セキュリティリスクと対策

2022年3月7日13時～
DX支援セミナー

セキュリティリスクと対策

株式会社ミライコミュニケーションネットワーク
加藤

デジタルアーツ株式会社
須戸様

Copyright © Mirai Communication Network Inc.

紹介

災害対策／防犯対策専用建物

免震建物

洪水対策建物

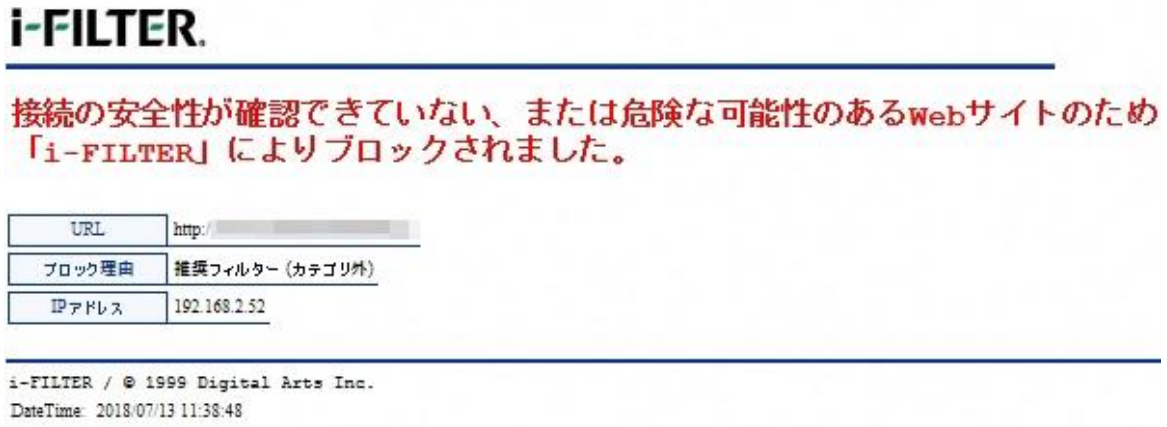
24時間365日有人監視

本人確認・ICカード・生体認証

危険なサイトへの閲覧ブロック

安心して仕事に集中できる環境

セキュリティ意識がある組織ほど採用率が高い



Copyright © Mirai Communication Network Inc.

アジェンダ

1. セキュリティリスク
2. 対策方法（対策製品のご紹介）
3. テレワークでのセキュリティ

Copyright © Mirai Communication Network Inc.

セキュリティリスク

組織にとって大切なデータの機密性・可用性・完全性をまもりましょう！

機密性

情報に対するアクセス権限を
徹底して保護・管理すること

例えば、

- **誰が見られるべき？**
- **誰が見てはいけないの？**

情報漏洩

完全性

改ざんや過不足のない
正確な情報を保持すること

例えば、

- **最新の正確なデータなの？**
- **ミスで間違った情報じゃない？**

改ざん

可用性

情報をいつでも使える状態を
保持すること

例えば、

- **HDD/CD-R等が壊れてない？**
- **間違って廃棄してしまってない？**

情報紛失

※最近もニュースになっている有名なランサムウェア被害って？
例：偽メールで真面目社員を騙して、ウイルス感染させ、アクセスできるネットワーク内全てを暗号化するウイルス
その後、「漏らされたくなければ」「暗号化解除してほしければ」と身代金要求される。

Copyright © Mirai Communication Network Inc.

事例

YAHOO! JAPAN ニュース

キーワードを入力

トップ | 速報 | ライブ | 個人 | オリジナル | みんなの意見 | ランキング

主要 | 国内 | 国際 | 経済 | エンタメ | スポーツ | IT | 科学 | ライフ | 地域

トヨタ、国内全工場が再開　セキュリティー対策で注意喚起

3/2(水) 9:59 配信 0

JIJI.COM 時事通信社

トヨタ自動車のロゴマーク（ＥＰＡ時事）

トヨタ自動車は2日朝、国内全14工場28生産ラインの稼働を再開した。

サイバー攻撃を受けた取引先部品メーカーの小島プレス工業（愛知県豊田市）でシステム障害が起きたため、1日は操業を休止した。2日以降、システムが復旧するまでは代替手段で対応し、通常通り稼働する予定という。

小島プレスでは2月26日夜、サーバーがウイルスに感染し、脅迫メッセージが確認された。同社は外部とのネットワークを遮断し、システムをすべて止めたため、部品の受発注システムも使用できなくなった。

トヨタは今回の事態を受け、直接取引がある国内外の部品、資材メーカーなど約1300社に対し、同社の規定に沿ってセキュリティー対策を徹底するよう改めて注意喚起を行った。

CAPCOM

2021 年 4 月 13 日

大阪市中央区内平野町三丁目 1 番 3 号
株 式 会 社 カ プ コ ン
代表取締役社長 辻 本 春 弘
（コード番号：9697 東証第 1 部）

不正アクセスに関する調査結果のご報告【第 4 報】

株式会社カプコンは、第三者による不正アクセス攻撃を受け、当社グループが保有する個人情報が流出しましたこと（以下「本インシデント」といいます。）を 2020 年 11 月 4 日から 2021 年 1 月 12 日にかけて公表いたしました（以下「既報」といいます。）。

この度、外部の専門企業の協力のもと進めてまいりました本インシデントに関する調査報告書を受領しましたので、当該調査結果および再発防止に向けた取り組みにつきましてあげます。なお、当社グループのシステムは現時点でほぼ復旧しており、新設の「セキュ委員会」と連携し、今後も継続的にセキュリティ、個人情報保護の強化を図ってまいりま

お客様はじめ多くのご関係先にご心配とご迷惑をおかけいたしましたことを、深くお詫ます。また、お客様はじめ関係各位のご支援に深く感謝申しあげます。

記

1．対応の経緯

2020 年 11 月 2 日	社内システムへの接続障害を確認。システムを遮断し被害状況の把握に着手
2020 年 11 月 2 日	障害の原因が，ランサムウェアの攻撃によるネットワーク上の機器に対するファイルの暗号とが判明。被害を受けた端末において「Ragnar Locker」を名乗る集団からの脅迫メッセージ大阪府警察に通報。外部企業に復旧支援を要請
2020 年 11 月 3 日	関係各国の捜査当局および個人情報保護当局を含む関係機関への連絡を順次開始
2020 年 11 月 4 日	「不正アクセスによるシステム障害発生に関するお知らせ」公表
2020 年 11 月 12 日	9 件の個人情報および一部の企業情報の流出を確認
2020 年 11 月 13 日	大手セキュリティ専門企業へ原因究明調査を打診
2020 年 11 月 16 日	「不正アクセスによる情報流出に関するお知らせとお詫び」公表 情報の流出および流出可能性について調査を継続
2020 年 12 月 21 日	外部専門家によるシステムセキュリティに関するアドバイザリー組織として、「セキュリティ監督委員会」の発足に向けた準備会を開催
2021 年 1 月 12 日	「不正アクセスによる情報流出に関するお知らせとお詫び【第 3 報】」公表
2021 年 1 月 18 日	第 1 回セキュリティ監督委員会を開催
2021 年 2 月 25 日	第 2 回セキュリティ監督委員会を開催
2021 年 3 月 26 日	第 3 回セキュリティ監督委員会を開催
2021 年 3 月 31 日	大手セキュリティ専門企業より調査報告書を受領
2021 年 3 月 31 日	大手ソフトウェア企業より報告書を受領
2021 年 4 月 13 日	本ご報告「不正アクセスに関する調査結果のご報告【第 4 報】」公表

日本経済新聞

朝刊・夕刊 | LIVE | Myニュース | 日経会社情報 | 人事ウオッチ | 日経ビジネス | お申込み | ログイン

トップ | 速報 | オピニオン | 経済 | 政治 | ビジネス | 金融 | マーケット | マネーのまなび | …

ランサム攻撃でカルテ暗号化　徳島の病院、インフラ打撃

事件・司法　＋フォローする

2021年11月12日 11:30

保存

サイバー攻撃で電子カルテによる診療が中断されている半田病院（2日、徳島県つるぎ町）＝共同

徳島県つるぎ町の町立半田病院を10月末、サイバー攻撃が襲った。病院のシステム

大企業や病院だから狙われたなんて思っていませんか？

Copyright © Mirai Communication Network Inc.

お話のみの情報

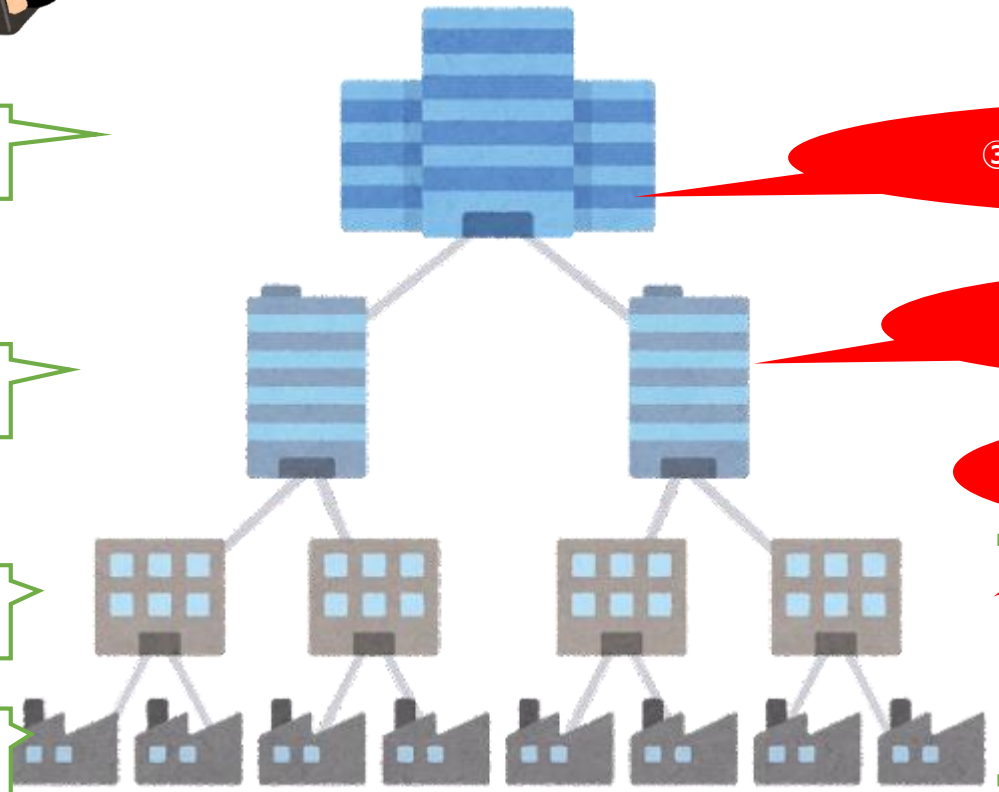
ニュースにもなりましたが。。。

Copyright © Mirai Communication Network Inc.

