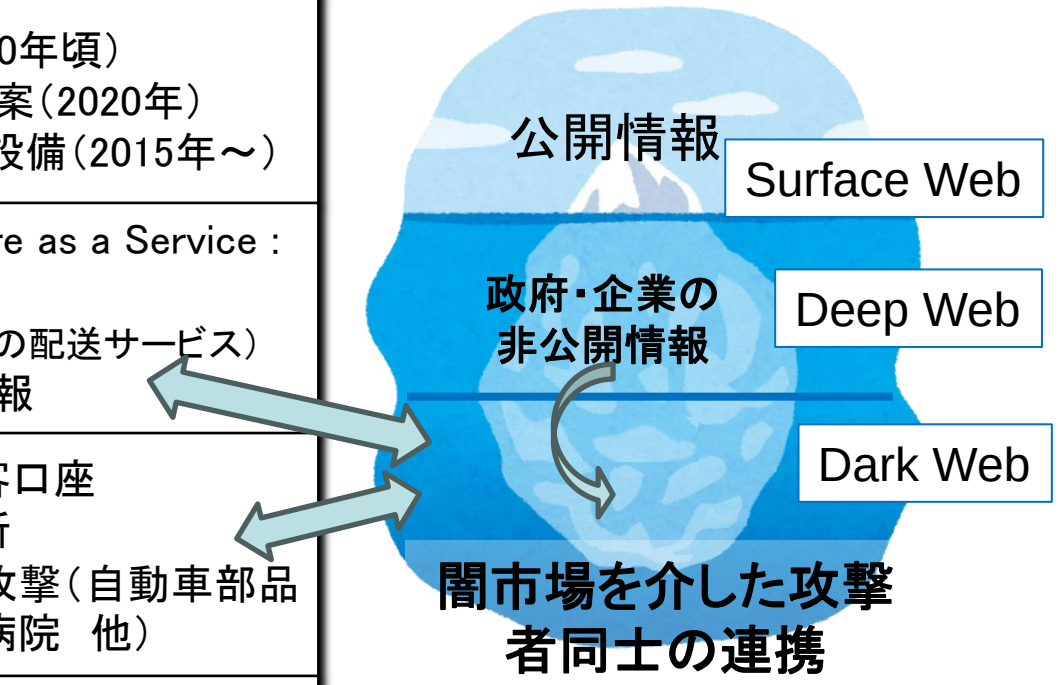
- ✓ 国家が背景にあり、「極めて高度な技術力と戦術」を有する者（A)が作るサイバー攻撃技術は、ツールやノウハウとして水面下で広がっている（**コモディティ化**）
- ✓ 技術力を活かして**攻撃ツールビジネス**を展開するもの（B)が現れ、そのツールやサービス（RaaS等）を利用し、主に金銭目的でのセイバー攻撃（C)が急増している
- ✓ 攻撃ツールや、攻撃対象に関する情報（ID、パスワード等）、ランサムウェア攻撃で盗み出したものが、Dark Webなどの「闇市場」で売買されている（人材リクルートも）。

	技術力	目　的	被害例
A	**極めて高度な技術力と戦術**	政治的・軍事的動機（State-Sponsored）	• イラン核施設（2010年頃） • 米国SolarWinds事案（2020年） • ウクライナの電力設備（2015年～）
B	**極めて高度な技術力**	攻撃ツールビジネス	• RaaS（Ransomware as a Service：LockBit 他） • Emotet（マルウェアの配送サービス） • ゼロDay脆弱性情報
C	**コスト効率**重視	金銭的価値	• 金融機関等の顧客口座 • 暗号通貨の取引所 • サプライチェーン攻撃（自動車部品メーカ、地域中核病院　他）
D	高度な技術	標的の評判にダメージ	• 政府機関WebへのDDoS攻撃 • 選挙妨害

