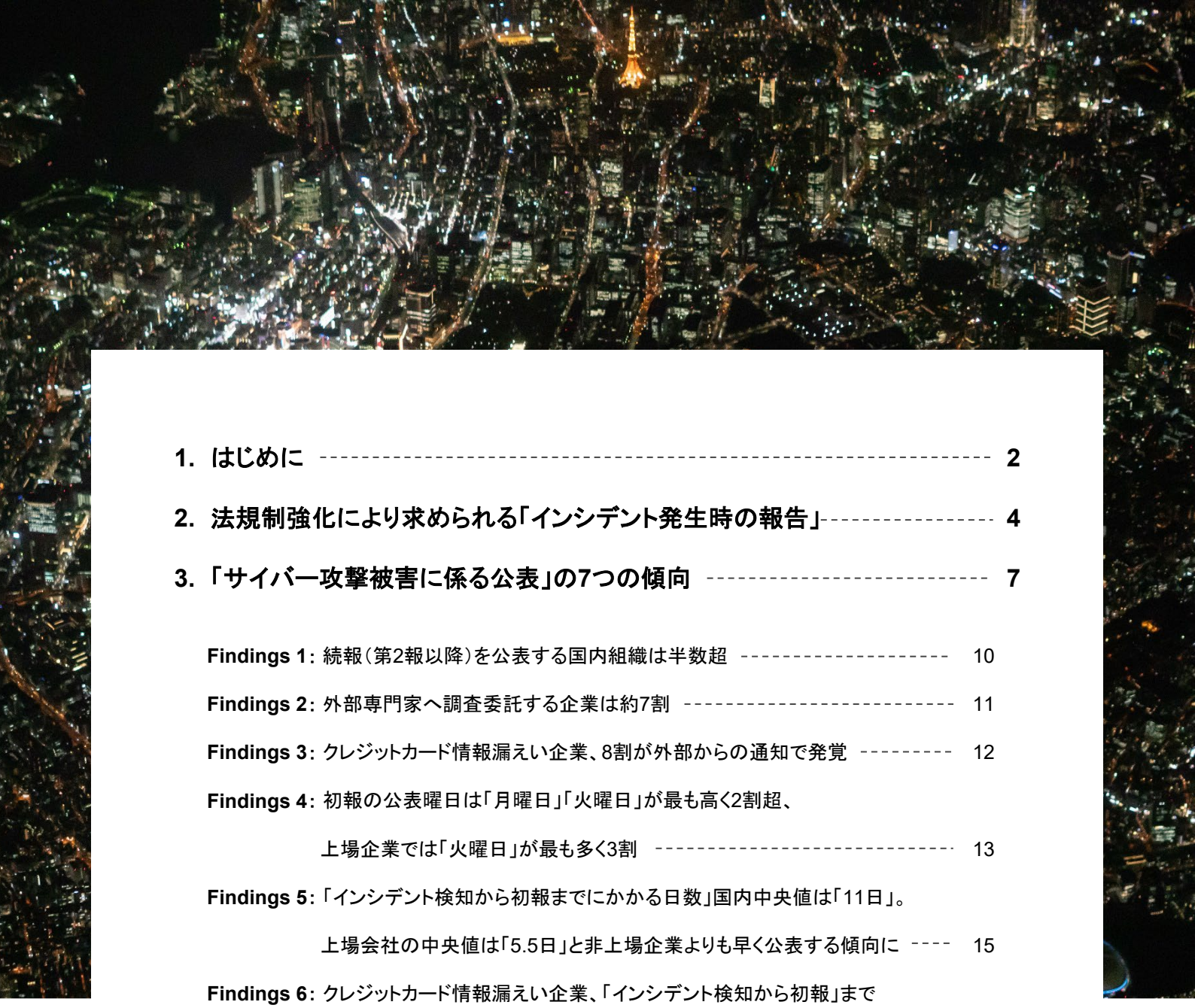
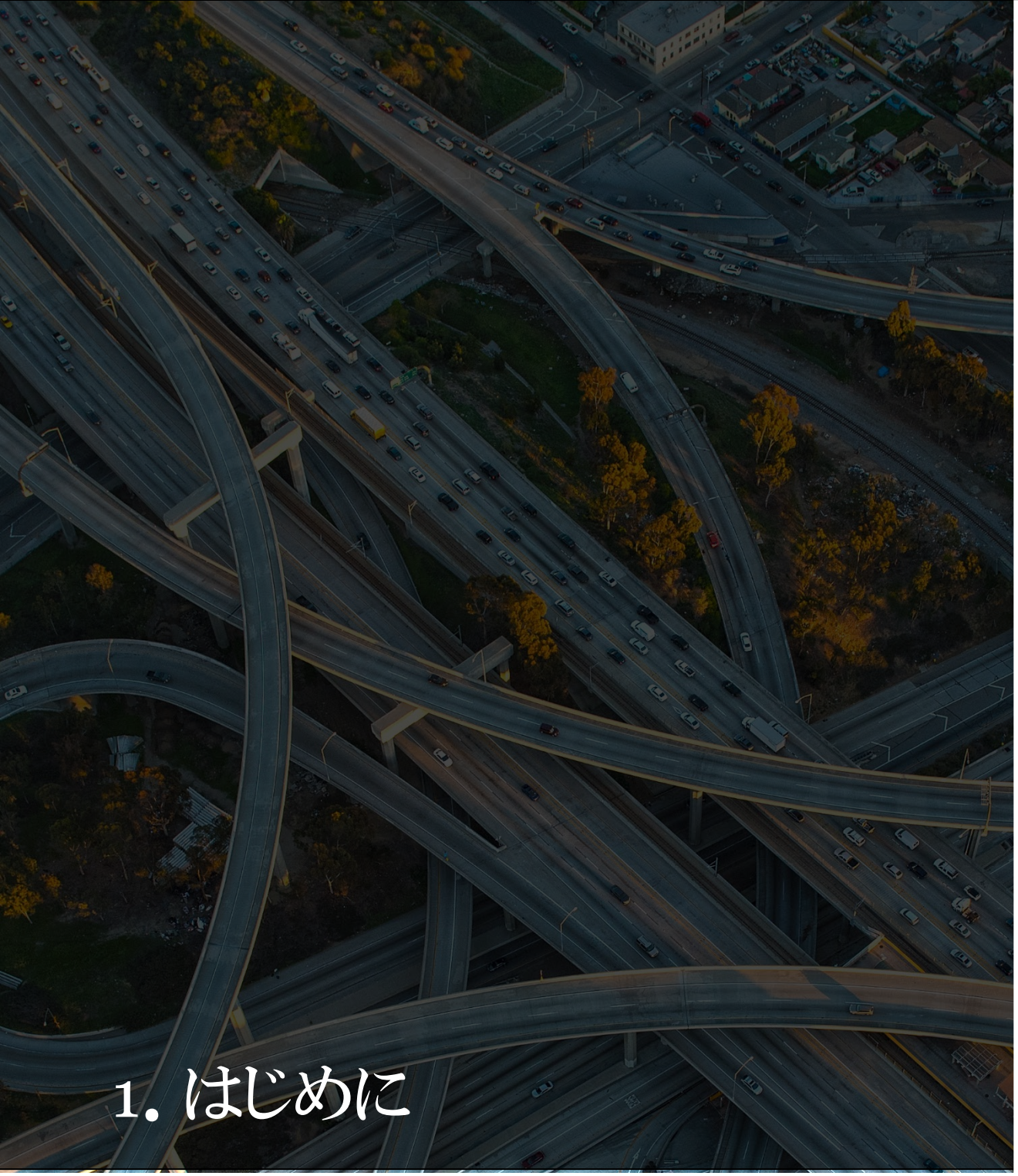
「サイバー攻撃被害に係る公表」に関する国内組織実態調査2023