身近な人のフリをするために

どこが一番攻略が簡単？

企業なら？	行政なら？
T社	省庁
K社	県庁
K社支店	市町村
K社工場	外郭/委託先



③困ることをやって、お金になる行動

②攻撃または、さらに個人情報を入手し上位組織に送る。

①まずは下部組織に成り済ましたメールを上位組織に送る。

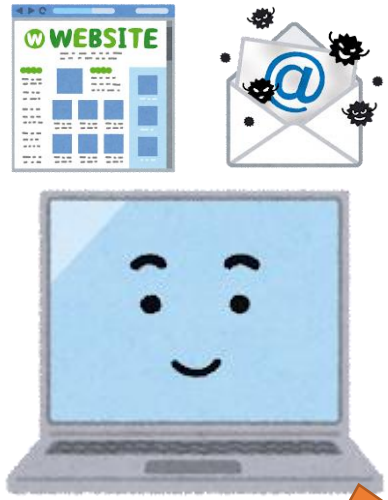
財力に余裕がなく、
セキュリティにかける費用も少ないため
脆弱性の多さや社員教育レベルの低さが狙えそう？
名刺や個人情報も簡単に入手できそう！

小さな組織でも、小規模店舗でも、攻撃価値が無さそうでも、常に攻撃にあっている！

Copyright © Mirai Communication Network Inc.

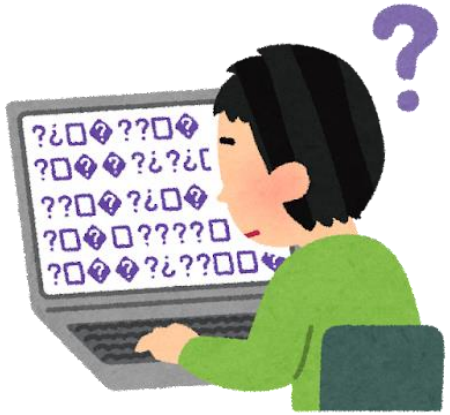
PCのウイルス対策ソフトで十分ではないの？

①Webサイトやメールから
ウイルスが持ち込まれる



入ってくるとき
に対策できれば
良いのに。

②パソコン内で実行され感染
発症、ネットワーク内感染



③ハッカー専用サイトで
共有・販売される

流出するときも
対策できれば良
いのに。

ウイルス対策ソフトはここで活躍！
しかし100%有効ではない
だから多層防御が必要！

未だにウイルス対策ソフトだけの組織多数！

Copyright © Mirai Communication Network Inc.

デジタルアーツ様から色々な情報をいただきしょう！

インターネットやメールを使うことで起きるリスク

最近の事情

対策方法

Copyright © Mirai Communication Network Inc.

Web・メールからのリスクと対策

デジタルアーツ株式会社
中部営業所
須戸

Copyright © Digital Arts Inc.

アジェンダ

1. 私たちの身近にある情報漏洩
2. 最近の攻撃手法の特徴
3. DigitalArts製品での入口・出口対策

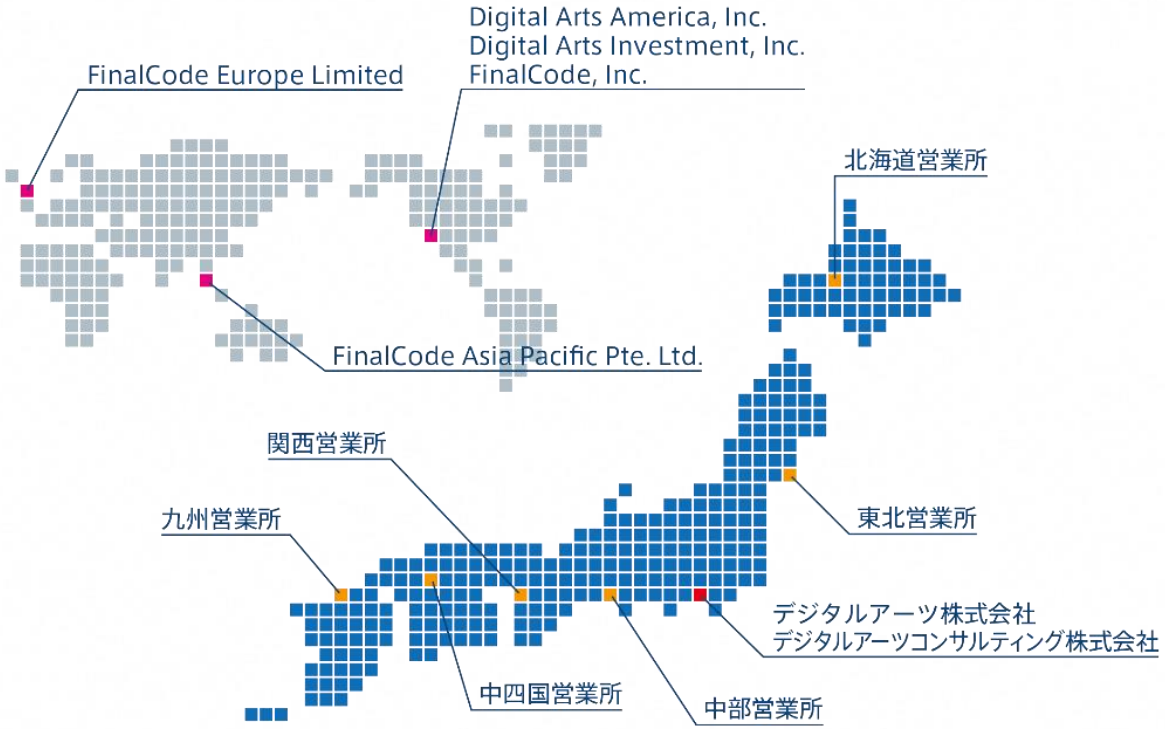
Copyright © Digital Arts Inc.

デジタルアーツ概要

「より便利な、より快適な、より安全なインターネットライフに
貢献していく」 企業として、これからも成長しつづけます。

商号	デジタルアーツ株式会社　Digital Arts Inc.
設立	平成7年（1995年）6月21日
資本金	7億1,359万0,262円
代表	代表取締役社長　道具　登志夫
株式	東京証券取引所 市場第一部 （証券コード：2326）
決算期	3月31日
業務内容	インターネットセキュリティ関連ソフトウェアおよび アプライアンス製品の企画・開発・販売

http://www.daj.jp/
info@daj.co.jp
Facebook　デジタルアーツ株式会社



Copyright © Digital Arts Inc.

デジタルアーツの製品ラインナップ

	オンプレミス	DigitalArts@Cloud
Webセキュリティ	外部攻撃対策からWebフィルタリングまで、ひとつの製品で実現 i-FILTER	i-FILTER@Cloud
メールセキュリティ	内部からの情報漏洩対策と外部からの攻撃メール対策の両方 を実現 m-FILTER	m-FILTER@Cloud
ファイルセキュリティ	ファイルが作成された瞬間から"自動で守り”、渡した後でも”あとから消せる” FINALCODE	FINALCODE@Cloud
コミュニケーションツール		安全・スピーディな コミュニケーションを実現 Desk@Cloud

Copyright © Digital Arts Inc.

アジェンダ

1 私たちの身近にある情報漏洩

2 最近の攻撃手法の特徴

3 DigitalArts製品での入口・出口対策

Copyright © Digital Arts Inc.

私たちの身近にある情報漏洩と脅威

従業員による
内部不正

Emoteに感染

メール
宛先ミス

ランサムウェアに
感染

CCとBCCの
設定間違い

改竄サイトへ
アクセス

個人アドレスへの
転送

Copyright © Digital Arts Inc.

メールによる情報漏洩の種類

メールによる情報漏洩は**「過失」**によるものと**「故意」**によるものの**2種類**ある

「過失」による情報漏洩

「過失」による情報漏洩とは、
利用者の**“ヒューマンエラー”**
によって起こってしまう情報漏洩

例えば、

- **宛先を間違えてしまう**
- **誤った添付ファイルを送ってしまう**
- **宛先をBccとするはずがTo/Ccにしてしまう**

「故意」による情報漏洩

「故意」による情報漏洩とは、
利用者が**“悪意をもって”**
起こってしまう情報漏洩

例えば、

- **競合他社企業にとって有益となる情報を持ち出す**
- **金銭目的での顧客情報持ち出し**
- **自宅で業務するための情報持ち出し**

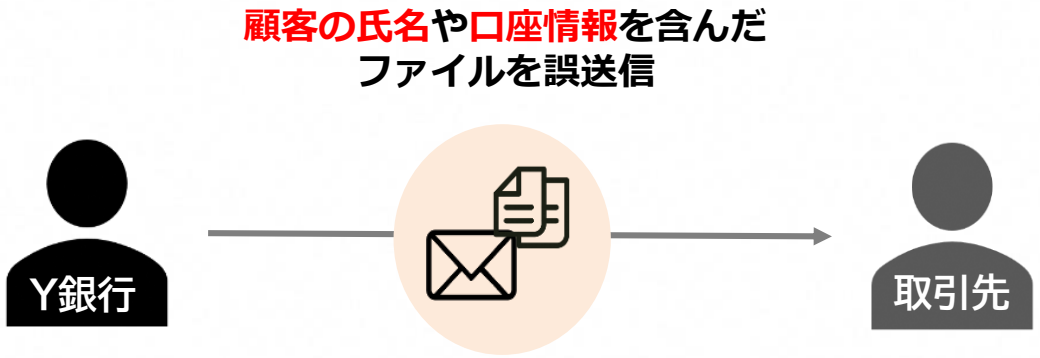
Copyright © Digital Arts Inc.

