IIA 会報

現在の最緊急課題に関する内部監査人の視点　2020年2月

（一般社団法人日本内部監査協会　事務局仮訳）

対策の再考：パンデミックとサイバーセキュリティ

新型コロナウィルスの流行は、事業継続と災害対策という、組織体が見落しがちな問題に鋭く焦点を当てている。

現在の流行は範囲と期間がはっきりしないため、従業員の出張計画を見直す組織体から、不安を募らせて株を売る投資家にまで、すでに影響を及ぼしている。サプライチェーン、労働者の生産性、および第三者との関係に影響を及ぼす可能性があるため、経営幹部も内部監査リーダーも大流行が拡大するリスクに留意すべきである。最低限、内部監査リーダーは、パンデミック、災害対策、および事業継続計画に対して更新が必要かを検討して提言する準備をすべきである。

組織体が新型コロナウィルスの事業活動への潜在的な影響を見極める最初の段階にあるとしても、付随的なリスク、すなわちソーシャルエンジニアリング[1]の危機は発生している。サイバー犯罪者は、致死性ウィルスに対する関心の高まりに乗じている。英国を拠点とする消費者向けテクノロジーのニュースとレビューのウェブサイトであるテックレーダー・プロによると、新型コロナウィルスに関する情報を装ったマルウェア入りの電子メールが日本の3つの県で発見された。ハッカーは、新型コロナウィルスの拡散を防ぐための情報とされる電子メールの添付ファイルにマルウェアを隠した。テックレーダー・プロによると、電子メールには別の種類のウィルスが仕込まれていたという。

危機に乗じるサイバー犯罪者は、増え続けそうである。組織体は、フィッシング、プリテキスティング、ベイティングなどのソーシャルエンジニアリングを防ぐための手順と実務を構築しなければならない。

組織体の災害対策を評価するための一般的な質問

以下は、災害対策と事業継続計画を組織体が適切に行っているかを判断するために、内部監査部門が尋ねるべき一般的な質問である。

- 組織体の復旧計画を主なステークホルダーが最後に見直したのはいつか？　組織体の計画を最後にテストしたのはいつで、誰が行ったか？
- 現在の計画は、組織体の施設、従業員、クラウドプロバイダ、サプライヤー、おおび顧客に影響を与える可能性のある自然災害、パンデミック、またはその他の潜在的な混乱要因にどう対処しているか？ 組織体が事業復旧のためのパートナーとの契約を最後に見直したのはいつか？

訳注[1] コンピュータやネットワークの管理者や利用者、また、その関係者などから、話術や盗み聞き、盗み見などの「社会的」な手段によって、パスワードなどの保安上重要な情報を入手すること。

- ベンダー、緊急時対応者、規制当局、保険代理店、およびその他の重要なステークホルダーは、連絡先の変更をどのように通知されているか？
- 組織体は、事業に不可欠な自動化された業務を手動で実施できるか？　必要な様式と手順書は利用可能か？　手動で実施するための適切な人員配置はされているか？
- 組織体は、復旧の順序が適切であることを確認するために、様々な事業プロセスの重要性をどの程度の頻度で検証しているか？　ITは、重要なインフラ構成要素が事業復旧要件に対応できるようになっているかをどのように検証しているか？
- インターネットや携帯電話へのアクセスが遮断されたり制限された場合、どのような事業目標が妨げられたり制約されるか？
- 従業員や仕事上の関係者は、自然災害やパンデミックが発生した場合の対応についてどのような研修を受けているか？
- データセンターやクラウドプロバイダは、「ライツアウト」、すなわち長時間従業員がいない状況でも稼働できるか？
- 事業に不可欠なプロセスや業務のうち、別の場所に移せないものはどれか？　規制上の影響があるのは、事象のタイミングと事象の継続期間のどちらか？

ソーシャルエンジニアリングに対する脆弱性を評価するための一般的な質問

以下は、ソーシャルエンジニアリングに対する組織体の脆弱性を判断するために、内部監査部門が尋ねるべき一般的な質問である。

- ソーシャルエンジニアリングの脅威に対する組織体の実務、方針、研修にはどのようなものがあるか？　これらは従業員にどのように周知徹底されているか？
- ソーシャルエンジニアリングの脅威は、組織体の全階層の従業員に完全に理解され伝達されているか？
- ソーシャルエンジニアリングに対して特に脆弱なのは、どのシステムやプロセスか？　主な業務プロセスのうち影響を受ける可能性があるのはどれか？
- IT部門は、ソーシャルエンジニアリングに対する特定の脆弱性の分野に関して、どのようなテストを行っているか？
- 内部監査部門には、組織体のソーシャルエンジニアリングに対する特定の脆弱性を監査する計画があるか？

出典　内部監査人協会　“IIA Bulletin: Latest on Prepping for Disaster and Business Continuity”
https://global.theiia.org/news/Pages/IIA-Bulletin-Disaster-Preparedness.aspx

IIAの資源

Knowledge Brief

- Strategic Pablic Asset Protection

Practice Guides

- Assessing the Risk Management Process
- Auditing Third-Party Risk Management
- Coordination and Reliance Developing an Assurance Map
- Business Continuity Management
- GTAG: Business Continuity Management
- GTAG: Assessing Cybersecurity Risks

Internal Auditor magazine

- In the Face of Nature

IIAについて

内部監査人協会(IIA)は、内部監査専門職に関する提唱者、教育機関、ならびに基準、ガイダンスおよび各種認定資格の提供者として、世界で最も広く認識されています。1941に設立され、現在、世界170以上の国と地域に200,000 以上の会員がおります。国際本部は、米国フロリダ州レイクメリーにあります。詳しくは、www.theiia.org をご参照ください。

著作権