BlackBerry
Intelligent Security. Everywhere.

ソリューション概要

ランサムウェアを予防し、被害を修復

ランサムウェアインシデントのリスクと影響を軽減

はじめに

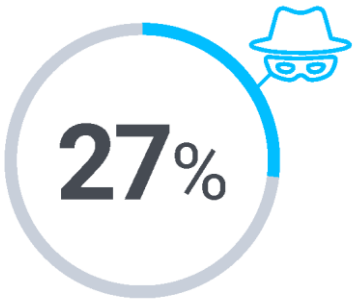
ランサムウェアは、ファイルを暗号化することによって被害者がシステムやデータにアクセスできないようにする、恐喝型マルウェアの一種です。多くの場合、暗号化されたファイルは、ランサムウェアの脅威アクターから復号鍵を購入することによってのみ回復できます。被害者が身代金要求に速やかに応じなかった場合、攻撃者が身代金の額を釣り上げたり復号鍵を削除したりして、ファイルを回収できなくする場合があります。

現在最も一般的な攻撃ベクトルがフィッシングであることに変わりはないものの、脅威アクターが導入したさまざまな戦術、技法、手順により、今では、悪意のあるリンクをクリックしたり武器化されたドキュメントを開封したりしなくても、被害者を感染させることが可能になっています。この攻撃では、EternalBlue などのエクスプロイトと一般的でないプログラミング言語を使ってデータ形式を不明瞭化し[1]、被害者のシステムにランサムウェアを直接送り込むことで、暗号化鍵の交換や支払い処理に必要な永続的アクセス権を取得します。ネットワークセキュリティ制御には、感染したシステムと外部のコマンドアンドコントロール（C2）サーバー間を行き来する疑わしいトラフィックを検知・遮断する機能がありますが、こうした攻撃には、このようなネットワークセキュリティ制御を回避する能力があります。

また、被害者からデータを抜き取った脅威アクターが、身代金要求に応じない場合はデータ流出や規制当局への通報を行うことを脅迫するケースも増えています。たとえば 2019 年 12 月、ランサムウェアグループ Maze は、被害者とされる人々から盗み出したデータの抜粋を専用の Web サイトに掲載し始めました[2]。

警察当局は支払いを拒否するよう被害者に指導しているものの、業務が機能不全に陥るレベル、顧客や株主に対する影響の大きさ、回復と正常化にかかるコストや、データ漏洩によって生じる法的な罰則、ブランドイメージの毀損、評判低下の程度を考慮した結果、多くの企業が結局は支払いを選ぶでしょう。

企業に対する
ランサムウェア攻撃のペース
（2021 年末までの予測）

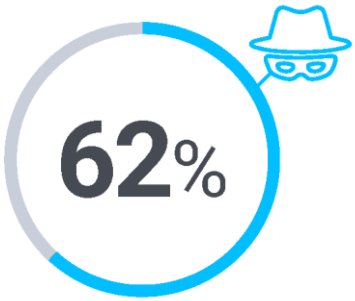


マルウェア関連の
セキュリティインシデントに
ランサムウェアが占める割合

ビジネス上の課題

現在ランサムウェアは国家アクターにとってもサイバー犯罪組織にとっても大きなビジネスに位置付けられており、マルウェア関連のセキュリティインシデント全体の 27% をランサムウェアが占めています[3]。私たちは次のような悩ましい数字を直視しなければなりません。

- 企業に対するランサムウェア攻撃は、2021 年末までには 11 秒に 1 回のペースで発生し[4]、いずれかの攻撃が 40 秒に 1 回成功しています[5]。
- 『2020 Cyberthreat Defense Report（2020 年サイバー攻撃の脅威防御レポート）』に参加した企業の 62% が、ランサムウェア被害を受けた経験があると回答[6]し、そのうち 58% が身代金の支払いを選択しています（前年比 13% 増）。



ランサムウェア被害を受けた
経験があると回答した、
『2020 Cyberthreat Defense Report
（2020 年サイバー攻撃の脅威防御レポート）』
参加企業の割合

