RESEARCH

業界別サイバーエクスポージャーレポート：日経 225 銘柄企業

By Rapid7 Labs

June 3, 2020

はじめに

サイバーセキュリティ脅威が増大している中で、「サイバーエクスポージャー」対策への集中的な取り組みと、その費用対効果の重要性は以前よりも増して高まってきています。Rapid7 のリサーチチームがまとめたレポートでは、サイバーエクスポージャーを「インターネットに接続されたサービスにおける外部公開設定の弱点」と定義しています。

業種別にサイバー攻撃に対するレジリエンス（耐性）について正確に把握しておくことは非常に重要です。なぜなら、より正確なコストモデルを構築し、全業種でもっとも軽減が必要なサイバーエクスポージャーに標的を絞るだけでなく、官民の協力活動の絆を強めてユーザーや企業の保護が強化できるからです。業種別のサイバーエクスポージャーを測定することで、サイバーセキュリティ情報とセキュリティ脅威の調査結果を収集し公開している各機関への情報提供が可能となるからです。

とりわけ、日本においてはご存知の方が少ないとは思われますが、Rapid7 が最新のインターネットの利用実態を反映した包括的でかつ正確な公開レポートを発行するのは、今回が 4 回目です。日本におけるサイバーエクスポージャーとレジリエンスが、現状どのレベルにあるのかを把握するために、Rapid7 Labs は、日経 225 銘柄企業[1]の 2019 年第 2 四半期におけるインターネットセキュリティの現状を測定し、以下の点について業種別の統計的なデータを明らかにしました。

- 全体の攻撃面（サイバーエクスポージャーのあるサーバ/デバイスの台数）
- 危険またはセキュリティが確保されていないサービスの存在
- フィッシング防御ポスチャ
- 外部公開サービスとメタデータ設定の弱点
- 接続されたサードパーティの Web サイトへの依存のリスク

上記のサイバーセキュリティを測定することで、調査した各業種においてもっとも共通性のある問題に絞り込み、それぞれの点における防御ついて実践的で具体的なアドバイスが可能となりました。

今回、明らかになった弱点について考察する上で重要なのは、日経 225 銘柄企業が、一般的に IT やセキュリティを含め幅広い分野の業務で優秀な人材を確保できる企業である点です。そのような一流企業においてサイバーエクスポージャーのあるサービスに、さまざまな弱点が発見されるということは、外部公開のインターネットに対して少ない人材しか投入できない中小企業において、さらに重大なサイバーエクスポージャーやリスクが存在している可能性を示唆しています。

今回の調査により以下の点が明らかになりました。

- 日経 225 銘柄企業は、平均 107 台のサーバ/デバイスの攻撃面が攻撃可能な状態にさらされています。あります。また多くの企業が 750 台以上のシステム/デバイスを公開しています。
- 評価した日経 225 銘柄企業の 196 社 （全体の 87%）が、外部公開メールのプライマリドメイン設定で、アンチフィッシング防御（DMARC など）を実施していないか、もしくは実施していても弱点があり、 13 社（6%）が不正なレコード設定をしています。これは、これまで発行した Rapid7 の業種別サイバーエクスポージャーレポート（ICER）の中で、アンチフィッシングに関してはもっとも弱点が大きいという結果となりました。[2]
- 全体の 18%の日経 225 銘柄企業において、メインの Web サイトで SSL/TLS セキュリティ対応がされていません。これにより、通信時に Web コンテンツの改ざんが可能なため、サイト訪問者はさまざまな一般的で破壊的な悪意ある攻撃に晒されています。
- 各業種において、少なくとも 1 社はマルウェアに感染しています。IT とコンシューマ製品の業種の企業においては、毎月一定して感染の兆候が確認されています。業種全体としてのインシデントは、企業のリソースに対する DoS 増幅攻撃にまで及ぶものから、WannaCry や NotPetya に類似した EternalBlue ベースのキャンペーンの兆候にまで多岐にわたります。
- 日経 225 銘柄の全業種の企業で、どのクラウドサービスをいくつ利用しているか外部公開の DNS のメタデータから検知できます。46 社が 2〜5 社のクラウドサービスを利用しています。この情報により、他の方法と比較して非常に効率的で標的を明確にした攻撃が可能です。
- Telnet や Windows SMB ファイル共有のような深刻な脆弱性を持つサービスは、ごくわずかな企業のみにサイバーエクスポージャーがあります。これは良い点です。
- すべての業種で殆どの企業が、インターネットに接続されたシステムにおいて、古いソフトウエアに依存したサービスにサイバーエクスポージャーがあります。

---

[1] *日経 225 銘柄リスト：*

https：//indexes.nikkei.co.jp/en/nkave/index/component?idx=nk225 （2019 年 8 月 12 日時点情報）

[2] *この数字は、米国がメインのフォーチュン 500 企業において 73%であり、オーストラリアが中心の ASX 200 企業において 68%、また、英国が中心の FTSE 250 企業において 88%である。*

業種別の攻撃面

Project Sonar[3] を使用して Rapid7 がインターネットへのエクスポージャーがあるシステムやデバイスをスキャンしている方法については、本レポートの**調査方法**のセクションで詳しく説明します。日経 225 銘柄の企業は、平均で約 107 のサービスにサイバーエクスポージャーがあります。この数字は、良いか悪いかを判断するものではありません。しかし、サイバーエクスポージャーのあるそれぞれのノードは企業の攻撃面を増やし、潜在的に攻撃者にとっての足がかりを増やしています。別の言い方をすると、サイバー攻撃のリスクを減らすためには、サイバーエクスポージャーのあるサーバやデバイスを正しく設定し、管理しパッチを当て防御する必要があるのです。サイバーエクスポージャーのあるサービスが、いつバランスを崩してリスクを生むかについては、明確な判断基準がありません。これは、インターネットへのエクスポージャーがあるリソースをどの程度防御できるかが、複数の要因に依存しているからです。しかし、防御機能に関わらずサイバーエクスポージャーのあるシステムが多いほど、攻撃者により多くの攻撃のチャンスが与えられます。

図 1： 検出された企業のアセットの業種別の分布（それぞれの点は、各企業を表しています。横軸は、検出されたアセット数。）

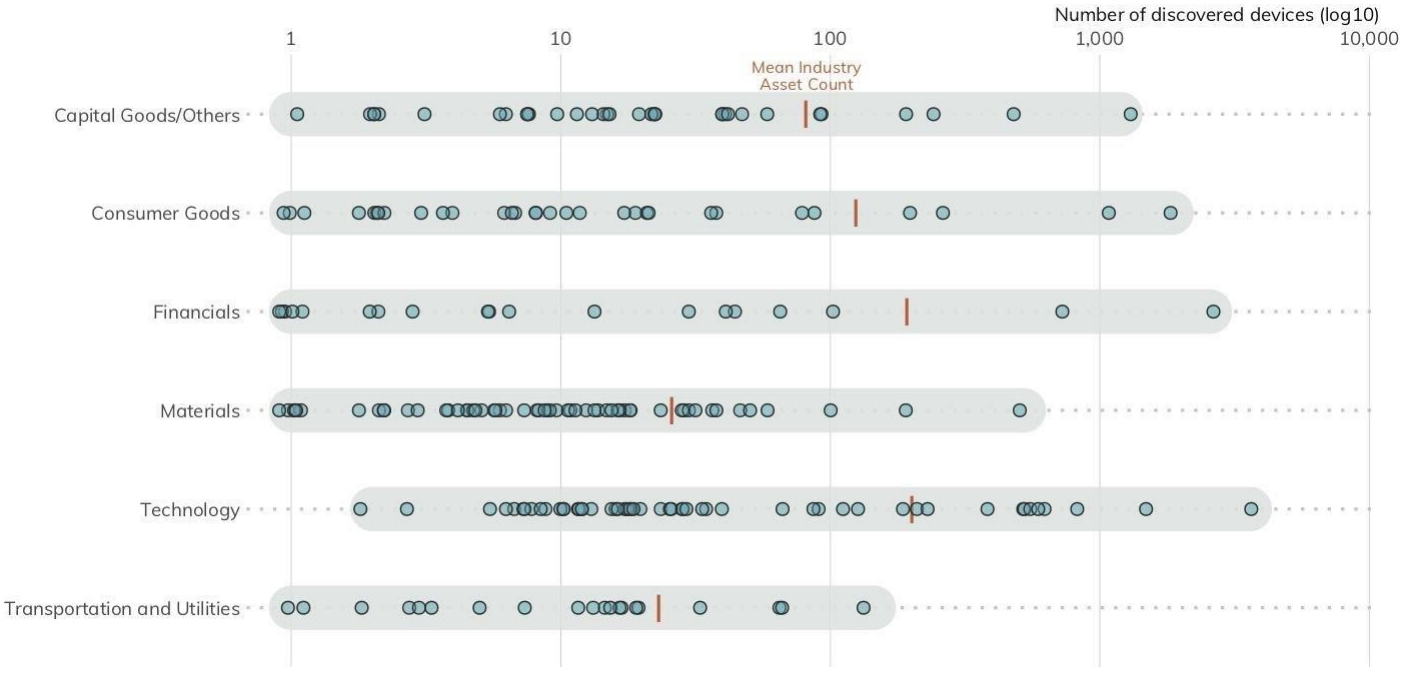


図 1 を見ると、1,000 以上のアセットが検出されている特出した値が 4 つあります。Capital Goods（資本財）、Consumer Goods（消費財）、Financials（金融）にそれぞれ 1 つと、Technology（テクノロジー）に、1 つ存在しています。事業プロセス上、サイバーエクスポージャーのあるアセットを増やす必要がないのであれば（これらの企業はそうであるかのように見受けられますが）、脆弱性の管理やパッチングと管理に関する業務プロセスを開始する必要があり

ます。これは、発見された弱点や、企業のサービスに侵入する攻撃者の試みに迅速に対応する必要があるからです。業務プロセスで必要であることがサイバーエクスポージャーの直接の理由でなかったり、スムースなアセットの特定が不可能だったりしている中で、設定管理のプロセスが徹底されているのであれば、IT とセキュリティの業務強化計画の一環で攻撃面の削減は非常に重要な位置付けとなります。

推奨事項 攻撃面の削減。業務プロセスで必要な場合にのみ、システムやデバイスをインターネットに露出させるように企業は努力する必要があります。またアセットの識別と設定管理のプロセスを強化してサイバーエクスポージャーのあるシステムを、攻撃者にとっての企業の入り口にならないようにする必要があります。

---

[3] *Rapid7、 Project Sonar、 https：//www.rapid7.com/research/project-sonar （2019 月 8 月 12 日最終アクセス）*

フィッシング防御機能

フィッシングは、現在でも代表的な企業のサイバー攻撃ベクトルのひとつです。業種横断的に監視を行なっている団体であるアンチフィッシングワーキンググループ（APWG）では、2018 年の第 3 四半期に記録的な数字となる約 25 万件にのぼるフィッシングの報告を受けました。[4] 残念ながら、日経 225 銘柄の殆どの企業は、フィッシング攻撃に対する最新の防御対策を導入していません。[5]

調査方法のセクションで説明している通り、DNS レコードのサイバーエクスポージャーにより、ドメインベースのメッセージ認証、レポーティング、適合（DMARC）のレコードからどの程度、電子メールサービスがスパムやフィッシングから防御されているかを識別することが可能です。[6]企業は、DMARC により以下のことが可能となります。

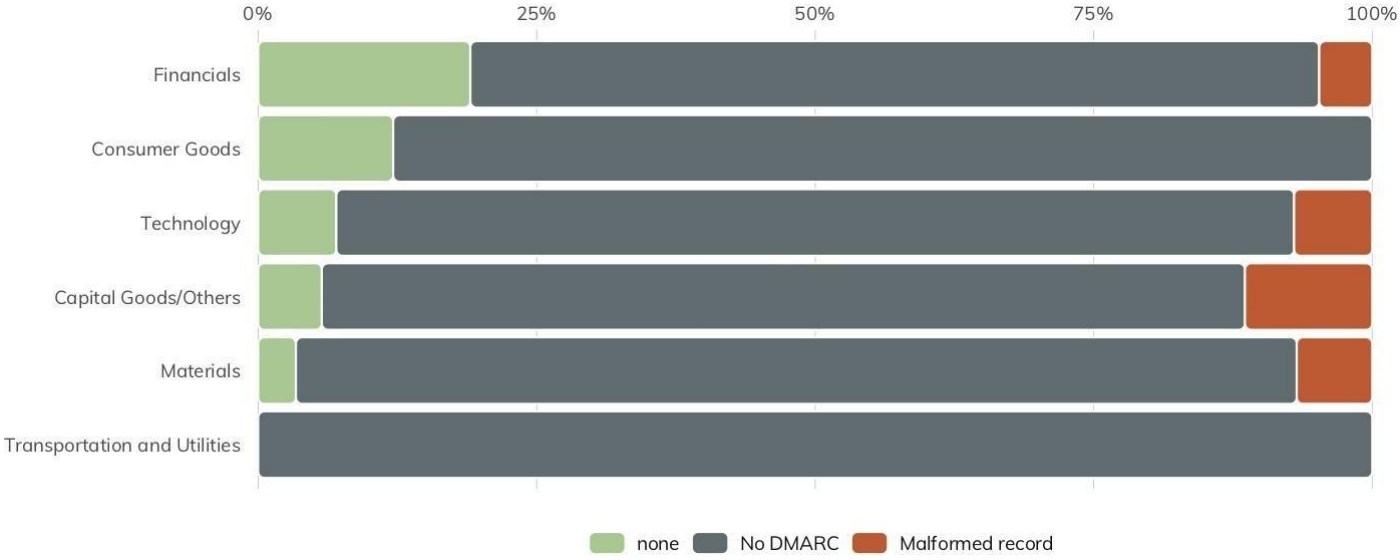
- メール認証によりメールが偽造されているかどうかの確認
- 送信元メールアドレスが正規のドメインを利用したメッセージかどうかの確認
- 認証が失敗したメッセージに対するポリシーの適用（「none（何もしない）」、「quarantine（隔離）」または「reject（拒否）」）

DMARC レコードが設定されていないか、もしくは DMARC レコードで「none」が設定されている場合、スパムやフィッシングから第一線で防御がされていないことを意味しています。しかしながら、「none」レコードは、企業がより強固なメール防御対策を講じる前段階にあり DMARC を設定中であることを示している可能性があります。

DMARC レコードを「quarantine」や「reject」で適切に設定している場合は、積極的なメール防御対策が講じられています。図 2 は、日経 225 銘柄企業の各業種の DMARC（設定カテゴリー別）の導入率を示しています。 緑の部分は、DMARC を導入しているか導入途上の企業です。残念な

がら日経 225 銘柄企業の大多数（87%）が最新の電子メールの安全性に関する設定を行なっていません。加えて、6%の企業で誤った DMARC レコードが設定されており、フィッシング攻撃のリスクが高まっています。すべての企業で DMARC で「 quarantine」もしくは「reject」設定を行なっている業種はありませんでした。

図 2：日経 225 銘柄企業のプライマリ電子メールドメインの設定から見た電子メールセキュリティ



直接スキャンを行なっている訳ではないので、DNS レコードは、Project Sonar のオプトアウトのブラックリスト（以降のセクションで説明します）には反映されていません。つまり、脆弱性サービスでアクティブスキャンを行なえば、電子メールの安全性についてさらに全貌を明らかにすることが可能なのです。本レポートの「**今後の調査**」のセクションでは、電子メールの安全性について深掘りするために、精査の範囲を広げる際に利用可能な手順について解説します。

サイバーエクスポージャーレポートで DMARC レコードの評価中に、Rapid7 Labs が同じ形式の不正な DMARC TXT レコードに複数遭遇したのはこれが初めてであることは注目に値します。 不正な形式のレコードはすべて「= spf1 <CIDR SPEC または DNS SPEC>～all」（SPF レコードで見つかると予想されるもの）の形式であり、このようになった原因は共通の技術情報が元になっているのではないかと推測されます。

推奨事項： DMARC の導入。DMARC の制御は、数年前から可能になっており、ほとんどすべての電子メールプロバイダでサポートされています。元々は、企業の外部のお客様を狙ったフィッシング攻撃への対策のために導入されましたが、DMARC には、社内の電子メールアドレスに対するスプーフィングしにくくするというメリットもあります。3 種類の DMARC ポリシーレベルを反映した適切な制限を行なう DMARC 設定を、計画し導入するには時間がかかります。[7] しかしながら、時間を投資することにより、内部と外部のセキュリティレベルの大幅な改善が可能です。

