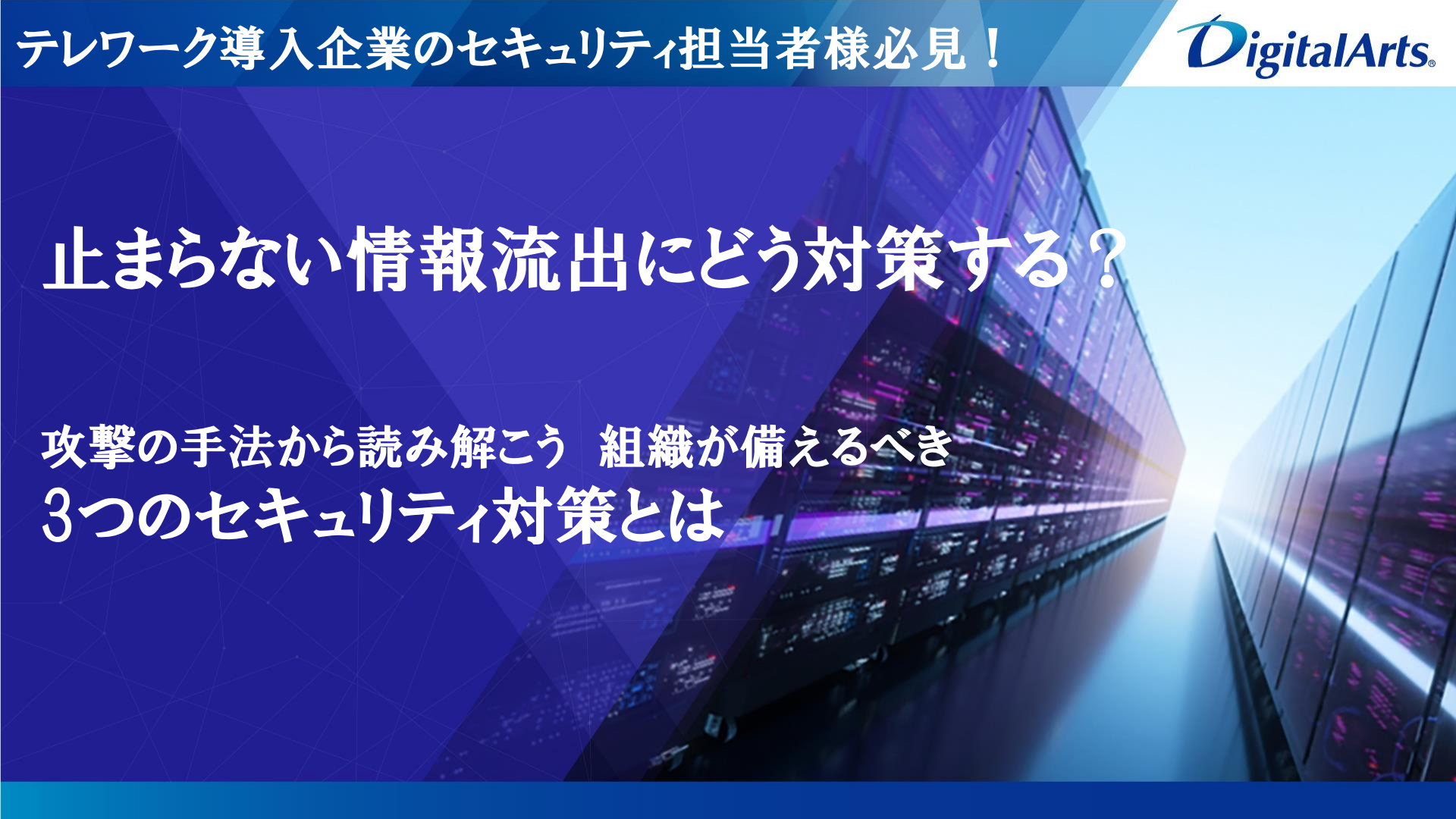
テレワーク導入企業のセキュリティ担当者様必見！

DigitalArts

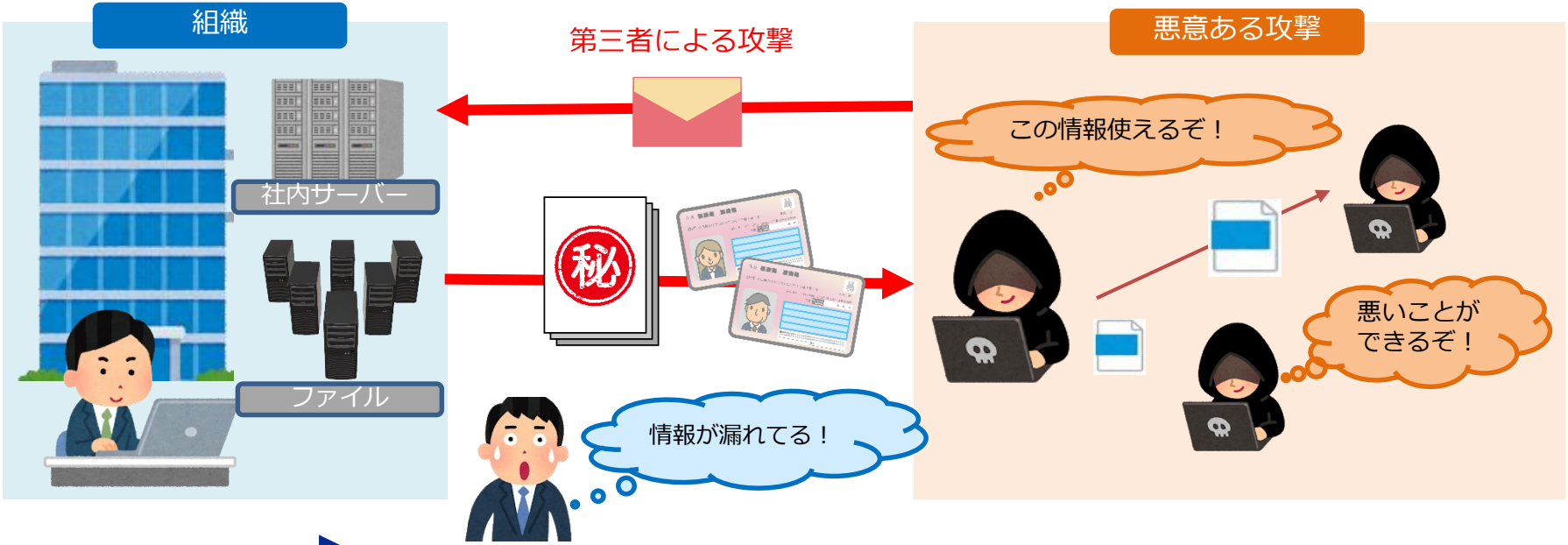
止まらない情報流出にどう対策する？

攻撃の手法から読み解こう　組織が備えるべき
