令和4年度契約
加入率
約６０％
（令和4年7月1日時点）

令和5年度

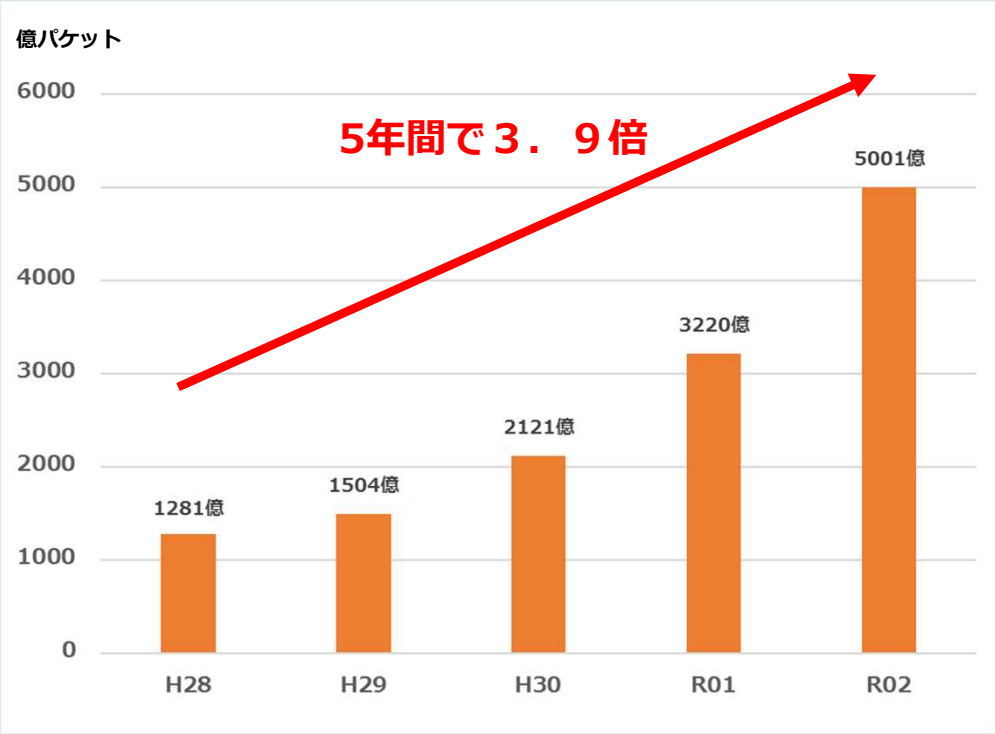
サイバー保険の概要について

損害保険ジャパン株式会社
団体・公務開発部　第三課

1．サイバー攻撃リスクの高まり

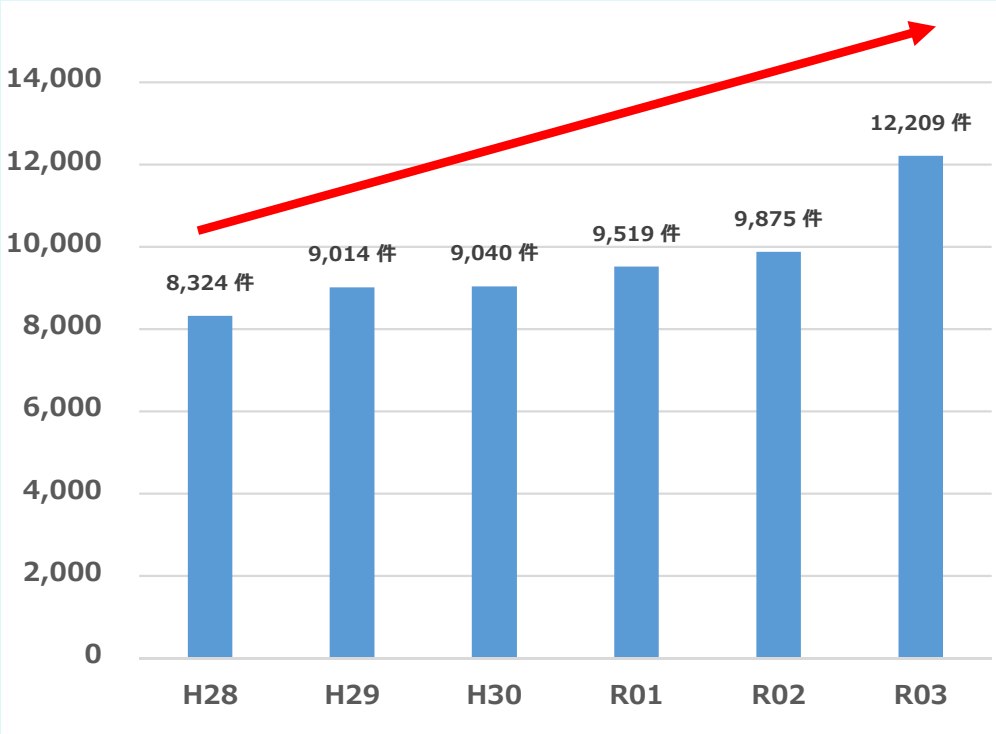
■サイバー攻撃のリスクは確実に拡がっています。

ダークネット観測網（約30万IPアドレス）において観測された サイバー攻撃関連通信数



出典：国立研究開発法人情報通信研究機構「NICTER観測レポート2020」

警察のサイバー犯罪の検挙件数の推移



出典：警察庁 『令和3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』

ダークネットとは、インターネット上で到達可能かつ未使用のIPアドレス空間のことを指します。
未使用のIPアドレスに対しパケットが送信されることは、通常のインターネット利用の範囲においてはまれであり、実際にダークネットを観測してみると、相当数のパケットが到着することが分かります。これらのパケットの多くは、マルウェアの感染活動など、インターネットで発生している何らかの不正な活動に起因しています。そのため、ダークネットに到着するパケットを観測することで、インターネット上の不正な活動の傾向把握が可能になります。