過失による情報漏洩事例

2021年 4月

Y銀行でメール誤送信 取引先に顧客情報を含んだファイルを流出した事例

顧客情報が含まれたファイルを
取引先に誤送信したことにより、
41,729件の顧客の氏名や
口座情報が流出



幸いにも暗証番号の流出はなかった為、大事には至らなかったものの、
たった一通のメール誤送信で巨額の補償が発生する大事件に発展する可能性がある

- インシデントの事後の対応
- 信用失墜 ブランドイメージのきそん
- 営業中止などの事業への影響

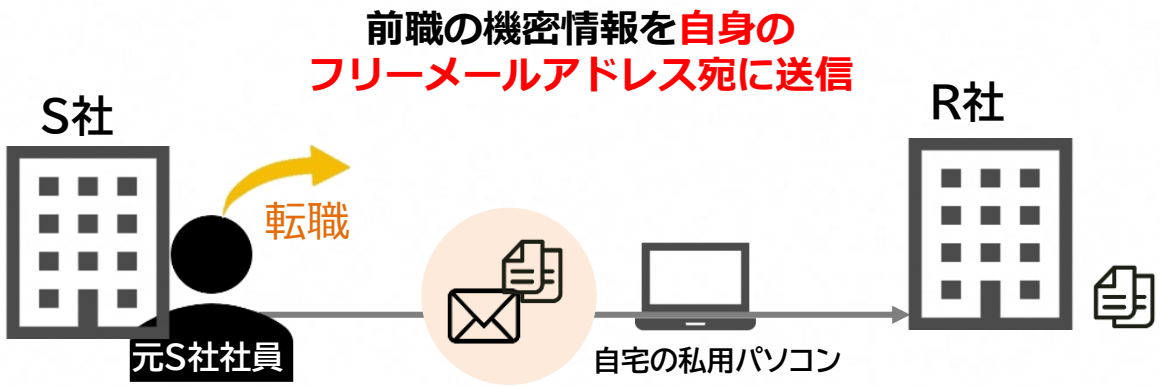
Copyright © Digital Arts Inc.

故意による情報漏洩事例

2021年 1月

転職した元社員が前職の機密情報を自身のメールにて情報漏えいした事例

S社からR社へ転職した元社員が
前職の機密情報を自身のフリーメール
アドレスに送信し、情報を持ち出した。



元社員が転職後にS社の調査で機密情報を送信した痕跡を確認
S社では持ち出した機密情報の利用停止と10億円規模の訴訟を提起

インシデントの事後の対応

損害賠償

事業への影響

Copyright © Digital Arts Inc.

フィッシングサイト

フィッシングサイトへ誘導するメールを送信

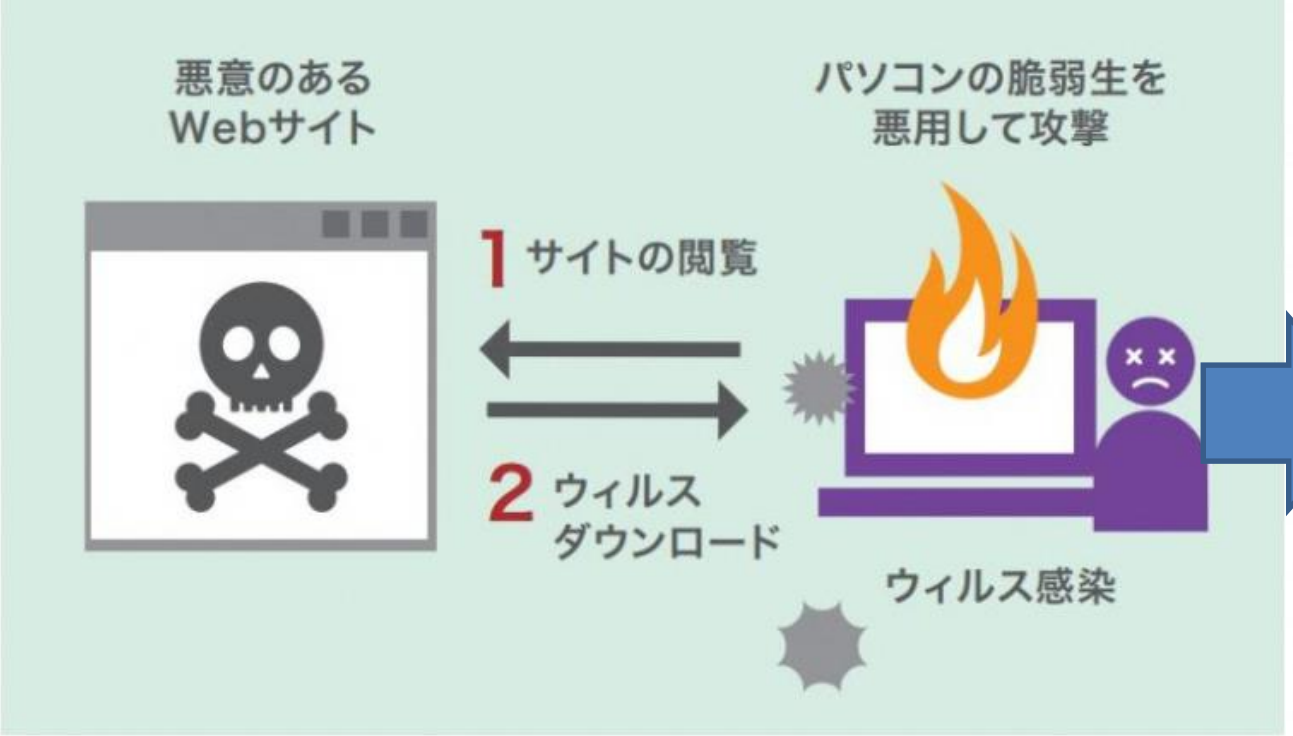
カード番号などを入力させる

個人情報搾取成功！

ユーザーID・パスワード・銀行口座情報など、大切な情報が流出！

Copyright © Digital Arts Inc.

ドライブ・バイ・ダウンロード



改ざんされたサイトをクリックした
瞬間、悪意のある
不正プログラムをダウンロード！

気付かないまま
ウィルス感染して、大切な情報を
外部に漏洩させてしまう危険も

Copyright © Digital Arts Inc.

アジェンダ

1 私たちの身近にある情報漏洩

2 最近の攻撃手法の特徴

3 DigitalArts製品での入口・出口対策

Copyright © Digital Arts Inc.

ランサムウェアによる被害

ランサムウェアによる被害が、現在最も重大な脅威！

■IPA「情報セキュリティ10大脅威 2022」

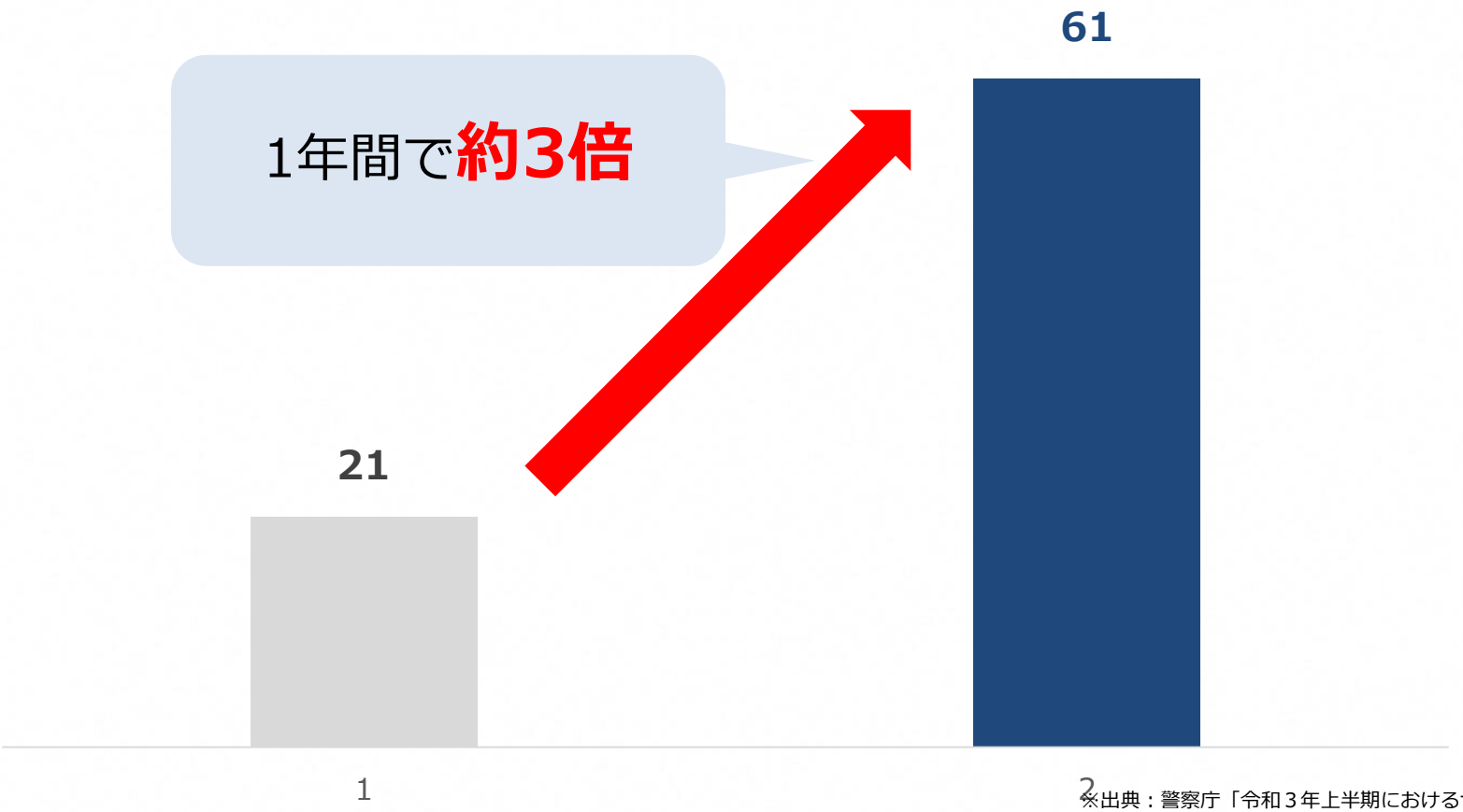
2022順位	概要	2021順位
1位	**ランサムウェアによる被害**	**1位**
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
5位	内部不正による情報漏えい	6位

