船舶におけるサイバーセキュリティ対策の構築

KDDIデジタルセキュリティ株式会社
基盤セキュリティ本部　プロダクト部
福島　健二

サイバー攻撃とは

■サイバー攻撃とは

サイバー攻撃とは、インターネットを通じて他のコンピューターに不正にアクセスし、ダメージを与える行為。
「サイバーテロ」とも呼ばれる。

■サイバー攻撃の特徴 ※警察庁HPより

①攻撃実行者の特定が難しい
②攻撃の被害が潜在化する傾向がある
③国境を容易に超えて実行可能である

■サイバー攻撃の見える化

NICTOR　※情報通信研究機構（NICT）
https://www.nicter.jp/atlas
https://www.nicter.jp/top10

サイバー攻撃とは

ClassNK Consulting Service

◎攻撃者のプロファイル

○個人

- ネットワーク、プログラミングの知識に長けている人物
- ハッキング技術に興味を持っている人物
- 特定の思想を持つ人物
- 金銭の取得を狙った人物

ハッカー
クラッカー

○組織

- 特定の思想を持つ人物の集合体
- 自社の事業を他社より優位に進めたい企業（国家の場合も）

アノニマス等

○国家

- 国家として外貨獲得手段が欲しい
- 他国との交渉を優位に進めたい
- 他国に対して水面下でダメージを与えたい
- ハッカーを育成している

某東アジア
の国家等

サイバー攻撃とは

ClassNK Consulting Service

◎攻撃者の目的

減少　○興味・自己顕示欲

- 自分の知識や技術力を試したい
- 自分の技術力をアピールしたい

減少　○自己主張・思想

- 社会的・政治的な主張を表面化

増加　○金銭

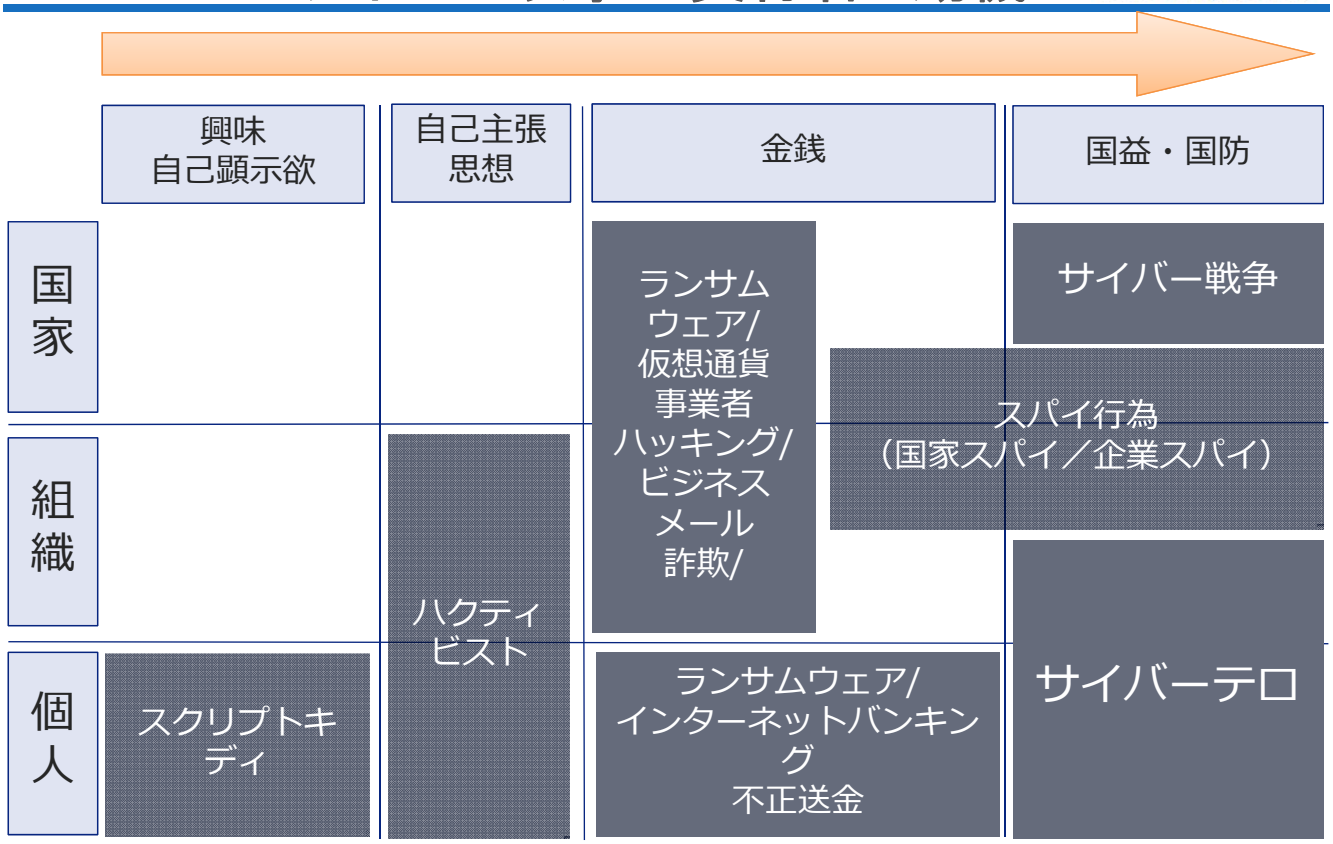
- 仮想通貨取得
- 偽装振込み（現金、仮想通貨）
- 知的財産情報取得（自社で利用）
- 知的財産情報取得（※）
- クレジットカード情報など個人情報取得（※）
  ※ブラックマーケット等で売買するため