2．多様化するサイバー攻撃の手口

■サイバー攻撃の手口は多様化しており、脅威も様々なものになっています。

標的型メール攻撃

メールやweb等により、特定の自治体のPCをウイルスに感染させ、機密情報の窃取やシステム・設備の破壊・停止を行う攻撃。標的型攻撃は長期間継続して行われることが多いという特徴がある。

ばらまき型メール攻撃

メールやweb等により、不特定多数の自治体や企業等のPCをウイルスに感染させ、機密情報の窃取やシステム・整備の破壊・停止を行う攻撃。

ビジネスメール詐欺

取引先との請求書の偽装など巧妙な偽メールを自治体へ送り付けて職員を騙し、攻撃者の口座に送金させる行為。
その準備行為として、職員の個人情報等の詐取が行われることもある。

ランサムウェア

ファイルサーバやPC等のファイルを暗号化し、使用不能にするウィルス。
その暗号化解除と引き換えに金銭（身代金）を要求する不正プログラムが仕込まれている。

DDoS攻撃

同時に攻撃対象のサーバに対して大量のデータを送信することで、サーバの処理能力を飽和させたり、ネットワーク帯域を枯渇させたりし、使用不能にする攻撃。

ソフトウェアの脆弱性攻撃

脆弱性が存在するwebサーバなどに対して、ウイルスを感染させる攻撃。
情報窃取や機器破壊等の被害がある。

3．サイバー攻撃における現状

■サイバー攻撃における現状を数値でご案内いたします。

＜1つ目の数字＞	＜２つ目の数字＞
205日	55%

3．サイバー攻撃における現状②

■先ほどご案内したサイバー攻撃における現状の数値データの回答となります。

＜1つ目の数字の回答＞

セキュリティ侵害が発生してから組織がその侵入を発見するまでの平均日数

※FireEye社による発表(2015/10/29)

＜２つ目の数字の回答＞

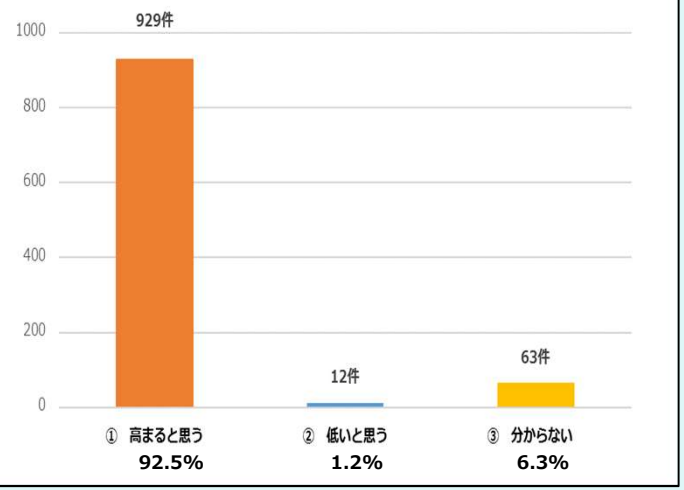
アンチウィルスソフトが検知できないマルウェア

※Symantec社による発表(2014/5/7)