3つのセキュリティ対策とは



後を絶たない組織の情報流出インシデント…

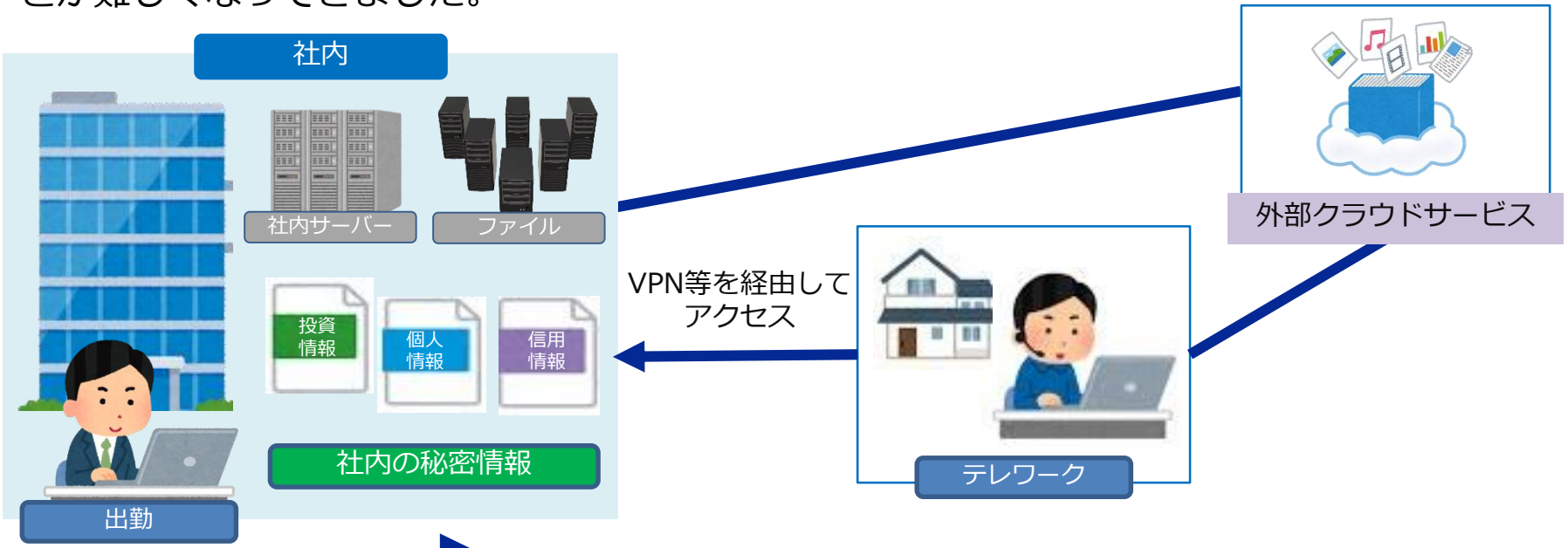
昨今、名だたる企業の情報流出インシデントが後を絶ちません。
企業側の発表によると、第三者によりサーバー等が不正アクセスを受け、
顧客情報が大量に流出してしまった、という事案が多いようです。



