KDDI China

境界型セキュリティはもう限界？
グローバルに展開する企業が目指すべき

「ゼロトラスト」導入のステップ

INTRODUCTION

狙われる日本企業の海外拠点

凶悪なサイバー攻撃が依然として猛威を振るっています。脅威から身を守るべく、多くの企業が防御を固めていますが、そこには盲点がいくつか存在しています。その1つが海外拠点です。帝国データバンクの調査※1によると2023年現在、28.1％の日本企業が海外に進出しています。拠点が国外へ拡大した分、カバーすべきセキュリティ範囲も広がることを忘れてはいけません。

「本社ほど重要な情報を持っていないから大丈夫」と軽視するのは危険です。悪意を持った攻撃者は最も守りの薄いところから侵入し、社内ネットワークを通じて重要拠点に致命的な攻撃を仕掛けてきます。ひとたびセキュリティインシデントが発生すると企業全体の問題として認識され、機会損失、株価低下、顧客からの信用失墜など、大きなダメージを受ける恐れがあります。国内本社だけでなく海外拠点を考慮したセキュリティ対策をきちんと検討しておくことが重要です。

CONTENTS

S＆J株式会社
代表取締役社長
三輪 信雄氏

1. 注目を集める「ゼロトラストセキュリティ」とは

新たなセキュリティ上の脅威が次々と登場する中で、大きな注目を集めているのが「ゼロトラストセキュリティ」という考え方です。そのきっかけは、企業ネットワークでクラウドの利用が進んだことと、コロナ禍でテレワークが増えたことでした。

従来の「境界防御型セキュリティ」モデルでは「内部は安全、外部は危険」という大原則のもと、社内と社外の間に様々な防御策を講じ攻撃者が外から社内に侵入しないように全力でストップしていました（図1）。

ただ、外部のクラウドを利用したり、自宅など社外から社内ネットワークに接続したりするのが当たり前になってくると、境界の部分で完全に防ぐのは難しくなります。ひとたび侵入を許してしまうと、内部で防御対策をしていない境界防御型では社内のリソースへ自由にアクセスされてしまう危険性がありました。

すべてのアクセスを疑い精査した上で許可

一方、文字通り「何も信用しない」ゼロトラストでは、すべてのアクセスに対して常に“攻撃者からかもしれない”と疑います。社内・社外からにかかわらず、アクセスしてきた従業員のIDやパソコンのMACアドレスなどの情報を基に、利用を許すか（認証）、社内システムのどこまでアクセスを許可するか(認可)といったアクセスの可否を、その都度精査して判断します。正規の従業員の正しい利用であっても常に最小限の権限しか許可しません。

従業員や端末のセキュリティに関する情報は常に収集して更新しています。例えば、正規の従業員や端末であっても、業務と直接関係のないデータベースへ深夜にアクセスを試みるといった疑わしい行動を検出すれば、一時的に社内で利用できる範囲を狭めるといったコントロールも可能です。

万が一従業員のパソコンがマルウェアに感染したとしても、社内ネットワークを自由に動き回ることはできません。いつもとは異なる振る舞いをする従業員や端末については、感染を疑って動的に利用を制御するため、マルウェアの拡散リスクを抑制できます。

何よりも、ゼロトラストセキュリティであれば、国内拠点と海外拠点を区別なく同じセキュリティポリシーで管理できます。そのため、従業員が社内にいないなど、正確な状況が把握しづらい環境のセキュリティを管理するのに適しているのです。

ただし、ゼロトラストセキュリティはメリットだけではありません。実際に使いこなすには、境界防御型よりも複雑で難しい運用が必要となることは留意しておく必要があります。

