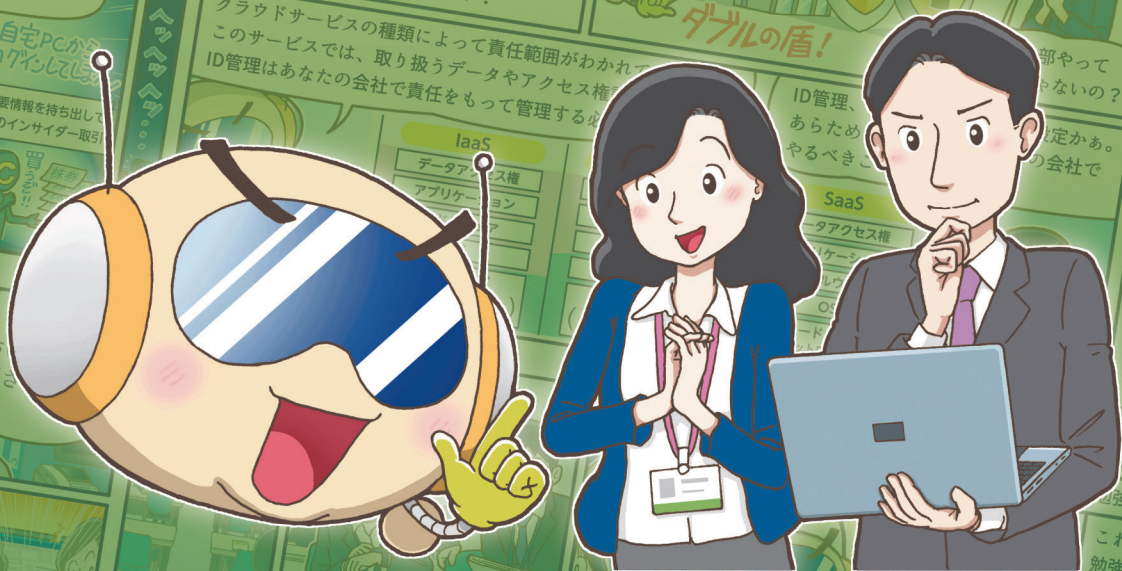


マンガでわかる サイバーセキュリティ

法人編

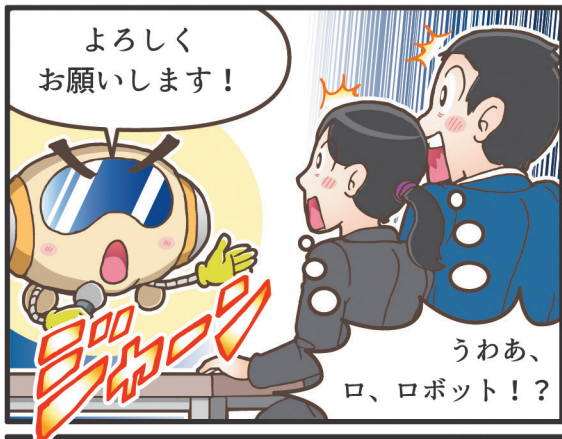


目次

- サイバー攻撃とマルウェアの種類・特徴を知ろう
- 「人の脆弱性」を狙った攻撃に注意しよう
- SNSによる投稿のリスクを学ぼう
- 標的型攻撃メールの手口を知ろう
- 不審なメールの添付ファイルを開いてしまったら…？
- 報告することの重要性を学ぼう
- ランサムウェアの対策と対処を学ぼう
- クラウドサービス利用時のセキュリティに注意しよう
- 内部不正の対策について知ろう

マンガでわかる サイバーセキュリティ

サイバー攻撃とマルウェアの種類・特徴を知ろう



サイバー攻撃の手法は多岐に渡りますが、企業や組織を狙った主なものには、

Webサイトへの大量アクセスを行うことでインターネットサービスを停止させる「DDoS攻撃」や、

標的型攻撃
情報窃取 破壊!

不正アクセス
中にいってやり放題

特定の企業や個人のPCをマルウェアに感染させ、情報窃取やデータの破壊等を行う「標的型攻撃」、脆弱性等のセキュリティ上の欠陥を悪用して社内環境へ侵入し、情報窃取やサーバ・システムを停止させる「不正アクセス」等があります。

特に近年は、企業や組織の情報を暗号化して金銭をゆすり取る「ランサムウェア攻撃」が流行しており、情報処理推進機構 (IPA) が毎年公表する「情報セキュリティ10大脅威」では、何年も連続で第1位に選ばれるほど、身近なものになっていると言えます。

順位	情報セキュリティ 10大脅威	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位
4位	内部不正による情報漏えい	5位
5位	テレワークなどのニューノーマルな働き方を狙った攻撃	4位
6位	修正プログラムの公開前を狙った攻撃	7位



良い質問ですね!

まず、マルウェアは **"malicious"** (悪意のある) と **"Software"** (ソフトウェア) を組み合わせた造語で、

malicious (悪意のある) + **Software** (ソフトウェア) = **malware** (マルウェア)

不正かつ有害な動作を行う意図で作成された、悪意のあるソフトウェアや悪質なコードの総称です。



その通りです。

「ウイルス」は、インフルエンザ等のヒトに感染するものと同じく「宿主が必要」という特徴があります。

他のプログラムに寄生した後、自身をさらに別のプログラムにコピーして感染を拡大させます。

単体では存在できず、増殖の形態がヒトの病気の感染に似ていることから名付けられました。

次に「ワーム」ですが、自身を複製させて感染を拡大する形態はウイルスと同じです。

宿主が不要という違いから、「ネットワーク中を這い回る虫 (worm)」と呼ばれています。単体で増殖できることから感染力が非常に強く、注意が必要です。

そして「トロイの木馬」ですが、単体で存在できる一方で自己増殖の機能はありません。

一見無害に見えるプログラムを装って侵入し、ユーザーに見つからないように、情報の窃取、他のマルウェアのダウンロード、不正アクセスするためのバックドア(*)の設置等を行います。

	自己増殖する	自己増殖しない
実行ファイルに寄生	ウイルス	
実行ファイルとして動作	ワーム	トロイの木馬

マルウェアって言っても色んなものがあるんだね…

あなたが被害者にならないためにも、まず知識を得ることは非常に大切なことです。

さすらいのロボはセキュリティ課題あるところに現れる!

あなたのところにも!

種類や特徴を知って、改めてその怖さを実感したよ。

この調子でこれからもサイバーセキュリティへの意識を高めていきましょう!

