



SOMPO CYBER SECURITY

サイバーリスクセミナー

～ 身近に潜むサイバーリスクを考える ～

SOMPOリスクマネジメント株式会社

サイバーセキュリティ・コンサルティング部

2024年9月13日

SOMPOグループとSOMPOリスクマネジメント

会社概要

社 名：SOMPOリスクマネジメント株式会社

(英文表記 Sompo Risk Management Inc.)

設立年月日：1997年11月19日

本社所在地：〒160-0023

東京都新宿区西新宿1-24-1エステック情報ビル

事業内容：デジタル事業／リスクマネジメント事業／サイバーセキュリティ事業

拠 点：東京・名古屋・大阪

従業員数：519名 (2024.4 時点)

資本金：3,000万円

株 主：SOMPOホールディングス株式会社 (100%)



SOMPOリスクマネジメント

- 損害保険ジャパン
- センソ自動車火災

- 損保ジャパン海外ネットワーク



サイバーセキュリティ事業

環境変化に伴い深刻化するサイバー攻撃に対して、お客さまのリスク・課題に応じた最適なソリューションを提供するサイバーセキュリティ事業を展開

3つの特長

- 1 リスクのプロ集団による経営リスク対策の経験と実績
- 2 エコシステムによる柔軟かつ最適なサービスの提供
- 3 世界最高水準の高度な技術力



1 サイバーリスクの動向

2 サイバーリスクへの対応のポイント

3 サイバー攻撃等によるインシデント発生時における対応

1

サイバーリスクの動向

多くの組織にとってサイバー攻撃は関係ないのでしょうか？

ウチが標的にされるなんてありえない！
ウチには個人情報や独自ノウハウのような機密情報はなから...

サイバー？ そんなの良くわからない。
業者に任せている（サポートがある）から大丈夫だよ...



ウチは外部とつながっていないから大丈夫だよ...

なぜ、サイバー攻撃は行われるのでしょうか？

- サイバー攻撃の多くはほとんどが金銭目的であり、非常に効率のよい“儲かるビジネスモデル”といわれています。

⇒ あなたや組織が重要機密を保持しているかはそれほど関係がないです。

効率的な攻撃



※コツコツと定期収入が得られる手堅いビジネス

高度な攻撃



※難易度が高いが、成功すれば大きな収益が見込まれるビジネス

より儲かりやすい攻撃へと進化を続ける

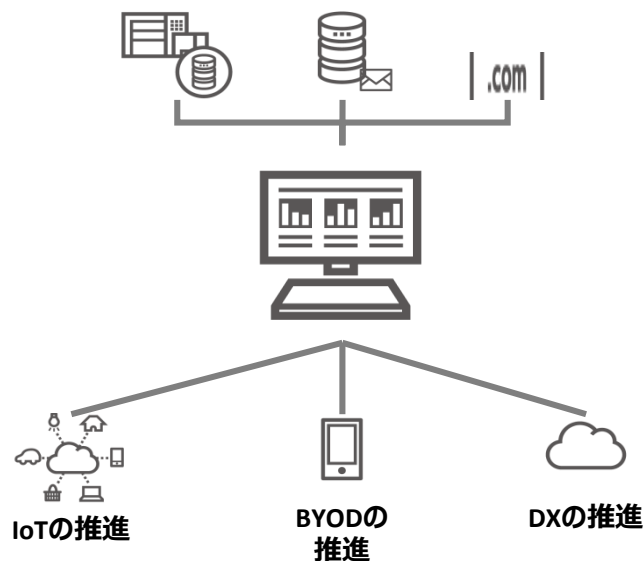
※まるで、どこかの優良企業のような改革・改善マインドで高い業績を目指している

※攻撃側は常に防御側の先を行っているため、攻撃を防ぐことは不可能に近い

近年の環境変化①

- デジタルトランスフォーメーション（DX）推進のために、クラウドサービスやテレワーク環境などを導入する組織が増えている一方、これらのシステム環境を狙ったサイバー攻撃が増加しています。

デジタル（IOT）推進や働き方改革などにより、
システム環境は日々変化



サイバー攻撃は日々巧妙化し、
多種多様な攻撃手法で組織をターゲットに

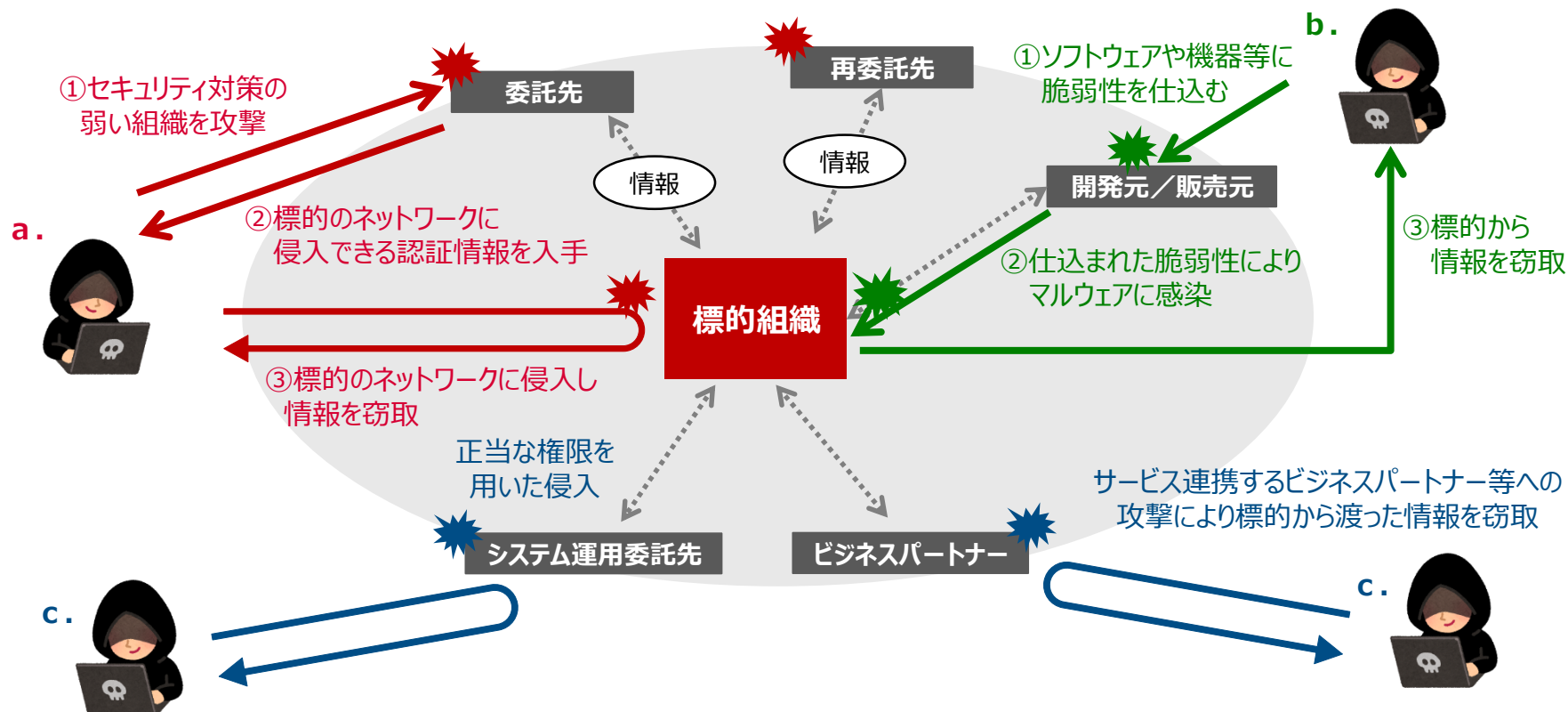


近年の環境変化②

- 昨今、リモートワークやビジネスパートナーとのサービス連携の増加に起因する隙など、**サプライチェーン（委託先・ビジネスパートナーなど）上の「攻撃起点」がますます拡大**しています。

