2022年
サイバーセキュリティレポート
紹介動画

ご紹介内容

1章:2022年マルウェア検出統計

2章:マルウェアファミリーに着目したESET統計情報と上位マルウェアの紹介

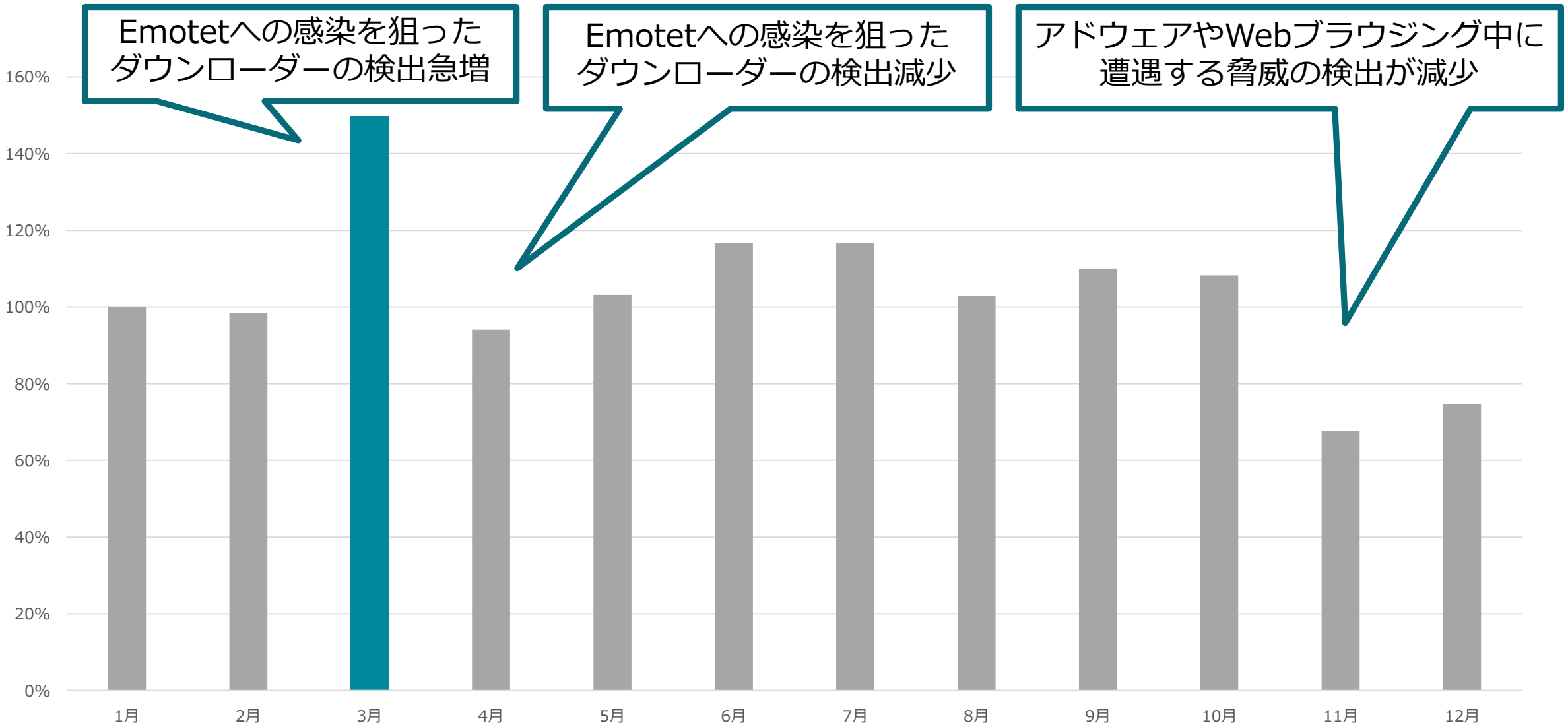
3章:2022年に公表された不正アクセスによるセキュリティインシデントについて

4章:病院を狙うサイバー攻撃の増加と背景

5章:なぜ、脆弱性対応ができないのか

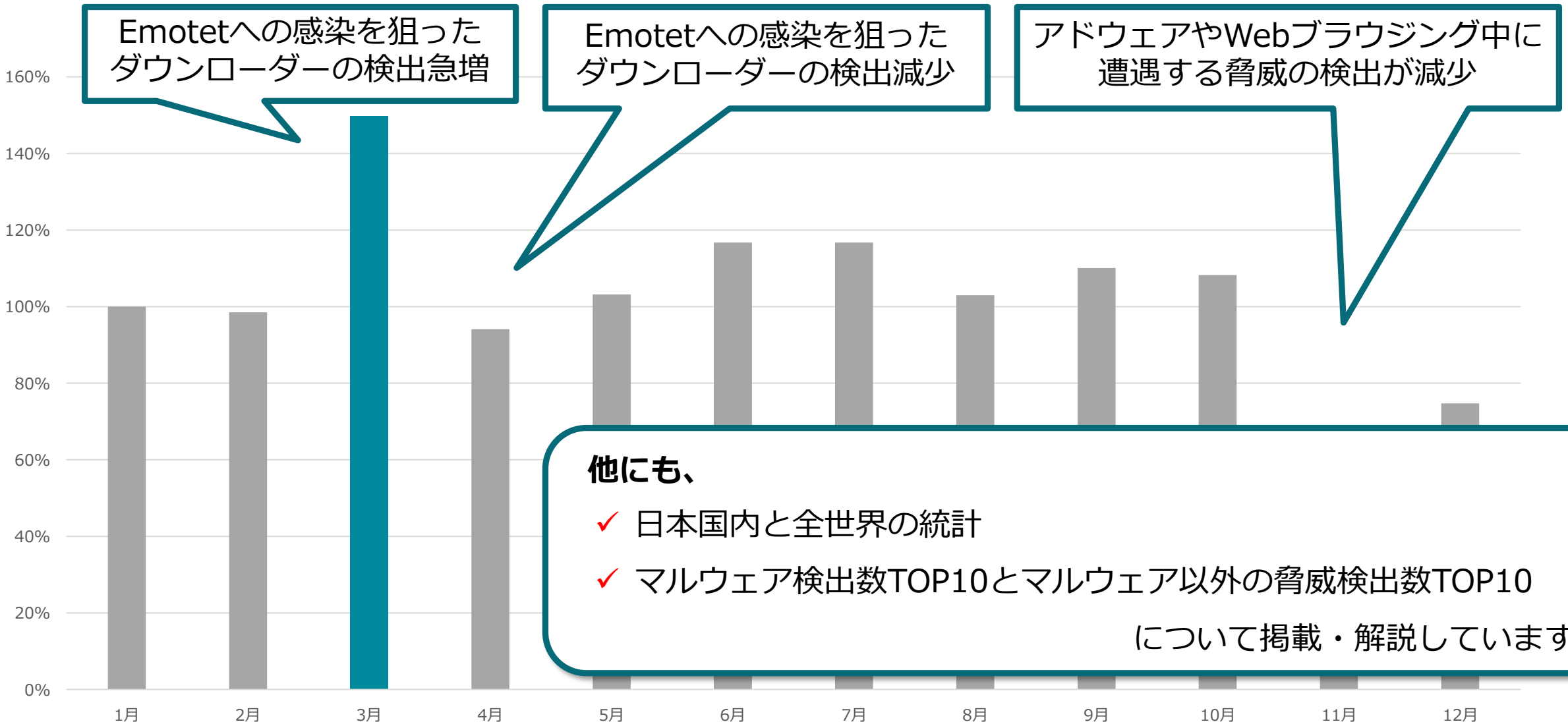
6章:Web証明書/PKIの最新動向と展望

2022年マルウェア検出統計　～国内検出数月別推移～



国内におけるマルウェア検出数の月別推移（2022年）

2022年マルウェア検出統計　～国内検出数月別推移～



国内におけるマルウェア検出数の月別推移（2022年）

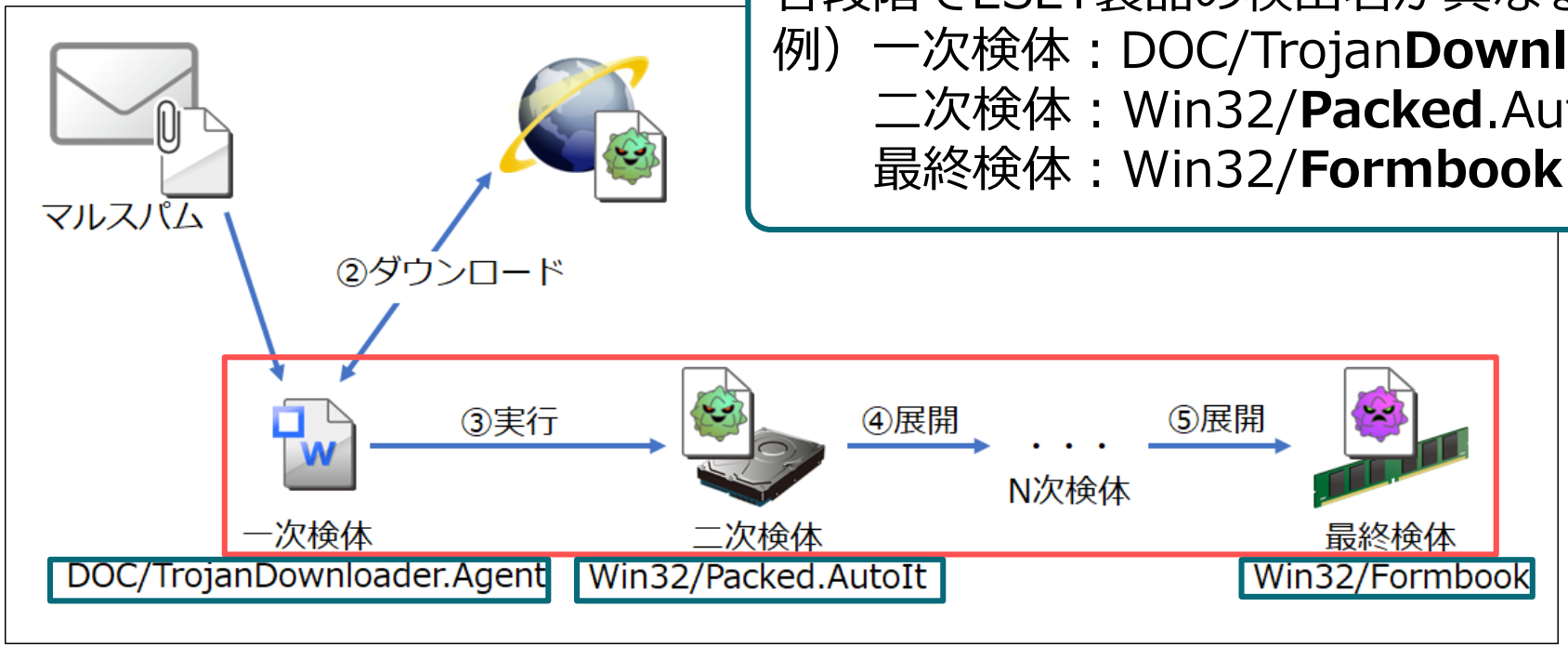
他にも、

- ✓ 日本国内と全世界の統計
- ✓ マルウェア検出数TOP10とマルウェア以外の脅威検出数TOP10

について掲載・解説しています

マルウェアの高度化に伴い、
近年、複数の段階を経て目的のマルウェアに感染させる挙動が多く見られるようになった

各段階でESET製品の検出名が異なる
例）一次検体：DOC/Trojan**Downloader**.Agent
