

- 作成/収集 – データは従業員や自動化されたシステムによって生成されることもありますが、顧客やサプライヤーから送信されることもあります。この段階においては、データを分類してタグ付けする必要があります。
- 配布/使用 – 認証済みアカウントの所有者やサードパーティによる認可された使用のために、データを必要な人だけに利用可能にします。
- 保持 – データを使用する期間が過ぎたあとも、規制上の理由でデータをアーカイブに保管しなければならないことがあります。
- 破棄 – 使用または保持がこれ以上必要なくなったとき、データ資産を保存しているメディアをサニタイズして残余データを消去する必要があります。



どの組織においても、情報管理は膨大なタスクです。大半のスキームは構造化されたデータ（つまり、ディレクトリ階層の中で保存され、管理用アクセス制御の対象となる情報）に焦点を当てています。構造化されていないデータ（電子メール、チャットセッション、電話による通話など）の管理と分類はさらに骨の折れるタスクですが、この問題への対処を目的としたソフトウェアソリューションが用意されています。

データに関する役割と責任

データガバナンスポリシーとは、ライフサイクルの各段階でデータを保護するために適用されるセキュリティ管理を記述するものです。ライフサイクルにおける情報資産の監視と管理には、組織的なガバナンスの重要な役割があります。

- データオーナー** – 情報資産の機密性、完全性、可用性を維持する上で最終的な責任を負う上級（エグゼクティブ）の役割です。所有者はアセットのラベリング（アクセス権を有するのは誰かを決定する、資産の重要性と機密性を決定する、など）の責任と、その資産が適切な管理（アクセス制御、バックアップ、保持など）によって保護されていることを保証する責任を負っています。また、所有者は通常、スチュワードとカストディアンを選定して彼らの行動を指示し、十分な管理に向けて予算とリソースの割り当てを行います。
- データスチュワード** – この役割は主に、データの品質の責任を負っています。この役割には、適切なメタデータでデータをラベリングして識別し、適用される法律や規制に準拠した形式と値でそのデータを収集・保存するというタスクが含まれます。
- データカストディアン** – この役割は、データ資産が保存されているシステムの管理を扱います。ここには、アクセス制御、暗号化、バックアップ/リカバリーの手段を実施する責任が含まれます。
- データ保護責任者(DPO)** – この役割は、会社が管理している、個人を特定できる情報（Personally Identifiable Information、PII）資産のすべてを監督する責任を負っています。データ保護責任者は、PIIの処理、開示、保持が、法律上・規制上のフレームワークに準拠していることを保証します。

個人のプライバシーを保護する法令と規制に関して言えば、次の2つの制度上の役割が重要になります。

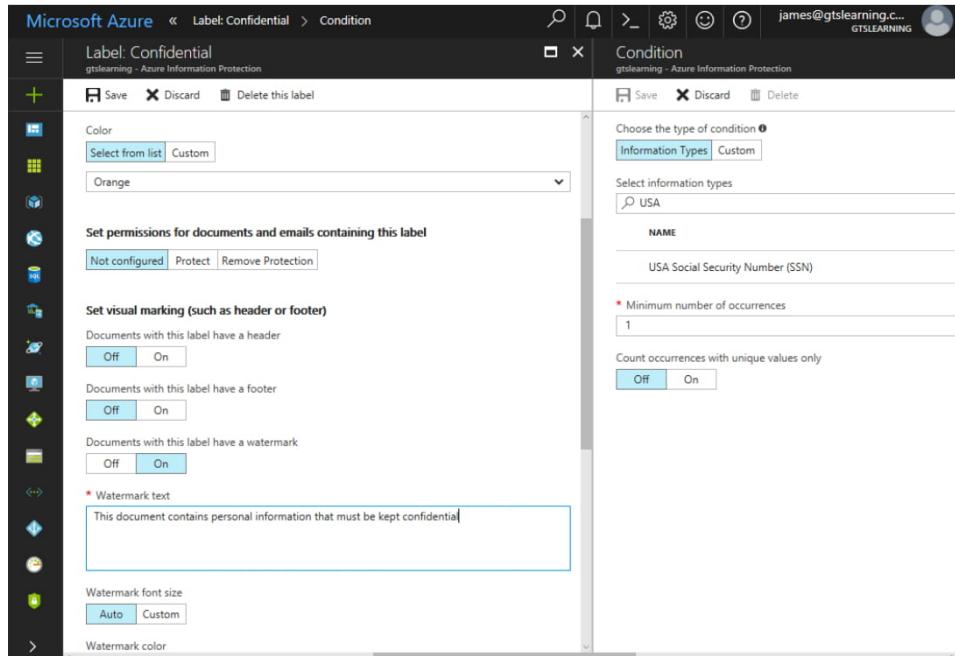
- データコントローラー** – データが保存・収集・使用される理由と方法を判断し、それらの目的と手段が合法であることを保証する責任を負うエンティティです。プライバシーの侵害についてではデータコントローラーに最終的な責任があり、その責任を移転することは許されていません。
- データプロセッサ** – データコントローラーによって任命されるエンティティで、収集・保存・分析の各技術的タスクを支援します。収集ないし処理について、データプロセッサはデータコントローラーの指示に従います。

データコントローラーとデータプロセッサは多くの場合個人の役割ではなく、組織的な役割になります。例えば、Widget.fooが自身のクラウド上でWebストアを運営するために個人データを収集する場合、それはデータコントローラーでありデータプロセッサです。Widget.fooが集約されたデータをGrommet.fooに渡し、AI支援型クラウド上のさまざまな顧客セグメントについて採算性を分析するよう依頼したとすると、Grommet.fooはWidget.fooの指示の下で行動するデータプロセッサになります。Grommet.fooとWidget.fooの社内において、データオーナーは、データコントローラーとデータプロセッサの職務が合法的に行われることに個人的な責任を負う場合があります。

データ分類

データ分類とタイプ付けのスキーマによってデータ資産がタグ付けされ、情報ライフサイクルを通じて管理できるようになります。データ分類スキーマとは、それぞれのデータアセットに1つ以上のタグまたはラベルを適用する、決定木のことです。多くのデータ分類スキーマは、必要とされる機密性の度合いが基になっています。

- パブリック（未分類） – データの閲覧に関する制限はありません。パブリック情報は、開示されても組織にリスクをもたらしませんが、改ざんされたり利用不可になればリスクとなる情報です。
- 機密（秘密） – この情報は機密度が高く、所有者の組織内の承認された人物だけが閲覧でき、またNDAの下で、信頼できるサードパーティの閲覧が許可される場合もあります。
- 極秘（最高機密） – この情報は非常に価値が高く、盗用のリスクは一切許されません。閲覧できる人物は非常に限られています。



Microsoft Azure Information Protectionを使用して、ドキュメントの自動ラベリングとウォーターマーキングのポリシーを定義する。(スクリーンショットはMicrosoftからの許可を得て使用。)

