NISC National center of Incident readiness and Strategy for Cybersecurity

サイバーセキュリティを取り巻く現状と政府の取組

内閣官房 内閣サイバーセキュリティセンター 副センター長
中溝 和孝

2024年「サイバーセキュリティ月間」

- 毎年**2月1日から3月18日**を「**サイバーセキュリティ月間**」に設定。 産官学民を巻き込み、幅広い年齢層に向け、サイバーセキュリティに関する**普及啓発活動を集中的に実施**。
- 2010年より、毎年2月を「情報セキュリティ月間」として発足。2015年「サイバーセキュリティ月間」と改名、2024年で**15回目の開催**
- 日米豪印の４か国、いわゆるQUAD(クアッド)の取組である「サイバーチャレンジ」をはじめ、国際社会とも連携。

普及啓発・情報発信

●**官房長官からのビデオメッセージ**
月間開始日（2/1）に発信

●**月間コンテンツ等の作成**
○デジタルサイネージ等
『王林』さんを起用しポスター・サイネージ・周知用動画を制作
ポスターは関係機関・主要駅等に配布

ポスター

○普及啓発用動画
IPA 10大脅威 個人編の
フィッシング、サポート詐欺を深掘り
一般国民に向け、SNS等で周知

○月間特設ページ（NISCポータルサイトにて公開）
コラムや月間関連イベント等の特別コンテンツを掲載
コラムのテーマ：サイバーセキュリティを支える人々
～未来のサイバーセキュリティ人材を育てる

●**公式SNSでの情報発信**
NISC公式Xアカウントでの情報発信

イベント

●**キックオフイベント（2/1（木））**
月間開始日にキックオフイベントを開催

●**経営層向けセミナー（3/14（木））**
「経営者のためのサイバーセキュリティ戦略：
リスクを軽減し、サプライチェーンを守る」
組織内体制整備やサプライチェーンリスク等、経営層を対象とした政府機関・関係団体等による講演を予定。
（会場・オンラインのハイブリッド開催）

●**NISC-CTF（Capture The Flag）の開催**
大臣による表彰を予定。
各府省庁・独法等の職員がサイバーセキュリティに関する幅広い技術・能力を競う。