コスト度外視

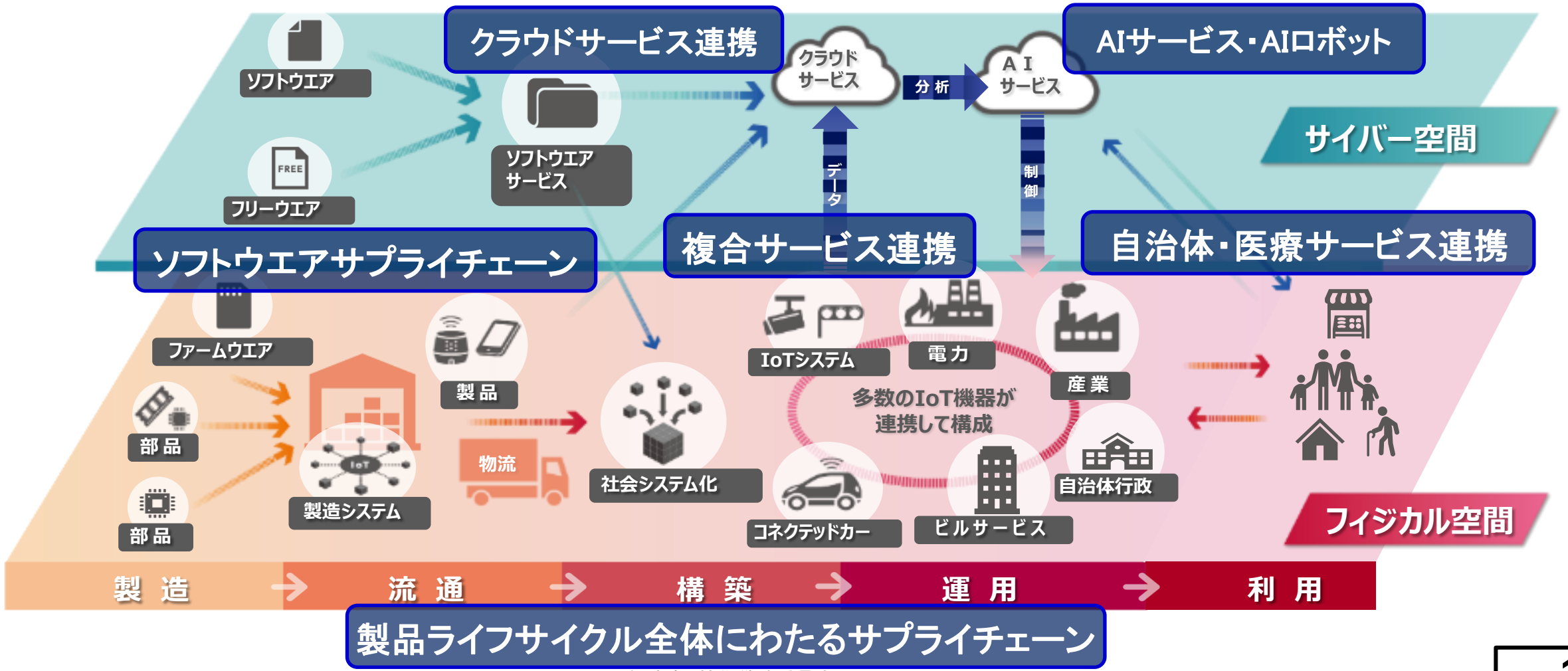
攻撃技術のコモディティ化

ビジネス化



サイバー空間とフィジカル空間に跨るネットワーク社会

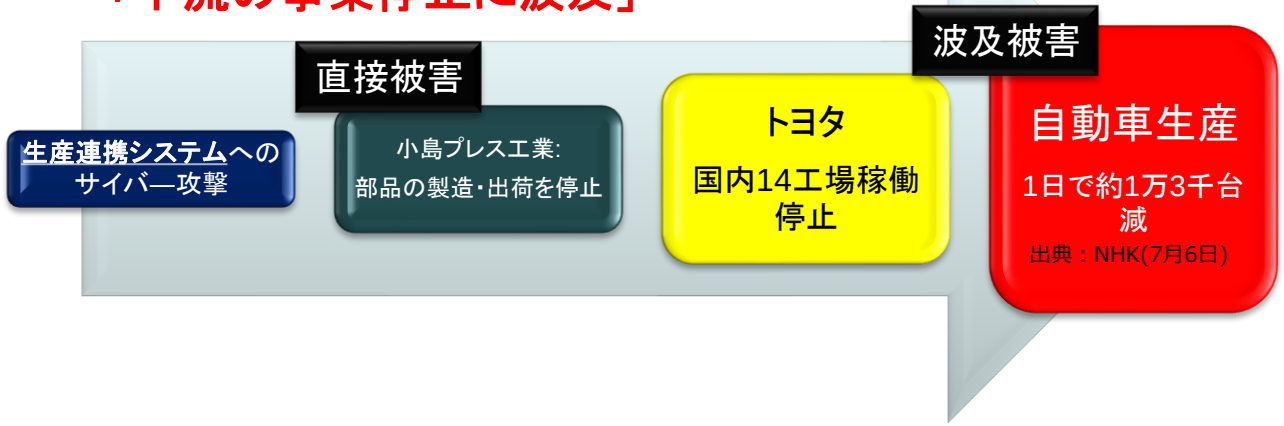
- ✓ 多様な製品やソフトウェアのサプライチェーン、自治体・医療サービスやクラウドサービスは、情報通信技術・サービスを介して、グローバルに連結し、社会全体に大きな価値を提供（社会全体がデジタルに依存）。
- ✓ 連結される個々の組織やサービスの事業継続の喪失は、広範かつ深刻な影響につながる。