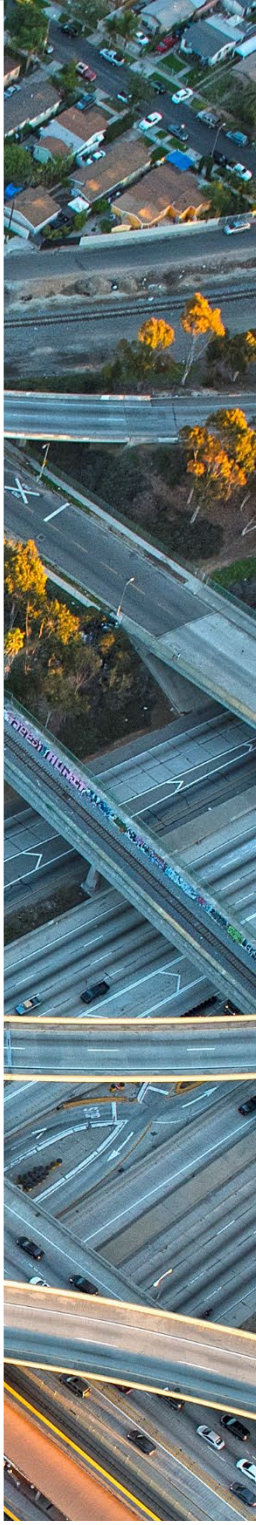
―上場企業はインシデント検知後1週間以内に初報を公表―

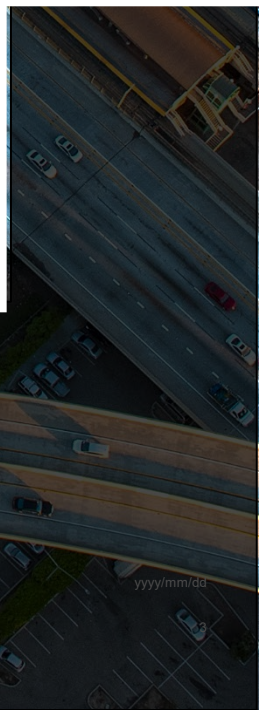
PwCコンサルティング合同会社





1. はじめに





1. はじめに

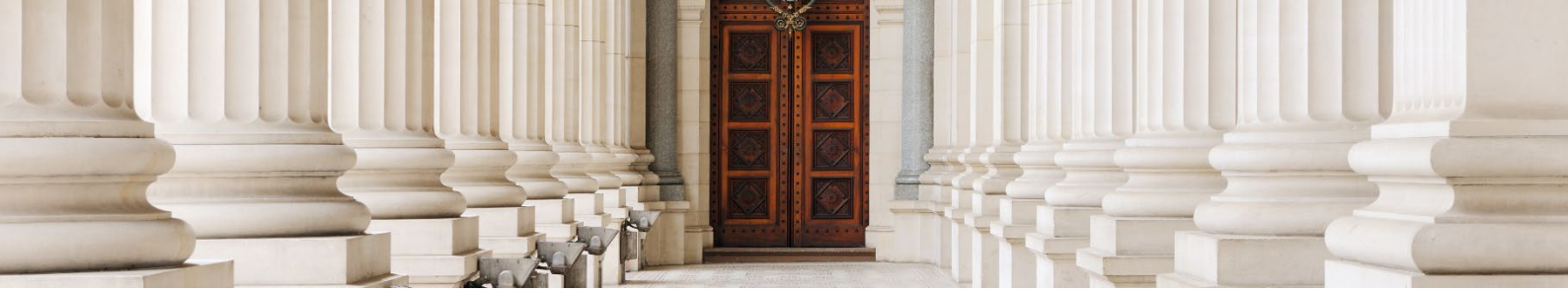
ビジネスへのサイバー脅威が高まる中、サイバー攻撃被害（以下「インシデント」）時に情報を公表することは、ビジネスへの影響や風評被害を軽減する上で非常に重要です。

今後、国内組織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に留め、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難しいです。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ました。

本レポートでは、①国内外のインシデント発生時の報告に関する法規制動向、②2021年10月から2022年9月までに確認された主要な国内インシデント公表事例194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。

本調査が、皆様が自組織のインシデント公表に係る施策を講じる上で参考になれば幸いです。

2. 法規制強化により求められる「インシデント発生時の報告」



2. 法規制強化により求められる「インシデント発生時の報告」

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、とりわけ海外での動きが活発になっています（図表1）。

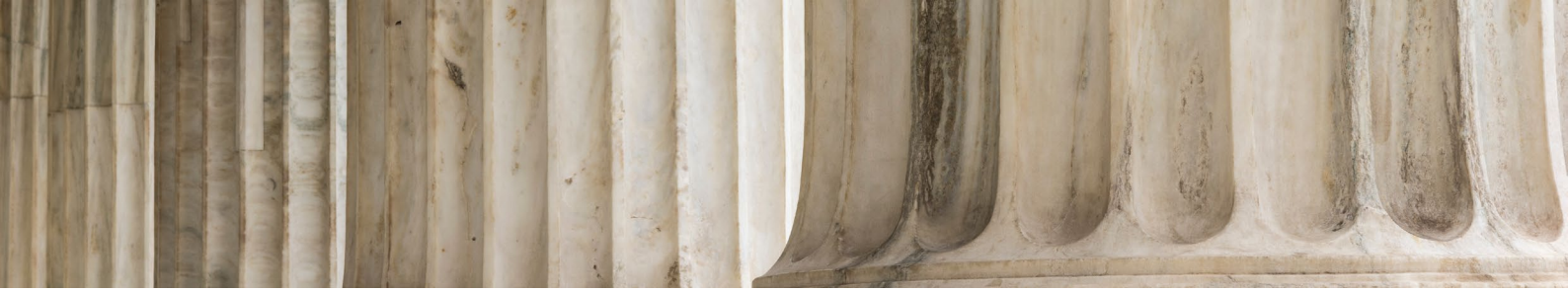
例えば、米国では「重要インフラサイバーインシデント報告法2022（CIRCIA）[1]」により重要インフラ事業者は、重大なインシデントを認識してから72時間以内、ランサムウェアに感染し身代金を支払った場合は、身代金支払い後24時間以内に米国サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）への報告が求められています。また、米国証券取引委員会（SEC）においては、公開会社に対して重大なインシデント報告を求める規則の検討を行っています。[2]

欧州では、2022年末に改正された「NIS2指令[3]」において、インシデントが組織の事業に混乱をもたらす、または財産的損失を被るなど一定のビジネス影響を及ぼす場合には、24時間以内に欧州ネットワーク情報セキュリティ庁（ENISA）への報告を求めています。また、2016年4月27日に制定された「EU一般データ保護規則（GDPR）[4]」では個人情報の漏えいを認識してから72時間以内の報告が要求されています。さらに、現在審議中であるIoT製品セキュリティ分野に焦点を当てた「欧州サイバーレジリエンス法案[5]」では、悪用される脆弱性やインシデントを知り得てから24時間以内にENISAに通知することを規定しています。

また、インシデント報告について具体的な時間を規定する動きはAPACの国・地域に広がりつつあります。例えば、オーストラリアでは、2021年「重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）」の改正[6]において、重要インフラの責任事業体に対して重大なインシデントを認識してから12時間以内に、またその他関連インシデントについては認識してから72時間以内に当局への報告を義務付けています。また、インドでは「Cyber Security Directions of 28th April 2022[7]」においてインシデントを認識してから6時間以内に報告するよう規定しています。さらに中国では、具体的な時間規制は設けていないものの、2017年の「中国サイバーセキュリティ法[8]」で速やかなインシデント報告を求めています。日本においても、個人情報保護法[9]に基づき、報告対象事態を認識してから速やか（概ね3～5日以内）に個人情報保護委員会へ報告、本人へ通知することが求められています。また、2023年3月8日には、サイバーセキュリティ協議会に設置されたサイバー攻撃被害に係る情報の共有・公表ガイダンス検討会[10]より「サイバー攻撃被害に係る情報の共有・公表ガイダンス[11]」（以下「検討会ガイダンス」という）が公表されるなど、当局への報告だけでなく公表の必要性についても国内政府や有識者間で議論されています。

今後グローバルにおいてインシデント報告の義務化はさらに進むと思われます。

1. Congress.gov, “H.R.2471 - Consolidated Appropriations Act, 2022”（2022/3/15） https://www.congress.gov/bill/117th-congress/house-bill/2471/text
2. Securities and Exchange Commission, “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure”（2022/3/23） https://www.sec.gov/rules/proposed/2022/33-11038.pdf
3. The European Union, “Network and Information Security 2 Directive”（2022/12/14） https://eur-lex.europa.eu/eli/dir/2022/2555/oj
4. European Commission, “REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016”（2016/4/27） https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
5. PwC「欧州サイバーレジリエンス法案（EU Cyber Resilience Act）概説～日本の製造業への影響と最低限押さえるべき要点～」（2022/10/21） https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/eu-cyber-resilience-act.html
6. Parliament of Australia, “Security Legislation Amendment（Critical Infrastructure）Bill 2021” https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6657
7. Ministry of Electronics & Information Technology, Government of India, “Cyber Security Directions of 28th April 2022” https://www.cert-in.org.in/Directions70B.jsp



図表1：主要各国におけるサイバーインシデント報告に関する主な法規制

国	年	根拠とする法規制	報告の基準	報告義務
米国	2021年	Ransomware Guidance[12]	インシデント発生後72時間以内に米国ニューヨーク州金融サービス局（NYDFS）へ報告	○
	2022年	重要インフラサイバーインシデント報告法2022（CIRCIA）	インシデント発生後72時間以内、ランサムウェア身代金支払い後24時間以内にCISAへ報告	○
	提案中	Form 8-K[13]	重大なインシデントを4営業日以内にForm 8-Kを用いて米国証券取引委員会（SEC）へ報告	—
欧州	2016年	EU一般データ保護規則（GDPR）	漏えいを認識してから72時間以内に監督当局へ報告	○
	2022年	NIS2指令	重大なインシデントを把握してから24時間以内に早期警告、72時間以内にインシデント通知、1か月以内に最終報告書を提出	○
	審議中	欧州サイバーレジリエンス法案	悪用される脆弱性や、サイバーインシデントを認識してから24時間以内にENISAへ通知	–
中国	2017年	中国サイバーセキュリティ法	提供する製品やサービスにセキュリティ上の欠陥や脆弱性が見つかった場合には、直ちに対処し、当局へ報告	○
オーストラリア	2021年	重要インフラ安全保障法（Security of Critical Infrastructure Act 2018）の改正	重要インフラ責任事業体は重大なサイバーインシデントの発生を認識してから12時間以内に、またその他関連サイバーインシデントについては発生を認識してから72時間以内に当局へ報告	○
インド	2022年	Cyber Security Directions of 28th April 2022	サイバーインシデントを認識してから6時間以内に報告	○

