重要インフラにおける信頼性低下への対応

世界のサイバー セキュリティ リスクの測定と透明性がポイント

SecurityScorecard

サイバー脅威からの防御は、
どの組織においても難しい
課題です。

**顧客、取引先、規制当局、そして
社会全体との信頼関係を構築し、
維持することは、一層難しい
課題です。**

企業、行政機関、報道機関でサイバーセキュリティへの関心が高まってから 10 年以上が経過しているにもかかわらず、サイバー レジリエンスは改善されるどころか悪化しています。サイバー攻撃の増加や情報漏洩の深刻化により、社会のレジリエンスに対する信頼は損なわれ、世界中のビジネスリーダーや法律家が信頼不足を解消するための解決策を模索しています。

デジタル化と自動化が急速に進む第 4 次産業革命[1]では、組織が顧客や関係者に価値を提供するうえで、データ処理、接続性、取引先への 依存度が一層高まっています。こうした取引先が重大なサイバーリスクを生み出しています。これまでに確認された侵害の 54% は、他の組織のサイバー セキュリティの対策不足が要因となっています[2]。

サイバー犯罪者は、このように拡大するアタックサーフェスを悪用し、詐欺、恐喝、嫌がらせ、スパイ行為などで、それぞれの目的を達成しています。サイバー犯罪者は狡猾で適応力があり、冷酷です。闇市場を作り上げ、そこから大金を手にしています。

サイバー インシデントに見舞われた組織は、 ビジネスの中断、修復コスト、風評被害、 規制や責任問題にさらされるなど、直接的・間接的なコストを被ることになります。顧客をはじめとするステークホルダーは、自らが利用している商品やサービスの流れが阻害されることでその影響を実感することになります。また、第 4 次産業革命によってデジタル世界と現実世界がシームレスにつながっていることから、物理的な危険が生じることにもなります。

54%

の侵害は、他の組織のサイバー セキュリティの対策不足が要因となっています。

1.“The Fourth Industrial Revolution: what it means, how to respond,” World Economic Forum, January 14, 2016.
2.Report:54% of organizations breached through third parties in the last 12 months, September 16, 2022.

たとえば、自動運転は、自動車の構成要素のうち最も危険な要素、つまり、ドライバーとしての人間を取り除くことで自動車の安全性を高めることが期待されています。しかしその反面、自動車が安全に走行するためにハッキング可能な部品に依存するようになってきているとも言えます。

そのリスクは、特に重要インフラの管理者や運営者にとって高いものとなっています。社会は、エネルギー、水道、通信、医療、金融など、さまざまな重要インフラ業界に依存しています。重要インフラ業界は相互にも依存しています。たとえば、エネルギー業界は事実上、全重要インフラ業界の基盤となっています。

2021 年に米国内外の重要インフラ業界に影響を与えた一連のランサムウェア攻撃は、脅威の持つ破壊力を広く社会に知らしめました。2022 年、ランサムウェアによる被害が続く一方で、ロシアによるウクライナ侵攻を受け、悪意のあるサイバー活動の標的として重要インフラが再び注目されるようになりました。ロシアは軍事施設と政府機関を攻撃目標とすることに加え、ウクライナのエネルギー業界や通信業界に対するサイバー攻撃と武力攻撃を開始しました。これらの攻撃は、被害者とそのステークホルダーそれぞれに損害をもたらしました。

信頼の構築と維持に不可欠な サイバー レジリエンス

世界のサイバー レジリエンスを向上させるには、複雑なリスク相互依存関係を考える必要があり、政策当局や企業経営者は、法律、政策、リスク管理戦略という側面から対処しようとしています。