分類スキーマの別のタイプとして、情報アセットの種類を特定するものがあります。

- プロプライエタリー **プロプライエタリ情報ないし知的財産(IP)**は、会社によって作成され、所有されている情報であり、通常はその会社が製造している製品や実施しているサービスに関するものです。IPは会社の競争相手にとって明白なターゲットであり、一部の業界（防衛産業やエネルギー業界）のIPは外国政府に狙われています。またIPは偽造されることもあります（映画、音楽、書籍など）。
- プライベート/個人データ 個人の身元に関連する情報です。
- 要配慮（センシティブ） – このラベルは通常、個人データのコンテキストで用いられます。個人のプライバシーに関するセンシティブな情報は、公開されるとその人に害を及ぼす恐れがあり、また社内の手順によって参照されると、その人に関する決定が偏見を基に行われる可能性もあります。EUの一般データ保護規則(GDPR)で定義されている通り、センシティブな個人データには宗教、政治的意見、労働組合への加入状況、性別、性的指向、人種または民族、遺伝子データ、医療情報が含まれます(ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en)。

データタイプ

タイプスキーマは、単純な分類よりも詳細なラベルをデータに付与します。

個人を特定できる情報(PII)

個人を特定できる情報 (Personally Identifiable Information、PII) は、個人を特定する、その個人に連絡する、またはその個人の位置を特定する目的で使用できるデータを指します。米国の社会保障番号(SSN)はPIIの好例です。この他にも、氏名、生年月日、電子メールアドレス、電話番号、住所、生体認証データなどが含まれます。SSNなど一部の情報は唯一のものですが、組み合わせることで個人を一意に特定するその他の情報もあります（氏名と、誕生日や住所を組み合わせるなど）。

場合によってPIIとみなされる可能性のある情報もあります。例えば、静的IPアドレスを使用してWebを開覧した場合、そのIPアドレスはPIIとなります。ISPによって動的に割り当てられたアドレスはPIIとはみなされない可能性があります。PIIは、パスワードをリセットする際や電話での本人確認などで頻繁に使用されています。PIIはまた、「好きな色/ペット/映画は何ですか」といった本人確認の質問に対する回答としても定義される場合があります。個人データの収集や保存を管理するための規定を導入する際には、このような複雑性についても考慮する必要があります。

顧客データ

顧客データは組織情報である場合もありますが、セールスやテクニカルサポートの連絡先など、その顧客の従業員に関する個人情報である場合もあります。この個人的な顧客データは、PIIとして扱う必要があります。組織情報は、その保存と処理に契約上の義務を課す、秘密保持契約(NDA)の下で共有されることがあります。

医療情報

個人医療情報(PHI)または保護されるべき医療情報とは、医療と保険の記録、さらには関連する病院とラボでの検査結果を指します。PHIは特定の個人と関連付けられたり、匿名化または非特定化されたデータセットとして分析や研究目的で使用されたりする場合があります。匿名化されたデータセットでは、個人を特定できる部分が完全に排除されています。また非特定化されたデータセットには、データプロバイダーが対象者の情報を再構築できるようにするコードが含まれています。

PHIは、高値で闇取引されるため、格好のターゲットとなります。犯罪者は、保険詐欺や脅迫などの目的でデータを悪用しようとします。PHIデータは極めてセンシティブであり、それが失われると永遠に影響が残ります。これは、クレジットカード番号や銀行口座番号とは違い、変更することができません。そのため、PHIデータの侵害によって引き起こされる風評被害は甚大です。

財務情報

財務情報とは、銀行口座や証券口座に関するデータ、さらには給与や税金還付などの情報を指します。クレジットカード情報は、カード番号、有効期限、3桁のセキュリティコード(CVV)から成っています。またカードはPINと紐付けられていますが、これを販売業者に送信したり、販売業者に扱わせたりしてはいけません。またカードの悪用には、カードを登録している所有者の氏名と住所も必要となります。ペイメントカード業界データセキュリティ基準(PCI DSS)は、この情報の安全な取り扱いと保管を定義しています(pcisecuritystandards.org/pci_security)。

政府のデータ

政府機関の内部には、データの収集と処理に関する複雑な要求事項があります。米国では、市民や納税者に関するデータの収集と処理を行う機関には、連邦法によって特定の要求事項が課されています。このデータは、セキュリティとプライバシーを確保する厳格な同意の下で、分析目的で企業と共有されることがあります。

プライバシー通知とデータ保持

データオーナーは、個人データの収集と処理に影響を及ぼす法律上・規制上の問題を意識しなければなりません。EUの一般データ保護規則(GDPR)などによって立法化されたプライバシー権では、十分な説明を行い同意を得ること（インフォームドコンセント）なく、個人データの収集、処理、あるいは保持を行ってはならないことになっています。GDPR (ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr)はデータの対象者に対し、同意を取り下げ、自分に関するデータを検査、修正、消去する権利を与えています。

プライバシー通知

インフォームドコンセントとは、データは言明された目的のためにのみ収集・処理されなければならず、その目的は法律用語ではなく簡明な言葉でユーザーにはっきり説明されなければならない、という意味です。この同意ステートメントをプライバシー通知と呼びます。同意ステートメントの下で収集されたデータを、その他の目的のために使用することはできません。例えば、アカウントIDとして使用するために電子メールアドレスを収集した場合、そのメールアドレス宛てにマーケティングメッセージを送るといったことは、その個別の目的のために別途同意を得ていない限り禁じられています。目的の制限も、あなたがサードパーティにデータを転送することを制限します。

インパクトアセスメント

同意ステートメントを追跡し、与えられた同意に従う形でデータが使用されることには、管理面における重要な管理タスクとなります。大量の個人データを処理する組織では、個人データレコードのタグ付けと相互参照を行なう技術的なツールが必要となります。データ保護インパクトアセスメントは、ビジネスワークフローやプロジェクトのコンテキストにおいて個人データを収集・処理することのリスクを突き止め、それらのリスクを軽減するメカニズムを特定することを目的としたプロセスです。

データ保持

データ保持とは、ビジネスポリシーや該当する法律と規制を遵守するために、情報資産のバックアップとアーカイブを行うことを指します。コンプライアンスとeディスクバリーリの要件を満たすため、ある種のデータを一定期間にわたって保持するよう、企業が法律によって拘束されていることもあります。この種の要件は特に財務データやセキュリティのログデータに影響を及ぼします。それとは逆に、プライバシー関連法令における保存の制限の原則により、必要以上に長く個人データを保持できないこともあります。これにより、バックアップとアーカイブにPIIを含めることが困難になる場合もあります。

