「サイバー攻撃被害に係る公表」に関する国内組織実態調査 第2回

―インシデント検知から1週間以内に公表する企業は半数を超える―

pwc

1. はじめに

1. はじめに

ビジネスへのサイバー脅威が高まる中、サイバー攻撃被害（以下「インシデント」）時に情報を公表することは、ビジネスへの影響や風評被害を軽減する上で非常に重要です。また昨今、グローバルにおいてインシデント報告を求める法規制が強化される傾向にあり（図表1）、2023年は米国証券取引委員会（SEC）によるSEC登録企業へのサイバーリスクやインシデント報告の義務化[1]が話題を集めました。

今後、国内組織にはサイバーインシデントや個人情報漏えいについて「対外公表の迅速化」や「内容の適切化」が一層求められていきます。セキュリティ責任者は風評被害などの影響を最小限にとどめ、事業継続を図るために、平時からインシデント発生時における対外公表の準備をしておく必要があります。そのためには、どのタイミングで、どのような内容を公表すべきか、というインシデント公表事例の収集が不可欠ですが、自社だけでこれらを継続的に調査・分析することはリソースの観点上非常に困難です。そこでPwCでは、独自に収集するインシデントデータベースをもとに国内組織のインシデント公表事例を分析しています。本書は2回目の調査結果をまとめたレポートとなります。

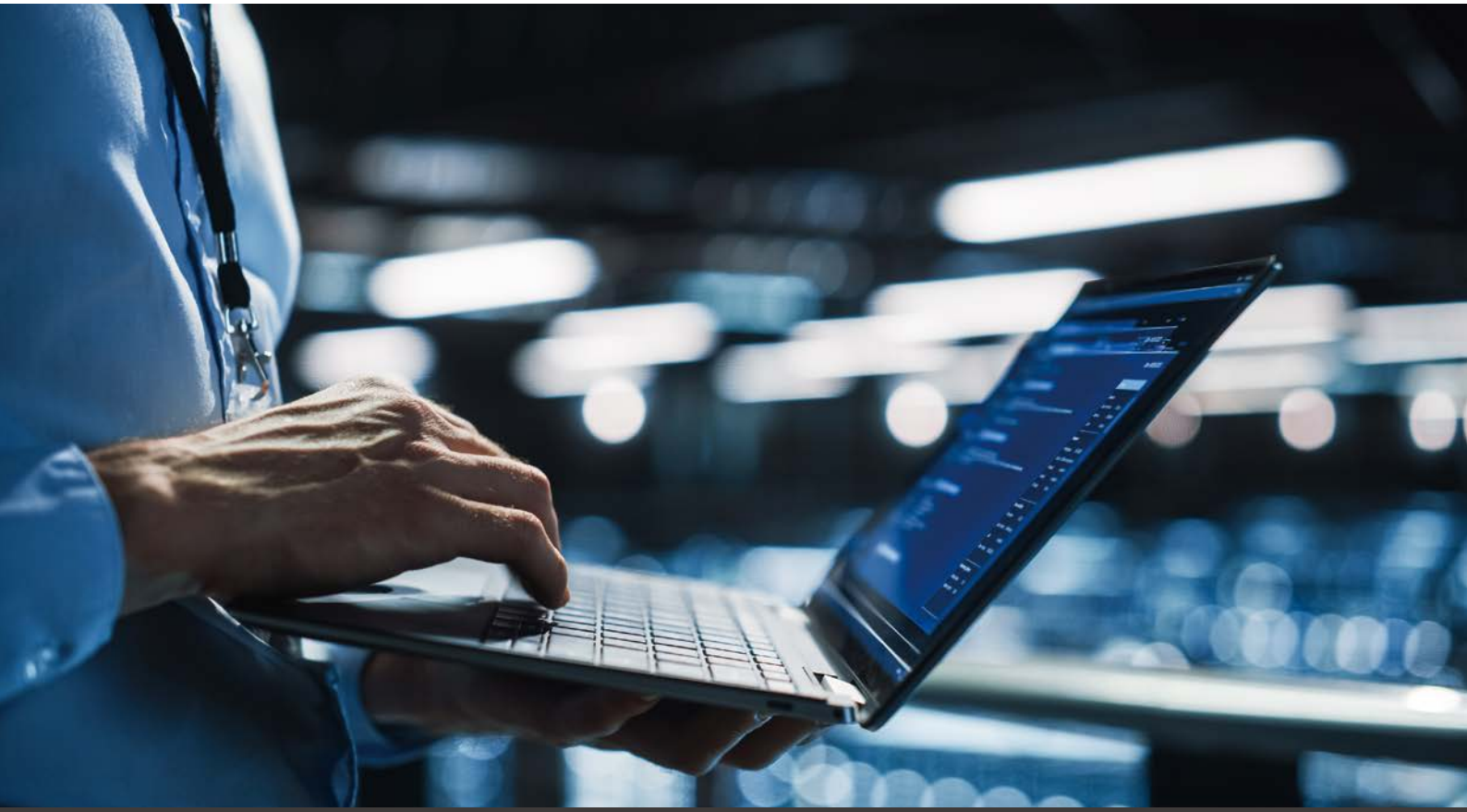
2024年調査では、2022年10月から2023年9月末までに確認された主要な国内インシデント公表事例337件の分析結果（追跡調査含む）をもとに、国内の傾向および国内組織への推奨事項をまとめています。

なお、今回の調査では、国内組織に加え、米国組織における公表事例（N=265）も同条件で分析しました。いくつか傾向が確認できたため参考情報として文末でご紹介します。

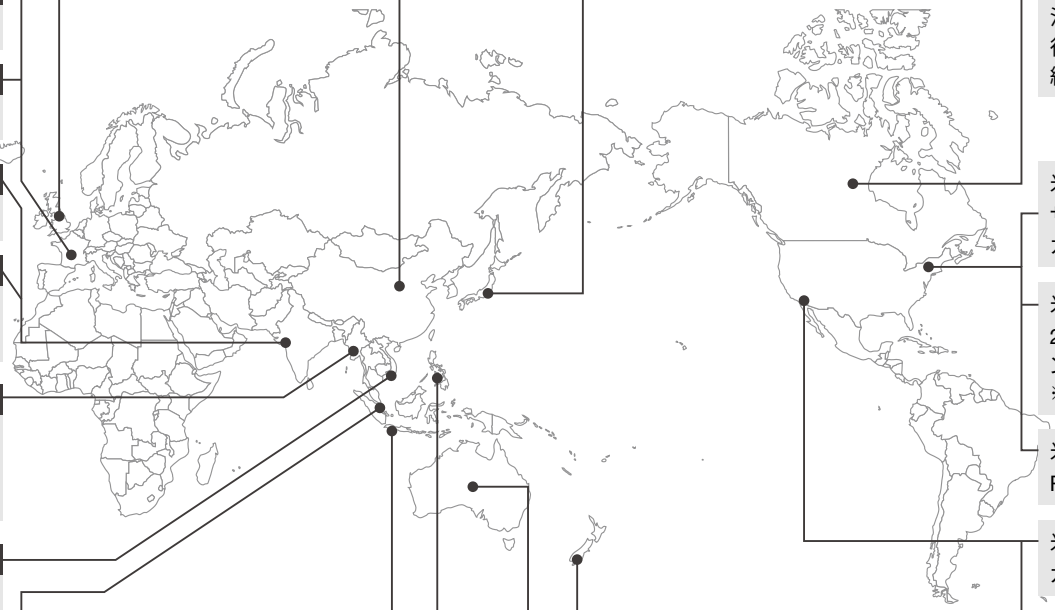
本調査が、皆様の自組織におけるインシデント公表に係る施策を講じる上での参考になれば幸いです。

2023年調査はこちらから参照いただけます。
「サイバー攻撃被害に係る公表」に関する国内組織実態調査2023
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/cyber-attack-survey2023.html

1 The Securities and Exchange Commission, “SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies” (July 26, 2023) https://www.sec.gov/newsroom/press-releases/2023-139



図表1：サイバーインシデント報告（個人情報漏えい含む）を義務化する主な法規制



英国（2021施行）
英国GDPR
72時間以内

EU（2024施行）
NIS2
早期警告24時間

EU（2024施行）
EUサイバーレジリエンス（CRA）法
24時間以内

EU（2018施行）
EU一般データ保護規則（GDPR）
72時間以内

インド（2023施行）
デジタル個人情報保護法2023
未確定

インド（2022施行）
Cyber Security Directions of 28th April 2022
6時間以内

タイ（2022施行）
個人情報保護法（PDPA）個人データ侵害通知の規則および方法に関する監督当局通知 B.E. 2565（2022）
72時間以内

ベトナム（2023施行）
個人情報の保護に関する政令
第13/2023/ND-CP号
72時間以内

ベトナム（2026施行見通し）
個人情報保護法草案
72時間以内

シンガポール（2024施行）
サイバーセキュリティ法改正案
2時間以内

シンガポール（2022改正法施行）
個人情報保護法
72時間以内

中国（審議中）
中国サイバーインシデント報告管理弁法案
1時間以内

中国（2017施行）
サイバーセキュリティ法
直ちに

フィリピン（2017施行）
個人情報保護法（DPA）
※「正当な利益」に関するガイドライン（NPC Circular No. 2023-07）は2024年1月施行
72時間以内