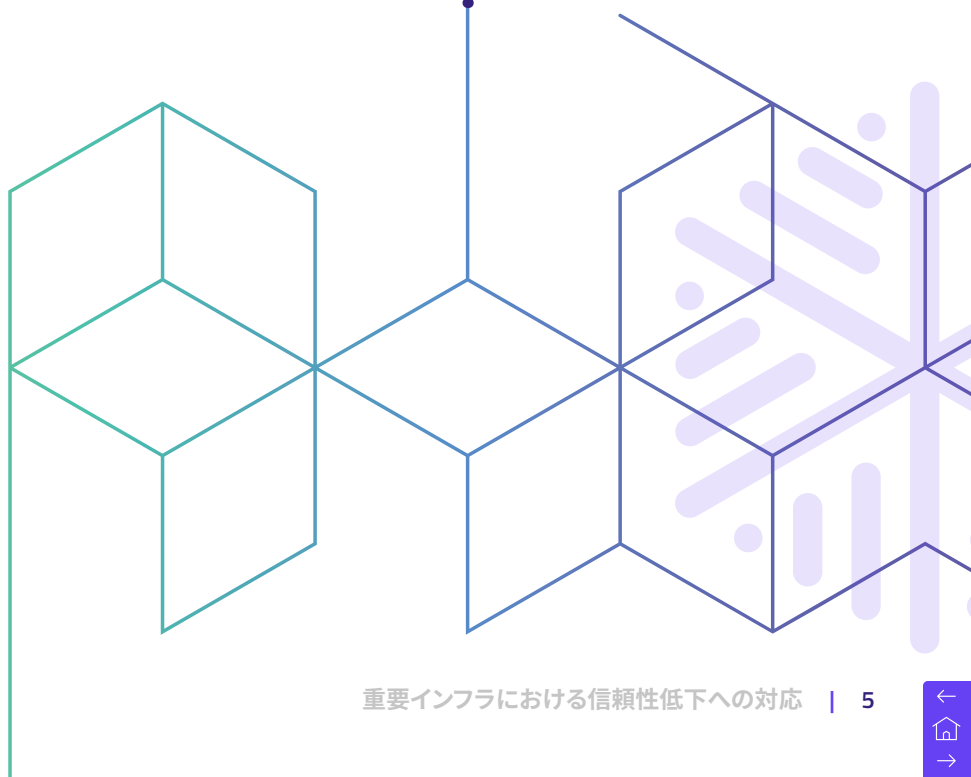
こうした取り組みの多くに欠けている重要な点は、リスクがもたらす結果の測定です。結局のところ、リーダーが最終的に重視するのは組織のレジリエンスであり、組織が規制などに準拠しているかどうかではありません。レジリエンスとは、組織が困難な状況を乗り越え、「自信を持って使命を追求し、自らの文化を広め、望ましい活動方法を維持する」能力を指します [3]。世界経済フォーラム (WEF) によると、自社がサイバー レジリエンスを備えていると自信を持っているのは、わずか 19% の経営者にすぎません [4]。

サイバー レジリエンスとそれが生み出す信頼性の測定は、政策当局と企業が同様にリスク管理施策の一環として常に実行すべきイノベーションであり、積極的な開発が進められています。

世界経済フォーラム (WEF) によると、

わずか 19%

の経営者しか、自社のサイバー レジリエンスに自信を持っていません[4]。



3 & 4. **"Global Cybersecurity Outlook 2022,"** World Economic Forum, January 2022 (以降、「Global Cybersecurity Outlook 2022」).

危機的状況にある重要インフラ

重要インフラを攻撃対象とするサイバー インシデントは、以前は比較的少なかったものの、近年大幅に増加してきています。これらのインシデントの多くはランサムウェアが関与しており、サイバー犯罪者（多くは犯罪グループ）は、恐喝によって金銭をゆすり取ることを主な目的としています。

医療、金融、政府機関への金銭を目的としたランサムウェア攻撃の急増はよく知られていますが[5]、犯罪者による攻撃の犠牲になっているのは、こうした業界だけではありません。たとえば、2021 年 5 月に発生した Colonial Pipeline に対するランサムウェア攻撃では、米国の大西洋沿岸におけるガスの供給が一時的に寸断されました。連邦捜査局のデータによると、米国政府が重要インフラとみなす 16 業界のうち、14 業界が 2021 年に 1 回以上のランサムウェア攻撃を受けています[6]。

ランサムウェアの被害は世界的な問題です。2021 年 11 月、オーストラリアのクイーンズランド州に本拠を置く CS Energy がランサムウェア攻撃の被害に遭ったことを公表しました[7]。2022 年 2 月、ドイツとベルギーの港湾都市ハンブルクとアントワープの石油施設に対する一連の攻撃は、エネルギー会社の業務を妨害し、ランサムウェアの結果であった可能性が高いとのことです[8]。2022 年 4 月、コスタリカ財務省が攻撃を受け、税務および輸出処理サービスが停止し、データの流出が発生しました[9]。さらに最近では、2022 年 11 月、デンマークの国鉄の下請け会社に対してランサムウェアによるものと思われる攻撃が行われ、鉄道サービスが中断しました[10]。また、バヌアツでは、行政システムに対して行われた攻撃により、政府が多くのサービスを提供できなくなる事態に陥りました[11]。

5.**"Internet Crime Report 2021,"** Federal Bureau of Investigation, 2022（以下「Internet Crime Report 2021」）.
6.**"Internet Crime Report 2021"** (2022).
7.**"CS Energy hit by ransomware attack,"** Energy Source & Distribution, November 30, 2021.
8.**"Belgium investigates cyberattack on energy companies,"** DW, February 2, 2022.
9.**"Cyber attack on Costa Rica grows as more agencies hit, president says,"** Reuters, May 16, 2022.
10.**"Danish train standstill on Saturday caused by cyber attack,"** Reuters, November 3, 2022.
11.**"3 Weeks After Hack, This Country's Government Is Still Off-line,"** New York Times, November 28, 2022.