8. PwC「中国サイバーセキュリティ法のポイントと日本企業が講じるべき対策」（2022/5/16）
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/china-cyber-security.html
9. 政府インターネットテレビ「個人データの漏えい等事案と発生時の対応について」（2022/3/8）「4.報告義務の主体、速報・確報について」12:50,（閲覧日：2023/3/8 19:21）
https://nettv.gov-online.go.jp/prg/prg24040.html
10. サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会事務局：警察庁、総務省、経済産業省、サイバーセキュリティ協議会事務局（NISC及び政令指定法人JPCERT/CC）
11. サイバーセキュリティ協議会・サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（2023/3/8），
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html
12. New York State Department of Financial Services, “Re: Ransomware Guidance”（2021/6/30）
https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance
New York Codes, Rules and Regulations, “23 CRR-NY 500.17 Notices to superintendent”（2021/6/30）
https://govt.westlaw.com/nycrr/Document/I60c644590d5f11e79781d30ba488e782?transitionType=Default&contextData=%28sc.Default%29
13. U.S. SECURITIES AND EXCHANGE COMMISSION “FACT SHEET Public Company Cybersecurity; Proposed Rules”（2022/3/9） https://www.sec.gov/files/33-11038-fact-sheet.pdf, https://www.sec.gov/news/press-release/2022-39

国	年	根拠とする法規制	報告の基準	報告義務
日本	2022年	個人情報の保護に関する法律施行規則[14]	報告対象事態を認識してから速やか（概ね3～5日以内[15]）に個人情報保護委員会へ報告、本人へ通知	○
	2023年	サイバー攻撃被害に係る情報の共有・公表ガイダンス	具体的ないつまでに公表すべきという記載はないものの、サイバーセキュリティ協議会やJPCERT/CCやISACなど業界団体への情報共有、公表に関する内容やタイミングを紹介	―

このように、国内外でインシデントに関する報告規制が強まる一方で、2023年に公表したPwCの調査[16]によると、グローバル企業3,522社のうち「インシデントに関する開示要件を問題なく満たせる」と回答した企業は、たった9%にすぎませんでした。この結果から、世界をリードするグローバル企業においてすら、有事における情報開示の設計は決して容易でない、もしくは十分に検討がなされていないことが読み取れます。

14. e-gov「個人情報の保護に関する法律施行規則」（2022/10/1） https://elaws.e-gov.go.jp/document?lawid=428M60020000003
15. 政府インターネットテレビ「個人データの漏えい等事案と発生時の対応について」（2022/3/8）「4.報告義務の主体、速報・確報について」12:50,（閲覧日：2023/3/8 16:21） https://nettv.gov-online.go.jp/prg/prg24040.html
16. PwC「サイバー有事に備えたCxO結束の必要性『Global Digital Trust Insights 2023年版』調査結果より」（2023/1） P.8参照。 https://www.pwc.com/jp/ja/knowledge/thoughtleadership/2023/assets/pdf/cxo-unity-in-preparation-for-cyber-emergencies.pdf

3.「サイバー攻撃被害に係る公表」の7つの傾向

3.「サイバー攻撃被害に係る公表」の7つの傾向

本調査は、2021年10月から2022年9月末までにCISO Cyber Concierge[17]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194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2022年10月から2023年3月末までの半年間に続報（第2報以降）の有無を追跡調査したものです（図表2）。これらの調査結果として、以下7つの傾向が明らかになりました（図表3）。

図表2：調査対象とするインシデント公表事例

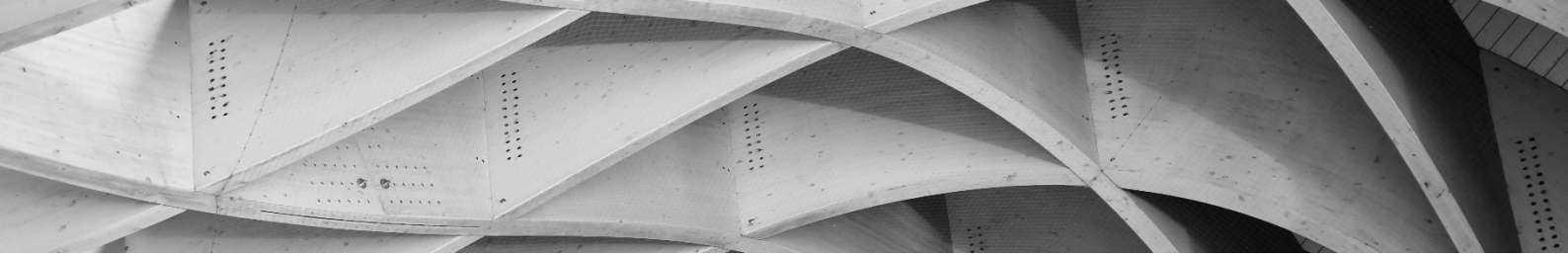
	フェーズ	調査対象期間	調査の説明
A	本調査	2021年10月1日～2022年9月30日	A調査期間にCISO Cyber Conciergeに掲載されたインシデント公表事例（194件）[18]の記載内容やタイミングについて調査
B	追跡調査	2022年10月1日～2023年3月31日	Aで対象としたインシデント公表事例（194件）に対し、続報（第2報以降）が公表されているかを調査

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	1. 続報（第2報以降）を公表する国内組織は半数超 2. 外部専門家へ調査委託する国内組織は約7割と多数派 3. クレジットカード情報漏えい企業、8割が外部からの通知でインシデントが発覚
公表タイミングにおける傾向	4. 初報の公表曜日は「月曜日」「火曜日」が最も高く2割超、上場企業では「火曜日」が最も多く3割 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「11日」。上場企業の中央値は「5.5日」と非上場企業よりも早い傾向 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
公表内容の傾向	7.「対応状況」「今後の対応」記載の割合は、比較的少ない傾向

17. 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

18. 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。



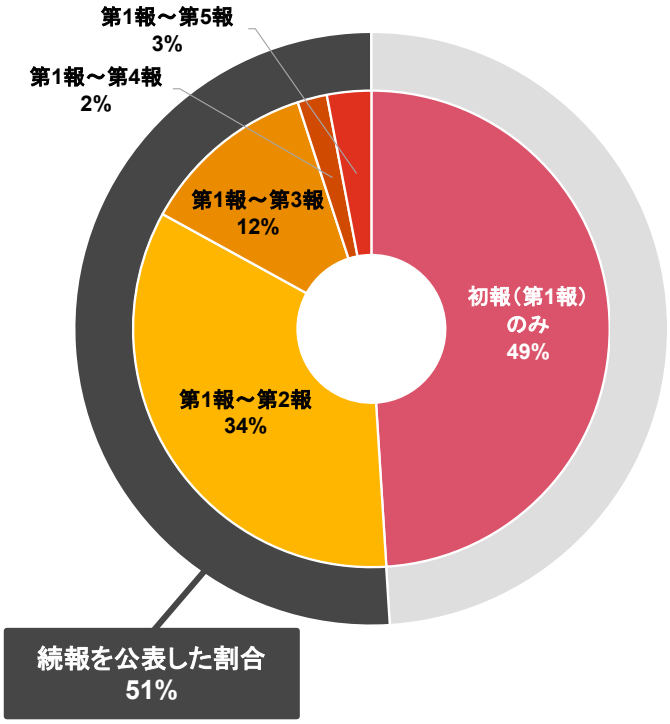
公表事例からみる企業の傾向

Findings 1：続報（第2報以降）を公表する国内組織は半数超

インシデント公表事例（N=194）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49%、「第1報から第2報まで」を公開した国内組織は全体の51%、「第1報から第3報まで」は12%、「第1報から第4報まで」は2%、「第1報から第5報まで」は3%存在していることが分かりました。

また、「初報（第1報）まで」の公表事例をみると、図5に示すように「企業向けビジネス（B2B）を営む企業」では、全てが完了して公表する場合や「被害の種類」によっては、続報が不要の場合もあることが分かりました。

図表4：インシデント1件あたりの公表回数（N=194）



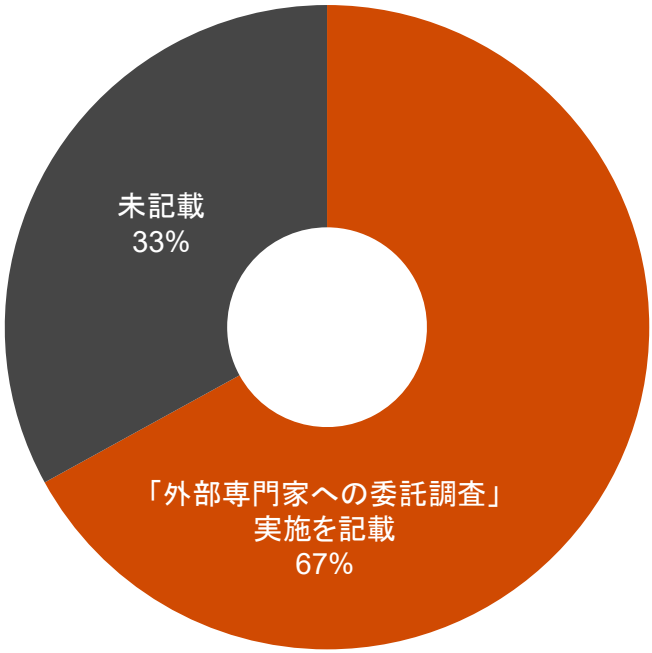
図表5：公表事例からみる傾向

カテゴリ	事例
初報のみの公表事例の傾向	• 企業向けビジネス（B2B）を営む企業において、全ての調査が完了してから公表をする公表事例は多い（利害関係者には事前に情報共有し、不要な風評被害を避ける点において良いと考える）。 • 被害の種類（例：ビジネスメール詐欺（BEC）やフィッシング詐欺）によっては続報がない場合も多い。

