TLP:AMBER【全分野】

別紙

2024 年 3 月 26 日

内閣官房　内閣サイバーセキュリティセンター
重要インフラグループ

最近のインシデントから得られた教訓について(参考情報)

1. 趣旨

2023 年度第３四半期に重要インフラ所管省庁を通じて内閣サイバーセキュリティセンターに集約されたインシデント情報から得られた教訓を情報提供するものです。なお、説明を簡潔にするため、複雑な状況を簡易に整理しており、一部具体性に欠ける記載がある旨を御承知置きください。また、各重要インフラ事業者等の規模や事業の特性等に応じて、適宜、記載の内容を参考にしてください。

2. インシデントから得られた教訓

システムの更改やメンテナンスに際してのリスクについて、影響範囲などの想定が十分にできていなかったことや、その対応についての管理が不十分であったことなどから、システム障害に至った事例が複数あった。自組織の情報資産の把握、リスクの特定、分析及び評価といった一連のリスクアセスメントと、それを踏まえたリスク対応などリスクマネジメントの継続的な向上が重要である。

(1) システム更改時などにおける適切なリスクアセスメントが必要

システム更改時などにおけるリスクに関して、本番環境への影響を十分に想定できず大規模障害に発展してしまった事例や、一つのシステム障害が複数のサービスに影響を及ぼした事例など、リスクアセスメントが不足していたと考えられる事例が多数あった。リスクアセスメントの継続的な改善と、それを可能にするための組織的な取組が必要。

適切なリスクアセスメントの検討に資する参考 URL

- 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書(NISC)「5 リスクアセスメント」等
  https://www.nisc.go.jp/pdf/policy/infra/rmtebiki202307.pdf
- 制御システムのセキュリティリスク分析ガイド 第２版(IPA)
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

システム障害対策の検討に資する参考 URL

- 重要インフラ分野のシステム障害への対策(IPA)
  https://www.ipa.go.jp/archive/digital/iot-en-ci/system/index.html

(2) 委託先を含み、適切な事前準備やシステム管理が必要

システムメンテナンス時の設定誤りを起因とするシステム障害や、障害発生時における代替手段の実施に際しマニュアルどおりに対応しなかったことにより、サービスの提供に支障が出た事例が引き続きあった。また、アプリケーションのライセンス更新漏れ、システムに使用している機器の不具合情報に係る委託先内における共有漏れなど、情報共有不足によるシステム障害も発生している。

委託先管理の検討に資する参考 URL
- 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書(NISC)「11.2.2 委託先管理」等
  https://www.nisc.go.jp/policy/group/infra/siryou/index.html

(3) 認証情報の適切な管理が必要

システム開発の委託先が発行したアクセスキーが漏えいし悪用された事例や、サポート詐欺やフィッシングメールなどの手法により認証情報が漏えいしリークサイトに公開された事例、漏えいした認証情報により迷惑メールの発信に悪用された事例などがあった。委託先を含め、認証情報の適切な管理が求められる他、漏えいしてしまうことも想定した多要素認証の導入も重要。

サポート詐欺対策の検討に資する参考 URL
- 偽のセキュリティ警告に表示された番号に電話をかけないで(IPA)
  https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211116.html
- サポート詐欺対策(警察庁)
  https://www.npa.go.jp/bureau/cyber/countermeasures/support-fraud.html
- サポート詐欺の手口について（動画解説）(JC3)
  https://www.jc3.or.jp/threats/examples/article-356.html

サポート詐欺に関するセキュリティ教育に資する参考 URL
- 偽セキュリティ警告（サポート詐欺）画面の閉じ方体験サイト(IPA)
  https://www.ipa.go.jp/security/anshin/measures/fakealert.html

メールを用いた攻撃への対策の検討に資する参考 URL
- フィッシング対策(警察庁)
  https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html
- ビジネスメール詐欺の対策について知る(IPA)
  https://www.ipa.go.jp/security/bec/bec_measures.html
- 情報セキュリティ 10 大脅威 2024(IPA)
  「組織第 4 位 標的型攻撃による機密情報の窃取」、「組織第 8 位 ビジネスメール詐欺による金銭被害」
  https://www.ipa.go.jp/security/10threats/10threats2024.html