攻撃被害の広範かつ深刻な影響への対応が必要に

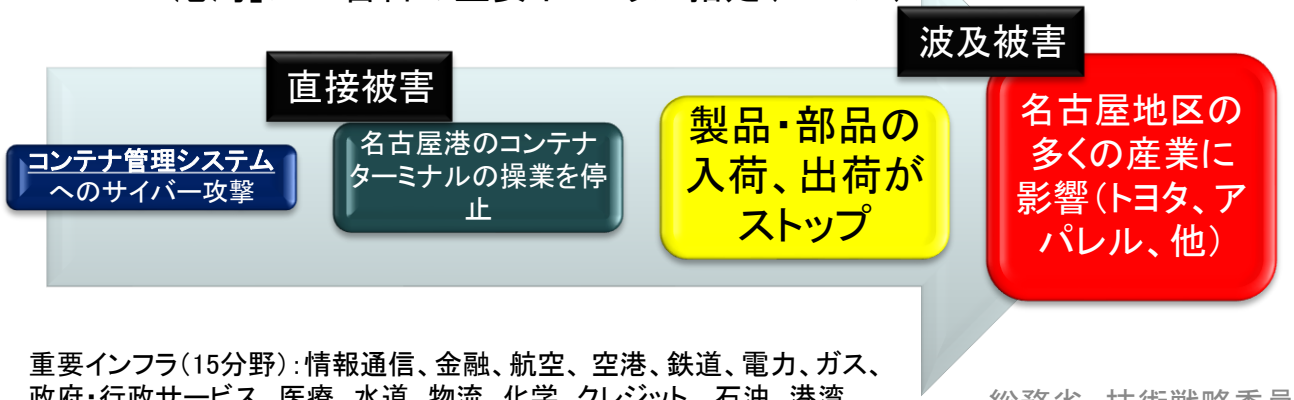
✓ 自動車産業のサプライチェーン（事案1）、港湾をハブとするコンテナ物流（事案2）、ソフトウェアのメンテナンス機構を介した多数のユーザ組織（事案3）など、広範かつ深刻な影響（被害）を及ぼした国内外の事案

