## サイバー攻撃対応費用特約の概要

| | |
|---|---|
| **保険金をお支払いする場合** | 保険期間中に保険契約者または子会社（※1）が所有または使用するコンピュータシステムに対するセキュリティ事故が発覚（※2）した場合に、被保険者に対し損害賠償請求がなされることを防止するために被保険者が負担するサイバー攻撃対応費用（※3）に対して、保険金をお支払いします。<br>（※1）保険証券に記載された子会社をいいます。<br>（※2）セキュリティ事故の発覚とは、次の1または2のいずれかをいいます。なお、これらいずれかのことが最初になされた時を発覚の時とします。<br>1. セキュリティ事故の発生または発生のおそれがあることについて、次のことがなされたこと<br>(1) 第三者から被保険者に対する通報または報告。公的機関またはセキュリティ運用管理会社、クレジットカード会社、決済代行会社等から通報または報告があった場合など、セキュリティ事故の発生が合理的に推察できる場合に限ります。<br>(2) 新聞、雑誌、テレビ、ラジオ、インターネットなどによる報道<br>2. 被保険者がセキュリティ事故の発生または発生のおそれがあることを知り、次のいずれかの対応を行ったこと<br>(1) ホームページ・新聞・テレビなどでの公表<br>(2) 不正アクセス行為の禁止等に関する法律に基づく公的機関に対する援助の依頼の申出<br>(3) 警察署への被害届の提出<br>（※3）サイバー攻撃対応コンサルティングに対して、被保険者が支払う報酬で、弊社が妥当かつ必要であると認めたものをいいます。 |
| **支払限度額など** | 1. この特約の支払限度額は、保険期間中1,500万円です。<br>（注）ただし、個人情報漏洩特約の支払限度額を限度とします。<br>（※）この特約で支払う保険金は、個人情報漏洩特約で支払う保険金およびセットされるその他の特約で支払う保険金と合算して、個人情報漏洩特約の支払限度額内でのお支払いとなります。<br>2. 自己負担額（免責金額）および自己負担割合を適用しません。<br>3. セキュリティ事故の発覚から90日以内に実施されたサイバー攻撃対応コンサルティングに対して支払われるサイバー攻撃対応費用が補償の対象となります。<br>4. 通知いただいたセキュリティ事故が発覚した日より60日以内に発覚したすべての事故は、通知いただいた事故と同日に発覚したものとみなします。<br>5. この特約のほかに「危機管理コンサルティング費用特約」または「危機管理実行費用特約」のご契約をされている場合には、発生した事故および損害の内容によってはそれぞれの特約で重複して補償の対象となる可能性がありますが、重複しては保険金をお支払いしません。 |
| **被保険者<br>保険の補償を受けられる方** | 次の方をいいます。<br>1. 保険契約者および子会社（※）<br>2. 保険契約者および子会社（※）の現在および過去の代表者、役員等<br>3. 保険契約者および子会社（※）の従業員<br>4. 保険契約者または子会社（※）に派遣された派遣社員<br>5. 保険証券に記載された者<br>6. 上記2. および3. に該当する被保険者の相続人および遺産に関する代理人<br>（※）保険証券に記載された子会社をいいます。 |
| **保険金をお支払いできない主な場合** | 次の事由によって生じたサイバー攻撃対応費用に対しては、保険金をお支払いできません。<br>1. 被保険者役員の犯罪行為または故意に起因するセキュリティ事故<br>2. 保険期間の開始日前に発覚したセキュリティ事故<br>3. 財物の損壊に起因するセキュリティ事故<br>4. 戦争・テロ行為等に起因するセキュリティ事故 |

