

TRAINING

AI時代に学ぶサイバーセキュリティ

3日目 会社としての対処法とこれからの考え方

スタッフサービス・エンジニアリング様 派遣エンジニア向けオンラインセミナー

2026年11月27日（金） 全3回の3回目



本資料の二次転載禁止について

本資料は株式会社ギブリーが作成した研修教材であり、著作権法により保護されています。受講者ご本人の学習目的に限りご利用いただけます。

無断での複製、改変、第三者への提供、社外への公開は禁止です。

本資料に掲載した外部サービスとニュースの画面は、各社の権利に帰属します。

講師紹介



人的資本インテリジェンス部門講師
生成AIエバンジェリスト

安田 光喜

Mitsuki Yasuda

メッセージ

みなさんがこれから生成AIをパートナーに新しい時代を生きていけるように、3日間全力でサポートしていきます！なにかご不明点などありましたら、講師陣になんでも気軽にご質問ください。

#ClaudeCode #Codex #Cursor #Antigravity
#全国統一生成AI活用技能試験S1 #生成AIサポート #G検定

得意領域

- ・生成AIをはじめとした世界最先端トレンド
- ・生成AIを用いた新規事業の開発、運営、補助
- ・アプリケーション開発/自動化プログラム環境構築
- ・教育（大学講師、研修、スクール運営など）

実績

- ・生成AI研修
- ・大手企業、外資、教育機関(小中高大)でのITトレンド講演
- ・自治体と連携した地域教育実績
- ・上場企業社員対象のリスキリング支援

公立はこだて未来大学 大学院（メディアデザイン領域）を卒業し、街づくり会社での複合商業ビルの立ち上げにおける情報インフラ整備やデザイン全般業務の責任として関与。その後デザイン事務所を立ち上げ、飲食店を中心としたデザイン業務や美術館展示のアートコンテンツ開発などを行う。また、地域ブランディングにも注力し、市主催の企画運営業務を行なった。2018年10月『小中学生向けのプログラミング教育』に注目し、函館市で初めての小中学生向けプログラミングスクール『D-SCHOOL北海道』を立ち上げて運営。その後北海道のドラッグストア『サッポロドラッグストアー』からスクールの買収を受け、教育を専門とするグループ会社『株式会社シーラクス』にて技術開発責任者として運営。スクール設計・運営、20以上の自治体連携（イベントや出張教室運営）、大人向けプログラミングスクールメンターなどさまざまな『次世代IT教育』に取り組む。

Dify公式資料の日本語翻訳や、SecondMeアンバサダーなど生成AI最新トレンドに注力。

全3回の進み方

全3回は「知る」「守る」「対応する」の3ステップ

1日目 知る

11月17日（火）
生成AIと情報セキュリティ。AIが攻撃と社内の使い方をどう変えたかを知ります

2日目 守る

11月25日（水）
世界のハッキング事例と個人での対処法。自分のアカウントと端末を点検します

3日目 対応する

11月27日（金）
会社としての対処法とこれからの考え方。事故の初動と報告文を作ります

各回だけの参加でも分かるように作っています。前の回の要点は、毎回の始めに振り返ります。

これまでの要点

1日目と2日目に出ていない方も、**ここだけ**押さえれば進めます

- 1 1日目 攻撃する側はAIを道具にし、社内のAI利用からも情報は外に出る**
AIに入れる前に、情報を社外可、加工して可、入れないの3段階に分けます
- 2 2日目 大きな事件の入口はVPN機器、盗まれたID、ヘルプデスクへの電話の3つ**
漏れたパスワードは別のサービスで使われ、証券口座の乗っ取りのように換金されます
- 3 本日 会社として先に手を付けることと、事故が起きたときの動き方**
最初の1時間の動きと、経営層へ送る第一報を作ります

本日の流れ

前半は会社の対策で後半はインシデントの初動

枠	内容	形式	時間
S01	前回の振り返りと本日の到達点	講義	[10min]
S02	会社としての対処	講義	[25min]
S03	これからのセキュリティの考え方	講義	[25min]
S04	ハンズオン インシデントの初動と報告文	ハンズオン	[40min]
S05	持ち帰りチェックリスト	講義	[10min]
閉会	質疑応答		[10min]

