TLP:AMBER【全分野】

別紙

2023 年 12 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２四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

海外グループ会社経由の不正アクセスを許し情報漏えいに至ってしまった事例の他、ランサムウェア感染や DDoS 攻撃などのサイバー攻撃の被害の報告もあった。委託先を含め多層防御の必要がある。また、システム障害では、引き続き、設定ミス、手順ミスなどを起因とするものが複数寄せられており、適切な事前準備が求められる。

(1) ネットワークの適切なセグメント分けとアクセス制御、監視が必要

海外グループ会社を経由した不正アクセスによる情報漏えいが発生した事例があった。一方で、侵害にあったネットワークと基幹系ネットワークが分離されていたため、主要なサービスへの影響が限定的であった事例があった。グループ企業間でセキュリティに関する運用の水準が異なる場合があることも踏まえ、組織内でのマルウェアの感染拡大を防ぐための措置が必要。

また、認証情報が漏えいした場合も想定し、事後の不正アクセスを防ぐために多要素認証などの認証強化が必要。

グループ会社や委託先の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)「6 リスク対応」等
  https://www.nisc.go.jp/policy/group/infra/siryou/index.html
- サイバーセキュリティ経営ガイドラインと支援ツール(経済産業省)「付録 F サイバーセキュリティ体制構築・人材確保の手引き第 2.0 版『2 サイバーセキュリティリスク管理体制の構築』」等
  https://www.meti.go.jp/policy/netsecurity/mng_guide.html
  https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf
- 情報セキュリティ 10 大脅威 2023(IPA)「組織第 2 位 サプライチェーンの弱点を悪用した攻撃」
  https://www.ipa.go.jp/security/10threats/10threats2023.html
  https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf

アクセス制御や多要素認証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/policy/group/infra/siryou/index.html

(2) 委託先を含み、適切なネットワーク接続部分の資産管理及び脆弱性管理が必要

閉鎖的なネットワーク環境での運用を前提としていたシステムについて、委託先がインターネットに接続したことによりランサムウェアに感染した事例があった。また、VPN機器に関して、適切なアクセス制限をしておらず、かつ、既知の脆弱性への修正プログラムが未適用であったことにより、ランサムウェアが侵入したと考えられる事例があった。

資産管理や脆弱性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 対策項目」等
  https://www.nisc.go.jp/policy/group/infra/siryou/index.html
- 脆弱性対策情報(IPA)
  https://www.ipa.go.jp/security/vuln/index.html

ランサムウェア攻撃への対策の検討に資する参考 URL
- ストップ！ ランサムウェア ランサムウェア特設ページ(NISC)
  https://www.nisc.go.jp/tokusetsu/stopransomware/index.html

(3) 攻撃を想定したシステム設計と障害発生時における適切な広報の実施が必要

DDoS 攻撃とみられる大量のアクセスを受けた事例が複数あった。サービスの重要度に応じた DDoS 攻撃への耐性向上のための対策に加え、障害発生時における代替手段の用意と適切な広報など事前の備えが必要。

DDoS 攻撃への対策の検討に資する参考 URL
- DDoS 攻撃への対策について(警察庁、NISC)
  https://www.nisc.go.jp/pdf/press/20230501NISC_press.pdf
  https://www.nisc.go.jp/pdf/press/20230501NISC_gaiyou.pdf

閲覧障害に係る公表タイミングの検討に資する参考 URL
- サイバー攻撃被害に係る情報の共有・公表ガイダンス(サイバー攻撃被害に係る情報の共有･公表ガイダンス検討会)
  https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

適切な公表内容の検討に資する参考 URL
- 注意喚起や情報共有活動における受信者側の「コスト」の問題について(JPCERT/CC)「補稿：DDoS 攻撃の「被害」と「コスト」」
  https://blogs.jpcert.or.jp/ja/2023/05/cost-and-effectiveness-of-alerts.html#6

(4) ウェブサイト作成のためのソフトウェアの適切な管理が必要

ウェブサイトに無関係な海外のサイトへのリンクが設定された事例や、既知の脆弱性への修正プログラムが未適用だったことを原因としたウェブサイトの改ざん事例があった。作成したいウェブサイトに応じたソフトウェアの選択と、機能拡張のために追加したソフトウェアを含めた適切な脆弱性管理が必要。また、復旧に長期間要した事例もあり、ウェブサイトの停止や再構築の手順を確立しておくなどの事前準備が必要。

ウェブサイトのセキュリティ実装の検討に資する参考 URL
- 安全なウェブサイトの作り方(IPA)
  https://www.ipa.go.jp/security/vuln/websecurity/about.html
- ウェブサイト改ざん対策(警察庁)
  https://www.npa.go.jp/bureau/cyber/countermeasures/hacked-website.html

(5) 作業手順書の確認など適切な事前準備が必要

システムメンテナンスの際の設定ミス、データの誤削除といった作業ミスによるシステム障害や、テスト環境から本番環境へ移行する際の確認不足によるウェブサイトの誤表示など、適切な事前準備により防げるインシデントが複数あった。

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)「11.1.3 運用管理」等
  https://www.nisc.go.jp/policy/group/infra/siryou/index.html

(6) リスクアセスメントを踏まえた IT-BCP が必要

機器の故障に起因したシステム障害が多数あった。故障自体を防ぐことは困難であることから、提供するサービスの重要度も踏まえた冗長化等を検討することが必要。また、冗長化していたはずのシステムが適切に機能せず、サービスの提供に影響が出た事例も複数あった。機器故障が起きた場合を想定した影響の検討や、それを踏まえた対応手順の確立などの準備が必要。