テレワーク時代の今、どのような攻撃が発生しているのでしょうか？

テレワークの環境

テレワークの環境では、従来組織内で使用していたネットワークやファイルサーバーに、組織の外側からアクセスします。VPN（Virtual Private Network）や、様々なクラウドサービスの利用が増加しており、従来とは比べ物にならない程ネットワークの内外を区別することが難しくなってきました。



こうした環境の中でどのような攻撃が起きているのでしょうか？

インシデントの多くは外部攻撃、しかもWebとメールに起因

では、こうしたテレワーク環境ではどのようなインシデントが発生しやすいのでしょうか？
デジタルアーツが独自に行った調査によると、テレワーク導入組織が2020年中に経験したインシデントの要因の多くは外部攻撃、それもWebとメールに起因するものが上位でした。

テレワーク導入組織が2020年に経験したインシデント要因ランキング			
1位	**フィッシングメール　65.3%**	7位	サービス妨害　16.8%
2位	**ビジネスメール詐欺　50.1%**	8位	内部不正による情報漏えい　16.6%
3位	**不正サイトへのアクセス　37.1%**	9位	Emotet等マルウェア　11.6%
4位	**メール誤送信など意図しない情報漏えい　35.7%**	10位	サプライチェーン　9.2%
5位	標的型攻撃　32.4%	11位	自社サイトの改ざん　7.6%
6位	ランサムウェア　29.0%	12位	その他　1.6%

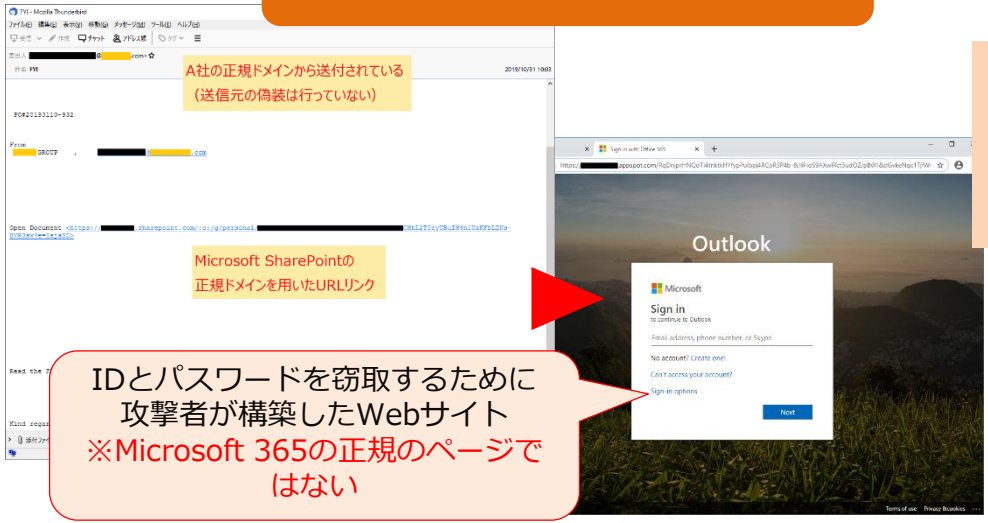
出典：デジタルアーツ調べ　テレワーク導入組織が2020年に経験したインシデント要因

