HYLANT

FRIENDS OF FINDLAY & HYLANT

PRESENTS

企業を取り巻くサイバーリスク

February 8, 2023

企業を取り巻くサイバーリスク

1.サイバーを取り巻く環境　Hylant

2.サイバー保険　Hylant

3.企業を取り巻くサイバーリスク　SGR
～現状とベスト・プラクティス～

4.Q&A

Presenter from Hylant

田中伸司

Shinji Tanaka

Vice President

Business Development Executive

Hylant Group, Inc.

Address : 24 Frank Lloyd Wright Dr., Ann Arbor | MI 48105

Telephone : 248-974-8580

E-mail : Shinji.Tanaka@hylant.com

日本出身（東京都練馬区）

現Hylant Group、Vice President/Business Development Executive。

1987年東海銀行入社。

1999年より三井住友海上火災保険トロント事務所長。

2004年より三井住友海上火災保険デトロイト事務所長。

2020年より現職。

米国中西部を中心に日系企業向け損害保険・健康保険の営業を担当。

労災保険・物流保険の分析による保険コストの削減、ギャップ分析などが得意分野。

Presenter from Hylant

シャーウィンまゆか

Mayuka Sherwin
Vice President
Client Executive
Hylant Group, Inc.
Address : 24 Frank Lloyd Wright Dr., Ann Arbor | MI 48105
Telephone : 201-314-6993
E-mail : Mayuka.Sherwin@hylant.com

日本出身（兵庫県芦屋市）
現Hylant Group、 Client Executive/Vice President。

米国損害保険ブローカー営業として24年の経験を持つ。日本・ニューヨークでカスタマーサービスオペレーションの主管担当。1999年よりニューヨークにて伊藤忠商事保険部門の海外法人にて保険ブローカー業務開始、2012年MarshにてClient Executive/Vice President、そして2018年よりArthur J. GallagherにてAsia Pacific Practice Senior Director/Area Vice President、 2020年より現職。

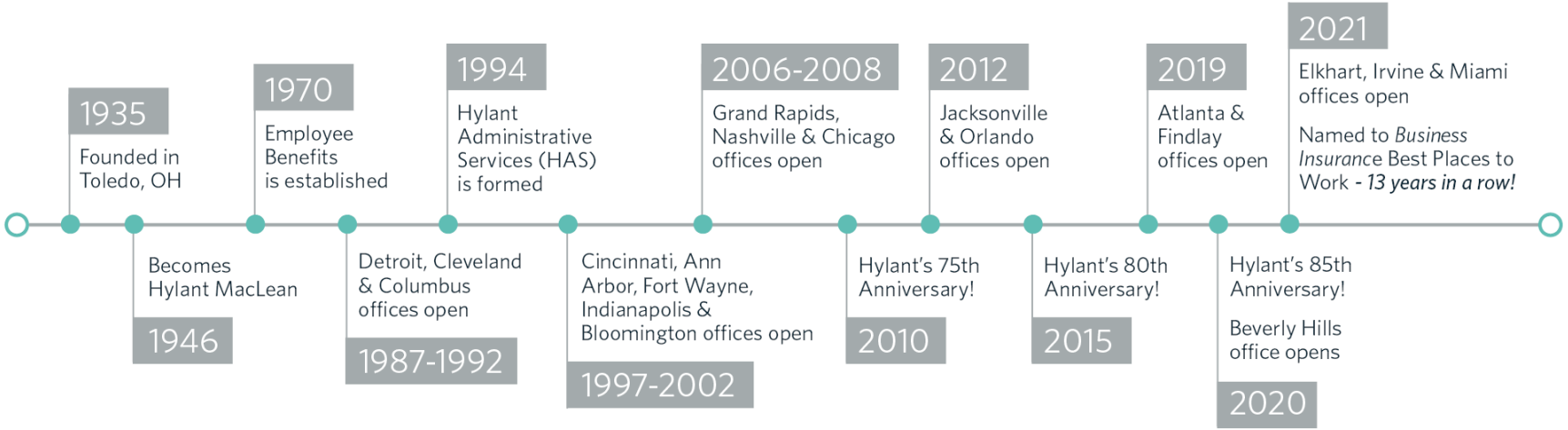
中西部を中心に日系企業向け損害保険・健康保険の営業を担当。
損害保険分野で日系企業の抱える問題の対応・改善・解決のリスクコンサルティング及び、福利厚生プログラムのコンサルティングサービスを提供。

THE HYLANT STORY

HYLANT MISSION STATEMENT

To strengthen and protect the businesses, employees and communities of our client family by embracing them as our own.

HYLANT'S HISTORY



OUR FOOTPRINT 弊社の軌跡

弊社ハイラントは1935年に設立、オハイオ州トレド市に本社を置く非上場企業です。現在約970名の保険専門家を擁し、中西部を中心に8州18拠点よりお客様のリスクマネージメントを行っています。

CALIFORNIA
- Encino

FLORIDA
- Jacksonville
- Miami
- Orlando

GEORGIA
- Atlanta

ILLINOIS
- Chicago

INDIANA
- Bloomington
- Elkhart
- Fort Wayne
- Indianapolis

MICHIGAN
- Ann Arbor
- Detroit
- Grand Rapids

OHIO
- Cincinnati
- Cleveland
- Columbus
- Findlay
- Toledo

TENNESSEE
- Nashville

WE ANSWER TO YOU

BUSINESS INSURANCE RANKINGS

#9	#30	#26
全米9位 非上場の保険 ブローカー	全米30位 法人向け 保険ブローカー	全米26位 医療・健康 保険ブローカー

数字で見るハイラント
HYLANT BY THE NUMBERS

970+ EMPLOYEES
従業員数：970名超

20,000 CLIENTS
クライアント数：2万社

95% YTD RETENTION
顧客定着率：95%

$3B+ IN PREMIUM DOLLARS
取扱い保険料：約30億ドル

BUSINESS INSURANCE
BEST PLACES TO WORK 2022
2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022

Ranked a Best Places to Work in Insurance for 14 years running.

HYLANT JAPANESE PRACTICE

- 弊社Japanese Practice部門は、日系企業様に特化して損害保険・健康保険・個人保険をご提供する専門部署です。
- アトランタ・ミシガン・ニューヨークに拠点を持ち、12名（内、6名は日本語・英語バイリンガル）からなる保険のプロ集団であり、日系の保険部門としては国内最大級を誇ります。
- 大手ブローカー・保険会社で20年以上の経験を積んだプロフェッショナルが、保険プログラムを精査・分析・戦略・改善のお手伝いを致します。
- Hylantは、非上場企業なので規模は追求しません。我々は、個々のお客様に対するベストな保険ソリューションを提供するコンサル型ブローカーです。
- 保険のカバレッジ漏れ・重複の検証、コスト削減のための大胆な切り口、保険料のモデル化、リスクマネージメントなど、非上場ブローカーが得意とする独自性の強いアドバイスをご提案を致します。

