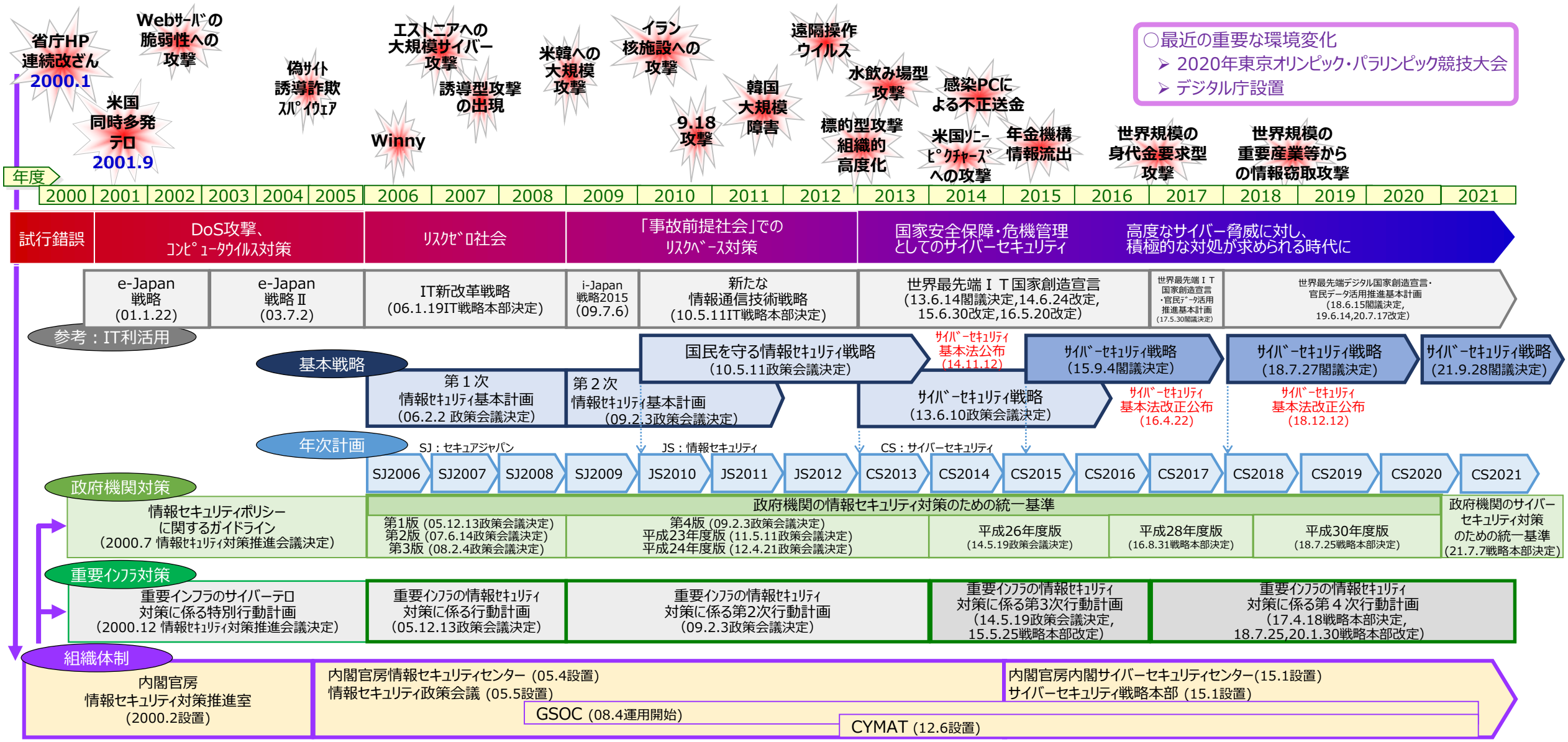
資料２

重要インフラにおける
サイバー事案対応

2021年12月17日

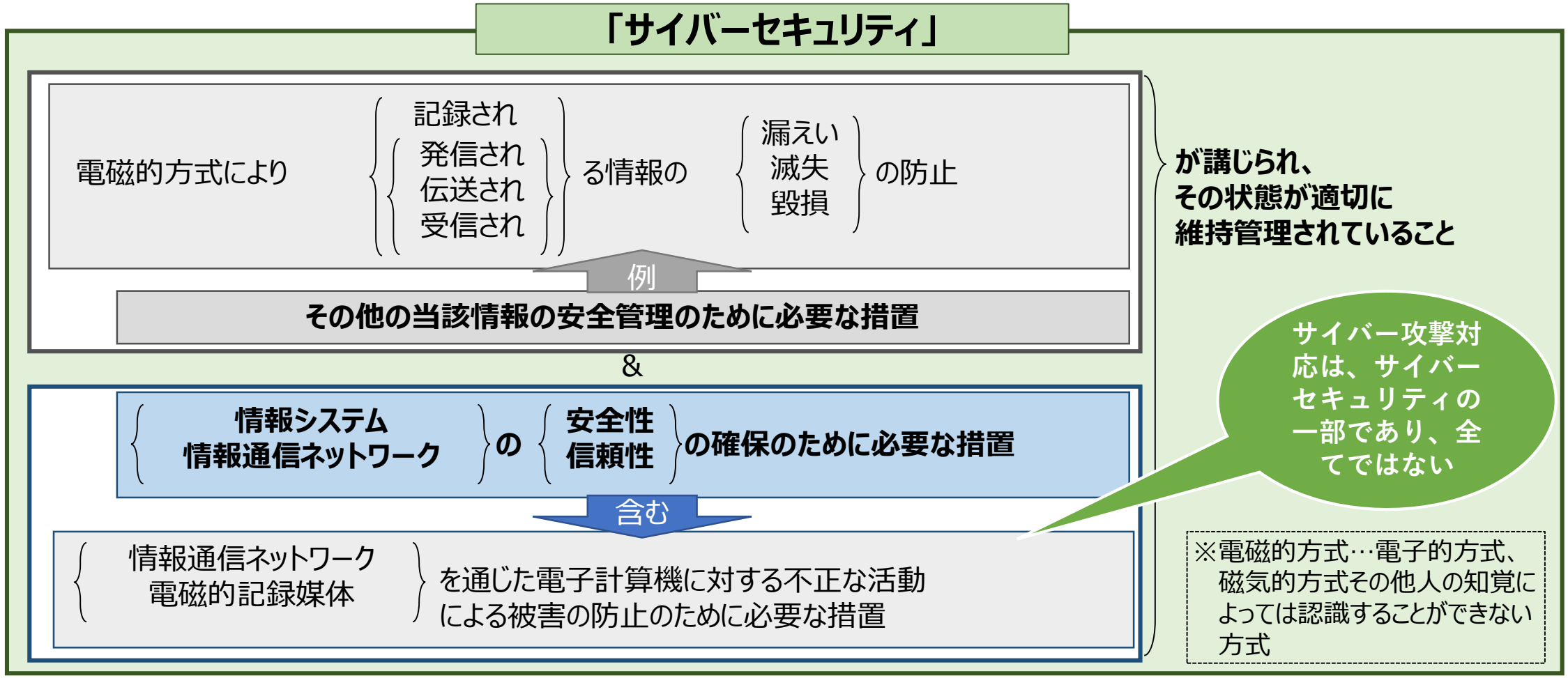
内閣官房内閣サイバーセキュリティセンター
重要インフラグループ
内閣参事官　結城 則尚

サイバーセキュリティ政策の経緯



サイバーセキュリティの定義(サイバーセキュリティ基本法第２条)

（定義）
第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の**当該情報の安全管理のために必要な措置**並びに**情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置**（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が**講じられ、その状態が適切に維持管理されている**ことをいう。



世界における深刻なサイバー事案の例

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している

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

2002年～2021年　日本の大手金融機関にて複数回にわたりATM障害や振込遅延等のシステム障害

2018年～2021年　日本の幾つか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

2019年　日本の幾つかの自治体が利用するクラウドサービスにおいてシステム障害、一部自治体では、復旧まで1ヶ月以上要するなど影響が長期化

2021年　日本の重要インフラ事業者等が利用するクラウドにおける設定不備による意図しない情報漏えい

2021年　ランサムウエア攻撃により、重要インフラ事業者等が利用する業務委託先で7億5000万円の特別損失を計上

2020年9月　米国の医療サービス大手Universal Health Servicesに対するランサムウエア攻撃、復旧に70億円以上

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

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

2021年6～7月　CDN事業者の世界同時多発的な障害によりWebサービスを提供できなくなる事案が発生、ECサイトなど複数の事業者が数時間停止

留意すべきサイバー事案の例（国内）

留意すべき事例１
日本の大手金融機関の主なシステム障害の事例 [2002年4月～2021年9月]