[4] *Phishing Activity Trends Report（フィッシングのトレンドに関するレポート）、 http：//docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf （2018 年 12 月 11 日）*

[5] *日経 225 銘柄リストにある企業のプライマリドメインに関する内容。DMARC は、ブランドサイトにはあるものの、前回のレポートの調査方法に一致していたのは、「vanity」ドメインでした。*

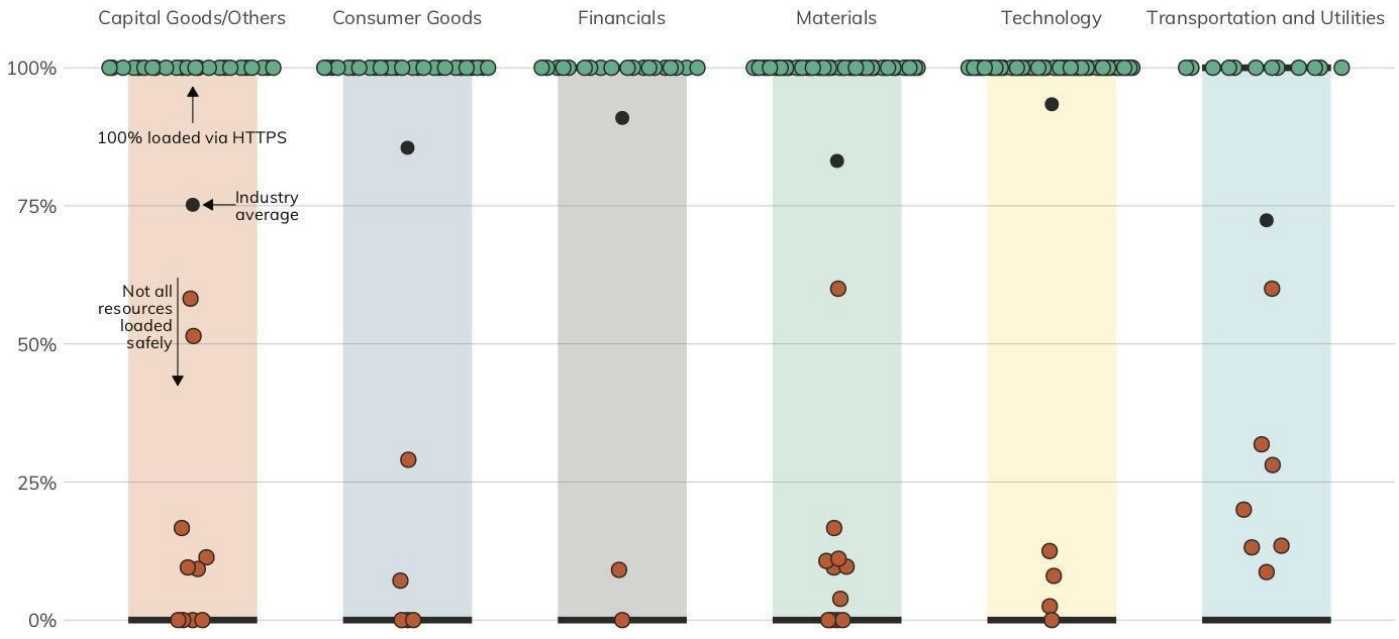
[6] *DMARC、https：//dmarc.org （2019 年 8 月 12 日にアクセスした内容に基づく）*

[7] 複雑で多様な電子メール通信の業務で、「No DMARC」から「reject」に移行するのには、18 か月は必要となると英国の NCSC が CyberUK 2019 で明言しています。

SSL/TLS の未設定

Rapid7 Labs では、多くの FTSE 企業が HTTP リクエストの自動更新を設定していないことを知り、FTSE 250+ ICER[8]企業の SSL/TLS 設定について調査を開始しました。以前、Fortune 500 と ASX 200 向けに実施した調査のデータセットでは、対象企業は、プライマリ Web サーバの設定で、もともとのリクエストが HTTP であっても、自動的に SSL/TLS を使用した（「HTTPS」などの）セッションに更新される設定を確実に行っていました。

図 3：日経 225 銘柄企業の業種別の TLS/SSL の設定状況（日経 225 銘柄企業の多く業種で、プライマリ Web サイトが自動的に HTTP のリクエストを HTTPS に更新している。訪問者を攻撃者に公開しない設定となっている。）



残念なことに、日経 225 銘柄企業の 18%近く （39 社）[9]が、HTTP リクエストの HTTPS への自動更新を行なっていません（図 3）。つまり、訪問者が中間者攻撃に晒されてしまっているのです。[10]

HTTPS への自動更新さえされていれば、HTTPS が有効になっているサイトの設定が適切だとい

う訳でもありません。図4は、精査したWebサイトのHTTPヘッダーのヒートマップです。オレンジ色のヘッダーは、削除されるべきか、最低限の情報のみを開示すべきヘッダーを示しています。攻撃者は、このようなメタデータから非常に多くの情報を得ることが可能です。

緑色は、設定が必須だと考えられるヘッダーで[11]、クロスサイトスクリプティングやサイト訪問者を勝手に誘導するiframeの悪用に対する保護に加えて、サイトから悪質なリソースがロードされる際にアラートを出すレイヤーを追加することが可能です。

図 4：セキュアなヘッダーとセキュアでないヘッダー（オレンジ色は、開示が推奨されないヘッダー）

推奨事項：HTTPSの有効化とヘッダーの適切な設定。これは、影響を受けるすべての日経225銘柄企業が、早急に修復努力を行なうべきであることを顕著に示す設定内容です。HTTPSは、著名なすべてのドメインにとって業種標準であり、多くのブラウザがはっきりとHTTPプロトコルは「安全ではありません」というテキスト表示を行なっています。[12] HTTPSを設定すると共に、サイトとサイト訪問者を安全に保つために、可能な限りの設定制御をきちんと行なってください。

---

[8] *https://blog.rapid7.com/2019/06/11/rapid7-releases-industry-cyber-exposure-report-ftse-250/（2019年6月11日）*

[9] *JavaScriptによって自動的に有効化されたプローブを4つのWebサイトが拒否*

[10] *中間者（MITM）攻撃、https://www.rapid7.com/fundamentals/man-in-the-middle-*

attacks/（2019 年 8 月 12 日に最終アクセス）

[11] *OWASP セキュアヘッダープロジェクト、https://www.owasp.org/index.php/OWASP_Secure_Headers_Project（2019 年 1 月 7 日に変更された通り）*

[12] *Google Chrome、Brave および Microsoft Edge のいくつかのバージョンなどの、Chromium ベースのすべてのブラウザが、HTTP に「安全ではありません」と表示している。加えて、Firefox などの Mozilla ブラウザは、フォームエレメントが存在している HTTP ページに「安全ではありません」と表示している。2019 年末までに、Mozilla ブラウザが Chromium ブラウザのような挙動になる見込みである。*

システムへの外部からの侵入の証拠

本レポートで収集した多くのデータは、アクティブスキャンと DNS クエリによるものです。しかし、Rapid7 では、グローバルなパッシブセンサのネットワークである Project Heisenberg も維持しています。[13]Heisenberg センサネットワークの詳しい内容は調査方法のセクションで説明しますが、簡単に言うと、このネットワークは、HTTP/HTTPS、Telnet、SMB およびその他のアドバタイズされていないサービスのハニーポットの集合体で正規のインターネットトラフィックではないことを想定しています。

図 5 は、Heisenberg センサーネットワークから業種別のすべての企業への日別のユニークな接続を示しています。このチャートは、空白になっている状態が理想です。しかしながら、本調査のデータセットでは、すべての業種で制御がされていないことが示されています。Technology（テクノロジー）や Consumer Goods（消費財）などいくつかの業種で、若干高い率でシステマティックに制御がされていないことが示されていますが、それが全体を的確に説明している訳ではありません。つまり、最新のネットワークの多くは、数千もの従業員や契約業者とデバイスと通信を行なっている単一のインターネットアドレスの背後にあるからです。

図 5：Project Heisenberg への日別のユニークな接続数

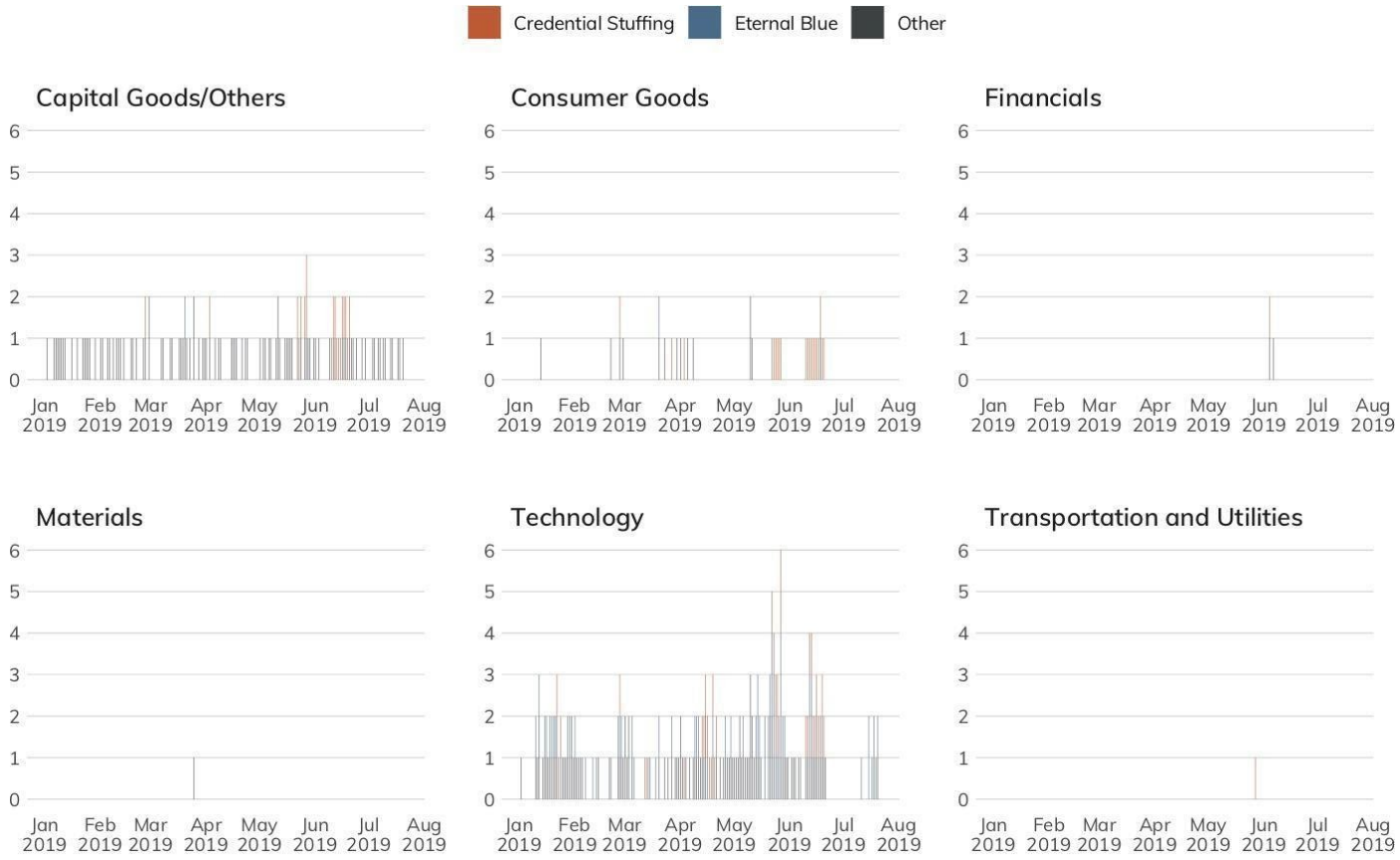
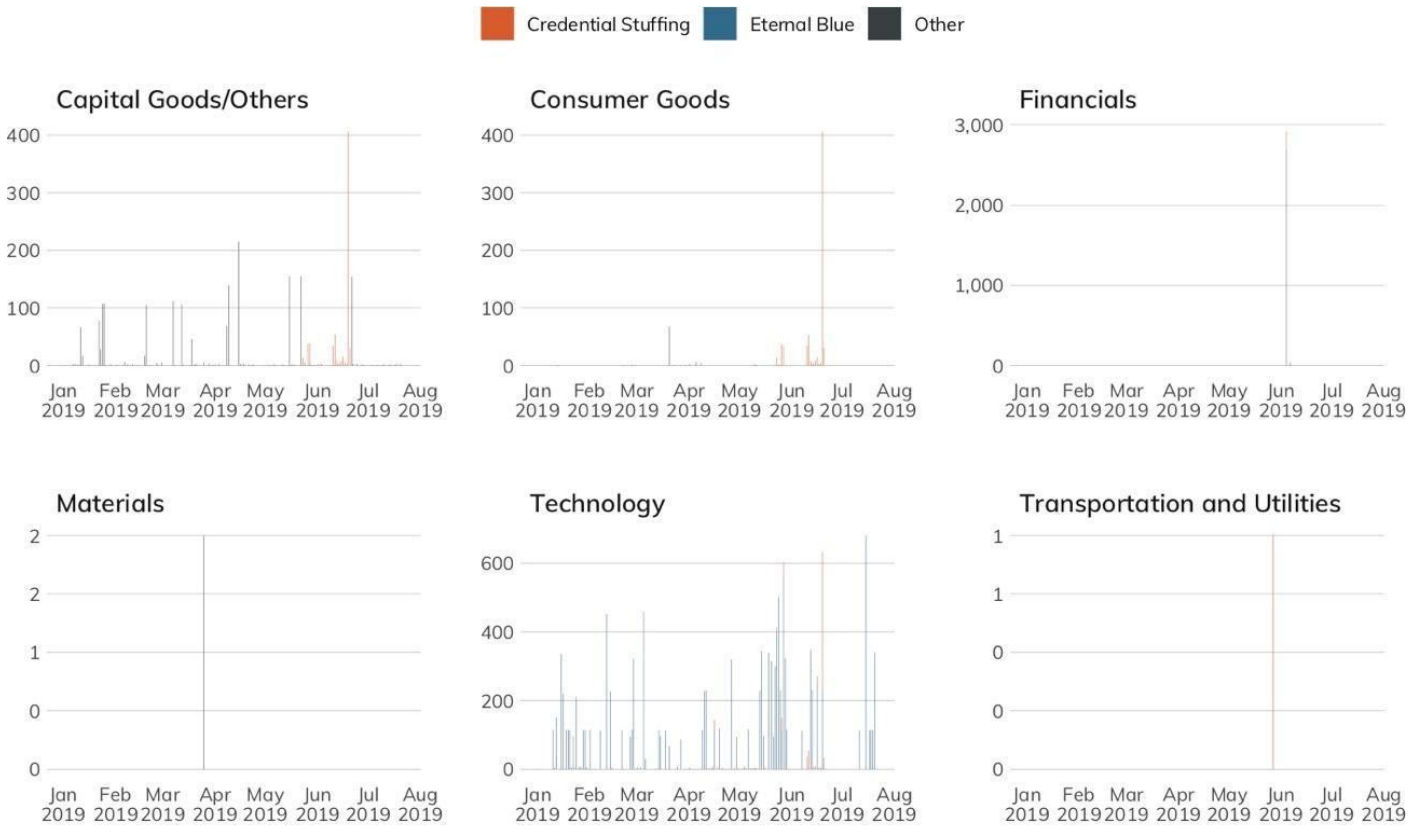


図 5 は、接続そのものを見るのには便利ですが、別途、そのボリュームを見ておく必要があります。個々の接続状況ではなく、図 6 では、測定した業種別の Project Heisenberg の日別の全接続数を示しています。このフリースケール表示によって、より簡単に潜在的な問題を区別してそれぞれの業種に「ズームイン」して見ることが可能です。ある業種の Heisenberg センサーへのユニークなノードの接続数が少ないからと言って、 その業種がアクティブではないは言えません。この図を見ることで、内部から企業全体にマルウェアの感染が大きく広がっている（数十、数百、もしくは数千の感染したシステムがインターネットにまで達しているなどの）ことや、いくつかのシステムが DoS キャンペーンの被害にあっている兆候が確認できます。