Findings 2：外部専門家へ調査委託する企業は約7割

インシデント公表事例（N=194）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67%に上りました。多くのインシデントを経験する国内組織において、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（図表6）。このことから、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、窓口の開設をしておくことを検討すると良いでしょう。

図表6：「外部専門家への委託調査実施」記載の有無（N=194）



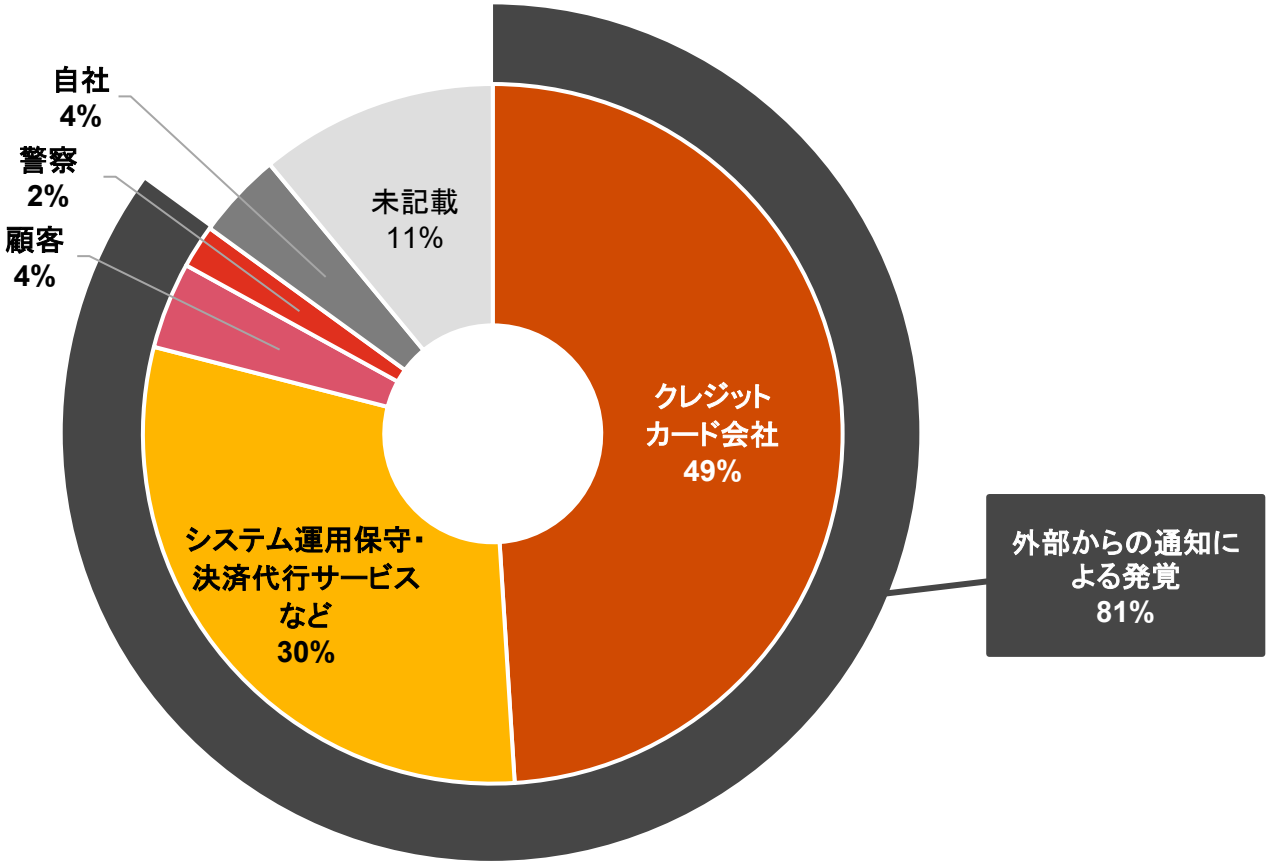
Findings 3：クレジットカード情報漏えい企業、8割が外部からの通知で発覚

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＝47）をみると、「発覚者の記載」は全体の9割でした。

まず、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85%、「自社による発覚」が4%、「未記載」が11%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特定できていない傾向にあることが分かります（図表7）。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49%、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30%、「顧客」が4%、「警察」が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は、セキュリティ能力の高いシステム会社の選定や定期的なセキュリティ診断、継続的なモニタリングサービスをセキュリティ専門企業と契約するなどし、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言えます。

図表7：クレジットカード情報漏えいにおける発覚者の割合（N=47）



公表タイミングにおける傾向

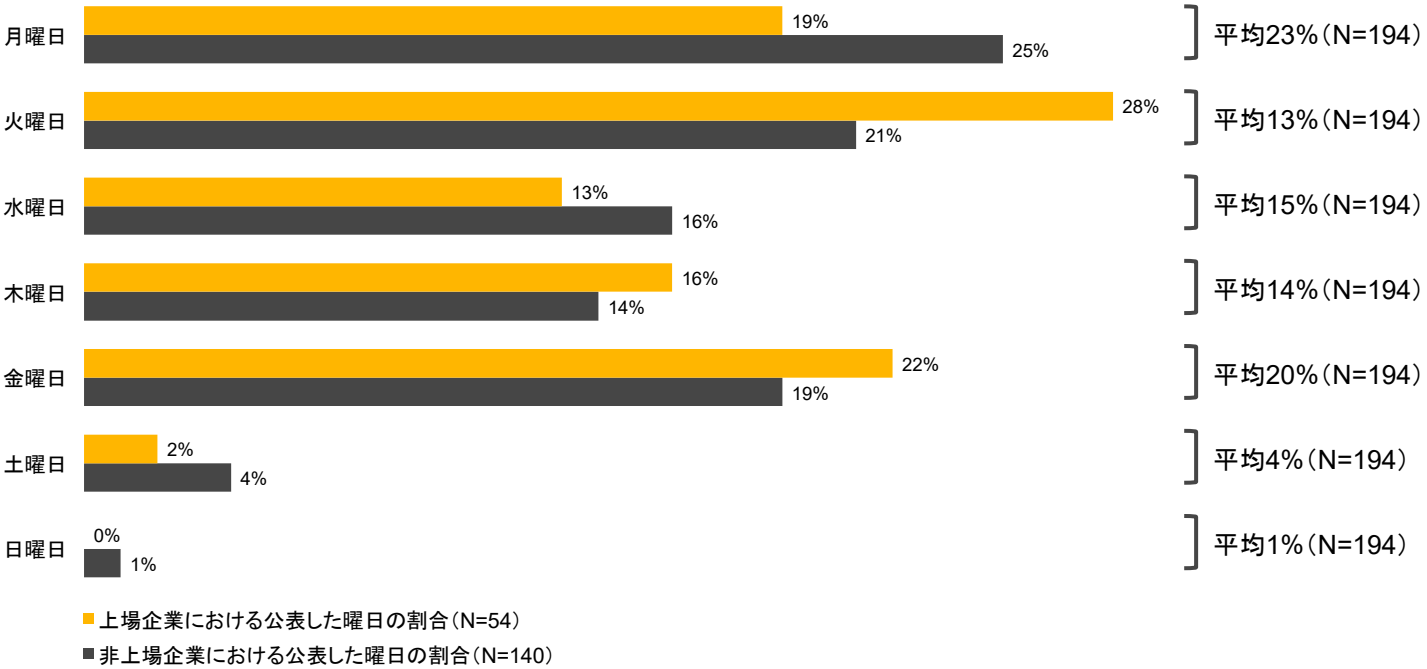
Findings 4：初報の公表曜日は「月曜日」「火曜日」が最も高く2割超、上場企業では「火曜日」が最も多く3割

インシデント公表事例（N=194）における初報（第1報）の公表日を曜日別にみると、「月曜日」および「火曜日」が最も多く全体の23%、次いで「金曜日」が19%、「木曜日」が14%の順となりました（図表8）。

また、「土曜日」や「日曜日」など休日の公表事例も5%存在しますが、これらの公表事例の多くは消費者向けビジネス（B2C）を営む傾向にあり、インシデント検知当日または少なくとも2日以内に公表していました。このことから、B2Cを営む企業においては、平日・休日関係なく、消費者への影響を最小限とするために、できるだけ早いタイミングでインシデント公開する傾向にあることが分かります。

さらに、上場有無で分析すると、上場企業の初報（N=54）の曜日では「火曜日」が最も多く28%、次いで「金曜日」が22%、「月曜日」が19%、「木曜日」が16%、「水曜日」が13%、「土曜日」が2%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=140）においては、「月曜日」が最も多く25%、次いで「火曜日」が21%、「金曜日」が19%、「水曜日」が16%、「木曜日」が14%、「土曜日」が4%、「日曜日」が1%の順となりました。

