ITmedia NEWS SPECIAL

CYCOGNITO

# “情報システム部門も知らない資産”がサイバー攻撃の標的に「CyCognito」で隠れたリスクを洗い出せ！

サイバー攻撃は日に日に激しさを増している。攻撃側の進化は防御側を次第に疲弊させ、もはや完全に侵入を防ぐことはできないというのが定説になりつつある。攻撃を検知し、事後対応の支援につなげる「EDR」（Endpoint Detection and Response）や、インシデント対応のための費用をカバーするサイバー保険の導入など、侵入されることを前提にしたツールやサービスの導入を検討する企業も多いだろう。

これらはすべて「侵入されるのは仕方がない、だからその後のどこかで止めよう」という考えを前提にしている。もちろんこの考え方は間違ってはいない。近年は、「数打ちゃ当たる」という意識で行われる無差別型攻撃よりも、その企業をピンポイントに狙い、あらかじめきっちりとした偵察行動の後にひそかに侵攻する標的型攻撃に注目が集まっている。このような攻撃は、侵入にも気づきにくく、被害が大きくなってしまう。

しかし、未然に侵入を防ぐことができれば、対策もよりシンプルになるはずである。侵入前提のセキュリティは重要だが、それがあるからといって、侵入を防ぐ努力を怠っていいわけではない。そもそも攻撃者に狙わせないよう、攻撃の入り口になるセキュリティホールを正確に把握し、それを埋める対策が重要だ。

標的型攻撃の初期段階では、攻撃者は対象企業のシステムがインターネットにつながっている入り口を探し、侵入の足がかりにできそうな脆弱（ぜいじゃく）性がないかを丹念に調べて攻撃を始める。脆弱性は、あらゆるOS、プログラムに存在する可能性があり、既に対策をとっている企業もあるだろう。

ところが、対策したはずなのに被害を受けるという不思議な状況に陥る場合がある。その原因は、企業のセキュリティ部門が把握できていない資産の存在や、対策が不十分なまま放置していた脆弱性にある。各事業部門が独自に立てたWebサーバ、知らないうちに外部公開されたサービス、勝手に作られたキャンペーン用のドメイン、セキュリティパッチが未適用の公開サーバなどが攻撃の入り口になるケースだ。

クラウド時代、テレワーク時代においてはデジタルトランスフォーメーション（DX）の旗の下、インターネットを介してスピード感のあるサービス展開ができるようになってきている。一方、これまでリスク管理や危機管理を行ってきたセキュリティ部門からすると、知らないうちに管理すべき対象が増えている状態だ。いつの間にか知らない場所に鍵のかかっていない入り口ができているような状況では、侵入を防ぎようがない。

このようなセキュリティホールは、内側からはなかなか見つけられない。だからこそ、攻撃者の視点に立って徹底的に入り口を探す脆弱性検査が効力を発揮する。

しかし、脆弱性検査が一時的な対応にとどまってしまい、継続的な実施ができていないことも問題の一つだ。脆弱性は日々新たなものが尽きることなく発見されていく。中にはネットワークにつながっているだけで攻撃され、悪意ある第三者に任意のプログラムを実行されてしまい、権限を奪われ機器が乗っ取られる可能性もある。