### 用語の説明

1. セキュリティ事故
   コンピュータシステムに対する不正アクセス・不正使用、DoS攻撃、または悪性コードの送付をいいます。
2. コンピュータシステム
   保険契約者または子会社が所有または使用している、ネットワーク化されたコンピュータハードウェアおよびソフトウェアをいいます。
3. 不正アクセス・不正使用
   不正アクセス行為の禁止等に関する法律第2条4項に定める行為をいい、次のいずれかをいいます。
   (1) 他人のIDやパスワードなどをネットワークを経由してコンピュータに入力することで、他人になりすましてアクセスする行為
   (2) コンピュータシステムの安全対策上の不備（セキュリティ・ホールなど）を利用してネットワークを経由してアクセスする行為
4. DoS攻撃
   ネットワークを経由してコンピュータシステムに不正なデータを大量に送りつけるなどの手段によりなされる攻撃をいいます。
5. サイバー攻撃対応コンサルティング
   セキュリティコンサルティング機関が、セキュリティ事故の悪影響を管理および最小化する目的で被保険者に提供する次のセキュリティコンサルティングサービスをいいます。
   (1) セキュリティ事故の被害状況の把握
   (2) セキュリティ事故の証拠保全および被害拡大防止対応
   (3) (2) の結果保全された証拠の調査
6. セキュリティコンサルティング機関
   弊社が承認する、セキュリティ事故の悪影響を管理および最小化するための機関をいいます。（ただし被保険者を除きます）

**サイバー攻撃対応費用特約は個人情報漏洩特約とセットでのご契約となり、単独ではご契約できません。個人情報漏洩特約の詳細については、パンフレットなどをご覧ください。**

●このチラシは保険商品の概要をご説明したものです。詳細につきましては、パンフレットをご覧いただくか、取扱代理店・扱者または弊社にお問い合わせください。また、ご契約に際しては、保険商品についての重要な情報を記載した重要事項説明書（「契約概要」「注意喚起情報」等）を、事前に必ずご覧ください。
●弊社の損害保険募集人は、保険契約締結の代理権を有しています。

AIG損害保険株式会社

〒105-8602　東京都港区虎ノ門4-3-20
03-6848-8500
午前9時～午後5時（土・日・祝日・年末年始を除く）
**https://www.aig.co.jp/sonpo**

お問い合わせ・お申し込みは

AIG損保

高まるサイバー攻撃の脅威!

# サイバー攻撃対応費用特約

## （個人情報漏洩保険）

業務過誤賠償責任保険普通保険約款 / 個人情報漏洩特約 / サイバー攻撃対応費用特約

業務過誤賠償責任保険

| | |
|---|---|
| 2019年2月版 | 2019年4月1日以降保険始期契約用 |

標的型メール攻撃などサイバー攻撃が大きな脅威となっています。
サイバー攻撃への初期対応を誤った場合、企業経営に深刻なダメージを与えかねません。
サイバー攻撃は完全に防ぐことは困難なことからも、攻撃された際の初期対応が極めて重要です。

# 「サイバー攻撃対応費用特約」なら、サイバー攻撃に対する「デジタル・フォレンジック」(※)などの調査費用を補償し、初期対応を支援します。

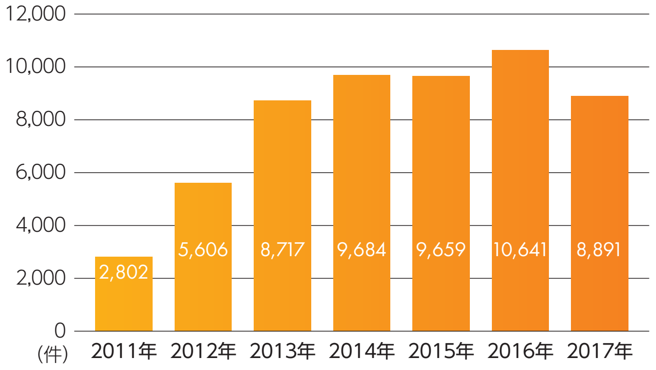
（※）「デジタル・フォレンジック」とは　不正アクセスなどのサイバー攻撃を受けた際に、攻撃を受けたパソコンやサーバなどに残る電子的記録を保全・復元・解析することで原因や情報漏洩の影響範囲を調査することなどをいいます。