増加　○国益・国防

- 国家間の交渉を優位に進めるための情報取得
- 他国のシステムを破壊し混乱させる
- 国家として金銭取得
- 国家的スパイ行為

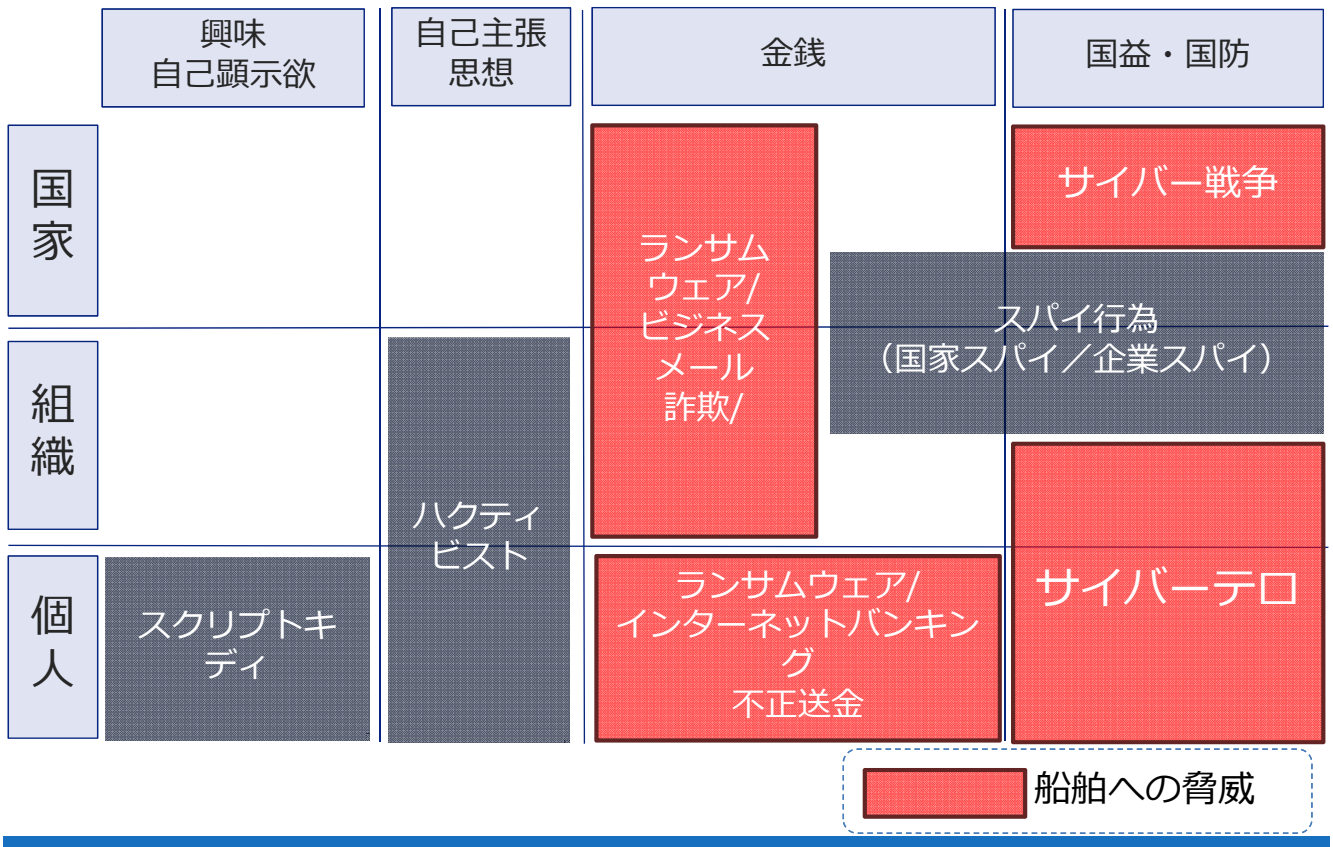
サイバー攻撃の実行者と動機

ClassNK Consulting Service



サイバー攻撃の実行者と動機

ClassNK Consulting Service



サイバー攻撃の実行者と動機

ClassNK Consulting Service

	興味 自己顕示欲	自己主張 思想	金銭	国益・国防
国家				
組織	主に 公開WEBサーバを狙った攻撃 （WEBサイトの改ざん） （DDoS攻撃）		主に PCを狙った攻撃 （ランサムウェア） （標的型攻撃）	主に PCを狙った攻撃 （標的型攻撃）
個人				

情報セキュリティの10大脅威（国内）

ClassNK Consulting Service