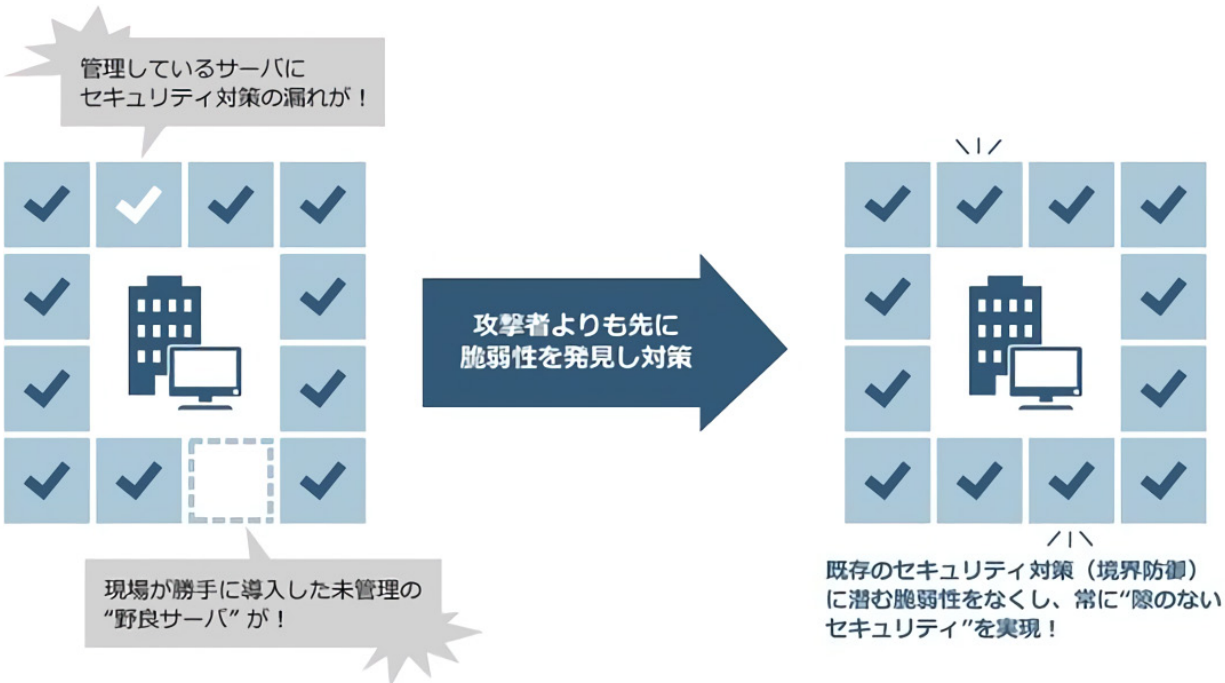
「ウチは脆弱性検査をサービス開始前にしっかり行っているから大丈夫！」というわけではなく、サービス開始後に新発見された脆弱性への対処も、インシデントの芽をつぶすためには必須だ。

