セキュサポ

事業継続を揺るがす サイバー攻撃の脅威

～これからのセキュリティで大事な考え方～

AMIYA

Index

■ 警察庁発表のレポートから読み取るサイバー攻撃の動向 ・・・・・・・・・・・・・・ 2

■ 大規模化するランサムウェア攻撃 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 3

■ サイバー攻撃は事業継続上の大きなリスクに ・・・・・・・・・・・・・・・・・・・・・・・ 3

■ 効果的なセキュリティ対策とは？
ツールの導入より、まずは脆弱性への対応を！ ・・・・・・・・・・・・・・・・・・・ 4

■ サイバー攻撃を受ける前提でセキュリティ対策を考える
被害を最小化する方法とは？ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 5

■「表向きには異常性がない被害」にも注意を ・・・・・・・・・・・・・・・・・・・・・・・ 5

■ 迅速なインシデント対応にはログが必要不可欠 ・・・・・・・・・・・・・・・・・・・・・ 6

■「サイバー攻撃対策に注力したいけれど、
人材の確保も予算投資も難しい……」 ・・・・・・・・・・・・・・・・・・・・・・・・・・ 7

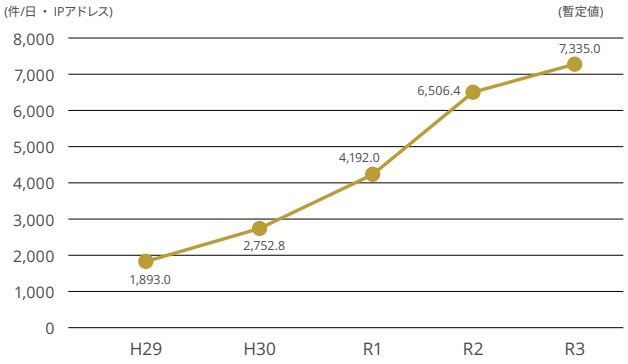
■ 中堅・中小企業で大手企業レベルのサイバーセキュリティを
セキュサポ ・・ 7

警察庁発表のレポートから読み取る**サイバー攻撃の動向**

令和 4 年 2 月 10 日、警察庁より「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」が発表されました。これによるとサイバー攻撃の脅威は年々拡大しており、たとえば、観測されたサイバー空間における脆弱性探査行為等の件数は前年の約 1.3 倍、3 年前の平成 30 年と比較すると 2.5 倍以上に増加しています。

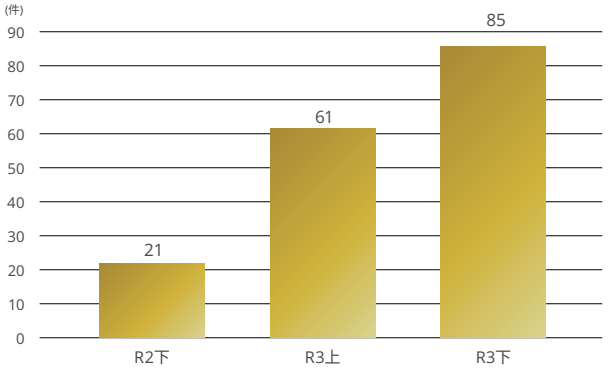
また今回のレポートでは、特にランサムウェア攻撃について多くのページを割いており、その注目度がうかがえます。実際、被害件数は令和 3 年上期は前年下期の約 3 倍まで拡大しており、増加傾向はその後も続いています。

サイバー空間における脆弱性探査行為等の観測状況



センサーにおいて検知したアクセス件数の推移
出典：警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」

ランサムウェア被害の報告件数の推移



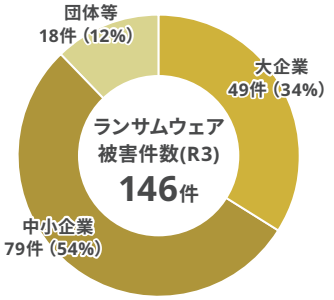
企業・団体等におけるランサムウェア被害の報告件数の推移
出典：警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」

同レポートに掲載された被害企業の規模のデータによると、企業規模や業種を問わず攻撃を受けていることが見て取れます。特に医療を狙った事件が目立っており、徳島県の病院がランサムウェア被害に遭ったことは、社会に大きなインパクトを与えました。