https://www.ipa.go.jp/security/vuln/10threats2019.html

順位	組織向け脅威	昨年順位
1位	標的型攻撃による被害	1位
2位	ビジネスメール詐欺による被害	3位
3位	ランサムウェアによる被害	2位
4位 (NEW)	サプライチェーンの弱点を悪用した攻撃の高まり	—
5位	内部不正による情報漏えい	8位
6位	サービス妨害被害によるサービスの停止	9位
7位	インターネットサービスからの個人情報の窃取	6位
8位	IoT機器の脆弱性の顕在化	7位
9位	脆弱性対策情報の公開に伴う悪用増加	4位
10位	不注意による情報漏えい	12位

情報セキュリティの10大脅威（国内）

順位	組織向け脅威
1位	標的型攻撃による被害
2位	ビジネスメール詐欺による被害
3位	ランサムウェアによる被害

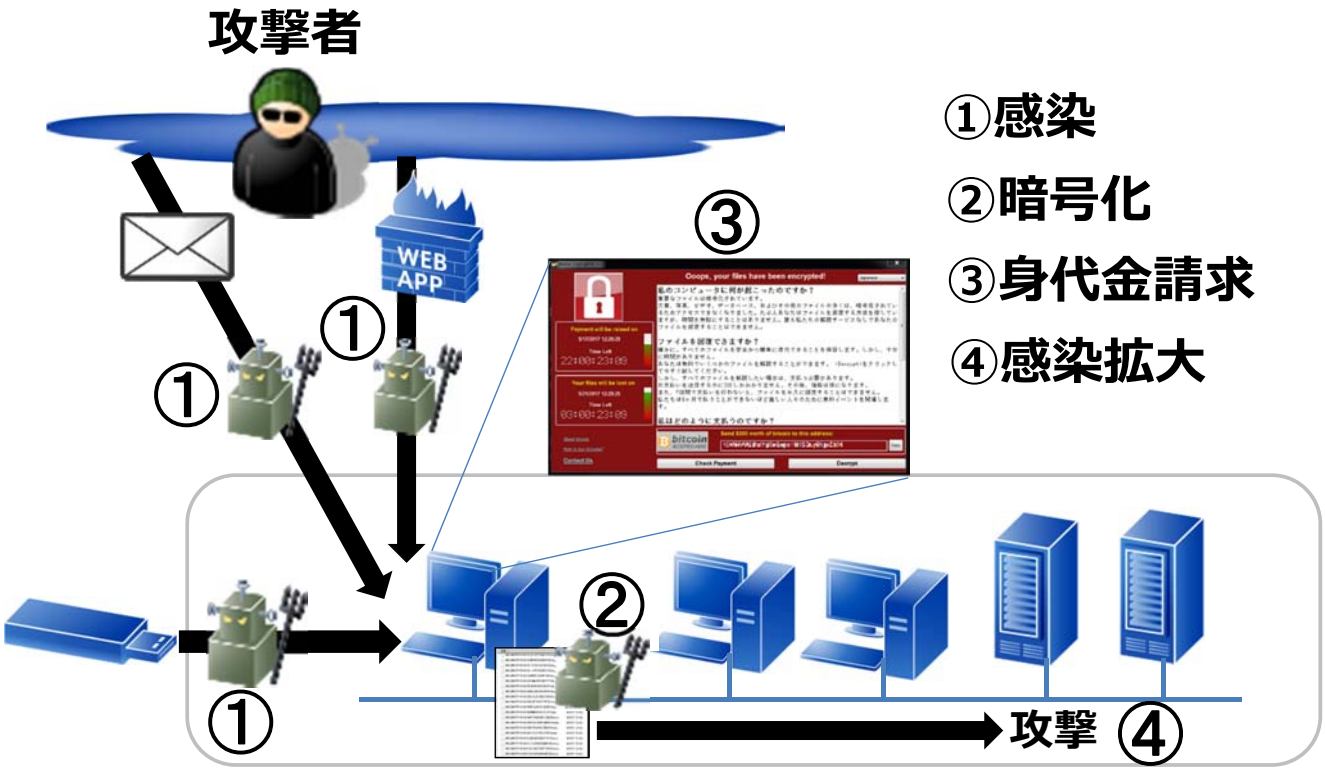
8位	IoT機器の脆弱性の顕在化	7位
9位	脆弱性対策情報の公開に伴う悪用増加	4位
10位	不注意による情報漏えい	12位

