RAPID7

調査

業界別サイバーエクスポージャーレポート（ICER）：日経225

©RAPID7 2021年

目次

目次

要旨

世界中がパンデミックに見舞われ、在宅勤務が主流となっている昨今。それを狙ったかのように脆弱な箇所にサイバー攻撃を仕掛けてくるケースが後を断ちません。また、ランサムウェアがインターネット上で猛威を振るう中、世界的企業がインターネット上でどれだけ情報の露出を意図せずにしているかを測定することは、これまで以上に重要になっています。今回のインターネットサイバーエクスポージャーレポート（ICER）では、インターネット上で、あるいはインターネットを介して事業を継続するため、また、CISO、ITセキュリティ担当者、およびその他の社内のビジネスパートナーが真っ向から取り組むためにも重要となる、5つのサイバーセキュリティ分野についてRapid7の研究者が評価しています。

インターネットに面したサイバーエクスポージャーとリスクの5つの側面は、次のとおりです。

1. 認証されたメールの送信と取り扱い（DMARC）
2. パブリックWebアプリケーション（HTTPSとHSTS）の暗号標準規格
3. Webサーバおよびメールサーバのバージョン管理（主にIIS、nginx、Apache、Exchange）
4. インターネットに適さないリスクのあるプロトコル（RDP、SMB、およびTelnet）
5. 脆弱性開示プログラム（VDP）の急増

本レポートでは、日本の日経銘柄企業225社[1]に挙げられたトップ企業について、そのインターネット上のサイバーエクスポージャーについて独自調査を実施しました。各セクションには、専門家が今すぐ実践できる現実的かつ実用的なアドバイスも含まれています。これらのアドバイスは、日経225社の企業に属するCISOにとってだけでなく、これらトップ企業のメンバーとビジネスや規制上の関係性を持つセキュリティ専門家にとっても役立つものです。

2021年上半期を通して、Rapid7は世界の先進国5カ国を対象に、サイバーセキュリティの基礎となる5つの重要な分野について測定したレポートを公開します。

1. 米国のFortune 500[2]
2. 英国のFTSE 350[3]
3. オーストラリアのASX 200[4]
4. ドイツのDeutsche Börse Prime Standard 314[5]
5. 日本の日経225（本レポート）

[1] https://indexes.nikkei.co.jp/en/nkave/index?type=index
[2] https://www.rapid7.com/research/report/2021-industry-cyber-exposure-report/
[3] https://www.rapid7.com/research/reports/2021-industry-cyber-exposure-report-uk
[4] https://www.rapid7.com/research/report/2021-industry-cyber-exposure-report-anz/
[5] https://www.rapid7.com/research/report/icer-germany-2021/

重要なポイント

本レポートは、上記に取り上げた分野をカバーする5つのセクションに分けられており、全体をまとめると次のとおりです。

- **日経225の電子メールに対するセキュリティ体制は、米国と英国に遅れをとっています。**2021年初期の時点で、日経225の電子メールセキュリティは、米国と英国の同業者に追いついていません。米国と英国におけるDMARCの採用率はおよそ50%でしたが、日本で事業を展開する調査対象企業のうち、DMARCレコードを構成していたのはわずか13%に過ぎず、その29社のうちの25社（約86%）はp=なし（またはパススルー）ポリシーを設定していました。つまり、日経225の企業のうち、DMARCの p=隔離、またはp=拒否ポリシーを通じて、自社のブランド、従業員、顧客を保護するために積極的な対策を取っているのは、わずか4社（2%以下）でした。

- **露出された、危険が伴うサービスについて日本ではあまり懸念されていません。**Windows Remote Desktop（RDP）ファイル共有（SMB）とTelnetの危険なプロトコルの露出は、調査対象企業の間で依然として問題とされていますが、米国のFortune 500でみられたほどの問題とはなっていないようです。日経225企業の90%以上にRDPとSMBに対する露出はありませんでした。

- **しかしながら、TelnetとHSTSについては依然として懸念されています。**Telnetとなると話は別で、日経225の約27%には、インターネットに露出されている何らかのレガシーtelnetがありました。また、セキュアHTTP（HTTPS）の導入について見た場合、日経225の企業の100%がHTTPSを標準で使用していることがわかりましたが、常にHTTPSインフラが使用されるようにHSTSディレクティブを実装している上場企業はわずか18%でした。

- **バージョンの分散は日本で順調に進んでいます。**日経企業のうち、（マネージドクラウドインスタンスではなく）自社のExchangeサーバーを実行しているのはわずか16社のみにとどまっており、企業の約75%がサポートされている最新バージョンのインスタンスを最低でも1つ実行していました。とはいえ、Apacheでは93の異なるバージョン、Nginxでは75の異なるバージョン、そしてIISでは17の異なるバージョンが日経225で見られました。

- **日本のテクノロジー業界は、脆弱性の開示に単独で取り組んでいます。**調査対象企業225社の中で見つかった16のVDPのうちのほぼすべてが、テクノロジー業界か、テクノロジーを多用する消費材企業に属していました。つまり、これは日本のハイテク企業にとってはかなり良いことですが、製品やインフラのVDPを標準化していないその他の日本企業にとってはあまり良いことではありません。

これらの調査結果を踏まえ、本レポートの以降のセクションでは、日経225で測定できるサイバーセキュリティの5つの各分野について調査しています。

詳しく見ていく前に、ここで1つ注意があります。あなたの組織がこういった事象の影響を受けていたり、今も影響を受けていたりする場合、緊急事態に対応することに時間とエネルギーを費やすばかりで、本レポートに解説されているような、より慢性的な問題に専念することはできないと感じられるかもしれません。組織の安全性と回復力をサポートして、これらを維持できるようにするため、Rapid7では付録も用意しています。以下のセクションへと進む前に、まずはそちらの付録をぜひご覧ください。

日経255社における
メールセキュリティ

私たちは皆、電子メールについてよく知り、好んで使っており、少なくとも依存しています。現代の通信の要となるものですが、残念ながらスプーフィングやフィッシングなどの悪意のある行動のメカニズムとして活用される可能性も非常に高いものです。

電子メールに関連した主な懸念事項はソースの信頼性です。近年では、専用の電子メール検証システムとしてDMARCが登場しました。DMARCは、Sender Policy Framework（SPF）とDomainKeys Identified Mail（DKIM）という2つの古いメール認証システムを基盤にしており、それぞれがキー署名に基づいて、メールサーバー認証（「送信者か認証されているかどうか?」）と電子メールの完全性（「コンテンツが変更されていないか?」）をチェックします。DMARCに含まれるさまざまなコンポーネントは、直接的な脅威や、パートナー、サプライヤーまたは顧客を誤解させることを目的としたスプーフィングメールなどの、評判を損なう原因となる潜在的な損害を緩和するために役立ちます。

適切に実装されたDMARCシステムでは、不正な電子メールを特定し、どのように処理するべきかを定義することができます。DMARCでは、IT管理者の積極性に応じて、疑わしいソースからの電子メールを異なるレベルで処理するように設定することができます。DMARCポリシーのオプションには、次のようなものが含まれます。

- **なし**、疑わしいメールは、DMARCからの通知の監視用に指定されたメールアドレスに報告されます。
- **検疫**、疑わしいメールはスパムフォルダに振り分けられ、その受信報告が監視用のメールアドレスに送信されます。
- **拒否**、監視用メールアドレスに通知され、疑わしいメールは一切配信されません。

メールを介した悪意のあるメッセージを緩和する有効性を備えていることから、DMARCは重要なリスク軽減策であると考えられ、その実装が強く推奨されます。残念ながら、DMARCのメリットは広範囲にわたるものの、グローバルには実装されていません。DMARCの実装は、パブリックドメインシステム（DNS）レコードで追跡されます。組織がDMARCを利用しているかどうかは、組織が公開するDMARCレコードを調査するだけでわかります。日経組織の主要な有名ドメインと、DNSに表示されるこれらの組織のDMARCレコードを比較することで、DMARCの実装の規模と種類を見分けることができます。

なお、本調査では、主に組織のAPEXドメインに注力しており、組織が所有する他のドメインについては深く調査していません。Rapid7では、組織によってドメインセットの所有権が大きく異なる可能性があるため、この方法を選択しました。APEXドメインに注力して、事実上、それを組織全体のメールセキュリティ対策への姿勢を示す指標として扱うことができます。結局のところ、組織がプライマリドメインにDMARCを実装していない場合、その組織がより重要度の低いドメイン全体で健全なメール体制を実践しているとは言えなくなるからです。

公開されているDMARCレコードは、アクセス性を高く保つことを意図したものです。これらのレコードは、メール受信者が、DMARCを利用してメールを検証する方法を判断するための手段であり、DMARC検証に失敗したメールを受信した場合に通知するメールアドレスと、無効なメールを処理する際に適用すべきDMARCポリシーを特定するための手段となります。

結果

日経225組織のうちの29社（約13%）が、主要なドメインにDMARCを実装しており、そのすべては有効にフォーマットされていました。ICERシリーズでこれまでに調査した国別インデックス企業と比較すると、DMARCのカバー率は非常に低くなっています。

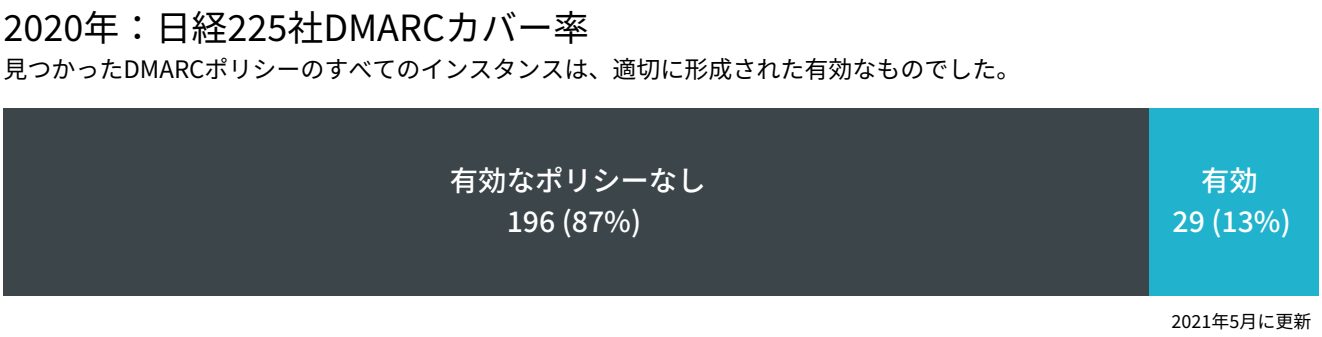

図1：2020年日経企業のDMARCカバー率

DMARCポリシーをさらに詳しく調査した結果、有効になっているDMARCポリシーのほとんどは「なし」と設定されているか、単純に監視および通知してから「拒否」と設定されていることがわかりました。これは最も積極的なアプローチです。最も少なかったポリシー実装は、疑わしいメールを隔離するためのポリシーである「検疫」でした。とはいえ、数値がかなり小さかったことから、これらの結果からパターンを描こうとしても意味がありません。

