サイバー攻撃から
中小企業350万社を守る
セキュリティ製品

RICOHサイバーセキュリティパック　インシデント対応サービス
監視・初動対応プラン

個人情報保護法改正の公布　※経産省にてセキュリティ格付けスタート予定

2020年6月12日

企業の個人情報の漏洩が一定数以上となった場合、
①政府の個人情報保護委員会に報告
②本人に通知
が義務づけされました。

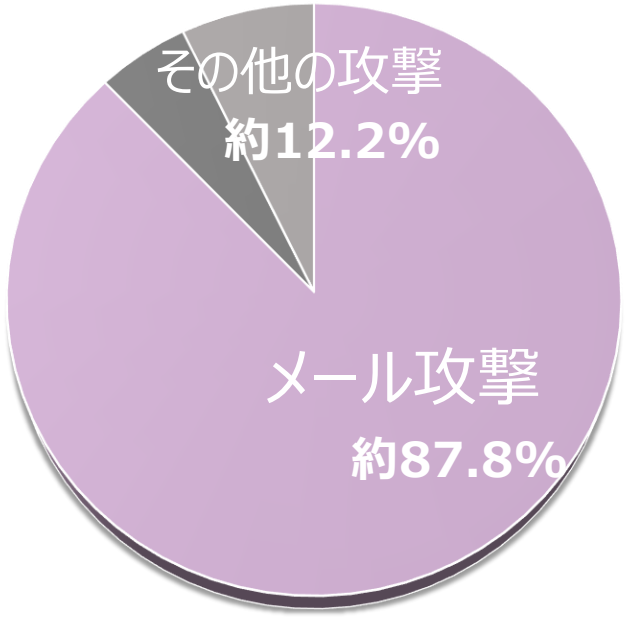
罰則も強化され、罰金の上限額が
50万円→1億円に引き上げられます。

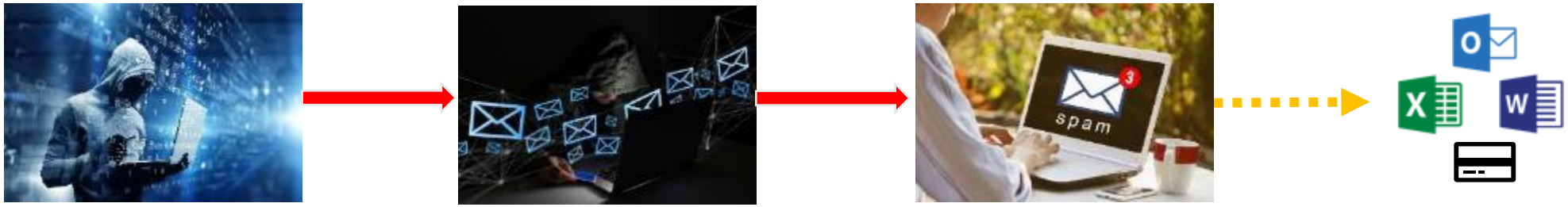
今までは
5,000人以上の個人情報のみ適用対象
→すべての事業者が適用
年々個人情報取り扱いに
対する国からの要求水準は高まっています。

	Before	After
個人情報対象	5,000名以上	**1名以上**
罰金の上限額	50万円	**1億円**

標的型攻撃の手法

約9割がメールによる攻撃





出典：IPA情報処理推進機構「コンピュータウイルス・不正アクセスの届出状況および相談状況」

サイバー攻撃の手法とビジネスリスク

RICOH imagine. change.