データ主権と地理的考慮事項

データプライバシーをどの程度尊重しているかは州や国によってさまざまですし、特定のデータの性質やコンテンツを承認していない国もあります。また、暗号化などのセキュリティ対策に懐疑的な国もあります。データが自国以外の地域で保存または送信される場合、あるいは他の州や国の市民からデータを収集する場合、予測どおりに、または希望どおりにデータを「所有」できるとは限りません。

データ主権

データ主権とは、ある管轄区域において、その管轄区域内に物理的に存在していないシステム上でデータの処理と保管が行われるのを防止する、または制限することを指します。データ主権によって、クラウドサービスにおいて地域を特定したストレージ施設を使用するなど、ある種の譲歩を求められることもあります。

一例を挙げると、GDPRの保護規則は、EUまたはEEA（欧州経済領域）の境界内にいる、すべてのEU市民に拡張されます。データ主体は転送を許可することに同意できますが、同意を拒否する有意義な選択肢がなければなりません。転送先の管轄区域がGDPRに匹敵するレベルでの十分なプライバシー規制を敷いていない場合、契約上の安全措置によってGDPRの権利をそのデータ主体に拡大させる必要があります。米国では、[プライバシーシールドスキーム \(privacyshield.gov/US-Businesses\)](#)の下、自社の提供する保護が十分であることを、企業が自己証明しています。

地理的考慮事項

地理的なアクセス要件は、次に挙げる2つの異なるシナリオに分類されます。

- データ主権の問題を軽減すべく、ストレージの場所を選ばなければならない場合がある。大半のクラウドプロバイダーは、処理とストレージを行うデータセンターを選択できるようにしており、同意を得ることなく、情報が特定のプライバシー管轄区域から違法に転送されることがないようにしています。
- 複数の地理的位置からのアクセスを必要とする従業員。クラウド型のファイルおよびデータベースサービスは、制約型のアクセス制御を適用することで、アクセスを承認する前に、そのユーザーの地理的位置を検証することができます。

プライバシーの侵害とデータ侵害

データ侵害は、許可されることなく情報が読み取られたり、改変されたりした際に発生します。この場合の「読み取り」とは、個人に見られることを意味する場合もあれば、ネットワークやストレージメディアに転送されることを意味する場合もあります。データ侵害があらゆるタイプのデータの喪失を意味する一方、プライバシーの侵害は、特に個人データやセンシティブなデータが喪失したり開示されたりすることを指します。

組織的影響

データやプライバシーの侵害により、次のような深刻な組織的影響が発生することもあります。

- 信用低下 – データの侵害によって悪い評判が広まります。自社の情報アセットを保護できない会社が顧客に信頼される機会は少なくなるでしょう。
- 個人情報の窃盗 – 侵害されたデータが個人情報の窃盗に悪用された場合、そのデータの対象者は損害賠償を求めて訴訟を起こせることができます。
- 罰金 – 法律により、罰金を課す権限が規制機関に与えられている場合もあります。これは決まった額のこともあります、最悪の場合、売上高の一定割合であることもあります。

- 知的財産(IP)の盗難 – 企業データの喪失によって利益が失われることもあります。これは通常、著作権のあるもの（未公開の映画や楽曲など）が侵害された場合に起こります。特許、デザイン、商業上の秘密などが競争相手や国家アカターの手に渡った場合に商業上の損失が発生することもあり、法的措置を通じてIP盗難による損害を回復することが難しい海外市場において、特にそれが当てはまります。

侵害の通知

さまざまなタイプの侵害に関する必要事項が、法律や規制の中で定められています。こうした必要事項は、誰に通知しなければならないかを指示しています。データ侵害とは、情報の喪失や盗難、偶発的な情報開示、または情報の損失や損害を意味します。有効な手順が実施されていない場合、偶発的な侵害によるかなりのリスクがあることに注意してください。データベース管理者が、編集されていないクレジットカード番号を表示させるクエリを実行できたとすると、そのクエリがデータベースサーバーの外に出るかどうかに関わらず、それはデータ侵害となります。

エスカレーション

技術スタッフによって侵害が検知されることもあり、そのイベントが重大なものでないと判断された場合、システムを修復してそれ以上の通知を行わないという誘惑に駆られることがあります。これにより、会社が法的な危機に晒される可能性が生じます。個人データのすべての侵害と、IPの大半の侵害は、上位の意志決定者へエスカレーションし、法律と規制による影響を正しく検討しなければなりません。

公示と開示

通知は規制機関だけでなく、法執行機関や、その侵害によって影響を受けた個人やサードパーティ企業に対しても行わなければならず、マスコミやソーシャルメディアを通じて公に行う必要があります。一例を挙げると、[医療保険の相互運用性と説明責任に関する法律\(HIPAA\)](#)は条文の中で報告要件を定めており、影響を受けた個人、米国保健福祉省長官、また500名以上が影響を受けた場合はメディアに侵害を通知するよう求めています([hhs.gov/hipaa/professionals/breach-notification/index.html](https://www.hhs.gov/hipaa/professionals/breach-notification/index.html))。この要件はまた、これらの当事者に通知を行うべき時期も定めています。例えばGDPRの下では、個人データの侵害を認識してから72時間以内に通知を行わなければなりません(csoonline.com/article/3383244/how-to-report-a-data-breach-under-gdpr.html)。また、開示の要件、もしくは影響を受けた各当事者に提供すべき情報も、規則の中で定められています。多くの場合、どのような情報が侵害されたかの説明、主たる連絡先の情報、侵害から生じると思われる影響、その侵害を軽減するためにとられる手段が、開示内容に含まれることになります。

米国の大半の連邦法や州法は業界特有の規制に焦点を当てがちで、個人データの定義は狭く、データ主体に対する権利や保護も少ないのでですが、GDPRはそれより強力な保護措置を提供しています。しかしカリフォルニア州顧客プライバシー法(CCPA)が成立したことにより、米国国内法の様相は変わっています(csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html)。

データ共有と契約書のプライバシー条項

誰もが基本的にあらゆるサービスや活動をサードパーティに委託できますが、こうしたサービスや活動の法的責任は委託できないことを覚えておいてください。こうしたサードパーティが行うサービスや活動に最終的な責任を負うのはあなたになります。サードパーティがあなたのデータやシステムにアクセスできる場合、サードパーティの組織のセキュリティ違反（不正なデータ共有など）は事実上あなたの違反になります。セキュリティリスクの認識、義務の共有、契約上の責任の問題は、正式な法的契約書に記載することができます。一般的な契約書の種類は次のとおりです。