それぞれ、どのような攻撃があるのでしょうか？

①フィッシングメール

テレワーク下で、世界的に増加していると言われている攻撃の一つがフィッシングメールです。
日本でも、件名や送信者を偽装し、不正な添付ファイルやURLにアクセスさせる攻撃が
多発しています。IDやパスワード、アカウント情報を窃取するなど目的は様々です。

Microsoft365アカウントの乗っ取りを目的とした**フィッシングメール**



▲国内有名企業A社のメールアカウントが乗っ取られたフィッシングメール
出典： デジタルアーツ「テレワークの今こそ必要な、ラテラルフィッシングへの対策」
https://www.daj.jp/company/release/2020/0514_01/

新型コロナウイルス感染症に便乗した**フィッシング詐欺が横行**

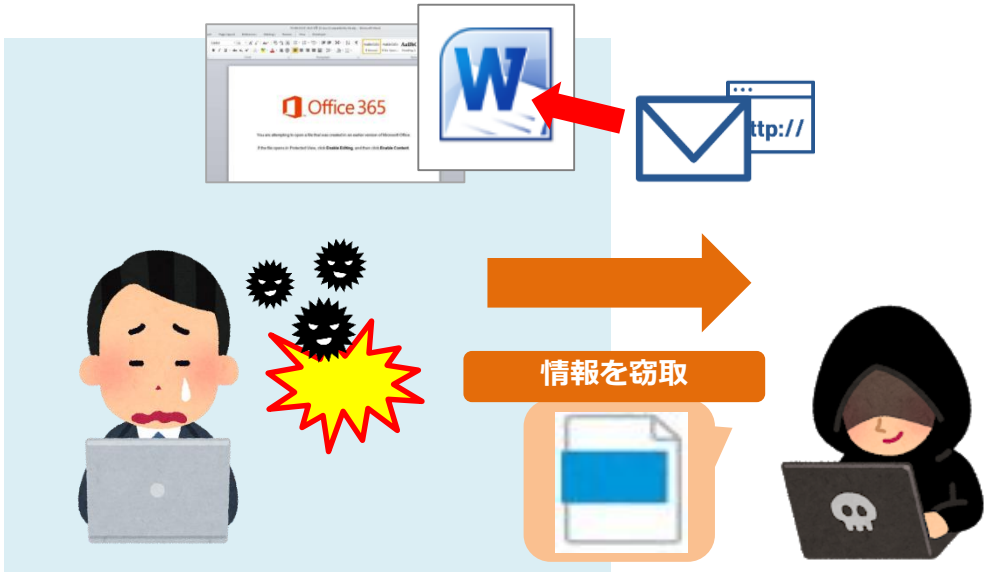
- **新型コロナウイルス感染症に関連したサイバー攻撃が増加**
- **「給付金が受け取れる」「税還付が受けられる」といった不正メールに由来するものが多い**

2020年1-6月期の被害総額は 5億1200万円
（前年同期比の3倍！！）

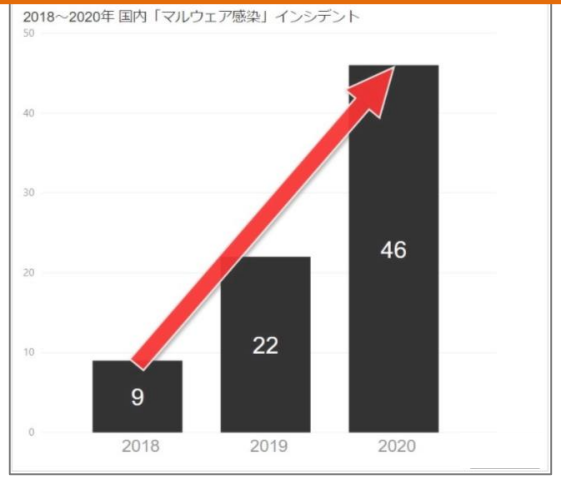
▲公的機関を装い、件名や送信者名を偽装したフィッシングメール
出典： デジタルアーツ「コロナ便乗詐欺やフィッシング詐欺が横行」
https://www.daj.jp/webtopics/16/