主な類型

- a. 委託先（再委託先を含む）等を踏み台とした攻撃
- b. ソフトウェアやソフトウェアの更新プログラム、ハードウェアのファームウェアを介した攻撃
- c. 重要情報を共有するビジネスパートナー等に対する攻撃



行政分野に関連したサイバーインシデント（事故）事例

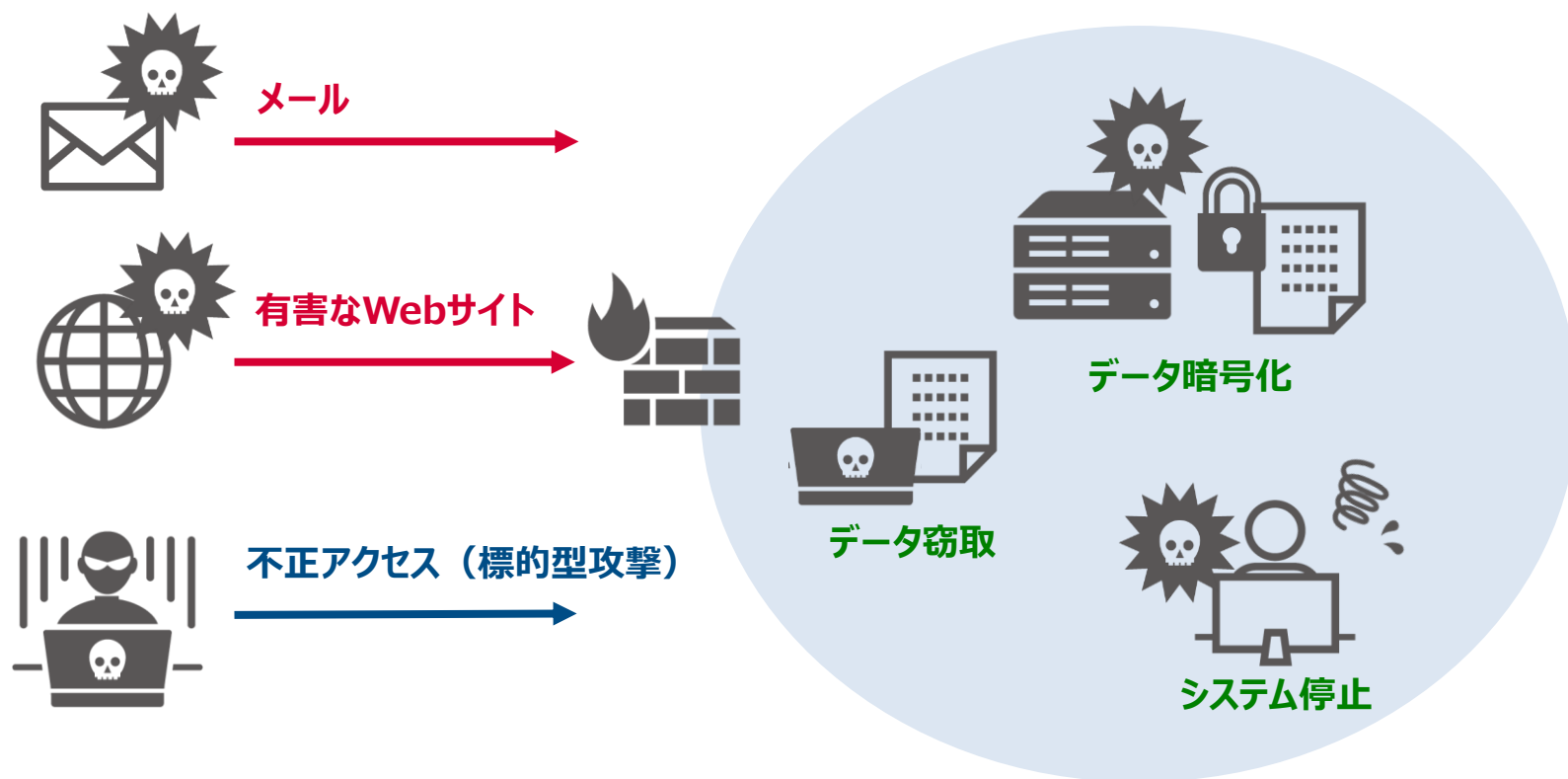
- 近年では金銭やテロが主な目的となり、行政分野においても事業活動に影響を及ぼすサイバー攻撃等によるインシデント事例が増加しています。

時期	概要	内容
2024年6月	委託先がランサムウェアに感染し、個人情報 が漏えい	愛知県豊田市で、委託先の複数のサーバ・端末内の情報が ランサムウェア によって暗号化され、新型コロナの予防接種券や軽自動車税の納税者などの個人情報（14万8620人）が漏えいしたおそれがあることを公表した。 ※徳島県（約20万件）や和歌山市（151,421件）、平塚市（286件）、京都府（177件）、広島県（101件）、愛媛県（80件）、東京都大田区（46人）、東京都教育委員会（37人）などでも同様に漏えいのおそれを公表した。
2024年3月	外部からサーバに不正アクセス	交流広場の施設職員がインターネット閲覧中に警告を受け、指示に従って操作した結果、パソコンが使用不能になり、 サーバへの不正アクセス により個人情報が漏えいした可能性があったと公表した。 ※漏えいの可能性があった情報は、120人分の氏名、住所、年齢、生年月日、電話番号を含む。
2023年7月	公園施設予約システムにおける情報流出	公園施設予約システムで導入予定の新規サーバ（テストサーバ）で検知した 不正通信 より、情報流出の可能性があることを公表した。 ※流出の可能性がある情報は、氏名、生年月日、性別、住所、電話番号、メールアドレス、銀行口座、ログインID、ログインパスワードである。
2022年7月	小中学校が使用する校務ネットワークに対して悪意のある第三者による不正アクセス	校務支援システムが ランサムウェア攻撃 を受けた結果、市内の6小学校と6中学校の全児童・生徒にあたる小学生1,293人、中学生724人の個人情報（住所、氏名、保護者連絡先、成績、出席情報など）のほか、教職員の人事情報や教育活動の記録といった学校業務のデータがすべて暗号化され、閲覧できなくなった。
2022年3月	自治体情報セキュリティクラウドへの不正アクセス	自治体情報セキュリティクラウドのメールシステムに対して 不正アクセス があり、青森県、秋田県、新潟県、栃木県の自治体を装った不正メールが送信（約91万件）された。 ※発注先でのシステム切替作業中の一時的な設定ミスが原因という。

（報道等により公表された事例をもとに作成）

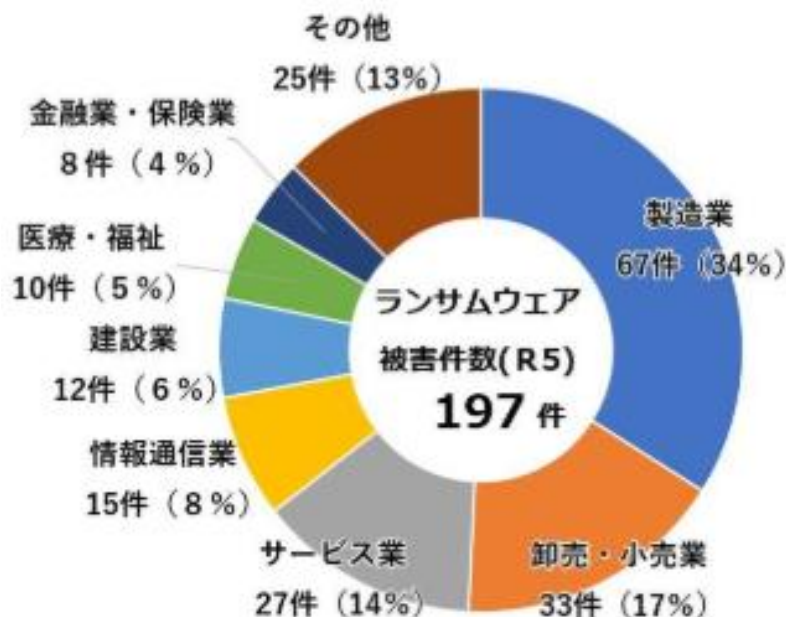
ランサムウェア (Ransomware)