本日の到達点

本日の終わりにできるようになること

- 1 会社が先に手を付ける3つの対策を、根拠の事件とともに挙げられる**
露出した機器のパッチ、例外のない多要素認証、オフラインのバックアップ
- 2 攻撃の速さと規制の変化から、これからの備え方を説明できる**
セキュリティエンジニアの仕事の地図も見ます
- 3 インシデントに気づいた最初の1時間の動きと、第一報の6項目が分かる**
ハンズオンで、時系列メモと第一報を作ります

S02

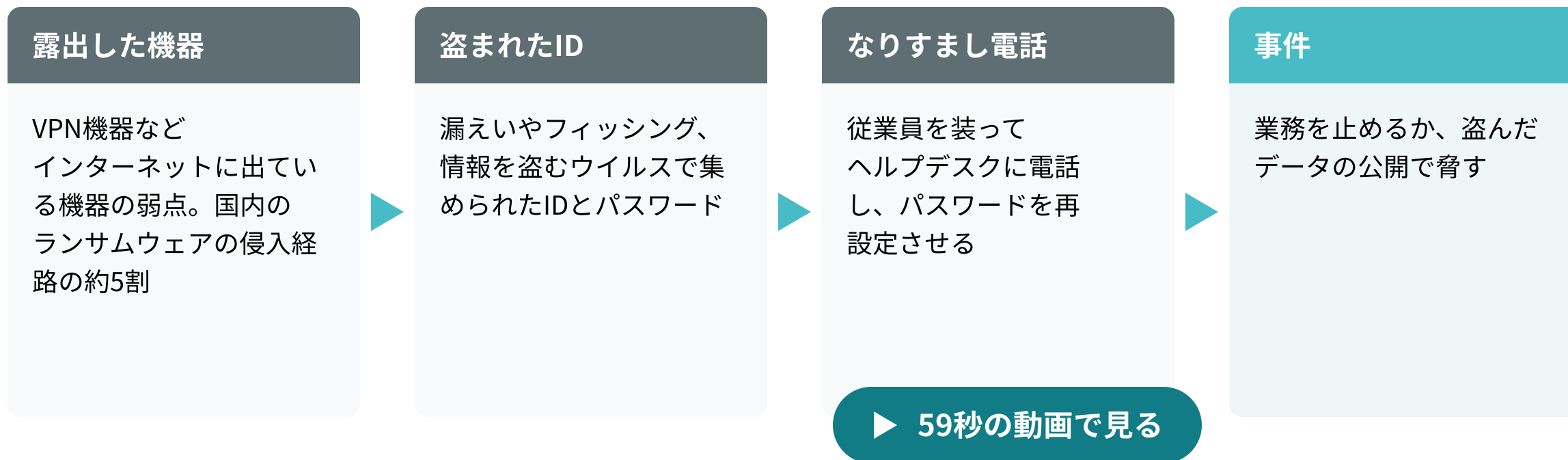
会社としての対処

入口をふさぎ、気づける仕組みを作り、止まっても戻れるようにする

- 侵入口の3つと先に手を付ける対策
- 多要素認証の種類
- 検知と記録、委託先とヘルプデスク
- ITなしで業務を続ける手順

侵入口の3つ

国内も海外も入口はほぼ3つに集まる



出典 警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」、TechRadar（英国小売への攻撃とヘルプデスクの悪用）

先に手を付ける3つ

根拠は国内の事件と警察庁の統計でそろっている

- 1 露出した機器を棚卸しして、更新をすぐに当てる**
アサヒはグループ拠点のネットワーク機器から入られました
- 2 社外から入る経路と管理者のアカウントに、例外なく多要素認証をかける**
アスクルは、例外として外していた委託先のアカウントから入られました
- 3 バックアップをネットワークから切り離して保管し、戻す練習をする**
バックアップを取っていた組織は約9割でも、戻せたのは2～3割でした

出典 警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」、アサヒグループホールディングス（2025年11月27日の発表）、Impress Watch（アスクルの侵入口と流出の件数）