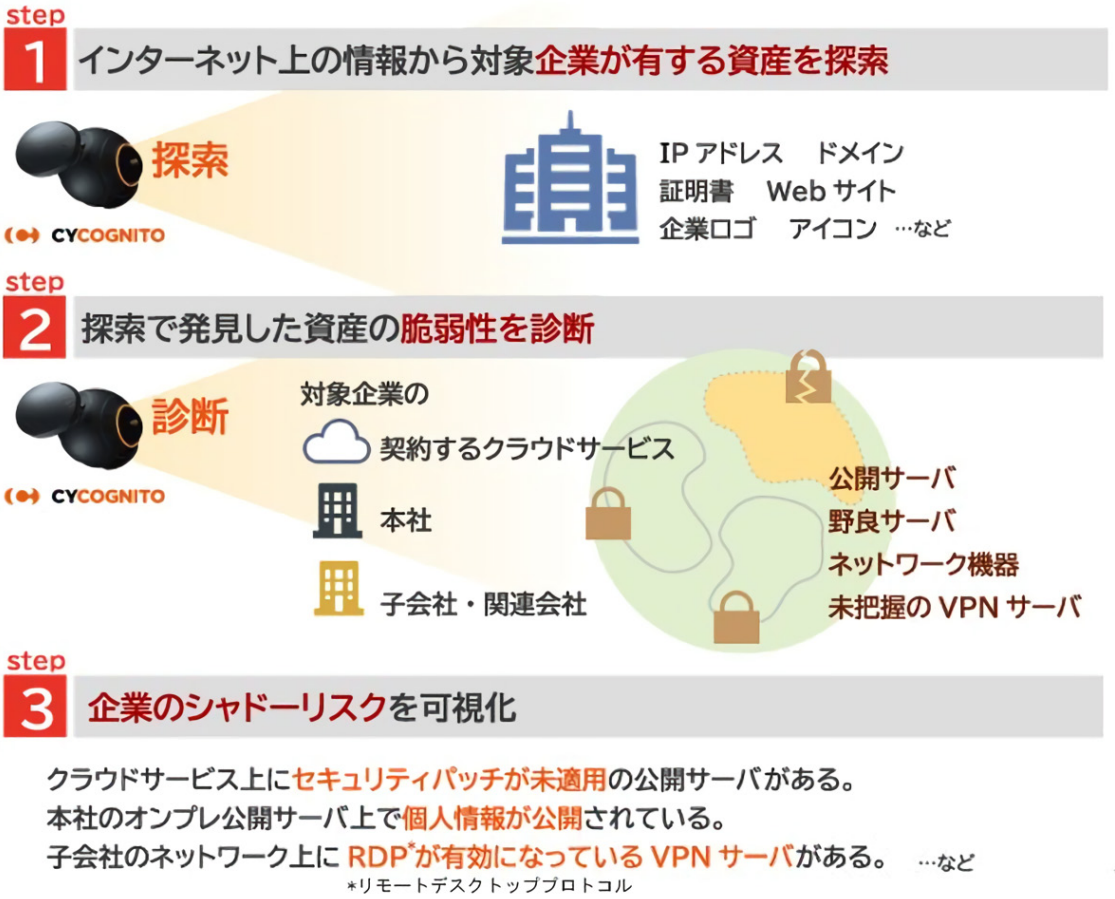
## めざすのは「狙わせないこと」

多くの企業は、インターネットに公開されたサーバを設置している。しかし、しっかりとした管理が行われていない場合、脆弱性を修正するためのアップデートが適切に行われていなかったり、設定ミスによるポート開放が知らぬうちに放置されて自由に侵入できるようになってしまっていたりと、問題の種になってしまう。

日立ソリューションズの長田義之氏（セキュリティソリューション本部）は「世間では侵入前提の対策が必要だと叫ばれているが、ここ

長田義之氏（セキュリティソリューション本部）






でもう一度基本に立ち返ってみよう」と述べる。インターネットにつながっている資産をチェックし、外部から見える脆弱性の一覧を作り、その状況と対処方法を可視化し対策できれば、侵入される可能性そのものを小さくすることができる。入り口さえ見つからなければ入ってこられないはずだ。

「引き継ぎミスなどで把握できていない公開サーバ、設定ミスなどで意図せず公開されている状態、ネットワークにつながる機器のパッチ未適用などメンテナンスがされていない状況を放置しないことが重要だ。このように管理者が気づいておらず、攻撃を受ける可能性がある状態を『シャドーリスク』と捉え、対策を行う必要がある」（長田氏）

これが、日立ソリューションズが提供するシャドーリスク対策「CyCognito」（サイコグニト）の基本的な考え方だ。

## CyCognitoが可能にすること

CyCognito は、イスラエルのエンジニアが作り出した。企業が所有するサーバやネットワーク機器などの資産を攻撃者の目線で探し、そこに存在する脆弱性を調査、調査結果とともに適切な対処方法を提示する。外部の攻撃者から見える資産をチェックするため、セキュリティ部門が把握しているかどうかにかかわらず可視化できる。これまで持っていた管理台帳以上に、正確な姿を把握できることが大きなメリットになる。

CyCognito の特長は、企業の保有する資産の探索、調査から可視化までを継続的かつ自動的に行う点だ。サーバに限らず、IP アドレス、ドメイン、証明書、Web サイトを含む資産を定期的に調査することで、システムのサービス開始後に発見された脆弱性も適切に診断できるようになる。攻撃者は偵察活動において、既知の脆弱性を順に試し、そのうち活用可能なものを特定して侵入につなげていく。その可能性を一つでも減らすことが、攻撃のターゲットに選定させないという視点で重要だ。

