日本のサイバーセキュリティを「連携」「学び」「創造」

CoRePo

振り返り教材

日本ネットワークセキュリティ協会(JNSA)
ゲーム教育ワーキンググループ

1. NEXT ACTION

- 皆さんはゲームを通して以下の情報を入手しています。
  - インシデントの対応状況　… 概要（対応～復旧までの進捗）
    … 被害状況とその対応
    … 攻撃と関連する技術情報
    … 対策・再発防止策
  - 関連組織への報告、情報共有、公表

- この状況を用いて**「インシデントを説明する会見」をチームごとに行います**。

- 対応の過不足はゲームの運次第ですが、「今ある状況で最善の説明」が出来るかを互いに評価し、対応の気付き・注意点を学びましょう。

- 「うまく言いくるめること」が会見の目的ではありません。
  信用を損なわず事業を継続させつつも、引き続きインシデント調査を進められる状態にすることが重要です。

2. この後の流れ

座学	チームディスカッション	発表 / 質疑応答	講評
			
30分	10-15分	(発表 3分 / 質疑 7分) x チーム数	5分

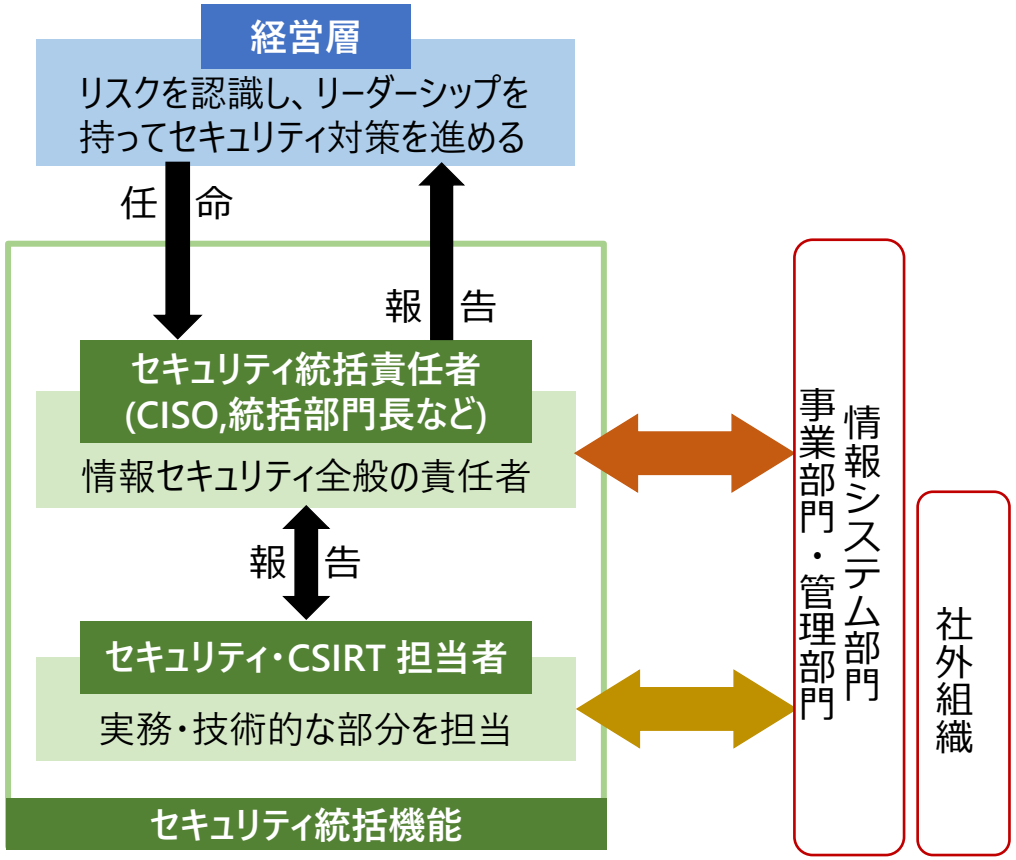
➢ 発表を見据えた座学のススメ

- ゲームプレイで対応した**調査と外部への報告状況を踏まえ、どのような要素を報告をすべきか学習**しましょう。
- ゲーム内で各種報告済みの内容であっても、ユーザの大多数はまだこのインシデントについて深く知っていません。**改めて状況を整理し不要な憶測などを抑制することを目的**に、記者会見を実施してください。
- ゲーム内では「オンラインサイトの改ざん」としか被害の記載がありませんが、それによって**どのような被害が起こったのかは、参加チームごとに決定してもらってOK**です。

3-1. CISOへの報告

■CISO（Chief Information Security Officer）の役割

- CISOは組織のセキュリティ対策を所管する立場であり、経済産業省の「サイバーセキュリティ経営ガイドライン」では、経営者が認識すべき3原則とCISOなどに指示すべき10の重要事項が記載されている



サイバーセキュリティ経営の重要10項目

#	指示	内容
1	サイバーセキュリティリスクの管理体制構築	
	①	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
	②	サイバーセキュリティリスク管理体制の構築
	③	サイバーセキュリティ対策のための資源（予算、人材）確保
2	サイバーセキュリティリスクの特定と対策の実装	
	④	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
	⑤	サイバーセキュリティリスクに効果的に対応する仕組みの構築
	⑥	PDCAサイクルによるサイバーセキュリティ対策の継続的改善
3	インシデント発生に備えた体制構築	
	⑦	インシデント発生時の緊急対応体制の整備
	⑧	インシデントによる被害に備えた事業継続・復旧体制の整備
4	サプライチェーンセキュリティ対策の推進	
	⑨	ビジネスパートナーや委託先などを含めたサプライチェーン全体の状況把握及び対策
5	ステークホルダーを含めた関係者とのコミュニケーションの推進	
	⑩	サイバーセキュリティに関する情報の収集、共有および開示の促進

参照：サイバーセキュリティ経営ガイドラインと支援ツール（METI/経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

1. 必要な報告項目

■インシデント発生時におけるCISOの役割

- インシデント対応の役割分担
  - CSIRT　：具体的なインシデントハンドリングを担当
  - CISO　：ビジネスへの影響を考慮したステークホルダーとの調整と対応
    （例）　経営陣、顧客、関連省庁など

■CISOに報告が必要な項目

- インシデントが発生した場合、CISOはその影響や原因、再発の有無についても説明できる必要があり、右記の項目が発表内容として想定される
- インシデントハンドリングを行う担当者は、同項目についてCISOに報告することが求められる