インドネシア（2022施行）
個人情報保護法（PDPL）
72時間以内

日本（2024改正法施行）
個人情報保護法および個人情報保護法施行規則
速報3-5日以内

ニュージーランド（2020施行）
個人情報保護法2020
速やかに

オーストラリア（2024施行）
個人情報保護法1988 改正法2024年
速やかに

オーストラリア（2024）
重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）の改正
速やかに

オーストラリア（2025施行予定）
サイバーセキュリティ法2024
72時間以内

カナダ（2019施行）
個人情報保護および電子文書法（PIPEDA）
速やかに

カナダ
法案C-26サイバーセキュリティに関する法律、電気通信法の改正、および他の法律の結果的改正
直ちに

米国（2023施行）
サイバーセキュリティ・リスク管理、戦略、ガバナンス、インシデント開示（SEC）
4営業日以内

米国（2022施行）
2022年重要インフラ向けサイバーインシデント報告法（CIRCIA）
※同法に関する施行規則案を2024年3月に発表
72時間以内

米国（2021発行）
Ransomware Guidance
72時間以内

米国（2024施行）
カリフォルニア州プライバシー権法（CPRA）

米国（2022施行）
カリフォルニア州データ漏洩通知法
速やかに

■ 当該事象を主要なインシデントとして認識してから当局へ求められる報告期間　　施行済

出所：各国政府等公表資料を基にPwC作成

2.「サイバー攻撃被害に係る公表」の7つの傾向

2.「サイバー攻撃被害に係る公表」の7つの傾向

本調査は、2022年10月から2023年9月末までにCISO Cyber Concierge[2]にて掲載されたインシデントのうち、国内に所在する被害組織がインシデント公表を行った事例337件を調査対象として公表内容やタイミングなどを分析し、さらに2023年10月から2024年3月末までの半年間での続報（第2報以降）の有無を追跡調査したものです（図表2）。これらの調査から、以下7つの傾向が明らかになりました（図表3）。

図表2：2024年調査の対象とするインシデント公表事例

	フェーズ	調査対象期間	調査の説明
A	本調査	2022年10月1日～2023年9月30日	調査期間にCISO Cyber Conciergeに掲載されたインシデント公表事例（337件）[3]の記載内容やタイミングについて調査
B	追跡調査	2023年10月1日～2024年3月31日	Aで対象としたインシデント公表事例（337件）に対し、続報（第2報以降）が公表されているかを調査

図表3：PwCのインシデントデータベースからみる「サイバー攻撃被害に係る公表」の7つの傾向

カテゴリ	7つの傾向
公表事例からみる国内組織の傾向	• 続報（第2報以降）を公表する国内組織は約半数 • 外部専門家へ調査委託する国内組織は6割強 • クレジットカード情報漏えい企業では、外部からの通知によるインシデント発覚が9割と前年に続き高い
公表タイミングにおける傾向	• 初報の公表曜日は「火曜日」「金曜日」が多い傾向 •「インシデント検知から初報までにかかる日数」の国内中央値は「5日」、1週間以内に公表する企業が55%と半数を超える • クレジットカード情報漏えい企業では、「インシデント検知から初報」まで1カ月以上要する割合が8割超
公表内容の傾向	•「今後の対応」記載割合は、前年と比較し約20ポイントも高い

2 PwC「CISO Cyber Concierge」における「Cyber Incident」では、サイバー脅威インテリジェンスリサーチャーが主要と判断した国内外のインシデントを掲載しています。
https://www.pwc.com/jp/ja/services/assurance/governance-risk-management-compliance/digital-trust-service-platform/ciso-cyber-concierge.html

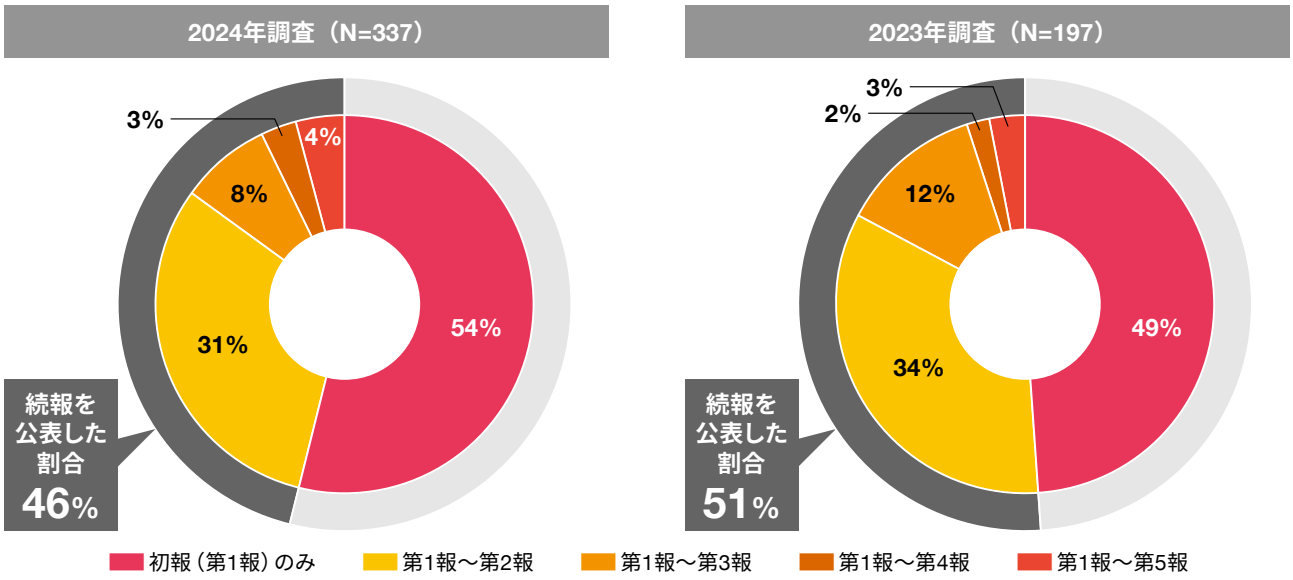
3 ここでいう「インシデント公表事例」とは、国内組織が当該インシデントを認め、公式に公表を行った事例を指します。

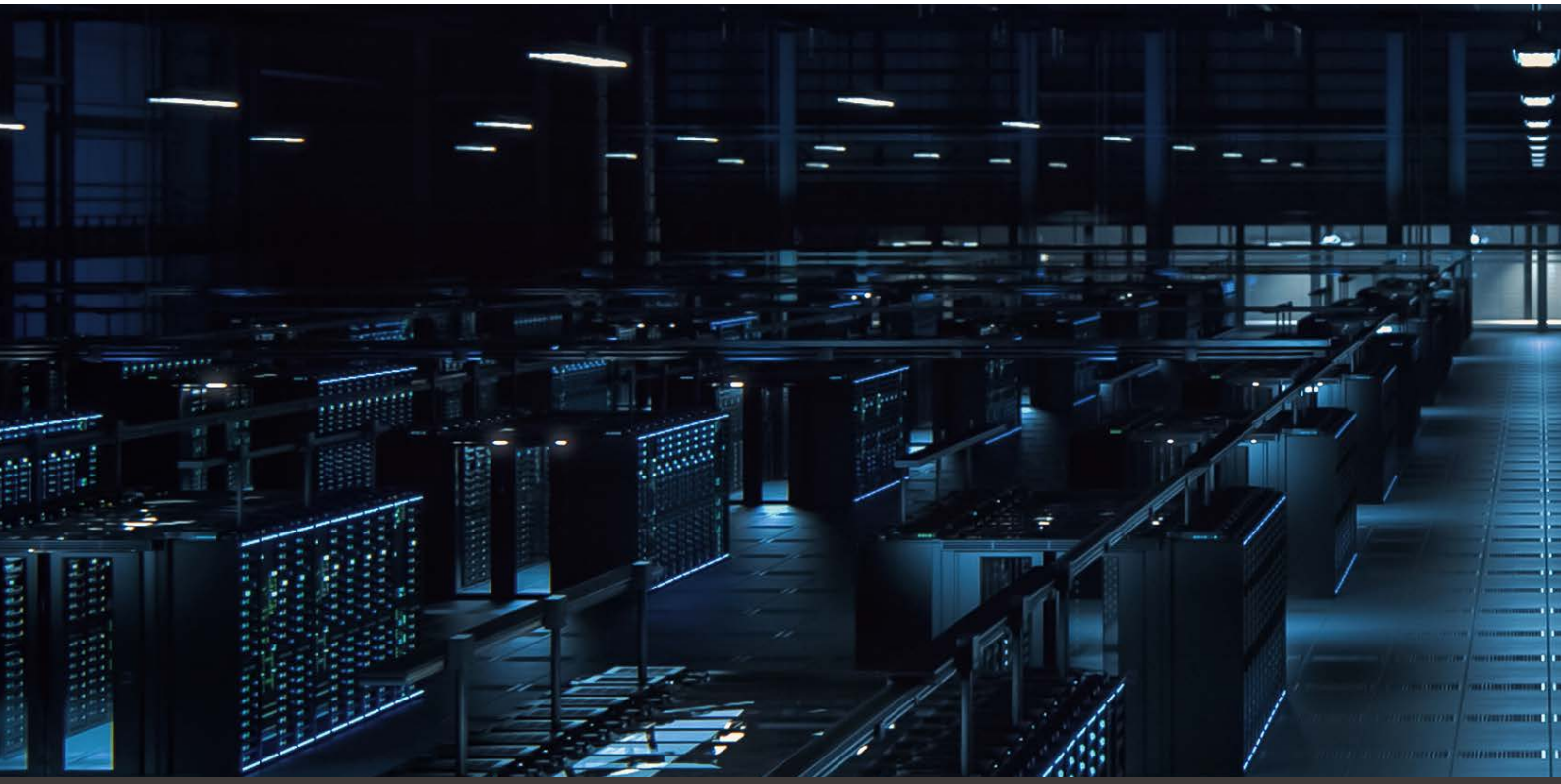
公表事例からみる企業の傾向

Findings 1：続報（第2報以降）を公表する国内組織は約半数

インシデント公表事例（N=337）において、続報（第2報）を公表する国内組織は過半数に上りました（図表4）。具体的には、インシデント公表事例1件あたりの公表回数として、「初報（第1報）のみ」公開した国内組織は全体の54%、「第1報から第2報まで」を公開した国内組織は全体の31%、「第1報から第3報まで」は8%、「第1報から第4報まで」は3%、「第1報から第5報まで」は4%存在していることが分かりました。これらの割合は前年調査と同じような傾向にあることから、国内組織のインシデント公表の実態を反映しているといえます。

