危機管理連絡会議

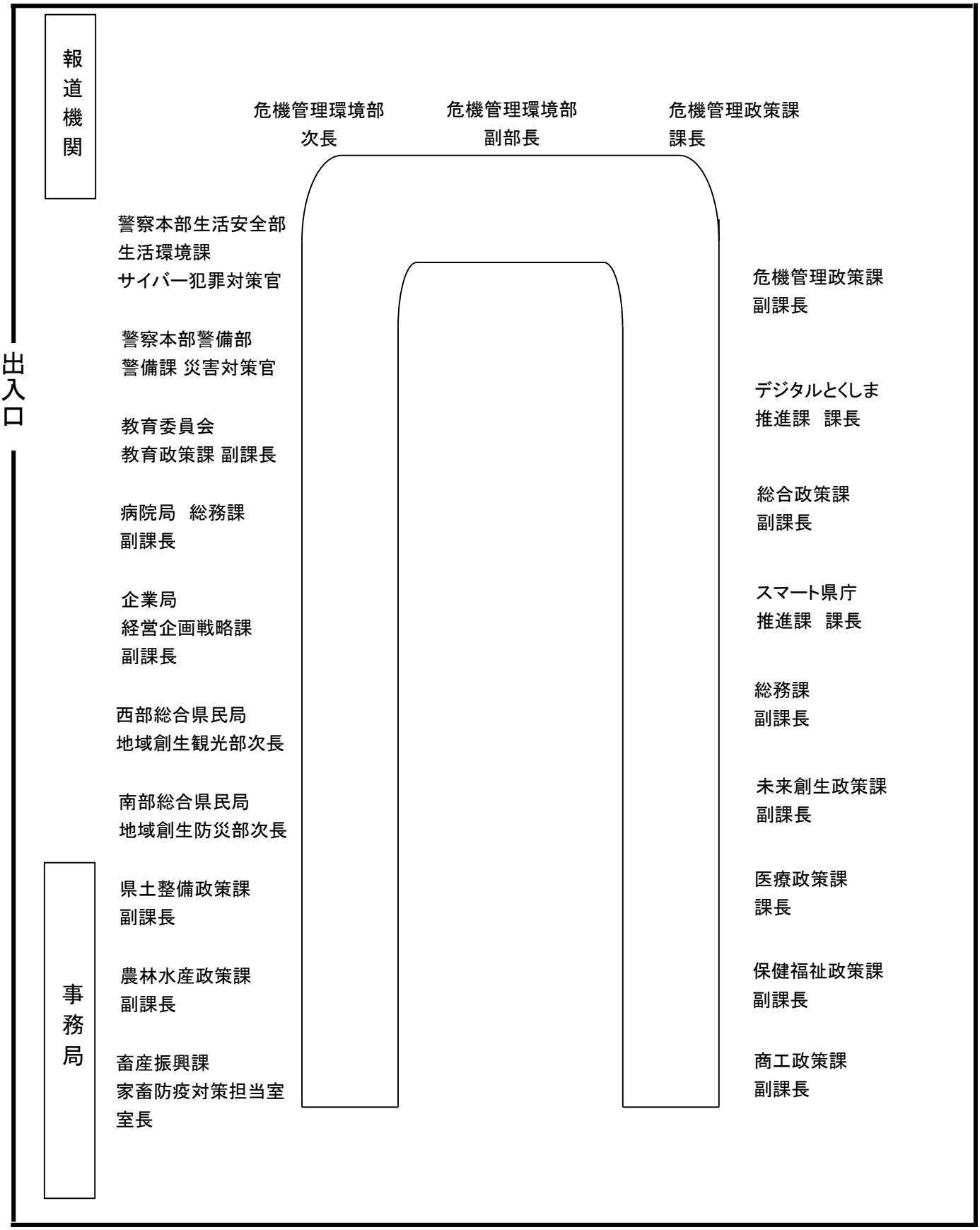
日時：令和４年６月２０日（月）午後５時３０分
場所：県庁３階特別会議室

協議事項

○ 県内医療機関でのサイバー攻撃事案の発生について

危機管理連絡会議　配席図

令和4年6月20日（月）17:30～



医第１８８号
令和４年６月２０日

各医療機関管理者　殿

徳島県保健福祉部医療政策課長
（公　　印　　省　　略）

「医療情報システムの安全管理」について

昨日，県内の医療機関において，ランサムウェアに感染し，電子カルテシステムが利用停止となる事案が発生しました。

つきましては，再度，医療情報システムの安全管理について，下記通知等を参考の上，対策を徹底してくださいますようお願いいたします。

なお，通知については，県ホームページ「医療とくしま」を御確認ください。

■　「医療情報システムの安全管理に関するガイドライン」に関する「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」について
http://anshin.pref.tokushima.jp/med/experts/docs/2021102100038/

■　医療機関を標的としたランサムウェアによるサイバー攻撃について
http://anshin.pref.tokushima.jp/med/experts/docs/2021110200034/

■　「医療情報システムの安全管理に関するガイドライン第 5.2 版」の策定について
http://anshin.pref.tokushima.jp/med/experts/docs/2022052600067/

担当　医事指導担当
電話　088-621-2366

ランサムウェアにご注意ください

令和４年６月２０日

ランサムウェアとは