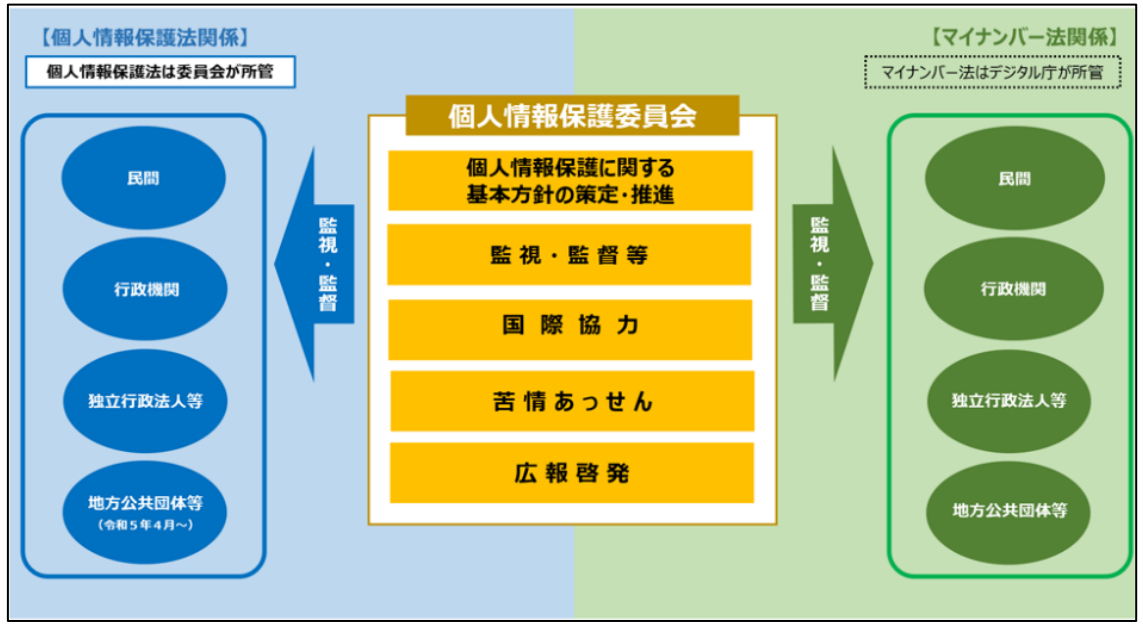
インシデント発生時に想定される発表内容

- インシデントの概要
- 影響を受ける顧客数と特徴
- 想定される二次被害
- 顧客などに推奨する対策
- インシデントの原因・要因
- 事業への影響の有無
- 再発防止策

参照：
CISO ハンドブック（CISO支援WG） | NPO日本ネットワークセキュリティ協会
https://www.jnsa.org/result/2018/act_ciso/index.html

3-2. 個人情報保護委員会への報告

- 個人情報保護委員会は、個人情報の適正な取扱いの確保を図る行政機関
- 個人情報が漏えいした場合には、**個人情報保護法**に基づき、一定の要件を満たす場合において、個人情報保護委員会への報告および本人への通知が義務付けられている



【個人情報保護委員会の業務】

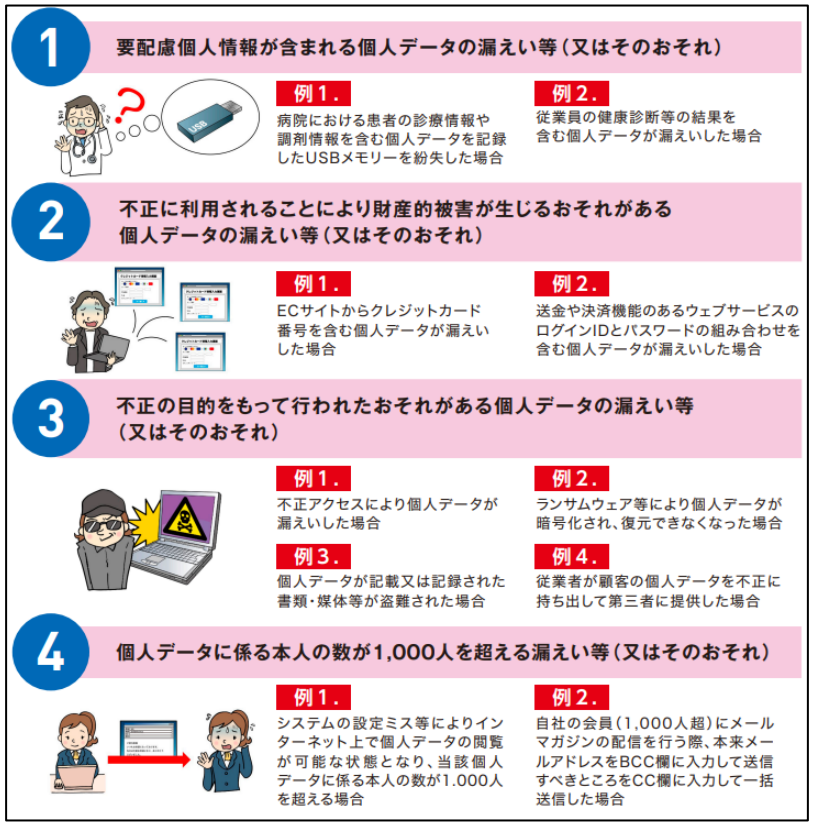
1. 個人情報の保護に関する記法方針の策定・推進
2. 個人情報等の取扱いに関する監視・監督
3. 海外の関係機関との情報交換
4. 相談・苦情あっせん等
5. 個人情報の保護に関する広報・啓発活動