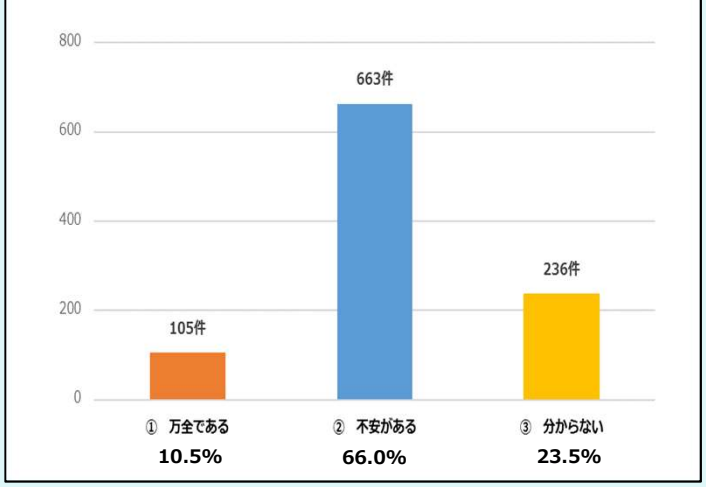
4．関係町村からのアンケート回答結果

■令和3年6月に実施したアンケート結果についてご案内します。

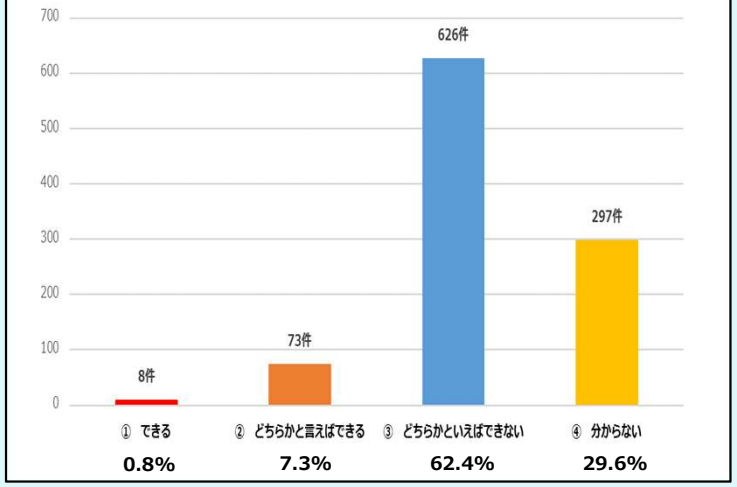
設問１．今後、各種手続きのオンライン利用の本格化や情報システムの高度化等、電子自治体が進展することとなりますが、サイバー攻撃やセキュリティ関連のリスクは高まると思いますか



設問２．総務省の情報セキュリティポリシーのガイドラインに①情報セキュリティ対策の実行性を高めるとともに対策レベルを一層強化していくこと、②情報セキュリティインシデントが発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じること、とありますが貴町村の対策についてどう思われていますか。



設問３．サイバー攻撃等で重大なサイバーインシデントが発生した場合は、調査や被害拡大防止、広報対応、システム機器の復旧・修理等の各種対応や多額の費用が発生しますが、現在の体制や予算で対応できると思いますか



サイバー攻撃やセキュリティ関連のリスクは、今後92.5%の町村が「高まると思う」という回答をしており、**リスクの高まりについては、多数の町村で既に身近で認知されている**ものと判断できる結果となっています。

町村が実施している現在の対策について、「万全である」と回答したのは10.5%の町村のみでありました。
また、「不安がある」と回答した割合は、66.0%、「わからない」を含めた割合は、全体の約90%に該当し、**多数の町村が、現在の対策について不安等を抱いている**ことが分かる結果となっています。

重大なサイバーインシデントが発生した場合において、現在の体制や予算で対応することが「できる」、「どちらかと言えばできる」と回答したのは、約8%の町村のみでありました。また、**「どちらかと言えばできない」と回答した町村は62.4%、「分からない」を含めた割合は全体の92%**にのぼる結果となっています。

5.実際に発生した事故事例

■実際に国内外の地方公共団体で発生したサイバー攻撃の事故事例についてご案内いたします。

実際に発生した事故例

■**ランサム攻撃**（2021年3月）
支援事業を委託している外部業者のサーバーがランサムウェアに感染し、収集した意識調査票に記載されている氏名や住所など町民の個人情報4,000件が流出した可能性が発生。結果的には、外部業者にて行った専門の調査会社の調査から明確な情報流出の痕跡が確認できなかったことから流出の可能性が極めて低いと判断された。

■**不正アクセス**(2020年5月)
運営するショッピングサイトに対し複数回の不正アクセスが発生し情報が流出した。1回目の不正アクセスでは顧客情報約3万件、注文情報6万件が流出、2回目では約400件の情報が流出したことがわかっている。この流出に伴い、個人情報の入力を求めるフィッシングメールが被害者へ届いた。

■**ランサム攻撃**（2020年11月）
ウェブサイトが閲覧できないことに職員が気づき、調査を行ったところ、不正アクセスを受けていたことが判明。ウェブサイトよりデータが削除され、データの復旧を交換条件として暗号資産であるBitcoinを支払うよう求める英文の脅迫文も残されていた。
2017年から2020年にかけて問い合わせフォームを利用した個人793件および法人180件のデータが流出した可能性が高い。

■**不正アクセス**(2018年10月)
業務での使用を禁止しているフリーメールを複数の職員が使用していたことにより、メールアカウントが不正アクセスを受け情報が流出。流出した情報の中には、補助金申請書や口座情報、免許証情報などが含まれていた。

■**インフラへの攻撃**（2021年2月）
約1万5千人の住民に水を供給している浄水場がサイバー攻撃を受けて、飲料水に含まれる水酸化ナトリウムの濃度の設定値が引き上げられた。職員がすぐに異変に気付き、実害は発生しなかった。