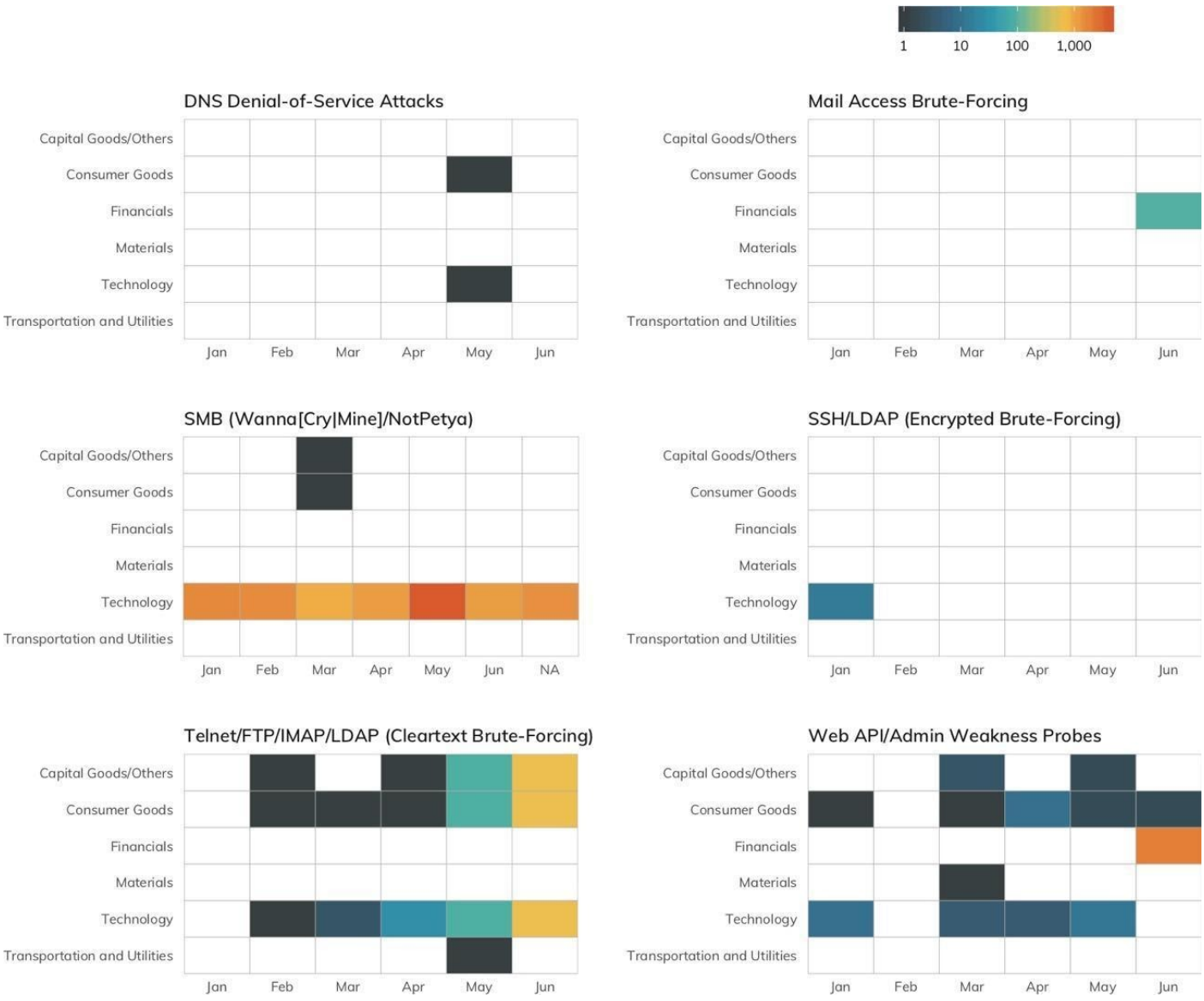
図 6：Project Heisenberg への日別の全接続数



いくつかの接続は、他よりも深刻で、本調査における企業から Heisenberg への上位 4 種類の接続タイプがとりわけ大問題です。図 7 に示されている通り、2019 年の前半で、Heisenberg は、複数の企業が以下の問題の影響を受けていることを示しています。

- SMB に関連するマルウェア（WannaCry、WannaMine および NotPetya など）
- DNS DoS 攻撃
- メールアクセスブルートフォース
- Telnet/FTP/IMAP/LDAP クリアテキスト（平文）クレデンシャルブルートフォース
- SSH 暗号化クレデンシャルブルートフォース

図 7：業種別の悪意ある活動の兆候（識別されたサービス別の全攻撃数（log10 スケール）



推奨事項：イングレスフィルターへの注意。ある程度のハニーポットトラフィックは想定しておくべきです。最新のインターネットは、結局のところ、容易に成果を得ようとして機会を探っている攻撃者で溢れかえっています。今回、観察されたトラフィックの不正なリダイレクトに関しては、ネットワークの設定ミスの可能性があり避けられません。そう言う意味で、明確に日経 225 銘柄企業が発信元となっているトラフィックあることから、これらの企業にイングレスフィルターが存在しないことが想定されます。ネットワーク管理者は、コネクティビティをスムースでかつ割り込みがない状態にし、接続が失敗した場合に修正することを習慣にしています。しかし、その反面で、エラーや悪意あるトラフィックをドメインから排除する必要もあります。データセンターと LAN の奥い部分の双方で、アウトバウンドのトラフィックルールを常に監査してテストしておき、不適切な設定で自らセキュリティブリーチを引き起こす事故を起こさないようにしておく必要があります。

[13] *Rapid7 Project Heisenberg、 https://www.rapid7.com/research/project-heisenberg/（2019 年 8 月 12 日に最終アクセス）*

サードパーティリスクのサイバーエクスポージャー

ほとんどすべての業種と地域でインターネットが全世界の商取引のバックボーンになっていることは紛れもない事実です。つまり、このような相互接続性が大きな理由で、外部業者に依存することなく Web サイトや業務プロセス、E コマースサイトを構築するなど、ほとんどの企業にとって不可能なのです。企業のデジタル化が進展するとともに、サービスの接続性を保ちスムースに業務を遂行するために必要となるメタデータにサイバーエクスポージャーがあり、サードパーティに依存しているより多くの内容が外部に流出していきます。

これにより日経 225 銘柄企業では、DNS レコードがサイバーエクスポージャーのあるサードパーティーサービスのメタデータに基づくフィッシング攻撃への脆弱性があると言う不幸な結果が生じています。さらに、不適切な設定がされたサードパーティーの Web サービスに依存している結果、多くの日経 225 銘柄企業とその Web サイトの訪問者がリスクに晒されています。わずか 3 つの Web サイトのみが、プライマリ Web サイトに対してコンテントセキュリティポリシーを使用した薄層なサードパーティー保護を提供しています。[14]

企業がオンラインのアセットを補完するために、サードパーティーのリソースを使用する場合、サードパーティーのリソースに起因するリスクが生じます。脆弱なサードパーティーのリソースは、当事者企業に対する攻撃の入り口として利用される可能性があります。例として 2018 年 9 月に、セキュリティのリサーチャーは、多くのサイトがサードパーティーのコンテンツデリバリーネットワーク（CDN）に依存している結果、Web ベースのクレジットカードスキミング攻撃に対する脆弱性を持っていると発表しています。[15]他の例として、2015 年には、Syrian Electronic Army が侵入された CDN により、著名なニュース媒体の Web サイトを乗っ取り、読者に対して独自のプッシュ通知を送信しています。[16]

本調査では、以下の場合に「サードパーティーリスクのサイバーエクスポージャー」が発生すると定義しています。

- 測定対象の企業が Web サイトとアプリケーションを構築する際に、サードパーティーサイトからのリソースに依存しているように見受けられる場合。 もしくは、
- 測定対象の企業が、センシティブなアーティファクトとなる可能性のある内容を公開しているメタデータに残したままアクティブに使用している場合。

調査方法のセクションで、サードパーティーリスクの属性の収集、分析方法について説明します。

図 8〜13 のそれぞれの棒グラフでは、Advertising（広告）、Analytics（アナリティクス）、CDN（コンテンツデリバリーネットワーク）からロードされる 4 種類の JavaScript の利用状況を示しています。グラフを見ることで業種別と業種内のサードパーティーへの依存状況について比較が可能です。

本レポートでは、 タグマネージャーを除外しました。[17]タグマネージャーは、適切に利用した場合、リスクを生むのではなくむしろ Web サイトとサイト訪問者を保護するのに役立つからです。

図 8：Capital Goods（消費財）/Others（その他）業種の Web サプライチェーンが共有しているリスク （棒グラフとラベルは同一のサービスをセキュアではない状態で使用している業種内の企業の割合）

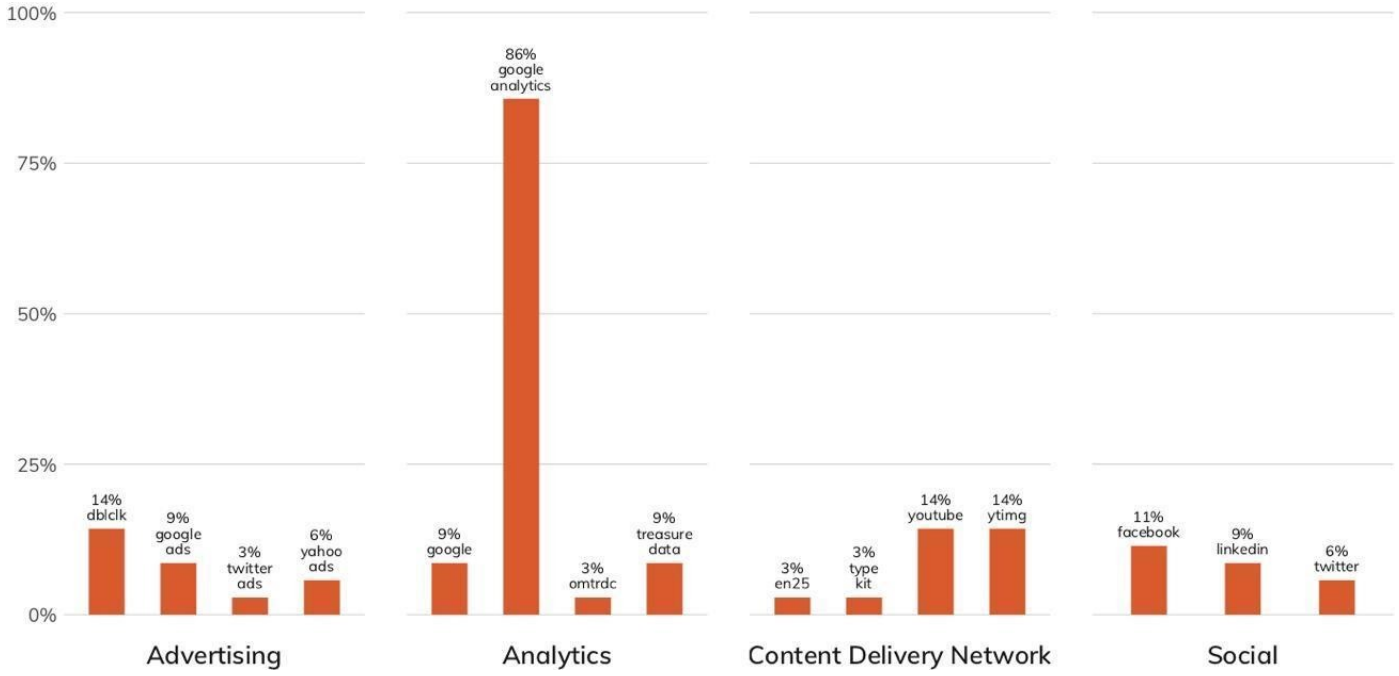


図 9：Consumer Goods（消費財）業種の Web サプライチェーンが共有しているリスク （棒グラフとラベルは同一のサービスをセキュアではない状態で使用している業種内の企業の割合）

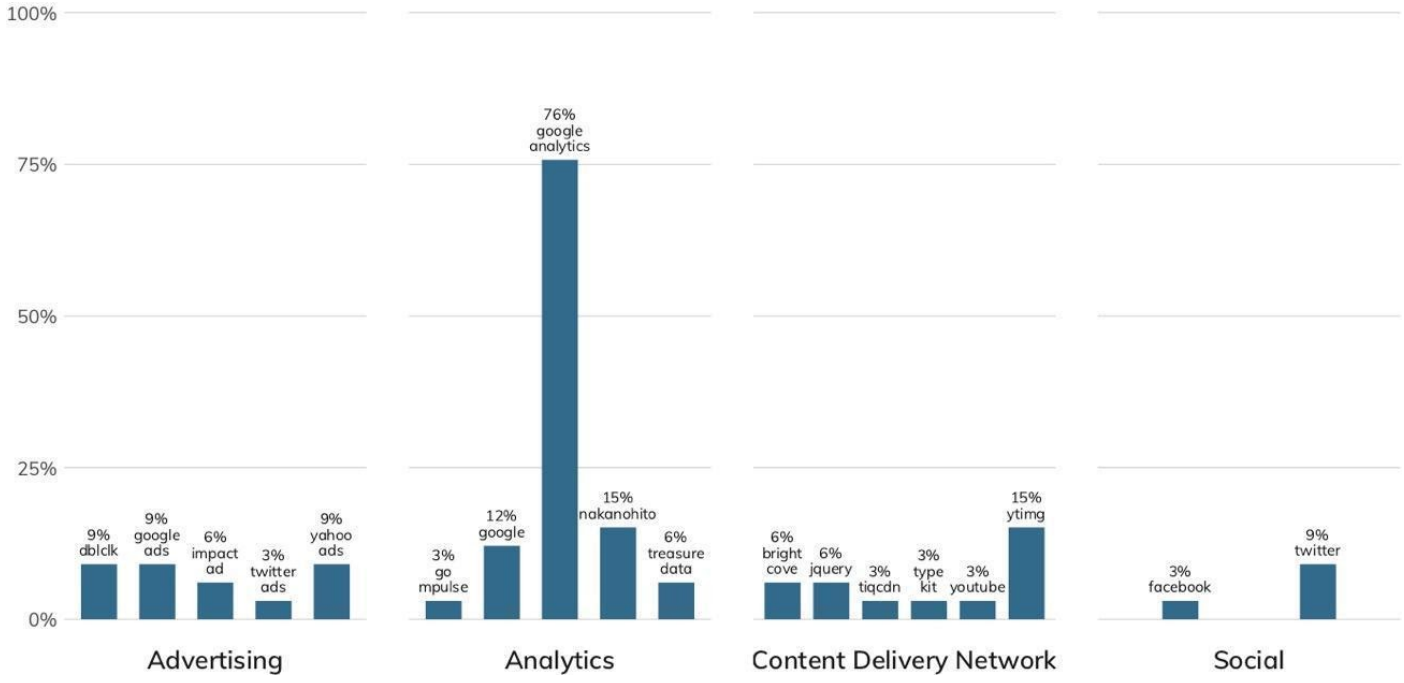


図 10：Financials（金融）業種の Web サプライチェーンが共有しているリスク （棒グラフとラベルは同一のサービスをセキュアではない状態で使用している業種内の企業の割合）

