デジタル活用の拡大と
大規模サイバーセキュリティ災害への“備え”

情報セキュリティ大学院大学

サイバーセキュリティ戦略本部員

内閣府 SIP プログラムディレクタ（PD）

後藤　厚宏

プロフィール　後藤　厚宏

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

- 1984年東京大学大学院にて情報工学の博士課程修了（工学博士）。
  NTT研究所にて先進ICT技術の研究開発等に従事。
  - 第5世代コンピュータPJ（1985～1990）、米国シリコンバレー拠点（1994～1996）
- 2011年7月より情報セキュリティ大学院大学教授。2017年4月より学長
- 2015年11月より内閣府SIPプログラムディレクター
  - SIP第1期：重要インフラ等のサイバーセキュリティ確保（2015～2019）
  - SIP第2期：IoT社会に対応したサイバー・フィジカル・セキュリティ(2018～2022）
- 2019年2月よりサイバーセキュリティ戦略本部員を併任。

概要

社会全体のデジタル基盤依存が高まる時代において、サイバー攻撃を契機とする被害連鎖が関連産業に拡大する大規模リスクへの対応が求められる。

デジタル改革（DX）の恩恵を享受するために、どのような“備え”が必要であるかについて考える。

東京大会2020の振り返り

海外メディアからの「賛辞」

2021年8月17日 Security Magazine　Dr. Brian Gan
https://www.securitymagazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story

“The Tokyo Olympics are a cybersecurity success story”

・・・ the Tokyo Olympics have been a real success story from a cybersecurity perspective ・・・

Over the course of these games, it’s become increasingly clear that the organizers did indeed exercise preventative measures and that despite the challenges and limitations of holding an Olympics during a pandemic, the Tokyo Olympics have been a real success story from a cybersecurity perspective. Organizers of all large-scale, televised sporting events—and indeed just all organizations in general—should look to this year’s games as a model to emulate.

The **Best Kind of Defense**, having **the Right People in Place**, and **Going on the Offensive**
「最高な防御手段」　「適切な人を適切な場に配置」　「攻め＝先回りの対策」

東京大会2020の振り返り

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

■この夏、COVID-19感染拡大に伴う社会・産業面での制約下で開催されたオリンピック・パラリンピック東京大会2020では、大きなサイバーセキュリティ事案は報道されていません。

■大会を支えてきた関係組織や重要インフラ事業者によるサイバーセキュリティ対策とその真摯な運用努力の賜物

■最悪の事態をも想定し、準備を重ねることによって、大規模イベントを乗り越えられた

■このレガシーを将来社会に活かす取組みの一つとして・・・

本日のアジェンダ

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

- サイバー攻撃脅威があらゆる社会・経済活動に潜む
- 「大規模被害」懸念があるサイバー攻撃の類型
- 新たなサイバーセキュリティ戦略
- デジタル依存時代の“備え”

サイバー攻撃脅威があらゆる社会経済活動に潜む

CPS（サイバーフィジカルシステム）のセキュリティリスク

- ◆世界のサイバー犯罪による経済損失は6,000億米ドル/2018
  （世界GDP 0.8%相当 ⇒日本で**約3兆円**）
- ◆IoT社会では、サイバー攻撃がフィジカル空間まで到達し、**経済損失が拡大**するリスク
- ◆遠隔業務等でクラウド・モバイル機器活用の急増：**セキュリティ対策が急務！**

拡大する課題への取組みが活発に

米国：大統領令 EO14028 2021/5/12
“Improving the Nation’s Cybersecurity”