https://www.ipa.go.jp/security/vuln/10threats2019.html

ランサムウェアについて

ランサムウェアの仕組み

ClassNK Consulting Service



①感染

②暗号化

③身代金請求

④感染拡大

ランサムウェアの被害事例

ClassNK Consulting Service

Moller-Maersk社（デンマーク）

業務用のPC（陸上）が
新種ランサムウェアに感染し
社内の情報システムに拡散

サーバ4千台、PC4万5千台が
影響を受け、全社の情報システム
と業務管理が停止

10日間に渡り、
「深刻な事業の中断」
が発生し、
最大**3億ドルの損失**が発生

MAERSK

掲載日時： 2018-01-29 10:19:00

ZDNet Japan **海運大手マースク、2017年の「NonPetya」攻撃による深刻な影響を公表**

海運大手のA.P. Moller-Maerskは、2017年に欧州のさまざまな企業を襲った大規模ランサムウェア攻撃で、ほぼ「全てのインフラストラクチャ」の検査と何千台ものマシンの再インストールを余儀なくされたことを明かした。

著者：Charlie Osborne（Special to ZDNet.com）翻訳校正：編集部

URL：https://japan.zdnet.com/article/35113829/

海運大手のA.P. Moller-Maerskは、2017年に欧州のさまざまな企業を襲った大規模ランサムウェア攻撃で、ほぼ「全てのインフラストラクチャ」の検査と何千台ものマシンの再インストールを余儀なくされたことを明らかにした。

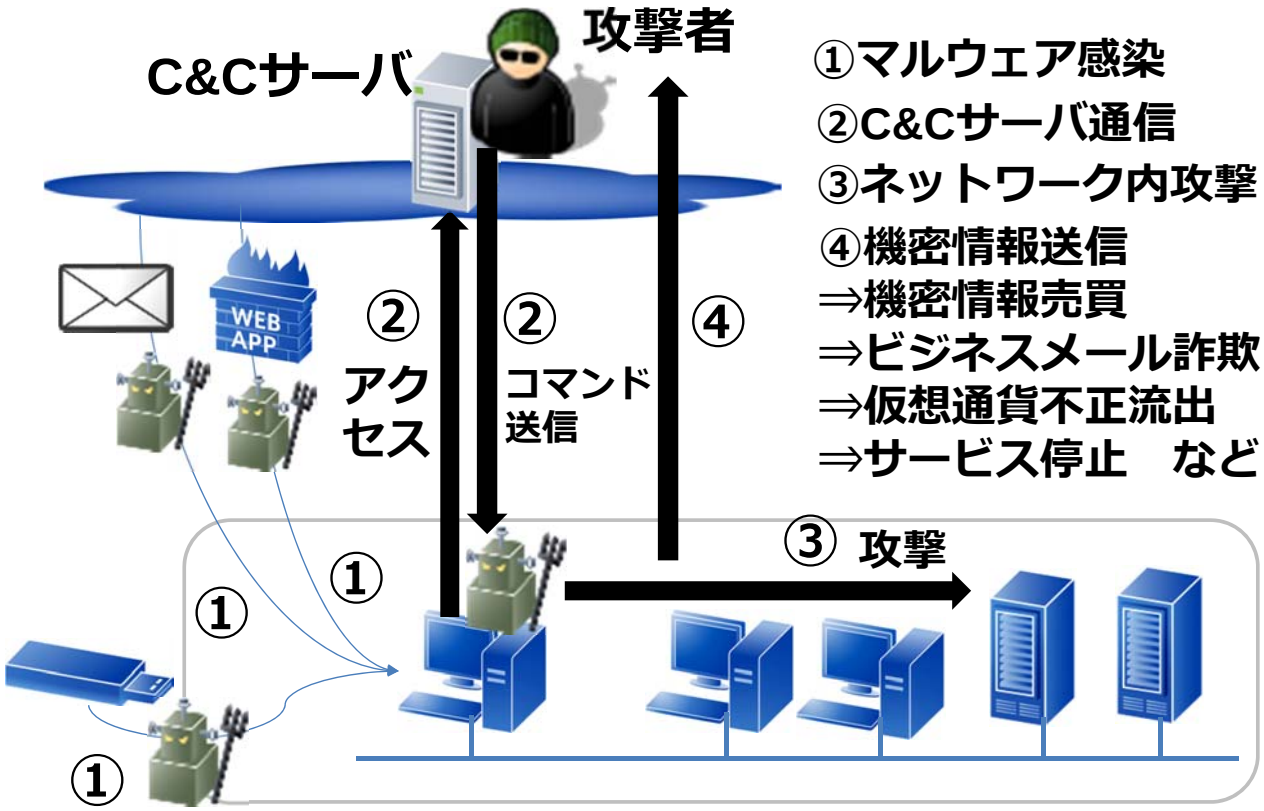
Maerskは、「Petya」ランサムウェアの新種「NonPetya」（NotPetya）を使用する攻撃の被害に遭い、情報システムと業務管理が全体的に停止に追い込まれた。