■ 事案1：サイバー攻撃被害が自動車のサプライチェーン「下流の事業停止に波及」



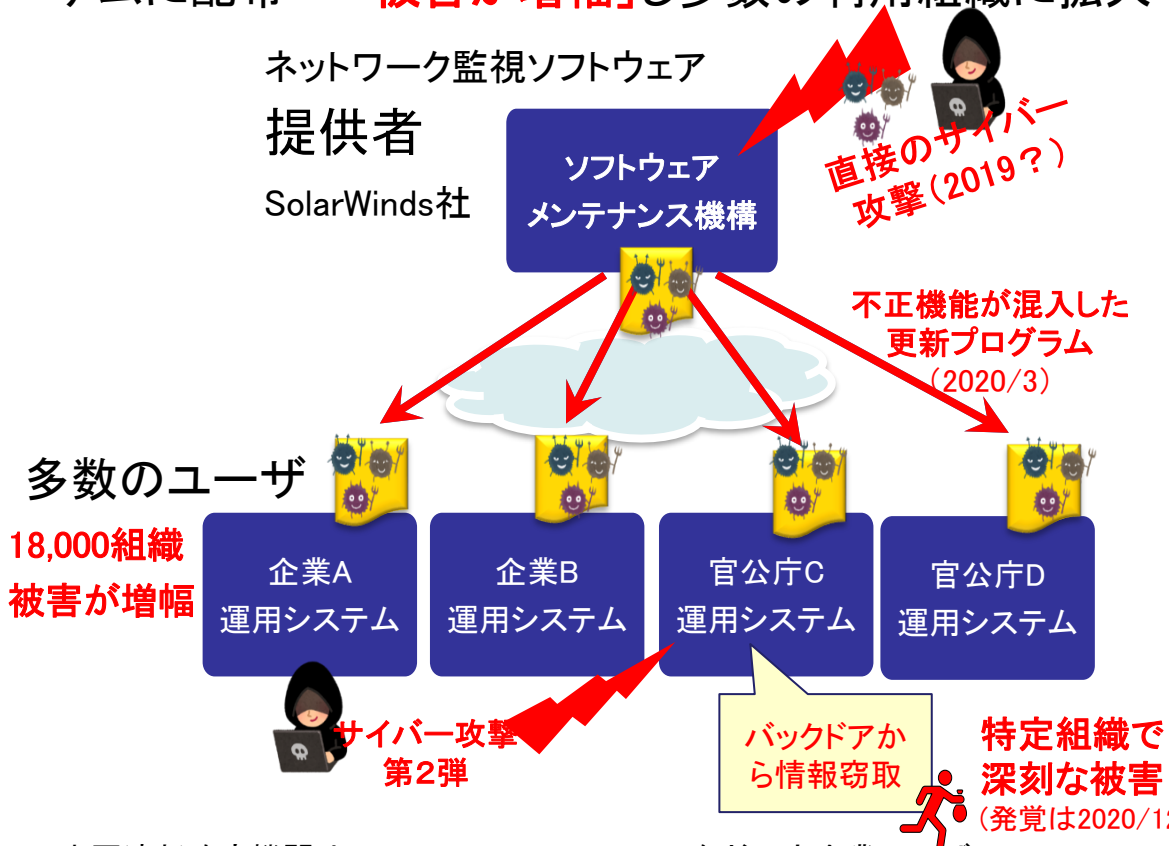
■ 事案2： コンテナ物流停止が「地域の経済活動に影響」

