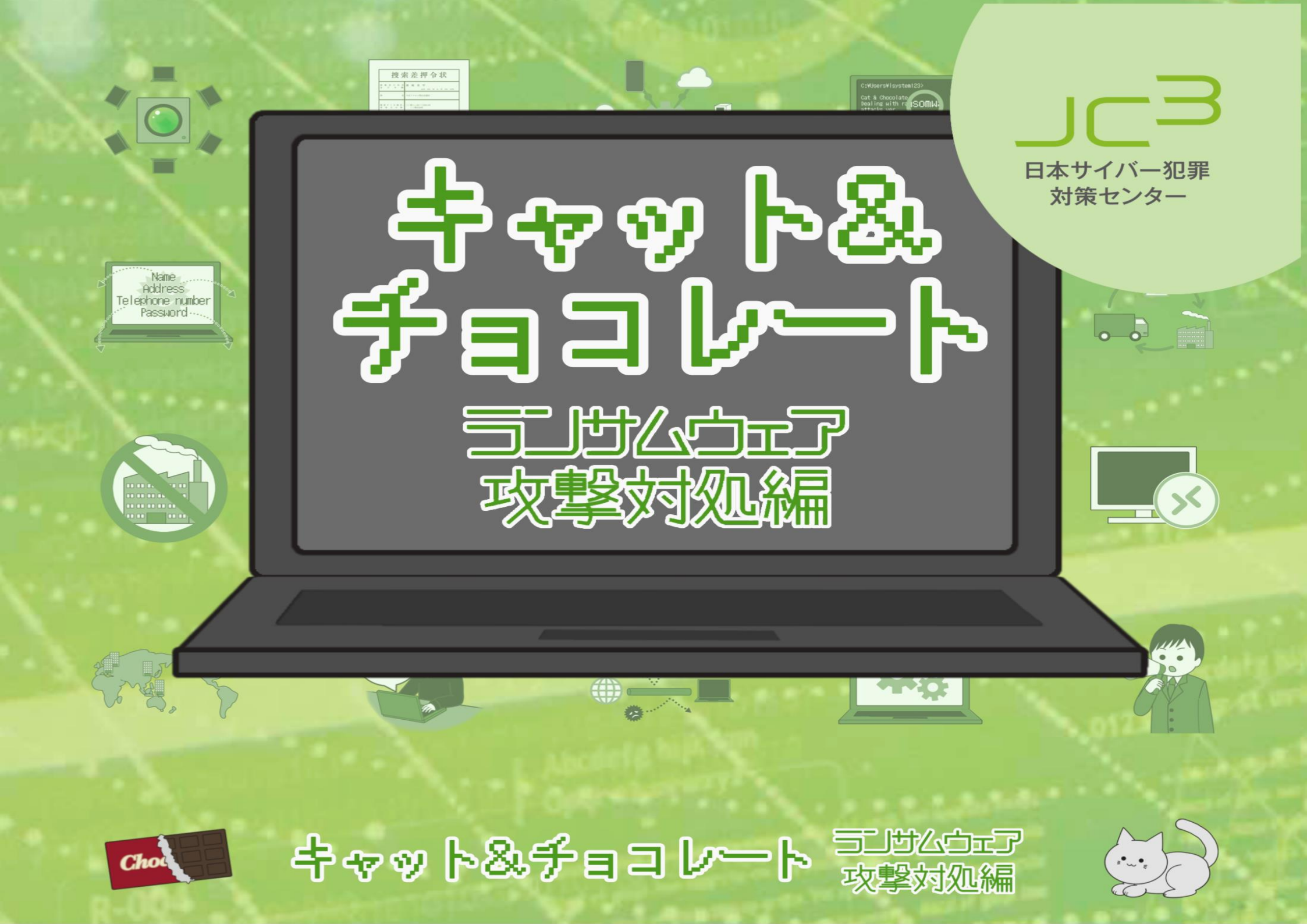

JC3
日本サイバー犯罪
対策センター
キャット&
チョコレート
ランサムウェア
攻撃対処編
Name
Address
Telephone number
Password
Choc
キャット&チョコレート
ランサムウェア
攻撃対処編