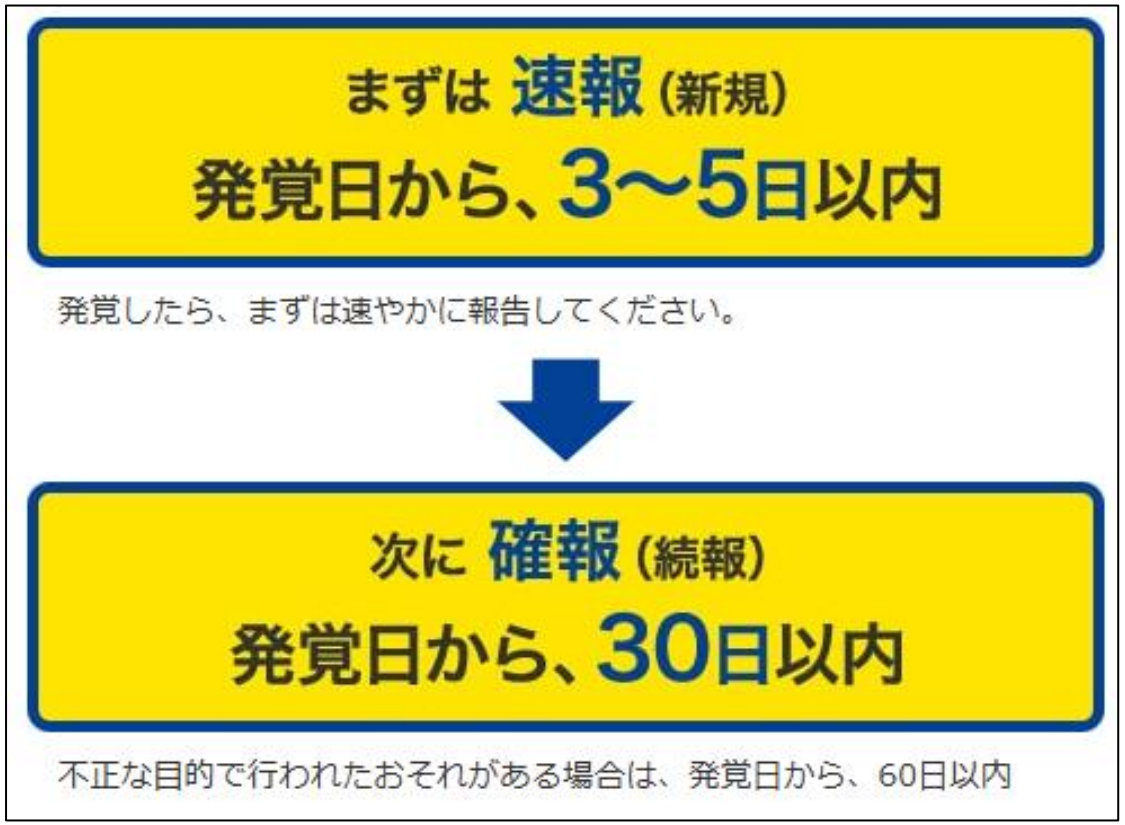
など

参照：個人情報保護委員会について
https://www.ppc.go.jp/aboutus/commission/

1. 報告が必要なケースと報告期限

以下の要件に該当する場合、個人情報保護委員会への報告が必要となる（民間事業者、行政機関で基準が異なる。以下は民間事業者の場合）



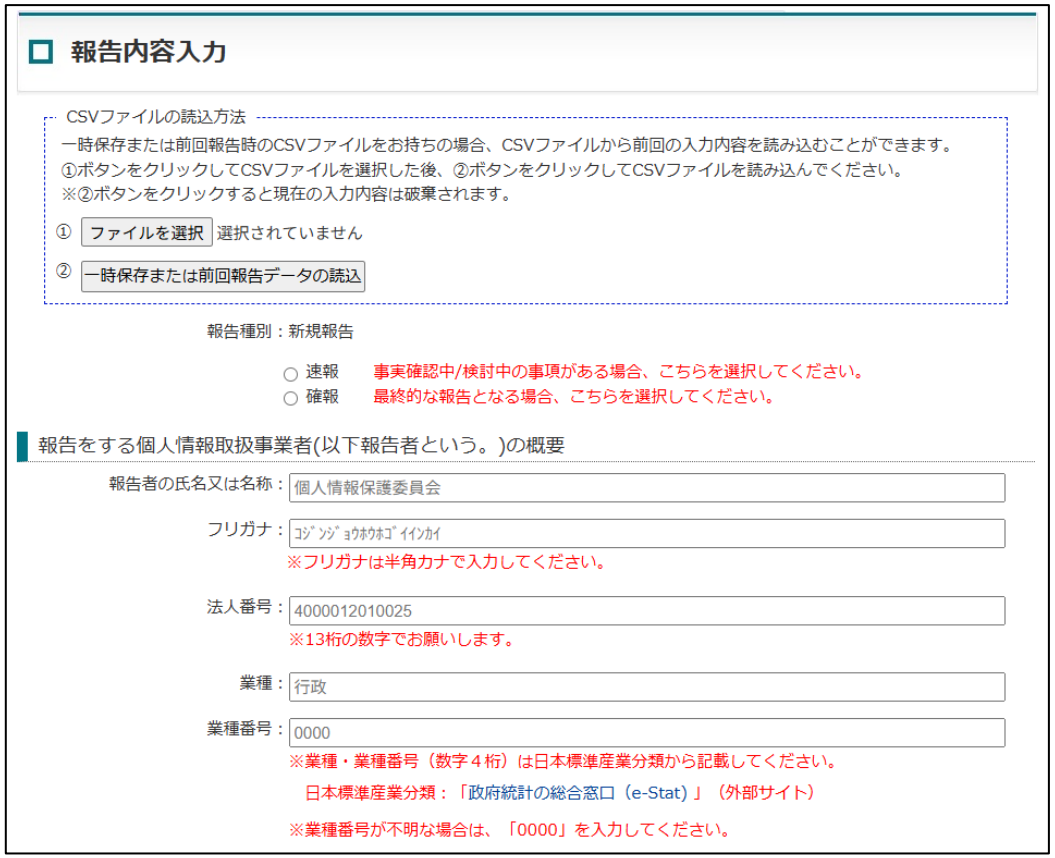


参照：個人情報保護委員会「漏えい等の対応とお役立ち資料」
https://www.ppc.go.jp/personalinfo/legal/leakAction/

2. 必要な報告項目

個人情報保護委員会への報告には、以下の項目を報告する必要がある

1. 事態の概要
2. 個人データの項目
3. 個人データに係る人数
4. 原因
5. 二次被害又はその恐れの有無及びその内容
6. 本人への対応の実施状況
7. 公表の実施状況
8. 再発防止のための措置
9. その他参考となる事項



参照：個人情報保護委員会「報告フォーム」
https://roueihoukoku.ppc.go.jp/incident/incidentacceptance_r2

3-3. 所管省庁との連携

所管省庁への報告については、法令で義務付けられているものと法的拘束力はないがガイドラインに基づく推奨事項として挙げられているものがある

＜法的拘束力のある義務＞

（1）法令に基づく義務

個人データの漏えい・滅失・毀損（漏えい等）に対する報告義務	個人情報保護法ほか	一定の要件に該当する個人データの漏えい等又はそのおそれのある事態（報告対象事態）について個人情報保護委員会等への報告義務（個人情報保護法 26 条） ※原則本人への通知が必要、漏えい等事案の内容等に応じて公表が望ましい
特定個人情報の漏えい等に対する報告義務	マイナンバー法	一定の要件に該当する特定個人情報（マイナンバーを含む個人情報）の漏えい等又はそのおそれのある事態等について個人情報保護委員会への報告義務（マイナンバー法 29 条の 4） ※原則本人への通知が必要、漏えい等事案の内容等に応じて公表が望ましい
業法に基づく事故報告義務	各業法	各業法に基づく事故（サイバーセキュリティインシデントを含む）発生時の所管省庁等への報告義務 例）電気通信事業法 28 条（通信の秘密の漏えい・重大事故）
報告等の求めへの対応義務	サイバーセキュリティ基本法ほか各業法等	○当局から法令に基づく報告等の求めがあった場合、原則として対応する義務あり（情報提供・資料提出の求め等） 例）サイバーセキュリティ基本法 17 条 3 項 ○報告徴収をベースとした事故報告義務 例）電気通信事業報告規則 7 条の 3（事故の四半期報告）