⇒「港湾」が15番目の重要インフラに指定（2024/4）



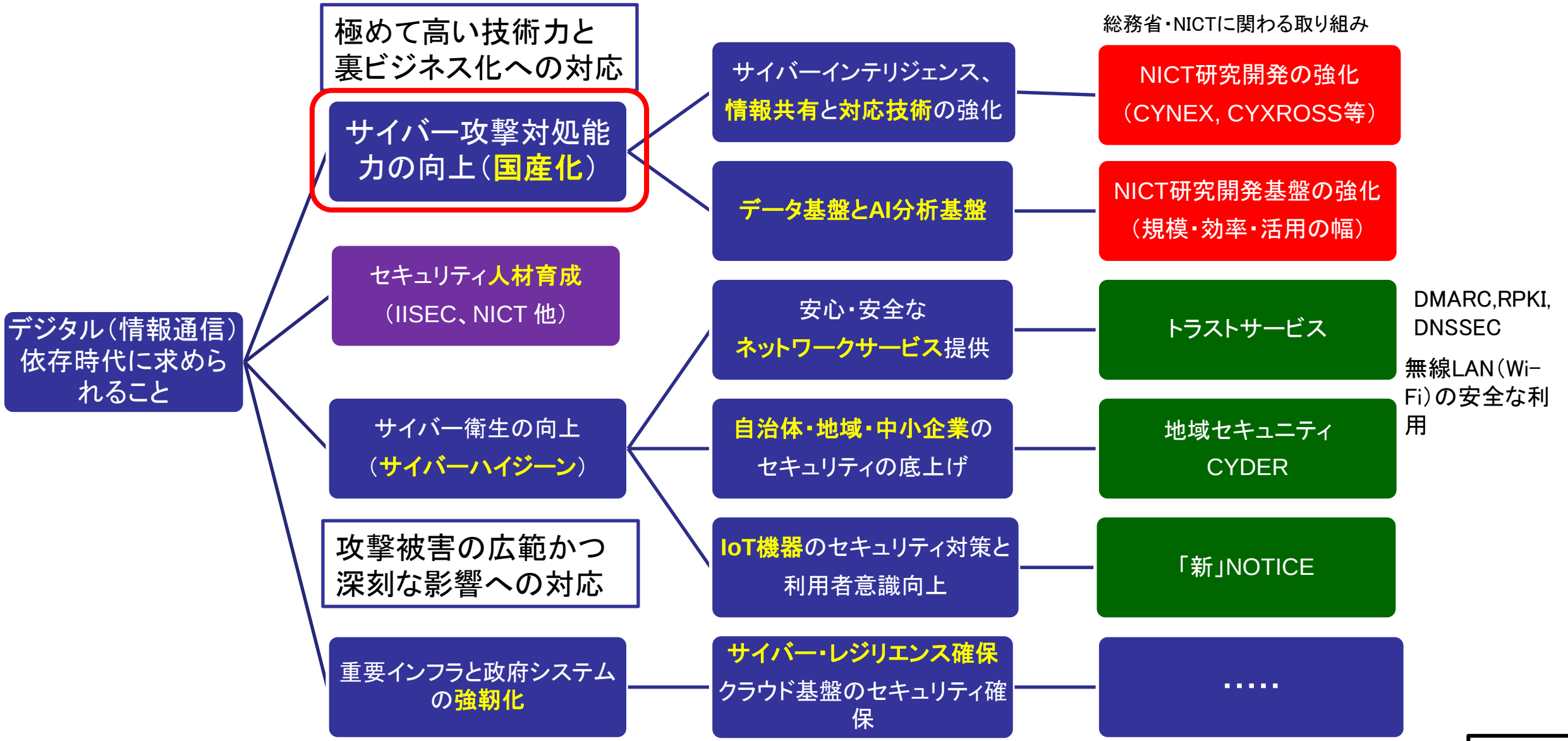
重要インフラ（15分野）：情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油、港湾