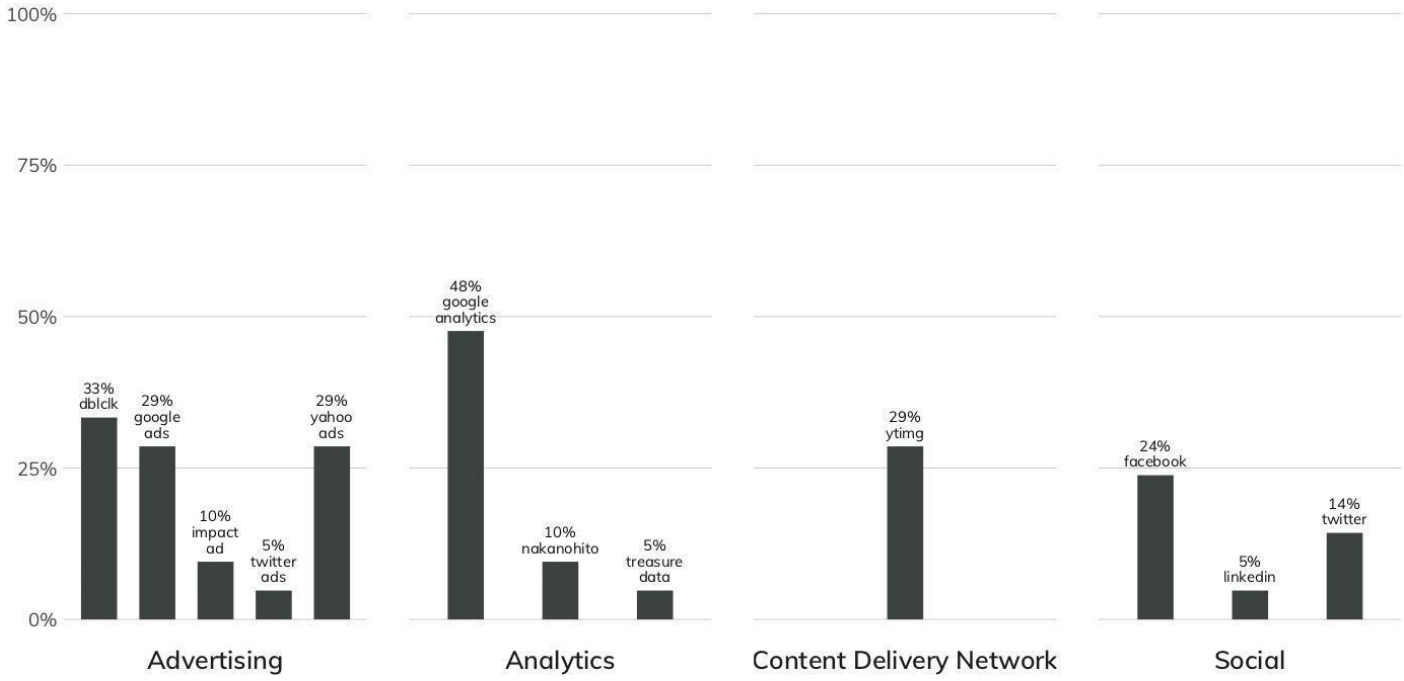


図 11：Materials （素材）業種の Web サプライチェーンが共有しているリスク （棒グラフとラベルは同一のサービスをセキュアではない状態で使用している業種内の企業の割合）

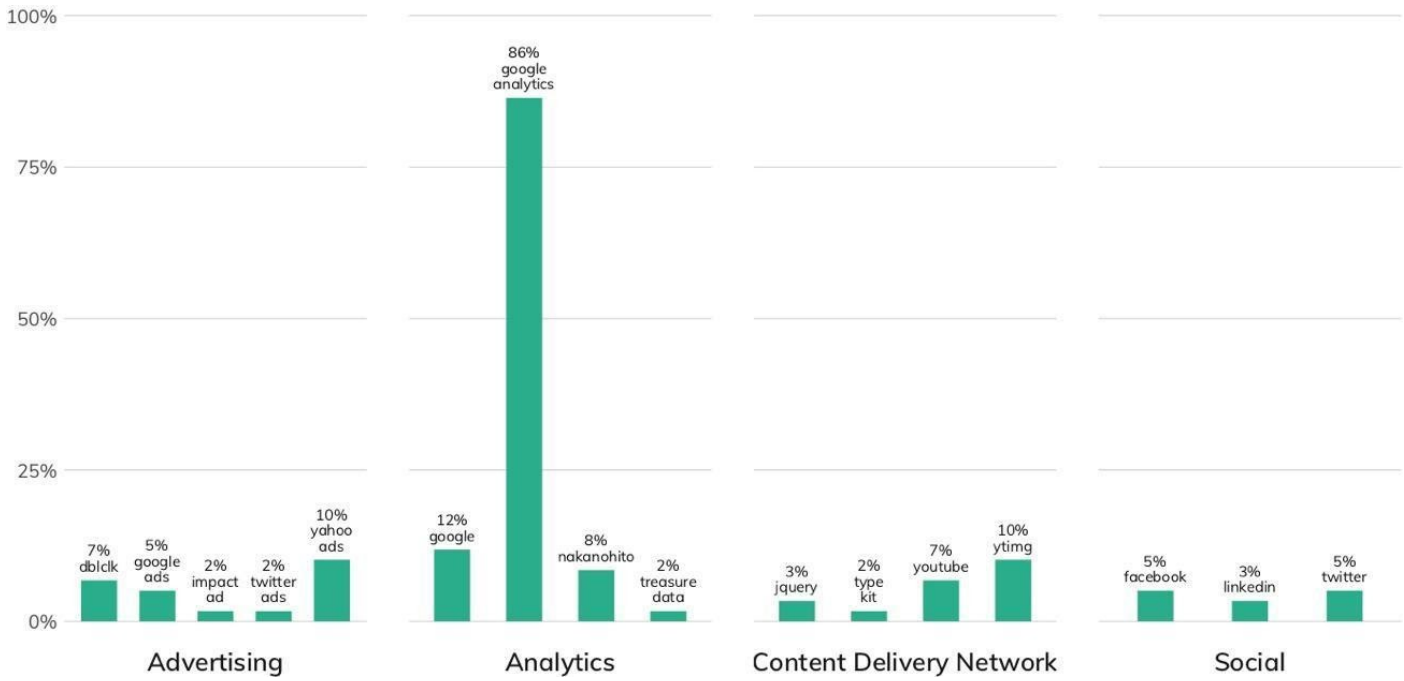


図 12：Technology（テクノロジー）業種の Web サプライチェーンが共有しているリスク （棒グラフとラベルは同一のサービスをセキュアではない状態で使用している業種内の企業の割合）

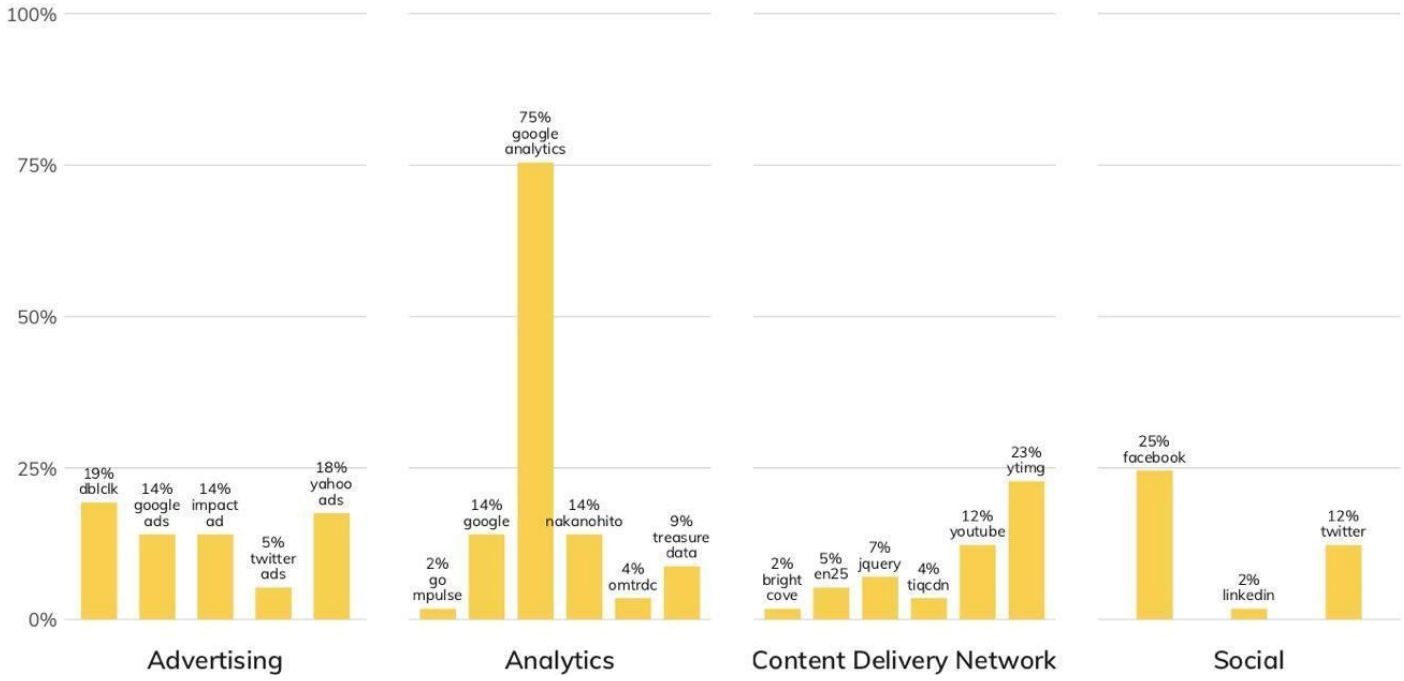
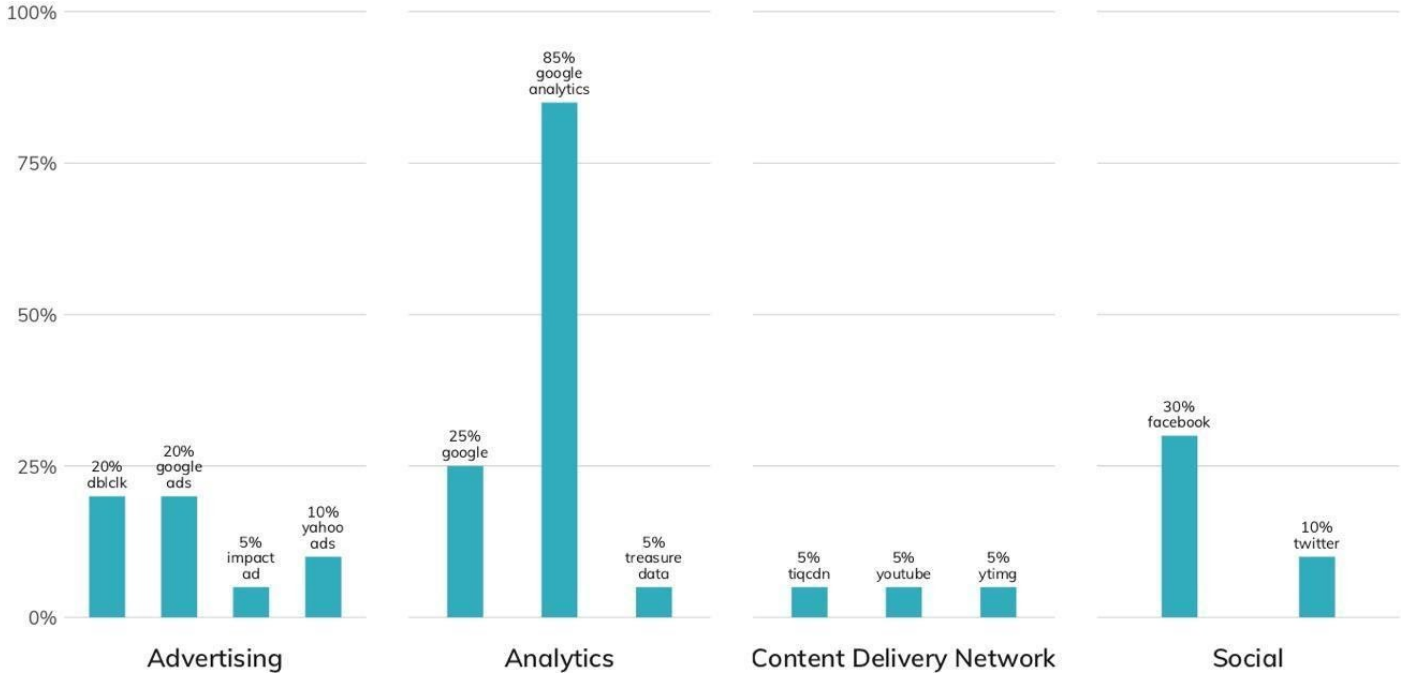


図 13：Transportation and Utilities （運輸および通信、電気、ガス、水道）業種の Web サプライチェーンが共有しているリスク （棒グラフとラベルは同一のサービスをセキュアではない状態で使用している業種内の企業の割合）



これらいくつかのサードパーティーサービスは、サイバー攻撃に対するレジリエンスがあり、当

事者企業のサイバーエクスポージャーの度合いにはあまり関係がありません。例として、Google Analytics には、顧客企業に対する悪意ある活動の隠れた踏み台にならないように十分な対策がなされています。しかしながら、頻繁にネットワーク上で悪意ある広告になっている DoubleClick のように広く普及しているサードパーティーサービスは、同一業種におけるリスクを増大させてしまいます。

図 14：サードパーティーアプ/クラウドの利用による DNS メタデータ経由のサイバーエクスポージャー

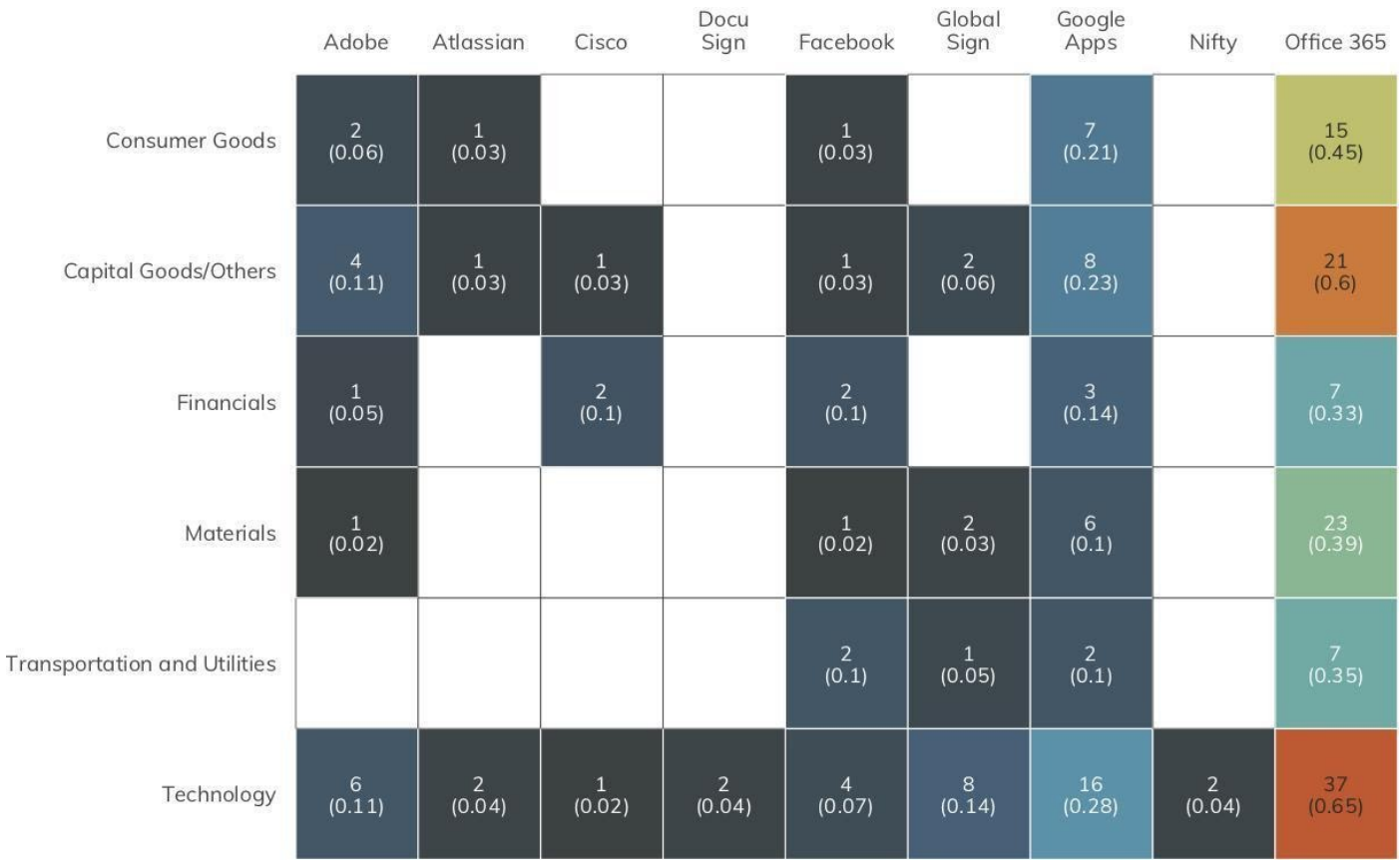


図 14 は、サードパーティーのサイバーエクスポージャーの後のコンポーネントについて、どのベンダーのアプリケーション/クラウドサービスに接続されているかまとめています。

DNS レコードからは、www.rapid7.com といった接続先のアドレスが判別できるだけでなく、フィッシング防御機能のセクションで詳しく説明をする通り、セキュアなメール設定がされているかどうか識別できます。また、アプリケーション開発からクラウドホスティング環境やファイル共有サービスに至るまで、企業が利用しているあらゆるサードパーティーの情報も得られます。

フリーフォームの TXT レコードに格納されている検証情報を利用することで、これらのサービスにサイバーエクスポージャーがあります。説明のために、表 1 に、 rapid7.com の DNS の TXT レコードを示します。

表 1：Rapid7 の DNS TXT テキストレコードのサンプル

DNS RECORD KEY	DNS TXT RECORD VALUE
rapid7.com.	smartsheet-site-validation.rapid7.com=wfJFw8OnJ0WwBCBDP7NuqH
rapid7.com.	MS=ms93061892
rapid7.com.	atlassian-domain-verification=+ Mx+hFjC77glTvA7K9Tp/5x7LvbyawRYOe ZpkXhE/Xys/xciI66aaIgyQQAD88E7
rapid7.com.	citrix-verification-code=3d0b36 42-a1b3-4cf3-8616-c9fb8cd0c2da

- "**smartsheet-site-validation**" signals that Rapid7 uses SmartSheet, a cloud spreadsheet service.
- "**atlassian-domain-verification**" signals that Rapid7 uses cloud-based services by Atlassian, a provider of popular software development tools and platforms.
- "**citrix-verification-code**" signals that Rapid7 uses services offered by Citrix.

