ISCO

EC-COUNCIL

テレワークセキュリティセミナー

テレワークを狙ったサイバー攻撃に備える

～攻撃に対応するための技術的なセキュリティ対策に今、何が必要なのか～

GSX
GLOBAL SECURITY EXPERTS

Mina Secure

2021年11月11日

グローバルセキュリティエキスパート株式会社

自己紹介

武藤 耕也

@ KoyaMuto

RISS / 情報処理安全確保支援士
CEH / 認定ホワイトハッカー
JNSA ISEPA（教育事業者連絡会）メンバー
GSX-CSIRT PoC担当官
日本CSIRT協議会 インシデント分析WG
ISOG-J　セキュリティ連携WG

GSX（グローバルセキュリティエキスパート）
CCO 兼 コーポレートエバンジェリスト

ISMS
PCIDSS
CSIRT構築支援
標的型攻撃対策
レッドチームなど

グローバルセキュリティエキスパート株式会社　会社概要

設立

2000年4月

資本金

6.36億円

主要株主

株式会社ビジネスブレイン太田昭和
兼松エレクトロニクス株式会社
株式会社野村総合研究所

東京本社：港区海岸1丁目15-1 スズエベイディアム
西日本支社：大阪市中央区淡路町3-1-9
名古屋オフィス：名古屋市中区錦1-5-13　オリックス名古屋錦ビル

事業ドメイン

GSXは、サイバーセキュリティ教育カンパニーです

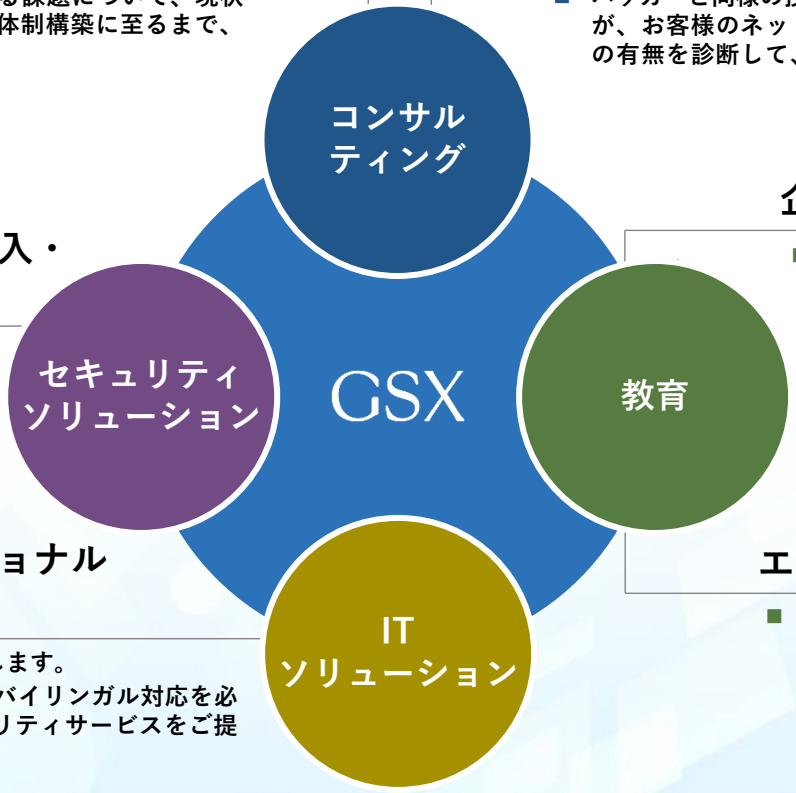
DXが加速し、サイバーセキュリティニーズが拡大する市場で
各事業の軸に「教育」を据え、日本の情報セキュリティレベル向上に貢献します

マネジメントコンサルティング

- お客様が抱える情報セキュリティに関する課題について、現状の可視化から、解決に向けた計画策定・体制構築に至るまで、一貫した支援をご提供します。

テクニカルコンサルティング

- ハッカーと同様の技術を持つ専門エンジニア(ホワイトハッカー)が、お客様のネットワークシステムに擬似攻撃を行い、脆弱性の有無を診断して、対策措置、結果報告書までをご提供します。



サイバーセキュリティ製品導入・運用サービス

- 最新の脅威や攻撃手法などに対して有効なサイバーセキュリティ製品・サービスを、実装・運用を組み合わせたワンストップソリューションでご提供します。

企業向けセキュリティ訓練

- 業界シェアNo.1(アイ・ティ・アール調べ※1)標的型メール訓練サービスや、ITセキュリティeラーニングサービスのMina Secure®によって従業員のセキュリティリテラシー向上をご支援します。

バイリンガルITプロフェッショナルサービス

- バイリンガルのIT人材リソースをご提供します。
  グローバル拠点への対応はじめ、国内のバイリンガル対応を必要とするお客様へのIT+サイバーセキュリティサービスをご提供します。

エンジニア向け教育講座

- セキュリティ全体像を網羅した教育サービスをご提供します。EC-Councilセキュリティエンジニア養成講座、日本発のセキュリティ人材資格「SecuriST(セキュリスト)認定脆弱性診断士」などで、セキュリティ人材を育成します。

※1 出典：ITR、標的型攻撃メール訓練サービス市場　従業員1,000～5,000人未満　2019年度　ベンダー別売上金額シェア

今日の結論は

敵を知り己を知れば百戦危うからず

孫子の兵法

【その１】 サイバー犯罪が止まらない背景

現在のサイバー犯罪とはどういうものか？

実被害が止まらない


製造業では、設計データ
だけでなく、生産技術情
報や、サプライ情報が

建設業（特にJV）では、プラント/工場建設時の施主情報、設計データが

大手メディアでは、視聴者情報やコンテンツ、人事情報が

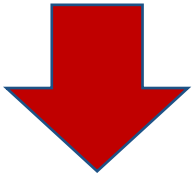
ランサムウェアの被害も拡大の一途

実被害の例（20年12月）

国内大手製造業：**Web会議通知を装ったメール**

12月18日（金）　**ウイルス感染　社内のPC**

GW / メールサーバ / 端末それぞれでアンチウィルスを実行していたが検知できず



犯人が使う裏口

12月19日（土）　**乗っ取られバックドアに**

12月21日（月）　**ファイルサーバ7台**
ADサーバ を含む合計51台が
一斉にランサムによりロック

システムを管理する
重要なサーバ

脅迫

「機密データを第三者へ販売されたくなければ、

相応の価格で買い取れ」

暗号化された範囲（犯行グループが到達した範囲）

本社イントラネットのシステム

ーイントラネットは全ての情報にアクセスできたと考えられる

本社の基幹システム

ーこれで、受発注業務が止まってしまった

工場の生産管理システム

ー2箇所の工場ではラインも停止

開発部局、営業、総務部門のファイルサーバ

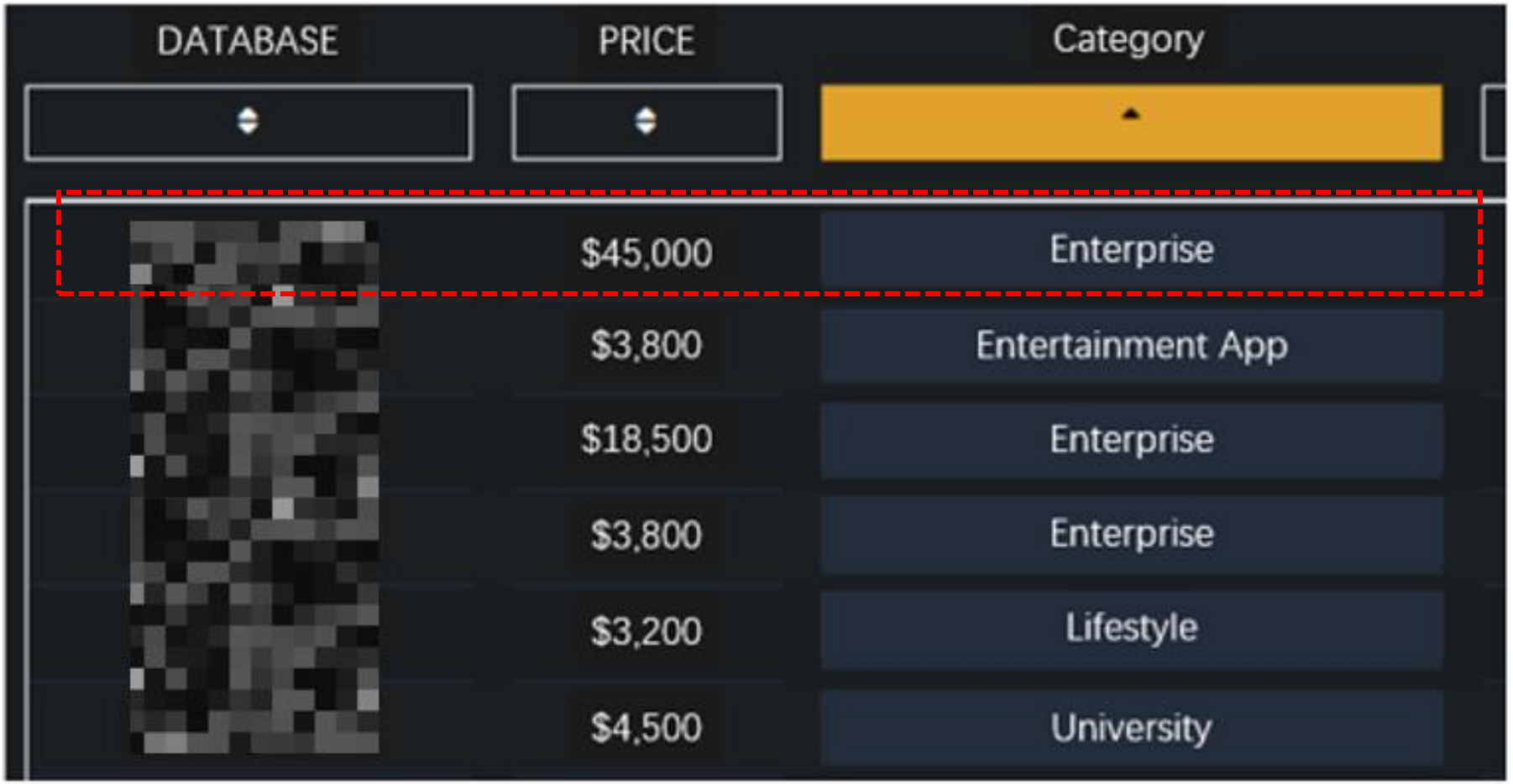
ー営業活動や、本社活動業務も事実上ダウン

【実例】窃盗被害にあったデータは

犯行グループは、企業の機密情報をデータベース化して販売

DATABASE	PRICE	Category	RECORDS
ShareThis	$3,800	Web Plugin	1,900,000
500px	$2,800	Photography	206,000
Houzz	$4,500	Lifestyle	3,400,000
MyFitnessPal	$3,800	Lifestyle	50,000,000
MyHeritage	$3,200	Lifestyle	65,700,000
Dubsmash	$4,500	Entertainment App	15,500,000
YouNow	$3,200	Entertainment App	40,000,000
Armor Games	$900	Entertainment	7,800,000
Wanelo	$3,800	ecommerce	2,900,000

【実例】窃盗被害にあったデータは



DATABASE	PRICE	Category
[redacted]	$45,000	Enterprise
[redacted]	$3,800	Entertainment App
[redacted]	$18,500	Enterprise
[redacted]	$3,800	Enterprise
[redacted]	$3,200	Lifestyle
[redacted]	$4,500	University