2002年　営業初日から、システム障害が発生

2011年　ATM障害や大量の振込処理遅延

2021年　ATMの利用停止など、
年内に合計8回のシステム障害が発生※

【※一部の障害に関する第三者委員会報告書抜粋】

■ **障害に共通する原因として、危機対応力やIT システム統制の弱さ等がある**

**大規模なシステム障害により、
顧客に影響を与えた一例**

留意すべき事例２
日本の重要インフラ事業者等が利用する業務委託先に対するランサムウエア攻撃 [2021年]

- 委託した複数自治体で本件に伴う被害が生じた可能性があると相次ぎ報道
- 委託先1社はランサムウエア攻撃の影響により、**約7億5000万円の特別損失**※計上発表

※2021年9月期(2020年10月～2021年9月)の連結業績
復旧に向けた調査及び対応関連費用として

■ **ランサムウエアの登場に伴い、サイバー攻撃が事業者の事業継続や経営に大きな影響を及ぼすものに変化**

■ **国外で確認されていたランサムウエア攻撃が、ここ数年、国内の事業者でも多く確認**

**サイバー攻撃により、
事業者の決算に影響を与えた一例**

我が国におけるサービス停止事案の最近の特徴

統計上から得られる知見

- サービス停止の原因は、**自然災害、管理ミスが主流**
- **サイバー攻撃事案**といえるものは、**管理不十分**で発生したものが多い

管理を適切にすれば防止できる事案が毎年繰り返されている

- 「サービス停止」は重要インフラサービスの目的からの逸脱
  - 原因にかかわらず、「結果の保証」
- 「**組織全体のマネジメント**」と「**CSIRT**」の**連携が弱い**ようにみえる
  - サイバー事案は、サイバー部門だけで閉じていない
  - **総合的観点からのリスクが共有されていないのでは？**

組織に潜在するリスクをどのようにしたら組織内で共有できるのか

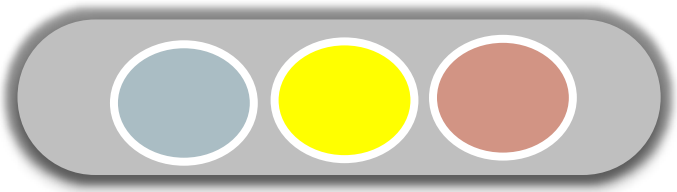
潜在リスクの共有を踏まえた本格的な体制整備の迅速な実施の必要性

これまでの事例・傾向分析

国内における重要インフラの状況

被害拡大寸前で留まっている危うい状態

黄色信号が点灯



サイバー攻撃やシステム障害による影響の拡大

- サイバー攻撃やシステム障害が**社会に影響を及ぼす**ものに変化

【国外】 SolarWinds(米国)、コロニアルパイプライン(米国)、JBS USA(米国)、UHS(米国)、フロリダ州オールズマー市水道局(米国)、証券取引所(ニュージーランド)、上級司法裁判所(ブラジル)など

【国内】 銀行、証券取引所、地方自治体、医療機関など

- サイバー攻撃やシステム障害が**事業者の経営に影響を及ぼす**ものに変化

【国外】 Norsk Hydro(ノルウェー)など
【国内】 重要インフラ事業者等が利用する業務委託先、証券取引所など

システム障害発生後の復旧が長期化

- 昨今、システム障害やサイバー攻撃の発生に伴い、**復旧が長期化**

【国内】

- ✓ 2018年、病院の電子カルテシステムがランサムウエアに感染、事象発生から約5ヶ月後、暗号化されたデータを復元
- ✓ 2019年、自治体向けクラウドサービスで障害が発生、一部では、復旧まで1ヶ月以上要するなど影響が長期化
- ✓ 2020年、証券取引所の株式売買システムに発生した障害により、1999年の取引全面システム化以降初めて全銘柄の売買を終日停止