●**月間関連イベント**
産学官民の普及啓発・人材育成等のイベントを集約・発信。各府省庁とも連携・

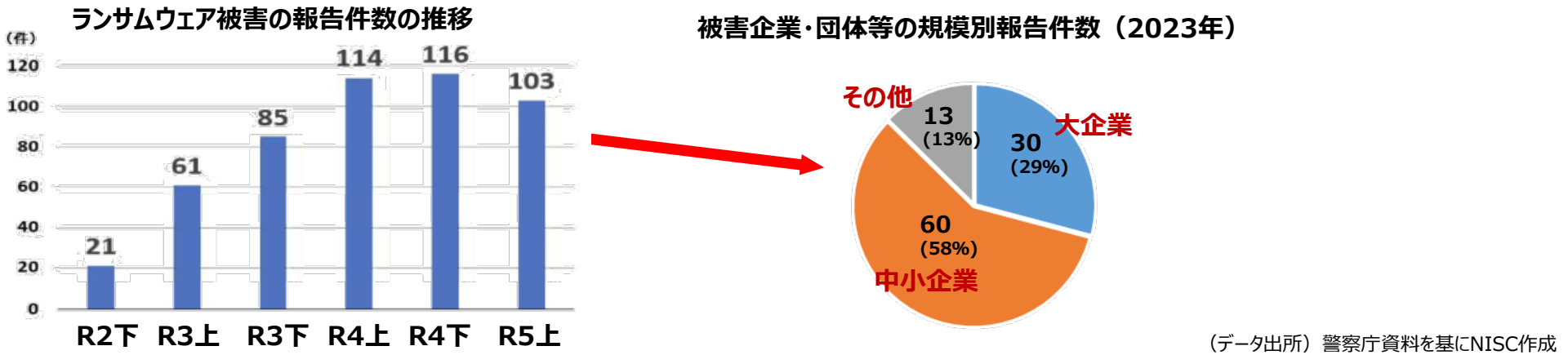
最近のサイバー関連の動き

		主なサイバーインシデント	主なセキュリティ政策動向
2022年	10月	大阪府内の総合医療機関におけるランサムウェア攻撃事案	
	12月		国家安保戦略等３文書の閣議決定
2023年	５月	広島市サイトの閲覧障害事案	（Ｇ７広島サミット）
	７月	中部地方の港湾におけるコンテナターミナルのシステム障害	「サイバーセキュリティ2023」「政府統一基準群の改定」「重要インフラの安全基準等策定指針の改定」のサイバーセキュリティ戦略本部決定
	８月	福島市サイトの閲覧障害事案 内閣サイバーセキュリティセンター（ＮＩＳＣ）のメールシステムへの不正通信事案	
	９月	Black Techのサイバー攻撃に対する日米合同アドバイザリー（注意喚起）	
	10月		「セキュアバイデザイン・セキュアバイデフォルトに関する文書」のサイバーセキュリティ戦略本部決定・NISC共同署名
	11月	JAXAが不正アクセスを公表	「セキュアAIシステム開発ガイドライン」の内閣府科技イノベ・NISC共同署名

ランサムウェアによる被害拡大、最近の主なインシデント

ランサムウェア

- 2022年に全国の都道府県警察から警察庁に報告があった件数は**230件**であり、前年と比較し、**約1.5倍に増加**。2023年上半期は103件であり、ほぼ横ばいで推移。
- 被害件数(103件)の内訳は、**大企業が30件（29%）**に対して、**中小企業は60件（58%）と過半数**。



