OCH SG-ONE　勉強会資料

OCH株式会社
営業部

2022年4月

2022年度の情報セキュリティトレンド

IPA情報セキュリティ10大脅威2022　脅威ランキング

社会的に影響の大きかったセキュリティ脅威ランキング

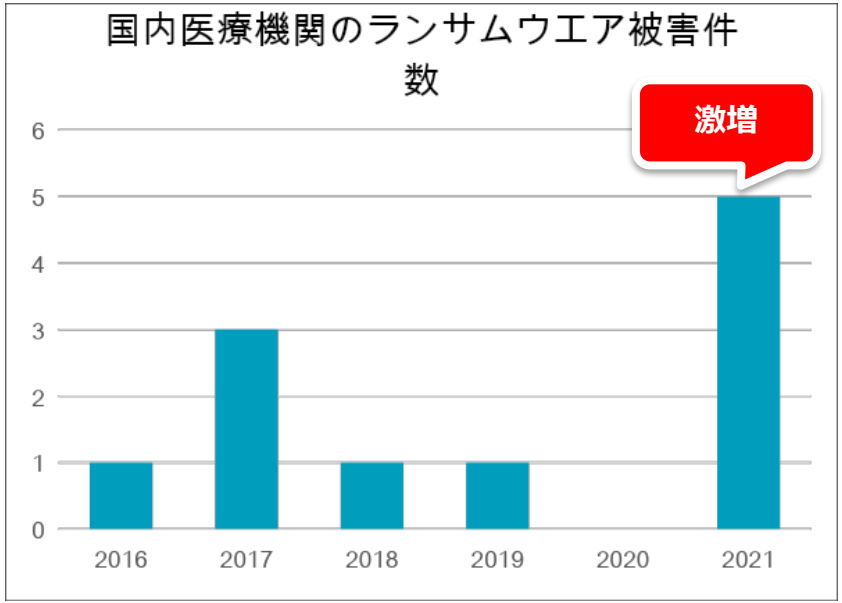
順位	「組織」の脅威	昨年順位
1位	ランサムウェアによる被害	1位
2位	標的型攻撃による機密情報の窃取	2位
3位	サプライチェーンの弱点を悪用した攻撃	4位
4位	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
5位	内部不正による情報漏洩	6位
6位	脆弱性対策情報の更改に伴う悪用増加	10位
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8位	ビジネスメール詐欺による金銭被害	5位
9位	予期せぬIT基盤の障害に伴う業務停止	7位
10位	不注意による情報漏えい等の被害	9位

出所：IPA「情報セキュリティ10大脅威 2022」https://www.ipa.go.jp/security/vuln/10threats2022.html

- 2022年も**「ランサムウエア」「標的型攻撃」**が上位
- セキュリティ体制がしっかりした大企業を攻撃する足掛かりとして、**セキュリティの緩い中小企業やリモートワーク環境が狙われ**ている。

サイバー攻撃の事例①：地方中小病院へのサイバー攻撃

2016年以降、少なくとも**国内11病院が「ランサムウェア」による被害**をうけている。



参考：読売新聞オンライン2021/12/29 https://www.yomiuri.co.jp/national/20211228-OYT1T50173/

2021年10月　徳島県つるぎ町立半田病院（120床）被害額約2億円

サイバー攻撃「もはや災害」　地域の中核病院、長期化に頭抱え

社会　暮らし・学び・医療　速報　徳島　医療・健康

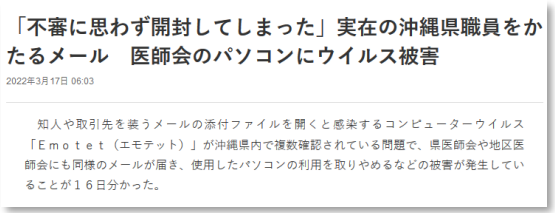
毎日新聞　2021/11/12 16:15（最終更新 11/12 19:49）　有料記事　1718文字

