AIG

AIG損保

静岡県土木施工管理技士会研修会

守るべき情報資産をあらためて意識する！建設業の情報セキュリティ

2025年11月28日

AIG損害保険㈱
リスクコンサルティングユニット
森　喜一

1

「守るべき情報」を把握

例えば、

◆図面、工程表、写真、打合せ記録
◆発注者、近隣、工事関係者の個人情報（個人の名前が記載された書類等）
◆建物の内部や設備の状況（写真等）
◆工事の技術やノウハウ（仕様等）
◆関係各社の管理情報
◆契約の内容

※
■機密情報：機密事項と明記された文書や機密であることを前提にした情報
■個人情報：個人を識別できる情報（氏名・性別・年齢・住所・電話番号等）

AIG AIG損保

2

建設業界での事例

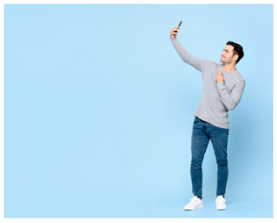
- ●図面を紛失
- ●SNS用に現場写真投稿
- ●身内への写真共有→流出
- ●メール誤送信
- ●不正アクセス
- ●サイバー攻撃によるランサムウェア感染
- ●現場・オフィス・自宅間で車上荒らし盗難、紛失
- ●従業員による不正情報持ち出し
- ●パソコン盗難
- ●宅配業者になりすました、偽のショートメッセージからフィッシング攻撃
- ●サイバー攻撃でマルウエア感染させデジタルデータ窃取
- ●コンビニで図面をコピーした後、原稿を置き忘れ紛失

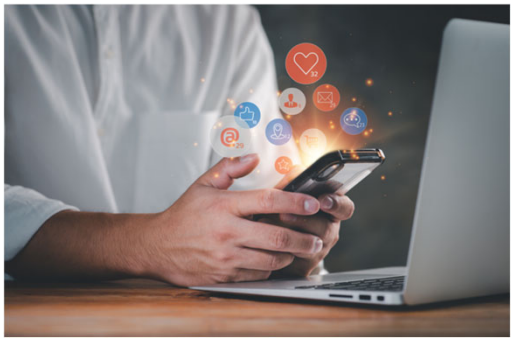
などなど

AIG AIG損保

3

SNS投稿・写真





AIG AIG損保

4

手口

出典：独立行政法人情報処理推進機構『宅配便業者をかたる偽ショートメッセージで、また新たな手口が出現』より
https://www.ipa.go.jp/security/anshin/attention/2019/mgdayori20190320.html

AIG AIG損保

5

手口

図3：不在通知の偽SMSの手口事例

出典：独立行政法人情報処理推進機構『URLリンクへのアクセスに注意』より
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html

AIG AIG損保

6

手口

出典：独立行政法人情報処理推進機構『宅配便業者をかたる偽ショートメッセージに引き続き注意』より
https://www.ipa.go.jp/security/anshin/attention/2020/mgdayori20200220.html

AIG AIG損保

7

手口

※ アプリのインストール後に偽の警告メッセージが表示されます

④ メッセージから誘導されたフィッシングサイトで情報を入力する
→ さらなる被害につながる

出典：独立行政法人情報処理推進機構『宅配便業者をかたる偽ショートメッセージに引き続き注意』より
https://www.ipa.go.jp/security/anshin/attention/2020/mgdayori20200220.html

AIG AIG損保

8

手口

出典：独立行政法人情報処理推進機構『宅配便業者をかたる偽ショートメッセージに引き続き注意』より
https://www.ipa.go.jp/security/anshin/attention/2020/mgdayori20200220.html

AIG AIG損保

9

手口

出典：独立行政法人情報処理推進機構『宅配便業者をかたる偽ショートメッセージに引き続き注意』より
https://www.ipa.go.jp/security/anshin/attention/2020/mgdayori20200220.html