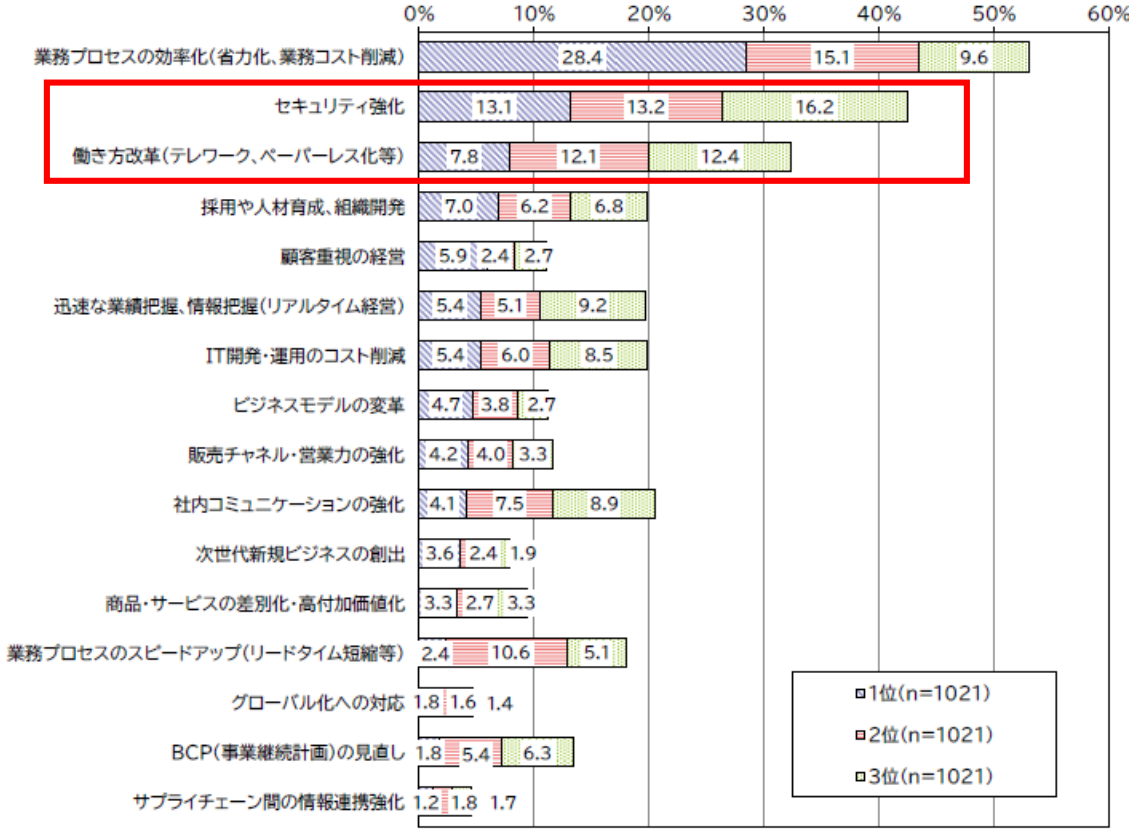
（データ出所）警察庁資料を基にNISC作成

- 2022年10月、大阪市内の総合病院がランサムウェア攻撃を受け、電子カルテシステムに障害が発生。電子カルテが閲覧できない事態となり、一時急患以外の診療を停止するとともに、新規外来患者の受入れを停止。
- 2023年7月　中部地方の港湾がランサムウェア攻撃を受け、コンテナの積み下ろし、搬入・搬出等を一元的に管理するシステムが３日間停止し、船舶の荷役スケジュールやコンテナの搬入・搬出等に大きな影響を与えた。

企業の傾向

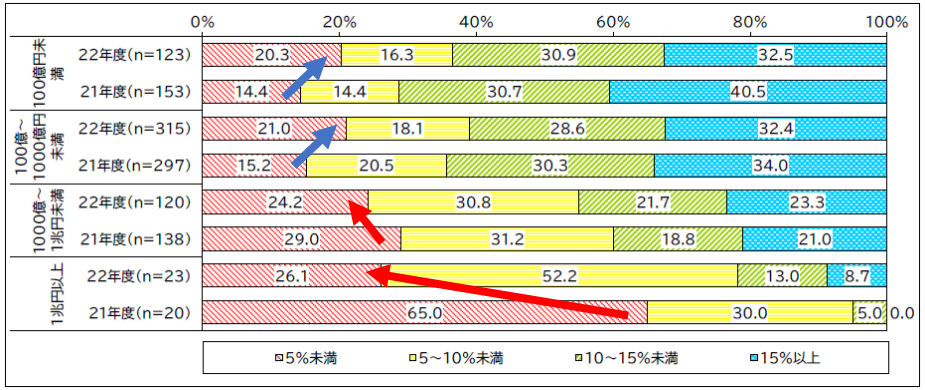
- IT投資で解決したい短期的な**経営課題として「セキュリティ強化」が高い伸び**（「働き方改革」を抜いて2位。前年度調査から順位が逆転）
- IT予算に占める情報セキュリティ関連費用の割合は、**売上高1000億円未満は減少、売上高1000億円以上は増加**しており、新型コロナや地政学的リスクなどによる不安定な情勢や先行き不透明な経済状況を受けて、情報セキュリティへの投資が企業の売上高規模によって二極化
- 大きな脅威として警鐘が鳴らされている「サプライチェーンの弱点の悪用（委託先へのなりすまし等）による被害」は「特に対策を実施・見直ししていない」と回答したのが69.1%と、対策状況はまだまだ十分ではない。