6.ひとたびサイバーセキュリティ事故が発生すると・・・

■サイバー攻撃が起こると、原因調査から住民・企業等への謝罪など各種対応や巨額な損害賠償が発生する可能性があります。

個人情報・企業情報が漏れた！

システムが使えず業務に阻害が！

データの消失やプログラムの改ざん！

システム機器や通信機器が損壊した！

データを暗号化され予期せぬ復旧費用が発生！

メールシステムの不正アクセスにより犯罪に巻き込まれた！

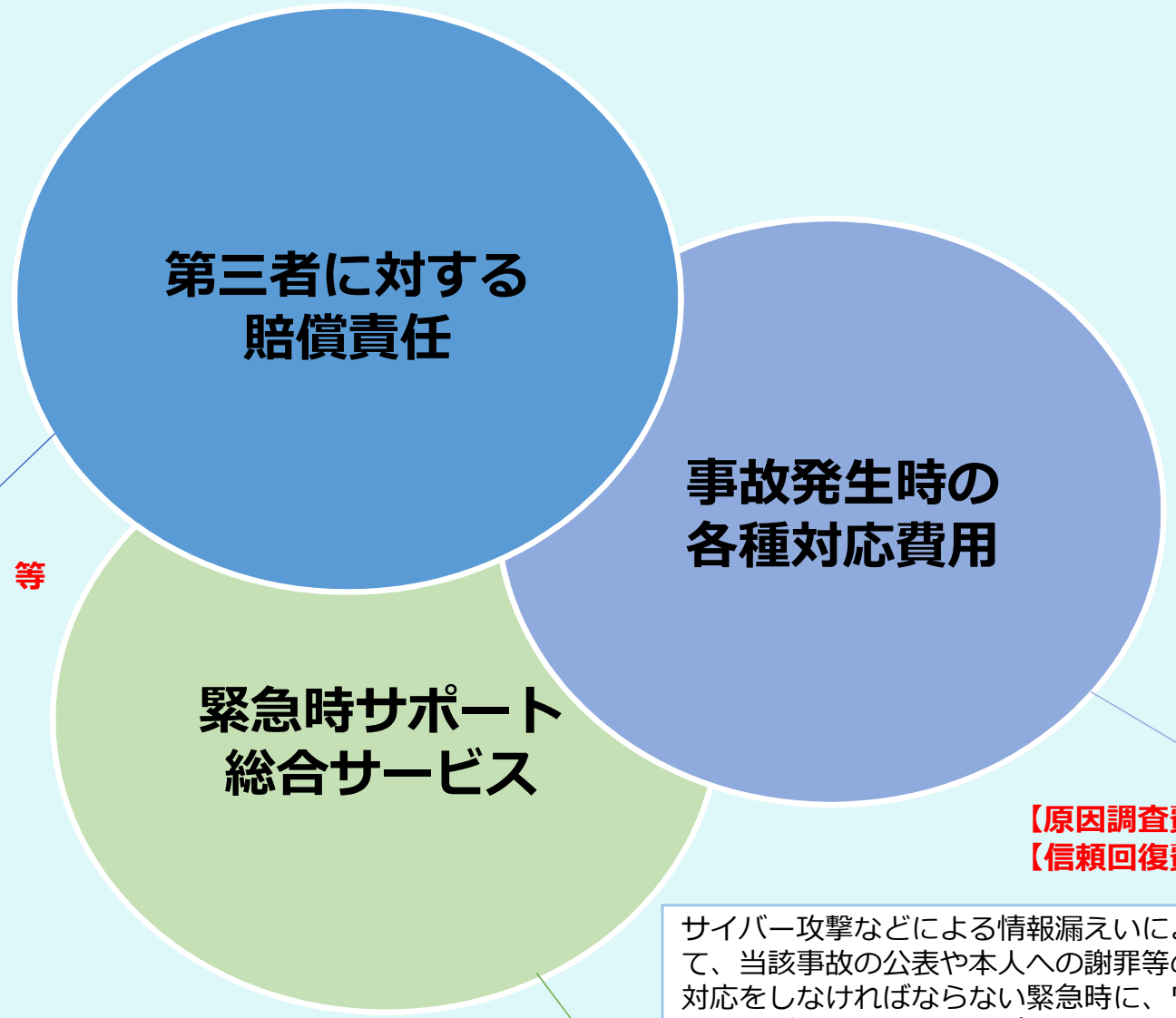
情報が流通して他人の権利侵害！

事故対応の遅延により住民・企業の信頼が失墜！

法令等の違反により対応が発生！

7.サイバー保険の補償構成

サイバー保険は、情報化社会をとりまく新たなリスクに対して、3つの補償をご用意しています。



サイバー攻撃によるシステムの機能停止や情報漏えいの発生によって、住民や企業に損害を与え、賠償責任を負った。

【損害賠償金】【争訟費用】等

事故原因を調査し、影響範囲の特定や損害の拡大防止、被害者対応などに関する費用が発生した。

【原因調査費用】【見舞費用】
【信頼回復費用】【データ復旧費用】等

サイバー攻撃などによる情報漏えいによって、当該事故の公表や本人への謝罪等の対応をしなければならない緊急時に、ワンストップかつ総合的にサポートすることができます。

サイバーセキュリティ事故が発生した際にはトータルでサポート

8.サイバー保険の補償内容

サイバー保険とは

■ 町村等においてサイバー攻撃や情報漏えい、システムやネットワークの管理誤りや停止、職員の犯罪行為などに関連して発生するセキュリティ事故に起因した第三者への賠償責任や事故対応に要する諸費用を総合的に補償する保険です。