②マルウェア感染

2020年1年間でマルウェア感染インシデントは前年から2倍となりました。
昨今では、「Emotet」など他のマルウェアを引き込むプラットフォーム的な役割をするものもあります。多くはメールの添付ファイルを通じて感染させますが、アンチウイルスを回避するなど手口が巧妙化しているものが多く見られます。



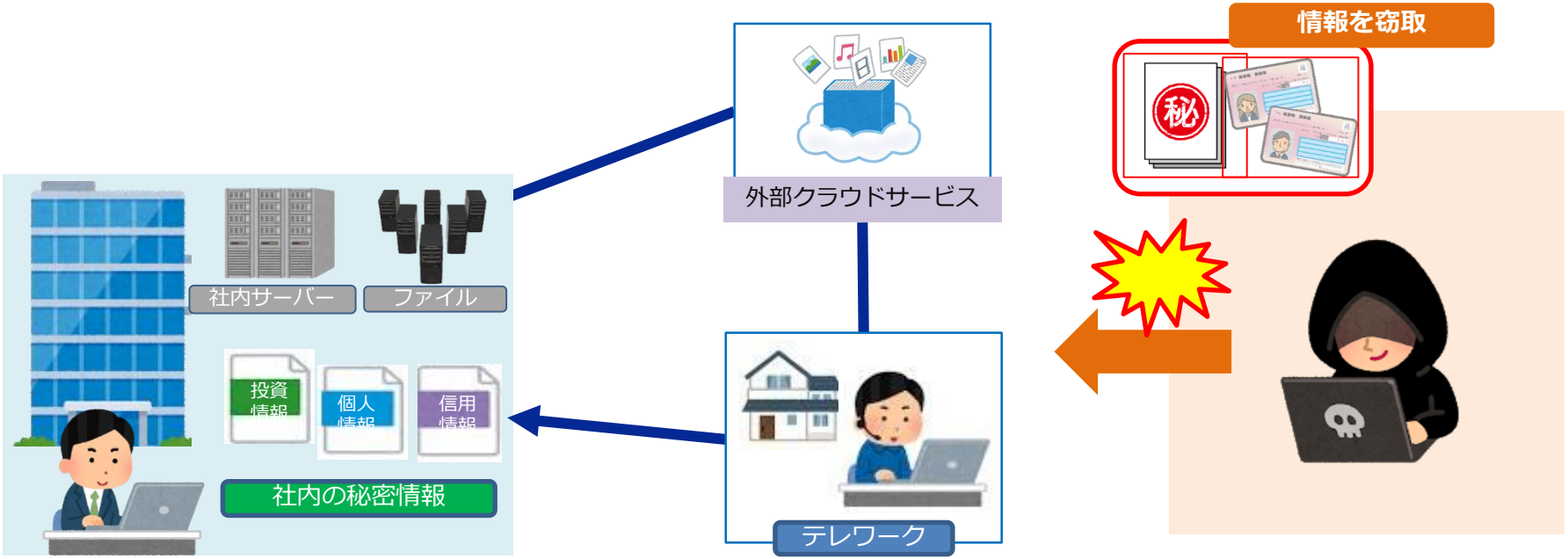
マルウェア感染インシデントが
前年比 2 倍に！！



出典：デジタルアーツ調べ
2018～2020年 国内「マルウェア感染」インシデント件数
対象組織による公開報告書およびマスメディアによる報道資料をもとに独自に集計
https://www.daj.jp/security_reports/210126_1/

③不正アクセスによる情報流出

サーバーやテレワークで利用が増加したVPN機器に、何らかの方法で第三者が不正アクセスし、機密情報や顧客情報を窃取する事案です。情報漏えいによる事業への悪影響や、顧客への被害拡大による信用失墜に繋がり、重大な業績悪化に繋がる恐れがあります。