はい!!

(※)外部からコンピュータに侵入しやすいように、“裏口”を開ける行為、または裏口を開けるプログラムのこと

他の事例

- 企業のサーバーが不正アクセスを受けて Web サイトが改ざんされた結果、閲覧者の PC がウイルスに感染した
- 脆弱性を悪用された結果ワームに感染し、暗号化されたファイルを復号するための金銭を要求された(WannaCry)
- 正規の送信元を装ったメール内のリンクにアクセスしてトロイの木馬に感染してしまい、メール情報が流出した(Emotet)

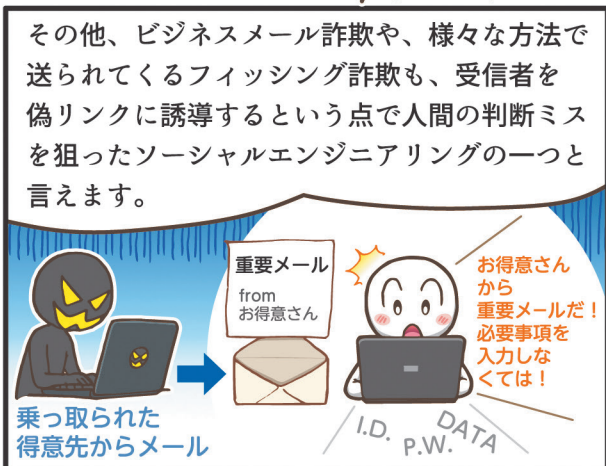
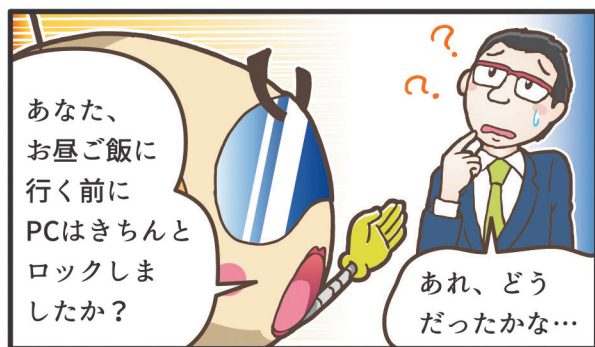
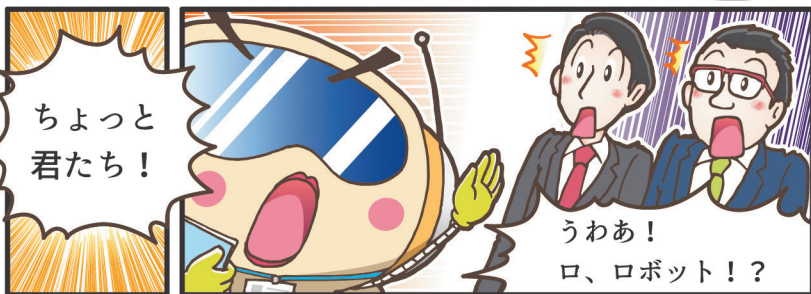
ここがポイント

- 組織や企業を狙う主なサイバー攻撃には、「DDoS 攻撃」「標的型攻撃」「不正アクセス」「ランサムウェア攻撃」等がある
※特に「ランサムウェア攻撃」は年々被害が拡大、2022年に警察庁へ報告された被害件数は前年比 57.5% 増加
- マルウェアは、「不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称」であり、自己増殖機能の有無や単体での存在可否によって、「ウイルス」「ワーム」「トロイの木馬」等の種類に分かれる

<参考文献>

- マルウェアとは：特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)
<https://www.jnsa.org/ikusei/03/08-01.html>
- インターネットの安全・安心ハンドブック：内閣サイバーセキュリティセンター(NISC)
<https://security-portal.nisc.go.jp/guidance/handbook.html>
- 情報セキュリティ 10 大脅威：独立行政法人情報処理推進機構(IPA)
<https://www.ipa.go.jp/security/10threats/index.html>

「人の脆弱性」を狙った攻撃に注意しよう



なるほど、普段の生活や仕事の中でも
何気ないところにリスクがあるんだね。



「人の脆弱性」とも言われるソーシャルエンジニアリング
については、こういった危険性に対してひとりひとりが
意識をきちんと向けることが重要です！



たとえばこのような
対策も有効です！

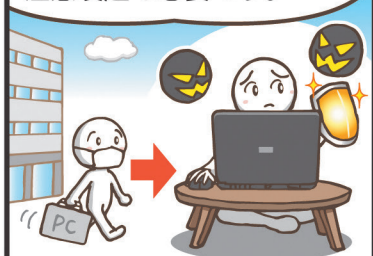


- 公共の場所でスマートフォンやPCを操作する際は
周囲の状況を確認する
- 離席時のPCのロックを徹底する
- 機密情報はそのまま捨てずにシュレッダー等で処理
- 不審なメールやファイルは開かない

また企業の場合は、
管理者が情報セキュリティポリシー(※)
を定めることで従業員への意識づけを
行うことも対策の一つですね。



最近ではテレワーク等により
社外で機密情報を扱うこと
も増えているので、
執務環境や周囲の状況への
注意喚起も必要です。



社会のデジタル化はどんどん進んでいますが、
そんな時だからこそ、アナログな視点から
セキュリティを見つめ直すことも大切なことです。



さすらいのロボは
セキュリティ課題
あるところに現れる！



他の事例

- パスワードや機密情報が書かれた印刷物を、ゴミの中から漁り出されて悪用される(トラッシング)
- AI で生成した音声(ディープフェイク)を利用して関係者になりすまし、電話で機密情報を聞き出す
- データを仕込んだ USB デバイス等をオフィス周辺に落としておき、拾得者が PC 接続・開封することで社内システムに侵入する
- 立ち入りが制限されている区画に入場資格を持たない人が、資格を持つ人が入場する際に一緒に入り込む(共連れ)