＜法的拘束力はないが推奨される事項＞

（1）ガイドライン等に基づく推奨事項

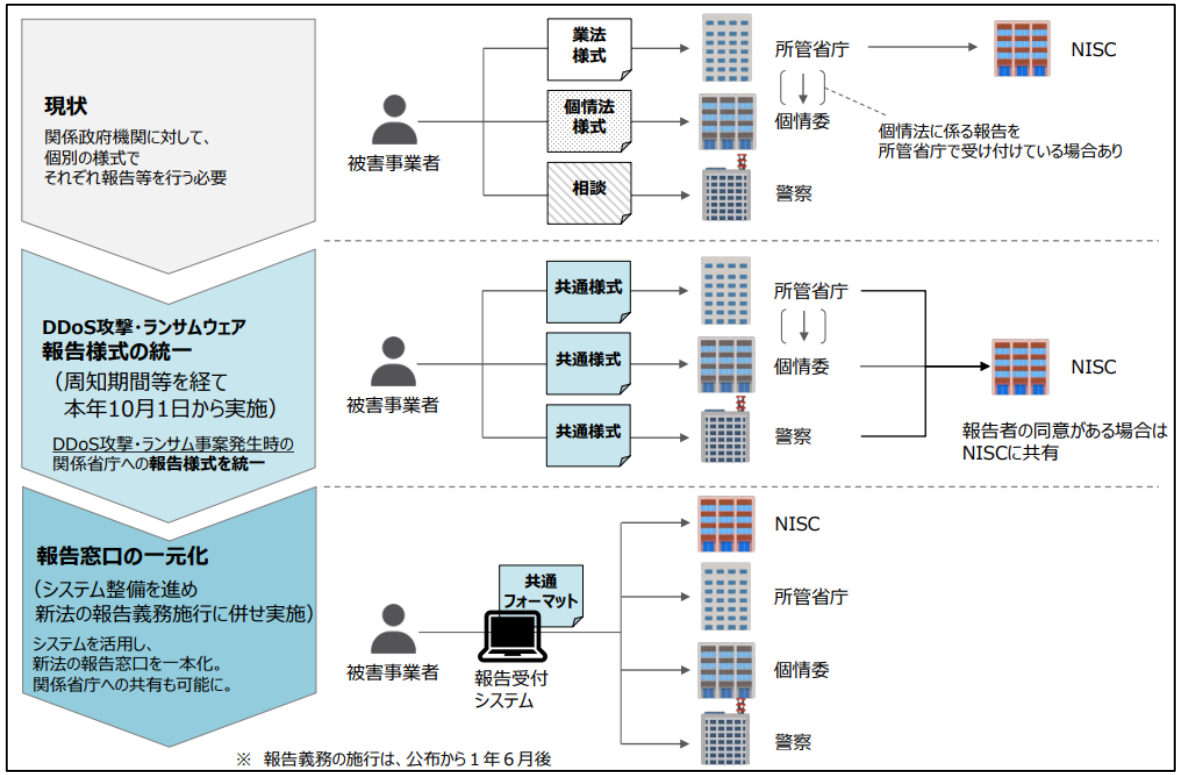
分野別のガイドライン等	個人情報保護関係やセキュリティ関係のガイドラインにおいて、所管省庁等への報告や公表が求められる場合がある 「金融分野における個人情報保護に関するガイドライン
重要インフラ事業者による情報連絡	重要インフラ事業者は、重要インフラサービス障害を含むシステムの不具合等に関する情報について、所管省庁を通じて NISC に連絡することとされている（重要インフラのサイバーセキュリティに係る行動計画（サイバーセキュリティ戦略本部））
不正アクセス等に関する届出	コンピュータウイルス・不正アクセス検知時には、IPA へ届け出ることが望ましい 「コンピュータウイルス対策基準」（平成 7 年通商産業省告示第 429 号） 「コンピュータ不正アクセス対策基準」（平成 8 年通商産業省告示第 362 号）
脆弱性発見時の届出	ソフトウェア製品の脆弱性およびウェブサイトの脆弱性を発見した者は、IPA へその旨を届け出ることが望ましい 「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）
警察への通報・相談	サイバー事案に係る犯罪の被害に遭った場合には、警察へ通報・相談する対応が望ましい（Q18（83 頁）、Q19（85 頁）参照） 「サイバーセキュリティ戦略」（令和 3 年 9 月閣議決定）等

参照：経済産業省「サイバー攻撃に係る情報の共有・公表ガイダンス」
https://www.meti.go.jp/press/2022/03/20230308006/20230308006-2.pdf

1. インシデント報告様式統一の動き

現在、所管官庁への報告は各機関ごとに異なる書式で提出する必要があり、手続きが煩雑化している。これに対し、今後は**報告様式の統一**や**窓口の一元化**が進められる見込みであり、手続きの簡素化が期待されている。

DDos攻撃・ランサムウェアの報告様式の統一は
令和7年10月１日から実施され、適用開始から
１年後を目途に必要な見直しが行われる



参照：内閣サイバーセキュリティセンター「資料５ インシデント報告様式の統一について」
https://www.nisc.go.jp/pdf/council/cs/dai43/43shiryou5.pdf