図表4：インシデント1件あたりの公表回数（2024年調査、2023年調査比較）

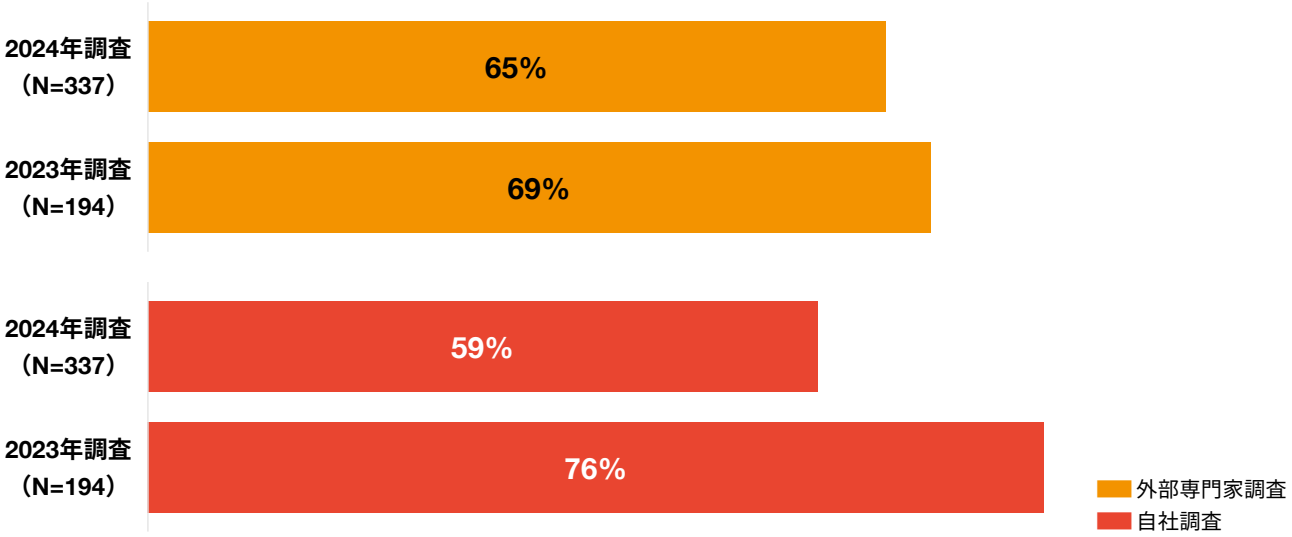


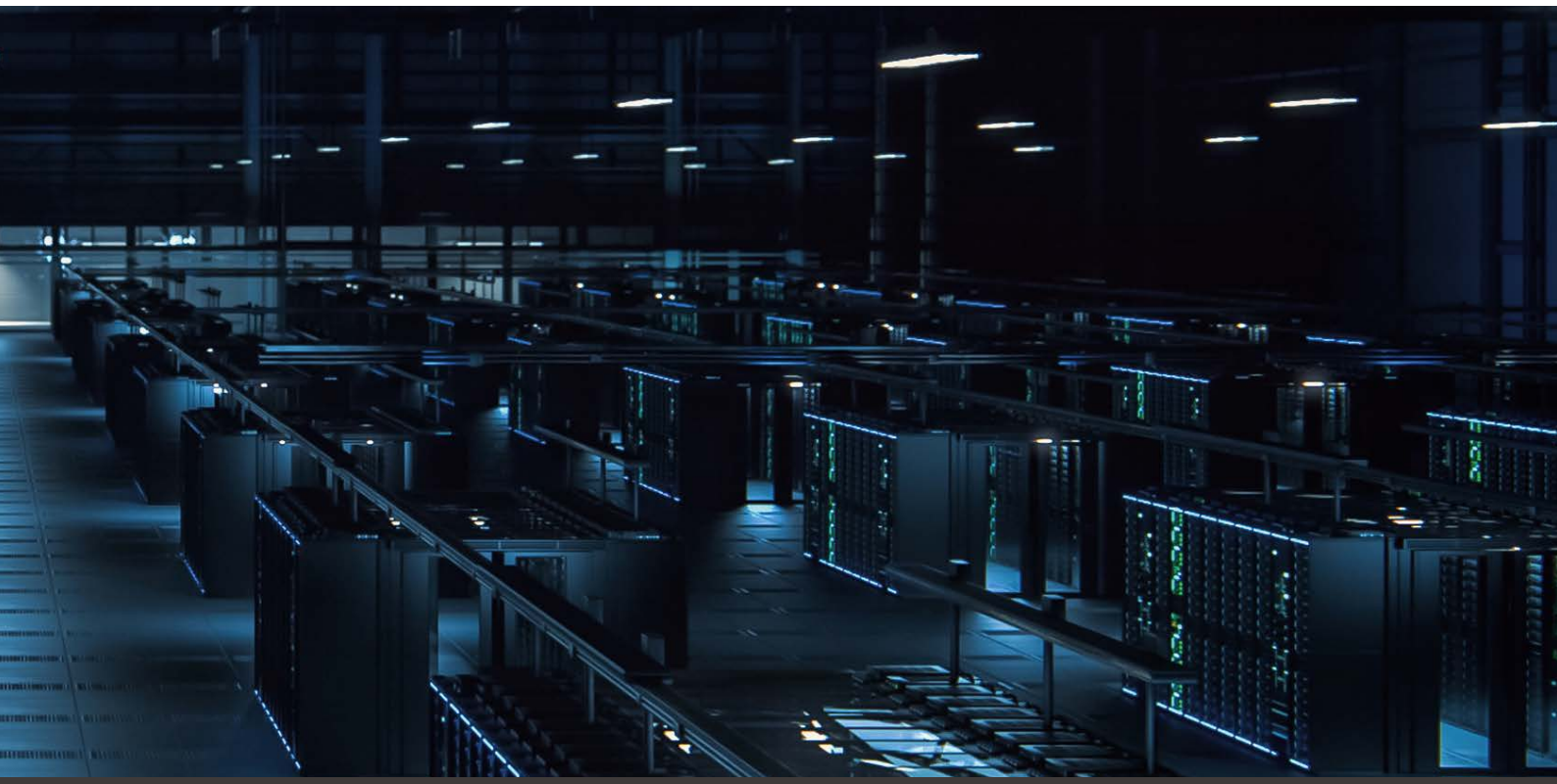


Findings 2：外部専門家へ調査委託する企業は6割強

2024年インシデント公表事例（N=337）をみると、当該インシデントについて「外部専門家への委託調査を実施した」と記載した割合は65%に上りました（図表5）。多くのインシデントを経験する国内組織では、調査を外部専門家へ委託する傾向にあることが分かりました。国内組織は有事に備え、必要に応じて事前に調査委託先を選定し、相談窓口を開設しておくことを検討すると良いでしょう。

図表5：「外部専門家への委託調査実施」記載の有無（2024年調査、2023年調査比較）





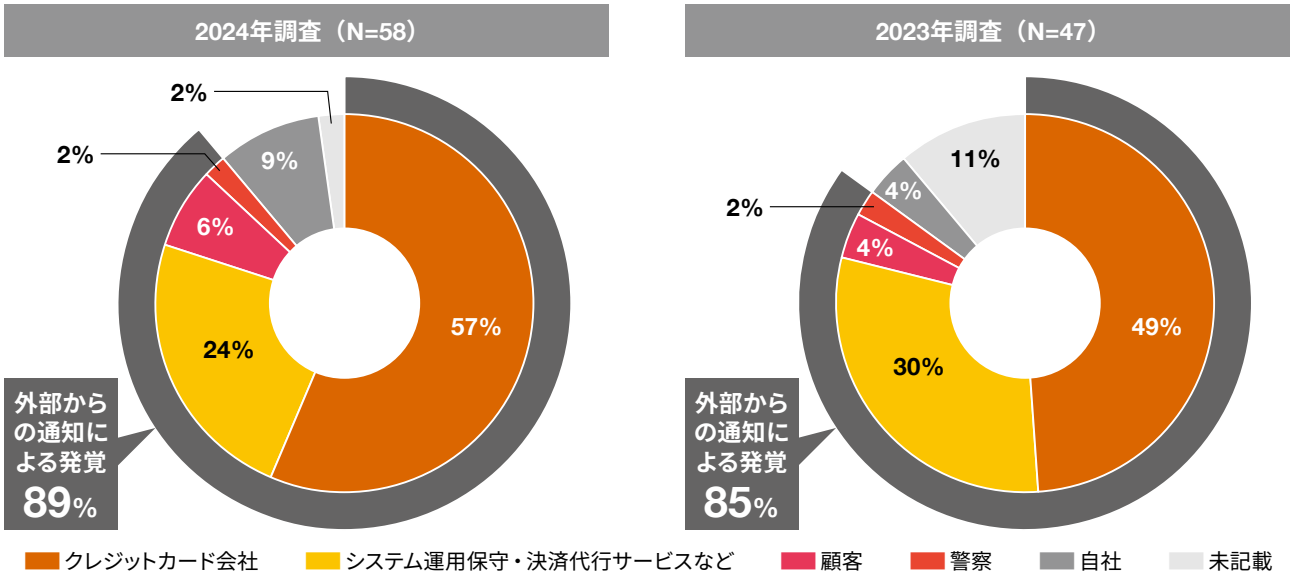
Findings 3：クレジットカード情報漏えい企業では、外部からの通知による インシデント発覚が9割と前年に続き高い