- 「ランサムウェア」は、感染したPC端末をロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに『身代金』を要求するマルウェアに感染させる攻撃のことです。

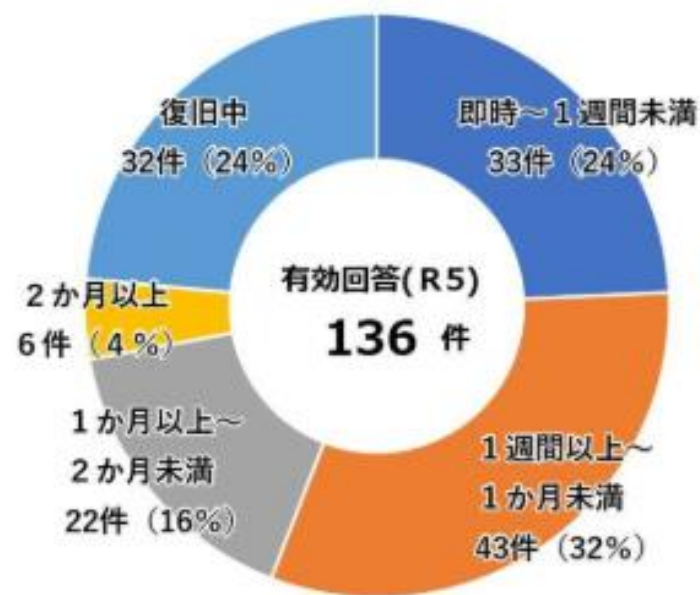


- 国内のランサムウェア被害として、令和5年に都道府県警察から警察庁に報告のあった件数は197件でした。
⇒1週間以上～1か月未満に復旧したものが43件と最も多かったが、**復旧までに1か月以上を要した被害が28件**あった。

ランサムウェア被害の企業・団体等の業種別報告件数



復旧に要した期間



出典：警察庁."令和5年におけるサイバー空間をめぐる脅威の情勢等について.",

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf, (アクセス日:2024-3-26)

サポート詐欺

- 「サポート詐欺」は、画面に突然、偽のセキュリティ警告画面（サポート詐欺サイト）を表示させるなどして、ユーザの不安をあおり、画面に表示された電話番号に電話をかけさせ、PCを遠隔操作するソフトウェア等をインストールするように促し、有償のサービス契約の締結等をさせられる手口のことです。

【サポート詐欺の手口】

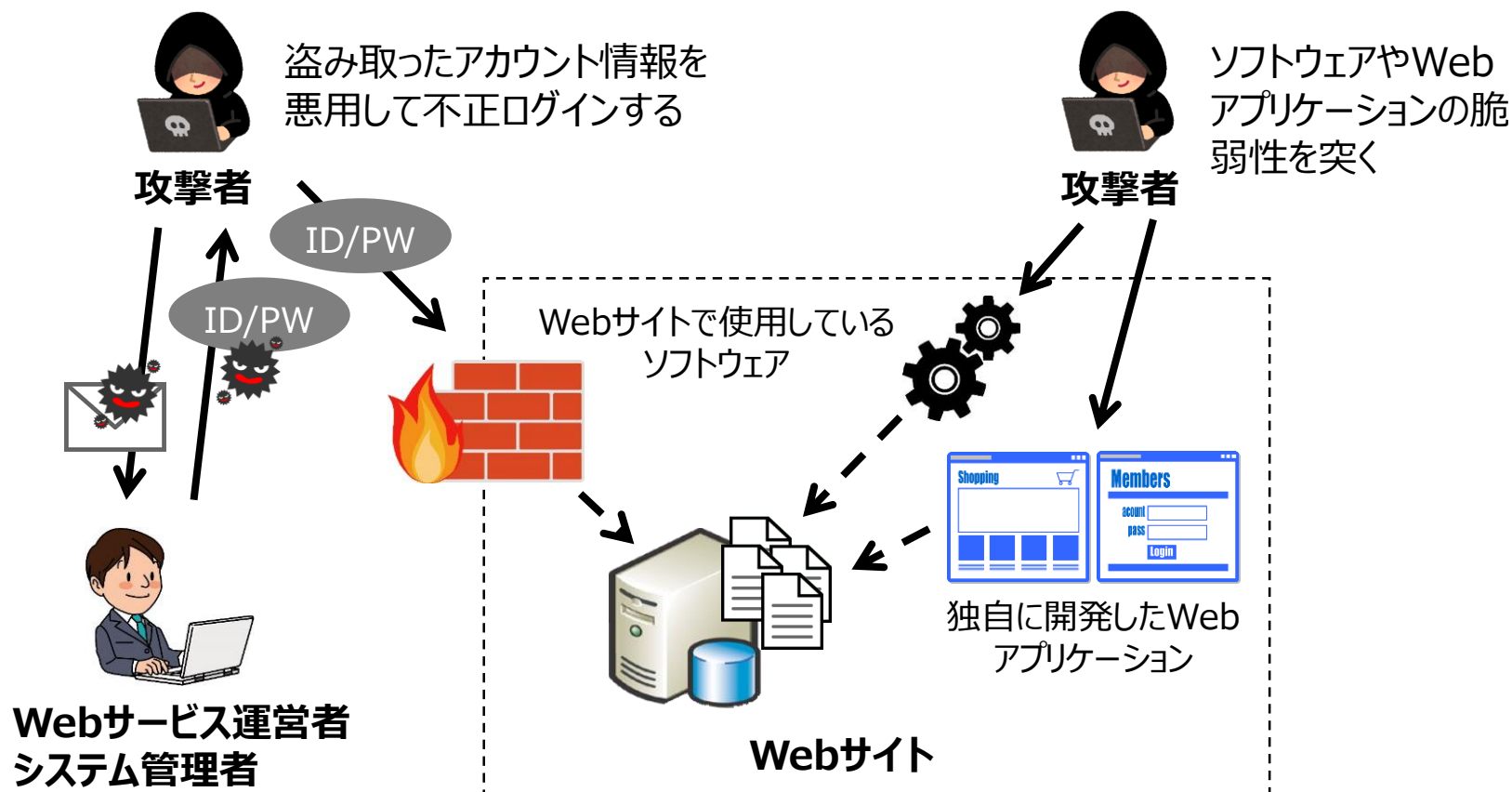
1. Webサイトの広告に警告メッセージを仕掛ける
2. ユーザのブラウザに警告メッセージが表示される
※偽のセキュリティ警告画面は消せない場合も多い
3. 「サポート窓口」を装う電話番号への連絡を促す
4. リモートデスクトップソフトをインストールさせる
5. 有償のサポートサービスの契約を促す



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”,
<https://www.ipa.go.jp/security/anshin/measures/fakealert.html>,（アクセス日:2024-1-4）

Webサイトの改ざん

- Webサイトの脆弱性（※1）が悪用され、個人情報やアカウント情報（ID・パスワード）等の重要な情報を窃取される被害が多発しています。



（※1） 脆弱性：コンピュータのOSやソフトウェアにおいてプログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことをいいます。