昨今のサイバー攻撃手法

順位	組織被害
1位	**標的型攻撃よる被害(ランサムウエア含む)**
2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	サプライチェーンの弱点を悪用した攻撃の高まり
4位	ビジネスメール詐欺による金銭被害

出典：ＩＰＡ情報処理推進機構「情報セキュリティ10大脅威 2021」

情報流出によるビジネスリスク

- 社会的信用の失墜
- 行政指導、業務停止命令
- マスコミ対応、顧客対応
- 情報流出平均損害賠償額

6億3,767万円／件

出典：JNSA日本ネットワークセキュリティ協会
「2018年 情報セキュリティインシデントに関する調査報告書」

【標的型攻撃】

特定の組織内の情報を狙って行われるサイバー攻撃

■標的型攻撃による被害事例

日付	法人・団体名	被害内容（件数・人数・金額）
2011年	ソニー	2,460万人
2013年	Yahoo! JAPAN	2,200万人
2014年	日本航空(JAL)	4,131人
2015年	三菱東京UFJ銀行	14,000件
2015年	日本年金機構	125万件
2016年	JTB	678万人
2017年	GMOインターネット	14,612件
2017年	エイチ・アイ・エス	11,975件
2018年	コインチェック	580億円分
2018年	プリンスホテル	12万4,963件
2018年	テックビューロ（Zaif）	70億円分
2019年	トヨタ東京販売ホールディングス	310万件
2019年	九州旅客鉄道（JR九州）	8,206件
2020年	三菱電機	9,750件
2020年	カプコン	15,649件

※件数：情報流出件数
人数：個人情報流出人数
金額：仮想通貨流出額

出典：IPA情報処理推進機構「サイバー攻撃被害一覧」
サイバーセキュリティ.com
日本経済新聞

中小企業へのサプライチェーン攻撃（踏み台攻撃）

・中小企業は大企業に比べるとセキュリティ対策に十分な投資が出来ていない。
・ハッカーは中小企業に攻撃を行い、①大手企業に侵入する**足掛かり**とする。
②その中小企業が保有の大企業情報を窃取する。