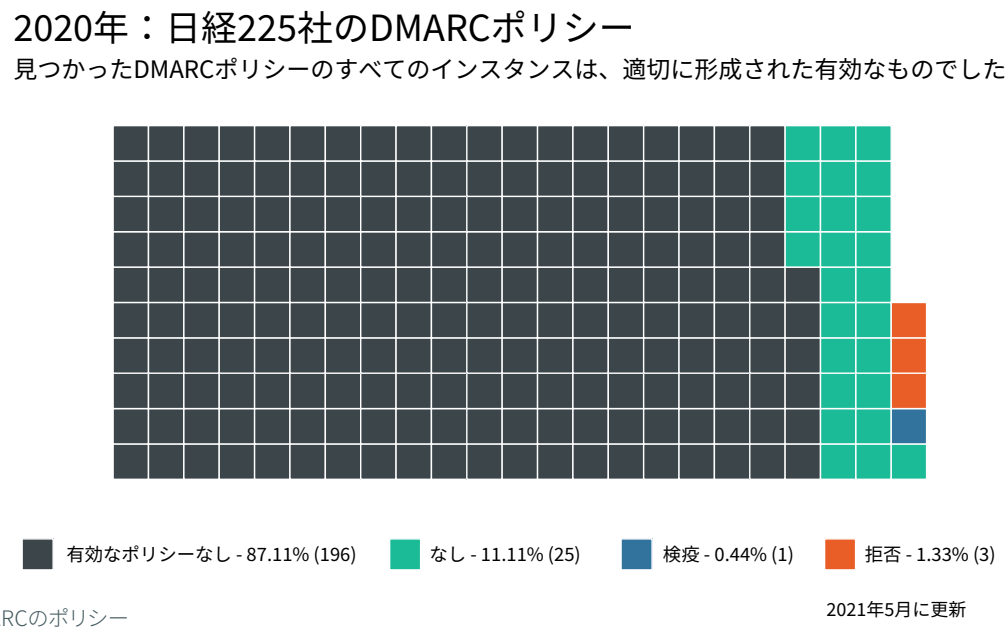

図2：2020年日経DMARCのポリシー

業種別

また、組織を業種別に分ければ、業種ごとのDMARCのバリエーションについても理解することができます。日経225で最も注目される業種はテクノロジーおよび原材料産業です。

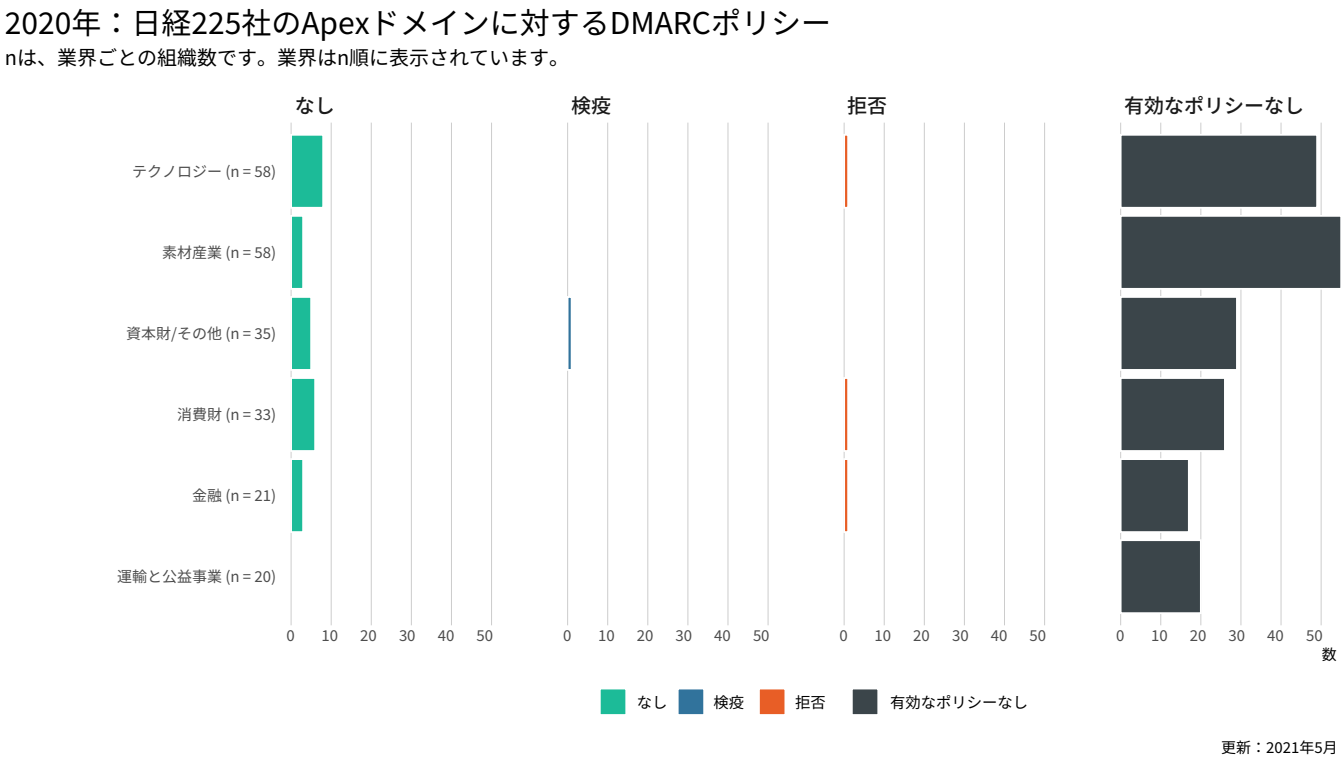

図3：2020年Apexドメインの日経企業DMARCポリシー

CISOへの重要ポイント

組織にDMARCが既に実装されていないのであれば、プロアクティブな対策を実施して設定してください。

今日では、DMARCはメールの衛生管理の基礎となるものと考えられており、最新の情報セキュリティ規範に対する組織の取り組みを広く示しています。また、DMARCを実装していない場合、組織は、規模、ソース、および深刻度に関する情報が得られるDMARC監視によってキャプチャーされなかった悪意のあるメールキャンペーンに気づかない可能性があります。

DMARCを実装する決定を下したら、ポリシーの実装についてより慎重に検討する必要があります。積極的な拒否ポリシーの場合、非常に安全性は高くなりますが、正当なメールがブロックされる可能性があります。より寛容な検疫ポリシーの場合、悪化の防止と何らかの形の救済とのバランスの釣り合いを取ることができます。少なくとも、不正なメールや設定が不十分なメールのトラフィックを監視するために、何らかの形式のDMARCを実装する必要があります。

Webサービスセキュリティ
日経225社

平均的な人のテクノロジーでのやり取りの大半は、何らかの形のWebアプリケーションを通したものですが、何が「Webアプリ」を構成しているのかは非常に不明瞭であり、こういったアプリケーションを強化するためのセキュリティ対策も同様に広範なものです。API、分散認証スキーム、単1ページアプリケーション、および静的Webサイトはすべて、「Webアプリケーション」の一般的なカテゴリに入る可能性があります。参照しているアプリケーションの具体的なタイプをさらに細分化することなく、広範にわたるすべてのWebアプリケーションに適用されるセキュリティ対策はほとんどありません。しかしながら、本レポートで調査したものがいくつかあります。

すべてのWebアプリケーションには、わずかな例外があるとしても、強力な暗号化が必要です。これは、個人を識別可能な情報（PII）などの重要な情報や機密情報を提供するアプリケーションにとって最も重要なものですが、静的な情報コンテンツのみを提供する場合にも重要となります。よくある誤解に、保護されていない接続を使用した場合の唯一のリスクは、機密性の喪失であるというものがあります。ユーザーが閲覧している情報が悪意のある第三者によって観察されてしまうというものです。これも確かにリスクではありますが、暗号化が欠如していることで、接続を変更される脆弱性が生じる（完全性の喪失）という点は見落とされがちです。つまり、悪意のある第三者が機密情報を監視できる可能性だけでなく、これらの情報が変更されたり、ユーザーを侵害する恐れのある第三者のコンテンツが注入されたりする可能性もあるということです。

Webアプリケーションが機密情報を提供しているのか、猫の可愛い写真を提供しているのかに関係なく、悪意のあるコンテンツがインジェクションされるリスクは存在します[6]。このような、サイトのユーザーやサイト所有者のブランド評価に対する普遍的なリスクがあることから、Rapid7では、強力な暗号化（ここではTLS）のサポートと、 HTTP Strict Transport Security（HSTS）を通した使用の実施について検討しています。本セクションでは、企業のブランド評価に最も影響を与えるドメインであることから、各企業の主要ドメインについて調査しています。

HTTPSサポート

HTTPSは、Webトラフィックの暗号化と安全性を保証するプロトコルです。環境でHTTPSを設定できる方法はいくつかあります。

- 利用不可（HTTPのみ）
- 利用可能で任意
- 必須（HTTPの「厳格なトランスポートセキュリティ」またはHSTSを設定済み）
- HSTSのプリローディングに必須

サイトでHTTPSをサポートすることは、ウェブ上での存在感を示すためには絶対に必要な要素であり、その次にくるのが暗号化の義務です。HSTSのプリローディングにはいくつかの技術的な課題もありますが、これはWebセキュリティプログラムが積極的に取り組むべき課題です。

それでは、まずは良いニュースからご紹介しましょう。日経225で調査したサイトのうち、100%がHTTPSをサポートしていました。

[6] https://www.sanrio.co.jp/

HSTSの採用

HSTSの採用に関する見通しは、残念ながら少し厳しいものでした。

ご覧の通り、調査したサイトのうちHSTSをサポートしているのは約18%のみでした。これは、他のレポートで見られた数値と比べてかなり少ないものです。サイトがすでにHTTPSをフルサポートしている場合（これらのサイトはすべてサポートしています）、ユーザーがサイトの安全なバージョンを確実に訪問できるように、HSTSを実装するのは比較的簡単なはずです。これらのサイトのほとんどは、安全でないバージョンのホームページからのリダイレクトを提供していますが、これでは中間者（MiTM）攻撃を緩和できるわけではありません。

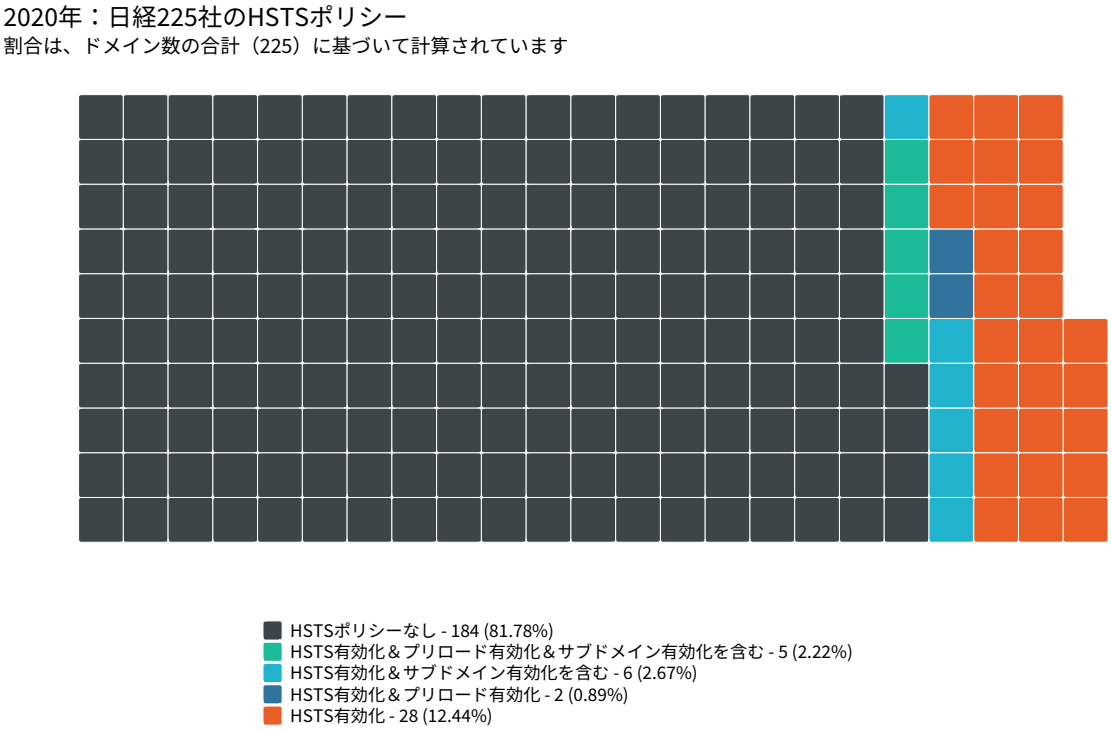

図4：2020年日経225社のHSTSポリシー

調査したドメインに、HSTSを手動で無効化しているドメインはありませんでした。この設定のドメインの割合は低い傾向にあったことから、この調査結果は、このリストに含まれているHSTSをサポートするドメインの合計数が少ないことによるものと見られます。
HSTSをサポートするサイトの27%は、「includeSubDomains」ディレクティブもサポートしており、ドメイン全体とすべてのサブドメインも保護しています。これは素晴らしいセキュリティ機能ですが、状況によっては実装するのが困難な場合があります。

