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

# DX with Cybersecurity

## ～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

# 概要



社会経済活動においてIoTやクラウド等のデジタル技術を広く活用するDX（デジタル改革）の恩恵を享受するためには、サイバーセキュリティ確保を同時並行して進めることが欠かせない。

特に交通インフラ等では、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。

今後、社会全体のデジタル基盤依存が高まる時代に向けて、どのような“備え”を急ぐ必要があるかについて考える。

# 新型コロナ：企業ICT環境でのテレワーク雪崩



コロナ前

まずはDX（デジタル化）推進室の設置から。。。。

コロナ（禍）渦中

業務継続のためにデジタル化が**突如強制**される

- **在宅勤務が社会経済活動の中核に！**
- **クリティカルサービスも在宅オペレーション？**

デジタル化の「**強風・追風**」を活用し、一気にDXにつなげる！

**with Cybersecurity** をお忘れなく！

# 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
- サイバー攻撃が大規模被害に拡大する懸念
- 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

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：Europoll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

# 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

調達側からサプライヤーへ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と信頼性確保

サプライヤー側から調達元へ供給される部品・製品に不正機能が混入
⇒ 製造から流通までをカバーする混入防止対策・異常検知

グローバルサプライチェーン全体での企業責任
⇒企業不正への対処に加え、SDGs, ESG等の新たなルール形成への対応に関する説明責任とトラストの確立

# サプライチェーン：サイバー攻撃リスク

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

2019年 防衛装備品情報の漏えい事案？

2020年 自動車サプライチェーンの事案？

**営業秘密の漏洩**
**（設計情報・製造情報等）**


**不正なソフトウェアの混入**

**不正な部品の混入**

**不正なハード
ウェアの挿入**

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。

# 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



## 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**

# グローバルサプライチェーンがサイバー攻撃対象に



## サプライチェーンセキュリティ課題の深刻化

「ソフトウェアサプライチェーン攻撃」（例 Solar Winds事案）

ソフトウェアの正規の更新プロセスを乗っ取り、多数のシステムにマルウェアを配信　⇒セキュリティ維持の枠組み再点検

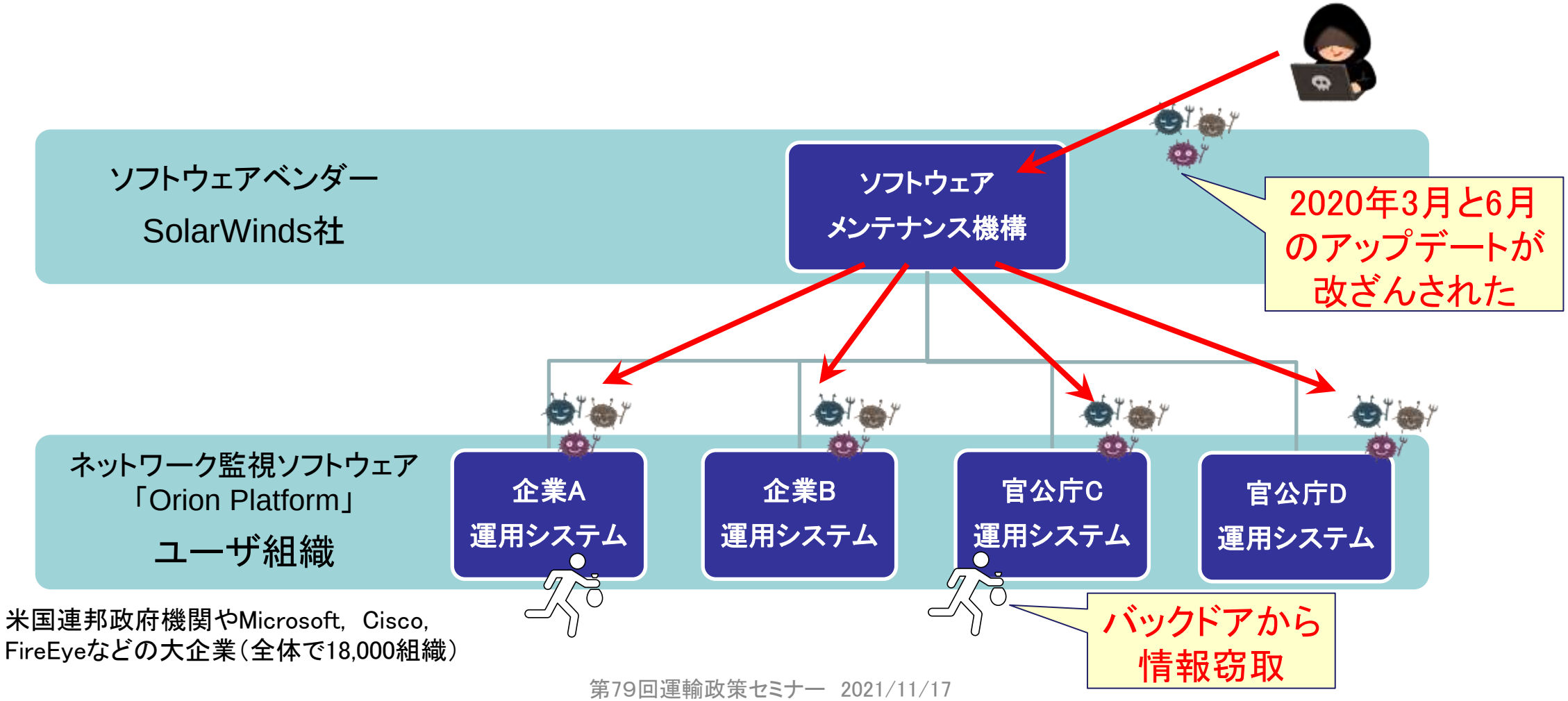
「インフラへのランサムウェア攻撃」（例　Colonial社石油パイプライン事案）⇒サイバー攻撃被害連鎖（大規模化）への対処