AIG AIG損保

10

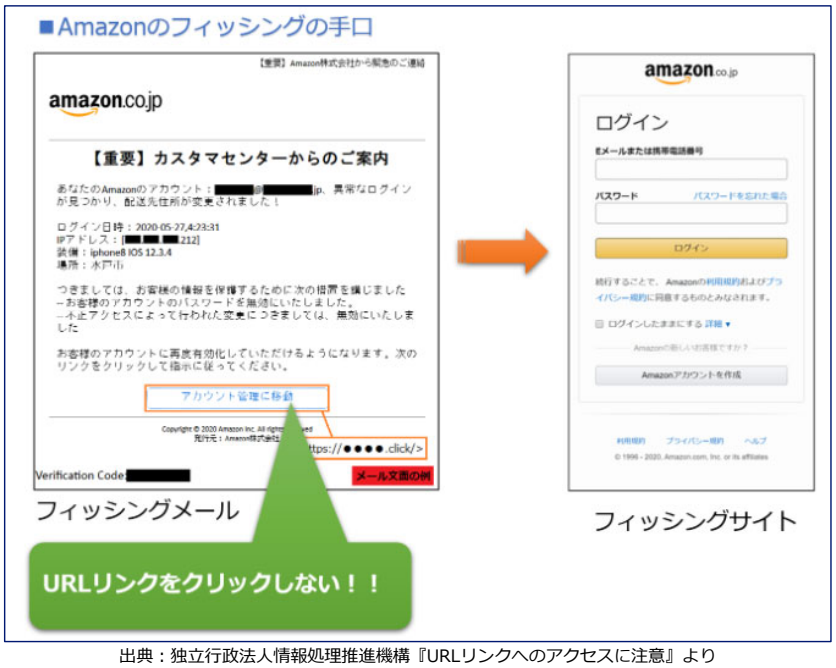
手口

出典：独立行政法人情報処理推進機構『宅配便業者をかたる偽ショートメッセージに引き続き注意』より
https://www.ipa.go.jp/security/anshin/attention/2020/mgdayori20200220.html

AIG AIG損保

11

手口



出典：独立行政法人情報処理推進機構『URLリンクへのアクセスに注意』より
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html

AIG AIG損保

12

手口

実在する金融機関、通信事業者等のログイン画面や支払いページを模した偽画面の例

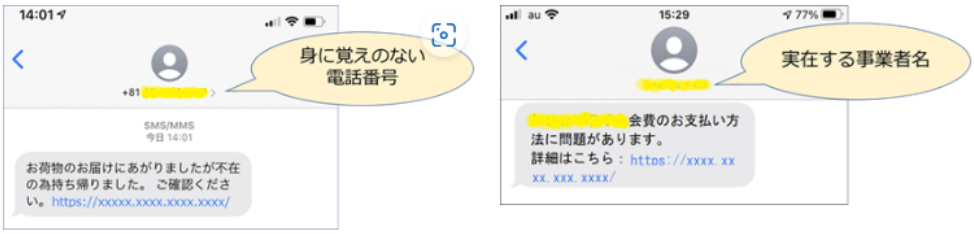
出典：警察庁『フィッシング対策』Webサイトより
https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html

AIG AIG損保

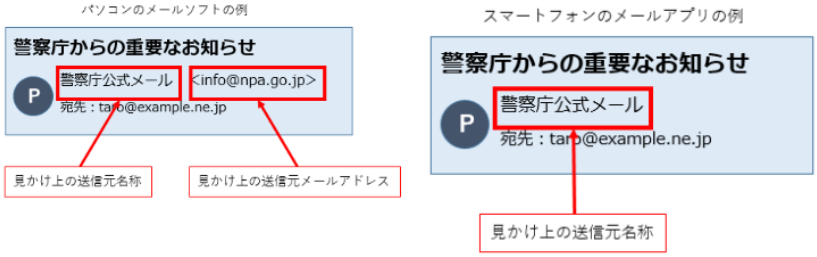
13

手口

ＳＭＳを悪用したフィッシングサイトへの誘導例



メールでの誘導例



出典：独立行政法人情報処理推進機構『URLリンクへのアクセスに注意』より
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html