Shinji Tanaka
Ann Arbor, MI
248-974-8580
Shinji.Tanaka@hylant.com

Mayuka Sherwin
Ann Arbor, MI
201-314-6993
Mayuka.Sherwin@hylant.com

Tian Tian
Atlanta, GA
201-245-8598
Tian.Tian@hylant.com

Yuriko Kyobashi
Atlanta, GA
404-630-9150
Yuriko.Kyobashi@hylant.com

Alex Zhu
New York, NY
201-247-2251
Alex.Zhu@hylant.com

CLIENT PARTNERSHIPS　クライアントリスト（抜粋）

KLOSTERMAN

The Anderson-DuBose Company

Kellogg's

OWENS CORNING

GLICK
GENE B. GLICK COMPANY

DANA

Marathon Petroleum Corporation

Winsupply
THE WINSUPPLY FAMILY OF COMPANIES

DAMAR

MIURA

MIZUNO

molten

1. サイバーを取り巻く環境

ホンダ襲った標的型ランサムウエアの正体、3度目のサイバー攻撃で世界9工場が停止

外薗祐理子　日経クロステック／日経コンピュータ

2020.07.31

全4075文字

Social engineering takes center stage in latest Marriott bre

By Erin Ayers, Advisen

Marriott Hotels confirmed a new data
on July 6 that affected just one hotel
in Baltimore and exposed credit card
information and other data for 300 to 4

トヨタの工場を止めたサイバー攻撃　サプライチェーン攻撃のリスクが露呈

島津 忠承　日経コンピュータ

2022.03.14

全2920文字

トヨタ自動車のサプライチェーン（供給網）に連なる小島プレス工業がマルウエア被害を受けた。これがきっかけで、トヨタの14工場の28ラインが止まった。かねて指摘されていた「サプライチェーン攻撃」のリスクと被害の大きさが浮き彫りになった。

トヨタ自動車の主要サプライヤーの1社として自動車の内外装部品を生産する小島プレス工業が、マルウエア（悪意のあるプログラム）の感染被害を2022年3月1日に公表した。この影響からトヨタ自動車に加えグループの日野自動車、ダイハツ工業が同日の一部生産を見合わせた。

誰が、なぜ？　史上最悪規模・ソニー個人情報流出事件を時系列順に整理

2011年05月06日 19時41分 公開　[小林伸也，ITmedia]

印刷　見る　Share　B!　372

情報流出を公表するSCEのサイト。情報開示の遅れが批判されている

ソニーグループのオンラインサービスから合計1億件以上の個人情報が流出した可能性がある事件。ソニートップの経営責任の追及や、ソニーのタブレット端末などネットワーク製品戦略に与える悪影響への懸念など、史上最悪規模の個人情報流出事件のインパクトは大きい。今回の事件を時系列順に整理すると、その発端は1年半近く前にさかのぼることになる。

2009年後半：ハンドルネーム「geohot」で知られ、2008年にiPhoneのセキュリティを破った米国人ハッカー、ジョージ・ホッツ氏（1989年10月生まれ）がプレイステーション 3

（PS3）のハックに挑戦する

米ヤフー｜2014年のサイバー攻撃でユーザー情報５億人分が流出したと発表

インターネットサービス大手の米ヤフー（Yahoo）は、2016年９月22日、2014年に同社が受けたサイバー攻撃により、少なくとも５億人分のユーザー情報が流出していたことを発表しました。

サイバー攻撃、日本に矛先　3年で攻撃数倍増

チャートは語る

チャートは語る　＋フォローする
2023年1月22日 2:00 [有料会員限定]

保存

Think!　多様な観点からニュースを考える　森幹晴さん他1名の投稿

【この記事のポイント】

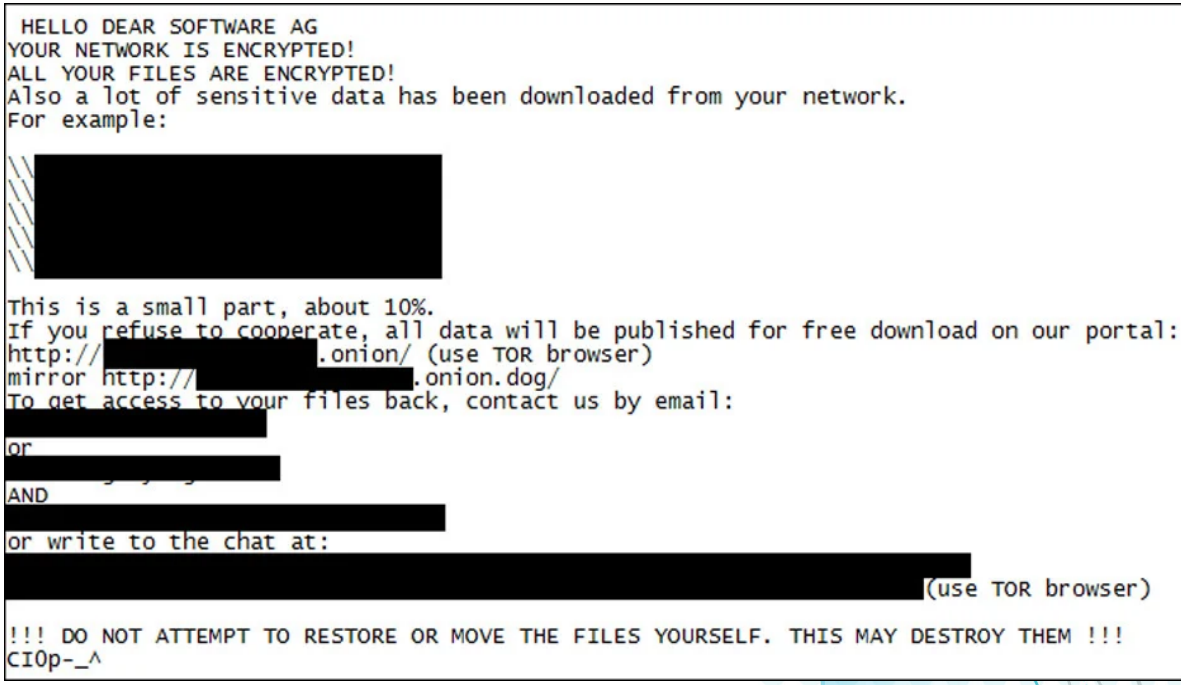
- 海外からのサイバー攻撃が3年で倍増。対応も遅く
- 「翻訳ソフトの発達で日本語による壁が崩れつつある」
- 開発丸投げの慣習。サイバー防衛への当事者意識薄く