欧州：EuropolによるEmotet拠点のテイクダウン。IoT機器のセキュリティ要件の議論が活発

日本：新サイバーセキュリティ戦略（9/28 閣議決定）
経産省：CPSF、総務省：ICT総合対策2021
警察庁：サイバー局

CONNECTED（繋がり）と大規模被害リスク

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

CPS：サイバーフィジカルシステムの繋がり

- IoTデバイス、フォグコンピューティング、クラウドとインターネット

テクノロジーのサプライチェーン：開発・生産・運用のつながり

- ハードウェア、ソフトウェア、クラウドサービス、通信サービス

企業活動・社会活動のサプライチェーン：人の繋がり

- 受委託サービス契約、業務プロセス、雇用

産業・社会の連鎖：社会の繋がり

- グローバル社会、グローバル経済としての連鎖

グローバルサプライチェーンがサイバー攻撃対象に

サプライチェーンのセキュリティ課題

調達側から提供される営業秘密の漏えい（窃取）
⇒ サプライチェーン全体でのセキュリティ対策強化
（米 防衛調達 DFARS）

サプライヤー側から調達元への部品・製品の提供時における不正部品・不正機能の混入
⇒ 製造から流通までをカバーする混入検知・防御

サプライチェーン全体での企業責任・トラスト
⇒ SDGs, ESG, 企業不正対処、ルール形成対応
説明責任とトラスト

課題の深刻化

ソフトウェア
サプライチェーン攻撃

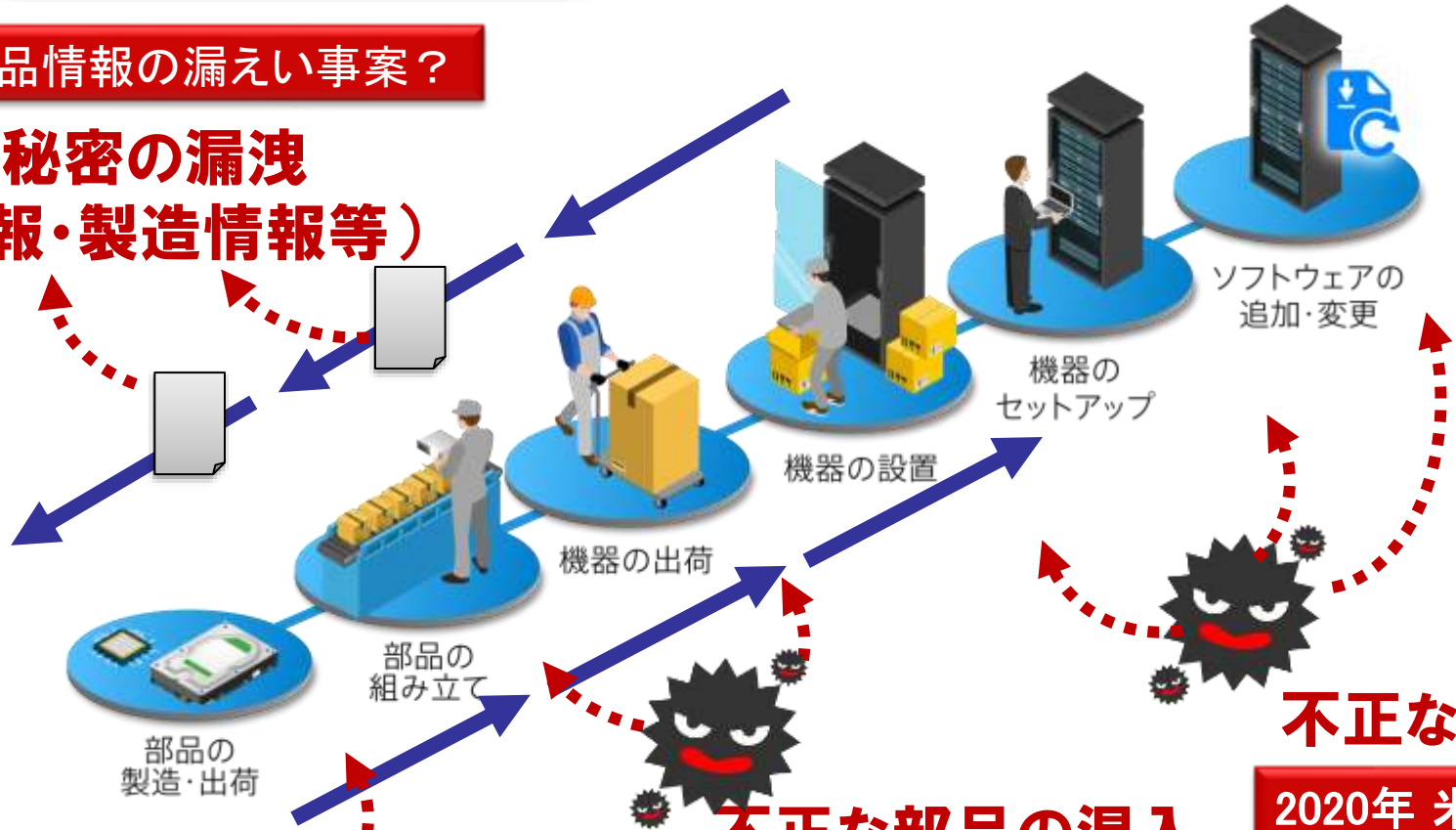
ソフトウェアの正規の更新プロセスに便乗して、（多数の）運用中のシステムにマルウェアを配信する攻撃

「セキュリティ維持の枠組み」そのものの危機！

サプライチェーン：サイバー攻撃リスク

2019年 防衛装備品情報の漏えい事案？

営業秘密の漏洩
（設計情報・製造情報等）



不正なハード
ウェアの挿入

不正な部品の混入

2016年、米国セキュリティ会社が携帯電話のフラッシュメモリのファームウェアに仕込まれている不正プログラムを発見。

不正なソフトウェアの混入

2020年 米国でのSolarWinds社の事案
ソフトウェアアップデートがサプライチェーン攻撃によって改ざん

重要情報（CUI）のセキュリティ確保が調達要件に

CUI　Controlled Unclassified Information 管理された 非格付け情報

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

DFARS

(Defense Federal Acquisition Regulation Supplement
米国国防総省取得規則補足)

◆防衛調達の全参加企業にセキュリティ対策（SP800-171の遵守）を義務化（DFARS）

◆他の産業へ波及？
⇒全米自動車産業協会（AIAG）

NIST SP800-171のセキュリティ要件ファミリ

要件ファミリー	要件数	要件ファミリー	要件数
アクセス制御	22	メディア保護	9
監査と責任追跡性	9	要員のセキュリティ	2
意識向上と訓練	3	物理的保護	6
構成管理	9	リスクアセスメント	3
システムと通信の保護	16	セキュリティアセスメント	4
インシデント対応	3	識別と認証	11
メンテナンス	6	システムと情報の完全性	7

https://www.ipa.go.jp/files/000057365.pdf

DoDは更なる強化に向けて Cybersecurity Maturity Model Certification (CMMC)を開発中

事案：SolarWinds社のソフトウェア更新機能改ざん

- SolarWindsが提供するネットワーク監視ソフトウェア「Orion Platform」を用いる米国連邦政府機関（財務省・国務省・国家核安全保障局など）やMicrosoft, Cisco, FireEyeなどの大企業（全体で18,000組織）が大規模なサイバー攻撃の被害を受けた可能性
- 同社が2020年3月と6月に配布した**アップデートが改ざん**された?

ソフトウェアサプライチェーン攻撃はセキュリティ維持の枠組みの危機！

- 攻撃は 2020年3月から9月まで？
- 国家の関与？

「史上最大かつ最も巧妙」＝マイクロソフト社長

遠隔更新機構の再点検と本格的なSBoM活用の是非

SBoM: Software Bill of Materials（ソフトの部品表）

社会インフラ・産業インフラのセキュリティ課題

金銭目的のサイバー攻撃

- 情報窃取を狙いとするサイバー攻撃 ⇒ 銀行口座からの不正引出し
- 暗号通貨の窃取（サイバー空間上での金融犯罪）

サービス（事業継続）妨害のサイバー攻撃

- サイバー空間でのサービス停止（妨害）を狙う攻撃（DDoS等）
- 重要インフラへの攻撃（ウクライナ停電）

社会インフラへのランサムウェア攻撃

社会・産業活動（**事業継続性**）へのサイバー攻撃

＋

金銭目的サイバー攻撃（**ランサムウェア**）

社会インフラ・主要産業へのランサムウェア攻撃

2021年5月8日 日経新聞
「米最大の石油パイプライン停止」

米石油パイプライン最大手のコロニアル・パイプラインは7日、サイバー攻撃を受けて全ての**業務を停止**

https://www.nikkei.com/article/DGXZQOGN084D30Y1A500C2000000/

2021年5月14日 日経新聞
「サイバー攻撃　身代金5億円　米パイプライン会社が支払い」

https://www.nikkei.com/article/DGKKZO71878100U1A510C2MM0000/

2021年6月3日 日経新聞
「サイバー攻撃、生活産業に 食肉世界最大手で**供給の懸念** 消費者へ被害、標的に」

https://www.nikkei.com/article/DGKKZO72530410S1A600C2TB1000/

2022年2月28日　日経新聞
「トヨタ、**国内全工場を停止**へ　部品会社にサイバー攻撃」

トヨタ自動車は28日、3月1日に国内全工場（14工場28ライン）の稼働を停止すると発表した。トヨタ車の部品をつくるサプライヤーがサイバー攻撃を受け、部品供給を管理するトヨタのシステムが影響を受けたため。

https://www.nikkei.com/article/DGXZQOFD289MK0Y2A220C2000000/

社会インフラ・主要産業へのランサムウェア攻撃

社会・産業活動（事業継続）妨害を狙うサイバー攻撃
⇒被害範囲の拡大、大規模化

- サイバー犯罪はデータ窃取から企業や政府機関のコアオペレーションの妨害攻撃へ

  CNBC： The Biden administration is urging corporate executives and business leaders to take immediate steps to prepare for ransomware attacks, warning in a new memo that cybercriminals are shifting from stealing data to disrupting core operations.