キャット&チョコレート
ランサムウェア攻撃対処編

JC3
日本サイバー犯罪
対策センター

このゲームは、人気カードゲームである「キャット&チョコレート」を原案としています。

ランサムウェア被害に遭った企業、その通報を受けた警察が、訪れるさまざまな困難に対して、それぞれの立場から危機回避、証拠保全・犯人検挙のため、どのように行動する必要があるかについて議論、解決までのストーリーを作成する中で、官民の相互理解、企業のセキュリティ課題への気付き、被害時の対応力強化を目的としたゲームです。

JC3より発刊した「ランサムウェア攻撃に対する捜査ハンドブック」の姉妹品として作成したものであり、本ゲームと併せ同書を読んでいただくことで、更にランサムウェア攻撃対処に関する知識、官民の相互理解を深めることができると考えております。ランサムウェア事案打開に向けた一筋の光明となれば幸いです。

ゲームデザイン：一般財団法人日本サイバー犯罪対策センター
（JC3）

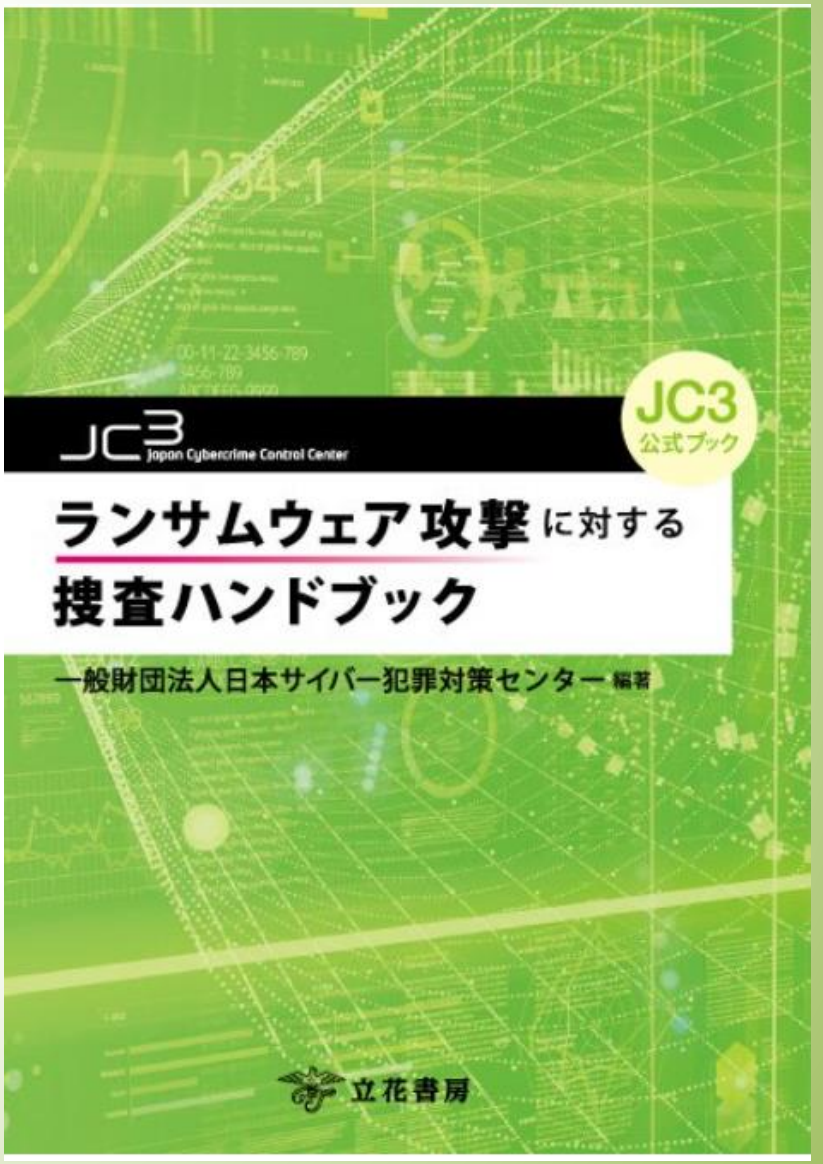
イラストデザイン：有山 有

●ゲームの構成、ルールは、
『キャット＆チョコレート　日常編』※
を原案として作成しています。

※『キャット＆チョコレート　日常編』
ゲームデザイン：秋口ぎぐる
販売元：株式会社幻冬舎

「ランサムウェア攻撃に対する捜査ハンドブック」

- 本書はJC3の特徴である「官民連携」により作り出されたもので、警察のサイバー捜査官、民間のセキュリティ技術者、検事、弁護士の皆様の経験・知見をも取り込んだ一冊であり、捜査員の初動対応に有用であることはもちろんのこと、民間企業などランサムウェア攻撃への対応に関わる方にとって法執行機関が何を求めているかを知ることができる内容です。
- 下記のURLより購入可能ですので、是非ご購読ください。
  https://tachibanashobo.co.jp/products/detail/3896