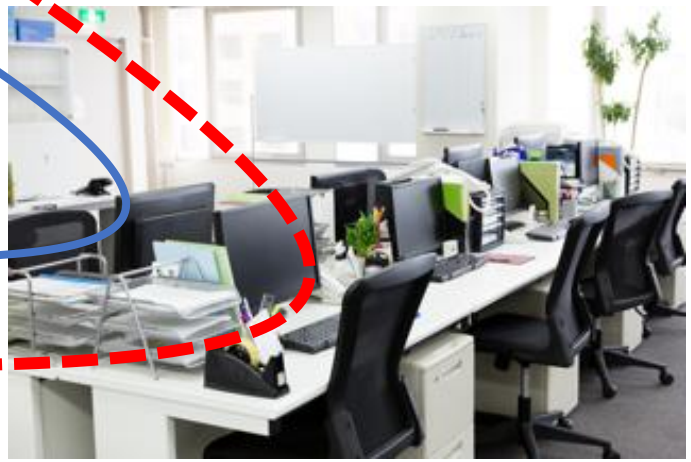
ハッカー

①マルウェア
PASS

Guard

大企業

中小企業

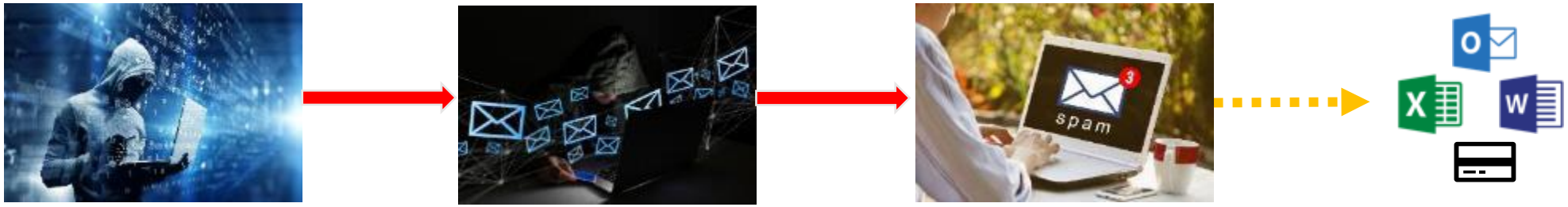


②マルウェア
PASS

標的型攻撃の手法

①メール攻撃

マルウェアを忍ばせたメール等で感染させます。
感染したパソコンは強制的にハッカーが使用する専用サーバに接続され、遠隔操作にて情報を窃取されます。

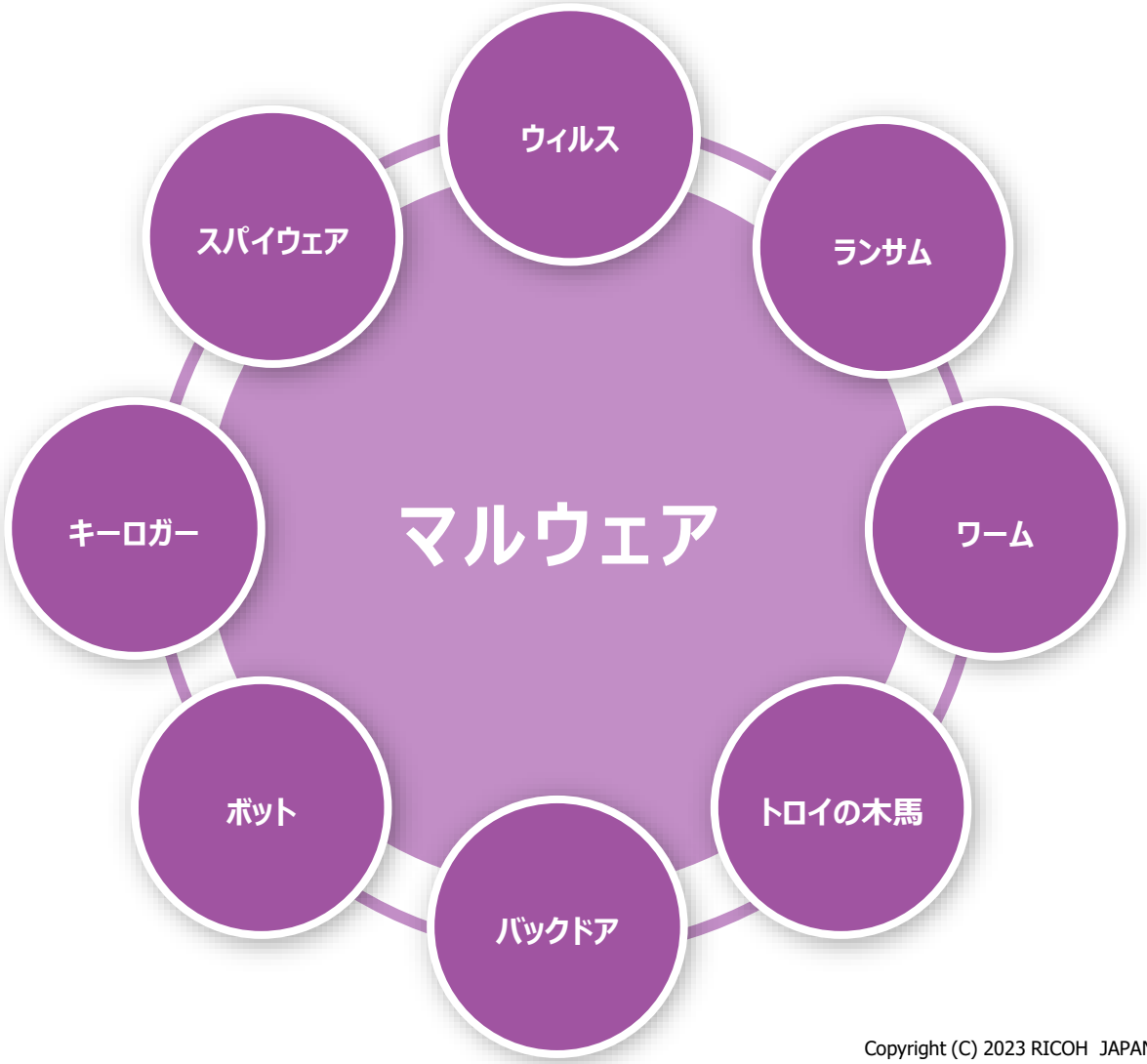