Maerskは以前、このランサムウェア攻撃による「深刻な事業の中断」が原因で、最大3億ドル（約330億円）の損失が発生する見通しだとしていた。

出典：ZD Net Japan　2018年01月29日付

標的型攻撃について

標的型攻撃の仕組み



①マルウェア感染
②C&Cサーバ通信
③ネットワーク内攻撃
④機密情報送信
⇒機密情報売買
⇒ビジネスメール詐欺
⇒仮想通貨不正流出
⇒サービス停止　など

ビジネスメール詐欺（2017年12月）

ClassNK Consulting Service

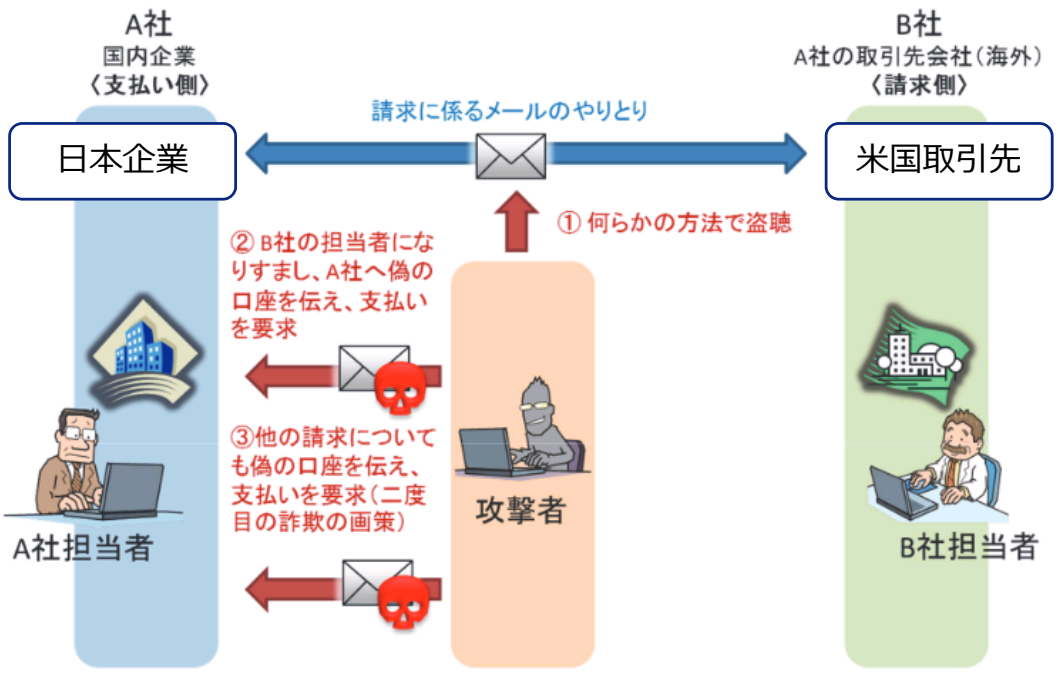
日本航空が“振り込め”詐欺被害に！航空機リース料名目で3億8千万円

日本航空（ＪＡＬ）は２０日、取引先を装った電子メールに指定された不正な銀行口座に航空機のリース料などを送金し、計約３億８千万円をだまし取られる被害に遭ったと発表した。同社は警視庁品川署や香港の警察当局などに被害届を提出、受理された。担当者の処分を検討しており、平成２９年度決算に特別損失の計上を予定している。　同社によると、ＪＡＬ本社財務部に９月下旬、「ボーイング７７７－３００ＥＲ」をリースしている米国の金融会社の担当者を装い、リース料の支払先を香港の銀行の別名義口座に変更するよう電子メールが届いた。偽のアドレスだったが、パソコンには担当者と同一のものが表示されていたため、信用したＪＡＬ社員は４日後の支払期日に３カ月分のリース料約３２５万５千ドル（約３億６千万円）を送金した。