- 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

# 事案：SolarWinds社のソフトウェア更新機能改ざん



■ 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）

# 社会・産業インフラへのランサムウェア攻撃

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

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/

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」

運営会社コロニアル・パイプラインが500万ドル（約5億5000万円）近い身代金を支払っていた

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

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/

7月5日 日経新聞
「米でまたサイバー攻撃、1000社影響も　ITサービス狙う」

米IT企業カセヤの法人向けソフトウエアが標的となり、利用企業の間でランサムウエア（身代金要求型ウイルス）の被害が拡大していたことがわかった。影響は1000社に及ぶ

https://www.nikkei.com/article/DGXZQOGN044JN0U1A700C2000000/

# 事業継続停止による被害の連鎖



■ サイバー攻撃によるサプライチェーン寸断による経済活動への悪影響

サイバー攻撃 → サプライヤ工場の停止 → 最終製品の生産停止 → 経済活動への悪影響

■ 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

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」**

# クラウド停止がもたらす大規模被害予測

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

■ 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**

■ 社会全体のサイバー化、デジタル化を進める上での**「備え」**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**の議論と取組みが**国全体として**必要に

# 国全体を俯瞰したリスク分析と被害シミュレーション



**自然災害のハザードマップ**

**南海トラフ巨大地震**

資産等への被害（被災地）
97.6兆円～169.5兆円

経済活動への影響（全国）
30.2兆円～44.7兆円

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

**サイバー攻撃被害のハザードマップ?**

**大規模セイバー攻撃**

直接の被害は？

二次被害・三次被害は？

コロニアル社のランサム被害 → 米国東海岸の社会経済への二次被害

クラウドダウンの被害 → 二次被害
0.7兆円～1.6兆円

**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**
  - CPSを対象とした未知の**脆弱性のDB**（DBそのものを耐攻撃性も重要）
  - 日本で分析した**マルウェアDB**（日本版ウイルストータル for CPS）

# 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

サイバー攻撃が大規模被害に拡大する懸念

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