重要インフラへの攻撃は、地政学的な目的を追求する国家やその代行者によるものが増加しています。たとえば、ロシアの国家的支援を受けたサイバー犯罪者は、高度なサイバー攻撃能力を駆使して、医療、エネルギー、通信、行政サービスなど、さまざまな米国や国際的な重要インフラ組織を標的にしています[12]。

より一般的には、Microsoft の報告によれば、重要インフラに対する国家的攻撃（主権国家から技術的、資金的、その他の支援を受けたもの）の割合が、2021 年 7 月から 2022 年 6 月の間に 20% から 40% へと倍増したとしています[13]。

その割合は、今なお増加し続けています[14]。最近注目すべきインシデントとしては、2022 年 8 月にはモンテネグロの水道インフラに対する攻撃[15]、2022 年 9 月にはイランによるアルバニア政府システムに対する攻撃でアルバニアの移民関連 IT システムがダウン[16]、リトアニアの国営エネルギー企業に対する連続的な DoS（サービス拒否）攻撃[17]などが発生しており、枚挙に暇がありません。モンテネグロとリトアニアでの攻撃は、ロシアの関与が疑われています。

12. **"Russia Cyber Threat Overview and Advisories,"** Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, 2022.
13. **"Microsoft Digital Defense Report 2022,"** Microsoft, 2022
14. **"Significant Cyber Incidents,"** Center for Strategic and International Studies, n.d
15. **"FBI's team to investigate massive cyberattack in Montenegro,"** Associated Press, August 31, 2022
16. **"Iranian State Actors Conduct Cyber Operations Against the Government of Albania,"** Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, September 23, 2022
17. **"Lithuania's state-owned energy group hit by 'biggest cyber attack in a decade,'"** LRT, July 11, 2022.

地政学的な要因で重要インフラの脆弱性が増大

重要インフラに対する国家的攻撃が増加した大きな要因は、ロシアがウクライナ侵攻に関連してサイバー攻撃を行ったことです。実際、SecurityScorecard の脅威調査チームは、2022 年 3 月に Zhadnost として追跡されているロシア関連のボットネットを発見したと発表し、ウクライナ政府とウクライナの主要銀行に対する一連の DDoS 攻撃がこのボットネットによるものだとしています [18]。その後、調査チームによって、フィンランド政府 [19] とウクライナ国営郵便サービス [20] を標的としたボットネットが確認されました。また、これらの攻撃後、SecurityScorecard では、Zhadnost ボットネットはロシアの主要諜報機関（GRU）によって操作されていると分析しています [21]。

18.**"SecurityScorecard discovers new botnet, 'Zhadnost,' responsible for Ukraine DDoS attacks,"** SecurityScorecard, March 10, 2022.
19.**"Zhadnost Botnet Attacks Again:This Time in Finland,"** Security Scorecard, April 13, 2022.
20.**"Zhadnost Targets Ukrainian National Postal Service,"** Security Scorecard, April 29, 2022.
21.**"Zhadnost and Killnet:Distant cousins or aligned strangers?,"** Security Scorecard, May 11, 2022.

ウクライナを標的とした攻撃では、実際にインフラに物理的な損傷を与えることができるワイパーを使用しているケースもありますが、ウクライナ以外を標的とした攻撃では、KillNet などの親ロシア派のハッカー集団による DDoS 攻撃にとどまっています。2022 年 11 月 23 日、KillNet に属する Anonymous Russia が、欧州議会のウェブサイトに対して DDoS 攻撃を行ったと犯行声明を出しました[22]。これは、欧州議会がロシアをテロ支援国家と宣言し、EU にロシアをさらに外交的に孤立させるよう求める決議を採択した後のことです[23]。KillNet はその数ヶ月前、米国の州政府[24]および空港のウェブサイト[25]に対して攻撃を行ったという犯行声明を出しています。また、これに似た犯罪グループである[26] Cyber Army of Russia Reborn は、別の州政府と米国の政党運営組織のウェブサイトに対して攻撃を行ったという犯行声明を出しました。SecurityScorecard の脅威評価では、こうしたグループは、DDoS 攻撃が作戦上与える影響は限定的かつ一時的なものだと理解していても、ウクライナに連帯を示す国々の政府機関や重要インフラの安全性に関する世論に影響を与えることはできると認識していることから、DDoS 攻撃を継続する可能性があると判断しています。

ロシアによるウクライナ侵攻から 1 年以上経った現在、この軍事侵攻が重要インフラへの脅威について示したことを振り返ってみる必要があります。ロシアは、2014 年の選挙システムに対する妨害工作、2015 年および 2016 年のウクライナのエネルギーインフラに対する破壊工作、2017 年の全世界で数百億円の被害をもたらした NotPetya による攻撃など、ウクライナに対して長年サイバー攻撃力を誇示してきました。ロシアは、2022 年 2 月の侵攻に至るまで、またそれ以降も、ウクライナに対するサイバー攻撃や、ウクライナに連帯を示す国々に対する攻撃など、執拗に攻撃を繰り返しています[27]。

22.**"Pro-Russian hacktivists take down EU Parliament site in DDoS attack,"** Bleeping Computer, November 23, 2022.
23.**"European Parliament declares Russia to be a state sponsor of terrorism,"** European Parliament News, November 23, 2022.
24.**"KillNet Targeting U.S. State Government Websites,"** Security Scorecard, October 27, 2022.
25.**"KillNet Operations Against U.S. Targets Persist with Attempted Airport Website Attacks,"** Security Scorecard, 2022.
26.**"Russian-Speaking Threat Actors Claim New DDoS Attacks Against U.S. Targets,"** Security Scorecard, November 17, 2022.
27.**"UKRAINE:Timeline of Cyberattacks on critical infrastructure and civilian objects,"** Cyber Peace Institute, June 8, 2022.