※出典：IPA　https://www.ipa.go.jp/security/vuln/10threats2022.html
※上位5位までを抜粋

Copyright © Digital Arts Inc.

ランサムウェアの被害件数

ランサムウェアの被害件数は急増中！



※出典：警察庁「令和３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」4P
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_kami_cyber_jousei.pdf

Copyright © Digital Arts Inc.

ランサムウェアの主な侵入経路

攻撃者

VPN

VPNの脆弱性を狙い、ゼロディ攻撃などを仕掛けて侵入

メール

標的型メールやばらまき型メールにより、感染・侵入
また、二次感染（三次感染）させる機能を持った
マルウェアへの感染からランサムウェアが侵入する
ケースもある

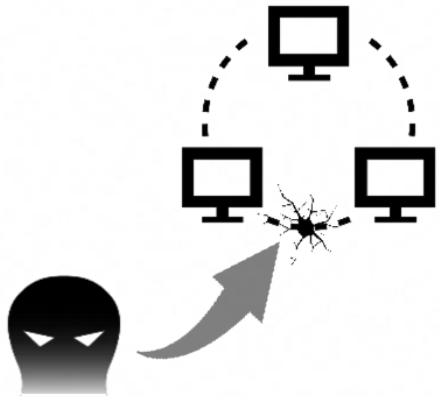
リモートデスクトップ

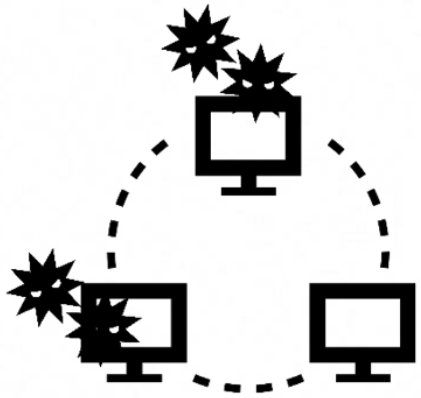
リモートデスクトップのアカウントを
不正入手（認証突破）して侵入

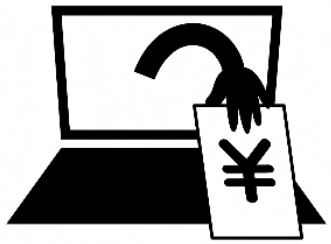
Copyright © Digital Arts Inc.

VPN機器からの侵入例

STEP 1	STEP2	STEP3	STEP4
VPNサーバの脆弱性から内部NWに侵入	ログやキャッシュ等からアカウントデータを取得	ネットワークを横移動しランサムウェアを拡散	ランサムウェア攻撃を実施





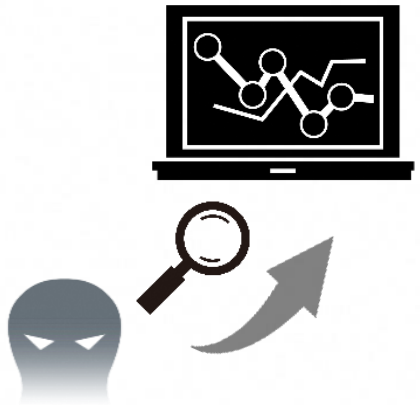


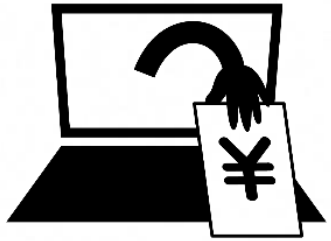
※出典：Tech＋
https://news.mynavi.jp/techplus/article/20200109-951531/

Copyright © Digital Arts Inc.

リモートデスクトップからの侵入例

STEP 1	STEP2	STEP3	STEP4
リモートデスクトップが脆弱な会社情報を取得	リモートデスクトップの脆弱性から不正ログイン	管理者情報の取得or権限の昇格の実施	ランサムウェア攻撃を実施



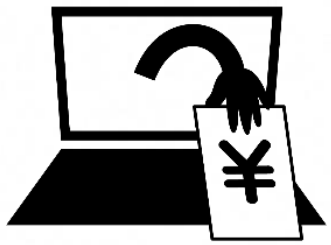


※出典：日経クロステック
https://xtech.nikkei.com/atcl/nxt/column/18/00598/121500146/

Copyright © Digital Arts Inc.

メールからの侵入例

STEP 1	STEP2	STEP3	STEP4
本文のURL/添付ファイルに不正プログラムを挿入	「標的型」「ばらまき型」メールなどで感染、侵入	管理者情報の取得しデータを窃取	ランサムウェア攻撃を実施



Copyright © Digital Arts Inc.

代表的なランサムの事例1（VPN）

VPNの脆弱性を突かれ、ランサムウェアに感染

■被害を受けた企業

・国内大手ゲームソフト会社

■流出した情報

・取引先や退職者など**1万6000人の個人情報**や、顧客や取引先**約39万人の個人情報**が流出。

■攻撃の経緯

・同社海外法人が保有していた**旧型VPNの脆弱性**を突かれ、
社内ネットワークに侵入された。

■攻撃への対応

・攻撃者は身代金として**11億円**を要求。同社は支払いを拒否。
・攻撃の影響で、一部ログを喪失したため、**2週間以上復旧に時間を要した。**

※出典：日経クロステック
https://xtech.nikkei.com/atcl/nxt/column/18/00989/112400040/

Copyright © Digital Arts Inc.

代表的なランサムの事例2（リモートデスクトップ）

リモートデスクトップ経由で、攻撃者が侵入

■被害を受けた団体
・国内某町

■流出した情報
・なし

■攻撃の経緯
・同町が提供するスマホアプリの保守再委託先の、脆弱性のある端末が不正アクセスされ**リモートデスクトップ**経由で侵入された。その後管理者情報を窃取される。
・その後、ランサムウェアが実行され、**データが暗号化されアプリが利用不可**に。

■攻撃への対応
・攻撃から**1週間**の間、アプリが使用できない状態に。
・代替の環境をクラウド上に構築し、復旧。

※出典：日経クロステック
https://xtech.nikkei.com/atcl/nxt/column/18/00598/121500146/

Copyright © Digital Arts Inc.

代表的なランサムの事例3（メール）

偽装メール感染、サーバーの9割以上が暗号化被害

■被害を受けた団体
・国内大手建設会社

■流出した情報
・サーバーの**9割**以上が**暗号化被害**。サーバーに保存した情報の一部が外部のサイトに**公開**

■攻撃の経緯
・社員PCに**取引先企業を装ったメール**が届き、メールを開封したことでウイルスに感染、システム内に侵入されたことが明らかに。
・認証サーバーが特定され**管理者権限**が奪われたことで攻撃を受けるに至った。

■攻撃への対応
・全社員使用 PC の切断、別環境のメールシステムを契約
・メールサーバーの被害が大きく、復旧に**2カ月近く時間を要した**

※出典：日経クロステック
https://xtech.nikkei.com/atcl/nxt/mag/nnw/18/031800050/111800021/

Copyright © Digital Arts Inc.

日本国内での主なランサムウェア被害事例

企業・団体	被害概要
A団体	データが一部暗号化される被害を受け、 事務局内のサーバー、PCに一時アクセスできない状況が発生
B社	サイバー攻撃によりバックアップを含む大量のデータが 暗号化想定するBCPでは立ち行かなくなる事態が発生
C社	取引先偽装メールで感染し、管理者権限奪われ、 サーバーの9割以上が暗号化被害
D社	サーバーの保存情報の暗号化やアクセスログの抹消に加えて、 会社情報や個人情報が流出
E病院	メインサーバーのみならず、バックアップ用のサーバーも 感染電子カルテは閲覧できず、診療費計算も不能に

出典： 各団体、各社に関する公表情報よりデジタルアーツ作成

DD-11153-001
Copyright © Digital Arts Inc.