徳島県つるぎ町立半田病院

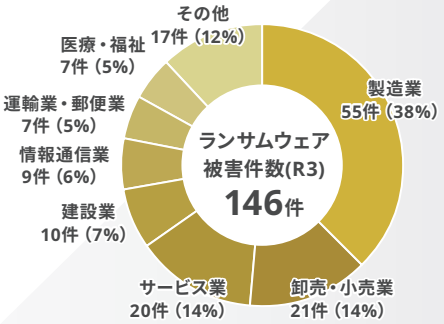
感染状況	電子カルテシステムがランサムウェアに感染
被害	患者の診断履歴や病歴などを正確に把握できない状態に
生じた影響	システムの復旧に**約2か月**を要した

企業規模別 報告件数



被害企業・団体等の規模別 報告件数（令和3年）
出典：警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」

業種規模別 報告件数



被害企業・団体等の業種別報告件数（令和3年）
出典：警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」

大規模化するランサムウェア攻撃

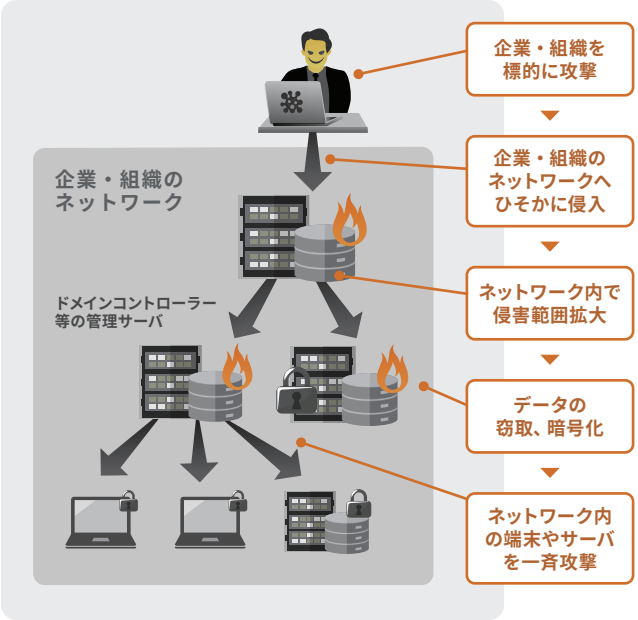
この背景には、ランサムウェア攻撃で新たな潮流が生まれていることがあります。これまでのランサムウェア攻撃は、一部のシステムが暗号化されるというケースが多く、バックアップでリカバリーするという対応が有効とされてきました。

しかし昨年の大手製品会社の事例や、先日発生した自動車グループの事例にみられるように、組織全体のシステムを破壊するケースが散見されるようになってきました。

たとえば LockBit と呼ばれるランサムウェアは、秘匿性、浸透力、暗号化の処理速度が非常に高く、Active Directory の権限を盗み、グループポリシーを利用して一気に展開、さらにはバックアップや隠しドライブを探り出し、それらを含めて暗号化します。暗号化の処理には独自の技術を複数用いており、データサイズに関わらず高速で暗号化するため、気が付いた時には広範囲のシステムが壊滅状態、頼みの綱のバックアップも使い物にならないという、システム管理者にとっては悪夢のような代物です。このランサムウェアは、前述の病院でも使われたとみられています。

新たなランサムウェア攻撃

IT システム全体が停止。事業継続を揺るがすリスク。



サイバー攻撃は事業継続上の大きなリスクに

新しいサイバー攻撃のトレンドから導かれる影響としては、「どんな企業もサイバー攻撃によって大きなダメージを被る」ということです。

従来のサイバー攻撃は、重要情報の窃取を目的とした標的型攻撃や、ランサムウェアによる部分的な情報の暗号化が主流でした。しかし最近の事件は1つの組織内の被害にとどまらず、グループやサプライチェーン全体を巻き込んだ大規模なものとなっています。

そのため「やられたらしょうがない」、「諦める」という選択肢や、「うちには盗まれて困るような情報はない」という言い逃れは通用しません。

また、自社の対策がしっかりしていても、関連する組織のセキュリティの穴を突いて侵入されれば、ドミノ式に自社のシステムも被害にあうため、関連組織のセキュリティ対策にまで目を光らせ、セキュリティに対する認識の甘い組織には、厳しく対応を迫る必要が生じています。