賠償責任

以下記載の対象事由①～④の発生に起因して他人に損害を与えた場合の賠償責任・争訟費用を補償します。

他人の損害

損害賠償金（※1）　争訟費用

事故発生時の各種対応費用

以下記載の対象事由①～④の発生に起因して生じる「事故の調査」から「解決/再発防止」までの諸費用を補償します。

事故対応に要する諸費用

原因調査費用　データ復旧費用　再発防止費用

対象事由		概要
①	サイバー攻撃	不正アクセスやＤｏＳ攻撃(※2）、データの改ざん・破壊など被保険者のシステムに対する外部からの攻撃
②	情報漏えい・おそれ（※3）	業務における情報漏えいおよびそのおそれ
③	デジタルコンテンツ不当事由	デジタルコンテンツ(※4)の使用の結果生じた名誉棄損や、プライバシー侵害、著作権または商標権侵害など
④	ITユーザー業務	上記①～③以外の業務の一環としてのシステムの所有・使用・管理に起因する偶然な事由

（※1）サイバー攻撃等による身代金や脅迫金、欧州連合（ＥＵ）の一般データ保護規則（ＧＤＰＲ）を違反したことによる罰金などは対象外となります。

（※2）大量のデータを送り付けることで、システムを正常に稼働できない状態にすること。１か所から攻撃することを DoS、複数個所から攻撃することを DDoS と言います。

（※3）現在の「総合賠償補償保険」では「②情報漏えい・おそれ」が事由となった場合のみ対象です。（個人情報に限る）

（※4）人の知覚で認識可能な形式で構成され、コンピューターシステム上で表現されているテキスト、サウンド、グラフィック、画像、動画等をいい、それらの構成の元となるソフトウェアまたは電子データを含みません。