サイバーを取り巻く環境

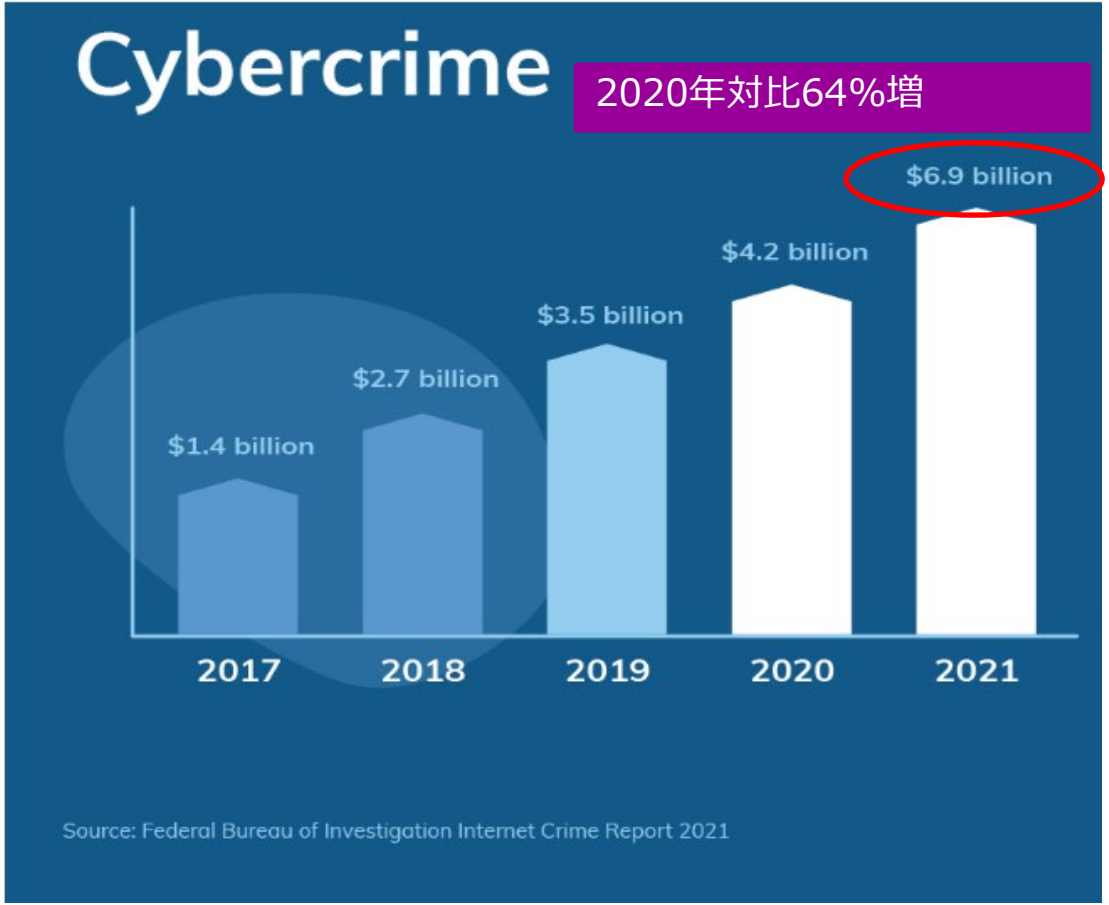
Software AG
右側は、2020/10/3にSoftware AGをターゲットとした$23Mの身代金を要求した実際の恐喝文です（ランサムウエア）。

身代金を断った事例：
City of Atlanta
2018年4月に$52,000の身代金を要求。謝絶した結果、データが破壊され$17Mの被害が発生。

City of Baltimore
2019年4月に身代金として$100,000のビッドコインを要求。謝絶した結果、$18M+の被害が発生。



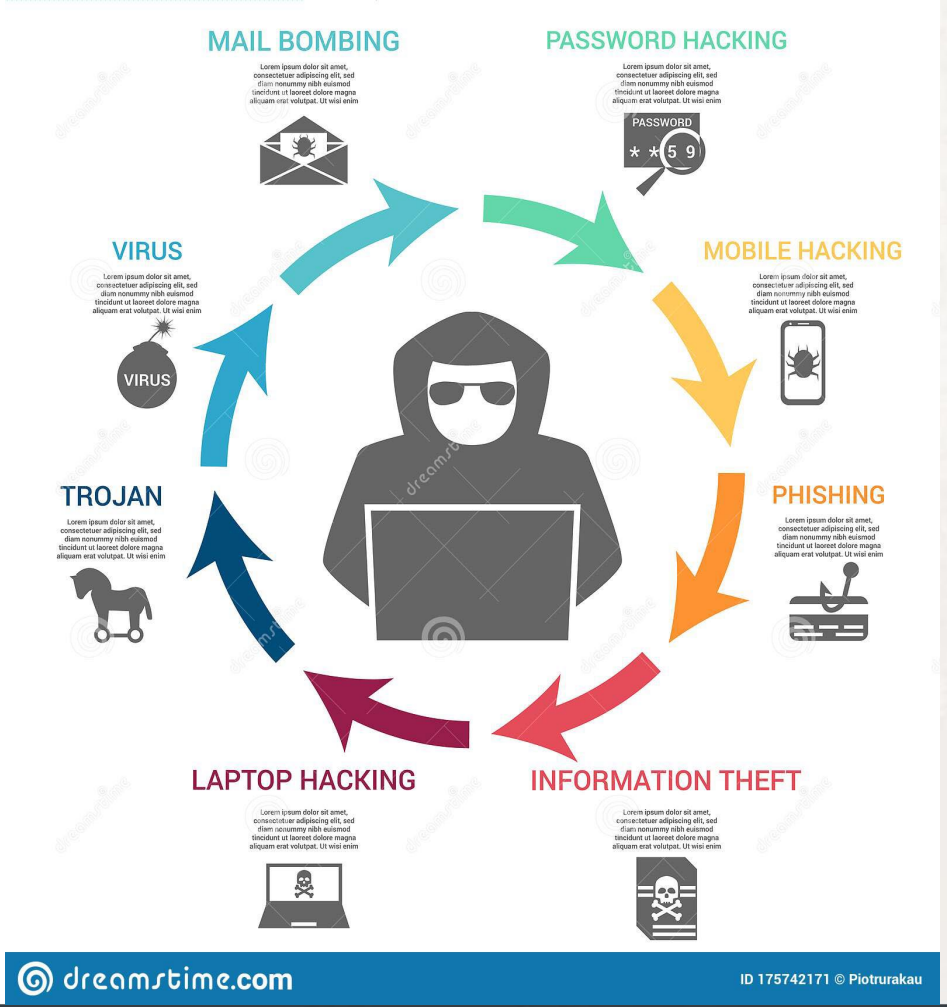
サイバーを取り巻く環境（FBIのInternet Crime Report 2021より）