サイバー犯罪者 = 悪いハッカー
というイメージは過去のもの

組織化が急激に進行

サイバー犯罪の犯人達も、様々な立場、思惑があるが・・・

金銭目的

儲かる市場だと理解
組織化・**分業化**が進み
ブラックマーケットが成立

国営スパイ

ハクティビスト

テロ/破壊活動

金銭目的

儲かる市場だと理解
組織化・**分業化**が進み
ブラックマーケットが成立

昔のサイバー犯罪のイメージ

単独犯

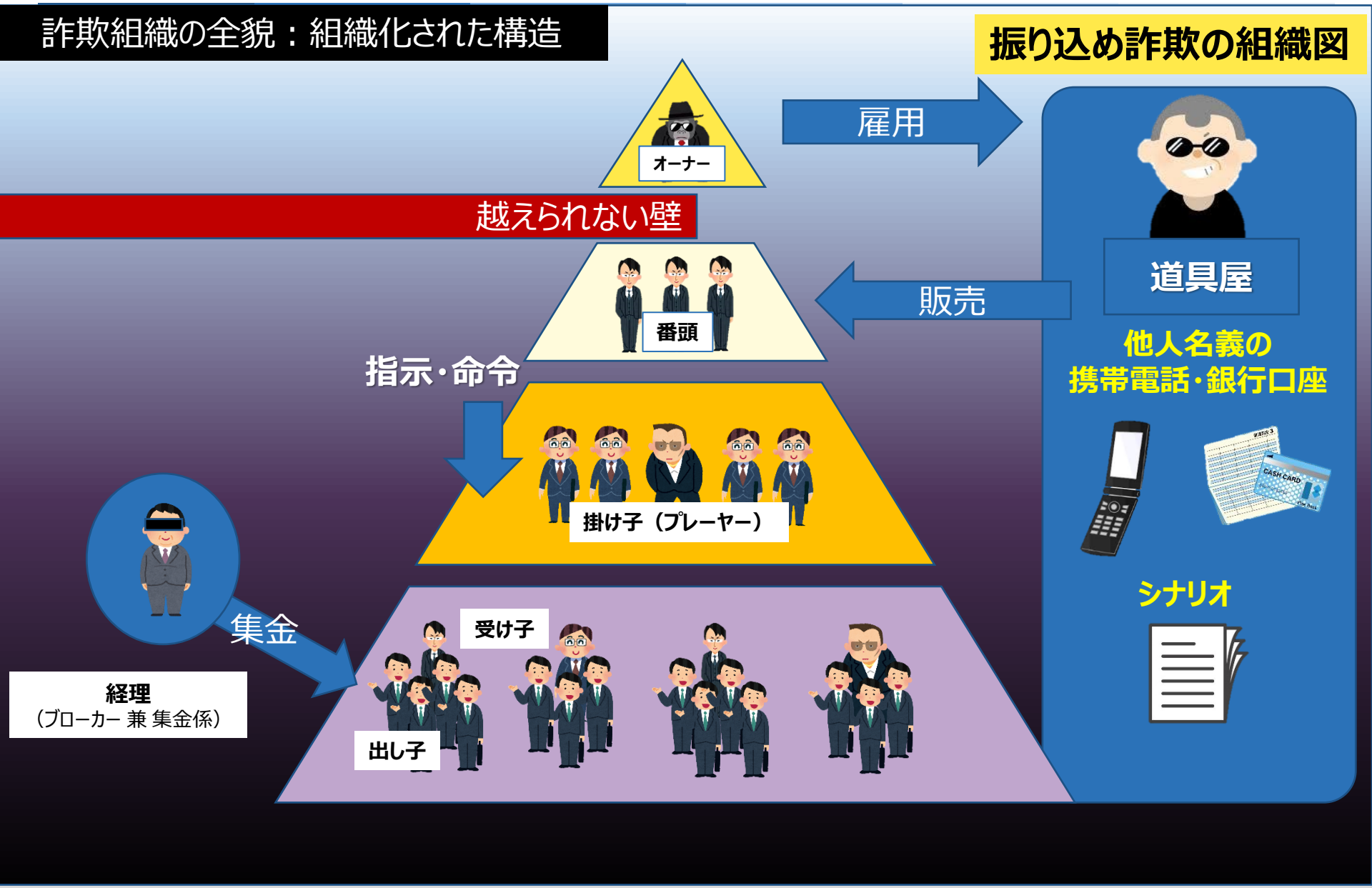
ITやハッキングに関する
専門知識を持った犯罪者
（ブラックハットハッカー）

被害者

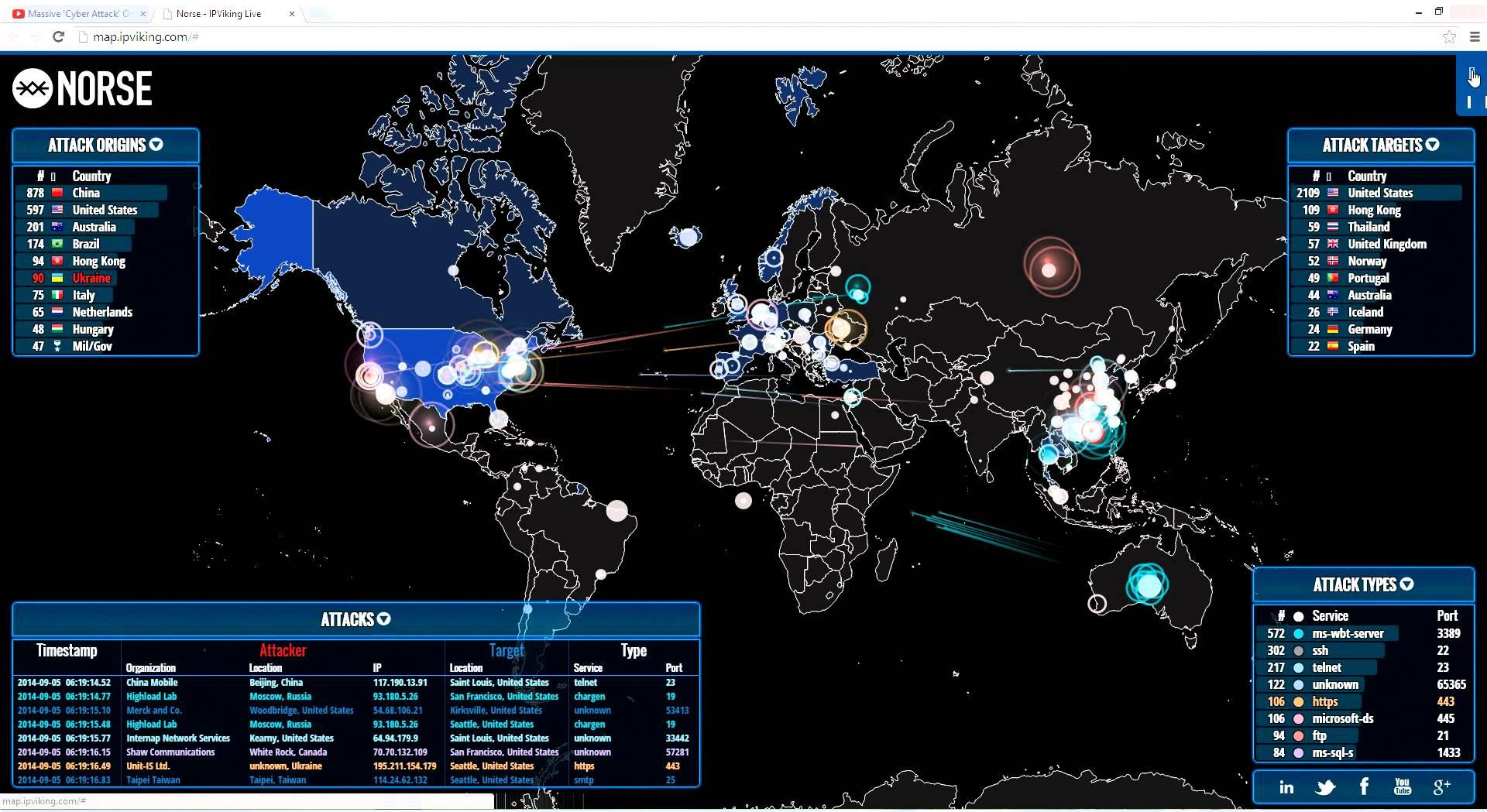
現在では、他の犯罪と同じ構造となっている

GSX
GLOBAL SECURITY EXPERTS

詐欺組織の全貌：組織化された構造



「サイバー攻撃」のような、こういうイメージは誤解を招く



http://map.norsecorp.com/#/

ゲームの話でも
アニメや映画の話でもない

サイバーセキュリティの話とはつまり

GSX
GLOBAL SECURITY EXPERTS

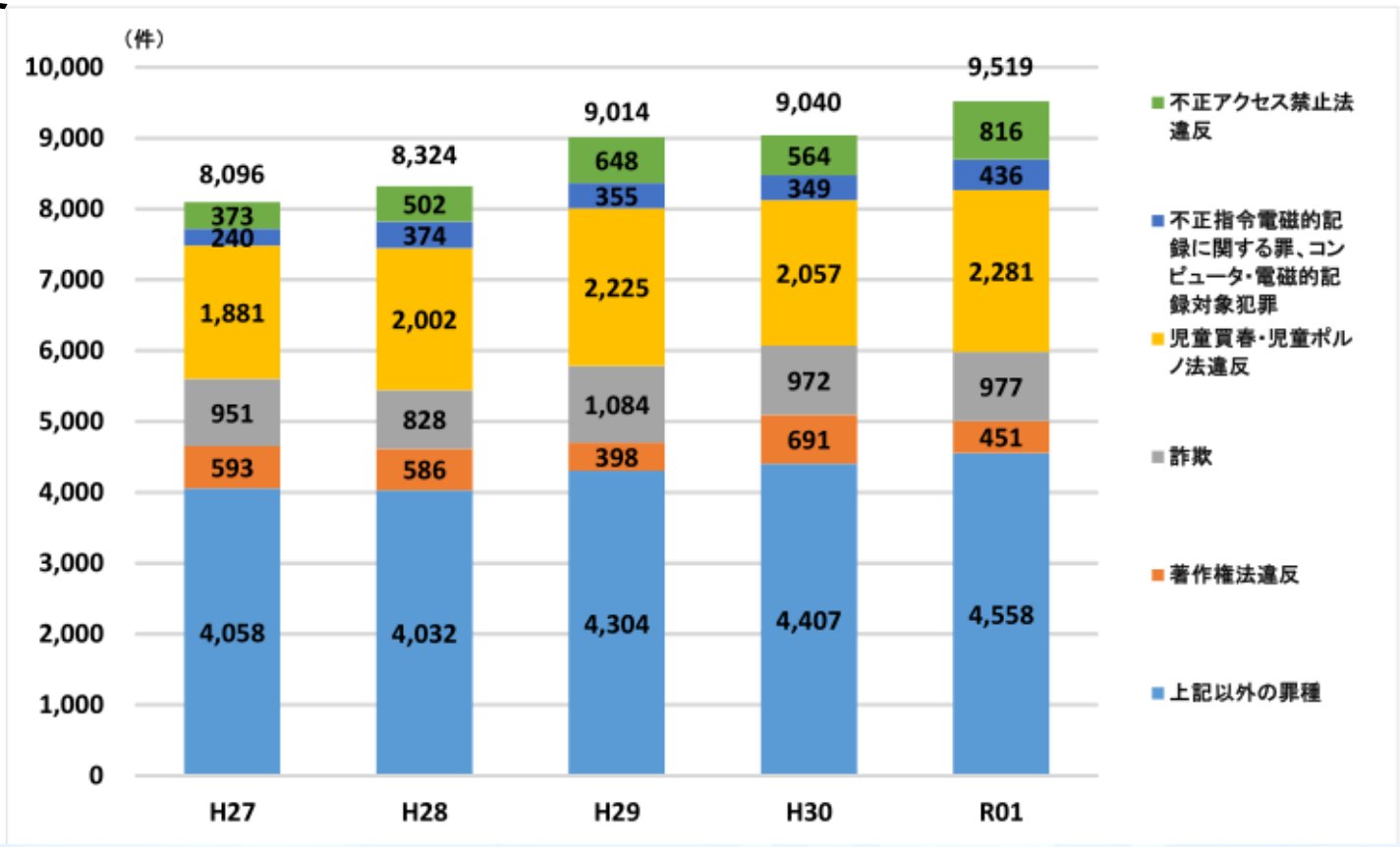
犯罪

の話です

国内でのサイバー犯罪検挙件数: 9,519件

令和元年度

【図表９　サイバー犯罪の検挙件数の推移】



不正アクセスによる犯行：816件　　**ウイルスなどを使った犯行：436件**
ビジネスメール詐欺など　：977件　　**著作権法違反　　：451件**

身の回りでおきる犯罪

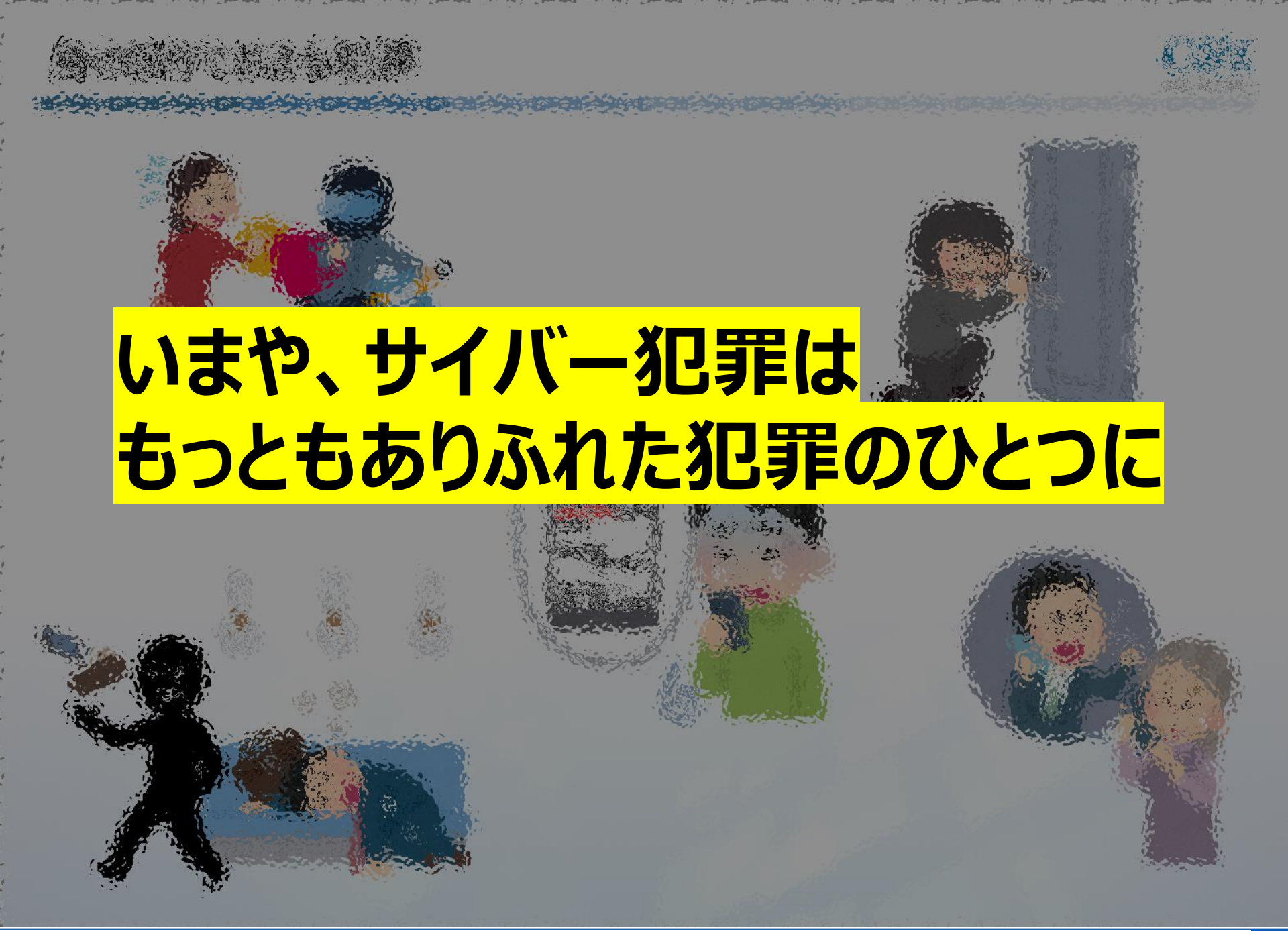
ひったくり

あきす

架空請求

おきびき

オレオレ詐欺

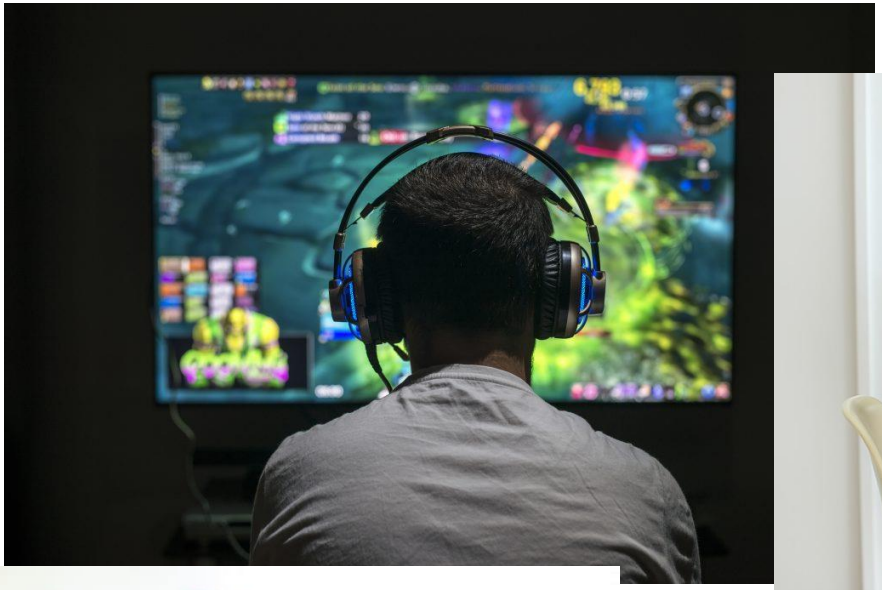


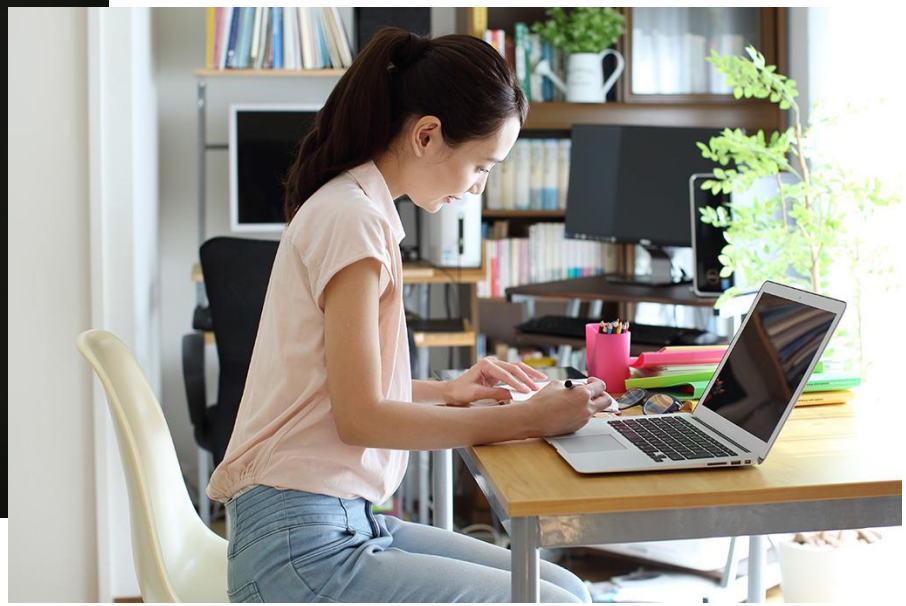
【その２】 被害が増え続ける背景

大きな環境変化で、既存の管理手法が陳腐化

働き方改革が一気に加速

誰が何をしているのか？何を利用しているのか？





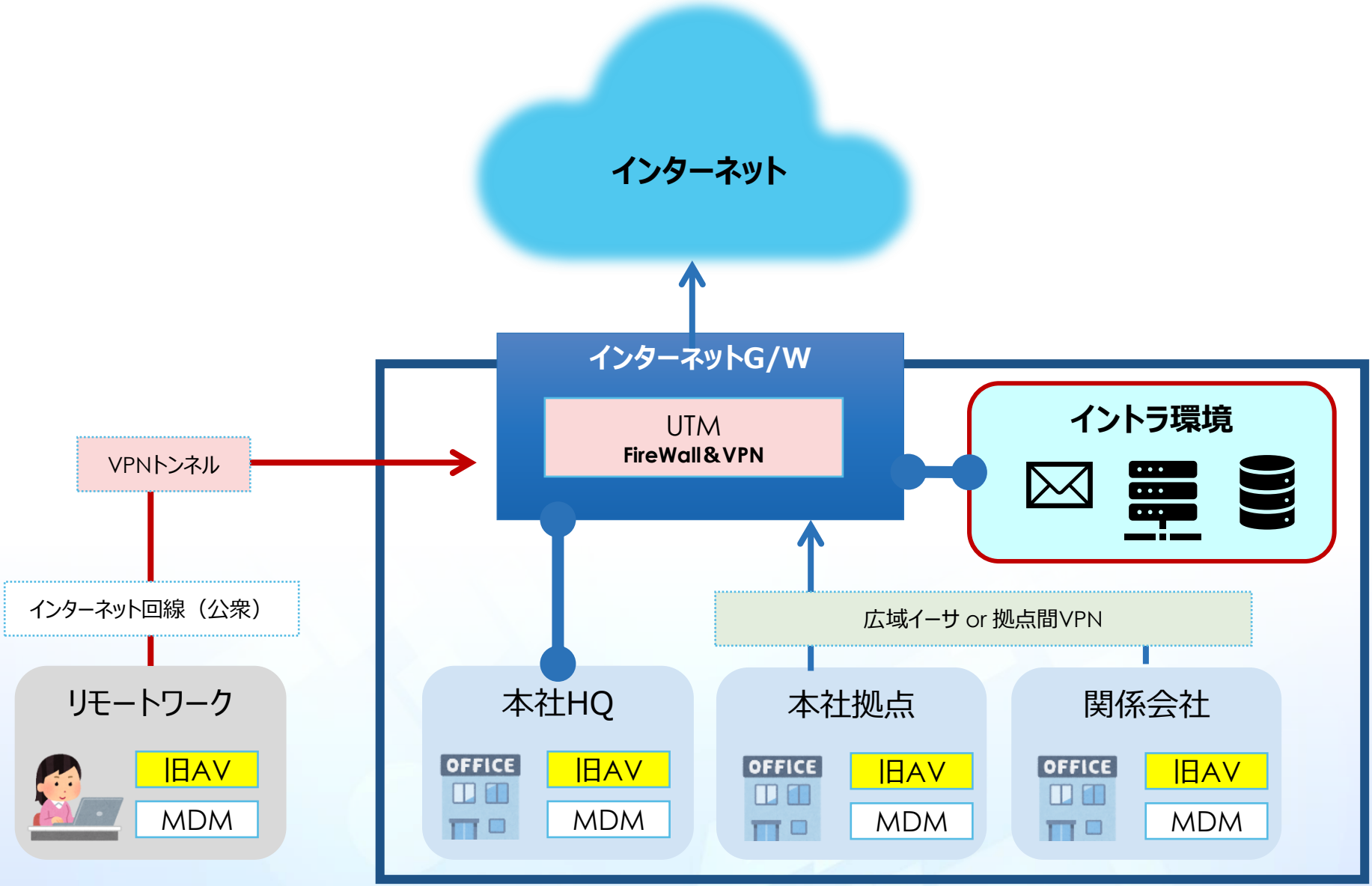
自由に使えるようになる

誰が何をしているのか分からない

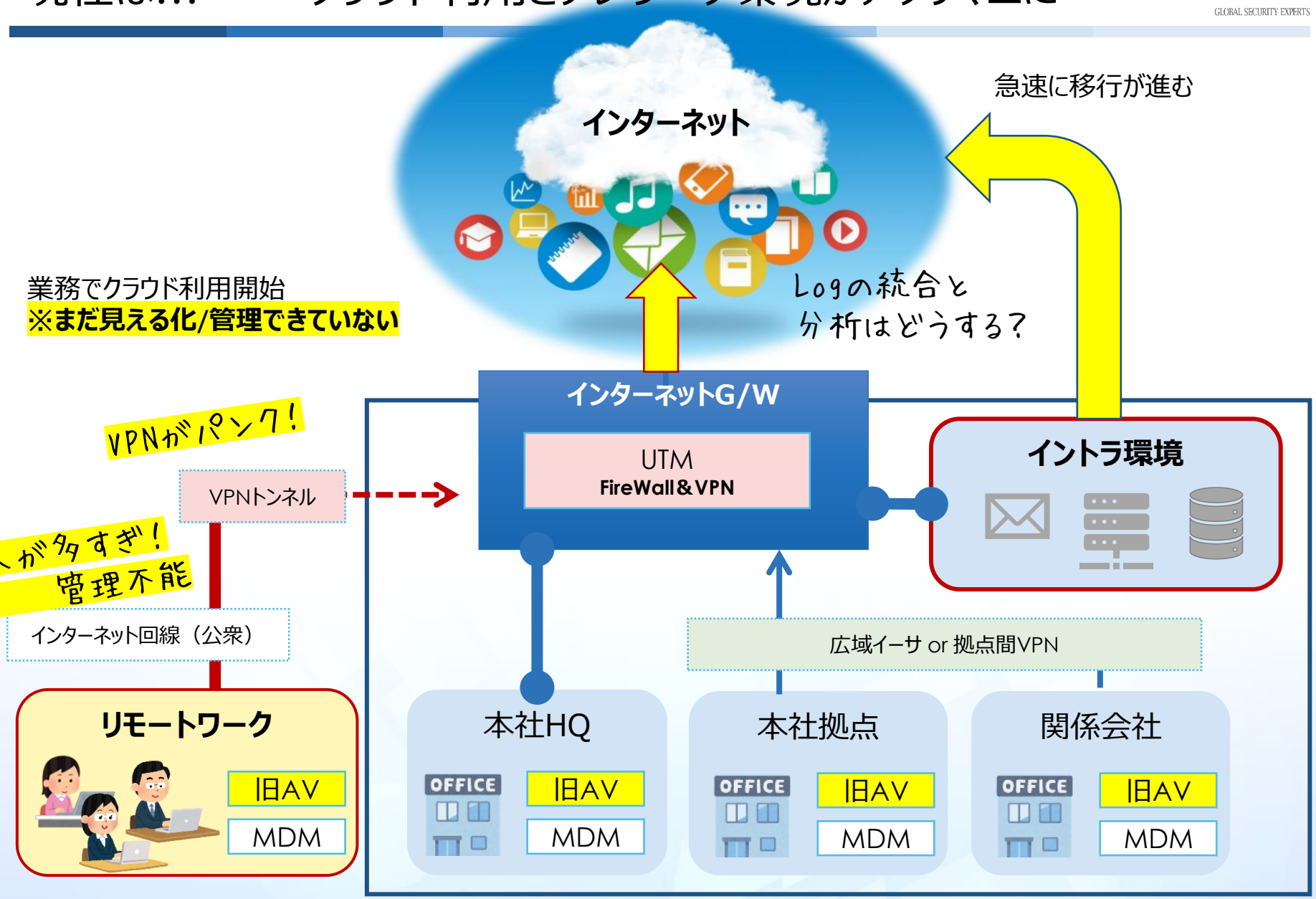
でも…

巨大団地を全部ひとりでチェックできない

昔のネットワーク構成：10年前まではみなこの構成だった

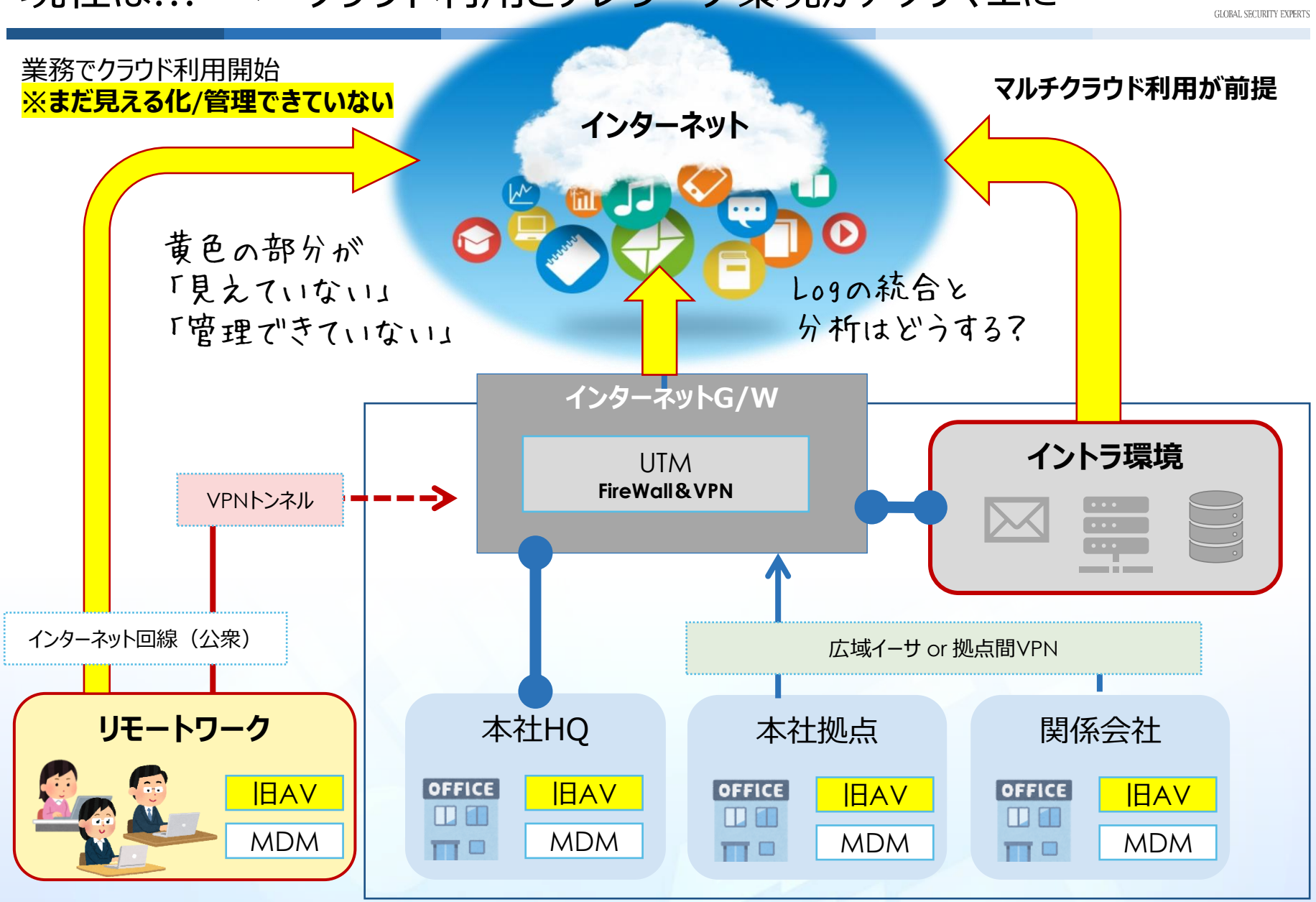


現在は… ⇒ クラウド利用とテレワーク環境がアタリマエに



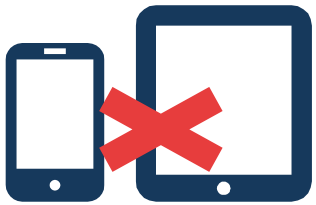
現在は… ⇒ クラウド利用とテレワーク環境がアタリマエに

業務でクラウド利用開始
※まだ見える化/管理できていない



悪いことをする人は 狙っている

被害が拡大している原因（犯人が狙ってくるポイント）

VPN / RDP	標的型攻撃 （端末への感染）	クラウド/Webサービスの認証	クラウドやサーバの管理画面
			

セキュリティ対策は、昔の考え方（境界防御）のままになっている
だからテレワークとクラウド利用を前提とした仕組になっていない
ルールやポリシーも古いまま

ひとことで言えば

犯人のほうが、

- ちゃんと「調べて」
- ちゃんと「リスト化して」
- ちゃんと「連携を取って」
- ちゃんと「PDCAを回して」…

ちゃんと（犯行の）準備している

犯罪の手口を知る

今のサイバー犯罪
多数はみな
「**なりすまし**」である

- 標的型攻撃
- フィッシング
- RAT/トロイ/バックドア
- 不正アクセス
- 不正アプリ
- 不正デバイス
- 不正広告　…etc

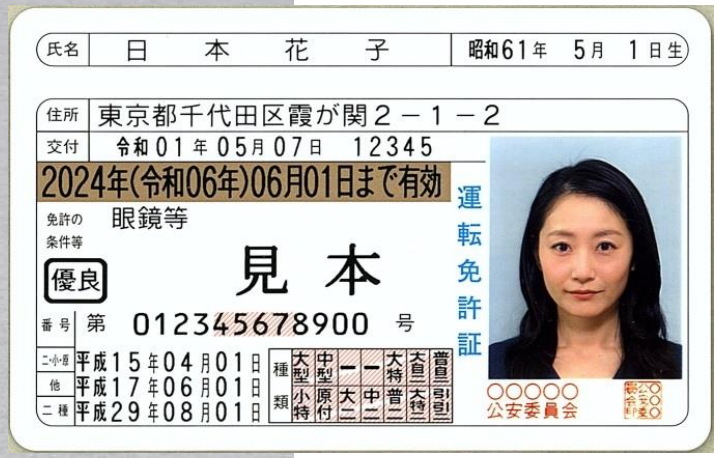
誰かのアカウント、誰かの端末、誰かのページ、誰かのデバイス、誰かのアプリ に

なりすます

なりすましテクニック

どうやって？

手口：身分証と合鍵を買ってくる



どこで？

ダークウェブで

GSX
GLOBAL SECURITY EXPERTS

Filter

- Limit: 15
- Page: 1/9
- Results: 131

Reset filter

Search for..

- + Drugs 5240
- + Counterfeits 260
  - Clothing 40
  - Electronics 22
  - Jewelry 17
  - Cash 21
  - ID´s 131
  - Other 29
- + Jewelry & Gold 17
- + Carding Ware 83
- + Services 898
- + Software & Malware 431
- + Security & Hosting 31
- + Fraud 877
- + Digital goods 1340
- + Guides & Tutorials 1332

Top vendors

ladyskywalker (759) L12
foggyperson (1133) L11

Filter

Sort Popularity - 1 week descending Send

Products

ID TEMPLATES FULL PACK || COMPLETE

4.72