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」「6 リスク対応」「11.2.2 委託先管理」等
  https://www.nisc.go.jp/policy/group/infra/siryou/index.html
- 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

システムの冗長構成等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

3. 「2.インシデントから得られた教訓(1)～(6)」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) 海外グループ会社経由の攻撃等（サイバー攻撃）	**＜事象概要＞** ・グループ会社が利用する VPN 機器への不正アクセスから、ネットワーク経由で他のグループ会社のディレクトリーサーバが侵害され情報が漏えい ・侵害にあったネットワークと基幹系ネットワークが分離されていた事例では、主要なサービスに関わるシステムへの感染拡大は防御 **＜原因＞** ・海外グループ会社経由の不正アクセス	・組織全体におけるサイバーセキュリティ確保、例えば、グループ企業間における監視体制、セキュリティ運用水準の整合 ・適切なセグメント分けと、適切なアクセス制御 ・データベース内のパスワードのハッシュ化 ・今後、漏えい情報が不正アクセスに利用される可能性を踏まえ、多要素認証の実装など認証の強化
(2) ランサムウェア攻撃（サイバー攻撃）	**＜事象概要＞** ・閉鎖的なネットワーク環境において、委託先がインターネットに接続し、外部からの不正アクセスを受け、サーバに保存していたファイルが暗号化 ・保守作業用の VPN 通じてサーバがランサムウェアに感染し、重要なサービスが停止し大規模なインシデントに発展 **＜原因＞** ・外部接続部分の資産管理、既知の脆弱性への修正プログラムの未適用 ・VPN のアクセス制限の設定不備	・リスクアセスメントを踏まえ適切な委託先の管理 ・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 ・VPN などの特に外部接続部分に関する資産管理（脆弱性管理を含む）の重要性の再認識 ・多要素認証の利用/強制・不要なアカウントの削除・適切なアクセス制限 ・適切な取得頻度・対象及び保存期間によるシステムログを含むバックアップの実施（ネットワークから切り離し、データの変更不可とするなど）及び復旧手順の確認など IT-BCP の点検

区　分	概　要	対応・対策の一案
(3) DDoS 等大量アクセスによる攻撃（サイバー攻撃）	＜事象概要＞ ・ハクティビストが攻撃を示唆する内容をSNS に投稿し、同時期に DDoS 攻撃が発生 ・公式ウェブサイトのお問い合わせフォームに大量の投稿があり、データベースとの連携に不具合が発生し、問い合わせデータが閲覧できない状況となった ＜原因＞ ・DDoS 攻撃又は大量アクセス ・特定の者による大量の投稿	・リスクアセスメントを踏まえた上で、DDoS プロテクション、WAF、CDN の導入（※キャッシュ無効化攻撃の対策にも留意） ・リスクアセスメントを踏まえた上で、ロードバランサの使用の検討（※帯域や機器の処理能力の検討にも留意、この点はウェブサーバ、FW 等も同様の留意が必要） ・権威 DNS サーバとキャッシュ DNS サーバの分離や、オープンリゾルバ対策の実施など、攻撃の踏み台にならないための対策の実施 ・重要な情報を提供しているウェブサイトの代替手段の用意 ・ウェブサイトがダウンした際に Sorry ページが表示されるように設定 ・業務への影響を踏まえつつ FW において特定の IP アドレスからの通信を遮断 ・同一 IP アドレスからのアクセス回数制限の設定 ・ハクティビストの目的をよく理解した上での適切な公表
(4) ウェブサイトの改ざん（サイバー攻撃）	＜事象概要＞ ・公式ウェブサイトに、無関係な海外のショッピングサイトへのリンクが設定 ・悪用が確認されている既知の脆弱性を原因とし、ブログ記事が改ざん ・復旧に長時間要した事例もあり ＜原因＞ ・既知の脆弱性の未対応	・ウェブサイトの停止や再構築の手順の確立 ・作成したいウェブサイトに応じたソフトウェアの選択、使わない拡張機能の削除 ・機能拡張のために追加したソフトウェアを含めた脆弱性の情報収集と、脆弱性への適切な処置 ・既知の脆弱性に対する修正プログラムの適用
(5) 管理不足･オペミス等（システム障害）	＜事象概要＞ ・データ移行作業時にデータの一部を誤って削除したことにより、基幹サービスが停止 ・委託先による設定変更作業におけるミス（再起動実施漏れ等）に起因して重要インフラサービスに影響 ・作業対象外の設定ファイルを誤って変更し重要インフラサービスに影響 ・アクセス権の設定誤りにより権限のない者からの閲覧が可能な状態 ・変更作業時の設定項目に不備があったことによりウェブサイトが閲覧不可 ・テスト用の申請書を本番用に切り替えることを失念し、利用者が申請できなかった ＜原因＞ ・データの誤削除、設定誤り、設定手順の不備 ・作業後の再起動実施及び動作確認不足 ・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	・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が必要 ・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 ・リグレッション試験の徹底 ・障害発生時の迅速な復旧のための作業手順の確認 ・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）
(6) リスクの洗い出し不足等（システム障害）	＜事象概要＞ ・機器が故障した際、 代替機器に切り替わらずシステム障害となり、サービスの提供に影響 ＜原因＞ ・IT-BCP における実効性の確認不足	・機器故障が発生した際の冗長化等の検討 ・冗長化のために設置した代替機器が正常に作動するかの定期的な確認 ・定期的な訓練などによる IT-BCP の実効性の確保