診療費は後日請求することを知らせる張り紙＝徳島県つるぎ町半田の町立半田病院で2021年11月10日午後0時1分、国本ようこ撮影

徳島県つるぎ町立半田病院が10月末、サイバー攻撃に遭い、深刻な事態に陥っている。データを勝手に暗号化し、復旧と引き換えに身代金を要求するコンピューターウイルス「ランサムウエア」に院内のシステムが感染。患者約8万5000人分の電子カルテが見られず、診療費の会計もできなくなった。外来患者の新規受け入れを全面的に停止し、診療内容は手書きでカルテに記録するなど対応に追われている。現時点で復旧の見通しは立たず、病院関係者は「もはや災害だ」と頭を抱える。

出所：毎日新聞2021/11/12 https://mainichi.jp/articles/20211112/k00/00m/040/128000c

2022年3月　沖縄県医師会および地区医師会に沖縄県職員名をかたるEmotetメール経由でウィルス被害。



「不審に思わず開封してしまった」実在の沖縄県職員をかたるメール　医師会のパソコンにウイルス被害

2022年3月17日 06:03

知人や取引先を装うメールの添付ファイルを開くと感染するコンピューターウイルス「Ｅｍｏｔｅｔ（エモテット）」が沖縄県内で複数確認されている問題で、県医師会や地区医師会にも同様のメールが届き、使用したパソコンの利用を取りやめるなどの被害が発生していることが１６日分かった。

出所：沖縄タイムス2022/3/17 https://www.okinawatimes.co.jp/articles/-/927017

サイバー攻撃の事例②：活発化するサプライチェーン攻撃

サプライチェーン攻撃のパターン

委託先のセキュリティ脆弱性を狙った「委託先踏み台型」

委託先企業の脆弱性が狙われて踏み台とされ、 委託元企業に対してマルウェアを含んだメールでの攻撃が行われる、委託先から窃取された秘密情報によって委託元企業が攻撃されるケース。
（主な事例）小島プレス、三菱パワー、など

脆弱性を埋め込んだソフトウエアを利用する「ソフトウエア埋め込み型」

委託先（販売元）の納品物（ソフト）に脆弱性が埋め込まれ、これを受け取った委託元（購入先）が攻撃を受けるケース。
（主な事例）SolorWinds、Kasayaなど

委託先に渡された個人情報を窃取する「委託先情報攻撃型」

委託元企業から委託先へ個人情報などの重要な情報を渡している場合、委託先の脆弱性を狙って個人情報が窃取され、外部に漏洩するケース
（主な事例）Peatix Inc., Dear Uなど

2022年3月　トヨタ自動車取引先部品メーカへのサイバー攻撃
国内14工場の稼働停止、1万3000台の生産に影響

ランサムウェアによるサイバー攻撃受けた小島プレス工業「リモート接続機器に脆弱性あった」調査結果を発表

4/1(金) 18:59 配信 23

メ～テレ

小島プレス工業（愛知県豊田市）

トヨタ自動車に部品を供給する小島プレス工業が2月末にサイバー攻撃を受け、影響でトヨタの国内の全工場が稼働を停止した件で、小島プレス工業は子会社が利用していたリモート接続機器に脆弱性があったとの調査結果を発表しました。

小島プレスによりますと脆弱性が見つかったのは、子会社が特定の外部企業との専用通信に利用していたリモート接続の機器です。

この機器から子会社を経由し本社のネットワークに侵入されたとみられ、2月26日の午後8時すぎに攻撃を受けた痕跡があったということです。

出所：Yahoo！Japanニュース　2022/4/1
https://news.yahoo.co.jp/articles/e5d2bc3acd3d90647b19151952cbd91ca3f04c2c

サプライチェーン攻撃の怖さ

1. 対策が厳重なターゲット企業を直接狙わず、**セキュリティ対策の手薄な企業を狙う**
2. 攻撃者は「付き合いのある企業や、使い慣れた製品なので大丈夫」との**思い込みの隙を突いてくる**
3. サプライチェーンがより大きく複雑になってきており、**委託元だけではサプライチェーンの把握困難**。
4. 攻撃された企業は**被害者でありながら、加害者となってしまう**