■IT投資で解決したい短期的な経営課題（1位・2位・3位）



［出典］　（一社）日本情報システムユーザー協会「企業IT動向調査報告書 2023」より、NISC作成

■売上高別 IT 予算に占める情報セキュリティ関連費用の割合

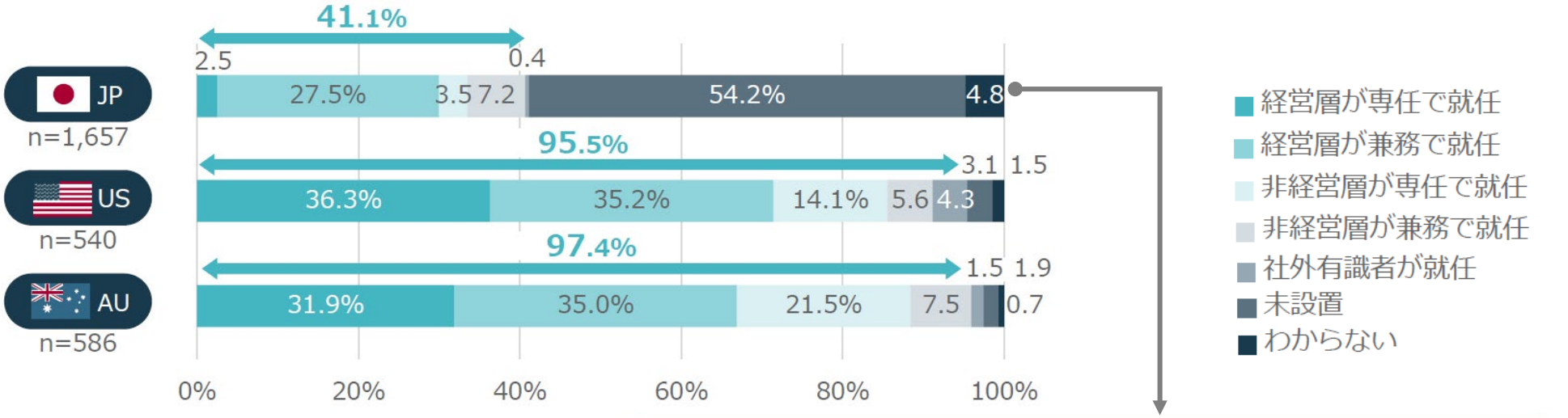


■（過去1 年間）情報セキュリティインシデント 対策の実施・見直し状況

	セキュリティ商材の追加や強化	監視体制強化	復旧手順明確化	業務プロセスの見直し	想定訓練の実施	特に対策を実施・見直ししていない
Webサイト等を狙ったサイバー攻撃(改ざんなど)(n=986)	19.9	20.5	4.1	4.0	6.3	56.8
インターネットサービスからの個人情報等の搾取(n=936)	16.2	18.7	2.6	4.4	8.2	59.4
インターネットサービスへの不正ログイン(n=947)	17.6	23.4	2.7	4.6	6.1	56.0
工場など制御系システムへのサイバー攻撃(n=769)	11.1	13.8	4.2	2.9	4.3	71.3
ランサムウェア感染による脅迫等の被害(n=1007)	26.8	21.0	9.3	4.8	20.5	38.5
標的型攻撃(メール添付ウイルス等による攻撃)による被害(n=1015)	25.4	22.3	5.0	3.9	33.8	31.1
サービス妨害(DoS)攻撃によるサービス停止(n=987)	13.6	20.3	4.4	2.0	4.1	64.0
ビジネスメール詐欺等による不正送金などによる被害(n=1012)	13.3	17.0	2.8	5.5	25.2	48.4
内部不正や不注意による情報漏洩(n=1012)	11.9	22.4	3.4	10.8	11.6	51.3
IoT機器(情報家電、オフィス機器等)の脆弱性を利用した攻撃(n=876)	7.4	12.7	2.2	3.2	3.0	76.1
サプライチェーンの弱点の悪用(委託先へのなりすまし等)による被害(n=930)	6.8	13.5	2.0	6.2	10.1	69.1
テレワークで利用するシステムの脆弱性を利用した攻撃(n=971)	20.3	20.4	2.8	5.6	6.4	56.2