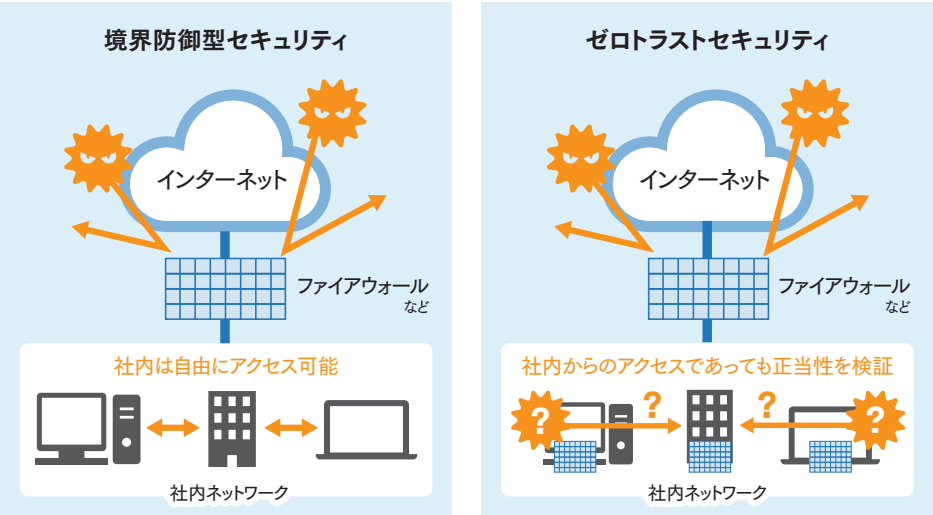


図1:社内と社外の境界で守る境界防御型と違い、ゼロトラストセキュリティでは社内・社外を問わずすべてのアクセスを信頼せずに正当性を検証した上で利用を許可する

2. 日本企業のゼロトラスト導入はまだこれから

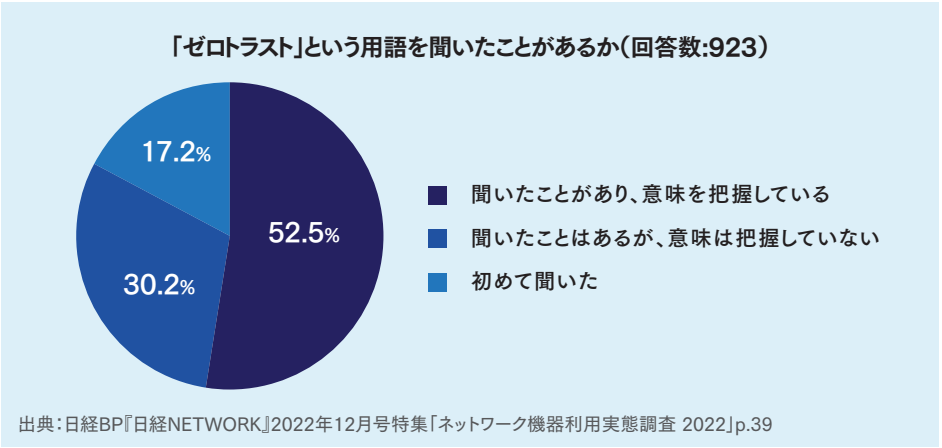
境界防御型の限界に対処できるセキュリティモデルとして、今や日本企業の多くがゼロトラストセキュリティへ高い関心を寄せています。『日経NETWORK』2022年12月号掲載の「ネットワーク機器利用実態調査2022」によると、回答者の8割超が「ゼロトラスト」という用語を聞いたことがあるとしています※2。さらに全体の半数超が「聞いたことがあり、意味を把握している」と回答しています※3（図2）。

その一方で、実際の導入となるとまだまだこれからのようです。同じ日経NETWORKの調査によると、ゼロトラストに関連するツールやサービスを導入しているとした回答者は約19%で、「全面的に切り替えた」のは4.3%に過ぎませんでした※4。