クレジットカード情報が漏えいしたとするインシデント公表事例（N＝58）をみると、「発覚者の記載」は全体の98%と前年調査（同89%）より高くなりました（図表6）。

発覚者の内訳をみると「外部からの通知による発覚」が最も多く89%、「自社による発覚」が9%、「未記載」が2%であり、クレジットカード情報漏えいを経験する国内組織では自社でインシデントを検知できていない傾向にあることが分かります。また、外部発覚者の内訳をみると、「クレジットカード会社」が最も多く全体の57%（前年調査49%）を占め、次いで「システム運用保守・決済代行サービス事業者など」が24%（前年調査30%）、「顧客」が6%（前年調査4%）、「警察」が2%（前年調査2%）の順となりました。

これらのことから、クレジットカード情報を取り扱う国内組織においてシステムを外部委託する場合は、セキュリティ能力の高いシステム会社を選定したり、セキュリティ専門企業と定期的なセキュリティ診断や継続的なモニタリングサービスを契約したりするなど、インシデントの早期発見のための体制を整える必要があるといえます。

図表6：クレジットカード情報漏えいにおける発覚者の割合（2024年調査、2023年調査比較）



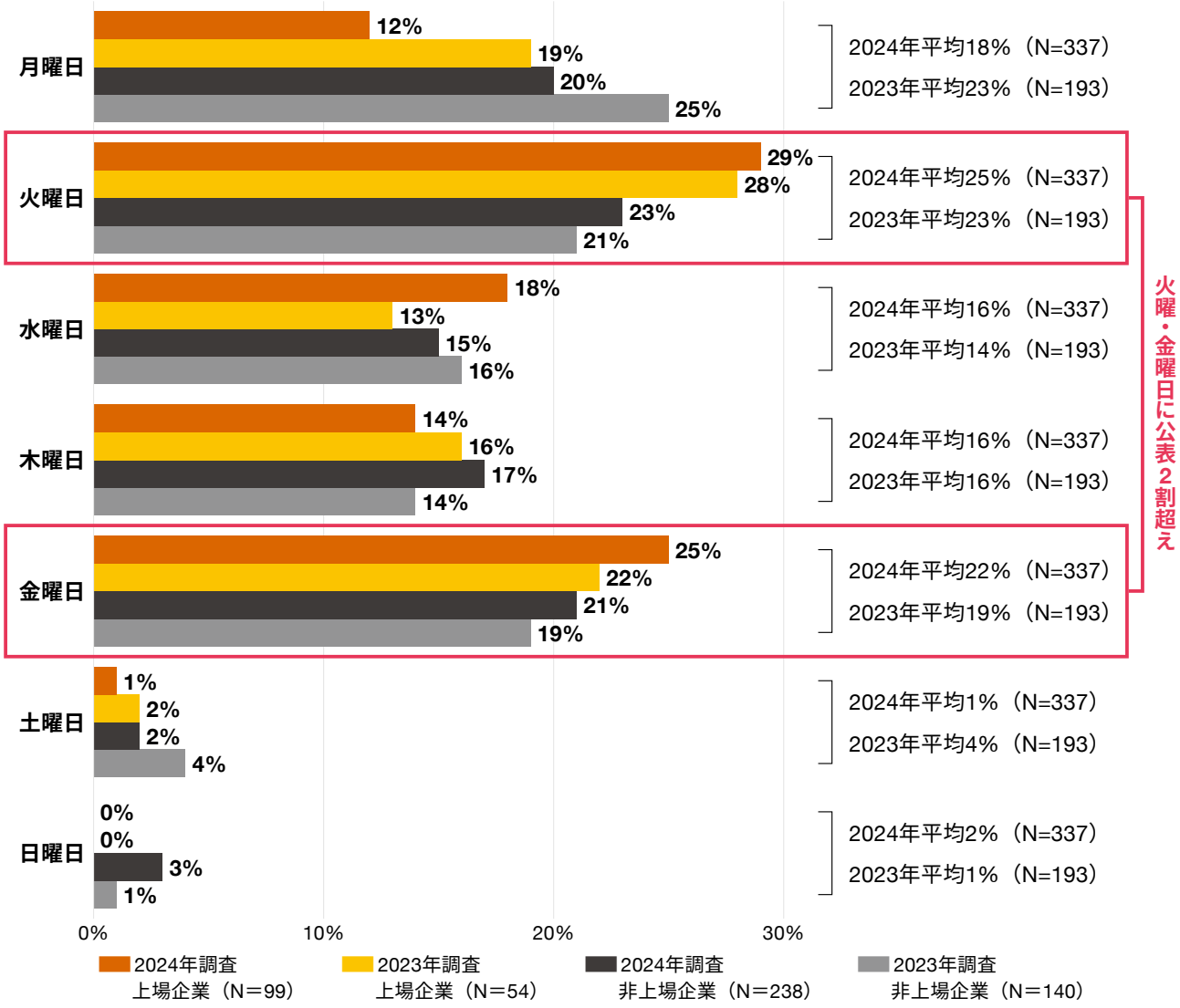
公表タイミングにおける傾向

Findings 4：初報の公表曜日は「火曜日」「金曜日」が多い傾向

インシデント公表事例（N=337）において、続報（第2報）インシデント公表事例（N=337）における初報（第1報）の公表日を曜日別にみると、「火曜日」が最も多く全体の25%、次いで「金曜日」が22%、「月曜日」が18%の順となりました（図表7）。

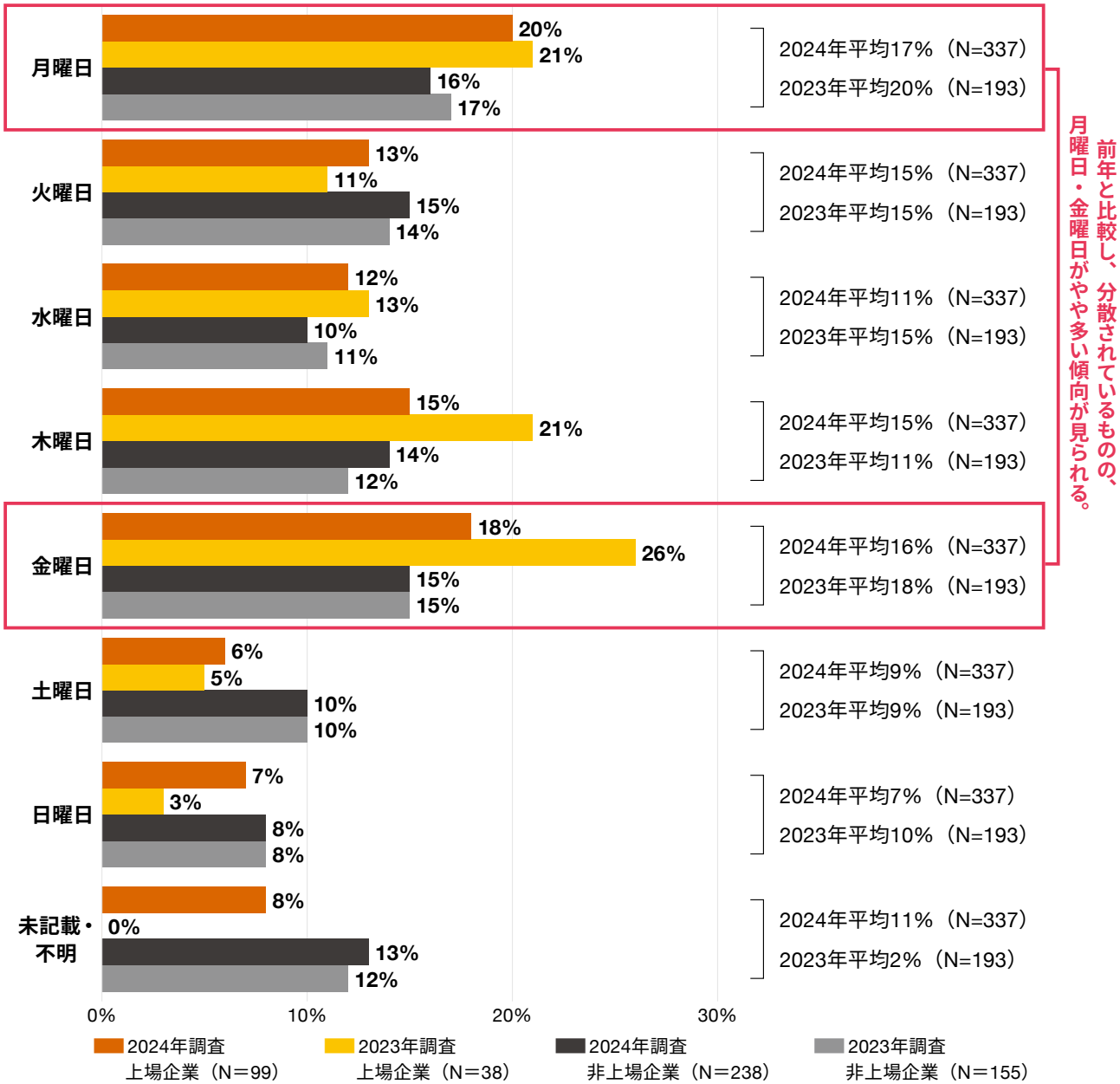
さらに、上場有無で分析すると、上場企業の初報（N=99）の曜日でも、前年調査（28%）に引き続き「火曜日」が最も多く29%、次いで「金曜日」が25%、「水曜日」が18%、「木曜日」が14%、「月曜日」が12%、「土曜日」が1%の順となり、「日曜日」には公表していないことが分かりました。また、非上場企業の初報（N=238）においても「火曜日」が最も多く23%、次いで「金曜日」が21%、「月曜日」が20%、「木曜日」が17%、「水曜日」が15%、「土曜日」が2%、「日曜日」が3%の順となりました。