■ 米国と豪州のCISOの設置状況は90%を超えているのに対して、日本は従業員１万人以上の場合は約60%であるものの、全体を見た場合、半分に満たない状況。

■CISO（情報セキュリティを統括する人材）の設置状況

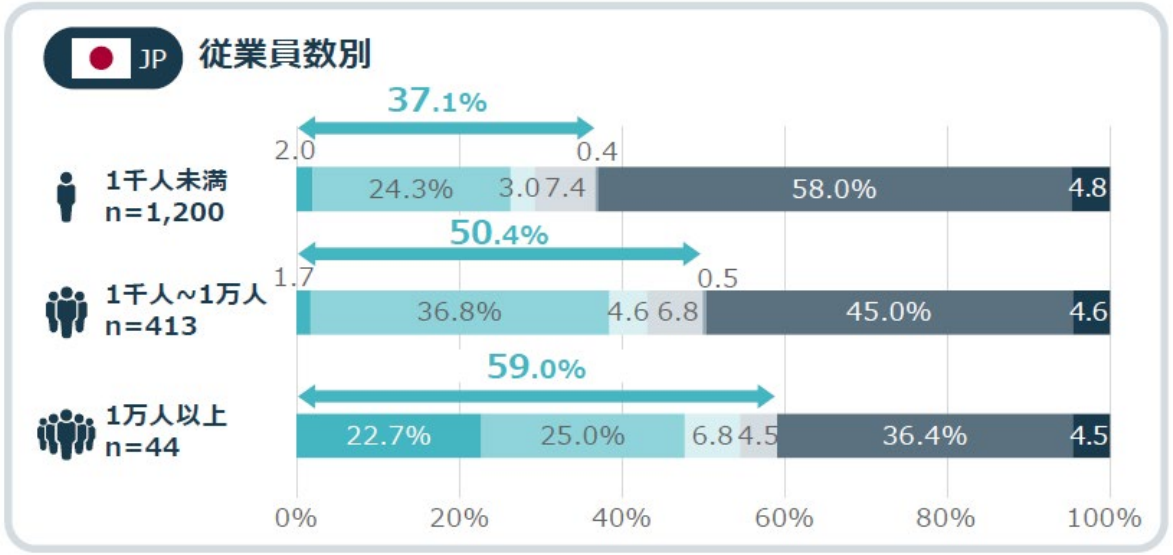


CISOの設置状況

US AU 約97%

従業員1万人以上の日本企業 CISOの設置状況

JP 約60%



[出典] NRIセキュアテクノロジーズ㈱「NRI Secure Insight 2023」（2024年1月）

政府統一基準群の改定の概要（令和5年7月４日サイバーセキュリティ戦略本部決定）

- 政府統一基準群（※）は、サイバーセキュリティ基本法に基づく、政府機関及び独立行政法人等の情報セキュリティ水準を維持・向上させるための統一的な枠組み。（※）統一規範、統一基準、ガイドラインで構成される文書群をいう。
- **サプライチェーンの脆弱な部分を起点としたサイバー攻撃によるリスクが増大していることを踏まえた業務委託先に求める対策**やソフトウェアに係る対策の強化（定期的な設定の確認等）、最新のDDoS攻撃の特徴を踏まえたサーバ装置の冗長化等のDDoS対策の強化を盛り込む等、昨今の状況を踏まえた見直しを行うもの。

【「政府統一基準」改定のポイント】

第４部 外部委託 （※「業務委託」及び「クラウドサービスの利用」）

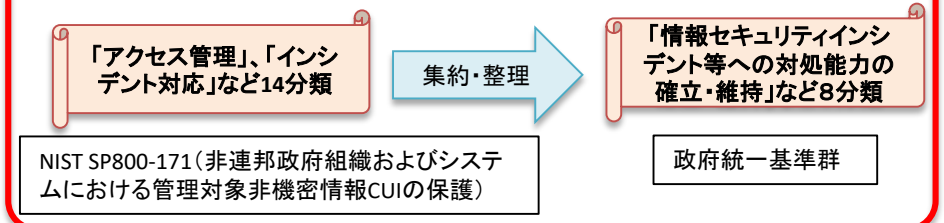
- 業務委託（例 情報システムの保守の委託）の委託先に求める対策の明確化
  - 委託先に担保させる具体的なセキュリティ対策（情報へのアクセス制御、ログの取得・監視など）を追加
- クラウドサービス利用時のセキュリティ対策の明確化
  - 調達時にISMAPクラウドサービスリストから選定することを明記