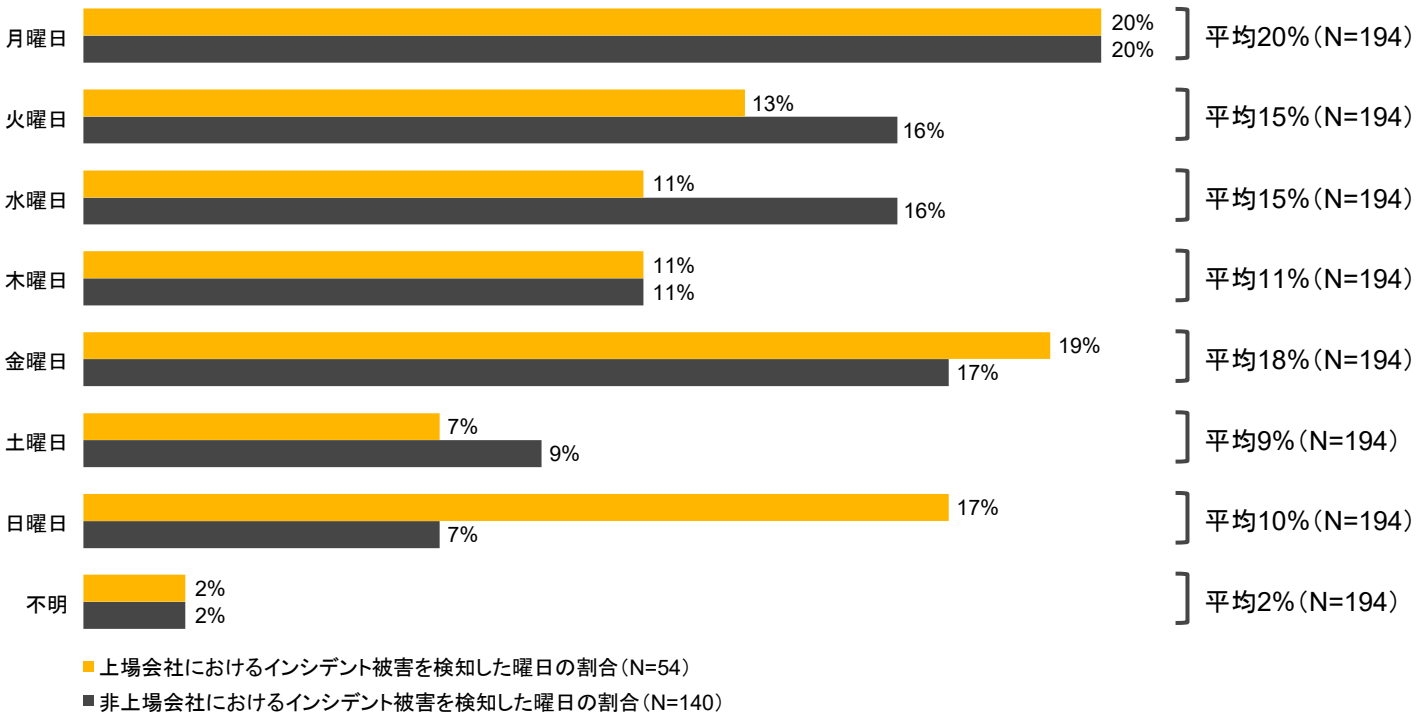
図表8：インシデント被害を公表（初報）した曜日の割合（N=194）
（上場会社および非上場企業との比較）



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=194）におけるインシデントを検知した曜日は、「月曜日」が最も高く20%、次いで「金曜日」が18%、「火曜日」「水曜日」が15%、「木曜日」が11%、「日曜日」が10%、「土曜日」が9%の順となりました（図表9）。「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約6割を占めることから、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と言えます。

また、インシデントを検知した曜日を上場有無で分析すると、おおよそ同じような傾向ですが「日曜日」に差を確認しました。上場企業のインシデント公表事例（N=54）では「日曜日」に検知した割合は17%だったのに対し、非上場企業のインシデント公表事例（N=140）では7%と、10ポイントの差が現れました。