このような様々な攻撃手法には複雑な対策が必要なのでしょうか？

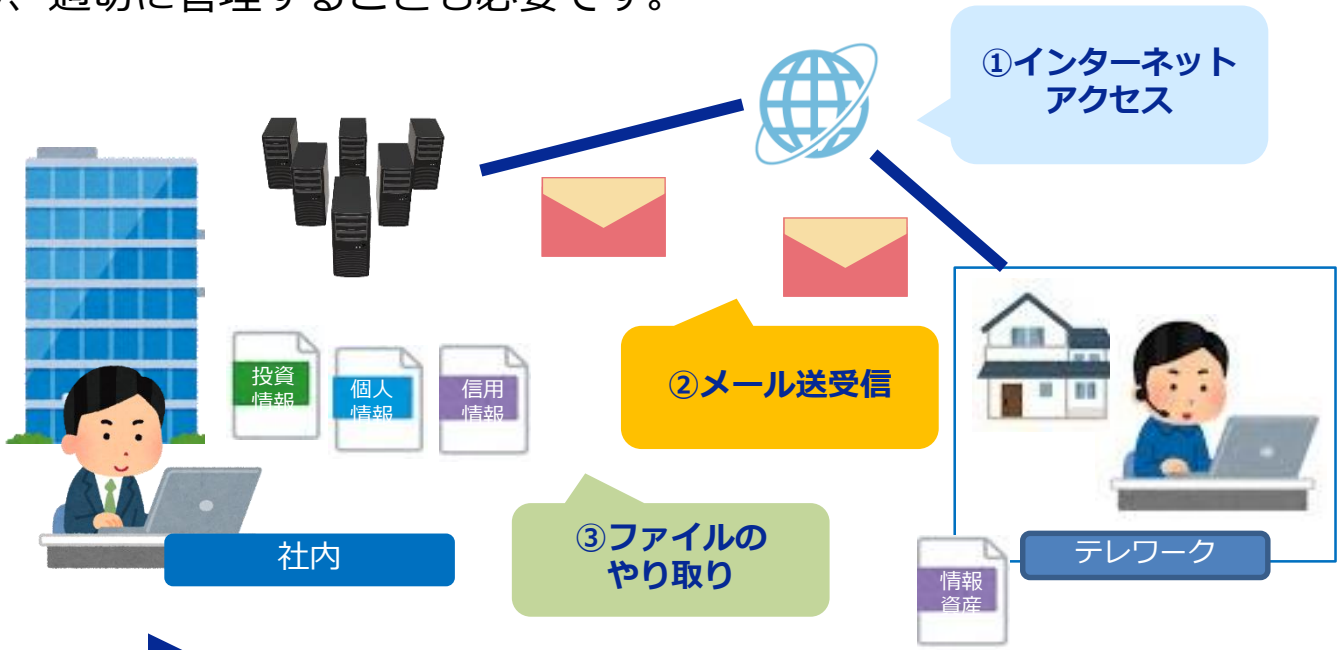
ここだけは押さえたい3つのセキュリティ対策

外部攻撃の多くはWebとメールに起因するものです。
不正なURLや添付ファイルへのアクセスを防ぐことができれば、情報漏えいのリスクを下げることができます。また、不正アクセスや内部からの情報漏えいを防ぐには、重要な情報（ファイル）を暗号化し、適切に管理することも必要です。