第６部 情報システムの構成要素・第７部 情報システムのセキュリティ要件

- ソフトウェアの利用時の対策の強化
  - 重要なソフトウェアの設定手順の整備やシステム担当者への教育、定期的な設定の確認等のソフトウェアのセキュリティ水準を維持するための対策を強化
- 脅威・技術動向を踏まえての対策の強化
  - テレワーク環境など厳格な主体認証が必要な場合において、多要素認証方式（パスワード＋生体認証など）を必須化
  - 昨今のサービス不能攻撃（DDoS）を踏まえ、専用の対策装置やサービス導入、サーバ装置や通信回線等の冗長化等の対策を必須化
  - ゼロトラストを実装するため、アクセス元の信頼度に応じたアクセス制御「動的なアクセス制御」を追加

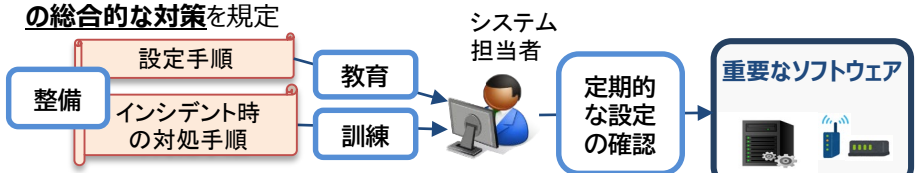
＜業務委託の委託先に求める対策＞

委託先に求める対策の明確化・・・**米国NISTのサプライチェーン対策を参考**に委託先に担保させるべき情報セキュリティ対策を例示



＜ソフトウェア利用時の対策の強化＞

統合的な主体認証管理などの**情報システムを制御する上でセキュリティ上重要な機能を有している重要なソフトウエア**について、**セキュリティ水準を維持するための総合的な対策**を規定



＜サービス不能攻撃（DDoS）対策の強化＞

サービス不能攻撃対策のための専用装置等の導入、サーバ装置等の冗長化等

政府機関が業務委託先に実施を求める情報セキュリティ対策

- 政府統一基準改定において、政府情報の適切な取扱いのため業務委託先に求める情報セキュリティ対策の事項を明確化。
- 情報セキュリティ対策の事項は、米国国立標準技術研究所（NIST）が公表しているガイドライン（SP800-171）（※）を参考に、14項目ある基準の類似のものを統合して8項目を規定し、米国では項目毎に詳細に規定されている必須の要件については柔軟な対応がとれるよう我が国ではガイドラインとして記載。
  （※）米国防省が全世界の取引先に対して準拠を求めている調達から販売・供給までの一連のサプライチェーンに存在する、業務委託先や関連企業のすべてが準拠すべきセキュリティ基準。
- 今後、各府省の調達において、委託先に求める要件としてこれらを契約に含めることとなる。

基本対策事項4.1.1(3)-1（８項目）	実施内容の概要		SP800-171の関連条項（14項目）
a) 情報セキュリティインシデント等への対処能力の確立・維持	**インシデントの予防、万一の発生時に的確な対処** • インシデント対処体制及び報告フロー等の概要について、説明ができる　など	←	○ インシデント対応
b) 要保護情報へアクセスする主体の識別とアクセスの制御	**必要な者だけが情報にアクセスできる** • 主体やその属性ごとにアクセス制御、管理者権限は必要最低限の権限と利用に制限するなど	集約	○ アクセスコントロール ○ 主体識別と認証
c) ログの取得・監視	**インシデント兆候の検知・分析、証跡の確保** • 取得したログ情報やその分析内容に応じて、不正アクセス等への対応を取る　など	←	○ 監査と説明責任
d) 要保護情報を取り扱う機器等の物理的保護	**適切な物理的管理策** • 委託事業の実施場所において、鍵管理や入退室記録等の入退管理対策を行う　など	集約	○ メディアの保護 ○ 物理的保護
e) 要保護情報を取り扱う要員への周知と統制	**適切な人的管理策** • 業務遂行に必要な情報セキュリティに係る訓練等を確実に受講させる　など	集約	○ 意識啓発と訓練 ○ 要員のセキュリティ
f) セキュリティ脅威に対処するための資産管理・リスク評価	**セキュリティ対策の前提となる資産の識別、リスクの評価** • 定期的及び重大な脆弱性の公表時の脆弱性スキャン、適時な脆弱性対策　など	集約	○ 構成管理 ○ メンテナンス ○ リスクアセスメント
g) システム及び情報の完全性の保護	**適切な技術的管理策** • 定期的な検索等によりシステムの欠陥を適時に検出し是正する　など	集約	○ システムと通信の保護 ○ システムと情報の完全性
h) セキュリティ対策の検証・評価・見直し	**対策の有効性の評価、定期的な見直し** • システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施する　など	←	○ セキュリティアセスメント