図表7：インシデント被害を公表（初報）した曜日の割合（上場企業および非上場企業との比較）



次に、インシデントを検知した曜日においても傾向が確認されました。インシデント公表事例（N=337）におけるインシデントを検知した曜日は、「月曜日」が前年調査に引き続き最も高く17%、次いで「金曜日」が16%、「火曜日」「木曜日」が15%、「水曜日」が11%、「土曜日」が9%、「日曜日」が7%の順となりました（図表8）。「金曜日」から「月曜日」にかけてインシデントを検知する割合が全体の半数（49%）を占めることから、国内組織は休日を挟む週末から週明けにかけてインシデント検知した場合の公表フローやタイミングについて平時から方針を決めておくと良いでしょう。

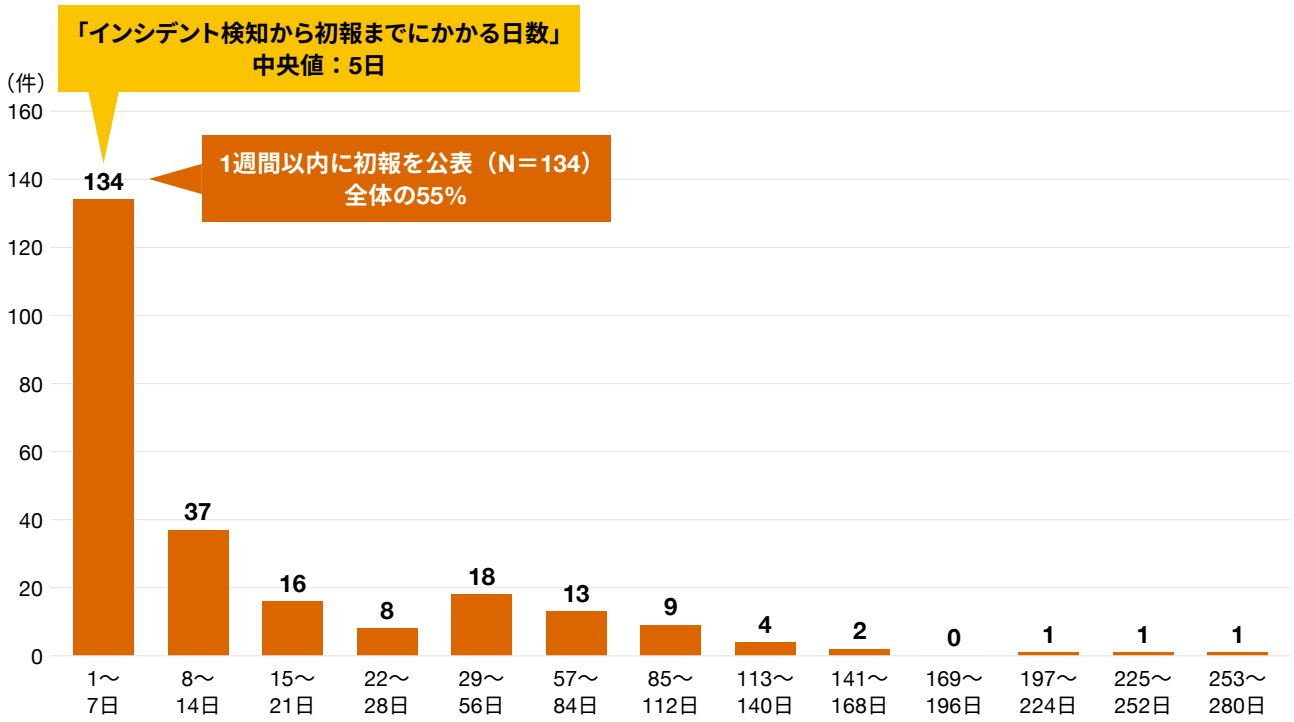
図表8：インシデント被害を検知した曜日の割合（2024年調査、2023年調査比較）（上場企業平均および非上場企業との比較）



Findings 5：「インシデント検知から初報までにかかる日数」の国内中央値は「5日」、1週間以内に公表する企業が55%と半数を超える

インシデント公表事例（N=234）[4]における、インシデント検知から初報公表までにかかる日数を分析すると、国内中央値は「5日間」で、全体の過半数が1週間以内（1～7日）に公表していることが分かりました（図表9）。

図表9：インシデント検知から初報までにかかる日数：クレジットカード情報漏えい事例を除く（N=243）



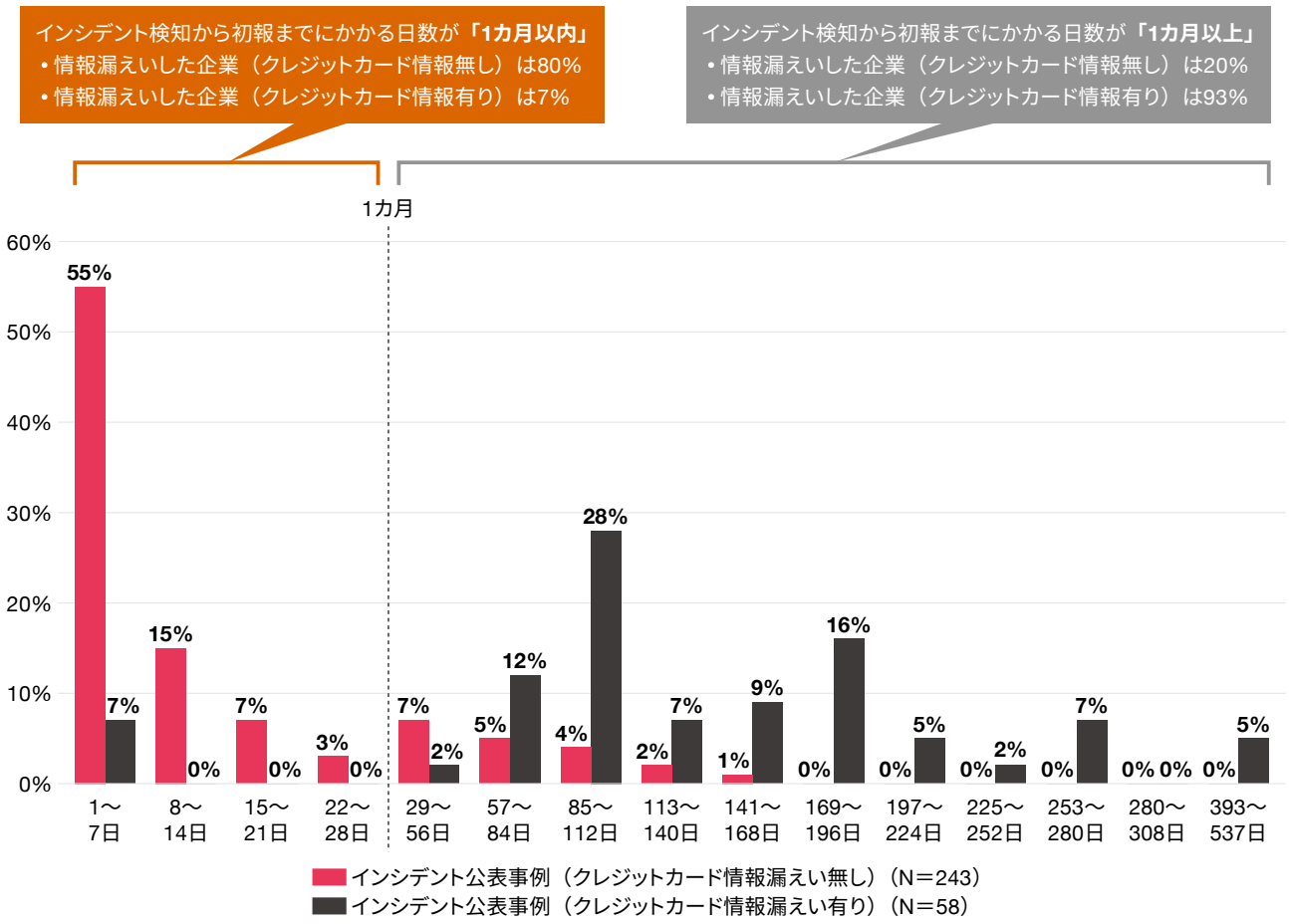
4 本項目で取り扱うインシデント公表事例は「検知日」が記載の事例、かつクレジットカード情報を含まないインシデント公表事例（N=234）を対象とする