HSTSを搭載したサイトの17%は、「プリロード」ディレクティブもサポートしています。このディレクティブにより、クローラーは、サイトをHSTSをサポートする既知のサイトのグローバルリストに自動的に追加するようになります。サポートするブラウザがHSTSのプリロードを有効にしたサイトに誘導された場合、最初の接続は常にHTTPSを通したものになります。つまり、サイトのユーザーがMiTM攻撃を受けやすいたった1つの場所、HSTSヘッダーが出現する前にサイトへ最初に接続される場所が排除されることになります。この設定オプションは、ユーザーのためにさらなる保護レイヤーを追加する簡単な方法です。HSTSを有効化するのであれば、このオプションはぜひ追加しておく必要があります。ブラウザのサポートが少ない比較的新しいディレクティブではありますが、含めることによるデメリットはありません（HSTSをサポートしていないブラウザは単純に無視します）。

概要

ユーザーに面するドメインへのトラフィックを保護し暗号化することは、良い実践であるだけでなく、企業のブランドも保護することになります。この数年間にわたり、TLSでHTTPを保護することがWebセキュリティコミュニティの主要な関心事となっていますが、これにはちゃんとした理由があります。日経225の企業はすべて、主要なWebサイトの安全なバージョンを提供していますが、ベストプラクティスの観点からはまだまだ不十分です。

日経225全体でHSTSの採用がとりわけ不十分な状態は、これらの企業のアプリケーションセキュリティプログラムが遅れていることを示している可能性があります。他のより洗練された緩和策は実装がかなり複雑なものになる可能性があることを考えればなおさらです。基準が進むスピードは確かに速いものですが、このスピードについていくことが重要です。ブランドの評判に影響が出る場合は特にそうです。

CISOへの重要ポイント

サイトの暗号化についてしばらく考慮していなかったのであれば、今がその時かもしれません。消費者に面するWebアプリケーションがセキュリティ障害に見舞われると、企業のブランドに対する評価が損なわれます。さまざまなセキュリティプログラムの投資に対する意思決定を行う際にはこの事実を考慮することが重要です。

あなたの企業のWebサイトがHSTSをサポートしていないのであれば、その理由を知ることに価値があるかもしれません。技術的な制約ですか？それとも組織的、あるいは予算上の制約ですか？原因を見いだすことが、アプリケーションセキュリティプログラム全体を見直すのにぴったりのきっかけとなるかもしれません。

日経225における
バージョン管理の複雑さ

組織でセキュリティを成功させるためには、複雑性が敵となります。システム、テクノロジー、およびビジネスプロセスに多様性があると、非常に成熟したセキュリティチームでさえ日々直面する現実的な課題となります。パッチや脆弱性の管理という面では特にそうです。

たった1つの主要な脆弱性にパッチを適用するだけでも、多くの場合至難の業となり得ます。多様性は、それぞれの技術コンポーネントの中に複雑さを生み出します。つまり、1つの組織で数多くの異なるWebサーバーテクノロジーが使用されている可能性があります。その結果、それぞれのテクノロジーに独自のバージョンが存在する可能性があり、これによって構成管理やパッチ管理に直接的な（そして否定的な）影響がおよびます。

この分野において、これらのリソース豊かな組織がどのようなパフォーマンスを発揮しているかを知るために、Rapid7では3つの要因について調査しました。

1. 各組織が使用している、Webサーバーという特定の技術のポートフォリオにおける多様性
2. このポートフォリオの維持管理状況
3. 組織における、メールゲートウェイなどの重要なサービスの維持管理状況

調査では次の事項がわかりました。

- 単一のテクノロジースタック（Webサーバー）においては、資本財/その他、消費財、テクノロジー、運輸、公益事業などのいくつかの主要な業種の組織が、**9種類以上の異なるバージョンのApacheおよび/またはNginxに露出していました。**資本財/その他、消費財、テクノロジー、運輸、公益事業の業種では、1社以上の組織が、3種類上の異なるバージョンのIISに露出していました。**これにより、それぞれの攻撃面が増加しており**、テストと品質保証が複雑になることから（わざわざパッチを適用する場合）パッチの導入が困難になっています。

- 一部の組織では、Microsoft Exchangeなどの**重要なITインフラを最新の状態**に保つことが非常に困難になっています。驚くべきことに、日経225の約75%（16社中12社）が、依然として少なくとも1つの現行のサポートされているバージョンのExchangeを、自社でホストしているMicrosoft Exchangeで実行していました。その一方で、約56%（16社中9社）が、少なくとも1つのサポートが終了したExchange 2010を使用しており、**将来的に脆弱性が悪用される危険性がありました。**[7]

Rapid7では、Project Sonar[8]とRecog[9]を使用して、日経225の各組織で使用されているWebサーバー、ファイルサーバー、DNS、SSHなどのインターネットに面するテクノロジーを特定しました。その後、これらの技術を利用可能なCommon Platform Enumeration[10]（CPE）文字列にマッピングしました。この方法では、結果が制約されることからいくつかの制限が生じます。

- Recogで利用できるフィンガープリント
- フィンガープリントが可能な各サービスがどの程度混乱しているか（Recogがバージョン情報を抽出できるかどうか）

[7] 同じ組織内で、既存のExchangeとサポートが終了したExchangeの両方を稼働させることができるため、これを合計すると100%以上になります。
[8] https://www.rapid7.com/research/project-sonar
[9] https://github.com/rapid7/recog
[10] 共通プラットフォーム一覧の定義とデータベース：https://nvd.nist.gov/products/cpe

- Project Sonarが調査するポートとプロトコル
- IPv4アドレスのみに対するRapid7の測定
- SonarのIPv4のオプトアウト要求への対応

これらの制約があることから、どちらかというと、調査結果の程度が過小評価される傾向にあります。

Webサーバー間のバージョン分散

2018年に、日経225のサイバーエクスポージャーについて調査を開始した頃、私達は個々の組織がインターネットに露出しているサービスコンポーネント内にあるバージョンの多様性を指す言葉として、「バージョン分散」という言葉を作りました。Kubernetes[12]などの企業向けのツールが急激に使用されるようになり[11]、これまで測定していたIIS、Apache、Nginxの3つのWebサーバーで見られたバージョン分散は、減少するであろうと予想していました。

Apacheでは少なくとも93の異なるバージョン、Nginxでは75の異なるバージョン[13]、そして17-そうです。17ものIISバージョン[14]が日経225の組織全体で実行されていました。これを業界別に見てみましょう。

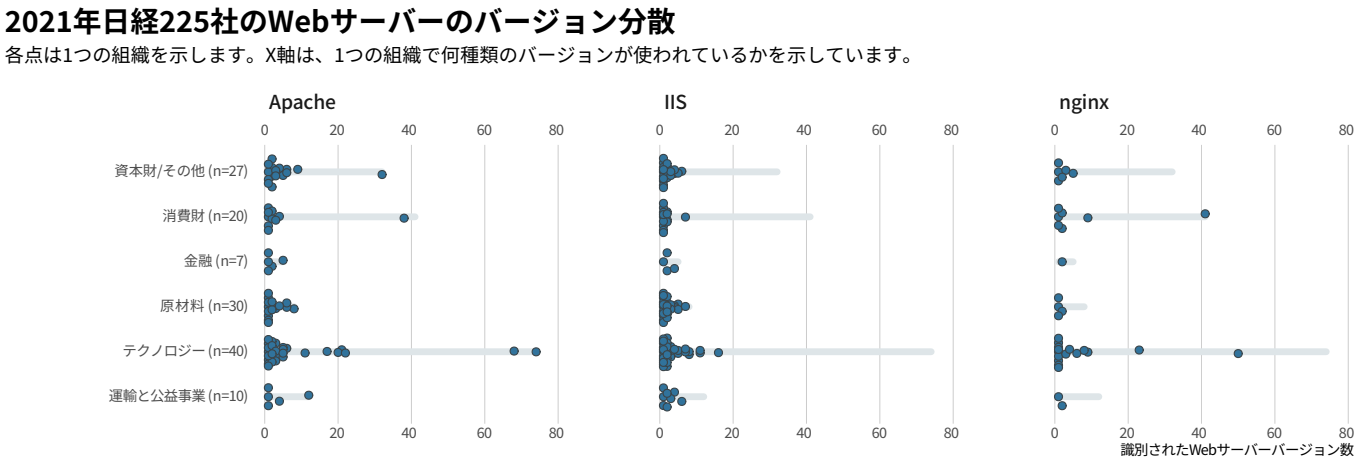

図5：2021年日経225の組織におけるWebサーバーのバージョン分散

X軸で「1」に向かうポイントの密度が高いほど、それらのポイントが存在する各組織が、バージョン分散が少ない状態で運営されていることを示しています。サーバーやサービスの導入と設定の管理も向上し、パッチをテストするバージョンが少なくなるため、他社よりも迅速に、そしてより確実に変更を加えることができます。また、X軸でより右側寄りの組織よりも、「インターネット上でサーバーを展開するには、この条件を満たさなければならない」というより厳格なルールがあるということになります。

[11] Cloud Native Computing Foundationによる2019年の調査では、**回答者の78%がKubernetesを本番環境で使用していることがわかりました。2018年の58%から大幅に増加しています。**

[12] Kubernetesのメインサイト：**https://kubernetes.io**

[13] 部の組織は、特定のサーバータイプを使用していることを発表していますが、個別のバージョン番号は伏せられています。

[14] IISの展開において、公開されたサーバーのヘッダーバナーにIISのビルド文字列が漏れる現象が頻繁に発生しています。

攻撃者もサイバー保険の査定者もこういった状況に気付いており、より「未開拓の領域」を示している組織をターゲットにする可能性があります。日経225におけるWebサーバーバーのバージョン分散と、ICER　FTSE 350およびICER Fortune 500 で報告されたバージョン分散には、大きな違いがあります。その理由のうちの1つが、日経に上場している企業が、「クラウド」を好む傾向にあることです。これは、自社が露出するWebサービスから提供される情報やサービスで、より迅速なグローバル接続性を確保するためのようです。ICERでは「クラウド」上にあるアセットについて測定していません。ですからこのポジティブな結果には、上記の注意点も含まれます。

バージョン分散：Microsoft Exchangeにフォーカス

インターネットに面するサービスの中には、他よりも重要なものがあります。古いApache HTTPDサーバーがインターネットに接続されていることも問題ですが、ここにあるのはサービス妨害の弱点のみです。ですが、Microsoft ExchangeサーバーやVPN/ゲートウェイ/リモートアクセスサービスなどのほとんどの組織が重要なインフラストラクチャとみなす（またはみなされるべき）ものの、古いバージョンを実行することは、まったく別の話です。