サイバー攻撃等によるインシデント発生にともなう事業活動への影響

- ITがビジネスや暮らしに深く浸透している現在、サイバー攻撃によって事業活動に影響を及ぼす範囲は広く、高額な損害をともなうインシデントも増えています。

金銭の損失

顧客などからの **損害賠償**

原因の調査、関係者対応などにかかるさまざまな **事故対応費用**

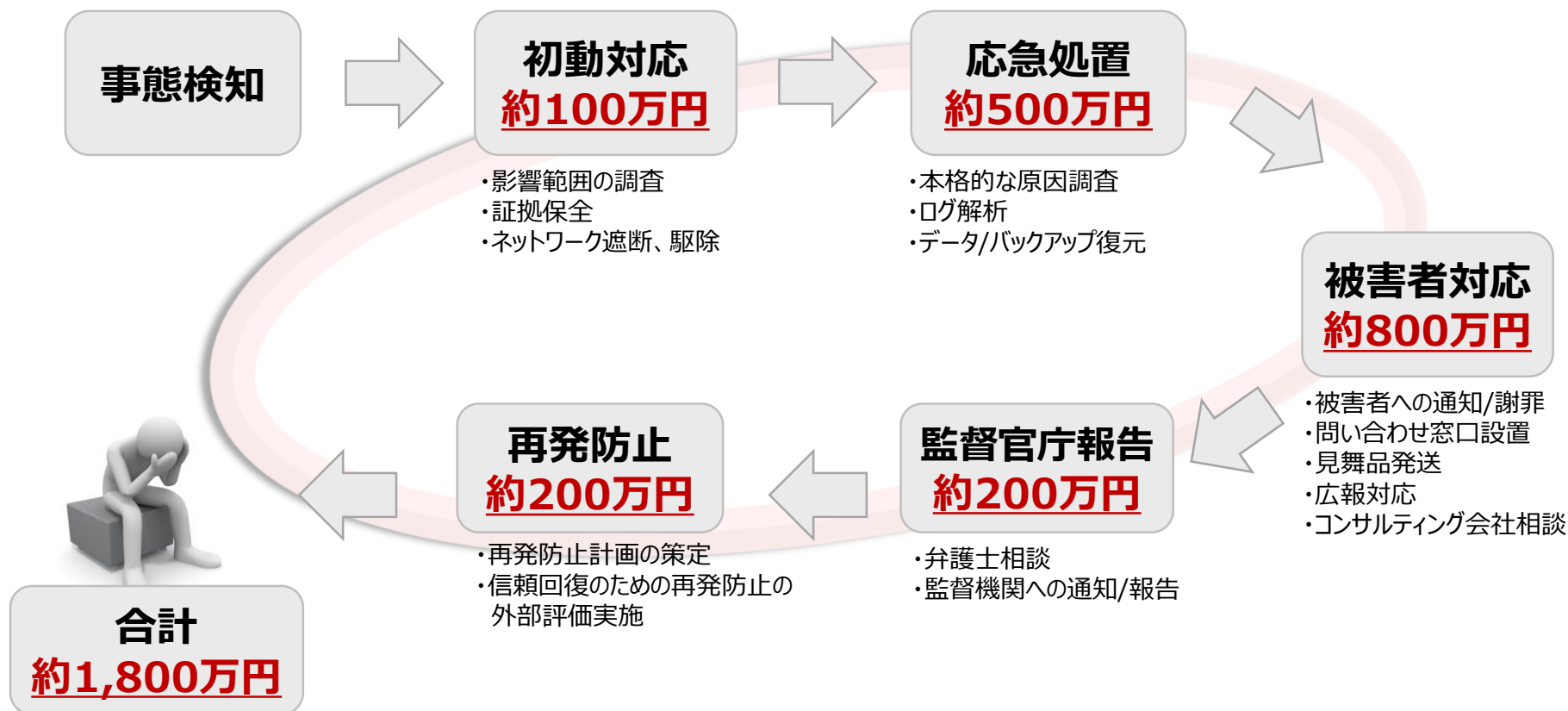
事業継続の阻害

業務関連システムやメールの停止による **サービス提供機会の損失**

組織内のモラル・士気低下が遠因となる **人材流出**

【想定事例】

組織内のパソコンがマルウェアに感染し、遠隔操作によりメールが発信され、パソコン内に保存していた自社や取引先の情報が漏えいした。



2

サイバーリスクへの対応のポイント

みなさんはどのように見えますか？




出典：<http://mathworld.wolfram.com/YoungGirl-OldWomanIllusion.html>, (アクセス日:2015-01-21)

- 「正常性バイアス」とは、人間の心理特性の一つであり、自然災害、事故、事件などといった何らかの被害が予想される状況下にあっても、自分にとって都合の悪い情報を無視したり、過小評価してしまうことをいいます。

喫茶店の座席などに鞆を置いてトイレに行く

飲食店でパソコンを開いて食事をする

社用車の中に鞆を置いて食事に行く

A cartoon illustration of a man with black hair, wearing a green shirt, with his arms crossed. Above his head is a large, light blue thought bubble containing three lines of text.

・周りに人がいるから盗
まれない！
・盗み見してる人がいた
ら気付く！
・ちょっとの時間だし！

残念ながら、このように多くの人や組織には正常性バイアスが存在します・・・

本当にサイバー攻撃は関係ないのでしょうか？

【重要】Amazon株式会社から緊急のご連絡

amazon.co.jp

【重要】カスタマセンターからのご案内

あなたのAmazonのアカウント：[redacted]@[redacted].jp、異常なログインが見つかり、配送先住所が変更されました！

ログイン日時：2020-05-27 4:23:31
IPアドレス：[redacted] [redacted] 212]
装備：iphone8 IOS 12.3.4
場所：水戸市

つきましては、お客様の情報を保護するために次の措置を講じました
- お客様のアカウントのパスワードを無効にいたしました。
- 不正アクセスによって行われた変更につきましては、無効にいたしました

お客様のアカウントに再度有効化していただけるようになります。次のリンクをクリックして指示に従ってください。

アカウント管理に移動

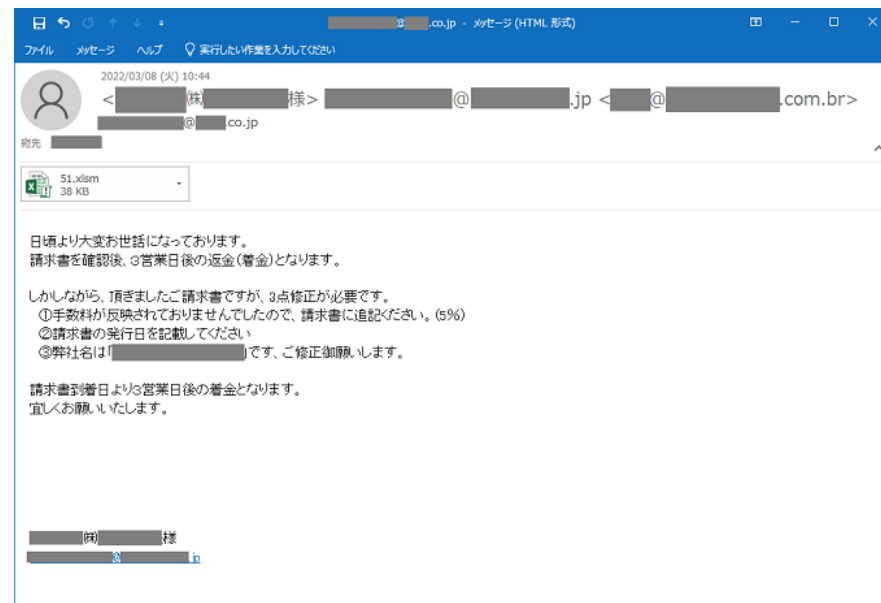
Copyright © 2020 Amazon Inc. All rights reserved
発行元：Amazon株式会社

<https://[redacted].click/>

Verification Code: [redacted]

メール文面の例

出典：フィッシング対策協議会。“Amazon をかたるフィッシング（2020/05/29）。”
https://www.antiphishing.jp/news/alert/amazon_20200529.html.”（アクセス日：2020-05-29）



出典：独立行政法人情報処理推進機構セキュリティセンター。
“Emotet（エモテット）と呼ばれるウイルスへの感染を狙うメールについて。”
https://www.ipa.go.jp/security/announce/20191202.html.”（アクセス日：2022-04-26）

偽宅配便業者

佐川急便よりお荷物のお届けに上がりましたが宛先不明の為持ち帰りました。[http://\[redacted\].com](http://[redacted].com)

お荷物の確認は日本郵便サイトに
てご確認ください。[http://\[redacted\].com](http://[redacted].com)