アサヒとアスクルの違い

使えるバックアップの有無で交渉の要否が分かれた

アスクル

- オンラインのバックアップまで暗号化されました
- 一部の物流センターにEDRが入っていませんでした
- 全物流センターの再開まで約3か月半かかりました

アサヒグループ

- バックアップから戻せると早い段階で分かりました
- 攻撃者と接触せず、身代金も払っていません
- それでも全商品の出荷の再開まで約6か月かかりました

出典 アサヒグループホールディングス（2025年11月27日の発表）、Impress Watch（アスクルの侵入口と流出の件数）

多要素認証の種類

多要素認証は種類まで選ぶ

97%

認証情報を盗まれたことが原因の被害で、多要素認証が何らかの形で入っていた割合（Sophosの調査、2026年版）

FIDO

CISAが勧めるフィッシングに強い方式。パスキーもこの仲間です

SMSの番号やアプリの通知は、偽サイトに入力させたり通知を連打したりして突破されます。

出典 Sophos（ランサムウェアの現状 2026年版）、CISA（フィッシング耐性のある多要素認証）

気づける仕組みと記録

侵入に気づくには**見張り**と**記録**が要る

1 EDRを全拠点の端末に入れ、24時間の監視体制を作る

EDRは端末の不審な動きを見張る仕組みです。アスクールではEDRのない拠点がありました

2 ネットワーク機器と端末の記録を、最低1年保存する

アサヒの事件では、最初の侵入は暗号化の約10日前でした

3 調査と復旧の費用の目安を知っておく

調査と復旧に1,000万円以上かかった組織は、2026年上半期に60.0%でした

出典 警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」

委託先とヘルプデスク

自社が入られていなくても委託先から漏れる

対象	確かめること	根拠
委託先のアカウント	誰にどの権限を渡しているかの一覧を作り、使っていないものを止める	アスクルの侵入口は委託先の管理者アカウント
委託の契約	委託先が事故に気づいたら、すぐに知らせる義務を契約に書く	第三者が関わる侵害は48%（Verizonの調査、2026年版）
ヘルプデスク	パスワードの再設定や多要素認証の登録し直しを頼まれたときの本人確認の手順を決める	M&Sでは委託先のヘルプデスクが欺かれた

出典 Verizon（2026年版データ侵害調査報告書の発表）、IPA「情報セキュリティ10大脅威 2026」

ITが止まっても業務を続ける

紙とExcelで受注を続けた それでも出荷の正常化に**約6か月**

経営層は、ITなしで業務を続ける手順を事業継続計画に入れ、机上演習をします。警察、JPCERT/CC、保険会社、調査会社、個人情報保護委員会の連絡先は、紙でも用意しておきます。

Sophosの2026年版の調査で、認証情報を盗まれたことが原因の被害のうち、多要素認証が何らかの形で入っていた割合はどれですか。

A 約3割

B 約5割

C 97%

D 多要素認証が入っていた例はなかった

C

答えはC 97%

多要素認証が入っていても、偽サイトに入力させたり、通知を連打して承認させたりして突破されています。

CISAは、FIDOやパスキーのようなフィッシングに強い方式を勧めています。

出典 Sophos（ランサムウェアの現状 2026年版）、CISA（フィッシング耐性のある多要素認証）

S03

これからのセキュリティの考え方

攻撃は速くなり、規制は増え、守る人の仕事は広がる

- 攻撃の速さと暗号化しない脅し
- AIとセキュリティの3つの向き
- AI企業と研究者が示す守り方
- セキュリティエンジニアの仕事の地図

攻撃の速さ

人の手の対応より**攻撃のほうが速い**

22 秒

侵入した攻撃者が、別のグループにアクセスを渡すまでの時間（2025年。2022年は8時間超）

88 %

2026年上半期に公開された攻撃コードのうち、公開から48時間以内に悪用された割合

26 %

重大な脆弱性のうち、2025年中に完全に修正されたものの割合

出典 Help Net Security（M-Trends 2026の要点）、GuidePoint（2026年第3四半期のランサムウェアの報告）、Help Net Security（Verizon DBIR 2026の要点）

暗号化しない脅し

暗号化より盗んで公開すると脅す手口へ



バックアップから戻しても、公開の脅しは止まりません。対応の手順は、暗号化とデータの持ち出しの両方に備えます。

出典 警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」、Palo Alto Networks Unit 42（インシデント対応の報告）