Findings 6：クレジットカード情報漏えい企業、「インシデント検知から初報」まで1カ月以上要する企業が8割超

さらに、前年調査に引き続き、クレジットカード情報漏えいの有無により「インシデント検知から初報までにかかる日数」に差があることが確認できました（図表11）。

インシデント公表事例（N=301）のうち、クレジットカード情報漏えいを含まないインシデント公表事例（N=243）では、7日以内に公表する国内組織が55%と最も多く、次いで8～14日以内は15%、15～21日以内は7%、22～28日以内は3%と、インシデント検知から1カ月以内に公表した国内組織は全体の80%に上りました。一方、クレジットカード情報漏えいを含むインシデント公表事例[5]（N=58）における「インシデント初報までにかかる日数」をみると、7日以内に公表する国内組織は7%、8～14日以内、15～21日以内、22～28日以内はそれぞれ0%と、1カ月以内に公表した企業は1割に満たず、公表に1カ月以上要する事例が全体の9割超と、クレジットカード情報漏えいを含まないインシデント公表事例と比較し、公表までに時間を要する傾向にあることが分かりました。Findings 3に示したように、今回対象となったインシデント公表事例の多くはクレジットカード会社からの指摘によって発覚しています。また、類似の公表文章が採用されていることから、クレジットカード会社が推奨する外部調査機関による第三者調査が実施されており、これが自社単独でインシデント対応が完結できない要因となり、公表までに時間がかかるのではないかと推察します。

図表11：国内組織における「インシデント検知から初報までにかかる日数」（クレジットカード情報漏えいの記載有無による比較）



5 クレジットカード情報を漏えいした、または漏えいの恐れがあると言及したインシデント公表事例

公表内容の傾向

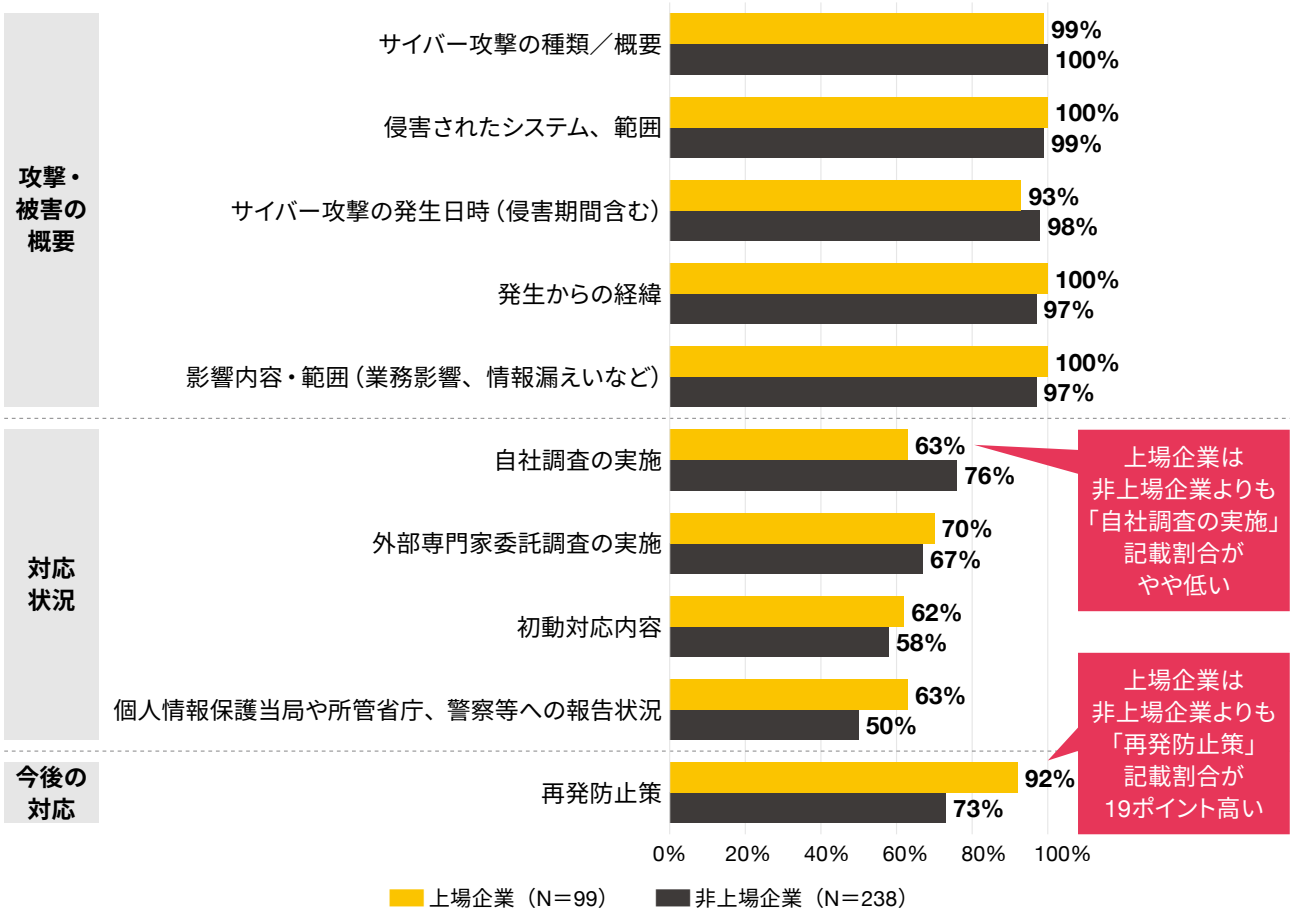
Findings 7：「今後の対応」記載割合は、前年と比較し約20ポイントも高い

インシデント公表事例（N=337）の記載内容を「攻撃・被害概要[6]」「対応状況」「今後の対応」の3つのカテゴリに分けて分析すると、「攻撃・被害概要」および「今後の対応」関連項目は多くの事例で記載を確認できました（図表12）。前年調査に引き続き「対応状況」の関連項目記載は少ない傾向にある一方で、「今後の対応」の記載割合は前年と比較し約20ポイントも高くなり、記載することが標準になったといえます。

まず、「攻撃・被害の概要」の関連項目とした「サイバー攻撃の種類／概要」「侵害されたシステム、範囲」「サイバー攻撃の発生日時（侵害期間含む）」「発生からの経緯」「影響内容・範囲（業務影響、情報漏えいなど）」は全項目で100%近く記載されており、国内組織におけるインシデント公表内容では上記項目を記載することが一般的であると分かりました。次に、「対応状況」の関連項目においては、「自社調査の実施」を記載した公表は全体の63%、「外部専門家委託調査の実施」が70%、「初動対応内容」が62%、「個人情報保護当局や所管省庁、警察等への報告状況」は63%となりました。最後に、「今後の対応」の関連項目とした「再発防止策」の記載は92%と前年調査（73%）と比較して19ポイントも記載割合が高くなりました。

これらの傾向から、2023年2月に公表された国内のインシデント公表事例も、NISC（内閣サイバーセキュリティセンター）の「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の記載項目に概ね則した形で記載されていることが分かりました。

図表12：インシデント公表事例からみる主な記載項目（N=337）



6 NISC「サイバー攻撃被害に係る情報の共有・公表 ガイダンス」における「公表の内容（P.72）」を加味し、PwCが項目を選定

3. インシデント公表事例からみる国内組織への推奨事項

3. インシデント公表事例からみる国内組織への推奨事項

今回の調査において、インシデント公表事例における7つの傾向を示しました。この傾向から、国内組織が検討すべき推奨事項を以下に記載します（図表13）。

セキュリティ責任者は、自組織におけるインシデント公表方針の見直しにあたってNISCガイドラインやこれらの公表事例からみる推奨事項を参照し、事前に対外公表のひな形を作成して記載内容・公表フローについて広報部門やIR部門などの専門部門と合意を得ておくことで、有事の際に組織にとって適切な情報開示に臨むことができるでしょう。

図表13：インシデント公表事例からみる国内組織における「7つの傾向」と「推奨事項」

4. 調査概要

4. 調査概要

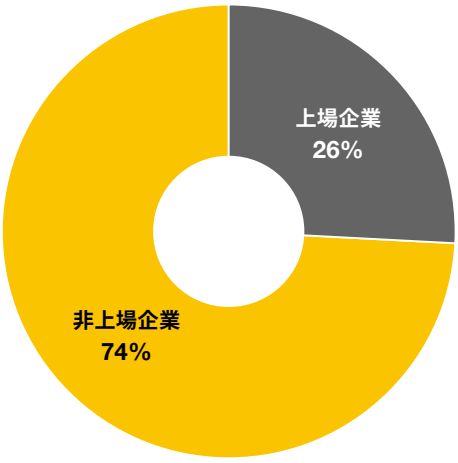
調 査 名	サイバー攻撃被害公表に関する国内組織の実態調査 第2回
調査対象	**【本調査】** 2022年10月1日2023年9月30日までにCISO Cyber Conciergeにて掲載されたインシデントのうち、国内組織が当該インシデントの公表を行ったインシデント公表事例337件 **【追跡調査】** 2023年10月1日～ 2024年3月31日までに公開された「インシデント公表事例337件」の続報（第2報以降）
調査期間	2022年10月～ 2024年3月末日
調査方法	机上調査