本調査では、Rapid7 のリサーチャーは、Project Sonar の DNS 収集データを利用して日経 225 銘柄企業の TXT レコードを評価しています。一般的に知られているドメイン名のみを使っています。（今後の活動のセクションで説明している通り、それ以外のドメインにも調査対象を広げていこうと努力しています。）また、図 14 は、もっとも広く普及している著名なサードパーティーサービスのみに関する内容です。

すべての業種で Microsoft Office 365 がある程度利用されていることは驚くべきことではありません。また、Microsoft が、非国家攻撃の餌食となり Office 365 が企業への悪意ある侵入の入り口となることは考えにくいことです。 日経 225 銘柄企業では、Google Apps もかなり普及しています。インターネットの他のリソースのほとんどが利用されていることも判ります。

確立していてレジリエントなサービスプロバイダから企業が離れ始めるようのであれば、フィッシングの成功や、それ以外の攻撃が確認されるリスクが高まります。有能な攻撃者にとっては、大量な DNS クエリを作成してターゲットのリストを作るだけのことなのです。

推奨事項：サードパーティーのサイバーエクスポージャーの低減。個々の調査結果を見れば、これらの内容は大きなリスクにはなっていないかも知れません。実際のところ、これらの「検証」レコードは、最初に検証する際に必要となるだけで、それ以降は削除することが可能です。レコードによって、ドメインの本当の所有者の確認ができます。理論的に、本当の所有者のみが、これらの DNS エントリを追加したり変更したり削除したりすることが可能だからです。それらのレコードを一括して調べれば、多数の企業や、ブティックサービスプロバイダが、共通のサードパーティーサービスを共有していることが判ります。複数の企業に侵入しようとしている悪意あるアクターにとって、これらの情報はとても高い価値の標的です。従って、サードパーティーサービスにとってレジリエントであることがとても重要になっているのです。

---

[14] *コンテンツセキュリティーポリシーhttps://content-security-policy.com/（2019 年 8 月 12 日に最終更新）*

[15] *Kevin Beaumont 、 Magecart—new tactics leading to massive unreported fraud」DoublePulsar、2018 年 9 月 19 日、 https://doublepulsar.com/magecart-new-tactics-leading-to-massive-unreported-fraud-5211c9883dea*

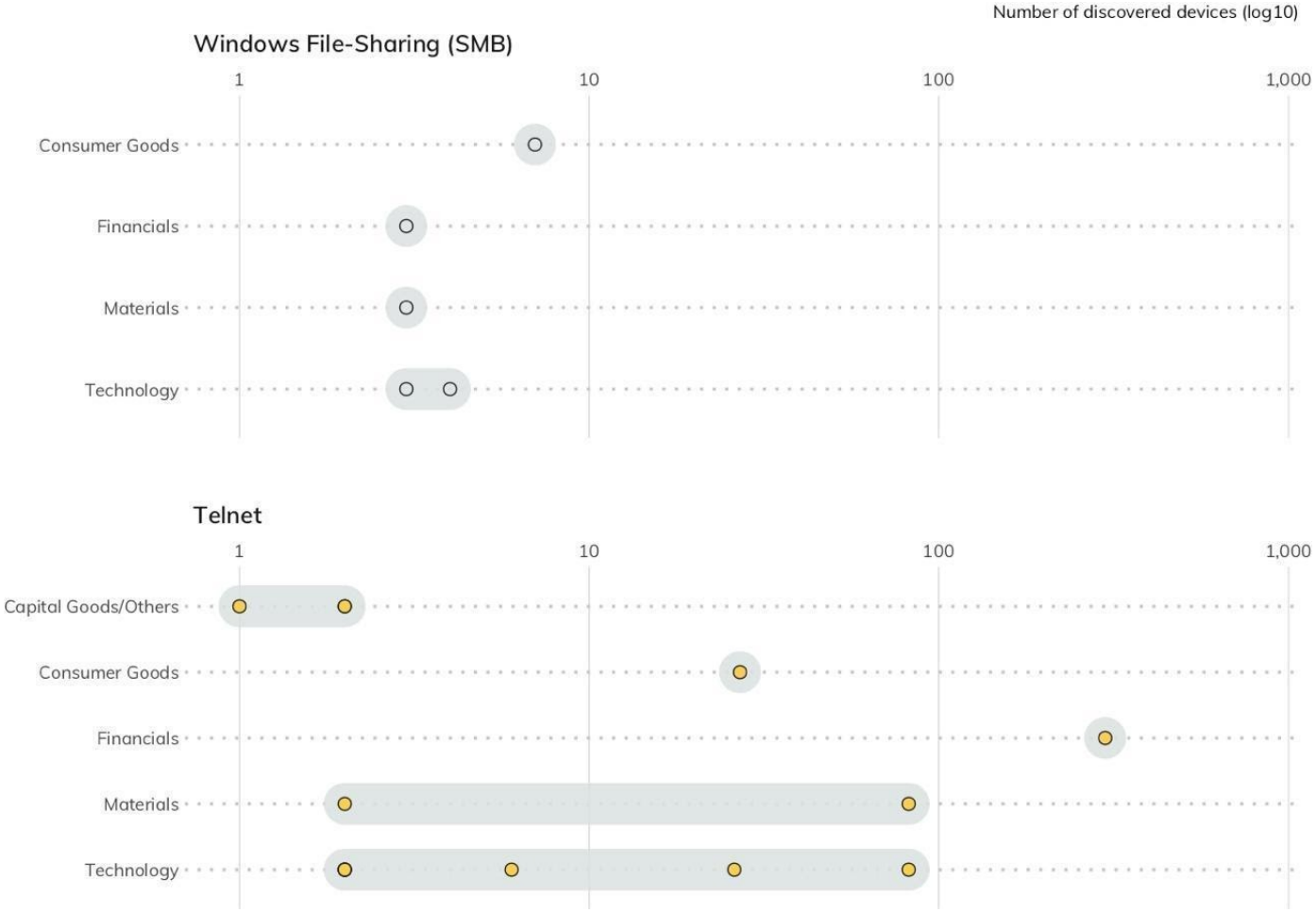
[16] *Thu Pham、「Malicious Hackers Take Over Media Sites via Content Delivery Network Providers」Duo Security、2015 年 5 月 19 日、 https://duo.com/blog/malicious-hackers-take-over-media-sites-via-content-delivery-providers*

[17] *Tag management system、https://en.wikipedia.org/wiki/Tag_management_system（2019 年 8 月 12 日に最終アクセス）*

不適切なサービス：SMB と Telnet

サイバーエクスポージャーのあるサービスのタイプによって深刻さが大きく異なります。（サービスによっては他のサービスに比べて「安全性」が劣ります。）図 15 は、日経 225 銘柄企業が、Telnet とウインドウズファイル共有のような深刻な脆弱性を持つサービスを標的とした攻撃に対して免疫を持っていないことを示しています。

図 15：業種別の Telnet とウィンドウズファイル共有のサイバーエクスポージャー（それぞれの点は、企業を表しています。横軸は、検出されたサービスの数です。）



サーバメッセージブロック（SMB）は、システムのサイバーエクスポージャーを生じさせるもっとも危険なサービスです。SMB は、ファイル共有とリモート管理プロトコルをオールインワンで提供します。通常は、ウインドウズに関連して利用され、攻撃者やリサーチャーのような人々が数十年にわたり攻撃の標的にしてきています。2003 年に MS03-049、2008 年に MS08-067（別名 Conficker）、2017 年に MS17-010（別名 EternalBlue）のすべてが、プロトコルの複雑性とウインドウズのネットワークの中心部を狙って出回っています。[18]最近は、SMB サービスの脆弱性が WannaCry や NotPetya 攻撃の標的になっています。これらは、ネットワークに障害を生じさせ、重要なビジネスプロセスに重大な攻撃を与え多くの企業に億単位の売り上げ損失をもたらしました。[19]

Telnet のサイバーエクスポージャーは、SMB のサイバーエクスポージャーと同様のリスクを生じさせます。Telnetの歴史はインターネットの黎明期に「最新」の標準だった1983年に遡ります。[20]Telnet は、サーバやネットワーク機器に直接ログインするために使用されるクリアテキスト（平文）のプロトコルです。通常、デバイスの OS レベルで、コマンドを叩いて直接スクリプトを実行します。Telnet サービスには、長年の脆弱性とサイバーエクスポージャーの歴史があります。企業は、クレデンシャルを盗まれたり、パッシブ、アクティブの盗聴にあったり。リモートコード実行をされたりしてきました。 プロトコルがクリアテキストだということは、適切にネッ

トワークに入っている攻撃者が、どんなユーザー名やパスワードも送信されたデータでさえも読むことが可能だという意味です。さらに弱いデフォルト設定のエンドポイントや、盗聴されたパスワードがハイジャックされて、悪意あるコードを OS 上で直接実行することが可能になってしまいます。

ひとつだけあるプラス要素は、すべての業種でこれら問題の多いサービスが利用されている訳ではない点です。利用している企業が 1 社か 2 社が存在する業種で Telnet かもしくは SMB のサイバーエクスポージャーがあります。良いニュースはそれだけで、2 社に 100 台を超えるデバイスで Telnet のサイバーエクスポージャーがあり、金融業種の 1 社で、500 台近い Telnet サーバのサイバーエクスポージャーがあります。2019 年の今、およそ必要とは考えられないほどの大きな攻撃面となっています。今日のインターネットでは、Telnet や SMB にまったくサイバーエクスポージャーがないことが理想ですが、日経 225 銘柄企業は、Fortune 500 企業に比較すると、絶対数と割合において SMB/Telnet のサイバーエクスポージャーが少ない状況ではあります。[21]

推奨事項：公開されている SMB と Telnet の排除。日経 225 銘柄企業では、これらのサービスのサイバーエクスポージャーは、とりわけウインドウズの SMB で非常に少ないものの、公共のインターネットに SMB サービスのサイバーエクスポージャーを生じさせること自体が安全ではありません。そのため Microsoft は、通常のデスクトップとラップトップのクライアントで、SMB のサイバーエクスポージャーを減らす努力をしています。例として、現在、Microsoft のドキュメンテーションでは、インターネットからファイヤーウォールで SMB をブロックすることを明示的に推奨しています。さらに Windows 10 デスクトップは、デフォルト設定でポート 445 へのアクセスをファイヤウォールで制限しています。[22]ひとつでも SMB が動作していると WannaCry や NotPetya、その他の最新の亜種が全社に蔓延して感染（再感染）してしまう可能性が生じます。今やもう Telnet サービスを使用する技術的、実践的な理由がありません。セキュアシェル（SSH）通信レイヤープロトコルに取って代わられています。暗号化通信であり接続認証で電子証明書の使用が推奨されています。[23]ローカルのコンピュータのリソースの制約で、SSH がどうしても動作しないデバイスで、Telnet しか使用できないのであればそのようなデバイスは、40 年前の暗号化非対応デバイスであるかどうかに関係なく、設計上、インターネットにエクスポージャーするには単純に安全性に問題があります。日経 225 銘柄企業の約 3 分の 1（80 社）では、Telnet のサイバーエクスポージャーが一切なく SSH サービスにのみサイバーエクスポージャーがあります。つまり、プロトコルの強度に対してある程度の認識がされているように見受けられるのです。

---

[18] *Rapid7、National Exposure Index 2018、「Inappropriate Services」、14 ページ、2018 年 6 月 14 日、https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf*

[19] *Bob Rudis、「No More Tears? WannaCry, One Year Later」、Rapid7、2018 年 5 月 14 日、https://blog.rapid7.com/2018/05/14/no-more-tears-wannacry*

[20] *J. Postel and J. Reynolds、Telnet Protocol Specification、Internet Engineering Task Force、1983 年 5 月、https://tools.ietf.org/html/rfc854*

[21] *Rapid7、Industry Cyber-Exposure Report: Fortune 500、13〜14 ページ、2018 年 12 月 11 日、https://www.rapid7.com/info/industry-cyber-exposure-report-fortune-500*

[22] *Rapid7、Industry Cyber-Exposure Report: Fortune 500、13～14 ページ、 2018 年 12 月 11 日 、 https://support.microsoft.com/en-us/help/3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic*

[23] *T. Ylonen and C. Lonvick、 The Secure Shell （SSH） Transport Layer Protocol、 The Internet Society、2006 年 1 月、 https://tools.ietf.org/html/rfc4253（2019 年 8 月 12 日に最終アクセス）*

古いパッチングがされていない Web サービスのサイバーエクスポージャー

インターネットサービスの設定や、パッチング、サポートされている OS やインターネットに接続されたアプリケーションの維持管理など、攻撃者の妨害をするのには多大な労力を要します。最新バージョンのソフトウェアを使用していないと、企業は、パッチされていない既知の脆弱性をついた攻撃の大きなリスクに晒されてしまいます。残念ながら、ほとんどの日経 225 銘柄企業が、古くてサポートされていないバージョンの場合もある汎用的な 3 種類の Web サーバを使用しています。それは、マイクロソフトのインターネットインフォメーションサービス（IIS）、Apache HTTPD、F5'の nginx です。

Microsoft IIS

Netcraft 社に拠るとマイクロソフトの IIS は、2019 年 7 月時点で 3 番目によく使われている Web サーバです。[24]図 16 には、Project Sonar で検出された、日経 225 銘柄企業の 6 業種すべてに分布する 123 社の合計 2,873 台の IIS サーバとそのバージョンが示されています。