8.サイバー保険の補償内容②

事故発生時の費用の詳細

事故対応特別費用

原因調査から事態収拾まで、サイバー事故の対応にあたり必要となる諸費用を幅広く補償

調査/対応/事態収拾/復旧/再発防止

CHECK（支払要件

前項の対象となる事由①～④によって、他人の損失（※1）が発生するおそれのある場合

CHECK（対応費用例

- 調査：事故原因調査・影響調査
- 事態収拾：会見・マスコミ対応・コールセンター設置
- 復旧：データ復旧・情報機器復旧
- 再発防止：コンサルティング

サイバー攻撃対応費用

サイバー攻撃またはそのおそれに起因して被保険者が支出した諸費用を補償

初動/早期発見・早期復旧

CHECK（支払要件

サイバー攻撃のおそれが保険期間中に発見された場合（※2）

CHECK（対応費用例

- サイバー攻撃発生の有無の確認のための外部委託費用
- ネットワークの遮断のための外部委託費用
- 弁護士等の外部の専門家への相談費用

欧州ＧＤＰＲおよび改正個人情報保護法に対応！！

情報漏えい対応費用

情報漏えいまたはそのおそれに起因して被保険者が支出した諸費用を補償

見舞金・見舞品/モニタリング

CHECK（支払要件

情報漏えいまたはそのおそれが発生（※3）した場合

CHECK（対応費用例

- 上記の事故対応特別費用
- 被害者への見舞金・見舞品
- 情報漏えいのモニタリング

法令等対応費用

情報漏えいまたはサイバー攻撃によって、公的機関から調査等が行われた場合に、被保険者が支出した諸費用を補償

相談・調査

CHECK（支払要件

規制手続もしくは、法令等に抵触するおそれがある場合

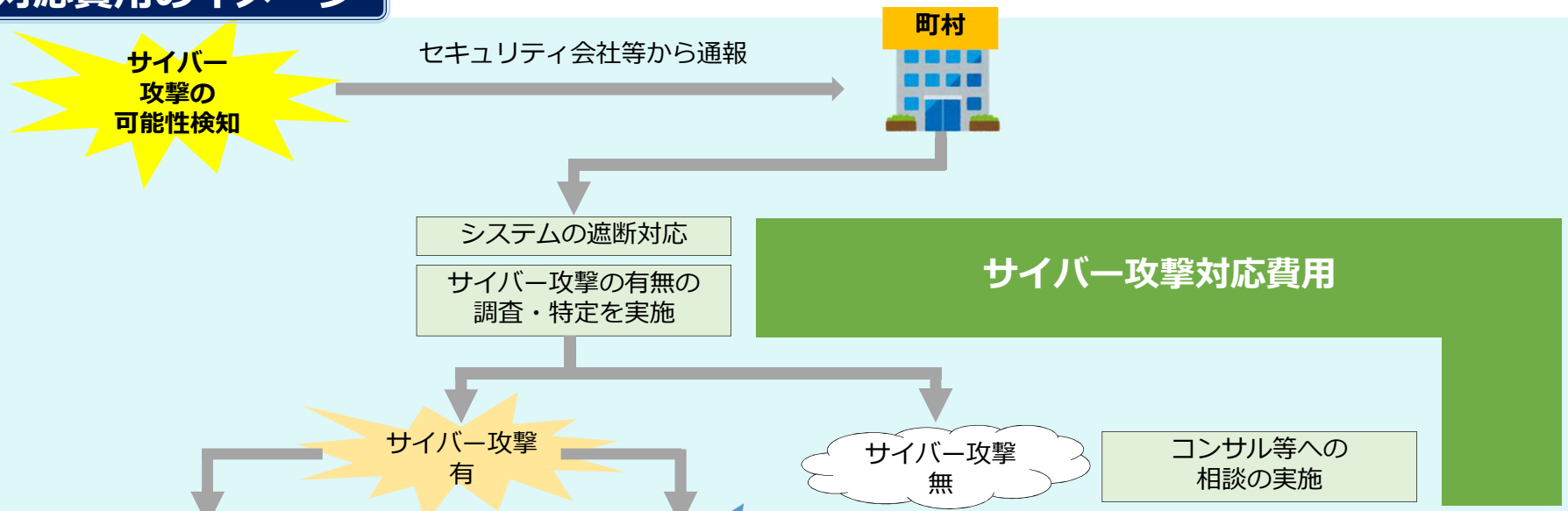
CHECK（対応費用例

- 弁護士・コンサルタント等の専門家への相談費用
- 報告書等の文書作成費用、公的機関への報告にかかる費用
- 証拠収集費用・翻訳費用

（※1）他人の業務の休止または阻害、他人のソフトウェアもしくは電子データの損壊または消失、不測の事由による他人の経済的な損失の発生等をいいます。
（※2）公的機関からの通報、被保険者がセキュリティ運用を委託している会社からの通報または報告により発見された場合に限ります。公的機関に被害があった町村自体は含みません、また、サイバー攻撃に関する被害の届出および情報の受付等を行なっている独立行政法人または一般社団法人を含みます。
（※3）個人情報に関しては、次に掲げる事由のいずれかがなされることにより、個人情報の漏えいまたはそのおそれが客観的に明らかになる場合にかぎります。
①サイバー攻撃が生じたことの保険会社への書面による通知、②被保険者が行う新聞、雑誌、テレビ、ラジオまたはこれらに準じる媒体による会見、発表、広告等
③本人またはその家族への謝罪文の送付、④公的機関に対する文書による届出、報告等または公的機関からの通報

8.サイバー保険の補償内容③

各種対応費用のイメージ



事故対応特別費用

- 対策本部用のコピー機の増設
- 被害状況、事故原因の調査
- 事故拡大の防止策の実施
- 従業員の派遣
- 問い合わせ対応用のコールセンターの設置
- 謝罪広告、会見の実施
- 弁護士・コンサル等への相談
- 被害者への謝罪文送付
- 再発防止策の策定、実施
- 損傷したデータの修復
- 損害したシステム機器の修理

情報漏えい対応費用

- 見舞金、見舞品の購入・送付
- 漏えい情報の不正使用モニタリング
- 再発防止としての外部機関認証の取得

サイバー攻撃対応費用

【対象要件】サイバー攻撃のおそれが保険期間中に発見された場合
(※1)公的機関からの通報、被保険者がセキュリティ運用を委託している会社からの通報または報告により発見された場合に限ります。
(※2)被保険者が導入しているセキュリティ監視のソフトウェア、サービス等からの通知を含み、当該サイバー攻撃のおそれを被保険者が認識した時以降に調査等を委託した会社からの報告を除きます。

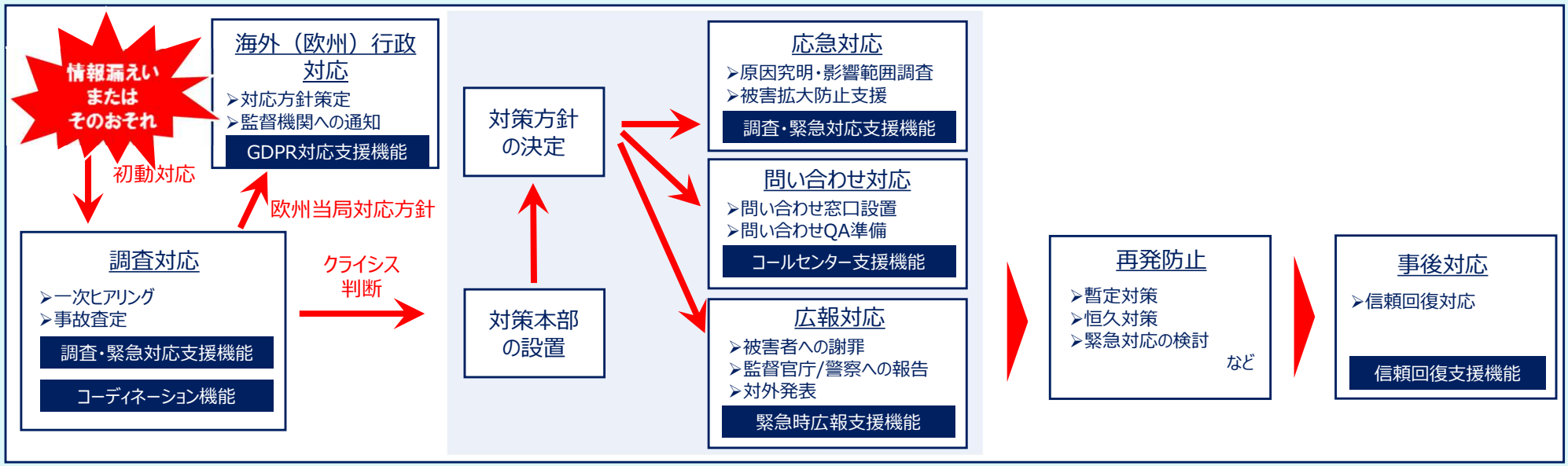
事故対応特別費用

【対象要件】サイバー攻撃、デジタルコンテンツ不当事由、ＩＴユーザー業務による偶然な事由によって、他人の損失等が発生するおそれのある場合
(※1)他人の損失等とは、他人の業務の休止または阻害、他人のソフトウェアもしくは電子データの損壊または消失、不測の事由による他人の経済的な損失の発生等をいいます。