導入を検討する企業が続々

実際、日本企業のゼロトラストセキュリティの導入は、世界的に見ても遅れをとっています。トレンドマイクロ株式会社が2023年5月に公開した「サイバーリスク国際意識調査『Cyber Risk Index』」（2022 年下半期版）によれば、「積極的なゼロトラスト推進プロジェクトを発足」した企業の割合は世界平均を下回っており、調査した28カ国中で27位という順位になりました※5。

とは言え、まったく導入する気がないかと言えばそうではないようです。一般社団法人日本情報システム・ユーザー協会が発表した「企業IT動向調査報告書2023」では、新規テクノロジーとして挙げたAI（人工知能）やパブリッククラウド、AR(拡張現実)・VR(仮想現実)など31項目中、導入を検討しているテクノロジーとして「ゼロトラスト」が35.0%で1位となっていました※6。



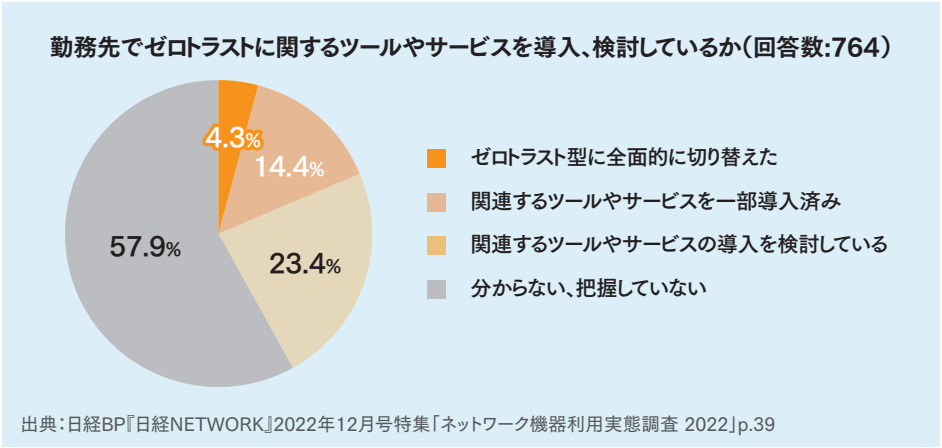


図2:日本企業におけるゼロトラストセキュリティの認知度と導入状況

Interview

3. 有識者に聞く “勘違い”されているゼロトラストセキュリティ

ゼロトラストに関心があっても導入まではなかなか踏み出せていない日本企業の現状は、情報セキュリティ有識者の目にはどのように映っているのでしょうか。日本の情報セキュリティビジネスをリードしてきた三輪 信雄・S&J株式会社 代表取締役社長は、最近のゼロトラストセキュリティの捉え方について警鐘を鳴らします。

三輪 信雄氏 S&J株式会社 代表取締役社長

セキュリティソリューションサービスを提供する株式会社LACの創業など、常に情報セキュリティ業界をリードする。2009年から総務省CIO補佐官を務めるなど、政府系委員も数多くこなす。現在は自分で創設した独立系セキュリティ会社「S&J」の代表取締役社長を務める。

――現在の日本では“ゼロトラストセキュリティ”という言葉が独り歩きしているように思います。ゼロトラストセキュリティという考え方さえ採り入れればセキュリティは万全になる、メリットが得られる、と特効薬のように考えている企業が多いようですが、それは大きな勘違いで夢物語です。

境界型より労力がかかることを覚悟すべき

――ゼロトラストとは『何も信用しない』ということです。そのため、これまでより厳格なアクセス制御を施したり、企業のネットワークの内部をなるべく細かく分割してセキュリティ上の制限を設けるマイクロセグメンテーションを実施したり、24時間・週7日体制でログ監視をしたりと、やるべきことが山ほど出てきます。本気で実現しようとするなら、ゼロトラストセキュリティは非常に労力がかかるものです。何か1つツールを入れたらそれで終わり、という簡単なものではないのです。

