COVID-19: Cyber Preparedness & Response(サイバー における準備と対応)

展 望

テクノロジーに依存した今日のビジネス世界において、COVID-19によりどのようなインパクトがもたらされるのかについての**前例は限られています**。過去の伝染病と異なり、COVID-19は**非連続的な金融「ショック」をもたらします。混乱は日々拡大していることから、サイバーにおいても二次的、三次的な影響がおよぶ可能性があります。**

サイバーの考察

当面のインパクト / 一時的な混乱への対応

長期的なインパクト / 経済環境への対応

	リモートワーク、人材調達/人員確保の混乱	クリックベイト / ソーシャルエンジニアリングの増加	第三者に対するリスク許容度の緩和	潜在的脅威と支出の削減/再分配	日和見的M&A活動の増加	レイオフ/不満を抱えた従業員
Trend						
Cyber Impact	• 遠隔からのアクセス増加に伴い、VPNの帯域幅および管理の検証が必要 • テクノロジーの導入が簡素化 • 自宅におけるネットワークを確保し、モニタリングを行う必要性が新たに発生 • 家族に対して特別なケアが必要になることから、人材の確保に影響が及ぶ	• 財務情報や個人情報を狙ったソーシャルエンジニアリングによるサイバー攻撃が増加 • テーマ型フィッシングやマルウェアを使った攻撃により、サイバーリスクの脅威が高まる • 誤った情報が拡散することで、危機対応が困難	• サプライチェーンの混乱により、セキュリティの運用に影響が及びます。不測の事態においては、プロバイダーは、同等のセキュリティ範囲に対応しきれない可能性があり、デジタルリスクが高まる • セキュリティーサービスのプロバイダーが対応する範囲は、検疫の影響を受ける。	• 予算の削減によりセキュリティ機能に十分なリソースを割けなくなることから、デジタルリスクが高まる • 初期の日和見攻撃による脅威が潜み続けていることから、持続的に高いリスクにさらされる	• 長期的な経済のダイナミズムでは、日和見的なM&Aが性急に進められることから、十分なサイバーデューディリジェンスがなされない可能性がある (例：敵対者分析、脅威回避選好度評価、侵害評価、レッドチームセキュリティ評価)	• 通常のビジネスサイクルが阻害されることで、組織再編や大規模な従業員数の削減を余儀なくされる • 業務環境や経済環境が、内部者脅威に関するリスクを高める
Consideration	リモートアクセスコントロールは拡張可能ですか？優先テクニカルプロジェクトと新しいサポートのニーズにセキュリティは、どのように対応しますか？	悪意のある動きを積極的に特定するための知識を持ち、意識を高めていますか？脅威の検出やそれらへの対応を強化していますか？	サービスへのアクセスや可用性の優先付けを行うにあたり、第三者のセキュリティプランをどのように進めていますか？	厳しい経済環境下において、貴社のセキュリティプログラムをどのようにしてより効果的、効率的なものにしますか？	M&Aやコーポレート戦略にサイバーをどのように組み入れていますか？	リスクに基づいた内部者脅威のモニタリングプログラムをどのように推進しますか？

Steps to Secure your Environment

Today

- **日誌を作成 (例：トランスクリプト)**
  - 記録をつける担当者を指名
- **チームがバーチャルでどのように協同できるかを把握**
  - システムが拡張可能であることを確認
  - テクノロジーの導入前に脅威およびリスク評価が完了していることを確認
  - 遠隔で勤務する従業員 (データセンターやデリバリーセンターを含む) をグローバルベースで特定
- **サプライチェーンの依存関係と混乱を識別**
  - サービスレベルアグリーメントを評価し、第三者の混乱が下流に及ぼすインパクトを分析
- **事業継続計画を更新**
  - 後継計画を策定します
  - 不可欠な機能を決定し、保持すべきシステムと、後日検討すべきシステムを特定する活動を支援

Tomorrow

- **従業員は、在宅勤務に伴うセキュリティ上の影響を検討**
  - リモートワークにかかわる主要リーディングプラクティスを網羅する
  - (例：安全なファイル共有、VPNの使用、パスワードの安全性確保、無線および自宅のネットワークコンフィギュレーションの安全性の確保、他者と共有された生活環境への適合、企業が保有する物理的IT資産の安全性の確保)
- **リモートアクセスの安全性を確保**
  - VPNのガバナンスセキュリティ態勢 (例：パッチステータス、拡張性)、多要素認証の導入及び遠隔で安全にアクセスできる業務範囲を見直します
  - 従業員のために遠隔で業務を実施できるワークスペースを導入し、環境設定が安全に行われていることを確認します