■ 事案3：ベンダのソフトウェア保守機構が攻撃され、不正機能が混入した更新プログラムが多数の利用者システムに配布⇒「被害が増幅」し多数の利用組織に拡大



米国連邦政府機関やMicrosoft, Cisco, FireEyeなどの大企業ユーザに被害が及ぶ⇒バイデン大統領のEO14028（2021/5）

深刻化・増大・加速するサイバーリスクに必要な取組み



サイバー攻撃対処能力の向上（国産化）の必要性

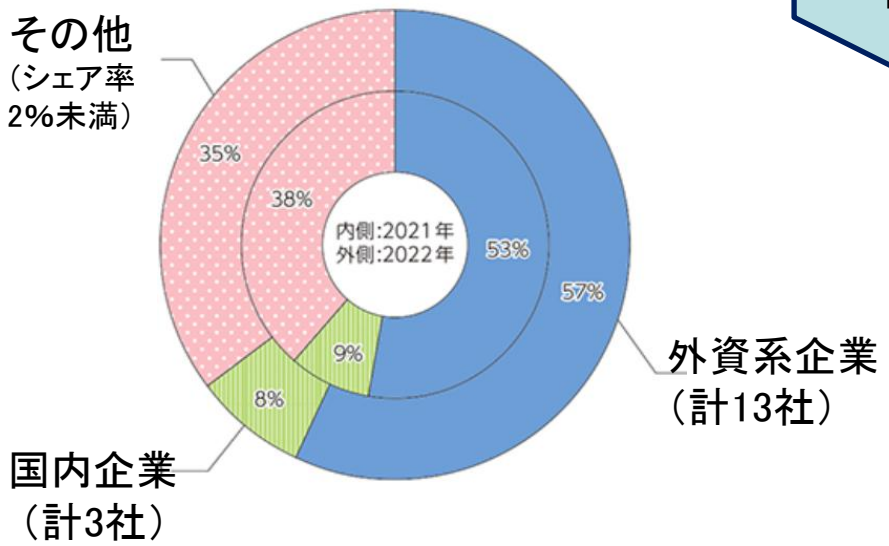
サイバー攻撃対処能力の向上（国産化）の必要性：現状

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

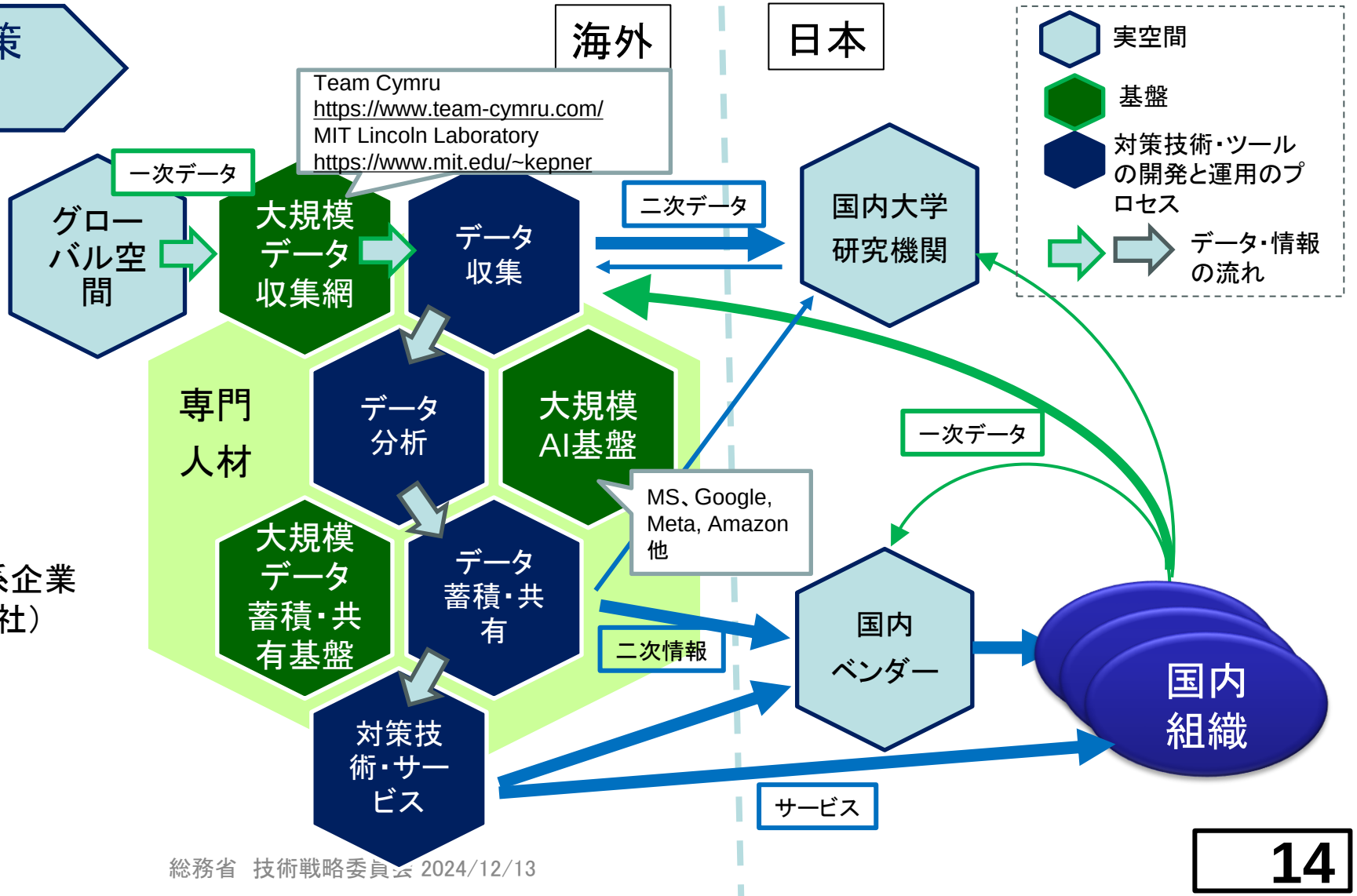
✓ 我が国のサイバーセキュリティ製品・サービスは海外依存度が高い。技術・サービス開発の源泉となる「一次データ（マルウエア、脆弱性、管理ログ等）」の収集・分析も海外依存度が高く、国内ユーザ組織のシステム監視データも海外ベンダー等に提供される割合が多いと推察。

サイバーセキュリティ対策 現状は海外依存

国内情報セキュリティ製品市場シェア（売上額）



令和6年版 情報通信白書



サイバー攻撃対処能力の向上（国産化）の必要性

✓ サイバーセキュリティ製品・サービスの国産化を進めるためには、一次データ（マルウエア、脆弱性、管理ログ等）を自ら収集・分析して対策技術・サービスを開発・運用するプロセスを実現するとともに、それらを支える基盤を国内で構築する必要あり。