　　二次検体：Win32/**Packed**.AutoIt
　　最終検体：Win32/**Formbook**



マルスパムの添付ファイルからマルウェア感染する流れの例

段階ごとの検出名を理解する

▼

検知ログの分析で役に立つ
- ✓ 組織に迫ったマルウェア
- ✓ 感染時の影響

マルウェアファミリーに着目したESET統計情報と上位マルウェアの紹介

マルウェアファミリー名を含むESETマルウェア検出数上位（2022年・国内）
1位のMSIL/Spy.AgentTeslaの検出数を100とした相対値で算出

順位	ESET検出名	相対値	マルウェアファミリー名
1	MSIL/Spy.AgentTesla	100.0	AgentTesla
2	Win32/Formbook	61.7	Formbook
3	INF/Conficker	26.3	Conficker
4	Win32/TrojanDownloader.Delf	23.7	Delf
5	Win32/PSW.Fareit	18.9	Fareit（別名：Pony、Siplog）
6	Win32/Conficker	13.0	Conficker
7	JS/TrojanDownloader.Nemucod	10.5	Nemucod
8	MSIL/TrojanDownloader.Tiny	5.5	Tiny（別名：Tinba）
9	Win32/Rescoms	5.4	Rescoms（別名：Remcos）
10	Win32/Netsky	4.2	Netsky

情報窃取型のマルウェアの１つ
2014年頃から確認されており、MaaS
（Malware as a Service）として提供されている

AgentTeslaを含む情報窃取型マルウェアは安価で購入可能
→2023年も猛威を奮うと考えられるため警戒が必要

マルウェアファミリーに着目したESET統計情報と上位マルウェアの紹介

マルウェアファミリー名を含むESETマルウェア検出数上位（2022年・国内）
1位のMSIL/Spy.AgentTeslaの検出数を100とした相対値で算出

順位	ESET検出名	相対値	マルウェアファミリー名
1	MSIL/Spy.AgentTesla	100.0	AgentTesla
2	Win32/Formbook	61.7	Formbook
3	INF/Conficker	26.3	Conficker
4	Win32/TrojanDownloader.Delf	23.7	Delf
5	Win32/PSW.Fareit	18.9	Fareit
6	Win32/Conficker	13.0	Confi
7	JS/TrojanDownloader.Nemucod	10.5	Nemu
8	MSIL/TrojanDownloader.Tiny	5.5	Tiny
9	Win32/Rescoms	5.4	Resco
10	Win32/Netsky	4.2	Netsky