②その他攻撃

パスワードクラックを用いた侵入や、セキュリティ対策の脆弱性を突いた侵入を試みます。
侵入、脱出経路の足跡を削除しながら情報を窃取するため時間を要します。

情報を抜き取る「マルウェア」とはどのようなものか？

マルウェアとは悪意のあるソフトウェアの総称です



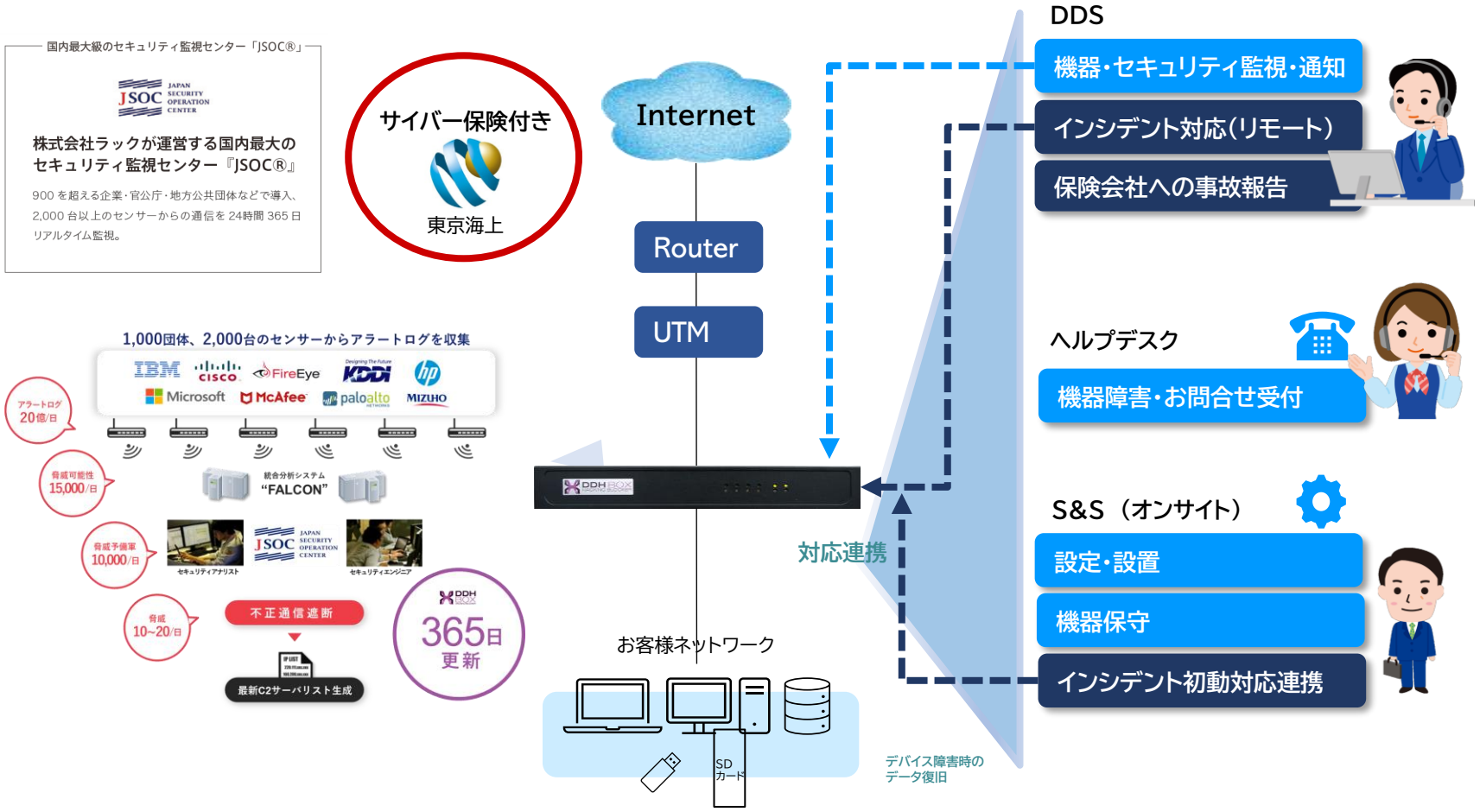
ウイルス	他のプログラムに寄生し、動作を妨げたりユーザの意図に反する有害な作用を及ぼす。感染機能や自己拡散機能を持つ。
ランサム	システムを乗っ取り、利用者の利用を制限する。制限を解除する為に身代金を要求される。
ワーム	独立のファイルで他のプログラムの動作を妨げたりユーザの意図に反する有害な作用を及ぼす。
トロイの木馬	攻撃者の意図する動作を侵入先のコンピュータで秘密裏に行うプログラム
バックドア	攻撃者が侵入するためのネットワーク上の裏口を開ける
ボット	感染したパソコンの内部情報を外部に勝手に送信する
キーロガー	ユーザのキーボード操作をそのまま外部に送信する。スパイウェアの一種
スパイウェア	攻撃者からの指令により、他のコンピュータやネットワークへの攻撃、サーバからのファイルの盗み出しなど有害な動作を行うプログラム