ウクライナは過去の攻撃から学び、以降のロシアによる攻撃に対して堅固な防御策を講じています。また、サイバー攻撃は与えられた任務を遂行するための一つの手段に過ぎず、特に武力による影響やその他の物理的影響をもたらそうとする作戦では、通常兵器が使用される場合があることも認識しておくことが重要です。このような場合、サイバー攻撃は、砲撃、ミサイル、爆弾と比較して、費用対効果が低く、望む効果を得られない可能性があります。同程度の標的に対して有用性を維持する従来の攻撃とは異なり、サイバー攻撃は、基盤となるツール、戦術、攻撃手順を防衛側に知られるリスクがあります。防衛側は得られた情報からネットワーク防衛策を修正して、その後の攻撃を阻止できる可能性があります。

ロシアは、依然としてサイバースペースの脅威となる危険な攻撃者です。ウクライナは、ロシアとの戦時体制下にあり、主権国家としての存亡を賭けて抗戦し、防衛のため総動員が行われています。

他の国は異なります。ウクライナに連帯を示す国々は、ロシアに対して、開戦状態にあるか平時の国交状態にあるかの立場を明確にしていません。ロシアは重要インフラに対する攻撃能力を備えていることが判明しており、これまでも攻撃を実行する意図を度々示しています。サイバー攻撃の能力も備えていることは、ほぼ確実です。さらに懸念されるのは、世界中の重要インフラに攻撃を仕掛けるには、必ずしも大規模で特殊なサイバー攻撃を展開する必要はないということです。この業界はサイバー攻撃に対して脆弱だからです。

重要インフラを狙うサイバー犯罪者は、ロシアだけではありません。ランサムウェア攻撃を行うことで金銭が得られるのであれば、サイバー犯罪者は脆弱な組織を狙って攻撃を続けるでしょう。イランなどの他の国も、地政学的な目的を追求するために重要インフラを攻撃する能力と意思の両方を示しています。

重要インフラへの注力を強化する政策当局

世界の政策当局は、こうした状況をただ看過しているわけではありません。各国政府は、投資（アメ）と規制（ムチ）を巧みに利用して、重要インフラ業界にサイバーリスクに対するレジリエンスの向上を奨励する取り組みを強化しています。政府にとって、国民の健康と安全を守ることが第一の責務です。市場原理だけでは、重要インフラの多くでサイバー脅威に対する十分なレジリエンスが得られないため、ある程度の政府の介入が望まれます。

米国の状況に関しては、ホワイトハウスのサイバー・新興技術担当副国家安全保障顧問であるアン・ノイバーガー氏が「私たちの関心は、重要なサービスの質の低下や提供の中断を最も懸念するところまできています」と説明しています [28]。注目すべき「アメ」は、国土安全保障省（DHS）が 9 月に発表した「State and Local Cybersecurity Grant Program（SLCGP）」と「Tribal Cybersecurity Grant Program（TCGP）」の実施です [29]。これまでに前例のないこの制度は、Bipartisan Infrastructure Law（超党派インフラ法）によって設置され、州・地方・部族政府がサイバー セキュリティ リスクに対処し、重要インフラを強化し、持続的脅威からシステムを保護できるよう、4 年間で 10 億ドルを交付する予定です [30]。議会は、資金の 80% を地方自治体の支援に回し、そのうち 25% 以上を地方に振り分けるべきだと明言しています。

28.**"Cyber officials prioritizing securing critical sectors, foreign partnerships amid rising threats,"** The Hill, October 27, 2022.
29.**"State and Local Cybersecurity Grants,"** Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, 2022.
30.**"President Biden's Bipartisan Infrastructure Law,"** The White House, 2022.