- 著者：一般財団法人日本サイバー犯罪対策センター 編著



- **両面A4用紙（厚口：175μm）での印刷を推奨します。**
- **印刷する際は、両面印刷（短片綴）で、『6ページから23ページ』を印刷してください。**

- **以下、カードゲームのデータになります。**

暗号化されたデータをバックアップから復元しようと試みたが、バックアップごと暗号化されていた。

Event Card

調査の結果、海外拠点から侵入されていることが判明した。

Event Card

VPNを設定した業者が放置していた脆弱性から侵入されていたことが分かった。

Event Card

感染端末がネットワークに繋がれており、インターネットへの接続がされている状態であった。

Event Card

担当者の独自判断により、調査前に多くのシステムと機器が初期化・更新されてしまっていた。

Event Card

侵入原因が分からないままシステムを復旧させたが、数日後に再び暗号化された。

Event Card

社内が管理しているネットワーク構成図が、実際の運用と異なっていることが判明した。

Event Card

社内全ての業務用システムが暗号化され、業務が完全に停止した。

Event Card


JC3
Japan Cybercrime
Control Center
3
JC3
Japan Cybercrime
Control Center
3
JC3
Japan Cybercrime
Control Center
3
JC3
Japan Cybercrime
Control Center
3
JC3
Japan Cybercrime
Control Center
3
JC3
Japan Cybercrime
Control Center
3
JC3
Japan Cybercrime
Control Center
3
JC3
Japan Cybercrime
Control Center
3