ビジネスメール詐欺の手口

ClassNK Consulting Service

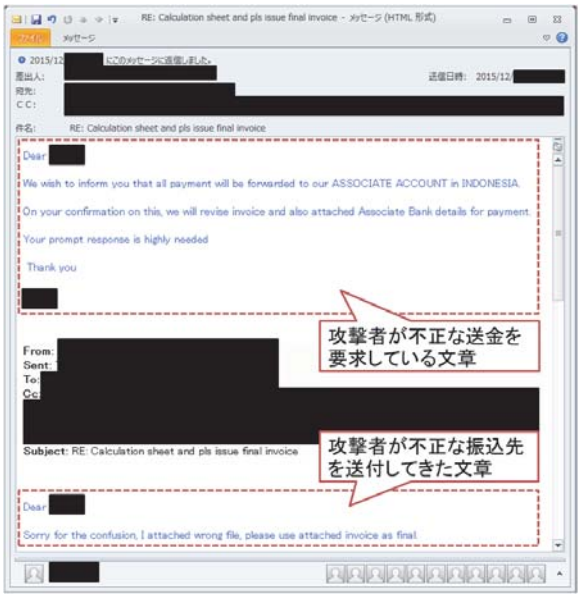
詐欺メールを送信する為に、長期に渡り請求に関するメールのやりとりを外部から見られていた可能性が高い。



出典：IPA「ビジネスメール詐欺「BEC」に関する事例と注意喚起」

ビジネスメール詐欺の手口

限りなく実際のメールの内容に近い詐欺メールを送信



- メールの題名
- メール本文
- 宛先の担当者名
- 差出人名称の偽装
- 送信元メールアドレス偽装
- メール送信のタイミング

出典：IPA「ビジネスメール詐欺「BEC」に関する事例と注意喚起」より

仮想通貨不正流出（2018年1月）

コインチェックの仮想通貨不正流出、過去最大580億円

仮想通貨取引所大手のコインチェック（東京・渋谷）は26日、利用者から預かっている約580億円分の仮想通貨が外部からの不正アクセスにより流出したと発表した。2014年に日本のビットコイン取引所だった「マウントゴックス」が約470億円分を消失させて以来、過去最大の仮想通貨の流出となる。　同日都内で記者会見を開いた和田晃一良社長は「このような事態になり深く反省している」と謝罪した。現在は一部サービスを停止し、再開の見通しは立っていない。　26日午前３時前に仮想通貨の一種である「ＮＥＭ（ネム）」のほぼ全額が不正に外部に送金された。同日午前11時過ぎに社内で異常を検知し、全通貨の出金を中止した。ＮＥＭ以外の仮想通貨の売買も中止している。

引用：日本経済新聞「コインチェックの仮想通貨不正流出、過去最大580億円」2018.1.27
https://www.nikkei.com/article/DGXMZO26231090X20C18A1MM8000/

コインチェック不正送金の手口

ClassNK Consulting Service

偵察／準備期間

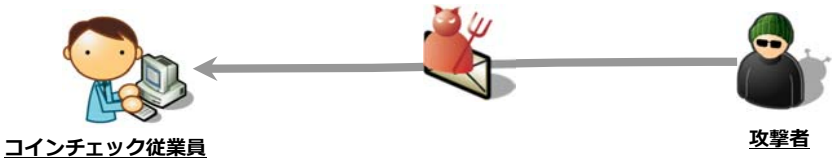
約6か月間

攻撃開始

不正送金完了

公開情報から得られたコインチェック内部者と攻撃者の間で長期に渡りメールのやりとりがあった

相手が信じきったところで攻撃開始。
マルウェアを仕込んだメールを送信。



標的型攻撃が成功し長期潜伏。
タイミングを見計らって不正送金操作！

たった20分程度で575億円が引き出された

現在のサイバー攻撃まとめ

ClassNK Consulting Service

目的	**金銭目的／国益・国防**
攻撃者	**組織的／国家的**
攻撃の種類	**PCを狙った攻撃 （標的型攻撃／ランサムウェア）**
攻撃の入口	**マルウェアを送り込む （メール、WEB、USBなど）**

船舶における
サイバー攻撃のリスク

船舶におけるサイバーリスク増大

船舶と陸上の通信は音声のみ
（船舶　～　陸上）データ通信なし

IoTやビッグデータ解析の普及により、
船舶からの情報収集ニーズが高まる
（船舶　→　陸上）片方向通信

データ解析からの運航支援、自動操舵、
自立運航システムなど、船陸間の
双方向通信が年々加速する
（船舶　⇔　陸上）双方向通信

船舶におけるサイバーセキュリティリスクは
今後、増大する見込み

船舶における
ランサムウェアの被害シナリオ

船内の１台のPCへランサムウェアが入り込む

船内に接続された他のPCへ感染が拡大する

感染したPCが暗号化、またはロックされ、使用不能になり、身代金（Bitcoin）の請求画面が表示される。

航行や荷役に必要なPCがもし感染してしまったら・・・・

船舶における
標的型攻撃の被害シナリオ

船内の１台のPCが標的型攻撃マルウェアへ感染する

C&Cサーバ経由で、船内のPCが外部から操作される

船内のシステム等へ更に攻撃を仕掛け、侵入範囲拡大

攻撃者の目的が、
- **船舶をリモートで操作してのサイバーテロ行為**
- **船舶のシステムを乗っ取り、身代金の要求**
- **国家間の水面下のサイバー戦争が目的だったら・・。**