ランサムウェアの傾向

ランサムウェアは攻撃者にとって利益が大きく組織的にビジネス化されてきている

組織化

集団によっては成果報酬モデルなどが構築され、まるで企業組織のように活動が広まっている

身代金請求

機密情報窃取と暗号化を行い二重脅迫により身代金を請求する

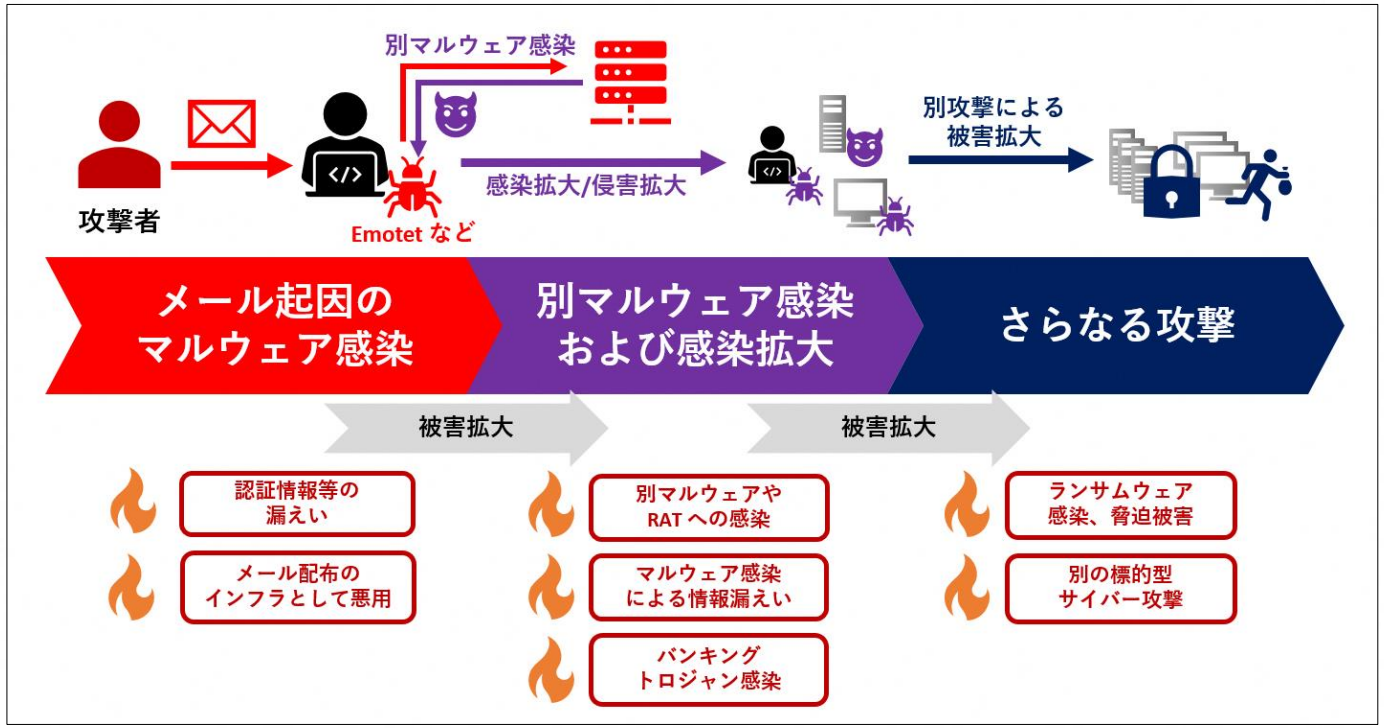
情報売買

攻撃者同士がシステムへ侵入するための窃取情報を売買

今後ますます増加の傾向！ランサムウェア対策が急務に！！

DD-11153-001
Copyright © Digital Arts Inc.

Emotet（2020年12月）

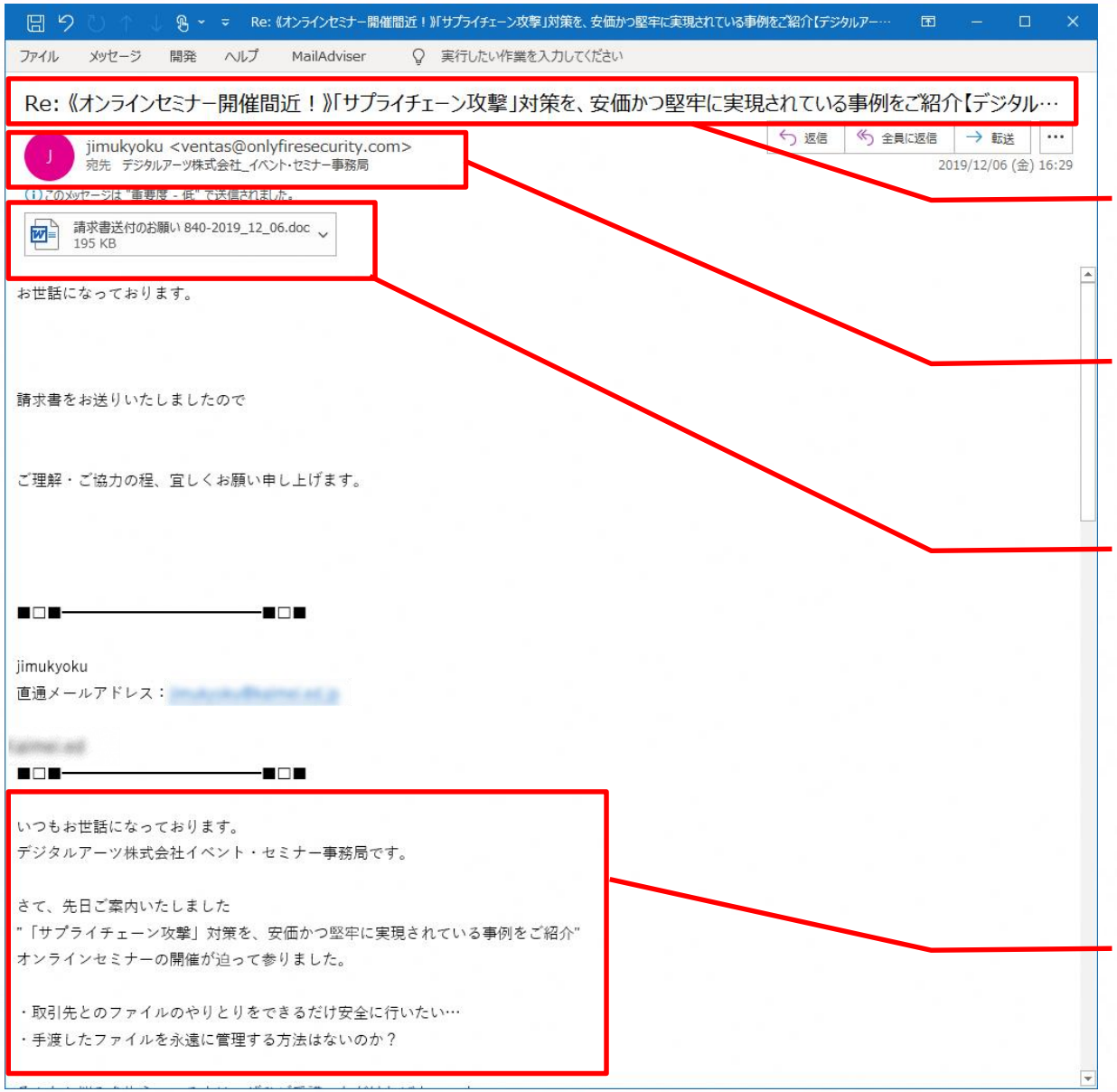


- ✓ 初期バージョンは銀行情報を窃取することを目的としたトロイの木馬
- ✓ その後進化を遂げTrickBot、Qbotと言われるマルウェアに感染させる
- ✓ 最終的には口座情報等を窃取され金銭的被害に

出典：JPCERT https://www.jpcert.or.jp/newsflash/2020122201.html

Copyright © Digital Arts Inc.

テレワーク環境を狙った攻撃 – Emotet



Re: 《オンラインセミナー開催間近！》「サプライ・・・
弊社から送信したオンラインセミナー案内の件名

jimukyoku <ventas@onlyfiresecurity.com>
ニックネームは、元メールの送信先のアカウント部
メールアドレスは、全く関係のないもの

請求書送付のお願い 840-2019_12_06.doc
添付：古い形式のマクロ付きWordファイル（*.doc型式）

本文：弊社から送信した本文をそのまま引用し返信の形式

Copyright © Digital Arts Inc.