■ **重要インフラ防護は、システム担当だけで対応できるものではなく、組織全体で対応する必要があるとの考え方のもとで、障害対応体制強化が必要**

■ **将来の環境変化を先取りし、リスクを明確化し対応できるようにするための取組が必要**

重要インフラ行動計画改定への提言

令和３年(2021 年)10 月 25 日

サイバーセキュリティ戦略本部

重要インフラ専門調査会 政策部会

NISCホームページからダウンロード可能
https://www.nisc.go.jp/conference/cs/ciip/dai26/pdf/26shiryou05.pdf

重要インフラ行動計画改定への提言（概要）

現状認識

重要インフラを取り巻く環境は、予断を許さない状況まで来ている

- **第４次行動計画策定以降の状況変化**
  - ✓ サイバーセキュリティを取り巻く環境変化
  - ✓ 新たなサイバーセキュリティ戦略の策定
  - ✓ 近年のサービス障害の原因は、自然災害、管理ミスが主流、多くは管理不十分によって発生

課題の明確化

管理を適切にすれば防げた類似障害が繰り返し発生していることを踏まえ経営層を含め組織的対策が必要

- **第４次行動計画「本行動計画の検証」に基づく評価としては、一定の成果あり**
- **上記評価から直接導出されない課題が存在**
  - ✓ 経営層を含めた組織統治の在り方の検討
  - ✓ サイバーセキュリティ基本法に規定された責務等が認識されていない懸念
  - ✓ 将来を見据えた環境変化、新たなリスクへの対応

改定への提言

第４次行動計画における有効な取組は継続しつつ、特に以下の2点に留意すべき

- **（提言１）障害対応体制の強化の在り方の抜本的な見直し**
  - ✓ 現在の「経営層への働きかけ」から、組織統治の一部としてサイバーセキュリティを組み入れる方針を具体的に記載
  - ✓ サイバーセキュリティ基本法が公布・施行されたことを踏まえ、各関係主体の責務等を明確化
- **（提言２）将来の環境変化を先取りし、サプライチェーン等を含め包括的に対応**

重要インフラ関連インシデントの例

サイバー攻撃・管理ミスの例

ランサムウエアに感染し、**データが暗号化**されたのに加え、**機密情報を公開**すると身代金を要求された。

1. セキュリティアップデート未適用のVPNの脆弱性を突いた認証情報の窃取
2. 海外拠点等セキュリティ対策の弱い拠点からの侵入
3. 委託先クラウドのランサムウエア感染

対応・対策の一案

- **ネット接続にかかる資産管理の重要性の再認識(予防策)**
  - VPNの重要性の再認識と脆弱性を含めた管理の厳格化
- **侵入を前提とした多層防御を備えたシステム設計の検討(予防策)**
- サプライチェーン管理の徹底(予防策)
  - リスクに応じた外部サービスの利用
  - サプライチェーンに携わる事業者間のコミュニケーション強化
- **バックアップの重要性の再認識(緩和策)**
  - 二重脅迫型ランサムウエアにはバックアップだけでは不十分→暗号化、秘匿化が必要

バックアップの321ルールを応用したランサムウエア対策の例

✓ ランサムウエア感染時バックアップも暗号化され、復旧できない事例発生
✓ これまで発出した注意喚起で、一般的なグッドプラクティスの例を何度か紹介
✓ こうした対策がなされていれば、復旧は円滑に行えたものと考えられる

■ 「321ルール」を応用したランサムウエア対策の例

3. データを3つ保存
2. バックアップファイルを異なる2種類の媒体に保存
1. 1つをオフラインに保管

NISC重要インフラグループから主な注意喚起等（直近の公表ベース）

■ **2020年11月26日**

✓ ランサムウエアによるサイバー攻撃について【注意喚起】
https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf

■ **2021年4月26日**

✓ 大型連休等に伴うセキュリティ上の留意点について
https://ww.nisc.go.jp/active/infra/pdf/renkyu20210426.pdf

■ **2021年4月30日**

✓ ランサムウエアによるサイバー攻撃に関する注意喚起について
https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf

■ **2021年5月7日**

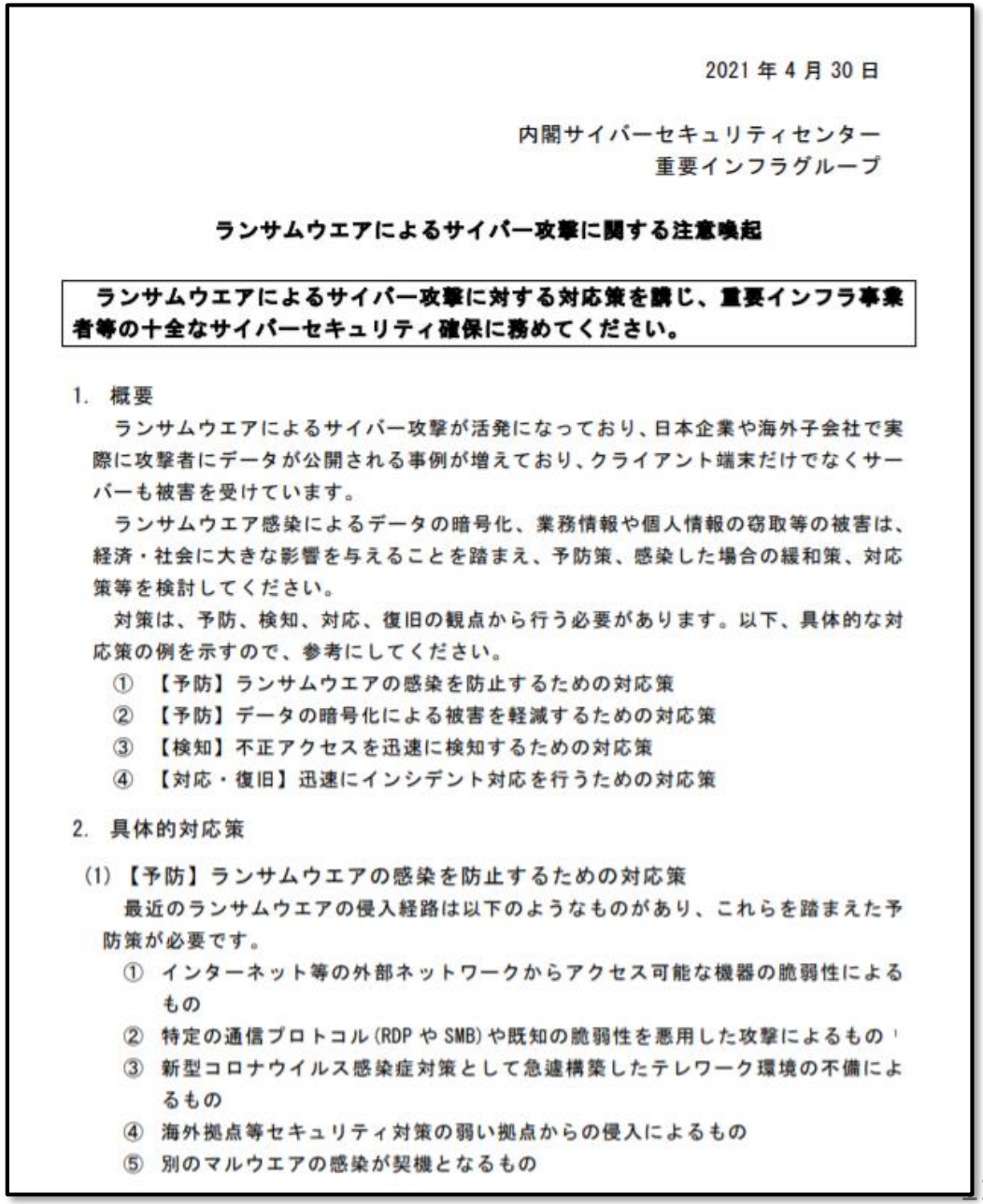
✓ 大型連休明けに確認が必要な情報について
https://www.nisc.go.jp/active/infra/pdf/renkyuake20210507.pdf

■ **2021年7月21日**

✓ 夏季休暇等に伴うセキュリティ上の留意点について
https://www.nisc.go.jp/active/infra/pdf/summer20210721.pdf

■ **2021年10月13日**

✓ ランサムウェア特設ページを公開
https://security-portal.nisc.go.jp/stopransomware/



2021 年 4 月 30 日

内閣サイバーセキュリティセンター
重要インフラグループ

ランサムウエアによるサイバー攻撃に関する注意喚起

ランサムウエアによるサイバー攻撃に対する対応策を講じ、重要インフラ事業者等の十全なサイバーセキュリティ確保に務めてください。

1. 概要

ランサムウエアによるサイバー攻撃が活発になっており、日本企業や海外子会社で実際に攻撃者にデータが公開される事例が増えており、クライアント端末だけでなくサーバーも被害を受けています。