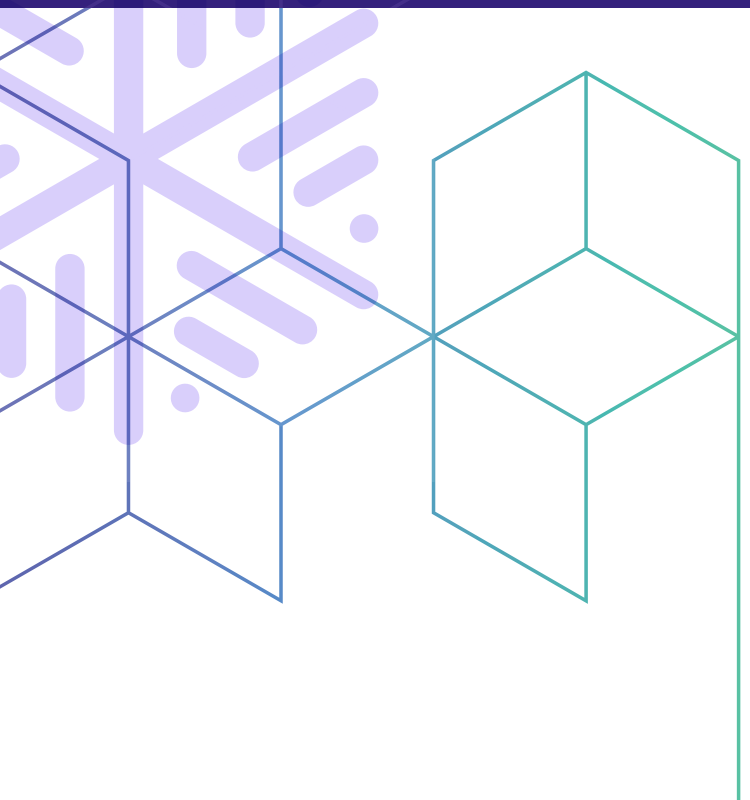
施策では、「ムチ」を打つことも忘れていません。議会は2022 年に「 Cyber Incident Reporting for Critical Infrastructure Act of 2022」を制定し、重要インフラ業界に対し、DHS のCybersecurity and Infrastructure Security Agency (CISA) に特定のサイバー インシデントを報告することを義務付けています [31]。また、CISA では規制を策定し、実施しています。連邦エネルギー規制委員会、証券取引委員会、財務省などの規制当局も、それぞれの管轄下にある事業体を対象に、さまざまな段階のルール作りを行っています。

世界に目を向けると、EU でも、「重要インフラの物理的耐性およびサイバー レジリエンスを強化するための最新かつ包括的な法的枠組み」を提供する 2 つの新しい指令を推進しています [32]。重要インフラのレジリエンスに関するCER 指令 [33] は、「重要インフラの事業体が破壊的なインシデントを防止、抑制、緩和、復旧できるようにする」ことを目的としています [34]。NIS2 指令は、「企業に課されるサイバーセキュリティ要件を強化し、サプライチェーンとサプライヤー関係のセキュリティに取り組み、サイバーセキュリティの義務不履行に対する経営陣の説明責任を導入しています」[35]。

SecurityScorecardは、特に米国におけるサイバーセキュリティの規制政策に関する政策論争に積極的に参加し、貢献を続けています。組織がサイバーリスクを測定し、それに対処する方法を変えることで、エコシステム全体のサイバーレジリエンス力を向上することが急務となっています。

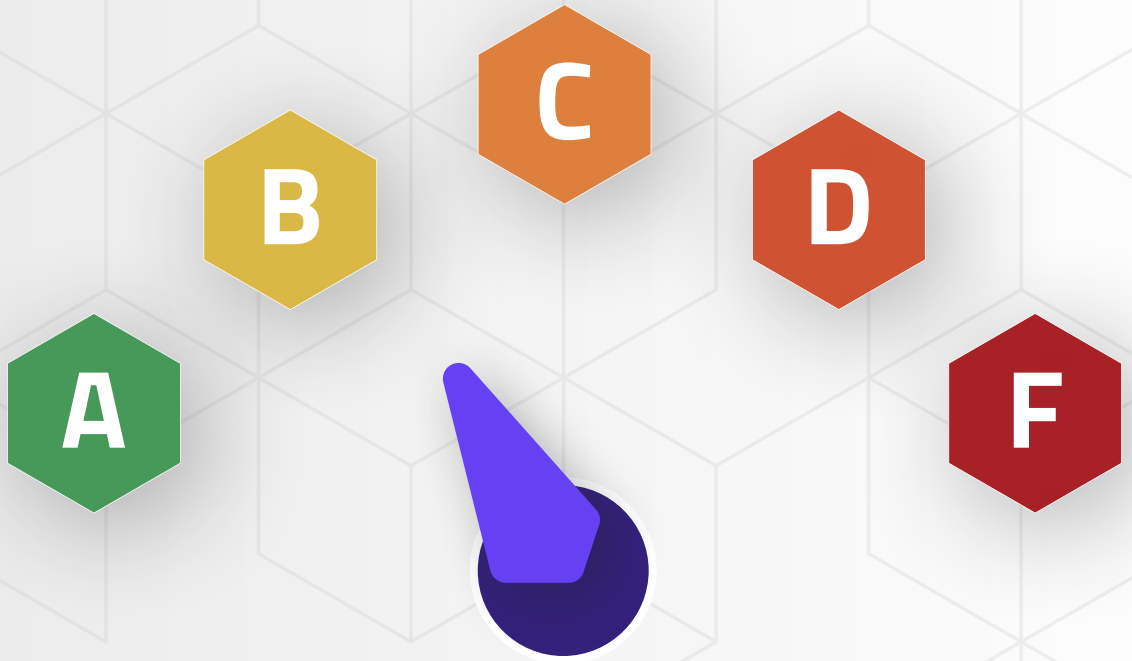
31.**"Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet,"** Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, 2022.
32.**"Critical Infrastructure:Commission accelerates work to build up European resilience,"** European Commission, October 18 2022.
33.**"Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities,"** European Commission, December 16, 2020.
34.**"The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU,"** European Commission, December 16, 2020.
35.**"Commission welcomes political agreement on new rules on cybersecurity of network and information systems,"** European Commission, May 13, 2022.

