

サイバー事案の被害発生時に備えて 警察等への**連絡体制**を整備しましょう！

★警察からのお願い★

警察との連絡体制の確保！

- ・被害発生時の対応マニュアル等に警察の連絡先を記載する。
- ・被害の発生を想定した**事業継続計画 (BCP)**を策定する。初動対応における警察との連携を記載する。

速やかな通報・相談

最寄りの警察署へ通報
または
「サイバー事案に関する相談窓口」に
相談して下さい。

<https://www.npa.go.jp/bureau/cyber/Soudan.html>



初動対応における警察との連携

侵入経路や侵害範囲特定のため、外部接続機器を中心としたログの保全に努めてください。
また、必要に応じて以下の内容を伺いますので情報提供にご協力をお願いします。

- ・被害端末に関する情報（データの暗号化の有無）
- ・ネットワークの構成図 等



企業の皆様からの情報提供がサイバー空間の安全につながります！

警察へ寄せられたサイバー事案に関する情報を分析し、事件捜査を行うほか、被害企業における対策に必要な情報の提供・助言、他の企業等への被害拡大を防止するための注意喚起等の被害防止のための取組を行っています。

よくある質問

通報したら被害を公表させられるのでは？（信用の毀損・風評被害が心配）

警察から被害の公表を求めることはなく、保秘を徹底します！
通報して必要な捜査を行うこと、つまり「社会的責任を果たすこと」が、顧客や取引先等に対する説明責任を負う上で重要な要素となります。



警察

通報すると警察対応で時間を取られ復旧作業が遅れそう。

警察は、被害組織の復旧作業や業務継続に最大限配慮し対応します。



警察

◆ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手法や対策などを、ホームページやX（旧Twitter）に掲載していますのでぜひご覧ください。

◆ 万が一サイバー事案の被害に遭われた際は、管轄警察署に通報してください。

[X]



[HP]