「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の背景

【重要インフラ事業者等における対策等の状況】　（出典）NISC「重要インフラにおける安全基準等の浸透状況等に関する調査について」［2022年度］

- サイバーセキュリティに関する基本方針を策定している：91.7%
- **サイバーセキュリティリスクが経営のリスクと認識され、セキュリティ方針の策定に経営層が関与している：67.4%**
- CISOを設置している：82.8%
- リスクアセスメントを実施している：72.6%
- 事業継続計画を策定している：77.2%
- **バックアップデータから復旧確認をしている：31.2%**
- クラウドサービスを利用していない：7.7%

⇒ **「重要インフラのサイバーセキュリティに係る安全基準等策定指針」を改定**
（2023年7月4日サイバーセキュリティ戦略本部決定）

背景	現行指針	改定指針のポイント
○サイバー攻撃やシステム障害が重要インフラの**事業経営に影響を及ぼす**ものに変化。	○経営層のコミットメント等を含めた情報セキュリティ方針を策定。	○経営方針にセキュリティ確保を組み入れるとともに、**経営層に相当する者の中からCISO等を任命することを推奨**。
○デジタル化の進展等に伴い、**取引先等を経由したサイバー攻撃**が発生。	○サプライチェーンとの依存関係を把握し、リスクアセスメントを実施。	○取引先等の対策状況も踏まえたリスク評価の実施。**取引先との契約を通じた、サプライチェーンリスク対策の確保**。
○ランサムウェア攻撃等のサイバー攻撃や、クラウドサービス等のサプライチェーンにおけるシステム障害による**復旧が長期化**。	○サイバーセキュリティに関する事業継続計画等を策定し、復旧対応、情報共有等の体制を整備。	○**ランサムウェア対策として、バックアップからの復旧確認を定期的に実施**する必要性を明記。

「重要インフラのサイバーセキュリティに係る安全基準等策定指針」の概要

令和5年7月4日サイバーセキュリティ戦略本部決定

- 重要インフラ事業の防護に関し、サイバーセキュリティ基本法に基づき、官民共通の計画である「行動計画」を策定・改定。さらに同計画を踏まえて、「安全基準等策定指針（※）」を策定。

  （※）重要インフラ所管省庁等が分野ごとに策定する「安全基準等」の中に盛り込むことが望まれる項目を整理・記載した指針。

- サイバーインシデントが重要インフラの事業経営へ与える影響の拡大や、取引先等を経由したサイバー攻撃の発生等を踏まえ、「安全基準等策定指針」を改定。
  - 組織統治に関するセクションを新設し、**事業の継続・信頼といった経営の視点から経営層がサイバーセキュリティリスクを管理する体制の整備を促進**
  - 委託先等との契約を通じた実効性の確保により**サプライチェーンリスク対策**を強化
  - **バックアップのネットワークからの隔離等、ランサムウェア対策、クラウドサービス利用に係る対策等**を強化

