海外コメンタリー

**ゼロトラストとサイバーセキュリティ--英政府機関NCSCが考える意義や重要性**

Liam Tung （Special to ZDNet.com） 翻訳校正： 村上雅章 野崎裕子

2021-09-13 06:30

* [MSとVMのタッグでパブリッククラウドへのスムーズな移行を支援](https://h.f1.impact-ad.jp/pub_click/2452/mvx26CuW7RVXATdLx3VPT8MblyVSbs9_TfCnoRj0Vht5UugTgWwP4lKqkamg4BPl0iVCTltVypeBoah9bQadLcgOCXhoe2pXUOPG8YcY0dXcGbxKS4gRCeZYJohhtqCkTC_Fq5IO1MkQljXzqKXEaQn1tJKFAXa6OsJdrTJ-h99sYFAzcmTC340mx_BV8K7wTL-alVGzMfQrOYOokmNUN7z4TNWZFV2XMmZNj6hzMWdTwo4ePQuvq4BPLScj99Gr5aDqtmaKF-GKFuhTMIH0xdETb7ICkfmnTvGEolV1Jnpf7dS_QbHFBlNERE_H0om7q8eXSLZaGJ6OQxALr9Hd3YkcuF3E4y7PNHBuccxmLNXt4TjZYaOrqZ3mcVOZ9PsNe85IofkarjdhFQ_qp3f6X13GhB1o3jlUjbUhBXaOkoJOX2R960C640G8mlUUvhAmYe4bADGvdXVOHeT_HvcCKxDdacThQQ/92285/124711/)
* [導入事例、製品情報、調査・レポートなど、ホワイトペーパー多数掲載](https://h.f1.impact-ad.jp/pub_click/2452/vEfd8BH4HGJZU3TRuTtUCpaAgp3RzNGHCl95odFN5JENFTbmSD5Sxq_I1kCbVwg9fEbKOSRsEiWwsB2dkwr0UcNeixiZrY_huo9l5lm9XRnGLKzQP7UnFTR2Wa5NTRTCjmH6uUwqfn2LHQ0YmGSw__kD6SOOG17vbxY_Tg70AV25t4s6lftqKBnN70fxHtmZLvp96pdxL5BzEDfNRwugSMXqnW1LDFL4ItIj2GUT_MfasBJbojrNljOHll6fYUtMTTaVfs9-iOiix8hpxiTKPdYsBEWIGqbfKnf2Ex5iJ6bZDJxG0VcckEseoFtHvJgePynM13wOuBEInwwBxwT9Od44SwYl4ONo3KxdXEJyytUg9furb-_2iElkpEvQQpi6FZX4wqeKwa9n01nC708zSK9i79b7cir35SA3fsT9VpG7zflafBEyn-kl7abGe45JLcbNzaYqWnmQ3mhy_hR9KXuCAs_L/42663/54066/)

　ありとあらゆるITセキュリティ企業が、ますます深刻化してきているサイバー攻撃に対する回答として「ゼロトラスト」を前面に押し出しているように見受けられる。しかし、英国家サイバーセキュリティセンター（National Cyber Security Centre：NCSC）のサイバーセキュリティ専門家らは、そのつかみどころのない定義ゆえに、顧客は慎重にアプローチすべきだと警告している。

　NCSCは、ゼロトラストがITの世界で「大きな流行語」になっていると指摘した。そしてその定義の不明瞭さに取り組んでいくために、ゼロトラストへの移行を掲げる組織が気を付けるべきワナや落とし穴について概説している。

　では、NCSCによるゼロトラストの定義とはどのようなものだろうか。

　NCSCはブログ上で「ゼロトラストとは、ネットワーク上に当初から存在している信頼を取り除くというアイデアだ。ファイアウォールやVPN（仮想私設網）という『信頼された』内側に配置されている機器だからといって、当たり前のように信頼すべきではない」と[説明](https://www.ncsc.gov.uk/blog-post/zero-trust-is-it-right-for-me)している。

　そして「そうではなく、発生するさまざまなトランザクションの中で確信を築いていく方法に目を向けるべきだ。これは、数々のシグナルを吟味し、コンテキストを築き上げていくことで可能になる。こうしたシグナルは、機器の健全性やロケーションといった情報の断片であり、これによってリソースへのアクセスを許可する上で必要となる確信がもたらされる」と続けている。