9.緊急時サポート総合サービス

緊急時サポート総合サービスの仕組

■情報漏えいやネットワーク中断が発生した場合、早期対応による被害の拡散防止が急務となります。
■提携事業者との連携を密にしており、SOMPOリスクマネジメントが**必要なサポートをコーディネート、緊急時におけるお客様の被害拡散防止・早期復旧のための支援を実施します。**



緊急時の各種サポート機能

万が一の際、ご用命により、SOMPOリスクマネジメント㈱が必要な各種サポート機能を調整し、ご提供します。
また、これらの機能にかかる費用は、サイバー保険を通じて充当することが可能です。

調査・緊急対応支援機能	緊急時広報支援機能		コールセンター支援機能	信頼回復支援機能	ＧＤＰＲ対応支援機能	コーディネーション機能
✓ 事故判定 ✓ 原因究明・影響範囲調査支援 ✓ 被害拡大防止アドバイス　など	✓ 記者会見実施支援 ✓ 報道発表資料のチェックや助言 ✓ 新聞社告支援　など	✓ SNS炎上対応支援（公式アカウント対応サポート） ✓ WEBモニタリング・緊急通知	✓ コールセンター立上げ ✓ コールセンター運営 ✓ コールセンターのクローズング支援　など	✓ 再発防止策の実施状況について証明書を発行 ✓ 格付機関として結果公表を支援　など	✓ GDPR対応に要する対応方針決定支援 ✓ 監督機関への通知対応支援 ✓ 外部フォレンジック業者・協力弁護士事務所の紹介　など	✓ 必要となる各種サポート機能の調整 ✓ 法令対応等について協力弁護士事務所を紹介　など
(株)ラック / AOデータ(株)	(株)プラップジャパン	(株)エルテス	(株)ベルシステム24	(株)アイ・エス・レーティング	(株)インターネットイニシアティブ	SOMPOリスクマネジメント

ご紹介する企業が状況により変更となる場合がございます。

10.想定される事故事例①

想定される事故事例

① サイバー攻撃

■ランサム攻撃
システムへの接続障害が発生し、身代金を要求するメッセージがホームページやWEBサイト上で確認された。調査したところ、第三者からの不正アクセスがあり、ランサムウェアによりファイルが暗号化されていた。データについてはバックアップを行っていたため、ホームページやWEBサイトは復旧できたが、データを窃取された可能性が高い。

■脆弱性攻撃
ホームページのお問い合わせフォームを踏み台として、大量の迷惑メールが第三者へ送信される事態が発生した。原因はお問い合わせフォームへ外部からシステムを利用した機械的な連続投稿がされたことであると判明した。これを防止するため、お問合せフォームにGoogle社のシステムを組み込み機械的な大量投稿を防ぐ対策と講じた。

■インフラ攻撃①
町が管理するクリーンセンターの制御システムへ監視カメラの脆弱性を利用して侵入され、制御システムの警報装置の動作を停止させた上で、センター内のシステムを操作し、その結果、爆発事故が引き起こされた。

■インフラ攻撃②
町が管理する水道施設の制御ネットワーク上の機器がマルウェアに感染し、制御システムの性能が低下し、住民に健康被害が生じるなどの重大な被害を及ぼした。

10.想定される事故事例②

① サイバー攻撃

■ホームページの改ざん
ホームページの一部が改ざんされる不正アクセスがあり、住民が該当ページを閲覧すると不正なサイトに誘導され詐欺行為の被害を受ける可能性があったことが判明した。ホームページのNEWSページにアクセスすると「Windows システムが古くなり破損していることが検出されました。」と表示され、PCの修復画面へ移動し不正なツールをダウンロードするよう誘導され、ダウンロードを実行するとパソコン内部のスキャンが実行され、問題対処のためフリーダイヤル「0120-***-***」に電話するよう誘導され、その結果、カード情報の聞き取りなどの詐欺行為が行われる可能性があった。

■システムやネットワークの停止
職員のパソコンがウイルスに感染し、IDとPWが不正に利用されたことが発端となり、システム内部に不正なプログラムを仕込まれ、自治体のサーバーやネットワークが使用できない状況が発生。
行政サービスが長時間停止となり、住民や企業に損害を与えた。

■委託業者での事故
支援事業や助成事業を委託している業者のサーバーがランサムウェアに感染し、法人の申請内容や金融機関、メールアドレスなどの情報が流出した。

■町村が運営するサテライトオフィスでの事故
地方創生テレワークの推進で町村が運営するサテライトオフィスのWi-Fi設備が不正アクセスを受け、オフィスを利用していた企業職員のPCがコンピューターウイルスに感染し、損害を与えてしまった。

10.想定される事故事例③

②情報漏えい・おそれ

■犯罪行為
職員が個人情報3,０00件を不正にコピーし持ち出し、サイバー犯罪対策課に逮捕された。
これらの情報は住民基本台帳から抽出されていた。また、押収したパソコンやスマートフォンからは役場の内部資料も見つかった。

■紛失
防災課において避難行動要支援者名簿作成に使用していたUSBメモリを誤って紛失してしまい、メモリ内に保存されていた個人情報約5,000件が流出した可能性がある。