これらの組織が重要なサービスをどのように維持しているのかを理解するため、Microsoft Exchangeの衛生状態について調査しました。Fortune 500の組織とは異なり、日経225の組織のうち、少なくとも1つのインターネットに面するExchangeサーバーがビジネスに重要なメールを処理していたのは6%のみでした[15]。Exchangeには、長年にわたってさまざまな重要度の高い脆弱性が見つかっています。

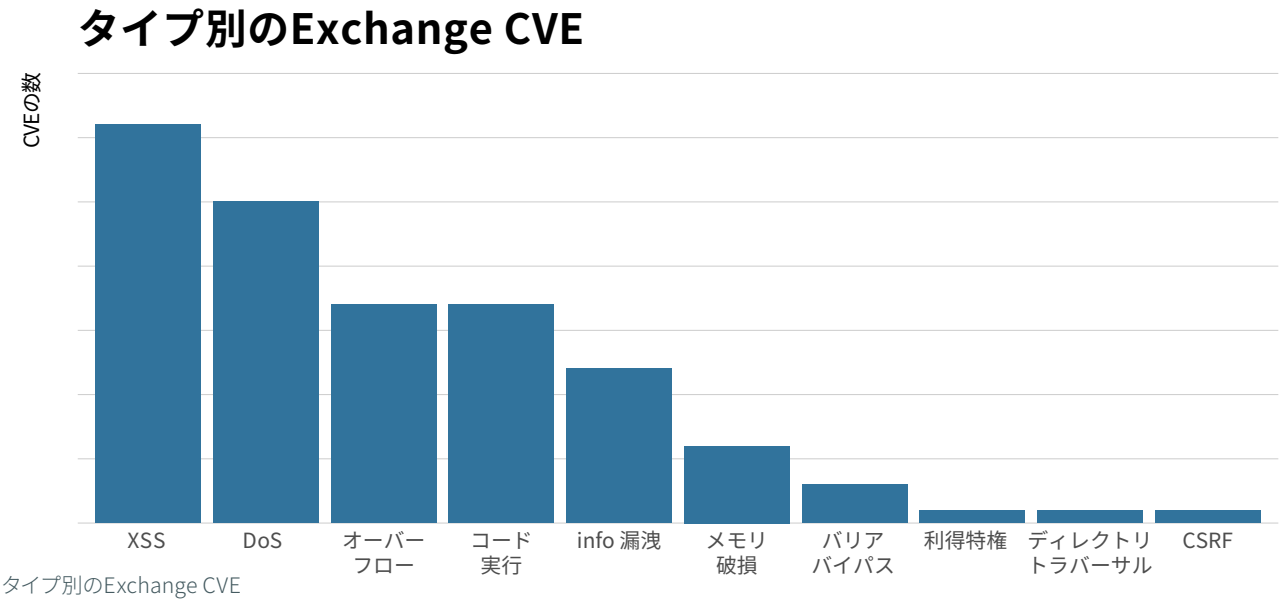

図6：タイプ別のExchange CVE

16の組織（一般的なサービスホスティングを許可する2つのISPを除く）は、メールを自社でホスティングすることを選択していますから、自己ホスト型Exchangeで直面する危険性についてもちろん知っており、少なくとも、セキュリティパッチに関しては、この重要なサービスが最高の回復力を持つように注意しているはずです。本当にそうでしょうか？

[15] Microsoft 365/Office 365の導入は全般的に大きな伸びを続けており、Fortune 500企業の70%がホスト型Exchangeを含む1つ以上のサービスを利用しています。出典：https://www.thexyz.com/blog/microsoft-office-365-usage-statistics/

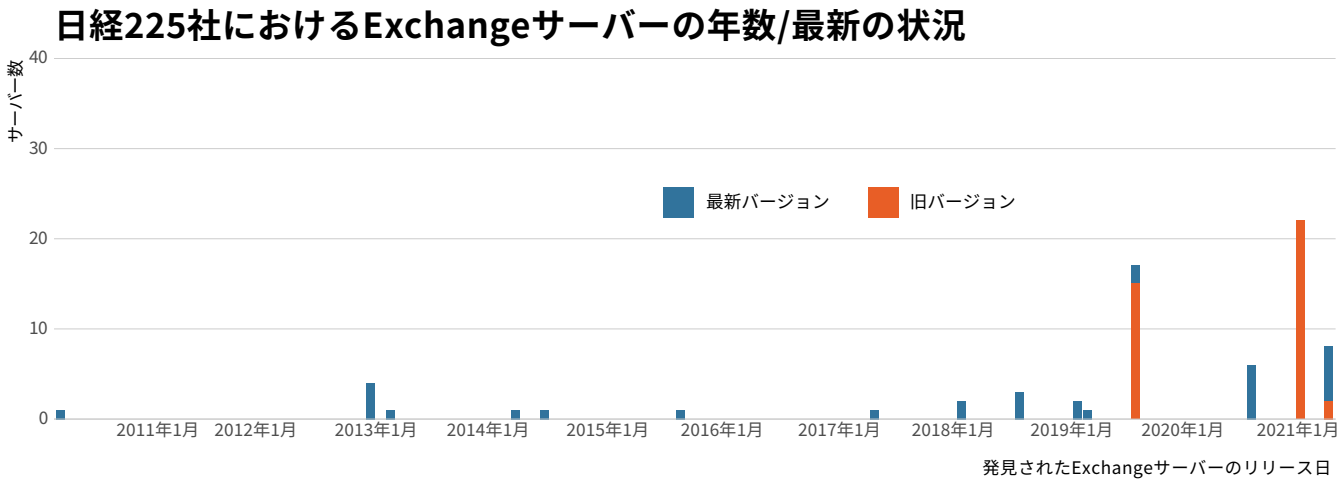

図8：日経225の日経におけるExchangeサーバーの年齢/最新の状況

上記の図は、日経225におけるMicrosoft Exchangeの状況が、その普及（一部のサーバーバージョンの古さ）と、導入されているバージョンに対する標準的なMicrosoftサポート契約[17]でのサポート状況[16]という両方の点において、かなり憂慮すべき状況であることを示しています。プラス面は、検出されたバージョンのうちフィンガープリントされたインスタンスの50%強が2020/2021年にリリースされたものであることです。

ASX 200 ICERでの調査結果が再現されて、（長い間サポートが終了した状態にある）Exchange 2007がゼロになることを期待していましたが、残念ながら、主要なテクノロジー企業で1つのインスタンスが見つかりました。また、日経225の数社には、2020年10月には、Exchange 2010のサポートが終了すること[18]が伝わっていなかったようです。

[16] https://docs.microsoft.com/en-us/exchange/new-features/build-numbers-and-release-dates
[17] Microsoftとのカスタムサポート契約や延長サポート契約がある場合については考慮されていませんが、脆弱性の悪用に関しては、これはほとんど関係ありません。
[18] https://docs.microsoft.com/en-us/microsoft-365/enterprise/exchange-2010-end-of-support?view=o365-worldwide

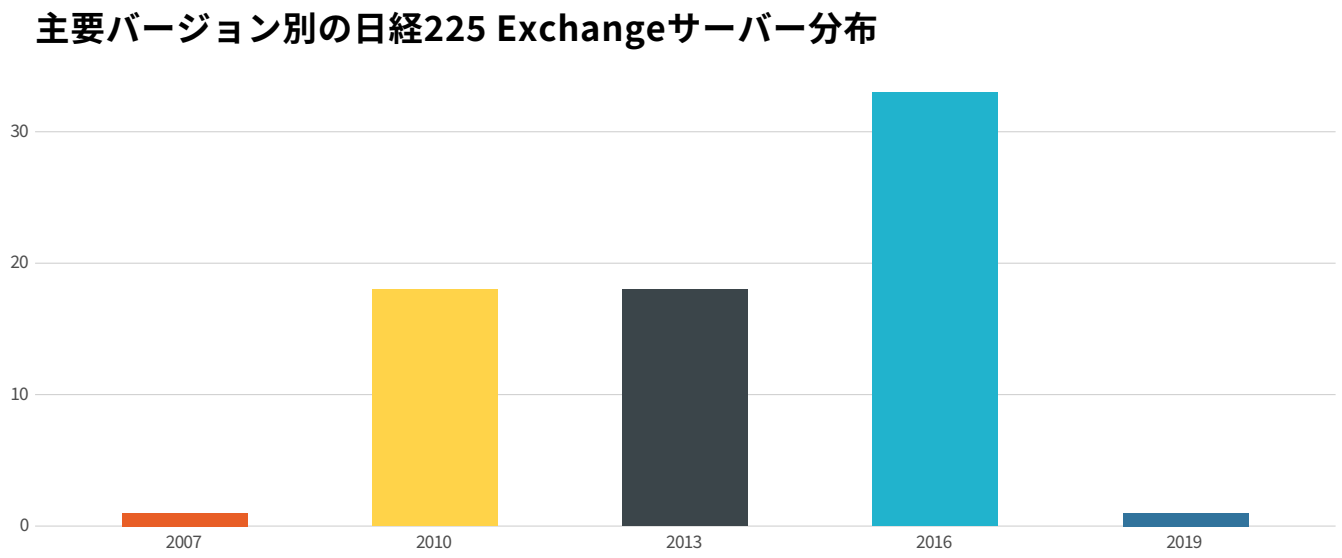

図9：日経225 Exchange Server主要バージョンの分布

あなたの組織がExchangeへのパッチ適用に苦労しているのなら、その言い訳は通用するかもしれません。少なくとも最新バージョンのExchangeの年度内のアップデートの量を見れば、Microsoftがいかにあなたを忙しくさせているのかがわかります。

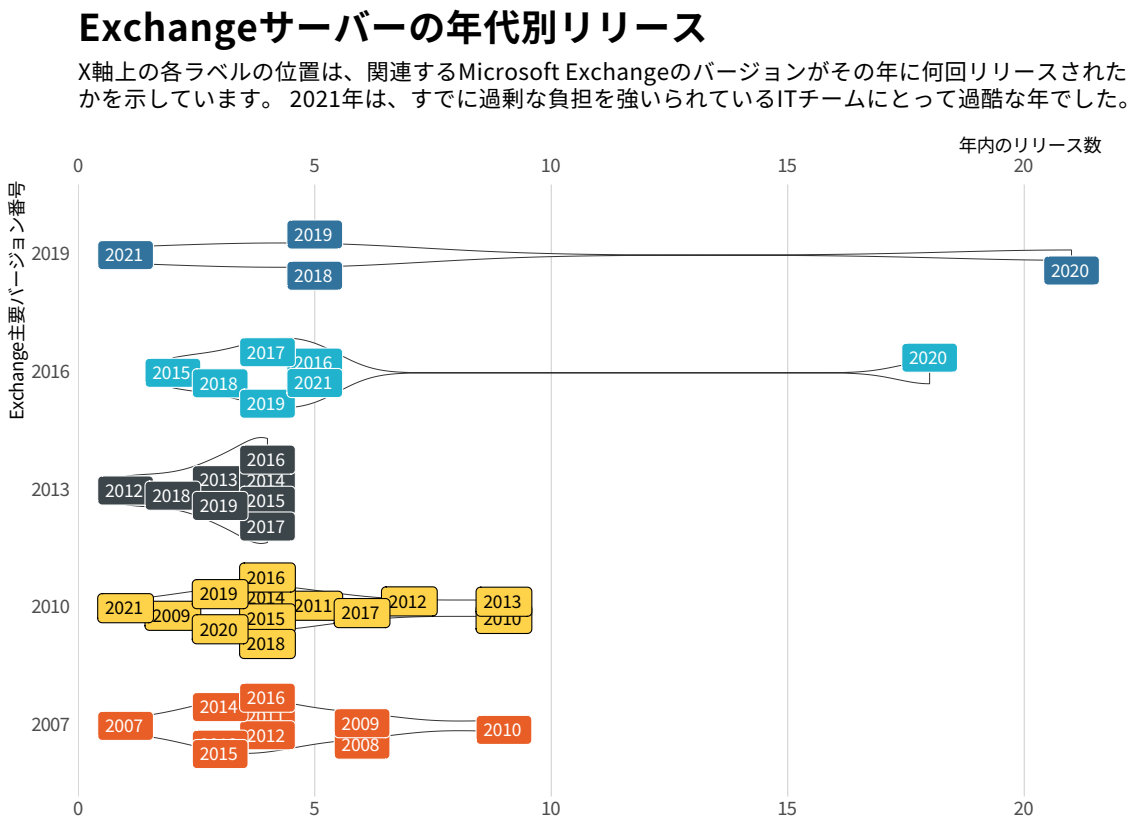

図10：年別のExchange Serverリリース

依然として、業界全体の見通しはかなり厳しいものです。[19]図11は、各業界における Exchange のリリースとサポート状況を示していますが、ほぼすべての業界が最新の状態を維持するのに苦労しています。