「大規模被害」懸念があるサイバー攻撃の類型

「大規模被害」懸念があるサイバー攻撃の類型

社会経済のグローバルな**つながり**による攻撃被害の大規模化

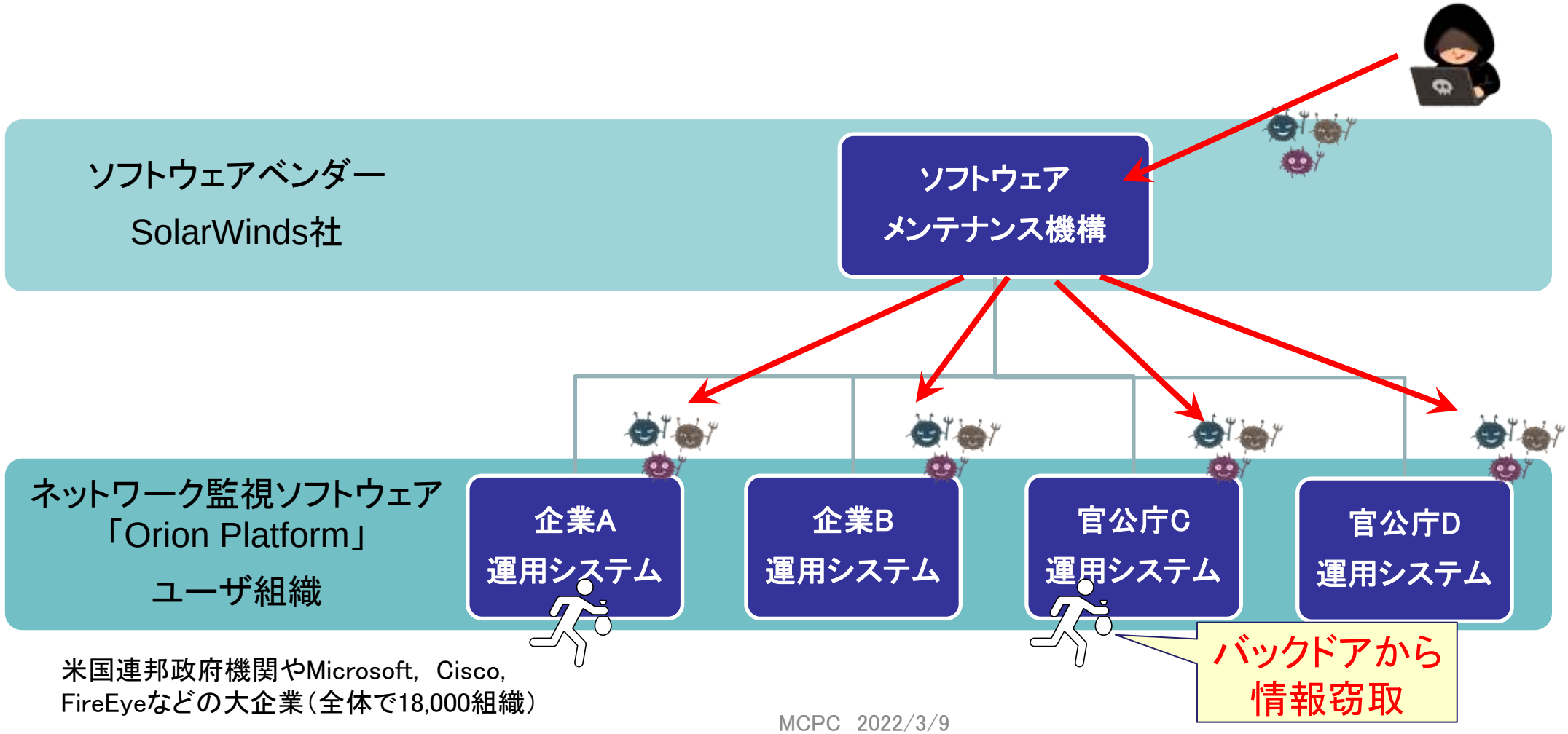
類型Ⅰ ソフトウェアサプライチェーン攻撃による攻撃被害が大規模化 — ソフトウェアサプライチェーン攻撃