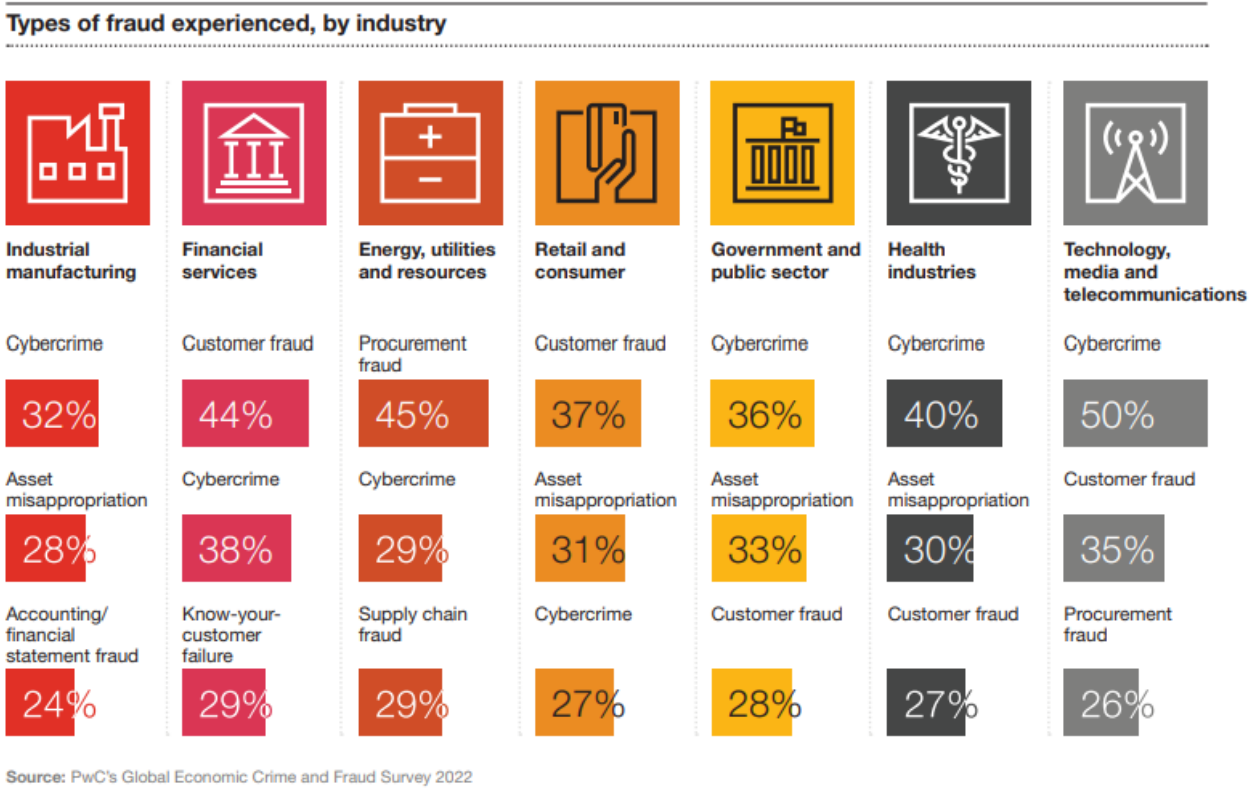
サイバーを取り巻く環境

サイバー犯罪のActorたち

- サイバーギャング
- 国家
- 従業員
- 政治・社会的活動犯 (Hacktivists)
- Dark Web （闇サイト）
- Yelp Review （ハッカーレーティング）

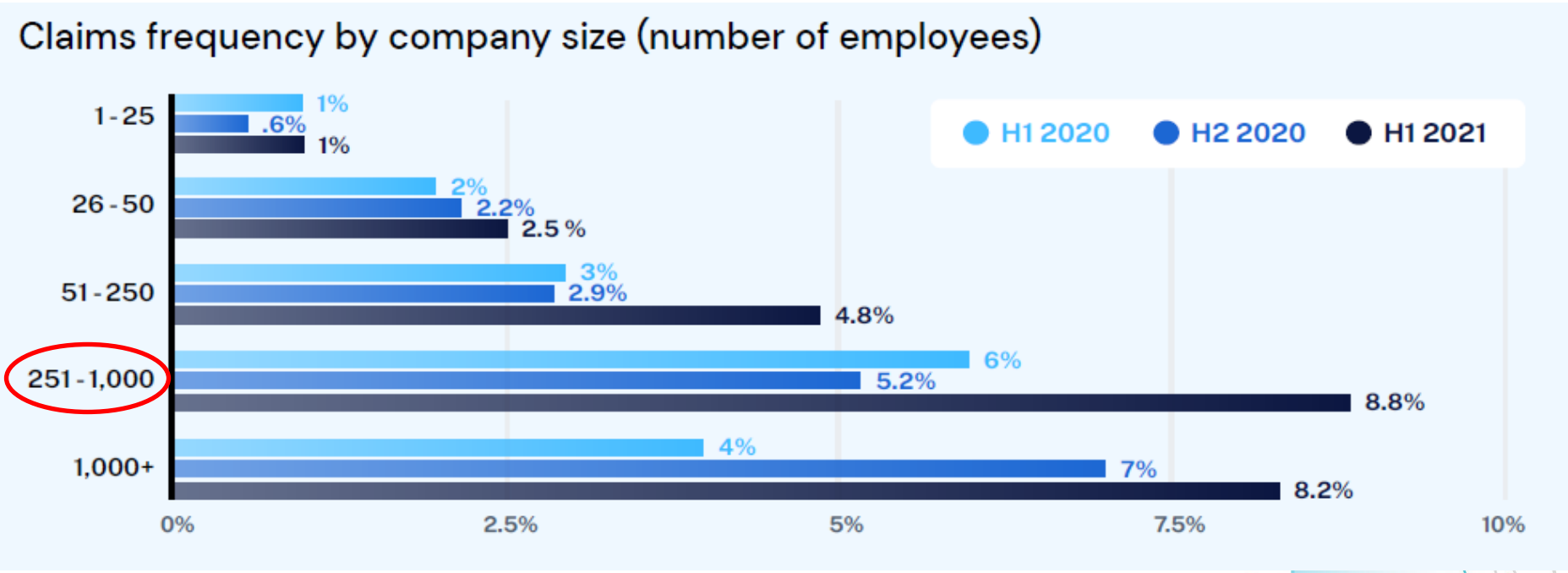


サイバーを取り巻く環境（詐欺犯罪に関する統計）



PwC社の2022年版調査によると、**製造業の32%が過去2年間に何らかのサイバー被害に合っている。**

サイバーを取り巻く環境（中規模企業がターゲット）



サイバーを取り巻く環境（サイバー攻撃の手口）

- **ビジネスメール詐欺　(Business Email Compromise)**

FBIによると、2021年に24億件のビジネスeメールアカウントがハッキングされ、うち、振込詐欺が約15億件に使用。

- **ランサムウエア　(Ransomware)**

ランサムとソフトウェアを組み合わせた造語で、暗号化する事でファイルを利用不可な状態にした上で、そのファイルを元に戻す事と引き換えに金銭（身代金）を要求するマルウェア。

- **フィッシング**

メールなどに記載したリンクなどで有名企業や取引先を装った偽のサイトに誘導し、個人情報（クレジットカードや銀行口座情報）を騙し取る。

- **サプライチェーン攻撃**

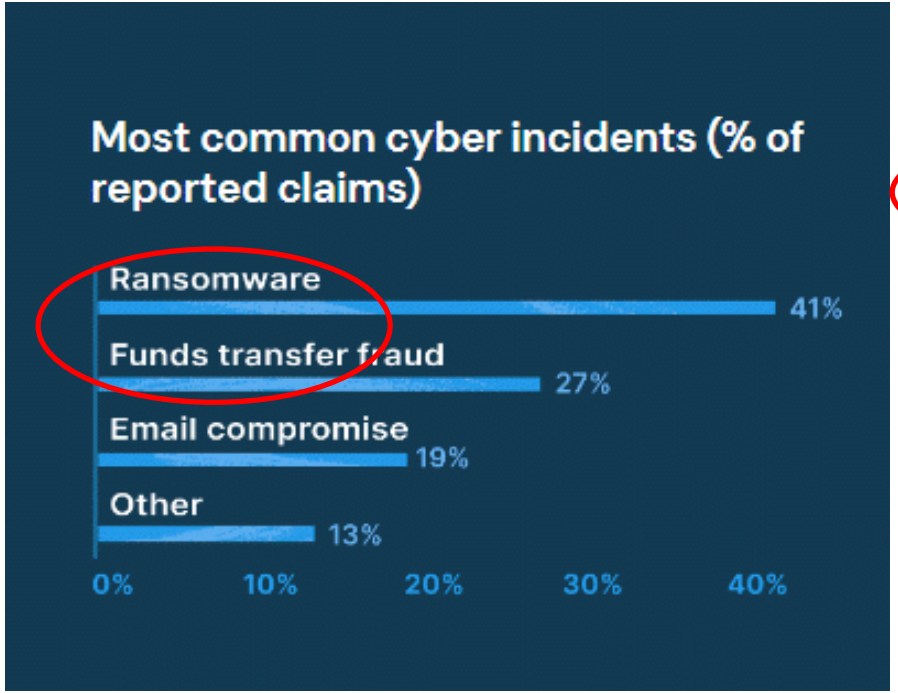
標的企業に直接サイバー攻撃を仕掛けるのではなく、セキュリティレベルの低いと思われる子会社や協力企業（サプライチェーン）を攻撃、踏み台にして標的企業のシステムに不正侵入する。