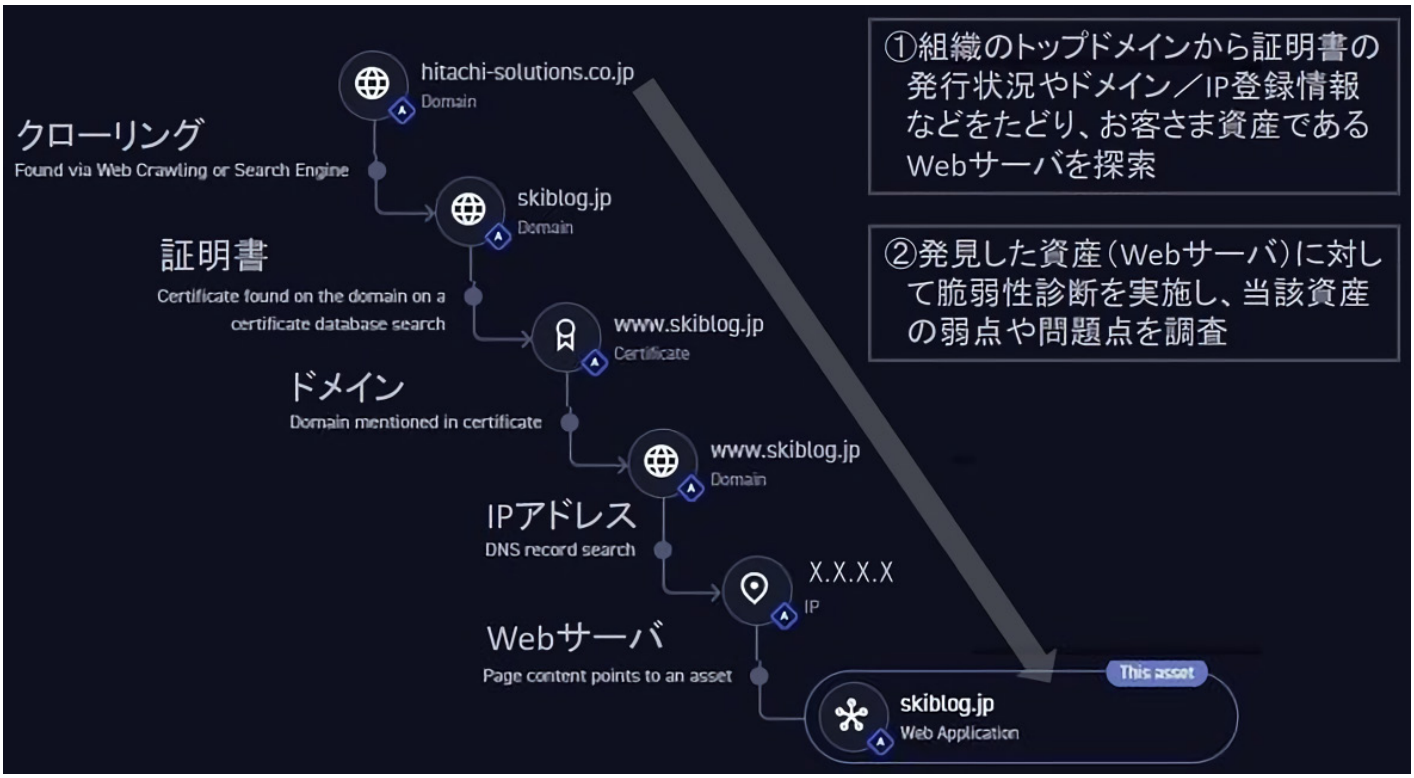
もちろん、この継続的な探索、調査は既存サービスの運用動作に影響を与えないよう、しっかりと調整されている。継続的かつ自動的に探索、調査を行い、対処法まで提示するため、利用している企業が常にセキュリティに詳しい人材を割り当てる必要もない。攻撃者視点で攻撃対象となりうる、インターネットにつながる資産を自動的に探し、脆弱性診断を手間なく継続的に実施することで、サイバーセキュリティにおける理想「狙わせないことをめざす」を実現できるのだ。