今こそ求められる
世界的に信頼性の高い
サイバーリスクの測定



重要インフラなどの組織が信頼を獲得し、レジリエンスを構築するには、パートナー、請負業者、サードパーティ/フォースパーティベンダー、サプライチェーンなど、世界中のあらゆる組織のリスクを測定し、信頼性を数値化するシンプルな方法が必要です。こうした数値を利用することで、すべてのサプライヤーが抱えるサイバーリスクを把握し、ビジネスパートナーが自社のサイバー防衛策を強化できるよう、情報に基づいた意思決定を行うことができるのです。

セキュリティ レーティングは、組織のサイバーセキュリティ態勢を客観的に監視し、サイバーセキュリティ態勢が時間の経過とともに改善しているか、それとも悪化しているかを測定する手段として、また、侵害対策を改善するための有効な手段として活用できます。セキュリティ レーティングを提供する企業は、公共および民間の外部情報源から収集または購入したデータを組み合わせて使用し、独自のアルゴリズムを適用して、組織のセキュリティの効果性を定量的なスコアで明示します。サイバー犯罪者のインテリジェンスが巧妙化するにつれ、組織が潜在的なパートナーやベンダーのサイバー健全性を評価する必要が増え、セキュリティ レーティングが急速に普及にし始めました。この情報をもとに、サイバー保険会社はリスク評価の精度を高め、官民間の信頼関係を築くうえで必要な仲介役を果たすことができます[36]。セキュリティ部門は、セキュリティ レーティングを用いて課題に優先順位を付け、必要な対応を実施することで、セキュリティ態勢を大幅に改善し、侵害が成功した場合のリスクを軽減できます。

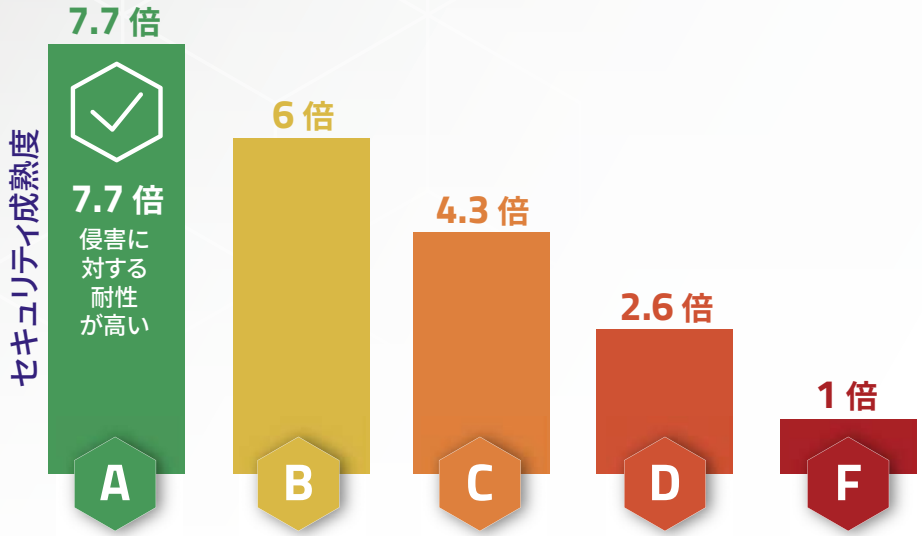


セキュリティ レーティングは、サイバー レジリエンスのバロメーターとして信頼を獲得しつつあります。

2022 年 4 月、SecurityScorecard は、脆弱性が高くリソースが不足しがちな重要インフラ業界のサイバー レジリエンスを強化することを目的として CISA が作成した「Free Cybersecurity Services and Tools」目録[37] に掲載されました。

36. **"How to use security ratings to build public and private trust,"** Securityinfowatch.com, April 2022m.
37. **https://www.cisa.gov/free-cybersecurity-services-and-tools**

セキュリティリスクの測定と管理で得られる安心感



87% のリスク低減
F から A へのスコア改善で最大 87% のリスク低減。

83% の時間短縮
ベンダーアンケート作成の時間短縮と省力化を実現。

198% の ROI（投資利益率）
3 ヶ月以内に投資回収。

SecurityScorecard は、さまざまな規模、業界、地域にわたる、1,200 万以上のグローバル組織を継続的に評価しています。このサイバーセキュリティデータを分析することで、どのような組織でも、組織自体のサイバー健全性と、取引先や子会社、同業者など、その組織にとって重要な関係先のサイバー健全性を速やかに把握し、継続的に監視できます。SecurityScorecard のレーティングは、侵害の可能性と相関しています。たとえば、機械学習（ML）を活用した最近の調査では、レーティングが A の組織は F の組織と比較して、侵害に対する耐性が 7.7 倍高いことを明らかにしました。