当初、情報漏洩はないと広報していたが、後日顧客情報が漏洩していることが発覚した。

Event Card

リークサイトで公開された情報が、SNSで拡散され炎上している。

Event Card

業務影響が広範囲に及んでおり、被害の全容が特定出来ていない。

Event Card

従業員がランサムウェア攻撃に関連している可能性が出てきた。

Event Card

顧客からサービスが利用できない旨の問い合わせが殺到し、お客様窓口がパンクしている。

Event Card

取引先から、契約を更新するため高額な追加セキュリティ対策を要求されている。

Event Card

初動対応は終わったが、ランサムウェアアクターがまだシステム内に潜伏しているかもしれない。

Event Card

ステークホルダーから、身代金の支払いをしてシステムの復旧を急げと言われている。

Event Card


JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
4

業務を委託している業者においてランサムウェア被害が発生し、顧客の個人情報が漏洩した。

Event Card

複数拠点で同時に被害が発生していることが発覚、同時に対応しなければならない。

Event Card

経営層が、被害公表と警察への連絡に難色を示している。

Event Card

インシデント対応が終了した後にリークサイトに機密情報が掲載された。

Event Card

ノーウェアランサム攻撃の被害に遭い、影響範囲が不明である。

Event Card

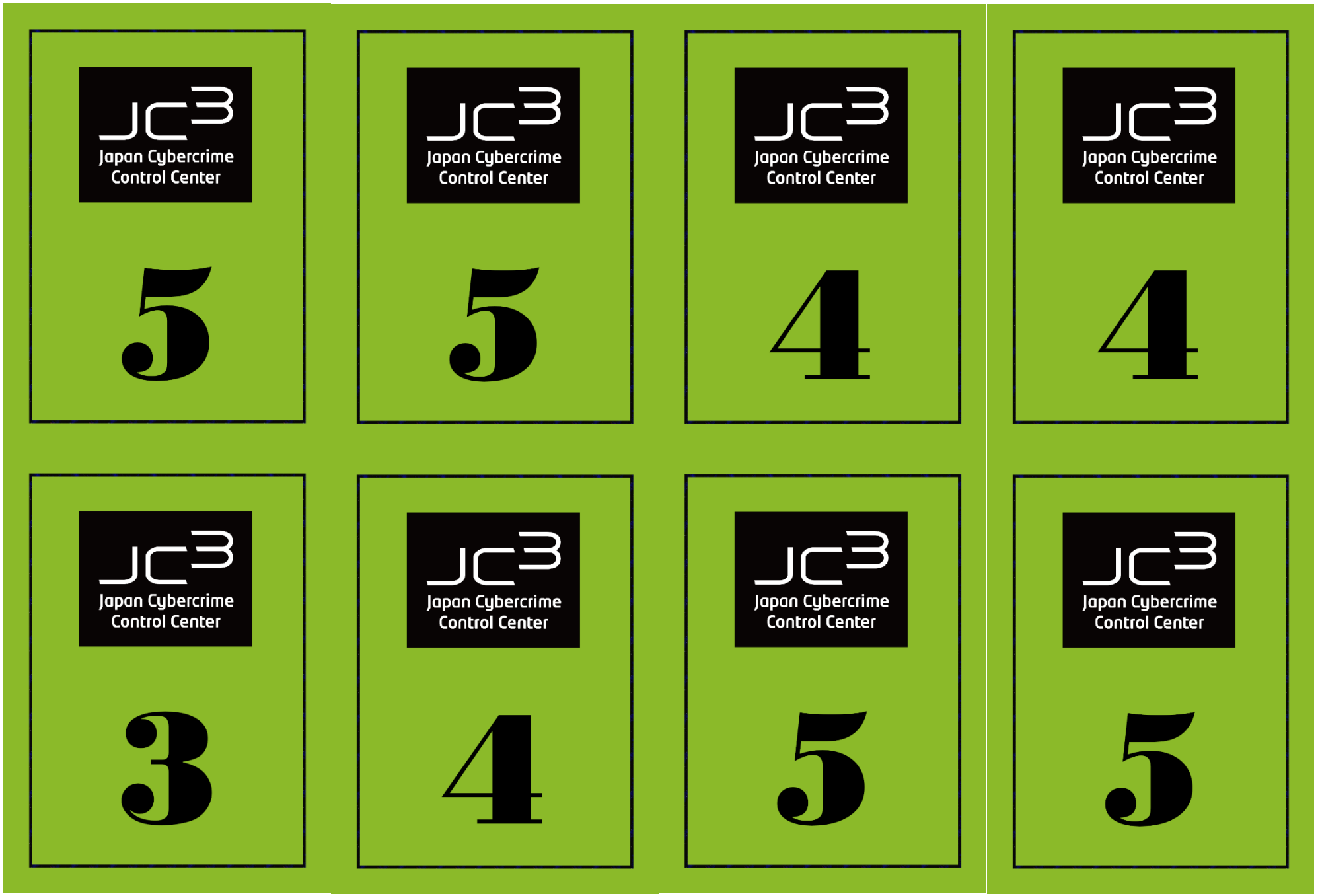
従業員の個人用アドレスに対して、ランサムウェアアクターから、身代金を払えとメールが送られてきた。