対象報告書の属性

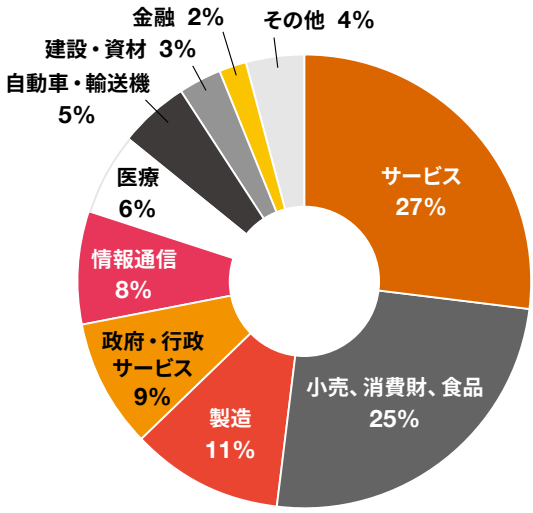
今回調査対象となった国内インシデント公表事例（N=337）の属性は以下のとおりです。上場有無については、上場企業が26%、非上場企業が74%でした（図表14：左）。業界別にみると「サービス」が最も多く27%、次いで「小売、消費財、食品」が25%、「製造」が11%、「政府・行政サービス」が9%、「情報通信」が8%、「医療」が6%の順になっています（図表14：右）。

図表14：調査対象とした国内インシデント公表事例の属性
（上場有無・業界、インシデント1件あたりの公表回数）

上場有無（N=337）



業界（N=337）



5. その他

5. その他

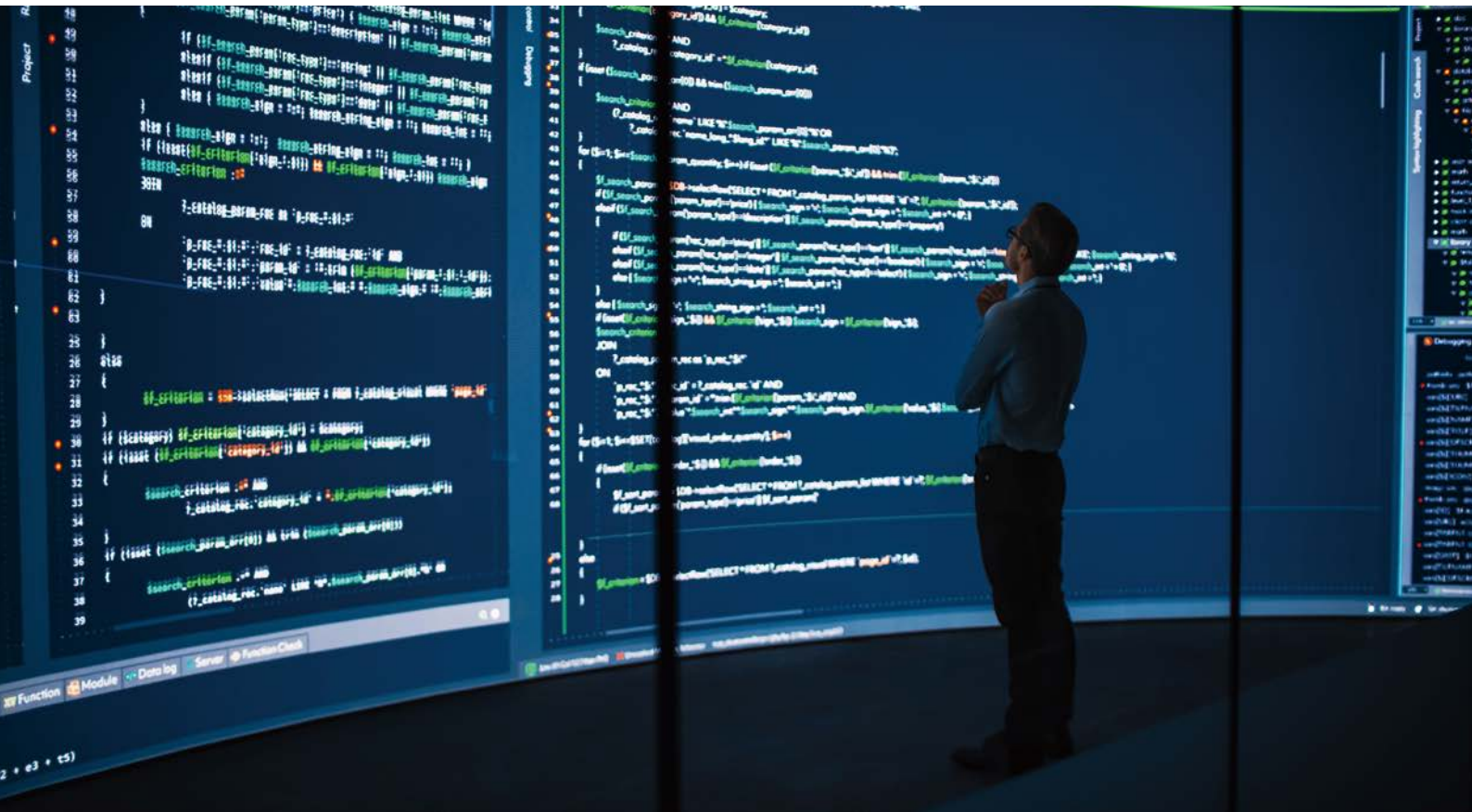
今回調査において、国内調査と同じ条件で抽出した米国に所在する被害組織のインシデント公表事例（N=265）と比較したところ、以下の傾向が確認できました。

図表15：インシデント公表事例からみる傾向（日米比較）

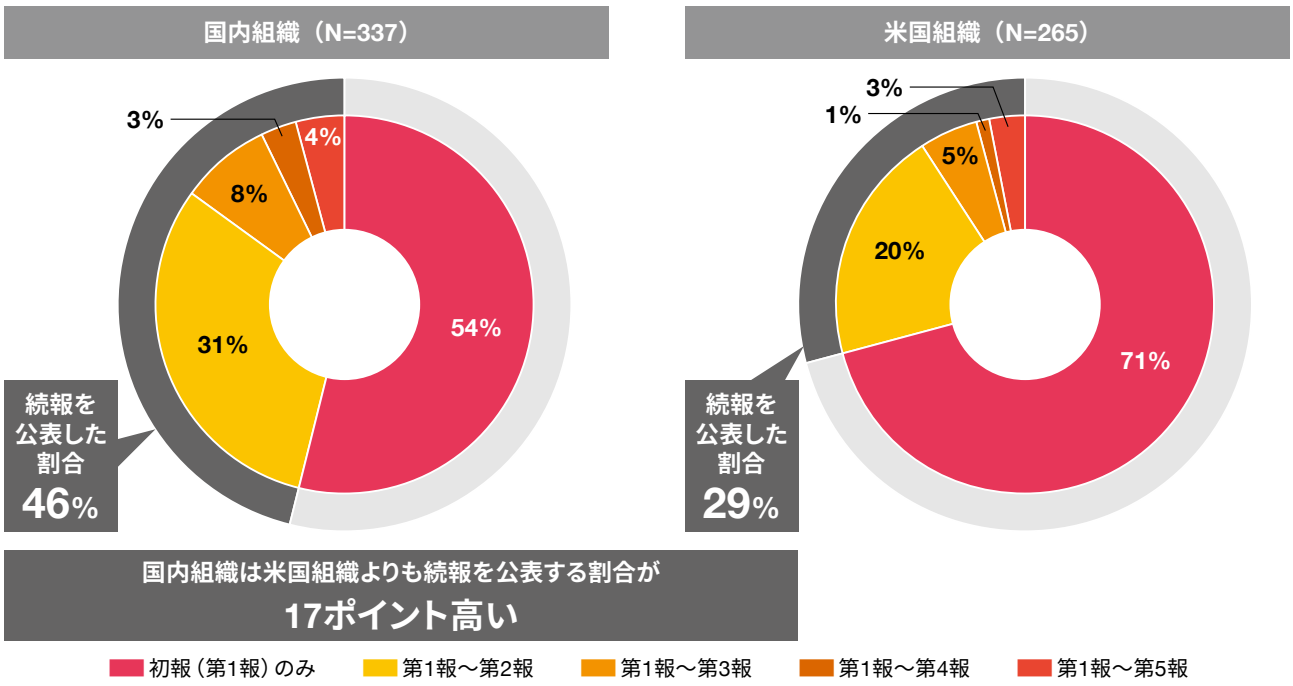
米国組織の傾向	• 米国組織は、初報のみを公表する割合が高く全体の7割を占める（日本組織：5割）（図表16）。
公表場所	• 情報公開場所として、今回対象となった全ての日本組織はウェブサイトにて公表し、うち約1割は東証上場会社情報サービスでも並行して公表していた。米国組織は、ウェブサイトでの公表は7割にとどまり、顧客等への本人通知のみとする傾向がある（図表17）。
公表内容	• 米国組織は、国内組織と比較し、①二次被害の防止策（1～2年間の信用監視サービスや個人情報盗難保護サービスなど）を該当顧客へ提供したり、②該当顧客の個人情報悪用の兆候がある場合に法執行機関へ通報するよう推奨事項が記載されている傾向にある。 • 米国組織は、他社を起因とするインシデントについては、その背景を詳細に記載する傾向がある（おそらく訴訟対策を念頭に置くものと推察される）。 •「公表が遅れた経緯」の記載は国内組織は2割、米国組織は1割と、どちらも記載傾向としては少ない。 • 日米組織ともに、ランサムウェア感染被害時に支払いの対応状況に関する記載は確認できなかった（なお公表ではないが、米国ではランサムウェア支払い時にはCISAに72時間以内の報告義務がある）。