コンピュータウイルスの一種で、パソコンやスマートフォンなどに感染すると、端末に保存されている画像や文書などのファイルを暗号化したり、端末自体を操作不能にして、利用者に対し、データを復元する対価に、金銭を要求する不正なプログラムです。

さらに、データを盗み取った上、「対価を支払わなければデータを公開する」などと金銭を要求するダブルエクストーション（二重恐喝）という手口も発生しています。

感染を防止するための対応策

○　最近のランサムウェアの進入経路として、

・インターネット等の外部ネットワークからアクセス可能な機器の脆弱性によるもの

・特定のプロトコルや既知の脆弱性を悪用した攻撃によるもの

・新型コロナウイルス感染症対策として急遽構築したテレワーク環境の不備によるもの

などが報告されており、これらを踏まえた予防策が必要です。

被害を軽減するための対策

○　重要なデータに対する定期的なバックアップ

バックアップの検討に当たっては、ランサムウエア感染時でもバックアップが保護されるように、

・ファイルのコピーを３個取得した上で、ファイルは異なる２種類の媒体に保存

・コピーのうち、１個はクラウドサービスや保護対象のネットワークからアクセスできない場所等に保管する

といった対策等を検討する。

○　バックアップデータから実際に復旧できることを確認

○　アクセス権等の権限の最小化

公開された場合、実際に支障が生じるような機微データや個人情報等に対して、特別なアクセス制御や暗号化を実施する。

○　システムの再構築を含む復旧計画が適切に策定できていることを確認

被害に遭われた際は、最寄りの警察署へ

詳しくは、

内閣サイバーセキュリティセンター　ランサムウェア特設ページ（外部サイト）
https://security-portal.nisc.go.jp/stopransomware/