Event Card

Event Card

Event Card

この2枚はホワイトカードです。自社の環境に沿ったイベントを追加したい場合に使用してください。


JC3
Japan Cybercrime
Control Center
5
JC3
Japan Cybercrime
Control Center
5
JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
3
JC3
Japan Cybercrime
Control Center
4
JC3
Japan Cybercrime
Control Center
5
JC3
Japan Cybercrime
Control Center
5

セキュリティ
ベンダー

Keyword Card・Security Vender

身代金

Keyword Card・Ransom

チョコレート

Keyword Card・Chocolate

ネコ

Keyword Card・Cat

VPN

Keyword Card・Virtual Private Network

警察官

Keyword Card・Police Officer

記者会見

Keyword Card・Press Conference

バックアップ

Keyword Card・Backup

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

フィッシング
メール

Keyword Card・Phishing Mail

ランサムノート

Keyword Card・Ransomware Notes

RDP

Keyword Card・Remote Desktop Protocol

フォレンジック
ツール

Keyword Card・Forensic Tools

NW構成図

Keyword Card・Network Diagram

EDR

Keyword Card・Endpoint Detection and Response

復号ツール

Keyword Card・Decryption Tool

攻撃者交渉

Keyword Card・Negotiation

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

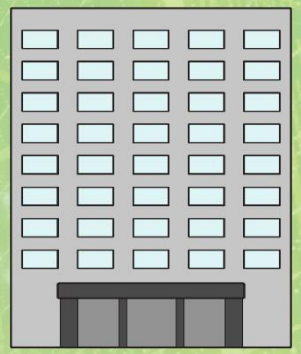
経営者

Keyword Card・Executive

CSIRT

Keyword Card・CSIRT

監督官庁



Keyword Card・Supervisory Authority

被害広報