■誤交付
債権回収代理業務に伴う住民票交付請求に対し同姓同名の別個人の住民票を交付してしまった。

■ケアレスミス
新型コロナウイルス感染症者の個人名の入った一覧表をWebサイト上に掲載してしまった。
職員が誤って個人情報を削除する前のデータを誤って使用したことが原因。

③デジタルコンテンツ不当事由

■名誉棄損・プライバシー侵害
ホームページの掲載内容について住民から名誉棄損やプライバシー侵害などで賠償請求された。

④ ＩＴユーザー業務

■不適切な使用
職員が不適切なやり方でシステムへログインし、業務を行おうとした。その行動をシステムが異常と検知し、システムを遮断した。その結果、クラウドサービスが利用できなくなり、他の町村へ損害を与えた。

11.サイバー保険の加入方法

■サイバー保険の加入方法についてご案内いたします

保険金額

総合賠償補償保険制度の契約類型１～６の場合
賠償責任・・・１事故・期間中　１億円
対応費用・・・１事故・期間中　３，０００万円

総合賠償補償保険制度の契約類型7～10の場合
賠償責任・・・１事故・期間中　２億円
対応費用・・・１事故・期間中　３，０００万円

契約類型・保険料分担金

契約類型	身体賠償	財物賠償	健診賠償	予防接種	公金総合	補償保険	個人情報	対応費用	保険料分担金率
1	5,000万円	1,000万円	○	○	○	－	1億円	○	48.4円
2	5,000万円	1,000万円	○	○	○	Ⅰ型	1億円	○	56.4円
3	1億円	2,000万円	○	○	○	Ⅰ型	1億円	○	67.9円
4	1億円	2,000万円	○	○	○	Ⅱ型	1億円	○	75.4円
5	1.5億円	2,000万円	○	○	○	Ⅰ型	1億円	○	76.5円
6	1.5億円	2,000万円	○	○	○	Ⅱ型	1億円	○	84.0円
7	2億円	2,000万円	○	○	○	Ⅱ型	2億円	○	87.2円
8	2億円	2,000万円	○	○	○	Ⅲ型	2億円	○	91.8円
9	2億円	1億円	○	○	○	Ⅲ型	2億円	○	93.1円
10	3億円	1億円	○	○	○	Ⅲ型	2億円	○	100.8円

+4.2円

サイバー保険に加入する場合は、保険料分担金率が右記となります。

サイバー	対応費用	保険料分担金率
1億円	○	52.6円
1億円	○	60.6円
1億円	○	72.1円
1億円	○	79.6円
1億円	○	80.7円
1億円	○	88.2円
2億円	○	91.4円
2億円	○	96.0円
2億円	○	97.3円
2億円	○	105.0円

加入依頼書

（様式第１号）　（契約確認用）①　損保ジャパン本社用

記入例

都道府県　町村会長　殿

町村長（市）　㊞

保険始期をご記入ください。

全国町村会総合賠償補償保険加入依頼書

全国町村会と損害保険ジャパン株式会社を幹事とする損害保険会社と締結した「全国町村会総合賠償補償保険」に下記事項が事実に相違ないことを確認し、下記のとおり加入の申込みをします。

１．保険期間　令和　年　月　日 ～ 令和 5 年 5 月 31 日

２．契約類型

(1) 前票「加入のご案内」の「１．契約類型」および オプションの有無を○で囲んでください。

加入する契約類型、オプションの付保を○で囲んでください。

契約類型（ご加入型を○で囲んでください。）	〈オプション〉サイバー保険
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩	付保する　付保しない

(2) 加入を希望する契約類型と保険料分担金率を下記①②欄に、また前票「加入のご案内」の「２．加入手続きについて」より住民数を下記③欄に記入してください。

サイバー保険に加入する場合は、前票１のサイバー保険込みの分担金率となります。

(3) 保険料分担金率に住民数を乗じた金額を下記④欄に記入してください。

記載内容を訂正する際は訂正印を押印ください。

契約類型	保険料分担金率	住民数	保険料分担金
① 9	② 97.3 円	③ 10,866 人	②×③ 1,057,262 円

（円未満を四捨五入）

加入する契約類型および保険料分担金率をご記入ください。

97.3円×10,866人＝1,057,261.8円 →1,057,262円

３．そ　場合の所管課及び担当者名を記入してください。

所管課・係	職名	氏名
総務課　庶務係	庶務課長	甲野　乙一
Tel：●●●●－●●●－●●●●		

契約方法

特約（オプション）になりますので、任意となります。

１２.問い合わせ先について

引受幹事保険会社

損害保険ジャパン株式会社　団体・公務開発部第三課
〒160-8338　東京都新宿区西新宿1-26-1　損保ジャパン本社ビル12階
TEL　03-3349-5408　（受付時間：平日の午前9時から午後5時まで）

取扱代理店

株式会社千里
〒100-0014　東京都永田町1-11-32　全国町村会館西館内
TEL　03-5512-4750　（受付時間：平日の午前9時半から午後5時まで）

本資料は、2022年度に全国町村会総合賠償補償保険制度に特約として導入するサイバー保険の概要を説明したものです。
詳細は、全国町村会総合賠償補償保険制度の手引きやあらましをご参照下さい。