やまと運輸よりお荷物を発送しましたが、宛先不明です、下記より
ご確認ください。[http://\[redacted\].com](http://[redacted].com)

auお客様センターです。ご利用料
金のお支払い確認が取れておりま
せん。ご確認が必要です。[http://\[redacted\].com](http://[redacted].com)

ドコモお客様センターです。ご利用
料金のお支払い確認が取れており
ません。ご確認が必要です。
[http://\[redacted\].com](http://[redacted].com)

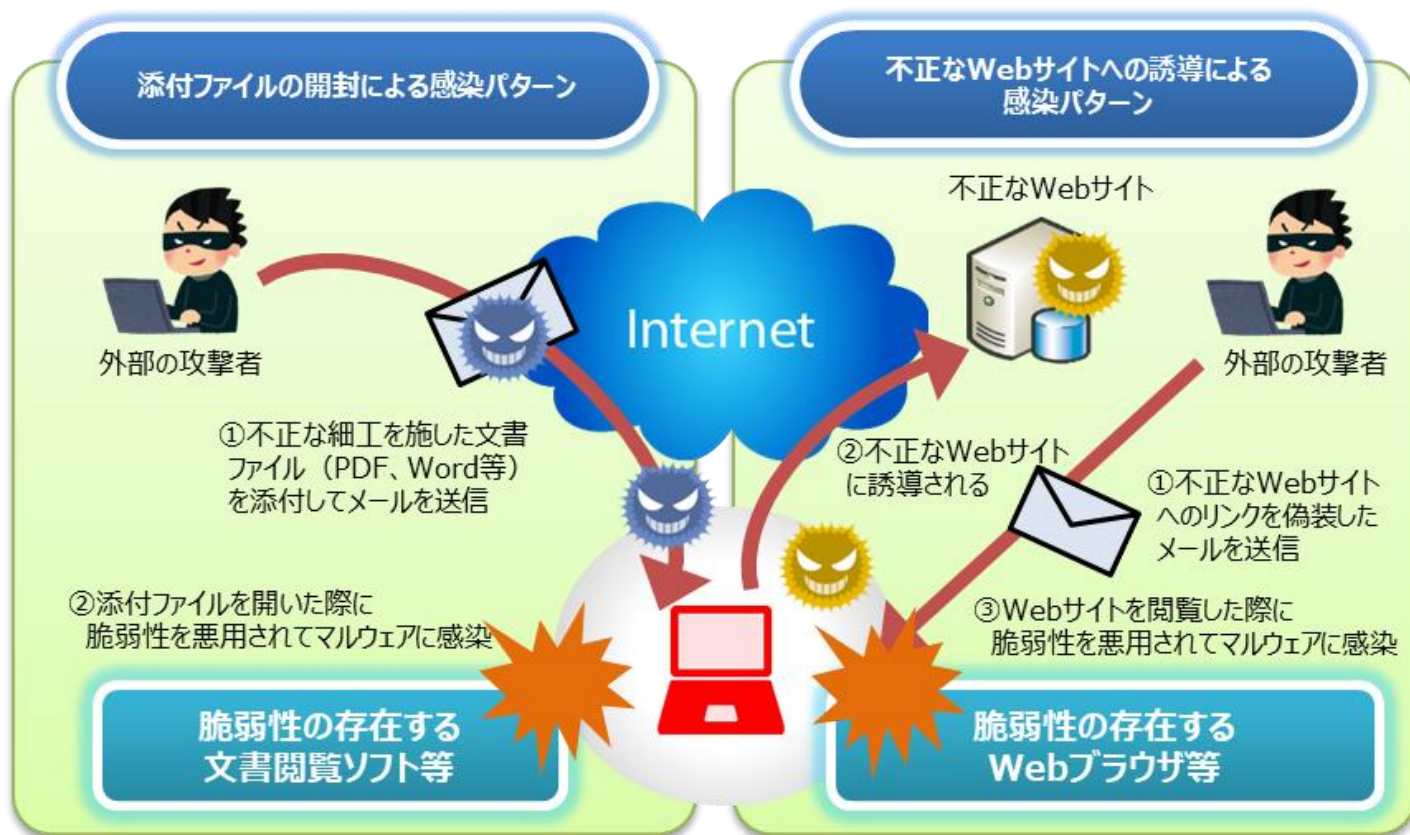
【KDDI】利用料金の未払い金があり
ます。お支払期限を過ぎた利用
料金があります。ご確認ください。
[http://\[redacted\].com](http://[redacted].com)

偽通信事業者

出典：独立行政法人情報処理推進機構セキュリティセンター。“安心相談窓口だより。”
https://www.ipa.go.jp/security/anshin/mgdayori20211222.html.”（アクセス日：2021-12-22）

不審なメールへの対応①

- 外部からの攻撃においては、攻撃者がもっともらしい偽の文面、件名のメールを標的とする組織宛てに送り、メールの受信者をだまして添付ファイルを開封あるいはURLをクリックさせ、PC端末をマルウェアに感染させる手口が多く利用されています。



不審なメールへの対応②

- 不審なメールを介した手口は多種多様かつ常に進化しており、システム（技術）で攻撃を防ぐことはある程度可能ですが、限界があります。
- そのため、このような標的型攻撃メールに対しては、「人」と「システム」の両面の観点から、複数の対策を組み合わせることが最も有効です。

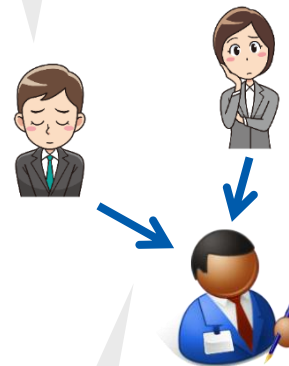
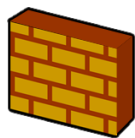
モニタリング（検知）