サイバーセキュリティ対策を進めるには

サイバーセキュリティ対策の指針

船舶におけるサイバーセキュリティ
マネジメントシステムガイドライン
第2部　管理策

技術的対策

組織的対策

人的対策

船舶におけるサイバーセキュリティ
マネジメントシステムガイドライン
第1部　要求事項

サイバーセキュリティ対策を進めるには

組織的対策

- ◆サイバーセキュリティ対応体制の確立
- ◆サイバーセキュリティマネジメントマニュアルの作成
- ◆サイバーセキュリティに関する運用保守手順書の作成
- ◆運用保守セキュリティチェックリストの作成
- ◆サイバーセキュリティ運用規則の作成
- ◆インシデント対応手順書の作成　など。

サイバーセキュリティ対策を進めるには

人的対策

- ◆セキュリティ教育計画の作成
- ◆セキュリティ教育コンテンツの作成
- ◆乗組員向け、及び陸上担当者向け教育の実施
- ◆セキュリティ教育の記録　　など

サイバーセキュリティ対策を進めるには

技術的対策

- ◆ PC向けマルウェア（ウイルス）対策
- ◆ メールマルウェア（ウイルス）対策
- ◆ WEBマルウェア（ウイルス）対策
- ◆ ゲートウェイ型セキュリティ製品の導入
- ◆ USB接続制御ソフトウェアの導入
- ◆ ネットワーク分離スイッチの導入