- サービスレベル同意書 (Service Level Agreement : SLA) — サービスが提供される詳細な条件を定めた契約上の合意です。セキュリティアクセス制御とリスク評価の条項に加え、機密データやプライベートなデータの処理に関する要件を含むことがあります。
- 相互接続セキュリティ協定(ISA)** — ISAはNISTのSP800-47「相互接続情報テクノロジーシステム」によって定義されているものです(csrc.nist.gov/publications/detail/sp/800-47/final)。ITシステムをサードパーティに相互接続する連邦政府機関は、ISAを作成してその関係を管理する必要があります。ISAは、セキュリティリスクの認識プロセスを設定し、政府機関とサプライヤーにセキュリティ制御の実装に責任を持たせるものです。
- 秘密保持契約書 (NonDisclosure Agreement : NDA) — 情報資産の保護に関する法的根拠です。NDAは企業と従業員、企業と請負業者、企業と企業の間で使用されます。従業員または請負業者がこの契約を違反し、当該の情報を共有する場合、法的措置が取られる場合があります。NDAは、従業員や請負業者が、雇用者の信頼を破ることを阻止するため有用です。
- データの共有と使用に関する同意書 — GDPRやHIPAAといったプライバシー規則の下では、個人データは特定の目的に限って収集することができます。データセットは個人データを除去するための疑似匿名化または匿名化の対象になる場合がありますが、その他のデータソースと組み合わされた場合、再特定のリスクがあります。データの共有と使用に関する同意書は、そのリスクを防ぐ法的手段です。その中で、データセットの分析方法に関する条件が定められ、再特定テクニックの使用が禁じられることになります。

レビュー アク ティビティ： プライバシーとデータセンシティビティの概念

次の質問にお答えください。

1. データスチュワードの役割とデータカストディアンの役割の違いは何ですか？
2. データラベリングプロジェクトにおいては、どういった範囲の情報分類を実行できますか？
3. PIIとは何を意味しますか？
4. 世界的なユーザーを持つ趣味サイトのメンバーシップのデータベースについて、あなたはそれに関するセキュリティ上・プライバシー上の問題をレビューしています。このサイトは現在口座情報を収集しており、それ以上の情報は集めていません。データ保護規則を遵守するには、何を追加すべきですか？
5. ある組織が起こしたデータ侵害とプライバシー侵害について、あなたはその影響を顧客に説明する資料を準備しています。そして信用低下、個人情報の盗難、IPの盗難に関するセクションを書き終えました。CompTIA Security+の目的に従えば、他にどのようなセクションを追加すべきですか？

トピック 16B

プライバシーとデータ保護の制御を説明する



対象試験範囲

- 2.1 エンタープライズ環境におけるセキュリティコンセプトの重要性を説明することができます。
- 3.2 与えられたシナリオに基づいて、ホストまたはアプリケーションのセキュリティソリューションを実装することができます。
- 5.5 セキュリティに関するプライバシーおよび機密データの概念を説明することができます。

ポリシーと手順は効果的なデータガバナンスに不可欠ですが、技術的制御によってそれらをサポートすることもできます。あなたはセキュリティのプロフェッショナルとして、データ損失防止(DLP)システムや、プライバシー強化データベース制御の能力に加え、データがホスト上、メールシステム内、またはクラウド内などどこにあろうとも、それらの能力をどう使えばデータを保護できるかを認識する必要があります。

データ保護

信頼できるOSの内部に保存されているデータは認可メカニズムの対象にすることができ、そこでは何らかのタイプのACLを使用してOSがアクセスを仲介します。しかし、信頼できるOSの存在が常に保証されているわけではありません。その他のデータ保護メカニズム、特に暗号化を使用することで、認可メカニズムが無効にされるリスクを軽減できます。データ資産を保護するために暗号システムをデプロイ（展開）する際は、情報が傍受され得るあらゆる方法を検討しなければなりません。これはディスクに保存されるデータファイルというシンプルな概念を超えて検討する必要があることを意味します。データは、次に挙げる3つの状態のどれかにあるものとして説明することができます。

- **保存中データ** — これはデータがある種の永続ストレージメディアに保存されている状態です。保存状態にあるデータの例として、データベースに保存されている財務情報、アーカイブされたオーディオビジュアルメディア、運用ポリシーやその他の管理文書、システム構成データなどがあります。通常この状態のデータは、完全なディスクの暗号化や、**データベース暗号化**、ファイルやフォルダーレベルの暗号化といった技術を使って暗号化することができます。またアクセス許可、つまりアクセス制御リスト(ACL)を適用することで、認可されたユーザのみがそのデータの読み取りと修正を行えるようにすることも可能です。データへのアクセスが信頼できるOSによって完全に仲介される場合にのみ、ACLを適用することができます。
- **転送中のデータ**（または**移動中のデータ**）— これはネットワーク経由で送信されているデータの状態です。転送中のデータの例としては、Webサイトのトラフィック、リモートアクセストラフィック、クラウドリポジトリ間で同期中のデータなどがあります。この状態において、データはTLSやIPSecといった転送暗号化プロトコルによって保護することができます。



暗号化鍵をより長期にわたって安全に保護する必要があるので、保存データにおける暗号化の課題は、移動中のデータにおけるそれより大きくなります。転送の暗号化では、一時鍵(セッション鍵)を使用することができます。

- **使用中のデータ**（または**処理中のデータ**）— これは、システムRAMやCPUのレジスタとキャッシュといった揮発性メモリの中にデータが存在している状態です。使用中のデータの例として、ワープロアプリケーションで開かれているドキュメント、現在修正中のデータベースのデータ、オペレーティングシステムの動作中に生成されるイベントログなどがあります。ユーザーがデータを使って作業する場合、そのデータは通常、保存状態から使用状態へ移る際に

復号化される必要があります。作業セッション全体を通じてデータが暗号化されていないこともあります、それによってデータはリスクに晒されます。しかし、Intel Software Guard Extensions (software.intel.com/content/www/us/en/develop/topics/software-guard-extensions/details.html)などの信頼できる実行環境(TEE)メカニズムは、信頼できないプロセスが情報を復号化できないよう、メモリ内に存在しているデータを暗号化することができます。

データ流出

大容量のモバイルデバイスが急増し、高帯域幅のネットワークリンクが容易に使用可能な職場では、PCやネットワークへの接続を許可されるストレージデバイスの種類を制限してデータ損失を防止することが、非現実的な場合があります。データをシステムから不正にコピーまたは回収することをデータ流出と言います。データ流出攻撃は、個人を特定できる情報(PII)や支払情報といった価値ある情報を、脅威アクターが読み出す主な手段の1つであり、そうした情報は多くの場合、その後闇市場で売られることになります。データ流出は、次に挙げるさまざまなメカニズムを介して実行されます。

- USBドライブ、デジタルカメラのメモリーカード、またはスマートフォンなど、リムーバブルメディアやその他のストレージデバイスへとデータをコピーする。
- HTTP、FTP、SSH、電子メール、またはインスタントメッセージ(IM)/チャットなどのネットワークプロトコルを使用する。高度な技術を持つ脅威アクターはリモートアクセス型トロイの木馬(RAT)を使用することで、非標準のネットワークポート上でデータ転送を実行したり、パケット工作ツールを使用して標準ポート上で非標準の方法でデータ転送を行ったりする可能性があります。また脅威アクターは、暗号化を用いて持ち出そうとするデータを偽装することができます。
- 電話、携帯電話、またはボイスオーバー IP (VoIP)ネットワークを介して口頭で伝える。携帯電話のテキストメッセージ機能が使われる場合もあります。
- データの画像またはビデオを使用する – テキスト情報が画像フォーマットに変換されると、コンピューター型の検知システムによってその画像データから元の情報を識別するのが非常に困難になります。