経路上で怪しい
通信先やファイルを
ブロック

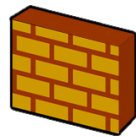
PC上で
怪しいファイルや
動きをブロック

パソコンのOSやソフトウェアを
最新化して、
脆弱性を露呈しない

それでもすり抜けてくる
通信の存在を認識し、
ユーザが注意を払う



経路上で怪しい
通信先やファイルを
ブロック



P

ウイルス対策ソフトと不審な
挙動を検知・防御するソフト
(EDR) の最新維持

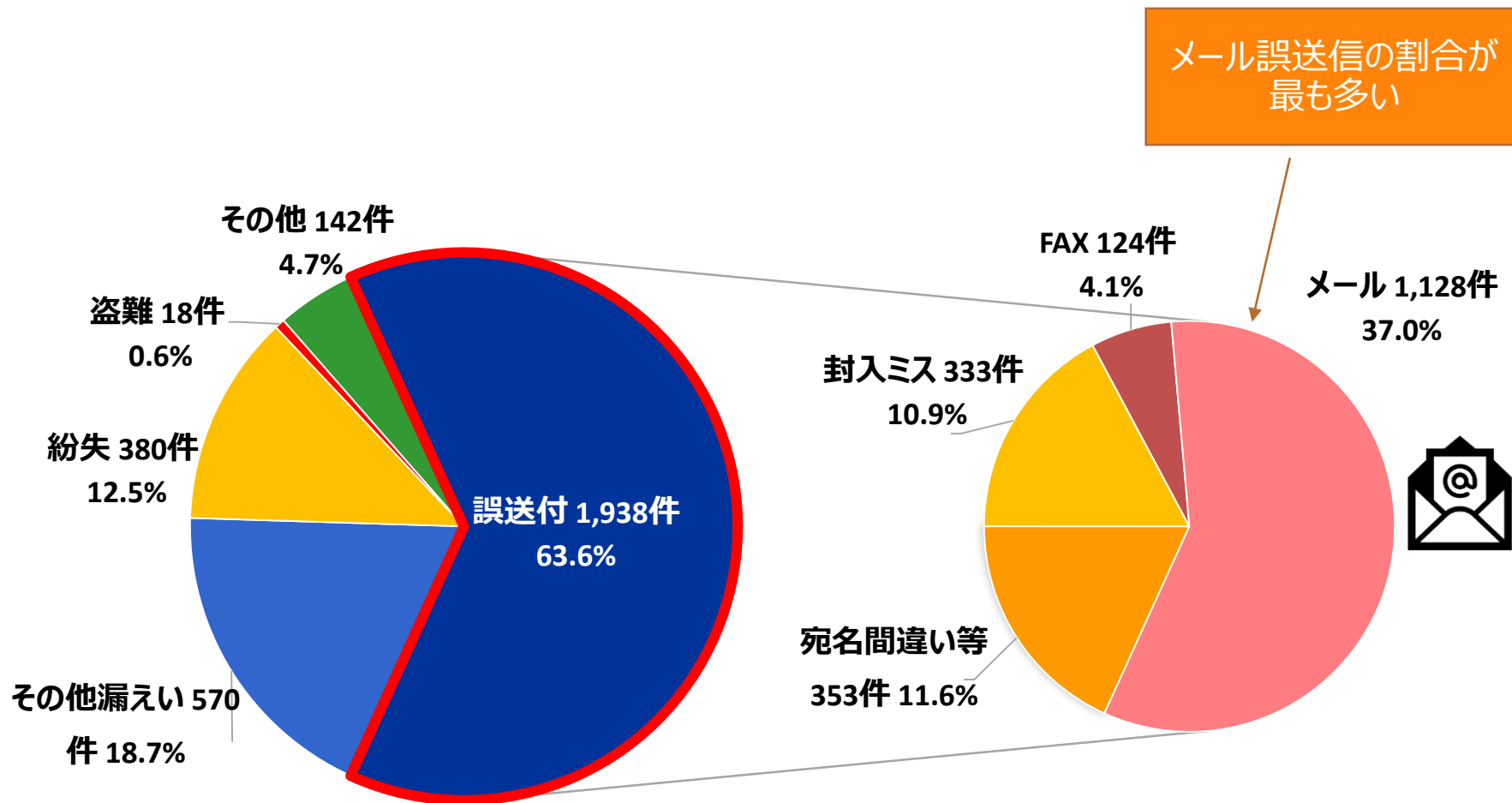
ファイアウォール機能や不審な送受信を検知・防御する
機能を持つ統合機器（UTM）の最新維持