1 脅威のスポットライト：教育業界とソフトウェア業界を標的にする Tycoon ランサムウェア
2 Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up（ランサムウェア攻撃者、支払いに応じない被害企業のデータを漏洩へ）
3 Verizon 2020 Data Breach Investigations Report（2020 年 Verizon データ侵害調査レポート）
4 Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021（全世界のランサムウェア被害額、2021 年までに 200 億ドルに達する見込み）
5 What It Means to Have A Culture of Cybersecurity（サイバーセキュリティの文化を根付かせる意味とは）
6 2020 Cyberthreat Defense Report（2020 年サイバー攻撃の脅威防御レポート）

- 2021 年における全世界のランサムウェア被害の予測コストは、2017 年の 50 億ドルから 300 %増加し、200 億ドルに達すると見られています[7]。このコストには、身代金の支払い額に加え、回復と修復の費用や、失った生産性や毀損された評判を換算した金額が含まれます。

数多くのリスクが知られているにもかかわらず、多くの企業は、ランサムウェア攻撃やその影響に対してあまりにも無防備です。そのことを裏付ける NTT セキュリティの調査データ[8]があります。

- 回答者の 1/3 は、セキュリティへの先行投資によって侵害発生を回避するよりも、身代金を支払うことを選んでいます。
- 正式なセキュリティポリシーを整備しているという回答者はわずか 58%
- 48% の回答者はインシデント対処（IR）計画を策定していません。策定していると答えた人のうち、すべての内容を把握しているのはわずか 57%

セキュリティへの先行投資によって
侵害発生を回避するよりも、
身代金を支払うことを選ぶ
回答者の割合

BlackBerryのアプローチ

BlackBerry Spark® Unified Endpoint Security アプリケーションスイートと BlackBerry Security Services ソリューションは、事後対処型から防御優先型へのセキュリティ体制の変革を通して、企業におけるランサムウェアのリスクを最小化します。

BlackBerry® Protect：アプリケーション/スクリプト制御、メモリ保護、デバイスポリシー適用の各機能に最先端の人工知能（AI）技術を組み合わせ、マルウェア、ランサムウェア、ファイルレスマルウェア、悪意あるスクリプトによるクライアントシステムとデータの侵害を阻止する、エンドポイント防御プラットフォームです。BlackBerry Protect は、WannaCry、Goldeneye、Satan が一般で発見されるはるか昔の 2015 年 9 月から現在までを対象とする予測数理モデルを活用し、これらのランサムウェアの亜種が実行されるのを防止します。この予測優位性は第三者によって実証済みで、ほかにも Emotet（816 日）、GandCrab（795 日）、Glassrat（548 日）、PolyRansom（862 日）、Sauron/Strider/Remsec（548 日）、Zcryptor（182 日）をはじめ数多くのランサムウェアやマルウェアに対処します。

BlackBerry® Optics：エンドポイントのテレメトリデータの収集・転送～システムのオフライン化に至る検知・対処ワークフローを自動化し、BlackBerry Protect が提供する脅威防御をさらに拡張する、エンドポイント検知・対処（EDR）ソリューションです。ワークフローのトリガーには、AI ベースのコンテキスト分析エンジン（CAE）モデル、カスタムルール、MITRE ATT&CK® による APT 攻撃の戦術、技法、手順に基づくルールなどを使用できます[9]。さらに BlackBerry Optics は、根本原因分析やスマート脅威ハンティングなどの最先端の機能も提供します。

インシデント対処（IR）計画を
策定していない回答者の割合

7 Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021（全世界のランサムウェア被害額、2021 年までに 200 億ドルに達する見込み）
8 NTT レポート『Risk:Value 2019 Destination standstill. Are you asleep at the wheel?（Risk:Value 2019：停滞するセキュリティの現状と、今確認すべき目的とは）』
9 BlackBerry Outperforms on the MITRE ATT&CK Framework Testing（BlackBerry、MITRE ATT&CK フレームワークテストで優れたパフォーマンスを発揮）