TheShop (216)
4.42 Level 3 Trusted

From **$9.99**/Piece
Ships from: XX
Ships Worldwide
Multisig Escrow First
Auto-Accept

Go to Offer

Custom British Drive r License Scan, Any Details

0

homodei
0 Level 1 Trusted

From **10,00€**/Piece
Ships from: US
Ships Worldwide
Multisig
Auto-Accept

Go to Offer

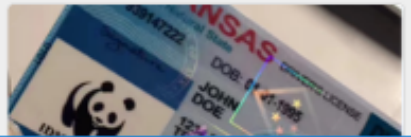
(BEST WORK) South Carolina Fake ID driv ers licence

5

idmaster21 (8)
5 Level 3

From **$70.00**/Piece
Ships from: HK
Ships Worldwide
Escrow
Auto-Accept

Go to Offer



【実例】ダークウェブ

企業から盗んだIDパスワードをリストにして販売している

DATABASE	PRICE	Category	RECORDS
ShareThis	$3,800	Web Plugin	1,900,000
500px	$2,800	Photography	206,000
Houzz	$4,500	Lifestyle	3,400,000
MyFitnessPal	$3,800	Lifestyle	50,000,000
MyHeritage	$3,200	Lifestyle	65,700,000
Dubsmash	$4,500	Entertainment App	15,500,000
YouNow	$3,200	Entertainment App	40,000,000
Armor Games	$900	Entertainment	7,800,000
Wanelo	$3,800	ecommerce	2,900,000

なぜ？
仕入元は？

【30億件】前代未聞の個人情報漏洩：米ヤフー

GSX
GLOBAL SECURITY EXPERTS

産経ニュース 東京 18℃ 産経WEST iRONNA フォト Powered by popIn 検索

ホーム 速報 スポーツ パラスポーツ エンタメ ライフ 地方 大河原邦男展 JAPAN Forward
社会 政治 国際 経済 コラム 東京五輪 GQ WIRED 特集 写真 ランキング 主張 産経抄
中国・台湾 朝鮮半島 アジア 米州 欧州・ロシア 中東・アフリカ 国際問題

2017.10.4 06:46

文字の大きさ 小 中 大 印刷

米ヤフー、３０億件情報流出　全利用者が被害、過去最大規模、不正侵入か

ツイート 反応 シェア 0 G+ プッシュ通知

米検索大手ヤフーの全利用者が作成した**約３０億件のアカウント**に関連する個人情報が流出していたことが３日、分かった。米メディアによると、個人情報流出では過去最大規模となる。ヤフーの中核事業を６月に買収した米通信大手ベライゾン・コミュニケーションズが発表した。２０１３年８月にヤフーのネットワークに不正侵入した第三者によって盗まれたとみている。

米メディアによると、流出した情報には利用者の氏名や電話番号、生年月日などが含まれている。利用者にはパスワードの変更などを呼び掛けている。クレジットカードや銀行口座の情報は含まれないという。

史上最大規模、30億件もの個人情報が盗難

マリオットではカード番号を含む5億人のお客様ID情報が盗難

［３０日　ロイター］ - ホテル世界最大手の米マリオット・インターナショナル(MAR.O)は３０日、**「シェラトン」**や**「リッツ・カールトン」**などのホテルを展開する傘下スターウッド・ホテルズの予約データベースがハッカー攻撃を受け、

約５億人の顧客情報が盗まれた可能性があると発表した。

今回の個人情報流出は、２０１３年に起きたヤフーの３０億アカウントの情報流出に次いで、

過去２番目の規模となる見通し。

マリオットによると、３億２７００万人の顧客については、パスポートや電話番号、電子メールアドレスなどの情報が流出した恐れがある。一部の顧客については、クレジットカード番号が流出した情報に含まれる可能性があるという。

日本人のID・パスワードが大量盗まれ、売られている

HOME | 脅威 | 脆弱性 | 情報漏えい | インシデント | 不正アクセス | 報告書 | 講演 | 業界

› 個人情報漏えい › 個人情報漏えい › IDが攻撃 » ASCIIアクセス

› インシデント・事故 › インシデント・情報漏えい › 記事

インシデント・事故 ／ インシデント・情報漏えい　2019年5月30日（木） 08時05分

最大37,832名のカード情報流出、新規カード登録停止は不正アクセス疑義判明から10日後（ヤマダ電機）

株式会社ヤマダ電機は6月29日、同社が運営する「ヤマダウエブコム・ヤマダモール」にて第三者からの不正アクセスを受け、カードの情報が流出した可能性が4月16日に判明したと発表した。

株式会社ヤマダ電機は6月29日、同社が運営する「ヤマダウエブコム・ヤマダモール」にて第三者からの不正アクセスを受け、カードの情報が流出した可能性が4月16日に判明したと発表した。

これは第三者から同サイトに不正アクセスを受け、ペイメントアプリケーションの改ざんが行われたというもので、クレジットカード情報が最大37,832件流出した可能性がある。