AIとセキュリティの3つの向き

AIは**守る対象**であり道具であり攻撃の手段でもある

向き	中身	例
AIを守る	AIのシステムと、AIに渡すデータと権限を守る	入れてよい情報の仕分け、エージェントの権限の決め方
AIで守る	AIを使って監視や調査を速くする	大量の警告の仕分け、記録の読み解き、報告文の下書き
AIの攻撃に備える	AIを使った攻撃に気づき、止める	ディープフェイクのなりすまし、AIで作ったフィッシング

出典 ギブリー「サイバーセキュリティスキル標準 2026」

AI企業と研究者が示す守り方

まず固めるのは強い認証と最小の権限

1 フィッシングに強い多要素認証を入れる

IDを狙う攻撃の99%以上を防げます。AIで作ったフィッシングのクリック率は54%で、AIなしの4.5倍でした

2 AIエージェントの権限は最小にし、重い操作の前に人の承認を挟む

OWASPの指針とAnthropicの枠組みが、同じことを求めています

3 守る側もAIを使い、弱点を先に見つけて塞ぐ

GoogleのAIエージェントは、攻撃者が使う直前の脆弱性を見つけ、先に塞ぎました

▶ 30秒の動画で見る

出典 Microsoft (2025年版デジタル防衛レポートの発表)、OWASP「LLM06:2025 Excessive Agency」、Anthropic (安全で信頼できるエージェントの枠組み)、Google (2025年夏のセキュリティの取り組み)

2026年は報告の義務とAIの規制が同時に動いた

- 2026年7月17日 ○ 改正個人情報保護法が公布された。課徴金を入れたが、安全管理措置の違反は対象外
- 2026年10月1日 ● サイバー対処能力強化法の報告義務が始まった。15分野258の基幹インフラ事業者は3～5日以内に速報
- 2026年10月14日 ○ EUがAI法で初めての執行手続きとして、OpenAIとAnthropicに情報の提供を求めた
- 2026年10月 ○ 米国のFTCが、AIの安全に関わる事故についてOpenAIとAnthropicに書類の提出を求めた

出典 個人情報保護委員会（改正個人情報保護法の概要）、国家サイバー統括室ほか（サイバー対処能力強化法の施行）、Technology.org（EUがAI法で初の執行手続き）、Gizmodo（FTCがOpenAIとAnthropicに召喚状）

セキュリティエンジニアの仕事の地図

3日間の演習はそれぞれ現場の仕事の入口

仕事	何をするか	3日間の演習とのつながり
監視（SOC）	警告や通報を見て、本物の攻撃かを判定する	2日目 5通のメールの判定
インシデント対応	被害を広げないように動き、原因を調べ、報告する	3日目 最初の1時間と第一報
脆弱性診断	機器やアプリの弱点を、攻撃者より先に探す	3日目 露出した機器の棚卸し
クラウドとAIの設定点検	権限と設定を点検し、鍵の放置をなくす	1日目 エージェントに渡す権限
ルールづくりと教育	情報の扱いのルールを作り、社員に教える	1日目 情報の3段階の仕分け

出典 ギブリー「サイバーセキュリティスキル標準 2026」

AIに何を渡し何をさせるかを 決める場面は誰にでも来る

AIを業務に組み込むと、どのデータをAIに渡すか、AIに何を操作させるかを決める場面が出ます。セキュリティを専門にしない人にも、この判断は回ってきます。この3日間で扱った仕分けと権限の考え方は、その場面の判断にそのまま使える内容です。

サイバーセキュリティスキル標準 2026

100項目のうち24項目にAI時代の観点を付けた

2026.10.09 **Press**

Share  

ギブリー、AI時代のサイバーセキュリティ人材を定義する「サイバーセキュリティスキル標準 2026」を公開

～セキュリティ戦略から逆算した組織づくりを、スキルアセスメントによるギャップの可視化と74講座の研修で一気通貫に支援～

サイバーセキュリティスキル標準 2026

レベル	レベル定義	評価項目カテゴリ			
		全職種共通	セキュリティ専門職	マネジメント・経営層	
Lv.7	CISO・サイバーセキュリティ経営レベル 全社のセキュリティ戦略・投資・説明責任を担う最上位リーダー CISO・CxOクラス			サイバーセキュリティ経営・戦略	
Lv.6	セキュリティ事業推進・変革者レベル 部門・事業の戦略を意思決定し、事業に直接的なインパクトを与える セキュリティ部門長・CSIRT統括				
Lv.5	セキュリティ高度専門・エキスパートレベル 担当領域の標準を設定し、品質と方向性を担保する		セキュリティ		