まず基本的なセキュリティ対策を確実に進めることが大切です。

新UTMサービス「OCH SG-ONE」

OCH SG-ONEとは

内閣サイバーセキュリティセンターが**企業に求めるサイバー攻撃対策を**
この1台でカバーする統合セキュリティ（UTM）です。

まるで浄水器のようにネットワーク通信を浄化します。

特長１：LAN全体を低コストで守る

✓ PC、タブレット、オフィス機器、監視カメラなど、**ネットワーク内の機器すべてのセキュリティをこの1台で守ります**。

✓ 接続ユーザ数は**無制限**です。

※快適な動作は光回線1Gbps100台前後を推奨します

✓ 本体価格に**5年間のライセンスおよび先出センドバック保守**を含みます。低コストながら強力なセキュリティ機能を提供します。

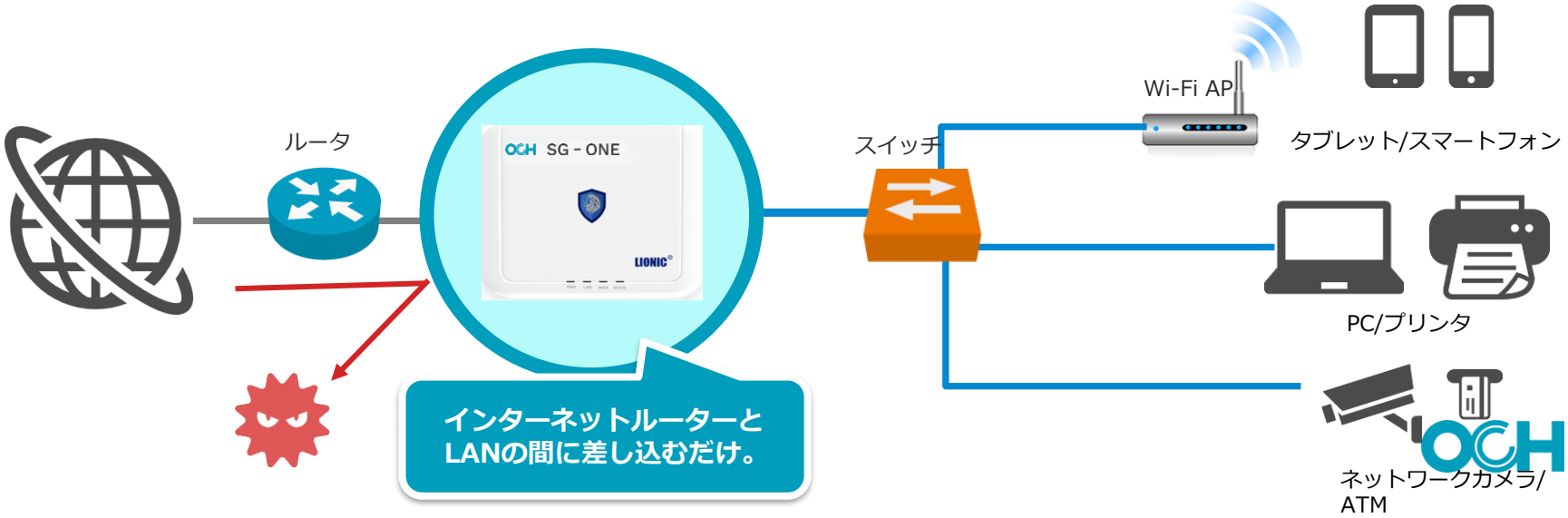
特長２：強力なコンパクトUTM

✓ ファイアウォール、アンチウィルス、IPSをはじめ、複数の強力なインターネットセキュリティ機能を**手のひらサイズのコンパクトボディ**に搭載しています。

特長３：ルータにつなぐだけ

✓ 推奨設定済の機器を出荷するため、**顧客毎の設定作業は不要**です。

✓ 設置工事も専門知識も不要。**在宅勤務や出張でも手軽に持ち運んですぐに設置**できます。