テレワーク環境を狙った攻撃－COVID-19関連

Zoom、Webex、TeamsなどのWeb会議のInvitationメールを装ったメール見受けられる

トピック：Emergency meeting
緊急性の高い文言の記載

Zoom ミーティングに参加する
https://zxxm.us/j/123456789

Web会議へのURLを模した記載
短縮URLやリダイレクトURLが利用されることが多くURLだけで判別は難しい

Emotetに感染！

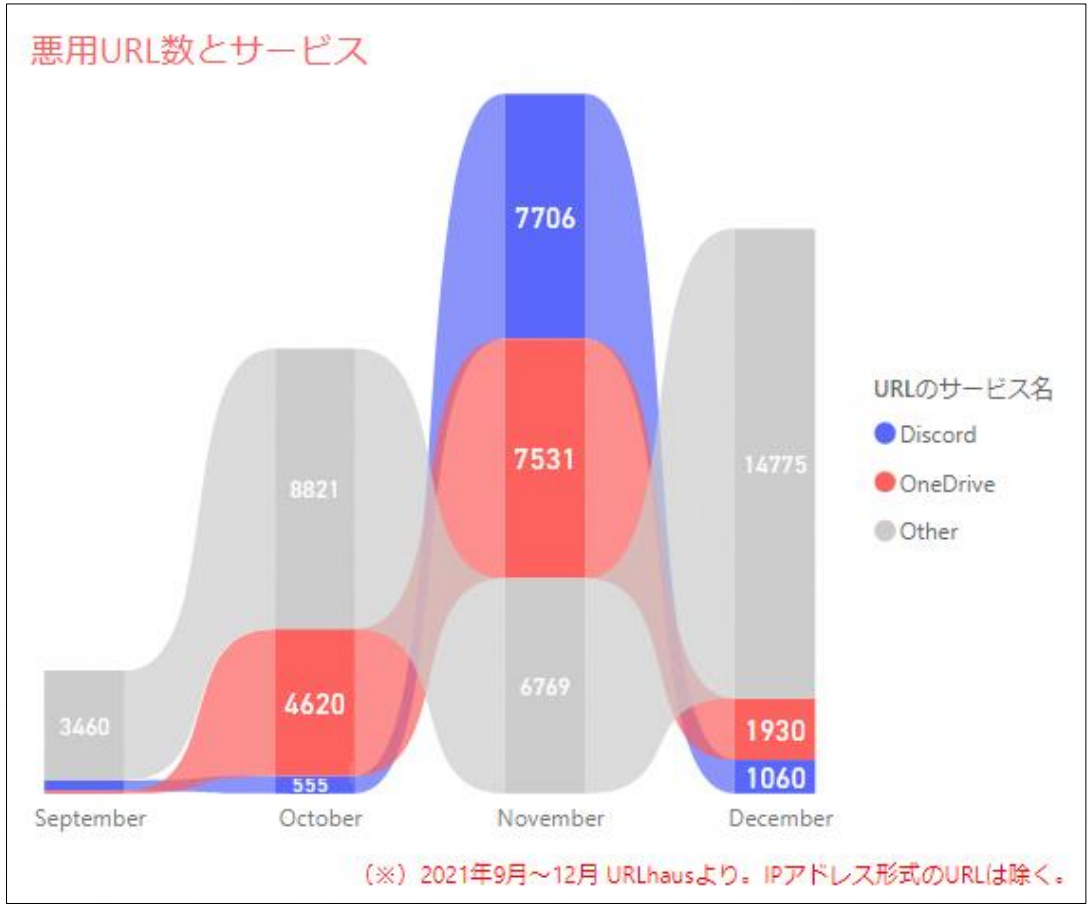
Copyright © Digital Arts Inc.

マルウェアに悪用されるファイル共有サービス

正規のファイル共有サービスにマルウェアを仕込んだファイルをアップロードし、その悪用URLをメールやメールの添付ファイルで拡散することで、マルウェア感染を広げるという攻撃が増えています。

・Discordを悪用したマルウェアは
【Dridex】が9割以上を占める

・OneDriveで悪用されるドメインは正規のもの
api.onedrive.com/onedrive.live.com/files.1drv.com/1drv.msなど



POINT

近年、PPAP廃止の動きが加速し、ファイル共有サービスを利用する企業が増えていると思います。

正規サービスのURLだからといって単純に安心はできません。

出典：デジタルアーツ　マルウェアに悪用されるファイル共有サービスに要注意
https://www.daj.jp/webtopics/133/

Copyright © Digital Arts Inc.

一般的な対策方法

- ネットワーク機器・OSの**脆弱性パッチの迅速な適用**
- アンチウイルス等の**定義ファイルは常に最新の状態**をキープ
- 管理者情報の窃取を防ぐため、**不審なメールは開かない**
- メールに添付された**怪しいWebサイトにはアクセスしない**

Copyright © Digital Arts Inc.

対策のポイント

- ネットワーク機器・OSの脆弱性パッチの迅速な適用
- アンチウイルス等の定義ファイルは常に最新の状態をキープ

定義ファイル・パッチ自動更新で対策可能

- 管理者情報の窃取を防ぐため、不審なメールは開かない
- マルウェア感染の恐れがある、危険なWebサイトにはアクセスしない

目視での判断には限界がある

Copyright © Digital Arts Inc.

アジェンダ

1 私たちの身近にある情報漏洩

2 最近の攻撃手法の特徴

3 DigitalArts製品での入口・出口対策

Copyright © Digital Arts Inc.

デジタルアーツ製品による対策

感染対策

メールの添付ファイルからの感染への対策

- なりすまし対策
- メール内のURL確認
- 添付ファイル確認
- Zipパスワード強制検査
- 誤送信対策
  BCC自動変換

m-FILTER

メールのURLアクセスによる感染への対策

- 悪性/改ざんサイトへのアクセスをブロック
- 不適切なサイトブロック
- 不正ダウンロード対策
- 未知の脅威通信からも守る

i-FILTER

情報窃取対策

ファイルの不正持ち出しへの対策

- 自動暗号化による情報窃取ブロック
- ファイル追跡/送った後から遠隔削除も可能

FINALCODE

Web経由でのファイル持ち出しへの対策

- Webへのアップロードを制御
- 会社利用のストレージのみ利用可能
- 不正なアップロードの調査や分析も可能

i-FILTER

DD-11153-001
Copyright © Digital Arts Inc.

デジタルアーツ製品によるランサムウェア対策①

攻撃者

対策可能

VPN

VPNの脆弱性を狙い、ゼロディ攻撃などを仕掛けて侵入

メール

標的型メールやばらまき型メールにより、感染・侵入
また、二次感染（三次感染）させる機能を持った
マルウェアへの感染からランサムウェアが侵入する
ケースもある

リモートデスクトップ

リモートデスクトップのアカウントを
不正入手（認証突破）して侵入

DD-11153-001
Copyright © Digital Arts Inc.

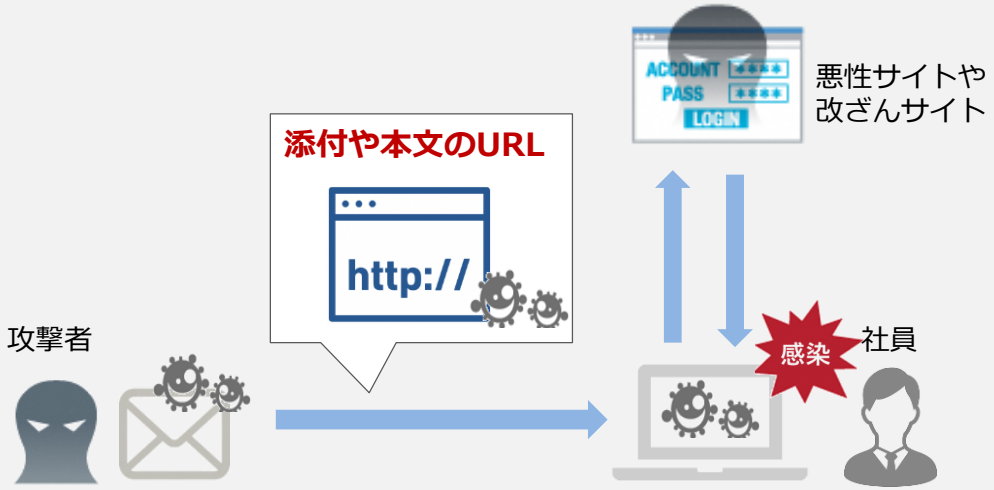
メール攻撃の注意すべきポイント

メールの「添付ファイル」や「URLリンク」に潜む感染原因を対策することが必要！

例1 メールの添付ファイルから マクロが実行されることで感染

マクロ実行後にマルウェアを
ダウンロードされて感染

例2 メールに記載のURL（悪性サイトや 改ざんサイト）にアクセスさせて感染



悪性サイトや改ざんサイトに
アクセスさせて感染

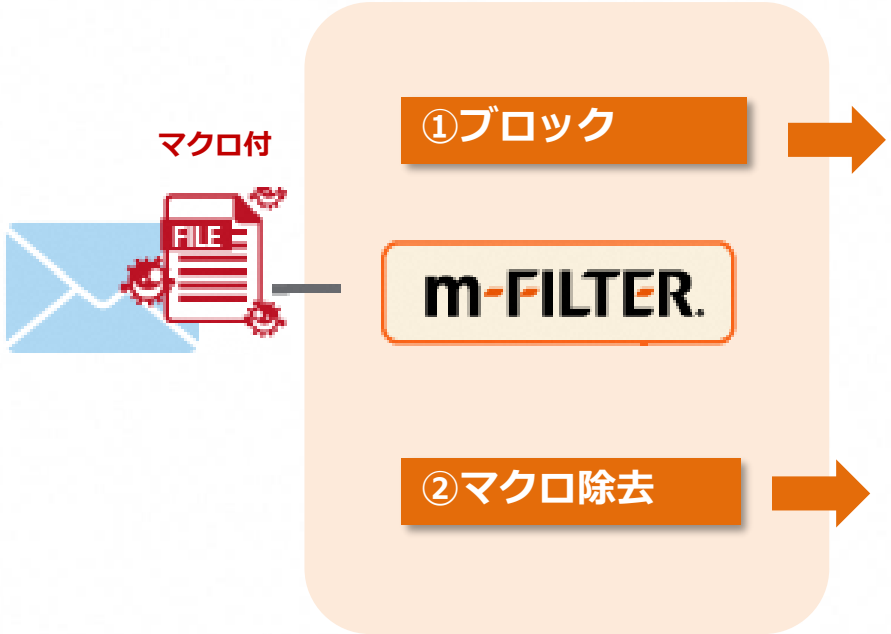
DD-11153-001
Copyright © Digital Arts Inc.

メールの添付ファイルからの感染への対策

m-FILTER

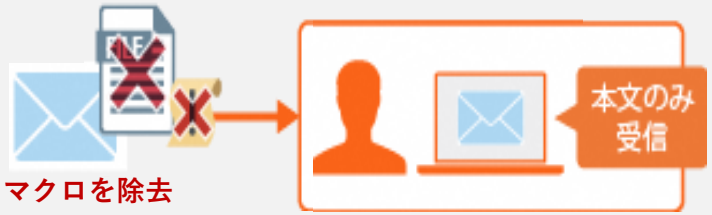
**添付ファイルにマクロを含むメールは、
ブロックまたは、マクロを除去することが可能です。**

メールの運用方法に合わせてブロックやマクロ除去の設定が可能！また、添付ファイルにマクロを含むメールを受信する、しないをグループや部署単位で設定することも可能です。



添付ファイルにマクロを含むメール自体をブロック可能

添付ファイルのマクロを除去し、無害化してから配信可能



DD-11153-001
Copyright © Digital Arts Inc.