ここがポイント

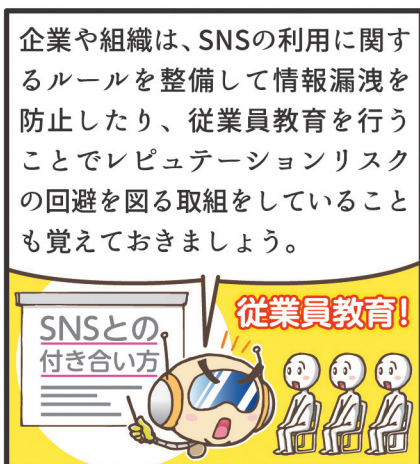
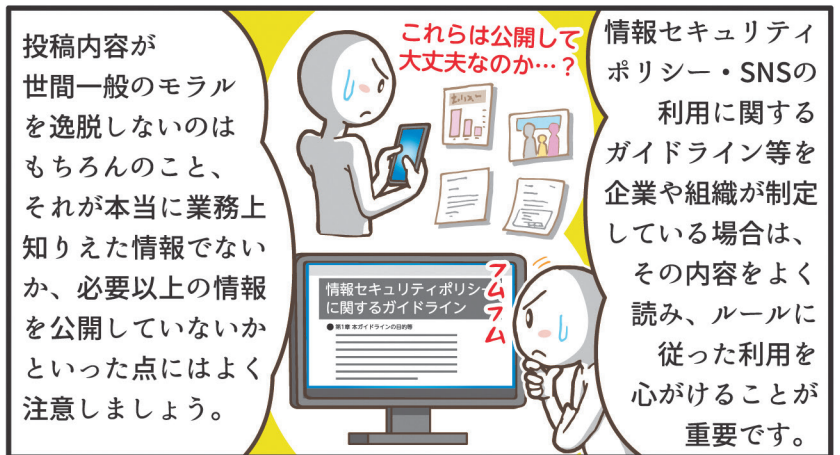
- 普段の生活や仕事の中に潜むセキュリティのリスクを知り、対策を意識した行動を継続的に実践する
(例：公共の場所でスマートフォンやPCを用いるときは周囲に注意する、離席時にはPCをロックする)
- 企業の場合、管理者が情報セキュリティポリシー(※)を定めることで従業員への意識づけを行う
(※)どのような情報資産をどのような脅威からどのようにして守るかについての基本的な考え方や、
情報セキュリティを確保するための体制、組織及び運用を含めた規定のこと

<参考文献>

- インターネットの安全・安心ハンドブック：内閣サイバーセキュリティセンター(NISC)
<https://security-portal.nisc.go.jp/guidance/handbook.html>
- 管理者向けセキュリティ対策：警視庁
<https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/security/cyber49.html>

SNSによる投稿のリスクを学ぼう





他の事例

- 職場の写真を SNS へ投稿したところ、業務に用いる書類が映り込んでしまい、機密情報が漏洩した
- SNS で不適切な内容を投稿した結果、個人情報だけでなく所属する組織まで特定されてしまい、苦情が殺到した
- SNS のプロフィールや投稿から氏名や誕生日を特定してパスワードを推測された結果、アカウントを不正に乗っ取られてしまった

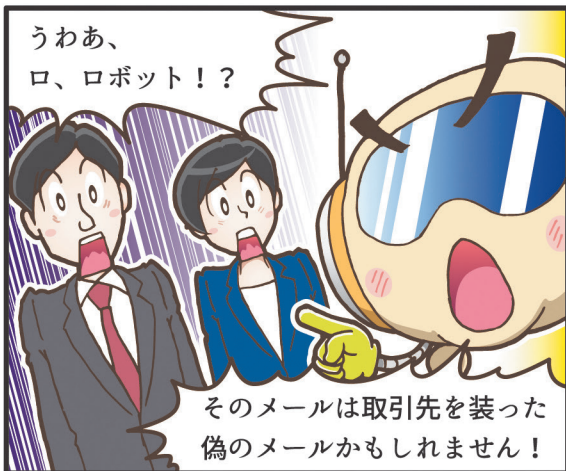
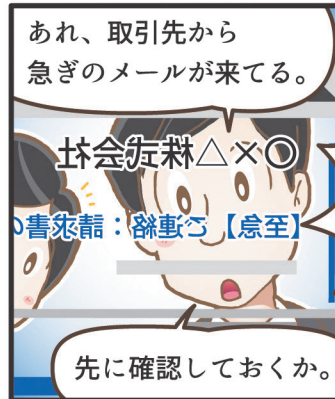
ここがポイント

- SNSで投稿を行う際は、写真や内容に不必要な情報が公開されていないか注意する
- SNSを利用する際は、企業や組織が制定する情報セキュリティポリシー、SNSの利用に関するガイドライン等を遵守する
- 企業や組織は、SNSの業務利用だけでなく私的利用についてもルールを整備したり、情報セキュリティに関する従業員への教育・啓発を実施することで情報漏洩やレピュテーションのリスクを回避する必要がある

<参考文献>

- SNS の正しい利用：国民のためのサイバーセキュリティサイト(総務省)
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/13/
- インターネットの安全・安心ハンドブック：内閣サイバーセキュリティセンター(NISC)
<https://security-portal.nisc.go.jp/guidance/handbook.html>

標的型攻撃メールの手口を知ろう



またメールの件名や 内容に「至急」や「重要」 などの言葉を入れて、 緊急に添付ファイル や文中のリンクを開く ことを要求するメール にも警戒する必要があります。

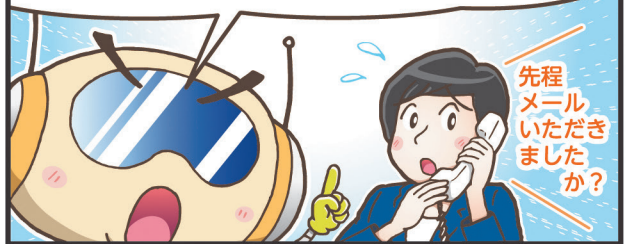


攻撃者は、受信者の端末をウイルスに感染させるために、受信者の興味を引いたり、「読まないといけない」と思わせたりするような細工をすることが多いのです。



連休明け等でメール確認が増えて、油断しがちなタイミングを狙ってやることもあるので気をつけましょう。

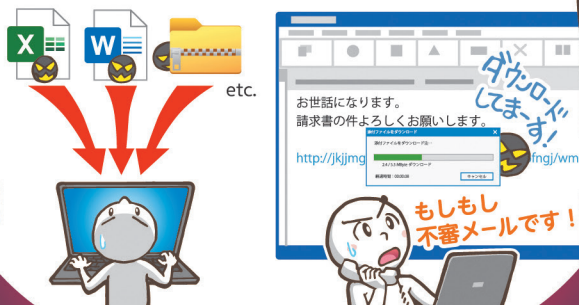
今回のように取引先を騙っているかもしれない不審なメールを受け取った場合は、その取引先に対して、メールではなく電話などの別の連絡手段で問い合わせをすることも一つの確認手段になりますね。