Keyword Card・Damage Publicity

弁護士

Keyword Card・Lawyer

広報担当者

Keyword Card・Public Relations Officer

情報システム担当者

Keyword Card・Systems Officer

情報システム責任者

Keyword Card・Systems Manager

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

情報流出

Keyword Card・Information Leak

SIベンダー

Keyword Card・Systems Integrator

サイバー保険

Keyword Card・Cyber Insurance

内部犯行

Keyword Card・Insider

海外支社

Keyword Card・Overseas Branches

システム再構築

Keyword Card・System Reconstruction

サーバ再起動

Keyword Card・Server Restart

NW遮断

Keyword Card・Network Shutdown

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

KEYWORD CARD

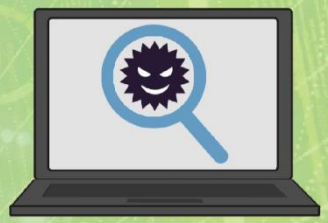
JC3 Japan Cybercrime Control Center

KEYWORD CARD

JC3 Japan Cybercrime Control Center

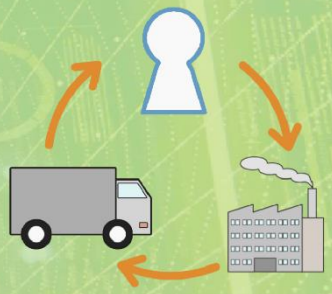
KEYWORD CARD

ウィルススキャン



Keyword Card・Virus Scan

サプライチェーン



Keyword Card・Supply Chain

社内教育

Keyword Card・Internal Education

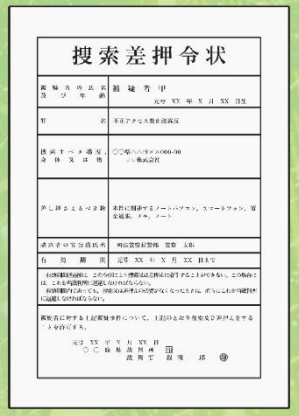
業務停止

Keyword Card・Business Suspension

警察手帳

Keyword Card・Police Badge

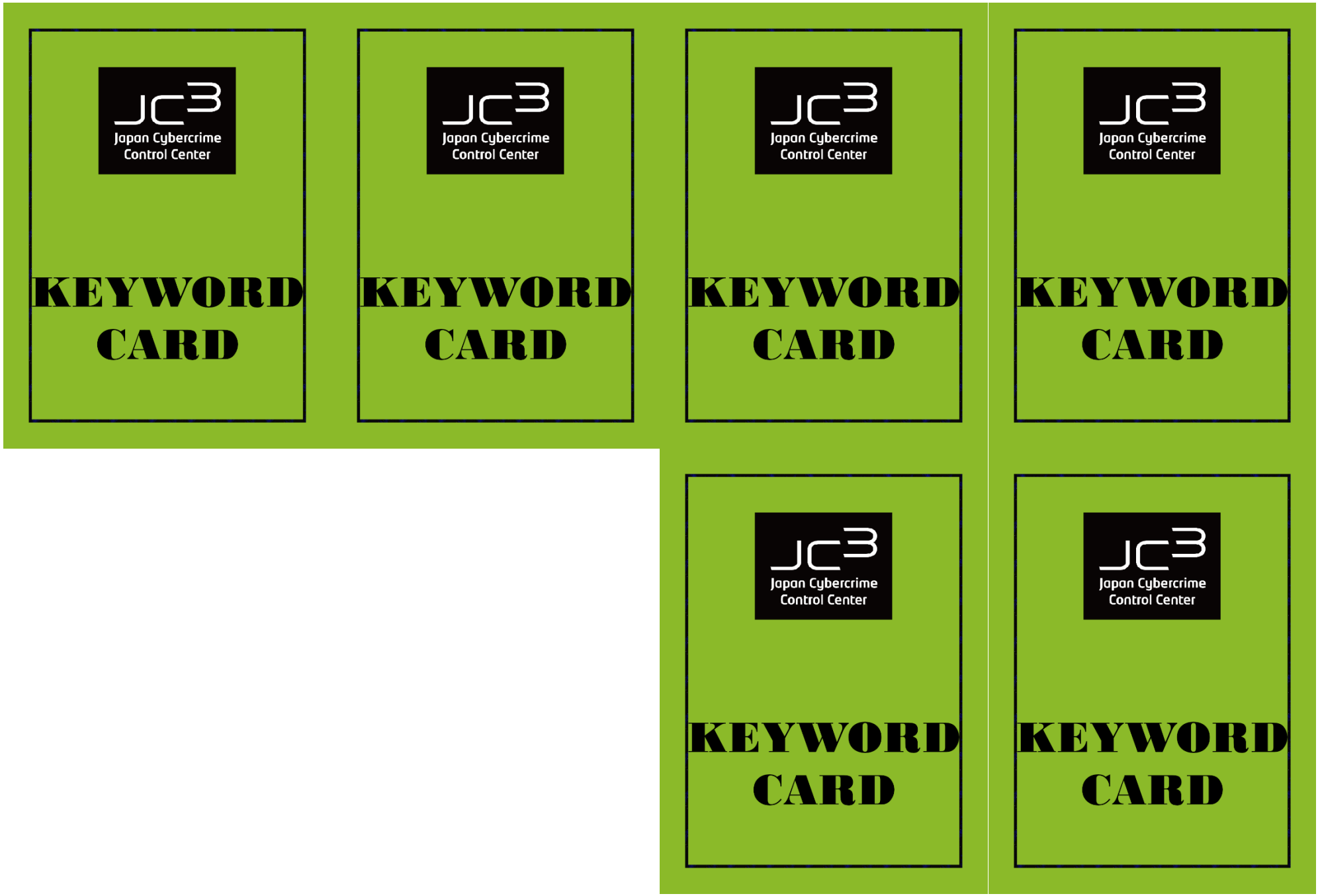
捜索差押令状



捜索差押令状

被疑者の氏名及び年齢	被疑者甲 元号 XX 年 X 月 XX 日生
罪名	不正アクセス禁止法違反
捜索すべき場所、身体又は物	○○県△△市××0-00 □□株式会社