コロナ禍以前からサイバー攻撃は巧妙化の一途をたどっています。守るべき情報資産をきちんと把握し、対象に応じた対策を講じるというのが本来のセキュリティの在り方です。ゼロトラストセキュリティが出てきて、セキュリティ対策をもっと強化しなければならなかったということに日本企業がようやく気付き始めたというのが実情です。

海外拠点ならではの特徴を理解しよう

盲点になりがちな海外拠点のセキュリティ強化を考える場合、まず考えるべきは海外拠点ならではの組織の特徴だと三輪氏は言います。働いているのがほとんど日本人であるため統制しやすい国内拠点と違い、海外拠点で働く現地の従業員はバックグラウンドが様々で、日本人とは考え方が根本的に異なる

Interview

有識者に聞く “勘違い”されているゼロトラストセキュリティ

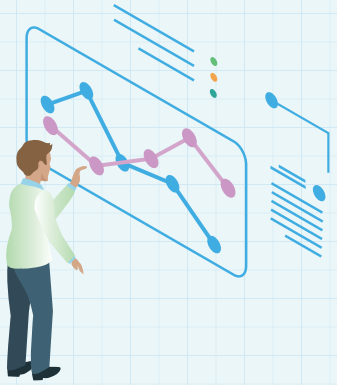
ケースが多いからです。評価や給与に反映されるというのでもない限り、なかなかガバナンスが効きにくいというのが実情です。

――信じられないかもしれませんが、ある朝出社したら工場のパソコンが全部盗まれてなくなっていたということも珍しくありません。そのため、『この人は大丈夫』という例外をつくるべきではなく、『Aさんの仕事に必要な情報はこれだけだからこれだけの権限を与えよう』とシステムできめ細かく制限していく必要があります。ガイドラインで周知徹底という方法はなかなか通用しません。

また、海外拠点に出入りしている保守事業者などにも注意する必要があると言います。

――実際に、保守事業者からネットワークに侵入された脅威案件がありました。その事業者がどうしていたかというと、全社のリソース情報をWindows の Active Directory (AD)※のドメインコントローラーでまとめて管理していたのですが、その保守をWindowsのリモートデスクトップ機能でID/パスワード認証だけで遠隔地からリモートでログインして作業していたのです。そのID/パスワードが破られました。

このようにID/パスワード情報は一度外部へ漏えいすると悪用される危険性があります。重要な情報を扱う場合は、本来であれば追加で別の認証情報も要求する多要素認証にすべきです。また保守事業者を採用する際にも気をつけるべきです。現地で調達することは仕方ありませんが、このような事件を回避するなら、日本からグローバル展開している保守事業者を探すか、あるいは日本水準のセキュリティサービスを提供できる現地保守事業者をしっかり選定するといった対策は不可欠です。



※Windowsのサーバーが標準で搭載している機能で、ユーザーやコンピュータ、パソコン、プリンタ、アプリケーションなど企業内のIT資産情報を一元管理するディレクトリサービスを実現する

4. 海外拠点のセキュリティで注意すべきポイントは

海外拠点においてセキュリティを強化するにはどうしたらいいのでしょう。単にID管理一式、EDR（Endpoint Detection and Response）ツール一式といった形でおしなべて等しくソリューションを採用するのではなく、海外拠点ごとに守るべき情報資産は何なのか、それに対する最適なセキュリティ対策は何なのか、をきちんと正確に見極めることが重要です。

セキュリティ面で考えた場合、工場がある拠点かどうかで大きく2種類に分類できます。

工場を持たない事務系のオフィスでは、電子メールを使った業務が主となり、監視対象も送られてくるフィッシングメールや添付ファイルが中心になります。EUや北米など、個人情報の意識の高い国や地域の拠点は、従業員情報や顧客情報などが漏れると訴訟に発展する可能性があるため、個人情報を管理するシステムを導入するなどの対策を考える必要があるでしょう。