こうしたメカニズムの一部は、セキュリティツールを使って容易に軽減することができますが、対処がそれほど簡単でないメカニズムもあります。以前に検討した次のメカニズムやセキュリティ管理を使ってデータを保護することができます。

- すべてのセンシティブなデータを暗号化した上で保存する。データがネットワークの外部に転送されても、復号鍵を持たない脅威アクターにとってそのデータはまったく無意味です。
- 破壊や身代金目的の標的となり得るデータのバックアップをオフサイトで作成・維持する。
- センシティブなデータを保存または転送するシステムがアクセス制御を実行していることを確認する。アクセス制御メカニズムが特定のアカウントに過度の特権を与えていないかどうかをチェックする。
- 脅威アクターがネットワークから外部にデータを転送するのに使用し得るネットワークチャネルのタイプを制限する。アーカイブされたデータを保存しているシステムをネットワークから切り離す。
- ドキュメントの機密性と、データを安全に保存・転送するための暗号化の使用について、ユーザーにトレーニングを施す。これには人事部(HR)のバックアップと、スタッフが信頼できることを保証する監査ポリシーによるバックアップも必要です。

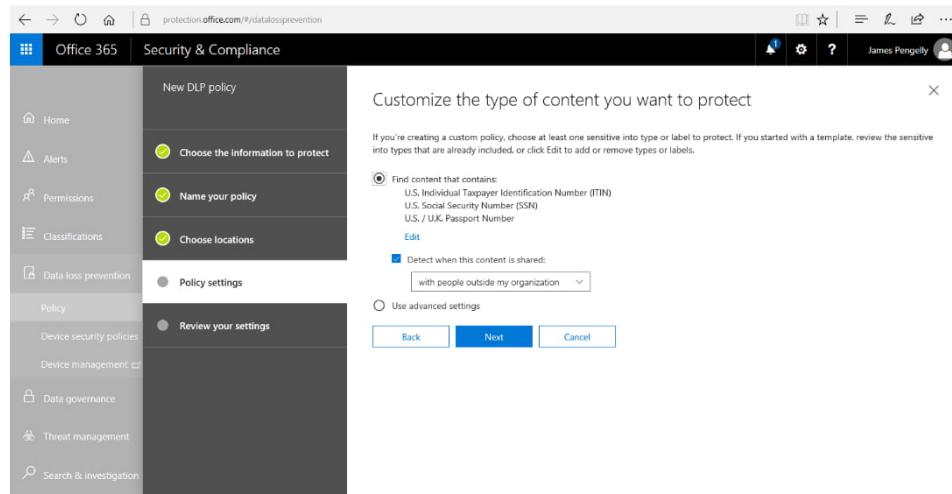
これらのポリシーや制御を念入りに適用したとしても、インサイダーの脅威や、高度標的型脅威(APT)マルウェアによるデータへのリスクは依然として存在します。結果として、データが所在するホストやネットワークだけではなく、データに直接アクセスポリシーを適用するタイプのセキュリティ管理ソフトウェアが開発されています。

データ損失防止

データ保護のポリシーと手順を適用するにあたり、小規模な組織はデータの分類とタイプ分けを手作業で行うことがあります。しかし大量の個人データを作成・収集する組織では通常、自動化されたツールを用いてこのタスクを支援することが必要になります。また、価値の高い知的財産(IP)データを保護するための要件があるかもしれません。**データ損失防止(DLP)**製品は、データ型の検知と分類を自動化し、適切な許可がないままそのデータが閲覧または送信されることがないよう、ルールを適用します。このような解決策は通常、以下のコンポーネントで構成されます。

- ポリシーサーバー – 分類、機密性、プライバシーのルールとポリシーを構成し、インシデントをログに記録すると共に、レポートをまとめます。
- エンドポイントエージェント – ネットワークに接続されていない間もクライアントコンピューターにポリシーを適用します。
- ネットワークエージェント – ネットワーク境界での通信と、Webとメッセージングサーバーのインターフェイスでの通信をスキャンし、ポリシーを適用します。

DLPエージェントは、正式なアクセス制御モデルを持つデータベースなど構造化された形式のコンテンツ、または電子メールやワープロ文書など構造化されていない形式のコンテンツをスキャンします。ファイルクラッキングのプロセスは構造化されていないデータに適用し、スキャン可能な一貫したフォーマットに変換します。コンテンツをUSBデバイスなどのリムーバブルメディアに転送する、または電子メール、インスタントメッセージ、さらにはソーシャルメディアによって転送することは、それが事前に定義されたポリシーに合致していない場合、ロックすることができます。大半のDLPソリューションは、アクセスを仲介するプロキシ、またはスキャンとポリシー適用を行うクラウドサービスプロバイダーのAPIを使用することで、保護メカニズムをクラウドストレージサービスに拡張することができます。



Office 365でDLPポリシーを作成する。(スクリーンショットはMicrosoftからの許可を得て使用。)

DLPソフトウェアがポリシー違反を検知した場合は修復が行われます。典型的な修復メカニズムとして次のものがあります。

- アラートのみ – そのコピー操作は許可されますが、管理システムがインシデントを記録し、管理者に警告する場合があります。
- ブロック – ユーザーはオリジナルファイルのコピー操作はできませんが、そのファイルへのアクセスは保持します。ポリシー違反についてユーザーに警告される場合もあればされない場合もありますが、管理エンジンによりインシデントとしてログに記録されます。

- 隔離 – そのユーザー（場合によってはすべてのユーザー）による元のファイルへのアクセスが拒否されます。これは所定の位置にあるファイルを暗号化するか、ファイルシステム内の隔離エリアへ移動することで実施します。
- 墓石 – 元のファイルは隔離され、ポリシー違反と、ユーザーがそれを再び解放する方法を記したファイルで置き換えられます。