AIG AIG損保

14

URLリンクから

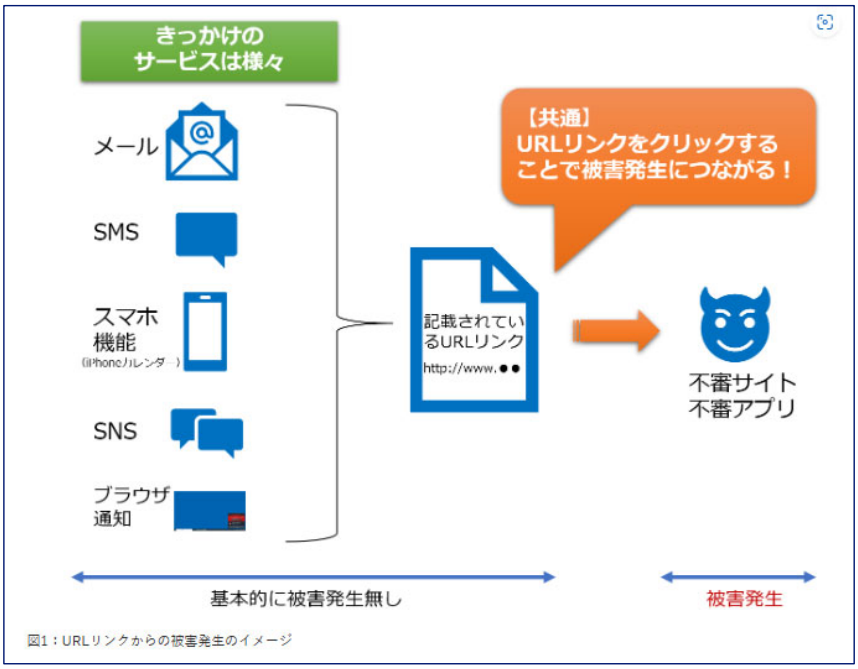


図1：URLリンクからの被害発生のイメージ

出典：独立行政法人情報処理推進機構『URLリンクへのアクセスに注意』より
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210831.html

AIG AIG損保

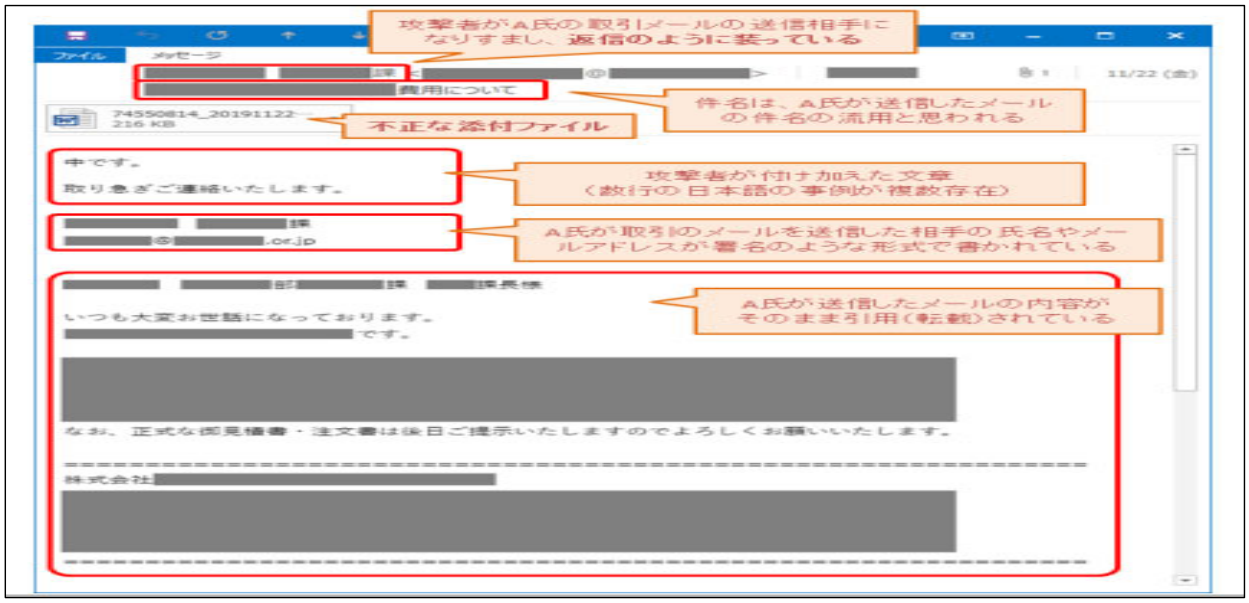
15

QRコードから

AIG AIG損保

16

Emotet（エモテット）攻撃の手口



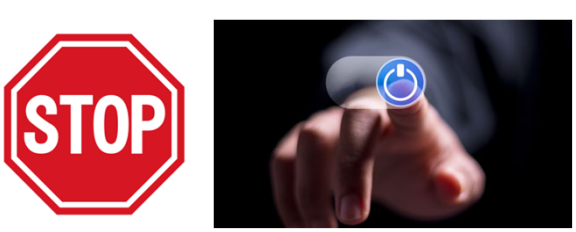
AIG損保引用：IPA『Emotet（エモテット）攻撃の手口より』 https://www.ipa.go.jp/security/emotet/attack.html

17

Q：
サイバー攻撃のおそれを感じた従業員がそのPCなどの端末に対して"すぐ行うべきこと"、"行ってはならないこと"、についてご存じですか？

マルウェア感染時に“電源オフは✕（Don't do that.）”