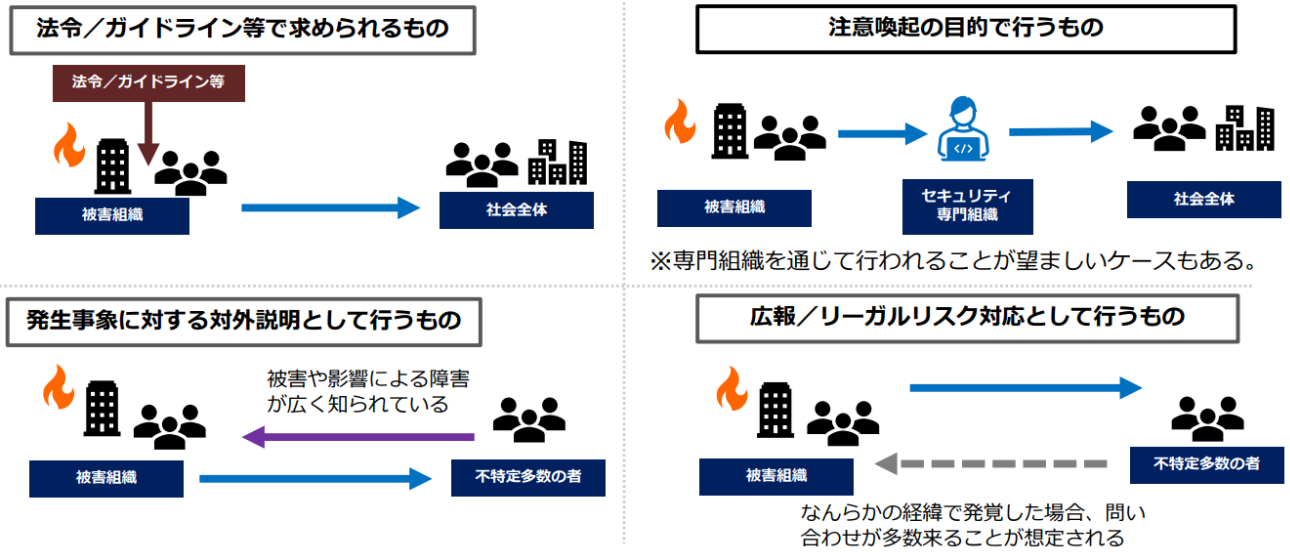
3-4. 脅威情報の共有

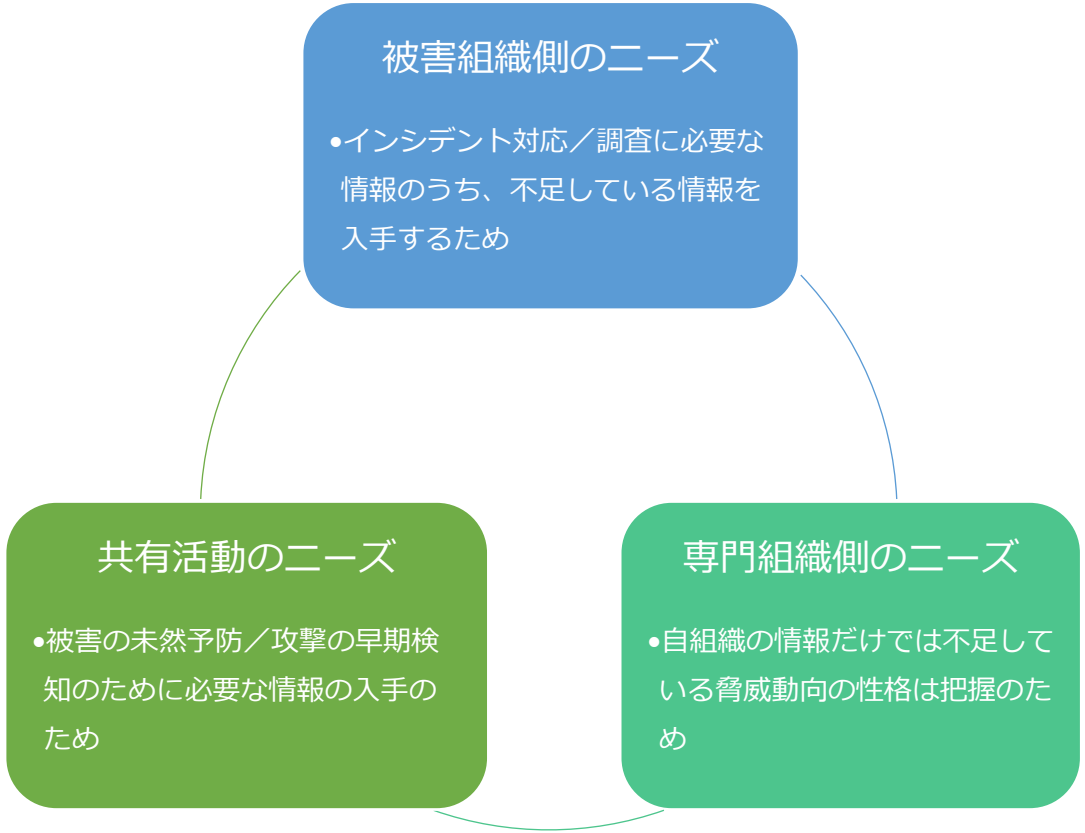
- 攻撃や被害につての情報共有は、自組織で知りえない情報を得られるという利点があり、共助の観点から実施することが望まれる。
- 「サイバー攻撃被害に係る情報の共有・好評ガイダンス」では、**攻撃技術情報**と**被害公表**を分けて考え、考慮すべきポイントがまとめられている。

1. 何のために共有するのか
2. どのような情報を共有するのか
3. どのタイミングで共有するのか
4. どのような主体に対して共有するのか

1. 何のために共有するのか

共有目的を整理することで、公表すべきタイミング、公表に必要な情報を決めることができる



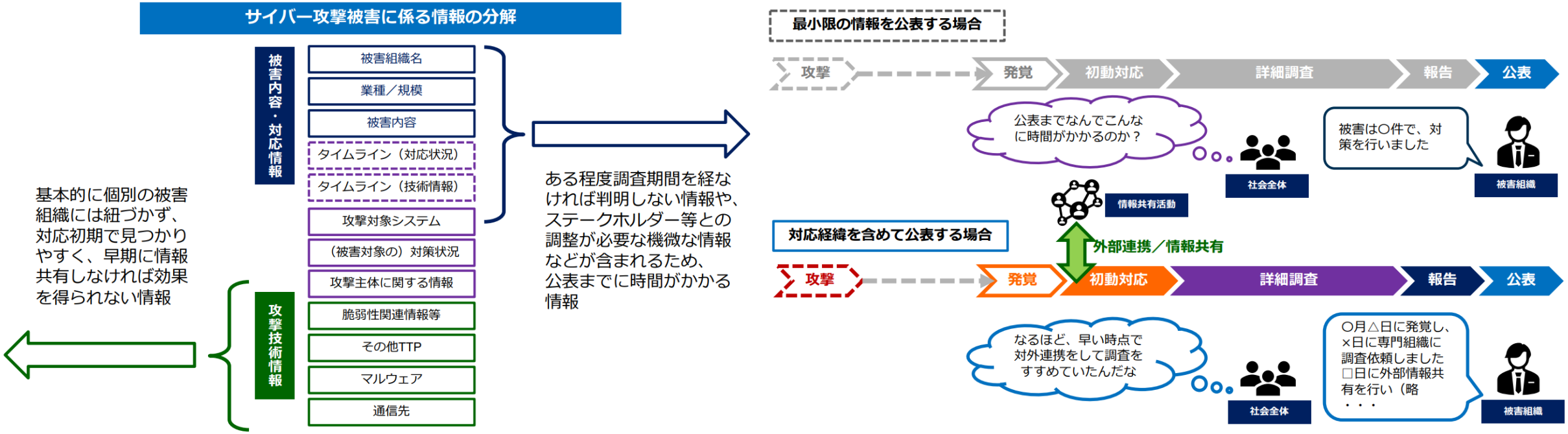


参照：経済産業省「サイバー攻撃に係る情報の共有・公表ガイダンス」
https://www.meti.go.jp/press/2022/03/20230308006/20230308006.html