対処能力向上のために国産化が必要な技術例

サイバー空間の情報を収集・調査する状況把握力

- マルウェア（特にランサムウェア）の特徴・暗号化機能の分析技術
- 攻撃主体の狙いや攻撃手段に関する情報の獲得・分析技術
- 高度かつ未知の攻撃の早期発見技術

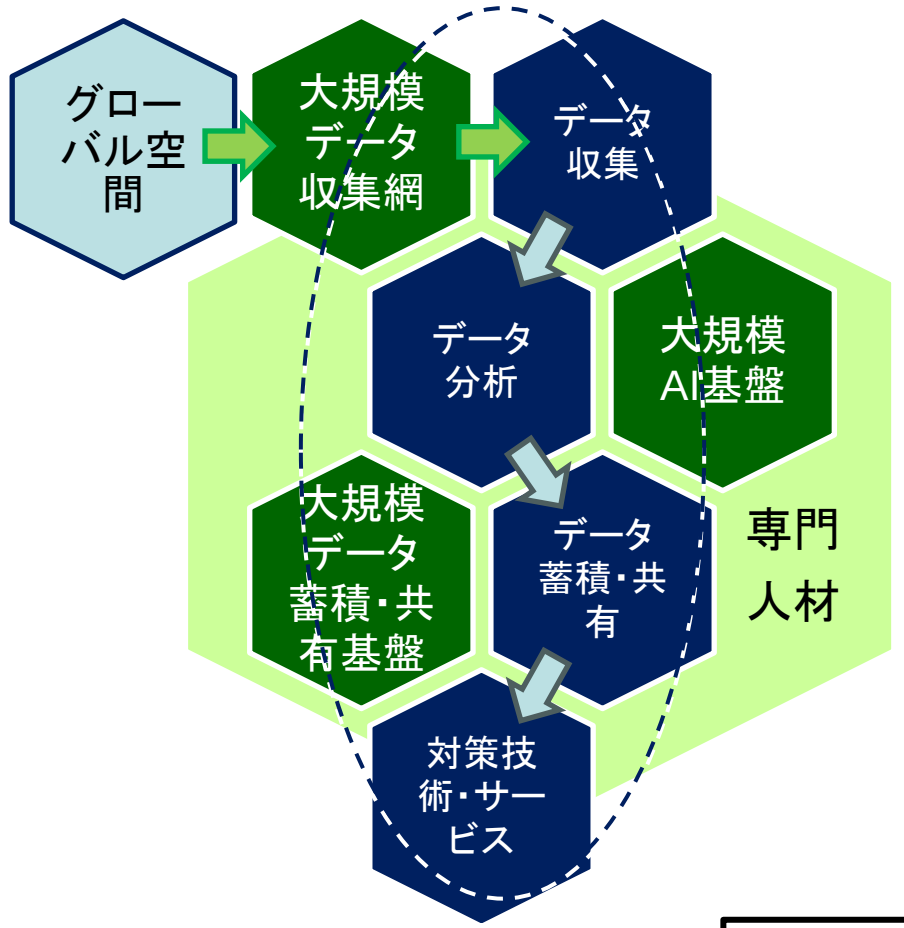
サイバー攻撃から機器やシステムを守る防御力

- 機器やシステムの脆弱性探査技術
- 同　防御能力の評価（ペネトレーションテスト含む）・向上技術

機器やシステム・社会の強靭化

- 耐量子計算機暗号技術と社会システム全体の移行技術
- 耐タンパー性向上技術
- 組織と人材の強化

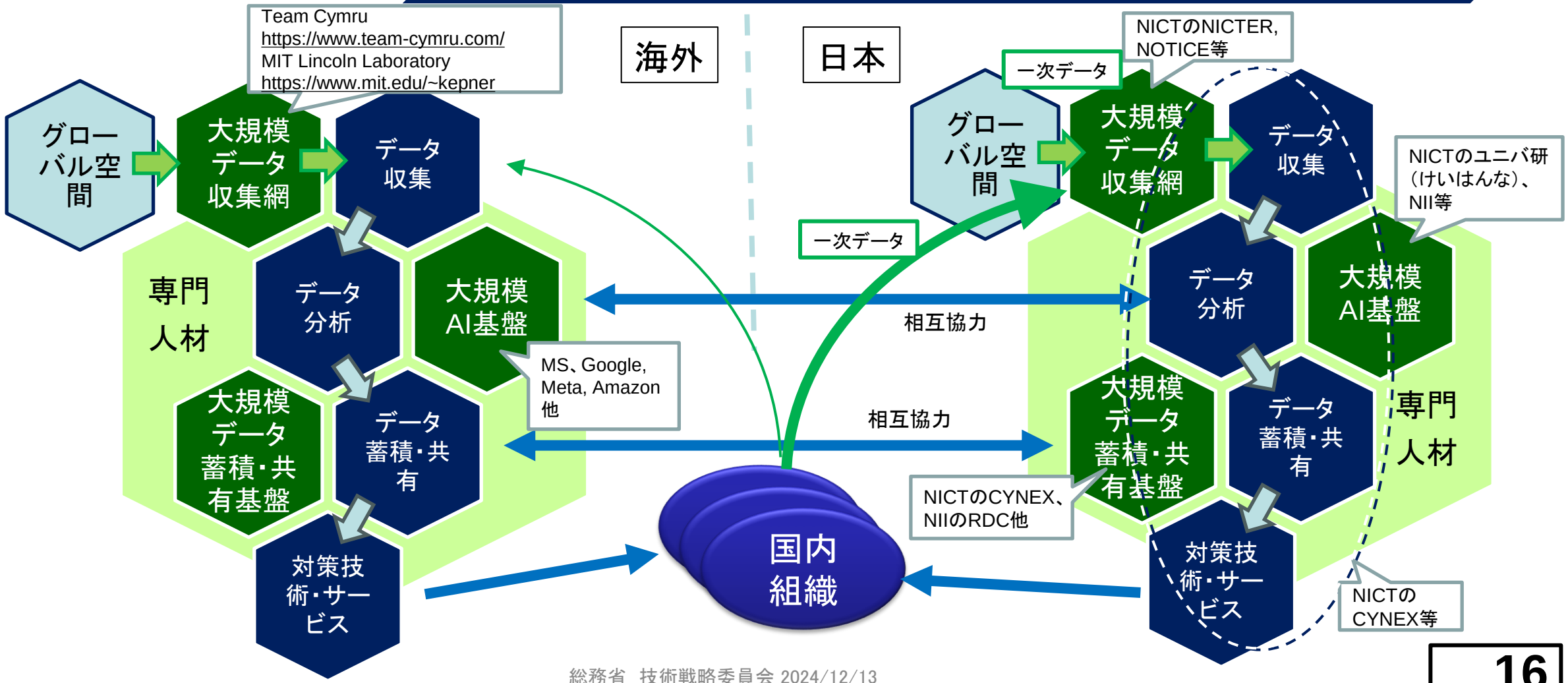
国内で主体的に実施



サイバー攻撃対処能力の向上（国産化）の必要性：目標像

サイバーセキュリティ対策
現状は海外依存

国産化と能力向上：“一次データ”を収集・分析・蓄積により国産技術開発
大規模AI基盤・蓄積・共有基盤と専門人材育成で能力向上



NICTに期待すること

NICTに期待すること

- サイバーセキュリティ製品・サービスやサイバーセキュリティの一次データ・情報は**海外依存（輸入超過）**。我が国の安心・安全を支えるサイバーセキュリティ確保に向けて、その技術・製品・サービスの**国産化**を進めること、および、それを可能とする**一次データの収集、分析・蓄積・共有の基盤強化**による研究開発と実運用が重要。