類型Ⅱ サイバー攻撃によるサプライチェーン寸断（事業継続停止）がもたらす被害の連鎖 — 事業継続攻撃

類型Ⅲ 脆弱性が内在するIoTの大量かつ急速な普及による攻撃被害の大規模化 — 大量IoTへの攻撃

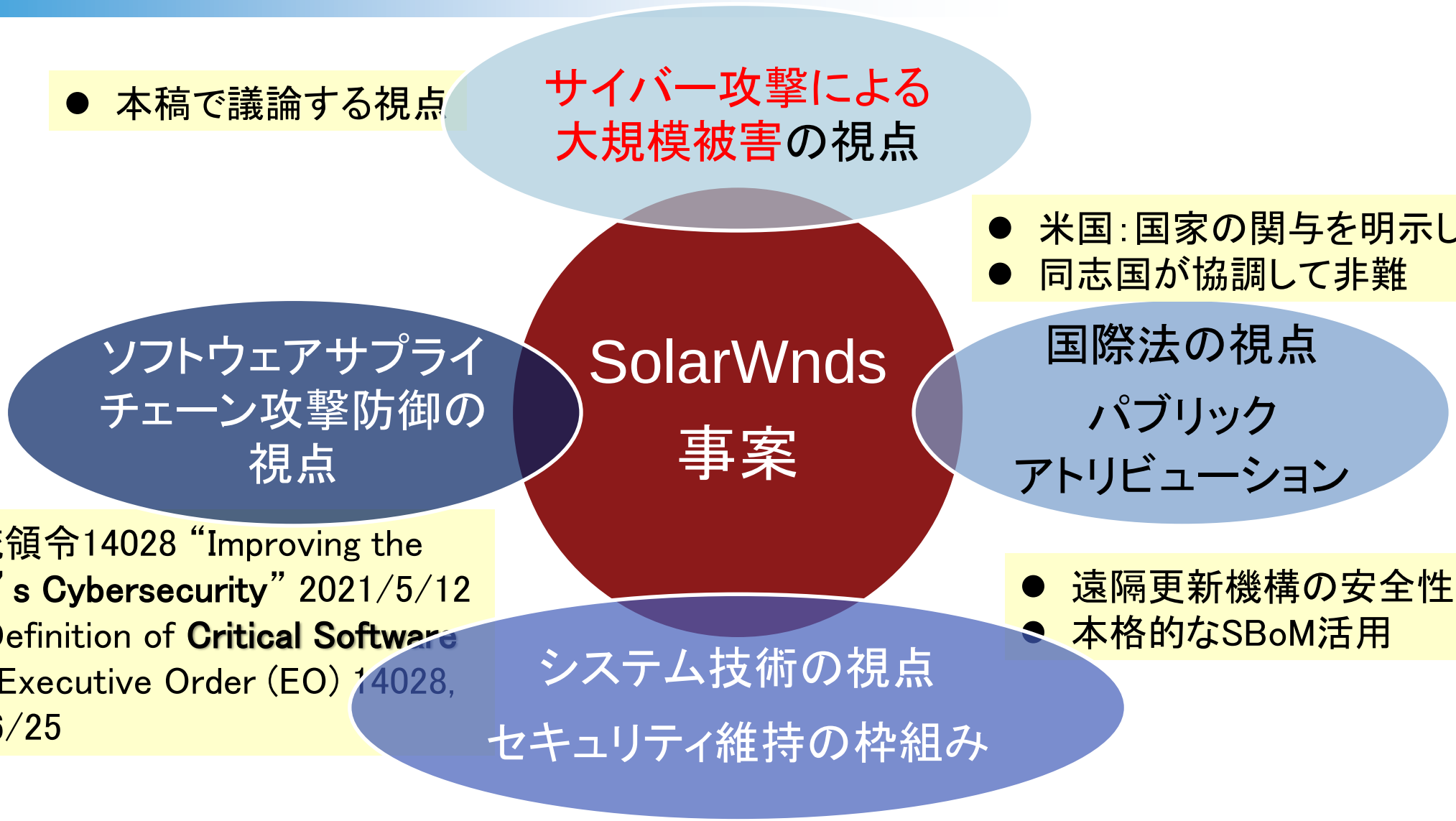
類型Ⅰ：ソフトウェアサプライチェーン被害の連鎖

■ SolarWinds事案：ソフトウェアの更新機構が攻撃され、更新機構により多数のシステムに悪性機能が埋め込まれた（「ソフトウェアサプライチェーン攻撃」）



米国連邦政府機関やMicrosoft，Cisco，FireEyeなどの大企業（全体で18,000組織）

SolarWinds事案を巡る4つの視点



- 本稿で議論する視点

- 米国：国家の関与を明示して非難
- 同志国が協調して非難

- 米大統領令14028 “Improving the **Nation’s Cybersecurity**” 2021/5/12
- NIST Definition of **Critical Software** Under Executive Order (EO) 14028, 2021/6/25

- 遠隔更新機構の安全性強化策
- 本格的なSBoM活用

類型Ⅱ：サプライチェーン寸断（事業継続停止）がもたらす被害の連鎖

■ 小島プレス工業事案：サイバー攻撃で停止によるトヨタの自動車生産事業の停止（国内産業全体への負のインパクト）

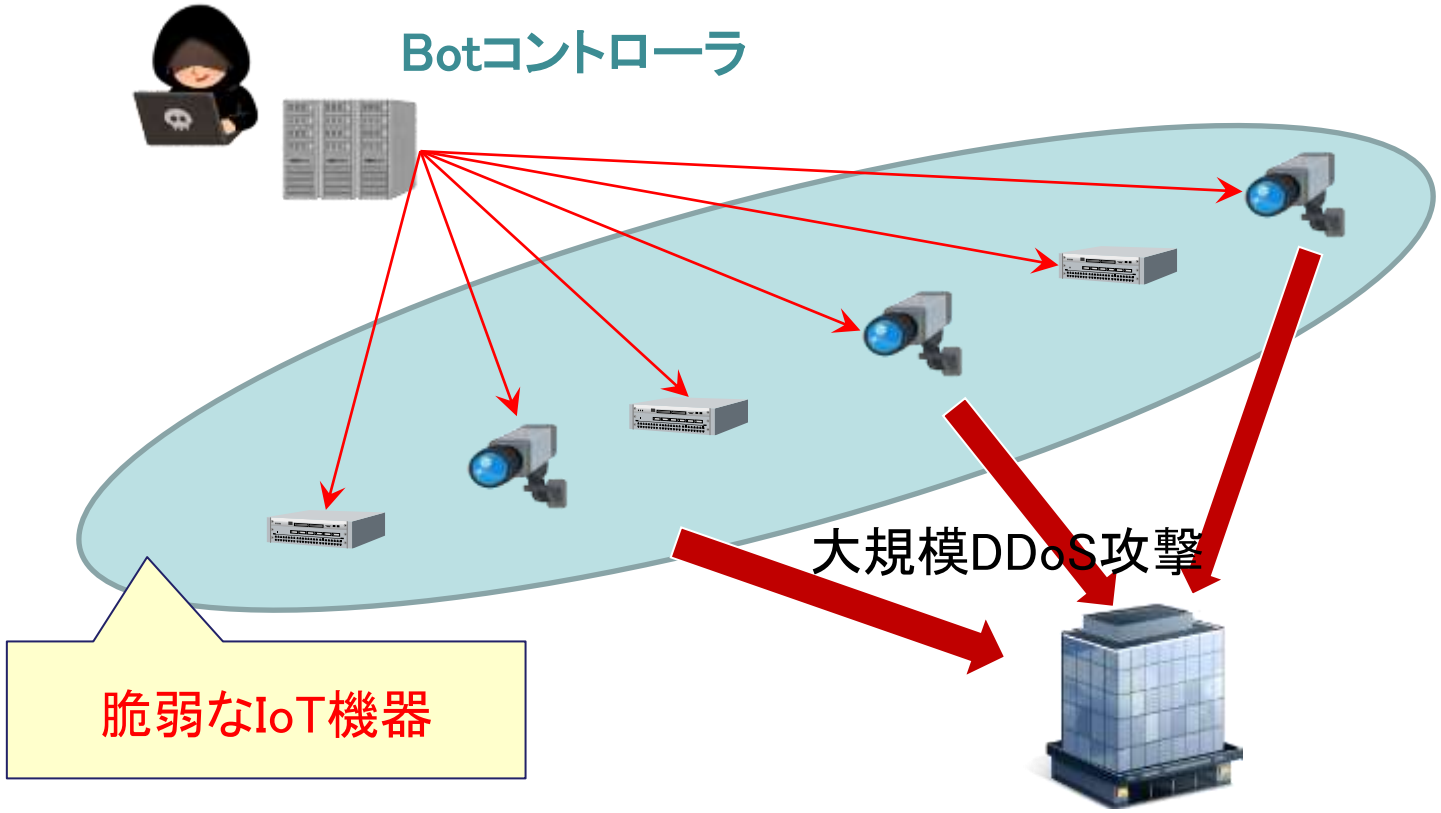
攻撃者 ランサムウェア攻撃 → 小島プレス工業: 生産連携のシステム障害 → トヨタ 国内14工場稼働停止 → 自動車生産 1日で約1万3千台減