図表9：インシデント被害を検知した曜日の割合（N=194）
（上場会社平均および非上場企業との比較）

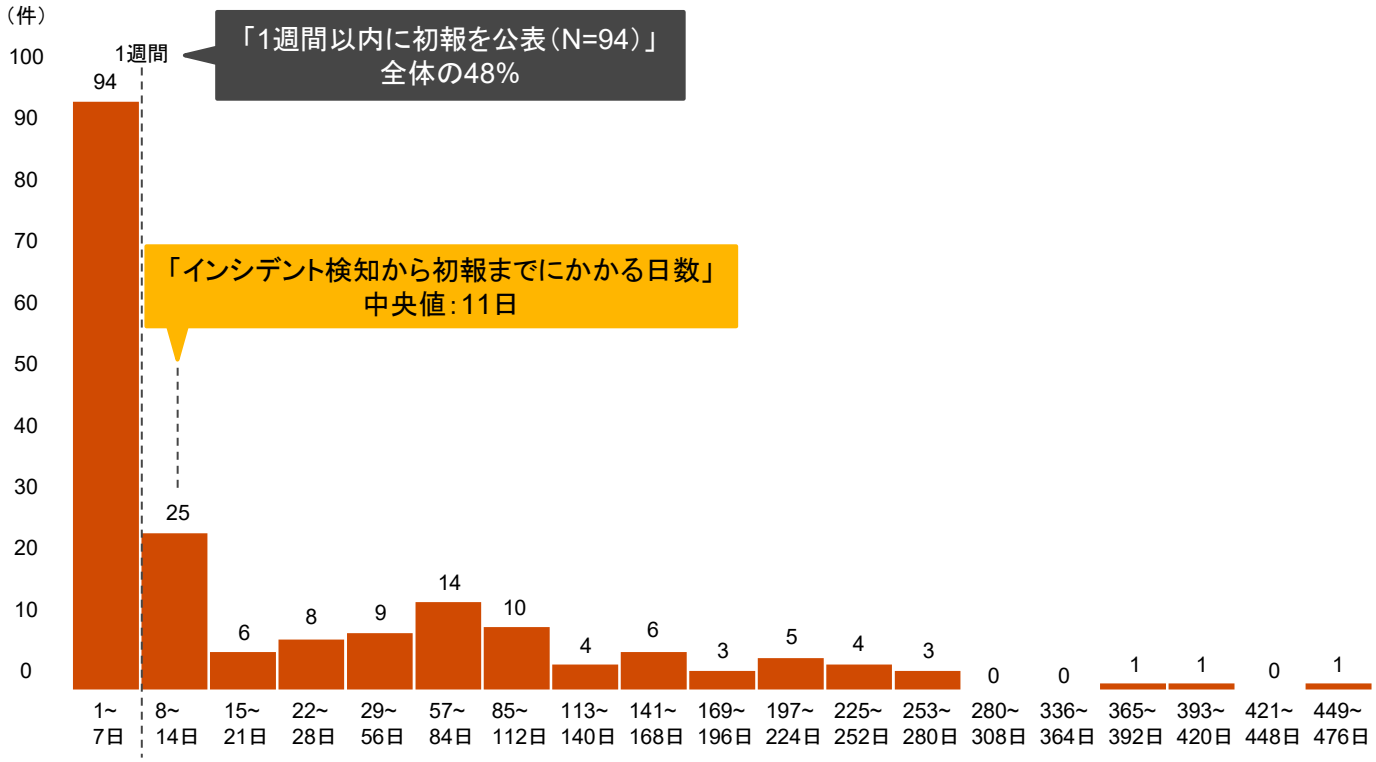


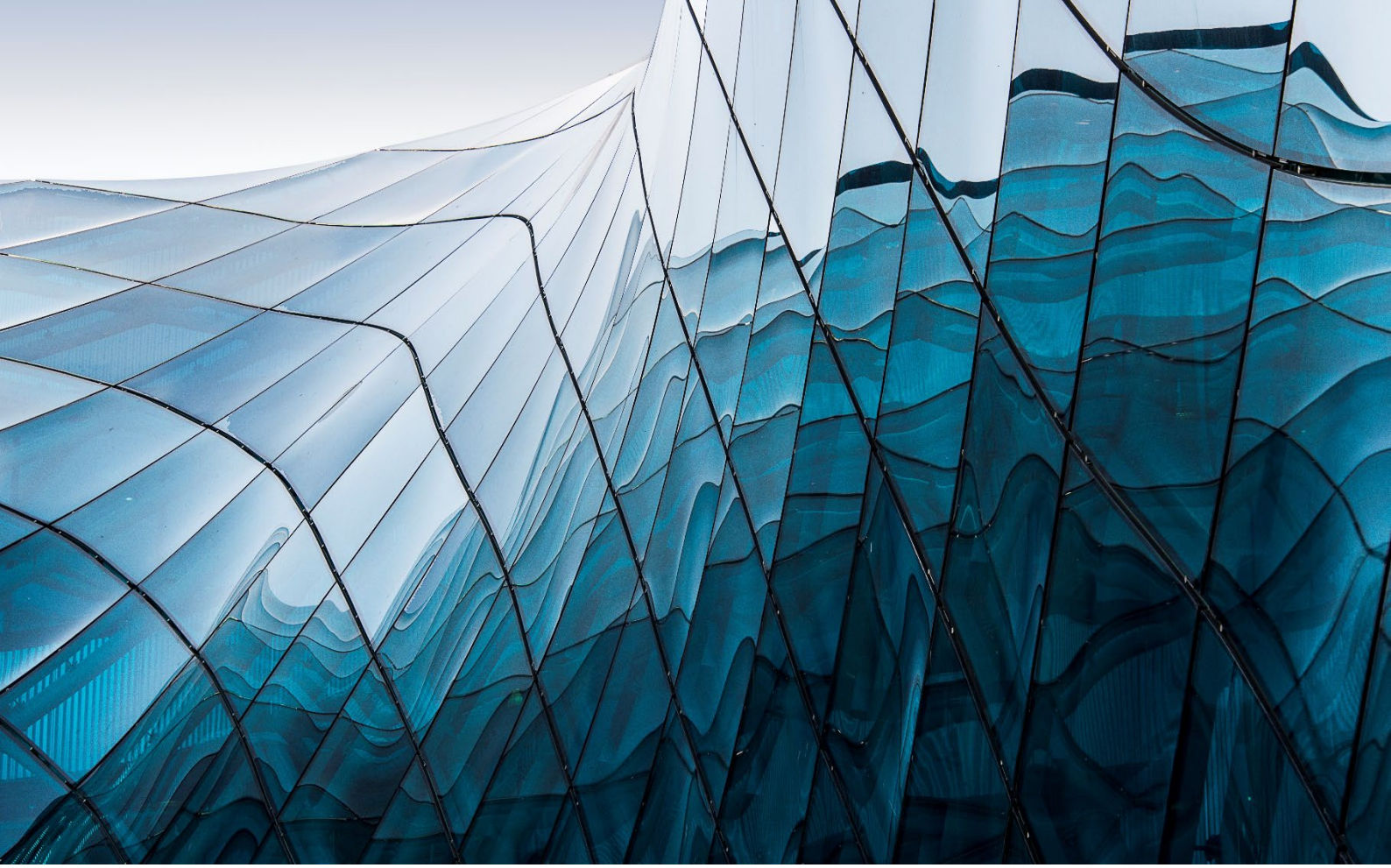
Findings 5:「インシデント検知から初報までにかかる日数」国内中央値は「11日」。上場会社の中央値は「5.5日」と非上場企業よりも早く公表する傾向に

インシデント公表事例（N=194）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「11日間」で、全体の約半数が1週間以内（1～7日以内）に公表していることが分かりました（図表10）。

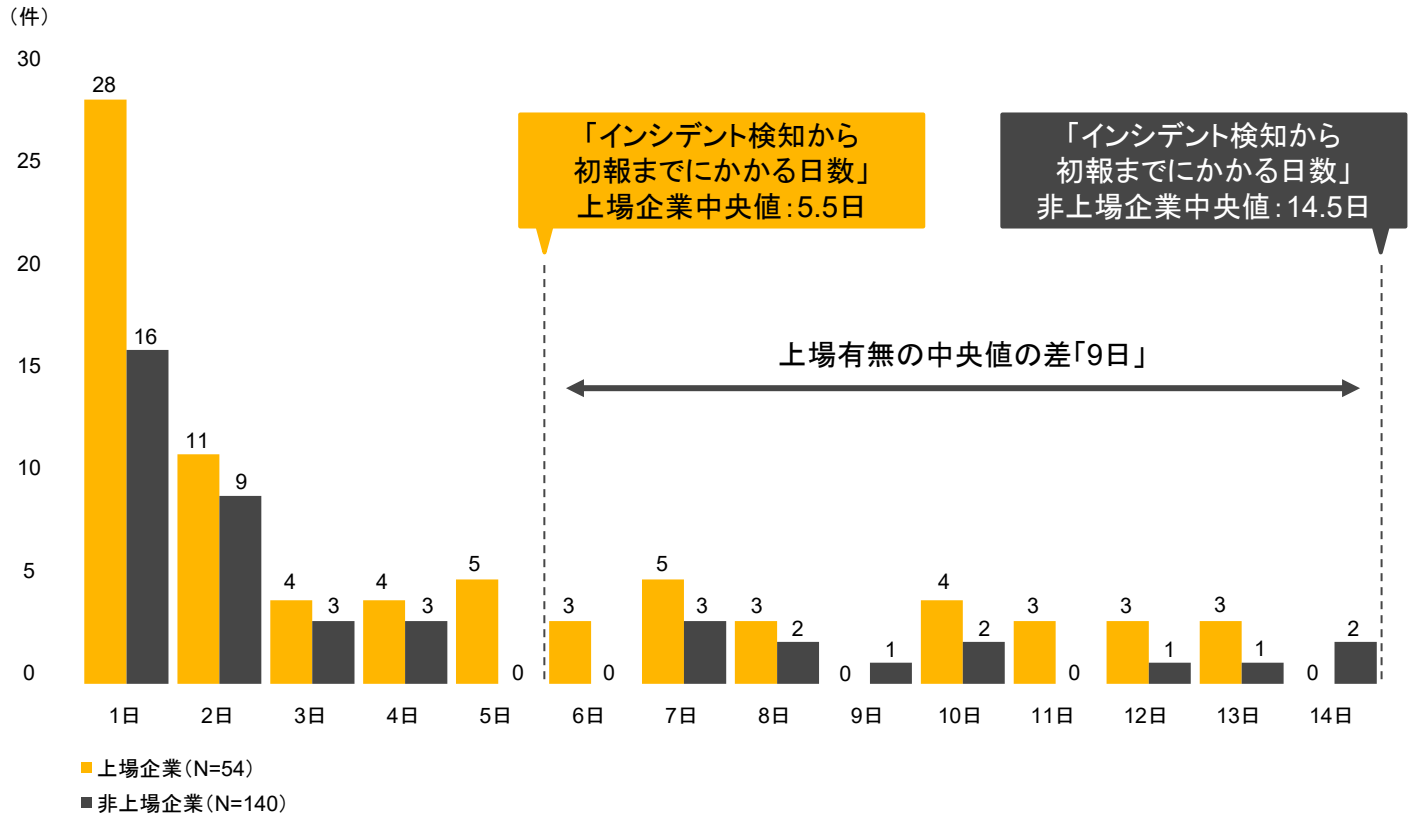
また、上場有無で分析すると、上場企業のインシデント公表事例（N＝54）では初報までの中央値は「5.5日」、非上場企業のインシデント公表事例（N=140）の中央値は「14.5日」と、上場会社は非上場企業と比較し中央値が9日早かったことが分かりました（図表11）。

図表10：インシデント検知から初報までにかかる日数とその件数（N=194）





図表11：インシデント検知から初報までにかかる日数とその件数における上場企業、非上場企業の比較
（検知後2週間以内を抜粋）

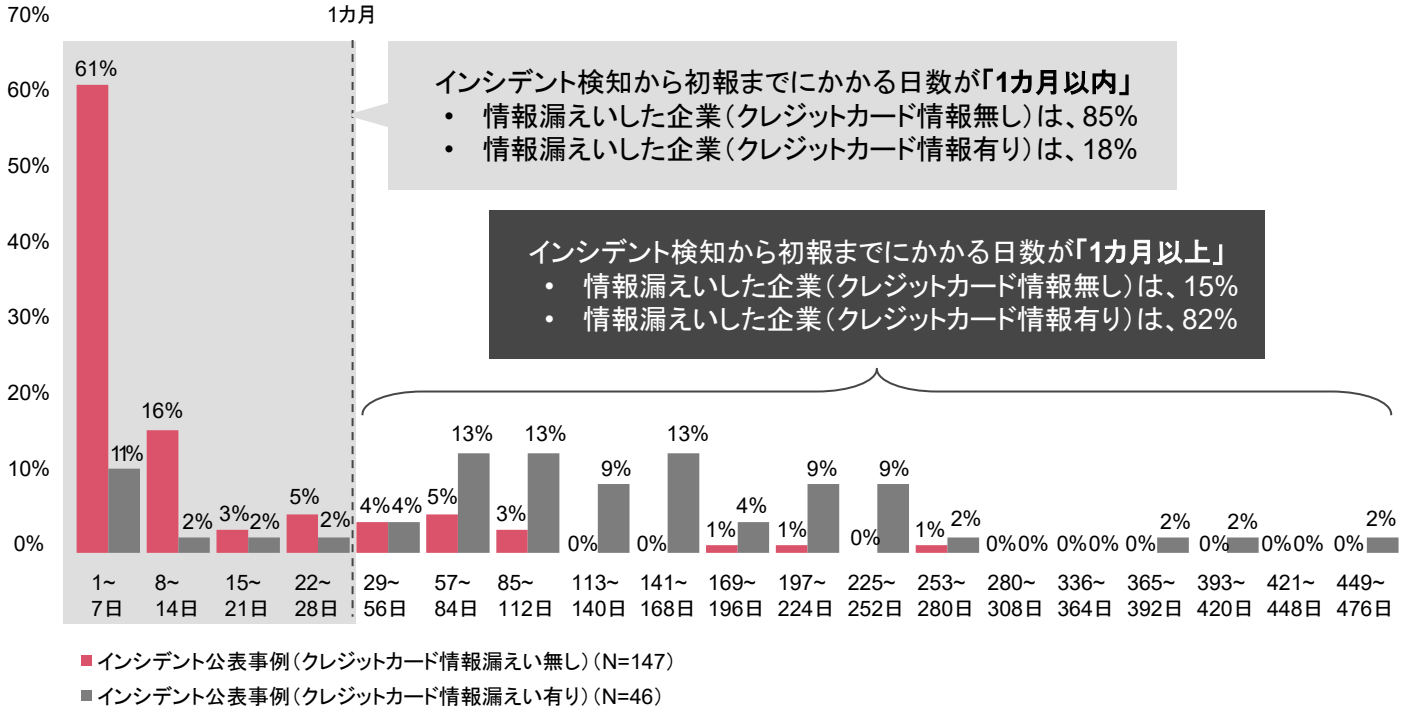


Findings 6：クレジットカード情報漏えい企業、「インシデント検知から初報」まで1カ月以上有する企業が8割超

さらに、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12）。

インシデント公表事例（N=194）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=147）では、「7日以内」に公表する国内組織が最も多く61%、「8～14日以内」は16%、「15～21日以内」は3%、「22～28日以内」は5%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85%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[19]（N=47）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11%、「8～14日以内」「15～21日以内」「22～28日以内」はそれぞれ2%と、1カ月以内に公表した企業は2割に満たず、公表に1カ月以上要する事例が全体の8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。