情報窃取型のマルウェアの１つ
2014年頃から確認されており、MaaS
（Malware as a Service）として提供されている

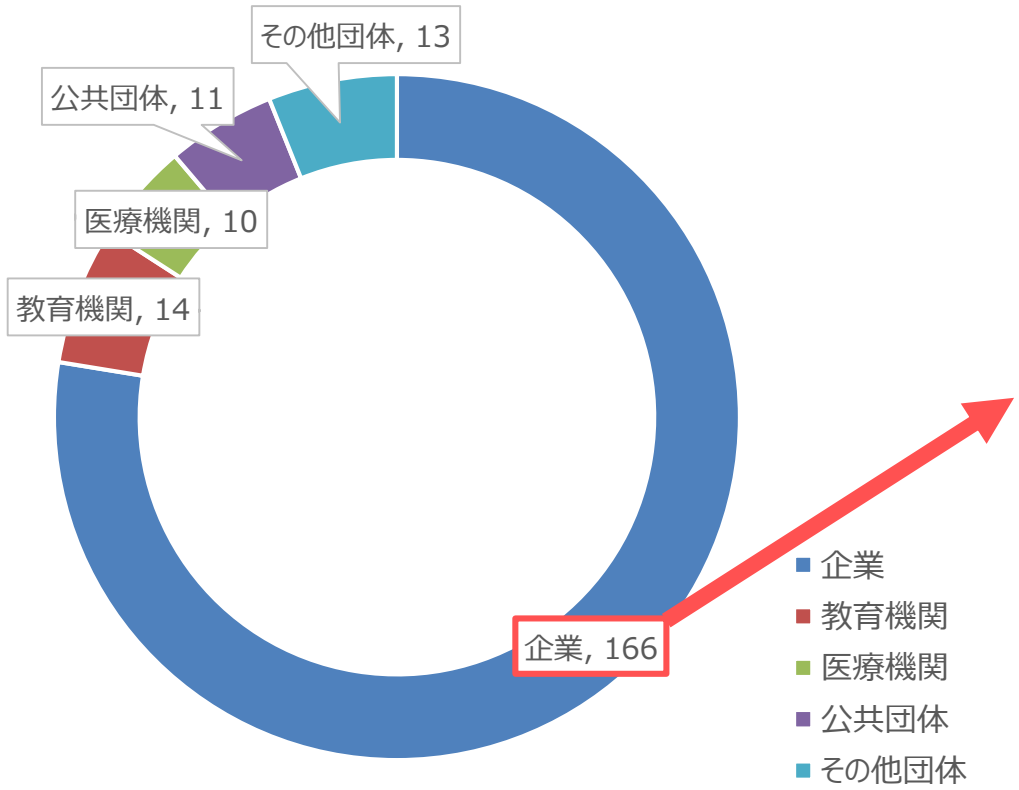
他にも

- ✓ 検出数TOP10に入ったマルウェアファミリー解説
- ✓ AgentTeslaの感染段階ごとの解析結果
- ✓ AgentTeslaの窃取対象リスト

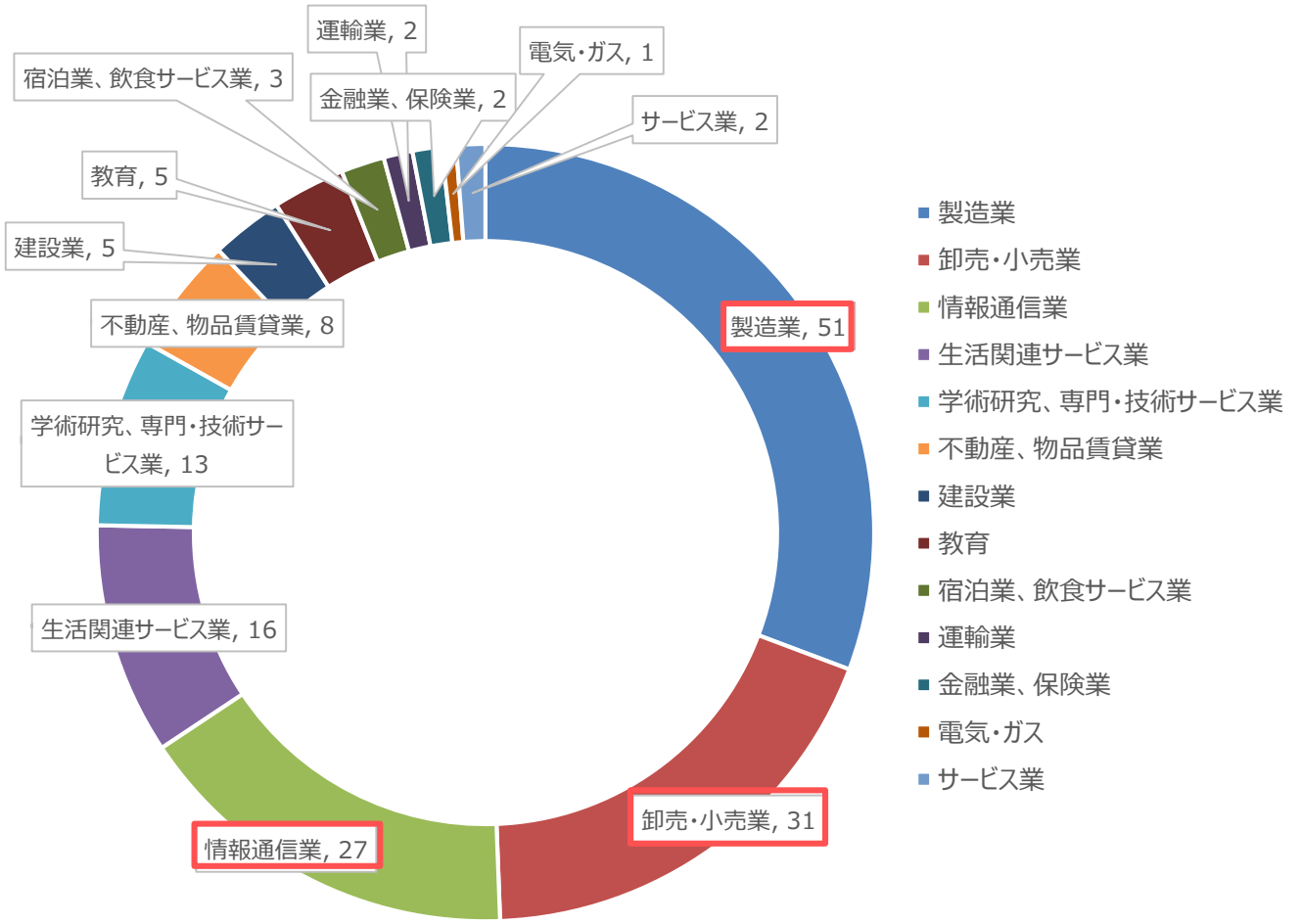
について掲載・解説しています

AgentTeslaを含む情報窃取型マルウェアは安価で購入可能
→2023年も猛威を奮うと考えられるため警戒が必要

2022年もさまざまなセキュリティインシデントが発生
