AMT/NEWSLETTER
Cyber & AI Security

2026 年 11 月 20 日

内閣官房、サイバーセキュリティに関する関係閣僚会議（第 2 回）「サイバーセキュリティに関する緊急対策パッケージ」を公表

弁護士 清水 亘 / 弁護士 髙橋 麟太朗 / 弁護士 田中 滉大

Contents

Ⅰ. はじめに

Ⅱ. 背景

Ⅲ. 概要

Ⅳ. 主なポイント
1. 個人データの最小化と安全管理の強化
2. 安全な本人確認の徹底
3. 委託先管理・システム関連契約
4. インシデント対応と官民連携
5. 二次被害の防止

Ⅴ. まとめ

Ⅰ. はじめに

内閣官房、サイバーセキュリティに関する関係閣僚会議（第 2 回）は、2026 年 11 月 6 日、「サイバーセキュリティに関する緊急対策パッケージ」（以下「本パッケージ」という。）を公表した[1]。

本パッケージは、早期に実施または着手できる施策を中心に、4 つの柱の下に取りまとめたものである。また、本パッケージは、AI 時代にふさわしいサイバーセキュリティの在り方へとわが国を移行させていく出発点であると位置付けられている。

本稿では、公表資料（概要・本文・施策一覧）をもとに、法律実務に関係の深い点を中心に速報として紹介する。

1 内閣官房「サイバーセキュリティに関する関係閣僚会議（第 2 回）（2026 年 11 月 6 日）
https://www.cas.go.jp/jp/seisaku/cybersecurity_kakuryokaigi/dai2/gijishidai.html

II. 背景

近時、サイバー攻撃による不正アクセスや情報漏えいの事案が相次ぎ、国民生活や企業活動に大きな不安と影響が生じている。本パッケージによれば、昨今の漏えい事案には、既知の脆弱性の放置、ウェブサイト等の設定不備、アプリケーション開発時のセキュリティ対策の不足など、自らの組織や委託先における基本的な対策が十分でなかった事例が多くみられる。さらに、本パッケージは、AI の進展により、こうした隙が短時間かつ大規模に突かれる時代となっていると述べ、サイバーセキュリティは日本社会全体で対応すべき課題であるとしている。

サイバーセキュリティに関する関係閣僚会議（第 2 回）の参考資料によれば、日本では、特に 2026 年 10 月に、重要インフラ事業者からの報告件数や個人情報保護委員会への報告件数が急増した。攻撃者は、インターネット上に公開されている日本のウェブサイト等を標的に大規模な調査を行い、侵入方法が見つかったウェブサイト等に侵入して個人情報を窃取したとみられている。また、標的の調査や侵害に「AI を使用している可能性も高い」とも評価されている。

III. 概要

本パッケージが目指すのは、あらゆる組織が基本的な対策を当たり前に講じることで被害を予防することができ、仮にサイバー攻撃による被害が生じたとしても、官民が攻撃の情報を共有していち早く対処し、迅速に支援を受けて立ち直ることができる世界最高水準のサイバーレジリエンスを確保した社会である。

本パッケージの施策は、次の 4 つの柱で構成されている。

① AI も活用した基本的な対策の徹底
② 情報収集・集約、捜査・分析体制の強化
③ サイバー攻撃への対処の戦略的な実施
④ 被害者支援・被害拡大防止策の強化

また、本パッケージ全体の考え方として、情報の集約・分析と、その結果の対策への活用という循環を作ることで社会全体のサイバー対処能力の向上につなげることが示されている。

そして、本パッケージは、上記の施策と併せて、次のような中長期的な課題についても検討を深めるとしている。

- 情報収集の在り方を含む制度面の整備
- 政府の基準の見直し
- ベンダとその契約事業者のシステム関連契約の在り方の周知
- 高性能 AI のサイバー攻撃への悪用や量子技術の進展など、将来の脅威への備え

IV. 主なポイント

本パッケージの主なポイントは、次のとおりである。

1. 個人データの最小化と安全管理の強化

個人情報保護委員会は、2026 年 10 月 7 日、保有する個人データの必要性の確認と不要なデータの消去について注意喚起を行った。今後の予定は次のとおりである。