図 16: IIS のバージョン分布（各色はそれぞれの業種、横軸はバージョン）

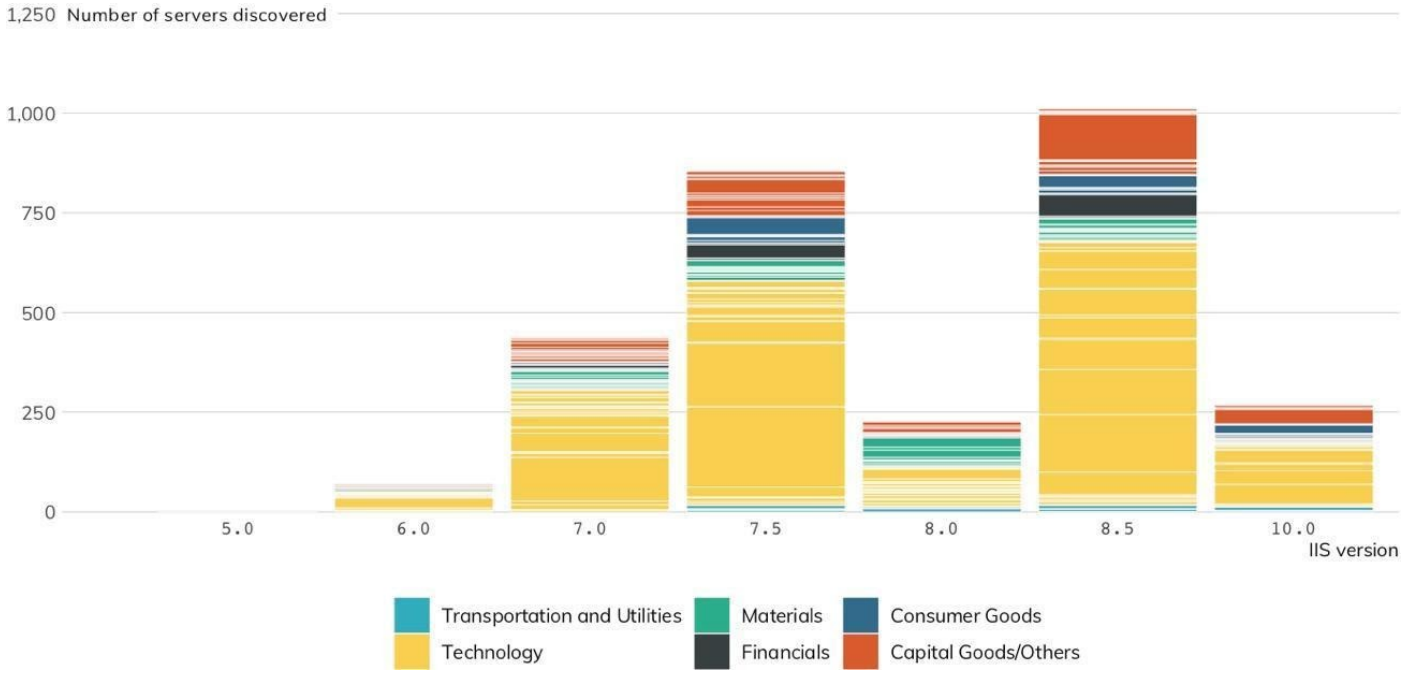
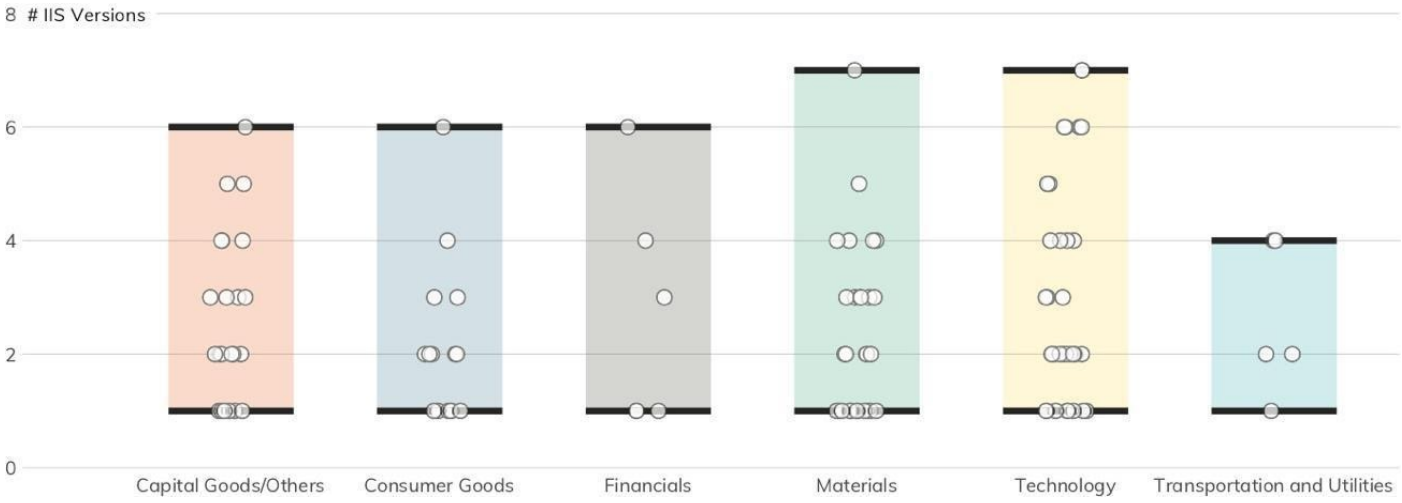


図 17 は、「バージョン分布」を示しています。日経 225 銘柄企業の業種別の IIS サーバのバージョンです（それぞれの企業で使用されている IIS の異なるインスタンスの数）。32%近くの企業が、単一バージョン、26%近くの企業が 3 バージョン以上の IIS を稼働させています。バージョンが多岐にわたることと、エンドオブライフに近づいているバージョンの IIS を継続して使用していることで、防御と管理がより複雑化し、古いバージョンの IIS サーバが増やすことが攻撃者にとって侵入の入り口になる可能性があります。

図 17：IIS のバージョン分布（それぞれの点は、企業を示しています。多くの企業が 10 以上の異なる バージョンの IIS を同時に使用しています。）



Apache HTTPD

Apache の場合、web サーバの利用状況は少し複雑です。図 18 は、日経 225 銘柄企業の 6 業種すべてに分布する 99 社で Project Sonar が検出した 320 サーバが 71 種類のバージョンにわたっていることを示しています。Apache のバージョン分布（図 19）は、複数の企業（35%）が、単一バージョンの Apache HTTPD にサイバーエクスポージャーがある一方で、40%近くの企業が 3 種類以上のバージョンにサイバーエクスポージャーがあり、繰り返すようですが、管理をより複雑化させてしまっています。

図 18：Apache HTTPD バージョン分布（縦軸は上から下に向かって古い順でバージョン、各色は企業の業種を示しています。ラベルはリリース年です。）

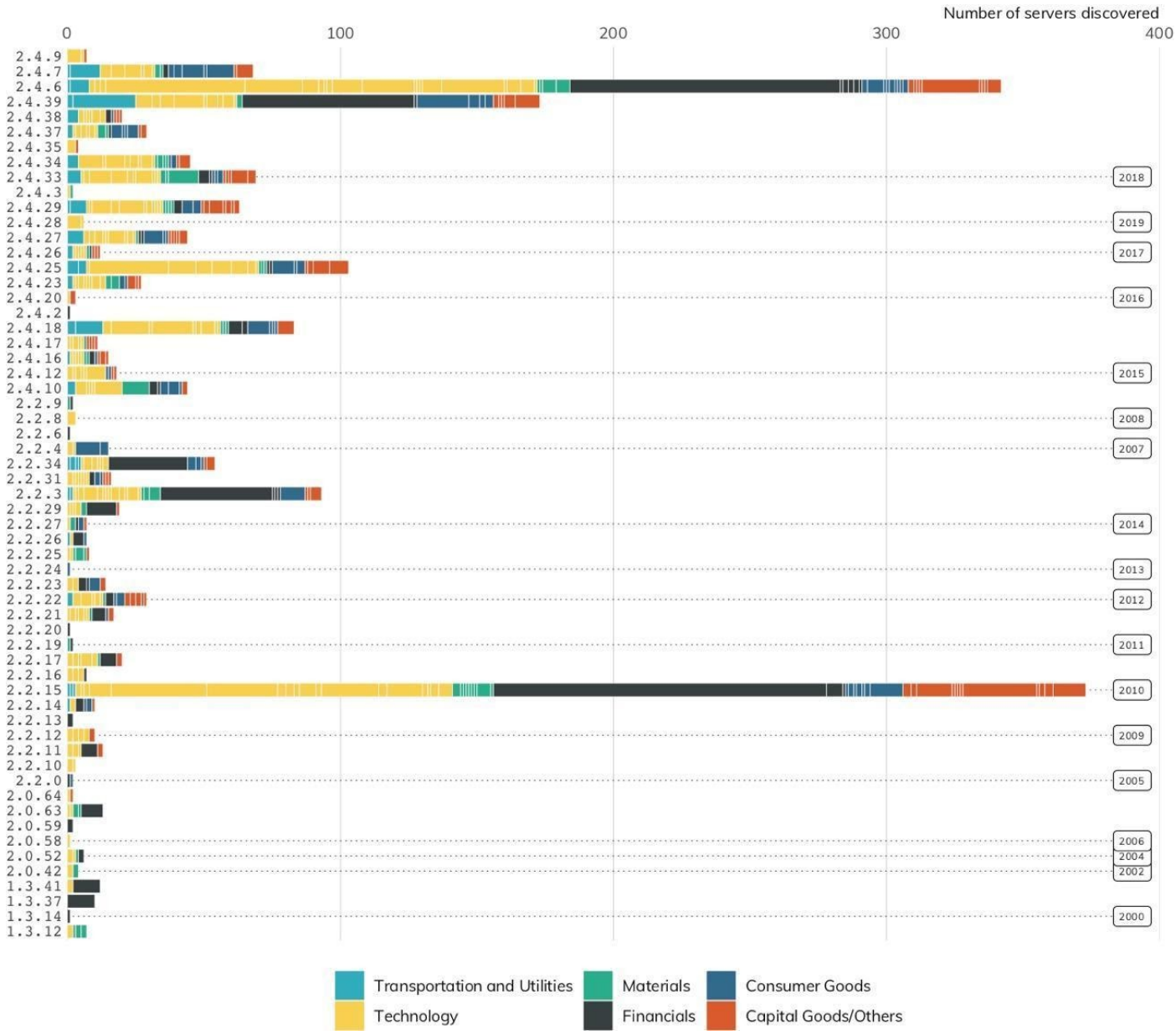
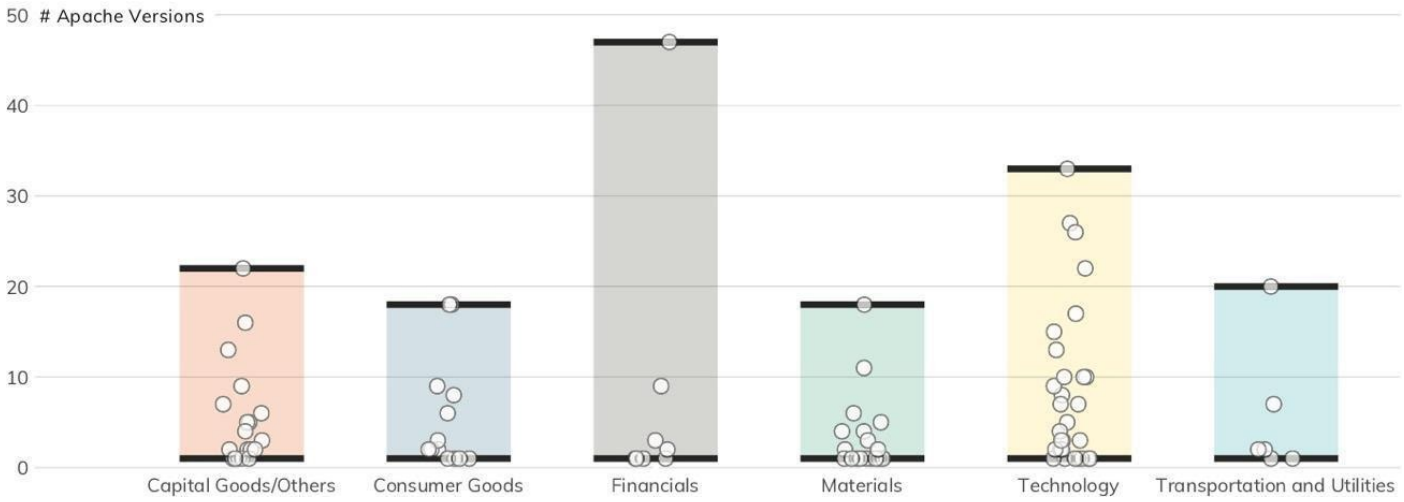


図 19：Apache バージョン分布（それぞれの点は、企業を示しています。多くの企業が 10 以上の異なる バージョンの Apache を同時に使用しています。）



驚くほど幅広いバージョンのソフトウェアが使用されている一方で、検出されたのは、ほとんどが 1 年以上古いバージョンです。つまり、企業が Apache を最新バージョンに更新していないということを示しています。米国企業では、サードパーティーの脆弱性管理ツールで、Apach サーバの棚卸しを行ない、バージョンとパッチレベルを識別することが必須になっているのとは対照的です。Apache ソフトウエア財団では、機能追加、問題の修正、セキュリティ問題に対するパッチを反映した新バージョンを常にリリースしています。さらに、Apache HTTPD がオープンソースであることから、攻撃者は、ソースコードに 100%アクセスできるため、より簡単に盲点をついて悪用することが可能です。

nginx

nginx web サーバは、2019 年 7 月の Netcraft 社の調査では利用社数が 1 位でした。しかし、日経 225 銘柄企業で Project Sonar が検出した利用社数は 2 位（60 社）でした。図 20 は、日経 225 銘柄企業の全業種にわたり 36 社で検出された nginx サーバーです。.

図 20：nginx バージョン分布（縦軸は上から下に向かって古い順でバージョン、各色は企業の業種を示しています。ラベルはリリース年です。）

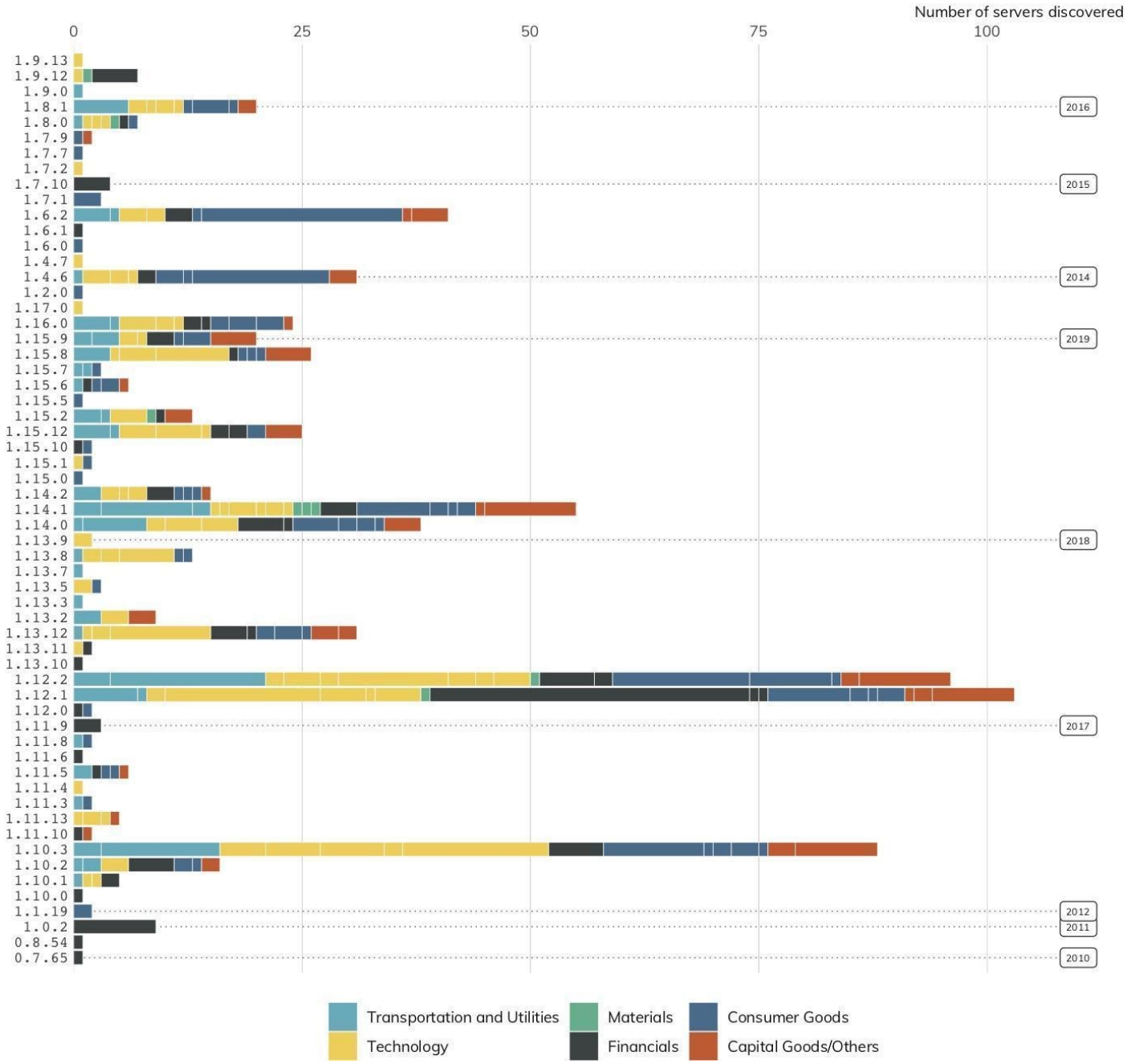
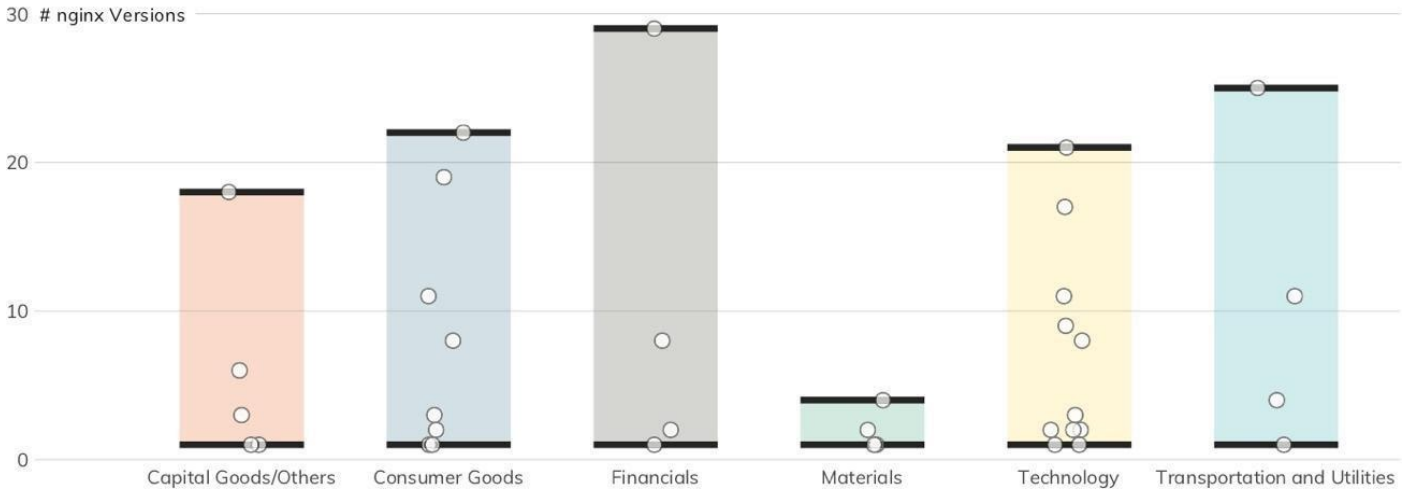