同社では4月16日に不正アクセスの可能性が判明後、調査を経て4月26日時点で同サイトでの新規クレジットカード登録とクレジットカード登録の変更を停止し、第三者調査機関「P.C.F.FRONTEO株式会社」による調査を開始した。

トップページ

リリース（弊社が運営する「ヤマダウエブコム・ヤマダモール」への不正アクセスによる個人情報流出に関するお詫びとお知らせ）

リリース（情報公開について）

リリース（再発防止策ならびに弊社が運営するサイトの再開について）

シェア　ツイート

「プレミアム・アウトレット」からの流出データ、5カ所で公開を確認

三菱地所・サイモンは、同社が運営する「プレミアム・アウトレット」の顧客情報が流出した問題で調査結果を明らかにした。「SQLインジェクション」が原因で、流出した情報が少なくとも5カ所で公開されていることが確認されたという。

同社では、メールマガジン「ショッパークラブ」を購読する一部会員のメールアドレスやログインパスワードが、外部に流出した可能性があることを4月7日に公表。外部事業者による調査を進めていた。

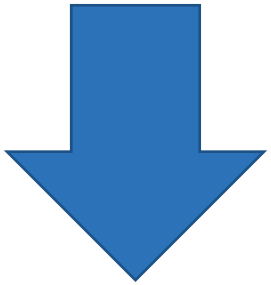
臨時ページで注意喚起を行っているプレミアム・アウトレット

調査結果によると、不正アクセスは、2017年5月から2018年1月にかけて、国内外より複数回にわたり行われたという。ウェブアプリケーションのSQLインジェクションの脆弱性を突かれたことが原因で、情報漏洩が発生した。

その結果・・・

個人情報…値がつくのはむしろ「**アカウント情報**」

住所・氏名・年齢・電話番号



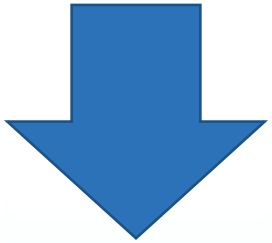
メアド・ID・パスワード・カード番号

だから
簡単に
なりすませる

合鍵を使って侵入 「パスワードリスト型攻撃」

パスワード使いまわしは自殺行為！

盗まれた「パスワード」が闇市場（ダークウェブ）で販売される



同じパスワードのサイトも侵入される

パスワードリストに加えて、弱いパスワードも

“弱いパスワード” も 当然狙われ、被害に遭っている

総当たり攻撃
（ブルートフォース）

ID固定		PW変更
username	+	0000
username	+	0001
username	+	0002
username	+	0003
.....	+	.....

不正ログイン

逆総当たり攻撃
（リバースブルートフォース）

ID変更		PW固定
username	+	1234
admin	+	1234
user01	+	1234
sato123	+	1234
.....	+	.....

アカウントリストを使った不正アクセスは枚挙に暇がない

インシデント・事故 › インシデント・情報漏えい › 記事

インシデント・事故／インシデント・情報漏えい　2018年8月16日（木） 08時15分

dアカウントへの不正ログインで商品購入を確認、防止のため2段階認証の利用を呼びかけ（NTTドコモ）

株式会社NTTドコモは8月14日、不正に取得したdアカウントを使いドコモオンラインショップで商品購入する事象が確認されたと発表した。

これは外部の第三者が、不正に取得したdアカウントを使い、ドコモオンラインショップへ不正ログインし同ショップで商品を購入する事象が確認されたというもの。

同社では、第三者によるdアカウントへの不正ログインを防止するために2段階認証を利用するよう呼びかけている。

またユーザーが2段階認証を「利用しない」に設定している場合でも、同社の判断によりユーザーの端末に送信されるセキュリティコードの入力を求める場合があるとのこと。

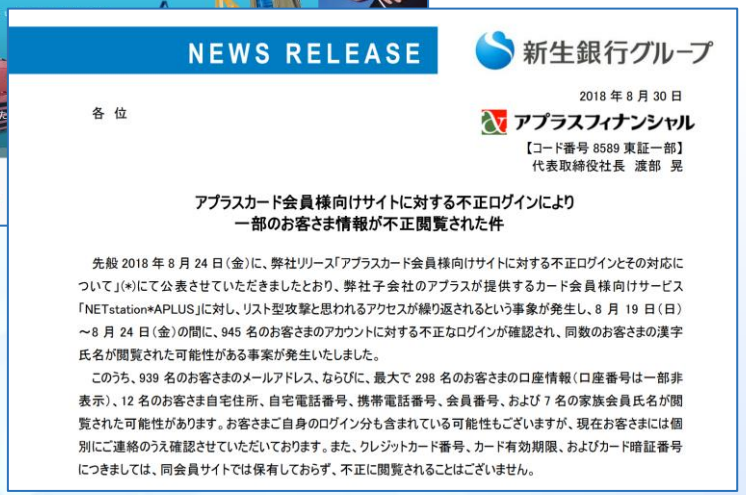
トップページ

リリース（不正なアクセス対策としての「2段階認証」ご利用のお願い）

リリース（2段階認証とは？）

シェア

もっと「顧客情報い」のニュース



NEWS RELEASE

新生銀行グループ

2018 年 8 月 30 日

各 位

アプラスフィナンシャル

【コード番号 8589 東証一部】

代表取締役社長　渡部　晃

アプラスカード会員様向けサイトに対する不正ログインにより一部のお客さま情報が不正閲覧された件

先般 2018 年 8 月 24 日（金）に、弊社リリース「アプラスカード会員様向けサイトに対する不正ログインとその対応について」(*)にて公表させていただきましたとおり、弊社子会社のアプラスが提供するカード会員様向けサービス「NETstation*APLUS」に対し、リスト型攻撃と思われるアクセスが繰り返されるという事象が発生し、8 月 19 日（日）～8 月 24 日（金）の間に、945 名のお客さまのアカウントに対する不正なログインが確認され、同数のお客さまの漢字氏名が閲覧された可能性がある事案が発生いたしました。

このうち、939 名のお客さまのメールアドレス、ならびに、最大で 298 名のお客さまの口座情報（口座番号は一部非表示）、12 名のお客さま自宅住所、自宅電話番号、携帯電話番号、会員番号、および 7 名の家族会員氏名が閲覧された可能性があります。お客さまご自身のログイン分も含まれている可能性もございますが、現在お客さまには個別にご連絡のうえ確認させていただいております。また、クレジットカード番号、カード有効期限、およびカード暗証番号につきましては、同会員サイトでは保有しておらず、不正に閲覧されることはございません。