■ Colonial社の石油パイプライン事案：重要インフラがサイバー攻撃で停止による社会経済全体への負のインパクト

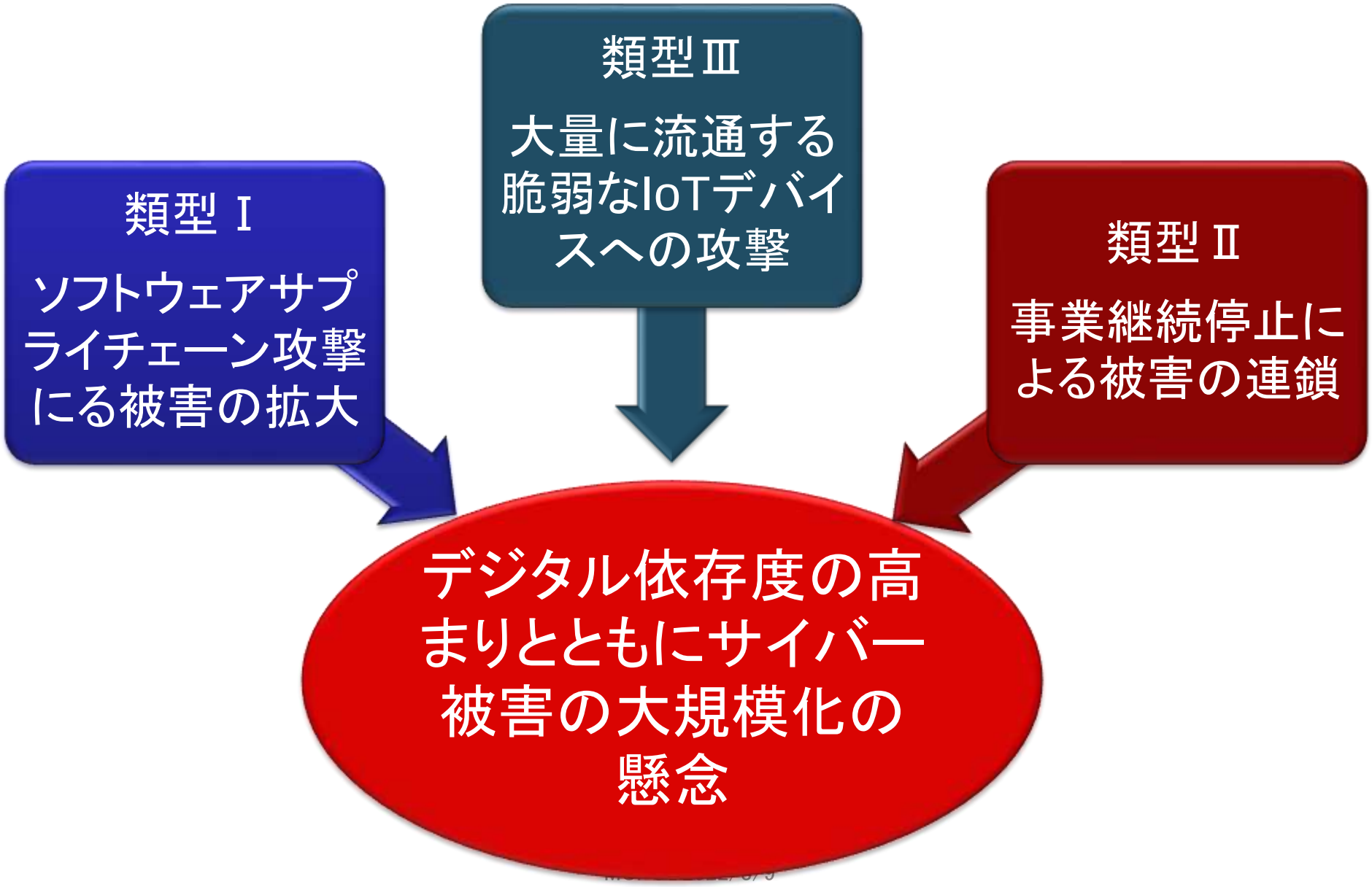
攻撃者 ランサムウェア攻撃 → Colonial社: 安全のためパイプライン停止 → 米国東海岸 石油供給不足 → NewYork ガソリン価格上昇

類型Ⅲ：IoT機器の大量流通と CPSネットワーキングによる被害の大規模化（広域化）

■ Miraiの事案：　脆弱性のあるIoT機器（ノラIoT）が大規模DDoS攻撃の踏み台



デジタル依存時代の「備え」の議論が必要な時代に



クラウド停止がもたらす大規模被害予測

■ 英Lloyd's of London（ロイズ社）の調査レポート

"Cloud Down – Impacts on the US economy"（2018年）

https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2018/cloud-down/aircyberlloydspublic2018final.pdf

- 米国のクラウドサービス（=現代のインフラ）事業者上位3社が3日から6日間オフラインになった場合の全損害額は69億（7,500億円）から147億ドル（1兆6,000億円）との予測

◆製造業：42～86億ドル
◆小売・卸売業：14～36億ドル
◆ 財務・保険：　～4億4700万ドル
◆ 運送・倉庫：　～4億3900万ドル
◆ 情報：　～8億4700万ドル