ランサムウエア感染によるデータの暗号化、業務情報や個人情報の窃取等の被害は、経済・社会に大きな影響を与えることを踏まえ、予防策、感染した場合の緩和策、対応策等を検討してください。

対策は、予防、検知、対応、復旧の観点から行う必要があります。以下、具体的な対応策の例を示すので、参考にしてください。

① 【予防】ランサムウエアの感染を防止するための対応策
② 【予防】データの暗号化による被害を軽減するための対応策
③ 【検知】不正アクセスを迅速に検知するための対応策
④ 【対応・復旧】迅速にインシデント対応を行うための対応策

2. 具体的対応策

(1) 【予防】ランサムウエアの感染を防止するための対応策

最近のランサムウエアの侵入経路は以下のようなものがあり、これらを踏まえた予防策が必要です。

① インターネット等の外部ネットワークからアクセス可能な機器の脆弱性によるもの
② 特定の通信プロトコル(RDP や SMB)や既知の脆弱性を悪用した攻撃によるもの
③ 新型コロナウイルス感染症対策として急遽構築したテレワーク環境の不備によるもの
④ 海外拠点等セキュリティ対策の弱い拠点からの侵入によるもの
⑤ 別のマルウエアの感染が契機となるもの

サイバーセキュリティは全員参加で

チームワークをもって全員参加

セキュリティは組織運営の一部

- **始めはみんな初心者**
  - 知らないことを知ることが第一歩
  - 自助(一人一人)、**共助(組織、ISAC)**、公助(国)で対応
- **セキュリティは、全分野ひとりで出来ないチーム戦**
  - 優秀な選手を集めるのは重要
  - それ以上に優秀なコーチ、監督がいないと勝てない
- **セキュリティは、他部門には常に疎まれる立場**
  - リーダーがその価値を認め、チームを支えないとチーム全体の士気は下がる
    - 一人ですべてできないことを知る
    - トップ、ミドル、ローがそれぞれ適切な役割分担がなされて全員参加
    - 各人の役割、これまで歩んできたキャリアパスで得た経験を総動員する

チームワークをもって全員参加で対応するもの

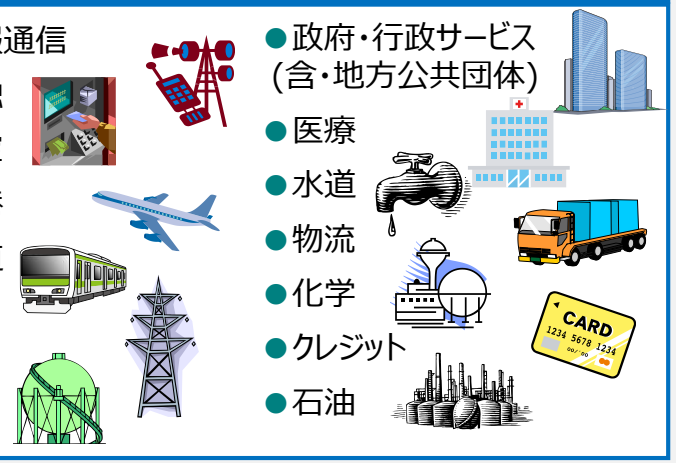
重要インフラの情報セキュリティ対策に係る第４次行動計画

官民連携による重要インフラ防護の推進

重要インフラにおいて、機能保証の考え方を踏まえ、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

重要インフラ(全14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（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油



NISCによる調整・連携

重要インフラ所管省庁

- 金融庁　［金融］
- 総務省　［情報通信、行政］
- 厚生労働省［医療、水道］
- 経済産業省［電力、ガス、化学、クレジット、石油］
- 国土交通省［航空、空港、鉄道、物流］

関係機関等

- 情報セキュリティ関係省庁　［総務省、経済産業省等］
- 事案対処省庁　［警察庁、防衛省等］
- 防災関係府省庁　［内閣府、各省庁等］
- 情報セキュリティ関係機関　［NICT、IPA、JPCERT等］
- サイバー空間関連事業者　［各種ベンダー等］