図表12：インシデント検知から初報までにかかる日数と報告件数の割合における「クレジットカード情報漏えい」の記載有無



19. 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

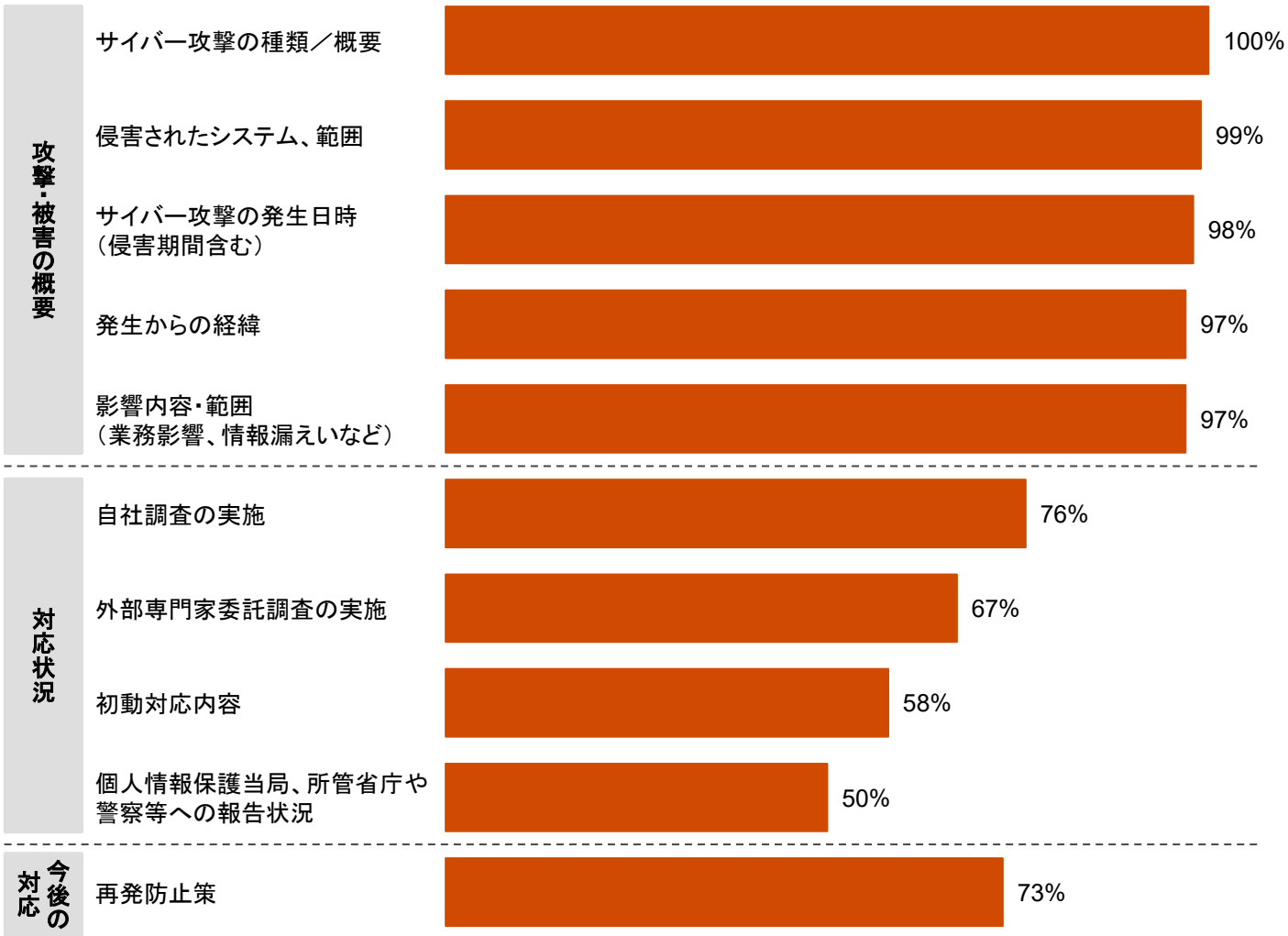
Findings 7:「対応状況」「今後の対応」記載の割合は、比較的少ない傾向

インシデント公表事例（N=194）の記載内容を「攻撃・被害概要」「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」関連項目は多くの事例で記載を確認できましたが、「対応状況」や「今後の対応」の関連項目記載は「攻撃・被害概要」よりも少ない傾向にあることが分かりました（図表13）。

まず、「攻撃・被害概要」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」において、全項目で97%以上記載されており、国内組織はインシデント公表内容において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76%、「外部専門家委託調査の実施」が67%、「初動対応内容」が58%、「個人情報保護当局、所管省庁や警察等への報告状況」は50%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73%となりました。

これらの傾向から、国内のインシデント公表事例も、検討会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。また、検討会ガイダンスでは、検知から公表までにある程度の日数を要した場合はレピュテーションリスクを下げないための配慮として対応経緯を含めて公表することを推奨していますが、インシデント公表事例においても、公表が遅れた場合に「公表が遅れた経緯」を記載する組織は一定数（24%）存在しており、顧客など利害関係者への不安解消のための配慮としてグッドプラクティスの一つと言えます（図表14）。

図表13：インシデント公表事例からみる主な記載項目（N=194）



※主な記載項目は、サイバーセキュリティ協議会・サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会「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

図表14：公表事例からみる傾向（記載内容）

カテゴリ	事例
検知から公表までに時間を要した事例の傾向	• 公表が遅延した場合「公表が遅れた経緯」を記載する事例が一定数存在した。
見せ方の傾向	• B2Cでは、プレスリリースとは別に顧客用のFAQページを掲載していることが多い（膨大となりうる顧客からの問い合わせ数への対応、顧客の不安を解消する目的に適う効果的な施策と考える）。 • B2Cでは、インシデント経緯一覧をWebサイトのHome画面に掲示し、閲覧者に対し一目で進捗状況が分かるようにしている事例もある（透明性を図る上で良い対応と言える）。 • B2Cでは、続報の内容について、調査進捗を続報として公表する事例だけではなく、顧客のセキュリティ向上の施策として希望顧客へ無料で多要素認証やセキュリティサービスを提供することを公表する事例もある（顧客ロイヤルティを維持するには後者は良い対応であると言える）。 • 通達する問い合わせ先には、顧客対応だけでなくマスコミ対応の窓口を併記する傾向にあるが、記載していないケースも多々みられる。
公表削除の傾向	• 公表から一定期間後、当該情報を削除する組織は少なくはない。 • インシデント公表内容をWebサイトから削除したものの、SNS公式アカウントの公表が削除されていないケースもみられた。 • インシデント公表自体は削除せず、他のプレスリリースを大量に発することで当該公表が埋もれている事例もみうけられた。