## サイバー攻撃を受けた場合の初期対応の重要性

1. セキュリティに関する高度な知識と技術をもった専門家による迅速な対応が求められます。
2. 情報漏洩、信用失墜、システム停止などの被害を最小限に食い止める必要があります。
3. 損害賠償請求への対応、事件解決のため、証拠保全と調査・分析が必要です。

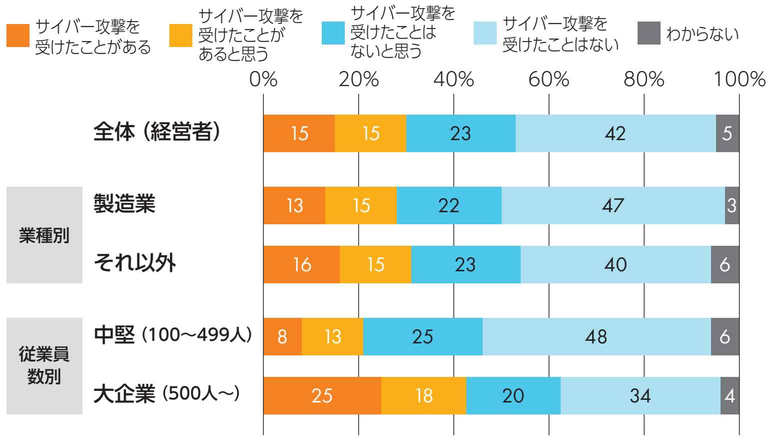
## 不正アクセスなどサイバー攻撃が深刻なリスクに!!

### コンピュータセキュリティインシデント※報告件数（年間調整件数の推移）



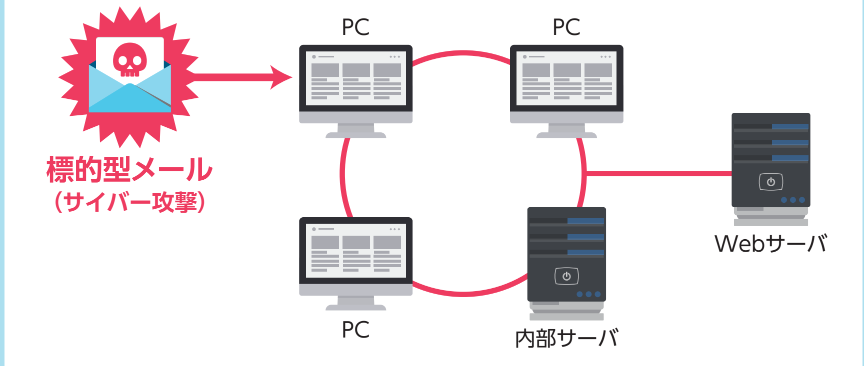
※「コンピュータセキュリティインシデント」とは、情報システムの運用におけるセキュリティ上の問題として捉えられる事象、コンピュータのセキュリティに関わる事件、できごとの全般をいいます。
（出典：JPCERT/CCインシデント報告対応レポート【2018年1月1日～2018年3月31日】）
https://www.jpcert.or.jp/ir/report.html
※報告件数はJPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）が受け付けた件数です。

### サイバー攻撃を受けたことがあるか



▶ 3割の企業がサイバー攻撃を受けたことがある（その可能性を含む）と認識
（出典：サイバーリスクに関する調査　2017年弊社調べ）

### サイバー攻撃とデジタル・フォレンジックのイメージ



PC、サーバ等のハードディスクの複製作成
▼
ログを解析し不正アクセスの記録の特定
▼
情報漏洩の影響範囲の解析
▼
サイバー攻撃の実態解明へ

## 初期対応のコスト（PC3台、サーバ2台の場合の例）

| 項目 | 作業の概要 | | コスト概算 |
|---|---|---|---|
| 被害状況の把握 | ・被害状況のヒアリング | ・情報収集 | 約30万円 |
| 被害拡大防止 | ・脅威からの隔離 | ・国内外調査機関への対応依頼 | 約120万円 |
| 証拠保全 | ・ハードディスクの複製作成 | | 約270万円 |
| 保全された証拠の調査 | ・ログの解析 | ・情報漏洩の影響範囲の解析 | 約630万円 |
| | | 合計 | 約1,050万円 |