先程メールいただきましたか？

2021年11月後半より感染被害が再拡大している Emotet というマルウェアを使った攻撃手口では、主にマクロ付きの Excel や Word ファイル、あるいはこれらをパスワードの付いた Zip ファイルに入れてメールに添付する形式での配信が確認されています。

Emotet 2021年より再拡大中



他にも、メール本文中のリンクをクリックすることで悪質な Excel や Word ファイルがダウンロードされたり、アプリケーションのインストールを装って Emotet 感染を狙うケースも観測されています。不審だと思うメールを受け取った場合は、情報管理者にすぐに報告・相談するようにしましょう。

このような標的型攻撃を一つの手手段だけで防ぐことは難しいですが、標的型攻撃メールの手口をよく知り、そのようなメールが届いても添付ファイルを開いたり、リンクをクリックしないことが大切です。



攻撃者も僕らを騙すために色々な手口を考えているんだな…油断しないように改めて気をつけよう！



連休明け等でメールが溜まっている時は特に注意したいですね。

さすらいのロボはセキュリティ課題あるところに現れる！

あなたのところにも！

他の事例

- 銀行・行政サービス・インターネットプロバイダ等を騙り、マルウェアを仕込んだ添付ファイルや Web サイトのリンクを含むメールを送付される
- 実在する社員や職員を騙り、日程や内容の調整に関するメールのやり取りをしばらく続けた後、資料や依頼内容と称した URL リンクを記載したメールや、偽の資料ファイルを添付したメールを送付される
- 業務上やり取りするメールの送信者、よく使われているメールの件名や宛先、内容、添付ファイルの形式、署名などを真似ることで、一見不審には思わないほど精巧な偽メールを送付される

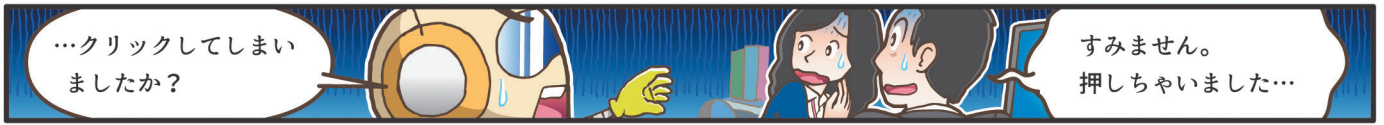
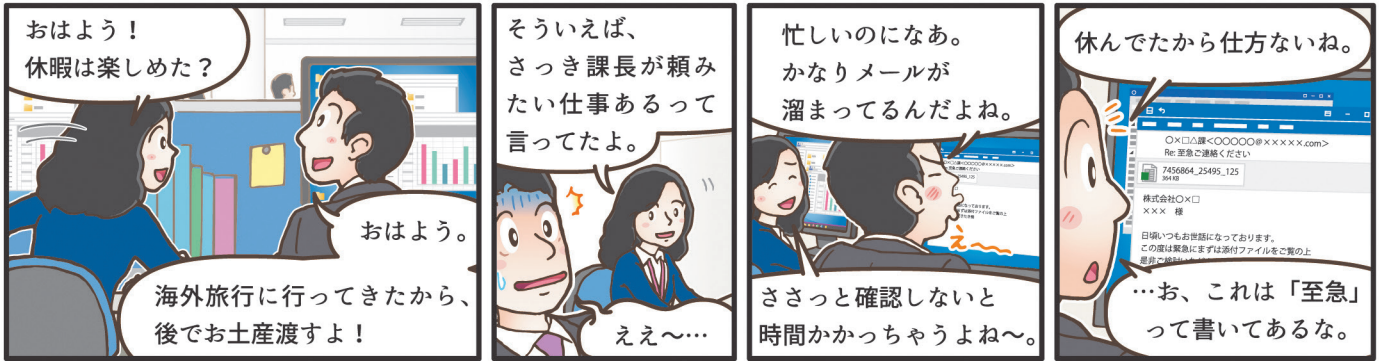
ここがポイント

- 標的型攻撃メールの手口をよく知り、不審なメールが届いても添付ファイルを開いたり、リンクをクリックしない
- 【攻撃に使われるメールの例】
- ・件名や内容に「至急」や「重要」などの言葉が入っており、受信者による操作を煽るようなメール
 - ・突然ファイル付のメールが届く、従前のやり取りと脈絡がないリンクを含むメール（ファイル形式やリンクをよく確認、特に短縮 URL には注意）
 - ・マクロ付の Excel や Word ファイル、それらをパスワード付の Zip ファイルに入れて添付しているメール（必要ない場合はマクロを有効にしない）

<参考文献>

- 標的型攻撃への対策：国民のためのサイバーセキュリティサイト（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/04/
- インターネットの安全・安心ハンドブック：内閣サイバーセキュリティセンター（NISC）
<https://security-portal.nisc.go.jp/guidance/handbook.html>

不審なメールの添付ファイルを開いてしまったら…?



…で、さっき言っていた「Emotet」って何だったの？

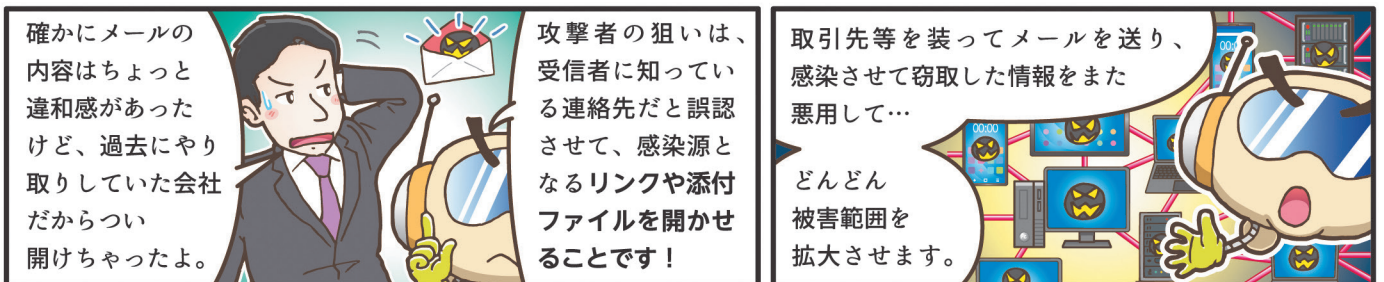
過去にやり取りしたメールへの返信を装ったメールを送信し、添付ファイルの開封を促す