- 10のスキルカテゴリーと100項目を、7段階のレベルで定義しています
- 24項目に、AIを守る、AIで守る、AIの攻撃に備えるの観点を付けました
- 国内では約11万人のサイバーセキュリティ人材が不足していると推計されています

出典 ギブリー「サイバーセキュリティスキル標準 2026」

個人情報の漏えいのおそれに基づいた会社が、個人情報保護委員会へ速報を出す期限はどれですか。

- A 気づいてから24時間以内
- B 気づいた時点からおおむね3～5日以内
- C 30日以内
- D 60日以内

B

答えはB 気づいた時点からおおむね3～5日以内

会社のどこかの部署が知った時点から数えます。確報は30日以内で、不正の目的によるおそれがあるときは60日以内です。

要配慮個人情報、財産的な被害のおそれ、不正の目的のおそれ、本人1,000人超の4つのどれかに当たると報告の対象です。

出典 個人情報保護委員会「漏えい等の対応とお役立ち資料」

[▶ 28秒の動画で見る](#)

S04

ハンズオン インシデントの初動と報告文

架空の会社で起きたランサムウェアの被害を題材に、最初の1時間と第一報を作る

- STEP1 シナリオと検知メモを読む
- STEP2 最初の1時間にする行動を選ぶ
- STEP3 時系列メモを作る
- STEP4～5 Geminiで第一報を下書きし、確かめる
- STEP6 報告の期限を確かめる

どんな場面か

A社（架空・物流会社）の月曜の朝、経理担当のパソコンでファイルが開けなくなり、EDRが警告を出しました。あなたは情報システム部の担当者です。最初の1時間の動きを決め、経営層へ送る第一報を作ります。

使うもの

Gemini（ログインなしでも使えます）と、配布フォルダ day3_handson

つくるもの

時系列メモと、経営層へ送る第一報

目安の時間

[40min]

決まりごと

分からないことは推測で埋めず「調査中」と書きます

この演習で身に付くこと

インシデントに気づいた最初の1時間でする行動と、しない行動を区別し、事実だけで第一報を組み立てられるようになります。

STEP1 シナリオを読む

AIは開かずに、何が起きたかをつかみます

- 1 配布フォルダの「01_シナリオ」を開き、「インシデントのシナリオ.txt」を読みます
- 2 「検知メモ.txt」で、EDRの警告、ランサムノートの要点、VPN機器の記録を確認めます
- 3 顧客台帳に何人分の、どんな情報が入っているかを書き留めます

8つの行動をしないとしないに分けてください

記号	行動
A	感染したパソコンのLANケーブルを抜き、Wi-Fiを切る
B	感染したパソコンの電源を切る
C	上長と情報システム部の窓口へ、電話で連絡する
D	画面とランサムノートをスマートフォンで撮影し、時刻を書き留める
E	ランサムノートに書かれた連絡先へ、交渉のためにメールを送る
F	自分でウイルス対策ソフトを動かして、駆除を試みる
G	共有フォルダのほかのファイルを開いて、被害の範囲を確かめる
H	委託先の保守アカウントを止めるよう、VPN機器の担当者に依頼する

STEP3 時系列メモを作る

見たことと推測を分けて、時刻順に書きます

- 1 「02_初動」の「時系列メモの様式.txt」をメモ帳で開きます
- 2 1行に、時刻と出来事を1つだけ書きます。推測には「推測」と付けます
- 3 最後に「分かっていないこと」を3つ以上並べます
- 4 書ききれなかったときは、「時系列メモ_記入例.txt」を使って次へ進みます

この時点では、Geminiを開きません。

STEP4 第一報の下書きを作る

時系列メモだけをGeminiに渡します

- 1 下の文面に続けて、自分の時系列メモか記入例を貼り付けて送ります
- 2 返ってきた第一報が、6項目に分かれているかを確認めます

Geminiに送る文面

あなたはA社の情報システム部の担当者です。次の時系列メモをもとに、社内の経営層へ送る第一報を作ってください。項目は、攻撃の種類、判明している範囲、影響、初動対応、外部への報告の状況、二次被害の相談先の6つです。メモに書いていないことは推測で埋めず、「調査中」と書いてください。