もはや「IDパスワードは漏洩するもの」として管理する必要がある

⇒　使い回しはリスクが高すぎる

これだけリスト攻撃が増えると多要素認証はもはや必須

セブンペイは 僅か1ヶ月でサービス廃止に

Business Insider Japan 2019年8月2日 報道 より

企業のVPNや、イントラなどでも同様の被害が多発

テレワークを狙ったサイバー攻撃：狙われるポイント①

VPN

RDP

クラウド/Web
ログイン

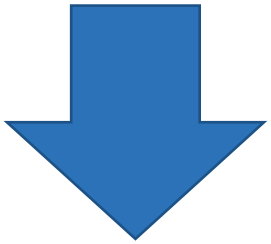
大きな被害が多発

この事例でのポイント

- 他者が管理している「IDパスワード」は**漏洩する前提**で考える
- **「パスフレーズ」**と**「多要素認証」**を必ず利用する
- 多要素認証は「所持情報」（SMSやAuthenticator）を使うと手軽

多要素認証の例

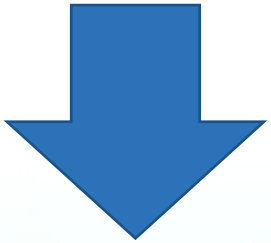
多要素認証は必ずONに！



- 万が一、漏洩しても「犯人のログイン試行が分かる」
- 自分が持っている「端末やPINが盗まれない限り安全」

パスワードを覚えていられない！？

自分だけの「パターン」を作ってしまおう



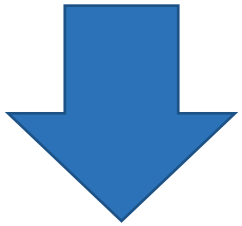
たとえば…

クルマの名前＋サービス名＋ペットの名前

（例）Roadster ni notta amazon to torafure

犯罪の手口を知る

詐欺（騙して端末に感染）



みなさんの端末に対する

標的型攻撃

テレワークを狙った攻撃メールが起点となり被害多数

GSX
GLOBAL SECURITY EXPERTS

Web会議への招待メールを偽装

送信者：会議システム<telework@xxx.net>
件名　：会議連絡

以下の時間に会議が設定されました。

テレワーク会議システムに参加する。
http://teleworkmeeting.xxx.net/i.php?fff=xxxxx

ミーティングNo：1455 5775 8695
パスワード：754935

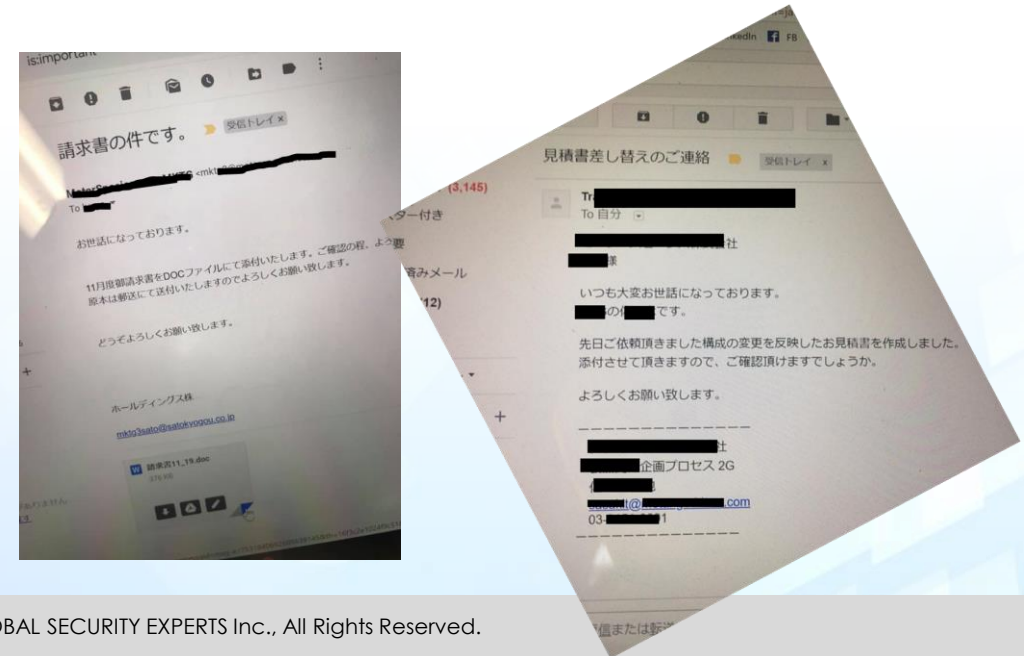
テレワーク手当の申請通知を偽装

送信者：管理部<kanri@xxx.net>
件名　：テレワーク手当について

社員各位

一部の社員から問い合わせを多く受けておりますので、再度周知いたします。
まだ申請していない方は、ご連絡ください。

テレワーク手当の申請ページは以下です。
http://mask.office-all.net/i.php?fff=xxxxx



既に実被害が発生

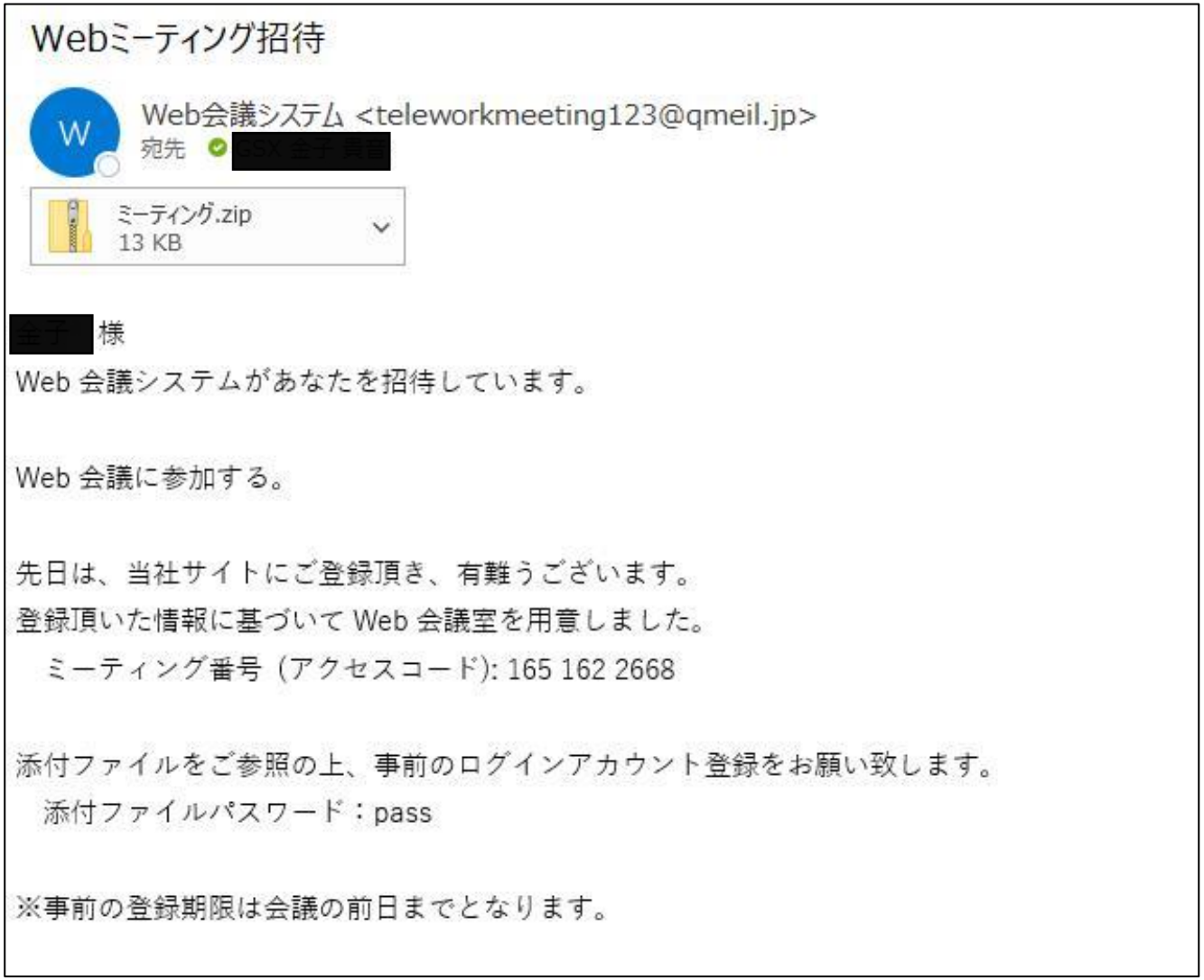
怪しまれないようにしてくる

スーツ姿で名刺を持って、堂々と入ってくるような状況

受付にガードマンはいるが、アポイント管理はやっていない（各社まかせ）

標的型メールから
大きな被害に
標的型攻撃の実例

冒頭ご紹介した事例：疑いのあるメールが届いた



Webミーティング招待

W

Web会議システム <teleworkmeeting123@qmeil.jp>

宛先 [redacted]

ミーティング.zip
13 KB

[redacted] 様

Web 会議システムがあなたを招待しています。

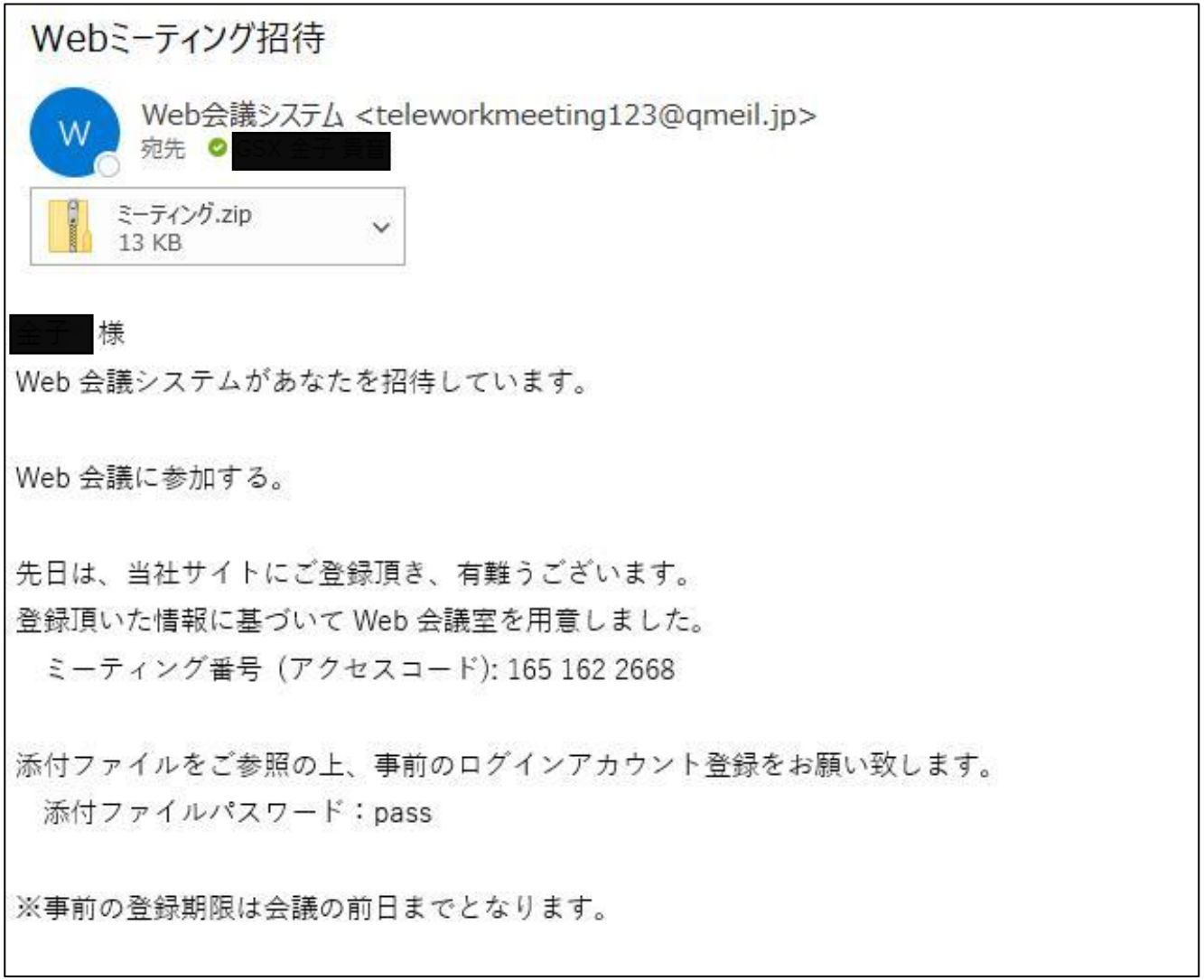
Web 会議に参加する。

先日は、当社サイトにご登録頂き、有難うございます。
登録頂いた情報に基づいて Web 会議室を用意しました。
　ミーティング番号（アクセスコード): 165 162 2668

添付ファイルをご参照の上、事前のログインアカウント登録をお願い致します。
　添付ファイルパスワード：pass

※事前の登録期限は会議の前日までとなります。

確認すべきポイントは？



Webミーティング招待

W

Web会議システム <teleworkmeeting123@qmeil.jp>

宛先 [redacted]

ミーティング.zip
13 KB

[redacted] 様

Web 会議システムがあなたを招待しています。

Web 会議に参加する。

先日は、当社サイトにご登録頂き、有難うございます。
登録頂いた情報に基づいて Web 会議室を用意しました。
　ミーティング番号（アクセスコード): 165 162 2668

添付ファイルをご参照の上、事前のログインアカウント登録をお願い致します。
　添付ファイルパスワード：pass

※事前の登録期限は会議の前日までとなります。

確認すべきポイントは？

Webミーティング招待

Web会議システム <teleworkmeeting123@qmeil.jp>
宛先 [redacted]

ミーティング.zip
13 KB

[redacted] 様

Web 会議システムがあなたを招待しています。

Web 会議に参加する。

先日は、当社サイトにご登録頂き、有難うございます。
登録頂いた情報に基づいて Web 会議室を用意しました。
ミーティング番号（アクセスコード): 165 162 2668