価値の高い情報を一本釣り

対象組織の広範な情報を破壊

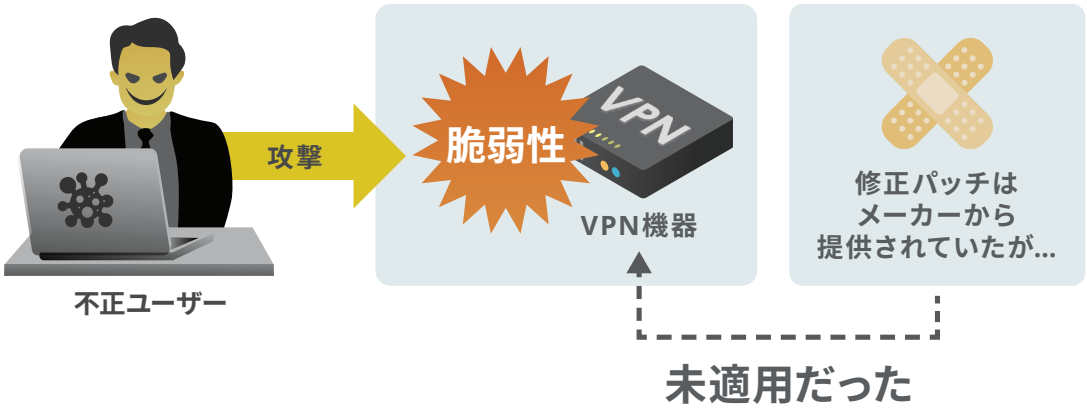
効果的なセキュリティ対策とは？
ツールの導入より、まずは脆弱性への対応を！

さて、ホラーストーリー（といってもかなり現実的な話ですが……）はこの程度にして、効果的なサイバーセキュリティ対策について考えてみましょう。

「セキュリティ対策」には様々な手段があります。多くの方は「防御」に関連した手段を考えられるのではないでしょうか。UTM のようなネットワークセキュリティに始まり、最近導入する企業が増えている EDR のようなエンドポイントセキュリティ、クラウド利用の拡大にともなう SASE なども人気です。

しかし、このようなツールの導入の前に実施して欲しいことがあります。それは「脆弱性への対応」です。事業継続を揺るがすリスクとなったランサムウェアは、社内ネットワークへ侵入するところからすべてが始まりますが、その侵入経路として、徳島の病院や大手製粉会社はセキュリティ強化のために導入した UTM の脆弱性を利用されました。UTM メーカーからは、該当の脆弱性に対するセキュリティパッチが提供されていたものの、被害にあった組織では未適用のまま脆弱性を放置。いくらセキュリティツールを導入しても、十分な運用ができなければ、逆にセキュリティレベルを下げる結果となってしまいます。

また、ランサムウェアに限らず、ほとんどのサイバー攻撃はシステムの脆弱性を利用します。グローバル IP アドレスへのスキャンなどにより、攻撃しやすいターゲットを探索し、脆弱性が見つかれば、攻撃を仕掛けるのが一般的な流れです。つまり、脆弱性を放置すれば攻撃される可能性が高まり、脆弱性がなければ、攻撃対象になりにくいと言えます。そのため、IT システムの脆弱性を適切に管理する体制を構築・運用することは、非常に効果的なセキュリティ対策と言えるでしょう。



脆弱性対策に

「脆弱性診断サービス」

脆弱性を適切に管理するためには、「脆弱性がある」ことを知るところから始まります。その方法は二つです。一つは、「グローバル IP を持つ機器をリスト化し、定期的に公開されている脆弱性について確認する」という方法。これは適切に運用できれば、その機器が持つ脆弱性をゼロにすることができるのですが、機器が増えるほど管理の手間がかかるのが難点です。

もう一つは、グローバル IP をもつ機器に対して「定期的に脆弱性スキャン」をすることです。半自動的にできるため、機器が増えても手間が増えないことがポイントです。注意点としては「全ての脆弱性を検知できるわけではない」ということ。どうしても漏れは生じてしまいます。とはいえ、攻撃者自身もこの方法で脆弱性のある機器を探していることから、攻撃者と同じ視点で脆弱性をなくしておけば、かなりの確率でサイバー攻撃を防ぐことができるでしょう。