ネットワークから切り離し、電源オフはせず、ネットワークから隔離した上で、
専門のフォレンジック会社に調査を依頼するのが正しい初期対応です。



AIG損保

18

マルウェア感染時の対応について

●ネットワークから隔離する

感染拡大を防ぐため、**LANケーブルを抜く**、**Wi-Fiを切断する**、などしてネットワークからPC端末等を隔離。

●電源は落とさない

メモリ（RAM）に保存されている情報を失わないために、PC端末等の電源は落とさず電源供給を維持。

※電源を切るとメモリ（RAM）の内容が消去されてしまうため、インシデントが発生した際は、電源を落とさずに
メモリ内のデータを維持した上で、対応進める必要があります。

●専門家に調査依頼する

専門のフォレンジック調査会社へ調査依頼。

監理責任、説明責任

AIG AIG損保

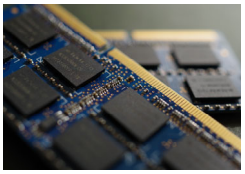
19

フォレンジック調査

フォレンジック調査は、調査対象により名称が異なり、主に以下のようなものなどがあります。

- **・ディスクフォレンジック**とは、HDDやSSDのようなストレージを調査対象とするもの。
- **・ネットワークフォレンジック**とは、パケットキャプチャやNetFlow、ProxyやFWのログのような通信情報を対象とするもの。
- **・メモリフォレンジック**とは、メモリ（RAM：ランダムアクセスメモリ）という一時的な記憶装置を調査対象とするもの

迅速に被害の範囲や影響を把握し早期に対策を講じることは、被害の拡大防止と現状把握のために、フォレンジック調査は欠かせません。



AIG AIG損保

20

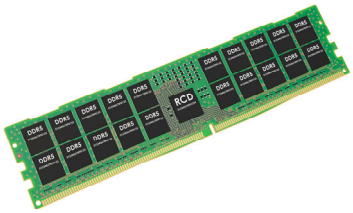
メモリフォレンジック

“メモリフォレンジック”が重要な理由は、昨今の一部のマルウェアには、HDDやSSDのようなストレージドライブに痕跡を残さないようにつくられているもの（ファイルレスマルウェア）が存在するからです。メモリフォレンジックでは、メモリに残る情報を分析し、マルウェアの実行痕跡や不正なアクティビティに関する情報を取得することなどが可能です。

しかし

メモリに保存される情報は、電源が供給されている間はデータを保持することができますが、電源が切れるとメモリのデータは消去されてしまいます。

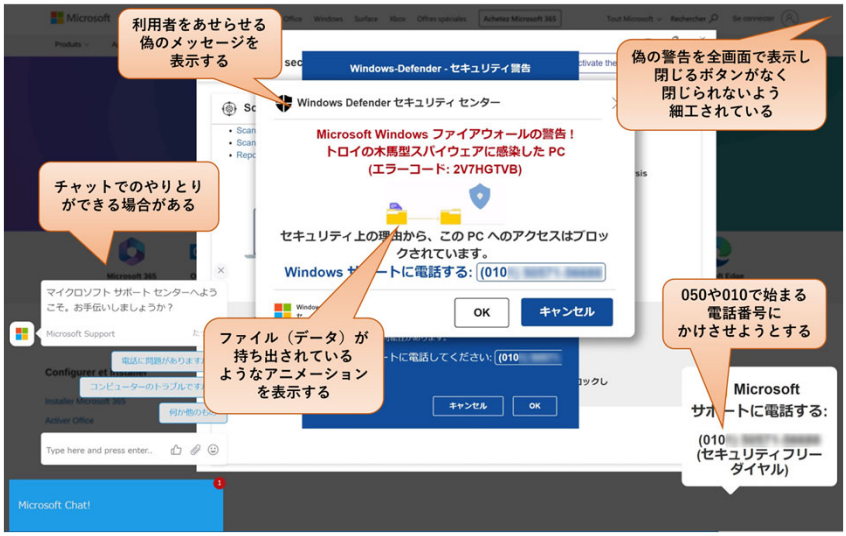
セキュリティインシデントとは、マルウェアの感染や不正アクセス、あるいは機密情報の流出など、セキュリティ上の脅威となる事象のことをいいますが、企業が事業活動を行っていくなかで、セキュリティインシデントが発生した場合は、発生した事象に関する情報の収集と分析、被害拡大などに向けた対策の実施、再発防止策の検討などを行ってください。PC端末などの取り扱いを間違えると、取引企業や社会からの信頼を失うことに繋がる可能性もあるため、ご注意ください。