  - サイバーセキュリティの研究開発を長年実施してきたNICTは一次データ収集能力を強化し、それをベースとする我が国の技術開発において、CYNEXを通して中核的な役割を果たすべき。
- IoTボットネット等による**DDoS攻撃対策**のさらなる強化
  - ICT-ISAC他と連携して進めているNOTICEおよびC&Cサーバの検知・対処では、IoTボットネットの全体像の可視化・対策を推進するために、NICTが端末側・ネットワーク側双方の情報を収集・分析するハブ機能の更なる強化が必要（参照「ICTサイバーセキュリティ政策の中期重点方針」）
- **AI for Security**による情報収集・分析の高度化
  - 収集した大量の一次データの分析には、大規模AI基盤による分析の高度化が必須であり、我が国の関連研究機関のハブとして、専門人材の育成を含め、NICTがリーダーシップを発揮することが必要。
- 暗号技術は、社会生活から経済活動まで、すべての社会システムの安全を支える基礎・基盤技術であるため、新たな暗号の研究開発に取り組む人材・チームを**長期的・継続的に維持**することが**我が国の安全保障**として重要
  - 暗号研究には高度な専門的知見が必要であるため、NICTが主体となって我が国の長期的な人材確保に取り組むべき。
  - 全社会システムにおいて、混乱なく次世代暗号（PQC等）への移行が可能となるように、幅広い暗号応用分野への指導的な役割を期待。