「重要インフラの情報セキュリティ対策に係る第４次行動計画」

安全基準等の整備・浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化

リスクマネジメント及び対処態勢の整備

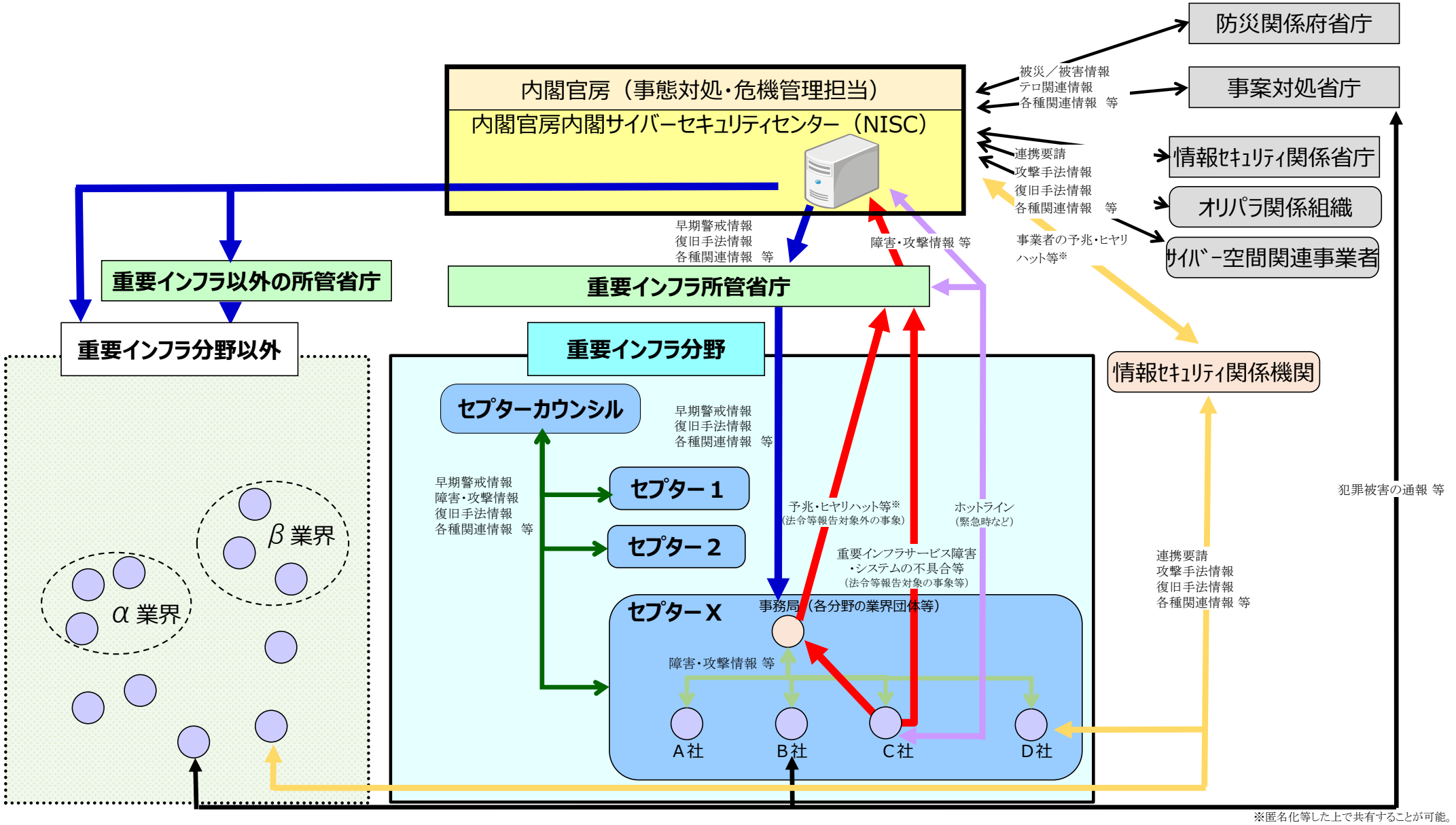
リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

2022年度初期に決定すべく現在改定検討中

第４次行動計画における情報共有体制



※匿名化等した上で共有することが可能。

分野別情報共有体制の現状(セプターマップ)