認証情報等の情報管理の検討に資する参考 URL
- 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書(NISC)「11.4 技術的対策」等
  https://www.nisc.go.jp/pdf/policy/infra/rmtebiki202307.pdf

(4) 組織間の連携・情報共有が必要

SoC などの関係機関と連携し、ウェブサイトへの攻撃を試行する通信を検知・遮断するなどにより、インシデントを未然に防止できた事例があった。また、インシデントの発生を速やかにグループ企業間で共有し、被害拡大防止につなげている事例もあった。グループ企業・関係機関との連携・情報共有は重要であり継続的な取組が必要。

関係機関等との情報共有の検討に資する参考 URL
- 重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書(NISC)「8 運用」等
  https://www.nisc.go.jp/pdf/policy/infra/rmtebiki202307.pdf

(5) 廃止済のドメインについて適切な管理が必要

閉鎖したウェブサイトのドメインが第三者に取得される事例が複数あり、偽サイトが公開されている事例もあった。他方、ウェブサイト閉鎖後、一定期間組織で保持し、保持期間終了後も当該ドメインについてモニタリングし、第三者に取得されている旨を公表するなど適切にリスク管理をしている事例もあった。ドメインの廃止に関しては、顧客への影響を踏まえた適切な対応が求められる。

廃止済みドメインの第三者による取得等への対策の検討に資する参考 URL
- フィッシング対策ガイドライン 2023 年度版(事業者向け)(フィッシング対策協議会)「付録 A Web サイト運営者が考慮すべき要件一覧 要件 20(ドメイン名の登録、利用、廃止にあたっては、自社のブランドとして認識して管理すること」等
  https://www.antiphishing.jp/report/antiphishing_guideline_2023.pdf

3.「2.インシデントから得られた教訓(1)～(5)」の各インシデント概要とその対策・対応の一案

区　分	概　要	対応・対策の一案
(1) リスクアセスメント不足 （システム障害）	**＜事象概要＞** ・システム更改時のリスクに関して、設計等への理解や、本番環境への影響の想定が十分でなく大規模障害に発展 ・リスク分析不足等により一つのシステム障害が、複数の重要なサービスに影響 **＜原因＞** ・システム更改時などのイベントにおけるリスクアセスメント（リスク特定・リスク分析・リスク評価）が不十分	・リスク特定について、定量評価が可能な、気づけるもののみ実施するなど、簡便な方法に留まらず、システム又は組織の目的達成に影響を与えるリスクを様々な場面を想定して体系的に実施することが重要 ※システムの更改等が、本番環境を含む情報資産等に与えるリスクを、作業プロセスのインシデントが組織目的に与える可能性を検討することで、重要なリスクを確実に特定することが重要（必要に応じて、当該システムに係る設計・実装方法の考え方を、開発に携わった者等から情報収集することや、当該システムに関わるサイバー攻撃の動向、自然災害等の当該システムを取り巻く環境の把握も重要） ・リスク分析について、リスクの起こりやすさを算出する際の各要素の特性等の分析も重要。また、情報資産の重要度を分析する際には、他の重要なサービスへの影響度などを十分に考慮することが重要 ・リスク評価について、リスク分析を踏まえ、組織の実情と合わせた形で適切に実施することが重要 ・リスクアセスメントは、事業環境の変化も踏まえ、新たなリスクが発生していないかなど、継続的に改善することが重要 ・インシデントの事後対応としてリスクアセスメントを見直す際には、見落としてしまったインシデントの発生原因に繋がるリスクを追加するのみでは不十分で、なぜ、見落としてしまったのか、リスクの特定・分析・評価の各段階における手法まで立ち返って見直すことが必要（保有しているリスクの中で大きな影響をもたらす事象等を特定できるように、必要に応じてセキュリティ専門家の支援を受けて実施することも重要） ・属人的な知見等に頼るのでなく、組織的な取組（単に過去の知見を伝承するだけでなく、技術進展等に伴う新たな知見も取り入れる）が必要
(2) 設定ミス・オペミス等 （システム障害）	**＜事象概要＞** ・システムメンテナンス時の設定誤りを起因とするシステム障害 ・障害発生時における代替手段の実施に際しマニュアルどおりに対応しなかったことによりサービスの提供に支障 ・アプリケーションのライセンス更新漏れによるシステム障害 ・システムに使用している機器の不具合情報に係る委託先内における共有漏れによるシステム障害 **＜原因＞** ・委託先任せとなり、作業の重要度に応じた委託先への管理が不十分 ・委託先と委託元の認識合わせ及び情報共有が不十分 ・障害発生時の代替手段の実効性の確認不足	・適切な委託先における管理体制の構築及び委託元による管理 ・委託元・委託先、各々で管理すべき項目の整理及び共通認識の構築 ・作業手順書の確認など適切な事前準備がなされるよう、作業の重要度に応じた委託先への適切な管理及び委託先からの作業内容に関する適切な説明 ・重要インフラサービスを継続させるための代替措置の準備及び定期的な訓練などによる IT-BCP の実効性の確保 ・リグレッション試験等の徹底 ・障害発生時の適切な広報の実施（経営層の判断、広報部門との連携構築、SNS 等複数手段の準備）