重要なインフラ設備を保有する企業にとって、テクノロジーへの投資は負担が大きいと思われるかもしれません。しかし現実的には、特に情報漏洩によって被る甚大な損害を考慮すれば、テクノロジーへの投資は、非常に費用対効果が高いものです。IBMの調査によると、米国において、情報漏洩の平均被害額は 944 万ドルにものぼります[38]。情報漏洩が発生した場合の損害額を考えれば、セキュリティ レーティングは十分に価値があるといえるでしょう。実際、Forrester Consulting は、SecurityScorecard の測定テクノロジーを利用する顧客が 3 ヶ月以内に投資回収を達成し、3 年間で 198% の ROI を実現していると報告しています [39]。

38."Cost of a data breach 2022," IBM, 2022.
39."The Total Economic Impact of SecurityScorecard," Forrester Consulting, May 2021.

懸念を抱える重要製造業

CISA が指定する重要インフラ業界におけるサイバー レジリエンスの現状把握のため、SecurityScorecard の調査部門は多数の業界を対象に詳細な調査を実施しました。

特に重要製造業が、サイバー レジリエンスを実現するうえでかなり力を入れていかなければならないことがわかりました。CISA が定義する重要製造業には、「第一次金属製造業」、「機械製造業」、「電気機器・家電・電気部品製造業」、「輸送機器製造業」が含まれます [40]。本書では、Forbes Global 2000 [41] リストに掲載されるすべての重要製造業者のグループを分析しました。

40."Critical Manufacturing Sector," Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, n.d.
41."The Global 2000," Forbes, May 12 2022

この業界の 48% の企業が、SecurityScorecard によるレーティングで F、D、または C のスコアだと判明しました。SecurityScorecard では、組織のセキュリティレーティングを作成する際に10種類のリスクファクターを考慮します [42]。重要製造業をさらに分析したところ、これらのファクターのうち「パッチ適用頻度」が 2021 年から 2022 年の 1 年間で大幅に低下し、88 点 (B) から 76 点 (C) に落下したことが確認されました。「パッチ適用頻度」は、企業が保有している古いアセットの量や、組織における同業他社と比較したパッチの修正率と適用率を示すものですが、この数値の低下は、脆弱性の量が増加したためだと考えられます。重要製造業では、重大度の高い脆弱性が前年比で 38% 増加しました。2022年だけで、重要製造業者の 76% が重大度が高・中の CVE を保有しています。このなかには、こうした CVE を保有しているがために、ランサムウェアグループの標的になりやすい製造業者もあります。

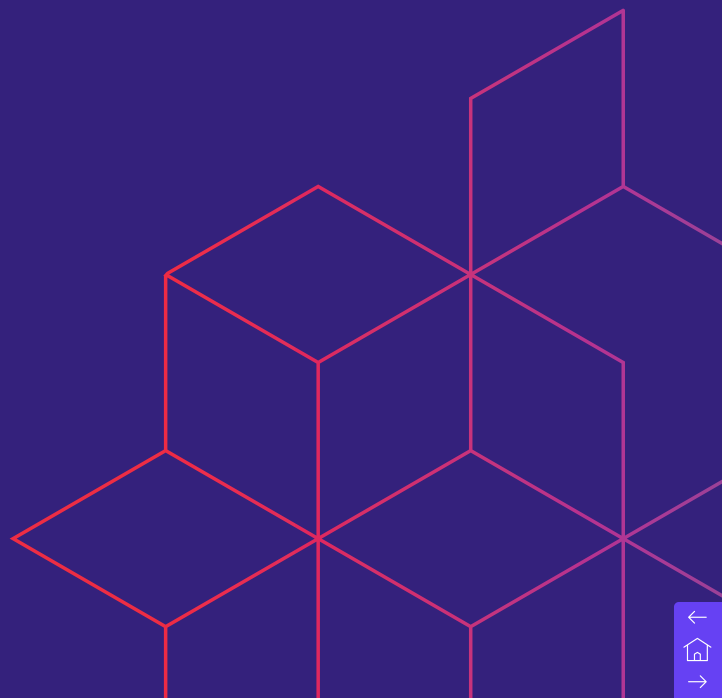
重要製造業に関してさらに懸念される点として、以下が挙げられます。SecurityScorecard の脅威インテリジェンスチームは、同業界では 2021 年から 2022 年にかけてマルウェア感染が増加したことを明らかにしました。2022 年、重要製造業者の 37% がマルウェアに感染しました。

ランサムウェアグループは製造業者を最も頻繁に標的としており、製造業の中でも金属部品メーカーを最大の攻撃対象としています [43]。Conti グループと LockBit グループが、製造業者への侵害件数が最多のランサムウェアです [44]。