感染するとPCから社内の認証情報やID、パスワード、メール本文等の様々な情報を窃取される

窃取した情報を悪用して感染拡大を目的としたメールをさらに送信し、社内だけでなく取引先等も巻き込んだ二次被害が発生する可能性もある

Emotetに感染した端末が別のマルウェアをダウンロードし、結果としてランサムウェア(身代金要求型マルウェア)感染等の更なる被害に繋がる可能性が高まる

Emotetは、主にメールの添付ファイルを感染経路としたマルウェア(不正プログラム)です。



また、Emotetはウイルス対策ソフト等で検知・解析されにくく、他のマルウェアに比べても感染力が高いのが特徴です。

感染したかもしれないときは、何をすればいいのかな。

Wi-Fi OFF

まず最初に、LANケーブルの抜線やWi-Fi接続の停止等、感染端末をネットワークから隔離してください。

その後システム部署やセキュリティ部署へ連絡して指示を仰ぎましょう。

とにかくネットワークから切り離すのが重要なね。

Wi-Fi P.W. 変更

はい。それが被害の拡大防止や証拠保全に繋がり、後に端末の調査を行う際に必要な情報を得やすくなります。

そして、感染端末で利用していたメールアドレスのパスワード変更も行いましょう。

他に気をつけることはある？

取引先 取引銀行 保険会社 知り合い

Emotetの感染を狙うメールには、知り合いや取引先を装ったメール以外にも、時事関連の内容や行政の話題等、心理的に開けたくなるものも多く、常に冷静な判断が求められます。

不審なメールを受信した際、このようなことも判断材料になりますので、よく確認しましょう！

送信元メールアドレスにフリーアドレスが使用されていたり、正式なアドレスに似せて偽装されたものでないか確認する

x△@example.com x@abcbanku.co.jp

添付ファイルにマクロが設定されていないか確認する(*)

見つけた相手からのメールや自分が送ったメールへの返信に見える場合も、身に覚えがなかったり不審な点があるときは、信頼出来る手段で相手に直接確認する

メールした？ してないよ

どんなに忙しくても、メールはしっかり確認しないとイケないんだな...

攻撃者は、メールに限らず様々な手法で我々を狙っており、そのリスクは高まっている状況です。

はい！

日頃からのセキュリティ意識の向上も継続しましょう！

さすらいのロボはセキュリティ課題あるところに現れる！

あなたのところにも！

(*)マクロを無効にする場合、「ファイル」>「オプション」>「トラストセンター」>「マクロの設定」>「警告を表示せずに/表示してすべてのマクロを無効にする」を選択。また、利用するOfficeは常に最新バージョンへ更新すること。

他の事例

- パスワード付き Zip ファイルを添付したり、本文中の URL リンクを介して Emotet に感染させる事例
- Microsoft OneNote 形式のファイル(.one)を悪用し、Emotet に感染させる事例 (メールに添付された OneNote 形式のファイルを開き、ファイル内の指示に従いボタンを模した画像をクリックすると、ボタンの裏に隠された悪意のあるファイルが実行されて Emotet に感染)

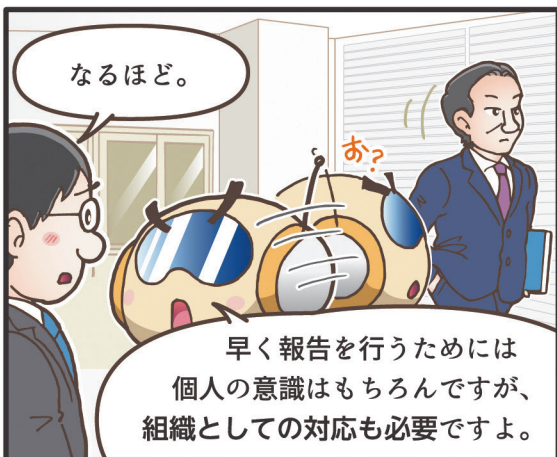
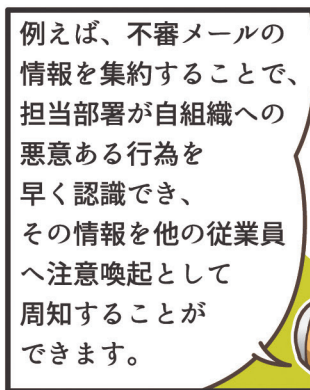
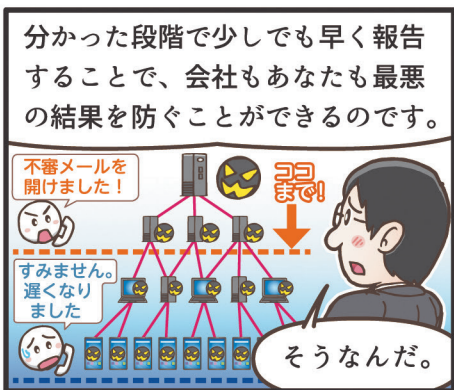
ここがポイント

- 不審なメールの添付ファイル等を開封してしまい、端末のマルウェア感染が疑われる場合は、すぐに LAN ケーブルの抜線や Wi-Fi 接続の停止等を行い、端末をネットワークから隔離する
- その後、感染端末で利用していたメールアドレスのパスワード変更を行う
- 一般的なセキュリティ対策に加えて、以下のような対策も検討する(システム・セキュリティ部署向け)
 - ・組織内への注意喚起の実施や、従業員のセキュリティ意識向上を目的とした啓発
 - ・マクロ自動実行機能の無効化 (*), メールセキュリティ製品や不正通信ブロックサービスの導入

<参考文献>

- Emotet 対策：警察庁 <https://www.npa.go.jp/bureau/cyber/countermeasures/emotet.html>
- Emotet(エモテット)関連情報 / Microsoft OneNote形式のファイルを悪用した攻撃(2023年3月17日):独立行政法人情報処理推進機構(IPA) <https://www.ipa.go.jp/security/emotet/index.html> / <https://www.ipa.go.jp/security/emotet/situation/emotet-situation-15.html>
- マルウェア Emotet への対応 FAQ: JPCERT/CC <https://blogs.jpCERT.or.jp/ja/2019/12/emotetfaq.html>