## トップドメインから資産をクローリング、子会社、関連会社も対象に

調査のステップを詳細に見てみよう。CyCognito は企業の資産を「ドメイン名」「IP アドレス」「Web サーバ証明書」「Web サイト」の 4 つと定義して管理する。企業のトップドメインから CyCognito の bot が企業の資産を継続的に探索、取得したドメインやサブドメインなど、企業の全資産をチェックする。例えば、管理外だった Web サーバ、FTP サーバ、開発環境、意図しない RDP サーバ、VPN サーバなどを洗い出す。これらに対し、継続的に脆弱性や各種設定をチェックする。

これらのチェックにより、近年問題となっている VPN サーバの脆弱性放置による不正な侵入や、「サブドメインテイクオーバー」と呼ばれる不正な乗っ取りを防ぐことができる。脆弱性以外にも、意図しないポート解放や設定ミスによるデータの公開に対しても可視化が可能だ。気づいていないことには対処が行えないからこそ、手間をかけずに攻撃者目線での自動チェックを実現する CyCognito は大きな力になるだろう。

発見された脆弱性に関しては、ベンダーの公式ドキュメントへのリンク、適用すべきアッ



企業をクローリングすることで関連する別ドメインも探し出し、そのサーバに問題点がないか調査可能だ

プデートプログラムなどを表示する。リスクの大きさなども解説があるので、対処の優先順位を付ける参考にもなる。

## 対処すべきは「把握できていない現状」

サイバー攻撃をどう防ぐかは非常に難しい問題だ。今注目されている考え方の一つに「ゼロトラストセキュリティ」という概念もある。すべての情報資産へのアクセスにおいて「認証を都度行い、それをクリアしなければ信頼しない」という考え方はサイバー攻撃に対抗しうる、素晴らしい考え方であるといえる。しかし、それを実現するためには大きな構造変革が必要で、これまで投資してきたセキュリティ対策を大きく変える必要がある。

しかし、その前にできることはたくさんある。境界防御を強化するということも重要だ。これはゼロトラストセキュリティと相反するものではない。その一歩として、自社が持つ資産をしっかりと把握し、何があるのかを漏れなく知っておくこと、そして見えるようになった各資産に対して、今できる対策をしっかりと行うことこそ、最初のステップなのではないだろうか。これこそが、CyCognitoと日立ソリューションズの狙いだ。

日立ソリューションズの真島秀一氏（セキュリティソリューション本部）は、今後の展望として日本語化をはじめとするCyCognitoのUI（ユーザーインターフェース）の強化に加え、日立グループに所属するホワイトハッカーたちによるコンサルティングサービスとCyCognitoを組み合わせるなど、これまで提供してきた各種サービスとのシナジーを生かすことを検討している。


真島秀一氏（セキュリティソリューション本部）

「脆弱性診断サービスはパートナーと共同で既に提供している。CyCognitoを付加価値として提供することで、サイバー攻撃対策にどこから手を付けていいか分からないという企業に対して、適切な提案が可能になる」（真島氏）

今、新型コロナウイルス感染症の影響でテレワークの導入が進み、インターネットにつながる入り口が広がり続けている。サプライチェーンのリスクとして、関連企業のセキュリティチェックも必要だろう。CyCognitoにはトライアルもある。「何か対策しなくては」と考えている企業は、まずCyCognitoを試してみてはいかがだろうか。

● お問い合わせ
**株式会社 日立ソリューションズ**
URL : https://www.hitachi-solutions.co.jp/cycognito/



※この冊子は、ITmedia NEWS（https://www.itmedia.co.jp/news/）に2021年3月に掲載されたコンテンツを再構成したものです。
https://www.itmedia.co.jp/news/articles/2103/16/news003.html


W21K-01-00