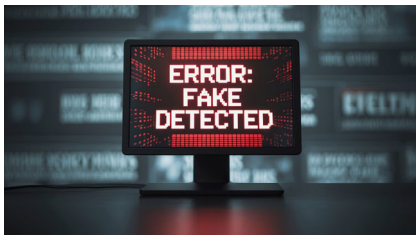


AIG AIG損保

21

サポート詐欺





出典：独立行政法人情報処理推進機構『偽セキュリティ警告（サポート詐欺）対策特集ページ』より
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

AIG AIG損保

22

サポート詐欺

図2：体験サイトで表示される偽のセキュリティ警告画面

出典：独立行政法人情報処理推進機構『偽セキュリティ警告（サポート詐欺）対策特集ページ』より
https://www.ipa.go.jp/security/anshin/measures/fakealert.html

AIG AIG損保

23

そもそも初期侵入できる場所を攻撃者たちはどう見つけてるのか？

外部から推測できるOSやアプリケーション

許可されている暗号プロトコル

漏洩済みのメールアドレス

空いているポート

アクセスできる外部公開資産

証明書の有効期限

漏洩済みのパスワード

存在する可能性のある古い脆弱性

サブドメインの名称など
から役割を推測

実際にアクセスしてみる

AIG AIG損保

24

敵から見える自分を知る　敵からどう見えるか

OSINT（オシント）って

インテリジェンス（intelligence）は、意思決定のために情報を分析して得られる知見、それを得るための活動など

OSINTとは

オープン・ソース・インテリジェンス(**O**pen **S**ource **int**elligence)の略称。

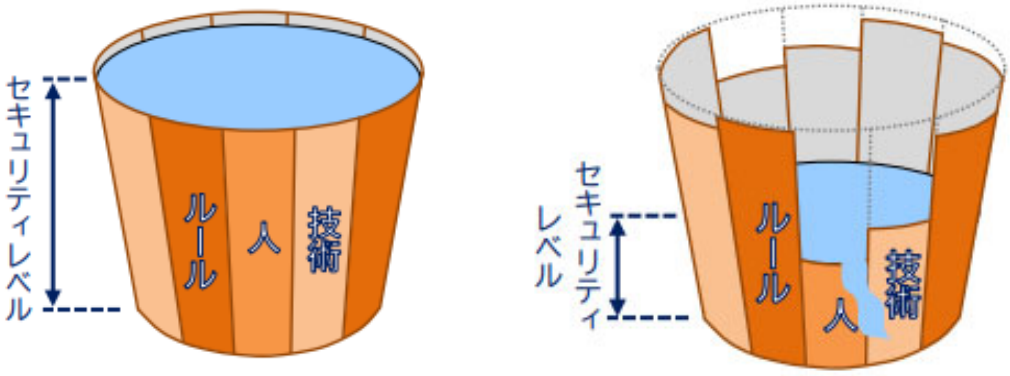
元来は、諜報活動の一種のことば。
一般に公開され利用可能な情報を情報源に、機密情報等を収集する手法。
合法的に入手できる資料を調べて突き合わせる手法。

一般に公開され利用可能な情報とは、
合法的にインターネット情報等から調べてわかる情報などで、
これを分析することにより、一見、断片的なデータから、意味を持った情報が得ることもできる

AIG AIG損保

25

取り組む



引用：総務省『テレワークセキュリティガイドライン第5版』
https://www.soumu.go.jp/main_content/000752925.pdf

AIG AIG損保

26

（会社および仲間を想像して）

情報資料にまつわるどんな最悪の事故が起こりえますか？

（自分は関与しない）

マルウェア感染

どんな経緯で

程度

いつ？

なぜ？

クリック

どんな状況

メール

同僚・仲間

（会社および仲間を想像して）

最悪の事故の後どうなっていきますか？

（自分は関与してないが）

電話

うわさ

家族

信用

仕事

会社

TV

収入

給料

AIG AIG損保

27

何が情報資産なのか

まずは洗い出し　　認識にバラツキはないか

企業にとっての情報資産（紙媒体・電子データを含む情報等）とは、
蓄積されたノウハウであり、取引先の機密情報であり、お客さまや関係者の情報。

情報漏えい、コンピュータウィルスの感染、など、情報セキュリティ事故を発生させた企業は、被害者に対する損害賠償の負担だけで なく、「情報化社会に適用できない企業」というレッテルを貼られ、社会的な信用を失墜し、企業の事業活動そのものにも大きな負の影響を受けることも。

事業の継続に関係がある
それぞれ自分ごととして認識する必要

AIG AIG損保

28

未来は、
仲間と社会と共に

ご清聴ありがとうございました。

この資料は、本講習用に作成したものです。

29