※全14種類、うち8種類抜粋

出典：Mc Afee 公式Blog

RICOHサイバーセキュリティパック インシデント対応サービス　監視・初動対応プラン

万が一の事故に備えたいお客様へ
データとセキュリティインシデントの対応と費用をサポートできるサービス



標的型攻撃に対応する ２つのセキュリティ対策

(1) 入口対策

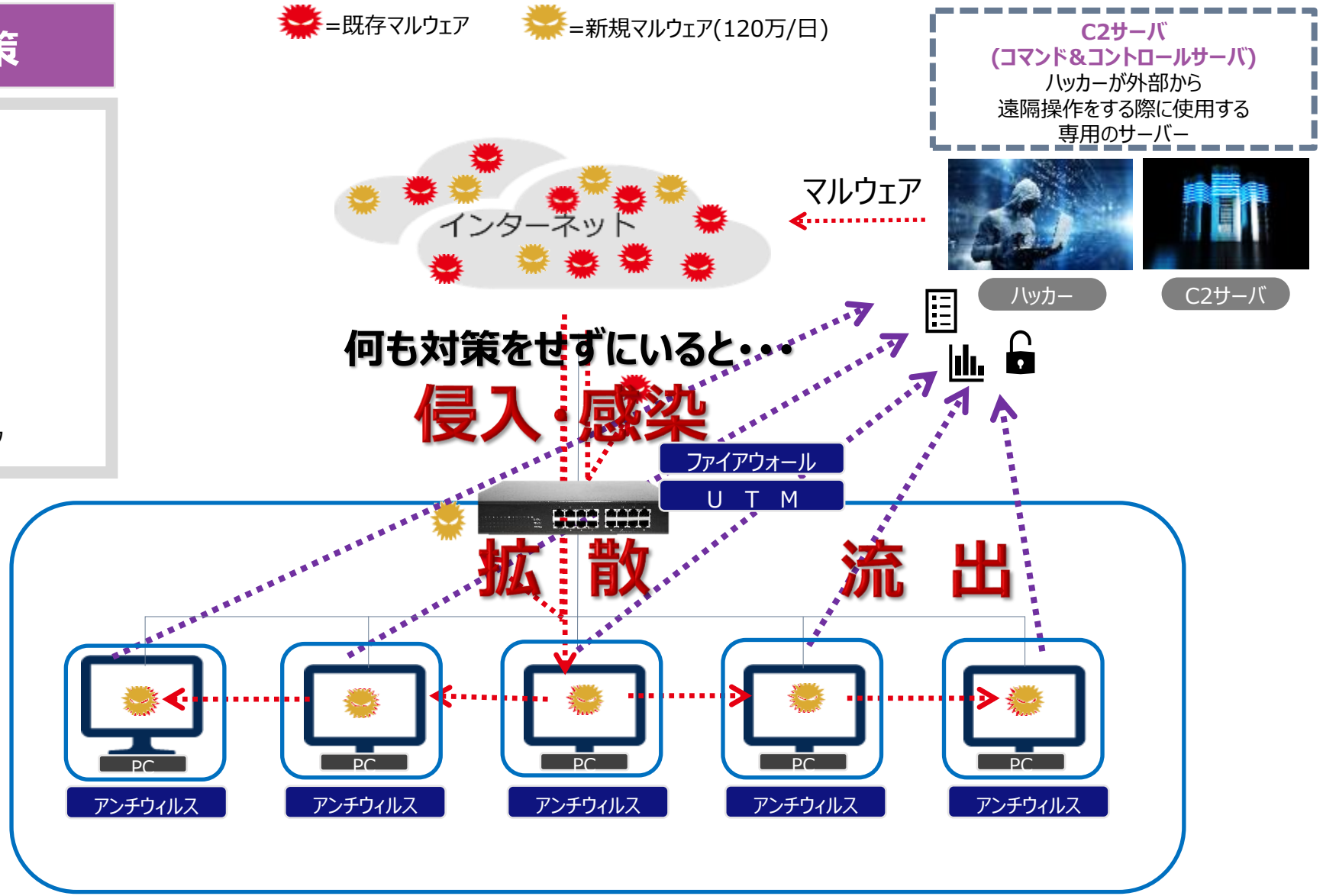
- ✓ ファイアウォール
- ✓ ＵＴＭ
- ✓ アンチウイルス

機　能
侵入しようとするウイルスなどの
脅威情報を検知し、侵入をブロック

対　策
最新のウイルスをリスト化しておき、
リストにあるウイルスが侵入したらブロック

「ウイルス対策ソフトは死んだ」

従来型のウイルス対策ソフトでは現状のサイバー攻撃に対し45%程度しか防御する能力が無いと、2014年5月にSymantec社上級副社長ブライアン・ダイ氏が衝撃の発言を行った。