A社の情報システム部より、経営層の皆様へ向けたセキュリティインシデントに関する第一報をご報告いたします。

ご提示いただいた時系列メモに基づき、以下の通り状況をまとめました。メモに記載のない事項につきましては、現時点では推測で補わず「調査中」としております。

セキュリティインシデントに関する第一報

1. 攻撃の種類
 - ランサムウェアによる攻撃（疑い）および不正アクセスの可能性
 - （根拠：EDRによる「ランサムウェアの疑い」の警告、身代金を求める文面のファイル「README_RESTORE.txt」の確認、および予定外の保守アカウントによるVPNログインの検知）
2. 判明している範囲
 - 該当端末：経理担当のパソコン（PC-KEIRI-03）にて、共有フォルダのファイル名末尾が .locked に変更され、暗号化されていることを確認。
 - アクセス記録：共有フォルダ「顧客台帳」への読み出し記録を確認（取引先の担当者約2,300人分の氏名、電話番号、メールアドレスが含まれています）。

時系列メモの記入例から作られた第一報の冒頭

STEP5 下書きを確かめる

メモにないことが足されていないかを、Geminiと自分の両方で見ます

- 1 続けて下の文面を送り、メモにない内容と言い切っている文を一覧にさせます
- 2 第一報を自分でも読み、メモの記述と1文ずつ照らし合わせます

Geminiに送る文面

いま作った第一報の中で、時系列メモに書いていない内容と、メモでは分かっていないのに言い切っている文を抜き出して、一覧にしてください。あいさつの文は除いてください。なければ「なし」と書いてください。

いま作った第一報の中で、時系列メモに書いていない内容と、メモでは分かっていないのに言い切っている文を抜き出して、一覧にしてください。あいさつの文は除いてください。なければ「なし」と書いてください。

作成した第一報の中で、時系列メモに書かれていない内容（推測や補足）およびメモでは分かっていないのに言い切っている文の抜き出し一覧は以下の通りです。

一覧

1. 攻撃の種類

- 該当箇所：「ランサムウェアによる攻撃（疑い）および不正アクセスの可能性」およびその根拠の説明文
- 該当理由：メモにはEDRの警告やファイル名、身代金要求文、VPNのログイン記録の事実のみが書かれており、「ランサムウェアによる攻撃（疑い）および不正アクセスの可能性」というまとめ（解釈）はメモに直接書かれていない内容です。

2. 影響

Geminiが自分の下書きを点検した結果

AIの点検をすり抜けた言い切りを人を見つける

時系列メモに書いてあること

- 02:14に、委託先の保守アカウントでVPN機器にログインした記録が残っている
- 予定にない深夜の作業だった
- 攻撃者が誰かは分かっていない

Geminiの第一報が書いたこと

- 「侵入経路の端緒：委託先の保守アカウントによる予定外の深夜ログイン履歴を確認」
- 侵入経路と言い切ったのは推測です。Geminiの点検の一覧にも、この文は出ませんでした

個人情報保護委員会への速報は3～5日以内です

The screenshot shows the official website of the Personal Information Protection Commission (PPC). The header includes the PPC logo, a search bar, and navigation links. The main menu highlights '個人情報保護法等' (Personal Information Protection Law, etc.). The breadcrumb trail indicates the path: ホーム > 個人情報保護法等 > 漏えい等の対応とお役立ち資料. The page title is '漏えい等の対応とお役立ち資料'. A list of links is provided, including '漏えい等報告について', '漏えい等報告をする', '漏えい時の対応について（事業者編）', '漏えい時の対応について（行政機関等編）', '研修動画等お役立ち資料', and 'その他留意事項'. A prominent yellow box with a blue border contains the text: 'まずは 速報（新規） 発覚日から、3～5日以内'. Below this, a smaller line of text reads: '発覚したら、まずは速やかに報告してください。'