サイバー攻撃を受ける前提でセキュリティ対策を考える
被害を最小化する方法とは？

まず抑えておきたいポイントは、どれだけサイバー攻撃対策をしても「リスク発生の可能性はゼロにはならない」ということ。サイバー攻撃の脅威と対策はイタチごっこの状況で、攻撃者は次々と新しい方法で攻撃を仕掛けてきます。つまり多額のコストをかけたとしても、全てのサイバー攻撃に対応することは事実上不可能と言えるでしょう。

そこで、大切な考え方は、サイバー攻撃を受けることを前提とし、事業継続における被害を最小化することです。サイバー攻撃被害に遭った場合、「原因 / 侵入経路 / 影響範囲の確認、感染端末の隔離、システム復旧、そして説明責任の遂行と再発防止」というのが一般的な対応の流れです。そして、この対応を迅速に行うことが、事業継続上の被害を最小化するポイントとなります。

「表向きには異常性がない被害」にも注意を

例えば、重要 IT システムがランサムウェア被害を受けた場合。利用できないシステムはすぐに特定できるため、まずはバックアップから被害にあったシステムの復旧を試みると思います。しかし、ここで注意していただきいポイントが一つ。サイバー攻撃には、「表向きには異常性がない被害」が存在します。侵入経路や、攻撃者のコントロール配下になっているシステムなどですね。これらの特定と対策も合わせて行わなければ、重要 IT システムをバックアップから復旧しても、再度被害にあうことでしょう。一連のインシデント対応を迅速に行うことが、サイバー攻撃の被害を最小化するポイントとなります。

一般的なインシデント対応フロー

1

原因/侵入経路/影響範囲の確認

2

感染端末の隔離

3

システム復旧

4

対外的説明と再発防止

迅速なインシデント対応には**ログが必要不可欠**

前述したように、迅速なインシデント対応ができる体制を整備していれば、事業への影響を最小限にすることができます。そのためには、原因の特定と影響範囲の特定が重要ポイント。原因が特定できなければその対策をすることができず、影響範囲が特定できなければ、全システムの調査、場合によっては全システムのクリーンインストールをする必要が出てきます。迅速なインシデント対応には、原因と影響範囲を迅速に特定する必要があります。そこで有効なのがログです。システムが出力するログから、そのシステムの現状や過去の事象を読み解くことができるためです。

VPN 機器のログからは、不正侵入された記録を。PC のログからはどの PC が感染しているかを。Active Directory のログはどういったコマンドを実施したかを。ファイルサーバのログからはどのファイルが暗号化されたかを。このように、ログからサイバー攻撃の流れを調査することで、原因、影響範囲の特定とその対策が実施できるようになりまし、裏を返せば、ログがなければ原因も影響範囲も特定できません。

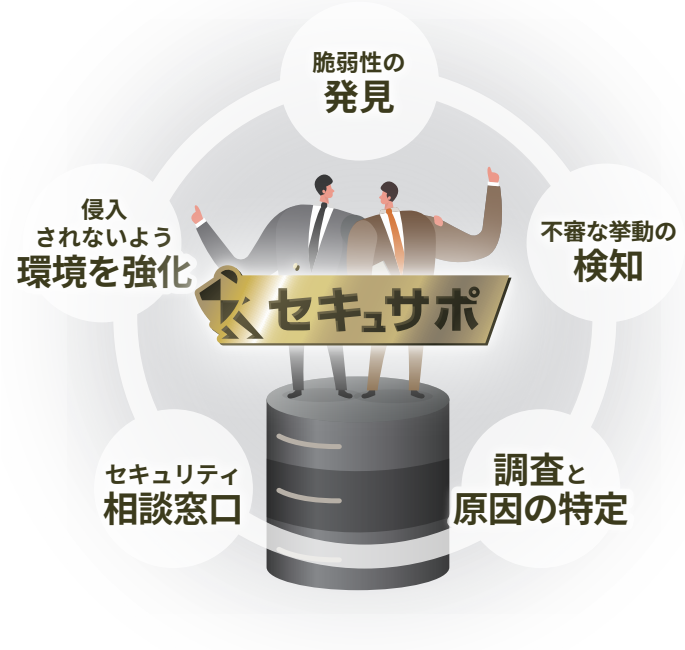
また、ログからはサイバー攻撃の兆候がうかがえます。VPN 機器への異常なログイン試行や異常な時間帯でのログイン、さらには普通ではありえない海外からのログインなど。このような兆候をログがあれば捉えることができ、サイバー攻撃被害発生前に攻撃から防御することも可能です。