■ 最近のICTインフラ障害の事例

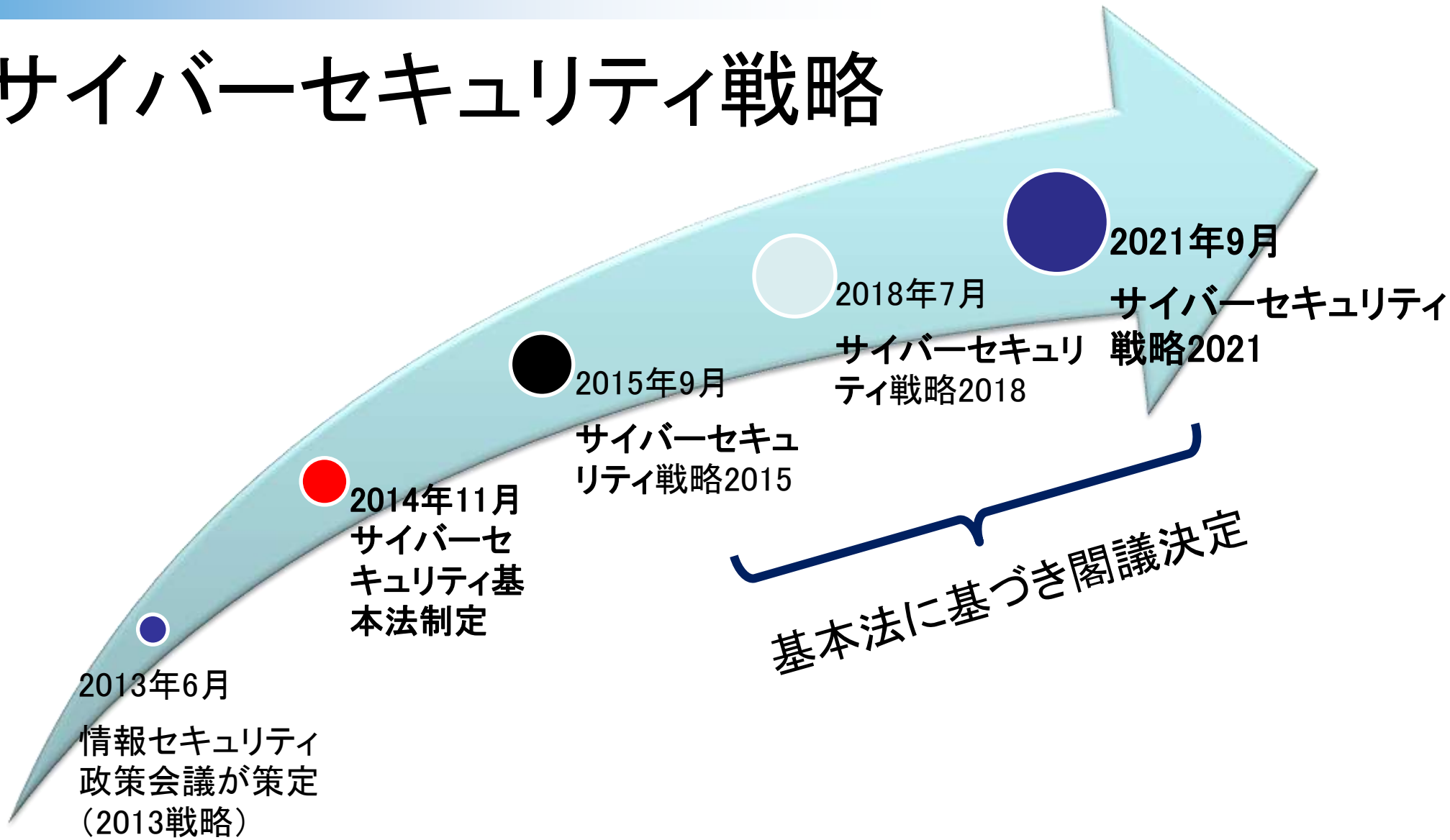
- コンテンツ配信ネットワークCDN "ファストリーFastly"のサービスに障害が発
- AWSの障害（9/2）：金融系、気象庁、空港システムに波及

デジタル依存時代の「備え」

■ 今後、政府から産業界から市民生活まで社会全体のデジタル化が急伸することは明らか　⇒**デジタル依存の急速な高まり**（具体的には、インターネット、クラウド、IoT、・・・）

デジタル依存時代の大規模リスクへの「備え」の議論が必要に

新たなサイバーセキュリティ戦略



次期サイバーセキュリティ戦略の課題と方向性

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験
テレワーク、オンライン教育等の進展
- 厳しさを増す
安全保障環境
- **SDGｓ**への
デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**
に向けて行ってきた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映
国家間競争の場に
安全保障上の課題にも
- 不適切な利用は
国家分断、人権の阻害へ
- 官民の取組の
活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

「次期サイバーセキュリティ戦略」の構成

中長期的

1　2020年代を迎えた日本をとりまく時代認識

1－1　デジタル経済の浸透・デジタル改革の推進、SDGsへの貢献に対する期待、安全保障環境の変化、新型コロナウイルスの影響・経験、東京大会に向けた取組の活用

2　本戦略における基本的な理念

2－1　確保すべきサイバー空間は「自由、公正かつ安全な空間」

2－2　基本原則は従来の戦略で掲げた５つの原則を堅持（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3　サイバー空間をとりまく課題認識

環境変化からみたリスク、国際情勢からみたリスク、近年のサイバー空間における脅威の動向

戦略期間

4　目的達成のための施策

＜3つの方向性＞（１）デジタル改革を踏まえたデジタルトランスフォーメーション とサイバーセキュリティの同時推進
（２）公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
（３）安全保障の観点からの取組強化

経済社会の活力の向上及び持続的発展

1．経営層の意識改革

2．地域・中小企業におけるDX with Cybersecurity の推進

3．新たな価値創出を支えるサプライチェーン等の信頼性確保に向けた基盤づくり

4．誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

国民が安全で安心して暮らせるデジタル社会の実現

1．国民・社会を守るためのサイバーセキュリティ環境の提供

2．デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

3・4・5．経済社会基盤を支える各主体における取組
①(政府機関等)
②(重要インフラ)
③(大学・教育研究機関等)

6．多様な主体によるシームレスな情報共有・連携と東京大会に向けた取組から得られた知見等の活用

7．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

1．「自由、公正かつ安全なサイバー空間」の確保

2．我が国の防御力・抑止力・状況把握力の強化

3．国際協力・連携

横断的施策

研究開発の推進　人材の確保・育成・活躍促進　全員参加による協働・普及啓発

5　推進体制

「自由、公正かつ安全なサイバー空間」を確保するための政府一体となった推進体制

「Cybersecurity for All」を踏まえた対応の強化

サイバー空間の課題認識

- あらゆる主体が参画する**公共空間化**
- **サイバー・フィジカルの相互連関・連鎖の深化**
- **サイバー攻撃の複雑化・巧妙化**
- **安全保障上の脅威の増大**

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

個人		組織	
DXに向き合う**地方、中小企業、若年層、高齢者等**	目に見えないリスクと向き合う**個人・組織**	サイバー攻撃による**重要インフラ**停止、知財の窃取、金銭被害等の増大	**国家の関与**が疑われる攻撃