　しかしNCSCは、すべての組織がゼロトラストアーキテクチャーを採用できる段階に至るわけではないと認めてもいる。また、これは標準や規格ではなく、「ネットワーク設計に向けた1つのアプローチ」だと強調してもいる。つまり、適切に実施できているかどうかを知るのは困難な場合もあるということだ。

　さらに、ゼロトラストネットワーク設計に向けた移行で発生する直接的あるいは間接的なコストもあるだろう。直接的なコストには新たな製品や機器、サービスが含まれる。一方、間接的なコストにはエンジニアの訓練や、新たなライセンスやサブスクリプションの費用が含まれる。しかしNCSCは、継続的に発生するこうしたコストについて、既存のネットワークサービスの維持や刷新のコストを下回ることもあるとしている。

　NCSCは「ゼロトラストアーキテクチャーへの移行は組織に大きな混乱を巻き起こす可能性がある。『完全なゼロトラスト』モデルへの移行は、組織全体の変革を必要とすることもあるため、達成までに数年を要する場合もある」と警告している。

　またNCSCは、「目的とするモデルがその途中で発展していく場合、どういった状態が移行完了なのかを定義するのは困難だ」と続けている。

　また、ゼロトラストというコンセプトに合致しない大規模システム、例えば二要素認証といったモダンな認証手法を搭載していないレガシーな給与支払いシステムを稼働させている多くの組織にとって、さまざまな面での考慮が必要となる。

[**Page 2**](https://japan.zdnet.com/article/35176364/2/)

　さらに、BYODアーキテクチャーといった、ゼロトラストとは両立しない製品やサービスも存在している。組織にとって、ワーカーのプライバシーを侵害することなく、機器のセキュリティが確保されているかどうかを確認するのは困難な場合もあるかもしれない。その一方、物理的に切り離されたエアギャップネットワークではクラウドベースのゼロトラストサービスを使用できない可能性がある。

　最後にNCSCは、組織が将来的にあるシステムから他のシステムに移行する能力に制限を加える可能性のあるベンダーロックインとクラウドロックインについて警告している。

　Googleは米国時間8月25日、Joe Biden米大統領とのミーティングの後、同国の重要インフラのセキュリティ強化を支援するために100億ドル（約1兆1000億円）を投資すると[発表](https://japan.zdnet.com/article/35175889/)した。また、Microsoftも200億ドル（約2兆2000億円）を投資すると[発表](https://japan.zdnet.com/article/35175745/)した。両社は、最近になって発生している重要インフラに対するソフトウェアサプライチェーン攻撃とランサムウェア攻撃に取り組むためにゼロトラスト能力に注力している。そしてIBMもSecure Access Service Edge（SASE）と呼ばれる比較的新しいカテゴリーを通じて[ゼロトラストサービスの拡充に拍車をかけている](https://japan.zdnet.com/article/35175754/)。また米国立標準技術研究所（NIST）も上述した企業を含む多数のベンダーらとともにゼロトラストアーキテクチャーのベンチマークの策定に向けて取り組んでいる。

　NCSCは以下の5つの理由から、ゼロトラストは優れた指針になり得るとしている。

* ゼロトラストモデルでは、ユーザーの操作やデバイスの動作すべてが、ポリシー上の何らかの意思決定の対象となる。これにより組織はデータやリソースに対するアクセスの試みすべてを検証できるようになるため、「攻撃が極めて難しいものになる」。
* ゼロトラストによって、企業のネットワークをユーザーの家庭まで拡大する際のネットワークオーバーヘッドを軽減しつつ、強力な認証と権限付与が実現できるようになる。
* ゼロトラストセキュリティにおける統制の中には、より良いユーザーエクスペリエンスをもたらすものもある。例えば、シングルサインオン（SSO）を用いることで、さまざまなアプリケーションを使用するたびに認証が要求されるのではなく、認証情報を一度入力するだけで済むようになる。
* データアクセスに対する統制が強化されることで、適切なユーザーに適切なデータへのアクセスを許可できるようになる。
* ユーザーのデバイスやサービスから発生したイベントをログに含めるよう、ロギング機能を拡張することで、環境内で起こっている事象についてより詳細に把握できるようになり、セキュリティ侵害をより高い精度で検知できるようになる。

この記事は海外Red Ventures発の[記事](https://www.zdnet.com/article/zero-trust-and-cybersecurity-heres-what-it-means-and-why-it-matters/)を朝日インタラクティブが日本向けに編集したものです。