区　分	概　要	対応・対策の一案
(3) 不正アクセス(認証情報の漏えい) (サイバー攻撃)	**＜事象概要＞** ・システム開発の委託先が発行したアクセスキーが漏えいし悪用 ・サポート詐欺やフィッシングメールなどの手法により認証情報が漏えいし、リークサイトに公開 ・漏えいした認証情報により迷惑メールの発信に悪用 **＜原因＞** ・認証情報を守るための対策の不備や職員のリテラシー不足	・委託先での認証情報の管理状況に関する委託元による適切な管理 ・様々な不正アクセスを前提とした多層防御を備えたシステム設計 ・多要素認証の導入など認証の方法の強化 ・イニシャルアクセスから横展開を防ぐための適切なセグメント分けとアクセス制御 ・認証情報が漏洩した場合などの不正ログインに備えた、認証情報のソルト付きハッシュ化などの対応 ・定期的な研修受講など継続的な職員のリテラシー向上
(4) 組織間の連携･情報共有 (サイバー攻撃)	**＜事象概要＞** ・SoCなどの関係機関と連携し、ウェブサイトへの攻撃を試行する通信を検知・遮断するなどにより、インシデントを未然に防止 ・インシデントの発生を速やかにグループ企業間で共有し、被害拡大防止につなげた	・ヒヤリハットの共有など、グループ企業間での連携 ・サイバーセキュリティ関連の組織との連携 ・インシデント発生時の連携が必要な機関等への連絡先の確認
(5) 廃止済のドメインの悪用 (システム障害)	**＜事象概要＞** ・閉鎖したウェブサイトのドメインが第三者に取得され、偽サイトが公開 ・ウェブサイト閉鎖後、一定期間組織で保持し、保持期間終了後も当該ドメインについてモニタリングし、第三者に取得されている旨を公表するなど適切にリスク管理を実施	・ドメインを新たに取得することが本当に必要か、必要であればその後の管理をどうしていくのか、事前の十分な検討 ・一度取得したドメインを手放すことにはセキュリティ上の懸念が伴うことに十分留意 ・ドメイン名の登録、利用、廃止に当たっては、自組織のブランドとして認識して管理していくことが重要 ・管理の仕組みがあっても、組織全体で徹底されなければ防ぐことはできず、レピュテーションリスク（信用低下）にもつながる恐れがあることに留意 ・委託先に管理を任せているものについても、漏れが無いようにする必要 ・セキュリティ部門や管理部門だけではなく、各業務部門まで徹底する必要 ・定期的にドメインの管理状況を確認するなど適切な管理を行い、同ドメイン　上で提供するサービスの重要度等に応じて、不使用となった後も一定期間登録保持することを推奨