【「安全基準等策定指針」改定のポイント】

1. 行動計画を踏まえた見直し

- 組織統治に関するセクションを新設
  - 組織方針（経営方針、リスクマネジメント方針等）に当たる文書に、重要インフラのサイバーセキュリティ確保に関する事項も組入れ
  - サイバーセキュリティに関するリスク及びそれが業務運営に及ぼす影響を経営層が理解し評価できる体制を整備
  - 組織全体の監査の一部としてサイバーセキュリティに関する監査を実施　等
- リスクマネジメントの活用・危機管理に係る事項を追記
  - サプライチェーン・リスクマネジメントを実施し、事業者間の契約を通じてその実効性を確保
  - 組織状況と資産を把握し、任務保証の考え方に基づくリスクアセスメントを実施（特に、事業被害シナリオを活用したリスク分析を推奨）　等

2．最近の動向を踏まえた追記

- ランサムウェア対策、クラウドサービス利用に係る対策等を追記

＜経営層がサイバーセキュリティリスクを管理する体制の整備＞
- リスクマネジメントの方針として、「情報システム及び情報を活用する事業、事業者としての信頼、その他の経営リスクについて、サイバーセキュリティを確保できないことによってどのような影響を受けるのか」との視点から実施する旨を追記。
- サイバーセキュリティに関する責任者（CISO等）を任命すべきであり、その任命に当たっては、経営層の責任において実施する旨を追記。
- 監査に当たり、新たに脆弱性診断、ペネトレーションテスト等の実施を推奨。

＜サプライチェーンリスク対策の強化＞
- ①不正機能等の埋め込み、②サービスの供給途絶、③外部サービスにおける情報の不適切な取扱い、④海外拠点、グループ組織、取引先等を経由したサイバー攻撃等の脅威に対応。
- 直接の供給者を対象に、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化する旨を追記。

＜ランサムウェア対策の強化＞
- バックアップからの復旧確認を定期的に実施する必要性を明記。
- バックアップに当たり、ネットワークからの隔離について追記。

＜クラウドサービス利用に係る対策の強化＞
- 情報公開等の設定確認や、ステークホルダーとの障害対応体制の構築について追記。

3月公開

事例で学ぶサイバーリスクマネジメント　～経営トップがすべきこと 実践編～

https://security-portal.nisc.go.jp/guidance/executives2/index.html

視聴しやすい動画で、サイバーセキュリティ対策への具体的なアクションの要諦を伝える

サイバーセキュリティの重要性を意識し、経営テーマに盛り込みたいと考える経営層が、具体的なアクションを起こす際に必要となるノウハウが習得できる動画を提供

本動画の特徴

- 経営者の立場での悩み・解決策に特化
- 事例を中心とした納得感ある内容
- 短時間の視聴しやすい動画講座

自社だけでなく「事業」を守る：強靭なサプライチェーンの構築

- サプライチェーンのサイバーセキュリティを高めることは、自社の被害を防ぐだけではなく、自社がサプライチェーン上の他社に対する被害の原因になるリスクを低減させるためにも大切
- 脆弱な箇所の把握、協働体制の構築といった対策のポイントを解説

強固なセキュリティを体現する企業風土の醸成

- 3月中公開予定

経営層向けセミナー

- 企業経営者は日々、様々なリスクに相対しており、サイバーセキュリティのリスクも、そのうちの最重要事項のひとつ。
- 企業を狙うサイバー犯罪は年々高度化しており、機密情報漏えいやランサムウェア被害などのセキュリティインシデントが起こると企業の業種・規模に関わらず、事業継続性や企業価値の低下に繋がる。これらのリスクに対抗するには経営層の積極的なサイバーセキュリティの理解と組織的な取組が重要。

名だたる専門家のご講演を通して、
経営層を含めた皆様に知っておいていただきたいポイントをご紹介

- 経営課題としてのサイバーセキュリティと法律実務
- サイバーインシデントの実例とその背景
- サイバー攻撃と事業継続セキュリティ人材事業
- サイバーセキュリティ人材と強化の取り組み

本セミナーをお楽しみいただき、
さらなるサイバーセキュリティの向上へ！