2. どのような情報を共有するのか

機微な情報については配慮が必要であり、専門機関と調整を行う必要がある

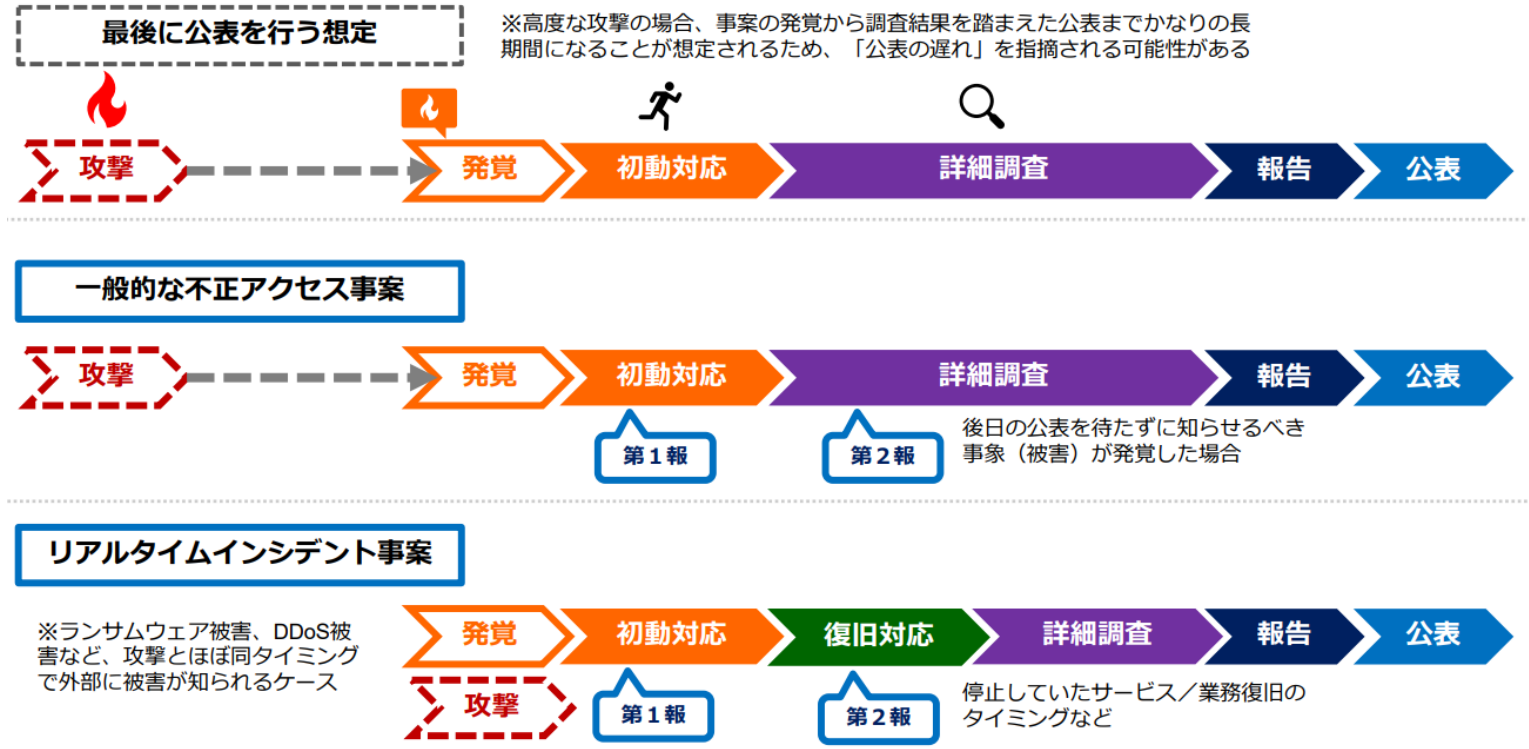
- 第三者の不利益になるような情報
- 未修整の脆弱性情報や「第三者の被害を示す情報」（被害企業を示すデータ等）



参照：経済産業省「サイバー攻撃に係る情報の共有・公表ガイダンス」
https://www.meti.go.jp/press/2022/03/20230308006/20230308006.html

3. どのようなタイミングで共有するのか

全ての調査を終えてから最後に公表を行うだけではなく、二次被害が発生する恐れや社会的にインパクトの大きな被害が判明した時点で、適宜第一報として公表を検討することが望ましい



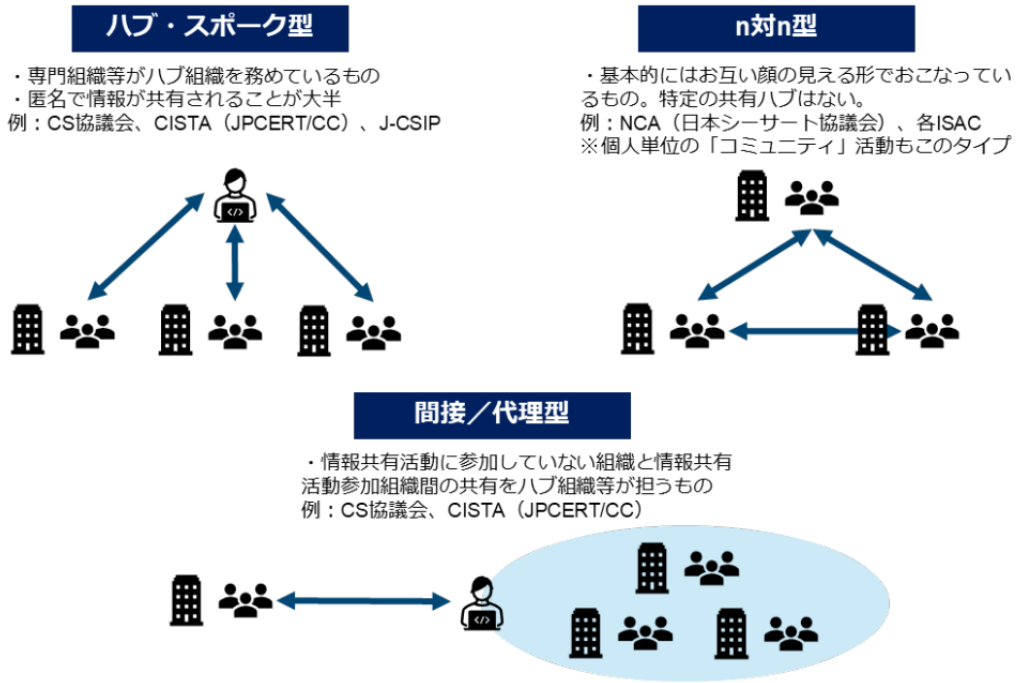
参照：経済産業省「サイバー攻撃に係る情報の共有・公表ガイダンス」
https://www.meti.go.jp/press/2022/03/20230308006/20230308006.html

4. どのような主体に対して共有するのか

攻撃技術情報の共有は、大きく分けて以下の3つの方法がある

- 参加している情報共有活動のハブ組織に情報提供をし、共有してもらう
- 参加している情報共有活動の参加者に対して、自らが提供する
- 情報共有活動とかかわりのある専門組織に情報提供し、共有してもらう

情報提供者や第三者の不利益にならないよう
配慮が必要であり、情報展開／共有先の
コントロールが必要になるため、基本的には
「情報共有活動」内で取り扱う



参照：経済産業省「サイバー攻撃に係る情報の共有・公表ガイダンス」
https://www.meti.go.jp/press/2022/03/20230308006/20230308006.html

5. まとめ

	情報共有	被害公表
タイミング	可能な限り早期のタイミング	ケースバイケース ※ 二次被害発生の恐れなどの注意喚起を目的とする速報が必要な場合は直ちに公表
被害内容・対応情報 • 被害組織名 • 被害業種／規模 • 被害内容 • 対応のタイムライン	–	○
中間の情報 • 攻撃のタイムライン • 攻撃対象システムについて • 脆弱性悪用の情報等	△ ※ 共有に必要なものは専門機関への相談等を踏まえて共有することが望ましい(共有しないほうが良い情報も)	○
攻撃技術情報 • マルウェア • 不正通信先 • その他攻撃手法に関する情報	○	△

参照：経済産業省「サイバー攻撃に係る情報の共有・公表ガイダンス」
https://www.meti.go.jp/press/2022/03/20230308006/20230308006.html