- **Dos攻撃**

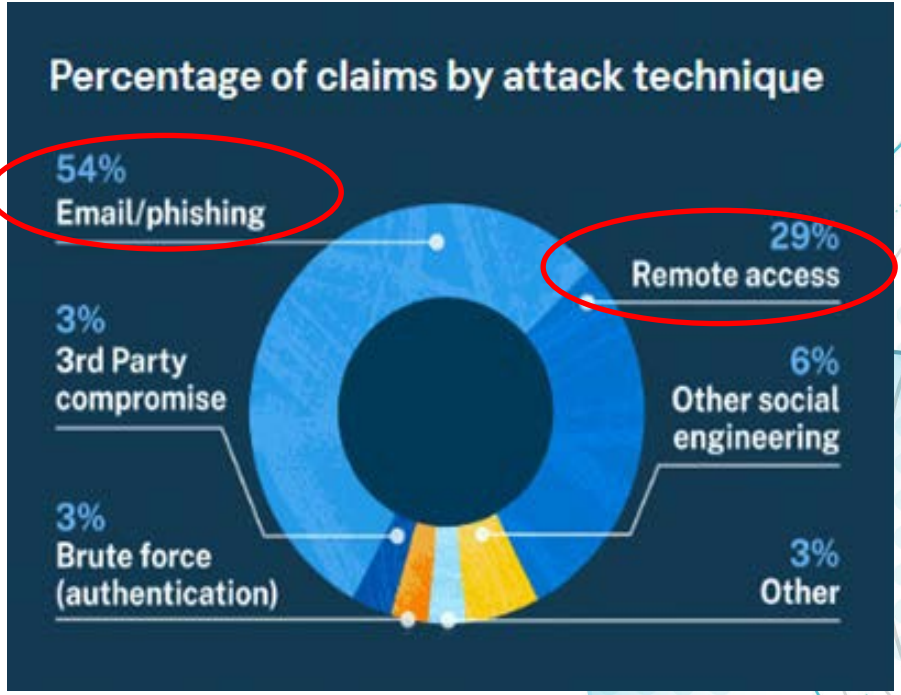
”Denial of Service Attack”の略称で、アクセスが集中することでサーバーがパンクする事を利用し、悪意をもってサーバーに大量のデータを送りつけるサイバー攻撃。

サイバーを取り巻く環境（サイバー攻撃の手口）

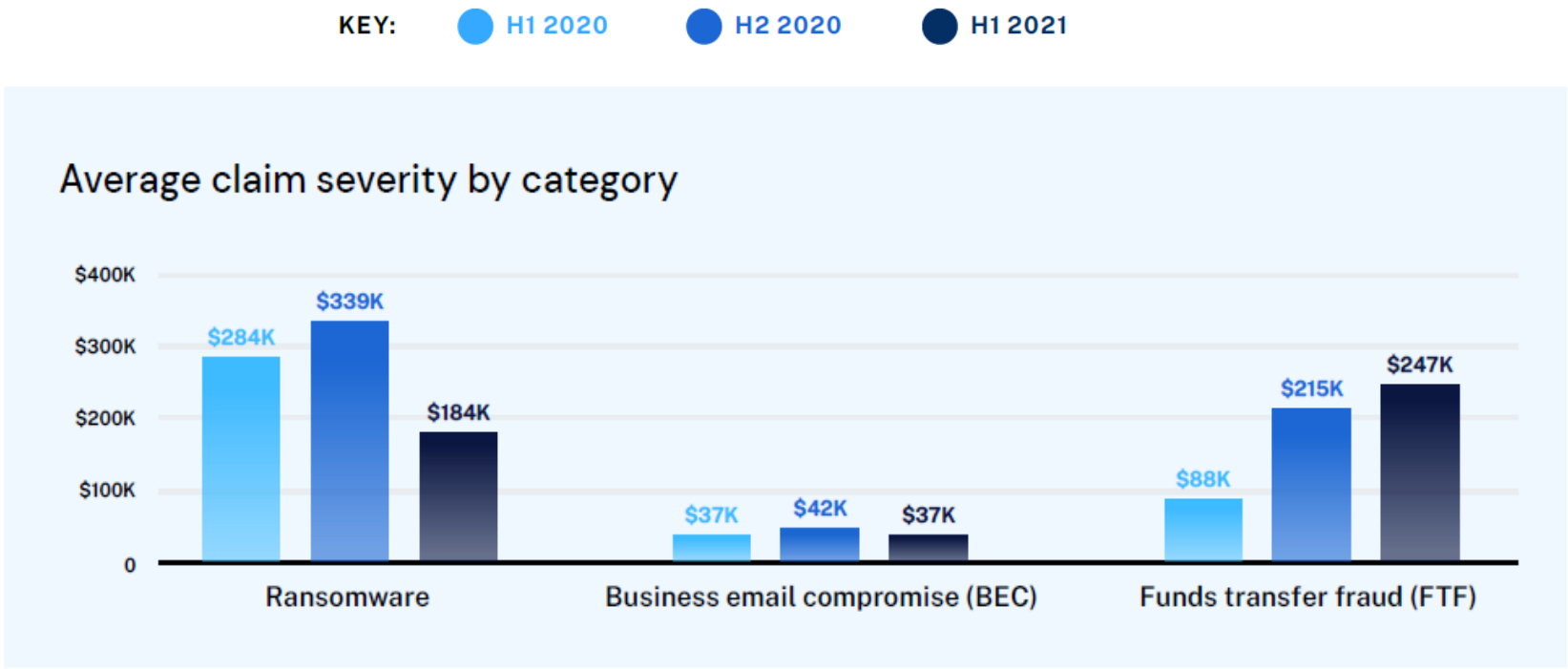
サイバー犯罪の分類



アクセス手法



サイバーを取り巻く環境（手口別の保険金支払い金額）



Coalition社（保険会社）の統計

サイバーを取り巻く環境（サイバー攻撃の手口・最近のトレンド）

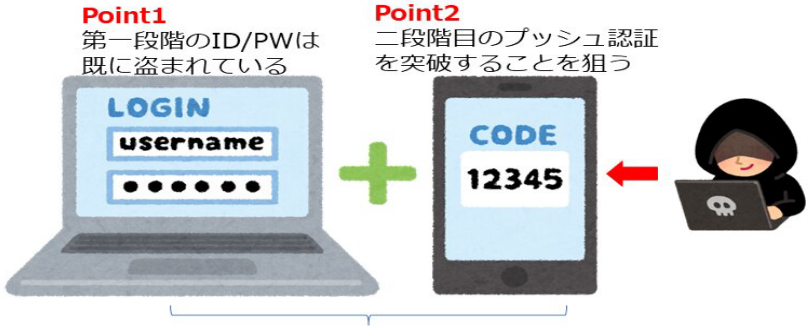
- **多重認証疲労攻撃(Multi Factor Authentication Fatigue)**