Contiランサムウェアグループは、Delta Electronicsに対する攻撃を行ったと表明しています。Delta Electronics は、Apple や Tesla などに電源部品を供給している電子機器メーカーです [45]。この攻撃により、Delta 社のサーバー 1,500 台以上と個別のワークステーション 12,000 台が暗号化され、公式サイトがオフラインの間に新しい Web サーバーを使った新しい Web サイトを立ち上げざるを得なかったといわれています（おそらく、もとの Web サーバーが、攻撃で暗号化された12,000台のうちの一つだったためと思われます）。

また、Conti は、風力発電機メーカー Nordex SE に対する攻撃についても犯行声明を出しており、このことから、地政学の影響が特定の製造業に及ぶ可能性が示されました。Conti は、ロシアによるウクライナ侵攻への支持を公言し、（Nordexのような）再生可能エネルギーを支持する欧州のメーカーも標的にすることを表明しています。

ロシアのウクライナ侵攻に対する欧州の対応により、欧州の日常生活においてロシアから輸入された石油・ガスの占める割合の高さが改めて注目されており、欧州の輸入依存度を下げようとする試みは、再生可能エネルギーの需要を喚起する可能性があります。その後、SecurityScorecard の脅威インテリジェンス部門が調査した結果、Nordex は攻撃に関連する継続的なリスクにさらされている可能性があることが判明しました。



42. https://securityscorecard.com/product/security-ratings
43."2021 ICS Cybersecurity Year in Review," Dragos, February, 2022.
44."GRF Ransomware Report Mid-Year Update," Global Resilience Federation, September, 2022.
45."Conti ransomware hits Apple, Tesla supplier," The Record, January 27, 2022.

信頼性を築くためには 測定と透明性が不可欠

数十年にわたり、IT リスク管理における一般的な測定方法は、パフォーマンス要件に対して「緑」は「要件を満たしている」、「黄」は「部分的に満たしている」、「赤」は「満たしていない」という、色分けされた信号機方式でした。これはビジネスエコシステムには適用されず、現在では、ほとんど検証されることのない質問票に大きく依存しています。

現代の脅威環境においては、これでは十分とはいえません。政策当局や企業経営者は、規制対象企業、自組織、（サプライヤーなどの）サードパーティなど、自組織に影響を及ぼす他組織のセキュリティ体制について、一層忠実な対応を求める必要があります。データと測定方法は、リーダーがリスクエクスポージャーを理解し、それを削減するオプションやトレードオフを理解するうえで役立ちます。

また、組織は、自組織のセキュリティレベルについて透明性を高める方策を講じる必要があります。透明性を重視する文化を醸成することで、ビジネスエコシステム全体のセキュリティ対策を強化し、ネットワーク内の全員が恩恵を受けられるようにできます。透明性の高いビジネス環境は、顧客との強い関係を築くことにもつながります。それは顧客が、組織の講じているデータ保護施策をすべて把握でき、業務上の目標だけでなく、セキュリティやリスク許容度を考慮した経営判断を行えるようになるためです。

「信頼は、現存するエコシステムのパートナーシップやシステム間の関係の根幹となっています。

組織は、自らのネットワークや防壁の中では自信や安全性を感じていても、サードパーティベンダーのサイバーセキュリティインシデントによって悪影響を受けると、エコシステムのレジリエンスを信用できなくなる場合があります」[46]。

46.“Global Cybersecurity Outlook 2022,” World Economic Forum, 2022.

詳細や無料アカウントの作成については、SecurityScorecard.com/jp をご覧ください。

SecurityScorecardについて

SecurityScorecard 株式会社は、アメリカのニューヨーク州に本社を置く、2013年に設立されたサイバー リスク レーティングの世界的リーディングカンパニーです。セキュリティとリスクの専門家、アレクサンドル・ヤンポルスキー（AleksandrYampolskiy）博士とサム・カシューメ（SamKassoumeh）が 2013 年に設立した SecurityScorecard の特許取得済みの評価テクノロジーは、企業のリスク管理、サードパーティリスク管理、経営者向けレポート、デューデリジェンス、サイバー保険の査定のため、30,000 以上の組織で活用されています。1,200万以上の組織を継続的に評価している特許取得済みのレーティング技術は3,000以上の組織で、自社のリスクマネジメント、サプライチェーン リスクマネジメント、経営陣向けのレポート、サイバーデューデリジェンス、またサイバー保険の料率算定などに活用されています。自社グループ・取引先のセキュリティリスクを定量的に可視化し、サイバー攻撃による侵害発生の可能性を低減するための具体的なアクションを促すことにより、世界をより安全な場所にすることを目標にしています。すべての組織は、信頼性と透明性の高いInstant SecurityScorecard のセキュリティレーティングを受ける普遍的な権利を有しています。詳細については、securityscorecard.com/jp をご覧ください。

SecurityScorecard

SecurityScorecard.com/jp
sales-jp@securityscorecard.io