添付ファイルをご参照の上、事前のログインアカウント登録をお願い致します。
添付ファイルパスワード：pass

※事前の登録期限は会議の前日までとなります。

①よくみると
Qmail.jpになっている

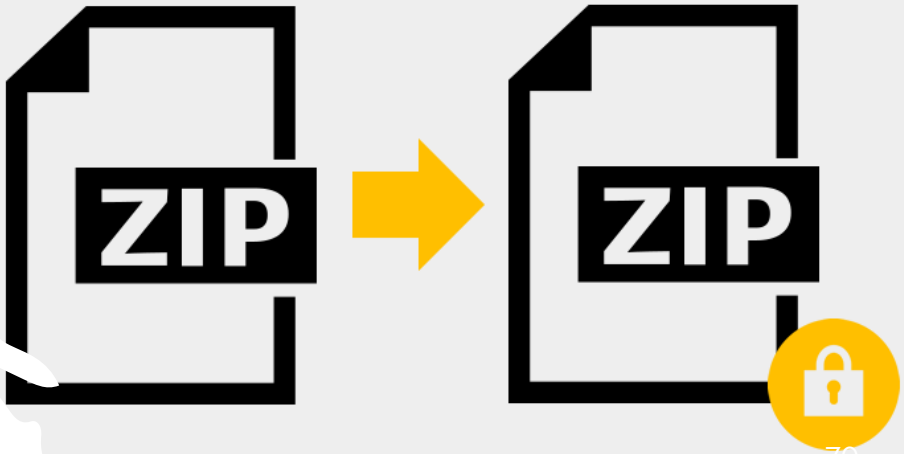
②何となく違和感のあるメール文面
サービス名も書いていない

③会議日程等がなにも書いていない

④パスワード付ZIPファイル添付

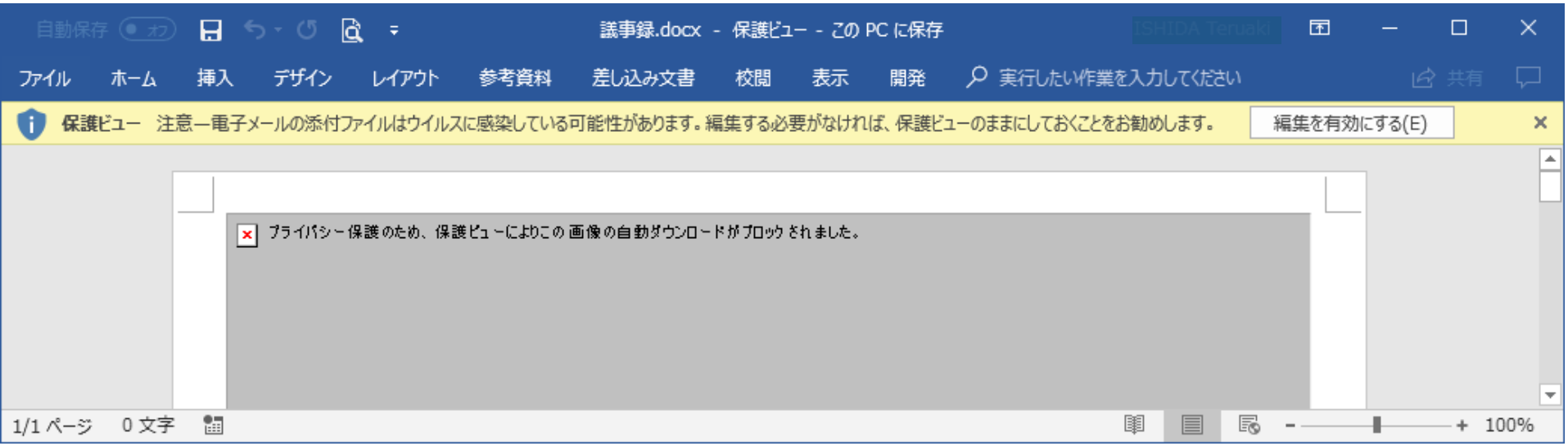
パスワード付き添付を使った犯行手口

- １．検知に引っかからない
- ２．習慣的に開いてしまう



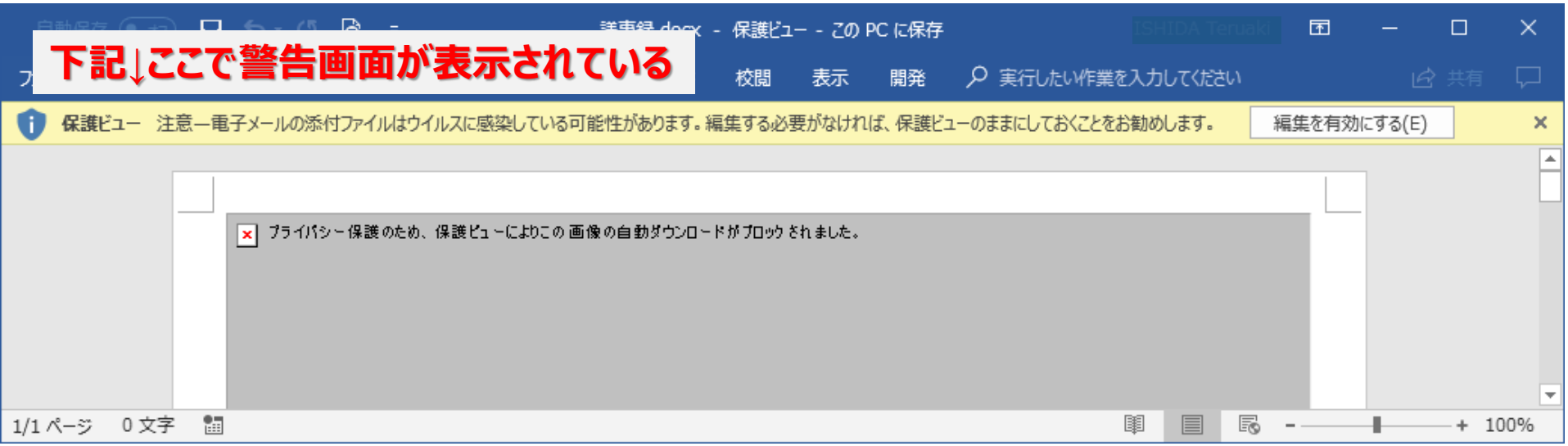
犯行に使われたメールの再現

メールに添付されたZipファイルを解凍し、Wordファイルを開くと、「保護ビュー」状態で表示される



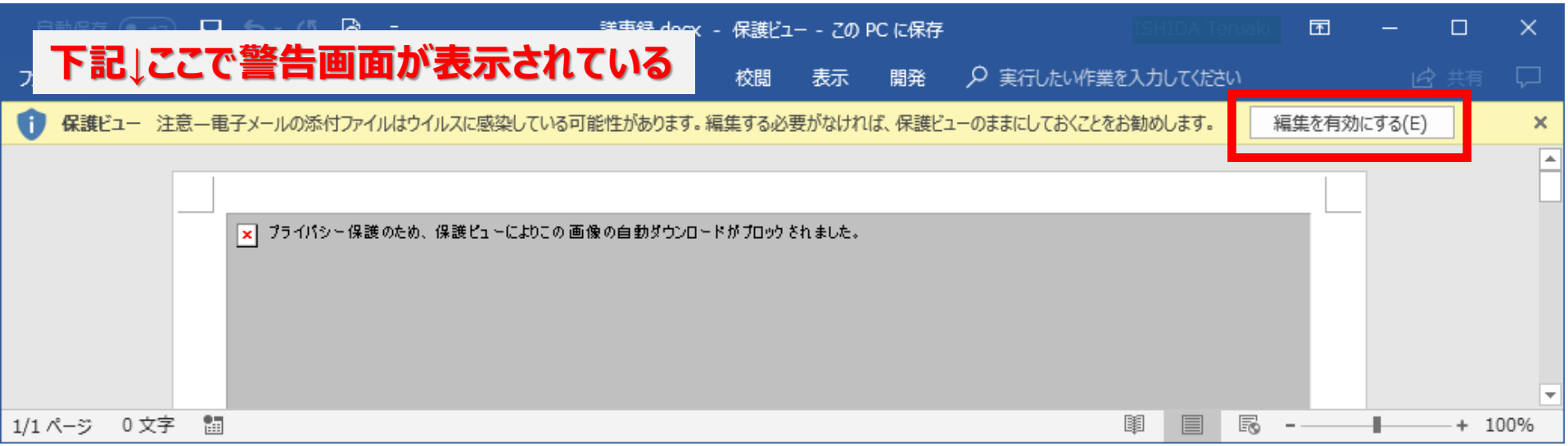
犯行に使われたメールの再現

メールに添付されたZipファイルを解凍し、Wordファイルを開くと、「保護ビュー」状態で表示される



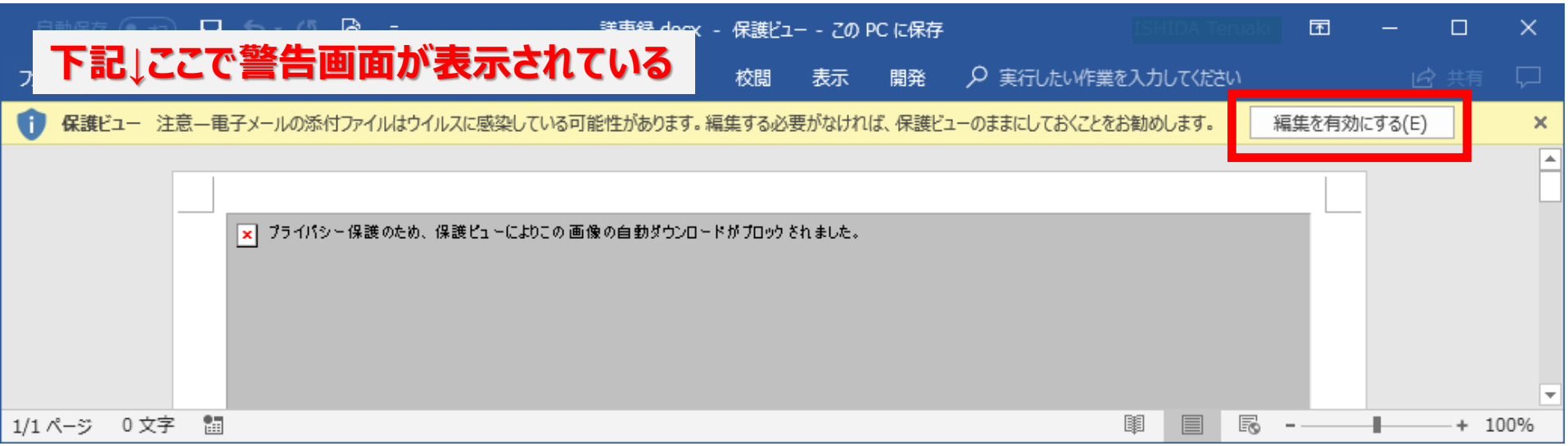
犯行に使われたメールの再現

メールに添付されたZipファイルを解凍し、Wordファイルを開くと、「保護ビュー」状態で表示される



犯行に使われたメールの再現

メールに添付されたZipファイルを解凍し、Wordファイルを開くと、「保護ビュー」状態で表示される



解凍した勢いで、そのまま「有効にする」ボタンを押してしまう人が多い

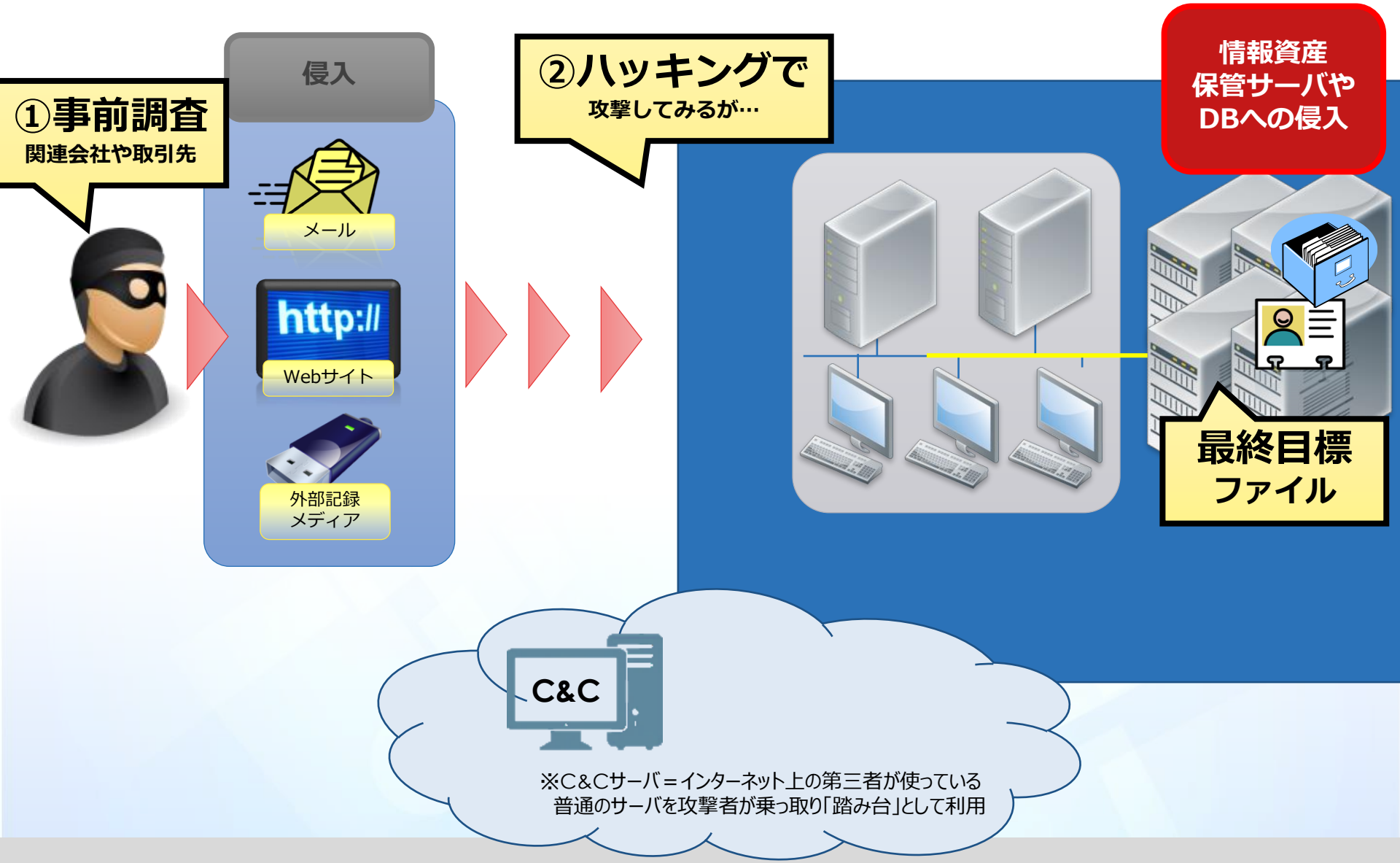
マクロを悪用して感染する

まさに詐欺の手口

ウィルスを使って犯人は何をする？

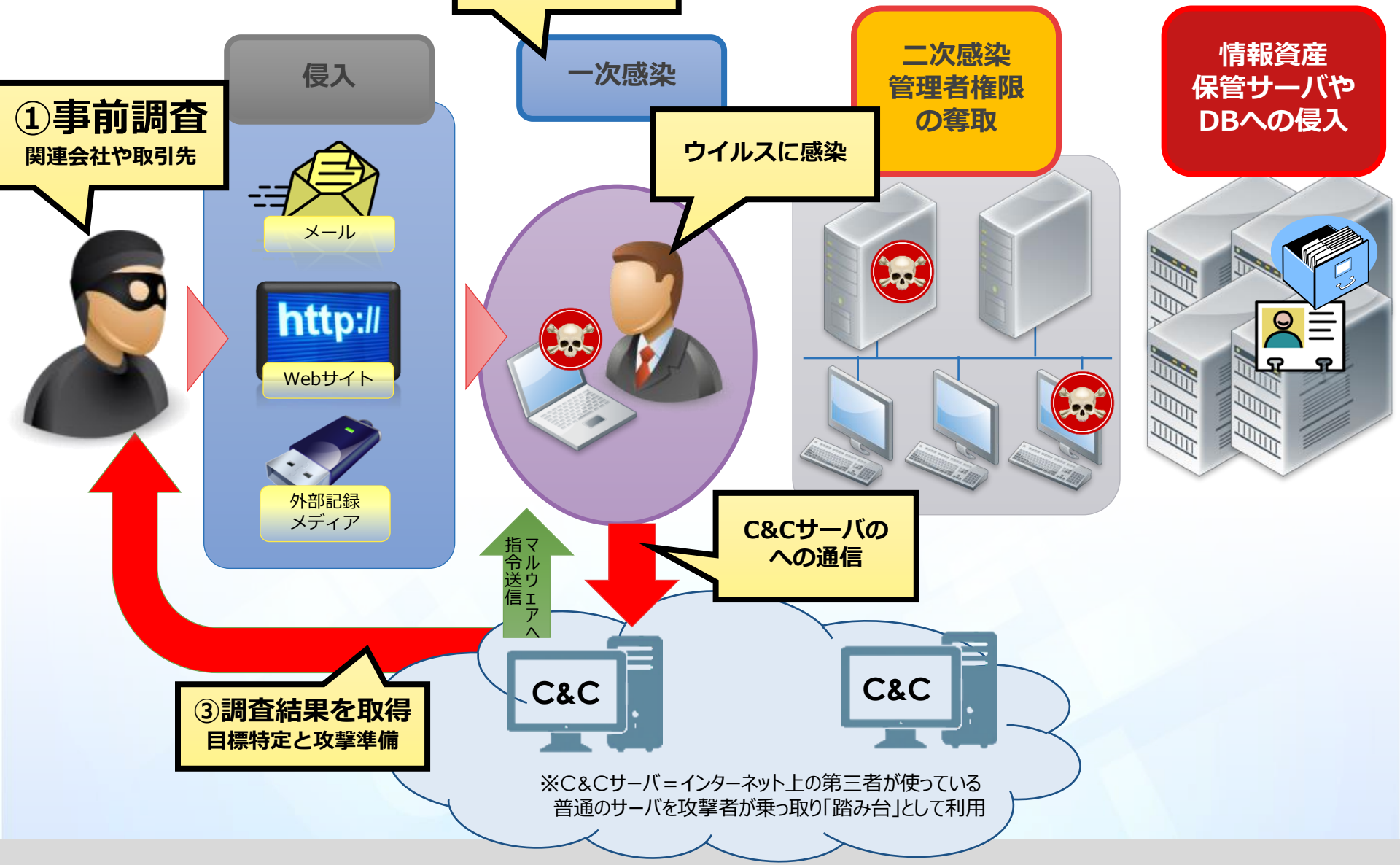
しっかり守りを固めた企業システムには簡単に侵入できない

GSX
GLOBAL SECURITY EXPERTS



だから皆さんを狙う！

GSX
GLOBAL SECURITY EXPERTS



だから皆さんを狙う！

GSX
GLOBAL SECURITY EXPERTS

①事前調査
関連会社や取引先

侵入

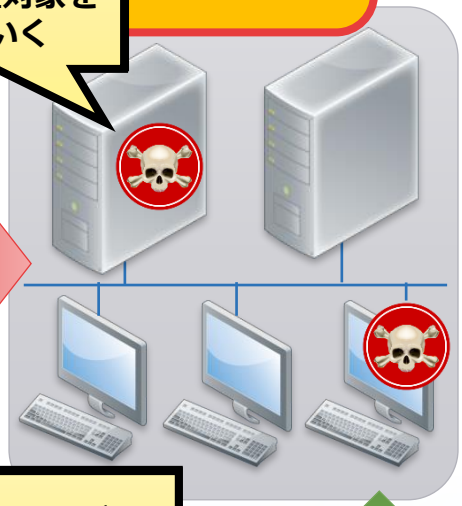
②内部調査
ウイルスによる

一次感染

取得した情報で
新たに調査対象を
広げていく

④攻撃基盤
を構築する

二次感染
管理者権限
の奪取



情報資産
保管サーバや
DBへの侵入

⑤最終目標
ファイル作成

C&Cサーバへ
調査結果送信

マルウェアへ指令送信

マルウェアへ指令送信

⑥情報漏洩

送信

⑦奪取成功

③調査結果を取得
目標特定と攻撃準備