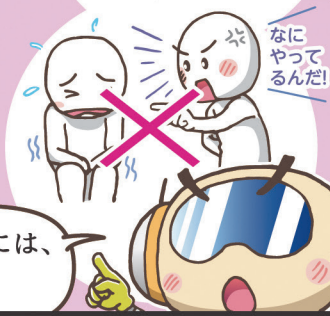
報告することの重要性を学ぼう



セキュリティインシデント発生時に重要なのは、「同じ過ちを繰り返さない」ことであり、

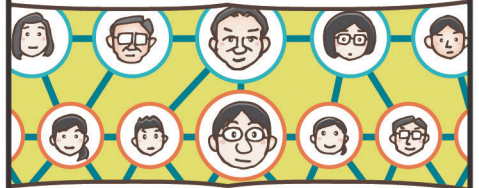


マルウェア感染メールを開いた従業員や設定ミスをした人等（インシデントの原因に関係した人）を責めないことがとても大切です。



組織としてのセキュリティ体制を強化するには、こういった風土の醸成も必要です。

また実際に被害に遭った時の対応を想定して、連絡先や関係者を事前に整理しておくことも非常に大切です。



その情報を定期的に周知する等して、組織に所属する全員に浸透させておきましょう。

確かにそうだな。

そこまで徹底できていなかったからこれからしっかり対応するよ。



実はさっき…



すぐにネットワーク抜線！システム部に連絡して！



報告が遅くなってしまってすみませんでした。



ひとりひとりが不審なメールに気づけることも重要ですが、その情報を適切な関係者へ報告できる環境も同じく大切です！



さすらいのロボはセキュリティ課題あるところに現れる！

あなたのところにも！



他の事例

- 社内 PC が不審な動作を示しマルウェア感染の可能性を考えたが、処罰や人事評価への影響を恐れて報告しなかった結果、被害が組織のネットワーク全体に広がってしまった
- 情報漏洩の事実を然るべき部署へ報告しなかった結果、初動が遅れて会社の信用がさらに失われてしまった

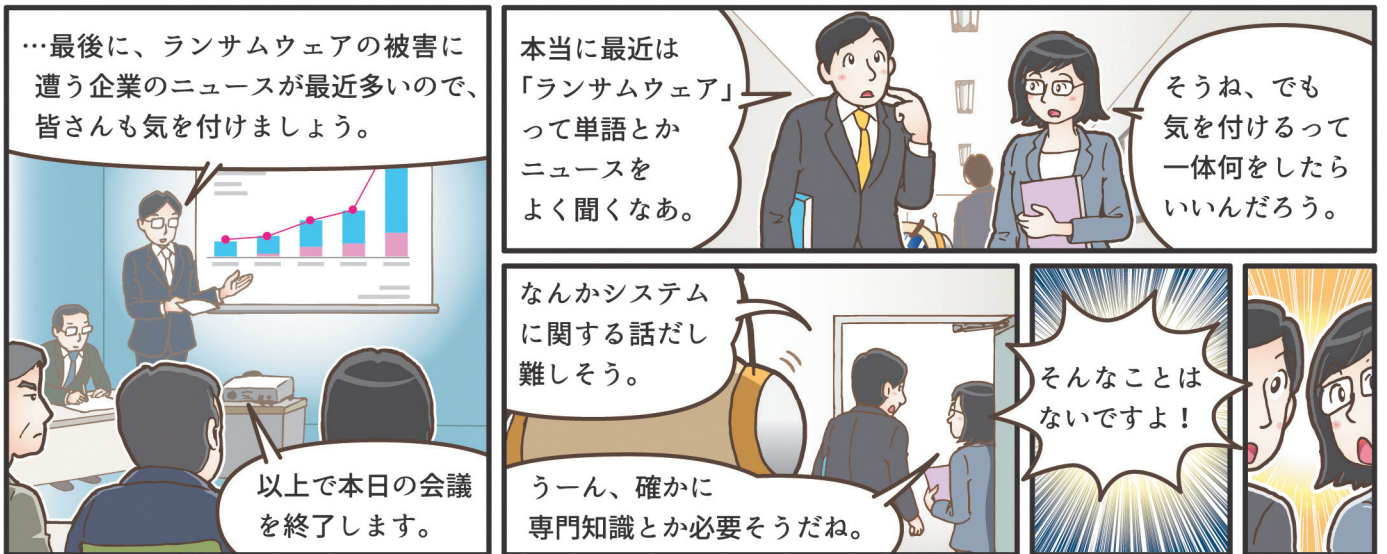
ここがポイント

- 不審なメールを発見したり、リンクや添付ファイルを開封してしまった場合は、上司や決められた部署へすぐに報告する
- 組織として、セキュリティインシデントに関係する事案があった際にすぐに連絡報告が可能な環境を整える（マルウェア感染メールを開いた従業員や設定ミスをした人等、インシデントの原因に関係した人を責めない）
- インシデントが発生した際の連絡先や関係者を事前に整理し、その情報を組織に所属する全員へ周知する

<参考文献>

- 電子メールと Web サイトにおける対策：国民のためのサイバーセキュリティサイト（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/admin/05/
- ビジネスメール詐欺（BEC）の特徴と対策：独立行政法人情報処理推進機構（IPA）セキュリティセンター
<https://www.ipa.go.jp/security/bec/hjuojm00000037nn-att/000102392.pdf>
- 情報セキュリティインシデントの事後対応：JPCERT/CC
<https://www.jpCERT.or.jp/magazine/security/illustration/part3.html>

ランサムウェアの対策と対処を学ぼう



ランサムウェアの感染経路には様々なものがあるため、このような基本的な対策を多重的に行うことで、被害に遭う可能性を最小限に抑えることが何より大切なんです！



一方で、ランサムウェアは近年日本でも被害件数が大幅に増加しており、今や他人事ではない状況です。



万が一ランサムウェアの被害に遭ってしまった時の対処についても少しお話ししましょう。

まず大前提として、ランサムウェアによって身代金を要求されても以下の観点から絶対に支払ってはいけません。

<p>1 暗号化されたファイルやデータが復元される保証はない</p>	<p>2 被害を受けた原因は未解消のまま</p>
<p>3 支払った後に別の攻撃や更なる支払要求を受ける可能性がある</p>	<p>4 犯罪者に利益供与を行ったと見做される可能性がある</p>