4. インシデント公表事例からみる国内組織への推奨事項

4. インシデント公表事例からみる国内組織への推奨事項

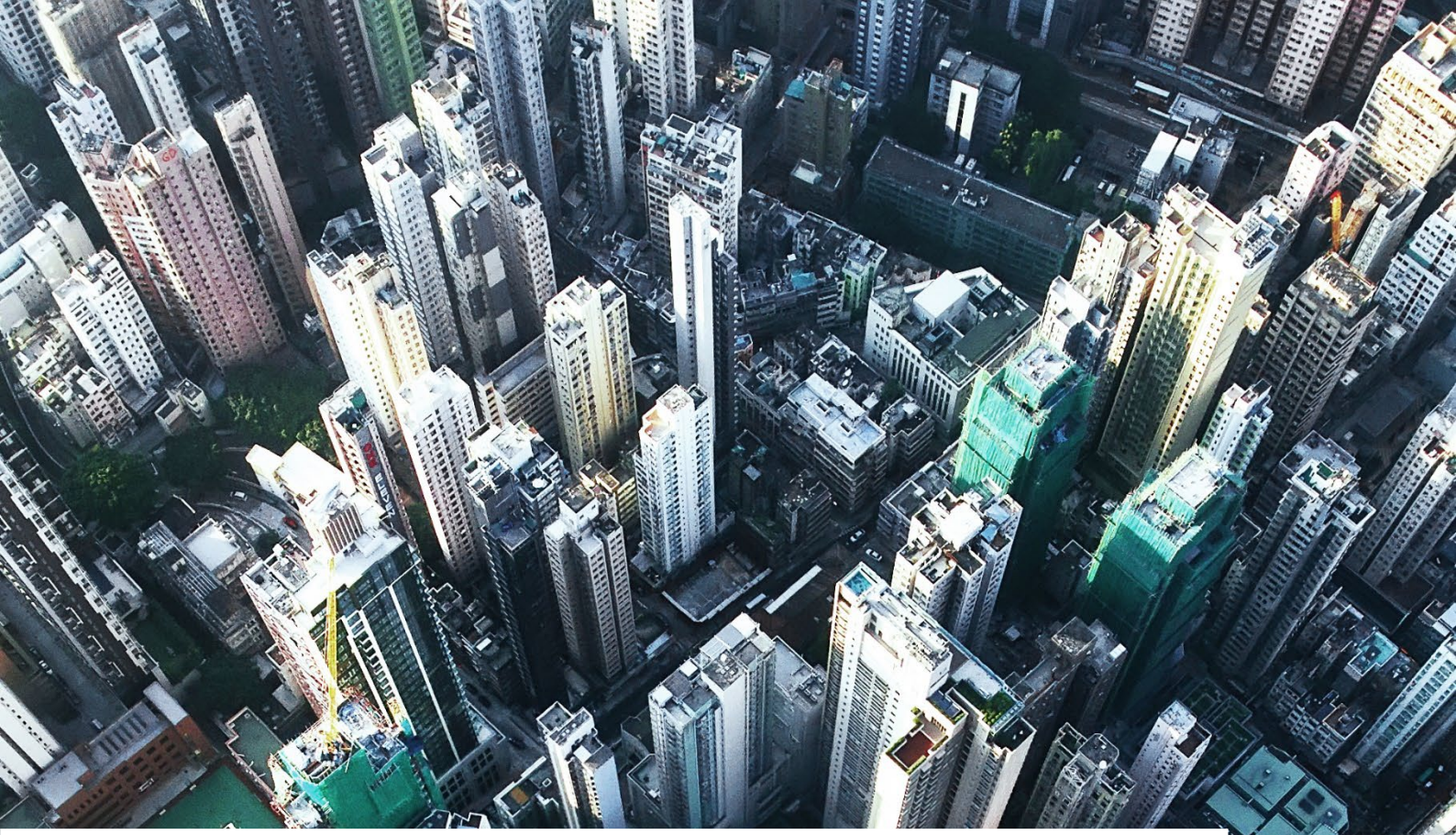
今回の調査において、インシデント公表事例における7つの傾向を示しました。この傾向から国内組織が検討すべき推奨事項を以下に記載します（図表16）。

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検討会ガイダンス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16：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」

7つの傾向		推奨事項	
公表事例からみる国内組織の傾向	1.続報（第2報以降）を公表する国内組織は半数超 2.外部専門家へ調査委託する国内組織は約7割と多数派 3.クレジットカード情報漏えい企業、8割が外部からの通知でインシデントが発覚	**【上場企業は、インシデント検知から1週間以内に公表】** 公表事例からみると、上場企業では1週間以内に公表する傾向があることから、2週間以上経過後に公表する場合は、一般的には「公表が遅い」という印象を与える可能性があります。 **【公表が遅れる場合は、経緯を示す】** 公表までに2週間以上、時間を要する場合は、遅れた経緯が分かるよう示すことを推奨します。	公表タイミング
公表タイミングにおける傾向	4.初報の公表曜日は「月曜日」「火曜日」が最も高く2割超、上場企業では「火曜日」が最も多く3割 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「11日」。上場企業の中央値は「5.5日」と非上場企業よりも早い傾向 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	**【続報の必要有無は、つど検討】** 続報を公表する組織は半数以上でしたが、必ずしも続報が必要なケースばかりではありませんでした。このため、セキュリティ責任者は、回数にはとらわれず、攻撃手法や被害に応じて、必要なタイミングで必要な情報を必要なステークホルダーへ開示することをつど検討して公表していくことが求められます。	
公表内容の傾向	7.「対応状況」「今後の対応」記載の割合は、比較的少ない傾向	**【公表内容には「対応状況」も記載】** 半数以上が「攻撃・被害概要」だけでなく「対応状況」も記載するため、「対応状況」が未記載の場合、株主などへ情報不足の印象を与える恐れがあります。「サイバーセキュリティ経営ガイドライン（指示10）[20]」で参照する検討会ガイダンスにも記載項目として挙げられるため「対応状況」は記載すべきです。 **【最終報には「今後の対応」を記載】** また、最終報においては組織のセキュリティに対する姿勢を示すために「今後の対応」を記載することを推奨します。	公表内容
		【インシデント対応者が自社の場合、可能な限り記載】 「誰」がインシデントを検知／初動対処／調査を実施したか開示傾向にあります（外部専門委員会設置時は「誰」が委員か）。このため、活動主体を明確化することは一般的で、外部へ透明性を図るため重要です。特に自社で対応した活動は、自社のセキュリティ能力の高さが正しく外部評価されるためにも、「主体」を明記することを推奨します。	

19. 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」（2023/3/24） https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf



5. 調査概要

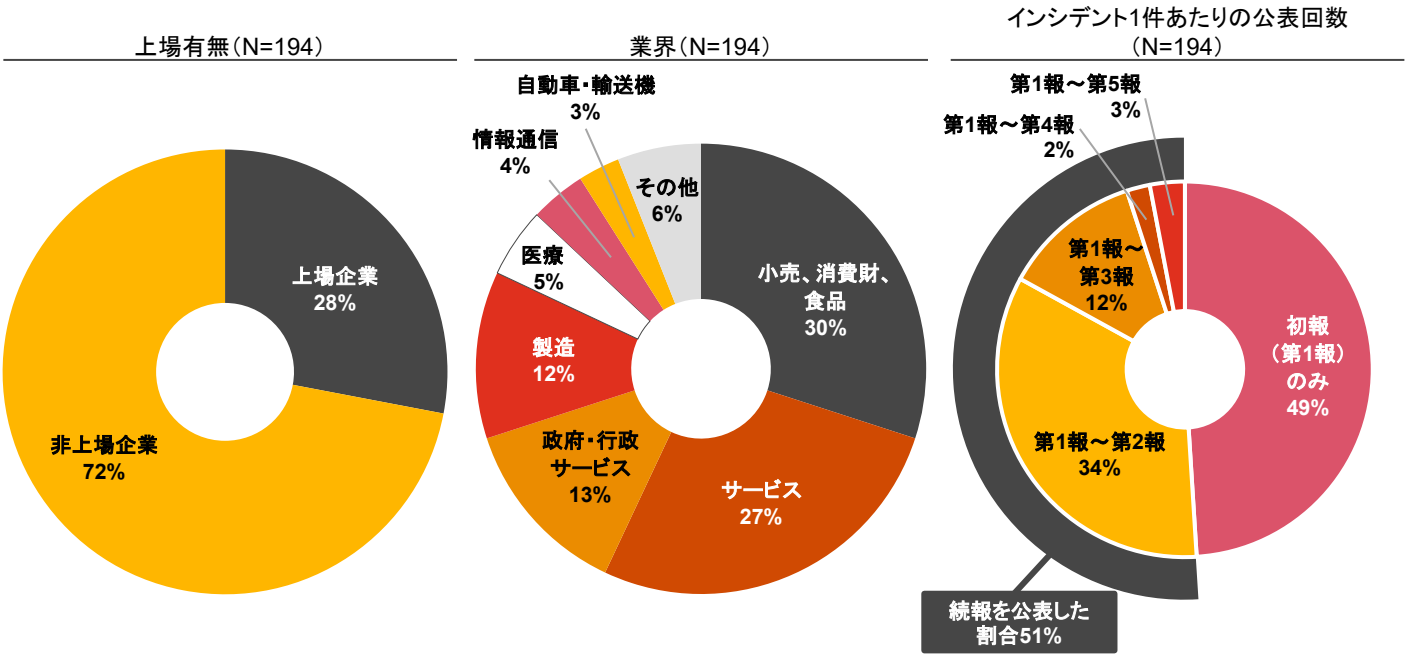
5. 調査概要

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2023
調査対象	【本調査】 2021年10月1日2022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194件 【追跡調査】 2022年10月1日～2023年3月31日までに公開された「インシデント公表事例194件」の続報（第2報以降）
調査期間	2021年10月～2023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=194）の属性は以下のとおりです。上場有無については、上場会社が28%、非上場企業が72%でした（図表17：左）。業界別にみると「小売、消費財、食品」が最も多く30%、次いで「サービス」27%、「政府・行政サービス」が13%、「製造」が12%、「医療」が5%の順に多くなりました（図表17：中央）。また、インシデント1件に対する公表件数の割合は、「初報（第1報）のみ」が49%、「第2報以降」は51%、「第3報以降」は17%、「第4報以降」は5%となりました（図表17：右）。

図表17：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）



お問い合わせ先

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

監修

丸山 満彦
PwCコンサルティング合同会社
パートナー

執筆

上杉 謙二
PwCコンサルティング合同会社
ディレクター

エレドン ビリゲ
PwCコンサルティング合同会社
マネージャー

愛甲 日路親
PwCコンサルティング合同会社
シニアアソシエイト

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あらた有限責任監査法人、PwC京都監査法人、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、監査およびアシュアランス　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9,400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156カ国に及ぶグローバルネットワークに285,000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。

電子版はこちらからダウンロードできます。www.pwc.com/jp/ja/knowledge/thoughtleadership.html

発刊年月：　2023年4月

I202303-15 rev.1