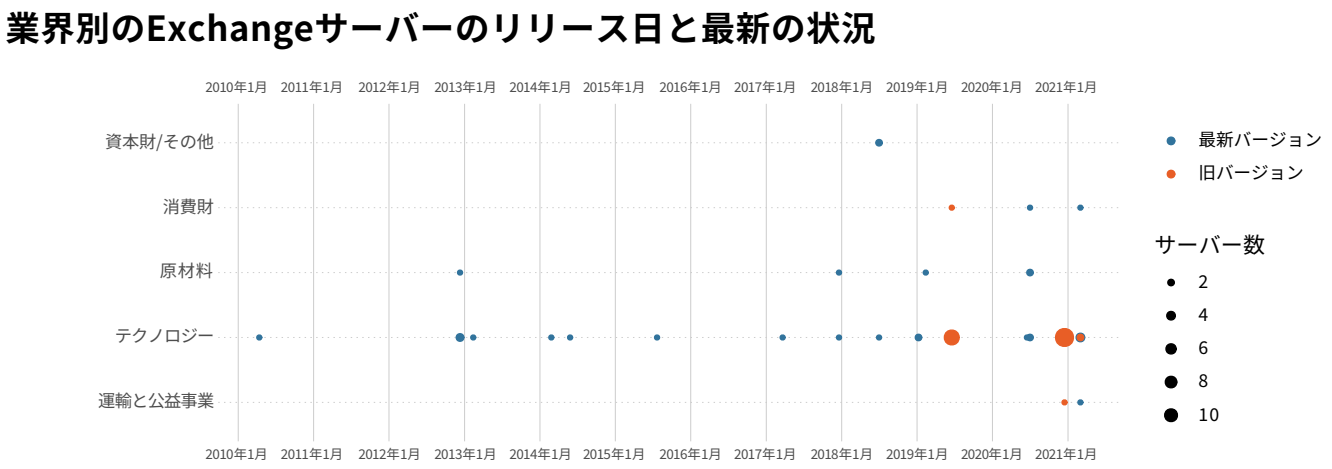

図11：業界別のExchange Serverのリリース日と最新の状況

Exchangeの導入を更新して、安全性を保ち回復力を備えることが難しいと感じるのであれば、Microsoftでさえ、ホストしているExchange（Microsoft 365）のビルドレベルを正規化しようとして問題を抱えているので安心してください。しかしながら、このグラフは、ICER Fortune 500で使用された2020年12月のスナップショットと比べるとはるかにましなものです。ICER Fortune 500のスナップショットでは、最新の導入が図の「中央に固まっている」状態となり、ほぼ同じ数の分散バージョンがインターネットの端に残っていました。

[19] わかりやすいダジャレです。

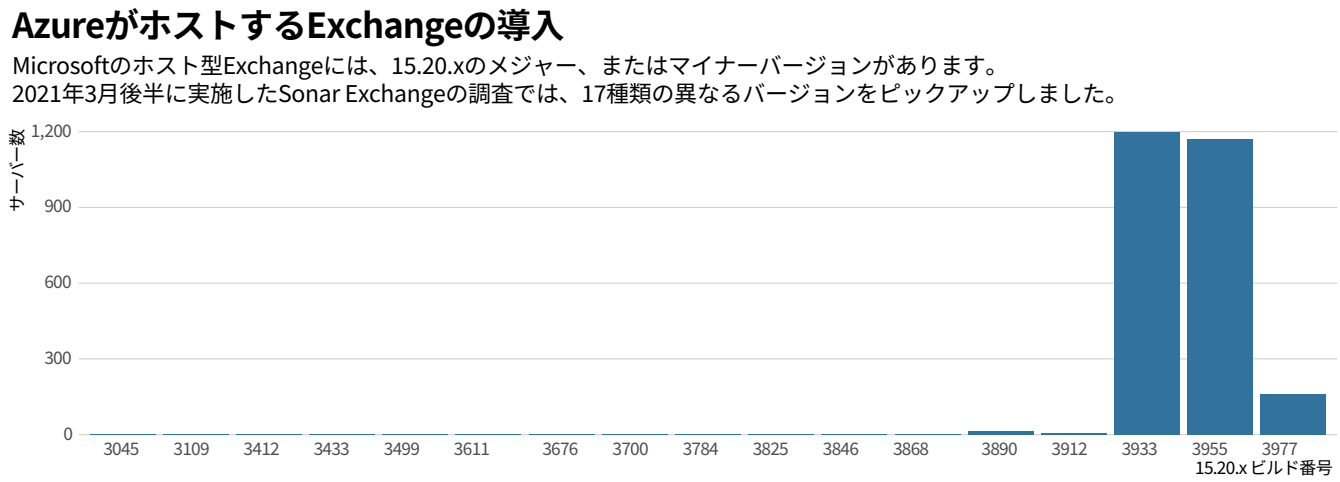

図12：AzureがホストするExchangeの導入

CISOへの重要ポイント

本章では、異なる2つのタイプのCISOに対して説明しています。各分野の典型的なCISOとなる人と、このような組織をビジネスパートナーまたはサプライヤーとして抱える人です。

もしあなたが、組織のDNAに回復力と安全性を構築するために取り組むセキュリティリーダーなのであれば、テクノロジーの乱用、バージョン管理、重要なサービスの維持などの問題は、譲れない必須事項です。幸い、これらの問題は単なる「セキュリティ」問題ではありません。組織は、ビジネスのニーズを満たすためにサービスを導入しています。そして維持するものの変化要素が少ないほど、サービスのアップタイムや安定性を維持することも、はるかに容易になります。同僚からの同意を得るために、サービスの低下（および/または停止）に関するこれまでの履歴データと最新のデータを収集してください。そしてこれらのデータに、IT、アプリケーション、および運用チームが各ビジネスプロセスの各要素をサポートするために必要となる時間を追加します。特定された弱点の数と深刻度（CVEベースまたはその他）に関する情報と組み合わせれば、改善のための協力を確保できる、堅固なビジネスケースのある領域を見つけることができます。それぞれの分野が改善されていく中で、遅れている他の分野に影響を与える力も大きくなります。

本セクションで判明した事項に身震いした人は、組織内のビジネスプロセスのステークホルダーを代表してサードパーティを評価する際に、これらの項目を確認してください。このような潜在的な弱点についてしっかりと質問し[20]、受け取った回答が正確であるかどうかを確認するのは非常に簡単です。組織の内部エクスポージャーが外部から見えるエクスポージャーを反映しているという保証はありません。しかしながら、一般的には、社内の様子は、外部の世界に示されているものよりもさらに悪いものである可能性が高いのです。パートナーとサプライヤーをより高いレベルの安全性と回復力に保つことは、組織へのリスクを軽減するだけでなく、他の組織があなたが設定した基準に従うことで、連鎖的なプラスの効果をもたらします。

[20] しかも無料です！https://opendata.rapid7.com/

日経225における高リスクサービス

一般的に、インターネット上で公開されている場合、リスクが高いと考えられる特定のサービスがあります。例えば、SMBファイル共有をインターネットに置いて共有することは、ごく少数の例外を除き[21]悪いこととみなされています。これにより、データが漏洩したり、ドメイン名などの環境情報が流出したり、認証情報に対するブルートフォース攻撃が可能になったり、Conficker[22]やWannaCry[23]ワームに見られるようなWindows Server Message Block（SMB）実装における脆弱性を利用できる攻撃ベクトルが提供されたりする可能性があります。

公共のインターネットを調査するときには、表面的な情報しか見ていないことはわかっているため、これらのサービスを運営している組織について何か理解できる方法はないか、常に見つけようとしています。構成やプロトコルの詳細を見ることで、組織の内部環境やセキュリティの成熟度を示す指標とすることができます。

例えば、SMBサービスが見つかり、それがWindows Vista[25]やServer 2008で導入されたSMBv2[24]をサポートしていないことが検出できれば、オペレーティングシステムの年代および/またはレガシー互換性の要件について、ある程度の仮定を立てることができます。

組織が異なる国からのルーターへのTelnet[26]接続を許可している場合は、機器の年代や、安全なプロトコルやネットワークアクセス制御リスト（ACL）に対するセキュリティポリシーについて推測することができます。

この分野での日経225社のパフォーマンスを把握するため、パブリックIPv4アドレス空間のデフォルトポート上のSMB、Windows Remote Desktop Protocol（RDP）、およびTelnetを調査し、サービスデータがある場合はそれについても確認しました。

調査では次の事項がわかりました。

- ルーターやスイッチでは、依然としてTelnetベースの制御が頻繁に使用されていました。
- SMBを公開しているホストのすべてでは、ホスト上で構成されているSMBのホスト名、DNS名、完全修飾ドメイン名（FQDN）がすべて漏洩していました。
- 18の企業で89のRDPサービスが検出されました。この状況は、1社の影響が大きいことから、消費財業種に大きく偏っていました。

私達は、Project SonarとRecogを使用して、日経225の各組織で使用されているデフォルトポートでインターネットに面しているSMB、Windows Remote Desktop Protocol（RDP）[27]、およびTelnetサービスを特定しました。いずれの場合も、プロトコルを完全にネゴシエートして、実際に期待されるサービスと通信できていることを確認しました。この方法では、次の点によって結果が限定されるという制限があります。

[21] https://docs.microsoft.com/en-us/sysinternals/
[22] https://en.wikipedia.org/wiki/Conficker
[23] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
[24] https://wiki.wireshark.org/SMB2
[25] 現在、ほとんどの州では運転できる年齢になるほど古いものです（2006年11月に誕生しました）。
[26] https://en.wikipedia.org/wiki/Telnet
[27] https://en.wikipedia.org/wiki/Remote_Desktop_Protocol

この方法では、次の点によって結果が限定されるという制限があります。

- サービスは、デフォルトのポートでのみ観察されます。Telnetやあまり一般的ではないRDPは、デフォルトではないポートに移動する可能性があります。
- 測定はIPv4空間のみで行われます。
- リクエストにより、一部のIP範囲はSonarでは調査されません。
- 一部のクラウドやISP関連の範囲は除外されています。この除外の影響は、企業によって大きく異なります。
- 一部のネットワークは、顧客に割り当てられたり、その他のサードパーティに割り当てられたりしている場合に除外されます。