第3章では、不正アクセスによるセキュリティインシデントを収集・分類し、解説



セキュリティインシデントの組織別分類（2022年、国内）



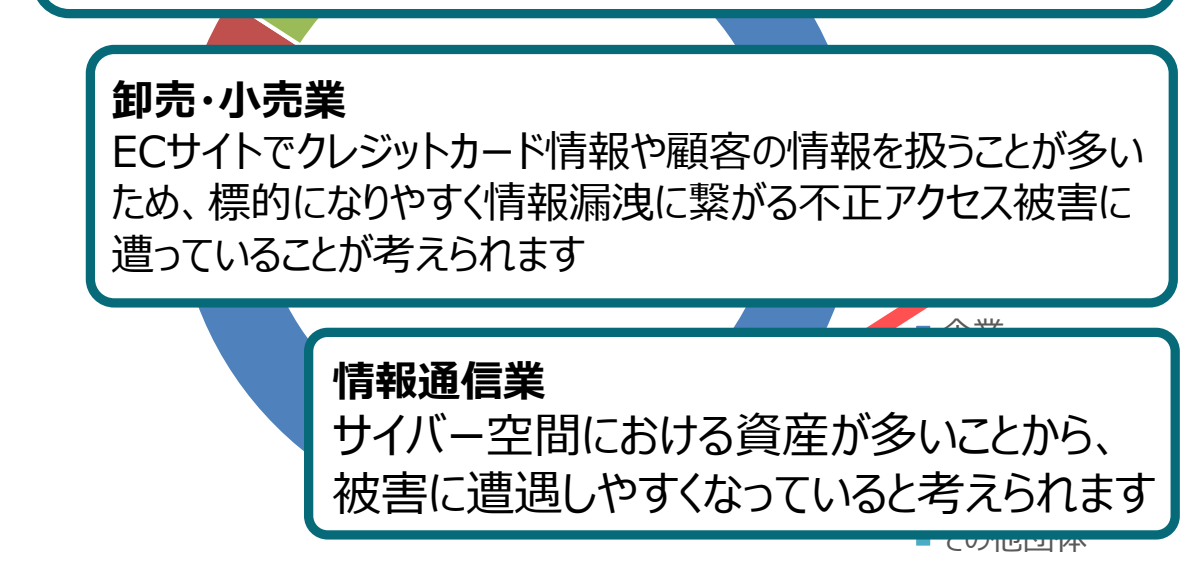
セキュリティインシデントの業種別分類（2022年、国内）

2022年もさまざまなセキュリティインシデントが発生
第3章では、不正アクセスによるセキュリティインシデントを収集・分類し、解説

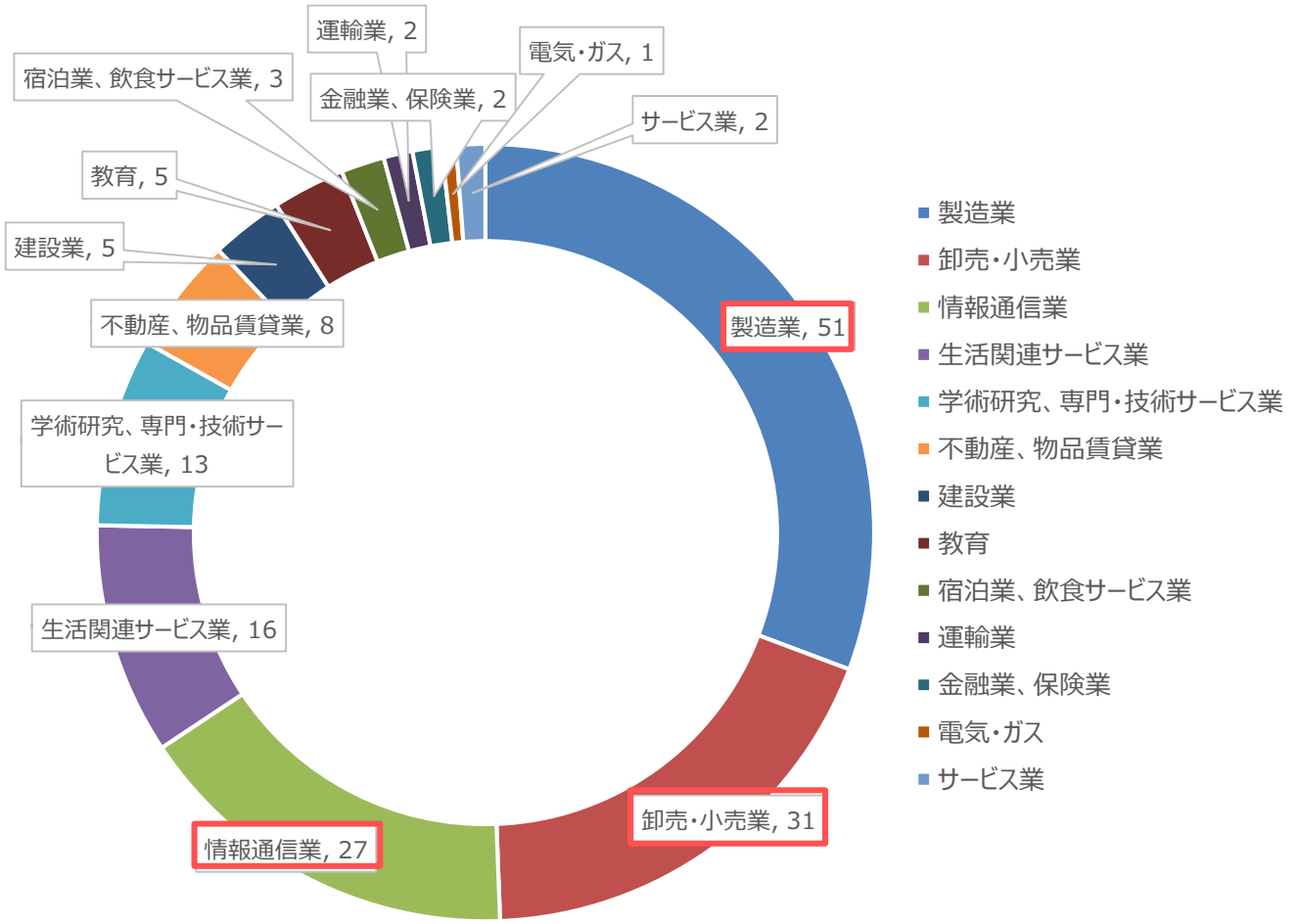
製造業
企業数が多く、さまざまな被害が生じています
関連企業やグループ会社が多いため、サプライチェーン攻撃による情報漏洩やランサムウェア被害といった特定の企業を狙った被害が起きていることも考えられます