DXとサイバーセキュリティの同時推進

○デジタル改革と一体で：経営層の意識改革、地域・中小企業の取組促進
（経営インセンティブ、安価かつ効果的な支援サービス・保険の普及）

○誰も取り残さないリテラシーの向上と定着
（高齢者向けデジタル活用支援講習会との連携、GIGAスクール構想にあわせた普及啓発、サイバー防犯ボランティア）

安全保障の観点からの取組強化

○中露北からの脅威等を踏まえた外交・安全保障上のサイバー分野の優先度向上

○防衛省・自衛隊におけるサイバー防衛能力の抜本的強化

○「妨げる能力」、外交的手段や刑事訴追等を含めた対応、日米同盟の維持・強化

○国際協力・連携

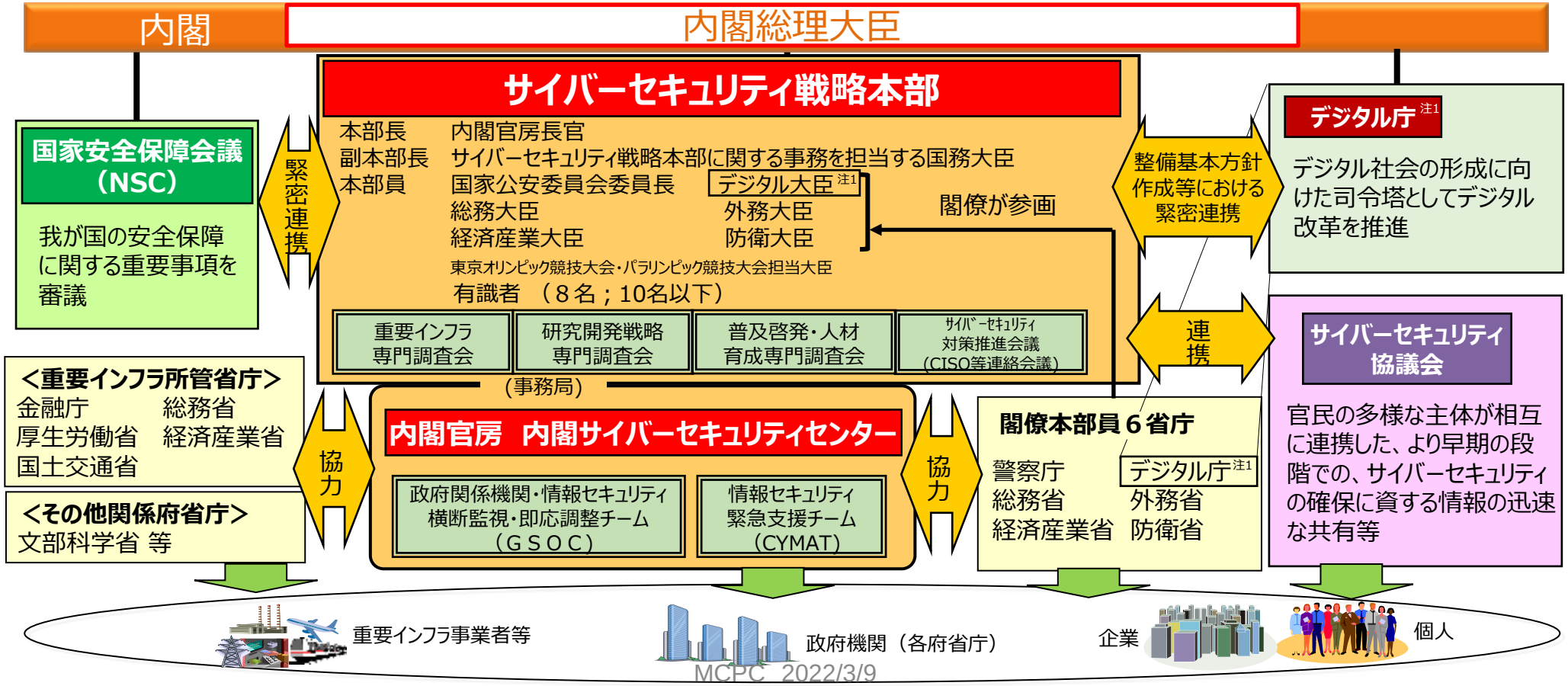
公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

○国民・社会を守るためのサイバーセキュリティ環境の提供
（産業横断的なサプライチェーン管理、サイバー犯罪対策、クラウドサービス利用のための対策の多層的な展開、経済安全保障の視点を含むサイバー空間の信頼性確保）

○深刻なサイバー攻撃から国民生活・経済を守る包括的なサイバー防御等の展開
（情報収集から対処調整、政策措置までの一体的推進の総合調整を担うナショナルサートの機能強化、政府機関・重要インフラ等の各主体のセキュリティ対策）

推進体制

- 我が国のサイバーセキュリティ政策により、自由、公正かつ安全なサイバー空間を確保するためには、政府一体となった推進体制が必要。デジタル庁が司令塔として推進するデジタル改革に寄与するとともに、公的機関が限られたリソースを活用しその役割を果たせるよう、関係機関の一層の対応能力強化・連携強化を図る。
- 各主体に期待される具体的な対策につながるよう、また、国際協調の重要性を認識し、攻撃者に対する抑止の効果や各国政府に対する我が国の立場への理解を訴求するよう、NISCと関係府省庁が連携して、本戦略を国内外の関係者に積極的に発信。
- 本部は、サイバー攻撃等に対して国全体として網羅的な対処が可能となるよう、ナショナルサート（CSIRT/CERT）の枠組み整備を行う。
- 年次報告・年次計画は、一体的に検討を行い、前年度の取組実績、評価及び次年度の取組を、戦略の事項に沿って、一連の流れを示すように整理。



（注1）デジタル社会形成基本法（令和３年法律第35号）、デジタル庁設置法（令和３年法律第36号）。（令和３年９月１日施行）

急速な「デジタル化」＝「デジタル依存度」の急増

デジタル依存時代の「備え」

デジタル依存時代の大規模リスクへの「備え」

■ 今後、政府から産業界から市民生活まで社会全体のデジタル化が急伸することは明らか　⇒**デジタル依存の急速な高まり**（具体的には、インターネット、クラウド、IoT、・・・）

デジタル依存時代の大規模リスクへの「備え」の議論が必要に

■ 戦略4.2節の「国全体のリスクの低減とレジリエンスの向上」の具体的な活動として

国全体を俯瞰したリスク分析と被害シミュレーション

に基づく

サイバー技術、デジタルサービス、データ流通の取組み

国全体を俯瞰した被害シミュレーション

	自然災害のハザードマップ	サイバー攻撃被害のハザードマップ?
	南海トラフ巨大地震	大規模サイバー攻撃
直接被害	資産等への被害（被災地） 97.6兆円～169.5兆円	直接の被害は？
波及被害	経済活動への影響（全国） 30.2兆円～44.7兆円	二次被害・三次被害は？

北米最大の石油パイプラインを創業するコロニアル社のランサム被害

米国東海岸への二次被害（NYでのガソリン不足と値上がり）

内閣府 「南海トラフ巨大地震の被害想定（第二次報告）のポイント ～施設等の被害及び経済的な被害～」
http://www.bousai.go.jp/jishin/nankai/taisaku_wg/pdf/20130318_kisha.pdf

被害想定を意識したレジリエンス策

技術、サービス、データにおける「備え」

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

データ流通「断」への備え：DFFT対応の前提の元で

- データ共有における信頼できるプロヴァナンス確保（データ汚染対策）

デジタルサービス「断」への備え：クラウドダウンへの備え

- レジリエンス確保のためにクラウドサービス分散利用
- ITサービスを支える**デジタル時代のエッセンシャルワーカー**の継続確保

サイバー技術「断」への備え：「グローバル連携」の中で

- 国産技術として保持すべきサイバー技術は何か？
- 国家として強化・保有すべき**セキュリティ脅威インテリジェンス能力**

本日のまとめ

サイバー攻撃脅威があらゆる社会・経済活動に潜む

「大規模被害」懸念があるサイバー攻撃の類型

新たなサイバーセキュリティ戦略

デジタル依存時代の“備え”