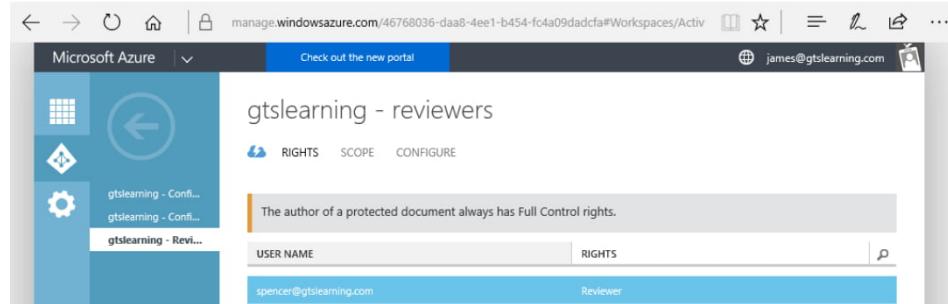
電子メールなどの通信チャネルを保護するよう構成されている場合、DLPによる修復はクライアントサイドまたはサーバーサイドのメカニズムを使って行われることがあります。例えばDLPソリューションの中には、メールが送信される前に、そのメールへの実際のファイル添付を防ぐものがあります。また、メールの添付ファイルとメッセージコンテンツをスキャンし、特定のデータを取り去ったり、そのメールが宛先に到着するのを防ぐものもあります。

この分野をリードするベンダーとして、Symantec/Broadcom (broadcom.com/products/cyber-security/information-protection/data-loss-prevention)、およびDigital Guardian (digitalguardian.com)などがあります。またDLPソリューションとコンプライアンスソリューションは、MicrosoftのOffice 365スイートでも利用可能です(docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide)。

ライツマネージメント（著作権管理）サービス

データ保護と情報管理ソリューションのもう1つの例として、MicrosoftがOffice製品スイート、SharePoint文書コラボレーションサービス、そしてExchangeメッセージングサーバーで提供しているInformation Rights Management (IRM)機能があります。IRMはActive Directory Rights Management Services (RMS)、またはクラウド型のAzure Information Protectionと連携します。これらの技術により、次の機能が管理者に与えられます。

- 作者、エディター、またはレビューなどのドキュメントロールにそれぞれ異なるファイルアクセス許可を割り当てる。
- 添付ファイルとして送信された場合でも、ドキュメントのプリントアウトと転送を制限する。
- 電子メールメッセージのプリントアウトと転送を制限する。



ライツマネージメントテンプレートを構成する。(スクリーンショットはMicrosoftからの許可を得て使用。)

ライツマネージメントはAdobe Acrobatなど、他のセキュアなドキュメントソリューションにも組み込まれています。

プライバシー強化技術

データ最小化とは、データの処理と保存は、収集目的を実行するのに必要な場合にのみ行われるべきであるという原則です。データ最小化という原則に従っていることを証明するために、個人データを使用する各プロセスは文書化しなければなりません。特定のフィールドまたはデータポイントの処理と保存が必要な理由については、ワークフローがその証拠をもたらすことができます。データ最小化はデータ保持ポリシーに影響を与えます。データポイントが収集されてからどれほど長く保存されているかと、継続保持によって合法的な処理機能がサポートされているのかどうかの追跡が必要です。影響が及ぶ別の分野としてテスト環境があり、そこでは最小化の原則によって実際のデータ記録の使用が禁じられています。

直感に反するようですが、最小化の原則には充足性または妥当性の原則も含まれます。このことは、データ主体が明確な同意を与えるべきである業務における、言明された目的のために必要なデータを収集すべきである、ということを意味します。後に追加のデータを収集することは、この原則に従っているとは言えません。

特に医療業界では、大規模なデータセットが組織間や企業間で共有されたり売買されたりすることがよくあります。これらのデータセットにPIIやPHIが含まれている場合、個人情報や個人を識別できる情報を除去する手段をとります。これらの匿名化プロセスは内部でも使用することができ、それによってプライバシーを不必要なリスクに晒すことなく、企業内の1グループが分析目的でデータを受け取れるようになります。また匿名化の各方式は、個人データが業務を実行するために収集されたものの、その後保持する必要がない場合にも使用できます。これは最小化の原則を適用することにより、データを保存する際のコンプライアンスリスクを減少させます。例として、顧客のクレジットカード番号を用いて注文の支払いを受ける会社のことを考えます。注文情報を保存する際、この会社はカード番号全体ではなく、最後の4桁だけをトランザクションログの一部として保存します。

完全に匿名化されたデータセットは、たとえそのデータセットに他のデータソースを組み合わせても、各個人主体をもはや識別できないデータセットのことであり、個人を特定する情報が永久的に取り除かれています。とは言え、完全な匿名化を保証し、かつ分析のためのデータの有用性を維持することは、通常は非常に困難です。結果として、代わりに疑似匿名化方式が一般的に用いられています。疑似匿名化は、個人を特定する情報を修正または置き換えることで、再特定するには分離して保存しているもうひとつのデータソースが必要となります。もうひとつデータへのアクセスにより、疑似匿名化方式は可逆性を有します。

コンテキスト情報が十分にある場合、データ主体が再特定されることもあるので、さまざまなソースへ配布するために匿名化方式を適用する際には、十分な注意を払わなければなりません。再特定攻撃は、匿名化されたデータセットを投票記録など他のデータソースと組み合わせ、用いられている匿名化方式がどの程度セキュアかを突き止める攻撃です。



K匿名情報は、2名以上の個人とリンクし得るデータです。このことは、そのデータがある個人を明確に再特定することはないものの、Kの値が与えられた場合に再特定の大きなリスクがあることを意味します。例えばK=5の場合、そのデータセット内の特定可能なすべてのグループは、少なくとも5名の個人を含んでいることになります。本書の執筆時点で、NISTは匿名化問題の概要のドラフト文書を作成しています(csrc.nist.gov/CSRC/media/Publications/sp/800-188/draft/documents/sp800_188_draft2.pdf)。

データベース匿名化方式

通常、匿名化の各方式は、そのデータをホストするデータベース管理システム(DBMS)の一部として実装されます。クエリやレポートが実行されるたび、センシティブなフィールドが匿名化のためにタグ付けされます。

データマスキング

データマスキングとは、例えばすべての文字列を「x」などで置き換えることにより、あるフィールドのコンテンツの全部、またはその一部を編集することを意味します。分析目的でメタデータを保存するために、フィールドが部分的に編集されていることもあります。例えば電話番号において、市内局番が保持されているものの、加入者番号が編集されている場合がそれにあたります。またデータマスキングでは、フィールドの元のフォーマットを保持する手法を使うこともできます。データマスキングは非可逆的な匿名化テクニックです。

トークン化

トークン化とは、あるフィールドのデータの全部または一部が、ランダムに生成されたトークンで置き換えられることを指します。トークンは、本番用データベースとは別に、トークンサーバーまたはトークンポールト（保管庫）に元の値とともに保存されます。許可されたクエリやアプリは元の値を必要に応じてポールトから回収することができるので、トークン化は可逆的なテクニックです。規制上の観点から見ると、暗号化されたフィールドは元のデータと同じ価値があるので、トークン化は暗号化の代替手段として用いられます。