7 2022年10月から2023年9月末までにCISO Cyber Conciergeにて掲載されたインシデントのうち、米国に所在する被害組織がインシデント公表を行った事例件を調査対象として公表内容やタイミングなどを分析、さらに20232年10月から20243年3月末までの半年間に続報（第2報以降）の有無を追跡調査（図表2参照）。

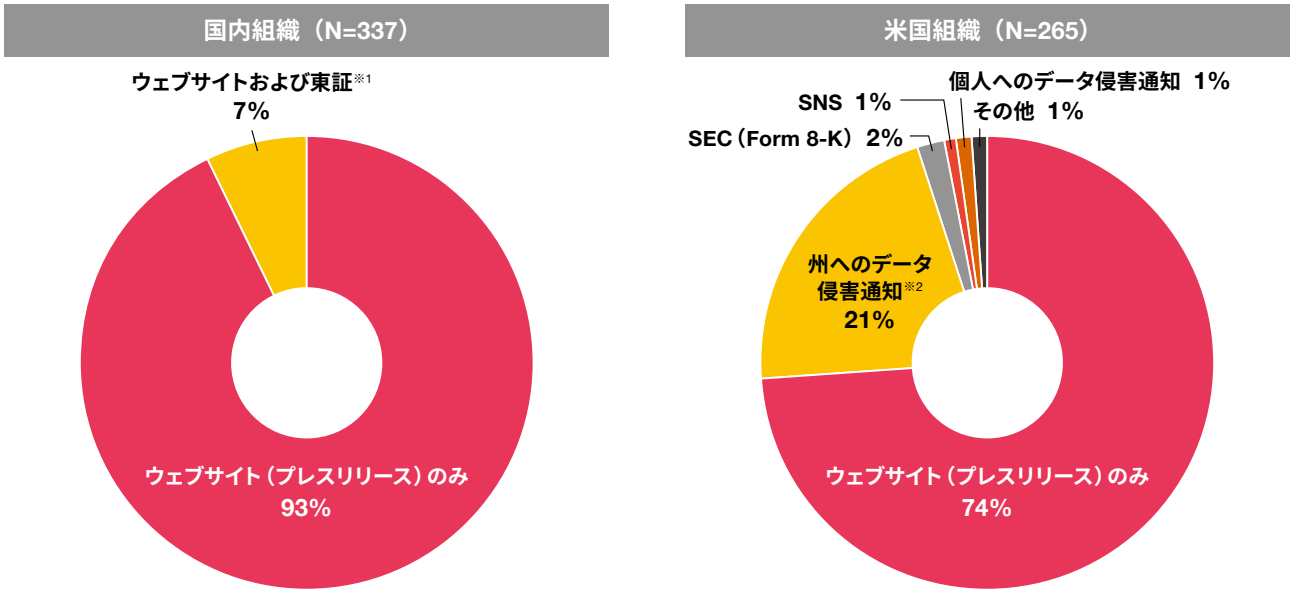
8 日本取引所東京証券取引所「東証上場会社情報サービス」 https://www2.jpx.co.jp/tseHpFront/JJK010030Action.do



図表16：インシデント公表事例1件あたりの公表回数（日米比較）

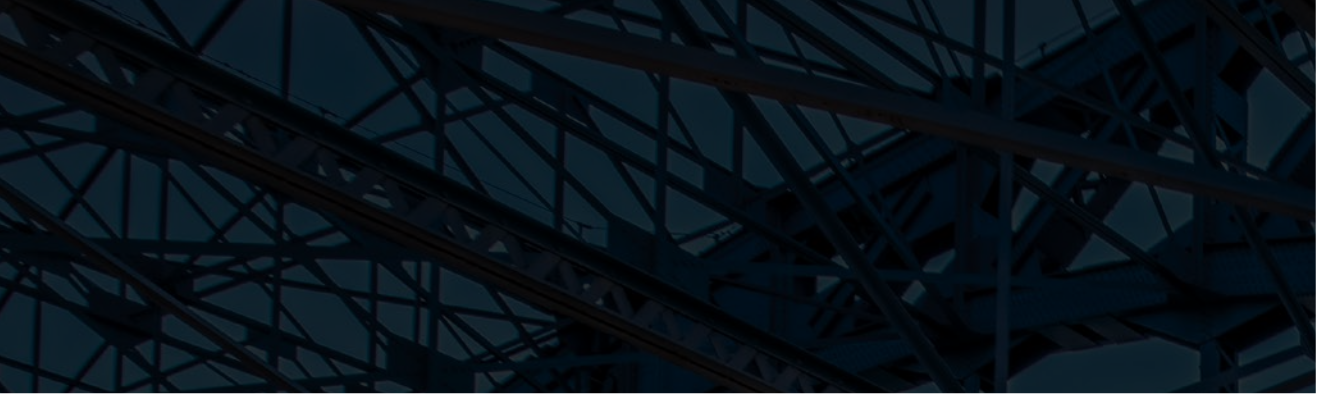
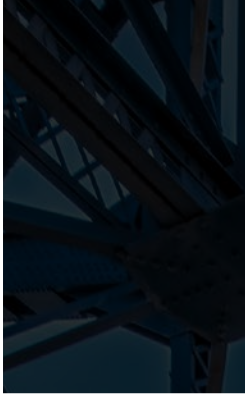


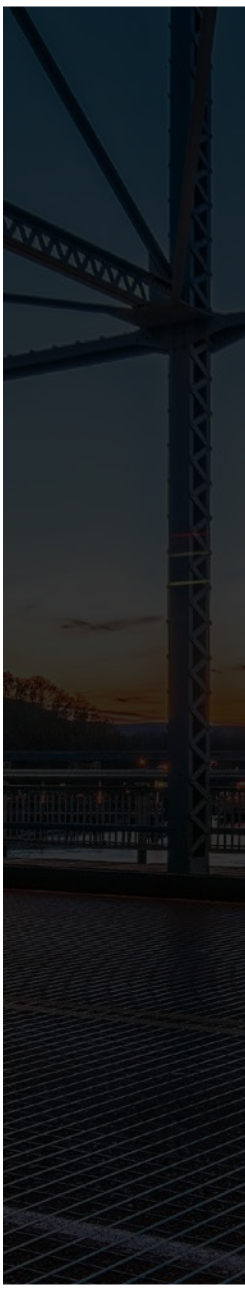
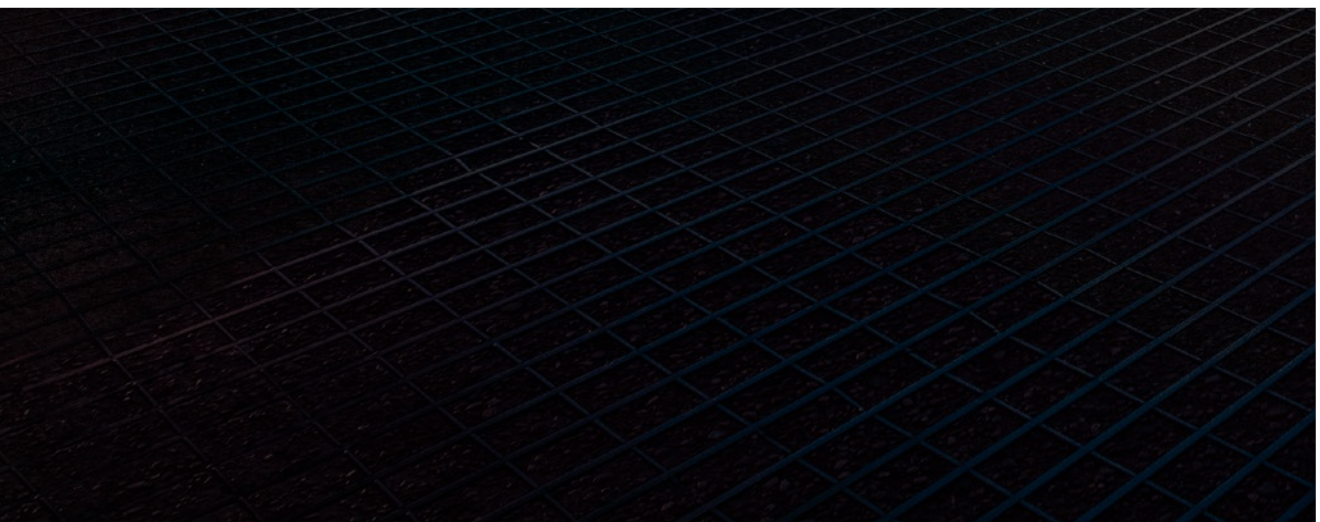
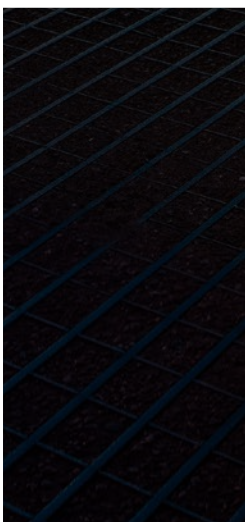
図表17：インシデント公表における情報源（日米比較）



※1 ここでいう「東証」とは「東証上場会社情報サービス」を指す。日本取引所東京証券取引所「東証上場会社情報サービス」
https://www2.jpx.co.jp/tseHpFront/JJK010030Action.do

※2 ここでいう「州へのデータ侵害通知事例」では、当該州のウェブサイトで個人への通知書が公開されたものを対象としている。

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約12,700人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界149カ国に及ぶグローバルネットワークに370,000人以上のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細はwww.pwc.comをご覧ください。

発刊年月：2025年2月　　管理番号：I202411-04