特長4：高速スキャン約700Mbps、圧倒的なスループット

✓ 業界最速クラスの処理速度で**業務の遅延無く利用できます。**

	OCH SG-ONE	Fortinet	Watch Guard	Juniper Network	SonicWall
モデル	SG-O100	FortiGate 30E	Firebox T30	SRX300	TZ300
アンチウィルス(AV) パフォーマンス	868 Mbps	200 Mbps	180 Mbps	100 Mbps	200 Mbps
侵入防止(IPS) パフォーマンス	846 Mbps	300 Mbps	240 Mbps	200 Mbps	300 Mbps
UTM パフォーマンス (FW+AV+IPS)	680 Mbps	150 Mbps	135 Mbps	100 Mbps	235 Mbps

3~5倍の サクサク通信

特長５：常時クラウド接続で常に最新

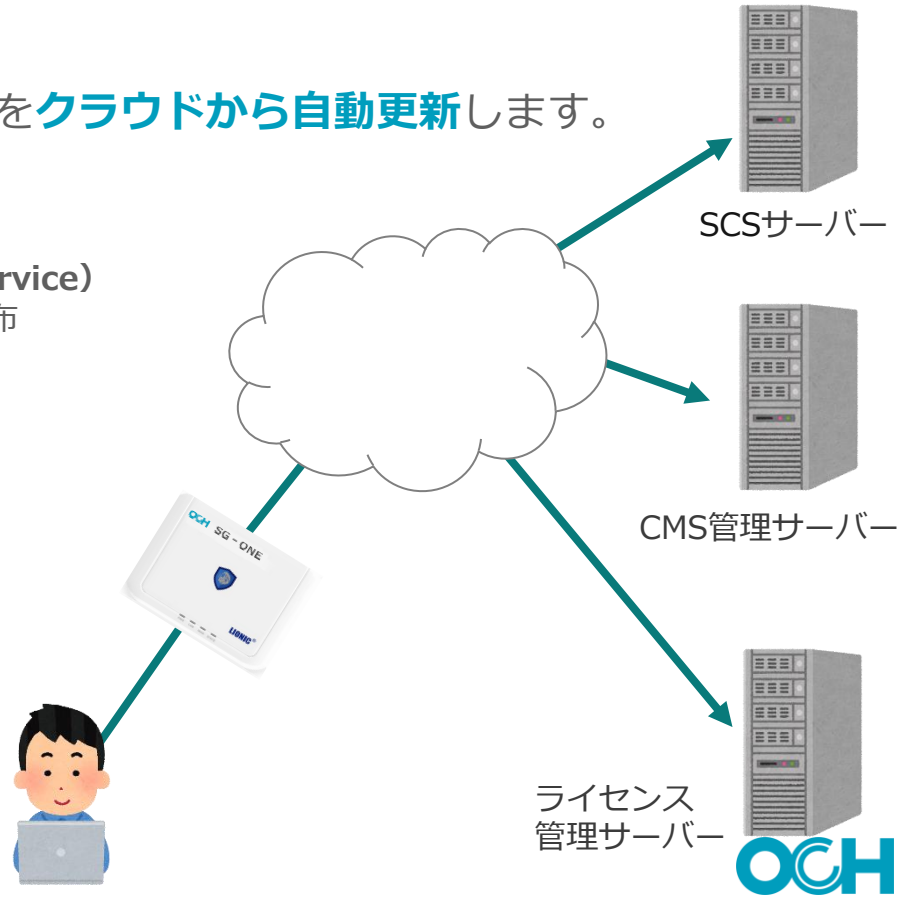
✓ 最新のセキュリティ情報とファームウエアを**クラウドから自動更新**します。

■ **セキュリティクラウドサービス（SCS：Security Cloud Service）**
有効期限情報を確認し、新しいシグネチャファイル(*1)を配布
シグネチャファイルはすべて、定期的に自動更新(*2)