怪しいメールの添付ファイルを開いたかも！
URLリンクに接続してしまったかも！
という時はすぐに上司や情報システム部門に連絡

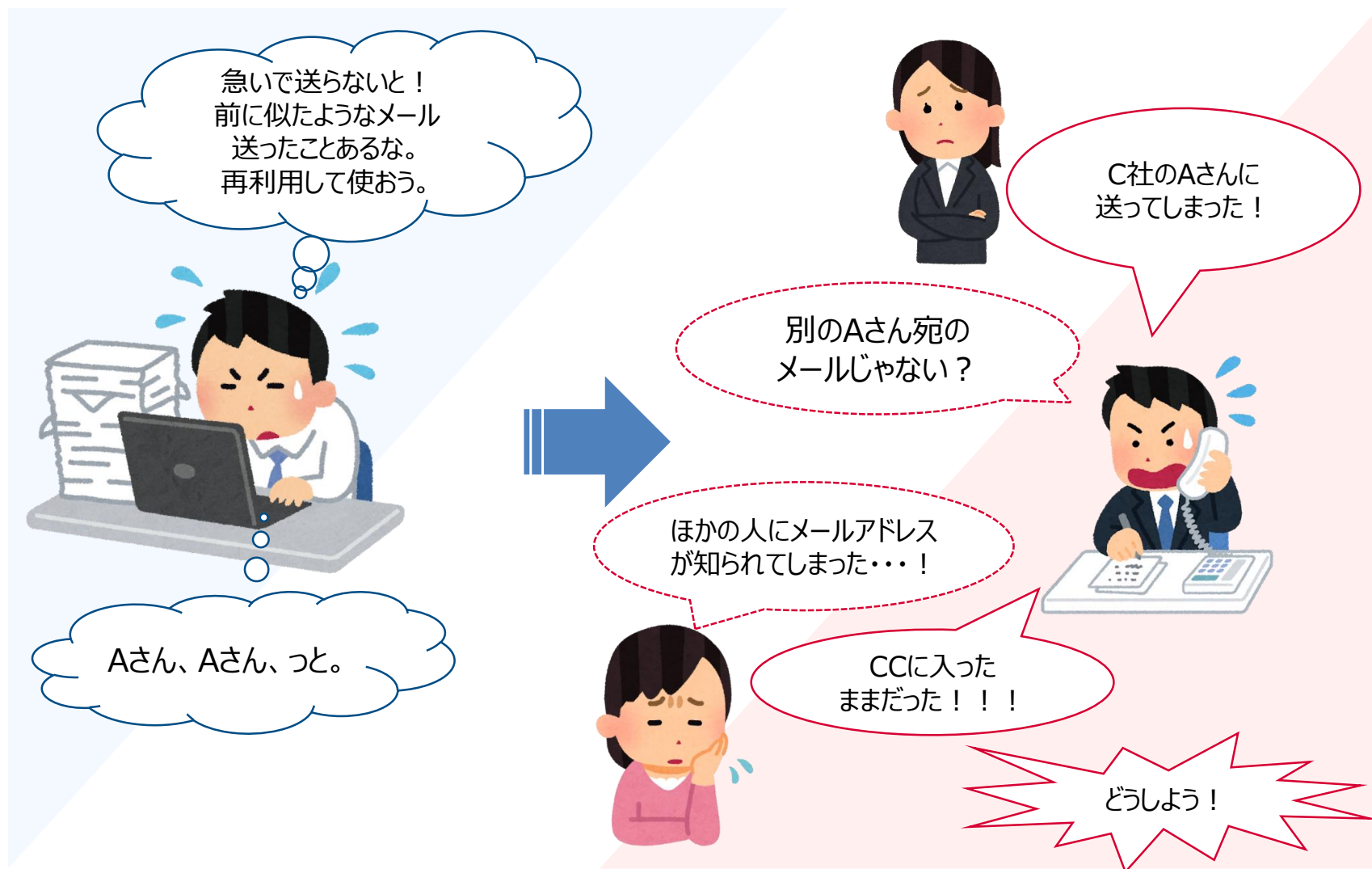
P

インシデント発生時の相談先の確保

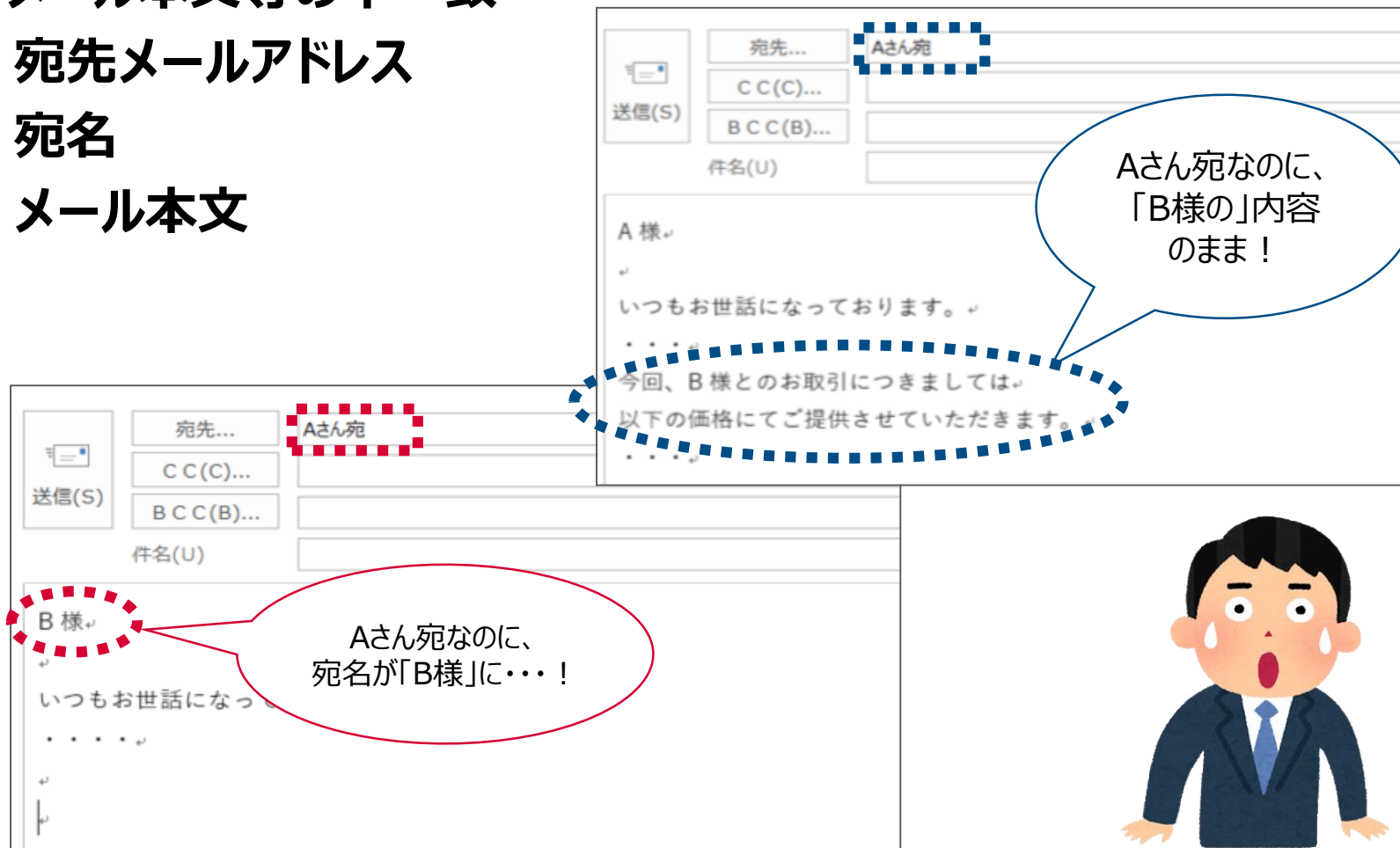
- 近年、情報セキュリティに対する意識の低さに起因とした漏えいも散見されます。



一般財団法人日本情報経済社会推進協会（JIPDEC）プライバシーマーク推進センター. 2021年度「個人情報の取扱いにおける事故報告集計結果」を参考に作成



- ・メール本文等の不一致
宛先メールアドレス
宛名
メール本文



・アドレス帳からの選択ミス

名前	所属	アドレス
A田さん	A社	a@example.jp
A田さん	B社	b-a@example.co.jp
A田さん	C社	aaaa@example.ne.jp

どのA田さん？

送信(S) 宛先... A田さん
C C(C)...
B C C(B)...
件名(U) 資料の件

A 田様
いつもお世話になっております。

・アドレス入力ミス


別の佐藤さんに届いてしまった！

送信(S) 宛先... sato@example.co.jp
C C(C)...
B C C(B)...
件名(U)

佐藤様

sato@example.co.jp
⇒ 本来は、satou@example.co.jpが正しい

・送信先アドレス欄の選択ミス



The screenshot shows an email composition interface. On the left is a '送信(S)' (Send) button with a paper plane icon. To its right are three fields: '宛先...' (To), 'B C C (B)...' (BCC), and '件名(U)' (Subject). The '宛先...' field contains a list of email addresses: xxx@example.jp; yyy@example.co.jp; zzz@example.jp; aaa@example.ne.jp; bbb@example1.co.jp; ccc@example2.ne.jp; ddd@example1.jp; eee@example9.co.jp; fff@example1.jp. A dashed blue box highlights the 'B C C (B)...' field, which is currently empty. Below the fields is the '件名(U)' field with the text '社員募集の件' (Recruitment of staff). At the bottom is the email body with the text 'この度は、弊社の社員募集にご応募いただきありがとうございます' (Thank you for applying to our company's recruitment).

BCC (※1) にするはず
だったのに！

(※1) BCCとは、ブラインド・カーボン・コピー（Blind Carbon Copy）の略で、CC：と同様に宛先の相手へ送った内容について、他の人にも知らせたい場合に使用しますが、ここに入力されたメールアドレスは受信者には表示されません。他の受信者がいることや、他の受信者のメールアドレスをわからないようにしたい場合は、BCC：を使用します。

出典：総務省."国民のための情報セキュリティサイト.",
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/04.html

・添付間違い

The screenshot shows an email composition interface. The '宛先...' (To) field contains 'Aさん宛'. The '件名(U)' (Subject) field contains '資料の件'. The '添付ファイル(T)' (Attachments) field shows a document icon and the text '(B様) 見積書.docx .docx ファイル'. A blue dashed box highlights the attachment field. A speech bubble points to the attachment with the text '添付ファイルを間違えた！' (I attached the wrong file!). The email body contains 'A 様' and 'いつもお世話になっております。'.

・隠れた原稿添付

The screenshot shows an email composition interface. The '宛先...' (To) field contains 'Aさん宛'. The '件名(U)' (Subject) field contains 'リストの送付'. The '添付ファイル(T)' (Attachments) field shows a spreadsheet icon and the text '〇〇リスト.xlsx 10 KB'. A red dashed box highlights the attachment field. The email body contains 'A 様' and 'いつもお世話になっております。'.

A社のほかに、B社とC社の
シートが入っていた！

5			
6			
	A社	B社	C社

3

サイバー攻撃等によるインシデント発生時における対応

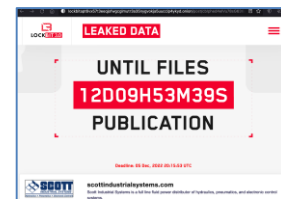
サイバーインシデント発生かも!? いったい何が起きてるの？

突然、職員から報告が...