※C&Cサーバ＝インターネット上の第三者が使っている
普通のサーバを攻撃者が乗っ取り「踏み台」として利用

テレワークを狙ったサイバー攻撃：狙われるポイント②

組織としての

防犯意識の無さ

端末の

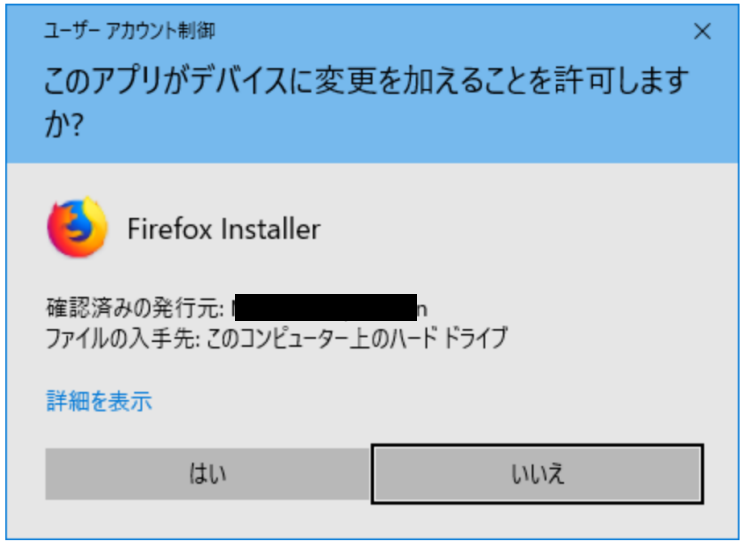
挙動が見えていない

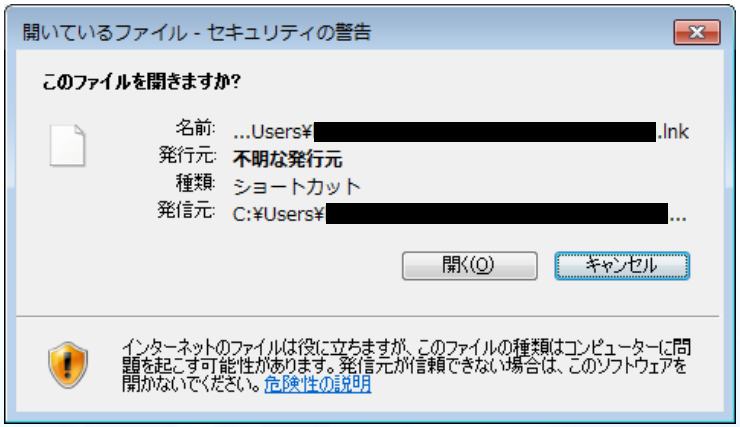
おやっ？と思う心が、詐欺の被害を防ぐ！

1．いつもと文面の印象が違った
2．突然重要な連絡が来た
3．端末の動きがおかしくなった
4．返信したのにエラーで返ってきた
5．当の本人がそのメールを知らなかった

あれっ？　と思ったらすぐに相談！

警告画面が表示された場合、いったん「止まって」考えましょう！





ちょっとでも
「あれ？」
と思ったら注意する！

声を掛け合い、情報を共有することで詐欺の被害を防ぐ

被害者に罪は無い

必要なのは

犯行を見逃さない事！

悪いのは犯人：**事後報告**でも、**しっかり報告しよう**！

体験すれば、本当に理解できる

犯罪に「自分が巻き込まれる」体験をすることで、「自分ごと」として意識できるように

だから、防犯訓練や防災訓練のように、実体験することが重要

GSX
GLOBAL SECURITY EXPERTS

着弾中

ふだんの仕事中だと気づかない！

あれー？
添付ファイル間違えて送ってきたのか？
まぁいいか。。。

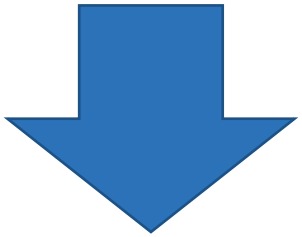
感染

※写真はイメージです

気づかずに仕事してしまう！

これが怖い

気づかずに仕事してしまう！



そして、1ヶ月後には…

1ヶ月後には。。。

感染拡大

※写真はイメージです

警察も「手口の啓蒙」を進めて被害を食い止めた

GSX
GLOBAL SECURITY EXPERTS

警察庁・SOS47
特殊詐欺対策ページ

HOME | SOS47の活動 | 特殊詐欺の手口と対策 | 特殊詐欺 発生状況 | ムービー | ダウンロード | 防犯マンガ | 防犯力チェック

オレオレ詐欺

親族、警察官、弁護士等を装い、親族が起こした事件・事故に対する示談金等を名目に金銭等をだまし取る（脅し取る）手口です。

詳細を見る ›

預貯金詐欺

親族、警察官、銀行協会職員等を装い、あなたの口座が犯罪に利用されており、「キャッシュカードの交換手続きが必要である」などの名目で、キャッシュカード、クレジットカード、預貯金通帳等をだまし取る（脅し取る）手口です。

詳細を見る ›

キャッシュカード詐欺盗

警察官や銀行協会、大手百貨店等の職員を装って被害者に電話をかけ、「キャッシュカードが不正に利用されている」などの名目により、キャッシュカードを準備させた上で、隙を見るなどし、キャッシュカード等を窃取する手口です。