デジタル・フォレンジックのコストは1台あたり次の金額が目安です。
PC：100万円　サーバ：200～300万円　（※）左記のコストは弊社調べ

## サイバー攻撃を受けた場合の補償イメージ

サイバー攻撃対応費用特約をセットすることで、サイバー攻撃が発覚した段階から、4つのステップでトータルにお客さまをサポートします。

**Step0　サイバー攻撃対応**
セキュリティ・コンサルティング会社をご案内し、デジタル・フォレンジックなど初期対応を支援。要した費用を補償

サイバー攻撃対応費用特約の補償範囲

**Step1　危機管理コンサルティング**
危機管理コンサルティング機関をご案内し、危機管理対応をアドバイス。要した費用を補償

**Step2　危機管理実行**
危機管理コンサルティングに基づいて、被害者など関係者に対する危機管理対応に要した費用を補償

**Step3　訴訟対応**
被害者などから損害賠償請求された場合に、損害賠償金および弁護士費用などを補償

漏洩発覚後の補償内容の詳細はパンフレットをご覧ください。

## サイバー攻撃対応費用特約の特長

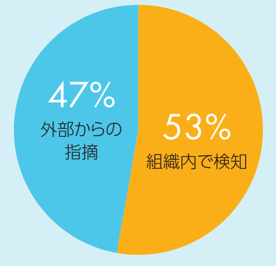
**特長 1**
### 「セキュリティ・コンサルティング会社」をご案内
サイバー攻撃を受けた場合、「セキュリティ・コンサルティング会社」をご案内して、初期対応をサポートします。
（注）弊社からご案内する「セキュリティ・コンサルティング会社」以外は、弊社の承認が必要です。

**特長 2**
### 高額なデジタル・フォレンジック費用などを1,500万円まで補償!
最近のサイバー攻撃は、「巧妙化」「複雑化」「大規模化」しており、デジタル・フォレンジック費用が高額化しています。
そこで最大1,500万円まで、高額化するデジタル・フォレンジック費用などを補償します。

**特長 3**
### 自己負担がないので安心!
免責金額および自己負担割合を適用しないので、
被保険者（保険の補償の対象となる方）の自己負担なしで1,500万円を限度に全額補償します。

**特長 4**
### 外部のセキュリティ会社、クレジットカード会社などからの通報であっても補償の対象!
サイバー攻撃は、外部から通報を受けてサイバー攻撃が発覚するケースが約半数を占めています。
この特約では、業務委託していないセキュリティ会社や
クレジットカード会社などの外部からの通報であっても補償の対象となります。

### セキュリティ侵害の発覚経緯



（出典：経済産業省、独立行政法人 情報処理推進機構 サイバーセキュリティ経営ガイドラインVer2.0）

### この特約の発動要件

この特約は、コンピュータシステムに対する不正アクセス・不正使用、DoS攻撃または悪性コードの送付などのセキュリティ事故が発覚したときに発動します。

発覚の具体例は、次のとおりです（発覚の定義は、裏面にてご確認ください）。
①業務委託先のセキュリティ会社が不正ログを発見し、不正アクセスの可能性があると報告を受けた
②業務委託していないセキュリティ会社から、不正アクセスの可能性があるとの通報を受けた
③クレジットカード会社より、不正アクセスの可能性があるとの通報を受けた
④自社のシステム担当者が不正アクセスがあった痕跡を発見し、ホームページで調査することを公表した