図 21 にある nginx の状況は、Apache での状況よりは確実に良く、多くの企業が 3 種類未満のバージョンを稼働させており（44%）、3 種類以上のバージョンを稼働させている企業は 55%です。

図 21：nginx バージョン分布（それぞれの点は、企業を示しています。多くの企業が 10 以上の異なる バージョンの nginx を同時に使用しています。）



単一の Web サーバプラットフォームの複数バージョンのセキュリティポスチャを維持することは、成熟したオペレーション部門にとって果たすべき機能の一部かどうかを疑う声もあるでしょう。しかし、複数のベンダーのテクノロジーを利用すると複雑性が増す結果となります。日経 225 銘柄企業の半分近くが、複数のインターネットに接続された Web サーバベンダーのテクノロジーを利用しています（表 2）。[25]複数のベンダーと多様なバージョンを同時に利用することで、攻撃者が盲点をついて悪用する可能性を生む設定の弱点を見落とすリスクが大幅に増大してしまいます。

表 2：日経 225 銘柄企業における利用ベンダー数

NUMBER OF NGINX VERSIONS MAINTAINED	NUMBER OF ORGANIZATIONS	PERCENTAGE OF NIKKEI 225
1	69	46%
2	51	34%
3	29	20%

推奨事項：バージョンを極力、統一すること。サーバへのパッチングと維持は、当たり前で些細なことのように思われるかも知れません。しかし、変更管理のスケジューリングや、コアサービスとなりうる部分に対するシステム停止のオーケストレーションは、大企業にとって非常に複雑な作業です。退屈な作業かも知れませんが、サイバーエクスポージャーのあるシステムの棚卸しを行ない最新のリストを維持し、サポートされていてパッチングされているバージョンのソフトウェアのみを使用するように、業務部門とアプリケーション開発部門に徹底することが死活問題なのです。

[24] *Netcraft July. 2019 Web Server Survey*、*https://news.netcraft.com/archives/2019/07/26/july-2019-web-server-survey.html*（*2019 年 8 月 12 日に最終アクセス*）

[25] *電卓で計算するか、付加情報について細心の注意を払っている賢明な読者なら、2 列目の数字の合計が 149 になっていることにお気づきかも知れない。Cloudflare や Akamai のような CDN が、背後のサーバテクノロジーにマスクをかけてしまっているからである。背後にあるサーバの複雑性についてカテゴリー分けをすることが不可能なため、それらのバージョンはレポートに含まれていない。*

結論

本レポートでは、外部公開されたインターネット接続を介して、特定の企業と業種におけるサイバーセキュリティリスクに対するサイバーエクスポージャーの複数の測定方法を説明しています。それらの企業のサイバーセキュリティのポスチャは、を完全には明らかにすることができないものの、日経 225 銘柄企業のサイバーエクスポージャーに関して本調査の結果、非常に重要な内容を把握することができました。

- 日経 225 銘柄企業は、平均で 107 サーバ/デバイスにサイバーエクスポージャーがあります。また多くの企業では、 750 近くのシステム/デバイスにサイバーエクスポージャーがあります。システムの数が多いほど、攻撃の試みの対象となりやすいことを意味します。

- 日経 225 銘柄企業の圧倒的多数（87%）が、強化されたメールセキュリティ設定を行なっていません。さらに 6%の企業が、不正な DMARC レコードを設定しており、フィッシング攻撃のリスクを増大させています。サイバーエクスポージャーを減少させるため、企業は DMARC 設定を評価して強化する必要があります。

- すべての業種の日経 225 銘柄企業が、ビジネスクリティカルなインターネット接続システムに対してパッチ/バージョン管理を行なっていません。インターネット接続システムの設定とバッチの管理を優先順位のトップに位置付けて、古いソフトウェアの脆弱性をついた悪用を排除することは企業にとって死活問題です。

- 日経 225 銘柄企業の 18%が、プライマリドメインに HTTPS 接続を求めていません。これにより訪問者を中間者攻撃の重大なリスクに晒してしまっています。

- 日経 225 銘柄企業で多くのサイバーエクスポージャーのあるサードパーティーサービスが共有されています。これにより、共有されたサードパーティーサービスの脆弱性が複数の企業に対する悪用を招き、さらに重大なリスクを生じさる可能性があります。サードパーティーサービスプロバイダが、適切なステップでセキュリティを強化し、それらのサービスを利用する際には、共通して悪用されてしまう状況を回避するために、サブリソース整合性署名などのツールを利用するように徹底する必要があります。

- Telnet やウインドウズファイル共有のような極端に弱いサービスは、1 社を除き、日経 225 銘柄企業ではあまり多くはないものの使用されてしまっています。それぞれが、SMB の脆弱性の悪用の可能性の重大リスクを生じさせます。サイバーエクスポージャーを減らすために、企業は、可能な限りポート 445 を閉じて、Telnet から SSH への移行をする必要があります。

日経 225 銘柄企業は、一般的に IT やセキュリティを含め幅広い分野の業務で優秀な人材を確保できる企業ですので、日経 225 銘柄企業よりも小さく無数に存在する企業においては、さらに重大なサイバーエクスポージャーやリスクが存在している可能性を示唆しています。サイバーセキュリティに対応するステップの中で、継続しているサイバーエクスポージャーの理由に関して、主要な関連部門で議論がされることが、デジタルのエコシステムにとってメリットのあるものになる可能性があります。

業種別のサイバー脅威の測定：調査方法の概要

本レポートは、インターネット経由で企業の外部公開のシステムと通信することで得られるデータを利用して、サイバーセキュリティリスクへのエクスポージャーに関する調査結果をまとめています。これらのデータにより、日本にある日経 225 企業のサイバーエクスポージャーを数値化し業種別に結果を集計しました。このレベルで、サイバーエクスポージャーを測定しておくことは、サイバーリスクの削減の活動目標の設定や、業種内の情報共有、将来のサイバーエクスポージャーを削減するための企業活動に関する認知度の向上に役立ちます。

2016 年以来、Rapid7 では、特定の国における特定のサイバーセキュリティリスクへの露出を測定し報告しています。[26] そこで得られた情報により、国レベルの Computer Emergency Response Teams（CERT）におけるサイバーエクスポージャーのより詳細な分析を促し、死活問題ともなりえるサービスのサイバーエクスポージャーを削減するための活動を支援しています。これらのレポートを作成するために、Rapid7 では、自社のスキャニングプラットフォームである Project Sonar と[27]、パッシブセンサーのネットワークである Project Heisenberg[28]を使用しています。これらのプロジェクトによりオンラインのアセットが脆弱性の高いインターネットサービスをアドバタイズしているか、そして疑わしい外部接続を行なっていないかを確認しています。ここから国家レベルの集計結果を算出しています。

サイバーエクスポージャーのデータを国家レベルで集計するのは比較的単純な作業です。Rapid7 では、国の場所とインターネットアドレスを照合する高精度なデータベースを有しており、常に更新することで 98%の精度を維持しています。[29]しかしながら、サイバーエクスポージャーについて深掘りするためには、さらなる作業が必要となっています。特定の企業に関するより詳細なサイバーエクスポージャーの測定には、企業が保有し業務プロセスに利用している専用のインターネットアドレスを分析する必要があります。まず企業のインターネットアドレスを照合してから、アクティブスキャンとパッシブセンサーで得られる外部公開のデータによって、特定のサイバーセキュリティリスクは数値化することが可能になります。本セクションでは、以下のステップで実施されているステップについて詳しく解説します。

- 日経 225 銘柄企業のインターネットアドレスとプライマリドメインとの紐付け
- 各企業に紐付けされたインターネットアドレスを使用している脆弱性のあるサービスとシステムに対する Project Sonar によるアクティブスキャンデータ
- Rapid7 のグローバルなパッシブセンサーネットワークである Project Heisenberg による、各企業に紐付けられたインターネットアドレスとの相互通信の頻度と内容の識別によるサイバーエクスポージャーデータの詳細化
- 直接的なサイバーエクスポージャーの測定により推定されるサイバーエクスポージャーに関する補足。推測のために Rapid7 では、DNS レコードに記載された電子メールの「安全性」の設定や、検知可能な OS とアプリケーションのバージョン情報など、企業が紐付けられたインターネットアドレスの「メタデータ」を分析

これらの測定結果は、以下の 3 つの分野に分類できます。詳細については、以降のセクションで解説します。

- **パブリック DNS レコードを使用した推定による測定：**もっとも重要なのはフィッシング攻撃に対する企業の防除について測定できます。
- **Rapid7Project Sonar を使用したアクティブスキャン：**外部公開されたシステムおよびサービスの測定に加えて、それらのシステムおよびサービスにあるサイバーエクスポージャーの内容が含まれます。
- **Rapid7 の Project Heisenberg を使用したパッシブセンサー:** 企業のネットワークにあるシステムが、Project Heisenberg のハニーポットコレクションに接触し、どのような活動を接続中に試みたかに関する記録です。.

---

[26] *Rapid7、National Exposure Index, Jun. 7, 2018、https://www.rapid7.com/info/national-exposure-index（2019 年 8 月 12 日に最終アクセス）*

[27] *Rapid7、Project Sonar、https://www.rapid7.com/research/project-sonar（2019 年 8 月 12 日に最終アクセス）*

[28] *Rapid7、Project Heisenberg、https://www.rapid7.com/research/project-heisenberg（2019 年 8 月 12 日に最終アクセス）*

[29] *MaxMind、https://www.maxmind.com（2019 年 8 月 12 日に最終アクセス）*

Project Sonar のアクティブスキャン

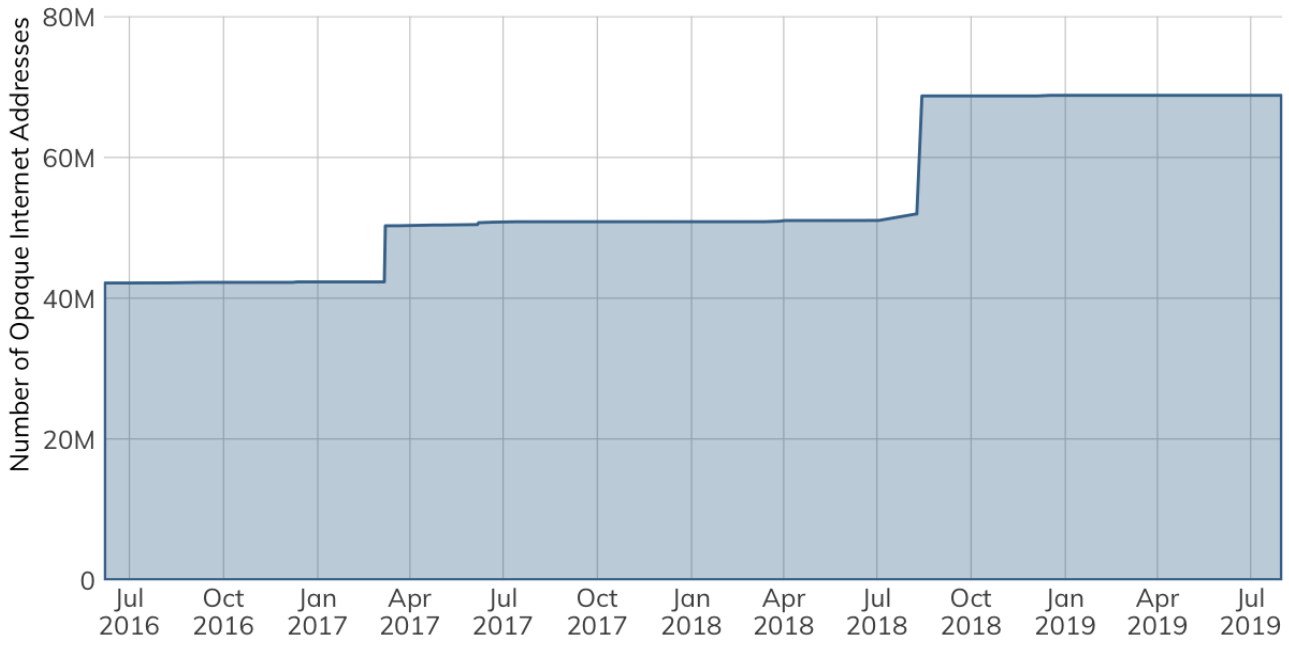
Project Sonar は、インターネットの多岐にわたるサービスをスキャンします。「サービス」とは、Web サーバ、メールサーバ、ファイルサーバ、データベースサーバ、ネットワーク機器、カメラなど、インターネット経由のリクエストをリスニングする設定になっているその他の幅広い種類のサーバを意味します。スキャナーのプローブに対して、特定のインターネットアドレスのサービスに応答がある場合、その結果を応答データとともに記録します。スキャンされたサービスによって、スキャンされたサービスの詳細なバージョンや設定の情報が応答データに含まれています。

Rapid7 は、インターネットのスキャンに関する法令を遵守しています。従って、Project Sonar のプローブは、例えパスワードや悪用方法が広く知られていたり明白であったりしても、クレデンシャル、既知の脆弱性、プローブが検知したサービスに害を及ぼすようなペーロードの情報を取得しません。これによって、スキャンすることで得られる情報や、取得するサービスのメタデータの種類に制約は生じています。しかしながら、それでも十分に幅広く有益な情報を取得することは可能です。

Rapid7 では、「オプトアウト」プロセスを自主的に定めて、さらなる制限を行なっています。Project Sonar がスキャンするインターネットアドレスの範囲に対して、企業は、特定のインター

ネットアドレスの除外を求めることが可能です。Rapid7 には、この要求に応じる義務があるので、スキャンプロセスからブラックリストとして、除外を求められたインターネットアドレスの範囲を除外します。（図 22）

図 22：Rapid7 の Project Sonar のブラックリストインターネットアドレス数の推移



Fortune 500 企業向けの 2018 年の ICER とは異なり、オプトアウトされたブラックリストには 2019 年第 2 四半期の日経 225 銘柄企業が 1 社もありません。[30]

---

[30] *Rapid7、Industry Cyber-Exposure Report: Fortune 500、10〜11 ページ、2018 年 12 月 11 日、https://www.rapid7.com/info/industry-cyber-exposure-report-fortune-500（2019 年 8 月 12 日に最終アクセス）*

Project Heisenberg のパッシブスキャン

Rapid7 の Project Heisenberg の中心となっているのは、HTTP、SMB、SSH、その他のさまざま種類のフェイクサービスをホスティングしている 250 におよぶアドバタイズされていないシステムです。これらのハニーポットは、積極的にシステムへの接続を求めていないにも関わらず、一方的に勝手に行なわれる接続を注意深く監視しています。インターネット全体をスキャンする調査方法とは異なり、企業のシステムは、Heisenberg センサーネットワークに接続する正当な理由がないので、Heisenberg が記録した活動により、企業が外部接続について管理を行なっていないことを如実に示すことが可能です。つまり、悪意ある活動もしくは、企業のシステムからの不正な設定が行なわれたサービスのトラフィックが存在することが推測されます。単純に言うと、Heisenberg にコンタクトがある場合、企業には何らかのサイバーエクスポージャーが存在しているのです。