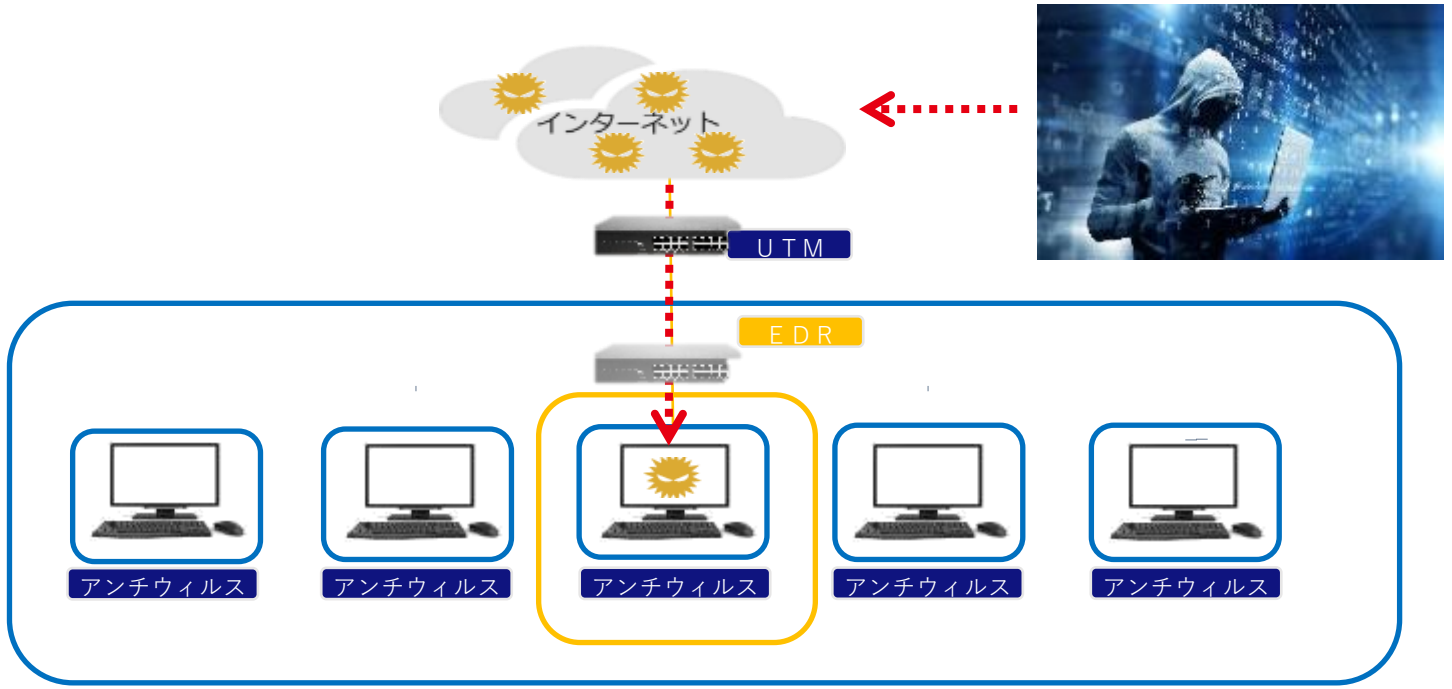


セキュリティ対策とマルウェア感染の矛盾

セキュリティ対策をしっかりしているのに
なぜ、マルウェアに感染してしまうのか？

(1) 入口対策　**(2) 内部対策**

- ✓ 入口・内部対策でブロックしているのは既存のマルウェアのみ
- ✓ マルウェアは毎日120万件もつくられる為、全てをブロックすることが出来ません。



発想を変えたセキュリティ対策

入口対策・内部対策では
サイバー攻撃を100%ブロックできません

これからの企業のセキュリティ対策は

感染しても外に出さない**「出口対策」**の強化が重要なのです

ワンストップのセキュリティサービスを実現（サイバー保険標準付帯）

RICOH imagine. change.

インシデント発生後のサポート体制が万全です。

東京海上日動

インシデント発生後、年間300万円までの調査・対策を無償で行います。
一般的なセキュリティ対策製品の場合、アラート発報までは行いますが、
その後のサポート体制がない、もしくは有償のケースが多いと言われています。

初動対応
(駆けつけ対応、電話サポート等)

インシデント発生後の初動対応のサポートをおこないます。

フォレンジック調査

攻撃にあった機器に対して、どこから、どのような攻撃があったか？情報流出がなかったか？などの調査を行います。

コンサルティング

インシデント発生後に企業としてどのような対応を取ればよいか(メディア対応、社内セキュリティ対応)等をトータルでコンサルティングします。
今後の対応のアドバイスをおこないます。

まとめ

1 ゼロ情シスでも安心

不正通信の検知・遮断・通知を全て自動で行います。
難しい運用の必要が無いため**ゼロ情シスでも安心**です。

2 低コストでセキュリティ対策

有人の監視サービス（SOC等）と比較した場合、**低コスト**でサービス利用が可能です。
機械が自動的に検知・遮断するため、運用にかかる人件費の削減にもなります。

3 サイバー保険付帯

DDH BOXが不正通信を検知・遮断した場合は調査・対策の費用として、
保険適用可能。（年間300万円まで）