	ログがなければ	ログがあれば
異常の検知	システム的に制御できない **抜け穴が無防備**に	システム的に制御できないルートは **異常検知で監視**
原因究明	原因が特定できず **再発リスク**が残る	具体的な **原因の特定が容易**に
影響範囲調査	**全システムの調査**が 最低限必要	具体的な **影響範囲の特定が容易**に
対策	あらゆるケースを想定した 対策が必要となり**コストがかかる**	把握した攻撃内容から **効果の高い対策**が可能に
対応スピード	上記の理由から**時間がかかる**	比較的**早期**に対応可能
納得性のある報告	原因も影響範囲もわからないため **説得力に欠ける**	原因・影響範囲・対策が明確となり **説得力のある報告**が可能に

「サイバー攻撃対策に注力したいけれど、人材の確保も予算投資も難しい……」

本資料では主に、脆弱性管理とログ管理が効率的なサイバー攻撃対策だと解説しました。連日のニュースでも報道されている通り、日本企業は今、かつてない規模のサイバー攻撃の危険にさらされています。凶悪化した最近のサイバー攻撃は、セキュリティが強固な大企業を直接狙うのではなく、比較的セキュリティ対策が不十分な中堅・中小企業を経由し、その企業グループやサプライチェーン全体に影響を及ぼす傾向にあります。こうした社会情勢を受け、サイバーセキュリティ対策が急がれる一方で、特に中堅・中小企業で顕著に不足しており、人材不足を理由にセキュリティ対策が進んでいないのが実情です。

中堅・中小企業で大手企業レベルのサイバーセキュリティを



クラウド CSIRT サービス「セキュサポ」はセキュリティ対策の導入から事故時の対応までをワンストップで提供するセキュリティ代行サービスです。

「脆弱性診断サービス」や「セキュリティ相談窓口」といったサイバー攻撃対策サービスを加えることで、中堅・中小企業のセキュリティ強化をトータルに支援。サイバー攻撃・内部不正の監視や脆弱性診断、事件時の原因特定や影響範囲の調査、日ごろのセキュリティ相談の窓口など、サイバーセキュリティの専門チームが、貴社のセキュリティ対策に求められる包括的な対応を月額固定料金で提供します。

サイバー攻撃対策
お客様環境に検知システムを常設。外部攻撃を常時監視

内部不正対策
内部不正の兆候を AI を使って常時監視

脆弱性対策
公開サイトを脆弱性検査し、脆弱性の発見と改善を実施

強化レポート
対策を証明する各種レポートを定期で提出

インシデントレスポンス
事故発生時には、インシデントレスポンスを実施
（原因や影響範囲の調査など）

サイバー保険
インシデントレスポンス費用をサイバー保険でカバーリング。原則無償対応を実現

＼さらに！／

セキュリティ相談窓口
不審なメールの安全確認など、日常の CSIRT 対応を代行

セキュサポ

セキュサポ

セキュリティ専門チームがお客様の環境全体を監視し、
ランサムウェア攻撃をはじめとした一連のサイバー攻撃への対策を包括代行。
コストと手間を減らしながら最高のセキュリティレベルを月額固定料金でご提供します。

詳しい製品概要資料はこちら

詳しい製品のご紹介、評価版のご依頼は以下にお問い合わせください。

お問い合わせ先

株式会社網屋　データセキュリティ事業部

TEL：**03-6822-9996**　E-mail：**bv-sales@amiya.co.jp**

開発元

AMIYA 株式会社 網屋

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999 FAX: 03-6822-9998

https://www.amiya.co.jp/

記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。
このパンフレットの内容の一部またはすべての複写・転用・転載等を株式会社網屋に無断で行った場合、
著作権の侵害になります。

販売元