卸売・小売業
ECサイトでクレジットカード情報や顧客の情報を扱うことが多いため、標的になりやすく情報漏洩に繋がる不正アクセス被害に遭っていることが考えられます

情報通信業
サイバー空間における資産が多いことから、被害に遭遇しやすくなっていると考えられます



セキュリティインシデントの組織別分類（2022年、国内）



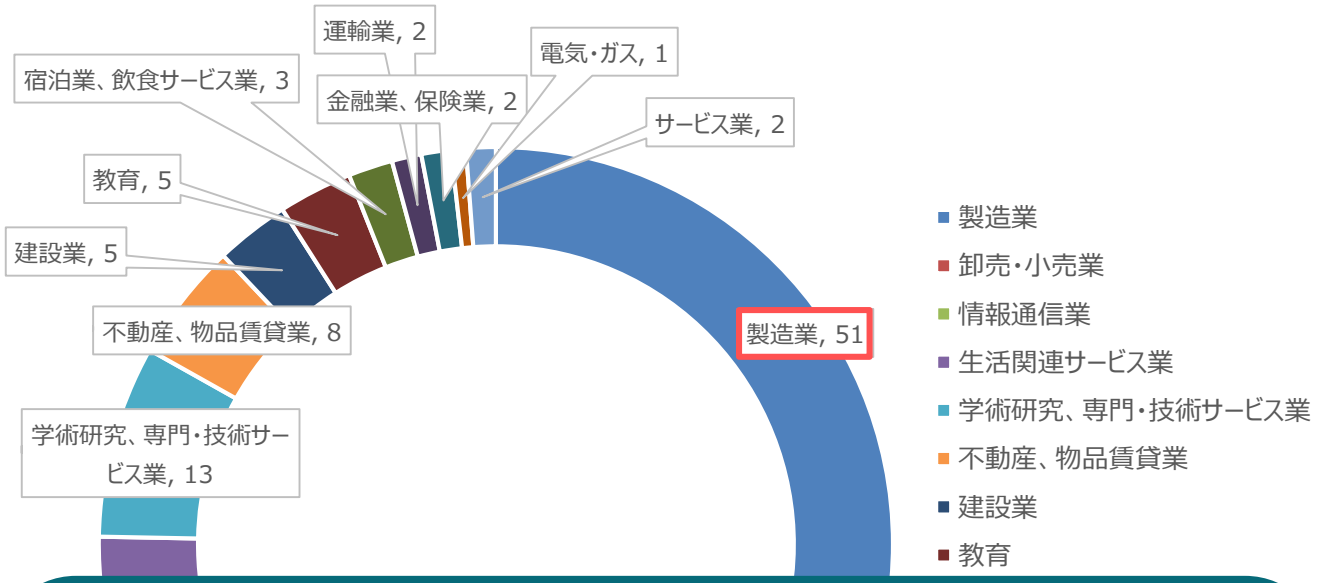
セキュリティインシデントの業種別分類（2022年、国内）

2022年もさまざまなセキュリティインシデントが発生
第3章では、不正アクセスによるセキュリティインシデントを収集・分類し、解説

製造業
企業数が多く、さまざまな被害が生じています
関連企業やグループ会社が多いため、サプライチェーン攻撃による情報漏洩やランサムウェア被害といった特定の企業を狙った被害が起きていることも考えられます