インシデント対処とフォレンジックのコンサルティングサービス：ランサムウェアその他のセキュリティ侵害の調査、封じ込め、修復、再発防止に必要なサポートと方針策定を、BlackBerry Security Services IR チームのエキスパートが提供するもので、AIが組み込まれた BlackBerry チーム独自のツールとプロセスによって初動調査の結果をスピーディに生成し、初回のデータ収集から数時間以内には、ランサムウェアや APT 攻撃の検知、フォレンジック分析、封じ込めを開始します。

攻撃シミュレーションのコンサルティングサービス：現実的な条件設定の下、BlackBerry Security Services の攻撃シミュレーションチームが企業の防御体制に対するテストと演習を実施し、防御・検知・対処機能における致命的ギャップの特定を支援します。防御機能の実践演習、セキュリティ前提条件の検証、セキュリティ体制の致命的ギャップ特定を希望する企業には、侵害シミュレーションが推奨されます。自社の業界に頻繁に攻撃を仕掛けている現実の脅威アクターグループの攻撃を検知・対処する経験を積んでおきたい企業には、攻撃者シミュレーションが推奨されます。

BlackBerry® Guard：サブスクリプションベースのマネージド型検知・対処サービスです。BlackBerry Protect と BlackBerry Optics に加え、BlackBerry のエキスパートチームによる世界水準のインシデント対処・防御サポートを 24 時間 365 日利用できます。セキュリティ侵害からの回復作業を BlackBerry Guard に任せることで、企業のセキュリティチームが重要なセキュリティの取り組みに集中できるようになります。

詳細情報

ランサムウェアの防御・修復に関する BlackBerry のソリューションポートフォリオについて詳しくは、こちらをクリックしてください。お急ぎの場合は 03-5575-1511（代表番号）までお問い合わせください。

期待されるメリット

BlackBerry のランサムウェアに関するソフトウェア/サービスソリューションポートフォリオにより、次のことが可能になります。

- **インシデントの発生を最小限に抑える**：検知・対処・修復の一連の処理を自動化し、プロアクティブな脅威ハンティングと根本原因分析を支援することで、ランサムウェアの実行と拡散を防止します。
- **リスクへの露出を最小限に抑える**：CISO とセキュリティチームは、エキスパートのガイダンスとサポートを活用して、セキュリティファブリックのギャップを特定して対処し、サイバー防御力を強化し、堅牢なインシデント対処プロセスを実装して、事後対処型から防御優先型へのセキュリティ体制の変革を効率的に推進できます。
- **ランサムウェアインシデントに迅速に対処する**：中規模のプロバイダーや大規模なコンサルティング企業の場合、侵害対処の待機時間が数週間にもなることがあります。その間にも被害は広がり回復と正常化のコストも上昇していきますが、BlackBerry が誇るランサムウェア専門のエキスパートがいれば、業界最高水準の一貫性あるサービスを問題発生の直後から利用できます。
- **迅速に回復する**：『*Forrester's Guide To Paying Ransomware (Forrester ガイド：ランサムウェアに対する支払い)*』では、ランサムウェア攻撃からの回復支援を担うわずか 6 社の 1 つに BlackBerry が選出されています。

BlackBerry について

BlackBerry（NYSE：BB、TSX：BB）は、インテリジェントなセキュリティソフトウェアおよびサービスを世界中のエンタープライズと政府機関に提供しています。現在 BlackBerry がセキュリティ保護しているエンドポイントの数は 5 億台を上回り、そのうちの 1 億 7,500 万台は道路を走行する車両です。BlackBerry はカナダのオンタリオ州ウォータールーに本拠を置き、AI と機械学習を活用してサイバーセキュリティ、安全、データプライバシーソリューションの分野に革新的なソリューションを提供しています。また、エンドポイントセキュリティ管理、暗号化、組み込みシステムの分野におけるトップクラスの企業です。BlackBerry のビジョンは明確です。つながる未来に信頼性あるセキュリティを確保することです。

詳細については、BlackBerry.com にアクセスし、@BlackBerryJPsec をフォローしてください。

BlackBerry
Intelligent Security. Everywhere.

MKTG20-0504 | 200923