3-5. サイバーセキュリティを考慮した経営：情報セキュリティガバナンス

「ISO/IEC27014」(JIS Q27014)では、情報セキュリティガバナンスの目標として、以下の6項目を挙げている。

目標1: 事業体全体に対する包括的かつ統合的な情報セキュリティを確立する

目標2: リスクに基づくアプローチを用いて意思決定を行う

目標3: 取得(投資/購入/技術の採用/外部委託契約等)の方向性を定める

目標4: 内部及び外部の要求事項への適合性を確実にする

目標5: セキュリティを重視する文化を育てる

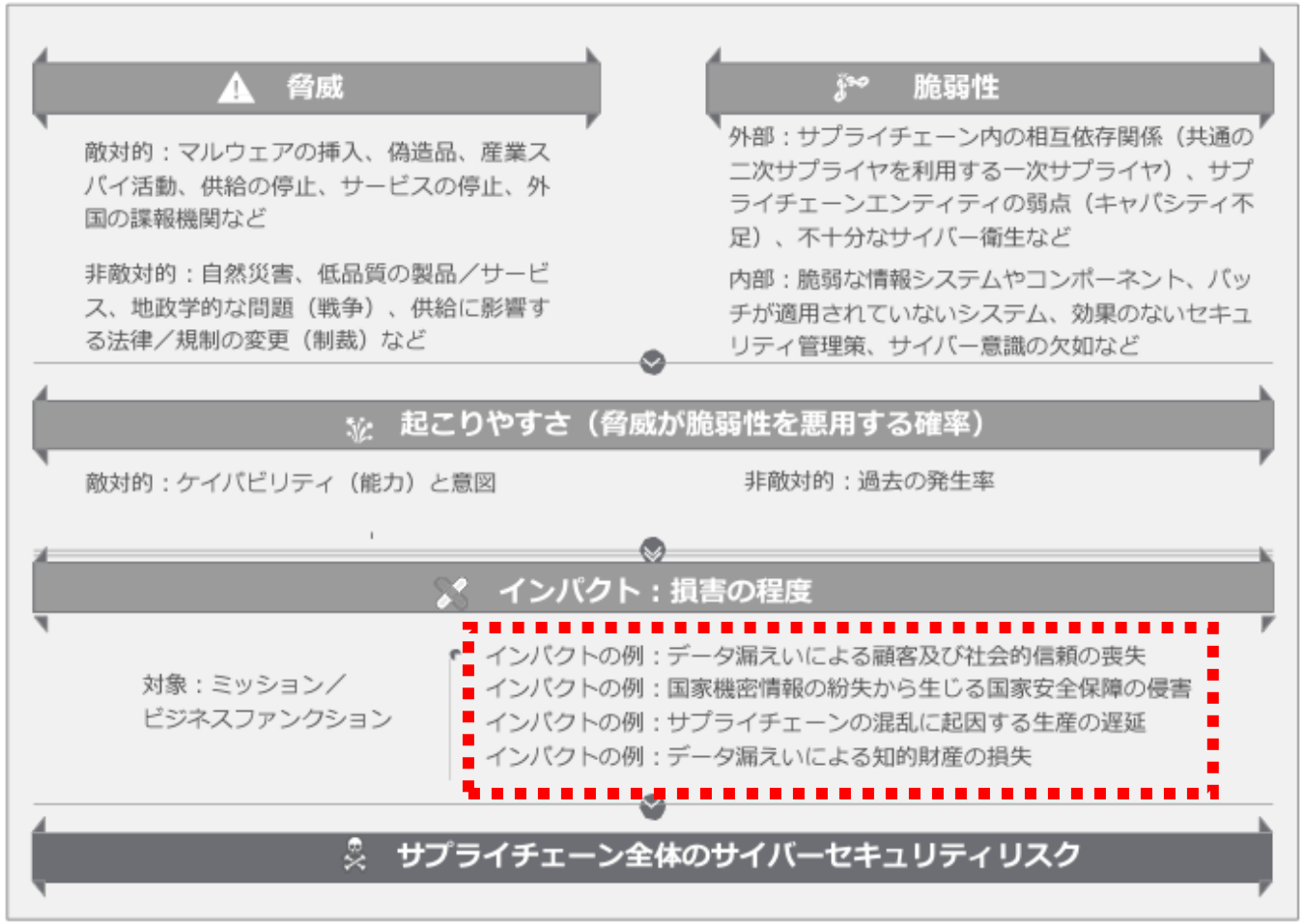
目標6: セキュリティのパフォーマンスが現在及び将来の事業体の要求事項を満たしていることを確実にする

1. サイバーセキュリティ経営ガイドライン Ver 3.0

サイバーセキュリティ経営の重要10項目	
サイバーセキュリティリスクの管理体制構築	(1) サイバーセキュリティリスクの認識、組織全体での対応方針の策定
	(2) サイバーセキュリティリスク管理体制の構築
	(3) サイバーセキュリティ対策のための資源(予算、人材等)確保
サイバーセキュリティリスクの特定と対策の実装	(4) サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
	(5) サイバーセキュリティリスクに効果的に対応する仕組みの構築
	(6) PDCAサイクルによるサイバーセキュリティ対策の継続的改善
インシデント発生に備えた体制構築	(7) インシデント発生時の緊急対応体制の整備
	(8) インシデントによる被害に備えた事業継続・復旧体制の整備
サプライチェーンセキュリティ対策の推進	(9) ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
ステークホルダーを含めた関係者とのコミュニケーションの推進	(10) サイバーセキュリティに関する情報の収集、共有及び開示の促進

参照：経済産業省「サイバーセキュリティ経営ガイドライン Ver 3.0」
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

2. サプライチェーンのサイバーセキュリティリスクマネジメント



【想定されるインパクト】
- 顧客および社会的信頼の損失
- 国家安全保障の侵害
- 生産(業務)の遅延
- 知的財産の損失

など

参照：システム及び組織におけるサプライチェーンのサイバーセキュリティリスクマネジメントのプラクティス
(Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations)
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/NIST.SP.800-161r1_JA_v1.1.pdf

4. チームディスカッション(10-15分)

全員で相談し「発表を行う人」と「情報をまとめるリーダー」を決め、ゲーム終了までのインシデント対応状況や報告状況を整理してください。またそれによって発生した被害などオリジナルの追加要素を決めてください。

発表者　　**リーダー**

整理する観点		ゲーム終了時点の対応状況		オリジナルの状況付与
インシデント対応状況	インシデント概要 (対応～復旧までの進捗)	現在までの状況 今後の方針	原因がまだ明確になっておらず、その他影響が未判明なので判明後まずは対策を迅速に実施して、サービスを再開させる予定。社内の脆弱性対策フローと対象機器の再確認を実施する。	
	被害状況とその対応	改ざん期間 漏えい被害 被害者への対応	時期不明(ログは半年保存) 漏えい内容・件数が大体判明 -	システム移行しているため、最長でも 24/8 から 被害者数1000件、クレジットカード情報なし (氏名、住所、性別、メールアドレス、購入履歴)
	攻撃と関連する技術情報	改ざん原因 その他調査 不正通信先	CMSパッチ未対策が原因 業者調査の調整中 どこの何が怪しいか不明	業者に調査を依頼する予定 調査完了予定は 1ヶ月後 業者に調査を依頼する予定
	対策・再発防止策	改ざん内容 対策状況 対策・再発防止	改ざん場所は推定したが詳細不明 対策パッチは一切実施してない -	CMS内に作られた偽入力ページの遷移と思われる 社内規則だとするはずになっていた 脆弱性対策に漏れた理由と対策をメインに考える
関連組織への報告、情報共有、公表		CISO には逐次状況報告を実施 所管省庁、個人情報保護団体へは初報を報告済み サプライチェーン報告は未実施		原因・その他影響調査の目途を報告予定 確報になり次第、再度報告予定 今後は web サイトにて経過報告する予定