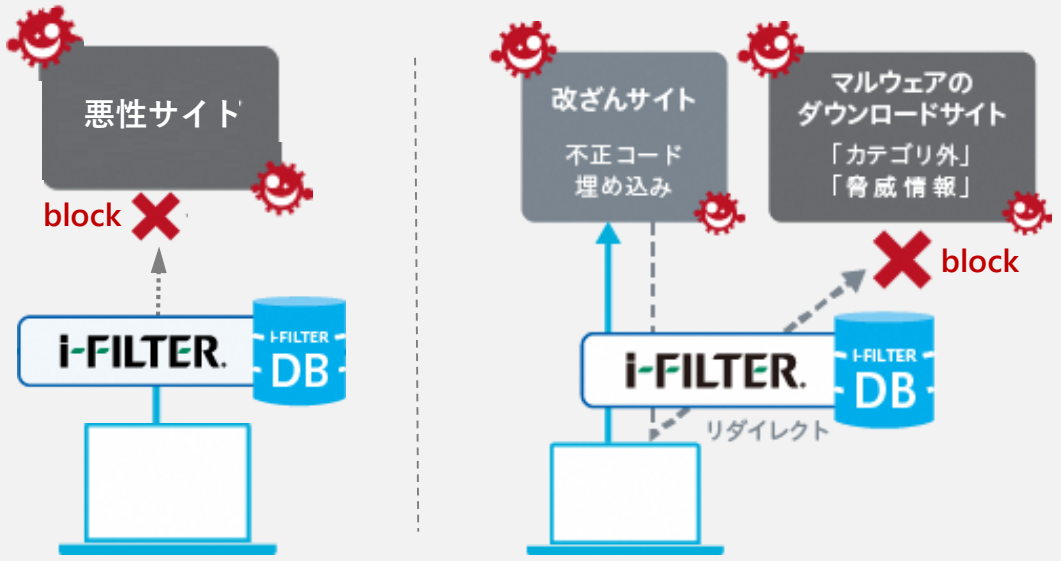
メールに記載のURLアクセスによる感染への対策

i-FILTER

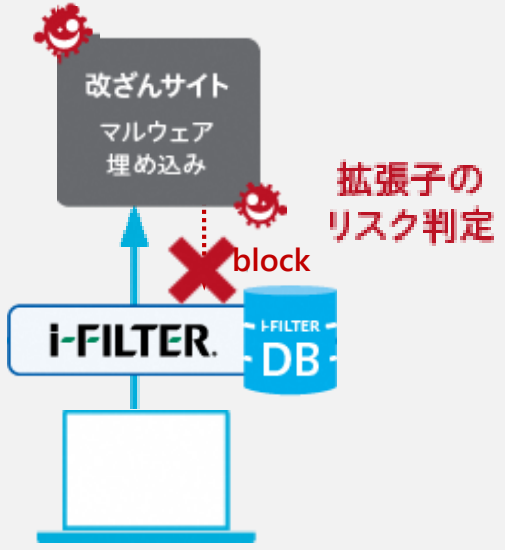
悪性サイトや改ざんサイトへアクセスした場合でも、
ランサムウェア感染をブロックすることが可能です！

メール運用上、「m-FILTER」を導入していても添付ファイルにマクロを含むメールを受信しないといけない時は、
「i-FILTER」を使えば、悪性サイトや改ざんサイトへのアクセスの段階でブロックが可能！

悪性サイトへのアクセスはブロック
改ざんサイトからのリダイレクトもブロック可能



改ざんサイトからの
直接マルウェアダウンロードもブロック！



DD-11153-001
Copyright © Digital Arts Inc.

デジタルアーツ製品によるランサムウェア対策②

DigitalArts

端末やファイルを暗号化

業務に必要な機密情報のファイルを
暗号化し、事業継続を困難にさせる

ロックを解除して
欲しいならお金を払え

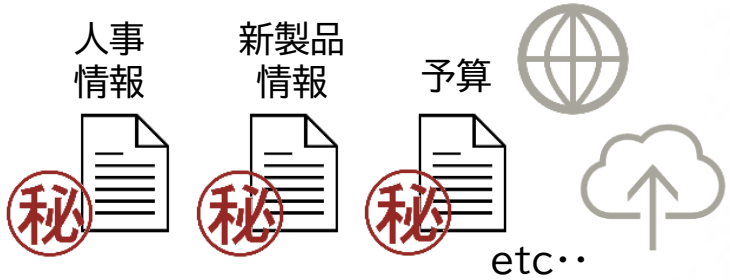
二重脅迫

攻撃者

対策可能

機密情報窃取

企業の損失に関わる機密情報を
インターネット上に公開し脅迫



外部に情報を公開されたく
なければお金を払え

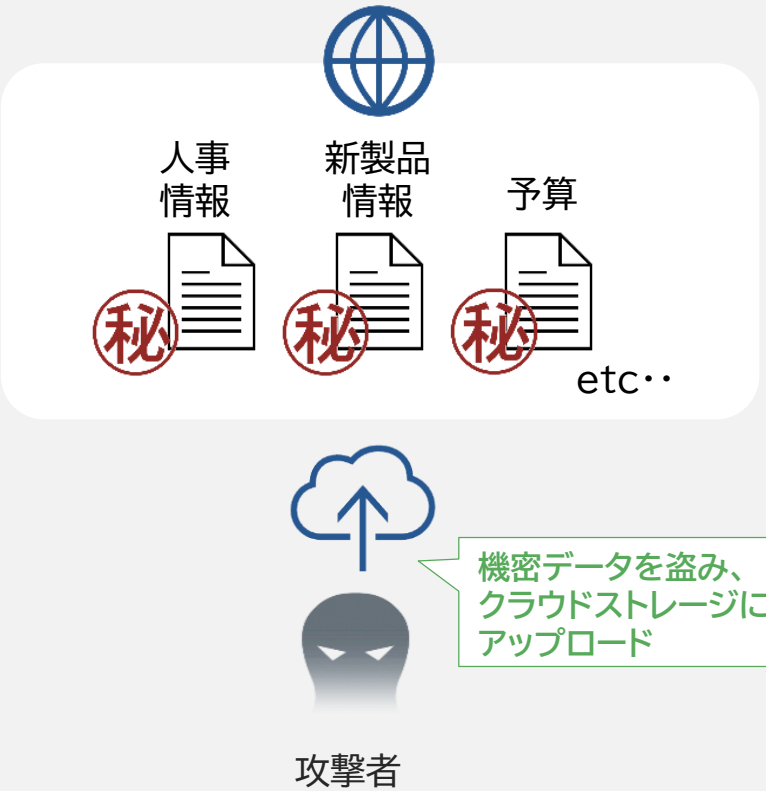
DD-11153-001
Copyright © Digital Arts Inc.

情報窃取対策の注意すべきポイント

DigitalArts

情報窃取

インターネット上に機密情報を公開



人事情報などの機密情報を窃取し、脅迫！
身代金が支払われない場合には情報を外部に公開！

重要な機密情報を守るには・・・

対策

**重要ファイルは事前に
暗号化をしておくことが必要**

デジタルアーツ製品で対策可能！

- ファイル自動暗号化
- ファイルの追跡・閲覧権限の削除
- Webへのファイルアップロードの制御、調査・分析

DD-11153-001
Copyright © Digital Arts Inc.

ファイル自動暗号化

FINALCODE

重要ファイルはフォルダで自動暗号化！

フォルダごとに暗号化条件の設定が可能。管理者がフォルダを作成し、社員はいつも通りにフォルダーへファイルを保存するだけで機密ファイルを守ることができます。また、閲覧・編集・印刷・コピーの可否など人や部署ごとに細かに権限を設定することで、情報漏洩リスクを低減します。

管理者にて暗号化条件を設定した
フォルダを作成

ファイルをフォルダーへ保存するだけで
重要ファイルを自動で暗号化！

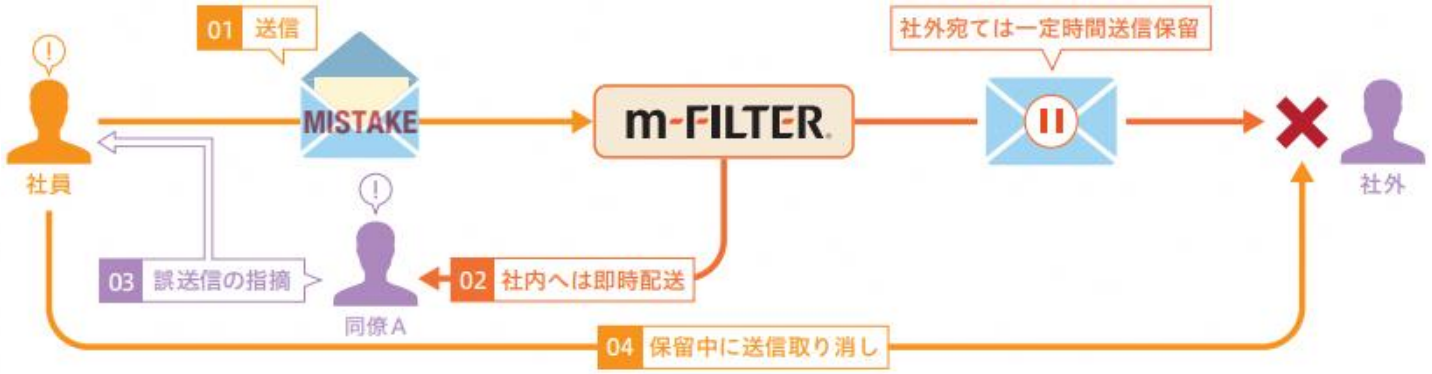
DD-11153-001
Copyright © Digital Arts Inc.