差し押さえるべき物	本件に関係するノートパソコン、スマートフォン、写真撮影、メモ、ノート
請求者の官公職氏名	司法警察員警部　警察 太郎
有効期間	元号 XX 年 X 月 XX 日まで

Keyword Card・Search Seizure Warrant


JC3
Japan Cybercrime
Control Center
KEYWORD
CARD
JC3
Japan Cybercrime
Control Center
KEYWORD
CARD
JC3
Japan Cybercrime
Control Center
KEYWORD
CARD
JC3
Japan Cybercrime
Control Center
KEYWORD
CARD
JC3
Japan Cybercrime
Control Center
KEYWORD
CARD
JC3
Japan Cybercrime
Control Center
KEYWORD
CARD

チョコレート
チーム

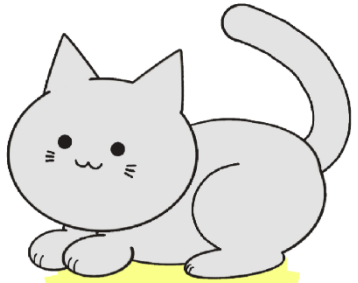
Team Card

チョコレート
チーム

Team Card

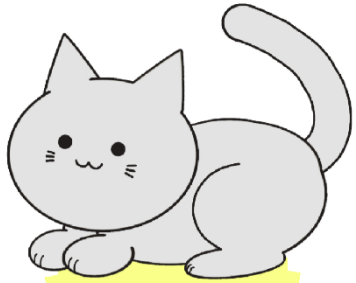
チョコレート
チーム

Team Card



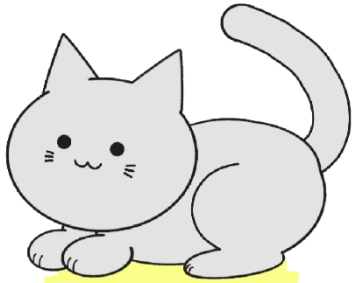
キャット
チーム

Team Card



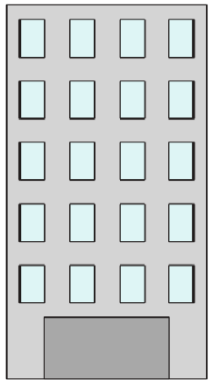
キャット
チーム

Team Card



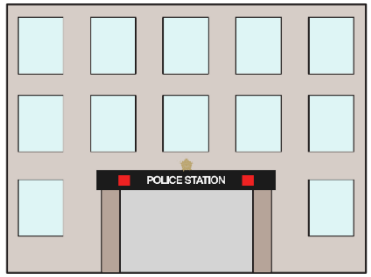
キャット
チーム

Team Card



Role Card

企業役



Role Card

警察役

JC3 Japan Cybercrime Control Center

TEAM CARD

JC3 Japan Cybercrime Control Center

TEAM CARD

JC3 Japan Cybercrime Control Center

TEAM CARD

JC3 Japan Cybercrime Control Center

TEAM CARD

JC3 Japan Cybercrime Control Center

ROLE CARD

JC3 Japan Cybercrime Control Center

ROLE CARD

JC3 Japan Cybercrime Control Center

TEAM CARD

JC3 Japan Cybercrime Control Center

TEAM CARD