卸売・小売業
ECサイトでクレジットカード情報や顧客の情報を扱うことが多いため、標的になりやすく情報漏洩に繋がる不正アクセス被害に遭っていることが考えられます

情報通信業
サイバー空間における資産が多いことから、被害に遭遇しやすくなっていると考えられます



セキュリティインシデントの組織別分類（2022年、国内）

他にも

- ✓ 組織規模別、業種別や不正アクセスによる被害とその原因別の分類
- ✓ 集計結果で多く確認された被害原因への対策

について掲載・解説しています

病院を狙うサイバー攻撃の増加とその背景

ランサムウェアをはじめ
病院・診療所を狙うサイバー攻撃が増加

病院・診療所を狙うサイバー攻撃の影響

- ✓ 診療業務の停止、または縮小
- ✓ 診療会計業務の停止
- ✓ 受診者の住所、氏名、年齢、既往歴などの個人情報の漏えい

→フィジカル空間へ大きな影響

▼ 背景には

- ✓ 医療分野における情報化
- ✓ 外部ネットワークとの接続増加 etc

時期		医療機関	被害種別
2021年	1月	公立病院（静岡県）	不正アクセス
	5月	公立病院（大阪府）	ランサムウェア
	7月	民間病院（神奈川県）	不正アクセス
	10月	民間病院（静岡県）	ランサムウェア
	10月	公立病院（徳島県）	ランサムウェア
2022年	1月	大学付属病院（東京都）	マルウェア感染
	1月	民間病院（愛知県）	ランサムウェア
	2月	大学付属病院（愛知県）	不正アクセス
	3月	公立病院（沖縄県）	マルウェア感染（Emotet）
	3月	公立病院（栃木県）	マルウェア感染（Emotet）
	4月	民間病院（大阪府）	ランサムウェア
	5月	民間病院（岐阜県）	不正アクセス
	6月	民間病院（徳島県）	ランサムウェア
	10月	民間病院（静岡県）	ランサムウェア
	10月	公立病院（大阪府）	ランサムウェア
	12月	民間病院（石川県）	不正アクセス

病院を狙うサイバー攻撃の増加とその背景

ランサムウェアをはじめ
病院・診療所を狙うサイバー攻撃が増加

病院・診療所を狙うサイバー攻撃の影響

- ✓ 診療業務の停止、または縮小
- ✓ 診療会計業務の停止
- ✓ 受診者の住所、氏名、年齢、既往歴などの個人情報の漏えい

→フィジカル空間へ大きな影響

▼ 背景には

- ✓ 医療分野における情報化
- ✓ 外部ネットワークとの接続増加 etc

時期		医療機関	被害種別
2021年	1月	公立病院（静岡県）	不正アクセス
	5月	公立病院（大阪府）	ランサムウェア
	7月	民間病院（神奈川県）	不正アクセス
	10月	民間病院（静岡県）	ランサムウェア
	10月	公立病院（徳島県）	ランサムウェア
2022年	1月	大学付属病院（東京都）	マルウェア感染
	1月	民間病院（愛知県）	ランサムウェア
	2月	大学付属病院（愛知県）	不正アクセス
	3月	公立病院（沖縄県）	マルウェア感染（Emotet）

他にも

- ✓ 2021年以降に発生した医療機関の被害事例
- ✓ 医療機関へのサイバー攻撃増加の背景
- ✓ サイバー攻撃対策

について掲載・解説しています

なぜ、対策方法が公開されている脆弱性が、対応されず放置されてしまうのか

脆弱性対応が放置されてしまう理由

- ✓ 脆弱性情報の収集不足
- ✓ 不十分なリスク評価
- ✓ リソース不足
- ✓ 優先順位
- ✓ 保守サポート期間切れ

▼ これらの背景には、さまざまな要因が…

- ✓ 日本の商習慣
- ✓ 運用・保守業務の責任範囲の認識のずれなどの影響 etc

IPA 情報セキュリティ10大脅威 2023

■「情報セキュリティ10大脅威 2023」

圏外：昨年はランクインしなかった脅威

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5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	4位
7位	不正アプリによるスマートフォン利用者への被害	6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの個人情報の窃取	8位	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の不当請求による金銭被害	10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

なぜ、脆弱性対応が放置されるのか

なぜ、対策方法が公開されている脆弱性が、対応されず放置されてしまうのか

脆弱性対応が放置されてしまう理由

- ✓ 脆弱性情報の収集不足
- ✓ 不十分なリスク評価
- ✓ リソース不足
- ✓ 優先順位
- ✓ 保守サポート期間切れ

▼ これらの背景には、さまざまな要因が…

- ✓ 日本の商習慣
- ✓ 運用・保守業務の責任範囲の認識のずれなどの影響 etc

IPA　情報セキュリティ10大脅威 2023

■「情報セキュリティ10大脅威 2023」

圏外：昨年はランクインしなかった脅威

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5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	4位
7位	スマートフォン利用者を狙った攻撃	6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位
8位	インターネット上のサービスからの個人情報の窃取	8位	脆弱性対策情報の公開に伴う悪用増加	6位
10位	インターネット上のサービスへの不正ログイン	9位	不注意による情報漏えい等の被害	10位
圏外	ワンクリック請求等の不当請求による金銭被害	10位	犯罪のビジネス化（アンダーグラウンドサービス）	圏外