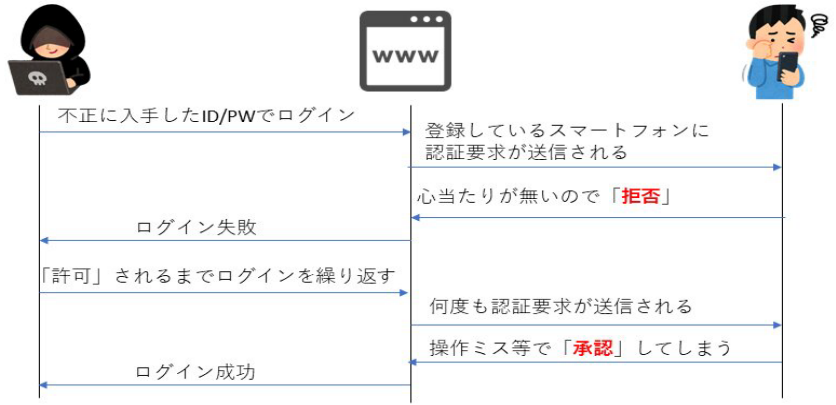
不正アクセスを防止する目的で企業による多重認証(MFA)の導入が急速に進んでいます。しかし、サイバー攻撃者は普及したMFAを突破するために「多重認証疲労攻撃(MFA Fatigue)」と呼ばれる攻撃によって攻撃成果を挙げています。

■多要素認証疲労攻撃とは?

「プッシュ」通知を利用する多重認証に対して、わざとプッシュ通知を乱発することで、うっかり「承認」することを期待する攻撃手法です。
この攻撃が成立する前提条件としてIDとパスワードはサイバー攻撃者が既に入手していることが前提となります。

ハッカーは第1段階の認証を既に盗んだIDとパスワードで突破しますが、MFAがある場合、登録されているスマートフォンに認証要求が「プッシュ」されます。
勿論受け取った当人は自分がログインしていないので最初「拒否」しますが、ハッカーは何度もこれを繰り返します。何度も繰り返しているうちに、心理的攻撃から「システムテスト」かもしれないと誤解し、「承認」ボタンを押させるように仕向けます。
その瞬間にハッカーは不正アクセスに成功、そしてシステムに入り込みます。





2. サイバー保険について

最近のトレンドに関する統計

- 2021年の統計によると、**37%**のグローバル企業がサイバー攻撃を受けている。
- 小規模企業でサイバー保険を購入しているのは**17%**に過ぎない。
- 2021年のRansom（身代金）は前年比大幅増、平均支払い金額は**$300k**程度。
- Breachからサイバー犯罪の発見まで平均**287日**。
- Ransomwareによるサイバー犯罪から、平均**20日**で復旧。

サイバー保険の特徴

他の損害保険と類似点：

- **偶然外来**の損害を担保
- **保険約款**の構成

他の損害保険と相違点：

- 事故の際、**緊急性**
- 保険会社によりカバー内容が**大きく異なる**
- カバレッジが**日々変化**する

サイバー保険のカバー内容

First Party Coverage: 自社の損害

Incident Response
（事故対応費用）

Business Interruption
（利益損害）

Cyber Extortion
（身代金請求）

Social Engineering
（ソーシャルエンジニアリング）

一般的なカバレッジ

First Party　(自社の損害)

Incident Response （事故対応費用）	**サイバー攻撃に対する修復費用全般**。侵入経路の確認及びシステム・データの修復。 その他にも弁護士、コンサル、事故の告知、広告、クレジットモニター、IDモニター、苦情対応センター設置、など。
Business Interruption/Extra Expense （利益保険、臨時営業継続費用）	**Business Interruption（利益保険）** サイバー事故により操業が停止、その間に発生する**利益損害**。 **（保険金：操業停止中の見込み利益＋固定費）** **Extra Expense（臨時営業継続費用）** 営業を最低限度継続させるための臨時費用。 例：代替システム機器のリース費用、ITスタッフの残業代金、本邦からの空輸費用。
Contingent Business Interruption （構外利益保険）	自社ではなく、サプライヤー・客先がサイバー被害に会うことで、間接的に操業停止、その間に発生する利益損害。

利益損害は製造業に大きな損害

一般的なカバレッジ

First Party　(自社の損害)

Cyber Extortion **身代金請求**	システムを乗っ取り、復旧のために身代金を請求。
Social Engineering **ソーシャルエンジニアリング**	システム経由で偽の情報を送り、パスワードや金銭をだまし取るタイプの詐欺。 例）サプライヤーになりすまし、偽の請求書・銀行口座を送付。
PCI Expenses **ペイメントカード**	クレジットカードなどPayment Card Industryによる被害。

Third Party Coverage: 第三者賠償

Security Liability（セキュリティ関連の賠償責任）

Regulatory Penalties (公的機関からの罰金)

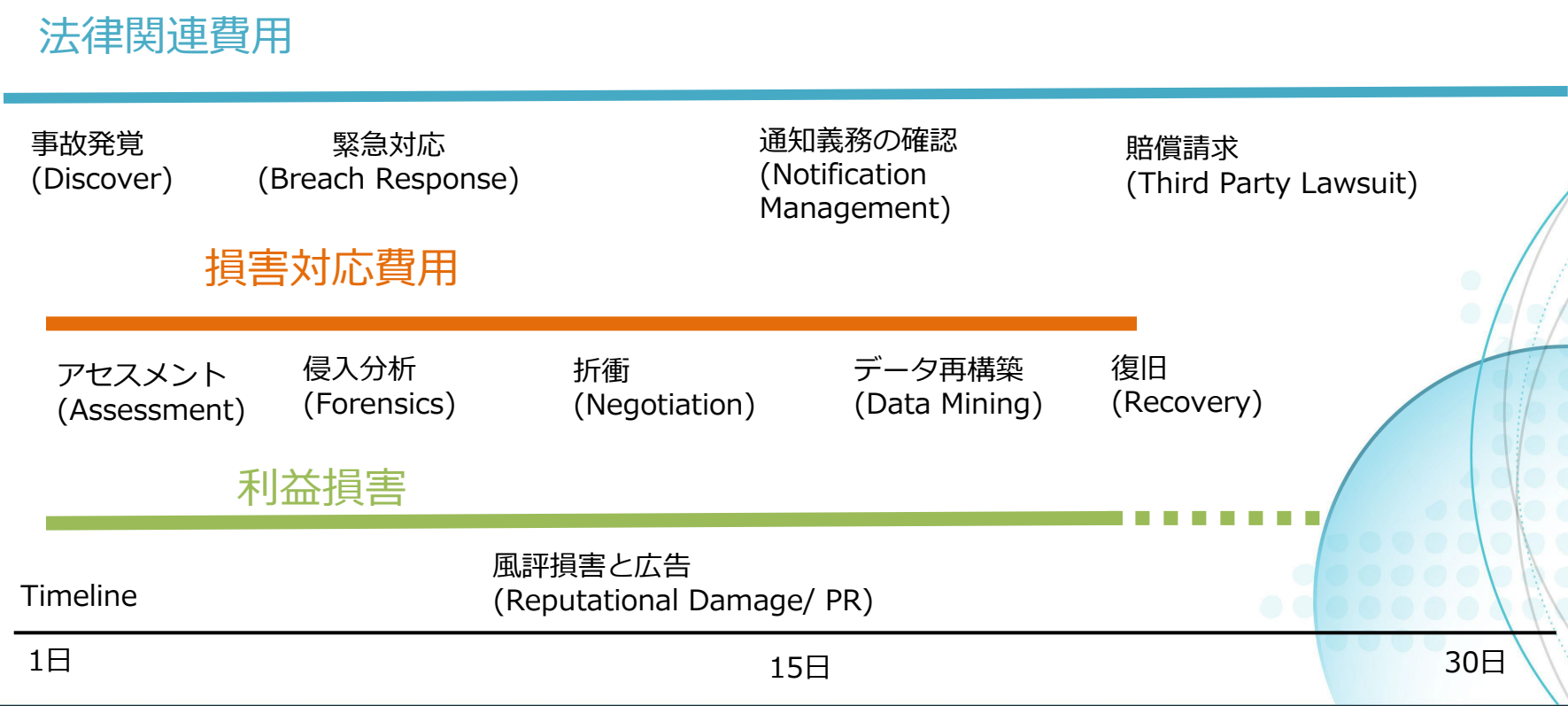
Privacy Liability (個人情報漏洩による賠償責任)