すべての条件が同じ場合、これらの制約によって、調査結果が過小評価される可能性があります。
ISPネットワーク上のSMBプロトコルに関して、特別な注意があります。通常どおり、日経225社のISP部門で使用されているデータセットからは一部のネットワークを除外しています。これは、私たちが注目している組織の企業セキュリティ対策を反映した結果ではないからです。とは言え、これらのISPに割り当てられたネットワークについては、900近くのSMBエンドポイントを観察しています。SMBに関連するリスクを考慮して、住宅および商業向けISPには、SMBトラフィックを完全にブロックすることを強く推奨します。

調査結果：RDP、SMB、およびTelnet

まずは、成熟したセキュリティプログラムを持つ組織では、**これらのサービスが公共のインターネットで利用可能になる数はゼロでなければ許容できない**ということを強調したいと思います。Rapid7のブログや過去のRapid7の調査レポートをご覧になった方なら、このアドバイスをよくご存知だと思いますが、2021年のカレンダーを見ると、インターネット上で最後に大規模なワームが発生してからしばらく経っていることに、注意する必要があります。NotPetya（SMB）は2018年、WannaCry（SMBも）は2017年、そしてMirai（Telnet）は2016年に発生しました。2019年と2020年には脆弱性やエクスプロイトが次々と発見されましたが、安全でないサービスのオープンポートで自己増殖する問題は、いつ発生してもおかしくないようです。このようなサービスに触れる機会をなくすことで、後々の後始末にかかる時間を確実に短縮することができます。

Windowsリモートデスクトッププロトコル（RDP）

RDPはこのルールの例外と考える人もいるかもしれませんが、仮想プライベートネットワーク（VPN）、RDPゲートウェイサーバー、ファイアウォールのアクセス制御リスト（ACL）など、一般的に利用可能な技術があり、この技術に関するリスクを取り除くことができることから、通常は**RDPを組織外のソースアドレスに公開すべきではなりません。**

RDPに関する話題ですから、まずは調査結果をもとに解説していきましょう。3389/tcpのデフォルトのRDPポートでは、18の企業で89のサービスが観察されました。消費財業界の組織の1つが、観察されたRDPサービスの45%を占めています。

業界別のポート3389分布

各点は1つの組織を表しています。X軸上の位置=見つかったその企業が所有するサーバー数

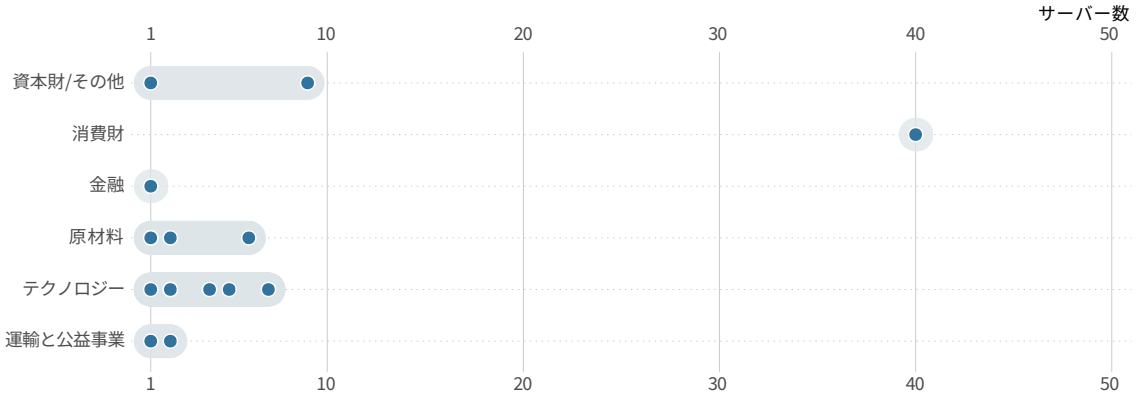

図13：業界別のポート3389分布

上記の図は、総合的な数のほとんどは少数の企業に起因していることを示していますが、数多くの業種が存在していることがわかります。

幸い、RDP認証のセキュリティ要件を見ると、94%がネットワークレベル認証（NLA）を必要としていることがわかりました。[28]Windows Server 2008で導入されたNLAは、実行中のトランスポート層セキュリティ（TLS）保護を強制するとともに、認証オプションを強化し、ブルートフォース攻撃や特定のサービス妨害攻撃に関連するリスクと影響を大幅に軽減します。Windows 2012以降、NLAはデフォルトで有効化されています。NLAサービスの欠如は、古いインフラがサーバー自体にあるか、または古いクライアントとの互換性のための要件となっているプロキシの指標となります。NLAを有効にしていない理由として他に考えられる唯一の理由は、有効期限が切れたパスワードでの認証を許可しないことです。これは、RDPゲートウェイサーバー、VPN、またはその他のインフラを導入して、パスワードを変更できる機能を提供し、リモートデスクトップサービスへのセキュリティアクセスを有効化するための理由にもなります。

Windowsリモートデスクトッププロトコル（RDP）

SMBプロトコルは、Windowsや互換性のあるネットワーク上でのファイル共有および印刷共有用、またプロセス間通信用のプロトコルです。**すべてのレポートで言っていることですが[29]、SMBは絶対にインターネットに公開してはいけません。**ファイル共有からのデータ漏洩、ブルートフォース攻撃による認証情報侵害、ホストオペレーティングシステムまたはサービスの脆弱性を通したマルウェア感染（前述のConficker やWannaCryを思い出してください）などのリスクがあります。ファイルを安全に共有するためのオプションは豊富にあります。SMB共有のリスクを冒す価値はありません。

[28] https://en.wikipedia.org/wiki/Network_Level_Authentication
[29] https://www.rapid7.com/research/report/nicer-2020/#smb-tcp-445

日経225を調査する場合、私達は139/tcpと445/tcpという2つの異なるSMBポートを確認しました。古いSMBバリエーションではポート139/tcpが使用されており、一般的に、非常に古いソフトウェアやレガシー要件がある兆候となります。調査では、6社の25台のサーバーがポート139/tcpで公開されていることがわかりました。これらのすべてが、Samba[30]というオープンソースのSMBサーバーを実行していました。観察された最も古いバージョンのSambaは3.0.36で、これは2009年後半にリリースされた、非常に重要な脆弱性が含まれるものです。

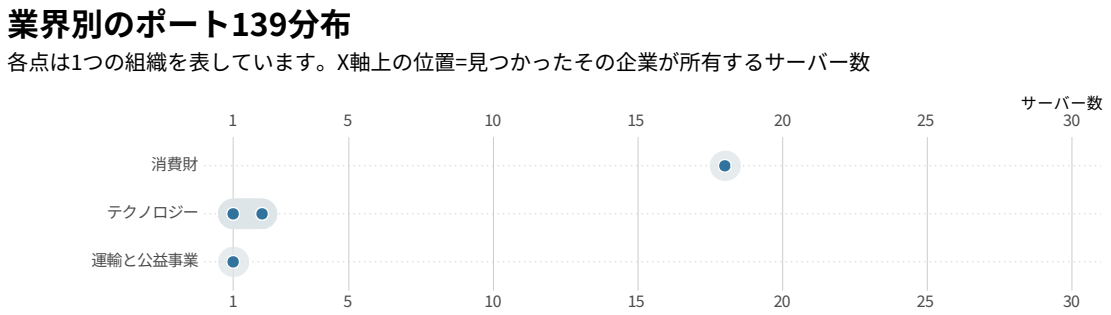

図14：業界別のポート139の分布

また、445/tcpポートのSMBも調査しました。Windows 2000で導入された、このSMBトランスポートでは、従来のプロトコルのオーバーヘッドの一部が取り除かれています。調査では、このポート上で17の組織の146台のサーバーが観察されました。

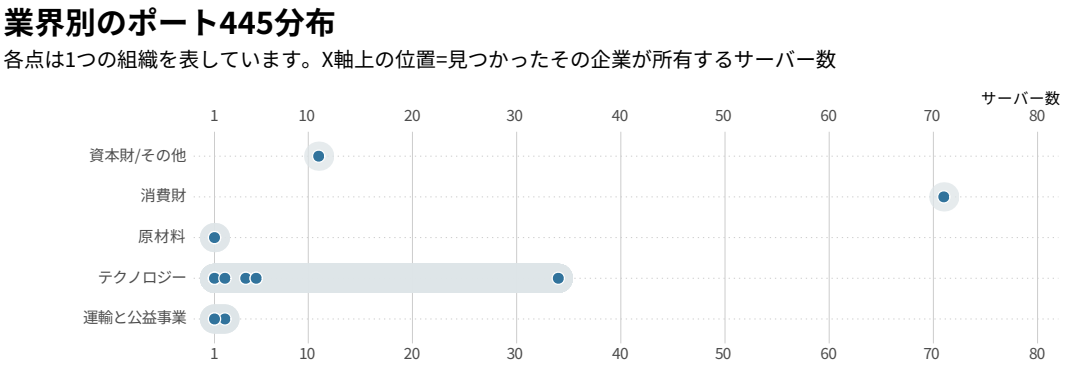

図15：業界別のポート3389の分布

[30] https://www.samba.org/

これらのSMBサーバーがインターネットに存在しているだけでも不安要素ですが、プロトコルの構成について深く掘り下げてみると、その懸念はますます大きくなりました。すべてのサーバーがSMBv1をサポートしていました。これは、いくつかの重要なセキュリティ制御が欠如していることを意味し、攻撃者はクライアントにより安全なバージョンのプロトコルからSMBv1へと、無理やりダウングレードさせることができます。観察した146台のサーバーはすべて、新しいバージョンのSMBをサポートしており、レガシーシステムによる依存関係もないため、SMBv1を有効にする必要性はありません。SMBv1を無効化するMicrosoftのガイダンスを強く推奨します。[31]

SMBv3は、Windows Server 2012でリリースされました。有線上のデータの暗号化やプロトコルのダウングレード保護など、多くのセキュリティやパフォーマンス上の改善が含まれています[32]。観察したサーバーの68%がSMBv3をサポートしていました。

これらのSMBサービスは、組織に関する情報も漏洩しています。すべてのサービスには、ホスト上で構成されているホスト名、DNS名、完全修飾ドメイン名（FQDN）が提供されています。これらの情報には、役割（VCENTER01）、または内部組織構造（db1.prod.us.corp.local）が示されている可能性があります。

Telnet

Telnetは、デバイスへのリモートコンソールアクセスを提供するために使用される、プレーンテキストベースのプロトコルです。ほぼ常に、認証情報やデータをクリアテキストで送信するため、コマンドやデータの中間者（MiTM）注入に対する保護はありません。

元々1969年に作られたTelnetは、「使用期間」をすでに過ぎており、SSHなどのより安全なテクノロジーに取って代わられています。調査の結果、62の企業で243台のホストが検出されました。これらのホストの大半は、テクノロジー業界のものでした。