万が一ランサムウェアの感染が疑われるような不審な挙動があった場合には、まず端末をネットワークから切断してください。



この時、端末内にデータの復号に必要な情報が残っていることもあるので電源は切らないようにしましょう。

そして、すぐにシステム担当やセキュリティ担当へ連絡です！

セキュリティ担当ですか？実は…！

連絡が遅れると、他の端末やネットワークにも感染が拡大して、状況がさらに悪化してしまいます。

ランサムウェアへの対処は初動が最も肝心ですので、被害を広げないためにもこれらは必ず行ってください。



被害に遭わないためには、普段から基本的なセキュリティ対策を怠らないことが大事なんだな。

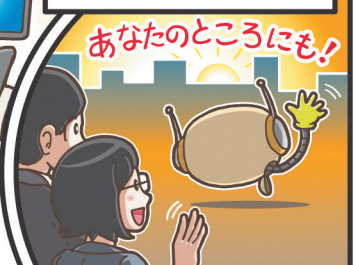


もし実際に起こった時も、早く正しく動けるように対処を知っておかなくちゃね。

ところで、あなた方の端末はしっかりアップデートされていますか？

あ、この間案内されたアップデートやってない！やらずに！

さすらいのロボはセキュリティ課題あるところに現れる！



二ポイント

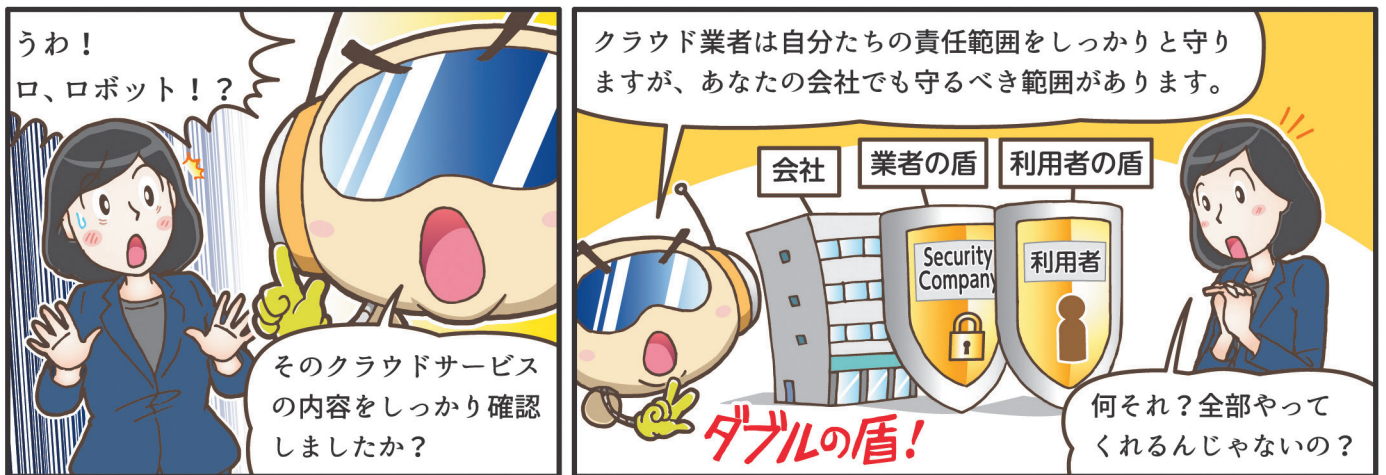
- ランサムウェア被害に遭わないためにも、基本的なセキュリティ対策を怠らない
 - ・不審な URL にはアクセスしない、メールの添付ファイルの開封には注意する
 - ・端末の OS やソフトウェアは常に最新のバージョンへアップデートする
 - ・機器や端末で利用するパスワードを推測されにくいものに設定する、同じパスワードを他の機器やシステムで使い回さない、システム等のログイン手段に多要素認証を導入する
- ランサムウェアによって身代金を要求されても以下の観点から絶対に支払わない
 - (1) 暗号化されたファイルやデータが復元される保証はない
 - (2) 被害を受けた原因は未解消のまま
 - (3) 支払った後に別の攻撃や更なる支払要求を受ける可能性がある
 - (4) 犯罪者に利益供与を行ったと見做される可能性がある
- ランサムウェアに感染した場合、端末をネットワークから切断し、すぐにシステム担当やセキュリティ担当に連絡する
 - ※初動について、企業のシステム担当やセキュリティ担当から指示がある場合はそちらを優先する

<参考文献>

- ランサムウェア対策特設サイト：JPCERT/CC
<https://www.jpcert.or.jp/magazine/security/nomore-ransom.html>
- ランサムウェア被害防止対策：警察庁
<https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html>
- マルウェア「ランサムウェア」の脅威と対策(対策編)：警視庁
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html
- 「No more Ransom」プロジェクト(司法当局と民間組織が連携してランサムウェアの被害低減を目指す国際的なプロジェクト)
<https://www.nomoreransom.org/ja/index.html>

マンガでわかる サイバーセキュリティ

クラウドサービス利用時のセキュリティに注意しよう



クラウドサービスの種類によって責任範囲がわかれていて、このサービスでは、取り扱うデータやアクセス権設定、ID管理はあなたの会社で責任をもって管理する必要があります！

ID管理、データのアクセス権設定かあ。あらためて思うと、当然自分の会社でやるべきことだよな。

	IaaS	PaaS	SaaS
利用者の責任範囲	データアクセス権	データアクセス権	データアクセス権
	アプリケーション	アプリケーション	アプリケーション
	ミドルウェア	ミドルウェア	ミドルウェア
	OS	OS	OS
クラウド業者の責任範囲	ハードウェア (ネットワーク、サーバ、ストレージ等)	ハードウェア (ネットワーク、サーバ、ストレージ等)	ハードウェア (ネットワーク、サーバ、ストレージ等)



他の事例

- クラウド事業者側での作業ミスや構成不備等により、数時間に渡りクラウドサービスが利用できない事象が発生した
- クラウド上での設定ミスにより、利用者が意図しない情報が公開されてしまう事象が発生した
- 使い方によっては、セキュリティ監視やインシデント対応が必要となるケースがあることにも注意