Web サーバのサードパーティリスクの測定

Web サーバや Web サービスにインターネットへのエクスポージャーがある場合のサードパーティーリスクは、Web ページがブラウザに読み込まれている際の各ページのリソースを調べること把握できます。Project Sonar は、仮装ブラウザを制御することでこのタスクを広範囲に実行できます。企業の広く知られているドメインにあるページを訪問して各サイトのリソースを読み込む際の動作をすべてキャプチャーします。

これらの Web サイトでは、大量なサードパーティーのリソースが読み込まれるので、すべてのリストを可視化して理解するのは困難です。結果として得られるリストには、調査対象リストで全般的に使用されている主要なサードパーティリソースのみが記載されます。

今後の調査

本レポートのサイバーエクスポージャー分析のプロセスと手順は、インターネットの遠隔測定の一貫で、包括的な業種別の「サイバーヘルス」を広く世の中に周知させる初めての試みです。本セクションでは、今回、明らかになった測定の限界について解説をします。

インターネットアドレスと属性の正確性の向上

もっとも一般的に使用されているインターネットアドレス（バージョン 4、 IPv4）は、完全に枯渇しています。つまり、企業にインターネットアドレスを割り当てるための「空いている」ブロックが無くなっています。しかしながら、企業が保有している IPv4 アドレスのすべてが利用し尽くされている訳ではありません。有限のリソースに不足が生じていることから、IPv4 のインターネットアドレスを売買可能な市場が形成されました。[31]歴史の長いいくつかの企業が IPv4 のインターネットアドレスのブロックを他社に販売し、いくつかの企業は所有権を保持しつつ他社に貸し出しています。このような取引から属性エラーが生じるようになり、とりわけ企業のインターネットアドレスが、属性の変更ができない状態で貸し出された際に、非常に苛立たしい結果が生じています。

本レポートのために、Rapid7 のリサーチャーは、手作業で事前に属性の把握と、属性に異常がないか確認を行ないました。つまりインターネットアドレスの使用状況と既知のホスティングとクラウドサービスのプロバイダーの情報の比較です。そして、**調査方法**のセクションで解説するように、企業の DNS レコードから直接、属性を確認して、それらのレコードから企業が所有している IPv4 のインターネットアドレスを推測することで情報を補完しました。インターネットアドレスと属性の情報をさらに正確化して、分類を自動化するために、さらなる作業を行なう予定です。そうすることで、ホスティングとクラウドサービスのブロックを全体的に除外することが可能になります。

RIPE データベースに記載された自社所有の IPv4 のインターネットアドレスと DNS レコードを組み合わせて調査する今回の方法は、Rapid7 が 2018 年に実施した Fortune 500 ICER と、2019 年に実施した ASX 200 と FTSE 250 ICER の調査方法とは異なる点についてご注意願います。

---

[31] *IPv4 Brokers、 ARIN IPv4 Market Prices & Transfer Statistics、https://ipv4brokers.net/arin-ipv4-prices-transfer-statistics/ （2019 年 8 月 12 日に最終アクセス）*

オプトアウトによる不透明性の排除

本レポートのような調査は、Rapid7 の Project Sonar で提供されているような、継続的で簡易的なスキャンに依存しています。従って、数多くの企業がスキャンに対してオプトアウトした場合、インターネットリサーチのコミュニティは間違いなく痛手を被ります。将来、Project Sonar の「オプトアウト」リストによる不透明性で生じる影響を減らすには、2 つの方法が考えられます。ひとつは責任あるインターネットの市民として、Rapid7 が、オプトアウトリストのプロセスを継続する一方で、現状のオプトアウトのプロセスを年次ベースに変更する方法です。つまり、企業

に IPv4 のインターネットアドレスをオプトアウトリストに残しておくかどうか再度、確認連絡を求めていきます。そうすることで、Project Sonar によるスキャンのメリットを再度、訴求する機会が生まれ、オプトアウトリストのサイズを小さくして調査の統計的な一貫性を維持することが可能になります。

もうひとつは、本社の所在地を問わず業種内の調査対象を広げることでサンプル数を増やす方法です。この方法を採用すると、Inc. 5000、S&P 50、ASX 200、FTSE 250、DAX 30 のような他の有名企業のリストで、各業種で大幅にサンプル数を増やすことが可能です。そうすることで、不透明な IPv4 のインターネットアドレスの数を、1%未満に（恐らく）減らすことが可能です。以前に説明した属性の正確性と調査方法の改善が、対象を拡大した場合の調査結果の妥当性と調査効率を高めるための重要な要素となります。

リソースの安全性評価の強化

追加でドメイン名を見つけていく今後の作業は、本レポートの電子メールの安全性に関する分析に直接影響を与えます。さらに、本レポートでは電子メールの安全性の一面に過ぎない DMARC のみを調査しています。電子メールの安全性に関する設定で、これ以外のリソースレコードとして、Sender Policy Framework（SPF）があります。これを使用することで、スパムメールの削減や、誤った電子メールのドメインを使用した攻撃者からの防御が可能になります。将来の分析では、この点についても触れていく予定です。

その他のタイプの DNS レコードも（電子メールに関連しないものとして）、他のタイプのサイバーエクスポージャーや安全性に関して調べられるものがあります。将来の調査では、それらの情報についても探っていく予定です。

サードパーティーへの依存/リスク分析

最後になりますが、企業の DNS レコードの全般的な設定の分析によって、企業の IPv4 ネットワークがどのようにルーティングされて、Web と、Web アプリケションサービスで企業が依存しているサードパーティーのリソースがどのようにエミュレートされて、その他のものが間接的にどうのように動作しているかを把握することができました。このような外部公開情報による測定により、企業のインターネット上の全体的なプレゼンスの脆さと、すべての企業におけるサードパーティーへの依存に関するサイバーエクスポージャの全貌の双方についてレポートをまとめることができました。

調査方法

日経 225 銘柄企業を選定した理由

日本に本社を置く業種の特定企業のサイバーエクスポージャーについてデータを集計することで日本特有の状況が明らかになりました。ひとつは、インターネットアドレスの数を増やす余裕があるという点です。大量な数のある IPv6 を考慮に入れずとも、IPv4 だけで 42 億アドレス（一部は割り当てが不可能）がサポートされています。これらのアドレスは、世界のさまざまな政府、企業、サービスプロバイダーに割り当てられています。もうひとつは、動的なインフラ（クラウド）の普及の開始です。サービスのホスティングのために、インターネットアドレスを企業間で貸し出すことが一般的になってきています。これにより、従来のように（WHOIS lookup ツールを使用して）特定のインターネットアドレスを企業に紐付けることが完全にはできなくなりました。インターネットアドレスの所有者が、サイバーエクスポージャーの評価対象のサービスの所有者ではない可能性が生じているからです。[32]

インターネットアドレスを企業に紐付けて、日経 225 銘柄企業でフィルターをかける代わりに、Rapid7 では、グローバルインターネットアドレスとダイナミックなインフラでホスティングされているサービスで紐付けとフィルターをかけることで、2019 年第 2 四半期の日経 225 銘柄企業を代表的なサンプルとしました。

2019 年第 2 四半期の日経 225 銘柄企業リストを選んだ理由はいくつもあります。まず、リストには確立されたクライテリアを使用して選定された多様な企業（表 3 の通り）が含まれているからです。[33]売り上げの合計は、日本の GDP の 21%（純利益ベース）で、従業員数の合計は、グローバルで 500 万人に達します。さらに、これらの企業は、日本で設立されているので、日本を中心に見た場合のサイバーエクスポージャーを調査することで経済的な影響をモデル化にすることが可能です。

表 3：日経 225 銘柄企業の構成

INDUSTRY	NUMBER OF ORGANIZATIONS
Capital Goods/Others	35
Consumer Goods	33
Financials	21
Materials	59
Technology	57
Transportation and Utilities	20

3 社（KDDI、NTT グループ、NTT ドコモ）がクラウド、インターネット、モバイルサービスを提供しています。結果的に、インターネットに接続された大量のサブネットを持っています。本レポートの準備のための説明用にデータの分析を行なっている際、3 社のネットワーク範囲を使用

してインターネットに接続された企業とサービスプロバイダーの IPv4 のインターネットアドレスが、相互に混じり合っているため、Sonar と Heisenberg によるデバイスのカウント数が結果を歪ませることが明らかになりました。そこで、それらのインターネットアドレスはそのセクションから除外しています。しかしながら、3 社のプライマリドメインと企業 Web サイトは調査対象に含まれています。

最後になりますが、日経 225 銘柄企業は、さまざまな階層で優秀な人材を確保が可能です。これには、内部と外部のネットワークとシステムの管理者に加えて、高技能で経験のあるアプリケーション開発とオペレーションの人員も含まれます。多くの企業が、IT やインターネットの標準の制定に対してリーダシップやガバナンスを司る委員会に代表を送り込んでいます。また、多くの企業が、設立されてから 20 年以上になり、インターネット技術を先取りしてきています。別の言い方をすると、サイバーエクスポージャーの問題がこれらの企業に生じるとすれば、同じような環境ない、より小さな企業にとってサイバーエクスポージャーの問題がより深刻になることが予想されます。

---

[32] *ICANN WHOIS、https://whois.icann.org/en（2019 年 8 月 12 日に最終アクセス）*

[33] *Nikkei Stock Average Index Guidebook、 https://indexes.nikkei.co.jp/nkave/archives/file/nikkei_stock_average_guidebook_en.pdf（2019 年 8 月 12 日に最終アクセス）*

企業のインターネットアセットとメタデータの属性の調査方法

Internet Assigned Numbers Authority（IANA）は、インターネットのガバナンスの調整とスムースなオペレーションの促進を行なっています。[34]ガバナンスの 2 つの要素には、インターネットのアドレス（IP アドレス）とドメイン名（http://www.example.com のような Web アドレスをインターネットアドレスに切り替えることでシステムがインターネットのリソースに接続するシステム）があります。

インターネットアドレスと企業の紐付け

IANA は、全世界と地域の少数のインターネットレジストラに業務を委任しています。それらのレジストリは、さらに国のレジストリと地域レジストリにインターネットアドレスのブロックと割り当てられたインターネットアドレスに関連するメタデータの管理を委任しています。そして最終的には、インターネットアドレスをユーザーや組織に割り当てるインターネットサービスプロバイダ（ISP）に管理を委任しています。

インターネットアドレスの割り当てに関連する、組織名、場所情報、連絡先と場合によってはペアレントインターネットサービスプロバイダなどのメタデータは、WHOIS サービスという名称で配信されているデータベースに保存されています。WHOIS サービスは、ユーザーが IP 番号について、インターネットアドレスを保有する組織とその連絡先を含めて情報を取得できる公共のリソースです。各レジストリは、独自の WHOIS データベースを維持運営しています。[35]WHOIS を使用する個人は、システムに対して双方向のクエリを行なうことが可能で、WHOIS データベース全体のコピーは、技術的な研究目的でデータを使用する組織が利用可能です。

組織が、独自のインターネット接続のリソースを管理したい場合は、地域の ISP または地域レジストリに依頼することで、複数の連番のアドレスを使用することが可能です。これらの属性メタデータは、適切な WHOIS サービスに保存されます。どのような内容か説明をするために、表 4 は、

Rapid7 に割り当てられたインターネットアドレスブロック示しています。

表 4：Rapid7 の WHOIS レコードの概要

INTERNET ADDRESS ASSIGNMENT	WHOIS ATTRIBUTION
71.6.233.0/24	Rapid7 Labs. Traffic originating from this network is expected and part of Rapid7 Labs Project Sonar sonar.labs.rapid7.com (C07045996)
208.118.237.0/24	Rapid7 LLC (C02934565)

Fortune 500 ICER と比較して、IANA のレジストリを使用した日経 225 銘柄企業のインターネットアドレスの検索は、RIPE ネットワーク割り当てデータベースに詳細な内容が記載されているため、より簡単に行なうことが可能でした。[36] 90%以上の企業が RIPE IPv4 レジストリで識別可能です。残りの 10% が、企業に割り当てられていないのではなく、それらのブロックを紐付け用とするとエラー率が増えるからです。

エンドユーザーや事業者のインターネットサービスプロバイダである組織に割り当てられた IPv4 の範囲を除外するように細心の注意を払いました。

DNS レコードと企業の紐付け

同様な WHOIS 登録とデータベースサービスが、DNS の割り当てにも存在します。組織が取得するドメインのすべてのレコードを直接、管理するためのもので、WHOIS よりもはるかに分散されたデータベースです。ドメイン名を割り当てると（例として rapid7.com）、組織は専用の DNS サーバ（または、DNS サービスプロバイダやクラウドプロバイダ）の設定を行ない、DNS 名にさまざまなレコードタイプと値がマップされたレコードを発行し維持管理します。組織は、自在にレコードの追加、変更、削除ができます。

DNS「A」（アドレス）レコードは、インターネットアドレス（www.rapid7.com は現在、13.33.37.212 にマップされています）に名前をマップしますが、インターネット名の他のタイプの情報を関連づけることも可能です。

DNS「TXT」（テキスト）レコードは、インターネット名に属性テキスト配列を保存します。インターネット名のリソースもしくはドメイン名の正式な所有者に関する追加のメタデータを伝達する、特定フォーマットのテキストレコードの作成方法についてルールを定めたさまざまな正式標準が存在します。

DMARC[37]と SPF[38]が、組織の電子メール設定の「安全性」を推定するために重要となる 2 種類のテキストレコードです。これらの標準により、組織はどのシステムが組織のために電子メールを送信するのに認可されているのかを送信先に連絡することが可能となります。また、攻撃者により捏造された電子メールや、スパムメール送信者によるメールに対してどのような対処を行なうか設定が可能です。これらのレコードの設定がなかったり、不正な設定がされていたり、レコードの許可設定が過剰に寛容だったりすると、スパムメールの増加やフィッシング攻撃のリスクの増大が生じます。フィッシング攻撃は、過去数年間にわたり、組織における攻撃の足場としての主要な手段となってきています。従って、不適切な DMARC と SPF の設定に対して十分に注意を払わないと、組織に対する攻撃が成功してしまうリスクを著しく増大させる結果となります。こ

れらを含めてすべての DNS レコードは、誰でもクエリが可能です。エコスシステム全体に及ぶサイバーセキュリティに関する研究の一貫で、Rapid7 は、月に数百万件もの DNS lookups を行ない、タイムスタンプ付きの記録を巨大な履歴データベースに保存しています。これにより、広範囲に及ぶクエリや長期間にわたる変更履歴の確認が可能になっています。

日経 225 銘柄企業の第 2 四半期のリストには、リストの企業のよく知られているプライマリドメインが含まれています。 例として、「www.hitachi.co.jp」は、日立製作所のよく知られているドメイン名です（Technology/Electric Machinery の企業）。これらのサイトは、Project Sonar によりシステマティックにスキャンされ、企業に紐付けられ関連付けられた DNS 名が DMARC と SPF の確認のために使用されています。.

---

[34] *Internet Assigned Numbers Authority*、 *https://www.iana.org/*（*2019 年 8 月 12 日に最終アクセス*）

[35] *RIPE WHOIS Database Index*、 *https://www.ripe.net/about-us/*（*2019 年 8 月 12 日に最終アクセス*）

[36] *RIPE Database*、 *https://apps.db.ripe.net/db-web-ui/#/fulltextsearch*（*2019 年 8 月 12 日に最終アクセス*）

[37] *The DMARC Standard*、 *https://dmarc.org/*（*2019 年 8 月 12 日に最終アクセス*）

[38] *RFC 7208*、 *Sender Policy Framework*、 *Apr. 2014* *https://tools.ietf.org/html/rfc7208* （*Last accessed Aug. 12*、*2019*）

Rapid7 について

Rapid7 は、Rapid7 Insight Cloud によって、Visibility - 可視化、Analytics - 分析、Automation - 自動化をもたらし、企業のサイバーセキュリティのさらなる向上を実現します。Rapid7 のソリューションなら、複雑なタスクがシンプルになり、セキュリティ部門がより効率的に IT 部門や開発部門と共に、脆弱性を減らし、悪意ある行動を監視し、攻撃を調査し遮断し、ルーチン業務を自動化することが可能になります。全世界で、7,900 社のお客様が Rapid7 のテクノロジー、サービス、リサーチを活用することで、セキュリティを向上させています。詳しい情報は、ホームページをご覧ください。