個人情報保護委員会の「漏えい等の対応とお役立ち資料」。発見日から3～5日以内の速報が案内されています

出典 個人情報保護委員会「漏えい等の対応とお役立ち資料」

最初の1時間の答え

行動	判断	理由
A LANを抜きWi-Fiを切る	する	ほかの端末へ広がるのを止める。警察庁もまず隔離を求めています
B 電源を切る	しない	メモリ上の記録が消える。隔離できないときだけ検討します
C 電話で連絡する	する	社内のメールも見られている前提で、別の手段で伝えます
D 撮影して時刻を書く	する	あとで時系列を組み立てる材料になります
E 攻撃者へ連絡	しない	接触するかは会社として判断します。個人では連絡しません
F 自分で駆除	しない	調査に要る痕跡が消えます
G ほかのファイルを開く	しない	被害を広げ、記録を上書きするおそれがあります
H 保守アカウントを止める	する	侵入に使われた入口をふさぎます

出典 警察庁「ランサムウェア被害防止対策」、CISA（ランサムウェア対策の手引き）

▶ 36秒の動画で見る

- ☒ 最初の1時間の8つの行動を、する4つとしない4つに分け、それぞれ理由を1行で書けた
- ☒ 時系列メモで、見たことと推測を分け、分かっていないことを3つ以上並べた
- ☒ 第一報が6項目に分かれ、分かっていない項目は「調査中」になっている
- ☒ 第一報の中から、メモにない言い切りを自分で1つ以上見つけて直した

この演習とセキュリティの仕事

今日の演習はインシデント対応の担当者の仕事

今日やったこと	セキュリティの現場での仕事	担う人
最初の1時間の行動を選んだ	被害の広がりを止め、証拠を残す初動を指揮する	CSIRT、インシデント対応の担当者
時系列メモを作った	記録から何がいつ起きたかを組み立て、原因を調べる	フォレンジックの調査員
第一報を作った	経営層、当局、取引先へ、事実だけを期限内に伝える	CSIRT、広報、法務

この事案が個人情報保護委員会への速報の対象かを考えます

- 1 下の文面をGeminiに送ります
- 2 Geminiの答えを、「報告の期限早見表.txt」の4つの類型と照らし合わせます

Geminiに送る文面

この事案で、個人情報保護委員会への速報が必要かどうかを、判断の理由とともに説明してください。報告の対象になる4つの類型に当てはめて考えてください。

S05

持ち帰りチェックリスト

職場で確かめる8項目と、次の一歩

職場のチェック表

研修のあとに職場で8つを確かめる

No	確かめること	確かめる相手
1	インターネットに出ている機器の一覧があり、更新を当てているか	情報システム部
2	社外からの接続と管理者のアカウントすべてに多要素認証がかかっているか	情報システム部
3	委託先に渡したアカウントの一覧があり、使わないものを止めているか	情報システム部
4	バックアップを、ネットワークから切り離れた場所にも保管しているか	情報システム部
5	端末とネットワーク機器の記録を、1年以上残しているか	情報システム部
6	生成AIの利用ルールがあり、使ってよいサービスが決まっているか	上長、派遣元
7	パスワード再設定の依頼を受けたときの本人確認の手順が決まっているか	ヘルプデスク
8	インシデントに気づいたときの連絡先を、紙でも持っているか	上長

次の一歩

- 1 職場のチェック表のうち、分からない項目を1つ選んで担当者に聞く**
表は提出しません。危ない点に気づいたら、派遣先の指揮命令者か上長に相談します
- 2 自分の職場で、机上演習ができないかを上長に相談する**
今日のシナリオと6項目の様式は、そのまま題材に使えます
- 3 セキュリティの仕事に関心があれば、スキル標準の項目で自分の位置を確かめる**
10カテゴリー100項目のうち、今日の演習はインシデント対応とルールづくりに当たります

全3回のまとめ

回	ステップ	持ち帰ったこと
1日目	知る	AIで攻撃が変わったことと、AIに入れてよい情報の3段階
2日目	守る	漏えいの照会、使い回しの洗い出し、パスキー、偽のメールの見分け方
3日目	対応する	会社が先に手を付ける3つ、最初の1時間の動き、第一報の6項目