脆弱性が対応されていれば防げたインシデントも

なぜ、対策方法が公開されている脆弱性が、対応されず放置されてしまうのか

脆弱性対応が放置されてしまう理由

- ✓ 脆弱性情報の収集不足
- ✓ 不十分なリスク評価
- ✓ リソース不足
- ✓ 優先順位
- ✓ 保守サポート期間切れ

▼ これらの背景には、さまざまな要因が…

- ✓ 日本の商習慣
- ✓ 運用・保守業務の責任範囲の認識のずれなどの影響

etc

IPA 情報セキュリティ10大脅威 2023

■「情報セキュリティ10大脅威 2023」

圏外：昨年はランクインしなかった脅威

前年順位	個人	順位	組織	前年順位
1位	フィッシングによる個人情報等の詐取	1位	ランサムウェアによる被害	1位
2位	ネット上の誹謗・中傷・デマ	2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位	標的型攻撃による機密情報の窃取	2位
4位	クレジットカード情報の不正利用	4位	内部不正による情報漏えい	5位
5位	スマホ決済の不正利用	5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	4位
7位	スマートフォン利用を狙った攻撃	6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	7位
6位	偽警告によるインターネット詐欺	7位	ビジネスメール詐欺による金銭被害	8位

脆弱性が対応されていれば防げたインシデントも

他にも

- ✓ サプライチェーンや予算・体制による影響
- ✓ ランニングコスト削減とアウトソース

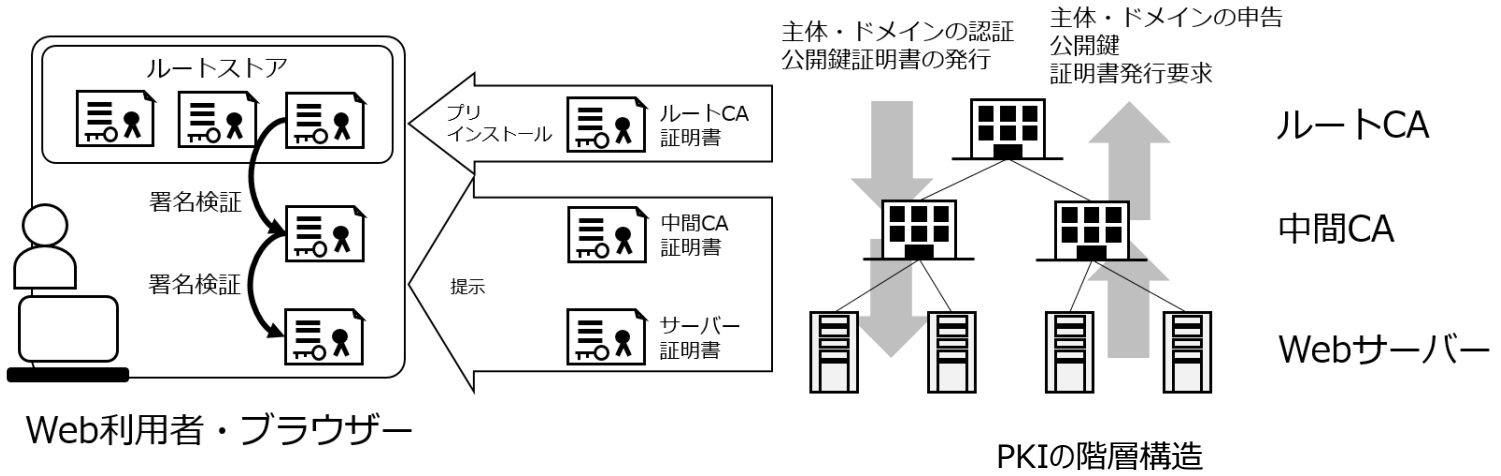
について掲載・解説しています

Web証明書／PKIの最新動向と展望

PKI（ Public Key Infrastructure）は、公開鍵証明書とCAの階層構造で構成された認証基盤
信頼性が問われるインシデント後、信頼向上のための対策を行ってきた

公開鍵証明書
公開鍵に加えて、Webサイトのドメインや所有者、証明書の発行元を記載

CA（Certification Authority）
Webサイト管理者とドメインの関係を確認し、サーバー証明書を発行している
信頼性の高い第三者機関



2011年に**不正証明書大量発行**が発生
さまざまな対策を実施
- ✓ 業界団体でCA運用ルール策定
- ✓ 証明書発行をログに記録し見える化
- ✓ ドメインとCAの関係を検証するしくみ

他にも
- ✓ PKIの仕組み
- ✓ PKI関連の過去のインシデントや改善策
- ✓ 近年のPKIに関するトピックや今後の展望

について掲載・解説しています

キヤノンマーケティングジャパンが提供する最新のセキュリティ情報

最新のセキュリティ動向やキーワード解説のほか
サイバーセキュリティラボがまとめた
日本におけるマルウェア動向を
詳細なレポートにて提供

情報収集にご活用ください

サイバーセキュリティ情報局 **検索**

ご視聴ありがとうございました。