集約/バンディング

別の匿名化テクニックとして、特定の年齢をそれよりも広い年齢幅で置き換えるといったように、データを一般化するというものがあります。

ハッシュ化とソルト化

暗号学的ハッシュは、SHAなどのアルゴリズムを使用して、任意の長さを持つ平文データから固定長の文字列を生成します。この機能がセキュアであれば、ハッシュを平文にマッチさせるのは不可能なはずです。ほとんどの場合、ハッシュ化は完全性の証明に使用されます。2つのソースが同じ平文へのアクセスを有している場合、それらは同じハッシュ値を導出するはずです。ハッシュ化はデータベース内の2つの主要な目的のために使用されます。

- 検索を高速化し、レコードへの匿名化された参照を提供するインデックス方式としてしようする。
- 元の平文を保持する必要がない、パスワードなどのデータの保存手段として使用する。

ソルトはハッシュ化されたデータフィールドと共に保存される追加の値です。ソルトの目的は、ハッシュのクラッキングを防ぐことです。これは、脅威アクターが平文の辞書を用いて、事前に計算されたハッシュの表を使用できないことを意味します。それらの表は、ソルトの値を含む形で再コンパイルする必要があります。

レビューアク ティビティ：

プライバシーとデータ保護の制御

次の質問にお答えください。

1. 信頼できる実行環境によってデータ保護が適用されるのは、データのどの状態ですか？
2. SharePointサイト上のREPORT.docxファイルにアクセスしようとしているユーザーから、あなたはインシデントレポートを受け取りました。このファイルが、ポリシー違反通知を含むREPORT.docx.QUARANTINE.txtファイルで置き換えられたというのです。最も可能性の高い原因は何ですか？
3. あなたはCompTIA Security+のシラバスに記載された目的を基に、プライバシー強化技術に関するソリューションの概要を準備しており、次の見出しのノートを書き終えましたが、他にどのようなレポート項目が必要ですか？

データ最小化、匿名化、疑似匿名化、データマスキング、集約/バンディング

レッスン16

概要

データ侵害とプライバシー侵害のリスクを軽減し、データ保護に向けたセキュリティソリューションを実装するために、データガバナンスのポリシーとツールの重要性を説明できる必要があります。

データのプライバシーと保護に向けたガイドライン

データガバナンスのポリシーと制御を作成し改善する際は、次のガイドラインに従ってください。

- 情報ライフサイクルモデルを使用して、機密データと個人データが分類・管理されていることを保証する。
- ライフサイクルの内部でデータの正しい管理が行われるようにするために、役割を割り当てる（オーナー、スチュワード、カストディアン、保護責任者、コントローラー、プロセッサ）。
- パブリック、プライベート、要配慮（センシティブ）、機密、極秘、プロプライエタリ、PII、医療情報、財務情報、顧客情報といった標準的なラベルを基に、機密データと個人データの分類を行う。
- 侵害イベントに対するインパクトアセスメントを行い、通知と報告の要件を特定する。
- ファイルやレコードに対する分類タグ付けを可能にする、コンテンツ管理システムを使用する。
- 暗号化製品を使用して、保存中、転送中、処理中のデータが保護されるようにする。
- 異なる転送メカニズム（ファイルシステム、電子メール、メッセージング、クラウド）に対してファイルやレコードの共有と配布のポリシーを強制するデータ損失防止システムをデプロイする。
- 個人データを共有する際は、マスキングやトークン化など、適切な匿名化メカニズムが適用されるようにする。

レッスン17

インシデント対応を実行する

レッスン概要

インシデント対応とは、日常的な観点から、監視システムによって生成されたアラートとユーザーによって報告された問題を調査することを意味します。このアクティビティは、ポリシーと手順によって導かれ、さまざまな技術的制御によってサポートされます。

インシデント対応は重要なセキュリティ機能で、セキュリティのプロフェッショナルとしての業務のほとんどがこれになります。インシデント対応の段階をまとめ、調査をサポートするために適切なデータソースを活用し、緩和策を適用してイベント発生後の環境を保護できる必要があります。

レッスンの目的

このレッスンの内容は、以下のとおりです。

- ・ インシデント対応手順をまとめる。
- ・ インシデント対応に適切なデータソースを活用する。
- ・ 緩和策を適用する。

トピック17A

インシデント対応手順を要約する



対象試験範囲

4.2 インシデント対応のポリシー、プロセス、手順の重要性を要約することができる

効果的なインシデント対応は、インシデント対応チームの役割と責任を定めた正式なポリシーと手順によって管理されます。これらの手順に従うこと、およびチーム内で割り当てられた役割を最大限に果たすことの重要性を理解する必要があります。

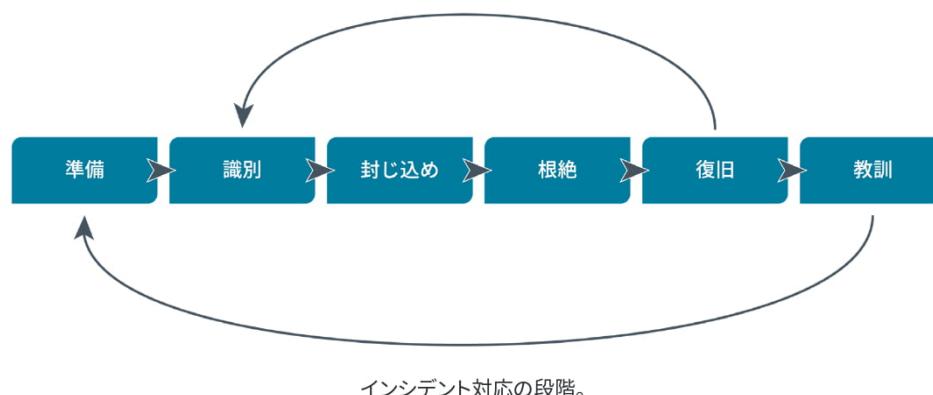
インシデント対応プロセス

インシデント対応ポリシーは、セキュリティインシデントに対処するためのリソース、手順、ガイドラインを規定しています。インシデント管理はリスクを緩和するために不可欠です。有効なインシデント管理により、セキュリティへの差し迫った脅威や特定の脅威を制御するだけでなく、組織の評判を維持できます。

インシデント対応は、NISTのComputer Security Incident Handling Guide特別刊行物 (nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)で既定されるような、適切に構成されたプロセスに従います。次は、インシデント対応ライフサイクルの主な段階です。