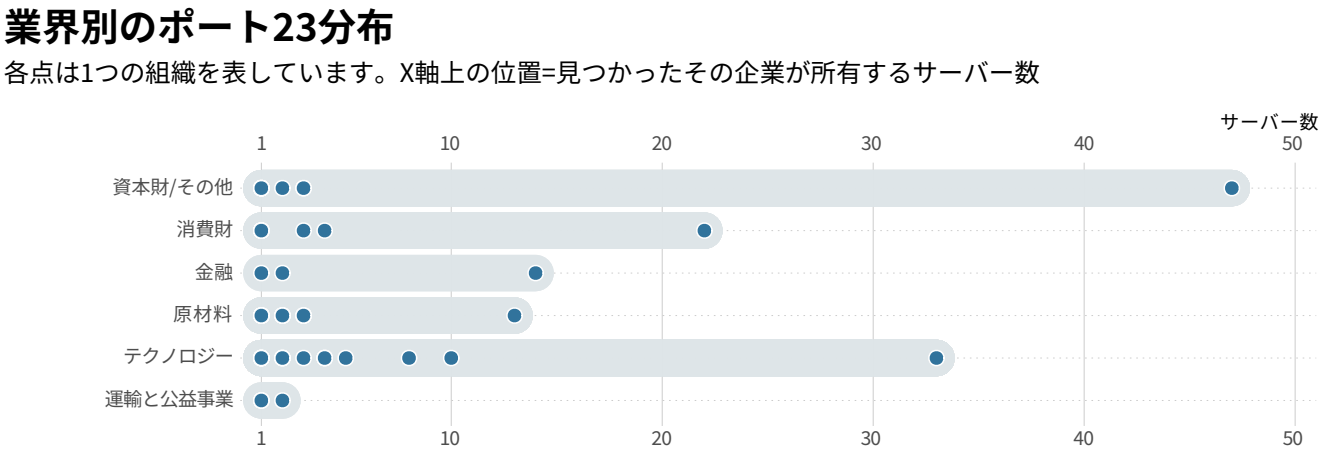

図16：業界別のポート23の分布

[31] https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858
[32] https://docs.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview

ほとんどの機器は、ルーターまたはスイッチであることがわかりました。一般的に、SSHのような安全なプロトコルではなく、Telnetを使用することは安全ではないと考えられています。

また、やむを得ずTelnetを使用する場合は、ファイアウォールのアクセス制御リスト（ACL）やその他の制御を使用して、デバイスにアクセスできるインターネットIPアドレスを制限する必要があります。今回の調査では、サービスを検証するために複数のIP（場合によっては異なる国）から接続する必要があったため、ACLが設定されていないか、または過剰に広範になっている可能性が高いと言えます。

エクスポージャーの概要

調査したプロトコルや業種を確認すると、特定のホットスポットがあることがわかります。

図17：業界のヒートマップ別の高リスクエクスポージャー

上記の図では、注目すべき点がいくつかあります。まず、SMB関連の行（135、445）は完全に空になるべきですが、そうではありません。

調査結果のほとんどは、消費財業界の1つの組織によるものですが、これらのサービスを公開されている組織が他にも16社あります。次に、多くの業界で、Telnetが頻繁に幅広く使用されていることがわかります。最後に、RDPエクスポージャーのほとんどは消費財業界のもので、これは1つの企業が大きく影響していることが原因です（明白な理由から名前は伏せています）。

CISOへの重要ポイント

調査結果では、リソースを豊富に持つ企業でも、リスクが大きいサービスを公開していることがわかりました。

上記のリスクに対処するための私達からのアドバイスは、いくつかの高度なセキュリティ対策やソフトウェアを実装するのではなく、基本に立ち返ることです。これらの基本については、CIS Top 20[33]コントロールの前半で説明しています。

- インターネットに面したホストのインベントリーを作成して維持してください。このインベントリーには、ソフトウェアのバージョン、役割、公開されることが予想されるサービス、そしてその理由も含めます。このインベントリは、公開されているすべてのIP範囲を外部から内側へスキャンすることで、必ず検証するようにしてください。

- セキュリティポリシーと、安全なプロトコルや構成設定を強化するためのサポートする構成基準を導入してください。Telnetを例にとると、現在Telnetを使用している機器はすべてSSHに対応しているはずです。もし対応していなければ、インターネットに直接接続するには古すぎたり、安全性に問題があると考えられます。

- ソフトウェアやハードウェアを最新の状態に保つようにしてください。多くの場合、Microsoft Windowsなどの新しいソフトウェアから、より良いセキュリティ機能やコントロールが得られます。これらの機能が欠如している古いソフトウェアでは、セキュリティ面で妥協を強いられるため、代償となるコントロールの実装が必要になり、複雑さが増すことになります。

[33] https://www.cisecurity.org/controls/cis-controls-list/

日経225における
脆弱性開示プログラム

世界中の主要な企業はすべて、テクノロジー企業です[34]。数十億ユーロの収入を生み出し、世界中で数万十人もの労働者を雇用する企業が、自社の製品、プロセス、物流に大きな技術的な投資をしていないとは考えられません。現代の生活の中で、私たちはあらゆる面において素晴らしい高度なテクノロジーに依存しています。もちろん、これらのテクノロジーを分析した経験がある人なら、特にインターネットベースのテクノロジーにおいて、私達は日常的に脆弱性に悩まされていることに気づくでしょう。

偶然にも、私たちには主要技術の脆弱性の流れを止めるための強力で実証済みの手段があります。 協調的な脆弱性の公開[35]（CVD）、そして現在ではCVDに参加するための標準的な手段となっている脆弱性開示プログラム[36]（VDP）です。

公開されたVDPの存在は、日経225のほとんどの企業で驚くほど欠如しており、その結果、これらの企業が自社の製品や技術インフラの脆弱性を建設的に知ることが難しくなっています。

現在、米国の Fortune 500ではVDPが普及していますが（約20%）、日経225銘柄企業のうち、発見可能なVDPを持っているのは16社（約7%）に過ぎませんでした。脆弱性開示プログラムを導入していないこれらの業界は、意図的であれそうでないのであれ、自分たちの脆弱性を株主や顧客に知られたくないと知らせているのです。
今回の調査では、日経225の企業やこれらの企業の主要ブランドに関連するVDPを、これらの企業の製品やサービスの脆弱性を開示しようとする場合と同じ方法で検索しました。2021年5月末の時点で、以下について次の順序で調査しました。

- Bugcrowd[37]のまたはHackerOne[38]のクラウドソースされている脆弱性報奨金制度、またはDisclose.io[39]プログラムデータベースに掲載されている、日経225の企業（またはこれらの企業の主要ブランド）と関連付けられたVDPの存在。
- 発見された脆弱性をWebサイトの管理者と共有できるようにするための、標準化されたsecurity.txtファイルが各企業または主要ブランドのウェブサイトに存在するかどうか。
- 「脆弱性」、「開示」、「セキュリティ」というキーワードを、企業名や主要ブランドと共にGoogleで検索することで、VDPが候補企業から提供されていることがわかる明らかなポインターまたは兆候があるかどうか。

しかしながら、調査した企業のうち、VDPを提供していないと思われる企業の中には、実際には脆弱性インテリジェンスを受けるプロセスを持っているものの、（企業で好まれる言語または英語のいずれかで）容易に発見できるVDPが欠如していることから、研究者と企業の両者に対するVDPの有効性が大幅に損なわれています。

[34] https://www.wsj.com/articles/every-company-is-now-a-tech-company-1543901207
[35] https://blog.rapid7.com/2018/10/31/prioritizing-the-fundamentals-of-coordinated-vulnerability-disclosure/
[36] https://blog.rapid7.com/2016/11/28/never-fear-vulnerability-disclosure-is-here/
[37] https://www.bugcrowd.com/bug-bounty-list/
[38] https://hackerone.com/directory/programs
[39] https://github.com/disclose/diodb/

個々のVDPの相対的なメリットを評価することは本ドキュメントの範囲外となりますが、すべてのVDPが同じように作られているわけではない点にも注意が必要です。強固な「安全域」を提供することで、脆弱性を報告・公開する際に、研究者や偶発的な発見者を保護するものもあれば、評価できる内容や結果の取り扱い・伝達方法について、研究者を制限する契約で縛ろうとするものもあります。このレポートでは、VDPが自由なものなのか、制限されているものなのかに関係なく、VDPが存在すること自体をプラスとみなしています。

結果：VDP採用の普及

2019年1月、Bugcrowdの創業者でオーストラリアの著名人であるCasey Ellisが、ブログ記事で、「Fortune 500の中で脆弱性開示プログラムを実行しているのは9%のみ[40]」と指摘しました。これは、2021年上半期の日本で観察されたものよりもわずかに高い数値です。

2021年5月に調査した日経銘柄企業225社では、合計で16の脆弱性開示プログラムが発見されました。これは日経225社の約7%を占めています。

非常に少ない数であり、この中でどの業種や評価統計数がVDPの広告を慣習化しているのかを特定することは難しい状況です。しかしながら、もっとも良い調査結果が見られたのはテクノロジー（13社）、次に消費財（3社）となっており、消費財企業であっても技術的な要素が強いことがわかります。

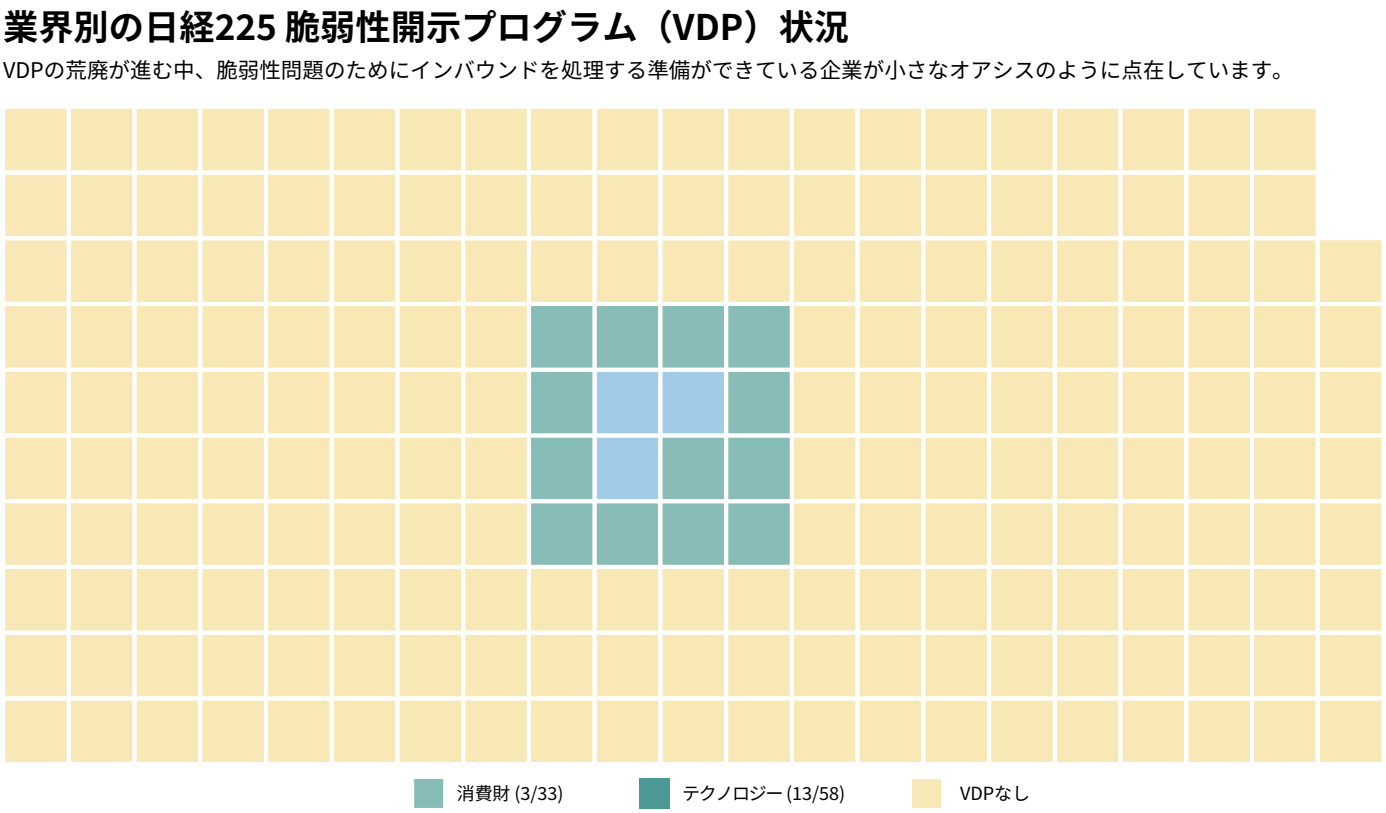

図18：業界別の日経脆弱性開示プログラム（VDP）の状況

[40] https://www.bugcrowd.com/blog/3-reasons-why-every-company-should-have-a-vdp/