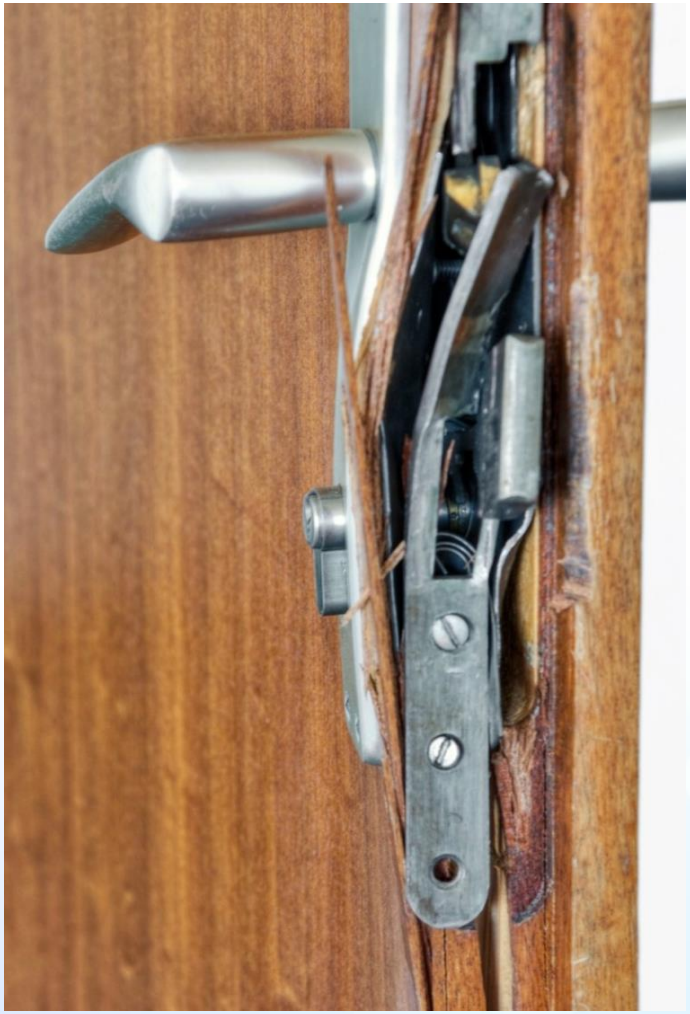
詳細を見る ›

特殊詐欺の手口と対策

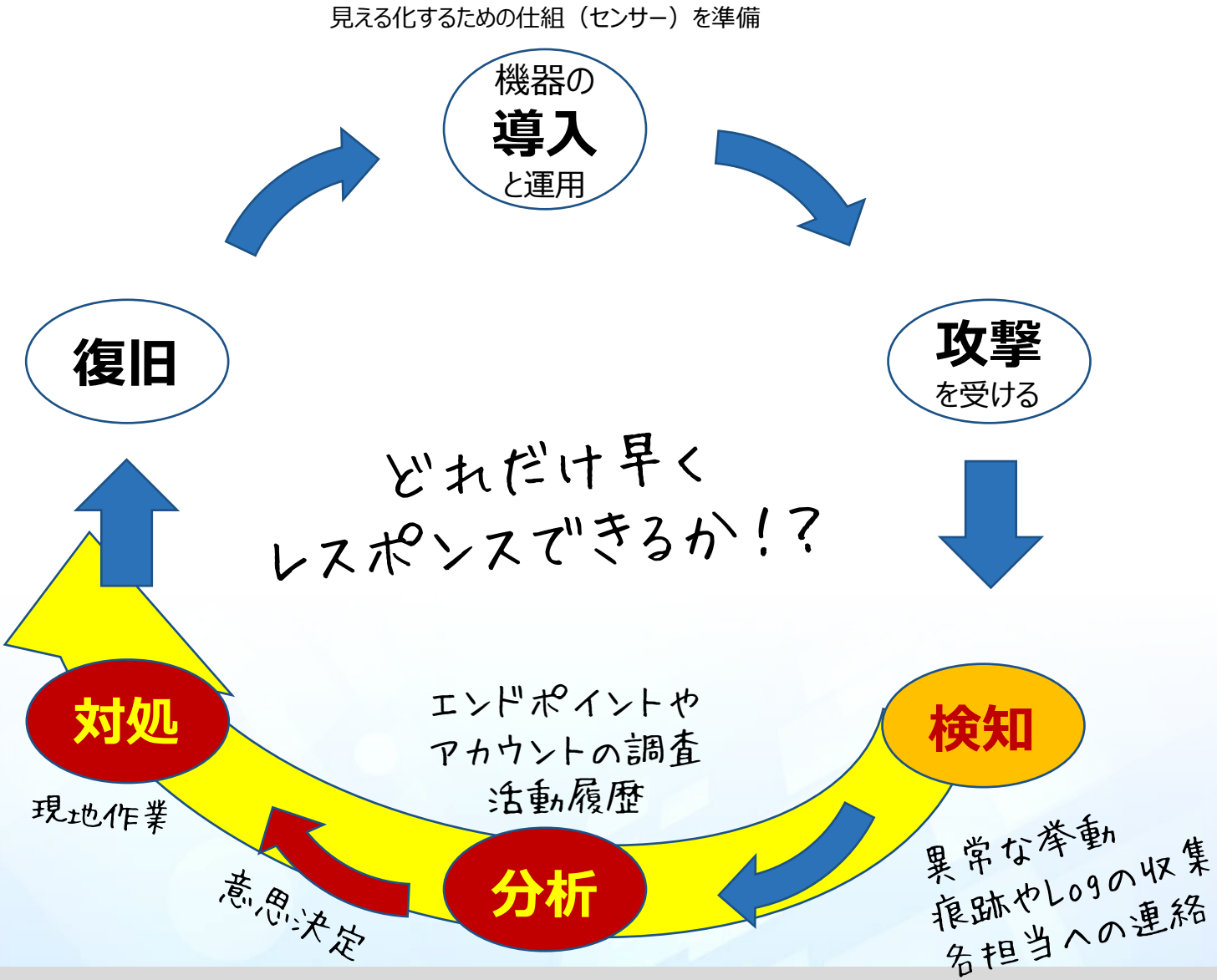
被害者に電話をかけるなどして対面することなく信頼させ、
指定した預貯金口座への振込みその他の方法により、
不特定多数の者から現金等をだまし取る犯罪を特殊詐欺といいます。
オレオレ詐欺以外にも巧妙な手口が多様に存在しますので、手口の特徴をしっかり把握しておきましょう。

犯人たちは防犯意識のない人を狙っている

犯人の事前準備　＆　防犯意識の欠如　⇒　だから犯行が成功



ここが最も重要！



GSX
GLOBAL SECURITY EXPERTS

本格攻撃前に
次の攻撃を
止める

防犯意識があれば…

- **ダマされない！　何かおかしい？と気づいたら相談できる**

防犯意識があれば…

- ダマされない！　何かおかしい？と気づいたら相談できる

気付ける

さらに、端末の挙動確認や事故対応を**遠隔で**行う

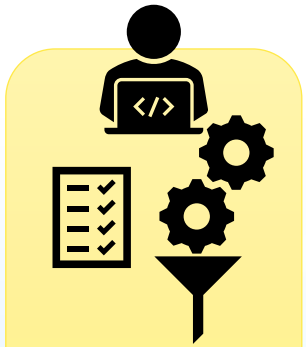
技術的に大きく進歩！

テレワークで遠隔に散らばった端末の管理や可視化は問題だった

GSX
GLOBAL SECURITY EXPERTS

アンチウィルス → 資産管理 → 衛生管理 → 端末内部挙動検知

今までの課題



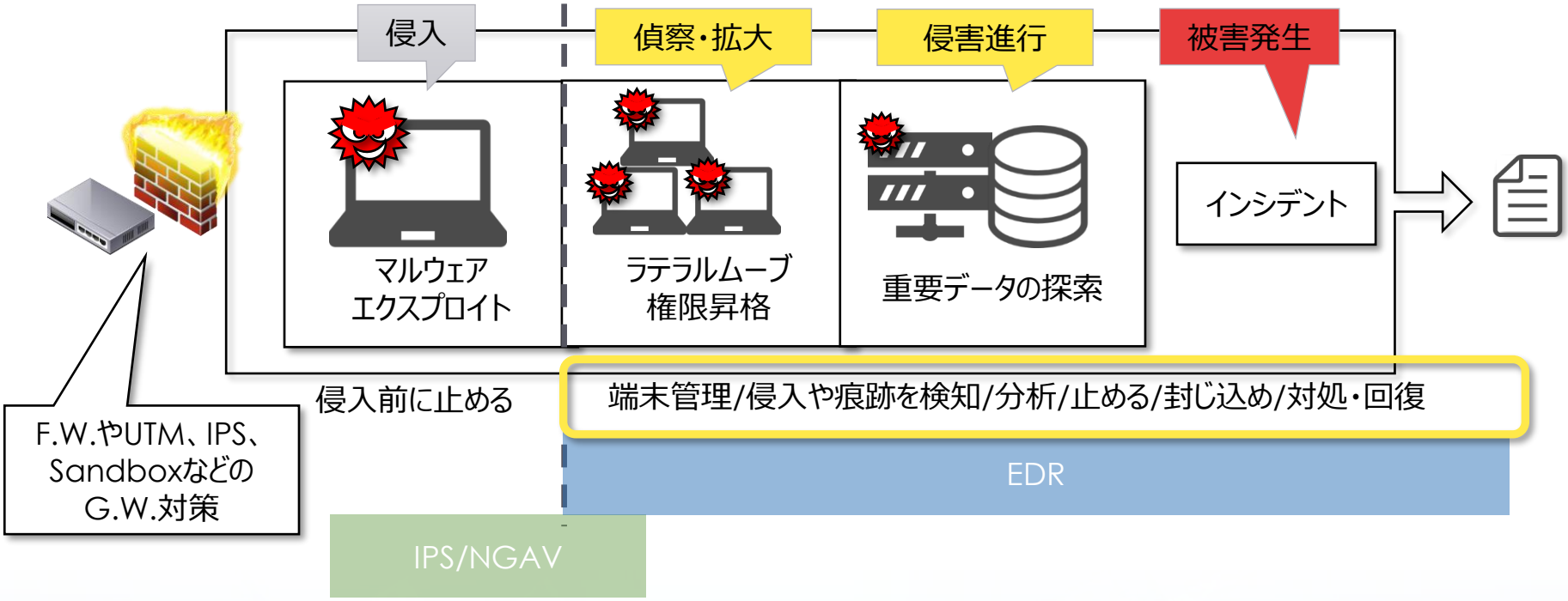
今までの対策だけでは防げない

管理がバラバラ
内部可視化には
運用が大変

マルウェアが変わる
資産が変わる
アプリが変わる

運用が…
破綻する

ここ数年で一気に進化したEDR



いまや「EDR」は感染検知だけじゃない

端末の動きが見えていれば…

- **内部で何をしているのか？侵入された後の動き**

端末の動きが見えていれば…

- **内部で何をしているのか？侵入された後の動き**

気付ける

「見えなかった動き」が見える。さらに「遠隔対応」できる。

GSX
GLOBAL SECURITY EXPERTS

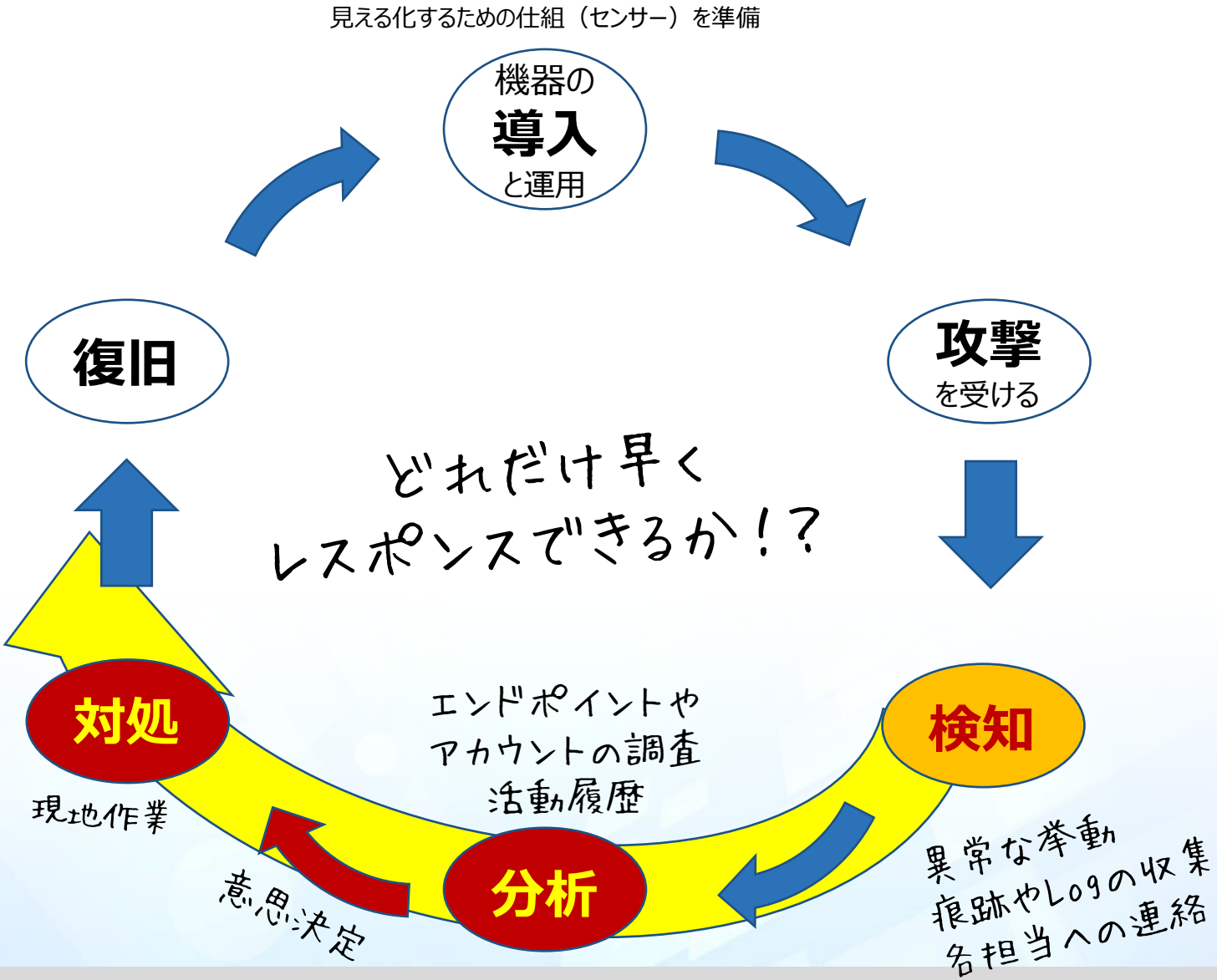
中の動きを可視化し、即応できる準備を

テレワークでも即応できるように

通常はアクセスしないIDから、時間帯から、エリアから
普段発生しないリクエストや、業務上使わないプロトコル
特徴的なスキャン、PowerShell、規則的すぎる挙動

→ **ここを見える化できる**
これは**内部不正にも有効**

ここが最も重要！



実被害前に
次の攻撃を
止める

まとめ

環境が大きく変わった

1. システムのクラウドサービスへの移行

2. テレワークへの移行

3. サイバー犯罪の高度化/頻発化

準備するには何が必要か？（課題解決のレシピ）

GSX
GLOBAL SECURITY EXPERTS

全社教育と訓練 — **防犯意識**

情報資産の棚卸し と ロードマップ — **アセスメント**

センサー と 状況可視化 — **仕組を準備**

組織体制強化 ＜CSIRT & SOC＞ — **体制を準備**

上記4項目は全て **厚労省**の**監督指針・還元資料**や**報告書**
また経産省のサイバーセキュリティ経営ガイドライン に明記

準備の全体像

GSX
GLOBAL SECURITY EXPERTS

サイバー脅威を、小さくても認識共有

守る情報を棚卸・リスクアセスメント

何を守るか？を明確にし、どこまで対応できるか？想定外は無いのか？リスクを見える化

ロードマップ

組織体制

検知した脅威を早期に分析し、対処する
仕組みの構築(社内体制)

システム化

外部からの攻撃を検知する仕組みの導入
(センサー/統合ログ管理/監視体制)

教育・訓練による、意識と運用の定着

GSX
GLOBAL SECURITY EXPERTS

まず必要なのは社内の

防犯意識

侵入されてるかも・盗まれるかも・壊されるかも

何を守りたいか？本気で考えられる
ポリシーやルールの意味が分かる
自発的に「見える化」や「声がけ」ができる

サイバー犯罪を体験⇒みんなで認識共有

守る情報を棚卸・リスクアセスメント

何を守るか？を明確にし、使っているシステムを棚卸し⇒リスクを見える化

なんのためにやっているのか？
が分かる！

遠隔でもリアルタイムで状況が分かる！対処できる！

ロードマップ

組織体制

検知した脅威を早期に分析し、対処する仕組みの構築(社内体制)

システム化

外部からの攻撃を検知する仕組みの導入(センサー/統合ログ管理/監視体制)

教育・訓練による、意識と運用の定着

犯人のほうが、

- ちゃんと「調べて」
- ちゃんと「リスト化して」
- ちゃんと「連携を取って」
- ちゃんと「PDCAを回して」…

ちゃんと（犯行の）準備している

GSX
GLOBAL SECURITY EXPERTS

事前準備

守る側も

- ちゃんと「調べて」
- ちゃんと「リスト化して」
- ちゃんと「人を育てて」
- ちゃんと「連携を取って」…

迎え撃つための

ちゃんと　準備を！

サイバー犯罪に対抗するために

「常に狙われている」前提にたって
防犯意識を全社で醸成する

犯行に対応するためには
手口を知り、具体的な対応策を

犯人は常に犯行の準備をしている
テレワークでも見える化/管理できる
事前準備を整え対抗しよう

みんなで防犯！犯罪者を許さない！　いま行動を！

緊急対応サービス

情報セキュリティインシデントに関わる緊急事態に、
迅速なご支援をいたします。

もし、万が一、緊急で対応する事態が発生した際には

03-3578-9001

https://www.gsx.co.jp/

防犯・保安活動と同じように

備えましょう！

GLOBAL
SECURITY
EXPERTS

GSX

GLOBAL
SECURITY
EXPERTS