2021年9月末日現在

重要インフラ分野	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
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会				航空CEPTOAR	空港CEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
				銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR												
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟、日本放送協会	(一社)全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部経営企画・法務グループ	(一社)日本損害保険協会 ＩＴ推進部品質管理グループ	定期航空協会	空港・空港ビル協議会	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術部	地方公共団体情報システム機構 情報化支援戦略部	(公社)日本医師会 情報システム課	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員(のべ数)	23社 1団体	311社 1団体	196社・団体	1,296社	280社 7機関	42社	47社	14社 1団体	8社	22社 1団体	25社 3機関	10社・団体	47 都道府県 1,741 市区町村	1グループ 20機関	8水道事業体	6団体 17社	13社	50社	11社
NISCからの情報の展開先(構成員以外)	378社・団体	394社	11社	2社・団体	ー	ー	ー	ー	ー	ー	15社・機関	172社・団体	ー	391社・団体	内容に応じ1,326事業体へ展開	ー	ー	ー	ー
	その他(核物質防護等の措置が要求される企業、ビルディング・オートメーション協会、サイバーディフェンス連携協議会、大学等(内容に応じ展開先を選定))																		

■ その他

既存事業領域を越える連携等	情報通信(ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟)、金融(金融ISACにおいて、加盟金融機関間で情報共有・活動連携)、航空・空港・鉄道・物流(交通ISACにおいて、参加事業者間で情報共有・活動連携)、電力(電力ISACにおいて、加入する電気事業者間で情報共有・活動連携)、化学(石油化学工業協会と日本化学工業協会の情報共有・活動連携)、クレジット(ネットワーク事業者と情報共有・活動連携)、制御システム(JPCERT/CCが提供するConPaS等)、J-CSIP(IPA：標的型攻撃等に関する情報共有)、サイバーテロ対策協議会(重要インフラ事業者等と警察との間で連携、47都道府県に設置)、早期警戒情報CISTA(JPCERT/CC: セキュリティ情報全般)

業界内の情報共有機能としてのセプター及びISAC

- セプター(CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response)
  - 各セプターは、分野内の情報共有のハブとなるだけではなく、重要インフラ防護の関係主体間における情報連携の結節点としても機能(全19セプター)
  - **重要インフラ行動計画**における**公助の受け皿**的な機能もある
- ISAC (Information Sharing and Analysis Center)
  - **国から独立して、自主的な分野内情報共有体制**が確立されている(金融、ICT、電力、交通等)
  - NISCは、金融ISAC等の支援を得つつ、**医療のISAC設立のための支援を2018年度から継続的に実施**
  - **米国H-ISACも厚労省に対して協力する用意がある**としている

互助の観点からこうした業界独自の情報共有機能を構築し活用することが効果的

いざというときに
のために

いざという時に備える体制を確認しましょう

備えあれば患いなし

- 予防に勝る対処なし
- 注意喚起について専属者を決めて、チェックできる体制に
- ちょっとした対応で、大損害から守ることができる

いざという時にとる行動は、シンプルに

- 人は緊急時に多くのことを覚えられない
- 頭の中で覚えられるのは3つくらい
- 頼れる相手にまずは一報を！
- NISCダイレクトパスを躊躇せずに

対外公表は、戦略的に以下の2タイプに分類

- 精度は低くとも早く公表すべきもの
- 時間をかけても精度を高めるべきもの

失敗は成功の基

1. **大事故は突然やってこない**
   - 大事故は、気づかない小さなことが積み重なって**必然的に発生**
2. **芽のうちに刈り取る**
   - 眼にみえるようにするには？
   - **何が正常なのかを知る(本物を知っている)**
     - ➢ 異常状態が検知できる
3. **インシデントハンドリングは宝の山**
   - 1つのインシデントハンドリングから得られる知見は、100冊の本を読むよりも価値がある
   - 積極的に参加し、**許される失敗を多く体感**
   - **成功するためにはその背景に数多くの失敗あり**

ブレーキに「今度」はない

警視庁交通安全教室の際にいただいた教え

- 「じゃあ、今度」
  「まあいいっか」
  が通じる場合もある

しかし

- 適切な対応をその時
  行わないと致命傷と
  なるものがある
- 時計は元に戻せない
- その瞬間を逃すな

NISC

ご清聴ありがとうございました

内閣サイバーセキュリティセンター