Next Week

- **脅威の検出及び対応能力の強化**
  - 脅威インテリジェンスプログラムがセキュリティイベントのモニタリングと統合されていることを確認
  - 脆弱性の発見と脅威のハンティングを積極的に実施
  - 貴社の従業員や第三者との間で積極的なコミュニケーションを行い、防止に焦点をあてることを確認
  - 24時間365日中断することなく、急なデータの増加にあってもアラート可能なプランを策定
- **セキュリティのモニタリングに関する統制を再考**
  - トラフィックや行動パターンのベースラインを再考
  - 新たなモニタリングルールセット、基準値及びエスカレーション方法を調整、導入
  - シャドーITに対するスキャンを強化

Next Month

- **セキュリティソリューションの拡張性及び持続性を評価するとともに、セキュリティインシデント対応プレイブックを更新し、アクション後のレポートを作成**
  - コールツリー、連絡窓口、IT手順及びシステムの優先付けについて行った変更について記載
  - 特定されたギャップ、得られたインサイト及び改善の余地について記載
- **高リスク領域のセキュリティを強化**
  - セキュリティアーキテクチャを更新し、内部者脅威やサイバーディリジェンスに対応しきれていることを確認
- **企業全体で成熟した危機管理能力を構築し、以下を実現**
  - センシング、モニタリング及びレポーティングの実施により、オペレーションの概要を微調整します
  - 対応に関する経営者の意図や戦略を策定
  - ステークホルダーとの関わり、危機に関するコミュニケーション及びオペレーション上の対応について計画を作成

脅威が高まり続ける今日において、持続的なリスク環境にさらされています

Deloitteのサービス

サイバー融合サービス
- セキュリティモニタリング
- 脅威インテリジェンス
- アタックサーフェイス管理
- 脅威ハンティング
- 情報漏えい防止

意識向上トレーニングの実施
- フィッシング対する意識向上
- トレーニングの実施
- 社内コミュニケーション

インシデント対応 (IR) & 事業継続
- インシデント対応計画とその保持機能
- デジタルフォレンジック、マルウェア、脅威分析、漏えいインパクト分析
- 事業継続、テクニカル・レジリエンスプラン

アイデンティティとデータ保護
- アイデンティティ・ガバナンス
- アクセス管理
- リスクに基づいた認証
- データガバナンス
- データプライバシー (例：GDPRの遵守)

その他の検討事項

セキュリティプログラムおよびリスクトレランスの概要

- *セキュリティシステム及びプロセスの拡張*
- *アタックサーフェイスの拡大*
- *アイデンティティ・ガバナンス管理*
- *新規採用、解雇*
- *リモートワークが不可能な領域*
- *e-コマース推進のためのクラウドセキュリティ*
- *BYOD & 会社貸与以外のデバイスのリスク*
- *複雑に入り組んだ電力、諸設備*
- *従業員の健康のモニタリングに関するプライバシーの問題*

政府・公共機関向け:

- *市民のアイデンティティを盗み、政府の税務機関及び給付金機関からお金をだまし取る新たなサイバースキームのモニタリング*
- *機密活動の安全性を確保する代替方法の検索 (例:モバイル軍事情報施設、決済処理のための遠隔でのアイデンティティ認証、ハードトークン)*
- *学生、教員、職員が取引を実施するにあたっての新手法の導入 (例:安全な検証、リサーチラボのセキュリティ)*

For further clarification on services and next steps to consider, please contact:

Asia Pacific: James Nunn-Price, jamesnunnprice@deloitte.com.au | **Australia:** Ian Blatchford, iblatchford@deloitte.com.au | **China/Hong Kong SAR:** Tonny Xue tonxue@deloitte.com.cn | **India:** Shree Parthasarathy, sparthasarathy@deloitte.com | **Japan:** Kenichi Kimura, kenichi.kimura@tohmatsu.co.jp | **New Zealand:** Anu Nayar anayar@deloitte.co.nz | **South Korea:** Young Soo Seo youngseo@deloitte.com | **Southeast Asia:** Tse Gan Thio, tgthio@deloitte.com | **Taiwan:** Chia-han Wu, chiahwu@deloitte.com.tw

Deloitte Cyberグローバルの翻訳になります。