サイバー犯罪被害に係る企業・団体を対象としたアンケート調査結果及び対策

過去１年以内に受けたことのある被害

ランサムウェア被害が倍増

	R2	
1位	メール不正中継	12.8%
2位	ランサムウェア	11.9%
3位	情報流出	6.4%

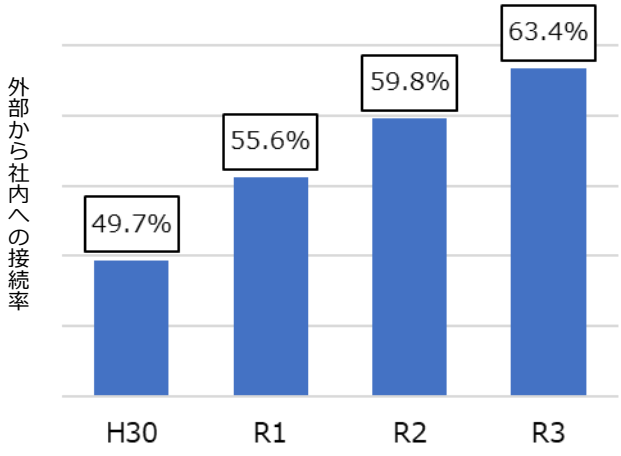
※ 被害を受けた団体における割合

	R3	
1位	**ランサムウェア**	**22.1%**
2位	メール不正中継	15.8%
3位	情報流出	12.6%

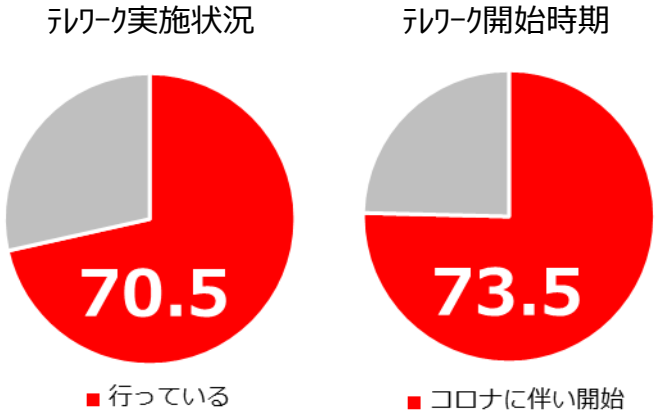
※ ランサムウェアとは、感染すると端末等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価として金銭を要求する不正プログラム

外部から社内への接続・テレワーク

業務上の外部からの接続が急増



新型コロナ拡大による開始は７割以上

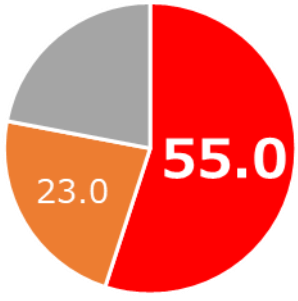


セキュリティ対策

VPNの導入が増加

	H30	R1	R2	R3
1位	ファイヤーウォール	IDパスワード	IDパスワード	IDパスワード
2位	IDパスワード	ファイヤーウォール	ファイヤーウォール	ファイヤーウォール
3位	Proxyサーバ	Proxyサーバ	**VPNの利用**	**VPNの利用**

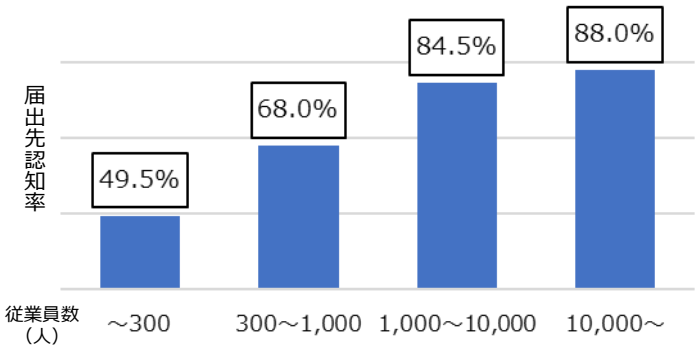
ランサム感染経路は半数以上がVPN



「令和３年上半期サイバー空間脅威情勢」（警察庁）抜粋

被害発生時の届出先の認知状況等

中小企業の認知率が低い



最も多い届出先は「警察」

1位 警察

2位　情報処理推進機構

3位　監督官庁

被害に遭わないために

OSなどの脆弱性対策

OSやアプリケーションソフト、VPN機器などに脆弱性があると
マルウェアに感染したりネットワークに侵入されるおそれがあります。

- OS・ソフトウェアの更新
- ウイルス対策ソフトの更新
- ネットワーク機器ソフトウェアの更新

認証情報の適切な管理

VPN機器やリモート・デスクトップ・サービスなどの認証パスワードが
脆弱な場合、ネットワークに侵入されるおそれがあります。

- パスワード長は一定以上に
- 異動で使わなくなったIDは削除
- IDを複数ユーザで共有しない

⚠被害に遭ってしまったら
警察へ通報

より詳しい被害防止対策は警察庁「ランサムウェア被害防止対策ページ」→
https://www.npa.go.jp/cyber/ransom/index.html

警察庁 National Police Agency

都道府県警察本部のサイバー犯罪相談窓口はこちら →
https://www.npa.go.jp/cyber/soudan.html