『パソコン画面に変な表示が出て、全く操作ができない!!』

『ファイルが開けない!! 急いでいるのに!!』

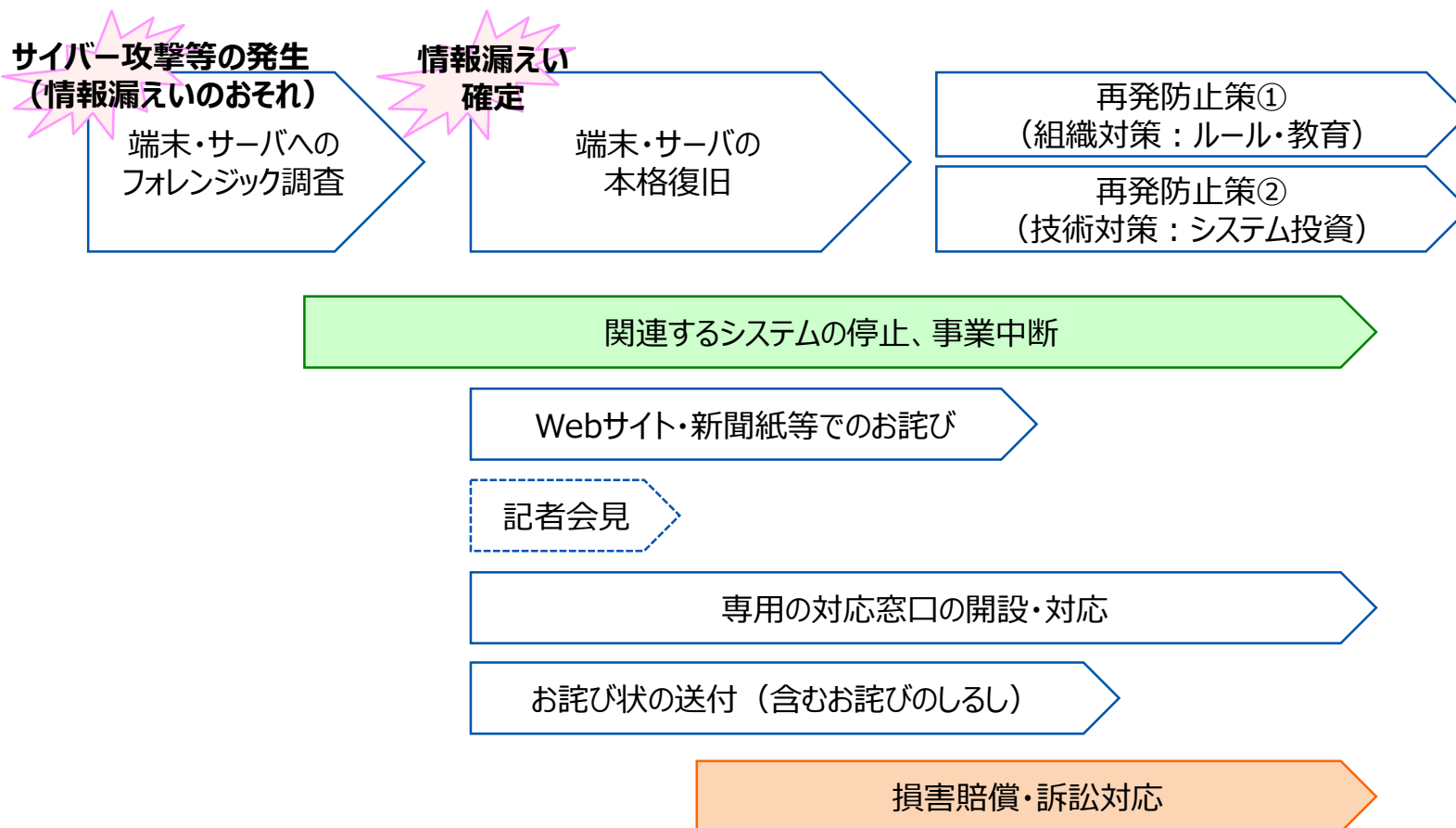
『ワタシも!!』 『私も!!』 『みんなも?』



この時、まず何をしなければならないか、すぐに思い浮かびますか？

サイバー攻撃等によるインシデント対応（例）

- 実際にサイバー攻撃等によるインシデントが発生した場合、多くの組織ではあらかじめ緊急時対応の手順を決めていても、緊急時対応による現場の混乱を抑えつつ対応方針を決定し、適切な対応を実施することが困難になる場合が多く見受けられます。



その時、今後に向けた『イメージ』ができないと？..

インターネットが使えない？
メールが使えない？
or 使用禁止を指示？

パソコンが使えない？
or 使用禁止を指示？

パソコン依存の業務？
請求も、振込も
サービス提供も止まる？

3日間？一週間？
わからない？

まずは調べなきゃ！
いつものIT業者へ!!
サポート契約外？新規見積？

取引先で影響が発生？
お詫び？ご説明？
損害が出てる？

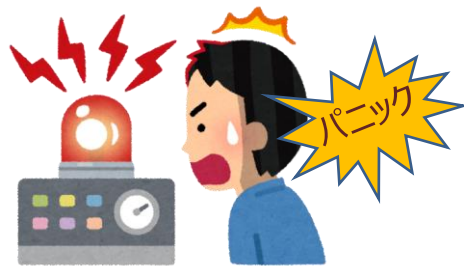
犯罪？届出？
各方面へ速やかに報告？

他の取引先からも説明要求？
安全確認まで取引中断？



インシデント発生時における対応①セキュリティ担当者への異常報告

異常を見つけた人が必ずしも
セキュリティ担当者ではない



情報システム部門に
連絡するため
周りの協力を得る



インシデント対応はここからスタート



何かあったみたい

私には関係がない

今時間がないな！

インシデント発生時における対応②ステークホルダーへの対応も重要！

- 不正アクセス等により、1件でも個人情報を漏えいしてしまうと個人情報保護委員会への報告および本人への通知が必要となります。

■ 個人情報保護委員会への報告義務化（努力義務から「義務化」へ）

漏えい等が発生し、個人の権利利益を害するおそれがある場合に、個人情報保護委員会への報告（速報：発覚日から3～5日以内、確報：発覚日から30日以内〔不正な目的で行われたおそれがある場合は、発覚日から60日以内〕）および本人への通知が義務化されます。

＜対象事案（それぞれの漏えいの「おそれ」がある場合も対象）＞

- ✓要配慮個人情報の漏えい
- ✓不正アクセス等による漏えい
- ✓不正の目的をもった漏えい
- ✓1,000件を超える漏えい

件数に関わらず対象

サイバー攻撃等の発生
（個人情報that漏えい）



- ◆漏えいの原因がわからない
- ◆被害範囲がわからない
- ◆再発防止策がわからない



適切な報告・通知ができない



インシデント発生時における対応③発生前なら安く済む対策コスト

- 当社がインシデント対応を支援した組織さまからは、セキュリティ対策や体制整備の未実施を悔やむ声が多く聞かれます。
- またインシデント発生前に比べ、発生後はセキュリティ対策の要求が高くなるとの声も聞かれます。

組織さまの声

- 1 聞いてはいたが、自社が巻き込まれるとは思ってもいなかった
- 2 誰が何をどこへどのように対応するかも決まっておらず、混乱した
- 3 業務影響が大きく、システム部門の問題ではないと身に染みた
- 4 外部から通報を受ける前にせめて内部で先に気付きたかった
- 5 謝罪対応からお客さまのセキュリティ意識の高さを痛感した
- 6 自社の管理状況が十分でなく、謝罪時の説明に窮した
- 7 インシデント後はセキュリティ要求レベルが高まり、対策のコストがかさむ

- サイバー攻撃はどれだけ対策を万全にしたとしても完全に防ぐことはできない（リスクをゼロにできない）ため、リスクの一部を他者へ移転することも有効な対策となります。

損害賠償責任

被保険者（補償の対象者）が法律上負担する損害賠償金や争訟費用等による損害を補償

損害賠償費用**争訟費用****事故対応費用**

サイバー事故に起因して一定期間内に生じた各種費用を補償

事故原因調査**コールセンター設置****記者会見****見舞金の支払****法律相談****再発防止策の策定****利益損害****営業継続費用**

ネットワークを構成するIT機器等が機能停止することによって生じた利益損害（喪失利益・収益減少防止費用）や営業継続費用を補償

※上記の補償のほか、保険会社によっては関連する付帯サービス（情報セキュリティ診断サービス等）を提供している場合があります。
※補償内容は保険会社や保険会社が提供するサイバー保険のプランにより異なります。詳細は保険会社・代理店にご確認ください。

- インシデントの発生時から、事象のヒアリング、初動対応の判断やアドバイス、原因究明や被害影響範囲の調査、对外発表、監督官庁への報告、恒久対策にいたるまで、**緊急時に必要な一連の対応を戦略的にコーディネート**します。

⇒**初動対応（判断やアドバイス）は無償で利用**できます。その他インシデントの対処に必要となるサービス（デジタルフォレンジック、データリカバリ等）の提案、再発防止の為のコンサルティング等を含む**恒久対策は有償**となります。



まとめ

- サイバー攻撃はより儲かりやすい攻撃に進化し、様々な業種の組織に被害が拡大している
- セキュリティ対策は被害を受ける前の方が低コストである
⇒ 「技術」的な観点だけでなく、「組織・人」による多層的な体制強化によって速やかに対処することが重要
- サイバー保険は「保険金」のみならず「付帯サービス」を活用する
⇒ 平時からパートナーとの協業体制を確認し、万が一被害にあったときには速やかに対処できるようにしておくことが重要

ご清聴ありがとうございました。



Innovation for Wellbeing

SOMPOリスクマネジメント

サイバーセキュリティ・コンサルティング部

〒160-0023 東京都新宿区西新宿1-24-1 エステック情報ビル

[TEL] 0120-211-180

[E-mail] cyber@sompo-rc.co.jp

[URL] <https://www.sompocybersecurity.com/>



SOMPO CYBER SECURITY