工場のある拠点の場合は、さらに重要な情報を扱っています。例えば、CAD図面など機密情報を扱っていたり、IoT（モノのインターネット）を進めてセンサー情報が飛び交っていたりします。それらを流出しないようにするための機密情報管理システムや通信路の暗号化といった厳格な管理が求められます。

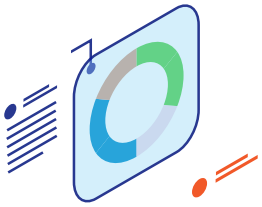
重要な情報がある大事なところを重点的に守る

セキュリティ対策を考えるときには、どこがよりリスクが高いのかという観点で優先順位を付けた上で、メリハリを付けながらよりセキュリティリスクが高い拠点に絞り込んでしっかり対策を施すことが肝要です。

対策を検討する上でも、注意するべき点が2つあります。1つは「何をリスクと考えるか社内でしっかり合意形成を図る」こと、もう1つは「ヒアリングに頼りすぎると真実に迫れない」ことです。

前者の例を挙げましょう。製造業の場合、現場の従業員はCAD図面が盗まれることがリスクと考える人が多いでしょう。しかし、もしかしたら経営陣の考えは違うかもしれません。「図面はいくらでも設計し直せるが、A社への卸値がB社に知られたら倒産する」と考えているとしたら、真に守るべき重要な情報は図面データベースではなく、販売担当者のパソコンに入っている卸値を記録したExcelファイルということになります。何を守るかによって対策も変わってくるため、何が自社にとって最大の情報資産なのかを社内であらかじめ合意を得ておくことは非常に重要です。

後者はある対象者のみに実施するヒアリングに頼らずツールなどの使用により正しい実態を把握することが大事という話です。守るべき情報資産や潜在リスクを把握するために、従業員にヒアリングを実施するのは定番の手段です。しかし、「会社で許可していないツールを入れていませんか」と尋ねても、素直に「実は入れています」と本当のことを答える従業員はまれです。ヒアリングで得た回答を鵜呑みにせず、調査対象者以外の従業員への取材やIT資産ツールの使用と組み合わせることで正しい実態を把握することが大切です。



5. 企業がゼロトラストセキュリティを実現するには

これらのツールを組み合わせて導入すれば完了、といったゼロトラストセキュリティを実現する簡単な方程式はありません。まず守るべき資産が何なのかを把握することが最重要です。しかし、『一刻も早くゼロトラストを実現させたい』と考える企業もあるでしょう。そうした企業に、三輪氏は次のようにアドバイスします。

「大企業に比べると情報システムの規模が小さい中堅・中小の企業なら、海外拠点も含めてフルクラウド環境にするのが1つの方法として考えられます。そうすれば、本社ですべてコントロールできます。例えば東京にあるパソコンとインドネシアにあるパソコンも同じように管理できるのです」。

海外拠点だけでセキュリティを確保する必要がある場合でも、ゼロトラストを導入するならフルクラウド環境に移行することは有力な選択肢です。人員などのリソースが限られる海外拠点で、ファイアウォールやサーバーのお守りやセキュリティを社内で続けるのは負担が大きいからです。

『フルクラウドは無理だし、リスクを洗い出している時間もない』という企業の場合、三輪氏はまず社外から狙われやすいVPN（Virtual Private Network）装置に最新のパッチを適用してセキュリティホールを防ぎつつ、次にEDRツールを導入し従業員に対してメール訓練を行うべきだとアドバイスします。ツールの導入だけでは十分とは言えないため、脅威の監視を強化するようにも求めています。理想を言えば社内の情報を集中管理するディレクトリサービスやパソコンを24時間・週7日体制でモニタリングすべきで、社内にリソースがなくても予算を確保しアウトソーシングでの監視に力を入れたいところです。