誤送信対策も同時に可能

送信時のフィルタリングルールを設定することで、誤送信対策に

送信ディレイ（時間差送信）

一定期間、送信メールを滞留させます。滞留中であれば、誤送信などの場合に送信を取り消すこともできます。



添付ファイル自動暗号化

添付ファイルを自動でパスワード付きZIPファイルに変換して送信できます。

上長承認/強制Bcc化送信

多数の宛先、複数のドメインが宛先にある場合に、To、CcをBccに強制的に変換してメールを送信することが可能です。

Copyright © Digital Arts Inc.

まとめ

攻撃者は、手法を変えて攻めてきます
社員は人間ですから間違いを起こす可能性があります

狙われやすいメールと、出口になるインターネットのセキュリティを見直しませんか？

- **安全なメール、Webサイトのみへアクセスできる環境**
- **誤送信や内部不正をシステムでブロック**
- **万が一の場合に備えて、ファイルを高度な技術で暗号化**

Copyright © Digital Arts Inc.

私たちの身近にある情報漏洩

DigitalArts

従業員による
内部不正

Emotet感染

メール
宛先ミス

ランサムウェアに
感染

CCとBCCの
設定間違い

改竄サイトへ
アクセス

個人アドレスへの
転送

Copyright © Digital Arts Inc.

- 本書 は2022年2月現在の情報に基づいて作成しております。（※記載内容は変更される場合があります）
- 本書は、弊社「i-FILTER」、「m-FILTER」および関連製品の導入検討のためにのみご利用いただき、他の目的のためには使用しないようご注意ください。
- デジタルアーツ、DIGITAL ARTS、i-FILTER、m-FILTER、D-SPAはデジタルアーツ株式会社の登録商標です。
- FinalCode、Desk@Cloudはデジタルアーツグループの登録商標です。
- その他、本書に記載されている各社の社名、製品名、サービス名およびロゴ等は、各社の商標または登録商標です。

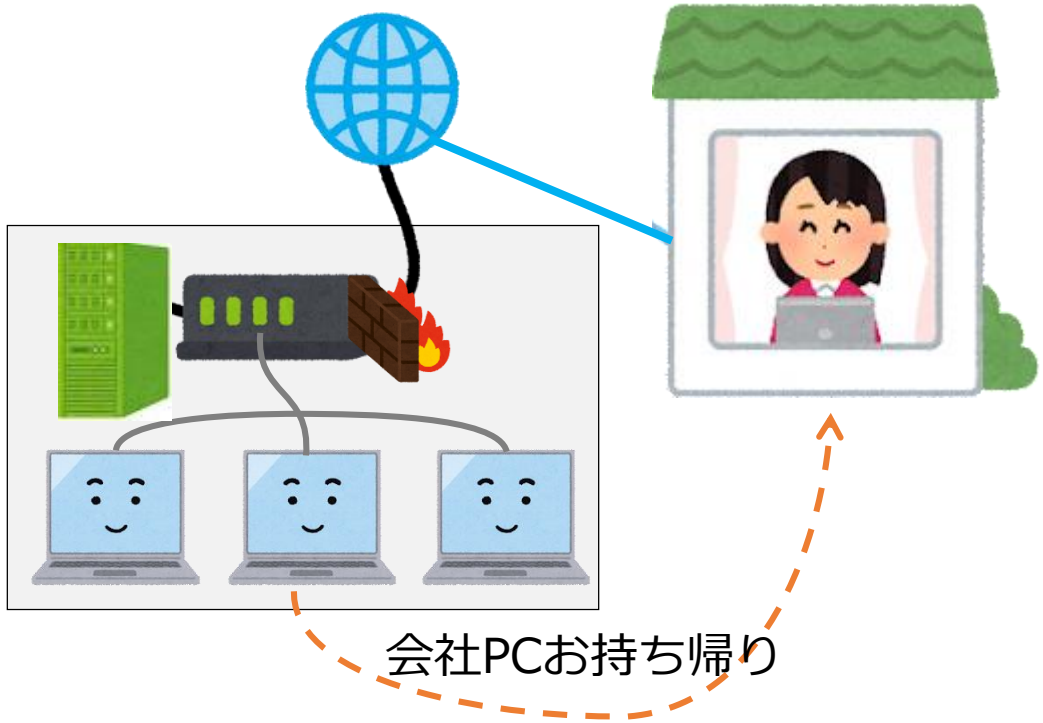
デジタルアーツ株式会社

〒100-0004　東京都千代田区大手町1-5-1
大手町ファーストスクエア ウエストタワー14F
Tel 03-5220-3090　Fax 03-5220-1130
sales-info@daj.co.jp　　www.daj.jp

※本書掲載内容の複写・無断転載を禁じます。

Copyright © Digital Arts Inc.

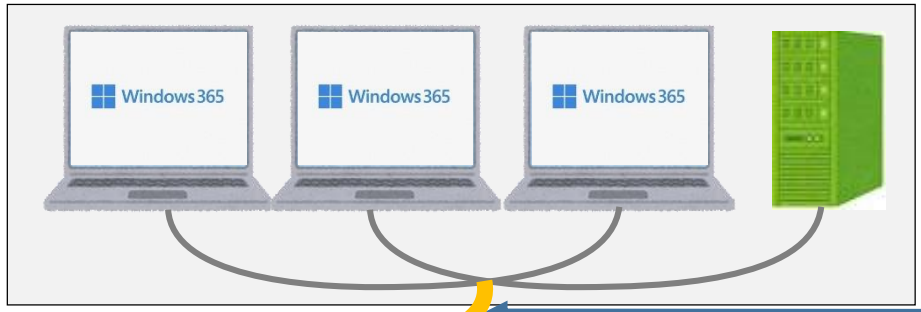
テレワークならではのリスクが増える



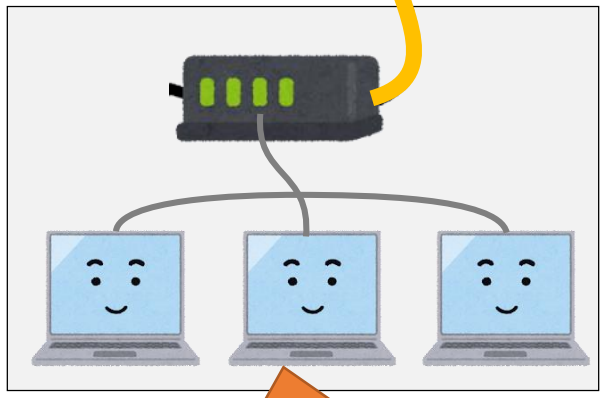
事象	リスク
端末の紛失・故障	情報の消失
端末の紛失・盗難	情報の漏洩
私物端末利用	ウイルス感染
公衆Wi-Fi利用	通信傍受・情報漏洩
自宅Wi-Fi利用	LAN内感染

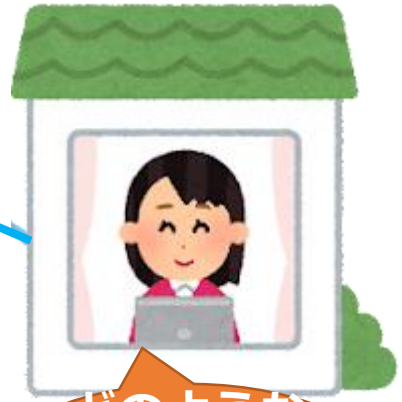
Copyright © Mirai Communication Network Inc.

テレワーク・リモートワークのこれから



クラウド側出入口ポイント
でセキュリティ





どのような
ネットワークでも
端末でもOK

アップデート
できてなくても
OK

端末紛失しても
OK

どのような
端末でもOK

クラウドサービスとの通信間を
・岐阜情報スーパーハイウェイ
・SJCC（ソフトピアジャパンクラウドコネクト）
で安全かつ高速に！しかも安価に！！

Copyright © Mirai Communication Network Inc.

SJCC（ソフトピアジャパンクラウドコネクト）

SJ Cloud Connect SJCC

データセンターと併用して使うハイブリッド利用も可能です

SJCC なら基幹システムのクラウド利用も安心

各種クラウドに直接接続を「簡単に」「セキュアに」「最良のコスト」でご提供いたします。
インターネット VPN 接続よりも安全で安定したクラウド接続環境をご利用いただけます。

（表記金額は全て税込）

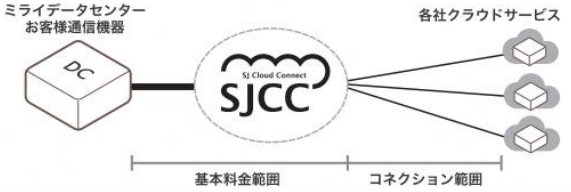
初期費用（共通）	¥110,000-

SJCC : One　単一クラウド接続で最のコストパフォーマンス

基本料金（月額）	
50M	¥55,000-
100M	¥77,000-
1G	¥143,000

SJCC : Multi　多数のクラウドサービスに接続ができるマルチクラウド対応サービス

月額基本料金			コネクション料金	
50M	¥200,200-	＋	50M	¥27,500-
100M	¥217,800-		100M	¥31,900-
1G	¥462,000-		1G	¥84,700-



※弊社接続ポイントまでの回線費用は含まれておりません。
※接続するためにはお客様側でクラウドサービスとの手続き、操作・設定が必要です。
※接続先クラウドサービスの利用料金（接続ポート費用・データ転送量等含む）は含まれておりません。
※お客様通信機器（BGP ルータ）までは Ether ケーブル（CAT6）でお渡しいたします。

Copyright © Mirai Communication Network Inc.

不明点は・・・

ミライネット　加藤
kato@mirai.ad.jp
080-9712-4711

ご清聴ありがとうございました

Copyright © Mirai Communication Network Inc.