ご質問・コメント・アドバイスをお願いします

情報セキュリティ大学院大学 https://www.iisec.ac.jp/

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

学長　後藤　厚宏

- ◆横浜市神奈川区鶴屋町2−14−1（横浜駅きた西口徒歩1分）
- ◆情報セキュリティ専門の大学院大学
  - 修士（情報学）・・・473名（2006年3月～2021年9月）
  - 博士（情報学）・・・46名（2007年8月～2021年9月）
- ◆約7割が社会人：平日昼間＋夜間＋土曜日
  - 企業や官公庁が求める情報セキュリティ人材
  - 将来のCIO(chief information officer)
- ◆密な企業連携、実社会のセキュリティ人脈
- ◆2021年秋から東京丸の内に東京オフィス開設

  東京都千代田区丸の内3丁目3−1

  新東京ビル（9F）946号室

社会人学生の所属組織（2020−2021実績）

IQVIA ジャパン／NRIセキュアテクノロジーズ（株）／NTTコムウェア（株）／NTTテクノクロス（株）／F5ネットワークスジャパン（同）／海上保安庁／外務省／（株）ウフル／（株）エヌ・ティ・ティ　エムイー／（株）協和エクシオ／（株）静岡銀行／（株）タツノ／（株）ディー・エヌ・エー／神奈川県警察／（株）ラック／キヤノンビズアテンダ（株）／金融庁／警察庁／警視庁／さくら情報システム（株）／日本コムシス（株）／日本電気（株）／日本放送協会／農林中央金庫／東日本旅客鉄道（株）／富士フイルムビジネスイノベーション（株）／防衛省／法務省／横浜市役所　など

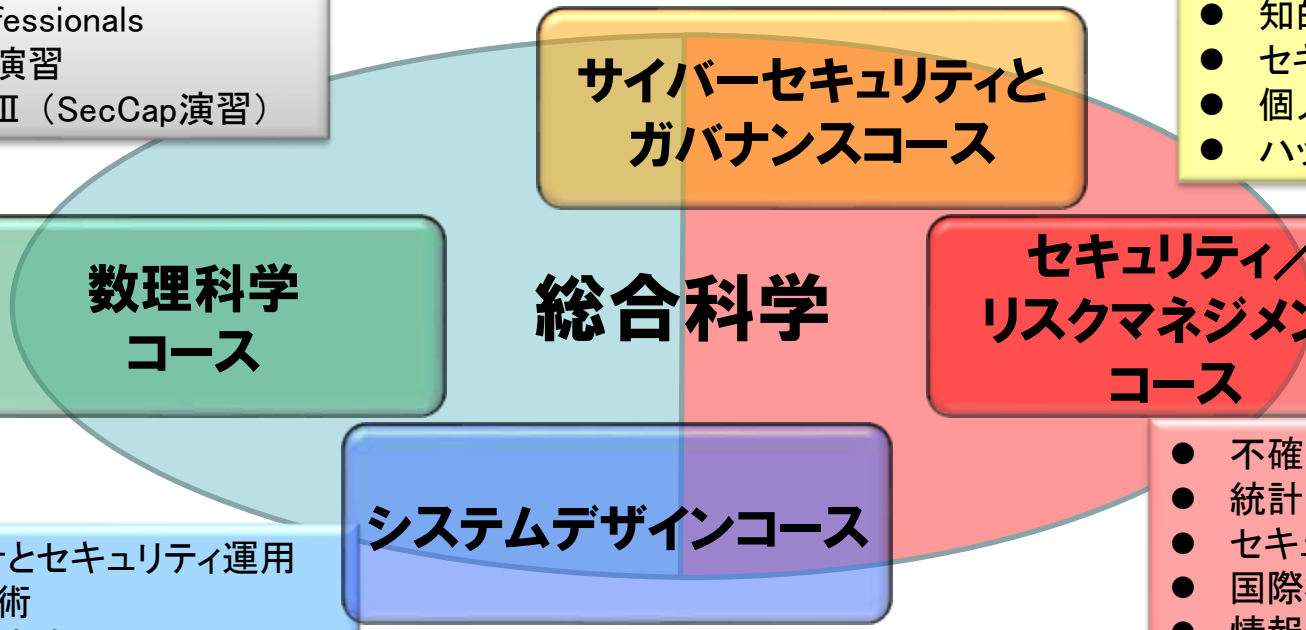
情報セキュリティ（専門の）大学院大学

https://www.iisec.ac.jp/

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

総合学習とハンズオン

- 情報セキュリティ特別講義
- 情報セキュリティ輪講 Ⅰ・Ⅱ
- Presentations for Professionals
- 情報セキュリティ技術演習
- セキュリティ実践 Ⅰ ＆ Ⅱ（SecCap演習）



- サイバーセキュリティ技術論
- セキュアシステム構成論
- セキュア法制と情報倫理
- 法学基礎
- 知的財産制度
- セキュリティの法律実務
- 個人識別とプライバシー保護
- ハッキングとマルウェア解析＊

- 暗号・認証と社会制度
- 暗号プロトコル
- アルゴリズム基礎
- 数論基礎
- 量子計算と暗号理論
- AIと機械学習
- ブロックチェーン理論＊

- ネットワーク設計とセキュリティ運用
- 情報デバイス技術
- 情報システム構成論
- オペレーティングシステム
- セキュアプログラミングとセキュアOS
- プログラミング
- ソフトウェア構成論
- 実践的IoTセキュリティ

- 不確実性下の意思決定
- 統計的方法論
- セキュリティシステム監査
- 国際標準とガイドライン
- 情報セキュリティ心理学
- リスクマネジメントと情報セキュリティ
- セキュリティ経営とガバナンス
- 組織行動と情報セキュリティ
- マスメディアとリスク管理
- データサイエンスとアナリティクス＊
- クリティカルシンキングとイノベーション

修士（情報学）
博士（情報学）

課程修了要件

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

	博士前期課程 [2年制]	博士前期課程 [1年制]	博士後期課程
標準修業年限	2年	1年	3年 （1年以上）
所要単位	46単位以上 専攻科目24 (含必修4) 研究指導22	46単位以上 専攻科目40 (含必修4) プロジェクト研究指導6	8単位以上 博士専門8 (含必修8)
学位論文等	修士論文	リサーチペーパー	博士論文

◆ 横浜市神奈川区鶴屋町2-14-1
（横浜駅きた西口徒歩1分）