Media Liability (メディア関連の賠償責任)

一般的なカバレッジ

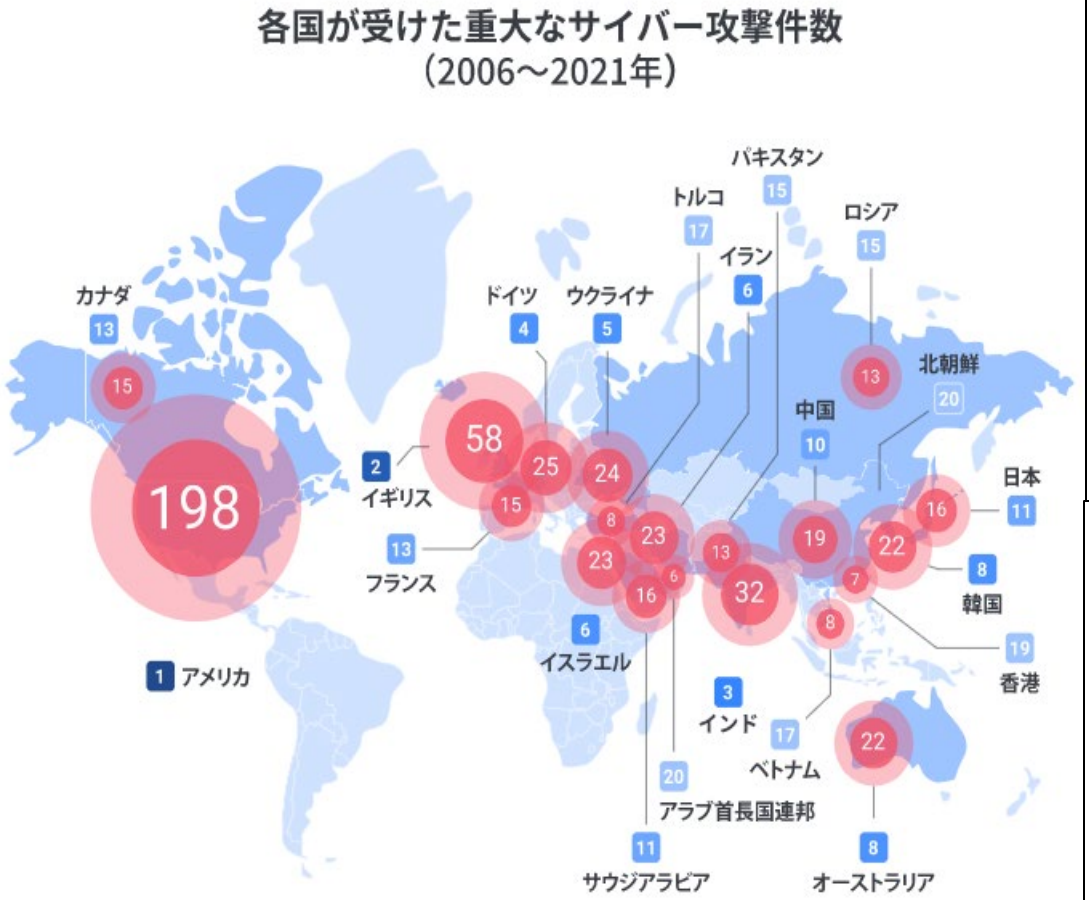
Third Party　(賠償責任)	
Privacy & Network Security Liability	サイバーセキュリティの不備により発生する賠償責任。 例）個人情報の漏洩 例）自社経由で取引先にハッカーが侵入
Regulatory Fine/Penalties	公的機関からの罰金、それに伴う調査費用・弁護士費用、など (取引先などからの罰金は原則カバーされません。)
Media Liability	メディア経由で発生する賠償責任。 例）ソーシャルメディアを介して他社を誹謗中傷など。

タイムライン例


法律関連費用
事故発覚
(Discover)
緊急対応
(Breach Response)
通知義務の確認
(Notification
Management)
賠償請求
(Third Party Lawsuit)
損害対応費用
アセスメント
(Assessment)
侵入分析
(Forensics)
折衝
(Negotiation)
データ再構築
(Data Mining)
復旧
(Recovery)
利益損害
風評損害と広告
(Reputational Damage/ PR)
Timeline
1日
15日
30日

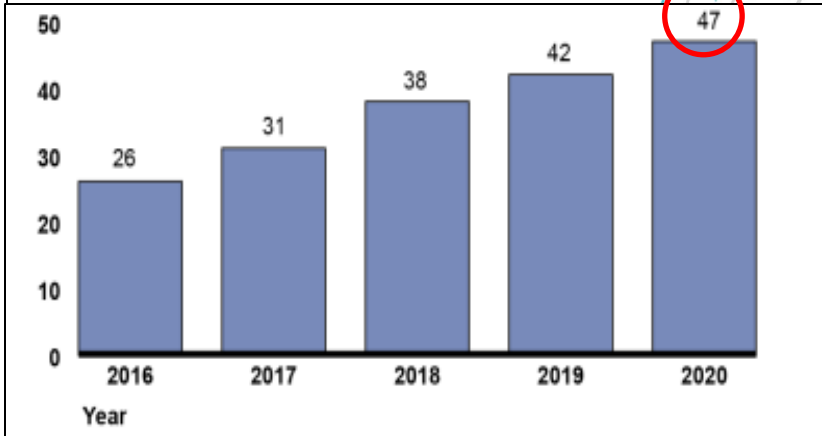
サイバー保険（年間保険料の目安）

従業員数 / 補償金額	25名	100名	500名	1000名
$1M	$7,000	$12,000	$18,000	$25,000
$2M	$14,000	$24,000	$36,000	$50,000
$3M	$21,000	$36,000	$54,000	$75,000