VDPは、日本経済の主要分野には全く存在しないようです。具体的には、資本財/その他（主に重機と不動産）、金融、材料、運輸、公益事業の分野です。

日経225の調査から得られた重要なポイントは、すべての主要企業が何らかの技術的要素を持っている（したがって技術的な脆弱性を持っている）にもかかわらず、日本のこれらのトップ企業の90%以上が正式な脆弱性開示プログラムを持っていないということです。

しかしながら、日本は独特のケースです。2004年以降、日本政府は、日本企業が情報処理推進機構[41]（IPA）やJPCERT/CC[42]と連携することを奨励しています。IPAは、日本政府が直接設立した組織ですが、JPCERT/CCは主に公費で運営されている非政府組織です。この2つの組織は、国のITの利益を守ることを目的としており、IPAはウェブサイトに関する問題を扱い、JPCERT/CCがその他のソフトウェアやファームウェアに関する問題を担当することで、問題をトリアージ[43]しながら解決へと導きます。

しかしながら、こういった機関は、VDPに関しては、旧来のインフラとみなすべきです。1つや2つの政府から資金を調達された機関が扱うには、あまりにも多くのテクノロジーが存在しており、これらの機関はこれ以外にも、政府の資産自体も守る必要があります。日本経済の上層部でVDPが欠如していることから、製品やサービス、インフラで新たに発見された脆弱性を合理的かつ責任を持って開示することが難しくなっています。結局のところ、VDPはソフトウェアアプリケーションで見つかったソフトウェアのバグを報告するためのものだけではありません。保護されていないクラウドストレージに公開されている顧客や企業内部情報にある機密データの発見にも役立ちます。もちろん、正式なVDPなく業界の企業に対する脆弱性を公開することも可能ですが、VDPが欠如していることから、企業の非効率性や研究者への法的リスクが生じます。

また、VDPが機能しているということは、その企業が情報セキュリティプログラム全体に何らかの投資を行っていることを示しており、VDPがないということは、その逆を示していることになります。このリストに掲載されているすべての企業がWebサイトのプライバシーポリシーを持っています。このためこれらすべての企業に、脆弱性レポートを受信および処理するための正式な方法が必要です。

CISOへの重要ポイント

このレポートの著者らが、明確に定義され、容易に発見できる脆弱性開示プログラムを強く支持していることはおわかりいただけたと思います。日経225（そしてそれ以外）のすべての企業が採用すべきだと私たちは考えています。

VDPの導入と運用を成功させることは難しいかもしれません。結局のところ、VDPが存在するということは、その企業にはまだ存在していないセキュリティ成熟度があることを示しています。VDPを持たない組織のCISOは、脆弱性開示の基本を熟知しておくことが強く求められます。

[41] https://www.ipa.go.jp/
[42] https://www.jpcert.or.jp/
[43] 脆弱性処理に対する日本独自のアプローチについては、https://www.ipa.go.jp/files/000044731.pdfにある「情報セキュリティ早期警告パートナーシップ」をご覧ください。

VDPの構築と維持に関するCISOの専門知識は十分に蓄積されており、この分野の他の人々の経験から学ぶ機会は十分にあると考えています。私達の経験では、CISOはVDPで得られる経験を個人的に楽しんでおり、話し始めると止めるのが難しいこともあります。

ISO 29147[44]（情報テクノロジー、セキュリティテクニック、脆弱性開示）およびISO 30111[45]（情報テクノロジー、セキュリティテクニック、脆弱性処理プロセス）は、脆弱性開示プログラムを構築、維持、および改善するための優れた出発点となります。これらのISOは、国際的に認識された脆弱性開示の専門家の協力のもとに開発されており、CISOが向上するのに役立ちます。

また、最低限のVDPを確立するための最初のステップとして、<hxxps://your-company.com/.well-known/security.txt>にある連絡先およびポリシー文書もよい出発点となります。 これは、VDPの規格としては比較的新しいもので、人とマシンの両方が読み取れる、基本的な連絡先情報のシグナル化を提供します。[46]

[44] https://www.iso.org/standard/72311.html
[45] https://www.iso.org/standard/69725.html
[46] 興味のあるCISOの方はhttps://securitytxt.org/をご覧ください。

まとめ

世界中で発生したCOVID-19パンデミックにより、これらの企業の多くは短期間で大規模な在宅勤務への移行を余儀なくされました。各企業が、このような前例のない急激な職場の変化に直面しながら、企業の生き残りをかけた独自の奇跡を起こしています。また、日本企業は、Rapid7の調査対象となった地域と比較しても、危険なリスクのあるサービスやバージョンの分散を根絶することに成功しています。

しかしながら、これらの企業は、DMARC、HSTS、VDPの採用という3つの他の分野において、海外の企業に比べて遅れています。より多くの進歩を、より早く遂げる必要があります。これらの企業は日本のビジネス界で大きな地位を占めているため、世界中の優秀なサイバーセキュリティの専門家を利用できる傾向にあり、インターネット市民の模範として行動する義務があります。本レポートに協力したRapid7研究者は、これらの企業とこれらの企業とビジネス関係にある組織にとって、すべての人のためにセキュリティを向上させるという共通の責任において、この情報やアドバイスが役立つことを心から願っています。

CISOのまとめ

本レポートでは、ここで取り上げた最も一般的な問題に対するエクスポージャーを減らすために、日経255のCISOが今からできることに焦点を当てています。わかりやすいように、これらの推薦事項を以下にまとめました。

メールセキュリティ：あなたが日経225の13%と同様に、ドメインベースのメッセージ認証、レポート＆準拠（DMARC）に向かって取り組んでいるのであれば素晴らしいことです。今がp=なしからp=検疫ポリシーへと移行し、最終的にはp=拒否ポリシーへと移行する計画を立てる時です。これは簡単なことではありません。自社のメールインフラを運営しているITに隠された暗い部分を見つけることになりますから。しかしながら、主要ブランドのドメインからのメールを認証できるという自信は非常に素晴らしいものであり、取締役会にぜひ報告したい事項となること間違いありません。

Webセキュリティ：HTTP Strict Transport Security（HSTS）は、合理的な安全性を備えたWebサイトを運営するための手段として急激に普及しており、Google、Apple、Microsoft、Mozillaなどのブラウザメーカーが今後のChrome、Safari、Edge、Firefoxでも強化する可能性が高いセキュリティ機能です。CISOが比較的簡単に切り替えられる機能です（サイバーセキュリティの世界にある持っていると良いものと比べて）。 ですから、あなたの組織でHSTSを使用しているかどうか確認し、使用していない場合はその理由もぜひ調査してください。

バージョンの分散：資本主義の世界を闊歩する巨大企業にとって、合併買収は1年を通してかなり頻繁に行われる活動です。これは、日経225社のCISOは、本当の意味で「完了させていない」ことを意味します。 優れた資産と脆弱性管理ツールを導入ながらも、企業全体のバージョンの整合性を確保することができていません。新しいネットワークやネットワークサービスが加わることで、こういった新しい資産の近代化や正規化の取り組みが、かなり継続的に行われることになります。この継続的な取り組みを行うことは、予定されているか否かにかかわらず、次のパッチサイクルの計画をより簡単に、よりわかりやすくすることにつながります。

高リスクサービス：Telnet、SMB、RDPは広く世界に直接公開されるべきものではなく、次の自己繁殖するサイバー攻撃が繰り広げられるのを待っているだけの存在です。内部と外部のスキャンで得られた露出されたサービスの最新情報は、ビットコインに匹敵する価値があり、インターネットに曝されているネットワークサービスのエクスポージャーに対して、常識的なポリシーを強化するためにも役立ちます。しかしながら、前述の通り、2021年時点の日経225では、このような露出度の高いサービスはほとんど残っていません。

脆弱性開示プログラム：CISOとして、最高のソフトウェア、QA、プラットフォームエンジニアを雇っているかもしれません。しかしながら、世界中にいる何万人もの優秀なハッカーの知識を上手く活用する方法がなければ、自社の製品やサービスに潜む最も重要な脆弱性について学ぶことはできません。VDPは、あなたと同じように、より安全で安心なインターネットという目標を持った、善意の調査員たちで構成された巨大なコミュニティへの架け橋となります。このプログラムを今すぐ立ち上げることで、より安全なソフトウェアの製作を実践する時間を十分に確保できます。さらに、ISO 29147とISO 30111という形で、開拓な作業のほとんどはすでに実施されています。

付録：危機の時代における優先順位付け

SolarWindsに関連する複数の技術的な脆弱性（および関連するキャンペーン）の公開、活発な悪用キャンペーンに対応するためのMicrosoft Exchangeの帯域外パッチのリリース、そして間違いなく多くのソフトウェア開発のCI/CDプロセスに影響を与えるであろうCodecovの危殆化は、あらゆる業界のほぼすべての情報セキュリティチームに影響を与えました。私たちは、皆さんが今、より安全な場所にいられるようにお手伝いしたいと思っています。ここで、各セクションを今年私たちが対応しなければならなかった危機に照らし合わせながら説明したいと思います。

SolarWindsとCodecovの状況により、サードパーティのリスクがこれまでにないほどクローズアップされました。パートナーやベンダーの確固たるリストがあり、綿密な連絡計画も立てていたのであれば（多くの組織がそうでした）、このような大規模な事件もうまく切り抜けられているかもしれません。そうでない場合は、こういった事項を導入するための必要なサポートを得て、その後に発生する深刻な脆弱性開示や悪用キャンペーンでは使用できるようになっていることを願っています。

パートナーやベンダーが安全性や回復力をどの程度重視しているのかを知りたいのであれば、「CISOまとめ」セクションにあるアドバイスを参考にしてください。サードパーティ連絡先の大部分がメールの安全性を優先し、インターネットに危険なサービスを公開することを避け、パッチや高度な暗号化の基準を維持していることを知っていれば、夜眠るのもずっと楽になります。また、脆弱性開示プログラムが導入されているため、製品やサービスにセキュリティ上の問題が発見された場合でも、連絡方法も知っておくことができます。

また、大規模なExchangeの脆弱性とそれに関連した悪意のあるキャンペーンでは、何十万もの組織で使用されているコンポーネントに1つの弱点があるだけで、どんなに綿密に作成された企業の情報セキュリティロードマップであっても、その実行に支障をきたす可能性があることが示されました。社内外で展開されているものについて最新かつ正確なテレメトリを持ち、（「バージョンの複雑性」の項で述べたように）高度にアジャイルな品質保証と変更管理プロセスを行うことで、（Exchangeのような）予期せぬパッチが、（攻撃者に狙う時間を持たせないようにするための）ちょっとしたトリアージを行うだけの迅速な作業で済むか、それとも「総力戦」で臨む大規模な事件になるかの違いが生まれます。

この2つの大きな事件から抜け出して、2021年に私達を待ち受ける残りの課題に立ち向かうにあたり、私たちが提供する数値、コンテキスト、そしてアドバイスが役立つことを願っています。