1. 準備 — まずシステムの攻撃に対する耐性を高めます。これには、システムの強化、ポリシーと手順の作成、機密情報の通信手段の設定などが含まれます。また、インシデント対応のリソースと手順を作成することも示唆されます。
2. 識別 — アラートやレポートの情報から、インシデントが発生したかどうかを判断し、インシデントの重度を評価して（トリアージ）、ステークホルダーに通知します。
3. 封じ込め — インシデントの範囲と重要さを制限します。インシデント対応の主な目的は、顧客やビジネスパートナーへの差し迫った影響を制限しつつ、データを保護することです。
4. 根絶 — インシデントを封じ込めたら、原因を排除して、セキュアな構成設定を適用して、パッチをインストールすることで、影響を受けたシステムをセキュアな状態に戻します。
5. 復旧 — インシデントの原因が根絶できたら、システムをビジネスプロセスに再統合できます。この回復段階には、バックアップからのデータ復元とセキュリティテストが含まれる場合があります。システムは、攻撃の再発の検知と予防のために一定期間、より厳密に監視される必要があります。完全に解決するために、対応プロセスでは、識別、封じ込め、根絶、回復の複数の段階を繰り返す必要がある可能性があります。
6. 教訓 — インシデントと対応を分析し、手順またはシステムを改善することが可能かどうかを判断します。インシデントは文書化する必要があります。この段階からの出力は、サイクルの新しい準備段階にフィードバックされます。

インシデント対応では、さまざまな部門やマネージャーからの調整されたアクションと承認が必要になる可能性があり、これによりさらに複雑さが増します。



サイバーインシデント対応チーム

インシデント対応の準備とは、セキュリティ侵害に対応するための文書化されたポリシーと手順を確立し、これらのポリシーを実施する人員を育成してリソースを確保することです。

最初の課題の1つは、インシデントのタイプを定義して、分類することです。通常、インシデントはセキュリティが侵害されたイベントや、侵害の試みがあったイベントとして説明されます。NISTでは、インシデントを「明示的または暗示的なセキュリティポリシーの違反行為」と説明しています。インシデントを特定して管理するには、トラブルシューティングのサポートでインシデントを記録および管理する方法と同様に、インシデントを報告し、分類して優先順位付け（トリアージ）する何らかの方法を開発する必要があります。

インシデント対応には、適切な検知と分析ソフトウェアへの投資に加えて、専門スタッフが必要です。大きな組織では、セキュリティインシデントの通知の単一窓口として専門チームがあります。このチームは、サイバーインシデント対応チーム(CIRT)、コンピューターセキュリティインシデント対応チーム(CSIRT)、またはコンピューター緊急対応チーム(CERT)など、さまざまに呼ばれています。インシデント対応チームには、セキュリティオペレーションセンター(SOC)が関与したり、SOC内に配置されたりすることもあります。どのように設定されていても、このチームには、（最も重大なインシデントに対するアクションを承認できる）上級意思決定者（重役レベルまで）と、管理者、軽微なインシデントに独自の裁量で対応できる技術者を含む混合チームである必要があります。

もう1つの重要な考慮点は可用性です。通常インシデント対応には24時間年中無休の可用性が必要になり、実現するにはコストがかかります。また潜入行動の可能性を阻止するために、CIRTのメンバーを定期的に入れ替えることを検討すべきです。重大なインシデントについては、他の事業部門からの専門知識とアドバイスが必要になります。

- 法務部 - チームが法律や業界規制の順守の観点からインシデント対応を評価できるように、法的な専門知識にアクセスできることが重要です。また、法執行機関の専門家と緊密に連絡を取る必要がある場合があります。これは、専門家の法的助言がなければ困難になる可能性があります。
- 人事(HR)部 - インシデントの予防と修復の措置は、従業員の契約や雇用法などに影響がある場合があります。インシデント対応では、従業員の通信を傍受したり、監視する権限が必要になります。
- マーケティング部 - チームでは重大なインシデントからの否定的な評判を管理できるよう、マーケティングまたは広報のインプットを必要とする場合があります。

組織によっては、インシデント対応プロバイダーを確保して、CIRT機能の一部をサードパーティーにアウトソーシングする場合があります。外部のエージェントは、インサイダーの脅威に対して効果的に対処できます。

通信プランとステークホルダー管理

インシデント対応ポリシーでは、インシデントを報告し、その後インシデント管理の進捗に伴い影響を受けた当事者に連絡するための明確な通信手段を確立する必要があります。連絡先情報が容易に入手できるようにすることは極めて重要です。

インシデントの処理を許可されたチーム以外に、情報が不注意により公開されるのを防ぐ必要があります。ステータスとイベントの詳細は、必要最小限で、**連絡先リスト**で特定された信頼できる当事者のみに配布してください。

通信プラン

CIRTの信頼できる当事者間のセキュアな通信は、インシデントを正常に管理するために不可欠です。脅威アクターに対して取られようとしている検知と修復の措置について、脅威アクターに知られないようにすることが重要です。CSIRTのメンバー全員にすべてのインシデントの詳細を知らせるのは適切ではない場合があります。

チームには、傍受できない「アウトオブバンド」または「オフバンド」の通信方法が必要になります。企業メールやVoIPを使用することにより、脅威アクターが通信を傍受できるというリスクが発生します。明らかな方法の1つに携帯電話がありますが、携帯電話では音声とテキストメッセージのみがサポートされます。ファイルとデータの交換には、Off-the-Record (OTR)、Signal、WhatsAppなどのエンドツーエンド暗号化を使用するメッセージングシステム、またはメッセージ暗号化 (S/MIMEまたはPGP) を使用する外部メールシステムがあります。これらでは、防御対象のネットワークのID管理プロセスとは完全に分離されたシステムのデジタル署名と暗号化キーを使用する必要があります。

ステークホルダー管理

信頼できる当事者には、社内と社外のステークホルダーの両方が含まれる可能性があります。インシデントが、マスコミやソーシャルメディアを通じて計画された通信外で公表されることは有益ではありません。機密情報を持つ当事者が、意図的または不注意にかかわらず、その情報を信頼できない当事者に公開しないようにします。

攻撃を報告する義務を検討する必要があります。インシデント発生時または発生直後に独自の修復が実施できるように、影響を受けた当事者に伝える必要がある場合があります。また監督機関や法執行機関に報告する必要がある場合があります。さらに、マーケティングと広報におけるインシデントの影響についても考慮する必要があります。これは大きな損害を与える可能性があるため、セキュリティシステムが改善されたことを顧客に示す必要があります。

インシデント対応プラン

インシデント対応プラン(IRP)では、さまざまなインシデントカテゴリで対応者が利用できる手順、連絡先、リソースをリストにしています。CSIRTは、一般的なインシデント (DDoS攻撃、ウイルス/ワームの発生、外部脅威アクターによるデータの流出、内部脅威アクターによるデータ改ざんなど) のプロファイルやシナリオを作成するべきです。これにより、調査員は優先順位と修復計画を決定することができるようになります。**ブレイブック** (またはランブック) は、データに基づく標準業務手順書(SOP)で、フィッシングの試み、SQLインジェクションによるデータの流出、ブラックリストに登録されたIP範囲への接続など、特定のサイバー脅威のシナリオを検知して対応する際に初級アーリストをサポートします。ブレイブックは、インシデントを検知し、検知、封じ込め、根絶の主要なステップを特定するために設計されたSIEMレポートとクエリからスタートします。