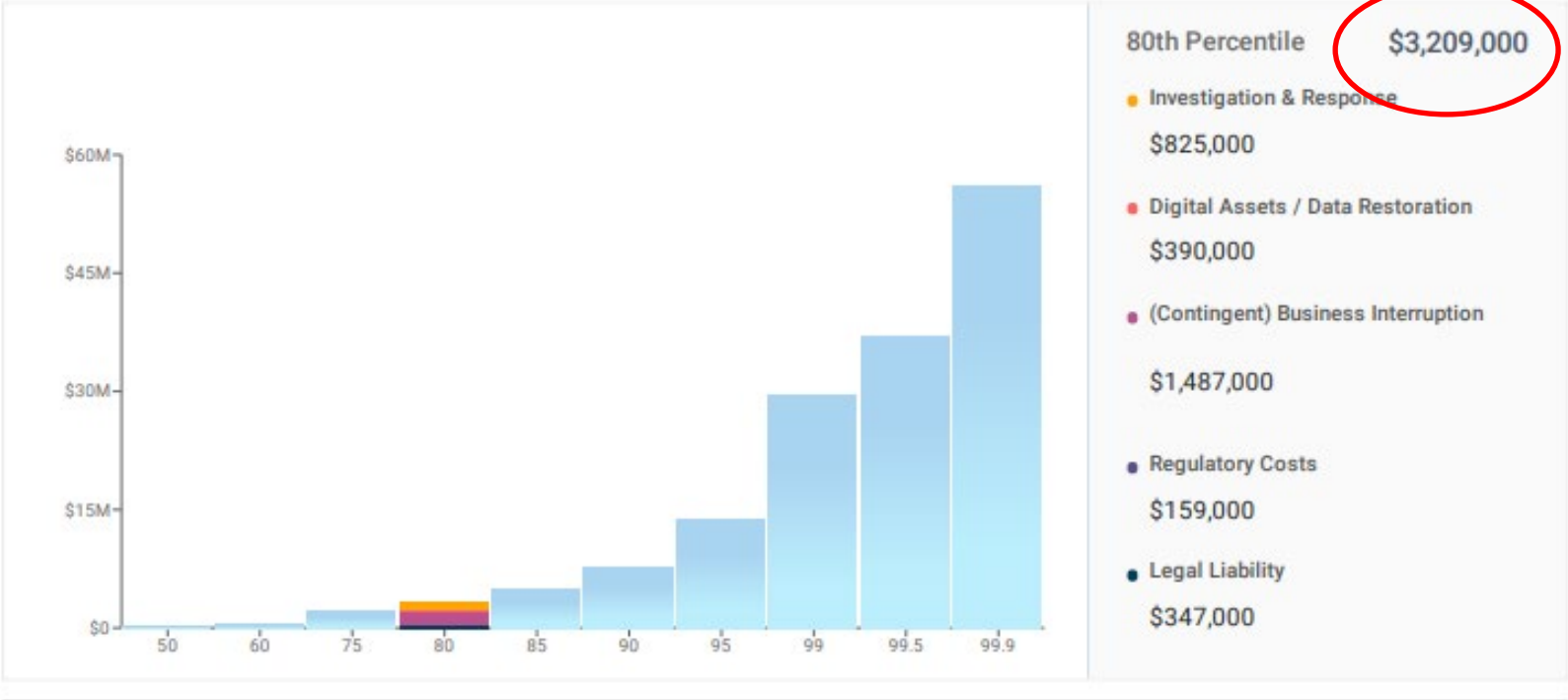
米国でのサイバー保険加入率

- 損保協会の調査によると、日本では8%。
- 本社に米国での状況を理解して貰いにくい。



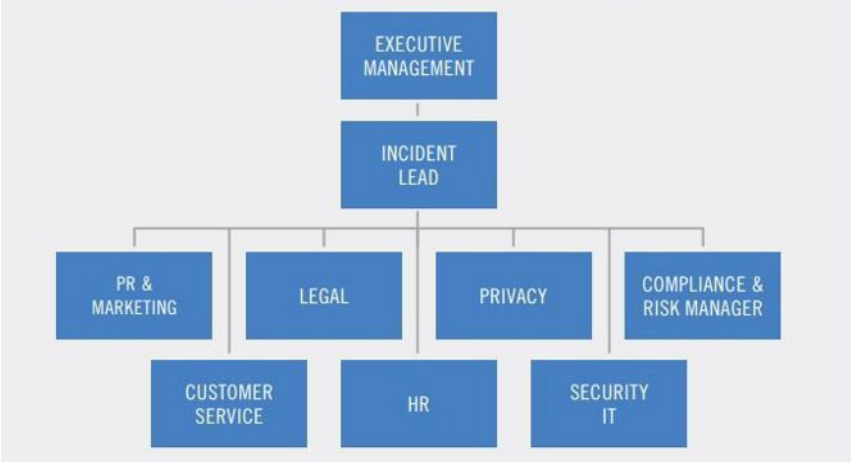
補償金額

製造業での例

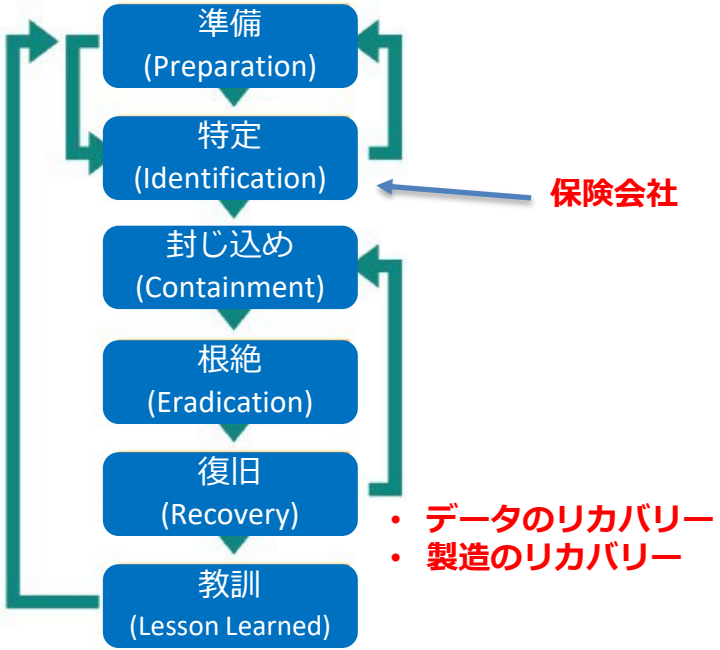

$60M
$45M
$30M
$15M
$0
50
60
75
80
85
90
95
99
99.5
99.9
80th Percentile
$3,209,000
Investigation & Response
$825,000
Digital Assets / Data Restoration
$390,000
(Contingent) Business Interruption
$1,487,000
Regulatory Costs
$159,000
Legal Liability
$347,000

事故時の対応計画

社内レスポンスチーム



レスポンスのモデル



事前確認事項

1. 保険で利用できるT業者の確認
2. 身代金支払いの際の決定権者
3. IT部門の対応責任者・指揮者・各自の役割
4. 保険クレーム手続き方法

サイバー保険（損害防止・最小化）

Multi Factor Authentication

Endpoint Detection and Response

Backups: Frequency, Encrypted, Offline, Tested

E-mail Filtering and Web Security

Patch Management

Incident Response Planning and Testing

Employee Training

Service Accounts with limited domain privileges

- サイバー保険では、保険会社を選ぶ際に保険料だけで選ぶことはお勧めしません。
- カバレッジ、事故防止のメニュー・事故対応力・保険料などを総合的に選ぶ必要があります。