①Web

②メール

③ファイル



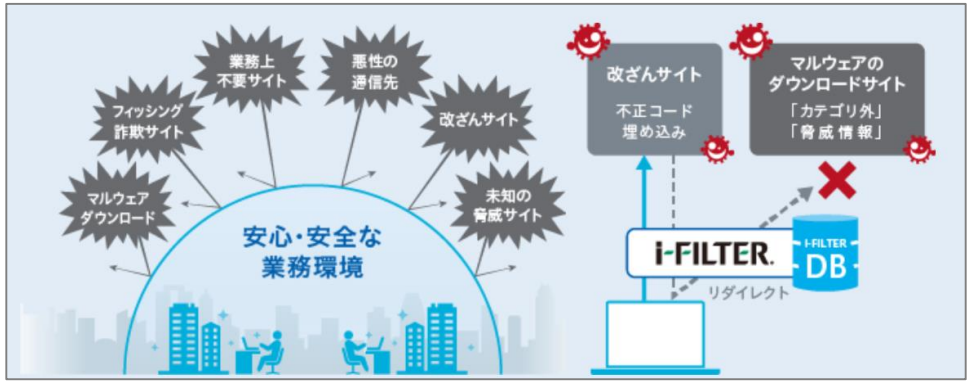
それぞれ、どのような対策が必要でしょうか？

①Webセキュリティ対策

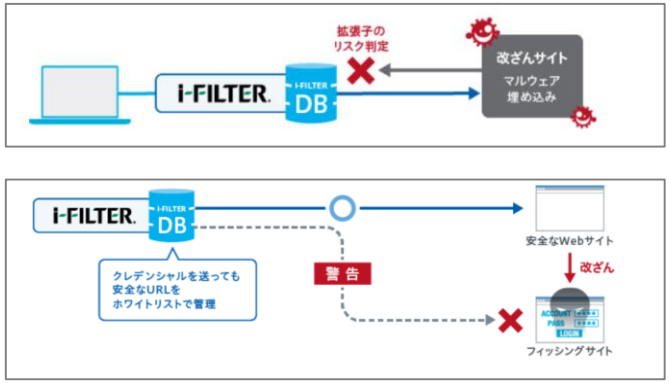
「i-FILTER」Ver.10は、不正なURLへのアクセスやマルウェアのダウンロードをブロック
- テレワーク下でもWebアクセスを安全に
- URLデータベースをデジタルアーツが管理するため、運用負担も軽減

▶ テレワーク下でも安全な環境で業務が可能

国内で検索可能なURLをデータベースに登録
悪意あるURLはブロック



正規サイトの改ざんにも対応
マルウェアダウンロードや
アカウントの窃取をブロック



②メールセキュリティ対策

「m-FILTER」Ver.5は、あらゆる攻撃メールをブロック

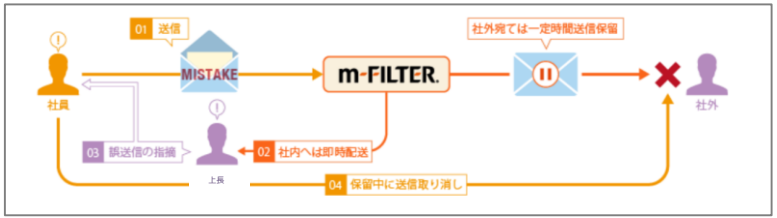
・不正添付ファイルや不正URL、送信元偽装も見抜き、誤送信対策も対応

・デジタルアーツが安全な送信元のデータベースを管理　運営負担を軽減

▶ メールの安全を確認する必要なく業務が可能

安全な送信元のIPアドレスとメールドメイン
をデータベースに登録
攻撃メールをブロック

上長承認など、メールのルールを設定できる
誤送信防止機能

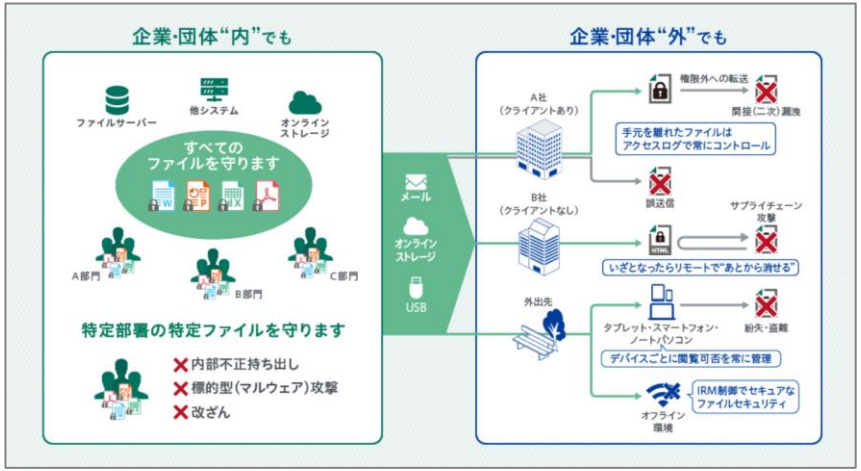


③ファイルセキュリティ対策

「FinalCode」Ver.6は、ファイルを『守る・後から消せる』機能で情報漏えいを防ぐ
・高度な暗号化で、ファイルを開封したり閲覧する権限を相手を制限して設定できる
・万が一の漏えいでもファイルを追跡して後から消すことが可能

ファイルが漏えいしない仕組みで徹底管理が可能

ファイルへの操作権限を相手を制限して設定
操作履歴を取ることができ、外部に漏れても後から消せる
組織内のファイルを徹底管理



メールセキュリティ「m-FILTER」と連携し
安全で効率的なファイル送信も可能に

詳しくはこちら

テレワークでもセキュアに

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 03-5220-1110　Fax 03-5220-1130

製品に関するお問い合わせ： Tel 03-5220-3090【受付時間】平日9:00～18:00（土、日、祝日、弊社指定休業日を除く）　E-Mail sales-info@daj.co.jp　URL www.daj.jp

2021/1　DD-00000-000