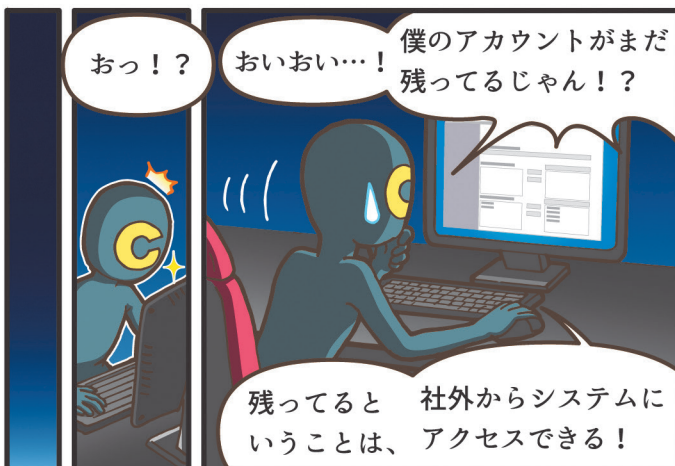
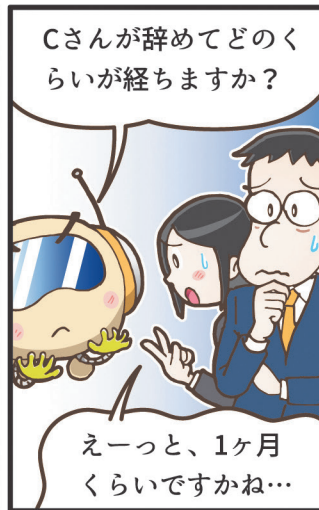
二点がポイント

- クラウドサービスの利用設定(異動や退職時のアカウント削除といったID管理、アクセス制限等)は定期的に見直す
- 各社のシステム部門やセキュリティ部門が、クラウドサービス利用に係るチェックリスト等を作成している場合は参考にする
- クラウドは簡単に始められるが、外部と繋がった環境を利用することになるため、実績があるベンダと共に、クラウド特有のリスクとメリットを認識しながら環境を構築する
- 契約書や利用規約を確認し、IaaS/PaaS/SaaSといった利用形態に応じて、クラウド業者と利用者の責任範囲を十分に認識する

<参考文献>

- クラウドサービスに預けていた重要データが消えた：国民のためのサイバーセキュリティサイト(総務省)
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/case/business/09/
- 中小企業の情報セキュリティ対策ガイドライン：独立行政法人情報処理推進機構(IPA)
<https://www.ipa.go.jp/security/guide/sme/about.html>

内部不正の対策について知ろう



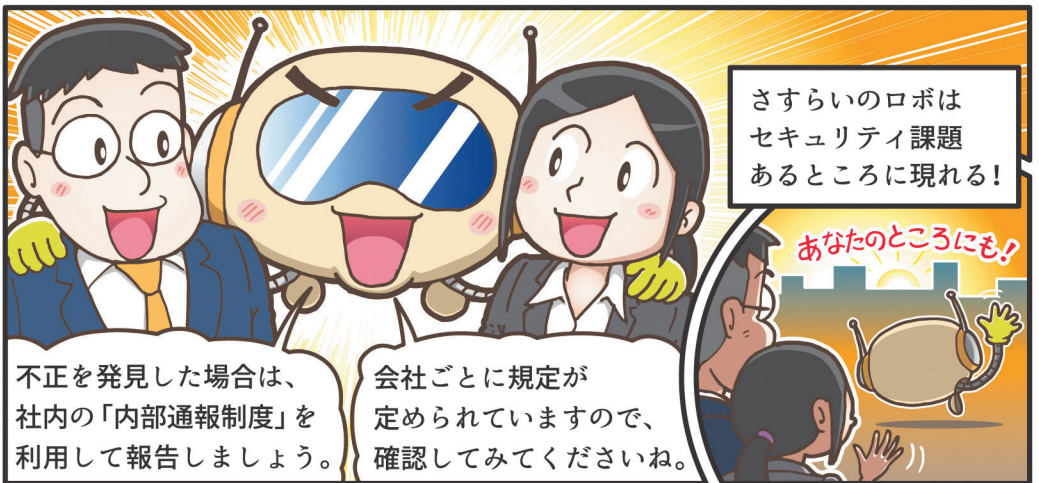


せっかくなので、内部不正防止の基本原則をおさらいしてみましょう。

<p>1 犯行を難しくする</p> <p>対策を強化することで犯罪行為をやりにくくする</p> <p>デジタル管理</p> <ul style="list-style-type: none"> 入退出管理の徹底 退職者のID削除 PC・データ持ち出しの禁止 	<p>2 捕まるリスクを高める</p> <p>管理や監視を強化することで捕まるリスクを高める</p> <p>警備会社</p> <ul style="list-style-type: none"> 通報制度の設置 情報機器の棚卸 監視カメラの設置 	<p>3 犯行の見返りを減らす</p> <p>標的を隠したり排除したり、利益を得にくくすることで犯行を防ぐ</p> <ul style="list-style-type: none"> アクセス権限の設定や保存データの暗号化 モバイル機器の施錠管理 警察への迅速な届出 	<p>4 犯行の誘因を減らす</p> <p>犯罪を行う気持ちにさせないことで抑止する</p> <ul style="list-style-type: none"> 公正な人事評価 適正な労働環境 円滑なコミュニケーション 	<p>5 犯罪の弁明をさせない</p> <p>犯罪者による自らの行為の正当化理由を排除する</p> <p>ルール</p> <ul style="list-style-type: none"> ルールを決めて遵守させる 誓約書へのサイン 定期的な啓発活動
--	--	--	--	--

「退職者のアカウントを削除する」は①の対策ですね。

人事評価や労働環境が内部不正防止に繋がるなんて初めて知ったよ！



- 他の事例**
- 退職者が在職中に他の社内メールを転送しており、退職後にその重要情報を漏えいさせてしまった
 - 家に持ち帰って仕事をする為に自宅のPCにデータを転送したが、自宅のPCがマルウェアに感染してしまい情報が漏えいしてしまった
 - 顧客情報を取り扱っていた業務委託先の従業員が、不正に情報を持ち出して販売していた
 - 犯罪者集団から「報酬を1億円支払うので社内にランサムウェアを仕掛けてほしい」と持ち掛けられた

- ニギがポイント**
- 退職者のIDは速やかに削除するなど、人事の異動に伴うアカウント管理を徹底する
 - 内部不正防止規程や通報制度を設置し、従業員にしっかりと周知する
 - PCやスマートフォンにはスクリーンセーバーや画面ロックの設定を徹底する
 - 基本的にはPCや顧客情報・重要情報の持ち出しは制限し、持ち出し管理を行う
 - 公正な人事評価、労働環境を徹底することは内部不正防止にも繋がる

<参考文献>
 ● 組織における内部不正防止ガイドライン：独立行政法人情報処理推進機構 (IPA)
<https://www.ipa.go.jp/security/fy24/reports/insider/>



Memo