警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

アサヒグループホールディングス（2025年11月27日の発表）

<https://www.asahigroup-holdings.com/newsroom/detail/20251127-0104.html>

Impress Watch（アスクルの侵入口と流出の件数）

<https://www.watch.impress.co.jp/docs/news/2070955.html>

Sophos（ランサムウェアの現状 2026年版）

<https://itbranschen.com/wp-content/uploads/2026/07/sophos-state-ransomware-report-2026.pdf>

CISA（フィッシング耐性のある多要素認証）

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>

Verizon（2026年版データ侵害調査報告書の発表）

<https://www.verizon.com/about/news/breach-industry-wide-dbir-finds>

IPA「情報セキュリティ10大脅威 2026」

<https://www.ipa.go.jp/security/10threats/10threats2026.html>

TechRadar（英国小売への攻撃とヘルプデスクの悪用）

<https://www.techradar.com/pro/avoiding-service-desk-exploitation-deconstructing-the-modern-retail-attack>

JNSA「インシデント損害額調査レポート」

https://www.jnsa.org/result/incidentdamage/data/incidentdamage_20250723.pdf

Help Net Security（M-Trends 2026の要点）

<https://www.helpnetsecurity.com/2026/03/24/mandiant-m-trends-2026-report/>

GuidePoint（2026年第3四半期のランサムウェアの報告）

<https://www.guidepointsecurity.com/wp-content/uploads/2026/10/GRIT-Q3-2026-Ransomware-Cyber-Threat-Insights-Report.pdf>

Help Net Security（Verizon DBIR 2026の要点）

<https://www.helpnetsecurity.com/2026/05/25/lessons-from-verizon-dbir-2026-findings/>

Palo Alto Networks Unit 42（インシデント対応の報告）

<https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report>

Microsoft（2025年版デジタル防衛レポートの発表）

<https://news.microsoft.com/source/asia/2026/01/07/microsoft-releases-2025-digital-defense-report-highlighting-the-changing-cyber-threat-landscape-and-the-importance-of-security-in-the-ai-era/>

OWASP「LLM06:2025 Excessive Agency」

<https://genai.owasp.org/llmrisk/llm062025-excessive-agency/>

Anthropic（安全で信頼できるエージェントの枠組み）

<https://www.anthropic.com/news/our-framework-for-developing-safe-and-trustworthy-agents>

Google（2025年夏のセキュリティの取り組み）

<https://blog.google/technology/safety-security/cybersecurity-updates-summer-2025/>

ギブリー「サイバーセキュリティスキル標準 2026」

https://givery.co.jp/news/20261009_1/

ISC2（2025年のサイバーセキュリティ人材調査）

<https://www.isc2.org/Insights/2025/12/ISC2-Publishes-2025-Cybersecurity-Workforce-Study>

国家サイバー統括室ほか（サイバー対処能力強化法の施行）

https://www.cyber.go.jp/pdf/press/siryou_20260930.pdf

個人情報保護委員会（改正個人情報保護法の概要）

https://www.ppc.go.jp/files/pdf/260407_kisyahaifusiryoku.pdf

Technology.org（EUがAI法で初の執行手続き）

<https://www.technology.org/2026/10/15/eu-ai-act-first-enforcement-openai-anthropic-ai-office/>

Gizmodo（FTCがOpenAIとAnthropicに召喚状）

<https://gizmodo.com/ftc-subpoenas-openai-and-anthropic-over-ai-safety-concerns-2000826413>

警察庁「ランサムウェア被害防止対策」

<https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html>

CISA（ランサムウェア対策の手引き）

<https://www.cisa.gov/stopransomware/ransomware-guide>

個人情報保護委員会「漏えい等の対応とお役立ち資料」

<https://www.ppc.go.jp/personalinfo/legal/leakAction/>

個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」

https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

サイバー攻撃被害に係る情報の共有・公表ガイダンス

https://www.cyber.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

JPCERT/CC 「侵入型ランサムウェア攻撃を受けたら読むFAQ」

<https://www.jpccert.or.jp/magazine/security/ransom-faq.html>

ご質問をお受けします

ZOOMのチャットか、手を挙げる機能でお知らせください。全3回へのご参加、ありがとうございました。



株式会社ギブリー (Givery, Inc.)

〒150-0036 東京都渋谷区南平台町15-13 帝都渋谷ビル8F