確実に防ぐには人ではなくシステムでの対策が重要

セキュリティ対策というと、日本では注意喚起や周知といった「人的対策」を取ることが多いかもしれません。ですが、確実にセキュリティを確保するには欧米で当たり前のシステムで防ぐ「技術的対策」を取ることが望ましいと三輪氏は指摘します。

NRIセキュアテクノロジーズ株式会社が2022年7～9月に実施した調査※7では、サイバー注意喚起を契機に実施した措置として「従業員への注意喚起や周知」を挙げた企業が、米国や豪州が3割前後だったのに対し日本は約7割と2倍以上に達しています（表1）。逆に、「クラウドサービスの設定見直し」や「多要素認証の有効化」といったシステムでの対策を実施した日本企業は、米国や豪州の半分以下となっています。

三輪氏は「海外はシステム側でガバナンスを効かせるのが当たり前。やらないときのペナルティが何もない単なるお願いで人的対策を実施しようとしても、なかなか言うことを聞かないのが現実」と語ります。

表1:2022年2月以降に発生したサイバー注意喚起を契機に実施したリスク低減のための措置

	日本（回答数1772）	米国（回答数540）	豪州（回答数528）
従業員への注意喚起や周知	67.10%	35.20%	29.70%
脆弱性の把握とパッチの適用	30.30%	33.00%	34.50%
アカウントの棚卸しやパスワードの見直し	28.60%	30.60%	29.70%
情報資産の保有状況と機器構成の把握	18.00%	39.80%	44.90%
多要素認証の有効化	15.20%	41.90%	45.80%
クラウドサービスの設定見直し	9.40%	25.40%	19.50%

出典：NRIセキュアテクノロジーズ株式会社「NRI Secure Insight 2022 企業における情報セキュリティ実態調査」

6. 海外拠点自らが最初の一歩を踏み出すなら

読者の皆さんの中には、海外拠点へ赴任したものの情報システム関係は現地従業員が担当しており、運用状況が詳しく分かっていないという人もいるかもしれません。そのような状況下で、日本本社に極力頼らずに手早く海外拠点だけでできるセキュリティ対策をどのように講じていくべきでしょうか。三輪氏は次のように助言します。

「何が起きたら会社のブランドを傷つけるかを徹底的に調べ上げ、それを回避するのに効果的な対策を一人ひとりに講じるべきです。守るべきポイントを局所化することが肝心です。セキュリティがどうあるべきかということ以前に、従業員個々人の業務を理解し、その人の業務にとって最も重要なことは何なのかを嘘のない形で引き出した上で、海外拠点として守るべきことは何なのかを追求します」。

「インターネットとはそもそも自分の身は自分で守らなければならぬ西部劇の世界」と三輪氏は語ります。丸腰で出て行ったら狙撃されても仕方がないと考えるべきなのです。「ゼロトラストセキュリティ」実現を目指すのをきっかけに、脅威から身を守るためにはどうすればいいか、私たちは常に自分の頭で考える習慣を身に付けなければならないようです。

引用元

※1　帝国データバンク

「海外進出企業の生産・販売拠点に関する実態調査（2023年）」
https://www.tdb.co.jp/report/watching/press/p230716.html

※2、3、4　日経BP『日経NETWORK』2022年12月号特集

「ネットワーク機器利用実態調査 2022」p.39

※5　トレンドマイクロ株式会社

「サイバーリスク国際意識調査『Cyber Risk Index』」（2022年下半期版）
https://www.trendmicro.com/ja_jp/about/press-release/2023/pr-20230508-01.html

※6　一般社団法人日本情報システム・ユーザー協会

「企業IT動向調査報告書2023」
https://juas.or.jp/cms/media/2023/07/JUAS_IT2023.pdf

※7　NRIセキュアテクノロジーズ株式会社

「NRI Secure Insight 2022　企業における情報セキュリティ実態調査」
https://www.nri-secure.co.jp/hubfs/NRIS/download/ebook/NRISecure_Insight2022_230201_Report.pdf