- 本人確認等のために取得した画像等の「保存期間・保存方法などに関する基本ルール」について、令和 8 年度中に業種ごとの注意喚起等を検討する。
- 安全管理措置に関するガイドラインについて、全項目の「手法の例示」の改正を加速し、2027 年（令和 9 年）1 月中の施行を目指す。

・　報告された漏えい等については、個人情報保護法上の問題点がみられた場合には、厳格に指導・助言等の監視・監督権限を行使する。

2. 安全な本人確認の徹底

運転免許証の画像による本人確認については、「国民が不安を感じている」とされている。そのため、マイナンバーカード等の IC チップの読取による「安全かつ確実な本人確認」の利活用場面を広げる方針である。

また、流出した個人情報を悪用したなりすましによる口座開設等を防ぐため、取引事業者に対し、犯罪収益移転防止法等に定められた本人確認の徹底を要請するとしている。

3. 委託先管理・システム関連契約

「サプライチェーン強化に向けたセキュリティ対策評価制度」（SCS 評価制度）が令和 9 年（2027 年）3 月から開始される予定であり、企業の委託先管理手法として推奨されている。また、「★」を取得した企業が攻撃を受けた場合には、国家サイバー統括室から「★」取得企業に対して関係情報を求めることができる仕組みも導入される予定である。

4. インシデント対応と官民連携

本パッケージによれば、事案の段階に応じて、次の体制が整備されるべきである。

段階	主な体制
潜在的な被害のおそれがある組織に国家サイバー統括室から能動的に接触する場合	「アウトリーチ・チーム（仮称）」を 2026 年 11 月中に新設
政府による支援の必要性が特に認められる場合	「官民サイバー救援隊（仮称）」を整備

段階	主な体制
国民の生命、身体または財産に対する重大な危害が現に発生しまたはそのおそれが大きい事案であって、わが国の安全保障や社会経済に重大な影響を与える場合	被害組織の同意を得て派遣する「ジョイント・レスポンス・チーム（仮称）」

（筆者らが作成）

なお、警察[2]には、ログの保全等の初期対応を担う「ファスト・フォレンジック・フォース（仮称）」が新設され、所管企業等に対しては、通報やログ等の証拠の提供について要請が行われる。また、全都道府県警察には、「法人専用相談・通報窓口 サイバー被害 110 番（仮称）」が開設される予定である（令和 8 年中）。攻撃の基盤に対しては、「アクセス・無害化措置」を含むあらゆる手段を戦略的に選択・実行するとされている。

2 警察庁は、令和 8 年（2026 年）11 月 6 日、「企業等を対象とする高度な技術を悪用した不正アクセス行為に起因する 大規模な個人情報等の流出事案に係る警察庁長官の指示について」を公表している。
https://www.npa.go.jp/news/release/2026/20261106news.pdf

5. 二次被害の防止

本パッケージは、漏えいした個人情報を悪用した詐欺やなりすまし、偽・誤情報による二次被害を防ぐため、注意喚起の体制を強化する方針を示すとともに、通信事業者によるアクセス抑止策の在り方についても法的課題を含め早急に検討するとしている。

Ⅴ. まとめ

本パッケージは、攻撃を受けることを前提に、社会の機能を止めない、止まってもすぐに立ち直る「サイバーレジリエンス」を確保するという考え方に立っている。その上で、発注者・委託先・経営層それぞれが責任を持ち、基本的な対策を「当たり前」に講じることを求めている。

企業法務の立場では、委託先との契約条項、データ保有方針、インシデント発生時の当局対応・証拠保全の手順などを早めに点検しておくことが必要であろう。

以上

■ 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

■ 本ニュースレターの執筆者は、以下のとおりです。

弁護士 清水 亘 wataru.shimizu[at]amt-law.com
弁護士 髙橋 麟太朗 rintaro.takahashi[at]amt-law.com
弁護士 田中 滉大 koudai.tanaka[at]amt-law.com
※メールを送信する際には、[at]を@に変更してお送りください。

■ ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

■ ニュースレターのバックナンバーは、こちらにてご覧いただけます。

本記事（または本記事の一部）は商事法務 CODE にも掲載しています。