4. チームディスカッションメモ(10-15分)

発表者		リーダー	

整理する観点		ゲーム終了時点の対応状況		オリジナルの状況付与
インシデント対応状況	インシデント概要 (対応～復旧までの進捗)	現在までの状況 今後の方針		
	被害状況とその対応	改ざん期間 漏えい被害 被害者への対応		
	攻撃と関連する技術情報	改ざん原因 その他調査 不正通信先		
	対策・再発防止策	改ざん内容 対策状況 対策・再発防止		
関連組織への報告、情報共有、公表				

4. チームディスカッション(10-15分)

例）

株式会社Example、〇〇〇です。
弊社オンラインサイトのコンテンツ改ざん被害に伴う情報漏洩が発生しました。
本日は、その事象および現在の対応状況、今後の対応方針についてご報告いたします。

弊社オンラインサイトが＜日付＞に改ざん被害を受け、＜期間＞の間の＜情報種類＞が漏洩しました。
対象となるアカウントは＜被害者数＞アカウントで、 ＜漏洩データ種別＞が漏洩しました。
本漏えいをきっかけとした二次被害についての報告は受けておりません。

現在の対応状況については、＜現在の対応状況＞という状況です。
今後のサービス再開に向け＜再発防止策＞などを実施し、社内体制の整備に努めます。

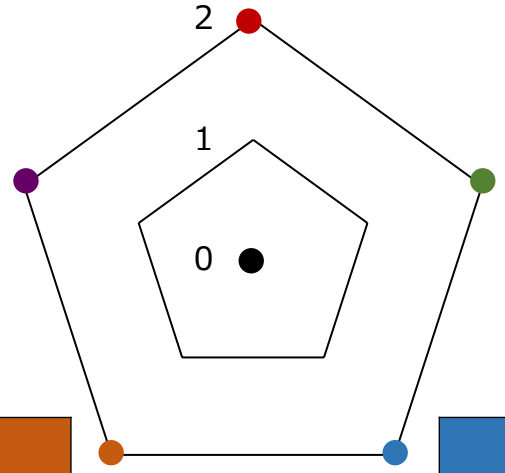
＜まとめの文言＞

以上、よろしくお願いいたします。

5. 発表・質疑応答（発表3分/質疑応答7分）

それでは、発表をお願いします。また、以下の観点を基に質疑応答を実施してください。

A. インシデント概要・対応状況の明確さ		
0点	1点	2点
何が起きたか 不明瞭	インシデント概要 のみ提示されている	発生原因、被害の 内容、対応進捗が 明示されている



E. 再発防止策の実現性		
0点	1点	2点
スローガンのみ	対策は明示するが 曖昧または考慮が 不十分	根本原因がわかり、 対策・体制・計画に 実現性が感じられる

B. 真実に基づく適切な判断		
0点	1点	2点
不正確な情報 または推測だらけの 情報	判明した情報が 一部正確に記載 されているが曖昧	事実を正確に述べ、 不明点は「未確認」 と明示している

D. 被害リカバリ施策		
0点	1点	2点
言及されていない または曖昧な表現	十分な説明に加え、 適切な補償について 言及されている	十分な説明に加え、 補償の具体策・ 期日、窓口を明示

C. ステークホルダーへの配慮		
0点	1点	2点
全てのステークホル ダーへの対応がどこか 不足している	一部のステークホル ダーにのみ配慮して 対応している	規制当局・顧客・従 業員・投資家全てに 配慮し対応している

5. 発表・質疑応答（発表3分/質疑応答7分）

ステークホルダーごとに評価する視点としては以下を参考にしてください。

グループ	第一の関心事	聞きたい具体的内容	A 概要・対応の明確さ	B 真実に基づく判断	C ｽﾃｰｸﾎﾙﾀﾞｰ配慮	D 被害リカバリ施策	E 再発防止の実現性
所管省庁 規制当局	法令順守 報告期限 サービス影響	影響範囲 通知済み/予定日 技術的対策		○	○	○	○
顧客 利用者	個人情報保護 サービス継続	何が漏れたか、被害に係る補償 対応誠意(通知までの時間など) サービスの利用再開時期			○	○	
株主 投資家	財務状況 被害影響 経営責任	直接/間接損失 再発防止への投資額 ガバナンス変更点	○	○	○	○	○
従業員	雇用と安全 業務影響	内部調査の有無 社内支援窓口・問い合わせ先 業務影響			○	○	

6. 講評

ファシリテータから、皆様の発表について簡単にコメントします

7. 終わりに

セキュリティ専門家人狼、Malware Containment 好評発売中！

講演資料やゲーム進行の参考資料、購入はこちら：http://www.jnsa.org/edu/secgame/

セキュリティ専門家人狼

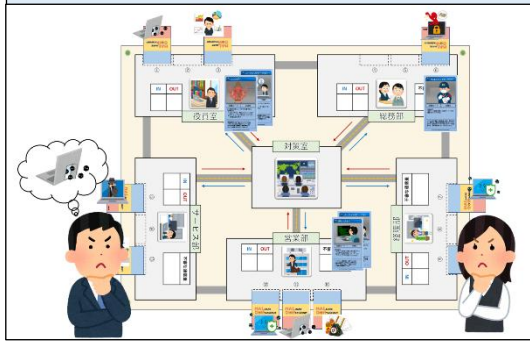
「人狼ゲーム」のセキュリティ版。

CSIRT陣営と犯罪者陣営に分かれ、内部不正の手口(ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞ)とと傾向(不正行為者のﾌﾟﾛﾌｧｲﾘﾝｸﾞ等)、その対策(SCP状況的犯罪防止理論等)を学ぶことができます。

ハッシュタグ… #セキュ狼

4000円

Malware Containment



インシデントの初動対応におけるロールプレイを学ぶゲームです。

ゲーム参加者は CSIRT となり、割り振られた役職の能力を駆使して、社内で発生したインシデント対応の初動対応を行います。

ハッシュタグ… #Malcon

4000円

※ 価格は 2025年5月時点の情報です。

ゲームファシリテーター、派遣致します

既にゲームを購入したが演習の進め方や効果的なゲーム演習ができない、学校の授業や、同好会部活等でゲーム演習をしてみたいなどにお答えします。お気軽にお声がけください。
派遣対象組織：学校(大学・大学院、高専、専門学校、高等学校等)、
NPOや社団法人等の団体、コミュニティの勉強会等

※ 誠に申し訳ありませんが、企業への派遣は実施しておりません
※ 交通費・宿泊費などのご負担をお願いします、また少額で結構ですので謝金をご用意いただけると助かります