など

セキュリティ対策の導入と セキュリティマネジメントシステム

組織（体制）作り

文書作成

緊急時対応手順作成

内部監査、経営者レビュー

教育・訓練

組織的対策

セキュリティマネジメントシステムの構築

人的対策

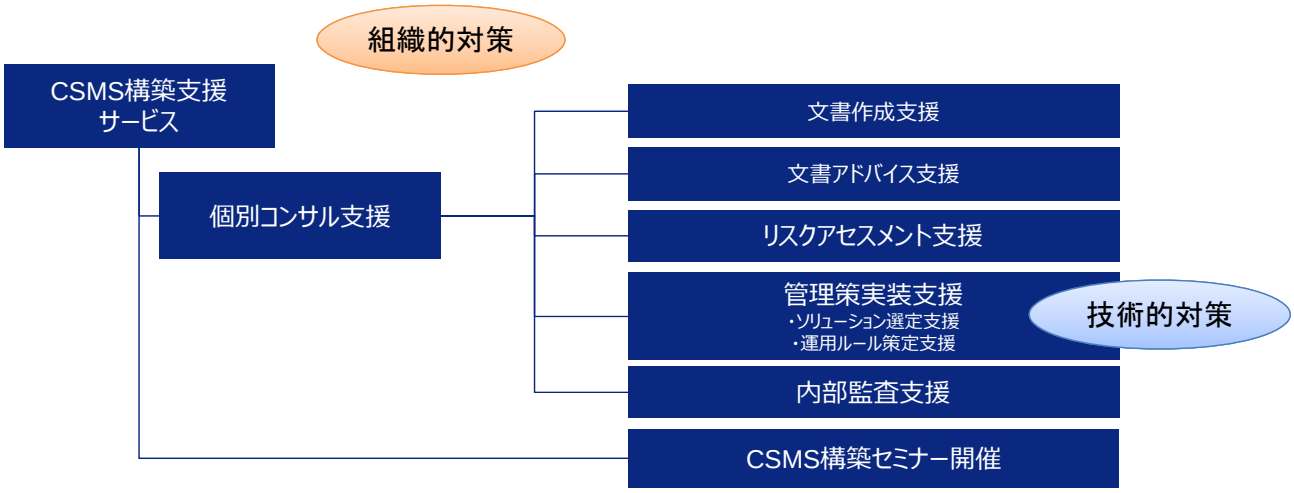
教育・訓練の継続実施

技術的対策

セキュリティ対策の導入（管理策）

- ファイアウォール
- PCウイルス対策
- USB対策
- WEBフィルタリング
- メールセキュリティ

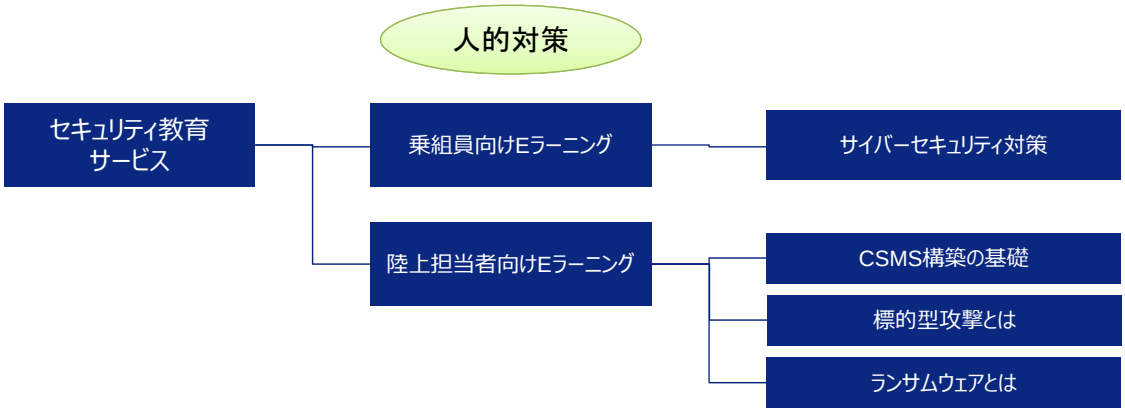
CSMS構築支援サービス



- CSMSの構築をサポート
- CSMS文書ひな形提供
- 各種CSMS運用フォーマットひな形提供
- 2020年1月以降サービス提供開始予定

※詳細は、株式会社ClassNKコンサルティングサービスWEBサイトにてご案内予定

セキュリティ教育サービス



※順次提供コンテンツを追加予定

- ClassNKコンサルティングサービスからの受講修了証発行
- インターネット環境があればどこからでも受講可能
- BIMCOサイバーセキュリティガイドラインVer5.3対応
- 2020年1月サービス提供開始予定

※詳細は、株式会社ClassNKコンサルティングサービスWEBサイトにてご案内予定

ご清聴ありがとうございました。

船舶におけるサイバーセキュリティ対策の構築

1. はじめに

　ここ数年、衛星通信でのブロードバンド環境が提供され始め、船舶においてもインターネットへの常時接続化が可能となってきている。それに伴い、陸上で発生していたマルウェアなどのサイバー脅威が、船舶においても発生するリスクが増大している。本講演では、サイバー事件、事故の事例をもとにして、ランサムウェアや標的型攻撃について概要を理解し、船舶におけるサイバーリスクへの対策の指針について説明する。

2. 船舶におけるサイバーセキュリティ対策の構築

　サイバー攻撃は、時代とともにその攻撃者やその目的は変わってきている。インターネット創世記では、ネットワークやプログラミングの知識に長けた一部の人間が、興味本位や自己の技術力を試す為に、インターネット上に公開されている WEB サイトを改ざんするなど、趣味の延長レベルでの攻撃であった。その後、アノニマスに代表される、政治的な主張のためにハッキング行為をおこなう集団が出てきたことで、組織化されていった。

　それまでは、攻撃者のターゲットとなるのは、インターネット上に公開されていた WEB サーバ等であったが、金銭を奪うことを目的としたサイバー攻撃が増加してくるに従い、企業や組織などが業務で使用している PC を狙ったマルウェアによる攻撃が増加していった。

　その例としては、ランサムウェア、標的型攻撃、インターネットバンキングの不正操作をおこなうマルウェアなどがある。特に、標的型攻撃では長期に渡って潜伏し続け、情報を盗み見し続ける、その結果、企業内の PC を外部から操作することで、仮想通貨を不正に取得するなどの事件が発生している。

　また国家間のサイバー戦争が現実のものとなっており、ハッキングを行う部隊を組織し、ハッカーの育成を行っている国家もある。船舶は今まで攻撃のターゲットとなることは少なかったが、インターネットと常時接続されることにより、サイバー攻撃のターゲットとなる可能性は高まっている。海運は世界中の物流の要であり、海上での物流が機能しなくなった場合、世界経済に与える影響は莫大である。そのため、業界全体でサイバー対策のレベルを上げていくことが急務である。

3. おわりに

　船舶におけるサイバーセキュリティ対策を行う場合には、組織的、人的、技術的の 3 つの観点から対策を考え、また、現状のリスクを分析し、継続的な対策を行っていくことが効果的である。

　現在、弊社では株式会社 ClassNK コンサルティングサービスと協業にて、海運業界向けのサイバーセキュリティ対策支援ツールの提供を予定している。