(*1)シグネチャファイルで具体的に更新するファイルは、
ウィルスシグネチャ、ウェブガードシグネチャ、IPSシグネチャ
(*2)本体の管理画面からでも手動更新が可能

■ **CMS管理サーバー**
機器をリモート管理するサーバー
接続状況の確認、ファームウェアアップ等
運用に必要な機能を提供
※管理サーバは顧客の要望があればオプションで
管理権限を委譲する事が可能(メーカー側資源
での環境提供も可能)

■ **ライセンス管理サーバー**
ライセンスの付け替え等の実施



特長6：安心の5年保証

- ✓ 5年間のライセンスおよび先出センドバック保守が含まれます。**万一のトラブル時は機器の交換を行うだけですぐに復旧**できます。(*1)
- ✓ Web問合せフォームを準備。**エンドユーザから直接OCHサポートへ**、故障対応依頼、操作・設定方法の質問など問合せが可能です。
- ✓ オンライン管理マニュアルを展開し、**エンドユーザ独自でも管理・運用が簡単に実施**できるようになります。

【備考】*1：交換機についても標準設定のみ投入し出荷します。
故障機にお客様側で個別の設定が行われていた場合には、お客様自身でバックアップファイルを保管いただき、代替機が届いたら復元作業を実施いただく必要があります。予めご了承ください。

特長７：数多くの国際特許を取得

✓ 合計11個の国際特許を取得し**高速且つ精度の高い検知**を実現します。

■主な特許技術

・製品独自にパターンを整理/分類し、パケット単位で分析を行うオリジナル解析手法

・分類されたパケット毎に特性を付与し、パターンマッチ精度を劇的に高める特性付与手法

・Webページ、保存、アプリケーション、P2P等、種別毎に分析する精密分析手法

✓ **特許技術を最大限に活用**するために、特別に設計されたボード及びCPUを採用しています。

✓ **Googleにも技術提供**しています。

特長８：豊富な導入事例

世界各国での導入実績があり、**安心してご提案いただけます**。

- ✓ 国土交通省 運輸安全委員会
- ✓ 米スターバックス社
- ✓ 台湾銀行

等

仕様一覧

	OCH　SG-ONE
製品名	SG-O100
製造元	Lionic（台湾）
プロセッサ	Qualcomm IPQ4018, ARMv7コア×4個, 716MHz
システムメモリ	256MB
フラッシュ	512MB
インターフェース	WAN×1ポート、LAN×1ポート
電源	ユニバーサルスイッチング電源アダプタ100-240V AC IN, 12V DC OUT
外形寸法	約116（幅）×25（高）×91（奥）mm
重量	約135g（本体のみ）
ライセンス及び保守期間	60ケ月保証 （本体ライセンス、自動アップデート、先出センドバック保守、OCHサポートを含む）

機能一覧

分類	機能
ネットワークプロテクション	ファイアウォール
	侵入防御（IPS）
	侵入検知（IDS）
Web脅威対策	URLフィルタリング
	アンチフィッシング
	webアンチウィルス
アンチウィルス、アンチマルウェア	Windowsファイル共有（CIFS）
	ファイル共有（FTP）
	暗号化されていない圧縮ファイル（ZIP/GZIP/RAR）
ログ	各サービスのログ取得
自動アップデート	アンチウィルスパターンファイル
	Webフィルタリング

【備考】HTTPSスキャン機能、アンチスパム機能の搭載はありません。

OCHサポートに含まれる内容

- ✓ 障害発生時のライセンス対応　(付け替え作業)
- ✓ エンドユーザ向けWeb問合せフォームからの問い合わせ対応
  故障、操作/設定方法　(回答方法：メール)
- ✓ 本体マニュアルの提供
- ✓ 運用費用5年間無償
- ✓ 先出しセンドバック保守(5年)

ターゲットカスタマー

- 中小病院やクリニック
- フリーWi-Fi
- スマートファクトリー
- 個人情報を扱う業界
- IoTデバイス
- スモールビジネス
- 店舗
- テレワークや出張先


OCH
つくり、むすび、ささえ